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

（2013 年版）

2013 年 7 月 5 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，中山雅哉，西村浩二，野川裕記，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が 2012 年 4 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群（平成 24 年度版）」に準拠するものである。

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）
http://www.nii.ac.jp/csi/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（個人情報保護法）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」（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/csi/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、CP/CPS(Certificate Policy / Certificate Practice Statement)をはじめとした各種ガイドラインは国立情報学研究所および UPKI イニシアティブが検討・公開しているので、次のサイトを参考にされたい。

（参考） https://upki-portal.nii.ac.jp/

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。

このうち、今回（2013 年7 月）公開するのは、B1xxx および B2xxx の文書番号をもつ、実施規程以上の文書である。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、今回の公開分より、文書番号冒頭の記号を A から B に変更した。

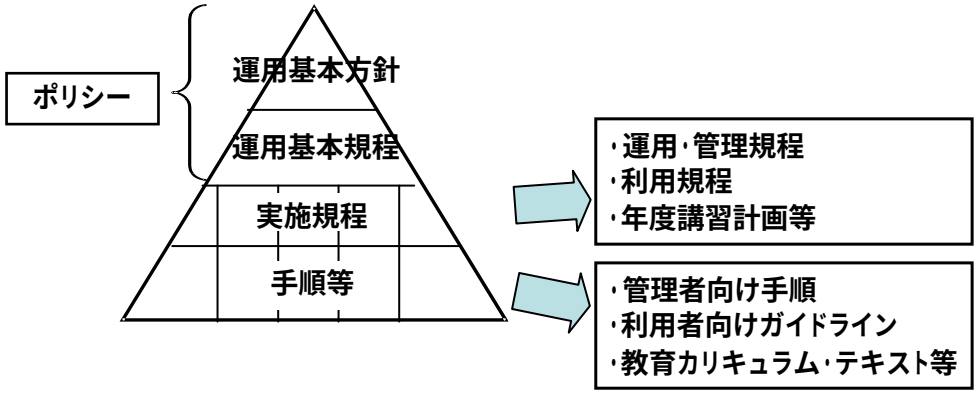

図１　ポリシー・実施規程・手順等の位置付け

ポリシー	実施規程	手順･ガイドライン等
B1000 情報システム運用基本方針 B1001 情報システム運用基本規程	B2101 情報システム運用･管理規程 B2102 情報システム運用リスク管理規程 B2103 情報システム非常時行動計画に関する規程 B2104 情報格付け基準	B3100 情報システム運用･管理手順の策定に関する解説書 B3101 情報システムにおける情報セキュリティ対策実施手順(策定手引書) B3102 例外措置手順書 B3103 インシデント対応手順 B3104 情報格付け取扱手順 B3105 情報システム運用リスク評価手順 B3106 人事異動の際に行うべき情報セキュリティ対策実施手順 B3107 機器等の購入における情報セキュリティ対策実施手順(策定手引書) B3108 外部委託における情報セキュリティ対策実施手順 B3109 外部委託における情報セキュリティ対策に関する評価手順
	B2151 情報セキュリティ要件の明確化に関する技術規程 B2152 情報セキュリティ対策に関する技術規程 B2153 情報システムの構成要素に関する技術規程	B3151 セキュリティホール対策計画に関する様式(策定手引書) B3152 ウェブサーバ設定確認実施手順(策定手引書) B3153 電子メールサーバのセキュリティ維持手順(策定手引書) B3154 ソフトウェア開発における情報セキュリティ対策実施手順(策定手引書)
	B2201 情報システム利用規程 B2202 認証基盤利用規程	B3200 情報システム利用者向け文書の策定に関する解説書 B3211 学外情報セキュリティ水準低下防止手順 B3212 自己点検の考え方と実務への準備に関する解説書
		B3251 情報機器取扱ガイドライン B3252 電子メール利用ガイドライン B3253 ウェブブラウザ利用ガイドライン B3254 情報発信ガイドライン B3255 利用者パスワードガイドライン
	B2301 年度講習計画	B3300 教育テキストの策定に関する解説書 B3301 教育テキスト作成ガイドライン(利用者向け) B3302 教育テキスト作成ガイドライン(システム管理者向け) B3303 教育テキスト作成ガイドライン(CIO/役職者向け)
	B2401 情報セキュリティ監査規程	B3401 情報セキュリティ監査実施手順
	B2501 事務情報セキュリティ対策管理基準	B3500 各種マニュアル類の策定に関する解説書 B3501 各種マニュアル類(**) B3502 責任者等の役割から見た遵守事項
	B2551 事務情報セキュリティ対策技術基準	
		B3601 情報システムアカウント取得手順
	B2651 証明書ポリシー(*) B2652 認証実施規程(*)	B3650 認証手順の策定に関する解説書

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

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、2012 年 4 月に内閣官房情報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 24 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。また本サンプル規程集には、上記統一基準の利用を支援するために内閣官房情報セキュリティセンターが公開している適用個別マニュアル群の文書を大学向けに調整の上取り込んでいる部分がある。この関係を表２に示す。

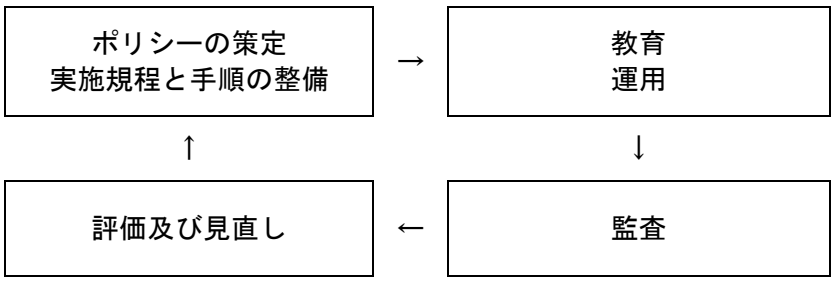

図３　ポリシーの評価及び見直し

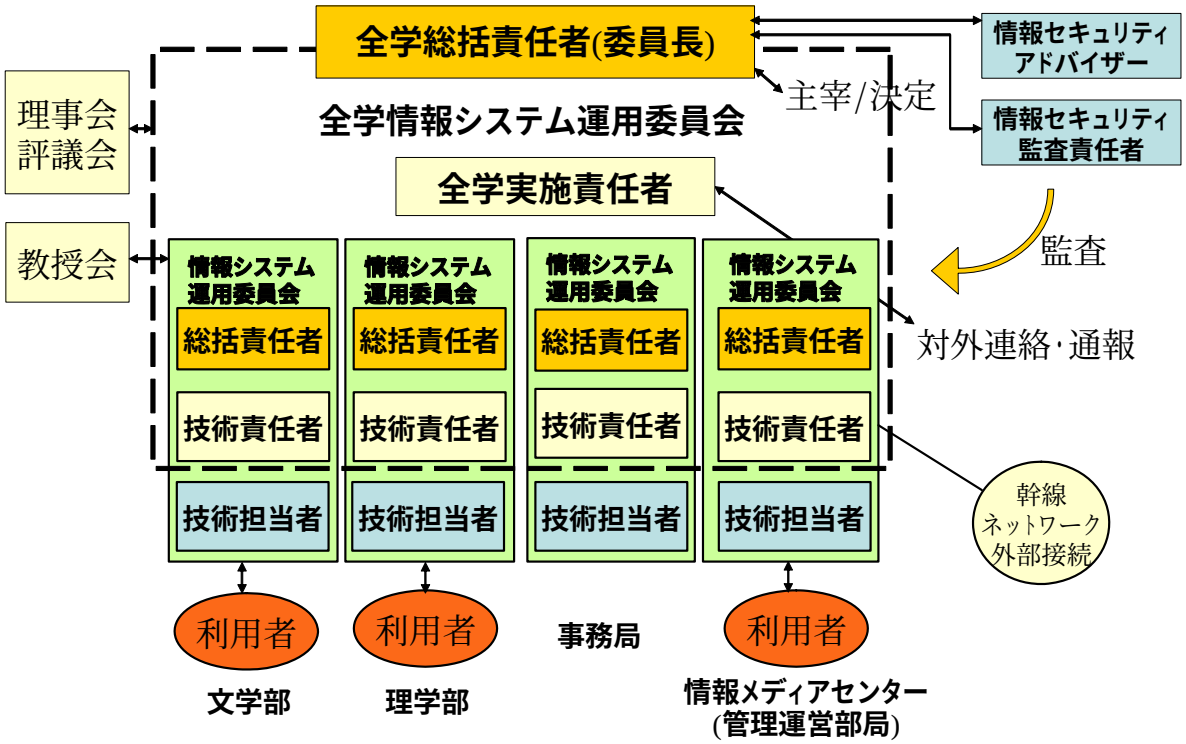

図４　情報システム運用管理体制

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。

表 2　政府機関統一基準適用個別マニュアル群とサンプル規程集の対応

文書番号	文書名	対応文書	取扱
DM2-01	政府機関統一基準で定める責任者等の役割から見た遵守事項一覧	B3502	△
DM2-02	人事異動等の際に行うべき情報セキュリティ対策実施規程 策定手引書 人事異動等の際に行うべき情報セキュリティ対策実施規程 雛形	B3106	△
DM2-03	違反報告書に関する様式 策定手引書		
DM2-04	例外措置手順書 策定手引書 例外措置手順書 雛形 例外措置申請・終了報告書に関する様式 策定手引書 例外措置申請・終了報告書	B3102	△
DM2-05	障害等対処手順書 策定手引書 障害等対処手順書 雛形 障害等報告書に関する様式 策定手引書 障害等報告書	B3103	◎
DM2-06	障害等再発防止策報告書に関する様式 策定手引書 障害等再発防止策報告書 自己点検の考え方と実務への準備 解説書	B3202	◎
DM2-07	情報セキュリティ監査実施手順 策定手引書	B3401	△
DM3-01	情報の格付け及び取扱制限に関する規程 策定手引書	B2104	○
DM3-02	情報取扱手順書 策定手引書 情報取扱手順書 雛形 機密性3情報印刷書面管理表に関する様式 策定手引書 機密性3情報印刷書面管理表 機密性3情報移送・提供許可申請書に関する様式 策定手引書 機密性3情報移送・提供許可申請書 機密性2情報移送・提供届出書に関する様式 策定手引書 機密性2情報移送・提供届出書	B3104	◎
DM4-01	情報システムにおける情報セキュリティ対策実施規程 策定手引書 情報システムにおける情報セキュリティ対策実施規程 雛形	B3101	○
DM4-02	セキュリティホール対策計画に関する様式 策定手引書 セキュリティホール対策計画	B3151	○
DM5-01	庁舎内における PC 利用手順 PC の取扱編 策定手引書 庁舎内における PC 利用手順 PC の取扱編 雛形	B3251	★
DM5-02	庁舎内におけるクライアント PC 利用手順 電子メール編 策定手引書 庁舎内におけるクライアント PC 利用手順 電子メール編 雛形	B3252	★
DM5-03	庁舎内における PC 利用手順 ウェブブラウザ編 策定手引書 庁舎内における PC 利用手順 ウェブブラウザ編 雛形	B3253	★
DM5-04	モバイル PC 利用手順 策定手引書 モバイル PC の利用手順 雛形	B2201	★
DM5-05	サーバ設定確認実施手順 ウェブサーバ編 策定手引書	B3152	△
DM5-06	電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程 策定手引書 電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程 雛形	B3153	○
DM6-01	機器等の購入における情報セキュリティ対策実施規程 策定手引書 機器等の購入における情報セキュリティ対策実施規程 雛形	B3107	○
DM6-02	外部委託における情報セキュリティ対策実施規程 策定手引書 外部委託における情報セキュリティ対策実施規程 雛形	B3108	○
DM6-03	ソフトウェア開発における情報セキュリティ対策実施規程 策定手引書 ソフトウェア開発における情報セキュリティ対策実施規程 雛形	B3154	○
DM6-04	府省庁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規程 策定手引書 府省庁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規程 雛形	B3201	○
DM6-05	府省庁支給以外の情報システムによる情報処理の手順書 PC 編 策定手引書	－	※
DM6-06	外部委託における情報セキュリティ対策に関する評価手法の利用の手引	B3109	△
DM6-07	情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書	－	◆
DM6-08	情報システムの構築等における ST 評価・ST 確認の実施に関する解説書	－	◆

（表 2 の凡例）

△：NISC 発行の文書の用語を大学向けに変更したもの

〇：NISC 発行の文書の用語を大学向けに変更した上、内容を一部変更したもの

◎：NISC 発行の文書の用語を大学向けに変更した上、内容を大幅に変更したもの

★：NISC 発行の文書の内容とは全く別個に策定したもの

－：本サンプル規程集において対応する文書を用意しないもの

※：サンプル規程集が対象とする大学環境においては学生等が個人所有する PC 等を例外扱いすることが現実的ではないため、手順として整備しない

◆：大学向けに内容を変更すべき事項が無いため、解説書として整備しない（必要に応じて各大学が内閣官房情報セキュリティセンターの当該解説書を参照すべき）

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

○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），
佐藤慶浩（日本 HP），庄司勇木（デジタルアーツ），須川賢洋（新潟大学），
曽根秀昭（主査，東北大学），長谷川明生（中京大学），冨士原裕文（元富士通），
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) 高等教育機関のための情報セキュリティポリシー策定支援ポータル
http://www.uispp.jp/
本サンプル規程集の活用に関する各種情報の提供を行っているほか、情報セキュリティポリシーを公開している大学へのリンク等がある。

(2) 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。

(3) 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/csi/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) 京都大学情報セキュリティ対策室 規程集
http://www.iimc.kyoto-u.ac.jp/ismo/regulation/
大学における情報セキュリティ対策に関する規定の策定事例である。

(5) UPKI イニシアティブ
https://upki-portal.nii.ac.jp/
本サンプル規程集における「B2601 証明書ポリシー（CP）」や「B2602 認証実施規程（CPS）」は本サイトで公開されている「キャンパス PKI CP/CPS ガイドライン」に相当する。

イ．情報セキュリティや著作権保護に関するもの

(1) 内閣官房情報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
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/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 情報セキュリティに関する政策、緊急情報
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）セキュリティセンター
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) 有限責任中間法人 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/
企業向けの情報セキュリティポリシーのサンプル等を活動成果として公開。

(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/index.htm
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。

B1000 情報システム運用基本方針

B1000-01　（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。

B1000-02　（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。

B1000-03　（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。

B1000-04　（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。

B1001 情報システム運用基本規程

B1001-01　（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。

B1001-02　（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。

B1001-03　（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。五項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「B1000 情報システム運用基本方針」及び「B1001 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。十一項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、九項と十項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　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：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　明示等

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。

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。

B1001-04　（全学総括責任者）

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。

B1001-05　（全学情報システム運用委員会）

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棄損、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　インシデントの再発防止策の検討及び実施

B1001-06　（全学情報システム運用委員会の構成員）

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。

B1001-07　（全学情報システム運用委員会の委員長）
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。

B1001-08　（全学実施責任者）
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（２項）と教育（３項）及び連絡・通報窓口（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。

B1001-09　（情報セキュリティ監査責任者）
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。

B1001-10　（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。

B1001-11　（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

B1001-12　（部局総括責任者）
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。

B1001-13　（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

B1001-14　（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

B1001-15　（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。

B1001-16　（部局技術責任者）
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。

B1001-17　（部局技術担当者）
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、技術担当者を置く。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技術担当者を兼務することができる。
２　技術担当者は、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、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。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。

B1001-18　（役割の分離）
第十八条　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。

B1001-19　（情報の格付け）

第十九条　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こと。

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「B2104 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。

B1001-20　（本学外の情報セキュリティ水準の低下を招く行為の防止）

第二十条　全学実施責任者は、本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：本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。本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、本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：本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。

B1001-21　（情報システム運用の外部委託管理）

第二十一条　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。

B1001-22　（情報セキュリティ監査）

第二十二条　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である。

B1001-23　（見直し）

第二十三条　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。

B2101 情報システム運用・管理規程

第一章　総則

解説：(1) 規程の構成

本規程は、「B1000 情報システム運用基本方針」及び「B1001 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。

サンプル規程集では、管理規程である本規程の他、本規程に記載された情報セキュリティ対策を実施する上での具体的な技術規程として、「B2151 情報セキュリティ要件の明確化に関する技術規程」「B2152 情報システムの構成要素に関する技術規程」「B2153 アプリケーションソフトウェアに関する技術規程」を定めている。管理に関する規程は下二桁を 00 番台、技術に関する規程は下二桁を 50 番台とする。これらの規程は、情報技術の進歩や大学を取り巻く環境の変化に応じて、定期的に見直しを行い、必要に応じて改訂する必要がある。技術的な内容であり、改訂頻度が高いものについては、技術規程に定めることが考えられる。

(2) 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管理基準（平成 24 年度版）」及び「政府機関の情報セキュリティ対策のための統一管理基準（平成 24 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管理基準の対応項番を付してある。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。

(3) 規程の表現

本規程で定める遵守事項は、政府機関統一基準に従い、「……すること」の述語を用いている箇所も多い。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ことも必要だろう。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必要がある。「……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しばしば見られる。

B2101-01　（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、「B1000 情報システム運用基本方針」及び「B1001 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規制等（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。

(1) 文部科学省「学校における生徒等に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」
http://www.mext.go.jp/b_menu/public/2004/ 04111001/001.pdf

(2) 社団法人私立大学情報教育協会「個人情報保護法施行に伴う電子化対応アンケート」http://www.shijokyo.or.jp/pi2004/shiryo.html

B2101-02　（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「B1000 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「B1001 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　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。

七　端末　利用者等が直接操作を行う電子計算機（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。）であり、いわゆる PC のほか、PDA 等も該当する。

八　通信回線　これを利用して複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みであり、物理的なものと論理的なものがある。

九　通信回線装置　回線の接続のために設置され、電子計算機により回線上を送受信される情報の制御を行うための装置をいう。いわゆるリピータハブ、スイッチングハブ及びルータ、ファイアウォールのほか、情報コンセントや無線ネットワークアクセスポイント等も該当する。

十　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。

十一　学外通信回線　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、本学が管理していない電子計算機が接続され、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。

十二　情報取扱区域　本学の内外において情報を取り扱う区域をいう。情報取扱区域のうち、求める対策の基準ごとに「クラス」の区分を定める。情報取扱区域におけるクラス及びクラスにおける区分の基準は、それぞれ以下のとおりとする。

クラス	区分の基準
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
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
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
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

十三　要管理対策区域　施設及び環境に係る管理対策が講じられている区域であって、情報取扱区域におけるクラス１以上の区域をいう。

十四　要管理対策区域外　情報取扱区域におけるクラス０の区域をいう。

十五　要管理対策区域外での情報処理　利用者等が情報取扱区域におけるクラス０の区域において教育研究事務の遂行のための情報処理を行うことをいう。なお、オンラインで学外から本学の情報システムに接続して、情報処理を行う場合だけではなく、オフラインで行う場合も含むものとする。

十六　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状態を確保することをいう。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、秘密文書に相当する機密性を要する情報
機密性２情報	本学で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、利用者等の権利が侵害され又は本学の教育研究事務の遂行に支障を及ぼすおそれがある情報
機密性１情報	機密性２情報又は機密性３情報以外の情報

十七　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。）

十八　可用性　情報及び関連資産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、情報及び関連資産にアクセスできる状態を確保することをいう。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。）

十九　要機密情報　機密性２情報及び機密性３情報をいう。

二十　要保全情報　完全性２情報をいう。

二十一　要安定情報　可用性２情報をいう。

二十二　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。

二十三　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。

二十四　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。

二十五　情報の移送　要管理対策区域外に、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。

二十六　情報の抹消　廃棄した情報が漏えいすることを防止するために、全ての情報を復元が困難な状態にすることをいう。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態ではない。

二十七　主体　情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。

二十八　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。

二十九　識別　情報システムにアクセスする主体を特定することをいう。

三十　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。

三十一　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。

三十二　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。

三十三　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、利用状況等を考慮して、１つの識別コードを複数の主体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。

三十四　アクセス制御　主体によるアクセスを許可する客体を制限することをいう。

三十五　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。

三十六　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。

三十七　最少特権機能　管理者権限を実行できる範囲を管理作業に必要な最少の範囲に制限する機能をいう。

三十八　不正プログラム　コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。

三十九　不正プログラム定義ファイル　アンチウイルスソフトウェア等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。

四十　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「B2201 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、「B2101 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（B1000 及び B1001）、実施規程（B2***（管理に関する規程は下二桁を 00 番台、技術に関する規程は下二桁を 50 番台とする。））、手順（B3***）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「B2104 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「B1001 情報システム運用基本規程」に置くことも考えられる。

B2101-03　（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、情報セキュリティ監査責任者、情報セキュリティアドバイザー、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、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

第一節　組織・体制

B2101-04　（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　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。

B2101-05　（職場情報セキュリティ責任者の設置）（政府機関統一管理基準の対応項番 1.2.1.1(7)）

第五条　部局総括責任者は、教室、研究室、事務室等の管理組織毎に職場情報セキュリティ責任

者を１人置くこと。

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毎に１人任命し、全学実施責任者に報告するものである。

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セキュリティ対策に関する事務を統括すること。

３　部局総括責任者は、職場情報セキュリティ責任者を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。

４　全学実施責任者は、全ての職場情報セキュリティ責任者に対する連絡網を整備すること。

B2101-06　（区域情報セキュリティ責任者の設置）（政府機関統一管理基準の対応項番 1.2.1.1(8)）

第六条　全学実施責任者は、要管理対策区域について、情報セキュリティ対策の運用に係る管理を行う区域の単位を定め、その単位ごとに区域情報セキュリティ責任者を置くこと。

解説：要管理対策区域について、情報セキュリティ対策の運用に係る管理を行う単位を決め、区域ごとの情報セキュリティ対策を実施する者を置くことを定めた事項である。

要管理対策区域には、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。

「管理を行う区域の単位」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、上記以外の要管理対策区域（ロビー、廊下等）を一つの区域とする場合も考えられる。

なお、区域情報セキュリティ責任者は、当該区域の利用用途や設置環境等を勘案して、部局総括責任者、職場情報セキュリティ責任者、部局技術責任者又は建物等の管理に関する部門の責任者等の中から定めることが考えられる。定める単位としては、例えば、

・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要管理対策区域（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
等を区域情報セキュリティ責任者として定めることが考えられる。

２　区域情報セキュリティ責任者は、所管する単位における区域ごとの情報セキュリティ対策に関する事務を統括すること。

３　全学実施責任者は、全ての区域情報セキュリティ責任者に対する連絡網を整備すること。

B2101-07　（禁止事項）

第七条　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　違反と例外措置

解説：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は、万一違反があった場合に、定められた手続に従って、適切に対処する必要がある。
また、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等の理由により、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についても、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るものでなければ、当該規程の実効性を確保することが困難となる。
これらのことを勘案し、本節では、違反と例外措置に関する対策基準として、

違反への対処方法及び例外措置の適用方法についての遵守事項を定める。
例外措置の申請手続や審査手続等については、「B3102 例外措置手順書」を併せて参照すること。

B2101-08　（違反への対処）（政府機関統一管理基準の対応項番 1.2.1.3(1)）

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には、各規定の実施に責任を持つ部局総括責任者にその旨を報告すること。

解説：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。本学においては、例規への違反を知った者に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。
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来すもの又はその可能性のあるものをいう。

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こと。

解説：情報セキュリティ関係規程への違反があった場合に、違反者及び当該規程の実施に責任を持つ者を含む必要な者に対して、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ことを求める事項である。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、問題の早期解決、拡大防止の必要がある。例えば、情報セキュリティ関係規程について再度周知する方法が考えられる。

３　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、全学総括責任者にその旨を報告すること。

解説：情報セキュリティ関係規程への違反があった場合に、違反の事実を、その内容、結果、業務への影響、社会的評価等を含めて、全学総括責任者に報告することを求める事項である。

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。

B2101-10　（例外措置）（政府機関統一管理基準の対応項番 1.2.1.3(2)）

第十条　全学情報システム運用委員会は、例外措置の適用の申請を審査する者（以下本条において「許可権限者」という。）を定め、審査手続を整備すること。

解説：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ための事項である。緊急を要して申請される場合は、遂行に不要の遅滞を生じさせずに審査を速やかに実施する必要がある。そのため、申請の内容に応じ、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、部局技術担当者又は職場情報セキュリティ責任者の中から許可権限者を定めておくことが重要である。

2　利用者等は、例外措置の適用を希望する場合には、定められた審査手続に従い、許可権限者に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する等の場合であって、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、事後速やかに申請し許可を得ること。利用者等は、申請の際に以下の事項を含む項目を明確にすること。

一　申請者の情報（氏名、所属、連絡先）

二　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）

三　例外措置の適用を申請する期間
四　例外措置の適用を申請する措置内容（講ずる代替手段等）
五　例外措置の適用を終了した旨の報告方法
六　例外措置の適用を申請する理由

解説：例外措置を利用者等の独断で行わせないための事項である。
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。ただし、教育研究事務の遂行に緊急を要する等の場合であって、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を実施しないことが不可避のときは、事後速やかに申請して許可を得ること。
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場合の被害の大きさと影響を検討、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、リスク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。

3　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。また、決定の際に、以下の項目を含む例外措置の適用審査記録を作成し、全学総括責任者に報告すること。

一　決定を審査した者の情報（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

解説：許可権限者に、例外措置の適用の申請を適切に審査させるための事項である。
審査に当たっては、例外措置の適用を許可した場合のリスクと不許可とした場合の教育研究義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。
例外措置の適用審査記録の報告を受け、全学総括責任者は適用審査記録の台帳を整備することとなるが、これは、将来、許可をさかのぼって取り消す場合に、該当する申請を全て把握し、一貫性をもって取り消すために必要となる。
第一号の「役割名」には、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、部局技術担当者又は職場情報セキュリティ責任者のいずれか

を記載する。

4　利用者等は、例外措置の適用について許可を受け、例外措置を適用した場合には、それを終了した時に、当該例外措置の許可権限者にその旨を報告すること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

解説：例外措置の適用の終了を確認するための事項である。

例外措置の適用期間が終了した場合及び期間終了前に適用を終了する場合には、許可を受けた利用者等が、許可権限者に終了を報告しなければならない。

5　許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な措置を講ずること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

解説：例外措置の適用期間を、許可を受けた者に遵守させるための事項である。

必要な措置としては、許可を受けた者が報告を怠っているのであればそれを督促すること、許可を受けた者が例外措置の適用を継続している場合にはその延長について申請させそれについて審査すること、が挙げられる。

6　全学総括責任者は、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査責任者からの求めに応ずること。

解説：全学総括責任者に、例外措置の適用審査記録の台帳を維持・整備することを求める事項である。例外措置の適用を許可したとしても、それが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採用すること又は遵守事項を実施していないことに変わりはない。もしも、例外措置を適用していることにより重大な情報セキュリティの侵害が発生した場合には、同様の例外措置を適用している者に対して、情報セキュリティの侵害発生の予防について注意を喚起したり、例外措置適用の許可について見直しをしたりする等の対処を検討する必要がある。そのためには、例外措置を適用している者や情報システムの現状について、最新の状態のものを集中して把握する必要がある。

