高等教育機関の情報セキュリティ対策のためのサンプル規程集

（2017 年版）

2017 年 10 月 17 日

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

編者代表　曽根秀昭
編者　　岡田仁志，小川賢
著者　　飯田勝吉，板垣毅，稲葉宏幸，上田浩，上原哲太郎，岡田仁志，岡部寿男，
岡村耕二，小川賢，折田彰，垣内正年，笠原義晃，金谷吉成，上岡英史，
貴志武一，木下宏揚，楠元範明，佐藤周行，佐藤慶浩，下川俊彦，庄司勇木，
須川賢洋，鈴木孝彦，曽根秀昭，高井昌彰，高倉弘喜，高橋郁夫，竹内義則，
辰己丈夫，谷本茂明，中西通雄，中野博隆，中村素典，中山雅哉，西村浩二，
野川裕記，野田英明，長谷川明生，林田宏三，平塚昭仁，冨士原裕文，布施勇，
前野譲二，松下彰良，丸橋透，三島健稔，南弘征，湯浅富久子

「高等教育機関の情報セキュリティ対策のためのサンプル規程集」（以下、「サンプル規程集」という。）の検討は、大学共同利用機関法人情報・システム研究機構国立情報学研究所（以下、「国立情報学研究所」という。）学術情報ネットワーク運営・連携本部「国立大学法人等における情報セキュリティポリシー策定作業部会」と、社団法人電子情報通信学会「ネットワーク運用ガイドライン検討ワーキンググループ」との合同で実施された。全国共同利用情報基盤センター群および国立大学法人等情報化推進協議会とも連携し、文部科学省の大臣官房政策課情報化推進室と研究振興局情報課、および内閣官房情報セキュリティセンターの協力も得た。運営と取りまとめの支援は、みずほ情報総研株式会社に委託した。

サンプル規程集は、「ネットワーク運用ガイドライン検討ワーキンググループ」による「高等教育機関におけるネットワーク運用ガイドライン（第二版）」（平成 18 年 1 月）と、内閣官房情報セキュリティセンターの「政府機関の情報セキュリティ対策のための統一基準」（2005 年 12 月）をもとに、多くの機関の例も参考にしつつ、「国立大学法人等における情報セキュリティポリシー策定作業部会」での検討を経て 2007 年 2 月に初めて策定された。以降、「政府機関の情報セキュリティ対策のための統一基準」の改定内容、ならびに大学における実際の策定事例や公開以後に指摘された課題等を踏まえ、大学共同利用機関法人情報・システム研究機構国立情報学研究所学術情報ネットワーク運営・連携本部に設置された「高等教育機関における情報セキュリティポリシー推進部会」での検討結果をもとに、数回の改定を実施している。本文書は、内閣官房情報セキュリティセンター（現内閣サイバーセキュリティセンター）が 2016 年 8 月に公表した「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」に準拠するものである。2017 年版では、情報セキュリティインシデント対応チーム（CSIRT）の設置及び運用に関する内容の強化その他全体にわたって改訂が行われたことに対応した。

この文書と関連資料はインターネットにより次のところで配布している。

国立大学法人等における情報セキュリティポリシー策定について（国立情報学研究所）
https://www.nii.ac.jp/service/sp/

目　次

本文書について

１．背景

大学の教育、研究、運営などの活動における情報化の進展とともに、情報セキュリティが重要になっている。情報セキュリティレベルを確保し向上させていくために、各大学においてその必要性を十分に認識し、情報セキュリティの基本方針と組織・体制、対象を決定して、情報セキュリティポリシー、実施規程、啓発用テキストなどを作成することが必要である。しかし、情報セキュリティポリシー等の策定は、大学における教学との関係、大学の組織および運営における意思決定や運用・利用の扱い方などを考慮しなければならず、あるいは法律・制度や組織運営、情報・通信・セキュリティ技術等に関する専門知識が求められるために、取り組みが難しい課題である。

この取り組みを支援するために、例えば、全国共同利用大型計算機センター群による「大学のセキュリティポリシーに関する研究会」は「大学における情報セキュリティポリシーの考え方」（平成 14 年 5 月）を作成して、大学における問題点と具体例の分析などを示した。あるいは、電子情報通信学会は「ネットワーク運用ガイドライン検討ワーキンググループ」を設置し、ネットワークの健全な運用・利用の実現に資することを願って「高等教育機関におけるネットワーク運用ガイドライン」（平成 15 年 4 月）を作成し各高等教育機関が独自の規程類を整備するためのキャンパスネットワークの運用管理ポリシーと実施要領策定に関する指針を提言した。

これらの資料によって、考え方や指針、解説が提供されたが、これらを参照するだけで上述の難しい課題を解決することは困難であり、さらに参考となる具体的なサンプル規程集や詳細な運用マニュアルを必要とする意見も少なくない。また、情報セキュリティに関する最近の状況として、個人情報の保護に関する法律の施行や「政府機関の情報セキュリティ対策のための統一基準」（以下、「政府機関統一基準」）の制定があり、セキュリティ水準の向上も求められている。国立大学においては、平成 16 年度の法人化後に情報システムの運用や情報セキュリティの確保を実施する組織と予算について、全学的方針と新しい制度の構築が新しい課題として加わった。

このような高等教育機関を取り巻く社会情勢の変化をガイドラインに反映させる必要があり、高等教育機関における情報セキュリティポリシーのサンプル規程集として、本文書の作成を検討することとなった。

２．経緯

本文書の検討は、国立情報学研究所 学術情報ネットワーク運営・連携本部が設置した「国立大学法人等における情報セキュリティポリシー策定作業部会」（以下、「策定作業部会」）と、社団法人電子情報通信学会が企画室のもとに設置した「ネットワーク運用ガイドライン検討ワーキンググループ」（以下、「検討 WG」）との合同で実施された。

国立情報学研究所の策定作業部会は、「大学における情報セキュリティポリシーの考え方」から政府機関統一基準を踏まえた見直しを行い、国立大学法人等に適した標準的かつ活用可能な情報セキュリティポリシーの策定を行って各大学へ提供するために設置された。ネットワーク，認証，事務及びこれらの運用が密接に関係することから、策定作業部会には国立情報学研究所のネットワーク作業部会，認証作業部会，学術ネットワーク研究開発センター、ならびに全国共同利用情報基盤センター群のコンピュータ・ネットワーク研究会と認証研究会、および国立大学法人等情

報化推進協議会とも連携して対応し、文部科学省の大臣官房政策課情報化推進室と研究振興局情報課、および内閣官房情報セキュリティセンターの協力も得た。

電子情報通信学会の検討 WG は、平成 15 年度からの第二期で策定してきた「高等教育機関におけるネットワーク運用ガイドライン（第二版）」を完成させて成果を公開するために活動を延長して利用者，教育・倫理の領域を中心に引き続き検討することとして、電子情報通信学会の技術と社会・倫理研究専門委員会とインターネットアーキテクチャ研究専門委員会から協力を得た。

策定作業部会と検討 WG は、平成 18 年 8 月に合同で検討と策定を開始した。総論・体制，ネットワーク運用，認証運用，事務利用，利用者，教育・倫理の 6 つの領域分科会を設定し、領域ごとに電子メールを中心とした検討と会合を行った。各領域に幹事及び幹事補佐をおいて、検討をとりまとめ、あるいは関連する領域分科会と連絡し、必要に応じて他の分科会に参加した。また各領域の幹事と策定作業部会の主査・副主査、検討 WG の主査・幹事により幹事会を構成し、全体の調整にあたった。また、国立情報学研究所の研究部門の共同研究課題（国立情報学研究所・岡田仁志，代表・神戸学院大学・小川賢）による研究とも連携した。策定作業部会の運営と取りまとめの支援は、外部（みずほ情報総研株式会社）に担当を委託した。策定作業部会と検討 WG はいずれも年度末までの期限で設置された。その成果を「高等教育機関の情報セキュリティ対策のためのサンプル規程集」としてとりまとめて、平成 19 年 2 月にインターネットで配布を始めた。これには、想定される規程体系のうち基本方針、規程類から手順書、教育テキストまで 17 本のサンプル規程を収めて、本文 298 ページ（ほかに前文 7 ページ）であった。また、成果の普及のため「大学における情報セキュリティおよび電子認証基盤に関するワークショップ」および電子情報通信学会総合大会において説明を実施した。

平成 18 年度の活動では時間的制約などで公開レベルまで精査できずサンプル規程集の公開対象外とした部分があり、情報セキュリティポリシーの規則体系としての完成度を高める要請に応えてサンプル規程集を完成させるため、また公開済みのサンプル規程集に対するコメントに対応するために、策定作業部会と検討 WG のいずれも平成 19 年 10 月まで活動を延長し、前年度と同様の連携体制により合同で検討と策定を継続した。平成 19 年度の活動は、課題が多く残っている領域の検討を推進して完成させるために、領域を再構成して 5 の大領域と 10 の小領域として、運用（運用総論領域、システム運用領域、情報管理領域）、認証（認証運用領域）、事務（事務領域）、利用（利用領域、自己点検領域）、教育（利用者教育領域、管理者教育領域、役職者教育領域）の分科会を設定した。その成果が本書であり、平成 19 年 8 月の「情報セキュリティセミナー」等で成果普及のための説明を実施した。

なお、策定作業部会は平成 19 年 10 月末で解散し、公開したサンプル規程集に対する対応や次回改訂に向けた準備等に対応するための組織として、国立情報学研究所 学術情報ネットワーク運営・連携本部に「高等教育機関における情報セキュリティポリシー推進部会」が平成 19 年 12 月に設置され、以後サンプル規程集についての継続的な更新を行っている。

本書と関連資料は国立情報学研究所の以下の Web サイトにて配布している。

（参考）http://www.nii.ac.jp/service/sp/

３．策定

本文書でとりまとめたサンプル規程集は、政府機関統一基準を踏まえ、各機関の事情に合わせて作成する際の具体的な参考として役立つよう、大学に適した標準的かつ活用可能な情報セキュリティ規程群を策定したものである。情報セキュリティに関する規程のほかに、情報セキュリティポリシーも含み、一部のマニュアルも対象に含めたが、いずれも期間内に検討可能であった範囲で成果を収録した。必ずしも必要性や重要度に沿って優先順位をつけて策定したとは限らない。政府機関統一基準は大学が準拠するよう要求しているものではないが、政府機関以外でも情報セキュリティ対策の体系の例として参照し利用する価値があるので、大学の事情に合わせて可能な範囲で政府機関統一基準の考え方にあわせる形で策定した。ほかにも情報セキュリティに係わる基準としてISOのものやプライバシーマーク制度などがそれぞれの目的により定められているが、それらも含めて検討して、大学における実施にもっとも適する規程とすることを意図した。

サンプル規程集は電子情報通信学会の検討WGにおいて策定された「高等教育機関におけるネットワーク運用ガイドライン」をベースとして含む形となっている。ただし、同ガイドラインがネットワーク運用に関するセキュリティに重点を置いたものであるのに対し、本文書では「政府機関の情報セキュリティ対策のための統一基準」が情報資産のセキュリティを確保することを目的としていることを考慮し、対象を情報システムにおけるネットワーク運用以外の要素まで広げている。

サンプル規程集のスタイルとして、規程の条文サンプルと解説から構成した。規程のスタイルや文章は大学の慣習に沿ったものとしたが、基準など一部では情報セキュリティポリシーの分野の標準的なスタイルを採った。それぞれの条文について、規定している内容が理解しにくい項目や、各大学の状況に応じて修正することが望ましい項目、他の選択（政府機関統一基準やISOのものとの相違など）や議論の余地があるものは解説を付記して、各大学における策定の参考として供した。各大学等で本文書を参考として自組織向けの規程等を作成する際には、これらの内容を参照した上で必要な修正や加除を検討していただきたい。例えば、仮想A大学と比べて学部数が多い大学や複数キャンパスにまたがる大学等では導入に際してセキュリティの管理体制を含め、各規程の前提条件の適合性に関する検討を行うことが望ましい。なお、定め方に判断の幅がある部分については、必ずしも一貫した規程になっていない部分もありえる。

情報システムの利用者認証(主体認証)については､ID とパスワードによる認証から生体認証、さらにはPKI(Public Key Infrastructure)を使用した認証などさまざまなものがあるが、ID とパスワードによる利用者認証を対象とした。PKI による利用者認証については、国立情報学研究所による UPKI 電子証明書発行サービスにおいて各種の参考ドキュメントが公開されているので、次のサイトを参考にされたい。

（参考） https://certs.nii.ac.jp/document/

４．サンプル規程

サンプル規程集は、仮想の国立大学法人Ａ大学における体制と規則を想定して検討した。Ａ大学の概要は次の通りである。

- 文学部と理学部の２学部で構成され、両学部とも在学生が 1,000 人（１学年 250 名）ずつである。さらに、学内共同利用施設として情報メディアセンターや図書館がある。
- 学内ネットワークや学内共同利用の情報システムは情報メディアセンターの担当であり、Ａ大学の管理運営部局は情報メディアセンターである。なお、事務情報システムは事務局が担当する。
- 副学長の一人がいわゆる最高情報責任者（CIO）であり、最高情報セキュリティ責任者（CISO）の役も兼ねており、本サンプルでは全学総括責任者となっている。

サンプル規程集は、図１に示すような階層構造を有する。情報システムの運用に関する基本的な考え方を定めた運用基本方針と運用に関する基本的事項を定めた運用基本規程をポリシー、ポリシーに基づいて、運用・管理や利用、教育等に関する事項を定めた規則を実施規程、実施規程に基づいて策定される手順やマニュアルなどを手順等としている。最上位のポリシーは全学規程として制定すべきものであるが、実施規程には全学情報システム運用委員会で決定すべき規程の他に各大学の運営体制によって情報メディアセンターあるいは事務局の内規とすべきものがあり、手順については、内規あるいは手引書とすべきものなどがある。手順等のうち、各大学における情報セキュリティ対策のために遵守すべき規則として策定されることが望ましい標準的な内容を手順とし、各大学での実情に即した内容で策定されることが望ましい事項はガイドラインとした。各階層において必要となるポリシー、実施規程、手順等の体系を図２に示す。

平成 26 年度版政府機関統一基準群の構成が大きく変化していることに伴い、以前のサンプル規程集とは文書番号の整合性の確保が難しくなったことから、2015 年版より、文書番号冒頭の記号を C に変更した。これまで公開している A 及び B で始まる文書番号の文書とは、同じ番号であっても内容が整合しないものが含まれることに留意されたい。

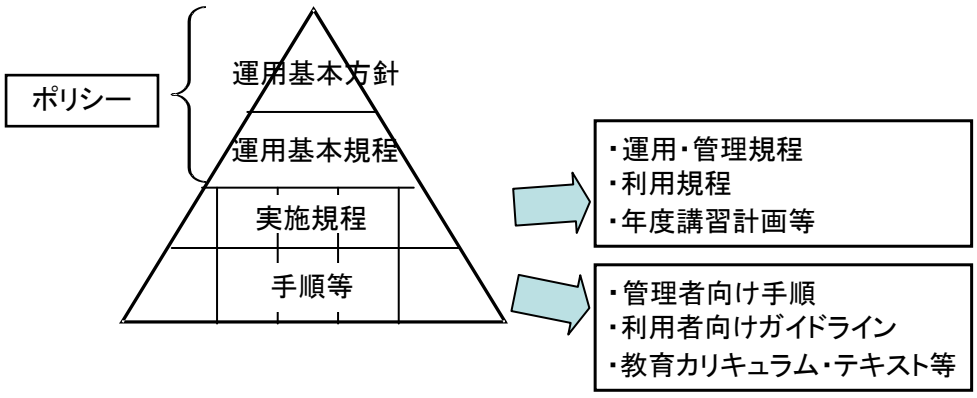


図１　ポリシー・実施規程・手順等の位置付け

ポリシー	実施規程	手順・ガイドライン等
C1000 情報システム運用基本方針	C2101 情報システム運用・管理規程 C2102 情報システム非常時行動計画に関する規程 C2103 情報格付け基準	C3100 情報システム運用・管理手順の策定に関する解説書 C3101 例外措置手順書 C3102 インシデント対応手順 C3103 情報格付け取扱手順 C3104 情報システム運用リスク評価手順
C1001 情報システム運用基本規程	C2201 情報システム利用規程（C2202）※	C3200 情報システム利用者向け文書の策定に関する解説書
		C3251 情報機器取扱ガイドライン C3252 電子メール利用ガイドライン C3253 ウェブブラウザ利用ガイドライン C3254 情報発信ガイドライン C3255 利用者パスワードガイドライン
C1101 情報セキュリティインシデント対応チーム（CSIRT）設置規程	C2301 年度講習計画	C3300 教育テキストの策定に関する解説書 C3301 教育テキスト作成ガイドライン(利用者向け) C3302 教育テキスト作成ガイドライン(システム管理者向け) C3303 教育テキスト作成ガイドライン(CIO/役職者向け)
	C2401 情報セキュリティ監査規程	C3401 情報セキュリティ監査実施手順
	C2501 事務情報セキュリティ対策基準 C2502 事務情報セキュリティ対策基準策定のためのガイドライン	C3500 各種マニュアル類の策定に関する解説書 C3501 各種マニュアル類(**)
	C2601 全学認証基盤運用管理規程 C2602 全学認証基盤接続規程 C2603 全学認証基盤アカウント利用規程	C3600 認証手順の策定に関する解説書 C3601 情報システムアカウント取得手順
	C2651 証明書ポリシー(*) C2652 認証実施規程(*)	

水色の網掛け部分は、技術系の規程・手順書（より現場に近いレベルでの策定・運用を可能とするもの）

(*) 外部文書の参照のみ

(**) 各大学にて策定することを想定

※C2202（全学認証基盤利用規程）はその内容が C2601（全学認証基盤運用管理規程）、C2602（全学認証基盤接続規程）、C2603（全学認証基盤アカウント利用規程）の 3 文書に移管されたことにより廃止とする。

図２　ポリシー・実施規程・手順等の体系

なお、各大学における情報セキュリティの確立のためには、これらのポリシーや実施規程、手順の整備だけではなく、図３に示すとおり、ポリシーに沿った教育活動や組織の運用、さらにはその状況の監査と評価・見直しが重要で、いわゆる Plan・Do・Check・Action のサイクルを回す必要がある。本ポリシーで規定している組織を図示すると、図４のとおりとなるので、参考にしていただきたい。

本ポリシー及び、実施規程、手順における管理体制は、2016 年 8 月に内閣サイバーセキュリティセンターから発行された「政府機関の情報セキュリティ対策のための統一基準群」（平成 28 年度版）の体制と表１のとおりに対応づけられるので参考にされたい。

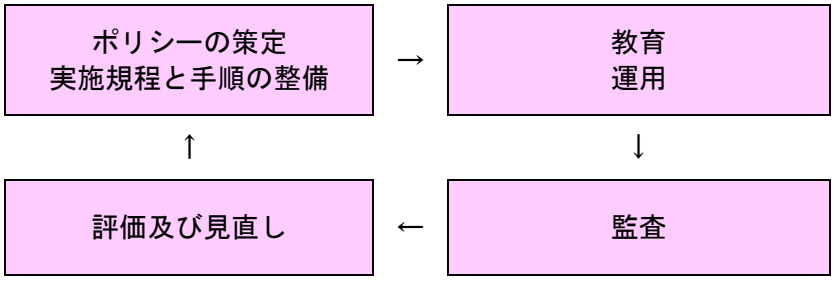


図３　ポリシーの評価及び見直し

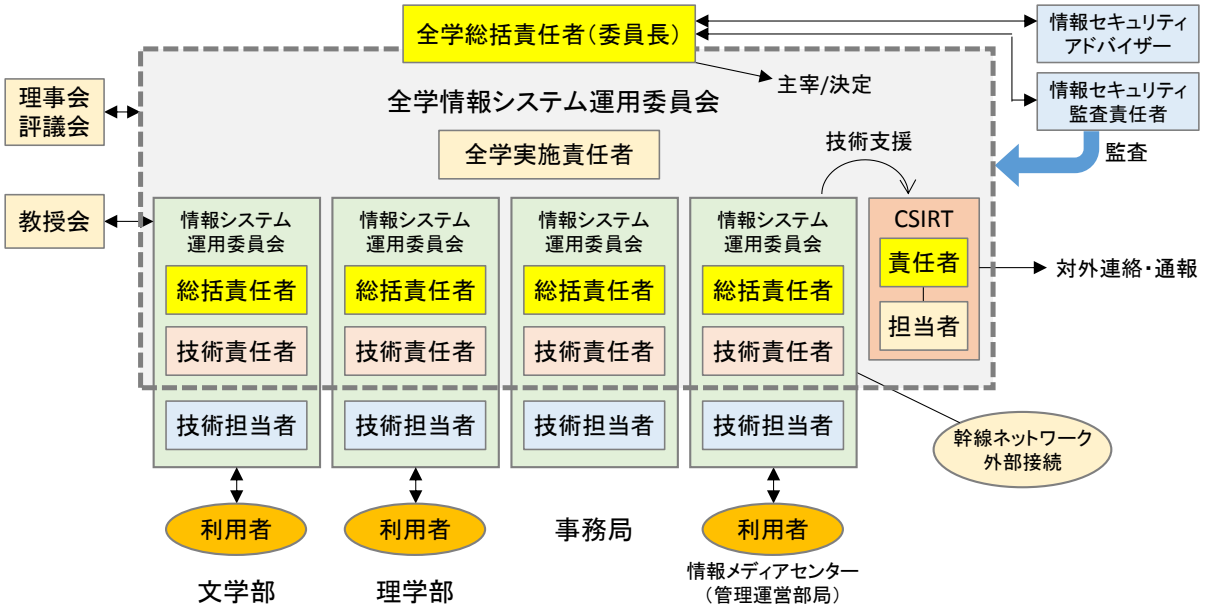


図４　情報システム運用管理体制

表 1　情報システム運用管理体制の対応

	政府機関統一基準	本サンプル規程集
1	最高情報セキュリティ責任者	全学総括責任者
2	情報セキュリティ監査責任者	情報セキュリティ監査責任者
3	最高情報セキュリティアドバイザー	情報セキュリティアドバイザー
4	統括情報セキュリティ責任者	全学実施責任者
5	情報セキュリティ責任者	部局総括責任者
6	情報システムセキュリティ責任者	部局技術責任者
7	情報システムセキュリティ管理者	部局技術担当者
8	課室情報セキュリティ責任者	職場情報セキュリティ責任者
9	区域情報セキュリティ責任者	区域情報セキュリティ責任者
10	上司	上司（注）
11	情報セキュリティ委員会	全学情報システム運用委員会
12		部局情報システム運用委員会

（注）研究室においては教授、学生にとっては担当教員を指す一般用語として上司を使用している。

A 大学における情報取扱区域に関するクラス分類を下表に示す。A 大学では政府機関統一技術基準においてクラス 1 の要件として定義されている「セキュリティゲート」または「警備員等による立ち番」を満たす施設は事務棟、情報メディアセンター、図書館の 3 箇所のみであるため、これ以外の施設は原則としてすべてクラス 0 の区域として扱う。クラス 1 の区域のうち、個別に施錠可能な区域（事務室、機器室、学長室等）をクラス 2 とする。さらに重要情報や設備を設置し、担当外の事務従事者の立入を制限する必要がある区域（サーバ室、資料保管室（＝バックアップメディアの保管場所として想定)）をクラス 3 としている。

表 3　情報取扱区域のクラスの決定

	政府機関統一技術基準における定義	A 大学における設定
クラス 0	クラス 3、クラス 2 及びクラス 1 以外の区域であり、情報セキュリティを確保するため、利用制限対策を実施する必要がある区域	学内における下記以外のすべての区域
クラス 1	最低限必要な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域	事務棟内立入制限区域 情報メディアセンター内立入制限区域 図書館内立入制限区域
クラス 2	クラス 1 より強固な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域	事務室、学長室及びこれに準ずる個別施錠が可能な区域
クラス 3	クラス 2 より強固な情報セキュリティを確保するための厳重な管理対策及び利用制限対策を実施する必要がある区域	（本欄の内容は本来非公開とすべきものであるが、サンプル用に掲載） 情報メディアセンター内サーバ室 事務棟内資料保管室
クラス 4 以上	（統一基準外）	区域設定無し。

５．検討メンバー（所属は参加時点のもの）

○大学共同利用機関法人情報・システム研究機構 国立情報学研究所 学術情報ネットワーク運営・連携本部「高等教育機関における情報セキュリティポリシー推進部会」

稲葉宏幸（京都工芸繊維大学），上田浩（京都大学），上原哲太郎（京都大学），
岡田仁志（副主査，国立情報学研究所），小川賢（幹事，神戸学院大学），
岡部寿男（京都大学），折田彰（京都大学），金谷吉成（東北大学），木下宏揚（神奈川大学），
佐藤周行（東京大学），佐藤慶浩（日本 HP），庄司勇木（日本開発研究所三重），
須川賢洋（新潟大学），曽根秀昭（主査，東北大学），高倉弘喜（国立情報学研究所），
中村素典（国立情報学研究所），中山雅哉（東京大学），西村浩二（広島大学），
長谷川明生（中京大学），冨士原裕文（富士通），丸橋透（ニフティ）

○大学共同利用機関法人情報・システム研究機構 国立情報学研究所 学術情報ネットワーク運営・連携本部「国立大学法人等における情報セキュリティポリシー策定作業部会」

飯田勝吉（東京工業大学），板垣毅（東北大学），上原哲太郎（京都大学），
岡田仁志（副主査，国立情報学研究所），岡部寿男（京都大学），岡村耕二（九州大学），
折田彰（京都大学），垣内正年（奈良先端科学技術大学院大学），笠原義晃（九州大学），
金谷吉成（東北大学），上岡英史（芝浦工業大学），貴志武一（東京工業大学），
鈴木孝彦（九州大学），曽根秀昭（主査，東北大学），高井昌彰（北海道大学），
高倉弘喜（京都大学），竹内義則（名古屋大学），谷本茂明（国立情報学研究所），
中野博隆（大阪大学），中山雅哉（東京大学），西村浩二（広島大学），林田宏三（熊本大学），
平塚昭仁（徳島大学），布施勇（徳島大学），松下彰良（東京大学），南弘征（北海道大学），
湯浅富久子（高エネルギー加速器研究機構）
協力：文部科学省大臣官房政策課情報化推進室，文部科学省研究振興局情報課，
内閣官房情報セキュリティセンター

○社団法人電子情報通信学会「ネットワーク運用ガイドライン検討ワーキンググループ」

稲葉宏幸（京都工芸繊維大学），岡田仁志（国立情報学研究所），
小川賢（幹事，神戸学院大学），垣内正年（奈良先端科学技術大学院大学），
金谷吉成（東北大学），木下宏揚（神奈川大学），楠元範明（早稲田大学），
佐藤慶浩（日本 HP），下川俊彦（九州産業大学），須川賢洋（新潟大学），
曽根秀昭（主査，東北大学），高倉弘喜（京都大学），高橋郁夫（弁護士），
辰己丈夫（東京農工大学），中西通雄（大阪工業大学），中野博隆（大阪大学），
西村浩二（広島大学），野川裕記（東京医科歯科大学），長谷川明生（中京大学），
冨士原裕文（富士通），前野譲二（早稲田大学），丸橋透（ニフティ），三島健稔（埼玉大学）

６．参考資料等

ア．大学の情報セキュリティポリシーに関連するもの

(1) 電子情報通信学会 高等教育機関におけるネットワーク運用ガイドライン
http://www.ieice.org/jpn/teigen/
本サンプル規程集の母体となった、大学等のネットワーク運用を対象とした情報セキュリティポリシーに関するガイドラインを公開している。

(2) 大学における情報セキュリティポリシーの考え方
http://www.nii.ac.jp/service/sp/
上記(2)の策定とほぼ同時期に実施された、「大学の情報セキュリティポリシーに関する研究会」による検討成果をとりまとめたものである。

(4) 京都大学情報環境機構　情報セキュリティ
https://www.iimc.kyoto-u.ac.jp/ja/services/ismo/
学内向けの情報セキュリティ関連情報、関連規程等のポータルページである。

(5) 学術認証フェデレーション“学認”
https://www.gakunin.jp/
国内大学等と学術サービスを提供する企業を対象に、国立情報学研究所が運営している認証連携基盤である。

イ．情報セキュリティや著作権保護に関するもの

(1) 内閣サイバーセキュリティセンター
http://www.nisc.go.jp/
政府機関の情報セキュリティ対策のための統一基準に関する関連資料がある。

(2) 警察庁 サイバー犯罪対策プロジェクト
http://www.npa.go.jp/cyber/
サイバー犯罪に関する啓発資料等。

(3) 総務省 国民のための情報セキュリティサイト
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
情報セキュリティ対策に関する啓発資料等。

(4) 経済産業省 情報セキュリティ政策
http://www.meti.go.jp/policy/netsecurity/
情報セキュリティ監査制度に関する基準類等がある。

(5) 独立行政法人情報処理推進機構（IPA）　情報セキュリティ
http://www.ipa.go.jp/security/
コンピュータウイルスや不正アクセスの届出状況や、各種啓発資料を参照できる。

(6) 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
http://www.jpcert.or.jp/
最新の脅威に関する注意喚起や緊急報告等。

(7) 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）
http://www.jnsa.org/
情報セキュリティ対策製品・サービス提供企業の会員による各種活動成果を公開。

(8) 特定非営利活動法人情報セキュリティ研究所（RIIS）
http://www.riis.or.jp/
情報セキュリティ関連のシンポジウムや研修を実施。

(9) 社団法人著作権情報センター（CLIC）
http://www.cric.or.jp/
著作権に関する関係法令や Q&A 集などを参照することができる。

(10) プロバイダ責任制限法ガイドライン等協議会（社団法人テレコムサービス協会内）
http://www.telesa.or.jp/consortium/provider/
著作権関係ガイドライン等が参照できる。

(11) インターネットホットラインセンター
http://www.internethotline.jp/
有害情報や違法情報に関する具体例などがある。

C1000 情報システム運用基本方針

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A1000	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2013年7月5日 B1000	文書番号の変更のみ	ー
2015年10月9日 C1000	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C1000-01　（情報システムの目的）

第一条　Ａ大学（以下「本学」という。）情報システムは、本学の理念である「研究と教育を通じて、社会の発展に資する」ことの実現のための、本学のすべての教育・研究活動及び運営の基盤として設置され、運用されるものである。

解説：組織の基本方針（ポリシー）であるので、この条で「本学」は大学ではなく法人とする考え方もある。規程の名称（位置づけ）に法人名を冠することもある。本学の基本理念であるかぎ括弧部分は、各大学のものに差し替えるか、あるいは「本学の理念と使命の実現のため」などとする。

規程の第一条は規程の目的を述べる例が多いので、情報システム運用基本方針を制定する目的を述べるよう書き改めても良い。この基本方針規程を情報セキュリティポリシーとして、この条で情報資産の保護の実施をうたうようにして、以下の条でも情報資産の保護の実施を定めるやり方もある。

本基本方針を実施するために、各種規程や手順など（情報セキュリティポリシーの体系を構成するもの）を規定することをこの条か別の条で述べるべきかもしれない。

C1000-02　（運用の基本方針）

第二条　前条の目的を達するため、本学情報システムは、円滑で効果的な情報流通を図るために、別に定める運用基本規程により、優れた秩序と安全性をもって安定的かつ効率的に運用され、全学に供用される。

解説：本基本方針は、本学における情報システム運用に際して次の事項に関する基本的な取り組みを規定することにより、本学情報システムの健全な運用と利用を実現するとともに情報社会の発展に貢献することを目的とする。

（a）情報資産の保護

（b）情報システム運用に関連する法令の遵守

不正アクセス禁止法、プロバイダ責任制限法、著作権、個人情報保護法等

（c）学問の自由・言論の自由・通信の秘密(プライバシー保護等)とルールによる規制とのバランス

もし情報セキュリティを中心に据えた基本方針とするならば、それをここで「以下の対策を基本方針とし」のように書いて、不正アクセス対策、不正利用対策、情報資産管理、教育、および評価・見直しなどの事項を掲げる。

C1000-03　（利用者の義務）

第三条　本学情報システムを利用する者や運用の業務に携わる者は、本方針及び運用基本規程に沿って利用し、別に定める運用と利用に関する実施規程を遵守しなければならない。

C1000-04　（罰則）

第四条　本方針に基づく規程等に違反した場合の利用の制限および罰則は、それぞれの規程に定めることができる。

解説：情報システムの利用に関わる違反に対して、利用者や運用担当者などの個人あ

るいは部局に対する利用制限措置と、その個人である教職員あるいは学生に対する懲戒とがありえる。これらを規程に定める場合に、アカウント停止のような利用制限措置については、情報システム上で行う業務（職員）や講義（学生）、あるいは申請手続き等のように情報システム利用を必須とする行為が行えなくなる副作用またはそれを防止する代替手段の用意などを考慮に入れることが必要である。また、懲戒について所属部局で決定する場合には情報メディアセンターの調査報告から懲戒決定までの手続きを規定しておくことと、部局間での懲戒の内容のバランスをとることを考慮すべきである。

C1001 情報システム運用基本規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A1001	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A1001	一部語句の調整と解説の追記	国立大学法人等における情報セキュリティポリシー策定作業部会
2011年3月31日 A1001	定義の見直し及び担当者の役割に関して不明確であった一部の条文を修正	冨士原裕文（富士通）
2013年7月5日 B1001	文書番号の変更のみ	ー
2015年10月9日 C1001	C2101の改定内容と整合をとるための用語定義等の見直し	金谷吉成（東北大学）
2017年10月17日 C1001	統一基準（平成28年度版）の改訂への対応とC1101との整合性確保	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C1001-01　（目的）

第一条　本規程は、Ａ大学（以下「本学」という。）における情報システムの運用及び管理について必要な事項を定め、もって本学の保有する情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

C1001-02　（適用範囲）

第二条　本規程は、本学情報システムを運用・管理するすべての者、並びに利用者及び臨時利用者に適用する。

解説：来学中に利用する訪問者や受託業務従事者などの臨時利用者を含む。

C1001-03　（定義）

第三条　本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

一　情報システム

情報処理及び情報ネットワークに係わるシステムで、次のものをいい、本学情報ネットワークに接続する機器を含む。

(1) 本学により、所有又は管理されているもの

(2) 本学との契約あるいは他の協定に従って提供されるもの

解説：情報ネットワークに接続されている情報処理システムだけではなく、スタンドアロンの情報処理システムも含まれる。また、上記の二つの項目に該当しない機器、例えば私物 PC であっても本学の情報ネットワークに接続する時は本規程の対象となる。第五号の事務情報システムは情報システムに含まれるので、ここで定義してもよい。

二　情報

情報には次のものを含む。

(1)　情報システム内部に記録された情報

(2)　情報システム外部の電磁的記録媒体に記録された情報

(3)　情報システムに関係がある書面に記載された情報

解説：情報には、ネットワークに接続している、いないに関わらず情報処理システムの内部に記録されている情報、及び情報システム外部の電磁的記録媒体に記録された情報、その情報を印刷した紙も含まれる。情報システムの運用管理に関する資料（仕様、設計、運用、管理、操作方法などの資料）を含む考え方もありうる。

三　情報資産

情報システム並びに情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。

四　事務情報

事務情報とは情報のうち次のものをいう。

(1)　「法人文書の管理に関する規程」の対象となる法人文書

(2)　(1)以外の法人文書で、部局長が指定した文書

五　事務情報システム

事務情報を扱う情報システムをいう。

解説：事務情報システムには、事務局が運用責任を持つ情報システムばかりではなく、教員等が成績管理に使用するパソコン等も含まれる。

六　ポリシー

本学が定める「C1000 情報システム運用基本方針」及び「C1001 情報システム運用基本規程」をいう。

七　実施規程

ポリシーに基づいて策定される規程及び、基準、計画をいう。

八　手順

実施規程に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。

九　利用者

教職員等及び学生等で、本学情報システムを利用する許可を受けて利用するものをいう。

解説：利用者とは本学情報システムを単に使用するだけではなく、パソコンをはじめとした機器を情報ネットワークに接続して使用する者を含む。教職員等及び学生等に限定しない考え方もありうる。第十二号の臨時利用者は関連するので、ここで定義しても良い。

十　教職員等

本学を設置する法人の役員及び、本学に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、部局総括責任者が認めた者をいう。

解説：同窓会、生協、TLO、インキュベーションセンター、地域交流センター、財団などの職員を含む考え方もある。また、受託業務従事者についても委託業務の内容に応じて教職員として扱う考え方もある。学内規定の体系の中で「教職員」「学生」が定義されているならば、第十号と第十一号は省略可能であるが、定義に含む範囲に注意が必要である。

十一　学生等

本学通則に定める学部学生、大学院学生、研究生、研究員、研修員並びに研究者等、その他、部局総括責任者が認めた者をいう。

十二　臨時利用者

教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。

解説：訪問者や受託業務従事者などの本学構成員以外の者が本学情報システムを臨時に利用する場合は、所定の手続きで身元を確認した上で、ポリシー及び関連規程を遵守することを条件に利用を許可するものとする。

十三　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

解説：情報セキュリティには、情報資産の機密性、完全性及び可用性を維持することが含まれ、適切なアクセス制限を確保するとともに、情報を保全して一貫性を確保し、利用に支障が生じないように対策を施すことが求められる。また、情報セキュリティが損なわれた場合に、その情報資産だけではなく、社会的評価が損なわれたり、他者への二次的損害を与えたりするなど、被害が拡大することもあるので、多面的な情報セキュリティ対策が必須である。

十四　電磁的記録

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

解説：法律の定める「電磁的記録」の定義である。電子的方式、磁気的方式に限らず、媒体の化学変化を応用する方式や紙面上の記録方式であっても、人の知覚による認識ができず、コンピュータシステムによる記録と読取を目的としたものはこれに含まれる。一方、マイクロフィルムのように人の知覚による認識を前提とした方式を用いた記録は含まない。

電磁的記録として扱われる記録方式を用いる媒体の例：

メモリ、ハードディスク、CD、DVD、光磁気(MO)ディスク、磁気テープ、磁気カード、IC カード、二次元バーコード（QR コード等）

電磁的記録ではないものの例：

人の知覚による認識を目的としたコンピュータからの印刷出力、入力用に記入する伝票、フォーム等の帳票類、マイクロフィルム

十五　情報セキュリティインシデント

情報セキュリティに関し、意図的または偶発的に生じる、本学規程または法律に反する事故あるいは事件をいう。

解説：情報セキュリティインシデントの例としては、地震等の天災、火災、事故等によるネットワークを構成する機器や回線の物理的損壊や滅失によるネットワークの機能不全や障害、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等がある。その疑いがある場合及びそれに至る行為もこれに準じて扱うことが適当であろう。

十六　CSIRT（シーサート）

本学において発生した情報セキュリティインシデントに対処するため、本学に設置された体制をいう。Computer Security Incident Response Team の略。

十七　明示等

情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

解説：情報ごとに格付けを記載することにより明示することを原則とするが、その他にも、当該情報の格付けに係わる認識が共通となる措置については、明示等に含まれる。例えば、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等に明記し、当該情報システムを利用するすべての者に当該規定を周知することができていれば明示等に含むものである。

C1001-04　（全学総括責任者）（政府機関統一基準の対応項番 2.1.1(1)）

第四条　本学情報システムの運用に責任を持つ者として、本学に全学総括責任者を置く。学長がこれを任命する。

２　全学総括責任者は、ポリシー及びそれに基づく規程の決定や情報システム上での各種問題に

対する処置を行う。

解説：その業務に関する予算と人事の権限および責任を有する副学長あるいは理事に相当する者が望ましい。全学総括責任者は、いわゆる最高情報責任者（CIO）の役を務める。

いわゆる最高情報セキュリティ責任者（CISO）と同じ者を充てる考え方と、相互チェックのために異なる者を充てる考え方とがありうる。

3　全学総括責任者は、全学の情報基盤として供される本学情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

4　全学総括責任者は、全学向け教育及び全学情報システムを担当する部局技術担当者向け教育を統括する。

5　全学総括責任者に事故があるときは、全学総括責任者があらかじめ指名する者が、その職務を代行する。

6　全学総括責任者は、原則として、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置く。

解説：情報セキュリティに関する専門家を情報セキュリティアドバイザーとして置くことを定めた事項である。本学における情報セキュリティ対策については、情報システムに関する技術や事案に対する対処等の専門的な知識及び経験が必要となるため、実施規程の策定・導入から運用、評価、見直しまで専門的な助言を行う専門家を活用することが重要である。

全学総括責任者が、情報システムに関する専門的な知識及び経験を高度な水準で有しているため、専門家の助言を必要としないといった特殊な場合を除き、置くことを義務付けているものである。なお、情報セキュリティアドバイザーはいわゆる CIO 補佐官に相当すると考えられる。

C1001-05　（全学情報システム運用委員会）（政府機関統一基準の対応項番 2.1.1(2)）

第五条　本学情報システムの円滑な運用のための最終決定機関として、本学に全学情報システム運用委員会を置く。

解説：全学総括責任者が主宰し、本学情報システムの目的に合致した健全な運用と利用を実現できるよう、情報システム運用に関する決定を行う。

情報システムのセキュリティに関する最終決定機関としての役割を兼ねる考え方と、あるいは別の機関を設ける考え方がある。委員会形式とは限らない。

2　全学情報システム運用委員会は以下を実施する。

一　ポリシー及び全学向け教育の実施ガイドラインの改廃

二　情報システムの運用と利用及び教育に係る規程及び手順の制定及び改廃

解説：情報システムの運用と管理及び管理者に関することについて、情報システム運用・管理規程を定める。

情報システムの円滑な運用のために、情報システムの利用及び利用者に関することについて情報システム利用規程を定めて、利用者に対して制約を課す。

利用者は、契約等により本学情報システムを利用する権利を有するが、その利用に伴うすべての行動について責任を自覚しなければならない。本学情報シス

テムを利用した情報発信は本学内にとどまらず、社会へ広く伝達される可能性があることを自覚し法令遵守等、責任をもった行動が望まれる。また、目的に示す基本理念を大きく逸脱するような私的利用や商業利用は制限される。

本学情報システムの運用においては、表現の自由とプライバシーに最大限配慮するが、第三者に対する誹謗中傷や名誉毀損、著作権侵害等と判断されるコンテンツを制限する場合がある。また、利用者の通信の秘密を尊重するが、ネットワークの円滑な運用のため、必要最小限の範囲において通信ログを保存・調査する場合がある。このほか、上位ネットワークプロバイダの定める利用規約（AUP）の制約もありうる。

情報システム運用委員会が実施する教育を受講し内容を十分理解の上、所定の手続きをとりポリシー及び関連規程の遵守を承諾した者に本学情報システムを利用する許可（アカウント等）が与えられる。利用者が、本学情報システムに接続する機器を持ち込み使用する場合は、別途定める基準に従うものとする。

三　情報システムの運用と利用に関する教育の年度講習計画の制定及び改廃、並びにその計画の実施状況の把握

解説：利用者に対して、情報セキュリティ管理の内容を周知しポリシーの他、必要な実施規程及び、関連する実施手順の遵守を図るため、毎年、年度講習計画を策定し、教育・啓発を実施する。

四　情報システム運用リスク管理規程の制定及び改廃、並びにその実施状況の把握

解説：リスク分析と対策手順の策定について、情報システム運用リスク管理規程を定める。

五　情報セキュリティ監査規程の制定及び改廃、並びにその実施

解説：情報システム運用について、定期的な見直しを行うとともに、学内外の適切な者による監査等を実施し、その結果に基づいた必要な改善を行うことを情報セキュリティ監査規程として定める。

情報システムに係る情報セキュリティ監査の実施は、リスク分析結果、実施手順の整合性及びその実施状況について行う。情報セキュリティ監査業務の一部又は全部を、本学以外の事業者に委託することができる。情報セキュリティ監査の実施にあたっては、個人情報を関係者以外に開示してはならない。

六　情報システム非常時行動計画の制定及び改廃、並びにその実施

解説：不測の事態への対応手順を定める情報システム非常時行動計画（contingency plan）の実施には、情報システムの運用と利用に関する事件、事故の発生時の対応が含まれる。

情報システム非常時行動計画を作成して、コンピュータ犯罪等の事件や情報セキュリティ事故、災害等のトラブルが発生した場合の連絡体制及び対応手順を整備し、これをあらかじめ関係者に周知しておく。これには、外部からの苦情等、トラブルの通知について受付窓口を設置し、エスカレーションルールを定めることも含まれる。

トラブルが発生した場合には、情報システム非常時行動計画に従って速やかに緊急対策チームを編成するとともに、適切な対応を行う。トラブル対応が完了した後も、トラブル原因を究明し、その対策をポリシー等に反映し、トラブル

の再発防止に努める。

七　情報セキュリティインシデントの再発防止策の検討及び実施

C1001-06　（全学情報システム運用委員会の構成員）（政府機関統一基準の対応項番 2.1.1(2)-1）

第六条　全学情報システム運用委員会は、委員長及び次の各号に掲げる委員をもって組織する。

一　全学実施責任者

二　部局総括責任者

三　部局技術責任者

四　その他全学総括責任者が必要と認める者

解説：全学総括責任者は委員長としてこの委員会の構成に含まれ、次の条で規定されている。

C1001-07　（全学情報システム運用委員会の委員長）（政府機関統一基準の対応項番 2.1.1(2)-1）

第七条　全学情報システム運用委員会の委員長は、全学総括責任者をもって充てる。

２　委員長は、会務を総理する。

C1001-08　（全学実施責任者）（政府機関統一基準の対応項番 2.1.1(4)(a)）

第八条　本学に全学実施責任者を置く。

解説：本学情報システムについて、構成の決定などの整備と、技術的問題（第２項）と教育（第３項）及び連絡・通報窓口（第４項）を含む運用に関する事項を実施する者である。

全学実施責任者は管理運営部局のセンター長や上級の職員が想定されるが、全学総括責任者が兼務する考え方もありうる。

２　全学実施責任者は、全学総括責任者の指示により、本学情報システムの整備と運用に関し、ポリシー及びそれに基づく規程並びに手順等の実施を行う。

３　全学実施責任者は、情報システムの運用に携わる者及び利用者に対して、情報システムの運用並びに利用及び情報システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。

４　全学実施責任者は、本学の情報システムのセキュリティに関する連絡と通報において本学情報システムを代表する。

５　全学実施責任者は、全学総括責任者の推挙により学長が任命する。

C1001-09　（情報セキュリティ監査責任者）（政府機関統一基準の対応項番 2.1.1(3)）

第九条　全学総括責任者は、情報セキュリティ監査責任者を置く。

２　情報セキュリティ監査責任者は、全学総括責任者の指示に基づき、監査に関する事務を統括する。

解説：本ポリシーに基づき監査を行う責任者を定めた事項である。

情報セキュリティ監査責任者は、部局総括責任者が所管する組織における情報セキュリティ監査を実施するため、情報セキュリティ対策を実行する各責任者と兼務することはできない。

監査の実効性を確保するために、部局総括責任者より職務上の上席者を情報セ

キュリティ監査責任者として置くことが望ましい。
このサンプルと異なって全学総括責任者から独立させて、本学に情報セキュリティ監査責任者を置くことと学長が任命することを定めて、全学総括責任者の指示に基づくことを削除する考え方もありうる。
情報セキュリティ監査責任者は、本学の情報セキュリティに関する情報を共有するために、全学情報システム運用委員会にオブザーバとして参加することが望まれる。情報セキュリティ監査責任者の業務を補佐するために、各部局内及び部外の担当者を置く必要性を検討することが望まれる。また、業務の実効性を担保するために外部組織の活用も考えられる。
本学に監査室のような組織があったとしても、それをここの監査責任者あるいは実施組織とできるかについて、情報セキュリティ監査の業務を担当するために適格かの確認を要する。

C1001-10　（管理運営部局）
第十条　全学情報システム運用委員会は、本学情報システムの管理運営部局を定める。
解説：規程の中で管理運営部局を定めても良い。
例えば、事務局総務部である。ただし、幹線ネットワークと外部ネットワーク接続の運用は情報メディアセンターの業務であるし、情報メディアセンターを管理運営部局とする考えもある。

C1001-11　（管理運営部局が行う事務）
第十一条　管理運営部局は、全学実施責任者の指示により、以下の各号に定める事務を行う。
一　全学情報システム運用委員会の運営に関する事務
二　本学情報システムの運用と利用におけるポリシーの実施状況の取りまとめ
三　講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
四　本学の情報システムのセキュリティに関する連絡と通報

C1001-12　（部局総括責任者）（政府機関統一基準の対応項番 2.1.1(4)(a)）
第十二条　各部局に部局総括責任者を置く。部局長が任命する。
解説：部局内情報システムの運用に責任を持つ者である。VPN などによる拡張ネットワークの部分を含む。学部長が兼ねても良いし、あるいは学部長をもって充てることを規定しても良い。
２　部局総括責任者は、部局における運用方針の決定や情報システム上での各種問題に対する処置を担当する。

C1001-13　（部局情報システム運用委員会）
第十三条　各部局に部局情報システム運用委員会を置く。
２　部局情報システム運用委員会は以下の各号に掲げる事項を実施する。
一　部局におけるポリシーの遵守状況の調査と周知徹底
二　部局におけるリスク管理及び非常時行動計画の策定及び実施
三　部局における情報セキュリティインシデントの再発防止策の策定及び実施

四　部局における部局技術担当者向け教育の計画と企画

C1001-14　（部局情報システム運用委員会の構成員）
第十四条　部局情報システム運用委員会は、委員長及び次の各号に掲げる者を委員として組織する。
一　部局技術責任者
二　部局技術担当者
三　その他部局総括責任者が必要と認める者

C1001-15　（部局情報システム運用委員会の委員長）
第十五条　部局情報システム運用委員会の委員長は、部局総括責任者をもって充てる。

C1001-16　（部局技術責任者）（政府機関統一基準の対応項番 2.1.1(4)(d)）
第十六条　部局に部局技術責任者を置く。部局長が任命する。
解説：部局総括責任者は部局技術責任者を兼務することができる。
２　部局技術責任者は、部局情報システムの構成の決定や技術的問題に対する処置を担当する。
３　部局技術責任者は、部局技術担当者に対して、ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。

C1001-17　（部局技術担当者）（政府機関統一基準の対応項番 2.1.1(4)-6）
第十七条　部局技術責任者は、当該部局の情報システムの管理業務において必要な単位ごとに、部局技術担当者を置く。部局技術担当者は部局技術責任者が推挙し部局長が任命する。なお、部局技術責任者自ら部局技術担当者を兼務することができる。
２　部局技術担当者は、部局技術責任者の指示により、部局の情報システムの運用の技術的実務を担当し、利用者への教育を補佐する。
解説：例えば、部屋ごとに１名を任命する。情報コンセントや無線アクセスポイントの場合には、接続する者ではなく設置者側から任命する。VPN などによる外部への拡張ネットワークの接続サーバには必ず置く必要がある。
部局の規模が大きいケースでは、部局技術担当者が多数になるので、学科や建物など適切な単位で中間的なグループ化を設けたほうが良いこともある。部局技術担当者として任命される者の要件については、大学職員であることが考えられるが、運用の実態と齟齬が生じないように定める。

C1001-18　（区域情報セキュリティ責任者の設置）（政府機関統一基準の対応項番 2.1.1(4)(b)）
第十八条　部局総括責任者は、施設及び環境に係る対策を行う単位ごとの区域を定め、その区域ごとに、区域情報セキュリティ責任者１人を置く。
２　区域情報セキュリティ責任者は、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を総括する。
解説：「C2101 情報システム運用・管理規程」第五十四条第１項（区域ごとの対策の決定）で定める区域ごとに、当該区域における情報セキュリティ対策の事務を総括する者を置くことを定めた事項である。

「施設及び環境に係る対策を行う単位ごとの区域」には、教室、研究室、事務室やサーバ室だけでなく、建物内のロビーや廊下といった区域も含まれる。そのため、本学において漏れなく情報セキュリティ対策を実施する観点から、それぞれの区域に区域情報セキュリティ責任者を置く必要がある。

「対策を行う単位」は、当該区域の利用用途や設置環境等を勘案して、例えば、

・部局又は研究室単位で管理している部屋（会議室等）ごと

・情報システムが設置された部屋（サーバ室等）ごと

等とすることが挙げられる。また、上記以外の区域（ロビー、廊下等）を一つの区域とする場合も考えられる。

区域情報セキュリティ責任者は、所管する区域について規定された対策の基準に従い、自ら対策を定めそれを実施する。また、区域情報セキュリティ責任者は、その役割の性質上、施設の管理者が兼任することが想定される。定める単位としては、例えば以下が考えられる。

・単一の研究室が利用する部屋（会議室等）を管理する場合は、職場情報セキュリティ責任者

・複数の研究室が利用する部屋（会議室等）を管理する場合は、部局総括責任者

・情報システムが設置された部屋（サーバ室等）を管理する場合は、部局技術責任者

・異なる区域（クラスが異なる場合も含む）をまとめて管理する場合は、部局総括責任者

・教室、研究室、事務室又はサーバ室以外の区域（ロビー、廊下等）を管理する場合は、建物等の管理に関する部門の責任者

なお、「C2101 情報システム運用・管理規程」第五十三条第１項（要管理対策区域における対策）で規定するクラス１は、施設管理の観点から行う措置が、情報セキュリティ上の対策と同等であれば、施設管理者が指定されていることをもって、区域情報セキュリティ責任者を設置しているとみなしてよい。

C1001-19　（職場情報セキュリティ責任者の設置）（政府機関統一基準の対応項番 2.1.1(4)(c)）

第十九条　部局総括責任者は、教室、研究室、事務室等の管理組織ごとに、職場情報セキュリティ責任者１人を置く。

２　職場情報セキュリティ責任者は、教室、研究室、事務室等の管理組織における情報の取扱いその他の情報セキュリティ対策に関する事務を総括する。

解説：教室、研究室、事務室等の管理組織単位での情報セキュリティ対策の事務を統括する者を置くことを定めた事項である。

職場情報セキュリティ責任者は、所管する事務や利用者等における情報の取扱い等に関して、その是非を判断し、情報の持ち出しや公開等についての責任を有する者であり、例えば、部局においては部局長（部局総括責任者）、研究室においては教授、委員会等においては当該委員会等の委員長、医局においては医局長、事務組織内の課室においては課室長などが想定される。部局総括責任者が教室、研究室、事務室等の管理組織ごとに１人任命するものである。

C1001-20 （全学情報セキュリティアドバイザーの設置）（政府機関統一基準の対応項番 2.1.1(5)）

第二十条　全学総括責任者は、情報セキュリティについて専門的な知識及び経験を有する者を全学情報セキュリティアドバイザーとして置く。

２　全学総括責任者は、以下を例とする全学情報セキュリティアドバイザーの業務内容を定める。

一　本学全体の情報セキュリティ対策の推進に係る全学総括責任者への助言

二　情報セキュリティ関係規程の整備に係る助言

三　対策推進計画の策定に係る助言

四　教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援

五　情報システムに係る技術的事項に係る助言

六　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言

七　利用者に対する日常的な相談対応

八　情報セキュリティインシデントへの対処の支援

九　前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

解説：全学総括責任者は、情報セキュリティに関する技術的事項等について自らへの助言等を含む本学の情報セキュリティ対策への助言、支援等を行う者として全学情報セキュリティアドバイザーを置く。

全学情報セキュリティアドバイザーは、本学における情報システムに関する技術的事項、情報セキュリティインシデントへの対処その他の情報セキュリティ対策に対する助言・支援を担うため専門的な知識及び経験を有した者、すなわち情報セキュリティに関する資格及び実務経験を有する者である必要がある。

なお、外部人材のみならず学内の職員を充ててもよい。この場合、当該職員が部局総括責任者やその他の責任者を兼務してもよい。

C1001-21 （情報セキュリティインシデントに備えた体制の整備）（政府機関統一基準の対応項番 2.1.1(6)）

第二十一条　全学総括責任者は、情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るため、CSIRT を設置し、その役割を明確化する。

２　全学総括責任者は、教職員等のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任する。そのうち、本学における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置く。

３　全学総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

解説：本学の情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、本学が、発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を整備することが必要である。

一般的に、情報セキュリティインシデントの認知時の対処においては、不完全で断片的な情報しかない状況で判断を下し、指示を出して、調査等により状況の解明を進めることとなる。CSIRT は、時々刻々と明らかになる情報を基に、

状況を整理し、事態の収束に向けてさらに必要な対応を行い、適切な頻度で幹部に状況を報告する。

CSIRT に属する職員は、本学における情報セキュリティインシデントを認知した際、全学総括責任者の指揮の下、これに対処する職員であることから、全学総括責任者に対して適切に状況を報告し、全学総括責任者の指示を受け適切に対処できることが必要である。
現場の対処においては、情報セキュリティ、情報システム等に関する知識及び技能を持つ者で、本学のネットワーク構成や個別システムの部局技術責任者及び管理者を把握している職員が当たることが望ましい。
また、CSIRT に属する職員には、上述した技術的な対処のほか、発生した情報セキュリティインシデントの影響の大きさによっては、対外的な対応も必要となることから、広報を担当する職員を CSIRT に含めておくことも考えられる。

CSIRT 責任者とは、情報セキュリティインシデントの対処に係る責任者であり、情報セキュリティインシデントに関する全般的な対応が求められる。ただし、重大な情報セキュリティインシデントが生じ、全学総括責任者自らが、情報セキュリティインシデントへ対処する必要があるときには、その指揮監督の下で必要な対応を行うこととなる。

CSIRT 責任者が情報システムを所管している場合、当該情報システムの情報セキュリティインシデントを認知した際、二つの役職が利害相反関係にあることから、全学総括責任者等の幹部に報告を上げない、事実関係の一部しか報告しない、報告を遅らせるなど、管理責任に影響を及ぼすおそれがある。
これを避けるため、例えば、CSIRT 責任者には部局総括責任者以外の者を充てる、全学総括責任者等の幹部に情報セキュリティインシデントについて報告する役割を別途 CSIRT 責任者以外の者に与えるなどにより、迅速かつ適切な報告経路を確保することが必要である。

C1001-22　（CSIRT の役割）（政府機関統一基準の対応項番 2.1.1(6)-1,2）
第二十二条　全学総括責任者は、以下を含む CSIRT の役割を別の規程にて定める。
一　報告窓口からの情報セキュリティインシデントの報告の受付
二　情報セキュリティインシデントの全学総括責任者等への報告
三　対外的な連絡
四　被害の拡大防止を図るための応急措置の指示又は勧告

解説：CSIRT の代表者は、学内外の関係機関と必要に応じて、情報セキュリティインシデントに関する情報共有を行うなど、外部窓口の役割を担うことが想定される。

C1001-23　（役割の分離）（政府機関統一基準の対応項番 2.1.1(7)）
第二十三条　情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。

一　承認又は許可事案の申請者とその承認又は許可を行う者（以下、本項において「承認権限者等」という。）

二　監査を受ける者とその監査を実施する者

解説：承認又は許可する役割の者自らが、申請をする場合には、その申請について自らが承認又は許可することはできない。このため、組織・体制及び申請手続を整備するに当たっては、このことに十分留意する必要がある。

2　前項の定めに係わらず、教職員等は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可（以下「承認等」という。）の可否の判断を行うことが不適切と認められる場合には、当該承認権限者等の上司に承認等の申請をする。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。

解説：承認や許可事案の内容によっては、承認権限者等が承認等の可否の判断を行うことが適切でない場合も想定される。このような場合は、その上司に申請し承認等を得ることになる。

なお、「兼務を禁止する役割の規定」を遵守する必要がある。したがって、自らが承認権限者の上司であったとしても、当該上司は自らに係る承認等の事案について自らが承認等してはならない。

3　教職員等は、前事項の場合において承認等を与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずる。

解説：承認権限者等の上司が承認等を行った場合に、当該上司に当該承認権限者等が遵守すべき事項に準じて、措置を講ずることを求める事項である。

例えば、機密性３情報、完全性２情報又は可用性２情報について、本学外での情報処理や本学支給以外の情報システムによる情報処理を職場情報セキュリティ責任者に代わって、その上司が許可する場合は、その上司に対して、許可の記録を取得することなどが求められる。

C1001-24　（情報の格付け）

第二十四条　全学情報システム運用委員会は、情報システムで取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備する。

解説：本学情報システムで取り扱う情報に対し、格付けを行うために必要となる基準等を定めることを求める事項である。なお、本規程に基づく情報の格付けについては「C2104 情報格付け基準」を参照されたい。

なお、本条項では政府機関統一基準に準拠し、書面については機密性の観点のみを考慮すればよいこととしているが、情報の格付け等の実施に際しては、情報システムに関する設計書等の書面についても完全性や可用性の観点から考慮することが望ましい。

C1001-25　（学外の情報セキュリティ水準の低下を招く行為の防止）

第二十五条　全学実施責任者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備する。

解説：学外の情報セキュリティ水準の低下を招く行為の防止に関して、全学実施責任

者が、規定を整備することを求める事項である。学外の情報セキュリティ水準の低下を招く行為としては、例えば、以下のものが挙げられる。
・本学のウェブのコンテンツを利用するために、ブラウザのセキュリティ設定の下方修正を明示的に要求する行為
・本学のウェブにより実行形式のファイル（Windows® の場合、「.exe」ファイル）を提供（メールに添付する場合も同様）する行為
・本学のウェブにより署名していない実行モジュール（Java® アプレットや Windows® の ActiveX® ファイル）を提供する行為
・本学から HTML メールを送信する行為
なお、後者の２つについては、利用者のウェブブラウザ等のセキュリティ設定の下方修正を誘発する可能性がある行為である。

２　本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずる。

解説：学外の情報セキュリティ水準の低下を招く行為の防止に関する各部局の役割を定めた事項である。本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、組織及び個人として措置を講ずることが重要である。

C1001-26　（情報システム運用の外部委託管理）

第二十六条　全学総括責任者は、本学情報システムの運用業務のすべてまたはその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

解説:その際、当該第三者との契約等により責任の範囲を明確にしておくものとする。

C1001-27　（情報セキュリティ監査）

第二十七条　情報セキュリティ監査責任者は、情報システムのセキュリティ対策がポリシー（情報システム運用基本方針及び本規程）に基づく手順に従って実施されていることを監査する。情報セキュリティ監査に際しては、別途定める情報セキュリティ監査規程に従う。

解説：情報セキュリティの確保のためには、本ポリシーに基づく実施規程、手順が適切に運用されることによりその実効性を確保することが重要であって、その準拠性、実効性及び対策の妥当性の有無が確認されなければならない。そのためには、独立性を有する者による情報セキュリティ監査を実施する必要がある。

C1001-28　（見直し）

第二十八条　本ポリシー、実施規程及び手順を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。

解説：本ポリシーに基づく実施規程、手順の内容を、必要に応じて見直すことを求める事項である。見直しを行う時期は、新たなセキュリティ脅威の出現、監査の評価結果等により、セキュリティ対策に支障が発生しないように本ポリシーに基づく実施規程、手順を整備した者が判断する必要がある。
情報セキュリティ対策の課題及び問題点に対処するため本ポリシーに基づく実施規程、手順を見直した者は、当該規定を見直した者が所属する部門以外の部

門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、その課題及び問題点に関連する部門の本ポリシーに基づく実施規程、手順を整備した者に対しても、同種の課題及び問題点の有無を確認するように連絡することを推奨する。

２　本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。

解説：本ポリシーに基づく実施規程、手順としては整備されていない情報セキュリティ対策についても、その見直しを本学情報システムを運用・管理する者、並びに利用者及び臨時利用者に求める事項である。

C1101 情報セキュリティインシデント対応チーム（CSIRT）運営規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2015年10月9日 C1101	新規作成	上原哲太郎（立命館大学）
2016年2月5日 C1101	PoCに関する記述を一部修正	上原哲太郎（立命館大学）
2017年10月17日 C1101	CSIRT及びその構成員の役割の明確化及び他規程等との整合確保のための修正	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説： A 大学においては、CSIRT は全学 CSIRT のみが単独で設置されている。大学の事情によっては、拠点や部局単位で複数の CSIRT を設置するほうが適切な場合も想定される。例えば附属大学病院が、教育・研究系部局とは高い独立性を有する形で運用され、情報セキュリティ対策に関しても独立した体制にて実施されている場合に、附属大学病院向けに別の CSIRT を設置・運用することが考えられる。また、学外へのインターネット接続を拠点ごとに行っているような場合も、接続単位で CSIRT を設置するほうが効率的なこともある。一方で、学内で複数の CSIRT を階層的に組織すると緊急時に CSIRT 間での相互連絡等が必要となるため、全学統括責任者等への報告により多くの手間や時間を要するなどの弊害もあり、大学の事情に応じて最適な体制を検討することが望ましい。また、CSIRT の運用を少人数で行わざるを得ない場合、夜間や長期休暇中に CSIRT が十分に機能しない可能性があり、こうした状況において情報セキュリティインシデントが発生したときの扱いについても定めておく必要がある（A 大学では外部委託にて対応している）。

１．設置

(1) 全学統括責任者は、情報セキュリティインシデント対応チーム（以下「CSIRT」という。）の活動が円滑に行えるよう、予算措置や適切な権限委譲を含めた環境を整えるとともに、必要に応じて活動内容について助言または指導を行うものとする。

(2) 部局統括責任者は情報セキュリティインシデントの発生に備え、CSIRT と連携して、連絡、報告、情報集約および被害拡大防止のための緊急対応に必要な体制を整える。

２．組織

解説： A 大学 CSIRT は、監視機能を外部 SOC に委託している。また、情報ネットワークに関する実務については、メディアセンタースタッフが CSIRT 構成員を支援することを想定している。また、(4)の対象者は学内教職員に限定されず、学外の専門家等をあてることも可能である。

(1) CSIRT は、情報セキュリティインシデント対応チーム責任者（以下、「CSIRT 責任者」という。）及び担当者で組織する。

(2) CSIRT 責任者は、CSIRT の業務を統括するとともに、学内外の関係機関と、必要に応じて情報セキュリティインシデントに関する情報共有に関する活動の責任者を務め、全学総括責任者が指名する。

(3) 担当者は、各部局総括責任者が本学教職員から１名以上を推薦し、全学総括責任者が委嘱する。このとき、自部局の教職員を推薦することを原則とするが、教職員の所属部局の部局総括責任者及び CSIRT 責任者の承認のもとで、他部局の教職員を推薦することも認める。

(4) CSIRT 責任者は、必要があると認めるときは、全学統括責任者の承認を得た上で、(3)に掲げた以外の者を指名して担当者に加えることができる。

(5) CSIRT 責任者は CSIRT の構成員の中から 1 名以上の情報セキュリティインシデント対応チーム副責任者（以下、「CSIRT 副責任者」という。）を指名する。CSIRT 副責任者は CSIRT 責任者から委譲を受けた場合に CSIRT 責任者の業務を代行することができる。

３．活動

解説： A 大学 CSIRT では、夜間・休日における情報セキュリティインシデント及びその他の連絡の受付と初動対応を、民間サービスに外部委託している。

担当者は、次に掲げる活動を行うものとする。このうち活動の一部について、CSIRT 責任者は予め全学統括責任者の承認を得た上で、外部委託を行うことができる。

(1) 本学における情報セキュリティインシデントの報告窓口として、学内からの情報セキュリティインシデントの可能性のある事象に関する情報を受け付けるとともに、本学情報ネットワークの監視に関する情報も活用することにより、情報セキュリティインシデントに関する事象を正確に把握すること。

解説： 学内利用者（教職員、学生等）に情報セキュリティインシデントであることを判断した上で報告させることは、判断誤りによる報告漏れにつながるため、その可能性を認知した段階で報告を求める必要がある。ただしこうした可能性を含めると端末やアプリケーションの不具合や混雑による応答低下なども含めた膨大な報告を受け付けざるを得なくなり、CSIRT における対応負荷も増えるため、ウェブによる報告記入画面を設けたり、トラブル相談窓口を別に設けたりするなどにより、CSIRT の機能を持続的に維持できるような仕組みを検討することが必要である。

(2) 情報セキュリティインシデントに関する外部機関との連絡窓口（PoC：Point of Contact）機能を、本学の総務部門や広報部門と連携して提供すること。

解説： この場合の外部機関としては、監視業務を委託している外部 SOC や他大学 CSIRT 等が該当する。なお、情報セキュリティインシデントが発生した際に文部科学省への報告を行うのは、CSIRT ではなく本学総務部門である。

(3) 情報セキュリティインシデントの発生時に、必要に応じて被害の拡大防止、復旧及び再発の防止にかかる技術的支援や助言を行うこと。

(4) 情報セキュリティインシデントの発生時に、予め全学統括責任者による承認を得た条件を満たす場合には、CSIRT 責任者による判断に従って本学情報ネットワークの緊急遮断措置を行うこと。これ以外の権限については、必要な場合はあらかじめ全学統括責任者から委譲を受けた措置について、全学統括責任者の承認を都度受けることなく行うことができる。

解説： CSIRT が本学情報ネットワークを緊急遮断する権限は、情報セキュリティインシデント対応に関する責任を全うするために必要な手段として全学統括責任者から CSIRT にあらかじめ与えられており、遮断を行う場合に全学統括責任者等に許可を求める必要はない。なお、情報セキュリティインシデントが解消した場合の本学情報ネットワークの復元については、CSIRT には部局情報シス

テムやネットワークに問題がないことを確認する権限がないことから、CSIRTが復元の可否を判断することはできず、各部局が自らの責任のもとで行うこととしている。

なお、A 大学では遮断に際して CSIRT 責任者（CSIRT 副責任者による代行を含む）が実施を判断することを前提としているが、これが不適切と考えられる場合は、各担当者に対応の優先順位を設定し、情報セキュリティインシデント発生時に対応可能な最上位の担当者が判断を行うことと定めてもよい。

(5) 学内の情報セキュリティインシデントの発生状況を定期的に取りまとめ、全学統括責任者に報告するとともに、対策に関する意思決定を支援すること。

(6) 情報セキュリティインシデントへの対処能力を向上させるため、必要に応じて CSIRT 構成員を対象とする研修や訓練などを実施すること。

４．雑則

この規程に定めるほか、CSIRT の運営に関して必要な事項は、別に定める。

解説： A 大学における CSIRT によるインシデント対応等の具体的な運用手順については、「C3102 インシデント対応手順」にて規定しているので、あわせて参照のこと。

附　則

この規程は、平成 XX 年 X 月 X 日から施行する。

C2101 情報システム運用･管理規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A2101	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A2101	統一基準（第2版）への対応と補足	国立大学法人等における情報セキュリティポリシー策定作業部会
2008年7月22日 A2101	誤記訂正	高等教育機関における情報セキュリティポリシー推進部会事務局
2011年3月31日 A2101	統一基準（第4版）対応と、A2101をもとに運用管理規程を策定した大学において修正された事項の取り込み	金谷吉成（東北大学）
2013年7月5日 B2101	統一基準（平成24年度版）をもとに全面改定	金谷吉成（東北大学）
2015年10月9日 C2101	統一基準（平成26年度版）をもとに全面改定	金谷吉成（東北大学）
2017年10月17日 C2101	統一基準（平成28年度版）をもとに改定	金谷吉成（東北大学）

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

第一章　総則

解説：(1) 本規程について

本規程は、「C1000 情報システム運用基本方針」及び「C1001 情報システム運用基本規程」（以下「ポリシー」という。）に基づき、A大学が最低限行うべき情報セキュリティ対策を定めるものである。

(2) 前版からの変更点

サンプル規程集（2013 年版）では、管理に関する規程として B210x シリーズを、技術に関する規程として B215x シリーズを定めていたが、本規程はこれらを統合するものとなっている。

(3) 政府機関統一基準との対応

本規程において、「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」及び「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」（以下「政府機関統一基準」という。）に対応する規定には、条文番号の後ろに政府機関統一基準の対応項番を付した。ただし、政府機関と大学とでは、その取り巻く環境、情報セキュリティ対策に取り組むべき主体等が異なることから、大学の実情に合わせて書き換えている箇所も多い。

(4) 規程の表現

本規程で定める多くの遵守事項は、政府機関統一基準に倣い、「……すること」の述語を用いている。サンプル規程集の学内規程化にあたっては、学内の他の規程に様式を合わせる必要がある。その場合、条文の内容を精査して、「……しなければならない」「……してはならない」（一定の作為又は不作為の義務を表す）や「……することができる」「……することができない」（一定の権利・権限等を与え又はこれを否認することを表す）などの述語に適宜あらためるとよい。「……しなければならない」ではニュアンスがきつすぎる場合は、「……するものとする」として表現を緩和する方法もある。

C2101-01　（趣旨）

第一条　この規程は、A大学情報システム運用基本規程第五条第二項第二号に基づき、A大学（以下「本学」という。）における情報システムの適切な運用及び管理について必要な事項を定めるものとする。

解説：本学の情報システムを適切に運用・管理するためには、「C1000 情報システム運用基本方針」及び「C1001 情報システム運用基本規程」（以下「ポリシー」という。）に基づき、情報システムの運用・管理の枠組みを構築し、情報セキュリティ水準の引上げを図ることが必要である。そこで本規程は、情報システムを適切に運用・管理するにあたって、いわゆる情報システムの管理者が情報セキュリティの確保のために採るべき対策、及びその水準を高めるための対策の基準を定めたものである。

情報及び情報システムの取扱いに関しては、大学の規程以外に法令や関連するガイドライン等（以下「関係法令等」という。）においても規定されているが、これらの関係法令等は本学情報システムの運用・管理にかかわらず当然に遵守すべきものであるため、本規程では、あえて関係法令等の遵守について明記し

ていない。
個人情報の取扱いについては、個人情報の保護に関する総合的な規程やガイドラインを別途定める方法の他、学内の各種規程の中に個人情報保護に関する規程を組込む方法などが考えられる。

C2101-02　（定義）

第二条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　運用基本方針　本学が定める「C1000 情報システム運用基本方針」をいう。

二　運用基本規程　本学が定める「C1001 情報システム運用基本規程」をいう。

三　実施手順　ポリシー及び実施規程に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。

四　情報セキュリティ関係規程　ポリシー、実施規程及び実施手順を総称したものをいう。

五　情報　運用基本規程第三条第二号に定めるものをいう。（参考：図 1）

六　情報システム　ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。（参考：図 1）

七　利用者　教職員等及び学生等で、本学情報システムを利用する許可を受けて利用する者をいう。

八　臨時利用者　教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用する者をいう。

九　利用者等　利用者及び臨時利用者のほか、本学情報システムを取り扱う者をいう。

十　機器等　情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。（参考：図 2）

十一　サーバ装置　情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。

十二　端末　情報システムの構成要素である機器のうち、利用者等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。

十三　モバイル端末　端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

十四　通信回線　複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

十五　通信回線装置　通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチルータ等のほか、ファイアウォール等も含まれる。

十六　学内通信回線　本学が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、本学の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。学内通信回線には、専用線や VPN 等物理的な回線を本学が管理していないものも含まれる。

十七　学外通信回線　通信回線のうち、学内通信回線以外のものをいう。

十八　VPN（Virtual Private Network）　暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。

十九　無線 LAN　IEEE802.11a、802.11b、802.11g、802.11n 等の規格により、無線通信で情報を送受信する通信回線をいう。

二十　MAC アドレス（Media Access Control address）　機器等が備える有線 LAN や無線 LAN のネットワークインタフェースに割り当てられる固有の認識番号である。識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割り当てる番号の組合せによって表される。

二十一　複合機　プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。

二十二　特定用途機器　テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。

二十三　ソフトウェア　サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OS や OS 上で動作するアプリケーションを含む広義の意味である。

二十四　アプリケーション　OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。

二十五　アルゴリズム　ある特定の目的を達成するための演算手順をいう。

二十六　記録媒体　情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。

二十七　基盤となる情報システム　学外の機関と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。

二十八　リスク　目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。

二十九　要管理対策区域　本学が管理する建物等（外部の組織から借用している施設等を含む。）本学の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。要管理対策区域の安全性を確保するため、以下のとおり３段階のクラスを定める。

クラス	説明
クラス３	一部の限られた者以外の者の立入りを制限する必要があるな

	ど､クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス２	教職員等以外の者の立入りを制限する必要があるなど､情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対策区域

便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。

三十　機密性　情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。機密性についての格付の区分は、以下のとおりとする。

格付の区分	分類の基準
機密性３情報	本学で取り扱う情報のうち､行政文書の管理に関するガイドライン（平成 23 年 4 月 1 日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	本学で取り扱う情報のうち､独立行政法人の保有する情報の公開に関する法律（平成 13 年 12 月 5 日法律第 140 号。以下、「独立行政法人等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって､「機密性３情報」以外の情報
機密性１情報	独立行政法人等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

三十一　完全性　情報が破壊、改ざん又は消去されていない特性をいう。完全性についての格付の区分は、以下のとおりとする。

格付の区分	分類の基準
完全性２情報	本学で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により､利用者等の権利が侵害され又は本学の教育研究事務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

三十二　可用性　情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。可用性についての格付の区分は、以下のとおりとする。

格付の区分	分類の基準
可用性２情報	本学で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより､利用者等の権利が侵害され又は本学の教育研究事務の安定的な遂行に支障(軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

三十三　要機密情報　機密性２情報及び機密性３情報をいう。

三十四　要保全情報　完全性２情報をいう。

三十五　要安定情報　可用性２情報をいう。

三十六　要保護情報　要機密情報、要保全情報及び要安定情報をいう。

三十七　取扱制限　情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを利用者等に確実に行わせるための手段をいう。

三十八　例外措置　利用者等がポリシー並びにそれに基づく規程及び手順等を遵守することが困難な状況で、教育研究事務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

三十九　情報の抹消　電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

四十　外部委託　本学の情報処理業務の一部又は全部について、契約をもって学外の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。

四十一　約款による外部サービス　民間事業者等の学外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

四十二　委託先　外部委託により本学の情報処理業務の一部又は全部を実施する者をいう。

四十三　クラウドサービス　事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

> 参考：ISO/IEC 17788 におけるクラウドサービスの定義
> ・cloud service
> One or more capabilities offered via cloud computing invoked using a defined interface
>
> ・cloud computing
> Paradigm for enabling network access to a scalable and elastic pool of Shareable physical or virtual resources with self-service provisioning and administration on-demand.
>
> NOTE - Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

四十四　クラウドサービス事業者　クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・運用する事業者をいう。

四十五　業務継続計画　本学において策定する BCP（Business Continuity Plan: 事業継続計画）をいう。

四十六　BCP（Business Continuity Plan: 事業継続計画）　組織において特定する事業の継続に支障をきたすと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適切に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。狭義には、このうちの事態発生後の事業の維持を主とした計画をいう。

四十七　主体　情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。

四十八　主体認証　識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、この規程における「主体認証」については、公的又は第三者による証明に限るものではない。

四十九　識別　情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。

五十　識別コード　主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。

五十一　主体認証情報　主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

五十二　主体認証情報格納装置　主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、IC カード等がある。

五十三　共用識別コード　複数の主体が共用するために付与された識別コードをいう。原則として、１つの識別コードは１つの主体のみに対して付与されるものであるが、情報システム上の制約や利用状況等に応じて、識別コードを組織で共用する場合もある。このように共用される識別コードを共用識別コードという。

五十四　アクセス制御　情報又は情報システムへのアクセスを許可する主体を制限することをいう。

五十五　権限管理　主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

五十六　アカウント　主体認証を行う必要があると認めた情報システムにおいて、主体に付与された正当な権限をいう。アカウントの付与は、主体認証情報（識別コードと主体認証情報を含む。）の配布、主体認証情報格納装置の交付、アクセス制御における許可、またはそれらの組み合わせ等によって行われる。

五十七　最小限の特権機能　管理者権限を実行できる範囲を必要最小限に制限する機能をいう。

五十八　暗号化　第三者が容易に復元することができないよう、定められた演算を施しデータを変換することをいう。

五十九　電子署名　情報の正当性を保証するための電子的な署名情報をいう。

六十　暗号モジュール　暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。

六十一　耐タンパ性　暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。

六十二　CRYPTREC（Cryptography Research and Evaluation Committees）　電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。

六十三　S/MIME（Secure Multipurpose Internet Mail Extensions）　公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。

六十四　不正プログラム　コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

六十五　不正プログラム定義ファイル　不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。

六十六　サービス不能攻撃　悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。

六十七　踏み台　悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。

六十八　セキュリティパッチ　発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。

六十九　アプリケーション・コンテンツ　アプリケーションプログラム、ウェブコンテンツ等の総称をいう。

七十　電子メールサーバ　電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。

七十一　電子メールクライアント　電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。

七十二　ウェブクライアント　ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。

七十三　ドメイン名　国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.example.ac.jp というウェブサイトの場合は、example.ac.jp の部分がこれに該当する。

七十四　名前解決　ドメイン名やホスト名と IP アドレスを変換することをいう。

七十五　ドメインネームシステム（DNS）　クライアント等からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係について回答を行うシステムである。

七十六　DNS サーバ　名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させるサーバ装置をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の２種類に分けることができる。

七十七　ルートヒントファイル　最初に名前解決を問い合わせる DNS コンテンツサーバ（以下

「ルート DNS」という。）の情報をいう。ルートヒントファイルには、ルート DNS のサーバ名と IP アドレスの組が記載されており、ルート DNS の IP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC（Internet Network Information Center）のサイトから入手可能である。

七十八　IPv6 移行機構　物理的に一つのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、サーバ装置及び端末並びに通信回線装置が２つの通信プロトコルを併用するデュアルスタック機構や、相互接続性の無い２つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。

七十九　その他の用語の定義は、運用基本規程の定めるところによる。

解説：(1) 用語の取り扱い

用語は、ポリシー、実施規程、手順・ガイドライン等を通して統一しておくこと。ただし、それぞれの規程の適用範囲に応じて特に定義しておくべき事柄については、それぞれの規程に定義を定めることができる。例えば、学生は「C2201 情報システム利用規程」を閲読してこれを遵守しなければならないが、「C2101 情報システム運用・管理規程」には必ずしも目を通さなくてよい。もちろん、アカウンタビリティの観点から、必要な場合に閲覧できるように準備しておくことは必要である。

サンプル規程集は、上位からポリシー（C1000 及び C1001）、実施規程（C2***）、手順（C3***）のような階層構造を有する。複数の下位規程において共通の用語を上位規程に定めることで、用語の不統一や同じ定義が複数の規程に現れる煩雑さをなくすことができる。しかし、ポリシーに詳細な用語定義を盛り込むことが規程体系の形式上難しかったり、用語定義を追加・変更するたびにポリシーを改訂することが手続き上複雑だったりするため、必要な用語定義を規程毎に置くことも多い。上位規程では参照しないが下位規程で参照する用語について、上位規程には置かず下位規程でその都度定める方法である。

(2) 利用者等

「利用者等」に外部委託の第三者を含むよう明記することも考えられる。なお、「本学情報システムを取り扱う」とは、情報システムを運用・管理するだけでなく、情報システムに係る情報を作成・利用することも含まれる。

本規程では、利用者、臨時利用者を含む広い概念として「利用者等」という用語を用いている。なお、主体認証の場面では、情報システムにアクセスする主体として利用者等に加え他の情報システムや装置も含めた「主体」という用語が用いられる。

(3) 情報の格付け及び取扱制限

情報の格付け及び取扱制限は、機密性、完全性、可用性の３つの観点を区別して行われなければならない。本規程では、機密性、完全性、可用性のそれぞれについて３ないし２段階の区分を定めている。これらの定義は「C2104 情報格付け基準」においても参照されるため、上位規程である「C1001 情報システム運用基本規程」に置くことも考えられる。

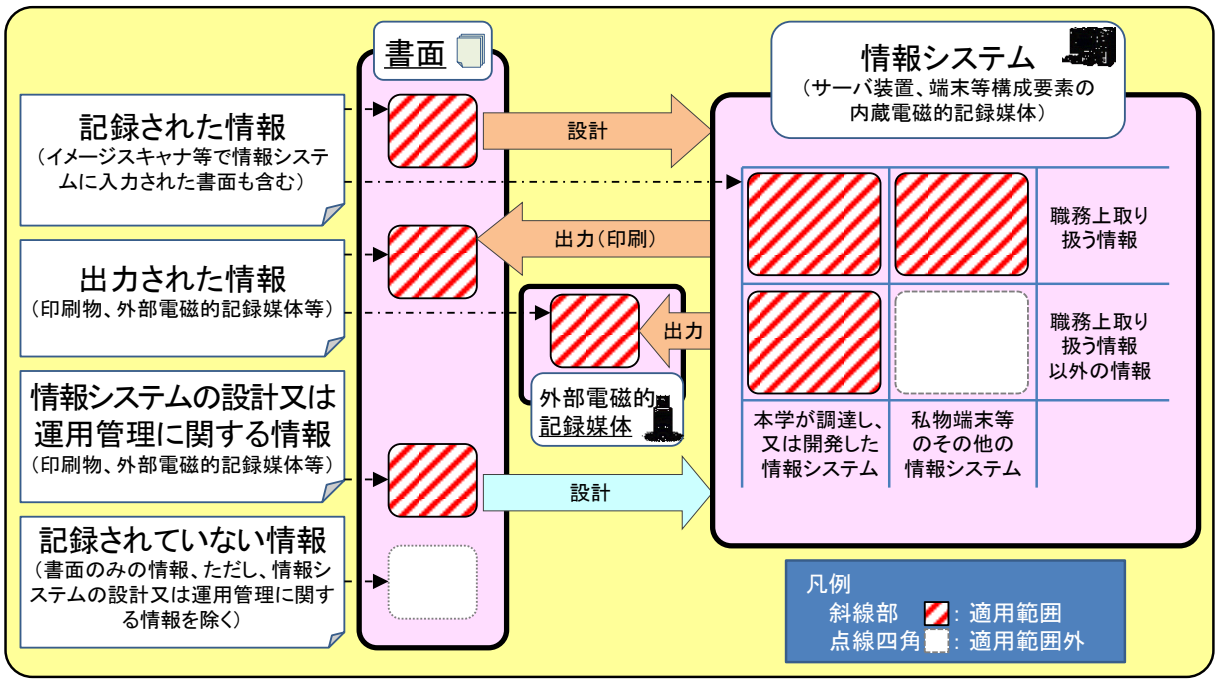


図１　本規程の適用を受ける「情報」の範囲

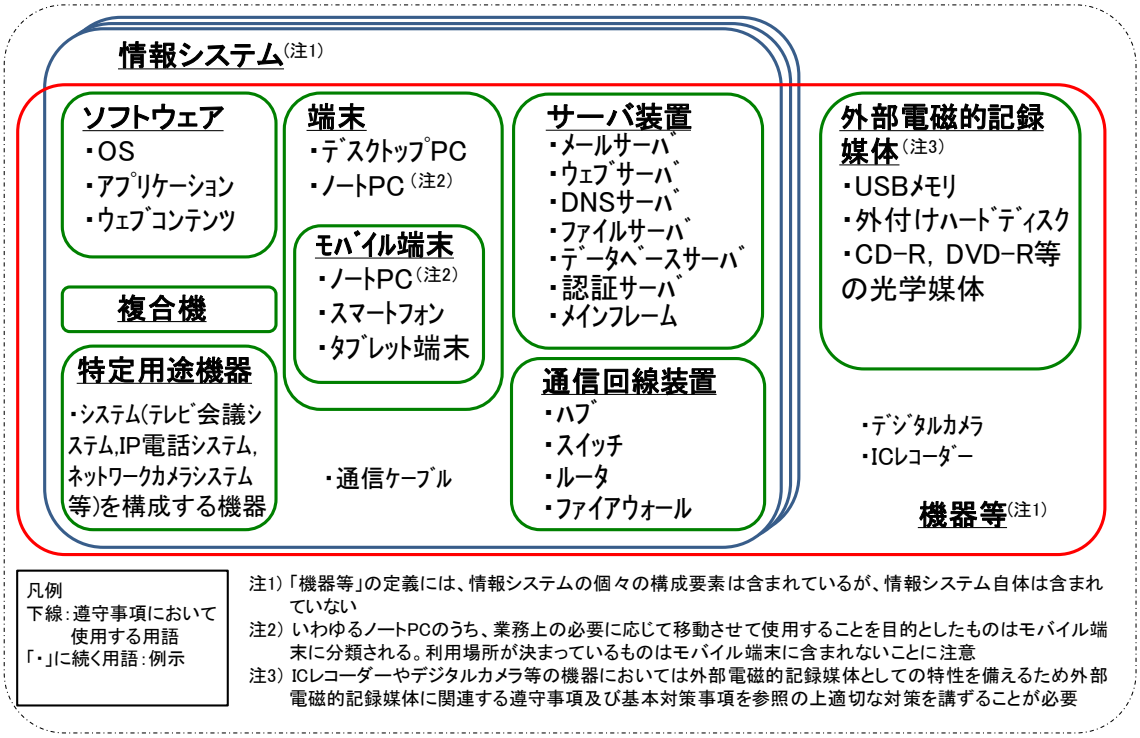


図２　「情報システム」、「機器等」及びその関係

C2101-03　（適用範囲）

第三条　この規程は、情報システムを運用・管理する者に適用する。

解説：情報システムを運用・管理する者とは、主としてポリシーに規定される全学総括責任者、全学実施責任者、情報セキュリティ監査責任者、部局総括責任者、

部局技術責任者、部局技術担当者、区域情報セキュリティ責任者、職場情報セキュリティ責任者、全学情報セキュリティアドバイザー、及び全学／部局情報システム運用委員会を指すが、教職員や学生等のいわゆる一般利用者にあっても、本学の情報システムの運用・管理を行う場合は、本規程を遵守しなければならない。

なお、「この規程は、情報システムを運用・管理する教職員等に適用する。」のように適用範囲を教職員等に限定し、学生等を対象とするものは利用規程に委ねてしまう考え方もある。学生を対象としないことを明記することで、学生に情報システムの運用・管理に関する何らかの義務や責任が生じることを避ける効果がある。また、大学によっては、情報システムの運用・管理は専ら教職員等の役割であって、学生等がそれらを行う場合であっても、あくまで教職員等の指揮監督の下で行われるという考え方もあって、その場合は敢えて学生等を除外しなくても同じことになる。適用範囲が明確な場合は、本条そのものを不要とする方法もある。

第二章　導入・計画

第一節　組織・体制

解説：情報セキュリティ対策は、それに係る全ての利用者等が、その身分並びに職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。

サンプル規程集では、組織・体制については「1001 情報システム運用基本規程」において定められている。

C2101-04　（組織・体制）

第四条　全学情報システムの運用・管理は、運用基本方針及び運用基本規程に従い、全学総括責任者の下、全学実施責任者、部局総括責任者及び部局技術責任者等からなる全学情報システム運用委員会が執り行うものとする。

２　部局情報システムの運用・管理は、運用基本方針並びに運用基本規程及び部局の運用方針に従い、部局総括責任者の下、部局技術責任者、部局技術担当者等からなる部局情報システム運用委員会が執り行うものとする。

３　全学の通信回線と部局の通信回線との調整及び学内通信回線と学外通信回線との接続に関する事項は、管理運営部局が執り行うものとする。

解説：組織・体制については、運用基本規程を参照のこと。

全学情報システム運用委員会及び部局情報システム運営委員会の所掌事務については、例えば次のような事項がある。規程において、これらの所掌事務をさらに具体的に明記する方法もある。

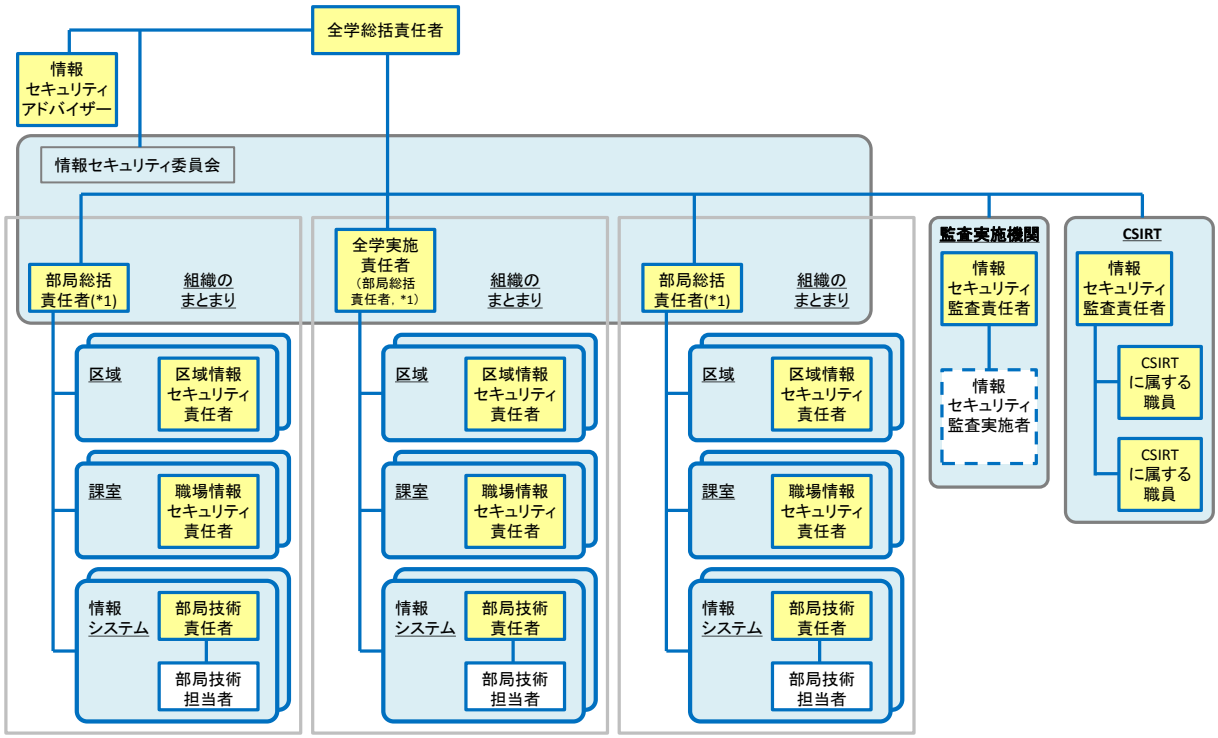
全学情報システム運用委員会の所掌事務：

一　ポリシー及び全学向け教育の実施ガイドラインの改廃に関する事項

二　情報システムの運用と利用及び教育に係る規程及び手順の制定及び改廃に

関する事項
三　情報システムの運用と利用に関する教育の年度講習計画の制定及び改廃、並びにその計画の実施状況の把握に関する事項
四　情報システム運用リスク管理規程の制定及び改廃に関する事項
五　情報セキュリティ監査規程の制定及び改廃に関する事項
六　情報システム非常時行動計画の制定及び改廃、並びにその計画の実施状況の把握に関する事項
七　情報セキュリティインシデントの再発防止策の検討及び実施に関する事項
部局情報システム運用委員会の所掌事務：
一　部局におけるポリシーの遵守状況の調査と周知徹底に関する事項
二　情報システムの運用と利用及び教育に係る規程及び手順に関して、部局において必要な規則の制定及び改廃に関する事項
三　情報システム運用リスク管理規程に関して、部局において必要な規則の制定及び改廃に関する事項
四　情報システム非常時行動計画に関して、部局において必要な規則の制定及び改廃に関する事項
五　部局における情報セキュリティインシデントの再発防止策の検討及び実施に関する事項
六　部局情報システムを運用・管理する者及び利用者等に対する教育研修の計画と企画及び実施に関する事項
なお、大学によっては、所掌事務に応じて複数の委員会を設置することもあり得る。例えば、情報システムにおける危機管理に関する事項について情報システム危機管理委員会を、情報システムにおける人権侵害及び著作権侵害情報等の発信防止等に関する事項について情報システム倫理委員会を設置するなどが考えられる。既存の他の学内委員会と所掌事務が重複するような場合は、その旨を規定において示す。

【参考】本学の情報セキュリティ体制のイメージ例
本学の情報セキュリティ体制のイメージを図 3 に示す。



※1　約款による外部サービス（ソーシャルメディアサービスを含む）を利用する場合に責任者を定める権限あり

図３　本学の情報セキュリティ体制のイメージ

C2101-05　（禁止事項）

第五条　部局技術責任者及び部局技術担当者は、次に掲げる事項を行ってはならない。

一　情報資産の目的外利用

二　守秘義務に違反する情報の開示

三　部局総括責任者の許可なく通信回線上を送受信される通信内容を監視し、又は通信回線装置及び電子計算機の利用記録を採取する行為

四　部局総括責任者の要請に基づかずにセキュリティ上の脆弱性を検知する行為

五　法令又は学内規則に違反する情報の発信

六　管理者権限を濫用する行為

七　上記の行為を助長する行為

解説：管理者権限の濫用とは、管理者権限を用いて一般利用者の個人情報を不正に取得したり、ネットワークを通じて行われる通信を規程によらず不正に傍受したりすること（積極的な濫用）の他、管理者用の端末装置で管理者アクセスの状態のまま席を離れたり、学外のインターネットカフェで管理者アクセスを行ったりすること（消極的な濫用）を含む。特に不特定多数の者が利用する共用端末では、キーロガー（キーボードからの入力を監視して記録するソフト等）が設置されていたりネットワーク上の通信が傍受されていたりする可能性があるため注意する。

第二節　対策推進計画の策定

解説：本学の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合

的に低減させるためには、本学として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果を踏まえ、計画的に対策を実施することが重要である。

C2101-06　（対策推進計画の策定）（政府機関統一基準の対応項番 2.1.2(2)）

第六条　全学総括責任者は、全学情報システム委員会における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めること。また、対策推進計画には、本学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含めること。

一　情報セキュリティに関する教育
二　情報セキュリティ対策の自己点検
三　情報セキュリティ監査
四　情報システムに関する技術的な対策を推進するための取組
五　前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

解説：「対策推進計画」について

対策推進計画は、情報セキュリティ対策に関する一連の取組を対象とした全体計画であり、情報セキュリティ対策に関する取組の全体方針のほか、本条の各号に掲げる情報セキュリティ対策に関する個々の取組について、全体方針に応じた個々の方針や重点、大まかな実施（予定）時期を設定するものである。

対策推進計画は、本学が組織として、種々の情報セキュリティ対策を如何なる考え方や方向性に基づいて進めていくのかといった一連の取組全体の大枠について、全学総括責任者があらかじめ総合的に定めるものであり、個々の取組の実施に当たって詳細計画が必要となる場合は、対策推進計画に則して、それぞれの取組の責任者がその権限の下に詳細計画を策定する。

「リスク評価の結果を踏まえた全体方針」について

情報セキュリティ対策は、情報セキュリティを取り巻く様々な脅威や、組織及び取り扱う情報の特性等を踏まえたリスクの分析・評価を行った上で、対策の方針や優先度を判断し、計画的に推進することが重要である。また、限られた予算や人的資源を最大限に活用して情報セキュリティ対策を推進するためには、対策全体としての方向付けを行った上で個々の対策を実施していくことが必要である。

全体方針としては、例えば、優先的に対応すべき脅威や優先的に対策を講ずるべき対象を設定し、それらへの対応を重点として掲げることが考えられる。

また、自組織の目的等を踏まえ、情報セキュリティ対策の自己点検の結果等を考慮した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講ずることが求められる。

「取組の方針・重点」について

本条の各号に掲げる情報セキュリティ対策に関する個々の取組の方針・重点は、

全体方針を踏まえ、例えば、情報セキュリティ対策の教育において、特定の脅威（例：標的型攻撃、サプライチェーン・リスク）、特定の対象（例：業務の内容や役職に応じた者）、特定の内容（例：情報セキュリティ関係規程の改正点）を掲げることが考えられる。

「情報システムに関する技術的な対策を推進するための取組」について
情報システムに関する技術的な対策を推進するための取組については、情報セキュリティ対策推進会議による「高度サイバー攻撃対処のためのリスク評価等のガイドライン」が参考になる。取組には、本学において独自に推進している技術的な対策を含めることが望ましい。技術的対策には、情報システムを構成する機器等の更新等の投資による対策も含まれる。

第三章　運用

第一節　情報セキュリティ関係規程の運用

解説：情報セキュリティ関係規程に定められた対策を実施するため、具体的な実施手順を定める必要がある。
実施手順が整備されていない、又はそれらの内容に漏れがあると、対策が実施されないおそれがあることから、全学総括責任者は、全学実施責任者に実施手順の整備を指示し、その結果について定期的に報告を受け、状況を適確に把握することが重要である。

C2101-07　（情報セキュリティ対策に関する実施手順の整備・運用）（政府機関統一基準の対応項番 2.2.1(1)）

第七条　全学実施責任者は、本学における情報セキュリティ対策に関する実施手順を整備（本規程で整備すべき者を別に定める場合を除く。）し、実施手順に関する事務を統括し、整備状況について全学総括責任者に報告すること。

２　全学実施責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動時等（入学、卒業を含む。）に関する管理の規定を整備すること。

３　部局総括責任者又は職場情報セキュリティ責任者は、利用者等より情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、全学実施責任者に報告すること。

解説：第１項「実施手順を整備（本規程で整備すべき者を別に定める場合を除く。）」について
本規程で整備を求めている実施手順は、以下のとおり。
（１）全学実施責任者
・情報セキュリティ対策における雇用の開始、終了及び人事異動時等（入学、卒業を含む。）の管理に関する規程（第七条第２項）
・情報セキュリティインシデントの可能性を認知した際の報告窓口を含む本学関係者への報告手順（第十九条第１項）
・情報セキュリティインシデントの可能性を認知した際の学外との情報共有を含む対処手順（第十九条第２項）

・情報の取扱いに関する規定（第三十六条）
・要管理対策区域の対策の基準（第五十四条第２項）
・外部委託に係る規定（第六十条）
・約款による外部サービスの利用に関する規定（第六十五条第１項）
・ソーシャルメディアサービスによる情報発信時における情報セキュリティ対策に関する運用手順等（第六十八条第１項）
・機器等の調達に係る選定基準（第七十六条第１項）
・機器等の納入時の確認・検査手続（第七十六条第２項）
・アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規定（第百四十二条）
・本学の情報システムの利用のうち、情報セキュリティに関する規定（第二百十三条第１項）
・要管理対策区域外で情報処理を行う際の安全管理措置に関する規定及び許可手続（第二百十三条第２項）
・USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順（第二百十三条第３項）
・本学支給以外の端末により情報処理を行う場合の許可等の手続に関する手順（第二百二十八条第１項）
・本学支給以外の端末により情報処理を行う場合の安全管理措置に関する規定（第二百二十八条第２項）

その他の者が定めるもの
a）全学総括責任者
・例外措置の適用の申請を審査する者及び審査手続（第十条第１項）
b）部局総括責任者
・利用者等ごとの自己点検票及び自己点検の実施手順（第二十四条第２項）
c）部局技術責任者
・情報セキュリティ対策を実施するために必要な文書（第七十四条）
・情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法（第百二十五条第２項）
・通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順（第百九十条第９項）

第１項「実施手順に関する事務を統括」について
全学実施責任者は、本学における情報セキュリティ対策に関する実施手順について、監査結果を通じて、ポリシー及びそれに基づく規程等に従って整備されていないことを把握した場合には、整備すべき者に対して指導することが想定される。
また、全学実施責任者は、情報セキュリティ関係規程について自己点検や監査の結果、例外措置の申請状況等を通じ、課題又は問題点について把握し得ることから、実施手順の整備主体が、特定の部局の部局総括責任者に係るものであ

ったとしても、同種の課題又は問題点の有無を他の部局等に確認することも想定される。

C2101-08　（違反への対処）（政府機関統一基準の対応項番 2.2.1(2)）

第八条　利用者等は、情報セキュリティ関係規程への重大な違反を知った場合は、部局総括責任者にその旨を報告すること。

２　部局総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、全学実施責任者を通じて、全学総括責任者に報告すること。

解説：第１項「部局総括責任者にその旨を報告する」について

本学において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉するための事項である。一般的に、本学においては、違反を知った者はこれを報告する義務が課されており、情報セキュリティ関係規程への違反においては、各規定の実施に責任を持つ部局総括責任者に報告することとなる。本規程は、利用者等から部局総括責任者への直接の報告を必須とするものではなく、重大な違反等の有無を部局総括責任者が確実に認識できるようにすること求めている。

なお、利用者等は、自ら違反した場合に限らず、他の利用者等が違反している場合においても、迅速な是正措置を促す理由から、当該利用者等への助言に加えて部局総括責任者に報告するなど適切に対応することが求められる。また、情報セキュリティ関係規程に係る課題及び問題点を認識した場合についても、部局総括責任者に報告することが望ましい。

第２項「情報セキュリティ関係規程への重大な違反」について

情報セキュリティ関係規程への重大な違反とは、当該違反により本学の業務に重大な支障をきたすもの又はその可能性のあるものをいう。例えば、機密性の極めて高い情報を保存した端末を、許可無く要管理対策区域外に持ち出し、それを紛失し、情報の漏えいが発生し、教育研究事務の遂行に著しく支障を来してしまった場合等が考えられる。

部局総括責任者は、本学において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉し、被害の未然防止又は拡大防止のための措置を適切に講じさせるとともに、再発防止に関する取組を進めることが求められる。

第２項「違反者及び必要な者」について

情報セキュリティ関係規程への重大な違反があった場合には、違反者自身が対策を講ずることは当然であるが、それ以外の「必要な者」として措置を義務付けられるのは、部局技術責任者、職場情報セキュリティ責任者及び区域情報セキュリティ責任者等の当該規程の実施に責任を有する者が挙げられる。情報システムの運用者や担当者、委託先等とも協力し、情報セキュリティを維持するために必要な措置を講ずる必要がある。

第２項「情報セキュリティの維持に必要な措置」について
重大な違反により、情報が漏えい、滅失、き損し又は情報システムの利用に支障を来した場合、早期解決、拡大防止等の対処を行う。拡大防止としては、情報セキュリティ関係規程について再周知の徹底が考えられる。

第２項「全学総括責任者に報告する」について
報告を受けた全学総括責任者は、その内容、結果、業務への影響、社会的評価等を確認し、本学全体として再発防止を徹底するなど、適切に対応する必要がある。
また、全学実施責任者は、同様の違反が多発している可能性の有無を考慮し、違反の原因について分析し、必要に応じて情報セキュリティ関係規程の見直しを含めた対策を検討する必要がある。

B2101-09　（違反に対する措置）

第九条　部局総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、速やかに調査を行い、事実を確認すること。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取すること。

２　部局総括責任者は、調査によって違反行為が判明したときには、次号に掲げる措置を講ずることができる。

一　当該行為者に対する当該行為の中止命令

二　部局技術責任者に対する当該行為に係る情報発信の遮断命令

三　部局技術責任者に対する当該行為者のアカウント停止命令、または削除命令

四　本学の懲罰委員会への報告

五　その他法令に基づく措置

３　部局総括責任者は、前項第二号及び第三号については、他部局の部局総括責任者を通じて同等の措置を依頼することができる。

４　部局総括責任者は、第二項の措置を講じた場合には、全学総括責任者にその旨を報告すること。

解説：違反行為によって引き起こされる影響が甚大である場合など、部局総括責任者による調査の前又は調査中であっても、緊急に必要最小限の措置を取らなければならない場合もあり得る。そのような場合を想定して、例えば次のような規定をここに置くことも考えられる。
「第二項に定めるほか、部局総括責任者は、第一項の調査の前又は調査中であっても、緊急の必要があると認める場合は、必要最小限の範囲で第二項第一号乃至第三号に掲げる措置を講ずることができる。」
また、全学総括責任者が必要に応じ、部局総括責任者に代わって措置する場合も考えられる。例えば、次のような規定になるだろう。
「全学総括責任者は、必要があると認める場合は、第一項から第三項までに定める行為を部局総括責任者に代わって行うことができる。全学総括責任者は、第一項から第三項までに定める行為を部局総括責任者に代わって行ったときは、その旨を部局総括責任者へ通知するとともに、当該措置の適切性について再検

証することとする。」
なお、本条の規定は政府機関統一基準に厳密に対応するものではない。政府機関統一基準では、情報セキュリティ関係規程への重大な違反により機密性、完全性、可用性が損なわれる等した情報及び情報システムの回復並びに情報セキュリティ対策の適切な実施の再徹底に主眼が置かれているが、本条では違反行為者への対処を中心に規定している。この部分は、各大学の特質や事情に応じて慎重に検討する必要がある。

第二節　例外措置

解説：例外措置はあくまで例外であって、濫用があってはならない。しかしながら、情報セキュリティ関係規程の適用が教育研究事務の適正な遂行を著しく妨げるなどの理由により、規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合がある。このような場合に対処するために、例外措置の手続を定めておく必要がある。

C2101-10　（例外措置手続の整備）（政府機関統一基準の対応項番 2.2.2(1)）

第十条　全学総括責任者は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び、審査手続を定めること。

２　全学実施責任者は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めること。

解説：第１項「例外措置の適用の申請を審査する者」について
例外措置の適用の申請を受けた際に審査を遅滞なく実施できるように、許可権限者を定め、審査手続を整備しておく必要がある。情報セキュリティ関係規程の誤った解釈や恣意的な例外運用を防止するために、例えば、情報セキュリティ関係規程を策定した者を許可権限者に充てることが考えられる。申請の内容に応じて、適切な許可を与える者を許可権限者として定めておくことが重要である。

C2101-11　（例外措置の審査手続）（政府機関統一基準の対応項番 2.2.2(1)(a)）

第十一条　全学総括責任者は、例外措置について以下を含む手順を定めること。

一　例外措置の許可権限者
二　事前申請の原則その他の申請方法
三　審査項目その他の審査方法

・申請者の情報（氏名、所属、連絡先）
・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
・例外措置の適用を申請する期間
・例外措置の適用を申請する措置内容（講ずる代替手段等）
・例外措置により生じる情報セキュリティ上の影響と対処方法
・例外措置の適用を終了した旨の報告方法
・例外措置の適用を申請する理由

C2101-12　（例外措置の適用審査記録の台帳）（政府機関統一基準の対応項番 2.2.2(1)(b)）

第十二条　許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、全学実施責任者へ定期的に報告すること。

一　審査した者の情報（氏名、役割名、所属、連絡先）

二　申請内容

・申請者の情報（氏名、所属、連絡先）
・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
・例外措置の適用を申請する期間
・例外措置の適用を申請する措置内容（講ずる代替手段等）
・例外措置の適用を終了した旨の報告方法
・例外措置の適用を申請する理由

三　審査結果の内容

・許可又は不許可の別
・許可又は不許可の理由
・例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等）
・例外措置の適用を許可した期間
・許可した措置内容（講ずるべき代替手段等）
・例外措置を終了した旨の報告方法

C2101-13　（例外措置の運用）（政府機関統一基準の対応項番 2.2.2(2)）

第十三条　利用者等は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請すること。ただし、教育研究事務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ること。

２　許可権限者は、利用者等による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。

３　許可権限者は、例外措置の申請状況を台帳に記録し、全学実施責任者に報告すること。

４　全学実施責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行い、全学総括責任者に報告すること。

解説：第１項「例外措置の適用を申請」について

利用者等は、定められた審査手続に従い例外措置の適用を申請し、許可を得てから例外措置を講ずることが原則であるが、教育研究事務の遂行に緊急を要するなどの場合であって、情報セキュリティ関係規程の規定内容とは異なる代替の方法を直ちに採用すること又は規定された対策を実施しないことが不可避のときは、事後速やかに届け出ることが必要である。

利用者等は、例外措置の適用を希望する場合には、当該例外措置を適用したときの情報セキュリティ上の影響を検討、分析する必要がある。その上で、例外措置の適用が必要であると判断した場合は、その影響を低減させるための補完措置を提案し、適用の申請を行う必要がある。

第２項「例外措置の適用の申請」・「審査」について
許可権限者は、例外措置の適用の申請を適切に審査しなければならない。審査に当たっては、例外措置の適用を許可した場合の情報セキュリティ上の影響と、不許可とした場合の教育研究事務遂行等への影響を評価した上で、その判断を行う必要がある。
例外措置の適用期間が長期にわたる場合等においては、例外措置の実施によるリスクが変化する可能性を踏まえ、定期的に当該措置の適用状況等を許可権限者において把握することも重要である。

第３項「全学実施責任者に報告」について
全学実施責任者は、許可権限者から例外措置の適用状況の報告を受ける。これは、第十三条第４項で情報セキュリティ関係規程の追加又は見直しの検討を行うためである。

第４項「情報セキュリティ関係規程の追加又は見直しの検討」について
例外措置の適用が多い状況は、例外とはみなせないと考えるべきである。その場合には、代替手段の導入を含め、情報セキュリティ関係規程の見直しを検討する必要がある。

第三節　教育

解説：情報セキュリティ関係規程が適切に整備されているとしても、その内容が利用者等に認知されていなければ、当該規定が遵守されないことになり、情報セキュリティ水準の向上を望むことはできない。このため、全ての利用者等が、情報セキュリティ関係規程への理解を深められるよう、適切に教育を実施することが必要である。
また、高等教育機関等における近年の情報セキュリティインシデントの増加等に鑑み、情報セキュリティの専門性を有する人材を育成することも求められる。

C2101-14　（教育体制等の整備）（政府機関統一基準の対応項番 2.2.3(1)）

第十四条　全学実施責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備すること。

C2101-15　（教育のための資料の整備）（政府機関統一基準の対応項番 2.2.3(1)-1）

第十五条　全学実施責任者は、利用者等の役割に応じて教育すべき内容を検討し、教育のための資料を整備すること。

解説：「教育すべき内容を検討」について
教育の内容については、最新の脅威動向、本学の実状や情報セキュリティインシデントの発生状況等、情報セキュリティ環境の変化等を踏まえ、幅広い角度から検討し、受講者の役割、責任及び技術に適したものにする必要がある。
さらに、教育の内容は、利用者等が対策内容を十分に理解できるものとする必要があり、そのためには、網羅的な資料ではなく、理解しておくべき事項に制

限した資料を教育に用いるべきである。例えば、情報セキュリティ関係規程の教育資料の作成においては、遵守事項を遵守すべき者ごとに整理し、利用者等が遵守する必要のない事項は、含まないように配慮すべきである。
また、違反の抑止効果を期待することを目的、ウェブサイトの閲覧に係るログを取得していることや、必要に応じて当該ログを調査することがあること等の情報システムの運用ルールを利用者等の教育内容に含めることも考えられる。
このような教育内容の検討に加えて、教育実施後に簡単なテストを実施することにより受講者の理解度を把握したり、受講者にアンケートを記入してもらったりすることで、次回開催のテーマや現在の教育方法等についての改善を検討することも考えられる。
なお、情報セキュリティ関係部署の者や CSIRT に属する職員に対して、情報セキュリティに関する知識及び技能を向上させるため、研修及び実務を模擬した訓練を実施することも有効である。訓練内容や実施結果の評価等について、全学情報セキュリティアドバイザーの助言を受けることも有用である。より高度な技能の習得や将来的な脅威への対応等を求めた訓練を実施する場所等においては、外部の専門事業者に委託することにより訓練を実施してもよい。

C2101-16　（教育実施計画の策定）（政府機関統一基準の対応項番 2.2.3(1)-2）

第十六条　全学実施責任者は、利用者等が毎年度最低１回は教育を受講できるように、教育実施計画を立案するとともに、その実施体制を整備すること。

解説：「利用者等が毎年度最低１回は教育を受講」について

対策推進計画に基づき、対象者、手段及び実施時期等の教育実施計画を定める。
教育実施計画の策定に当たっては、学内外の研修プログラムや e-learning 等の活用を含め、効率性や受講のしやすさにも配慮する必要がある。
また、教育実施計画には、情報セキュリティ担当者及び CSIRT に属する職員の人材育成について、キャリアパスにも配慮し、策定する必要がある。

C2101-17　（教育実施体制の整備）（政府機関統一基準の対応項番 2.2.3(1)-3）

第十七条　全学実施責任者は、利用者等の入学、着任又は異動後に、３か月以内に受講できるように、その実施体制を整備すること。

解説：「３か月以内に受講」について

入学、着任、異動した利用者等に対しては、早期に情報セキュリティ対策の教育を受講させることも有益であり、入学、着任後３か月以内には受講させるべきである。ただし、異動した後に使用する情報システムが、異動前と変わらないなど、教育をしないことについて合理的な理由がある場合は、対象から除外しても差し支えない。

C2101-18　（教育の実施）（政府機関統一基準の対応項番 2.2.3(2)）

第十八条　職場情報セキュリティ責任者は、利用者等に対して、情報セキュリティ関係規程に係る教育を適切に受講させること。

２　利用者等は、教育実施計画に従って、適切な時期に教育を受講すること。

３　職場情報セキュリティ責任者は、CSIRT に属する職員に教育を適切に受講させること。
４　全学実施責任者は、全学総括責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。

解説：第１項「適切に受講」について

職場情報セキュリティ責任者は、利用者等に情報セキュリティ対策の教育を受講させる責務があり、利用者等に対して教育の実施を周知するとともに、教育を受講しない者に対して受講を勧告するほか、受講状況を把握するなどして、積極的に受講を促すこと等が求められる。また、受講時間を確保するなどの利用者等が受講できるための環境を整備するなどの配慮も必要である。

第２項「適切な時期に教育を受講」について

利用者等は、教育実施計画に従って、毎年度最低１回は教育を受講することを求められる。

入学時、着任時又は異動時の場合には、新しい職場等で、情報セキュリティ対策の教育の受講方法について職場情報セキュリティ責任者に確認することも求められる。

第３項「CSIRT に属する職員に教育を適切に受講」について

情報セキュリティインシデントに迅速かつ適切に対処するための組織として本学に CSIRT が整備されている。これらに属する職員への教育も、その責務に照らすと極めて重要である。

第四節　情報セキュリティインシデントへの対処

解説：情報セキュリティインシデントを認知した場合には、全学総括責任者に早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、情報セキュリティインシデントの対処が完了した段階においては、原因について調査するなどにより、情報セキュリティインシデントの経験から今後に生かすべき教訓を導き出し、再発防止や対処手順、体制等の見直しにつなげることが重要である。

C2101-19　（情報セキュリティインシデントに備えた事前準備）（政府機関統一基準の対応項番 2.2.4(1)）

第十九条　全学実施責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む本学関係者への報告手順を整備し、報告が必要な具体例を含め、利用者等に周知すること。
２　全学実施責任者は、情報セキュリティインシデントを認知した際の学外との情報共有を含む対処手順を整備すること。
３　全学実施責任者は、情報セキュリティインシデントの可能性に備え、教育研究事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。
４　全学実施責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、教育

研究事務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備すること。

5　全学実施責任者は、情報セキュリティインシデントについて学外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を学外の者に明示すること。

6　全学実施責任者は、統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認すること。

解説：第１項「報告手順」について

報告手順として明記すべき事項としては、情報セキュリティインシデントの可能性が認知されてから全学総括責任者に報告するまでの具体的な手順等が考えられる。

また、情報セキュリティインシデントの可能性の報告窓口については、報告手順の中で明らかにしておくほか、情報セキュリティ対策の教育の中で周知する、報告窓口の連絡先を教室、研究室、事務室内に掲示するなどして、緊急時に利用者等が速やかに報告できるようにする必要がある。

報告窓口を CSIRT とは異なる部門に設ける場合は、当該部門から CSIRT への報告が速やかに実施される体制にすることが求められる。

第１項「報告が必要な具体例」について

第二十一条の解説「情報セキュリティインシデントの可能性を認知した場合は、本学の報告窓口に報告」を参照のこと。

第２項「対処手順」について

対処手順として情報セキュリティインシデントの認知時において緊急を要する対処等の必要性に備えて、通常とは異なる例外的な承認手続を定めておくことも併せて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想されるため、そのようなことがないよう検討すること。

第３項「緊急連絡網」について

全学実施責任者は、通常時の全ての情報セキュリティ関連の責任者及び管理者の連絡網の整備に加えて、情報セキュリティインシデントを認知した場合に速やかに対処するための「緊急連絡網」を整備する必要がある。

緊急連絡網には、該当する利用者等の自宅や携帯電話の番号等が含まれることも想定される。また、緊急連絡網には当該システムに係る責任者及び管理者のほか、重大な情報セキュリティインシデントに備えて全学総括責任者も含める必要がある。

第４項「訓練の内容及び体制を整備」について

実際に情報セキュリティインシデントへの対処を模擬的に行うことにより、対処能力を向上させるために実施する訓練の内容及び体制の整備を求める事項である。

実効的な訓練を実施するためには、情報システム部門だけでなく、情報セキュリティインシデントに関する報告窓口となる部門、情報セキュリティ対策に関する事務を総括する部門や CSIRT も参加することが望ましい。
なお、あらかじめ全学実施責任者が認めた場合には、全学実施責任者が指定した者に当該訓練の内容及び体制を整備させることも考えられる。その際には、全学実施責任者は、指定した者より適宜報告を受けることが望ましい。

第５項「学外の者から報告を受けるための窓口を設置」について
例として、外部の者が本学の情報セキュリティ対策の不備を発見した場合、本学への攻撃のおそれ等を認知した場合、本学の利用者等に情報セキュリティ上の脅威を与えていることを認知した場合（与えるおそれがある場合を含む。）等に、学外の者から連絡を受ける体制を整備することを求めている。

第６項「対処手順が適切に機能することを訓練等により確認」について
情報セキュリティインシデントは定常的に発生するものではないが、実際に発生した場合には、本学の事務に大きな影響をもたらすおそれがあるため、迅速かつ的確に対処を行うことが求められる。そのため、定めた対処手順が適切に機能することを訓練等によって確認しておくことが重要である。
訓練等には、実際に使用する機器を利用した「実機訓練」や、逐次の状況付与を受けて判断等を行う「ロールプレイング」、状況設定の上で手順の検証を行う「シミュレーション」といった大掛かりなもののほか、より簡易な「ウォークスルー」や「机上チェック」といった手法も存在する。CSIRT の取組状況や職員の習熟度等に応じて、必要な訓練等を検討し実施することが望まれる。

C2101-20　（情報セキュリティインシデント発生時の対処と報告に係る対策）（政府機関統一基準の対応項番 2.2.4(1)-1,2,3）

第二十条　全学実施責任者は、本学の附属機関等における情報セキュリティインシデント発生が報告された際にも、本学における情報セキュリティインシデントの場合と同様に、全学総括責任者や文部科学省に速やかに報告されるよう手順を定めること。

２　全学実施責任者は、情報セキュリティインシデト発生時の対処手順のうち、 意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等をあらかじめ定めておくこと。

３　全学実施責任者は、本学の附属機関等において発生した情報セキュリティインシデントについて、当該機関から報告・連絡を受ける窓口について定めるとともに、各機関にその窓口の連絡先を周知すること。

解説：第２項「意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等」について
例えば、本学 LAN 内での不正プログラム感染拡大やそれに伴う情報流出等が疑われる場合には、被害の拡大を阻止する措置を直ちに講ずることが重要である。そのような場合において、情報の重要度、情報が失われた場合のリスク、業務継続方法等を勘案した上で、調整等に時間をかけず直ちにネットワークを遮断するなどの措置を講ずるため、その手続や対象範囲等を事前に定めておく

ことが考えられる。これらの基準や手続は、政府機関を取り巻くサイバー攻撃事例や情報セキュリティインシデント事例を基に、適時見直すことが求められる。

C2101-22　（情報セキュリティインシデントへの対処）（政府機関統一基準の対応項番 2.2.4(2)）

第二十一条　利用者等は、情報セキュリティインシデントの可能性を認知した場合には、本学の報告窓口に報告し、指示に従うこと。

２　CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うこと。

３　CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、全学総括責任者に速やかに報告すること。

４　CSIRT は、情報セキュリティインシデントに関係する部局総括責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行うこと。

５　部局技術責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、本学で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処すること。

６　部局技術責任者は、認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処すること。

７　CSIRT は、本学の情報システムについて、情報セキュリティインシデントを認知した場合において、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。

８　CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて対処全般に関する指示、勧告又は助言を行うこと。

９　CSIRT は、情報セキュリティインシデントに関する対処の内容を記録すること。

１０　CSIRT は、情報セキュリティインシデントに関して、本学を含む関係機関と情報共有を行うこと。

解説：第１項「情報セキュリティインシデントの可能性を認知した場合には、本学の報告窓口に報告」について

利用者等に、情報セキュリティインシデントであることを判断した上で報告させることは、判断誤りによる報告漏れ等につながるため、その可能性を認知した段階で報告を求める必要がある。また報告窓口は CSIRT が担うことが望ましいが、別途の窓口を設ける場合には、CSIRT との連携が円滑に行われるよう連絡体制を整備する必要がある。報告窓口に報告する内容には、情報セキュリティインシデントの防止策を無効化したり、すり抜けられたりすることにより、被害に至らないまでも蓋然性が高まった状態も含まれる。例えば、不審な電子メールの添付ファイルを開いたり、URL リンクをクリックしたりしてしまった場合や、機密性の高い情報を保存したモバイル端末の所在が不明であるが、紛失したことや盗難されたことが確定的でない場合、平時の情報システムの利用において確認されないはずのエラーメッセージが端末に表示される場合等が想

定される。

第３項「全学総括責任者に速やかに報告」について
情報セキュリティインシデントの性質上、全ての状況が判然とするまでに時間がかかるものであるため、一度の報告で完了することはまれである。例えば、未確定情報を含んだ状態で第一報として報告し、その後に第二報、第三報と続けるような､適切な頻度で報告内容を更新する報告運用が望ましい｡その場合、何が確定し、何が未確定であるのかを明らかにすることが望ましい。全ての情報が確定するまで待って報告を遅らせるようなことは、あってはならない。

第４項「応急措置の実施及び復旧に係る指示又は勧告」について
応急措置や復旧に当たっては、情報セキュリティインシデントが発生した情報システムの停止、ネットワークの遮断等について、被害の拡大可能性、証拠保全、業務継続等を勘案し、CSIRT 責任者の判断で指示又は勧告をする。この場合には、情報セキュリティを推進する部局が CSIRT 責任者の指示又は勧告を支援することが望ましい。
なお、応急措置や復旧に関して、事前に決められた手順がある場合はその手順に従うことが求められる（第二十条解説「意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等」についてを参照のこと｡)。

第７項「サイバー攻撃又はそのおそれのあるもの」について
サイバー攻撃の例としては、不正侵入、改ざん、不正コマンド実行、情報かく乱、ウイルス攻撃、サービス不能攻撃等が挙げられる。また､「そのおそれのあるもの」とは、明らかなサイバー攻撃の痕跡が発見されていなくても、単なる機器の故障や操作上の誤りではなく、サイバー攻撃により発生した情報セキュリティインシデントであることが疑われる場合のことである。

第７項「情報セキュリティインシデントの内容に応じ」について
サイバー攻撃又はそのおそれがある情報セキュリティインシデントを認知した場合で、当該情報セキュリティインシデントが犯罪に該当するときには、警察への通報・連絡等を求めるものである。明らかなサイバー攻撃に限らず、そのおそれがある場合についても、被害拡大の防止の観点から、可能な限り速やかな通報等を行うことが望ましい。

第７項「警察への通報・連絡等」について
「通報・連絡等」の内容としては、相談、届出、告訴又は告発を想定している。
サイバー攻撃又はそのおそれがある情報セキュリティインシデントが発生した場合、当該サイバー攻撃等による被害の拡大を防止するとともに、攻撃者を追跡するため、警察が的確に初動措置を講ずる必要があることから、可能な限り速やかな通報・連絡等を求めている。
なお、その通報先は、各都道府県警察のサイバー攻撃対策部門であり、具体的

には、警視庁では公安部公安総務課、道府県警察では警備部のサイバー攻撃対策担当課である。また、警察への通報に関する質問等については、警察庁警備局警備企画課において受け付けている。

第１０項「情報共有を行う」について
政府機関における情報共有の枠組みとしては、「政府におけるサイバー攻撃等への対処態勢の強化について」（平成 22 年 12 月 27 日情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ）において、「各府省庁は、その業務において得たサイバー攻撃に係る情報を、可能な限り速やかに内閣官房情報セキュリティセンターに連絡する。また、内閣官房情報セキュリティセンターは、収集・集約された情報をサイバー攻撃に対する初動対処、被害の拡大防止及び再発防止に活用するため、情報連絡を行った府省庁の同意を得た上で、各府省庁に対して積極的な情報提供を行う」と記載されている。

C2101-22　（CSIRT における情報共有と役割分担に係る対策）（政府機関統一基準の対応項番 2.2.4(2)-1,2）

第二十二条　CSIRT は、情報セキュリティインシデントではないと評価した場合であっても、注意喚起が必要と考えられるものについては、関係する者に情報共有を行うこと。

２　CSIRT 責任者は、認知した情報セキュリティインシデントの種類や規模、影響度合い等を勘案し、必要に応じて、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局の役割分担を見直すこと。

C2101-23　（情報セキュリティインシデントの再発防止・教訓の共有）（政府機関統一基準の対応項番 2.2.4(3)）

第二十三条　部局総括責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として全学総括責任者に報告すること。

２　全学総括責任者は、部局総括責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示すること。

３　CSIRT 責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、全学実施責任者、関係する部局総括責任者等に共有すること。

解説：第１項「再発防止策を検討」について

一般に、再発防止策を定めるには、十分な原因調査を行い、どのような要素が絡んで情報セキュリティインシデントに至ったのか、因果関係を明らかにした上で、原因から情報セキュリティインシデントの発生段階の間で、因果関係の進行を断ち切るための防護策を複数検討し、講ずることが有効である。また、対策については、情報セキュリティインシデントが発生したシステム単独で講ずるよりも、他のシステムにも同様に展開することにより（水平展開）、類似事案の発生を組織全体にわたって食い止めることが可能となる。

なお、水平展開については、自らの組織の再発防止策に限らず、他組織の事案を参照することにより、事後対処よりも先んじた未然防止が可能となり、対応

コストの低減も期待される。
さらに、再発防止策は、情報システムの利用手順で対策する方法及び情報システムへの情報セキュリティ機能の実装による対策を部局技術責任者へ求める方法の両面から検討し、必要な対策を定めて実施する必要がある。情報システムへの情報セキュリティ機能の実装には一定の時間を要することも考えられることから、利用手順による対策を暫定的に実施し、その後、機能追加により本格的な対策を行うなど段階的な実施も考慮する必要がある。

第２項「再発防止策を実施するために必要な措置」について
全学総括責任者は、情報セキュリティインシデントの再発防止策の報告を受けた場合は、その内容を確認する必要がある。
情報システムへの情報セキュリティ機能の実装等計画的に実施する必要がある再発防止策については、対策推進計画に反映させるなどして、適切に実施させるよう取組を推進することが求められる。また、他大学と連携して再発防止策を講ずることが有効と想定される場合は、他大学と協力して取組を進めることも求められる。

第３項「得られた教訓を、全学実施責任者、関係する部局総括責任者等に共有」について
CSIRT 責任者には、全学実施責任者、関係する部局総括責任者等に対し、単に情報セキュリティインシデントの情報を共有するだけでなく、情報セキュリティインシデントの対処を踏まえ、全学実施責任者が定める対処手順等の改善や、個別の情報システムの情報セキュリティ水準の改善につなげられるような事項を含めて共有することが求められる。

第四章　点検

第一節　情報セキュリティ対策の自己点検

解説：情報セキュリティ対策の実効性を担保するためには、情報セキュリティ関係規程の遵守状況等を点検し、その結果を把握・分析することが必要である。
自己点検は、利用者等が自らの役割に応じて実施すべき対策事項を実際に実施しているかどうかを確認するだけではなく、組織全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要である。
また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

C2101-24　（自己点検計画の策定・手順の準備）（政府機関統一基準の対応項番 2.3.1(1)）
第二十四条　全学実施責任者は、対策推進計画に基づき年度自己点検計画を策定すること。
２　部局総括責任者は、利用者等ごとの自己点検票及び自己点検の実施手順を整備すること。

解説：第１項「年度自己点検計画を策定」について
点検を実施するに当たり、対策推進計画に基づき適切に実施するため、実施頻

度、実施時期、確認及び評価の方法や自己点検項目等を定めた年度自己点検計画を策定することが求められる。
自己点検項目の選定に当たっては、情報セキュリティインシデントの発生状況に鑑みた項目や、前年度の自己点検実施率が低かった遵守事項等、様々な選択肢が考えられる。

第２項「利用者等」について
本規定における「利用者等」は、教職員等及び学生等の利用者並びに臨時利用者以外に部局総括責任者、職場情報セキュリティ責任者及び部局技術責任者等、情報セキュリティ対策の体制ごとの責任者を含む。具体的にどの責任者を対象に自己点検を実施するかについては、年度自己点検計画で策定する。
部局総括責任者や職場情報セキュリティ責任者は、所管する組織の情報セキュリティ対策について、部局技術責任者（管理者）は、所管する情報システムについて、区域情報セキュリティ責任者は、所管する区域における情報セキュリティ対策について実施するなど、役割に応じて異なることに留意が必要である。
なお、部局技術責任者の点検は、情報システムに係る各種セキュリティ対策の実施状況等を様々な観点で実施することが必要である。例えば、ソフトウェアの脆弱性への対処状況の点検であれば、セキュリティパッチや不正プログラム定義ファイルの更新状況を把握したり、実際の文書を確認したりすることで実施状況を把握するなど、代替の確認方法を含めた点検が考えられる。

第２項「自己点検票」について
各利用者等が自己点検を実施するに当たっては、各自の業務における情報の取扱方法や、実施すべき情報セキュリティ対策上の役割が異なるため、それぞれの職務内容に即した自己点検票が必要となる。そのため、部局総括責任者は、利用者等ごとの自己点検票を作成するとともに、自己点検の正確性を高めるために詳細な実施手順を準備することが重要である。

C2101-25　（自己点検の実施）（政府機関統一基準の対応項番 2.3.1(2)）
第二十五条　部局総括責任者は、年度自己点検計画に基づき、利用者等に自己点検の実施を指示すること。
２　利用者等は、部局総括責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。

解説：　第１項「自己点検の実施」について
自己点検は、年に２度以上の頻度で実施することが望ましい。例えば、情報システム部門に対しては、毎月実施し、それ以外の部門に対しては、半年に一度の頻度で実施するなどが考えられる。

C2101-26　（自己点検結果の評価・改善）（政府機関統一基準の対応項番 2.3.1(3)）
第二十六条　全学実施責任者及び部局総括責任者は、利用者等による自己点検結果を分析し、評

価すること。全学実施責任者は評価結果を全学総括責任者に報告すること。

２　全学総括責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、全学実施責任者及び部局総括責任者に改善を指示し、改善結果の報告を受けること。

解説：第２項「自己点検結果を全体として評価」について

利用者等による自己点検の結果については、部局総括責任者が評価し、さらに、部局総括責任者の自己点検の結果を全学実施責任者が評価する。

評価においては、自己点検が正しく行われていること、情報セキュリティ関係規程に準拠していること、改善すべき事項が改善されていること、対策が有効であること等を評価する。この自己点検の評価においても、数値評価を中心とし、客観性を持った評価とすることが望ましい。例えば、自己点検実施率（対策実施数／自己点検回答数）等の把握が挙げられる。

第二節　情報セキュリティ監査

解説：情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。

また、監査の結果で明らかになった課題を踏まえ、全学総括責任者は、部局総括責任者に指示し、必要な対策を講じさせることが重要である。

C2101-27　（監査実施計画の策定）（政府機関統一基準の対応項番 2.3.2(1)）

第二十七条　情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定めること。

２　情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施の指示を、全学総括責任者から受けた場合には、追加の監査実施計画を定めること。

解説：第１項「対策推進計画に基づき監査実施計画を定める」について

第六条に規定する対策推進計画には、監査の基本的な方針として、重点とする監査の対象及び目標（今年度の監査でどのような部分を重視するかを明確にする）・監査の実施時期・監査業務の管理体制等を簡潔に記載することを想定している。監査の基本的な方針の案は、情報セキュリティ監査責任者が作成することを想定している。また、情報セキュリティ監査責任者は、対策推進計画に基づき、個別の監査実施計画を策定し、監査を実施する。

第２項「追加の監査実施計画を定める」について

全学総括責任者は、学内外における注目すべき情報セキュリティインシデントが発生した場合又は情報セキュリティ対策の実施内容に重大な変更が生じた場合等において、本学の実態を把握するため、追加的に監査の実施を求めることが想定される。この監査の実施の指示を受けた場合、情報セキュリティ監査責任者は、対策推進計画に基づき策定した監査実施計画のほかに、当該指示に係る監査実施計画を策定することとしている。

C2101-28　（監査実施計画の記載事項）（政府機関統一基準の対応項番 2.3.2(1)-1）

第二十八条　情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定すること。

一　監査の目的（例：自己点検の適切性を監査すること等）

二　監査の対象（例：監査の対象となる組織、情報システム、業務等）

三　監査の方法（例：自己点検結果を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、ポリシー及びそれに基づく規程等とする）

四　監査の実施体制（例：監査責任者、監査実施者の所属、氏名）

五　監査の実施時期（例：対象ごとの実施時期）

解説：「監査実施計画」について

対策推進計画に基づき実施すべき監査についての詳細な計画として、監査実施計画を策定する必要がある。監査実施計画に記載すべき項目としては、この条に例示のとおり、監査の目的、対象、方法、実施体制及び実施時期等が考えられる。この他に経済産業省「情報セキュリティ監査基準 実施基準ガイドライン Ver1.0」等にも詳細が説明されているので参考にするとよい。

参考：経済産業省「情報セキュリティ監査基準 実施基準ガイドライン Ver1.0」（http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex05.pdf）

被監査部門に対して監査の内容や範囲を明確化するために、監査実施期間、監査実施者の氏名、監査対象等を含む事項等を、情報セキュリティ監査責任者より事前通知することが望ましい。

なお、監査実施者が監査過程で情報セキュリティの向上につながる対策等の監査以外の行為を行った場合には、その行為に対する別途の監査が必要となる可能性がある。したがって、情報セキュリティ監査責任者は、情報セキュリティ対策の向上になり得る行為や、作業を効率的に行うことにつながる行為であるとしても、監査以外の行為を監査実施計画の中に取り込むべきではない。

C2101-29　（監査の実施）（政府機関統一基準の対応項番 2.3.2(2)）

第二十九条　情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む監査の実施を監査実施者に指示し、結果を監査報告書として全学総括責任者に報告すること。

二　実施手順がポリシー及びそれに基づく規程等に準拠していること

三　自己点検の適正性の確認を行うなどにより、被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること

解説：「監査報告書」について

監査報告書の作成に際しては、根拠となる監査調書を適切に作成することが必要である。監査調書とは、情報セキュリティ監査実施者が行った監査業務の実施記録であって、監査報告書に記載する監査意見の根拠となるべき監査証拠、その他関連資料等をつづり込んだものをいう。情報セキュリティ監査実施者自らが直接に入手した資料や試験の結果、被監査部門側から提出された資料のほか、場合によっては外部の第三者から入手した資料等を含むことがある。

監査の結果は、監査報告書として文書化した上で、全学総括責任者へ確実に提

出する必要がある。監査報告書には、実際の運用状況が情報セキュリティ関係規程に準拠して行われているかなどの結果を記載する。さらに、監査の過程において、情報セキュリティ対策の内容の妥当性に関連して改善すべき課題及び問題点が検出された場合には、この検出事項や助言・提案を監査報告書に含める。反対に組織として推奨すべき優れた取組等がある場合には、それらを組織全体に広めるなどの助言・提案があってもよい。

第３号「実際の運用」について
自己点検の適正性の確認や自己点検結果に基づく担当者への質問、記録文書の査閲及び機器の設定状況の点検等の方法により、運用の準拠性を確認する。また、必要に応じて、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かを確認することも求められる。例えば、監査対象によってはソフトウェアやウェブアプリケーション等の情報システムに関連する脆弱性の検査、情報システムに対する侵入検査といった方法によっても確認することができる。

C2101-30　（情報セキュリティ監査実施者）（政府機関統一基準の対応項番 2.3.2(1)-1,2）

第三十条　情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名すること。

２　情報セキュリティ監査責任者は、組織内における監査遂行能力が不足等している場合には、学外の者に監査の一部を請け負わせること。

解説：第１項「被監査部門から独立した者」について
情報セキュリティ監査実施者には、監査人としての独立性及び客観性を有することが求められる。例えば、情報システムを監査する場合に、当該情報システムの構築をした者や運用を行っている者が監査をしてはならない。また、情報の取り扱われ方に関する監査を行う場合には、当該情報を取り扱う者はその監査をしないこととする。

第２項「学外の者に監査の一部を請け負わせる」について
情報セキュリティ監査責任者は、監査を実施するに当たり、学内に情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮することが重要である。また、監査業務を外部事業者に請け負わせることは、外部委託に該当することから、関連する規定にも留意する必要がある。また、情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の業務への関与等を考慮することが望ましい。
参考：経済産業省「情報セキュリティ監査企業台帳に関する規則」
（http://www.meti.go.jp/policy/netsecurity/docs/isaudit/audit_register_regulation.pdf）

C2101-31　（監査結果に応じた対処）（政府機関統一基準の対応項番 2.3.2(3)）

第三十一条　全学総括責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を部局総括責任者に指示すること。

２　部局総括責任者は、監査報告書等に基づいて全学総括責任者から改善を指示されたことについて、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を全学総括責任者に報告すること。

解説：第２項「計画を策定」について

部局総括責任者が、監査報告書に基づいて全学総括責任者からの改善を指示されたことについて、改善計画の策定及び全学総括責任者への報告を求める事項である。部局総括責任者は、監査報告書において指摘された課題及び問題点の改善が困難であることについて正当な理由がある場合には、その影響を低減させるための補完措置を示した上で、達成することが可能な対処計画を全学総括責任者へ報告する。

C2101-32　（政府機関統一基準の対応項番 2.3.2(3)-1）

第三十二条　全学総括責任者は、監査報告書の内容を踏まえ監査を受けた部門以外の部門においても同種の課題又は問題点がある可能性が高く、並びに緊急に同種の課題又は問題点があることを確認する必要があると判断した場合には、他の部門の部局総括責任者に対しても、同種の課題又は問題点の有無を確認するように指示すること。

解説：「指示」について

全学総括責任者は、監査報告書において指摘事項が、他の組織にも同種の課題又は問題点として存在する可能性が高い場合、並びに同種の課題又は問題点の存在を緊急に確認する必要性が高い場合、想定される他の組織についても、調査を求める事項である。

B2101-33　（監査への協力）

第三十三条　部局総括責任者その他の関係者は、情報セキュリティ監査責任者の行う監査の適正かつ円滑な実施に協力すること。

第五章　見直し

第一節　情報セキュリティ対策の見直し

解説：情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、本学の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、実際の運用において生じた課題、自己点検、監査の結果や情報セキュリティに係る重大な変化等を踏まえ、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、適時見直しを行う必要がある。

また、情報セキュリティに係る取組をより一層推進するためには、上記のリス

ク評価の結果を対策推進計画に反映することも重要である。

C2101-34　（情報セキュリティ関係規程の見直し）（政府機関統一基準の対応項番 2.4.1(1)）

第三十四条　全学総括責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、全学情報システム運用委員会の審議を経て、ポリシー及びそれに基づく規程等について必要な見直しを行うこと。

２　全学実施責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について全学総括責任者に報告すること。

解説：第１項「情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価」について

学内における情報セキュリティインシデントの発生状況、例外措置の申請状況、自己点検や情報セキュリティ監査の結果、利用者等からの相談等を踏まえ、ポリシー及びそれに基づく規程等に課題及び問題点が認められるかどうかなどの観点から、総合的な評価を行い、所要の見直しを行うことについて、全学総括責任者に求めている。

また、本部監査において助言された事項に関し、規程等を見直す必要があるかどうかを確認し、必要とされる場合には規程等の見直しを行う。

第２項「整備した者に対して規定の見直しを指示」について

学内における情報セキュリティインシデントの発生状況、自己点検や情報セキュリティ監査の結果、本部監査の結果、利用者等からの相談、全学総括責任者からの指示等を踏まえ、情報セキュリティ対策に関する実施手順を見直すことの必要性を検討し、部局技術責任者等の実施手順を整備した者に、その見直しを指示することを全学実施責任者に求めている。

なお、策定済みの実施手順を見直すだけではなく、例えば、学内における共通のルールが存在しないため、各所属等において個別にルールを定めて運用しているなどの場合について、学内における共通のルールを整備するか否かを検討することも考えられる。

C2101-35　（対策推進計画の見直し）（政府機関統一基準の対応項番 2.4.1(2)）

第三十五条　全学総括責任者は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、全学情報システム運用委員会の審議を経て、対策推進計画について定期的な見直しを行うこと。

解説：「情報セキュリティ対策の運用及び点検・監査等を総合的に評価」について

学内における情報セキュリティインシデントの発生状況、自己点検、情報セキュリティ監査の結果、利用者等からの相談等を踏まえ、対策推進計画に加えるべき事項の有無、策定済みの計画の変更が必要であるか等の観点から、評価を行う。

また、本部監査において助言された事項において、対策推進計画に盛り込むべき事項がある場合は、当該事項の実施優先順位を検討した上で、適切に計画に

盛り込むこととする。

「情報セキュリティに係る重大な変化等」について
サイバー攻撃の量的な拡大や攻撃手法の高度化等による質的な変化等、計画策定時に前提としていた条件から大きく異なり、情報セキュリティに係るリスクが高まった場合や、年度途中における種々の要因により、当初の対策推進計画では課題解決が図られていない場合等を想定している。

第六章　情報の取扱い

第一節　情報の取扱い

解説：教育研究事務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下、本項において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての教職員等が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、教職員等は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。
なお、秘密文書の管理に関しては、文書管理ガイドラインの規定を優先的に適用した上で、当該ガイドラインに定めが無い情報セキュリティ対策に係る事項については、本規程の規定に基づき、適切に情報が取り扱われるよう留意すること。

C2101-36　（情報の取扱いに係る規定の整備）（政府機関統一基準の対応項番 3.1.1(1)）

第三十六条　全学実施責任者は、以下を含む情報の取扱いに関する規定を整備し、教職員等へ周知すること。

一　情報の格付及び取扱制限についての定義
二　情報の格付及び取扱制限の明示等についての手続
二　情報の格付及び取扱制限の継承、見直しに関する手続

解説：第１号「格付及び取扱制限についての定義」について
「C1001 情報システム運用基本規程」第二十四条及び第二条第三十号から第三十二号までに掲げる情報の格付の区分（機密性・完全性・可用性についての格付の定義）並びに第二条第三十七号に掲げる取扱制限の定義に基づき、機密性、完全性、可用性に係る情報の格付と取扱制限について、本学の基準を整備する必要がある。
なお、文書ガイドラインにおいて、「文書の作成者は、当該文書が極秘文書又は秘文書に該当すると考えられる場合には、それぞれに準じた管理を開始する」とされており、指定前の秘密文書も、機密性３情報として管理することが求められる。

第２号「格付け及び取扱制限の明示等」について
秘密文書においては、文書管理ガイドラインにおける「秘密文書表示」を行った場合には、別途「機密３情報」に係る明示等を行う必要はない。

C2101-37　（情報の取扱いに係る手順の整備）（政府機関統一基準の対応項番 3.1.1(1)-1）
第三十七条　全学実施責任者は、情報の取扱いに関する規定として、以下を例とする手順を整備すること。
一　情報のライフサイクル全般にわたり必要な手順（教育研究事務の遂行以外の目的で情報を利用等しないよう努めること等）
二　情報の入手・作成時の手順
三　情報の利用・保存時の手順
四　情報の提供・公表時の手順
五　情報の運搬・送信時の手順
六　情報の消去時の手順
七　情報のバックアップ時の手順

解説：「手順を整備」について
第１号～第７号は、第四十条～第五十三条における教職員等を名宛人とした対策事項とそれぞれ対応している。本事項では、これらの内容を包含する形で手順を定めることを求めている。

C2101-38　（格付と取扱制限の明示に係る規定の整備）（政府機関統一基準の対応項番 3.1.1(1)-2,3）
第三十八条　全学実施責任者は、情報の格付及び取扱制限の明示の方法について、以下を例に、規定を整備すること。
一　電磁的記録として取り扱われる情報に明示する場合
・電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載
・電磁的ファイル等の取扱単位ごとにファイル名自体へ記載
・フォルダ単位等で取り扱う情報は、フォルダ名に記載
・電子メールで取り扱う情報は、メール本文又はメール件名に記載
二　外部電磁的記録媒体に保存して取り扱う情報に明示する場合
・保存する電磁的ファイル又は文書等の単位ごとに記載
・外部電磁的記録媒体本体に記載
三　書面に印刷されることが想定される場合
・書面のヘッダ部分等に記載
・冊子等の単位で取り扱う場合は、冊子の表紙、裏表紙等に記載
四　既に書面として存在している情報に対して格付や取扱制限を明示する場合
・手書きによる記入
・スタンプ等による押印

解説：第１項「明示の方法」について
当該情報を参照する者が、情報の格付及び取扱制限を確実に視認することがで

きるよう、当該情報に記載することによる明示を原則とする。また、情報の格付及び取扱制限の明示については、以下の事項についても留意すること。
・本文において格付を明示することに加え、ファイル名の先頭に格付を付す。（例：「【機２】○○整備計画」）
・格付及び取扱制限の明示と併せて、情報の作成者又は入手者の氏名、所属、連絡先等も記載する。
・文書の一部の情報に取扱制限を追加するときは、追加する取扱制限を当該情報に近接した場所に明記する。
・電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記する。
・文書の作成者名、組織名その他の記録に使用できる「プロパティ」に格付の区分を記載することは明示に当たらない。

２　全学実施責任者は、情報の格付及び取扱制限の明示を省略する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、規定を整備すること。

解説：第２項「明示を省略」について

情報の格付及び取扱制限を確実に視認することができるよう、当該情報に明示しておくことが原則ではあるが、必要な場合には、以下を例に明示が省略可能な条件について定めておくとよい。
・情報システムに記録される情報の格付及び取扱制限を当該情報システムの手順書等により明記し、当該情報システムの利用者にあらかじめ周知している場合。
・情報の格付及び取扱制限の省略時における当該情報の格付及び取扱制限の取扱について、取扱手順に規定し、教職員等にあらかじめ周知している場合。ただし、格付及び取扱制限の明示を省略した場合には、以下の事項に注意する必要がある。

－格付及び取扱制限の省略を認識できない者への情報の提供

格付の区分及び取扱制限が明示されていない要保護情報を、格付及び取扱制限の決定内容を認識できない教職員等に提供する必要が生じた場合（例えば、他大学に情報を提供等する場合）は、当該情報に格付の区分及び取扱制限を明示した上で提供するなどしなければならない。

－取扱制限の明示を省略した場合における取扱制限の追加・変更

例えば、ある文書の取扱制限の明示を省略している場合であって、当該文書の一部に取扱制限を追加するときは、追加する取扱制限を明示すること。

C2101-39　（格付と取扱制限の継承、見直しに係る規定の整備）（政府機関統一基準の対応項番3.1.1(1)-4）

第三十九条　全学実施責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例に、規定を整備すること。

一　情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付及び取扱制限を継承する。

二　既存の情報に、より機密性の高い情報を追加するときは、格付及び取扱制限を見直す。

三　機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直す。
四　情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。
五　完全性及び可用性については、作成時又は複製時に適切な格付を決定する。
六　他者が決定した情報の格付及び取扱制限を見直す必要がある場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下この条において「決定者等」という。）に確認を求める。

解説：第５号「複製時に適切な格付を決定」について

複製された情報は、一般的には完全性１情報及び可用性１情報と考えられるが、原本を複製し、それをバックアップファイルとして保存する場合も考えられるため、完全性及び可用性については、適宜、複製の目的に応じて格付を決定する必要がある。

第６号「見直す必要がある場合」について

利用する元の情報への修正、追加又は削除のいずれでもないが、元の格付又は取扱制限そのものがその時点で不適当と考える場合には、格付又は取扱制限の見直しについてその決定者に確認を求める必要がある。また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は当該決定者の上司に相談し、その是非を検討することになる。決定者等による見直しが無い限り、当該情報の利用者がこれらの者に無断で、格付又は取扱制限を変更することは許されない。

なお、見直しを行わなければならない場合については、以下を参考に規定すること。

・作成時には要機密情報だった情報の機密性が失われた場合（時間の経過により変化した場合）
・機密性３情報として格付けされている資料等から機密性３情報に係る部分を全て削除した場合
・取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合
・取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合
・格付及び取扱制限を決定した時の判断が不適切であったと考えられる場合
・文書管理規則等が、情報の作成又は入手時以降に改定されており、当該文書管理規則等における情報の取扱いに変更がある場合

解説：【参考】　取扱制限の例

取扱制限は、情報の機密性、完全性、可用性等の内容に応じた情報の取扱い方を具体的に指定するものであるから、「情報の作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させる」という目的を果たすために適切に明示等する必要がある。以下の例のように、代表的な取扱制限を指定してもよい。例えば「複製禁止」の代わりに「複写禁止」や「複

製厳禁」、「複製を禁ず」等と記載しても目的を果たせると考えられる。

○ 機密性についての取扱制限の定義の例

表　機密性についての取扱制限の定義の例

取扱制限の種類	指定方法
複製について	複製禁止、複製要許可
配布について	配布禁止、配布要許可
暗号化について	暗号化必須、保存時暗号化必須、通信時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り
期限について	○月○日まで○○禁止

上記の指定方法の意味は以下のとおり。

・「○○禁止」
　当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。
・「○○要許可」
　当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。
・「暗号化必須」
　当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」等、情報を取り扱う者が分かるように指定する。
・「○○限り」
　当該情報について、参照先を○○に記載した者のみに制限する必要がある場合に指定する。例えば、「セキュリティセンター限り」「○○委員会出席者限り」等、参照を許可する者が分かるように指定する。
・「○月○日まで○○禁止」
　例えば、○月○日まで複製を禁止したい場合、「○月○日まで複製禁止」として期限を指定することで、その日に取扱制限を変更しないような指定でも構わない。

例えば、上記の「○○要許可」は、「○○する行為を禁止するが、許可を得ることにより○○することができる」という意味を持たせている。取扱制限は、このように、教職員等にとって簡便かつ分かりやすい表現を採用することが望ましい。

○ 完全性についての取扱制限の定義の例

表　完全性についての取扱制限の定義の例

取扱制限の種類	指定方法
保存期間について	○○まで保存
保存場所について	○○において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

情報の保存期間の指定の方法は、以下のとおり。

・保存の期日である「年月日」又は期日に「まで保存」を付して指定する。
　例）平成○○年 7 月 31 日まで保存
　例）平成○○年度末まで保存
・完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。
　例）年度内保存文書用共有ファイルサーバに保存
　例）3 カ年保存文書用共有ファイルサーバに保存

○ 可用性についての取扱制限の定義の例

表　可用性についての取扱制限の定義の例

取扱制限の種類	指定方法
復旧までに許容できる時間について	○○以内復旧
保存場所について	○○において保存

復旧許容時間の指定の方法は以下のとおり。

・復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。
　例）1 時間以内復旧
　例）3 日以内復旧
・可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用においては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、端末のファイルについては定期的にバックアップが実施されておらず、研究室共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。
　例）研究室共有ファイルサーバ保存必須
　例）各自 PC 保存可

C2101-40　（情報の目的外での利用等の制限）（政府機関統一基準の対応項番 3.1.1(2)）

第四十条　教職員等は、自らが担当している教育研究事務の遂行以外の目的で、情報を利用等しないよう努めること。

解説：「情報を利用等」について

教育研究事務の遂行以外の目的で、情報を利用しないよう努めることを求める事項である。

政府機関統一基準においては、行政事務の遂行以外の目的での情報の利用を一切禁止しているが、大学の特性又は実情を鑑みるに、実効的な運用を図るためには、教育研究事務の遂行の目的以外の情報の利用を一切禁止することは困難と思われる。もちろん、本サンプル規程集を利用する大学においては、本条以上の情報セキュリティの確保を目的として、政府機関統一基準同様の規定とすることは構わない。

情報の目的外利用に当たる場合としては、例えば、業務上知り得た情報をソーシャルメディアサービスの個人アカウントの掲示板等に掲示するなどの行為が考えられる。その他にも、情報の利用形態は様々であり、注意が必要である。なお、本規定で対象としている情報は、教職員等が従事する業務において利用する本学の情報システムから入手可能な業務に係る情報（業務上知り得る情報）や、情報システムにおいて利用される主体認証情報であり、情報システムの仕様やデータ設定等に係る情報も含んでいる。一方、業務時間外に自宅等の私物端末から本学のウェブサイトにアクセスして、公表されている情報を入手するなどの行為については、本規定の対象とはしていない。

C2101-41　（情報の格付及び取扱制限の決定・明示等）（政府機関統一基準の対応項番 3.1.1(3)）

第四十一条　教職員等は、情報の作成時及び学外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。

２　教職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

３　教職員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下この条において決定者等という。）に確認し、その結果に基づき見直すこと。

解説：第１項「格付及び取扱制限を決定」について

格付及び取扱制限が不十分な場合、情報漏えい等のリスクが高まるが、一方で、情報の利用を円滑に行うためには、格付及び取扱制限を必要以上に高くしないことが必要である。そのため、格付及び取扱制限を決定する際には、本学の基準に照らして、要件に過不足が生じないようにすること。例えば、機密性１情報に相当する公開しても差し支えない情報をむやみに要保護情報に決定すると、過度な保護対策を求めることになり、教育研究事務の効率的な運営に支障をき

たすおそれがある。
また、他大学との情報の受け渡しを行う際には、本学のポリシー及びそれに基づく規程等との格付定義の差分に関する情報を当該大学から得るなどして、本学の基準との差分について考慮の上、格付及び取扱制限を決定する必要がある。

第２項「継承」について
業務資料等を参考に新たに別の資料を作成する場合等において、元となった資料等に記載されていた情報の機密性に関する格付及び取扱制限について、新たに作成した資料等に適切に引き継ぐことを求めている。例えば機密性３情報を他の資料等に転用する場合においては、当該資料に記載されている転用部分については機密性３情報として取り扱われるべきである。また、要保全情報又は要安定情報を複製する場合については、複製された情報に対して過度な保護対策を求めないように、完全性１情報又は可用性１情報として格付を見直し再決定することが望ましい。ただし、バックアップを原本として情報を保管する目的で複写する場合は、要保全情報とすべきであるなど、状況に応じた適切な判断が求められる。

第３項「決定者等に確認し、その結果に基づき見直す」について
第三十九条「(解説) 第６号「見直す必要がある場合」について」を参照のこと。

C2101-42　（情報の利用・保存）（政府機関統一基準の対応項番 3.1.1(4)）

第四十二条　教職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

２　教職員等は、機密性３情報について要管理対策区域外で情報処理を行う場合は、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。

３　教職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。

４　教職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。

５　教職員等は、USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。

解説：第３項「要管理対策区域外で情報処理」について
学外で開催される会議への出席時等に要保護情報を用いて情報処理を行う際には、のぞき見の防止や不要となった情報の削除等の安全管理措置を講ずる必要がある。

第４項「保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること」について
情報システムに、ファイルに対する書込権限者の制限や、ファイルのセキュリティ設定でパスワード設定等のアクセス制御機能が装備されている場合、当該情報の格付及び取扱制限に従って、必要なアクセス制御の設定を行うことが求

められる。例えば、取扱制限として閲覧範囲の制限が指定されている場合は、第三者等から参照されないよう、読取制限の属性を付与することや、要保全情報であれば、第三者等から変更されないよう、上書き禁止の属性を付与することがこれに当たる。
アクセス制御は、サーバ装置、端末、OS、アプリケーション、ファイル等を単位に行うことができるため、これらを選択し組み合わせて、適切なアクセス制御を実現するとよい。
なお、文書管理ガイドラインの秘密文書の管理に関するモデル要領において、「秘密文書については、インターネットに接続していない電子計算機又は媒体等に保存し、暗号化等による保護を行うとともに、当該秘密文書を記録する電子計算機、媒体等について、保存を金庫等で行うなどにより物理的な盗難防止措置を施すこと。秘文書については、インターネットからの侵入に対する多重防御による情報セキュリティ対策が施された電子計算機でも保存することができる。」とされている。

第５項「外部電磁的記録媒体」について
外部電磁的記録媒体には、USB メモリ等の、繰返し情報を書き換えできる媒体と、CD-R 等の書き換えできない媒体が存在する。特に前者の媒体を利用する場合は、不正プログラムに感染するおそれが大きいため、その取扱いには細心の注意を払う必要がある。(具体的な対策等については、第二百十三条解説の【参考】を参照のこと。)

第５項「定められた利用手順」について
第二百十三条第３項において定められた利用手順を指す。

C2101-43　(格付と取扱制限に応じた情報の取り扱い)(政府機関統一基準の対応項番 3.1.1(4)-1)
第四十三条　教職員等は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱うこと。
一　要保護情報を放置しないこと。
二　要機密情報を必要以上に複製しないこと。
三　電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。
四　電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。
五　情報の保存方法を変更する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずる。
２　教職員等は、入手した情報の格付及び取扱制限が不明な場合には、情報の作成元又は入手元への確認を行う。

解説：第１号「放置しない」について
悪意ある第三者等による不正な操作や盗み見等を防止することを求める事項である。例えば、離席する際には、ロック付きスクリーンセーバを起動する又は

ログアウトして画面に情報を表示しない、机の上に書類を放置して長時間離席しない、印刷した書面を速やかに回収し出力トレイに放置しないこと等を徹底する必要がある。

第２号「必要以上に複製しない」について
電磁的記録は比較的容易に複製することができるという特性があり、可用性の観点から複製された情報が多数の端末に散在する傾向になることが想定されるため、機密性３情報に該当しない情報であっても、複製は必要最小限にとどめるよう留意する必要がある。
なお、秘密文書に関しては、文書管理ガイドラインにおいて、「秘密文書の複製等は必要最小限にとどめること。」と定められていることに留意すること。

第５号「保存方法を変更」について
当該情報が記載されている文書が歴史公文書等に該当する場合は、情報の取扱制限を解除するか、利用の制限についての意見を付すなどして移管する必要がある。その際、パスワードを設定していた場合は解除するなどして、移管先がその内容を参照できるように配慮する必要がある。

C2101-44　（情報の提供・公表）（政府機関統一基準の対応項番 3.1.1(5)）

第四十四条　教職員等は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。

２　教職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。

３　教職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずること。

解説：第１項「機密性１情報に格付されるもの」について
保有する情報をウェブサイト等により広く一般に提供する場合、公表しようとする情報の格付の適正さを再度検討し、格付及び取扱制限の明示を削除するなどを考慮する必要がある。
なお、情報の公表ではないものの、電子調達システム等において調達情報を委託先候補事業者に閲覧を許可する場合が考えられる。情報システムの構成図等サイバー攻撃を企図する者が有利になるような情報については、開示対象者と機密保持契約を締結するなどして厳重な管理のもと閲覧を許可するなどして、細心の注意を払う必要がある。

第２項「決定者等に相談」について
第三十九条「（解説）第６号「見直す必要がある場合」について」を参照のこと。

第２項「提供先において」・「適切に取り扱われるよう」について

要保護情報を学外の者に提供する場合には、提供先において当該情報が適切に取り扱われるように、情報の取扱い上の留意事項を提供先へ確実に伝達する必要がある。
伝達方法としては、他大学や委託先等の情報の提供先に、ポリシー及びそれに基づく規程等や情報の取扱いに関する手順書、本学における格付定義に関する説明等を提示し、格付や取扱制限に応じた取扱方法を示す方法が考えられる。
この場合、格付の区分だけを示しても、提供先においては当該格付区分がどのように取り扱われるべきものであるか認識できない可能性があるため、当該格付の区分の定義について提供先にあらかじめ周知しておく必要がある。また、提供する情報を適切に管理するために必要な措置が具体的に分かるようにする（例えば、「委員以外への再配布を禁止する」と明示する。）など、格付以外の方法で取扱方法を示すことも考慮する必要がある。

第４項「不用意な情報漏えい」について
情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDF ファイルの「しおり」等に残留した不要な情報を除去する必要がある。
また、ソフトウェアを用いて文書の特定の部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

C2101-45　（電磁的記録媒体の第三者提供）（政府機関統一基準の対応項番 3.1.1(5)-1）
第四十五条　教職員等は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

C2101-46　（情報の運搬・送信）（政府機関統一基準の対応項番 3.1.1(6)）
第四十六条　教職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保のための適切な措置を講ずること。
２　教職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

C2101-47　（情報の運搬を第三者に依頼する場合の対策）（政府機関統一基準の対応項番 3.1.1(6)-1）
第四十七条　教職員等は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬すること。

解説：「セキュアな運送サービス」について
セキュアな運送サービスとしては、受領印が必要となる書留郵便や、専用車両

による配達サービス、配達状況の追跡が可能なサービス等が存在する。

C2101-48 （情報漏えいの防止､情報の改ざんの防止）（政府機関統一基準の対応項番 3.1.1(6)-1,2）

第四十八条　教職員等は、要機密情報である電磁的記録を要管理対策区域外に運搬又は学外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。

一　運搬又は送信する情報を暗号化する。

二　運搬又は送信を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬または送信する。

三　主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。

解説：第１号「運搬又は送信する情報を暗号化する」について

暗号化された情報の復号に用いる鍵は、十分な長さと複雑さを有することが求められる。また、暗号化された情報の復号に用いる鍵を、暗号化された情報と同じ経路で送信等したり、第三者が容易に知り得る方法で送信等したりしてしまうと、第三者によって情報が復号されるおそれが高くなると考えられることから、暗号化された情報の復号に用いる鍵は、暗号化された情報とは別の方法で送信するなどして秘匿性を確保することが考えられる。

第２号「複数の情報に分割し」について

この考え方は、秘密分散技術といわれ、例えば、１個の電子情報について、分割された一方のデータからは情報が復元できない方法でファイルを２個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方を DVD、USB メモリ等の外部電磁的記録媒体で郵送する方法が考えられる。

第１項第３号「セキュアな外部電磁的記録媒体」について

セキュアな外部電磁的記録媒体が備える機能としては、主体認証機能、暗号化機能の他、不正プログラムの検閲・駆除機能、遠隔データ消去機能及び接続管理機能等がある。USB メモリ等の外部電磁的記録媒体の運搬に当たっては、必要最小限の情報のみを保存するよう留意するとともに、盗難・紛失等による情報漏えいに備え、当該機能を適切に利用することが必要である。

C2101-49 （情報の送信に係る対策）（政府機関統一基準の対応項番 3.1.1(6)-4）

第四十九条　教職員等は､要保護情報である電磁的記録を送信する場合は､安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。

一　本学管理の通信回線を用いて送信する。

二　信頼できる通信回線を使用して送信する。

三　VPN を用いて送信する。

四　S/MIME 等の暗号化された電子メールを使用して送信する。

五　本学独自で運用するなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。

解説：第２号「信頼できる通信回線」について

空港や商業施設等が提供する無線 LAN 等の通信回線は、十分なセキュリティ対策が採られていない場合もあるため、要保護情報を送信する場合にこれを用いるべきではない。

C2101-50　（情報の消去）（政府機関統一基準の対応項番 3.1.1(7)）

第五十条　教職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。

２　教職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。

３　教職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

解説：第１項「速やかに情報を消去」について

情報セキュリティの観点からは、不正プログラム感染による情報窃取や操作ミスによる情報漏えい等を防ぐ観点から、職務上不要となった情報を速やかに消去する必要がある。

第２項「抹消する」について

「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。電磁的記録媒体に記録されている情報を抹消するための方法としては、例えば、次の方法が挙げられる。

・データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法

・ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法

・媒体を物理的に破壊する方法

また、媒体を物理的に破壊する方法としては、例えば、次の方法が挙げられる。

・（フロッピーディスク等の磁気媒体の場合）当該媒体を切断するなどして情報を記録している内部の円盤を破壊する方法

・（CD-R/RW、DVD-R/RW 等の光学媒体の場合）カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法

・（媒体全般）メディアシュレッダーやメディアクラッシャー等の専用の機器を用いて破壊する方法

また、ファイルの情報に別の情報を上書きした場合であっても、特殊な手段を用いることにより残留磁気から当該情報を復元される可能性があるため、特に機密性の高い情報の抹消に当たっては、留意する必要がある。

なお、教職員等自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と抹消の措置を行う者を情報システム又は課室等の組織の単位で定めて実施してもよい。

第３項「復元が困難な状態にする」について
電磁的記録の抹消と同様に、書面が不要となった場合には、シュレッダーによる細断処理、焼却、溶解等により、復元が困難な状態にする必要がある。
なお、廃棄すべき書類が大量にあるなどの理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃棄処理証明書の取得等により、書面が確実に廃棄されていることを確認するとよい。また、無人の教室、研究室、事務室に設置されている又は設置場所及び利用場所が確定していないなどの環境で利用される情報システム、外部電磁的記録媒体等については、不要な情報を可能な限り抹消しておくことが望ましい。

C2101-51　（情報のバックアップ）（政府機関統一基準の対応項番 3.1.1(8)）
第五十一条　教職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。
２　教職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。
３　教職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。

解説：第１項「適切な方法で情報のバックアップを実施する」について
災害や情報セキュリティインシデントが発生し、サーバ装置等の電磁的記録が使用不可能になった際の復旧に備えて、要保全情報や要安定情報に格付される情報等の重要な情報を外部の記録媒体へバックアップすることを求めている。
以下の例を参考に、情報のバックアップ方法について考慮するとよい。
・バックアップの対象（対象とするシステム、データ、ソフトウェアその他）
・バックアップの範囲（フルバックアップ、差分バックアップ等）
・バックアップを保存する電磁的記録媒体等の種類
・バックアップの周期、世代管理の方法
・使用するバックアップツール
・バックアップデータの秘匿性確保、改ざん防止の方法

第２項「格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め」について
バックアップデータに要機密情報が含まれる場合は、バックアップデータの盗難・紛失による情報漏えい等を回避するために、バックアップデータを要管理対策区域に保管することが望ましい。また、バックアップデータを保存する媒体の耐久性にも留意し、定期的に媒体を新しいものに入れ替えるなども考慮するとよい。

C2101-52　（要保全情報又は要安定情報のバックアップ）（政府機関統一基準の対応項番 3.1.1(8)-1）
第五十二条　教職員等は、要保全情報又は要安定情報である電磁的記録又は重要な設計書につい

て、バックアップを取得すること。

C2101-53　（要保全情報又は要安定情報のバックアップ）（政府機関統一基準の対応項番 3.1.1(8)-2）

第五十三条　教職員等は、要保全情報、要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップの保管について、災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定すること。

解説：「重要な設計書」について

情報システムの委託先から書面のみで提示された設計書類等、情報システムに記録されていない書面のみの情報であって、紛失、改ざん等により情報システムの運用に支障を及ぼす可能性のあるものを指している。バックアップが外部に流出することにより、攻撃者に有利になるものについては、保管の際に機密性を確保することにも留意する必要がある。

「災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定する」について

災害等を想定してバックアップを取得する場合は、バックアップを耐火性のある保管庫や耐震性の高い施設、同時被災しない遠隔地に保管すること等も考えられる。また、遠隔地に保管するに当たっては、実際にバックアップを用いた復旧に要する時間が、情報システム運用継続計画における復旧目標時間内に納まるよう、緊急時のバックアップデータの配送手段、配送時間等を考慮し、保管場所を決定する必要がある。

第二節　情報を取り扱う区域の管理

解説：サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

したがって、教室、研究室、事務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

C2101-54　（要管理対策区域における対策の基準の決定）（政府機関統一基準の対応項番 3.2.1(1)）

第五十四条　全学実施責任者は、要管理対策区域の範囲を定めること。

２　全学実施責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。

一　許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。

二　許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の

不正な行為を防止するための入退管理対策。

解説：第１項「要管理対策区域の範囲を定める」について

教室、研究室、事務室やサーバ室のほか、学外の組織と共用する施設や、教職員等が書面やモバイル端末等を運搬するときの安全性を高めるために、教室、研究室、事務室間に接続されている廊下等も要管理対策区域に含めることを考慮してもよい。

なお、要管理対策区域外で教育研究事務を行う必要がある場合には、施設及び環境に係る対策が講じられないことから情報の漏えい等の可能性が高くなる。情報の漏えい等の可能性を低減するためには、要管理対策区域外でのモバイル端末の利用に関する遵守事項（「端末」の遵守事項に係る第百四十六条第１項・第２項、「情報システムの利用」の遵守事項に係る第二百十三条第２項等）を参照し、適切な対策を行うことが必要である。

第２項第２号「入退管理対策」について

次条第２項～第４項に示した対策の基準のほか、以下を対策の基準に含めてもよい。

・共連れ（立入りを許可された者が立ち入る際に、立入りを許可されていない者を同時に立ち入らせるような行為）を防止する措置を講ずること。具体的な対策として、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。

・立入りを許可されていない者の侵入等、区域の安全性が侵害された場合に追跡することができるように、立入り及び当該区域からの退出を記録及び監視する措置を講ずること。「記録及び監視する」具体的な対策として、警備員、監視カメラ等による記録及び監視のほか、要管理対策区域への立入り及び当該区域からの退出を管理する装置における立入り及び退出の記録を取得し、当該立入り及び退出の記録を定期的に確認することが挙げられる。継続的に立入りが許可されている者以外の者の立入りがあった場合には、立入りの記録として立ち入った者の氏名及び所属、訪問目的、訪問相手の氏名及び所属、訪問日、立入り及び退出の時刻を記録することが挙げられる。

・受渡業者と物品の受渡しを行う場所を制限すること。

なお、「受渡業者」とは、教職員等との物品の受渡しを行う者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

C2101-55　（要管理対策区域における対策）（政府機関統一基準の対応項番 3.2.1(1)-1,2,3,4,5）

第五十五条　全学実施責任者は、以下を例とする、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を定めること。

一　下表のとおり、３段階のクラスを定める。

クラス	説明
クラス３	一部の限られた者以外の者の立入りを制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域

クラス２	教職員等以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対策区域

※便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。

２　全学実施責任者は、クラス１の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

一　不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。

二　不特定の者が容易に立ち入らないように、立ち入る者の身元、訪問目的等の確認を行うための措置を講ずること。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。

三　クラス２以上の区域に不正に立ち入った者を容易に判別することができるように、以下を含む措置を講ずること。

・教職員等は、身分証明書等を着用、明示する。クラス２及びクラス３の区域においても同様とする。

・一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス２及びクラス３の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。

３　全学実施責任者は、クラス２の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

一　クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。ただし、窓口のある教室、研究室、事務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は教職員等が窓口を常に目視できるような措置を講ずること。

二　クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠すること。

三　クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。

４　全学実施責任者は、クラス３の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

一　クラス３の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分すること。

二　クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。

三　クラス３の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにすること。

四　一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずること。業者が作業を行う場合は立会いや監視カメラ等により監視するための措置を講ずること。

５　全学実施責任者は、以下を例とする、区域へのクラスの割当ての基準を定めること。

一　クラスの割当ての基準を以下のように定める。

・サーバ室や日常的に機密性が高い情報を取り扱う研究室、事務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス３を割り当てる。

・一般的な研究室、事務室や会議室には、教職員等及び関係の学生等以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス２を割り当てる。

解説：第２項第２号「立ち入る者の身元、訪問目的等の確認を行うための措置」について

クラス１の区域に「立ち入る者」について、継続的に立入りを許可された者のほか、一時的に立ち入る者（訪問者）がある。継続的に立入りを許可された者として、教職員等及び学生等並びに一定期間立入りを認められ、認められたことを示す許可証（入館カード等）が貸与されている業者等を想定している。また、一時的に立ち入る者として、不定期に訪れる来客や受渡業者等を想定している。

「身元、訪問目的等の確認を行うための措置」の具体的な対策として、以下が挙げられる。

・セキュリティゲートの設置、警備員や受付係等の配置をして立ち入る者に身分証明書等の提示を求める。

・一時的に立ち入る者の氏名及び所属、訪問目的等を記録する。

第３項第３号「クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置」について

具体的な対策として、以下が挙げられる。

・継続的に立入りが許可されている者に IC カードを貸与して IC カードによる主体認証を行う。

なお、IC カード等による主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずることが望ましい。

・継続的に立入りが許可されている者以外の者が立ち入る場合は、立入りを許可する者が自ら区域の境界まで迎えに行く。

・立入りを監視する警備員、受付係等を配置している場合は、許可する者が警備員等にあらかじめ一時的に立ち入る者の氏名及び所属、訪問目的、訪問相手の氏名及び所属、訪問日時等を伝えておき、一時的に立ち入る者が来訪した際に警備員、受付係等が照合する。

クラス２の区域への立入り時の「許可された者であることの確認」について、

クラス１の区域への立入り時に「身元、訪問目的等の確認」ではなく「許可された者であることの確認」を行っている場合においては、それをもって代替してもよい。

第４項第３号「クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置」について
具体的な対策として、以下が挙げられる。
・継続的に立入りが許可されている者に IC カードを貸与して IC カードによる主体認証を行う。
・継続的に立入りが許可されている者以外の者が立ち入る場合は、立入りを許可する者が自ら区域の境界まで迎えに行く。
・継続的に立入りが許可されている者のみに、常時施錠される扉の鍵を貸与したり、解錠するための暗証番号を通知したりしておき、鍵の所持や入力した暗証番号の一致により、確認する。

第５項「クラスの割当ての基準」について
本規程においては、例としてサーバ室や日常的に機密性が高い情報を取り扱う研究室、事務室にはクラス３、一般の研究室、事務室や会議室にはクラス２を割り当てるという基準を示している。
全学実施責任者は、区域情報セキュリティ責任者に、管理する区域で取り扱う情報、設置される情報システムの特性から、外部からの侵入があった場合の被害の大きさを考慮してクラスを決定させる必要があることを踏まえ、本規程で示す基準を参考とし、クラスの割当ての基準を定める必要がある。
また、教育研究事務の単位でクラスの割当ての基準（例：〇〇、××に関係する教育研究事務を行う研究室、事務室はクラス３、これら以外の教育研究事務を行う研究室、事務室はクラス２）を定めておくことも考えられる。

なお、区域へのクラスの割当ての基準は、大学の特性や実情に合わせて、現実に運用が可能かどうかを考える必要がある。

【参考】要管理対策区域へのクラスの割当ての例
要管理対策区域へのクラスの割当ての例を図 4～6 に示す。

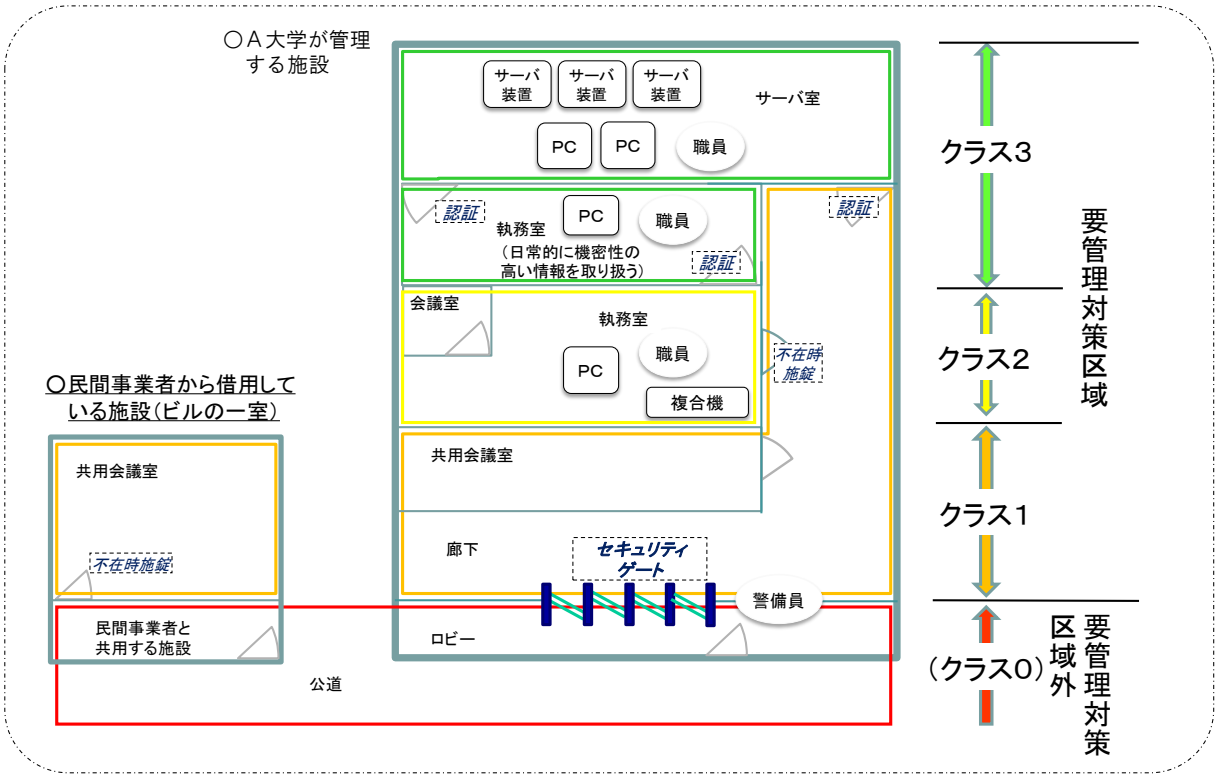


図４　要管理対策区域へのクラスの割当ての例１
（建物及び民間事業者から借用する施設の例）

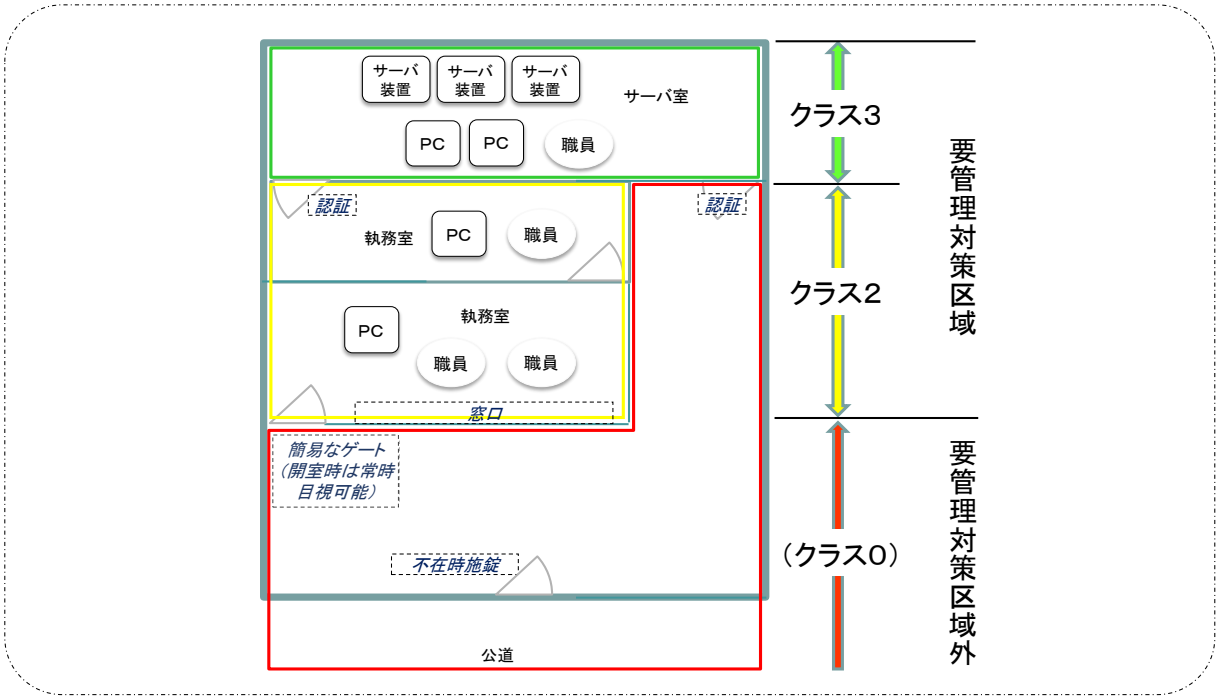


図５　要管理対策区域へのクラスの割当ての例２
（窓口のある教室、研究室、事務室等の例）

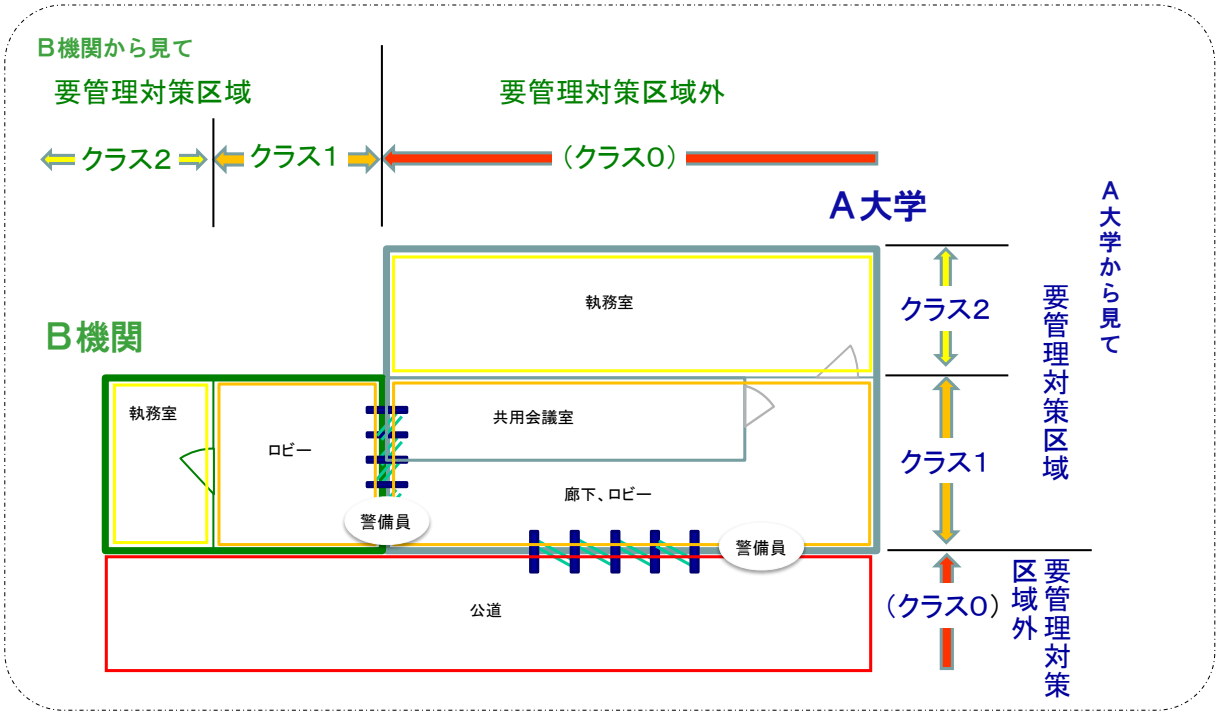


図 6　要管理対策区域へのクラスの割当ての例３（複数の組織で共用する施設の例）

C2101-56　（区域ごとの対策の決定）（政府機関統一基準の対応項番 3.2.1(2)）

第五十六条　部局総括責任者は、全学実施責任者が定めた対策の基準を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定めること。

２　区域情報セキュリティ責任者は、管理する区域について、全学実施責任者が定めた対策の基準と、周辺環境や当該区域で行う教育研究事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。

解説：第１項「施設及び環境に係る対策を行う単位ごとの区域を定める」について

複数の部局で共用する廊下等の施設については、施設管理の観点での各部門の管理範囲を確認した上で「施設及び環境に係る対策を行う単位ごとの区域」を定めるとよい。共用する施設の区域情報セキュリティ責任者の定め方については、「C1001 情報システム運用基本規程」第十八条の解説を参照のこと。

C2101-57　（区域ごとの対策）（政府機関統一基準の対応項番 3.2.1(2)-1）

第五十七条　区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う教育研究事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定すること。

解説：「割り当てるクラスを決定する」について

クラス３、クラス２以外の要管理対策区域はクラス１となることにも留意して決定する必要がある。クラス１の区域は、不特定の者が容易に立ち入れない程度の安全性が確保された区域である。したがって、原則として、盗難や盗み見

等への対策が講じられていない端末や書面が置かれる区域にクラス１を割り当ててはならない。クラス１の区域に端末を置く必要がある（例：来訪者受付に来訪者の個人情報が保存されている端末を置く）場合には、セキュリティワイヤ等で固定することや、常時目視により監視するなどの措置を講ずる必要がある。

「当該区域において実施する対策を決定する」について
周辺の区域のクラスや管理状況も確認して具体的な対策を決定するとよい。例えば、クラス３の区域がクラス０の区域と接続している場合は、クラス３の区域の扉の施錠管理をより厳重にすることが考えられる。
なお、必要な対策が庁舎管理等の別の仕組みにより実施されている場合については、その対策をもって代替しても構わない。

「個別の対策」について
個別の対策については、第五十四条「(解説）第２項第２号「入退管理対策」について」に示した例（対策の基準となっていない場合）のほか、以下に示す例を参考に決定するとよい。
・施設内の案内板等において、サーバ室等の所在の表示を禁止する。
・外部から室内が見えるような場所にある会議室において、要機密情報の取扱い時はブラインドを閉じる。
・外部の者が周辺の会議室等へ出入りする時間帯には、教室、研究室、事務室の扉を施錠する又は開放しない。
・低階層の窓際等における無線 LAN の傍受対策を行う。
・ワイヤレスマイクの電波が室外にも到達するような会議室において、要機密情報の取扱い時はワイヤレスマイクの使用を禁止する。
・ディスプレイケーブル等から生ずる電磁波から情報が漏えいするおそれがある場合には電磁波軽減フィルタを取り付ける。
・飲食物をこぼした際に情報システムの運用上の障害が発生するような場所での飲食を禁止する。
・情報システムに関係する機器の不正な持ち出しが行われていないかを確認するために定期的又は不定期に施設からの退出時に持ち物検査を行う。
・クラス３の区域の中でもより厳重な管理が必要な区域において、機器の持込み、利用、持ち出しについて制限を設ける。
・会議室において、重要な情報を取り扱う会議が開催される時間帯には機器の持込み、利用について制限を設ける。
機器の持込み、利用、持ち出しの制限について詳細を以下に示す。
・「機器の持込み」とは、利用者等が、教室、研究室、事務室に教育研究事務に関係しない機器を持ち込むことや情報システムが設置される区域に当該情報システムに関係しない機器を持ち込むことを指す。「機器」には、モバイル端末、デジタルカメラ等の撮影機器、IC レコーダー等の録音機器、USB メモリ等の外部電磁的記録媒体等が含まれる。また、私物のスマートフォン等の本学支給

以外の機器も含まれる。以下に示すように、利用のみを禁止する対策もあるが、例えば、持ち込まれたスマートフォンが不正プログラムに感染していて、持ち込んだ者の意図に反して撮影や録音をされるという脅威も存在するため、持ち込ませないという対策も考えられる。

・「機器の利用」とは、利用者等が、持ち込んだ機器を利用することを指す。「利用」には、モバイル端末の起動や、デジタルカメラ等による撮影、IC レコーダー等による録音等が含まれる。管理する区域で取り扱う情報の機密性の高さに応じて、利用の制限を設けるか決めるとよい。スマートフォン等の通常電源をオンにしている機器であれば、立ち入る際に電源をオフにさせるという対策も有効である。

・「機器の持ち出し」とは、情報システムが設置される区域から当該情報システムに関係する者が、当該情報システムに関係するサーバ装置、端末、外部電磁的記録媒体等を持ち出すことを指す。情報セキュリティインシデント発生時に追跡等できるように、機器の持ち出し時には、持ち出しの記録を取ることが考えられる。記録の内容としては、持ち出しを行う者の氏名及び所属、日時、機器名、事由等が挙げられる。

C2101-58　（要管理対策区域における対策の実施）（政府機関統一基準の対応項番 3.2.1(3)）

第五十八条　区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。利用者等が実施すべき対策については、利用者等が認識できる措置を講ずること。

２　区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずること。

３　利用者等は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、利用者等が学外の者を立ち入らせる際には、当該学外の者にも当該区域で定められた対策に従って利用させること。

解説：第１項「利用者等が認識できる措置を講ずる」について

当該区域のクラスや当該クラスにおいて利用者等が実施すべき対策を周知することが考えられる。扉の施錠や一時的に立ち入る者が許可された者であることの確認等の利用者等に実施させる事項については、利用手順を定めて周知するとよい。

なお、関係者限りで利用する区域については、関係者のみに周知することでも構わない。

第２項「物理的な対策」について

地震、火災、停電等の災害から情報システムを保護するための対策を指す。

具体的な対策として、例えば、サーバラックの利用のほか、以下の設備等の設置が挙げられる。

・ハロゲン化物消火設備
・無停電電源装置
・自家発電装置
・空調設備

・耐震又は免震設備
これらの対策については、必ずしも区域情報セキュリティ責任者単独で実施できるものではないが、例えば、情報システムに関係する対策であれば部局技術責任者、施設管理に関係する対策であれば施設管理を行う部門の関係者と調整することが求められる。
また、情報システムへの対策として、作業する者が災害によりサーバ装置等に近づくことができない場合に、作業する者の安全性を確保した上で遠隔地からサーバ装置等の電源を遮断できるようにする機能を設けておくことも考えられる。

第３項「利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する」について
利用者等は、自身が所属する大学が管理する区域を利用する場合は、当該本学が定めた対策に従って利用することが求められる。一方、他の大学が管理する区域を利用する場合には、他の大学が定めた対策に従って利用する必要がある。

C2101-59　（要管理対策区域における利用手順等の整備）（政府機関統一基準の対応項番3.2.1(3)-1）

第五十九条　区域情報セキュリティ責任者は、管理する区域について、以下を例とする利用手順等を整備し、当該区域を利用する利用者等に周知すること。

一　扉の施錠及び開閉に関する利用手順
二　一時的に立ち入る者が許可された者であることを確認するための手順
三　一時的に立ち入る者を監視するための手順

第七章　外部委託

第一節　外部委託

解説：学外の者に、情報システムの開発、アプリケーションプログラムの開発等を委託する際に、教職員等が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先においてポリシー及びそれに基づく規程等に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。
外部委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任等様々であるが、いずれの場合においても外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。
なお、クラウドサービスの利用に係る外部委託については、クラウドサービス特有のリスクがあることを理解した上で、第四節（クラウドサービスの利用）についても本条に加えて遵守する必要がある。
また、民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等、第二条第四十一号において「約款による外部サービス」として定

義するものを利用し、研究教育事務を遂行する場合も外部委託の一つの形態と考えられるが、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、その際は本項に代えて第七章第二節「約款による外部サービスの利用」を適用すること。

＜外部委託の例＞
・情報システムの開発及び構築業務
・アプリケーション・コンテンツの開発業務
・情報システムの運用業務
・業務運用支援業務（統計、集計、データ入力、媒体変換等）
・プロジェクト管理支援業務等
・調査・研究業務（調査、研究、検査等）
・情報システム、データセンター、通信回線等の賃貸借

C2101-60　（外部委託に係る規定の整備）（政府機関統一基準の対応項番 4.1.1(1)）
第六十条　全学実施責任者は、外部委託に係る以下の内容を含む規定を整備すること。
一　委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準
二　委託先の選定基準

解説：第１号「委託先によるアクセスを認める情報及び情報システムの範囲」について

委託先や第三者による許可されていない情報及び情報システムへのアクセス等が行われないように、委託先におけるそれらの取扱いに関する本学の基準を規定することを求めている。規定すべき内容としては、例えば以下の事項が考えられる。
・外部委託を許可（又は禁止）する業務又は情報システムの範囲
・外部委託を許可（又は禁止）する業務又は情報システムの具体的例示（公開ウェブサーバは外部委託可等）
・格付及び取扱制限その他取り扱う情報の特性に応じた、情報の取扱いを許可（又は禁止）する場所（機密性３情報は庁舎外での取扱いを禁止するなど）
特に、委託業務において使用される情報システムが海外のデータセンターに設置されている場合等においては、保存している情報に対して現地の法令等が適用されるため、国内であれば不適切と判断されるアクセスをされる可能性があることに注意が必要である。「個人情報の保護に関する法律」（平成 15 年法律第 57 号）、「行政機関の保有する個人情報の保護に関する法律」（平成 15 年法律第 58 号）及び「独立行政法人等の保有する個人情報の保護に関する法律」（平成 15 年法律第 59 号）で定義する個人情報については、国内法が適用される場所に制限する必要があると考えるため、個人情報を取り扱う委託業務においては、保存された情報等において国内法令が適用されること等を外部委託の際の判断条件としておくべきである。

第２号「委託先の選定基準」について

全学実施責任者は、委託先の選定基準の整備に当たって、当該委託先が、事業の継続性を有し存続する可能性が高く、ポリシー及びそれに基づく規程等の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。
選定基準としては、委託先がポリシー及びそれに基づく規程等の該当項目を遵守し得る者であること、ポリシー及びそれに基づく規程等と同等の情報セキュリティ管理体制を整備していること、ポリシー及びそれに基づく規程等と同等の情報セキュリティ対策の教育を委託先の事業従事者に対して実施していること等が挙げられる。
また、本学の情報セキュリティ水準を一定以上に保つために、委託先に対して要求すべき情報セキュリティ要件を学内で統一的に整備することが重要である。
委託先の選定基準策定に当たって、委託先の情報セキュリティ水準の評価方法を整備する際、例えば、ISO/IEC 27001 等の国際規格とそれに基づく認証制度の活用、情報セキュリティガバナンスの確立促進のために開発された自己評価によるツール等の応用も考えられる。その場合、委託先の情報セキュリティ水準の認証に関わる認定・認証機関について、これら機関がマネジメントシステム認証の信頼性向上を目的とした取組である「MS 認証信頼性向上イニシアティブ」に参画し、不祥事への対応や透明性確保に係る取組を実施していることを確認することも考えられる。
なお、委託先の選定基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、外部委託の実施時に反映することが必要である。

C2101-61　（外部委託に係る契約）（政府機関統一基準の対応項番 4.1.1(2)）

第六十一条　部局技術責任者又は職場情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。

一　委託先に提供する情報の委託先における目的外利用の禁止

二　委託先における情報セキュリティ対策の実施内容及び管理体制

三　委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制

四　委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

五　情報セキュリティインシデントへの対処方法

六　情報セキュリティ対策その他の契約の履行状況の確認方法

七　情報セキュリティ対策の履行が不十分な場合の対処方法

２　部局技術責任者又は職場情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。

一　情報セキュリティ監査の受入れ

二　サービスレベルの保証

３　部局技術責任者又は職場情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保される

よう、第一項及び前項の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本学に提供し、本学の承認を受けるよう、仕様内容に含めること。

解説：第１項「委託先の選定条件とし、仕様内容にも含める」について

一般競争入札の中でも総合評価落札方式で行う場合は、第１項の第１号～第７号について、評価の際に入札者に対し提出を求めるなど、選定条件を満たしているかの確認をすること。また、事前に評価を行えない最低価格落札方式等で行う場合であっても、仕様書に対する履行能力証明書等を提出させるなどにより、第１項の第１号～第７号について契約時までに提出することを確約させること。

なお、委託事業の内容によっては、一部の条件が設定不可能な場合や意味をなさない場合も考えられるため、そのような場合には、除外することもやむを得ない。

第１項第３号「意図せざる変更が加えられないための管理体制」について

情報システムの開発等の外部委託において、「意図せざる変更が加えられないための管理体制」が確保されることを求めている。

具体的に仕様書等に記載する事項としては、例えば以下が考えられる。

・情報システムの開発工程において、本学の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

・情報システムに本学の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、本学と委託先が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

第１項第４号「委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供」について

第１項第３号「意図せざる変更が加えられないための管理体制」における管理体制等を確認する際の参照情報として用いるため、提供を求める規定である。

第１項第４号「委託事業の実施場所」について

データセンター等のスペースを借用して情報システムを設置する場合等では、要安定情報を取り扱う情報システムにおいて、自然災害による影響を考慮し、データセンターの立地条件をあらかじめ考慮しておく必要がある。

また、委託業務において使用する情報システムが民間事業者等の学外のデータセンターに設置される場合においては、第六十条「（解説）第１号「委託先によるアクセスを認める情報及び情報システムの範囲」について」を参照のこと。

第１項第５号「情報セキュリティインシデントへの対処方法」について

委託先において発生した情報セキュリティインシデントによる被害を最小限に

食い止めるための対処方法（対処手順、責任分界、対処体制等）について、契約時にあらかじめ委託先と合意しておくとよい。対処方法について合意していないと、インシデントが発生しているにもかかわらず委託先と連絡がつかない、営業時間外の対応を断られるなどのトラブルになるおそれがあるため、可能な範囲で事前に合意しておくことが重要である。
対処方法には、例えば、復旧を優先する場合は委託業務を一時的に停止するための手順を規定し、業務継続を優先する場合は、委託事業を継続した上で情報セキュリティインシデントに対処する手順について、対処の主体とともに規定することが考えられる。また、情報セキュリティインシデントに係る委託先と本学間の情報エスカレーション方法やそのタイミングについて規定することも考えられる。

第１項第６号「情報セキュリティ対策その他の契約の履行状況の確認方法」について
委託先における情報セキュリティ対策の水準を維持するためには、その履行状況を委託元が継続的に確認すべきであり、また、履行が不十分である場合に速やかに適切な対処をすべきである。
情報セキュリティ対策の履行状況を確認するための方法としては、例えば、委託先における情報セキュリティ対策の実施状況について定期的に報告させることや情報セキュリティ監査等が考えられる。情報セキュリティ監査の内容には、請け負わせる業務のうち監査の対象とする範囲、実施者（本学が指定する第三者、委託先が選定する第三者、本学又は委託先において当該業務を行う部門とは独立した部門）、実施方法（情報セキュリティ監査基準の概要、実施場所等）等、当該情報セキュリティ監査を受け入れる場合の委託先の負担及び委託先候補の情報セキュリティポリシーとの整合性等を委託先候補が判断するために必要と考えられる事項を含める。
情報セキュリティ監査により履行状況を確認する場合は、第六十一条第２項第１号に示す情報セキュリティ監査の受入れを仕様書に明記するとよい。

第１項第７号「情報セキュリティ対策の履行が不十分な場合の対処方法」について
情報セキュリティ対策の履行が不十分である場合の対処方法としては、例えば、委託先と改善について協議を行い、合意した改善策を実施させること等が考えられる。また、部局技術責任者又は職場情報セキュリティ責任者自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼する必要がある。

第２項「取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること」について
要保護情報を委託先にて取り扱う場合には、必要時に情報セキュリティ対策の履行状況の報告を求めるものである。また、委託先への立入検査又は情報セキ

ュリティに関する監査を実施する場合には、監査の対象とする範囲、実施者及び実施方法等を含む委託先と合意した事項について、契約に含めるなどにより明らかとしておくことが必要である。
また、要安定情報を取り扱う場合には、サービスレベルの保証について委託先と契約を取り交わすことを検討する必要がある。サービスレベルに関しては、セキュリティ確保の観点からも、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、委託先に保証させることが重要である。

第３項「再委託先」について
「再委託先」には、再委託先の事業者が受託した事業の一部を別の事業者に委託する再々委託等、多段階の委託が行われる場合の委託先を含む。

C2101-62　（外部委託に係る対策）（政府機関統一基準の対応項番 4.1.1(2)-1,2）
第六十二条　部局技術責任者又は職場情報セキュリティ責任者は、以下の内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させること。また、変更があった場合は、速やかに再提出させること。
一　当該委託業務に携わる者の特定
二　当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容
２　部局技術責任者又は職場情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱うこと。

解説：第２項「情報の取扱手順」について
格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、委託先においてもポリシー及びそれに基づく規程等に定める内容と同等の取扱いが行われるよう、あらかじめ委託先と合意しておくことが重要である。また、委託先に提供する情報は必要最小限にとどめる必要があるが、情報システムの利用等において目的外の不必要なアクセスが行われる可能性も考慮し、委託先における情報の取扱状況を適宜把握することも重要である。
なお、委託先において、約款による外部サービス、ソーシャルメディアサービス、クラウドサービス等を用いて委託業務を遂行することが考えられる場合は、本規程第六十五条、第六十六条、第六十七条、第六十八条、第六十九条、第七十条、第七十一条の規定を委託先においても遵守させるよう仕様書等に規定し、委託先とあらかじめ合意しておくことが望ましい。

C2101-63　（外部委託における対策の実施）（政府機関統一基準の対応項番 4.1.1(3)）
第六十三条　部局技術責任者又は職場情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。
２　部局技術責任者又は職場情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を利用

者等より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく必要な措置を講じさせること。

３　部局技術責任者又は職場情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

解説：第１項「情報セキュリティ対策の履行状況を確認する」について

委託先における情報セキュリティ対策の履行状況の確認に際し、情報セキュリティ監査を利用することとした場合には、契約に基づいた監査の範囲及び実施方法に従い、本学自らが情報セキュリティ監査を行う以外に、第三者又は委託先に情報セキュリティ監査を行わせることが考えられる。

第３項「情報が確実に返却、又は抹消されたことを確認する」について

当該遵守事項を部局技術責任者又は職場情報セキュリティ責任者に求めるに当たり、委託先ともあらかじめ具体的な確認手段を定め、合意しておくことが望ましい。情報が完全に抹消されたことを確認することが困難な場合は、確認書を委託先に提出させるなどの方法も考慮する必要がある。

情報の抹消については、第五十条「(解説) 第２項「抹消する」について」及び第九十条「(解説) 第２号「情報の抹消」について」を参照し、確認手段を定めるとよい。

C2101-64　(外部委託における情報の取扱い) (政府機関統一基準の対応項番 4.1.1(4))

第六十四条　利用者等は、委託先への情報の提供等において、以下の事項を遵守すること。

一　委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。

二　提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。

三　委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに部局技術責任者又は職場情報セキュリティ責任者に報告すること。

解説：「委託先への情報の提供」について

委託契約開始から終了に至るまでに行う委託先への情報の提供に伴う要機密情報の漏えい等を防止するためには、委託業務に係る利用者等それぞれが委託先との情報の授受時に情報セキュリティを確保することが重要である。

委託先への情報の提供に関する解説については、第四十四条「(解説) 第２項「提供先において」・「適切に取り扱われるよう」について」を参照のこと。

第二節　約款による外部サービスの利用

解説：外部委託により研究教育事務を遂行する場合は、原則として第七章第一節「外部委託」にて規定する事項について、委託先と特約を締結するなどし、情報セキュリティ対策を適切に講ずる必要がある。しかしながら、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合には、民間事業者が不特定多数の利用者向けに約款に基づきインターネット上で提供する情報処理サービス等、第二条第四十一号において「約款

による外部サービス」として定義するものを利用することも考えられる。
このような「約款による外部サービス」をやむを得ず利用する場合には、種々の情報を本学からサービス提供事業者等に送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断し、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

C2101-65　（約款による外部サービスの利用に係る規定の整備）（政府機関統一基準の対応項番4.1.2(1)）

第六十五条　全学実施責任者は、以下を含む約款による外部サービスの利用に関する規定を整備すること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

一　約款による外部サービスを利用してよい業務の範囲

二　業務に利用する約款による外部サービス

三　利用手続及び運用手順

２　部局総括責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定めること。

解説：第１項「約款による外部サービス」について

「約款による外部サービス」としては、民間事業者等がインターネット上で不特定多数の利用者（主に一般消費者）に対して提供する電子メール、ファイルストレージ、グループウェア等のクラウドサービスが代表的であり、有料、無料に関わらず、画一的な約款や利用規約等への同意、簡易なアカウントの登録（登録が不要な場合もある）等により利用可能なサービスは、約款による外部サービスとなる。その他にインターネットの検索サービスや辞書サービス等も約款による外部サービスに該当する。
また、利用者等自身が個人で取得した電子メールアカウント等を業務で利用する場合についても約款による外部サービスの利用に当たる。
このようなサービスは、利用の際の情報管理について保証がないことが一般的であり、不用意な利用によって学内の情報が意図せず漏えいすることが懸念されることから、要機密情報が取り扱われないよう、適切に管理することが重要である。
その他に民間事業者が約款により提供する情報処理に関わるサービスとしては、電気通信サービスや郵便、運送サービス等があるが、これらは「約款による外部サービス」の適用範囲外である。

第１項第１号「約款による外部サービスを利用してよい業務の範囲」について
取り扱う情報の格付及び取扱制限に応じて、情報セキュリティの確保の観点から、約款による外部サービスを利用してよい業務の範囲を定めることを求めている。
約款による外部サービス利用に当たってのリスクには、以下のようなものがある。全学実施責任者は、これらのリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、許可する業務の範囲を決定する必要がある。

・サービス提供者は、保存された情報を自由に利用することが可能である。また、約款、利用規約等でその旨を条件として明示していない場合がある。加えて、サービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にある。
・情報が意に反して公開されてしまった場合や、情報が改ざんされた場合でも、サービス提供者は一切の責任を負わない。
・サービス提供者が海外のデータセンター等に情報を保存している場合は、保存している情報に対し、現地の法令等が適用され、現地政府機関等から情報にアクセスされる可能性がある。
・突然サービス停止に陥ることがある。また、その際に預けた情報の取扱いは保証されず、損害賠償も行われない場合がある。約款の条項は一般的にサービス提供者に不利益が生じないようになっており、このような利用条件に合意せざるを得ない。また、サービスの復旧についても保証されない場合が多い。
・保存された情報が誤って消去又は破壊されてしまった場合に、復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。
・約款及び利用規約の内容が、サービス提供者側の都合で利用開始後事前通知等無しで一方的に変更されることがある。
・情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。
・利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、その対応には時間を要することが多い。
なお、本項において、約款による外部サービスで要機密情報を取り扱うことを禁止しているが、例外措置としてやむを得ず要機密情報を約款による外部サービスにおいて取り扱う場合においても、上記リスクを踏まえ、適切な対策を講じた上で利用することが求められる。例えば、海外のデータセンター等に情報を保存し、現地の法令等が適用されることで情報の漏えいにつながるリスクについては、国内にサーバが設置される事業者に委託し、国内法令が適用されることを事前に確認できれば当該リスクを低減することが可能と判断できる。このように、サービス提供者のサービス提供形態により回避可能なリスクもあることから、約款、利用規約等の詳細を確認するなどして例外措置の可否を判断することが重要である。

第１項第２号「業務に利用する約款による外部サービス」について
約款による外部サービスのうち利用可能なサービスについて、以下を例にサービスを特定し、本学の基準として定めることが考えられる。
なお、以下の例は要機密情報を取り扱わないことが前提であることに注意すること。
・サービス約款や利用規約の内容
・サービス事業者の情報セキュリティポリシー及びプライバシーポリシー
・提供サービスにおけるセキュリティ設定及びプライバシー設定の方法（初期設定を含む。）

・情報セキュリティインシデント発生時における個別対応の可否（運用実績等を勘案するとよい。）
また、要機密情報を取り扱わない場合であっても、例えば検索サービスの利用においては、インターネット上に政府職員の身分を明らかにして検索ワード等の情報を提供する行為に等しく、膨大な検索ワード等の情報から、政府機関の関心事項等が分析されるおそれがあることに留意しなければならない。検索サービスを業務に利用する組織において特にそのようなリスクが懸念される場合は、上記のサービス提供条件の確認に加えて、インターネット上で利用端末や通信元を匿名化する対策を導入し、システム部門による適切な管理の下で利用すること等を考慮するとよい。

第２項「責任者」・次条第１号「許可権限者」について
第２項に定める「責任者」と次条第１号に定める「許可権限者」は同一であり、約款による外部サービスを利用する場合において、利用可否を判断する責任者となる。当該責任者は、利用可能なサービスごとに設置され、利用部門からの申請を受け付けて、申請内容に従い利用を許可することになる。一人の責任者が複数のサービスを所管してもよい。また、当該責任者は、所管する約款による外部サービスについて、約款及び利用規約の変更の有無等について定期的に状況把握することが求められる。
なお、当該責任者には、所管する約款による外部サービスに関する技術的な知見を有し、約款による外部サービスを利用する際に考慮すべきリスクを十分理解し、個々の利用申請に対して適切に判断することが可能な者を充てることが必要である。

C2101-66　（約款による外部サービスの利用に係る対策）（政府機関統一基準の対応項番4.1.2(1)-1）

第六十六条　全学実施責任者は、本学において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定めること。

一　利用申請の許可権限者

二　利用申請時の申請内容

・利用する組織名
・利用するサービス
・利用目的（業務内容）
・利用期間
・利用責任者（利用アカウントの責任者）

三　サービス利用中の安全管理に係る運用手順

・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
・情報の滅失、破壊等に備えたバックアップの取得
・利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等）

四　情報セキュリティインシデント発生時の連絡体制

解説：前条第２項「責任者」・第１号「許可権限者」について

第六十五条「(解説) 第２項「責任者」・次条第１号「許可権限者」について」について」を参照のこと。

第２号「利用責任者（利用アカウントの責任者)」について
前条第２項及び第１号において定めている責任者（許可権限者）とは別に、約款による外部サービスを利用する際に利用アカウントごとの責任者を利用責任者として定めることを求めている。利用部門において利用責任者を定めることになるが、職場情報セキュリティ責任者、部局技術責任者、又は約款による外部サービスの許可権限者が利用責任者を兼ねるなど、組織の規模や特性に応じて柔軟に定めてよい。

【参考】約款による外部サービスの利用申請フローの例
約款による外部サービスの申請手続及び申請許可権限者、運用管理者等の配置例を図７に示す。

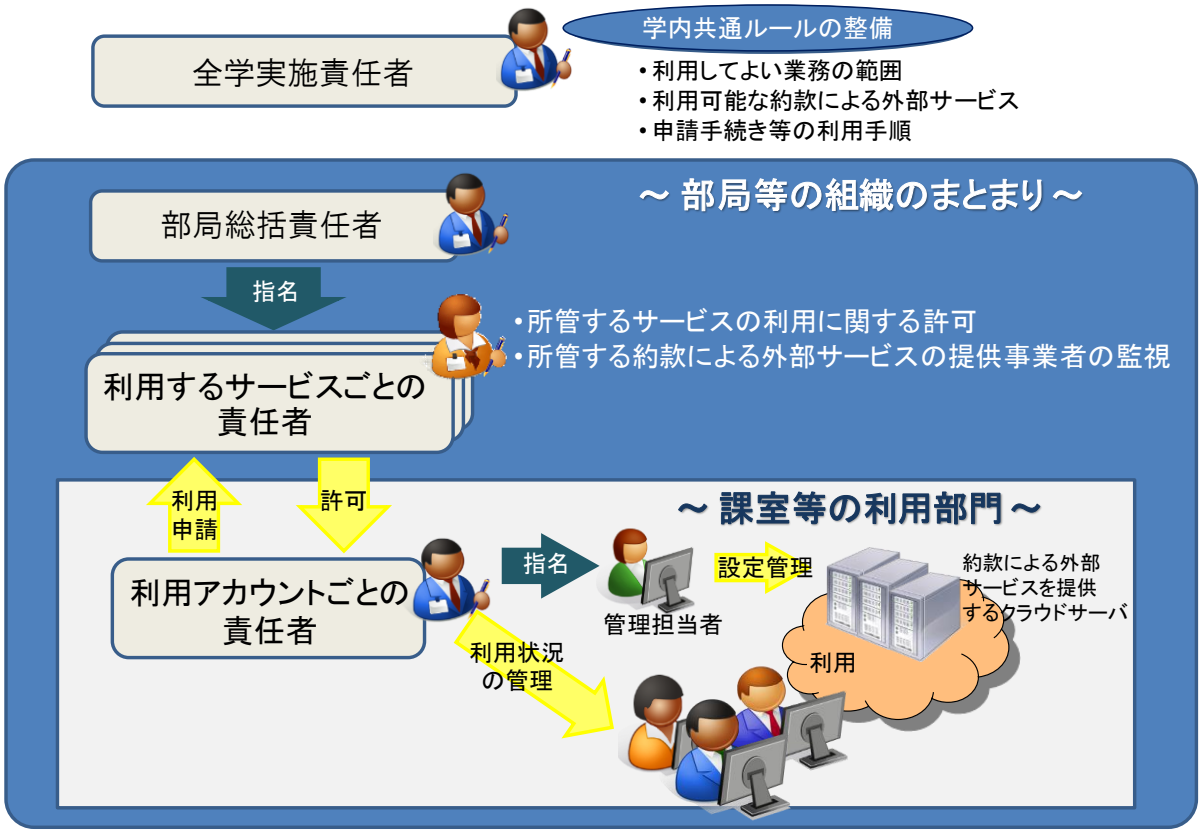


図７　約款による外部サービスの申請手続及び責任者の役割例

C2101-67　（約款による外部サービスの利用における対策の実施）（政府機関統一基準の対応項番 4.1.2(2)）
第六十七条　利用者等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

解説：「利用に当たってのリスク」について

個々の研究教育事務の遂行において、約款による外部サービスの利用を検討する際は、当該サービスの約款、利用規約、その他の利用条件を確認し、以下のリスクや課題への対策を明確化した上で、適切に利用の必要性を判断することが必要である。
なお、以下に掲げるリスクの例は、要機密情報を約款による外部サービスにて取り扱わないことを前提としたものであることに注意すること。
・サーバ装置の故障や運用手順誤り等により、サーバ装置上の情報が滅失して復元不可能となるおそれがある。
・サーバ装置上の要保全情報が第三者等により改ざんされ、復元が困難となるおそれがある。
・サービスが突然停止されるおそれがある。
・約款や利用規約等が予告なく一方的に変更され、セキュリティ設定が変更されるおそれがある。
・情報の取扱いが保証されず、一旦記録された情報を確実に消去することができないおそれがある。

第三節　ソーシャルメディアサービスによる情報発信

解説：インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していく様々なソーシャルメディアサービスが普及している。大学等の教育機関においても、積極的な広報活動等を目的に、こうしたサービスが利用されるようになっている。しかし、ソーシャルメディアサービスを使うには、民間事業者等により提供されているソーシャルメディアサービスは、本学のドメイン名を使用することができないため、真正なアカウントであることを一般利用者等が確認できるようにする必要がある。また、本学のアカウントを乗っ取られた場合や、利用しているソーシャルメディアサービスが予告なく停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く提供する際には、当該情報を必要とする利用者等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により一般利用者の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。
このようなソーシャルメディアサービスは機能拡張やサービス追加等の技術進展が激しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。
なお、ソーシャルメディアサービスの利用は、約款による外部サービスの利用に相当することから、第六十五条、第六十六条及び第六十七条の規定と同様に、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

C2101-68　（ソーシャルメディアサービスによる情報発信時の対策）（政府機関統一基準の対応

項番 4.1.3(1)）

第六十八条　全学実施責任者は、本学が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

一　本学のアカウントによる情報発信が実際の本学のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。

二　パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。

２　部局総括責任者は、本学において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めること。

３　利用者等は、要安定情報の一般利用者への提供にソーシャルメディアサービスを用いる場合は、本学の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

解説：第１項「運用手順等を定める」について

運用手順等を定めるに当たっては、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準を低下させることがないよう留意する必要がある。本学のアカウントにおいて、第三者アカウントの投稿の引用や、第三者が管理又は運用するウェブサイト等へのリンクを掲載することは、当該の投稿やウェブサイト等の内容を信頼性のあるものとして認めていると受け取られることや、リンク掲載後に当該の投稿やウェブサイト等の内容が変更される可能性があることを考慮した上で、慎重に行う必要がある。

第２項「情報発信」について

一旦発信した情報は、ソーシャルメディアを通じて瞬時に拡散してしまうため、完全に削除することは不可能となる。このため、当該情報が公開可能な情報であるか否かについて、情報発信する前に十分に確認する必要がある。

第２項「責任者」について

第六十五条第２項にて定めている責任者と同等であり、ソーシャルメディアサービスの利用申請を受け付けて、利用を許可する許可権限者となる。申請手順や利用責任者の設置等の運用方法については、第７章第２節「約款による外部サービスの利用」を参照すること。

C2101-69　（ソーシャルメディアサービスによる情報発信時の対策の手順）（政府機関統一基準の対応項番 4.1.3(1)-1,2,3,4）

第六十九条　全学実施責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定めること。

一　アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

二　URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する

機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

2　全学実施責任者は、本学のアカウントによる情報発信が実際の本学のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定めること。

一　本学からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、本学が運用していることを利用者に明示すること。

二　本学からの情報発信であることを明らかにするために、本学が A 大学ドメイン名を用いて管理しているウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

三　運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページの URL を記載すること。

四　ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

3　全学実施責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定めること。

一　パスワードを適切に管理すること。具体的には、ログインパスワードは十分な長さと複雑さを持たせ、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

二　二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

三　ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭ったりした場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行うこと。

四　ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。

4　全学実施責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定めること。

一　自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。

二　アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織の CSIRT に報告するなど、適切な対処を行うこと。

第四節　クラウドサービスの利用

解説：業務及び情報システムの高度化・効率化等の理由から、政府機関において今後クラウドサービスの利用の拡大が見込まれている。クラウドサービスの利用に

当たっては、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。
クラウドサービスを利用する際、政府機関がクラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、政府機関による委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分考慮することが求められる。

C2101-70　（クラウドサービスの利用における対策）（政府機関統一基準の対応項番 4.1.4(1)）

第七十条　部局技術責任者は、クラウドサービス（民間事業者が提供するものに限らず、政府等が提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。

２　部局技術責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。

３　部局技術責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。

４　部局技術責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めること。

５　部局技術責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

解説：第１項「情報の取扱いを委ねることの可否」について

クラウドサービスの利用に当たっては、情報の管理や処理をクラウドサービス事業者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなる。そこで、適切なクラウドサービス事業者を選定することにより以下のようなリスクを低減することが考えられる。
クラウドサービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる半面、クラウドサービス事業者の運用詳細は公開されないために利用者にブラックボックスとなっている部分があり、利用者の情報セキュリティ対策の運用において必要な情報の入手が困難である。
オンプレミスとクラウドサービスの併用やクラウドサービスと他のクラウドサービスの併用等、多様な利用形態があるため、利用者とクラウドサービス事業者との間の責任分界点やサービスレベルの合意が容易ではない。
クラウドサービス事業者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者

の情報やプログラムを一つのクラウド基盤で共用することとなるため、情報が漏えいするリスクが存在する。
クラウドサービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスクが存在する。
サーバ装置等機器の整備環境がクラウドサービス事業者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易ではない。
なお、情報セキュリティ確保のためにクラウド利用者自らが行うべきことと、クラウドサービス事業者に対して求めるべきこと等をまとめたガイドラインについては、以下の取組を参考にするとよい。
参考：総務省
「クラウドサービス提供における情報セキュリティ対策ガイドライン」
（平成 26 年 4 月）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html）
参考：経済産業省
「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」、「クラウドセキュリティガイドライン活用ガイドブック」（平成 26 年 3 月 14 日）
（http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html）
参考：公益財団法人 金融情報システムセンター
「金融機関におけるクラウド利用に関する有識者検討会報告書」（平成 26 年 11 月 4 日）
（https://www.fisc.or.jp/isolate/?id=759&c=topics&sid=190）

上記のウェブサイトのアドレスは、平成 29 年 10 月 10 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

第２項「国内法以外の法令が適用されるリスク」について
国内法以外の法令が適用されるリスクとして、データセンターが設置されている国が、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取り決めを遵守しないなどのリスクの高い国である場合、データセンター内のデータが外国の法執行機関の命令により強制的に開示される、データセンターの他の利用者等が原因でサーバ装置等の機器が政府機関のデータを含んだまま没収されるなどが考えられる。

第２項「委託事業の実施場所」について
バックアップデータ、サーバ装置内のデータ等、政府機関の情報が存在し得る場所全てを委託事業の実施場所として考慮することが必要である。

第４項「クラウドサービスの特性」について

クラウドサービスを利用した情報システムは、従来のオンプレミスによる情報システムと比べ、主に以下の特性がある。
クラウドサービス事業者の用意するコンピューティング資源を多くのクラウド利用者で共有し、その上に各クラウド利用者が利用する情報システムが構築される。そのため、本学が情報システムを構築する際のセキュリティ対策のみでなく、クラウドサービス事業者やコンピューティング資源を共有している他のクラウド利用者の情報システムにおいて情報セキュリティインシデントが発生し、その影響を受ける可能性がある。
クラウド利用者は処理能力やストレージ等のコンピューティング資源を、利用者の操作で追加又は削減することができる。しかし、クラウドサービス事業者の用意する資源の不足等が発生した場合に即座に資源の追加ができず、可用性を損なう可能性がある。
クラウドサービス事業者はコンピューティング資源を分散して配置することが可能であり、海外に配置されている可能性がある。

第５項「クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること」について
クラウドサービス事業者及び当該サービスの信頼性が十分であることを総合的に判断するためには、クラウドサービスで取り扱う情報の機密性・完全性・可用性が確保されるように、クラウドサービス事業者のセキュリティ対策を含めた経営が安定していること、クラウドやアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。
このような評価に当たって、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。その場合、監査や認証等によって保証される対象範囲がクラウドサービス事業者の全部又は一部の場合があるので、政府機関が委託するクラウドサービスが当該対象範囲に含まれていることを確認する必要がある。また、監査の場合には、監査項目の網羅性に留意して、重要な監査項目が除かれていないか、監査意見に除外事項（内部統制の不備）が含まれていないかなどを確認する必要がある。さらに、その監査や認証等によっては、クラウドサービス事業者の経営の安定性やサプライチェーン・リスク等は上記の評価に含まれていないことが考えられるため、これらのリスクについては本学において評価する必要がある。
なお、参考となる認証には、ISO/IEC 27017 によるクラウドサービス分野における ISMS 認証の国際規格があり、そこでは「クラウドサービス事業者が選択する監査は、一般的には、十分な透明性をもった当該事業者の運用をレビューしたいとする利用者の関心を満たすに足りる手段とする」ことが要求されており、これらの国際規格をクラウドサービス事業者選定の際の要件として活用することも考えられる。その他、日本セキュリティ監査協会のクラウド情報セキ

ュリティ監査やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告書である SOC 報告書（Service Organization Control Report）を活用することも考えられる。特に、SOC2・SOC3 は、米国公認会計士協会が開発した「Trust サービス原則と基準」で定義された「セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシー」の５つの原則を適用したものであるため、クラウドサービス事業者及びサービスに対する評価の際の参考となり得る。また、SOC2・SOC3 については、日本公認会計士協会の IT 委員会の実務指針により国内でも同様の保証報告書が制度化されている。ただし、SOC2・SOC3 及び実務指針第 7 号においては、この５つの原則の一部のみを選択して実施することができるため、当該監査で選択した原則に「セキュリティ」が含まれていることを保証報告書により確かめる必要がある。

参考：国際規格

「ISO/IEC 27017（安全なクラウドサービス利用のための分野別 ISMS 規格）」

参考：日本セキュリティ監査協会

「クラウド情報セキュリティ管理基準」

（http://jcispa.jasa.jp/documents/）

「クラウド情報セキュリティ監査制度規程」

（http://jcispa.jasa.jp/cloud_security/jcispa_regulation/）

参考：日本公認会計士協会

「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書（日本公認会計士協会 IT 委員会実務指針第 7 号）」

（http://www.hp.jicpa.or.jp/specialized_field/45_8.html）

参考：米国公認会計士協会

「Service Organization Control (SOC) Reports」

（ http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/sorhome.aspx）

上記のウェブサイトのアドレスは、平成 29 年 10 月 10 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

C2101-71　（クラウドサービスの中断や終了時の業務移行に係る対策）（政府機関統一基準の対応項番 4.1.4(1)-1,2）

第七十一条　部局技術責任者は、クラウドサービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することをクラウドサービスの選定条件とし、仕様内容にも含めること。

一　取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件

二　取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

２　部局技術責任者は、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティ対策を構築すること。また、対策を実現するために、以下を例とするセキュリティ要件をクラウドサービスに求め、契約内容にも含めること。特に、運用段階で委託先が変更となる場合、

開発段階等で設計したクラウドサービスのセキュリティ要件のうち継承が必須なセキュリティ要件について、変更後の委託先における維持・向上の確実性を事前に確認すること。

一　クラウドサービスに係るアクセスログ等の証跡の保存及び提供
二　インターネット回線とクラウド基盤の接続点の通信の監視
三　クラウドサービスの委託先による情報の管理・保管の実施内容の確認
四　クラウドサービス上の脆弱性対策の実施内容の確認
五　クラウドサービス上の情報に係る復旧時点目標（RPO）等の指標
六　クラウドサービス上で取り扱う情報の暗号化
七　利用者の意思によるクラウドサービス上で取り扱う情報の確実な削除・廃棄
八　利用者が求める情報開示請求に対する開示項目や範囲の明記

解説：第１項「サービスの中断や終了時に際し、円滑に業務を移行するための対策」について

クラウドサービス事業者が何らかの理由で、クラウドサービスの継続的な提供ができなくなった場合に、他のクラウドサービス事業者に対し、情報の移行を円滑に実施することにより、利用者側での業務を継続できるようにすることが求められる。
そのため、移植性又は相互運用性を確保する観点から、可能な限り、標準化されたデータ形式やインタフェースを使用することが望ましい。

第２項第１号「アクセスログ等の証跡の保存」について
クラウドサービス上におけるアクセスログ等の証跡に係る保存期間については、オンプレミスと同様に情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。
なお、記憶媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する（第百十七条「(解説) 第２項「保存期間」について」を参照のこと。)。

第２項第３号「クラウドサービスの委託先による情報の管理・保管」について
情報管理上の問題として、仮に情報がクラウド上にあったとしても、当該情報の責任は利用者である情報オーナーが負うことになるため、利用者はクラウドサービス事業者による情報の管理・保管方法について事前に把握する必要がある。
また、クラウドサービス事業者が外部委託先に情報の管理・保管を委託した場合、当該情報が利用者の意図しない場面で二次利用されることも懸念されるため、外部委託先における情報セキュリティ水準や情報の取扱方法に関してクラウドサービス事業者に確認の上、合意しておく必要がある。

第２項第４号「脆弱性対策」について
例えば、仮想化技術を用いたマルチテナントの環境において、OS 等の脆弱性

に加えてハイパーバイザーを経由して他の利用者が享受するサービスを阻害する脆弱性はクラウドに対するリスクであり、対策を講ずる必要がある。このような脆弱性を発見する方法として、脆弱性検査ツールを用いた手法やペネトレーションテスト等が挙げられる。

第２項第８号「情報開示請求に対する開示項目や範囲」について
クラウドサービスに関し、クラウドサービス事業者が一般に公開している内容以上の情報提供について、情報セキュリティ対策や監査の観点から、事前に本学とクラウドサービス事業者が協議の上、クラウドサービス事業者が提供する内容の項目や範囲を契約において明記することが必要である。また対象情報の機密性が高い場合、両者間で秘密保持契約（NDA：Non-Disclosure Agreement）を締結するなど必要な措置を講じた上で取得することが求められる。

第八章　情報システムに係る文書等の整備

第一節　情報システムに係る台帳等の整備

解説：本学が所管する情報システムの情報セキュリティ水準を維持するとともに、情報セキュリティインシデントに適切かつ迅速に対処するためには、本学が所管する情報システムの情報セキュリティ対策に係る情報を情報システム台帳で一元的に把握するとともに、情報システムの構成要素に関する調達仕様書や設定情報等が速やかに確認できるように、日頃から文書として整備しておき、その所在を把握しておくことが重要である。

C2101-72　（情報システム台帳の整備）（政府機関統一基準の対応項番 5.1.1(1)）

第七十二条　全学実施責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。

２　部局技術責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について全学実施責任者に報告すること。

解説：第１項「情報システム台帳に整備する」について
あらかじめ全学実施責任者が認めた場合には、全学実施責任者が指定した者に当該台帳を整備させることが考えられる。その際には、全学実施責任者は、指定した者より適宜情報システム台帳の整備状況について報告を受けることが望ましい。全学実施責任者は、台帳の整備状況について把握しておくことが重要である。
情報システムに関する資産管理を行っている組織であれば、資産管理台帳を本項で作成を求めている台帳に代えることが可能である。その場合、本項を削除して関連項目を読み替えても良い。

第２項「情報システムを新規に構築し、又は更改する際には」について
台帳の整備内容の網羅性維持のため、部局技術責任者は、情報システムを新規

に構築した際又は更改した際には、速やかに台帳に記載の事項を報告する必要がある。
なお、台帳を最新に保つため、台帳に記載の事項に変更が生じた場合には、当該変更事項を報告し、台帳を更新する必要があるが、その報告の方法や時期については、本学において別途定めることが望ましい。

C2101-73　（情報システム台帳の記載事項）（政府機関統一基準の対応項番 5.1.1(1)-1）
第七十三条　全学実施責任者は、以下の内容を含む台帳を整備すること。
一　情報システム名
二　管理する職場
三　当該部局技術責任者の氏名及び連絡先
四　システム構成
五　接続する学外通信回線の種別
六　取り扱う情報の格付及び取扱制限に関する事項
七　当該情報システムの設計・開発、運用・保守に関する事項
２　全学実施責任者は、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備すること。
一　情報処理サービス名
二　契約事業者
三　契約期間
四　情報処理サービスの概要
五　ドメイン名（インターネット上で提供される情報処理サービスを利用する場合）
六　取り扱う情報の格付及び取扱制限に関する事項

解説：第１項第４号「システム構成」について
当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、本学としての情報セキュリティ対策を行うために一元的に把握する必要があると判断する事項を含める必要がある。

第１項第７号「設計・開発、運用・保守に関する事項」について
当該情報システムの設計・開発、運用・保守に関する事項の記載は、実施責任者又は実施担当組織、外部委託した場合には委託先及び委託契約形態に関する情報が考えられるが、当該情報システムのライフサイクルに関する経緯や現状を把握し、情報セキュリティ上の問題等が発生した場合に適切な対策を指示するために必要な事項である。

第２項「民間事業者等が提供する情報処理サービスにより情報システムを構築する場合」について
本学として独自の情報システムを構築せずに、民間事業者等が提供するクラウドサービス等の情報処理サービスを利用して情報システムを構築し運用する場合や通信事業者が提供する回線サービスを利用して情報処理業務を行う場合は、利用する情報処理サービス名や契約事業者等の事項を記載したサービス契約に

係る書類を適切に管理しておくことが重要である。これらの書類を集約し、容易に参照できるようにすることをもって台帳整備に代えることができる。
なお、約款による外部サービスを利用する際は、事業者から提供される情報が十分でない場合が想定されるため、その場合は、利用する外部サービスに応じた内容の台帳を整備することも考えられる。

C2101-74　（情報システム関連文書の整備）（政府機関統一基準の対応項番 5.1.1(2)）

第七十四条　部局技術責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備すること。

一　情報システムを構成するサーバ装置及び端末関連情報

二　情報システムを構成する通信回線及び通信回線装置関連情報

三　情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

四　情報セキュリティインシデントを認知した際の対処手順

解説：「情報システム関連文書を整備する」について

当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、本学としての情報セキュリティ対策を行うために一元的に把握する必要があると判断するものを含める必要がある。
文書の整備に当たっては、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は電磁的記録として整備してもよい。
また、所管する情報システムに変更があった場合、また、想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になるため、文書の見直しを定期的に行うことをあらかじめ定めておくとよい。
なお、約款による外部サービスを利用する際は、事業者から提供される情報が十分でない場合が想定されるため、その場合は、利用する外部サービスに応じた内容の情報システム関連文書を整備することも考えられる。

第４号「情報セキュリティインシデントを認知した際の対処手順」について
情報セキュリティインシデントが発生した際の対処手順は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。
・業務継続計画で定める当該情報システムを利用する業務の重要性
・情報システムの運用等の外部委託の内容
また、手順に記載される内容として、例えば以下が想定される。
・情報セキュリティインシデントの内容・影響度の大きさに応じた情報連絡先のリスト
・情報システムを障害等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準
・情報セキュリティインシデントに対する情報システムの構成要素ごとの対処に関する事項
・不正プログラム対策ソフトウェアでは検知されない新種の不正プログラムに感染した場合等に支援を受けるための外部の専門家の連絡先

なお、全学実施責任者が整備する対処手順（第十九条「(解説）第２項「対処手順」について」を参照のこと。）が、情報システムの事情に応じた内容で整備されているならば、情報システム別に整備しなくても構わない。

C2101-75　（情報システム関連文書の記載事項）（政府機関統一基準の対応項番 5.1.1(2)-1,2,3）

第七十五条　部局技術責任者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備すること。

一　サーバ装置及び端末の管理者及び利用者を特定する情報

二　サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン

三　サーバ装置及び端末の仕様書又は設計書

２　部局技術責任者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、以下を含む文書を整備すること。

一　通信回線及び通信回線装置の管理者を特定する情報

二　通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン

三　通信回線及び通信回線装置の仕様書又は設計書

四　通信回線の構成

五　通信回線装置におけるアクセス制御の設定

六　通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応

七　通信回線の利用部門

３　部局技術責任者は、所管する情報システムについて、情報システム構成要素ごとのセキュリティ維持に関する以下を含む手順を定めること。

一　サーバ装置及び端末のセキュリティの維持に関する手順

二　通信回線を介して提供するサービスのセキュリティの維持に関する手順

三　通信回線及び通信回線装置のセキュリティの維持に関する手順

解説：第１項第１号・第２項第１号「管理者」について

サーバ装置及び端末の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システムの構成要素の管理状況を確実に把握できるようにするとともに、障害等を防止する責任の所在を明確化するために必要な事項である。

第１項第２号・第２項第２号「機種並びに利用しているソフトウェアの種類及びバージョン」について

サーバ装置及び端末、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアに脆弱性が存在することにより使用上のリスクが高まった場合に、速やかに脆弱性対策を行うなど、適切に対処するために必要な事項である。

第１項第３号・第２項第３号「仕様書又は設計書」について

情報システムに係る仕様書又は設計書は、情報セキュリティ対策の実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。

第３項「セキュリティ維持に関する以下を含む手順」について
情報システムの構成要素のセキュリティ維持に関する手順は、当該構成要素のセキュリティを維持する目的で管理者が実施すべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理及びログ管理の設定・変更等の手順が挙げられる。

第二節　機器等の調達に係る規定の整備

解説：調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。
これらの課題に対応するため、ポリシー及びそれに基づく規程等に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

C2101-76　（機器等の調達に係る規定の整備）（政府機関統一基準の対応項番 5.1.2(1)）

第七十六条　全学実施責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を本学が確認できることを加えること。

２　全学実施責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

解説：第１項「機器等の選定基準」について
調達する機器等が、ポリシー及びそれに基づく規程等の該当項目を満たし、本学のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を学内で統一的に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映することが必要である。
整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

第１項「必要に応じて」について
機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、当該事項の適用要否を判断した上で整備することを求めている。

第１項「不正な変更」について

ここでいう「不正な変更」とは、機器等の製造工程で不正プログラムを含む予期しない又は好ましくない特性を組み込むことを意味している。
不正な変更が行われない管理がなされていることとは、例えば、機器等の製造工程における不正行為の有無について、定期的な監査を行っていること、機器等の製造環境にアクセス可能な従業員が適切に制限され、定期点検が行われていること等が考えられる。その他、特に高い信頼性が求められる製品を調達する場合は、各製造工程の履歴が記録されているなどの厳格な管理されていることが考えられる。

C2101-77　（機器等の選定基準）（政府機関統一基準の対応項番 5.1.2(1)-1,2）

第七十七条　全学実施責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を例に規定すること。

一　調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、本学と調達先が連携して原因を調査・排除できる体制を整備していること。

２　全学実施責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408 に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定めること。

解説：第１項第１号「原因を調査・排除できる体制」について

OEM（Original Equipment Manufacturer）によって提供される機器等についても、OEM 製品の製造者においても不正な変更が加えられないよう、OEM 製品の販売者が機器等のサプライチェーン全体について適切に管理していることも含めて、要件を定めることが考えられる。

第２項「ISO/IEC 15408 に基づく認証」について

機器等の調達においては、ISO/IEC 15408 に基づく認証を取得している製品の優遇を選定基準の一つとすることで、第三者による情報セキュリティ機能の客観的な評価を受けた製品を活用でき、信頼度の高い情報システムが構築できる。
ISO/IEC 15408 に基づく認証では、第三者によって、対抗する脅威に必要な機能が設計書に反映されていること、その機能が設計どおり実装されていること、開発現場や製造過程においてセキュリティが侵害される可能性が無いこと、利用マニュアル・ガイダンス等にセキュリティを保つための必要事項が明確に示されていること等が客観的に評価され、評価結果及び既知の情報から懸念される脆弱性についての評定及びテストが実施される。ただし、第三者によって評価・保証される範囲は、適合する Protection Profile（国際標準に基づくセキュリティ要件）や、評価保証レベル（EAL：Evaluation Assurance Level）によって異なるため、どの程度の保証を得ている認証製品であるかを、調達時に確認することが必要となる。

C2101-78　（納品時の確認・検査手続）（政府機関統一基準の対応項番 5.1.2(1)-3）

第七十八条　全学実施責任者は、機器等の納入時の確認・検査手続には以下を含む事項を確認で

きる手続を定めること。
一　調達時に指定したセキュリティ要件の実装状況
二　機器等に不正プログラムが混入していないこと

解説：「以下を含む事項を確認できる手続」について

機器等の納入時の確認・検査手続の具体例として、以下の内容が考えられる。

・調達時に指定したセキュリティ要件（機器等に最新のセキュリティパッチが適用されているかどうか、不正プログラム対策ソフトウェア等が最新の脆弱性に対応しているかどうか等にも留意）に関する試験実施手順及び試験結果を納品時に報告させて確認

・セキュリティ要件として調達時に指定した機能が正しく動作することを受入れテストにより確認

・内部監査等により不正な変更が加えられていないことを確認した結果を納品時に報告させて確認

第九章　情報システムのライフサイクルの各段階における対策

第一節　情報システムの企画・要件定義

解説：情報システムのライフサイクル全般を通じて、情報セキュリティを適切に維持するためには、情報システムの企画段階において、適切に情報セキュリティ要件を定義する必要がある。

セキュリティ要件の曖昧さや過不足は、過剰な情報セキュリティ対策に伴うコスト増加のおそれ、要件解釈のばらつきによる提案内容の差異からの不公平な競争入札、設計・開発工程での手戻り、運用開始後の情報セキュリティインシデントの発生といった不利益が生じる可能性に繋がる。

そのため、情報システムが対象とする業務、業務において取り扱う情報、情報を取り扱う者、情報を処理するために用いる環境・手段等を考慮した上で、当該情報システムにおいて想定される脅威への対策を検討し、必要十分なセキュリティ要件を仕様に適切に組み込むことが重要となる。

加えて、構築する情報システムへの脆弱性の混入を防止するための対策も、構築前の企画段階で考慮することが重要となる。

また、情報システムの構築、運用・保守を外部委託する場合については、第７章第１節「外部委託」についても併せて遵守する必要がある。

C2101-79　（実施体制の確保）（政府機関統一基準の対応項番 5.2.1(1)）

第七十九条　部局技術責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者に求めること。

２　部局技術責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し、運用管理する本学が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めること。

解説：第１項「情報システムを統括する責任者に求める」について

情報システムを統括する責任者（情報化統括責任者（CIO））が確立した体制が、

セキュリティ維持の側面からも実施可能な体制（人員、機器、予算等）となるように求める事項である。

C2101-80　（情報システムのセキュリティ要件の策定）（政府機関統一基準の対応項番 5.2.1(2)）

第八十条　部局技術責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定すること。

一　情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

二　情報システム運用時の監視等の運用管理機能要件

三　情報システムに関連する脆弱性についての対策要件

２　部局技術責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。

３　部局技術責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

４　部局技術責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

解説：第１項「インターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離する」について

標的型攻撃による不正プログラム感染の脅威は避けられないものになっており、外部のネットワークと接続する情報システムは、不正プログラムの感染を前提とした対策を講ずることの重要度が、年々増加している。

外部ネットワークとの接続形態を含む情報システムの全体構成は、情報システムにおいて取り扱われる情報の格付や取扱制限、情報システムを利用する業務の形態等によって決定する必要があるが、特に重要な情報を取り扱う情報システムについては、インターネットからの直接的なサイバー攻撃を受けないよう、インターネット回線や、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することが求められる。また、分離した情報システムの USB ポート等の外部ネットワーク・システムとの接点についても適切に運用することが望ましい。

第１項「情報システムのセキュリティ要件」について

「情報システムのセキュリティ要件」には、ハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された

情報システムの運用のセキュリティ要件がある。
なお、前者のセキュリティ要件については、構築環境や構築手法等のセキュリティに関する手順も含まれる。
決定されたセキュリティ要件は、システム要件定義書や仕様書等の形式で明確化した上で、実装していくことが望ましい。
情報システムのセキュリティ要件を検討する際には、仮想化技術の活用の有無を確認し、物理的に分割されたシステムに限らず、論理的に分割されたシステムであるかを考慮したセキュリティ要件を検討することも重要である。「論理的に分割されたシステム」とは、一つの情報システムの筐体上に複数のシステムを共存させることを目的として、論理的に分割させた状態の情報システムをいう。
また、外部の情報システムを利用する場合は、第７章第１節「外部委託」も参照の上、委託先との管理責任範囲の分担を明確化し、セキュリティ対策の実施に漏れが生じないようにすることも重要である。
このように、情報システムの構築形態及び調達形態に応じてセキュリティ要件を定めることが求められる。

第２項「接続するインターネット回線を定めた上で」について
構築する情報システムごとに、個々にインターネット回線を構築すると、当該インターネット回線の監視等に係る体制や運用コストが分散し、効率的かつ集中的なセキュリティ監視が行われず、セキュリティ水準が低下するおそれがある。このような観点から、機関としてインターネット接続口を統合・集約し、集中的なセキュリティ監視を行うなどの取組を行っている場合は、当該取組の範疇とするか否か検討した上で、構築する情報システムに接続するインターネット回線を仕様書等において明確化しておくことを求めている。
なお、既設のインターネット回線を利用せずに、独立したインターネット回線を調達してセキュリティ監視等の運用を個別に行う場合も想定される。情報システムが取り扱う情報の格付や取扱制限等の特性に従って、既設のインターネット回線の利用可否を判断することが望ましい。

第２項「IT 製品の調達におけるセキュリティ要件リスト」について
「IT 製品の調達におけるセキュリティ要件リスト」には、複合機、OS、USB メモリ等の製品分野ごとに一般的に想定されるセキュリティ上の脅威が記載されており、それらが自身の運用環境において該当する場合には対抗する必要がある。
対抗手段の一つとして、「IT 製品の調達におけるセキュリティ要件リスト」には、IT セキュリティに関わる「国際標準に基づくセキュリティ要件」が記載されており、それを調達時に活用することで脅威に対抗するための機能を有した製品を調達することが可能となる。
「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」のうち、製品の利用環境や製品に実装されている機能によっ

ては、一部の脅威だけに対抗すればよい場合もあり得る。そのような場合には、「国際標準に基づくセキュリティ要件」では過剰な要件（要求仕様）となる可能性もあるので、個別にセキュリティ要件を策定して脅威に対抗してもよい。
参考：経済産業省「IT 製品の調達におけるセキュリティ要件リスト」
（http://www.meti.go.jp/policy/netsecurity/cclistmetisec.pdf）

C2101-81　（情報システムのセキュリティ要件に係る対策）（政府機関統一基準の対応項番 5.2.1(2)-1,2,3,4,5）

第八十一条　部局技術責任者は、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定すること。

２　部局技術責任者は、開発する情報システムが運用される際に想定される脅威の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書等に明記すること。

３　部局技術責任者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、ST 確認を受けること。

４　部局技術責任者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、以下を含む措置を実施すること。

一　情報システム運用時に情報セキュリティ確保のために必要となる管理機能を仕様書等に明記すること。

二　情報セキュリティインシデントの発生を監視する必要があると認めた場合には、監視のために必要な機能について、以下を例とする機能を仕様書等に明記すること。

・学外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能
・不正プログラム感染や踏み台に利用されること等による学外への不正な通信を監視する機能
・学内通信回線への端末の接続を監視する機能
・端末への外部電磁的記録媒体の挿入を監視する機能
・サーバ装置等の機器の動作を監視する機能

５　部局技術責任者は、開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を含む対策を仕様書等に明記すること。

一　既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

二　開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針。

三　セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。

四　ソフトウェアのサポート期間又はサポート打ち切り計画に関する本学への情報提供。

解説：第２項「開発する情報システムが運用される際に想定される脅威」について
汎用ソフトウェアをコンポーネントとして情報システムを構築する場合はもとより、全てを独自開発する場合であっても、外部から脆弱性をつかれる可能性があるため、開発する情報システムの機能、ネットワークの接続状況等から、想定される脅威を分析する必要がある。

また、情報システムを構成する端末、サーバ装置、それらに搭載されているソフトウェア等に関して想定される脅威に対しては、第１４章～第１６章で規定された対策が適切に実施されるようにセキュリティ要件を策定することが必要となる。策定に当たっては、運用開始後に適切に対策が講じられるようにシステムの企画段階から留意する必要がある。例えば、サーバ装置の運用時に必要になる不正アクセス等の監視機能を実装すること、端末やサーバ装置等に利用を認めるソフトウェア以外のソフトウェアが意図せず混入されないこと等について留意が必要となる。

第３項「ST 確認」について
セキュリティ要件の策定に当たっては、脅威に対抗するために妥当なセキュリティ要件となっていることの確認を求める事項である。
セキュリティ要件の妥当性確認には、学内でのレビューの実施等の他に、対象とする情報システムが扱う業務及び情報の重要度によっては、セキュリティ要件の策定に関っていない客観的な立場の者による検証を実施することが望ましい。
「ST 確認」とは、情報システムが対抗すべき脅威について適切なセキュリティ要件が策定されていることを確認するために、セキュリティ設計仕様書(ST:Security Target)を IT セキュリティ評価基準(ISO/IEC 15408)に基づき、第三者である評価機関が評価し、その評価結果が妥当であることを認証機関（独立行政法人情報処理推進機構）が検証し、確認することをいう。

第４項第１号「管理機能」について
「管理機能」とは、真正確認、権限管理等のセキュリティ機能を管理するための機能のほか、情報セキュリティインシデントの発生時に行う対処及び復旧に係る機能、証跡保全の機能等を指し、これらの必要性を情報システムの設計時から検討することにより、必要がある場合には情報システムに組み込む必要がある。

第４項第２号「監視のために必要な機能」について
情報システム及び取り扱う情報の格付や取扱制限等を考慮して、情報システムの各所において様々なイベントを監視する必要性を見極める必要がある。監視するイベントとしては、通信回線を通してなされる不正アクセス又は不正侵入、情報システムの管理者・運用者又は利用者の誤操作若しくは不正操作、サーバ装置等機器の動作、許可されていない者の要管理対策区域への立入り等があり得る。
なお、監視によりプライバシーを侵害する可能性がある場合は、関係者への説明について定めること。

第５項「脆弱性への対策」について
脆弱性対策を怠った場合には、セキュリティ侵害の機会を増大することにつな

がるため、情報システムの企画段階から対策を講じておく必要がある。
脆弱性が存在することが公表されているソフトウェア等については対策が施されているバージョンのものを利用することや、開発後の情報システムに脆弱性が存在することが発覚した場合に備えて、調達時の仕様書に対策のための要件を明記しておくことが重要となる。

第５項第２号「脆弱性が混入されることを防ぐためのセキュリティ実装方針」について
「脆弱性が混入されることを防ぐためのセキュリティ実装方針」とは、情報システム開発者が情報システムに脆弱性を混入することを防ぐために、開発時における脆弱性への具体的な対策方法を定めたものである。脆弱性は種類ごとに対策が異なり、懸念される脆弱性の種類ごとに方針を定める必要がある。具体的に定めるものとして例えば以下の内容が考えられる。
・バッファオーバーフローによる不正なプログラムの挿入及び実行を防ぐために、データを転記する場面においてメモリ領域長とデータ長を検査する処理を付加する。
・SQL インジェクションによるデータベース内の情報の漏えい・改ざんを防ぐために、プレースホルダにより SQL 文を組み立てる。
・OS コマンドインジェクションによる不正なシステム操作を防ぐために、シェルを起動できる言語機能を利用しない。
本規程第百二十九条「ソフトウェアに関する脆弱性対策」及び第十五章第二節「ウェブ」の規定内容も参考にして、懸念される全ての脆弱性の種類に対して、実装方針を定め、仕様書に明記する必要がある。

C2101-82　（政府機関統一基準の対応項番 5.2.1(2)-6）
第八十二条　部局技術責任者は、構築する情報システムの構成要素のうち製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施すること。
一　「IT 製品の調達におけるセキュリティ要件リスト」を参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とすること。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。
二　「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定すること。

解説：第２号「機器等の利用環境において対抗すべき脅威」について
機器等に関連したセキュリティ上の脅威は利用環境によって変わるため、調達時にどのような環境で運用するのかを把握し、その環境において存在する脅威を分析した上で、必要となるセキュリティ要件を策定する必要がある。

例えば、ネットワークに接続し、通信データとして要保護情報を送受信する場合に盗聴による情報漏えいが想定される場合には、通信データの保護に係るセキュリティ要件が必要となるが、スタンドアロンで利用する場合で、盗聴による情報漏えいが想定されない場合には、通信データの保護に係るセキュリティ要件は不必要なセキュリティ要件となる可能性がある。
また、特定の人物しか物理的にアクセスできないように隔離された場所へ機器等を設置すること等で、誰もが物理的にアクセスできる環境で想定される脅威を軽減することも考えられる。
調達する機器ごとの利用環境において想定される脅威を漏れなく分析した上で、脅威に対抗するために必要十分なセキュリティ要件を策定することが重要である。

C2101-83　（情報システムの構築を外部委託する場合の対策）（政府機関統一基準の対応項番5.2.1(3)）

第八十三条　部局技術責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させること。

一　情報システムのセキュリティ要件の適切な実装

二　情報セキュリティの観点に基づく試験の実施

三　情報システムの開発環境及び開発工程における情報セキュリティ対策

C2101-84　（情報セキュリティの観点に基づく試験の実施）（政府機関統一基準の対応項番5.2.1(3)-1）

第八十四条　部局技術責任者は、情報セキュリティの観点に基づく試験の実施について、以下を含む事項を実施させること。

一　ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離すること。

二　情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。

三　情報セキュリティの観点から実施した試験の実施記録を保存すること。

解説：第１号「運用中の情報システムに悪影響」について

運用中の情報システムを利用してソフトウェアの作成及び試験を行う場合は、運用中の情報システムに悪影響が及ぶことを回避することが大前提となる。
また、開発中のソフトウェアの動作確認のために、運用中の情報システムの要機密情報をテストデータとして、試験を行う情報システムにおいて使用しないようにする必要がある。

第２号「情報セキュリティの観点から必要な試験」について

攻撃が行われた際に情報システムがどのような動作をするかを試験する項目として想定しており、具体的には、想定の範囲外のデータの入力を拒否できるか、サービス不能攻撃等により情報システムが過負荷状態に陥った場合に処理中のデータは保証されるか、レースコンディションが発生しないか第百七十七条

（「(解説) 第１２号「レースコンディション脆弱性」について」を参照のこと。）といった項目が挙げられる。
なお、セキュリティ機能の試験だけにとどまらず、情報システムの脆弱性の有無、必要なチェック機能の欠如等について、必要な試験が網羅されるよう留意することが望ましい。

第３号「実施記録」について
「実施記録」とは、試験の項目、実施結果、実施時に判明した不具合及び当該不具合の修正の記録等を指し、これらを保存することにより、脆弱性を発見した場合の対処に利用できるようにすることが求められる。

C2101-85　（情報システムの開発環境及び開発工程における情報セキュリティ対策）（政府機関統一基準の対応項番 5.2.1(3)-2）

第八十五条　部局技術責任者は、開発工程における情報セキュリティ対策として、以下を含む事項を実施させること。

一　ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。
・ソースコードの変更管理
・ソースコードの閲覧制限のためのアクセス制御
・ソースコードの滅失、き損等に備えたバックアップの取得

二　情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

三　セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること。

解説：「開発工程における情報セキュリティ対策」について
情報システム開発に係る情報資産についてセキュリティを維持するための手順及び環境を定めることを求めている。
具体的な手順としては、例えば、仕様書、ソースコード等の成果物に対して情報システムのライフサイクル全般にわたって一貫性を確保及び維持するための構成管理の手順及び利用するツール等が考えられる。
開発環境については、例えば、ドキュメント及びソースコードに対するアクセス権、開発に利用するサーバ装置及び端末の設置場所及びアクセス制御の方法等がある。
なお、情報システム開発を外部委託する場合は、委託先に対するセキュリティ要件定義の策定手順や導入時のセキュリティ評価試験手順等を整備しておく必要がある。

第３号「設計レビュー」について
情報システムの設計について、脆弱性の原因となる設計の不具合をなくすために、設計レビューの実施が求められる。

一般に設計レビューには、①レビュー対象内にあるエラーの発見を第一目的とし、開発責任者等が実施する確認手法（インスペクション）、②開発担当者自身が開発関係者を集め、レビュー対象プログラムを実行の流れに従って追跡し確認する手法（ウォークスルー）等があり、これらを、いつ、誰が、何に対して実施するのか、といったことを定める必要がある。

第３号「ソースコードレビュー」について
ソースコードに脆弱性が混入しないように、ソースコードレビューの範囲及び方法について、あらかじめ定めておくことが求められる。例えば、脆弱性の原因となるソースコードについては、開発言語ごとに典型的なパターンが知られていることから、ソースコードレビューによる検証が有効な場合がある。ソースコードレビューについては、開発する情報システムだけを対象として想定しており、市販製品を組み込む場合等、ソースコードの入手が困難な場合に実施することは想定していない。

C2101-86　（情報システムの運用・保守を外部委託する場合の対策）（政府機関統一基準の対応項番 5.2.1(4)）
第八十六条　部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。

C2101-87　（情報システムの運用・保守を外部委託する場合の対策）（政府機関統一基準の対応項番 5.2.1(4)-1）
第八十七条　部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を含む要件を調達仕様書に記載するなどして、適切に実施させること。
一　情報システムの運用環境に課せられるべき条件の整備
二　情報システムのセキュリティ監視を行う場合の監視手順や連絡方法
三　情報システムの保守における情報セキュリティ対策
四　運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

解説：第１号「運用環境に課せられるべき条件」について
情報システムの運用環境に課せられるべき条件としては、物理的、接続的（ネットワーク環境）及び人的側面を考慮する必要がある。どのような条件を設定するかによって想定される脅威が異なってくるため、脅威を想定する上で必要となる条件は全て調達仕様書、契約書等に記載する必要がある。
物理的な設置環境に関する条件とは、サーバ装置を設置する場所の特定、耐震・防火に関する基準、電源供給に関する基準等に関する条件を示すものである。
接続面（ネットワーク環境等）に関する条件とは、情報システムが接続されるネットワーク環境や通信回線の基準、情報セキュリティ上の何らかのリスクを伴う外部サービスをネットワーク経由で利用する場合の条件等を示すものである。

人的環境とは、対象とするシステムの管理者や業務担当職員の信頼性に関する条件、当該システムに関わる組織・体制として実現すべきことに関する条件、当該システムの使用方法として当然実現されるべきことに関する条件等を示すものである。

第２号「監視手順」について
情報システムのセキュリティ監視を行う体制を特別に設けずに情報システムの運用を行う体制においてセキュリティ監視も行うことも考えられる。
監視によりプライバシーを侵害する可能性がある場合は、対象となる関係者への説明等の手順についても本学として定めておくこと。

第３号「保守における情報セキュリティ対策」について
情報システムの保守においては、保守担当者が作業中に権限外の情報にアクセスできないよう、アクセス制御や権限管理を考慮する必要がある。また、保守担当者へのなりすましが脅威として想定される場合には、保守担当者に対する主体認証も開発する情報システムのセキュリティ要件策定時に考慮する必要もある。

第４号「脆弱性が存在することが判明」について
ソフトウェアやウェブアプリケーション等の情報システムに関連する脆弱性は日々新たなものが報告されており、調達時に策定した脆弱性についての対策要件だけでは十分に対処できない可能性もあり得る。
また、運用・保守を行う委託先が、情報システムの構築を行った委託先と異なる場合、情報システム運用開始後に発見された脆弱性に対して、情報システムの構築を行った委託先のみでは対処することが困難な場合もあり得る。そのため、運用・保守を行う委託先に対して、運用開始後に発見された脆弱性への対処を求めることも、契約又は仕様書において考慮する必要がある。

第二節　情報システムの調達・構築

解説：情報システムを調達・構築する際には、策定したセキュリティ要件に基づく情報セキュリティ対策を適切に実施するために、選定基準に適合した機器等の調達や、情報システムの開発工程での情報セキュリティ対策の実施が求められる。
また、機器等の納入時又は情報システムの受入れ時には、整備された検査手続に従い、当該情報システムが運用される際に取り扱う情報を保護するためのセキュリティ機能及びその管理機能が、適切に情報システムに組み込まれていることを検査することが必要となる。

C2101-88　（機器等の選定時の対策）（政府機関統一基準の対応項番 5.2.2(1)）

第八十八条　部局技術責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用すること。

解説：「選定基準に対する機器等の適合性を確認」について

第七十六条第１項において整備された機器等の選定基準に従って、機器等の開発等のライフサイクルにおいて不正な変更が加えられない管理体制が確認できることや、第三者による情報セキュリティ機能の客観的な評価が行われていることを確認すること等を求めている。
なお、ISO/IEC 15408 に基づく認証を取得していることを選定基準として活用した場合には、調達先から認証取得を証明するための認定書等を調達先に提示させることも考えられる。

C2101-89　（情報システムの構築時の対策）（政府機関統一基準の対応項番 5.2.2 (2)）
第八十九条　部局技術責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。
２　部局技術責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。
解説：第２項「移行手順及び移行環境」について
情報システムの開発環境、テスト環境から本番運用の環境への移行時において、情報システムに保存されている情報の取扱い手順の整備、人為的な操作ミスを防止するための手順・環境の整備、移行の際に関連システム停止が伴う場合には可用性確保のための環境整備等が必要となる。

C2101-90　（情報システムの構築時の対策事項）（政府機関統一基準の対応項番 5.2.2 (2)-1,2）
第九十条　部局技術責任者は、情報システムの構築において以下を含む情報セキュリティ対策を行うこと。
一　情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備すること。
二　セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。
三　情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。
四　セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施すること。
五　脆弱性検査を含む情報セキュリティの観点での試験を実施すること。
２　部局技術責任者は、情報システムの運用保守段階へ移行するに当たり、以下を含む情報セキュリティ対策を行うこと。
一　情報セキュリティに関わる運用保守体制の整備
二　運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施
三　情報セキュリティインシデントを認知した際の対処方法の確立
解説：第１項「情報セキュリティ対策」について
情報システムの構築を外部委託する場合には、第９章第１節「情報システムの企画・要件定義」の第八十三条（情報システムの構築を外部委託する場合の対策）の内容を委託先に適切に実施させることが求められる。
また、情報システムの構築を外部委託せず、本学自らが構築する場合であっても、同項の内容を参照し、必要な対策を実施することが求められる。

C2101-91　（納品検査時の対策）（政府機関統一基準の対応項番 5.2.2 (3)）

第九十一条　部局技術責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。

解説：「情報セキュリティ対策に係る要件が満たされていることを確認する」について情報セキュリティ対策の視点を加味して整備された納入時の確認・検査手続に従い、納入された情報システム及び機器等が要求仕様どおりに正しく動作することの検査を行うことが求められる。

本学における受入れテストの実施、納入元が実施したテストに関する資料の提出要求及びその検査内容の確認、第三者への受入れテストの委託、ISO/IEC 15408 に基づく第三者認証取得の確認等、検査対象の情報システム及び機器等の特性に応じて適切な検査を実施する必要がある。

第三節　情報システムの運用・保守

解説：情報システムの運用段階に移るに当たり、企画又は調達・構築時に決定したセキュリティ要件が適切に運用されるように、人的な運用体制を整備し、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を実施する必要がある。

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生することが大半であることから、適宜情報システムの情報セキュリティ対策の実効性を確認するために、情報システムの運用状況を監視することも重要である。

また、情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても、ポリシー及びそれに基づく規程等に基づく情報セキュリティ対策について適切に措置を講ずることが求められる。

C2101-92　（情報システムの運用・保守時の対策）（政府機関統一基準の対応項番 5.2.3(1)）

第九十二条　部局技術責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。

２　部局技術責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し、運用管理する本学との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

３　部局技術責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

C2101-93　（情報システムの運用・保守時の対策事項）（政府機関統一基準の対応項番 5.2.3(1)-1,2,3,4）

第九十三条　部局技術責任者は、情報システムのセキュリティ監視を行う場合は、以下の内容を

含む監視手順を定め、適切に監視運用すること。
一　監視するイベントの種類
二　監視体制
三　監視状況の報告手順
四　情報セキュリティインシデントを認知した場合の報告手順
五　監視運用における情報の取扱い（機密性の確保）

2　部局技術責任者は、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認すること。

3　部局技術責任者は、情報システムにおいて取り扱う情報について、当該情報の格付及び取扱制限が適切に守られていることを確認すること。

4　部局技術責任者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。

解説：第２項「セキュリティ機能が適切に運用されていること」について
運用する情報システムについて、外部環境が大きく変化した場合等には、セキュリティ機能が適切に運用されるために、機器等のパラメータ設定、物理的な設置環境、ネットワーク環境、人的な運用体制等について問題が無いことを適宜確認する必要がある。

第３項「当該情報の格付及び取扱制限が適切に守られていること」について
情報の格付けの見直し及び再決定が行われた際や、当該情報システムに係る教職員等の異動や職制変更等が生じた際には、情報に対するアクセス制御の設定や職務に応じて与えられている情報システム上の権限が適切に変更される必要がある。

第４項「脆弱性の存在が明らかになった場合」について
本学が運用する情報システムに関連する脆弱性が存在することが発覚した場合、セキュリティパッチの適用等の情報セキュリティ対策が必要となる。
また、情報セキュリティ対策が適用されるまでの間にセキュリティ侵害が懸念される場合には、当該情報システムの停止やネットワーク環境の見直し等情報セキュリティを確保するための運用面での対策を講ずる必要もある。

第四節　情報システムの更改・廃棄

解説：情報システムの更改・廃棄において、情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。
情報システムに機密性の高い情報が記録されている場合や、格付や取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講ずることが必要となる。

C2101-94　（情報システムの更改・廃棄時の対策）（政府機関統一基準の対応項番 5.2.4(1)）
第九十四条　部局技術責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システム

に保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。

一　情報システム更改時の情報の移行作業における情報セキュリティ対策

二　情報システム廃棄時の不要な情報の抹消

解説：第１号「情報の移行」について

情報システムを更改する際は、更改元の情報システムから更改先の情報システムに情報（本番データ）を移行する作業が発生する場合が多いが、移行作業の過程で情報が外部に漏えいすることのないよう、移行用の本番データを適切に管理することが必要である。移行用の本番データの管理手順や外部電磁的記録媒体を使用する場合の安全管理措置等をあらかじめ定めておくとよい。

移行作業を外部委託する場合においては、委託先とあらかじめ手順について合意し、仕様書に明記しておく必要がある。

第２号「情報の抹消」について

情報システムの廃棄を行う場合には、情報システムを構成する機器等並びに内部に保存されている情報の格付及び取扱制限を考慮して、適切に抹消する必要がある。要機密情報を保存している情報システムにおいては、情報の抹消が求められる。廃棄の際に本規定を考慮すべき機器等としては、サーバ装置や端末以外にも、複合機等の内蔵電磁的記録媒体を備えた機器については同様に考慮する必要がある。第１４章・第１６章において機器ごとの廃棄時の対応を規定しているので、併せて考慮されたい。

なお、情報システムの廃棄を外部委託する際は、委託先において情報の抹消が適切に実施されるよう、第五十条「情報の消去」の規定も参考に、抹消方法等についてあらかじめ合意し仕様書等に明記しておく必要がある。委託先の抹消作業に関する作業完了届（廃棄したことが証明されるもの）等を書面で受け取るなどするとよい。

第五節　情報システムについての対策の見直し

解説：情報セキュリティを取り巻く環境は常時変化しており、新たに発生した脅威等に的確に対応しない場合には、情報セキュリティ水準を維持できなくなる。このため、情報システムの情報セキュリティ対策を定期的に見直し、さらに外部環境の急激な変化等が発生した場合は、適時見直しを行うことが必要となる。

C2101-95　（情報システムについての対策の見直し）（政府機関統一基準の対応項番 5.2.5(1)）

第九十五条　部局技術責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

解説：「見直し」について

情報システムの情報セキュリティ対策について、新たな情報セキュリティ上の脅威、情報セキュリティインシデント発生事案例及び情報セキュリティインシデント発生時の影響等を検討した上で、情報システムの情報セキュリティ対策について定期的に見直しを行い、セキュリティ要件の追加、修正等の必要な措

置を求める事項である。
所管する情報システムに変更があった場合、また、情報システムの外部環境に変化が生じた場合には、定期的な情報セキュリティ対策の見直しに加えて、適時見直すことも必要となる。

第十章　情報システムの運用継続計画

第一節　情報システムの運用継続計画の整備・整合的運用の確保

解説：業務の停止が一般利用者の安全や利益に重大な脅威をもたらす可能性のある業務は、非常時でも継続させる必要があり、本学においては業務継続計画を策定し運用している。
一方、非常時に情報システムの運用を継続させる場合には、非常時における情報セキュリティに係る対策事項を検討し、定めることが重要となる。
なお、業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。

C2101-96　（情報システムの運用継続計画の整備・整合的運用の確保）（政府機関統一基準の対応項番 5.3.1(1)）

第九十六条　全学実施責任者は、本学において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討すること。

２　全学実施責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認すること。

解説：第１項「非常時優先業務」について
応急業務（災害応急対策業務及び被災状況に応じて速やかな実施が必要となる他の緊急業務）及び継続の必要性の高い通常業務を合わせたものを「非常時優先業務」という。

第１項「情報システムの運用継続計画を整備」について
非常時優先業務を支える情報システムの運用継続計画を整備するに当たっては、情報システムの運用継続計画の作成に資する資料として、内閣官房情報セキュリティセンターが取りまとめた以下の資料を参照することが考えられる。
参考：内閣官房情報セキュリティセンター「「中央省庁における情報システム運用継続計画ガイドライン」及び関連資料」（平成 25 年 6 月）
（http://www.nisc.go.jp/active/general/itbcp-guideline.html）

第１項「非常時における情報セキュリティに係る対策事項」について
情報システムの運用継続を脅かす危機的事象の例として、地震、風水害等の自然災害、火災等の人的災害・事故、停電等の社会インフラの不全、不正アクセス等の運用妨害、機器等の故障等が想定される。これらの非常時に対して、業務継続計画、情報システムの運用継続計画、ポリシー及びそれに基づく規程等

のそれぞれで定める対策に矛盾があると、非常時に利用者等は一貫性のある行動をとることができない。このため、非常時における情報セキュリティに係る対策事項を検討する際は、業務継続計画及び情報システムの運用継続計画とポリシー及びそれに基づく規程等との間で整合性を確保するよう検討することが必要である。
例えば、非常時に、情報システムの主体認証情報として設定したパスワードを設定した者以外の者が当該情報システムを使用しなければならない場合が想定される。このような場合の実施手順について、業務継続計画及び情報システムの運用継続計画で安易に定めるのではなく、ポリシー及びそれに基づく規程等において、非常時でも情報セキュリティ水準を確保した実施手順を整備する必要がある。手順の一例としては、通常時に利用する識別コードとパスワードとは別に、非常時用の識別コードとパスワードをあらかじめ設定しておく方法が考えられる。この場合、非常時用のパスワードは人が記憶困難な文字列で設定し、そのパスワードを記載した紙面を施錠された安全な保管場所に保管することで、通常時のパスワードを非常時に聞き出したり、通常時にパスワードを共用したりすることなく、非常時においても情報システムの利用が可能となる。
また、パスワードを記載した紙面を保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用すれば、通常時における不正使用の有無を確認できる。
また、非常時には、本学の施設の一部に帰宅困難者等を受け入れる場合等、通常時の情報セキュリティ水準の確保に支障をきたす状況が考えられる。このような場合を想定し、あらかじめ情報セキュリティ水準の確保を要する施設や業務への影響を分析し、必要な対策を十分検討した上で、通常時及び非常時の対応を定める必要がある。例えば、各執務室や各教職員等の卓上の情報セキュリティ対策を含め、通常時から不特定の者の出入りを想定した対策を講ずること等が考えられる。
なお、停電や交通機関の麻痺等の社会インフラの不全等により、通常時に利用している情報システムが利用できなくなる場合や、通常時に利用している場所で情報システムを利用することができない場合等、情報システムを利用する環境が制限される状況が考えられる。このような場合を想定し、約款による外部サービス、本学支給以外の端末等の利用が非常時優先業務の継続に有効であると判断される場合には、それらを利用して業務を継続することについても、そのリスクや情報セキュリティ水準の確保等を十分に検討した上で、あらかじめ定めておく必要がある。

第２項「運用可能であるかを確認」について
情報システムの運用継続を脅かす非常時においては、非常時の情報セキュリティに係る対策事項を整備した際には想定していなかった様々な不整合が発生し、整備した対策事項が有効に機能しないことも考えられる。このため、非常時の対策事項を定期的に見直し、課題を発見した場合は改善することが重要である。
なお、情報システムの運用継続計画の教育訓練を行う際は、非常時の対策事項

の理解と対応能力の向上の他、対策事項の有効性の確認も目的とすることが望ましい。

第十一章　情報システムのセキュリティ機能

第一節　主体認証機能

解説：情報又は情報システムへのアクセス可能な主体を制限するためには、主体認証機能の導入が必要である。その際、アクセス権限のある主体へのなりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講ずることが重要となる。

また、本学の情報システムにおいて、一般利用者向けのサービスを提供する場合は、国民が情報システムへのアクセスの主体となることにも留意して、主体認証情報を適切に保護しなければならない。

C2101-97　（主体認証機能の導入）（政府機関統一基準の対応項番 6.1.1(1)）

第九十七条　部局技術責任者は、情報システムや情報へのアクセスを管理するため、主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けること。

２　部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。

解説：第１項「識別」について

識別のための機能が実装されていない情報システムにおいて主体認証を行う場合（例えば、識別コード自体が存在せず、主体認証情報の検証のみで主体認証を行う場合）は、例外措置として判断し、主体を識別しないことによる影響について勘案し、必要に応じて代替又は追加の措置を講ずる必要がある。

第２項「主体認証」について

情報セキュリティ水準と情報システムの利便性等を考慮し、主体認証機能の運用に係る以下の要件の実装要否を情報システムの導入時に考慮するとよい。

・正当な主体以外の主体認証を受諾しないこと。（誤認の防止）

・正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。（誤否の防止）

・正当な主体が容易に他の主体に主体認証情報の付与（発行、更新及び変更を含む。以下この項において同じ。）及び貸与ができないこと。（代理の防止）

・主体認証情報が容易に複製できないこと。（複製の防止）

・部局技術責任者の判断により、ログインを個々に無効化できる手段があること。（無効化の確保）

・必要時に中断することなく主体認証が可能であること。（可用性の確保）

・新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）

・主体に付与した主体認証情報を利用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保）

加えて、主体認証を行う情報システムにおいて、情報セキュリティ強度の更なる向上を図るため、多要素主体認証の導入など、以下を例とする機能を設けることを検討することが重要である。

	機能	解説
①	多要素主体認証方式で主体認証を行う機能	複数要素の主体認証方式を組み合わせて、単一の主体認証方式よりも強固な主体認証を行う機能を指す。一般に、異なる認証方式を組み合わせた方が、強度が高くなる。 多要素主体認証方式であれば、仮に一つの主体認証情報が露呈してしまっても、残りの主体認証情報が露呈しない限り、不正にログインされる可能性は低いと考えられる。 また、通常の運用時は単一の主体認証を実施するが、認証の要求時に、アクセス元の IP アドレス、アクセスする時間帯、位置情報等が通常のアクセスとは異なる特徴が確認された場合は、不正ログインのリスクが高まったと判断して多要素主体認証を行う方法も考えられる。
②	前回のログインに関する情報を通知する機能	主体ごとに割り当てられた識別コードに対して、前回のログインに関する情報（日時や装置名等）を、次回のログイン時等のタイミングで主体に通知する機能を指す。 正当な主体以外の者が主体に割り当てられた識別コードを使用して不正にログインした場合に、正当な主体がそれを検知することができるようになると考えられる。
③	不正にログインしようとする行為を検知又は防止する機能	特定の識別コードによるログインにおいて、指定回数以上の主体認証情報の誤入力が検知された場合に、その旨を正当な主体や情報システムの運用担当者等に通知し、一定期間当該端末（又は識別コード）からのログイン操作受付を停止する機能を指す。 当該識別コードによる情報システムへの以後のログインを無効にすることも考えられる。 この機能により、不正なログインの試行の有無等について、正当な主体や情報システムの運用担当者等がその状況を確認するとともに、一定程度不正ログイン等を防止することができる。
④	情報システムへのログイン時にメッセージを表示する機能	情報システムへのログインの際に、軽率に不正アクセスに及ぶ行為を抑止する効果が期待されるメッセージを画面に表示する機能を指す。 通知メッセージとして、以下の例が考えられる。 ・アクセス履歴が管理者に通知されること ・利用状況を監視、記録しており、監査対象となること ・情報の目的外利用は禁止されていること ・情報システムへの不正アクセス行為は禁止されており、不正アクセス禁止法の罰則対象となること
⑤	主体認証情報の変更の際に、以前に設定した主体認証情報の再設定を防止する機能	利用者に対して主体認証情報の定期的な変更を求める場合に、以前に設定した主体認証情報と同じものを再設定することを防止する機能を指す。 利用者に主体認証情報の定期的な変更を求める必要がある情報システムを対象としたものであり、利用者が以前に設定した主体認証情報と同じものを再設定すると、変更によってもたらされる効果が損なわれることから、変更履歴の世代管理を行い、何世代か前までの主体認証情報を再設定することを防止する方法が考えられる。 「（解説）第九十九条第１項「利用者に主体認証情報の定期的な変更を求める場合」について」も参照。

⑥	管理者権限によるログインの際に個別の識別コードによりログインすることを併せて求める機能	管理者権限を有する共有識別コードの利用において、実際の作業者となる個別の識別コードによるログインを併せて行うことを求める機能を指す。 管理者権限を有する共有識別コードのログイン記録だけでは、実際に作業をした管理者を個人単位で特定することが困難となるため、作業者個別の識別コードによるログインを行った後に管理者権限を有する共用識別コードによるログインを許可するものである。 例えば、当該情報システムの OS が Unix 系の場合には、一般利用者でログインした後に su コマンドで root に切り替えるという手順により、これを達成できる。また、その場合には、root によるログインを禁止する設定により、その手順を強制することができる。

C2101-98　（主体認証に係る対策）（政府機関統一基準の対応項番 6.1.1(1)-1,2）

第九十八条　部局技術責任者は、主体認証は、以下を例とする主体認証方式を決定すること。

一　知識（パスワード等、利用者本人のみが知り得る情報）による認証

二　所有（電子証明書を格納する IC カード又はワンタイムパスワード生成器等、利用者本人のみが所有する機器等）による認証

三　生体（指紋や静脈等、本人の生体的な特徴）による認証

２　部局技術責任者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、文字の種類や組合せ、桁数等のパスワード設定条件を利用者に守らせる機能を設けること。

解説：第１項第１号「知識」について

端末によっては、例えばパスワード以外にも、自分のみが知る「パターン」を主体認証情報として扱うケースがあるが、これも「知識」に分類される。

第１項第２号「所有」について

「所有」による認証の例として、本学が提供する利用者認証基盤における電子証明書を用いた認証、職員証や学生証といった IC カードを用いた認証等が挙げられる。

第１項第３号「生体」について

生体情報による主体認証を用いる場合には、その導入前に、この方式特有の他人受入率（本人を他人と誤って認証してしまう確率）と本人拒否率（本人の認証が受け入れられない確率）の課題があることを考慮して情報システムを設計する必要がある。

C2101-99　（不正行為を防止するための措置）（政府機関統一基準の対応項番 6.1.1(1)-3,4,5）

第九十九条　部局技術責任者は、主体認証を行う情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下の機能を設けること。

一　利用者が定期的に変更しているか否かを確認する機能

二　利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

２　部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下を例とする方法を用いて適切に管理すること。

一　主体認証情報を送信又は保存する場合には、その内容を暗号化する。
二　主体認証情報に対するアクセス制限を設ける。
3　部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に利用され、又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設けること。
一　当該主体認証情報及び対応する識別コードの利用を停止する機能
二　主体認証情報の再設定を利用者に要求する機能解説：第１項「利用者に主体認証情報の定期的な変更を求める場合」について
利用者に主体認証情報の定期的な変更を求めることの情報セキュリティ上の効果は、主体認証情報の運用方法や情報システムの認証技術の方式により異なるものであり、また、生体情報による主体認証方式のように利用者本人でも変更が不可能なものもある。定期的な変更に一定の効果がある場合、変更を求める間隔が短いほど効果は高まることになるが、変更を強制する頻度が高すぎれば、利用者の利便性を著しく低下させ、利用者が強度の低い安易なパスワードを設定しやすくなるなど、結果的に主体認証機能の安全性を低下させて逆効果をもたらし得る。
したがって、利用者に主体認証情報の定期的な変更を求めるか否かは、その効果と逆効果を総合的に検討した上で判断する必要がある。
なお、識別コード自体が存在せず、主体認証情報を複数の主体で共用せざるを得ない機器等の利用においては、例えば、人事異動等で利用者に変更が生じた際に利用者に主体認証情報の変更を求めるなどして、主体認証情報の漏えいによる不正行為を防止することが考えられる。

C2101-100　（識別コード及び主体認証情報の管理）（政府機関統一基準の対応項番 6.1.1(2)）
第百条　部局技術責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。
2　部局技術責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。
解説：第１項「主体認証情報を適切に付与」について
情報システムにおいて認証機能を統合している場合、各機器等の管理者権限を持つローカルアカウントは通常の運用では未使用となるが、その場合においてもデフォルトパスワードのままにせず、設定するパスワードについても同一の値にしないといった措置を講ずる必要がある。
なお、主体認証が必要となる場面が多岐にわたるような情報システムの場合、認証連携を適切に用いることにより、業務の効率化を図ることも考えられる。

C2101-101　（識別コード及び主体認証情報の管理に係る対策）（政府機関統一基準の対応項番 6.1.1(2)）
第百一条　部局技術責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）すること。
2　部局技術責任者は、識別コードの付与に当たっては、以下を例とする措置を講ずること。
一　単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）

を別の主体に対して付与することの禁止

二　主体への識別コードの付与に関する記録を消去する場合の部局総括責任者からの事前の許可

3　部局技術責任者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること。

4　部局技術責任者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。

5　部局技術責任者は、知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促すこと。

6　部局技術責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、部局技術責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。

7　部局技術責任者は、主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、以下を例とする措置を講ずること。

一　当該主体の識別コードを無効にする。

二　当該主体に交付した主体認証情報格納装置を返還させる。

三　無効化した識別コードを他の主体に新たに発行することを禁止する。

解説：第３項「安全な方法で主体認証情報を配布する」について

利用者以外の者（情報システムの管理者等）が主体認証情報を設定する場合には、以下を例とする方法で、当該主体認証情報を安全な方法で利用者に配布する必要がある。

・本人の電子メールアドレスに対し、必要に応じて、暗号化を施すことにより、主体認証情報を送付する。この際、暗号化された主体認証情報が添付された電子メールに復号するための鍵を同時に付すのは情報セキュリティ上、好ましくない。

・本人の電子メールアドレスに対して主体認証情報を入手するためのウェブサイト及びパスワードを送付し、当該パスワードによる認証の上で当該ウェブサイトから主体認証情報をダウンロードする。

・本人の住所に対して主体認証情報を運搬する。

第５項「他の情報システムで利用している主体認証情報を設定しない」について

複数の情報システムにおいて共通の主体認証情報を設定していた場合、ある情報システムから漏えいした主体認証情報が他の情報システムで不正に利用されるというリスクが発生する。本学の管理下にない情報システムからの漏えいを防止することは不可能であるため、このような情報システムから主体認証情報が漏えいした場合の本学の情報システムへの影響について考慮しておく必要がある。対策の例としては、他の情報システムで利用している主体認証情報を本学の情報システムに設定しないよう注意喚起を表示する、識別コードを情報シ

ステム側で割り当てることで識別コードの共通利用を防止する、といった方法が考えられる。

第６項「共用識別コードを付与する必要がある場合」について
共用識別コードは、その利用履歴だけでは利用者を特定できないため、情報セキュリティインシデントが発生した場合に、真相究明の支障となる可能性がある。この点を踏まえ、やむを得ず、共用識別コードを利用する場合には、利用者を特定するための以下を例とする仕組みを講ずる必要がある。
・当該情報システムにおける別途の認証手段を併用する
・入退室管理装置等の物理的認証手段を併用する

第７項第１号「識別コードを無効にする」について
識別コードの付与を最小限に維持するため、退職等により不必要となった識別コードについては、これを無効にする必要がある。また、本人からの届出による場合のほか、人事異動等の時期を考慮の上、定期的及び必要に応じて不要な識別コードが存在しないことを確認することにより、無効化漏れを防止することが期待できる。

第一節の二　アカウント管理

C2101-102　（アカウント管理手続の整備）

第百二条　部局技術責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理について、以下の事項を含む手続を定めること。

一　主体からの申請に基づいてアカウント管理を行う場合には、その申請者が正当な主体であることを確認するための手続

二　主体認証情報の初期配布方法及び変更管理手続

三　アクセス制御の設定方法及び変更管理手続

解説：情報システムへアクセスする主体に対して、識別コード及び主体認証情報を付与する際の関連手続を明確に定めることを求める事項である。また、情報システムへアクセスする主体ごとに、確実にアクセス制御を設定するため、関連手続を明確に定めることを求める事項である。
アカウントの管理においては、アカウントの発行及び削除の手続き並びに違反行為を発見した場合のアカウントの停止及び復帰の手続き等を定める。利用者から見たアカウント申請手続きについては「C2201 情報システム利用規程」において定める。

２　部局技術責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理を行う者を定めること。

解説：アカウントの管理については、情報システムのセキュリティ保護上、非常に重要な役割を果たすため、アカウント管理を行う者を定め、厳格な運用を求める事項である。
アカウント管理を行う者は、例えば、部局において広く利用される情報システ

ムにおいては部局技術担当者が相当である。ただし、ウェブページや個人 PC など、アカウント管理の場面は広く考えられるため、その場合は、部局技術責任者が適宜アカウント管理を行う者を定めるものとする。

C2101-103　（共用識別コード）

第百三条　部局技術責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、共用識別コードの利用許可については、情報システムごとにその必要性を判断すること。

解説：原則として、識別コードは、情報システムへアクセスする主体へ個別に付与することになる。しかしながら、情報システム上の制約や利用状況などを考慮して、１つの識別コードを複数の主体で共用する必要がある場合には、当該情報システムごとに利用許可の判断をすることを求める事項である。

共用識別コードを利用できるのは、部局技術責任者がその利用を認めた情報システムに限られることに注意すること。

C2101-104　（アカウントの発行）

第百四条　アカウント管理を行う者は、利用者等からのアカウント発行申請を受理したときは、申請者が第九条第二項第三号による処分期間中である場合を除き、遅滞無くアカウントを発行すること。

３　アカウント管理を行う者は、アカウントを発行するにあたっては、期限付きの仮パスワードを発行する等の措置を講じることが望ましい。

C2101-105　（アカウント発行の報告）

第百五条　アカウント管理を行う者は、アカウントを発行したときは、速やかにその旨を部局総括責任者に報告すること。

２　全学総括責任者は、必要により部局総括担当者にアカウント発行の報告を求めることができる。

C2101-106　（アカウントの有効性検証）

第百六条　アカウント管理を行う者は、発行済のアカウントについて、次号に掲げる項目を一か月毎に確認すること。

一　利用資格を失ったもの

二　部局総括責任者が指定する削除保留期限を過ぎたもの

三　パスワード手順に違反したパスワードが設定されているもの

四　六か月以上使用されていないもの

２　アカウント管理を行う者は、入学や卒業、人事異動等、アカウントを追加又は削除する時に、不適切なアクセス制御設定の有無を点検すること。

解説：利用者によるパスワードの取り扱いについては、「C2201 情報システム利用規程」や「C3205 利用者パスワードガイドライン」に定める。ただし、管理者の側面から、例えば辞書にある単語はパスワードに指定できないような仕掛けを組み入れたり、六か月間パスワードを変更しないときは警告する等の規定を盛り込むことも考えられる。

C2101-107　（アカウントの削除）

第百七条　アカウント管理を行う者は、第百条第一項第一号及び第二号に該当するアカウントを発見したとき、又は第九条第二項第三号による削除命令を受けたときは、速やかにそのアカウントを削除し、その旨を部局総括責任者に報告すること。

２　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等のアカウントを削除し、その旨を部局総括責任者に報告すること。

３　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等に交付した主体認証情報格納装置を返還させ、その旨を部局総括責任者に報告すること。

４　部局総括責任者は、第一項乃至第三項の報告を受けたときは、速やかにその旨を利用者等に通知すること。ただし、電話、郵便等の伝達手段によっても通知ができない場合はこの限りでない。

５　全学総括責任者は、必要により部局総括責任者にアカウント削除の報告を求めることができる。

C2101-108　（アカウントの停止）

第百八条　アカウント管理を行う者は、第百条第一項第三号及び第四号に該当するアカウントを発見したとき、第九条第二項第三号よる停止命令を受けたとき、又は主体認証情報が他者に使用され若しくはその危険が発生したことの報告を受けたときは、速やかにそのアカウントを停止し、その旨を部局総括責任者に報告すること。

２　部局総括責任者は、前項の措置の報告を受けたときは、速やかにその旨を利用者等に通知すること。ただし、電話、郵便等の伝達手段によっても通知ができない場合はこの限りでない。

３　全学総括責任者は、必要により部局総括責任者にアカウント停止の報告を求めることができる。

C2101-109　（アカウントの復帰）

第百九条　アカウントの停止を受けた利用者等がアカウント停止からの復帰を希望するときは、その旨を部局総括責任者に申し出させること。

２　部局総括責任者は、前項の申し出を受けたときは、アカウント管理を行う者に当該アカウントの安全性の確認及びアカウントの復帰を指示すること。

３　アカウント管理を行う者は、前項の指示に従い当該アカウントの安全性を確認した後、速やかにアカウントを復帰させること。

C2101-110　（管理者権限を持つアカウントの利用）

第百十条　管理者権限を持つアカウントを付与された者は、管理者としての業務遂行時に限定して、当該アカウントを利用すること。

解説：管理者権限を持つアカウントを管理者としての業務遂行時に限定して、利用することを求める事項である。

例えば、情報システムのオペレーションシステムが Windows であれば、

Administrator 権限を付与された場合であって、PC の設定変更などをしないときには、Administrator 権限なしのアカウントを使用し、設定変更をするときにだけ Administrator 権限で再ログインすることを遵守しなければならない。Windows のユーザーアカウント制御（UAC : User Account Coltrol）機能により管理者権限でプログラムの実行を行う場合も、管理者権限を持つアカウントの利用に該当すると考える。
なお、この遵守事項は、実際には繁雑な操作を必要とする場合があるため、最小限の特権機能が設けられている場合は、これを遵守するべきであるが、当該の情報システムで取り扱う情報の重要性などを勘案し、必要に応じて遵守事項として本条を選択されたい。

C2101-111　（主体認証情報の変更、アカウントの失効）
第百十一条　部局総括責任者は、情報セキュリティインシデント又はその可能性が認められる場合、主体認証情報の変更を求め又はアカウントを失効させることができる。

C2101-112　（無権限のアクセス行為の対策）
第百十二条　部局技術責任者及び部局技術担当者は、無権限のアクセス行為を発見した場合は、速やかに部局総括責任者に報告すること。部局総括責任者は、上記の報告を受けたときは、遅滞なく全学総括責任者にその旨を報告すること。
２　全学総括責任者及び部局総括責任者は、前項の報告を受けた場合は、新たな防止対策等必要な措置を講じること。

第二節　アクセス制御機能

解説：アクセス制御とは、情報システム及び情報へのアクセスを許可する主体を制限することである。複数の主体が情報システムを利用する場合、当該情報システムにおいて取り扱う情報へのアクセスを業務上必要な主体のみに限定することによって、情報漏えい等のリスクを軽減することができると考えられる。

C2101-113　（アクセス制御機能の導入）（政府機関統一基準の対応項番 6.1.2(1)）
第百十三条　部局技術責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。
２　部局技術責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。

C2101-114　（アクセス制御に係る対策）（政府機関統一基準の対応項番 6.1.2(1)-1）
第百十四条　部局技術責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、必要に応じて、以下を例とするアクセス制御機能の要件を定めること。
一　利用時間や利用時間帯によるアクセス制御
二　同一主体による複数アクセスの制限
三　IP アドレスによる端末の制限

四　ネットワークセグメントの分割によるアクセス制御

解説：第１号「主体の属性、アクセス対象の属性に基づくアクセス制御」について
具体的な手法としては、端末や共有フォルダ上のファイルやフォルダ（ディレクトリ）に対する許可属性のリストであるアクセス制御リスト（ACL： Access Control List）が挙げられる。ACL では例えば、アクセス対象の所有者／所有者の属するグループ／全利用者といったアクセス主体に対して、読み取り／書き込み／実行の権限を設定する。
ただし、一般的な情報システムでは、利用者が適切なアクセス制御の設定を行っても、システムの管理者は全てのファイルやフォルダへアクセス可能である。実際に、運用保守の担当者が、管理者権限相当のアクセス権限を行使して、機密性の高い情報を不正に閲覧するといった事案も確認されている。そのため、アクセス対象が要機密情報等の場合は、アクセス制御機能のみに頼らず、アクセス権限の無い者に閲覧等されないよう、アクセス制限の対象に対して暗号化等の措置を考慮することが求められる。

第４項「ネットワークセグメントの分割によるアクセス制御」について
業務や取り扱う情報の性質・量に応じて、重要な情報に攻撃が到達しないよう、情報システムの重要な情報を取り扱う部分を他の情報システムやインターネットから分離するといった対策をとる必要がある。特に、情報システムの管理を行う部分を独立したセグメントとし、これをインターネットから切り離しておくことは、攻撃の拡大阻止の観点から有効である。同時に、セグメント分割の意義を損なうことのないよう、各システムで取り扱うことができる情報についてルール化し、職員に徹底することも重要である。
なお、第七十六条において、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否について判断を求めているが、本条は、その際に併せて検討し、情報システムのネットワーク構成の要件を決定するとよい。

第三節　権限の管理

解説：重要システムのアクセス制御機能を適切に運用するためには、主体から対象に対するアクセスの権限を適切に設定することが必要である。権限の管理が不適切になると、情報又は情報システムへ不正アクセスされるおそれが生じる。
また、情報システムの管理機能として、一般的に管理者権限にはあらゆる操作が許可される特権が付与されている。当該特権が悪意ある第三者等に入手された場合、主体認証情報等の漏えい、改ざん又は情報システムに係る設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念されることから、限られた主体のみに管理者権限が付与されることが重要である。

C2101-115　（権限の管理）（政府機関統一基準の対応項番 6.1.3(1)）
第百十五条　部局技術責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、

措置を講ずること。

２　部局技術責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

解説：第２号「内部からの不正操作や誤操作を防止するための措置」について

権限管理を行う情報システムのうち、内部からの不正操作や誤操作を防ぐための特に強固な権限管理が必要な情報システムについては、ある処理に対し、複数名による主体認証操作がなければ、その処理自体を完遂できない「デュアルロック機能」を導入することが考えられる。

その他の情報システムについては、操作ログを取得したり、確認画面を表示したりするなどの措置が考えられる。

C2101-116　（権限管理に係る対策）（政府機関統一基準の対応項番 6.1.3(1)-1）

第百十六条　部局技術責任者は、権限管理を行う情報システムにおいて、以下を含めた機能を導入すること。

一　業務上必要な場合に限定する

一　必要最小限の権限のみ付与

二　管理者権限を行使できる端末をシステム管理者等の専用の端末とする

解説：第１号「必要最小限の権限のみ付与」について

管理者権限等の特権は、システム全体へのアクセス権を持ち、あらゆる操作が可能であることが多く、仮に不正な目的を有する悪意ある第三者等が当該権限を入手すれば、当該システムに対して不正な操作が可能となってしまう。必要最小限の権限のみ付与とは、特権が利用できる時間的な機会を限定すること又はあらかじめ限られた操作が可能な特権を付与することにより、当該特権を使った不正な操作が発生する機会を減らし、結果的に安全性を強化するものである。

例えば、管理作業をするときに限定してその識別コードを利用することを可能とする方式（例 Unix 系システムにおける sudo 等）や、あらかじめ実行できるプログラムやアクセス可能な領域を限定し、特権を付与する方式がある。

第四節　ログの取得・管理

解説：情報システムにおけるログとは、システムの動作履歴、利用者のアクセス履歴、通信履歴その他運用管理等に必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の情報セキュリティインシデント及びその予兆を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

C2101-117　（ログの取得・管理）（政府機関統一基準の対応項番 6.1.4(1)）

第百十七条　部局技術責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。

２　部局技術責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。

３　部局技術責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

解説：第２項「ログを取得する目的」について

情報システムにおいて出力できる様々なログは、その全てを無期限に保存し、定期的にその点検や分析を行うことができれば理想的であるが、そのためには莫大なストレージ容量が必要になり、解析にかかる時間も長くなるなど、現実的ではない。

そのため、情報システムの特性（取り扱われる情報、接続されるネットワーク、設置環境、利用者等）に応じ、当該情報システムでどのような事象を検知すべきかを目的として設定した上で、取得すべきログ情報やその保存期間等を検討することが望ましい。

例えば、標的型攻撃の早期発見・初期調査を目的とした場合には、以下のようなログを取得することが考えられる。

・電子メールサーバ： 電子メールクライアントで表示される表記名*、送信者アドレス*、実際の電子メール送信者アドレス*、添付ファイル名*

・ファイアウォール： ファイアウォールポリシーのアクション、送信先のゾーン設定*、送信元アドレス、送信元ポート、送信先アドレス、送信先ポート

・Web プロキシサーバ： URL アドレス、送信先サイトのポート、メソッド、UserAgent*、アクセス時間

・DNS キャッシュサーバ： 名前解決を行おうとしている PC 等の IP アドレス*、要求及び応答したホストや IP アドレスの情報*

・認証サーバ（Active Directory）： 資格認証の確認の監査*、Kerberos 認証サービスの監査*、ログオンの監査*、その他ログオン／ログオフイベントの監査*、特殊なログオンの監査*

なお、上記のログの例において、項目名の終わりに*を付与しているログ項目は各機器の標準設定では出力されない場合があるため、注意が必要である。

第２項「保存期間」について

保存期間については、情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。

なお、ログの長期保存にはコストがかかるため、費用を抑える観点から、直近のログはすぐに調査可能なハードディスク等のオンラインの電磁的記録媒体に保存し、それ以降はテープや光ディスク等の長期保存に適した外部電磁的記録媒体に保存する方法も考えられる。オンラインの電磁的記録媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する。

第２項「ログが取得できなくなった場合の対処方法」について
以下を例とする対処方法が考えられる。
・古いログに上書きする設定を施し、ログの取得を継続する。
・ログが取得できなくなった際に出力されているメッセージ、エラーコード等を確認し、障害の原因を特定すると同時に当該障害の原因の対処を実施する。
なお、情報システムにおいて、事前に収集したログのバックアップ設定を行っている場合は、復旧手順に従い、速やかにログを復旧させる。このとき、復旧するバックアップの古さの目標値を示す RPO（Recovery Point Objective）は情報システムの特性及び取り扱う情報によって、適切に設定する必要がある。
・あらかじめ用意したファイル容量を使い切った場合、情報システムに対する挙動がログに保存されないため、一旦情報システムを停止し、ファイル容量を新たに用意するなどした後に、ログの取得を再開する。

第３項「点検又は分析」について
情報システムの特性等に応じて、点検・分析の頻度や分析の精度を高める必要がある場合には、専任の分析担当者の設置や監視事業者への委託を検討することが考えられる。

C2101-118　（ログの取得に係る対策）（政府機関統一基準の対応項番 6.1.4(1)-1）
第百十八条　部局技術責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。

解説：「時刻を同期」について
具体的な実装例としては、ログを取得する機器のシステム時刻を、タイムサーバを用いて同期する方法がある。タイムサーバは、NTP（Network Time Protocol）や SNTP（Simple Network Time Protocol）等の方式により、ネットワーク上のクライアント機器に対して、時刻を提供する。例えば、公開 NTP サービスを用いる方式や組織内にタイムサーバを設置し、サーバ装置・端末・通信回線装置をタイムサーバに時刻同期するよう設定する方式が挙げられる。
なお、後者については、タイムサーバを複数利用することにより、時刻の精度や冗長性を高めることができる。
また、機器によっては明示的に設定を行わないとログに出力する時刻が現地時間とならない場合があるため注意が必要である。

C2101-119　（ログの管理に係る対策）（政府機関統一基準の対応項番 6.1.4(1)-2,3,4,5）

第百十九条　部局技術責任者は、所管する情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理すること。

一　事象の主体（人物又は機器等）を示す識別コード
二　識別コードの発行等の管理記録
三　利用者による情報システムの操作記録
四　事象の種類
五　事象の対象
六　正確な日付及び時刻
七　試みられたアクセスに関わる情報
八　電子メールのヘッダ情報及び送信内容
九　通信パケットの内容
十　操作する者、監視する者、保守する者等への通知の内容

２　部局技術責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。

３　部局技術責任者は、ログが取得できなくなった場合の対処方法を定めること。

解説：第１項第４号「事象の種類」について

事象の種類の例を以下に示す。

・ウェブサイトへのアクセス
・ログイン及びログアウト
・サーバ、ファイルへのアクセス
・要保護情報の書き出し
・アプリケーションの起動及び終了
・特定の操作指令

第１項第５号「事象の対象」について

事象の対象の例を以下に示す。

・アクセスした URL
・ログインしたアプリケーション名
・アクセスしたファイル名及びファイル内容
・起動及び終了したアプリケーション名
・特定の操作指令の対象

第２項「ログ情報の保全方法」について

取得したログ情報に対する不正な消去、改ざん及びアクセスを防止するためのログ情報の保全方法として、以下の例が考えられる。

・ログ収集サーバにログを転送し保存する。ログ収集サーバの管理者を他のサーバ等の管理者と異なる者とし、他の管理者によるログ情報の消去や改ざんが行われないようにする。
・ログをテープ等の外部電磁的記録媒体に書き出し、情報システムから切り離して保管する。

・ログを書き換え不能な外部電磁的記録媒体（DVD-R 等）に書き出して保管する。

C2101-120　（ログの分析・点検に係る対策）（政府機関統一基準の対応項番 6.1.4(1)-6）

第百二十条　部局技術責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入すること。

一　ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化

解説：第１号「自動化」について

ログとして取得する項目数、利用者数等が多くなるにつれて、ログの量は膨大になり、システム担当者等がログを目視することによって問題（又はその予兆）を検出するのは、困難を極める。システム自体に実装される機能や各種運用管理ツールを組み合わせ、ログの点検・分析・通知が自動的に実行されるなど、ログ管理作業を支援する仕組みを構築することが望ましい。

第四節の二　通信の監視

解説：ログは、情報システムにおいて情報セキュリティインシデントが発生した場合に、誰がいつ何をしたかを特定し原因を明らかにするためのものであり、以下を主たる対象とする。

・ID の発行等の管理履歴
・各 ID へのアクセス許可設定の管理履歴
・それらの権限管理者の許認可そのものの管理履歴

これらは、ログ管理のための最低必要条件となる。なお、ログ管理の強度を上げるために、サンプル規程集では「通信の監視記録」や「利用記録」を採取する手続きを本節において定めている。

「通信の監視記録」には、通信の主体及び客体の情報、通信の種類、日付及び時刻、通信内容、通信パケット内容をも含む。「利用記録」は、利用者が情報システムにおいてどのような振る舞いをしたかを記録するものである。

C2101-121　（通信の監視）

第百二十一条　情報システムを運用・管理する者及び利用者等は、ネットワークを通じて行われる通信を傍受してはならない。ただし、全学総括責任者又は当該ネットワークを管理する部局総括責任者は、セキュリティ確保のため、あらかじめ指定した者に、ネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

２　全学総括責任者又は部局総括責任者は、監視の範囲をあらかじめ具体的に定めておかなければならない。ただし、不正アクセス行為又はこれに類する重大なセキュリティ侵害に対処するために特に必要と認められる場合、全学総括責任者又は部局総括責任者は、セキュリティ侵害の緊急性、内容及び程度に応じて、対処のために不可欠と認められる情報について、監視を行うよう命ずることができる。

３　監視を行う者は、監視によって知った通信の内容又は個人情報を、他の者に伝達してはなら

ない。ただし、前項ただし書きに定める情報については、全学総括責任者並びに部局総括責任者、及び、全学情報システム運用委員会並びに部局情報システム運用委員会に伝達することができる。

4　監視によって採取された記録（以下「監視記録」という。）は要機密情報、要保全情報、要安定情報とし、監視を行わせる者を情報の作成者とする。

5　監視を行わせる者は、監視を行う者に対して、監視記録を保存する期間をあらかじめ指示するものとする。監視を行う者は、指示された期間を経過した監視記録を直ちに破棄しなければならない。ただし、監視記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

6　監視を行う者及び監視記録の伝達を受けた者は、ネットワーク運用・管理のために必要な限りで、これを閲覧し、かつ、保存することができる。監視記録を不必要に閲覧してはならない。不必要となった監視記録は、直ちに破棄しなければならない。監視記録の内容を、法令に基づく場合等を除き、他の者に伝達してはならない。

解説：ネットワーク上の通信は傍受してはならないというのが原則であるが、運用上の理由により、限定的に通信の監視を行う場合があるということを明記しておく。「C2101 情報システム運用・管理規程」において、どのような場合に誰に何をさせ何をさせないかを定めるとともに、「C2201 情報システム利用規程」においても、禁止事項の中に通信の傍受を組み込むべきである。

なお、本条文においては、犯罪捜査のための通信傍受に関する法律（いわゆる通信傍受法）を過度に連想しないよう、規程に基づいて行われる行為を「通信の監視」として記述を工夫している。通信の監視には、トラフィックの監視・ネットワーク状況の把握・データ流通に異常がないかの監視、のみならず、ここではパケットの中身を見ることまでを想定している。

本学情報ネットワークにおける利用者等の通信の秘密は尊重されるべきであるが、ネットワークの円滑な運用のため、必要最小限の範囲において通信ログを保存・調査する場合がある。また、本学情報ネットワークの運用においては、表現の自由とプライバシーに最大限配慮するが、第三者に対する誹謗中傷や名誉毀損、著作権侵害等と判断されるコンテンツを制限する場合がある。「C2101 情報システム運用・管理規程」の策定にあたっては、これらのことに十分配慮するとともに、「C2201 情報システム利用規程」を通じて、利用者等に対して一定の制約を課す。

部局技術責任者及び部局技術担当者並びに利用者等は、本学情報ネットワーク全体の円滑な運用のため、協力する義務がある。

利用者等は、契約等により本学情報ネットワークを利用する権利を有するが、その利用に伴うすべての行動について責任を自覚しなければならない。本学情報ネットワークを利用した情報発信は本学内にとどまらず、社会へひろく伝達される可能性があることを自覚し法令遵守等、責任をもった行動が望まれる。また、目的に示す基本理念を大きく逸脱するような私的利用や商業利用は制限される。「C2101 情報システム運用・管理規程」及び「C2201 情報システム利用規程」を策定する際は、これらのことを配慮して策定する。

情報システム運用委員会が実施する教育を受講し内容を十分理解の上、所定の手続きをとり本方針等の遵守を承諾した者に本学情報ネットワークを利用する許可（アカウント等）が与えられる。
利用者等が、本学情報ネットワークに接続する機器を持ち込み使用する場合は、別途定める基準に従うものとする。

C2101-122　（利用記録）

第百二十二条　複数の者が利用する情報機器を管理する部局技術担当者（以下「当該情報機器の管理者」という。）は、当該機器に係る利用記録（以下「利用記録」という。）をあらかじめ定めた目的の範囲でのみ取得することができる。当該目的との関連で必要性の認められない利用記録を取得することはできない。

２　前項に規定する目的は、法令の遵守、情報セキュリティの確保、課金その他当該情報機器の利用に必要なものに限られる。個人情報の取得を目的とすることはできない。

３　利用記録は要機密情報、要保全情報とし、当該情報機器の管理者を情報の作成者とする。

４　当該情報機器の管理者は、第一項の目的のために必要な限りで、利用記録を閲覧することができる。他人の個人情報及び通信内容を不必要に閲覧してはならない。

５　当該情報機器の管理者は、第二項に規定する目的のために必要な限りで、利用記録を他の者に伝達することができる。

６　当該情報機器の管理者は、第二項の目的、これによって取得しようとする利用記録の範囲及び前項により利用記録を伝達する者を、あらかじめ部局総括責任者に申告し、かつ、当該機器の利用者等に開示しなければならない。部局総括責任者は、申告の内容を不適切と認めるときは、これを修正させるものとする。

７　当該情報機器の管理者又は利用記録の伝達を受けた者は、第一項の目的のために必要な限りで、これを保有することができる。不要となった利用記録は、直ちに破棄しなければならない。ただし、当該情報機器の管理者は、利用記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

C2101-123　（個人情報の取得と管理）

第百二十三条　電子的に個人情報の提供を求めようとする者は、提供を求める情報の範囲、利用の目的、その情報が伝達される範囲を、あらかじめ相手方に示さなければならない。

２　前項の個人情報は、当人の請求により開示、訂正又は削除をしなければならない。また、そのための手続を示さなければならない。

解説：個人情報保護は、情報システムに限られるものではない。学内に既に個人情報保護規程が存在する場合は、そちらを参照することとして、本条を削除する考え方もある。

C2101-124　（利用者等が保有する情報の保護）

第百二十四条　複数の者が利用する情報機器を管理する部局技術担当者は、利用者等が保有する情報をネットワーク運用に不可欠な範囲又は情報セキュリティインシデントへの対処に不可欠な範囲において、閲覧、複製又は提供することができる。

解説：ネットワークの監視や利用記録の取得が、あらかじめそれぞれの条文に定められた目的や範囲に限定されるのと同様に、利用者等が保有する情報の閲覧等についても範囲を限定しておく必要がある。ここでは、例えば、不正アクセス行為又は重大なセキュリティ侵害があった場合に利用者等のメール本文を閲覧する行為、利用者等の実行したプログラムにより重大なシステム障害が発生した場合に当該プログラムやプログラムデータを閲覧する行為等が考えられる。事件があったときはメール本文を閲覧する必要もあるだろうが、手続きや範囲については「C3102 インシデント対応手順」に明確に定めておく必要がある。
個人情報の取り扱いに関しては前条に定めがあるが、個人情報が含まれているかどうかはメール本文を閲覧してみないとわからない場合も多い。閲覧等によって得られた情報の削除の手続きについても、あらかじめ定めておくべきである。

第五節　暗号・電子署名

解説：情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。
暗号化機能及び電子署名機能を導入する際は、使用するアルゴリズムに加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズムが危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

C2101-125　（暗号化機能・電子署名機能の導入）（政府機関統一基準の対応項番 6.1.5(1)）

第百二十五条　部局技術責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。

一　要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

二　要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

２　部局技術責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

一　利用者等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

二　情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

三　暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

四　暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

3　部局技術責任者は、本学における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を UPKI 電子証明書発行サービスが発行している場合は、それを使用するように定めること。

解説：第２項第２号「やむを得ない場合」について

情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用することが原則であるが、連携する他の情報システム側で対応していないなどの場合も想定される。このような場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズム以外のものを採用することもやむを得ないと考えられるが、「推奨候補暗号リスト」や「運用監視暗号リスト」を参照の上、安全性が高いアルゴリズムを採用することが必要である。

第２項第３号「アルゴリズムが危殆化」について

暗号化や電子署名に用いられる暗号アルゴリズムは、年月が経つにつれ、情報システムの処理能力の向上や新たな暗号解読技法の考案等によって、アルゴリズム設計当初の強度を失い、結果として、安全性を保てなくなる。このことを一般に「アルゴリズムが危殆化する」という。

暗号アルゴリズムの強度には理論上の強度及び実装上の強度が存在する。理論上の強度の低下は情報システムの処理能力の向上や暗号解読法の考案によるところが大きく、実装上の強度の低下はサイドチャネル攻撃等の攻撃技術によるところが大きい。サイドチャネル攻撃の例として、実装時に暗号アルゴリズムの動作に伴う消費電力や暗号モジュールから漏えいする電磁波等の付加的な情報を悪意ある第三者等が知り得る場合には、実装上の強度は極端に低下する可能性がある。

第２項第３号「管理手順を定めること」について

暗号化された情報の復号又は電子署名の付与に用いる鍵（以降本項において「鍵」という。）の管理手順として、以下の視点を含む鍵のライフサイクルを考慮した管理手順を策定するとよい。また、暗号化された情報の復号や電子署名の付与の際には、本人及び管理上必要のある者のみが知り得る秘密の情報を用いる必要があることから、適切に管理する必要がある。

●鍵の生成

適切な暗号モジュールの内部において、その値を推定することが困難である乱数又は擬似乱数に係る処理を通じて生成し、かつ利用者以外の者が入手できないことを保証する仕組みが必要である。

●鍵の配送

鍵の受取先と事前に対面等で確認し合うなどにより、受取先の正当性に係る十分な確証が得られない限り、オンライン上での鍵の配送を行うべきではない。鍵を配送する際は、受取先のなりすまし対策等、配送先が確実であることを保証するとともに当該鍵に係る情報が適切に保護される仕組みが必要である。

●鍵の保管
　鍵は、例えば HSM 等の保存装置又は記録媒体等に適切に保護された環境で保管され、第三者等による窃取の防止に加え、改ざんからの保護、検知及び回復を実現する仕組みを備えることが必要である。
●鍵の利用
　鍵はその運用期限が有効な限り、当該鍵へのアクセスが取扱いの許可されたものだけに限定されるよう可用性が確保され、かつ適切に実装された上で利用することが必要である。
●鍵の期限切れ
　有効期限を過ぎた鍵は使用を停止し、適切な手段で取り除かれることが必要である。
●鍵の更新
　鍵の有効期限が終了した後も運用を継続する場合、鍵としての継続性を維持するため、基本的に有効期限の終了前に古い鍵のパラメータを基に、新たな鍵を生成することが望ましい。
なお、古い鍵は適切に廃棄されることが必要である。
●鍵の失効
　鍵の漏えいによる危殆化や、鍵を利用していた行政事務従事者が組織から離れることに伴う鍵の登録抹消等により、そのコピーやバックアップが存在する場合も含め、有効期限前の鍵の利用を適切に停止することが必要である。
●鍵の廃棄
　特別な理由を除き、不要となった鍵の情報はそのコピーやバックアップが存在する場合も含め、有効期限後に適切な物理的又は電磁気学的な消去方法を用いて確実に消去される仕組みが必要である。

第３項「電子証明書を UPKI 電子証明書発行サービスが発行している」について
UPKI 電子証明書発行サービス以外が発行するサーバ証明書、コード署名証明書等の電子証明書が有効期限内の場合、次期更新時には、UPKI 電子証明書発行サービスで発行している電子証明書を利用することが求められる。

C2101-126　（暗号化・電子署名に係る対策）（政府機関統一基準の対応項番 6.1.5(1)-1）
第百二十六条　部局技術責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。
一　情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。
二　複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。
三　選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護される製品を利用することを確実にするため、「暗号モジュール試験及び認証制

度」に基づく認証を取得している製品を選択する。

四　暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。

五　機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のある暗号プロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

解説：第１号「暗号モジュールを交換」について

暗号モジュールは、暗号化、電子署名、ハッシュ関数等の暗号に関連した機能を提供するソフトウェアの集合体又はハードウェアとして定義される。選択した暗号化アルゴリズムが将来危殆化することを想定し、暗号モジュールの交換が可能な構成とすることを、情報システムの設計段階から考慮する必要がある。また、あらかじめ暗号モジュールのアプリケーションインタフェースを統一しておくなどを考慮する必要がある。

第２号「複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択」について

選択したアルゴリズムが将来危殆化することを想定し、危殆化していない他のアルゴリズムへ直ちに変更できる機能と併せて、暗号利用モード等との組合せ等により脆弱性の顕在化が認められない安全なプロトコルを選択できる機能も、あらかじめ情報システムに設けておく必要がある。

第３号「「暗号モジュール試験及び認証制度」に基づく認証」について

アルゴリズム自体が安全であっても、それをソフトウェアやハードウェアへ実装する際、生成する疑似乱数に偏りが生じるなどの理由で疑似乱数が推測可能であったり、鍵によって処理時間に統計的な偏りが生じるなどの理由で鍵情報の一部が露呈したりすると、情報システムの安全性が損なわれるおそれがあることから、これらを確認するには、ISO/IEC19790 に基づく「暗号モジュール試験及び認証制度」が利用可能である。

第４号「耐タンパ性」について

JIS X 19790 (ISO/IEC 19790)の規定によると、耐タンパ性は以下の 3 つの機能から構成される。

・タンパ検出

暗号モジュールのセキュリティを危殆化する試みがなされたことの、暗号モジュールによる自動的な判定

・タンパ証跡

暗号モジュールのセキュリティを危殆化する試みがなされたことを示す、外観上の表示

・タンパ応答

暗号モジュールがタンパを検出したときに採る自動的な動作

また、暗号モジュールを利用する環境等に応じ、セキュリティレベルが 1 から 4 まで設定されている。セキュリティレベル 1 は、最小限の物理的保護を要求

している。セキュリティレベル 2 では、タンパ証跡メカニズムの追加を要求している。セキュリティレベル 3 では、除去可能なカバー及びドアに対して、タンパ検出及びタンパ応答メカニズム付きの強固な囲いの利用の要求事項を追加している。セキュリティレベル 4 では、囲い全体に対して、タンパ検出及びタンパ応答メカニズム付きの強固な囲いの利用の要求事項を追加している。
なお、タンパ検出及びタンパ応答は、タンパ証跡の代わりにはならない。
暗号モジュールの耐タンパ性に関わるセキュリティレベルは、情報システムが取り扱う以下の特性を踏まえて選択することが望ましい。
・暗号化及び／又は復号する情報の特性
・電子署名が付与される情報の特性

第５号「安全性に実績のある暗号プロトコル」について
情報システムで暗号を用いるとき、暗号アルゴリズムの適切な選択に加え、暗号プロトコル（暗号アルゴリズムをどのように用いるかの手順）が適切なものとなっている必要がある。一般に、情報システムを新規に構築するときに、独自の暗号プロトコルを設計することは、その安全性について十分に検証されないときは、期待される安全性が確保されていない可能性がある。安全な暗号プロトコルの設計は高度な専門性を有する者以外には容易なことではないため、可能な限り、独自の設計を避け、既に広く利用実績のある著名な暗号プロトコルを用いることが求められる。
なお、必要とする機能を実現する暗号プロトコルとして既存のものが存在しない場合はこの限りでないが、独自に暗号プロトコルを設計するときは、その安全性に関して十分に検証する必要がある。

第５号「長期的な秘匿性」について
情報システム上で機微な情報のやり取りを行う場合、情報を暗号化して通信しても、その暗号文が悪意ある第三者等に傍受され、将来の解読に備えて長期間にわたり保管されるという脅威が想定される。この場合に、「前方秘匿性（Forward Secrecy）」を有しない暗号プロトコルを用いた結果、公開鍵暗号の鍵が将来破られることになれば、過去に遡って全ての暗号文が解読されてしまうことになる。そのため、長期の機密性を確保する必要のある機微な情報のやりとりを行う情報システムを構築するときは、「前方秘匿性」を実現する暗号プロトコルの採用を検討し、必要かつ可能であれば、採用することが求められる。

C2101-127　（暗号化・電子署名に係る管理）（政府機関統一基準の対応項番 6.1.5(2)）
第百二十七条　部局技術責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。
一　電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。
二　暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関

する情報を定期的に入手し、必要に応じて、利用者等と共有を図ること。

C2101-128　（政府機関統一基準の対応項番 6.1.5(2)-1）

第百二十八条　部局技術責任者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とすること。

一　信頼できる機関による電子証明書の提供

二　本学の窓口での電子証明書の提供

解説：第１号「信頼できる機関による電子証明書の提供」について

例えば、信頼できる機関のサイトから、利用者が電子署名を検証するための電子証明書をダウンロードできるように環境を整備する方法である。利用者はダウンロードした電子証明書を端末に取り込み、それを基に署名検証を行う。

第２号「本学の窓口での電子証明書の提供」について

本学において、利用者に電子署名を検証するための電子証明書を記録媒体で配布する方法である。利用者は記録媒体経由で電子証明書を端末に取り込み、それを基に署名検証を行う。

第十二章　情報システムの脅威への対策

第一節　ソフトウェアに関する脆弱性対策

解説：本学の情報システムに対する脅威としては、第三者が情報システムに侵入し本学の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に、一般利用者向けに提供するサービスが第三者に侵入され、個人情報の漏えい等が発生した場合、本学に対する社会的な信用が失われる。

一般的に、このような攻撃では、情報システムを構成するサーバ装置、端末及び通信回線装置のソフトウェアの脆弱性を悪用されることが想定される。したがって、本学の情報システムにおいては、ソフトウェアに関する脆弱性について、迅速かつ適切に対処することが求められる。

なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、第９章第２節「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。

C2101-129　（ソフトウェアに関する脆弱性対策の実施）（政府機関統一基準の対応項番 6.2.1(1)）

第百二十九条　部局技術責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。

２　部局技術責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。

３　部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョン

アップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。

4　部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。

解説：第２項「公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策」について
脆弱性が明らかになっていない段階においても、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施する。対策としては、特定のメモリ上の実行権限の削除又はバッファオーバーフローの検知によるアプリケーションの実行停止等の対策を実施すること等が挙げられる。

第３項「サーバ装置、端末及び通信回線装置上で利用するソフトウェア」について
情報システムの構築時に、ソフトウェアを効率的に開発するためにソフトウェアフレームワーク開発用のフレームワークとして情報システムに組み込まれたまま納入されるソフトウェア等、情報システムの運用中に動作しないものについても考慮する必要がある。当該ソフトウェアの脆弱性による影響についても考慮し、脆弱性対策の対象とするソフトウェアを定めておくことが望ましい。

C2101-130　（ソフトウェアに関する脆弱性対策）（政府機関統一基準の対応項番 6.2.1(1)-1,2,3,4,5,6,7）

第百三十条　部局技術責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む情報を適宜入手すること。

一　脆弱性の原因
二　影響範囲
三　対策方法
四　脆弱性を悪用する不正プログラムの流通状況

2　部局技術責任者は、利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しないこと。

3　部局技術責任者は、構成要素ごとにソフトウェアのバージョン等を把握し、脆弱性対策の状況を確認すること。

4　部局技術責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項について判断すること。

一　対策の必要性
二　対策方法
三　対策方法が存在しない場合又は対策が完了するまでの期間に対する一時的な回避方法
四　対策方法又は回避方法が情報システムに与える影響
五　対策の実施予定
六　対策試験の必要性
七　対策試験の方法

八　対策試験の実施予定

5　部局技術責任者は、脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。

一　実施日

二　実施内容

三　実施者

6　部局技術責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「対策用ファイル」という。）は、信頼できる方法で入手すること。

7　部局技術責任者は、脆弱性対策の状況を確認する間隔は、可能な範囲で短くすること。

解説：第１項「情報を適宜入手」について

情報システムを構成するサーバ装置、端末及び通信回線装置上で利用するソフトウェアの脆弱性に関する情報は、製品ベンダや脆弱性情報提供サイト等を通じて適時調査を行う必要がある。自動アップデート機能を持つソフトウェアの場合には、当該機能を利用して、定期的に脆弱性に関連する情報が報告されているかを確認する方法で差し支えないが、自動アップデート機能の対象範囲を把握し、対象範囲外のソフトウェアについては適時調査を行う必要がある。例えば、ウェブアプリケーション等のソフトウェアを効率的に開発するためにソフトウェアフレームワークを利用する場合があるが、ソフトウェアフレームワークを利用して開発したアプリケーションは自動アップデートが行えないため、脆弱性の有無については適宜調査を行う必要がある。

入手した脆弱性に関連する情報及び対策方法に関しては、脆弱性対策を効果的に実施するために、他の部局技術責任者と共有することが望ましい。

第１項第４号「脆弱性を悪用する不正プログラムの流通状況」について

脆弱性が既知になると、インターネット上の情報交換コミュニティ等を通じて、その脆弱性を悪用する方法が考案され、その悪用方法を機械的に実行するための不正プログラム（exploit コードとも呼ばれる）が作られ、次第に広まっていく。この「脆弱性を悪用する不正プログラム」が流通している段階に入ると、脆弱性が攻撃されるリスクが格段に高まると考えられる。脆弱性を悪用する不正プログラムが世の中に流通していることが確認された場合には、速やかに当該の脆弱性について対処することが望ましい。

第２項「サポート期間を考慮」について

利用するソフトウェアのサポート期間が過ぎた場合、それ以降はセキュリティ関連の脆弱性を修正するためのセキュリティパッチは、原則としてソフトウェアベンダから提供されなくなる。したがって、情報システムのライフサイクルを考慮し、少なくとも情報システムの次期改修までは対策用ファイルの提供が継続されるソフトウェアを選定する必要がある。

また、情報システムは特定のソフトウェアバージョンに依存しないよう設計することが望ましいが、情報システムの中には、特定のソフトウェアバージョン

に強く依存する場合がある。この場合には、ソフトウェアをバージョンアップすることが困難となるが、新しいバージョンのソフトウェアでしか対処できない脆弱性が発生したときに、情報システムの停止という最悪の事態も想定される。したがって、情報システムが特定のソフトウェアバージョンに依存せざるを得ない場合には、当該ソフトウェアのサポート期間を考慮して情報システムの更改について検討しておく必要がある。

第２項「サポートが受けられないソフトウェア」について
ソフトウェアベンダによるサポートや他の事業者によるサポートサービスが一切受けられないものを対象としている。ソフトウェアベンダの製品ロードマップの見直し等により、サポートの打ち切りが突然予告されることもあり得るため、利用するソフトウェアのサポート期間に関する情報を適時入手し、ソフトウェア更改やサポート事業者の切替え等の対策が適切に講じられるよう考慮することが望ましい。

第３項「ソフトウェアのバージョン等を把握」について
把握すべき情報としては、ソフトウェアのバージョンのほか、脆弱性対策の最終実施日、未実施の脆弱性対策等がある。

第３項「脆弱性対策の状況を確認」について
OS や各種サーバ、ファイアウォール等の通信回線装置等における脆弱性対策の状況を効率的に確認する方法として、専用ツールや事業者が提供するサービス等を利用する脆弱性診断の実施が挙げられる。脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、ソフトウェアの種類によって利用する脆弱性診断を使い分ける必要がある。
ソースコード診断では、独自に開発したソフトウェアのソースコードを対象に、静的解析ツール等を用いて脆弱性の有無を検証する。したがって、運用開始までにソースコード診断を実施し、運用開始後にソースコードへ修正を加えた場合は、再度診断を実施することが望ましい。
プラットフォーム診断では、OS や各種サーバ、ファイアウォール等を対象に、テスト用の通信パケットを送信するなどの方法によって、最新のセキュリティパッチが適用されているか、設定が適切に行われているか、不要な通信ポートが開いていないかなどを検証する。したがって、運用開始までにプラットフォーム診断を実施し、その後も例えば年に１回診断を実施するなど、定期的に実施することが望ましい。
ウェブアプリケーション診断では、独自に開発したウェブアプリケーションを対象に、実際に不正なデータをウェブアプリケーションに送信するなどの方法によって、SQL インジェクションやクロスサイトスクリプティング等の脆弱性が存在しないかを検証する。したがって、運用開始までにウェブアプリケーション診断を実施し、運用開始後においても、ウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合は、再度診断を実施することが望ま

しい。

第４項第３号「一時的な回避方法」について
ソフトウェアにおいて脆弱性が顕在化した際に、ソフトウェアベンダが対応するまでの間は、当該ソフトウェアの利用を禁止する又は脆弱性が関係する機能を無効化するなどの対応が必要となる。
しかし、これらの対応によって業務に著しく悪影響を与えることが想定される場合は、事前に必要な措置を講じておくことが求められる。例えば、ブラウザは業務上利用せざるを得ないケースが多いが、異なるソフトウェアベンダが提供する複数のブラウザを端末に導入しておくことで、業務継続性を維持しつつ、脆弱性を悪用した攻撃を受けるリスクを低減することができる。複数のブラウザを導入することは、情報システムのコスト増加を招く可能性があるが、一方のブラウザを常時利用するとともに、他方を緊急時のインターネットへのアクセス手段として利用するなど、用途を分ける方法も考えられる。また、ログ出力の設定を確認し、対応が完了するまでの期間、出力されたログの監視を強化するなどの対応も考えられる。

第４項第６号「対策試験」について
「対策試験」とは、脆弱性対策の実施による情報システムへの影響の有無を確認するために、事前に試験用の情報システムを用いて試験することが想定される。

第６項「対策用ファイル」について
入手した対策用ファイルに悪意のあるコードが含まれている可能性を考慮し、対策用ファイルは信頼できる方法で入手する必要がある。
信頼できる方法としては、ソフトウェアの開発元等が公開するウェブサイトからダウンロードする方法、又は郵送により対策用ファイルが記録された外部電磁的記録媒体を入手する方法が挙げられる。また、対策用ファイルが改ざんされていないこと等の完全性を検証できる手段があれば、併せてこれを実行する必要がある。

第二節　不正プログラム対策

解説：情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼすおそれがある。このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

C2101-131　（不正プログラム対策の実施）（政府機関統一基準の対応項番 6.2.2(1)）

第百三十一条　部局技術責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

２　部局技術責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

３　部局技術責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。

解説：第１項「動作可能な不正プログラム対策ソフトウェア等」について

不正プログラム対策ソフトウェアの例としては、コンピュータウイルスを検知対処する「ウイルス対策ソフトウェア」や、キーロガーやアドウェア等のいわゆるスパイウェアを検知対処する「スパイウェア対策ソフトウェア」等がある。

多くのメインフレームシステム並びに OS 及びアプリケーションを搭載していないサーバ装置及び端末については、動作可能な不正プログラム対策ソフトウェア等が存在しないため、本対策事項の対象外である。ただし、新たに動作可能な不正プログラム対策ソフトウェア等が出現した場合には、速やかな導入が求められることから、部局技術責任者は、該当するサーバ装置及び端末の把握を行っておくとともに、不正プログラム対策ソフトウェア等に関してベンダが提供するサポート情報に常に注意を払っておくことが望ましい。

また、新たな不正プログラムの存在が明らかになった後でも、利用中の不正プログラム対策ソフトウェア等に用いる定義ファイルがベンダから配布されないなど、日常から行われている不正プログラム対策では対処が困難と判断される場合、部局技術責任者は利用者等に回避策の実施を指示する必要がある。

なお、回避策は一律ではなく、個々の状況によって様々な内容があり得る。例えば、インターネット上の一部のウェブサイトを閲覧すると不正プログラムに感染することが判明している場合に、不正プログラム対策ソフトの定義ファイルが対応するまでの間、一時的にインターネット閲覧を制限する、という回避策が想定される。

C2101-132　（不正プログラム対策ソフトウェア等に係る対策）（政府機関統一基準の対応項番 6.2.2(1)-1,2,3）

第百三十二条　部局技術責任者は、不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるよう構成すること。

２　部局技術責任者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

３　部局技術責任者は、不正プログラム対策ソフトウェア等は、定期的に全てのファイルを対象としたスキャンを実施するよう構成すること。

C2101-133　（想定される不正プログラムの感染経路の全てにおける対策）（政府機関統一基準の対応項番 6.2.2(1)-4）

第百三十三条　部局技術責任者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行うこと。

解説：「感染経路を特定」について

不正プログラムの感染経路には、電子メール、ウェブ等のネットワーク経由のほか、不正プログラムに感染した外部電磁的記録媒体経由も考えられる。

不正プログラム対策ソフトウェア等は、製品ごとに不正プログラム定義ファイルの提供時期及び種類が異なる。また、これらは現存する全ての不正プログラムを検知及び除去できるとは限らず、不正プログラム対策ソフトウェア等の不具合により不正プログラムの検知又は除去に失敗する危険性もある。このことから、不正プログラムによる被害を低減させるため、感染経路において、異なる定義ファイルを用いる不正プログラム対策製品を組み合わせる、又は、定義ファイルパターンマッチングやふるまい検知等の異なる技術を用いる製品を組み合わせることにより、どれか一つの不具合で、その環境の全てが不正プログラムの被害を受けることのないようにすることが望ましい。例えば、電子メールサーバに導入するウイルス対策ソフトウェアと端末に導入するウイルス対策ソフトウェアについて、それぞれ異なるウイルス定義ファイルを用いる製品を導入すること等が考えられる。

「感染拡大の防止」について

ネットワークを経由した感染拡大の防止策としては、例えば以下が挙げられる。

・OS やアプリケーションに関するセキュリティパッチ及び不正プログラム定義ファイルについて最新化されていない端末をネットワークに接続させない仕組みの導入

・通信に不正プログラムが含まれていることを検知したときに、その通信をネットワークから遮断する仕組みの導入

C2101-134　（不正プログラム対策の状況の把握）（政府機関統一基準の対応項番 6.2.2(1)-5）

第百三十四条　部局技術責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。

一　不正プログラム対策ソフトウェア等の導入状況

二　不正プログラム対策ソフトウェア等の定義ファイルの更新状況

第三節　サービス不能攻撃対策

解説：インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、本学の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。

C2101-135　（サービス不能攻撃対策の実施）（政府機関統一基準の対応項番 6.2.3(1)）

第百三十五条　部局技術責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下この条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手

段を用いてサービス不能攻撃への対策を行うこと。

２　部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。

３　部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。

解説：第１項「サービス不能攻撃」について

サービス不能攻撃は、DoS 攻撃(Denial of Service)とも呼ばれる。また、このDoS攻撃を複数の拠点から一か所に対して行う攻撃は、DDoS攻撃(Distributed Denial of Service)と呼ばれ、攻撃元が複数に分散しているために防御側の対処が困難な攻撃として知られている。

C2101-136　（サービス不能攻撃への対策）（政府機関統一基準の対応項番 6.2.3(1)-1）

第百三十六条　部局技術責任者は、サーバ装置、端末及び通信回線装置について、以下を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。

一　パケットフィルタリング機能

二　3-way handshake 時のタイムアウトの短縮

三　各種 Flood 攻撃への防御

四　アプリケーションゲートウェイ機能

C2101-137　（サービス不能攻撃を受けた場合を想定した対策）（政府機関統一基準の対応項番 6.2.3(1)-2,3,4）

第百三十七条　部局技術責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築すること。

２　部局技術責任者は、サーバ装置、端末及び通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、以下を例とする対策を検討すること。

一　インターネットに接続している通信回線の提供元となる事業者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策

二　サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入

三　サーバ装置、端末及び通信回線装置及び通信回線の冗長化

３　部局技術責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討すること。

解説：第２項第１号「インターネットに接続している通信回線」について

情報システムに対してサーバ装置、端末及び通信回線装置に係るサービス不能攻撃の対策を実施しても、学外へ接続する通信回線及び通信回線装置への過負荷の影響を完全に排除することは不可能である。このため、インターネットに接続している通信回線の提供元となる事業者に確認した上で、サービス不能攻撃発生時の対処手順や連絡体制を整備する必要がある。

第２項第３号「冗長化」について
冗長化の例としては、サービス不能攻撃が発生した場合に備え、サービスを提供するサーバ装置、端末、通信回線装置又は通信回線について、負荷を分散させる、又はそれぞれ代替のものに切替えるなどにより、サービスを継続することができるように情報システムを構成することが考えられる。
なお、代替のものへの切替えについては、サービス不能攻撃の検知及び代替サーバ装置等への切替えが許容される時間内に行えるようにする必要がある。

第３項「攻撃への対処を効率的に実施できる手段」について
対処例としては、サービス提供に利用している通信回線がサービス不能攻撃により過負荷状態に陥った場合においても、サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するための装置を操作できる手段を確保することが挙げられる。具体的には、管理者が当該装置を操作するためのサーバ装置、端末及び通信回線を、サービス提供に利用しているものとは別に用意することが挙げられる。
また、サービス不能攻撃に伴い、本学の自己管理ウェブサイトの閲覧障害が発生した場合においても、緊急性・重要度が高い情報が長時間閲覧できなくなることは極力回避すべきである。これに鑑み、災害情報等の緊急性が高く、国民の生命や財産に著しく影響を及ぼしうるような重要情報については、広報担当とも協力するなどして、サービス不能攻撃を受けた際にも発信を可能とするよう、閲覧障害時の告知ページに最低限のテキストデータを掲載するなどの必要な措置を考慮するとよい。

C2101-138　（サービス不能攻撃を受けることに関する監視）（政府機関統一基準の対応項番 6.2.3(1)-5,6）
第百三十八条　部局技術責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定めること。
２　部局技術責任者は、監視対象の監視記録を保存すること。
解説：「監視方法及び監視記録の保存期間」について
インターネットからアクセスされるサーバ装置や、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する必要がある。
「監視方法」については、サービス不能攻撃を受けることに関する監視には、稼動中か否かの状態把握や、システムの構成要素に対する負荷の定量的な把握（CPU 使用率、プロセス数、ディスク I/O 量、ネットワークトラフィック量等）がある。監視方法は多種多様であるため、当該情報システムの構成等の特性に応じて適切な方法を選択する必要がある。
「監視記録の保存期間」については、監視対象の状態の変動を把握するという目的に照らして、保存期間を定める必要がある。

第２項「監視記録を保存」について
サーバ装置、端末、通信回線装置及び通信回線を監視している場合、監視対象の状態は一定ではなく変動することが一般的である。時間変動、曜日変動、週変動、月変動、季節変動等を検討した上で記録を一定期間保存する。

第四節　標的型攻撃対策

解説：標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。
したがって、標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

C2101-139　（標的型攻撃対策の実施）（政府機関統一基準の対応項番 6.2.4(1)）

第百三十九条　部局技術責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。

２　部局技術責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。

解説：第１項「標的型攻撃」について
以下の各項における規定内容は、標的型攻撃への対策としても有効であるため、それぞれに示される対策を行う必要がある。
・第１１章第１節「主体認証機能」
・第１１章第２節「アクセス制御機能」
・第１１章第３節「権限の管理」
・第１１章第４節「ログの取得・管理」
・第１１章第５節「暗号・電子署名」
・第１２章第１節「ソフトウェアに関する脆弱性対策」
・第１２章第２節「不正プログラム対策」
・第１４章第１節「端末」
・第１４章第２節「サーバ装置」
・第１５章第１節「電子メール」
・第１６章第１節「通信回線」
・第１８章「情報システムの利用」

C2101-140　（標的型攻撃に係る入口対策）（政府機関統一基準の対応項番 6.2.4(1)-1,2）

第百四十条　部局技術責任者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下を例とする対策を行うこと。

一　不要なサービスについて機能を
削除又は停止する。

二　不審なプログラムが実行されないよう設定する。

三　パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

２　部局技術責任者は、USB メモリ等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下を例とする対策を行うこと。

一　出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接続する外部電磁的記録媒体を事前に特定しておく。

二　外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。

三　サーバ装置及び端末について、自動再生（オートラン）機能を無効化する。

四　サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする。

五　サーバ装置及び端末について、使用を想定しない USB ポートを無効化する。

六　組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。

解説：第１項第２号「不審なプログラムが実行されないよう設定する」について

具体的な設定手段としては、あらかじめ利用するアプリケーションを登録してそれ以外のアプリケーションの実行を拒否するよう設定する、通常のアプリケーションでは利用しないメモリ空間を利用しようとしたアプリケーションを不審と判定して実行を拒否するソフトウェアを利用する、情報システムにおいては不正プログラムの起動又は動作を拒否する手法を導入するなどが挙げられる。なお、これらを導入する場合には、業務で利用するアプリケーションに影響が及ぶ可能性があるため、事前に検証する必要がある。

第２項第３号「自動再生（オートラン）機能を無効化」について

自動再生（オートラン）機能とは、OS がその機能を備えている場合において、サーバ装置や端末に USB メモリ等の外部電磁的記録媒体を接続した際に、その媒体に格納されている特定のプログラムを自動的に実行する機能を指す。

標的型攻撃に用いられる手段として、この機能を悪用するものがあり、例えば、不正プログラムを格納した USB メモリを端末に接続させることにより、不正プログラムを実行させるという手法が想定される。

自動再生（オートラン）機能を無効化しておくことにより、この機能を悪用する手段による被害に遭うリスクを低減することができる。

第２項第４号「外部電磁的記録媒体内にあるプログラムを一律に実行拒否」について

OS によっては、あらかじめ設定することにより、USB メモリ等の外部電磁的

記録媒体を端末に接続した場合において、その媒体にあるプログラムを、その媒体にある状態のまま実行することを一律に拒否することができる。プログラムを実行したい場合には、端末の内蔵電磁的記録媒体（PC 内蔵 HDD 等）にいったんコピーしてから実行する運用となる。この設定により、接続した途端に外部電磁的記録媒体上の不正プログラムが実行されるリスクを低減することができる。

第２項第５号「USB ポートを無効化」について
物理的に又はシステム的に USB ポートを利用できない状態にすることで、USB メモリ等の外部電磁的記録媒体を接続することによって生じる情報セキュリティインシデントの発生を抑止できる。

第２項第６号「組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービス」について
外部電磁的記録媒体のポートへの接続や利用を制御及び管理するため、以下のような機能を持つ製品やサービスが市場に提供されている。
・端末の USB ポートのインタフェースを無効化し、外部電磁的記録媒体を含む全ての機器を利用不可とする。
・USB ポートに接続された機器のうち、全ての外部電磁的記録媒体を利用不可とする。
・利用を認める外部電磁的記録媒体を一元管理するサーバに事前に登録しておき、登録されていない外部電磁的記録媒体の利用不可とする。
・利用を認める外部電磁的記録媒体の個体識別情報（製品番号等）と利用者の組合せを一元管理するサーバに事前に登録しておき、組合せ以外での利用を不可とする。
・外部電磁的記録媒体の接続の際における、利用者、出力日時、出力ファイル名等のログを自動的に取得する。

C2101-141　（標的型攻撃に係る内部対策）（政府機関統一基準の対応項番 6.2.4(1)-3,4,5）
第百四十一条　部局技術責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を例とする対策を行うこと。
一　重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。
二　認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずる。
２　部局技術責任者は、端末の管理者権限アカウントについて、以下を例とする対策を行うこと。
一　不要な管理者権限アカウントを削除する。
二　管理者権限アカウントのパスワードは、容易に推測できないものに設定する。
３　部局技術責任者は、重点的に守るべき業務・情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って、対策を講ずること。

解説：第１項「情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバ」について
悪意ある第三者等は、入口対策を突破して内部への侵入に成功すると、外部から遠隔指令を出して内部侵入の範囲を拡大しつつ、目的の達成を目指すと想定される。その目的としては、重要情報の窃取や破壊が想定され、したがって、識別コード及びアクセス権限を集中管理する認証サーバ、又は、情報が集中的に保存されるファイルサーバは、攻撃対象となる蓋然性が高いと考えられる。これら重要サーバには、特に注意を払って情報セキュリティ対策を講ずる必要がある。

第１項第２号「管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策」について
管理者権限を狙う攻撃としては、機械的にパスワードを変えながら連続してログイン試行する攻撃が考えられる。このような攻撃を受けることを想定した対策としては、以下に挙げるものが考えられる。
・連続でのログイン失敗回数に上限値を設け、この上限値を超えた場合は、次回ログイン試行までに一定の期間（例：15 分）ログイン試行を受け付けないようにシステム等で設定する。
・ログイン失敗ログを取得し、その取得内容を継続的に監視することにより、大量のログイン失敗を検知する仕組みを導入する。

なお、辞書攻撃とは、パスワードに単語の組み合わせや人名を用いている場合に有効なパスワード解析方法をいう。英語の辞書に限らず各国語の単語を用いる場合もあるため、日本語の単語、日本人の人名も安全ではない。また、単語と数桁の数字のような単純な組み合わせも解析の対象となる。また、ブルートフォース攻撃とは、無意味な英数記号の組み合わせも含めた、総当たりでのパスワード解析方法をいう。辞書攻撃より効率は劣るが、原理的には必ず正しいパスワードに到達する。

第十三章　アプリケーション・コンテンツの作成・提供

第一節　アプリケーション・コンテンツ作成時の対策

解説：本学では、教育研究事務に係る情報の提供、事務手続等のためにアプリケーション・コンテンツを用意し、広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に、利用者端末の情報セキュリティ水準の低下を招いてしまうことは避けなければならない。本学は、アプリケーション・コンテンツの提供に際しても、情報セキュリティ対策を講じておく必要がある。
また、アプリケーション・コンテンツの開発・提供を外部委託する場合については、第７章第１節「外部委託」についても併せて遵守する必要がある。

C2101-142　（アプリケーション・コンテンツの作成に係る規定の整備）（政府機関統一基準の対応項番 6.3.1(1)）

第百四十二条　全学実施責任者は、アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること。

解説：「アプリケーション・コンテンツ」について

教育研究事務に係る情報の提供、事務手続等の各種サービスは、アプリケーションプログラムやウェブコンテンツ等を用いて一般利用者等に提供されている。特にウェブコンテンツでは、本学以外が提供するコンテンツ（以下「外部コンテンツ」という。）を組み込むことによって、容易に様々な機能を提供することが可能となるが、本学において外部コンテンツの信頼性を担保することは不可能であることから、このような利用方法には注意を要する。例えば、外部コンテンツが事前に通知されることなく変更されてしまい、各種サービスの利用者の意図に反して利用者の個人に関する情報が取得される可能性がある。また、外部コンテンツに不正プログラムが組み込まれ、各種サービスの利用者がそれに感染する被害が生じることも考えられる。そのため、ウェブコンテンツでは外部コンテンツを利用しないことが望ましいが、必要があって利用する場合には、これらの脅威に対して適切なセキュリティ対策を実施することが求められる。

「学外の情報セキュリティ水準の低下を招く行為を防止する」について

一般利用者等が本学によって提供される各種サービスを利用する場合、各種サービスの利用によって、利用者の端末が不正プログラムに感染しやすい状況を強制したり、利用者個人の情報が利用者の意図に反して第三者に提供させられるといった状況を作り出したりすることは避けなければならない。本学は、一般利用者等の学外の情報セキュリティ水準を低下させないように留意して、各種サービスのためのアプリケーション・コンテンツを提供する必要がある。

「規定を整備」について

全学実施責任者は、アプリケーション・コンテンツの提供に関する規定の整備に当たり、次条において規定した事項を含める必要がある。

C2101-143　（アプリケーション・コンテンツのセキュリティ要件の策定）（政府機関統一基準の対応項番 6.3.1(2)）

第百四十三条　部局技術責任者は、学外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含めること。

一　提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

二　提供するアプリケーションが脆弱性を含まないこと。

三　実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

四　電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテン

ツの提供先に与えること。

五　提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

六　サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

2　教職員等は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前号に掲げる内容を調達仕様に含めること。

解説：第１項第１号「不正プログラムを含まない」について

不正プログラムとは、一般的なコンピュータウイルスの他、ワームやスパイウェア等が該当する。不正プログラムを含まないようにすべきものは、学外の利用者の端末にインストールさせるプログラムの他、利用者に閲覧させるウェブサイトのウェブページも含む。

第１項第２号「脆弱性を含まない」について

脆弱性は、アプリケーションプログラムが動作する OS や利用する開発言語によって様々な種類のものが存在する。例えば、C 言語によって開発されたアプリケーションプログラムにバッファオーバーフローの脆弱性が存在した場合は、利用者の端末上で任意のプログラムを実行される可能性がある。したがって、OS や開発言語の特性に応じて適切な脆弱性対策を実施する必要がある。

第１項第３号「実行プログラムの形式でコンテンツを提供しない」について

実行プログラムの形式とは、利用者がダブルクリックするなどしてファイルを開いたときに自動的にプログラムコード（当該ファイルの作成者が意図した任意のコード）が実行される形式のファイルのことであり、拡張子が「.exe」の形式のものがこれに該当するほか、「.pif」、「.scr」、「.bat」等のものも該当する。

本号に違反する例としては、会議資料等のプログラムではない文書を提供する際に、自己展開式圧縮ファイル作成ソフトウェアを用いて拡張子が「.exe」の圧縮ファイルを作成してこれを配布する行為が典型例として挙げられる。この場合は、拡張子「.zip」等の形式の圧縮ファイルを作成して配布すればよい。

なお、電子メールの添付により文書等を配布する場合については、第十七章の第二百十八条第２項第４号「(解説)「実行プログラム形式のファイルを削除等する」について」を参照のこと。

実行プログラムの形式は、不正プログラムがその感染手段として利用することが多く、特に電子メールに添付された実行形式のファイルは、不正プログラム感染防止のため、基本的に開かないようにしなければならない。これは、拡張子「.zip」等の圧縮ファイル中に含まれる実行プログラムの形式のファイルについても同様である（第二百二十七条第３項第４号にも規定しているため、参照のこと。）。それにもかかわらず、本学が日ごろから実行プログラムの形式で

のコンテンツ提供を行う場合、本学の利用者等だけでなく、一般の各種サービスの利用者に対しても、実行プログラムの形式のファイルを開くことに慣れさせてしまうことになり、利用者の情報セキュリティ水準を低下させてしまうことになる。そのため、本号は、そもそも実行プログラムの形式や実行プログラムの形式を含む圧縮ファイルの形式でのコンテンツ提供をしないよう求めている。
なお、本学が各種サービスのためにアプリケーションプログラムを提供する必要がある場合等、「実行プログラムの形式以外にコンテンツを提供する手段がない」場合は、実行プログラムの形式で提供してもよいが、第百四十三条及び第百四十四条第４項に従った措置を行う必要がある。

第１項第４号「改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与える」について
改ざん等がなく真正なものであることを確認できる手段には、利用者に提供するものがアプリケーションプログラムである場合は、「コードサイニング証明書」等と呼ばれる電子証明書を用いてアプリケーションプログラムに署名を施すことがこれに該当する。利用者はアプリケーションプログラムに施された署名を確認することで、改ざんがないことを確認でき、さらに、そのアプリケーションプログラムの提供者が本学であることを確認できる。提供するコンテンツがウェブサイト上にある場合には、TLS（SSL）を用いた「https://」で始まる URL のウェブページとすることにより、利用者は当該ウェブページが改ざんなく受信できていることを確認できる。TLS（SSL）を用いる際に、本学のサーバ証明書を用いれば、当該サイトが本学のものであることを確認できる。
コンテンツを電子メールで提供する場合には、S/MIME 等の電子署名の技術を用いることで、電子メールが配送途中で改ざんされていないこと及び発信者が本学であることを確認できる。
本学によりその手段を提供する準備が整っている場合は、アプリケーション・コンテンツの提供先に必ず与える必要がある。技術的にそのような手段が存在するものの本学がまだその手段を提供する準備を整えていない場合については、可能な限りその準備を整えることが望ましい。技術的にそのような手段が存在しない場合としては、文書ファイルを提供するときに、文書ファイルの形式によっては署名を施す手段がない場合があり、この場合にはその手段を与えなくてもよい。

第１項第５号「脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制する」について
各種サービスを提供する情報システムの提供において、当該情報システムを利用するために、学外の事業者等が作成した汎用のソフトウェアやミドルウェアのインストールが利用者の端末で必要となる場合がある。この場合、利用者は本学から指示されたソフトウェアを自身の端末にインストールせざるを得ないが、指定されるソフトウェア（又はソフトウェアバージョン）のサポート期間

が過ぎているなどの理由により脆弱性が存在するものであると、利用者の情報セキュリティ水準を本学が低下させることになる。したがって、脆弱性が存在するバージョンの OS の利用やソフトウェアのインストールを本学が暗黙又は明示的に要求することにならないよう、アプリケーション・コンテンツの提供方式を定めて開発しなければならない。
具体的には、当該サービスを提供するシステムが準備された時点では脆弱性が発見されていなくても、運用開始後に発見されることがある。そのとき、利用者が迅速に当該脆弱性を回避できるようになっている必要がある。例えば、当該サービスを利用するために、第三者が提供している汎用のソフトウェアのインストールを必要としていたとする。このとき、当該ソフトウェアに脆弱性が発見され、それを修正した新バージョンのソフトウェアが公開された場合に、当該新バージョンのソフトウェアをインストールすることで当該サービスに不具合等が生じて利用が不可能になるような事態が発生すると、利用者は、当該ソフトウェアを新バージョンに更新することができなくなる。結果として、本学の各種サービスが利用者の脆弱性回避を妨げることになってしまう。こうしたことが起きないよう、各種サービスを提供するシステムは、第三者の汎用ソフトウェアの併用を前提とする場合は、当該汎用ソフトウェアが新バージョンに置き換わっても、正常に動作するように設計する必要がある。予期せず不具合が発生する事態が発生した場合にも、各種サービスを提供するシステムを修正することができるよう、迅速に新バージョンのソフトウェアに対応することを保守契約に盛り込んでおくことが望ましい。
また、特定の種類のウェブブラウザに脆弱性が発見され、利用する危険性が高くなった場合においても､他の種類のウェブブラウザも利用可能とすることで、提供するサービスを継続可能にする必要がある。そのためには、例えば、2 種類以上のウェブブラウザ又は同一製品の異なるバージョンが動作するように、情報システムの構築時に配慮し、その動作確認をおこなうことが考えられる。
なお、開発時に公開されているバージョンだけでなく、例えば、利用を想定しているブラウザの次期バージョンについて、ソフトウェアの配布前に情報が公開された状態又は試用版ソフトウェアが配布され動作検証可能な状態にあれば、前もって利用可能かどうかを検証するなど、その後に公開が想定されるバージョンにも対応できるよう、構築時に配慮することが望ましい。

第 1 項第 5 号「情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求する」について
各種サービスを提供する情報システムを利用するために、利用者の端末にインストールされているソフトウェア（本学が直接提供していないソフトウェア（例えば、端末の OS やウェブブラウザ等））の設定変更を必要とするとき、その設定変更が情報セキュリティ水準の低下を招くものである場合、そのような設定変更を要求してはならない。必要があって利用者に設定変更を求めるときは、その OS やブラウザの標準設定（初期設定）に変更することのみを求めるものとすることである。

第１項第６号「サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能」について
これに該当する典型的な例は、本学のウェブサイトを構成する各 HTML ファイルの中に、学外のサイト（例として広告事業者の広告提供サーバ）のコンテンツを見えない形又は見える形で組み込むことで、本学のウェブサイトの閲覧者のアクセス履歴を当該広告サーバへ自動的に送信する、いわゆる「トラッキング処理」を行う機能である。このとき、当該広告提供サーバが HTTP の cookie 機能を用いて閲覧する利用者に識別番号を付番している場合は、アクセス履歴等の、サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が、本人の意思に反して当該広告提供サーバを運営する第三者に提供されることになるので、本号はこのような機能がアプリケーション・コンテンツに組み込まれることがないようにすることを求めている。
また、トラッキング処理ではなくとも、例えば、利用者のキー入力の全てを当該利用者が意図しない形で送信するなどの機能も、「サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能」に該当し得る。
なお、対象はウェブサイトの HTML ファイルに限られず、アプリケーションプログラムを提供する場合に、そのプログラムに含まれ得る機能についても同様である。

第２項「調達仕様に含める」について
例えば、本学が何らかのキャンペーンとして啓発コンテンツを提供する際に、その作成を広告会社等に外部委託する場合は、情報システム部門以外の教職員等がその外部委託の調達仕様を定めることになると考えられる。このような場合でも、学外の情報セキュリティ水準を低下させないよう、第１項のセキュリティ要件を調達仕様に含めることが求められる。

C2101-144　（アプリケーション・コンテンツのセキュリティ要件に係る対策）（政府機関統一基準の対応項番 6.3.1(2)-1,2,3,4,5）

第百四十四条　部局技術責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を含む対策を行うこと。

一　アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

二　外部委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。

２　部局技術責任者は、提供するアプリケーション・コンテンツにおいて、学外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、当

該学外へのアクセスが情報セキュリティ上安全なものであることを確認すること。

3　部局技術責任者は、提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない学外へのアクセスを自動的に発生させる機能を含めないこと。

4　部局技術責任者は、文書ファイル等のコンテンツの提供において、当該コンテンツが改ざん等なく真正なものであることを確認できる手段がない場合は、「https://」で始まる URL のウェブページから当該コンテンツをダウンロードできるように提供すること。

5　部局技術責任者は、改ざん等がなく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、国立情報学研究所 UPKI 電子証明書発行サービス（UPKI）の利用が可能である場合は、国立情報学研究所 UPKI 電子証明書発行サービスにより発行された電子証明書を用いて署名を施すこと。

解説：第２項「必要があって当該機能を含める場合」について

学外へのアクセスを自動的に発生させる機能を含める必要がある場合の例としては、ソーシャルメディアサービスとの連携機能を提供するためのボタン（ボタン画像の他、ボタン押下時の機能等を提供するプログラムを含む。）等を本学のウェブページ上に設置する場合が挙げられる。万が一、学外のウェブサイトが提供するプログラムに不正なコードが含まれていると、当該プログラムを使用した本学のウェブサイトが利用者に危険をもたらすことになるため、その安全性が確認できているボタン等のみを使用することが求められる。これはウェブページ等のコンテンツに限られず、本学が提供するアプリケーションプログラム内においても同様である。

第３項「学外へのアクセスを自動的に発生させる機能」について

学外へのアクセスを自動的に発生させる機能とは、例えば、本学が提供するウェブページの HTML ファイルに、<script src=”http://学外のサイト/foo.js”>等の記述があり、学外のウェブサイトからプログラムを読み込んで実行する機能が該当する。もし、学外のウェブサイトが提供するプログラムに不正なコードが含まれる場合、当該プログラムを使用した本学のウェブサイトが利用者に危険をもたらすことになるため、そのような機能をウェブページに含めることは可能な限り避けるべきである。具体的には、当該ファイルを本学ウェブサイトのサーバ上に置いて提供することで解決できる。これはウェブページ等のコンテンツに限られず、本学が提供するアプリケーションプログラム内においても同様である。

第４項「「https://」で始まる URL のウェブページから当該コンテンツをダウンロードできるように提供」について

情報システムの利用者が、現在閲覧しているウェブページが「https://」で始まる URL のウェブページであることを目視確認の上で、そこからリンクをクリックするなどしてファイルをダウンロードする手順を踏むことにより、当該ファイルは、暗号化された通信によって改ざんなくダウンロードされることになる。本項は、このような機能を利用者に提供することを求めたものである。

具体的には、本学が提供するウェブサイトのサーバで SSL（TLS）通信を利用

可能とし、「https://」で始まる URL での閲覧を可能とすればよい。
なお、そのときにダウンロードさせるファイル自身も SSL（TLS）通信を通じてダウンロードされるよう、当該ファイルへのリンクも「https://」で始まる URL としておく必要がある。

第二節　アプリケーション・コンテンツ提供時の対策

解説：本学では、教育研究事務に係る情報の提供、事務手続等のためにウェブサイト等を用意し、一般利用者等の利用に供している。これらのサービスは通常インターネットを介して利用するものであるため、一般利用者等にとっては、そのサービスが実際の本学のものであると確認できることが重要である。また、本学になりすましたウェブサイトを放置しておくと、本学の信用を損なうだけでなく、一般利用者等が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講ずる必要がある。

C2101-145　（A 大学ドメイン名の使用）（政府機関統一基準の対応項番 6.3.2(1)）

第百四十五条　部局技術責任者は、学外向けに提供するウェブサイト等が実際の本学提供のものであることを利用者が確認できるように、example.ac.jp で終わるドメイン名（以下「A 大学ドメイン名」という。）を情報システムにおいて使用するよう仕様に含めること。ただし、第七章第三節に掲げる場合を除く。

２　教職員等は、学外向けに提供するウェブサイト等の作成を外部委託する場合においては、前号と同様、A 大学ドメイン名を使用するよう調達仕様に含めること。

解説：第 1 項「example.ac.jp で終わるドメイン名（以下「A 大学ドメイン名」という。）を情報システムにおいて使用する」について
「.ac.jp で終わるドメイン名」は、株式会社日本レジストリサービスが定める「属性型（組織種別型）・地域型 JP ドメイン名登録等に関する規則」に基づき登録等を行うこととなっている。また、登録資格は、
(a) 学校教育法および他の法律の規定による次の組織
・学校（ED.JP ドメイン名の登録資格の(a)に該当するものを除く）
・大学共同利用機関
・大学校
・職業訓練校
(b) 学校法人、職業訓練法人、国立大学法人、大学共同利用機関法人、公立大学法人
とされている。
学外向けに提供するウェブサイト等が実際に本学が提供しているものであることを利用者が確認できるように、日頃から A 大学ドメイン名を用いることを徹底しておくことにより、なりすましが発生しても、学外の者がウェブサイト等の真偽を見分けることが容易なものとすることができる。
現在、外部で独自ドメイン名を低廉な費用で取得することが可能であるが、いったん実用に処したドメイン名は、実質的に半永久的にその利用者が利用権を維持する必要がある。いったんドメイン名の利用権を放棄すると、そのドメイ

ン名は他の事業者による用途（風俗的、反社会的な用途もあり得る）に転用（ドロップキャッチ）され、当初の用途を参照する目的でアクセスしてきた第三者の利用者に対して誤解等を生じさせる恐れがある。よって、目的に関わらず安易に外部のドメイン名を取得・利用することのないよう、教職員等への啓発を行うことも重要である。

A 大学ドメイン名を用いるべき場合の例を以下に示す。

・本学の出先機関等が組織の紹介サイトを提供する場合:A 大学ドメイン名は、本学が提供していることを示すものとして、閲覧者に理解される。サーバを外国に設置している場合であっても、当該サーバのホスト名として A 大学ドメイン名を設定することは可能である。

・本学が主催する講演会等に係るウェブサイトの提供において、参加者の登録をオンラインで行うために、ウェブサイト上で閲覧者に個人情報を入力させる場合：閲覧する者にとって、当該ウェブサイトが本学によって運営されているものであることの確認は、個人情報の入力を要する場合には特に重要となる。

・本学の広報活動として期間限定でキャンペーンサイトを広告会社に制作させ提供する場合：一時的に提供するウェブサイトを構築する場合や、広告会社に制作からサーバ管理までを委託する場合であっても、本学の公式な告知であると閲覧者が認識すべき内容である限りは、A 大学ドメイン名を用いるべきである。サーバが広告会社管理のもので、サーバに割り当てられた IP アドレスが学外のものであっても、そのホスト名として A 大学ドメイン名を用いることはできる。

第２項「調達仕様に含める」について

学外向けのウェブサイトを構築する場合に、情報システム部門以外の教職員等がウェブサイトの構築業務を外部委託することが考えられる。このような場合でも、学外の情報セキュリティ水準の低下を招かないよう、A 大学ドメイン名の使用を調達仕様に含めることが求められる。

C2101-146　（不正なウェブサイトへの誘導防止）（政府機関統一基準の対応項番 6.3.2(2)）

第百四十六条　部局技術責任者は、利用者が検索サイト等を経由して本学のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。

解説：「本学のウェブサイトになりすました不正なウェブサイト」について

学外の者が、本学の名前をタイトルに掲げるなどして、本学のウェブサイトと誤認されかねないウェブサイトを作成することがあり、これを完全に防ぐことはできない。本来ならば、利用者は当該サイトの URL 中のドメイン名が A 大学ドメイン名であるかを確認することで、本学のウェブサイトかを確認できるところであるが、検索サイト等を利用して本学名で検索して訪れる利用者も多いことから、検索サイトで検索したときに、正規の本学サイトが検索結果の上位に現れるようになっていることが望ましい。通常は、特別な対策をすることなく、そのような結果になることがほとんどであるが、正規の本学サイトの側で、不適切な設定になっていたり、コンテンツが適切に構成されていない場合

に、検索サイトで、正規の本学サイトが最上位に現れなかったり、適切な表示がなされないことがある。本条はそのような事態を防止するための措置を講ずることを求めている。

C2101-147　（検索サイトに係る対策）（政府機関統一基準の対応項番 6.3.2(2)-1,2）

第百四十七条　部局技術責任者は、学外向けに提供するウェブサイトに対して、以下を例とする検索エンジン最適化措置（SEO 対策）を講ずること。

一　クローラからのアクセスを排除しない。

二　cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする。

三　適切なタイトルを設定する。

四　不適切な誘導を行わない。

２　部局技術責任者は、学外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、不審なサイトへのアクセスを防止するための対策を講ずること。

解説：第１項「検索エンジン最適化措置（SEO 対策）」について

正規のウェブサイトが検索サイトで上位に現れるように正規のウェブサイト側で工夫を施すことを、一般に「検索エンジン最適化」又は「SEO 対策」と呼ぶ。本項は、本学サイトにおいても一般的な検索エンジン最適化の措置を講ずることを求めている。

第１項第１号「クローラからのアクセスを排除しない」について

一般に、検索サイトは、ウェブクローラと呼ばれる自動的にウェブサイトのリンクをたどって全てのページを巡回するプログラムを、自ら稼働させることによって収集した HTML データを用いて検索機能を実現している。そのため、検索サイトのクローラからのアクセスを拒否する設定をしている場合、当該サイトは検索サイトの検索結果に現れなくなることがある。そのような設定は、ウェブサイトの「/robots.txt」のファイルの記述で簡単にできるものであるため、誤ってクローラからのアクセスを拒否する設定にしてしまう状況が想定される。通常、このファイルを設定する必要はないため、何ら記述しないでおくことが望ましい。

第１項第２号「cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする」について

一般に、検索サイトが自ら稼働させるウェブクローラは、HTTP の cookie 機能に対応していない。そのため、cookie 機能を無効に設定したブラウザで閲覧したときに、正常に表示されないウェブページは、検索サイトの検索結果に正常に表示されない事態が起きる。通常のウェブサイトの構成では、cookie 機能を無効にしても正常に表示されるものであるが、一部の CMS（Content Management System）には、cookie を無効にして閲覧すると「cookie を有効にしてください」とだけ記述したエラー画面を表示するものがあり、そのような CMS を用いてウェブサイトを構成すると、前述の事態が生じる。実際に、

過去にそのような事態が発生した事例があるため、ウェブサイトの構築を外部委託する場合を含め、注意する必要がある。

第１項第３号「適切なタイトルを設定する」について
一般に、検索サイトの検索結果には、当該ページのタイトル（HTML 中の TITLE 要素で設定される文字列）が見出しとして表示され、利用者はこれを頼りにサイトを訪れることから、本学サイトにおいても、ページのタイトルに本学名を含めるなど、適切なタイトルを設定することが重要である。
その他の対策として、HTML 中の H1 要素や H2 要素を適切に記述することで、そこに含まれる単語や文で検索したときに、検索サイトの上位に当該ページが現れやすくなる。本学サイトにおいても、H1 要素や H2 要素を適切に記述することで、検索結果の上位に現れやすくすることができる。また、HTML 中のメタタグ（「description」や「keywords」等）に概要やキーワード等を記述することで、そこに含まれる単語や文で検索したときに、検索サイトの上位に当該ページが現れやすくなる。本学サイトにおいても、メタタグを適切に記述することで、検索結果の上位に現れやすくすることができる。

第１項第４号「不適切な誘導を行わない」について
一般に、HTML 中に見えない文字等でページ内容に関係のないキーワードを過剰に記述するなどして、当該ページへのアクセスを無用に誘う行為（「SEO スパム」等と呼ばれる。）は、不適切な行為として検索サイトからペナルティを科され、検索結果の上位に表示されなくなることがある。本学のウェブサイトにおいて、故意にそのような行為が行われることは考えにくいが、コンテンツの作成を外部委託した場合に、委託先が独自判断で行うことも想定されるため、そのようなコンテンツを作成しないよう注意が必要である。

第２項「不審なサイトへのアクセスを防止するための対策」について
不審なサイトを確認した場合は、本学のウェブサイト等において注意喚起を行うなどの対応を図るとともに、必要に応じて自組織や管理運営部局（情報メディアセンター）等の関係部門に状況を報告する。特に悪質な場合は、誤って当該サイトにアクセスすることを防止するため、検索サイト業者に対して検索結果に表示されないよう依頼する、本学 LAN からアクセスできないよう当該サイトに対してフィルタを設定する、といった対策が考えられる。

C2101-148　（学外のアプリケーション・コンテンツの告知）（政府機関統一基準の対応項番 6.3.2(3)）
第百四十八条　アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。
２　利用者等は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つこと。
解説：「学外の者が提供するアプリケーション・コンテンツを告知する」について

学外の者が提供するアプリケーション・コンテンツを告知する場合、告知を開始した時点では、当該アプリケーション・コンテンツが、告知した URL 等の誘導先に確かに存在していても、将来にわたりその誘導先に意図したアプリケーション・コンテンツが存在し続けるとは限らない。誘導先のドメイン名等が放棄された場合には、悪意ある者に当該ドメイン名が取得され、偽のアプリケーション・コンテンツに差し替えられる攻撃が想定される。したがって、学外の者が提供するアプリケーション・コンテンツを本学が告知する場合には、誘導先の有効性を保つことが求められる。

C2101-149　（アプリケーション・コンテンツの告知に係る対策）（政府機関統一基準の対応項番 6.3.2(3)-1,2,3）

第百四十九条　利用者等は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示すること。また、短縮 URL を用いないこと。

２　利用者等は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示すること。

３　利用者等は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つために以下の措置を講ずること。

一　告知するアプリケーション・コンテンツを管理する組織名を明記する。

二　告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する。

解説：第１項「URL 等を用いて直接誘導」について

URL を用いた直接誘導に該当する例としては、ウェブサイトにハイパーリンクを設ける場合のほか、電子メールに URL を記載して告知する場合、印刷物に URL を表示して誘導する場合等が挙げられる。URL「等」としているのは、例えば、ホスト名（FQDN 形式での表記）もこれに該当するものとする趣旨である。

第１項「検索サイトで指定の検索語を用いて検索することを促す方法」について

印刷物やテレビ CM により告知する際に、URL 等の文字列が長すぎると、利用者にその全部を入力させることが困難であることから、検索サイトで検索するよう検索語を指定して促す方法が広く普及している。

しかし、この誘導方法では、偽サイトや別のサイトに誘導されてしまうリスクを否定できない。検索結果の上位に目的の誘導先が現れない可能性があるだけでなく、検索サイトの広告部分に悪意あるサイトを出現させる攻撃手法も想定され、利用者が検索サイトの広告部分を誘導先として解釈してしまうおそれがある。

また、アプリケーション・コンテンツの告知を広告代理店に委託している場合、広告代理店が検索サイトの広告枠を購入し、広告部分を用いて目的の誘導先に

誘導する方法が用いられることがある。この誘導方法が広告代理店によって頻繁に用いられると、広告部分を正規の誘導先として利用者が解釈するようになると考えられ、広告部分に攻撃者による偽サイトが現れることのリスクを無視することはできなくなる。したがって、政府機関がアプリケーション・コンテンツを告知する場合には、検索サイトの広告枠を購入して誘導する方法は用いないようにすることが望ましい。

第１項「間接的な誘導方法を用いる場合」について
間接的な誘導方法を用いて本学の提供するアプリケーション・コンテンツを告知する場合は、当該誘導方法による誘導の状況を適時確認するなどして、不正な又は不適切なウェブサイトところへ誘導されてしまう可能性が高い状況になっているか否かを確かめることが望ましい。

第１項「URL 等と一体的に表示する」について
アプリケーション・コンテンツの告知は URL 等を用いて直接誘導することを原則とするが、間接的な誘導方法を用いたい場合があることも想定されることから、その場合に実施すべき措置として、間接的な誘導方法と一体的に URL 等を表示することを求めている。

第１項「短縮 URL を用いない」について
短縮 URL を提供する民間事業者のサービスは、将来にわたり永続的に運営が保証されるものではなく、いずれサービスが消滅し、ドメイン名が放棄されれば、悪意ある者に当該ドメイン名が取得され、偽のアプリケーション・コンテンツに差し替えられる攻撃が想定される。したがって、やむを得ない場合を除き、短縮 URL を用いるべきでない。やむを得ない場合の例としては、ソーシャルメディアサービスにおいて URL を告知する場合に、当該ソーシャルメディアサービスが強制的に所定の短縮 URL を用いてしまう場合が挙げられる。

第２項「アプリケーション・コンテンツの内容に係る記述を当該バーコードと一体的に表示」について
印刷物等でアプリケーション・コンテンツを告知する際に、URL 等の表示に代わるもの又は URL 等と一体的に表示するものとして、二次元コード等を用いて誘導する方法がある。この方法は、特にスマートフォンや携帯電話の利用者にとって利便性が高く、政府機関や教育機関においても用いられるようになってきている。
しかしながら、二次元コード等のみを単体で表示した場合、それがどこへ誘導するものであるかが、利用者にとって必ずしも明確でない場合がある。そこで、本項では、当該二次元コード等がどこへ誘導するものであるかを、当該二次元コード等と一体的に表示することにより利用者に明示することを求めている。
「アプリケーション・コンテンツの内容に係る記述」の例としては、誘導先の URL 等や、誘導先のアプリケーション・コンテンツの内容を示す記述が考えら

れる。

第３項「告知する URL 等の有効性を保つために以下の措置を講ずる」について
この措置を講ずるための対策事項第一号及び第二号について、具体的な記載例を以下に示す。
・本件についての問合わせは、〇〇@example.ac.jp までご連絡ください。
・このウェブサイトは〇〇学会が運営しており、A 大学が運営しているものではありません。
・このウェブサイトのアドレスについては、20〇〇年〇〇月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、ご自身でご確認ください。

第十四章　端末・サーバ装置等

第一節　端末

解説：端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等のおそれがある。また、利用者等の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。モバイル端末の利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。
なお、本節の遵守事項のほか、第１１章「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、第１２章第１節「ソフトウェアに関する脆弱性対策」、第１２章第２節「不正プログラム対策」、第１６章第２節「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

C2101-150　（端末の導入時の対策）（政府機関統一基準の対応項番 7.1.1(1)）

第百五十条　部局技術責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

２　部局技術責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。

３　部局技術責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

解説：第３項「利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める」について
利用を認めるソフトウェア及び利用を禁止するソフトウェアそれぞれのリストに登録する単位について、ソフトウェアの個別の製品名やバージョン単位で列

挙すると分かりやすいが、利用を禁止する全てのソフトウェアについて製品名等を個別に列挙するのが難しい場合は、例えば、個別に把握できるソフトウェアの製品名に加えてカテゴリ単位で登録することも考えられる。カテゴリ単位で登録する例としては、いわゆるピアツーピアで通信を行うソフトウェア、ファイル交換ソフトウェア、端末内の情報又は端末に入力した情報が自動で学外のサーバ装置等に送信されるソフトウェア、というような単位で定めておき、利用者に周知しておくと不要な手続が減らせるほか、利用者の意識向上にも寄与すると考えられる。また、情報セキュリティリスクを低減する観点からは、利用を認めるソフトウェアを極力限定することが望ましい。
利用者が端末にソフトウェアをインストールすることができるような環境においては、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて、利用者に周知徹底を図ることが重要である。

C2101-151　（物理的な脅威から保護するための対策）（政府機関統一基準の対応項番 7.1.1(1)-1,2,3）

第百五十一条　部局技術責任者は、モバイル端末を除く端末について、原則としてクラス２以上の要管理対策区域に設置すること。

２　部局技術責任者は、端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

一　モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。

二　モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意する。

３　部局技術責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。

一　一定時間操作が無いと自動的にスクリーンロックするよう設定する。

二　要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。

解説：第１項「原則としてクラス２以上の要管理対策区域に設置する」について
要保護情報を取り扱う端末はクラス２以上の区域に設置することが望ましい。クラス２より低位の区域に設置する必要がある場合は、利用者が常時目視できる場所への設置を義務付けるなど、クラス２の区域に設置する場合と同程度の安全性を確保するための代替の対策を講ずること。

第３項「第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずる」について
第三者による不正操作等の防止のための対策事項であるが、その他、端末の操作のロックの解除に IC カード等の主体認証情報格納装置を使用し、主体認証情報格納装置が無い状態で又は操作の無い状態が一定時間続くことで端末の操作がロックされるようにし、かつ、当該主体認証情報格納装置を教室、研究室、事務室への立入りの確認にも利用するという方法が考えられる（これにより、

利用者が教室、研究室、事務室の外にいる際には端末の操作が確実にロックできる)。
また、正規の利用者による不正操作や誤操作の防止策として、端末が備える機能のうち、利用しない機能を停止することが考えられる。停止する機能の例としては、無線 LAN 等の通信用のインタフェース、USB ポート等の外部電磁的記録媒体を接続するためのインタフェース、マイク、ウェブカメラ等が考えられる。

C2101-152　(第三者により情報窃取されることを防止するための対策)(政府機関統一基準の対応項番 7.1.1(1)-4)

第百五十二条　部局技術責任者は、第三者により情報窃取されることを防止するために、以下を例とする、端末に保存される情報を暗号化するための機能又は利用者が端末に情報を保存できないようにするための機能を設けること。

一　端末に、ハードディスク等の電磁的記録媒体全体を暗号化する機能を設ける。

二　端末に、ファイルを暗号化する機能を設ける。

三　ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。

四　シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。

五　セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。

六　ハードディスク等電磁的記録媒体に保存されている情報を遠隔から消去する機能(遠隔データ消去機能)を設ける。

解説:「暗号化」について

モバイル端末が第三者の者の手に渡った場合には、モバイル端末から取り外された内蔵電磁的記録媒体や、モバイル端末で利用していた外部電磁的記録媒体に保存されている情報を他の端末を利用して解読するなどの手段によって要機密情報が窃取される危険性がある。このような情報の窃取への対策として、端末に暗号化機能を搭載することが有効である。
暗号化する方法としては、ハードディスク全体又はファイル単体を暗号化するソフトウェアの導入や OS が備えている暗号化機能を使用することが挙げられる。その他、第 3 号の「ファイル暗号化等のセキュリティ機能を持つアプリケーション」を用いる方法もある。
ハードディスク全体を暗号化している場合でも、端末の起動中等の復号可能な状態で盗難等に遭った場合には情報窃取されるおそれがあるため、第 6 号の「遠隔データ消去機能」と組み合わせて用いると情報窃取される可能性をより低減できる。
また、暗号化を行う場合は鍵の管理が重要になる。鍵の管理の方法として、端末内の耐タンパ性を備えた TPM(Trusted Platform Module)を利用する方法や、鍵を USB セキュリティトークンに格納して、利用時以外は端末とは別に管理するという方法等が考えられる。

第３号「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について
第二百三十一条「(解説）第３号「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について」を参照のこと。

第４号「シンクライアント等」について
第二百三十一条「(解説）第１号「シンクライアント等」について」を参照のこと。

第５号「セキュアブラウザ等」について
第二百三十一条「(解説）第２号「セキュアブラウザ等」について」を参照のこと。

第６号「遠隔データ消去機能」について
端末の通信機能を利用して、遠隔から端末内のデータを消去する機能であるが、通信が確立できないために遠隔からデータ消去できない場合に備え、主体認証の失敗した回数をカウントして一定数を超えた際に消去するなど特定の条件で自律的に消去する機能についても考慮するとよい。また、データ消去ではなく、端末の操作をロックするという対策も考えられる。

C2101-153　（端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアに係る対策）（政府機関統一基準の対応項番 7.1.1(1)-5）

第百五十三条　部局技術責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。

一　ソフトウェアベンダのサポート状況

二　ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容

三　インストール時に同時にインストールされる他のソフトウェア

四　その他、ソフトウェアの利用に伴う情報セキュリティリスク

解説:「利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める」について
利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める際には、以下を行うことが考えられる。
・ソフトウェアベンダによるセキュリティパッチ等のサポートが提供されていることや、セキュリティベンダ等の第三者が提供するソフトウェアの脆弱性等に関する情報を確認する。
・外部と通信を行う機能を有することが明確なもの又は外部との通信の有無について利用規約により確認できるものについては、当該機能による通信内容を事前に確認する。
・インストール時に、他のソフトウェアのインストールの同意を求めるものについては、当該ソフトウェアの利用の可否についても併せて定める。

・ブラウザ等のソフトウェアで利用される機能拡張用のソフトウェア（いわゆる、プラグインやアドオン）の利用の可否についても併せて定める。
また、一度利用を認めたソフトウェアであっても、バージョンが上がった際に、旧バージョンと比べ、機能が変わったり、同時にインストールされる他のソフトウェアが追加されたりする場合があるので、利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める際には、バージョンも含めて定めることが重要である。なお、ソフトウェアによっては、バージョンによらず一律で利用を禁止するソフトウェアに指定できる場合もある。

C2101-154　（端末の運用時の対策）（政府機関統一基準の対応項番 7.1.1(2)）

第百五十四条　部局技術責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

２　部局技術責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

解説：第１項「見直しを行う」について

ソフトウェアのバージョン更新、サポート期限切れ、新しいソフトウェアの出現等に適切に対応するため、また、利用者の要求に柔軟に対応するため、利用を認めるソフトウェア及び利用を禁止するソフトウェアの見直しを行うことが必要である。
「定期的」以外の見直しの契機として、端末の利用者から利用を認めるソフトウェア以外のソフトウェアの利用承認の申請（第１７章「情報システムの利用」を参照のこと。）を受け付けたときが考えられる。申請のあったソフトウェアについて、引き続き利用を認める場合には、利用を認めるソフトウェアのリストに追加し、引き続き利用を禁止する場合には、利用を禁止するソフトウェアのリストに追加することで、一つのソフトウェアにつき１回の手続で済ませることができる。

第２項「不適切な状態にある端末を検出等した場合には、改善を図る」について

「不適切な状態」とは、利用を認めるソフトウェア以外のソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていないなどの状態のことをいう。
利用を認めるソフトウェア以外のソフトウェアが稼働している場合には、当該ソフトウェアを停止する、又は削除する必要がある。セキュリティパッチについては、第１２章第１節「ソフトウェアに関する脆弱性対策」を参照のこと。

C2101-155　（端末の運用終了時の対策）（政府機関統一基準の対応項番 7.1.1(3)）

第百五十五条　部局技術責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

解説：「端末の運用を終了する際」について

端末を廃棄処分する場合やリース契約が終了し端末を返却する場合が考えられ

る。

「抹消する」について
抹消の方法については、第五十条「(解説) 第２項「抹消する」について」を参照のこと。
なお、運用を外部委託しているなど、調達元の本学において抹消できない場合においては、保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずることが必要である。

第二節　サーバ装置

解説：電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に本学が有するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、社会からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。
なお、本節の遵守事項のほか、第１１章「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、第１２章第１節「ソフトウェアに関する脆弱性対策」、第１２章第２節「不正プログラム対策」、第１２章第３節「サービス不能攻撃対策」、第１６章第２節「IPv6 通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベースについては、本節での共通的な対策に加え、それぞれ第１５章「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。

C2101-156　（サーバ装置の導入時の対策）（政府機関統一基準の対応項番 7.1.2(1)）

第百五十六条　部局技術責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

２　部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。

３　部局技術責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

４　部局技術責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報

が漏えいすることを防止するための対策を講ずること。

解説：第３項「利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める」について

第百五十条「(解説）第３項「利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める」について」を参照のこと。

第４項「保守作業を行う際に送受信される情報が漏えいすることを防止するための対策」について

部局技術責任者から保守作業を許可されている者がサーバ装置へログインして作業する場合を想定し、例えばインターネットを介してサーバ装置の保守作業を行う場合等、通信内容を秘匿する必要がある場合には、サーバ装置の設置時に暗号化するための機能を設け、運用時に情報の暗号化を実施できるようにしておくこと等が考えられる。

C2101-157　（物理的な脅威から保護するための対策）（政府機関統一基準の対応項番 7.1.2(1)-1,2,3）

第百五十七条　部局技術責任者は、要保護情報を取り扱うサーバ装置については、クラス２以上の要管理対策区域に設置すること。

２　部局技術責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

一　施錠可能なサーバラックに設置して施錠する。

二　容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

３　部局技術責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。

一　一定時間操作が無いと自動的にスクリーンロックするよう設定する。

解説：第１項「クラス２以上の要管理対策区域に設置する」について

サーバ装置に関しては、取り扱う情報の重要性に応じてクラス３の区域に設置することも考慮するとよい。また、クラス２の区域（教室、研究室、事務室等）に設置する場合においても常時施錠されたサーバラックに置くことも考慮するとよい。

C2101-158　（可用性を確保するための対策）（政府機関統一基準の対応項番 7.1.2(1)-4）

第百五十八条　部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため要安定情報を取り扱う情報システムについては、将来の見通しも考慮し、以下を例とする対策を講ずること。

一　負荷分散装置、DNS ラウンドロビン方式を利用した等による負荷分散

四　同一システムを２系統で構成することによる冗長化

解説：第４号「冗長化」について

「冗長化」とは、障害や過度のアクセスが発生した場合を想定し、サービスを提供するサーバ装置を代替サーバ装置に切り替えること等により、サービスが

中断しないように、情報システムを構成することである。可用性を高めるためには、サーバ装置本体だけでなく、ハードディスク等のコンポーネント単位で冗長化することも考えられる。
なお、災害等を想定して冗長化する場合には、代替のサーバ装置を遠隔地に設置することが望ましい。

C2101-159　（サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアに係る対策）（政府機関統一基準の対応項番 7.1.2(1)-5）