第三章　運用

第一節　情報セキュリティ対策の教育

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、利用者等にその内容が周知されず、利用者等がこれを遵守しない場合には、情報セキュリティ対策の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、情報セキュリティ対策の教育を通じて、情報セキュリティ関係規程に関する理解を深め、情報セキュリティ対策を適切に実践できるようにすることが必要である。これらのことを勘案し、本節では、情報セキュリティ対策の教育に関する対策基準として、全学実施責任者及び職場情報セキュリティ責任者による教育体制の整備に係る規程及び利用者等による教育の受講についての遵守事項を定める。

B2101-11　（情報セキュリティ対策の教育の実施）（政府機関統一管理基準の対応項番 1.2.2.1(1)）

第十一条　全学実施責任者は、情報セキュリティ関係規程について、部局総括責任者、部局技術

責任者、部局技術担当者及び利用者等（以下「教育啓発対象者」という。）に対し、その啓発をすること。

解説：全学実施責任者に情報セキュリティ対策の啓発の実施を求める事項である。

2　全学実施責任者は、情報セキュリティ関係規程について、教育啓発対象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。

解説：全学実施責任者に情報セキュリティ対策の教育のための資料を整備することを求める事項である。

教育の内容については、大学の実情に合わせて幅広い角度から検討し、教育啓発対象者が対策内容を十分に理解できるものとする必要がある。

そのためには、本学の情報セキュリティに係る網羅的な資料ではなく、受講する者が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。すなわち、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、受講する者が遵守する必要がない事項は極力含まないように配慮する必要がある。

なお、遵守すべき事項以外であっても、教育内容に含めることが望ましい情報セキュリティ対策の例として、違反の監視機能に係る説明が挙げられる。これは、当該機能の存在を周知することで、その違反についての抑止効果を期待できる場合があるためである。

3　全学実施責任者は、教育啓発対象者の役割に応じて毎年度最低１回、受講できるように、情報セキュリティ対策の教育に係る計画を企画及び立案するとともに、その実施体制を整備すること。

解説：情報セキュリティ対策の教育の最低限の受講回数等について定めた事項である。

なお、情報セキュリティ事案の発生等、情報セキュリティ環境の変化に応じて、適宜、教育を行うことが重要である。計画の作成に際しては、関係する教育計画を参照し、効率性に注意するとともに人材育成にも留意すること。

4　全学実施責任者は、教育啓発対象者の入学時、着任時又は異動時に、その役割に応じて新しく所属することとなる部局等で３か月以内に受講できるように、情報セキュリティ対策の教育を企画及び立案するとともに、その実施体制を整備すること。

解説：入学、着任、異動した教育啓発対象者に対して、早期に情報セキュリティ対策の教育を受講させることによって、当該教育啓発対象者の情報セキュリティ対策の適正な実施を求める事項である。

なお、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等、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。

5　全学実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備すること。

解説：情報セキュリティ対策の教育の受講状況について把握できる仕組みを整備することを求める事項である。

6　全学実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況について、職場情報セキュリティ責任者に通知すること。

解説：計画された教育の実施に向けて、情報セキュリティ対策の教育を受講していな

い教育啓発対象者を職場情報セキュリティ責任者に通知することを定めた事項である。

７　職場情報セキュリティ責任者は、教育啓発対象者に情報セキュリティ対策の教育を受講させること。

解説：職場情報セキュリティ責任者が、教育啓発対象者に情報セキュリティ対策の教育を受講させる責務について定めた事項である。
なお、例えば、受講時間を確保する等の教育啓発対象者が受講できるための環境を整備することも必要である。

８　職場情報セキュリティ責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告すること。教育啓発対象者が当該勧告に従わない場合には、全学実施責任者にその旨を報告すること。

解説：情報セキュリティ対策の教育を受講しない者への対策を定めた事項である。
なお、計画された教育を受講しない教育啓発対象者は、その遵守違反について責任を問われることになる。

９　全学実施責任者は、毎年度１回、全学総括責任者及び全学情報システム運用委員会に対して、教育啓発対象者の情報セキュリティ対策の教育の受講状況について報告すること。

解説：全学総括責任者及び全学情報システム運用委員会に情報セキュリティ対策の教育の受講状況を報告することを求める事項である。

１０　全学実施責任者は、情報セキュリティ関係規程について、教育啓発対象者に対する情報セキュリティ対策の訓練の必要性を検討し、必要と判断した場合には、その訓練の内容及び体制を整備すること。

解説：実際に情報セキュリティ対策のための模擬的な機会を設けることにより、情報セキュリティ関係規程に係る知識・技能等を習得するために実施する訓練の内容及び体制を整備することを求める事項である。
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。
訓練の内容については、大学の実情に合わせて幅広い角度から検討し、教育啓発対象者が対策内容を十分に理解できるものとする必要がある。
情報セキュリティ対策の訓練は、時間的にも財政的にも大きな負担となり得るため、大学によってはこの項を削除することもあり得る。

１１　全学情報システム運用委員会及び部局情報システム運用委員会は、利用者等からの情報セキュリティ対策に関する相談に対応すること。

解説：全学情報システム運用委員会があらゆる相談に直接応じるという訳ではない。
ヘルプデスクを設置するなど、相談に対応するための体制作りを行う。

B2101-12　（教育の実施）

第十二条　部局情報システム運用委員会は、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を実施すること。

２　部局技術責任者及び部局技術担当者は、利用者等に対して、講習計画の定める講習を実施す

ること。

B2101-13　（情報セキュリティ対策の教育の受講）（政府機関統一管理基準の対応項番 1.2.2.1(2)）

第十三条　教育啓発対象者は、毎年度最低１回、情報セキュリティ対策の教育に関する計画に従って、情報セキュリティ対策の教育を受講すること。

解説：教育啓発対象者が、情報セキュリティ対策の教育に関する計画に従って、これを受講することを求める事項である。

２　教育啓発対象者は、入学時、着任時又は異動時に新しく所属することとなる部局等で、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。

解説：入学、着任、異動した教育啓発対象者が、確実に情報セキュリティ対策の教育を受講するための事項である。

３　教育啓発対象者は、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場合には、その理由について、職場情報セキュリティ責任者を通じて、全学実施責任者に報告すること。

解説：情報セキュリティ対策の教育を受講できない理由についての報告をしないままで、計画された教育を受講しない場合には、教育啓発対象者は、その遵守違反について責任を問われることになる。

４　教育啓発対象者は、情報セキュリティ対策の訓練に関する規定が定められている場合には、当該規定に従って情報セキュリティ対策の訓練に参加すること。

解説：教育啓発対象者が、情報セキュリティ対策の訓練に関する規定に従って、これを受講することを求める事項である。

第二節　インシデント対応

解説：情報セキュリティに関するインシデント（障害・事故等を含む。以下「インシデント」という。）が発生又はそのおそれがある場合には、早急にその状況を検出又は確認し、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、その際には、インシデントの影響や範囲に関する責任者への報告及び学内外の関係部門との情報共有により、インシデントの発生現場の混乱や誤った指示の発生等を最小限に抑えるとともに、被害の拡大防止策や再発防止策を講ずることが重要である。

これらのことを勘案し、本節では、インシデントの発生時に関する対策基準として、インシデントの発生に備えた事前準備、発生時における報告と対処の流れ、原因調査と再発防止策についての遵守事項を定める。

B2101-14　（インシデントの発生に備えた事前準備）（政府機関統一管理基準の対応項番 1.2.2.2(1)）

第十四条　全学総括責任者は、情報セキュリティに関するインシデント（障害・事故等を含む。以下「インシデント」という。）の発生に対応するために以下の役割及び機能を有する体制を整備すること。

一　インシデントに対応する責任者の決定

二　インシデントの発生の報告
三　インシデントの発生報告の受付
四　関係する部門へのインシデントの発生に関する速やかな連絡
五　応急措置の実施（被害の拡大防止）
六　インシデントからの復旧
七　原因調査の実施
八　再発防止策の策定及び実施
九　再発防止策の実施の確認

解説：全学総括責任者にインシデントに対する体制の整備を求める事項である。本遵守事項が効果的に機能するように他の規程との整合性に配意することも必要である。

インシデントに対する体制を整備するに当たっては、複数の部門で機能を分担することも考えられる。

「インシデントに対応する責任者」とは、インシデントが発生した場合の対応に係る責任者であり、その役割としては、インシデントに関する全般的な対応が求められる。また、全学総括責任者が自らインシデントへの対応に当たる場合は、その指揮監督の下で必要な対応を行うこととなる。

インシデントに対応する責任者は、情報セキュリティ対策に関する事務を総括する部門の責任者がその役割を担うことが考えられるが、全学実施責任者又は部局総括責任者がその役割を担うことも考えられる。その場合は、インシデントに関係する部門及び情報セキュリティ対策に関する事務を総括する部門との間で速やかな連絡ができる体制にすることが望ましい。

「関係する部門へのインシデントの発生に関する速やかな連絡」には、学内だけでなく、学外の関係部門への連絡も含まれる。なお、インシデントの発生時に、学外の関係部門へ速やかに連絡するためには、学外の関係部門と日常的な情報共有等の連携を図る必要がある。その場合、インシデントの発生時の連絡と日常的な連携を複数の部門で分担することも考えられる。ただし、機能を分担する場合は、互いの部門間で、インシデントに関する情報や日常的な連携で得られた情報を共有する必要がある。

なお、情報セキュリティに関するインシデントとは、機密性、完全性及び可用性が侵害されるものを対象としており、可用性等に影響を及ぼさない程度の故障等は対象としていない。

また、「インシデント」とは、JIS Q 27002:2006（ISO/IEC 17799:2005）及びISO/IEC 27035:2010 における情報セキュリティインシデントと同意である。

2　全学実施責任者は、インシデントについて報告手順を整備し、当該報告手段を全ての利用者等に周知すること。

解説：報告手順として、インシデントの発生を知った利用者等から報告を受け、インシデントに対応する責任者が、全学総括責任者に報告するまでの具体的な手順や決定されたインシデントに対応する責任者に対し、確実に報告ができる連絡手段等について明記する必要がある。

また、報告手順の中には、例えば、全学総括責任者にインシデントの報告を集約するための窓口を設けることが考えられる。窓口についての周知は、情報セキュリティ対策の教育の中で行うとともに、窓口の連絡先を教室、研究室、事務室内に掲示する等して、緊急時に利用者等がすぐに参照できるようにする必要がある。なお、情報システムが利用不能となる状況も想定して、複数の連絡手段の導入を検討すること。

窓口は、情報セキュリティ対策に関する事務を総括する部門に設置することが考えられるが、別の部門に窓口を設ける場合は、当該部門からインシデントに関係する部門への連絡や情報セキュリティ対策に関する事務を総括する部門への報告が速やかに実施される体制にすることが望ましい。

3　全学実施責任者は、インシデントが発生した際の学内及び学外との情報共有を含む対処手順を整備すること。

解説：対処手順としてインシデントの発生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措置の承認手続を設けることもあわ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。

対処手順は、より具体的に整備することが重要である。例えば、対処手順において、インシデントの発生日及び内容、インシデントへの対処の内容及び対処者等を利用者等が記録すべきこと並びに学内外の関係部門へのインシデントの情報共有を行うまでの目標時間を定めること等も考えられる。

4　全学実施責任者は、インシデントに備え、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。

解説：全学実施責任者は、通常全ての部局技術責任者及び部局技術担当者の連絡網を整備することが求められるが、インシデントが発生した場合に速やかに対応するため、「緊急」連絡網を加えて整備することを定める事項である。

緊急連絡網には、通常の連絡網とは異なり、該当する利用者等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、この場合、それぞれの連絡網の取扱いが異なることに注意する必要がある。

なお、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、大規模な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。

5　全学実施責任者は、インシデントへの対処の訓練の必要性を検討し、必要と判断した場合には、その訓練の内容及び体制を整備すること。

解説：実際にインシデントへの対処を模擬的に行うことにより、対応力を強化す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。

訓練には、情報システム部門だけでなく、インシデントの報告の窓口となる部門や情報セキュリティ対策に関する事務を総括する部門も参加することが望ましい。この場合、インシデントの報告の窓口となる部門や情報セキュリティ対策に関する事務を総括する部門では、インシデントへの専門的な対処を行う必要があるため、必要となる知識もより高度になる。そのため、訓練の一部とし

て、インシデントの対処に関する教育を受講したり、外部から情報セキュリティに関する情報を適宜収集したりする必要がある。
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。

6　利用者等は、インシデントへの対処の訓練に関する規定が定められている場合には、当該規定に従って、インシデントへの対処の訓練に参加すること。

解説：利用者等が、インシデントへの対処の訓練に関する規定に従って、これに参加することを求める事項である。

7　全学実施責任者は、インシデントについて学外から報告を受けるための窓口を設置し、その窓口への連絡手段を学外に公表すること。

解説：本学における情報セキュリティ対策の不備について外部の者が発見したり、本学において管理する電子計算機がサービス不能攻撃を外部に行った場合等、本学を取り巻く外部に対して、関連業務に支障を生じさせたり、情報セキュリティ上の脅威を与えたりした際に、その連絡を外部から受ける体制についても整備し、連絡先を学外に公表することを求める事項である。
なお、IP アドレスやドメイン名（および AS 番号）に関する Whois 情報がここでいう「窓口」とみなされ、学外からの連絡に利用されることも多い。Whois では、技術連絡担当者や登録担当者の氏名、所属組織名、電子メールアドレス、電話番号等も公開されるため、Whois 情報についても適切に管理することが必要である。

B2101-15　（インシデントの発生時における報告と対処の流れ）（政府機関統一管理基準の対応項番 1.2.2.2(2)）

第十五条　利用者等は、インシデントの発生を知った場合には、それに関係する者に連絡するとともに、全学実施責任者が定めた報告手順により、インシデントに対応する責任者、及びインシデントに対応する責任者を通じて全学総括責任者にその旨を報告すること。ただし、緊急やむを得ない事情により、インシデントに対応する責任者に報告することができない場合は、定められた報告手順に従って、全学総括責任者に報告すること。

解説：インシデントが発生した場合に、利用者等から速やかに関係者に連絡し、連絡を受けた者が当該インシデントへの対処を開始すること、及びインシデントが発生したことについて利用者等からインシデントに対応する責任者に報告され、インシデントに対応する責任者が速やかに全学総括責任者に報告することにより、全学総括責任者が状況を把握し、適切に対処することができるようにすることを求める事項である。
なお、連絡又は報告については、その内容により必要に応じて定められた受理者よりも上位の者に対して行う場合も考えられる。
また、インシデントに対応する責任者に報告することができない場合は、他の手順により全学総括責任者に確実に報告される必要がある。

2　インシデントに対応する責任者は、被害の拡大防止等を図るための応急措置の実施及びイン

シデントからの復旧に係る指示又は勧告を行うこと。

解説：インシデントに対応する責任者に対し、報告を受けたインシデントに係る必要な措置を講ずることを求める事項である。

応急措置や復旧に当たっては、インシデントが発生している情報システムの停止又は隔離について、インシデントに対応する責任者の判断で指示又は勧告ができるようにする必要がある。

なお、インシデントに対応する責任者の役割を情報セキュリティ対策に関する事務を総括する部門の責任者が担う場合は、当該部門の責任者が応急措置及び復旧に関する具体的な指示又は勧告を行うこととなるが、全学実施責任者又は各部門の情報セキュリティ責任者が担う場合についても情報セキュリティ対策に関する事務を総括する部門が、具体的な指示又は勧告の取りまとめを支援する体制にすることが望ましい。

3　利用者等は、インシデントが発生した際の対処手順の有無を確認し、それを実施できる場合には、その手順に従うこと。

解説：利用者等の判断による被害拡大防止策が常に適切なものであるとは限らないため、インシデントへの対処手順に従うことを求める事項である。

4　利用者等は、インシデントが発生した場合であって、当該インシデントについて対処手順がないとき及びその有無を確認できないときは、その対処についての指示を受けるまで、インシデントによる被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。

解説：対処手順が想定していないインシデントが発生した場合、利用者等は対処の指示を受けるまでの間もインシデントの拡大防止に努めることを求める事項である。

5　全学総括責任者は、報告を受けたインシデントについて、定められた対処手順に従って、学内外の関係部門と情報共有を行うこと。

解説：インシデントが発生した場合に、学内外の関係部門と情報を共有することで、被害の拡大防止策及び再発防止策が講じられるようにすることを求める事項である。

B2101-16　（インシデントの原因調査と再発防止策）（政府機関統一管理基準の対応項番1.2.2.2(3)）

第十六条　部局総括責任者は、インシデントが発生した場合には、インシデントに対応する責任者が実施した内容も踏まえ、インシデントの原因を調査するとともに再発防止策を策定し、その結果を報告書として全学総括責任者に報告すること。

解説：部局総括責任者に対し、インシデントに対応する責任者が把握しているインシデントの状況や実施した応急措置・復旧等の内容も踏まえて、インシデントの原因を究明し、それに基づきインシデントの再発防止策の策定を求める事項である。

2　全学総括責任者は、部局総括責任者から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こと。

解説：インシデントの再発防止策を講ずることを、全学総括責任者に求める事項であ

る。

B2101-17　（インシデントの発生するおそれがある場合の対処）（政府機関統一管理基準の対応項番 1.2.2.2(4)）

第十七条　全学総括責任者、全学実施責任者、部局総括責任者又はインシデントに対応する責任者は、インシデントの発生するおそれがある場合においては、この章の各遵守事項に準じて、必要な措置を講ずること。

解説：攻撃予告等により、インシデント等の発生するおそれがある場合については、それぞれの役割の者が、この章の各遵守事項に準じて必要な措置を講ずることを求める事項である。

２　利用者等は、インシデントの発生するおそれがある場合においては、第十四条の規定による報告手順や対処手順等に基づき、適切な措置を講ずること。

解説：攻撃予告等により、インシデント等の発生するおそれがある場合において、利用者等は、「B2101 情報システム運用・管理規程」第 14 条（インシデントの発生に備えた事前準備）の規定に基づいて整備された報告手順や対処手順等に従い、適切な措置を講ずることを求める事項である。

第四章　評価

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は、それに係る全ての教職員等が、各自の役割を確実に行うことで実効性が担保されるものであることから、全ての教職員等自らが情報セキュリティ関係規程に準拠した運用を行っているか否かについて点検することが重要である。また、自己点検の結果に基づき、それぞれの当事者又はその管理者がその責任において、必要となる改善策を実施する必要がある。

これらのことを勘案し、本節では、自己点検に関する対策基準として、自己点検に関する年度計画の策定とその実施に関する準備、自己点検の実施、結果の評価及び自己点検に基づく改善についての遵守事項を定める。

B2101-18　（自己点検に関する年度計画の策定）（政府機関統一管理基準の対応項番 1.2.3.1(1)）

第十八条　全学実施責任者は、年度自己点検計画を策定し、全学総括責任者の承認を得ること。

解説：自己点検を実施するに当たり、その実施頻度、実施時期、確認及び評価の方法、実施項目の選択等に関する年度自己点検計画を策定することを求める事項である。

実施頻度については、自己点検は年に 2 度以上実施することが望ましいが、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等、様々な選択肢が考えられる。

実施時期については、例えば、当初は毎月 10 項目ずつ自己点検し、教職員等の意識が高まった後、半年に一度、全項目を実施するように変更する等、様々な選択肢が考えられる。

確認及び評価の方法については、例えば、単純に実施したことを確認するほか、遵守率を確認する等、数値評価により客観性を持った評価とすることが望ましく、様々な選択肢が考えられる。
実施項目の選択については、例えば、当初は全ての教職員等が容易に遵守できる項目のみを自己点検し、教職員等の意識が高まった後、遵守率が低いと想定される項目を実施するように変更する等、様々な選択肢が考えられる。
なお、教職員等自らが行う自己点検を原則とするが、システム的な仕組みを用いてパッチやパターンファイルの更新状況を把握したり、実際の文書を確認することによりその整備状況を把握する等、自己点検と同等以上の信頼性を有する方法が存在する場合には、代替方法としてそれを採用しても良い。

B2101-19　（自己点検の実施に関する準備）（政府機関統一管理基準の対応項番 1.2.3.1(2)）

第十九条　部局総括責任者は、教職員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：各教職員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、教職員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を求める事項である。

B2101-20　（自己点検の実施）（政府機関統一管理基準の対応項番 1.2.3.1(3)）

第二十条　部局総括責任者は、全学実施責任者が定める年度自己点検計画に基づき、教職員等に対して、自己点検の実施を指示すること。

解説：年度自己点検計画に基づき、部局総括責任者自らも含めた教職員等に対して、自己点検の実施に関し指示することを求める事項である。

２　教職員等は、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実施手順を用いて自己点検を実施すること。

解説：情報セキュリティに関わる教職員等に対して、自己点検を実施し、自らが実施すべき対策事項について、実施の有無を確認することを求める事項である。

B2101-21　（自己点検結果の評価）（政府機関統一管理基準の対応項番 1.2.3.1(4)）

第二十一条　部局総括責任者は、教職員等による自己点検が行われていることを確認し、その結果を評価すること。

解説：教職員等による自己点検の結果について、部局総括責任者が評価することを求める事項である。
なお、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、自己点検実施率や、情報セキュリティ関係規程遵守率、要改善対策数/対策実施数等の準拠率

の把握が挙げられる。

2　全学実施責任者は、部局総括責任者による自己点検が行われていることを確認し、その結果を評価すること。

解説：部局総括責任者による自己点検が適切に行われていることを、全学実施責任者が評価することを求める事項である。

3　全学実施責任者は、自己点検の結果を全学総括責任者へ報告すること。

解説：全学実施責任者は、自己点検の結果を全学総括責任者へ報告することを求める事項である。

B2101-22　（自己点検に基づく改善）（政府機関統一管理基準の対応項番 1.2.3.1(5)）

第二十二条　教職員等は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、部局総括責任者にその旨を報告すること。

解説：自己の権限の範囲で改善可能である問題点については、情報セキュリティに関わる全ての教職員等自らが自己改善することを求める事項である。

2　全学総括責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には部局総括責任者に改善を指示すること。

解説：自己点検の結果により明らかとなった問題点について、全学総括責任者が部局総括責任者に対して改善することを求める事項である。

第二節　情報セキュリティ対策の監査

解説：情報セキュリティの確保のためには、ポリシーが適切に策定され、かつ、情報セキュリティ関係規程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、その準拠性と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、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。

これらのことを勘案し、本節では、情報セキュリティ対策の監査に関する対策基準として、監査計画の策定とその実施に関する指示、個別の監査業務における監査実施計画の策定、監査の実施に係る準備、監査の実施及びその結果に対する対処についての遵守事項を定める。

B2101-23　（監査計画の策定）（政府機関統一管理基準の対応項番 1.2.3.2(1)）

第二十三条　情報セキュリティ監査責任者は、年度監査計画を策定し、全学総括責任者の承認を得ること。

解説：監査の基本的な方針として、年度監査計画を策定し、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、不正アクセス防止等）
・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、年度監査計画に盛り込むこと。

B2101-24　（監査の実施に関する指示）（政府機関統一管理基準の対応項番 1.2.3.2(2)）

第二十四条　全学総括責任者は、年度監査計画に従って、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こと。

解説：年度監査計画に従って監査を実施することを求める事項である。

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、年度監査計画で計画されたこと以外の監査の実施を指示すること。

解説：年度監査計画において実施する監査以外に、学内外における注目すべき事案の発生又は情報セキュリティ対策の実施内容について重大な変更が生じた場合に、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。

B2101-25　（個別の監査業務における監査実施計画の策定）（政府機関統一管理基準の対応項番 1.2.3.2(3)）

第二十五条　情報セキュリティ監査責任者は、年度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こと。

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

・監査の実施場所

・監査実施者及び担当職務の割当て

・準拠性監査（情報セキュリティ関係規程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情報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

なお、被監査部門に対し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に関して、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。

また、「B2101 情報システム運用・管理規程」においては、監査業務に対して監査を別途実施することを必須とはしてない。しかし、監査実施者が監査過程で被監査者を監査すること以外のことを実施した場合には、その実施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、監査実施計画を策定する際は、監査実施者が実施することが情報セキ

ュリティ対策の向上になり得ることや、何らかの作業を効率的に行えるとしても、それを安易に監査実施計画の中に取り込むべきではない。

B2101-26　（監査の実施に係る準備）（政府機関統一管理基準の対応項番 1.2.3.2(4)）

第二十六条　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。

解説：情報セキュリティ監査責任者に、本学において監査業務を実施するに当たり、必要となる者を情報セキュリティ監査実施者に指名することを求める事項である。

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は、当該情報システムの構築をした者は、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、学外の者に監査の一部を請け負わせる必要性を検討し、必要と判断した場合には、学外の者に監査の一部を請け負わせること。

解説：情報セキュリティ監査責任者に、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、学内の情報システム部門に加えて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等を考慮することが望ましい。

B2101-27　（監査の実施）（政府機関統一管理基準の対応項番 1.2.3.2(5)）

第二十七条　情報セキュリティ監査実施者は、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こと。

解説:情報セキュリティ監査実施者が適切に監査を実施することを求める事項である。

2　情報セキュリティ監査実施者は、情報セキュリティ関係規程がポリシーに準拠していることを確認すること。

解説：情報セキュリティ関係規程がポリシーに準拠して設計されていることの確認を求める事項である。

3　情報セキュリティ監査実施者は、実施手順が情報セキュリティ関係規程に準拠していることを確認すること。

解説：被監査部門における実施手順が情報セキュリティ関係規程に準拠して設計されていることの確認を求める事項である。

4　情報セキュリティ監査実施者は、自己点検の適正性の確認を行う等により、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を確認すること。

解説：被監査部門における実際の運用が、本学の情報セキュリティ関係規程に準拠して実施されていること（運用の準拠性）の確認を求める事項である。運用の準拠性の確認は、自己点検の適正性の確認によることが実効性の高い方法であると考えられる。

監査に当たっては、自己点検結果に基づく担当者への質問、記録文書の査閲、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の妥当性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脆弱性検査、侵入検査等のその他の方法によっても確認することができる。

5　情報セキュリティ監査実施者は、監査調書を作成すること。

解説：監査報告書の根拠となる監査調書を適切に作成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綴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。

6　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こと。

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、情報セキュリティ関係規程がポリシーに準拠しているか、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。

B2101-28　（監査結果に対する対処）（政府機関統一管理基準の対応項番 1.2.3.2(6)）

第二十八条　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、指摘されたことに対する対処の実施を指示すること。

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処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、他の部門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こと。

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、対処計画を策定し、報告すること。

解説：監査報告書や監査調書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、対処計画の策定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処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、提示された対処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、既存の情報セキュリティ関係規程の妥当性を評価し、必要に応じてその見直しを指示すること。

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、課題とその改善に対する助言意見等の指摘を受けた場合には、既存の情報セキュリティ関係規程の見直しを検討することを求める事項である。

検討の結果、情報セキュリティ関係規程の見直しを行わない場合には、その理由について明確化すること。

B2101-29　（監査への協力）

第二十九条　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、情報セキュリティレベルは維持できなくなる。このため、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、作成、導入、運用、評価の各段階において、適時見直しを行う必要がある。

これらのことを勘案し、本章では、情報セキュリティ対策の見直しに関する対策基準について定める。

B2101-30　（情報セキュリティ対策の見直し）（政府機関統一管理基準の対応項番 1.2.4.1(1)）

第三十条　情報セキュリティ関係規程を整備した者は、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こと。