第百五十九条　部局技術責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。

一　ソフトウェアベンダのサポート状況

二　ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容

三　インストール時に同時にインストールされる他のソフトウェア

四　その他、ソフトウェアの利用に伴う情報セキュリティリスク

解説:「利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める」について
第百五十三条「（解説）「利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める」について」を参照のこと。

C2101-160　（サーバ装置の運用時の対策）（政府機関統一基準の対応項番 7.1.2(2)）

第百六十条　部局技術責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

２　部局技術責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図ること。

３　部局技術責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

４　部局技術責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講ずること。

解説：第１項「見直しを行う」について
ソフトウェアのバージョン更新、サポート期限切れ、新しいソフトウェアの出現等に適切に対応するため、定期的に利用を認めるソフトウェア及び利用を禁止するソフトウェアの見直しを行うことが必要である。

第２項「不適切な状態にあるサーバ装置を検出等した場合には改善を図る」について
「不適切な状態」とは、サーバ装置のハードウェアの構成が不正に変更されている、又はセキュリティ水準の低下を招くような変更がされている、利用を認めるソフトウェア以外のソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていないなどの状態のことをいう。

利用を認めるソフトウェア以外のソフトウェアがインストールされているか否かについては、構成管理ツールを使用するほか、プロセスやその他挙動等を監視する方法もある。また、利用を認めるソフトウェアであっても、利用しない機能については無効化するなどの措置が考えられる。セキュリティパッチについては、第１２章第１節「ソフトウェアに関する脆弱性対策」を参照のこと。

C2101-161　（サーバ装置の運用管理作業の記録に係る対策）（政府機関統一基準の対応項番 7.1.2(2)-1）

第百六十一条　部局技術責任者は、所管する範囲内のサーバ装置の構成やソフトウェアの状態を定期的に確認する場合は、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。

C2101-162　（サーバ装置の監視に係る対策）（政府機関統一基準の対応項番 7.1.2(2)-2）

第百六十二条　部局技術責任者は、サーバ装置への無許可のアクセス等の不正な行為を監視するために、以下を例とする対策を講ずること。

一　アクセスログ等を定期的に確認する。

二　IDS/IPS、WAF 等を設置する。

三　不正プログラム対策ソフトウェアを利用する。

四　ファイル完全性チェックツールを利用する。

五　CPU、メモリ、ディスク I/O 等のシステム状態を確認する。

解説：第１号「アクセスログ等を定期的に確認する」について

不正アクセスを検知するために、サーバ装置へのアクセスに関するログのほか、サーバ装置が異常等を検出した際に出力するログ（エラーログ）を確認することも有効である。

アクセスログを確認する際は、運用管理作業の記録、管理者権限を持つ識別コードを付与された者の出退勤記録又は入退室記録等との相関分析を併せて行うことにより、不正なアクセスが行われた可能性を確認することも考えられる。

C2101-163　（サーバ装置の復元に係る対策）（政府機関統一基準の対応項番 7.1.2(2)-3）

第百六十三条　部局技術責任者は、要安定情報を取り扱うサーバ装置については、運用状態を復元するために以下を例とする対策を講ずること。

一　サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。

二　定期的なバックアップを実施する。

三　サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。

四　バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。

解説：第２号「バックアップ」について

バックアップには、サービスの提供に当たって必要なデータやサービスの利用者が入力したデータのバックアップのほか、運用に必要となるシステム設定のバックアップも含まれる。バックアップの取得方法として、前回内容からの変

更部分のみバックアップを実施する方法でもよい。
なお、バックアップの手段や保管場所については、第五十三条「(解説)「災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定する」について」も参照のこと。

C2101-164　(サーバ装置の運用終了時の対策)(政府機関統一基準の対応項番 7.1.2(3))
第百六十四条　部局技術責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。

解説:「サーバ装置の運用を終了する際」について
サーバ装置を廃棄処分する場合やリース契約が終了し返却する場合のほか、当該サーバ装置のサービス又は機能の提供を終了する場合も考えられる。

「抹消する」について
第百五十五条「(解説)「抹消する」について」を参照のこと。

第三節　複合機・特定用途機器

解説:本学においては、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている複合機が利用されている。複合機は、学内通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。
また、本学においては、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。
したがって、複合機や特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずることが重要である。

C2101-165　(複合機)(政府機関統一基準の対応項番 7.1.3(1))
第百六十五条　部局技術責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。
2　部局技術責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。
3　部局技術責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。

C2101-166　(複合機の導入時の対策)(政府機関統一基準の対応項番 7.1.3(1)-1)
第百六十六条　部局技術責任者は、「IT 製品の調達におけるセキュリティ要件リスト」を参照するなどし、複合機が備える機能、設置環境及び取り扱う情報の格付及び取扱制限に応じ、当該複

合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記すること。

解説：「「IT 製品の調達におけるセキュリティ要件リスト」を参照」について

第９章第１節「情報システムの企画・要件定義」の第八十条第３項及び第八十二条に記載されている「IT 製品の調達におけるセキュリティ要件リスト」には、複合機について一般的に想定される「セキュリティ上の脅威」が記載されているため、それらが自身の運用環境において該当する場合には対抗する必要がある。当該リストには、「国際標準に基づくセキュリティ要件」が記載されており、それを調達時に活用することで脅威に対抗するための機能を有した製品を調達することが可能となる。

なお、「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」のうち、利用環境や複合機に実装されている機能によっては、一部の脅威だけに対抗すればよい場合もあり得る。そのような場合には、「国際標準に基づくセキュリティ要件」では過剰な要件（要求仕様）となる可能性もあるので、個別にセキュリティ要件を策定して脅威に対抗してもよい。

C2101-167　（複合機の運用時の対策）（政府機関統一基準の対応項番 7.1.3(1)-2）

第百六十七条　部局技術責任者は、以下を例とする運用中の複合機に対する、情報セキュリティインシデントへの対策を講ずること。

一　複合機について、利用環境に応じた適切なセキュリティ設定を実施する。

二　複合機が備える機能のうち利用しない機能を停止する。

三　印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用する。

四　学内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする。

五　複合機をインターネットに直接接続しない。

六　リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

七　利用者ごとに許可される操作を適切に設定する。

解説：第１号「適切なセキュリティ設定」について

自身の利用環境における脅威に対抗するために、運用前に複合機のセキュリティ機能の設定値が適切な値となっていることを確認する必要がある。例えば、管理者パスワードが初期設定のままでないか、イメージスキャナで複合機内部に保存したデータへのアクセス制御設定が適切であるかなどを確認する必要がある。

第２号「利用しない機能を停止」について

運用において必要としていない機能が利用者の意図に反して動作していた場合、セキュリティ対策が不十分になっていることが考えられる。対策が不十分である場合は、情報セキュリティインシデントが発生するおそれがあるため、運用上不必要な機能については、運用前に停止した状態にする必要がある。

第３号「操作パネルで利用者認証が成功した者のみ印刷が許可される機能」について
複合機の設置環境によっては、印刷された文書が第三者に閲覧される可能性がある。そのような場合には、印刷の際に複合機内部に一旦データを保存し、複合機本体の操作パネルで主体認証に成功した者だけが印刷できるように設定しておくなどの対策を講ずる必要がある。

第４号「複合機の内部において接続されないようにする」について
複合機にモデム機能が搭載されている場合、公衆通信回線から複合機に接続された後に、複合機を経由して本学 LAN にアクセスされる可能性がある。そのため、モデム機能の無効化等の対策が必要となる。

第６号「ファイアウォール等の利用により適切に通信制御を行う」について
トナー残量の通知や遠隔地からの状態監視等の遠隔保守サービス等を利用する場合には、インターネットを介して外部と通信する必要が生じる。その際には必要最小限の通信のみを許可するようにする必要がある。また、ファイアウォール等の通信制御を行うための機器に例外的な設定を行う場合には、その設定によって脆弱性が生じないようにする必要がある。

第７号「利用者ごとに許可される操作を適切に設定する」について
様々な機能を備えている複合機では、利用者ごとに許可される操作権限の管理が重要となる。例えば、ファクシミリで受信したデータを複合機内部に保存する場合のデータの読み出し権限等を適切に設定していない場合には、情報の漏えいにつながる可能性がある。

C2101-168　（複合機の運用終了時の対策）（政府機関統一基準の対応項番 7.1.3(1)-3）
第百六十八条　部局技術責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消すること。当該機能を備えていない複合機については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずること。

解説：「別の手段で対策を講ずる」について
内蔵電磁的記録媒体の全領域完全消去機能を備えていない複合機については、調達元の本学において内蔵電磁的記録媒体の全ての情報を抹消することが困難であるため、外部委託先と情報の抹消サービスを契約するなどの情報の漏えいへの対策を講ずることが必要となる。

C2101-169　（特定用途機器）（政府機関統一基準の対応項番 7.1.3(2)）
第百六十九条　部局技術責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。

解説：「当該機器の特性に応じた対策を講ずる」について

例えば、テレビ会議システム、IP 電話システム等は本学 LAN を経由してインターネットに接続されて利用されることが想定され、その場合外部からの攻撃対象となり得る。また、これら情報システムを構成する機器が内蔵電磁的記録媒体を備える場合は、運用終了時に内蔵電磁的記録媒体に残された情報が漏えいするおそれがある。

このような脅威に対抗するために、情報システムや端末、サーバ装置に対して定められた遵守事項を参考にして、情報システム、特定用途機器の特性に応じて対策を講ずるとよい。

C2101-170　（特定用途機器の運用時の対策）（政府機関統一基準の対応項番 7.1.3(2)-1）

第百七十条　部局技術責任者は、特定用途機器の特性に応じて、以下を例とする対策を講ずること。

一　特定用途機器について、利用環境に応じた適切なセキュリティ設定を実施する。

二　特定用途機器が備える機能のうち利用しない機能を停止する。

三　特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

四　インターネットに接続されている特定用途機器についてソフトウェアに関する脆弱性が存在しないか確認し、脆弱性が存在する場合、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。

五　特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。

六　特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消すること。

解説：第４号「バージョンアップやセキュリティパッチの適用」について

調達元の本学で対処できないような機器の場合には、特定用途機器の調達に当たって保守契約締結の必要性等について検討することも重要である。

第十五章　電子メール・ウェブ等

第一節　電子メール

解説：電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する利用者等が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本章の遵守事項のほか、第１４章第２節「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

C2101-171　（電子メールの導入時の対策）（政府機関統一基準の対応項番 7.2.1(1)）

第百七十一条　部局技術責任者は、電子メールサーバが電子メールの不正な中継を行わないよう

に設定すること。

２　部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

３　部局技術責任者は、電子メールのなりすましの防止策を講ずること。

解説：第１項「不正な中継」について

不正な中継が行われると、迷惑メールの送信等に悪用される問題がある。これにより、電子メールサーバや通信回線のリソースが消費されて運用に支障をきたす、不正な中継を行う電子メールサーバとして他の電子メールサーバ等から接続や電子メールの転送を拒否される、又は迷惑メールの受信者からの苦情や問合わせへの対応が必要になるなどの問題が生じるおそれがある。これらを回避するため、電子メールの不正な中継を行わないように電子メールサーバを設定することが必要である。

C2101-172　（電子メールの受信時及び送信時の主体認証）（政府機関統一基準の対応項番 7.2.1(1)-1）

第百七十二条　部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする利用者等の主体認証を行う機能を備えること。

一　電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入する。

C2101-173　（電子メールのなりすましの防止）（政府機関統一基準の対応項番 7.2.1(1)-2）

第百七十三条　部局技術責任者は、以下を例とする電子メールのなりすましの防止策を講ずること。

一　SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）等の送信ドメイン認証技術による送信側の対策を行う。

二　SPF、DKIM、DMARC 等の送信ドメイン認証技術による受信側の対策を行う。

三　S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用する。

解説：第１号「送信ドメイン認証技術」について

送信ドメイン認証技術には、SPF、DKIM 等が挙げられる。これらは、送信する電子メールのドメインを管理する DNS サーバに登録・公開された、送信側の電子メールサーバの情報や電子署名で使用する公開鍵を利用することで実現する。

また、送信ドメイン認証技術によって電子メールのなりすましを防止するためには、送信した電子メールの正当性を受信者が確認できるようにするための送信側の対策と、受信した電子メールの正当性を判定して、なりすまされた電子メールから受信者を保護するための受信側の対策があり、両方の実施が求められる。

DMARC は、送信元ドメインに対し、効果的な認証基準が得られるよう、認証技術を自身のインフラに実装するに当たっての、より統合的な手法を定義する

とともに、電子メールの受信者が SPF、DKIM 等に係る送信ドメイン認証の詳細な結果を電子メールの送信者にフィードバックするフレームワークを実現するための仕様である。

第１号「送信側の対策」について
送信ドメイン認証技術による送信側の対策として、電子メールで使用するドメインを管理する DNS サーバに、受信者が電子メールの正当性を確認するための情報を登録し公開する必要がある。例えば、SPF の場合は送信側の電子メールサーバの情報を DNS サーバに登録する。また、DKIM の場合は電子メールに付与する電子署名の検証に使用する公開鍵を DNS サーバに登録する。
なお、SPF については、以下の事項に留意すること。
・電子メールを利用していないドメインについても、その情報を SPF レコードに登録する。(「SPF レコード」とは、SPF において、DNS サーバの TXT レコードに記述される送信側の電子メールサーバ等の情報をいう。)
・SPF レコードの末尾は、”~all”ではなく”-all”を記述する。
・SPF レコードは、チェックツール等で、文法的に記述間違いのないことを確認する。
・なりすましの防止策のため、ウェブによるサービス等も含め全く利用していない、又は将来にわたって利用の予定の無いドメインについては、なりすましの防止策を講ずるか、ドメイン名の登録を廃止する。
・民間事業者等において提供されている、他の利用者と共用する電子メールサービスを利用する場合は、本学をなりすました電子メールが、当該電子メールサービスを利用する他の利用者から送信されないような仕組みを備えていることを確認する。他の利用者と共用しない専用の IP アドレスを割り振ることが可能なサービスが提供されている場合は、当該サービスの利用を検討する。

第２号「受信側の対策」について
送信ドメイン認証技術による受信側の対策としては、受信した電子メールに対し送信ドメイン認証に基づくなりすまし判定（例えば SPF の場合、受信時に通信を行った送信側の電子メールサーバと、受信した電子メールに記載されている送信側ドメインを管理する DNS サーバに登録されている送信側の電子メールサーバの情報との比較による判定）を行い、なりすましと判定した場合には、以下に例示するような電子メールの受信者への注意喚起等を行うことが挙げられる。
・電子メールの件名（Subject）や本文への注意喚起文の挿入
・電子メールクライアントの機能によるラベリングやメッセージの表示
・電子メールクライアント又は電子メールサーバにおける電子メールの隔離や削除等のフィルタリング
また、送信者が DMARC に対応している場合は、送信者のポリシーに従って隔離や受信自体の拒否を行うことが可能となる。

第３号「S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名」について
外部に一斉送信する電子メールに、組織の電子証明書で電子署名をすることは、電子メールのなりすまし防止の観点から効果的である。
また、通常のメールについては、職員に電子証明書を配布し、電子署名を付与することにより、電子メールクライアントによっては、同時に電子メールを自動的に暗号化することが可能となるというメリットもある。

第二節　ウェブ

解説：インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ（ウェブページとして公開している情報）の改ざん、ウェブサーバの利用停止、偽サイトへの誘導等の被害が想定されるため、適切な対策を組み合わせて実施することが求められる。
なお、本章の遵守事項のほか、第１４章第２節「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

C2101-174　（ウェブサーバの導入・運用時の対策）（政府機関統一基準の対応項番 7.2.2(1)）

第百七十四条　部局技術責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずること。

一　ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

二　ウェブコンテンツの編集作業を担当する主体を限定すること。

三　公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。

四　ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。

五　サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。

２　部局技術責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

C2101-175　（ウェブサーバの管理や設定）（政府機関統一基準の対応項番 7.2.2(1)-1,2,3,4,5）

第百七十五条　部局技術責任者は、不要な機能の停止又は制限として、以下を例とするウェブサーバの管理や設定を行うこと。

一　CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする。

二　ディレクトリインデックスの表示を禁止する。

三　ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する。

四　ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。

２　部局技術責任者は、ウェブコンテンツの編集作業を担当する主体の限定として、以下を例と

するウェブサーバの管理や設定を行うこと。

一　ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えない。

二　OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。

3　部局技術責任者は、公開してはならない又は無意味なウェブコンテンツが公開されないよう管理することとして、以下を例とするウェブサーバの管理や設定を行うこと。

一　公開を想定していないファイルをウェブ公開用ディレクトリに置かない。

二　初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。

4　部局技術責任者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行うこと。

一　ウェブコンテンツの更新の際は、専用の端末を使用して行う。

二　ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する。

三　ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行う。

5　部局技術責任者は、通信時の盗聴による第三者への情報の漏えいの防止及び正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を例とするウェブサーバの実装を行うこと。

一　SSL（TLS）機能を適切に用いる。

二　SSL（TLS）機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる。

三　暗号技術検討会及び関連委員会（CRYPTREC）により作成された「SSL/TLS 暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する。

解説：第 1 項第 1 号「CGI 機能」について

CGI（Common Gateway Interface）とは、ウェブブラウザから送信された文字列を、スクリプト等のプログラムへの入力パラメータとして受け取り、当該スクリプト等をウェブサーバ上で実行するための仕組みである。外部からの文字列に基づいて実行されるスクリプト等は脆弱性の原因となり易い部分であり、細心の注意を払って脆弱性の無いスクリプト等のみを設置しなければならない。そのため、本号は、サーバに設置するスクリプト等は必要最低限のものに限定することを求めている。

第 1 項第 2 号「ディレクトリインデックスの表示を禁止する」について

ウェブサーバの機能であるディレクトリインデックスの表示機能とは、ウェブサイトの公開対象となるディレクトリが、ファイル名を指定しない形式の URL（すなわち、例えば「http://exmaple.ac.jp/directory_name/」の形式）又は「index.html」等の所定のファイル名を指定した形式の URL によってアクセスされたときに、当該ディレクトリに存在するファイル名の一覧を自動的に生成して表示する機能である。万が一、公開するつもりのないファイルがディレ

クトリに混入していた場合、ディレクトリインデックス機能が有効であると、外部から容易にそのファイル名を見つけられてしまい、アクセスされてしまう。本来、公開対象のディレクトリには、非公開にすべきファイルが混入していてはならないところであるが、念のため、本号は、ディレクトリインデックスの表示機能を無効にすることを求めている。

第１項第３号「不要な機能を制限する」について
不要な機能の典型的な例としては、管理者画面の機能が挙げられる。ウェブコンテンツ作成ツールや CMS には、コンテンツを編集する管理者向けのログイン画面を有するものがある。このログイン画面がインターネットから閲覧可能であると、管理者のパスワードを破って不正にログインされ、ウェブサイトのコンテンツを改ざんされるリスクを生じさせる。管理者画面は、学内からのアクセスのみを許可し、インターネットからの利用を制限することを求めている。その他の不要な機能として制限すべき例として、アクセス解析の機能がインターネットから閲覧できるようになっている場合等が挙げられる。

第４項第１号「専用の端末」について
ウェブコンテンツを管理する端末では、ウェブコンテンツの管理に関係する作業のみを行い、その作業に関係の無いウェブサイトを閲覧しない、セキュリティ対策が不十分な USB メモリを利用しないなど、情報セキュリティを確保した運用が必要である。また、ウェブサーバのみでなく、ウェブコンテンツを管理する専用の端末においても、不正プログラム対策やソフトウェアに関する脆弱性対策を行うことが重要である。

第４項第３号「情報セキュリティを確保した管理」について
ウェブコンテンツを更新する際の主体認証情報について、パスワードを設定する場合は十分な長さと複雑さを持ったものとする、多要素主体認証方式で主体認証を行う機能を設けるなどにより、情報セキュリティを確保することが求められる。また、ウェブコンテンツの更新に利用する識別コードや主体認証情報は、他の情報システムの認証で使用しているものを使い回さない、ウェブコンテンツを更新する者以外に知らせない、複数の更新を実施する者で共有しないなどの情報セキュリティを確保した管理が求められる。

第５項第１号「TLS（SSL）機能を適切に用いる」について
ウェブサーバに TLS（SSL）機能を搭載することにより、利用者が当該ウェブサーバのサイトを「https://」で始まる URL でアクセスできるようになる。「https://」で始まる URL のページ（以下「セキュアページ」という。）へのアクセスは、ブラウザからウェブサーバへの入力及びウェブサーバからブラウザへの出力が自動的に暗号化されて送受信される。
盗聴による情報の漏えいを防止するには、盗聴を防ぐべき情報を出力するウェブページがセキュアページとなっていることが必要である。また、盗聴を防ぐ

べき情報を利用者に入力させるウェブページを設ける場合には、入力された情報の送信先となる URL がセキュアページとなっていることが必要であり、かつ、利用者に情報を入力させるウェブページ（入力欄が設置されている画面）自体もセキュアページとなっていることが必要である。
ウェブサーバに TLS（SSL）機能を搭載することは、当該ウェブサーバが正当なサーバである（偽のサーバでない）ことを確認できる手段を利用者に提供することにもなる。利用者は、当該サイトを「https://」で始まる URL でアクセスし、エラーなく正常に表示されたことで、当該サーバが当該ドメイン名の正当なサイトのものであると確認することができる。
なお、TLS（SSL）機能を用いるに当たっては、使用するバージョンの脆弱性に関する最新の情報も踏まえ、適切に使用することが必要である。

第５項第２号「利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局」について
TLS（SSL）機能を用いるには、ウェブサーバ側に「サーバ証明書」と呼ばれる電子証明書の設置が必要であり、サーバ証明書はそれを発行する「認証局」から取得する必要がある。サーバ証明書の取得は、国立情報学研究所 UPKI 電子証明書発行サービス（UPKI）の「利用申請」から取得することもできるほか、民間事業者から取得することもできる。
本号は、サーバ証明書をどの認証局から取得するかの選択において、「利用者が事前のルート証明書のインストールを必要とすることなくその正当性を検証できる認証局」を選択することを求めている。それ以外の認証局を選択した場合、利用者のウェブブラウザには、サーバ証明書の正当性検証ができないことを示す警告やエラー画面が表示されることになる。この警告やエラー画面は、事前に当該認証局の自己署名証明書をブラウザにルート証明書としてインストールすることによって解消することができる。しかし、一般に、利用者によるルート証明書のインストールは安全に行うことが容易でないものであり、利用者に危険を伴うルート証明書のインストールを強いるのはそもそも避けるべきことである。そのため、本号は、利用者にルート証明書のインストールを求めなくても、警告やエラー画面が現れることなく、正常に TLS（SSL）通信ができるよう、適切に認証局を選択してサーバ証明書を取得することを求めている。
なお、ウェブサーバの利用が学内の管理された端末からのアクセスに限定されている場合には、対象となる全ての端末に対して事前に安全な方法でルート証明書をインストールすることも可能であるから、そのような管理がなされている場合には、当該ウェブサーバで使用するサーバ証明書として、本学で独自に用意した認証局から発行されたものを用いることができる。

第５項第３号「「SSL/TLS 暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する」について
CRYPTREC が発行している「SSL/TLS 暗号設定ガイドライン」は、TLS（SSL）通信での安全性と可用性（相互接続性）のバランスを踏まえた TLS（SSL）サ

ーバの設定方法のガイドラインを示すものである。
このガイドラインでは、「高セキュリティ型」、「推奨セキュリティ型」、「セキュリティ例外型」の 3 段階の設定基準に分けて、各々の要求設定が示されており、どの設定基準を採用するかは、安全性の確保と相互接続の必要性の両面を鑑みてサーバ管理者が選択するものとされている。
「高セキュリティ型」は、利用例として「政府内利用（G2G 型）のなかでも、限定された接続先に対して、とりわけ高い安全性が要求される通信を行う場合」が示されているように、一般の利用者がウェブブラウザ等で接続することのないサーバの場合を対象とし、専用システム内又は専用システム間で閉じたネットワークを構成して暗号化通信に TLS（SSL）を用いる際に選択すべき設定基準である。
他方、「推奨セキュリティ型」は、利用例に「電子申請等、企業・国民と役所等の電子行政サービスを提供する場合」とあるように、一般の利用者がウェブブラウザで接続することを前提としたサーバを構成する場合に選択する設定基準であり、普及している PC、スマートフォン等で問題なく相互接続性を確保できる要求設定が示されたものである。
ガイドラインは、巻末に付録として「チェックリスト」を提供しており、ここに、設定基準ごとに満たすべき要求設定として「プロトコルバージョン設定」、「サーバ証明書設定」、「暗号スイート設定」の具体的な基準が示されているので、これに従うことで、容易に適切な TLS（SSL）設定を行うことができる。
部局技術責任者は、TLS（SSL）を導入するシステムの特性に応じて、どの設定基準が相応しいかを決定し、その設定基準に対応する要求設定に従ったサーバ設定を、「チェックリスト」を活用して確認するなどして、適切に行うことが求められる。
また、ガイドラインは、「サーバ証明書の作成・管理について注意すべきこと」として、鍵ペアの適切な生成方法や鍵の適切な管理方法を示し、また、「さらに安全性を高めるために」として、HTTP Strict Transport Security (HSTS) の設定有効化その他を推奨している。これらについても併せて検討することが望ましい。

参考：CRYPTREC「SSL/TLS 暗号設定ガイドライン」（平成 27 年 8 月 3 日）
（http://www.cryptrec.go.jp/report/c14_oper_guideline_SSLTLS_web_1_1.pdf）

上記のウェブサイトのアドレスは、平成 29 年 10 月 10 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

C2101-176　（ウェブアプリケーションの開発時・運用時の対策）（政府機関統一基準の対応項番 7.2.2(2)）

第百七十六条　部局技術責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、

これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

解説：「ウェブアプリケーションの脆弱性を排除するための対策」について

ウェブアプリケーションの開発時には、既知の種類のウェブアプリケーションの脆弱性を排除するための対策が求められる。脆弱性を排除したウェブアプリケーションを実装する方法の詳細については、独立行政法人情報処理推進機構（IPA）による「安全なウェブサイトの作り方」を参照することも考えられる。

参考：独立行政法人情報処理推進機構
「安全なウェブサイトの作り方 改訂第 7 版」
（https://www.ipa.go.jp/security/vuln/websecurity.html）

このウェブサイトのアドレスについては、平成 29 年 10 月 10 日時点のものである。ウェブサイトのアドレスについては廃止や変更されることがあるため、最新のアドレスを確認した上で利用すること。

C2101-177　（ウェブアプリケーションの脆弱性の排除）（政府機関統一基準の対応項番 7.2.2(2)-1）

第百七十七条　部局技術責任者は、以下を含むウェブアプリケーションの脆弱性を排除すること。

一　SQL インジェクション脆弱性
二　OS コマンドインジェクション脆弱性
三　ディレクトリトラバーサル脆弱性
四　セッション管理の脆弱性
五　アクセス制御欠如と認可処理欠如の脆弱性
六　クロスサイトスクリプティング脆弱性
七　クロスサイトリクエストフォージェリ脆弱性
八　クリックジャッキング脆弱性
九　メールヘッダインジェクション脆弱性
十　HTTP ヘッダインジェクション脆弱性
十一　eval インジェクション脆弱性
十二　レースコンディション脆弱性
十三　バッファオーバーフロー及び整数オーバーフロー脆弱性

解説：第 1 号「SQL インジェクション脆弱性」について

ウェブアプリケーションのプログラムがデータベースを操作する手段として SQL 言語を用いている場合に、プログラムが SQL 文を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が SQL 文に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、データベースを破壊されたり、データベース内の情報を盗まれたりするなどの被害が生じ得る。このような欠陥は一般に「SQL インジェクション脆弱性」と呼ばれている。SQL インジェクション脆弱性を排除するには、SQL 文の組み立てにプレースホルダを用いる実装方法を採用することを徹

底するなどの対策が考えられる。

第２号「OS コマンドインジェクション脆弱性」について
ウェブアプリケーションのプログラムが OS のコマンドを操作する必要がある場合に、プログラムが OS のシェルのコマンドラインを用いてコマンド呼出しをする構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列がコマンドラインに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、サーバに侵入される被害が生じ得る。このような欠陥は一般に「OS コマンドインジェクション脆弱性」と呼ばれている。OS コマンドインジェクション脆弱性を排除するには、OS コマンドの操作にシェルのコマンドラインを用いない実装方法を採用することを徹底するなどの対策が考えられる。

第３号「ディレクトリトラバーサル脆弱性」について
ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっている場合に、指定されたパス名をプログラムがそのまま使用する構造になっていると、公開を想定しないファイルが参照されて、その内容が外部から閲覧され得る欠陥となる場合がある。このような欠陥は一般に「ディレクトリトラバーサル脆弱性」と呼ばれている。ディレクトリトラバーサル脆弱性を排除するには、外部のパラメータからパス名を指定する仕様を排除する対策、それができない場合には、ファイルにアクセスする直前に、使用するパス名の妥当性検査を行う方法、又は、ファイルのディレクトリと識別子を固定にしてアクセスするなどの対策が考えられる。

第４号「セッション管理の脆弱性」について
ウェブアプリケーションのプログラムがログイン機能を有するなど、セッション管理の仕組みを持つ場合に、そのセッション管理の実装方法に欠陥がある場合がある。例えば、セッション管理に用いられるセッション ID が推測可能な値となっている場合、セッション ID を URL パラメータに格納している場合、TLS（SSL）を使用しているセッションの管理に用いる cookie に secure 属性がセットされていない場合等が、この脆弱性に該当する。この欠陥を攻撃されると、正規の利用者がログイン中に、その利用者になりすまして不正にアクセスする「セッションハイジャック」の被害が生じ得る。この脆弱性を排除するには、暗号論的疑似乱数生成器（CSPRNG）で生成する十分な長さの文字列をセッション ID として推測困難なものとし、secure 属性のセットされた cookie にこれを格納することでセッション ID の漏えいを防ぐ対策方法が考えられる。

第５号「アクセス制御欠如と認可処理欠如の脆弱性」について
ウェブアプリケーションがログイン機能を有し、ログイン中の利用者にのみ利用を許可すべき機能がある場合に、ログインしていない利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「アクセス制御欠如の脆弱性」と呼ばれる。また、ログイン中の利用者のうち、一部の利

用者にのみ利用を許可すべき機能がある場合に、それ以外の利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「認可処理欠如の脆弱性」と呼ばれる。これらの欠陥を攻撃されると、秘密情報の漏えい、なりしまし操作等の被害が生じ得る。これらの脆弱性を排除するには、アクセス制御と認可処理が必要な画面の仕様を明確にし、仕様に沿った実装を徹底するなどの対策が考えられる。

第６号「クロスサイトスクリプティング脆弱性」について
ウェブアプリケーションのプログラムが HTML ページを出力する場合に、プログラムが HTML を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が HTML に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、cookie の値を盗まれてセッションハイジャックされるほか、画面の内容を改ざんされるなどの被害が生じ得る。このような欠陥は一般に「クロスサイトスクリプティング脆弱性」と呼ばれている。クロスサイトスクリプティング脆弱性を排除するには、以下を含む対策が考えられる
・HTML の出力に際して HTML タグの出力以外の全ての出力において文字列を HTML エスケープ処理することを徹底する。
・URL を出力するときは「http://」又は「https://」で始まる URL のみを許可する。
・SCRIPT 要素の内容を動的に生成しないようにする。
・スタイルシートを任意のサイトから取り込める仕様を排除する。
・全てのページについて HTTP レスポンスヘッダの「Content-Type」フィールドの「charset」に文字コードの指定を行う。
ただし、当該ウェブアプリケーションの仕様の都合で、これらだけでは解決できない場合もあり、その場合には追加的な対策が必要となる。

第７号「クロスサイトリクエストフォージェリ脆弱性」について
ウェブアプリケーションが、ログイン中の利用者にのみ利用を許可する機能を有している場合に、その機能のウェブページに前記第５号の対策が施されている場合であっても、外部のサイトから当該ウェブページにリンクを張る方法により、利用者本人にそのリンクをたどらせることで、当該利用者の意図に反して当該機能が利用されてしまうという構造になっている場合がある。このような欠陥は一般に「クロスサイトリクエストフォージェリ脆弱性」と呼ばれている。この欠陥を攻撃されると、悪意ある者が仕掛けたリンクによって、不正に当該機能を操作される被害（具体的には、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害）が生じ得る。この脆弱性を排除するには、外部からのリンクによって機能が作動してはならないウェブページは、処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行するように実装するな

どの対策方法が考えられる。

第８号「クリックジャッキング脆弱性」について
ウェブアプリケーションが、サイト内のボタンやリンクをクリックするだけで作動する機能を有している場合に、悪意ある者が、当該サイトを透明化した（透明色で表示して利用者の目に見えないように設定された）フレームとして外部のサイト上に表示するようにし、利用者を当該外部サイトへ誘導して、当該ボタンやリンクの表示された画面上の位置をクリックさせるよう誘導することで、利用者の意図に反して当該機能を作動させることができてしまう場合がある。このような欠陥は一般に「クリックジャッキング脆弱性」と呼ばれている。この欠陥を攻撃されると、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害が生じ得る。この脆弱性を排除するには、ウェブサーバの設定で、HTTP レスポンスに「X-Frame-Options」ヘッダを出力するようにし、そのフィールド値に「deny」又は「sameorigin」の値をセットすることで、当該ウェブページが外部のサイトにフレームとして表示されることを拒否するよう利用者のブラウザに指示する機能を用いるといった対策方法が考えられる。

第９号「メールヘッダインジェクション脆弱性」について
ウェブアプリケーションが電子メールを送信する機能を有し、その宛先となる電子メールアドレスをウェブアプリケーションのパラメータから指定する構造になっている場合に、悪意ある者により任意の電子メールアドレスが当該パラメータに与えられ、迷惑メールの送信のために当該ウェブアプリケーションが悪用されてしまうという被害が生じ得る。この欠陥を排除するには、電子メールの送信先電子メールアドレスはプログラム中に固定的に記述する実装方法（又は設定ファイルから読み込む実装方法）を採用して、ウェブアプリケーションのパラメータを用いるのを避けるなどの対策方法が考えられる。

第１０号「HTTP ヘッダインジェクション脆弱性」について
ウェブアプリケーションが HTTP レスポンスヘッダの「Location」や「Set-Cookie」のフィールド値を動的に出力する構造になっている場合、外部から悪意ある者によって与えられた改行文字を含む攻撃用の文字列が HTTP レスポンスヘッダに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、クロスサイトスクリプティング脆弱性の場合と同じ被害が生じ得る。このような欠陥は一般に「HTTP ヘッダインジェクション脆弱性」と呼ばれている。HTTP ヘッダインジェクション脆弱性を排除するには、HTTP レスポンスヘッダを出力する際に、直接にヘッダ文字列を出力するのではなく、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する実装方法を採用するなどの対策が考えられる。

第１１号「eval インジェクション脆弱性」について

ウェブアプリケーションのプログラムを作成する言語が、「eval」等、文字列をプログラムとして実行する機能を持つ言語である場合に、プログラムがこの機能を使用していると、外部から悪意ある者によって与えられた攻撃用の文字列が、その eval に与える文字列に混入し得る欠陥となることがある。この欠陥を攻撃されると、任意のプログラムがサーバで実行されることとなり、様々な被害が生じ得る。このような欠陥は一般に「eval インジェクション脆弱性」と呼ばれる。この脆弱性を排除するには、eval 機能を一切使用しない実装方法を採用するなどの対策が考えられる。

第１２号「レースコンディション脆弱性」について
ウェブアプリケーションの機能を複数の利用者が全く同時に利用したときに、一方の利用者向けの処理ともう一方の利用者向けの処理を途中で取り違えてしまう事態が一定の確率で発生する場合がある。このような欠陥は一般に「レースコンディション脆弱性」と呼ばれる。この欠陥により、利用者の秘密にすべき情報が第三者に閲覧される被害が生じる。この被害は、攻撃者がいなくても偶然に発生する場合もあれば、攻撃者が大量のアクセスをすることで意図的に引き起こされる場合もある。この脆弱性を排除するには、ソースコードレビューによってレースコンディションが起きえない構造にプログラムが記述されていることを確認する方法や、大量のアクセスを同時に発生させて異常が発生しないことを十分に確認するテストを行うなどの対策方法が考えられる。

第１３号「バッファオーバーフロー及び整数オーバーフロー脆弱性」について
ウェブアプリケーションのプログラムを作成する言語として、バッファオーバーフロー脆弱性等が生じない言語を採用することが望ましいが、その場合であっても、ウェブアプリケーションが、内部で C 言語等を用いて独自に作成されたプログラムを呼び出す構造になっている場合がある。その呼び出されるプログラムにバッファオーバーフロー脆弱性や整数オーバーフロー脆弱性が存在し、ウェブアプリケーションに外部から与えた文字列が当該プログラムに引き渡される構造になっていると、それらの欠陥を攻撃されて、サーバに侵入される被害が生じ得る。このような脆弱性を排除するためには、C 言語等のバッファオーバーフロー脆弱性等が生じ得る言語により作成されたプログラムが内部で呼び出されることを避けるなどの対策が考えられる。

第三節　ドメインネームシステム（DNS）

解説：ドメインネームシステム（DNS：Domain Name System）は、インターネットを使った階層的な分散型システムで、主としてインターネット上のホスト名や電子メールに使われるドメイン名と、IP アドレスとの対応づけ（正引き、逆引き）を管理するために使用されている。DNS では、端末等のクライアント（DNS クライアント）からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係等について回答を行う。DNS には、本学が管理するドメインに関する問合せについて回答を行うコンテンツサーバと、DNS クライア

ントからの要求に応じてコンテンツサーバに対して問合せを行うキャッシュサーバが存在する。キャッシュサーバの可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また、コンテンツサーバが提供する情報の完全性が損なわれ、誤った情報を提供した場合は、端末等の DNS クライアントが悪意あるサーバに接続させられるなどの被害に遭う可能性がある。さらに、電子メールのなりすまし対策の一部は DNS で行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNS サーバの適切な管理が必要である。

なお、本章の遵守事項のほか、第１４章第２節「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

C2101-178　（DNS の導入時の対策）（政府機関統一基準の対応項番 7.2.3(1)）

第百七十八条　部局技術責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。

２　部局技術責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。

３　部局技術責任者は、DNS のコンテンツサーバにおいて、本学のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。

C2101-179　（DNS のコンテンツサーバに係る対策）（政府機関統一基準の対応項番 7.2.3(1)-1）

第百七十九条　部局技術責任者は、要安定情報を取り扱う情報システムの名前解決を提供する DNS のコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講ずること。

一　コンテンツサーバを冗長化する。

二　通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。

解説：第１号「冗長化」について

コンテンツサーバは、冗長化しておくことが一般的である。その際には、ネットワーク障害等を考慮して各々の DNS のコンテンツサーバをそれぞれ異なるネットワークに配置しておく、災害等を考慮して物理的に離れた建物や遠隔地に設置しておくなど、情報と情報システムに要求される可用性に応じて、最適な構成を検討する必要がある。ISP 等が提供するセカンダリ DNS の利用も、遠隔地への設置による冗長化の措置の例である。

また、要求される可用性の度合いに応じて、保守作業による復旧等、冗長化以外の措置を探ることも考えられる。

C2101-180　（DNS のキャッシュサーバに係る対策）（政府機関統一基準の対応項番 7.2.3(1)-2）

第百八十条　部局技術責任者は、学外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は必要であれば学内からの名前解決の要求のみに応答をするよう、以下を例とする措置を講ずること。

一　キャッシュサーバの設定でアクセス制御を行う。
二　ファイアウォール等でアクセス制御を行う。

解説：「学外からの名前解決の要求に応じる必要性」について

不特定の DNS クライアントからの名前解決の要求に応じるキャッシュサーバはオープンリゾルバと呼ばれる。オープンリゾルバは、存在しないホスト名の名前解決の問合せを大量に送信することで上位の DNS サーバの過負荷を狙う DNS 水責め攻撃や、DNS リフレクター攻撃といったサービス不能攻撃等の踏み台として悪用される危険性がある。そのため本学で利用するキャッシュサーバが学外からの名前解決の要求に応じる必要性があるか検討することが必要である。

C2101-181　（DNS キャッシュポイズニング攻撃に係る対策）（政府機関統一基準の対応項番 7.2.3(1)-3）

第百八十一条　部局技術責任者は、DNS キャッシュポイズニング攻撃から保護するため、以下を例とする措置を講ずること。

一　ソースポートランダマイゼーション機能を導入する。
二　DNSSEC を利用する。

解説：「DNS キャッシュポイズニング攻撃」について

DNS キャッシュポイズニング攻撃とは、DNS のキャッシュサーバにキャッシュされている情報を偽の情報に書き換える攻撃である。この攻撃により、例えば、利用者は正しい URL のウェブサイトに接続しているつもりでも、書き換えられた偽の情報により不正なウェブサイトに誘導されるといった被害を受ける可能性がある。

第１号「ソースポートランダマイゼーション」について

ソースポートランダマイゼーションとは、キャッシュサーバからコンテンツサーバへの問合せに使用される UDP ポート番号をランダム化する技術である。UDP ポート番号をランダム化することにより、攻撃者がキャッシュポイズニング攻撃を行う際に UDP ポート番号の推測を困難にすることができ、攻撃の成功確率を低下させることが可能となる。

第２号「DNSSEC」について

DNSSEC では、コンテンツサーバによって応答に電子署名が行われ、キャッシュサーバがその署名を検証することで、応答が改ざん等されているか確認することができる。DNSSEC は、公開鍵暗号技術を用いるため、その導入には情報の提供側であるコンテンツサーバと情報の問合せ側であるキャッシュサーバの双方に対応が必要となる。学外への信頼できるサービスの提供と、本学の情報セキュリティ向上の観点から、A 大学ドメインを管理するコンテンツサーバ及び学内のキャッシュサーバに対する円滑な DNSSEC の導入が望ましい。

C2101-182　（学内のみで使用する名前の解決を提供するコンテンツサーバに係る対策）（政府機

関統一基準の対応項番 7.2.3(1)-4）

第百八十二条　部局技術責任者は、学内のみで使用する名前の解決を提供するコンテンツサーバにおいて、以下を例とする当該コンテンツサーバで管理する情報の漏えいを防止するための措置を講ずること。

一　外部向けのコンテンツサーバと別々に設置する。

二　ファイアウォール等でアクセス制御を行う。

解説：「当該コンテンツサーバで管理する情報の漏えいを防止するための措置」について

コンテンツサーバにおいて、学内のみで使用する名前の解決を提供する場合、内部のみで使用している名前情報を学外の者が取得できないようにすることを求めている。

C2101-183　（DNS の運用時の対策）（政府機関統一基準の対応項番 7.2.3(2)）

第百八十三条　部局技術責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。

２　部局技術責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。

３　部局技術責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。

解説：第１項「サーバ間で整合性を維持」について

複数台の DNS のコンテンツサーバでドメインに関する情報を保有し管理する場合に、各コンテンツサーバ間でドメインに関する情報の整合性を維持することを求める事項である。例えば、主系統のコンテンツサーバで管理するドメインに関する情報が変更された場合に、ゾーン転送等によって、情報システムの可用性に影響を及ぼさない適切なタイミングで副系統のコンテンツサーバが管理するドメインに関する情報も更新するといった方法が考えられる。

なお、主系統のコンテンツサーバから副系統のコンテンツサーバへ安全にゾーン転送を行う対策として、例えば、TSIG（Transaction Signature）の利用等が考えられる。

第２項「ドメインに関する情報が正確であることを定期的に確認」について

近年、国内で使用されているドメイン名の登録情報が不正に書き換えられ、攻撃者が用意したネームサーバの情報が追加される“ドメイン名ハイジャック”と呼ばれる攻撃が複数報告されている。このような攻撃への対策として、コンテンツサーバで管理するドメインに関する情報について、設定誤りや不正な改ざん等が発生していないかを定期的に確認することで、情報の正確性を維持することを求めている。管理するドメインに関する情報の具体例として、以下に挙げる登録内容等を確認することが考えられる。

・ホストの IP アドレス情報を登録する A（AAAA）レコード

・ドメインの電子メールサーバ名を登録する MX レコード

・なりすましメールを防ぐための SPF レコード等を登録する TXT レコード

なりすまし防止の観点からは、管理するドメインについての SPF レコードが正確であるかどうかを確認したり、ドメインを廃止する場合には、ドメインの廃止申請を行い、当該ドメインが確実に廃止されていることを確認したりすることが重要である。

C2101-184　（キャッシュサーバに係る対策）（政府機関統一基準の対応項番 7.2.3(2)-1）

第百八十四条　部局技術責任者は、キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（３か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持すること。

第四節　データベース

解説：本項における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。

要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び事務従事者の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

特に大量のデータを保管するデータベースの場合、そのデータが漏えい等した際の影響が大きく、また、そのようなデータは攻撃者の標的となりやすい。

なお、本項の遵守事項のほか、第１１章「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、第１２章第１節「ソフトウェアに関する脆弱性対策」、第２節「不正プログラム対策」、第１６章第２節「IPv6 通信回線」において定める遵守事項のうち、データベースに関係するものについても併せて遵守する必要がある。

C2101-185　（データベースの導入・運用時の対策）（政府機関統一基準の対応項番 7.2.4(1)）

第百八十五条　部局技術責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。

２　部局技術責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。

３　部局技術責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。

４　部局技術責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

５　部局技術責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。

解説：第２号「データベースに格納されているデータにアクセスした利用者を特定」について

一般的に、データベースの使用形態は図８のように、データベースから見たアクセス主体が「人間の利用者」となる場合と、「中間アプリケーションサーバ」となる場合の２つのモデルに分けられる。中間アプリケーションサーバを利用するモデルでは、中間アプリケーションサーバ用にデータベースアクセス用のアカウントを作成して運用する構成となるのが通常である。この構成では、データベースのログにはアクセス主体が中間アプリケーションサーバとして記録されることになるため、不正な操作が行われた場合に実際には誰が操作をしたものかをデータベースのログのみからでは特定できない可能性がある。そのため中間アプリケーションサーバにおいて、データベースの利用者とデータベースへの操作要求とを紐づけてログを取得し、利用者を特定できるようにしておく必要がある。

図８　データベース利用形態モデル

第５項「適切に暗号化」について
データベースに格納されるデータを暗号化する方法には、電磁的記録媒体の暗号化、データベースのテーブルの暗号化、カラムの暗号化等がある。想定される脅威や利用環境等によってメリット・デメリットがあるため、適切な方式を選択することが望ましい。

C2101-186　（データベースの管理者権限に係る対策）（政府機関統一基準の対応項番 7.2.4(1)-1,2,3）

第百八十六条　部局技術責任者は、必要に応じて情報システムの管理者とデータベースの管理者を別にすること。

２　部局技術責任者は、データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しないこと。

３　部局技術責任者は、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずること。

解説：第１項「データベースの管理者」について
データベースの管理者は、データベースに格納されるデータの管理、アカウント・権限の管理、ネットワーク環境の構成等の管理を行う。多数の管理者特権を保持するアカウントを奪取された場合、甚大な被害を受けるおそれがあるため、重要な情報を管理するデータベースの管理者の特権を他の管理者と分掌することが望ましい。

第３項「権限の不適切な付与」について
行政事務の遂行、データベースの運用・管理等をするに当たって不必要なデータに対するアクセス権の付与のほか、他のアカウントに対して権限を付与する権限の付与等がある。

C2101-187　（データベースの操作ログに係る対策）（政府機関統一基準の対応項番 7.2.4(1)-4）
第百八十七条　部局技術責任者は、業務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずること。
一　一定数以上のデータの取得に関するログを記録し、警告を発する。
二　データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。

C2101-188　（データベースにおける脆弱性に係る対策）（政府機関統一基準の対応項番 7.2.4(1)-5,6）
第百八十八条　部局技術責任者は、データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除すること。
２　部局技術責任者は、データベースにアクセスする機器上で動作するプログラムに対して SQL インジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討すること。
一　ウェブアプリケーションファイアウォールの導入
二　データベースファイアウォールの導入

C2101-189　（データベースにおける暗号化に係る対策）（政府機関統一基準の対応項番 7.2.4(1)-7）
第百八十九条　部局技術責任者は、格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

第十六章　通信回線

第一節　通信回線

解説：サーバ装置や端末への不正アクセスやサービス不能攻撃等は、当該サーバ装置や端末に接続された通信回線及び通信回線装置を介して行われる場合がほとんどであることから、通信回線及び通信回線装置に対する情報セキュリティ対策については、情報システムの構築時からリスクを十分検討し、必要な対策を実施しておく必要がある。通信回線の運用主体又は物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。また、情報システムの運用開始時と一定期間運用された後とでは、通信回線の構成や接続される情報システムの条件等が異なる場合があり、攻撃手法の変化も想定されることから、情報システムの構築時に想定した対策では十分でなくなる可能性がある。そのため、通信回線の運用時においても、継続的な対策を

実施することが重要である。

C2101-190　（通信回線の導入時の対策）（政府機関統一基準の対応項番 7.3.1(1)）

第百九十条　部局技術責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。

２　部局技術責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。

３　部局技術責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。

４　部局技術責任者は、利用者等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。

５　部局技術責任者は、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。

６　部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。

７　部局技術責任者は、学内通信回線にインターネット回線、公衆通信回線等の学外通信回線を接続する場合には、学内通信回線及び当該学内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。

８　部局技術責任者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視するための措置を講ずること。

９　部局技術責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

１０　部局技術責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。

１１　部局技術責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくこと。

解説：第１項「適切な回線種別を選択」について

通信回線に利用する物理的な回線（通信事業者の回線・公衆無線 LAN 回線　等）の種別によって、盗聴、改ざん等の脅威及びそれらに対する有効なセキュリティ対策が異なることから、適切な回線を選択することが求められる。

例えば、要安定情報を取り扱う情報システムにおいて、通信経路の破壊等による可用性への影響を回避することを目的として仮想的な通信回線を複数の通信経路により構築する場合、物理的にも分離された通信経路上にそれぞれ仮想的な通信回線を構築しなければ、本来求められる可用性の維持に関する要件を満たすことにはならない。

第９項「ソフトウェアを定め」について
通信回線装置としての機能や動作の明確化を行うとともに、ソフトウェアの脆弱性に関する対策を確実なものとするために、通信回線装置で使用するソフトウェアについて、バージョンを含めて定めておくことが望ましい。通信回線装置の更新ソフトウェアの提供を受けた際に、それを無条件に適用せずに、更新内容等をあらかじめ確認し、適用する必要性を判断することが重要である。

第１１項「契約時に取り決めておく」について
公衆通信回線サービスを使用する場合においては、回線の利用規約等に記載されているセキュリティレベルやサービスレベルを合意した上で当該回線を選択する必要がある。役務提供契約で通信回線を利用するなど、本学において直接回線を調達しない場合については、通信回線に求めるセキュリティレベル及びサービスレベルについて、役務提供事業者と合意形成する必要がある。

C2101-191　（通信経路の分離に係る対策）（政府機関統一基準の対応項番 7.3.1(1)-1）
第百九十一条　部局技術責任者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じて、以下を例とする通信経路の分離を行うこと。
一　外部との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離する。
二　業務目的や取り扱う情報の格付及び取扱制限に応じて情報システムごとに VLAN により通信経路を分離し、それぞれの通信制御を適切に行う。
三　他の情報システムから独立した専用の通信回線を構築する。

解説：第３号「専用の通信回線を構築」について
リスクを検討した結果、他の情報システムと共通的な通信回線を利用すると情報システムのセキュリティが確保できないと判断した場合には、他の通信回線から独立させて閉鎖的な通信回線とするなどの構成を採用することが考えられるが、過剰なセキュリティ要件とならないように、閉鎖的な通信回線とする必要性を見極めることが重要である。例えば、通信回線を VLAN 等で論理的に分割し、分割された論理的な通信回線ごとに情報セキュリティを確保することで十分要件を満たすのであれば、費用や維持管理の面でメリットがある。このように情報セキュリティ以外の観点とのバランスをとって要件を定めることが重要である。

C2101-192　（通信回線の秘匿性確保に係る対策）（政府機関統一基準の対応項番 7.3.1(1)-2）
第百九十二条　部局技術責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、SSL（TLS）、IPsec 等による暗号化を行うこと。また、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。

C2101-193　（通信回線への情報システムの接続に係る対策）（政府機関統一基準の対応項番

7.3.1(1)-3）

第百九十三条　部局技術責任者は、学内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずること。

一　情報システムの機器番号等により接続機器を識別する。

二　クライアント証明書により接続機器の認証を行う。

C2101-194　（通信回線及び通信回線装置の保護に係る対策）（政府機関統一基準の対応項番 7.3.1(1)-4）

第百九十四条　部局技術責任者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講ずること。

一　通信回線装置を施錠可能なラック等に設置する。

二　施設内に敷設した通信ケーブルを物理的に保護する。

三　通信回線装置の操作ログを取得する。

C2101-195　（要安定情報を取り扱う情報システムが接続される通信回線に係る対策）（政府機関統一基準の対応項番 7.3.1(1)-5）

第百九十五条　部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずること。

一　通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。

二　通信回線及び通信回線装置を冗長構成にする。

解説：第２号「通信回線及び通信回線装置を冗長構成にする」について

高い可用性が求められる情報システムを構築する場合は、大規模災害の発生を想定し、通信回線を冗長構成にしておくことが望ましい。また、本学の建物から外部に敷設する通信回線の管路についても、例えば、異なる通信事業者による複数の経路で構築しておくことで、災害を受けた際に復旧にかかる時間が短縮されるなどの効果が期待される。

C2101-196　（学内通信回線と学外通信回線との接続に係る対策）（政府機関統一基準の対応項番 7.3.1(1)-6）

第百九十六条　部局技術責任者は、学内通信回線に、インターネット回線や公衆通信回線等の学外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講ずること。

一　ファイアウォール、WAF（Web Application Firewall）、リバースプロキシ等により通信制御を行う。

二　通信回線装置による特定の通信プロトコルの利用を制限する。

三　IDS/IPS により不正アクセスを検知及び遮断する。

C2101-197　（遠隔地から通信回線装置に対して行われるリモートアクセスに係る対策）（政府機関統一基準の対応項番 7.3.1(1)-7）

第百九十七条　部局技術責任者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、以下を例とする対策を講ずること。

一　リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う。

二　主体認証によりアクセス制御する。

三　通信内容の暗号化により秘匿性を確保する。

四　ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにする。

C2101-198　（通信回線の運用時の対策）（政府機関統一基準の対応項番 7.3.1(2)）

第百九十八条　部局技術責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずること。

２　部局技術責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。

３　部局技術責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。

４　部局技術責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。

解説：第２項「アクセス制御の設定の見直しを行う」について

アクセス制御の設定の見直しにより、設定条件を変更したり又は設定の不備を修正したりする場合は、当該通信回線に接続されている情報システムの部局技術責任者にも事前の連絡及び結果の通知が必要である。

第３項「ソフトウェアの状態を定期的に調査」について

通信回線の重要性、想定される脅威及び機器の特性等から調査の必要性及び調査の間隔を検討する必要がある。例えば、基幹回線等の重要な通信回線を構成する機器、ファイアウォールのようにインターネット等と直接接続されている機器、頻繁にソフトウェアがアップデートされるような機器等は調査の必要性が高く、より短期間に繰り返し調査を実施することが考えられる。また、必要性が低いと判断された機器についても、ソフトウェア等に脆弱性が報告されたり、通信回線の構成変更が発生したりする場合に随時調査することが望ましい。

第３項「不適切な状態」について

許可されていないソフトウェアがインストールされている場合や、定められたソフトウェアが動作するための設定が適切でないなどの状態のことを指す。

C2101-199　（作業記録・設定情報等のバックアップの取得と保管）（政府機関統一基準の対応項番 7.3.1(2)-1,2）

第百九十九条　部局技術責任者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施

する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管すること。

２　部局技術責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。

C2101-200　（通信回線の運用終了時の対策）（政府機関統一基準の対応項番 7.3.1(3)）

第二百条　部局技術責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。

解説：「情報を抹消するなど適切な措置」について

運用を終了した通信回線装置が再利用されたとき又は廃棄された後に、保存されていた情報が漏えいすることを防ぐための抹消の方法としては、通信回線装置の初期化、内蔵電磁的記録媒体の物理的な破壊等の方法がある。通信回線装置内にも、設定情報や通信ログ等の情報が保存されていることから、サーバ装置及び端末と同様に運用終了時に留意しておくことが必要である。

通信回線装置は通信事業者からリース提供されることがあり、その場合は通信回線の運用終了に伴い通信事業者に装置を返却することになるため、通信回線装置の初期化の手順等本条を遵守するための方法について、通信事業者に確認する必要がある。

C2101-201　（リモートアクセス環境導入時の対策）（政府機関統一基準の対応項番 7.3.1(4)）

第二百一条　部局技術責任者は、VPN 回線を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。

２　部局技術責任者は、事務従事者の業務遂行を目的としたリモートアクセス環境を、学外通信回線を経由して本学の情報システムへリモートアクセスする形態により構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。

解説：第１項「VPN 回線を整備」について

VPN 回線には、IP-VPN 等の閉域網をベースとした回線とインターネット VPN 等の公衆回線網をベースとした回線があるが、どちらを整備する場合であっても通信内容の暗号化及びリモートアクセス端末（又は利用者）の認証は、必ず講じておくべき措置となる。さらに、特に機密性の高い情報を取り扱う場合においては二重の暗号化を行う（例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行う）などを考慮してもよい。

C2101-202　（VPN 回線によるリモートアクセス環境に係る対策）（政府機関統一基準の対応項番 7.3.1(4)-1）

第二百二条　部局技術責任者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。

一　利用開始及び利用停止時の申請手続の整備
二　通信を行う端末の識別又は認証
三　利用者の認証
四　通信内容の暗号化
五　主体認証ログの取得及び管理
六　リモートアクセスにおいて利用可能な公衆通信網の制限
七　アクセス可能な情報システムの制限
八　リモートアクセス中の他の通信回線との接続禁止

解説：第５号「主体認証ログ」について

例えば MS-CHAPv2 のような、認証情報を第三者に窃取されるなどの脆弱性が認められる認証プロトコル（リモートアクセスによる利用者認証の際に汎用的に用いられるプロトコル）については、暗号化されている通信路上で認証処理を行い、認証ログを厳重に管理するなどの対策を講ずる必要がある。運用中のサーバ装置や通信回線装置の認証ログを定期的に確認するなどして、不正アクセスが行われていないことに留意することも重要である。

第６号「利用可能な公衆通信網の制限」について

リモートアクセスの際に足回りの回線として使用する通信回線については、安全な通信回線サービスに限定することが望ましいが、海外で利用する場合等においては、利用可能な通信回線サービスが限られており、通信回線サービスを制限できない。このような場合は、「通信回線サービスを限定しない」という前提条件のもと、通信回線サービスの安全性や信頼性に関わらず、取り扱われる情報のセキュリティが確保されるよう、VPN 接続時の認証処理及び通信内容の暗号化等の対策を考慮する必要がある。

C2101-203　（リモートアクセス環境に係る対策）（政府機関統一基準の対応項番 7.3.1(4)-2）

第二百三条　部局技術責任者は、学外通信回線を経由した本学の情報システムへのリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。

一　利用開始及び利用停止時の申請手続の整備
二　利用者の認証又は発信者番号による識別及び認証
三　主体認証ログの取得及び管理
四　アクセス可能な情報システムの制限
五　リモートアクセス中の他の通信回線との接続禁止

C2101-204　（無線 LAN 環境導入時の対策）（政府機関統一基準の対応項番 7.3.1(5)）

第二百四条　部局技術責任者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。

C2101-205　（無線 LAN 環境導入時の対策）（政府機関統一基準の対応項番 7.3.1(5)-1）

第二百五条　部局技術責任者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信

回線の構築時共通の対策に加えて、以下を例とする対策を講ずること。

一　SSID の隠蔽

二　無線 LAN 通信の暗号化

三　MAC アドレスフィルタリングによる端末の識別

四　802.1X による無線 LAN へのアクセス主体の認証

五　無線 LAN 回線利用申請手続の整備

六　無線 LAN 機器の管理手順の整備

七　無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対処手順の整備

解説：第 2 号「無線 LAN 通信の暗号化」について

暗号化方式として、例えば WPA2 Enterprise（Wi-Fi Protected Access 2 Enterprise）方式を選択することが考えられる。WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信を妨害できたりするという脆弱性が報告されており、利用すべきではない。他の暗号化方式においても同様の問題が起こる可能性があるため、最新の情報に従い適切な方式や設定値を選択することが求められる。

第 6 号「無線 LAN 機器の管理」について

無線 LAN 機器の管理については、例えば、以下が考えられる。

・無線 LAN 機器の電波出力・周波数チャンネル等の管理

・管理外の無線 LAN アクセスポイント、端末の検出及び除去

なお、無線 LAN 回線を構築する場合は、政府機関から公表している以下の研究会報告書等を参考にするとよい。

参考：総務省「国民のための情報セキュリティサイト」の「情報管理担当者のための情報セキュリティ対策」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/index.html）にある、「安全な無線 LAN 利用の管理」のページの解説

参考：各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告「無線 LAN セキュリティ要件の検討」（平成 23 年 3 月）（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf）

参考：総務省「無線 LAN ビジネス研究会」報告書（平成 24 年 7 月 20 日）（http://www.soumu.go.jp/menu_news/s-news/02kiban04_03000093.html）

参考：総務省「無線 LAN ビジネスガイドライン」（平成 25 年 6 月 25 日）（http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000058.html）

第 7 号「不正プログラム感染を認知した場合の対処手順」について

本学 LAN 端末が不正プログラムに感染した場合は、通常は通信ケーブルを抜去するといった手順が設けられていることが多いが、無線 LAN 回線を使用している場合においては、不正プログラムに感染した端末が無線 LAN 回線を介して他の端末に感染を拡大しないように、無線 LAN 通信を遮断するための手

順をあらかじめ定め、利用者等へ周知しておく必要がある。例えば、以下の手順が考えられる。
・感染を認知した際に電磁波を遮断するシールドボックスに感染端末を隔離する。
・無線 LAN の通信圏外へ端末を移動し、保管する。
・端末の無線 LAN 通信機能を停止する。

C2101-206　（情報コンセント設置時の対策）

第二百六条　部局技術責任者は、情報コンセントを設置する場合は、以下を例とする対策を講ずること。

一　利用開始及び利用停止時の申請手続の整備
二　通信を行う端末の識別又は認証
三　利用者の認証
四　主体認証ログの取得及び管理
五　情報コンセント経由でアクセス可能な情報システムの明確化
七　情報コンセント接続中の他の通信回線との接続禁止
八　情報コンセント接続方法の機密性の確保
九　情報コンセントに接続する端末及び通信回線装置の管理

解説：情報コンセントを設置する場合に、セキュリティを確保することを求める事項である。

C2101-207　（端末の学内通信回線への接続の管理）

第二百七条　部局総括責任者は、端末の学内通信回線への接続の申請を受けた場合は、別途定める接続手順に従い、申請者に対して接続の諾否を通知し必要な指示を行うこと。

解説：要点は、部局総括責任者が、「誰が」「いつ」「どこで」「何を」しているか把握できるような仕組みを端末の学内通信回線への接続の段階で作り上げることである。なお、全学ネットワーク、部局サブネット、学科サブネット、研究室サブネットのように、ネットワークの論理的な構成に合わせて権限委譲を行ったり、特定の利用に関して包括的な許可を与えたりする場合もあり得る。例えば、大学を会場とする学会や研究会において、学外からのゲスト利用者に接続を許可することもあるだろう。
なお、学内通信回線と通信を行わないスタンドアローン PC については、接続申請は不要である。
また、学外通信回線に接続した PC からの通信が、VPN 接続により学内通信回線に論理的に接続されることも考えられる。それらをどのように取り扱うかについては、各大学のポリシーによるものとする。このような技術的な問題もあるため、接続にあたっての技術的要件をあらかじめ接続手順等に定めておくことが求められる。

C2101-208　（電子計算機及び情報ネットワーク資源の管理）

第二百八条　部局技術責任者は、電子計算機及び情報ネットワークの利用を総合的かつ計画的に

推進するため、電子計算機の CPU 資源及びディスク資源並びにネットワーク帯域資源を利用者等の利用形態に応じて適切に分配し管理すること。

C2101-209　（ネットワーク情報の管理）

第二百九条　部局技術責任者は、部局情報ネットワークで使用するドメイン名や IP アドレス等のネットワーク情報について、全学情報システム運用委員会から割り当てを受け、利用者等からの利用形態に応じて適切に分配し管理すること。

C2101-210　（上流ネットワークとの関係）

第二百十条　全学実施責任者は、学内通信回線を構築し運用するにあたっては、学内通信回線の上流ネットワークとなる学外通信回線との整合性に留意すること。

解説：大学によっては、複数の対外接続を持つこともあり得る。その場合、そのすべてについて本規程が適用されるが、上流ネットワークの利用規程（上位 AUP（Acceptable Use Policy）という。）によって利用が制限されることもあるため注意が必要である。

なお、大学としての上流接続とは別に、例えば研究室等で学外の ISP と契約を行い対外接続することも考えられるが、その場合本規程は適用されない。そのような接続方法を認めるか否か、また認めるとしてどのような手続や規程に基づくべきかは、本規程とは別に定めることになるだろう。

利用者との関係では、利用者が上位 AUP に抵触しないよう「C2201 情報システム利用規程」等で定めるとともに、学内通信回線の構築及び運用に携わる者は、学内通信回線の上流ネットワークとなる学外通信回線との整合性を常に注意しなければならない。

第二節　IPv6 通信回線

解説：本学において、インターネットの規格である IPv6 通信プロトコルに対応するための取組が進められているが、IPv6 通信プロトコルを採用するに当たっては、グローバル IP アドレスによるパケットの直接到達性や IPv4 通信プロトコルから IPv6 通信プロトコルへの移行過程における共存状態等、考慮すべき事項が多数ある。

近年では、サーバ装置、端末及び通信回線装置等に IPv6 技術を利用する通信（以下「IPv6 通信」という。）を行う機能が標準で備わっているものが多く出荷され、運用者が意図しない IPv6 通信が通信ネットワーク上で動作している可能性があり、結果として、不正アクセスの手口として悪用されるおそれもあることから、必要な対策を講じていく必要がある。

なお、IPv6 技術は今後も技術動向の変化が予想されるが、一方で、IPv6 技術の普及に伴い情報セキュリティ対策技術の進展も期待されることから、本学においても、IPv6 の情報セキュリティ対策に関する技術動向を十分に注視し、適切に対応していくことが重要である。

C2101-211　（IPv6 通信を行う情報システムに係る対策）（政府機関統一基準の対応項番 7.3.2(1)）

第二百十一条　部局技術責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択すること。

２　部局技術責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

一　グローバル IP アドレスによる直接の到達性における脅威

二　IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

三　IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

四　アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

解説：第２項第１号「グローバル IP アドレスによる直接の到達性における脅威」について

IPv6 通信を想定して構築する情報システムにおいて、グローバル IP アドレスによる通信パケットの直接到達性における脅威に対抗するために、以下を例に対策を講ずることが考えられる。

・不正な機器からの経路調査コマンド（traceroute 等）への応答の禁止
・ICMP エコー要求への応答の禁止
・許可した宛先からのみアクセス可能とするなどの経路制御の設定
・サービス不能攻撃の検知及びフィルタ

第２項第２号「不正アクセスの脅威」について

IPv6 の特徴として、アドレスが長いこと、アドレスの省略形が複数パターン存在して一意に定まらない可能性があること、端末が複数の IP アドレスを持つこと等が挙げられる。このため、複雑なアクセス制御の設定が必要になり、設定不備等による不正アクセスにつながるリスクが想定される。

対策としては、外部ネットワークとの通信において、OSI 基本参照モデルのネットワーク層（第３層）及びトランスポート層（第４層）を中心にフィルタリングを行う機能及び断片化された通信の再構築を行う機能を適切に設定すること等、通信機器を流れる通信そのものを制御することが挙げられる。

なお、IPv6 通信を想定して構築する情報システムにおいて、IPv6 のログを取得し、分析する場合は、IPv6 アドレスでは桁数が大幅に増えること等から、IPv6 対応のログの解析ツールを利用することで、IPv6 アドレスの読み間違い等の運用上の作業ミスを軽減するための対策を検討することが望ましい。

第２項第３号「共存させる際の処理考慮漏れに起因する脆弱性」について

IPv6 通信プロトコルに対応している端末やサーバ装置には、多様な IPv6 移行機構（デュアルスタック機構、IPv6-IPv4 トンネル機構等）が実装されている。それらの IPv6 移行機構は、それぞれが想定する使用方法と要件に基づき設計されていることから、その選定と利用に当たっては、セキュリティホールの原因をつくらないよう十分な検討と措置が必要である。

例えば、デュアルスタック機構を運用する場合には、IPv4 のプライベートアド

レスを利用したイントラネットの情報システムであっても外部ネットワークとの IPv6 通信が可能となるため、デュアルスタック機構を導入したサーバ装置及び端末を経由した当該外部ネットワークからの攻撃について対策を講ずる必要がある。また、IPv6-IPv4 トンネル機構を運用する場合、トンネルの終端が適切に管理されないと本来通信を想定しないネットワーク間の IPv6 通信が既設の IPv4 ネットワークを使って可能となるため、本学のネットワークが外部から攻撃される危険性がある。管理されたサーバ装置及び端末以外のトンネル通信を当該 IPv4 ネットワークに設置されたファイアウォールにて遮断するなど、不適切な IPv6 通信を制御する対策が必要である。

第２項第４号「IPv6 アドレスの取扱い考慮漏れに起因する脆弱性」について
IPv4 のみに対応する機器及びソフトウェアが IPv6 ネットワーク上で動作する際、システム内部での IP アドレスの取扱いが IPv4 に依存している場合、IPv6 アドレスが取り扱えない、若しくはバッファオーバーラン等を引き起こす可能性があるというリスクを認識し、これが無いことを確認するなどが挙げられる。
統合認証システムや、システム間連動を行うようなアプリケーションでは、IPv4/IPv6 が混在した状況でも適切なシステム連携を行う必要がある。
また、「IPv4 対応システムが IPv6 アドレスに対応するため、IPv6／IPv4 コンバータ等が使用される場合がある。このような場合、内部からは個別の IPv6 アドレスを特定できないため、通信ログの取得やパケットフィルタリング等の機能を実装し運用する際等において留意する必要がある。

C2101-212　（意図しない IPv6 通信の抑止・監視）（政府機関統一基準の対応項番 7.3.2(2)）

第二百十二条　部局技術責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずること。

解説：「IPv6 通信を抑止するなどの措置」について

複数の本学キャンパスの間及び学内のみで利用する情報システムについて、通信回線が IPv6 通信を想定していない場合には、当該通信回線に接続される端末等の IPv6 通信の機能を停止する必要がある。
IPv6 通信を想定していない通信回線においては、ファイアウォールや IDS/IPS 等のセキュリティ機能に不正な IPv6 通信を制御する措置が講じられず、悪意ある者による IPv6 通信を使った攻撃に対して無防備となるおそれがある。さらに、IPv6 通信が可能なサーバ装置及び端末においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該サーバ装置及び端末への接続を可能とする自動トンネリング機能を提供するものがある。この機能を利用すると、サーバ装置及び端末と外部のネットワークとの間に情報システムの利用者や情報システムの運用管理者が気付かないうちに意図しない経路が自動生成され、これがセキュリティを損なうバックドアとなりかねないことから、自動トンネリング機能を動作させないようサーバ装置及び端末を設定する必要がある。ま

た、ルータ等の通信回線装置についても IPv6 通信をしないよう設定し、意図しない IPv6 通信を制限することが求められる。
なお、外部と直接通信を行う情報システム等についても、現時点において IPv6 対応がされていない場合には、意図しない IPv6 通信を抑止又は遮断するための措置を講ずることが必要である。

第十七章　情報システムの利用

解説：利用者等は、研究教育事務の遂行のため、端末での事務処理のほか電子メール、ウェブ等様々な情報システムを利用している。これらを適切に利用しない場合、情報セキュリティインシデントを引き起こすおそれがある。
このため、情報システムの利用に関する規定を整備し、利用者等は規定に従って利用することが求められる。

C2101-213　（情報システムの利用に係る規定の整備）（政府機関統一基準の対応項番 8.1.1(1)）

第二百十三条　全学実施責任者は、本学の情報システムの利用のうち、情報セキュリティに関する規定を整備すること。

２　全学実施責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。

３　全学実施責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。

解説：第３項「USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順」について
USB メモリ等の外部電磁的記録媒体に関する対策は、情報システムの構成等によって様々であると考えられるが、第二百十六条及び「【参考】USB メモリ等の外部電磁的記録媒体について」を参照しつつ、①端末等の不正プログラム感染、②盗難・紛失等による情報漏えい、③バックドアの埋め込み等のサプライチェーン・リスク、といった脅威に対抗するための利用手順を定める必要がある。また、利用者等は当該手順に従う必要がある（第四十二条第５項を参照のこと。）。
なお、USB メモリ等の外部電磁的記録媒体の管理に際しては、利用手順の整備のほか、組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入も有効である（第百四十条第２項第６号を参照のこと。）。

【参考】USB メモリ等の外部電磁的記録媒体について
USB メモリ等の外部電磁的記録媒体に関連する脅威（①②③）及び脆弱性（箇条書き）としては、以下が想定される。
①端末等の不正プログラム感染
・利用者、用法等が不明な物が使用されている。
・外部電磁的記録媒体を接続した際に自動的にプログラムが実行される。

・不正プログラム対策ソフトウェアによる検疫・駆除を行っていない。
②盗難・紛失等による情報漏えい
・利用者、用法等が不明な物が使用されている。
・運搬の際等に暗号化等の安全管理措置がなされていない。
・不要な要機密情報が保存されている。
③バックドアの埋め込み等のサプライチェーン・リスク
・製造元、製造過程が不明な物が使われる。

上記の脅威及び脆弱性に対しては、次に掲げる対策が想定される。

USB メモリ等の外部電磁的記録媒体に関する対策の例

脅威	対策	対策の種類	関連する規定
①不正プログラム感染	主体認証機能や暗号化機能を備える外部電磁的記録媒体を導入する	調達時の対策	第八十条関連
	不正プログラムの検疫・駆除機能を備える外部電磁的記録媒体を導入する	調達時の対策	第八十条関連
	情報を暗号化するための機能を備えたソフトウェアを導入する	調達時の対策	第八十条関連 第１１章第５節関連
	外部電磁的記録媒体の検疫・駆除機能を備える不正プログラム対策ソフトウェアを導入する	調達時の対策	第百二十九条関連
	サーバ装置及び端末の自動再生（オートラン）機能を無効にする	技術的な設定	第百四十条第２項第３号
	サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする	技術的な設定	第百四十条第２項第４号
	サーバ装置及び端末において使用を想定しない USB ポート等を無効にする	技術的な設定	第百四十条第２項第５号
	外部電磁的記録媒体の使用前に、不正プログラム対策ソフトウェアや外部電磁的記録媒体に備わる機能による不正プログラムの検疫・駆除を行う	利用時の対策	第二百十六条第４号 第二百二十六条関連
②情報漏えい	運搬の際等に主体認証機能や暗号化機能の利用等の安全管理措置を講ずる	利用時の対策	第四十八条第１項第３号 第二百十六条第２号
	要機密情報は保存される必要がなくなった時点で速やかに削除する	利用時の対策	第二百十六条第３号

③サプライチェーン・リスク	安全と考えられる製造元、製造過程の製品を調達する	調達時の対策	第８章第２節関連
①②③共通	使用可能な媒体の制限や利用方法等に関する手順を定める	管理対策	第二百十六条
	組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する	管理対策 調達時の対策	第百四十条第２項第６号 第二百十六条
	管理下に置かれた外部電磁的記録媒体を使用する（私物や出所不明の外部電磁的記録媒体を使用しない）	利用時の対策	第二百十六条第１号

C2101-214　（情報システムの利用に係る実施手順の整備）（政府機関統一基準の対応項番 8.1.1(1)-1）

第二百十四条　全学実施責任者は、本学の情報システムの利用のうち、情報セキュリティに関する規定として、以下を例とする実施手順を定めること。

一　情報システムの基本的な利用のうち、情報セキュリティに関する手順

二　電子メール及びウェブの利用のうち、情報セキュリティに関する手順

三　識別コードと主体認証情報の取扱手順

四　暗号と電子署名の利用に関する手順

五　不正プログラム感染防止の手順

六　アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為の防止に関する手順

七　ドメイン名の使用に関する手順

解説：「以下を例とする実施手順を定める」について

第１号～第５号は、それぞれ第二百十九条～第二百二十七条において、利用者等を名宛人とした対策事項が規定されている。同様に、第６号は第百四十二条において、また、第７号は第百四十二条において対策事項が規定されている。本条では、これら規定内容を包含する形で、本学の実施手順等を定めることを求めている。

C2101-215　（要管理対策区域外で情報処理を行う場合の対策）（政府機関統一基準の対応項番 8.1.1(1)-2,3）

第二百十五条　全学実施責任者は、要管理対策区域外にて情報処理を行う際の安全管理措置として、以下を例とする措置を規定し、利用者等に遵守させること。

一　モバイル端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化

二　盗み見に対する対策（のぞき見防止フィルタの利用等）

三　盗難・紛失に対する対策（不要な情報をモバイル端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）
四　利用する場所や時間の限定
五　端末及び外部電磁的記録媒体等についての盗難・紛失が発生した際の緊急対応手順

２　全学実施責任者は、要管理対策区域外にて利用者等が情報処理を行う際の許可等の手続として、以下を例とする手続を規定し、利用者等に遵守させること。
一　許可権限者の決定（部局技術責任者又は職場情報セキュリティ責任者が想定される。）
二　利用時の許可申請手続
三　手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線の接続形態等）
四　利用期間満了時の手続
五　許可権限者による手続内容の記録

解説：第１項第３号「盗難・紛失に対する対策」について
一般的に、以下に例を挙げる状況では、盗難・紛失が発生しやすいため、要機密情報を含むモバイル端末を携行する場合には十分注意させること。
・電車等での移動中に、モバイル端末の入ったかばん等を網棚に置き、そのまま下車する。
・飲酒が想定されるいわゆる宴会等でモバイル端末の入ったかばん等を置いたまま帰宅する。

第２項第４号「利用期間満了時の手続」について
利用期間満了時の際は、利用者等に報告を求めるよう手続に定める必要がある。特に機密性３情報等の取扱いに注意すべき情報を要管理対策区域外に持ち出す場合においては、以下を例とする管理手順を設けるとよい。
・利用期間満了時の連絡が無い場合は、当該利用者に確認する。
・利用期間の延長が必要であれば、再手続を要請する。
・利用期間満了前に利用が終了した際には、利用終了時に報告を求める。

C2101-216　（政府機関統一基準の対応項番 8.1.1(1)-4）

第二百十六条　全学実施責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順として以下の事項を含めて定めること。
一　本学支給の外部電磁的記録媒体を使用する（私物や出所不明の媒体を使用しない）。
二　主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。
三　要機密情報は保存される必要がなくなった時点で速やかに削除する。
四　外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行う。

解説：第１号「出所不明の媒体」について
USB デバイスの設計上の脆弱性を悪用するなどして、USB デバイスのファームウェアを不正に書き換えることによる攻撃手法が確認されている。

例えば、悪意のある者が、端末を不正プログラムに感染させることを目的にUSB メモリのファームウェアを書き換え、当該 USB メモリを攻撃対象者や不特定多数の者等に配ることが考えられる。当該 USB メモリは、USB ポートに挿入されると不正プログラムを自動的に実行し、端末が不正プログラムに感染してしまう。
このようなファームウェアを書き換えられた USB デバイスは、不正プログラム対策ソフトウェアでは検出できない場合もあることから、出所不明の USB デバイスの使用は慎むべきである。

第２号「セキュアな外部電磁的記録媒体」について
第四十八条「(解説) 第１項第３号「本学支給のセキュアな製品」について」を参照のこと。

C2101-217　(情報システム利用者の規定の遵守を支援するための対策)(政府機関統一基準の対応項番 8.1.1(2))

第二百十七条　部局技術責任者は、利用者等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。

解説：「利用者等による規定の遵守を支援する機能」について

利用者等がポリシー及びそれに基づく規程等を守ることを前提としつつ、情報システムの仕組みとして、情報セキュリティインシデントが発生しにくい利用環境を利用者等に提供することにより、組織全体のセキュリティ水準を確保することを求める事項である。例えば、次条に示したとおり、閲覧するとウイルス感染被害に遭うことが判明しているサイトや受信した電子メールをフィルタリングして閲覧不可にすることで被害を回避するなどが考えられる。
これ以外にも、例えば、利用者等が意図しない相手に電子メールを送信することをシステム的に抑止する対策として以下のような機能を情報システムに導入すること等も考えられる。
・送信者のメールアドレスのドメイン名以外のドメインのアドレスが宛先アドレスに含まれる場合に警告を表示するなど、入力された宛先アドレスをチェックして警告する機能
・To、Cc、Bcc に入力された宛先アドレスの数が設定数以上になっているときに警告する機能
・添付ファイルがある場合に警告する機能
・送信メールの件名、本文、添付ファイルにあらかじめ設定した文字列が含まれる場合に警告する機能
・送信者が送信指示を行った後、あらかじめ設定された時間だけ送信を保留することにより、送信者が誤送信に気が付いた場合に、送信を取り消すことができる機能

C2101-218　(情報システム利用者の規定の遵守を支援するためのウェブサイト、電子メールに

係る対策）（政府機関統一基準の対応項番 8.1.1(2)-1,2）

第二百十八条　部局技術責任者は、学外のウェブサイトについて、利用者等が閲覧できる範囲を制限する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

一　ウェブサイトフィルタリング機能

二　事業者が提供するウェブサイトフィルタリングサービスの利用

２　部局技術責任者は、利用者等が不審なメールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

一　受信メールに対するフィルタリング機能

二　受信メールをテキスト形式で表示する機能

三　スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがないメールクライアントの導入

四　受信メールに添付されている実行プログラム形式のファイルを削除することで実行させない機能

解説：第２項第２号「テキスト形式で表示する機能」について

いわゆるフィッシング等の脅威が想定される外部からの電子メールを受信する情報システムを対象とした規定である。HTML 形式の電子メールは、その形式の特徴が悪用され、本文中の URL を偽装した電子メールを送ることにより、フィッシング行為や不正プログラムを埋め込んだウェブサイトへの誘引行為に利用されている。フィッシング等の被害に遭うリスクが想定される場合には、テキスト形式や RTF(Rich Text Format)形式等の URL 偽装のリスクの無い形式で表示することが望ましい。

第２項４号「実行プログラム形式のファイルを削除する」について

実行プログラム形式のファイルとは、利用者がダブルクリックするなどしてファイルを開いたときに自動的にプログラムコード（当該ファイルの作成者が意図した任意のコード）が実行される形式のファイルのことであり、拡張子が「.exe」の形式のものがこれに該当するほか、「.pif」、「.scr」、「.bat」等のものも該当する。実行プログラム形式のファイルは、不正プログラムを感染させる手段として標的型攻撃等に悪用されることが多いことから、特に電子メールに添付された実行プログラム形式のファイルについては、行政事務従事者がこれを開くことができないよう、システム的に抑止する機能を導入することを基本対策事項としている。ファイルを削除等する機能の例としては、電子メールの中継サーバにおいて、中継する電子メールの全てを検査して、実行プログラム形式のファイルが添付ファイルとして含まれている場合にはその添付ファイルを削除する機能が挙げられるほか、中継サーバでの削除に代えて、電子メールを受信した端末側で該当する添付ファイルを開けないようにする機能等が想定される。

また、実行プログラム形式のファイルは、「.zip」、「.lzh」等の圧縮形式のファイルの内部に含められることがあり、行政事務従事者が圧縮形式のファイルを

展開し、展開後に現れる実行プログラム形式のファイルを開いてしまうことにより、不正プログラムに感染する事態も想定されることから、圧縮形式のファイルの内部に含められた実行プログラム形式のファイルも削除等の対象とする必要がある。
なお、パスワードを用いて暗号化された圧縮形式のファイルについては、当該ファイル中に実行プログラム形式のファイルが含まれるか否かを技術的に検査できないことから、そのような場合は、暗号化された圧縮形式のファイル自体を添付ファイルから削除等する機能の導入を考慮する必要がある。圧縮形式のファイル中のファイルの検査をする機能を導入する代わりに、暗号化の有無にかかわらず圧縮形式のファイルのすべてを削除等する措置を用いてもよい。
これらファイル削除等の機能の導入は、行政事務従事者に一定の不便をもたらすことになり得るが、これを実施せず、開いてよいファイルか否かを行政事務従事者に添付ファイルの拡張子を個々に確認させる方法を代用策とした状態では、標的型攻撃等を企図した電子メールの添付ファイルを誤って開いてしまう危険性を十分に抑制することは困難であることから、これをシステム的に抑止する機能の導入が推奨される。

C2101-219　（情報システムの利用時の基本的対策）（政府機関統一基準の対応項番 8.1.1(3)）

第二百十九条　利用者等は、研究教育事務の遂行以外の目的で情報システムを利用しないよう努めること。

２　利用者等は、部局技術責任者が接続許可を与えた通信回線以外に本学の情報システムを接続しないこと。

３　利用者等は、学内通信回線に、部局技術責任者の接続許可を受けていない情報システムを接続しないこと。

４　利用者等は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを研究教育事務上の必要により利用する場合は、部局技術責任者の承認を得ること。

５　事務従事者は、接続が許可されていない機器等を情報システムに接続しないこと。

６　利用者等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。

７　利用者等は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。

８　利用者等は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、部局技術責任者又は職場情報セキュリティ責任者の許可を得ること。

解説：第１項「研究教育事務の遂行以外の目的で情報システムを利用しないよう努める」について
研究教育事務の遂行以外の目的で情報システムを利用した場合の脅威を回避するための規定である。脅威の例としては、意図せず悪意のあるウェブサイトを閲覧することによって、不正プログラムに感染することが想定される。

第２項「接続許可を与えた通信回線以外」について
適切な管理がなされていない通信回線に端末を接続することにより、通信傍受等の脅威にさらされることを回避するための規定である。
学内通信回線であっても学外通信回線であっても、許可を得ていない通信回線に接続してはならない。モバイル端末を持ち出した際に接続する通信回線については、学内通信回線以外の利用となり、盗聴等の脅威が増大することから、許可されていない通信回線への接続は回避すべきである。ただし、出張先等で利用する通信回線が未定の場合は、事前の許可が難しいことから、回線の種別（通信事業者の回線・公衆無線 LAN 回線等）で管理すること等も考えられる。

第３項「接続許可を受けていない情報システム」について
学内通信回線を保護するための対策である。私物の端末等、利用を許可されていないサーバ装置、端末等を学内通信回線に接続することを禁止している。

第４項「部局技術責任者の承認を得る」について
利用者等が、利用を認めるソフトウェア以外のソフトウェアを利用する必要がある場合に、部局技術責任者に利用を申請し承認を得ることを求める規定である。なお、承認を得る際には、製品名、バージョン、入手方法（ソフトウェアの入手元となる URL、事業者名等）、入手可能な場合には利用規約等を添付して、部局技術責任者に申請することが望ましい。

第５項「接続が許可されていない機器等」について
出所不明の USB デバイスやセキュリティ管理が不十分な私物のスマートフォン等が情報システムに接続されることが許容されていると、不正プログラム感染等のリスクが高まることから、情報システムへ接続可能な機器等（又は接続を禁止する機器等）をあらかじめ定めておくとよい。
第二百十六条「(解説)「出所不明の媒体」について」も参照のこと。

第７項「定められた安全管理措置」について
第二百十三条「情報システムの利用に関する規定の整備」において全学実施責任者が定めた安全管理措置の実施を求めている。取り扱う情報の格付や取扱制限に応じた、適切な安全管理措置が求められる。

第８項「許可を得る」について
第二百十三条「情報システムの利用に関する規定の整備」において全学実施責任者が定めた許可手続の実施を求めている。情報システムの利用開始時の許可申請だけではなく、利用期間満了時又は利用終了時の手続等を定めている場合があるので、定められた手順に従って、適切に措置する必要がある。

C2101-220　（情報システムを不正操作から保護するための対策）（政府機関統一基準の対応項番 8.1.1(3)-1）

第二百二十条　利用者等は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下を例とする措置を講ずること。
一　スクリーンロックの設定
二　利用後のログアウト徹底
三　利用後に情報システムを鍵付き保管庫等に格納し施錠

C2101-221　（電子メール・ウェブの利用時の対策）（政府機関統一基準の対応項番 8.1.1(4)）
第二百二十一条　利用者等は、要機密情報を含む電子メールを送受信する場合には、本学が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。
２　利用者等は、学外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名にＡ大学ドメイン名を使用すること。ただし、当該学外の者にとって、当該利用者等が既知の者である場合は除く。
３　利用者等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。
４　利用者等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。
５　利用者等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。
６　利用者等は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。
一　送信内容が暗号化されること
二　当該ウェブサイトが送信先として想定している組織のものであること

解説：第１項「送受信」について

「送受信」には電子メールの「転送」が含まれる。したがって、本学支給以外の電子メールサービスの電子メールアドレスに要機密情報を含む電子メールを転送することは、許可を得ている場合を除き、認められない。特に、自動転送については、許可を受けている場合であっても、当該電子メールに含まれる情報の格付及び取扱制限にかかわらず行われるため、第四十六条「情報の運搬又は送信」に規定されている要機密情報の送信についての遵守事項に違反しないように留意する必要がある。

第３項「不審な電子メール」について

「不審な電子メール」とは、受信する覚えのない電子メールであって、電子メール本文中に URL が記載されているもの、実行形式や文書形式のファイルが添付されているもの等が該当する。こういった電子メールについて、むやみに URL のリンク先や添付ファイルを開かないことも重要であるが、開かなかった場合でも他の者が同種の電子メールを受信することも考えられるため、情報提供を行うことも重要である。定められた連絡先としては、CSIRT や当該電子メールを扱う情報システムの部局技術責任者等が考えられる。

第４項「情報セキュリティに影響を及ぼすおそれのある設定変更を行わない」

について
例えば、以下のようなブラウザのセキュリティ設定項目について、変更すると悪意のあるソフトウェアが端末において実行されること等により、情報の漏えいや、他のサーバ装置及び端末を攻撃することを引き起こすことも考えられるため、変更が可能であったとしても勝手に変更しないようにする必要がある。
＜ブラウザのセキュリティ設定項目の例＞
・ActiveX コントロールの実行
・Java の実行

第６項第１号「送信内容が暗号化されること」について
主体認証情報等を入力して送信する場合には、ブラウザの鍵アイコンの表示を確認するなどにより、SSL（TLS）等の暗号化通信が使用され、要機密情報が適切に保護されることを確認することを求める事項である。
なお、「閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合」とは、例えばウェブメール本文の入力欄に要機密情報を入力すること等を指す。

第６項第２号「当該ウェブサイトが送信先として想定している組織のものであること」について
ブラウザで主体認証情報等を入力して送信する場合には、ウェブサーバの電子証明書の内容から当該ウェブサイトが想定している組織のものであることを確認するなどの方法により、適切でない送信先に当該情報を誤って送信することを回避する必要がある。
なお、ウェブサイトの閲覧時にウェブサーバの電子証明書が適切でない旨の警告ダイアログが表示された場合には、当該ウェブサイトがなりすましに利用されている可能性があるため、利用を中止する必要がある。
近年において被害が広がっている「フィッシング(Phishing)」と呼ばれる悪質な行為に対しても十分警戒する必要がある。フィッシングは、悪意ある第三者等が、実在する機関等からのお知らせであるかのように偽装した電子メールを送りつけ、受け取った者にその電子メールに記載された URL をクリックさせ、あらかじめ用意された偽のウェブサイトに誘導し、ID、パスワード、その他重要な情報を記入させて、情報を窃取するという行為である。このようなフィッシングの被害を避けるためにも、本項で示す対策を実施することが重要である。

C2101-222　（識別コード・主体認証情報の取扱い）（政府機関統一基準の対応項番 8.1.1(5)）
第二百二十二条　利用者等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。
２　利用者等は、自己に付与された識別コードを適切に管理すること。
３　利用者等は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。
４　利用者等は、自己の主体認証情報の管理を徹底すること。

解説：第１項「自己に付与された識別コード以外の識別コード」について

自己に付与された識別コード以外の識別コードを使って、情報システムを利用することは、合理的な理由が無い限り「なりすまし行為」である。仮に、悪意がなくても、他者の識別コードを使って情報システムを利用することは、許容されてはならない。例えば、何らかの障害により自己の識別コードの使用が一時的に不可能になった場合には、まず、当該情報システムを利用して行おうとしている業務について、他者へ代行処理を依頼することを検討すべきであり、仮に他者の許可を得たとしても、他者の識別コードを使用することはあってはならない。要するに、行為が正当であるか否かにかかわらず、他者の識別コードを使って、情報システムを利用するということは制限されなければならない。業務の継続のために、他者の識別コードを使うことが不可避の場合には、例外措置の手続を行う際に本人の事前の了解に加えて、部局技術責任者の承認を得ることが最低限必要である。また、他者の識別コードを使用していた期間とアクセスの内容を、事後速やかに、部局技術責任者に報告しなければならない。部局技術責任者は、その理由と使用期間を記録に残すことによって、事後に当該識別コードを実際に使用していた者を特定できるように備えることが望ましい。

いずれの場合も、使用する識別コードの本人からの事前の許可を得ずに、その者の識別コードを使って、情報システムを利用することは禁止されるべきである。

第３項「管理者としての業務遂行時に限定して」について

例えば、情報システムの OS が Windows であれば、管理者権限なしの識別コードと管理者権限ありの識別コードの両方を付与された場合において、端末の設定変更等の管理者権限が必要な操作をしないときには、管理者権限なしの識別コードを使用し、その一方、管理者権限が必要な操作をするときに限って管理者権限を使用するなどの運用が考えられる。

C2101-223　（識別コードの適切な管理に係る対策）（政府機関統一基準の対応項番 8.1.1(5)-1）

第二百二十三条　利用者等は、自己に付与された識別コードを適切に管理するため、以下を含む措置を講ずること。

一　知る必要のない者に知られるような状態で放置しない。

二　他者が主体認証に用いるために付与及び貸与しない。

三　識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止する。

解説：第１号「知る必要のない者に知られるような状態で放置しない」について

多くの場合、識別コード単体は必ずしも秘密ではないが、必要以上の範囲に開示する、又は公然となるような状態で放置しないように求めている。

主体認証には、識別コードと主体認証情報の組合せが用いられる。識別コードの開示範囲を必要最小限に止めることによって、第三者が不正に主体認証を行う可能性をより低くすることができる。そのため、識別コードを適切に管理す

ることが必要である。

第２号「他者が主体認証に用いるために付与及び貸与しない」について
部局技術責任者が明示的に共用識別コードとしているもの以外の識別コードを共用してはならない。

第３号「定められた手続に従い、識別コードの利用を停止する」について
識別コードを使用する必要がなくなった場合に、利用者等自らが部局技術責任者へ届け出ること等、定められた手続に従い、識別コードを使用できない状態に変更することを求めている。ただし、例えば、卒業、人事異動等によって、利用者等の識別コードが大規模に変更となる場合や、その変更を部局技術責任者が利用者等自らからの届出によらず把握できる場合等、利用者等自らの届出が不要となる条件を部局技術責任者が定めてもよい。

C2101-224　（主体認証情報の適切な管理に係る対策）（政府機関統一基準の対応項番 8.1.1(5)-2,3）

第二百二十四条　利用者等は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。

一　自己の主体認証情報を他者に知られないように管理する。

二　自己の主体認証情報を他者に教えない。

三　主体認証情報を忘却しないように努める。

四　主体認証情報を設定するに際しては、容易に推測されないものにする。

五　異なる識別コードに対して、共通の主体認証情報を用いない。

六　異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない。（シングルサインオンの場合を除く。）

七　部局技術責任者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更する。

２　利用者等は、所有による主体認証情報を用いる場合には、以下の管理を徹底すること。

一　主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する。

二　主体認証情報格納装置を他者に付与及び貸与しない。

三　主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する。

四　主体認証情報格納装置を利用する必要がなくなった場合には、これを部局技術責任者に返還する。

解説：第１項第１号「自己の主体認証情報を他者に知られないように管理する」について
例えば、以下に挙げる他者からのパスワード窃取行為に注意する必要がある。
・パスワードを入力する際に他者が周囲から盗み見する。
・他者が管理者を名乗ってパスワードを聞き出す。
また、以下に挙げる行為は行うべきではない。

・自己のパスワードを、内容が分かる状態で付箋等に記入してモニタ、端末本体、及びその周辺に貼付する。
・自己のパスワードを、特段の保護をせずに平文のままテキスト形式で保存する。など、容易に他者に知られてしまう状態で、情報システム上に記録する。

第１項第２号「自己の主体認証情報を他者に教えない」について
たとえ、他者に処理を代行させる目的であっても、利用者等は自己の主体認証情報を他者に教示してはならない。主体認証情報を他者に教示することによって、情報システムの識別コードと実際の操作者との関係が曖昧になり、アクセス制御、権限管理、ログ管理その他のセキュリティ対策が効果を失う可能性がある。また、教示された者にとっても、例えば、当該識別コードによって不正行為が発生した場合は、その実行者として疑義を受ける可能性がある。そのため、自己の主体認証情報は他者に「教えない」ことを徹底すべきである。

第１項第３号「主体認証情報を忘却しないように努める」について
他者が容易に見ることができないような措置（施錠して保存するなど）や、他者が見ても分からないような措置（独自の暗号記述方式等）をしていれば、必ずしも、メモを取る行為を禁ずるものではない。むしろ、忘れることのないように努めなければならない。
なお、本人の忘却によって主体認証情報を初期化（リセット）する場合には、初期化が不正に行われたり、初期化された情報が本人以外に知られたりすることのないように情報システムを構築・運用することが望ましい。例えば、情報システムによる自動化により無人で初期化できるようにすることが、初期化情報の保護のみならず、運用の手間を低減することに役立つことについても勘案して検討すること等が考えられる。

第１項第４号「容易に推測されないもの」について
辞書に載っている単語、利用者の名前や利用者個人に関連する情報から簡単に派生させたもの等、容易に推測されるものを用いてはならない。また、使用する文字種として、数字だけでなく、アルファベットの大文字及び小文字、さらに特殊記号等も織り交ぜて主体認証情報を構成することが望ましい。

第１項第５号「共通の主体認証情報を用いない」について
複数の識別コードを付与されている場合に、それら識別コードに対して共通の主体認証情報を用いると、一つの識別コードに対応する主体認証情報が漏えいした場合に、他方の識別コードを用いた不正アクセスを受ける危険性が高くなる。したがって、共通の主体認証情報を用いてはならない。

第１項第６号「識別コード及び主体認証情報についての共通の組合せ」について
複数の情報システムにおいて、共通の識別コードを使用し、かつ、共通の主体

認証情報を設定していた場合、ある情報システムから漏えいした主体認証情報が他の情報システムで不正に使用されるという情報セキュリティインシデントが発生することが考えられる。したがって、複数の情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを使用しないようにしなければならない。特に、本学支給の情報システムと本学支給以外の情報システムとの間では、共通の識別コード及び主体認証情報を使用しないよう注意する必要がある。

第１項第７号「主体認証情報を定期的に変更する」について
定期的な変更の要求をシステムで自動化できることが望ましいが、技術的に困難な場合には、定期的に変更依頼を通達するなどの運用によって対処してもよい。

第２項第１号「主体認証情報格納装置を本人が意図せずに使われることのないように」について
主体認証格納装置の例としては、建物への入退や端末ログインに必要となるICカード等が挙げられる。所有による主体認証方式では、本人でなくとも主体認証情報格納装置を保持する者が正当な主体として主体認証されるため、他者に当該装置を使用されることがないように適切に管理する必要がある。

C2101-225　（暗号・電子署名の利用時の対策）（政府機関統一基準の対応項番 8.1.1(6)）

第二百二十五条　利用者等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。

２　利用者等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。

３　利用者等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

解説：第１項「定められたアルゴリズム及び方法に従う」について
情報システムにおいて、認められていないアルゴリズムを利用することを禁止しているものである。暗号アルゴリズムは、ファイル単体の暗号化やハードディスク全体の暗号化、ブラウザを使う通信の暗号化等、様々な場面で利用されていることから、利用する場面ごとに適切なアルゴリズムを適切な方法で利用する必要がある。
部局技術責任者は、利用者等の暗号機能の利用において、認められていないアルゴリズムが利用されないよう、あらかじめ情報システムにおいて対処しておくことが望ましい。

暗号化された情報の復号や電子署名の付与に用いる鍵（以降本項において「鍵」という）の管理手樹として、情報システム共通として鍵の保存手順を定めている場合と、情報システムごとに鍵の保存手順を個別に定めている場合があるので、各情報システムに対応した手順に従うことが求められる。

第３項「鍵のバックアップ手順に従い、そのバックアップを行う」について
暗号化された情報の復号に用いる鍵の滅失により、情報の可用性が損なわれるおそれがあることから、適切に鍵をバックアップすることを求めている。
バックアップが必要な鍵については、バックアップの取得又は第三者への鍵情報の預託に関する手順等の規定に従う必要がある。
また、バックアップしてはならない鍵や、鍵情報の複製が、その漏えいに係るリスクを高める可能性があるなどについても留意し、バックアップは必要最小限にとどめることも大切である。

C2101-226　（不正プログラム感染防止）（政府機関統一基準の対応項番 8.1.1(7)）
第二百二十六条　利用者等は、不正プログラム感染防止に関する措置に努めること。
２　利用者等は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずること。

解説：第１項「不正プログラム感染防止に関する措置に努める」について
情報システムの利用に当たっては、利用者等自らが不正プログラム感染の予防に努めなければならない。また、不正プログラム対策ソフトウェアが全ての不正プログラムを検知できるとは限らないことを念頭に入れ、不正プログラムに感染するリスクを低減するために、可能な措置の実施に努める必要がある。

第２項「通信回線への接続を速やかに切断するなど、必要な措置を講ずる」について
不正プログラムに感染したおそれがある情報システムについては、他の情報システムへの感染等の被害の拡大を防ぐ必要がある。当該情報システムを構成するサーバ装置又は端末が通信回線に接続している場合には、それを切断するなど感染拡大を防止する措置を行い、第３章第４節「情報セキュリティインシデントの対処」に定められた報告や連絡等の対処を行うことが求められる。
不正プログラムに感染したおそれのある場合の対処について、手順が規定されている場合、その内容に従う必要がある。

C2101-227　（不正プログラム感染防止に係る対策）（政府機関統一基準の対応項番 8.1.1(7)-1,2,3）
第二百二十七条　利用者等は、不正プログラム対策ソフトウェアを活用し、不正プログラム感染を回避するための以下措置に努めること。
一　不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しない。また、検知されたデータファイルをアプリケーション等で読み込まない。
二　不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持する。
三　不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にする。
四　不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施する。

2　利用者等は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

3　利用者等は、不正プログラムに感染するリスクを低減する情報システムの利用方法として、以下のうち実施可能な措置を講ずること。

一　不審なウェブサイトを閲覧しない。

二　アプリケーションの利用において、マクロ等の自動実行機能を無効にする。

三　プログラム及びスクリプトの実行機能を無効にする。

四　安全性が確実でないプログラムをダウンロードしたり実行したりしない。

解説：第１項第１号「実行ファイルを実行しない」について

不正プログラムとして検知された実行プログラム形式のファイルを実行した場合には、たとえ他の情報システムへ感染を拡大させることがなくても、復旧に相当な労力を要することとなるため、このような実行プログラム形式のファイルを実行しないよう努めなければならない。

第１項第２号「最新の状態に維持する」について

一般的に不正プログラムはほぼ毎日のように新種や亜種が出現しているため、不正プログラム対策ソフトウェア等のアプリケーション及び不正プログラム定義ファイル等を更新機能や更新プログラムにより最新の状態に維持することで、不正プログラム等に感染することを回避する必要がある。自動的に最新化する機能を持つ製品については、当該機能を利用することにより最新状態の維持が可能になる。

また、最新の状態に維持する方法としては、端末ごとに利用者が自動化の設定をする方法のほか、部局技術責任者等が管理する端末を一括して自動化する方法もあるため、情報システムごとに定められた方法に従うこと。

第１項第３号「自動検査機能を有効にする」について

手動による対策実施は、実施漏れや遅れが発生する可能性があるため、不正プログラム対策の中で自動化が可能なところは自動化することが望ましい。

自動検査機能の例としては、ファイルの作成や参照のたびに検査を自動的に行う機能等がある。

第１項第４号「不正プログラムの検査を実施する」について

第１項第３号の自動検査機能が有効になっていたとしても、検査した時点における不正プログラム定義ファイルでは検知されない不正プログラムに感染している危険性が残る。このような危険性への対策として、定期的に全てのファイルについて検査する必要がある。

第２項「外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合」について

「外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合」には、ウェブの閲覧や電子メールの送受信等のネットワークを経由する場合だけ

でなく、USB メモリや CD-ROM 等の外部電磁的記録媒体を経由するものも含む。

第十八章　本学支給以外の端末の利用

解説：研究教育事務の遂行においては、本学から支給された端末を用いて研究教育事務を遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず本学支給以外の端末を利用して情報処理を行う必要が生じる場合がある。この際、当該端末は本学が支給したものではないという理由で、利用者等へ情報セキュリティ対策の実施を求めなかった場合、当該端末で取り扱われる情報セキュリティ水準が、ポリシー及びそれに基づく規程等を満たさないおそれがある。
したがって、そのような可能性がある場合は、本学支給以外の端末を利用者等が安全に利用するための手続や安全管理措置の規定をあらかじめ整備し、本学における厳格な管理の下で利用させることが必要である。
また、本学支給以外の端末であっても、本学から支給されるモバイル端末と同等の情報セキュリティ水準の確保が求められることから、第１４章第１節「端末」も参照し、同等の安全管理が実施されるよう、規定を整備し、利用者等に安全管理措置を講じさせる必要がある。

C2101-228　（本学支給以外の端末の利用規定の整備・管理）（政府機関統一基準の対応項番 8.2.1(1)）

第二百二十八条　全学実施責任者は、本学支給以外の端末により研究教育事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。

２　全学実施責任者は、要機密情報について本学支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。

３　部局総括責任者は、本学支給以外の端末による研究教育事務に係る情報処理に関する安全管理措置の実施状況を管理する責任者を定めること。

４　前項で定める責任者は、要機密情報を取り扱う本学支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、利用者等に適切に安全管理措置を講じさせること。

解説：第１項「許可等の手続に関する手順」について
本学支給以外の端末の利用に当たっては、第１８章「(解説)」にも記載されているとおり、厳格な管理を行うことが不可欠である。利用に関する手続や安全管理措置を定めて、利用者等にそれを適切に講じさせないと、以下のようなリスクが想定される。
・不正プログラムに感染し、要機密情報が外部に漏えいする。
・端末の盗難・紛失等により、要機密情報が外部に漏えいする。
・利用者の知識不足により、利用者の意図に反して要機密情報が海外のクラウドに保存され、第三者に閲覧される。
・家族や知人の端末操作により端末内の要機密情報が外部に漏えいする。
本学支給以外の端末の利用を許可するに当たり、本学としての利用方針を定めておくことが望ましい。個別判断により本学支給以外の端末の利用を認めてし

まうと、上記のリスクが顕在化する可能性が高いことから、本学支給以外の端末の利用を認めるのであれば、本学としての利用方針の下、厳格な管理を行う必要がある。
本学支給以外の端末の利用方針として、例えば以下の事項の明確化が考えられる。
・利用を許可する部局・職場等の組織の単位
・利用を許可する利用者等の条件
・利用を許可する端末の種類（スマートフォン、携帯電話、PC 等）
・利用する機能（電子メール及びウェブ閲覧に限定 等）
また、本学支給以外の端末の利用に際して、利用する通信回線やサーバ装置等、情報システム全体として情報セキュリティを確保することが重要であることから、リモートアクセス環境や端末の安全管理措置について、システム機能として提供することも考慮すべきである。
なお、本学において本学支給以外のスマートフォン等を利用する場合の基本的な考え方、私物端末利用に当たって考慮すべきリスク、代表的な私物端末の管理対策及び技術対策については、以下の政府機関における取組を参考にするとよい。さらに、民間団体等においても、私物端末の安全な利用方法について有効な資料が公表されているので、併せて考慮されたい。

参考：各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告
「私物端末の業務利用におけるセキュリティ要件の考え方」（平成 25 年 3 月）
（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/index.html）
参考：総務省スマートフォン・クラウドセキュリティ研究会最終報告
「スマートフォンを安心して利用するために実施されるべき方策」（平成 24 年 6 月 26 日）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html）

第 2 項・第二百三十条「安全管理措置」について
本学支給以外の端末を業務に利用することを認めるのであれば、当該本学支給以外の端末が不正プログラムの感染源や情報の漏えいの要因とならないようにすべきであり、取り扱う情報の格付及び取扱制限に関わらず、情報セキュリティ確保のための安全管理措置を利用者等に講じさせることが必要である。
なお、利用者等が講ずるべき安全管理措置が不十分であることが十分考えられるため、第二百三十一条に示すシステム機能による情報セキュリティ対策により、一定のリスクを低減した上で利用者等に利用させる方法を実施することが望ましい。

第 3 項「安全管理措置の実施状況を管理」について
本学支給以外の端末を利用者等が利用するに当たって、申請時に安全管理措置の実施状況について端末を目視確認する方法や、定期的な実施状況の確認を管

理者にて行うことをあらかじめ定めておく方法等が考えられる。管理工数の増加が懸念される場合は、サンプリングによる確認や定期的な注意喚起を利用者に行うなどの方法で管理作業の効率化を図ることも考えられる。

第３項「責任者」について
本学支給以外の端末の安全管理措置の実施状況を管理する責任者であり、PC やスマートフォン等に対して一定以上の知見を有している者がその任に当たることが望ましい。例えば、本学 LAN システムの部局総括責任者等が考えられる。ただし、利用者等の安全管理措置の実施状況について適時状況を把握することが求められるため、職場情報セキュリティ責任者が兼ねることも考えられる。

C2101-229　（本学支給以外の端末を利用する際の許可等の手続に関する手順の整備）（政府機関統一基準の対応項番 8.2.1(1)-1）

第二百二十九条　全学実施責任者は、以下を例に本学支給以外の端末を利用する際の許可等の手続に関する手順を整備し、利用者等に周知すること。

一　以下を含む本学支給以外の端末利用時の申請内容
- 申請者の氏名、所属、連絡先
- 利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）
- 利用する端末の機種名
- 利用目的、取り扱う情報の概要、機密性３情報の利用の有無等
- 主要な利用場所
- 利用する主要な通信回線サービス
- 利用する期間

二　利用許諾条件

三　申請手順

四　利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順

五　利用期間満了時の利用終了又は利用期間更新の手続方法

六　許可権限者（前条第３項において定める、本学支給以外の端末の安全管理措置の実施状況を管理する責任者（以下、次条及び第二百三十一条において「端末管理責任者」という。））

解説：第１号「利用する端末の契約者の名義」について
契約者の名義の提示を求めるのは、業務に使用する端末の名義人と使用人の一致を確認するためである。端末の名義人が端末の利用に係る契約者であり、業務への使用や通信費用に係る訴訟リスクを回避するためには、利用申請時に使用人と名義人が一致していることの確認が必要である。
なお、名義人と使用人である申請者が同一であることを利用条件とする場合は、名義人の確認を求める必要はない。

第１号「利用する期間」について
本学支給以外の端末を利用する際に、利用の都度申請手続を行うと事務処理が煩雑化する可能性があるため、例えば１年間の利用期間を定め、包括的な許可

を与えるなどして事務処理を効率化する方法も考えられる。この場合は、安全管理措置の実施状況について定期的なチェックを行うなどの対応が求められる。

第２号「利用許諾条件」について
利用者等に本学支給以外の端末の利用を許可するに当たり、以下の内容を例とした利用許諾条件を示し、許諾書にサインするなどして利用者の同意を証拠として残しておく必要がある。
・情報の格付及び取扱制限に応じた取扱いの遵守
・定められた安全管理措置の遵守
・組織による利用状況の情報収集の承諾
・組織による利用端末の制御及び端末の設定変更の承諾
・盗難・紛失時に個人の情報を含めた遠隔データ消去を行うことの承諾（職務上取り扱う情報のみ遠隔消去可能なツールを導入する場合は不要）
・情報セキュリティインシデント発生時の迅速な届出
・機種変更や端末交換の際の再届出の遵守
・その他、部局技術責任者等の管理責任者の指示の遵守

第６号「許可権限者」について
本学支給以外の端末の利用の許可申請においては、許可権限者である端末管理責任者の許可を得ることになるが、必要に応じて取り扱う情報の管理責任を持つ職場情報セキュリティ責任者の許可を同時に得る手続を定めるとよい。また、リモートアクセスにより本学の情報システムへのアクセスを行わせる場合には、当該情報システムを所管する部局技術責任者の許可を得る手続を併せて定めることも考えられる。（職場情報セキュリティ責任者又は部局技術責任者への許可申請については、第二百三十二条第１項で規定。）

C2101-230　（本学支給以外の端末により要機密情報を取り扱う場合の実施手順の整備）（政府機関統一基準の対応項番 8.2.1(1)-2）
第二百三十条　全学実施責任者は、本学支給以外の端末により要機密情報を取り扱う場合は、利用者等が講ずるべき安全管理措置の実施手順について、以下を例に整備すること。
一　パスワード等による端末ロックの常時設定
二　OS やアプリケーションの最新化
三　不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（本学として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）
四　遠隔データ消去機能の設定
五　要機密情報の暗号化等による秘匿性の確保
六　端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）
七　本学提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）
八　以下を例とする禁止事項の遵守
・端末、OS、アプリケーション等の改造行為

・安全性が確認できないアプリケーションのインストール及び利用
・利用が禁止されているソフトウェアのインストール及び利用
・許可されない通信回線サービスの利用（利用する回線を限定する場合）
・第三者への端末の貸与

解説：第３号「不正プログラム対策ソフトウェアの導入」について

OS の構造等により、不正プログラム対策ソフトウェアが提供されていない、又は部分的にしか対策機能が有効でないスマートフォンや携帯電話等の利用については、通信事業者によって事前に安全性が確認されたアプリケーションのみ当該端末へダウンロード可能とされているなどの別の方法で安全性を確保する必要がある。

第４号「遠隔データ消去機能」について
第百五十二条「(解説) 第６号「遠隔データ消去機能」について」を参照のこと。

第５号「要機密情報の暗号化等による秘匿性の確保」について
本学支給以外の端末に要機密情報を保存して業務を行う場合は、端末に保存する情報を暗号化して盗難・紛失時の情報漏えいのリスクを低減する必要がある。情報へのアクセス権を管理する方法もあるが、記憶媒体の内容を直接読み出されるなどの手法でアクセス権管理機構を回避されるリスクが残るため、要機密情報は暗号化して保存することが望ましい。遠隔データ消去機能を補助的な機能として組み合わせると効果的である。
また、安全性を確保するためには暗号化に用いる鍵の管理が重要になる。端末紛失時に端末内に鍵や、鍵を生成するために必要な全ての情報を保持していると暗号化したデータを復号されるリスクがある。
したがって、業務利用していないときはこれらを保持しないなど、鍵の漏えいリスクが低減されるような管理の仕組みを持つ以下の例のようなツールを導入するとよい。
<例> 暗号化する範囲を業務領域に限定しパスワードを入力するタイミングを業務システムへのログイン時、パスワードを基に生成した鍵を消去するタイミングをログアウト時（又はタイムアウト時）とする。
なお、次条に示すリモートアクセス環境を本学として整備し、当該環境以外での要機密情報の取扱いを禁止すれば、利用者等による安全管理措置が不要になる。

第８号「端末、OS、アプリケーション等の改造行為」について
iOS における Jailbreak や Android における root 化のように、ソフトウェア等の改造が行われた端末は外部からの攻撃の的となりやすく、不正パケットの受信によって不正プログラムに感染したり、端末が乗っ取られたりする危険性が高くなる。
このような改造された端末が業務に使用されると、端末に保存された情報が漏えいするなどの情報セキュリティインシデントが発生する可能性があるため、

本学支給以外の端末を利用する際は、事前に端末、OS、アプリケーション等の改造行為を行わないことについて、利用者等と同意しておくことが重要である。私物のスマートフォンを業務利用することを目的とした、MDM（Mobile Device Management）ツール等を本学のリモートアクセス環境と組み合わせ、改造された端末を検知するなどして、システム的に改造端末の使用を回避する方法も考えられる。

第８号「安全性が確認できないアプリケーション」について
スマートフォンにおいては、専用のアプリケーション提供サイト等からオンデマンドでアプリケーションをダウンロードする利用形態が一般的であるが、不正プログラム等が混在する提供サイトの存在が懸念されるため、業務に利用する私物のスマートフォン等においては安全性が不明なアプリケーションがインストールされた状態で利用されることがないように、例えば OS 提供事業者や通信事業者等がアプリケーションの安全性の審査を行っている信頼性の高いアプリケーション提供サイトにて提供されるアプリケーションのみに利用を限定すること等を対策にするとよい。ただし、大手の事業者であっても安全なアプリケーションを提供しているとは限らないので、提供サイトを運営する事業者のセキュリティ対策水準を十分見極めた上で判断することが求められる。
スマートフォンを安全に利用するための留意事項として、OS の最新化及び不正プログラム対策とともに注意喚起されているので、参考にすること。

参考：総務省「スマートフォン情報セキュリティ３カ条」（スマートフォン・クラウドセキュリティ研究会中間報告）（平成 23 年 12 月 19 日公表）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000015.html）

第８号「利用が禁止されているソフトウェア」について
第百五十条第３項の対策として、本学支給の端末において規定される利用を禁止するソフトウェアと同等であることが考えられるが、例えば個人利用の範囲を必要以上に制限しないよう考慮する必要がある。

第８号「許可されない通信回線サービスの利用」について
公衆無線 LAN サービスのうち無線経路の秘匿性や安全性が不明なものや接続経路の管理状況が不明な無料のインターネット接続サービス等は、通信内容の盗聴やなりすましによる情報の窃取等のおそれがあり、このような情報セキュリティ水準が不明な通信回線は業務に利用すべきではない。ただし、海外等で、情報セキュリティ水準が不明な通信回線サービスを利用せざるを得ない場合が想定されることから、例えば、情報システムへのリモートアクセス経路において VPN 回線を設定し end-end の秘匿性を確保するなどの方法を用いるとよい。なお、無線 LAN の利用に関する対策については、第１６章第１節「通信回線」の第二百四条「無線 LAN 環境導入時の対策」の内容を併せて考慮する必要がある。

第８号「第三者への端末の貸与」について
家族や知人に私物の端末等を貸与することがあるが、その際に意図的に機密性の高い情報を閲覧したり又は誤操作により機密性の高い情報を外部に転送してしまったりすることが懸念される。
私物端末であっても業務に利用するのであれば、第三者への貸与は原則禁止すべきであり、それに同意できない利用者等には私物端末を利用させるべきではない。

C2101-231　（本学支給以外の端末により要機密情報を取り扱う本学の情報システムにリモートアクセスする環境を構築する場合の対策）（政府機関統一基準の対応項番 8.2.1(1)-3）
第二百三十一条　部局技術責任者は、本学支給以外の端末により要機密情報を取り扱う本学の情報システムにリモートアクセスする環境を構築する場合、基盤となる情報システムにより本学に提供されるリモートアクセス環境が利用可能であれば活用し、端末の盗難・紛失や不正プログラム感染等により情報窃取されることを防止するために、以下を例とする対策を講ずること。
一　シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。
二　セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。
三　ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。利用者は専用のアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。

解説：「部局技術責任者」について
本条にて指定している部局技術責任者は、本学 LAN システム等のリモートアクセス先の情報システムを所管する部局技術責任者である。
第二百二十八条第３項に従って定められる“本学支給以外の端末の安全管理措置の実施状況を管理する責任者”に対して、第二百二十八条第４項において、本学支給以外の端末の盗難・紛失や不正プログラム感染等により情報窃取されることを防止するための措置を講ずることを求めているが、当該措置の例として、本学 LAN システムへの安全なリモートアクセス環境があらかじめ提供されている場合に、これを活用することを想定している。

第１号「シンクライアント等」について
端末に情報を保存させずに本学支給以外の端末を業務利用することを可能とする仕組みとして、シンクライアントやリモートデスクトップと呼ばれる技術の活用が有効である。シンクライアントやリモートデスクトップ関連の製品やソリューションサービスは、既に市場において提供されているが、外部のクラウドサービスを組み合わせて利用する場合は、第７章第１節「外部委託」又は第７章第２節「約款による外部サービスの利用」についても参照する必要がある。

なお、当該機能については、本学支給のモバイル端末においても利用することが可能であることから、本学支給のモバイル端末及び本学支給以外の端末を業務利用において共存させたい場合でも有効な対策となる。
＜シンクライアントの主な機能及び特徴＞
・業務ネットワーク内の仮想デスクトップ画面を転送
・ユーザデータを端末に残さない
・ウェブキャッシュ、接続情報、作業履歴等全てサーバ内に保管
・外部情報出力（クリップボードへのコピー、スクリーンショット、印刷、他アプリケーション連携）を抑制可能

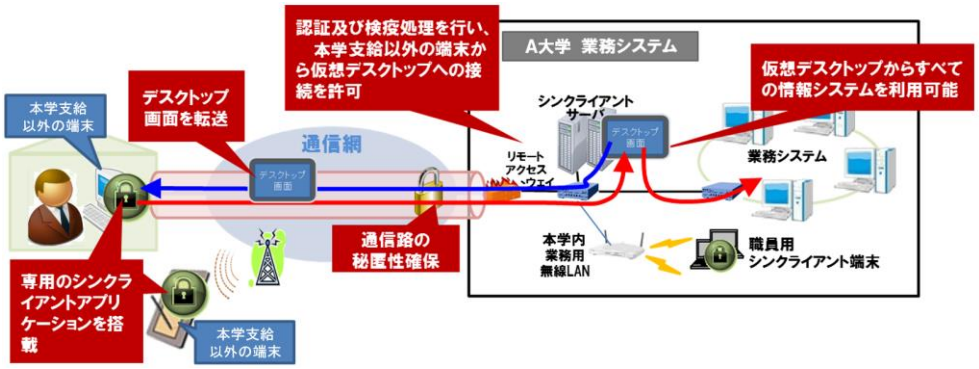


図９　シンクライアントのシステム構成例

また、シンクライアントの発展形として、仮想デスクトップ環境の利用機能（ネットワーク接続や画面描画・ディスプレイ出力、キーボード・マウス入力等）のみに機能が絞り込まれたゼロクライアントやシンクライアント専用端末の利用も有効である。特にゼロクライアントは、汎用 OS や汎用ブラウザ等を搭載していないことから、不正プログラム対策やソフトウェア更新等のセキュリティ管理の負荷が軽減でき、万一端末が故障しても、端末を交換するだけですぐに利用可能になるなど、セキュリティ管理面の負荷の軽減も期待される。処理能力やコスト負担等の課題も考えられるので、それらも勘案した上で利用を検討するとよい。

第２号「セキュアブラウザ等」について
端末に情報を保存させずに本学支給以外の端末を業務利用する別の仕組みとして、セキュアブラウザを選択することも可能である。
セキュアブラウザ製品についても、各種クラウドサービスと組み合わせたソリューションとして提供される場合があることから、外部の情報処理サービスを組み合わせて利用する場合は、第７章第１節「外部委託」又は第７章第２節「約款による外部サービスの利用」についても参照する必要がある。
当該の仕組みについても、本学支給のモバイル端末においても利用することが可能である。
＜セキュアブラウザの主な機能及び特徴＞

・電子メール、ファイル閲覧等を画面転送等で行い、ユーザデータを端末に残さない
・ブラウザ終了時に閲覧に関連する情報（ウェブキャッシュ、URL、cookie 等）を消去可能
・外部出力（クリップボードへのコピー、スクリーンショット、印刷、他アプリケーション連携）を抑制可能

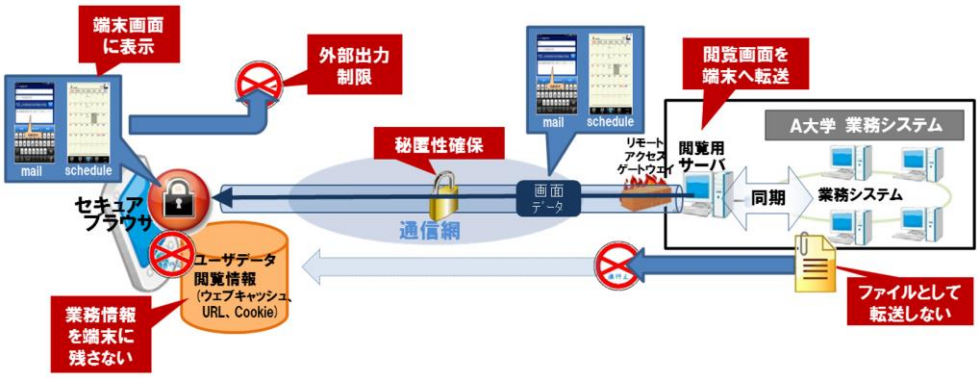


図 10　セキュアブラウザ活用型ソリューションのシステム構成例

なお、当該機能については、本学支給のモバイル端末においても利用することが可能であることから、本学支給のモバイル端末及び本学支給以外の端末を共存させたい場合において有効な対策となる。

第３号「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について
通信回線との接続環境が無い場所で業務を行うなど、やむを得ず情報を端末に保存させる必要がある場合は、セキュアブラウザやシンクライアントは利用できないことから、他の方法で安全な利用環境の提供を考える必要がある。この場合は、本学支給以外の端末にファイル暗号化等のセキュリティ機能を持つ業務専用のアプリケーションを搭載し、アプリケーション単位で情報を暗号化するなどの方法が考えられる。当該機能を有するセキュリティソリューションが製品として民間事業者より提供されていることから、それらの活用を検討するとよい。

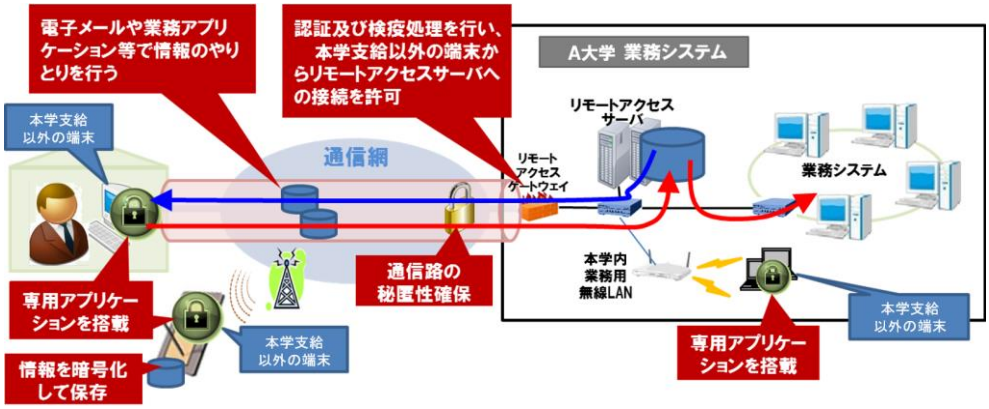


図 11　ファイル暗号化等セキュリティ機能を持つアプリケーションを活用したシステム構成例

なお、当該機能については、本学支給のモバイル端末においても利用することが可能であることから、本学支給のモバイル端末及び本学支給以外の端末を共存させたい場合において有効な対策となる。

C2101-232　（本学支給以外の端末の利用時の対策）（政府機関統一基準の対応項番 8.2.1(2)）

第二百三十二条　利用者等は、本学支給以外の端末により研究教育事務に係る情報処理を行う場合には、第二百二十八条第３項で定める責任者の許可を得ること。

２　利用者等は、要機密情報を本学支給以外の端末で取り扱う場合は、職場情報セキュリティ責任者の許可を得ること。

３　利用者等は、本学支給以外の端末により研究教育事務に係る情報処理を行う場合には、本学にて定められた手続及び安全管理措置に関する規定に従うこと。

４　利用者等は、情報処理の目的を完了した場合は、要機密情報を本学支給以外の端末から消去すること。

解説：第２項「職場情報セキュリティ責任者の許可を得る」について

利用者等は、本学支給以外の端末の利用を開始するに当たり、本学支給以外の端末の許可権限者に対して許可申請を行うことになるが、当該申請以外に、本学支給以外の端末を用いて行う業務及び取り扱う情報の管理責任者である職場情報セキュリティ責任者に対して許可を求める必要がある。

第３項「安全管理措置に関する規定に従う」について

利用者等は、本学支給以外の端末の利用に係る本学全体のポリシーをよく理解し、安全管理措置を徹底し、情報セキュリティインシデントの発生の回避に努めなければならない。特にスマートフォン等の利用については、その特性に応じたリスクを利用者である利用者等自身もよく理解した上で利用することが求められる。

第４項「要機密情報を本学支給以外の端末から消去する」について

要機密情報を消去することは必須であるが、不必要な情報及び業務用のアプリ

ケーション等についても併せて消去しておくことが望ましい。

C2102 情報システム非常時行動計画に関する規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A2103	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2013年7月5日 B2103	文書番号の変更のみ	ー
2015年10月9日 C2102	文書番号の変更のみ	ー
2016年2月5日 C2102	第一条の解説においてCSIRTに関する説明を追加	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C2102-01（目的）

第一条 この規程は、Ａ大学情報システムの運用において非常事態が発生した場合の行動を非常時行動計画として事前に定め、早期発見・早期対応により、事件・事故の影響を最小限に抑え、早急な情報システムの復旧と再発防止に努めるために必要な措置を講じることを定めることを目的とする。

解説：非常時行動計画は、情報システム運用に関するインシデントのうち特に緊急性を要する事態が発生した場合の対応を定めるものである。本学の事業の継続に重大な支障をきたす可能性が想定される大規模な火災や地震その他の災害等の事態を特定し、当該事態への対応計画は、業務継続計画（BCP：Business Continuity Plan）として策定されるべきであるが、BCP が策定されている場合には、本計画は BCP の一部として統合されるべきである。

BCP が未整備である場合を想定し、本計画は災害等による情報システムの大規模な物理的損壊、大規模障害、大規模セキュリティインシデント（ワーム等による本学情報ネットワークの輻輳や停止）、及び重大な社会的影響や法的問題に発展する可能性のある本学関係者による情報発信や、本学に対する情報発信による事件・事故（コンテンツインシデント）に関する部分を扱う。

非常時行動計画とインシデント対応手順との扱う内容の線引きについては様々な整理の仕方が考えられる。一方、すべてのインシデントには一定の緊急性が認められるともいえるので、両者を一体化しても良いかもしれない。ただし、CSIRT（情報セキュリティインシデント対応チーム）が設置されている組織であっても、非常時対策本部は非常事態ごとに臨時に設置されるものであり、両者は区別して扱う必要がある。本サンプル例では、非常時連絡窓口の設置、非常時対策本部の設置などまでを非常時行動計画に書き、物理的インシデント、セキュリティインシデント、コンテンツインシデントそれぞれに対応する具体的緊急処置は「C3102 インシデント対応手順」にて示している。

C2102-02（定義）

第二条 この規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

一　運用基本方針　本学が定めるＡ大学情報システム運用基本方針をいう。

二　運用基本規程　本学が定めるＡ大学情報システム運用基本規程をいう。

三　非常事態　本学情報システムの運用に関するインシデントのうち特に緊急性を要するものをいう。

四　その他の用語の定義は、運用基本方針及び運用基本規程で定めるところによる。

C2102-03（非常事態の報告）

第三条　全学実施責任者は、インシデントについての報告または通報を学内または学外から受けつけ、迅速に情報を集約する手段を整備し、周知・公表する。

２　全学実施責任者は、報告または通報を受けたインシデントのうち、非常事態の発生またはそのおそれがある場合には、全学総括責任者へ報告し、非常時対策本部の設置を提案する。

C2102-04（非常時対策本部）

第四条　全学総括責任者は、非常事態が発生しまたは発生するおそれが特に高いと認められる場合に、被害の拡大防止、被害からの早急な復旧その他非常事態の対策等を実施するために非常時対策本部を設置する。
２　非常時対策本部は次の各号に定める委員をもって構成する。
一　全学総括責任者
二　全学実施責任者
三　関連する部局情報システムの部局総括責任者
３　全学総括責任者は、非常時対策本部の本部長となる。
４　全学総括責任者が必要と認めたときは、委員以外の者を出席させて意見を聞くことができる。

解説：非常時対策本部は、全学総括責任者が設置し、全学総括責任者、全学実施責任者、関連する部局情報システムの部局総括責任者で構成する。全学総括責任者が本部長として全権をもち、関係者の間の緊急連絡網、情報共有体制を構築して、情報収集、証拠保全をした上で、対策を実施する。

C2102-05（非常時連絡網）

第五条　非常時対策本部には、緊急連絡及び情報共有等を行うために全学実施責任者が担当する非常時連絡窓口を設置し、関係者に周知徹底する。
２　非常時連絡窓口は、非常時対策本部長の指示に基づき、通報者や捜査当局、クレームの相手方、報道関係者等、外部との対応を直接または広報窓口を通じて行う。
３　非常時連絡窓口は、非常時対策本部長の指示に基づき、学内関係者からの情報の受付および収集、被害拡大防止や復旧のための緊急対策等の伝達を直接行う。
４　全学実施責任者は、非常時連絡窓口を中心とする非常時連絡網を整備する。
５　非常時連絡網の連絡先には、非常時対策本部委員の他、全学情報システムについては情報メディアセンター、総務部、部局情報システムについては部局技術責任者及び部局技術担当者、必要に応じて法律専門家、広報部門を設定する。

解説：連絡窓口は、全学実施責任者が担当し、通報者や捜査当局、弁護士、報道等の内外からの連絡の受付と回答（あるいはヘルプラインの役割も）を行う。連絡窓口は、全学情報システムについて情報メディアセンター（設置されている場合は CSIRT）や総務部と、部局情報システムについて部局技術責任者（及び同担当者）と連携し、法律専門家とも相談する。
本計画では、非常時対策本部設置後は、通常のインシデントの通報連絡体制がピラミッド構造だったとしても、それとは異なったフラットな連絡体制をとり、情報の集約と共有を一元化し、非常時対策本部による緊急な判断や行動を実現することを想定している。

C2102-06（インシデント対応手順）

第六条　具体的なインシデント対応は、別途定める「C3102 インシデント対応手順」に基づき対処する。
２　非常事態においては、非常時対策本部の指示がインシデント対応手順に優先する。

C2102-07（再発防止策の検討）

第七条　全学総括責任者は、非常事態への対応が終了した場合、非常時対策本部から全学情報システム運用委員会への報告書の提出をもって、非常時対策本部を解散する。

２　全学総括責任者は、報告書をもとに再発防止策の実施を図る。

C2103 情報格付け基準

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A2104	新規作成（情報格付け規程）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A2104	「情報格付け基準」として様式等を修正	国立大学法人等における情報セキュリティポリシー策定作業部会
2013年7月5日 B2104	文書番号の変更のみ	ー
2015年10月9日 C2103	文書番号の変更のみ	ー
2017年10月17日 C2103	要機密情報の定義を修正 （C2501の定めるものと一致させた）	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

1. 目的

情報の格付けは、本学におけるポリシー及び実施規程に沿った対策を適正に実施するための基礎となる重要な事項である。

情報の格付け及び取扱制限は、その作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させ、当該情報の重要性や講ずべき情報セキュリティ対策を明確にするための手段である。このため、情報の格付け及び取扱制限が適切に行われないと、当該情報の取扱いの重要性が認知されず、必要な対策が講じられないことになってしまう。

また、情報の格付け及び取扱制限を実施することで、情報の利用者に対し、日々の情報セキュリティ対策の意識を向上させることができる。具体的には、情報を作成又は入手するたびに格付け及び取扱制限の判断を行い、情報を取り扱うたびに格付け及び取扱制限に従った対策を講ずることで、情報と情報セキュリティ対策が不可分であることについての認識を継続的に維持する効果も生ずる。

本規程は、情報の格付け及び取扱制限の意味とその運用について教職員等が正しく理解することを目的とする。

2. 本規程の対象者

本規程は、情報を取り扱うすべての教職員等を対象とする。

3. 格付けの区分及び取扱制限の種類の定義

3.1 格付けの区分

(1) 情報の格付けの区分は、機密性、完全性、可用性について、それぞれ以下のとおりとする。

【基準利用者への補足説明】
情報について、機密性（情報に関して、アクセスを認可された者だけがこれにアクセスできる状態を確保すること）、完全性（情報が破壊、改ざん又は消去されていない状態を確保すること）、可用性（情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること）の３つの観点を区別し、それぞれにつき格付けの区分の定義を示す。

(2) 機密性についての格付けの定義

格付けの区分	分類の基準
機密性３情報	本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年4月1日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	本学で取り扱う情報のうち、独立行政法人の保有する情報の公開に関する法律（平成13年12月5日法律第140号。以下、「独立行政法人等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
機密性１情報	独立行政法人等情報公開法第５条各号における不開示情

	報に該当すると判断される蓋然性の高い情報を含まない情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

(3) 完全性についての格付けの定義

格付けの区分	分類の基準
完全性２情報	本学で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

なお、完全性２情報を「要保全情報」という。

(4) 可用性についての格付けの定義

格付けの区分	分類の基準
可用性２情報	本学で取り扱う情報（書面を除く。）のうち、その滅失､紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。 また、要機密情報、要保全情報及び要安定情報を「要保護情報」という。

3.2 取扱制限の種類

情報の取扱制限の種類は、機密性、完全性、可用性について、それぞれ以下のとおりとする。

【基準利用者への補足説明】
情報について、機密性、完全性、可用性の３つの観点を区別し、それぞれにつき取扱制限の種類の定義を行う。「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。

3.2.1 機密性についての取扱制限

機密性についての取扱制限の定義

取扱制限の種類	指定方法
複製について	複製禁止、複製要許可
配付について	配付禁止、配付要許可
暗号化について	暗号化必須、保存時暗号化必須、通信時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り

【基準利用者への補足説明】
上記の指定方法の意味は以下のとおり。
・「○○禁止」 当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。
・「○○要許可」 当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。
・「暗号化必須」 当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」など、情報を取り扱う者が分かるように指定する。
・「○○限り」 当該情報について、参照先を○○に記載した者のみに制限する必要がある場合に指定する。例えば、「部局内限り」「委員会出席者限り」など、参照を許可する者が分かるように指定する。

3.2.2 完全性についての取扱制限

完全性についての取扱制限の定義

取扱制限の種類	指定方法
保存期間について	○○まで保存
保存場所について	○○において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

【基準利用者への補足説明】

保存期間の指定の方法は、以下のとおり。
保存を要する期日である「年月日」又は期日を特定できる用語に「まで保存」を付して指定する。
例）平成１８年７月３１日まで保存
例）平成１８年度末まで保存
完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。
例）年度内保存文書用共有ファイルサーバに保管
例）３カ年保存文書用共有ファイルサーバに保管

3.2.3 可用性についての取扱制限

可用性についての取扱制限の定義

取扱制限の種類	指定方法
復旧までに許容できる時間について	○○以内復旧
保存場所について	○○において保存

【基準利用者への補足説明】

復旧許容時間の指定の方法は以下のとおり。
復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。
例）１時間以内復旧
例）３日以内復旧
可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用においては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、各自PCのファイルについては定期的にバックアップが実施されておらず、部局共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。
例）部局共有ファイル保存必須
例）各自PC保存可

4. 格付け及び取扱制限の手順

4.1 格付け及び取扱制限の決定

4.1.1 決定

部局総括責任者が決定を行う場合：

(1) 部局総括責任者は、教職員等による格付けの適正性を確保するため、格付け及び取扱制限の定義に基づき、当該部局総括責任者が所掌する事務で取り扱う情報について、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、これが格付け及び取扱制限の定義のいずれに分類されるものであるのかを例示した表（以下「格付け及び取扱制限の判断例」という。）を作成し、当該情報の格付け及び取扱制限を決定する（取扱制限の必要性の有無を含む。）こと。

教職員等が個々に決定を行う場合：

(2) 教職員等は、情報の作成時又は情報を入手しその管理を開始する時に、当該情報について、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、その決定を行う（取扱制限の必要性の有無を含む。）こと。

【基準利用者への補足説明】

情報の格付け及び取扱制限を行うとは、情報の格付け及び取扱制限を決定し、指定することである。すなわち、情報システムで取り扱う情報について、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、当該情報が、どのように取り扱われるべきか、どのような対策が講じられるべきかを検討して、それぞれの定義のいずれに分類されるものであるのかを決定し、決定された格付け及び取扱制限を指定することが、格付け及び取扱制限の本質である。
決定に当たっての考え方を以下に例示する。

- 機密性の格付けについては、秘密文書に相当する機密性を要する情報であり、[教職員等のうち、特定の者だけがアクセスできる状態を確保されるべき]情報は機密性３情報に、[教職員等以外がアクセスできない状態を確保されるべきであるが、特定の者に限定する必要がない]情報は機密性２情報に、それ以外の情報には、機密性１情報に決定する。
- 完全性の格付けについては、情報が破壊、改ざん又は消去されていない状態を確保されるべき情報は完全性２情報に、それ以外の情報は、完全性１情報に決定する。
- 可用性の格付けについては、情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保されるべき情報は可用性２情報に、それ以外の情報は可用性１情報に決定する。

4.1.2 決定に当たっての注意事項

部局総括責任者が決定を行う場合：

(1) 部局総括責任者は、格付け及び取扱制限の決定に当たっては、要件に過不足が生じないように注意すること。

教職員等が個々に決定を行う場合：

(2) 教職員等は、格付け及び取扱制限の決定に当たっては、要件に過不足が生じない

ように注意すること。

【基準利用者への補足説明】
格付け及び取扱制限として決定する要件が不十分であると、そのための情報セキュリティ対策が不十分となり、情報が適切に保護されなくなる。逆に、過度の要件を求めると、情報の保護が必要以上に厳しくなり、情報の利便性や有用性が損なわれる。そのため、格付け及び取扱制限の決定をする際は、要件に過不足が生じないように注意しなければならない。
機密の情報（例えば、本来要機密情報とする情報）を要機密情報に格付けないことは不適切であるが、逆に、機密ではない情報（例えば、公開しても差し支えない情報）をむやみに要機密情報に格付けることも不適切であることに注意すること。

4.2 格付け及び取扱制限の指定

部局総括責任者が決定を行う場合：

(1) 教職員等は、情報の作成時又は情報を入手しその管理を開始する時に、部局総括責任者が策定した格付け及び取扱制限の判断例に基づき、格付け及び取扱制限の指定を行うこと。ただし、格付け及び取扱制限の判断例で規定されていない情報については、当該情報の作成時又は当該情報を入手しその管理を開始する時に、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定をし、決定した格付け及び取扱制限に基づき、その指定を行うこと。

教職員等が個々に決定を行う場合：

(2) 教職員等は、決定した格付け及び取扱制限に基づき、その指定を行うこと。

4.3 格付け及び取扱制限の明示等

教職員等は、情報の格付け及び取扱制限を指定した場合には、それを認識できる方法を用いて明示等すること。

【基準利用者への補足説明】
情報の格付け及び取扱制限を指定した者が、当該情報に対して行う格付け及び取扱制限の明示等についての考え方は以下のとおり。
① 格付け及び取扱制限の明示の簡便化
「明示等」とは、情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示等に含むものとする。
② 取扱制限の明示を簡便化した場合における取扱制限の追加・変更
例えば、機密性３情報の取扱制限について事前に規定しておくことで、取扱制限の明記を省いて運用する方法を用いる場合、特定の機密性３情報について取扱制限を追加するときは、当該追加する取扱制限のみを明記し、逆に取扱制限を解除するときは、当該解除する取扱制限を「送信可」「印刷可」と明記することが想定される。
したがって、当該情報システムに記録される情報の格付け及び取扱制限を規定等により明記し、当該情報システムを利用するすべての者に当該規定が周知されていない場合（特に他大学に情報を提供等する場合）は、格付け及び取扱制限について記載しなければならない。
なお、記載が必須でない場合も、記載することによる問題がない限り、記載することが望ましい。

4.4 格付け及び取扱制限の継承

教職員等は、情報を作成する際に、参照した情報又は入手した情報が既に格付け又は取扱制限の指定がなされている場合には、元となる格付け及び取扱制限を継承すること。

【基準利用者への補足説明】

作成の際に参照した情報又は入手した情報が既に格付け又は取扱制限の指定がされている場合には、元となる格付け及び取扱制限を継承し、同一情報について一貫した対策を実施する必要がある。

4.5 格付け及び取扱制限の変更

【基準利用者への補足説明】

情報の格付け及び取扱制限は、情報システム運用基本規程に沿った対策を適正に実施するための基礎となる重要な事項であることについては、前記のとおりである。このため、これらを変更するに当たっても適正な手続により実施する必要がある。情報の格付け及び取扱制限の変更には、大別して再指定と見直しがあり、以下において、それぞれにつきその手順を示す。

4.5.1 格付け及び取扱制限の再指定

教職員等は、元の情報の修正、追加、削除のいずれかにより、他者が指定した情報の格付け及び取扱制限を再指定する必要があると思料する場合には、決定と指定の手順に従って処理すること。

【基準利用者への補足説明】

元の情報の修正、追加、削除のいずれかにより、格付け又は取扱制限を変更する必要が生じた場合には、格付け及び取扱制限の変更を行う必要がある。
例えば、以下のような場合が考えられる。

・機密性の低い情報に機密性の高い情報を追加したことによって、情報の機密性が上がる場合
・機密性の高い情報から機密に該当する部分を削除したことによって、情報の機密性が下がる場合

4.5.2 格付け及び取扱制限の見直し

(1) **教職員等は、元の情報への修正、追加、削除のいずれもないが、元の格付け又は取扱制限がその時点で不適当と考えるため、他者が指定した情報の格付け及び取扱制限を見直す必要があると思料する場合には、その指定者若しくは決定者又は同人らが所属する上司に相談すること。**

【基準利用者への補足説明】

元の情報への修正、追加、削除のいずれもないが、元の格付け又は取扱制限がその時点で不適当と考える場合には、格付け及び取扱制限の変更を行う必要がある。
例えば、以下のような場合が考えられる。

・作成時には非公開だった情報が正規の手続によって公開されることで機密性が失われた場合（時間の経過により変化した場合）
・格付け及び取扱制限を決定したときの判断が不適切であったと考えられる場合
・取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合
・取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合

(2) **相談者又は被相談者は、情報の格付け及び取扱制限について見直しを行う必要性の有無を検討し、必要があると認めた場合には、当該情報に対して新たな格付け及び取扱制限を決定又は指定すること。**

(3) 相談者又は被相談者は、情報の格付け及び取扱制限を見直した場合には、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け及び取扱制限とならないように努めること。

(4) 教職員等は、自らが指定した格付け及び取扱制限を変更する場合には、その以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け及び取扱制限とならないように努めること。

【基準利用者への補足説明】
いずれの理由であっても、適正な格付け及び取扱制限がなされていない場合は、情報セキュリティ対策が適正に実施されないおそれが生ずるため、情報を利用する教職員等が、当該情報の格付けを変更する場合に、その指定者等に相談した上、妥当な格付けに変更する必要がある。
なお、当初の格付けが指定者等によって不適正に設定されていれば、当該格付けを修正し、その旨を通知することによって、指定者等への教育的効果も期待できる。また、同一の情報が異なる格付け及び取扱制限とならないように、変更以前に当該情報を参照した者に対しても、格付け及び取扱制限が変更された旨を周知させることに努める必要がある。
なお、異動等の事由により、当該情報の指定者等と相談することが困難である場合においては、引継ぎを受けた者又は職場情報セキュリティ責任者に相談し、その是非を検討することになる。

4.5.3 変更後の指定者

情報の格付け及び取扱制限を変更する者は、変更後の格付け及び取扱制限の指定者について、変更前の指定者が継続するのか、変更者が新たに指定者となるのかについて明確にすること。

【基準利用者への補足説明】
変更後の格付け及び取扱制限の指定者は、再指定の場合には再指定をした者、見直しの場合には元の指定者が継続することを原則とするが、それ以外の場合には変更時点で明確にしておく必要がある。

5 既存の情報についての措置

5.1 既存の情報について

【基準利用者への補足説明】
本学における情報システム運用基本規程の施行日より以前の情報については、格付けと取扱制限は適宜実施することとしており、それらをすべて処理することは求めていない。

(1) 教職員等は、本規程の施行日以前に作成又は入手した情報を取り扱う場合には、当該情報の格付けを行うこと。

(2) 教職員等は、本規程の施行日以前に作成又は入手した情報を取り扱う場合には、取扱制限の必要性の有無を検討し、必要と認めるときは、それを行うこと。

【基準利用者への補足説明】
情報の格付け及び取扱制限の指定については、本学におけるポリシー及び実施規程の施行日以後に作成又は入手したすべての情報について適用するものであるが、施行日以前に作成又は入手した情報についても、適宜その指定を行うことが望ましい。
なお、施行日以前に作成又は入手した情報にあっては、これを取り扱う場合には、格付け及び取扱制限の指定を行う必要がある。

【付表】

文書の種類に基づく分類例

情報類型	格付け	取扱制限
公開前会議資料	機密性２情報 完全性２情報 可用性２情報	複製禁止、配付禁止
各部局協議	機密性２情報 完全性２情報 可用性２情報	暗号化必須
勉強会・研修会資料	機密性２情報 完全性２情報 可用性２情報	教職員等限り
ＨＰ掲載資料	機密性１情報 完全性２情報 可用性２情報	３日以内復旧、ハックアップ必須
情報セキュリティ検査結果とりまとめ報告書	機密性２情報 完全性２情報 可用性２情報	５年間保存
個人等の秘密を侵害し、又は名誉、信用を損なうおそれのある情報	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ａシステムにおいて保存、書換禁止、保存期間満了後要廃棄

特定文書に対応させた分類例

文書類型	格付け	取扱制限
個人情報を含むパブリックコメント受領文書	機密性２情報 完全性２情報 可用性２情報	パブリックコメント終了後３年間保存
ポリシー及び実施規程	機密性１情報 完全性２情報 可用性２情報	作成後５年
未実施の各種試験問題案	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ｂシステムにおいて保存、書換禁止、削除禁止

大学活動の内容に基づく分類例

事務類型	格付け	取扱制限
○○○に関する事務において知り得た○○○の情報	機密性２情報 完全性２情報 可用性２情報	
非公開の会議において知り得た非公知の情報	機密性２情報 完全性２情報 可用性２情報	配付禁止、暗号化必須、書換禁止、削除禁止、関係者限り
未実施の各種試験問題作成に関する事務において知り得た情報	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ｂシステムにおいて保存、書換禁止、削除禁止

C2201 情報システム利用規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A2201	新規作成（利用規程）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A2201	「情報システム利用規程」として構成等を修正	国立大学法人等における情報セキュリティポリシー策定作業部会
2011年3月31日 A2201	対象範囲を明確化し、取扱制限事項を追加・変更するとともに条文構成を整理	長谷川明生（中京大学）
2013年7月5日 B2201	高等教育機関における情報システム利用の実態に合わせた修正	長谷川明生（中京大学）
2015年10月9日 C2201	文書番号の変更のみ	ー
2016年2月5日 C2201	C2601及びC2603の両規程の新規策定に伴い、整合をとるために全体的な調整を実施	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：この文書は、大学の情報システムのための利用規程の雛形として使われることを想定している。大学の情報システム利用規程の策定では、規程の改変の機会を少なくするように、規程には具体的な記述を記載せず、具体的項目を内規や手順に記載することが一般的である。この雛形の利用に当たっては、この点にも留意してほしい。また、この文書では、情報機器の利用、ウェブブラウザ利用や電子メールの利用および一般利用者向けのウェブ公開基準については、ガイドラインとして作成し強制力を持たせないこととしている。ガイドラインではなく、違反した場合にペナルティを課す手順や内規とする場合には、対応するガイドラインの修正だけでなく対応する条項（C2201-13、C2201-14 および C2201-15）の修正が必要である。

A大学では、ネットワーク接続の際にも認証が行われるので、利用者全員がアカウント（全学アカウントと呼ぶ）を持つことを想定した規程となっている。学会開催時等の訪問者のネットワーク利用についても臨時の全学アカウント発行が必要とされる。A大学では、このアカウントは管理運営部局（情報メディアセンター）が全学アカウントとして交付している（詳細は第五条を参照）。A大学とアカウント管理体制が異なる場合には、A大学との差異に配慮した利用規程としなければならない。この規程は、PC 等の端末やネットワークを利用する際に利用者が守らなければならない一般規定であって、事務情報システムおよび教務・事務用アプリケーションの利用にあたっては、それぞれの利用規程や手順書に従う必要がある。（ただし、手順書部分の改訂は未着手である。）

現在のひな形の規程は部局や研究室等でシステムを構築、または、ASP、PaaS やクラウド等のアウトソースを考慮していないが、電子メールのアウトソースやクラウドの利用が大学でも進行しており、実際の規程制定では、それらも考慮する必要がある。考慮事項として、アカウント管理の規程との整合性、電子メール等の情報の保全や業者との紛争処理が国内法で対応できるかといったことがあげられる。

なお、情報システム利用規程の定めに反した行為があった場合に、それに対する懲戒として、学生・職員の所属によるもの（学部長による停学処分など）と情報メディアセンターによるもの（一定期間の利用禁止処分など）の 2 種類がありうる。前者は、懲戒規程などによって所属部局で対応すべきものであるが、所属によって懲戒の内容に差異が生じないようにするため、あるいは違反行為の認定に専門知識が必要とされる場合に、情報メディアセンターの助言を得ることが望ましい。後者の懲戒について、学生に対する利用制限によって、情報処理演習システムを利用する科目の履修や教務システムを用いる手続きに支障が生じて結果として留年など過度の不利益を招かないよう、教学との関係に対する配慮が必要である。

C2201-01　（目的）

第一条　この規程は、A 大学（以下「本学」という。）における情報システムの利用に関する事項を定め、情報セキュリティの確保と円滑な情報システムの利用に資することを目的とする。

解説：この項目では、上記のように、システムやネットワークの利用目的を明示し、規程制定の理由を示す。

C2201-02　（定義）

第二条　この規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

一　運用基本方針　本学が定める「C1000 情報システム運用基本方針」をいう。

二　運用基本規程　本学が定める「C1001 大学情報システム運用基本規程」をいう。

三　利用者　教職員等及び学生等で、本学情報システムを利用する許可を受けて利用する者をいう。

四　臨時利用者　教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用する者をいう。

五　利用者等　利用者及び臨時利用者のほか、本学情報システムを取り扱う者をいう。

六　全学アカウント A 大学全学認証基盤で主体認証を行う情報システムにおいて、主体に付与された正当な権限をいう。全学アカウントの付与は、識別コードと主体認証情報の配布、主体認証情報格納装置の交付、アクセス制御における許可、またはそれらの組み合わせ等によって行われる。

七　その他の用語の定義は、運用基本方針及び運用基本規程で定めるところによる。

解説：上記のように、本規程内で引用される手順書等への参照や用語を明確にしておく。

C2201-03　（適用範囲）

第三条　この規程は本学構成員および別途定める手続きにより許可を受けて本学情報システムを利用する者に適用する。

解説：規程の制限が及ぶ範囲を明確にする。研究および教育用に利用する私物の扱いにも留意して規程を整備する必要がある。また、格付けされた情報を格納した情報機器やクラウドストレージも情報システムの対象とし規程の対象とする。BYOD 機器、パブリッククラウドの個人での利用や ASP 等の利用についても規程外にならないように制定する必要がある。A 大学では、部局や研究室で独自に構築するシステムに適用する規程は部局が準備することになっている。なお、「C3501 各種マニュアル類」は各大学にて策定することを想定した文書であって本サンプル規程集の策定対象外である。研究用の情報システムであっても、成績処理や事務会計処理に使用している場合には事務情報システムとみなされることに注意。本学の公開情報を Web 等により閲覧する行為は本利用規程の範囲外である。

C2201-04　（遵守事項）

第四条　利用者等は、この規程及び本学情報システムの利用に関する手順及び本学個人情報保護規程を遵守しなければならない。

解説：利用に際して、利用手順書や他の規程との関連を記述する。

C2201-05　（全学アカウントの申請）

第五条　本学情報システムを利用する者は、C2603 全学認証基盤アカウント利用規程およびその関連手順に従い、全学アカウントの交付を受けなければならない。

２　来訪者に本学情報システムを臨時的利用させることを目的として全学アカウントの交付を受ける場合、申請者は来訪者に本規程を遵守させなければならない。同目的による全学アカウントの利用が不要になった場合、申請者は速やかに全学実施責任者に届け出なければならない.

解説：A大学では、アカウントの管理方法についての規程は以下のようになる。A大学では、ID とパスワードによる全学統一認証方式を採用し、ネットワークを含めて、全学統一認証に対応した情報システムの利用にあたって全学アカウントを用いている。これは政府機関統一基準の「知識による主体認証情報」に相当する。全学統一認証に対応しないシステムの管理責任者は、それぞれにアカウントの発行のルールを定めて、すべての利用について状況を把握しておかなければならない。研究室の Web や Wiki の供用アカウントの管理については、研究教育活動に支障のでないような配慮が必要であろう。

全学アカウントは、全学実施責任者（管理運営部局のセンター長が相当、「C1001 情報システム運用基本規程」の C1001-08（第八条）の解説を参照のこと）から交付を受けなければならない。A大学では、利用の申請と承認は全学情報システム運用委員会が処理をするが、利用承認とアカウント指定を行うのは全学実施責任者なので、申請宛先も全学実施責任者となっている。ただし、実際の処理については、職員と学生についてはほとんど無条件に全学アカウントを発行し、それ以外の者の申請に当たっては関係部局長（来学中に利用する訪問者などの臨時利用者を受け入れた部局の長など）の認印を要件とするなどの申請処理手順を定めておいて、実質的な判断を不要とするものとする。学会等での来訪者のネットワーク利用についても考慮が必要である.

なお、ネットワークの接続と利用にあたってアカウントが必要な認証ネットワークの場合は、このまま適用可能であるが、ネットワーク接続にオンラインでの認証が不要の場合はアカウント条項にかわる利用開始手順を記述しておく。

学外からのインターネットを介しての利用に関しては、大学の実情に合わせて適宜変更する必要がある。

また、盗聴によるアカウント情報漏洩防止注意するとともに eduroam 等の利用を妨げないような規程を考えなければならない。暗号化された Web メールサービスを提供することにより、学外からのメールソフトによる電子メールサーバへの直接アクセスを禁止している大学もある。アカウントには SSH のパスフレーズやワンタイムパスワードのアルゴリズムも含まれる。また、クラウドサービスやアウトソースした場合のアカウント管理についても考慮する必要がある。

C2201-06　（ID とパスワードによる認証の場合）

第六条　利用者等は、全学アカウントの利用に際して次の各号に掲げる事項を遵守しなければな

らない。

一　利用者等は、全学アカウントを利用して、学外から本学情報システムにアクセスする場合には、定められた手順に従ってアクセスしなければならない。

二　自分の全学アカウントを他者に使用させ、または主体認証情報を他者に開示してはならない。

三　他者の主体認証情報を聞き出し、又は使用してはならない。

四　主体認証情報（パスワード）は、C3255 利用者パスワードガイドラインに従って適切に管理しなければならない。

五　利用者は、全学アカウントによる認証接続中の利用者端末において、他の者が無断で画面を閲覧・操作することができないように配慮しなければならない。

六　学外の不特定多数の人が操作（利用）可能な端末を用いて全学アカウントによる認証接続を行ってはならない。

七　全学アカウントを他の者に使用され、またはその危険が発生した際には、直ちに本基盤の運用責任者に届け出なければならない。

八　姓名の変更等識別コードの変更が必要になった際は、遅滞なく本基盤の運用責任者に届け出なければならない。

九　本基盤の利用者の資格を喪失した際又は利用する必要がなくなった際は、別途定める様式により、本基盤の運用責任者に全学アカウント廃止を届け出なければならない。ただし、個別の届出が必要ないと、あらかじめ本基盤の運用責任者が定めている場合は、この限りでない。

十　識別コードもしくは主体認証情報を失念した場合は、別途定める様式により、本基盤の運用責任者に識別コード再交付の申請を行うこととする。

C2201-06-2 （IC カードを用いた認証の場合）

第六条の２　IC カードの交付を受けた利用者は、IC カードの管理について次の各号を遵守しなければならない。

一　IC カードを本人が意図せずに使われることのないように安全措置を講じて管理しなければならない。

二　IC カードを他の者に付与又は貸与したり、他の者の IC カードを使用したりしてはならない。

三　IC カードを紛失しないように管理しなければならない。紛失した際には、直ちに IC カードを発行責任組織にその旨を報告しなければならない。

四　IC カードを利用する必要がなくなった際、又は利用資格がなくなった際には、遅滞なくこれを発行責任組織が定める手続きによりに返納しなければならない。

五　IC カードに記載された券面及び格納された電子証明書の内容が変更される場合には、遅滞なく発行責任組織にその旨を報告しなければならない。

六　運用責任者が IC カードに格納した電子証明書を、運用責任者の許可なく削除してはならない。

七　IC カード使用時に利用する PIN は、利用者パスワードガイドラインに準じて適切に管理しなければならない。

２　IC カードについて前項第三号の報告を受けた発行責任組織の長は、直ちに本基盤の運用責

任者に報告しなければならない。

解説：上記の規程例は、IC カード等の「所有による主体認証」を利用する場合に、上記規程を置き換えるものである。利用承認の規程も、「パスワードの交付」から「IC カードの貸与」等に変更する必要がある。

C2201-07　（情報機器の利用）

第七条　利用者等は、様々な情報の作成、利用、保存等のための情報機器の利用にあたっては以下の各号に従わなければならない。

一　利用者等は、本学情報ネットワークに新規かつ固定的に情報機器を接続しようとする場合は、事前に接続を行おうとする部局の部局総括責任者に接続の許可を得なければならない。（ただし、情報コンセントや無線 LAN からあらかじめ指定された方法により本学情報システムに接続する場合はこの限りではない。）

二　利用者等は、一項により許可を受けた情報機器の利用を取りやめる場合には部局総括責任者に届け出なければならない。

三　情報機器において、認証システムおよびログ機能を動作させることが定められている場合には、それらの機能を設定し、動作させなければならない。不正ソフトウェア対策機能が導入されている機器にあっては、その機能が最新の状態でシステムを保護するように努めなければならない。

四　情報機器は既知の脆弱性の影響を被ることのないよう可能な限り最新の状態を保たなければならない。

五　利用者等は、情報漏えいを発生させないように対策し、情報漏えいの防止に努めなければならない。

六　利用者等は、情報機器の紛失および盗難を発生させないように注意しなければならない。

七　情報機器の紛失および盗難が発生した場合は、すみやかに部局技術担当者に届け出なければならない。

八　別途定める「C3251 情報機器取扱ガイドライン」に従い、これらの情報機器の適切な保護に注意しなければならない。

解説：本条で扱う情報機器とは、「C2501 事務情報セキュリティ対策基準」1.3 の情報システムに関する定義を満たした上で、大学の備品か利用者の私物かによらず、本学の情報資産を扱うものをいう。スマートフォンや PDA および PC 機能を持ちネットワークに接続可能な装置等を含む。情報機器の学外利用に際しては、盗難や紛失の他に覗き見等による情報漏えいに注意しなければならない。このような機器の利用について、情報漏えいとともに不正アクセスソフトウェア対策の観点からも考慮しなければならない。

C2201-08　（利用者等による情報セキュリティ対策教育の受講義務）

第八条　利用者等は、毎年度１回は、年度講習計画に従って、本学情報システムの利用に関する教育を受講しなければならない。

２　教職員等は、着任時、異動時に新しい職場等で、本学情報システムの利用に関する教育の受講方法について部局総括責任者に確認しなければならない。

３　教職員等は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではないと

思われる場合には、その理由について、部局総括責任者を通じて、全学実施責任者に報告しなければならない。

（４　利用者等は、情報セキュリティ対策の訓練に参加しなければならない。）

解説:情報セキュリティ教育の受講義務について、規程として明文化した条項である。オンライン教育や講義等を通じて年１回は、すべての利用者がセキュリティ教育を受講することが必要である。情報セキュリティ訓練規程および手順が定められている場合には、訓練参加義務を規定化する。

C2201-09　（情報の取り扱い）

第九条　利用者等は、格付けされた情報について、情報格付け取扱手順（C3103）に従い、文書に明示された方法にしたがって取り扱わなければならない。

解説：C1001-19 にしたがって C2103 および C3103 が策定され、教職員等は B2103 および C3103 に従って文書の格付けし、格付け文書の取り扱いを文書に明示しなければならない。利用者は C3103 にあるように文書に明示された方法に従って文書を取り扱う。

本規程の対象としているシステムや機器では、格付けになじまないという考え方もあるが、情報格付け基準で対象外システムを明記しておいて、格付けは包括的に実施するという考え方もあるので、この条項を置いた。なお A 大学では学生に情報の格付け権限はない。

C2201-10　（制限事項）

第十条　利用者等が本学情報システムについて以下の各号に定める行為を行おうとする場合には本学実施責任者の許可を受けなければならない。

一　ファイルの自動公衆送信機能を持った P2P ソフトウェアを教育・研究目的で利用する行為

二　教育・研究目的で不正ソフトウェア類似のコードやセキュリティホール実証コードを作成、所持、使用および配布する行為

三　ネットワーク上の通信を監視する行為

四　本学情報機器の利用情報を取得する行為及び本学情報システムのセキュリティ上の脆弱性を検知する行為

五　本学情報システムの機能を著しく変える可能性のあるシステムの変更

解説：A大学では、構成員による知的財産権侵害と意図せぬ情報漏洩やファイルの流出を防ぐためにファイルの自動公衆送信機能を持った P2P ソフトウェアの利用を研究教育目的にのみ許可制としている。ここで自動公衆送信とは著作権法での用語であり、自動公衆送信機能を持った P2P ソフトウェアとは、ファイルを自動的にダウンロードし、またダウンロードしたファイルやファイルの断片を自動的に不特定多数に再送信するような機能を持った P2P ソフトウェアのことをいう。マルウェア研究に関しても同様の扱いとしている。

C2201-11　（禁止事項）

第十一条　利用者等は、本学情報システムについて、次の各号に定める行為を行ってはならない。

一　当該情報システム及び情報について定められた目的以外の利用
二　指定以外の方法での学外からの全学アカウントを用いての本学情報システムへのアクセス
三　あらかじめ指定されたシステム以外の本学情報システムを本学外の者に利用させる行為
四　守秘義務に違反する行為
五　差別、名誉毀損、侮辱、ハラスメントにあたる行為
六　個人情報やプライバシーを侵害する行為
七　前条に該当しない不正ソフトウェアの作成、所持および配布行為
八　著作権等の財産権を侵害する行為
九　通信の秘密を侵害する行為
十　営業ないし商業を目的とした本学情報システムの利用

解説：本サンプル規程集の「C1001 情報システム運用基本規程」第三条十号「教職員等」の解説にあるように、大学の活動との関連で同窓会、生協、TLO、インキュベーションセンター、地域交流センター、財団などが利用することは想定される。ただし、その利用の目的を大学の教育・研究活動および運営を支援する業務に限定して、営利業務のネットワークを別に用意するとしている大学の例があり、A 大学もそのような運用をしている。二項については手順書等で明示。ただし、大学施設内の組織や関連事業の営利業務に利用できることを利用規程の定めあるいは全学総括責任者の判断によって認めるような方針もありえる。

十一　過度な負荷等により本学の円滑な情報システムの運用を妨げる行為
十二　不正アクセス禁止法に反する行為、またはこれに類する行為
十三　その他法令に基づく処罰の対象となる行為
十四　上記の行為を助長する行為

解説：利用に際しての禁止条項および制限事項を上記で条文化している。

C2201-12　（違反行為への対処）

第十二条　利用者等の行為が前条に掲げる事項に違反すると被疑される行為と認められたときは、部局総括責任者は速やかに調査を行い、事実を確認するものとする。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取しなければならない。

２　部局総括責任者は、上記の措置を講じたときは、遅滞無く全学総括責任者にその旨を報告しなければならない。

３　調査によって違反行為が判明したときは、部局総括責任者は全学総括責任者を通じて次の各号に掲げる措置を講ずること依頼することができる。

一　当該行為者に対する当該行為の中止命令
二　管理運営部局に対する当該行為に係る情報発信の遮断命令
三　管理運営部局に対する当該行為者のアカウント停止、または削除命令
四　本学懲罰委員会への報告
五　本学学則および就業規則に定める処罰
六　その他法令に基づく措置

解説：前条の禁止規定に明白に違反した場合の対処、処罰について上記のように明示

する。一般に、部局総括責任者が処罰可能なのは管轄部局のみで、他学部や管理運営部局に対しては、全学責任者を通じて処罰を依頼するのが自然であろう。

解説：以下（第十三条～十四条）の条文は、利用者が守るべき手順書を示している。

C2201-13　（電子メールの利用）

第十三条　利用者等は、電子メールの利用にあたっては、別途定める「C3252 電子メール利用ガイドライン」に従い、規則の遵守のみならずマナーにも配慮しなければならない。

C2201-14　（ウェブの利用および公開）

第一四条　利用者等は、ウェブの利用およびウェブによる情報公開に際し、以下の各号に従わなければならない。

一　利用者等は、ウェブブラウザを利用したウェブサイトの閲覧、情報の送信、ファイルのダウンロード等を行う際には、「C3253 ウェブブラウザ利用ガイドライン」に従わなければならない。

二　利用者等は、部局情報システム運営委員会に許可を得て、「C3254 情報発信ガイドライン」に従いウェブページを作成し、公開することができる。

三　利用者等は、ウェブサーバを運用し情報を学外へ公開する場合は、事前に部局情報システム運営委員会に申請し、許可を得なければならない。また、ウェブサーバを公開する利用者は、運用期間中、ウェブサーバの脆弱性対策や情報の改ざんに関する点検を定期的に行わなければならない。

四　ウェブページやウェブサーバ運用に関して、規程やガイドラインに違反する行為が認められた場合には、全学実施責任者は公開の許可の取り消しやウェブコンテンツの削除を行うことができる。

C2201-15　（学外からの本学情報システムの利用）

第十五条　利用者等は、学外からの本学情報システムへのアクセスにおいて、以下の各号にしたがわなければならない。

一　利用者等は、学外から全学アカウントを使って本学情報システムへアクセスするには事前に全学実施責任者の許可を得たうえで、指定された方法で利用しなければならない。

二　利用者等は、アクセスに用いる情報システムを許可された者以外に利用させてはならない。

三　利用者等は、全学実施責任者の許可なく、これらの情報システムに要保護情報を複製保持してはならない。

解説：学外へ持ち出した情報機器や、学生、教職員等の自宅 PC 等、学外の情報システムからの本学ネットワークへの接続や学内システムの利用にあたっては、全学実施責任者の事前許可が必要である。学外との接続方法については VPN 等情報センターが指定するのが一般的である。

eduroam 等の制約にならないように条文に工夫が必要である。ログおよびアンチウイルス機能に関しては実情に合わせて条文を変更することも可能であるが、証跡管理の点からは好ましくない。ネットカフェ等、情報セキュリティ対策が不十分な情報システムやネットワークからの学内情報システムの利用は情報漏えいのリスクが大きく推奨できない。C2201-07 に集約することが可能と思わ

れる。

C2201-16　（安全管理義務）

第十六条　利用者等は、自己の管理する情報機器について、本学情報ネットワークとの接続状況に関わらず、安全性を維持する一次的な担当者となることに留意し、次の各号にしたがって利用しなければならない。

一　ソフトウェアの状態および不正ソフトウェア対策機能を最新に保つこと。

二　不正ソフトウェア対策機能により不正プログラムとして検知されるファイル等を開かないこと。

三　不正ソフトウェア対策機能の自動検査機能を有効にしなければならない。

四　不正ソフトウェア対策機能により定期的にすべての電子ファイルに対して、不正プログラムが存在しないこと確認すること。

五　外部からデータやソフトウェアを情報機器に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正ソフトウェアが存在しないことを確認すること。

六　常に最新のセキュリティ情報に注意し、不正ソフトウェア感染の予防に努めること。

C2201-17 (インシデント対応)

第十七条　利用者等は、本学情報システムの利用に際して、インシデントを発見したときは、「C3102 インシデント対応手順」に従って行動しなければならない。

C2301 年度講習計画

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A2301	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A2301	教育テキスト作成ガイドラインの拡充に対応した修正及び追記	国立大学法人等における情報セキュリティポリシー策定作業部会
2013年7月5日 B2301	文書番号の変更のみ	ー
2015年10月9日 C2301	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：「C2101 情報システム運用・管理規程」において、利用者等に対する講習について「講習計画の定める講習」との定めがあるので、利用者向け年度講習計画を定めることになる。部局総括責任者、部局技術責任者及び部局技術担当者に対して「情報セキュリティ対策の教育」との定めがあり、これについてはその実施概要を部局で情報システムの運用管理に携わる者向けの講習計画の形で定めるのが良いと考えられる。また、役職者に対する教育についても講習計画の形で明確化することが望ましい。よって、ここでは利用者向け年度講習計画に加えて、システム管理者向けと役職者向けの講習計画も定めている。

１．適用範囲

本文書は、以下の目的で実施される講習の年度計画について規定するものである。なお、いずれの講習とも、情報セキュリティ対策教育を単独で行う必要はなく、関連分野と合わせた講習の中で実施する形で差し支えない。

(1) 新たに大学の情報システムを利用することとなった学生、教職員等を対象とした、情報セキュリティ対策の基礎知識習得のための講習（以下、「基礎講習」と表記）
(2) (1)以外の利用者（教職員、学生等）を対象とした、最新状況への対応法等からなる情報セキュリティ対策の基礎知識習得のための講習（以下、「定期講習」と表記）
(3) 情報システム管理者を対象とした、運用に必要な情報セキュリティ対策の応用知識習得のための講習（以下、「システム管理者講習」と表記）
(4) 学長、事務局長、全学総括責任者（CIO）、部局総括責任者（部局長）を対象とした、大学運営における情報セキュリティ対策の基本的知識を理解するための講習（以下、「役職者講習」と表記）

解説：関連規程:「C1001 情報システム運用基本規程」C1001-5（第五条）、C1001-08（第八条）、「C2201 情報システム利用規程」C2201-07（第七条）

なお、臨時職員、臨時利用者等、一時的に大学の設備を利用する利用者への教育については、本文書によらず、各利用者の利用条件に応じて必要かつ簡潔な教育を実施するものとし、本文書の適用範囲としない。

２．年度講習計画

年度講習計画を策定する場合には、対象者と実施時期に応じて以下の４種類を区別し、それぞれの区分について実施時期と教育する内容を定めること。

(1) 基礎講習：学生の場合は入学・編入学後の関連講義の初回、もしくは利用者講習会において、また教職員については着任後の講習会において、情報システムを利用する際の事故やトラブルの発生を予防するために、事前に理解しておくべき知識を集中的に教育するもの
(2) 定期講習：すでに(1)を習得済みの利用者に対し、習得状況の維持・確認や最新動向の教育などを目的として実施するもの
(3) システム管理者講習: 情報システムの管理者に対して、技術面を中心として、法令なども含めて実施するもの
(4) 役職者講習：着任時および年 1 回（部局総括責任者については全学情報システム運用委員会等の席上で年１回）、本学における情報セキュリティの状況と、大学運営における情報セキュリティのあり方について実施するもの

３．計画例

(1) 基礎講習

　情報セキュリティ対策の基礎知識だけでなく、法令、マナー、学内関連諸規程について併せて教育を実施する。

講習時期	講習内容	備考
4月～5月、および10月	A. 導入事項 ①事故から身を守るための知識 ・事故例と対策の必要性（導入として） ②利用規則と罰則 ・目的外利用の禁止 ・大学設備・環境の損壊、重大な影響を及ぼす行為の禁止 ・他利用者への迷惑行為の禁止 ・パスワード等の適正管理 ③学内情報システムの基本理念 ・言論の自由、学問の自由 ・他者の生命、安全、財産を侵害しない ・他者の人格の尊重 B. 情報セキュリティの基礎的知識 ・Internet のしくみ（IP address, URL, https） ・virusとworm（感染兆候と予防対策+事後対策） ・spyware（予防対策） ・情報発信（個人情報、責任、Accessibility） ・迷惑メール（対策） ・phishing、架空請求（しくみと注意喚起、対策） ・ファイル交換（情報漏洩、著作権） C. マナー・関連法令 ①法令の遵守 ・個人情報・秘密情報の保護 ・不正アクセス行為の禁止 ・著作権・肖像権 ②利用上のマナー ・社会慣行の尊重 ・ネットワーク利用のマナーの理解と尊重 ・運用への協力 ・ネット中毒 D. 便利な使い方 ・Webメール ・学外から学内へのアクセス手段	講義「情報リテラシー」が必修の学科については、その講義の中で実施する。それ以外の学科では、情報メディアセンター主催の講習会を受講するものとする。教職員については、情報メディアセンター主催の教職員向け講習会を受講するものとする。 毎回の講義の中で、関連学習内容に関連した情報セキュリティに関する知識を習得させる

(2) 定期講習

最新の情報セキュリティ動向を教育するためのテキストを配布する。

講習時期	講習内容	備考
6 月～7 月	・最近の脅威の動向 ・主要な情報セキュリティ対策の確認	ｅラーニング形式による実施も検討

(3) システム管理者講習

講義および、必要に応じて実習形式にて実施する。

講習時期	講習内容	備考
4 月～5 月	・システム管理の重要性 ・最低限知っておくべきセキュリティ対策 （各回カリキュラムによる）	講義初回時に、サーバ運用等に際して最低限必要なセキュリティ知識を初回に集中的に習得させる ２回目以降の講義で、カリキュラムに応じた知識の習得を図る（「C3302 教育テキスト作成ガイドライン（システム管理者向け）」参照）

(4) 役職者講習

簡単な資料を用いて短時間の報告により実施する。以下の計画のほか、重大インシデント発生の際には臨時で実施する。

役職	講習時期	講習内容	備考
学長、事務局長	着任時および年１回	・CIO による本学の情報セキュリティ状況報告（体制・対策、事例） ・テキスト：　状況報告資料	学長への状況報告は、詳細情報よりも、統計および重大インシデント（学外に対して重大な被害を与えたもの）の発生事例に重点をおく
全学総括責任者（CIO）	着任時および１年に１回	・大学運営における情報セキュリティのあり方 (1) 本学における情報セキュリティ状況 ・インシデント発生状況の詳細情報（扱い件数の統計） ・重大インシデントの詳細な分析	

		(2) 情報セキュリティ対策に必要な措置 ・情報セキュリティ対策の必要性 ・情報セキュリティの責任体制 (3) 情報システムの構築・運用・インシデント対応 ・体制の整備に関する課題 ・体制の整備の方法 ・テキスト： メディア教育センター教員が進講。「C3303 教育テキスト作成ガイドライン（CIO/役職者向け）」を参照。	
部局総括責任者（各部局長）	１年に１回（全学情報システム運用委員会（または役員会、部局長会議など）の席上）	・CIO が学内ケーススタディを出す。メディア教育センター教員が状況報告を補佐するのも可。 ・テキスト： 状況報告資料	状況報告には、ケーススタディと、統計がある。状況報告は、ケーススタディが効果的。必要に応じて秘密扱い。 また、状況の分析を外部講師に依頼することも効果的。

C2401 情報セキュリティ監査規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A2401	新規作成（監査規程）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A2401	「情報セキュリティ監査規程」に文書名変更	ー
2013年7月5日 B2401	文書番号の変更のみ	ー
2015年10月9日 C2401	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C2401-01 （目的）

第一条　独立性を有する者による情報セキュリティ監査の実施基準を定めることにより、本学ポリシー、実施規程、及びそれに基づく手順が確実に遵守され、問題点が改善されることを目的とする。

C2401-02 （監査計画の策定）

第二条　情報セキュリティ監査責任者は、年度情報セキュリティ監査計画を策定し、全学総括責任者の承認を得る。

解説：監査の基本的な方針として、年度情報セキュリティ監査計画を策定し、承認を受けることを求める事項である。年度情報セキュリティ監査計画には、次の事項が含まれる。

・重点とする監査対象及び監査目標（情報漏えい防止、不正アクセス防止など）
・監査実施期間
・監査業務の管理体制
・外部委託による監査の必要性及び範囲
・監査予算

なお、以前実施した監査結果で明らかになった課題及び問題点の改善状況について、監査を実施する場合には、年度情報セキュリティ監査計画に盛り込む。

C2401-03 （情報セキュリティ監査の実施に関する指示）

第三条　全学総括責任者は、年度情報セキュリティ監査計画に従って、情報セキュリティ監査責任者に対して、監査の実施を指示する。

２　全学総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、情報セキュリティ監査責任者に対して、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示する。

解説：年度情報セキュリティ監査計画において実施する監査以外に、本学内、本学外における事案の発生の状況又は情報セキュリティ対策の実施についての重大な変化が生じた場合に、必要に応じて臨機応変に監査を実施することを求める事項である。

なお、本学内において甚大な情報セキュリティ侵害が発生した場合であって、その侵害の規模や影響度をかんがみ、より客観性・独立性が求められるときは、外部組織による監査を検討することが求められる。

C2401-04 （個別の監査業務における監査実施計画の策定）

第四条　情報セキュリティ監査責任者は、年度情報セキュリティ監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を策定する。

解説：監査の基本的な方針に基づいて、実施すべき監査についての詳細な計画を策定することを求める事項である。監査実施計画には、次の事項が含まれる。(経済産業省 情報セキュリティ監査基準 実施基準ガイドライン Ver1.0 等を参考)

・監査の実施時期

・監査の実施場
・監査の実施担当者及び割当て
・準拠性監査（ポリシー及び実施規程に基づく手順に準拠した手続が実施されていることを確認する監査）のほか、必要に応じて妥当性監査（実施している手続が有効なセキュリティ対策であることを確認する監査）を行うかについての方針
・実施すべき監査の概要（監査要点、実施すべき監査の種類及び試査の範囲を含む。）
・監査の進捗管理手段又は体制

C2401-05 （情報セキュリティ監査を実施する者の要件）

第五条　情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した情報セキュリティ監査を実施する者に対して、監査の実施を依頼する。

解説：情報セキュリティ監査を実施する者に監査人としての独立性及び客観性を有することを求める事項である。情報システムを監査する場合には、当該情報システムの構築又は開発をした者は、その監査をしないこととする。また、情報資産の運用状況に関する監査を行う場合には、当該情報資産を運用している者はその監査をしないこととする。

２　情報セキュリティ監査責任者は、必要に応じて、本学外の者に監査の一部を請け負わせる。

解説：情報セキュリティ監査を実施する者は、監査を実施するに当たり、必要に応じて監査対象システムの詳細情報を有する組織、本学内の情報システム部門又は外部専門家の支援を受けることを求める事項である。
組織内に監査を実施する者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮し、外部委託に関する対策基準に従うこと。また、情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の業務への関与などを考慮することが望ましい。

C2401-06 （情報セキュリティ監査の実施）

第六条　情報セキュリティ監査を実施する者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施する。

２　情報セキュリティ監査を実施する者は、実施手順が作成されている場合には、それらが本ポリシーに準拠しているか否かを確認する。

３　情報セキュリティ監査を実施する者は、被監査部門における実際の運用が本ポリシー及び実施規程に基づく手順に準拠しているか否かを確認する。

解説：３項は、被監査部門における実際の運用が、ポリシー及び実施規程に基づく手順に準拠して実施されているか否かの確認を求める事項である。監査に当たっては、必要に応じて、自己点検記録の査閲、機器の設定状況の点検等により、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かを確認することが求められる。

4　情報セキュリティ監査を実施する者は、監査調書を作成し、あらかじめ定められた期間保存する。

解説：監査意見表明の根拠となる監査調書を適切に作成し、保存することを求める事項である。監査調書とは、情報セキュリティ監査を実施する者が行った監査業務の実施記録であって、監査意見表明の根拠となるべき監査証拠、その他関連資料等を綴り込んだものをいう。情報セキュリティ監査を実施する者自らが直接に入手した資料やテスト結果だけでなく、被監査部門側から提出された資料等を含み、場合によっては組織の外部の第三者から入手した資料等を含むことがある。

5　情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、全学総括責任者へ提出する。

解説：監査結果を報告書として文書化した上で、全学総括責任者へ確実に提出をすること求める事項である。なお、本監査は、実際の運用状況がポリシー及び実施規程に基づく手順に準拠して行われているか等、準拠性の監査を意図したものであるが、監査の過程において、遵守内容の妥当性に関連して改善すべき課題及び問題点が検出された場合には、この検出事項や助言提案を監査報告書に含めることが望ましい。

C2401-07　（情報セキュリティ監査結果に対する対応）

第七条　全学総括責任者は、監査報告書の内容を踏まえ、被監査部門の部局総括責任者に対して、指摘事案に対する対応の実施を指示する。

解説：監査報告書において指摘された課題及び問題点に対する改善を図るため、全学総括責任者へ被監査部門の部局総括責任者に対する対応実施の指示を求める事項である。

2　全学総括責任者は、監査報告書の内容を踏まえ、監査を受けた部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、他の部局の部局総括責任者に対しても、同種の課題及び問題点の有無を確認するように指示する。

解説：監査報告書において指摘された課題及び問題点が、他の監査対象にも同種の課題及び問題点として存在する可能性が高い場合又は同種の課題及び問題点の存在を緊急に確認する必要性が高い場合には、想定される他の監査対象についても同様に調査を実施する必要がある。そのため、全学総括責任者から部局総括責任者に対する確認の指示を求める事項である。

3　部局総括責任者は、監査報告書に基づいて全学総括責任者から改善を指示された事案について、対応計画を作成し、報告する。

解説：監査報告書に基づいて全学総括責任者から改善を指示された事案について、対応計画の作成及び報告を求める事項である。監査報告書において指摘された課題及び問題点の改善が困難であることについて正当な理由がある場合には、リスク軽減策を示した上で、達成することが可能な対応目標を提示することが重要である。また、その課題及び問題点が人為によるものである場合には、部局総括責任者は、提示された対応目標を情報セキュリティ対策の教育方法や教育

施策に反映することが必要である。

4　全学総括責任者は、監査の結果を踏まえ、本ポリシー及び実施規程に基づく既存の手順の妥当性を評価し、必要に応じてその見直しを指示する。

解説：情報セキュリティ監査責任者から報告された監査報告書において、遵守内容の妥当性に関連した改善指摘を受けた場合には、ポリシー及び実施規程に基づく既存の手順の更新を検討することを求める事項である。検討の結果、ポリシー及び実施規程に基づく手順の更新を行わない場合には、その理由について明確化すること。

C2501 事務情報セキュリティ対策基準

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A2501	統一基準（全体版初版）をもとに新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A2501	統一基準（第2版）に対応した修正	国立大学法人等における情報セキュリティポリシー策定作業部会
2011年3月31日 A2201	統一基準（第4版）をもとに全面改定	国立大学法人等における情報セキュリティポリシー策定作業部会
2013年7月5日 B2501/B2551	統一基準（平成24年度版）をもとに全面改定 （管理基準と技術基準に分割）	高等教育機関における情報セキュリティポリシー推進部会事務局
2015年10月9日 C2501	統一基準（平成26年度版）をもとに全面改定	高等教育機関における情報セキュリティポリシー推進部会事務局
2017年10月17日 C2501	統一基準群（平成28年度版）をもとに改定	高等教育機関における情報セキュリティポリシー推進部会事務局

（注）統一基準＝政府機関の情報セキュリティ対策のための統一基準

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

目　次

第 1 部　総則

1.1　本基準の目的･適用範囲

(1) 本基準の目的

情報セキュリティの基本は、高等教育機関で取り扱う情報の重要度に応じた「機密性」･「完全性」･「可用性」を確保することであり、それぞれの高等教育機関が自らの責任において情報セキュリティ対策を講じていくことが原則である。しかし、高等教育機関共通の IT 環境の利用、本学間の情報流通の現状を踏まえると、高等教育機関全体の統一的な枠組みを構築し、それぞれの高等教育機関の情報セキュリティ水準の斉一的な引上げを図ることが必要である。

「事務情報セキュリティ対策基準」（以下、「本基準」という。）は、国立大学法人 A 大学（以下、「本学」という。）の事務局管理の情報及び情報システムの情報セキュリティ強化のための基準である。本基準は、「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」（平成 28 年 8 月 31 日付サイバーセキュリティ戦略本部決定。以下、「政府機関統一基準」という。）に基づいて作成したものであり、各国立大学法人が、政府機関統一基準を踏まえた情報セキュリティポリシーの策定ならびに見直しを行う際に、検討のたたき台として活用いただくための標準版である。検討の参考にしていただければ幸いである。

また、政府機関統一基準は、定期的に見直しを行い、その適用性を将来にわたり維持する方針であるため、本基準は、政府機関統一基準の改訂に対応できるよう、構成をほぼ同様にしていることを申し添える。

(2) 本基準の適用範囲

(a) 本基準において適用範囲とする者は、全ての事務従事者とする。

(b) 本基準において適用範囲とする情報は、以下の情報とする。

(ア) 事務従事者が職務上使用することを目的として本学が調達し、又は開発した情報システム若しくは外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

(イ) その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、事務従事者が職務上取り扱う情報

(ウ) (ア)及び(イ)のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報

(c) 本基準において適用範囲とする情報システムは、本基準の適用範囲となる情報を取り扱う全ての情報システムとする。

(3) 本基準の改訂

情報セキュリティ水準を適切に維持していくためには、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。

このため、情報技術の進歩に応じて、本基準を定期的に点検し、必要に応じ規定内容の追

加・修正等の見直しを行う。

(4) 法令等の遵守

情報及び情報システムの取扱いに関しては、本基準のほか法令及び基準等（以下「関連法令等」という。）を遵守しなければならない。なお、これらの関連法令等は情報

セキュリティ対策にかかわらず当然に遵守すべきものであるため、本基準では、あえて関連法令等の遵守について明記していない。また、情報セキュリティを巡る状況に応じて策定される政府決定等についても同様に遵守すること。

(5) 対策項目の記載事項

本基準では、本学が行うべき対策について、目的別に部、節及び項の３階層にて対策項目を分類し、各項に対して目的、趣旨及び遵守事項を示している。遵守事項は、事務情報セキュリティ対策基準において必ず実施すべき対策事項である。本学が別途整備する事務情報セキュリティ対策基準策定のためのガイドライン及び関連規程等において規定する統一基準の遵守事項に対応した個別具体的な対策実施要件、対策の実施例や解説等も参照し、事務情報セキュリティ対策基準を策定する必要がある。

1.2 情報の格付の区分･取扱制限

(1) 情報の格付の区分

情報について、機密性、完全性及び可用性の３つの観点を区別し、本基準の遵守事項で用いる格付の区分の定義を示す。

本学において格付の定義を変更又は追加する場合には、それぞれの高等教育機関の対策基準における格付区分と遵守事項との関係が本基準での関係と同等以上となるように準拠しなければならない。また、他本学へ情報を提供する場合は、自身の格付区分と本基準における格付区分の対応について、適切に伝達する必要がある。

機密性についての格付の定義

格付けの区分	分類の基準
機密性３情報	本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年4月1日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	本学で取り扱う情報のうち、独立行政法人の保有する情報の公開に関する法律（平成13年12月5日法律第140号。以下、「独立行政法人等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
機密性１情報	独立行政法人等情報公開法第５条各号における不開示情

	報に該当すると判断される蓋然性の高い情報を含まない情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

完全性についての格付の定義

格付けの区分	分類の基準
完全性２情報	本学で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

なお、完全性２情報を「要保全情報」という。

可用性についての格付の定義

格付けの区分	分類の基準
可用性２情報	本学で取り扱う情報（書面を除く。）のうち、その滅失､紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。

また、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」という。

(2) 情報の取扱制限

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを事務従事者に確実に行わせるための手段をいう。

事務従事者は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。本学は、取り扱う情報について、機密性、完全性及び可用性の３つの観点から、取扱制限に関する基本的な定義を定める必要がある。

1.3 用語定義

事務情報セキュリティ対策基準において次の各号に掲げる用語の定義は、当該各号に定めるところによる。

【あ】

- 「アプリケーション・コンテンツ」とは、アプリケーションプログラム、ウェブコンテンツ等の総称をいう。
- 「委託先」とは、外部委託により本学の情報処理業務の一部又は全部を実施する者をいう。

【か】

- 「外部委託」とは、本学の情報処理業務の一部又は全部について、契約をもって学外の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。
- 「学外通信回線」とは、通信回線のうち、学内通信回線以外のものをいう。
- 「学内通信回線」とは、一つの本学が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該高等教育機関の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。学内通信回線には、専用線や VPN 等物理的な回線を本学が管理していないものも含まれる。
- 「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。
- 「基盤となる情報システム」とは、他の機関と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。
- 「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。
- 「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。
- 「クラウドサービス事業者」とは、クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・提供する事業者をいう。