解説：情報セキュリティ関係規程を整備した者は、新たなセキュリティ脅威の出現、自己点検及び監査の評価結果等を踏まえつつ、情報セキュリティ対策に支障が生じないように見直しを行う時期を判断する必要がある。

情報セキュリティ関係規程を見直した者は、他部門へも影響があると思われる場合、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　利用者等は、情報セキュリティ関係規程に課題及び問題点が認められる場合には、情報セキュリティ関係規程を整備した者に相談すること。

解説：利用者等自らが整備したものではない情報セキュリティ関係規程について、課題及び問題点が認められる場合には、情報セキュリティ関係規程を整備した者に相談することを求める事項である。

3　情報セキュリティ関係規程を整備した者は、情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合は、必要な措置を講ずること。

解説：情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合に、その是非を検討し、必要な措置を講ずることを求める事項である。例えば、利用者等からの相談が妥当であると思料する場合に情報セキュリティ関係規程の見直しを行ったり、逆に利用者等の理解不足が原因であると思料する場合は、再教育の措置を講ずること等が考えられる。

第六章　その他

第一節　外部委託

解説：学外の者に情報処理業務を委託する場合（外部の設備を利用した役務提供も含む。）には、本学が委託先を直接管理することができないため、学内で行う場合と比べ、情報の機密性、完全性及び可用性が損なわれるリスクが増大する。

このリスクに対応するため、情報処理業務を外部委託する際は、委託先においても本学のポリシー並びにそれに基づく規程及び手順等と同等の対策を実施させるべく、委託先への要求事項を定める必要がある。

これらのことを勘案し、本節では、外部委託に関する対策基準を定める。具体的には、

・情報セキュリティ確保のための学内共通の仕組みの整備
・委託先に実施させる情報セキュリティ対策の明確化
・委託先の選定
・外部委託に係る契約
・外部委託の実施における手続
・外部委託終了時の手続

についての遵守事項を定めるものである。

B2101-31　（適用範囲）（政府機関統一管理基準の対応項番 1.2.5.1）

第三十一条　この章の規定は、本学による貸借、請負その他の契約に基づき提供される役務のうち、情報処理に係る業務であって、例えば次の各号に掲げる営業品目に該当するものに適用する。

一　ソフトウェア開発（プログラム作成、システム開発等）

二　情報処理（統計、集計、データエントリー、媒体変換等）

三　賃貸借
四　調査・研究（調査、研究、検査等）

B2101-32　（情報セキュリティ確保のための学内共通の仕組みの整備）（政府機関統一管理基準の対応項番 1.2.5.1(1)）

第三十二条　全学実施責任者は、外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準を整備すること。

解説：外部委託の対象としてよい範囲としてはいけない範囲を判断する基準を本学として整備することを定めた事項である。学内の情報システム及び関連する業務に関し、網羅性を確保しつつ統一的な基準で当該範囲を設定することが重要である。

また、データの所在については、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切とな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。例えば、「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」及び「個人情報の保護に関する法律」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判断すること等が考えられる。

２　全学実施責任者は、委託先の選定基準及び選定手続を整備すること。

解説：委託先の選定において整備すべき手続や基準に関して定めた事項である。

全学実施責任者は、委託先の選定基準の整備に当たっては、当該委託先が、事業の継続性を有し存続可能であり、情報セキュリティ関係規程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、例えば、委託先が情報セキュリティ関係規程の該当項目を遵守し得る者であること、ポリシー並びにそれに基づく規程及び手順等と同等の情報セキュリティ管理体制を整備すること、ポリシー並びにそれに基づく規程及び手順等と同等の情報セキュリティ対策の教育を実施す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 等に基づく認証制度の活用や、国際規格を踏まえ、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（http://www.jisc.go.jp/mss/other.html）」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が望ましい。

なお、本基準は、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、外部委託の実施に反映することが必要である。

B2101-33　（委託先に実施させる情報セキュリティ対策の明確化）（政府機関統一管理基準の対応項番 1.2.5.1(2)）

第三十三条　部局技術責任者又は職場情報セキュリティ責任者は、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容を定め、委託先候補に事前に周知すること。

解説：委託先に実施させる情報セキュリティ対策の内容を具体的に定めることを求める事項である。

外部委託に係る業務において納入される成果物（特に情報システム）に関しては、委託先における情報セキュリティ対策が適切に実施されていることがその後の情報システム等の運用におけるセキュリティレベルの維持及び向上の前提となることから、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容を定め、周知しておくことが重要である。

なお、職場情報セキュリティ責任者が外部委託に係る業務について責任を負う場合には、例えば、部局において保有する情報の加工・処理を外部委託により行う場合がある。

2　部局技術責任者又は職場情報セキュリティ責任者は、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処方法を整備し、委託先候補に事前に周知すること。

解説：委託先に請け負わせる業務における情報セキュリティの侵害発生時の対処方法を本学として整備することを定めた事項である。情報セキュリティの侵害の業務に対する影響度の大きさや機密性、完全性及び可用性の要求度に応じて、対処の緊急性等を考慮することが重要である。

3　部局技術責任者又は職場情報セキュリティ責任者は、委託先におけ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及び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を整備し、委託先候補に事前に周知すること。

解説：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ること、及び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ことにかんがみ、これらのための方法の整備を求める事項である。

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。

周知す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で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、本学及び委託先が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こと。

B2101-34　（委託先の選定）（政府機関統一管理基準の対応項番 1.2.5.1(3)）

第三十四条　部局技術責任者又は職場情報セキュリティ責任者は、選定基準及び選定手続に基づき、委託先を選定すること。

解説：委託先の選定時における手続等の遵守に関して定めた事項である。

B2101-35　（外部委託に係る契約）（政府機関統一管理基準の対応項番 1.2.5.1(4)）

第三十五条　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、委託先に請け負わせる業務における情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む。）、情報セキュリティの侵害発生時の対処方法、情報セキュリティ対策の履行状況の確認方法及び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を含む外部委託に伴う契約を取り交わすこと。また、必要に応じて、以下の事項を当該契約に含めること。

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

解説：情報セキュリティの観点から、外部委託に係る契約に含めるべき事項を定めた事項である。

機密保持に関する条項は、要機密情報が委託範囲に含まれるか否かにかかわらず、請け負った業務及びその業務の遂行により知り得る情報を守るべきであることから、これを記載する必要がある。

情報セキュリティ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を契約に含める。

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、事故発生時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。

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、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書等を提出させること。また、必要に応じて、以下の事項を当該確認書等に含めさせること。

一　当該委託業務に携わる者の特定

二　遵守すべき情報セキュリティ対策を実現するために、当該者が実施する具体的な取組内容

解説：外部委託に係る契約者双方の責任の明確化と合意形成に基づく委託先からの確認書等の提出に関し定めた事項である。

必要に応じて、当該委託業務に携わる委託先の者の特定や、当該者が実施する取組内容を、委託先に確認することが重要になる。

特に、情報システムの構築及びソフトウェア開発等の外部委託の場合には、成果物における情報セキュリティ対策の実施が、その作成プロセスと不可分であることが想定されるため、遂行される業務全体の責任者を報告させることが重要である。

3　部局技術責任者又は職場情報セキュリティ責任者は、外部委託契約の継続に関しては、選定基準及び選定手続に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。

解説：外部委託契約の継続、特に随意契約に関し、都度審査することを定めた事項である。

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こと。

4　部局技術責任者又は職場情報セキュリティ責任者は、委託先の提供する役務（情報セキュリティ基本方針、実施手順、管理策の維持及び改善を含む。）の変更に関しては、選定基準及び選定手続に基づき、その是非を審査すること。

解説：委託契約の実施中の契約変更に関して定めた事項である。変更がある場合にはその是非を審査し、必要に応じて、契約変更をする等の対応が必要である。

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こと。

5　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措置を委託先に担保させること。

解説：委託先がその委託内容を再委託することは、セキュリティレベルの低下を招くことが懸念されることから原則として避けるべきである。一方、委託先がその委託内容を再委託する場合には、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措置を委託先に担保させることを定めた事項である。

情報セキュリティを十分に確保するためには、委託先自体が業務を実施する場合に求めるべき水準と同一水準の情報セキュリティ対策を再委託先においても確保させる必要がある。

B2101-36　（外部委託の実施における手続）（政府機関統一管理基準の対応項番 1.2.5.1(5)）

第三十六条　教職員等は、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、以下の措置を講ずること。

一　委託先に情報を提供する場合は、安全な受渡し方法によりこれを実施し、提供した記録を取得すること。

二　外部委託の業務終了等により提供した情報が委託先において不要になった場合には、これを確実に返却させ、又は廃棄させ、若しくは抹消（全ての情報を復元が困難な状態にすることをいう。以下同じ。）させること。

解説：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を必要最小限に

止め、また、提供に伴う要保護情報の漏えいや滅失等を防止するための措置の実施を求める事項である。

委託先への情報の提供における遵守事項は、「B2101 情報システム運用・管理規程」第 7 章第 4 節（情報の移送）及び第 7 章第 5 節（情報の提供）の定めに準ずるが、例えば機密性 3 情報を提供する場合には、当該外部委託について責任を負う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、また、機密性 2 情報を提供する場合には、これらの者のいずれかに届け出ることが必要となる。委託先の選定基準や情報セキュリティの侵害時の対処方法を整備した上で、当事者間の情報の授受において上記の措置に従うことにより情報セキュリティを確保することが重要である。

2　部局技術責任者又は職場情報セキュリティ責任者は、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、取り交わした契約の対処方法に従い、委託先に必要な措置を講じさせること。

解説：請け負わせた業務の実施中に情報セキュリティの侵害が発生した場合に、契約に記載した対処方法に従い、委託先に必要な措置を講じさせること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事項である。

3　部局技術責任者又は職場情報セキュリティ責任者は、取り交わした契約の対処方法に従い、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。

解説：委託先に請け負わせた業務の実施中に、契約に記載した方法に従い、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事項である。

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、契約に記載し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。

B2101-37　（外部委託終了時の手続）（政府機関統一管理基準の対応項番 1.2.5.1(6)）

第三十七条　部局技術責任者又は職場情報セキュリティ責任者は、外部委託の終了時に、委託先に請け負わせた業務において行われた情報セキュリティ対策を確認し、その結果を納品検査における確認の判断に加えること。

解説：外部委託に係る業務の終了時における情報セキュリティ対策の確認に関して定めた事項である。

委託先に請け負わせた業務において情報セキュリティ対策が契約に従い適切に実施されていることが、その後の運用におけるセキュリティレベルの維持及び向上の前提となる。このため、部局技術責任者又は職場情報セキュリティ責任者は、委託先において実施された情報セキュリティ対策を確認し、その結果を納品検査の判断に加えることが重要である。

第二節　業務継続計画及び情報システム運用継続計画との整合的運用の確保

解説：大学においては、教育研究事務の継続に重大な支障を来し、あるいは大学関係

者やその他の者の安全と利益に重大な脅威となる可能性が想定される事態を特定し、当該事態に対応する計画を業務継続計画として策定することが想定される。また、必要な情報システムについて、運用を継続するために必要な計画（以下「情報システム運用継続計画」という。）を策定することが求められる。他方、業務継続計画及び情報システム運用継続計画の対象とする事態は、多くの場合に情報セキュリティを損なうものともなり、本学の情報セキュリティ関係規程に基づく対策も講じられることとなる。この場合、業務継続計画及び情報システム運用継続計画の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要である。

これらのことを勘案し、本節では、業務継続計画及び情報システム運用継続計画と情報セキュリティ対策との間の整合性の確保並びに情報セキュリティ関係規程との間の不整合の報告に関する対策基準を定める。

B2101-38　（業務継続計画及び情報システム運用継続計画と情報セキュリティ対策との間の整合性の確保）（政府機関統一管理基準の対応項番 1.2.5.2(1)）

第三十八条　全学情報システム運用委員会は、本学において業務継続計画、情報システム運用継続計画又は情報セキュリティ関係規程を整備する場合には、業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間の整合性の確保のための検討を行うこと。

解説：業務継続計画、情報システム運用継続計画及び情報セキュリティ関係規程は、それぞれの目的を達成するために、特定の事態に対して異なる対応が定められることも考えられる。当該事態の例として、情報システムの稼動を損なう地震及び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、並びに情報機器の故障等が想定される。これらの事態に対して業務継続計画、情報システム運用継続計画及び情報セキュリティ関係規程のそれぞれで定める対策に矛盾があると、それぞれの遵守を求められる学内組織及び利用者等は、日常及び事態発生時に一貫性のある適切な行動をとることができない。このため、業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間で整合性を確保するよう検討を行うことが必要である。

「B1001 情報システム運用基本規程」第 5 条第 2 項で全学情報システム運用委員会は情報セキュリティ関係規程の策定を求められているが、その策定及び見直しの際に、本学が業務継続計画及び情報システム運用継続計画で定め、又は定めることが予定されている要求事項を全学情報システム運用委員会が把握した上で、業務継続計画及び情報システム運用継続計画の整備を担当する者と協議しそれぞれが定める内容を調整する必要がある。また、業務継続計画及び情報システム運用継続計画に変更が生じ、又は生ずることが予定されている場合には、その変更が情報セキュリティ関係規程に影響するかどうかを確認し、必要があれば、情報セキュリティ関係規程の改訂を行う等して、業務継続計画及び情報システム運用継続計画との整合性の確保に努めなければならない。

2　全学実施責任者、部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者は、本学において業務継続計画及び情報システム運用継続計画を整備する場合には、全ての情報シス

テムについて、当該業務継続計画及び情報システム運用継続計画との関係の有無を検討すること。

解説：業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間の整合性を確保する前提として、本学の情報システムのうち、業務継続計画及び情報システム運用継続計画と関係のある情報システムを特定することを求める事項である。

3　全学実施責任者、部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者は、本学において業務継続計画及び情報システム運用継続計画を整備する場合には、当該業務継続計画及び情報システム運用継続計画と関係があると認めた情報システムについて、業務継続計画及び情報システム運用継続計画との整合性を考慮し、必要な措置を講ずること。

一　通常時において業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との整合的運用が可能となるよう必要な措置を講ずること。

解説：例えば、事態発生時には、業務の継続以外の対応として、本学の施設の一部を帰宅困難者や救命等が必要な外来者の退避場所として使用する場合等も考えられる。このような場合を想定した対策を講じていないと、不特定者の出入りによって通常時と比べてセキュリティレベルの確保に支障を来すおそれがある。このため、セキュリティ確保の面で配慮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、施設全体の入館管理だけでなく、教室、研究室、事務室等の各室や各教職員等の卓上の情報セキュリティ対策を含め、通常時から不特定者の出入りを想定した対策を講ずる必要がある。

また、事態発生時にも利用することを想定している情報システムについては、事態発生時に確実に利用できるように、通常時において耐震対策等の物理的な対策を講ずる必要がある。

二　事態発生時において業務継続計画、情報システム運用継続計画及び情報セキュリティ関係規程との整合的運用が可能となるよう実施手順の整備等の必要な措置を講ずること。

解説：事態発生への対応として、業務継続計画、情報システム運用継続計画及び情報セキュリティ関係規程のそれぞれにおいて事態発生時における情報システムの稼動水準及び復旧までの所要時間の目標を定め、その達成を図る様々な対応を実施手順において具体的に定めることとなるため、相互の整合性を確保するための実施手順の整備が必要となる。この場合、対策として、例えば、施設の耐災害性確保、施設・情報システムの地理的分散及び冗長化、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用等がある。また、事態発生時の対応体制及び担当者の指名も整備対象となり得る。

また、事態発生時には、情報システムの主体認証情報（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。しかしながら、個人が管理しているパスワードの共用（共用識別コードに係るものを除く。）は、そもそも情報セキュリティ対策の観点では厳に禁止されるべきものである上、事態発生時には、パスワードを聞き出す者についての本人確認等が不十分となることも想定される。

このような事態発生時の手順については、業務継続計画及び情報システム運用継続計画で安易に定めるのではなく、事態発生時においても必要な情報セキュリティを確保するために、情報セキュリティ関係規程において事態発生時の実施手順として整備する必要がある。

手順の一例としては、起動のためのパスワードを通常時には使用者だけが主として管理するような端末の管理者権限アカウントについては、本人が設定するアカウントのほかに、事態発生時用のアカウントをあらかじめ設定しておく方法が考えられる。この方法を用いる場合は、まず、その事態発生時用のアカウントのパスワードを人が記憶困難な文字列で設定し、設定内容を記載した紙面を施錠された安全な保管場所で保管しておく。そして、事態発生時には、その紙面を参照し事態発生時用のアカウントで起動する。このような手順を採用することで、パスワードの聞き出しや事態発生時以外の共用を回避することができる。また、設定内容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の確認が可能となる。なお、このような手順の方が、事態発生時に本人に連絡して聞き出すよりも、迅速に対応ができるものと思われる。

B2101-39　（業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間の不整合の報告）（政府機関統一管理基準の対応項番 1.2.5.2(2)）

第三十九条　利用者等は、本学において業務継続計画及び情報システム運用継続計画を整備する場合であって、業務継続計画、情報システム運用継続計画及び情報セキュリティ関係規程が定める要求事項との違い等により、実施の是非の判断が困難なときは、関係者に連絡するとともに、全学実施責任者が整備したインシデントが発生した際の報告手順により、部局総括責任者にその旨を報告して、指示を得ること。

解説：本来、業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程が定める要求事項との間の整合性については、前条の遵守事項を適正に実施することで担保されるものである。しかしながら、情報セキュリティ関係規程との間では、業務継続計画及び情報システム運用継続計画の対象となる状況においては、事前に想定していなかった様々な不整合が発生すると考えられる。業務継続計画の重要性を考慮すると、万が一、不整合について、全学情報システム運用委員会等が事前に想定できなかった場合にも、それを迅速に改善できるようにしておくべきである。

第三節　情報取扱区域

解説：悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる設置環境にある場合においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改ざん等が行われるおそれがある。また、その他にも、設置環境に関する脅威としては、自然災害の発生による情報システムの損傷や情報の紛失等が発生するおそれもある。

このように施設全体や区域ごとに様々な脅威が考えられるため、それぞれの区域に応じた管理と想定される利用形態に応じた情報の取扱いを行う必要がある。これらのことを勘案し、本節では、情報取扱区域にクラスの区分を設け、クラスに応じた管理及び利用を行うための対策基準として、情報取扱区域のクラス、管理及び利用制限の決定、情報取扱区域の管理並びに情報取扱区域における利用制限についての遵守事項を定める。

B2101-40　（情報取扱区域のクラス、管理及び利用制限の決定）（政府機関統一管理基準の対応項番 1.2.5.3(1)）

第四十条　全学実施責任者は、情報取扱区域にクラスの区分を定め、クラスに応じた管理対策及び利用制限対策を決定すること。なお、決定する内容は、「B2152 情報システムの構成要素に関する技術規程」第一条から第九条まで（別表 1 及び別表 2 を含む。）に定める。

解説：情報取扱区域にクラスの区分を設け、各クラスの利用用途に応じたセキュリティの確保を求めるための事項である。

２　部局総括責任者は、要管理対策区域については、当該区域を管理又は利用する利用者等がクラスについて認識できる措置を講ずること。

解説：決定された情報取扱区域のクラス区分について共通の認識となるように措置することで、クラスに応じた管理対策及び利用制限対策が講じられるようにするための事項である。

「認識できる措置」には、情報取扱区域のクラス区分の一覧表を定めその内容を周知する、区域ごとにクラスを掲示する、若しくは当該区域で情報を取り扱う際に必要な利用制限対策を掲示又は周知する等が考えられる。

なお、関係者限りで管理及び利用する区域については、関係者のみにクラスを周知することでも構わない。

３　区域情報セキュリティ責任者は、個別の管理対策及び利用制限対策を決定する必要性の有無を検討し、必要と認めた場合は、当該対策を決定し、全学実施責任者に報告すること。

解説：決定したクラスの区域において、必要な対策が不足していると認められる区域、又は定められたクラスとは別の区分で対策を講ずる必要がある区域があるときは、求める情報セキュリティ水準を確保又は向上させるために、定められたクラス別管理及び利用制限にかかわらず、当該区域ごとに個別に管理対策及び利用制限対策を決定することを求める事項である。

B2101-41　（情報取扱区域の管理）（政府機関統一管理基準の対応項番 1.2.5.3(2)）

第四十一条　区域情報セキュリティ責任者は、要管理対策区域を管理する場合には、全学実施責任者が定めた当該区域のクラスを確認し、「B2152 情報システムの構成要素に関する技術規程」第一条から第九条まで（別表 1 を含む。）に定める管理対策を講ずること。また、個別の管理対策を決定している場合には、同様に対策を講ずること。

解説：区域情報セキュリティ責任者が要管理対策区域を管理する場合に、当該区域で求められる管理対策を講ずることを求める事項である。

B2101-42　（情報取扱区域における利用制限）（政府機関統一管理基準の対応項番 1.2.5.3(3)）

第四十二条　区域情報セキュリティ責任者は、全学実施責任者が定めた情報取扱区域のクラスを確認し、「B2152 情報システムの構成要素に関する技術規程」第一条から第九条まで（別表 2 を含む。）に定める利用制限対策を講ずること。なお、個別に利用制限対策を決定している場合には、同様に講ずること。

解説：区域情報セキュリティ責任者が当該区域で求められる利用制限対策を講ずることを求める事項である。

2　教職員等は、情報を取り扱う場合には、全学実施責任者が定めた情報取扱区域のクラスを確認し、「B2152 情報システムの構成要素に関する技術規程」第一条から第九条まで（別表 2 を含む。）に定める利用制限対策に従って利用すること。なお、個別の利用制限対策を決定している場合には、同様に従うこと。

解説：教職員等が要管理対策区域を利用する場合に、当該区域で求められる利用制限対策に従って利用することを求める事項である。

なお、教職員等が学外の者を立ち入らせる際に、当該区域で求められる利用制限対策に従って利用させることも含まれる。

第七章　情報の取扱い

第一節　情報の作成と入手

解説：大学においては、その教育研究事務の遂行のために複数の者が共通の情報を利用する場合がある。この際、利用者により当該情報の取扱いに関する認識が異なると、当該情報に応じた適切な情報セキュリティ対策が採られないおそれがあるため、情報を作成し、又は入手した段階で、全ての利用者において認識を合わせるための措置が必要となる。

これらのことを勘案し、本節では、情報の作成及び入手に関する対策基準として、教育研究事務以外の情報の作成又は入手の禁止に係る努力義務、情報の作成又は入手時における格付と取扱制限の決定、格付と取扱制限の明示等、格付と取扱制限の加工時における継承についての遵守事項を定める。

B2101-43　（教育研究事務以外の情報の作成又は入手）（政府機関統一管理基準の対応項番 1.3.1.1(1)）

第四十三条　教職員等は、教育研究事務の遂行以外の目的で、情報を作成し、又は入手しないよう努めること。

解説：教育研究事務の遂行以外の目的で、情報を作成し、又は入手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作成又は入手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作成又は入手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。

B2101-44　（情報の作成又は入手時における格付と取扱制限の決定）（政府機関統一管理基準の対応項番 1.3.1.1(2)）

第四十四条　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すること。

解説：作成又は入手した情報について、以降、適切な情報セキュリティ対策が実施されるように、機密性、完全性及び可用性の格付及び取扱制限を決定することを求める事項である。

情報の格付が適切に決定されていなかった、また、明示等されていなかったことを一因としてインシデントが発生した場合には、インシデントの直接の原因となった人物のほか、情報の格付及び明示等を適切に行わなかった情報の作成者にも責任が及ぶことがある。その観点からも、教職員等が、情報の格付及び取扱制限とその明示等を確実に行うことは重要である。

なお、格付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十分注意しなければならない。格付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って事務が繁雑になり、情報の利便性や有用性が損なわれたり、事務の繁雑さを教職員等が煩わしく思うことで適切な管理が行われなくなったりするおそれがある。

特に、格付及び取扱制限を必要以上に高くしないように配慮することも、情報の利用を円滑に行うために注意が必要である。

例えば、本来要機密情報とする情報を要機密情報に決定しないことは不適切であるが、逆に、本来要機密情報ではない情報（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決定することも不適切であることに注意すること。

また、取扱制限については必要性の有無を検討し、その結果指定しないという決定を行っても差し支えない。

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、格付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、決定した格付及び取扱制限に基づき、その指定を行うこと。

なお、本遵守事項に基づき、情報セキュリティ確保の観点から、取扱制限として保存期間を指定する場合も考えられる。

２　教職員等は、元の情報の修正、追加、削除のいずれかにより、他者が決定した情報の格付及び取扱制限を変更する必要があると思料する場合には、前項に従って再決定すること。

解説：元の情報の修正、追加、削除のいずれかにより、格付又は取扱制限を変更する必要が生じた場合には、格付及び取扱制限の再決定を行う必要がある。

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
なお、情報の格付及び取扱制限は、「B2104 情報格付け基準」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。情報の格付及び取扱制限の変更には、大別して再決定と見直しがある。
再決定した場合には、再決定後の新たな格付等の決定者は再決定した者となる。
見直しについては、「B2101 情報システム運用・管理規程」第 50 条（格付及び取扱制限の見直し）を参照のこと。

B2101-45　（格付と取扱制限の明示等）（政府機関統一管理基準の対応項番 1.3.1.1(3)）
第四十五条　教職員等は、情報の格付及び取扱制限を決定（再決定を含む。以下同じ。）した際に、当該情報の参照が許されている者が認識できる方法を用いて明示等すること。

解説：作成者又は入手者によって格付及び取扱制限が決定された情報に対して、以降、他者が当該情報を利用する際に必要とされる情報セキュリティ対策の内容を示すため、情報の格付及び取扱制限の明示等を行うことを求める事項である。「明示等」とは、情報を取り扱う全ての者が当該情報の格付及び取扱制限について共通の認識となるように措置することをいい、情報ごとの格付の区分及び取扱制限の種類を当該情報に記載することによる明示を原則とする。なお、格付の区分及び取扱制限の種類を記載していたとしても、当該ファイルを参照する者が、その内容を参照する際に格付の区分及び取扱制限の種類を特段の手順なく視認することができない状態（例えば、文書ファイルのプロパティ設定に格付の区分を記載することや、文章閲覧時に画面表示はされず印刷しかされないヘッダ部分に記載すること等）については、記載しても明示に当たらない。
格付及び取扱制限の明示等は、当該情報が、電磁的ファイルとして取り扱われることが想定される場合にはファイル名自体又は情報内容の中に、外部電磁的記録媒体に保存して取り扱うことが想定される場合には外部電磁的記録媒体に、書面に印刷されることが想定される場合には書面のヘッダ部分等に、それぞれ記載する必要がある。
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等する場合には、手書きによる記入又はスタンプ等による押印が必要である。
なお、原則として各書面それぞれに明示等すべきであるが、取り扱う単位がフォルダ単位や冊子単位の時には、その単位ごとに明示等することも可能である。
なお、格付及び取扱制限の明示等とあわせて、情報の作成者又は入手者の氏名、所属、連絡先等を記載することも有益である。

明示等を行うに当たっては、格付の区分及び取扱制限の種類を記載することに

よる明示が原則であるが、以下のような場合に明示等を簡便化してもよい。
① 格付及び取扱制限の明示等を簡便化できる場合
特定の情報（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）の格付及び取扱制限を規定等により明記し、当該情報にアクセスする全ての者に当該規定を周知している場合は、格付の区分及び取扱制限の種類について記載することを省略することができる。
具体的な例としては、次のような場合が考えられる。
・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の区分及び取扱制限を規定等により明記し、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。
・取り扱う情報の格付が機密性１、完全性１及び可用性１の場合には、記載による明示を簡便化できることを規定等により周知している場合。
ただし、格付及び取扱制限の明示等を簡便化した場合には、以下の事項に注意する必要がある。

格付及び取扱制限の明示等を簡便化した場合の注意事項
① 格付及び取扱制限の決定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の種類が記載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者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の種類を記載した上で提供しなければならない。
② 取扱制限の明示等を簡便化した場合における取扱制限の追加・変更
例えば、簡便化に係る規定等により、特定の文書ファイルについて、取扱制限の種類の記載を省略している場合において、当該ファイルのうち一部のファイルについて取扱制限を追加するときは、追加する取扱制限の種類のみを記載すること。また、取扱制限を解除する場合は、当該解除する取扱制限を「送信可」「印刷可」等のように記載することが考えられる。
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。

B2101-46 （格付と取扱制限の加工時における継承）（政府機関統一管理基準の対応項番1.3.1.1(4)）

第四十六条 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又は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。

解説：作成の際に参照した情報又は入手した情報が既に機密性に係る格付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維持することを求める事項である。なお、完全性及び可用性については、引用した新たな情報において適切な格付及び取扱制限を決定すること。

第二節　情報の利用

解説：大学においては、その教育研究事務の遂行のために多くの情報を利用するが、利用者の認識不足等により情報を不適切に取り扱うと、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれがある。このリスクに対応するため、教育研究事務の遂行において、情報は、格付等に応じて定められた手続に従い、適切に利用しなければならない。

これらのことを勘案し、本節では、情報の利用に関する対策基準として、教育研究事務以外の利用の禁止に係る努力義務、格付及び取扱制限に従った情報の取扱い、格付及び取扱制限の複製時における継承、格付及び取扱制限の見直し、要保護情報の取扱いについての遵守事項を定める。

B2101-47　（教育研究事務以外の利用）（政府機関統一管理基準の対応項番 1.3.1.2(1)）

第四十七条　教職員等は、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。

解説：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。

B2101-48　（格付及び取扱制限に従った情報の取扱い）（政府機関統一管理基準の対応項番 1.3.1.2(2)）

第四十八条　教職員等は、利用する情報に明示等された格付に従って、当該情報を適切に取り扱うこと。格付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取り扱うこと。

解説：情報に明示等された格付及び取扱制限に従って、適切に取り扱うことを求める事項である。

B2101-49　（格付及び取扱制限の複製時における継承）（政府機関統一管理基準の対応項番 1.3.1.2(3)）

第四十九条　教職員等は、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こと。

解説：複製の際に元となる情報が既に機密性に係る格付又は取扱制限の明示等がされている場合には、元となる格付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維持することを求める事項である。なお、完全性及び可用性については、複製した新たな情報において適切な格付及び取扱制限を決定すること。

B2101-50　（格付及び取扱制限の見直し）（政府機関統一管理基準の対応項番 1.3.1.2(4)）

第五十条　教職員等は、情報を利用する場合に、元の格付又は取扱制限がその時点で不適切と考えるため、他者が決定した情報の格付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。）に相談すること。

解説：利用する元の情報への修正、追加、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同人の上司に相談し、その是非を検討することになる。

ただし、元の決定者等のいずれかによる再決定がない限り、当該情報の利用者がそれらの者に無断で、格付又は取扱制限を変更することは許されない。

見直しにより元の決定者等に相談することが必要となる例として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）

・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

・本学における文書管理規則等が、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

相談を受けた決定者等は、次項に基づいて所要の措置を講ずることになる。

２　教職員等は、自らが格付及び取扱制限の決定者等である情報に対して、見直しの必要があると認めた場合には、当該情報の格付又は取扱制限を再決定し、それを明示等すること。また、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すること。

解説：いずれの理由であっても、適切な格付又は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、適切な格付又は取扱制限に変更することを求める事項である。

また、同一の情報が異なる格付又は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、格付又は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。

当該情報を直接提供した相手やそれを参照したと思われる者を特定することが困難な場合には、わかる範囲で構わない。

B2101-51　（要保護情報の取扱い）（政府機関統一管理基準の対応項番 1.3.1.2(5)）

第五十一条　教職員等は、教育研究事務の遂行以外の目的で、要保護情報を要管理対策区域外に持ち出さないこと。

解説：情報の漏えい、改ざん、破損、紛失等を未然に防ぐため、教職員等が教育研究事務の遂行以外の目的で要保護情報を要管理対策区域外へ持ち出すことを禁止する事項である。
なお、これを徹底させる手段として、「持出禁止」の取扱制限の明示等が挙げられる。

2　教職員等は、要保護情報を放置しないこと。

解説：第三者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ーを起動するあるいはログオフして、画面に情報を表示しないこと、また、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。

3　教職員等は、機密性３情報を必要以上に複製しないこと。

解説：不必要な複製によって情報漏えいの危険性が高くなることを考慮し、必要以上に機密性３情報を複製しないことを求める事項である。
なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ）第 6 項では、「『極秘』の文書の複製は、絶対に行なわないこと。『秘』の文書は、指定者の承認をうけて複製することができること。」と定めている。
なお、これを徹底させる手段として、「複製禁止」の取扱制限の明示等が挙げられる。

4　教職員等は、要機密情報を必要以上に配付しないこと。

解説：情報漏えいを未然に防ぐため、要機密情報の配付は最小限にとどめることを求める事項である。
なお、これを徹底させる手段として、「配付禁止」の取扱制限の明示等が挙げられる。

5　教職員等は、情報を機密性３情報と決定した場合には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付を下げる又は取扱制限を緩和する必要性があると思料される場合には、格付及び取扱制限の見直しに必要な処理を行うこと。

解説：秘密としての管理を求められる期間を明記することにより、必要以上の秘密管理を防止するための事項である。
なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ）第 5 項では、「秘密文書には、秘密にしておく期間を明記し、その期間が経過した時は、秘密の取扱いは、解除されたものとする。ただし、その期間中秘密にする必要がなくなったときは、その旨を通知して秘密の解除を行うものとすること。」と定めている。

6　教職員等は、情報を機密性３情報と決定した書面のうち、必要なものには、一連番号を付し、その所在を明らかにしておくこと。

解説：機密性３情報である書面に一連番号を付与し、個別に所在管理を行うことを求める事項である。
配付時に一連番号を付与することによって、当該機密性３情報を受領した者に、一定の管理義務を要請する効果も期待できる。

なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ）第 4 項では、「『極秘』の文書には、必ず一連番号を付し、その所在を明らかにしておくこと。」と定めている。

第三節　情報の保存

解説：大学においては、その教育研究事務の継続性を確保する等の必要性から情報を保存する場合があるが、情報の保存を続ける限り、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれも継続する。
これらのことを勘案し、本節では、情報の保存に関する対策基準として、格付に応じた情報の保存及び保存期間における取扱い又は保存期間満了後の取扱期間についての遵守事項を定める。

B2101-52　（格付に応じた情報の保存）（政府機関統一管理基準の対応項番 1.3.1.3(1)）

第五十二条　教職員等は、情報の格付及び取扱制限に応じて、情報を適切に保存すること。

解説：電磁的記録媒体に保存された情報、書面に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、適切に保存することを求める事項である。
例えば、教職員等が書面を保存する場合は、要管理対策区域内の棚に保存したり、必要なく情報の参照等をさせないために、施錠のできる書庫・保管庫に保存すること等が考えられる。ここで、外部電磁的記録媒体に情報を保存する場合は、主体認証情報（パスワード）によるロック機能を利用して、当該媒体の利用を防止することが可能であるが、ロック機能を持たない外部電磁的記録媒体も多く、保存する情報に応じた外部電磁的記録媒体を選択する必要がある。
一方、教職員等が要保護情報に関する情報処理を行う場合は、例えば、要管理対策区域内に設置された情報システム上に保存すること等が考えられる。また、教職員等が許可を得て、個人で利用する ASP・SaaS サービスの外部の情報システムを用いて、要保護情報に関する情報処理を行う場合は、ポリシー並びにそれに基づく規程及び手順等と同等の情報セキュリティ対策が実施される場所に保存する必要がある。なお、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切とな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。

２　教職員等は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うこと。

解説：電磁的記録媒体に保存された情報に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、必要のない者に情報へアクセスさせないためのアクセス制御を可能な範囲で実施することを求める事項である。
電磁的記録媒体に保存された情報には電子計算機等を利用してアクセスすることになるため、アクセス制御は、電子計算機、オペレーティングシステム、アプリケーション及びファイル等を単位として行うことができ、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。
情報システムに教職員等自らがアクセス制御設定を行う機能が装備されている

場合には、教職員等は、当該情報の格付及び取扱制限の指示内容に従って、必要なアクセス制御の設定を行うこと。例えば、要機密情報であれば、不適当な者から参照されないよう、読取制限の属性を付与し、完全性２情報であれば、不適当な者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。例えば、上書き禁止の属性を付与する方法としては、ファイルに対する書込権限者の制限、又はファイルのセキュリティ設定でパスワード設定した上での読取専用の設定等がある。

ただし、複製禁止の取扱制限がされていたとしても、情報システムに複製禁止とする機能がなければ、そのアクセス制御の設定をすることはできない。その場合には、情報システムが備えていない機能については、教職員等が取扱上注意することで、その指示を遵守することになる。

3　教職員等は、要機密情報を電磁的記録媒体に保存する場合には、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、情報にパスワードを設定すること。

解説：電磁的記録媒体に保存された情報の機密性を確保するために、要機密情報を容易に参照できないようにするため、パスワードによって保護することを求める事項である。

方法としては、文書作成アプリケーションによるパスワード保護オプション、圧縮・解凍ソフトによるパスワード保護オプションの利用等が挙げられる。

なお、パスワードは、適切な文字列の長さ及び複雑さを持つように設定する必要がある。

4　教職員等は、要機密情報を電磁的記録媒体に保存する場合には、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。

解説：電磁的記録媒体に保存された情報の機密性を確保するために、その暗号化を行うことを求める事項である。

暗号化を行うと情報の復号ができる者を限定することとなり、学内において情報の機密性を高めるために有効である。また、万一 PC、光ディスク、USB メモリ等の紛失・盗難が発生しても、暗号が解読されない限り、情報の漏えいは防ぐことができる。

情報を暗号化する際は、「B2101 情報システム運用・管理規程」第 11 章第 5 節（暗号と電子署名の標準手順）の定めに従うこと。

5　教職員等は、要保全情報を電磁的記録媒体に保存する場合には、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は、情報に電子署名を付与すること。

解説：要保全情報を電磁的記録媒体に保存する場合、その改ざんのおそれを勘案し、必要に応じて電子署名を付与することを求める事項である。

情報に電子署名を付与する際は、「B2101 情報システム運用・管理規程」第 11 章第 5 節（暗号と電子署名の標準手順）の定めに従うこと。

6　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、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。

解説：情報のバックアップ又は複写の取得を求める事項である。

バックアップは、その取得頻度が復元の手順及び所要時間に関係することも考慮して、頻度を定める。インシデントに備えて適切な頻度で復元の演習も行い、教職員等に習熟させる。

なお、バックアップした記録媒体の紛失・盗難により情報が漏えいするおそれがあるため、必要に応じて、その情報を暗号化することが望ましい。

7　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のバックアップ又は重要な設計書の複写の保管について、災害等により生ずる支障の有無を検討し、支障があると認めたときは、適切な措置を講ずること。

解説：バックアップ又は複写の適切な保管を求める事項である。

例えば、バックアップ又は複写を防火金庫に保管することや、同時被災に備えて遠隔地に保管すること等が考えられる。

B2101-53　（情報の保存期間）（政府機関統一管理基準の対応項番 1.3.1.3(2)）

第五十三条　教職員等は、電磁的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し、保存期間を延長する必要性がない場合は、速やかに消去すること。

解説：電磁的記録媒体に保存された情報に関して、情報セキュリティ確保の観点から保存期間を定めている場合に、当該保存期間に従って管理することを求める事項である。

教職員等は、情報セキュリティ上、必要な期間は確実に情報を保存するとともに、その期間を経過した場合には当該情報を速やかに消去してリスクの増大を回避する必要がある。また、当該情報が記載されている法人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等して移管するものとする。その際、ポリシー並びにそれに基づく規程及び手順等における遵守事項に従いつつ、例えば、教職員等でパスワードを設定していた場合は、解除する等して移管先がその内容を参照できるように配慮すること。

第四節　情報の移送

解説：大学においては、その教育研究事務の遂行のために他者又は自身に情報を移送する場合がある。移送の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部電磁的記録媒体及び PC の運搬、書面の運搬等の方法が挙げられるが、いずれの方法を用いるにせよ、情報の移送により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになる。

これらのことを勘案し、本節では、情報の移送に関する対策基準として、情報の移送に関する許可及び届出、情報の送信と運搬の選択、移送手段の決定、記録媒体及び電磁的記録の保護対策についての遵守事項を定める。

B2101-54　（情報の移送に関する許可及び届出）（政府機関統一管理基準の対応項番 1.3.1.4(1)）

第五十四条　教職員等は、機密性３情報、完全性２情報又は可用性２情報を移送する場合には、職場情報セキュリティ責任者の許可を得ること。

解説：機密性３情報、完全性２情報又は可用性２情報を移送する際に職場情報セキュリティ責任者の許可を求める事項である。

なお、機密性３情報、完全性２情報又は可用性２情報を定常的に移送する必要がある場合には、送信又は運搬の別、移送手段、情報の保護対策に関して、手続を定めておくことが望ましい。

２　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情報である書面を移送する場合には、職場情報セキュリティ責任者に届け出ること。ただし、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

解説：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情報である書面を移送する際に職場情報セキュリティ責任者に届け出ることを求める事項である。

なお、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情報である書面を定常的に移送する必要がある場合には、送信又は運搬の別、移送手段、情報の保護対策に関して、手続を定めておくことが望ましい。また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

B2101-55　（情報の送信と運搬の選択）（政府機関統一管理基準の対応項番 1.3.1.4(2)）

第五十五条　教職員等は、要保護情報である電磁的記録を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを選択し、職場情報セキュリティ責任者に届け出ること。ただし、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の移送であり、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

解説：要保護情報の安全確保に留意した移送を求める事項である。

届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

B2101-56　（移送手段の決定）（政府機関統一管理基準の対応項番 1.3.1.4(3)）

第五十六条　教職員等は、要保護情報を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、職場情報セキュリティ責任者に届け出ること。ただし、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情報である書面の移送であり、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

解説：多種多様な移送手段の中から要保護情報を安全に移送するための手段の選択を求める事項である。

「移送手段」とは、送信については学内通信回線、信頼できるプロバイダ、VPN及び暗号メール（S/MIME）等、運搬については信頼できる運送業者や、部局総括責任者が指定する運送役務及び教職員等自らによる携行等が挙げられる。

なお、「S/MIME（Secure Multipurpose Internet Mail Extensions）」とは、電

子メールの暗号化の方式の１つである。
また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

B2101-57　（記録媒体の保護対策）（政府機関統一管理基準の対応項番 1.3.1.4(4)）

第五十七条　教職員等は、要機密情報が記録又は記載された記録媒体を運搬する場合には、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。

解説：要機密情報が記録又は記載された記録媒体を運搬する場合における情報セキュリティ対策を求める事項である。
教職員等は、外部電磁的記録媒体、PC、書面等を運搬する場合には、例えば、外見ではその内容が要機密情報であると知られないこと、送付先において適切な取扱いがなされるように二重封筒とすること、「親展」の指定を行うこと、専用ケースに保存して施錠すること等、安全確保のための適切な措置を講ずる必要がある。

B2101-58　（電磁的記録の保護対策）（政府機関統一管理基準の対応項番 1.3.1.4(5)）

第五十八条　教職員等は、要機密情報である電磁的記録を移送する場合には、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、情報にパスワードを設定すること。

解説：移送手段の種別を問わず、受取手以外の者が要機密情報を容易に参照できないようにするため、パスワードによって保護することを求める事項である。
方法としては、文書作成アプリケーションによるパスワード保護オプション及び圧縮・解凍ソフトによるパスワード保護オプションの利用等が挙げられる。
なお、パスワードは、適切な文字列の長さ及び複雑さを持つように設定する必要がある。

２　教職員等は、要機密情報である電磁的記録を移送する場合には、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。

解説：要機密情報を移送する場合、その漏えいに係るリスクを勘案し、必要に応じて暗号化することを求める事項である。情報を暗号化する際は、「B2101 情報システム運用・管理規程」第 11 章第 5 節（暗号と電子署名の標準手順）の定めに従うこと。

３　教職員等は、要保全情報である電磁的記録を移送する場合には、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は、情報に電子署名を付与すること。

解説：要保全情報を移送する場合、必要に応じて電子署名の付与を行うことを求める事項である。情報に電子署名を付与する際は、「B2101 情報システム運用・管理規程」第 11 章第 5 節（暗号と電子署名の標準手順）の定めに従うこと。

４　教職員等は、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ときは、情報のバックアップを取得すること。

解説：要保全情報を移送する場合、必要に応じてバックアップを取得することを求める事項である。

５　教職員等は、要安定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等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。

解説：要安定情報を移送する場合、必要に応じて所要の措置を講ずることを求める事項である。

６　教職員等は、電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いる必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：情報を分割し、これを異なる経路で移送することを求める事項である。

要機密情報を移送する場合には、当該要機密情報が情報量的に解読不能となるように、分割して移送を行うこと。

この考え方は、専門用語で秘密分散技術といわれ、例えば、１個の電子情報についてファイルを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 CD-R、DVD、MO、USB メモリ、フラッシュメモリ等の外部電磁的記録媒体で郵送する方法が挙げられる。

第五節　情報の提供

解説：大学においては、その教育研究事務の遂行のために学外の者に情報を提供する場合があるが、提供先における情報の不適切な取扱いにより、当該情報の漏えい又は不適切な利用等が発生するおそれがある。

これらのことを勘案し、本節では、情報の提供に関する対策基準として、情報の公表及び他者への情報の提供についての遵守事項を定める。

B2101-59　（情報の公表）（政府機関統一管理基準の対応項番 1.3.1.5(1)）

第五十九条　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。

解説：公表すべきでない情報の公表を防止することを求める事項である。

本学の業務においては、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がある。この場合には、公表しようとする情報に対する格付の適正さを再度検討し、必要に応じて格付の変更等を行った上で、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必要がある。

なお、情報セキュリティ関係規程の定めによらず、当該情報が法律の規定等で公表が禁じられたものでないことは別途確認する必要がある。

２　教職員等は、電磁的記録を公表する場合には、当該情報の付加情報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：教職員等が意図せず情報を漏えいすることを防止するための事項である。

例えば、公開する文書ファイルの作成者名、組織名その他の記録に使用できる「プロパティ」と呼ぶ部分に個人情報が残っている又は文書に作成履歴が残っていることがないように除去することが考えられる。また、電子ファイル上で

アプリケーションの機能を用いて特定の部分の情報を黒塗りしたとしても、当該部分の情報の閲覧が可能となる場合があることに留意し、黒塗りされた部分の情報そのものの削除や置換えを行うことも検討する必要がある。

B2101-60　（他者への情報の提供）（政府機関統一管理基準の対応項番 1.3.1.5(2)）

第六十条　教職員等は、機密性３情報、完全性２情報又は可用性２情報を学外の者に提供する場合には、職場情報セキュリティ責任者の許可を得ること。

解説：機密性３情報、完全性２情報又は可用性２情報を学外の者に提供する際に職場情報セキュリティ責任者の許可を得ることを求める事項である。

２　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情報である書面を学外の者に提供する場合には、職場情報セキュリティ責任者に届け出ること。ただし、職場情報セキュリティ責任者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。

解説：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情報である書面を学外の者に提供する際に職場情報セキュリティ責任者に届け出ることを求める事項である。

届出を必要としない提供を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

３　教職員等は、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、当該情報に付された情報の格付及び取扱制限に応じて適切に取り扱われるための措置を講ずること。

解説：要保護情報を学外の者に提供する場合において遵守すべきことを定める事項である。

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、情報の格付及び取扱制限の取扱上の留意事項を提供先へ確実に伝達し、必要に応じ、提供先における当該情報の適切な管理のために必要な措置及び情報の利用目的を協議の上、決定する必要がある。

情報の格付及び取扱制限の取扱上の留意事項を伝達する場合、格付の区分だけを示すのでは不十分である。なぜなら、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が認識できないからである。格付の区分（例えば、「機密性２」と記載する）で示すのであれば、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か、格付の区分で示す以外の方法としては、提供する情報にそれを適切に管理するために必要な措置が具体的にわかるように示す（例えば、「委員以外への再配布を禁止する」と記載する）等をする必要がある。

また、提供した情報が提供先の別の者によって取り扱われる際にも、それが適切に取り扱われることを確実にするため、必要な措置について口頭による伝達ではなく記載する等の方法によって伝達する必要がある。

教職員等は、格付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及び取扱制限に従っ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。

4　教職員等は、電磁的記録を提供する場合には、当該記録の付加情報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：教職員等が意図せず情報を漏えいすることを防止するための事項である。

例えば、提供する文書ファイルの作成者名、組織名その他の記録に使用できる「プロパティ」と呼ぶ部分に個人情報が残っている又は文書に作成履歴が残っていることがないように除去することが考えられる。

第六節　情報の消去

解説：教育研究事務において利用した電子計算機、通信回線装置及び外部電磁的記録媒体については、不要となった後、適切に処分されずに放置された場合には、盗難や紛失により、記録されている情報が漏えいするおそれがある。また、情報を消去する際に、適切な措置が講じられていなければ、復元ツールや復元サービス等を用いて当該情報を復元することが可能であり、情報漏えいのおそれは払拭されない。

これらのことを勘案し、本節では、情報の消去に関する対策基準として、電磁的記録の消去方法及び書面の廃棄方法についての遵守事項を定める。

B2101-61　（電磁的記録の消去方法）（政府機関統一管理基準の対応項番 1.3.1.6(1)）

第六十一条　教職員等は、電磁的記録媒体を廃棄する場合には、全ての情報を抹消すること。

解説：電磁的記録媒体を廃棄する場合に、全ての情報を復元が困難な状態にすることを求める事項である。

「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。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、内蔵電磁的記録媒体及び外部電磁的記録媒体に記録されている全ての情報を適切な方法で復元が困難な状態にする必要がある。

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）によりファイルを個々に抹消する方法

・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

なお、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。

・FD 等の磁気媒体の場合には、当該媒体を折り曲げる、切断する等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

る方法

2　教職員等は、電磁的記録媒体を他の者へ提供する場合には、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：電磁的記録媒体に保存された不要な情報を抹消することを求める事項である。長期にわたり利用された内蔵電磁的記録媒体及び外部電磁的記録媒体には、要機密情報が断片的に残留した状態となっているおそれがある。そのため、電磁的記録媒体を用いて学外の者に情報を提供する場合や、担当者間による業務の引継ぎを伴わず、別の業務に機器等を引き継ぐことが想定される場合には、データを抹消する必要がある。

3　教職員等は、電磁的記録媒体について、設置環境等から要機密情報を抹消する必要性の有無を検討し、必要と認めたときは、当該電磁的記録媒体の要機密情報を抹消すること。

解説：無人の執務室に設置されていたり、設置場所及び利用場所が確定していない電子計算機、通信回線装置及び外部電磁的記録媒体等、安全といえない環境で利用される電子計算機等に要機密情報を残留させないことを求める事項である。教職員等は、要機密情報が保存された電子ファイル又は空き領域に残留する情報を抹消すること。

B2101-62　（書面の廃棄方法）（政府機関統一管理基準の対応項番 1.3.1.6(2)）

第六十二条　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：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、焼却又は溶解等により、復元が困難な状態にすることを求める事項である。なお、廃棄すべき書類が大量である等の理由により、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。

第八章　情報システムの利用

第一節　情報システムの利用

解説：情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

これらのことを勘案し、識別コード及び主体認証情報の管理等に関する対策基準として、識別コードと主体認証情報の管理及び付与管理、代替手段等の適用についての遵守事項を定める。

なお、「B2101 情報システム運用・管理規程」第 11 章第 4 節において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する判断基準を、「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 章第 1 節

～第 5 節においても各機能の導入等に関する対策基準を定めている。

B2101-63　（識別コードの管理）（政府機関統一管理基準の対応項番 1.4.1.1(1)）

第六十三条　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。

解説：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、なりすまし行為であることを認識する必要がある。仮に、悪意がない行為であっても、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、安易に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利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使って行おうとしている業務について、他者へ代行処理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、当該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用いて、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。また、業務の継続のために、他者の識別コードを用いることが不可避の場合には、例外措置の承認を行う際に本人の事前の了解に加えて、部局技術担当者の了解を得ることが最低限必要である。極めて緊急性が高い場合には、他者の識別コードを利用していた期間とアクセスの内容を、事後速やかに、部局技術担当者に報告しなければならない。部局技術担当者は、その理由と利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のが望ましい。

いずれの場合も、用い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用いて、情報システムを利用することは禁止されるべきである。

遵守事項に「主体認証の際に」とあるのは、主体認証以外の目的で他者の識別コードを使用することを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、電子メール送信先のアドレスとして他者の識別コードを指定してメール送信のための情報システムを利用することについては問題がない。

２　利用者等は、自己に付与された識別コードを他者が主体認証に用いるために付与及び貸与しないこと。

解説：共用する識別コードについても部局技術担当者から各本人に個別に付与されるものであり、付与された者がそれを他者に付与、貸与してはならない。また、部局技術担当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。

遵守事項に「主体認証に用いるために」とあるのは、主体認証に用いる目的以外で他者に知らせることを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、自分宛の電子メールアドレスとして知らせることについては問題がない。

３　利用者等は、自己に付与された識別コードを、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。

解説：ほとんどの場合には、識別コード自体は必ずしも秘密ではないが、積極的に公開したり、公然となるような放置はしないようにすることを求める事項である。本来、主体認証のためには、主体認証情報が用いられるが、識別コード自体も秘密にすることによって、不正に主体認証される可能性をより低くすることが可能となる。そのため、識別コードについても適切に管理することが求められる。

4　利用者等は、教育研究事務のために識別コードを利用する必要がなくなった場合は、その旨を部局技術担当者に届け出ること。ただし、個別の届出が必要ないと、部局技術責任者が定めている場合は、この限りでない。

解説：識別コードを利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担当者へ届け出ることを求める事項である。

ただし、例えば、卒業や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担当者が利用者等自らからの届出によらずして把握できる場合等、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良い。

5　部局技術責任者は、管理者権限を持つ識別コードを付与された利用者等に、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させる必要性の有無を検討し、必要と認めたときは、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させること。