【さ】

- 「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。
- 「CSIRT（シーサート）」とは、本学において発生した情報セキュリティインシデントに対処するため、当該高等教育機関に設置された体制をいう。Computer Security Incident Response Team の略。
- 「実施手順」とは、事務情報セキュリティ対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。
- 「事務従事者」とは、本学の事務に従事している本学の指揮命令に服している者であって、本学の管理対象である情報及び情報システムを取り扱う者をいう。事務従事者には、個々の勤務条件にもよるが、例えば、派遣労働者等も含まれている。
- 「事務情報セキュリティ対策基準」とは、本学における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。
- 「情報」とは、「1.1(2) 本基準の適用範囲」の(b)に定めるものをいう。
- 「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理及び通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。
- 「情報セキュリティインシデント」とは、JIS Q 27000:2014 における情報セキュリティインシデントをいう。
- 「情報セキュリティ関係規程」とは、事務情報セキュリティ対策基準及び実施手順を総称したものをいう。
- 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

【た】

- 「端末」とは、情報システムの構成要素である機器のうち、事務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。
- 「通信回線」とは、複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信

回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

- 「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。
- 「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。

【は】

- 「不正プログラム」とは、コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

【ま】

- 「抹消」→「情報の抹消」を参照。
- 「明示等」とは、情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。
- 「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

- 「約款による外部サービス」とは、民間事業者等の学外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。
- 「要管理対策区域」とは、本学が管理する施設等（外部の組織から借用している施設等を含む。）本学の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。

第 2 部　情報セキュリティ対策の基本的枠組み

2.1　導入･計画

2.1.1　組織・体制の整備

目的・趣旨

情報セキュリティ対策は、それに係る全ての事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。特に全学総括責任者は、情報セキュリティ対策を着実に進めるために、自らが組織内を統括し、組織全体として計画的に対策が実施されるよう推進しなければならない。

なお、全学総括責任者は、その権限に属する事務の一部を本基準に定める責任者等に担わせることができる。

遵守事項

(1) 全学総括責任者の設置

(a) 本学は、本学における情報セキュリティに関する事務を統括する全学総括責任者１人を置くこと。

【 基本対策事項 】

(1)-1　全学総括責任者は、次に掲げる事務を統括すること。

a) 情報セキュリティ対策推進のための組織・体制の整備

b) 事務情報セキュリティ対策基準の決定、見直し

c) 対策推進計画の決定、見直し

d) 情報セキュリティインシデントに対処するために必要な指示その他の措置

e) 前各号に掲げるもののほか、情報セキュリティに関する重要事項

(2) 全学情報システム運用委員会の設置

(a) 全学総括責任者は、事務情報セキュリティ対策基準等の審議を行う機能を持つ組織として、本学の情報セキュリティを推進する部局及びその他高等教育機関の事務を実施する部局の代表者を構成員とする全学情報システム運用委員会を置くこと。

【 基本対策事項 】

(2)-1　全学情報システム運用委員会の委員長及び委員は、全学総括責任者が情報セキュリティを推進する部局及びその他の高等教育機関の事務を実施する部局の代表者から指名すること。

(2)-2　全学情報システム運用委員会は、次に掲げる事項を審議すること。
a) 事務情報セキュリティ対策基準
b) 対策推進計画
c) 前各号に掲げるもののほか、情報セキュリティに関し必要な事項

(3) 情報セキュリティ監査責任者の設置
(a) 全学総括責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くこと。

【 基本対策事項 】
(3)-1　情報セキュリティ監査責任者は、命により次の事務を統括すること。
a) 監査実施計画の策定
b) 監査実施体制の整備
c) 監査の実施指示及び監査結果の全学総括責任者への報告
d) 前各号に掲げるもののほか、情報セキュリティの監査に関する事項

(4) 全学実施責任者・部局総括責任者等の設置
(a) 全学総括責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、部局総括責任者１人を置くこと。そのうち、部局総括責任者を統括し、全学総括責任者を補佐する者として、全学実施責任者１人を選任すること。
(b) 部局総括責任者は、遵守事項 3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者１人を置くこと。
(c) 部局総括責任者は、課室ごとに情報セキュリティ対策に関する事務を統括する職場情報セキュリティ責任者１人を置くこと。
(d) 部局総括責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、部局技術責任者を、当該情報システムの企画に着手するまでに選任すること。

【 基本対策事項 】
(4)-1　全学実施責任者は、命を受け、次の事務を統括すること。
a) 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定
b) 情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務のとりまとめ
c) 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備
d) 例外措置の適用審査記録の台帳整備等
e) 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等
f) 前各号に掲げるもののほか、情報セキュリティ対策に係る事務

(4)-2　部局総括責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括すること。
　a) 定められた区域ごとの区域情報セキュリティ責任者の設置
　b) 課室の職場情報セキュリティ責任者の設置
　c) 情報システムごとの部局技術責任者の設置
　d) 情報セキュリティインシデントの原因調査、再発防止策等の実施
　e) 情報セキュリティに係る自己点検計画の策定及び実施手順の整備
　f) 前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務

(4)-3　区域情報セキュリティ責任者は、命を受け、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を統括すること。

(4)-4　職場情報セキュリティ責任者は、命を受け、課室における情報の取扱いその他の情報セキュリティ対策に関する事務を統括すること。

(4)-5　部局技術責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。

(4)-6　部局技術責任者は、所管する情報システムの管理業務において必要な単位ごとに部局技術担当者を置くこと。

(5) 情報セキュリティアドバイザーの設置

(a) 全学総括責任者は、情報セキュリティについて専門的な知識及び経験を有する者を情報セキュリティアドバイザーとして置き、自らへの助言を含む情報セキュリティアドバイザーの業務内容を定めること。

【 基本対策事項 】

(5)-1　全学総括責任者は、以下を例とする情報セキュリティアドバイザーの業務内容を定めること。
　a) 本学全体の情報セキュリティ対策の推進に係る全学総括責任者への助言
　b) 情報セキュリティ関係規程の整備に係る助言
　c) 対策推進計画の策定に係る助言
　d) 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
　e) 情報システムに係る技術的事項に係る助言
　f) 情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
　g) 事務従事者に対する日常的な相談対応
　h) 情報セキュリティインシデントへの対処の支援
　i) 前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

(6) 情報セキュリティインシデントに備えた体制の整備

(a) 全学総括責任者は、CSIRT を整備し、その役割を明確化すること。

(b) 全学総括責任者は、事務従事者のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、本学における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う職員を定めること。

(c) 全学総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。

【 基本対策事項 】

(6)-1 全学総括責任者は、以下を含む CSIRT の役割を規定すること。

a) 本学に関わる情報セキュリティインシデント発生時の対処の一元管理

- 外局等を含む本学全体における情報セキュリティインシデント対処の管理
- 情報セキュリティインシデントの可能性の報告受付
- 本学における情報セキュリティインシデントに関する情報の集約
- 本学の附属機関等における情報セキュリティインシデントに関する情報の集約
- 情報セキュリティインシデントの全学総括責任者等への報告
- 情報セキュリティインシデントへの対処に関する指示系統の一本化

b) 情報セキュリティインシデントへの迅速かつ的確な対処

- 情報セキュリティインシデントであるかの評価
- 被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
- 文部科学省への連絡
- 外部専門機関等からの情報セキュリティインシデントに係る情報の収集
- 他大学 CSIRT 等の機関への情報セキュリティインシデントに係る情報の共有
- 情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

(6)-2 全学総括責任者は、実務担当者を含めた実効性のある CSIRT 体制を構築すること。

(6)-3 最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておくこと。

c) (6)-4 全学総括責任者は、本学全体における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の役割分担を規定すること。

(7) 兼務を禁止する役割

(a) 事務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

(ア) 承認又は許可（以下、本項において「承認等」という。）の申請者と当該承認等を行う者（以下、本項において「承認権限者等」という。）

(イ) 監査を受ける者とその監査を実施する者

(b) 事務従事者は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該

承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。

2.1.2 事務情報セキュリティ対策基準・対策推進計画の策定

目的・趣旨

本学の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、本学として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果を踏まえ、計画的に対策を実施することが重要である。

遵守事項

(1) 事務情報セキュリティ対策基準の策定

(a) 全学総括責任者は、全学情報システム運用委員会における審議を経て、統一基準に準拠した事務情報セキュリティ対策基準を定めること。

(2) 対策推進計画の策定

(a) 全学総括責任者は、全学情報システム運用委員会における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めること。また、対策推進計画には、本学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含めること。

(ア) 情報セキュリティに関する教育

(イ) 情報セキュリティ対策の自己点検

(ウ) 情報セキュリティ監査

(エ) 情報システムに関する技術的な対策を推進するための取組

(オ) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

2.2 運用

2.2.1 情報セキュリティ関係規程の運用

目的・趣旨

本学は、事務情報セキュリティ対策基準に定められた対策を実施するため、具体的な実施手順を定める必要がある。

実施手順が整備されていない、又はそれらの内容に漏れがあると、対策が実施されないおそれがあることから、全学総括責任者は、全学実施責任者に実施手順の整備を指示し、その結果について定期的に報告を受け、状況を適確に把握することが重要である。

遵守事項

(1) 情報セキュリティ対策に関する実施手順の整備・運用
  (a) 全学実施責任者は、本学における情報セキュリティ対策に関する実施手順を整備（本基準で整備すべき者を別に定める場合を除く。）し、実施手順に関する事務を統括し、整備状況について全学総括責任者に報告すること。
  (b) 全学実施責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動時等に関する管理の規定を整備すること。
  (c) 部局総括責任者又は職場情報セキュリティ責任者は、事務従事者より情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、全学実施責任者に報告すること。

(2) 違反への対処
  (a) 事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合は、部局総括責任者にその旨を報告すること。
  (b) 部局総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、全学実施責任者を通じて、全学総括責任者に報告すること。

2.2.2 例外措置

目的・趣旨

例外措置はあくまで例外であって、濫用があってはならない。しかしながら、情報セキュリティ関係規程の適用が高等教育機関の事務の適正な遂行を著しく妨げるなどの理由により、規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合がある。このような場合に対処するために、例外措置の手続を定めておく必要がある。

遵守事項

(1) 例外措置手続の整備
  (a) 全学総括責任者は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び、審査手続を定めること。
  (b) 全学実施責任者は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めること。

【 基本対策事項 】

(1)-1 全学総括責任者は、例外措置について以下を含む手順を定めること。
  a) 例外措置の許可権限者
  b) 事前申請の原則その他の申請方法

c) 審査項目その他の審査方法
- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を申請する期間
- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置により生じる情報セキュリティ上の影響と対処方法
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

(1)-2 許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、全学実施責任者へ定期的に報告すること。

a) 審査した者の情報（氏名、役割名、所属、連絡先）

b) 申請内容
- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を申請する期間
- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

c) 審査結果の内容
- 許可又は不許可の別
- 許可又は不許可の理由
- 例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を許可した期間
- 許可した措置内容（講ずるべき代替手段等）
- 例外措置を終了した旨の報告方法

(2) 例外措置の運用

(a) 事務従事者は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請すること。ただし、高等教育機関の事務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ること。

(b) 許可権限者は、事務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。

(c) 許可権限者は、例外措置の申請状況を台帳に記録し、全学実施責任者に報告すること。

(d) 全学実施責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加

又は見直しの検討を行い、全学総括責任者に報告すること。

2.2.3 教育

目的・趣旨

情報セキュリティ関係規程が適切に整備されているとしても、その内容が事務従事者に認知されていなければ、当該規定が遵守されていないことになり、情報セキュリティ水準の向上を望むことはできない。このため、全ての事務従事者が、情報セキュリティ関係規程への理解を深められるよう、適切に教育を実施することが必要である。

また、近年の情報セキュリティインシデントの増加等に鑑み、情報セキュリティの専門性を有する人材を育成することも求められる。

遵守事項

(1) 教育体制等の整備

(a) 全学実施責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備すること。

【 基本対策事項 】

(1)-1 全学実施責任者は、事務従事者の役割に応じて教育すべき内容を検討し、教育のための資料を整備すること。

(1)-2 全学実施責任者は、事務従事者が毎年度最低１回は教育を受講できるように、教育実施計画を立案するとともに、その実施体制を整備すること。

(1)-3 全学実施責任者は、事務従事者の着任又は異動後に、３か月以内に受講できるように、その実施体制を整備すること。

(2) 教育の実施

(a) 職場情報セキュリティ責任者は、事務従事者に対して、情報セキュリティ関係規程に係る教育を適切に受講させること。

(b) 事務従事者は、教育実施計画に従って、適切な時期に教育を受講すること。

(c) 職場情報セキュリティ責任者は、CSIRT に属する職員に教育を適切に受講させること。

(d) 全学実施責任者は、全学総括責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。

2.2.4 情報セキュリティインシデントへの対処

目的・趣旨

情報セキュリティインシデントを認知した場合には、全学総括責任者に早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、情報セキュリティインシデントの対処が完了した段階においては、原因について調査するなどにより、情報セキュリティインシデントの経験から今後に生かすべき教訓を導き出し、再発防止や対処手順、体制等の見直しにつなげることが重要である。

遵守事項

(1) 情報セキュリティインシデントに備えた事前準備

(a) 全学実施責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む本学関係者への報告手順を整備し、報告が必要な具体例を含め、事務従事者に周知すること。

(b) 全学実施責任者は、情報セキュリティインシデントの可能性を認知した際の学外との情報共有を含む対処手順を整備すること。

(c) 全学実施責任者は、情報セキュリティインシデントに備え、高等教育機関の事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

(d) 全学実施責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、高等教育機関の事務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備すること。

(e) 全学実施責任者は、情報セキュリティインシデントについて学外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を学外の者に明示すること。

(f) 全学実施責任者は、対処手順が適切に機能することを訓練等により確認すること。

【 基本対策事項 】

(1)-1 全学実施責任者は、本学の附属機関等における情報セキュリティインシデント発生が報告された際にも、本学における情報セキュリティインシデントの場合と同様に、全学総括責任者や文部科学省に速やかに報告されるよう手順を定めること。

(1)-2 全学実施責任者は、情報セキュリティインシデント発生時の対処手順のうち、意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等をあらかじめ定めておくこと。

(1)-3 全学実施責任者は、本学の附属機関等において発生した情報セキュリティインシデントについて、当該機関から報告・連絡を受ける窓口について定めるとともに、各機関にその窓口の連絡先を周知すること。

(2) 情報セキュリティインシデントへの対処

(a) 事務従事者は、情報セキュリティインシデントを認知した場合には、本学の報告窓口に報告し、指示に従うこと。

(b) CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うこと。

(c) CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、全学総括

責任者に速やかに報告すること。

(d) CSIRT は、情報セキュリティインシデントに関係する部局総括責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行うこと。

(e) 部局技術責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、本学で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処すること。

(f) 部局技術責任者は、認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処すること。

(g) CSIRT は、本学の情報システムについて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、所管官庁等に連絡すること。また、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。さらに、国民の生活、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態においては、「大規模サイバー攻撃等への初動対処について（平成 22 年 3 月 19 日内閣危機管理監決裁)」に基づく報告も行うこと。

(h) CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて対処全般に関する指示、勧告又は助言を行うこと。

(i) CSIRT は、情報セキュリティインシデントに関する対処の内容を記録すること。

(j) CSIRT は、情報セキュリティインシデントに関して、本学を含む関係機関と情報共有を行うこと。

(k) CSIRT は、学外事業者等による情報セキュリティ関連サービスの支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うこと。

【 基本対策事項 】

(2)-1 CSIRT は、情報セキュリティインシデントではないと評価した場合であっても、注意喚起が必要と考えられるものについては、関係する者に情報共有を行うこと。

(2)-2 CSIRT 責任者は、認知した情報セキュリティインシデントの種類や規模、影響度合い等を勘案し、必要に応じて CSIRT、情報セキュリティインシデントのの当事者部局、その他関連部局の役割分担を見直すこと。

(3) 情報セキュリティインシデントの再発防止・教訓の共有

(a) 部局総括責任者は、CSIRT から応急処置の実施または復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として全学総括責任者に報告すること。

(b) 全学総括責任者は、部局総括責任者から情報セキュリティインシデントについての報

告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示すること。

(c) CSIRT 責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、全学実施責任者、関係する部局総括責任者等に共有すること。

2.3 点検

2.3.1 情報セキュリティ対策の自己点検

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ関係規程の遵守状況等を点検し、その結果を把握・分析することが必要である。

自己点検は、事務従事者が自らの役割に応じて実施すべき対策事項を実際に実施しているかどうかを確認するだけではなく、組織全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要である。

また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

遵守事項

(1) 自己点検計画の策定・手順の準備

(a) 全学実施責任者は、対策推進計画に基づき年度自己点検計画を策定すること。

(b) 部局総括責任者は、事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。

(2) 自己点検の実施

(a) 部局総括責任者は、年度自己点検計画に基づき、事務従事者に自己点検の実施を指示すること。

(b) 事務従事者は、部局総括責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。

(3) 自己点検結果の評価・改善

(a) 全学実施責任者及び部局総括責任者は、事務従事者による自己点検結果を分析し、評価すること。全学実施責任者は評価結果を全学総括責任者に報告すること。

(b) 全学総括責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、全学実施責任者及び部局総括責任者に改善を指示し、改善結果の報告を受けること。

2.3.2 情報セキュリティ監査

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。

また、監査の結果で明らかになった課題を踏まえ、全学総括責任者は、部局総括責任者に指示し、必要な対策を講じさせることが重要である。

遵守事項

(1) 監査実施計画の策定

(a) 情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定めること。

(b) 情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施の指示を、全学総括責任者から受けた場合には、追加の監査実施計画を定めること。

【 基本対策事項 】

(1)-1 情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定すること。

a) 監査の目的（例：自己点検の適切性を監査すること等）

b) 監査の対象（例：監査の対象となる組織、情報システム、業務等）

c) 監査の方法（例：自己点検結果を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、事務情報セキュリティ対策基準及び実施手順とする）

d) 監査の実施体制（例：監査責任者、監査実施者の所属、氏名）

e) 監査の実施時期（例：対象ごとの実施時期）

(2) 監査の実施

(a) 情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む監査の実施を監査実施者に指示し、結果を監査報告書として全学総括責任者に報告すること。

(ア) 事務情報セキュリティ対策基準に統一基準を満たすための適切な事項が定められていること

(イ) 実施手順が事務情報セキュリティ対策基準に準拠していること

(ウ) 自己点検の適正性の確認を行うなどにより、被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること

【 基本対策事項 】

(2)-1 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名すること。

(2)-2 情報セキュリティ監査責任者は、組織内における監査遂行能力が不足等している場合に

は、学外の者に監査の一部を請け負わせること。

(3) 監査結果に応じた対処

(a) 全学総括責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を部局総括責任者に指示すること。

(b) 部局総括責任者は、監査報告書等に基づいて全学総括責任者から改善を指示されたことについて、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を全学総括責任者に報告すること。

【 基本対策事項 】

(3)-1 全学総括責任者は、監査報告書の内容を踏まえ監査を受けた部門以外の部門においても同種の課題又は問題点がある可能性が高く、並びに緊急に同種の課題又は問題点があることを確認する必要があると判断した場合には、他の部門の部局総括責任者に対しても、同種の課題又は問題点の有無を確認するように指示すること。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、本学の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、実際の運用において生じた課題、自己点検、監査の結果や情報セキュリティに係る重大な変化等を踏まえ、保有する情報及び利用する情報システムに係る驚異の発生の可能性及び顕在化時の損失等を分析し、リスクを評価し、適時見直しを行う必要がある。

また、情報セキュリティに係る取組をより一層推進するためには、上記のリスク評価の結果を対策推進計画に反映することも重要である。

遵守事項

(1) 情報セキュリティ関係規程の見直し

(a) 全学総括責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、全学情報システム運用委員会の審議を経て、事務情報セキュリティ対策基準について必要な見直しを行うこと。

(b) 全学実施責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について全学総括責任者に報告すること。

(2) 対策推進計画の見直し

(a) 全学総括責任者は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、全学情報システム運用委員会の審議を経て、対策推進計画について定期的な見直しを行うこと。

第 3 部　情報の取扱い

3.1　　情報の取扱い

3.1.1　　情報の取扱い

目的・趣旨

高等教育機関の事務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下、本項において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての事務従事者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、事務従事者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

なお、秘密文書の管理に関しては、文書ガイドラインの規定を優先的に適用した上で、当該ガイドラインに定めが無い情報セキュリティ対策に係る事項については、本基準の規定に基づき、適切に情報が取り扱われるよう留意すること。

遵守事項

(1) 情報の取扱いに係る規定の整備

(a) 全学実施責任者は、以下を含む情報の取扱いに関する規定を整備し、事務従事者へ周知すること。

(ア) 情報の格付及び取扱制限についての定義

(イ) 情報の格付及び取扱制限の明示等についての手続

(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続

【 基本対策事項 】

(1)-1　全学実施責任者は、情報の取扱いに関する規定として、以下を例とする**手順を整備**すること。

a) 情報のライフサイクル全般にわたり必要な手順（高等教育機関の事務の遂行以外の目的での情報の利用等の禁止等）

b) 情報の入手・作成時の手順

c) 情報の利用・保存時の手順

d) 情報の提供・公表時の手順

e) 情報の運搬・送信時の手順

f) 情報の消去時の手順

g) 情報のバックアップ時の手順

(1)-2　全学実施責任者は、情報の格付及び取扱制限の**明示の方法**について、以下を例に、規定を整備すること。

a) 電磁的記録として取り扱われる情報に明示する場合
- 電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載
- 電磁的ファイル等の取扱単位ごとにファイル名自体へ記載
- フォルダ単位等で取り扱う情報は、フォルダ名に記載
- 電子メールで取り扱う情報は、電子メール本文又は電子メール件名に記載

b) 外部電磁的記録媒体に保存して取り扱う情報に明示する場合
- 保存する電磁的ファイル又は文書等の単位ごとに記載
- 外部電磁的記録媒体本体に記載

c) 書面に印刷されることが想定される場合
- 書面のヘッダ部分等に記載
- 冊子等の単位で取り扱う場合は、冊子の表紙、裏表紙等に記載

d) 既に書面として存在している情報に対して格付や取扱制限を明示する場合
- 手書きによる記入
- スタンプ等による押印

(1)-3　全学実施責任者は、情報の格付及び取扱制限の明示を省略する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、規定を整備すること。

(1)-4　全学実施責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例に、規定を整備すること。

a) 情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付及び取扱制限を継承する。

b) 既存の情報に、より機密性の高い情報を追加するときは、格付及び取扱制限を見直す。

c) 機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直す。

d) 情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。

e) 完全性及び可用性については、作成時又は複製時に適切な格付を決定する。

f) 他者が決定した情報の格付及び取扱制限を見直す必要がある場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下本項において「決定者等」という。）に確認を求める。

(2) 情報の目的外での利用等の禁止

(a) 事務従事者は、自らが担当している高等教育機関の事務の遂行のために必要な範囲に限って、情報を利用等すること。

(3) 情報の格付及び取扱制限の決定・明示等

(a) 事務従事者は、情報の作成時及び学外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等す

ること。

(b) 事務従事者は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。

(c) 事務従事者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下この項において決定者等という。）に確認し、その結果に基づき見直すこと。

(4) 情報の利用・保存

(a) 事務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

(b) 事務従事者は、機密性３情報について要管理対策区域外で情報処理を行う場合は、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。

(c) 事務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。

(d) 事務従事者は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。

(e) 事務従事者は、USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。

【 基本対策事項 】

(4)-1 事務従事者は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱うこと。

a) 要保護情報を放置しないこと。

b) 要機密情報を必要以上に複製しないこと。

c) 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。

d) 電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。

情報の保存方法を変更する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずる。

(4)-2 事務従事者は、入手した情報の格付け及び取扱制限が不明な場合には、情報の作成元または入手元への確認を行う。

(5) 情報の提供・公表

(a) 事務従事者は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。

(b) 事務従事者は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格

付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。

(c) 事務従事者は、電磁的記録を提供又は公表する場合には、当該電磁的記録の付加記録等からの不用意な情報漏えいを防止するための措置を講ずること。

【 基本対策事項 】

(5)-1 事務従事者は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

(6) 情報の運搬・送信

(a) 事務従事者は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。ただし、他本学の要管理対策区域であって、全学実施責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域と見なすことができる。

(b) 事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

【 基本対策事項 】

(6)-1 事務従事者は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬すること。

(6)-2 事務従事者は、要機密情報である電磁的記録を要管理対策区域外に運搬又は学外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。

a) 運搬又は送信する情報を暗号化する。

b) 運搬又は送信を複数の情報に分割してそれぞれ異なる経路及び手段を用いる。

c) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。

(6)-3

(6)-3 事務従事者は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。

a) 本学管理の通信回線を用いて送信する。

b) 信頼できる通信回線を使用して送信する。

c) VPN を用いて送信する。

d) S/MIME 等の暗号化された電子メールを使用して送信する。

e) 本学独自で運用するなどセキュリティが十分確保されたウェブメールサービス又はオ

ンラインストレージ環境を利用する。

(7) 情報の消去

(a) 事務従事者は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。

(b) 事務従事者は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。

(c) 事務従事者は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

(8) 情報のバックアップ

(a) 事務従事者は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。

(b) 事務従事者は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。

(c) 事務従事者は、保存期間を過ぎた情報のバックアップについては、本項(7)の規定に従い、適切な方法で消去、抹消又は廃棄すること。

【 基本対策事項 】

(8)-1 事務従事者は、要保全情報又は要安定情報である電磁的記録又は重要な設計書について、バックアップを取得すること。

(8)-2 事務従事者は、要保全情報、要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップの保管について、災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定すること。

3.2 情報を取り扱う区域の管理

3.2.1 情報を取り扱う区域の管理

目的・趣旨

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

したがって、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

遵守事項

(1) 要管理対策区域における対策の基準の決定

(a) 全学実施責任者は、要管理対策区域の範囲を定めること。

(b) 全学実施責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。

(ア) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。

(イ) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。

【 基本対策事項 】

(1)-1 全学実施責任者は、以下を例とする、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を定めること。

a) 下表のとおり、３段階のクラスを定める。

クラス	説明
クラス３	一部の限られた者以外の者の立入りを制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス２	事務従事者以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対策区域

※便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。

(1)-2 全学実施責任者は、クラス１の区域について、以下を含む施設の整備、設備の設置等の物

理的な対策及び入退管理対策の基準を定めること。

a) 不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。

b) 不特定の者が容易に立ち入らないように、立ち入る者の身元、訪問目的等の確認を行うための措置を講ずること。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。

c) クラス２以上の区域に不正に立ち入った者を容易に判別することができるように、以下を含む措置を講ずること。

- 事務従事者は、身分証明書等を着用、明示する。クラス２及びクラス３の区域においても同様とする。
- 一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス２及びクラス３の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。

(1)-3 全学実施責任者は、クラス２の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

a) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。ただし、窓口のある執務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は事務従事者が窓口を常に目視できるような措置を講ずること。

b) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠すること。

c) クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。

(1)-4 全学実施責任者は、クラス３の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

a) クラス３の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分すること。

b) クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。

c) クラス３の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにすること。

d) 一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずること。業者が作業を行う場合は立会いや監視カメラ等により監視するための措置を講ずること。

(1)-5　全学実施責任者は、以下を例とする、区域へのクラスの割当ての基準を定めること。
a) クラスの割当ての基準を以下のように定める。
- サーバ室や日常的に機密性が高い情報を取り扱う執務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス３を割り当てる。
- 一般的な執務室や執務室内の会議室には、事務従事者以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス２を割り当てる。

(2) 区域ごとの対策の決定
(a) 部局総括責任者は、全学実施責任者が定めた対策の基準を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定めること。
(b) 区域情報セキュリティ責任者は、管理する区域について、全学実施責任者が定めた対策の基準と、周辺環境や当該区域で行う高等教育機関の事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。

【 基本対策事項 】

(2)-1　区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う高等教育機関の事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定すること。

(3) 要管理対策区域における対策の実施
(a) 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。事務従事者が実施すべき対策については、事務従事者が認識できる措置を講ずること。
(b) 区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずること。
(c) 事務従事者は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、事務従事者が学外の者を立ち入らせる際には、当該高等教育機関外の者にも当該区域で定められた対策に従って利用させること。

【 基本対策事項 】

(3)-1　区域情報セキュリティ責任者は、管理する区域について、以下を例とする利用手順等を整備し、当該区域を利用する事務従事者に周知すること。
a) 扉の施錠及び開閉に関する利用手順
b) 一時的に立ち入る者が許可された者であることを確認するための手順
c) 一時的に立ち入る者を監視するための手順

第 4 部　外部委託

4.1　外部委託

4.1.1　外部委託

目的・趣旨

学外の者に、情報システムの開発、アプリケーションプログラムの開発等を委託する際に、事務従事者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において事務情報セキュリティ対策基準に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

外部委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお、クラウドサービスの利用に係る外部委託については、クラウドサービス特有のリスクがあることを理解した上で、4.1.4 項「クラウドサービスの利用」についても本項に加えて遵守する必要がある。

また、民間事業者が不特定多数向けに約款に基づきインターネット上で提供する情報処理サービス等、1.3 節において「約款による外部サービス」として定義するものを利用し、高等教育機関の事務を遂行する場合も外部委託の一つの形態と考えられるが、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、その際は本項に代えて 4.1.2 項「約款による外部サービスの利用」を適用すること。

＜外部委託の例＞

- 情報システムの開発及び構築
- アプリケーション・コンテンツの開発業務
- 情報システムの運用業務
- 業務運用支援業務（統計、集計、データ入力、媒体変換等）
- プロジェクト管理支援業務
- 調査・研究業務（調査、研究、検査等）
- 情報システム、データセンター、通信回線等の賃貸借

遵守事項

(1) 外部委託に係る規定の整備

(a) 全学実施責任者は、外部委託に係る以下の内容を含む規定を整備すること。

(ア) 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準

(イ) 委託先の選定基準

(2) 外部委託に係る契約

(a) 部局技術責任者又は職場情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。

(ア) 委託先に提供する情報の委託先における目的外利用の禁止

(イ) 委託先における情報セキュリティ対策の実施内容及び管理体制

(ウ) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制

(エ) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

(オ) 情報セキュリティインシデントへの対処方法

(カ) 情報セキュリティ対策その他の契約の履行状況の確認方法

(キ) 情報セキュリティ対策の履行が不十分な場合の対処方法

(b) 部局技術責任者又は職場情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

(c) 部局技術責任者又は職場情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(a)(b)の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を府省庁に提供し、府省庁の承認を受けるよう、仕様内容に含めること。

【 基本対策事項 】

(2)-1 部局技術責任者又は職場情報セキュリティ責任者は、以下の内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させること。また、変更があった場合は、速やかに再提出させること。

a) 当該委託業務に携わる者の特定

b) 当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

(2)-2 部局技術責任者又は職場情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱うこと。

(3) 外部委託における対策の実施

(a) 部局技術責任者又は職場情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。

(b) 部局技術責任者又は職場情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はそ

の旨の報告を事務従事者より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせること。

(c) 部局技術責任者又は職場情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

(4) 外部委託における情報の取扱い

(a) 事務従事者は、委託先への情報の提供等において、以下の事項を遵守すること。

(ア) 委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。

(イ) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。

(ウ) 委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに部局技術責任者又は職場情報セキュリティ責任者に報告すること。

4.1.2 約款による外部サービスの利用

目的・趣旨

外部委託により高等教育機関の事務を遂行する場合は、原則として 4.1.1 項「外部委託」にて規定する事項について、委託先と特約を締結するなどし、情報セキュリティ対策を適切に講ずる必要がある。しかしながら、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合には、民間事業者が不特定多数の利用者向けに約款に基づきインターネット上で提供する情報処理サービス等、1.3 節において「約款による外部サービス」として定義するものを利用することも考えられる。

このような「約款による外部サービス」をやむを得ず利用する場合には、種々の情報を政府機関からサービス提供事業者等に送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断し、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(1) 約款による外部サービスの利用に係る規定の整備

(a) 全学実施責任者は、以下を含む約款による外部サービスの利用に関する規定を整備すること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

(ア) 約款による外部サービスを利用してよい業務の範囲

(イ) 業務に利用する約款による外部サービス

(ウ) 利用手続及び運用手順

(b) 部局総括責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定めること。

【 基本対策事項 】

(1)-1　全学実施責任者は、本学において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定めること。

a) 利用申請の許可権限者

b) 利用申請時の申請内容

- 利用する組織名
- 利用するサービス
- 利用目的（業務内容）
- 利用期間
- 利用責任者（利用アカウントの責任者）

c) サービス利用中の安全管理に係る運用手順

- サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
- 情報の滅失、破壊等に備えたバックアップの取得
- 利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等）

d) 情報セキュリティインシデント発生時の連絡体制

(2) 約款による外部サービスの利用における対策の実施

(a) 事務従事者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

4.1.3　ソーシャルメディアサービスによる情報発信

目的・趣旨

インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していく様々なソーシャルメディアサービスが普及している。本学においても、積極的な広報活動等を目的に、こうしたサービスが利用されるようになっている。しかし、民間事業者等により提供されるソーシャルメディアサービスは、.example.ac.jp で終わるドメイン名（以下「A 大学ドメイン名」という。）を使用することができないため、真正なアカウントであることを利用者等が確認できるようにする必要がある。また、本学のアカウントを乗っ取られる場合や、利用しているソーシャルメディアサービスが予告なくサービス停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く提供する際には、当該情報を必要とする利用者等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により利用者等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。

このようなソーシャルメディアサービスは機能拡張やサービス追加等の技術進展が著しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。

なお、ソーシャルメディアサービスの利用は、約款による外部サービスの利用に相当することから、4.1.2 項の規定と同様に、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(1) ソーシャルメディアサービスによる情報発信時の対策

(a) 全学実施責任者は、本学が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

(ア) 本学のアカウントによる情報発信が実際の本学のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。

(イ) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。

(b) 部局総括責任者は、本学において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めること。

(c) 事務従事者は、要安定情報の学外への提供にソーシャルメディアサービスを用いる場合は、本学の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

【 基本対策事項 】

(1)-1　全学実施責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定めること。

a) アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

b) URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

(1)-2　全学実施責任者は、本学のアカウントによる情報発信が実際の本学のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定めること。

c) 本学からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、本学が運用していることを利用者に明示すること。

d) 本学からの情報発信であることを明らかにするために、本学が A 大学ドメイン名を用いて管理しているウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

e) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページの URL を記載すること。

f) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

(1)-3　全学実施責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定めること。

a) パスワードを適切に管理すること。具体的には、ログインパスワードは十分な長さと複雑さを持たせ、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

b) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

c) ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭ったりした場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行うこと。

d) ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実

施すること。

(1)-4　全学実施責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定めること。

a) 自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。

b) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織の CSIRT や文部科学省、内閣サイバーセキュリティセンターに報告するなど、適切な対処を行うこと。

4.1.4　クラウドサービスの利用

目的・趣旨

業務及び情報システムの高度化・効率化等の理由から、政府機関において今後クラウドサービスの利用の拡大が見込まれている。クラウドサービスの利用に当たっては、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。

クラウドサービスを利用する際、政府機関がクラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、政府機関による委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分考慮することが求められる。

遵守事項

(1)　クラウドサービスの利用における対策

(a)　部局技術責任者は、クラウドサービス（民間事業者が提供するものに限らず、政府等が提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。

(b)　部局技術責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。

(c)　部局技術責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。

(d)　部局技術責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めること。

(e)　部局技術責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

【 基本対策事項 】

(1)-1　部局技術責任者は、クラウドサービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することをクラウドサービスの選定条件とし、仕様内容にも含めること。

a）取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件

b) 取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

(1)-2 部局技術責任者は、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティ対策を構築すること。また、対策を実現するために、以下を例とするセキュリティ要件をクラウドサービスに求め、契約内容にも含めること。特に、運用段階で委託先が変更となる場合、開発段階等で設計したクラウドサービスのセキュリティ要件のうち継承が必須なセキュリティ要件について、変更後の委託先における維持・向上の確実性を事前に確認すること。

a) クラウドサービスに係るアクセスログ等の証跡の保存及び提供
b) インターネット回線とクラウド基盤の接続点の通信の監視
c) クラウドサービスの委託先による情報の管理・保管の実施内容の確認
d) クラウドサービス上の脆弱性対策の実施内容の確認
e) クラウドサービス上の情報に係る復旧時点目標（RPO）等の指標
f) クラウドサービス上で取り扱う情報の暗号化
g) 利用者の意思によるクラウドサービス上で取り扱う情報の確実な削除・廃棄
h) 利用者が求める情報開示請求に対する開示項目や範囲の明記

第 5 部　情報システムのライフサイクル

5.1　　情報システムに係る文書等の整備

5.1.1　　情報システムに係る台帳等の整備

目的・趣旨

本学が所管する情報システムの情報セキュリティ水準を維持するとともに、情報セキュリティインシデントに適切かつ迅速に対処するためには、本学が所管する情報システムの情報セキュリティ対策に係る情報を情報システム台帳で一元的に把握するとともに、情報システムの構成要素に関する調達仕様書や設定情報等が速やかに確認できるように、日頃から文書として整備しておき、その所在を把握しておくことが重要である。

遵守事項

(1) 情報システム台帳の整備

(a) 全学実施責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。

(b) 部局技術責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について全学実施責任者に報告すること。

【 基本対策事項 】

(1)-1　全学実施責任者は、以下の内容を含む台帳を整備すること。

a) 情報システム名
b) 管理課室
c) 当該部局技術責任者の氏名及び連絡先
d) システム構成
e) 接続する学外通信回線の種別
f) 取り扱う情報の格付及び取扱制限に関する事項
g) 当該情報システムの設計・開発、運用・保守に関する事項

また、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備すること。

a) 情報処理サービス名
b) 契約事業者
c) 契約期間
d) 情報処理サービスの概要
e) ドメイン名

f) 取り扱う情報の格付及び取扱制限に関する事項

(1)-2 部局技術責任者は、政府情報システム管理データベースの登録対象となるシステムについては、当該データベースに必要な情報を記録し、適時最新の情報に更新すること。

(2) 情報システム関連文書の整備

(a) 部局技術責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備すること。

(ア) 情報システムを構成するサーバ装置及び端末関連情報

(イ) 情報システムを構成する通信回線及び通信回線装置関連情報

(ウ) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

(エ) 情報セキュリティインシデントを認知した際の対処手順

【 基本対策事項 】

(2)-1 部局技術責任者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備すること。

a) サーバ装置及び端末を管理する事務従事者及び利用者を特定する情報

b) サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン

c) サーバ装置及び端末の仕様書又は設計書

(2)-2 部局技術責任者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、以下を含む文書を整備すること。

a) 通信回線及び通信回線装置を管理する事務従事者を特定する情報

b) 通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン

c) 通信回線及び通信回線装置の仕様書又は設計書

d) 通信回線の構成

e) 通信回線装置におけるアクセス制御の設定

f) 通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応

g) 通信回線の利用部門

(2)-3 部局技術責任者は、所管する情報システムについて、情報システム構成要素ごとのセキュリティ維持に関する以下を含む手順を定めること。

a) サーバ装置及び端末のセキュリティの維持に関する手順

b) 通信回線を介して提供するサービスのセキュリティの維持に関する手順

c) 通信回線及び通信回線装置のセキュリティの維持に関する手順

5.1.2 機器等の調達に係る規定の整備

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製

造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。

これらの課題に対応するため、事務情報セキュリティ対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1) 機器等の調達に係る規定の整備

(a) 全学実施責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を本学が確認できることを加えること。

(b) 全学実施責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

(1)-1 全学実施責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を例に規定すること。

a) 調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、本学と調達先が連携して原因を調査・排除できる体制を整備していること。

(1)-2 全学実施責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408 に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定めること。

(1)-3 全学実施責任者は、機器等の納入時の確認・検査手続には以下を含む事項を確認できる手続を定めること。

a) 調達時に指定したセキュリティ要件の実装状況

b) 機器等に不正プログラムが混入していないこと

5.2 情報システムのライフサイクルの各段階における対策

5.2.1 情報システムの企画・要件定義

目的・趣旨

情報システムのライフサイクル全般を通じて、情報セキュリティを適切に維持するためには、情報システムの企画段階において、適切にセキュリティ要件を定義する必要がある。

セキュリティ要件の曖昧さや過不足は、過剰な情報セキュリティ対策に伴うコスト増加のおそれ、要件解釈のばらつきによる提案内容の差異からの不公平な競争入札、設計・開発工程での手戻り、運用開始後の情報セキュリティインシデントの発生といった不利益が生じる可能性に繋がる。

そのため、情報システムが対象とする業務、業務において取り扱う情報、情報を取り扱う者、情報を処理するために用いる環境・手段等を考慮した上で、当該情報システムにおいて想定される脅威への対策を検討し、必要十分なセキュリティ要件を仕様に適切に組み込むことが重要となる。

加えて、構築する情報システムへの脆弱性の混入を防止するための対策も、構築前の企画段階で考慮することが重要となる。

また、情報システムの構築、運用・保守を外部委託する場合については、4.1 節「外部委託」についても併せて遵守する必要がある。

遵守事項

(1) 実施体制の確保

(a) 部局技術責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者に求めること。

(b) 部局技術責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し、運用管理する本学が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めること。

(2) 情報システムのセキュリティ要件の策定

(a) 部局技術責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定すること。

(ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

(イ) 情報システム運用時の監視等の運用管理機能要件

(ウ) 情報システムに関連する脆弱性についての対策要件

(b) 部局技術責任者は、インターネット回線と接続する情報システムを構築する場合は、

接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。

(c) 部局技術責任者は、学外利用者・企業と本学との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定すること。

(d) 部局技術責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

(e) 部局技術責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

【 基本対策事項 】

(2)-1 部局技術責任者は、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定すること。

(2)-2 部局技術責任者は、開発する情報システム**が運用される際に想定される脅威**の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書等に明記すること。

(2)-3 部局技術責任者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、ST 確認を受けること。

(2)-4 部局技術責任者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、以下を含む措置を実施すること。

a) 情報システム運用時に情報セキュリティ確保のために必要となる管理機能を仕様書等に明記すること。

b) 情報セキュリティインシデントの発生を監視する必要があると認めた場合には、監視のために必要な機能について、以下を例とする機能を仕様書等に明記すること。

- 学外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能
- 不正プログラム感染や踏み台に利用されること等による学外への不正な通信を監視する機能
- 学内通信回線への端末の接続を監視する機能
- 端末への外部電磁的記録媒体の挿入を監視する機能
- サーバ装置等の機器の動作を監視する機能

(2)-5 部局技術責任者は、開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を含む対策を仕様書等に明記すること。

a) 既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。
b) 開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針。
c) セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。
d) ソフトウェアのサポート期間又はサポート打ち切り計画に関する本学への情報提供

(2)-6 部局技術責任者は、構築する情報システムの構成要素のうち製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施すること。
a) 「IT 製品の調達におけるセキュリティ要件リスト」を参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とすること。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。
b) 「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定すること。

(3) 情報システムの構築を外部委託する場合の対策
(a) 部局技術責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させること。
(ア) 情報システムのセキュリティ要件の適切な実装
(イ) 情報セキュリティの観点に基づく試験の実施
(ウ) 情報システムの開発環境及び開発工程における情報セキュリティ対策

【 基本対策事項 】

(3)-1 部局技術責任者は、情報セキュリティの観点に基づく試験の実施について、以下を含む事項を実施させること。
a) ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離すること。
b) 情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。
c) 情報セキュリティの観点から実施した試験の実施記録を保存すること。

(3)-2 部局技術責任者は、開発工程における情報セキュリティ対策として、以下を含む事項を実施させること。
a) ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコード

の管理を適切に行うこと。
- ソースコードの変更管理
- ソースコードの閲覧制限のためのアクセス制御
- ソースコードの滅失、き損等に備えたバックアップの取得

b) 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

c) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること。

(4) 情報システムの運用・保守を外部委託する場合の対策

(a) 部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。

【 基本対策事項 】

(4)-1 部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を含む要件を調達仕様書に記載するなどして、適切に実施させること。

a) 情報システムの運用環境に課せられるべき条件の整備

b) 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

c) 情報システムの保守における情報セキュリティ対策

d) 運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

5.2.2　情報システムの調達・構築

目的・趣旨

情報システムを調達・構築する際には、策定したセキュリティ要件に基づく情報セキュリティ対策を適切に実施するために、選定基準に適合した機器等の調達や、情報システムの開発工程での情報セキュリティ対策の実施が求められる。

また、機器等の納入時又は情報システムの受入れ時には、整備された検査手続に従い、当該情報システムが運用される際に取り扱う情報を保護するためのセキュリティ機能及びその管理機能が、適切に情報システムに組み込まれていることを検査することが必要となる。

遵守事項

(1) 機器等の選定時の対策

(a) 部局技術責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用すること。

(2) 情報システムの構築時の対策

(a) 部局技術責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。

(b) 部局技術責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。

【 基本対策事項 】

(2)-1　部局技術責任者は、情報システムの構築において以下を含む情報セキュリティ対策を行うこと。

a) 情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備すること。

b) セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。

c) 情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。

d) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施すること。

e) 脆弱性検査を含む情報セキュリティの観点での試験を実施すること。

(2)-2　部局技術責任者は、情報システムの運用保守段階へ移行するに当たり、以下を含む情報セキュリティ対策を行うこと。

f) 情報セキュリティに関わる運用保守体制の整備

g) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

h) 情報セキュリティインシデントを認知した際の対処方法の確立

(3) 納品検査時の対策

(a) 部局技術責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。

5.2.3 情報システムの運用・保守

目的・趣旨

情報システムの運用段階に移るに当たり、企画又は調達・構築時に決定したセキュリティ要件が適切に運用されるように、人的な運用体制を整備し、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を実施する必要がある。

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生することが大半であることから、適宜情報システムの情報セキュリティ対策の実効性を確認するために、情報システムの運用状況を監視することも重要である。

また、情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても、事務情報セキュリティ対策基準に基づく情報セキュリティ対策について適切に措置を講ずることが求められる。

遵守事項

(1) 情報システムの運用・保守時の対策

(a) 部局技術責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。

(b) 部局技術責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し運用管理する本学との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

(c) 部局技術責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

【 基本対策事項 】

(1)-1 部局技術責任者は、情報システムのセキュリティ監視を行う場合は、以下の内容を含む監視手順を定め、適切に監視運用すること。

(a) 監視するイベントの種類

(b) 監視体制

(c) 監視状況の報告手続
(d) 情報セキュリティインシデントの可能性を認知した場合の報告手順
(e) 監視運用における情報の取扱い（機密性の確保）

(1)-2 部局技術責任者は、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認すること。

(1)-3 部局技術責任者は、情報システムにおいて取り扱う情報について、当該情報の格付及び取扱制限が適切に守られていることを確認すること。

(1)-4 部局技術責任者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。

5.2.4 情報システムの更改・廃棄

目的・趣旨

情報システムの更改・廃棄において、情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。

情報システムに機密性の高い情報が記録されている場合や、格付や取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講ずることが必要となる。

遵守事項

(1) 情報システムの更改・廃棄時の対策
(a) 部局技術責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。
(ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策
(イ) 情報システム廃棄時の不要な情報の抹消

5.2.5 情報システムについての対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、新たに発生した脅威等に的確に対応しない場合には、情報セキュリティ水準を維持できなくなる。このため、情報システムの情報セキュリティ対策を定期的に見直し、さらに外部環境の急激な変化等が発生した場合は、適時見直しを行うことが必要となる。

遵守事項

(1) 情報システムについての対策の見直し

(a) 部局技術責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

5.3 情報システムの運用継続計画

5.3.1 情報システムの運用継続計画の整備・整合的運用の確保

目的・趣旨

業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、非常時でも継続させる必要があり、本学においては業務継続計画を策定し運用している。

一方、非常時に情報システムの運用を継続させる場合には、非常時における情報セキュリティに係る対策事項を検討し、定めることが重要となる。

なお、業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。

遵守事項

(1) 情報システムの運用継続計画の整備・整合的運用の確保

(a) 全学実施責任者は、本学において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討すること。

(b) 全学実施責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認すること。

第 6 部　情報システムのセキュリティ要件

6.1　　情報システムのセキュリティ機能

6.1.1　　主体認証機能

目的・趣旨

情報又は情報システムへアクセス可能な主体を制限するためには、主体認証機能の導入が必要である。その際、アクセス権限のある主体へのなりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講ずることが重要となる。

また、本学の情報システムにおいて、一般向けのサービスを提供する場合は、一般の利用者が情報システムへのアクセスの主体になることにも留意して、主体認証情報を適切に保護しなければならない。

遵守事項

(1) 主体認証機能の導入

(a) 部局技術責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けること。

(b) 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。

【 基本対策事項 】

(1)-1　部局技術責任者は、主体認証は、以下を例とする主体認証方式を決定すること。

a）**知識**（パスワード等、利用者本人のみが知り得る情報）による認証

b）**所有**（電子証明書を格納する IC カード又はワンタイムパスワード生成器等、利用者本人のみが所有する機器等）による認証

c）**生体**（指紋や静脈等、本人の生体的な特徴）による認証

(1)-2　部局技術責任者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、文字の種類や組合せ、桁数等のパスワード設定条件を利用者に守らせる機能を設けること。

(1)-3　部局技術責任者は、主体認証を行う情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下の機能を設けること。

a）利用者が定期的に変更しているか否かを確認する機能

b) 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

(1)-4 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下を例とする方法を用いて適切に管理すること。

a) 主体認証情報を送信又は保存する場合には、その内容を暗号化する。

b) 主体認証情報に対するアクセス制限を設ける。

(1)-5 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に利用され、又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設けること。

a) 当該主体認証情報及び対応する識別コードの利用を停止する機能

b) 主体認証情報の再設定を利用者に要求する機能

(2) 識別コード及び主体認証情報の管理

(a) 部局技術責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。

(b) 部局技術責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。

【 基本対策事項 】

(2)-1 部局技術責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）すること。

(2)-2 部局技術責任者は、識別コードの付与に当たっては、以下を例とする措置を講ずること。

a) 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

b) 主体への識別コードの付与に関する記録を消去する場合の部局総括責任者からの事前の許可

(2)-3 部局技術責任者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること。

(2)-4 部局技術責任者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。

(2)-5 部局技術責任者は、知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促すこと。

(2)-6 部局技術責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、部局技術責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。

(2)-7 部局技術責任者は、主体認証情報の不正な利用を防止するために、主体が情報システムを

利用する必要がなくなった場合には、以下を例とする措置を講ずること。
a）当該主体の識別コードを無効にする。
b）当該主体に交付した主体認証情報格納装置を返還させる。
c）無効化した識別コードを他の主体に新たに発行することを禁止する。

6.1.2 アクセス制御機能

目的・趣旨

アクセス制御とは、情報システム及び情報へのアクセスを許可する主体を制限することである。複数の主体が情報システムを利用する場合、当該情報システムにおいて取り扱う情報へのアクセスを業務上必要な主体のみに限定することによって、情報漏えい等のリスクを軽減することができると考えられる。

遵守事項

(1) アクセス制御機能の導入
(a) 部局技術責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。
(b) 部局技術責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。

【 基本対策事項 】

(1)-1 部局技術責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、必要に応じて、以下を例とするアクセス制御機能の要件を定めること。
a）利用時間や利用時間帯によるアクセス制御
b）同一主体による複数アクセスの制限
c）IP アドレスによる端末の制限
d）ネットワークセグメントの分割によるアクセス制御

6.1.3 権限の管理

目的・趣旨

重要システムのアクセス制御機能を適切に運用するためには、主体から対象に対するアクセスの権限を適切に設定することが必要である。権限の管理が不適切になると、情報又は情報システムへ不正アクセスされるおそれが生じる。

また、情報システムの管理機能として、一般的に管理者権限にはあらゆる操作が許可される特権が付与されている。当該特権が悪意ある第三者等に入手された場合、主体認証情報等

の漏えい、改ざん又は情報システムに係る設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念されることから、限られた主体のみに管理者権限が付与されることが重要である。

遵守事項

(1) 権限の管理

(a) 部局技術責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。

(b) 部局技術責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

【 基本対策事項 】

(1)-1 部局技術責任者は、主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するため、以下を例とする措置を講ずること。

a) 業務上必要な場合に限定する

b) 必要最小限の権限のみ付与する

c) 管理者権限を行使できる端末をシステム管理者等の専用の端末とする

6.1.4 ログの取得・管理

目的・趣旨

情報システムにおけるログとは、通信履歴その他運用管理等に必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の情報セキュリティインシデント及びその予兆を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

遵守事項

(1) ログの取得・管理

(a) 部局技術責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。

(b) 部局技術責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの

保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。

(c) 部局技術責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

【 基本対策事項 】

(1)-1 部局技術責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。

(1)-2 部局技術責任者は、所管する情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理すること。

a) 事象の主体（人物又は機器等）を示す識別コード
b) 識別コードの発行等の管理記録
c) 利用者による情報システムの操作記録
d) 事象の種類
e) 事象の対象
f) 正確な日付及び時刻
g) 試みられたアクセスに関わる情報
h) 電子メールのヘッダ情報及び送信内容
i) 通信パケットの内容
j) 操作する者、監視する者、保守する者等への通知の内容

(1)-3 部局技術責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。

(1)-4 部局技術責任者は、ログが取得できなくなった場合の対処方法を定めること。

(1)-5 部局技術責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入すること。

a) ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化

6.1.5 暗号・電子署名

目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用するアルゴリズムに加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズムが危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せ

て考慮することが必要となる。

遵守事項

(1) 暗号化機能・電子署名機能の導入

(a) 部局技術責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。

(ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(b) 部局技術責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

(ア) 事務従事者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」又は、本学における検証済み暗号リストがあればその中に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

(ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

(c) 部局技術責任者は、本学における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書をUPKI 電子証明書発行サービスが発行している場合は、それを使用するように定めること。

【 基本対策事項 】

(1)-1 部局技術責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。

a) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。

b) 複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。

c) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護される製品を利用することを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。
d) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。
e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のある暗号プロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

(2) 暗号化・電子署名に係る管理
(a) 部局技術責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。
(ア)電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。
(イ)暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、事務従事者と共有を図ること。

【 基本対策事項 】
(2)-1 部局技術責任者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とすること。
a) 信頼できる機関による電子証明書の提供
b) 本学の窓口での電子証明書の提供

6.2 情報セキュリティの脅威への対策

6.2.1 ソフトウェアに関する脆弱性対策

目的・趣旨

本学の情報システムに対する脅威としては、第三者が情報システムに侵入し本学の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に、一般向けに提供するサービスが第三者に侵入され、個人情報の漏えい等が発生した場合、本学に対する社会的な信用が失われる。

一般的に、このような攻撃では、情報システムを構成するサーバ装置、端末及び通信回線装置のソフトウェアの脆弱性を悪用されることが想定される。したがって、本学の情報システムにおいては、ソフトウェアに関する脆弱性について、迅速かつ適切に対処することが求められる。

なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2 項「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。

遵守事項

(1) ソフトウェアに関する脆弱性対策の実施

(a) 部局技術責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。

(b) 部局技術責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。

(c) 部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。

(d) 部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。

【 基本対策事項 】

(1)-1 部局技術責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む情報を適宜入手すること。

a) 脆弱性の原因
b) 影響範囲
c) 対策方法
d) 脆弱性を悪用する不正プログラムの流通状況

(1)-2 部局技術責任者は、利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しないこと。

(1)-3 部局技術責任者は、構成要素ごとにソフトウェアのバージョン等を把握し、脆弱性対策の状況を確認すること。

(1)-4 部局技術責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項について判断すること。

a) 対策の必要性
b) 対策方法
c) 対策方法が存在しない場合又は対策が完了するまでの期間に対する一時的な回避方法
d) 対策方法又は回避方法が情報システムに与える影響
e) 対策の実施予定
f) 対策試験の必要性
g) 対策試験の方法

h）対策試験の実施予定

(1)-5　部局技術責任者は、脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。

a）実施日

b）実施内容

c）実施者

(1)-6　部局技術責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「対策用ファイル」という。）は、信頼できる方法で入手すること。

(1)-7　部局技術責任者は、脆弱性対策の状況を確認する間隔は、可能な範囲で短くすること。

6.2.2　不正プログラム対策

目的・趣旨

情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼすおそれがある。このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

遵守事項

(1) 不正プログラム対策の実施

(a) 部局技術責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

(b) 部局技術責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

(c) 部局技術責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。

【 基本対策事項 】

(1)-1　部局技術責任者は、不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるよう構成すること。

(1)-2　部局技術責任者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

(1)-3　部局技術責任者は、不正プログラム対策ソフトウェア等は、定期的に全てのファイルを対象としたスキャンを実施するよう構成すること。

(1)-4　部局技術責任者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行うこと。

(1)-5　部局技術責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。

a）不正プログラム対策ソフトウェア等の導入状況

b）不正プログラム対策ソフトウェア等の定義ファイルの更新状況

6.2.3 サービス不能攻撃対策

目的・趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、本学の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。

遵守事項

(1) サービス不能攻撃対策の実施

(a) 部局技術責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下この項において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。

(b) 部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。

(c) 部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。

【 基本対策事項 】

(1)-1　部局技術責任者は、サーバ装置、端末及び通信回線装置について、以下を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。

a）パケットフィルタリング機能

b）3-way handshake 時のタイムアウトの短縮

c）各種 Flood 攻撃への防御

d）アプリケーションゲートウェイ機能

(1)-2　部局技術責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報シ

ステムを構築すること。

(1)-3　部局技術責任者は、サーバ装置、端末及び通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、以下を例とする対策を検討すること。

a) インターネットに接続している通信回線の提供元となる事業者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策

b) サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入

c) サーバ装置、端末及び通信回線装置及び通信回線の冗長化

(1)-4　部局技術責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討すること。

(1)-5　部局技術責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定めること。

(1)-6　部局技術責任者は、監視対象の監視記録を保存すること。

6.2.4　標的型攻撃対策

目的・趣旨

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。

したがって、標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

遵守事項

(1) 標的型攻撃対策の実施

(a) 部局技術責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。

(b) 部局技術責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。

【 基本対策事項 】

(1)-1　部局技術責任者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以

下を例とする対策を行うこと。

a) 不要なサービスについて機能を削除又は停止する。

b) 不審なプログラムが実行されないよう設定する。

c) パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

(1)-2 部局技術責任者は、USB メモリ等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下を例とする対策を行うこと。

a) 出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接続する外部電磁的記録媒体を事前に特定しておく。

b) 外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。

c) サーバ装置及び端末について、自動再生（オートラン）機能を無効化する。

d) サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする。

e) サーバ装置及び端末について、使用を想定しない USB ポートを無効化する。

f) 組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。

(1)-3 部局技術責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を例とする対策を行うこと。

a) 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。

b) 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずる。

(1)-4 部局技術責任者は、端末の管理者権限アカウントについて、以下を例とする対策を行うこと。

a) 不要な管理者権限アカウントを削除する。

b) 管理者権限アカウントのパスワードは、容易に推測できないものに設定する。

(1)-5 部局技術責任者は、重点的に守るべき業務・情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って、対策を講ずること。

6.3 アプリケーション･コンテンツの作成･提供

6.3.1 アプリケーション・コンテンツの作成時の対策

目的・趣旨

本学では、情報の提供、諸手続、意見募集等のサービスのためにアプリケーション・コンテンツを用意し、広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に、利用者端末の情報セキュリティ水準の低下を招いてしまうことは避けなければならない。本学は、アプリケーション・コンテンツの提供に際しても、情報セキュリティ対策を講じておく必要がある。

また、アプリケーション・コンテンツの開発・提供を外部委託する場合については、4.1.1 項「外部委託」についても併せて遵守する必要がある。

遵守事項

(1) アプリケーション・コンテンツの作成に係る規定の整備

(a) 全学実施責任者は、アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること。

(2) アプリケーション・コンテンツのセキュリティ要件の策定

(a) 部局技術責任者は、学外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含めること。

(ア) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

(イ) 提供するアプリケーションが脆弱性を含まないこと。

(ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

(エ) 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

(オ) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

(カ) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

(b) 事務従事者は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前号に掲げる内容を調達仕様に含めること。

【 基本対策事項 】

(2)-1 部局技術責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を含む対策を行うこと。

a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

b) 外部委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。

(2)-2 部局技術責任者は、提供するアプリケーション・コンテンツにおいて、学外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、当該高等教育機関外へのアクセスが情報セキュリティ上安全なものであることを確認すること。

(2)-3 部局技術責任者は、提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない学外へのアクセスを自動的に発生させる機能を含めないこと。

(2)-4 部局技術責任者は、文書ファイル等のコンテンツの提供において、当該コンテンツが改ざん等なく真正なものであることを確認できる手段がない場合は、「https://」で始まる URL のウェブページから当該コンテンツをダウンロードできるように提供すること。

(2)-5 部局技術責任者は、改ざん等がなく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

6.3.2 アプリケーション・コンテンツ提供時の対策

目的・趣旨

本学では、情報の提供、諸手続及び意見募集等のサービスのためにウェブサイト等を用意し、一般利用者等の利用に供している。これらのサービスは通常インターネットを介して利用するものであるため、一般利用者等にとっては、そのサービスが実際の本学のものであると確認できることが重要である。また、本学になりすましたウェブサイトを放置しておくと、本学の信用を損なうだけでなく、利用者等が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講ずる必要がある。

遵守事項

(1) A 大学ドメイン名の使用

(a) 部局技術責任者は、学外向けに提供するウェブサイト等が実際の本学提供のものであることを利用者が確認できるように、A 大学ドメイン名を情報システムにおいて使用するよう仕様に含めること。ただし、4.1.3 項に掲げる場合を除く。

(b) 事務従事者は、学外向けに提供するウェブサイト等の作成を外部委託する場合におい

ては、前号と同様、A 大学ドメイン名を使用するよう調達仕様に含めること。

(2) 不正なウェブサイトへの誘導防止

(a) 部局技術責任者は、利用者が検索サイト等を経由して本学のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。

【 基本対策事項 】

(2)-1 部局技術責任者は、学外向けに提供するウェブサイトに対して、以下を例とする検索エンジン最適化措置（SEO 対策）を講ずること。

c) クローラからのアクセスを排除しない。

d) cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする。

e) 適切なタイトルを設定する。

f) 不適切な誘導を行わない。

(2)-2 部局技術責任者は、学外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、不審なサイトへのアクセスを防止するための対策を講ずること。

(3) アプリケーション・コンテンツの告知

(a) 事務従事者は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。

(b) 事務従事者は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つこと。

【 基本対策事項 】

(3)-1 事務従事者は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示すること。また、短縮 URL を用いないこと。

(3)-2 事務従事者は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示すること。

(3)-3 事務従事者は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つために以下の措置を講ずること。

a) 告知するアプリケーション・コンテンツを管理する組織名を明記する。

b) 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する。

第 7 部　情報システムの構成要素

7.1　端末･サーバ装置等

7.1.1　端末

目的・趣旨

端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等のおそれがある。また、事務従事者の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。モバイル端末の利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、7.3.2 項「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

遵守事項

(1) 端末の導入時の対策

(a) 部局技術責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 部局技術責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。

(c) 部局技術責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

【 基本対策事項 】

(1)-1　部局技術責任者は、モバイル端末を除く端末について、原則としてクラス２以上の要管理対策区域に設置すること。

(1)-2　部局技術責任者は、端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

a) モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。

b) モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意する。

(1)-3　部局技術責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。
　a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。
　b) 要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。

(1)-4　部局技術責任者は、第三者により情報窃取されることを防止するために、以下を例とする、端末に保存される情報を暗号化するための機能又は利用者が端末に情報を保存できないようにするための機能を設けること。
　a) 端末に、ハードディスク等の電磁的記録媒体全体を暗号化する機能を設ける。
　b) 端末に、ファイルを暗号化する機能を設ける。
　c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。
　d) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。
　e) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。
　f) ハードディスク等電磁的記録媒体に保存されている情報を遠隔から消去する機能（遠隔データ消去機能）を設ける。

(1)-5　部局技術責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。
　a) ソフトウェアベンダのサポート状況
　b) ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容
　c) インストール時に同時にインストールされる他のソフトウェア
　d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

(2) 端末の運用時の対策

(a) 部局技術責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

(b) 部局技術責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

(3) 端末の運用終了時の対策

(a) 部局技術責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

7.1.2 サーバ装置

目的・趣旨

電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に本学が有するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、学外からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、6.2.3 項「サービス不能攻撃対策」、7.3.2 項「IPv6 通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベースについては、本項での共通的な対策に加え、それぞれ 7.2 節「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。

遵守事項

(1) サーバ装置の導入時の対策

(a) 部局技術責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。

(c) 部局技術責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

(d) 部局技術責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずること。

【 基本対策事項 】

(1)-1 部局技術責任者は、要保護情報を取り扱うサーバ装置については、クラス２以上の要管理対策区域に設置すること。

(1)-2 部局技術責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

a) 施錠可能なサーバラックに設置して施錠する。

b) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

(1)-3 部局技術責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。

a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。

(1)-4 部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため要安定情報を取り扱う情報システムについては、将来の見通しも考慮し、以下を例とする対策を講ずること。

a) 負荷分散装置、DNS ラウンドロビン方式等による負荷分散

b) 同一システムを２系統で構成することによる冗長化

(1)-5 部局技術責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。

a) ソフトウェアベンダのサポート状況

b) ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容

c) インストール時に同時にインストールされる他のソフトウェア

d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

(2) サーバ装置の運用時の対策

(a) 部局技術責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

(b) 部局技術責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図ること。

(c) 部局技術責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

(d) 部局技術責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講ずること。

【 基本対策事項 】

(2)-1 部局技術責任者は、所管する範囲内のサーバ装置の構成やソフトウェアの状態を定期的に確認する場合は、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。

(2)-2 部局技術責任者は、サーバ装置への無許可のアクセス等の不正な行為を監視するために、以下を例とする対策を講ずること。

a) アクセスログ等を定期的に確認する。

b) IDS/IPS、WAF 等を設置する。

c) 不正プログラム対策ソフトウェアを利用する。

d) ファイル完全性チェックツールを利用する。
e) CPU、メモリ、ディスク I/O 等のシステム状態を確認する。

(2)-3 部局技術責任者は、要安定情報を取り扱うサーバ装置については、運用状態を復元するために以下を例とする対策を講ずること。
a) サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。
b) 定期的なバックアップを実施する。
c) サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。
d) バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。

(3) サーバ装置の運用終了時の対策
(a) 部局技術責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。

7.1.3 複合機・特定用途機器

目的・趣旨

本学においては、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている複合機が利用されている。複合機は、学内通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、本学においては、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。

したがって、複合機や特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずることが重要である。

遵守事項

(1) 複合機
(a) 部局技術責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。
(b) 部局技術責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。
(c) 部局技術責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての

情報を抹消すること。

【 基本対策事項 】

(1)-1　部局技術責任者は、「IT 製品の調達におけるセキュリティ要件リスト」を参照するなどし、複合機が備える機能、設置環境及び取り扱う情報の格付及び取扱制限に応じ、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記すること。

(1)-2　部局技術責任者は、以下を例とする運用中の複合機に対する、情報セキュリティインシデントへの対策を講ずること。

a) 複合機について、利用環境に応じた適切なセキュリティ設定を実施する。

b) 複合機が備える機能のうち利用しない機能を停止する。

c) 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用する。

d) 学内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする。

e) 複合機をインターネットに直接接続しない。

f) リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

g) 利用者ごとに許可される操作を適切に設定する。

(1)-3　部局技術責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消すること。当該機能を備えていない複合機については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずること。

(2) 特定用途機器

(a) 部局技術責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。

【 基本対策事項 】

(2)-1　部局技術責任者は、特定用途機器の特性に応じて、以下を例とする対策を講ずること。

a) 特定用途機器について、利用環境に応じた適切なセキュリティ設定を実施する。

b) 特定用途機器が備える機能のうち利用しない機能を停止する。

c) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

d) インターネットに接続されている特定用途機器についてソフトウェアに関する脆弱性が存在しないか確認し、脆弱性が存在する場合、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。

e) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。
f) 特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消すること。

7.2 電子メール・ウェブ等

7.2.1 電子メール

目的・趣旨

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する事務従事者が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本項の遵守事項のほか、7.1.2 項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) 電子メールの導入時の対策

(a) 部局技術責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

(b) 部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

(c) 部局技術責任者は、電子メールのなりすましの防止策を講ずること。

【 基本対策事項 】

(1)-1 部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする事務従事者の主体認証を行う機能を備えること。

a) 電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入する。

(1)-2 部局技術責任者は、以下を例とする電子メールのなりすましの防止策を講ずること。

a) SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）等の送信ドメイン認証技術による送信側の対策を行う。

b) SPF、DKIM、DMARC 等の送信ドメイン認証技術による受信側の対策を行う。

c) S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用する。

7.2.2 ウェブ

目的・趣旨

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ（ウェブページとして公開している情報）の改ざん、ウェブサーバの利用停止、偽サイトへの誘導等の被害が想定されるため、適切な対策を組み合わせて実施することが求められる。

なお、本項の遵守事項のほか、7.1.2 項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) ウェブサーバの導入・運用時の対策

(a) 部局技術責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずること。

(ア) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

(イ) ウェブコンテンツの編集作業を担当する主体を限定すること。

(ウ) 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。

(エ) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。

(オ) サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。

(b) 部局技術責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

【 基本対策事項 】

(1)-1 部局技術責任者は、不要な機能の停止又は制限として、以下を例とするウェブサーバの管理や設定を行うこと。

a) CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする。

b) ディレクトリインデックスの表示を禁止する。

c) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する。

d) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。

(1)-2 部局技術責任者は、ウェブコンテンツの編集作業を担当する主体の限定として、以下を例とするウェブサーバの管理や設定を行うこと。

a) ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えない。
b) OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。

(1)-3 部局技術責任者は、公開してはならない又は無意味なウェブコンテンツが公開されないよう管理することとして、以下を例とするウェブサーバの管理や設定を行うこと。
a) 公開を想定していないファイルをウェブ公開用ディレクトリに置かない。
b) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。

(1)-4 部局技術責任者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行うこと。
a) ウェブコンテンツの更新の際は、専用の端末を使用して行う。
b) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する。
c) ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行う。

(1)-5 部局技術責任者は、通信時の盗聴による第三者への情報の漏えいの防止及び正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を例とするウェブサーバの実装を行うこと。
a) TLS（SSL）機能を適切に用いる。
b) TLS（SSL）機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる。
c) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された「SSL/TLS 暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する。

(2) ウェブアプリケーションの開発時・運用時の対策

(a) 部局技術責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

【 基本対策事項 】

(2)-1 部局技術責任者は、以下を含むウェブアプリケーションの脆弱性を排除すること。
a) SQL インジェクション脆弱性
b) OS コマンドインジェクション脆弱性
c) ディレクトリトラバーサル脆弱性
d) セッション管理の脆弱性
e) アクセス制御欠如と認可処理欠如の脆弱性
f) クロスサイトスクリプティング脆弱性

g) クロスサイトリクエストフォージェリ脆弱性
h) クリックジャッキング脆弱性
i) メールヘッダインジェクション脆弱性
j) HTTP ヘッダインジェクション脆弱性
k) eval インジェクション脆弱性
l) レースコンディション脆弱性
m) バッファオーバーフロー及び整数オーバーフロー脆弱性

7.2.3 ドメインネームシステム（DNS）

目的・趣旨

ドメインネームシステム（DNS : Domain Name System）は、インターネットを使った階層的な分散型システムで、主としてインターネット上のホスト名や電子メールに使われるドメイン名と、IP アドレスとの対応づけ（正引き、逆引き）を管理するために使用されている。DNS では、端末等のクライアント（DNS クライアント）からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係等について回答を行う。DNS には、本学が管理するドメインに関する問合せについて回答を行うコンテンツサーバと、DNS クライアントからの要求に応じてコンテンツサーバに対して問合せを行うキャッシュサーバが存在する。キャッシュサーバの可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また、コンテンツサーバが提供する情報の完全性が損なわれ、誤った情報を提供した場合は、端末等の DNS クライアントが悪意あるサーバに接続させられるなどの被害に遭う可能性がある。さらに、電子メールのなりすまし対策の一部は DNS で行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNS サーバの適切な管理が必要である。

なお、本項の遵守事項のほか、7.1.2 項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) DNS の導入時の対策

(a) 部局技術責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。

(b) 部局技術責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。

(c) 部局技術責任者は、コンテンツサーバにおいて、本学のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。

【 基本対策事項 】

(1)-1 部局技術責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講ずること。

a) コンテンツサーバを冗長化する。

b) 通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。

(1)-2 部局技術責任者は、学外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は必要であれば府省庁内からの名前解決の要求のみに応答をするよう、以下を例とする措置を講ずること。

a) キャッシュサーバの設定でアクセス制御を行う。
b) ファイアウォール等でアクセス制御を行う。

(1)-3 部局技術責任者は、DNS キャッシュポイズニング攻撃から保護するため、以下を例とする措置を講ずること。
a) ソースポートランダマイゼーション機能を導入する。
b) DNSSEC を利用する。

(1)-4 部局技術責任者は、学内のみで使用する名前の解決を提供するコンテンツサーバにおいて、以下を例とする当該コンテンツサーバで管理する情報の漏えいを防止するための措置を講ずること。
a) 外部向けのコンテンツサーバと別々に設置する。
b) ファイアウォール等でアクセス制御を行う。

(2) DNS の運用時の対策

(a) 部局技術責任者は、DNS のコンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。

(b) 部局技術責任者は、DNS のコンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。

(c) 部局技術責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。

【 基本対策事項 】

(2)-1 部局技術責任者は、キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（３か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持すること。

7.2.4 データベース

目的・趣旨

本項における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。

要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び事務従事者の不適切な利用や過失等の内的要因によるリスクに対して、

管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

特に大量のデータを保管するデータベースの場合、そのデータが漏えい等した際の影響が大きく、また、そのようなデータは攻撃者の標的となりやすい。

なお、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、7.3.2 項「IPv6 通信回線」において定める遵守事項のうち、データベースに関係するものについても併せて遵守する必要がある。

遵守事項

(1) データベースの導入・運用時の対策

(a) 部局技術責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。

(b) 部局技術責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。

(c) 部局技術責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。

(d) 部局技術責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

(e) 部局技術責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。

【 基本対策事項 】

(1)-1 部局技術責任者は、必要に応じて情報システムの管理者とデータベースの管理者を別にすること。

(1)-2 部局技術責任者は、データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しないこと。

(1)-3 部局技術責任者は、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずること。

(1)-4 部局技術責任者は、行政事務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずること。

c) 一定数以上のデータの取得に関するログを記録し、警告を発する。
d) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。

(1)-5 部局技術責任者は、データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除すること。

(1)-6 部局技術責任者は、データベースにアクセスする機器上で動作するプログラムに対して SQL インジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討すること。
a) ウェブアプリケーションファイアウォールの導入
b) データベースファイアウォールの導入

(1)-7 部局技術責任者は、データベースに格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

7.3 通信回線

7.3.1 通信回線

目的・趣旨

サーバ装置や端末への不正アクセスやサービス不能攻撃等は、当該サーバ装置や端末に接続された通信回線及び通信回線装置を介して行われる場合がほとんどであることから、通信回線及び通信回線装置に対する情報セキュリティ対策については、情報システムの構築時からリスクを十分検討し、必要な対策を実施しておく必要がある。通信回線の運用主体又は物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。

また、情報システムの運用開始時と一定期間運用された後とでは、通信回線の構成や接続される情報システムの条件等が異なる場合があり、攻撃手法の変化も想定されることから、情報システムの構築時に想定した対策では十分でなくなる可能性がある。そのため、通信回線の運用時においても、継続的な対策を実施することが重要である。

遵守事項

(1) 通信回線の導入時の対策

(a) 部局技術責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。

(b) 部局技術責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。

(c) 部局技術責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。

(d) 部局技術責任者は、事務従事者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。

(e) 部局技術責任者は、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。

(f) 部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。

(g) 部局技術責任者は、学内通信回線にインターネット回線、公衆通信回線等の学外通信回線を接続する場合には、学内通信回線及び当該高等教育機関内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。

(h) 部局技術責任者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視するための措置を講ずること。

(i) 部局技術責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。
(j) 部局技術責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。
(k) 部局技術責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくこと。

【 基本対策事項 】

(1)-1 部局技術責任者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じて、以下を例とする通信経路の分離を行うこと。
a) 外部との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離する。
b) 業務目的や取り扱う情報の格付及び取扱制限に応じて情報システムごとに VLAN により通信経路を分離し、それぞれの通信制御を適切に行う。
c) 他の情報システムから独立した専用の通信回線を構築する。

(1)-2 部局技術責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、SSL（TLS）、IPsec 等による暗号化を行うこと。また、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。

(1)-3 部局技術責任者は、学内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずること。
a) 情報システムの機器番号等により接続機器を識別する。
b) クライアント証明書により接続機器の認証を行う。

(1)-4 部局技術責任者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講ずること。
a) 通信回線装置を施錠可能なラック等に設置する。
b) 施設内に敷設した通信ケーブルを物理的に保護する。
c) 通信回線装置の操作ログを取得する。

(1)-5 部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずること。
a) 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。
b) 通信回線及び通信回線装置を冗長構成にする。

(1)-6 部局技術責任者は、学内通信回線に、インターネット回線や公衆通信回線等の学外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例と

する対策を講ずること。
a) ファイアウォール、WAF（Web Application Firewall）、リバースプロキシ等により通信制御を行う。
b) 通信回線装置による特定の通信プロトコルの利用を制限する。
c) IDS/IPS により不正アクセスを検知及び遮断する。

(1)-7 部局技術責任者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、以下を例とする対策を講ずること。
a) リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う。
b) 主体認証によりアクセス制御する。
c) 通信内容の暗号化により秘匿性を確保する。
d) ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにする。

(2) 通信回線の運用時の対策

(a) 部局技術責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずること。

(b) 部局技術責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。

(c) 部局技術責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。

(d) 部局技術責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。

【 基本対策事項 】

(2)-1 部局技術責任者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管すること。

(2)-2 部局技術責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。

(3) 通信回線の運用終了時の対策

(a) 部局技術責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。

(4) リモートアクセス環境導入時の対策

(a) 部局技術責任者は、VPN 回線を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。

(b) 部局技術責任者は、リモートアクセス環境を構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。

【 基本対策事項 】

(4)-1 部局技術責任者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。

a) 利用開始及び利用停止時の申請手続の整備
b) 通信を行う端末の識別又は認証
c) 利用者の認証
d) 通信内容の暗号化
e) 主体認証ログの取得及び管理
f) リモートアクセスにおいて利用可能な公衆通信網の制限
g) アクセス可能な情報システムの制限
h) リモートアクセス中の他の通信回線との接続禁止

(4)-2 部局技術責任者は、学外通信回線を経由した本学の情報システムへのリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。

a) 利用開始及び利用停止時の申請手続の整備
b) 利用者の認証又は発信者番号による識別及び認証
c) 主体認証ログの取得及び管理
d) アクセス可能な情報システムの制限
e) リモートアクセス中の他の通信回線との接続禁止

(5) 無線 LAN 環境導入時の対策

(a) 部局技術責任者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。

【 基本対策事項 】

(5)-1 部局技術責任者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、以下を例とする対策を講ずること。

a) SSID の隠ぺい
b) 無線 LAN 通信の暗号化
c) MAC アドレスフィルタリングによる端末の識別
d) 802.1X による無線 LAN へのアクセス主体の認証
e) 無線 LAN 回線利用申請手続の整備
f) 無線 LAN 機器の管理手順の整備

g) 無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対処手順の整備

7.3.2 IPv6 通信回線

目的・趣旨

本学において､インターネットの規格である IPv6 通信プロトコルに対応するための取組が進められているが、IPv6 通信プロトコルを採用するに当たっては、グローバル IP アドレスによるパケットの直接到達性や IPv4 通信プロトコルから IPv6 通信プロトコルへの移行過程における共存状態等、考慮すべき事項が多数ある。

近年では、サーバ装置、端末及び通信回線装置等に IPv6 技術を利用する通信（以下「IPv6 通信」という。）を行う機能が標準で備わっているものが多く出荷され、運用者が意図しない IPv6 通信が通信ネットワーク上で動作している可能性があり、結果として、不正アクセスの手口として悪用されるおそれもあることから、必要な対策を講じていく必要がある。

なお、IPv6 技術は今後も技術動向の変化が予想されるが、一方で、IPv6 技術の普及に伴い情報セキュリティ対策技術の進展も期待されることから、本学においても、IPv6 の情報セキュリティ対策に関する技術動向を十分に注視し、適切に対応していくことが重要である。

遵守事項

(1) IPv6 通信を行う情報システムに係る対策

(a) 部局技術責任者は､IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択すること。

(b) 部局技術責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

(ア) グローバル IP アドレスによる直接の到達性における脅威

(イ) IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

(ウ) IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

(エ) アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

(2) 意図しない IPv6 通信の抑止・監視

(a) 部局技術責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずること。

第 8 部　情報システムの利用

8.1　　情報システムの利用

8.1.1　　情報システムの利用

目的・趣旨

事務従事者は、業務の遂行のため、端末での事務処理のほか電子メール、ウェブ等様々な情報システムを利用している。これらを適切に利用しない場合、情報セキュリティインシデントを引き起こすおそれがある。

このため、情報システムの利用に関する規定を整備し、事務従事者は規定に従って利用することが求められる。

遵守事項

(1) 情報システムの利用に係る規定の整備

(a) 全学実施責任者は、本学の情報システムの利用のうち、情報セキュリティに関する規定を整備すること。

(b) 全学実施責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。

(c) 全学実施責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。

【 基本対策事項 】

(1)-1　全学実施責任者は、本学の情報システムの利用のうち、情報セキュリティに関する規定として、以下を例とする実施手順を定めること。

a) 情報システムの基本的な利用のうち、情報セキュリティに関する手順

b) 電子メール及びウェブの利用のうち、情報セキュリティに関する手順

c) 識別コードと主体認証情報の取扱手順

d) 暗号と電子署名の利用に関する手順

e) 不正プログラム感染防止の手順

f) アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為の防止に関する手順

g) ドメイン名の使用に関する手順

(1)-2　全学実施責任者は、要管理対策区域外にて情報処理を行う際の安全管理措置として、以下を例とする措置を規定し、事務従事者に遵守させること。

a) モバイル端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化

b) 盗み見に対する対策（のぞき見防止フィルタの利用等）
c) 盗難・紛失に対する対策（不要な情報をモバイル端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）
d) 利用する場所や時間の限定
e) 端末及び外部電磁的記録媒体等についての盗難・紛失が発生した際の緊急対応手順

(1)-3 全学実施責任者は、要管理対策区域外にて事務従事者が情報処理を行う際の許可等の手続として、以下を例とする手続を規定し、事務従事者に遵守させること。
a) 許可権限者の決定（部局技術責任者又は職場情報セキュリティ責任者が想定される。）
b) 利用時の許可申請手続
c) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線の接続形態等）
d) 利用期間満了時の手続
e) 許可権限者による手続内容の記録

(1)-4 全学実施責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順として以下の事項を含めて定めること。
a) 本学支給の外部電磁的記録媒体を使用する（私物や出所不明の媒体を使用しない）。
b) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。
c) 要機密情報は保存される必要がなくなった時点で速やかに削除する。
d) 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行う。

(2) 情報システム利用者の規定の遵守を支援するための対策

(a) 部局技術責任者は、事務従事者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。

【 基本対策事項 】

(2)-1 部局技術責任者は、学外のウェブサイトについて、事務従事者が閲覧できる範囲を制限する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。
a) ウェブサイトフィルタリング機能
b) 事業者が提供するウェブサイトフィルタリングサービスの利用

(2)-2 部局技術責任者は、事務従事者が不審なメールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。
a) 受信メールに対するフィルタリング機能
b) 受信メールをテキスト形式で表示する機能

c) スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがないメールクライアントの導入
d) 受信メールに添付されている実行プログラム形式のファイルを削除することで実行させない機能

(3) 情報システムの利用時の基本的対策
(a) 事務従事者は、高等教育機関の事務の遂行以外の目的で情報システムを利用しないこと。
(b) 事務従事者は、部局技術責任者が接続許可を与えた通信回線以外に本学の情報システムを接続しないこと。
(c) 事務従事者は、学内通信回線に、部局技術責任者の接続許可を受けていない情報システムを接続しないこと。
(d) 事務従事者は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、部局技術責任者の承認を得ること。
(e) 事務従事者は、接続が許可されていない機器等を情報システムに接続しないこと。
(f) 事務従事者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。
(g) 事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。
(h) 事務従事者は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、部局技術責任者又は職場情報セキュリティ責任者の許可を得ること。

【 基本対策事項 】
(3)-1 事務従事者は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下を例とする措置を講ずること。
a) スクリーンロックの設定
b) 利用後のログアウト徹底
c) 利用後に情報システムを鍵付き保管庫等に格納し施錠

(4) 電子メール・ウェブの利用時の対策
(a) 事務従事者は、要機密情報を含む電子メールを送受信する場合には、それぞれの高等教育機関が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。
(b) 事務従事者は、学外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名にA大学ドメイン名を使用すること。ただし、当該高等教育機関外の者にとって、当該事務従事者が既知の者である場合は除く。
(c) 事務従事者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に

従い、対処すること。

(d) 事務従事者は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。

(e) 事務従事者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

(f) 事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。

(ア) 送信内容が暗号化されること

(イ)当該ウェブサイトが送信先として想定している組織のものであること

(5) 識別コード・主体認証情報の取扱い

(a) 事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。

(b) 事務従事者は、自己に付与された識別コードを適切に管理すること。

(c) 事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。

(d) 事務従事者は、自己の主体認証情報の管理を徹底すること。

【 基本対策事項 】

(5)-1 事務従事者は、自己に付与された識別コードを適切に管理するため、以下を含む措置を講ずること。

a) 知る必要のない者に知られるような状態で放置しない。

b) 他者が主体認証に用いるために付与及び貸与しない。

c) 識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止する。

(5)-2 事務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。

a) 自己の主体認証情報を他者に知られないように管理する。

b) 自己の主体認証情報を他者に教えない。

c) 主体認証情報を忘却しないように努める。

d) 主体認証情報を設定するに際しては、容易に推測されないものにする。

e) 異なる識別コードに対して、共通の主体認証情報を用いない。

f) 異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない。（シングルサインオンの場合を除く。）

g) 部局技術責任者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更する。

(5)-3 事務従事者は、所有による主体認証情報を用いる場合には、以下の管理を徹底すること。

a) 主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する。

b) 主体認証情報格納装置を他者に付与及び貸与しない。
c) 主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する。
d) 主体認証情報格納装置を利用する必要がなくなった場合には、これを部局技術責任者に返還する。

(6) 暗号・電子署名の利用時の対策
(a) 事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。
(b) 事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。
(c) 事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

(7) 不正プログラム感染防止
(a) 事務従事者は、不正プログラム感染防止に関する措置に努めること。
(b) 事務従事者は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずること。

【 基本対策事項 】

(7)-1 事務従事者は、不正プログラム対策ソフトウェアを活用し、不正プログラム感染を回避するための以下措置に努めること。
a) 不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しない。また、検知されたデータファイルをアプリケーション等で読み込まない。
b) 不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持する。
c) 不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にする。
d) 不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施する。

(7)-2 事務従事者は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

(7)-3 事務従事者は、不正プログラムに感染するリスクを低減する情報システムの利用方法として、以下のうち実施可能な措置を講ずること。
a) 不審なウェブサイトを閲覧しない。
b) アプリケーションの利用において、マクロ等の自動実行機能を無効にする。

c) プログラム及びスクリプトの実行機能を無効にする。
d) 安全性が確実でないプログラムをダウンロードしたり実行したりしない。

8.2 本学支給以外の端末の利用

8.2.1 本学支給以外の端末の利用

目的・趣旨

高等教育機関の事務の遂行においては、本学から支給された端末を用いて高等教育機関の事務を遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず本学支給以外の端末を利用して情報処理を行う必要が生じる場合がある。この際、当該端末は本学が支給したものではないという理由で、事務従事者へ情報セキュリティ対策の実施を求めなかった場合、当該端末で取り扱われる情報セキュリティ水準が、事務情報セキュリティ対策基準を満たさないおそれがある。

したがって、そのような可能性がある場合は、本学支給以外の端末を事務従事者が安全に利用するための手続や安全管理措置の規定をあらかじめ整備し、本学における厳格な管理の下で利用させることが必要である。

また、本学支給以外の端末であっても、本学から支給されるモバイル端末と同等の情報セキュリティ水準の確保が求められることから、7.1.1 項「端末」も参照し、同等の安全管理が実施されるよう、規定を整備し、事務従事者に安全管理措置を講じさせる必要がある。

遵守事項

(1) 本学支給以外の端末の利用規定の整備・管理

(a) 全学実施責任者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。

(b) 全学実施責任者は、要機密情報について本学支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。

(c) 部局総括責任者は、本学支給以外の端末による高等教育機関の事務に係る情報処理に関する安全管理措置の実施状況を管理する責任者を定めること。

(d) 前号で定める責任者は、要機密情報を取り扱う本学支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、事務従事者に適切に安全管理措置を講じさせること。

【 基本対策事項 】

(1)-1 全学実施責任者は、以下を例に本学支給以外の端末を利用する際の許可等の手続に関する手順を整備し、事務従事者に周知すること。

a）以下を含む本学支給以外の端末利用時の申請内容

- 申請者の氏名、所属、連絡先
- 利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）
- 利用する端末の機種名

- 利用目的、取り扱う情報の概要、機密性３情報の利用の有無等
- 主要な利用場所
- 利用する主要な通信回線サービス
- 利用する期間

b) 利用許諾条件
c) 申請手順
d) 利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順
e) 利用期間満了時の利用終了又は利用期間更新の手続方法
f) 許可権限者（遵守事項 8.2.1(1)(c)において定める、本学支給以外の端末の安全管理措置の実施状況を管理する責任者（以下、この項において「端末管理責任者」という。））

(1)-2 全学実施責任者は、本学支給以外の端末により要機密情報を取り扱う場合は、事務従事者が講ずるべき安全管理措置の実施手順について、以下を例に整備すること。

a) パスワード等による端末ロックの常時設定
b) OS やアプリケーションの最新化
c) 不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（本学として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）
d) 遠隔データ消去機能の設定
e) 要機密情報の暗号化等による秘匿性の確保
f) 端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）
g) 本学提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）
h) 以下を例とする禁止事項の遵守

- 端末、OS、アプリケーション等の改造行為
- 安全性が確認できないアプリケーションのインストール及び利用
- 利用が禁止されているソフトウェアのインストール及び利用
- 許可されない通信回線サービスの利用（利用する回線を限定する場合）
- 第三者への端末の貸与

(1)-3 部局技術責任者は、本学支給以外の端末により要機密情報を取り扱う本学の情報システムにリモートアクセスする環境を構築する場合、基盤となる情報システムにより各高等教育機関に提供されるリモートアクセス環境が利用可能であれば活用し、端末の盗難・紛失や不正プログラム感染等により情報窃取されることを防止するために、以下を例とする対策を講ずること。

a) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。
b) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システム

へリモートアクセスする。

c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。利用者は専用のアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。

(2) 本学支給以外の端末の利用時の対策

(a) 事務従事者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合には、遵守事項 8.2.1(1)(c)で定める責任者の許可を得ること。

(b) 事務従事者は、要機密情報を本学支給以外の端末で取り扱う場合は、職場情報セキュリティ責任者の許可を得ること。

(c) 事務従事者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合には、本学にて定められた手続及び安全管理措置に関する規定に従うこと。

(d) 事務従事者は、情報処理の目的を完了した場合は、要機密情報を本学支給以外の端末から消去すること。

C2502 事務情報セキュリティ対策基準策定のためのガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2015年10月9日 C2502	統一基準（平成26年度版）に対応した「府省庁対策基準策定のためのガイドライン」をもとに新規作成	高等教育機関における情報セキュリティポリシー推進部会事務局
2017年10月17日 C2502	統一基準群（平成28年度版）をもとに改定	高等教育機関における情報セキュリティポリシー推進部会事務局

（注）統一基準＝政府機関の情報セキュリティ対策のための統一基準

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

目次

第1部 総則

1.1 目的

事務情報セキュリティ対策基準策定のためのガイドライン（以下「本ガイドライン」という。）は、本学が政府機関の情報セキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定　以下「統一基準」という。）に準拠して C2501 事務情報セキュリティ対策基準を策定する際に参照するものであり、事務情報セキュリティ対策基準の策定手順や統一基準の遵守事項を満たすために採られるべき基本的な対策事項（以下「基本対策事項」という。）の例示、考え方等を解説することを目的としている。

1.2 事務情報セキュリティ対策基準の策定手順

本学では、C1000 情報システム基本運用方針に基づき、統一基準に定める基本原則である遵守事項等の規定を満たすよう、具体的な対策事項を事務情報セキュリティ対策基準に規定する必要がある。本ガイドラインには、本学が事務情報セキュリティ対策基準を策定する際に参照するための基本対策事項を例示し、考え方等を解説として示している。

本学における組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性によって、達成すべき情報セキュリティの水準や採るべき対策は異なるため、事務情報セキュリティ対策基準の策定に当たっては、本ガイドラインの基本対策事項をそのまま適用するのではなく、自らの組織が如何なる手段を採れば情報セキュリティが最も適切に確保されるのかとの視点から、上記に掲げた本学の特性等を勘案しつつ、これに適した対策を検討し、基準に定める必要がある。

なお、事務情報セキュリティ対策基準の構成としては、統一基準と本ガイドラインの関係と同様に、遵守事項と対策事項を分けて記載する方法や、対策事項のみを記載する方法等、本学における状況に応じてよりよい構成とすることが望ましい。

1.3 本ガイドラインの改訂

情報セキュリティの水準を適切に維持していくためには、脅威の変化や技術の進展を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。

このため、本ガイドラインの規定内容については、環境の変化に応じて適宜内容の見直しを行い、必要に応じて項目の追加やその内容の充実等を図ることによって、規定内容の適正性を将来にわたり維持することとする。

本学においては、本ガイドラインが更新された場合には、その内容を事務情報セキュリティ対策基準に適切に反映させることが期待される。

1.4 統一基準、本ガイドライン及び実施手順の関係

政府機関の情報セキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定。以下「統一規範」という。）、政府機関等の情報セキュリティ対策の運用等に関する指針（サイバーセキュリティ戦略本部決定。以下「運用指針」という。）及び統一基準と本ガイドラインの関係は図 1.4-1 のとおりであり、これらを総称して、政府機関の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）と呼ぶ。また、統一基準群と本学の情報セキュリティポリシーの関係についても、併せて図 1.4-1 に示す。

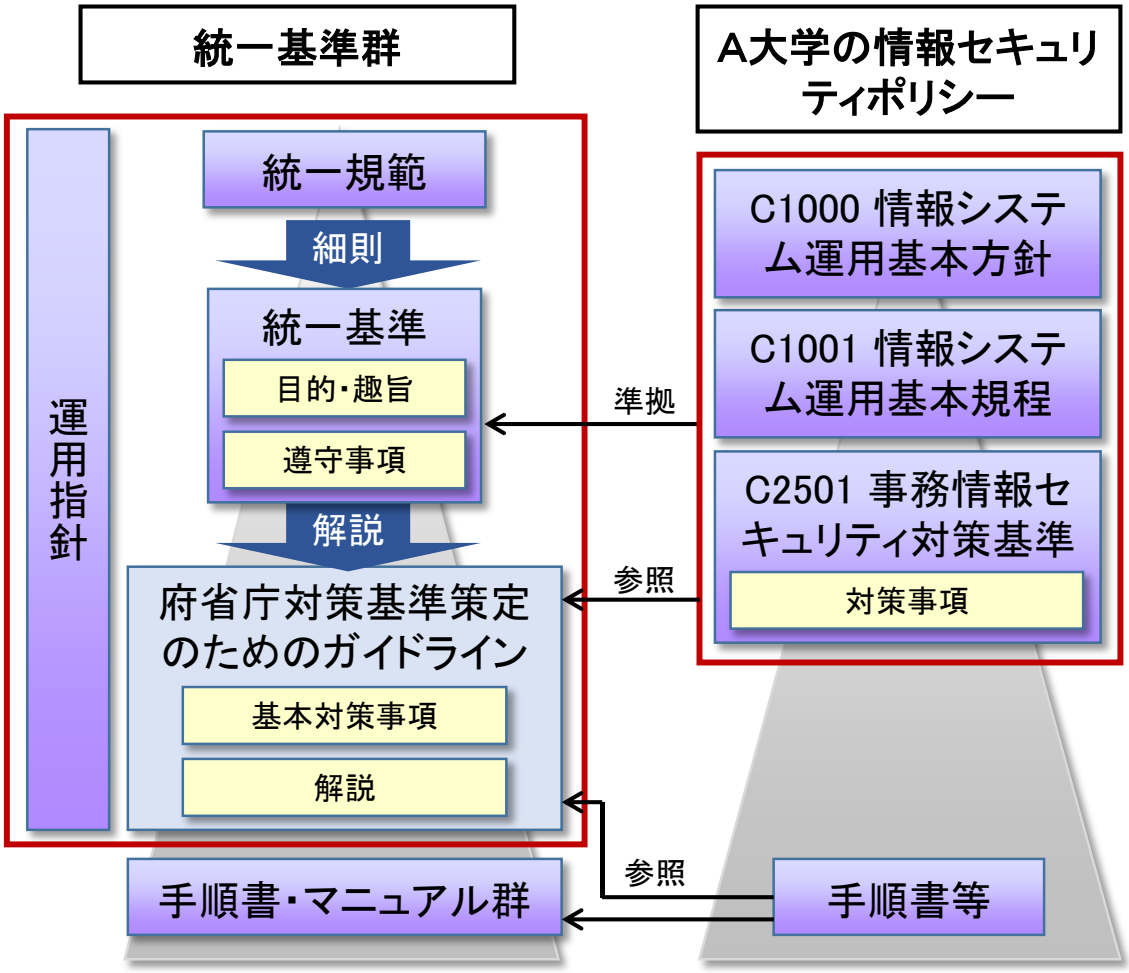


図 1.4-1 統一基準群と本学の情報セキュリティポリシーの関係について

1.5　統一基準で定義されている用語

統一基準 1.2 項において定義されている情報の格付の区分・取扱制限、1.3 項において定義されている用語について、本学における運用に適した形で読み替えたものを以下に掲載する。

(1) 情報の格付の区分

情報について、機密性、完全性及び可用性の３つの観点を区別し、本基準の遵守事項で用いる格付の区分の定義を示す。

本学において格付の定義を変更又は追加する場合には、それぞれの高等教育機関の対策基準における格付区分と遵守事項との関係が本基準での関係と同等以上となるように準拠しなければならない。また、他本学へ情報を提供する場合は、自身の格付区分と本基準における格付区分の対応について、適切に伝達する必要がある。

機密性についての格付の定義

格付けの区分	分類の基準
機密性３情報	本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年4月1日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	本学で取り扱う情報のうち、独立行政法人の保有する情報の公開に関する法律（平成13年12月5日法律第140号。以下、「独立行政法人等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
機密性１情報	独立行政法人等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

完全性についての格付の定義

格付けの区分	分類の基準
完全性２情報	本学で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）

	を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

なお、完全性２情報を「要保全情報」という。

可用性についての格付の定義

格付けの区分	分類の基準
可用性２情報	本学で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。

また、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」という。

(2) 情報の取扱制限

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを行政事務従事者に確実に行わせるための手段をいう。

事務従事者は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。本学では、取り扱う情報について、機密性、完全性及び可用性の３つの観点から、取扱制限に関する基本的な定義を定める必要がある。

【参考】 取扱制限の例

取扱制限は、情報の機密性、完全性、可用性等の内容に応じた情報の取扱い方を具体的に指定するものであるから、「情報の作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させる」という目的を果たすために適切に明示等する必要がある。以下の例のように、代表的な取扱制限を指定してもよい。例えば「複製禁止」の代わりに「複写禁止」や「複製厳禁」、「複製を禁ず」等と記載しても目的を果たせると考えられる。

○ 機密性についての取扱制限の定義の例

表 3.1.1-1　機密性についての取扱制限の定義の例

取扱制限の種類	指定方法
複製について	複製禁止、複製要許可
配布について	配布禁止、配布要許可
暗号化について	暗号化必須、保存時暗号化必須、通信時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り
期限について	○月○日まで○○禁止

上記の指定方法の意味は以下のとおり。

・「○○禁止」
　当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。
・「○○要許可」
　当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。
・「暗号化必須」
　当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」等、情報を取り扱う者が分かるように指定する。
・「○○限り」
　当該情報について、参照先を○○に記載した者のみに制限する必要がある場合に指定する。例えば、「セキュリティセンター限り」「政策会議委員会出席者限り」等、参照を許可する者が分かるように指定する。
・「○月○日まで○○禁止」
　例えば、○月○日まで複製を禁止したい場合、「○月○日まで複製禁止」として期限を指定することで、その日に取扱制限を変更しないような指定でも構わない。

例えば、上記の「○○要許可」は、「○○する行為を禁止するが、許可を得ることにより○○することができる」という意味を持たせている。取扱制限は、このように、事務従事者にとって簡便かつ分かりやすい表現を採用することが望ましい。

○ 完全性についての取扱制限の定義の例

表 3.1.1-2　完全性についての取扱制限の定義の例

取扱制限の種類	指定方法
保存期間について	○○まで保存
保存場所について	○○において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

情報の保存期間の指定の方法は、以下のとおり。

・保存の期日である「年月日」又は期日に「まで保存」を付して指定する。

例）平成○○年 7 月 31 日まで保存

例）平成○○年度末まで保存

・完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。

例）年度内保存文書用共有ファイルサーバに保存

例）3 カ年保存文書用共有ファイルサーバに保存

○ 可用性についての取扱制限の定義の例

表 3.1.1-3　可用性についての取扱制限の定義の例

取扱制限の種類	指定方法
復旧までに許容できる時間について	○○以内復旧
保存場所について	○○において保存

復旧許容時間の指定の方法は以下のとおり。

・復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。

例）1 時間以内復旧

例）3 日以内復旧

・可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用においては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、端末のファイルについては定期的にバックアップが実施されておらず、課室共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。

例）課室共有ファイルサーバ保存必須

例）各自 PC 保存可

(3) 事務情報セキュリティ対策基準 1.3 項「用語定義」において定義されている用語

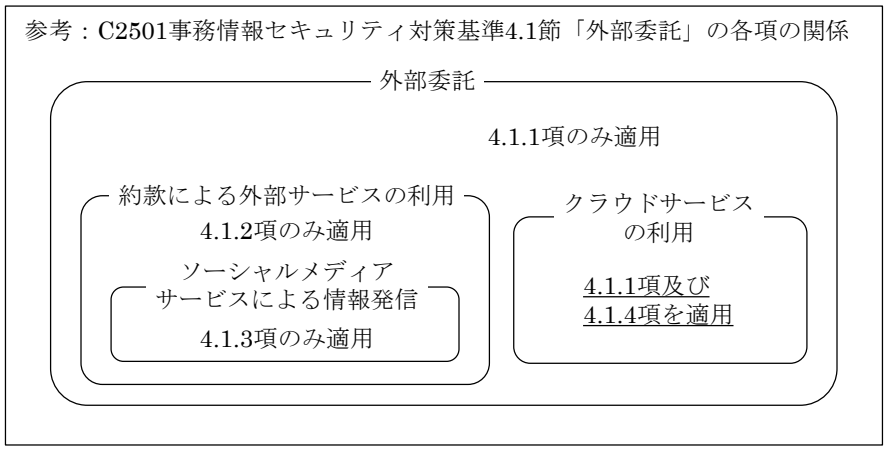
【あ】

● 「アプリケーション・コンテンツ」とは、アプリケーションプログラム、ウェブコンテンツ等の総称をいう。

● 「委託先」とは、外部委託により本学の情報処理業務の一部又は全部を実施する者をいう。

【か】

● 「外部委託」とは、本学の情報処理業務の一部又は全部について、契約をもって学外の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。



● 「学外通信回線」とは、通信回線のうち、学内通信回線以外のものをいう。

● 「学内通信回線」とは、一つの本学が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該高等教育機関の管理下にないサーバ装 F 置又は端末が論理的に接続されていないものをいう。学内通信回線には、専用線や VPN 等物理的な回線を本学が管理していないものも含まれる。

● 「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。（参考：図 1.5-1）

● 「基盤となる情報システム」とは、他の機関と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。

● 「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認

識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。

● 「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

> 参考：ISO/IEC 17788 におけるクラウドサービスの定義
> ・cloud service
> One or more capabilities offered via cloud computing invoked using a defined interface
>
> ・cloud computing
> Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
>
> NOTE - Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

● 「クラウドサービス事業者」とは、クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・運用する事業者をいう。

【さ】

● 「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。

● 「CSIRT（シーサート）」とは、本学において発生した情報セキュリティインシデントに対処するために設置された体制をいう。Computer Security Incident Response Team の略。

● 「実施手順」とは、事務情報セキュリティ対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。

● 「事務従事者」とは、本学の事務に従事している本学の指揮命令に服している者であって、本学の管理対象である情報及び情報システムを取り扱う者をいう。事務従事者に

は、個々の勤務条件にもよるが、例えば、派遣労働者等も含まれている。

● 「事務情報セキュリティ対策基準」とは、本学における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。

● 「情報」とは、統一基準の「1.1(2) 本統一基準の適用範囲」の(b)に定めるものをいう。（参考：図 1.5-2）

参考：統一基準の「1.1(2) 本統一基準の適用範囲」（抄）

(b) 本統一基準において適用範囲とする情報は、以下の情報とする。

(ア) 事務従事者が職務上使用することを目的 として本学が調達し、又は開発した情報システム若しくは 外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

(イ) その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、事務従事者が職務上取り扱う情報

(ウ) （ア）及び（イ）のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報

● 「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理及び通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。（参考：図 1.5-1）

参考：統一基準の「1.1(2) 本統一基準の適用範囲」（抄）

(c) 本統一基準において適用範囲とする情報システムは、本統一基準の適用範囲となる情報を取り扱う全ての情報システムとする。

● 「情報セキュリティインシデント」とは、JIS Q 27000:2014 における情報セキュリティインシデントをいう。

参考：JIS Q 27000:2014（抄）

・情報セキュリティインシデント
望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。

・情報セキュリティ事象
情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

● 「情報セキュリティ関係規程」とは、事務情報セキュリティ対策基準及び実施手順を総称したものをいう。

● 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

【た】

● 「端末」とは、情報システムの構成要素である機器のうち、事務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。

● 「通信回線」とは、複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

● 「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

● 「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。

【は】

● 「不正プログラム」とは、コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

【ま】

● 「抹消」→「情報の抹消」を参照。

● 「明示等」とは、情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

● 「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

● 「約款による外部サービス」とは、民間事業者等の学外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

● 「要管理対策区域」とは、本学が管理する施設等（外部の組織から借用している施設等を含む。）本学の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。

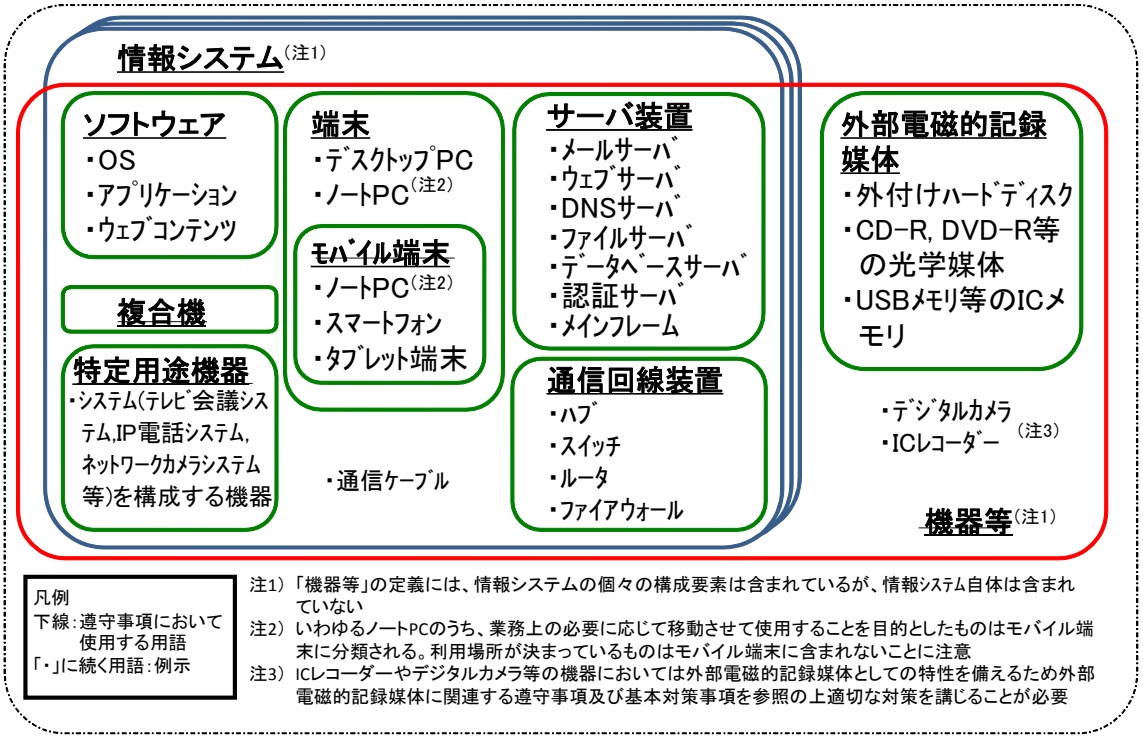


図 1.5-1 「情報システム」、「機器等」及びその関係

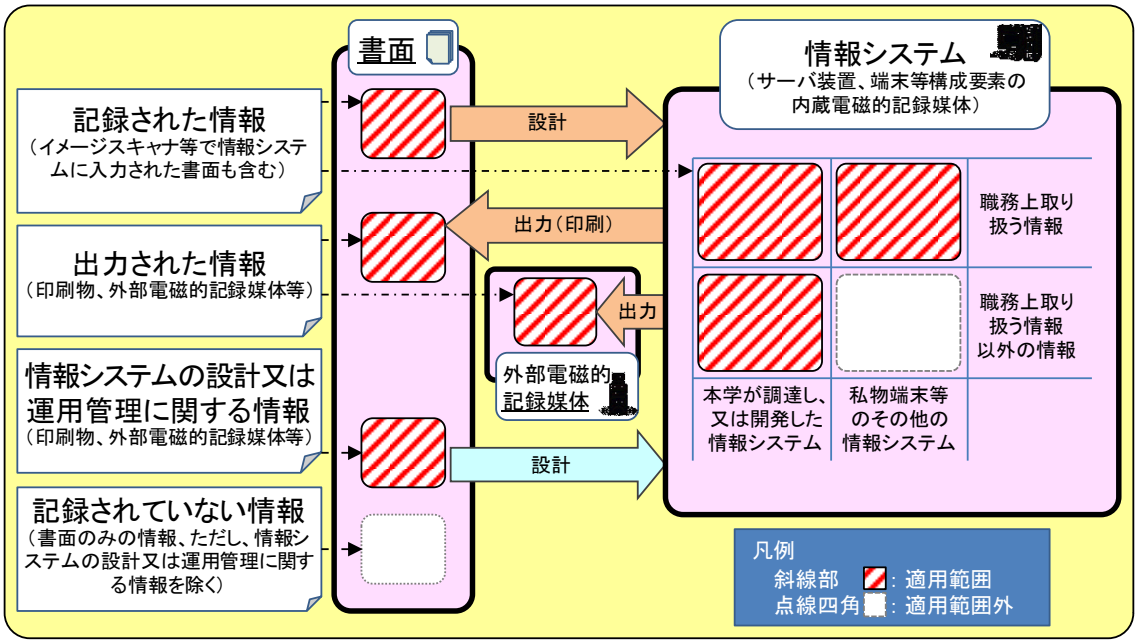


図 1.5-2　統一基準の適用を受ける「情報」の範囲

1.6　一般用語の解説

留意すべき一般用語を以下に解説する。

【あ】

● 「アクセス制御」とは、情報又は情報システムへのアクセスを許可する主体を制限することをいう。

● 「アプリケーション」とは、OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。

● 「アルゴリズム」とは、ある特定の目的を達成するための演算手順をいう。

● 「暗号化」とは、第三者に容易に解読されないよう、定められた演算を施しデータを変換することをいう。

● 「暗号モジュール」とは、暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。

● 「ウェブクライアント」とは、ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。

【か】

● 「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。

● 「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。

● 「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。

● 「業務継続計画」とは、本学において策定されている BCP（Business Continuity Plan: 事業継続計画）をいう。

● 「共用識別コード」とは、複数の主体が共用するために付与された識別コードをいう。原則として、一つの識別コードは一つの主体のみに対して付与されるものであるが、情報システム上の制約や利用状況等に応じて、識別コードを組織で共用する場合もある。このように共用される識別コードを共用識別コードという。

● 「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

【さ】

● 「サービス不能攻撃」とは、悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサ

ーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。

● 「最小限の特権機能」とは、管理者権限を実行できる範囲を必要最小限に制限する機能をいう。

● 「識別」とは、情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。

● 「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。

● 「主体」とは、情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。

● 「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。

● 「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

● 「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、IC カード等がある。

● 「セキュリティパッチ」とは、発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。

● 「ソフトウェア」とは、サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OS や OS 上で動作するアプリケーションを含む広義の意味である。

【た】

● 「耐タンパ性」とは、暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。

● 「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。

● 「電子メールクライアント」とは、電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。

● 「電子メールサーバ」とは、電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。

● 「ドメインネームシステム（DNS)」とは、クライアント等からの問合わせを受けて、ドメイン名やホスト名とIPアドレスとの対応関係について回答を行うシステムである。

● 「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.sample.ac.jp というウェブサイトの場合は、sample.ac.jp の部分がこれに該当する。

【な】

● 「名前解決」とは、ドメイン名やホスト名とIPアドレスを変換することをいう。

【は】

● 「不正プログラム定義ファイル」とは、不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。

● 「複合機」とは、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。

● 「踏み台」とは、悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。

【ま】

● 「無線 LAN」とは、IEEE802.11a、802.11b、802.11g、802.11n 等の規格により、無線通信で情報を送受信する通信回線をいう。

【ら】

● 「リスク」とは、目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。

● 「ルートヒントファイル」とは、最初に名前解決を問合わせる DNS コンテンツサーバ（以下「ルート DNS」という。）の情報をいう。ルートヒントファイルには、ルート DNS のサーバ名とIPアドレスの組が記載されており、ルート DNS の IP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC（Internet Network Information Center）のサイトから入手可能である。

【A～Z】

● 「BCP（Business Continuity Plan: 事業継続計画)」とは、組織において特定する事業の継続に支障をきたすと想定される自然災害、人的災害・事故、機器の障害等の事態

に組織が適切に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。狭義には、このうちの事態発生後の事業の維持を主とした計画をいう。

- 「CRYPTREC（Cryptography Research and Evaluation Committees）」とは、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。

- 「DNS サーバ」とは、名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させるサーバ装置をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の二種類に分けることができる。

- 「IPv6 移行機構」とは、物理的に一つのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、サーバ装置及び端末並びに通信回線装置が二つの通信プロトコルを併用するデュアルスタック機構や、相互接続性の無い二つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。

- 「MAC アドレス（Media Access Control address）」とは、機器等が備える有線 LAN や無線 LAN のネットワークインタフェースに割り当てられる固有の認識番号である。識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割り当てる番号の組み合わせによって表される。

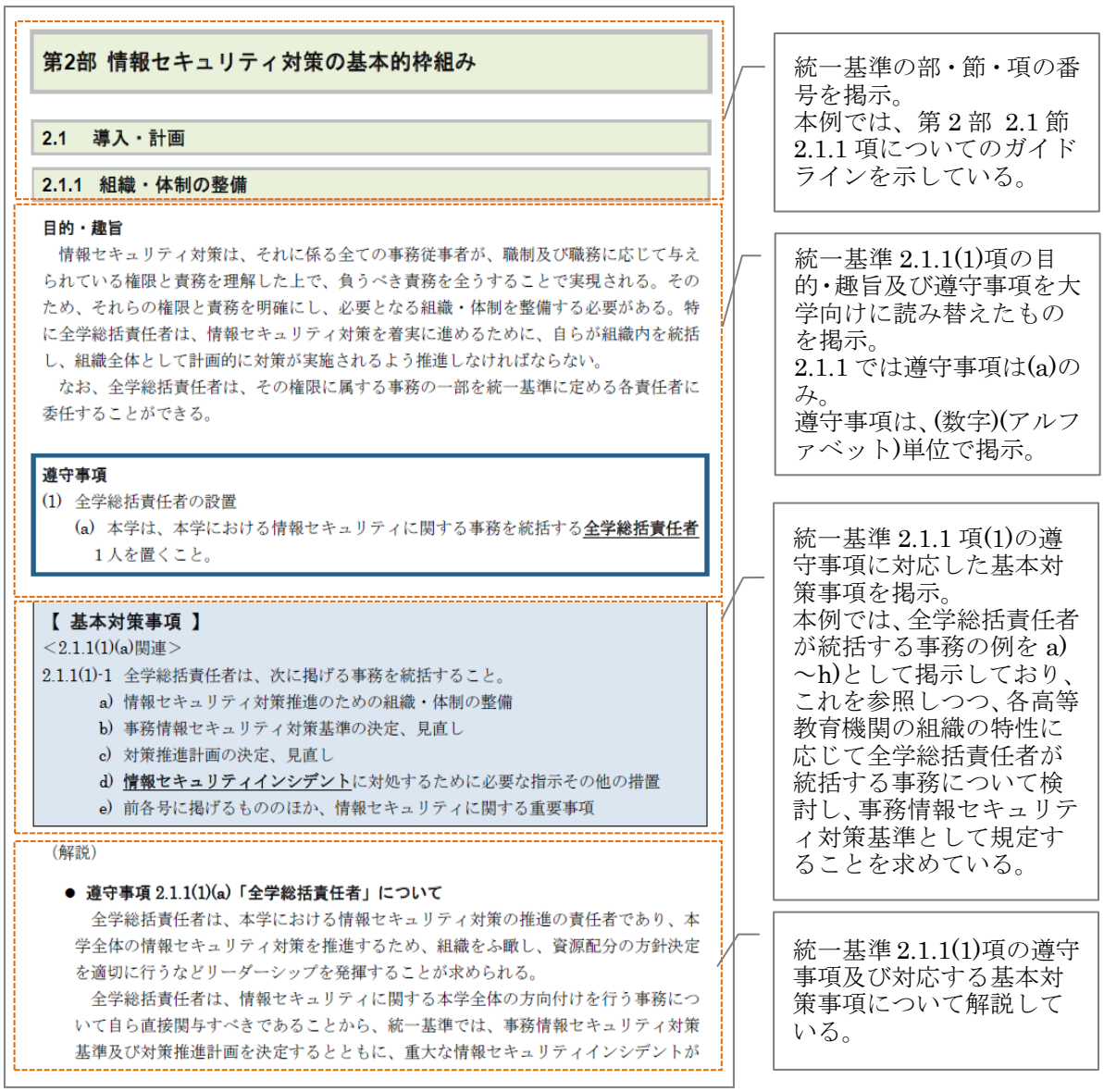
- 「S/MIME（Secure Multipurpose Internet Mail Extensions）」とは、公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。

- 「VPN（Virtual Private Network）」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。

1.7　基本対策事項及び解説の読み方

本ガイドラインの第２部以降に記述する遵守事項に対応した基本対策事項及び解説を参照するに当たり、留意すべき点を以下に示す。

◆第２部以降の基本的な記述構成



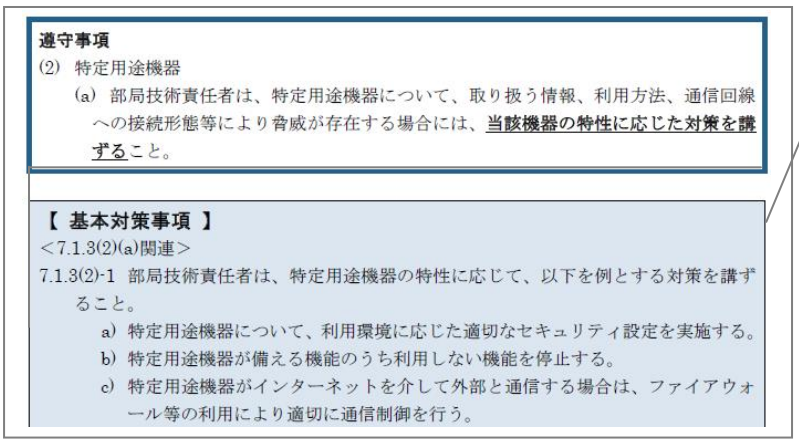
統一基準の部・節・項の番号を掲示。
本例では、第 2 部 2.1 節 2.1.1 項についてのガイドラインを示している。

統一基準 2.1.1(1)項の目的・趣旨及び遵守事項を大学向けに読み替えたものを掲示。
2.1.1 では遵守事項は(a)のみ。
遵守事項は、(数字)(アルファベット)単位で掲示。

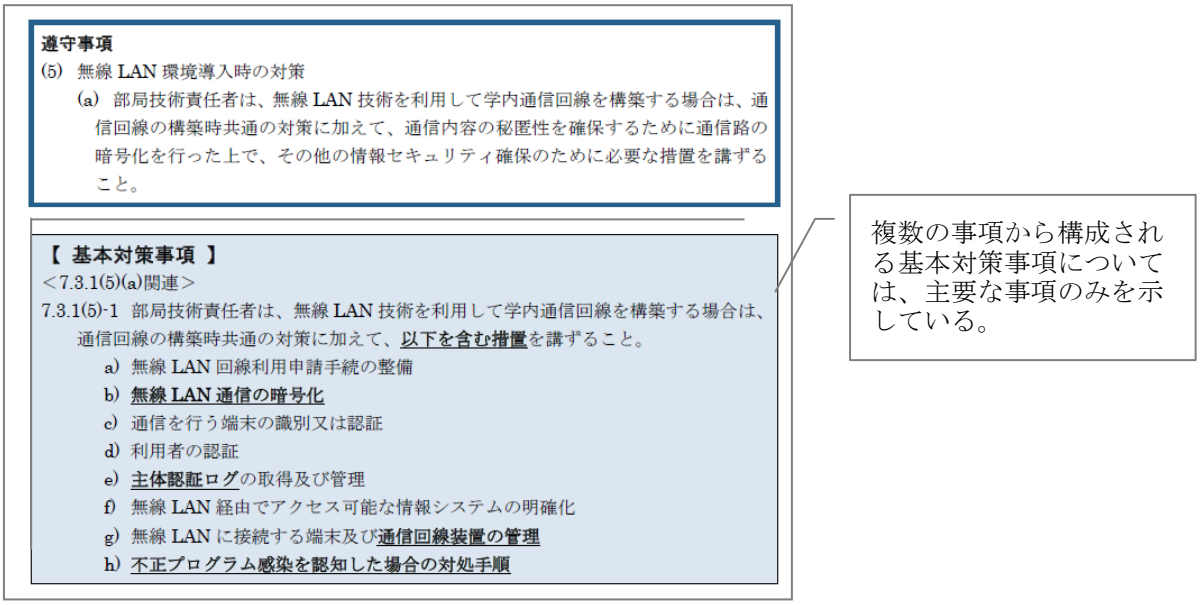
統一基準 2.1.1 項(1)の遵守事項に対応した基本対策事項を掲示。
本例では、全学総括責任者が統括する事務の例を a)～h)として掲示しており、これを参照しつつ、各高等教育機関の組織の特性に応じて全学総括責任者が統括する事務について検討し、事務情報セキュリティ対策基準として規定することを求めている。

統一基準 2.1.1(1)項の遵守事項及び対応する基本対策事項について解説している。

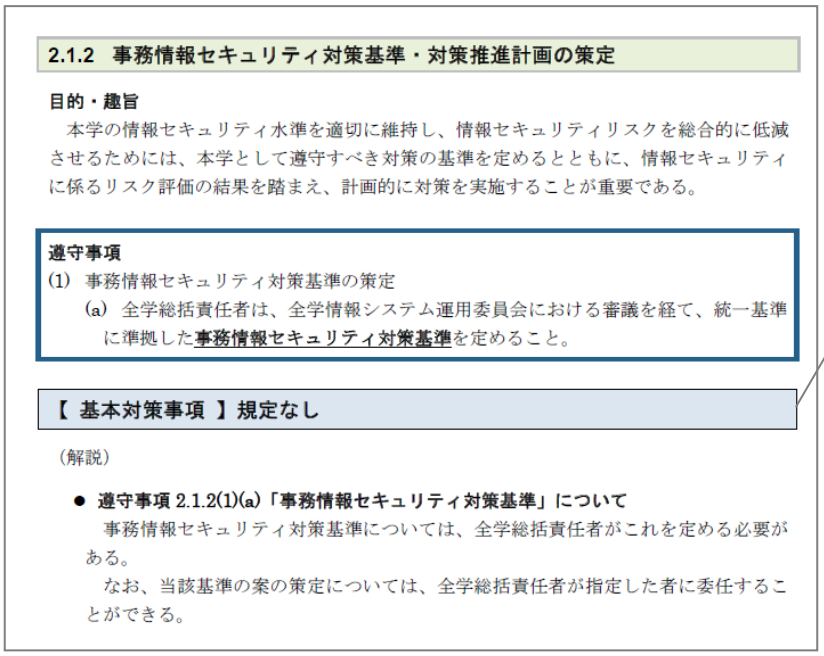
◆基本対策事項に個別対策事項が例示されている場合



◆基本対策事項の個別対策事項について、“～を含む”として例示されている場合



◆基本対策事項が規定されていない場合



2.1.2　事務情報セキュリティ対策基準・対策推進計画の策定

目的・趣旨

本学の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、本学として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果を踏まえ、計画的に対策を実施することが重要である。

遵守事項

(1)　事務情報セキュリティ対策基準の策定

(a)　全学総括責任者は、全学情報システム運用委員会における審議を経て、統一基準に準拠した**事務情報セキュリティ対策基準**を定めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.2(1)(a)「事務情報セキュリティ対策基準」について**

事務情報セキュリティ対策基準については、全学総括責任者がこれを定める必要がある。

なお、当該基準の案の策定については、全学総括責任者が指定した者に委任することができる。

遵守事項が具体的な対策事項となっている場合は、基本対策事項を定めていない。
この場合は、遵守事項の解説を参照し、事務情報セキュリティ対策基準を定めることになる。

第2部 情報セキュリティ対策の基本的枠組み

2.1 導入・計画

2.1.1 組織・体制の整備

目的・趣旨

情報セキュリティ対策は、それに係る全ての事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。特に全学総括責任者は、情報セキュリティ対策を着実に進めるために、自らが組織内を統括し、組織全体として計画的に対策が実施されるよう推進しなければならない。

なお、全学総括責任者は、その権限に属する事務の一部を本基準に定める責任者等に担わせることができる。

遵守事項

(1) 全学総括責任者の設置

(a) 本学は、本学における情報セキュリティに関する事務を統括する全学総括責任者１人を置くこと。

【 基本対策事項 】

＜2.1.1(1)(a)関連＞

2.1.1(1)-1 全学総括責任者は、次に掲げる事務を統括すること。

a) 情報セキュリティ対策推進のための組織・体制の整備
b) 事務情報セキュリティ対策基準の決定、見直し
c) 対策推進計画の決定、見直し
d) 情報セキュリティインシデントに対処するために必要な指示その他の措置
e) 前各号に掲げるもののほか、情報セキュリティに関する重要事項

（解説）

- **遵守事項 2.1.1(1)(a)「全学総括責任者」について**

全学総括責任者は、本学における情報セキュリティ対策の推進の責任者であり、本学全体の情報セキュリティ対策を推進するため、組織をふ瞰し、資源配分の方針決定を適切に行うなどリーダーシップを発揮することが求められる。なお、その際には、国内外の情報セキュリティに関連する動向を注視するとともに、有益な最新の技術の活用を検討するなど、先手を打って必要な対策をとることが重要である。

全学総括責任者は、情報セキュリティに関する本学全体の方向付けを行う事務について自ら直接関与すべきであることから、事務情報セキュリティ対策基準及び対策推

進計画を決定するとともに、重大な情報セキュリティインシデントが発生した場合には、それに対処するための必要な指示その他の措置を行うこととしている。

- **基本対策事項 2.1.1(1)-1 d)「情報セキュリティインシデント」について**

  情報セキュリティインシデントについては、統一基準 1.3 項「用語の定義」（本ガイドライン 1.5 項「統一基準で定義されている用語」）に示すとおりであるが、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものとして、実際に業務等への影響は顕在化していないものの、そのおそれがある場合を含むことに留意する必要がある。情報システムに関する情報セキュリティインシデントとしては、例えば、以下が考えられる。

  - 要機密情報が含まれる内容の電子メールの外部への誤送信
  - 要機密情報が格納された USB メモリを紛失
  - 不正プログラムへの感染
  - 外部からのサーバ装置、端末への不正侵入
  - サービス不能攻撃等による情報システムの停止

遵守事項

(2) 全学情報システム運用委員会の設置

(a) 全学総括責任者は、事務情報セキュリティ対策基準等の審議を行う機能を持つ組織として、本学の情報セキュリティを推進する部局及びその他高等教育機関の事務を実施する部局の代表者を構成員とする全学情報システム運用委員会を置くこと。

【 基本対策事項 】

＜2.1.1(2)(a)関連＞

2.1.1(2)-1 全学情報システム運用委員会の委員長及び委員は、全学総括責任者が情報セキュリティを推進する部局及びその他の高等教育機関の事務を実施する部局の代表者から指名すること。

2.1.1(2)-2 全学情報システム運用委員会は、次に掲げる事項を審議すること。

a) 事務情報セキュリティ対策基準

b) 対策推進計画

c) 前各号に掲げるもののほか、情報セキュリティに関し必要な事項

（解説）

- **遵守事項 2.1.1(2)(a)「全学情報システム運用委員会」について**

全学総括責任者は、横断的な事項を審議するため、情報セキュリティを推進する部門及び各部局（部門）の代表者から構成される委員会を設置する。委員長及び委員は、全学総括責任者の指名によるが、全学総括責任者自らが委員長を兼ねてもよい。

委員会は、各部門間の意見調整を図り情報セキュリティ対策と組織の方針を整合的なものとするため、組織全体としての方向付けを要する事務情報セキュリティ対策基準及び対策推進計画について審議する。

なお、審議事項については、本学の実態に応じて柔軟に運用することが考えられる。さらに、委員会の配下に実務を担当する下位委員会を設置する、既存の情報システム管理部門に情報セキュリティ対策の運用を統括する機能を持たせるなど、部門の横断的な連携の仕組みを確立させることも考えられる。

遵守事項

(3) 情報セキュリティ監査責任者の設置

(a) 全学総括責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くこと。

【 基本対策事項 】

＜2.1.1(3)(a)関連＞

2.1.1(3)-1 情報セキュリティ監査責任者は、命により次の事務を統括すること。

a) 監査実施計画の策定

b) 監査実施体制の整備

c) 監査の実施指示及び監査結果の全学総括責任者への報告

d) 前各号に掲げるもののほか、情報セキュリティの監査に関する事項

（解説）

- **遵守事項 2.1.1(3)(a)「情報セキュリティ監査責任者」について**

本学における情報セキュリティ対策は、全学総括責任者の指揮の下で推進することとなるが、全学総括責任者は、自らが決定した情報セキュリティ対策が適切に実施されているか否かを正しく把握する必要がある。そのため、全学総括責任者は、情報セキュリティ監査責任者にその実施状況等の確認を行わせることにより、情報セキュリティ対策の実効性を確保しようとするものである。

なお、情報セキュリティ監査責任者は、組織のまとまりごとの情報セキュリティに関する事務を担う部局総括責任者よりも職務上の上位の者を置くことが望ましい。

情報セキュリティ監査責任者は、情報セキュリティ対策が適切に実施されているか否かを監査し、その結果について全学総括責任者に的確に報告しなければならない。

情報セキュリティ監査責任者は、これら監査事務を効率的に実施するため、担当者（監査実施者）を置き、必要に応じて外部組織を活用するなど、監査実施体制の整備を行う。

なお、本学の実情に応じて、監査責任者を補佐する立場として監査副責任者を独自に設置してよい。

遵守事項

(4) 全学実施責任者・部局総括責任者等の設置

(a) 全学総括責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、**部局総括責任者**１人を置くこと。そのうち、部局総括責任者を統括し、全学総括責任者を補佐する者として、**全学実施責任者**１人を選任すること。

(b) 部局総括責任者は、遵守事項 3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する**区域情報セキュリティ責任者** 1 人を置くこと。

(c) 部局総括責任者は、課室ごとに情報セキュリティ対策に関する事務を統括する**職場情報セキュリティ責任者**１人を置くこと。

(d) 部局総括責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、**部局技術責任者**を、当該情報システムの企画に着手するまでに選任すること。

【 基本対策事項 】

＜2.1.1(4)(a)関連＞

2.1.1(4)-1 全学実施責任者は、命を受け、次の事務を統括すること。

a) 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定

b) 情報セキュリティ対策に関する**実施手順**の整備及び見直し並びに実施手順に関する事務のとりまとめ

c) 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備

d) 例外措置の適用審査記録の台帳整備等

e) 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等

f) 前各号に掲げるもののほか、情報セキュリティ対策に係る事務

2.1.1(4)-2 部局総括責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括すること。

a) 定められた区域ごとの区域情報セキュリティ責任者の設置

b) 課室の職場情報セキュリティ責任者の設置

c) 情報システムごとの部局技術責任者の設置

d) 情報セキュリティインシデントの原因調査、再発防止策等の実施

e) 情報セキュリティに係る自己点検計画の策定及び実施手順の整備

f) 前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務

＜2.1.1(4)(b)関連＞

2.1.1(4)-3 区域情報セキュリティ責任者は、命を受け、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を統括すること。

＜2.1.1(4)(c)関連＞

2.1.1(4)-4 職場情報セキュリティ責任者は、命を受け、課室における情報の取扱いその他

の情報セキュリティ対策に関する事務を統括すること。
＜2.1.1(4)(d)関連＞
2.1.1(4)-5 部局技術責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。
2.1.1(4)-6 部局技術責任者は、所管する情報システムの管理業務において必要な単位ごとに部局技術担当者を置くこと。

（解説）

- **遵守事項 2.1.1(4)(a)「部局総括責任者」について**

全学総括責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能となる組織のまとまりごとに、その対策を委ねた方が効率的であることから、取りまとめの責任者として、部局総括責任者を設置する。情報セキュリティ対策の運用が可能なまとまりとしては、部局（内局、外局、地方支分局、附属機関）ごとが想定される。

部局総括責任者は、全学総括責任者の委任に基づき、所管する組織の情報セキュリティ対策を推進及び運用するため、組織内の体制整備及び事務を行う。

- **遵守事項 2.1.1(4)(a)「全学実施責任者」について**

全学総括責任者は、自らの事務を補佐させるため、組織のまとまりごとに設置する部局総括責任者のうちから１人を全学実施責任者として選任する。

全学実施責任者は、全学総括責任者からの委任（全学総括責任者が自ら行うべき重要事項を除き、事務を任せること。任命及び監督の責任は、全学総括責任者に残る。）に基づき本学の情報セキュリティ対策について総合調整する事務を担うとともに、全学総括責任者を補佐する役割を担う。例えば、事務情報セキュリティ対策基準や対策推進計画の案の作成を担うことが想定される。

- **遵守事項 2.1.1(4)(b)「区域情報セキュリティ責任者」について**

部局総括責任者は、所管する組織のまとまりの情報セキュリティ対策のうち施設及び環境に係る対策について、定められた区域ごとにその対策を推進する責任者として区域情報セキュリティ責任者を指名する。

区域情報セキュリティ責任者は、所管する区域について規定された対策の基準に従い、自ら対策を定めそれを実施する。また、区域情報セキュリティ責任者は、その役割の性質上、施設の管理者が兼任することが想定される。定める単位としては、例えば以下が考えられる。

- 単一の課室が利用する執務室及び会議室を管理する場合は、職場情報セキュリティ責任者
- 情報システムが設置された部屋（サーバ室等）を管理する場合は、部局技術責任者
- ロビー、廊下等を管理する場合は、施設等の管理に関する部門の責任者

なお、基本対策事項 3.2.1(1)-1 で後述するクラス１は、庁舎管理の観点から行う措置が、情報セキュリティ上の対策と同等であれば、庁舎管理者が指定されていることを

もって、区域情報セキュリティ責任者を設置しているとみなしてよい。

- **遵守事項 2.1.1(4)(c)「職場情報セキュリティ責任者」について**

  部局総括責任者は、課室内の情報の取扱い及び情報セキュリティ対策の責任者として、職場情報セキュリティ責任者を設置する。職場情報セキュリティ責任者は、情報の取扱い等に関して、その是非を判断する役割を担うため、課室長又はそれに相当する者であることが望ましい。

- **遵守事項 2.1.1(4)(d)「部局技術責任者」について**

  部局総括責任者は、情報システムごとの情報セキュリティ対策及び運用の責任者として、部局技術責任者を指名する。

  部局技術責任者は、所管する情報システムのライフサイクル全般にわたって適切に情報セキュリティ対策を実施することが求められる。このため、部局総括責任者は、新規の情報システムについて企画に着手するまでに部局技術責任者を選任しなければならない。本学 LAN システムのような全省庁的なシステム、特定部門における個別業務システム等、本学の全ての情報システムについて、情報システムごとにセキュリティ対策の運用の責任の所在を明確にすることが重要である。また、アプリケーションのみ別組織が管理するといったように、情報システムを共同で管理する場合は、あらかじめ責任分担を明確にする必要がある。

  部局技術責任者は、情報セキュリティ対策の技術的事項について補佐する者（基本対策事項 2.1.1(4)-6 で定める部局技術担当者）をデータベース、アプリケーション等の装置・機能ごとに、必要に応じて置き、技術的対策の実効性を確保することが望ましい。

- **基本対策事項 2.1.1(4)-1 b)「実施手順」について**

  「（解説）遵守事項 2.2.1(1)(a)「実施手順を整備（本基準において整備すべき者を別に定める場合を除く。）」について」を参照のこと。

- **基本対策事項 2.1.1(4)-6「部局技術担当者」について**

  部局技術担当者は、部局技術責任者が定めた手順や判断された事項に従い、所管する情報システムのセキュリティ対策を実施する。

遵守事項

(5) 情報セキュリティアドバイザーの設置

(a) 全学総括責任者は、情報セキュリティについて専門的な知識及び経験を有する者を情報セキュリティアドバイザーとして置き、自らへの助言を含む情報セキュリティアドバイザーの業務内容を定めること。

【 基本対策事項 】

＜2.1.1(5)(a)関連＞

2.1.1(5)-1 全学総括責任者は、以下を例とする情報セキュリティアドバイザーの業務内容を定めること。

a) 本学全体の情報セキュリティ対策の推進に係る全学総括責任者への助言
b) 情報セキュリティ関係規程の整備に係る助言
c) 対策推進計画の策定に係る助言
d) 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
e) 情報システムに係る技術的事項に係る助言
f) 情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
g) 事務従事者に対する日常的な相談対応
h) 情報セキュリティインシデントへの対処の支援
i) 前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（解説）

- **遵守事項 2.1.1(5)(a)「情報セキュリティアドバイザー」について**

全学総括責任者は、情報セキュリティに関する技術的事項等について自らへの助言等を含む本学の情報セキュリティ対策への助言、支援等を行う者として情報セキュリティアドバイザーを置く。

情報セキュリティアドバイザーは、本学における情報システムに関する技術的事項、情報セキュリティインシデントへの対処その他の情報セキュリティ対策に対する助言・支援を担うため専門的な知識及び経験を有した者、すなわち情報セキュリティに関する資格及び実務経験を有する者である必要がある。

なお、外部人材のみならず学内の職員を充ててもよい。この場合、当該職員が部局総括責任者やその他の責任者を兼務してもよい。

遵守事項

(6) 情報セキュリティインシデントに備えた体制の整備

(a) 全学総括責任者は、**CSIRT** を整備し、その役割を明確化すること。

(b) 全学総括責任者は、事務従事者のうちから **CSIRT に属する職員**として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、本学における情報セキュリティインシデントに対処するための責任者として **CSIRT 責任者**を置くこと。また、**CSIRT 内の業務統括及び外部との連携等を行う職員**を定めること。

(c) 全学総括責任者は、**情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制**を整備すること。

【 基本対策事項 】

＜2.1.1(6)(a)関連＞

2.1.1(6)-1 全学総括責任者は、以下を含む CSIRT の役割を規定すること。

a) 本学に関わる情報セキュリティインシデント発生時の対処の一元管理
- 外局等を含む**本学全体における情報セキュリティインシデント対処の管理**
- 情報セキュリティインシデントの可能性の報告受付
- 本学における情報セキュリティインシデントに関する情報の集約
- 本学の附属機関等における情報セキュリティインシデントに関する情報の集約
- 情報セキュリティインシデントの全学総括責任者等への報告
- 情報セキュリティインシデントへの対処に関する指示系統の一本化

b) 情報セキュリティインシデントへの迅速かつ的確な対処
- 情報セキュリティインシデントであるかの評価
- 被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
- 文部科学省への連絡
- 外部専門機関等からの情報セキュリティインシデントに係る情報の収集
- 他大学 CSIRT 等の機関への情報セキュリティインシデントに係る情報の共有
- 情報セキュリティインシデントへの対処に係る**専門的知見の提供、対処作業の実施**

2.1.1 (6)-2 全学総括責任者は、**実務担当者を含めた実効性のある CSIRT 体制**を構築すること。

2.1.1 (6)-3 全学総括責任者は、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する**外部の専門家等による必要な支援を速やかに得られる体制**を構築しておくこと。

2.1.1 (6)-4 全学総括責任者は、本学全体における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の**役割分担を規定**すること。

（解説）

- **遵守事項 2.1.1(6)(a)「CSIRT」について**

本学の情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、当該高等教育機関が、全学総括責任者等の幹部の指揮の下、情報セキュリティインシデントへの対処を一元的に管理し、発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を整備することが必要である。

一般的に、情報セキュリティインシデントの認知時の対処においては、不完全で断片的な情報しかない状況で判断を下し、指示を出して、調査等により状況の解明を進めることとなる。CSIRT は、時々刻々と明らかになる情報を基に、状況を整理し、事態の収束に向けてさらに必要な対応を行い、適切な頻度で全学総括責任者等の幹部に状況を報告する。

- **遵守事項 2.1.1(6)(b)「CSIRT に属する職員」について**

CSIRT に属する職員は、本学における情報セキュリティインシデントを認知した際、全学総括責任者の指揮の下、これに対処する職員であることから、全学総括責任者に対して適切に状況を報告し、全学総括責任者の指示を受け適切に対処できることが必要である。

CSIRT に属する職員には、情報セキュリティ、情報システム等に関する知識及び技能を持つ者並びに本学のネットワーク構成や個別システムの部局技術責任者及び管理者を把握している者を含めることが求められる。

また、CSIRT に属する職員には、上述した技術的な対処のほか、発生した情報セキュリティインシデントの影響の大きさによっては、対外的な対応も必要となることから、広報を担当する職員を CSIRT に含めておくことも考えられる。

- **遵守事項 2.1.1(6)(b)「CSIRT 責任者」について**

CSIRT 責任者とは、情報セキュリティインシデントの対処に係る責任者であり、情報セキュリティインシデントに関する全般的な対応が求められる。ただし、重大な情報セキュリティインシデントが生じ、全学総括責任者自らが、情報セキュリティインシデントへ対処する必要があるときには、その指揮監督の下で必要な対応を行うこととなる。

- **遵守事項 2.1.1(6)(b)「CSIRT 内の業務統括及び外部との連携等を行う職員」について**

CSIRT 内の業務統括及び外部との連携等を行う職員は、CSIRT 責任者の指揮の下、CSIRT の業務や連絡を一元的に管理し統括する機能を担う。ここでいう職員は、一人の職員に制限するものではなく、いわゆる総括班のような位置付けで複数名置くことが望ましい。

- **遵守事項 2.1.1(6)(c)「情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制」について**

CSIRT 責任者が情報システムを所管している場合、当該情報システムの情報セキュ

リティインシデントを認知した際、二つの役職が利害相反関係にあることから、全学総括責任者等の幹部に報告を上げない、事実関係の一部しか報告しない、報告を遅らせるなど、管理責任に影響を及ぼすおそれがある。

これを避けるため、例えば、CSIRT 責任者には部局総括責任者以外の者を充てる、全学総括責任者等の幹部に情報セキュリティインシデントについて報告する役割を別途 CSIRT 責任者以外の者に与えるなどにより、迅速かつ適切な報告経路を確保することが必要である。

- **基本対策事項 2.1.1(6)-1 a)「本学全体における情報セキュリティインシデント対処の管理」について**

  情報セキュリティインシデントへの対処に当たっては、「検知／連絡受付」、「トリアージ（情報セキュリティインシデントであるか否かの評価、優先度付け等）」、「インシデントレスポンス（応急措置の実施、原因調査、復旧、再発防止等）」、「報告／情報公開（報道発表等の対外対応）」といったプロセスが必要となる。

  CSIRT には、これらのプロセス全体について、学内外の関係組織と連携・調整を図り、状況を把握し、適宜幹部等への報告を行うとともに、迅速かつ的確な対処が行われるように当事者部局への指示・勧告・助言を行うことが求められる。

- **基本対策事項 2.1.1(6)-1 b)「専門的知見の提供、対処作業の実施」について**

  本学において、サイバーセキュリティや情報セキュリティインシデントへの対処に係る専門組織や専門知識を持った職員を有する場合は、それらの組織・職員の CSIRT への組み込み、又は情報セキュリティインシデント発生時に連携できる体制の構築を行うことが望ましい。

- **基本対策事項 2.1.1(6)-2「実務担当者を含めた実効性のある CSIRT 体制」について**

  CSIRT 体制には、情報セキュリティインシデント対処における全学総括責任者への早急な状況報告、被害拡大防止及び復旧のための対策の実施を果たし得るよう、実務担当職員を複数含むことが必要である。

  また、CSIRT は、情報セキュリティアドバイザー等から情報セキュリティインシデントへの対処の支援が円滑に受けられるような体制とすることが望ましい。

- **基本対策事項 2.1.1(6)-3「外部の専門家等による必要な支援を速やかに得られる体制」について**

  外部の専門家等による必要な支援を迅速に得られる体制の構築の例としては、情報セキュリティインシデント発生時にそうした事案への対処に精通した専門家を速やかに派遣してもらうための契約を事業者と結ぶこと等が挙げられる。

- **基本対策事項 2.1.1(6)-4「役割分担を規定」について**

  情報セキュリティインシデント発生時に、関係者が速やかに必要な対処を行えるように、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局（広報担当部局、調達担当部局、サイバーセキュリティ専門部局等）の役割分担をあらかじめ定めておくことが望ましい。ただし、役割分担は、情報セキュリティインシデント

の種類や規模、影響度合い等によって変更されることも考えられるため、発生の頻度が比較的高いと考えられる情報セキュリティインシデントを想定した役割分担をあらかじめ定めておき、必要に応じて役割分担を再設定することも考えられる。

遵守事項

(7) 兼務を禁止する役割

(a) 事務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

(ア) 承認又は許可（以下、本項において「承認等」という。）の申請者と当該承認等を行う者（以下、本項において「承認権限者等」という。）

(イ) 監査を受ける者とその監査を実施する者

(b) 事務従事者は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.1(7)(b)「承認権限者等の上司又は適切な者」について**

承認等の申請において、申請する者と承認する者が同一の場合又は申請する者が承認する者の上司である場合は、手続規定において定められた承認権限者等をもって承認等の可否の判断を行うことは適切とは言えない。

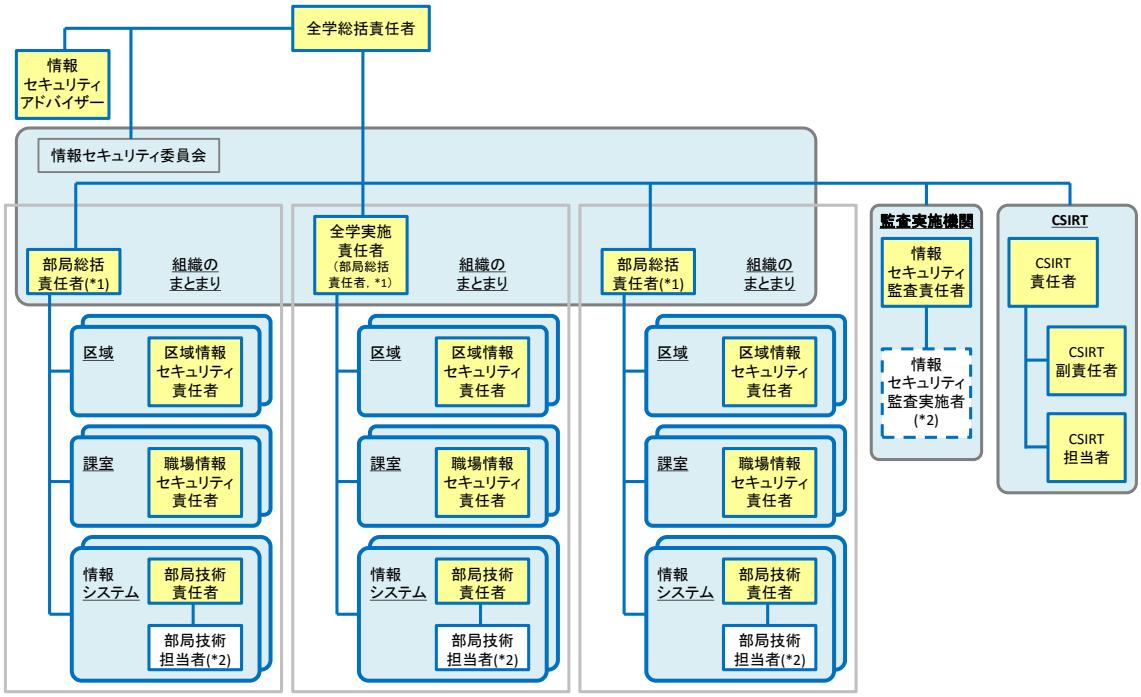
このような場合に対応するために、承認権限者等の上司等をもって承認するなどの手続をあらかじめ定めておく必要がある。

部局総括責任者等よりも高位の事務従事者が承認等を申請する場合においては、例えば、全学総括責任者が当該承認等の判断を行うことが想定される。他方、技術的な事項は、承認権限者等の上司よりも内容を理解している者が可否の判断を行う方が適切な場合もあり、この場合には、本来の承認権限者等が判断してよい。

また、全学総括責任者と同等以上の職位の者が、承認等を申請する場合も想定される。このような場合においても、全学総括責任者が、適切に判断することが考えられる。

【参考 2.1.1-1】 本学の情報セキュリティ体制のイメージ例

本学の情報セキュリティ体制のイメージを図 2.1.1-1 に示す。



※1 約款による外部サービス（ソーシャルメディアサービスを含む）を利用する場合に責任者を定める権限あり
※2 ガイドラインのみに記載

図 2.1.1-1 本学の情報セキュリティ体制のイメージ

2.1.2 事務情報セキュリティ対策基準・対策推進計画の策定

目的・趣旨

本学の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、本学として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果を踏まえ、計画的に対策を実施することが重要である。

遵守事項

(1) 事務情報セキュリティ対策基準の策定

(a) 全学総括責任者は、全学情報システム運用委員会における審議を経て、統一基準に準拠した**事務情報セキュリティ対策基準**を定めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.2(1)(a)「事務情報セキュリティ対策基準」について**

  事務情報セキュリティ対策基準については、全学総括責任者がこれを定める必要がある。

  なお、当該基準の案の策定については、全学総括責任者が指定した者に委任することができる。

遵守事項

(2) 対策推進計画の策定

(a) 全学総括責任者は、全学情報システム運用委員会における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「**対策推進計画**」という。）を定めること。また、対策推進計画には、本学の業務、取り扱う情報及び保有する情報システムに関する**リスク評価の結果を踏まえた全体方針**並びに以下に掲げる**取組の方針・重点**及びその実施時期を含めること。

(ア) 情報セキュリティに関する教育

(イ) 情報セキュリティ対策の自己点検

(ウ) 情報セキュリティ監査

(エ) **情報システムに関する技術的な対策を推進するための取組**

(オ) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.1.2(2)(a)「対策推進計画」について**

対策推進計画は、情報セキュリティ対策に関する一連の取組を対象とした全体計画であり、情報セキュリティ対策に関する取組の全体方針のほか、遵守事項 2.1.2(2)(a)の各号に掲げる情報セキュリティ対策に関する個々の取組について、全体方針に応じた個々の方針や重点、大まかな実施（予定）時期を設定するものである。

対策推進計画は、本学が組織として、種々の情報セキュリティ対策を如何なる考え方や方向性に基づいて進めていくのかといった一連の取組全体の大枠について、全学総括責任者があらかじめ総合的に定めるものであり、個々の取組の実施に当たって詳細計画が必要となる場合は、対策推進計画に則して、それぞれの取組の責任者がその権限の下に詳細計画を策定する。

- **遵守事項 2.1.2(2)(a)「リスク評価の結果を踏まえた全体方針」について**

情報セキュリティ対策は、情報セキュリティを取り巻く様々な脅威や、組織及び取り扱う情報の特性等を踏まえたリスクの分析・評価を行った上で、対策の方針や優先度を判断し、計画的に推進することが重要である。また、限られた予算や人的資源を最大限に活用して情報セキュリティ対策を推進するためには、対策全体としての方向付けを行った上で個々の対策を実施していくことが必要である。

全体方針としては、例えば、優先的に対応すべき脅威や優先的に対策を講ずるべき対象を設定し、それらへの対応を重点として掲げることが考えられる。

また、自組織の目的等を踏まえ、情報セキュリティ対策の自己点検の結果やサイバーセキュリティ基本法第 25 条第 1 項第 2 号に基づく監査（以下「本部監査」という。）の結果等を考慮した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリテ

ィ対策を講ずることが求められる。

- **遵守事項 2.1.2(2)(a)「取組の方針・重点」について**

  遵守事項 2.1.2(2)(a)の各号に掲げる情報セキュリティ対策に関する個々の取組の方針・重点は、全体方針を踏まえ、例えば、情報セキュリティ対策の教育において、特定の脅威（例：標的型攻撃、サプライチェーン・リスク）、特定の対象（例：業務の内容や役職に応じた者）、特定の内容（例：事務情報セキュリティ対策基準の改正点）を掲げることが考えられる。

- **基本対策事項 2.1.2(2)(a)(エ)「情報システムに関する技術的な対策を推進するための取組」について**

  情報システムに関する技術的な対策を推進するための取組としては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに基づく取組等、政府全体としての取組のほか、各高等教育機関において独自に推進している技術的な対策を含めることが望ましい。技術的対策には、情報システムを構成する機器等の更新等の投資による対策も含まれる。

2.2　運用

2.2.1　情報セキュリティ関係規程の運用

目的・趣旨

本学は、事務情報セキュリティ対策基準に定められた対策を実施するため、具体的な実施手順を定める必要がある。

実施手順が整備されていない、又はそれらの内容に漏れがあると、対策が実施されないおそれがあることから、全学総括責任者は、全学実施責任者に実施手順の整備を指示し、その結果について定期的に報告を受け、状況を適確に把握することが重要である。

遵守事項

(1) 情報セキュリティ対策に関する実施手順の整備・運用

(a) 全学実施責任者は、本学における情報セキュリティ対策に関する**実施手順を整備（本統一基準で整備すべき者を別に定める場合を除く。）**し、**実施手順に関する事務を統括**し、整備状況について全学総括責任者に報告すること。

(b) 全学実施責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動時等に関する管理の規定を整備すること。

(c) 部局総括責任者又は職場情報セキュリティ責任者は、事務従事者より情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、全学実施責任者に報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.1(1)(a)「実施手順を整備（本基準で整備すべき者を別に定める場合を除く。）」について**

事務情報セキュリティ対策基準で整備を求めている実施手順は、以下のとおり。

（１）全学実施責任者

- 情報セキュリティ対策における雇用の開始、終了及び人事異動時等の管理に関する規程（遵守事項 2.2.1(1)(b)）
- 情報セキュリティインシデントの可能性を認知した際の報告窓口を含む本学関係者への報告手順(遵守事項 2.2.4(1)(a)）
- 情報セキュリティインシデントの可能性を認知した際の学外との情報共有を含む対処手順(遵守事項 2.2.4(1)(b)）
- 情報の取扱いに関する規定(遵守事項 3.1.1(1)(a)）
- 要管理対策区域の対策の基準(遵守事項 3.2.1(1)(b))
- 外部委託に係る規定(遵守事項 4.1.1(1)(a))
- 約款による外部サービスの利用に関する規定(遵守事項 4.1.2(1)(a)）

- ソーシャルメディアサービスによる情報発信時における情報セキュリティ対策に関する運用手順等(遵守事項 4.1.3(1)(a))
- 機器等の調達に係る選定基準(遵守事項 5.1.2(1)(a))
- 機器等の納入時の確認・検査手続(遵守事項 5.1.2(1)(b))
- アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規定(遵守事項 6.3.1(1)(a))
- 本学の情報システムの利用のうち、情報セキュリティに関する規定(遵守事項 8.1.1(1)(a))
- 要管理対策区域外で情報処理を行う際の安全管理措置に関する規定及び許可手続（遵守事項 8.1.1(1)(b))
- USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順(遵守事項 8.1.1(1)(c))
- 本学支給以外の端末により情報処理を行う場合の許可等の手続に関する手順（遵守事項 8.2.1(1)(a))
- 本学支給以外の端末により情報処理を行う場合の安全管理措置に関する規定(遵守事項 8.1.1(1)(b))

（2）その他の者が定めるもの

- 全学総括責任者
  - 例外措置の適用の申請を審査する者及び審査手続（遵守事項 2.2.2(1)(a))
- 部局総括責任者
  - 事務従事者ごとの自己点検票及び自己点検の実施手順(遵守事項 2.3.1(1)(b))
- 部局技術責任者
  - 情報セキュリティ対策を実施するために必要な文書（遵守事項 5.1.1(2)(a))
  - 情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法(遵守事項 6.1.5(1)(b))
  - 通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順(遵守事項 7.3.1(1)(i))

- **遵守事項 2.2.1(1)(a)「実施手順に関する事務を統括」について**

全学実施責任者は、本学における情報セキュリティ対策に関する実施手順について、監査結果を通じて、事務情報セキュリティ対策基準に従って整備されていないことを把握した場合には、整備すべき者に対して指導することが想定される。

また、全学実施責任者は、情報セキュリティ関係規程について自己点検や監査の結果、例外措置の申請状況等を通じ、課題又は問題点について把握し得ることから、実施手順の整備主体が、特定の部門の部局総括責任者に係るものであったとしても、同種の課題又は問題点の有無を他の部局等に確認することも想定される。

遵守事項

(2) 違反への対処

(a) 事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合は、部局総括責任者にその旨を報告すること。

(b) 部局総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、全学実施責任者を通じて、全学総括責任者に報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.1(2)(a)「部局総括責任者にその旨を報告する」について**

本学において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉するための事項である。一般的に、本学においては、違反を知った者はこれを報告する義務が課されており、情報セキュリティ関係規程への違反においては、各規定の実施に責任を持つ部局総括責任者に報告することとなる。本規定は、行政事務従事者から情報セキュリティ責任者への直接の報告を必須とするものではなく、重大な違反等の有無を情報セキュリティ責任者が確実に認識できるようにすることを求めている。

なお、事務従事者は、自ら違反した場合に限らず、他の事務従事者が違反している場合においても、迅速な是正措置を促す理由から、当該事務従事者への助言に加えて部局総括責任者に報告するなど適切に対応することが求められる。また、情報セキュリティ関係規程に係る課題及び問題点を認識した場合についても、情報セキュリティ責任者に報告することが望ましい。

- **遵守事項 2.2.1(2)(b)「情報セキュリティ関係規程への重大な違反」について**

情報セキュリティ関係規程への重大な違反とは、当該違反により本学の業務に重大な支障をきたすもの又はその可能性のあるものをいう。例えば、機密性の極めて高い情報を保存した端末を、許可無く要管理対策区域外に持ち出し、それを紛失し、情報の漏えいが発生し、高等教育機関の事務の遂行に著しく支障を来してしまった場合等が考えられる。

部局総括責任者は、本学において情報セキュリティを継続的に維持するために、重大な違反を確実に捕捉し、被害の未然防止又は拡大防止のための措置を適切に講じさせるとともに、再発防止に関する取組を進めることが求められる。

- **遵守事項 2.2.1(2)(b)「違反者及び必要な者」について**

情報セキュリティ関係規程への重大な違反があった場合には、違反者自身が対策を講ずることは当然であるが、それ以外の「必要な者」として措置を義務付けられるのは、部局技術責任者、職場情報セキュリティ責任者及び区域情報セキュリティ責任者等の当該規程の実施に責任を有する者が挙げられる。情報システムの運用者や担当者、

委託先等とも協力し、情報セキュリティを維持するために必要な措置を講ずる必要がある。

- **遵守事項 2.2.1(2)(b)「情報セキュリティの維持に必要な措置」について**

  重大な違反により、情報が漏えい、滅失、き損し又は情報システムの利用に支障を来した場合、早期解決、拡大防止等の対処を行う。拡大防止としては、情報セキュリティ関係規程について再周知の徹底が考えられる。

- **遵守事項 2.2.1(2)(b)「全学総括責任者に報告する」について**

  報告を受けた全学総括責任者は、その内容、結果、業務への影響、社会的評価等を確認し、本学全体として再発防止を徹底するなど、適切に対応する必要がある。

  また、全学実施責任者は、同様の違反が多発している可能性の有無を考慮し、違反の原因について分析し、必要に応じて情報セキュリティ関係規程の見直しを含めた対策を検討する必要がある。

2.2.2 例外措置

目的・趣旨

例外措置はあくまで例外であって、濫用があってはならない。しかしながら、情報セキュリティ関係規程の適用が高等教育機関の事務の適正な遂行を著しく妨げるなどの理由により、規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合がある。このような場合に対処するために、例外措置の手続を定めておく必要がある。

遵守事項

(1) 例外措置手続の整備

(a) 全学総括責任者は、**例外措置の適用の申請を審査する者**（以下「許可権限者」という。）及び、審査手続を定めること。

(b) 全学実施責任者は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めること。

【 基本対策事項 】

＜2.2.2(1)(a)関連＞

2.2.2(1)-1 全学総括責任者は、例外措置について以下を含む手順を定めること。

a) 例外措置の許可権限者

b) 事前申請の原則その他の申請方法

c) 審査項目その他の審査方法

- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を申請する期間
- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置により生じる情報セキュリティ上の影響と対処方法
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

＜2.2.2(1)(b)関連＞

2.2.2(1)-2 許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、全学実施責任者へ定期的に報告すること。

a) 審査した者の情報（氏名、役割名、所属、連絡先）

b) 申請内容

- 申請者の情報（氏名、所属、連絡先）
- 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を申請する期間

- 例外措置の適用を申請する措置内容（講ずる代替手段等）
- 例外措置の適用を終了した旨の報告方法
- 例外措置の適用を申請する理由

c) 審査結果の内容

- 許可又は不許可の別
- 許可又は不許可の理由
- 例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等）
- 例外措置の適用を許可した期間
- 許可した措置内容（講ずるべき代替手段等）
- 例外措置を終了した旨の報告方法

（解説）

- **遵守事項 2.2.2(1)(a)「例外措置の適用の申請を審査する者」について**

例外措置の適用の申請を受けた際に審査を遅滞なく実施できるように、許可権限者を定め、審査手続を整備しておく必要がある。情報セキュリティ関係規程の誤った解釈や恣意的な例外運用を防止するために、例えば、情報セキュリティ関係規程を策定した者を許可権限者に充てることが考えられる。

遵守事項

(2) 例外措置の運用

(a) 事務従事者は、定められた審査手続に従い、許可権限者に規定の**例外措置の適用を申請**すること。ただし、高等教育機関の事務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ること。

(b) 許可権限者は、事務従事者による**例外措置の適用の申請**を、定められた審査手続に従って**審査**し、許可の可否を決定すること。

(c) 許可権限者は、例外措置の申請状況を台帳に記録し、**全学実施責任者に報告**すること。

(d) 全学実施責任者は、例外措置の申請状況を踏まえた**情報セキュリティ関係規程の追加又は見直しの検討**を行い、全学総括責任者に報告すること。

【 基本対策事項 】規定なし

(解説)

- **遵守事項 2.2.2(2)(a)「例外措置の適用を申請」について**

事務従事者は、定められた審査手続に従い例外措置の適用を申請し、許可を得てから例外措置を講ずることが原則であるが、高等教育機関の事務の遂行に緊急を要するなどの場合であって、情報セキュリティ関係規程の規定内容とは異なる代替の方法を直ちに採用すること又は規定された対策を実施しないことが不可避のときは、事後速やかに届け出ることが必要である。

事務従事者は、例外措置の適用を希望する場合には、当該例外措置を適用したときの情報セキュリティ上の影響を検討、分析する必要がある。その上で、例外措置の適用が必要であると判断した場合は、その影響を低減させるための補完措置を提案し、適用の申請を行う必要がある。

- **遵守事項 2.2.2(2)(b)「例外措置の適用の申請」・「審査」について**

許可権限者は、例外措置の適用の申請を適切に審査しなければならない。審査に当たっては、例外措置の適用を許可した場合の情報セキュリティ上の影響と、不許可とした場合の高等教育機関の事務遂行等への影響を評価した上で、その判断を行う必要がある。

例外措置の適用期間が長期にわたる場合等においては、例外措置の実施によるリスクが変化する可能性を踏まえ、定期的に当該措置の適用状況等を許可権限者において把握することも重要である。

- **遵守事項 2.2.2(2)(c)「全学実施責任者に報告」について**

全学実施責任者は、許可権限者から例外措置の適用状況の報告を受ける。これは、遵守事項 2.2.2(2)(d)で情報セキュリティ関係規程の追加又は見直しの検討を行うため

である。

- **遵守事項 2.2.2(2)(d)「情報セキュリティ関係規程の追加又は見直しの検討」について**

  例外措置の適用が多い状況は、例外とはみなせないと考えるべきである。その場合には、代替手段の導入を含め、情報セキュリティ関係規程の見直しを検討する必要がある。

2.2.3 教育

目的・趣旨

情報セキュリティ関係規程が適切に整備されているとしても、その内容が事務従事者に認知されていなければ、当該規定が遵守されていないことになり、情報セキュリティ水準の向上を望むことはできない。このため、全ての事務従事者が、情報セキュリティ関係規程への理解を深められるよう、適切に教育を実施することが必要である。

また、近年の情報セキュリティインシデントの増加等に鑑み、情報セキュリティの専門性を有する人材を育成することも求められる。

遵守事項

(1) 教育体制等の整備

(a) 全学実施責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備すること。

【 基本対策事項 】

＜2.2.3(1)(a)関連＞

2.2.3(1)-1 全学実施責任者は、事務従事者の役割に応じて**教育すべき内容を検討**し、教育のための資料を整備すること。

2.2.3(1)-2 全学実施責任者は、**事務従事者が毎年度最低１回は教育を受講**できるように、教育実施計画を立案するとともに、その実施体制を整備すること。

2.2.3(1)-3 全学実施責任者は、事務従事者の着任又は異動後に、**３か月以内に受講**できるように、その実施体制を整備すること。

（解説）

- **基本対策事項 2.2.3(1)-1「教育すべき内容を検討」について**

教育の内容については、最新の脅威動向、本学の実状や情報セキュリティインシデントの発生状況等、情報セキュリティ環境の変化等を踏まえ、幅広い角度から検討し、受講者の役割、責任及び技能に適したものにする必要がある。

さらに、教育の内容は、事務従事者が対策内容を十分に理解できるものとする必要があり、そのためには、網羅的な資料ではなく、理解しておくべき事項に制限した資料を教育に用いるべきである。例えば、情報セキュリティ関係規程の教育資料の作成においては、遵守事項を遵守すべき者ごとに整理し、事務従事者が遵守する必要のない事項は、含まないように配慮すべきである。

また、違反の抑止効果を期待することを目的に、ウェブサイトの閲覧に係るログを取得していることや、必要に応じて当該ログを調査することがあること等の情報システムの運用ルールを事務従事者の教育内容に含めることも考えられる。

このような教育内容の検討に加えて、教育実施後に簡単なテストを実施することに

より受講者の理解度を把握したり、受講者にアンケートを記入してもらったりすることで、次回開催のテーマや現在の教育方法等についての改善を検討することも考えられる。

なお、情報セキュリティ関係部署の者や CSIRT に属する職員に対して、情報セキュリティに関する知識及び技能を向上させるため、研修及び実務を模擬した訓練を実施することも有効である。訓練内容や実施結果の評価等について、情報セキュリティアドバイザーの助言を受けることも有用である。より高度な技能の習得や将来的な脅威への対応等を求めた訓練を実施する場所等においては、外部の専門事業者に委託することにより訓練を実施してもよい。

- **基本対策事項 2.2.3(1)-2「事務従事者が毎年度最低１回は教育を受講」について**

対策推進計画に基づき、対象者、手段及び実施時期等の教育実施計画を定める。

教育実施計画の策定に当たっては、本学の統一研修プログラムや e-learning 等の活用を含め、効率性や受講のしやすさにも配慮する必要がある。

また、教育実施計画には、情報セキュリティ担当者、CSIRT に属する職員の人材育成について、キャリアパスにも配慮し、策定する必要がある。

- **基本対策事項 2.2.3(1)-3「3 か月以内に受講」について**

着任、異動した事務従事者に対しては、早期に情報セキュリティ対策の教育を受講させることも有益であり、着任後 3 か月以内には受講させるべきである。ただし、異動した後に使用する情報システムが、異動前と変わらないなど、教育をしないことについて合理的な理由がある場合は、対象から除外しても差し支えない。

遵守事項

(2) 教育の実施

(a) 職場情報セキュリティ責任者は、事務従事者に対して、情報セキュリティ関係規程に係る教育を**適切に受講**させること。

(b) 事務従事者は、教育実施計画に従って、**適切な時期に教育を受講**すること。

(c) 職場情報セキュリティ責任者は、**CSIRT に属する職員に教育を適切に受講**させること。

(d) 全学実施責任者は、全学総括責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.3(2)(a)「適切に受講」について**

職場情報セキュリティ責任者は、事務従事者に情報セキュリティ対策の教育を受講させる責務があり、事務従事者に対して教育の実施を周知するとともに、教育を受講しない者に対して受講を勧告するほか、受講状況を把握するなどして、積極的に受講を促すこと等が求められる。また、受講時間を確保するなどの事務従事者が受講できるための環境を整備するなどの配慮も必要である。

- **遵守事項 2.2.3(2)(b)「適切な時期に教育を受講」について**

事務従事者は、教育実施計画に従って、毎年度最低 1 回は教育を受講することを求められる。

着任時又は異動時の場合には、新しい職場等で、情報セキュリティ対策の教育の受講方法について職場情報セキュリティ責任者に確認することも求められる。

- **遵守事項 2.2.3(2)(c)「CSIRT に属する職員に教育を適切に受講」について**

サイバー攻撃等の情報セキュリティに対する脅威が増大している状況を踏まえ、情報セキュリティインシデントに迅速かつ適切に対処するための組織として本学に CSIRT が整備されている。これらに属する職員への教育も、その責務に照らすと極めて重要である。

2.2.4 情報セキュリティインシデントへの対処

目的・趣旨

情報セキュリティインシデントを認知した場合には、全学総括責任者に早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、情報セキュリティインシデントの対処が完了した段階においては、原因について調査するなどにより、情報セキュリティインシデントの経験から今後に生かすべき教訓を導き出し、再発防止や対処手順、体制等の見直しにつなげることが重要である。

遵守事項

(1) 情報セキュリティインシデントに備えた事前準備

(a) 全学実施責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む本学関係者への**報告手順**を整備し、**報告が必要な具体例**を含め、事務従事者に周知すること。

(b) 全学実施責任者は、情報セキュリティインシデントの可能性を認知した際の学外との情報共有を含む**対処手順**を整備すること。

(c) 全学実施責任者は、情報セキュリティインシデントに備え、高等教育機関の事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む**緊急連絡網**を整備すること。

(d) 全学実施責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、高等教育機関の事務の遂行のため特に重要と認めた情報システムについて、その**訓練の内容及び体制を整備**すること。

(e) 全学実施責任者は、情報セキュリティインシデントについて**学外の者から報告を受けるための窓口を整備**し、その窓口への連絡手段を学外の者に明示すること。

(f) 全学実施責任者は、**対処手順が適切に機能することを訓練等により確認**すること。

【 基本対策事項 】

＜2.2.4(1)(a)関連＞

2.2.4 (1)-1 全学実施責任者は、本学の附属機関等における情報セキュリティインシデント発生が報告された際にも、本学における情報セキュリティインシデントの場合と同様に、全学総括責任者や文部科学省に速やかに報告されるよう手順を定めること。

＜2.2.4(1)(b)関連＞

2.2.4(1) 2 全学実施責任者は、情報セキュリティインシデト発生時の対処手順のうち、**意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等**をあらかじめ定めておくこと。

＜2.2.4(1)(e)関連＞

2.2.4(1)-3 全学実施責任者は、本学の附属機関等において発生した情報セキュリティインシデントについて、当該機関から報告・連絡を受ける窓口について定めるとともに、各機関にその窓口の連絡先を周知すること。

（解説）

- **遵守事項 2.2.4(1)(a)「報告手順」について**

  報告手順として明記すべき事項としては、情報セキュリティインシデントの可能性が認知されてから全学総括責任者に報告するまでの具体的な手順等が考えられる。

  また、情報セキュリティインシデントの可能性の報告窓口については、報告手順の中で明らかにしておくほか、情報セキュリティ対策の教育の中で周知する、報告窓口の連絡先を執務室内に掲示するなどして、緊急時に事務従事者が速やかに報告できるようにする必要がある。

  報告窓口を CSIRT とは異なる部門に設ける場合は、当該部門から CSIRT への報告が速やかに実施される体制にすることが求められる。

- **遵守事項 2.2.4(1)(a)「報告が必要な具体例」について**

  「(解説) 遵守事項 2.2.4(2)(a)「情報セキュリティインシデントの可能性を認知した場合には、本学の報告窓口に報告」について」を参照のこと。

- **遵守事項 2.2.4(1)(b)「対処手順」について**

  対処手順として情報セキュリティインシデントの認知時において緊急を要する対処等の必要性に備えて、通常とは異なる例外的な承認手続を定めておくことも併せて検討する必要がある。対処する者に、ある程度の権限の委任がされないと、適切な措置に遅延等が発生することが予想されるため、そのようなことがないよう検討すること。

- **遵守事項 2.2.4(1)(c)「緊急連絡網」について**

  全学実施責任者は、通常時の全ての情報セキュリティ関連の責任者及び管理者の連絡網の整備に加えて、情報セキュリティインシデントを認知した場合に速やかに対処するための「緊急連絡網」を整備する必要がある。

  緊急連絡網には、該当する事務従事者の自宅や携帯電話の番号等の個人情報が含まれることも想定される。また、緊急連絡網には当該システムに係る責任者及び管理者のほか、重大な情報セキュリティインシデントに備えて全学総括責任者も含める必要がある。

- **遵守事項 2.2.4(1)(d)「訓練の内容及び体制を整備」について**

  実際に情報セキュリティインシデントへの対処を模擬的に行うことにより、対処能力を向上させるために実施する訓練の内容及び体制の整備を求める事項である。

  実効的な訓練を実施するためには、情報システム部門だけでなく、情報セキュリティインシデントに関する報告窓口となる部門、情報セキュリティ対策に関する事務を総括する部門や CSIRT も参加することが望ましい。

  なお、あらかじめ全学実施責任者が認めた場合には、全学実施責任者が指定した者に当該訓練の内容及び体制を整備させることも考えられる。その際には、全学実施責任者は、指定した者より適宜報告を受けることが望ましい。

- **遵守事項 2.2.4(1)(e)「学外の者から報告を受けるための窓口を整備」について**

  例として、外部の者が本学の情報セキュリティ対策の不備を発見した場合、本学へ

の攻撃のおそれ等を認知した場合、学外の者に情報セキュリティ上の脅威を与えていることを認知した場合（与えるおそれがある場合を含む）等に、学外の者から連絡を受ける体制を整備することを求めている。

- **遵守事項 2.2.4(1)(f)「対処手順が適切に機能することを訓練等により確認」について**

  情報セキュリティインシデントは定常的に発生するものではないが、実際に発生した場合には、本学の事務に大きな影響をもたらすおそれがあるため、迅速かつ的確に対処を行うことが求められる。そのため、定めた対処手順が適切に機能することを訓練等によって確認しておくことが重要である。

  訓練等には、実際に使用する機器を利用した「実機訓練」や、逐次の状況付与を請けて判断等を行う「ロールプレイング」、状況設定の上で手順の検証を行う「シミュレーション」といった大掛かりなもののほか、より簡易な「ウォークスルー」や「机上チェック」といった手法も存在する。CSIRT の取組状況や職員の習熟度等に応じて、必要な訓練等を検討し実施することが望まれる。

- **基本対策事項 2.2.4(1)-2「意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等」について**

  例えば、本学 LAN 内での不正プログラム感染拡大やそれに伴う情報流出等が疑われる場合には、被害の拡大を阻止する措置を直ちに講ずることが重要である。そのような場合において、情報の重要度、情報が失われた場合のリスク、業務継続方法等を勘案した上で、調整等に時間をかけず直ちにネットワークを遮断するなどの措置を講ずるため、その手続や対象範囲等を事前に定めておくことが考えられる。これらの基準や手続は、政府機関を取り巻くサイバー攻撃事例や情報セキュリティインシデント事例を基に、適時見直すことが求められる。

遵守事項

(2) 情報セキュリティインシデントへの対処

(a) 事務従事者は、**情報セキュリティインシデントの可能性を認知した場合には、本学の報告窓口に報告**し、指示に従うこと。

(b) CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うこと。

(c) CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、**全学総括責任者に速やかに報告**すること。

(d) CSIRT は、情報セキュリティインシデントに関係する部局総括責任者に対し、被害の拡大防止等を図るための**応急措置の実施及び復旧に係る指示又は勧告を行う**こと。

(e) 部局技術責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、本学で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処すること。

(f) 部局技術責任者は、認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処すること。

(g) CSIRT は、本学の情報システムについて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、**所管官庁等に連絡**すること。また、認知した情報セキュリティインシデントが**サイバー攻撃又はそのおそれのあるもの**である場合には、当該**情報セキュリティインシデントの内容に応じ**、**警察への通報・連絡等**を行うこと。さらに、国民の生活、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態等又はその可能性がある事態においては、「大規模サイバー攻撃等への初動対処について（平成 22 年 3 月 19 日内閣危機管理監決裁）」に基づく報告も行うこと。

(h) CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて**対処全般に関する指示、勧告又は助言**を行うこと。

(i) CSIRT は、情報セキュリティインシデントに関する対処の内容を記録すること。

(j)CSIRT は、情報セキュリティインシデントに関して、本学を含む関係機関と**情報共有を行う**こと。

【 基本対策事項 】

<2.2.4(2)(b)関連>

2.2.4(2)-1 CSIRT は、情報セキュリティインシデントではないと評価した場合であっても、注意喚起が必要と考えられるものについては、関係する者に情報共有を行うこと。

<2.2.4(2)(d)関連>

2.2.4(2)-2 CSIRT 責任者は、認知した情報セキュリティインシデントの種類や規模、影響度合い等を勘案し、必要に応じて、CSIRT、情報セキュリティインシデントの当事者

部局、その他関連部局の役割分担を見直すこと。

（解説）

- **遵守事項 2.2.4(2)(a)「情報セキュリティインシデントの可能性を認知した場合には、本学の報告窓口に報告」について**

  事務従事者に、情報セキュリティインシデントであることを判断した上で報告させることは、判断誤りによる報告漏れにつながるため、その可能性を認知した段階で報告を求める必要がある。報告窓口に報告する内容には、情報セキュリティインシデントの防止策を無効化したり、すり抜けられたりすることにより、被害に至らないまでも蓋然性が高まった状態も含まれる。例えば、不審な電子メールの添付ファイルを開いたり、URL をリンクしたりしてしまった場合や、機密性の高い情報を保存したモバイル端末の所在が不明であるが、紛失したことや盗難されたことが確定的でない状況や、平時の情報システムの利用において確認されないはずのエラーメッセージが端末に表示されるなどが想定される。

- **遵守事項 2.2.4(2)(c)「全学総括責任者に速やかに報告」について**

  情報セキュリティインシデントの性質上、全ての状況が判然とするまでに時間がかかるものであるため、一度の報告で完了することはまれである。例えば、未確定情報を含んだ状態で第一報として報告し、その後に第二報、第三報と続けるような、適切な頻度で報告内容を更新する報告運用が望ましい。その場合、何が確定し、何が未確定であるのかを明らかにすることが望ましい。全ての情報が確定するまで待って報告を遅らせるようなことは、あってはならない。

- **遵守事項 2.2.4(2)(d)「応急措置の実施及び復旧に係る指示又は勧告」について**

  応急措置や復旧に当たっては、情報セキュリティインシデントが発生した情報システムの停止、ネットワークの遮断等について、被害の拡大可能性、証拠保全、業務継続等を勘案し、CSIRT 責任者の判断で指示又は勧告をする。この場合には、情報セキュリティを推進する部局が CSIRT 責任者の指示又は勧告を支援することが望ましい。

  なお、応急措置や復旧に関して、事前に決められた手順がある場合はその手順に従うことが求められる（「（解説）基本対策事項 2.2.4(1)-2『意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等』について」を参照のこと。）。

- **遵守事項 2.2.4(2)(g)「所管官庁等に連絡」について**

  所管官庁等の連絡内容としては、以下が考えられる。

  - 情報セキュリティインシデントが発生した部署
  - 報道発表及び報道の有無
  - 他部署への被害波及の可能性
  - 業務への影響
  - 発生日時とその内容
  - 復旧状況及び復旧見込み

  連絡方法については、「（解説）遵守事項 2.2.4(2)(c)『全学総括責任者に速やかに報告』

について」と同様に、適切な頻度で連絡内容を更新することが望ましく、全ての情報が確定するまで待って報告を遅らせるようなことは、あってはならない。

- **遵守事項 2.2.4(2)(g)「サイバー攻撃又はそのおそれのあるもの」について**

サイバー攻撃の例としては、不正侵入、改ざん、不正コマンド実行、情報かく乱、ウイルス攻撃、サービス不能攻撃等が挙げられる。また、「そのおそれのあるもの」とは、明らかなサイバー攻撃の痕跡が発見されていなくても、単なる機器の故障や操作上の誤りではなく、サイバー攻撃により発生した情報セキュリティインシデントであることが疑われる場合のことである。

- **遵守事項 2.2.4(2)(g)「情報セキュリティインシデントの内容に応じ」について**

サイバー攻撃又はそのおそれがある情報セキュリティインシデントを認知した場合で、当該情報セキュリティインシデントが犯罪に該当するときには、警察への通報・連絡等を求めるものである。明らかなサイバー攻撃に限らず、そのおそれがある場合についても、被害拡大の防止の観点から、可能な限り速やかな通報等を行うことが望ましい。

- **遵守事項 2.2.4(2)(g)「警察への通報・連絡等」について**

「通報・連絡等」の内容としては、相談、届出、告訴又は告発を想定している。

サイバー攻撃又はそのおそれがある情報セキュリティインシデントが発生した場合、当該サイバー攻撃等による被害の拡大を防止するとともに、攻撃者を追跡するため、警察が的確に初動措置を講ずる必要があることから、可能な限り速やかな通報・連絡等を求めている。

なお、その通報先は、各都道府県警察のサイバー攻撃対策部門であり、具体的には、警視庁では公安部公安総務課、道府県警察では警備部のサイバー攻撃対策担当課である。また、警察への通報に関する質問等については、警察庁警備局警備企画課において受け付けている。

- **遵守事項 2.2.4(2)(g)「「大規模サイバー攻撃事態等への初動対処について（平成 22 年 3 月 19 日内閣危機管理監決裁）」に基づく報告連絡」について**

国民の生命、身体、財産又は国土に重大な被害が生じ、又は生じるおそれがある緊急事態に際して政府一体となった初動対処体制をとる必要があることから、内閣官房副長官補（事態対処・危機管理担当）付等に関連情報等を迅速に報告連絡することとしている。

- **遵守事項 2.2.4(2)(g)「対処全般に関する指示、勧告又は助言」について**

本学における情報セキュリティインシデント発生時の対処として、以下のプロセスが想定される。CSIRT には、これらの対処が迅速かつ的確に行われるように、対処状況を把握し、必要に応じて指示、勧告又は助言を行うことが求められる。

・検知／連絡受付
  - 情報セキュリティインシデントの可能性の報告受付
・トリアージ

- 報告された情報セキュリティインシデントの可能性に関する状況確認
- 状況確認結果に基づく情報セキュリティインシデントであるか否かの評価
- 対処する情報セキュリティインシデントの優先順位付け（事案が多発している場合等）

・インシデントレスポンス
- 応急措置の実施
- 被害規模・範囲等の特定を含む状況分析
- 関係部局、セキュリティベンダ等の外部組織
- 復旧対応の実施
- 情報セキュリティインシデントの原因調査と原因が生じた理由の究明
- 再発防止策の検討

・報告／情報公開
- 全学総括責任者への報告
- 所管官庁等への連絡
- 警察等の関係組織への通報・連絡・報告等
- 報道発表等の対外対応

● **遵守事項 2.2.4(2)(g)「情報共有を行う」について**

政府機関における情報共有の枠組みとしては、「政府におけるサイバー攻撃等への対処態勢の強化について」（平成 22 年 12 月 27 日情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ）において、「各府省庁は、その業務において得たサイバー攻撃に係る情報を、可能な限り速やかに内閣官房情報セキュリティセンターに連絡する。また、内閣官房情報セキュリティセンターは、収集・集約された情報をサイバー攻撃に対する初動対処、被害の拡大防止及び再発防止に活用するため、情報連絡を行った府省庁の同意を得た上で、各府省庁に対して積極的な情報提供を行う」と記載されている。

遵守事項

(3) 情報セキュリティインシデントの再発防止・教訓の共有

(a) 部局総括責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として全学総括責任者に報告すること。

(b) 全学総括責任者は、部局総括責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示すること。

(c) CSIRT 責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.2.4(3)(a)「再発防止策を検討」について**

一般に、再発防止策を定めるには、十分な原因調査を行い、どのような要素が絡んで情報セキュリティインシデントに至ったのか、因果関係を明らかにした上で、原因から情報セキュリティインシデントの発生段階の間で、因果関係の進行を断ち切るための防護策を複数検討し、講ずることが有効である。また、対策については、情報セキュリティインシデントが発生したシステム単独で講ずるよりも、他のシステムにも同様に展開することにより（水平展開）、類似事案の発生を組織全体にわたって食い止めることが可能となる。

なお、水平展開については、自らの組織の再発防止策に限らず、他組織の事案を参照することにより、事後対処よりも先んじた未然防止が可能となり、対応コストの低減も期待される。

さらに、再発防止策は、情報システムの利用手順で対策する方法及び情報システムへの情報セキュリティ機能の実装による対策を部局技術責任者へ求める方法の両面から検討し、必要な対策を定めて実施する必要がある。情報システムへの情報セキュリティ機能の実装には一定の時間を要することも考えられることから、利用手順による対策を暫定的に実施し、その後、機能追加により本格的な対策を行うなど段階的な実施も考慮する必要がある。

- **遵守事項 2.2.4(3)(b)「再発防止策を実施するために必要な措置」について**

全学総括責任者は、情報セキュリティインシデントの再発防止策の報告を受けた場合は、その内容を確認する必要がある。

情報システムへの情報セキュリティ機能の実装等計画的に実施する必要がある再発防止策については、対策推進計画に反映させるなどして、適切に実施させるよう取組を推進することが求められる。また、本学全体として再発防止策を講ずることが有効

と想定される場合は、本学全体での取組を進めることも求められる。

- **遵守事項 2.2.4(3)(c)「得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有」について**

  CSIRT 責任者には、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に対し、単に情報セキュリティインシデントの情報を共有するだけでなく、情報セキュリティインシデントの対処を踏まえ、統括情報セキュリティ責任者が定める対処手順等の改善や、個別の情報システムの情報セキュリティ水準の改善につなげられるような事項を含めて共有することが求められる。

2.3　点検

2.3.1　情報セキュリティ対策の自己点検

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ関係規程の遵守状況等を点検し、その結果を把握・分析することが必要である。

自己点検は、事務従事者が自らの役割に応じて実施すべき対策事項を実際に実施しているかどうかを確認するだけではなく、組織全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要である。

また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

遵守事項

(1) 自己点検計画の策定・手順の準備

(a) 全学実施責任者は、対策推進計画に基づき年度自己点検計画を策定すること。

(b) 部局総括責任者は、事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(1)(a)「年度自己点検計画を策定」について**

点検を実施するに当たり、対策推進計画に基づき適切に実施するため、実施頻度、実施時期、確認及び評価の方法や自己点検項目等を定めた年度自己点検計画を策定することが求められる。

自己点検項目の選定に当たっては、前年度に情報セキュリティインシデントが発生した事案や、前年度の自己点検実施率が低かった遵守事項等、様々な選択肢が考えられる。

- **遵守事項 2.3.1(2)(b)「事務従事者」について**

本規定における「事務従事者」は、一般の職員以外に部局総括責任者、職場情報セキュリティ責任者及び部局技術責任者等、情報セキュリティ対策の体制ごとの責任者を含む。具体的にどの責任者を対象に自己点検を実施するかについては、年度自己点検計画で策定する。

部局総括責任者や職場情報セキュリティ責任者は、所管する組織の情報セキュリティ対策について、部局技術責任者は、所管する情報システムについて、区域情報セキュリティ責任者は、所管する区域における情報セキュリティ対策について実施するなど、役割に応じて異なることに留意が必要である。

なお、部局技術責任者の点検は、情報システムに係る各種セキュリティ対策の実施

状況等の点検を様々な観点で実施することが必要である。例えば、ソフトウェアの脆弱性への対処状況の点検であれば、セキュリティパッチや不正プログラム定義ファイルの更新状況を把握したり、実際の文書を確認したりすることで実施状況を把握するなど、代替の確認方法を含めた点検が考えられる。

- **遵守事項 2.3.1(1)(b)「自己点検票」について**

  各事務従事者が自己点検を実施するに当たっては、各自の業務における情報の取扱方法や、実施すべき情報セキュリティ対策上の役割が異なるため、それぞれの職務内容に即した自己点検票が必要となる。そのため、部局総括責任者は、事務従事者ごとの自己点検票を作成するとともに、自己点検の正確性を高めるために詳細な実施手順を準備することが重要である。

遵守事項

(2) 自己点検の実施

(a) 部局総括責任者は、年度自己点検計画に基づき、事務従事者に自己点検の実施を指示すること。

(b) 事務従事者は、部局総括責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(2)(a)「自己点検の実施」について**

  自己点検は、年に２度以上の頻度で実施することが望ましい。例えば、情報システム部門に対しては、毎月実施し、それ以外の部門に対しては、半年に一度の頻度で実施するなどが考えられる。

遵守事項

(3) 自己点検結果の評価・改善

(a) 全学実施責任者及び部局総括責任者は、事務従事者による自己点検結果を分析し、評価すること。全学実施責任者は評価結果を全学総括責任者に報告すること。

(b) 全学総括責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、全学実施責任者及び部局総括責任者に改善を指示し、改善結果の報告を受けること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.3.1(3)(b)「自己点検結果を全体として評価」について**

事務従事者による自己点検の結果については、部局総括責任者が評価し、さらに、部局総括責任者の自己点検の結果を全学実施責任者が評価する。

評価においては、自己点検が正しく行われていること、事務情報セキュリティ対策基準に準拠していること、改善すべき事項が改善されていること、対策が有効であること等を評価する。この自己点検の評価においても、数値評価を中心とし、客観性を持った評価とすることが望ましい。例えば、自己点検実施率（対策実施数／自己点検回答数）等の把握が挙げられる。

2.3.2 情報セキュリティ監査

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。

また、監査の結果で明らかになった課題を踏まえ、全学総括責任者は、部局総括責任者に指示し、必要な対策を講じさせることが重要である。

遵守事項

(1) 監査実施計画の策定

(a) 情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定めること。

(b) 情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施の指示を、全学総括責任者から受けた場合には、追加の監査実施計画を定めること。