解説：利用者等に、管理者権限を持つ識別コードを管理者としての業務遂行時に限定して、利用させることを求める事項である。

なお、本遵守事項は、実際には利用者等が繁雑な操作を必要とする場合があるため、最少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、当該情報システムで取り扱う情報の重要性等を勘案し、必要に応じて選択されたい。

6　利用者等は、管理者権限を持つ識別コードを付与され、かつ部局技術責任者が求めた場合には、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。

解説：管理者権限を持つ識別コード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ティングシステムが Windows であれば、Administrator 権限を付与された場合であって、PC の設定変更等をしないときには、Administrator 権限なしの識別コードを使用し、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。

B2101-64　（主体認証情報の管理）（政府機関統一管理基準の対応項番 1.4.1.1(2)）

第六十四条　利用者等は、主体認証情報が他者に使用され、又はその危険が発生した場合には、直ちに部局技術責任者又は部局技術担当者にその旨を報告すること。

解説：利用者等は、自らの主体認証情報自体の露呈や主体認証情報に関連する情報の露呈又はそれらが露呈した可能性がある場合には、直ちに部局技術責任者又は部局技術担当者へ報告することを求める事項である。

2　部局技術責任者又は部局技術担当者は、主体認証情報が他者に使用され、又はその危険が発生したことを知った場合には、必要な措置を講ずること。

解説：自らが発見したり、報告を受けたりして、主体認証情報の他者使用又は危険発生を知った部局技術責任者又は部局技術担当者が、必要な措置を講ずることを求める事項である。必要な対策としては、例えば、主体認証情報の変更や別の主体認証方式の併用、当該識別コードによるログオン制限等がある。

3　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こと。

解説：利用者等は、例えば自己の主体認証情報を内容が分かる状態で付箋に記入して貼付するようなことを行ってはならず、主体認証情報を入力する際に周囲からの盗み見に注意を払ったり、管理者を名乗って主体認証情報を聞き出す行為に注意したりする等、他者に知られないように管理すること。

また、主体認証情報を、容易に他者に知られてしまう状態で、主体認証を行う情報システムとは異なる情報システムに記憶させないこと。

二　自己の主体認証情報を他者に教えないこと。

解説：利用者等が他者に処理代行させるために自己の主体認証情報を教示しないことを求める事項である。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連があいまいとなる可能性があり、アクセス制御、権限管理、証跡管理その他のセキュリティ対策の基礎が崩壊する可能性がある。また、教示された側にとっても、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。

三　主体認証情報を忘却しないように努めること。

解説：他者が容易に見ることができないような措置（施錠して保存する等）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、メモを取ることそのものを禁ずるものではない。むしろ、忘れることのないようにもしなければならない。

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）する場合に備えて、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。

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こと。

解説：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、更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。

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こと。

解説：利用者等が付与された複数の識別コードで共通の主体認証情報を用いていると、

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ため、共通の主体認証情報を用いないことを求める事項である。複数の識別コードの権限レベルが異なっていたり、複数の識別コードを用いる情報システムのセキュリティレベルが異なっていたりする場合、低いレベルの主体認証情報の漏えいにより、高いレベルの権限や高いセキュリティレベルの情報システムが正規の主体認証方式を用いて容易に不正アクセスされないようにすることを求めている。対象となる識別コードには、本学支給の情報システムだけでなく、本学支給以外の情報システムで使用している識別コードも含める必要がある。

なお、シングルサインオンシステム等、一組の識別コード及び主体認証情報を用いて複数のシステムの利用を可能とするシステムは、当該複数システム間のそれぞれの主体認証情報が異なっていれば、本項目が想定する脅威は存在しないため、共通の主体認証情報を用いたことにはならない。

六　部局技術担当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こと。

解説：定期的な変更の要求を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等の運用によって対処することでも差し支えない。

なお、例えば、主体認証やその後の情報システムにおける処理を自動的に行うと、定期的な変更の際に、それらの処理をその都度修正する必要があることに注意すること。

4　利用者等は、所有による主体認証を用いる場合には、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こと。

二　主体認証情報格納装置を他者に付与及び貸与しないこと。

三　主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに部局技術責任者又は部局技術担当者にその旨を報告すること。

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又は部局技術担当者に返還すること。

解説：所有による主体認証方式では、それを取得した者が正当な主体として主体認証されることになるため、他者に使用されることがないように、また、紛失等で、その可能性がある場合の報告を徹底する必要がある。卒業や異動等により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、これを返却する必要がある。

5　部局技術責任者は、主体認証のために取得した情報を本人から事前に同意を得た目的以外の目的で使用しないこと。

解説：利用者の指紋情報等、主体認証情報として生体情報を取り扱う場合には、個人のプライバシーに配慮し、個人情報として厳格な管理が求められる。

管理方法としては、元の生体情報が再現できないように保存すること等が考えられる。

B2101-65　（識別コードと主体認証情報の付与管理）（政府機関統一管理基準の対応項番 1.4.1.1(3)）

第六十五条　部局技術責任者は、権限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、利用状況等を考慮して、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。

２　部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、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権限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　アクセス制御情報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、確実にアクセス権を設定するため、関連手続を明確に定めることを求める事項である。

３　部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。

解説：権限の管理については、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、権限管理を行う者を定める事項である。

B2101-66　（識別コードと主体認証情報における代替手段等の適用）（政府機関統一管理基準の対応項番 1.4.1.1(4)）

第六十六条　部局技術担当者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった利用者等から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。

解説：情報システムを利用する利用者等においては、何らかの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合が想定される。例えば、知識による主体認証方式であれば主体認証情報（パスワード）を忘れた場合、所有による主体認証方式であれば携帯するのを忘れた場合、指紋による主体認証方式であれば指を怪我した場合等が挙げられる。

それらの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合には、代替手段の使用に関する許可申請をすることができる。部局技術担当者は、その申請を受理した時には、その申請が正当な利用者からの許可申請であること及び許可申請の理由が妥当であること等を確認した上で、その必要性を判断し代替手段を提供することを求める事項である。な

お、代替手段としては、例えば、当日限り有効とした暫定的な識別コード及び主体認証情報の提供や、当該情報システムから切り離された代替 PC の提供、情報システムを利用しない業務環境の提供等が想定されるが、部局技術担当者が情報セキュリティ保護の観点に加えて利用者等本人による業務執行の緊急性、効率性、利便性及び当該情報システムの可用性等も考慮して、適正な代替手段を準備しておくこと。

なお、代替手段の提供に当たっては、その申請理由と使用期間、使用者等を記録として残すことが望ましい。

2　部局技術責任者及び部局技術担当者は、権限管理を行う必要があると認めた情報システムにおいて、識別コードの不正使用を知った場合には、直ちに当該識別コードによる使用を停止させること。

解説：自らが発見したり、報告を受けたりして、識別コードの不正使用を知った場合には、他の項目で定められているインシデントの対処に係る遵守事項とともに、本遵守事項の対処を実施する。

なお、不正使用による被害が甚大であると予想される場合には、例えば、全ての使用を停止した上で、状況把握、原因特定及び証拠保全のためにバックアップを取得することが望ましい。その後、不正使用に対する対策を講じた上で、使用を再開する場合には、改めて主体認証情報を再発行することが望ましい。

第九章　情報処理の制限

第一節　要管理対策区域外での情報処理の制限

解説：大学においては、その教育研究事務の遂行のため、要管理対策区域外において情報処理を実施する必要が生ずる場合がある。この際、要管理対策区域外での実施では物理的な安全対策を講ずることが比較的困難になることから、利用者等は、要管理対策区域内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。

これらのことを勘案し、本節では、要管理対策区域外での情報処理の制限に関する対策基準として、安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項を定める。

B2101-67　（安全管理措置についての規定の整備）（政府機関統一管理基準の対応項番 1.4.2.1(1)）

第六十七条　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の情報処理を行う場合の安全管理措置についての規定を整備すること。

解説：全学実施責任者が、要管理対策区域外において情報処理を行う場合の安全管理措置についての規定を整備することを求める事項である。ただし、情報処理の種類により個別の規定を設けても構わない。

要管理対策区域外において情報処理を行う場合を具体的に想定し、情報処理の内容と取り扱う情報、実施場所、回線を通した通信の形態、関与する学内外の者等に応じた措置を示した規定を整備する必要がある。

２　全学実施責任者は、要保護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の安全管理措置についての規定を整備すること。

解説：全学実施責任者が、要管理対策区域外に要保護情報を取り扱う情報システムを持ち出す場合の安全管理措置についての規定を整備することを求める事項である。持ち出す情報システム及び持ち出し先等を具体的に想定して規定を整備する必要がある。

B2101-68　（許可及び届出の取得及び管理）（政府機関統一管理基準の対応項番 1.4.2.1(2)）

第六十八条　利用者等は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外で情報処理を行う場合には、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。

解説：機密性３情報、完全性２情報又は可用性２情報に係る情報処理を要管理対策区域外で行う場合に、部局技術責任者と職場情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については職場情報セキュリティ責任者の、当該情報処理の安全性については部局技術責任者の許可を得ることとなる。

なお、「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

２　利用者等は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外で情報処理を行う場合には、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。

解説：要管理対策区域外で機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、部局技術責任者と職場情報セキュリティ責任者の両方に届け出ることを求める事項である。また、部局技術責任者又は職場情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない要管理対策区域外での情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

３　部局技術責任者及び職場情報セキュリティ責任者は、要管理対策区域外での要保護情報の情報処理に係る記録を取得すること。

解説：要管理対策区域外での要保護情報の情報処理に係る記録を取得することを求める事項である。

「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

４　部局技術責任者及び職場情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：要管理対策区域外での情報処理を行うことを許可した期間が終了した時に報告の有無を確認し、措置を講ずること等を求める事項である。

状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、利用者等に改めて許可を得るようにさせること。

5　部局技術責任者及び職場情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

解説：機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、期間の延長が必要な状況であれば利用者等に改めて届出をさせる等の措置を講ずることを求める事項である。

6　利用者等は、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には、教育研究事務の遂行に必要最小限の情報処理にとどめること。

解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を要管理対策区域外で情報処理することを最小限にとどめることを求める事項である。

7　利用者等は、機密性３情報、完全性２情報又は可用性２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、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。

解説：機密性３情報、完全性２情報又は可用性２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利用者等に、部局技術責任者と職場情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該持ち出しの業務上の必要性については職場情報セキュリティ責任者の、当該持ち出しの安全性については部局技術責任者の許可を得ることとなる。

8　利用者等は、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、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。

解説：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利用者等に、部局技術責任者と職場情報セキュリティ責任者の両方に届け出ることを求める事項である。また、部局技術責任者又は職場情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない要管理対策区域外への持ち出しを定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

9　部局技術責任者及び職場情報セキュリティ責任者は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しに係る記録を取得すること。

解説：要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しに係る記録を取得することを求める事項である。

「持ち出しに係る記録」には、持ち出しの実施者、端末、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

１０　部局技術責任者及び職場情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２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ことを許可した期間が終了

した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：情報システムを要管理対策区域外に持ち出すことを許可した期間が終了した時に報告の有無を確認すること等を求める事項である。

状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、利用者等に改めて許可を得るようにさせること。

１１　部局技術責任者及び職場情報セキュリティ責任者は、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ことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

解説：届出期間が長期にわたる場合等、必要に応じて、要管理対策区域外への持ち出しの状況を確認することを求める事項である。

状況を確認した際に、期間の延長が必要な状況であれば、利用者等に改めて届出をさせること。

１２　利用者等は、要保護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、教育研究事務の遂行に必要最小限の情報システムの持ち出しにとどめること。

解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を取り扱うシステムを要管理対策区域外に持ち出すことを最小限にとどめることを求める事項である。

B2101-69　（安全管理措置の遵守）（政府機関統一管理基準の対応項番 1.4.2.1(3)）

第六十九条　利用者等は、要保護情報について要管理対策区域外での情報処理について定められた安全管理措置を講ずること。

解説：利用者等に対して、要管理対策区域外での情報処理について定められた安全管理措置を講ずることを求める事項である。

２　利用者等は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを終了した時に、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。

解説：利用者等に対して、要管理対策区域外での情報処理が終了したことを、その許可を与えた者に報告することを求める事項である。

３　利用者等は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しについて定められた安全管理措置を講ずること。

解説：利用者等に対して、情報システムの要管理対策区域外への持ち出しについて定められた安全管理措置を講ずることを求める事項である。

定められた安全管理措置の内容としては、例えば、盗難及び亡失の防止に十分に注意すること、操作や画面の盗み見を防止するために、スクリーンに覗き見防止フィルターを貼ることや、スクリーンセーバーの機能を利用し、操作を実施できなくすること等が考えられる。

４　利用者等は、機密性３情報、完全性２情報又は可用性２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ことを終了した時に、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。

解説：利用者等に対して、要管理対策区域外へ情報システムの持ち出しが終了したことを、その許可を与えた者に報告することを求める事項である。

第二節　本学支給以外の情報システムによる情報処理の制限

解説：大学においては、その教育研究事務の遂行のため、本学支給以外の情報システムを利用する必要が生じる場合がある。この際、当該情報システムが、本学が支給したものでないという理由で対策を講じなかった場合、当該情報システムで取り扱われる情報のセキュリティは確保できない。

これらのことを勘案し、本節では、本学支給以外の情報システムによる情報処理の制限に関する対策基準として、安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項を定める。

B2101-70　（安全管理措置についての規定の整備）（政府機関統一管理基準の対応項番 1.4.2.2(1)）

第七十条　全学実施責任者は、要保護情報について本学支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備すること。

解説：利用者等が所有する個人の PC 等を用いて要保護情報に関する情報処理を行う場合であっても、本学支給の情報システムと同程度のセキュリティ対策を施す必要があるため、その安全管理措置についての規定を整備することを求める事項である。ただし、情報システムの種類により個別の規定を設けても構わない。

本学支給以外の情報システムには、いわゆる私物の PC のほか、学外者の持ち込み PC も含むものとする。

B2101-71　（許可及び届出の取得及び管理）（政府機関統一管理基準の対応項番 1.4.2.2(2)）

第七十一条　利用者等は、機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムにより情報処理を行う必要がある場合には、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。

解説：機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムにより情報処理を行う必要がある場合に、部局技術責任者と職場情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については職場情報セキュリティ責任者の、当該情報処理の安全性については部局技術責任者の許可を得ることとなる。

本学支給以外の情報システムによる機密性３情報、完全性２情報又は可用性２情報の情報処理を許可する場合は、その期間については、最長で１年間にすることが望ましい。ただし、期間の延長が必要な状況であれば、利用者等に改めて許可を得るようにさせること。

２　利用者等は、機密性２情報であって完全性１情報かつ可用性１情報である情報について本学支給以外の情報システムにより情報処理を行う必要がある場合には、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。

解説：本学支給以外の情報システムによる機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、部局技術責任者と職場情報セキュリティ責任者の両方に届け出ることを求める事項である。また、部局技術責任者又は職場情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない本学支給以外の情報システムによる情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

３　部局技術責任者及び職場情報セキュリティ責任者は、本学支給以外の情報システムによる要保護情報の情報処理に係る記録を取得すること。

解説：本学支給以外の情報システムによる要保護情報の情報処理に係る記録を取得することを求める事項である。

「本学支給以外の情報システムによる情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

４　部局技術責任者及び職場情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：本学支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、報告の有無を確認すること等を求める事項である。

状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告させる。期間の延長が必要な状況であれば、利用者等に改めて許可を得るようにさせること。

５　部局技術責任者及び職場情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について本学支給以外の情報システムによる情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

解説：届出期間が長期にわたる場合等、必要に応じて、本学支給以外の情報システムによる情報処理の状況を確認することを求める事項である。

状況を確認した際に、期間の延長が必要な状況であれば、利用者等に改めて届出をさせること。

B2101-72　（安全管理措置の遵守）（政府機関統一管理基準の対応項番 1.4.2.2(3)）

第七十二条　利用者等は、要保護情報について本学支給以外の情報システムによる情報処理を行う場合には、当該情報システムについて定められた安全管理措置を講ずること。

解説：利用者等が所有する個人の PC 等、本学支給以外の情報システムを用いて要保護情報に関する情報処理を行う場合であっても、本学支給の情報システムと同程度のセキュリティ対策を施す必要があるため、利用者等に安全管理措置を講ずることを求める事項である。

２　利用者等は、機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムによる情報処理を終了した時に、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。

解説：利用者等が機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムによる情報処理を終了した時に、その報告を求める事項である。

本学支給以外の情報システムの利用許可を与えた者は、その終了報告を受け、本学支給以外の情報システムによる情報処理の状況を把握することが可能となる。その結果、本学支給以外の情報システムを、本来必要とされる期間を超えて利用している場合には、これを検知し、利用実態を是正することが可能となる。

３　部局技術責任者は、要保護情報を取り扱う本学支給以外の情報システムについて、定められた安全管理措置が適切に講じられていることを定期的に確認すること。

解説：部局技術責任者に対して、許可又は届出を受理した要保護情報を取り扱う本学支給以外の情報システムについて、本学支給の情報システムと同程度のセキュリティ対策が施されていることの確認を求める事項である。

確認する頻度は、情報処理の開始時や一定期間経過後等、それぞれの大学の特性に応じて設定することが望ましい。また、当該情報システムが固定されている等の理由で、情報システムの運搬が不可能な場合には、当該情報システムが設置されている現地に赴いて確認することが望ましい。

なお、あらかじめ部局技術責任者が認めた場合には、部局技術責任者が指定した者に確認させることも考えられる。その際には、部局技術責任者は、指定した者より適宜報告を受けることが望ましい。

第十章　情報システムのセキュリティ要件

第一節　情報システムのセキュリティ要件

解説：情報システムは、目的業務を円滑に遂行するため、その計画、構築、運用、移行、廃棄及び見直しのライフサイクルを通じて様々な要件を満たすことが必要である。その要件の中にはセキュリティの観点からの要件も含まれ、情報システムのライフサイクルにあわせてセキュリティ対策を実施する必要がある。

これらのことを勘案し、本章では、情報システムのライフサイクルの視点に立ち、各段階において考慮すべき情報セキュリティの対策基準を定める。

B2101-73　（情報システムの計画）（政府機関統一管理基準の対応項番 1.5.1.1(1)）

第七十三条　部局技術責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、全学総括責任者又は情報システムを統括する責任者に求めること。

解説：全学総括責任者（最高情報責任者（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。

なお、「情報システムを統括する責任者」とは、情報システムのライフサイクルの全般にわたって情報システムの構築・運用等に責任を持ち、その責務を全う

するために人員、機器、予算等の資源を確保する者を想定している。部局においては、部局長がこれに該当すると考えられる。

２　部局技術責任者は、情報システムのセキュリティ要件を決定すること。

解説：情報システムに求められる要求事項のうち、セキュリティに関わる要求事項について検討し、その中で必要と判断する要求事項を当該情報システムのセキュリティ要件として決定することを求める事項である。

「情報システムのセキュリティ要件」には、情報システムを構成するハードウェア、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。

具体的なセキュリティ要件については、「B2151 情報セキュリティ要件の明確化に関する技術規程」「B2152 情報システムの構成要素に関する技術規程」「B2153 アプリケーションソフトウェアに関する技術規程」内の事項、「B2101 情報システム運用・管理規程」第 11 章（情報システムに係る規定の整備と遵守）に対応するものも含めた本学の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件を考慮して決める必要がある。

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。

また、ASP・SaaS サービス等の外部の情報システムを利用する場合は、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発生しないようにすること。

なお、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も同様に考慮すること。「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、仮想的・論理的に分割させた状態の情報システムをいう。例えば、仮想化技術を利用することが考えられる。

３　部局技術責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。

解説：情報システムのセキュリティ要件を満たすために必要な対策を定めることを求める事項である。

情報システムにおいて必要な対策としては、「B2151 情報セキュリティ要件の明確化に関する技術規程」「B2152 情報システムの構成要素に関する技術規程」「B2153 アプリケーションソフトウェアに関する技術規程」内の事項、「B2101 情報システム運用・管理規程」第 11 章（情報システムに係る規定の整備と遵守）に対応するものも含めた本学の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情

報システム固有の要件に基づく対策がある。

4　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及びソフトウェアについて、IT セキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性については、「IT セキュリティ評価及び認証制度に基づく認証取得製品分野リスト」を参照し、必要があると認めた場合には、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、当該製品を情報システムの構成要素として選択すること。

解説：情報セキュリティ機能が重要である機器等の購入において、要求する機能を有する製品に選択肢がある場合、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による認証を取得しているものを選択することを求める事項である。第三者による情報セキュリティ機能の客観的な評価によって、安全性の高い情報システムの構築が期待できる。

製品分野として当該認証を取得する必要性の判断については、「IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」に則ることが望ましい。なお、国際承認アレンジメント（CCRA）参加国における ISO/IEC 15408 に基づく認証取得製品又は実質的に CC 認証取得製品とセキュリティ機能上同等であると確認されている製品（上記のリストを参照）を活用することが考えられる。

5　部局技術責任者は、情報システムについて、情報セキュリティの侵害又はそのおそれのある事象の発生を監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定めること。

解説：情報システムの計画において、情報セキュリティの侵害又はそのおそれのある事象の監視のために必要な措置を定めることを求める事項である。

情報セキュリティの侵害とは、要保護情報について機密性、完全性又は可用性が損なわれること及び情報セキュリティ関係規程への違反をいう。

監視する必要性の有無を検討するとは、情報システム及び取り扱う情報等を考慮して、情報システムの各所において監視する必要性の有無を検討することをいう。なお、監視の対象には、学外から通信回線を通してなされる不正アクセス、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又は不正操作、サーバ装置等機器の動作、及び、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。

また、監視のために必要な措置を定めるとは、例えば以下の事項が考えられる。

（1）設ける監視機能を定める。監視機能には、以下の例がある。

・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（侵入検知システム等による）

・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 PC の接続を監視する機能

・PC への外部記録媒体の挿入を監視する機能

・サーバ装置等の機器の正常な動作を監視する機能

・要管理対策区域への入退出を監視する機能

（２）監視を行う運用時の体制を定める。情報システムの運用を行う体制において監視も行うことも考えられる。

（３）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、当該利用者等への説明について定める。

６　部局技術責任者は、構築した情報システムを運用段階へ導入するに当たって、情報セキュリティの観点から実施する導入のための手順及び環境を定めること。

解説：部局技術責任者に、セキュリティの観点での試験等の実施により当該情報システムがセキュリティ要件を満たすことを確認し、運用段階への導入の方法、体制、作業手順、スケジュール、期間、教育やトラブル対処について手順を整備することを求める事項である。

B2101-74　（情報システムの構築及び運用）（政府機関統一管理基準の対応項番 1.5.1.1(2)）

第七十四条　部局技術責任者は、情報システムの構築、運用に際しては、セキュリティ要件に基づき定めたセキュリティ対策を行うこと。

解説：情報システムのセキュリティ要件に基づき機器等の購入及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムについての対策及び監視を実施し、情報システムを構築、運用することを求める事項である。

B2101-75　（情報システムの移行及び廃棄）（政府機関統一管理基準の対応項番 1.5.1.1(3)）

第七十五条　部局技術責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を講ずること。

解説：情報システムの移行及び廃棄を行う場合に、情報システムを構成する機器の扱い、情報の格付等を考慮して、機器及び情報に関して廃棄、保存、消去等の適切な措置を講ずることを求める事項である。

B2101-76　（情報システムの見直し）（政府機関統一管理基準の対応項番 1.5.1.1(4)）

第七十六条　部局技術責任者は、情報システムのセキュリティ対策について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い、必要な措置を講ずること。

解説：情報システムのセキュリティ対策について、必要に応じて見直しとそれに必要な措置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、運用、監視等の状況により判断する必要がある。

第十一章　情報システムに係る規定の整備と遵守

第一節　情報システムに係る文書及び台帳整備

解説：本学の情報システムにおいて、適切なセキュリティ対策を行い、また、インシ

デントが発生した際に適切な対処を行うためには、情報システムの管理のために必要な情報を文書として整備する必要がある。また、大学全体としてセキュリティレベルを維持するとともに、より大規模なインシデントに対処するためには、本学が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備し、維持管理していく必要がある。
これらのことを勘案し、本節では、本学における情報システムに係る文書整備及び台帳整備に関する情報セキュリティの対策基準を定める。

B2101-77　（情報システムの文書整備）（政府機関統一管理基準の対応項番 1.5.2.1(1)）

第七十七条　部局技術責任者は、所管する情報システムについて以下の事項を記載した文書を整備すること。

一　当該情報システムを構成する電子計算機関連事項
- ・電子計算機の管理者及び利用者を特定する情報
- ・電子計算機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
- ・電子計算機の仕様書又は設計書

二　当該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事項
- ・通信回線及び通信回線装置の管理者を特定する情報
- ・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
- ・通信回線及び通信回線装置の仕様書又は設計書
- ・通信回線の構成
- ・通信回線装置におけるアクセス制御の設定
- ・通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応
- ・通信回線の利用部門

三　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
- ・電子計算機のセキュリティ維持に関する手順
- ・通信回線を介して提供するサービスのセキュリティ維持に関する手順
- ・通信回線及び通信回線装置のセキュリティ維持に関する手順

四　インシデントが発生した際の対処手順

解説：所管する情報システムにおいて、適切なセキュリティ対策を行い、また、インシデントが発生した際に適切な対処を行うために、情報システムの管理のために必要な情報を把握し、文書として整備することを定めた遵守事項である。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、文書は書面ではなく電磁的記録媒体として整備しても差し支えない。
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。
電子計算機、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セキュリティホール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、速やかにセキュリティホール対

策を行う等、適切に対処するために必要な事項である。
電子計算機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、インシデント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。
通信回線の構成、通信回線装置におけるアクセス制御の設定、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応、及び通信回線の利用部門の記載は、通信回線の管理状況を把握するために必要な事項である。
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。
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るべき手順であり、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、権限管理並びに証跡管理の設定・変更等の手順が挙げられる。
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。
・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
・情報システムをインシデント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
・インシデントから復旧等を行うための情報システムの構成要素ごとの対処に関する事項
・アンチウイルスソフトウェア等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（「B2101 情報システム運用・管理規程」第 14 条第 3 項及び「B3103 インシデント対応手順」を参照）により、上記のとおり整備されているならば、情報システム個別に整備しなくても構わない。

2　部局技術担当者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理においてセキュリティ対策を行うこと。

解説：所管する情報システムの運用管理において、適切なセキュリティ対策を行うことを求める遵守事項である。
整備した文書に基づいた運用管理を行い、担当者による個別の判断で運用管理を実施しないことが必要である。運用管理は専用のアプリケーションを利用しても差し支えない。

B2101-78　（情報システムの台帳整備）（政府機関統一管理基準の対応項番 1.5.2.1(2)）

第七十八条　全学実施責任者は、全ての情報システムに対して、当該情報システムに係る以下の事項を記載した台帳を整備すること。

一　情報システム名

二　管理部局、当該部局技術責任者の氏名及び連絡先

三　システム構成

四　接続する学外通信回線の種別

五　取り扱う情報の格付及び取扱制限に関する事項

六　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、情報処理業務を外部に委託する場合は、以下の事項を記載した台帳を整備すること。

七　役務名

八　管理部局、当該部局技術責任者の氏名及び連絡先

九　契約事業者

十　契約期間

十一　役務概要

十二　ドメイン名（インターネット上で提供されるサービス等を利用する場合）

十三　取り扱う情報の格付及び取扱制限に関する事項

解説：大学全体としてセキュリティレベルを維持するとともに、より大規模なインシデントに対処するため、本学が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備することを求める事項である。

情報システム名、管理部局及び当該部局技術責任者の氏名・連絡先の記載は、本学が所管する全ての情報システムを把握し、当該情報システムに係る管理責任を把握するために必要な事項である。

システム構成の記載は、情報システムを構成する電子計算機、通信回線及び通信回線装置に関する事項である。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。

接続する学外通信回線の種別、取り扱う情報の格付及び取扱制限に関する事項の記載は、当該情報システムを設置し、また運用管理することによるセキュリティ上のリスクを本学として把握するために必要な事項である。なお、取り扱う情報の格付及び取扱制限に関する事項については、情報システムを構成する電子計算機等について機器別又は機器の形態・目的別に記載することが望ましい。

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、実施責任者若しくは実施担当組織、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。

また、情報処理業務を外部委託する場合は、役務名、管理部局及び当該部局技

術責任者の氏名・連絡先、契約事業者、契約期間、役務概要、ドメイン名（インターネット上で提供される役務等を利用する場合）、取り扱う情報の格付及び取扱制限に関する事項を記載した決裁に係る書類を集約し、容易に参照できるようにすることで、台帳の代替とすることも可能である。
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台帳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。

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、当該情報システムの台帳の記載事項について全学実施責任者に報告すること。

解説：本学の各情報システムを所管する部局技術責任者が、情報システムに係る台帳に記載の事項について全学実施責任者に報告することを求める事項である。
台帳における網羅性の維持のため、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、台帳の最新性の維持のため、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、その報告の方法やタイミングについては、それぞれの大学ごとに定めることが望ましい。

第二節　機器等の購入

解説：機器等を購入（購入に準ずるリース等を含む。）する際に、当該機器等に必要なセキュリティ機能が装備されていない場合及び購入後にセキュリティ対策が継続的に行えない場合には、既存の情報システム又は購入する機器等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。
この課題に対応するため、機器等を購入する際は、本学のポリシー並びにそれに基づく規程及び手順等に準拠した機器等の購入を行うべく、購入先への要求事項を定める必要がある。
これらのことを勘案し、本節では、機器等の購入に関する対策基準として、全学実施責任者による機器等の購入に係る規定の整備、部局技術責任者による当該規定の遵守についての遵守事項を定める。

B2101-79　（適用範囲）（政府機関統一管理基準の対応項番 1.5.2.2）

第七十九条　この節の規定は、機器等の購入（購入に準ずるリース等を含む。以下同じ。）に適用する。

B2101-80　（機器等の購入に係る規定の整備）（政府機関統一管理基準の対応項番 1.5.2.2(1)）

第八十条　全学実施責任者は、機器等の選定基準を整備すること。

解説：機器等の選定に先立って、機器等の選定基準を整備することを求める事項である。
全学実施責任者は、機器等の選定基準の整備に当たっては、機器等がポリシー並びにそれに基づく規程及び手順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、機器等がポリシー並びにそれに基づく規程及び手順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。

なお、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、機器等の購入に反映することが必要である。

2　全学実施責任者は、機器等の購入において、セキュリティ機能の要求仕様があり、総合評価落札方式により購入を行う際には、IT セキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用することを選定基準として定めること。

解説：機器等の購入において、セキュリティ機能の要求仕様があり、総合評価落札方式により購入を行う際に、当該機能を有する製品の中でも ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による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を求める事項である。

第三者による情報セキュリティ機能の客観的な評価のある製品を選定することによって、より信頼度の高い情報システムが構築できる。

3　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：機器等の納入時の確認・検査に関する手続を定めるものである。

特に、確認・検査手続では、納入された機器等が定められた選定基準を満たすことを確認し、その結果を納品検査における確認の判断に加える手続を組み込む必要がある。

具体的な確認・検査の方法として、必要なセキュリティ機能の実装状況（機器等に最新のパッチが適用されているかどうか、アンチウイルス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）及び機器等に不正プログラムが混入していないことを、購入先からの報告で確認すること等が挙げられる。

B2101-81　（機器等の購入に係る規定の遵守）（政府機関統一管理基準の対応項番 1.5.2.2(2)）

第八十一条　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候補の選定における判断の一要素として活用すること。

解説：整備された選定基準に従って、機器等に必要なセキュリティ機能が実装されていること等を確認し、これを機器等の選定における判断の一要素として利用することを求める事項である。

2　部局技術責任者は、機器等の納入時において、定められた確認・検査手続に従って、納品検査を実施すること。

解説：情報セキュリティ対策の視点を加味して定められた納入時の確認・検査手続に準拠して、納入された機器等の納品検査を行うことを求める事項である。

第三節　ソフトウェア開発

解説：ソフトウェアを開発する際には、効果的なセキュリティ対策を実現するため、

当該ソフトウェアが運用される際に関連する情報資産に対して想定される脅威を分析し、その分析に基づいて脅威から情報資産を保護するためのセキュリティ機能（真正確認、アクセス制御、権限管理、証跡管理等）及びその管理機能を適切にソフトウェアに組み込む必要がある。

加えて、開発するソフトウェアの処理に対するセキュリティホールの混入（設計及び作成時のミス等によりセキュリティホールが埋め込まれてしまうこと、不正なコードが開発者により意図的に埋め込まれること等）についての防止対策も必要となる。

これらのことを勘案し、本節では、ソフトウェアを開発する際の対策基準として、全学実施責任者によるソフトウェア開発に係る規定の整備、部局技術責任者による当該規定の遵守についての遵守事項を定める。

B2101-82 （ソフトウェア開発に係る規定の整備）（政府機関統一管理基準の対応項番 1.5.2.3(1)）

第八十二条　全学実施責任者は、ソフトウェア開発について、セキュリティに係る以下の対策事項を部局技術責任者に求めるための規定を整備すること。

解説：本遵守事項では、全学実施責任者が部局技術責任者に求める規定を整備することとしているが、別途規定を整備することとはせずに、「B2101 情報システム運用・管理規程」内において部局技術責任者に対する遵守事項として第 1 号～第 14 号の事項を直接定める方法も可能である。ただし、後者の方法では、自己点検の対象が全学実施責任者ではなく部局技術責任者となることに留意すること。

一　部局技術責任者は、セキュリティに係る対策事項（第三号から第十四号までの遵守事項をいう。）を満たすことが可能な開発体制を確保すること。

解説：ソフトウェア開発を実施する体制が、セキュリティ維持の側面からも実施可能な開発体制（人員、機器、予算等）を確保することを求める事項である。

なお、開発体制の確保に当たっては、情報システムを統括する責任者に要求することとなる。ここで、情報システムを統括する責任者とは、情報システムのライフサイクルの全般にわたって情報システムの構築・運用等に責任を持ち、その責務を全うするために人員、機器、予算等の資源を確保する者を指す。部局においては、部局長がこれに該当すると考えられる。

二　部局技術責任者は、ソフトウェア開発を外部委託する場合には、セキュリティに係る対策事項（第三号から第十四号までの遵守事項をいう。）の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。

解説：ソフトウェア開発を委託先に行わせる場合には、ソフトウェア開発を実施する者に実施の責任を負わせるセキュリティに係る要件を選択し、それを委託先に保証させることを求める事項である。「委託先に実施について保証させる」手段は、契約（付随する確認書等を含む。）によることとなる。

三　部局技術責任者は、ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。

解説：ソフトウェア開発に係る情報資産を保護するための手順及び環境を定めること

を求める事項である。「手順」とは、例えば、仕様書及びソースコード等の成果物に対してソフトウェア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を指し、「環境」とは、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、開発に利用する電子計算機の設置場所及びアクセス制御の方法等を指す。

なお、ソフトウェア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。

四　部局技術責任者は、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と分離する必要性の有無を検討し、必要と認めたときは分離すること。

解説：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ことにより、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を求める事項である。これは運用中の情報システム全体ではなく一部だけの場合も同様である。例えば、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こと等も含まれる。

五　部局技術責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。

解説：開発するソフトウェアに必要となるセキュリティ機能について、その設計を適切に行うとともに、設計書に明確に記録することを求める事項である。

なお、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、外部から察知される脅威（例えば、SQL インジェクション、バッファオーバーフロー等）は存在するため、開発するソフトウェアの機能、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。

六　部局技術責任者は、開発するソフトウェアが運用される際に利用されるセキュリティ機能についての管理機能の必要性の有無を検討し、必要と認めたときは、管理機能を適切に設計し、設計書に明確に記述すること。

解説：「管理機能」とは、真正確認及び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、故障、事故及び障害等の発生時に行う対処及び復旧に係る機能、事故発生時の証跡保全の機能等を指し、これらの必要性をソフトウェアの設計時から検討することにより、必要がある場合にはソフトウェアに組み込むことを求める事項である。

七　部局技術責任者は、ソフトウェアの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。

解説：ソフトウェアの設計について、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を求める事項である。
一般にソフトウェア開発における設計レビューには、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。

八　部局技術責任者は、開発するソフトウェアにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要と認めたときは、その方法を適切に設計し、設計書に明確に記述すること。

解説：ソフトウェアの内部及び入出力するデータについて、処理の誤りや意図的な改ざん等を検出するための機能、又はセキュリティホールの原因となり得る不正な入出力データを排除する機能等を組み込むことを求める事項である。
「データの妥当性」とは、例えば、HTML タグや JavaScript、SQL 文等として機能する不正な文字列や通信過程において生じたデータ誤り等、適切なデータ処理の障害になる情報がデータ内に含まれない状態であることを意味している。データの妥当性を確認する方法として、不正な文字列を変換し、又は削除する機能（いわゆるサニタイジング）の付加、チェックデジット（検査数字）による処理の正当性を確認する機能の付加等がある。

九　部局技術責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価及び ST 確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書の ST 評価及び ST 確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

解説：重要なセキュリティ要件があるソフトウェアについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書の ST 評価及び ST 確認を行うことを求める事項である。
「ST 評価及び ST 確認を受けること」とは、ST 評価及び ST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入手がなされることである。ソフトウェアの開発が終了するまでにセキュリティ設計仕様書について、ST 評価及び ST 確認済みとなっている必要があるが、セキュリティ設計仕様が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。
なお、ソフトウェア開発を外部委託する場合には、契約時に条件として含め納品までに ST 評価及び ST 確認を受けさせることになる。

十　部局技術責任者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスから保護するとともに、バックアップを取得すること。

解説：ソフトウェア開発者が悪意を持って脆弱性を持つソースコードを組み込んでし

まうことを防ぐための変更管理や、ソースコードが流出することを防ぐための閲覧制限のためのアクセス制御、ソースコードの滅失及びき損等に備えたバックアップの取得等を求める事項である。

十一　部局技術責任者は、情報セキュリティの観点からコーディングに関する規定を整備すること。

解説：ソフトウェア開発者が意図せずに脆弱性の存在するソフトウェアを作成してしまわないように、ソフトウェア開発者が実施するコーディングに関する規定を定めるように求める事項である。

「コーディングに関する規定」とは、コードの可読性の向上や記述ミスの軽減のため、ソフトウェア開発担当者間のコードの記述スタイルのガイドラインとして、使用を控える構文、使用禁止語等を定めたいわゆるコーディング規約に相当する規定を指す。例えば、バッファオーバーフローによる情報の改ざんを防ぐために、データを更新する処理を実行する場合には、そのデータ量が適正であることを確認する処理を付加することを義務付ける等の規定が挙げられる。

十二　部局技術責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの必要性の有無を検討し、必要と認めたときは、ソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。

解説：ソースコードレビューの範囲及び方法について定めることを求める事項である。

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、これらについては静的解析ツール、又はソースコードレビュー等による検証が挙げられる。

なお、ソースコードレビューについては、開発するソフトウェア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。

十三　部局技術責任者は、セキュリティの観点から実施する試験の必要性の有無を検討し、必要と認めたときは実施する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。

解説：セキュリティの観点から必要な試験がある場合にその試験の項目及び試験方法を定めることを求める事項である。攻撃が行われた際にソフトウェア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、バッファオーバーフローが発生しないか、想定の範囲外のデータの入力を拒否できるか、DoS 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、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、ソフトウェアの試験計画全般について、セキュリティホールの有無、必要なチェック機能の欠如等について、単体試験、結合試験、統合試験等の複数の試験を通じて、必要な試験が網羅されるよう留意することが望ましい。

十四　部局技術責任者は、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：「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、セキュリティホールを発見した場合の対処に利用できるようにすることを求める事項である。

B2101-83　（ソフトウェア開発に係る規定の遵守）（政府機関統一管理基準の対応項番 1.5.2.3(2)）

第八十三条　部局技術責任者は、ソフトウェア開発に係る規定に基づいて、ソフトウェアの開発を行うこと。

解説：ソフトウェア開発を行う部局技術責任者が、本学で整備したソフトウェア開発に係る規定を遵守して、ソフトウェアの開発を行うことを定めた事項である。

第四節　主体認証・アクセス制御・権限管理・証跡管理・保証等の標準手順

解説：情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

一方、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。また、主体認証情報の機密性と完全性、及びアクセス制御情報の完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。

これらのことを勘案し、本節では、主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準として、全学実施責任者による主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備、部局総括責任者及び部局技術責任者による当該規定の遵守、部局技術責任者による取得した証跡の点検、分析及び報告についての遵守事項を定める。

なお、「B2101 情報システム運用・管理規程」第 8 章において識別コードと主体認証情報の管理等に関する判断基準を、「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 章第 1 節～第 5 節においても主体認証・アクセス制御・権限管理・証跡管理・保証等の導入等に関する対策基準を定めている。

B2101-84　（主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備）（政府機関統一管理基準の対応項番 1.5.2.4(1)）

第八十四条　全学実施責任者は、本学における主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定を、以下の事項を含めて定めること。

解説：本遵守事項では、全学実施責任者が部局総括責任者及び部局技術責任者に求める規定を整備することとしているが、別途規定を整備することはせずに、「B2101 情報システム運用・管理規程」内において部局総括責任者及び部局技術責任者に対する遵守事項として第 1 号～第 6 号の事項を直接定める方法も可

能である。ただし、後者の方法では、自己点検の対象が全学実施責任者ではなく部局総括責任者及び部局技術責任者となることに留意すること。

一　部局技術責任者は、全ての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要があると判断すること。

解説：主体認証を行う前提として、部局技術責任者に、各情報システムについて、アクセスする主体の主体認証を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、主体認証を行う必要があると判断すること。

二　部局技術責任者は、全ての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。

解説：アクセス制御を行う前提として、部局技術責任者に、各情報システムについて、アクセス制御を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、アクセス制御を行う必要があると判断すること。

なお、アクセス制御方式やセキュリティに配慮した OS に関する用語の解説については、内閣官房情報セキュリティセンターによる「電子政府におけるセキュリティを配慮した OS を活用した情報システム等に関する調査研究」を参照のこと。

http://www.nisc.go.jp/inquiry/pdf/secure_os_2004.pdf

三　部局技術責任者は、全ての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。

解説：権限管理を行う前提として、部局技術責任者に、各情報システムについて、アクセスする主体の権限管理を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、権限管理を行う必要があると判断すること。

なお、アクセス制御は、主体から客体へのアクセス条件を制限することで客体に対してのアクセス許可を管理することである。それに対して、権限とは、主体に付与（発行、更新及び変更を含む。以下この節において同じ。）される許可のことをいい、権限管理とは、主体に対する許可情報を管理することである。その主体が情報システムの管理を担う場合には、その主体に対して管理者権限を与える場合もある。

四　部局総括責任者は、全ての情報システムについて、証跡管理を行う必要性の有無を検討すること。

解説：証跡管理を行う前提として、部局総括責任者に、情報システムについて、証跡管理を行う必要性の有無を検討することを求める事項である。

情報セキュリティは、本学の内部及び外部からの不正アクセス、不正侵入、誤操作又は不正操作等の様々な原因により損なわれることがある。

また、教育研究事務の遂行以外の目的でウェブの閲覧や電子メールの送受信がなされることもある。万一問題が発生した場合にはその実行者を特定する必要があるため、一連の事象を情報システムで証跡として取得し、保存する必要がある。

証跡として多くの情報を取得すれば、事後追跡及び事前抑止の効果は高まる。その反面、多くの証跡を取得する場合には、情報システムの処理能力及び記憶容量を多く消費することになる。部局総括責任者は、この両面に配慮し、また情報システムの重要度や取り扱う証跡管理情報の機密性も考慮して、証跡として取得する情報と、証跡を取得する箇所を決定する必要がある。

証跡には、以下のような管理記録が考えられる。

・識別コードの発行等の管理履歴

・各識別コードへのアクセス権設定の管理履歴

・それらの権限管理者の許認可そのものの管理履歴

また、証跡として、上記の他に以下のような利用記録や監視記録等を含めることも考えられる。

・利用者による情報システムの操作記録

・操作する者、監視する者及び保守する者等による情報システムの操作記録

・ファイアウォール、侵入検知システム（Intrusion Detection System）等通信回線装置の通信記録

・プログラムの動作記録

なお、証跡管理を行う必要性の有無の判断に当たっては、情報システムの側面だけではなく、組織的な側面からの検討も必要であるため、部局総括責任者によるものとしている。

五　部局総括責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡として取得する情報項目及び証跡の保存期間を定めること。

解説：証跡を取得する場合に、取得する情報項目及び証跡の保存期間を適切に定めることを求める事項である。

以下に示す例は一般的に取得すべき基本的な情報項目であるが、限られた情報量で実効性のある証跡を取得するように設計することが重要である。

証跡に含める情報項目の例：

・事象の主体である者又は機器を示す識別コード等

・事象の種類（ウェブサイトへのアクセス、ログオン及びログアウト、ファイルへのアクセス、アプリケーションの起動及び終了、特定の操作指令等）

・事象の対象（アクセスした URL（ウェブアドレス）、ログオンしたアプリケーション、アクセスしたファイル、起動及び終了したアプリケーション、操作指令の対象等）

・日付、時刻

・成功、失敗の区別、事象の結果

・電子メールのヘッダ情報、通信内容

・通信パケットの内容

・操作する者、監視する者及び保守する者等への通知の内容
また、保存期間は、１つの情報システムであっても取得する箇所や情報項目により異なることもあり得る。
情報セキュリティに関する問題を事後に追跡し、また事前に抑止するという証跡管理の目的に照らして、保存期間を定めることになる。

六　部局技術責任者は、証跡を取得する必要があると認められた情報システムにおいては、部局技術担当者及び利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。

解説：証跡の取得等について、あらかじめ部局技術担当者及び利用者等に対して説明を行うことを求める事項である。
取得、保存する証跡には、情報システムの管理者、操作員及び利用者等の行動に関する情報が記録される。そのため、証跡を取得、保存し、事後に参照、点検、分析する可能性があることを、利用者等に説明する必要がある。なお、証跡を証拠として活用する際の正当性を高めるためにも周知することが望ましい。

七　部局技術責任者は、要保護情報を取り扱う情報システムについて、保証のための対策を行う必要性の有無を検討すること。

解説：要保護情報を取り扱う情報システムについて、情報が適切な状態であることを保証するための対策の必要性の有無を検討することを求める事項である。

B2101-85　（主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の遵守）（政府機関統一管理基準の対応項番 1.5.2.4(2)）

第八十五条　部局総括責任者及び部局技術責任者は、本学における主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定に基づいて、情報システムの導入を行うこと。

解説：部局総括責任者及び部局技術責任者が、本学で主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定を遵守して、情報システムの導入を行うことを定めた事項である。

B2101-86　（取得した証跡の点検、分析及び報告）（政府機関統一管理基準の対応項番 1.5.2.4(3)）

第八十六条　部局技術責任者は、証跡を取得する必要があると認められた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析することの必要性の有無を検討し、必要と認めたときは、当該措置を講じ、その結果に応じて必要な情報セキュリティ対策を講じ、又は部局総括責任者に報告すること。

解説：取得した証跡を用いて、定期的に又は何らかの兆候を契機に点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講ずることにより、情報セキュリティを維持し、あるいはその侵害を早期に検知することを求める事項である。
取得した証跡は、その全てを定期的に精査することは一般には困難であり、その一部を重点あるいは指標として点検及び分析することが有効である。重点項目の内容と証跡の量を定期的に点検し、その範囲で通常とは異なる状況が見ら

れた場合に更に詳細な点検及び分析を行うことも考えられる。
証跡の点検、分析及び報告を支援するための自動化機能が設けられていれば、これを利用することにより、作業を効率的かつ確実に行うことができる。
情報セキュリティの侵害が特定された場合は、復旧及び再発防止のために必要な対策を採らなければならない。

第五節　暗号と電子署名の標準手順

解説：情報システムの利用において、当該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には、情報の暗号化及び電子署名を行うことが有効な対策となりうるが、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップについては、様々な選択肢があり得ることから、利用者等による個別判断で選択されることのないよう、本学で標準となる手順を定めることが重要である。
これらのことを勘案し、本節では、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップの標準手順に関する対策基準として、全学実施責任者による暗号と電子署名に係る規定の整備、利用者等による当該規定の遵守についての遵守事項を定める。
なお、「B2101 情報システム運用・管理規程」第 11 章第 4 節において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する判断基準を、「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 章第 1 節～第 5 節においても各機能の導入等に関する対策基準を定めている。

B2101-87　（暗号と電子署名に係る規定の整備）（政府機関統一管理基準の対応項番 1.5.2.5(1)）

第八十七条　全学実施責任者は、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を、以下の事項を含めて定めること。

一　電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。

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、電子政府推奨暗号リストに記載されたアルゴリズムを使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。

解説：学内の情報システムにおける暗号化及び電子署名について、使用を認めるアルゴリズム及び方法を全学実施責任者が定めることを求める事項である。アルゴリズム及び方法は、暗号及び電子署名の使用場面等に応じて整備することも可能である。例えば、電子メールの暗号化に関してアルゴリズムを定めるとともにその方法を S/MIME とし、ウェブサーバとブラウザの通信の暗号化に関してアルゴリズムを定めるとともに方法を SSL とする。他に、データベースのデータ暗号化や、電子申請における電子署名等についても、アルゴリズム及び方法を定めることが考えられる。
利用者等は、文書の作成、電子メールの送受信等に汎用のソフトウェアを日常

的に使用しているが、これらのソフトウェアでは、暗号化及び電子署名について、複数のアルゴリズムを用意し、設定画面等で利用者等が選択できるようにしている場合がある。そのような場合には、利用者等は、第１号にもとづき電子政府推奨暗号リストに記載されたアルゴリズムを選択して使用することになる。

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、部局技術責任者は、本遵守事項に基づき全学実施責任者が定めたアルゴリズム及び方法を使用する。

暗号化又は電子署名を行う特定の箇所について見ると、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、複数のアルゴリズムを実装し、使用可能とする場合がある。この場合には、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、電子政府推奨暗号リストに記載されたアルゴリズムを少なくとも一つ含めることを求める。

暗号化の強弱は方式によって異なり、暗号化技術の進歩があるので、常に最新の情報を確認して運用する必要がある。なお、本学における検証済み暗号リストを作成する場合には、安全性も含めたその理由を明確にしておくことや、誰がそのように判断したかについても明確にしておく必要がある。

三　アルゴリズムが危殆化した場合の緊急対応計画の必要性の有無を検討し、必要と認めたときは、緊急対応計画を定めること。

解説：アルゴリズムが危殆化した場合に備えて、情報システムの停止等の緊急避難的な対応計画を策定することを求める事項である。対象となるアルゴリズムは、用途に応じて変わることに留意すること。

２　全学実施責任者は、暗号化された情報（書面を除く。以下この節において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の第一号から第三号の手順（以下「鍵の管理手順等」という。）を定めること。

一　鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等

解説：鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等を定めることによって、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の適正な管理を求める事項である。

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、その適切な運用管理が重要である。なお、オペレーティングシステムに標準搭載されている暗号化又は電子署名付与の機能を使用する場合や、パッケージソフトを使用する場合に、鍵の生成手順や有効期限等が定められている時は、安全性を検討の上、これを準用することが可能である。

また、電子署名の有効期限については、当該有効期限満了までの間、その正当性を検証可能なものとする必要がある。

二　鍵の保存手順

解説：鍵の保存手順を保存方法及び保存場所を含めて定めることによって、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の適正な管理を求める事項であ

る。
鍵の保存方法としては、電磁的記録媒体に保存することが考えられるが、それをどのように保存するかの方法や、保存する際に電磁的記録媒体以外の記録媒体と併用することの是非等についても定める必要がある。
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、その適切な運用管理が重要である。なお、オペレーティングシステムに標準搭載されている暗号化又は電子署名付与の機能を使用する場合や、パッケージソフトを使用する場合に、鍵を保存する電磁的記録媒体や保存場所が定められている時は、安全性を検討の上、これを準用することが可能である。
情報システム共通として鍵の保存手順を定める場合には、全学実施責任者が直接それを定めることが考えられる。あるいは、情報システムごとに鍵の保存手順を個別に定めるのであれば、各部局技術責任者にそれを定めさせることについて、定めるという方法でもよい。

三　鍵のバックアップ手順

解説：暗号化された情報の復号に用いる鍵の紛失及び消失に備え、鍵のバックアップ手順等を定めることを求める事項である。
鍵のバックアップ手順については、バックアップが必要な鍵とバックアップしてはならない鍵の区別を明確にし、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預託手順等を定める。
例えば、復号に用いる鍵を紛失し、又は消失した場合には、それ以前に暗号化した情報を復号できなくなる。そのため、鍵情報のバックアップを取得したり、信頼できる第三者へ鍵情報を預託したりする等の鍵のバックアップ対策が必要である。ただし、鍵情報の複製は、その漏えいに係るリスクを増大させる可能性があるため、最小限にとどめること。
なお、本遵守事項における鍵のバックアップ手順は、前号の鍵の管理手順等に含めて整備することも可能である。
なお、バックアップしてはならない鍵のタイプについては、例えば、乱数を生成するために用いられる鍵や暗号化に用いる鍵の共有を目的として一度だけ使用される鍵等が考えられる。また、米国国立標準技術研究所（NIST）が発行している文書「SP800-57」を参考とすることも考えられる。

3　全学実施責任者は、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全国大学共同電子認証基盤（UPKI）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：情報システムにおいて電子署名を生成するに当たり、当該電子署名の検証に使用可能な電子証明書を UPKI が発行している場合には、それを使用することを求める事項である。このような電子証明書には、サーバ証明書、コード署名証明書等がある。
なお、UPKI 以外で使用している電子証明書が有効期限内の場合、次期更新時には、UPKI で発行している電子証明書を使用するように求めることも考えら

れる。

B2101-88　（暗号と電子署名に係る規定の遵守）（政府機関統一管理基準の対応項番 1.5.2.5(2)）

第八十八条　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。

解説：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、本学で定めたアルゴリズム及び方法を遵守することを求める事項である。

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。

解説：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が露呈した場合、暗号化された情報の漏えいや電子署名の偽造等のおそれがある。そのため、利用者等による鍵情報の保護を求める事項である。

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：鍵の書換え、紛失、消失等により、その完全性、可用性が侵害された場合には、暗号化により保護されている情報を復号することが困難となり、可用性が損なわれる可能性がある。そのため、利用者等による鍵のバックアップを求める事項である。