【 基本対策事項 】

＜2.3.2(1)(a)関連＞

2.3.2(1)-1 情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定すること。

a) 監査の目的（例：自己点検の適切性を監査すること等）
b) 監査の対象（例：監査の対象となる組織、情報システム、業務等）
c) 監査の方法（例：自己点検結果を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、事務情報セキュリティ対策基準及び実施手順とする）
d) 監査の実施体制（例：監査責任者、監査実施者の所属、氏名）
e) 監査の実施時期（例：対象ごとの実施時期）

（解説）

- **遵守事項 2.3.2(1)(a)「対策推進計画に基づき監査実施計画を定める」について**

遵守事項 2.1.2(2)(a)に規定する対策推進計画には、監査の基本的な方針として、重点とする監査の対象及び目標（今年度の監査でどのような部分を重視するかを明確にする）・監査の実施時期・監査業務の管理体制等を簡潔に記載することを想定している。監査の基本的な方針の案は、情報セキュリティ監査責任者が作成することを想定している。また、情報セキュリティ監査責任者は、対策推進計画に基づき、個別の監査実施計画を策定し、監査を実施する。

- **遵守事項 2.3.2(1)(b)「追加の監査実施計画を定める」について**

全学総括責任者は、学内外における注目すべき情報セキュリティインシデントが発生した場合又は情報セキュリティ対策の実施内容に重大な変更が生じた場合等において、本学の実態を把握するため、追加的に監査の実施を求めることが想定される。この監査の実施の指示を受けた場合、情報セキュリティ監査責任者は、対策推進計画に基づき策定した監査実施計画のほかに、当該指示に係る監査実施計画を策定することとしている。

- **基本対策事項 2.3.2(1)-1「監査実施計画」について**

対策推進計画に基づき実施すべき監査についての詳細な計画として、監査実施計画を策定する必要がある。監査実施計画に記載すべき項目としては、基本対策事項 2.3.2(1)-1 に例示のとおり、監査の目的、対象、方法、実施体制及び実施時期等が考えられる。この他に経済産業省「情報セキュリティ監査基準 実施基準ガイドライン Ver1.0」等にも詳細が説明されているので参考にするとよい。

参考：経済産業省「情報セキュリティ監査基準 実施基準ガイドライン Ver1.0」
（http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex05.pdf）

被監査部門に対して監査の内容や範囲を明確化するために、監査実施期間、監査実施者の氏名、監査対象等を含む事項等を、情報セキュリティ監査責任者より事前通知することが望ましい。

なお、監査実施者が監査過程で情報セキュリティの向上につながる対策等の監査以外の行為を行った場合には、その行為に対する別途の監査が必要となる可能性がある。したがって、情報セキュリティ監査責任者は、情報セキュリティ対策の向上になり得る行為や、作業を効率的に行うことにつながる行為であるとしても、監査以外の行為を監査実施計画の中に取り込むべきではない。

遵守事項

(2) 監査の実施

(a) 情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む監査の実施を監査実施者に指示し、結果を**監査報告書**として全学総括責任者に報告すること。

(ア) 事務情報セキュリティ対策基準及び情報セキュリティ監査規程に**統一基準を満たすための適切な事項が定められていること**

(イ) 実施手順が事務情報セキュリティ対策基準に準拠していること

(ウ) 自己点検の適正性の確認を行うなどにより、被監査部門における**実際の運用**が情報セキュリティ関係規程に準拠していること

【 基本対策事項 】

＜2.3.2(2)(a)(ア)関連＞

2.3.2(2)-1 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、**被監査部門から独立した者**から選定し、情報セキュリティ監査実施者に指名すること。

2.3.2(2)-2 情報セキュリティ監査責任者は、組織内における監査遂行能力が不足等している場合には、**学外の者に監査の一部を請け負わせる**こと。

（解説）

- **遵守事項 2.3.2(2)(a)「監査報告書」について**

監査報告書の作成に際しては、根拠となる監査調書を適切に作成することが必要である。監査調書とは、情報セキュリティ監査実施者が行った監査業務の実施記録であって、監査報告書に記載する監査意見の根拠となるべき監査証拠、その他関連資料等をつづり込んだものをいう。情報セキュリティ監査実施者自らが直接に入手した資料や試験の結果、被監査部門側から提出された資料のほか、場合によっては外部の第三者から入手した資料等を含むことがある。

監査の結果は、監査報告書として文書化した上で、全学総括責任者へ確実に提出する必要がある。監査報告書には、事務情報セキュリティ対策基準及び情報セキュリティ監査基準に統一基準を満たすための適切な事項が定められているか、実際の運用状況が情報セキュリティ関係規程に準拠して行われているかなどの結果を記載する。さらに、監査の過程において、情報セキュリティ対策の内容の妥当性に関連して改善すべき課題及び問題点が検出された場合には、この検出事項や助言・提案を監査報告書に含める。反対に組織として推奨すべき優れた取組等がある場合には、それらを組織全体に広めるなどの助言・提案があってもよい。

- **遵守事項 2.3.2(2)(a)(ア)「統一基準を満たすための適切な事項が定められていること」について**

事務情報セキュリティ対策基準及び情報セキュリティ監査規程に、統一基準を満たすための適切な事項が定められているか否かを判断する際には、本学の組織の目的・

規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性等を踏まえ、必要な事項が事務情報セキュリティ対策基準及び情報セキュリティ監査規程に盛り込まれているか否かを確認する必要がある。このため、事務情報セキュリティ対策基準の策定に当たり、事務情報セキュリティ対策基準に各事項を盛り込んだ理由や本ガイドラインの基本対策事項との関係等について記録を残しておくと、監査の際に有用である。

- **遵守事項 2.3.2(2)(a)(ウ)「実際の運用」について**

  自己点検の適正性の確認や自己点検結果に基づく担当者への質問、記録文書の査閲及び機器の設定状況の点検等の方法により、運用の準拠性を確認する。また、必要に応じて、被監査部門において実施されている情報セキュリティ対策が有効に機能しているか否かを確認することも求められる。例えば、監査対象によってはソフトウェアやウェブアプリケーション等の情報システムに関連する脆弱性の検査、情報システムに対する侵入検査といった方法によっても確認することができる。

- **基本対策事項 2.3.2(2)-1「被監査部門から独立した者」について**

  情報セキュリティ監査実施者には、監査人としての独立性及び客観性を有することが求められる。例えば、情報システムを監査する場合に、当該情報システムの構築をした者や運用を行っている者が監査をしてはならない。また、情報の取り扱われ方に関する監査を行う場合には、当該情報を取り扱う者はその監査をしないこととする。

- **基本対策事項 2.3.2(2)-2「学外の者に監査の一部を請け負わせる」について**

  情報セキュリティ監査責任者は、監査を実施するに当たり、学内に情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮することが重要である。また、監査業務を外部事業者に請け負わせることは、外部委託に該当することから、関連する規定にも留意する必要がある。また、情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の業務への関与等を考慮することが望ましい。

  参考：経済産業省「情報セキュリティ監査企業台帳に関する規則」
  http://www.meti.go.jp/policy/netsecurity/docs/isaudit/audit_register_regulation.pdf

遵守事項

(3) 監査結果に応じた対処

(a) 全学総括責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を部局総括責任者に指示すること。

(b) 部局総括責任者は、監査報告書等に基づいて全学総括責任者から改善を指示されたことについて、必要な措置を行った上で**改善計画を策定**し、措置結果及び改善計画を全学総括責任者に報告すること。

【 基本対策事項 】

＜2.3.2(3)(a)関連＞

2.3.2(3)-1 全学総括責任者は、監査報告書の内容を踏まえ監査を受けた部門以外の部門においても同種の課題又は問題点がある可能性が高く、並びに緊急に同種の課題又は問題点があることを確認する必要があると判断した場合には、他の部門の部局総括責任者に対しても、同種の課題又は問題点の有無を確認するように**指示**すること。

（解説）

- **遵守事項 2.3.2(3)(b)「改善計画を策定」について**

  部局総括責任者が、監査報告書に基づいて全学総括責任者からの改善を指示されたことについて、改善計画の策定及び全学総括責任者への報告を求める事項である。部局総括責任者は、監査報告書において指摘された課題及び問題点の改善が困難であることについて正当な理由がある場合には、その影響を低減させるための補完措置を示した上で、達成することが可能な対処計画を全学総括責任者へ報告する。

- **基本対策事項 2.3.2(3)-1「指示」について**

  全学総括責任者は、監査報告書において指摘事項が、他の組織にも同種の課題又は問題点として存在する可能性が高い場合、並びに同種の課題又は問題点の存在を緊急に確認する必要性が高い場合、想定される他の組織についても、調査を求める事項である。

2.4　見直し

2.4.1　情報セキュリティ対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、本学の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、実際の運用において生じた課題、自己点検、監査の結果や情報セキュリティに係る重大な変化等を踏まえ、保有する情報及び利用する情報システムに係る驚異の発生の可能性及び顕在化時の損失等を分析し、リスクを評価し、適時見直しを行う必要がある。

また、情報セキュリティに係る取組をより一層推進するためには、上記のリスク評価の結果を対策推進計画に反映することも重要である。

遵守事項

(1) 情報セキュリティ関係規程の見直し

(a) 全学総括責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、全学情報システム運用委員会の審議を経て、事務情報セキュリティ対策基準について必要な見直しを行うこと。

(b) 全学実施責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について全学総括責任者に報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.4.1(1)(a)「情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価」について**

本学における情報セキュリティインシデントの発生状況、例外措置の申請状況、自己点検や情報セキュリティ監査の結果、事務従事者からの相談等を踏まえ、事務情報セキュリティ対策基準に課題及び問題点が認められるか否かなどの観点から総合的な評価を行い、事務情報セキュリティ対策基準について所要の見直しを行うことについて、全学総括責任者に求めている。

また、本部監査において助言された事項に関し、事務情報セキュリティ対策基準を見直す必要があるか否かを確認し、必要とされる場合には事務情報セキュリティ対策基準の見直しを行う。

- **遵守事項 2.4.1(1)(b)「整備した者に対して規定の見直しを指示」について**

本学における情報セキュリティインシデントの発生状況、自己点検や情報セキュリ

ティ監査の結果、本部監査の結果、事務従事者からの相談、全学総括責任者からの指示等を踏まえ、情報セキュリティ対策に関する実施手順を見直すことの必要性を検討し、部局技術責任者等の実施手順を整備した者に、その見直しを指示することを全学実施責任者に求めている。

なお、策定済みの実施手順を見直すだけではなく、例えば、学内における共通のルールが存在しないため、各所属等において個別にルールを定めて運用しているなどの場合について、学内における共通のルールを整備するか否かを検討することも考えられる。

遵守事項

(2) 対策推進計画の見直し

(a) 全学総括責任者は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、全学情報システム運用委員会の審議を経て、対策推進計画について定期的な見直しを行うこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 2.4.1(2)(a)「情報セキュリティ対策の運用及び点検・監査等を総合的に評価」について**

  本学における情報セキュリティインシデントの発生状況、自己点検、情報セキュリティ監査の結果、事務従事者からの相談等を踏まえ、対策推進計画に加えるべき事項の有無、策定済みの計画の変更が必要であるか等の観点から、評価を行う。

  また、本部監査において助言された事項において、対策推進計画に盛り込むべき事項がある場合は、当該事項の実施優先順位を検討した上で、適切に計画に盛り込むこととする。

- **遵守事項 2.4.1(2)(a)「情報セキュリティに係る重大な変化等」について**

  サイバー攻撃の量的な拡大や攻撃手法の高度化等による質的な変化等、計画策定時に前提としていた条件から大きく異なり、情報セキュリティに係るリスクが高まった場合や、年度途中における種々の要因により、当初の対策推進計画では課題解決が図られていない場合等を想定している。

第3部 情報の取扱い

3.1 情報の取扱い

3.1.1 情報の取扱い

目的・趣旨

高等教育機関の事務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下、本項において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての事務従事者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、事務従事者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

なお、秘密文書の管理に関しては、文書ガイドラインの規定を優先的に適用した上で、当該ガイドラインに定めが無い情報セキュリティ対策に係る事項については、本基準の規定に基づき、適切に情報が取り扱われるよう留意すること。

遵守事項

(1) 情報の取扱いに係る規定の整備

(a) 全学実施責任者は、以下を含む情報の取扱いに関する規定を整備し、事務従事者へ周知すること。

（ア） 情報の**格付及び取扱制限についての定義**

（イ） 情報の**格付及び取扱制限の明示等**についての手続

（ウ） 情報の格付及び取扱制限の継承、見直しに関する手続

【 基本対策事項 】

＜3.1.1(1)(a)関連＞

3.1.1(1)-1 全学実施責任者は、情報の取扱いに関する規定として、以下を例とする**手順を整備**すること。

a) 情報のライフサイクル全般にわたり必要な手順（高等教育機関の事務の遂行以外の目的での情報の利用等の禁止等）

b) 情報の入手・作成時の手順

c) 情報の利用・保存時の手順

d) 情報の提供・公表時の手順

e) 情報の運搬・送信時の手順

f) 情報の消去時の手順

g) 情報のバックアップ時の手順

＜3.1.1(1)(a)(イ)関連＞

3.1.1(1)-2 全学実施責任者は、情報の格付及び取扱制限の**明示の方法**について、以下を例に、規定を整備すること。

h) 電磁的記録として取り扱われる情報に明示する場合
- 電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載
- 電磁的ファイル等の取扱単位ごとにファイル名自体へ記載
- フォルダ単位等で取り扱う情報は、フォルダ名に記載
- 電子メールで取り扱う情報は、電子メール本文又は電子メール件名に記載

i) 外部電磁的記録媒体に保存して取り扱う情報に明示する場合
- 保存する電磁的ファイル又は文書等の単位ごとに記載
- 外部電磁的記録媒体本体に記載

j) 書面に印刷されることが想定される場合
- 書面のヘッダ部分等に記載
- 冊子等の単位で取り扱う場合は、冊子の表紙、裏表紙等に記載

k) 既に書面として存在している情報に対して格付や取扱制限を明示する場合
- 手書きによる記入
- スタンプ等による押印

3.1.1(1)-3 全学実施責任者は、情報の格付及び取扱制限の**明示を省略**する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、規定を整備すること。

＜3.1.1(1)(a)(ウ)関連＞

3.1.1(1)-4 全学実施責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例に、規定を整備すること。

a) 情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付及び取扱制限を継承する。

b) 既存の情報に、より機密性の高い情報を追加するときは、格付及び取扱制限を見直す。

c) 機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直す。

d) 情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。

e) 完全性及び可用性については、作成時又は**複製時に適切な格付を決定**する。

f) 他者が決定した情報の格付及び取扱制限を**見直す必要がある場合**には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下本項において「決定者等」という。）に確認を求める。

（解説）

- **遵守事項 3.1.1(1)(ア)「格付及び取扱制限についての定義」について**

「統一基準 1.2 (1) 情報の格付の区分」及び「統一基準 1.2 (2) 情報の取扱制限」に

て規定している情報の格付及び取扱制限の定義に基づき、機密性、完全性、可用性に係る情報の格付と取扱制限について、本学の基準を整備する必要がある。取扱制限については、1.5 節(2)【参考】**取扱制限の例**も参照のこと)。

なお、文書管理ガイドラインにおいて、「文書の作成者は、当該文書が極秘文書又は秘文書に該当すると考えられる場合には、それぞれに準じた管理を開始する」とされており、指定前の秘密文書も、機密性３情報として管理することが求められる。

- **基本対策事項 3.1.1(1)(イ)「格付及び取扱制限の明示等」について**

秘密文書においては、文書管理ガイドラインにおける「秘密文書表示」を行った場合には、別途「機密性３情報」に係る明示等を行う必要はない。

- **基本対策事項 3.1.1(1)-1「手順を整備」について**

a)～g)は、遵守事項 3.1.1(2)～(8)における事務従事者を名宛人とした対策事項とそれぞれ対応している。本事項では、これらの内容を包含する形で手順を定めることを求めている。

- **基本対策事項 3.1.1(1)-2「明示の方法」について**

当該情報を参照する者が、情報の格付及び取扱制限を確実に視認することができるよう、当該情報に記載することによる明示を原則とする。また、情報の格付及び取扱制限の明示については、以下の事項についても留意すること。

  - 本文において格付を明示することに加え、ファイル名の先頭に格付を付す。（例：「【機２】○○整備計画」）
  - 格付及び取扱制限の明示と併せて、情報の作成者又は入手者の氏名、所属、連絡先等も記載する。
  - 文書の一部の情報に取扱制限を追加するときは、追加する取扱制限を当該情報に近接した場所に明記する。
  - 電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記する。
  - 文書の作成者名、組織名その他の記録に使用できる「プロパティ」に格付の区分を記載することは明示に当たらない。

- **基本対策事項 3.1.1(1)-3「明示を省略」について**

情報の格付及び取扱制限を確実に視認することができるよう、当該情報に明示しておくことが原則ではあるが、必要な場合には、以下を例に明示が省略可能な条件について定めておくとよい。

  - 情報システムに記録される情報の格付及び取扱制限を当該情報システムの手順書等により明記し、当該情報システムの利用者にあらかじめ周知している場合。
  - 情報の格付及び取扱制限の省略時における当該情報の格付及び取扱制限の取扱について、取扱手順に規定し、事務従事者にあらかじめ周知している場合。ただし、格付及び取扱制限の明示を省略した場合には、以下の事項に注意する必要がある。
    - 格付及び取扱制限の省略を認識できない者への情報の提供

格付の区分及び取扱制限が明示されていない要保護情報を、格付及び取扱制限の決定内容を認識できない事務従事者に提供する必要が生じた場合（例えば、他本学に情報を提供等する場合）は、当該情報に格付の区分及び取扱制限を明示した上で提供するなどしなければならない。

- 取扱制限の明示を省略した場合における取扱制限の追加・変更
  例えば、ある文書の取扱制限の明示を省略している場合であって、当該文書の一部に取扱制限を追加するときは、追加する取扱制限を明示すること。

- **基本対策事項 3.1.1(1)-4 e)「複製時に適切な格付を決定」について**

複製された情報は、一般的には完全性１情報及び可用性１情報と考えられるが、原本を複製し、それをバックアップファイルとして保存する場合も考えられるため、完全性及び可用性については、適宜、複製の目的に応じて格付を決定する必要がある。

- **基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について**

利用する元の情報への修正、追加又は削除のいずれでもないが、元の格付又は取扱制限そのものがその時点で不適当と考える場合には、格付又は取扱制限の見直しについてその決定者に確認を求める必要がある。また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は当該決定者の上司に相談し、その是非を検討することになる。決定者等による見直しが無い限り、当該情報の利用者がこれらの者に無断で、格付又は取扱制限を変更することは許されない。

なお、見直しを行わなければならない場合については、以下を参考に規定すること。

- 作成時には要機密情報だった情報の機密性が失われた場合（時間の経過により変化した場合）
- 機密性３情報として格付けされている資料等から機密性３情報に係る部分を全て削除した場合
- 取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合
- 取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合
- 格付及び取扱制限を決定した時の判断が不適切であったと考えられる場合
- 行政文書管理規則等が、情報の作成又は入手時以降に改定されており、当該行政文書管理規則等における情報の取扱いに変更がある場合

遵守事項

(2) 情報の目的外での利用等の禁止

(a) 事務従事者は、自らが担当している高等教育機関の事務の遂行のために必要な範囲に限って、情報を利用等すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 3.1.1(2)(a)「情報を利用等」について**

情報は、高等教育機関の事務の目的を達成するために利用等するのであって、高等教育機関の事務の遂行以外の目的で情報を利用等すべきではない。国立大学法人法 第18条 第1項においても、「国立大学法人の役員及び職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後も、同様とする。」と定められている。

情報の目的外利用に当たる場合としては、例えば、業務上知り得た情報をソーシャルメディアサービスの個人アカウントの掲示板等に掲示するなどの行為が考えられる。その他にも、情報の利用形態は様々であり、注意が必要である。

なお、本規定で対象としている情報は、事務従事者が従事する業務において利用する本学の情報システムから入手可能な業務に係る情報（業務上知り得る情報）や、情報システムにおいて利用される主体認証情報であり、情報システムの仕様やデータ設定等に係る情報も含んでいる。一方、業務時間外に自宅等の私物端末から本学のウェブサイトにアクセスして、公表されている情報を入手するなどの行為については、本規定の対象とはしていない。

遵守事項

(3) 情報の格付及び取扱制限の決定・明示等

(a) 事務従事者は、情報の作成時及び学外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき**格付及び取扱制限を決定**し、明示等すること。

(b) 事務従事者は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を**継承**すること。

(c) 事務従事者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下この項において**決定者等**という。）**に確認し、その結果に基づき見直す**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 3.1.1(3)(a)「格付及び取扱制限を決定」について**

格付及び取扱制限が不十分な場合、情報漏えい等のリスクが高まるが、一方で、情報の利用を円滑に行うためには、格付及び取扱制限を必要以上に高くしないことが必要である。そのため、格付及び取扱制限を決定する際には、本学の基準に照らして、要件に過不足が生じないようにすること。例えば、機密性１情報に相当する公開しても差し支えない情報をむやみに要保護情報に決定すると、過度な保護対策を求めることになり、高等教育機関の事務の効率的な運営に支障をきたすおそれがある。

また、他機関との情報の受け渡しを行う際には、事務情報セキュリティ対策基準との格付定義の差分に関する情報を当該機関から得るなどして、本学の基準との差分について考慮の上、格付及び取扱制限を決定する必要がある。

- **遵守事項 3.1.1(3)(b)「継承」について**

業務資料等を参考に新たに別の資料を作成する場合等において、元となった資料等に記載されていた情報の機密性に関する格付及び取扱制限について、新たに作成した資料等に適切に引き継ぐことを求めている。例えば機密性３情報を他の資料等に転用する場合においては、当該資料に記載されている転用部分については機密性３情報として取り扱われるべきである。また、要保全情報又は要安定情報を複製する場合については、複製された情報に対して過度な保護対策を求めないように、完全性１情報又は可用性１情報として格付を見直し再決定することが望ましい。ただし、バックアップを原本として情報を保管する目的で複写する場合は、要保全情報とすべきであるなど、状況に応じた適切な判断が求められる。

- **遵守事項 3.1.1(3)(c)「決定者等に確認し、その結果に基づき見直す」について**

「（解説）基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について」を参照の

こと。

遵守事項

(4) 情報の利用・保存

(a) 事務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

(b) 事務従事者は、機密性３情報について要管理対策区域外で情報処理を行う場合は、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。

(c) 事務従事者は、要保護情報について**要管理対策区域外で情報処理**を行う場合は、必要な安全管理措置を講ずること。

(d) 事務従事者は、**保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること**。

(e) 事務従事者は、USB メモリ等の**外部電磁的記録媒体**を用いて情報を取り扱う際、**定められた利用手順**に従うこと。

【 基本対策事項 】

＜3.1.1(4)(a)関連＞

3.1.1(4)-1 事務従事者は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱うこと。

a) 要保護情報を**放置しない**こと。

b) 要機密情報を**必要以上に複製しない**こと。

c) 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。

d) 電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。

e) 情報の**保存方法を変更**する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずる。

3.1.1(4)-2 事務従事者は、入手した情報の格付け及び取扱制限が不明な場合には、情報の作成元または入手元への確認を行う。

（解説）

- **遵守事項 3.1.1(4)(c)「要管理対策区域外で情報処理」について**

学外で開催される会議への出席時等に、要機密情報を用いて情報処理を行う場合は、のぞき見の防止や不要となった情報の削除等の安全管理措置を講ずるなど、情報の格付や取扱制限に応じて適切な安全管理措置を講ずる必要がある。

- **遵守事項 3.1.1(4)(d)「保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること」について**

情報システムに、ファイルに対する書込権限者の制限や、ファイルのセキュリティ設定でパスワード設定等のアクセス制御機能が装備されている場合、当該情報の格付

及び取扱制限に従って、必要なアクセス制御の設定を行うことが求められる。例えば、取扱制限として閲覧範囲の制限が指定されている場合は、第三者等から参照されないよう、読取制限の属性を付与することや、要保全情報であれば、第三者等から変更されないよう、上書き禁止の属性を付与することがこれに当たる。

アクセス制御は、サーバ装置、端末、OS、アプリケーション、ファイル等を単位に行うことができるため、これらを選択し組み合わせて、適切なアクセス制御を実現するとよい。

なお、文書管理ガイドラインの秘密文書の管理に関するモデル要領において、「秘密文書については、インターネットに接続していない電子計算機又は媒体等に保存し、暗号化等による保護を行うとともに、当該秘密文書を記録する電子計算機、媒体等について、保存を金庫等で行うなどにより物理的な盗難防止措置を施すこと。秘文書については、インターネットからの侵入に対する多重防御による情報セキュリティ対策が施された電子計算機でも保存することができる。」とされている。

- **遵守事項 3.1.1(4)(e)「外部電磁的記録媒体」について**

  外部電磁的記録媒体には、USB メモリ等の、繰返し情報を書き換えできる媒体と、CD-R 等の書き換えできない媒体が存在する。特に前者の媒体を利用する場合は、不正プログラムに感染するおそれが大きいため、その取扱いには細心の注意を払う必要がある。（具体的な対策等については、【参考 8.1.1-1】を参照のこと。）

- **遵守事項 3.1.1(4)(e)「定められた利用手順」について**

  遵守事項 8.1.1(1)(c)において定められた利用手順を指す。

- **基本対策事項 3.1.1(4)-1 a)「放置しない」について**

  悪意ある第三者等による不正な操作や盗み見等を防止することを求める事項である。例えば、離席する際には、ロック付きスクリーンセーバを起動する又はログアウトして画面に情報を表示しない、机の上に書類を放置して長時間離席しない、印刷した書面を速やかに回収し出力トレイに放置しないこと等を徹底する必要がある。

- **基本対策事項 3.1.1(4)-1 b)「必要以上に複製しない」について**

  電磁的記録は比較的容易に複製することができるという特性があり、可用性の観点から複製された情報が多数の端末に散在する傾向になることが想定されるため、機密性３情報に該当しない情報であっても、複製は必要最小限にとどめるよう留意する必要がある。

  なお、秘密文書に関しては、文書管理ガイドラインにおいて、「秘密文書の複製等は必要最小限にとどめること。」と定められていることに留意すること。

- **基本対策事項 3.1.1(4)-1 i)「保存方法を変更」について**

  当該情報が記載されている行政文書が歴史公文書等に該当する場合は、情報の取扱制限を解除するか、利用の制限についての意見を付すなどして移管する必要がある。その際、パスワードを設定していた場合は解除するなどして、移管先がその内容を参照できるように配慮する必要がある。

遵守事項

(5) 情報の提供・公表

(a) 事務従事者は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。

(b) 事務従事者は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。

(c) 事務従事者は、電磁的記録を提供又は公表する場合には、当該電磁的記録の付加記録等からの不用意な情報漏えいを防止するための措置を講ずること。

【 基本対策事項 】

＜3.1.1(5)(d)関連＞

3.1.1(5)-1 事務従事者は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

（解説）

- **遵守事項 3.1.1(5)(a)「機密性１情報に格付されるもの」について**

保有する情報をウェブサイト等により広く国民に提供する場合、公表しようとする情報の格付の適正さを再度検討し、格付及び取扱制限の明示を削除するなどを考慮する必要がある。

なお、情報の公表ではないものの、電子調達システム等において調達情報を委託先候補事業者に閲覧を許可する場合が考えられる。情報システムの構成図等サイバー攻撃を企図する者が有利になるような情報については、開示対象者と機密保持契約を締結するなどして厳重な管理のもと閲覧を許可するなどして、細心の注意を払う必要がある。

- **遵守事項 3.1.1(5)(b)「決定者等に相談」について**

「（解説）基本対策事項 3.1.1(1)-4 f)「見直す必要がある場合」について」を参照のこと。

- **遵守事項 3.1.1(5)(b)「提供先において」・「適切に取り扱われるよう」について**

要保護情報を学外の者に提供する場合には、提供先において当該情報が適切に取り扱われるように、情報の取扱い上の留意事項を提供先へ確実に伝達する必要がある。

伝達方法としては、他本学や委託先等の情報の提供先に、事務情報セキュリティ対策基準や情報の取扱いに関する手順書、統一基準との格付定義の差分に関する説明等を提示し、格付や取扱制限に応じた取扱方法を示す方法が考えられる。この場合、格付の区分だけを示しても、提供先においては当該格付区分がどのように取り扱われるべきものであるか認識できない可能性があるため、当該格付の区分の定義について提

供先にあらかじめ周知しておく必要がある。また、提供する情報を適切に管理するために必要な措置が具体的に分かるようにする（例えば、「委員以外への再配布を禁止する」と明示する。）など、格付以外の方法で取扱方法を示すことも考慮する必要がある。

また、格付及び取扱制限の明示が省略されている場合においても、提供先にて情報が適切に取り扱われるよう、明示の省略が可能とされている情報の格付及び取扱制限を当該書面又は電磁的記録に明記するなどの措置を講ずる必要がある。

- **遵守事項 3.1.1(5)(d)「不用意な情報漏えい」について**

情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDF ファイルの「しおり」等に残留した不要な情報を除去する必要がある。

また、ソフトウェアを用いて文書の特定の部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

遵守事項

(6) 情報の運搬・送信

(a) 事務従事者は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。ただし、他本学の要管理対策区域であって、全学実施責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域と見なすことができる。

(b) 事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

【 基本対策事項 】

＜3.1.1(6)(a)関連＞

3.1.1(6)-1 事務従事者は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、**セキュアな運送サービス**を提供する運送事業者により運搬すること。

＜3.1.1(6)(a)(b)関連＞

3.1.1(6)-2 事務従事者は、要機密情報である電磁的記録を要管理対策区域外に運搬又は学外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。

a) **運搬又は送信する情報を暗号化する**。
b) 運搬又は送信を**複数の情報に分割して**それぞれ異なる経路及び手段を用いる。
c) 主体認証機能や暗号化機能を備える**セキュアな外部電磁的記録媒体**が存在する場合、これに備わる機能を利用する。

＜3.1.1(6)(b)関連＞

3.1.1(6)-3 事務従事者は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。

a) 本学管理の通信回線を用いて送信する。
b) **信頼できる通信回線**を使用して送信する。
c) VPN を用いて送信する。
d) S/MIME 等の暗号化された電子メールを使用して送信する。
e) 本学独自で運用するなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。

（解説）

- **基本対策事項 3.1.1(6)-1「セキュアな運送サービス」について**

セキュアな運送サービスとしては、受領印が必要となる書留郵便や、専用車両による配達サービス、配達状況の追跡が可能なサービス等が存在する。

- **基本対策事項 3.1.1(6)-2 a)「運搬又は送信する情報を暗号化する」について**

  暗号化された情報の復号に用いる鍵は、十分な長さと複雑さを有することが求められる。また、暗号化された情報の復号に用いる鍵を、暗号化された情報と同じ経路で送信等したり、第三者が容易に知り得る方法で送信等したりしてしまうと、第三者によって情報が復号されるおそれが高くなると考えられることから、暗号化された情報の復号に用いる鍵は、暗号化された情報とは別の方法で送信するなどして秘匿性を確保することが考えられる。

- **基本対策事項 3.1.1(6)-2 b)「複数の情報に分割して」について**

  例えば、１個の電子情報について、分割された一方のデータからは情報が復元できない方法でファイルを２個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方を DVD、USB メモリ等の外部電磁的記録媒体で郵送する方法が考えられる。

- **基本対策事項 3.1.1(6)-2 c)「セキュアな外部電磁的記録媒体」について**

  セキュアな外部電磁的記録媒体が備える機能としては、主体認証機能、暗号化機能の他、不正プログラムの検閲・駆除機能、遠隔データ消去機能及び接続管理機能等がある。USB メモリ等の外部電磁的記録媒体の運搬に当たっては、必要最小限の情報のみを保存するよう留意するとともに、盗難・紛失等による情報漏えいに備え、当該機能を適切に利用することが必要である。

- **基本対策事項 3.1.1(6)-4 b)「信頼できる通信回線」について**

  空港や商業施設等が提供する無線 LAN 等の通信回線は、十分なセキュリティ対策が採られていない場合もあるため、要保護情報を送信する場合にこれを用いるべきではない。

遵守事項

(7) 情報の消去

(a) 事務従事者は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。

(b) 事務従事者は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。

(c) 事務従事者は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 3.1.1(7)(a)「速やかに情報を消去」について**

情報セキュリティの観点からは、不正プログラム感染による情報窃取や操作ミスによる情報漏えい等を防ぐ観点から、職務上不要となった情報を速やかに消去する必要があるが、その際には、公文書管理法等で保存が求められる情報を誤って消去しないよう、注意を払う必要がある。

- **遵守事項 3.1.1(7)(b)「抹消する」について**

「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。電磁的記録媒体に記録されている情報を抹消するための方法としては、例えば、次の方法が挙げられる。

  - データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法
  - ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法
  - 媒体を物理的に破壊する方法

また、媒体を物理的に破壊する方法としては、例えば、次の方法が挙げられる。

  - （フロッピーディスク等の磁気媒体の場合）当該媒体を切断するなどして情報を記録している内部の円盤を破壊する方法
  - （CD-R/RW、DVD-R/RW 等の光学媒体の場合）カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法
  - （媒体全般）メディアシュレッダーやメディアクラッシャー等の専用の機器を用いて破壊する方法

また、ファイルの情報に別の情報を上書きした場合であっても、特殊な手段を用いることにより残留磁気から当該情報を復元される可能性があるため、特に機密性の高い情報の抹消に当たっては、留意する必要がある。

なお、事務従事者自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と抹消の措置を行う者を情報システム又は課室等の組織の単位で定めて実施してもよい。

- **遵守事項 3.1.1(7)(c)「復元が困難な状態にする」について**

電磁的記録の抹消と同様に、書面が不要となった場合には、シュレッダーによる細断処理、焼却、溶解等により、復元が困難な状態にする必要がある。

なお、廃棄すべき書類が大量にあるなどの理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃棄処理証明書の取得等により、書面が確実に廃棄されていることを確認するとよい。また、無人の執務室に設置されている又は設置場所及び利用場所が確定していないなどの環境で利用される情報システム、外部電磁的記録媒体等については、不要な情報を可能な限り抹消しておくことが望ましい。

遵守事項

(8) 情報のバックアップ

(a) 事務従事者は、情報の格付に応じて、**適切な方法で情報のバックアップを実施する**こと。

(b) 事務従事者は、取得した情報のバックアップについて、**格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め**、適切に管理すること。

(c) 事務従事者は、保存期間を過ぎた情報のバックアップについては、本項(7)の規定に従い、適切な方法で消去、抹消又は廃棄すること。

【 基本対策事項 】

＜3.1.1(8)(a)関連＞

3.1.1(8)-1 事務従事者は、要保全情報又は要安定情報である電磁的記録又は重要な設計書について、バックアップを取得すること。

＜3.1.1(8)(b)関連＞

3.1.1(8)-2 事務従事者は、要保全情報、要安定情報である電磁的記録のバックアップ又は**重要な設計書**のバックアップの保管について、**災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定する**こと。

（解説）

- **基本対策事項 3.1.1(8)(a)「適切な方法で情報のバックアップを実施する」について**

  災害や情報セキュリティインシデントが発生し、サーバ装置等の電磁的記録が使用不可能になった際の復旧に備えて、要保全情報や要安定情報に格付される情報等の重要な情報を外部の記録媒体へバックアップすることを求めている。以下の例を参考に、情報のバックアップ方法について考慮するとよい。

  - バックアップの対象（対象とするシステム、データ、ソフトウェアその他）
  - バックアップの範囲（フルバックアップ、差分バックアップ等）
  - バックアップを保存する電磁的記録媒体等の種類
  - バックアップの周期、世代管理の方法
  - 使用するバックアップツール
  - バックアップデータの秘匿性確保、改ざん防止の方法

- **基本対策事項 3.1.1(8)(b)「格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め」について**

  バックアップデータに要機密情報が含まれる場合は、バックアップデータの盗難・紛失による情報漏えい等を回避するために、バックアップデータを要管理対策区域に保管することが望ましい。また、バックアップデータを保存する媒体の耐久性にも留意し、定期的に媒体を新しいものに入れ替えるなども考慮するとよい。

- **基本対策事項 3.1.1(8)-2「重要な設計書」について**

  情報システムの委託先から書面のみで提示された設計書類等、情報システムに記録

されていない書面のみの情報であって、紛失、改ざん等により情報システムの運用に支障を及ぼす可能性のあるものを指している。バックアップが外部に流出することにより、攻撃者に有利になるものについては、保管の際に機密性を確保することにも留意する必要がある。

- **基本対策事項 3.1.1(8)-2「適切なバックアップの手段又は保管場所」について**

災害等を想定してバックアップを取得する場合は、バックアップを耐火性のある保管庫や耐震性の高い施設、同時被災しない遠隔地に保管すること等も考えられる。また、遠隔地に保管するに当たっては、実際にバックアップを用いた復旧に要する時間が、情報システム運用継続計画における復旧目標時間内に納まるよう、緊急時のバックアップデータの配送手段、配送時間等を考慮し、保管場所を決定する必要がある。

3.2　情報を取り扱う区域の管理

3.2.1　情報を取り扱う区域の管理

目的・趣旨

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

したがって、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

遵守事項

(1)　要管理対策区域における対策の基準の決定

(a)　全学実施責任者は、**要管理対策区域の範囲を定める**こと。

(b)　全学実施責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。

(ア)　許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。

(イ)　許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための**入退管理対策**。

【 基本対策事項 】

＜3.2.1(1)(b)(ア)(イ)関連＞

3.2.1(1)-1　全学実施責任者は、以下を例とする、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を定めること。

a）下表のとおり、３段階のクラスを定める。

クラス	説明
クラス３	一部の限られた者以外の者の立入りを制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス２	事務従事者以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対策区域

※便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。

3.2.1(1)-2　全学実施責任者は、クラス１の区域について、以下を含む施設の整備、設備の

設置等の物理的な対策及び入退管理対策の基準を定めること。

a) 不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。

b) 不特定の者が容易に立ち入らないように、**立ち入る者の身元、訪問目的等の確認を行うための措置**を講ずること。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。

c) クラス２以上の区域に不正に立ち入った者を容易に判別することができるように、以下を含む措置を講ずること。

- 事務従事者は、身分証明書等を着用、明示する。クラス２及びクラス３の区域においても同様とする。
- 一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス２及びクラス３の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。

3.2.1(1)-3 全学実施責任者は、クラス２の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

a) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。ただし、窓口のある執務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は事務従事者が窓口を常に目視できるような措置を講ずること。

b) クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠すること。

c) **クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置**を講ずること。

3.2.1(1)-4 全学実施責任者は、クラス３の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。

a) クラス３の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分すること。

b) **クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置**を講ずること。

c) クラス３の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにすること。

d) 一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずること。業者が作業を行う場合は立

会いや監視カメラ等により監視するための措置を講ずること。

3.2.1(1)-5 全学実施責任者は、以下を例とする、区域への**クラスの割当ての基準**を定めること。

a) クラスの割当ての基準を以下のように定める。

- サーバ室や日常的に機密性が高い情報を取り扱う執務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス３を割り当てる。
- 一般的な執務室や執務室内の会議室には、事務従事者以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス２を割り当てる。

（解説）

- **遵守事項 3.2.1(1)(a)「要管理対策区域の範囲を定める」について**

執務室やサーバ室のほか、複数の本学で共用する会議室や事務従事者が書面やモバイル端末等を運搬するときの安全性を高めるために、執務室間や会議室に接続されている廊下等も要管理対策区域に含めることを考慮してもよい。

なお、要管理対策区域外で高等教育機関の事務を行う必要がある場合には、施設及び環境に係る対策が講じられないことから情報の漏えい等の可能性が高くなる。情報の漏えい等の可能性を低減するためには、要管理対策区域外でのモバイル端末の利用に関する遵守事項（7.1.1 項「端末」の遵守事項 7.1.1(1)(a)(b)、8.1.1 項「情報システムの利用」の遵守事項 8.1.1(1)(b)等）を参照し、適切な対策を行うことが必要である。

- **遵守事項 3.2.1(1)(b)(イ)「入退管理対策」について**

基本対策事項 3.2.1(1)-2～4 に示した対策の基準のほか、以下を対策の基準に含めてもよい。

- 共連れ（立入りを許可された者が立ち入る際に、立入りを許可されていない者を同時に立ち入らせるような行為）を防止する措置を講ずること。具体的な対策として、１人ずつでないと立入り及び退出が不可能な設備の利用、警備員の配置による目視確認等が挙げられる。
- 立入りを許可されていない者の侵入等、区域の安全性が侵害された場合に追跡することができるように、立入り及び当該区域からの退出を記録及び監視する措置を講ずること。「記録及び監視する」具体的な対策として、警備員、監視カメラ等による記録及び監視のほか、要管理対策区域への立入り及び当該区域からの退出を管理する装置における立入り及び退出の記録を取得し、当該立入り及び退出の記録を定期的に確認することが挙げられる。継続的に立入りが許可されている者以外の者の立入りがあった場合には、立入りの記録として立ち入った者の氏名及び所属、訪問目的、訪問相手の氏名及び所属、訪問日、立入り及び退出の時刻を記録することが挙げられる。
- 受渡業者と物品の受渡しを行う場所を制限すること。
  なお、「受渡業者」とは、事務従事者との物品の受渡しを行う者をいう。物品の

受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

- **基本対策事項 3.2.1(1)-2 b)「立ち入る者の身元、訪問目的等の確認を行うための措置」について**

クラス１の区域に「立ち入る者」について、継続的に立入りを許可された者のほか、一時的に立ち入る者（訪問者）がある。継続的に立入りを許可された者として、事務従事者や一定期間立入りを認められ、認められたことを示す許可証（入館カード等）が貸与されている業者等を想定している。また、一時的に立ち入る者として、不定期に訪れる来客や受渡業者等を想定している。

「身元、訪問目的等の確認を行うための措置」の具体的な対策として、以下が挙げられる。

- セキュリティゲートの設置、警備員や受付係等の配置をして立ち入る者に身分証明書等の提示を求める。
- 一時的に立ち入る者の氏名及び所属、訪問目的等を記録する。

- **基本対策事項 3.2.1(1)-3 c)「クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置」について**

具体的な対策として、以下が挙げられる。

- 継続的に立入りが許可されている者に IC カードを貸与して IC カードによる主体認証を行う。
  なお、IC カード等による主体認証を行う機能を設けた場合は、立ち入る者の主体認証情報の管理に関する規定の整備、当該主体認証情報の読取防止のための措置を講ずることが望ましい。
- 継続的に立入りが許可されている者以外の者が立ち入る場合は、立入りを許可する者が自ら区域の境界まで迎えに行く。
- 立入りを監視する警備員、受付係等を配置している場合は、許可する者が警備員等にあらかじめ一時的に立ち入る者の氏名及び所属、訪問目的、訪問相手の氏名及び所属、訪問日時等を伝えておき、一時的に立ち入る者が来訪した際に警備員、受付係等が照合する。

クラス２の区域への立入り時の「許可された者であることの確認」について、クラス１の区域への立入り時に「身元、訪問目的等の確認」ではなく「許可された者であることの確認」を行っている場合においては、それをもって代替してもよい。

- **基本対策事項 3.2.1(1)-4 c)「クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置」について**

具体的な対策として、以下が挙げられる。

- 継続的に立入りが許可されている者に IC カードを貸与して IC カードによる主体認証を行う。
- 継続的に立入りが許可されている者以外の者が立ち入る場合は、立入りを許可する者が自ら区域の境界まで迎えに行く。
- 継続的に立入りが許可されている者のみに、常時施錠される扉の鍵を貸与した

り、解錠するための暗証番号を通知したりしておき、鍵の所持や入力した暗証番号の一致により、確認する。

- **基本対策事項 3.2.1(1)-5「クラスの割当ての基準」について**

各区域へのクラスの割当ての基準の策定に当たっては【参考 3.2.1-1】を参考にするとよい。本基本対策事項においては、例としてサーバ室や日常的に機密性が高い情報を取り扱う執務室にはクラス３、一般の執務室や執務室内の会議室にはクラス２を割り当てるという基準を示している。

全学実施責任者は、区域情報セキュリティ責任者に、管理する区域で取り扱う情報、設置される情報システムの特性から、外部からの侵入があった場合の被害の大きさを考慮してクラスを決定させる必要があることを踏まえ、本基本対策事項で示す基準を参考とし、クラスの割当ての基準を定める必要がある。

また、高等教育機関の事務の単位でクラスの割当ての基準（例：○○、××に関係する高等教育機関の事務を行う執務室はクラス３、これら以外の高等教育機関の事務を行う執務室はクラス２）を定めておくことも考えられる。

図に示した割当てはあくまで例示であって、実際の割当ては自組織の状況に応じた形で行うことでよい。たとえば、施設内であっても実質的に不特定の者の立ち入りが制限できない区域については、クラス０を割当てることになる。また、施錠可能な執務室であれば、鍵の管理が適切に行われることを前提として、クラス２もしくはクラス３として扱うことが可能である。

【参考 3.2.1-1】 要管理対策区域へのクラスの割当ての例

要管理対策区域へのクラスの割当ての例を図 3.2.1-1～3 に示す。

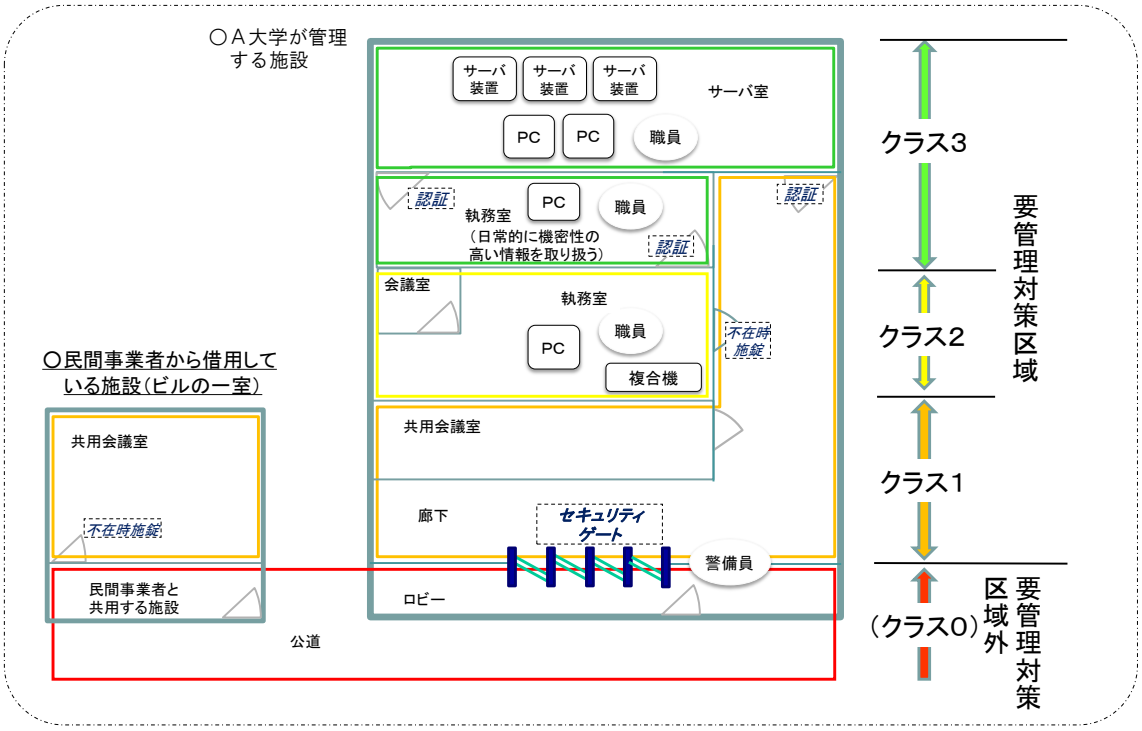


図 3.2.1-1 要管理対策区域へのクラスの割当ての例１
（本学施設又は民間事業者から借用する施設）

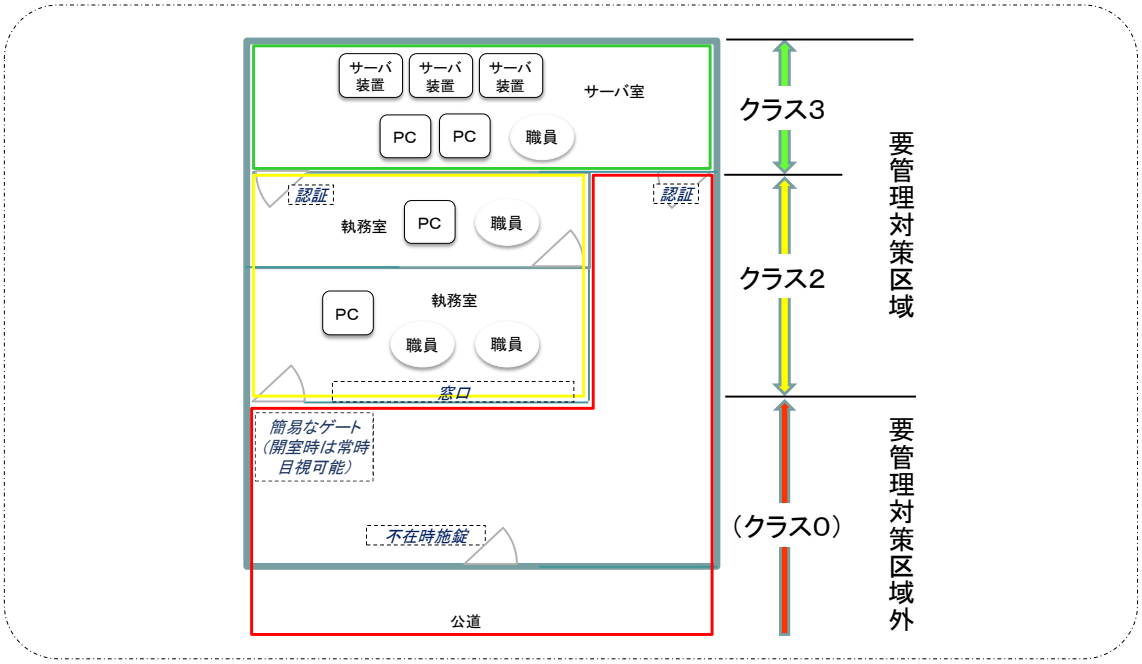


図 3.2.1-2 要管理対策区域へのクラスの割当ての例２（窓口のある執務室）

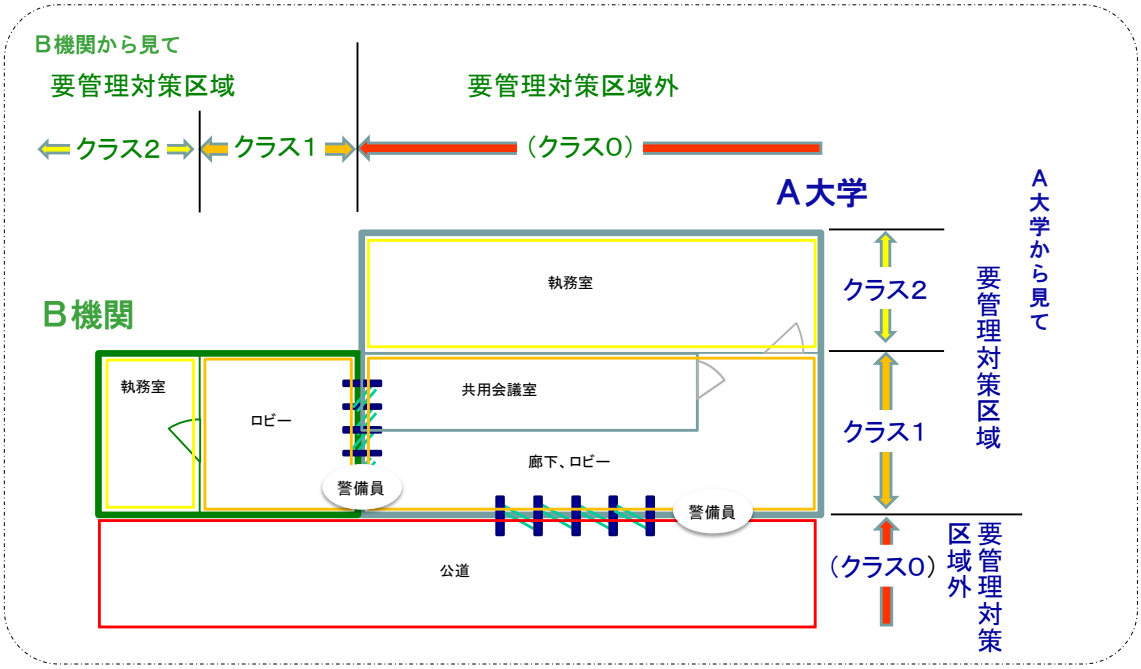


図 3.2.1-3 要管理対策区域へのクラスの割当ての例３
（他機関と共用する施設）

遵守事項

(2) 区域ごとの対策の決定

(a) 部局総括責任者は、全学実施責任者が定めた対策の基準を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定めること。

(b) 区域情報セキュリティ責任者は、管理する区域について、全学実施責任者が定めた対策の基準と、周辺環境や当該区域で行う高等教育機関の事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。

【 基本対策事項 】

＜3.2.1(2)(b)関連＞

3.2.1(2)-1 区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う高等教育機関の事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定すること。

（解説）

- **遵守事項 3.2.1(2)(a)「施設及び環境に係る対策を行う単位ごとの区域を定める」について**

  複数の部局で共用する廊下等の施設については、庁舎管理の観点での各部門の管理範囲を確認した上で「施設及び環境に係る対策を行う単位ごとの区域」を定めるとよい。共用する施設の区域情報セキュリティ責任者の定め方については、「(解説) 遵守事項 2.1.1(4)(b)「区域情報セキュリティ責任者」について」を参照のこと。

- **基本対策事項 3.2.1(2)-1「割り当てるクラスを決定する」について**

  クラス３、クラス２以外の要管理対策区域はクラス１となることにも留意して決定する必要がある。クラス１の区域は、不特定の者が容易に立ち入れない程度の安全性が確保された区域である。したがって、原則として、盗難や盗み見等への対策が講じられていない端末や書面が置かれる区域にクラス１を割り当ててはならない。クラス１の区域に端末を置く必要がある（例：来訪者受付に来訪者の個人情報が保存されている端末を置く）場合には、セキュリティワイヤ等で固定することや、常時目視により監視するなどの措置を講ずる必要がある。

- **基本対策事項 3.2.1(2)-1「当該区域において実施する対策を決定する」について**

  周辺の区域のクラスや管理状況も確認して具体的な対策を決定するとよい。例えば、クラス３の区域がクラス０の区域と接続している場合は、クラス３の区域の扉の施錠管理をより厳重にすることが考えられる。また、民間事業者が管理するビルの部屋を借りて高等教育機関の事務を行っているような場合は、当該ビルの共用部分等では十分な対策が講じられないことが想定される。そのような場合には、借用している部屋

の入退管理の強化や共用施設での高等教育機関の事務の禁止を徹底すること等により、安全性を高めることが重要である。

なお、必要な対策が庁舎管理等の別の仕組みにより実施されている場合については、その対策をもって代替しても構わない。

- **基本対策事項 3.2.1⑵-1「個別の対策」について**

個別の対策については、「(解説) 遵守事項 3.2.1(1)(b)(イ)「入退管理対策」について」に示した例（対策の基準となっていない場合）のほか、以下に示す例を参考に決定するとよい。

- 施設内の案内板等において、サーバ室等の所在の表示を禁止する。
- 外部から室内が見えるような場所にある会議室において、要機密情報の取扱い時はブラインドを閉じる。
- 外部の者が周辺の会議室等へ出入りする時間帯には、執務室の扉を施錠する又は開放しない。
- 低階層の窓際等における無線 LAN の傍受対策を行う。
- ワイヤレスマイクの電波が室外にも到達するような会議室において、要機密情報の取扱い時はワイヤレスマイクの使用を禁止する。
- ディスプレイケーブル等から生ずる電磁波から情報が漏えいするおそれがある場合には電磁波軽減フィルタを取り付ける。
- 飲食物をこぼした際に情報システムの運用上の障害が発生するような場所での飲食を禁止する。
- 情報システムに関係する機器の不正な持ち出しが行われていないかを確認するために定期的又は不定期に施設からの退出時に持ち物検査を行う。
- クラス３の区域の中でもより厳重な管理が必要な区域において、機器の持込み、利用、持ち出しについて制限を設ける。
- 会議室において、重要な情報を取り扱う会議が開催される時間帯には機器の持込み、利用について制限を設ける。

機器の持込み、利用、持ち出しの制限について詳細を以下に示す。

- 「機器の持込み」とは、事務従事者等が、執務室に高等教育機関の事務に関係しない機器を持ち込むことや情報システムが設置される区域に当該情報システムに関係しない機器を持ち込むことを指す。「機器」には、モバイル端末、デジタルカメラ等の撮影機器、IC レコーダー等の録音機器、USB メモリ等の外部電磁的記録媒体等が含まれる。また、私物のスマートフォン等の本学支給以外の機器も含まれる。以下に示すように、利用のみを禁止する対策もあるが、例えば、持ち込まれたスマートフォンが不正プログラムに感染していて、持ち込んだ者の意図に反して撮影や録音をされるという脅威も存在するため、持ち込ませないという対策も考えられる。
- 「機器の利用」とは、事務従事者等が、持ち込んだ機器を利用することを指す。「利用」には、モバイル端末の起動や、デジタルカメラ等による撮影、IC レコーダー等による録音等が含まれる。管理する区域で取り扱う情報の機密性の高

さに応じて、利用の制限を設けるか決めるとよい。スマートフォン等の通常電源をオンにしている機器であれば、立ち入る際に電源をオフにさせるという対策も有効である。

- 「機器の持ち出し」とは、情報システムが設置される区域から当該情報システムに関係する者が、当該情報システムに関係するサーバ装置、端末、外部電磁的記録媒体等を持ち出すことを指す。情報セキュリティインシデント発生時に追跡等できるように、機器の持ち出し時には、持ち出しの記録を取ることが考えられる。記録の内容としては、持ち出しを行う者の氏名及び所属、日時、機器名、事由等が挙げられる。

遵守事項

(3) 要管理対策区域における対策の実施

(a) 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。事務従事者が実施すべき対策については、**事務従事者が認識できる措置を講ずる**こと。

(b) 区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために**物理的な対策**を講ずること。

(c) 事務従事者は、**利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する**こと。また、事務従事者が学外の者を立ち入らせる際には、当該高等教育機関外の者にも当該区域で定められた対策に従って利用させること。

【 基本対策事項 】

＜3.2.1(3)(a)関連＞

3.2.1(3)-1 区域情報セキュリティ責任者は、管理する区域について、以下を例とする利用手順等を整備し、当該区域を利用する事務従事者に周知すること。

a) 扉の施錠及び開閉に関する利用手順

b) 一時的に立ち入る者が許可された者であることを確認するための手順

c) 一時的に立ち入る者を監視するための手順

（解説）

- **遵守事項 3.2.1(3)(a)「事務従事者が認識できる措置を講ずる」について**

当該区域のクラスや当該クラスにおいて事務従事者が実施すべき対策を周知することが考えられる。扉の施錠や一時的に立ち入る者が許可された者であることの確認等の事務従事者に実施させる事項については、利用手順を定めて周知するとよい。

なお、関係者限りで利用する区域については、関係者のみに周知することでも構わない。

- **遵守事項 3.2.1(3)(b)「物理的な対策」について**

地震、火災、停電等の災害から情報システムを保護するための対策を指す。

具体的な対策として、例えば、サーバラックの利用のほか、以下の設備等の設置が挙げられる。

- ハロゲン化物消火設備
- 無停電電源装置
- 自家発電装置
- 空調設備
- 耐震又は免震設備

これらの対策については、必ずしも区域情報セキュリティ責任者単独で実施できるものではないが、例えば、情報システムに関係する対策であれば部局技術責任者、庁舎管理に関係する対策であれば庁舎管理を行う部門の関係者と調整することが求めら

れる。

また、情報システムへの対策として、作業する者が災害によりサーバ装置等に近づくことができない場合に、作業する者の安全性を確保した上で遠隔地からサーバ装置等の電源を遮断できるようにする機能を設けておくことも考えられる。

- **遵守事項 3.2.1(3)(c)「利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する」について**

事務従事者は、自身が所属する高等教育機関が管理する区域を利用する場合は、自本学が定めた対策に従って利用することが求められる。一方、他の高等教育機関が管理する区域を利用する場合には、他の高等教育機関が定めた対策に従って利用する必要がある。

第4部 外部委託

4.1 外部委託

4.1.1 外部委託

目的・趣旨

学外の者に、情報システムの開発、アプリケーションプログラムの開発等を委託する際に、事務従事者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において事務情報セキュリティ対策基準に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

外部委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお、クラウドサービスの利用に係る外部委託については、クラウドサービス特有のリスクがあることを理解した上で、4.1.4 項「クラウドサービスの利用」についても本項に加えて遵守する必要がある。

また、民間事業者が不特定多数向けに約款に基づきインターネット上で提供する情報処理サービス等、1.3 節において「約款による外部サービス」として定義するものを利用し、高等教育機関の事務を遂行する場合も外部委託の一つの形態と考えられるが、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、その際は本項に代えて 4.1.2 項「約款による外部サービスの利用」を適用すること。

＜外部委託の例＞

- 情報システムの開発及び構築
- アプリケーション・コンテンツの開発業務
- 情報システムの運用業務
- 業務運用支援業務（統計、集計、データ入力、媒体変換等）
- プロジェクト管理支援業務等
- 調査・研究業務（調査、研究、検査等）
- 情報システム、データセンター、通信回線等の賃貸借

遵守事項

(1) 外部委託に係る規定の整備

(a) 全学実施責任者は、外部委託に係る以下の内容を含む規定を整備すること。

（ア） 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基

準
（イ） 委託先の選定基準

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.1(1)(a)(ア)「委託先によるアクセスを認める情報及び情報システムの範囲」について**

委託先や第三者による許可されていない情報及び情報システムへのアクセス等が行われないように、委託先におけるそれらの取扱いに関する本学の基準を規定することを求めている。規定すべき内容としては、例えば以下の事項が考えられる。

- 外部委託を許可（又は禁止）する業務又は情報システムの範囲
- 外部委託を許可（又は禁止）する業務又は情報システムの具体的例示（公開ウェブサーバは外部委託可等）
- 格付及び取扱制限その他取り扱う情報の特性に応じた、情報の取扱いを許可（又は禁止）する場所（機密３情報は庁舎外での取扱いを禁止するなど）

特に、委託業務において使用される情報システムが海外のデータセンターに設置されている場合等においては、保存している情報に対して現地の法令等が適用されるため、国内であれば不適切と判断されるアクセスをされる可能性があることに注意が必要である。「独立行政法人の保有する個人情報の保護に関する法律」（平成 15 年法律第 59 号）で定義する個人情報については、国内法が適用される場所に制限する必要があると考えるため、個人情報を取り扱う委託業務においては、保存された情報等において国内法令が適用されること等を外部委託の際の判断条件としておくべきである。

- **遵守事項 4.1.1(1)(a)(イ)「委託先の選定基準」について**

全学実施責任者は、委託先の選定基準の整備に当たって、当該委託先が、事業の継続性を有し存続する可能性が高く、事務情報セキュリティ対策基準の要件を満たしていると判断できる場合に限ること等を前提とすることが重要である。

選定基準としては、委託先が事務情報セキュリティ対策基準の該当項目を遵守し得る者であること、事務情報セキュリティ対策基準と同等の情報セキュリティ管理体制を整備していること、事務情報セキュリティ対策基準と同等の情報セキュリティ対策の教育を委託先の事業従事者に対して実施していること等が挙げられる。

また、本学の情報セキュリティ水準を一定以上に保つために、委託先に対して要求すべき情報セキュリティ要件を学内で統一的に整備することが重要である。

委託先の選定基準策定に当たって、委託先の情報セキュリティ水準の評価方法を整備する際、例えば、ISO/IEC 27001 等の国際規格とそれに基づく認証制度の活用、情報セキュリティガバナンスの確立促進のために開発された自己評価によるツール等の応用も考えられる。その場合、委託先の情報セキュリティ水準の認証に関わる認定・認証機関について、これら機関がマネジメントシステム認証の信頼性向上を目的とし

た取組である「MS 認証信頼性向上イニシアティブ」に参画し、不祥事への対応や透明性確保に係る取組を実施していることを確認することも考えられる。

なお、委託先の選定基準は、法令等の制定や改正等の外的要因の変化に対応して適時見直し、外部委託の実施時に反映することが必要である。

遵守事項

(2) 外部委託に係る契約

(a) 部局技術責任者又は職場情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを**委託先の選定条件とし、仕様内容にも含める**こと。

(ア) **委託先に提供する情報の委託先における目的外利用の禁止**

(イ) 委託先における情報セキュリティ対策の実施内容及び管理体制

(ウ) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による**意図せざる変更が加えられないための管理体制**

(エ) **委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供**

(オ) **情報セキュリティインシデントへの対処方法**

(カ) **情報セキュリティ対策その他の契約の履行状況の確認方法**

(キ) **情報セキュリティ対策の履行が不十分な場合の対処方法**

(b) 部局技術責任者又は職場情報セキュリティ責任者は、委託する業務において**取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること**。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

(c) 部局技術責任者又は職場情報セキュリティ責任者は、委託先がその役務内容を一部**再委託**する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(a)(b)の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本学に提供し、本学の承認を受けるよう、仕様内容に含めること。

【 基本対策事項 】

＜4.1.1(2)(a)関連＞

4.1.1(2)-1 部局技術責任者又は職場情報セキュリティ責任者は、以下の内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させること。また、変更があった場合は、速やかに再提出させること。

a) 当該委託業務に携わる者の特定

b) 当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

4.1.1(2)-2 部局技術責任者又は職場情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む**情報の取扱手順**について委託先と合意し、定められた手順により情報を取り扱うこと。

（解説）

- **遵守事項 4.1.1(2)(a)「委託先の選定条件とし、仕様内容にも含める」について**

一般競争入札の中でも総合評価落札方式で行う場合は、遵守事項 4.1.1(2)(a)の(ア)～(キ)について、評価の際に入札者に対し提出を求めるなど、選定条件を満たしているかの確認をすること。また、事前に評価を行えない最低価格落札方式等で行う場合であっても、仕様書に対する履行能力証明書等を提出させるなどにより、遵守事項 4.1.1(2)(a)の(ア)～(キ)について契約時までに提出することを確約させること。

なお、委託事業の内容によっては、一部の条件が設定不可能な場合や意味をなさない場合も考えられるため、そのような場合には、除外することもやむを得ない。

また、国の安全に関する重要な情報を委託先に取り扱わせることを内容とする外部委託契約については、「調達における情報セキュリティ要件の記載について」（平成 24 年 1 月 24 日、内閣官房副長官から各省庁大臣官房長等あて）に基づく情報セキュリティ要件も当該契約に含めること。

- **遵守事項 4.1.1(2)(a)(ア)「委託先に提供する情報の委託先における目的外利用の禁止」について**

「情報セキュリティ対策に関する官民連携の在り方について」（平成 24 年 1 月 19 日情報セキュリティ対策推進会議 官民連携の強化のための分科会）においては、「国の安全に関する重要な情報を国以外の者に扱わせることを内容とする契約を行う際には、契約方式にかかわらず、契約に係る業務の実施のために国が提供する国の安全に関する重要な情報その他当該業務の実施において知り得た国の安全に関する重要な情報については、情報のライフサイクルの観点から管理方法を定め、その秘密を保持させ、また当該業務の目的以外に利用させない」との旨が記載されている。

- **遵守事項 4.1.1(2)(a)(ウ)「意図せざる変更が加えられないための管理体制」について**

情報システムの開発等の外部委託において、「意図せざる変更が加えられないための管理体制」が確保されることを求めている。

具体的に仕様書等に記載する事項としては、例えば以下が考えられる。

- 情報システムの開発工程において、本学の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。
- 情報システムに本学の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、本学と委託先が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

- **遵守事項 4.1.1(2)(a)(エ)「委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供」について**

遵守事項 4.1.1(2)(a)(ウ)「意図せざる変更が加えられないための管理体制」における管理体制等を確認する際の参照情報として用いるため、提供を求める規定である。

- **遵守事項 4.1.1(2)(a)(エ)「委託事業の実施場所」について**

  データセンター等のスペースを借用して情報システムを設置する場合等では、要安定情報を取り扱う情報システムにおいて、自然災害による影響を考慮し、データセンターの立地条件をあらかじめ考慮しておく必要がある。

  また、委託業務において使用する情報システムが民間事業者等の学外のデータセンターに設置される場合においては、「(解説) 遵守事項 4.1.1(1)(a)(ア)「委託先によるアクセスを認める情報及び情報システムの範囲」について」を参照のこと。

- **遵守事項 4.1.1(2)(a)(オ)「情報セキュリティインシデントへの対処方法」について**

  委託先において発生した情報セキュリティインシデントによる被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について、契約時にあらかじめ委託先と合意しておくとよい。対処方法について合意していないと、インシデントが発生しているにもかかわらず委託先と連絡がつかない、営業時間外の対応を断られるなどのトラブルになるおそれがあるため、可能な範囲で事前に合意しておくことが重要である。

  対処方法には、例えば、復旧を優先する場合は委託業務を一時的に停止するための手順を規定し、業務継続を優先する場合は、委託事業を継続した上で情報セキュリティインシデントに対処する手順について、対処の主体とともに規定することが考えられる。また、情報セキュリティインシデントに係る委託先と本学間の情報エスカレーション方法やそのタイミングについて規定することも考えられる。

- **遵守事項 4.1.1(2)(a)(カ)「情報セキュリティ対策その他の契約の履行状況の確認方法」について**

  委託先における情報セキュリティ対策の水準を維持するためには、その履行状況を委託元が継続的に確認すべきであり、また、履行が不十分である場合に速やかに適切な対処をすべきである。

  情報セキュリティ対策の履行状況を確認するための方法としては、例えば、委託先における情報セキュリティ対策の実施状況について定期的に報告させることや情報セキュリティ監査等が考えられる。情報セキュリティ監査の内容には、請け負わせる業務のうち監査の対象とする範囲、実施者（本学が指定する第三者、委託先が選定する第三者、本学又は委託先において当該業務を行う部門とは独立した部門）、実施方法（情報セキュリティ監査基準の概要、実施場所等）等、当該情報セキュリティ監査を受け入れる場合の委託先の負担及び委託先候補の情報セキュリティポリシーとの整合性等を委託先候補が判断するために必要と考えられる事項を含める。

  情報セキュリティ監査により履行状況を確認する場合は、4.1.1(2)(b)に示す情報セキュリティ監査の受入れを仕様書に明記するとよい。

- **遵守事項 4.1.1(2)(a)(キ)「情報セキュリティ対策の履行が不十分な場合の対処方法」について**

  情報セキュリティ対策の履行が不十分である場合の対処方法としては、例えば、委託先と改善について協議を行い、合意した改善策を実施させること等が考えられる。

また、部局技術責任者又は職場情報セキュリティ責任者自身が契約を行わない場合には、本遵守事項に係る取決めについて、契約する者に対して依頼する必要がある。

- **遵守事項 4.1.1(2)(b)「取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること」について**

  要保護情報を委託先にて取り扱う場合には、必要時に情報セキュリティ対策の履行状況の報告を求めるものである。また、委託先への立入検査又は情報セキュリティに関する監査を実施する場合には、監査の対象とする範囲、実施者及び実施方法等を含む委託先と合意した事項について、契約に含めるなどにより明らかとしておくことが必要である。

  また、要安定情報を取り扱う場合には、サービスレベルの保証について委託先と契約を取り交わすことを検討する必要がある。サービスレベルに関しては、セキュリティ確保の観点からも、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、委託先に保証させることが重要である。

- **遵守事項 4.1.1(2)(c)「再委託先」について**

  「再委託先」には、再委託先の事業者が受託した事業の一部を別の事業者に委託する再々委託等、多段階の委託が行われる場合の委託先を含む。

- **基本対策事項 4.1.1(2)-2「情報の取扱手順」について**

  格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、委託先においても事務情報セキュリティ対策基準に定める内容と同等の取扱いが行われるよう、あらかじめ委託先と合意しておくことが重要である。また、委託先に提供する情報は必要最小限にとどめる必要があるが、情報システムの利用等において目的外の不必要なアクセスが行われる可能性も考慮し、委託先における情報の取扱状況を適宜把握することも重要である。

  なお、委託先において、約款による外部サービス、ソーシャルメディアサービス、クラウドサービス等を用いて委託業務を遂行することが考えられる場合は、統一基準 4.1.2 項、4.1.3 項、4.1.4 項の規定を委託先においても遵守させるよう仕様書等に規定し、委託先とあらかじめ合意しておくことが望ましい。

遵守事項

(3) 外部委託における対策の実施

(a) 部局技術責任者又は職場情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。

(b) 部局技術責任者又は職場情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を事務従事者より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせること。

(c) 部局技術責任者又は職場情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.1(3)(a)「情報セキュリティ対策の履行状況を確認する」について**

  委託先における情報セキュリティ対策の履行状況の確認に際し、情報セキュリティ監査を利用することとした場合には、契約に基づいた監査の範囲及び実施方法に従い、本学自らが情報セキュリティ監査を行う以外に、第三者又は委託先に情報セキュリティ監査を行わせることが考えられる。

- **遵守事項 4.1.1(3)(c)「情報が確実に返却、又は抹消されたことを確認する」について**

  当該遵守事項を事務従事者に求めるに当たり、委託先ともあらかじめ具体的な確認手段を定め、合意しておくことが望ましい。情報が完全に抹消されたことを確認することが困難な場合は、確認書を委託先に提出させるなどの方法も考慮する必要がある。

  情報の抹消については、「（解説）遵守事項 3.1.1(7)(b)「抹消する」について」及び「（解説）遵守事項 5.2.4(1)(a)(イ)「情報の抹消」について」を参照し、確認手段を定めるとよい。

遵守事項

(4) 外部委託における情報の取扱い

(a) 事務従事者は、委託先への情報の提供等において、以下の事項を遵守すること。

(ア) 委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。

(イ) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。

(ウ) 委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに部局技術責任者又は職場情報セキュリティ責任者に報告すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.1(4)(a)「委託先への情報の提供」について**

委託契約開始から終了に至るまでに行う委託先への情報の提供に伴う要機密情報の漏えい等を防止するためには、委託業務に係る事務従事者それぞれが委託先との情報の授受時に情報セキュリティを確保することが重要である。

委託先への情報の提供に関する解説については、「（解説）遵守事項 3.1.1(5)(b)「提供先において」・「適切に取り扱われるよう」について」を参照のこと。

4.1.2 約款による外部サービスの利用

目的・趣旨

外部委託により高等教育機関の事務を遂行する場合は、原則として 4.1.1 項「外部委託」にて規定する事項について、委託先と特約を締結するなどし、情報セキュリティ対策を適切に講ずる必要がある。しかしながら、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合には、民間事業者が不特定多数の利用者向けに約款に基づきインターネット上で提供する情報処理サービス等、1.3 節において「約款による外部サービス」として定義するものを利用することも考えられる。

このような「約款による外部サービス」をやむを得ず利用する場合には、種々の情報を政府機関からサービス提供事業者等に送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断し、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(1) 約款による外部サービスの利用に係る規定の整備

(a) 全学実施責任者は、以下を含む**約款による外部サービス**の利用に関する規定を整備すること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

（ア） **約款による外部サービスを利用してよい業務の範囲**

（イ） **業務に利用する約款による外部サービス**

（ウ） 利用手続及び運用手順

(b) 部局総括責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの**責任者**を定めること。

【 基本対策事項 】

＜4.1.2(1)(a)(ウ)関連＞

4.1.2(1)-1 全学実施責任者は、本学において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定めること。

a) 利用申請の**許可権限者**

b) 利用申請時の申請内容

- 利用する組織名
- 利用するサービス
- 利用目的（業務内容）
- 利用期間
- **利用責任者（利用アカウントの責任者）**

c) サービス利用中の安全管理に係る運用手順

- サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
- 情報の滅失、破壊等に備えたバックアップの取得

- 利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等）

d）情報セキュリティインシデント発生時の連絡体制

（解説）

- **遵守事項 4.1.2(1)(a)「約款による外部サービス」について**

「約款による外部サービス」としては、民間事業者等がインターネット上で不特定多数の利用者（主に一般消費者）に対して提供する電子メール、ファイルストレージ、グループウェア等のクラウドサービスが代表的であり、有料、無料に関わらず、画一的な約款や利用規約等への同意、簡易なアカウントの登録（登録が不要な場合もある）等により利用可能なサービスは、約款による外部サービスとなる。その他にインターネットの検索サービスや辞書サービス等も約款による外部サービスに該当する。

また、事務従事者自身が取得した電子メールアカウント等を業務で利用する場合についても約款による外部サービスの利用に当たる。

このようなサービスは、利用の際の情報管理について保証がないことが一般的であり、不用意な利用によって本学の情報が意図せず漏えいすることが懸念されることから、要機密情報が取り扱われないよう、適切に管理することが重要である。

その他に民間事業者が約款により提供する情報処理に関わるサービスとしては、電気通信サービスや郵便、運送サービス等があるが、これらは「約款による外部サービス」の適用範囲外である。

- **遵守事項 4.1.2(1)(a)(ア)「約款による外部サービスを利用してよい業務の範囲」について**

取り扱う情報の格付及び取扱制限に応じて、情報セキュリティの確保の観点から、約款による外部サービスを利用してよい業務の範囲を定めることを求めている。

約款による外部サービス利用に当たってのリスクには、以下のようなものがある。全学実施責任者は、これらのリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、許可する業務の範囲を決定する必要がある。

- サービス提供者は、保存された情報を自由に利用することが可能である。また、約款、利用規約等でその旨を条件として明示していない場合がある。加えて、サービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にある。
- 情報が意に反して公開されてしまった場合や、情報が改ざんされた場合でも、サービス提供者は一切の責任を負わない。
- サービス提供者が海外のデータセンター等に情報を保存している場合は、保存している情報に対し、現地の法令等が適用され、現地政府機関等から情報にアクセスされる可能性がある。
- 突然サービス停止に陥ることがある。また、その際に預けた情報の取扱いは保証されず、損害賠償も行われない場合がある。約款の条項は一般的にサービス提供者に不利益が生じないようになっており、このような利用条件に合意せざ

るを得ない。また、サービスの復旧についても保証されない場合が多い。
- 保存された情報が誤って消去又は破壊されてしまった場合に、復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。
- 約款及び利用規約の内容が、サービス提供者側の都合で利用開始後事前通知等無しで一方的に変更されることがある。
- 情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。
- 利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、その対応には時間を要することが多い。

なお、本項において、約款による外部サービスで要機密情報を取り扱うことを禁止しているが、例外措置としてやむを得ず要機密情報を約款による外部サービスにおいて取り扱う場合においても、上記リスクを踏まえ、適切な対策を講じた上で利用することが求められる。例えば、海外のデータセンター等に情報を保存し、現地の法令等が適用されることで情報の漏えいにつながるリスクについては、国内にサーバが設置される事業者に委託し、国内法令が適用されることを事前に確認できれば当該リスクを低減することが可能と判断できる。このように、サービス提供者のサービス提供形態により回避可能なリスクもあることから、約款、利用規約等の詳細を確認するなどして例外措置の可否を判断することが重要である。

- **遵守事項 4.1.2(1)(a)(イ)「業務に利用する約款による外部サービス」について**

約款による外部サービスのうち利用可能なサービスについて、以下を例にサービスを特定し、本学の基準として定めることが考えられる。

なお、以下の例は要機密情報を取り扱わないことが前提であることに注意すること。
- サービス約款や利用規約の内容
- サービス事業者の情報セキュリティポリシー及びプライバシーポリシー
- 提供サービスにおけるセキュリティ設定及びプライバシー設定の方法（初期設定を含む。）
- 情報セキュリティインシデント発生時における個別対応の可否（運用実績等を勘案するとよい。）

また、要機密情報を取り扱わない場合であっても、例えば検索サービスの利用においては、インターネット上に政府職員の身分を明らかにして検索ワード等の情報を提供する行為に等しく、膨大な検索ワード等の情報から、政府機関の関心事項等が分析されるおそれがあることに留意しなければならない。検索サービスを業務に利用する組織において特にそのようなリスクが懸念される場合は、上記のサービス提供条件の確認に加えて、インターネット上で利用端末や通信元を匿名化する対策を導入し、システム部門による適切な管理の下で利用すること等を考慮するとよい。

- **遵守事項 4.1.2(1)(b)「責任者」・基本対策事項 4.1.2(1)-1 a)「許可権限者」について**

遵守事項 4.1.2(1)(b)に定める「責任者」と基本対策事項 4.1.2(1)-1 a)に定める「許可権限者」は同一であり、約款による外部サービスを利用する場合において、利用可否を判断する責任者となる。当該責任者は、利用可能なサービスごとに設置され、利用

部門からの申請を受け付けて、申請内容に従い利用を許可することになる。一人の責任者が複数のサービスを所管してもよい。また、当該責任者は、所管する約款による外部サービスについて、約款及び利用規約の変更の有無等について定期的に状況把握することが求められる。

なお、当該責任者には、所管する約款による外部サービスに関する技術的な知見を有し、約款による外部サービスを利用する際に考慮すべきリスクを十分理解し、個々の利用申請に対して適切に判断することが可能な者を充てることが必要である。

- **基本対策事項 4.1.2(1)-1 b)「利用責任者（利用アカウントの責任者）」について**

遵守事項 4.1.2(1)(b)及び基本対策事項 4.1.2(1)-1 a)において定めている責任者（許可権限者）とは別に、約款による外部サービスを利用する際に利用アカウントごとの責任者を利用責任者として定めることを求めている。利用部門において利用責任者を定めることになるが、職場情報セキュリティ責任者、部局技術責任者、又は約款による外部サービスの許可権限者が利用責任者を兼ねるなど、組織の規模や特性に応じて柔軟に定めてよい。

【参考 4.1.2-1】約款による外部サービスの利用申請フローの例

約款による外部サービスの申請手続及び申請許可権限者、運用管理者等の配置例を図 4.1.2-1 に示す。

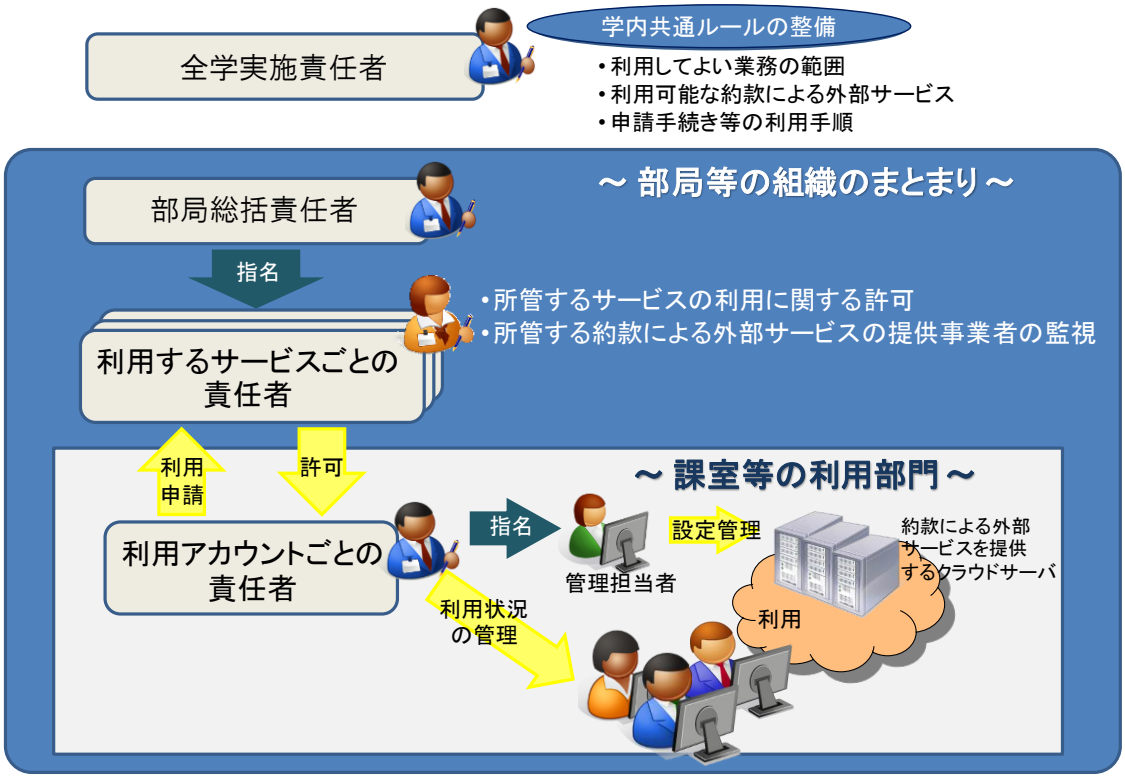


図 4.1.2-1　約款による外部サービスの申請手続及び責任者の役割例

遵守事項

(2) 約款による外部サービスの利用における対策の実施

(a) 事務従事者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 4.1.2(2)(a)「利用に当たってのリスク」について**

個々の高等教育機関の事務の遂行において、約款による外部サービスの利用を検討する際は、当該サービスの約款、利用規約、その他の利用条件を確認し、以下のリスクや課題への対策を明確化した上で、適切に利用の必要性を判断することが必要である。

なお、以下に掲げるリスクの例は、要機密情報を約款による外部サービスにて取り扱わないことを前提としたものであることに注意すること。

- サーバ装置の故障や運用手順誤り等により、サーバ装置上の情報が滅失して復元不可能となるおそれがある。
- サーバ装置上の要保全情報が第三者等により改ざんされ、復元が困難となるおそれがある。
- サービスが突然停止されるおそれがある。
- 約款や利用規約等が予告なく一方的に変更され、セキュリティ設定が変更されるおそれがある。
- 情報の取扱いが保証されず、一旦記録された情報を確実に消去することができないおそれがある。

4.1.3 ソーシャルメディアサービスによる情報発信

目的・趣旨

インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していく様々なソーシャルメディアサービスが普及している。本学においても、積極的な広報活動等を目的に、こうしたサービスが利用されるようになっている。しかし、民間事業者等により提供されるソーシャルメディアサービスは、.example.ac.jp で終わるドメイン名（以下「A 大学ドメイン名」という。）を使用することができないため、真正なアカウントであることを利用者等が確認できるようにする必要がある。また、本学のアカウントを乗っ取られる場合や、利用しているソーシャルメディアサービスが予告なくサービス停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く提供する際には、当該情報を必要とする国民等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により国民等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。

このようなソーシャルメディアサービスは機能拡張やサービス追加等の技術進展が著しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。

なお、ソーシャルメディアサービスの利用は、約款による外部サービスの利用に相当することから、4.1.2 項の規定と同様に、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(1) ソーシャルメディアサービスによる情報発信時の対策

(b) 全学実施責任者は、本学が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する**運用手順等を定める**こと。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。

(ア) 本学のアカウントによる情報発信が実際の本学のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。

(イ) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。

(c) 部局総括責任者は、本学において**情報発信**のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの**責任者**を定めること。

(d) 事務従事者は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、本学の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

【 基本対策事項 】

＜4.1.3(1)(a)関連＞

4.1.3(1)-1 全学実施責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定めること。

a) アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

b) URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

4.1.3(1)-2 全学実施責任者は、本学のアカウントによる情報発信が実際の本学のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定めること。

a) 本学からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、本学が運用していることを利用者に明示すること。

b) 本学からの情報発信であることを明らかにするために、本学が A 大学ドメイン名を用いて管理しているウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

c) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページの URL を記載すること。

d) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

4.1.3(1)-3 全学実施責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定めること。

a) パスワードを適切に管理すること。具体的には、ログインパスワードは十分な長さと複雑さを持たせ、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

b) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

c) ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭ったり

した場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行うこと。

d) ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。

4.1.3(1)-4 全学実施責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定めること。

a) 自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。

b) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織の CSIRT や所管官庁等に報告するなど、適切な対処を行うこと。

（解説）

- **遵守事項 4.1.3(1)(a)「運用手順等を定める」について**

運用手順等を定めるに当たっては、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準を低下させることがないよう留意する必要がある。本学のアカウントにおいて、第三者アカウントの投稿の引用や、第三者が管理又は運用するウェブサイト等へのリンクを掲載することは、当該の投稿やウェブサイト等の内容を信頼性のあるものとして認めていると受け取られることや、リンク掲載後に当該の投稿やウェブサイト等の内容が変更される可能性があることを考慮した上で、慎重に行う必要がある。

- **遵守事項 4.1.3(1)(b)「情報発信」について**

一旦発信した情報は、ソーシャルメディアを通じて瞬時に拡散してしまうため、完全に削除することは不可能となる。このため、当該情報が公開可能な情報であるか否かについて、情報発信する前に十分に確認する必要がある。

- **遵守事項 4.1.3(1)(b)「責任者」について**

遵守事項 4.1.2(1)(b)にて定めている責任者と同等であり、ソーシャルメディアサービスの利用申請を受け付けて、利用を許可する許可権限者となる。申請手順や利用責任者の設置等の運用方法については、4.1.2 項「約款による外部サービスの利用」を参照すること。

4.1.4 クラウドサービスの利用

目的・趣旨

業務及び情報システムの高度化・効率化等の理由から、政府機関において今後クラウドサービスの利用の拡大が見込まれている。クラウドサービスの利用に当たっては、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。クラウドサービスを利用する際、政府機関がクラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、政府機関による委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分考慮することが求められる。

遵守事項

(1) クラウドサービスの利用における対策

(a) 部局技術責任者は、クラウドサービス（民間事業者が提供するものに限らず、政府等が提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、**情報の取扱いを委ねることの可否**を判断すること。

(b) 部局技術責任者は、クラウドサービスで取り扱われる情報に対して**国内法以外の法令が適用されるリスク**を評価して委託先を選定し、必要に応じて**委託事業の実施場所**及び契約に定める準拠法・裁判管轄を指定すること。

(c) 部局技術責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。

(d) 部局技術責任者は、**クラウドサービスの特性**を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めること。

(e) 部局技術責任者は、**クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること**。

【 基本対策事項 】

＜4.1.4(1)(c)関連＞

4.1.4(1)-1 部局技術責任者は、クラウドサービスを利用するに当たり、**サービスの中断や終了時に際し、円滑に業務を移行するための対策**として、以下を例とするセキュリティ対策を実施

することをクラウドサービスの選定条件とし、仕様内容にも含めること。
a) 取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件
b) 取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

＜4.1.4(1)(d)関連＞

4.1.4(1)-2 部局技術責任者は、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティ対策を構築すること。また、対策を実現するために、以下を例とするセキュリティ要件をクラウドサービスに求め、契約内容にも含めること。特に、運用段階で委託先が変更となる場合、開発段階等で設計したクラウドサービスのセキュリティ要件のうち継承が必須なセキュリティ要件について、変更後の委託先における維持・向上の確実性を事前に確認すること。

a) クラウドサービスに係る**アクセスログ等の証跡の保存**及び提供
b) インターネット回線とクラウド基盤の接続点の通信の監視
c) **クラウドサービスの委託先による情報の管理・保管**の実施内容の確認
d) クラウドサービス上の**脆弱性対策**の実施内容の確認
e) クラウドサービス上の情報に係る復旧時点目標（RPO）等の指標
f) クラウドサービス上で取り扱う情報の暗号化
g) 利用者の意思によるクラウドサービス上で取り扱う情報の確実な削除・廃棄
h) 利用者が求める**情報開示請求に対する開示項目や範囲**の明記

（解説）

- **遵守事項 4.1.4(1)(a)「情報の取扱いを委ねることの可否」について**

クラウドサービスの利用に当たっては、情報の管理や処理をクラウドサービス事業者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなる。そこで、適切なクラウドサービス事業者を選定することにより以下のようなリスクを低減することが考えられる。

- クラウドサービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる半面、クラウドサービス事業者の運用詳細は公開されないために利用者にブラックボックスとなっている部分があり、利用者の情報セキュリティ対策の運用において必要な情報の入手が困難である。
- オンプレミスとクラウドサービスの併用やクラウドサービスと他のクラウドサービスの併用等、多様な利用形態があるため、利用者とクラウドサービス事業者との間の責任分界点やサービスレベルの合意が容易ではない。
- クラウドサービス事業者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つのクラウド基盤で共用することとなるため、情報が漏えいするリスクが存在する。
- クラウドサービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスク

が存在する。

- サーバ装置等機器の整備環境がクラウドサービス事業者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易ではない。

なお、情報セキュリティ確保のためにクラウド利用者自らが行うべきことと、クラウドサービス事業者に対して求めるべきこと等をまとめたガイドラインについては、以下の取組を参考にするとよい。

参考：総務省
「クラウドサービス提供における情報セキュリティ対策ガイドライン」
（平成 26 年４月）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html）

参考：経済産業省
「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」、
「クラウドセキュリティガイドライン活用ガイドブック」（平成 26 年３月 14 日）
（http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html）

参考：公益財団法人 金融情報システムセンター
「金融機関におけるクラウド利用に関する有識者検討会報告書」（平成 26 年 11 月 14 日）
（https://www.fisc.or.jp/isolate/?id=759&c=topics&sid=190）

上記のウェブサイトのアドレスは、平成 28 年６月１日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **遵守事項 4.1.4(1)(b)「国内法以外の法令が適用されるリスク」について**

国内法以外の法令が適用されるリスクとして、データセンターが設置されている国が、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取り決めを遵守しないなどのリスクの高い国である場合、データセンター内のデータが外国の法執行機関の命令により強制的に開示される、データセンターの他の利用者等が原因でサーバ装置等の機器が政府機関のデータを含んだまま没収されるなどが考えられる。

- **遵守事項 4.1.4(1)(b)「委託事業の実施場所」について**

バックアップデータ、サーバ装置内のデータ等、政府機関の情報が存在し得る場所全てを委託事業の実施場所として考慮することが必要である。

- **遵守事項 4.1.4(1)(d)「クラウドサービスの特性」について**

クラウドサービスを利用した情報システムは、従来のオンプレミスによる情報システムと比べ、主に以下の特性がある。

- クラウドサービス事業者の用意するコンピューティング資源を多くのクラウド利用者で共有し、その上に各クラウド利用者が利用する情報システムが構築さ

れる。そのため、本学が情報システムを構築する際のセキュリティ対策のみでなく、クラウドサービス事業者やコンピューティング資源を共有している他のクラウド利用者の情報システムにおいて情報セキュリティインシデントが発生し、その影響を受ける可能性がある。

- クラウド利用者は処理能力やストレージ等のコンピューティング資源を、利用者の操作で追加又は削減することができる。しかし、クラウドサービス事業者の用意する資源の不足等が発生した場合に即座に資源の追加ができず、可用性を損なう可能性がある。
- クラウドサービス事業者はコンピューティング資源を分散して配置することが可能であり、海外に配置されている可能性がある。

- **遵守事項 4.1.4(1)(e)「クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること」について**

クラウドサービス事業者及び当該サービスの信頼性が十分であることを総合的に判断するためには、クラウドサービスで取り扱う情報の機密性・完全性・可用性が確保されるように、クラウドサービス事業者のセキュリティ対策を含めた経営が安定していること、クラウドやアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

このような評価に当たって、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。その場合、監査や認証等によって保証される対象範囲がクラウドサービス事業者の全部又は一部の場合があるので、政府機関が委託するクラウドサービスが当該対象範囲に含まれていることを確認する必要がある。また、監査の場合には、監査項目の網羅性に留意して、重要な監査項目が除かれていないか、監査意見に除外事項（内部統制の不備）が含まれていないかなどを確認する必要がある。さらに、その監査や認証等によっては、クラウドサービス事業者の経営の安定性やサプライチェーン・リスク等は上記の評価に含まれていないことが考えられるため、これらのリスクについては本学において評価する必要がある。

なお、参考となる認証には、ISO/IEC 27017 によるクラウドサービス分野における ISMS 認証の国際規格があり、そこでは「クラウドサービス事業者が選択する監査は、一般的には、十分な透明性をもった当該事業者の運用をレビューしたいとする利用者の関心を満たすに足りる手段とする」ことが要求されており、これらの国際規格をクラウドサービス事業者選定の際の要件として活用することも考えられる。その他、日本セキュリティ監査協会のクラウド情報セキュリティ監査やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告書である SOC 報告書（Service Organization Control Report）を活用することも考えられる。特に、SOC2・SOC3 は、米国公認会計士協会が開発した「Trust サービス原則と基準」で定義された「セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシー」の５つの原則を適

用したものであるため、クラウドサービス事業者及びサービスに対する評価の際の参考となり得る。また、SOC2・SOC3 については、日本公認会計士協会の IT 委員会の実務指針により国内でも同様の保証報告書が制度化されている。ただし、SOC2・SOC3 及び実務指針第 7 号においては、この５つの原則の一部のみを選択して実施することができるため、当該監査で選択した原則に「セキュリティ」が含まれていることを保証報告書により確かめる必要がある。

参考：国際規格
「ISO/IEC 27017（安全なクラウドサービス利用のための分野別 ISMS 規格）」

参考：日本セキュリティ監査協会
「クラウド情報セキュリティ管理基準」
（http://jcispa.jasa.jp/documents/）
「クラウド情報セキュリティ監査制度規程」
（http://jcispa.jasa.jp/cloud_security/jcispa_regulation/）

参考：日本公認会計士協会
「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書（日本公認会計士協会 IT 委員会実務指針第 7 号）」
（http://www.hp.jicpa.or.jp/）

参考：米国公認会計士協会
「Service Organization Control (SOC) Reports」
（ http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/sorhome.aspx）

上記のウェブサイトのアドレスは、平成 29 年 10 月 10 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

- **遵守事項 4.1.4(1)-1「サービスの中断や終了時に際し、円滑に業務を移行するための対策」について**

クラウドサービス事業者が何らかの理由で、クラウドサービスの継続的な提供ができなくなった場合に、他のクラウドサービス事業者に対し、情報の移行を円滑に実施することにより、利用者側での業務を継続できるようにすることが求められる。

そのため、移植性又は相互運用性を確保する観点から、可能な限り、標準化されたデータ形式やインタフェースを使用することが望ましい。

- **遵守事項 4.1.4(1)-2 a)「アクセスログ等の証跡の保存」について**

クラウドサービス上におけるアクセスログ等の証跡に係る保存期間については、オンプレミスと同様に情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。

なお、記憶媒体に保存する期間については、過去に遡って調査する期間や頻度、ど

の程度のコストをログの保存にかけられるかを考慮して決定する（「(解説) 遵守事項 6.1.4(1)(b)「保存期間」について」を参照のこと。）。

- **遵守事項 4.1.4(1)-2 c)「クラウドサービスの委託先による情報の管理・保管」について**

  情報管理上の問題として、仮に情報がクラウド上にあったとしても、当該情報の責任は利用者である情報オーナーが負うことになるため、利用者はクラウドサービス事業者による情報の管理・保管方法について事前に把握する必要がある。

  また、クラウドサービス事業者が外部委託先に情報の管理・保管を委託した場合、当該情報が利用者の意図しない場面で二次利用されることも懸念されるため、外部委託先における情報セキュリティ水準や情報の取扱方法に関してクラウドサービス事業者に確認の上、合意しておく必要がある。

- **遵守事項 4.1.4(1)-2 d)「脆弱性対策」について**

  例えば、仮想化技術を用いたマルチテナントの環境において、OS 等の脆弱性に加えてハイパーバイザーを経由して他の利用者が享受するサービスを阻害する脆弱性はクラウドに対するリスクであり、対策を講ずる必要がある。このような脆弱性を発見する方法として、脆弱性検査ツールを用いた手法やペネトレーションテスト等が挙げられる。

- **遵守事項 4.1.4(1)-2 h)「情報開示請求に対する開示項目や範囲」について**

  クラウドサービスに関し、クラウドサービス事業者が一般に公開している内容以上の情報提供について、情報セキュリティ対策や監査の観点から、事前に本学とクラウドサービス事業者が協議の上、クラウドサービス事業者が提供する内容の項目や範囲を契約において明記することが必要である。また対象情報の機密性が高い場合、両者間で秘密保持契約（NDA：Non-Disclosure Agreement）を締結するなど必要な措置を講じた上で取得することが求められる。

第5部 情報システムのライフサイクル

5.1 情報システムに係る文書等の整備

5.1.1 情報システムに係る台帳等の整備

目的・趣旨

本学が所管する情報システムの情報セキュリティ水準を維持するとともに、情報セキュリティインシデントに適切かつ迅速に対処するためには、本学が所管する情報システムの情報セキュリティ対策に係る情報を情報システム台帳で一元的に把握するとともに、情報システムの構成要素に関する調達仕様書や設定情報等が速やかに確認できるように、日頃から文書として整備しておき、その所在を把握しておくことが重要である。

遵守事項

(1) 情報システム台帳の整備

(a) 全学実施責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。

(b) 部局技術責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について全学実施責任者に報告すること。

【 基本対策事項 】

＜5.1.1(1)(a)関連＞

5.1.1(1)-1 全学実施責任者は、以下の内容を含む台帳を整備すること。

a) 情報システム名
b) 管理課室
c) 当該部局技術責任者の氏名及び連絡先
d) システム構成
e) 接続する学外通信回線の種別
f) 取り扱う情報の格付及び取扱制限に関する事項
g) 当該情報システムの設計・開発、運用・保守に関する事項

また、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備すること。

a) 情報処理サービス名
b) 契約事業者
c) 契約期間
d) 情報処理サービスの概要
e) ドメイン名

f) 取り扱う情報の格付及び取扱制限に関する事項

＜5.1.1(1)(b)関連＞

5.1.1(1)-2 部局技術責任者は、政府情報システム管理データベースの登録対象となるシステムについては、当該データベースに必要な情報を記録し、適時最新の情報に更新すること。

（解説）

- **遵守事項 5.1.1(1)(a)「情報システム台帳に整備する」について**

  あらかじめ全学実施責任者が認めた場合には、全学実施責任者が指定した者に当該台帳を整備させることが考えられる。その際には、全学実施責任者は、指定した者より適宜情報システム台帳の整備状況について報告を受けることが望ましい。全学実施責任者は、台帳の整備状況について把握しておくことが重要である。

  情報システムに関する資産管理を行っている組織であれば、資産管理台帳を本項で作成を求めている台帳に代えることが可能である。その場合、本項を削除して関連項目を読み替えても良い。

- **遵守事項 5.1.1(1)(b)「情報システムを新規に構築し、又は更改する際には」について**

  台帳の整備内容の網羅性維持のため、部局技術責任者は、情報システムを新規に構築した際又は更改した際には、速やかに台帳に記載の事項を報告する必要がある。

  なお、台帳を最新に保つため、台帳に記載の事項に変更が生じた場合には、当該変更事項を報告し、台帳を更新する必要があるが、その報告の方法や時期については、本学ごとに定めることが望ましい。

- **基本対策事項 5.1.1(1)-1 d)「システム構成」について**

  当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、本学としての情報セキュリティ対策を行うために一元的に把握する必要があると判断する事項を含める必要がある。

- **基本対策事項 5.1.1(1)-1 g)「設計・開発、運用・保守に関する事項」について**

  当該情報システムの設計・開発、運用・保守に関する事項の記載は、実施責任者又は実施担当組織、外部委託した場合には委託先及び委託契約形態に関する情報が考えられるが、当該情報システムのライフサイクルに関する経緯や現状を把握し、情報セキュリティ上の問題等が発生した場合に適切な対策を指示するために必要な事項である。

- **基本対策事項 5.1.1(1)-2「民間事業者等が提供する情報処理サービスにより情報システムを構築する場合」について**

  本学として独自の情報システムを構築せずに、民間事業者等が提供するクラウドサービス等の情報処理サービスを利用して情報システムを構築し運用する場合や通信事業者が提供する回線サービスを利用して情報処理業務を行う場合は、利用する情報処理サービス名や契約事業者等の事項を記載したサービス契約に係る書類を適切に管理

しておくことが重要である。これらの書類を集約し、容易に参照できるようにすることをもって台帳整備に代えることができる。

なお、約款による外部サービスを利用する際は、事業者から提供される情報が十分でない場合が想定されるため、その場合は、利用する外部サービスに応じた内容の台帳を整備することも考えられる。

- **基本対策事項 5.1.1(1)-2「政府情報システム管理データベースの登録対象となるシステム」について**

  情報システム台帳の整備に当たっては、本学の情報システムを統一的に管理する政府情報システム管理データベースにおいて管理することが求められる。当該データベースの管理対象となるシステムについては、データベースにおいて管理することをもって台帳整備に代えることができる。

遵守事項

(2) 情報システム関連文書の整備

(a) 部局技術責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備すること。

(ア) 情報システムを構成するサーバ装置及び端末関連情報

(イ) 情報システムを構成する通信回線及び通信回線装置関連情報

(ウ) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

(エ) 情報セキュリティインシデントを認知した際の対処手順

【 基本対策事項 】

＜5.1.1(2)(a)(ア)関連＞

5.1.1(2)-1 部局技術責任者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備すること。

a) サーバ装置及び端末を管理する事務従事者及び利用者を特定する情報

b) サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン

c) サーバ装置及び端末の仕様書又は設計書

＜5.1.1(2)(a)(イ)関連＞

5.1.1(2)-2 部局技術責任者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、以下を含む文書を整備すること。

a) 通信回線及び通信回線装置を管理する事務従事者を特定する情報

b) 通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン

c) 通信回線及び通信回線装置の仕様書又は設計書

d) 通信回線の構成

e) 通信回線装置におけるアクセス制御の設定

f) 通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応

g) 通信回線の利用部門

＜5.1.1(2)(a)(ウ)関連＞

5.1.1(2)-3 部局技術責任者は、所管する情報システムについて、情報システム構成要素ごとのセキュリティ維持に関する以下を含む手順を定めること。

a) サーバ装置及び端末のセキュリティの維持に関する手順

b) 通信回線を介して提供するサービスのセキュリティの維持に関する手順

c) 通信回線及び通信回線装置のセキュリティの維持に関する手順

（解説）

- **遵守事項 5.1.1(2)(a)「情報システム関連文書を整備する」について**

当該事項については、各情報システムの運用管理に際して整備した文書に記載する事項のうち、本学としての情報セキュリティ対策を行うために一元的に把握する必要

があると判断するものを含める必要がある。

文書の整備に当たっては、維持管理が容易となるように適切な単位で整備することが望ましい。また、文書は電磁的記録として整備してもよい。

また、所管する情報システムに変更があった場合、また、想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になるため、文書の見直しを定期的に行うことをあらかじめ定めておくとよい。

なお、約款による外部サービスを利用する際は、事業者から提供される情報が十分でない場合が想定されるため、その場合は、利用する外部サービスに応じた内容の情報システム関連文書を整備することも考えられる。

- **遵守事項 5.1.1(2)(a)(エ)「情報セキュリティインシデントを認知した際の対処手順」について**

情報セキュリティインシデントが発生した際の対処手順は、当該情報システムの個別の事情に合わせて整備される対処手順である。本対処手順は、以下に示すような情報システムの事情に応じて整備されることが望ましい。

  - 業務継続計画で定める当該情報システムを利用する業務の重要性
  - 情報システムの運用等の外部委託の内容

また、手順に記載される内容として、例えば以下が想定される。

  - 情報セキュリティインシデントの内容・影響度の大きさに応じた情報連絡先のリスト
  - 情報システムを障害等から復旧させるために当該情報システムの停止が必要な場合の、停止の可否の判断基準
  - 情報セキュリティインシデントに対する情報システムの構成要素ごとの対処に関する事項
  - 不正プログラム対策ソフトウェアでは検知されない新種の不正プログラムに感染した場合等に支援を受けるための外部の専門家の連絡先

なお、全学実施責任者が整備する対処手順（「(解説) 遵守事項 2.2.4(1)(b)「対処手順」について」を参照のこと。）が、情報システムの事情に応じた内容で整備されているならば、情報システム別に整備しなくても構わない。

- **基本対策事項 5.1.1(2)-1 a)・基本対策事項 5.1.1(2)-2 a)「管理する事務従事者」について**

サーバ装置及び端末の管理者及び利用者、通信回線及び通信回線装置の管理者の記載は、情報システムの構成要素の管理状況を確実に把握できるようにするとともに、障害等を防止する責任の所在を明確化するために必要な事項である。

- **基本対策事項 5.1.1(2)-1 b)・基本対策事項 5.1.1(2)-2 b)「機種並びに利用しているソフトウェアの種類及びバージョン」について**

サーバ装置及び端末、通信回線装置の機種並びに利用ソフトウェアの種類及びバージョンの記載は、当該機種又は当該ソフトウェアに脆弱性が存在することにより使用上のリスクが高まった場合に、速やかに脆弱性対策を行うなど、適切に対処するため

に必要な事項である。

- **基本対策事項 5.1.1(2)-1 c)・基本対策事項 5.1.1(2)-2 c)「仕様書又は設計書」について**

  情報システムに係る仕様書又は設計書は、情報セキュリティ対策の実施状況の確認や見直しにおいて、当該情報システムの仕様や機能の確認を行うために必要な事項である。

- **基本対策事項 5.1.1(2)-3「セキュリティ維持に関する以下を含む手順」について**

  情報システムの構成要素のセキュリティ維持に関する手順は、当該構成要素のセキュリティを維持する目的で管理者が実施すべき手順であり、例えば、当該構成要素が具備する情報セキュリティ機能である主体認証、アクセス制御、権限管理及びログ管理の設定・変更等の手順が挙げられる。

5.1.2 機器等の調達に係る規定の整備

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。

これらの課題に対応するため、事務情報セキュリティ対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1) 機器等の調達に係る規定の整備

(a) 全学実施責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を本学が確認できることを加えること。

(b) 全学実施責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

＜5.1.2(1)(a)関連＞

5.1.2(1)-1 全学実施責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を例に規定すること。

a) 調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、本学と調達先が連携して原因を調査・排除できる体制を整備していること。

5.1.2(1)-2 全学実施責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408 に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定めること。

＜5.1.2(1)(b)関連＞

5.1.2(1)-3 全学実施責任者は、機器等の納入時の確認・検査手続には以下を含む事項を確認できる手続を定めること。

a) 調達時に指定したセキュリティ要件の実装状況

b) 機器等に不正プログラムが混入していないこと

（解説）

- **遵守事項 5.1.2(1)(a)「機器等の選定基準」について**

調達する機器等が、事務情報セキュリティ対策基準の該当項目を満たし、本学のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要

件を学内で統一的に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映することが必要である。

整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

- **遵守事項 5.1.2(1)(a)「必要に応じて」について**

機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、当該事項の適用要否を判断した上で整備することを求めている。

- **遵守事項 5.1.2(1)(a)「不正な変更」について**

ここでいう「不正な変更」とは、機器等の製造工程で不正プログラムを含む予期しない又は好ましくない特性を組み込むことを意味している。

不正な変更が行われない管理がなされていることとは、例えば、機器等の製造工程における不正行為の有無について、定期的な監査を行っていること、機器等の製造環境にアクセス可能な従業員が適切に制限され、定期点検が行われていること等が考えられる。その他、特に高い信頼性が求められる製品を調達する場合は、各製造工程の履歴が記録されているなどの厳格な管理されていることが考えられる。

- **基本対策事項 5.1.2(1)-1 a)「原因を調査・排除できる体制」について**

OEM（Original Equipment Manufacturer）によって提供される機器等についても、OEM 製品の製造者においても不正な変更が加えられないよう、OEM 製品の販売者が機器等のサプライチェーン全体について適切に管理していることも含めて、要件を定めることが考えられる。

- **基本対策事項 5.1.2(1)-2「ISO/IEC 15408 に基づく認証」について**

機器等の調達においては、ISO/IEC 15408 に基づく認証を取得している製品の優遇を選定基準の一つとすることで、第三者による情報セキュリティ機能の客観的な評価を受けた製品を活用でき、信頼度の高い情報システムが構築できる。

ISO/IEC 15408 に基づく認証では、第三者によって、対抗する脅威に必要な機能が設計書に反映されていること、その機能が設計どおり実装されていること、開発現場や製造過程においてセキュリティが侵害される可能性が無いこと、利用マニュアル・ガイダンス等にセキュリティを保つための必要事項が明確に示されていること等が客観的に評価され、評価結果及び既知の情報から懸念される脆弱性についての評定及びテストが実施される。ただし、第三者によって評価・保証される範囲は、適合する Protection Profile（国際標準に基づくセキュリティ要件）や、評価保証レベル（EAL：Evaluation Assurance Level）によって異なるため、どの程度の保証を得ている認証製品であるかを、調達時に確認することが必要となる。

- **基本対策事項 5.1.2(1)-3「以下を含む事項を確認できる手続」について**

  機器等の納入時の確認・検査手続の具体例として、以下の内容が考えられる。

  - 調達時に指定したセキュリティ要件（機器等に最新のセキュリティパッチが適用されているかどうか、不正プログラム対策ソフトウェア等が最新の脆弱性に対応しているかどうか等にも留意）に関する試験実施手順及び試験結果を納品時に報告させて確認
  - セキュリティ要件として調達時に指定した機能が正しく動作することを受入れテストにより確認
  - 内部監査等により不正な変更が加えられていないことを確認した結果を納品時に報告させて確認

5.2　情報システムのライフサイクルの各段階における対策

5.2.1　情報システムの企画・要件定義

目的・趣旨

情報システムのライフサイクル全般を通じて、情報セキュリティを適切に維持するためには、情報システムの企画段階において、適切にセキュリティ要件を定義する必要がある。

セキュリティ要件の曖昧さや過不足は、過剰な情報セキュリティ対策に伴うコスト増加のおそれ、要件解釈のばらつきによる提案内容の差異からの不公平な競争入札、設計・開発工程での手戻り、運用開始後の情報セキュリティインシデントの発生といった不利益が生じる可能性に繋がる。

そのため、情報システムが対象とする業務、業務において取り扱う情報、情報を取り扱う者、情報を処理するために用いる環境・手段等を考慮した上で、当該情報システムにおいて想定される脅威への対策を検討し、必要十分なセキュリティ要件を仕様に適切に組み込むことが重要となる。

加えて、構築する情報システムへの脆弱性の混入を防止するための対策も、構築前の企画段階で考慮することが重要となる。

また、情報システムの構築、運用・保守を外部委託する場合については、4.1 節「外部委託」についても併せて遵守する必要がある。

遵守事項

(1) 実施体制の確保

(a) 部局技術責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者に求めること。

(b) 部局技術責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し、運用管理する本学が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.1(1)(a)「情報システムを統括する責任者に求める」について**

  情報システムを統括する責任者（情報化統括責任者（CIO））が確立した体制が、セキュリティ維持の側面からも実施可能な体制（人員、機器、予算等）となるように求める事項である。

遵守事項

(2) 情報システムのセキュリティ要件の策定

(a) 部局技術責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムを**インターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離する**ことの要否を判断した上で、以下の事項を含む**情報システムのセキュリティ要件**を策定すること。

(ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

(イ) 情報システム運用時の監視等の運用管理機能要件

(ウ) 情報システムに関連する脆弱性についての対策要件

(b) 部局技術責任者は、インターネット回線と接続する情報システムを構築する場合は、**接続するインターネット回線を定めた上で**、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。

(c) 部局技術責任者は、国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定すること。

(d) 部局技術責任者は、機器等を調達する場合には、「**IT 製品の調達におけるセキュリティ要件リスト**」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

(e) 部局技術責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

【 基本対策事項 】

＜5.2.1(2)(a)関連＞

5.2.1(2)-1 部局技術責任者は、「**情報システムに係る政府調達におけるセキュリティ要件策定マニュアル**」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定すること。

5.2.1(2)-2 部局技術責任者は、**開発する情報システムが運用される際に想定される脅威**の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書等に明記すること。

＜5.2.1(2)(a)(ア)関連＞

5.2.1(2)-3 部局技術責任者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合

には、セキュリティ設計仕様書（ST：Security Target）を作成し、**ST 確認**を受けること。

＜5.2.1(2)(a)(イ)関連＞

5.2.1(2)-4 部局技術責任者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、以下を含む措置を実施すること。

a) 情報システム運用時に情報セキュリティ確保のために必要となる**管理機能**を仕様書等に明記すること。

b) 情報セキュリティインシデントの発生を監視する必要があると認めた場合には、**監視のために必要な機能**について、以下を例とする機能を仕様書等に明記すること。

- 学外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能
- 不正プログラム感染や踏み台に利用されること等による学外への不正な通信を監視する機能
- 学内通信回線への端末の接続を監視する機能
- 端末への外部電磁的記録媒体の挿入を監視する機能
- サーバ装置等の機器の動作を監視する機能

＜5.2.1(2)(a)(ウ)関連＞

5.2.1(2)-5 部局技術責任者は、開発する情報システムに関連する**脆弱性への対策**が実施されるよう、以下を含む対策を仕様書等に明記すること。

a) 既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

b) 開発時に情報システムに**脆弱性が混入されることを防ぐためのセキュリティ実装方針**。

c) セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。

d) ソフトウェアのサポート期間又はサポート打ち切り計画に関する本学への情報提供

＜5.2.1(2)(d)関連＞

5.2.1(2)-6 部局技術責任者は、構築する情報システムの構成要素のうち製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施すること。

a) 「IT 製品の調達におけるセキュリティ要件リスト」を参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とすること。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。

b) 「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する**機器等の利用環境において対抗すべき脅威**を分析し、必要なセキュリティ要件を策定すること。

（解説）

- **遵守事項 5.2.1(2)(a)「インターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離する」について**

標的型攻撃による不正プログラム感染の脅威は避けられないものになっており、外部のネットワークと接続する情報システムは、不正プログラムの感染を前提とした対策を講ずることの重要度が、年々増加している。

外部ネットワークとの接続形態を含む情報システムの全体構成は、情報システムにおいて取り扱われる情報の格付や取扱制限、情報システムを利用する業務の形態等によって決定する必要があるが、特に重要な情報を取り扱う情報システムについては、インターネットからの直接的なサイバー攻撃を受けないよう、インターネット回線や、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することが求められる。また、分離した情報システムの USB ポート等の外部ネットワーク・システムとの接点についても適切に運用することが望ましい。

- **遵守事項 5.2.1(2)(a)「情報システムのセキュリティ要件」・基本対策事項 5.2.1(2)-1「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」について**

「情報システムのセキュリティ要件」には、ハードウェア、ソフトウェア及び通信回線を含む情報システムの構成要素のセキュリティ要件並びに構築された情報システムの運用のセキュリティ要件がある。

なお、前者のセキュリティ要件については、構築環境や構築手法等のセキュリティに関する手順も含まれる。

セキュリティ要件の策定には、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の活用又はそれと同等以上の検討結果を最低限のセキュリティ対策水準であると考え、決定されたセキュリティ要件は、システム要件定義書や仕様書等の形式で明確化した上で、実装していくことが望ましい。

情報システムのセキュリティ要件を検討する際には、仮想化技術の活用の有無を確認し、物理的に分割されたシステムに限らず、論理的に分割されたシステムであるかを考慮したセキュリティ要件を検討することも重要である。「論理的に分割されたシステム」とは、一つの情報システムの筐体上に複数のシステムを共存させることを目的として、論理的に分割させた状態の情報システムをいう。

また、外部の情報システムを利用する場合は、4.1.1 項「外部委託」も参照の上、委託先との管理責任範囲の分担を明確化し、セキュリティ対策の実施に漏れが生じないようにすることも重要である。

このように、情報システムの構築形態及び調達形態に応じてセキュリティ要件を定めることが求められる。

- **遵守事項 5.2.1(2)(b)「接続するインターネット回線を定めた上で」について**

構築する情報システムごとに、個々にインターネット回線を構築すると、当該インターネット回線の監視等に係る体制や運用コストが分散し、効率的かつ集中的なセキュリティ監視が行われず、セキュリティ水準が低下するおそれがある。このような観点から、機関としてインターネット接続口を統合・集約し、集中的なセキュリティ監視を行うなどの取組を行っている場合は、当該取組の範疇とするか否か検討した上で、構築する情報システムに接続するインターネット回線を仕様書等において明確化しておくことを求めている。

なお、既設のインターネット回線を利用せずに、独立したインターネット回線を調達してセキュリティ監視等の運用を個別に行う場合も想定される。情報システムが取り扱う情報の格付や取扱制限等の特性に従って、既設のインターネット回線の利用可否を判断することが望ましい。

- **遵守事項 5.2.1(2)(d)「IT 製品の調達におけるセキュリティ要件リスト」について**

「IT 製品の調達におけるセキュリティ要件リスト」には、複合機、OS、USB メモリ等の製品分野ごとに一般的に想定されるセキュリティ上の脅威が記載されており、それらが自身の運用環境において該当する場合には対抗する必要がある。

対抗手段の一つとして、「IT 製品の調達におけるセキュリティ要件リスト」には、IT セキュリティに関わる「国際標準に基づくセキュリティ要件」が記載されており、それを調達時に活用することで脅威に対抗するための機能を有した製品を調達することが可能となる。

「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」のうち、製品の利用環境や製品に実装されている機能によっては、一部の脅威だけに対抗すればよい場合もあり得る。そのような場合には、「国際標準に基づくセキュリティ要件」では過剰な要件（要求仕様）となる可能性もあるので、個別にセキュリティ要件を策定して脅威に対抗してもよい。

参考：経済産業省「IT 製品の調達におけるセキュリティ要件リスト」
（http://www.meti.go.jp/policy/netsecurity/cclistmetisec2014.pdf）

- **基本対策事項 5.2.1(2)-2「開発する情報システムが運用される際に想定される脅威」について**

汎用ソフトウェアをコンポーネントとして情報システムを構築する場合はもとより、全てを独自開発する場合であっても、外部から脆弱性をつかれる可能性があるため、開発する情報システムの機能、ネットワークの接続状況等から、想定される脅威を分析する必要がある。

また、情報システムを構成する端末、サーバ装置、それらに搭載されているソフトウェア等に関して想定される脅威に対しては、第 7 部で規定された対策が適切に実施されるようにセキュリティ要件を策定することが必要となる。策定に当たっては、運用開始後に適切に対策が講じられるようにシステムの企画段階から留意する必要がある。例えば、サーバ装置の運用時に必要になる不正アクセス等の監視機能を実装する

こと、端末やサーバ装置等に利用を認めるソフトウェア以外のソフトウェアが意図せず混入されないこと等について留意が必要となる。

- **基本対策事項 5.2.1(2)-3「ST 確認」について**

セキュリティ要件の策定に当たっては、脅威に対抗するために妥当なセキュリティ要件となっていることの確認を求める事項である。

セキュリティ要件の妥当性確認には、学内でのレビューの実施等の他に、対象とする情報システムが扱う業務及び情報の重要度によっては、セキュリティ要件の策定に関っていない客観的な立場の者による検証を実施することが望ましい。

「ST 確認」とは、情報システムが対抗すべき脅威について適切なセキュリティ要件が策定されていることを確認するために、セキュリティ設計仕様書(ST:Security Target)を IT セキュリティ評価基準(ISO/IEC 15408)に基づき、第三者である評価機関が評価し、その評価結果が妥当であることを認証機関（独立行政法人情報処理推進機構）が検証し、確認することをいう。

- **基本対策事項 5.2.1(2)-4 a)「管理機能」について**

「管理機能」とは、真正確認、権限管理等のセキュリティ機能を管理するための機能のほか、情報セキュリティインシデントの発生時に行う対処及び復旧に係る機能、証跡保全の機能等を指し、これらの必要性を情報システムの設計時から検討することにより、必要がある場合には情報システムに組み込む必要がある。

- **基本対策事項 5.2.1(2)-4 b)「監視のために必要な機能」について**

情報システム及び取り扱う情報の格付や取扱制限等を考慮して、情報システムの各所において様々なイベントを監視する必要性を見極める必要がある。監視するイベントとしては、通信回線を通してなされる不正アクセス又は不正侵入、情報システムの管理者・運用者又は利用者の誤操作若しくは不正操作、サーバ装置等機器の動作、許可されていない者の要管理対策区域への立入り等があり得る。

なお、監視によりプライバシーを侵害する可能性がある場合は、関係者への説明について定めること。

- **基本対策事項 5.2.1(2)-5「脆弱性への対策」について**

脆弱性対策を怠った場合には、セキュリティ侵害の機会を増大することにつながるため、情報システムの企画段階から対策を講じておく必要がある。

脆弱性が存在することが公表されているソフトウェア等については対策が施されているバージョンのものを利用することや、開発後の情報システムに脆弱性が存在することが発覚した場合に備えて、調達時の仕様書に対策のための要件を明記しておくことが重要となる。

- **基本対策事項 5.2.1(2)-5 b)「脆弱性が混入されることを防ぐためのセキュリティ実装方針」について**

「脆弱性が混入されることを防ぐためのセキュリティ実装方針」とは、情報システム開発者が情報システムに脆弱性を混入することを防ぐために、開発時における脆弱

性への具体的な対策方法を定めたものである。脆弱性は種類ごとに対策が異なり、懸念される脆弱性の種類ごとに方針を定める必要がある。具体的に定めるものとして、例えば以下の内容が考えられる。

- バッファオーバーフローによる不正なプログラムの挿入及び実行を防ぐために、データを転記する場面においてメモリ領域長とデータ長を検査する処理を付加する。
- SQL インジェクションによるデータベース内の情報の漏えい・改ざんを防ぐために、プレースホルダにより SQL 文を組み立てる。
- OS コマンドインジェクションによる不正なシステム操作を防ぐために、シェルを起動できる言語機能を利用しない。

6.2.1 項「ソフトウェアに関する脆弱性対策」及び 7.2.2 項「ウェブ」の規定内容も参考にして、懸念される全ての脆弱性の種類に対して、実装方針を定め、仕様書に明記する必要がある。

- **基本対策事項 5.2.1(2)-6 b)「機器等の利用環境において対抗すべき脅威」について**

機器等に関連したセキュリティ上の脅威は利用環境によって変わるため、調達時にどのような環境で運用するのかを把握し、その環境において存在する脅威を分析した上で、必要となるセキュリティ要件を策定する必要がある。

例えば、ネットワークに接続し、通信データとして要保護情報を送受信する場合に盗聴による情報漏えいが想定される場合には、通信データの保護に係るセキュリティ要件が必要となるが、スタンドアロンで利用する場合で、盗聴による情報漏えいが想定されない場合には、通信データの保護に係るセキュリティ要件は不必要なセキュリティ要件となる可能性がある。

また、特定の人物しか物理的にアクセスできないように隔離された場所へ機器等を設置すること等で、誰もが物理的にアクセスできる環境で想定される脅威を軽減することも考えられる。

調達する機器ごとの利用環境において想定される脅威を漏れなく分析した上で、脅威に対抗するために必要十分なセキュリティ要件を策定することが重要である。

遵守事項

(3) 情報システムの構築を外部委託する場合の対策

(a) 部局技術責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させること。

(ア) 情報システムのセキュリティ要件の適切な実装

(イ) 情報セキュリティの観点に基づく試験の実施

(ウ) 情報システムの開発環境及び開発工程における情報セキュリティ対策

【 基本対策事項 】

＜5.2.1(3)(a)(イ)関連＞

5.2.1(3)-1 部局技術責任者は、情報セキュリティの観点に基づく試験の実施について、以下を含む事項を実施させること。

a) ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から**運用中の情報システムに悪影響**が及ばないように、運用中の情報システムと分離すること。

b) **情報セキュリティの観点から必要な試験**がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。

c) 情報セキュリティの観点から実施した試験の**実施記録**を保存すること。

＜5.2.1(3)(a)(ウ)関連＞

5.2.1(3)-2 部局技術責任者は、**開発工程における情報セキュリティ対策**として、以下を含む事項を実施させること。

a) ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。

- ソースコードの変更管理
- ソースコードの閲覧制限のためのアクセス制御
- ソースコードの滅失、き損等に備えたバックアップの取得

b) 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

c) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、**設計レビュー**及び**ソースコードレビュー**の範囲及び方法を定め、これに基づいてレビューを実施すること。

（解説）

- **基本対策事項 5.2.1(3)-1 a)「運用中の情報システムに悪影響」について**

運用中の情報システムを利用してソフトウェアの作成及び試験を行う場合は、運用中の情報システムに悪影響が及ぶことを回避することが大前提となる。

また、開発中のソフトウェアの動作確認のために、運用中の情報システムの要機密情報をテストデータとして、試験を行う情報システムにおいて使用しないようにする

必要がある。

- **基本対策事項 5.2.1(3)-1 b)「情報セキュリティの観点から必要な試験」について**

攻撃が行われた際に情報システムがどのような動作をするかを試験する項目として想定しており、具体的には、想定の範囲外のデータの入力を拒否できるか、サービス不能攻撃等により情報システムが過負荷状態に陥った場合に処理中のデータは保証されるか、レースコンディションが発生しないか(「(解説) 基本対策事項 7.2.2(2)-1 l)「レースコンディション脆弱性」について」を参照のこと。)といった項目が挙げられる。

なお、セキュリティ機能の試験だけにとどまらず、情報システムの脆弱性の有無、必要なチェック機能の欠如等について、必要な試験が網羅されるよう留意することが望ましい。

- **基本対策事項 5.2.1(3)-1 c)「実施記録」について**

「実施記録」とは、試験の項目、実施結果、実施時に判明した不具合及び当該不具合の修正の記録等を指し、これらを保存することにより、脆弱性を発見した場合の対処に利用できるようにすることが求められる。

- **基本対策事項 5.2.1(3)-2「開発工程における情報セキュリティ対策」について**

情報システム開発に係る情報資産についてセキュリティを維持するための手順及び環境を定めることを求めている。

具体的な手順としては、例えば、仕様書、ソースコード等の成果物に対して情報システムのライフサイクル全般にわたって一貫性を確保及び維持するための構成管理の手順及び利用するツール等が考えられる。

開発環境については、例えば、ドキュメント及びソースコードに対するアクセス権、開発に利用するサーバ装置及び端末の設置場所及びアクセス制御の方法等がある。

なお、情報システム開発を外部委託する場合は、委託先に対するセキュリティ要件定義の策定手順や導入時のセキュリティ評価試験手順等を整備しておく必要がある。

- **基本対策事項 5.2.1(3)-2 c)「設計レビュー」について**

情報システムの設計について、脆弱性の原因となる設計の不具合をなくすために、設計レビューの実施が求められる。

一般に設計レビューには、①レビュー対象内にあるエラーの発見を第一目的とし、開発責任者等が実施する確認手法（インスペクション)、②開発担当者自身が開発関係者を集め、レビュー対象プログラムを実行の流れに従って追跡し確認する手法（ウォークスルー）等があり、これらを、いつ、誰が、何に対して実施するのか、といったことを定める必要がある。

- **基本対策事項 5.2.1(3)-2 c)「ソースコードレビュー」について**

ソースコードに脆弱性が混入しないように、ソースコードレビューの範囲及び方法について、あらかじめ定めておくことが求められる。例えば、脆弱性の原因となるソースコードについては、開発言語ごとに典型的なパターンが知られていることから、ソースコードレビューによる検証が有効な場合がある。ソースコードレビューについ

ては、開発する情報システムだけを対象として想定しており、市販製品を組み込む場合等、ソースコードの入手が困難な場合に実施することは想定していない。

遵守事項

(4) 情報システムの運用・保守を外部委託する場合の対策

(a) 部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。

【 基本対策事項 】

＜5.2.1(4)(a)関連＞

5.2.1(4)-1 部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を含む要件を調達仕様書に記載するなどして、適切に実施させること。

a) 情報システムの運用環境に課せられるべき条件の整備

b) 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

c) 情報システムの保守における情報セキュリティ対策

d) 運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

（解説）

- **基本対策事項 5.2.1(4)-1 a)「運用環境に課せられるべき条件」について**

情報システムの運用環境に課せられるべき条件としては、物理的、接続的（ネットワーク環境）及び人的側面を考慮する必要がある。どのような条件を設定するかによって想定される脅威が異なってくるため、脅威を想定する上で必要となる条件は全て調達仕様書、契約書等に記載する必要がある。

物理的な設置環境に関する条件とは、サーバ装置を設置する場所の特定、耐震･防火に関する基準、電源供給に関する基準等に関する条件を示すものである。

接続面（ネットワーク環境等）に関する条件とは、情報システムが接続されるネットワーク環境や通信回線の基準、情報セキュリティ上の何らかのリスクを伴う外部サービスをネットワーク経由で利用する場合の条件等を示すものである。

人的環境とは、対象とするシステムの管理者や業務担当職員の信頼性に関する条件、当該システムに関わる組織・体制として実現すべきことに関する条件、当該システムの使用方法として当然実現されるべきことに関する条件等を示すものである。

- **基本対策事項 5.2.1(4)-1 b)「監視手順」について**

情報システムのセキュリティ監視を行う体制を特別に設けずに情報システムの運用を行う体制においてキュリティ監視も行うことも考えられる。

監視によりプライバシーを侵害する可能性がある場合は、対象となる関係者への説明等の手順についても本学として定めておくこと。

- **基本対策事項 5.2.1(4)-1 c)「保守における情報セキュリティ対策」について**

情報システムの保守においては、保守担当者が作業中に権限外の情報にアクセスで

きないよう、アクセス制御や権限管理を考慮する必要がある。また、保守担当者へのなりすましが脅威として想定される場合には、保守担当者に対する主体認証も開発する情報システムのセキュリティ要件策定時に考慮する必要もある。

- **基本対策事項 5.2.1(4)-1 d)「脆弱性が存在することが判明」について**

  ソフトウェアやウェブアプリケーション等の情報システムに関連する脆弱性は日々新たなものが報告されており、調達時に策定した脆弱性についての対策要件だけでは十分に対処できない可能性もあり得る。

  また、運用・保守を行う委託先が、情報システムの構築を行った委託先と異なる場合、情報システム運用開始後に発見された脆弱性に対して、情報システムの構築を行った委託先のみでは対処することが困難な場合もあり得る。そのため、運用・保守を行う委託先に対して、運用開始後に発見された脆弱性への対処を求めることも契約又は仕様書において考慮する必要がある。

5.2.2 情報システムの調達・構築

目的・趣旨

情報システムを調達・構築する際には、策定したセキュリティ要件に基づく情報セキュリティ対策を適切に実施するために、選定基準に適合した機器等の調達や、情報システムの開発工程での情報セキュリティ対策の実施が求められる。

また、機器等の納入時又は情報システムの受入れ時には、整備された検査手続に従い、当該情報システムが運用される際に取り扱う情報を保護するためのセキュリティ機能及びその管理機能が、適切に情報システムに組み込まれていることを検査することが必要となる。

遵守事項

(1) 機器等の選定時の対策

(a) 部局技術責任者は、機器等の選定時において、**選定基準に対する機器等の適合性を確認**し、その結果を機器等の選定における判断の一要素として活用すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.2(1)(a)「選定基準に対する機器等の適合性を確認」について**

  遵守事項 5.1.2(1)(a)において整備された機器等の選定基準に従って、機器等の開発等のライフサイクルにおいて不正な変更が加えられない管理体制が確認できることや、第三者による情報セキュリティ機能の客観的な評価が行われていることを確認すること等を求めている。

  なお、ISO/IEC 15408 に基づく認証を取得していることを選定基準として活用した場合には、調達先から認証取得を証明するための認定書等を調達先に提示させることも考えられる。

遵守事項

(2) 情報システムの構築時の対策

(a) 部局技術責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。

(b) 部局技術責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。

【 基本対策事項 】

＜5.2.2(2)(a)関連＞

5.2.2(2)-1 部局技術責任者は、情報システムの構築において以下を含む情報セキュリティ対策を行うこと。

a) 情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備すること。

b) セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。

c) 情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。

d) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施すること。

e) 脆弱性検査を含む情報セキュリティの観点での試験を実施すること。

5.2.2(2)-2 部局技術責任者は、情報システムの運用保守段階へ移行するに当たり、以下を含む情報セキュリティ対策を行うこと。

a) 情報セキュリティに関わる運用保守体制の整備

b) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

c) 情報セキュリティインシデントを認知した際の対処方法の確立

（解説）

- **遵守事項 5.2.2(2)(b)「移行手順及び移行環境」について**

情報システムの開発環境、テスト環境から本番運用の環境への移行時において、情報システムに保存されている情報の取扱い手順の整備、人為的な操作ミスを防止するための手順・環境の整備、移行の際に関連システム停止が伴う場合には可用性確保のための環境整備等が必要となる。

- **基本対策事項 5.2.2(2)-1「情報セキュリティ対策」について**

情報システムの構築を外部委託する場合には、5.2.1 項「情報システムの企画・要件定義」の「(3) 情報システムの構築を外部委託する場合の対策」の内容を委託先に適切に実施させることが求められる。

また、情報システムの構築を外部委託せず、本学自らが構築する場合であっても、同項の内容を参照し、必要な対策を実施することが求められる。

遵守事項

(3) 納品検査時の対策

(a) 部局技術責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、**情報セキュリティ対策に係る要件が満たされていることを確認する**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.2(3)(a)「情報セキュリティ対策に係る要件が満たされていることを確認する」について**

  情報セキュリティ対策の視点を加味して整備された納入時の確認・検査手続に従い、納入された情報システム及び機器等が要求仕様どおりに正しく動作することの検査を行うことが求められる。

  本学における受入れテストの実施、納入元が実施したテストに関する資料の提出要求及びその検査内容の確認、第三者への受入れテストの委託、ISO/IEC 15408 に基づく第三者認証取得の確認等、検査対象の情報システム及び機器等の特性に応じて適切な検査を実施する必要がある。

5.2.3 情報システムの運用・保守

目的・趣旨

情報システムの運用段階に移るに当たり、企画又は調達・構築時に決定したセキュリティ要件が適切に運用されるように、人的な運用体制を整備し、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を実施する必要がある。

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生することが大半であることから、適宜情報システムの情報セキュリティ対策の実効性を確認するために、情報システムの運用状況を監視することも重要である。

また、情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても、事務情報セキュリティ対策基準に基づく情報セキュリティ対策について適切に措置を講ずることが求められる。

遵守事項

(1) 情報システムの運用・保守時の対策

(a) 部局技術責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。

(b) 部局技術責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し、運用管理する本学との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

(c) 部局技術責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

【 基本対策事項 】

＜5.2.3(1)(a)関連＞

5.2.3(1)-1 部局技術責任者は、情報システムのセキュリティ監視を行う場合は、以下の内容を含む監視手順を定め、適切に監視運用すること。

(a) 監視するイベントの種類

(b) 監視体制

(c) 監視状況の報告手順

(d) 情報セキュリティインシデントの可能性を認知した場合の報告手順

(e) 監視運用における情報の取扱い（機密性の確保）

5.2.3(1)-2 部局技術責任者は、情報システムに実装された**セキュリティ機能が適切に運用されていること**を確認すること。

5.2.3(1)-3 部局技術責任者は、情報システムにおいて取り扱う情報について、当該情報の格付及び取扱制限が適切に守られていることを確認すること。
5.2.3(1)-4 部局技術責任者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。

（解説）

- **基本対策事項 5.2.3(1)-2「セキュリティ機能が適切に運用されていること」について**

  運用する情報システムについて、外部環境が大きく変化した場合等には、セキュリティ機能が適切に運用されるために、機器等のパラメータ設定、物理的な設置環境、ネットワーク環境、人的な運用体制等について問題が無いことを適宜確認する必要がある。

- **基本対策事項 5.2.3(1)-3「当該情報の格付及び取扱制限が適切に守られていること」について**

  情報の格付けの見直し及び再決定が行われた際や、当該情報システムに係る事務従事者の異動や職制変更等が生じた際には、情報に対するアクセス制御の設定や職務に応じて与えられている情報システム上の権限が適切に変更される必要がある。

- **基本対策事項 5.2.3(1)-4「脆弱性の存在が明らかになった場合」について**

  本学が運用する情報システムに関連する脆弱性が存在することが発覚した場合、セキュリティパッチの適用等の情報セキュリティ対策が必要となる。

  また、情報セキュリティ対策が適用されるまでの間にセキュリティ侵害が懸念される場合には、当該情報システムの停止やネットワーク環境の見直し等情報セキュリティを確保するための運用面での対策を講ずる必要もある。

5.2.4 情報システムの更改・廃棄

目的・趣旨

情報システムの更改・廃棄において、情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。

情報システムに機密性の高い情報が記録されている場合や、格付や取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講ずることが必要となる。

遵守事項

(1) 情報システムの更改・廃棄時の対策

(a) 部局技術責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。

(ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策

(イ) 情報システム廃棄時の不要な情報の抹消

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.4(1)(a)(ア)「情報の移行」について**

情報システムを更改する際は、更改元の情報システムから更改先の情報システムに情報（本番データ）を移行する作業が発生する場合が多いが、移行作業の過程で情報が外部に漏えいすることのないよう、移行用の本番データを適切に管理することが必要である。移行用の本番データの管理手順や外部電磁的記録媒体を使用する場合の安全管理措置等をあらかじめ定めておくとよい。

移行作業を外部委託する場合においては、委託先とあらかじめ手順について合意し、仕様書に明記しておく必要がある。

- **遵守事項 5.2.4(1)(a)(イ)「情報の抹消」について**

情報システムの廃棄を行う場合には、情報システムを構成する機器等並びに内部に保存されている情報の格付及び取扱制限を考慮して、適切に抹消する必要がある。要機密情報を保存している情報システムにおいては、情報の抹消が求められる。廃棄の際に本規定を考慮すべき機器等としては、サーバ装置や端末以外にも、複合機等の内蔵電磁的記録媒体を備えた機器については同様に考慮する必要がある。第 7 部において機器ごとの廃棄時の対応を規定しているので、併せて考慮されたい。

なお、情報システムの廃棄を外部委託する際は、委託先において情報の抹消が適切に実施されるよう、3.1.1 項(7)「情報の消去」の規定も参考に、抹消方法等についてあらかじめ合意し仕様書等に明記しておく必要がある。委託先の抹消作業に関する作業

完了届（廃棄したことが証明されるもの）等を書面で受け取るなどするとよい。

5.2.5 情報システムについての対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、新たに発生した脅威等に的確に対応しない場合には、情報セキュリティ水準を維持できなくなる。このため、情報システムの情報セキュリティ対策を定期的に見直し、さらに外部環境の急激な変化等が発生した場合は、適時見直しを行うことが必要となる。

遵守事項

(1) 情報システムについての対策の見直し

(a) 部局技術責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により**見直し**を適時検討し、必要な措置を講ずること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.2.5(1)「見直し」について**

情報システムの情報セキュリティ対策について、新たな情報セキュリティ上の脅威、情報セキュリティインシデント発生事案例及び情報セキュリティインシデント発生時の影響等を検討した上で、情報システムの情報セキュリティ対策について定期的に見直しを行い、セキュリティ要件の追加、修正等の必要な措置を求める事項である。

所管する情報システムに変更があった場合、また、情報システムの外部環境に変化が生じた場合には、定期的な情報セキュリティ対策の見直しに加えて、適時見直すことも必要となる。

5.3 情報システムの運用継続計画

5.3.1 情報システムの運用継続計画の整備・整合的運用の確保

目的・趣旨

業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、非常時でも継続させる必要があり、本学においては業務継続計画を策定し運用している。

一方、非常時に情報システムの運用を継続させる場合には、非常時における情報セキュリティに係る対策事項を検討し、定めることが重要となる。

なお、業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。

遵守事項

(1) 情報システムの運用継続計画の整備・整合的運用の確保

(a) 全学実施責任者は、本学において**非常時優先業務**を支える**情報システムの運用継続計画を整備**するに当たり、**非常時における情報セキュリティに係る対策事項**を検討すること。

(b) 全学実施責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が**運用可能であるかを確認**すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 5.3.1(1)(a)「非常時優先業務」について**

  内閣府による「中央省庁業務継続ガイドライン」では、応急業務（災害応急対策業務及び被災状況に応じて速やかな実施が必要となる他の緊急業務）及び継続の必要性の高い通常業務を合わせたもののことを非常時優先業務としている。

- **遵守事項 5.3.1(1)(a)「情報システムの運用継続計画を整備」について**

  非常時優先業務を支える情報システムの運用継続計画を整備するに当たっては、情報システムの運用継続計画の作成に資する資料として、内閣官房情報セキュリティセンター（当時）が取りまとめた以下の資料を参照することが考えられる。

  参考：内閣官房情報セキュリティセンター「「中央省庁における情報システム運用継続計画ガイドライン」及び関連資料」（平成 25 年 6 月）
  （http://www.nisc.go.jp/active/general/itbcp-guideline.html）

- **遵守事項 5.3.1(1)(a)「非常時における情報セキュリティに係る対策事項」について**

  情報システムの運用継続を脅かす危機的事象の例として、地震、風水害等の自然災

害、火災等の人的災害・事故、停電等の社会インフラの不全、不正アクセス等の運用妨害、機器等の故障等が想定される。これらの非常時に対して、業務継続計画、情報システムの運用継続計画及び事務情報セキュリティ対策基準のそれぞれで定める対策に矛盾があると、非常時に事務従事者は一貫性のある行動をとることができない。このため、非常時における情報セキュリティに係る対策事項を検討する際は、業務継続計画及び情報システムの運用継続計画と事務情報セキュリティ対策基準との間で整合性を確保するよう検討することが必要である。

例えば、非常時に、情報システムの主体認証情報として設定したパスワードを設定した者以外の者が当該情報システムを使用しなければならない場合が想定される。このような場合の実施手順について、業務継続計画及び情報システムの運用継続計画で安易に定めるのではなく、情報セキュリティ関係規程において、非常時でも情報セキュリティ水準を確保した実施手順を整備する必要がある。手順の一例としては、通常時に利用する識別コードとパスワードとは別に、非常時用の識別コードとパスワードをあらかじめ設定しておく方法が考えられる。この場合、非常時用のパスワードは人が記憶困難な文字列で設定し、そのパスワードを記載した紙面を施錠された安全な保管場所に保管することで、通常時のパスワードを非常時に聞き出したり、通常時にパスワードを共用したりすることなく、非常時においても情報システムの利用が可能となる。また、パスワードを記載した紙面を保管する際に、開封すると開封事実が明らかとなる特殊な封書（tamper evidence envelope）を併用すれば、通常時における不正使用の有無を確認できる。

また、非常時には、本学の施設の一部に帰宅困難者等を受け入れる場合等、通常時の情報セキュリティ水準の確保に支障をきたす状況が考えられる。このような場合を想定し、あらかじめ情報セキュリティ水準の確保を要する施設や業務への影響を分析し、必要な対策を十分検討した上で、通常時及び非常時の対応を定める必要がある。例えば、各執務室や各事務従事者の卓上の情報セキュリティ対策を含め、通常時から不特定の者の出入りを想定した対策を講ずること等が考えられる。

なお、停電や交通機関の麻痺等の社会インフラの不全等により、通常時に利用している情報システムが利用できなくなる場合や、通常時に利用している場所で情報システムを利用することができない場合等、情報システムを利用する環境が制限される状況が考えられる。このような場合を想定し、約款による外部サービス、本学支給以外の端末等の利用が非常時優先業務の継続に有効であると判断される場合には、それらを利用して業務を継続することについても、そのリスクや情報セキュリティ水準の確保等を十分に検討した上で、あらかじめ定めておく必要がある。

- **遵守事項 5.3.1(1)(b)「運用可能であるかを確認」について**

情報システムの運用継続を脅かす非常時においては、非常時の情報セキュリティに係る対策事項を整備した際には想定していなかった様々な不整合が発生し、整備した対策事項が有効に機能しないことも考えられる。このため、非常時の対策事項を定期的に見直し、課題を発見した場合は改善することが重要である。

なお、情報システムの運用継続計画の教育訓練を行う際は、非常時の対策事項の理

解と対応能力の向上の他、対策事項の有効性の確認も目的とすることが望ましい。

第6部 情報システムのセキュリティ要件

6.1 情報システムのセキュリティ機能

6.1.1 主体認証機能

目的・趣旨

情報又は情報システムへアクセス可能な主体を制限するためには、主体認証機能の導入が必要である。その際、アクセス権限のある主体へのなりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講ずることが重要となる。

また、本学の情報システムにおいて、国民向けのサービスを提供する場合等は、一般の利用者が情報システムへのアクセスの主体になることにも留意して、主体認証情報を適切に保護しなければならない。

遵守事項

(1) 主体認証機能の導入

(c) 部局技術責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の**識別**及び**主体認証**を行う機能を設けること。

(d) 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。

【 基本対策事項 】

＜6.1.1(1)(a)関連＞

6.1.1(1)-1 部局技術責任者は、主体認証は、以下を例とする主体認証方式を決定すること。

a) 知識（パスワード等、利用者本人のみが知り得る情報）による認証

b) 所有（電子証明書を格納する IC カード又はワンタイムパスワード生成器等、利用者本人のみが所有する機器等）による認証

c) 生体（指紋や静脈等、本人の生体的な特徴）による認証

6.1.1(1)-2 部局技術責任者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、文字の種類や組合せ、桁数等のパスワード設定条件を利用者に守らせる機能を設けること。

＜6.1.1(1)(b)関連＞

6.1.1(1)-3 部局技術責任者は、主体認証を行う情報システムにおいて、**利用者に主体認証情報の定期的な変更を求める場合**には、利用者に対して定期的な変更を促す機能のほか、以下の機能を設けること。

a) 利用者が定期的に変更しているか否かを確認する機能
b) 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

6.1.1(1)-4 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下を例とする方法を用いて適切に管理すること。
a) 主体認証情報を送信又は保存する場合には、その内容を暗号化する。
b) 主体認証情報に対するアクセス制限を設ける。

6.1.1(1)-5 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に利用され、又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設けること。
a) 当該主体認証情報及び対応する識別コードの利用を停止する機能
b) 主体認証情報の再設定を利用者に要求する機能

（解説）

- **遵守事項 6.1.1(1)(a)「識別」について**

識別のための機能が実装されていない情報システムにおいて主体認証を行う場合（例えば、識別コード自体が存在せず、主体認証情報の検証のみで主体認証を行う場合）は、例外措置として判断し、主体を識別しないことによる影響を勘案の上、必要に応じて代替又は追加の措置を講ずる必要がある。

- **遵守事項 6.1.1(1)(a)「主体認証」について**

情報セキュリティ水準と情報システムの利便性等を考慮し、主体認証機能の運用に係る以下の要件の実装要否を情報システムの導入時に考慮するとよい。

- 正当な主体以外の主体認証を受諾しないこと。（誤認の防止）
- 正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。（誤否の防止）
- 正当な主体が容易に他の主体に主体認証情報の付与（発行、更新及び変更を含む。以下この項において同じ。）及び貸与ができないこと。（代理の防止）
- 主体認証情報が容易に複製できないこと。（複製の防止）
- 部局技術責任者の判断により、ログインを個々に無効化できる手段があること。（無効化の確保）
- 必要時に中断することなく主体認証が可能であること。（可用性の確保）
- 新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）
- 主体に付与した主体認証情報を利用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保）

加えて、主体認証を行う情報システムにおいて、情報セキュリティ強度の更なる向上を図るため、多要素主体認証の導入など、以下を例とする機能を設けることを検討することが重要である。

	機能	解説
①	多要素主体認証方式で主体認証を行う機能	複数要素の主体認証方式を組み合わせて、単一の主体認証方式よりも強固な主体認証を行う機能を指す。一般に、異なる認証方式を組み合わせた方が、強度が高くなる。 多要素主体認証方式であれば、仮に一つの主体認証情報が露呈してしまっても、残りの主体認証情報が露呈しない限り、不正にログインされる可能性は低いと考えられる。 また、通常の運用時は単一の主体認証を実施するが、認証の要求時に、アクセス元の IP アドレス、アクセスする時間帯、位置情報等が通常のアクセスとは異なる特徴が確認された場合は、不正ログインのリスクが高まったと判断して多要素主体認証を行う方法も考えられる。
②	前回のログインに関する情報を通知する機能	主体ごとに割り当てられた識別コードに対して、前回のログインに関する情報（日時や装置名等）を、次回のログイン時等のタイミングで主体に通知する機能を指す。 正当な主体以外の者が主体に割り当てられた識別コードを使用して不正にログインした場合に、正当な主体がそれを検知することができるようになると考えられる。
③	不正にログインしようとする行為を検知又は防止する機能	特定の識別コードによるログインにおいて、指定回数以上の主体認証情報の誤入力が検知された場合に、その旨を正当な主体や情報システムの運用担当者等に通知し、一定期間当該端末（又は識別コード）からのログイン操作受付を停止する機能を指す。 当該識別コードによる情報システムへの以後のログインを無効にすることも考えられる。 この機能により、不正なログインの試行の有無等について、正当な主体や情報システムの運用担当者等がその状況を確認するとともに、一定程度不正ログイン等を防止することができる。
④	情報システムへのログイン時にメッセージを表示する機能	情報システムへのログインの際に、軽率に不正アクセスに及ぶ行為を抑止する効果が期待されるメッセージを画面に表示する機能を指す。 通知メッセージとして、以下の例が考えられる。 ・アクセス履歴が管理者に通知されること ・利用状況を監視、記録しており、監査対象となること ・情報の目的外利用は禁止されていること ・情報システムへの不正アクセス行為は禁止されており、不正アクセス禁止法の罰則対象となること
⑤	主体認証情報の変更の際に、以前	利用者に対して主体認証情報の定期的な変更を求める場合に、以前に設定した主体認証情報と同じものを再設定すること

	機能	解説
	に設定した主体認証情報の再設定を防止する機能	を防止する機能を指す。 利用者に主体認証情報の定期的な変更を求める必要がある情報システムを対象としたものであり、利用者が以前に設定した主体認証情報と同じものを再設定すると、変更によってもたらされる効果が損なわれることから、変更履歴の世代管理を行い、何世代か前までの主体認証情報を再設定することを防止する方法が考えられる。 「(解説) 基本対策事項 6.1.1(1)-3「利用者に主体認証情報の定期的な変更を求める場合」について」も参照。
⑥	管理者権限によるログインの際に個別の識別コードによりログインすることを併せて求める機能	管理者権限を有する共有識別コードの利用において、実際の作業者となる個別の識別コードによるログインを併せて行うことを求める機能を指す。 管理者権限を有する共有識別コードのログイン記録だけでは、実際に作業をした管理者を個人単位で特定することが困難となるため、作業者個別の識別コードによるログインを行った後に管理者権限を有する共用識別コードによるログインを許可するものである。 例えば、当該情報システムの OS が Unix 系の場合には、一般利用者でログインした後に su コマンドで root に切り替えるという手順により、これを達成できる。また、その場合には、root によるログインを禁止する設定により、その手順を強制することができる。

なお、国民・企業と政府との間で申請、届出等のオンライン手続を提供するシステムにおいては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づいてセキュリティ要件を決定する必要があるが、リスクの影響度を導出する手法やパスワード等の対策基準等について記載があるため、その他の情報システムにおいても参考にするとよい。

- **基本対策事項 6.1.1(1)-1 a)「知識」について**

端末によっては、例えばパスワード以外にも、自分のみが知る「パターン」を主体認証情報として扱うケースがあるが、これも「知識」に分類される。

- **基本対策事項 6.1.1(1)-1 b)「所有」について**

「所有」による認証の例として、本学が個別に保有するアカウント情報のマスターデータベース機能を提供する「統合ディレクトリ」とのデータ連携を行う「職員等利用者共通認証基盤（GIMA; Government Identity Management for Authentication)」を介し、政府認証基盤（GPKI）における電子証明書を用いた認証、国家公務員 IC カードを用いた認証等が挙げられる。

- **基本対策事項 6.1.1(1)-1 c)「生体」について**

  生体情報による主体認証を用いる場合には、その導入前に、この方式特有の他人受入率（本人を他人と誤って認証してしまう確率）と本人拒否率（本人の認証が受け入れられない確率）の課題があることを考慮して情報システムを設計する必要がある。

- **基本対策事項 6.1.1(1)-3「利用者に主体認証情報の定期的な変更を求める場合」について**

  利用者に主体認証情報の定期的な変更を求めることの情報セキュリティ上の効果は、主体認証情報の運用方法や情報システムの認証技術の方式により異なるものであり、また、生体情報による主体認証方式のように利用者本人でも変更が不可能なものもある。定期的な変更に一定の効果がある場合、変更を求める間隔が短いほど効果は高まることになるが、変更を強制する頻度が高すぎれば、利用者の利便性を著しく低下させ、利用者が強度の低い安易なパスワードを設定しやすくなるなど、結果的に主体認証機能の安全性を低下させて逆効果をもたらし得る。

  したがって、利用者に主体認証情報の定期的な変更を求めるか否かは、その効果と逆効果を総合的に検討した上で判断する必要がある。

  なお、識別コード自体が存在せず、主体認証情報を複数の主体で共用せざるを得ない機器等の利用においては、例えば、人事異動等で利用者に変更が生じた際に利用者に主体認証情報の変更を求めるなどして、主体認証情報の漏えいによる不正行為を防止することが考えられる。

遵守事項

(2) 識別コード及び主体認証情報の管理

(a) 部局技術責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。

(b) 部局技術責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。

【 基本対策事項 】

＜6.1.1(2)(a)関連＞

6.1.1(2)-1 部局技術責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）すること。

6.1.1(2)-2 部局技術責任者は、識別コードの付与に当たっては、以下を例とする措置を講ずること。

a) 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

b) 主体への識別コードの付与に関する記録を消去する場合の部局総括責任者からの事前の許可

6.1.1(2)-3 部局技術責任者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ**安全な方法で主体認証情報を配布**するよう、措置を講ずること。

6.1.1(2)-4 部局技術責任者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。

6.1.1(2)-5 部局技術責任者は、知識による主体認証方式を用いる場合には、**他の情報システムで利用している主体認証情報を設定しない**よう主体に注意を促すこと。

6.1.1(2)-6 部局技術責任者は、情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、部局技術責任者の判断の下、やむを得ず**共用識別コードを付与する必要がある場合**には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。

6.1.1(2)-7 部局技術責任者は、主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、以下を例とする措置を講ずること。

a) 当該主体の**識別コードを無効にする**。

b) 当該主体に交付した主体認証情報格納装置を返還させる。

c) 無効化した識別コードを他の主体に新たに発行することを禁止する。

（解説）

- **基本対策事項 6.1.1(2)(a)「主体認証情報を適切に付与」について**

情報システムにおいて認証機能を統合している場合、各機器等の管理者権限を持つ

ローカルアカウントは通常の運用では未使用となるが、その場合においてもデフォルトパスワードのままにせず、設定するパスワードについても同一の値にしないといった措置を講ずる必要がある。

なお、主体認証が必要となる場面が多岐にわたるような情報システムの場合、認証連携を適切に用いることにより、業務の効率化を図ることも考えられる。

- **基本対策事項 6.1.1(2)-3「安全な方法で主体認証情報を配布する」について**

利用者以外の者（情報システムの管理者等）が主体認証情報を設定する場合には、以下を例とする方法で、当該主体認証情報を安全な方法で利用者に配布する必要がある。

- 本人の電子メールアドレスに対し、必要に応じて、暗号化を施すことにより、主体認証情報を送付する。この際、暗号化された主体認証情報が添付された電子メールに復号するための鍵を同時に付すのは情報セキュリティ上、好ましくない。
- 本人の電子メールアドレスに対して主体認証情報を入手するためのウェブサイト及びパスワードを送付し、当該パスワードによる認証の上で当該ウェブサイトから主体認証情報をダウンロードする。
- 本人の住所に対して主体認証情報を運搬する。

- **基本対策事項6.1.1(2)-5「他の情報システムで利用している主体認証情報を設定しない」について**

複数の情報システムにおいて共通の主体認証情報を設定していた場合、ある情報システムから漏えいした主体認証情報が他の情報システムで不正に利用されるというリスクが発生する。本学の管理下にない情報システムからの漏えいを防止することは不可能であるため、このような情報システムから主体認証情報が漏えいした場合の本学の情報システムへの影響について考慮しておく必要がある。対策の例としては、他の情報システムで利用している主体認証情報を本学の情報システムに設定しないよう注意喚起を表示する、識別コードを情報システム側で割り当てることで識別コードの共通利用を防止する、といった方法が考えられる。

- **基本対策事項 6.1.1(2)-6「共用識別コードを付与する必要がある場合」について**

共用識別コードは、その利用履歴だけでは利用者を特定できないため、情報セキュリティインシデントが発生した場合に、真相究明の支障となる可能性がある。この点を踏まえ、やむを得ず、共用識別コードを利用する場合には、利用者を特定するための以下を例とする仕組みを講ずる必要がある。

- 当該情報システムにおける別途の認証手段を併用する
- 入退室管理装置等の物理的認証手段を併用する

- **基本対策事項 6.1.1(2)-7 a)「識別コードを無効にする」について**

識別コードの付与を最小限に維持するため、退職等により不必要となった識別コードについては、これを無効にする必要がある。また、本人からの届出による場合のほか、人事異動等の時期を考慮の上、定期的及び必要に応じて不要な識別コードが存在

しないことを確認することにより、無効化漏れを防止することが期待できる。

6.1.2 アクセス制御機能

目的・趣旨

アクセス制御とは、情報システム及び情報へのアクセスを許可する主体を制限することである。複数の主体が情報システムを利用する場合、当該情報システムにおいて取り扱う情報へのアクセスを業務上必要な主体のみに限定することによって、情報漏えい等のリスクを軽減することができると考えられる。

遵守事項

(1) アクセス制御機能の導入

(a) 部局技術責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。

(b) 部局技術責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。

【 基本対策事項 】

＜6.1.2(1)(b)関連＞

6.1.2(1)-1 部局技術責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、必要に応じて、以下を例とするアクセス制御機能の要件を定めること。

a) 利用時間や利用時間帯によるアクセス制御

b) 同一主体による複数アクセスの制限

c) IP アドレスによる端末の制限

d) ネットワークセグメントの分割によるアクセス制御

（解説）

- **基本対策事項 6.1.2(1)-1「主体の属性、アクセス対象の属性に基づくアクセス制御」について**

具体的な手法としては、端末や共有フォルダ上のファイルやフォルダ（ディレクトリ）に対する許可属性のリストであるアクセス制御リスト（ACL; Access Control List）が挙げられる。ACL では例えば、アクセス対象の所有者／所有者の属するグループ／全利用者といったアクセス主体に対して、読み取り／書き込み／実行の権限を設定する。

ただし、一般的な情報システムでは、利用者が適切なアクセス制御の設定を行っても、システムの管理者は全てのファイルやフォルダへアクセス可能である。実際に、運用保守の担当者が、管理者権限相当のアクセス権限を行使して、機密性の高い情報を不正に閲覧するといった事案も確認されている。そのため、アクセス対象が要機密情報等の場合は、アクセス制御機能のみに頼らず、アクセス権限の無い者に閲覧等さ

れないよう、アクセス制限の対象に対して暗号化等の措置を考慮することが求められる。

- **基本対策事項 6.1.2(1)-1 d)「ネットワークセグメントの分割によるアクセス制御」について**

  業務や取り扱う情報の性質・量に応じて、重要な情報に攻撃が到達しないよう、情報システムの重要な情報を取り扱う部分を他の情報システムやインターネットから分離するといった対策をとる必要がある。特に、情報システムの管理を行う部分を独立したセグメントとし、これをインターネットから切り離しておくことは、攻撃の拡大阻止の観点から有効である。同時に、セグメント分割の意義を損なうことのないよう、各システムで取り扱うことができる情報についてルール化し、職員に徹底することも重要である。

  なお、遵守事項 5.2.1(2)(a)において、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否について判断を求めているが、本基本対策事項は、その際に併せて検討し、情報システムのネットワーク構成の要件を決定するとよい。

6.1.3 権限の管理

目的・趣旨

重要システムのアクセス制御機能を適切に運用するためには、主体から対象に対するアクセスの権限を適切に設定することが必要である。権限の管理が不適切になると、情報又は情報システムへ不正アクセスされるおそれが生じる。

また、情報システムの管理機能として、一般的に管理者権限にはあらゆる操作が許可される特権が付与されている。当該特権が悪意ある第三者等に入手された場合、主体認証情報等の漏えい、改ざん又は情報システムに係る設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念されることから、限られた主体のみに管理者権限が付与されることが重要である。

遵守事項

(1) 権限の管理

(a) 部局技術責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。

(b) 部局技術責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

【 基本対策事項 】

＜6.1.3(1)(a)関連＞

6.1.3(1)-1 部局技術責任者は、主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するため、以下を例とする措置を講ずること。

a) 業務上必要な場合に限定する

b) 必要最小限の権限のみ付与する

c) 管理者権限を行使できる端末をシステム管理者等の専用の端末とする

（解説）

- **基本対策事項 6.1.3(1)(b)「内部からの不正操作や誤操作を防止するための措置」について**

権限管理を行う情報システムのうち、内部からの不正操作や誤操作を防ぐための特に強固な権限管理が必要な情報システムについては、ある処理に対し、複数名による主体認証操作がなければ、その処理自体を完遂できない「デュアルロック機能」を導入することが考えられる。

その他の情報システムについては、操作ログを取得したり、確認画面を表示したりするなどの措置が考えられる。

- **基本対策事項 6.1.3(1)-1 a)「最小限の特権機能」について**

  管理者権限等の特権は、システム全体へのアクセス権を持ち、あらゆる操作が可能であることが多く、仮に不正な目的を有する悪意ある第三者等が当該権限を入手すれば、当該システムに対して不正な操作が可能となってしまう。必要最小限の権限のみ付与とは、特権が利用できる時間的な機会を限定すること又はあらかじめ限られた操作が可能な特権を付与することにより、当該特権を使った不正な操作が発生する機会を減らし、結果的に安全性を強化するものである。

  例えば、管理作業をするときに限定してその識別コードを利用することを可能とする方式（例 Unix 系システムにおける sudo 等）や、あらかじめ実行できるプログラムやアクセス可能な領域を限定し、特権を付与する方式がある。

6.1.4 ログの取得・管理

目的・趣旨

情報システムにおけるログとは、通信履歴、その他運用管理等に必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の情報セキュリティインシデント及びその予兆を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

遵守事項

(1) ログの取得・管理

(a) 部局技術責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。

(b) 部局技術責任者は、情報システムにおいて、その特性に応じて**ログを取得する目的**を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの**保存期間**、要保護情報の観点でのログ情報の取扱方法、及び**ログが取得できなくなった場合の対処方法**等について定め、適切にログを管理すること。

(c) 部局技術責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について**点検又は分析**を実施すること。

【 基本対策事項 】

＜6.1.4(1)(a)関連＞

6.1.4(1)-1 部局技術責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の**時刻を同期**させ、ログに時刻情報も記録されるよう、設定すること。

＜6.1.4(1)(b)関連＞

6.1.4(1)-2 部局技術責任者は、所管する情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理すること。

a) 事象の主体（人物又は機器等）を示す識別コード
b) 識別コードの発行等の管理記録
c) 利用者による情報システムの操作記録
d) **事象の種類**
e) **事象の対象**
f) 正確な日付及び時刻
g) 試みられたアクセスに関わる情報

h) 電子メールのヘッダ情報及び送信内容
i) 通信パケットの内容
j) 操作する者、監視する者、保守する者等への通知の内容

6.1.4(1)-3 部局技術責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、**ログ情報の保全方法**を定めること。

6.1.4(1)-4 部局技術責任者は、**ログが取得できなくなった場合の対処方法**を定めること。

＜6.1.4(1)(c)関連＞

6.1.4(1)-5 部局技術責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入すること。

a) ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の**自動化**

（解説）

- **基本対策事項 6.1.4(1)(b)「ログを取得する目的」について**

情報システムにおいて出力できる様々なログは、その全てを無期限に保存し、定期的にその点検や分析を行うことができれば理想的であるが、そのためには莫大なストレージ容量が必要になり、解析にかかる時間も長くなるなど、現実的ではない。

そのため、情報システムの特性（取り扱われる情報、接続されるネットワーク、設置環境、利用者等）に応じ、当該情報システムでどのような事象を検知すべきかを目的として設定した上で、取得すべきログ情報やその保存期間等を検討することが望ましい。

例えば、標的型攻撃の早期発見・初期調査を目的とした場合には、以下のようなログを取得することが考えられる。

- 電子メールサーバ： 電子メールクライアントで表示される表記名*、送信者アドレス*、実際の電子メール送信者アドレス*、添付ファイル名*
- ファイアウォール： ファイアウォールポリシーのアクション、送信先のゾーン設定*、送信元アドレス、送信元ポート、送信先アドレス、送信先ポート
- Web プロキシサーバ： URL アドレス、送信先サイトのポート、メソッド、UserAgent*、アクセス時間
- DNS キャッシュサーバ： 名前解決を行おうとしている PC 等の IP アドレス*、要求及び応答したホストや IP アドレスの情報*
- 認証サーバ（Active Directory）： 資格認証の確認の監査*、Kerberos 認証サービスの監査*、ログオンの監査*、その他ログオン／ログオフイベントの監査*、特殊なログオンの監査*

なお、上記のログの例において、項目名の終わりに*を付与しているログ項目は各機器の標準設定では出力されない場合があるため、注意が必要である。

- **基本対策事項 6.1.4(1)(b)「保存期間」について**

保存期間については、情報システム又は当該システムに保存される情報の特性に基

づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは1年間以上保存することが望ましい。

なお、ログの長期保存にはコストがかかるため、費用を抑える観点から、直近のログはすぐに調査可能なハードディスク等のオンラインの電磁的記録媒体に保存し、それ以降はテープや光ディスク等の長期保存に適した外部電磁的記録媒体に保存する方法も考えられる。オンラインの電磁的記録媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する。

- **基本対策事項 6.1.4(1)(b)「ログが取得できなくなった場合の対処方法」について**

  以下を例とする対処方法が考えられる。

  - 古いログに上書きする設定を施し、ログの取得を継続する。
  - ログが取得できなくなった際に出力されているメッセージ、エラーコード等を確認し、障害の原因を特定すると同時に当該障害の原因の対処を実施する。
    なお、情報システムにおいて、事前に収集したログのバックアップ設定を行っている場合は、復旧手順に従い、速やかにログを復旧させる。このとき、復旧するバックアップの古さの目標値を示すRPO（Recovery Point Objective）は情報システムの特性及び取り扱う情報によって、適切に設定する必要がある。
  - あらかじめ用意したファイル容量を使い切った場合、情報システムに対する挙動がログに保存されないため、一旦情報システムを停止し、ファイル容量を新たに用意するなどした後に、ログの取得を再開する。

- **基本対策事項 6.1.4(1)(c)「点検又は分析」について**

  情報システムの特性等に応じて、点検・分析の頻度や分析の精度を高める必要がある場合には、専任の分析担当者の設置や監視事業者への委託を検討することが考えられる。

- **基本対策事項 6.1.4(1)-1「時刻を同期」について**

  具体的な実装例としては、ログを取得する機器のシステム時刻を、タイムサーバを用いて同期する方法がある。タイムサーバは、NTP（Network Time Protocol）やSNTP（Simple Network Time Protocol）等の方式により、ネットワーク上のクライアント機器に対して、時刻を提供する。例えば、公開NTPサービスを用いる方式や組織内にタイムサーバを設置し、サーバ装置・端末・通信回線装置をタイムサーバに時刻同期するよう設定する方式が挙げられる。なお、後者については、タイムサーバを複数利用することにより、時刻の精度や冗長性を高めることができる。

  また、機器によっては明示的に設定を行わないとログに出力する時刻が現地時間とならない場合があるため注意が必要である。

- **基本対策事項 6.1.4(1)-2 d)「事象の種類」について**

  事象の種類の例を以下に示す。

  - ウェブサイトへのアクセス
  - ログイン及びログアウト

- サーバ、ファイルへのアクセス
- 要保護情報の書き出し
- アプリケーションの起動及び終了
- 特定の操作指令

- **基本対策事項 6.1.4(1)-2 e)「事象の対象」について**

事象の対象の例を以下に示す。

- アクセスした URL
- ログインしたアプリケーション名
- アクセスしたファイル名及びファイル内容
- 起動及び終了したアプリケーション名
- 特定の操作指令の対象

- **基本対策事項 6.1.4(1)-3「ログ情報の保全方法」について**

取得したログ情報に対する不正な消去、改ざん及びアクセスを防止するためのログ情報の保全方法として、以下の例が考えられる。

- ログ収集サーバにログを転送し保存する。ログ収集サーバの管理者を他のサーバ等の管理者と異なる者とし、他の管理者によるログ情報の消去や改ざんが行われないようにする。
- ログをテープ等の外部電磁的記録媒体に書き出し、情報システムから切り離して保管する。
- ログを書き換え不能な外部電磁的記録媒体(DVD-R 等)に書き出して保管する。

- **基本対策事項 6.1.4(1)-6 a)「自動化」について**

ログとして取得する項目数、利用者数等が多くなるにつれて、ログの量は膨大になり、システム担当者等がログを目視することによって問題（又はその予兆）を検出するのは、困難を極める。システム自体に実装される機能や各種運用管理ツールを組み合わせ、ログの点検・分析・通知が自動的に実行されるなど、ログ管理作業を支援する仕組みを構築することが望ましい。

6.1.5 暗号・電子署名

目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用するアルゴリズムに加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズムが危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

遵守事項

(1) 暗号化機能・電子署名機能の導入

(a) 部局技術責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。

(ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(b) 部局技術責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

(ア) 事務従事者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、**やむを得ない場合**を除き、「電子政府推奨暗号リスト」又は、本学における検証済み暗号リストがあればその中に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

(ウ) 暗号化及び電子署名に使用する**アルゴリズムが危殆化**した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、**管理手順を定めること**。

(c) 部局技術責任者は、本学における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な**電子証明書を UPKI** 電子証明書発行サービス**が発行している**場合は、それを使用するよう

に定めること。

【 基本対策事項 】

＜6.1.5(1)(a)関連＞

6.1.5(1)-1 部局技術責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。

a) 情報システムのコンポーネント（部品）として、**暗号モジュールを交換**することが可能な構成とする。

b) **複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択**することが可能な構成とする。

c) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護される製品を利用することを確実にするため、**「暗号モジュール試験及び認証制度」に基づく認証**を取得している製品を選択する。

d) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、**耐タンパ性**を有する暗号モジュールへ格納する。

e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、**安全性に実績のある暗号プロトコル**を選択し、**長期的な秘匿性**を保証する観点を考慮する。

（解説）

- **遵守事項 6.1.5(1)(b)(イ)「やむを得ない場合」について**

情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用することが原則であるが、連携する他の情報システム側で対応していないなどの場合も想定される。このような場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズム以外のものを採用することもやむを得ないと考えられるが、「推奨候補暗号リスト」や「運用監視暗号リスト」を参照の上、安全性が高いアルゴリズムを採用することが必要である。

- **遵守事項 6.1.5(1)(b)(ウ)「アルゴリズムが危殆化」について**

暗号化や電子署名に用いられる暗号アルゴリズムは、年月が経つにつれ、情報システムの処理能力の向上や新たな暗号解読技法の考案等によって、アルゴリズム設計当初の強度を失い、結果として、安全性を保てなくなる。このことを一般に「アルゴリズムが危殆化する」という。

暗号アルゴリズムの強度には理論上の強度及び実装上の強度が存在する。理論上の強度の低下は情報システムの処理能力の向上や暗号解読法の考案によるところが大きく、実装上の強度の低下はサイドチャネル攻撃等の攻撃技術によるところが大きい。

サイドチャネル攻撃の例として、実装時に暗号アルゴリズムの動作に伴う消費電力や暗号モジュールから漏えいする電磁波等の付加的な情報を悪意ある第三者等が知り得る場合には、実装上の強度は極端に低下する可能性がある。

- **遵守事項 6.1.5(1)(b)(ウ)「管理手順を定めること」について**

暗号化された情報の復号又は電子署名の付与に用いる鍵（以降本項において「鍵」という。）の管理手順として、以下の視点を含む鍵のライフサイクルを考慮した管理手順を策定するとよい。また、暗号化された情報の復号や電子署名の付与の際には、本人及び管理上必要のある者のみが知り得る秘密の情報を用いる必要があることから、適切に管理する必要がある。

- 鍵の生成

  適切な暗号モジュールの内部において、その値を推定することが困難である乱数又は擬似乱数に係る処理を通じて生成し、かつ利用者以外の者が入手できないことを保証する仕組みが必要である。

- 鍵の配送

  鍵の受取先と事前に対面等で確認し合うなどにより、受取先の正当性に係る十分な確証が得られない限り、オンライン上での鍵の配送を行うべきではない。鍵を配送する際は、受取先のなりすまし対策等、配送先が確実であることを保証するとともに当該鍵に係る情報が適切に保護される仕組みが必要である。

- 鍵の保管

  鍵は、例えば HSM 等の保存装置又は記録媒体等に適切に保護された環境で保管され、第三者等による窃取の防止に加え、改ざんからの保護、検知及び回復を実現する仕組みを備えることが必要である。

- 鍵の利用

  鍵はその運用期限が有効な限り、当該鍵へのアクセスが取扱いの許可されたものだけに限定されるよう可用性が確保され、かつ適切に実装された上で利用することが必要である。

- 鍵の期限切れ

  有効期限を過ぎた鍵は使用を停止し、適切な手段で取り除かれることが必要である。

- 鍵の更新

  鍵の有効期限が終了した後も運用を継続する場合、鍵としての継続性を維持するため、基本的に有効期限の終了前に古い鍵のパラメータを基に、新たな鍵を生成することが望ましい。

  なお、古い鍵は適切に廃棄されることが必要である。

- 鍵の失効

  鍵の漏えいによる危殆化や、鍵を利用していた行政事務従事者が組織から離れることに伴う鍵の登録抹消等により、そのコピーやバックアップが存在する場合も含め、有効期限前の鍵の利用を適切に停止することが必要である。

- 鍵の廃棄

特別な理由を除き、不要となった鍵の情報はそのコピーやバックアップが存在する場合も含め、有効期限後に適切な物理的又は電磁気学的な消去方法を用いて確実に消去される仕組みが必要である。

- **遵守事項 6.1.5(1)(c)「電子証明書を UPKI 電子証明書発行サービスが発行している」について**

  UPKI 電子証明書発行サービス以外が発行するサーバ証明書、コード署名証明書等の電子証明書が有効期限内の場合、次期更新時には、UPKI 電子証明書発行サービスで発行している電子証明書を利用することが求められる。

- **基本対策事項 6.1.5(1)-1 a)「暗号モジュールを交換」について**

  暗号モジュールは、暗号化、電子署名、ハッシュ関数等の暗号に関連した機能を提供するソフトウェアの集合体又はハードウェアとして定義される。選択した暗号化アルゴリズムが将来危殆化することを想定し、暗号モジュールの交換が可能な構成とすることを、情報システムの設計段階から考慮する必要がある。

  また、あらかじめ暗号モジュールのアプリケーションインタフェースを統一しておくなどを考慮する必要がある。

- **基本対策事項 6.1.5(1)-1 b)「複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択」について**

  選択したアルゴリズムが将来危殆化することを想定し、危殆化していない他のアルゴリズムへ直ちに変更できる機能と併せて、暗号利用モード等との組合せ等により脆弱性の顕在化が認められない安全なプロトコルを選択できる機能も、あらかじめ情報システムに設けておく必要がある。

- **基本対策事項 6.1.5(1)-1 c)「「暗号モジュール試験及び認証制度」に基づく認証」について**

  アルゴリズム自体が安全であっても、それをソフトウェアやハードウェアへ実装する際、生成する疑似乱数に偏りが生じるなどの理由で疑似乱数が推測可能であったり、鍵によって処理時間に統計的な偏りが生じるなどの理由で鍵情報の一部が露呈したりすると、情報システムの安全性が損なわれるおそれがあることから、これらを確認するには、ISO/IEC19790 に基づく「暗号モジュール試験及び認証制度」が利用可能である。

- **基本対策事項 6.1.5(1)-1 d)「耐タンパ性」について**

  JIS X 19790 (ISO/IEC 19790)の規定によると、耐タンパ性は以下の 3 つの機能から構成される。

  - タンパ検出
    暗号モジュールのセキュリティを危殆化する試みがなされたことの、暗号モジュールによる自動的な判定
  - タンパ証跡
    暗号モジュールのセキュリティを危殆化する試みがなされたことを示す、外観

上の表示

- タンパ応答

暗号モジュールがタンパを検出したときに採る自動的な動作

また、暗号モジュールを利用する環境等に応じ、セキュリティレベルが 1 から 4 まで設定されている。セキュリティレベル 1 は、最小限の物理的保護を要求している。セキュリティレベル 2 では、タンパ証跡メカニズムの追加を要求している。セキュリティレベル 3 では、除去可能なカバー及びドアに対して、タンパ検出及びタンパ応答メカニズム付きの強固な囲いの利用の要求事項を追加している。セキュリティレベル 4 では、囲い全体に対して、タンパ検出及びタンパ応答メカニズム付きの強固な囲いの利用の要求事項を追加している。

なお、タンパ検出及びタンパ応答は、タンパ証跡の代わりにはならない。

暗号モジュールの耐タンパ性に関わるセキュリティレベルは、情報システムが取り扱う以下の特性を踏まえて選択することが望ましい。

- 暗号化及び／又は復号する情報の特性
- 電子署名が付与される情報の特性

- **基本対策事項 6.1.5(1)-1 e)「安全性に実績のある暗号プロトコル」について**

情報システムで暗号を用いるとき、暗号アルゴリズムの適切な選択に加え、暗号プロトコル（暗号アルゴリズムをどのように用いるかの手順）が適切なものとなっている必要がある。一般に、情報システムを新規に構築するときに、独自の暗号プロトコルを設計することは、その安全性について十分に検証されないときは、期待される安全性が確保されていない可能性がある。安全な暗号プロトコルの設計は高度な専門性を有する者以外には容易なことではないため、可能な限り、独自の設計を避け、既に広く利用実績のある著名な暗号プロトコルを用いることが求められる。

なお、必要とする機能を実現する暗号プロトコルとして既存のものが存在しない場合はこの限りでないが、独自に暗号プロトコルを設計するときは、その安全性に関して十分に検証する必要がある。

- **基本対策事項 6.1.5(1)-1 e)「長期的な秘匿性」について**

情報システム上で機微な情報のやり取りを行う場合、情報を暗号化して通信しても、その暗号文が悪意ある第三者等に傍受され、将来の解読に備えて長期間にわたり保管されるという脅威が想定される。この場合に、「前方秘匿性（Forward Secrecy）」を有しない暗号プロトコルを用いた結果、公開鍵暗号の鍵が将来破られることになれば、過去に遡って全ての暗号文が解読されてしまうことになる。そのため、長期の機密性を確保する必要のある機微な情報のやりとりを行う情報システムを構築するときは、「前方秘匿性」を実現する暗号プロトコルの採用を検討し、必要かつ可能であれば、採用することが求められる。

遵守事項

(2) 暗号化・電子署名に係る管理

(a) 部局技術責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。

(ア) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。

(イ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、事務従事者と共有を図ること。

【 基本対策事項 】

＜6.1.5(2)(a)(ア)関連＞

6.1.5(2)-1 部局技術責任者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とすること。

a) 信頼できる機関による電子証明書の提供

b) 本学の窓口での電子証明書の提供

（解説）

- **基本対策事項 6.1.5(2)-1 a)「信頼できる機関による電子証明書の提供」について**

  例えば、信頼できる機関のサイトから、利用者が電子署名を検証するための電子証明書をダウンロードできるように環境を整備する方法である。利用者はダウンロードした電子証明書を端末に取り込み、それを基に署名検証を行う。

- **基本対策事項 6.1.5(2)-1 b)「本学の窓口での電子証明書の提供」について**

  本学において、利用者に電子署名を検証するための電子証明書を記録媒体で配布する方法である。利用者は記録媒体経由で電子証明書を端末に取り込み、それを基に署名検証を行う。

6.2　情報セキュリティの脅威への対策

6.2.1　ソフトウェアに関する脆弱性対策

目的・趣旨

本学の情報システムに対する脅威としては、第三者が情報システムに侵入し政府の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に、国民向けに提供するサービスが第三者に侵入され、個人情報の漏えい等が発生した場合、政府に対する社会的な信用が失われる。

一般的に、このような攻撃では、情報システムを構成するサーバ装置、端末及び通信回線装置のソフトウェアの脆弱性を悪用されることが想定される。したがって、本学の情報システムにおいては、ソフトウェアに関する脆弱性について、迅速かつ適切に対処することが求められる。

なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2 項「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。

遵守事項

(1)　ソフトウェアに関する脆弱性対策の実施

(a)　部局技術責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。

(b)　部局技術責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。

(c)　部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。

(d)　部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。

【 基本対策事項 】

＜6.2.1(1)(a)(d)関連＞

6.2.1(1)-1　部局技術責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む情報を適宜入手すること。

a)　脆弱性の原因

b)　影響範囲

c)　対策方法

d) 脆弱性を悪用する不正プログラムの流通状況

6.2.1(1)-2 部局技術責任者は、利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しないこと。

6.2.1(1)-3 部局技術責任者は、構成要素ごとにソフトウェアのバージョン等を把握し、脆弱性対策の状況を確認すること。

＜6.2.1(1)(c)関連＞

6.2.1(1)-4 部局技術責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項について判断すること。

a) 対策の必要性
b) 対策方法
c) 対策方法が存在しない場合又は対策が完了するまでの期間に対する一時的な回避方法
d) 対策方法又は回避方法が情報システムに与える影響
e) 対策の実施予定
f) 対策試験の必要性
g) 対策試験の方法
h) 対策試験の実施予定

＜6.2.1(1)(c)(d)関連＞

6.2.1(1)-5 部局技術責任者は、脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。

a) 実施日
b) 実施内容
c) 実施者

6.2.1(1)-6 部局技術責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「対策用ファイル」という。）は、信頼できる方法で入手すること。

＜6.2.1(1)(d)関連＞

6.2.1(1)-7 部局技術責任者は、脆弱性対策の状況を確認する間隔は、可能な範囲で短くすること。

（解説）

- **遵守事項 6.2.1(1)(b)「公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策」について**

脆弱性が明らかになっていない段階においても、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施する。対策としては、特定のメモリ上の実行権限の削除又はバッファオーバーフローの検知によるアプリケーションの実行停止等の対策を実施すること等が挙げられる。

- **遵守事項 6.2.1(1)(c)「サーバ装置、端末及び通信回線装置上で利用するソフトウェア」について**

  情報システムの構築時に、ソフトウェアを効率的に開発するためにソフトウェアフレームワーク開発用のフレームワークとして情報システムに組み込まれたまま納入されるソフトウェア等、情報システムの運用中に動作しないものについても考慮する必要がある。当該ソフトウェアの脆弱性による影響についても考慮し、脆弱性対策の対象とするソフトウェアを定めておくことが望ましい。

- **基本対策事項 6.2.1(1)-1「情報を適宜入手」について**

  情報システムを構成するサーバ装置、端末及び通信回線装置上で利用するソフトウェアの脆弱性に関する情報は、製品ベンダや脆弱性情報提供サイト等を通じて適時調査を行う必要がある。自動アップデート機能を持つソフトウェアの場合には、当該機能を利用して、定期的に脆弱性に関連する情報が報告されているかを確認する方法で差し支えないが、自動アップデート機能の対象範囲を把握し、対象範囲外のソフトウェアについては適時調査を行う必要がある。例えば、ウェブアプリケーション等のソフトウェアを効率的に開発するためにソフトウェアフレームワークを利用する場合があるが、ソフトウェアフレームワークを利用して開発したアプリケーションは自動アップデートが行えないため、脆弱性の有無については適宜調査を行う必要がある。

  入手した脆弱性に関連する情報及び対策方法に関しては、脆弱性対策を効果的に実施するために、他の部局技術責任者と共有することが望ましい。

- **基本対策事項 6.2.1(1)-1 d)「脆弱性を悪用する不正プログラムの流通状況」について**

  脆弱性が既知になると、インターネット上の情報交換コミュニティ等を通じて、その脆弱性を悪用する方法が考案され、その悪用方法を機械的に実行するための不正プログラム(exploit コードとも呼ばれる)が作られ、次第に広まっていく。この「脆弱性を悪用する不正プログラム」が流通している段階に入ると、脆弱性が攻撃されるリスクが格段に高まると考えられる。脆弱性を悪用する不正プログラムが世の中に流通していることが確認された場合には、速やかに当該の脆弱性について対処することが望ましい。

- **基本対策事項 6.2.1(1)-2「サポート期間を考慮」について**

  利用するソフトウェアのサポート期間が過ぎた場合、それ以降はセキュリティ関連の脆弱性を修正するためのセキュリティパッチは、原則としてソフトウェアベンダから提供されなくなる。したがって、情報システムのライフサイクルを考慮し、少なくとも情報システムの次期改修までは対策用ファイルの提供が継続されるソフトウェアを選定する必要がある。

  また、情報システムは特定のソフトウェアバージョンに依存しないよう設計することが望ましいが、情報システムの中には、特定のソフトウェアバージョンに強く依存する場合がある。この場合には、ソフトウェアをバージョンアップすることが困難となるが、新しいバージョンのソフトウェアでしか対処できない脆弱性が発生したときに、情報システムの停止という最悪の事態も想定される。したがって、情報システム

が特定のソフトウェアバージョンに依存せざるを得ない場合には、当該ソフトウェアのサポート期間を考慮して情報システムの更改について検討しておく必要がある。

- **基本対策事項 6.2.1(1)-2「サポートが受けられないソフトウェア」について**

  ソフトウェアベンダによるサポートや他の事業者によるサポートサービスが一切受けられないものを対象としている。ソフトウェアベンダの製品ロードマップの見直し等により、サポートの打ち切りが突然予告されることもあり得るため、利用するソフトウェアのサポート期間に関する情報を適時入手し、ソフトウェア更改やサポート事業者の切替え等の対策が適切に講じられるよう考慮することが望ましい。

- **基本対策事項 6.2.1(1)-3「ソフトウェアのバージョン等を把握」について**

  把握すべき情報としては、ソフトウェアのバージョンのほか、脆弱性対策の最終実施日、未実施の脆弱性対策等がある。

- **基本対策事項 6.2.1(1)-3「脆弱性対策の状況を確認」について**

  OS や各種サーバ、ファイアウォール等の通信回線装置等における脆弱性対策の状況を効率的に確認する方法として、専用ツールや事業者が提供するサービス等を利用する脆弱性診断の実施が挙げられる。脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、ソフトウェアの種類によって利用する脆弱性診断を使い分ける必要がある。

  ソースコード診断では、独自に開発したソフトウェアのソースコードを対象に、静的解析ツール等を用いて脆弱性の有無を検証する。したがって、運用開始までにソースコード診断を実施し、運用開始後にソースコードへ修正を加えた場合は、再度診断を実施することが望ましい。

  プラットフォーム診断では、OS や各種サーバ、ファイアウォール等を対象に、テスト用の通信パケットを送信するなどの方法によって、最新のセキュリティパッチが適用されているか、設定が適切に行われているか、不要な通信ポートが開いていないかなどを検証する。したがって、運用開始までにプラットフォーム診断を実施し、その後も例えば年に 1 回診断を実施するなど、定期的に実施することが望ましい。

  ウェブアプリケーション診断では、独自に開発したウェブアプリケーションを対象に、実際に不正なデータをウェブアプリケーションに送信するなどの方法によって、SQL インジェクションやクロスサイトスクリプティング等の脆弱性が存在しないかを検証する。したがって、運用開始までにウェブアプリケーション診断を実施し、運用開始後においても、ウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合は、再度診断を実施することが望ましい。

- **基本対策事項 6.2.1(1)-4 c)「一時的な回避方法」について**

  ソフトウェアにおいて脆弱性が顕在化した際に、ソフトウェアベンダが対応するまでの間は、当該ソフトウェアの利用を禁止する又は脆弱性が関係する機能を無効化するなどの対応が必要となる。

  しかし、これらの対応によって業務に著しく悪影響を与えることが想定される場合は、事前に必要な措置を講じておくことが求められる。例えば、ブラウザは業務上利

用せざるを得ないケースが多いが、異なるソフトウェアベンダが提供する複数のブラウザを端末に導入しておくことで、業務継続性を維持しつつ、脆弱性を悪用した攻撃を受けるリスクを低減することができる。複数のブラウザを導入することは、情報システムのコスト増加を招く可能性があるが、一方のブラウザを常時利用するとともに、他方を緊急時のインターネットへのアクセス手段として利用するなど、用途を分ける方法も考えられる。また、ログ出力の設定を確認し、対応が完了するまでの期間、出力されたログの監視を強化するなどの対応も考えられる。

- **基本対策事項 6.2.1(1)-4 f)「対策試験」について**

  「対策試験」とは、脆弱性対策の実施による情報システムへの影響の有無を確認するために、事前に試験用の情報システムを用いて試験することが想定される。

- **基本対策事項 6.2.1(1)-6「対策用ファイル」について**

  入手した対策用ファイルに悪意のあるコードが含まれている可能性を考慮し、対策用ファイルは信頼できる方法で入手する必要がある。

  信頼できる方法としては、ソフトウェアの開発元等が公開するウェブサイトからダウンロードする方法、又は郵送により対策用ファイルが記録された外部電磁的記録媒体を入手する方法が挙げられる。また、対策用ファイルが改ざんされていないこと等の完全性を検証できる手段があれば、併せてこれを実行する必要がある。