第六節　学外の情報セキュリティ水準の低下を招く行為の防止

解説：本学が、学外の情報セキュリティ水準の低下を招くような行為をすることは、学外に対して適切な行為でないことは当然であって、その行為が他者の情報セキュリティ水準を低下させることによって、本学を取り巻く情報セキュリティ環境を悪化させるため、本学にとっても好ましくない。

これらのことを勘案し、本節では、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対策基準として、全学実施責任者による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の整備、利用者等による当該規定の遵守についての遵守事項を定める。

B2101-89　（措置についての規定の整備）（政府機関統一管理基準の対応項番 1.5.2.6(1)）

第八十九条　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こと。

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可能性のある行為としては、例えば、以下のものが挙げられる。

（ア）不適切なソフトウェア及びサービスの使用要求：情報サービス（例えば、本学のウェブによるコンテンツの提示等を言う。以下同じ。）を利用するために、脆弱性の問題が指摘されているソフトウェア及びサービスの使用（脆弱性の問題が指摘されているソフトウェア及びサービスのインストールや脆弱性の問題

が指摘されているバージョンへの変更による使用を言うが、脆弱性の問題が改善されているソフトウェア及びサービスへの変更ができないことによる使用継続を含む。）を暗黙又は明示的に要求する行為。
（イ）ソフトウェアの不適切な設定要求：情報サービスを利用するために、利用者の環境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、クライアント PC の OS やウェブブラウザ等）以下同じ。）について、セキュリティ設定の下方修正を暗黙又は明示的に要求する行為。
（ウ）ソフトウェア等の不適切な削除要求：本学のウェブのコンテンツを利用するために、利用者のセキュリティ対策に必要なソフトウェアやハードウェア等の無効化や削除を暗黙又は明示的に要求する行為。

「明示的に要求する行為」とは、「『このような設定を変更してください。』等のように明記すること」であるが、「暗黙に要求する行為」とは、「『このサービスを利用するためには、このような設定が必要です。』と婉曲に記載すること」だけではなく、何も記載しなくとも「結果的にそのような設定変更をしないと利用を継続できないような状態でサービスを提供すること」も含む。
以下のような場合に、暗黙の要求になることがあるので、注意する必要がある。
・ソフトウェアを実行させる場合：情報サービスのためのソフトウェアを実行させる場合に注意する必要がある。それらを大別すると、単独実行型（例えば、Windows の「.exe」ファイル等）、ランタイム環境実行型（例えば、Java アプレットや Windows の ActiveX ファイル等）、クライアントソフト内実行型（例えば、JavaScript やファイル中のマクロ等）があるが、これらの全てを含む。
・HTML メール等を送信する場合：本学から HTML メール等（利用者がセキュリティ上の理由から受信側のメールサーバやメールクライアントで処理を制限していることが想定されるメール文書形式を用いたメールのこと。）を送信する場合に注意する必要がある。

これらの場合については、結果的に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。実行させるソフトウェアの提供については、オンラインによる提供（ウェブへの掲載、メールの添付等）について特に注意して規定を整備する必要がある。その際に大別した種類ごとに整備しても構わない。例えば、単独実行型ファイルについてはオンライン提供の原則禁止、ランタイム環境実行型については電子署名を付けることの義務付け、HTML メール等の送信については受信者の事前同意を得た場合のみの送信と不同意者への別方式の送信手段の提供の義務付け等が考えられる。
やむをえず、単独実行型ファイルをオンライン提供する必要が生じた場合は、電子署名を付けることを義務付けること。
また、オンラインによる提供だけでなく、外部電磁的記録媒体を介したオフラインによる提供の場合も同様に考慮する必要がある。

ソフトウェアを提供する者は、ソフトウェアの動作や脆弱性に十分注意して署名を付与する必要がある。
また、オンライン又はオフラインでソフトウェアを提供する際に、ソフトウェアに対する署名（コード署名）が必要な場合には、全国大学共同電子認証基盤（UPKI）で発行したコード署名証明書を利用することが望ましい。
なお、正当な署名が付与されたソフトウェアに対しては、ユーザの確認なしに、端末上の機能が当該ソフトウェアに利用される場合があることに注意すること。
（ア）（イ）については、当該情報サービスの準備をした時点では、脆弱性の問題が指摘されていなくても、運用開始後に指摘される場合もある。そのような場合にも脆弱性を回避するための選択を利用者ができるように努めなければならない。回避に必要な当該情報サービスで用いるウェブのコンテンツやアプリケーション等の是正を容易にできるような準備や設計について規定を整備する必要がある。「容易にできる」とは、追加の予算措置を講じなくてもよい程度であり、運用担当者による変更ができるか、是正開発作業を保守費用の範囲に含める等の方法を考えることができる。
例えば、本学のウェブのアプリケーションを利用するために、利用者の PC 上にあらかじめ標準的にインストールされているソフトウェアがバージョン A であったとする。その後、そのソフトウェアの最新バージョンが B に更新され、また、バージョン A について脆弱性が公開された場合には、バージョン B で当該アプリケーションを利用できるようにしなければならない。このとき、当該アプリケーションがそのソフトウェアのバージョン A だけで動作するような設計では、利用者に脆弱性のあるバージョン A を利用することを暗黙に要求してしまうことになる。そのような場合に適切な対処（バージョン B でも当該アプリケーションを利用できるようにする等）を容易に実施できるように、設計内容又は業者との保守契約内容等について検討しておくことが重要である。
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で動作するように、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等、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。

「B1001 情報システム運用基本規程」第 20 条及び「B2101 情報システム運用・管理規程」第 89 条に基づいて全学総括責任者が整備した規定が、「B3211 学外情報セキュリティ水準低下防止手順」である。

B2101-90　（措置についての規定の遵守）（政府機関統一管理基準の対応項番 1.5.2.6(2)）

第九十条　利用者等は、学外の情報セキュリティ水準の低下を招く行為の防止の規定に基づいて、必要な措置を講ずること。

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本学の役割を定めた事項である。利用者等は、組織及び個人として措置を講ずることが重要である。

第七節　ドメイン名の使用についての対策

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ーバ、電子メール等を用意し、一般の利用に供している。これらのサービスはインターネットを介して利用するものであるため、一般利用者にとっては、そのサービスが実際の本学のものであると信頼できることが重要である。一方、インターネット上のサービスの特定はドメイン名（例えば、example.ac.jp のこと。）が重要な役割を果たしており、本学において一貫したドメイン名を使用することにより、万一学外の者による悪用や詐称がなされた場合にも一般利用者が気付くための条件を整備する必要がある。

これらのことを勘案し、本節では、本学におけるドメイン名の使用に関する対策基準として、全学実施責任者によるドメイン名の使用についての規定の整備、教職員等による当該規定の遵守についての遵守事項を定める。

B2101-91　（ドメイン名の使用についての規定の整備）（政府機関統一管理基準の対応項番 1.5.2.7(1)）

第九十一条　全学実施責任者は、ドメインネームシステムによるドメイン名（以下「ドメイン名」と言う。）の使用について、以下の事項を教職員等に求める規定を整備すること。

解説：本遵守事項では、全学実施責任者が教職員等に求める規定を整備することとしているが、別途規定を整備することとはせずに、「B2101 情報システム運用・管理規程」内において教職員等に対する遵守事項として第 1 号～第 3 号の事項を直接定める方法も可能である。ただし、後者の方法では、自己点検の対象が全学実施責任者ではなく教職員等となることに留意すること。

一　教職員等は、学外の者に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、以下のＡ大学のドメイン名であることが保証されるドメイン名（以下「Ａ大学ドメイン名」という。）を使用すること。

・example.ac.jp で終わるドメイン名

ただし、電子メール送信又はＡ大学ドメイン名のウェブページでの掲載に限り以下の条件を満たす場合には、Ａ大学ドメイン名以外のドメイン名を本学以外のものとして告知してもよい。

具体的には、電子メールの送信においては以下の条件を全て満たすことが必要である。

・告知内容についての問い合わせ先としてＡ大学ドメイン名による電子メールアドレスを明記しているか、又はＡ大学ドメイン名による電子署名をしていること。

・告知するドメイン名を管理する組織名を明記すること。
・告知するドメイン名の有効性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していること。
また、Ａ大学ドメイン名のウェブページでの掲載においては以下の条件を全て満たすことが必要である。
・告知するドメイン名を管理する組織名を明記すること。
・告知するドメイン名の有効性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していること。

解説：「.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。

アクセスさせることを目的にドメイン名を告知するとは、ウェブサイト（例えば、http://www.example.ac.jp/）や FTP サーバ（例えば、ftp://ftp.example.ac.jp/）等へのアクセスを促すことをいう。上記には、ウェブページの閲覧に必要なソフトウェア（プラグインを含む）を入手できるＡ大学ドメイン名以外のウェブサイトを告知する場合も含む。また、送信させることを目的にドメイン名を告知するとは、電子メールの宛先（例えば、null@example.ac.jp）への送信等を促すことをいう。

本遵守事項における告知にあたる場合とは、情報提供のきっかけが本学側にある場合で、告知にあたらない場合とは、情報提供のきっかけが本学側にない場合である。例えば、学外の者からの問い合わせに回答する場合は、問い合わせがきっかけであるので、告知にはあたらず、本遵守事項の対象とはならない。

なお、いずれの場合についても媒体の種類（郵送、電話、電子メール送信、ウェブ掲載、ポスター掲示等）を問わない。

「告知する場合に」としているが、実際には「告知内容を検討する際に告知するドメイン名を決める時点で」実施しなければならない遵守事項である。

なお、海外拠点のように国外在住の者を対象とし、かつ、現地のルールに従うことが適切であると考えられる場合には、この限りではない。これらドメイン名の使用については、本学ウェブサイト等において確認できるよう措置されることが適当である。

Ａ大学ドメイン名以外のドメイン名を告知してもよい条件を満たす記載の例としては、以下のようなものが考えられる。

（例）

・この告知についてのお問い合わせは、null@example.ac.jp までご連絡ください。

・この告知で案内しているウェブサイトは○○○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。

・この告知で案内しているウェブサイトのアドレスについては、2013 年 5 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。

二　教職員等は、学外の者に対して、送信に使用する電子メールのドメイン名は、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、当該教職員等が既知の者である場合を除く。

解説：送信に使用する電子メールのドメイン名としてA大学ドメインの使用を求める遵守事項である。

また、電子メールの送信元としてA大学ドメイン名を使用するに当たっては、その送信に用いる電子メールサーバは、当該A大学ドメイン名にかかる DNS サーバの MX レコードで指定している IP アドレスのサーバでなければならないとする厳格な考え方もある。

なお、送信元として使われる電子メールアドレスを外部に告知する場合には、適切なドメイン名で告知するように、事前に準備する必要がある。

三　教職員等は、学外の者に対して、アクセスさせることを目的として教育研究事務の遂行に係る情報を保存するためにサーバを使用する場合には、A大学ドメイン名のサーバだけを使用すること。

解説：学外の者にアクセスさせることを目的として情報を保存するサーバとは、主としてウェブサーバのことをいう。

第 1 号によりA大学ドメイン名以外のドメイン名を告知することを禁止しているが、告知していなくとも、本学としての情報をA大学ドメイン名以外のドメイン名のウェブサーバに保存していると、インターネット上の検索サービス等により表示される場合がある。そのような場合には、なりすましをしようとする者が、本学からの情報を装った内容を保存したウェブを作成して、検索されるのを待ち伏せするという方法によるなりすましが考えられる。普段からA大学ドメイン名のウェブサーバだけを使うことで、検索結果がA大学ドメイン名以外である場合に、そこに保存されている情報の真偽について学外の者が注意を心がけやすくできる。

なお、既存のウェブサーバ等においてこれら以外のドメイン名のサーバの使用が避けられない場合には、本遵守事項に対する例外措置を必要な期間に限り適用し、かつ、A大学ドメイン名のサイトから当該ドメイン名を案内することにより、新規に告知するドメイン名について第 1 号を遵守すること。

また、A大学ドメイン名以外のウェブサーバの使用を停止した後も、当該ドメイン名を不正に利用されないように管理することに注意しなければならない。

具体的には、そのような用途に使用した当該ドメイン名については、使用後も

登録管理を一定期間維持することを求める規定を設ける必要がある。

B2101-92　（ドメイン名の使用についての規定の遵守）（政府機関統一管理基準の対応項番 1.5.2.7(2)）

第九十二条　教職員等は、ドメイン名の使用についての規定に基づいて、必要な措置を講ずること。

解説：全ての教職員等が、インターネットを経由した教育研究事務に係る情報の提供に当たり、本学で整備したドメイン名の使用についての規定を遵守して、A大学ドメイン名等のドメイン名を適切に使用することを定めた事項である。
なお、ウェブサイトの構築・管理等の「ドメイン名の使用」を伴う業務を外部委託する場合は、教職員等が委託先への要求事項に含める必要がある。
そのような業務の外部委託は、情報システム部門以外の者が担当となる場合があるため、それらの者にも本遵守事項を周知すること。

第八節　不正プログラム感染防止のための日常的実施事項

解説：不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の要機密情報を漏えいさせることから機密性に対する脅威ともなる。また、他の情報システムへ感染を拡大させるなど、セキュリティ脅威の原因となり得る。
不正プログラムへの感染を防止するためには、情報システムを利用する全ての利用者等が、アンチウイルスソフトウェア等を活用して不正プログラムの検知・除去に努めるほか、ファイルの閲覧や実行、外部ファイルの取り込み等において十分な注意を払う必要がある。
これらのことを勘案し、本節では、不正プログラム感染の回避を目的とした対策基準として、全学実施責任者による不正プログラム対策に係る規定の整備、利用者等による当該規定の遵守について遵守事項を定める。

B2101-93　（不正プログラム対策に係る規定の整備）（政府機関統一管理基準の対応項番 1.5.2.8(1)）

第九十三条　全学実施責任者は、不正プログラム感染の回避を目的として、以下の措置を利用者等に求める規定を整備すること。

解説：本事項では、全学実施責任者が利用者等に求める規定を整備することとしているが、別途規定を整備することとせずに、「B2201 情報システム利用規程」内において直接に利用者等に対する遵守事項として第 1 号～第 7 号の事項を定める方法も可能である。ただし、後者の方法では、自己点検の対象が全学実施責任者ではなく利用者等となることに留意すること。

一　利用者等は、アンチウイルス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ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

解説：不正プログラムに感染したソフトウェア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、復旧に労力を要するため、不正

プログラムとして検知された実行ファイル等の実行を禁止する事項である。
なお、アンチウイルスソフトウェア等が全ての現存する不正プログラムを検知できるとは限らないことに留意し、あわせて必要な予防措置を行うことが望ましい。予防措置とは、例えば、不審な添付ファイルは差出人が判明している場合でも実行しないこと、差出人が判明している場合には相手に確認すること、ウェブクライアントのセキュリティ設定を不必要に低下させないこと、不審なウェブサイトを閲覧しないこと等である。

二　利用者等は、アンチウイルス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こと。

解説：アンチウイルス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最新化することで、不正プログラム等の検知漏れによる感染を回避することを求める事項である。
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。ただし、利用に当たってはアンチウイルスソフトウェア等を自動更新する情報システムが提供するサービスの内容、当該アンチウイルスソフトウェア等に不具合が含まれていた場合に影響が及ぶ範囲、自動更新しない場合に不正プログラムに感染するリスクが高まること等を勘案すべきである。
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、部局総括責任者が適切な方法を選択すること。同様に第 3 号～第 5 号の事項は、部局総括責任者が適切な方法を選択すること。

三　利用者等は、アンチウイルス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こと。

解説：人為による対策の漏れや遅れを回避するために、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を求める事項である。
ファイルの作成、参照等のたびに検査を自動的に行う機能をオンに設定し、その機能をオフにしないことが必要である。

四　利用者等は、アンチウイルスソフトウェア等により定期的に全ての電子ファイルに対して、不正プログラムの有無を確認すること。

解説：定期的に不正プログラムの有無を確認することを求める事項である。
前事項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、定期的に全ての電子ファイルを検査する必要がある。

五　利用者等は、外部からデータやソフトウェアを電子計算機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。

解説：外部とやり取りするデータやソフトウェアには、ウェブの閲覧やメールの送受信等のネットワークを経由したもののほか、USB メモリや CD-ROM 等の外部電磁的記録媒体によるものも含む。

不正プログラムの自動検査による確認ができていればそれで差し支えない。

六　利用者等は、不正プログラム感染の予防に努めること。

解説：不正プログラム感染の予防に役立つ措置の実施を求める事項である。アンチウイルスソフトウェア等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に注意して、例えば、アプリケーションでマクロの自動実行を無効にすることによりマクロウイルスの実行を防ぐことや、ソフトウェアのセキュリティ設定により読み込まれるプログラムやスクリプトの実行を無効にすること、安全性が確実では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こと等がある。

七　利用者等は、不正プログラムに感染したおそれのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講ずること。

解説：不正プログラムに感染したおそれがある電子計算機については、他の電子計算機への感染等の被害の拡大を防ぐために、当該電子計算機が通信回線に接続している場合には、それを切断して、必要な措置を講ずることを求める事項である。切断後に必要となる措置としては、例えば、不正プログラムの有無を検知して駆除することや、「B2101 情報システム運用・管理規程」第 3 章第 2 節（インシデント対応）に定められた連絡等をすることが挙げられる。

B2101-94　（不正プログラム対策に係る規定の遵守）（政府機関統一管理基準の対応項番 1.5.2.8(2)）

第九十四条　利用者等は、定められた不正プログラム対策に係る規定に基づいて、不正プログラムの感染を防止するための対策を行うこと。

解説：全ての利用者等が、不正プログラム対策に係る規定に基づき、不正プログラムの感染を防止するための対策を行うことを定めた事項である。

B2102 情報システム運用リスク管理規程

B2102-01（目的）

第一条　この規程は、情報システム運用基本方針及び運用基本規程（以下「ポリシー」という。）に基づき本学情報システムの運用におけるリスクを分析し、必要な対策を立て、情報セキュリティを確保することを目的とする。

B2102-02（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　機密性(Confidentiality)　アクセス権を持つ者だけが、情報にアクセスできることを確実にすること。

二　完全性(Integrity)　情報及び処理方法が正確であること及び完全であることを保護すること。

三　可用性(Availability)　認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

四　その他の用語の定義はポリシーの定めるところによる。

B2102-03（リスク評価手順）

第三条　全学総括責任者は、情報資産の価値と脅威、脆弱性を評価するための情報システム運用リスク評価手順を定める。

解説：リスク管理のため、リスクアセスメントを実施するための手順について、サンプルの「A大学情報システム運用リスク評価手順」に示したリスク分析票のようなリスク評価のチェック項目を定める。

B2102-04（リスク管理）

第四条　全学総括責任者は、全学実施責任者を含む各情報資産の管理者に対して、少なくとも年に一回、リスク管理を次の各号に従って実施し、その結果を報告するよう指示する。

一　当該管理者は、自らが扱う情報資産について情報システム運用リスク評価手順に基づきリスク評価を行う。

二　当該管理者は、評価結果に従い、リスクに対する事前の対策を必要とするものについてその具体策を定め、あるいはトラブルが発生した場合の具体的な対応について当該情報資産についてのインシデント対応手順を定める。対策を施さないと判断したものについても報告する。

三　全学総括責任者は、報告に基づいて、ポリシー及び実施規程等の見直しを行う。

解説：リスク管理のため、定期的なリスク評価と対応手順などの策定を行うことと、この結果により定期的な見直しを実施する。

B2103 情報システム非常時行動計画に関する規程

B2103-01（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。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「B3103 インシデント対応手順」に書くことにしている。

B2103-02（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。

B2103-03（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。

B2103-04（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。

B2103-05（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。

B2103-06（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「B3103 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。

B2103-07（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。

B2104 情報格付け基準

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、秘密文書に相当する機密性を要する情報
機密性２情報	本学で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報
機密性１情報	機密性２情報又は機密性３情報以外の情報

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

B2151 情報セキュリティ要件の明確化に関する技術規程

第一章　情報セキュリティについての機能

第一節　主体認証機能

解説：情報システムの利用においては、主体認証により、電子計算機を利用した者を特定することが可能となる。サーバ装置や複数の者が利用する共用 PC 等の端末の場合、利用者に識別コードを個別に割り当て、本人性を確認することが望ましい。情報システムに主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

これらのことを勘案し、本節では、主体認証機能の導入に関する対策基準を定める。

また、本学が有する各情報システムの利用者は、本学の教職員等及び学生等のほか、それ以外の者がある。例えば、学外向けのサービスを提供する情報システムの利用者は、学外の者である場合がある。識別コードと主体認証情報については、このような利用者の別にかかわらず保護すべきであるが、学外の者は本規程及び「B2101 情報システム運用・管理規程」の適用範囲ではないため、それらの者に対しては、これを保護するよう注意喚起することが望ましい。

なお、「B2101 情報システム運用・管理規程」第 8 章第 1 節において識別コードと主体認証情報の管理等に関する対策基準を、「B2101 情報システム運用・管理規程」第 11 章第 4 節において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

B2151-01　（主体認証機能の導入）（政府機関統一技術基準の対応項番 2.2.1.1(1)）

第一条　部局技術責任者は、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、識別及び主体認証を行う機能を設けること。

解説：識別のための機能を設けることが技術的にできない情報システム（識別コード自体が存在せず、主体認証情報（パスワード）の設定のみ可能であるような装置等）は、例外措置として判断されることになる。その場合には、識別されないことによる影響について勘案し、必要に応じて代替あるいは追加の措置を講ずる必要がある。

主体認証の方式として、知識、所有、生体情報の 3 つの方法が代表的である。「知識」による主体認証とは、パスワード等、本人のみが知り得る情報を提示することにより、検証する方法である。「所有」による主体認証とは、IC カード等、本人のみが所有する機器等を主体認証処理に介在させることにより、検証する方法である。「生体情報」による主体認証とは、指紋や虹彩等、本人の生体的な特徴により、検証する方法である。生体情報による主体認証を用いる場

合には、その導入を決定する前に、この方式特有の誤認率と誤否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。この方式では、正当な本人に対して、本人の非によらない理由で、主体認証が正しくできなくなる場合があることを想定し、そのような場合の教育研究事務の遂行への影響について検討してから導入を決定すること。

なお、本項における解説としては上記３つの方式について記述するが、その他、位置情報等による方式もある。

機微な情報へのアクセスであれば、本人であっても主体認証が解決できるまでアクセス不可能でよいとするか、あるいは、別の方式と組み合わせる等について考慮するとよい。

２　部局技術担当者は、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、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。

一　主体認証情報を保存する場合には、その内容の暗号化を行うこと。

二　主体認証情報を通信する場合には、その内容の暗号化を行うこと。

三　保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更及び提供（入力）させる際に、暗号化が行われない旨を通知すること。

解説：主体認証情報の保存や通信を行う際に暗号化できない場合には、利用者は他の情報システムで用いていない主体認証情報を設定すべきである。その旨を利用者が判断できるように通知しなければならない。

保存又は通信を行う際に主体認証情報を暗号化できない情報システムでは、主体認証情報が漏えいする危険性がある。もしも、そのような問題が生じた場合に、そこで使われていた主体認証情報と同じものが他の情報システムでも使われた場合には、暗号化できる情報システムにおいても、不正に使われてしまうという二次被害を招きかねない。その危険性を低減するため、暗号化されない情報システムでの主体認証情報については、他の情報システムで用いていないものを利用者が設定する等の回避策をとる必要がある。そのため、利用者が暗号化されない旨を知る機会を得られるようにしておかなければならない。

したがって、暗号化できない情報システムにおいて、主体認証情報を入力させる際には、例えば、「この情報システムでは入力される情報が暗号化されません。他の情報システムで使用している主体認証情報（パスワード）を入力しないようにしてください。」等の警告を表示するようにすることが必要である。

３　部局技術担当者は、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、利用者等に主体認証情報の定期的な変更を求める場合には、利用者等に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。

一　利用者等が定期的に変更しているか否かを確認する機能

二　利用者等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

解説：定期的な変更を遵守事項とする場合には、それが実施されているか否かを確認できる機能を用意しておく必要がある。

その機能によって確認作業を自動化することが技術的に困難な場合は、例外措置の手続を実施した上で、管理者が定期的にパスワードの変更を促すメールを

利用者等に送信し、利用者等がこれに従ってパスワードを変更した旨を返信することで確認するといった代替措置の適用も考えられる。
なお、生体情報による主体認証方式のように、利用者等本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。

4　部局技術責任者は、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、主体認証情報又は主体認証情報格納装置を他者に使用され、又は使用される危険性を認識した場合に、直ちに当該主体認証情報若しくは主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けること。

解説：主体認証情報自体の露呈、主体認証情報に関連する情報の露呈又はそれらが露呈した可能性について報告を受けた場合には、主体認証の停止、識別コードによる情報システムの利用停止のほか、主体認証情報の変更や別の主体認証方式の併用等の対策を講ずること。

5　部局技術責任者は、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、知識による主体認証方式を用いる場合には、以下の機能を設けること。

一　利用者等が、自らの主体認証情報を設定する機能

解説：知識による主体認証方式の場合には、本人による設定を可能にすることによって、以下の利点が期待できる。
・他者に設定された主体認証情報に比べ、本人が設定した主体認証情報の方が容易に記憶できる。
・本人以外の者が主体認証情報を設定する場合には、その設定者によるなりすましが懸念されるが、本人自身が設定することにより、そのおそれが少なくなる。
なお、例えば、運用上の理由等で他者による再設定を認めた場合には、同様に本人になりすますことは可能であるため、主体認証情報（パスワード）変更の通知機能によって、本人に設定が変更されたことについて通知することが望ましい。

二　利用者等が設定した主体認証情報を他者が容易に知ることができないように保持する機能

解説：部局技術責任者であっても、他者の主体認証情報を知ることができないようにする必要がある。部局技術責任者に悪意がなくとも、悪意のある第三者によってその管理者権限が奪取されてしまった場合には、全ての利用者の主体認証情報を知られてしまうおそれがあるため、不可逆の暗号化を用いる等により、部局技術責任者自らも、他者の主体認証情報を知ることができないような措置を講ずる必要がある。

三　主体認証情報を設定する時は、セキュリティ上の強度が指定以上となるように要求する機能

解説：安易な主体認証情報（パスワード）を設定すると、悪意のある第三者によって解読されてしまうため、必要なセキュリティ上の強度を持つようにする必要がある。
セキュリティ上の強度の指定については、次の要素を考慮する必要がある。
・パスワードに用いる文字の種類
・パスワードの桁数

・パスワードの有効期間
・アカウントをロックする方法
・アカウントのロックを解除する方法
・当該情報システムを利用する人数
・当該情報システムへログインする方法
・当該情報システムに保存される情報の格付　等

なお、パスワード等のセキュリティ上の強度に関する設定例については、
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
（各府省情報化統括責任者（CIO）連絡会議決定、2010 年 8 月 31 日）
http://www.kantei.go.jp/jp/singi/it2/guide/index.html
を参考にされたい。

6　部局技術責任者は、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、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項のうちその特性に応じて適用可能な要件を全て満たす主体認証方式を導入すること。