6.2.2 不正プログラム対策

目的・趣旨

情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼすおそれがある。このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

遵守事項

(1) 不正プログラム対策の実施

(a) 部局技術責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で**動作可能な不正プログラム対策ソフトウェア等**が存在しない場合を除く。

(b) 部局技術責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

(c) 部局技術責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。

【 基本対策事項 】

＜6.2.2(1)(a)関連＞

6.2.2(1)-1 部局技術責任者は、不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるよう構成すること。

6.2.2(1)-2 部局技術責任者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

6.2.2(1)-3 部局技術責任者は、不正プログラム対策ソフトウェア等は、定期的に全てのファイルを対象としたスキャンを実施するよう構成すること。

＜6.2.2(1)(b)関連＞

6.2.2(1)-4 部局技術責任者は、想定される全ての**感染経路を特定**し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による**感染拡大の防止**等の必要な対策を行うこと。

＜6.2.2(1)(c)関連＞

6.2.2(1)-5 部局技術責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。

a) 不正プログラム対策ソフトウェア等の導入状況

b) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況

（解説）

- **遵守事項 6.2.2(1)(a)「動作可能な不正プログラム対策ソフトウェア等」について**

不正プログラム対策ソフトウェアの例としては、コンピュータウイルスを検知対処する「ウイルス対策ソフトウェア」や、キーロガーやアドウェア等のいわゆるスパイウェアを検知対処する「スパイウェア対策ソフトウェア」等がある。

多くのメインフレームシステム並びに OS 及びアプリケーションを搭載していないサーバ装置及び端末については、動作可能な不正プログラム対策ソフトウェア等が存在しないため、本対策事項の対象外である。ただし、新たに動作可能な不正プログラム対策ソフトウェア等が出現した場合には、速やかな導入が求められることから、部局技術責任者は、該当するサーバ装置及び端末の把握を行っておくとともに、不正プログラム対策ソフトウェア等に関してベンダが提供するサポート情報に常に注意を払っておくことが望ましい。

また、新たな不正プログラムの存在が明らかになった後でも、利用中の不正プログラム対策ソフトウェア等に用いる定義ファイルがベンダから配布されないなど、日常から行われている不正プログラム対策では対処が困難と判断される場合、部局技術責任者は事務従事者に回避策の実施を指示する必要がある。

なお、回避策は一律ではなく、個々の状況によって様々な内容があり得る。例えば、インターネット上の一部のウェブサイトを閲覧すると不正プログラムに感染することが判明している場合に、不正プログラム対策ソフトの定義ファイルが対応するまでの間、一時的にインターネット閲覧を制限する、という回避策が想定される。

- **基本対策事項 6.2.2(1)-4「感染経路を特定」について**

不正プログラムの感染経路には、電子メール、ウェブ等のネットワーク経由のほか、不正プログラムに感染した外部電磁的記録媒体経由も考えられる。

不正プログラム対策ソフトウェア等は、製品ごとに不正プログラム定義ファイルの提供時期及び種類が異なる。また、これらは現存する全ての不正プログラムを検知及び除去できるとは限らず、不正プログラム対策ソフトウェア等の不具合により不正プログラムの検知又は除去に失敗する危険性もある。このことから、不正プログラムによる被害を低減させるため、感染経路において、異なる定義ファイルを用いる不正プログラム対策製品を組み合わせる、又は、定義ファイルパターンマッチングやふるまい検知等の異なる技術を用いる製品を組み合わせることにより、どれか一つの不具合で、その環境の全てが不正プログラムの被害を受けることのないようにすることが望ましい。例えば、電子メールサーバに導入するウイルス対策ソフトウェアと端末に導入するウイルス対策ソフトウェアについて、それぞれ異なるウイルス定義ファイルを用いる製品を導入すること等が考えられる。

- **基本対策事項 6.2.2(1)-4「感染拡大の防止」について**

ネットワークを経由した感染拡大の防止策としては、例えば以下が挙げられる。

  - OS やアプリケーションに関するセキュリティパッチ及び不正プログラム定義ファイルについて最新化されていない端末をネットワークに接続させない仕組

みの導入

- 通信に不正プログラムが含まれていることを検知したときに、その通信をネットワークから遮断する仕組みの導入

6.2.3 サービス不能攻撃対策

目的・趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、本学の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。

遵守事項

(1) サービス不能攻撃対策の実施

(a) 部局技術責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下この項において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いて**サービス不能攻撃**への対策を行うこと。

(b) 部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。

(c) 部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。

【 基本対策事項 】

＜6.2.3(1)(a)関連＞

6.2.3(1)-1 部局技術責任者は、サーバ装置、端末及び通信回線装置について、以下を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。

a) パケットフィルタリング機能
b) 3-way handshake 時のタイムアウトの短縮
c) 各種 Flood 攻撃への防御
d) アプリケーションゲートウェイ機能

＜6.2.3(1)(b)関連＞

6.2.3(1)-2 部局技術責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築すること。

6.2.3(1)-3 部局技術責任者は、サーバ装置、端末及び通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、以下を例とする対策を検討すること。

a) **インターネットに接続している通信回線**の提供元となる事業者が別途提供す

る、サービス不能攻撃に係る通信の遮断等の対策
b) サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入
c) サーバ装置、端末及び通信回線装置及び通信回線の冗長化

6.2.3(1)-4 部局技術責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討すること。

＜6.2.3(1)(c)関連＞

6.2.3(1)-5 部局技術責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定めること。

6.2.3(1)-6 部局技術責任者は、監視対象の監視記録を保存すること。

（解説）

- **遵守事項 6.2.3(1)(a)「サービス不能攻撃」について**

サービス不能攻撃は、DoS 攻撃(Denial of Service)とも呼ばれる。また、この DoS 攻撃を複数の拠点から一か所に対して行う攻撃は、DDoS 攻撃(Distributed Denial of Service)と呼ばれ、攻撃元が複数に分散しているために防御側の対処が困難な攻撃として知られている。

- **基本対策事項 6.2.3(1)-3 a)「インターネットに接続している通信回線」について**

情報システムに対してサーバ装置、端末及び通信回線装置に係るサービス不能攻撃の対策を実施しても、学外へ接続する通信回線及び通信回線装置への過負荷の影響を完全に排除することは不可能である。このため、インターネットに接続している通信回線の提供元となる事業者に確認した上で、サービス不能攻撃発生時の対処手順や連絡体制を整備する必要がある。

- **基本対策事項 6.2.3(1)-3 c)「冗長化」について**

冗長化の例としては、サービス不能攻撃が発生した場合に備え、サービスを提供するサーバ装置、端末、通信回線装置又は通信回線について、負荷を分散させる、又はそれぞれ代替のものに切替えるなどにより、サービスを継続することができるように情報システムを構成することが考えられる。

なお、代替のものへの切替えについては、サービス不能攻撃の検知及び代替サーバ装置等への切替えが許容される時間内に行えるようにする必要がある。

- **基本対策事項 6.2.3(1)-4「攻撃への対処を効率的に実施できる手段」について**

対処例としては、サービス提供に利用している通信回線がサービス不能攻撃により過負荷状態に陥った場合においても、サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するための装置を操作できる手段を確保することが挙げられる。具体的には、管理者が当該装置を操作するためのサーバ装置、端末及び通信回線を、サービス提供に利用しているものとは別に用意することが挙げられる。

また、サービス不能攻撃に伴い、本学の自己管理ウェブサイトの閲覧障害が発生した場合においても、緊急性・重要度が高い情報が長時間閲覧できなくなることは極力

回避すべきである。これに鑑み、災害情報等の緊急性が高く、国民の生命や財産に著しく影響を及ぼしうるような重要情報については、広報担当とも協力するなどして、サービス不能攻撃を受けた際にも発信を可能とするよう、閲覧障害時の告知ページに最低限のテキストデータを掲載するなどの必要な措置を考慮するとよい。

- **基本対策事項 6.2.3(1)-5「監視方法及び監視記録の保存期間」について**

インターネットからアクセスされるサーバ装置や、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する必要がある。

「監視方法」については、サービス不能攻撃を受けることに関する監視には、稼動中か否かの状態把握や、システムの構成要素に対する負荷の定量的な把握(CPU 使用率、プロセス数、ディスク I/O 量、ネットワークトラフィック量等)がある。監視方法は多種多様であるため、当該情報システムの構成等の特性に応じて適切な方法を選択する必要がある。

「監視記録の保存期間」については、監視対象の状態の変動を把握するという目的に照らして、保存期間を定める必要がある。

- **基本対策事項 6.2.3(1)-6「監視記録を保存」について**

サーバ装置、端末、通信回線装置及び通信回線を監視している場合、監視対象の状態は一定ではなく変動することが一般的である。時間変動、曜日変動、週変動、月変動、季節変動等を検討した上で記録を一定期間保存する。

6.2.4 標的型攻撃対策

目的・趣旨

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。

したがって、標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

遵守事項

(1) 標的型攻撃対策の実施

(a) 部局技術責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。

(b) 部局技術責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。

【 基本対策事項 】

＜6.2.4(1)(a)関連＞

6.2.4(1)-1 部局技術責任者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下を例とする対策を行うこと。

a) 不要なサービスについて機能を削除又は停止する。

b) 不審なプログラムが実行されないよう設定する。

c) パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

6.2.4(1)-2 部局技術責任者は、USB メモリ等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下を例とする対策を行うこと。

a) 出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接続する外部電磁的記録媒体を事前に特定しておく。

b) 外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。

c) サーバ装置及び端末について、自動再生（オートラン）機能を無効化する。

d) サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする。

e) サーバ装置及び端末について、使用を想定しない USB ポートを無効化する。

f) 組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。

＜6.2.4(1)(b)関連＞

6.2.4(1)-3 部局技術責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を例とする対策を行うこと。

a) 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。

b) 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずる。

6.2.4(1)-4 部局技術責任者は、端末の管理者権限アカウントについて、以下を例とする対策を行うこと。

a) 不要な管理者権限アカウントを削除する。

b) 管理者権限アカウントのパスワードは、容易に推測できないものに設定する。

6.2.4(1)-5 部局技術責任者は、重点的に守るべき業務・情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って、対策を講ずること。

（解説）

- **遵守事項 6.2.4(1)(a)「標的型攻撃」について**

以下の各項における規定内容は、標的型攻撃への対策としても有効であるため、それぞれに示される対策を行う必要がある。

- 6.1.1 項「主体認証機能」
- 6.1.2 項「アクセス制御機能」
- 6.1.3 項「権限の管理」
- 6.1.4 項「ログの取得・管理」
- 6.1.5 項「暗号・電子署名」
- 6.2.1 項「ソフトウェアに関する脆弱性対策」
- 6.2.2 項「不正プログラム対策」
- 7.1.1 項「端末」
- 7.1.2 項「サーバ装置」
- 7.2.1 項「電子メール」
- 7.3.1 項「通信回線」
- 8.1.1 項「情報システムの利用」

- **基本対策事項 6.2.4(1)-1「不審なプログラムが実行されないよう設定する」について**

具体的な設定手段としては、あらかじめ利用するアプリケーションを登録してそれ以外のアプリケーションの実行を拒否するよう設定する、通常のアプリケーションでは利用しないメモリ空間を利用しようとしたアプリケーションを不審と判定して実行

を拒否するソフトウェアを利用する、情報システムにおいては不正プログラムの起動又は動作を拒否する手法を導入するなどが挙げられる。

なお、これらを導入する場合には、業務で利用するアプリケーションに影響が及ぶ可能性があるため、事前に検証する必要がある。

- **基本対策事項 6.2.4(1)-2 c)「自動再生（オートラン）機能を無効化」について**

自動再生（オートラン）機能とは、OS がその機能を備えている場合において、サーバ装置や端末に USB メモリ等の外部電磁的記録媒体を接続した際に、その媒体に格納されている特定のプログラムを自動的に実行する機能を指す。

標的型攻撃に用いられる手段として、この機能を悪用するものがあり、例えば、不正プログラムを格納した USB メモリを端末に接続させることにより、不正プログラムを実行させるという手法が想定される。

自動再生（オートラン）機能を無効化しておくことにより、この機能を悪用する手段による被害に遭うリスクを低減することができる。

- **基本対策事項 6.2.4(1)-2 d)「外部電磁的記録媒体内にあるプログラムを一律に実行拒否」について**

OS によっては、あらかじめ設定することにより、USB メモリ等の外部電磁的記録媒体を端末に接続した場合において、その媒体にあるプログラムを、その媒体にある状態のまま実行することを一律に拒否することができる。プログラムを実行したい場合には、端末の内蔵電磁的記録媒体（PC 内蔵 HDD 等）にいったんコピーしてから実行する運用となる。この設定により、接続した途端に外部電磁的記録媒体上の不正プログラムが実行されるリスクを低減することができる。

- **基本対策事項 6.2.4(1)-2 e)「USB ポートを無効化」について**

物理的に又はシステム的に USB ポートを利用できない状態にすることで、USB メモリ等の外部電磁的記録媒体を接続することによって生じる情報セキュリティインシデントの発生を抑止できる。

- **基本対策事項 6.2.4(1)-2 f)「組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービス」について**

外部電磁的記録媒体のポートへの接続や利用を制御及び管理するため、以下のような機能を持つ製品やサービスが市場に提供されている。

  - 端末の USB ポートのインタフェースを無効化し、外部電磁的記録媒体を含む全ての機器を利用不可とする。
  - USB ポートに接続された機器のうち、全ての外部電磁的記録媒体を利用不可とする。
  - 利用を認める外部電磁的記録媒体を一元管理するサーバに事前に登録しておき、登録されていない外部電磁的記録媒体の利用不可とする。
  - 利用を認める外部電磁的記録媒体の個体識別情報（製品番号等）と利用者の組合せを一元管理するサーバに事前に登録しておき、組合せ以外での利用を不可とする。

- 外部電磁的記録媒体の接続の際における、利用者、出力日時、出力ファイル名等のログを自動的に取得する。

- **基本対策事項 6.2.4(1)-3「情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバ」について**

悪意ある第三者等は、入口対策を突破して内部への侵入に成功すると、外部から遠隔指令を出して内部侵入の範囲を拡大しつつ、目的の達成を目指すと想定される。その目的としては、重要情報の窃取や破壊が想定され、したがって、識別コード及びアクセス権限を集中管理する認証サーバ、又は、情報が集中的に保存されるファイルサーバは、攻撃対象となる蓋然性が高いと考えられる。これら重要サーバには、特に注意を払って情報セキュリティ対策を講ずる必要がある。

- **基本対策事項 6.2.4(1)-3 b)「管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策」について**

管理者権限を狙う攻撃としては、機械的にパスワードを変えながら連続してログイン試行する攻撃が考えられる。このような攻撃を受けることを想定した対策としては、以下に挙げるものが考えられる。

- 連続でのログイン失敗回数に上限値を設け、この上限値を超えた場合は、次回ログイン試行までに一定の期間（例：15 分）ログイン試行を受け付けないようにシステム等で設定する。
- ログイン失敗ログを取得し、その取得内容を継続的に監視することにより、大量のログイン失敗を検知する仕組みを導入する。

なお、辞書攻撃とは、パスワードに単語の組み合わせや人名を用いている場合に有効なパスワード解析方法をいう。英語の辞書に限らず各国語の単語を用いる場合もあるため、日本語の単語、日本人の人名も安全ではない。また、単語と数桁の数字のような単純な組み合わせも解析の対象となる。また、ブルートフォース攻撃とは、無意味な英数記号の組み合わせも含めた、総当たりでのパスワード解析方法をいう。辞書攻撃より効率は劣るが、原理的には必ず正しいパスワードに到達する。

6.3　アプリケーション・コンテンツの作成・提供

6.3.1　アプリケーション・コンテンツの作成時の対策

目的・趣旨

本学では、情報の提供、諸手続、意見募集等のサービスのためにアプリケーション・コンテンツを用意し、広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に、利用者端末の情報セキュリティ水準の低下を招いてしまうことは避けなければならない。本学は、アプリケーション・コンテンツの提供に際しても、情報セキュリティ対策を講じておく必要がある。

また、アプリケーション・コンテンツの開発・提供を外部委託する場合については、4.1.1項「外部委託」についても併せて遵守する必要がある。

遵守事項

(1) アプリケーション・コンテンツの作成に係る規定の整備

(a) 全学実施責任者は、アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.3.1(1)(a)「アプリケーション・コンテンツ」について**

  行政サービスは、アプリケーションプログラムやウェブコンテンツ等を用いて国民等に提供されている。特にウェブコンテンツでは、本学以外が提供するコンテンツ（以下「外部コンテンツ」という。）を組み込むことによって、容易に様々な機能を提供することが可能となるが、本学において外部コンテンツの信頼性を担保することは不可能であることから、このような利用方法には注意を要する。例えば、外部コンテンツが事前に通知されることなく変更されてしまい、行政サービスの利用者の意図に反して利用者の個人に関する情報が取得される可能性がある。また、外部コンテンツに不正プログラムが組み込まれ、行政サービスの利用者がそれに感染する被害が生じることも考えられる。そのため、ウェブコンテンツでは外部コンテンツを利用しないことが望ましいが、必要があって利用する場合には、これらの脅威に対して適切なセキュリティ対策を実施することが求められる。

- **遵守事項 6.3.1(1)(a)「学外の情報セキュリティ水準の低下を招く行為を防止する」について**

  国民等が本学によって提供される行政サービスを利用する場合、行政サービスの利用によって、利用者の端末が不正プログラムに感染しやすい状況を強制したり、利用者個人の情報が利用者の意図に反して第三者に提供させられるといった状況を作り出したりすることは避けなければならない。本学は、国民等の学外の情報セキュリティ

水準を低下させないように留意して、行政サービスのためのアプリケーション・コンテンツを提供する必要がある。

- **遵守事項 6.3.1(1)(a)「規定を整備」について**

  全学実施責任者は、アプリケーション・コンテンツの提供に関する規定の整備に当たり、遵守事項 6.3.1(2)において規定した事項を含める必要がある。

遵守事項

(2) アプリケーション・コンテンツのセキュリティ要件の策定

(a) 部局技術責任者は、学外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含めること。

(ア) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

(イ) 提供するアプリケーションが脆弱性を含まないこと。

(ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

(エ) 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

(オ) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

(カ) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

(b) 事務従事者は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前号に掲げる内容を調達仕様に含めること。

【 基本対策事項 】

＜6.3.1(2)(a)(ア)関連＞

6.3.1(2)-1 部局技術責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を含む対策を行うこと。

a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

b) 外部委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。

＜6.3.1(2)(a)(ア)(カ)関連＞

6.3.1(2)-2 部局技術責任者は、提供するアプリケーション・コンテンツにおいて、学外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、当該高等教育機関外へのアクセスが情報セキュリティ上安全なものであることを確認すること。

6.3.1(2)-3 部局技術責任者は、提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない学外へのアクセスを自動的に発生させる機能を含めないこと。
＜6.3.1(2)(a)(エ)関連＞
6.3.1(2)-4 部局技術責任者は、文書ファイル等のコンテンツの提供において、当該コンテンツが改ざん等なく真正なものであることを確認できる手段がない場合は、「https://」で始まる URL のウェブページから当該コンテンツをダウンロードできるように提供すること。
6.3.1(2)-5 部局技術責任者は、改ざん等がなく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

（解説）

- **遵守事項 6.3.1(2)(a)(ア)「不正プログラムを含まない」について**

  不正プログラムとは、一般的なコンピュータウイルスの他、ワームやスパイウェア等が該当する。不正プログラムを含まないようにすべきものは、学外の利用者の端末にインストールさせるプログラムの他、利用者に閲覧させるウェブサイトのウェブページも含む。

- **遵守事項 6.3.1(2)(a)(イ)「脆弱性を含まない」について**

  脆弱性は、アプリケーションプログラムが動作する OS や利用する開発言語によって様々な種類のものが存在する。例えば、C 言語によって開発されたアプリケーションプログラムにバッファオーバーフローの脆弱性が存在した場合は、利用者の端末上で任意のプログラムを実行される可能性がある。したがって、OS や開発言語の特性に応じて適切な脆弱性対策を実施する必要がある。

- **遵守事項 6.3.1(2)(a)(ウ)「実行プログラムの形式でコンテンツを提供しない」について**

  実行プログラムの形式とは、利用者がダブルクリックするなどしてファイルを開いたときに自動的にプログラムコード（当該ファイルの作成者が意図した任意のコード）が実行される形式のファイルのことであり、拡張子が「.exe」の形式のものがこれに該当するほか、「.pif」、「.scr」、「.bat」等のものも該当する。本遵守事項に違反する例としては、会議資料等のプログラムではない文書を提供する際に、自己展開式圧縮ファイル作成ソフトウェアを用いて拡張子が「.exe」の圧縮ファイルを作成してこれを配布する行為が典型例として挙げられる。この場合は、拡張子「.zip」等の形式の圧縮ファイルを作成して配布すればよい。

  なお、電子メールの添付により文書等を配布する場合については、「（解説）基本対策事項 8.1.1(2)-2 d)「実行プログラム形式のファイルを削除等する」について」を参照のこと。

  実行プログラムの形式は、不正プログラムがその感染手段として利用することが多く、特に電子メールに添付された実行形式のファイルは、不正プログラム感染防止のため、基本的に開かないようにしなければならない。これは、拡張子「.zip」等の圧縮

ファイル中に含まれる実行プログラムの形式のファイルについても同様である（基本対策事項 8.1.1(7)-3 d）にも規定しているため、参照のこと。）。それにもかかわらず、本学が日ごろから実行プログラムの形式でのコンテンツ提供を行う場合、本学の事務従事者だけでなく、一般の行政サービスの利用者に対しても、実行プログラムの形式のファイルを開くことに慣れさせてしまうことになり、利用者の情報セキュリティ水準を低下させてしまうことになる。そのため、本遵守事項は、そもそも実行プログラムの形式や実行プログラムの形式を含む圧縮ファイルの形式でのコンテンツ提供をしないよう求めている。

なお、本学が行政サービスのためにアプリケーションプログラムを提供する必要がある場合等、「実行プログラムの形式以外にコンテンツを提供する手段がない」場合は、実行プログラムの形式で提供してもよいが、遵守事項 6.3.1(2)(a)(エ)又は基本対策事項 6.3.1(2)-4 に従った措置を行う必要がある。

- **遵守事項 6.3.1(2)(a)(エ)「改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与える」について**

改ざん等がなく真正なものであることを確認できる手段には、利用者に提供するものがアプリケーションプログラムである場合は、「コードサイニング証明書」等と呼ばれる電子証明書を用いてアプリケーションプログラムに署名を施すことがこれに該当する。利用者はアプリケーションプログラムに施された署名を確認することで、改ざんがないことを確認でき、さらに、そのアプリケーションプログラムの提供者が本学であることを確認できる。提供するコンテンツがウェブサイト上にある場合には、TLS(SSL）を用いた「https://」で始まる URL のウェブページとすることにより、利用者は当該ウェブページが改ざんなく受信できていることを確認できる。TLS（SSL）を用いる際に、本学のサーバ証明書を用いれば、当該サイトが本学のものであることを確認できる。コンテンツを電子メールで提供する場合には、S/MIME 等の電子署名の技術を用いることで、電子メールが配送途中で改ざんされていないこと及び発信者が本学であることを確認できる。

本学によりその手段を提供する準備が整っている場合は、アプリケーション・コンテンツの提供先に必ず与える必要がある。技術的にそのような手段が存在するものの本学がまだその手段を提供する準備を整えていない場合については、可能な限りその準備を整えることが望ましい。技術的にそのような手段が存在しない場合としては、文書ファイルを提供するときに、文書ファイルの形式によっては署名を施す手段がない場合があり、この場合にはその手段を与えなくてもよい。

- **遵守事項 6.3.1(2)(a)(オ)「脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制する」について**

行政サービスを提供する情報システムの提供において、当該情報システムを利用するために、学外の事業者等が作成した汎用のソフトウェアやミドルウェアのインストールが利用者の端末で必要となる場合がある。この場合、利用者は本学から指示されたソフトウェアを自身の端末にインストールせざるを得ないが、指定されるソフトウェア（又はソフトウェアバージョン）のサポート期間が過ぎているなどの理由により

脆弱性が存在するものであると、利用者の情報セキュリティ水準を本学が低下させることになる。したがって、脆弱性が存在するバージョンの OS の利用やソフトウェアのインストールを本学が暗黙又は明示的に要求することにならないよう、アプリケーション・コンテンツの提供方式を定めて開発しなければならない。

具体的には、当該行政サービスを提供するシステムが準備された時点では脆弱性が発見されていなくても、運用開始後に発見されることがある。そのとき、利用者が迅速に当該脆弱性を回避できるようになっている必要がある。例えば、当該行政サービスを利用するために、第三者が提供している汎用のソフトウェアのインストールを必要としていたとする。このとき、当該ソフトウェアに脆弱性が発見され、それを修正した新バージョンのソフトウェアが公開された場合に、当該新バージョンのソフトウェアをインストールすることで当該行政サービスに不具合等が生じて利用が不可能になるような事態が発生すると、利用者は、当該ソフトウェアを新バージョンに更新することができなくなる。結果として、本学の行政サービスが利用者の脆弱性回避を妨げることになってしまう。こうしたことが起きないよう、行政サービスを提供するシステムは、第三者の汎用ソフトウェアの併用を前提とする場合は、当該汎用ソフトウェアが新バージョンに置き換わっても、正常に動作するように設計する必要がある。予期せず不具合が発生する事態が発生した場合にも、行政サービスを提供するシステムを修正することができるよう、迅速に新バージョンのソフトウェアに対応することを保守契約に盛り込んでおくことが望ましい。

また、特定の種類のウェブブラウザに脆弱性が発見され、利用する危険性が高くなった場合においても、他の種類のウェブブラウザも利用可能とすることで、提供するサービスを継続可能にする必要がある。そのためには、例えば、2 種類以上のウェブブラウザ又は同一製品の異なるバージョンが動作するように、情報システムの構築時に配慮し、その動作確認をおこなうことが考えられる。

なお、開発時に公開されているバージョンだけでなく、例えば、利用を想定しているブラウザの次期バージョンについて、ソフトウェアの配布前に情報が公開された状態又は試用版ソフトウェアが配布され動作検証可能な状態にあれば、前もって利用可能かどうかを検証するなど、その後に公開が想定されるバージョンにも対応できるよう、構築時に配慮することが望ましい。

- **遵守事項 6.3.1(2)(a)(オ)「情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求する」について**

行政サービスを提供する情報システムを利用するために、利用者の端末にインストールされているソフトウェア（本学が直接提供していないソフトウェア（例えば、端末の OS やウェブブラウザ等））の設定変更を必要とするとき、その設定変更が情報セキュリティ水準の低下を招くものである場合、そのような設定変更を要求してはならない。必要があって利用者に設定変更を求めるときは、その OS やブラウザの標準設定（初期設定）に変更することのみを求めるものとすることである。

- **遵守事項 6.3.1(2)(a)(カ)「サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能」について**

これに該当する典型的な例は、本学のウェブサイトを構成する各 HTML ファイルの中に、学外のサイト（例として広告事業者の広告提供サーバ）のコンテンツを見えない形又は見える形で組み込むことで、本学のウェブサイトの閲覧者のアクセス履歴を当該広告サーバへ自動的に送信する、いわゆる「トラッキング処理」を行う機能である。このとき、当該広告提供サーバが HTTP の cookie 機能を用いて閲覧する利用者に識別番号を付番している場合は、アクセス履歴等の、サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が、本人の意思に反して当該広告提供サーバを運営する第三者に提供されることになるので、本遵守事項はこのような機能がアプリケーション・コンテンツに組み込まれることがないようにすることを求めている。

また、トラッキング処理ではなくとも、例えば、利用者のキー入力の全てを当該利用者が意図しない形で送信するなどの機能も、「サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能」に該当し得る。

なお、対象はウェブサイトの HTML ファイルに限られず、アプリケーションプログラムを提供する場合に、そのプログラムに含まれ得る機能についても同様である。

- **遵守事項 6.3.1(2)(b)「調達仕様に含める」について**

例えば、本学が何らかのキャンペーンとして啓発コンテンツを提供する際に、その作成を広告会社等に外部委託する場合は、情報システム部門以外の事務従事者がその外部委託の調達仕様を定めることになると考えられる。このような場合でも、学外の情報セキュリティ水準を低下させないよう、遵守事項 6.3.1(2)(a)のセキュリティ要件を調達仕様に含めることが求められる。

- **基本対策事項 6.3.1(2)-2「必要があって当該機能を含める場合」について**

学外へのアクセスを自動的に発生させる機能を含める必要がある場合の例としては、ソーシャルメディアサービスとの連携機能を提供するためのボタン（ボタン画像の他、ボタン押下時の機能等を提供するプログラムを含む。）等を本学のウェブページ上に設置する場合が挙げられる。万が一、学外のウェブサイトが提供するプログラムに不正なコードが含まれていると、当該プログラムを使用した本学のウェブサイトが利用者に危険をもたらすことになるため、その安全性が確認できているボタン等のみを使用することが求められる。これはウェブページ等のコンテンツに限られず、本学が提供するアプリケーションプログラム内においても同様である。

- **基本対策事項 6.3.1(2)-3「学外へのアクセスを自動的に発生させる機能」について**

学外へのアクセスを自動的に発生させる機能とは、例えば、本学が提供するウェブページの HTML ファイルに、<script src=”http://学外のサイト/foo.js”>等の記述があり、学外のウェブサイトからプログラムを読み込んで実行する機能が該当する。もし、学外のウェブサイトが提供するプログラムに不正なコードが含まれる場合、当該プログ

ラムを使用した本学のウェブサイトが利用者に危険をもたらすことになるため、そのような機能をウェブページに含めることは可能な限り避けるべきである。具体的には、当該ファイルを本学ウェブサイトのサーバ上に置いて提供することで解決できる。これはウェブページ等のコンテンツに限られず、本学が提供するアプリケーションプログラム内においても同様である。

- **基本対策事項 6.3.1(2)-4「「https://」で始まる URL のウェブページから当該コンテンツをダウンロードできるように提供」について**

  情報システムの利用者が、現在閲覧しているウェブページが「https://」で始まる URL のウェブページであることを目視確認の上で、そこからリンクをクリックするなどしてファイルをダウンロードする手順を踏むことにより、当該ファイルは、暗号化された通信によって改ざんなくダウンロードされることになる。本基本対策事項は、このような機能を利用者に提供することを求めたものである。

  具体的には、本学が提供するウェブサイトのサーバで SSL（TLS）通信を利用可能とし、「https://」で始まる URL での閲覧を可能とすればよい。

  なお、そのときにダウンロードさせるファイル自身も SSL（TLS）通信を通じてダウンロードされるよう、当該ファイルへのリンクも「https://」で始まる URL としておく必要がある。

6.3.2 アプリケーション・コンテンツ提供時の対策

目的・趣旨

本学では、情報の提供、諸手続及び意見募集等のサービスのためにウェブサイト等を用意し、国民等の利用に供している。これらのサービスは通常インターネットを介して利用するものであるため、国民等にとっては、そのサービスが実際の本学のものであると確認できることが重要である。また、本学になりすましたウェブサイトを放置しておくと、本学の信用を損なうだけでなく、国民等が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講ずる必要がある。

遵守事項

(1) A 大学ドメイン名の使用

(a) 部局技術責任者は、学外向けに提供するウェブサイト等が実際の本学提供のものであることを利用者が確認できるように、A 大学ドメイン名を情報システムにおいて使用するよう仕様に含めること。ただし、4.1.3 項に掲げる場合を除く。

(b) 事務従事者は、学外向けに提供するウェブサイト等の作成を外部委託する場合においては、前号と同様、A 大学ドメイン名を使用するよう調達仕様に含めること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 6.3.2(1)(a)「A 大学ドメイン名を情報システムにおいて使用する」について**

学外向けに提供するウェブサイト等が実際に本学が提供しているものであることを利用者が確認できるように、日頃から A 大学ドメイン名を用いることを徹底しておくことにより、なりすましが発生しても、学外の者がウェブサイト等の真偽を見分けることが容易なものとすることができる。

現在、外部で独自ドメイン名を低廉な費用で取得することが可能であるが、いったん実用に処したドメイン名は、実質的に半永久的にその利用者が利用権を維持する必要がある。いったんドメイン名の利用権を放棄すると、そのドメイン名は他の事業者による用途（風俗的、反社会的な用途もあり得る）に転用（ドロップキャッチ）され、当初の用途を参照する目的でアクセスしてきた第三者の利用者に対して誤解等を生じさせる恐れがある。よって、目的に関わらず安易に外部のドメイン名を取得・利用することのないよう、教職員等への啓発を行うことも重要である。

A 大学ドメイン名を用いるべき場合の例を以下に示す。

- 本学の出先機関等が組織の紹介サイトを提供する場合

  A 大学ドメイン名は、本学が提供していることを示すものとして、閲覧者に理解される。サーバを外国に設置している場合であっても、当該サーバのホスト名として A 大学ドメイン名を設定することは可能である。

- .本学が主催する講演会等に係るウェブサイトの提供において、参加者の登録を

オンラインで行うために、ウェブサイト上で閲覧者に個人情報を入力させる場合
　閲覧する者にとって、当該ウェブサイトが本学によって運営されているものであることの確認は、個人情報の入力を要する場合には特に重要となる。

- .本学の広報活動として期間限定でキャンペーンサイトを広告会社に制作させ提供する場合
  一時的に提供するウェブサイトを構築する場合や、広告会社に制作からサーバ管理までを委託する場合であっても、本学の公式な告知であると閲覧者が認識すべき内容である限りは、A 大学ドメイン名を用いるべきである。サーバが広告会社管理のもので、サーバに割り当てられた IP アドレスが学外のものであっても、そのホスト名として A 大学ドメイン名を用いることはできる。

- **遵守事項 6.3.2(1)(b)「調達仕様に含める」について**

　学外向けのウェブサイトを構築する場合に、情報システム部門以外の事務従事者がウェブサイトの構築業務を外部委託することが考えられる。このような場合でも、学外の情報セキュリティ水準の低下を招かないよう､A 大学ドメイン名の使用を調達仕様に含めることが求められる。

遵守事項

(2) 不正なウェブサイトへの誘導防止

(a) 部局技術責任者は、利用者が検索サイト等を経由して本学のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。

【 基本対策事項 】

＜6.3.2(2)(a)関連＞

6.3.2(2)-1 部局技術責任者は、学外向けに提供するウェブサイトに対して、以下を例とする検索エンジン最適化措置（SEO 対策）を講ずること。

a) クローラからのアクセスを排除しない。

b) cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする。

c) 適切なタイトルを設定する。

d) 不適切な誘導を行わない。

6.3.2(2)-2 部局技術責任者は、学外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、不審なサイトへのアクセスを防止するための対策を講ずること。

（解説）

- **遵守事項 6.3.2(2)(a)「本学のウェブサイトになりすました不正なウェブサイト」について**

  学外の者が、本学の名前をタイトルに掲げるなどして、本学のウェブサイトと誤認されかねないウェブサイトを作成することがあり、これを完全に防ぐことはできない。本来ならば､利用者は当該サイトの URL 中のドメイン名が A 大学ドメイン名であるかを確認することで、本学のウェブサイトかを確認できるところであるが、検索サイト等を利用して本学名で検索して訪れる利用者も多いことから、検索サイトで検索したときに、正規の本学サイトが検索結果の上位に現れるようになっていることが望ましい。通常は、特別な対策をすることなく、そのような結果になることがほとんどであるが、正規の本学サイトの側で、不適切な設定になっていたり、コンテンツが適切に構成されていない場合に、検索サイトで、正規の本学サイトが最上位に現れなかったり、適切な表示がなされないことがある。本遵守事項はそのような事態を防止するための措置を講ずることを求めている。

- **基本対策事項 6.3.2(2)-1「検索エンジン最適化措置（SEO 対策）」について**

  正規のウェブサイトが検索サイトで上位に現れるように正規のウェブサイト側で工夫を施すことを、一般に「検索エンジン最適化」又は「SEO 対策」と呼ぶ。本基本対策事項は、本学サイトにおいても一般的な検索エンジン最適化の措置を講ずることを求めている。

- **基本対策事項 6.3.2(2)-1 a)「クローラからのアクセスを排除しない」について**

  一般に、検索サイトは、ウェブクローラと呼ばれる自動的にウェブサイトのリンクをたどって全てのページを巡回するプログラムを、自ら稼働させることによって収集した HTML データを用いて検索機能を実現している。そのため、検索サイトのクローラからのアクセスを拒否する設定をしている場合、当該サイトは検索サイトの検索結果に現れなくなることがある。そのような設定は、ウェブサイトの「/robots.txt」のファイルの記述で簡単にできるものであるため、誤ってクローラからのアクセスを拒否する設定にしてしまう状況が想定される。通常、このファイルを設定する必要はないため、何ら記述しないでおくことが望ましい。

- **基本対策事項 6.3.2(2)-1 b)「cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする」について**

  一般に、検索サイトが自ら稼働させるウェブクローラは、HTTP の cookie 機能に対応していない。そのため、cookie 機能を無効に設定したブラウザで閲覧したときに、正常に表示されないウェブページは、検索サイトの検索結果に正常に表示されない事態が起きる。通常のウェブサイトの構成では、cookie 機能を無効にしても正常に表示されるものであるが、一部の CMS（Content Management System）には、cookie を無効にして閲覧すると「cookie を有効にしてください」とだけ記述したエラー画面を表示するものがあり、そのような CMS を用いてウェブサイトを構成すると、前述の事態が生じる。実際に、過去に一部の本学サイトでそのような事態が発生したことがあるため、ウェブサイトの構築を外部委託する場合を含め、注意する必要がある。

- **基本対策事項 6.3.2(2)-1 c)「適切なタイトルを設定する」について**

  一般に、検索サイトの検索結果には、当該ページのタイトル（HTML 中の TITLE 要素で設定される文字列）が見出しとして表示され、利用者はこれを頼りにサイトを訪れることから、本学サイトにおいても、ページのタイトルに本学名を含めるなど、適切なタイトルを設定することが重要である。

  その他の対策として、HTML 中の H1 要素や H2 要素を適切に記述することで、そこに含まれる単語や文で検索したときに、検索サイトの上位に当該ページが現れやすくなる。本学サイトにおいても、H1 要素や H2 要素を適切に記述することで、検索結果の上位に現れやすくすることができる。また、HTML 中のメタタグ（「description」や「keywords」等）に概要やキーワード等を記述することで、そこに含まれる単語や文で検索したときに、検索サイトの上位に当該ページが現れやすくなる。本学サイトにおいても、メタタグを適切に記述することで、検索結果の上位に現れやすくすることができる。

- **基本対策事項 6.3.2(2)-1 d)「不適切な誘導を行わない」について**

  一般に、HTML 中に見えない文字等でページ内容に関係のないキーワードを過剰に記述するなどして、当該ページへのアクセスを無用に誘う行為（「SEO スパム」等と呼ばれる。）は、不適切な行為として検索サイトからペナルティを科され、検索結果の上位に表示されなくなることがある。本学のウェブサイトにおいて、故意にそのような

行為が行われることは考えにくいが、コンテンツの作成を外部委託した場合に、委託先が独自判断で行うことも想定されるため、そのようなコンテンツを作成しないよう注意が必要である。

- **基本対策事項 6.3.2(2)-2「不審なサイトへのアクセスを防止するための対策」について**

  不審なサイトを確認した場合は、本学のウェブサイト等において注意喚起を行うなどの対応を図るとともに、必要に応じて自組織や文部科学省、内閣サイバーセキュリティセンター等の関係部門に状況を報告する。特に悪質な場合は、誤って当該サイトにアクセスすることを防止するため、検索サイト業者に対して検索結果に表示されないよう依頼する、本学 LAN からアクセスできないよう当該サイトに対してフィルタを設定する、といった対策が考えられる。

遵守事項

(3) 学外のアプリケーション・コンテンツの告知

(a) アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。

(b) 事務従事者は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つこと。

(ア)

【 基本対策事項 】

＜6.3.2(3)(a)関連＞

6.3.2(3)-1 事務従事者は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示すること。また、短縮 URL を用いないこと。

6.3.2(3)-2 事務従事者は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示すること。

6.3.2(3)-3 事務従事者は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つために以下の措置を講ずること。

a) 告知するアプリケーション・コンテンツを管理する組織名を明記する。

b) 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する。

（解説）

- **遵守事項 6.3.2(3)(b)「学外の者が提供するアプリケーション・コンテンツを告知する」について**

- **学外の者が提供するアプリケーション・コンテンツを告知する場合、告知を開始した時点では、当該アプリケーション・コンテンツが、告知した URL 等の誘導先に確かに存在していても、将来にわたりその誘導先に意図したアプリケーション・コンテンツが存在し続けるとは限らない。誘導先のドメイン名等が放棄された場合には、悪意ある者に当該ドメイン名が取得され、偽のアプリケーション・コンテンツに差し替えられる攻撃が想定される。したがって、学外の者が提供するアプリケーション・コンテンツを本学が告知する場合には、誘導先の有効性を保つことが求められる。遵守事項 6.3.2(3)-1「URL 等を用いて直接誘導」について**

URL を用いた直接誘導に該当する例としては、ウェブサイトにハイパーリンクを設ける場合のほか、電子メールに URL を記載して告知する場合、印刷物に URL を表示

して誘導する場合等が挙げられる。URL「等」としているのは、例えば、ホスト名（FQDN形式での表記）もこれに該当するものとする趣旨である。

- **遵守事項 6.3.2(3)-1「検索サイトで指定の検索語を用いて検索することを促す方法」について**

  印刷物やテレビ CM により告知する際に、URL 等の文字列が長すぎると、利用者にその全部を入力させることが困難であることから、検索サイトで検索するよう検索語を指定して促す方法が広く普及している。

  しかし、この誘導方法では、偽サイトや別のサイトに誘導されてしまうリスクを否定できない。検索結果の上位に目的の誘導先が現れない可能性があるだけでなく、検索サイトの広告部分に悪意あるサイトを出現させる攻撃手法も想定され、利用者が検索サイトの広告部分を誘導先として解釈してしまうおそれがある。

  また、アプリケーション・コンテンツの告知を広告代理店に委託している場合、広告代理店が検索サイトの広告枠を購入し、広告部分を用いて目的の誘導先に誘導する方法が用いられることがある。この誘導方法が広告代理店によって頻繁に用いられると、広告部分を正規の誘導先として利用者が解釈するようになると考えられ、広告部分に攻撃者による偽サイトが現れることのリスクを無視することはできなくなる。したがって、政府機関がアプリケーション・コンテンツを告知する場合には、検索サイトの広告枠を購入して誘導する方法は用いないようにすることが望ましい。

- **遵守事項 6.3.2(3)-1「間接的な誘導方法を用いる場合」について**

  間接的な誘導方法を用いて本学の提供するアプリケーション・コンテンツを告知する場合は、当該誘導方法による誘導の状況を適時確認するなどして、不正な又は不適切なウェブサイトところへ誘導されてしまう可能性が高い状況になっているか否かを確かめることが望ましい。

- **遵守事項 6.3.2(3)-1「URL 等と一体的に表示する」について**

  アプリケーション・コンテンツの告知は URL 等を用いて直接誘導することを原則とするが、間接的な誘導方法を用いたい場合があることも想定されることから、その場合に実施すべき措置として、間接的な誘導方法と一体的に URL 等を表示することを求めている。

- **遵守事項 6.3.2(3)-1「短縮 URL を用いない」について**

  短縮 URL を提供する民間事業者のサービスは、将来にわたり永続的に運営が保証されるものではなく、いずれサービスが消滅し、ドメイン名が放棄されれば、悪意ある者に当該ドメイン名が取得され、偽のアプリケーション・コンテンツに差し替えられる攻撃が想定される。したがって、やむを得ない場合を除き、短縮 URL を用いるべきでない。やむを得ない場合の例としては、ソーシャルメディアサービスにおいて URL を告知する場合に、当該ソーシャルメディアサービスが強制的に所定の短縮 URL を用いてしまう場合が挙げられる。

- **遵守事項 6.3.2(3)-2「アプリケーション・コンテンツの内容に係る記述を当該バーコー**

ドと一体的に表示」について

印刷物等でアプリケーション・コンテンツを告知する際に、URL 等の表示に代わるもの又は URL 等と一体的に表示するものとして、二次元コード等を用いて誘導する方法がある。この方法は、特にスマートフォンや携帯電話の利用者にとって利便性が高く、政府機関や教育機関においても用いられるようになってきている。

しかしながら、二次元コード等のみを単体で表示した場合、それがどこへ誘導するものであるかが、利用者にとって必ずしも明確でない場合がある。そこで、本項では、当該二次元コード等がどこへ誘導するものであるかを、当該二次元コード等と一体的に表示することにより利用者に明示することを求めている。

「アプリケーション・コンテンツの内容に係る記述」の例としては、誘導先の URL 等や、誘導先のアプリケーション・コンテンツの内容を示す記述が考えられる。

- **遵守事項 6.3.2(3)-3「告知する URL 等の有効性を保つために以下の措置を講ずる」について**

この措置を講ずるための対策事項 a)及び b)について、具体的な記載例を以下に示す。

- このウェブサイトは○○協会が運営しており、A 大学が運営しているものではありません。
- このウェブサイトのアドレスについては、○○年○○月時点のものです。ウェブサイトのアドレスについては廃止や変更されることがあります。最新のアドレスについては、ご自身でご確認ください。

第7部 情報システムの構成要素

7.1 端末・サーバ装置等

7.1.1 端末

目的・趣旨

端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等のおそれがある。また、事務従事者の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。モバイル端末の利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、7.3.2 項「IPv6 通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

遵守事項

(1) 端末の導入時の対策

(a) 部局技術責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 部局技術責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。

(c) 部局技術責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

【 基本対策事項 】

＜7.1.1(1)(a)関連＞

7.1.1(1)-1 部局技術責任者は、モバイル端末を除く端末について、原則としてクラス２以上の要管理対策区域に設置すること。

7.1.1(1)-2 部局技術責任者は、端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

a) モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。

b) モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット

等）を用意する。

7.1.1(1)-3 部局技術責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。

a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。

b) 要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。

＜7.1.1(1)(b)関連＞

7.1.1(1)-4 部局技術責任者は、第三者により情報窃取されることを防止するために、以下を例とする、端末に保存される情報を暗号化するための機能又は利用者が端末に情報を保存できないようにするための機能を設けること。

a) 端末に、ハードディスク等の電磁的記録媒体全体を暗号化する機能を設ける。

b) 端末に、ファイルを暗号化する機能を設ける。

c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。

d) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。

e) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。

f) ハードディスク等電磁的記録媒体に保存されている情報を遠隔から消去する機能（遠隔データ消去機能）を設ける。

＜7.1.1(1)(c)関連＞

7.1.1(1)-5 部局技術責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。

a) ソフトウェアベンダのサポート状況

b) ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容

c) インストール時に同時にインストールされる他のソフトウェア

d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

（解説）

- **遵守事項 7.1.1(1)(c)「利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める」について**

利用を認めるソフトウェア及び利用を禁止するソフトウェアそれぞれのリストに登録する単位について、ソフトウェアの個別の製品名やバージョン単位で列挙すると分かりやすいが、利用を禁止する全てのソフトウェアについて製品名等を個別に列挙するのが難しい場合は、例えば、個別に把握できるソフトウェアの製品名に加えてカテゴリ単位で登録することも考えられる。カテゴリ単位で登録する例としては、いわゆるピアツーピアで通信を行うソフトウェア、ファイル交換ソフトウェア、端末内の情報又は端末に入力した情報が自動で学外のサーバ装置等に送信されるソフトウェア、というような単位で定めておき、利用者に周知しておくと不要な手続が減らせるほか、

利用者の意識向上にも寄与すると考えられる。また、情報セキュリティリスクを低減する観点からは、利用を認めるソフトウェアを極力限定することが望ましい。

利用者が端末にソフトウェアをインストールすることができるような環境においては、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて、利用者に周知徹底を図ることが重要である。

- **基本対策事項 7.1.1(1)-1「原則としてクラス２以上の要管理対策区域に設置する」について**

要保護情報を取り扱う端末はクラス２以上の区域に設置することが望ましい。クラス２より低位の区域に設置する必要がある場合は、利用者が常時目視できる場所への設置を義務付けるなど、クラス２の区域に設置する場合と同程度の安全性を確保するための代替の対策を講ずること。

- **基本対策事項 7.1.1(1)-3「第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずる」について**

第三者による不正操作等の防止のための対策事項であるが、その他、端末の操作のロックの解除に IC カード等の主体認証情報格納装置を使用し、主体認証情報格納装置が無い状態で又は操作の無い状態が一定時間続くことで端末の操作がロックされるようにし、かつ、当該主体認証情報格納装置を執務室への立入りの確認にも利用するという方法が考えられる（これにより、利用者が執務室外にいる際には端末の操作が確実にロックできる）。

また、正規の利用者による不正操作や誤操作の防止策として、端末が備える機能のうち、利用しない機能を停止することが考えられる。停止する機能の例としては、無線 LAN 等の通信用のインタフェース、USB ポート等の外部電磁的記録媒体を接続するためのインタフェース、マイク、ウェブカメラ等が考えられる。

- **基本対策事項 7.1.1(1)-4「暗号化」について**

モバイル端末が第三者の者の手に渡った場合には、モバイル端末から取り外された内蔵電磁的記録媒体や、モバイル端末で利用していた外部電磁的記録媒体に保存されている情報を他の端末を利用して解読するなどの手段によって要機密情報が窃取される危険性がある。このような情報の窃取への対策として、端末に暗号化機能を搭載することが有効である。

暗号化する方法としては、ハードディスク全体又はファイル単体を暗号化するソフトウェアの導入や OS が備えている暗号化機能を使用することが挙げられる。その他、基本対策事項 7.1.1-4 c)の「ファイル暗号化等のセキュリティ機能を持つアプリケーション」を用いる方法もある。

ハードディスク全体を暗号化している場合でも、端末の起動中等の復号可能な状態で盗難等に遭った場合には情報窃取されるおそれがあるため、基本対策事項 7.1.1-4 f)の「遠隔データ消去機能」と組み合わせて用いると情報窃取される可能性をより低減できる。

また、暗号化を行う場合は鍵の管理が重要になる。鍵の管理の方法として、端末内

の耐タンパ性を備えた TPM (Trusted Platform Module) を利用する方法や、鍵を USB セキュリティトークンに格納して、利用時以外は端末とは別に管理するという方法等が考えられる。

- **基本対策事項 7.1.1(1)-4 c)「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について**

  「(解説) 基本対策事項 8.2.1(1)-3 c)「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について」を参照のこと。

- **基本対策事項 7.1.1(1)-4 d)「シンクライアント等」について**

  「(解説) 基本対策事項 8.2.1(1)-3 a)「シンクライアント等」について」を参照のこと。

- **基本対策事項 7.1.1(1)-4 e)「セキュアブラウザ等」について**

  「(解説) 基本対策事項 8.2.1(1)-3 b)「セキュアブラウザ等」について」を参照のこと。

- **基本対策事項 7.1.1(1)-4 f)「遠隔データ消去機能」について**

  端末の通信機能を利用して、遠隔から端末内のデータを消去する機能であるが、通信が確立できないために遠隔からデータ消去できない場合に備え、主体認証の失敗した回数をカウントして一定数を超えた際に消去するなど特定の条件で自律的に消去する機能についても考慮するとよい。また、データ消去ではなく、端末の操作をロックするという対策も考えられる。

- **基本対策事項 7.1.1(1)-5「利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める」について**

  利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める際には、以下を行うことが考えられる。

  - ソフトウェアベンダによるセキュリティパッチ等のサポートが提供されていることや、セキュリティベンダ等の第三者が提供するソフトウェアの脆弱性等に関する情報を確認する。
  - 外部と通信を行う機能を有することが明確なもの又は外部との通信の有無について利用規約により確認できるものについては、当該機能による通信内容を事前に確認する。
  - インストール時に、他のソフトウェアのインストールの同意を求めるものについては、当該ソフトウェアの利用の可否についても併せて定める。
  - ブラウザ等のソフトウェアで利用される機能拡張用のソフトウェア（いわゆる、プラグインやアドオン）の利用の可否についても併せて定める。

  また、一度利用を認めたソフトウェアであっても、バージョンが上がった際に、旧バージョンと比べ、機能が変わったり、同時にインストールされる他のソフトウェアが追加されたりする場合があるので、利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める際には、バージョンも含めて定めることが重要である。

なお、ソフトウェアによっては、バージョンによらず一律で利用を禁止するソフトウェアに指定できる場合もある。

遵守事項

(2) 端末の運用時の対策

(a) 部局技術責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

(b) 部局技術責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.1.1(2)(a)「見直しを行う」について**

ソフトウェアのバージョン更新、サポート期限切れ、新しいソフトウェアの出現等に適切に対応するため、また、利用者の要求に柔軟に対応するため、利用を認めるソフトウェア及び利用を禁止するソフトウェアの見直しを行うことが必要である。

「定期的」以外の見直しの契機として、端末の利用者から利用を認めるソフトウェア以外のソフトウェアの利用承認の申請（8.1.1 項「情報システムの利用」を参照のこと。）を受け付けたときが考えられる。申請のあったソフトウェアについて、引き続き利用を認める場合には、利用を認めるソフトウェアのリストに追加し、引き続き利用を禁止する場合には、利用を禁止するソフトウェアのリストに追加することで、一つのソフトウェアにつき１回の手続で済ませることができる。

- **遵守事項 7.1.1(2)(b)「不適切な状態にある端末を検出等した場合には、改善を図る」について**

「不適切な状態」とは、利用を認めるソフトウェア以外のソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていないなどの状態のことをいう。

利用を認めるソフトウェア以外のソフトウェアが稼働している場合には、当該ソフトウェアを停止する、又は削除する必要がある。セキュリティパッチについては、6.2.1 項「ソフトウェアに関する脆弱性対策」を参照のこと。

遵守事項

(3) 端末の運用終了時の対策

(a) 部局技術責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

【 基本対策事項 】規定なし

(解説)

- **遵守事項 7.1.1(3)(a)「端末の運用を終了する際」について**

  端末を廃棄処分する場合やリース契約が終了し端末を返却する場合が考えられる。

- **遵守事項 7.1.1(3)(a)「抹消する」について**

  抹消の方法については、「(解説) 遵守事項 3.1.1(7)(b)「抹消する」について」を参照のこと。

  なお、運用を外部委託しているなど、調達元の本学において抹消できない場合においては、保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずることが必要である。

7.1.2 サーバ装置

目的・趣旨

電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に本学が有するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、6.2.3 項「サービス不能攻撃対策」、7.3.2 項「IPv6 通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベースについては、本項での共通的な対策に加え、それぞれ 7.2 節「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。

遵守事項

(1) サーバ装置の導入時の対策

(a) 部局技術責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

(b) 部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。

(c) 部局技術責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で**利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める**こと。

(d) 部局技術責任者は、通信回線を経由してサーバ装置の**保守作業を行う際に送受信される情報が漏えいすることを防止するための対策**を講ずること。

【 基本対策事項 】

＜7.1.2(1)(a)関連＞

7.1.2(1)-1 部局技術責任者は、要保護情報を取り扱うサーバ装置については、**クラス２以上の要管理対策区域に設置する**こと。

7.1.2(1)-2 部局技術責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

a) 施錠可能なサーバラックに設置して施錠する。
b) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

7.1.2(1)-3 部局技術責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。
a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。

＜7.1.2(1)(b)関連＞

7.1.2(1)-4 部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため要安定情報を取り扱う情報システムについては、将来の見通しも考慮し、以下を例とする対策を講ずること。
a) 負荷分散装置、
DNS ラウンドロビン方式等による負荷分散
b) 同一システムを２系統で構成することによる冗長化

＜7.1.2(1)(c)関連＞

7.1.2(1)-5 部局技術責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。
a) ソフトウェアベンダのサポート状況
b) ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容
c) インストール時に同時にインストールされる他のソフトウェア
d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

（解説）

- **遵守事項 7.1.2(1)(c)「利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める」について**

「（解説）遵守事項 7.1.1(1)(c)「利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める」について」を参照のこと。

- **遵守事項 7.1.2(1)(d)「保守作業を行う際に送受信される情報が漏えいすることを防止するための対策」について**

部局技術責任者から保守作業を許可されている者がサーバ装置へログインして作業する場合を想定し、例えばインターネットを介してサーバ装置の保守作業を行う場合等、通信内容を秘匿する必要がある場合には、サーバ装置の設置時に暗号化するための機能を設け、運用時に情報の暗号化を実施できるようにしておくこと等が考えられる。

- **基本対策事項 7.1.2(1)-1「クラス２以上の要管理対策区域に設置する」について**

サーバ装置に関しては、取り扱う情報の重要性に応じてクラス３の区域に設置することも考慮するとよい。また、クラス２の区域（執務室等）に設置する場合においても常時施錠されたサーバラックに置くことも考慮するとよい。

- **基本対策事項 7.1.2(1)-4 d)「冗長化」について**

  「冗長化」とは、障害や過度のアクセスが発生した場合を想定し、サービスを提供するサーバ装置を代替サーバ装置に切り替えること等により、サービスが中断しないように、情報システムを構成することである。可用性を高めるためには、サーバ装置本体だけでなく、ハードディスク等のコンポーネント単位で冗長化することも考えられる。

  なお、災害等を想定して冗長化する場合には、代替のサーバ装置を遠隔地に設置することが望ましい。

- **基本対策事項 7.1.2(1)-5「利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める」について**

  「(解説) 基本対策事項 7.1.1(1)-5「利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める」について」を参照のこと。

遵守事項

(2) サーバ装置の運用時の対策

(a) 部局技術責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

(b) 部局技術責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図ること。

(c) 部局技術責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

(d) 部局技術責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講ずること。

【 基本対策事項 】

＜7.1.2(2)(b)関連＞

7.1.2(2)-1 部局技術責任者は、所管する範囲内のサーバ装置の構成やソフトウェアの状態を定期的に確認する場合は、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。

＜7.1.2(2)(c)関連＞

7.1.2(2)-2 部局技術責任者は、サーバ装置への無許可のアクセス等の不正な行為を監視するために、以下を例とする対策を講ずること。

a) アクセスログ等を定期的に確認する。
b) IDS/IPS、WAF 等を設置する。
c) 不正プログラム対策ソフトウェアを利用する。
d) ファイル完全性チェックツールを利用する。
e) CPU、メモリ、ディスク I/O 等のシステム状態を確認する。

＜7.1.2(2)(d)関連＞

7.1.2(2)-3 部局技術責任者は、要安定情報を取り扱うサーバ装置については、運用状態を復元するために以下を例とする対策を講ずること。

a) サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。
b) 定期的なバックアップを実施する。
c) サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。
d) バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。

（解説）

- **遵守事項 7.1.2(2)(a)「見直しを行う」について**

ソフトウェアのバージョン更新、サポート期限切れ、新しいソフトウェアの出現等に適切に対応するため、定期的に利用を認めるソフトウェア及び利用を禁止するソフトウェアの見直しを行うことが必要である。

- **遵守事項 7.1.2(2)(b)「不適切な状態にあるサーバ装置を検出等した場合には改善を図る」について**

「不適切な状態」とは、サーバ装置のハードウェアの構成が不正に変更されている、又はセキュリティ水準の低下を招くような変更がされている、利用を認めるソフトウェア以外のソフトウェアがインストールされている、ソフトウェアが動作するための適切な設定がなされていない、最新のセキュリティパッチが適用されていないなどの状態のことをいう。

利用を認めるソフトウェア以外のソフトウェアがインストールされているか否かについては、構成管理ツールを使用するほか、プロセスやその他挙動等を監視する方法もある。また、利用を認めるソフトウェアであっても、利用しない機能については無効化するなどの措置が考えられる。セキュリティパッチについては、6.2.1 項「ソフトウェアに関する脆弱性対策」を参照のこと。

- **基本対策事項 7.1.2(2)-2 a)「アクセスログ等を定期的に確認する」について**

不正アクセスを検知するために、サーバ装置へのアクセスに関するログのほか、サーバ装置が異常等を検出した際に出力するログ（エラーログ）を確認することも有効である。

アクセスログを確認する際は、運用管理作業の記録、管理者権限を持つ識別コードを付与された者の出退勤記録又は入退室記録等との相関分析を併せて行うことにより、不正なアクセスが行われた可能性を確認することも考えられる。

- **基本対策事項 7.1.2(2)-3 b)「バックアップ」について**

バックアップには、サービスの提供に当たって必要なデータやサービスの利用者が入力したデータのバックアップのほか、運用に必要となるシステム設定のバックアップも含まれる。バックアップの取得方法として、前回内容からの変更部分のみバックアップを実施する方法でもよい。

なお、バックアップの手段や保管場所については、「（解説）基本対策事項 3.1.1(8)-2「適切なバックアップの手段又は保管場所」について」も参照のこと。

遵守事項

(3) サーバ装置の運用終了時の対策

(a) 部局技術責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。

【 基本対策事項 】規定なし

(解説)

- **遵守事項 7.1.2(3)(a)「サーバ装置の運用を終了する際」について**

  サーバ装置を廃棄処分する場合やリース契約が終了し返却する場合のほか、当該サーバ装置のサービス又は機能の提供を終了する場合も考えられる。

- **遵守事項 7.1.2(3)(a)「抹消する」について**

  「(解説) 遵守事項 7.1.1(3)(a)「抹消する」について」を参照のこと。

7.1.3 複合機・特定用途機器

目的・趣旨

本学においては、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている複合機が利用されている。複合機は、学内通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、本学においては、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。

したがって、複合機や特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずることが重要である。

遵守事項

(1) 複合機

(a) 部局技術責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。

(b) 部局技術責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。

(c) 部局技術責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。

【 基本対策事項 】

＜7.1.3(1)(a)関連＞

7.1.3(1)-1 部局技術責任者は、「IT 製品の調達におけるセキュリティ要件リスト」を参照するなどし、複合機が備える機能、設置環境及び取り扱う情報の格付及び取扱制限に応じ、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記すること。

＜7.1.3(1)(b)関連＞

7.1.3(1)-2 部局技術責任者は、以下を例とする運用中の複合機に対する、情報セキュリティインシデントへの対策を講ずること。

a) 複合機について、利用環境に応じた適切なセキュリティ設定を実施する。

b) 複合機が備える機能のうち利用しない機能を停止する。

c) 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用する。

d) 学内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする。
e) 複合機をインターネットに直接接続しない。
f) リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
g) 利用者ごとに許可される操作を適切に設定する。

＜7.1.3(1)(c)関連＞

7.1.3(1)-3 部局技術責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消すること。当該機能を備えていない複合機については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずること。

（解説）

- **基本対策事項 7.1.3(1)-1「「IT 製品の調達におけるセキュリティ要件リスト」を参照」について**

遵守事項 5.2.1(2)(d)及び基本対策事項 5.2.1(2)-6 に規定されている「IT 製品の調達におけるセキュリティ要件リスト」には、複合機について一般的に想定される「セキュリティ上の脅威」が記載されているため、それらが自身の運用環境において該当する場合には対抗する必要がある。当該リストには、「国際標準に基づくセキュリティ要件」が記載されており、それを調達時に活用することで脅威に対抗するための機能を有した製品を調達することが可能となる。

なお、「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」のうち、利用環境や複合機に実装されている機能によっては、一部の脅威だけに対抗すればよい場合もあり得る。そのような場合には、「国際標準に基づくセキュリティ要件」では過剰な要件（要求仕様）となる可能性もあるので、個別にセキュリティ要件を策定して脅威に対抗してもよい。

- **基本対策事項 7.1.3(1)-2 a)「適切なセキュリティ設定」について**

自身の利用環境における脅威に対抗するために、運用前に複合機のセキュリティ機能の設定値が適切な値となっていることを確認する必要がある。例えば、管理者パスワードが初期設定のままでないか、イメージスキャナで複合機内部に保存したデータへのアクセス制御設定が適切であるかなどを確認する必要がある。

- **基本対策事項 7.1.3(1)-2 b)「利用しない機能を停止」について**

運用において必要としていない機能が利用者の意図に反して動作していた場合、セキュリティ対策が不十分になっていることが考えられる。対策が不十分である場合は、情報セキュリティインシデントが発生するおそれがあるため、運用上不必要な機能については、運用前に停止した状態にする必要がある。

- **基本対策事項 7.1.3(1)-2 c)「操作パネルで利用者認証が成功した者のみ印刷が許可される機能」について**

  複合機の設置環境によっては、印刷された文書が第三者に閲覧される可能性がある。そのような場合には、印刷の際に複合機内部に一旦データを保存し、複合機本体の操作パネルで主体認証に成功した者だけが印刷できるように設定しておくなどの対策を講ずる必要がある。

- **基本対策事項 7.1.3(1)-2 d)「複合機の内部において接続されないようにする」について**

  複合機にモデム機能が搭載されている場合、公衆通信回線から複合機に接続された後に、複合機を経由して本学 LAN にアクセスされる可能性がある。そのため、モデム機能の無効化等の対策が必要となる。

- **基本対策事項 7.1.3(1)-2 f)「ファイアウォール等の利用により適切に通信制御を行う」について**

  トナー残量の通知や遠隔地からの状態監視等の遠隔保守サービス等を利用する場合には、インターネットを介して外部と通信する必要が生じる。その際には必要最小限の通信のみを許可するようにする必要がある。また、ファイアウォール等の通信制御を行うための機器に例外的な設定を行う場合には、その設定によって脆弱性が生じないようにする必要がある。

- **基本対策事項 7.1.3(1)-2 g)「利用者ごとに許可される操作を適切に設定する」について**

  様々な機能を備えている複合機では、利用者ごとに許可される操作権限の管理が重要となる。例えば、ファクシミリで受信したデータを複合機内部に保存する場合のデータの読み出し権限等を適切に設定していない場合には、情報の漏えいにつながる可能性がある。

- **基本対策事項 7.1.3(1)-3「別の手段で対策を講ずる」について**

  内蔵電磁的記録媒体の全領域完全消去機能を備えていない複合機については、調達元の本学において内蔵電磁的記録媒体の全ての情報を抹消することが困難であるため、外部委託先と情報の抹消サービスを契約するなどの情報の漏えいへの対策を講ずることが必要となる。

遵守事項

(2) 特定用途機器

(a) 部局技術責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。

【 基本対策事項 】

＜7.1.3(2)(a)関連＞

7.1.3(2)-1 部局技術責任者は、特定用途機器の特性に応じて、以下を例とする対策を講ずること。

a) 特定用途機器について、利用環境に応じた適切なセキュリティ設定を実施する。

b) 特定用途機器が備える機能のうち利用しない機能を停止する。

c) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

d) インターネットに接続されている特定用途機器についてソフトウェアに関する脆弱性が存在しないか確認し、脆弱性が存在する場合、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。

e) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。

f) 特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消すること。

（解説）

- **遵守事項 7.1.3(2)(a)「当該機器の特性に応じた対策を講ずる」について**

例えば、テレビ会議システム、IP 電話システム等は本学 LAN を経由してインターネットに接続されて利用されることが想定され、その場合外部からの攻撃対象となり得る。また、これら情報システムを構成する機器が内蔵電磁的記録媒体を備える場合は、運用終了時に内蔵電磁的記録媒体に残された情報が漏えいするおそれがある。

このような脅威に対抗するために、情報システムや端末、サーバ装置に対して定められた遵守事項や基本対策事項を参考にして、情報システム、特定用途機器の特性に応じて対策を講ずるとよい。

- **基本対策事項 7.1.3(2)-1 d)「バージョンアップやセキュリティパッチの適用」について**

本学で対処できないような機器の場合には、特定用途機器の調達に当たって保守契約締結の必要性等について検討することも重要である。

7.2　電子メール・ウェブ等

7.2.1　電子メール

目的・趣旨

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する事務従事者が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本項の遵守事項のほか、7.1.2 項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) 電子メールの導入時の対策

(a) 部局技術責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

(b) 部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

(c) 部局技術責任者は、電子メールのなりすましの防止策を講ずること。

【 基本対策事項 】

＜7.2.1(1)(b)関連＞

7.2.1(1)-1 部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする事務従事者の主体認証を行う機能を備えること。

a) 電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入する。

＜7.2.1(1)(c)関連＞

7.2.1(1)-2 部局技術責任者は、以下を例とする電子メールのなりすましの防止策を講ずること。

a) SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）等の送信ドメイン認証技術による送信側の対策を行う。

b) SPF、DKIM、DMARC 等の送信ドメイン認証技術による受信側の対策を行う。

c) S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用する。

（解説）

- **遵守事項 7.2.1(1)(a)「不正な中継」について**

不正な中継が行われると、迷惑メールの送信等に悪用される問題がある。これにより、電子メールサーバや通信回線のリソースが消費されて運用に支障をきたす、不正な中継を行う電子メールサーバとして他の電子メールサーバ等から接続や電子メールの転送を拒否される、又は迷惑メールの受信者からの苦情や問合わせへの対応が必要になるなどの問題が生じるおそれがある。これらを回避するため、電子メールの不正な中継を行わないように電子メールサーバを設定することが必要である。

- **基本対策事項 7.2.1(1)-2 a)「送信ドメイン認証技術」について**

送信ドメイン認証技術には、SPF、DKIM 等が挙げられる。これらは、送信する電子メールのドメインを管理する DNS サーバに登録・公開された、送信側の電子メールサーバの情報や電子署名で使用する公開鍵を利用することで実現する。

また、送信ドメイン認証技術によって電子メールのなりすましを防止するためには、送信した電子メールの正当性を受信者が確認できるようにするための送信側の対策と、受信した電子メールの正当性を判定して、なりすまされた電子メールから受信者を保護するための受信側の対策があり、両方の実施が求められる。

DMARC は、送信元ドメインに対し、効果的な認証基準が得られるよう、認証技術を自身のインフラに実装するに当たっての、より統合的な手法を定義するとともに、電子メールの受信者が SPF、DKIM 等に係る送信ドメイン認証の詳細な結果を電子メールの送信者にフィードバックするフレームワークを実現するための仕様である。

- **基本対策事項 7.2.1(1)-2 a)「送信側の対策」について**

送信ドメイン認証技術による送信側の対策として、電子メールで使用するドメインを管理する DNS サーバに、受信者が電子メールの正当性を確認するための情報を登録し公開する必要がある。例えば、SPF の場合は送信側の電子メールサーバの情報を DNS サーバに登録する。また、DKIM の場合は電子メールに付与する電子署名の検証に使用する公開鍵を DNS サーバに登録する。

なお、SPF については、以下の事項に留意すること。

- 電子メールを利用していないドメインについても、その情報を SPF レコードに登録する。（「SPF レコード」とは、SPF において、DNS サーバの TXT レコードに記述される送信側の電子メールサーバ等の情報をいう。）
- SPF レコードの末尾は、”~all”ではなく”-all”を記述する。
- SPF レコードは、チェックツール等で、文法的に記述間違いのないことを確認する。
- なりすましの防止策のため、ウェブによるサービス等も含め全く利用していない、又は将来にわたって利用の予定の無いドメインについては、なりすましの防止策を講ずるか、ドメイン名の登録を廃止する。
- 民間事業者等において提供されている、他の利用者と共用する電子メールサービスを利用する場合は、本学をなりすました電子メールが、当該電子メールサ

ービスを利用する他の利用者から送信されないような仕組みを備えていることを確認する。他の利用者と共用しない専用の IP アドレスを割り振ることが可能なサービスが提供されている場合は、当該サービスの利用を検討する。

- **基本対策事項 7.2.1(1)-2 b)「受信側の対策」について**

送信ドメイン認証技術による受信側の対策としては、受信した電子メールに対し送信ドメイン認証に基づくなりすまし判定（例えば SPF の場合、受信時に通信を行った送信側の電子メールサーバと、受信した電子メールに記載されている送信側ドメインを管理する DNS サーバに登録されている送信側の電子メールサーバの情報との比較による判定）を行い、なりすましと判定した場合には、以下に例示するような電子メールの受信者への注意喚起等を行うことが挙げられる。

- 電子メールの件名（Subject）や本文への注意喚起文の挿入
- 電子メールクライアントの機能によるラベリングやメッセージの表示
- 電子メールクライアント又は電子メールサーバにおける電子メールの隔離や削除等のフィルタリング

また、送信者が DMARC に対応している場合は、送信者のポリシーに従って隔離や受信自体の拒否を行うことが可能となる。

- **基本対策事項 7.2.1(1)-2 c)「S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名」について**

外部に一斉送信する電子メールに、組織の電子証明書で電子署名をすることは、電子メールのなりすまし防止の観点から効果的である。

また、通常のメールについては、職員に電子証明書を配布し、電子署名を付与することにより、電子メールクライアントによっては、同時に電子メールを自動的に暗号化することが可能となるというメリットもある。

7.2.2 ウェブ

目的・趣旨

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ（ウェブページとして公開している情報）の改ざん、ウェブサーバの停止、偽サイトへの誘導等の被害が想定されるため、適切な対策を組み合わせて実施することが求められる。

なお、本項の遵守事項のほか、7.1.2 項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) ウェブサーバの導入・運用時の対策

(d) 部局技術責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずること。

(ア) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

(イ) ウェブコンテンツの編集作業を担当する主体を限定すること。

(ウ) 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。

(エ) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。

(オ) サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。

(e) 部局技術責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

【 基本対策事項 】

＜7.2.2(1)(a)(ア)関連＞

7.2.2(1)-1 部局技術責任者は、不要な機能の停止又は制限として、以下を例とするウェブサーバの管理や設定を行うこと。

a) CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする。

b) ディレクトリインデックスの表示を禁止する。

c) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する。

d) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。

＜7.2.2(1)(a)(イ)関連＞

7.2.2(1)-2 部局技術責任者は、ウェブコンテンツの編集作業を担当する主体の限定として、

以下を例とするウェブサーバの管理や設定を行うこと。
a) ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えない。
b) OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。

＜7.2.2(1)(a)(ウ)関連＞

7.2.2(1)-3 部局技術責任者は、公開してはならない又は無意味なウェブコンテンツが公開されないよう管理することとして、以下を例とするウェブサーバの管理や設定を行うこと。
a) 公開を想定していないファイルをウェブ公開用ディレクトリに置かない。
b) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。

＜7.2.2(1)(a)(エ)関連＞

7.2.2(1)-4 部局技術責任者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行うこと。
a) ウェブコンテンツの更新の際は、**専用の端末**を使用して行う。
b) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する。
c) ウェブコンテンツの更新に利用する識別コードや主体認証情報は、**情報セキュリティを確保した管理**を行う。

＜7.2.2(1)(a)(オ)関連＞

7.2.2(1)-5 部局技術責任者は、通信時の盗聴による第三者への情報の漏えいの防止及び正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を例とするウェブサーバの実装を行うこと。
a) **TLS（SSL）機能を適切に用いる**。
b) TLS（SSL）機能のために必要となるサーバ証明書には、**利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局**（証明書発行機関）により発行された電子証明書を用いる。
c) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された「SSL/TLS 暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する。

（解説）

- **基本対策事項 7.2.2(1)-1 a)「CGI 機能」について**

CGI（Common Gateway Interface）とは、ウェブブラウザから送信された文字列を、スクリプト等のプログラムへの入力パラメータとして受け取り、当該スクリプト等をウェブサーバ上で実行するための仕組みである。外部からの文字列に基づいて実行されるスクリプト等は脆弱性の原因となり易い部分であり、細心の注意を払って脆弱性の無いスクリプト等のみを設置しなければならない。そのため、本基本対策事項は、

サーバに設置するスクリプト等は必要最低限のものに限定することを求めている。

- **基本対策事項 7.2.2(1)-1 b)「ディレクトリインデックスの表示を禁止する」について**

ウェブサーバの機能であるディレクトリインデックスの表示機能とは、ウェブサイトの公開対象となるディレクトリが、ファイル名を指定しない形式の URL(すなわち、例えば「http://exmaple.go.jp/directory_name/」の形式）又は「index.html」等の所定のファイル名を指定した形式の URL によってアクセスされたときに、当該ディレクトリに存在するファイル名の一覧を自動的に生成して表示する機能である。万が一、公開するつもりのないファイルがディレクトリに混入していた場合、ディレクトリインデックス機能が有効であると、外部から容易にそのファイル名を見つけられてしまい、アクセスされてしまう。本来、公開対象のディレクトリには、非公開にすべきファイルが混入していてはならないところであるが、念のため、本基本対策事項は、ディレクトリインデックスの表示機能を無効にすることを求めている。

- **基本対策事項 7.2.2(1)-1 c)「不要な機能を制限する」について**

不要な機能の典型的な例としては、管理者画面の機能が挙げられる。ウェブコンテンツ作成ツールや CMS には、コンテンツを編集する管理者向けのログイン画面を有するものがある。このログイン画面がインターネットから閲覧可能であると、管理者のパスワードを破って不正にログインされ、ウェブサイトのコンテンツを改ざんされるリスクを生じさせる。管理者画面は、学内からのアクセスのみを許可し、インターネットからの利用を制限することを求めている。その他の不要な機能として制限すべき例として、アクセス解析の機能がインターネットから閲覧できるようになっている場合等が挙げられる。

- **基本対策事項 7.2.2(1)-4 a)「専用の端末」について**

ウェブコンテンツを管理する端末では、ウェブコンテンツの管理に関係する作業のみを行い、その作業に関係の無いウェブサイトを閲覧しない、セキュリティ対策が不十分な USB メモリを利用しないなど、情報セキュリティを確保した運用が必要である。また、ウェブサーバのみでなく、ウェブコンテンツを管理する専用の端末においても、不正プログラム対策やソフトウェアに関する脆弱性対策を行うことが重要である。

- **基本対策事項 7.2.2(1)-4 c)「情報セキュリティを確保した管理」について**

ウェブコンテンツを更新する際の主体認証情報について、パスワードを設定する場合は十分な長さと複雑さを持ったものとする、多要素主体認証方式で主体認証を行う機能を設けるなどにより、情報セキュリティを確保することが求められる。また、ウェブコンテンツの更新に利用する識別コードや主体認証情報は、他の情報システムの認証で使用しているものを使い回さない、ウェブコンテンツを更新する者以外に知らせない、複数の更新を実施する者で共有しないなどの情報セキュリティを確保した管理が求められる。

- **基本対策事項 7.2.2(1)-5 a)「TLS（SSL）機能を適切に用いる」について**

ウェブサーバに TLS（SSL）機能を搭載することにより、利用者が当該ウェブサー

バのサイトを「https://」で始まる URL でアクセスできるようになる。「https://」で始まる URL のページ（以下「セキュアページ」という。）へのアクセスは、ブラウザからウェブサーバへの入力及びウェブサーバからブラウザへの出力が自動的に暗号化されて送受信される。

盗聴による情報の漏えいを防止するには、盗聴を防ぐべき情報を出力するウェブページがセキュアページとなっていることが必要である。また、盗聴を防ぐべき情報を利用者に入力させるウェブページを設ける場合には、入力された情報の送信先となる URL がセキュアページとなっていることが必要であり、かつ、利用者に情報を入力させるウェブページ（入力欄が設置されている画面）自体もセキュアページとなっていることが必要である。

ウェブサーバに TLS（SSL）機能を搭載することは、当該ウェブサーバが正当なサーバである（偽のサーバでない）ことを確認できる手段を利用者に提供することにもなる。利用者は、当該サイトを「https://」で始まる URL でアクセスし、エラーなく正常に表示されたことで、当該サーバが当該ドメイン名の正当なサイトのものであると確認することができる。

なお、TLS（SSL）機能を用いるに当たっては、使用するバージョンの脆弱性に関する最新の情報も踏まえ、適切に使用することが必要である。

- **基本対策事項 7.2.2(1)-5 b)「利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局」について**

TLS（SSL）機能を用いるには、ウェブサーバ側に「サーバ証明書」と呼ばれる電子証明書の設置が必要であり、サーバ証明書はそれを発行する「認証局」から取得する必要がある。サーバ証明書の取得は、政府認証基盤（GPKI）の「アプリケーション認証局」から取得することもできるほか、民間事業者から取得することもできる。

本基本対策事項は、サーバ証明書をどの認証局から取得するかの選択において、「利用者が事前のルート証明書のインストールを必要とすることなくその正当性を検証できる認証局」を選択することを求めている。それ以外の認証局を選択した場合、利用者のウェブブラウザには、サーバ証明書の正当性検証ができないことを示す警告やエラー画面が表示されることになる。この警告やエラー画面は、事前に当該認証局の自己署名証明書をブラウザにルート証明書としてインストールすることによって解消することができる。しかし、一般に、利用者によるルート証明書のインストールは安全に行うことが容易でないものであり、利用者に危険を伴うルート証明書のインストールを強いるのはそもそも避けるべきことである。そのため、本基本対策事項は、利用者にルート証明書のインストールを求めなくても、警告やエラー画面が現れることなく、正常に TLS（SSL）通信ができるよう、適切に認証局を選択してサーバ証明書を取得することを求めている。

なお、ウェブサーバの利用が学内の管理された端末からのアクセスに限定されている場合には、対象となる全ての端末に対して事前に安全な方法でルート証明書をインストールすることも可能であるから、そのような管理がなされている場合には、当該ウェブサーバで使用するサーバ証明書として、本学で独自に用意した認証局から発行

されたものを用いることができる。

- **基本対策事項 7.2.2(1)-5 c)「「SSL/TLS 暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する」について**

CRYPTREC が発行している「SSL/TLS 暗号設定ガイドライン」は、TLS（SSL）通信での安全性と可用性（相互接続性）のバランスを踏まえた TLS（SSL）サーバの設定方法のガイドラインを示すものである。

このガイドラインでは、「高セキュリティ型」、「推奨セキュリティ型」、「セキュリティ例外型」の 3 段階の設定基準に分けて、各々の要求設定が示されており、どの設定基準を採用するかは、安全性の確保と相互接続の必要性の両面を鑑みてサーバ管理者が選択するものとされている。

「高セキュリティ型」は、利用例として「政府内利用（G2G 型）のなかでも、限定された接続先に対して、とりわけ高い安全性が要求される通信を行う場合」が示されているように、一般の利用者がウェブブラウザ等で接続することのないサーバの場合を対象とし、専用システム内又は専用システム間で閉じたネットワークを構成して暗号化通信に TLS（SSL）を用いる際に選択すべき設定基準である。

他方、「推奨セキュリティ型」は、利用例に「電子申請等、企業・国民と役所等の電子行政サービスを提供する場合」とあるように、一般の利用者がウェブブラウザで接続することを前提としたサーバを構成する場合に選択する設定基準であり、普及している PC、スマートフォン等で問題なく相互接続性を確保できる要求設定が示されたものである。

ガイドラインは、巻末に付録として「チェックリスト」を提供しており、ここに、設定基準ごとに満たすべき要求設定として「プロトコルバージョン設定」、「サーバ証明書設定」、「暗号スイート設定」の具体的な基準が示されているので、これに従うことで、容易に適切な TLS（SSL）設定を行うことができる。

部局技術責任者は、TLS（SSL）を導入するシステムの特性に応じて、どの設定基準が相応しいかを決定し、その設定基準に対応する要求設定に従ったサーバ設定を、「チェックリスト」を活用して確認するなどして、適切に行うことが求められる。

また、ガイドラインは、「サーバ証明書の作成・管理について注意すべきこと」として、鍵ペアの適切な生成方法や鍵の適切な管理方法を示し、また、「さらに安全性を高めるために」として、HTTP Strict Transport Security (HSTS) の設定有効化その他を推奨している。これらについても併せて検討することが望ましい。

参考：CRYPTREC「SSL/TLS 暗号設定ガイドライン」（平成 27 年 8 月 3 日）
（http://www.cryptrec.go.jp/report/c14_oper_guideline_SSLTLS_web_1_1.pdf）

上記のウェブサイトのアドレスは、平成 28 年 6 月 1 日時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

遵守事項

(2) ウェブアプリケーションの開発時・運用時の対策

(a) 部局技術責任者は、ウェブアプリケーションの開発において、既知の種類の**ウェブアプリケーションの脆弱性を排除するための対策**を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

【 基本対策事項 】

＜7.2.2(2)(a)関連＞

7.2.2(2)-1 部局技術責任者は、以下を含むウェブアプリケーションの脆弱性を排除すること。

a) **SQL インジェクション脆弱性**
b) **OS コマンドインジェクション脆弱性**
c) **ディレクトリトラバーサル脆弱性**
d) **セッション管理の脆弱性**
e) **アクセス制御欠如と認可処理欠如の脆弱性**
f) **クロスサイトスクリプティング脆弱性**
g) **クロスサイトリクエストフォージェリ脆弱性**
h) **クリックジャッキング脆弱性**
i) **メールヘッダインジェクション脆弱性**
j) **HTTP ヘッダインジェクション脆弱性**
k) **eval インジェクション脆弱性**
l) **レースコンディション脆弱性**
m) **バッファオーバーフロー及び整数オーバーフロー脆弱性**

（解説）

- **遵守事項 7.2.2(2)(a)「ウェブアプリケーションの脆弱性を排除するための対策」について**

ウェブアプリケーションの開発時には、既知の種類のウェブアプリケーションの脆弱性を排除するための対策が求められる。脆弱性を排除したウェブアプリケーションを実装する方法の詳細については、独立行政法人情報処理推進機構（IPA）による「安全なウェブサイトの作り方」を参照することも考えられる。

参考：独立行政法人情報処理推進機構「安全なウェブサイトの作り方 改訂第 7 版」（https://www.ipa.go.jp/security/vuln/websecurity.html）

このウェブサイトのアドレスについては、平成 28 年 6 月 1 日時点のものである。ウェブサイトのアドレスについては廃止や変更されることがあるため、最新のアドレスを確認した上で利用すること。

- **基本対策事項 7.2.2(2)-1 a)「SQL インジェクション脆弱性」について**

ウェブアプリケーションのプログラムがデータベースを操作する手段として SQL 言語を用いている場合に、プログラムが SQL 文を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が SQL 文に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、データベースを破壊されたり、データベース内の情報を盗まれたりするなどの被害が生じ得る。このような欠陥は一般に「SQL インジェクション脆弱性」と呼ばれている。SQL インジェクション脆弱性を排除するには、SQL 文の組み立てにプレースホルダを用いる実装方法を採用することを徹底するなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 b)「OS コマンドインジェクション脆弱性」について**

ウェブアプリケーションのプログラムが OS のコマンドを操作する必要がある場合に、プログラムが OS のシェルのコマンドラインを用いてコマンド呼出しをする構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列がコマンドラインに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、サーバに侵入される被害が生じ得る。このような欠陥は一般に「OS コマンドインジェクション脆弱性」と呼ばれている。OS コマンドインジェクション脆弱性を排除するには、OS コマンドの操作にシェルのコマンドラインを用いない実装方法を採用することを徹底するなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 c)「ディレクトリトラバーサル脆弱性」について**

ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっている場合に、指定されたパス名をプログラムがそのまま使用する構造になっていると、公開を想定しないファイルが参照されて、その内容が外部から閲覧され得る欠陥となる場合がある。このような欠陥は一般に「ディレクトリトラバーサル脆弱性」と呼ばれている。ディレクトリトラバーサル脆弱性を排除するには、外部のパラメータからパス名を指定する仕様を排除する対策、それができない場合には、ファイルにアクセスする直前に、使用するパス名の妥当性検査を行う方法、又は、ファイルのディレクトリと識別子を固定にしてアクセスするなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 d)「セッション管理の脆弱性」について**

ウェブアプリケーションのプログラムがログイン機能を有するなど、セッション管理の仕組みを持つ場合に、そのセッション管理の実装方法に欠陥がある場合がある。例えば、セッション管理に用いられるセッション ID が推測可能な値となっている場合、セッション ID を URL パラメータに格納している場合、TLS（SSL）を使用しているセッションの管理に用いる cookie に secure 属性がセットされていない場合等が、この脆弱性に該当する。この欠陥を攻撃されると、正規の利用者がログイン中に、その利用者になりすまして不正にアクセスする「セッションハイジャック」の被害が生じ得る。この脆弱性を排除するには、暗号論的疑似乱数生成器（CSPRNG）で生成する十分な長さの文字列をセッション ID として推測困難なものとし、secure 属性のセットされた cookie にこれを格納することでセッション ID の漏えいを防ぐ対策方法が考えら

れる。

- **基本対策事項 7.2.2(2)-1 e)「アクセス制御欠如と認可処理欠如の脆弱性」について**

ウェブアプリケーションがログイン機能を有し、ログイン中の利用者にのみ利用を許可すべき機能がある場合に、ログインしていない利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「アクセス制御欠如の脆弱性」と呼ばれる。また、ログイン中の利用者のうち、一部の利用者にのみ利用を許可すべき機能がある場合に、それ以外の利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「認可処理欠如の脆弱性」と呼ばれる。これらの欠陥を攻撃されると、秘密情報の漏えい、なりしまし操作等の被害が生じ得る。これらの脆弱性を排除するには、アクセス制御と認可処理が必要な画面の仕様を明確にし、仕様に沿った実装を徹底するなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 f)「クロスサイトスクリプティング脆弱性」について**

ウェブアプリケーションのプログラムが HTML ページを出力する場合に、プログラムが HTML を文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が HTML に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、cookie の値を盗まれてセッションハイジャックされるほか、画面の内容を改ざんされるなどの被害が生じ得る。このような欠陥は一般に「クロスサイトスクリプティング脆弱性」と呼ばれている。クロスサイトスクリプティング脆弱性を排除するには、以下を含む対策が考えられる

  - HTML の出力に際して HTML タグの出力以外の全ての出力において文字列を HTML エスケープ処理することを徹底する。
  - URL を出力するときは「http://」又は「https://」で始まる URL のみを許可する。
  - SCRIPT 要素の内容を動的に生成しないようにする。
  - スタイルシートを任意のサイトから取り込める仕様を排除する。
  - 全てのページについて HTTP レスポンスヘッダの「Content-Type」フィールドの「charset」に文字コードの指定を行う。

ただし、当該ウェブアプリケーションの仕様の都合で、これらだけでは解決できない場合もあり、その場合には追加的な対策が必要となる。

- **基本対策事項 7.2.2(2)-1 g)「クロスサイトリクエストフォージェリ脆弱性」について**

ウェブアプリケーションが、ログイン中の利用者にのみ利用を許可する機能を有している場合に、その機能のウェブページに前記 e)の対策が施されている場合であっても、外部のサイトから当該ウェブページにリンクを張る方法により、利用者本人にそのリンクをたどらせることで、当該利用者の意図に反して当該機能が利用されてしまうという構造になっている場合がある。このような欠陥は一般に「クロスサイトリクエストフォージェリ脆弱性」と呼ばれている。この欠陥を攻撃されると、悪意ある者が仕掛けたリンクによって、不正に当該機能を操作される被害（具体的には、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害）が生じ得る。

この脆弱性を排除するには、外部からのリンクによって機能が作動してはならないウェブページは、処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行するように実装するなどの対策方法が考えられる。

- **基本対策事項 7.2.2(2)-1 h)「クリックジャッキング脆弱性」について**

ウェブアプリケーションが、サイト内のボタンやリンクをクリックするだけで作動する機能を有している場合に、悪意ある者が、当該サイトを透明化した（透明色で表示して利用者の目に見えないように設定された）フレームとして外部のサイト上に表示するようにし、利用者を当該外部サイトへ誘導して、当該ボタンやリンクの表示された画面上の位置をクリックさせるよう誘導することで、利用者の意図に反して当該機能を作動させることができてしまう場合がある。このような欠陥は一般に「クリックジャッキング脆弱性」と呼ばれている。この欠陥を攻撃されると、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害が生じ得る。この脆弱性を排除するには、ウェブサーバの設定で、HTTP レスポンスに「X-Frame-Options」ヘッダを出力するようにし、そのフィールド値に「deny」又は「sameorigin」の値をセットすることで、当該ウェブページが外部のサイトにフレームとして表示されることを拒否するよう利用者のブラウザに指示する機能を用いるといった対策方法が考えられる。

- **基本対策事項 7.2.2(2)-1 i)「メールヘッダインジェクション脆弱性」について**

ウェブアプリケーションが電子メールを送信する機能を有し、その宛先となる電子メールアドレスをウェブアプリケーションのパラメータから指定する構造になっている場合に、悪意ある者により任意の電子メールアドレスが当該パラメータに与えられ、迷惑メールの送信のために当該ウェブアプリケーションが悪用されてしまうという被害が生じ得る。この欠陥を排除するには、電子メールの送信先電子メールアドレスはプログラム中に固定的に記述する実装方法（又は設定ファイルから読み込む実装方法）を採用して、ウェブアプリケーションのパラメータを用いるのを避けるなどの対策方法が考えられる。

- **基本対策事項 7.2.2(2)-1 j)「HTTP ヘッダインジェクション脆弱性」について**

ウェブアプリケーションが HTTP レスポンスヘッダの「Location」や「Set-Cookie」のフィールド値を動的に出力する構造になっている場合、外部から悪意ある者によって与えられた改行文字を含む攻撃用の文字列が HTTP レスポンスヘッダに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、クロスサイトスクリプティング脆弱性の場合と同じ被害が生じ得る。このような欠陥は一般に「HTTP ヘッダインジェクション脆弱性」と呼ばれている。HTTP ヘッダインジェクション脆弱性を排除するには、HTTP レスポンスヘッダを出力する際に、直接にヘッダ文字列を出力するのではなく、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する実装方法を採用するなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 k)「eval インジェクション脆弱性」について**

  ウェブアプリケーションのプログラムを作成する言語が、「eval」等、文字列をプログラムとして実行する機能を持つ言語である場合に、プログラムがこの機能を使用していると、外部から悪意ある者によって与えられた攻撃用の文字列が、その eval に与える文字列に混入し得る欠陥となることがある。この欠陥を攻撃されると、任意のプログラムがサーバで実行されることとなり、様々な被害が生じ得る。このような欠陥は一般に「eval インジェクション脆弱性」と呼ばれる。この脆弱性を排除するには、eval 機能を一切使用しない実装方法を採用するなどの対策が考えられる。

- **基本対策事項 7.2.2(2)-1 l)「レースコンディション脆弱性」について**

  ウェブアプリケーションの機能を複数の利用者が全く同時に利用したときに、一方の利用者向けの処理ともう一方の利用者向けの処理を途中で取り違えてしまう事態が一定の確率で発生する場合がある。このような欠陥は一般に「レースコンディション脆弱性」と呼ばれる。この欠陥により、利用者の秘密にすべき情報が第三者に閲覧される被害が生じる。この被害は、攻撃者がいなくても偶然に発生する場合もあれば、攻撃者が大量のアクセスをすることで意図的に引き起こされる場合もある。この脆弱性を排除するには、ソースコードレビューによってレースコンディションが起きえない構造にプログラムが記述されていることを確認する方法や、大量のアクセスを同時に発生させて異常が発生しないことを十分に確認するテストを行うなどの対策方法が考えられる。

- **基本対策事項 7.2.2(2)-1 m)「バッファオーバーフロー及び整数オーバーフロー脆弱性」について**

  ウェブアプリケーションのプログラムを作成する言語として、バッファオーバーフロー脆弱性等が生じない言語を採用することが望ましいが、その場合であっても、ウェブアプリケーションが、内部で C 言語等を用いて独自に作成されたプログラムを呼び出す構造になっている場合がある。その呼び出されるプログラムにバッファオーバーフロー脆弱性や整数オーバーフロー脆弱性が存在し、ウェブアプリケーションに外部から与えた文字列が当該プログラムに引き渡される構造になっていると、それらの欠陥を攻撃されて、サーバに侵入される被害が生じ得る。このような脆弱性を排除するためには、C 言語等のバッファオーバーフロー脆弱性等が生じ得る言語により作成されたプログラムが内部で呼び出されることを避けるなどの対策が考えられる。

7.2.3 ドメインネームシステム（DNS）

目的・趣旨

ドメインネームシステム（DNS：Domain Name System）は、インターネットを使った階層的な分散型システムで、主としてインターネット上のホスト名や電子メールに使われるドメイン名と、IP アドレスとの対応づけ（正引き、逆引き）を管理するために使用されている。DNS では、端末等のクライアント（DNS クライアント）からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係等について回答を行う。DNS には、本学が管理するドメインに関する問合せについて回答を行うコンテンツサーバと、DNS クライアントからの要求に応じてコンテンツサーバに対して問合せを行うキャッシュサーバが存在する。キャッシュサーバの可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また、コンテンツサーバが提供する情報の完全性が損なわれ、誤った情報を提供した場合は、端末等の DNS クライアントが悪意あるサーバに接続させられるなどの被害に遭う可能性がある。さらに、電子メールのなりすまし対策の一部は DNS で行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNS サーバの適切な管理が必要である。

なお、本項の遵守事項のほか、7.1.2 項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) DNS の導入時の対策

(a) 部局技術責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。

(b) 部局技術責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。

(c) 部局技術責任者は、コンテンツサーバにおいて、本学のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。

【 基本対策事項 】

＜7.2.3(1)(a)関連＞

7.2.3(1)-1 部局技術責任者は、要安定情報を取り扱う情報システムの名前解決を提供する DNS のコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講ずること。

a) コンテンツサーバを冗長化する。

b) 通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。

＜7.2.3(1)(b)関連＞

7.2.3(1)-2 部局技術責任者は、学外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は必要であれば学内からの名前解決の要求のみに応答をするよう、以下を例とする措置を講ずること。

c) キャッシュサーバの設定でアクセス制御を行う。

d) ファイアウォール等でアクセス制御を行う。

7.2.3(1)-3 部局技術責任者は、DNS キャッシュポイズニング攻撃から保護するため、以下を例とする措置を講ずること。

a) ソースポートランダマイゼーション機能を導入する。

b) DNSSEC を利用する。

＜7.2.3(1)(c)関連＞

7.2.3(1)-4 部局技術責任者は、学内のみで使用する名前の解決を提供するコンテンツサーバにおいて、以下を例とする当該コンテンツサーバで管理する情報の漏えいを防止するための措置を講ずること。

a) 外部向けのコンテンツサーバと別々に設置する。

b) ファイアウォール等でアクセス制御を行う。

（解説）

- **基本対策事項 7.2.3(1)-1 a)「冗長化」について**

コンテンツサーバは、冗長化しておくことが一般的である。その際には、ネットワーク障害等を考慮して各々のDNSのコンテンツサーバをそれぞれ異なるネットワークに配置しておく、災害等を考慮して物理的に離れた建物や遠隔地に設置しておくなど、情報と情報システムに要求される可用性に応じて、最適な構成を検討する必要がある。ISP 等が提供するセカンダリ DNS の利用も、遠隔地への設置による冗長化の措置の例である。

また、要求される可用性の度合いに応じて、保守作業による復旧等、冗長化以外の措置を探ることも考えられる。

- **基本対策事項 7.2.3(1)-2「学外からの名前解決の要求に応じる必要性」について**

不特定のDNSクライアントからの名前解決の要求に応じるキャッシュサーバはオープンリゾルバと呼ばれる。オープンリゾルバは、存在しないホスト名の名前解決の問合せを大量に送信することで上位の DNS サーバの過負荷を狙う DNS 水責め攻撃や、DNS リフレクター攻撃といったサービス不能攻撃等の踏み台として悪用される危険性がある。そのため本学で利用するキャッシュサーバが学外からの名前解決の要求に応じる必要性があるか検討することが必要である。

- **基本対策事項 7.2.3(1)-3「DNS キャッシュポイズニング攻撃」について**

DNS キャッシュポイズニング攻撃とは、DNS のキャッシュサーバにキャッシュされている情報を偽の情報に書き換える攻撃である。この攻撃により、例えば、利用者は正しい URL のウェブサイトに接続しているつもりでも、書き換えられた偽の情報により不正なウェブサイトに誘導されるといった被害を受ける可能性がある。

- **基本対策事項 7.2.3(1)-3 a)「ソースポートランダマイゼーション」について**

  ソースポートランダマイゼーションとは、キャッシュサーバからコンテンツサーバへの問合せに使用される UDP ポート番号をランダム化する技術である。UDP ポート番号をランダム化することにより、攻撃者がキャッシュポイズニング攻撃を行う際に UDP ポート番号の推測を困難にすることができ、攻撃の成功確率を低下させることが可能となる。

- **基本対策事項 7.2.3(1)-3 b)「DNSSEC」について**

  DNSSEC では、コンテンツサーバによって応答に電子署名が行われ、キャッシュサーバがその署名を検証することで、応答が改ざん等されているか確認することができる。DNSSEC は、公開鍵暗号技術を用いるため、その導入には情報の提供側であるコンテンツサーバと情報の問合せ側であるキャッシュサーバの双方に対応が必要となる。学外への信頼できるサービスの提供と、本学の情報セキュリティ向上の観点から、A 大学ドメインを管理するコンテンツサーバ及び学内のキャッシュサーバに対する円滑な DNSSEC の導入が望ましい。

- **基本対策事項 7.2.3(1)-4「当該コンテンツサーバで管理する情報の漏えいを防止するための措置」について**

  コンテンツサーバにおいて、学内のみで使用する名前の解決を提供する場合、内部のみで使用している名前情報を学外の者が取得できないようにすることを求めている。

遵守事項

(2) DNS の運用時の対策

(a) 部局技術責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報について**サーバ間で整合性を維持**すること。

(b) 部局技術責任者は、コンテンツサーバにおいて管理する**ドメインに関する情報が正確であることを定期的に確認**すること。

(c) 部局技術責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。

【 基本対策事項 】

＜7.2.3(2)(c)関連＞

7.2.3(2)-1 部局技術責任者は、キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（3か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持すること。

（解説）

- **遵守事項 7.2.3(2)(a)「サーバ間で整合性を維持」について**

複数台の DNS のコンテンツサーバでドメインに関する情報を保有し管理する場合に、各コンテンツサーバ間でドメインに関する情報の整合性を維持することを求める事項である。例えば、主系統のコンテンツサーバで管理するドメインに関する情報が変更された場合に、ゾーン転送等によって、情報システムの可用性に影響を及ぼさない適切なタイミングで副系統のコンテンツサーバが管理するドメインに関する情報も更新するといった方法が考えられる。

なお、主系統のコンテンツサーバから副系統のコンテンツサーバへ安全にゾーン転送を行う対策として、例えば、TSIG（Transaction Signature）の利用等が考えられる。

- **遵守事項 7.2.3(2)(b)「ドメインに関する情報が正確であることを定期的に確認」について**

近年、国内で使用されているドメイン名の登録情報が不正に書き換えられ、攻撃者が用意したネームサーバの情報が追加される“ドメイン名ハイジャック”と呼ばれる攻撃が複数報告されている。このような攻撃への対策として、コンテンツサーバで管理するドメインに関する情報について、設定誤りや不正な改ざん等が発生していないかを定期的に確認することで、情報の正確性を維持することを求めている。管理するドメインに関する情報の具体例として、以下に挙げる登録内容等を確認することが考えられる。

- ホストの IP アドレス情報を登録する A（AAAA）レコード
- ドメインの電子メールサーバ名を登録する MX レコード
- なりすましメールを防ぐための SPF レコード等を登録する TXT レコード

なりすまし防止の観点からは、管理するドメインについての SPF レコードが正確で

あるかどうかを確認したり、ドメインを廃止する場合には、ドメインの廃止申請を行い、当該ドメインが確実に廃止されていることを確認したりすることが重要である。

7.2.4 データベース

目的・趣旨

本項における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。

要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び事務従事者の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

特に大量のデータを保管するデータベースの場合、そのデータが漏えい等した際の影響が大きく、また、そのようなデータは攻撃者の標的となりやすい。

なお、本項の遵守事項のほか、6.1 節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、6.2.1 項「ソフトウェアに関する脆弱性対策」、6.2.2 項「不正プログラム対策」、7.3.2 項「IPv6 通信回線」において定める遵守事項のうち、データベースに関係するものについても併せて遵守する必要がある。

遵守事項

(1) データベースの導入・運用時の対策

(a) 部局技術責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。

(b) 部局技術責任者は、**データベースに格納されているデータにアクセスした利用者を特定**できるよう、措置を講ずること。

(c) 部局技術責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。

(d) 部局技術責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

(e) 部局技術責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、**適切に暗号化**をすること。

【 基本対策事項 】

＜7.2.4(1)(a)関連＞

7.2.4(1)-1 部局技術責任者は、必要に応じて情報システムの管理者と**データベースの管理者**を別にすること。

7.2.4(1)-2 部局技術責任者は、データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しないこと。

7.2.4(1)-3 部局技術責任者は、データベースの管理に関する**権限の不適切な付与**を検知できるよう、措置を講ずること。

＜7.2.4(1)(c)関連＞

7.2.4(1)-4 部局技術責任者は、事務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずること。
a) 一定数以上のデータの取得に関するログを記録し、警告を発する。
b) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。

＜7.2.4(1)(d)関連＞

7.2.4(1)-5 部局技術責任者は、データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除すること。

7.2.4(1)-6 部局技術責任者は、データベースにアクセスする機器上で動作するプログラムに対して SQL インジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討すること。
a) ウェブアプリケーションファイアウォールの導入
b) データベースファイアウォールの導入

＜7.2.4(1)(e)関連＞

7.2.4(1)-7 部局技術責任者は、データベースに格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

（解説）

- **遵守事項 7.2.4(1)(b)「データベースに格納されているデータにアクセスした利用者を特定」について**

一般的に、データベースの使用形態は図 7.2.4(1)-1 のように、データベースから見たアクセス主体が「人間の利用者」となる場合と、「中間アプリケーションサーバ」となる場合の２つのモデルに分けられる。中間アプリケーションサーバを利用するモデルでは、中間アプリケーションサーバ用にデータベースアクセス用のアカウントを作成して運用する構成となるのが通常である。この構成では、データベースのログにはアクセス主体が中間アプリケーションサーバとして記録されることになるため、不正な操作が行われた場合に実際には誰が操作をしたものかをデータベースのログのみからでは特定できない可能性がある。そのため中間アプリケーションサーバにおいて、データベースの利用者とデータベースへの操作要求とを紐づけてログを取得し、利用者を特定できるようにしておく必要がある。

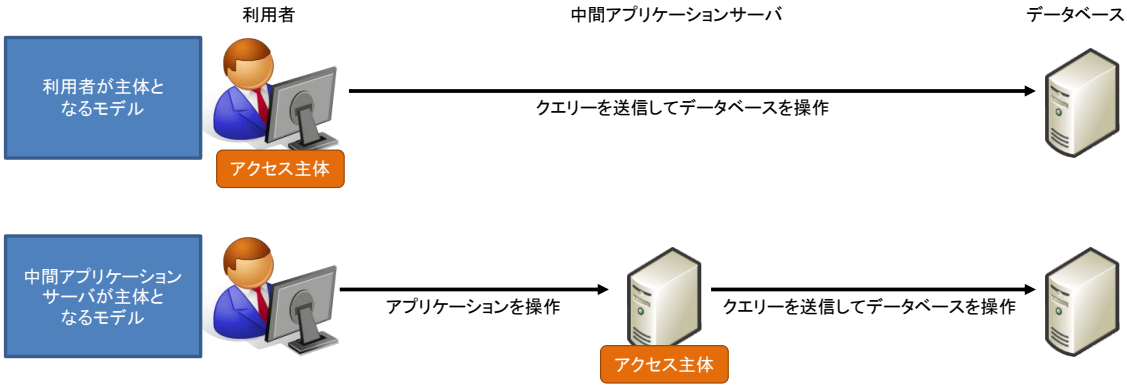


図 7.2.4(1)-1　データベース利用形態モデル

- **遵守事項 7.2.4(1)(e)「適切に暗号化」について**

  データベースに格納されるデータを暗号化する方法には、電磁的記録媒体の暗号化、データベースのテーブルの暗号化、カラムの暗号化等がある。想定される脅威や利用環境等によってメリット・デメリットがあるため、適切な方式を選択することが望ましい。

- **遵守事項 7.2.4(1)-1「データベースの管理者」について**

  データベースの管理者は、データベースに格納されるデータの管理、アカウント・権限の管理、ネットワーク環境の構成等の管理を行う。多数の管理者特権を保持するアカウントを奪取された場合、甚大な被害を受けるおそれがあるため、重要な情報を管理するデータベースの管理者の特権を他の管理者と分掌することが望ましい。

- **遵守事項 7.2.4(1)-3「権限の不適切な付与」について**

  行政事務の遂行、データベースの運用・管理等をするに当たって不必要なデータに対するアクセス権の付与のほか、他のアカウントに対して権限を付与する権限の付与等がある。

7.3　通信回線

7.3.1　通信回線

目的・趣旨

サーバ装置や端末への不正アクセスやサービス不能攻撃等は、当該サーバ装置や端末に接続された通信回線及び通信回線装置を介して行われる場合がほとんどであることから、通信回線及び通信回線装置に対する情報セキュリティ対策については、情報システムの構築時からリスクを十分検討し、必要な対策を実施しておく必要がある。通信回線の運用主体又は物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。

また、情報システムの運用開始時と一定期間運用された後とでは、通信回線の構成や接続される情報システムの条件等が異なる場合があり、攻撃手法の変化も想定されることから、情報システムの構築時に想定した対策では十分でなくなる可能性がある。そのため、通信回線の運用時においても、継続的な対策を実施することが重要である。

遵守事項

(1) 通信回線の導入時の対策

(a) 部局技術責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた**適切な回線種別を選択**し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。

(b) 部局技術責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。

(c) 部局技術責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。

(d) 部局技術責任者は、事務従事者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。

(e) 部局技術責任者は、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。

(f) 部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。

(g) 部局技術責任者は、学内通信回線にインターネット回線、公衆通信回線等の学外通信回線を接続する場合には、学内通信回線及び当該高等教育機関内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。

(h) 部局技術責任者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視するための措置を講ずること。
(i) 部局技術責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。
(j)部局技術責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。
(k) 部局技術責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくこと。

【 基本対策事項 】

＜7.3.1(1)(a)(b)関連＞

7.3.1(1)-1 部局技術責任者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じて、以下を例とする通信経路の分離を行うこと。

a) 外部との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離する。
b) 業務目的や取り扱う情報の格付及び取扱制限に応じて情報システムごとに VLAN により通信経路を分離し、それぞれの通信制御を適切に行う。
c) 他の情報システムから独立した専用の通信回線を構築する。

＜7.3.1(1)(c)関連＞

7.3.1(1)-2 部局技術責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、SSL（TLS）、IPsec 等による暗号化を行うこと。また、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。

＜7.3.1(1)(d)関連＞

7.3.1(1)-3 部局技術責任者は、学内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずること。

a) 情報システムの機器番号等により接続機器を識別する。
b) クライアント証明書により接続機器の認証を行う。

＜7.3.1(1)(e)関連＞

7.3.1(1)-4 部局技術責任者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講ずること。

a) 通信回線装置を施錠可能なラック等に設置する。

b) 施設内に敷設した通信ケーブルを物理的に保護する。
c) 通信回線装置の操作ログを取得する。

＜7.3.1(1)(f)関連＞

7.3.1(1)-5 部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずること。

a) 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。
b) 通信回線及び通信回線装置を冗長構成にする。

＜7.3.1(1)(g)関連＞

7.3.1(1)-6 部局技術責任者は、学内通信回線に、インターネット回線や公衆通信回線等の学外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講ずること。

a) ファイアウォール、WAF（Web Application Firewall）、リバースプロキシ等により通信制御を行う。
b) 通信回線装置による特定の通信プロトコルの利用を制限する。
c) IDS/IPS により不正アクセスを検知及び遮断する。

＜7.3.1(1)(j)関連＞

7.3.1(1)-7 部局技術責任者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、以下を例とする対策を講ずること。

a) リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う。
b) 主体認証によりアクセス制御する。
c) 通信内容の暗号化により秘匿性を確保する。
d) ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにする。

（解説）

- **遵守事項 7.3.1(1)(a)「適切な回線種別を選択」について**

通信回線に利用する物理的な回線（通信事業者の回線・公衆無線 LAN 回線 等）の種別によって、盗聴、改ざん等の脅威及びそれらに対する有効なセキュリティ対策が異なることから、適切な回線を選択することが求められる。

例えば、要安定情報を取り扱う情報システムにおいて、通信経路の破壊等による可用性への影響を回避することを目的として仮想的な通信回線を複数の通信経路により構築する場合、物理的にも分離された通信経路上にそれぞれ仮想的な通信回線を構築しなければ、本来求められる可用性の維持に関する要件を満たすことにはならない。

- **遵守事項 7.3.1(1)(i)「ソフトウェアを定め」について**

通信回線装置としての機能や動作の明確化を行うとともに、ソフトウェアの脆弱性に関する対策を確実なものとするために、通信回線装置で使用するソフトウェアについて、バージョンを含めて定めておくことが望ましい。通信回線装置の更新ソフトウ

ェアの提供を受けた際に、それを無条件に適用せずに、更新内容等をあらかじめ確認し、適用する必要性を判断することが重要である。

- **遵守事項 7.3.1(1)(k)「契約時に取り決めておく」について**

  公衆通信回線サービスを使用する場合においては、回線の利用規約等に記載されているセキュリティレベルやサービスレベルを合意した上で当該回線を選択する必要がある。役務提供契約で通信回線を利用するなど、本学において直接回線を調達しない場合については、通信回線に求めるセキュリティレベル及びサービスレベルについて、役務提供事業者と合意形成する必要がある。

- **基本対策事項 7.3.1(1)-1 c)「専用の通信回線を構築」について**

  リスクを検討した結果、他の情報システムと共通的な通信回線を利用すると情報システムのセキュリティが確保できないと判断した場合には、他の通信回線から独立させて閉鎖的な通信回線とするなどの構成を採用することが考えられるが、過剰なセキュリティ要件とならないように、閉鎖的な通信回線とする必要性を見極めることが重要である。例えば、通信回線を VLAN 等で論理的に分割し、分割された論理的な通信回線ごとに情報セキュリティを確保することで十分要件を満たすのであれば、費用や維持管理の面でメリットがある。このように情報セキュリティ以外の観点とのバランスをとって要件を定めることが重要である。

- **基本対策事項 7.3.1(1)-5 b)「通信回線及び通信回線装置を冗長構成にする」について**

  高い可用性が求められる情報システムを構築する場合は、大規模災害の発生を想定し、通信回線を冗長構成にしておくことが望ましい。また、庁舎から外部に敷設する通信回線の管路についても、例えば、異なる通信事業者による複数の経路で構築しておくことで、災害を受けた際に復旧にかかる時間が短縮されるなどの効果が期待される。

遵守事項

(2) 通信回線の運用時の対策

(a) 部局技術責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずること。

(b) 部局技術責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及び**アクセス制御の設定の見直しを行う**こと。

(c) 部局技術責任者は、通信回線装置が動作するために必要な**ソフトウェアの状態を定期的に調査**し、許可されていないソフトウェアがインストールされているなど、**不適切な状態**にある通信回線装置を認識した場合には、改善を図ること。

(d) 部局技術責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。

【 基本対策事項 】

＜7.3.1(2)(a)関連＞

7.3.1(2)-1 部局技術責任者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管すること。

7.3.1(2)-2 部局技術責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。

（解説）

- **遵守事項 7.3.1(2)(b)「アクセス制御の設定の見直しを行う」について**

  アクセス制御の設定の見直しにより、設定条件を変更したり又は設定の不備を修正したりする場合は、当該通信回線に接続されている情報システムの部局技術責任者にも事前の連絡及び結果の通知が必要である。

- **遵守事項 7.3.1(2)(c)「ソフトウェアの状態を定期的に調査」について**

  通信回線の重要性、想定される脅威及び機器の特性等から調査の必要性及び調査の間隔を検討する必要がある。例えば、基幹回線等の重要な通信回線を構成する機器、ファイアウォールのようにインターネット等と直接接続されている機器、頻繁にソフトウェアがアップデートされるような機器等は調査の必要性が高く、より短期間に繰り返し調査を実施することが考えられる。また、必要性が低いと判断された機器についても、ソフトウェア等に脆弱性が報告されたり、通信回線の構成変更が発生したりする場合に随時調査することが望ましい。

- **遵守事項 7.3.1(2)(c)「不適切な状態」について**

  許可されていないソフトウェアがインストールされている場合や、定められたソフトウェアが動作するための設定が適切でないなどの状態のことを指す。

遵守事項

(3) 通信回線の運用終了時の対策

(a) 部局技術責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての**情報を抹消するなど適切な措置**を講ずること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.3.1(3)(a)「情報を抹消するなど適切な措置」について**

運用を終了した通信回線装置が再利用されたとき又は廃棄された後に、保存されていた情報が漏えいすることを防ぐための抹消の方法としては、通信回線装置の初期化、内蔵電磁的記録媒体の物理的な破壊等の方法がある。通信回線装置内にも、設定情報や通信ログ等の情報が保存されていることから、サーバ装置及び端末と同様に運用終了時に留意しておくことが必要である。

通信回線装置は通信事業者からリース提供されることがあり、その場合は通信回線の運用終了に伴い通信事業者に装置を返却することになるため、通信回線装置の初期化の手順等本項を遵守するための方法について、通信事業者に確認する必要がある。

遵守事項

(4) リモートアクセス環境導入時の対策

(a) 部局技術責任者は、**VPN 回線を整備**する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。

(b) 部局技術責任者は、事務従事者の業務遂行を目的としたリモートアクセス環境を、学外通信回線を経由して本学の情報システムへリモートアクセスする形態により構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。

【 基本対策事項 】

＜7.3.1(4)(a)関連＞

7.3.1(4)-1 部局技術責任者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。

a) 利用開始及び利用停止時の申請手続の整備
b) 通信を行う端末の識別又は認証
c) 利用者の認証
d) 通信内容の暗号化
e) **主体認証ログ**の取得及び管理
f) リモートアクセスにおいて**利用可能な公衆通信網の制限**
g) アクセス可能な情報システムの制限
h) リモートアクセス中の他の通信回線との接続禁止

＜7.3.1(4)(b)関連＞

7.3.1(4)-2 部局技術責任者は、学外通信回線を経由した本学の情報システムへのリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。

a) 利用開始及び利用停止時の申請手続の整備
b) 利用者の認証又は発信者番号による識別及び認証
c) 主体認証ログの取得及び管理
d) アクセス可能な情報システムの制限
e) リモートアクセス中の他の通信回線との接続禁止

（解説）

- **遵守事項 7.3.1(4)(a)「VPN 回線を整備」について**

VPN 回線には、IP-VPN 等の閉域網をベースとした回線とインターネット VPN 等の公衆回線網をベースとした回線があるが、どちらを整備する場合であっても通信内容の暗号化及びリモートアクセス端末（又は利用者）の認証は、必ず講じておくべき措置となる。さらに、特に機密性の高い情報を取り扱う場合においては二重の暗号化を行う（例えば、インターネット VPN 回線において IPsec で通信経路の暗号化を行った上で HTTPS 通信によりコンテンツの暗号化を行う）などを考慮してもよい。

- **基本対策事項 7.3.1(4)-1 e)「主体認証ログ」について**

  例えば MS-CHAPv2 のような、認証情報を第三者に窃取されるなどの脆弱性が認められる認証プロトコル（リモートアクセスによる利用者認証の際に汎用的に用いられるプロトコル）については、暗号化されている通信路上で認証処理を行い、認証ログを厳重に管理するなどの対策を講ずる必要がある。運用中のサーバ装置や通信回線装置の認証ログを定期的に確認するなどして、不正アクセスが行われていないことに留意することも重要である。

- **基本対策事項 7.3.1(4)-1 f)「利用可能な公衆通信網の制限」について**

  リモートアクセスの際に足回りの回線として使用する通信回線については、安全な通信回線サービスに限定することが望ましいが、海外で利用する場合等においては、利用可能な通信回線サービスが限られており、通信回線サービスを制限できない。このような場合は、「通信回線サービスを限定しない」という前提条件のもと、通信回線サービスの安全性や信頼性に関わらず、取り扱われる情報のセキュリティが確保されるよう、VPN 接続時の認証処理及び通信内容の暗号化等の対策を考慮する必要がある。

遵守事項

(5) 無線 LAN 環境導入時の対策

(a) 部局技術責任者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。

【 基本対策事項 】

＜7.3.1(5)(a)関連＞

7.3.1(5)-1 部局技術責任者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、以下を例とする対策を講ずること。

a) SSID の隠ぺい

b) 無線 LAN 通信の暗号化

c) MAC アドレスフィルタリングによる端末の識別

d) 802.1X による無線 LAN へのアクセス主体の認証

e) 無線 LAN 回線利用申請手続の整備

f) 無線 LAN 機器の管理手順の整備

g) 無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対処手順の整備

（解説）

- **基本対策事項 7.3.1(5)-1 b)「無線 LAN 通信の暗号化」について**

暗号化方式として、例えば WPA2 Enterprise（Wi-Fi Protected Access 2 Enterprise）方式を選択することが考えられる。WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信を妨害できたりするという脆弱性が報告されており、利用すべきではない。他の暗号化方式においても同様の問題が起こる可能性があるため、最新の情報に従い適切な方式や設定値を選択することが求められる。

- **基本対策事項 7.3.1(5)-1 f)「無線 LAN 機器の管理」について**

無線 LAN 機器の管理については、例えば、以下が考えられる。

- 無線 LAN 機器の電波出力・周波数チャンネル等の管理
- 管理外の無線 LAN アクセスポイント、端末の検出及び除去

なお、無線 LAN 回線を構築する場合は、政府機関から公表している以下の研究会報告書等を参考にするとよい。

参考：総務省「国民のための情報セキュリティサイト」の「情報管理担当者のための情報セキュリティ対策」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/index.html）にある、「安全な無線 LAN 利用の管理」のページの解説

参考：各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告
「無線 LAN セキュリティ要件の検討」（平成 23 年 3 月）
（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf）

参考：総務省「無線 LAN ビジネス研究会」報告書（平成 24 年 7 月 20 日）
（http://www.soumu.go.jp/menu_news/s-news/02kiban04_03000093.html）

参考：総務省「無線 LAN ビジネスガイドライン」（平成 25 年 6 月 25 日）
（http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000058.html）

- **基本対策事項 7.3.1(5)-1 g)「不正プログラム感染を認知した場合の対処手順」について**

本学 LAN 端末が不正プログラムに感染した場合は、通常は通信ケーブルを抜去するといった手順が設けられていることが多いが、無線 LAN 回線を使用している場合においては、不正プログラムに感染した端末が無線 LAN 回線を介して他の端末に感染を拡大しないように、無線 LAN 通信を遮断するための手順をあらかじめ定め、事務従事者へ周知しておく必要がある。例えば、以下の手順が考えられる。

- 感染を認知した際に電磁波を遮断するシールドボックスに感染端末を隔離する。
- 無線 LAN の通信圏外へ端末を移動し、保管する。
- 端末の無線 LAN 通信機能を停止する。

7.3.2 IPv6 通信回線

目的・趣旨

本学において、インターネットの規格である IPv6 通信プロトコルに対応するための取組が進められているが、IPv6 通信プロトコルを採用するに当たっては、グローバル IP アドレスによるパケットの直接到達性や IPv4 通信プロトコルから IPv6 通信プロトコルへの移行過程における共存状態等、考慮すべき事項が多数ある。

近年では、サーバ装置、端末及び通信回線装置等に IPv6 技術を利用する通信（以下「IPv6 通信」という。）を行う機能が標準で備わっているものが多く出荷され、運用者が意図しない IPv6 通信が通信ネットワーク上で動作している可能性があり、結果として、不正アクセスの手口として悪用されるおそれもあることから、必要な対策を講じていく必要がある。

なお、IPv6 技術は今後も技術動向の変化が予想されるが、一方で、IPv6 技術の普及に伴い情報セキュリティ対策技術の進展も期待されることから、本学においても、IPv6 の情報セキュリティ対策に関する技術動向を十分に注視し、適切に対応していくことが重要である。

遵守事項

(1) IPv6 通信を行う情報システムに係る対策

(a) 部局技術責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択すること。

(b) 部局技術責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

（ア） グローバル IP アドレスによる直接の到達性における脅威

（イ） IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

（ウ） IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

（エ） アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.3.2(1)(b)（ア）「グローバル IP アドレスによる直接の到達性における脅威」について**

IPv6 通信を想定して構築する情報システムにおいて、グローバル IP アドレスによる通信パケットの直接到達性における脅威に対抗するために、以下を例に対策を講ずることが考えられる。

- 不正な機器からの経路調査コマンド（traceroute 等）への応答の禁止
- ICMP エコー要求への応答の禁止
- 許可した宛先からのみアクセス可能とするなどの経路制御の設定
- サービス不能攻撃の検知及びフィルタ

- **遵守事項 7.3.2(1)(b)(イ)「不正アクセスの脅威」について**

IPv6 の特徴として、アドレスが長いこと、アドレスの省略形が複数パターン存在して一意に定まらない可能性があること、端末が複数の IP アドレスを持つこと等が挙げられる。このため、複雑なアクセス制御の設定が必要になり、設定不備等による不正アクセスにつながるリスクが想定される。

対策としては、外部ネットワークとの通信において、OSI 基本参照モデルのネットワーク層（第３層）及びトランスポート層（第４層）を中心にフィルタリングを行う機能及び断片化された通信の再構築を行う機能を適切に設定すること等、通信機器を流れる通信そのものを制御することが挙げられる。

なお、IPv6 通信を想定して構築する情報システムにおいて、IPv6 のログを取得し、分析する場合は、IPv6 アドレスでは桁数が大幅に増えること等から、IPv6 対応のログの解析ツールを利用することで、IPv6 アドレスの読み間違い等の運用上の作業ミスを軽減するための対策を検討することが望ましい。

- **遵守事項 7.3.2(1)(b)(ウ)「共存させる際の処理考慮漏れに起因する脆弱性」について**

IPv6 通信プロトコルに対応している端末やサーバ装置には、多様な IPv6 移行機構（デュアルスタック機構、IPv6-IPv4 トンネル機構等）が実装されている。それらの IPv6 移行機構は、それぞれが想定する使用方法と要件に基づき設計されていることから、その選定と利用に当たっては、セキュリティホールの原因をつくらないよう十分な検討と措置が必要である。

例えば、デュアルスタック機構を運用する場合には、IPv4 のプライベートアドレスを利用したイントラネットの情報システムであっても外部ネットワークとの IPv6 通信が可能となるため、デュアルスタック機構を導入したサーバ装置及び端末を経由した当該外部ネットワークからの攻撃について対策を講ずる必要がある。また、IPv6-IPv4 トンネル機構を運用する場合、トンネルの終端が適切に管理されないと本来通信を想定しないネットワーク間の IPv6 通信が既設の IPv4 ネットワークを使って可能となるため、本学のネットワークが外部から攻撃される危険性がある。管理されたサーバ装置及び端末以外のトンネル通信を当該 IPv4 ネットワークに設置されたファイアウォールにて遮断するなど、不適切な IPv6 通信を制御する対策が必要である。

- **遵守事項 7.3.2(1)(b)(エ)「IPv6 アドレスの取扱い考慮漏れに起因する脆弱性」について**

IPv4 のみに対応する機器及びソフトウェアが IPv6 ネットワーク上で動作する際、システム内部での IP アドレスの取扱いが IPv4 に依存している場合、IPv6 アドレスが取り扱えない、若しくはバッファオーバーラン等を引き起こす可能性があるというリスクを認識し、これが無いことを確認するなどが挙げられる。統合認証システムや、

システム間連動を行うようなアプリケーションでは、IPv4/IPv6 が混在した状況でも適切なシステム連携を行う必要がある。

また、「IPv4 対応システムが IPv6 アドレスに対応するため、IPv6／IPv4 コンバータ等が使用される場合がある。このような場合、内部からは個別の IPv6 アドレスを特定できないため、通信ログの取得やパケットフィルタリング等の機能を実装し運用する際等において留意する必要がある。

遵守事項

(2) 意図しない IPv6 通信の抑止・監視

(a) 部局技術責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、**IPv6 通信を抑止するなどの措置**を講ずること。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 7.3.2(2)(a)「IPv6 通信を抑止するなどの措置」について**

本学キャンパスの拠点間及び学内のみで利用する情報システムについて、通信回線が IPv6 通信を想定していない場合には、当該通信回線に接続される端末等の IPv6 通信の機能を停止する必要がある。

IPv6 通信を想定していない通信回線においては、ファイアウォールや IDS/IPS 等のセキュリティ機能に不正な IPv6 通信を制御する措置が講じられず、悪意ある者による IPv6 通信を使った攻撃に対して無防備となるおそれがある。さらに、IPv6 通信が可能なサーバ装置及び端末においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該サーバ装置及び端末への接続を可能とする自動トンネリング機能を提供するものがある。この機能を利用すると、サーバ装置及び端末と外部のネットワークとの間に情報システムの利用者や情報システムの運用管理者が気付かないうちに意図しない経路が自動生成され、これがセキュリティを損なうバックドアとなりかねないことから、自動トンネリング機能を動作させないようサーバ装置及び端末を設定する必要がある。また、ルータ等の通信回線装置についても IPv6 通信をしないよう設定し、意図しない IPv6 通信を制限することが求められる。

なお、「政府情報システムに係る IPv6 対応の取組について」（2011 年 11 月 2 日各府省情報化統括責任者（CIO）連絡会議決定）において IPv6 対応の取組を進めることが確認されているが、外部と直接通信を行う情報システム等についても、現時点において IPv6 対応がされていない場合には、意図しない IPv6 通信を抑止又は遮断するための措置を講ずることが必要である。

第8部 情報システムの利用

8.1 情報システムの利用

8.1.1 情報システムの利用

目的・趣旨

事務従事者は、業務の遂行のため、端末での事務処理のほか電子メール、ウェブ等様々な情報システムを利用している。これらを適切に利用しない場合、情報セキュリティインシデントを引き起こすおそれがある。

このため、情報システムの利用に関する規定を整備し、事務従事者は規定に従って利用することが求められる。

遵守事項

(1) 情報システムの利用に係る規定の整備

(a) 全学実施責任者は、本学の情報システムの利用のうち、情報セキュリティに関する規定を整備すること。

(b) 全学実施責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。

(c) 全学実施責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。

【 基本対策事項 】

＜8.1.1(1)(a)関連＞

8.1.1(1)-1 全学実施責任者は、本学の情報システムの利用のうち、情報セキュリティに関する規定として、以下を例とする実施手順を定めること。

a) 情報システムの基本的な利用のうち、情報セキュリティに関する手順
b) 電子メール及びウェブの利用のうち、情報セキュリティに関する手順
c) 識別コードと主体認証情報の取扱手順
d) 暗号と電子署名の利用に関する手順
e) 不正プログラム感染防止の手順
f) アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為の防止に関する手順
g) ドメイン名の使用に関する手順

＜8.1.1(1)(b)関連＞

8.1.1(1)-2 全学実施責任者は、要管理対策区域外にて情報処理を行う際の安全管理措置と

して、以下を例とする措置を規定し、事務従事者に遵守させること。
a) モバイル端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化
b) 盗み見に対する対策（のぞき見防止フィルタの利用等）
c) **盗難・紛失に対する対策**（不要な情報をモバイル端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）
d) 利用する場所や時間の限定
e) 端末及び外部電磁的記録媒体等についての盗難・紛失が発生した際の緊急対応手順

8.1.1(1)-3 全学実施責任者は、要管理対策区域外にて事務従事者が情報処理を行う際の許可等の手続として、以下を例とする手続を規定し、事務従事者に遵守させること。
a) 許可権限者の決定（部局技術責任者又は職場情報セキュリティ責任者が想定される。）
b) 利用時の許可申請手続
c) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線の接続形態等）
d) **利用期間満了時の手続**
e) 許可権限者による手続内容の記録

＜8.1.1(1)(c)関連＞

8.1.1(1)-4 全学実施責任者は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順として以下の事項を含めて定めること。
a) 本学支給の外部電磁的記録媒体を使用する（私物や**出所不明の媒体**を使用しない）。
b) 主体認証機能や暗号化機能を備える**セキュアな外部電磁的記録媒体**が存在する場合、これに備わる機能を利用する。
c) 要機密情報は保存される必要がなくなった時点で速やかに削除する。
d) 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行う。

（解説）

- **遵守事項 8.1.1(1)(c)「USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順」について**

USB メモリ等の外部電磁的記録媒体に関する対策は、情報システムの構成等によって様々であると考えられるが、基本対策事項 8.1.1(1)-4 及び「【参考 8.1.1-1】USB メモリ等の外部電磁的記録媒体について」を参照しつつ、①端末等の不正プログラム感染、②盗難・紛失等による情報漏えい、③バックドアの埋め込み等のサプライチェーン・リスク、といった脅威に対抗するための利用手順を定める必要がある。また、事務従事者は当該手順に従う必要がある（遵守事項 3.1.1(4)(e)を参照のこと。）。

なお、USB メモリ等の外部電磁的記録媒体の管理に際しては、利用手順の整備のほ

か、組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入も有効である（基本対策事項 6.2.4(1)-2 f)を参照のこと。）。

- **基本対策事項 8.1.1(1)-1「以下を例とする実施手順を定める」について**

a)～e)は、それぞれ遵守事項 8.1.1(3)～(7)において、事務従事者を名宛人とした対策事項が規定されている。同様に、f)は遵守事項 6.3.1(1)において、また、g)は遵守事項 6.3.2(1)において対策事項が規定されている。本項では、これら規定内容を包含する形で、本学の実施手順等を定めることを求めている。

なお、統一基準及び本ガイドラインの規定内容を、事務情報セキュリティ対策基準に含めて定めることで代替しても差し支えない。

- **基本対策事項 8.1.1(1)-2 c)「盗難・紛失に対する対策」について**

一般的に、以下に例を挙げる状況では、盗難・紛失が発生しやすいため、要機密情報を含むモバイル端末を携行する場合には十分注意させること。

  - 電車等での移動中に、モバイル端末の入ったかばん等を網棚に置き、そのまま下車する。
  - 飲酒が想定されるいわゆる宴会等でモバイル端末の入ったかばん等を置いたまま帰宅する。

- **基本対策事項 8.1.1(1)-3 d)「利用期間満了時の手続」について**

利用期間満了時の際は、事務従事者に報告を求めるよう手続に定める必要がある。特に機密性３情報等の取扱いに注意すべき情報を要管理対策区域外に持ち出す場合においては、以下を例とする管理手順を設けるとよい。

  - 利用期間満了時の連絡が無い場合は、当該利用者に確認する。
  - 利用期間の延長が必要であれば、再手続を要請する。
  - 利用期間満了前に利用が終了した際には、利用終了時に報告を求める。

- **基本対策事項 8.1.1(1)-4 a)「出所不明の媒体」について**

USB デバイスの設計上の脆弱性を悪用するなどして、USB デバイスのファームウェアを不正に書き換えることによる攻撃手法が確認されている。

例えば、悪意のある者が、端末を不正プログラムに感染させることを目的に USB メモリのファームウェアを書き換え、当該 USB メモリを攻撃対象者や不特定多数の者等に配ることが考えられる。当該 USB メモリは、USB ポートに挿入されると不正プログラムを自動的に実行し、端末が不正プログラムに感染してしまう。

このようなファームウェアを書き換えられた USB デバイスは、不正プログラム対策ソフトウェアでは検出できない場合もあることから、出所不明の USB デバイスの使用は慎むべきである。

- **基本対策事項 8.1.1(1)-4 b)「セキュアな外部電磁的記録媒体」について**

「（解説）基本対策事項 3.1.1(6)-2 c)「本学支給のセキュアな製品」について」を参照のこと。

【参考 8.1.1-1】USB メモリ等の外部電磁的記録媒体について

USB メモリ等の外部電磁的記録媒体に関連する脅威（①②③）及び脆弱性（箇条書き）としては、以下が想定される。

① 端末等の不正プログラム感染
- 利用者、用法等が不明な物が使用されている。
- 外部電磁的記録媒体を接続した際に自動的にプログラムが実行される。
- 不正プログラム対策ソフトウェアによる検疫・駆除を行っていない。

② 盗難・紛失等による情報漏えい
- 利用者、用法等が不明な物が使用されている。
- 運搬の際等に暗号化等の安全管理措置がなされていない。
- 不要な要機密情報が保存されている。

③ バックドアの埋め込み等のサプライチェーン・リスク
- 製造元、製造過程が不明な物が使われる。

上記の脅威及び脆弱性に対しては、表 8.1.1-1 に掲げる対策が想定される。

表 8.1.1-1　USB メモリ等の外部電磁的記録媒体に関する対策の例

脅威	対策	対策の種類	関連する基本対策事項
①不正プログラム感染	主体認証機能や暗号化機能を備える外部電磁的記録媒体を導入する	調達時の対策	5.2.1(2)関連
	不正プログラムの検疫・駆除機能を備える外部電磁的記録媒体を導入する	調達時の対策	5.2.1(2)関連
	情報を暗号化するための機能を備えたソフトウェアを導入する	調達時の対策	5.2.1(2)関連 6.1.5 関連
	外部電磁的記録媒体の検疫・駆除機能を備える不正プログラム対策ソフトウェアを導入する	調達時の対策	6.2.1(1)関連
	サーバ装置及び端末の自動再生（オートラン）機能を無効にする	技術的な設定	6.2.4(1)-1 c)
	サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする	技術的な設定	6.2.4(1)-1 d)
	サーバ装置及び端末において使用を想定しない USB ポート等を無効にする	技術的な設定	6.2.4(1)-1 e)
	外部電磁的記録媒体の使用前に、不正プログラム対策ソフトウェアや外部電磁的記録媒体に備わる機能による不正プログラムの検疫・駆除を行う	利用時の対策	8.1.1(1)-4 d) 8.1.1(7)関連

②情報漏えい	運搬の際等に主体認証機能や暗号化機能の利用等の安全管理措置を講ずる	利用時の対策	3.1.1(6)-2 c) 8.1.1(1)-4 b)
	要機密情報は保存される必要がなくなった時点で速やかに削除する	利用時の対策	8.1.1(1)-4 c)
③サプライチェーン・リスク	安全と考えられる製造元、製造過程の製品を調達する	調達時の対策	5.1.2 関連
①②③共通	使用可能な媒体の制限や利用方法等に関する手順を定める	管理対策	8.1.1(1)-4
	組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する	管理対策 調達時の対策	6.2.4(1)-2 f) 8.1.1(1)-4
	管理下に置かれた外部電磁的記録媒体を使用する（私物や出所不明の外部電磁的記録媒体を使用しない）	利用時の対策	8.1.1(1)-4 a)

遵守事項

(2) 情報システム利用者の規定の遵守を支援するための対策

(a) 部局技術責任者は、事務従事者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。

【 基本対策事項 】

＜8.1.1(2)(a)関連＞

8.1.1(2)-1 部局技術責任者は、学外のウェブサイトについて、事務従事者が閲覧できる範囲を制限する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

a) ウェブサイトフィルタリング機能

b) 事業者が提供するウェブサイトフィルタリングサービスの利用

8.1.1(2)-2 部局技術責任者は、事務従事者が不審なメールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

a) 受信メールに対するフィルタリング機能

b) 受信メールをテキスト形式で表示する機能

c) スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがないメールクライアントの導入

d) 受信メールに添付されている実行プログラム形式のファイルを削除することで実行させない機能

（解説）

- **遵守事項 8.1.1(2)(a)「事務従事者による規定の遵守を支援する機能」について**

事務従事者が事務情報セキュリティ対策基準に定めた規定を守ることを前提としつつ、情報システムの仕組みとして、情報セキュリティインシデントが発生しにくい利用環境を事務従事者に提供することにより、組織全体のセキュリティ水準を確保することを求める事項である。例えば、基本対策事項に示したとおり、閲覧するとウイルス感染被害に遭うことが判明しているサイトや受信した電子メールをフィルタリングして閲覧不可にすることで被害を回避するなどが考えられる。

これ以外にも、例えば、事務従事者が意図しない相手に電子メールを送信することをシステム的に抑止する対策として以下のような機能を情報システムに導入すること等も考えられる。

- 送信者のメールアドレスのドメイン名以外のドメインのアドレスが宛先アドレスに含まれる場合に警告を表示するなど、入力された宛先アドレスをチェックして警告する機能
- To、Cc、Bcc に入力された宛先アドレスの数が設定数以上になっているときに

警告する機能
- 添付ファイルがある場合に警告する機能
- 送信メールの件名、本文、添付ファイルにあらかじめ設定した文字列が含まれる場合に警告する機能
- 送信者が送信指示を行った後、あらかじめ設定された時間だけ送信を保留することにより、送信者が誤送信に気が付いた場合に、送信を取り消すことができる機能

- **基本対策事項 8.1.1(2)-2 b)「テキスト形式で表示する機能」について**

いわゆるフィッシング等の脅威が想定される外部からの電子メールを受信する情報システムを対象とした規定である。HTML 形式の電子メールは、その形式の特徴が悪用され、本文中の URL を偽装した電子メールを送ることにより、フィッシング行為や不正プログラムを埋め込んだウェブサイトへの誘引行為に利用されている。フィッシング等の被害に遭うリスクが想定される場合には、テキスト形式や RTF(Rich Text Format)形式等の URL 偽装のリスクの無い形式で表示することが望ましい。

- **基本対策事項 8.1.1(2)-2 d)「実行プログラム形式のファイルを削除等する」について**

実行プログラム形式のファイルとは、利用者がダブルクリックするなどしてファイルを開いたときに自動的にプログラムコード（当該ファイルの作成者が意図した任意のコード）が実行される形式のファイルのことであり、拡張子が「.exe」の形式のものがこれに該当するほか、「.pif」、「.scr」、「.bat」等のものも該当する。実行プログラム形式のファイルは、不正プログラムを感染させる手段として標的型攻撃等に悪用されることが多いことから、特に電子メールに添付された実行プログラム形式のファイルについては、行政事務従事者がこれを開くことができないよう、システム的に抑止する機能を導入することを基本対策事項としている。ファイルを削除等する機能の例としては、電子メールの中継サーバにおいて、中継する電子メールの全てを検査して、実行プログラム形式のファイルが添付ファイルとして含まれている場合にはその添付ファイルを削除する機能が挙げられるほか、中継サーバでの削除に代えて、電子メールを受信した端末側で該当する添付ファイルを開けないようにする機能等が想定される。

また、実行プログラム形式のファイルは、「.zip」、「.lzh」等の圧縮形式のファイルの内部に含められることがあり、行政事務従事者が圧縮形式のファイルを展開し、展開後に現れる実行プログラム形式のファイルを開いてしまうことにより、不正プログラムに感染する事態も想定されることから、圧縮形式のファイルの内部に含められた実行プログラム形式のファイルも削除等の対象とする必要がある。

なお、パスワードを用いて暗号化された圧縮形式のファイルについては、当該ファイル中に実行プログラム形式のファイルが含まれるか否かを技術的に検査できないことから、そのような場合は、暗号化された圧縮形式のファイル自体を添付ファイルから削除等する機能の導入を考慮する必要がある。圧縮形式のファイル中のファイルの検査をする機能を導入する代わりに、暗号化の有無にかかわらず圧縮形式のファイルのすべてを削除等する措置を用いてもよい。

これらファイル削除等の機能の導入は、行政事務従事者に一定の不便をもたらすことになり得るが、これを実施せず、開いてよいファイルか否かを行政事務従事者に添付ファイルの拡張子を個々に確認させる方法を代用策とした状態では、標的型攻撃等を企図した電子メールの添付ファイルを誤って開いてしまう危険性を十分に抑制することは困難であることから、これをシステム的に抑止する機能の導入が推奨される。

遵守事項

(3) 情報システムの利用時の基本的対策

(a) 事務従事者は、高等教育機関の事務の遂行以外の目的で情報システムを利用しないこと。

(b) 事務従事者は、部局技術責任者が接続許可を与えた通信回線以外に本学の情報システムを接続しないこと。

(c) 事務従事者は、学内通信回線に、部局技術責任者の接続許可を受けていない情報システムを接続しないこと。

(d) 事務従事者は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、部局技術責任者の承認を得ること。

(e) 事務従事者は、接続が許可されていない機器等を情報システムに接続しないこと。

(f) 事務従事者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。

(g) 事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。

(h) 事務従事者は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、部局技術責任者又は職場情報セキュリティ責任者の許可を得ること。

【 基本対策事項 】

＜8.1.1(3)(e)関連＞

8.1.1(3)-1 事務従事者は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下を例とする措置を講ずること。

a) スクリーンロックの設定

b) 利用後のログアウト徹底

c) 利用後に情報システムを鍵付き保管庫等に格納し施錠

（解説）

- **遵守事項 8.1.1(3)(a)「高等教育機関の事務の遂行以外の目的で情報システムを利用しない」について**

  高等教育機関の事務の遂行以外の目的で情報システムを利用した場合の脅威を回避するための規定である。脅威の例としては、意図せず悪意のあるウェブサイトを閲覧することによって、不正プログラムに感染することが想定される。

- **遵守事項 8.1.1(3)(b)「接続許可を与えた通信回線以外」について**

  適切な管理がなされていない通信回線に端末を接続することにより、通信傍受等の

脅威にさらされることを回避するための規定である。

学内通信回線であっても学外通信回線であっても、許可を得ていない通信回線に接続してはならない。モバイル端末を持ち出した際に接続する通信回線については、学内通信回線以外の利用となり、盗聴等の脅威が増大することから、許可されていない通信回線への接続は回避すべきである。ただし、出張先等で利用する通信回線が未定の場合は、事前の許可が難しいことから、回線の種別（通信事業者の回線・公衆無線LAN回線等）で管理すること等も考えられる。

- **遵守事項 8.1.1(3)(c)「接続許可を受けていない情報システム」について**

学内通信回線を保護するための対策である。私物の端末等、利用を許可されていないサーバ装置、端末等を学内通信回線に接続することを禁止している。

- **遵守事項 8.1.1(3)(d)「部局技術責任者の承認を得る」について**

事務従事者が、利用を認めるソフトウェア以外のソフトウェアを利用する必要がある場合に、部局技術責任者に利用を申請し承認を得ることを求める規定である。

なお、承認を得る際には、製品名、バージョン、入手方法（ソフトウェアの入手元となるURL、事業者名等）、入手可能な場合には利用規約等を添付して、部局技術責任者に申請することが望ましい。

- **遵守事項 8.1.1(3)(e)「接続が許可されていない機器等」について**

出所不明のUSBデバイスやセキュリティ管理が不十分な私物のスマートフォン等が情報システムに接続されることが許容されていると、不正プログラム感染等のリスクが高まることから、情報システムへ接続可能な機器等（又は接続を禁止する機器等）をあらかじめ定めておくとよい。

「（解説）基本対策事項 8.1.1(1)-4 a)「出所不明の媒体」について」も参照のこと。

- **遵守事項 8.1.1(3)(g)「定められた安全管理措置」について**

遵守事項 8.1.1(1)「情報システムの利用に関する規定の整備」において全学実施責任者が定めた安全管理措置の実施を求めている。取り扱う情報の格付や取扱制限に応じた、適切な安全管理措置が求められる。

- **遵守事項 8.1.1(3)(h)「許可を得る」について**

遵守事項 8.1.1(1)「情報システムの利用に関する規定の整備」において全学実施責任者が定めた許可手続の実施を求めている。情報システムの利用開始時の許可申請だけではなく、利用期間満了時又は利用終了時の手続等を定めている場合があるので、定められた手順に従って、適切に措置する必要がある。

遵守事項

(4) 電子メール・ウェブの利用時の対策

(a) 事務従事者は、要機密情報を含む電子メールを送受信する場合には、本学が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。

(b) 事務従事者は、学外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に A 大学ドメイン名を使用すること。ただし、本学外の者にとって、当該事務従事者が既知の者である場合は除く。

(c) 事務従事者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。

(d) 事務従事者は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。

(e) 事務従事者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

(f) 事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。

（ア） 送信内容が暗号化されること

（イ） 当該ウェブサイトが送信先として想定している組織のものであること

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.1.1(4)(a)「送受信」について**

「送受信」には電子メールの「転送」が含まれる。したがって、本学支給以外の電子メールサービスの電子メールアドレスに要機密情報を含む電子メールを転送することは、許可を得ている場合を除き、認められない。特に、自動転送については、許可を受けている場合であっても、当該電子メールに含まれる情報の格付及び取扱制限にかかわらず行われるため、遵守事項 3.1.1(6)「情報の運搬又は送信」に規定されている要機密情報の送信についての遵守事項に違反しないように留意する必要がある。

- **遵守事項 8.1.1(4)(c)「不審な電子メール」について**

「不審な電子メール」とは、受信する覚えのない電子メールであって、電子メール本文中に URL が記載されているもの、実行形式や文書形式のファイルが添付されているもの等が該当する。こういった電子メールについて、むやみに URL のリンク先や添付ファイルを開かないことも重要であるが、開かなかった場合でも他の者が同種の電子メールを受信することも考えられるため、情報提供を行うことも重要である。定められた連絡先としては、CSIRT や当該電子メールを扱う情報システムの部局技術責任者等が考えられる。

- **遵守事項 8.1.1(4)(d)「情報セキュリティに影響を及ぼすおそれのある設定変更を行わない」について**

  例えば、以下のようなブラウザのセキュリティ設定項目について、変更すると悪意のあるソフトウェアが端末において実行されること等により、情報の漏えいや、他のサーバ装置及び端末を攻撃することを引き起こすことも考えられるため、変更が可能であったとしても勝手に変更しないようにする必要がある。

  ＜ブラウザのセキュリティ設定項目の例＞
  - ActiveX コントロールの実行
  - Java の実行

- **遵守事項 8.1.1(4)(f)「送信内容が暗号化されること」について**

  主体認証情報等を入力して送信する場合には、ブラウザの鍵アイコンの表示を確認するなどにより、TLS（SSL）等の暗号化通信が使用され、要機密情報が適切に保護されることを確認することを求める事項である。

  なお、「閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合」とは、例えばウェブメール本文の入力欄に要機密情報を入力すること等を指す。

- **遵守事項 8.1.1(4)(f)「当該ウェブサイトが送信先として想定している組織のものであること」について**

  ブラウザで主体認証情報等を入力して送信する場合には、ウェブサーバの電子証明書の内容から当該ウェブサイトが想定している組織のものであることを確認するなどの方法により、適切でない送信先に当該情報を誤って送信することを回避する必要がある。

  なお、ウェブサイトの閲覧時にウェブサーバの電子証明書が適切でない旨の警告ダイアログが表示された場合には、当該ウェブサイトがなりすましに利用されている可能性があるため、利用を中止する必要がある。

  近年において被害が広がっている「フィッシング(Phishing)」と呼ばれる悪質な行為に対しても十分警戒する必要がある。フィッシングは、悪意ある第三者等が、実在する機関等からのお知らせであるかのように偽装した電子メールを送りつけ、受け取った者にその電子メールに記載された URL をクリックさせ、あらかじめ用意された偽のウェブサイトに誘導し、ID、パスワード、その他重要な情報を記入させて、情報を窃取するという行為である。このようなフィッシングの被害を避けるためにも、本項で示す対策を実施することが重要である。

遵守事項

(5) 識別コード・主体認証情報の取扱い

(a) 事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。

(b) 事務従事者は、自己に付与された識別コードを適切に管理すること。

(c) 事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。

(d) 事務従事者は、自己の主体認証情報の管理を徹底すること。

【 基本対策事項 】

＜8.1.1(5)(b)関連＞

8.1.1(5)-1 事務従事者は、自己に付与された識別コードを適切に管理するため、以下を含む措置を講ずること。

a) 知る必要のない者に知られるような状態で放置しない。

b) 他者が主体認証に用いるために付与及び貸与しない。

c) 識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止する。

＜8.1.1(5)(d)関連＞

8.1.1(5)-2 事務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。

a) 自己の主体認証情報を他者に知られないように管理する。

b) 自己の主体認証情報を他者に教えない。

c) 主体認証情報を忘却しないように努める。

d) 主体認証情報を設定するに際しては、容易に推測されないものにする。

e) 異なる識別コードに対して、共通の主体認証情報を用いない。

f) 異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない。（シングルサインオンの場合を除く。）

g) 部局技術責任者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更する。

8.1.1(5)-3 事務従事者は、所有による主体認証情報を用いる場合には、以下の管理を徹底すること。

a) 主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する。

b) 主体認証情報格納装置を他者に付与及び貸与しない。

c) 主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する。

d) 主体認証情報格納装置を利用する必要がなくなった場合には、これを部局技術責任者に返還する。

（解説）

- **遵守事項 8.1.1(5)(a)「自己に付与された識別コード以外の識別コード」について**

  自己に付与された識別コード以外の識別コードを使って、情報システムを利用することは、合理的な理由が無い限り「なりすまし行為」である。仮に、悪意がなくても、他者の識別コードを使って情報システムを利用することは、許容されてはならない。例えば、何らかの障害により自己の識別コードの使用が一時的に不可能になった場合には、まず、当該情報システムを利用して行おうとしている業務について、他者へ代行処理を依頼することを検討すべきであり、仮に他者の許可を得たとしても、他者の識別コードを使用することはあってはならない。要するに、行為が正当であるか否かにかかわらず、他者の識別コードを使って、情報システムを利用するということは制限されなければならない。

  業務の継続のために、他者の識別コードを使うことが不可避の場合には、例外措置の手続を行う際に本人の事前の了解に加えて、部局技術責任者の承認を得ることが最低限必要である。また、他者の識別コードを使用していた期間とアクセスの内容を、事後速やかに、部局技術責任者に報告しなければならない。部局技術責任者は、その理由と使用期間を記録に残すことによって、事後に当該識別コードを実際に使用していた者を特定できるように備えることが望ましい。

  いずれの場合も、使用する識別コードの本人からの事前の許可を得ずに、その者の識別コードを使って、情報システムを利用することは禁止されるべきである。

- **遵守事項 8.1.1(5)(c)「管理者としての業務遂行時に限定して」について**

  例えば、情報システムの OS が Windows であれば、管理者権限なしの識別コードと管理者権限ありの識別コードの両方を付与された場合において、端末の設定変更等の管理者権限が必要な操作をしないときには、管理者権限なしの識別コードを使用し、その一方、管理者権限が必要な操作をするときに限って管理者権限を使用するなどの運用が考えられる。

- **基本対策事項 8.1.1(5)-1 a)「知る必要のない者に知られるような状態で放置しない」について**

  多くの場合、識別コード単体は必ずしも秘密ではないが、必要以上の範囲に開示する、又は公然となるような状態で放置しないように求めている。

  主体認証には、識別コードと主体認証情報の組合せが用いられる。識別コードの開示範囲を必要最小限に止めることによって、第三者が不正に主体認証を行う可能性をより低くすることができる。そのため、識別コードを適切に管理することが必要である。

- **基本対策事項 8.1.1(5)-1 b)「他者が主体認証に用いるために付与及び貸与しない」について**

  部局技術責任者が明示的に共用識別コードとしているもの以外の識別コードを共用してはならない。

- **基本対策事項 8.1.1(5)-1 c)「定められた手続に従い、識別コードの利用を停止する」について**

  識別コードを使用する必要がなくなった場合に、事務従事者自らが部局技術責任者へ届け出ること等、定められた手続に従い、識別コードを使用できない状態に変更することを求めている。ただし、例えば、人事異動等によって、事務従事者の識別コードが大規模に変更となる場合や、その変更を部局技術責任者が事務従事者自らからの届出によらず把握できる場合等、事務従事者自らの届出が不要となる条件を部局技術責任者が定めてもよい。

- **基本対策事項 8.1.1(5)-2 a)「自己の主体認証情報を他者に知られないように管理する」について**

  例えば、以下に挙げる他者からのパスワード窃取行為に注意する必要がある。

  - パスワードを入力する際に他者が周囲から盗み見する。
  - 他者が管理者を名乗ってパスワードを聞き出す。

  また、以下に挙げる行為は行うべきではない。

  - 自己のパスワードを、内容が分かる状態で付箋等に記入してモニタ、端末本体、及びその周辺に貼付する。
  - 自己のパスワードを、特段の保護をせずに平文のままテキスト形式で保存する。など、容易に他者に知られてしまう状態で、情報システム上に記録する。

- **基本対策事項 8.1.1(5)-2 b)「自己の主体認証情報を他者に教えない」について**

  たとえ、他者に処理を代行させる目的であっても、事務従事者は自己の主体認証情報を他者に教示してはならない。主体認証情報を他者に教示することによって、情報システムの識別コードと実際の操作者との関係が曖昧になり、アクセス制御、権限管理、ログ管理その他のセキュリティ対策が効果を失う可能性がある。また、教示された者にとっても、例えば、当該識別コードによって不正行為が発生した場合は、その実行者として疑義を受ける可能性がある。そのため、自己の主体認証情報は他者に「教えない」ことを徹底すべきである。

- **基本対策事項 8.1.1(5)-2 c)「主体認証情報を忘却しないように努める」について**

  他者が容易に見ることができないような措置（施錠して保存するなど）や、他者が見ても分からないような措置（独自の暗号記述方式等）をしていれば、必ずしも、メモを取る行為を禁ずるものではない。むしろ、忘れることのないように努めなければならない。

  なお、本人の忘却によって主体認証情報を初期化（リセット）する場合には、初期化が不正に行われたり、初期化された情報が本人以外に知られたりすることのないように情報システムを構築・運用することが望ましい。例えば、情報システムによる自動化により無人で初期化できるようにすることが、初期化情報の保護のみならず、運用の手間を低減することに役立つことについても勘案して検討すること等が考えられる。

- **基本対策事項 8.1.1(5)-2 d)「容易に推測されないもの」について**

  辞書に載っている単語、利用者の名前や利用者個人に関連する情報から簡単に派生させたもの等、容易に推測されるものを用いてはならない。また、使用する文字種として、数字だけでなく、アルファベットの大文字及び小文字、さらに特殊記号等も織り交ぜて主体認証情報を構成することが望ましい。

- **基本対策事項 8.1.1(5)-2 e)「共通の主体認証情報を用いない」について**

  複数の識別コードを付与されている場合に、それら識別コードに対して共通の主体認証情報を用いると、一つの識別コードに対応する主体認証情報が漏えいした場合に、他方の識別コードを用いた不正アクセスを受ける危険性が高くなる。したがって、共通の主体認証情報を用いてはならない。

- **基本対策事項 8.1.1(5)-2 f)「識別コード及び主体認証情報についての共通の組合せ」について**

  複数の情報システムにおいて、共通の識別コードを使用し、かつ、共通の主体認証情報を設定していた場合、ある情報システムから漏えいした主体認証情報が他の情報システムで不正に使用されるという情報セキュリティインシデントが発生することが考えられる。したがって、複数の情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを使用しないようにしなければならない。特に、本学支給の情報システムと本学支給以外の情報システムとの間では、共通の識別コード及び主体認証情報を使用しないよう注意する必要がある。

- **基本対策事項 8.1.1(5)-2 g)「主体認証情報を定期的に変更する」について**

  定期的な変更の要求を行う場合は、システムで自動化できることが望ましいが、技術的に困難な場合には、定期的に変更依頼を通達するなどの運用によって対処してもよい。

- **基本対策事項 8.1.1(5)-3 a)「主体認証情報格納装置を本人が意図せずに使われることのないように」について**

  主体認証格納装置の例としては、建物への入退や端末ログインに必要となる IC カード等が挙げられる。所有による主体認証方式では、本人でなくとも主体認証情報格納装置を保持する者が正当な主体として主体認証されるため、他者に当該装置を使用されることがないように適切に管理する必要がある。

遵守事項

(6) 暗号・電子署名の利用時の対策

(a) 事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。

(b) 事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。

(c) 事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.1.1(6)(a)「定められたアルゴリズム及び方法に従う」について**

  情報システムにおいて、認められていないアルゴリズムを利用することを禁止しているものである。暗号アルゴリズムは、ファイル単体の暗号化やハードディスク全体の暗号化、ブラウザを使う通信の暗号化等、様々な場面で利用されていることから、利用する場面ごとに適切なアルゴリズムを適切な方法で利用する必要がある。

  部局技術責任者は、事務従事者の暗号機能の利用において、認められていないアルゴリズムが利用されないよう、あらかじめ情報システムにおいて対処しておくことが望ましい。

- **遵守事項 8.1.1(6)(b)「定められた鍵の管理手順等に従い、これを適切に管理する」について**

  暗号化された情報の復号や電子署名の付与に用いる鍵（以降本項において「鍵」という）の管理手順として、

  情報システム共通として鍵の保存手順を定めている場合と、情報システムごとに鍵の保存手順を個別に定めている場合があるので、各情報システムに対応した手順に従うことが求められる。

- **遵守事項 8.1.1(6)(c)「鍵のバックアップ手順に従い、そのバックアップを行う」について**

  暗号化された情報の復号に用いる鍵の滅失により、情報の可用性が損なわれるおそれがあることから、適切に鍵をバックアップすることを求めている。

  バックアップが必要な鍵については、バックアップの取得又は第三者への鍵情報の預託に関する手順等の規定に従う必要がある。

  また、バックアップしてはならない鍵や、鍵情報の複製が、その漏えいに係るリスクを高める可能性があるなどについても留意し、バックアップは必要最小限にとどめることも大切である。

遵守事項

(7) 不正プログラム感染防止

(a) 事務従事者は、不正プログラム感染防止に関する措置に努めること。

(b) 事務従事者は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずること。

【 基本対策事項 】

＜8.1.1(7)(a)関連＞

8.1.1(7)-1 事務従事者は、不正プログラム対策ソフトウェアを活用し、不正プログラム感染を回避するための以下措置に努めること。

a) 不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しない。また、検知されたデータファイルをアプリケーション等で読み込まない。

b) 不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持する。

c) 不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にする。

d) 不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施する。

8.1.1(7)-2 事務従事者は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

8.1.1(7)-3 事務従事者は、不正プログラムに感染するリスクを低減する情報システムの利用方法として、以下のうち実施可能な措置を講ずること。

a) 不審なウェブサイトを閲覧しない。

b) アプリケーションの利用において、マクロ等の自動実行機能を無効にする。

c) プログラム及びスクリプトの実行機能を無効にする。

d) 安全性が確実でないプログラムをダウンロードしたり実行したりしない。

（解説）

- **遵守事項 8.1.1(7)(a)「不正プログラム感染防止に関する措置に努める」について**

情報システムの利用に当たっては、事務従事者自らが不正プログラム感染の予防に努めなければならない。また、不正プログラム対策ソフトウェアが全ての不正プログラムを検知できるとは限らないことを念頭に入れ、不正プログラムに感染するリスクを低減するために、可能な措置の実施に努める必要がある。

- **遵守事項 8.1.1(7)(b)「通信回線への接続を速やかに切断するなど、必要な措置を講ずる」について**

  不正プログラムに感染したおそれがある情報システムについては、他の情報システムへの感染等の被害の拡大を防ぐ必要がある。当該情報システムを構成するサーバ装置又は端末が通信回線に接続している場合には、それを切断するなど感染拡大を防止する措置を行い、2.2.4 項「情報セキュリティインシデントの対処」に定められた報告や連絡等の対処を行うことが求められる。

  不正プログラムに感染したおそれのある場合の対処について、手順が規定されている場合、その内容に従う必要がある。

- **基本対策事項 8.1.1(7)-1 a)「実行ファイルを実行しない」について**

  不正プログラムとして検知された実行プログラム形式のファイルを実行した場合には、たとえ他の情報システムへ感染を拡大させることがなくても、復旧に相当な労力を要することとなるため、このような実行プログラム形式のファイルを実行しないよう努めなければならない。

- **基本対策事項 8.1.1(7)-1 b)「最新の状態に維持する」について**

  一般的に不正プログラムはほぼ毎日のように新種や亜種が出現しているため、不正プログラム対策ソフトウェア等のアプリケーション及び不正プログラム定義ファイル等を更新機能や更新プログラムにより最新の状態に維持することで、不正プログラム等に感染することを回避する必要がある。自動的に最新化する機能を持つ製品については、当該機能を利用することにより最新状態の維持が可能になる。

  また、最新の状態に維持する方法としては、端末ごとに利用者が自動化の設定をする方法のほか、部局技術責任者等が管理する端末を一括して自動化する方法もあるため、情報システムごとに定められた方法に従うこと。

- **基本対策事項 8.1.1(7)-1 c)「自動検査機能を有効にする」について**

  手動による対策実施は、実施漏れや遅れが発生する可能性があるため、不正プログラム対策の中で自動化が可能なところは自動化することが望ましい。

  自動検査機能の例としては、ファイルの作成や参照のたびに検査を自動的に行う機能等がある。

- **基本対策事項 8.1.1(7)-1 d)「不正プログラムの検査を実施する」について**

  基本対策事項 8.1.1(7)-1 c)の自動検査機能が有効になっていたとしても、検査した時点における不正プログラム定義ファイルでは検知されない不正プログラムに感染している危険性が残る。このような危険性への対策として、定期的に全てのファイルについて検査する必要がある。

- **基本対策事項 8.1.1(7)-2「外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合」について**

  「外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合」には、ウェブの閲覧や電子メールの送受信等のネットワークを経由する場合だけでなく、

USB メモリや CD-ROM 等の外部電磁的記録媒体を経由するものも含む。

8.2　本学支給以外の端末の利用

8.2.1　本学支給以外の端末の利用

目的・趣旨

高等教育機関の事務の遂行においては、本学から支給された端末を用いて高等教育機関の事務を遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず本学支給以外の端末を利用して情報処理を行う必要が生じる場合がある。この際、当該端末は本学が支給したものではないという理由で、事務従事者へ情報セキュリティ対策の実施を求めなかった場合、当該端末で取り扱われる情報セキュリティ水準が、事務情報セキュリティ対策基準を満たさないおそれがある。

したがって、そのような可能性がある場合は、本学支給以外の端末を事務従事者が安全に利用するための手続や安全管理措置の規定をあらかじめ整備し、本学における厳格な管理の下で利用させることが必要である。

また、本学支給以外の端末であっても、本学から支給されるモバイル端末と同等の情報セキュリティ水準の確保が求められることから、7.1.1 項「端末」も参照し、同等の安全管理が実施されるよう、規定を整備し、事務従事者に安全管理措置を講じさせる必要がある。

遵守事項

(1)　本学支給以外の端末の利用規定の整備・管理

(a)　全学実施責任者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合の**許可等の手続に関する手順**を定めること。

(b)　全学実施責任者は、要機密情報について本学支給以外の端末により情報処理を行う場合の**安全管理措置**に関する規定を整備すること。

(c)　部局総括責任者は、本学支給以外の端末による高等教育機関の事務に係る情報処理に関する**安全管理措置の実施状況を管理**する**責任者**を定めること。

(d)　前号で定める責任者は、要機密情報を取り扱う本学支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、事務従事者に適切に安全管理措置を講じさせること。

【 基本対策事項 】

＜8.2.1(1)(a)(c)関連＞

8.2.1(1)-1　全学実施責任者は、以下を例に本学支給以外の端末を利用する際の許可等の手続に関する手順を整備し、事務従事者に周知すること。

a）以下を含む本学支給以外の端末利用時の申請内容

- 申請者の氏名、所属、連絡先
- **利用する端末の契約者の名義**（スマートフォン等の通信事業者と契約を行う端末の場合）
- 利用する端末の機種名

- 利用目的、取り扱う情報の概要、機密性３情報の利用の有無等
- 主要な利用場所
- 利用する主要な通信回線サービス
- 利用する期間

b) 利用許諾条件
c) 申請手順
d) 利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順
e) 利用期間満了時の利用終了又は利用期間更新の手続方法
f) 許可権限者（遵守事項 8.2.1(1)(c)において定める、本学支給以外の端末の安全管理措置の実施状況を管理する責任者（以下、この項において「端末管理責任者」という。））

＜8.2.1(1)(b)関連＞

8.2.1(1)-2 全学実施責任者は、本学支給以外の端末により要機密情報を取り扱う場合は、事務従事者が講ずるべき安全管理措置の実施手順について、以下を例に整備すること。

a) パスワード等による端末ロックの常時設定
b) OS やアプリケーションの最新化
c) 不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（本学として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）
d) 遠隔データ消去機能の設定
e) 要機密情報の暗号化等による秘匿性の確保
f) 端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）
g) 本学提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）
h) 以下を例とする禁止事項の遵守
    - 端末、OS、アプリケーション等の改造行為
    - 安全性が確認できないアプリケーションのインストール及び利用
    - 利用が禁止されているソフトウェアのインストール及び利用
    - 許可されない通信回線サービスの利用（利用する回線を限定する場合）
    - 第三者への端末の貸与

＜8.2.1(1)(d)関連＞

8.2.1(1)-3 部局技術責任者は、本学支給以外の端末により要機密情報を取り扱う本学の情報システムにリモートアクセスする環境を構築する場合、基盤となる情報システムにより各高等教育機関に提供されるリモートアクセス環境が利用可能であれば活用し、端末の盗難・紛失や不正プログラム感染等により情報窃取されることを防止するために、以下を例とする対策を講ずること。

a) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存さ

せないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。

b) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。

c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。利用者は専用のアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。

（解説）

- **遵守事項 8.2.1(1)(a)「許可等の手続に関する手順」について**

本学支給以外の端末の利用に当たっては、目的・趣旨にも記載されているとおり、厳格な管理を行うことが不可欠である。利用に関する手続や安全管理措置を定めて、事務従事者にそれを適切に講じさせないと、以下のようなリスクが想定される。

- 不正プログラムに感染し、要機密情報が外部に漏えいする。
- 端末の盗難・紛失等により、要機密情報が外部に漏えいする。
- 利用者の知識不足により、利用者の意図に反して要機密情報が海外のクラウドに保存され、第三者に閲覧される。
- 家族や知人の端末操作により端末内の要機密情報が外部に漏えいする。

本学支給以外の端末の利用を許可するに当たり、本学としての利用方針を定めておくことが望ましい。個別判断により本学支給以外の端末の利用を認めてしまうと、上記のリスクが顕在化する可能性が高いことから、本学支給以外の端末の利用を認めるのであれば、本学としての利用方針の下、厳格な管理を行う必要がある。

本学支給以外の端末の利用方針として、例えば以下の事項の明確化が考えられる。

- 利用を許可する部局・課室等の組織の単位
- 利用を許可する職員の条件
- 利用を許可する端末の種類（スマートフォン、携帯電話、PC 等）
- 利用する機能（電子メール及びウェブ閲覧に限定 等）

また、本学支給以外の端末の利用に際して、利用する通信回線やサーバ装置等、情報システム全体として情報セキュリティを確保することが重要であることから、リモートアクセス環境や端末の安全管理措置について、システム機能として提供することも考慮すべきである。

なお、本学において本学支給以外のスマートフォン等を利用する場合の基本的な考え方、私物端末利用に当たって考慮すべきリスク、代表的な私物端末の管理対策及び技術対策については、以下の政府機関における取組を参考にするとよい。さらに、民間団体等においても、私物端末の安全な利用方法について有効な資料が公表されているので、併せて考慮されたい。

参考：各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告

「私物端末の業務利用におけるセキュリティ要件の考え方」（平成 25 年 3 月）
（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/index.html）

参考：総務省スマートフォン・クラウドセキュリティ研究会最終報告
「スマートフォンを安心して利用するために実施されるべき方策」
（平成 24 年 6 月 26 日）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html）

- **遵守事項 8.2.1(1)(b)・基本対策事項 8.2.1(1)-2「安全管理措置」について**

本学支給以外の端末を業務に利用することを認めるのであれば、当該高等教育機関支給以外の端末が不正プログラムの感染源や情報の漏えいの要因とならないようにすべきであり、取り扱う情報の格付及び取扱制限に関わらず、情報セキュリティ確保のための安全管理措置を事務従事者に講じさせることが必要である。

なお、事務従事者が講ずるべき安全管理措置が不十分であることが十分考えられるため、基本対策事項 8.2.1(1)-3 に示すシステム機能による情報セキュリティ対策により、一定のリスクを低減した上で事務従事者に利用させる方法を実施することが望ましい。

- **遵守事項 8.2.1(1)(c)「安全管理措置の実施状況を管理」について**

本学支給以外の端末を事務従事者が利用するに当たって、申請時に安全管理措置の実施状況について端末を目視確認する方法や、定期的な実施状況の確認を管理者にて行うことをあらかじめ定めておく方法等が考えられる。管理工数の増加が懸念される場合は、サンプリングによる確認や定期的な注意喚起を利用者に行うなどの方法で管理作業の効率化を図ることも考えられる。

- **遵守事項 8.2.1(1)(c)「責任者」について**

本学支給以外の端末の安全管理措置の実施状況を管理する責任者であり、PC やスマートフォン等に対して一定以上の知見を有している者がその任に当たることが望ましい。例えば、本学 LAN システムの部局総括責任者等が考えられる。ただし、事務従事者の安全管理措置の実施状況について適時状況を把握することが求められるため、職場情報セキュリティ責任者が兼ねることも考えられる。

- **基本対策事項 8.2.1(1)-1 a)「利用する端末の契約者の名義」について**

契約者の名義の提示を求めるのは、業務に使用する端末の名義人と使用人の一致を確認するためである。端末の名義人が端末の利用に係る契約者であり、業務への使用や通信費用に係る訴訟リスクを回避するためには、利用申請時に使用人と名義人が一致していることの確認が必要である。

なお、名義人と使用人である申請者が同一であることを利用条件とする場合は、名義人の確認を求める必要はない。

- **基本対策事項 8.2.1(1)-1 a)「利用する期間」について**

本学支給以外の端末を利用する際に、利用の都度申請手続を行うと事務処理が煩雑化する可能性があるため、例えば 1 年間の利用期間を定め、包括的な許可を与えるなどして事務処理を効率化する方法も考えられる。この場合は、安全管理措置の実施状

況について定期的なチェックを行うなどの対応が求められる。

- **基本対策事項 8.2.1(1)-1 b)「利用許諾条件」について**

  事務従事者に本学支給以外の端末の利用を許可するに当たり、以下の内容を例とした利用許諾条件を示し、許諾書にサインするなどして利用者の同意を証拠として残しておく必要がある。

  - 情報の格付及び取扱制限に応じた取扱いの遵守
  - 定められた安全管理措置の遵守
  - 組織による利用状況の情報収集の承諾
  - 組織による利用端末の制御及び端末の設定変更の承諾
  - 盗難・紛失時に個人の情報を含めた遠隔データ消去を行うことの承諾（職務上取り扱う情報のみ遠隔消去可能なツールを導入する場合は不要）
  - 情報セキュリティインシデント発生時の迅速な届出
  - 機種変更や端末交換の際の再届出の遵守
  - その他、部局技術責任者等の管理責任者の指示の遵守

- **基本対策事項 8.2.1(1)-1 f)「許可権限者」について**

  本学支給以外の端末の利用の許可申請においては、許可権限者である端末管理責任者の許可を得ることになるが、必要に応じて取り扱う情報の管理責任を持つ職場情報セキュリティ責任者の許可を同時に得る手続を定めるとよい。また、リモートアクセスにより本学の情報システムへのアクセスを行わせる場合には、当該情報システムを所管する部局技術責任者の許可を得る手続を併せて定めることも考えられる。（職場情報セキュリティ責任者又は部局技術責任者への許可申請については、遵守事項 8.2.1(2)(a)で規定。）

- **基本対策事項 8.2.1(1)-2 c)「不正プログラム対策ソフトウェアの導入」について**

  OS の構造等により、不正プログラム対策ソフトウェアが提供されていない、又は部分的にしか対策機能が有効でないスマートフォンや携帯電話等の利用については、通信事業者によって事前に安全性が確認されたアプリケーションのみ当該端末へダウンロード可能とされているなどの別の方法で安全性を確保する必要がある。

- **基本対策事項 8.2.1(1)-2 d)「遠隔データ消去機能」について**

  「(解説) 基本対策事項 7.1.1(1)-4f)「遠隔データ消去機能」について」を参照のこと。

- **基本対策事項 8.2.1(1)-2 e)「要機密情報の暗号化等による秘匿性の確保」について**

  本学支給以外の端末に要機密情報を保存して業務を行う場合は、端末に保存する情報を暗号化して盗難・紛失時の情報漏えいのリスクを低減する必要がある。情報へのアクセス権を管理する方法もあるが、記憶媒体の内容を直接読み出されるなどの手法でアクセス権管理機構を回避されるリスクが残るため、要機密情報は暗号化して保存することが望ましい。遠隔データ消去機能を補助的な機能として組み合わせると効果的である。

  また、安全性を確保するためには暗号化に用いる鍵の管理が重要になる。端末紛失

時に端末内に鍵や、鍵を生成するために必要な全ての情報を保持していると暗号化したデータを復号されるリスクがある。

したがって、業務利用していないときはこれらを保持しないなど、鍵の漏えいリスクが低減されるような管理の仕組みを持つ以下の例のようなツールを導入するとよい。

<例> 暗号化する範囲を業務領域に限定しパスワードを入力するタイミングを業務システムへのログイン時、パスワードを基に生成した鍵を消去するタイミングをログアウト時(又はタイムアウト時)とする。

なお、基本対策事項 8.2.1(1)-3 に示すリモートアクセス環境を本学として整備し、当該環境以外での要機密情報の取扱いを禁止すれば、事務従事者による安全管理措置が不要になる。

- **基本対策事項 8.2.1(1)-2 h)「端末、OS、アプリケーション等の改造行為」について**

iOS における Jailbreak や Android における root 化のように、ソフトウェア等の改造が行われた端末は外部からの攻撃の的となりやすく、不正パケットの受信によって不正プログラムに感染したり、端末が乗っ取られたりする危険性が高くなる。

このような改造された端末が業務に使用されると、端末に保存された情報が漏えいするなどの情報セキュリティインシデントが発生する可能性があるため、本学支給以外の端末を利用する際は、事前に端末、OS、アプリケーション等の改造行為を行わないことについて、事務従事者と同意しておくことが重要である。

私物のスマートフォンを業務利用することを目的とした、MDM（Mobile Device Management）ツール等を本学のリモートアクセス環境と組み合わせ、改造された端末を検知するなどして、システム的に改造端末の使用を回避する方法も考えられる。

- **基本対策事項 8.2.1(1)-2 h)「安全性が確認できないアプリケーション」について**

スマートフォンにおいては、専用のアプリケーション提供サイト等からオンデマンドでアプリケーションをダウンロードする利用形態が一般的であるが、不正プログラム等が混在する提供サイトの存在が懸念されるため、業務に利用する私物のスマートフォン等においては安全性が不明なアプリケーションがインストールされた状態で利用されることがないように、例えば OS 提供事業者や通信事業者等がアプリケーションの安全性の審査を行っている信頼性の高いアプリケーション提供サイトにて提供されるアプリケーションのみに利用を限定すること等を対策にするとよい。ただし、大手の事業者であっても安全なアプリケーションを提供しているとは限らないので、提供サイトを運営する事業者のセキュリティ対策水準を十分見極めた上で判断することが求められる。

スマートフォンを安全に利用するための留意事項として、OS の最新化及び不正プログラム対策とともに注意喚起されているので、参考にすること。

参考：総務省「スマートフォン情報セキュリティ３カ条」（スマートフォン・クラウドセキュリティ研究会中間報告）（平成 23 年 12 月 19 日公表）
（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000015.html）

- **基本対策事項 8.2.1(1)-2 h)「利用が禁止されているソフトウェア」について**

  遵守事項 7.1.1(1)(c)の対策として、本学支給の端末において規定される利用を禁止するソフトウェアと同等であることが考えられるが、例えば個人利用の範囲を必要以上に制限しないよう考慮する必要がある。

- **基本対策事項 8.2.1(1)-2 h)「許可されない通信回線サービスの利用」について**

  公衆無線 LAN サービスのうち無線経路の秘匿性や安全性が不明なものや接続経路の管理状況が不明な無料のインターネット接続サービス等は、通信内容の盗聴やなりすましによる情報の窃取等のおそれがあり、このような情報セキュリティ水準が不明な通信回線は業務に利用すべきではない。ただし、海外等で、情報セキュリティ水準が不明な通信回線サービスを利用せざるを得ない場合が想定されることから、例えば、情報システムへのリモートアクセス経路において VPN 回線を設定し end-end の秘匿性を確保するなどの方法を用いるとよい。

  なお、無線 LAN の利用に関する対策については、7.3.1 項「通信回線」の「(5) 無線 LAN 環境構築時の対策」の内容を併せて考慮する必要がある。

- **基本対策事項 8.2.1(1)-2 h)「第三者への端末の貸与」について**

  家族や知人に私物の端末等を貸与することがあるが、その際に意図的に機密性の高い情報を閲覧したり又は誤操作により機密性の高い情報を外部に転送してしまったりすることが懸念される。

  私物端末であっても業務に利用するのであれば、第三者への貸与は原則禁止すべきであり、それに同意できない事務従事者には私物端末を利用させるべきではない。

- **基本対策事項 8.2.1(1)-3「部局技術責任者」について**

  本基本対策事項にて指定している部局技術責任者は、本学 LAN システム等のリモートアクセス先の情報システムを所管する部局技術責任者である。

  遵守事項 8.2.1(1)(c)に従って定められる“本学支給以外の端末の安全管理措置の実施状況を管理する責任者”に対して、遵守事項 8.2.1(1)(d)において、本学支給以外の端末の盗難・紛失や不正プログラム感染等により情報窃取されることを防止するための措置を講ずることを求めているが、当該措置の例として、本学 LAN システムへの安全なリモートアクセス環境があらかじめ提供されている場合に、これを活用することを想定している。

- **基本対策事項 8.2.1(1)-3 a)「シンクライアント等」について**

  端末に情報を保存させずに本学支給以外の端末を業務利用することを可能とする仕組みとして、シンクライアントやリモートデスクトップと呼ばれる技術の活用が有効である。シンクライアントやリモートデスクトップ関連の製品やソリューションサービスは、既に市場において提供されているが、外部のクラウドサービスを組み合わせて利用する場合は、4.1.1 項「外部委託」又は 4.1.2 項「約款による外部サービスの利用」についても参照する必要がある。

  なお、当該機能については、本学支給のモバイル端末においても利用することが可能であることから、本学支給のモバイル端末及び本学支給以外の端末を業務利用にお

いて共存させたい場合でも有効な対策となる。

＜シンクライアントの主な機能及び特徴＞

- 業務ネットワーク内の仮想デスクトップ画面を転送
- ユーザデータを端末に残さない
- ウェブキャッシュ、接続情報、作業履歴等全てサーバ内に保管
- 外部情報出力（クリップボードへのコピー、スクリーンショット、印刷、他アプリケーション連携）を抑制可能

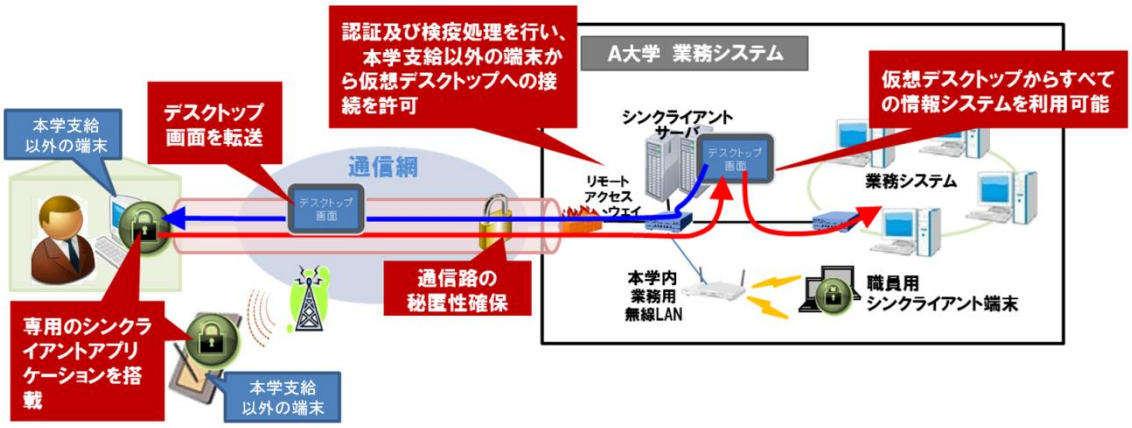


図 8.2.1-1　シンクライアントのシステム構成例

また、シンクライアントの発展形として、仮想デスクトップ環境の利用機能（ネットワーク接続や画面描画・ディスプレイ出力、キーボード・マウス入力等）のみに機能が絞り込まれたゼロクライアントやシンクライアント専用端末の利用も有効である。特にゼロクライアントは、汎用 OS や汎用ブラウザ等を搭載していないことから、不正プログラム対策やソフトウェア更新等のセキュリティ管理の負荷が軽減でき、万一端末が故障しても、端末を交換するだけですぐに利用可能になるなど、セキュリティ管理面の負荷の軽減も期待される。処理能力やコスト負担等の課題も考えられるので、それらも勘案した上で利用を検討するとよい。

- **遵守事項 8.2.1(1)-3 b)「セキュアブラウザ等」について**

端末に情報を保存させずに本学支給以外の端末を業務利用する別の仕組みとして、セキュアブラウザを選択することも可能である。

セキュアブラウザ製品についても、各種クラウドサービスと組み合わせたソリューションとして提供される場合があることから、外部の情報処理サービスを組み合わせて利用する場合は、4.1.1 項「外部委託」又は 4.1.2 項「約款による外部サービスの利用」についても参照する必要がある。

当該の仕組みについても、本学支給のモバイル端末においても利用することが可能である。

＜セキュアブラウザの主な機能及び特徴＞

- 電子メール、ファイル閲覧等を画面転送等で行い、ユーザデータを端末に残さ

ない

- ブラウザ終了時に閲覧に関連する情報(ウェブキャッシュ、URL、cookie 等)を消去可能
- 外部出力(クリップボードへのコピー、スクリーンショット、印刷、他アプリケーション連携)を抑制可能

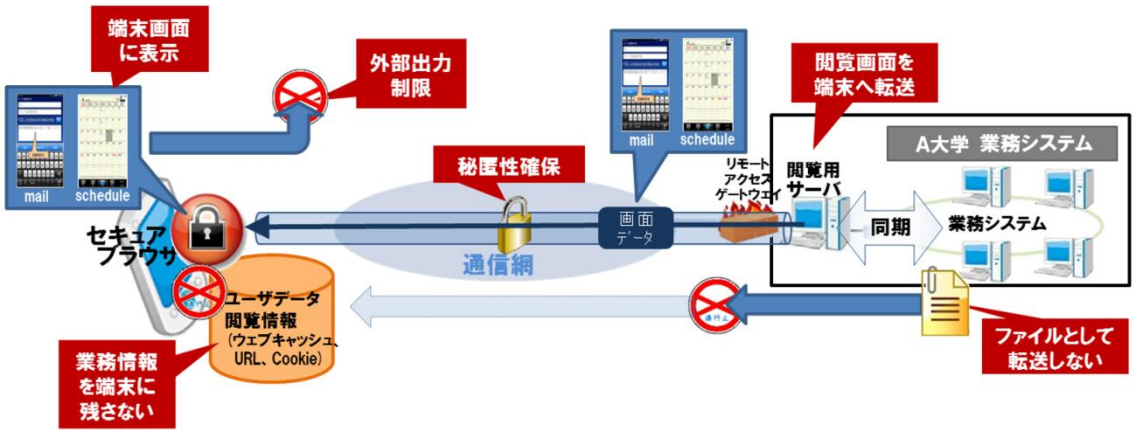


図 8.2.1-2　セキュアブラウザ活用型ソリューションのシステム構成例

なお、当該機能については、本学支給のモバイル端末においても利用することが可能であることから、本学支給のモバイル端末及び本学支給以外の端末を共存させたい場合において有効な対策となる。

- **基本対策事項 8.2.1(1)-3 c)「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について**

  通信回線との接続環境が無い場所で業務を行うなど、やむを得ず情報を端末に保存させる必要がある場合は、セキュアブラウザやシンクライアントは利用できないことから、他の方法で安全な利用環境の提供を考える必要がある。この場合は、本学支給以外の端末にファイル暗号化等のセキュリティ機能を持つ業務専用のアプリケーションを搭載し、アプリケーション単位で情報を暗号化するなどの方法が考えられる。当該機能を有するセキュリティソリューションが製品として民間事業者より提供されていることから、それらの活用を検討するとよい。

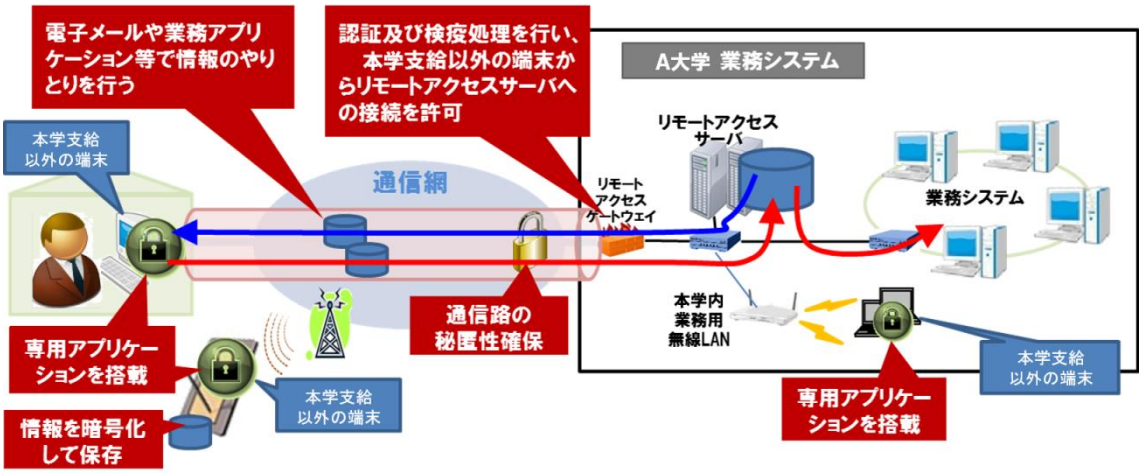


図 8.2.1-3　ファイル暗号化等セキュリティ機能を持つアプリケーションを活用したシステム構成例

なお、当該機能については、本学支給のモバイル端末においても利用することが可能であることから、本学支給のモバイル端末及び本学支給以外の端末を共存させたい場合において有効な対策となる。

遵守事項

(2) 本学支給以外の端末の利用時の対策

(a) 事務従事者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合には、遵守事項 8.2.1(1)(c)で定める責任者の許可を得ること。

(b) 事務従事者は、要機密情報を本学支給以外の端末で取り扱う場合は、**職場情報セキュリティ責任者の許可を得る**こと。

(c) 事務従事者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合には、本学にて定められた手続及び**安全管理措置に関する規定に従う**こと。

(d) 事務従事者は、情報処理の目的を完了した場合は、**要機密情報を本学支給以外の端末から消去する**こと。

【 基本対策事項 】規定なし

（解説）

- **遵守事項 8.2.1(2)(b)「職場情報セキュリティ責任者の許可を得る」について**

  事務従事者は、本学支給以外の端末の利用を開始するに当たり、本学支給以外の端末の許可権限者に対して許可申請を行うことになるが、当該申請以外に、本学支給以外の端末を用いて行う業務及び取り扱う情報の管理責任者である職場情報セキュリティ責任者に対して許可を求める必要がある。

- **遵守事項 8.2.1(2)(c)「安全管理措置に関する規定に従う」について**

  事務従事者は、本学支給以外の端末の利用に係る本学全体のポリシーをよく理解し、安全管理措置を徹底し、情報セキュリティインシデントの発生の回避に努めなければならない。特にスマートフォン等の利用については、その特性に応じたリスクを利用者である事務従事者自身もよく理解した上で利用することが求められる。

- **遵守事項 8.2.1(2)(d)「要機密情報を本学支給以外の端末から消去する」について**

  要機密情報を消去することは必須であるが、不必要な情報及び業務用のアプリケーション等についても併せて消去しておくことが望ましい。

付録

1. 情報セキュリティ対策に関する政府決定等

- サイバーセキュリティ戦略（平成 27 年９月４日 閣議決定）
- 日本再興戦略 改訂 2015（平成 27 年６月 30 日 閣議決定）
- 世界最先端 IT 国家創造宣言（平成 27 年６月 30 日 閣議決定）
- サイバーセキュリティ人材育成総合強化方針（平成 28 年３月 31 日 サイバーセキュリティ戦略本部）
- サイバーセキュリティを強化するための監査に係る基本方針（平成 27 年５月 25 日 サイバーセキュリティ戦略本部決定）
- 高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成 26 年６月 25 日 情報セキュリティ対策推進会議）
- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（2015 年５月 21 日 内閣サイバーセキュリティセンター）
- 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（2015 年５月 21 日 内閣サイバーセキュリティセンター）
- スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書（2015 年５月 21 日 内閣サイバーセキュリティセンター）
- 中央省庁業務継続ガイドライン 第２版（首都直下地震対策）（平成 28 年４月 内閣府（防災担当））
- 中央省庁における情報システム運用継続計画ガイドライン及び関連資料（平成 25 年６月 内閣官房情報セキュリティセンター）
- 大規模サイバー攻撃事態等への初動対処について（平成 22 年３月 19 日 内閣危機管理監決裁）
- 政府におけるサイバー攻撃等への対処態勢の強化について（平成 22 年 12 月 27 日 情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ）
- 調達における情報セキュリティ要件の記載について（平成 24 年１月 24 日 内閣官房副長官）
- オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（平成 22 年８月 31 日 各府省情報化統括責任者（CIO）連絡会議決定）
- 情報セキュリティ対策に関する官民連携の在り方について（平成 24 年１月 19 日 情報セキュリティ対策推進会議 官民連携の強化のための分科会）

- 情報セキュリティ管理基準（平成 28 年改正版）（平成 28 年経済産業省告示 37 号）
- クラウドサービス提供における情報セキュリティ対策ガイドライン(平成 26 年 4 月 総務省)
- クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013 年度版 経済産業省）
- クラウドセキュリティガイドライン活用ガイドブック（平成 26 年 3 月 14 日 経済産業省）
- 金融機関におけるクラウド利用に関する有識者検討会報告書(平成 26 年 11 月 14 日 公益財団法人 金融情報システムセンター)
- テレワークセキュリティガイドライン（第 3 版）（平成 25 年 総務省）
- 電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト）平成 25 年 3 月 1 日 総務省、経済産業省）
- SSL/TLS 暗号設定ガイドライン（平成 27 年 8 月 3 日 CRYPTREC）
- IT 製品の調達におけるセキュリティ要件リスト（平成 26 年 5 月 19 日 経済産業省）
- IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック（2014 年 5 月 独立行政法人情報処理推進機構）
- 安全なウェブサイトの作り方 改訂第 7 版（2015 年 3 月 独立行政法人情報処理推進機構セキュリティセンター)
- 「高度標的型攻撃」対策に向けたシステム設計ガイド (2014 年 9 月 独立行政法人情報処理推進機構セキュリティセンター)
- 地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）第 1.0 版（平成 24 年 10 月 22 日 財団法人地方自治情報センター）
- 無線 LAN セキュリティ要件の検討（平成 23 年 3 月 各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告）
- 「無線 LAN ビジネス研究会」報告書（平成 24 年 7 月 20 日 総務省）
- 無線 LAN ビジネスガイドライン（平成 25 年 6 月 25 日 総務省）
- 私物端末の業務利用におけるセキュリティ要件の考え方（平成 25 年 3 月 各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告）
- スマートフォンを安心して利用するために実施されるべき方策（平成 24 年 6 月 26 日 総務省スマートフォン・クラウドセキュリティ研究会最終報告）
- スマートフォン情報セキュリティ 3 カ条（スマートフォン・クラウドセキュリティ研究会中間報告（平成 23 年 12 月 19 日 総務省）
- 行政文書の管理に関するガイドライン（平成 23 年 4 月 1 日 内閣総理大臣決定）
- 行政文書の管理に関するガイドラインの一部改正に伴う政府機関の情報セキュリティ

対策のための統一基準の扱いについて（平成 27 年 1 月 23 日付閣サ第 19 号 内閣官房副長官（情報セキュリティ対策推進会議議長））

- 特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（平成 26 年 12 月 18 日 個人情報保護委員会）
- 行政機関の保有する個人情報の適切な管理のための措置に関する指針について（通知）（平成 16 年 9 月 14 日付総管情第 84 号 総務省行政管理局長）
- 政府情報システムの整備及び管理に関する標準ガイドライン（平成 26 年 12 月 3 日 各府省情報化統括責任者（CIO）連絡会議決定）

2. 情報セキュリティ対策に関する法律

〔法律〕

・サイバーセキュリティ基本法（平成 26 年法律第 104 号）

・行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号）

・行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）

・公文書等の管理に関する法律（平成 21 年法律第 66 号）

注）詳細については、原文を参照すること。

C2601 全学認証基盤運用管理規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2016年2月5日 C2601	新規作成	曽根秀昭（東北大学、高等教育機関における情報セキュリティポリシー推進部会主査） 岡部寿男（京都大学） 佐藤周行（東京大学） 野田英明（国立情報学研究所）

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C2601-01（目的）

第一条　この規程は、A 大学全学認証基盤（以下「本基盤」という。）の運用及び管理に必要な事項を定め、もってシステムの安定的・円滑な運用を維持することを目的とする。

備考：　この規程は全学認証基盤（システム）を扱い、他のシステムとの認証接続については C2602 全学認証基盤認証接続規程、全学アカウントについては C2603 全学認証基盤アカウント利用規程で定める

C2601-02（定義）

第二条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　A 大学全学認証基盤　A 大学における教育研究、福利厚生のためのサービスを提供する際に必要となる、利用者認証と主体認証情報の提供を行う情報システムをいう。

二　利用者　本基盤のアカウントの発行を受けることができる者をいう。

三　識別コード 本基盤及び本基盤より機能の提供を受ける情報システムにおいて用いる、利用者を一意に識別するための符号をいう。

四　主体認証情報　識別コードを提示した利用者が本人であることを確認するための秘密情報等をいう。

五　全学アカウント　本基盤で主体認証を行う情報システムにおいて、主体に付与された正当な権限をいう。全学アカウントの付与は、識別コードと主体認証情報の配布、主体認証情報格納装置の交付、アクセス制御における許可、またはそれらの組み合わせ等によって行われる。

五　属性情報　全学アカウントに付随して管理・提供される利用者に関する情報をいう。

六　アイデンティティ情報　利用者に関する全学アカウントおよび属性情報を総称する情報をいう。

七　認証接続　認証と認可を目的として、全学情報システム、もしくは部局情報システムが本基盤のアイデンティティ情報を利用することをいう。

備考：　部局情報システムには部局が契約する学外の情報サービスのシステムも含まれる。学外の情報サービスのシステムとの認証接続にはいずれかの部局の契約を必須とするので、学外の情報システムとの認証接続は存在しない。

八　認証接続システム　本基盤に認証接続された全学情報システムもしくは部局情報システムをいう。

九　認証接続責任者　認証接続システムの認証接続に係る責任を有する本学の職員をいう。

十　A 大学認証局　A 大学電子認証局ポリシー及び運用規則に定める認証局をいう。

十一 電子証明書 A 大学認証局から発行された証明書でログイン時の主体認証等に利用するため証明書をいう。

十二 IC カード C2101-02 情報システム運用・管理規程第二条三十八に定める主体認証情報格納装置のうち、主体認証情報を IC に格納するものをいう

十三 PIN (Personal Identification Number) 電子証明書を格納した IC カードを使った主体認証時に使われる主体認証情報をいう。

備考：　認証接続システムの部局技術責任者が認証接続責任者となる。

C2601-03（運用責任者）

第三条　本基盤の運用責任者（以下「運用責任者」という。）は全学実施責任者をもって充てる。

C2601-04（認証情報）

第四条　運用責任者は、本基盤において利用する主体認証情報について、パスワードを用いる場合には、別途定める利用者パスワードガイドラインに基づき、利用者に認証強度が一定以上のものを利用させるよう配慮するものとする。

備考：　C3255 利用者パスワードガイドラインがある。

C2601-05（属性情報）

第五条　本基盤が保有する利用者の属性情報の項目は運用責任者が別に定める。

２　本基盤が保有する利用者の属性情報のうち職員データベースおよび学生データベース（以下、総称してデータベース等という。）から転送されるものについて、それぞれ職員データベース運用管理規程および学生データベース運用管理規程に合致するものでなければならない。

３　運用責任者は、本基盤で登録する属性情報が真正であることを確保するため、必要な措置を講じなければならない。また、利用者または運用責任者が本基盤で更新登録する属性情報を最新の状況を反映させて適切に管理しなければならない。

４　運用責任者は、データベース等から転送された属性情報について、データベース等において更新があった場合にそれを本基盤へ転送しなければならない。

５　運用責任者は、データベース等から転送された属性情報について、利用者または運用責任者が本基盤で更新した属性情報をデータベース等へ反映させるよう適切に管理しなければならない。

６　認証接続システムの利用者または認証接続システムの認証接続責任者が設定して本基盤へ転送する属性情報は、当該認証接続システムの運用管理規定に合致するものでなければならない。

備考：認証基盤が保有する個人情報の登録・削除等の管理について、（ａ）源泉となる個人情報データベースを別に設けて転送（インポート）する、（ｂ）この認証基盤において（源泉として）行う、（ｃ）職員データベースや学生データベースなど既存のデータベース等から転送し、いずれのデータベースにも含まれない者をこの認証基盤において追加する、などの方法が考えられるが、この条では（ｃ）を想定している。

なお、５は認証基盤で属性情報の更新登録を可能とする場合に源泉となるデータベース等へ反映させることを、６は認証接続システムで属性情報の設定を可能とする場合に認証基盤へ反映させることを定めるものであるので、これらの機能を許さないシステムでは不要である。

C2601-06（認証接続）

第六条　本基盤と認証接続システムの認証接続に関することはＡ大学全学認証基盤認証接続規程に定める。

C2601-07（全学アカウント）

第七条　全学アカウントに関することは全学認証基盤アカウント利用規程に定める。

C2601-08（個人情報の取り扱い）

第八条　本基盤における個人情報の取扱いは、A 大学個人情報保護規程（以下、「個人情報保護規程」という。）の定めるところによる。

２　本基盤の保有個人データについて、本人からの開示、訂正、追加、削除及びその他の個人情報に関する問い合わせは運用責任者が別に定める。

備考：個人情報保護規程は，国立大学等であれば独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）に沿ったものである。
本基盤において個人情報を取得し、保有および利用することができるのは、次の各号に掲げる目的に必要な場合に限られる。
一 A 大学全学アカウント付与
二 A 大学全学認証基盤の維持管理
三 認証接続システムとの情報連携サービス
四 インシデント対応に不可欠な範囲での利用
五 その他運用責任者が必要と定める事項

C2601-09（運用環境）

第九条　本基盤は、物理環境的およびセキュリティ的に適切な環境に設置し、運用責任者は限定された運用管理者を指名してその任に当たらせるものとする。

２　本基盤は、C2101 情報システム運用・管理規程に定める情報セキュリティ基準に準拠して運用するものとする。

３　運用責任者は必要に応じて運用管理者に研修等を定期的に受けさせるものとする。

C2601-10（記録）

第十条　本基盤を用いた利用者の認証について、トランザクションごとに、時刻を認証接続サービスに渡されたアイデンティティ情報等のログ情報とともに記録するものとする。

２　本基盤は、本学が信頼する時刻情報を用いて時刻同期を取るものとする。

３　運用責任者は、ログ情報の保存期間を最低 3 か月の範囲で定めるものとする。運用管理者は、当該保存期間が満了する日までログ情報の記録を適切に保護された状態で保存し、保存期間を延長する必要がない場合は速やかにこれを消去するものとする。

４　運用責任者は、収集、保管されるログ情報の種類については、定期的にリスク評価を行い、見直すものとする。

C2601-11（雑則）

第十一条　この規程に定めるもののほか、本基盤の運用及び管理に関し必要な事項は、運用責任者が別に定める。

C2602 全学認証基盤認証接続規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2016年2月5日 C2602	新規作成	曽根秀昭（東北大学、高等教育機関における情報セキュリティポリシー推進部会主査） 岡部寿男（京都大学） 佐藤周行（東京大学） 野田英明（国立情報学研究所）

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C2602-01（目的）

第一条　この規程は、全学認証基盤運用管理規程第 9 条の規定に基づき、A 大学全学認証基盤（以下「本基盤」という。）の認証接続に必要な事項を定める。

C2602-02（定義）

第二条　この規程において使用する用語は、A 大学全学認証基盤運用管理規程（以下「運用管理規程」という。）において使用する用語の例による。

C2602-03（認証接続）

第三条　全学情報システムもしくは部局情報システムを認証接続するときには、当該システムに係る部局技術責任者が、当該システムの認証接続に係る認証接続責任者となり、別に定める手順に従い、利用目的及び認証接続において提供される情報の利用範囲を明示した上で、部局総括責任者を通して運用責任者へ認証接続申請し許可を受けなければならない。なお、運用責任者があらかじめ指定する範囲においてはこの限りで無い。

２　運用責任者は、前項の申請で許可した認証接続又はあらかじめ指定する範囲の認証接続において、属性情報として個人情報が提供される場合には、当該認証接続システムと個人情報の利用目的を当該認証接続に係る利用者に通知しまた学内公表する。

３　認証接続責任者は、認証接続の許可を受けたときあるいは認証接続したときには当該認証接続システムおよび当該認証接続に係る利用者の範囲、利用方法を部局総括責任者に報告し、また当該認証接続に係る利用者に通知しまた学内公表する。

４　認証接続申請の内容に変更があるときにはあらかじめ申請と許可の手続きを行う。

５　認証接続責任者は、認証接続の必要がなくなったときは遅滞なく運用管理者へ認証接続の廃止を届けなければならない。

６　運用責任者は、認証接続の運用に支障を発見したときは、認証接続の一時停止あるいは制限を行うことができる。この場合に、支障が除去されたことが確認された後，速やかに復帰を行うものとする。

備考：接続申請の申請書・許可書の項目として、以下のものが考えられる。接続責任者、利用目的、利用予定期間、接続する本基盤の統合認証システム、接続する情報システム・接続方式・通信方式、情報システムの運用者、情報システムが提供するサービス、対象となる利用者、利用方法、提供を希望する属性情報と範囲、属性情報の利用目的と利用範囲、情報システムの運用管理（情報セキュリティ対策，個人情報保護）ポリシー，情報システムの技術担当者等。
本基盤が提供する連携方式，通信方式（暗号化）、接続が許可される情報システム／サービスと属性情報の範囲のガイドライン、接続の技術的手順書も情報システム管理者向けに用意することが望ましい。

備考：　部局が契約する学外の情報サービスのシステムとの認証接続においても、部局情報システムとして扱いは同じである。

C2602-04（認証接続責任者の義務）

第四条　認証接続責任者は認証接続の安定な運用に協力しなければならない。

２　認証接続責任者は、認証接続により提供される情報の利用範囲が許可を受けた申請の利用目

的及び利用範囲を逸脱しないよう必要な措置を講じなければならない。また、情報セキュリティ対策と個人情報保護に努めなければならない。

C2602-05（包括的接続）

第五条　複数の情報システムについてこれらを特定して一括することにより、第三条の手続きを包括的に行って、各々の情報システムごとの手続きを省略して接続することができる。

備考：電子ジャーナルサービスパッケージを想定している。

２　接続責任者は、包括的接続に一括される情報システムの変更の通知を受けたときには、その影響を判断し、そのことを対象となる利用者に通知しまた学内公表しなければならない。

C2602-06（属性情報の提供）

第六条　本基盤が接続システムへ提供できる属性情報は運用管理者が別に定める。

２　学外へも提供できる属性情報は運用管理者が別に定める。

３　情報システムとの接続において、接続責任者は利用に必要でない属性情報を提供することのないように適切に運用管理しなければならない。

C2602-07

第七条　情報システムとの接続において、属性情報の提供は利用目的の通知または公表に対する利用者の本人同意を確認しなければならない。

２　本人同意において次回以降の同意を省略することの意思表示が事前に本基盤の操作においてあった場合には、接続システムと提供する属性情報に変更がなければ、省略することができる。

C2602-08（雑則）

第八条　この規程に定めるもののほか、本基盤の接続に関し必要な事項は、別に定める。

C2603 全学認証基盤アカウント利用規程

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2016年2月5日 C2603	新規作成	曽根秀昭（東北大学、高等教育機関における情報セキュリティポリシー推進部会主査） 岡部寿男（京都大学） 佐藤周行（東京大学） 野田英明（国立情報学研究所）

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C2603-01（目的）

第一条　この規程は、A 大学全学認証基盤（以下、「本基盤」という。）において用いる全学アカウントの利用に必要な事項を定め、もって利用者の保護と本基盤の安定的な運用に資することを目的とする。

C2603-02（定義）

第二条　この規程において使用する用語は、C2601 A 大学全学認証基盤運用管理規程（以下「運用管理規程」という。）において使用する用語の例による。

C2603-03（利用者の範囲）

第三条　本基盤の利用者は、次の各号に掲げる者とする。

一　C1001 情報システム運用基本規程に定める教職員等のうち運用責任者が登録したもの

二　C1001 情報システム運用基本規程に定める学生等のうち運用責任者が登録したもの

三　C1001 情報システム運用基本規程に定める臨時利用者のうち運用責任者が許可されたもの

C2603-04　（識別コードの交付）

第四条 全学情報システム又は部局情報システムを、識別コードによる主体認証を伴って利用する利用者は、本基盤の運用責任者が別途定める手続きにより、識別コードを取得しなければならない。

C2603-05　（臨時利用者への許可）

第五条 運用責任者は、第三条三号の臨時利用者について、以下の各号のいずれかに該当し必要があると認めるときは、本基盤の臨時利用者として、識別コードを交付するものとする。

一　部局総括責任者より臨時利用の目的・範囲・期間等を明示して臨時利用者による本基盤の利用の申請があったとき

二　その他運用責任者が特に必要があると認めたとき

備考：　臨時利用者の例として以下のようなものが想定される。

一　本学の名誉教授

二　本学若しくは本学の部局において定められた身分を持つ者又は本学との業務委託契約若しくは労働者派遣契約により派遣された者

三　本学との契約又はそれに準ずる行為により、本学施設内において活動する社団等に所属し本学施設内で常時業務する職員であり、本学に対する公益的な業務遂行のため本システムの利用を必要とする者。

四　本学施設内において特定の機能のシステムの利用を必要とする目的を有する者（本学施設を担当する配達事業従事者の入館カードの例、研究会合開催時の参加者のネットワーク利用の例、など）。利用者を識別しない入館カードの場合には、臨時利用者としてではなく認証情報とひもづけない IC カードとして扱うことも考えられる（第十三条（IC カードと電子証明書の取得）の備考を参照）。

備考：部局認証基盤の利用者等（部局が臨時に特に認めた者）は対象に含めていない。

２　部局総括責任者は、前項一号の臨時利用の申請事項について変更（利用資格の喪失を含む）が生じたときは、速やかに変更内容を運用責任者に届け出なければならない。
３　部局総括責任者は、第１項第一号に基づき臨時利用者の利用を申請し許可された際、許可された臨時利用者に対して本規程を遵守させるよう必要な措置を講じなければならない。また、許可された臨時利用者に対して、必要と認めた場合、情報セキュリティポリシー及び実施規程並びに情報システムの利用に関する講習を受講させなければならない。
４　運用責任者は、第１項第二号に基づき臨時利用者の利用を許可した際、許可した臨時利用者に対して本規則を遵守させるよう必要な措置を講じなければならない。また、許可した臨時利用者に対して、必要と認めた場合、情報セキュリティポリシー及び実施規程並びに情報システムの利用に関する講習を受講させなければならない。

C2603-06（識別コードの付与）
第六条　識別コードは利用者ごとに一意となるよう個人に対して付与するものとし、複数の者が共用する目的では付与しない。
２　かつて利用されていたが現在利用されていない識別コードを他者に再割り当てする場合には、最終の利用時から再割り当てまで最低 24 カ月の期間を設けるものとする。

備考：係員など複数の者（グループ）での共有はできない。役職に対して付与するアカウントは他者が共有・引継ぎするためにこの条の違反となりうるが，それを例外とするのは好ましくない。職員個人に対して役割（ロール）属性設定を管理する機能を備える情報システムを作るべきであるが，もし現有システムが対応しない場合には，個人アカウントに併せてロール別アカウントを職員個人へ付与することは許容される。

C2603-07（識別コードの交付）
第七条　本基盤の識別コードおよび主体認証情報を交付（再交付を含む）する場合は、本学発行の職員証または学生証による対面での確認、学内便を用いた送付、またはそれに準じる方法により本人性と実在性を確認して行う。

C2603-08　（識別コードの一時停止と復帰）
第八条　運用責任者は、法令、情報セキュリティに関する本学のポリシー、実施規程、その他本学の規程、規則に定める遵守事項に違反する利用者の識別コードを発見したとき、または利用者の主体認証情報が他者に使用され若しくはその危険が発生したことの報告を受けたときは、本基盤と認証接続している全部または一部の認証接続システムとの当該識別コードを使用した認証接続の一時停止または制限を行うことができる。一時停止または制限を行った場合は、その旨を当該利用者の所属する部局総括責任者に報告するものとする。
２ 部局総括責任者は、前項の措置の報告を受けたときには、速やかにその旨を当該の利用者に通知するものとする。ただし、電話、郵便等の伝達手段によっても通知ができない場合はこの限りでない。
３ 第１項の一時停止または制限を受けた利用者が、当該識別コードの違反の状況または危険を解消する措置を講じて識別コードを使用する認証接続の復帰を希望するときは、その旨を部局総

括責任者申し出るものとする。

4 部局総括責任者は、前項の申し出を受けたときは、当該識別コードの措置の状況を確認し適切であると判断した後、運用責任者に報告し、運用責任者は識別コードの復帰ならびに必要に応じて主体認証情報の再交付を行うものとする。

備考：アカウントの取り消しは規定していないが，停止から復帰させない場合がそれになる。

C2603-09（接続先サービスの利用）

第九条　本基盤から交付されるアカウントによる認証接続システムのサービスの利用資格は，接続先のサービスが定める規程等による。

C2603-10（利用者情報の提供）

第十条　本基盤は、利用者の同意に基づき、接続先のサービスに対して、利用者に関する属性情報を送信するものとする。

2　利用者は、接続先のサービスを利用する際、本基盤から送信される属性情報を確認し、個々のサービスの利用の可否を適切に判断するものとする。

C2603-11（遵守すべき規程等）

第十一条　利用者は、本基盤を利用して認証接続システムを利用する際、法令を遵守するとともに、当該情報システムあるいはそのシステムのサービスの利用に関して規程等を含む契約に基づく定めを遵守しなければならない。

備考：利用者の遵守すべき事項は C2201 にある。

C2603-12（IC カードと電子証明書の取得）

第十二条 認証接続システムを、IC カードによる主体認証を伴って利用する利用者は、本基盤の運用責任者が別途定める手続きにより、IC カードを取得しなければならない。

2 認証接続システムを、電子証明書による主体認証を伴って利用する利用者は、C2651 A 大学認証局ポリシーおよび運用規則に定める手続きにより電子証明書を取得しなければならない。

備考：IC カードの発行・交付は，運用責任者あるいは情報メディアセンターではない部署が行う例もあり得る。

例えば、IC 職員証（職員証取扱要項に基づき教職員等に交付される職員証であって、主体認証情報を IC に格納するもの）、認証 IC カード（認証 IC カード取扱要項に基づき非常勤の教職員等に交付される IC カードであって、主体認証情報を IC に格納するもの）、IC 学生証（学生に対して所属部局が交付する学生証であって、主体認証情報を IC に格納するもの）、施設利用証（前記のいずれも交付を受けていない者に対して施設利用証取扱要項に基づき発行する利用証であって、主体認証情報を IC に格納するもの）などがあり、別に規定する必要がある。また、これらに関する発行責任組織は例えば、IC 職員証においては総務部、IC 学生証においては当該学生の所属する部局、認証 IC カード及び施設利用証においては情報メディアセンターが該当すると考えられる。

備考：利用者がすでに所有してまたは貸与を受けて利用するカードであって所定の仕

様条件に適合するもの（ここで「その他のカード」と言う。）を用いて IC カードに格納された主体認証情報をコピーすることにより IC カードと同等の二次的な IC カードとして利用することも考えられる。これを許す方針をとる大学では、これをできると規定するとともに、IC カードの規定が準用されることを規定する。

また、新たに IC カードを支給することなく、その他のカードを用いて主体認証情報を書き込むなどして IC カードと同等の利用を可能とすることも考えられる。この場合には支給された IC カードのほかにそれ以外の IC カードを規定する。

A 大学認証局が発行したものではない電子証明書を主体認証に利用させることも考えられ、これを許す場合にも上記 IC カードのケースと同様の規定を設ける。

備考：臨時入館証等の IC カードについて利用者を識別しないで取得させる（交付する）場合には、主体認証を伴わないので、1 項の規定とは別に定める必要がある。

備考：IC カードおよび電子証明書利用者の遵守すべき事項は C2201 にある。

C2603-13（IC カード及び電子証明書の失効と再発行）

第十三条 運用責任者は、本規程に定める遵守事項に違反する IC カード及び電子証明書を発見したとき、又は主体情報が他者に使用され若しくはその危険が発生したことの報告を受けたときは、電子証明書を失効し、その旨を該当する IC カード及び電子証明書を利用している利用者等の所属する部局情報セキュリティ責任者に報告するものとする。

2 部局情報セキュリティ責任者は、前項の措置の報告を受けたときには、速やかにその旨を利用者等に通知するものとする。ただし、電話、郵便等の伝達手段によっても通知ができない場合はこの限りでない。

3 IC カードの失効を受けた利用者が、IC カード及び電子証明書の再発行を希望するときは、その旨を運用責任者に申し出るものとする。

4 電子証明書の失効を受けた利用者が、IC カード及び電子証明書の再発行を希望するときは、C2651 A 大学認証局ポリシーおよび運用規程に定める手続きにより申請するものとする。

5 運用責任者は、第 3 項の申し出を受けたときあるいは前項による申請で電子証明書が再発行されたときは、IC カードあるいは電子証明書を利用する上での安全性の確認を行った後、速やかに IC カードの再発行あるいは電子証明書の再格納を行うものとする。

C2603-14（雑則）

第十四条 この規程に定めるもののほか、アカウントの利用に関し必要な事項は、別に定める。

C2651 証明書ポリシー（CP）

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A2651	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2013年7月5日 B2651	文書番号の変更のみ	ー
2015年10月9日 C2651	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

大学等高等研究機関で運用する PKI（Public Key Infrastructure）のための認証局において策定すべき証明書ポリシー（CP：Certificate Policy）のサンプルについては、UPKI イニシアティブが策定・公開している以下の文書を参照のこと。

解説：学外との認証連携に学認を利用する場合、自機関において本ポリシーの策定は不要である。

UPKI 共通仕様書（UPKI イニシアティブ）
https://upki-portal.nii.ac.jp/upkispecific/

1) UPKI 共通仕様　利用の手引き
2-1) キャンパス PKI CP/CPS ガイドライン
2-2) キャンパス PKI CP/CPS テンプレート（フルアウトソース編）
2-3) キャンパス PKI CP/CPS テンプレート（IA アウトソース編）
3-1) キャンパス PKI 調達仕様ガイドライン
3-2) キャンパス PKI 調達仕様テンプレート（フルアウトソース編）
3-3) キャンパス PKI 調達仕様テンプレート（IA アウトソース編）

C2652 認証実施規程（CPS）

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A2652	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2013年7月5日 B2652	文書番号の変更のみ	ー
2015年10月9日 C2652	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

大学等高等研究機関で運用する PKI（Public Key Infrastructure）のための認証局において策定すべき認証実施規程（CPS：Certification Practice Statement）のサンプルについては、UPKI イニシアティブが策定・公開している以下の文書を参照のこと。

解説：学外との認証連携に学認を利用する場合、自機関において本規程の策定は不要である。

UPKI 共通仕様書（UPKI イニシアティブ）
https://upki-portal.nii.ac.jp/upkispecific/

1) UPKI 共通仕様　利用の手引き
2-1) キャンパス PKI CP/CPS ガイドライン
2-2) キャンパス PKI CP/CPS テンプレート（フルアウトソース編）
2-3) キャンパス PKI CP/CPS テンプレート（IA アウトソース編）
3-1) キャンパス PKI 調達仕様ガイドライン
3-2) キャンパス PKI 調達仕様テンプレート（フルアウトソース編）
3-3) キャンパス PKI 調達仕様テンプレート（IA アウトソース編）

C3100 情報システム運用･管理手順の策定に関する解説書

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3100	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3100	文書構成と文書番号の見直しへの対応	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

本書は、「C2101 情報システム運用・管理規程」を実際に適用する際に用いられる、情報セキュリティ対策を円滑に実施するための文書（手順、ガイドライン及びマニュアル等）の策定に関して、概要を解説するものである。

１．文書構成

情報システムの運用・管理に係る手順等（C3101～C3104）として、次に掲げる 4 種類の文書を用意した。

C3101 例外措置手順書
C3102 インシデント対応手順
C3103 情報格付け取扱手順
C3104 情報システムリスク評価手順

ポリシー及び関連する実施規程に従い、実際に情報システムを運用・管理する場合、情報セキュリティ維持のためにとるべき対策は多岐にわたる。そのためサンプル規程集では、個々の場面場面に応じて、そこで遵守すべき事項を複数の文書に定めることとした。これらの文書の他、さらに具体的な操作マニュアルとして、例えば次のような文書を整備することも考えられる。

・オペレーティング・システム設定手順（Windows®、Linux®、FreeBSD®等）
・ソフトウェア設定手順（DNS、SMTP、POP/IMAP、FTP、HTTP、SSL、SSH、VPN、IPFW 等）
・通信機器設定手順（ファイアウォール、ルータ、ハブ等）

あらかじめ詳細な手順を定めておくことで、情報システムを運用・管理する者が実施すべき事項が明確となり、情報セキュリティの向上につながる。ただし、実施規程や手順として定めた場合、そこには当然強制力が働くため、実施規程・手順のレベルで定めるか、ガイドライン・マニュアルのレベルで定めるかについては、慎重に検討する必要がある。

２．情報システムの運用・管理に係る手順等（C3101～C3104）の概要

(1) C3101 例外措置手順書

大学の業務を遂行するに当たって、ポリシー及び関連する実施規程・手順が業務の適正な遂行を著しく妨げる等の理由により、そこに規定された方法とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合がある。こうした場合において、情報セキュリティを維持しつつ柔軟に対応できるようにするための例外措置を定める。

(2) C3102 インシデント対応手順

災害等によるネットワーク設備の損壊、利用者等による規定違反や学外から学内への攻撃行為等により発生したインシデントへの対応について、具体的な対応手順を定める。インシデントが

発生した場合、適切な対応によりインシデントの影響が拡大することを防ぐと共に復旧を図ることが必要である。対応を誤ると無用な被害の拡大を招くことが懸念されるため、インシデントの発見から対処にいたる手続きを定め、適切な対処を実施することが必要である。

(3) C3103 情報格付け取扱手順

情報システムで取り扱う情報は格付けされ、格付けに応じて適切に取り扱う必要がある。取扱いが不適切なため、機密性が求められる情報の漏えい、完全性が求められる情報の改ざん等が生じた場合には、大学活動の停止や社会的信用の失墜の要因となる可能性もある。このようなリスクを軽減するため、教職員等が情報を適切に取り扱うために必要な事項を定める。

(4) C3104 情報システム運用リスク評価手順

情報システムを適切に運用し管理するためには、情報システムに対するさまざまなリスクに応じて、適切かつ効率的、あるいは実現可能なセキュリティ対策を実施する必要がある。そうしたリスクを検討するための手順として、情報資産の洗い出し、脆弱性分析、資産価値判断、脅威の判断、リスク値の算出、対策の必要性判断について定める。

３．情報システムの運用・管理に係る手順等（C3101～C3104）の使い方

これらの文書は、各大学が情報システムの運用・管理に係る実施手順等を作成する際の参考資料として提供されるものであり、実際の各大学の実施手順等がこれと同一の内容で作成されるものではない。各大学においては、サンプル規程集で定められた以上の情報セキュリティ確保を目標としながら、各大学の状況や特性を踏まえつつ、これらの文書を参考として実施手順等を策定する。文書の使い方として、本文書をそのまま取り込む、構成や表現を変えて盛り込む
等の方法がある。

４．事務情報セキュリティ対策基準との関係

サンプル規程集では、事務局管理の情報及び情報システムと、その他の大学の研究教育業務に係る情報及び情報システムとで、規程体系を二分している。すなわち、「C2101 情報システム運用・管理規程」には本文書及び C3101～C3104 の各手順が対応するのに対して、「C2501 事務情報セキュリティ対策基準」には「C3500 各種マニュアル類の策定に関する解説書」が対応する。事務情報システムに関連する文書（手順、ガイドライン及びマニュアル等）については、「C3500 各種マニュアル類の策定に関する解説書」を参照されたい。

C3101 例外措置手順書

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3102	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3102	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

1. 目的

本学における大学業務を遂行するに当たって、ポリシー・実施規程・手順の適用が大学業務の適正な遂行を著しく妨げる等の理由により、ポリシー・実施規程・手順とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合がある。

こうした場合においても、あらかじめ定められた例外措置のための手続により、情報セキュリティを維持しつつ柔軟に対応できなければ、ポリシー・実施規程・手順の実効性を確保することは困難となる。

本書は、教職員等が例外措置の適用を希望する場合の手続を定め、もって例外措置において必要な情報セキュリティ水準を確保することを目的とする。

2. 本手順書の対象者

本書は、すべての教職員等を対象としている。

3. 定義

本書における用語の定義は次のとおりである。

(1) 「例外措置」とは、教職員等がその実施に責任を持つポリシー・実施規程・手順を遵守することが困難な状況で、大学業務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

(2) 「申請者」とは、例外措置の適用を申請する者をいう。

(3) 「許可権限者」とは、例外措置の適用を審査する者をいう。

(4) 「代替措置」とは、例外措置の適用に伴い発生するリスクを低減するためにポリシー・実施規程・手順が定める内容とは異なる代替のセキュリティ対策をいう。

4. 格付け及び取扱制限の手順

4.1 許可権限者

(1) ポリシー・実施規程・手順の遵守事項に対する例外措置の許可権限者を下記に定める。

申請者 （遵守義務を負うもの）		許可権限者	
		通常の場合	その他
全学総括責任者		全学情報システム運用委員会	ポリシー・実施規程・手順の遵守事項に被報告者、被届出者、被返還者、被許可者、承認者、判断者がある場合は当該者
全学情報システム運用委員会		全学総括責任者	
全学実施責任者		全学総括責任者	
情報セキュリティ監査責任者		全学総括責任者	
情報セキュリティ監査を実施する者		情報セキュリティ監査責任者	
部局総括責任者		全学実施責任者	
部局技術責任者		部局総括責任者	
部局技術担当者		部局技術責任者	
職場情報セキュリティ責任者(上司)		部局総括責任者	
教職員等	[情報セキュリティ要件の明確化に基づく対策と情報システムの構成要素についての対策]に係る事項	部局技術責任者	
	上記以外の事項	職場情報セキュリティ責任者(上司)	

（注）上記にかかわらず、必要がある場合は、当該許可権限者の上位を許可権限者とする。

5. 例外措置の申請

5.1 前提条件

(1) 申請者は、以下の場合に、例外措置の申請を行わなければならない。
・部局固有の手順を作成するに当たって、ポリシー及び実施規程の遵守事項への準拠性を満足できない場合
・情報、情報システムを取扱う業務を遂行するに当たって、ポリシー・実施規程・手順の遵守事項への準拠性を満足できない場合

(2) 申請者は、例外措置を申請する理由と例外措置の実施により想定される被害の大きさと影響を検討・分析した上で、例外措置の申請を行わなければならない。

5.2 事前申請の原則

例外措置の申請は、原則として事前に行わなければならない。

5.3 事前協議の原則

他の組織と関連のある事項は、事前に協議し、調整を行った上で例外措置の申請を行わなければならない。

5.4 例外措置の申請

申請者は、付録に示す例外措置申請書に以下の事項を記入し押印した上、許可権限者に提出する。

(1) 申請日

(2) 申請者の氏名、所属、連絡先

(3) 例外措置の適用を申請するポリシー・実施規程・手順の適用箇所（規程名と条項等）

(4) 例外措置の適用を申請する期間

(5) 例外措置の適用を申請する措置内容（講ずる代替手段等）

(6) 例外措置の適用を終了したときの報告方法

(7) 例外措置の適用を申請する理由

5.5 関係書類の添付

申請者は、申請内容を明確化するために参考資料が必要となる場合、これを添付する。またやむを得ない事情で、事後申請となった場合は、経緯書を添付する。

6. 例外措置の審査

6.1 例外措置の申請の受理

(1) 例外措置の申請を受理した許可権限者は、リスクを分析し、それに対する意見を記述する。

(2) 許可権限者は、必要がある場合は、例外措置申請書を上位の許可権限者に回付する。

6.2 審査の手続

(1) 当該例外措置申請に対する許可権限者は、速やかに審査手続を実施し、例外措置申請書に以下の事項を記載する。

- 申請を審査した者の情報（氏名、役割名、所属、連絡先）
- 審査決定日
- 審査結果の内容
  - 許可又は不許可の別（許可の場合、許可番号）
  - 許可又は不許可の理由
  - 例外措置の適用を許可したポリシー・実施規程・手順の適用箇所（規程名と条項等）
  - 例外措置の適用を許可した期間
  - 許可した措置内容（講ずるべき代替手段等）
  - 終了報告の方法

(2) 許可権限者は、例外措置申請書に対して疑義又は意見のある際は、その旨の意見書を添

付する。

6.3 審査基準

許可権限者は、以下の条件をいずれも満たした場合に限り、例外措置の適用を許可すること。

(1) ポリシー・実施規程・手順の遵守事項を実施しないことについて、合理的理由があると認められるとき。

(2) ポリシー・実施規程・手順の遵守事項とは異なる代替の方法を採用する場合に、当該方法を採用した場合に想定される被害の大きさ・影響と採用しなかった場合の大学業務遂行への影響を比較、検討、分析した上で、その内容及び期間につき合理的理由があると認められるとき。

6.4 審査結果の通知

許可権限者は、例外措置申請書の副本を作成し、申請者に副本を返却して、審査結果を通知する。

6.5 例外措置の効力

例外措置は、例外措置の適用許可期間の開始日より効力を生ずる。ただし、承認された事項が次の各号のいずれかに該当した場合はその効力を失う。

(1) 適用を許可された期間を終了した場合

(2) 許可後、半年以内に実施できない場合

(3) 実施後、一時中断して、その中断期間が半年以上に及ぶ場合

7. 例外措置の適用

7.1 例外措置の関係者への周知

(1) 許可権限者は、適用した例外措置を、教職員等が参照可能な状態としておく。

7.2 例外措置の適用期間中のリスク管理

(1) 申請者は、例外措置によって行われる代替措置が暫定的な措置であることを認識し、その適用期間中におけるリスク管理に留意する。

8. 例外措置の修正

8.1 例外措置の修正

(1) 申請者は、許可された例外措置が以下に該当する場合は、速やかに許可権限者に例外措置申請書の修正申請を提出して承認を得る。

・許可された措置内容に大きな変更を加える場合

・例外措置の適用期間を延長する場合

(2) 申請者は、想定される被害の大きさと影響に変更がある場合は、必要に応じて別途の代替措置を適用し、速やかに許可権限者に例外措置申請書の修正申請を提出して承認を得る。

9. 例外措置の終了

9.1 終了の報告

申請者は、例外措置の適用終了時、速やかに許可権限者に付録に示す例外措置終了報告書を提出して確認を得る。ただし、許可権限者が報告を要しないとした場合は、この限りではない。

9.2 終了報告の確認

許可権限者は、例外措置の適用期間が終了した月の月末に例外措置終了報告書の提出の有無を確認する。ただし、報告を要しないとした場合は、この限りではない。

10. 例外措置の管理

10.1 例外措置の適用審査記録の管理

審査された例外措置申請書の正本は許可権限者が管理し、申請者に返却された副本は申請者が管理する。

10.2 例外措置の適用審査記録の提出

許可権限者は、毎月１回例外措置申請書の副本をもう一部作成し、全学総括責任者に提出する。

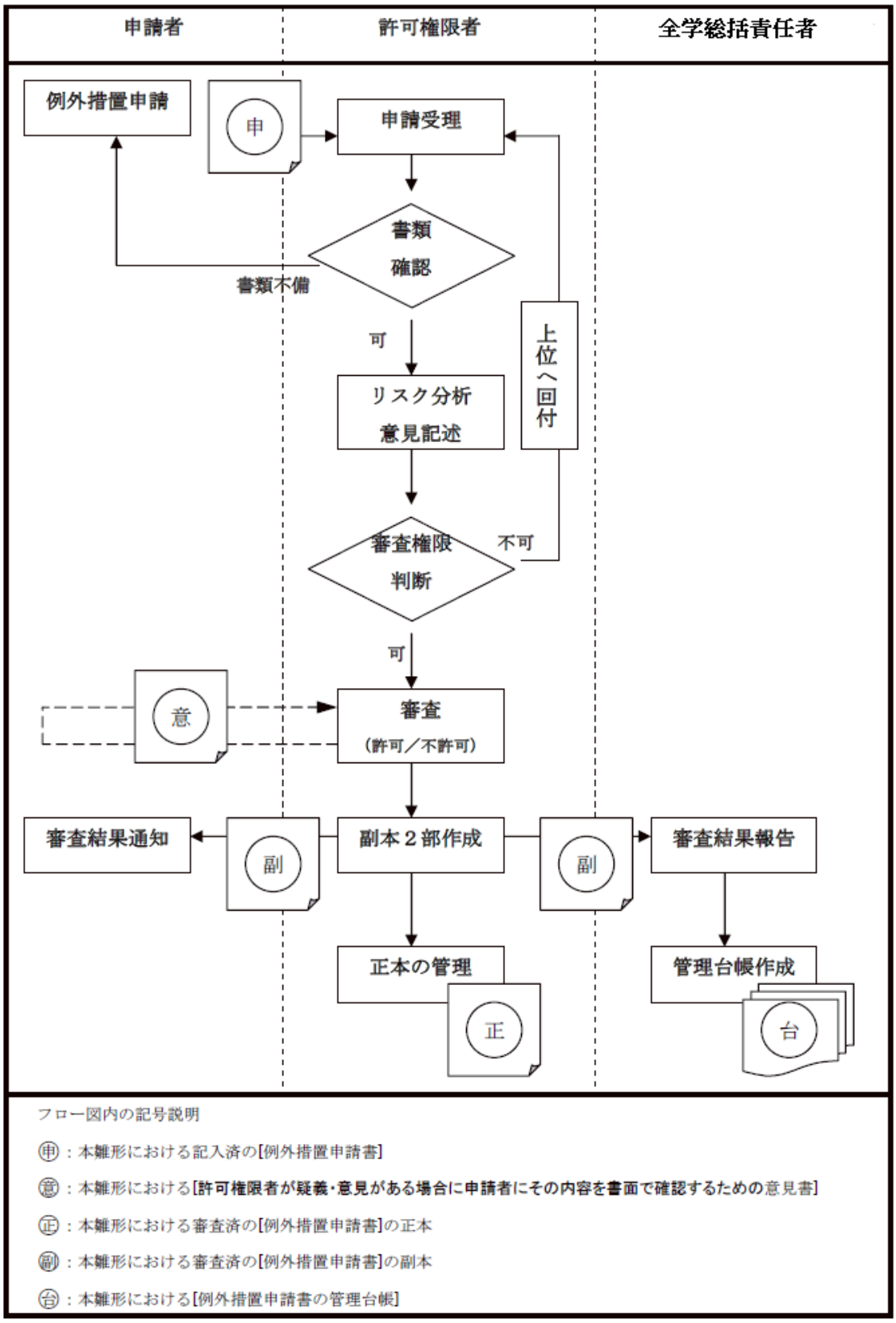
10.3 全学総括責任者による例外措置の適用審査記録の保管

全学総括責任者は、許可権限者から提出された例外措置申請書の副本を例外措置申請書の管理台帳として保管し、情報セキュリティ監査を実施する者からの申請に応じて閲覧を許可する。

11. 事務手続の代行

(1) 許可権限者は、書類の受付、書類の形式要件確認、書類の回付及び管理に関わる事務手続を、あらかじめ指定した総務担当者に行わせることができる。

付図 例外措置業務フロー



付録

例外措置申請・終了報告書

【申請・報告者記入欄】

申請・報告日 ※	年 月 日	所属 ※		印
適用開始希望日	年 月 日	氏名 ※		
適用終了希望日 ※	年 月 日	連絡先 ※	tel: mail:	
申請・報告の種別	(□新規 □延長 □修正 □終了報告)	適用許可番号 ※		
申請・報告対象規程	規程名称 ※			
	規程項番 ※			
申請・報告対象システム名 ※				
申請理由	【希望する例外措置終了時の報告方法 ：（ □ 報告書提出 □ メール連絡 □ その他_____）】			
申請する代替措置の内容				

【許可権限者記入欄】

決定結果	（ □許可 □不許可 ）	所属・役割 ※		印
適用許可期間	年 月 日～ 年 月 日	氏名 ※		
適用許可番号		連絡先 ※	tel: mail:	
適用対象規程	規程名称			
	規程項番		関係する手順の項番	
許可対象システム名				
決定理由				
許可する代替措置の内容				
適用終了後の措置	適用延長有無 ※	（□有 □無）	終了報告	（ □要 □否 ）
	適用終了日 ※	年 月 日	報告方法	（□報告書提出 □メール連絡 □ その他_____）

【申請書受理者記入欄】

本案件のリスク分析に対する意見

(注) 終了報告書として使用する場合は※欄について記載する。なお、適用終了日は「適用終了希望日」欄に記入。
新規の申請の場合、申請者による「適用許可番号」の記入は不要。

許可権限者記入欄			
受付日	審査決定日	申請書返却日	終了確認日 ※
. .	. .	. .	. .

C3102 インシデント対応手順

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A3103	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A3103	参考（インシデント対応手順にもとづくインシデント報告・承認要領）と解説を追加	国立大学法人等における情報セキュリティポリシー策定作業部会
2011年3月31日 A3103	参考2（インシデント対応手順による学外クレーム対応時の留意点）を追加	丸橋透（ニフティ）
2015年10月9日 C3102	刑法改正等への対応のための修正	丸橋透（ニフティ）
2017年10月17日 C3255	C1101（CSIRT運営規程）との整合性を確保するための修正	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：災害等によるネットワーク設備の損壊、利用者等による規定違反や学外から学内への攻撃行為等により発生したインシデントへの対応については、あらかじめ実施要領や対応マニュアルに具体的な手順を明記しておかなければならない。各高等教育機関においては、それぞれの実情に即して対応手順を個別に定めることになるだろう。具体的な対応については、以下のとおり物理的インシデント・セキュリティインシデント・コンテンツインシデントとで分けて考えるべきである。また、部局内の対応と全学の対応の分担と当事者の権限を明確にし、迅速な対処と、慎重な検討とを両立させることが必要である。なお、ネットワークをめぐる問題は多種多様であり、すべての対応を網羅的に定めることは難しいかもしれない。ポリシーの見直しが行われる際は、規定違反行為等への対応についても、実際の運用経験を反映させた見直しが行われるべきである。
なお、A 大学におけるインシデント発生時の連絡窓口は A 大学 CSIRT（情報セキュリティインシデント対応チーム。本文書では「CSIRT」として表記。）であり、その運営については別途 C1101（情報セキュリティインシデント対応チーム（CSIRT）運営規程）にて規定している。

1. 定義

(1) 物理的インシデント

地震等の天災、火災、事故、盗難等によるネットワークを構成する機器や回線の物理的損壊や滅失及びその他の物理的原因による情報システムやネットワークの機能不全や障害等、情報セキュリティの確保が困難な事由の発生およびそのおそれを言う。

(2) セキュリティインシデント

ネットワークや情報システムの稼動を妨害し、またはデータの漏えい、改ざんや消失を起こす行為及び利用行為の形態自体には問題は無いが、ネットワークの帯域やディスクや CPU の資源を浪費するなど、ネットワークやシステムの機能不全や障害または他の利用者の迷惑となる行為による情報セキュリティの確保が困難な事由の発生およびそのおそれを言い、下記原因によるものを含む。

－大量のスパムメールの送信
－コンピュータウイルス等のマルウェアの蔓延や意図的な頒布
－発信者を偽った電子メールへのファイル添付や偽装した URL への誘導などにより、利用者の環境に利用者の意図しないアプリケーション等をインストールさせる行為
－情報システムの脆弱性や利用者による不適切なアカウント管理等を利用することにより、ネットワークや情報システムのセキュリティに影響を及ぼす行為
－不正アクセス禁止法に定められた特定電子計算機のアクセス制御を免れる行為
－サービス不能攻撃その他部局総括責任者の要請に基づかずに管理権限のない情報システムのセキュリティ上の脆弱性を検知する行為
－利用規定により禁止されている形態での P2P ソフトウェアの利用
－禁止された方法による学外接続
－学内ネットワークへの侵入を許すようなアカウントを格納した PC の盗難・紛失
－管理上の過失による秘密情報（個人情報を含む）の漏えい、データの消失または改ざん

(3) コンテンツインシデント

ネットワークを利用した情報発信内容（以下「コンテンツ」という）が著作権侵害等の他人の権利侵害や児童ポルノ画像の公開等の違法行為または公序良俗違反である行為(及びその旨主張する被害者等からの請求）による事故を言い、下記原因を含む。

－ソーシャルネットワーキングサービス（電子掲示板、ブログ等を含む）やウェブページ等での他人及び本学の名誉・信用毀損にあたる情報の発信
－他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信
－通信の秘密を侵害する行為
－他人の著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信
－秘密であるデータやプログラムの不正公開等守秘義務に違反する情報の発信
－児童ポルノやわいせつ画像の公開
－ネットワークを利用したねずみ講
－差別、侮辱、ハラスメントにあたる情報の発信
－営業ないし商業を目的とした本学情報システムの利用行為

(4) インシデント

物理的インシデント、セキュリティインシデントまたはコンテンツインシデントを言う。

(5) 対外的インシデント

インシデントのうち、利用者等による行為であって、外部ネットワークにおけるあるいは外部のシステムに対して行われた行為による事故、事件を言う。

(6) 対内的インシデント

インシデントのうち、外部のネットワークから内部に向かって行われた行為による事故、事件を言う。

(7) 学外クレーム

学内の利用者等による情報発信行為（本学の業務としてなされたものを除く）の問題を指摘しての連絡・通報及び学外(学内の者が、弁護士等の代理人を立てる場合も含む)からの発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び証拠、証言の収集や犯罪捜査等にかかわる協力要請や強制的命令を言う。

(8) 対外クレーム

対内的インシデントに対し、学外の発信者に対して連絡・通報し、または発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び当局に犯罪捜査の告訴・告発をすることを言う。

(9) 運用･管理規程

「C2101 情報システム運用・管理規程」とそれにもとづく手順、命令、計画等を言う。

(10) 緊急連絡網

運用・管理規程に基づき整備された［インシデント/障害等]に備え、特に重要と認めた情報システムについて、その部局技術責任者及び部局技術担当者の緊急連絡先、連絡手段、連絡内

容を含む連絡網を言う。

(11) 学外窓口

インシデントについて学外から連絡・通報を受け、学外への連絡・通報、対外クレームをするための窓口を言う。

(12) 利用規定

「C2201 情報システム利用規程」とそれにもとづく手順、その他本学の情報ネットワークや情報システムの利用上のルールを言う。

(13) 利用規定違反行為

インシデントに係わるかどうかに限らず、利用規定に違反する行為を言い、下記を含む。

１　情報システム及び情報について定められた目的以外の利用
２　電子掲示板、ブログやウェブページ等での名誉・信用毀損にあたる情報の発信
３　差別、侮辱、ハラスメントにあたる情報の発信
４　他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信
５　守秘義務に違反する情報の発信
６　他人の著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信
７　通信の秘密を侵害する行為
８　営業ないし商業を目的とした本学情報システムの利用
９　部局総括責任者の許可（業務上の正当事由）なくネットワーク上の通信を監視し、又は情報機器の利用情報を取得する行為
１０　不正アクセス禁止法に定められたアクセス制御を免れる行為及びそれを助長する行為
１１　部局総括責任者の要請に基づかずに管理権限のないシステムのセキュリティ上の脆弱性を検知する行為
１２　サービス不能攻撃等、故意に過度な負荷を情報システムに与えることにより本学の円滑な情報システムの運用を妨げる行為
１３　その他法令に基づく処罰の対象となり、又は損害賠償等の民事責任を発生させる情報の発信
１４　上記の行為を助長する行為
１５　管理者の許可をえず、ソフトウェアのインストールやコンピュータの設定の変更を行う行為

解説：規定違反行為の内容とその対処方針は、明確に規定されている必要がある。何が規定違反に該当するかを明確にし、利用者等の予見性を高めることによりネットワークの適切な利用が促進されるからである。

2. インシデント通報窓口

(1) インシデント対応のための学外・学内の連絡・通報窓口は下記のとおりとする。

A.　学内窓口：CSIRT
B.　学外窓口：CSIRT／広報部門

(2) 学外窓口への学外からの e-mail による連絡手段は、[緊急連絡網参加者全員が受信可能とする]以下のメーリングリストとし、公表するものとする。
Email: abuse@example.ac.jp

(3) 学外への連絡・通報、対外クレームに当たっては、CSIRT 及び広報部門との連絡を密にし、無断で行わないものとする。

解説：問題発生時の対処を迅速・確実に行うためネットワーク運用と利用の問題についての学外・学内の連絡・通報窓口を設定しておくことが必要である。

連絡窓口は部署別あるいは機能別に複数設置してもよいが、問題の切り分けが効率的にできるならば、一箇所に集中して設け、関連部門の技術責任者や部局技術担当者等、学内への連絡網を整備し情報を配布することでも対応できよう。対外的連絡・通報については、全学広報部門との役割分担を明確にし、情報共有と意思疎通を密接にする必要がある。

メーリングリストのアドレスあるいは自動転送をして関係者で同時に情報共有をすることなども考えられるが、いずれにしても一次対応する責任者を明確にしておく必要がある。

特に、利用者等により違法行為がなされたおそれがあるとする被害者との対応や関連する捜査や取材の対応については、慎重にする必要がある。

3. インシデントの対応判断のエスカレーション手順

(1) CSIRT は、インシデントを認知した場合は、緊急連絡網その他所定の連絡網により、適宜、全学総括責任者、全学実施責任者、部局総括責任者、部局技術責任者、部局技術担当者のうち関係する者にインシデントの初期対応を依頼するものとする。

(2) 情報メディアセンターは、CSIRT との連携のもと、全学ネットワークに関るインシデントについては、必要に応じて自ら技術的対応をするものとし、部局ネットワークにのみ関連するインシデントについては、部局技術責任者を支援するものとする。

(3) 部局技術担当者は、インシデントを発見し、または CSIRT 等を通じて内部・外部からの通報を受けることにより認知した場合、ただちに部局技術責任者に状況報告するものとする。

(4) 部局技術責任者は、インシデントを自ら認知するか部局技術担当者から状況報告を受けた場合、下記の基準により一次切り分け判断を行うものとする。

① 部局内ネットワークに閉じた技術的問題か

i) 物理的インシデントまたはセキュリティインシデントの場合で、対外的インシデント及び体内的インシデントのいずれでも無く、部局内ネットワークにのみ影響が生じている場合、部局技術担当者に対策を指示し、対策結果を部局総括責任者に状況報告する。

ii) i)以外の場合、部局総括責任者を通じて全学実施責任者に状況報告をし、CSIRT 及び情報メディアセンターの支援を仰ぎながら、物理的インシデントまたはセキュリティインシデント対応のプロセスを実施する。

② コンテンツインシデントか

i) コンテンツインシデントの場合、加害者と被害者が部局内に閉じている場合であっても、法律的対策を講じる必要があるため、原則として部局総括責任者を通じて全学実施責任者に報告をし、CSIRT 等の支援を仰ぎながら、ログの保全等、必要な技術的措置を取るものとする。

ii) ただし、爆破予告・自殺予告など、生命・身体への危険等の緊急性がある場合で、部局内での対処が可能な場合は、コンテンツに関する緊急対応を実施の上、部局総括責任者と全学実施責任者に結果報告をする。

(5) 部局技術責任者は、あらかじめ定められた手順に従って、緊急な技術的対応が必要なときは部局技術担当者に指示を与え、部局総括責任者に対応結果を報告する。法的に慎重な判断を要する場合は、対応を実施する前に必ず部局総括責任者に報告し、指示を受けることとする。

(6) 部局技術責任者から報告を受けた部局総括責任者は、コンテンツインシデントについて、部局技術責任者・部局技術担当者を指揮監督する。セキュリティインシデント対応については、ポリシーに基づいて全学実施責任者に指示や承認を求める。また、法的判断を要する問題については、法務担当部門に対応を依頼する。

(7) 学外クレームか、対外クレームか

① 全学実施責任者は、学外クレームにより認知したインシデントの場合、学外クレーム対応プロセスを併せて実施する。

② 全学実施責任者は、法務担当部門に相談しながら、必要に応じて対外クレーム対応を実施するものとする。

③ 学内問題として処理可能であるインシデントは、通常の技術的対応または利用規定違反対応とする。

解説：インシデントについて、部局技術責任者が発見あるいは通報によって認知した場合の対応手順は、あらかじめ管理者向けマニュアルに明示しておかなければならない。

インシデントが発生した場合の報告･申請等の手続きに利用する様式および、当該様式を利用した報告・記録・申請・承認の要領については、「インシデント報告･承認要領」及び別紙を参照すること。

コンテンツインシデントについては、慎重な法的判断を要することが多く、また通信の秘密あるいはプライバシー保護の観点から、部局技術責任者と部局技術担当者が立ち入ることが適当でない場合が少なくないため、部局技術責任者がコンテンツインシデントと判断した場合は、部局総括責任者に一次判断を求めるものとする。一方、セキュリティインシデントに関する問題については、利用規定違反の判断が比較的容易であること、被害の拡大防止のために緊急の技術的対応が必要となる場合も少なくないことなどから、部局技術責任者と部局技術担当者の一次判断が重要となる。

インシデントと影響範囲による役割・責任分担例

インシデントと影響範囲による責任分担

インシデント分類	物理／セキュリティ		コンテンツ	
影響範囲	対外・全学	部局	対外・全学	部局
全学実施責任者 （非常時対策本部）	◎▲	----------	◎▲	◎（定形以外）
CSIRT	○	○	○	○（定形以外）
情報メディアセンター （非常時窓口）	○	○		
部局総括責任者		◎		○(定形のみ◎)
部局技術責任者	△	▲（定形のみ◎）	△	△（定形のみ▲）
部局技術担当者	△	△	△	△

◎インシデント総括　○判断・技術支援　▲技術対応判断　△技術対応実施

4. 物理的インシデント発生時の対応

(1) 発生から緊急措置決定まで

(ア) 通報・発見等で物理的インシデントの可能性を認知した部局技術担当者は、事実を確認するとともに部局技術責任者に報告し、被害拡大防止のための緊急措置の必要性について判断を求めるものとする。

(イ) 部局技術担当者は、後日の調査に備え、物理的インシデント発生時の状況に関する記録を作成し、ネットワーク運用に影響があるおそれがある場合、バックアップデータの作成、ハードディスクのイメージの保存等を行う。

(2) 被害拡大防止の応急措置の実施

(ア) 部局技術責任者は、個別システムの停止やネットワークからの遮断、機器の交換、ネットワークの迂回等の緊急措置の必要性を判断し、実施を部局技術担当者に指示する。

(イ) 利用者等による対処が必要な場合には、その旨命令する。

(3) 緊急連絡及び報告

(ア) 部局技術責任者は、緊急の被害拡大防止措置を実施する場合は、部局総括責任者に報告する。

(イ) 部局総括責任者は、被害拡大防止措置が全学ネットワークに影響が及ぶと判断するときは CSIRT に報告する。

(ウ) 全学実施責任者は CSIRT を通じて、緊急措置の実施により影響を受ける利用者等へ連絡するとともに、全学総括責任者の指示を仰いだ上で、必要に応じ非常時対策本部を組織する。

(エ) CSIRT は全学実施責任者または非常時対策本部の指示に基づき、関係するネットワークへの連絡、外部広報などを行う。

(オ) 非常時対策本部が設置された場合、CSIRT、部局総括責任者、部局技術責任者及び部局技術担当者は、その指示に従うものとする。

(4) 復旧計画

(ア) 部局技術担当者は、物理的インシデントによる被害や緊急措置の影響を特定し、システムやネットワークの復旧計画を立案する。

(イ) 部局技術責任者は、復旧計画を検討し、部局総括責任者の承認を得て実施する。

(5) 原因調査と再発防止策

(ア) 部局技術担当者は、物理的インシデント発生の要因を特定し、再発防止策を立案する。

(イ) 部局技術責任者は、利用者等への注意喚起等を含めた再発防止策を検討し、部局総括責任者は検討結果に基づき再発防止策を策定する。

(ウ) 部局技術担当者と部局技術責任者は、インシデント対応作業の結果をまとめ、部局総括責任者は、再発防止策とともに全学情報システム運用委員会に報告するとともに、必要によりポリシーや実施手順の改善提案を行う。

(エ) 全学実施責任者は、部局総括責任者から物理的インシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずる。

解説：セキュリティインシデント発生時の対応に準ずる一方、全学の災害等における事業継続計画（BCP：Business Continuity Plan）や非常時行動計画と整合性をとる必要がある。

5. セキュリティインシデント発生時の対応

⑴ 発生から緊急措置決定まで

(ア) 監視システムによるセキュリティインシデントの可能性を示す事象の検知や、通報等でセキュリティインシデントの可能性を認知した部局技術担当者は、事実を確認するとともに部局技術責任者に報告し、被害拡大防止のための緊急措置の必要性について判断を求めるものとする。

(イ) 部局技術担当者は、後日の調査に備え、セキュリティインシデント発生時の状況、例えばログイン状況、ネットワーク接続や手順の稼働状況に関する記録を作成し、バックアップデータの作成、ハードディスクのイメージの保存等を行う。

(ウ) セキュリティインシデントが、外部からの継続している攻撃等であって攻撃元ネットワークの管理主体等への対処依頼が必要な場合、部局総括責任者の承認を得て部局技術責任者から相手方サイトへの対処依頼を行う。

⑵ 被害拡大防止の応急措置の実施

(ア) 部局技術責任者は、個別システムの停止やネットワークからの遮断（他の情報システムと共有している学内通信回線又は学外通信回線から独立した閉鎖的な通信回線に構成を変更する等）等の緊急措置の必要性を判断し、実施を部局技術担当者に指示する。

(イ) 部局総括責任者および部局技術責任者は、情報システムのアカウントの不正使用の報告を受けた場合には、直ちに当該アカウントによる使用を停止させるものとする。

(ウ) 部局技術責任者は、利用者等による対処が必要な場合には、その旨命令する。

⑶ 緊急連絡及び報告

(ア) 部局技術責任者は、緊急の被害拡大防止措置を実施する場合は、部局総括責任者に報告する。

(イ) 部局総括責任者は、被害拡大防止措置が全学ネットワークに影響する場合は、部局総括責任者は学内窓口を通じて全学実施責任者に連絡する。
(ウ) 全学実施責任者は、CSIRT を通じて、緊急措置の実施により影響を受ける利用者等に被害拡大防止措置を連絡するとともに、全学総括責任者の指示を仰いだ上で、必要に応じ非常時対策本部を組織する。
(エ) CSIRT は、全学実施責任者または非常時対策本部の指示に基づき、攻撃元サイトや関係するサイトへの連絡、及び関係機関への報告などを指揮する。
(オ) 非常時対策本部が設置された場合、CSIRT、部局技術責任者及び部局技術担当者は、その指示に従うものとする。

(4) 復旧計画
(ア) 部局技術担当者は、セキュリティインシデントの被害や緊急措置の影響を特定し、システムやネットワークの復旧計画を立案する。
(イ) 部局技術責任者は、復旧計画を検討し、部局総括責任者（全学ネットワークに影響する場合は全学実施責任者）の承認を得て実施する。

(5) 原因調査と再発防止策
(ア) 部局技術担当者は、セキュリティインシデント発生の要因を特定し、再発防止策を立案する。
(イ) 部局技術責任者は、利用者等への注意喚起等を含めた再発防止策を検討し、部局総括責任者（全学ネットワークに影響する場合は全学実施責任者）の承認を得て実施する。
(ウ) 部局技術担当者と部局技術責任者は、インシデント対応作業の結果をまとめ、部局総括責任者は、再発防止策とともに全学実施責任者に報告するとともに、必要によりポリシーや実施規程の改善提案を行う。
(エ) 全学実施責任者は、部局総括責任者からセキュリティインシデントについての報告を受けた場合には、その内容を検討し、全学総括責任者の承認を仰ぎ、再発防止策を実施するために必要な措置を講ずる。

解説：セキュリティインシデントに対して、技術的対応とともに重要となるのが、事後の対応による見直しである。組織においていかに技術的対応を強固にしても、組織をインターネットに接続する限り常に情報セキュリティ上の脅威は存在しているのであって、潜在的かつ必然的にインシデントに対応しなければならない状況にあることをまず理解しなければならない。

JPCERT/CC によるセキュリティインシデントの対応手順の例は以下の通りである。

・手順の確認
・作業記録の作成
・責任者、担当者への連絡
・事実の確認
・スナップショットの保存
・ネットワーク接続やシステムの遮断もしくは停止
・影響範囲の特定
・渉外、関係サイトへの連絡

・要因の特定
・システムの復旧
・再発防止策の実施
・監視体制の強化
・作業結果の報告
・作業の評価、ポリシー・運用体制・運用手順の見直し

JPCERT/CC 技術メモーコンピュータセキュリティインシデントへの対応
JPCERT-ED-2002-0002 (Ver. 04)
http://www.jpcert.or.jp/ed/2002/ed020002.txt を参照のこと。

6. コンテンツインシデントに関する緊急対応

(1) 部局技術担当者は、生命・身体への危険の可能性を示唆するコンテンツ（殺人、爆破、自殺の予告等）を発見し、または通報等により認知した場合、部局技術責任者の指示によりコンテンツの情報発信元を探知し、その結果を部局技術責任者に報告するものとする。

(2) 部局技術責任者は、部局総括責任者にコンテンツの情報発信元の探知結果を報告し、学内緊急連絡についての指示を求める。

(3) 部局総括責任者は、全学実施責任者に、学内緊急連絡についての指示を仰ぐ。その際、広報、保護者、警察への連絡等の学内規則に従う。

7. 学外クレーム対応

(1) 原則
(ア) 学外クレームを受けた場合で、請求の法律的な効果や指摘されたコンテンツや行為の違法性の判断を要するときは、あらかじめ対応手順が明確になっていない限り、必ず法律の専門家に相談するものとする。
(イ) 部局技術責任者は、学外クレームについては、部局総括責任者及び全学実施責任者に報告を行ものとする。
(ウ) 学外クレームについての報告を受けた全学実施責任者は、全学総括責任者の承認を仰ぎ必要に応じ非常時対策本部を設置するものとする。
(エ) 全学実施責任者または非常時対策本部は、攻撃先サイトや関係するサイトへの連絡、外部広報、及び関係機関への報告などを指揮し、部局技術責任者及び部局技術担当者は、その指示に従うものとする。

(2) 利用者等のコンテンツの違法性を主張した送信中止・削除の要求
(ア) 発信元利用者等の特定
学外クレームが利用者等により不特定多数に宛て情報発信されたコンテンツの違法性や情報発信による権利侵害を主張してコンテンツの送信中止や削除の要求が被害を主張する者またはその代理人からなされたものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。

(イ)（通常手続き）コンテンツを発信した利用者等への通知と削除

a. 指摘されたコンテンツの違法性の判断が困難な場合、プロバイダ責任制限法第 3 条第 2 項第 2 号に基づき利用者等に請求があった旨通知し、通知後 7 日以内に利用者等から反論がない場合は、送信中止あるいは削除を実施するものとする。

b. 有効と思われる反論があった場合は、その旨、削除請求者に伝えるとともに、当事者間での紛争解決を依頼する。

(ウ)（緊急手続き）利用者等への通知前の一旦保留

a. 指摘されたコンテンツの違法性が疑いもなく明らかと判断できる場合、一旦利用者等のコンテンツの送信を保留し、その旨利用者等に伝えるものとする。有効な反論があればコンテンツ送信を復活するものとする。

b. 本手続きの対象は、著名な音楽 CD の丸写しや個人の住所や電話の暴露等、権利侵害の疑いが濃厚である場合、緊急な救済の必要性がある場合のみとする。

c. 本緊急手続が適用されることもあることは具体的に利用規定として明示する等、利用者等に周知するものとする。

解説：「プロバイダ責任制限法ガイドライン等検討協議会」の各ガイドラインを参照。
http://www.telesa.or.jp/consortium/provider

(3) 利用者等の発信したコンテンツの刑事的違法性の指摘及び送信中止・削除の要求

(ア) 利用者等の発信したコンテンツが刑事法上違法な可能性の高い旨指摘された場合で、名誉毀損や、著作権侵害等、被害者が存在する犯罪については、（２）と同様の手順を取るものとする。

(イ) わいせつ物陳列罪等、被害者のいない犯罪が外部クレームにより指摘された場合、

a. 部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。

b. 発信元利用者等に犯罪であるとする指摘があった旨通知し、7 日を経過しても利用者等から反論がない場合は、送信中止あるいは削除を実施する。

解説：情報内容についての刑事的な違法性判断は困難な場合が多く、基本的には、発信元利用者等の反論を待ってから送信防止措置を講ずることとする。

(4) 利用者等の行為（コンテンツ以外）の違法性を主張した送信中止・アカウント削除等の要求

i)（通常の対応）通信を発信した利用者等への通知とアカウント停止

- 学外クレームが利用者等による１対１の情報発信による権利侵害等による被害を主張して情報発信の中止を要求するものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。
- 事実確認を行い、特定できた利用者等に対し、問題の通信の発信を中止するよう通知する。これには再度行った場合には関連するアカウントを停止する旨警告することを含む。
- 利用者等から有効な反証があれれば、関連するアカウントの一時停止を解除する。
- 念書をとるなどの対応の後、アカウントの復活手続きを行う。
- 同様の手順を経て再発が確認できた場合には、Ａ大学の処罰の手順に移行する。

ii)（セキュリティインシデント対応）利用者等のアカウントの一時停止

- 学外クレームが利用者等による１対１の情報発信によるセキュリティインシデントによる被害を主張して情報発信の中止を要求するものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。
- 部局技術担当者は、事実を調査し、発信元利用者等を特定する。
- 部局技術担当者は、利用者等の行為がセキュリティインシデントの原因であると判断するのに十分な理由がある場合には、部局技術責任者に報告し、その判断を求めるものとする。
- 部局技術担当者からの報告を受けた部局技術責任者は、必要な場合、利用者等の関連するアカウントを一時停止するとともに、部局情報システム運用委員会に報告する。
- 請求者が連絡を要求しているときには一時停止した旨連絡する。
- アカウントを一時停止した旨利用者等に通知するとともに、再度行った場合には関連するアカウントを停止する旨警告する。
- 利用者等から有効な反証があれれば、関連するアカウントの一時停止を解除する。
- 念書をとるなどの対応の後、アカウントの復活手続きを行う。
- 同様の手順を経て再発が確認できた場合には、Ａ大学の処罰の手順に移行する。

解説：プロバイダ責任制限法第３条は、不特定の者により受信される通信（ウェブサイト、ブログや電子掲示板等によるいわゆる公然性を有する通信）を対象としており、インスタントメッセージやメールのような１対１の通信には適用されない。従って、脅迫メール、特定のメールボックスをターゲットにしたメール爆弾や、特定サーバへのクラッキング等、システムの機能障害を引き起こす通信やコンテンツが問題となる場合であっても特定の者相手の通信には適用がない。

しかし、プロバイダ責任制限法の適用範囲には入らず、免責の対象とはならないとはいえ、学内ネットワークの利用規定が、これらの行為についても手続きを明確にして利用規定違反とし、外部からの送信停止要求についても対応できるようにすることは法律上問題はない。これは学問の自由や表現の自由との関係においても問題が少ないと考えられる。

(5) 損害賠償請求等

（ア）利用者等の情報発信や学外でのネットワークを利用した行為について損害賠償請求や謝罪請求があった場合には、法律の専門家と相談の上、対応するものとする。

（イ）学外クレームに対して、法律的判断をせずに、謝罪することや、その他の約束をしてはならない。

（ウ）利用者等の発信者情報等、連絡先が特定できている場合、損害賠償を請求する相手方には、利用者等との自主的な紛争解決を依頼するものとする。

解説：利用者等の情報発信や学外でのネットワークを利用した行為について損害賠償請求があった場合には、法律の専門家と共に対応する必要がある。

プロバイダ責任制限法第３条第１項により、損害賠償責任の免責を受けられる場合とそうでない場合がある。都立大学事件判決やニフティ事件第二審判決のように、最終的にネットワーク管理者としての損害賠償責任を負わないこととされた事例、ニフティ事件第一審判決や２ちゃんねる事件のように損害賠償

責任を負うとされた事例が存在するため、慎重な判断が求められる。具体的な削除請求が事前または同時になされている場合には、上記(1)または(3)の手続きに従っていることにより作為義務違反が無いとされ、損害賠償責任を負わないとされる有力な根拠となり得る。

(6) 発信者情報の開示請求

(ア) プロバイダ責任制限法第 4 条に基づく場合

a. 利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって、Web ページ等 1 対多の通信によるものの場合、プロバイダ責任制限法の規定に基づき専門家と共に対処するものとし、発信者が開示に同意している場合を除き、発信者情報の開示請求には慎重に対処するものとする。

b. 電子メールアドレス等、事前に利用者等から開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼するものとする。

解説：利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって、Web ページ等 1 対多の通信によるものの場合、プロバイダ責任制限法の規定に基づき専門家と共に対処する必要がある。プロバイダ責任制限法第 4 条に基づく手順としては、概ね下記の通りとなる。

(ア) 発信者情報の保有の有無、技術的に特定できるかどうかの判断
開示できる発信者情報がなければその旨を請求者に通知する。

(イ) 発信者情報開示請求の根拠の確認と違法性の判断
必ず法律の専門家に相談する。

(ウ) 開示について発信者の意見を聞く。
発信者が開示に同意すれば開示してよい。

(エ) 発信者情報開示をする法律要件を確実には満たしていないと判断すれば開示を拒否する旨通知する。不開示の判断に故意または重過失がなければ責任を問われないので、少しでも法律要件を満たさない事実があれば、不開示判断をすべきである。

(オ) 発信者情報開示の要件に該当することが確実である場合には開示できる。しかし、開示判断を誤った場合には電気通信事業法や有線電気通信法上の通信の秘密侵害罪やプライバシー侵害による損害賠償責任からは免責されないため、慎重な判断を要する。発信者が開示に同意しない場合、特に慎重な判断を要する。

解説：「プロバイダ責任制限法ガイドライン等検討協議会」の発信者情報開示関係ガイドラインを参照。
http://www.telesa.or.jp/ftp-content/consortium/provider/pdf/provider_hguideline_20160222.pdf

(7) プロバイダ責任制限法に基づかない発信者情報の照会（民事）

利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の照会があった場合であって、メール等 1 対 1 の通信によるものの場合、下記の手順をとるものとする。なお、警察官、検察官、検察事務官、国税職員、麻薬取締官、弁護士会、裁判所等の法

律上照会権限を有する者から照会を受けた場合であっても、原則として発信者情報を開示してはならないので同様の手順となる。

i) 電子メールアドレス等、事前に開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼する。許諾を得ていない発信者情報の開示については発信者の意見を聴く。

ii) 発信者が開示に同意すれば開示してよい。発信者が開示に同意しない場合は、開示を拒絶する。その場合は、通信の秘密及びプライバシーの保護を理由とする。

iii) 発信者情報の保有の有無、技術的に特定できるか否かの判断をし、開示できる発信者情報がなければ、その旨を請求者に通知する。

(8) 強制捜査による発信者情報の差押え、記録命令等

(ア) 部局技術担当者は、発信者情報を含む情報の強制捜査の事前打診があった場合には、発信者情報その他の強制捜査対象の情報を印刷あるいは記録媒体に出力できるよう準備をしておくものとする。

(イ) 部局総括責任者もしくは対外折衝事務担当者は、部局技術担当者の協力を得て、ネットワークの稼動への影響が最小限になるような方法で強制捜査に協力するものとする。

(ウ) 捜査当局から強制捜査の令状の呈示を受けた場合、令状の記載事項等を確認の上、立会いを求められたときは立会い、押収物があるときは押収目録の交付を受けるものとする。

(エ) 部局技術担当者は、捜査当局から通信履歴（通信の送信先，送信元，通信日時など。通信内容は含まない。）について，暫定的に残しておくよう警察署長印等のある正式文書にて求められた場合（保全要請）、保全対象の情報を印刷あるいは記録媒体に出力して保管しておくものとする。

解説：情報処理の高度化等に対処するための刑法等の一部を改正する法律のうち手続法部分の施行（2012 年 6 月 22 日）により、記録命令付差押え（刑訴法 99 条の 2・218 条）、保全要請（刑訴法 197 条 3 項）の手続きが新設された。

また、①データではなく、ＰＣやサーバが差押え対象となった時には、リモート接続しているネットストレージにあるデータ等令状に記載された範囲のデータを複写する（刑訴法 99 条 2 項・218 条 2 項・219 条 2 項）　②記録媒体（ハードディスク等）が差押え対象となった場合に、記録媒体から必要なデータのみを複写・または移転する（刑訴法 110 条の 2・222 条 1 項）手続きも追加されている。

（ア）の準備作業は、従来手法である差押え（刑訴法 99 条）と新設の記録命令付差押えに共通するものである。従来から発信者情報等を出力した紙や記録媒体を差押える手続きは行われてきたが、発信者情報等を特定する作業により、利用者の通信の秘密を侵害したとされるリスクが皆無であるとは言い切れなかった。強制的な記録命令の対象となることによりそのリスクは無くなり、従来からの捜査協力手法が正面から認められることとなった。

（イ）の折衝により、サーバ等、サービス稼働に重大な影響を及ぼすハードウェアの差押えを回避すべく努力すべきである。

（ウ）の立会時には、リモートアクセスや、データの複写・移転についてサー

バの操作を協力する一方、令状記載の範囲内で複写されたか確認すべきである。（エ）は将来の通信ログの保存ではなく、要請時に現に残存している通信ログを 30 日(延長しても最大 60 日)間消えるままにしないようにすること（保全）を要請するものである。なお、保全したはずのログが消失しても罰則は無いが、セキュアな保管方法を選択すべきである。

8. 通常の利用規定違反行為の対応

(1) 発見または通報等による認知と事実確認（情報発信者の特定を含む）

部局技術担当者は発見あるいは通報により利用規定違反の疑いのある行為を知ったときは、すみやかに事実関係を調査し、発信元利用者等を特定した上で部局技術責任者に報告する。

(2) 利用規定違反の該当性判断

部局技術担当者の報告を受けた部局技術責任者は、通常の利用規定違反行為の対応手順にのせることが可能と考える場合は、その旨部局総括責任者に報告し、確認を得るものとする。

部局技術責任者は、技術的事項に関する利用規定違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置が必要であるかどうかを部局総括責任者に報告するものとする。

部局総括責任者は、技術的事項以外の利用規定違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置やアカウントの一時停止等、個別の情報発信の一時停止以上の措置が必要であるかを判断する。判断にあたっては、可能な限り当該行為を行った者の意見を聴取するものとし、必要に応じて部局情報システム運用委員会の判断を求めるものとする。

(3) 情報発信の一時停止措置

部局技術担当者は、部局総括責任者または部局技術責任者の指示を受けて、利用規定違反に関係する情報発信の一次停止またはアカウントの一時停止措置等を実施する。

(4) 情報発信者に対する通知・注意・警告・当事者間紛争解決要請

部局技術責任者または部局総括責任者は、事案に応じて下記内容を発信者に通知するものとする。

- 利用規定違反の疑いがあること
- アカウントの一時停止措置等の利用を制約する措置を講じた場合は、そのこと、及びその理由・根拠
- 利用規定違反行為の是正、中止の要請
- 利用規定違反行為が是正、中止されなかった場合の効果（情報の削除やアカウントの停止、学内処分等）
- 反論を受け付ける期間とその効果
- 利用者等当事者間の紛争解決の要請

(5) 個別の情報発信またはアカウントの停止と復活

(6) 部局総括責任者または部局技術責任者は、(4) の措置を講じたときは、遅滞無く全学実施責

任者にその旨を報告し、その後の利用者等の対応により、必要に応じ部局情報システム運用委員会の承認を得て、下記を実施するものとする。

- 個別の情報発信またはアカウントの停止と復活
- 有効な反論があった場合、または利用行為が是正された場合の個別の情報発信やアカウントの復活
- 利用行為が是正されなかった場合の情報の削除やアカウントの停止、学内処分の開始手続き-
- 利用者等の当事者間の紛争解決着手の有無の確認

9. 学内処分との関係

部局総括責任者は外部クレームの対象となった利用者等、利用規約違反をした利用者等につき、本学懲罰委員会への報告をすることができる。また、本学懲罰委員会による学内処分の検討に際し、アカウント停止処分やその他ネットワークやシステムの利用を制約する処分の必要性の有無について意見を述べることができる。

参考１　インシデント対応手順にもとづくインシデント報告・承認要領

1. 本書の目的

インシデントが発生した場合、適切な対応によりインシデントの影響が拡大することを防ぐと共に復旧を図ることが必要である。このとき対応を誤ると無用な被害の拡大を招くことが懸念されるため、インシデントの発見から対処、さらには再発防止策の実施にいたる手続きを定め、適切な対処を実施することが必要である。

本書では、インシデントが発生した場合の報告･申請等の手続きに利用する様式を定め、様式を利用した報告・記録・申請・承認の要領を定めることによりＡ大学において必要とされるインシデントへの対処を適切に実施することを目的とする。

2. 本書の対象者

本書は、すべての情報システム運用関係者を対象としている。利用者には、インシデントが発生した場合の部局技術担当者やCSIRT等の通報先を周知・徹底すること。

3. 承認権限者

(1) インシデントに対する対処方針の適否を審査等する者（「**インシデント対処承認権限者**」）は、部局技術責任者、部局総括責任者又は全学実施責任者とする。ただし、インシデントの内容に応じて必要がある場合は、その上位者を対処承認権限者とする。
(2) インシデントの再発防止策の適否を審査等する者（「**インシデント再発防止策承認権限者**」）は、部局総括責任者、全学実施責任者または全学総括責任者とする。

4. 障害等発生から再発防止策実施までの対応

4.1 障害等発生時における全般的な注意事項

(1) 全学実施責任者又は部局総括責任者は、インシデントが発生した場合において、緊急に対処が必要な場合の遅延を防止し、対処を円滑に実施するため、情報システム、組織等の状況を勘案し事前に詳細な手順を定め、関係者に周知すること。
(2) 部局技術担当者（外部からの通報の場合、CSIRTまたは広報部門）は、緊急の対処が必要なインシデントが発生した場合において、報告、審査等の手続が遅延することにより、必要な対処の実施が遅れることのないようにすること。
(3) 緊急の対処が必要な場合は、報告書に代わって口頭での報告、審査等を先行することや、発見者に代わって報告受理者が報告書を記入しインシデントの発見者から内容確認を得ること等により、遅滞なく障害等に対する対処を実施する。ただし、このような場合であっても、速やかに報告書を作成して記録を残すこと。

【事業継続計画（BCP：Business Continuity Plan）が策定されている場合】

(4) 部局技術担当者は、BCP と情報セキュリティ関係規程が定める要求事項において事前に想定されていない不整合が生じた場合、その旨を部局技術責任者を通じて部局総括責任者（必要により全学実施責任者）に報告し、指示を得ること。

4.2 インシデントの発見報告

(1) 自ら発見、または利用者等からの通報によりインシデントを認知した部局技術担当者（外部からの通報の場合、CSIRTまたは広報部門）は、**別紙１**「インシデント発生・再発防止策に関する報告・申請書（様式〇〇）」（以下「**インシデント報告書**」）により、インシデントの内容に応じて部局技術責任者または部局総括責任者（「**インシデント報告受理者**」）に報告を行うこと。

(2) インシデントによる被害の拡大が懸念されるため、**インシデント報告受理者**の指示により部局技術担当者が応急措置を実施した場合には、すみやかにインシデント報告書に応急措置の内容を記録すること。

(3) **インシデント報告受理者**は、対処を実施する者を選び、対処の指示を与えること。なお、口頭により報告を受けた場合は、インシデント報告書のインシデントの詳細についてすみやかに記録させること。

(4) **インシデント報告受理者**は、報告された内容を確認し、必要に応じてabuse@example.ac.jp等の連絡網を活用し、部局総括責任者、全学実施責任者及び関係部署等に通知させること。また、通知先をインシデント報告書に記録させること。

(5) 全学実施責任者は、危機管理、利用者の意識向上に資するインシデント及びその対処の事例について、情報セキュリティ対策上支障のない範囲で学内の広報に努めること。

4.3 インシデントの対処

インシデントの対処を実施する者は、インシデントの対処方針を提案し、インシデント報告書によりインシデントの内容に応じて**対処承認権限者**の承認を得ること。ただし、部局総括責任者または全学実施責任者が定めた詳細な手順において、対処方針が規定されている場合には、承認を受けたものとみなす。なお、対処方針を決定する際には、必要に応じて通知先の関係部署と連携すること。

4.4 インシデントの再発防止

インシデントの対処を実施する者は、インシデントが発生する前の状態に復旧するだけでは再発するおそれがあると考える場合には、速やかに根本的な再発防止策を提案し、インシデントの内容に応じて、**再発防止策承認権限者**の承認を受け、記録すること。

別紙1

【機密性2】複製要許可

様式○○

インシデント発生・再発防止策に関する報告・申請書

インシデント管理番号:		受理者確認	□部局技術責任者　年　月　日 □部局総括責任者 □全学実施責任者 □その他 （氏名・役職・連絡先）
発見・通報日	年　月　日		
被害の範囲	□（　　）部局内（部署名　　） □全学　□学外 （相手方名称・サイト）		
被害の有無：□有り　□無し（未遂）		発見者・通報者及び認知経路・発見方法	学外 （氏名、所属、連絡先*1） □情報メディアセンター 経由 □広報部門／学外窓口　経由 申告・請求内容
被害を受けた期間	年　月　日～　年　月　日		
被害対象	関連システム／ネットワークの名称・概要		
	機種：□Windows　台　□Mac　台　□iPad　台 □その他（機種名:　　）　台		学内 （氏名、所属、連絡先*1） □情報メディアセンター／非常時窓口 □部局技術担当者 □その他
	OS：□Windows　□Windows Server　□MacOS　□iOS □Android　□Linux　□その他Unix系 □その他(　　) バージョン等(　　)		
	利用目的：□学術研究 □事務 □情報公開(Web等) □その他(　　)		発見方法 □目視により発見 □アンチウィルスソフトで発見 （ソフト名:　　） □ツール類のログ （ツール名称:　　） □ その他疑いを持った状況
	情報種別：□個人情報　（　　） □その他　要保護レベル: （　　）		
	権利侵害・違法行為：□名誉・信用・プライバシー □著作権 □その他知的財産（　　） □営業秘密・通信の秘密 □営業・業務妨害 □その他の犯罪・違法行為（　　）	通知先	（氏名、所属、連絡先*1） □abuse@example.ac.jp □その他のML（　　@example.ac.jp） □情報メディアセンター／非常時窓口 □広報部門／学外窓口 □部局技術責任者 □部局総括責任者 □全学実施責任者 □全学総括責任者／非常時対策本部 □法律専門家 □その他（保護者、警察等）
インシデント種別	□対外的 or □対内的 □物理的インシデント □セキュリティインシデント □コンテンツインシデント □その他利用規程違反 （違反内容　　）		
感染／攻撃経路・手口（推定）	実施していたセキュリティ対策 （　　）	物理的被害状況	
	□国内　□海外　□不明 □電子メール　□ダウンロードファイル □WEBサイト閲覧　□外部からの媒体、 □パスワード盗用 □セキュリティホール悪用・設定不備 （ソフト名・バージョン　　） □その他（　　）		
被害状況（セキュリティ）	攻撃手法・ウイルス名称（不明な場合は症状）	応急措置／日時	年　月　日　時　分
	攻撃（未遂）の種別： □ファイル／データ奪取、改竄、消去、破壊 □不正プログラムの埋め込み （トロイの木馬、ボット、バックドアなど） □権限取得　□踏み台 □サービス妨害 □資源利用（ファイル、ＣＰＵ使用） □メールの不正中継 □メールアドレス詐称 □その他（　　）		□パッチ・サービスパック適用 □アンチウイルスソフトで駆除または削除 （社名:　ソフト名:　　） □フリーの専用駆除ソフトで駆除 （ソフト名、またはダウンロード先のURL等） □ファイル（メール）の削除　□初期化 □情報発信関連サーバ・BBS等の一時停止 □権利侵害・違法コンテンツ送信の一時停止 □権利侵害・違法コンテンツ送信の一時停止 □その他（　　） ・回復に要した人日−（ ）人・（ ）日 （0.5日単位で記述）

インシデントへの対処方針		対処方針の承認権限者承認*1 年 月 日
対処実施者	(役割、氏名、所属、日付、連絡先)	(役割、氏名、所属、連絡先)
対処区分	□緊急 □非常時対策本部の設置 □通常 □再現待ち □通常の利用規定違反	□部局技術責任者 □全学実施責任者 □全学総括責任者
方針の詳細	□情報機器・システム復旧計画 (内容:)	
	□学外クレームへの応答 □対外クレームの実施 (内容:) □個別システムの停止／ネットワークからの分離 □特定利用者アカウントの停止 □発信者である利用者への通知、注意、警告、当事者間紛争解決要請	

インシデントへの対処結果		対処結果の審査者確認*1 年 月 日
原因		(役割、氏名、所属、連絡先) □部局技術責任者 □全学実施責任者 □全学総括責任者
技術的対処	□パッチ・サービスパック適用 (パッチ・サービスパックの全てを列挙) □ソフトウェア・プログラム設定変更 (ソフトウエア・プログラムの名称、設定作業内容を明記) □ソフトウェア・プログラム更新・削除 (改竄されたものを回復した場合も含む。) (ソフトウエア・プログラムの名称を明記) □機器撤去 (永久使用しない場合のみ) □その他 (以下に詳細を明記)	
事務的対処	□利用者の懲罰委員会への報告 □外部機関への連絡・通報・届け出(警察、JPCERT,IPA等) □民事訴訟他の民事手続きの提起・応訴等	

インシデント再発防止策		インシデント報告受理者確認 年 月 日
実施予定日 年 月 日		再発防止策許可者承認 年 月 日
実施者	(役割、氏名、所属、連絡先) □部局技術担当者 □部局技術責任者 □部局総括責任者 □全学実施責任者	(役割、氏名、所属、連絡先) □部局技術責任者 □部局総括責任者 □全学実施責任者 □全学総括責任者
インシデント再発防止策の詳細*1		

【報告・申請経路】インシデントの発見者→受理者(インシデントの内容により部局技術責任者、部局総括責任者又は全学実施責任者がが受理)→対処実施者→対処方針の承認権限者者(インシデントの内容により必要に応じて受理者より上位の承認権限者に回付)→対処結果の審査者(対処方針を与えた者と承認した者と同一)→再発防止策実施者→インシデント報告実施者→再発防止策許可者→全学総括責任者

【注1】緊急の対処が必要なインシデントが発生した場合において、報告、審査等の手続により必要な対処が遅延することがないように留意すること。

【注2】記入欄に全てを書き込むことができない場合、適宜添付資料として通し番号を付すこと。

*1:複数の該当者がいる場合は、それぞれ記入する。

*2:再発防止の対処を暫定的な対処から段階的に実施する場合は、途中の段階における対処についても記入する。

参考 2　インシデント対応手順による学外クレーム対応時の留意点

1. コンテンツインシデントの権利者や被害者への返信の要否

学外クレームがあった際、C3102に基づき調査の上、対処するが、学外クレームを発した権利者や被害者への返信は不要な場合が多いことに留意する。

また、違法情報についての第三者からの指摘については、法的責任の観点からは、返信は不要である。ただし、地域コミュニティを無視している、等の風評を立てられることを回避するため、通報への謝辞（ご指摘ありがとうございます、学内ルールに基づき対処します、等）のみ記して返答するほうが良い場合もある。

権利者や被害者への返信が必要か望ましい場合は、以下のとおりのみ。

(1) 法律で義務とされている場合
　・プロバイダ責任制限法第4条の発信者情報開示請求の要件を満たす場合。
(2) 法律で義務とされていないが望ましい場合
　・発信者情報開示関係ガイドラインに基づき不開示決定を通知する場合
　・削除請求等のクレームに対して利用者等から有効と思われる反論があった場合
　・クレーム者と利用者等との当事者間解決を依頼するのが適当な場合
(3) 法律専門家の判断による場合
　・対処結果を報告する等、連絡することで、その後の交渉ポジションを不利にしないために有用な場合。（海外からの請求の場合、通常はあてはまらない。）

2. 海外の権利者、被害者からのクレームの特徴と、対処時の留意点

(1) そもそも、正式な法的請求といえないものが多い。
(2) 海外の権利者・被害者からの場合、正式な法的請求をする場合は、弁護士名での書面で送付されるとのが普通
(3) 少なくとも海外からの訴状はメールでは送られてこない。
(4) 米国のDigital Milemium Copyright Act（デジタルミレニアム著作権法。以下、「DMCA」という。）に基づく削除請求は、様式や内容が定められており、電子署名のないメールでは様式を満たさない。
(5) DMCAに基づく削除請求にもとづき削除することにより、免責を受けられるが、返事するのは義務ではない。
(6) DMCAにもとづく旨、明記しているかどうかにかかわりなく、著作権侵害通知メールのほとんどは、機械的に発見した結果をとりこんで自動的に処理しているもので、まじめに読んだ相手方がさっさと削除等して、権利侵害が是正されれば儲け物というスタンス。削除結果等を回答することは実は期待されていない。
(7) なお、DMCAでは、アクセスプロバイダーはエンドユーザの（P2P）通信については免責。ただし、常習の権利侵害者の接続を切断する方針を実施する義務があるので、P2Pを利用した著作権侵害についての警告が累積した場合には、米国のISPは回線を切断している、とのこと。
(8) 削除等の対処がされない場合は、権利者、被害者側は、それを記録し、正式な要求をするこ

とになった場合の有力な証拠の一つとすることになるが、国際的な裁判はコスト面でも準拠法や裁判管轄等の法的側面でも容易ではないので、これまでも裁判例は無い。

(9) 万が一、訴訟され反証せざるを得ない局面に備え、対利用者に対する警告、利用停止等の措置の記録はきちんと保存しておくほうが良い。

3. （特に海外からのクレームにおいて）返信をする場合のポイント

(1) 謝らない。故意の権利侵害を自認したことになる。
(2) 聞かれていないことには回答しない。
(3) 事実を正確に表現する。揚げ足をとられないように。

4. セキュリティインシデントの連絡への対処

(1) 他機関からの連絡への返信の際には、できるだけ正確な表現となるように努める。
(2) 法的権利を持っているわけではないが、ブラックリストに登録する権限をもった機関からの連絡は注意を要する。返信をするかどうかは別として、対処しない場合は、対象となるIPアドレスやホストをブラックリストに登録してしまうため、関連するサービス全体が巻き添えを食う恐れがある。(掲示板のアクセス制限も同様。同じアクセスポイントからの全アクセスを制限してしまうので、掲示板へのアクセスや書き込みを許す場合は、原因を取り除いた上で、アクセス制限の解除依頼をせざるを得ない。)
(3) 企業や個人が自営するメールサーバや、掲示板に対するSPAMや荒らし等の攻撃についての苦情も取扱いに注意を要するが、大学として故意にSPAMや業務妨害を行っていない限り、法的手段（訴訟や刑事告訴等）に訴えると脅されても攻撃の原因を取り除くことに集中し、淡々と対処してよい。

C3103 情報格付け取扱手順

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A3105	新規作成（情報取り扱い手順）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A3104	「情報格付け取扱手順」として構成を見直し	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3103	情報システムの実態に合わなくなった箇所の修正	高等教育機関における情報セキュリティポリシー推進部会事務局
2017年10月17日 C3103	要機密情報の定義を修正 （C2501の定めるものと一致させた）	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

1. 目的

情報システムで取り扱う情報は格付けされ、格付けに応じて適切に取り扱う必要がある。取扱いが不適切なため、機密性が求められる情報の漏えい、完全性が求められる情報の改ざん等が生じた場合には、大学活動の停止や社会的信用の失墜の要因となる可能性もある。

本書は、このようなリスクを軽減するため、教職員等が情報を適切に取り扱うために必要な事項を定めることを目的とする。

2. 本書の対象

本書は、情報を取り扱うすべての教職員等を対象とする。

3. 定義

本書における用語の定義は次のとおりである。

「情報」とは、情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。

4. 情報の取扱いに関する全般的な注意事項

4.1 大学活動の遂行以外の目的での情報の作成、入手及び利用禁止

教職員等は、大学活動の遂行以外の目的で、情報の作成、入手又は利用を行わないよう努めること。

4.2 情報の格付け及び取扱制限に応じた取扱い

(1) 教職員等は、作成又は入手した情報について、格付け及び取扱制限を指定し、当該指定の結果を電磁的記録であるか書面であるかに応じて明示等すること。

(2) 教職員等は、取り扱う情報に明示等された格付けに従って、当該情報を本書が定めるとおりに取り扱うこと。格付けに加えて、取扱制限の明示等がなされている場合には、当該取扱制限の指示内容に従って当該情報を取り扱うこと。

5. 情報の格付け

5.1 格付け及び取扱制限の指定

教職員等は、情報の格付け及び取扱制限について、「付録A： 格付け及び取扱制限の判断基準」に基づき、格付け及び取扱制限の指定を行うこと。ただし、「付録A： 格付け及び取扱制限の判断基準」で規定されていない情報については、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定（取扱制限については必要性の有無を含む。）をし、決定した格付け及び取扱制限に基づき、その指定を行うこと。

5.2 格付け及び取扱制限の明示手順

(1) 教職員等は、書面の場合には、格付け及び取扱制限を各ページに明記すること。

(2) 教職員等は、電磁的記録の場合には、参照、編集時に常に格付け及び取扱制限が分かるように、また印刷時に各ページに格付け及び取扱制限が印刷されるように、文章のヘッダ等において各ページに明記すること。ただし、電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記すること。

【格付け及び取扱制限をファイル名にも明記する場合】

(3) 教職員等は、電磁的記録の場合には、当該ファイルの内容を参照せずとも格付け及び取扱制限が分かるように、ファイル名に格付け及び取扱制限を明記すること。

(4) 教職員等は、当該情報を取り扱う教職員等に格付け又は取扱制限の認識が周知徹底されているため、格付け又は取扱制限を明記する必要がないと情報システム運用委員会において定められた情報に関しては、格付け又は取扱制限を書面又は電磁的記録に明記する必要はない。なお、明記が不要な情報については、「付録B： 格付け及び取扱制限の明記不要な情報一覧」を参照すること。

5.3 格付け及び取扱制限の変更手順

5.3.1 格付け及び取扱制限の再指定

(1) 教職員等は、元の情報への修正、追加、削除のいずれかにより、他者が指定した情報の格付け又は取扱制限を再指定する必要があると思料する場合には、「5.1 格付け及び取扱制限の指定」に従って、新たな格付け又は取扱制限を指定すること。

【再指定した場合の指定者をこれを行った教職員等とする場合】

(2) 教職員等は、情報の格付け又は取扱制限を再指定した場合には、指定者の責任として、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け又は取扱制限とならないように努めること。

5.3.2 格付け及び取扱制限の見直し

(1) 教職員等は、元の情報への修正、追加、削除のいずれもないが、元の情報の格付け又は取扱制限がその時点で不適当と考えるため、他者が指定した情報の格付け又は取扱制限そのものを見直す必要があると思料する場合には、その指定者又は同人が所属する上司に相談すること。

(2) 被相談者は、指定した情報の格付け又は取扱制限の見直しの必要性を検討し、必要があると認めた場合には、当該情報に対して新たな格付け又は取扱制限を「5.1 格付け及び取扱制限の指定」に従って指定すること。ただし、「付録A： 格付け及び取扱制限の判断基準」に規定されていない情報の場合には、「5.1 格付け及び取扱制限の指定」に従って決定及び指定すること。

(3) 被相談者は、指定した情報の格付け又は取扱制限の見直しに際して、「付録A： 格付

け及び取扱制限の判断基準」において決定されている情報の格付け又は取扱制限の見直しが必要と思料される場合には、上司に報告すること。

【見直した場合の指定者を元の格付け等を行った教職員等とする場合】

(4) 被相談者は、情報の格付け又は取扱制限を見直した場合には、指定者の責任として、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け及び取扱制限とならないように努めること。

6. 情報の作成・入手

6.1 情報を作成・入手する場合の注意事項

教職員等は、大学活動の遂行以外の目的で、情報を作成又は入手しないよう努めること。

6.2 情報を新規に作成した場合の格付け方法

教職員等は、情報を新規に作成した場合には、「5. 情報の格付け」に従って当該情報の格付け及び取扱制限を指定し、これを情報に明示等すること。

6.3 格付けされた情報を引用して情報を作成した場合の格付け方法

教職員等は、既に格付けされた情報を引用して情報を作成する場合には、引用した情報の格付け及び取扱制限と、「5. 情報の格付け」に従って指定した新規に作成した情報の格付け及び取扱制限とを比較した上で、より上位の格付けを行い、双方の取扱制限を併せた新たな取扱制限とし、これを情報に明示等すること。

6.4 格付け及び取扱制限が明示等されている情報を入手した場合の格付け方法

(1) 教職員等は、格付け又は取扱制限が明示等されている情報を入手した場合には、明示等されている格付け又は取扱制限を継承すること。

(2) 教職員等は、格付け又は取扱制限が明示等されている情報を入手した場合で、当該情報の継承すべき格付け又は取扱制限を変更する必要性があると思料するときは、「5 情報の格付け」に従って格付けを変更すること。

6.5 格付け及び取扱制限が明示等されていない情報を入手した場合の格付け方法

教職員等は、格付け又は取扱制限が明示等されていない情報を入手した場合には、「5 情報の格付け」に従って当該情報の格付け又は取扱制限を指定し、これを情報に明示等すること。

7. 情報の利用

7.1 情報の利用における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、情報を利用しないよう努めること。

(2) 教職員等は、取り扱う情報に明示等された格付けに従って、当該情報を取り扱うこと。

格付けに加えて、取扱制限の明示等がなされている場合には、当該取扱制限の指示内容に従って当該情報を取り扱うこと。

7.2 情報を利用する場合の保護方法

(1) 教職員等は、要保護情報が保存された外部記録媒体を利用する場合には、紛失及び盗難から保護するために、以下の措置を講ずること。

- 外部記録媒体の利用中に適切な保護が行えない場合には、当該外部記録媒体を放置せずに、施錠可能な保管庫、棚等に保管する。
- 外部記録媒体の利用が終了した場合には、当該外部記録媒体を机上、端末のドライブ内等に放置せずに、所定の場所に保管する。

(2) 教職員等は、要機密情報が記載された書面又は重要な設計書を利用する場合には、紛失及び盗難から保護するために、以下の措置を講ずること。

- 書面の利用中に適切な保護が行えない場合には、当該書面を放置せずに、施錠可能な保管庫、棚等に保管する。
- 書面の利用が終了した場合には、当該書面を机上等に放置せずに、所定の場所に保管する。
- プリンタ等で書面に印刷した場合には、出力トレイに当該書面を放置せずに、速やかに回収する。

(3) 教職員等は、機密性３情報が記載された書面又はこれが含まれる電磁的記録を必要以上に複製しないこと。

(4) 教職員等は、要機密情報が記載された書面又はこれが含まれる電磁的記録を必要以上に配付しないこと。

【書面に印刷された機密性３情報の所在を明らかにする場合（強化遵守事項）】

(5) 教職員等は、書面に印刷された機密性３情報には、一連番号を付し、その所在を[機密性３情報印刷書面管理表]の様式で明らかにしておくこと。

【機密性３情報に機密性３情報として取り扱う期間を明記する場合（強化遵守事項）】

(6) 教職員等は、機密性３情報には、機密性３情報として取り扱う期間を明記すること。

(7) 教職員等は、機密性３情報の格付けを下げた場合には、その旨を関係する教職員に通知するとともに、[機密性３情報印刷書面管理表]に記録すること。

8. 情報の保存・管理

8.1 情報の保存における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、要保護情報を電子計算機又は外部記録媒体に保存しないこと。

(2) 教職員等は、電子計算機又は外部記録媒体に保存された要保護情報について、保存の

理由となった業務事務の遂行目的が達成された等、保存する理由が滅失した場合には、速やかに当該情報を削除すること。

(3) 教職員等は、電子計算機又は外部記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存すること。

(4) 教職員等は、保存期間が満了した情報に関して、保存期間を延長する必要がない場合は、速やかに当該情報を消去すること。

(5) 教職員等は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、滅失、消失又は改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、バックアップ又は複写を取得すること。ただし、部局技術担当者によりバックアップされているファイルサーバに保存している等、既にバックアップが行われている場合は、この限りでない。

(6) 教職員等は、バックアップ若しくは複写された情報又は当該情報が保存された電磁的記録媒体若しくは記載された書面を、バックアップ又は複写元の情報と同等に管理すること。

8.2 電子計算機へ情報を保存する場合の保護方法

(1) 教職員等は、要保護情報を電子計算機に保存する場合には、他の者が当該情報を参照、変更、削除等できないようにアクセス制御すること。

(2) 教職員等は、機密性３情報を端末に保存する場合には、アクセス制御に加え、当該情報を暗号化すること。

(3) 教職員等は、要保全情報を端末に保存する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与すること。

8.3 外部記録媒体へ情報を保存する場合の保護方法

(1) 教職員等は、要機密情報を外部記録媒体に保存する場合には、当該情報を暗号化すること。ただし、機密性２情報の場合には、パスワードを用いた保護で代替することができる。

(2) 教職員等は、要保全情報を外部記録媒体に保存する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与すること。

8.4 要保護情報が保存された外部記録媒体並びに記載された書面及び重要な設計書の保管方法

教職員等は、要保護情報が保存された外部記録媒体又は記載された書面若しくは重要な設計書を保管する場合には、施錠管理された保管庫、棚等に保管すること。

9. 情報の公表・提供

9.1 情報の公表・提供における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、情報を公表・提供しないよう努めること。

(2) 教職員等は、要機密情報を提供する場合には、「9.2 情報の公表・提供に関する手続」の手続に従い、提供する情報及び提供先を必要最小限にとどめること。

(3) 教職員等は、要保護情報を提供するために当該情報を移送する場合には、「11. 情報の移送」に従って移送すること。

(4) 電磁的記録には、プロパティ等に作成者名、組織名、作成履歴等の付加情報が含まれている可能性があり、当該付加情報から情報が漏えいする場合がある。教職員等は、電磁的記録を公表又は提供する場合には、当該情報の付加情報に不要な情報が含まれていないか確認し、不用意な情報漏えいを防止すること。

(5) 教職員等は、格付け及び取扱制限の明記が不要とされている情報を含む書面又は電磁的記録の提供については、提供先においても格付け及び取扱制限に応じた取扱いを確保するため、提供する前に、明記が不要とされている情報の格付け及び取扱制限を当該書面又は電磁的記録に明記すること。

(6) 教職員等は、要保護情報又は重要な設計書を学外の者に提供する場合には、提供先において、当該情報が、本学の付した情報の機密性の格付けに応じて適切に取り扱われるための措置として、取扱いに関する留意事項の伝達、適切な管理のための取決め等の措置を講ずること。

9.2 情報の公表・提供に関する手続

(1) 教職員等は、保有する情報を公表する場合には、当該情報が機密性１情報に格付けされるものであることを確認すること。

(2) 教職員等は、機密性１情報を公表する場合には、当該情報が法律の規定等で公表が禁じられていないことを確認すること。

(3) 教職員等は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を本学外の者に提供する場合には、[機密性３情報移送・提供許可申請書]の様式で上司に申請し、許可を得ること。

(4) 教職員等は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報を記載した書面を本学外の者に提供する場合には、当該情報が機密性２情報に格付けされたものであることを確認し、秘密であると判断した情報を削除した上で、提供すると同時に、上司に届け出ること。メールに添付して提供する場合は、上司にBCC:で送信しておくなどの方法が考えられる。ただし、上司が届出を要しないと定めた提供については、この限りでない。

10. 情報の持出し

10.1 情報の持出しにおける注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、要保護情報を学外に持ち出さないこと。

(2) 教職員等は、大学活動の遂行の目的で、要保護情報を学外に持ち出す場合には、「10.2 情報の持出しに関する手続」の手続に従い、持ち出す情報及び持出先を必要最小限にとどめること。

(3) 教職員等は、要保護情報の持出しのため、当該情報を移送する場合には、「11. 情報の移送」に従って移送すること。

(4) 教職員等は、持出先においても学内と同様に情報を取り扱うこと。

10.2 情報の持出しに関する手続

(1) 教職員等は、大学活動の遂行の目的で、大学支給以外の情報システムにおける情報処理又は学外での情報処理を行うために、電子計算機、外部記録媒体、書面等で要保護情報（機密性２情報を除く。）を学外に持ち出す場合には、[要保護情報（機密性２情報を除く。）持出し許可申請書]の様式で部局技術責任者又は上司の許可を得ること。

(2) 教職員等は、要保護情報（機密性２情報を除く。）の持出しによる大学支給以外の情報システムにおける情報処理又は学外での情報処理が終了した場合には、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

11. 情報の移送

11.1 情報の移送に関する手続

教職員等は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を移送する場合には、[機密性３情報移送・提供許可申請書]の様式で上司に申請し、許可を得ること。当該申請において、移送方法（送信又は運搬のいずれか）及び移送手段（電子メールの添付、郵送、職員による携行等）を届け出ること。

11.2 移送方法・手段の選択方法

情報の格付け、種類等に応じて移送方法・手段を選択する。

11.3 書面及び外部記録媒体を運搬する場合の保護方法

(1) 教職員等は、要機密情報が記載された書面又は保存された外部記録媒体を建屋外に運搬する場合には、安全確保のため、以下の措置を講ずること。

- 外見から機密性の高い情報であることが分からないようにする。
- 郵便、信書便等の場合には、親展で送付する。
- 携行の場合には、封筒、書類鞄等に収め、当該封筒、書類鞄等の盗難、置き忘れ等に注意する。

【機密性３情報の暗号化を必須とする場合】

(2) 教職員等は、要機密情報が保存された外部記録媒体を建屋外に運搬する場合には、書面又は保存された外部記録媒体を建屋外に運搬する場合の措置に加え、以下の方法を用

いて当該記録媒体に保存された情報を保護すること。ただし、当該情報が機密性２情報の場合には、パスワードを用いた保護で代替することができる。

・ 情報の暗号化

【秘密分散を利用する場合（強化遵守事項）】

・ 秘密分散

(3) 教職員等は、要機密情報が記載された書面又は保存された外部記録媒体を建屋内で運搬する場合には、建屋外に運搬する場合の措置に準じて保護することが望ましい。

(4) 教職員等は、要保全情報が保存された外部記録媒体を建屋外に運搬する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与することが望ましい。

(5) 教職員は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めた時は、情報のバックアップを取得すること。

(6) 教職員は、要保全情報である電磁的記録を移送する場合には、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送するなどの措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。

11.4 電磁的記録を送信する場合の保護方法

【機密性３情報の暗号化を必須とする場合】

(1) 教職員等は、要機密情報である電磁的記録を学外に送信する場合には、以下の方法を用いて当該情報を保護すること。ただし、当該情報が機密性２情報の場合には、パスワードを用いた保護で代替することができる。

・ 通信路の暗号化

・ 電磁的記録の暗号化

【秘密分散を利用する場合（強化遵守事項）】

・ 秘密分散

(2) 教職員等は、要機密情報である電磁的記録を学内に送信する場合には、学外に送信する場合の措置に準じて保護することが望ましい。

(3) 教職員等は、要保全情報である電磁的記録を学外に送信する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与することが望ましい。

(4) 教職員は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めた時は、情報のバックアップを取得すること。

(5) 教職員は、要保全情報である電磁的記録を移送する場合には、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異

なる移送経路で移送するなどの措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。

12. 情報の消去

12.1 外部記録媒体及び書面の廃棄方法

【機密文書等の回収及び廃棄を外部委託している場合】

(1) 教職員等は、情報が保存された外部記録媒体を廃棄する場合には、専用の回収ボックスに投入すること。

(2) 教職員等は、要機密情報が記録された書面を廃棄する場合には、専用の回収ボックスに投入すること。

【細断機を利用する場合】

(1) 教職員等は、情報が保存された外部記録媒体を廃棄する場合には、細断機を利用して細断すること。

(2) 教職員等は、要機密情報が記録された書面を廃棄する場合には、細断機を利用して細断すること。

【外部記録媒体を教職員等が自身で処理する場合】

教職員等は、情報が保存された外部記録媒体を廃棄する場合には、以下のように外部記録媒体の物理的に破壊する等し、読取装置を利用して当該外部記録媒体から情報が読み出せないことを確認すること。ただし、物理的な破壊等により読取装置が利用できない場合に限り、確認を省くことができる。

・CD-R/RW、DVD-R/RW等の光学媒体の場合には、カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する。

・USBメモリは、チップの部分を取り出してペンチで折るか、袋に入れて袋の上からハンマー等で粉砕する（破片飛散防止のため）。

・メモリカード類はペンチ等で折り曲げるか、カッター等で切断する。

12.2 外部記録媒体を他者へ渡す場合の情報の消去方法

教職員等は、使用済みの外部記録媒体を他者へ渡す場合で、当該外部記録媒体に記録されている情報を提供する必要がないときは、データ消去ソフトウェア又はデータ消去装置を用いて、当該外部記録媒体に保存されている情報を復元が困難な状態にし、残留する情報を最小限に保つこと。

解説：USB メモリ、メモリカード等の記録媒体を他社に渡す場合、不要ファイルを OS 上で消去しただけでは、記録情報が復元される可能性に注意すること。完

全に消去するには、専用の消去ソフトウェア等を利用する必要がある[1]。

【利用環境等により適宜情報を消去する必要がある場合（強化遵守事項）】

12.3 利用環境等の理由により適宜情報の消去が求められる場合の消去方法

教職員等は、外部記録媒体について、無人の執務室で利用される環境等、必要があると認められる場合は、適宜、データ消去ソフトウェアを用いて、当該外部記録媒体の要機密情報を復元が困難な状態にし、残留する要機密情報を最小限に保つこと。

13. 本書に関する相談窓口

(1) 教職員等は、緊急時の対応又は本書の内容を超えた対応が必要とされる場合には、部局技術責任者に相談し、指示を受けること。

(2) 教職員等は、本書の内容について不明な点又は質問がある場合には、部局技術担当者に連絡し、回答を得ること。

[1] メモリカードの廃棄・譲渡時における内部のデータ消去に関するユーザ向けガイドライン
http://home.jeita.or.jp/page_file/20120906151218_mfFqh0cvox.pdf

付録A： 格付け及び取扱制限の判断基準

格付けの区分

【ポリシーの格付け分類に準拠する場合】

機密性についての情報の格付け

格付けの区分	分類の基準
機密性３情報	本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年4月1日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	本学で取り扱う情報のうち、独立行政法人の保有する情報の公開に関する法律（平成13年12月5日法律第140号。以下、「独立行政法人等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
機密性１情報	独立行政法人等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

完全性についての情報の格付け

格付けの区分	分類の基準
完全性２情報	本学情報システムで取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

可用性についての情報の格付け

格付けの区分	分類の基準
可用性２情報	情報システムで取り扱う情報（書面を除く。）のうち、滅失、紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

取扱制限の種類

機密性についての取扱制限

取扱制限の種類	概要
○○禁止	○○で指定した行為を禁止する必要がある場合に指定する。 例）複製禁止、配付禁止、印刷禁止、転送禁止、転記禁止、再利用禁止、送信禁止
○○要許可	○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。 例）複製要許可、配付要許可、印刷要許可、転送要許可、転記要許可、再利用要許可、送信要許可
○○必須	○○で指定した行為を必須とする必要がある場合に指定する。また、必須とする際の条件を設定する必要がある場合には、当該条件を付与する。 例）暗号化必須、通信時暗号化必須
○○限り	提供する範囲を○○に限定する必要がある場合に指定する。 例）教職員限り、課内限り

完全性についての取扱制限

取扱制限の種類	概要
○○まで保存	○○の期日まで保存する必要がある場合に指定する。 例）平成１８年７月３１日まで保存
○○において保存	完全性が確保可能な○○の場所において保存する必要がある場合に指定する。 例）共有ファイルサーバにおいて保存
保存期間満了後要廃棄	指定した保存期日を越えた際に廃棄する必要がある場合に指定する。
○○禁止	○○で指定した行為を禁止する必要がある場合に指定する。 例）書換禁止、削除禁止
○○要許可	○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。 例）書換要許可、削除要許可

可用性についての取扱制限

取扱制限の種類	概要
○○以内復旧	復旧に要する時間として許容可能な時間を設定する必要がある場合に指定する。 例） １時間以内復旧
○○において保存	可用性が確保可能な○○の場所において保存する必要がある場合に指定する。 例）年度内保存文書用共有ファイルサーバにおいて保存

格付け及び取扱制限の判断例

情報類型	格付け	取扱制限
○○資料	機密性２情報 完全性２情報 可用性２情報	複製禁止、配付禁止
△△資料	機密性２情報 完全性２情報 可用性２情報	暗号化必須
□□資料	機密性２情報 完全性２情報 可用性２情報	教職員限り
●●資料	機密性１情報 完全性２情報 可用性２情報	３日以内復旧、バックアップ必須
▲▲報告書	機密性２情報 完全性２情報 可用性２情報	５年間保存
■■情報	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ａシステムにおいて保存、書換禁止、保存期間満了後要廃棄
…	…	…

【手順書策定者への補足説明】

※ 取扱制限の種類については、情報を取り扱う他の者が制限すべき事項を理解できる形式であれば、例示したものである必要はない。

※ 判断例の構成としては、文書の種類に基づくもの、特定文書に対応させたもの、本学活動の内容に基づくもの等があるため、適宜の方法を採用する。

付録B： 格付け及び取扱制限の明記不要な情報一覧

教職員等に当該情報に関する格付け及び取扱制限の認識が周知徹底されているため、格付け及び取扱制限を明記する必要がないと定められた情報は以下のとおりである。

- ○○資料
- ■■情報
- …

様式X　　別紙4－2

決裁欄
承認日：

機密性3情報移送・提供許可申請書

殿

［申請日］＿＿＿＿＿＿＿＿

［所属］＿＿＿＿＿＿＿＿

［氏名］＿＿＿＿＿＿＿＿

［連絡先］＿＿＿＿＿＿＿＿

［区分（複数選択可）］

□ 移送

□ 提供

移送にかかわる情報

移送日		移送先	(所属)　(氏名)
情報の名称			
移送方法	□ 送信 □ 運搬	移送手段	
移送目的			

保護対策	はい	いいえ	該当なし
・書面を移送する場合に、安全確保を行う。	□	□	□
・電磁的記録を移送する場合に、暗号化を行う。	□	□	□
・電磁的記録を移送する場合に、秘密分散を行う。	□	□	□

提供にかかわる情報（移送と同じ場合は「同上」と記入。）

提供日		提供先	(所属)　(氏名)
情報の名称			
提供目的			

保護対策	はい	いいえ	該当なし
・電磁的記録の付加情報を削除する。	□	□	□

様式X　　別紙2－2

機密性3情報印刷書面管理表

［記入日］

［所属］

［氏名］

［連絡先］

［区分］

□ 印刷

□ 入手

書面にかかわる情報

［印刷・入手日］

［情報名称］

［部数］

所在にかかわる情報（印刷・入手した部数に応じて記載する。）

番号	所在	管理者	廃棄	廃棄者
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	

C3104 情報システム運用リスク評価手順

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3105	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3104	情報システムの実態に合わなくなった箇所の修正	高等教育機関における情報セキュリティポリシー推進部会事務局
2016年2月5日 C3104	添付1における項目の例示内容を更新	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

情報資産の管理者が行うリスク評価は、次に掲げる方法によるものとする。

(1) 情報資産の洗い出し

「リスク分析票」(添付１)の中項目ごとに関係する情報資産をすべて洗い出す。例えば、「6.6.1 コンピュータの取外し可能な付属媒体」の場合、USB 媒体、メモリカード、CD/DVD/BD、磁気テープ等、保有するすべての可搬媒体が該当する。これら情報資産を一つのセルに一つずつ記入する[2]。

(2) 脆弱性分析

「リスク分析票」(添付１)の安全対策項目と現状を比較し、脆弱性を数値で記入する。このとき、必要に応じ技術担当者の意見を取り入れ、現状を正確に把握する。脆弱性をあらわす数値は以下のとおりである。なお、未実施または即実施のものについては現在の状況を備考欄にメモしておくとよい。

数値	意味	判断基準
１	実施済み	関連のドキュメントが整理され、それに則った運用がなされている。
２	一部実施	関連のドキュメントが不足しているか、または運用が正確に行われていない。
３	未実施	ドキュメントもなく、運用もされていない。

(3) 資産価値判断

上記で洗い出した情報資産を機密性 (C)、完全性(I)、可用性(A)の観点で情報資産をリスク判断し、数値を記入する。判断基準は、これらの性格が損なわれたときに、その業務継続性に与える影響度から判断する。

- 機密性(C)
  - ３：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が著しく下がる。その結果、利用者や社会、本学情報システムの継続性など広範囲に影響が出る。
  - ２：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が下がる。その結果、利用者や社会、本学情報システムの継続性など一部に影響が出る。
  - １：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が下がる危険性が低い。また、利用者や社会、本学情報システムの継続性などに影響は出ない。
- 完全性(I)
  - ３：情報資産に対し、基準となる安全性が確保されなかった場合、その情報の正確性ま

[2] リスク分析票の安全対策項目は次を参照されたい。
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01_2.xls

たは業務処理の正確な運用ができなくなる。その結果、利用者や社会、本学情報システムの継続性など広範囲に影響が出る。

２：情報資産に対し、基準となる安全性が確保されなかった場合、その情報の正確性または業務処理の正確な運用ができなくなる。その結果、利用者や社会、本学情報システムの継続性など一部に影響が出る。

１：情報資産に対し、基準となる安全性が確保されなくても、その情報の正確性または業務処理は継続可能である。その結果、利用者や社会または本学情報システム運用など、どの面にも影響が少ない。

- 可用性(A)

３：情報資産に対し、基準となる安全性が確保されなかった場合、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスできなくなり、利用者や社会または本学情報システム運用など、広範囲に影響がある。

２：情報資産に対し、基準となる安全性が確保されなかった場合、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスできなくなり、利用者や社会または本学情報システム運用などの一部に影響がある。

１：情報資産に対し、基準となる安全性が確保されなくても、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスでき、利用者や社会または本学情報システム運用など、どの面にも影響が少ない。

(4)　脅威の判断

上記(2)で洗い出した情報資産について、脅威を判断する。脅威の判断は、CIA が損なわれる頻度によって判断する。

- 機密性(C)

３：機密性が失われる危険が常にある。

２：機密性が失われる危険が週に一度程度ある。

１：機密性が失われる危険が年に一度程度ある。

- 完全性(I)

３：情報の正確性や円滑な運用が失われる危険が常にある。

２：情報の正確性や円滑な運用が失われる危険が週に一度程度ある。

１：情報の正確性や円滑な運用が失われる危険が年に一度程度ある。

- 可用性(A)

３：利用すべき立場にあるものが、利用不可能に陥る危険が常にある。

２：利用すべき立場にあるものが、利用不可能に陥る危険が週に一度程度ある。

１：利用すべき立場にあるものが、利用不可能に陥る危険が年に一度程度ある。

(5)　リスク値の算出

脆弱性と資産価値と脅威の値を足しリスク値を算出する。

(6)　対策の必要性判断

上記 5.の結果、リスク値が４以上のものについて、対策を実施する。対策を実施しないものについては、その理由を明確にし、全学総括責任者の承認を受ける。

添付１　リスク分析票（例）

大項目 No	中項目	安全対策項目	情報資産	脆弱性	資産価値		脅威	リスク値	備考
6.7 媒体の取扱い									
	6.7.1 取外し可能な媒体の管理のための手順を備える								
6.7.1.1		不要となることで組織の管理外となる媒体が再利用可能なものであるときは、格納している内容を回復不能とすること			C				
					I				
					A				
					C				
					I				
					A				
6.7.1.2		組織の管理外とする媒体のすべてについて、認可を要求すること			C				
					I				
					A				
					C				
					I				
					A				
6.7.1.3		媒体を組織の管理外とする措置のすべてについて、監査証跡の維持のために記録を保管すること			C				
					I				
					A				
					C				
					I				
					A				
6.7.1.4		すべての媒体を、製造者の仕様に従って、安全でセキュリティが保たれた環境に保管すること			C				
					I				
					A				
					C				
					I				
					A				
6.7.1.5		情報を媒体の寿命（製造者の仕様に従う。）よりも長く保管することが必要な場合、媒体の劣化による情報の消失を避けるために、その媒体に保管された情報を他の媒体に記録・保管すること			C				
					I				
					A				
					C				
					I				
					A				

C3200 情報システム利用者向け文書の策定に関する解説書

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3200	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3200	対象文書名と文書番号の変更	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

この文書は、以下の文書の利用に際しての注意点について述べたものである。

C3251　情報機器取扱ガイドライン
C3252　電子メール利用ガイドライン
C3253　ウェブブラウザ利用ガイドライン
C3254　情報発信ガイドライン
C3255　利用者パスワードガイドライン

文書 C3251～C3555 は、「C2201 情報システム利用規程」の解説でも触れたが、内規や手順としてではなく、ガイドラインとして提示されている。これらのガイドラインには、昨今の教育環境の変化により、やむなく主観が入り込む余地のある道徳的条項が盛り込まれている。その結果として、これらの文書は手順や内規ではなくガイドラインとした。

ガイドラインではなく手順や内規として本ひな形を参考にする場合には、何が違反となるかを明確になるように文書を作成するとともに、「C2201 情報システム利用規程」を修正しなければならない。

C3251 情報機器取扱ガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A3201	新規作成（PC取扱手順）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A3201	「PC取扱ガイドライン」として、書式や表現を見直し	国立大学法人等における情報セキュリティポリシー策定作業部会
2011年3月31日 A3201	「情報機器ガイドライン」として、対象をPCに限定しないように記述を見直し	長谷川明生（中京大学）
2015年10月9日 C3251	情報機器の利用実態に合わなくなった箇所の修正	高等教育機関における情報セキュリティポリシー推進部会事務局
2017年10月17日 C3251	用語をC2103（情報格付け基準）で用いているものに統一	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：C2201（情報システム利用規程）で指定した情報機器の利用手順に関して述べている。ここでいう情報機器とは、利用者が相対して操作する端末等を想定している。サーバ機能やルータ機能を持つコンピュータは対象としていない。ただし、大学外からこれら情報機器へのリモートアクセスを可能にするためのサーバ機能は例外である。利用手順に倫理条項を含んでいるが、一般端末の利用手順の雛形としての利用を想定したためである。

1. 一般利用者向け利用手順

解説：ここでいう一般利用者は、計算機の特権利用者（Windows®であればAdministrator、UNIX®であればrootなど）以外の利用者を指し、特権利用があらかじめ用意したアカウントを利用する利用者である。一般利用者は計算機の設定（個人環境に関するものを除く）変更や、アプリケーションのインストールはできないものとしている。大学の場合は、演習室や図書館等に設置されている共用端末を利用する一般学生等が対象となる。もちろん、特権利用者も本項目に書かれている事項は遵守する必要がある。

1.1 利用者は以下に掲げる行為をはじめとする、端末等の設備を物理的に損傷する可能性のある行為をしてはならない。

(a) 演習室等における飲食。ただし、管理者が別途許可する場合を除く。
(b) コネクタ等を引き抜いたり、キーボードやマウス等周辺機器を取り外す行為
(c) IC カードリーダー等、開口部に異物を詰める行為
(d) キーボードの乱打、USB メモリ等の乱暴な抜き差しをする行為

解説：主として大学内の共用スペースに設置する共同利用端末に関して、端末設備を物理的に破損する行為等を禁止する。飲食等についてはカフェテリア等に設置する場合もあり、状況に応じて規定を設ける。これら端末を損傷する行為に対する対策は、規定等による対策の他に、管理者による適切な監視体制の整備等も重要である。それら対策が困難である場合には、シンクライアント端末の導入や、タッチパッド等の採用も考慮すべきである。

1.2 利用者は以下に掲げる行為をはじめとする、他の利用者の利用を妨げる行為をしてはならない。

(a) 共用端末の占有行為。端末をロックして長時間離席する行為も含む。
ただし、講義等で特に許可された場合を除く。
(b) 演習室で大声で騒ぐ行為や、ごみを放置する行為。
(c) プリンタの紙詰まりや紙切れ、トナー切れを放置する行為。

解説：ここに掲げられている事項の他に、ディスク記憶領域や、計算能力、メモリ等

の占有行為の禁止が必要になる場合があるかもしれない。しかし、これらの計算機資源の占有が危惧される場合には、クォータ等、システム側で対応を考えた方がよい。
また、ライセンス上、同時起動数が制限されているようなアプリケーションを導入している場合は、同様の規定が必要であろう。
さらに、前項と同様、管理者による監視体制の整備や、プリンタのトラブル等に迅速に対応できる体制作りも重要である。

1.3 利用者は以下に掲げる行為をはじめとするネットワーク帯域を占有する行為をしてはならない。

(a) 大きなサイズのファイルの転送
(b) 大きなサイズのメール送信
(c) 高い頻度で問い合わせパケット等を送出するアプリケーションの使用

解説：基本的には、1.2 項の規定に含まれるとも考えられるが、場合によっては、広範囲に影響が及ぶため独立した項目としている。「大きなサイズ」等の具体値をネットワーク性能等に応じて示す方がよい。

1.4 利用者がアプリケーションをインストール、使用する場合には、以下の各号を遵守しなければならない。

(a) 教育・研究目的、およびそれらを支援する目的に合致しないアプリケーションをインストール、使用してはならない。
(b) インストール、使用しようとするアプリケーションの利用条件に従って利用すること。
(c). アプリケーションをインストールする前に、ウイルスチェックソフトウェア等により、ウイルスやスパイウェア等、有害ソフトウェアが含まれていないことを確認すること。
(d) 出所の定かでないソフトウェアをインストール、使用しないこと。

解説：アプリケーションのインストールに関しては、管理者が行うべきものであり、利用者が共通領域にインストールできるようなシステム構築はセキュリティ上、極力避けるべきである。しかし、その場合でも、利用者権限で利用者用領域にインストール可能なソフトウェアも存在するので、本項目を設けている。
なお、利用者用ディスク容量の制約が厳しい場合等は、利用者がインストールしてほしいアプリケーションを管理者に申請できるような仕組みを設けることも考えられる。

1.5 利用者は、情報格付け規定において規定されている要保護情報や、その他重要なデータの取り扱いに関して以下の各号を遵守しなければならない。

(a) 要保護情報を PC 内部、あるいは外部記憶メディアに保管する場合は、暗号化するもの

とし、その暗号化鍵を適切に管理すること。
ただし、暗号化以外に十分な保護対策が採られていると管理者が認める場合はこの限りでない。

(b) 要保護情報を電子メール等を用いて送信する場合は暗号化するものとし、その暗号化鍵は別途安全な手段を用いて送信すること。

解説：個人情報等、重要な情報の保管、送信時の暗号化の必要性について述べている。
(a)の但し書きは、バックアップ用メディア等で、暗号化すると著しく利便性が損なわれるような場合に、メディアを厳重に管理することで暗号化に代えられるとしたもの。

1.6 利用者は、CD-ROM、USB メモリ、各種メモリカード等の外部記憶メディアを利用する場合には、以下の各号を遵守しなければならない。

(a) 利用者のファイルを保存した外部記憶メディアを放置しないこと。
(b) 放置してある、または出所が定かでない外部記憶メディアを端末に挿入しアクセスしてはならない。そのような媒体を発見した場合は、管理者に届け出ること。
(c) 使用済みの外部記憶メディアを譲渡、または廃棄する場合には、記録されていたデータが復元されることのないように、専用ツールを用いて消去するか、メディアを物理的に破壊すること。

解説：CD-ROM の内容を自動実行する設定にしている場合には、メディアを挿入するだけでソフトウェアが実行され、悪意のあるソフトウェアがインストールされる可能性に留意すること。
メディアを廃棄、譲渡する場合は、OS 上でファイルを消去しただけでは、記録情報が復元される可能性に注意すること[3]。なお、データ破壊に関しては、「要保護情報等の重要な情報」を記録した外部記憶メディアに対象を限定するという考え方もある。

1.7 利用者は、演習室等、共用スペースに設置してある PC 端末を利用する場合は、以下の各号を遵守しなければならない。

(a) 端末を操作中に一時的に離席する場合は、端末をロックすること。
(b) 演習室等の扉や窓を開放しないこと。また、空調機の設定温度を変更しないこと。ただし、管理者が別途指示する場合はこの限りでない。
(c) 使用後の端末等の電源を切ること。ただし、管理者が別途指示する場合はこの限りでない。
(d) プリンタで無駄な印刷をしないこと。

[3] メモリカードの廃棄・譲渡時における内部のデータ消去に関するユーザ向けガイドライン
http://home.jeita.or.jp/page_file/20120906151218_mfFqh0cvox.pdf

解説：(b)は、PC 端末の正常動作（温度、ほこり等）の保証と、PC 端末の盗難防止を目的とするものなので、これらの懸念がない場合は必要ない。
(c)についても、利用者に電源を切らせずに、管理者が電源を切る運用をしている場合は必要ない。
(d)に関しては、システム上で利用者毎に印刷枚数を制限する方法も考えられる。

1.8 利用者は、以下に掲げる各事項を発見したときは、すみやかに管理者に連絡をするとともに、「インシデント対応手順」に従って行動すること。

(a) 端末の OS やアプリケーション、あるいは、大学内に設置されているホストコンピュータやネットワーク機器等について、セキュリティ上の脆弱性など不具合を見つけた場合。
(b) 大学内のホスト上に、著作権を侵害しているおそれのあるコンテンツや、機密情報、個人情報等が公開されていることを見い出した場合。
(c) 大学外のホストで、大学の機密情報や、構成員の個人情報等が公開されている、または、大学が権利を有するコンテンツが無断で使用されていることを見い出した場合。

解説：ネットワークや PC 端末の管理業務をしていない一般利用者であっても本項目に掲げるような脆弱性等を発見した場合に報告させることで、構成員のセキュリティや知的財産に関する意識を向上させるとともに、管理業務の効率化をはかることができる。もちろん、管理側では、これら報告に対処する体制作りが必要である。

1.9 利用者は、大学外のネットワークから大学内の情報システム（不特定多数に公開されているもの（Web サービスなど）を除く）にアクセスする場合は以下の各号を遵守しなければならない。

(a) アクセスの際に必要となる認証情報（パスワードや秘密鍵）が漏洩しないように細心の注意を払うこと。万一、認証情報が漏洩した場合、またはその可能性がある場合は、迅速に管理者に報告し、その指示を仰ぐこと。
(b) 信頼性が保障できない端末（ネットカフェの端末等）からのアクセスは禁止する。

解説：本項は、利用者が、大学内の PC 端末やゲートウェイサーバ等にリモートアクセス可能な場合に必要な規定である。リモートアクセスのための認証情報が漏洩した場合には、単にメールを読むためのパスワード等が漏洩した場合に比較して、より深刻な被害をもたらす可能性が高いことを利用者が十分に理解していることが大切である。

2. 特権利用者向け利用手順

解説：特権利用者は、PC 端末を管理する権限を持つ特権利用者（Windows®であれば

Administrator、UNIX®であれば root）を指している。具体的には、演習室や図書館等に設置されている PC 端末を管理するセンター職員や、個人で PC 端末を管理する教員や事務職員、研究室に導入されている PC 端末を管理する大学院生等が含まれる。学生等の私物 PC を学内ネットワークに接続することを許可している場合は、その私物 PC の所有者も含まれる。

2.1 特権利用者は、自らが管理する端末が、ウイルス、ワーム等に感染しないように、以下に掲げる規定を遵守しなければならない。

(a) 利用している OS、アプリケーションの脆弱性情報をはじめとする情報に留意し、ソフトウェアの不具合を迅速に修正すること。
(b) ウイルス対策ソフトウェアをインストールするとともに、ウイルス情報データベースを常に最新に保っておくこと。

解説：主として利用される OS、アプリケーションに関しては、具体的なチェック方法、修正方法を示しておくことが望ましい。
また、ウイルス対策ソフトウェアをサイトライセンスにより導入している場合、学内からのみデータベースの更新が可能な場合がある。この場合、休暇中等に自宅で感染してしまう可能性があるので注意が必要。場合によっては検疫ネットワークの導入等も検討する。

2.2 特権利用者は、自らが管理する端末に、アプリケーションをインストールし、利用する際には、1.4 項に掲げる規定の他、以下に掲げる規定を遵守しなければならない。ただし、研究・教育目的およびそれらを支援する目的であって、対象となるネットワークの管理者が許可する場合にはこの限りでない。

(a) ネットワーク帯域を極度に圧迫するアプリケーションをインストール、利用してはならない。
(b) 自端末宛以外のパケットを傍受するアプリケーション（パケットスニファ）をインストール、利用してはならない。
(c) P2P ファイル交換ソフトウェアをインストール、利用してはならない。
(d) その他、情報システム利用規程、その他の本学ネットワークの利用に係わる規定等に反するネットワークアプリケーションをインストール、利用してはならない。

解説：1.4 項の規定の他に、主にネットワークに関連するアプリケーションのインストールについて規定している。(a)ではネットワーク資源の浪費、(b)では通信の秘密、(c)では著作権侵害等に関して問題が生じそうなアプリケーションを原則禁止している。大学の実態に応じて、これらの問題に関する教育を十分に行った上で、届出制等の形で利用を認めることも考えられる。
なお、情報システム利用規程には、ファイルのダウンロード（第十五条一号）、ソフトウェアを取り込む場合（第十七条五号）のように、関連する規定がある

ので参照のこと。

2.3.特権利用者は、自らが管理する端末に関して、以下の各規定を遵守すること。

(a) 利用者が当該端末を認証なしで利用できるようにしてはならない。
端末が認証機能を有さない場合には、あらかじめ許可された者のみが利用できるように別途手段を講じること。
アカウントの発行状況や利用状況（利用者識別の設定できないシステムにあっては、利用状況が把握できるもの）について部局責任者に定期的に報告すること。
(b) ネットワークを経由して、不特定多数の第三者が端末にアクセスできないようにすること。
(c) 当該端末にアカウントを有さない者に端末を使用させないこと。
ただし、教育・研究上必要な場合など、管理者が特に認める場合を除く。
(d) デスクトップ型端末においては、アカウントを有さない者が端末に物理的にアクセスできないように設置場所に施錠等の措置をとるとともに、必要に応じて、端末機器にワイヤーロック等の盗難防止措置をとること。
(e) 移動可能な端末においては、短時間であっても端末を放置しないこと。
保管時は施錠可能な場所に保管すること。
(f) 管理権限をもたない者によって CD、DVD 等、外部記憶メディアから起動されないように BIOS を設定し、BIOS パスワードを設定すること。
(g) 端末を廃棄、あるいは譲渡する場合は、内部ハードディスクや不揮発性メモリに、要保護情報やその他重要な情報が残留することのないように、専用ツールを用いて完全に消去するか、物理的に破壊すること。

解説：PC 端末への許可されていない者のアクセスや端末機器自体の盗難等を防止するための規定である。(f)は、管理者権限を有さない利用者が管理者権限を得る危険性を排除するためである。(g)は、1.6 項(c)と同様に、PC 端末から重要情報や認証情報が漏洩する危険性を排除するためである。リースおよびレンタルの機器に関してはデータの完全削除をソフトウェア的に実施すること。なお、データ破壊に関しては、「要保護情報等の重要な情報」を記録した端末に対象を限定するという考え方もある。

2.4 特権利用者は、自らが管理する端末に関して、利用者が大学外のネットワークから当該端末にアクセスできるようにする場合は、以下の各規定を遵守すること。

(a) アクセスに使用するポート番号、VPN ソフトウェア名等をセンターに届け出ること。
(b) 通信内容は全て暗号化されるようにすること。
(c) パスワードのみ（ワンタイムパスワードを除く）による認証方式は原則として避けること。パスワードによる認証を用いる場合は、パスワードの選定に関して利用者に十分な教育を行うこと。
(d) 特権アカウント（root など）によるリモートアクセスは原則として行えないように設定

すること。

(e) 大学が提供するネットワーク以外（電話回線など）の方法でアクセスできるようにしてはならない。教育・研究目的等で、特に必要な場合には、センターの許可を得ること。

解説：1.9 項の規定に加えて、特権利用者が、VPN サーバソフトウェア等をインストール、運用する場合の注意点を述べている。
(c)は、通信が暗号化されていても、認証パスワードが脆弱であれば不正侵入を許してしまう可能性を考慮したもの。また、リモートアクセスのパスワードとメール受信（POP/IMAP）のパスワードが共通になっている場合、メール受信は SSL/TLS を必須とする等の対策が必要である。

2.5 特権利用者は、自らが管理する情報機器を対象として実施される情報セキュリティ監査に対して、必要な協力を行うこと。

C3252 電子メール利用ガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A3202	新規作成（電子メール手順）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A3202	「電子メール利用ガイドライン」として、書式や表現を見直し	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3252	電子メールの利用実態に合わなくなった箇所の修正	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

1. 本書の目的

電子メールは日々の学習・教育・研究活動において必要不可欠なものになっている。そのため、電子メールは、ルールやマナーを守った安全な方法で使用しなければ、多くの利用者に迷惑をかけることになる。その上、誤った方法による使用は学習・教育・研究活動の停止や社会的信用を失わせる要因となる可能性もある。

本書は、このようなリスクを軽減し、情報資産を保護し、電子メールを安全に利用するための手順を提供する。

2. 本書の対象者

本書は、Ａ大学が整備・提供する電子メールを利用するすべての利用者を対象とする。

3. 電子メールソフトの設定

3.1 電子メール受信に係る設定

(1)利用者は、受信した電子メールをテキスト（リッチテキストを含む。）として表示することとし、偽のホームページへの誘導や不正なスクリプトの実行を未然に防ぐ目的からHTMLメールの利用は原則として認めない。

［操作手順］　各大学の電子メール利用環境に則した説明を記述する。

なお、HTMLメールの利用を許可する場合には、注意事項、許可に要する手続等についても記述する。

(2)利用者は、アンチウイルスソフトウェアに加えて、電子メールソフトウェア側においてもウイルス対策が設定可能であれば、これを実施すること。

［操作手順］　各大学の電子メール利用環境に則した説明を記述する。

【参考：プレビュー機能を停止することを求める場合】

(3)利用者は、HTMLメールのプレビュー機能を停止すること。

［操作手順］　各大学の電子メール利用環境に則した説明を記述する。

3.2 電子メール送信に係る設定

(1) 利用者は、原則として、HTML形式の電子メールを送信しないこと。これは、当方よりHTML形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

［操作手順］　各大学の電子メール利用環境に則した説明を記述する。

4. 電子メールに係る全般的な注意事項

4.1 電子メールの私的利用の禁止

(1) 利用者は、電子メールシステムを、学習・教育・研究活動を遂行する上で必要な場合のみ使用することとし、私的目的のために使用しないこと。

4.2 電子メールの自動転送の禁止

(1) 利用者は、原則として要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送することを禁止する。

(2) 利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要がある場合には、メール転送先・理由・期間・セキュリティ対策などを明確にした上で事前に電子メールシステムの部局技術担当者及び上司の了解を得ること。

(3) 利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要性がなくなった場合には、その旨を電子メールシステムの部局技術担当者及び上司に報告すること。

4.3 大学が整備した電子メールシステム以外の情報システム利用の禁止

(1) 利用者は、学習・教育・研究活動遂行にかかわる情報を含む電子メールを送受信する場合には、大学が整備した電子メールシステムを利用することを原則とする。

(2) 利用しようとする電子メールシステムの利用規程等で、明示的に許可されている場合を除き、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、電子メールシステムの部局技術担当者及び上司の許可を得ること。

(3) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、セキュリティ対策ソフトを導入するなど安全管理措置を講ずること。

(4) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要性がなくなった場合には、その旨を電子メールシステムの部局技術担当者及び上司に報告すること。

解説：利用者は、利用しようとするシステムの利用規程等で外部への転送や大学が整備した以外の情報システム（個人所有の PC 等）でのメールの送受信が許可されている場合、部局責任者や上司の許可を必要としない。学生の連絡先が携帯メールで、情報システムの運用で、携帯メールのアドレスや ISP のメールアドレスの登録が許可されている場合も同様である。システムの利用規程で IMAP、POP やウェブメールおよび VPN を介してモバイル PC 等による電子メールシステムへのアクセスを許可している場合も個別の許可を要しない。セキュリティ担当者の緊急連絡先として携帯電話等の外部の情報システムを登録すること

は広く行われていることであるが、送付する内容や外部情報システムのトラブル、設定ミス等での情報漏洩のリスクを考えると情報セキュリティ責任者が転送内容等について把握しておく必要がある。
研究室等の単位でアウトソースした場合のシステムは「大学が整備したシステム」とみなす。

4.4 電子メールの監視

(1) 電子メールシステムの適正な利用のため、その利用状況（あて先、内容、添付ファイル等）について証跡の取得、保存、点検及び分析が行われる可能性がある。利用者は、その趣旨を理解の上、電子メールの内容に関するモニタリング及び監査を実施していることを認識すること。

4.5 電子メールID及び電子メールアドレスの管理

(1) 利用者は、他人の電子メールID（電子メールサーバへのログインID。以下同じ。）及び電子メールアドレスを使用しないこと。

(2) 利用者は、電子メールID及び電子メールアドレスを他人と共用しないこと。

(3) 利用者は、自己に付与された電子メールIDを、それを知る必要のない者に知られるような状態で放置しないこと。

(4) 利用者は、電子メールを利用する必要がなくなった場合は、電子メールシステムの部局技術担当者へ届け出ること。

(5) 特定のサービス、職位、部門単位に付与される電子メールID及び電子メールアドレスのように、電子メールID及び電子メールアドレスを複数の関係者で共用する、あるいは担当者が引き継いで使用する必要がある場合には、利用者はその許可及び設定について電子メールシステムの部局技術担当者に相談すること。

4.6 ニュースグループ、メーリングリスト等の発信機関への電子メールID登録の制限

(1) 利用者は、ニュースグループ、メーリングリスト等(メールマガジン、Webマガジン、フリーメール)への電子メールID登録は、情報セキュリティ情報のメール配信サービスなど、学習・教育・研究活動上必要なものに限定すること。

5. パスワードの管理

5.1 クライアントPCのログイン管理・電源管理

(1) 利用者は、クライアントPCのログインパスワードを設定すること。

(2) 利用者は、クライアントPCを利用しない時にはクライアントPCの電源を切ること。

(3) 利用者は、離席時には、各自が利用しているクライアントPCをロックすること。また、ロックし忘れた場合に備えて、パスワード・スクリーンセーバが自動起動するように設

定すること。

5.2 電子メールパスワードの管理

(1) 利用者は、パスワードを設定すること。

(2) 利用者は、パスワードの管理にあたっては「C3255 利用者パスワードガイドライン」にしたがうこと。

(3) 利用者は、パスワードを電子メールソフトに永続的に保存しないこと。ただし、電子メールの受信のたびにパスワード入力を行うことが過度に煩雑である場合には、電子メールソフトに一時保存し､クライアントPC起動後のみパスワード入力とする仕組みを利用してもよい。

(4) 利用者は、パスワードを電子メールソフトに一時保存する場合には、当該パスワードを一時保存するクライアントPCを「主体認証情報格納装置」とみなして、以下の点に配慮して安全に取り扱うこと。

・パスワードを保存したクライアントPCを本人が意図せずに使用されることのないように安全措置を講じること。

・パスワードを保存したクライアントPCを他者に付与及び貸与しないこと。

・パスワードを保存したクライアントPCを紛失しないように管理すること。紛失した場合には、直ちに電子メールシステムの部局技術担当者又は部局技術担当者にその旨を報告すること。

6. 電子メールの受信

6.1 電子メールの受信確認

(1) 利用者は、定期的に、電子メールの受信確認を行うこと。

6.2 電子メール添付ファイルのウイルスチェック

(1) 利用者は、アンチウイルスソフトウェアによる自動ウイルスチェックを実施すること。

(2) 利用者は、電子メールシステムの部局技術担当者が自動的にウイルスチェックを実施するように設定している場合又は自動的にウイルスチェック最新データを更新するように設定している場合は、当該設定を変更しないこと。

(3) 利用者は、受信した電子メールの添付ファイルに対して、随時、ウイルスチェックを行うこと。これは、新種のウイルスに対応したパターンファイルの提供が間に合わず、ファイル受信時のウイルスチェックにおいてウイルスが発見されなかった場合を考慮し、最新のパターンファイルを用いて過去に受信した電子メールの添付ファイルに対してもウイルスの有無を確認するための対策である。

(4) 利用者は、緊急時対応が必要な時には、電子メールシステムの部局技術担当者からの指示に従うこと。

6.3 あて先間違いの電子メールを受信したときの対処

(1) 利用者は、あて先間違いの電子メールを受信し、送信者から正しい受信者へ再度送信する必要がある場合には、可能な範囲で送信者へあて先が間違っていたことを通知すること。

(2) 利用者は、あて先間違いの電子メールを受信した場合には、これを削除すること。

6.4 不審な電子メールを受信したときの対処

(1) 利用者は、不審な電子メールを受信した場合には、電子メールを開かず、電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

(2) 利用者は、電子メールに不審なファイルが添付されていた場合には、当該ファイルを開くことなく電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

6.5 ウイルスに感染したときの対処

(1) 利用者は、クライアントPCがウイルスに感染した場合、又は感染したと疑われる場合には、更なる感染を未然に防止するため直ちに当クライアントPCをネットワークから分離し、電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。
ネットワークからの分離は、具体的には、ネットワークケーブル、無線LANカード、USBキー型無線LANアダプタなどを取り外す。または、無線LANアダプタがPCに内蔵されている場合には無線LAN機能を停止させる。

6.6 迷惑メールの対処

(1) 利用者は、必要以上に電子メールアドレスを公表し又は通知しないこと。

(2) 利用者は、ネットワークを経由して電子メールアドレスを開示し又は通知する場合には、アドレスを自動収集されないように、工夫を施すことが望ましい。（画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等）

(3) 利用者は、送信される迷惑メールに対しては、これを無視することが望ましい。送信者へ停止要求を出した場合、その電子メールアドレスが使用されている事実を伝えてしまう結果となり、かえって迷惑メールが増加してしまう可能性もあるからである。

7. 電子メールの作成

7.1 To、Cc及び Bccの制限

(1) 利用者は、To（あて先）、Cc（カーボンコピー）及びBcc（ブラインドカーボンコピー）の総あて先件数は必要最低限とすること。

・使用するネットワークリソースは、電子メール１件の使用リソース×総あて先件数である。

(2) 利用者は、同時に多数の人へ電子メールを送信する場合、Bccを利用するか、あるいは各自に個別送信する等配慮すること。これは、その場合に電子メールアドレスをTo、Ccに列記してしまうと、当該電子メールを受信した者に、他の者の電子メールアドレスが露呈することになるからである。

7.2 電子メール１件当たりのファイル容量の制限

(1) 利用者は、電子メール本体と添付するファイルを含めた総容量が■■Mbyteを超えないこと。

・ 本電子メールシステムでは、送信の際の容量制限を■■MByteとしている。

(2) 利用者は、電子メール本体と添付するファイルを含めた総容量が■■Mbyteを超える場合、別手段による情報提供や分割送信などについて検討の上、電子メールシステムの部局技術担当者に相談し、指示を仰ぐこと。

7.3 電子メールの形式の制限

(1) 利用者は、原則として、HTML形式の電子メールを送信しないこと。これは、当方よりHTML形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

7.4 電子メールの内容

(1) 利用者は、要機密情報を電子メールで送信する場合は別途定められた安全措置を講ずること。

・利用者は、機密性3情報を電子メールで送信する場合には、電子メールシステムの部局技術担当者及び上司の許可を得ること。

・利用者は、機密性2情報を電子メールで送信する場合には、電子メールシステムの部局技術担当者及び上司に届け出ること。

・利用者は、要機密情報を電子メールで送信する場合には、安全確保に留意して送信手段を決定すること。例えば以下の手段が挙げられる。

- ○ 外部を経由しないネットワーク(専用線等)
- ○ 暗号化された通信路(VPN等)
- ○ 暗号メール(S/MIME等)

・利用者は、検討の上決定された送信手段について電子メールシステムの部局技術担当者及び上司へ届け出ること。

・利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、以下の保護対策の必要性を検討し、必要があると認めたときには、これを実施すること。

- ○ 添付ファイルに対するパスワード保護
- ○ 添付ファイルの暗号化(暗号化ソフトの使用等)

(2) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

(3) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

(4) 利用者は、他人になりすまして電子メールを作成しないこと。

(5) 利用者は、電子メールを転送する際に、作成者の許可なく内容の変更をしないこと。

(6) 利用者は、個人情報やプライバシーの保護を考慮すること。

(7) 利用者は、次の事項に該当する電子メールの送信を行わないこと。

- ・ 機密保護違反（■■方針・規程を遵守）
- ・ 権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）
- ・ セクシャルハラスメント及び人種問題に関わる内容
- ・ 無礼及び誹謗中傷
- ・ ねずみ講に相当する内容
- ・ 脅迫、個人的な儲け話や勧誘に相当する内容

7.5 ネチケット

(1) 利用者は、チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わないこと。

(2) 利用者は、スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール）、ジャンクメール（役に立たない情報が書かれている電子メール）等を送

信しないこと。

(3) 利用者は、電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。

(4) 利用者は、俗語的表現やあらかじめ定められていない省略語を使用しないこと。

(5) 利用者は、機種依存文字コードを使用しないこと。

·利用者が判断できない場合には、電子メールシステムの部局技術担当者に相談し、指示を仰ぐこと。

(6) 利用者は、電子メールを作成する際、各行とも全角30～35文字程度で改行を入れること。

(7) 利用者は、ToとCcとの使い分けを意識し、送信する電子メールに対する返事を要求する時には、To（あて先）を使用すること。

8. 電子メールの送信

8.1 送信時の注意

(1) 利用者は、To（受信者）の記述に誤りがないかを確認してから送信すること。

(2) 利用者は、電子メールにファイルを添付し送信する際に、当該ファイルのウイルスチェックを行うこと。

8.2 電子メールの暗号化

(1) 利用者は、要機密情報を電子メールで送信する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

·暗号メール(S/MIME等)

·添付ファイルの暗号化(暗号化ソフトの使用等)

(2) 利用者は、暗号化された情報の復号に用いる鍵を適切に管理すること。

(3) 利用者は、暗号化された情報の復号に用いる鍵のバックアップを取得しておくこと。

8.3 添付ファイルのパスワード保護

(1) 利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、添付ファイルにパスワードを設定すること。

［操作手順］　文書ファイルのパスワードのかけ方（Word®の場合）
Word®の[ファイル]メニューから[名前を付けて保存]を選択した後、[ツール]から[全般オプション]を選択し、[読み取りパスワード]を設定する。

(2) 利用者は、保護に用いたパスワードについては、あらかじめ受信者と合意した文字列を用いるかあるいは、電子メールで送信せずに電話などの別手段を用いて伝達すること。

8.4 電子メール送信時における情報漏えい防止の確認事項

(1) 利用者は、添付ファイルを電子メールで送信する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないか確認すること。

- 「プロパティ」に作成者や修正者等の個人情報が残っていないか
- 一見すると表示されていない部分（「非表示」の設定箇所、非表示としたコメント、裏に隠れたシート等）に要機密情報が含まれていないか
- 変更履歴が必要以上に保存されていないか

8.5 電子メールへの署名付与

(1) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

(2) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

8.6 電子メール送信時の受信確認機能の使用制限

(1) 利用者は、トラフィック増を防止するため、電子メール送信時の受信確認は必要最低限の使用とすること。

8.7 電子メールを誤って送信したときの対処

(1) 利用者は、電子メールを誤って送信した場合、相手先（受信者）へのフォローは発信者責任で実施すること。

8.8 ウイルスを送信したときの対処

(1) 利用者は、誤ってウイルスを送信したことが判明した場合、直ちに電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

9. 電子メールの保存・削除

9.1 メールボックス（サーバ側）における電子メールの保存・削除

(1) 利用者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、メールボックスから不要な電子メールを削除すること。

- サーバ側の個人別メールボックスに格納される電子メールの最大容量は、■■Mbytesに設定されている。

(2) 利用者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、クライアントPCへの保存を行うこと。

・サーバ側の個人別メールボックスに格納される電子メールの保存期限は、■か月に設定されている。

9.2 メールボックス（クライアントPC側）における電子メールの保存・削除

(1) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを保存する場合には、暗号化等の措置を講じた上で保存することが望ましい。

(2) 利用者は、本文や添付ファイルに要保全情報が含まれている電子メールについては、適宜バックアップすること。

(3) 利用者は、不要なメッセージは速やかにクライアントPCから削除すること。

(4) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを削除する場合には、その機密性に配慮し、復元が困難な状態にすること。

10. 本手順に関する相談窓口

(1) 利用者は、緊急時の対応及び本書の内容を超えた対応が必要とされる場合には、電子メールシステムの部局技術担当者に相談し、指示を受けること。

(2) 利用者は、本書の内容について不明な点及び質問がある場合には、電子メールシステムの部局技術担当者に連絡し、回答を得ること。

C3253 ウェブブラウザ利用ガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A3203	新規作成（ウェブブラウザ手順）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A3203	「ウェブブラウザ利用ガイドライン」として、全体的な内容を見直し	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3253	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：本ガイドラインの対象者は、事務従事者を除く一般利用者である。

1. 本書の目的

ウェブは、情報の伝達や共有に必要不可欠なツールとなっている。一方で、私的目的でのウェブの閲覧、掲示板への無断書き込み等は、大学の社会的信用を失わせる要因となる可能性もある。本書は、このようなリスクを軽減し、情報資産を保護し、利用者がウェブを安心・安全に利用するために必要な事項を定めることを目的とする。なお、ウェブブラウザを利用する PC 端末にはウイルス対策ソフトウェアが導入されているものとする。ウイルス対策ソフトウェアが導入されていない PC 端末でのウェブ閲覧は原則として禁止する。

2. 本書の対象者

2.1 対象者

本書は、ウェブブラウザを教育や研究目的で利用するすべての教員学生（以下利用者と呼ぶ。）を対象とする。 行政事務従事者は、事務手順書のブラウザ手順に従うものとする。

3. ウェブの利用に係る全般的な注意事項

ウェブブラウザを利用したウェブサイトの閲覧、各種情報システムの利用等、ウェブの利用において、利用者の安全性を確保するために、ウェブの利用に係る全般的な注意事項を記述する。

3.1 目的外利用の禁止

(1) 利用者は研究や教育および教育支援等、大学で活動する上で必要な範囲でウェブサイトを閲覧するものとし、それ以外で閲覧しないこと。営利目的でのネットワーク利用は禁止する。

(2) 利用者は学内から任意のウェブサイトを閲覧することにより、閲覧先のサーバに本学のドメイン名及び IP アドレス等が記録されることに留意すること。記録された情報をもとに、サーバ管理者により本学に対して不当な要求が行われるとか、閲覧者の個人情報の開示をサーバ管理者が要求する場合がある。また、掲示板等に名前やメールアドレスを記入して場合、不正請求をされることもある。

【閲覧可能なウェブサイトをコンテンツフィルタリング等により制限する場合（強化遵守事項）】

3.2 閲覧可能なウェブサイトの制限

(1) 適正なウェブ利用を維持するため、コンテンツフィルタリング等により閲覧可能なウェブサイトを制限している。利用者は、閲覧したいウェブサイトが閲覧制限されている可能性に留意すること。

(2) 利用者は、コンテンツフィルタリング等による閲覧制限がなされていないウェブサイトであっても、当該ウェブサイトの閲覧が許可されているわけではない点に留意すること。

(3) 利用者は、制限されているウェブサイトの閲覧が必要な場合には、部局技術管理者に連絡・相談すること。

3.3 プラグイン等の導入・利用の禁止

(1) 利用者は、部局技術責任者が端末で利用可能と定めていないプラグイン（ウェブブラウザの機能を拡張するためのソフトウェア）等の、端末への導入、利用を行わないこと。

(2) 利用者は、部局技術責任者が端末で利用可能と定めていないプラグイン等の導入、利用が必要な場合には、部局技術管理者に連絡・相談すること。

3.4 外部のウェブサイトで提供されているサービスの利用等の注意事項

(1) 利用者は、学外の掲示板、ブログ等への書き込み、ウェブメールの利用等にあたっては、情報漏えいの可能性に十分に注意すること。

(2) 公序良俗に反する不適切な書き込みや利用を行わないこと。掲示板等への単純な書き込みであっても、内容によっては本学や本学構成員の良識が疑われる場合がある。特に、他人への誹謗中傷と誤解されるような記事やプライバシーや著作権等の侵害と疑われかねない書き込みをしてはならない。

(3) 不正なサイトへの誘導を狙ったリンクやウイルス等の不正なソフトウェアをダウンロードさせることを目的としたリンクはインターネット上に多数存在する。有名なサイトであっても決して安全ではないので、不用意にリンクをクリックしないこと。

3.5 ウェブサイト閲覧の監視

(1) 適正なウェブ利用を維持するため、その利用状況（いつ、誰が、どのウェブサイトを閲覧したか等）について監査証跡の取得、保存、点検及び分析を行う可能性がある。利用者は、その趣旨を理解の上、自身のウェブサイトの閲覧がモニタリング及び監査されていることを認識すること。

4. ウェブサイトの閲覧

ウェブサイトの閲覧に使用するウェブブラウザの利用方法、ウェブサイトを閲覧する場合に想定される脅威を回避するための注意事項等について記述する。

4.1 ウェブサイト閲覧時の一般的な注意事項

(1) 利用者は、ウェブサイトを閲覧する場合には、以下の事項に留意すること。

- ウェブサイトの情報には、正しい情報だけでなく偽情報や誤情報が含まれている可能性があるので、ウェブサイトの情報を検討せずそのまま採り入れないこと。
- 目的とするウェブサイトの閲覧には、URI を直接入力すること。データ入力に中継サイトを利用するとデータの詐取やクロスサイトスクリプティングの危険性がある。また、認証を求められるページへ入って後で、そのページから張られたページへのリンクの参照は、認証情報が不正利用されることがあるので注意が必要である。
- ウェブページの再読み込みを短時間に繰り返すと、サービス不能攻撃（DoS 攻撃、サービスに不要な通信をおこさせて、サービスの質の低下を狙った攻撃）と見なされる可能性があるので注意すること。 サイトによっては、当該ドメインや当該 IP アドレスからのアクセスがブロックされる可能性がある。オンラインジャーナルの大量一時ダウンロードによっても、アクセスブロック等の問題が発生することがある。
- 検索サイトでは、検索結果に有害なウェブサイトへのリンクが含まれている可能性があるので、安易に検索結果のリンク先を閲覧しないこと。また、検索結果リストの表示の順番は重要度とか参照頻度といった特別な意味があるわけではない。先頭に表示されるからといって、正しいということはない。
- 有名で広く知られているサイトであっても、バナー広告等を安易にクリックしないこと。有害なサイトやウイルスダウンロードサイトがリンクされていることがある。
- 電子メールで送られてきた HTML メール内のリンクを安易にクリックしないこと。成りすましサイトやワンクリック詐欺サイトへの誘導、phishing 被害につながることがある。次ページに phishing サイトの例を示す。画面上で URI に見える部分は見せかけのテキストで、ID とパスワードを詐取するためのサイトへのリンクになっている。
- ウェブページ閲覧時に、見かけないセキュリティ警告表示とともにソフトウェアのダウンロードを求められてもダウンロードしないこと。ウイルスや不正なソフトウェアをインストールさせられる可能性がある。

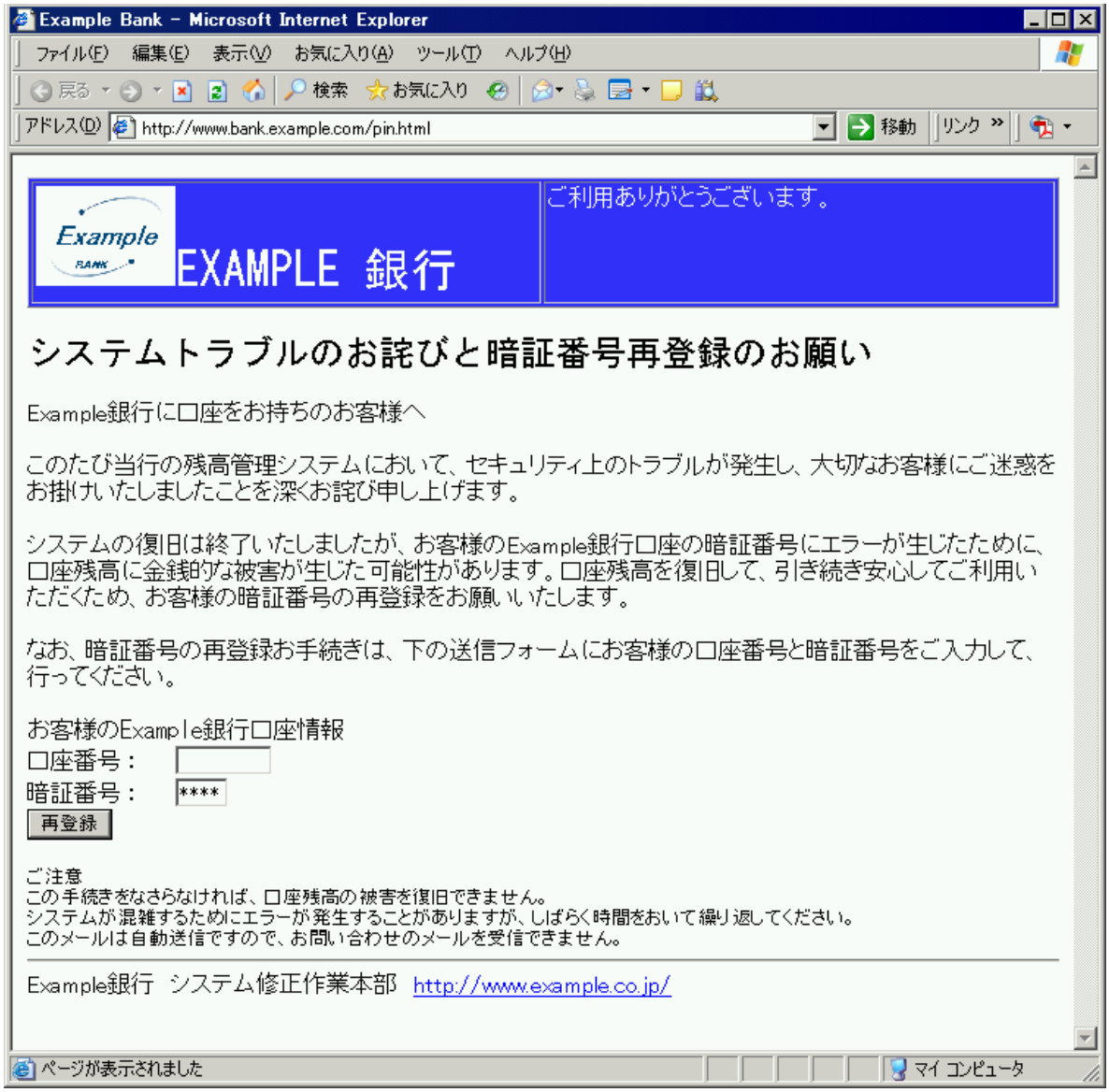


図１　金融機関からの連絡を装って暗証番号を盗み出そうとするサイトの例（説明用に作成）[4]

4.2 TLS（SSL）通信の確認

(1) TLS（SSL）[5]通信とは、通信内容の暗号化及び通信相手のなりすまし対策がなされた安全な通信であり、重要な情報等を送受信するウェブサイトで標準的に利用されている技術である。利用者は、閲覧しているウェブサイトと個人情報、重要な情報等を送受信する可能性がある場合には、TLS（SSL）通信が利用されていることを確認すること。また、その際提示される証明書が正当なものであることを確認すること。証明書によっては、次ペー

[4] 図１～図４では、Microsoft Corporation のガイドラインに従って画面写真を使用しています。
Windows® Internet Explorer® は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

[5] SSL（Secure Sockets Layer）には重大な脆弱性が発見されたため、2015 年時点で一般的に使われているのは SSL の後継プロトコルの TLS（Transport Layer Security）であるが、ウェブサイトとの通信内容を暗号化することは依然として「SSL で接続する」などと表現されることがある。

ジの図のような画面が表示される。このような場合には注意が必要である。

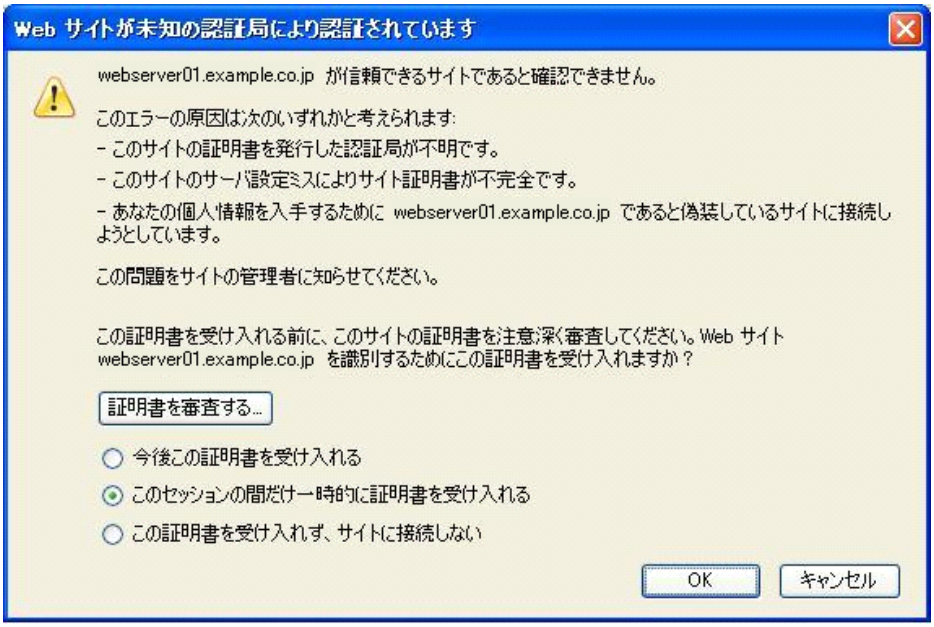


図２　注意を要する証明書への警告表示の例（１）

また、以下のような警告が表示されることもある。

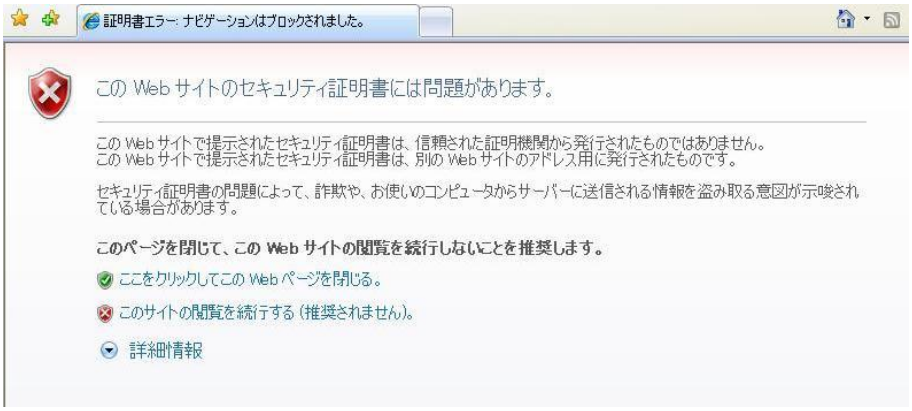


図３　注意を要する証明書への警告表示の例（２）

TLS を利用している場合には、下図のような錠前が表示されることが多い。

図４　TLS を利用していることを示す表示

ただしウェブサーバ証明書は誰でも取得できるものであることを 理解しておかなければならない。

【ウェブブラウザの設定によりダイアログを表示する設定にしている場合】

4.3 確認・警告等のダイアログへの対応

(1) セキュリティ機能に係る設定等により確認のためのダイアログ等が表示される可能性がある。当該ダイアログに関して安易に ActiveX®、Java®等のスクリプトの実行を許可すると、不正プログラムの感染、情報漏えい等の危険性があるため、利用者は、確認のためのダイアログが表示された場合には、中身を確認せずに安易に実行を許可してはいけない。

4.4 ウェブブラウザの設定変更を要求するウェブサイトの閲覧

(1) 利用者は、ウェブサイトから閲覧のためにプラグイン、スクリプト等の実行に関するウェブブラウザの設定変更を要求された場合であっても、ウェブブラウザのセキュリティレベルが低下し不正プログラムに感染する危険性等があるため、当該要求に従ってウェブブラウザの設定を安易に変更しないこと。

5. ウェブサイトへの情報送信（フォームへ入力した情報の送信、ファイルのアップロード等）

送信する情報の盗聴、なりすましによる誤った通信相手への情報送信その他ウェブサイトに情報を送信する場合に想定される脅威を回避するための注意事項等について記述する。

(1) 重要な情報のやりとりには TLS（SSL）等の安全な通信を利用すること。その際、証明書の正当性を確認すること。

(2) 情報の書き込みにあたっては、クロスサイトスクリプティング等の危険性に留意すること。入力の必要なページは、ポータル等を経由せずに参照すること。

6. ファイルのダウンロード

不正プログラムの感染その他ウェブサイトからダウンロードしたファイルを実行又は開く場合に想定される脅威を回避するための注意事項等について記述する。

6.1 ウェブブラウザから直接的に、実行ファイルを実行する行為及び文書ファイル等を開く行為の制限

(1) ウェブブラウザから実行ファイルを直接的に実行した場合でもアンチウイルスソフトウェア等の自動検査機能によりウイルスを検出することが可能であるが、利用者は、実行ファイルをダウンロードする場合には、電子署名及び不正プログラムの有無を確認し、また問題が生じた場合に原因となったファイルの特定を容易にするため、ウェブブラウザから直接実行するのではなく、端末上に一旦ダウンロードすることが望ましい。

(2) ウェブブラウザから文書ファイルを直接的に開いた場合でもアンチウイルスソフトウェア等の自動検査機能によりウイルスを検出することが可能であるが、利用者は、ウェブサイト上にある文書ファイル等を開こうとする（利用しようとする）場合には、不正プログラムの有無を確認し、また問題が生じた場合に原因となったファイルの特定を容易にするため、ウェブブラウザから直接開くのではなく、端末上に一旦ダウンロードすることが望ましい。ただし、信頼できるウェブサイト上にある文書ファイル等を開こうとする（利用しようとする）場合、この限りではない。

(3) 利用者は、ダウンロードした実行ファイルが部局技術責任者により定められた利用可能なソフトウェアに含まれていない場合には、導入、利用しないこと。

6.2 保存したファイルに対する不正プログラムの有無の確認

(1) 利用者は、保存したファイルを実行又は特定のソフトウェアにより開く前に、不正プログラムの有無の確認を行うこと。

(2) 利用者は、保存したファイルに不正プログラムが含まれていることが判明した場合には、当該ファイルを実行せずに又は特定のソフトウェアにより開かずに、部局技術管理者に連絡・相談し、指示を仰ぐこと。

6.3 保存した実行ファイルの電子署名の確認

(1) 利用者は、保存した実行ファイルについて電子署名により配布元が確認できる場合には、配布元が適切な組織であることを確認すること。

6.4 不正プログラムに感染した時の対処

(1) 利用者は、ダウンロードしたファイルを実行し又は開いたことにより、不正プログラムに感染したか又は感染の疑いがある場合には、直ちに LAN ケーブルを抜くことにより当該 PC をネットワークから分離し、部局技術管理者に連絡・相談し、指示を仰ぐこと。

7. 本手順に関する相談窓口

(1) 利用者は、緊急時の対応又は本書の内容を超えた対応が必要とされる場合には、部局技術責任者に相談し、指示を受けること。

(2) 利用者は、本書の内容について不明な点又は質問がある場合には、部局技術管理者に連絡し、回答を得ること。

C3254 情報発信ガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3204	新規作成（ウェブ公開ガイドライン）	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3254	「情報発信ガイドライン」として、ウェブ公開以外の情報発信を含めた形に修正	須川賢洋（新潟大学）
2016年2月5日 C3254	誤記修正と編集用コメントの削除	須川賢洋（新潟大学）

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

1. 本ガイドラインの目的

インターネットによって情報発信を行うことはもはや必要不可欠といえる。一方で、各種権利侵害を伴うような情報の発信は、その為のトラブル対応による業務効率の低下や、本学の社会的信用を失わせる要因となる可能性もある。

大学のドメインからの情報発信だけに限らず、個人契約 ISP の URL や私的な SNS（Twitter, Facebook など）から個人として情報を発信する場合（私的な情報発信）であっても、大学に籍を置く公人と見なされることが多いので注意が必要である。

本ガイドラインは、このようなリスクを軽減し、情報資産を保護し、利用者がインターネットを用いて各種コンテンツや情報を、正確かつ、安心・安全に公開するために必要な事項を定めることを目的とする。

解説：公開コンテンツの内容の多様さとそれに伴う注意事項を中心としたガイドラインとなっている。
その際にまず何より重要なことは、その発信される情報の内容が、正確かつ発信者・利用者にとって安全なものでなければならない。なお大学や学部の公式ウェブページの運用のための指針は、学内の広報規則等に別途定めてあるので、そちらの規則にまず従うことが前提となっている。

2. 本ガイドラインの対象者

本ガイドラインは、インターネットを用いて情報発信を行う本学構成員を対象とする。

解説：学生個人や研究室単位での情報の発信を主に想定したものである。また外部業者に委託する場合も、コンテンツの中身に関する責任は本学にも帰するので注意が必要である。

3. 情報発信に係る全般的な注意事項

各種情報を発信する際には、各種法令を遵守することはもちろんのこと、SINET の利用規約や、関連の学内規則をも守らなければならない。

また公序良俗に反する行為や社会通念上してはならないことは、情報発信の際にも同様に行ってはならない。

解説：各種情報の公開の際に、利用者の安全性を確保し、権利侵害などを防止し、また業務効率を向上させるために、全般的な注意事項を以下に記述する。特にコンプライアンスの精神が必要であることは言うまでもない。
本ガイドラインでは SINET への加入しているモデルとなっている。そうで無い場合でも、契約 ISP との取り決めなどを確認すること。

参考として、以下に SINET の加入規程の一部を記載する。全文は SINET のページ（http://www.sinet.ad.jp/）を参照のこと。

第６条（加入にあたっての遵守事項）
加入者は、次の各号に掲げる事項を遵守しなければならない。
一　研究・教育並びにその支援のための管理業務以外の目的にネットワークを利用しないこと。
二　営利を目的とした利用を行わないこと。
三　通信の秘密を侵害しないこと。
四　ネットワークの運用に支障を及ぼすような利用をしないこと。
五　ネットワーク及び接続するコンピュータに対する不正行為等が発生しないように最善の努力を払うこと。
六　その他所長が別に定める事項

ネットワークを用いた情報発信には大きなメリットがある反面、様々な危険やリスクを伴うことも承知しなければならない。情報発信者の責任として、その意義と危険性についての十分な認識が求められる。ネットワークの世界も現実の世界同様、自己責任の原則によって成り立っていることを忘れてはならない。

3.1 著作権等の知的財産の遵守

他人の知的財産を侵害してはならない。特に、ウェブページ作成・公開時には著作権侵害が発生しやすいので、十分に注意すること。

解説：およそ他人がつくった作品には著作権が存在する。よって自分の作ったコンテンツ以外は原則として許諾なしには掲載してはいけない。
また、ネット上に公開することを著作権者が許諾する「公衆送信権（送信可能化）」は、通常の複製を許諾する「複製権」とは別の支分権でありこれらは別個に許諾を受ける必要がある。その為、複製の許諾を受けたからと言って公衆送信も出来るわけではないことに注意が必要である。
同様に、著作権法第 35 条が規定している「学校その他の教育機関における複製等」の権利制限も、あくまで“複製”に対してのみ及ぶのであって、複製以外の公衆送信権などには適用されないので注意が必要である。
ただし「引用」など、条件を満たせば“著作権の制限”の一つとして、許諾なしでの利用を行うことができる場合もある。

解説：（著作物の保護期間）
著作権の保護期間は、原則、作者の死後 50 年（法人著作の場合は公表後 50 年）である。よって、明治期から戦前期などのものに関しては、著作権が消滅しているかどうか十分に確認すること。また、映像著作物に関しては保護期間が 70 年となったので注意すること。

解説：（引用が成立する条件）
引用は、例外的に著作権者の許諾なく行うことができる。

著作権法 32 条：公表された著作物は、引用して利用することができる。この場合において、その引用は、公正な慣行に合致するものであり、かつ、報道、批評、研究その他の引用の目的上正当な範囲内で行われるものでなければならない。

判例では引用が成立するためには次のような条件が必要とされている。

・正当性　→　それがその場所に引用するに相当する理由が必要である。前後の繋がりのないものをいきなり持ってきても引用とはならない。

・明瞭区分性　→　自己の文章と引用文との違いが明確に分かる必要がある。通常の論文であればカギ括弧で括るなどするのが普通であるが、ウェブ上で表現する場合は、境界線を引いたり、フォントの字体や色などを変えるというやり方でもよいであろう。

・出典元の明記　→　出典先は単なる書物名だけでなく、著者名・出版社・出版年、更に何ページからの引用なのかもできるだけ詳細に記載する必要がある。他のウェブ上から引用する場合は、URL 等を記載しておくと良いだろう。また、ウェブからの引用の場合は状況に応じて参照した年月日を記載しておくとよい。

・自分の文章が主たる物であり、引用先の文章が従たる物であること　→　引用はあくまで自己の著作を補完するものである必要がある。分量的にも、相手先の文章が自己の文章よりも多い場合には引用と認められない。

など。

解説：(著作人格権（特に“同一性保持権”))

作者は著作物の同一性を保持する権利を有している。日本の著作権法は、作者の意に反する改変を認めてはいない（これは人格権として一身専属の権利であり、売買や譲渡もできない)。そこで、許諾を得て他人の著作物を公開する際や、きちんと条件を守って引用をする際であっても、その著作物を掲載する際は改変せずにそのまま載せる必要がある。

解説：(著作権が存在しないもの)

単なるファクトデータ（経済指数や気象統計など）には著作権は存在しない。ただし、これらの他人が制作したファクトデータをそのままコピーして新たなデータベース（いわゆる「創作性のないデータベース」）を作成した場合には、他の法律によって処罰または損害賠償の対象になることがあるので注意すること。例えば、不正競争防止法や民法の不法行為(709 条)などに問われることがある。この件に関しては、自動車の性能情報等一覧データベースに関する判例「翼システム 対 システムジャパン」（東京地裁　平成 13 年 5 月 25 日）が参考になる。

○ネット上での著作権の扱いに関して参考となる URL:

文化庁：http://www.bunka.go.jp/

著作権情報センター（CRIC）：　http://www.cric.or.jp/

3.2 肖像権・パブリシティ権などを侵害してはならない

解説：人は各々、人格権的な権利として、肖像権を有すると考えられている。そこで、他人の顔が写っている写真等を掲載する際には、「肖像権」に十分注意すること。原則、本人の許諾なしに写真を掲載するべきではないだろう。
また著名人の場合は一般人よりは肖像権が制限されると考えられているが、その分、彼らは顧客吸引力という経済的利益を有するので、「パブリシティ権」という権利を持つと考えられている。よって芸能人やスポーツ選手などの写真は無許諾で掲載してはならない。

3.3 他人に迷惑をかけるような情報発信の禁止

ネットワーク上で情報発信する際は、他人に迷惑をかけるような情報を発信してはならない。
他人に迷惑をかけるような情報としては、
・人を誹謗中傷する内容のもの
・他者のプライバシーを侵害するような情報
などがある。

解説：他人への誹謗中傷は、自身のウェブページ、ブログ上ではもちろんのこと、ＳＮＳなどにも書き込んではいけない。こういった行為は名誉毀損に問われる可能性がある。名誉毀損は、民法上の損害賠償の対象となるだけではなく、場合によっては刑法上の名誉毀損罪（刑法 230 条）となり刑事罰（３年以下の懲役もしくは禁錮、または五〇万円以下の罰金）が科される場合があるので、注意が必要である。
また、他人のプライバシーに関する情報を自分のサイトなどに掲載する場合には十分な注意が必要となる。プライバシーは一般的には、他人に知られたくない情報、いわゆるセンシティブ情報だとされているが、プライバシーの概念は判例や法律で厳格に規定されたものでないが故、その判断が難しい。よって他人の情報の取扱に関しては、その掲載がその人に何らかの影響をあたえる可能性がある場合は、掲載するべきではない。（たとえ本人がよかれと思ってやっても、当事者からしてみれば望まぬ結果になる可能性もあるので、悪影響だけではなく、単に影響を与える可能性がある場合でも掲載すべきではない。）

3.4 研究成果や研究途中の情報を掲載する際の注意

研究成果や研究途中の情報を掲載する際には、公開に問題がないか十分留意すること。
実験等で取得したデータについても同様である。

解説：民間企業や他の研究者との共同研究の場合には、守秘義務契約等に違反していないか留意する必要がある。また、特許等の取得を考えている場合も、先にウェブに公開してしまうと公知の事実となり、特許取得の条件である新規性が失われるので注意が必要である。

3.5 企業名やロゴなどの扱い

学会やシンポジウム等で協賛企業のロゴを貼るときは、事前に大学側や相手側と協議すること。

3.6 顔写真の掲載によるリスク

自身の肖像写真を掲載する場合にも、顔を露出する際のリスクを十分に考慮すること。

解説：自分の名前や顔をネットワークに公開することは、そのメリット・デメリットを十分に考える必要がある。場合によっては、他人から謂われのない迫害や誹謗中傷を受けたり、発言に対する揚げ足とりや横やりなどが入ることがある。また、ストーカー被害などに遭うといったことも十分考えられるので、注意が必要である。

研究室構成員の紹介や集合写真などを掲載する場合は、自分一人分だけを掲載するときよりもさらなる注意をすること。原則的には学生の顔は掲載しないことが望ましい。どうしても必要な場合は、写真を似顔絵やイラストなどで代用する方法もある。

さらに、指導教員は学生が各自でウェブページを持つ場合などにおいて十分に注意を促す必要がある。

3.7 その他（公序良俗に反する情報発信の禁止など）

違法な情報はもちろんのこと、公序良俗に反する情報や有害情報を発信してはならない。

解説：わいせつな文書・図画などのほかに、有害情報としては、次のようなものがある。

・情報自体から、違法行為を誘引するような情報（銃器や爆発物、禁止薬物や麻薬の情報など）
・人を自殺に勧誘・誘引する情報
・ネズミ講やマルチ商法の勧誘
・ハラスメントに関する記述を伴うような情報

など。

有害情報や違法情報に関する具体例は、「インターネットホットラインセンター」（http://www.internethotline.jp/）などの運用ガイドラインに詳しいので、詳細はこちらを参考にすると良い。

4. デジタルアーカイブを行う際の注意事項

古典資料などのデジタルアーカイブをネットで公開する際には、各種権利処理が済んでいるかをきちんと確認すること。

解説：古典資料においては、通常、著作権は消滅しているが（＊著作権は、原則、作者の死後 50 年をもって消滅する）、それ以外にも、物件としての所有権やアー

カイブ時（デジタル化時）の費用負担者などとの間での様々な利害関係がある場合があるので、様々な方面からの検討が必要である。
例えば、大学所蔵の古典資料などに関しては、その昔、単に地元の旧家などから保管を委託されただけのものである可能性もありえるし、ネットワーク上で公開をしないことを条件に所有者がデジタル化を許諾したものでないかなども確認すること。
また判例では、「およそ正当な手段を持って入手された著作権の切れたコンテンツの複製物を公表する際には、その原版所有者の許諾は不要である」とされているが(*)、実務では、このような場合にでも、何らかの金銭的支払いを行うこともある。また、事後に資料提供者（デジタルアーカイブ化協力者）との間で、ウェブ上での公開の仕方を巡ってトラブルとなる場合が多いので、事前にできるかぎり詳細な打ち合わせを行っておくことが望ましい。この際に、口頭での取り決めのみしか行わなかった場合、事後にトラブルや遺恨を残すこともあるので、明文化した書類を取り交わしておくべきである。

(*) 顔真卿自書建中告身帖（がんしんけいじしょけんちゅうしんこくしんちょう）事件　最高裁判所昭和５９年１月２０日判決
　顔真卿は唐代の有名な書家である。その顔真卿の書である自書告身帖を複写した写真乾板を所有する出版社がその書集を出版したところ、その原書の所有者から出版の差し止め及び廃棄を求められた事件。その写真乾板はもちろん正当なる手段によって入手されたものである（つまり、盗品、盗撮品ではない）。
　最高裁は、「美術の著作物の原作品に対する所有権は、その有体物の面に対する排他的支配権能でとどまる」とし、複製された写真にまでは及ばないとした。また、「博物館や美術館において、著作権が現存しない著作物の原作品の観覧や写真撮影について料金を徴収し、あるいは写真撮影に許可を要するとしているのは、原作品の所有権に縁由するもので、一見、所有権者が無体物である著作物の複製等を許諾する権利を専有するようにみえるが、それは、所有者が無体物である著作物 を体現している有体物としての原作品を所有していることから生じる反射的効果にすぎない。」との見解を示している。
　3.1 で前述した、著作権情報センターの FAQ にも本事件の解説がある。

5. 各種利用規程の遵守と目的外利用の禁止

5.1 目的外利用の禁止

情報発信者は、本ガイドライン以外にも、関連の情報システムやサービスの利用に関する規程や規約を守らなければならない。また本学の定めるネットワーク利用目的や、SINET が定める目的以外の利用をしてはならない。

本学の情報設備および SINET は、もっぱら教育・研究の推進と職務・支援業務遂行のために提供されている。そのため、情報発信者は、公用と私用の区別を意識して、設置目的にそぐわない

情報を公開しないように注意することが求められる。目的外利用の典型は、本学の情報設備を研究目的ではなくもっぱら利益を上げる商業目的で利用するというような場合である。

解説：目的外利用の一例として、学生が以下のような行為を学術ネットワーク上で行う事は好ましくない。
・自身のページで家庭教師等のアルバイトの宣伝をすること
・アフェリエイトなどの運営　など
教員が自著を紹介する際も注意が必要である。本の紹介や学生へのテキスト販売などに必要な情報を超えての、書物の宣伝・販売行為は、学術ネットワークの目的を超えた利用と見なされる可能性がある。

5.2 本学では、学部や各研究室サーバからの政治や宗教に関する情報の発信はこれを禁止する。

解説：5.2 は「このような記述もあり得る」というサンプル規定である。
政治や宗教に絡む情報に関しては、その扱い方や考え方に様々な基準が考えられる。そこでこれらの情報発信に対する基準をあらかじめ明文化しておくことが大事である。その際の運営方針の一つとして、宗教や政治に関するものを全面的に禁止してしまう方式のポリシーもある。むろん大学や学部の性質によってはこれらに関する情報発信が必要な場合も逆に存在しうるであろう。重要なことは、いずれの場合にでも、その為のガイドラインをきちんと明文化しておくことである。

6. システムの安全性の確保

6.1.セキュリティの確保
　ウェブページを作成するときは、セキュリティの確保に十分注意する。特に OS や各種ソフトウェアなどは修正パッチなどを充て、恒常的に最新の情報を保つこと。
　ページの作成を外部の業者に委託するときも同様である。

解説：サーバシステムを可能な限り安全な状態にしておくことは言うまでもない。ウェブコンテンツを外部の業者に発注するときは、デザインや見栄え、アクセシビリティだけではなく、必ずセキュリティ技術も契約の要件とし、セキュリティ確保分に関しても、相応の投資をすること。外部業者に委託した場合でも、その責任は本学にも帰するので注意が必要である。

6.2 CGI の禁止、SSL/TLS 通信の使用
6.2.1 本学ではウェブページ内における CGI の使用を全面的に禁止する。
6.2.2 パスワードや個人情報を入力するページにおいては、必ず SSL/TLS などで保護された通信を用いること。

解説：6.2 は「このような記述もあり得る」というサンプル規定である。

ポップアップや CGI などを使うページはセキュリティレベルが下がるので、その扱いにおいては、できるだけ使用させないような方向で、統一した基準を設けておくことが望ましい。この場合、禁止としてしまうやり方、あらかじめ大学側が許可したものについてだけ使用を許可するやり方などが考えられる。
またパスワードの入力や個人情報などの入力を求める場合は、必要に応じて SSL/TLS などで保護された通信を用いること。

6.3 隠しディレクトリに関する注意

公開すべきでない情報は、たとえ隠しディレクトリであっても決して蔵置してはならない。

解説：公開ウェブページから直接リンクを張っていない、いわゆる「隠しディレクトリ」や「隠しファイル」であっても、検索エンジンのロボットはこれらの情報も取得していくので、広く一般の人の目に触れて困る情報は、public_html の下に置いてはならない。このやり方は、一部のメンバーだけに情報を提供する際などによく使われるが、どうしても必要な場合は、期間を限定する、Basic 認証を行うなどの手段を用いること。現実に、聴講生だけに成績を通知しようとして隠しディレクトリに成績をおいたまま放置しておいたが故に、それが検索エンジンに収集され学外に流失した事例がある。
いずれの場合においても、前述の通り、そもそも外部の人の目に触れると不都合な情報はウェブサーバ上においてはならない。
また、日付やファイル名をそのまま URL に使うことによって容易に想像されてしまうようなアドレスは、たとえトップページからのリンクを張っていなくても、他人がそれを入力してしまい情報を事前に入手してしまうことがあるので、決してそのようなことはやってはならない。現実に、過去にこのようなやり方を取ってしまったが故に、事前に合格者番号などが漏洩してしまった事例がある。

6.4 公開掲示板（BBS）等の開設の禁止

本学では、研究室サーバや個人のサーバで公開掲示板（BBS）等の開設を禁止する。

解説：6.4 は「このような記述もあり得る」というサンプル規定である。
誰でも自由に書き込める掲示板などは、様々な権利侵害やトラブルの原因となりやすいので、特別の事情がない限り立ち上げない方が望ましい。開設を許可する際も、その基準を明確にしておくことが望ましい。(1)全面禁止、(2)許可が必要、(3)自粛、(4)研究室内メンバーなどの限られた範囲でパスワード等の認証を用いて利用者制限を行う場合のみ許可、などの方針が考えられる。

6.5 十分なサーバ容量やネットワーク資源の確保

ウェブページを公開するためのサーバを設置する際には、そのマシンやネットワークが十分なアクセスに対応しうるものとすること。

解説：大規模な学会やシンポジウムの準備の為に、研究室内のサーバを使う場合などがよくあるが、そういった場合には、システムダウンが起こりやすいので十分注意すること。
特に、大容量のファイル等をやり取りする場合は、自身のサーバだけでなく、その上流のシステムの容量にも十分に配慮しなければならない。
これは、大学や学部の公式サーバで、大学入試の合格者発表を行う際も同様である。

7. ウェブページや掲示板の管理者等の責任の及ぶ範囲

「プロバイダ責任制限法」は、ウェブサイトや掲示板の管理者も「特定電気通信役務提供者」と見なしている。よってこれらのコンテンツの管理を行う者は、同法上の責任と義務を負うので十分に注意すること。

解説：「プロバイダ責任制限法」は、「特定電気通信役務提供者」に対して、損害賠償責任の制限と発信者情報の開示について定めたものである。ウェブサイトや掲示板の管理者も「特定電気通信役務提供者」とみなしている。

7.1 権利侵害があった場合

本学では、自己の管理するサーバやネットワーク内で権利侵害があることが明らかである場合、管理者は、別途定める書式を用い、可及的速やかにその情報を削除させるか、あるいは削除するものとする。

解説：7.1 は「このような記述もあり得る」というサンプル規定である。
自らが管理するウェブ上で、他人の書き込みにより権利侵害（人権侵害や知的財産権侵害）が行われていることを知った場合、管理者は削除義務を負うとされ、削除義務があるにもかかわらず、ただちに削除しなければ、(プロバイダ責任制限法以前から) 権利者／被害者に対して損害賠償責任を負う可能性がある。ただし、「プロバイダ責任制限法の手順に従って権利侵害情報を削除すれば、発信者への損害賠償責任を免れる」とされている。

⇒また、プロバイダ責任制限法ガイドライン等協議会の各種ガイドラインの手続きに準拠する場合には、裁判所も権利者／被害者に対する責任を認めないことが期待できる。詳細は、以下を参照のこと。
http://www.telesa.or.jp/consortium/provider/index.htm

（警告文の例）

警　告

年　　月　　日

＿＿＿＿＿＿＿＿＿＿＿＿＿＿殿

A大学〇〇学部　部局総括責任者
山田　太郎

あなたの開設するウェブページに掲載されている下記の情報の流通により他者への権利侵害が発生していると認められ、加えて被害者自らが被害の回復予防を図ることが諸般の事情を総合考慮して困難と認められますので、直ちに当該情報の送信を防止する措置を講じて下さい。

〇〇日までに送信防止措置がなされない場合、こちら側でコンテンツを削除させていただきます。

掲載されている場所：　※URL や情報の特定に必要な情報を記載
掲載されている情報：　※権利侵害の行われている情報の種類などを記載
プライバシーに関わる情報の掲載
他人の知的財産権の侵害など

なお、上記「プロバイダ責任制限法ガイドライン等協議会」のガイドラインのページにも各種文例があるので参照のこと。

7.2 発信者情報の開示

本学では、権利者（あるいは、権利者と称する者）または捜査機関から、発信者情報の開示請求があった場合は、法的拘束力のある書類（裁判所の令状など）がない限り、これに応じないこととする。

解説：7.2 は「このような記述もあり得る」というサンプル規定である。
自らが管理するウェブ上で「権利侵害が行われているので発信者情報を開示しろ」との要求が権利者を名乗る人物からあったが、権利侵害の事実が明白とは言えない場合、すぐに発信者情報を開示する義務は無い。
捜査機関からの問い合わせに関しても同様であり、令状を伴わない捜査協力依頼の段階ではまだ情報を開示する義務はない。もちろん、この段階で情報開示をすることを、大学としての方針としても構わない。重要なことは、どのようなどのような場合においても、発信者情報開示の際の基準を同一にしておき、

振らさないことである。

⇒その他、発信者情報開示の判断に当たっては、上記プロバイダ責任制限法ガイドライン等協議会の発信者情報開示関係ガイドライン（7.1 解説）を参照のこと。

8. ソーシャルメディアからの情報発信の際の留意点

プロフィールに大学に在籍していることを公開している場合、また公開していなくても検索によってそれが判明する場合には、A大学の信用を損なうことのないよう、学内からの情報発信と同等の注意を要する必要がある。また、発言内容からA大学に在籍していることを特定されてしまうこともある。

9. 本ガイドラインに関する相談窓口

ウェブ管理者は、緊急時の対応および本書の内容を超えた対応が必要とされる場合には、部局総括責任者に報告・相談し、指示を受けること。

解説：研究室レベルのウェブサーバの場合、その管理者が学生や大学院生である場合もある。そのため、彼らが直接判断することが困難な場合に直接相談できる窓口を作っておく必要がある。

C3255 利用者パスワードガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A3205	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3255	パスワードの最短文字数を修正（6文字→8文字）	高等教育機関における情報セキュリティポリシー推進部会事務局
2017年10月17日 C3255	パスワードの安全性に関する最近の考え方を反映	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

1. 本ガイドラインの目的

本ガイドラインは、本学情報システムのアカウントを利用する際のパスワードに関し、利用者が予め理解しておくべき事項を示すことを目的とする。

解説：パスワードの望ましい管理方法として、かつては「定期的な変更」や「記号を含む多様な文字列の利用」が推奨されていたが、現在は総当たり攻撃への対策の観点から、それらの方策よりもむしろ長い（少なくとも 9 文字以上）文字列（パスワードでなく、パスフレーズと呼ばれることもある）を設定することが推奨される傾向にある。ただし、パスワードとして長い文字列の設定や識別が不可能な情報システムやサービスも存在し、こうした情報システムやサービスでは多様な文字列の利用が引き続き有用である。
パスワードの管理を含めた最適な情報セキュリティ対策は情報システムの仕様や脅威の動向などとともに変化することから、本ガイドラインの規定内容については、定期的に見直しを行うことが望ましい。

2. パスワードに係る全般的な注意事項

2.1 初期パスワードの変更

利用者は、アカウントが発行されたら速やかに初期パスワードを自己のものに変更すること。初期パスワードのまま情報システムの利用を継続してはならない。

2.2 パスワードに使用する文字列

利用者が設定するパスワード文字列は、以下の条件を全て満足するものでなければならない。

- 最低限 8 文字以上の長さを持つ。
- 以下ア～ウの文字集合から各最低 1 文字以上を含み、エを加えても良い。
  - ア）英大文字（A～Z）
  - イ）英小文字（a～z）
  - ウ）数字（0～9）
  - エ）システムで使用可能な記号（@!#$%&=-+*/.,:;[]|）

また、以下の文字列は容易に推察可能であるため、パスワードとして設定してはならない。

- 利用者のアカウント情報から容易に推測できる文字列（名前、ユーザ ID 等）
- 上記を並べ替えたもの、上記に数字や記号を追加したもの
- 辞書の見出し語
- 著名人の名前等固有名詞

解説：パスワードとして設定可能な文字列の長さや使用可能な記号の種類は情報システムによって異なるので、ガイドライン策定に先立ち当該情報システムやサービスの仕様を確認する必要がある。

2.3 パスワードの変更

利用者は、アカウント発行者（全学アカウントに関しては情報メディアセンター、個別システムについてはシステム管理者）からパスワードの変更の指示を受けた場合には遅滞なくパスワードを変更しなければならない。変更後のパスワードは変更前のパスワードと類似のものであって

はならない。

解説：パスワード漏えいによる不正利用やパスワード破りによるリスクを減らす手段として、パスワードの定期的な変更には一定の効果があるという考えもある。パスワードの有効期間やパスワード文字列構成検査および世代管理が可能なシステムでは、パスワードポリシーを強制することも可能である。一方で、強固なパスワードを設定し、変更しない方がよいという考え方もある。ここでは、後者の考えを基本に、パスワード漏えいによる不正利用の可能性をシステム管理者が検知したり、一般的なパスワード検査ツールで容易に解読されるようなパスワードの利用者を発見したりした場合に、システム管理者がパスワードの変更を要求するというモデルを想定している。

2.4 パスワードの管理

利用者は、自己のパスワードについて、以下の管理を徹底しなければならない。

- 自己のパスワードを他者に知られないように最大限の注意を払うこと。
- 自己のパスワードを他者に教えないこと。
- パスワードを忘却しないように努めること。
- 他の情報システムやサービス等で用いているパスワードと同じものを用いない（シングルサインオンの場合を除く）。

解説：他の情報システムやサービス等で用いているパスワードと同じパスワードを用いることは、それらのシステムでパスワードの漏えい事故が発生した場合の影響が懸念されることから避けるべきである。この結果、利用者が管理すべきパスワードが増えることになるため、失念を避ける観点からパスワードをメモすることを禁止する必要はないが、パスワードをメモする場合は他者への漏えいを防止するために以下のいずれかの方法を用いることが望ましい。

- パスワードを構成する文字列の一部を伏せる。
- 鍵などの物理的手段で保護可能な場所に保存する。
- パスワード管理用アプリケーションを利用し、そのアプリケーションへのアクセスを何らかの方法で保護する。

3. パスワードに関する各種手続き

解説：本項で扱う事項は実施手順等で別途定めておくべき内容であるが、利用者の便宜を図るためにガイドラインにおいて手続きを説明している。

3.1 パスワードを失念した場合

利用者がパスワードを忘れた場合には、発行部局に対して、所定の様式で、身分証（学生証もしくは職員証等）を持参し、パスワードのリセットを申請しなければならない。パスワードのリセットを受けた場合には、速やかに新しいパスワードに変更すること。

3.2 パスワードの事故の報告

利用者は、アカウントを他者に使用され又はその危険が発生した場合には、直ちに全学実施責任者にその旨を報告しなければならない。

4. パスワード取扱に関する注意

解説：本項で扱う事項は利用者向けのガイドラインに記述してもよい。A 大学では利用者向けガイドラインに相当する文書が学内機器の利用を対象とするもののみであるため、学生等の私物機器での励行を対象に含める意図により、本ガイドラインに含めている。

4.1 パスワードの詐取の可能性のある場所での利用の禁止

パスワードやアカウントを詐取される可能性があるので、学外のインターネットカフェなどに設置されているような不特定多数の人が操作（利用）可能な端末を用いての学内情報システムへのアクセスを行ってはならない。

4.2 画面ロックの励行

利用者は、使用中のコンピュータにログインしたまま離席する場合は、他者が画面を閲覧したり操作したりすることができないよう、画面のロック操作を行わなければならない。

解説：画面ロックの方法としては、パスワードのほか、ジェスチャーや顔認証などがある。パスワードを用いる場合、短い数字（4 桁以内）や他者から容易に推測されるような文字列を設定するべきではない。

C3300 教育テキストの策定に関する解説書

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3300	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3300	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：本書では、このサンプル規程集に収められている教育テキスト(C3301～C3303)を参照する場合の、各大学における策定について説明する。

１．大学における情報セキュリティに関する教育の必要性

情報セキュリティは、一般論として、組織とその事業の運営にとって質や継続性に重大な影響を及ぼしかねない要素である。大学の組織運営においてもそれはあてはまる。さらに、教育機関である大学にとって、学生に対して情報セキュリティに関する教育を行い、情報を取り扱うために必要な資質を習得させることも欠かせない。

大学では多くの場合に、コンピュータのネットワーク接続やシステム設定のような管理業務を、「情報部」のような部署が一元的に行うのではなく、部局や研究室、事務室ごとにいわゆる「管理者」を定めて委ねていることが多いと考えられる。したがって、情報セキュリティの維持のために多くの「管理者」への教育も欠かせない。

２．大学における情報セキュリティ教育の種別

前節で述べた必要性に基づいて、A 大学が行うべき情報セキュリティに関する教育の対象者や内容などの事項を「C2301 年度講習計画」で定めている。これは、学内規程と同様に、大学として遵守すべきものである。

A 大学では、情報セキュリティ教育を次のように３つの種別に分けた。

(1) 一般利用者向け教育

これは、情報処理演習で情報教育システムや情報ネットワークを利用する立場の学生や、事務情報システムを端末や PC から利用する一般職員などを想定している。これらの対象者には、それらの利用に関して法律や学内規程によって定められている順守事項や許諾範囲、あるいはマナーや心がけるべきことがあることを理解させることができるように、教育しなければならない。

これらの対象者は情報システムやネットワークの設定操作や運用のような管理について権限をもたず、それに関する責任もないと考えられるので、管理に関する教育は必要がない。ただし、規定されている内容を利用者が理解するための最低限の技術的な知識も教育内容に含まれる。

一般利用者向けの教育は、学生の入学あるいは教職員の採用のときのように、新たな利用者に加わった者を対象として実施する「基礎講習」が基本である。これは、1 年生の情報処理演習の講義や、あるいは新規採用者講習の中で実施することも考えられる。そのほかに、定期的な再教育と、技術面や法律・制度面の最新知識を習得させるために「定期講習」も行う。

(2) システム管理者向け教育

A 大学には、全学的な情報システムを設置し運用する情報メディアセンターのほかに、部局や研究室でウェブサーバや電子メールサーバなどの情報システムを運用することがある。そのいずれのケースでも、情報セキュリティを高いレベルで維持できるように運用管理しなければならない。したがって、その管理を担当するシステム管理者に対して、情報セキュリティ対策の応用知識を定期的に教育する必要がある。

情報メディアセンター以外の一般の部局におけるシステム管理者に対しては、部局における運用に必要な技術や状況などの知識を習得させるために「部局管理者」向けの教育を講習会などの

スタイルで情報メディアセンターが実施する。

システム管理者のうち、情報メディアセンターの教職員については、とくに専門的分野に携わっていることから、他の部局の管理者と分けて教育を実施することが適当と考えられる。これは情報メディアセンターが内部的に実施するものであるが、学外のセミナー等を利用する方法もとりうる。

なお、たとえば PC 一台ごと、ネットワーク機器一台ごとについて適切なシステム管理が必要であって､PC やネットワークを設置する者には管理者責任を負えるような専門的知識の教育をなすべきであるという考え方があり、あるいは PC やネットワーク機器の設置を何らかの有資格者に限定すべきであるというような考え方もあり、厳密にはそうしなければならない。しかし一方で、専門的知識を習得した管理者をすべての PC について割り当てることは、多くの大学において現実的ではないことが考えられ、たとえば一般利用者とシステム管理者の中間的な位置づけの教育を実施する考え方もありうる。

(3) CIO/役職者向け教育

大学の運営、とくに業務遂行とそのための予算配分と人員配置に責任のある執行部（理事会、事務局長、CIO など）を対象とする教育は、情報セキュリティ対策の必要性と課題について理解を得るためのものである。その内容は、技術などの各論的知識ではなく、情報セキュリティのためのコスト（人と予算）の理解を得て、また、状況を的確に把握して、必要な対策を指揮できるように備えておくことである。

3. 大学における情報セキュリティ教育のテキスト

情報セキュリティ教育のそれぞれの種別について、教育を実施する際のテキスト（あるいは教材）が必要である。一般利用者を対象とする教育のうち、一般論については市販の教科書（情報処理演習の一部としているものを含む）を利用することもありうる。しかし、いずれの種別の教育でも各大学の情報セキュリティポリシーや情報システムサービスなどによって具体的な情報に関する内容が異なるので、その情報についてテキストを独自に準備することが必要になる。とくに、CIO/役職者向け教育はその大学における情報セキュリティの状況を説明することが重要であるから、そのときの状況を取り入れた説明資料を情
報メディアセンターにおいて作成することが必要になる。

このサンプル規程集に収めた３つの教育テキストは、講習計画に沿って教育すべき内容の概要を示しつつ、各大学の状況によって教育テキストを作成するためのガイドラインとして示した。

C3301 教育テキスト作成ガイドライン（一般利用者向け）

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A3301	新規作成（教育テキスト）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A3301	「教育テキスト作成ガイドライン（一般利用者向け）」として、内容を一般利用者向けに見直し	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3301	高等教育機関の実態に合わせた内容の見直し	上田浩（京都大学） 須川賢洋（新潟大学） 中西通雄（大阪工業大学）

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：本文書は独立した形で利用可能な、一般利用者向けの教育テキストです。内容はできるかぎり正確な記述とするよう心がけましたが、記述の簡潔さを優先したために一部不十分な表現になっていたり、逆に記述が重複しているところもあります。また、自習用のテキストではなく、講師が一般利用者の立場やスキルに応じて適切な助言を行いつつ講義を行うことを前提として、その講習用テキストとして作成してあることにご留意ください。

このテキストは、「C2301 年度講習計画」に従って、60 分ないし 90 分の基礎講習用として作成したものです。受講対象は、本学情報システムを新たに利用することとなった学生・教職員です。テキストの内容は、本学情報セキュリティポリシー（の各規程）に基づいて、できるだけ具体的にわかりやすい形で説明しています[6]。

1. はじめに

1.1 情報システムの目的

本学情報システムは、本学の理念である「研究と教育を通じて、社会の発展に資する」ことを実現するために、本学のすべての教育・研究活動および運営の基盤として設置され、運営されています。したがって、情報システムを秩序と安全性をもって安定的かつ効率的に運用することが不可欠です。このためには、本学情報システムを利用するすべての人が、本学のセキュリティポリシー（運用基本方針、運用基本規程）や利用に関する規則を遵守せねばなりません。

1.2 情報システム利用者の心構え

「コンピュータ教室で、ログインされたままのパソコンを何者かが操作した。」、「他人の著作物を無許可でウェブサーバに置いて公開し、著作権者から注意を受けた。」、「新しいパソコンをネットワークに接続して、OS のアップデートをしている間にウイルスに感染してしまった。」、「研究室のウェブサーバがフィッシングに利用された。」などの事件が発生しています。法令に違反しないことは当然ながら、本学の情報システムを円滑に運用するためには、各利用者が本学構成員の一員であるという認識をもって、十分な注意を払ってコンピュータを操作することが必要です。まず、このことをよく理解してください。

1.3 利用についての原則

（利用の精神）

(1) 本学情報システムの利用にあたっては、つぎのことに留意するとともに、基本的な社会常識

---

[6] 教育を担当される教員の方へ：学生に対して「情報リテラシー」などの講義の中で実施する場合には，一回ですべてを教えてしまうのではなく，毎回の講義の中で関連する部分をとりあげていくのがよいでしょう(マイクロインサーション)。例えば，個人のウェブサイト作成の授業ときに著作権に関することを教えるなどして，工夫してください。

に従い、他の利用者や通信先に対する配慮をもって利用してください。

- 言論の自由、学問の自由
- 他者の生命、安全、財産を侵害しない
- 他者の人権、人格の尊重
- 公共の福祉、公の秩序

（法令の遵守）

(2) 法令の遵守

本学情報システムでの行為は治外法権ではありません。日本国内においては日本国内法が適用されます。場合によっては海外の法律の適用をうける可能性もあります。法令や公序良俗に反する行為を行ってはなりません。

（目的外利用の禁止）

(3) 本学情報システムは、教育・研究活動および運営の基盤として設置・運営されているものです。これらの目的に該当する範囲で利用してください。

（利用規程と罰則）

(4) 「C2201 情報システム利用規程」に違反する行為をした場合には、警告、利用制限、所属部局への通報などの措置がとられることがあります。また、不正利用の発生とその対処について、利用者の氏名を含め公表されることがあります。なお、個々の部局等ネットワークの利用については、それぞれ規則が定められていますので、個別のルールに従ってください。

以下、2 章で具体的に説明しますが、1.3(1),(2)は本学情報システムに限らず一般の広域ネットワークの利用でも共通する事項であることに留意してください。

2. 法令および利用規則の遵守

2.1 法令および利用規則に違反する行為

関連する法令としては、憲法、刑法、民法、商法をはじめとして、不正アクセス禁止法、著作権法、不正競争防止法、プロバイダ責任制限法、その他多くのものがあります。また、外国に影響を及ぼすときは外国法の適用を受ける可能性があることにも留意せねばなりません。例えば、次のような行為をしてはなりません。また、他人の犯罪行為の手伝いもしてはなりません。幇助罪として処罰されることがあります。

(1) 基本的人権・プライバシーの侵害

本学情報システムの利用に限らず、基本的人権を尊重せねばなりません。人種・性別・思想信

条などに基づく差別的な発言をネットワークで公開すると、基本的人権の侵害となることがあります。誹謗中傷は名誉毀損で訴えられることがあります。
本学情報システム利用者のプライバシーは尊重されますが、利用者は他人のプライバシーも尊重しなければなりません。他人のプライバシーを勝手に公開してはなりません。私信の無断開示などもそれにあたります。慰謝料の請求を受けることがあります。
他者の名前やログイン名をかたって、電子メールを送ったり SNS に書き込みを行うこともしてはなりません。

(2) 不正アクセス行為

利用権限は正しく使用せねばなりません。また、パスワードを盗まれて不正行為が行われないようにするため、パスワードを厳格に管理することは、システム管理者および利用者の責務です。利用者は、以下のような行為をしてはなりません。

(a) 他者のアカウントを使う

利用者は、他者のログイン名を用いてログインしてはいけません。この行為は不正アクセス禁止法で犯罪とされています。また、利用者は、自分の利用権限(アカウント)を他人に使わせてはなりません。本人のログイン名で他者に本学情報ネットワークを使用させたり、ファイル格納領域などの資源を他者に使わせることもこれに含まれます。

(b) 他組織への侵入

セキュリティホール等を利用してコンピュータシステムに侵入する行為も不正アクセス行為です。本学情報システムの内外を問わず、利用資格のないコンピュータを使用してはなりません。また、他組織への侵入を試みるようなことも絶対にしてはなりません。

(c) 不正アクセスを助長する行為

直接に不正アクセスを行わなくとも、不正アクセスの用に供する目的で他人のパスワードを取得したり提供したり保管したりする行為も、同様に不正アクセス禁止法違反として罰せられます。その為のフィッシングサイト、フィッシングメールを作成・送信する行為も同様です。

(3) 知的財産権の侵害[7]

知的財産権は、人間の知的創作活動について創作者に権利保護を与えるものです。絵画・小説・ソフトウェアなどの著作物、デザインの意匠などを尊重することに心がけて下さい。 著作物の無断複製や無断改変はしてはなりません。例えば、本・雑誌・ウェブページなどに提供されている

[7] 著作権侵害とならない引用や私的使用については，講義時間に余裕がある場合は触れておくのがよいでしょう。特に，引用については，ウェブによる情報発信方法の講義や，レポートの書き方の講義で説明すべきです。

文章・図・写真・映像・音楽などを、無許可で複製あるいは改変して、自分のウェブページで公開したり、SNS に投稿したりしてはいけません。他人の肖像や芸能人の写真については、肖像権や・パブリシティ権の侵害になることがあります。

(a) 著作権

著作物（小説、音楽、絵画、映画、写真、プログラム、データベース等）には著作権があります。著作権は、著作物の作者が自分の作品を勝手に公開されたり改変されたりすることで気分を害されることのないようにするという働き（著作者人格権）と、著作物を勝手にコピーされたりして作品の価値が下がってしまうということのないようにする働きがあります。ただし、著作物の利用を永久に禁止すると、文化の普及や発展に悪影響を及ぼしますので、一定期間経過後は自由に利用してもよいことになっています。

著作物を著作権者の許可なくコピーして他人に渡したり、ウェブページなどで公開すると、著作権者から損害賠償を要求されたり、罰せられることもあります。海賊版(違法に複製 された著作物)の音楽や映像を大学や自分のパソコン、スマートフォンなどにダウンロードすることも違法で罰せられることもあります。著作物の一部を利用したり、改変、翻訳、編曲、翻案することも、著作権者に無断で行ってはいけません[8]。

意識的に公開したつもりがなくても、コンピュータがウイルスに感染していたり、ファイル共有ソフトウェアの設定によっては、著作物が外部に公開・共有されてしまうことがありますので、ファイル共有ソフトを使ってはいけません[9]。また、ディジタル著作物には、アクセス（利用）ができないように制限がかかっているものもありますが、その制限を無効にして対象機器以外でゲームをできるようにしたりする装置やソフトウェアを販売したり配布すると、罰せられることがあります。

また、コピーガードが外された著作物をコピーした場合にも著作権侵害に問われることがありますので、注意が必要です。

(4) 肖像権、パブリシティ権の侵害

他人の肖像を本人に無断で写真に撮ったりインターネットに公開したりしてはいけません。写真を撮られたり公開されたりすることが、嫌悪感につながることも多く、人格権の侵害であると考えられるからです。このような行為をすると、肖像権の侵害として訴えられ損害賠償を請求されることがあります。

また、タレントやスポーツ選手など有名人の写真は、それだけで経済的な価値がありますので、パブリシティ権の侵害として、経済的な損失について賠償請求されることになります。

---

[8] 受講対象者によっては，著作権法違反になりうる具体例を挙げて説明するのもよいでしょう。

[9] 「情報システム利用規程」(C2201)の第十条十五項で、教育研究目的以外での P2P ソフトウェアの利用は禁止されています。

(5) 個人情報・機微(センシティブ)情報の漏えい

以下に挙げるような､個人情報や機微(センシティブ)情報をパソコンやスマートフォンで取り扱う場合は、これらの情報が不必要に流出しないように細心の注意を払う必要があります。

(a) 氏名、住所、生年月日、電話番号、メールアドレスなど、個人を特定できる情報
(b) 個人の所在地などの位置情報
(c) 病歴、持病、血液型などの医療情報
(d) 家族・親族関係や出身地などの情報
(e) 個人の趣味や嗜好などに関する情報
(f) 借金の有無や残高などに関する情報
(g) 銀行口座番号やクレジットカード番号、健康保険証番号など

(6) 有害情報の発信

違法な情報はもちろんのこと、公序良俗に反する情報や有害情報を発信してはいけません。本学情報システムを用いてわいせつな文書・図画などを公開してはいけません。また、それらへのリンクを提供してはいけません。このほか、次のような情報の公開も、研究上必要な場合を除き、禁止します[10]。詳しくは、「C3254 情報発信ガイドライン」を参考にしてください。

・情報自体から違法行為を誘引するような情報（銃器や爆発物などの情報、禁止薬物や麻薬の情報など）
・人を自殺等に勧誘・誘引する情報
・ネズミ講やマルチ商法の勧誘

2.2 教育・研究目的に反する行為

本学情報システムは、教育・研究活動および運営の基盤として設置されています。教育、研究および運営という設置目的から逸脱する以下のような行為は、利用の制限や処分の対象になることがあります。

(1) 政治・宗教活動

本ネットワークは本学の財産ですから、特定の団体に利便を供するような活動に用いてはいけません。

(2) 営利活動の禁止

広告・宣伝・販売などの営利活動のためにウェブページや電子メールを用いてはいけません。

---

[10] 各大学で発信する情報をどこまで禁止しているかに依存します。

塾のプリントを作成したりすることもこれに含まれます。

(3) 運用妨害

物的な加害の有無に関わらず、本学情報システムの運用を妨害する行為は禁止します。例えば、本学情報システムに悪影響を与えたり、他の利用者に迷惑をかけたりするような過剰な利用は避けねばなりません。

(4) 目的外のデータの保持

個人に与えられたファイル領域やウェブページ領域に、教育・研究の目的に合致しないものを置くべきではありません。

3. 利用心得

3.1 ネットワークを快適に利用するために

法令や公序良俗に反せず、教育研究目的に合致した利用であっても、注意すべきことがいくつかあります。ここでは簡単に触れておきます。

(1) 品位をもって利用する

本学の構成員としての品位を保って利用すべきことは言うまでもありません。品位に欠けるメッセージの発信は謹んで下さい。

(2) 他人を思いやって利用する

動画など大量のデータを送受信したりすると、本学情報システムを利用している他人に迷惑をかけることになりますから、十分注意してください。また、共同で利用するコンピュータ設備は、ゲームで占有したりせずに、他人に対する思いやりをもって利用してください。

解説：ネットワーク帯域やチャネルを占有する行為との例として以下があります。

- YouTube などの動画を長時間視聴する
- ゲーム機やスマートフォンなどを学内無線 LAN に不必要に接続する

(3) パスワードを適正に管理する

パスワードはあなたが正規の利用者であることを確認するために大切なものです。自分のパスワードを友人に教えたり、友人のパスワードを使ってコンピュータを用いてはいけません。パスワードを教えた人、教えてもらって利用した人の双方が責任を負うことになります。

パスワードを他人に分かる状態にしないでください。メモが必要な場合は、自分なりに工夫して一目見ただけではそれがパスワードであることが分からないようにしましょう。他人がパスワードを入力するときには、顔をそむけるという配慮もよく行われています。

本学情報システム以外にも SNS やショッピングサイト、学外のメールサービスなど様々なサー

ビスを利用するためにパスワードが必要となりますが、サービスごとに違うパスワードを設定するようにしましょう。パスワードを共通のものにしていると、万が一パスワードが漏えいした場合、それらのサービスが不正に利用されるだけでなく、あなたの学務情報などへの不正アクセスが行われるかもしれません。

アカウントを盗用されても、直接的な経済的不利益は被らないかもしれません。しかし、例えば、パスワードを知られたために、自分のアカウントから他人を侮辱する内容の電子メールが発信された場合、あなたが侮辱行為者として扱われます。また、あなたのアカウントを利用して他の計算機への侵入行為が行われた場合(これを踏台アタックと呼びます)、アカウントを盗用された被害者が、まず最初に犯人として疑われるのです。

強い(破られにくい)パスワードの例：パスワードには、辞書に載っているような単語を避けること、および、英小文字だけでなく、英大文字・数字・記号を含めるようにしてください[11]。

(4) 自己の情報を守る

共用のサーバコンピュータに置かれたファイルには、他の利用者から読まれないようにアクセス権限を適切に設定しましょう。誰からも読める、または誰からも書き込めるという状態は非常に危険です。また、他人のファイルが読めるようになっていたとしても、無断でその内容を見ることはやめましょう。ウェブページ・・SNS などに、自分の個人情報やプライバシー情報、位置情報を提供することも危険につながります。

ウェブページやブログ・SNS 等に書いて公開すること以外に、情報を保存してあるパソコンやスマートフォン、メモリカードなどを放置したり紛失することで、意図せずに情報が流出することがあります。同様に、ファイル共有ソフトウェアを使用している場合に、これらの重要な情報が外部に対して公開されてしまっていることもあります。

このように、パソコンのセキュリティ対策が不十分であると、コンピュータウイルスなどの悪性プログラムに感染し、これらによって情報が自動的に外部に送信されたり、ファイル共有ソフトウェアで共有されることがあります。

いずれにしても、いったん流出した情報は、たとえ後で公開を取りやめたとしても、既に第三者にコピーされていることが多く、回収することは困難です。自分自身の個人情報や秘密情報を流出させてしまった場合には、自分自身に、肉体的、精神的、金銭的な被害が生じますし、他人の個人情報や機微(センシティブ)情報を流出させてしまった場合には、法的に訴えられる可能性が生じますので、十分な注意が必要です[12]。

(5) 本学情報システムのセキュリティ保持に協力する

---

[11] これらの文字を含まないようなパスワードは設定させないようにしているシステムもあります。

[12] ここでは，主に個人的なレベルの個人情報の取り扱いに関する注意を述べています。業務として，一定規模以上の個人情報を収集し取り扱う場合は，個人情報保護法（**国立大学法人の場合は、独立行政法人等個人情報保護法**）の規定や，本学情報格付け規定に従う必要があります。

セキュリティを保持するために、利用者自身が注意すべきことがあります。例えば、コンピュータウイルスを持ち込まない、不審な発信元からのメールを開かない、自分の管理しているコンピュータにウイルス対策ソフトを導入しウイルス検知パターンを常に最新状態に保つ、本学情報システムの故障や異常を見つけたら速やかに管理者に通報するなどが、これに該当します。

大学のネットワークは、多くの管理者によって支えられています。ネットワークでは、一部の利用者の自分勝手な行為や心無い行為によって、ネットワークの利用が著しく制限されたり、大学全体の信用が失われたりすることがあります。ひとりひとりのネットワーク運用への協力が、よりよい教育・研究環境の構築につながることを自覚しましょう。ネットワークの利用中に、ネットワークの安定運用に関わる問題点に気づいたら定められた窓口に報告してください。

3.2 メールの利用に関して[13]

・メールの信頼性を過信しないようにしましょう

電子メールは、複数のコンピュータを中継して配送されますので、遅れて届いたり、相手に届かないこともまれですがあり得ます。また、宛て先アドレスが変更になっていたり、迷惑メールと間違われて配送されないこともあります。重要な用件をメールのみに頼るのは避けて、状況に応じて他の手段を併用しましょう。

・あいさつ、自己紹介など、手紙としてのマナーを守りましょう

親しい友人へのメールであれば、用件のみを伝えることもありますが、そうでない人へのメールは、あいさつや自己紹介などを忘れないようにしましょう。

・宛て先を間違えないようにしましょう

メールの宛て先を間違えると、メールシステムに余計な負担をかけ、管理者に迷惑をかけることがあります。また、大切なメールが意図しない人に届き、個人情報などが漏えいすることもあります。メーリングリスト等で届いたメールに対して返事を出すと、メーリングリストの登録者全員にメールが届いてしまうことがあります。メールを送信する前に宛て先を確認するようにしましょう。

・Cc、Bcc の使い方

本来の宛て先ではない人にメールのコピーを送っておきたいときには Cc (Carbon Copy)や Bcc (Blind Carbon Copy) を使います。メールの返事を書くときは、Cc に書いてある人にも返事を出す必要があるかどうかを考えましょう。メールの宛て先(To)や Cc に書いたアドレスは、メールが届いた人全員が見ることができます。他に誰に出したメールか知られたくない

[13] 詳細は、C3252 電子メール利用ガイドラインを参照のこと。

場合は、Bcc に宛て先を書きましょう。

・サブジェクト（題名もしくは件名）をつけましょう

多くのメールが届く人は、サブジェクトを見てメールを整理します。内容を簡潔に表すサブジェクトを付けるようにしましょう。

・機種依存文字、HTML メールに関する注意

記号や罫線、絵文字等の中には、特定の機種でしか表示できないものがあります（ローマ数字（時計文字）や、丸数字（マルの中に数字）など）。また、いわゆる半角カナも使用してはいけません。HTML(リッチテキスト)形式のメールは、原則として使ってはいけません。これは、受信した側のセキュリティ水準の低下を招くおそれがあるからです。

解説：当事者同士の合意を得た上で HTML メールが使われる場合があります。

・添付ファイルに関する注意

添付ファイルを使用する場合は、ウイルス等と間違われないように、どのようなファイルを添付するのか、必ず本文中で説明をするようにしましょう。また、特にサイズの大きな添付ファイルは、メール配送システムに大きな負担をかけます。他の方法がないか検討し、相手先に確認をしてから送りましょう。

・メールの転送設定に関する注意

メールを自動転送している場合には、携帯電話などのアドレスを含め、転送先のアドレスが有効かどうか定期的に確認してください。届かないアドレスへの転送は、大学のメール配送システムに大きな負担をかけることに加え、授業に関するものなど、あなたへの重要な連絡が届かないことになります。

解説：スマートフォン等で直接メールシステムにアクセスできる環境が整備されている場合には、転送設定を推奨しない方が良いと考えられます。

・チェーンメール (chain mail)、デマメールの禁止

複数人へのメールの転送を求めるチェーンメール（不幸の手紙などのように、同じ内容を別の人に転送するように要請するもの）は、メールの配送システムに大きな負担をかけ、システム管理者にも迷惑をかけますので、加担してはいけません。メールの内容が重要かつ緊急を要すると思われてもデマの可能性もありますので、よく確認をして、必要であればマスコミ等、他の手段での伝達を考えるようにします。

・迷惑メールやフィッシングメールへの対策

迷惑メールやフィッシングメールが届いても、配送中止の依頼も含めて返事を出してはいけません。メールが確実に届いていることを相手に知らせることになります。迷惑メールやフ

ィッシングメールの本文には特定のサイトへのリンクが設定されていることが多いですが、それらをクリックしてはいけません[14]。また、自分のメールアドレスをウェブや掲示板に掲載すると、迷惑メールが多く届くようになりますから、メールアドレスの取り扱いは慎重に行いましょう。

・PC のメールと携帯電話のメールとの違い

PC のメールでは携帯電話のメールと異なり、すぐに返事ができるとは限りません。たとえ、すぐに返事が来なくても、怒ったりしてはいけません。

・メールアドレスの扱い

メールのアドレスはウェブなどで不用意に公開しないことが望ましいでしょう。しかし、講演会の連絡先等のために公開する必要が生じることもあります。そのような場合には、次のような方法をとるのがよいでしょう。

(i) メールアドレスをロボットで機械的に収集されないように、メールアドレスの全部あるいは一部を画像にしたり、アドレスの一部の@記号を --atmark-- のように別の文字列に置換したりしてウェブに掲載する。

(ii) 講演会への参加申し込みなどのように、掲載期間が限定されている場合は、申込み専用の時限アドレスを使用する。

3.3 グループウェアサービスの利用

研究室や研究グループなどの情報共有にグループウェアサービスを利用することがあるかもしれません。情報漏えいを避けるため、利用にあたり公開設定、共有設定、情報の格付けが適切になされるよう留意してください。また、機密情報や機微情報を掲載することについての判断は慎重に行ってください。

解説：A 大学では情報の格付けの対象は教職員のみを想定していますが、グループウェアサービスを研究に参加する学生が利用する場合には教職員の監督のもと、情報の格付け関連規定を学生にも遵守させる措置を取るなど各大学の判断が必要となります。

3.4 掲示板、SNS (Social Networking Service) などの利用

・誹謗中傷をしない

実名の場合はもちろん、匿名の掲示板であるからといって、誹謗・中傷をしてはいけません。

---

[14] フィッシングメールは，その内容が非常に巧妙なものもあり，利用者がフィッシングメールであることに気づかずに対応してしまう危険性もあるので，必要に応じて具体例をあげて解説を行うとよいでしょう。

名誉毀損などで訴えられることがあります。相手が特定できなくても、人種差別など許されない発言があります。一般社会で許されないことはネットワークでも許されません[15]。

・フレーミング（炎上）に注意

ネットワークでは、些細なことから議論が白熱し、誹謗中傷の応酬や水掛け論になってしまうことがよくあります。冷静かつ誠実な対応を心掛けましょう。

・掲示板毎のルールに従う

掲示板や、SNS には、そのコミュニティ毎に個別のルールが設けられていることがよくあります。いくつかの記事を読んで雰囲気を理解してから、発言するのがよいでしょう。

3.5 ネットワークの過度の利用による悪影響

パソコンやスマートフォンなどによるネットワーク利用は便利ですが、長時間にわたって過度な利用をすると、以下にあげるように心身面に様々な影響が生じることが指摘されています。十分な休息と適度な運動を心掛けましょう。

・対人関係などコミュニケーション能力の阻害
・学業成績の低下
・生活リズムが不規則になることによる心身障害
・姿勢や視力への悪影響

4. 情報セキュリティの基礎的知識

4.1 インターネットのしくみ（IP アドレス、URL、HTTP）

(1) IP アドレス

PC をインターネットに接続して利用するためには、その PC をインターネット上で一意に識別できるよう、住所や電話番号に相当する「アドレス」が必要となります。インターネットでは、「IP アドレス」と呼ばれるアドレス体系を利用します。具体的には 32 桁の 2 進数で表現されますが、それでは分かりづらいのでこれを 8 ビット毎に切って 10 進数で表現します[16]。つまり、「192.168.0.1」のように 0～255 までの数字を 4 つ、ピリオドで区切って並べたものになります（図１参照）。

---

[15] 匿名の掲示板等であっても，捜査機関等からの要請があれば，ログ情報から利用者が特定されます。
[16] IPv4 の場合。

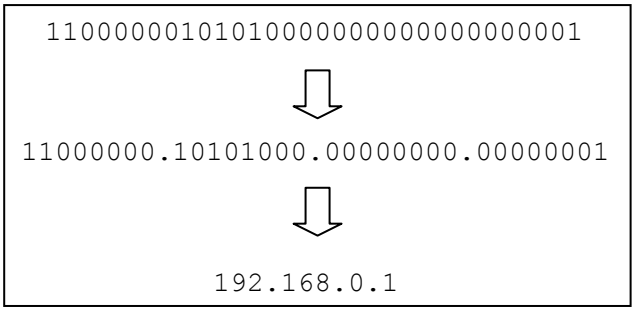


図１：IP アドレスの例

このような IP アドレスは基本的にインターネット上で固有のものでなければなりませんが、様々な理由から「プライベート IP アドレス」と呼ばれるものも利用されています。

インターネットにおいて、データは「パケット」という形式により共有回線上でやりとりされます（パケット交換方式）。パケットは、元々送信しようとしていたデータ（例えば電子メールのデータ）にヘッダ（小包の表書きのようなもの）等を加えたものです。

すべてのパケットについて、ヘッダに発信元および宛先の IP アドレスが書き込まれます。従って、基本的にインターネットにおける通信は匿名ではないと考えるべきです。また、たとえどのような暗号化を行ったとしても、「どのコンピュータから情報が発信されたか」「どのコンピュータ宛てに情報が送信されたか」という記録は残ります。暗号化しなければ基本的に万人が観察可能な状態で通信が行われますので、インターネットは安全であることを仮定することができない通信手段ということができます。電子メールにしてもウェブにしても、せいぜいはがき程度の秘匿性しか持ち合わせていません。機密性の高い情報は必ず暗号を利用するべきです。

(2) ドメイン名

さて、このような IP アドレスを覚えるのは現実的ではありません。そこで、コンピュータにニックネームを与え、そのニックネームを IP アドレスに変換するシステムを考えます。これを DNS（Domain Name System）と呼びます。これにより、例えば www.kantei.go.jp という「ドメイン名」を IP アドレスに変換することができます。ドメイン名は階層的な構造を持っており、ある程度類推をすることもできるといった特徴があります。

このドメイン名は安全なウェブの利用で重要なポイントとなりますので、どのドメイン名がどの企業や大学等の組織（のサービス）のものであるか、重要なものについては覚えておくようにしましょう。特に金銭や個人情報等の取り扱いに注意が必要な情報のやり取りを伴うサイト、つまり銀行等の金融機関、ショッピングサイトなどについては重要です。

(3) URL と HTTP

ウェブでは、URL（Uniform Resource Locator）という形式で情報の入手元を指定します。これは、図２のような構造を持ちます。

図２：URL の構造

一番左の「http://」が「スキーム」で、情報（正確にはリソースといいます）にアクセスするための方法を指定します。次が「オーソリティ」で、そのリソースを管理しているコンピュータを指定します。オーソリティにはドメイン名や IP アドレスを利用することができます。最後がパスで、そのオーソリティのどこにリソースがあるのかを指定します。ここでは「jp」というディレクトリ（フォルダ）の中にある「link.html」というファイルを指定しています。

ここで利用されているスキームは HTTP（Hyper Text Transfer Protocol）です。これは文字通り「転送」のためのプロトコル（決まり事）です。ウェブブラウザは URL に書かれているオーソリティにアクセスし、パスをたどってファイルを取得して表示等を行います。つまり、ウェブブラウザは基本的にダウンロードのためのシステムであるということができます。ここは重要なポイントです。ウェブはテレビ放送のように一方的に送りつけられている情報を受動的に画面に映しているわけではなく、あくまでも自分でリクエストした情報をダウンロードしているのです。IP アドレス等の情報がリクエスト先に残りますし、自分が望まないデータ（コンピュータウイルスなど）をダウンロードしてしまうこともあり得るのです。

HTTP では、ダウンロードだけでなく情報を送信することもできます。これによって、通信が双方向となり、より様々なサービスを受けることが可能になりますが、逆に言えばウェブを通じた自覚・無自覚の情報漏えいというものも起こりえますので注意しましょう。

4.2 コンピュータウイルスとワーム、Spyware（感染兆候と予防対策、事後対策）

ソフトウェアは人間に役立つように設計されているものですが、一般的に害を及ぼすことを目的に作成されたソフトウェアをマルウェア（malware）と呼びます。マルウェアにはコンピュータウイルス、ワーム、スパイウェア、アドウェアなど、広範な種類のソフトウェアが含まれます。

コンピュータウイルスは、自己伝染機能（自己を複製し他のコンピュータに感染を広げる機能）、潜伏機能（特定の条件がそろうまで活動を待機する機能）、発病機能（データの破壊・システムを不安定にする・バックドアを作成するなどの機能）を特徴としたプログラムです。コンピュータウイルスには、ウイルス、トロイの木馬、ボットなどがあります。

ウイルスは宿主となるプログラムに寄生するのが特徴で、様々な不利益（ハードディスクを消去するなど）をもたらします。トロイの木馬は一見有益ないし無害に見えるプログラムが、実は不正な動作をするというものです。スパイウェアは、トロイの木馬とほとんど同じですが、特にユーザに関する情報を収集するのに利用されるものをいいます。

ボットは、メールやネットワークを通じて感染範囲を広げ、感染したコンピュータにバックドア（正規の手続きを踏まずに内部に入る事が可能な侵入口）を仕掛けるというものです。このバ

ックドアにより感染したコンピュータは不正に操られ、著名なサイトなどを（数千、数万台の PC から）一斉攻撃するのに利用されます。

ワームは独立したプログラムであって宿主を必要としないところがウイルスとは異なるとされていますが、ネットワークを媒介として増殖し、コンピュータやネットワークに過大な負荷をかけます。

いずれにしても感染経路、ファイルの種類（アプリケーション、Microsoft Office のファイル、ウェブ Cookie など）、被害など、どのような側面で切ってもマルウェアには様々なものがあり、この対策だけ取っていればよいということはありません[17]。ここでは IPA（情報処理推進機構）による「パソコンユーザのためのウイルス対策 7 箇条[18]」を紹介しておきます。

最も重要なのは、アンチウイルスソフトウェアを導入しておくことです。本学ではアンチウイルスソフトウェアの全学ライセンスを取得していますので利用してください。

解説：アンチウイルスソフトウェアには、無償で利用することができるものもあります。次の 3 種類のソフトウェアを紹介しておきますので、検討して「自分の」パソコンに導入しておきましょう(無料で利用できる条件として、非営利の条件がついているものもありますので注意)。

- avast! [19]
- Avira[20]
- AVG® Anti-virus Free Edition[21]

アンチウイルスソフトウェアを導入しても、ウイルス検出のパターンファイルなどを定期的に更新しなければ意味がありません。これらのソフトウェアはいずれも自動でパターンファイルを更新するように設定することができますので、良く確認しておきましょう。

4.3 フィッシング、架空請求等

フィッシング（phishing）は「釣り」の fishing にかけた言葉ですが、ウェブや電子メールを利用した詐欺の一種です。典型的には、「ユーザアカウントの有効期限が近づいています」であるとか「登録情報の確認をしてください」などといった電子メールが届きます。電子メールにあるリンクをクリックすると本物そっくりのサイトが表示されるのですが、実際にはそれは犯罪者が仕立てたニセのサイトで、そこで銀行の口座番号や ID、パスワード、クレジットカードの番号等の情報を収集しているというものです。

ポータルサイトと呼ばれる統合的なサービスを提供しているサイトでは、オークションや小口決済機能を 1 つの ID で統合しているケースもあり、ID やパスワードを盗まれることで何重にも

---

[17] マルウェア(malware, malicious software）とは，悪意的なソフトウェアという意味の造語で、ネットワークやコンピュータに何らかの被害をもたらすように作られたソフトウェアの総称。
[18] http://www.ipa.go.jp/security/antivirus/7kajonew.html
[19] http://www.avast.com/jpn/download-avast-home.html
[20] http://www.avira.com/
[21] http://free.grisoft.com/

被害に遭い、また間接的に加害者になるケースもあるようです。

また、電子メールで利用してもいないサービスについて料金を請求されたり、またその請求が恐喝的な手口で行われることもあるようです。

このようなフィッシングや架空請求への対応は、次のようなものを挙げることができます。

1. ウェブブラウザやアンチウイルスソフトウェアのフィッシング詐欺対策機能を有効にすること
2. 正しい電子メールの知識を持ち、HTML メールを利用しない、リンクを安易にクリックしないこと
3. ウェブページの URL（特にオーソリティのドメイン名）を良く確認すること

フィッシング詐欺は様々な手口で行われていますが、最終的にはウェブを通じて情報収集が行われることが多いため、ウェブの安全な利用が鍵となります。ショッピングや銀行等だけでなく、ウェブを利用していて個人情報を入力しなければならないような場合は、とにかく慎重になる必要があります。

インターネットが普及するにつれ、インターネット上の経済活動も活発に行われるようになっており、それにともなって犯罪者もまたインターネットを活動の場にするようになっています。

4.4 ファイル交換（情報漏えい、著作権）

BitTorrent, Share などのファイル共有ソフトウェアの利用には常に著作権侵害とウイルス感染による情報漏えいがつきまといます。本学では、利用規程で BitTorrent, Share, Winny などの P2P ソフトウェアの利用を禁じていますので、それらのソフトウェアを利用してはなりません。

4.5 情報発信

インターネットは、だれもが気軽に情報発信ができるのがその特徴の 1 つです。以前から気軽に行うことのできた情報発信ですが、ブログや SNS、匿名掲示板などの普及によって、敷居の高さはより低くなっています。

インターネットへの情報発信として注意しなければならないのは、それが不特定多数への情報発信であることが多く、またコンピュータを利用しているため情報の再利用が簡単である、ということです。特定少数への発信であったとしても、一度自分の手を離れた情報がどのように再利用されるかコントロールするのは難しいですから、情報の発信にあたっては、特に慎重になってください。

特に慎重を期すべきなのは、個人情報です。自分の個人情報以上に、他者の個人情報の扱いについては、極めて慎重に行ってください。

また、文字のみのコミュニケーションでは真意が伝わらずに嫌な思いをすることもあるでしょう。基本的には情報の送り手としては真意が伝わるよう厳密に、誠意を持って対応し、情報の受け手としてはおおらかな気持ちで接するのが基本です。インターネット上のコミュニケーションで嫌な思いをしたら、相手が誰であれ、誹謗や中傷をやり返すのではなく、単にその場から離れ

るのが良いでしょう。

なお、インターネット上の情報発信について責任を問われるケースが増えています。最近の事例としては、SNS で、学生が遊園地のアトラクションで業務妨害を行ったこと、飲酒運転などの違法行為を告白し、社会的に非難を浴びたことなどがあります。真実かどうかは別として、無責任あるいは反社会的な言説については社会的な制裁が加えられる可能性が高くなっています。またそうなった場合に、インターネットでは発信者を特定するのがそれほど難しくないことから、民事や刑事上の責任すら負う可能性があることを自覚しておく必要があります。

4.6 関連情報

IPA、NISC、JPCERT/CC、@Police(警察庁) などが情報セキュリティに関する最新情報を発信しています。これらを日々チェックするようにしてください。

インターネットというすばらしい道具を得て、私たちの情報空間はこれまでとは桁違いに広いものとなりました。この広大な情報空間にどのように対応していくのかということを、技術的な面から、また社会的な面からも学ぶ必要があるのです。

C3302 教育テキスト作成ガイドライン（システム管理者向け）

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3302	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3302	高等教育機関の実態に合わせた内容の見直し	金谷吉成（東北大学） 中山雅哉（東京大学） 西村浩二（広島大学）

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

情報セキュリティ関連教育は、大学の特性を踏まえて行う必要があります。本文書では教育テキスト作成ガイドラインとして、システム管理者が踏まえるべき大学の特性と情報セキュリティ関連教育事項の関係を必要最小限の項目に絞って述べます。さらに、部局や情報センター所属のシステム管理者が情報サービスの維持・運用・管理も行う場合に必要な心構えや学習項目についても言及しています。なお部局での情報セキュリティ管理は、専門の担当部署や担当者が部局総括責任者や部局技術責任者として担当する場合と、システム管理者がこれらの役割を兼務する場合とがあります。このガイドラインの内容は部門技術責任者の役割を兼ねる可能性のあるシステム管理者を対象としたものですが、情報セキュリティ管理上の役割に応じて必要となる知識は変わってくることに留意してください。

解説：教育項目としての諸規程については、高等教育機関の情報セキュリティ対策のためのサンプル規程集（以下、本サンプル規程集：国立情報学研究所 学術情報ネットワーク運営・連携本部高等教育機関における情報セキュリティポリシー推進部会）そのものが最良のテキスト例である。必要に応じて参照願いたい。

第１章　概論

1.1 概要

大学の使命は、学生に質の高い教育を提供することと、学問における未知の問題の解決に取り組むことです。その目的を果たすために、大学には多くの資産があります。ここで資産というのは、建物や実験設備に代表される物理的なもの、教員や職員といった人材、そして、大学が所有するさまざまな情報のことを指します。ここでは、情報資産について考えてみたいと思います。大学が所有する情報資産には、例えば次のようなものがあります。

- 成り立ちが大学に属するもの
  - 教員、大学院学生の研究・教育内容
  - 学生、教員、職員の個人情報（氏名、住所、成績、履歴、業績など）
- 購入やライセンスの取得により使用できるもの
  - 情報システム（大学の情報ネットワークに接続する機器を含む）
  - コンピュータルームにある PC に内蔵されているソフトウェア
  - 図書館の電子ジャーナルやオンライン・データベース

現在、大学の情報資産の多くはコンピュータで取り扱うことができるようになっていて、その中のいくつかはインターネットを通じて外部に公開されています。しかし、公開に適さない情報資産は逆に、インターネットでは入手できないようになっています。もし、大学の情報資産を無断で消去してしまったり、外部に提供することが禁止されている情報資産を誰かが誤って提供してしまうと、大学の運営に支障を来すことがあります。このようなことは、情報資産以外の資産と同じように考えてください。大学の情報資産を不正に消したり書き換えたりすることは、大学に備え付けられている備品を破壊することと同じで、学則や就業規則に違反するときは懲戒の対象となり、法律に違反するときは犯罪になる可能性もあります。

本学の教員および職員は、大学の就業規則にしたがって大学の資産を管理する必要があります。そこでは、大学の資産が外部に流出したり、消失したりしないように、細心の注意を怠ってはいけないといえます。

法律や公序良俗に反する行為以外にも避けるべき行為があります。例えば、コンピュータやネットワークの正常な運用を阻害する行為を避けるべきです。ただし、個々の環境によって、避けるべき行為は様々です。

学内に設置してある各種の電子計算機、通信回線装置および通信回線は、大学という教育・研究機関に所属するものです。また、大学から利用資格として通知されたアカウントも、本学における教育・研究目的に必要不可欠であるからこそ全員に付与されています。したがって本学の教育・研究目的に著しく反するような形で、これらを利用すべきではありません。

近年、インターネットを始めとする情報通信技術の発達に伴い、大学が保有する情報資産の利用・流通にも変化が現われています。たとえば従来は、紙の学生証による本人確認によって交付されていたさまざまな証明書が、IC カードなどを利用した学生証によって本人宛に交付されるようになり、また、データベースの活用のおかげで、そのデータの正確性も確保されるようになりました。

電子情報の特徴の一つとして、「複製の容易さ」と「処理のし易さ」を挙げることができます。前者は、情報漏えいや著作物の不正複製の際は「悪い特徴」として捉えられます。一方、後者は暗号などの仕組みを利用した安全な通信を成立させる「よい特徴」として捉えることができます。

そして今後も、暗号技術、ネットワーク技術などさまざまな情報通信技術が高度に発展していくことが見込まれます。情報通信技術の発展は、システム管理者にとっては防御技術の進化に寄与しますが、一方でネットワーク犯罪者にとっては犯罪技術の進化に寄与しています。

情報に関する技術が、他の技術ともっとも異なる様相を見せるのは、変化の速さです。情報通信技術は他の技術の数倍の速さで変化するため、われわれのライフスタイルを変えてしまうような技術が突然現れたり、新しく開発された技術がわずか数か月で陳腐化し時代遅れのものとなってしまい、変化に対応できないと成長から取り残されてしまったりすることがあります。

システム管理者は、このように、犯罪防御も、犯罪行為も技術革新によって日々変化していて、そのなかで、安全な情報サービスの提供に努めるために何ができるかを考える必要がある、ということができます。

1.2 大学で守るべき情報

大学にある情報資産を、事務部門と教育研究部門の２つに分けて考えてみます。

事務部門には、教職員や学生の個人情報があります。個人情報には、氏名や住所などの基本的な個人情報の他に、研究活動・学習活動に伴う個人評価、健康状態、給与・学費の状況なども含まれます。また、大学として契約や調達に関わる情報を保有しています。

一方、教育研究部門としては、大学が持つ研究情報資産、具体的には未公開の特許情報や、大学として企画・制作した著作物などの知的財産があります。各部門の管理責任者は、自らの部門にどのような情報資産があるかを把握しておく必要があります。

1.3 大学において守るべき事項と特徴

研究のみを目的としている研究機関と異なり、大学の場合は、教育機関としての側面を同時に持ち合わせています。研究を行う教員と学生、教育を受ける学生、研究に参画する企業の研究者など、大学にはさまざまな立場の人間が出入りします。また、頻繁な人事異動、入学・卒業があります。そのため、大学にはさまざまな人が自由に出入りし、その状況調査も簡単ではありません。一方で、歴史的な経緯で、大学には学問の自由、自治権があり、また、大学の研究成果は広く公表されるべきだという考え方もあります。

このような状況を前提にして、情報資産を適切に運用するには、大学情報の機密性・完全性・可用性を十分に確保する必要があります。例えば、機密性については、すでに述べたように、最新の暗号技術を利用して、多彩な情報閲覧権限・編集権限を設定する必要があります。システム管理者は、自部局の情報閲覧権限や編集権限を十分調査し、適切に設定を行う必要があります。

なお、インターネットに接続をして、さまざまな情報を流通させる場合には、情報セキュリティについて注意する必要があります。大学だからといって、一般企業や行政機関と比べて情報セキュリティ対策が甘くてよいということはありません。サーバ攻撃（DoS、ポートスキャン、不正侵入、ウェブページ書き換え）、ウイルス・迷惑メール、P2P ファイル交換ソフトなどの不正アプリケーション使用による情報漏えい、踏み台、物理的脅威（盗聴、侵入、操作ミス、不正）などの対策が必要です。

1.4 大学の情報セキュリティ対策の特徴

情報セキュリティ維持の基本として大学全体の情報セキュリティポリシーが定められます。さらに大規模大学のように部局ごとに運用組織があるようなケースでは、各部局の事情に応じて部局毎に実施規程等として詳細化されることがあります。部局総括責任者にとって、情報セキュリティポリシーおよび実施規程間の矛盾に配慮することは重要です。全学のポリシーと、ある部局の実施規程等が矛盾することのないように、全学ポリシーの策定作業には全部局の部局総括責任者が参加すべきです。部局総括責任者は部局間の実施規程等の違いを部局の事情とともに理解し、それに起因する問題の解決に向けて努力すべきです。さらに、全学と各部局で実施規程等が異なる原因について検討する必要があります。多くの場合は、部局技術責任者の役割を担うシステム管理者のスキルに差が大きいため、スキルを身に付けた部局の提案が全学のポリシーに反映される傾向があります。また、附属機関として病院などがある部局と、そうでない部局では、利用者の個人情報の取扱が異なることがあります。このような情報セキュリティポリシーが適用される環境の差を認識し、全学の情報セキュリティポリシーに、部局毎の事情を矛盾なく追加できるようにしておく必要があります。

このような努力を有効なものとするため、インシデント（情報セキュリティに関して生じる事故や事件）に対応できる全学の組織をあらかじめ整えておくことが重要です。組織を整えておかない場合にはインシデントに対する迅速な対応が困難となることもあります。

また、大学のように、最先端の情報通信技術を利用しようという組織の場合、潜在的な脅威となる項目を発見することが困難であり、さらに、研究開発においては、リスクのように確定していない（未知の）脅威に対する対策費用を計上することも簡単ではありません。また、セキュリティ対策には終わりがなく、どんなに高価で高性能な機器を導入しても、どれだけコストをかけ

ても、完璧に対応できるものでもありません。システム管理者が技術者として求められるのは、情報通信技術に対する正しい理解と、技術が原因で発生した脅威には技術をもって対応するという姿勢です。

なお、大学には学問の自由があり、教員の研究は他者から干渉されるべきではなく、自由な立場で研究が行われなければならないという考え方があります。そのため、情報セキュリティ維持に欠かせないファイアウォールによる通信の制限やパケットフィルタリングを行うことを嫌うことがあり、その結果として、管理が行き届いていないパソコンがウイルス感染や情報漏えいなどの問題を引き起こすことがあります。したがって、システム管理者は、学問の自由等の憲法上の諸権利についても考慮しながらも、情報セキュリティを十分に確保する具体的な対策を検討していく必要があります。

ここで、情報セキュリティポリシーを作成する際に必要となる情報リスクマネジメントの注意事項を記します。

1. まず、情報セキュリティの確保を行う目的と場所を明らかにすることです。その際には、学内にある情報資産をすべて調べあげ、どのような脅威がどの程度の確率で発生するかを予想することが必要です。また、脅威に対する被害を予想することも必要です。これをアセスメントといいます。
2. 次に目的に応じた手法を計画（Plan）し、計画通りに実施（Do）し、そして実施がうまく出来ているかを監査（Check）し、改善（Act）する必要があります。この流れを PDCA と呼びます。
3. 一度 PDCA を実行したら、再び PDCA を行います。これを繰り返していくことで、日々の情報セキュリティの確保を行えるようになります。

各項目においては、制度・組織の見直し、技術的な解決、教育（研修）による対応などを同時に進める必要があります。また、予算確保や、規程・手順の作成も行う必要があります。

規程・手順の項目を作成する場合も、

a. インシデントを防ぐための項目
   例: 施錠、パスワード設定、フィルタリング
b. インシデントがあっても復旧可能にするための準備項目
   例: バックアップ、暗号化、予備電源
c. インシデント発生時の対応項目
   例: 緊急連絡網、バックアップからの復元、代替装置への切り替え
d. インシデント発生後の始末項目
   例: 報告（お詫び）、被害算出、保険の検討、規程の改定

のすべてを考える必要があります。

なお、近年、大学同士で図書館利用や単位互換、連合大学院、入試問題の共通利用なども行われています。また、大学においては企業との共同研究が活発化しています。そのため、情報セキュリティポリシーを作成した場合は、他機関や企業との矛盾点をうまく解決できるようにしておくべきであるといえます。

システム管理者が情報セキュリティポリシーについて学ばなければならない項目を、別の観点で整理してみます。個人の情報をデータとして取り扱うことができるようになった現在、私たちは簡単に他人を詐称したり、架空の個人を作り出すことができるようになり、その結果として、

さまざまな犯罪行為も行われるようになりました。

しかし、社会において人々が行為の自由を権利として行使できるのは、自由が、その行為に伴う責任と不可分であるからです。ところが、他人を詐称したり、架空の個人を作り出したり、インターネットの匿名性を悪用したりすることは、行為と責任を切り離します。しかし、サイバースペースは現実社会と同じなのであって、責任をはっきりと意識しなければ、本当の意味での自由な行動を保障することはできません。情報セキュリティポリシーは、このような観点からも検討していく必要があります。具体的には、情報資産利用の目的を明らかにし、個人用アカウントの貸し借りや共用、パスワードの盗用などを禁止するとともに、アカウントのトレーサビリティを確保する事項を情報セキュリティポリシーに盛り込むべきでしょう。大学は学術研究の場所です。商業的な利益に左右されることなく、真実・科学のために活動をすることが許されている場所であるともいえます。だからこそ、おかしな商業主義や、科学的な検証をうけていない態度に惑わされることなく、活動を行うことができます。情報セキュリティ教育についても同じです。情報セキュリティ教育が目指すべき学問的な健全さを追求し、他の組織の見本となる活動を行うべきであるといえます。

また、工学・経営学・教育学の研究者が関わることが可能ならば、その観点からも情報セキュリティ教育を評価し、改善するべきでしょう。システム管理者は、自身として教育者である場合と、自身は教育者でない場合があります。前者の場合は、自らが利用者（おもに学生）への教育に関わることになりますが、後者の場合は、自らが大学の教育課程の中で利用者教育を担当することはありません。しかし、後者の場合であっても、利用者とのやり取りの中で情報セキュリティ教育に相当する行為を行わざるを得ない場合があります。

そこで、利用者教育を担当する人（おもに情報リテラシー系の授業担当者）と連絡をとり、大学・各部局における情報セキュリティ教育の内容に、各部局固有の事情・内容・制限を反映させることが必要となります。

ある時にある仕組みや制度が成立しても、情報通信技術の変化は大変激しいので、その仕組み・制度が急速に陳腐化し利用されなくなる、ということがよく起こります。システム管理者は、情報通信技術に関する様々な内容を、

「技能」
　時間とともに変化する、商品知識的な内容。

「技術」
　時間とともに変化することは少ないが永遠の真実とはいえない内容。

「科学」
　時間とともに変化することがほとんどない内容。
　その知識が直接、情報セキュリティに役に立つことはないが、
　情報セキュリティの根幹をなす原理・原則である。

に分類しておき、それぞれを必要に応じて点検する計画を立てる必要があります。また、その中でも技能として分類される内容は時間とともに変化するため、その詳細を学ぶことが常に必要となります。ちょうど、携帯電話の新機種を購入すると、たいていの場合は使用方法が大きく変わっていて、そのため、取り扱い説明書をよく読まなければならなくなるのと同じです。

第１章では、情報セキュリティに関する概論を述べました。その内容は、上位（部局総括責任

者や部局技術責任者）の役割を兼ねる可能性のあるシステム管理者を想定し、情報セキュリティに関して知っておくべき知識と態度について、「科学の立場・教育学の立場」から述べたものです。ここでいう「科学の立場・教育学の立場」とは、情報科学のことではなく、「情報セキュリティの学習」という作業全体を科学的に分析した結果から得られた内容ということです。すなわち、「情報セキュリティを学ぶということはどのようなことか」「情報セキュリティを身に付けるとはどのようなことか」という内容を科学的に考察したものといえます。

個々の内容については、続く第２章以降で取り扱います。

第２章　ネットワークサービス・システム

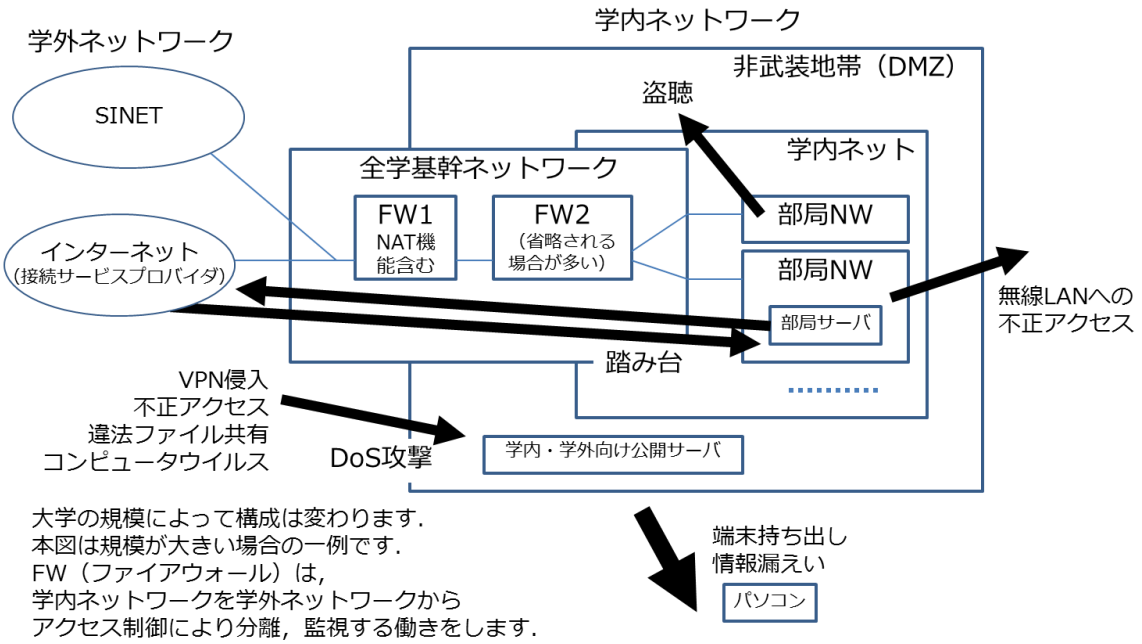


図１　大学ネットワークの構成例

図１に大学ネットワークの構成例を示します。図１は大規模な場合の例ですが、大学の規模によってネットワーク構成は変わってきます。小規模な場合には部局が直接インターネット（接続サービスプロバイダ）と接続する場合もあります。ある規模以上では多くの場合、部局ネットワークと全学基幹ネットワークの２階層構成になります。

基幹ネットワーク、部局ネットワークの入り口にはセキュリティを確保するためのファイアウォールが置かれます。大学から学外への接続は、インターネット（SINET への接続を含む）によってなされます。

高いセキュリティレベルを保つべき学内ネットワークと学外ネットワークの間に学内・学外向け公開サーバ等をおく中間的なセキュリティレベルを設ける場合があります（非武装地帯）。中小規模の大学では十分なグローバル IP アドレスを持たないため、アドレス変換（NAT）機能を持ったファイアウォールを用いることが一般的です。

大学ネットワークに対するセキュリティ攻撃は、例えば次のような多様な形で行われます。

- ネットワークの物理的盗聴
- 電磁的記録媒体、端末を経由した情報漏えい、ウイルス感染
- ガードの緩い無線 LAN への不正アクセス
- 学外向けサーバでは簡易なパスワードの走査（スキャン）による発見とその利用
- ファイル共有ソフトによる情報漏えい
- メールに添付されたウイルスを介した攻撃

2.1 コンピュータネットワークの構成

大学におけるコンピュータネットワークは、通常以下の要素によって構成されます。

1）LAN: 情報コンセント、無線 LAN アクセスポイントとそれに接続する電子計算機、周辺機器等から構成
2）部局ネットワーク: 1 つ以上の LAN をルータで接続したネットワーク
3）全学基幹ネットワーク: 学内の複数の部局ネットワークを接続し、さらに学外ネットワークにも接続するネットワーク

大学ネットワークの情報セキュリティを維持するためには、ネットワークに接続する各機器において情報セキュリティを確保すると共に、ネットワークを相互に接続するルータにおいてファイアウォールにより情報セキュリティポリシーに応じたアクセス制御が必要です。

地域交流センター、後援会、宿舎、インキュベーションセンターなどの学外の関連者がネットワークを利用する場合、学内ネットワークとの接続にファイアウォールを設置することにより、学内利用者と異なるアクセス制御が可能となります。

2.2 ファイアウォール

ファイアウォールはネットワークの情報セキュリティ維持に欠かせない要素です。システム管理者はファイアウォールの設置箇所、ファイアウォールのアクセス制御ルールを適切に設定しなければなりません。必要に応じて、ネットワーク間を接続するルータにファイアウォールを設定します。ファイアウォールでは、学内ネットワークへの攻撃を防ぐと共に、学外ネットワークへの意図しない通信（学外への攻撃、迷惑メールの発信、P2P ファイル共有ソフトによる通信等）を防ぐ必要があります。また、IP アドレス詐称による攻撃を防ぐために、Reverse Path Forwarding（RPF）を行うことも考慮すべきです。

解説：送信元を偽装した IP パケットの転送を防ぐ手法は、RFC2827（BCP38）では Ingress Filtering と呼ばれており、Multihomed Network 向けに改版された RFC3704（BCP84）では、Reverse Path Forwarding という用語が用いられるようになった。どちらの用語も広く使われているが、この文書では Reverse Path Forwarding を用いている。

Network Address Translation（NAT）は外部のグローバル IP アドレスネットワークから内部のプライベート IP アドレスネットワークへ直接通信できなくするために、簡易ファイアウォールとして機能しますが、NAT 越え技術、外部への意図しない通信には対応できないため、注意が必要です。

2.3 DMZ（Demilitarized Zone: 非武装地帯）

学内ネットワークと学外ネットワークの間に DMZ を設けて、そこに学外公開サーバを設置することがあります。DMZ から学内へのアクセス制御を適切に運用することで、例えば学外公開サーバが攻撃者に乗っ取られた場合においても学内ネットワークを守ることが可能となります。

2.4 VPN（Virtual Private Network）

大学が複数拠点にあり、拠点毎のネットワークがインターネット経由で接続されている場合があります。この場合、拠点間に VPN を設定することにより、拠点間通信を拠点内通信と同様のセキュリティレベルで提供できます。また、学外にいる組織構成員が VPN を使用することにより、安全に学内サービスを利用することができます。ただし、VPN の情報セキュリティを維持するために、システム管理者は VPN 接続鍵の有効期限設定、紛失時の無効化設定等を行う必要があります。

第３章 ネットワークサービス・システムを構成する要素技術

情報セキュリティを維持するためには、ネットワークサービス・システムを構成する技術要素を理解することが必要です。ここでは、基礎的なネットワーク技術要素の項目を列挙します。詳細な内容については、それぞれの技術要素の文献を参照してください。ネットワーク技術は進歩の激しい分野ですので、最新技術の動向を常に把握する必要があります。

なお、ここに示した要素技術についての教科書や文献は豊富に提供されていますので、詳細はそれぞれの教科書・参考書を参照してください。

3.1　IP アドレス体系

IP アドレス体系を構成するための技術要素の例を以下に示します。IP アドレスの確保や管理は大学内の情報資産管理の一環として重要です。IP アドレスにおけるクラスの概念などを熟知しておく必要があります。

- IPv4 / IPv6
- グローバル IP アドレス / プライベート IP アドレス / リンクローカルアドレス
- Classless Inter-Domain Routing（CIDR） / Variable Length Subnet Masks（VLSM）
- well known port

3.2 パケットフィルタリング

パケットフィルタリングを構成するための技術要素の例を以下に示します。パケットフィルタリングはアクセス制御に使われる重要な概念です。

- アクセスコントロールリスト（ACL）
- IP アドレスフィルタリング
- Reverse Path Forwarding（RPF）
- ICMP
- プロトコル・ポート番号フィルタリング
- IP フラグメント
- ステートレスフィルタリング / ステートフルフィルタリング
- 流量制限

3.3 NAT と NAT 越え（超え）

NAT を構成するための技術要素の例を以下に示します。NAT は学外向けの IP アドレスであるグローバル IP アドレスと、学内向けの IP アドレスであるプライベート IP アドレスを変換する機能です。グローバル IP アドレスを持たないものが、サーバ機能を外部に提供する場合や P2P 通信を行う場合などに「NAT 越え」が必要となります。NAT 越えは大変便利な機能ですが、情報セキュリティ上のリスクを招く恐れもあります。したがってネットワークの管理者・システム管理者は、利用実態、関連インシデントなどに気を配る必要があります。また、NAT を設置する場合には、インシデント対応を容易とするためセッションログをとるようにするのが好ましいと言えます。

- Network Address Translation（NAT）
- Network Address Port Translation（NAPT） / IP マスカレード
- NAT 越え
  - 静的マッピングテーブル
  - Universal Plug and Play（UPnP）
  - TCP connection reversal
  - UDP hole punching

3.4 MAC（Media Access Control）アドレス

MAC アドレスはイーサネットワークを構成する機器に付けられたユニークなアドレスであり、機器管理の基本情報の一つです。ネットワークの管理者・システム管理者は概念を熟知する必要があります。MAC セキュリティの例を以下に示します。

- MAC アドレス
- MAC アドレス認証

3.5 無線 LAN

無線 LAN を構成するための技術要素の例を以下に示します。安易に無線 LAN を設定することは、ネットワークにおける情報セキュリティ上のリスクを生じさせる原因となります。ネットワークの管理者・システム管理者は利用実態、関連インシデントなどに注意する必要があります。

- 無線 LAN の標準規格
- 認証・暗号化
- ESS-ID
- Wired Equivalent Privacy（WEP）/ Wi-Fi Protected Access（WPA2）
- IEEE802.1x / IEEE802.1i
- RADIUS 認証

解説：WEP はすでに数秒で解読される手法が発見されており、無線 LAN 機器を製造するベンダ間で作る Wi-Fi Alliance における Wi-Fi 認証を受けられない状況のため、速やかに WPA2-PSK 等のより安全な暗号化方式に移行することが求められている。WPA2 に対応していない無線 LAN アクセスポイントは更新が必要である。やむを得ず WEP にしか対応していないクライアント機器を接続する場合は、複数の暗号化方式を使い分けられる機能（マルチ SSID）を備えた無線 LAN アクセスポイントを使用し、MAC アドレス認証などによるアクセス制御を併用する。

第４章　セキュリティサービス・システム

大学においても情報セキュリティに対する脅威が拡大し、情報システムの情報セキュリティ強化が必須となっています。情報セキュリティを危うくする原因（以下「セキュリティホール」という。）はあらゆる所に存在するため、情報セキュリティの維持はあらゆる観点から行われる必要があります。情報システムを中心に考えると、利用者の意識の低さ、利用組織・体制の不備、物理媒体を含めた情報管理の不備、組織情報システムを囲う物理環境の脆弱性、情報システムとしての論理的な脆弱性などが全て関連します。どこかにセキュリティホールがあれば、一部だけ強固な情報セキュリティを維持しても意味がありません。このことを念頭に置きつつ、以下では情報システムとしての論理的な安全性を確保することについて述べます。

システムとしての論理的な安全性を確保するために必要な対策（及び関連技術）は以下の通りです。それぞれの対策はそれぞれに対応する最新の技術に立脚しなければなりません。

①自己を正しく識別し正しく情報を伝え、他者を正しく識別し正しい情報を受け取るための対策

（成りすまし防止、改ざん防止、事後否認防止、盗聴防止、電子証明書）

②迷惑を受けないための対策

（フィッシング防止、ウイルス防止、迷惑メール防止）

③他者に迷惑をかけないための対策

（踏み台防止、情報漏えい防止、ウイルス防止）

これらの中で基本となる対策は、大学構成員の正しい識別（識別コード（以下「ID」という。）の管理）です。大学構成員の多様化に伴い、ID の管理が分散化する場合が見受けられます。このような分散を避け、情報インフラとしての ID 管理と認証システムの確立が情報セキュリティ維持のための第一歩であるといえます。

インシデントの大規模化に伴い、予防措置の重要性が増しています。ここでは、様々な予防措置の中から、侵入検知、監査、アンチウイルス、アンチスパムについて述べます。

4.1 大学構成員の識別

大学構成員に付与する ID は情報システムの運用に欠かせない要素です。一般的に、学生は学籍番号、教職員は職員番号が付与されますが、これらの ID 体系は独立であることが多いようです。学籍番号は新学期に一括発行されます。情報システムログインのための ID は、これらの ID（またはそれから派生した ID）が流用されるか、新規に付けられることになります。情報システムログインのための ID には有効期限、再発行処理、パスワードの紛失対応などを行うシステム管理者が必要です。

解説：ID の種類ごとに管理元が分かれる場合がある。

［構成員例（管理元例）］

ａ）学生（学務部）

ｂ）常勤職員（人事部）

ｃ）非常勤職員（学科）

このため同一人物でも所属により ID が変わる場合がある。例えば、学部生から大学院生になる時、学籍番号が更新される。
以下に ID 種別例を示す。
a）管理元に対応した ID として、組織構成員に付与する ID
b）組織横断的に個人に付与する ID
c）臨時に付与する ID

4.2 ID 管理の統一と ID を用いたアクセス制御

付与した ID およびその ID に与えられた主体認証情報（以下「パスワード」という。）を用いて、学内サービスへのアクセス制御を行うことが広く行われています。パスワード設定ポリシーを定義しておくことにより、安易なパスワードの付与を避けることができます。

地域交流センター、後援会、宿舎、インキュベーションセンターなどの学外の関連者に ID を付与する場合はその属性を分け、完全なアクセス管理ができるようにしておく必要があります。

中小規模の大学では ID の管理元が一元化され、その結果 ID 付与体系の一元化に問題が起こらないのが一般的です。しかしながら大規模な大学になると、システム毎に ID が与えられることもあります。このような ID を効率的に管理するには、統一 ID を組織横断的に個人に付与し、個人の属性として所属部局、アクセス許可サービスなどを登録するようにします。ただし、情報システム毎の ID から統一 ID への移行には、情報システム毎の ID 付与ポリシーの統一に関する問題をクリアしなければなりません。さらに、パスワード付与ポリシーも統一する必要があります。

解説：認証を要求される通信（高信頼な情報交換）には 2 者間の認証を用いることもできるが、多くの利用者種別とサービスが存在する場合には、公開鍵基盤（PKI: Public Key Infrastructure）による電子証明書を使うことにより、認証コストを削減できる。電子証明書では信頼のおける機関（以下「信頼点」という。）を介して認証する。信頼点として、学外に開かれた公的なレベル（パブリック）と学内に閉じる私的なレベル（プライベート）がある。ブラウザには信頼できる認証局（パブリック）の電子証明書（ルート証明書）が組み込まれている。
大学におけるパブリックな証明書の利用シーンは、
①大学情報公開時のサーバ認証、
②電子商取引における個人認証、
③大学間で交換する情報の認証、
④物理トークンを用いた VPN へのアクセス制御
などである。
ID とパスワードの併用に比較した PKI の利点は、見破りやすいパスワード利用の害がない（セキュリティレベルが高い）、リアルシーンでの利用を含め多く応用シーンがある等であるが、サービス開始時のコストは高い。
大学間の PKI 利用を促進する動きとして、大学間連携のための全国共同認証基盤（UPKI）がある。UPKI イニシアティブが推進する。用途、目的、特徴は以下の通りである。

用途：大学間相互認証、ネットワークローミング、
　　グリッドコンピューティング
目的：学生・教員流動化への対応、導入・開発コストの削減、
　　国際連携への展開
特徴：パブリックとも連携

4.3 統一 ID とその応用（SSO アクセス制御管理）

ID を使ったアクセス制御方式には、情報システム毎に設計する個別アクセス制御方式と一回の認証で多くのサービスへのアクセスを可能とする SSO（シングルサインオン）アクセス制御方式とがあります。SSO アクセス制御方式は利用者にとっては便利ですが、高度な機能（SSO アプリケーション）が必要になります。SSO アプリケーションがサービス毎の ID とパスワードを記憶しておく方式もありますが、情報システム間で統一した ID を用いると、SSO アクセス制御を大幅に効率化できます。学内の情報サービスが多様化すると、統一 ID（ID 管理ポリシーの統一を含む。）を用いた SSO アクセス制御による管理コストの節約とサービス性の向上が有効になると考えられます。

解説：統一 ID を用いた情報システム構成例を図 2（シングルサインオンシステムの構成例）に示す。SSO サーバの機能は、①利用者のアクセス制御を個別サーバ（サービス）に代わって行い、②必要とする利用者属性を個別サーバに渡す。さらに、③オンラインによる SSO アクセス制御を行わないサーバ（サービス）のために、ID とその利用者属性を供給する役目も果たす、場合もある。
利用者属性を納めるデータベースをディレクトリデータベースと称す。ディレクトリデータベースにアクセスするプロトコルの一種に LDAP（Lightweight Directory Access Protocol）がある。
なお、学外のクラウドサービスと認証連携を行うことによって、学内サービスで利用している統一 ID をそのままクラウドサービスの認証に用いることが可能であるが、クラウド事業者に利用者属性を供給することにもなるため、特に注意が必要である。クラウドサービスのセキュリティについては、第 7 章で述べる。

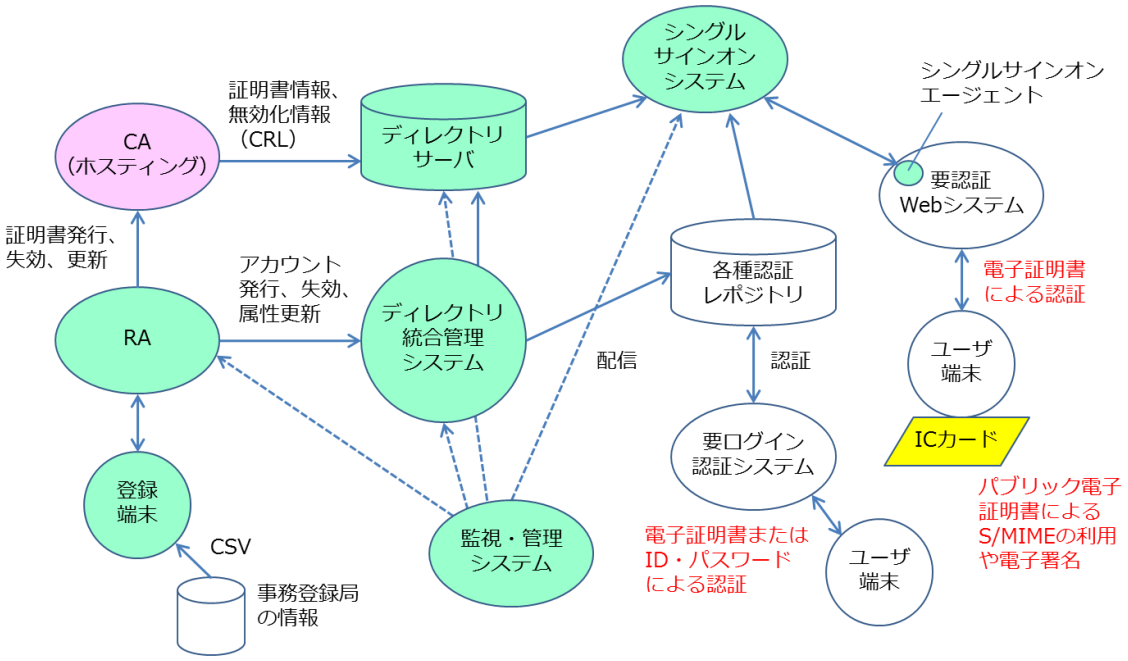


図２　シングルサインオンシステムの構成例

4.4 インシデントの予防措置

大規模化するインシデント、複雑化する情報セキュリティ攻撃に対して、予防措置の重要性が高まっています。予防は物理・論理的にインシデントを防ぐだけではなく、利用者の意識向上ももたらします。

１）トラヒックパターンによるネットワーク侵入検知

特定の IP アドレス・ポートに対する集中的なアクセスなどトラヒックパターンの観察によりネットワークに対する侵入を検知する情報セキュリティサービスです。特徴的なトラヒックパターンを伴う侵入の試みを検知することができます。攻撃を受ける場合にも、踏み台となって学外サーバを攻撃してしまう場合にも有効です。ただし、攻撃を受ける場合はファイアウォールで防御しておき、学外または学内への意図しない攻撃の検知に用いられる場合が一般的です。欠点は誤認識があることです。

大学では侵入検知後のアクションをあらかじめ確立しておくことが重要です。例えば、大学のサーバが踏み台となって学外サーバを攻撃してしまった場合、踏み台とされたサーバの管理者による迅速な分析・対応が不可欠です。アクションをあらかじめ確立しておかないと、迅速な対応ができません。

コストはかかりますが、大学の情報システム維持に有効なサービスといえるでしょう。

２）サーバ監査（脆弱性評価）

サーバの管理者の了解のもと、仮想的なアタックやサーバの分析（セキュリティホールの発見）を行います。評価コストを抑えるため、対象サーバが主要なサーバに限定されることもあります。セキュリティホールの種類としては、①OS、アプリケーションの既知の脆弱性、②見破られやす

いパスワードの存在、③通信回線、サーバ装置の物理的状態など多岐にわたります。実施頻度は実情に応じて設定されます。評価結果はリスクのランクとともにサーバの管理者に通知され、対処が求められます。運用なども含めた総合的評価を行うことが一般的です。

安易に設定されたパスワードによるインシデントが後を絶たないなかで、その抑止力ともなります。

３）ウイルスとアンチウイルス処理

他のソフトウェア（宿主）の一部として自己を複製し、拡散させていくソフトウェアのことをウイルスと呼びます。これに対して、独立したソフトウェアの形態をとるのがワームです。特定の条件が揃うまで活動を抑制する場合があり、被害を拡大する一因となります。情報システムに様々な悪影響を及ぼしますが、具体的には、システム不安定・停止、バックドア、踏み台などの原因になります。利用者が気づかないうちに感染が広がることがあるので、他者にも多大な迷惑（損害）をかけることになります。

こうしたウイルスやワームに対しては、しっかりした知識に基づき、感染予防、拡散予防に努めなければなりません。ウイルス発生に関する情報を常にチェックし、必要な対策をとることが重要です。不審なページへのアクセスや不審なソフトウェアをダウンロードしないなどの日常オペレーションにおける注意、ネットワークの入り口での対策、汚染された端末を持ち込まないなどの物理的対策が同時に必要となります。アンチウイルスソフトウェア（ウイルス対策ソフトウェア）を用いることも重要な対策であり、利用促進指導が必要です。また、キャンパス全体で対応しないと感染が収束しにくいものです。

解説：ウイルスの種類

ワーム型：単独で活動できるプログラムを指す。宿主のファイルが必要な場合のみをウイルスと定義する場合もある。

トロイの木馬型：見たくなるような画像やおもしろそうな文書になりすまし、電子メールに添付されたり悪意あるウェブサーバにアクセスすることで利用者に気づかれないように感染し、感染後に外部から遠隔操作できる機能を持っていたり、利用者情報の消去や不正持ち出し、システムを破壊するなどの動作を行うことがある。

ボット型：ロボットに因んだ命名。侵入後、端末が第三者の意思のままに動作するようになる。このようになると悪意の集団行動に知らぬうちに加担させられてしまう。

解説：感染経路と対策

ウイルスの特徴を表すデータ（パターンデータ）を用いて検出するのが一般的である。新しいウイルスの出現に対して、パターンデータをいち早く更新することが重要である。メールの添付ファイルなどネットワーク経由で侵入する場合が多い。このため、大学ネットワークの入り口でウイルス侵入を防ぐ必要があるが、媒体経由、持ち込み PC 経由などでも感染するため、端末毎の対策も不可欠である。ウェブ閲覧中にセキュリティホールを突かれて感染する場合もある。

解説：予防措置と対応組織の確立

予防措置の実施においては異常時に即応できるよう、対応する大学の組織を整えることが重要である。政府機関の情報セキュリティ対策のための統一基準（内閣官房情報セキュリティセンター）や本サンプル規程集に従うことで、しっかりした組織を整備することができる。

4.5 迷惑メールと対策

各大学とも迷惑メールが急激に増加しており、対応に苦慮しているのが現状です。完全な対応方法はありませんが、①メールアドレスの使い分け、②メールアドレスの公開を制限、③簡単に見破られないメールアドレスの利用などがあります。ネットワーク入り口での対処と、端末における対処を併用する場合もあります。

解説：迷惑メール対策には、ホワイトリスト方式、グレーリスト方式、ブラックリスト方式がある。図３（迷惑メール対策の例）に各方式の概要を示す。ホワイトリストは非迷惑メールのリスト、ブラックリストは迷惑メールのリストである。グレーリストは初めて受信するメールをリスト化したもので、このメールはいったん受信拒否される。ランダムに送りつけられる迷惑メールはほとんどの場合は再送されないが、非迷惑メールは再送される。再送されたメールは正常受信させホワイトリストに移行させる。メールの識別は送信元 IP アドレス、ヘッダ情報中の送受信者メールアドレスなどを使って行われる。

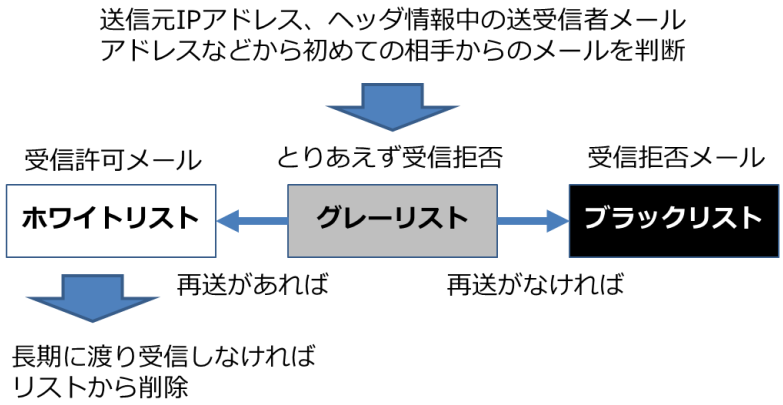


図３　迷惑メール対策の例

このほかの迷惑メールを受け取らなくするための対策としては、送信元 IP アドレスが正規なものであることを証明・確認する送信ドメイン認証、送信元 IP アドレスの危険度評価に基づいてフィルタリングを行う E-mail レピュテーションなどがある。ただしこれらは送信側、受信側双方で対応する必要がある、危険度評価データベースの精度により誤判定のリスクがあるなど、解決すべき課題も残されている。

一方迷惑メールを送信しないようにするための対策としては、あらかじめ許可されたメールサーバ以外からの送信をブロックする OP25B（Outbound Port 25 Blocking）などがある。
受信者が行う迷惑メール対策としては、ベイズフィルタを応用して本文中に存在する特定の単語群をもとに迷惑メールの確率を予想し、振り分けを行う方法がある。本文の内容に基づく判断が可能であり、学習により判断精度を向上させることができる。プロバイダの中には極めて優秀な迷惑メールフィルタ機能を提供しているものもあるため、受信したメールをプロバイダに転送して振り分けを行う方法も考えられる。しかし、所属組織の情報セキュリティポリシーによっては組織外へのメールの自動転送が禁止されている場合や、プロバイダによってはこのような方法は利用規約に反していたり、大量のメールが転送されることにより組織全体が迷惑サイト判定されて受信拒否されたりする場合があるため、利用に当たっては注意が必要である。

4.6 主体認証情報格納装置

実験室の入退出、図書館の入退館・貸出しなど、多くのカードがアプリケーション毎に使われていることがあります。アプリケーション毎に使われるカードは個別に管理されますが、主体認証情報格納装置（以下「IC カード」という。）を用いることにより、個別管理のコストを削減することができます。さらに、IC カードを応用した高度なサービスを提供できるようになります。即ち、IC カードは高度に情報化された大学の情報インフラとなることが期待されます。

解説： IC カードの用途を図４（IC カードの用途）に示す。その用途は、職員証、学生証、パブリック証明書（PKI）格納などが想定されている。

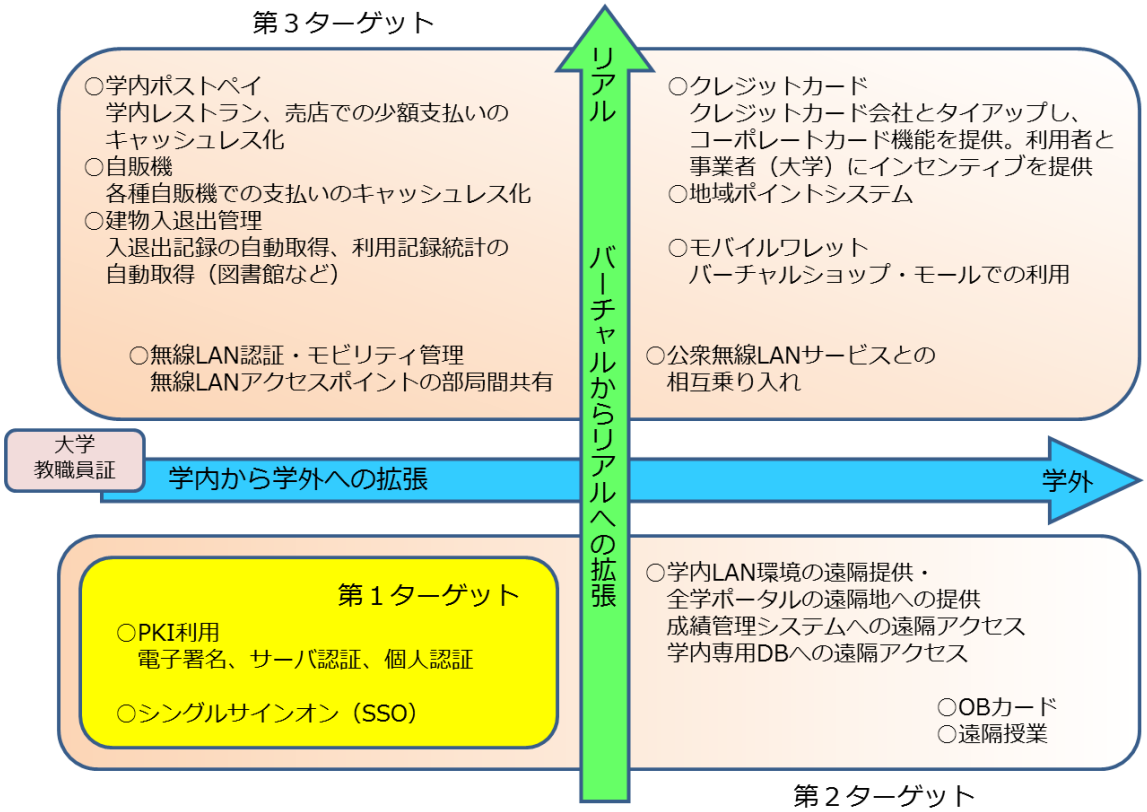


図４　ICカードの用途

第５章　セキュリティサービス・システムを構成する要素技術

セキュリティサービス・システムを構成するための要素技術の例を以下に示します。教科書や文献の豊富な分野です。詳細はそれぞれの教科書・参考書を参照してください。

１）公開鍵暗号による電子署名
２）認証・認可
３）暗号（秘匿）
４）改ざん検出
５）セキュリティプロトコル

第６章　サーバ（アプリケーション、OS）のセキュリティ

サーバ（アプリケーション、OS）のセキュリティの例を以下に示します。教科書や文献の豊富な分野です。詳細はそれぞれの教科書・参考書を参照してください。

１）電子メールサーバ
２）ウェブサーバ
３）DNS サーバ
４）OS のセキュリティ
　　UNIX®
　　Linux®
　　Windows®

第７章　クラウドサービスのセキュリティ

クラウドサービスはサーバ管理の煩雑さを軽減し、サービスの構築を迅速かつ低コストに行えることから注目を集めています。しかしその一方で、クラウドサービスはその運用の大部分がクラウド事業者の管理下で行われ、運用コスト最適化のため他の利用者とコンピュータ資源を共用する運用が行われるのが一般的です。そのため、データの保護・インシデントの管理など情報セキュリティに関する懸念が指摘されています。

大学等においても、管理運用業務の効率化の観点からクラウドサービスの積極的な活用が望まれますが、クラウドサービスの利用にあたっては、事業者の選定、サービス内容の確認、責任体制の構築等を慎重に行う必要があります。また大学が所有する情報資産については、情報格付け基準等によりそれぞれの区分に応じた取扱いを定めて、提供されるサービスとの整合性を確認する必要があります。

クラウドサービスのセキュリティを構成する要素の例を以下に示します。

１）情報の格付けとの整合性
　　取扱制限との整合性
　　利用組織の体制（責任者、担当者）

２）利用範囲の明確化
　　サービスの質（SLA）
　　機能とコスト
　　サポート体制
　　業務の継続性
３）事業者の選定
　　物理的セキュリティ
　　サービスの継続性
　　インシデントの管理
４）契約条件の確認
　　責任範囲の明確化
　　準拠法と管轄裁判所
　　データの所有権と返却・消去

解説：クラウドサービスのセキュリティを構成する要素は、一例に過ぎない。それぞれの大学およびクラウド事業者の実情に合わせて、詳細を検討していく必要がある。

例えば、クラウドサービスを利用するにあたっては、情報の格付けだけでなく取扱制限にも注意が必要である。クラウド事業者が海外の場合は、外国法が適用されたり、外国の裁判所で裁判が行われる可能性があり、契約時（約款による契約の場合を含む。）に注意を要する。

第８章　法令・基準

情報セキュリティに関連する法令として、内閣官房情報セキュリティセンター（http://www.nisc.go.jp/law/index.html）では、下記の概要と本文が紹介されています。

１）不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
２）電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）
３）高度情報通信ネットワーク社会形成基本法（IT 基本法）（平成 12 年法律第 144 号）

この他に、

４）特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）（平成 13 年法律第 137 号）
５）個人情報の保護に関する法律（平成 15 年法律第 57 号）、行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）、独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）
６）著作権法（昭和 45 年法律第 48 号）
７）特定電子メールの送信の適正化等に関する法律（平成 14 年法律第 26 号）

などが、情報セキュリティ周辺に関係する法令として重要です。

システム管理者は一通りの知識を持つことが望まれます。

解説：個人情報保護については、その法体系に注意する必要がある。すなわち、個人情報保護法の基本法的部分（第１章から第３章）は、私立大学・国立研究機関・

国立大学・公立大学等のすべての学校・機関に適用されるが、個人情報取扱事業者の義務に関しては、私立大学には個人情報保護法の第４章以下、国立研究機関には行政機関個人情報保護法、国立大学には独立行政法人個人情報保護法、公立大学には地方公共団体が制定する個人情報保護に関する条例が適用される。著作権については、ウェブによって情報を公開する際に利用者が注意すべき事項を示すものとして、サンプル規程集の中に「B3254 情報発信ガイドライン」があり、その中で著作権法との関係についても触れられている。

C3303 教育テキスト作成ガイドライン（CIO/役職者向け）

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3303	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3303	高等教育機関の実態に合わせた内容の見直し	曽根秀昭（東北大学） 高倉弘喜（国立情報学研究所）

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

本書は、役職者（学長、事務局長、全学総括責任者（CIO）、学部長（部局総括責任者））を対象とした大学運営における情報セキュリティ対策の基本的知識を説明するためのテキスト（資料）の必要項目を示すものである。

解説：対象は、ＣＩＯや大学執行部、経営陣。情報セキュリティの常識と事例を中心に、教育する。情報セキュリティのためのコスト（人、予算）を理解させる。情報セキュリティ対策はコストがかかるものであり効果が直ちに見えないこともあるので、予防的な対処は理解が得られにくいことがある。しかし、セキュリティ対策をあらかじめ施さないままにインシデント被害が発生すると、原因の特定や対処が困難になり、その困難な対応を直ちに短期間で実施することを迫られて、結果的に割高なコストがかかりがちで非効率的である。また、大学の評価が低下することに起因する副次的な被害につながることもあるので、「保険」のような必要コストであるという理解もありうる。

１．本学における情報セキュリティ状況

・本学の情報セキュリティ体制（ルール，チーム）
・インシデント発生状況の詳細情報（扱い件数の統計）＋対応状況（緊急措置，報道対応）
・重大インシデント（学外に対して重大な被害を与え、あるいは報道・苦情など問題化したもの）の詳細な分析

2. 情報セキュリティ対策に必要な措置

2.1　情報セキュリティ対策の必要性

・普段から情報セキュリティ対策を十分にしておかないと、インシデント発生時に業務遂行に支障が生じ、また対応にコストがかかって、労力と費用が失われる。情報セキュリティ対策にも労力と費用を要するので、合理的な労力および費用について考察して実施する。
・情報セキュリティは、大学の存亡にかかわりかねない重大な問題である。情報セキュリティ対策を怠ったがために、重大インシデントが起こった場合の影響を考えてみる。この場合、直接的に業務遂行に支障が生じるだけでなく、大学の評価が低下する。例えば、研究データの管理能力や研究成果の正当性が疑われるために、研究活動に困難が生じるとともに、共同研究が拒否される。さらに、社会的評価の低下は、受験生の減少にもつながる。共同研究先や受験生が減少する結果、大学経営が厳しくなって情報セキュリティ対策の実施が困難になり、さらに重大インシデントを呼び込むことになる。その結果、大学経営に非常に重大な影響を及ぼしかねない。
・情報ネットワークや情報システムあるいは情報の取り扱いについて，全学的な運営計画のなかでこれらの計画や運用に関わる責任をもつのが「CIO」の役割とされている。このサンプル規程集では，C1001 情報システム運用基本規程第四条で定める全学総括責任者が相当する。「CIO」に対して，情報セキュリティ対策の観点からチェックをして対策を実現するために「CISO」の役割がある。「CIO」が「CISO」を兼ねるケースも多いが，相互のチェック機能

を期待して異なる担当とする考えもあるので，全学的な計画を勘案し大学の方針によって判断すべきである。

・大学における情報セキュリティ対策の中でも、特に事務情報と医療情報については、特別な配慮を要する。事務情報には、学籍や職員に関する個人情報、財務情報、調達情報などがあり、適切な格付けに基づいた取り扱いを要する。また、医学部を有しない本学においても、学生の保健管理、あるいは人に係わる研究において医療情報をもつことがありうる。

・研究の成果は、やがて公表するものであっても、研究成果発表のプライオリティ維持のため、あるいは特許取得のため、情報管理が必要とされる。学生が実験で得た結果もその対象に含まれる。企業等との共同研究であれば、さらに厳密な管理が求められる。

・情報システムには，ハードウェアの耐用年数だけではなく，ソフトウェアにも機能とセキュリティレベル維持の耐用年数がある。このことを意識して，情報システムの構築と運用の計画には，運用期間中のセキュリティレベル維持と期間終了を見据えた次期更新計画も意識する必要がある。

・学内の情報サービス機能を，学外の商用サービス（クラウドサービス）を利用することで実現する方法があり，コスト削減や可用性向上のメリットも期待できる。これらを選定する際に，通常時の運用管理から運用事故発生時の対応までのセキュリティ対策も含めて検討すべきである。なお，外国のサービスについては，適用法を確認し，また，サービスの処理や保存の対象となる情報に機密情報や輸出管理技術などが含まれないかも確かめて判断する。

2.2 情報セキュリティの責任体制

・情報セキュリティ対策の有効化のために、情報システム運用管理体制を整備することが必要である。これには，人員と予算の確保及び規程類の制定が含まれる。

・「C2101 情報システム運用・管理規程」にもとづき、情報セキュリティ対策の最終責任は全学総括責任者にある。

・情報セキュリティ対策のために、通常業務として情報メディアセンター（管理運営部局）が整備、運用、監視を行う。

・現場である部局で対応に当たる部局統括責任者，部局実施責任者及び技術担当者から，情報メディアセンター及び全学総括責任者へ，及び逆方向の連絡体制の構築と役割分担をあらかじめ定めておく。担当者・連絡先の点検を兼ねて、定期的に情報を流すなどの活用を行なうことが望ましい。

・インシデント発生時の判断と対応は、「C3102 インシデント対応手順」に従い、法務と技術の両面から遺漏のなく行うことが必要である。広報も重要である。必要に応じて情報セキュリティ分野の法務について実務経験のある弁護士等の助言を得ることが望ましい。

・学外のクラウドサービスを利用する場合，あるいは運用やサービスを委託する場合には，情報セキュリティ体制の中でサービス提供業者などの責任範囲も明確にしておく。

・停電（計画と事故を含む）や大規模自然災害のときに情報システムが停止すると，大学の業務，とくに緊急業務の遂行に支障を及ぼすことが懸念される。情報システムの可用性を保障するために，非常時に情報システムを運用するための計画（情報システム BCP）をあらかじめ定めておくことが必要である。これには，非常時の業務継続に必要とされるシステムの選別や，運用に関係する職員の体制と連絡網の用意などが含まれる。

3. 情報システムの構築・運用・インシデント対応

3.1　体制の整備に関する課題

・情報セキュリティは情報システムの運用と利用のための安全保障である。
情報システムの構築時から、しっかり設備と体制をつくることが、情報セキュリティ対策上および TCO 削減のうえからも有効である。情報セキュリティ対策は、投資（労力と費用）効率を考慮すべきである。
情報セキュリティ規程を制定しても、実効的な設備および体制を構築しなければ、情報セキュリティ対策にならない。現実的な労力と費用において実施することができない情報セキュリティ規程を制定した場合、インシデントが発生すればその規程を制定した責任が問われる。

・情報セキュリティのため、通常運用の体制とインシデント対応のための体制の二つを整備することが必要である。
通常業務体制のために、情報メディアセンター（管理運営部局）の情報セキュリティ体制を整備する。すなわち、体制構築のための人員および必要な予算を確保する。
インシデント対応の体制のために、インシデント対応手順に合わせて、学内の法務と技術、広報等に関係する部署により体制を整備する。必要に応じて専門の弁護士等と契約する。
・通常業務の中で，インシデントの予防に有益な情報セキュリティ関連情報の収集と，学内への注意喚起にあたる業務も考慮すべきである。
・学外のクラウドサービスの利用や学外への運用委託をする際には，サービス提供業者との連絡体制について，故障など事故発生時の情報消失や運用中断に備えて，用意しておく。

3.2　体制の整備の方法

・情報セキュリティの体制を整える際に、要員は学外への業務委託や派遣などのアウトソーシングも選択肢になりうる。情報セキュリティ対策のための設備、あるいはその運用と監視もアウトソーシングの対象になる。インシデント対応のアウトソーシングについては、大学運営を勘案した判断を要する面に十分に考慮すべきである。アウトソーシングには、臨機応変に最適化できることや長期的人件費を削減できるメリットがあるが、継続的な取り組みも含めて、費用対効果を十分に検討して判断する。
・情報セキュリティの体制を全学的に整備していなくても、各部局ごと、あるいは PC 一台ごとに既に対策ソフトを導入したり監査を実施したりしているようなケースも考えられる。しかし、一般的に多数でまとめたほうが経費や手数が効率的になり、費用対効果が良くなると期待できるので、全学的な取り組みに改めることが望ましい。教育の効果や実施の徹底のためにも、全学レベルで取り組む姿勢を示すことは有意義である。
・情報セキュリティ対策に関連する情報を学内に周知する際に，注意喚起のための関係者への情報提供という直接的な効果のほかに，関係者を含めて情報セキュリティ体制と担当を再確認する効果も考慮して，周知を発することが望ましい。

4. ケーススタディ

解説：以下はあくまでも例なので、最新の事例を収集する。

4.1　不正侵入の事例

不正侵入の事件が発生した結果、外部から苦情が届き、不正侵入されたサーバの修復に加えて広報などの対応も必要になって、大きな労力を費やし、大学の社会的評判を落とすことになった例がある。被害者から損害賠償を請求された例もある。

・ウェブサーバが不正侵入されて、ウェブページを改ざんされた大学の例。

・不正侵入された結果、踏み台となって、スパムサーバや不正アクセスに利用された例。同様に、フィッシングサイトを置かれた例。インターネットの掲示板に不適切な発言を書き込むアクセスの踏み台として悪用された例。

4.2　情報漏えいの事例

大学がもつ情報が漏えいした場合、社会的信頼を損なうほか、個人情報である場合などに損害賠償責任が生じる例がある。

・学生の成績情報が漏えいした大学の例。

・職員が使用するパソコンがウイルス（暴露ウイルスと呼ばれる種類）に感染し、取扱注意の情報が漏えいした大学や官公庁の例。

4.3　ID・パスワードの漏えいの事例

・学内情報サービスを装った偽のウェブサイトに誘導する攻撃（フィッシング）にあって ID とパスワードを入力したために，その情報が流出した例。さらに，その ID とパスワードを用いてメールサーバを悪用されて大量の迷惑メールを発信された例。

・学外の情報サービスで、学内のメールアドレスを ID とし、これと同じパスワードを用いていたために、その情報が流出し、学内情報サービスの悪用を許してしまった例。

4.4　情報システム管理の体制ができてない事例

情報システムや情報セキュリティの体制が整備されていない場合に、業務に多大な支障が生じた例がある。

・大学院生が主体になって仕様書を作成し、システムを構築した。その後、リプレースのとき、その大学院生は卒業したため誰も仕様書を書けなかった大学の例。

・ネットワーク担当の教授が主体となってシステムを構築した後に定年退職となり、システムを理解する人が学内に皆無になったという大学の例。

・ネットワーク運用を学生（あるいは非常勤教員）に依存していたところ、その人が卒業（任期切れ）になった後、誰もネットワーク管理ができなくなり、安定運用ができず業務に支障をきたしたという大学の例。

・システムの導入の際に，設置業者の作業（ネットワーク接続，システム設定）を把握しなかったために不適切な設置・運用になって，インシデントが発生した例。

・コンピュータにインストールするソフトウェアの管理が不十分だったために，悪意のあるソフトウェアを意図に反してインストールしてしまい，情報流出インシデントが発生した事例。

・コンピュータにインストールするソフトウェアの管理が不十分だったために，許されるライセン

ス数を超えてインストールしてライセンス違反が生じた事例。
・実験装置の制御用に組み込まれたコンピュータやこれにインストールされたソフトウェアが耐用年数を過ぎても，専用システムの都合のために更新できない例。
・電気製品がインターネット接続機能をもっているにも関わらず，表面上は情報システムであると意識しにくいため，その機能の情報セキュリティ対策が不十分であることを把握できないまま接続して使用していたためにインシデントが発生した例。
・時限プロジェクトで使用していた専用のドメイン名（www.example.jp のような形式）が，プロジェクトが終了してドメイン名の有効期間が過ぎた後に他者に取得されて悪用されていた事例。

4.5　インシデント対応の体制ができてない事例

・インシデントが発生した部局の担当者が取材に対して，全学の体制と協調することなく応じて，不用意な発言が報道されてしまった例。
・　インシデントに関する取材に対して，体制に従わず広報から部局に丸投げとなった結果、不適切な対応となってしまった例。
・　インシデント発生後の役割分担が機能せず、技術担当者など特定の者に所掌範囲外の作業までもが集中した結果、インシデント対応が後手に回り被害が拡大してしまった例。

4.6　ソフトウェアの耐用期限を意識していない事例

ソフトウェアの耐用期限が過ぎても、それを使い続けていて，次のシステムへの移行していないため、業務の継続に支障を生じる例がある。
・Windows XP は業務で大量に使用されており、そのサポートの年限は数回延長されたにも関わらず、リプレース計画を立案していなかったため、サポート終了を目前にして、ソフトウェアのセキュリティ維持ができなくなったという，2014 年の例。
・ソフトウェアのサポート期間は、OEM 版など種別により異なることを把握しておらず、サポート終了に気付かないまま使用し続けていた例。
・ソフトウェアはセキュリティ更新が提供されなくなった時点で耐用期間が過ぎたと考えるべきであるのに，更新されなくなったフリーソフトウェアの安全性確認を失念し、使用し続けていた例。
・ソフトウェアが最新のハードウェアに対応できず、システム全てのリプレースが必要となった例。

4.7　著作権侵害の事例

•学生がインターネットに公開されたファイル交換システム上で長期間にわたって商用ソフトウェア（あるいは、音楽や映画）を配布した結果、多額の損害賠償が問題になったという例。
•商用ソフトウェアについて、許諾されるライセンスを大幅に超えて利用し続けた結果、損害賠償を支払った大学の例。

4.8　その他の事例

•学生が学内からインターネットの掲示板に名誉毀損を疑われる発言を書き込んだ結果、訴えられた例。同様に、インターネットオークションに海賊版ソフトウェアを出品した例。

C3401 情報セキュリティ監査実施手順

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年2月15日 A3401	新規作成（監査手順）	国立大学法人等における情報セキュリティポリシー策定作業部会
2007年10月31日 A3401	「情報セキュリティ監査手順」に文書名変更	ー
2015年10月9日 C3254	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

1. 目的

情報セキュリティの確保のためには、本学ポリシー、実施規程、及びそれに基づく手順が適切に運用されることによりその実効性を確保することが重要であって、その実効性及び対策の妥当性の有無が確認されなければならない。そのためには、独立性を有する者による情報セキュリティ監査を実施する必要がある。

本書は、本学における監査の適切な実施のための手順を定めることによって、情報セキュリティ対策の実効性を確保することを目的とする。

2. 本書の対象者

本書は、情報セキュリティ監査責任者及び情報セキュリティ監査を実施する者（以下「監査実施者」という。）を含む本学内における監査に携わる者（以下「学内監査関係者」という。）を対象とする。

3. 監査の概要

3.1 監査とは

本学における監査とは、本学ポリシーに従い、被監査部門とは独立性を有した組織又は者が行う情報セキュリティに関する確認行為（独立的評価）をいい、本学における自己点検結果等をサンプリングし、その確認・評価を行い、確認・評価の結果を全学総括責任者に報告することにより学内のセキュリティレベルの向上に資するものである。

一般的に、監査には「保証型監査」と「助言型監査」があり、これらは監査対象により使い分けられることになる。本学における監査では、ポリシー、実施規程及びそれに基づく手順については準拠性に対する保証型監査を行い、情報セキュリティ対策の運用については準拠性及び妥当性に対する助言型監査を行う。

3.2 基本的考え方

(1) 監査の実施は、本学ポリシーに根拠を置く。

(2) 監査の実施に係る本学内規定等を作成し、監査業務及び手続に関する学内での位置付けを明確化する。

(3) 監査は、年度情報セキュリティ監査計画に基づき、全学総括責任者の指示により実施する。

(4) 監査の客観性、実効性を確保するために、監査責任者は以下のことに配慮する。

- 専任の監査実施者の確保が困難であることを考慮し、監査業務を通常業務とは独立した業務として行うよう、監査実施者に指示する。
- 監査実施者の任命に当たっては、所属する上司等と協議をした上で、学内から広く選定することとし、原則として任期は【2年】とする。
- 監査責任者及び監査実施者で、本学内における監査チーム等の組織を編成する

ことを検討する。

- 監査実施者には、自らが直接担当している業務やシステムの監査を実施させない。
- 監査実施者に対して、監査で知りえたことをその業務以外では利用しないよう、周知徹底する。
- 適宜必要性に応じて、外部監査の活用を合わせて検討する。

(5) 監査調書又は監査報告書を含む監査関連文書は、学内の文書規定及び監査の重要性等をかんがみて、情報の格付けの実施等適切な取扱いを行うとともに、決定した保管方法、保管者、保存期間等に従い適切に保管する。

3.3 監査の目的及び位置付け

3.3.1 準拠性監査（保証意見及び助言意見）

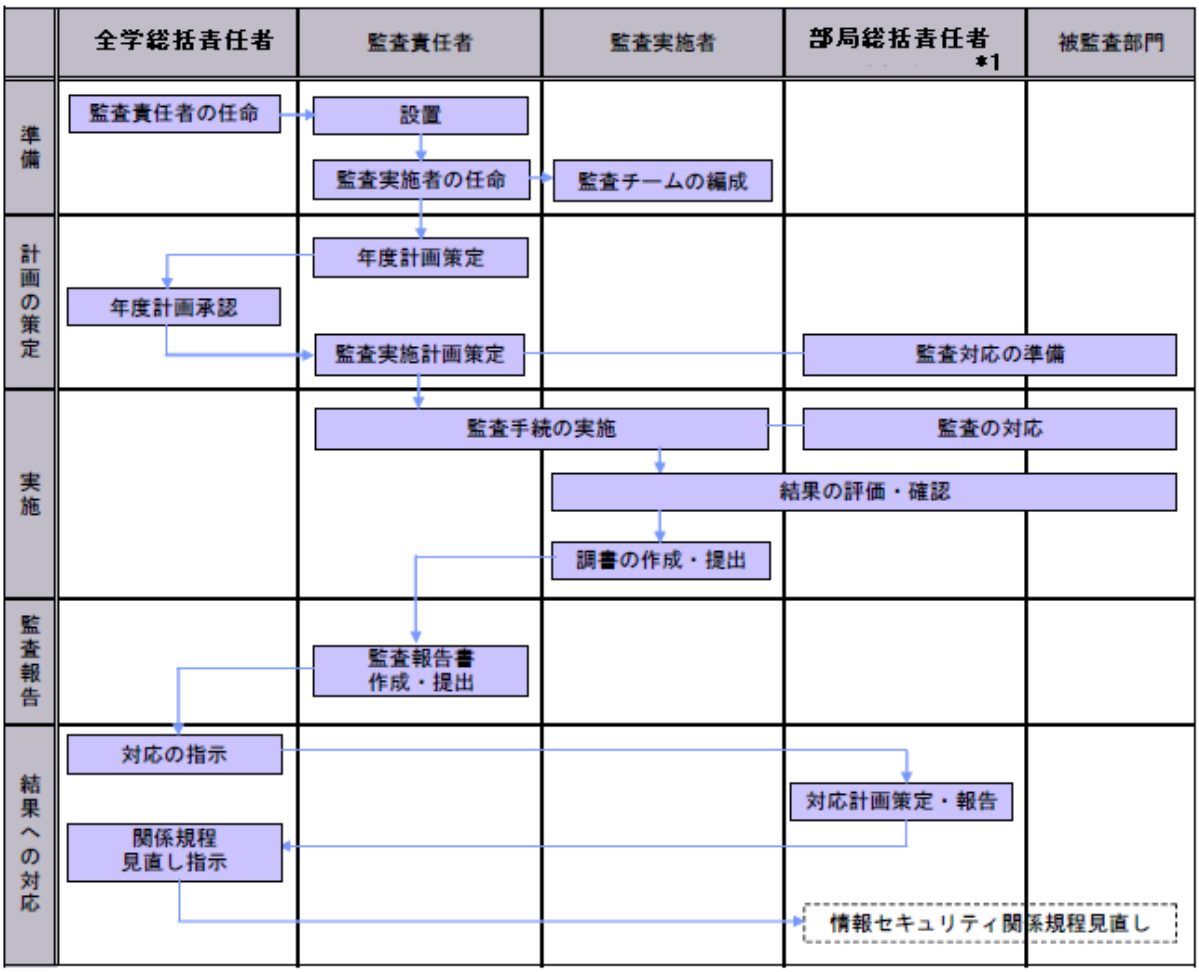
(1) 本学の実施手順が本学ポリシーに準拠しているかを確認・評価する。

(2) 本学における情報セキュリティ対策の運用がポリシー、実施規程及びそれに基づく手順に準拠しているかについて、自己点検結果等をもとに確認・評価する。

3.3.2 妥当性監査（助言意見）

本学のポリシー、実施規程及びそれに基づく手順が実効性のあるものになっているか、情報セキュリティ対策が妥当であるか又は有効に機能しているかについて、自己点検結果等をもとに確認し、改善提案等の助言を行う。

3.4 監査業務の全体像



＊1：被監査部門以外の部局総括責任者を含む場合がある。

4. 監査実施に当たっての前提及び準備

4.1 監査責任者の役割及び権限

(1) 監査責任者は、全学総括責任者の指示に基づき、監査に関する事務を統括する。

(2) 監査責任者は、年度情報セキュリティ監査計画及び監査実施計画（以下「監査計画」という。）を策定し、監査を実施する。

(3) 監査責任者は、監査実施者を任命【し、監査チームを編成】する。

(4) 監査責任者は、監査調書に基づき、監査の結果を監査報告書として作成し、全学総括責任者に報告する。

・ 監査責任者は、準拠性監査の結果を保証する。

・ 監査責任者は、妥当性監査の結果に基づき、改善提案等の助言を行う。

(5) 監査責任者は、監査計画の立案、監査マニュアルの整備及び監査調書のレビュー等

のプロセスを通じて、監査業務の品質を管理する。

(6) 監査責任者は、情報システム運用委員会への出席や各部局総括責任者へのヒヤリング等により、継続的に情報セキュリティ関係規程の整備状況や対策の実施状況、情報セキュリティ事案や違反の発生状況等の情報収集に努める。

4.2 監査実施体制の確立及び監査実施者の任命

(1) 監査責任者は、監査の客観性を確保することを考慮し、監査実施者を学内から広く選定し、監査実施体制を確立する。

(2) 監査責任者は監査実施者を任命する際に、監査責任者自らの所管する部局又は学内の各部局からメンバーを選定する。監査責任者は、必要に応じ監査実施者に対する兼務発令や業務指示を発効する。

(3) 監査責任者は、必要に応じ、監査責任者と監査実施者等で構成する監査チームを編成する。

(4) 監査責任者は、監査対象となる情報システムや業務、情報資産の運用に直接携わる者に、当該情報システム等の監査を実施させないものとする。

(5) 監査責任者又は監査実施者は、必要に応じて、監査対象システムの詳細情報を有する組織、学内の情報システム部門等の専門家の支援を受ける。

(6) 監査責任者は、監査の一部業務を外部に委託した場合でも、学内に相当程度の監査実施者を確保する必要があることに留意の上、監査実施体制を検討する。

(7) 監査責任者は、組織内に監査を実施する者又は監査遂行能力が不足していると判断した場合、必要に応じて監査の一部業務の外部委託を検討する。

(8) 監査責任者は、外部委託をする場合、委託先の選定に当り、被監査部門との独立性及び監査遂行能力を有している者を選択する。

4.3 情報収集及び状況の理解

監査責任者は、監査計画の策定及び監査の実施に当たり、事前に部局総括責任者等へのヒヤリングや学内の組織及び所管業務に関する情報収集を行い、学内のセキュリティ関連状況に関する理解に努める。

5. 年度情報セキュリティ監査計画の策定

5.1 目的及び位置付け

(1) 監査責任者は、学内監査関係者と情報を共有することにより、学内における監査業務を円滑に実施することを目的とし、継続的かつ定期的に行うべく当該年度における監査の年度計画を策定する。

(2) 監査責任者は、当該年度の監査計画の策定に当り、必要に応じて、3ヵ年程度以上の

中・長期計画を策定し、重点監査対象の年度展開及び当該年度に　実施すべき監査の水準・詳細度等を設定する。

5.2 概要

(1) 監査責任者は、【毎年2月末日】までに翌年度の「年度情報セキュリティ監査計画」を策定する。

(2) 策定した「年度情報セキュリティ監査計画」は、全学総括責任者の承認をもって、【当該年度4月1日より】発効する。

(3) 監査責任者は、監査実施計画の修正で適応しきれないほどのリスクの変動があった場合には、適宜本計画を修正し、全学総括責任者の承認を得る。

(4) 監査責任者は、当該年度に実施する監査の位置付けや目的、目標を明確化する。

(5) 中・長期計画を策定している場合は、当該中・長期計画に沿って当該年度における監査計画を策定する。

(6) 監査責任者は、当該年度計画の監査対象を明確化し、学内監査関係者に周知する。

(7) 監査責任者は、実施時期の調整や内容の重複の回避などを配慮し、会計検査や特定業務の監査等、恒常的に行われている通常の監査業務との連携を視野に入れて年度計画を策定する。

(8) 監査責任者は、年度情報セキュリティ監査計画に次の事項を記載する。

- 監査方針
- 監査の目的
- 監査対象（業務、システム、段階等）及び監査対象に係る監査目標（例えば、機密性、情報漏えい防止、不正アクセス防止等）
- 監査の想定カバー率
- 監査スケジュール
- 監査業務の管理体制
- 外部委託による監査及び外部専門家の活用の必要性及び範囲
- リソース管理（監査予算、人材育成計画等）

6. 監査実施計画の策定

6.1 目的及び位置付け

(1) 監査責任者は、年度情報セキュリティ監査計画で対象とした個別業務、システム等に応じて、具体的な監査方法及び監査時期等を計画する。

(2) 監査責任者は、学内における監査を円滑に実施することを目的とし、監査実施計画の内容を被監査部門及び当該部門の所属職員に対し事前に通知する。

6.2 概要

(1) 監査責任者は、年度情報セキュリティ監査計画及び情報セキュリティの状況の変化に応じた全学総括責任者からの実施指示に基づき、個別の監査対象ごとの監査実施計画を策定する。

(2) 監査責任者は、過年度の監査の実施状況その他過去の経験、事前の質問、世の中の状況等を勘案し、監査対象ごとの監査実施計画を策定する。

(3) 監査責任者は、監査実施計画に次の事項を記載する。

- 監査目的
- 背景（直前の情報セキュリティの状況認識）
- 監査対象
- 被監査部門及びその責任者
- 監査実施責任者及び実施担当者
- 監査の実施時期
- 監査の実施場所
- 監査の想定カバー率
- 実施する監査手続の概要（監査要点、評価方法の種類等）
- 監査の進捗管理手段
- 外部委託先との役割分担（外部委託を行う場合）

7. 監査の実施

7.1 監査の実施の指示

(1) 全学総括責任者は、年度情報セキュリティ監査計画に従って、監査責任者に対して、監査の実施を指示する。

(2) 全学総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、監査責任者に対して、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示する。監査責任者は監査実施計画を修正し、実施する。

(3) 監査責任者は、被監査部門から独立した監査実施者に対して、監査の実施を指示する。

- 情報システムを監査する場合、当該情報システムを構築又は開発した者はその

監査を担当しない。

・ 情報資産の運用状況を監査する場合、当該情報資産を運用している者はその監査を担当しない。

7.2 監査の実施における留意事項

(1) 監査実施者は、監査計画に基づいて、十分かつ適切な監査証拠を入手し評価する。

(2) 監査実施者は、学内基準等の規定文書の内容確認を行った上で、被監査部門への質問を基本とする。さらに、別途文書による裏づけをとったり（査閲）、実際に行っている作業を観察したり（観察）、自らが実際に行って点検したり（点検）することにより、質問への回答を検証する。

(3) 監査実施者は、対策の実施状況を効率的に確認するために、自己点検票及び自己点検結果を活用する。

(4) 入手した資料は、その入手元及び入手時の状況等を勘案して、監査証拠として採用するかについて、それらが有する信用性及び証明力の程度を慎重に判断する。

(5) 被監査部門から提出された資料、監査実施者自らが入手した資料、自らが行ったテスト結果等を総合的に勘案して、相互に矛盾があるか、異常性を示す兆候があるかを評価する。

7.3 実施結果の評価

7.3.1 準拠性に関する保証意見

(1) 監査実施者は、ポリシー、実施規程及びそれに基づく手順の間に矛盾、相違点、不足がなければ、準拠しているものと判断する。

(2) 監査実施者は、遵守事項違反がなければ、準拠しているものと判断する。

7.3.2 妥当性に関する助言意見

(1) 助言意見は、想定するリスクと比較して、対策が妥当であるかについての意見とする。

(2) 監査実施者は、将来の遵守事項違反につながる可能性のある事象について助言を行う。

(3) 監査実施者は、助言意見を検討するに当たり、実施すべき対策の実現可能性についてまでは考慮せず、原則を指摘することを役割とし、実現可能性についての検討は被監査部門の部局総括責任者が行う。

(4) 被監査部門の部局総括責任者は、実施すべき対策の実現可能性について、監査報告書に基づく全学総括責任者からの指示により検討する。

7.3.3 監査業務において発見された問題点・違反等の取扱い

(1) 監査実施者及び被監査部門の部局総括責任者は、発見された問題点に関する事実関係について、事実誤認等がないかを含め合意をしておく。

(2) 監査実施者は、準拠性に関する違反について、重大な違反と軽微な違反に区分して報告する。

7.4 監査調書の作成

(1) 監査実施者は、実施した監査業務ごとに、監査実施の過程を監査報告書作成の基礎とするため記録した監査業務の実施記録であり、監査意見表明の根拠となる監査証拠集である監査調書を作成し、監査責任者に報告する。

(2) 監査実施者は、参照符号等を整備して、監査の結論に至った経過が秩序整然と分かるように作成する。

(3) 監査実施者は、被監査部門から提出された資料や組織の外部の第三者から入手した資料を監査調書に添付する。

(4) 監査責任者は、監査調書の保管場所や保管責任者を決定し、情報漏えいや紛失等を考慮した上で、あらかじめ定められた期間保存する。

(5) 監査実施者は、監査調書に次の事項を記載する。

- 表題（何を確認したか、何を証明したいか）
- 監査実施者氏名・署名
- 実施期間
- 被監査部門及び責任者
- 発見された問題点（重大な違反、軽微な違反）
- 意見（保証意見、助言意見）
- 確認した遵守項目
- 確認した対策の内容
- サンプルの件数及び抽出方法
- 評価方法及び結果
- 監査証拠としての形態（文書か口頭か）
- 監査証拠の入手元（被監査部門から提出された資料か、監査実施者が直接入手した資料か、第三者から入手した資料か）
- 関連資料番号（チェックした項目をマーキングし、資料として添付する。）

8. 監査報告

8.1 監査報告書の作成と提出

(1) 監査責任者は、監査調書に基づき、監査報告書を作成し、全学総括責任者に報告する。

(2) 監査責任者は、監査報告書において、準拠性監査については、当該監査対象の準拠性に関する保証を行うとともに、違反を改善するための助言を行う。また、妥当性監査については、助言を行い、学内PDCAサイクルの実施により改善につなげる。

(3) 監査責任者は、監査報告書の読み手が全学総括責任者であることを意識し、全学総括責任者が報告内容の重要性や指摘事項の緊急性等を理解し、部局総括責任者等への指示すべき内容が明瞭になるように記述する。

(4) 監査責任者は、助言意見を述べるに際して、監査人の自由裁量ではなく、ポリシーや当該契約書等の監査の基準に照らして検出された課題及び問題点の指摘と改善提言とするものとし、保証を付与するかのような誤解を与える表現を用いないようにする。

(5) 監査責任者は、監査報告書の正本を全学総括責任者に提出、写を自らが保管する。

(6) 監査責任者は、監査報告書に次の事項を記載する。

- 報告書の名称
- 報告書の日付
- 報告書の宛名
- 監査人の署名、又は記名押印
- 監査実施期間
- 監査対象範囲（組織、システム、業務機能等）
- 監査の基準（判断の尺度）とした管理基準等
- 総合的所見
- 監査意見（違反の有無、課題及び問題点等）
- 監査人の独立性に関する事項 【独立性の例】
  - ○ 過去一度も当該監査対象業務に従事していない
  - ○ 過去2年の間、当該監査対象業務に従事していない
  - ○ 過去1年の間、当該監査対象業務に従事していなく、それ以前に当該業務に係る規定の整備又はシステムの設定等現在に影響の及ぶ行為をしていない
- 運用状況の準拠性に関する監査を実施した旨及びその結果（準拠性監査の場合）
- 遵守事項の整備状況の妥当性及び運用状況の準拠性に関する監査を実施した旨

及びその結果（妥当性監査の場合）

- 監査報告書の取扱い（利用及び利用者の制限事項等）
- 添付資料（個別業務ごとの監査調書等）

9. 監査結果に対する対応

9.1 監査報告書の内容の分析及び評価

(1) 全学総括責任者は、報告内容を分析し、全体像の把握と課題及び問題点の整理を行う。

(2) 全学総括責任者は、監査報告書において、改善提案等の助言があった場合、その内容の妥当性及び実現可能性等を検討する。

(3) 全学総括責任者は、同種の課題及び問題点が他の部門にもあり得るかの検討及び対策の見直し等の緊急性の検討を行う。

9.2 部局総括責任者への改善指示

(1) 全学総括責任者は、監査報告書の内容を踏まえ、被監査部門の部局総括責任者に対して、指摘事案に対する対応を指示する。

(2) 全学総括責任者は、被監査部門における課題及び問題点が他の部門にも発生する可能性があると判断した場合、他の部局総括責任者に確認する。

(3) 全学総括責任者は、(1)(2)に掲げるもののほか必要な事項について、該当する部局総括責任者に対応を指示する。

9.3 対応計画の作成及び報告

(1) 部局総括責任者は、監査報告書に基づいて全学総括責任者から改善を指示された事案について、対応計画を作成し、報告する。

(2) 部局総括責任者は、指示された改善が困難であることについて正当な理由がある場合には、リスク軽減策を示した上で、達成可能な対応目標を提示する。

(3) 部局総括責任者は、指示された改善内容が教育・訓練により解決すべき課題であると判断した場合には、全学実施責任者と相談の上、教育計画及び資料に反映する。

9.4 情報セキュリティ関係規程の見直しの指示

(1) 全学総括責任者は、監査報告書において情報セキュリティ対策の妥当性に関した改善提案を受けた場合、ポリシー、実施規程及びそれに基づく手順の妥当性を評価し、当該規定を整備した者に対して必要に応じてその見直しを指示する。

(2) 全学総括責任者は、改善提案を受けた場合であって、ポリシー、実施規程及びそれに基づく手順の見直しの必要がないと判断したときは、その理由を明確にする。

Ａ大学情報セキュリティ監査手順解説

本解説は、「C3401 情報セキュリティ監査手順」の各項における用語や例を示すものであり、本書における項番号は「C3401 情報セキュリティ監査手順」の項番号に対応させている。

3. 監査の概要

【手順策定者への補足説明：保証型監査と助言型監査の比較】

特定非営利活動法人 日本セキュリティ監査協会「情報セキュリティ監査制度利用促進等事業 実施報告書」より抜粋

	保証型監査	助言型監査	コンサルティング（参考）
保証	与える	与えない	
意見	述べる		
提言	しない	する	
客観的基準	存在することが前提		ない
実施者の独立性	必須		必須ではない
提言のフォローアップ	なし	あり	なし

4. 監査実施に当たっての前提及び準備

【手順策定者への補足説明：監査業務の品質とは】

実施された監査が、本学ポリシーや外部委託に係る契約書等の監査の基準に準拠して適切に行われているかという監査業務の信頼性及び有効性のこと。

【手順策定者への補足説明：監査実施者に求められる一般的な要件】

- 高い倫理観
- 監査対象業務についての知識・理解
- 情報セキュリティについての知識・技術
- 情報システムについての知識・技術
- 監査についての知識・技術

【手順策定者への補足説明：監査チーム編成における配慮事項】

・ 各監査実施者の通常業務と監査業務の負荷バランス

・ 監査実施者間の相互チェック機能の確保

・ 適切な職務の分担による監査対象からの独立性の確保

【手順策定者への補足説明：監査に必要な人的リソースの目安】

監査対象とする項目やシステム、業務の数及び実施する監査の方法により、必要となる監査実施者の人数や能力は異なるが、10～20名程度／大学、人年換算をすると５～10名程度の体制が目安と考えられる。

この一部の人員を外部委託することにより確保した場合でも、学内にかなりの人的リソースを確保しなければならないことに留意の上、計画を立てることが重要である。

【手順策定者への補足説明：監査遂行能力とは】

監査遂行能力とは、監査に関する能力や経験と監査対象業務及び情報セキュリティに対する知識・技術等からなる。

【手順策定者への補足説明：監査業務の委託先の選定に関する配慮事項】

委託先の選定に当たっては、情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の参画を考慮することが望ましい。

【手順策定者への補足説明：収集する情報の例】

・ 学内の組織図及び情報セキュリティ関係の体制図

・ 学内の情報セキュリティ関係規程（ポリシー、実施規程、実施手順等）

・ 各組織及び各情報セキュリティ関係の責任者の一覧

・ 各組織の業務内容

・ 各業務で取り扱う情報の種別

・ 保有している情報システムの一覧

・ ネットワーク図等の情報システムに関する情報

・ 以前に実施した監査に関する計画及び報告書等の監査結果

5. 年度情報セキュリティ監査計画の策定

【中・長期計画を策定する場合の例】

- 初年度 ：学内情報セキュリティ対策の実施状況の把握及び評価
- 2年度目：情報セキュリティ対策実施に関する日常業務への浸透
- 3年度目：情報セキュリティ対策実施の定着化及び学内セキュリティレベルの底上げ

【手順策定者への補足説明：監査対象選定のための観点の例】

- 自己点検が適切に行われているかを確認するための観点
- 遵守できていない（と思われる）ところを重点的に監査する観点
- 毎年同様の監査を実施し、対策状況の進捗や成熟度を経年で確認・評価する観　点（定点観測的に経年で確認・評価する観点）
- 環境の変化や監査時点での情報セキュリティ事案の動向・トピックス、体制・規定の変更等をかんがみ、年度別の重点監査対象の項目や重点システムを評価する観点（当該年度重点監査対象の選定）
- 導入段階、定常的運用段階等業務のライフサイクルに応じて確認する観点
- 以前実施した監査結果で明らかになった課題及び問題点の改善状況を確認する観点

【年度情報セキュリティ監査計画の雛形】

作成日：〇〇年4月1日

（情報セキュリティ監査責任者）

氏 名

〇〇年度 ××××大学情報セキュリティ監査計画書

１．監査方針

本年度は、本学内における情報セキュリティ関係の体制構築及び対策の実施状況を網羅的に把握・評価する。来年度以降の対策レベル向上に向けた基盤整備を行う。

２．監査の目的

本学内における情報セキュリティ関係の状況を網羅的に把握することにより、現在の情報セキュリティ関係規程(ポリシー、実施規程、手順等)の妥当性を評価し、来年度以降の対策レベル向上に向けた情報収集・分析を行う。

３．監査対象及び監査対象に係る監査目標

⑴ 重点監査対象

① 実施規程及び手順の準拠性監査（監査目標：〇〇〇）
② 情報セキュリティ管理体制の構築の監査（監査目標：〇〇〇）
③ 情報の格付け業務の監査（監査目標：〇〇〇）
④ 学内LANの運用状況の監査（監査目標：〇〇〇）

⑵ その他の監査対象

① インターネット接続口に設置されているサーバ群のセキュリティ設定の監査

４．監査の想定カバー率

⑴ 対象となる責任者、管理者、利用者（対象となる者/全員）

⑵ 対象となるシステム（対象システム数/全システム数）

⑶ 対象となる端末（対象端末数/全端末数）

５．監査スケジュール：別紙のとおり

６．監査業務の管理体制：別紙のとおり

７．外部委託による監査の範囲及び必要性

⑴ 外部委託の範囲及び必要性

① 範囲 インターネット接続口に設置されているサーバ群のセキュリティ設定の監査
② 必要性 脆弱性スキャン、システム侵入テスト等専門的技術を要するため

⑵ 委託契約の必要性の要否：要

８．リソース管理

⑴ 監査予算：別紙のとおり

⑵ 人材育成計画：詳細別紙のとおり 目標：監査スキルの向上と要員の確保

① 監査業務基礎講座：4月１日～4月30日の2週間程度
② 情報セキュリティ基礎講座：5月1日～5月30日の2週間程度

別紙

●監査業務の管理体制

（体制図の挿入）

●監査スケジュール

監査対象	作業フェーズ	2月	3月	4月	5月	6月	7月	・・・	10月	11月	12月	1月	2月	3月
年度計画策定								・・・						
本学基準及び実施手順の準拠性監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
体制の構築の監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
情報の格付けの監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
学内ＬＡＮの運用の監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
・								・・・						
・								・・・						
・								・・・						

●監査予算

予算項目	項目概要	予算費目	金額	実施時期	実施担当者
出張費					
宿泊費					
外部委託費					
・・・					

●　人材育成計画

育成内容	実施時期	実施方法	対象者	実施担当者
監査業務基礎講座	4/1～4/30	座学	利用者	○○○
・・・				

6. 監査実施計画の策定

【手順策定者への補足説明：監査実施計画策定上の配慮事項】

- 本学のシステム、業務、組織等の特性を分析した上で、影響度や脆弱性から判別し、リスクが高いと思われる領域を抽出する。
  - ○ 事件の発生可能性が高いと思われる領域（対策を実施していなければ事故の発生可能性が高い領域、対策が不十分と思われる領域、対策が十分に行われているか不明な領域等）
  - ○ 事件が発生した場合の影響が大きいと思われる領域（機密性の高い情報を取り扱っている領域、完全性の確保が必要となる情報・システムを取り扱っている領域、可用性の確保が必要となる情報・システムを取り扱っている領域等）
- 自己点検が終了している等、監査の受入れが十分と考えられる領域を選定する。
- 監査が円滑に実施できるように考慮する。
  - ○ 人的リソースや予算の状況
  - ○ 監査対象部門の負荷状況
  - ○ システムの運用状況（負荷の多い日、時間帯を避ける等）
- システムをカテゴリー分けし、監査頻度を決定する。

  【例】

  カテゴリーＡ：2回／年で監査を実施

  カテゴリーＢ：1回／年で監査を実施

  カテゴリーＣ：1回／3年で監査を実施

【監査実施計画の雛形】

作成日：〇〇年〇〇月〇〇日

（情報セキュリティ監査実施者）

氏 名

〇〇年度 ××××大学情報セキュリティ管理体制の構築に関する監査実施計画書

１．監査目的

本学ポリシー、実施規程及びそれに基づく手順で定めた情報セキュリティ管理体制の構築状況に関し、体制図・設置規定等の文書及び当該責任者への質問により確認する。

２．背景

平成18年12月に国立大学法人等における情報システム運用ポリシーが策定され、本学でも従来のセキュリティポリシーを改訂し、新たに本学ポリシーを策定したところ、昨今、情報漏えい事案も頻発しており、本学における情報管理体制の再確認が必要である。

３．監査対象：本学情報セキュリティ管理体制の監査

４．被監査部門及び責任者：××××

５．監査実施責任者：△△△△

６．監査の実施時期：7月1日～9月30日の各月末の週（計15日間）

７．監査の実施場所：本学内執務室

８．監査の想定カバー率

対象となる責任者、管理者および利用者（対象となる者/全員）

対象となるシステム（対象システム数/全システム数）

対象となる端末（全端末数/全端末数）

９．実施する監査手続の概要：別紙のとおり

１０．監査の進捗管理手段：別紙のとおり

別紙

●監査手続の概要

遵守事項	対策内容	評価方法	実施時期	実施担当者
部局技術責任者の設置	設置	体制図の確認	・・・	・・・
		質問	・・・	・・・
	連絡網の整備	体制図の確認	・・・	・・・

●監査の進捗管理手段

１．定期報告の実施

２．・・・

7. 監査の実施

【手順策定者への補足説明：情報セキュリティ状況の変化の例】

・新しいシステムが開発又は導入されたとき

・新たに他のシステム又はネットワーク等と接続したとき

・学内における大きな人事異動や組織改編があったとき

・学内外を問わず重大なセキュリティ侵害があったとき

・本学ポリシー等が改訂又は追加されたとき

【手順利用者への補足説明：監査証拠の十分かつ適切な入手方法例】

・関連書類の査閲

・担当者への質問

・現場への視察

・システムテストへの立会い

・テストデータによる検証

・脆弱性スキャン、システム侵入テスト

【手順策定者への補足説明：評価方法の解説】

・質問：講じた対策、行為

・査閲：規程類、設定文書（設計書等の設定一覧等）、記録文書、文書証拠

・観察：日常の行為

・点検：物理的状態、システム上のセキュリティ設定

【手順利用者への補足説明：点検による評価における配慮事項】

点検という手法を採用する場合には、システム運用を停止させること等がないように配慮し、実際の操作は部局技術担当者等に行ってもらうことが望ましい。

【手順利用者への補足説明：自己点検票の利用等チェックリストによる監査実施における配慮事項】

事前に監査チェックリスト等を用意して監査を実施することは、監査業務の経験の浅い監査実施者が行う場合等に有効であるが、通常、監査の最終段階で監査手続が網羅的に行われたかをチェックするために使用することが効果的とされており、以下のことに留意して行うことが望ましい。

・効率性確保の観点 リスト上のチェック項目の意味や重要性をかんがみ、上から下に順

番に行ったり、同じような質問を繰り返したりしない。

・ 有効性検討の観点 チェック項目の内容が現実に合っているかを考慮しながら監査を実施する。

・ 網羅性確保の観点 チェックリストに記載されていない重要な項目がないか検討する。

【自己点検票の活用例】

	自己点検の対象となるセキュリティ対策項目の整理・分析					自己点検の実施										備考
			分類			点検方法			実施時期&頻度		適用範囲			回答項目		
	自己点検項目一覧の作成	本学基準との対応	連続・単発	定期・不定期	頻度	随時点検型	一括点検型	断面調査型	自己点検の実施時期	自己点検の実施頻度	実施主体	管理者	責任者	回答項目	備考	監査における評価方法
1	人事異動の際には、識別コードの管理を徹底すること。	4.1.3 (2) (g)	連続	定期	年4	○			実施時	実施時	権限管理を行う者	部局技術管理者	部局技術責任者	Yes 日時	—	点検
2	情報入手時には、格付け・取扱制限を明示す	3.2.1 (2) (b)	連続	不定期	毎日		○		月末	月1	部局技術責任者	上司	部局総括責任者	Yes No	アンケート併用	質問
3	ウイルスパターンを最新にするこ	4.2.2 (2) (c)	連続	不定期	週1			○	15日 30日	半月1	利用者	部局技術管理者	部局技術責任者	設定値	バージョン番号	点検
4	ソフト開発時にST確認すること	4.3.1 (1) (d)	単発	定期	年1	○			実施時	実施時	利用者	—	部局総括責任者	Yes 日時	—	査閲
5	離席時には画面ロックすること。	3.2.2 (3) (b)	単発	不定期	毎日		○		月末	月1	利用者	上司	部局総括責任者	Yes No	—	質問
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
	Step 1-1	Step1-2	Step 1-3			Step 1-4			Step 1-5		Step 1-6			Step 1-7		Step 1-8

【準拠性判断の基準例（最大逸脱率が9%であることを90%の信頼度で確認する場合）】

・ 25件のサンプルのうち、1件も遵守事項違反がなければ、準拠しているものとする。

・ 25件のサンプルのうち、1件の遵守事項違反があっても、追加で20件のサンプルを選び、1件も遵守事項違反がなければ準拠しているものとする。

・ それ以外は準拠していないものとする。

【手順策定者への補足説明：重大な違反と軽微な違反の定義例】

・ 重大な違反とは、その違反単独で、又は他の違反と複合することにより、重大なリスクの発生を引き起こす可能性のあるものをいう。

・ 軽微な違反とは、重大な違反以外のものをいう。

【監査調書の雛形】

〇〇年〇〇月〇〇日

情報セキュリティ監査責任者 殿

（監査実施者）

署名

情報セキュリティ管理体制構築に係る情報セキュリティ監査の報告

平成〇〇年度情報セキュリティ管理体制の構築に関する監査実施計画に基づき、情報セキュリティ管理体制の構築状況を対象として監査を実施したので、以下のとおり報告する。

１．実施期間：××年××月××日から〇〇年〇〇月〇〇日まで

２．被監査部門及び責任者：・・・・・・

３．発見された問題点

(1) 重大な違反 ・・・・・・

(2) 軽微な違反 ・・・・・・

(3) 課題及び問題点等 ・・・・・・

４．意見

(1) 準拠性に関する保証意見 ・・・・・・

(2) 妥当性に関する助言意見 ・・・・・・

５．実施内容：別紙のとおり

別紙

順守事項	対策内容	評価方法	評価結果	サンプル		監査証拠		関連資料番号
				件数	抽出方法	形態	入手元	
部局技術責任者の設置	・・・	・・・	・・・	50/200	無作為	文書	第三者	001
	・・・	・・・	・・・	・・・	・・・	口頭	直接入手	－

8. 監査報告

【手順利用者への補足説明：監査報告書記載上の配慮事項】

- 要約と詳細を分ける
- 指摘事項等の対象となる部門や責任者をわかりやすく記述
- 準拠性の違反等の事実と妥当性の助言意見については、分けて記述
- 違反の事実については、重要性により区分けをし、記述

【監査報告書の雛形】

・ 準拠性監査報告書の雛形

〇〇年〇〇月〇〇日

全学総括責任者 殿

（情報セキュリティ監査責任者）

署 名

〇〇年度 ××××大学情報セキュリティ監査報告書

（準拠性監査報告）

平成〇〇年度情報セキュリティ監査計画に基づき、情報セキュリティの状況について準拠性監査を実施したところ、以下のとおり報告する。

1. 監査実施期間：××年××月××日から〇〇年〇〇月〇〇日まで
2. 監査対象範囲
   ・・・・・・
   ・・・・・・
3. 監査の基準：本学ポリシー及び当該請負契約書
4. 総合的所見：・・・・・・・・
5. 監査意見
   ⑴ 違反の有無
      ① 重大な違反 ・・・・・・
      ② 軽微な違反 ・・・・・・
   ⑵ 課題及び問題点 ・・・・・・
   ⑶ 助言意見 ・・・・・・
6. 添付資料
   ⑴ 平成〇〇年度×××に係る情報セキュリティ監査の報告
   ⑵ ・・・

なお、本職は、今回の監査対象の業務の実施には直接携わっておらず、十分な独立性を有しており、監査手続を実施した結果に基づいて、以上のとおり意見を表明するものである。

また、本報告書の利用は、本学における全学総括責任者及び部局総括責任者に限る。

・ 妥当性監査報告書の雛形

〇〇年〇〇月〇〇日

全学総括責任者 殿

（情報セキュリティ監査責任者）

署 名

〇〇年度 ××××大学情報セキュリティ監査報告書

（妥当性監査報告）

平成〇〇年度情報セキュリティ監査計画に基づき、情報セキュリティの状況について妥当性監査を実施したところ、以下のとおり報告する。

1. 監査実施期間：××年××月××日から〇〇年〇〇月〇〇日まで
2. 監査対象範囲

・・・・・・

・・・・・・

3. 監査の基準：本学ポリシー及び当該請負契約書
4. 総合的所見：・・・・・・・・
5. 監査意見
   (1) 課題及び問題点 ・・・・・・
   (2) 助言意見 ・・・・・・
6. 添付資料
   (1) 平成〇〇年度×××に係る情報セキュリティ監査の報告
   (2) ・・・

なお、本職は、今回の監査対象の業務の実施には直接携わっておらず、十分な独立性を有しており、監査手続を実施した結果に基づいて、以上のとおり意見を表明するものである。

また、本報告書の利用は、本学における全学総括責任者及び部局総括責任者に限る。

C3500 各種マニュアル類の策定に関する解説書

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3500	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3500	他文書の改定に伴う参照内容の修正	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

1. 本書の目的

「高等教育機関の情報セキュリティ対策のためのサンプル規程集」（以下サンプル規程集）では、「C2501 事務情報セキュリティ対策基準」に基づいた情報セキュリティ対策実施手順書の雛形として「C3501 各種マニュアル類」を策定することとしている。「C2501 事務情報セキュリティ対策基準」は、「政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）」（以下政府機関統一基準）と「府省庁対策基準策定のためのガイドライン」（以下ガイドライン）における基本対策事項をもとにしており、その内容は用語の違いをのぞき、多くの部分で共通である。政府機関統一基準に準拠した実施手順書の雛形としては、「政府機関統一基準適用個別マニュアル群」（以下統一基準マニュアル群）と呼ばれる文書群が整備されている。よって事務情報セキュリティ対策基準に基づいた「C3501 各種マニュアル類」の作成に当たっては、統一基準マニュアル群を基とすることが適切である。

一方、政府機関統一基準の平成 24 年度版から平成 26 年度版への改定において、大幅な変更が行われた結果、統一基準マニュアル群については平成 24 年度版までを対象とした文書群は更新対象外となり、平成 26 年度版に対応した新たな文書が作成・公表されることとなった。そこで本文書は、今後平成 26 年度版の政府機関統一基準に準拠した統一基準マニュアル群が改訂・追加されるのに備え、統一基準マニュアル群中の文書を基に「C3501 各種マニュアル類」を作成する際の手順および注意事項について記したものである。

2. 「C3501 各種マニュアル類」作成にあたっての基本的な考え方

本文書で述べる「C3501 各種マニュアル類」とは、「C1001 情報システム運用基本規程」第三条四に定義された事務情報システムの運用にあたり、「C2501 事務情報セキュリティ対策基準」を満たした情報システムの操作もしくは電子化された情報資産の取り扱いを、各業務を担当する教職員等が容易に理解し実行できるようにまとめたものである。統一基準マニュアル群の構成は 2015 年 9 月現在、表 1 のようになっている。

表 1 政府機関統一基準適用個別マニュアル群の構成（2015 年 9 月時点）

外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書
スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書

3. 「C3501 各種マニュアル類」作成の基本的な手順

既に述べたように、政府機関統一基準及びガイドラインの基本対策事項と、「C2501 事務情報セキュリティ対策基準」は用語の違いをのぞいて多くの部分が共通であるため、統一基準マニュアル群の各文書に対し以下のような作業を行うことにより、効率的に「C3501 各種マニュアル類」等を作成することができる。

3.1. 用語の置換

政府機関統一基準及びガイドラインと「C2501 事務情報セキュリティ対策基準」の間にはエラー! 参照元が見つかりません。のような用語の差異があるため、統一基準マニュアル群の各文書内の対応する用語を置き換えることによってある程度機械的に各種マニュアル類の雛形を作成す

ることができる。ただし完全に機械的な置換を行うと表現が崩れる部分があるため、適宜修正する必要がある。また、エラー! 参照元が見つかりません。中にない政府機関特有の用語が今後統一基準マニュアル群に表れる可能性もある。

表 2　政府機関統一基準と C2501 の主な用語の対応

	政府機関統一基準 （府省庁等対象）	C2501 事務情報セキュリティ対策基準 （高等教育機関対象）
役職名等	最高情報セキュリティ責任者	全学総括責任者
	情報セキュリティ監査責任者	情報セキュリティ監査責任者
	最高情報セキュリティアドバイザー	情報セキュリティアドバイザー
	総括情報セキュリティ責任者	全学実施責任者
	情報セキュリティ責任者	部局総括責任者
	情報システムセキュリティ責任者	部局技術責任者
	情報システムセキュリティ管理者	部局技術担当者
	課室情報セキュリティ責任者	職場情報セキュリティ責任者
	区域情報セキュリティ責任者	区域情報セキュリティ責任者
	情報セキュリティ委員会	全学情報システム運用委員会　または 部局情報システム運用委員会
利用者・関係者	行政事務従事者	事務従事者
	国民	学生や学外利用者
	職員	本学構成員
組織・施設	政府機関	本学
	（各）府省庁	本学　または　（各）部局
	庁内または庁舎内	学内
業務	行政事務	事務
	行政職務	職務
その他	国民の権利が侵害され	大学の運営に支障を及ぼす

3.2.　情報セキュリティ対策基準の構成の違いに起因する修正

政府機関統一基準は府省庁においては最上位に位置する規程であるが、「C2501 事務情報セキュリティ対策基準」には上位規程として「C1001 情報システム運用基本規程」があり、事務情報以外を取り扱う情報システムに関する他の規程も並列に存在するため、それらとの整合性を取ることが必要である。特に事務情報以外を取り扱う情報システムに関するマニュアル等が作成された場合には、情報システム利用者が遵守するべきマニュアル等は事務情報システムにかかるものになるか否かで異なってくるため、利用者が混乱しないような工夫が求められる。例えば事務情報システムに関連するマニュアルを他の情報システムに関連するマニュアル内の対策基準全てを含むように記述し、事務情報システムを利用する可能性のある者には事務情報システム向けの各種マニュアル等で代替可能にするなどの措置が考えられる。

3.3.　その他各大学固有の事情に応じた修正

その他、各大学で「C2501 事務情報セキュリティ対策基準」を基に施した修正等に関しては各種マニュアル類にも反映させる必要がある。

C3600 認証手順の策定に関する解説書

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3600	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3600	文書番号の変更のみ	ー

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

この文書は、「C2201 情報システム利用規程」C2201-05（全学アカウントの申請）に定める全学アカウントの申請と交付の手順の雛形として使われることを想定している。A大学では、IDとパスワードによる全学統一認証方式を採用し、ネットワークを含めて、全学統一認証に対応した情報システムの利用にあたって全学アカウントを用いている。これに基づき以下の４文書を雛形として示す。

(1) A 大学情報システムアカウント取得手順（「C3601 情報システムアカウント取得手順」に相当）
アカウントの申請・交付の手順として、学生、教職員それぞれに対して公開する文書。
(2) A 大学情報メディアセンターにおける全学アカウントに係る個人情報の保護
（「C3601 情報システムアカウント取得手順」別紙１に相当）
利用者からの全学アカウントの交付申請・登録などに際して収集した個人情報の取扱について、利用者に対して示す文書。
(3) A 大学情報システム利用申請書（「C3601 情報システムアカウント取得手順」別紙２に相当）
全学アカウントの申請書様式（複写式）。「A 大学情報システム利用心得」を示し、それを遵守することについての誓約書に署名させるようになっている。
(4) A 大学情報システム全学アカウント交付申請区分（「C3601 情報システムアカウント取得手順」別紙３に相当）
申請者の身分ごとに本人確認手順、更新手続きなどの認証手続きを定めた内部文書。原則非公開。年度ごとの手順の見直しが必要。

全学アカウントは、全学実施責任者（管理運営部局である情報メディアセンター長）から交付を受けなければならない。A大学では、利用の申請と承認は全学情報システム運用委員会が処理をするが、利用承認とアカウント指定を行うのは全学実施責任者なので、申請宛先も全学実施責任者としている。アカウントの発行に際しては原則として写真付身分証による対面での本人確認を義務付けている。また学生については全学アカウントの発行に際して講習会の受講を義務付けている。学生・教職員以外の者の申請に当たっては、関係部局長（来学中に利用する訪問者などの臨時利用者を受け入れた部局の長など）名での受入証明書の提出を要件とする。

なお、A 大学では身分証は IC カード化されていないが、身分証が IC カード化され PKI による利用者認証が可能になっている場合には、アカウントは電子申請によりオンラインで発行を受けることが可能である。ただしその場合には身分証の交付手順が CP（証明書ポリシー）／CPS（認証局実施規程）に基づくものでなければならない。

実際の運用にあたっては以下のような点についても検討が必要である。

- 医学部、歯学部、獣医学部、薬学部のような 6 年制の学部の学生に対して、卒業まで 6 年間有効のアカウントを発行してよいか、他の学部と合わせて 4 年＋2 年の更新とするか。博士課程 5 年一貫教育の場合も同様。
- 名誉教授に対するアカウントを発行するか、年度ごとの更新処理は必要か。
- 卒業生に対するアカウントを発行するか、有効期限の設定、利用者との契約をどうするか
- 産学連携施設など大学内に制度的に整備された施設で研究を行う、大学外の身分の研究者等にアカウントを発行するか。その場合の契約をどうするか。

- 本人死亡に伴うアカウント失効処理手順をどうするか。知財の継承のほか労災の認定などにおいてもデータの保全が求められることがある。

C3601 情報システムアカウント取得手順

国立情報学研究所 学術情報ネットワーク運営・連携本部
高等教育機関における情報セキュリティポリシー推進部会

改定履歴

日付・文書番号	改定内容	担当
2007年10月31日 A3601	新規作成	国立大学法人等における情報セキュリティポリシー策定作業部会
2015年10月9日 C3601	文書番号の変更のみ	ー
2016年2月5日 C3601	C2201の修正に伴う参照項番の変更	高等教育機関における情報セキュリティポリシー推進部会事務局

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

【全学アカウントの取得手順（学生等用）】

全学アカウント交付のための利用者講習会（情報セキュリティ基礎講習を含む）を受講してください。その際、学生証と筆記用具を持参してください。全学アカウント交付のための利用者講習会は、年度初めを中心に開催しています。都合の良い機会に、早めに受講してください。

講習会の実施日については、 情報メディアセンターのトップページにある 「イベント等のお知らせ」あるいは情報メディアセンター事務室前の掲示等を参照してください。

既に全学アカウントを取得している方で、転学部、進学等に伴い身分変更が生じた際には、手続きが必要となる場合があります。手続きが必要となる方には、例年メールでお知らせしています。詳しくは、情報メディアセンター事務室までお問い合わせください。

【全学アカウントの取得手順（教職員等用）】

1. 手続き

登録に必要な仮パスワードを発行しますので、職員証または大学が発行する身分証を持って、申請受付場所までお越しください。

- 情報メディアセンター事務室
- 図書館事務室

新規利用登録以外の申請は、情報メディアセンター以外では受付していない場合があります。

2. 申請用紙

所定の利用登録申請書（新規登録用）をご利用ください。

なお､情報メディアセンター､図書館については窓口に複写式の申請用紙を用意してあります。

3. 注意

情報メディアセンター窓口以外での申請分については、当日中の仮パスワード発行ができませんので、当日中の発行をご希望の方はセンター事務室での申請をお願い致します。

また、常勤教職員以外の方は、年度が変わった時点で利用延長の手続きが必要です。新年度になりましたら情報メディアセンター電子メールシステムのメールアドレス宛に、利用延長の手続きの案内を送ります。手続きの案内を受け取った後、継続して利用を希望される場合には、新年度継続して勤務していることを証明する書類を持って、手続きにお越しください。

4. その他

全学アカウント取得後速やかに、年度講習計画に定める情報セキュリティ基礎講習を受講してください｡また毎年度１回は年度講習計画に従い情報セキュリティ定期講習を受講してください。

別紙１　情報メディアセンターにおける全学アカウントに係る個人情報の保護

1. 個人情報について

利用者からの本学情報システムの全学アカウントの交付申請・登録などに際して収集した特定の個人を識別しうる情報を対象とします。情報メディアセンターは個人情報の保護に関して「独立行政法人等の保有する個人情報の保護に関する法律」及び関係法令ならびに「A 大学個人情報保護規程」等の A 大学の定める個人情報保護の方針に則って業務を行います。

2. 全学アカウントの交付等申請時に取得する個人情報の利用目的

本学情報システムの全学アカウントの交付、継続、停止、再開などの申請時に取得する個人情報の利用目的は以下のとおりです。

- A 大学ネットワークや情報処理演習システムなど情報メディアセンターで提供しているサービスのご利用に関しての利用者ご本人への連絡（学部、研究科等 A 大学各部局の保有する個人情報と結合することにより連絡先を得て利用することがあります。）
- 全学アカウントなどのご本人自身による照会に際してのご本人の確認
- 統計データの作成

3. 全学アカウントとパスワードの利用目的

本学情報システムの全学アカウントとパスワードは、本学が提供する教育研究その他業務のためのサービスにおいて、これらの組み合わせにより利用者個人を認証するために利用します。利用者個人の認証に際しては、サービスの必要に応じ氏名など利用者個人を特定する情報と結合することがあります。

4. 利用記録の取得とその利用目的

利用者による全学アカウントを用いた本学情報システムの利用に関して以下の事項について利用コードおよび時刻情報を含めて利用記録を取得します。

- A 大学ネットワークならびに全学統一認証方式を用いる A 大学内のすべての情報システムにおける、全学アカウントとパスワードを用いて行われる利用者の認証記録
- 情報メディアセンターの電子メールシステムにおける電子メールの送信と受信
- 情報メディアセンターの情報処理演習システムの端末からの Web サイトのアクセス

これらの利用記録は以下の目的のために利用します。

(1)利用者自身のご利用上の問題解決の支援
(2)情報メディアセンターの情報システムの運用の改善
(3)関係法令、本学関係規程ならびに情報システム利用心得遵守の確認のため
(4)統計データ

5. 個人情報の安全確保、利用、提供、開示、訂正並びに利用停止

収集した個人情報の安全確保、利用、提供、開示、訂正並びに利用停止については「A 大学個人情報保護規程」に則して取り扱います。

別紙２　A 大学情報システム利用申請書

情報メディアセンター提出用

A 大学情報システム利用申請書

A 大学情報システム利用規程第四条に基づき、全学アカウントの交付を申請します。

申請日 application date					年 Year			月 Month			日 Day

氏名/Name(Last,First)	フリガナ/Name in Kana	利用申請者の区分/ Current Status
		1. 学部学生/undergraduate 2. 大学院生/graduate 3. 常勤教職員/permanent staff 4. 非常勤教職員/part time staff 5. 名誉教授/emeritus 6. 研究生/research student 7. その他/other (　　)
所属部局・学科等/Faculty・Department	学生証、職員証、身分証の番号(左詰)/ ID Number(left-align)	
連絡先電話番号/Telephone Number	誕生日/Date of Birth	・該当する番号に○印 ・その他の方は括弧内に区分を記入
	月 Month / 日 Day	

A 大学情報システム利用心得

1. A 大学情報システムの全学アカウントの交付を受けた者(以下、利用者という)は利用に際して、関連法令を遵守しなければならない。利用者は、本学情報システム運用基本方針、本学情報システム運用基本規程、本学情報システム利用規程(以下、利用規程という)および本学個人情報保護規程を遵守しなければならない。
2. 利用者は、利用規程第五条に定めるアカウントの管理に関する規定を遵守しなければならない。
   利用者は利用に際して、当該システムを管理する部局の担当職員および当該部局がコンピュータシステムの管理を委託した者の指示に従わなければならない。
3. 利用者は、毎年度1回は、本学が定める年度講習計画に従って、本学情報システムの利用に関する教育を受講しなければならない。利用者は、本学が定める自己点検基準に基づいて自己点検を実施しなければならない。
4. 利用者は利用に際して、利用規程第十条に定める禁止事項に該当する行為を行ってはならない。
   利用者は利用に際して、利用規程第十二条に定める PC 取扱ガイドライン、利用規程第十三条に定める電子メール利用ガイドライン、利用規程第十四条に定めるウェブブラウザ利用ガイドラインおよびウェブ公開ガイドライン、利用規程第十五条に定めるモバイル PC の利用手順を遵守しなければならない。
   利用者は利用に際して、他人のプライバシーおよび人格を尊重しなければならない。
   利用者は利用に際して、他人の著作権およびその他の知的財産権を尊重しなければならない。
   利用者は利用に際して、A 大学の定めるセクシャルハラスメント等に関する方針を遵守しなければならない。
   利用者は利用に際して、A 大学の定める大学における言論に関する方針を遵守しなければならない。
5. 利用者は利用に際して、本学情報システムを構成する計算機のハードウェア、ソフトウェアおよび装置を毀損、破壊または改変してはならない。
   利用者は利用に際して、利用規程第十七条に定める安全管理に関する義務を負う。
6. 本学情報システムの利用にあたり故意または過失により本学情報システムを構成する計算機組織に損害を生じさせた利用者は、それによって生じた損害を賠償する責任を負う。本学情報システムによるサービス提供を妨害した利用者は、それによって生じた損害を賠償する責任を負う。

誓　約　書

A 大学情報メディアセンター長　殿

A 大学情報システム利用規程及び情報システム利用心得を遵守して、本学情報システムを利用することに同意します。これらに違反した場合、センター長が、私のアカウントを取り消すこと、あるいは私のアカウントの利用を一時停止すること、又は私のアカウントの権限により作成された本学情報システム上の電子情報ファイルの一部ないし全部を放棄させることに異議はありません。

(　　)年/Year　(　　)月/Month　(　　)日/Day

自署/Signature(　　)

申請者控(利用期間中は確実に保管のこと)

A 大学情報システム利用申請書(控)

A 大学情報システム利用規程第五条に基づき、全学アカウントの交付を申請します。

申請日 application date	年 Year	月 Month	日 Day

氏名/Name(Last,First)	フリガナ/Name in Kana	利用申請者の区分/ Current Status
		1. 学部学生/undergraduate 2. 大学院生/graduate 3. 常勤教職員/permanent staff 4. 非常勤教職員/part time staff 5. 名誉教授/emeritus 6. 研究生/research student 7. その他/other ( )
所属部局・学科等/Faculty・Department	学生証、職員証、身分証の番号(左詰)/ ID Number(left-align)	
連絡先電話番号/Telephone Number	誕生日/Date of Birth	
	月 Month / 日 Day	・該当する番号に○印 ・その他の方は括弧内に区分を記入

この用紙にはパスワードは書き込まないでください。
Don't write your password on this sheet!

全学アカウント/User ID	メールアドレス/e-mail address
	_____ @ mail.example.ac.jp

A 大学情報システム利用心得

1. A 大学情報システムの全学アカウントの交付を受けた者(以下、利用者という)は利用に際して、関連法令を遵守しなければならない。利用者は、本学情報システム運用基本方針、本学情報システム運用基本規程、本学情報システム利用規程(以下、利用規程という)および本学個人情報保護規程を遵守しなければならない。
2. 利用者は、利用規程第六条に定めるアカウントの管理に関する規定を遵守しなければならない。
   利用者は利用に際して、当該システムを管理する部局の担当職員および当該部局がコンピュータシステムの管理を委託した者の指示に従わなければならない。
3. 利用者は、毎年度1回は、本学が定める年度講習計画に従って、本学情報システムの利用に関する教育を受講しなければならない。利用者は、本学が定める自己点検基準に基づいて自己点検を実施しなければならない。
4. 利用者は利用に際して、利用規程第十条に定める禁止事項に該当する行為を行ってはならない。
   利用者は利用に際して、利用規程第七条に定める情報機器取扱ガイドライン、利用規程第十三条に定める電子メール利用ガイドライン、利用規程第十四条に定めるウェブブラウザ利用ガイドラインおよび情報発信ガイドラインを遵守しなければならない。
   利用者は利用に際して、他人のプライバシーおよび人格を尊重しなければならない。
   利用者は利用に際して、他人の著作権およびその他の知的財産権を尊重しなければならない。
   利用者は利用に際して、A 大学の定めるセクシャルハラスメント等に関する方針を遵守しなければならない。
   利用者は利用に際して、A 大学の定める大学における言論に関する方針を遵守しなければならない。
5. 利用者は利用に際して、本学情報システムを構成する計算機のハードウェア、ソフトウェアおよび装置を毀損、破壊または改変してはならない。
   利用者は利用に際して、利用規程第十六条に定める安全管理に関する義務を負う。
6. 本学情報システムの利用にあたり故意または過失により本学情報システムを構成する計算機組織に損害を生じさせた利用者は、それによって生じた損害を賠償する責任を負う。本学情報システムによるサービス提供を妨害した利用者は、それによって生じた損害を賠償する責任を負う。

誓 約 書

A 大学情報メディアセンター長 殿

A 大学情報システム利用規程及び情報システム利用心得を遵守して、本学情報システムを利用することに同意します。これらに違反した場合、センター長が、私のアカウントを取り消すこと、あるいは私のアカウントの利用を一時停止すること、又は私のアカウントの権限により作成された本学情報システム上の電子情報ファイルの一部ないし全部を放棄させることに異議はありません。

( )年/Year ( )月/Month ( )日/Day

自署/Signature( )

別紙３　ID 交付申請区分

<table>
<tr><th></th><th colspan="3">身　　分</th><th>講習会受講</th><th>更新手続き</th><th>備　　考</th></tr>
<tr><td rowspan="2">一　学生等</td><td>学部学生
大学院学生</td><td>学生証
（学生部発行・顔写真あり）</td><td rowspan="4">「学生証」「職員証」等の大学発行の身分証を提示、顔写真付のものについては対面にて確認</td><td rowspan="2">必要</td><td>必要
（身分変更が生じた年度のみ）</td><td>10 月入学生については所定の年限の 9 月末で失効</td></tr>
<tr><td>研究生
研究員
研修員
研究者
他</td><td>学生証
（部局発行・顔写真なし）</td><td>必要
（毎年度）</td><td>アカウントの有効期限は身分証の有効期限と年度末の早い方まで</td></tr>
<tr><td rowspan="3">二　教職員等</td><td>常勤教職員
特定有期雇用教職員</td><td>職員証
（人事部発行・顔写真あり）</td><td rowspan="3"></td><td></td><td>着任早々で身分証を未取得の場合は「人事異動通知書」の提示。身分証番号を所属人事又は総務担当より入手。さらに以下のいずれかの方法で顔写真を確認する。1）公的機関発行の顔写真付身分証の提示　2)1ヶ月以内に顔写真付職員証を持参して再確認</td></tr>
<tr><td>時間雇用職員
有期雇用職員
　事務補佐員
　技術補佐員
他</td><td rowspan="2">身分証（職員証等）
（部局発行・顔写真なし）</td><td>必要
（毎年度）</td><td>着任早々で身分証を未取得の場合は「労働条件通知書」または「受入証明書」の提示。身分証番号を所属人事又は総務担当より入手。</td></tr>
<tr><td>外国人研究員
外国人教師
客員教員
招聘外国人学者
派遣職員
他</td></tr>
<tr><td>三　臨時利用者</td><td>訪問者
受託業務従事者
他</td><td>身分証
（受入証明書に記載の所属機関発行）</td><td>受入部局長名で受入証明書等の提出</td><td>必要
（学生のみ）</td><td>必要
（毎年度）</td><td>個別に情報メディアセンター全学アカウント担当へ問い合わせる。</td></tr>
</table>

用語集

	用 語	説 明	定義文書
A	A 大学全学認証基盤	A 大学における教育研究、福利厚生のためのサービスを提供する際に必要となる、利用者認証と主体認証情報の提供を行う情報システムをいう。	C2601
	A 大学認証局	A 大学電子認証局ポリシー及び運用規則に定める認証局をいう。	C2601
B	BCP（Business Continuity Plan: 事業継続計画)	組織において特定する事業の継続に支障を来すと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適切に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。狭義には、このうちの事態発生後の事業の維持を主とした計画をいう。	C2502
C	CRYPTREC	Cryptography Research and Evaluation Committees の略称であって、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。	C2502
	CSIRT	本学において発生するインシデントに対処するために設置された体制をいう。Computer Security Incident Response Team の略。	C2501
D	DNS サーバ	名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させる電子計算機をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の二種類に分けることができる。	C2502
I	IC カード	C2101-02 情報システム運用・管理規程第二条三十八に定める主体認証情報格納装置のうち、主体認証情報を IC に格納するものをいう。	C2601
	IPv6 移行機構	物理的にひとつのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、電子計算機や通信回線装置が2つの通信プロトコルを併用するデュアルスタック機構や、相互接続性のない2つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。	C2502
	ISP	Internet Service Provider の略称であり、インターネットへの接続サービスを提供する事業者のことをいう。	―
M	MAC アドレス	機器等が備える有線 LAN や無線 LAN のネットワークインタフェースに割り当てられる固有の認識番号である。識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割り当てる番号の組み合わせによって表される。	C2502
P	PIN	電子証明書を格納した IC カードを使った主体認証時に使われる主体認証情報をいう。Personal Identification Number の略。	C2601
S	S/MIME	公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。	C2502
	SNS	Social Network Service の略称であり、会員による社会的コミュニケーションを目的とした情報交換や情報共有のためのサービスをいう。	―
U	UPKI 電子証明書発行サービス	大学共同利用機関法人情報・システム研究機構国立情報学研究所（NII）の事業として実施されている、高等教育機関等を対象とした電子証明書発行サービスをいう。	C2501
	URI	http://wwww.example.com/のようなウェブサイトをアクセスするためのキーとなる情報。URL（Universal Resource Locator）と呼ぶことも普通におこなわれている。Universal Resource Identifier の略。	―
	URL	http://wwww.example.com/のようなウェブサイトをアクセスするためのキーとなる情報。URI（Universal Resource Identifier）と呼ぶこともある。Universal Resource Locator の略。	―

	用 語	説 明	定義文書
V	VPN	暗号技術等を利用し、インターネットなどの公衆回線を私設通信回線として広域化するための技術をいう。Virtual Private Network の略。	C2502
あ	アイデンティティ情報	利用者に関する全学アカウントおよび属性情報を総称する情報をいう。	C2601
	アクセス制御	情報へのアクセスを許可する者を制限することをいう。	C2502
	アプリケーション	オペレーティングシステム上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。	C2502
	アルゴリズム	ある特定の目的を達成するための演算手順をいう。	C2502
	暗号化	第三者に容易に解読されないよう、定められた演算を施しデータを変換することをいう。	C2502
	暗号モジュール	暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。	C2502
い	委託先	外部委託により本学の情報処理業務の一部又は全部を実施する者をいう。	C2501
	インシデント	情報セキュリティに関し、意図的または偶発的に生じる、本学規程または法律に反する事故あるいは事件をいう。	C1001
		物理的インシデント、セキュリティインシデントまたはコンテンツインシデントを言う。	C3102
う	ウェブクライアント	ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。	C2502
	ウェブサーバ	HTTP サーバアプリケーション、当該サーバアプリケーションで動作するウェブアプリケーション及びデータベース並びに負荷分散装置等のようにウェブサーバと一体として動作するハードウェアをいう。	―
	受渡業者	事務従事者との物品の受渡しを目的とした者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。	C2502
か	外部委託	本学の情報処理業務の一部又は全部について、契約をもって学外の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。	C2501
	学外	本学が管理する組織又は施設の外をいう。	―
	学外クレーム	学内の利用者等による情報発信行為（本学の業務としてなされたものを除く）の問題を指摘しての連絡・通報及び学外(学内の者が、弁護士等の代理人を立てる場合も含む)からの発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び証拠、証言の収集や犯罪捜査等にかかわる協力要請や強制的命令を言う。	C3102
	学外通信回線	一つの本学が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該高等教育機関の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。学内通信回線には、専用線や VPN 等物理的な回線を本学が管理していないものも含まれる。	C2501
	学外窓口	インシデントについて学外から連絡・通報を受け、学外への連絡・通報、対外クレームをするための窓口を言う。	C3102
	学生等	本学通則に定める学部学生、大学院学生、研究生、研究員、研修員並びに研究者等、その他、部局総括責任者が認めた者をいう。	C1001
	学内	本学が管理する組織又は施設の内をいう。	―
	学内通信回線	物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び本学管理又は他組織管理）及び通信回線装置を問わず、本学が管理する電子計算機を接続し、当該電子計算機間の通信に利用する論理的な通信回線をいう。	C2501

	用 語	説 明	定義文書
	可用性	情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。	C2502
	可用性1情報	可用性2情報以外の情報（書面を除く。）をいう。	C2103
	可用性2情報	本学で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用者等の権利が侵害され又は本学の活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。	C2103
	完全性	情報が破壊、改ざん又は消去されていない特性をいう。	C2502
	完全性1情報	完全性2情報以外の情報（書面を除く。）をいう。	C2103
	完全性2情報	本学で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者等の権利が侵害され又は本学の活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。	C2103
き	機器等	情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。	C2501
	機密性	情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。	C2502
	機密性1情報	情報公開法第5条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報をいう。	C2103
	機密性3情報	本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年 4 月 1 日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報をいう。	C2103
	機密性2情報	本学で取り扱う情報のうち、独立行政法人の保有する情報の公開に関する法律（平成 13 年 12 月 5 日法律第 140 号）第5条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性3情報」以外の情報をいう。	C2103
	教職員等	本学を設置する法人の役員及び、本学に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、部局総括責任者が認めた者をいう。	C1001
	業務継続計画	本学において策定されている BCP（Business Continuity Plan: 事業継続計画）をいう。	C2502
	共用識別コード	複数の主体が共用することを想定した識別コードをいう。原則として、1つの識別コードは1つの主体のみに対して付与されるものであるが、情報システム上の制約や利用状況等に応じて、識別コードを組織で共用する場合もある。このように共用される識別コードを共用識別コードという。	C2502
	記録媒体	情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。	C2501
	緊急連絡網	運用・管理規程に基づき整備された[インシデント/障害等]に備え、特に重要と認めた情報システムについて、その部局技術責任者及び部局技術担当者の緊急連絡先、連絡手段、連絡内容を含む連絡網を言う。	C3102
け	権限管理	主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。	C2502

	用 語	説 明	定義文書
こ	コンテンツインシデント	ネットワークを利用した情報発信内容（以下「コンテンツ」という）が著作権侵害等の他人の権利侵害や児童ポルノ画像の公開等の違法行為または公序良俗違反である行為(及びその旨主張する被害者等からの請求）による事故を言い、下記原因を含む。 －電子掲示板、ブログやウェブページ等での名誉・信用毀損にあたる情報の発信 －他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信 －通信の秘密を侵害する行為 －他人の著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信 －秘密であるデータやプログラムの不正公開等守秘義務に違反する情報の発信 －児童ポルノやわいせつ画像の公開 －ネットワークを利用したねずみ講 －差別、侮辱、ハラスメントにあたる情報の発信 －営業ないし商業を目的とした本学情報システムの利用行為	C3102
さ	サーバ装置	通信回線等を経由して接続してきた電子計算機に対して、自らが保持しているサービスを提供する電子計算機をいう。	C2501
	サービス	サーバ装置上で動作しているアプリケーションにより、接続してきた電子計算機に対して提供される単独又は複数の機能で構成される機能群をいう。	－
	サービス不能攻撃	セキュリティホールを悪用しサーバ装置若しくは通信回線装置のソフトウェアを動作不能にさせること、又はサーバ装置、通信回線装置若しくは通信回線の容量を上回る大量のアクセスを意図的に行い通常の利用者のサービス利用を妨害する攻撃をいう。	C2502
	最小限の特権機能	管理者権限を実行できる範囲を必要最小限に制限する機能をいう。	C2502
し	識別	情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。	C2502
	識別コード	主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。	C2502
	事業継続計画	→BCP 参照	－
	実施規程	ポリシーに基づいて策定される規程及び、基準、計画をいう。	C1001
	実施手順	事務情報セキュリティ対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。	C2501
	事務従事者	本学の事務に従事している本学のの指揮命令に服している者であって、本学の管理対象である情報及び情報システムを取り扱う者をいう。事務従事者には、個々の勤務条件にもよるが、例えば、派遣労働者等も含まれている。	C2501
	事務情報	事務情報とは情報のうち次のものをいう。 (1) 「法人文書の管理に関する規程」の対象となる法人文書 (2) (1)以外の法人文書で、部局長が指定した文書	C1001
	事務情報システム	事務情報を扱う情報システムをいう。	C1001
	主体	情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。	C2502
	主体認証	識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。	C2502

	用 語	説 明	定義文書
	主体認証情報	主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。	C2502
	主体認証情報格納装置	主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、ICカード等がある。	C2502
	情報	情報には次のものを含む。 (1) 情報システム内部に記録された情報 (2) 情報システム外部の電磁的記録媒体に記録された情報 (3) 情報システムに関係がある書面に記載された情報	C1001
	情報資産	情報システム並びに情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。	C1001
	情報システム	情報処理及び情報ネットワークに係わるシステムで、次のものをいい、本学情報ネットワークに接続する機器を含む。 (1) 本学により、所有又は管理されているもの (2) 本学との契約あるいは他の協定に従って提供されるもの	C1001
	情報セキュリティ	情報資産の機密性、完全性及び可用性を維持することをいう。	C1001
	情報セキュリティインシデント	JIS Q 27001:2006 における情報セキュリティインシデントをいう。	C2501
	情報セキュリティ関係規程	事務情報セキュリティ対策基準及び実施手順を総称したものをいう。	C2501
	情報の移送	学外に、電磁的に記録された情報を送信すること並びに情報を記録した電磁的記録媒体及び書面を運搬することをいう。	－
	情報の抹消	電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。	C2502
せ	セキュリティパッチ	発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。	C2502
	セキュリティホール	オペレーティングシステム又はアプリケーション等に存在し、それら自身や処理する情報のセキュリティが侵害される原因となる可能性のある問題をいう。	－
	全学アカウント	A 大学全学認証基盤で主体認証を行う情報システムにおいて、主体に付与された正当な権限をいう。全学アカウントの付与は、識別コードと主体認証情報の配布、主体認証情報格納装置の交付、アクセス制御における許可、またはそれらの組み合わせ等によって行われる。	C2201
	全学情報システム	全学の情報基盤として供される本学情報システムのうち、全学認証基盤を利用可能なものをいう。	C1000
そ	ソフトウェア	サーバ装置、端末、通信回線装置を動作させる手順及び命令を、電子計算機が理解できる形式で記述したものをいう。オペレーティングシステムやオペレーティングシステム上で動作するアプリケーションを含む広義の意味である。	C2502
	属性情報	全学アカウントに付随して管理・提供される利用者に関する情報をいう。	C2601

	用 語	説 明	定義文書
た	対外クレーム	対内的インシデントに対し、学外の発信者に対して連絡・通報し、または発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び当局に犯罪捜査の告訴・告発をすることを言う。	C3102
	対外的インシデント	インシデントのうち、利用者等による行為であって、外部ネットワークにおけるあるいは外部のシステムに対して行われた行為による事故、事件を言う。	C3102
	代替措置	例外措置の適用に伴い発生するリスクを低減するためにポリシー・実施規程・手順が定める内容とは異なる代替のセキュリティ対策をいう。	C3101
	耐タンパ性	暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。	C2502
	対内的インシデント	インシデントのうち、外部のネットワークから内部に向かって行われた行為による事故、事件を言う。	C3102
	端末	情報システムの構成要素である機器のうち、事務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。	C2501
つ	通信回線	複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。	C2501
	通信回線装置	通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。	C2501
て	手順	実施規程に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。	C1001
	電子計算機	コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。	―
	電子署名	情報の正当性を保証するための電子的な署名情報をいう。	C2502
	電子証明書	A 大学認証局から発行された証明書でログイン時の主体認証等に利用するため証明書をいう。	C2601
	電磁的記録	電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。	C1001
	電子メールクライアント	電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。	C2502
	電子メールサーバ	電子メールの利用者に対する電子メールの送受信のサービス及び電子メールの配送を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。	C2502
と	特定用途機器	テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。	C2501
	ドメインネームシステム（DNS）	クライアント等からの問合わせを受けて、ドメイン名やホスト名と IP アドレスとの対応関係について回答を行うデータベースシステムである。	C2502
	ドメイン名	国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.sample.ac.jp というウェブサイトの場合は、sample.ac.jp の部分がこれに該当する。	C2502

	用 語	説 明	定義文書
	取扱制限	情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。	C2103
な	名前解決	ドメイン名やホスト名と IP アドレスを変換することをいう。	C2502
に	認証接続	認証と認可を目的として、全学情報システム、もしくは部局情報システムが A 大学全学認証基盤のアイデンティティ情報を利用することをいう。	C2601
	認証接続システム	A 大学全学認証基盤に認証接続された全学情報システムもしくは部局情報システムをいう。	C2601
	認証接続責任者	認証接続システムの認証接続に係る責任を有する本学の職員をいう。	C2601
ひ	非常事態	本学情報システムの運用に関するインシデントのうち特に緊急性を要するものをいう。	C2102
ふ	フィッシング（phishing）	悪意ある第三者等が、実在する機関等からのお知らせであるかのように偽装した電子メールを送りつけ、受け取った者にその電子メールに記載された URL をクリックさせ、あらかじめ用意された偽のウェブサイトに誘導し、ID、パスワード、その他重要な情報を記入させて、情報を窃取するという行為である。	C2102
	不正プログラム	コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。	C2501
	不正プログラム定義ファイル	不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。	C2502
	物理的インシデント	地震等の天災、火災、事故、盗難等によるネットワークを構成する機器や回線の物理的損壊や滅失及びその他の物理的原因による情報システムやネットワークの機能不全や障害等、情報セキュリティの確保が困難な事由の発生およびそのおそれを言う。	C3102
	踏み台	悪意ある第三者によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。	C2502
ほ	ポリシー	本学が定める「C1000 情報システム運用基本方針」及び「C1001 情報システム運用基本規程」をいう。	C1001
	本学支給以外の端末	本学が支給する端末の端末をいう。いわゆる私物の PC のほか、本学への出向者に対して出向元組織が提供する端末も含むものとする。	―
む	無線 LAN	IEEE802.11a、802.11b、802.11g、802.11n 等の規格により、無線通信で情報を送受信する通信回線をいう。	C2502
め	明示等	情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。	C1001
も	モバイル端末	端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。	C2501
や	約款による外部サービス	民間事業者等の学外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。	C2501
よ	要安定情報	可用性2情報をいう。	C2103

	用 語	説 明	定義文書
	要管理対策区域	本学が管理する施設等（外部の組織から借用している施設等を含む。）本学の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。	C2501
	要機密情報	機密性2情報及び機密性3情報をいう。	C2103
	要保護情報	要機密情報、要保全情報及び要安定情報をいう。	C2103
	要保全情報	完全性2情報をいう。	C2103
り	リスク	目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。	C2502
	利用者	教職員等及び学生等で、本学情報システムを利用する許可を受けて利用するものをいう。	C1001
	利用者等	利用者及び臨時利用者のほか、本学情報システムを取り扱う者をいう。	C2201
	臨時利用者	教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。	C1001
る	ルートヒントファイル	最初に名前解決を問合わせる DNS コンテンツサーバ（以下「ルート DNS」という。）の情報をいう。ルートヒントファイルには、ルート DNS のサーバ名と IP アドレスの組が記載されており、ルートDNS のIP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC （Internet NetworkInformation Center）のサイトから入手可能である。	C2502
れ	例外措置	教職員等がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、大学事務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。	C3101
ろ	ログイン	何らかの主体が主体認証を要求する行為をいう。ログインの後に主体認証が行われるため、ログインの段階ではその主体が正当であるとは限らない。	―

用語索引

本索引は用語の定義もしくは解説を行っているページのみを対象としている。用語が出現しているページすべてを参照しているわけではないので留意されたい。また、特定の文書内に限定して用語を用いている例もあるので注意のこと。

（注）**太字**のページ番号は、当該見出しを定義しているページを示す。

れ

ろ