一　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）
二　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）
三　正当な主体が容易に他者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）
四　主体認証情報が容易に複製できないこと。（複製の防止）
五　部局技術担当者の判断により、ログオンを個々に無効化できる手段があること。（無効化の確保）
六　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）
七　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）
八　主体に付与した主体認証情報を使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）

解説：代表的な方式である、知識、所有、生体情報による主体認証方式以外の方法を用いる場合の検討事項を列挙している。セキュリティ上の求められる強度や利便性等も考慮の上、方式を決定することを求める事項である。なお、これらの要件は、必ずしも全て充足することを求めるものではない。例えば、主体認証情報（パスワード）等による「知識」方式の場合には、第 3 号や第 4 号を技術的に充足する必要はない。また、上記各号以外に気づいた事項があれば、適宜追加することが望ましい。

7　部局技術責任者は、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、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。

一　複数要素（複合）主体認証方式で主体認証を行う機能

解説：複数要素（複合）による主体認証方式を用いることにより、より強固な主体認証が可能となる。
これは、単一要素（単一）主体認証方式（「単一要素（単一）主体認証（single factor authentication / single authentication）方式」とは、知識、所有、生体

情報等のうち、単一の方法により主体認証を行う方式である。）の場合には、何らかの理由によって主体認証情報が露呈してしまった際には、不正にログオンされる可能性が非常に高くなってしまうが、複数要素（複合）主体認証方式の場合には、仮に一方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、不正にログオンされる可能性は依然低いと考えられるからである。

二　ログオンした利用者等に対して、前回のログオンに関する情報を通知する機能

解説：識別コードによる前回のログオンに関する情報（日時や装置名等）を通知することで、本人の識別コードが他者によって不正に使われた場合に、本人が気付く機会を得られるようにすることを求める事項である。

三　不正にログオンしようとする行為を検知し、又は防止する機能

解説：通知によって本人が知る機会を得ること及び組織が状況を管理できること等が考えられる。例えば、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、その旨を本人に通知する、あるいは、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（アカウントをロックする）機能の付加が挙げられる。

なお、OS といった一般的に主体認証機能を有する機器やソフトウェア等を調達する場合には、当該機能を有する機器やソフトウェア等を選択することが望ましい。

四　利用者等が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能

解説：通知メッセージの例としては、以下のようなものがある。

・利用者が本学情報システムへアクセスしようとしていること
・情報システムの使用が監視、記録される場合があり、監査対象となること
・情報システムの不正使用は禁止されており、刑法の罰則対象となること

五　利用者等に主体認証情報の定期的な変更を求める場合には、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

解説：一度使用した主体認証情報（パスワード等）の再利用を禁止することを求める事項である。なお、生体情報による主体認証方式のように、利用者等本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。

六　管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能

解説：管理者権限を有した識別コードを管理者グループで共用した場合には、そのログオン記録だけでは、共用している管理者のうち、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。そのため、管理者個人を特定することを目的として、非管理者権限の識別コードを本人に付与した上、その識別コードで最初にログオンした後に限り、管理者権限を有する共用識別コードに切り替えて管理者作業を実施することを可能とする必要がある。

なお、当該情報システムのオペレーティングシステムが Unix 系の場合には、一般利用者でログオンした後に 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 によるログオンを禁止す

る設定により、その手順を強制することができる。

B2151-02　（主体認証機能の変更）

第二条　部局総括責任者は、セキュリティ侵害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。

第二節　アクセス制御機能

解説：主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。

主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。

これらのことを勘案し、本節では、アクセス制御に関する対策基準として、アクセス制御機能の導入、適正なアクセス制御についての遵守事項を定める。

なお、「B2101 情報システム運用・管理規程」第 8 章第 1 節において識別コードと主体認証情報の管理等に関する対策基準を、「B2101 情報システム運用・管理規程」第 11 章第 4 節において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

B2151-03　（アクセス制御機能の導入）（政府機関統一技術基準の対応項番 2.2.1.2(1)）

第三条　部局技術責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設けること。

解説：情報システムの利用者やそのグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式(任意アクセス制御)を利用すること。

なお、「任意アクセス制御（DAC：Discretionary Access Control)」とは、主体が客体に設定したアクセス制御について、その設定がそれ以後継承されるかが任意である方式であり、この方式では、その客体にアクセス許可されている主体が別の客体を作成し複製等する際に、元のアクセス制御を新しい客体のアクセス制御として継承するかは当該主体の任意であり、変更が可能である。

２　部局技術責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。

一　利用者及び所属するグループの属性以外に基づくアクセス制御機能の追加

解説：情報システムの利用者や所属するグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式のほか、情報システムの利用者やそのグループの属性以外に基づくアクセス制御を追加すること。

情報システムの利用者やそのグループの属性に基づくアクセス制御としては、例えば以下の方式が挙げられる。

・アクセス・コントロール・リスト（ACL）制御

情報システムの利用者やそのグループの属性以外に基づくアクセス制御としては、例えば以下の方式が挙げられる。

・利用時間による制御
・利用時間帯による制御
・同時利用者数による制限
・同一 ID による複数アクセスの禁止
・IP アドレスによる端末制限

二　強制アクセス制御機能

解説：強制アクセス制御機能（MAC）の組み込みを導入することを求める事項である。

強制アクセス制御機能を備えたものとして、トラステッド OS やセキュア OS 等で実装したものもある。

なお、強制アクセス制御機能の組み込みを導入した場合、任意アクセス制御機能の組み込みができなくなるが、強制アクセス制御機能の方がより強力な機能のため、前項を遵守していると考えられる。

B2151-04　（適正なアクセス制御）（政府機関統一技術基準の対応項番 2.2.1.2(2)）

第四条　部局技術責任者は、利用者等自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付及び取扱制限に従って、アクセス制御を行うこと。

解説：共有ファイルサーバのアクセス制御のように、情報システムを利用者等が利用する際に、自らがアクセス制御を行うことができない場合、情報システムの導入時及び運用時にアクセス制御を行うことを求めた事項である。例えば、要機密情報であれば、不適当な者から参照されないよう、読み取り制限の属性を付与し、完全性 2 情報であれば、不適当な者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。

また、利用者等自らがアクセス制御を行うことが出来る場合、「B2101 情報システム運用・管理規程」第 52 条第 2 項の規定に基づき対策を行うこと。

アクセス制御の例としては、ウェブサーバに情報を掲載する際に、ユーザ ID とパスワードを付与した者や特定ドメインからの閲覧者に限って公開するよう設定したり、ファイルのアクセス権を設定したりすることが挙げられる。情報の格付けや取扱制限は、情報の作成者又は入手者（「B2104 情報格付け規程」で教職員等としている）が行うが、アクセス制限については情報を取り扱う者、すなわち利用者等が適切に行わなければならない。なお、「B2101 情報システム運用・管理規程」第 3 条において適用範囲から学生を除外した場合、実質的に利用者等は教職員等とほぼ同様となる。

B2151-05　（無権限のアクセス行為の対策）

第五条　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。

第三節　権限管理機能

解説：主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。

これらのことを勘案し、本節では、権限管理に関する対策基準として、権限管理機能の導入、識別コードと主体認証情報の付与管理についての遵守事項を定める。

なお、「B2101 情報システム運用・管理規程」第 8 章第 1 節において識別コードと主体認証情報の管理等に関する対策基準を、「B2101 情報システム運用・管理規程」第 11 章第 4 節において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

B2151-06　（アカウント管理機能の導入）（政府機関統一技術基準の対応項番 2.2.1.3(1)）

第六条　部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。

解説：権限管理を行う機能を設ける必要性があると認められた場合に、当該機能を情報システムに設けることを求める事項である。

２　部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。

一　最少特権機能

解説：管理者権限を持つ識別コードを付与された者が、管理作業をする時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最少特権機能を、情報システムに設けることを求める事項である。

二　主体認証情報の再発行を自動で行う機能

解説：情報システムの利用を開始している主体が、主体認証情報の再発行を要求した場合には、当該情報システムにおいて、その主体により重要な情報が既に作成されている可能性があることから、再発行する主体認証情報を他の者が知り得ないように、新規に主体認証情報を発行する場合に比べて、一層安全な機能を設けることを求める事項である。

なお、再発行を自動化して他の者による操作を必要とすることなく主体認証情報を再発行することは、管理者による不正な操作が発生する機会を減らし、安全性を強化することができる。

三　デュアルロック機能

解説：不正操作及び誤操作を防止するために、情報システムにデュアルロック機能を設けることを求める事項である。デュアルロック機能とは、行為に対して、少なくとも２名の者が操作しなければその行為を完遂できない方式のことである。

B2151-07　（識別コードと主体認証情報の付与管理）（政府機関統一技術基準の対応項番 2.2.1.3(2)）

第七条　権限管理を行う者は、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発行すること。

解説：情報システムにおける識別コード及び主体認証情報は、情報システムを利用する許可を得た主体に対してのみ、本人確認の上で初期発行することが重要である。また、識別コード及び主体認証情報の安全な初期配布方法について求める事項である。

2　権限管理を行う者は、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。

解説：識別コードを利用者に発行する際に共用識別コードか共用ではない識別コードかの別について通知することにより、それらの区別を利用者が独自に判断するようなことを防ぐための事項である。ただし、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。

3　権限管理を行う者は、管理者権限を持つ識別コードを付与（発行、更新及び変更を含む。以下この項において同じ。）する場合は、以下の措置を講ずること。

一　業務又は業務上の責務に則した場合に限定すること

二　初期設定の識別コードを変更できる場合には、識別コードを初期設定以外のものに変更すること

三　初期設定の主体認証情報を変更できる場合には、主体認証情報を初期設定以外のものに変更すること

四　ネットワークからのログインを制限すること

解説：管理者権限を持つ識別コードの取扱いは、情報システムのセキュリティ対策上、非常に重要な事項である。そのため、管理者権限を持つ識別コードは、業務又は業務上の責務に即して最小限の者へ付与すること。必要以上の者に過大な管理者権限を付与しないこと。また、管理者権限に係る識別コード及び主体認証情報の取扱いについては、「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 条の識別コード及び主体認証情報に係る遵守事項も踏まえること。なお、管理者権限を持つ識別コードについては、初期設定の識別コードの使用を禁止し、又は必要時以外は無効化することが望ましい。

「ネットワークからのログインを制限する」こととしては、例えば、電子証明書による端末認証、IP アドレス、MAC アドレス等により制限することが考えられる。

4　権限管理を行う者は、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、当該利用者等の識別コードを無効にすること。また、入学や卒業、人事異動等により、識別コードを追加し、又は削除する時に、不要な識別コードの有無を点検すること。

解説：識別コードの付与を最小限に維持するため、卒業や退職等により不必要となった識別コードについては、これを無効にすることを求める事項である。また、本人からの届出による場合のほか、入学や卒業、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、無効の設定漏れを最小限にとどめることが期待できる。

5　権限管理を行う者は、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ること。

解説：識別コードの付与を最小限に維持し、かつ主体認証情報の不当な使用を防止するために、卒業や退職等により不要になった主体認証情報格納装置の回収を求める事項である。

6　権限管理を行う者は、利用者等の身分とそれに伴う責務及び必要性を勘案し、必要最小限の範囲に限って許可を与えるようにアクセス制御の設定をすること。また、入学や卒業、人事異動等により、識別コードを追加し、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：利用者等の身分とそれに伴う責務に即して、必要となる者に限り、当該者の利用目的の達成に必要な範囲内のアクセス権のみを付与することを求める事項である。

7　権限管理を行う者は、以下のそれぞれの措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

一　単一の情報システムにおいては、１人の利用者等に対して単一の識別コードのみの付与

解説：１人の利用者等に対して単一の識別コードのみを付与することを求める事項である。例えば、デュアルロック機能を備えた情報システムにおいては、１人の利用者等に複数の識別コードでの主体認証を許してしまうと、デュアルロック機能による強化が万全とならなくなる。

二　識別コードをどの主体に付与したかについての記録及び当該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

解説：識別コードの付与に係る記録は将来の障害・事故等の原因調査に備えて、不用意に消去しないことを求める事項である。その情報システムへの将来の調査が不要になったものについては、消去することになるが、その場合には、許可を得た上で消去しなければならない。情報システムの関係者だけの判断で、識別コードをどの主体に付与したかを知るための記録を消去してはならない。

三　ある主体に付与した識別コードをその後別の主体に対して付与することの禁止

解説：ある主体に付与した識別コードを再利用して別の主体に付与することを禁ずる事項である。このため、職位等に対応する識別コードが存在し、それを担当者が引き継いで使用する場合等、やむを得ずある主体に付与した識別コードをその後別の主体に対して付与する場合には、例外措置を申請する必要がある。そして、当該申請を許可するときは、その主体認証情報を新たに設定し、以前に使用していた主体による使用を禁ずるとともに、任意の時点で識別コードの利用主体を特定できるように、履歴を管理することが求められる。

なお、当該例外措置は、どの識別コードを誰が使用しているかを管理する ID マネジメントに係る重要事項であるため、部局総括責任者が許可・不許可を判断することが望ましい。

B2151-08　（権限管理手続の整備）

第八条　部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、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権限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　アクセス制御情報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、確実にアクセス権限を設定するため、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、アカウントの発行並びに削除の手続き及び違反行為を発見した場合のアカウントの停止並びに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「B2201 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、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。

解説：アクセス権限の管理については、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、権限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。

B2151-09　（共用識別コード）

第九条　部局技術責任者は、権限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。

B2151-10　（アカウントの発行）

第十条　権限管理を行う者は、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「B2101 情報システム運用・管理規程」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　権限管理を行う者は、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。

B2151-11　（アカウント発行の報告）

第十一条　権限管理を行う者は、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。

B2151-12　（アカウントの有効性検証）

第十二条　権限管理を行う者は、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　権限管理を行う者は、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、「B2201 情報システム利用規程」や「B3205 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るとか、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。

B2151-13　（アカウントの削除）

第十三条　権限管理を行う者は、第十二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「B2101 情報システム運用・管理規程」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　権限管理を行う者は、権限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　権限管理を行う者は、権限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。

B2151-14　（アカウントの停止）

第十四条　権限管理を行う者は、第十二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、「B2101 情報システム運用・管理規程」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。

B2151-15　（アカウントの復帰）
第十五条　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、権限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　権限管理を行う者は、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。

B2151-16　（管理者権限を持つアカウントの利用）
第十六条　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、最少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。

第四節　証跡管理機能

解説：情報システムの利用においては、当該情報システムの制御及び管理の実効性を高め、また情報セキュリティに関する問題が発生した場合にこれに適切に対処するために、当該情報システムの動作及びその他必要な事象を記録し、事後にこれを調査する証跡管理を行う必要がある。また、証跡管理により、外部又は内部の者による不正利用又は過失行為を事前に抑止し、また事後に追跡することが可能となる。
これらのことを勘案し、本節では、証跡管理に関する対策基準として、証跡管理機能の導入、証跡の取得と保存についての遵守事項を定める。
なお、「B2101 情報システム運用・管理規程」第 8 章第 1 節において識別コー

ドと主体認証情報の管理等に関する対策基準を、「B2101 情報システム運用・管理規程」第 11 章第 4 節において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

「証跡」は、情報システムにおいて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、証跡管理のための最低必要条件となる。なお、証跡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章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。

B2151-17　（証跡管理機能の導入）（政府機関統一技術基準の対応項番 2.2.1.4(1)）

第十七条　部局技術責任者は、証跡を取得する必要があると部局総括責任者が認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。

解説：証跡を取得する機能を設ける必要があると認められた場合に、当該機能を情報システムに設けることを求める事項である。

２　部局技術責任者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。

解説：証跡の取得ができなくなった場合及び取得できなくなるおそれがある場合に対処する機能を情報システムに設けることを求める事項である。

設けるべき機能としては、用意したファイル容量を使い切った場合に証跡の取得を中止する機能、古い証跡に上書きをして取得を継続する機能、ファイル容量を使い切る前に操作する者に通知して対処をさせる機能等が考えられる。

なお、「必要に応じ」とは、定めた対処方法を実現するために必要な場合に限られる。

３　部局技術責任者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。

解説：不正アクセス、不正操作若しくは研究教育事務以外の利用又は誤操作を行った者にとって、その証跡は自己に不利益をもたらすものであることも考慮し、証跡が不当に消去、改ざんされることのないように、適切な格付を与えてこれを管理することを求める事項である。証跡の格付は、多くの場合に、機密性２情報又は機密性３情報で、要保全情報となるものと考えられる。

証跡は、訴訟において証拠として利用されることがある。その適切な取扱いを

組織として定め、かつこれを遵守していることが、証跡に証拠力が認められる前提となることにも留意する必要がある。
また、証跡には情報システムを利用する者の行為が記録されるため、業務上の必要なくこれにアクセスすべきではない。
これらの理由で、証跡は、部局技術担当者を含む利用者が不当に消去、改ざん又はアクセスすることのないように、証跡を保存したファイルに適切なアクセス制御を適用する必要がある。
また、証跡として利用記録や監視記録を含めた場合には、対象となる利用者のプライバシーを侵害しないことにも配慮する必要があるため、アクセスできる者を制限することが重要になる。

4　部局技術責任者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を情報システムに設けること。

一　証跡の点検、分析及び報告を支援するための自動化機能

解説：取得した証跡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、その作業を自動化する機能を設けることを求める事項である。
証跡は、その量が膨大になるため、証跡の内容をソフトウェア等により集計し、時系列表示し、報告書を生成する等により、効率的かつ確実な点検、分析及び報告が可能となる。規模の大きい情報システムにおいては、複数のサーバ装置で取得した証跡をあわせた点検、分析及び報告の作業を支援する自動化も、必要に応じて導入する。

二　情報セキュリティの侵害の可能性を示す事象を検知した場合に、監視する者等にその旨を即時に通知する機能

解説：情報セキュリティの侵害の可能性を示す事象が発生した場合に、迅速な対処を可能とするために、監視する者等に即時に通知する機能を設けることを求める事項である。
学外からの不正侵入の可能性、学内における持込み PC の情報システムへの接続等、通知すべき事象を定め、これを通知する機能を情報システムに組み込む。
必要に応じ、情報システムの利用者に即時に注意を促す仕組みを設けることも考えられる。

B2151-18　（証跡の取得と保存）（政府機関統一技術基準の対応項番 2.2.1.4(2)）

第十八条　部局技術担当者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、情報システムに設けられた機能を利用して、証跡を取得すること。

解説：情報システムの運用中に、利用者の行動等の事象を証跡として取得することを求める事項である。
部局技術担当者は、証跡を取得するために、必要な操作を行う必要がある。

2　部局技術担当者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。

解説：取得した証跡を適正に保存し、又は消去することを求める事項である。

部局技術担当者は、証跡の保存期間が満了するまで当該証跡を保存する必要がある。
必要な期間にわたり証跡を保存するために、当該期間に取得する証跡を全て保有できるファイル容量としたり、証跡を適宜外部電磁的記録媒体に退避したりする方法がある。
なお、法令の規定により保存期間が定められている場合には、これにも従うこと。
保存期間は、例えば、学外からアクセスされる情報システムにおいては３か月以上とし、特に重要な情報を取り扱う情報システムにおいては１年以上として定めることが考えられる。

３　部局技術担当者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処方法に基づいて対処すること。

解説：証跡の取得ができない場合又は取得できなくなるおそれがある場合の対処を定める事項である。
これらの場合には、部局技術担当者は、対処方法に定められた操作を行うことが求められる。対処方法に定められた操作としては、用意したファイル容量の残りが少ないことを通知された場合に、ファイルの切替えと証跡の退避を指示する操作等が想定される。

B2151-19　（通信の監視）

第十九条　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。「B2101 情報システム運用・管理規程」及び「B2151 情報セキュリティ要件の明確化に関する技術規程」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、「B2201 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ものと考えるが、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棄損、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。

「B2101 情報システム運用・管理規程」及び「B2151 情報セキュリティ要件の明確化に関する技術規程」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、「B2201 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。

技術責任者並びに技術担当者及び利用者等は、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。「B2101 情報システム運用・管理規程」及び「B2151 情報セキュリティ要件の明確化に関する技術規程」並びに「B2201 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。

B2151-20　（利用記録）

第二十条　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。

B2151-21　（個人情報の取得と管理）

第二十一条　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。

B2151-22　（利用者等が保有する情報の保護）

第二十二条　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インシデント対応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「B3103 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　保証のための機能

解説：「B2101 情報システム運用・管理規程」及び「B2151 情報セキュリティ要件の明確化に関する技術規程」では、基本的なセキュリティ機能として、主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能の各項で具体的に遵守事項を規定している。しかし、情報が適切な状態であることを保証するためには、これらの機能によるセキュリティ対策より上位の機能やそれ以外の機能等による対策全般についても導入の必要性を検討することが重要である。こうした対策は、限られた情報システムに導入されることになると考えるが、基本的な対策ではないからといって最初から除外するのではなく、必要性の有無を確認し選択的に導入するという対応が適切である。
これらのことを勘案し、本節では、保証のための機能に関する対策基準を定める。
なお、「B2101 情報システム運用・管理規程」第 8 章第 1 節において識別コードと主体認証情報の管理等に関する対策基準を、「B2101 情報システム運用・管理規程」第 11 章第 4 節において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

B2151-23　（保証のための機能の導入）（政府機関統一技術基準の対応項番 2.2.1.5(1)）

第二十三条　部局技術責任者は、保証のための対策を行う必要があると認めた情報システムにおいて、保証のための機能を設けること。

解説：保証のための対策を行う必要性があると認めた場合に、保証のための機能を情報システムに設けることを求める事項である。
保証のための機能とは、「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 章第 1 節～第 4 節で示した遵守事項に限らない情報及び情報システムの安全性をより確実にするための機能のことをいう。これには大きく分けて以下の 2 つのものがある。
（ア）「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 章第 1 節～第 4 節の機能とは異なる観点での保護を高めるための機能：
「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 章第 1 節～第 4 節の機能は、主として情報及び情報システムの機密性、完全性及び可用性を保護することを目的とした機能である。これに加えて、情報及び情報システムの真正性（Authenticity）の保護、否認防止（Non-Repudiation）のための機能等を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。
真正性の保護及び否認防止のための機能としては、例えば、電子署名及びタイ

ムスタンプが挙げられる。
（イ）「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 章第 1 節～第 4 節の機能及び上の（ア）の機能の動作が適正であることを確認するための機能：
「B2151 情報セキュリティ要件の明確化に関する技術規程」第 1 章第 1 節～第 4 節の機能及び上の（ア）の機能は情報及び情報システムを保護するための機能といえる。それに対して（イ）は、それらの機能を監視して、異常やその兆候を検知し、検知された問題を解決する対処をすることによって、それらの機能の回復に備えるための機能である。これらの機能を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。
（イ）の機能としては、例えば、侵入検知システムやネットワーク監視等が挙げられる。
また、保証のための機能は、主体認証機能等のように個別のものではなく、複数の機能であったり、それら複数のものを組み合わせた機能であったりする場合もある。情報セキュリティをより高めるために必要となる機能を設けることで本遵守事項を達成することができる。

第六節　暗号と電子署名（鍵管理を含む）

解説：情報システムの利用においては、当該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に、情報の暗号化及び電子署名が有効とされている。この際、あらかじめ定めた暗号アルゴリズム及び方法に基づき、暗号及び電子署名を適切な状況で利用する必要がある。
これらのことを勘案し、本節では、暗号化及び電子署名に関する対策基準として、暗号化機能及び電子署名機能の導入、暗号化及び電子署名に係る管理についての遵守事項を定める。
なお、「B2101 情報システム運用・管理規程」第 8 章第 1 節において識別コードと主体認証情報の管理等に関する対策基準を、「B2101 情報システム運用・管理規程」第 11 章第 4 節において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

プライバシーに関わる情報やパスワード等の秘密情報の送受信、公文書の電子的な提出や受理の際は、暗号化や電子署名を用いた確認を行わなければならない。暗号化としては、電子メールの S/MIME やウェブサーバの SSL などが挙げられる。

B2151-24　（暗号化機能及び電子署名機能の導入）（政府機関統一技術基準の対応項番 2.2.1.6(1)）

第二十四条　部局技術責任者は、要機密情報（書面を除く。以下この条において同じ。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。

解説：暗号化を行う機能を情報システムに付加する前提として、部局技術責任者は、各情報システムについて、取り扱う情報の機密性の程度から暗号化を行う機能

を付加する必要性の有無を検討しなければならない。

2　部局技術責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。

解説：情報の機密性の程度から暗号化を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項である。

3　部局技術責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与及び検証を行う機能を付加する必要性の有無を検討すること。

解説：電子署名の付与及び検証を行う機能を情報システムに付加する前提として、部局技術責任者は、各情報システムについて、取り扱う情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与及び検証を行う機能を付加する必要性の有無を検討しなければならない。

4　部局技術責任者は、電子署名の付与又は検証を行う必要があると認めた情報システムには、電子署名の付与又は検証を行う機能を設けること。

解説：情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与又は検証を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項である。

5　部局技術責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、以下のそれぞれの措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

一　暗号モジュールの交換可能なコンポーネント化による構成

解説：選択したアルゴリズムが危殆化した場合を想定し、暗号モジュールを交換可能なコンポーネントとして構成するため、設計段階からの考慮を求める事項である。そのためには、暗号モジュールのアプリケーションインターフェイスを統一しておく等の配慮が必要である。

二　複数のアルゴリズムを選択可能にする構成

解説：選択したアルゴリズムが危殆化した場合を想定し、設定画面等によって、当該アルゴリズムを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等を、情報システムに設けることを求める事項である。

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、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主体認証情報等が安全に保護された製品を使用するため、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の選択

解説：アルゴリズムの実装状況及び鍵等の保護状況を確認するに当たり、ISO/IEC 19790 に基づく暗号モジュール試験及び認証制度による認証を取得している製品を選択することを求める事項である。

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ずる等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ずる等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。

なお、「適切に実装されている」とは、アルゴリズム自体の安全性だけではなく、疑似乱数の推測、鍵情報の一部露呈等の脅威に対応して実装していることをいい、その確認には、独立行政法人 情報処理推進機構（IPA）により運用されて

いる暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）等が利用可能である。

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の耐タンパー性を有する暗号モジュールへの格納

解説：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、技術的な対策等に加え、物理的対策を講ずることを求める事項である。鍵を格納する電磁的記録媒体が盗難され、鍵が開封される等しても、鍵情報が外部へ漏えいしない仕組みが必要である。

この場合、耐タンパー性を有するとは、例えば、JIS X 19790:2007 7.5 物理的セキュリティ（ISO/IEC 19790:2006）の規定に照らし合わせると、他のセキュリティ対策との組み合わせによりレベル２以上を選択することが可能であるが、他の組み合わせがない場合、レベル３以上が相当する。

B2151-25　（暗号化及び電子署名に係る管理）（政府機関統一技術基準の対応項番 2.2.1.6(2)）

第二十五条　部局技術責任者は、電子署名の付与を行う必要があると認めた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提供すること。

解説：電子署名の付与を実効的に機能させるために、付与された電子署名を受け取った者が、その電子署名の正当性を容易に検証できるようにすることを求める事項である。

通常、付与された電子署名を検証するためには、署名時に使用した署名鍵に対応する検証鍵が必要であるが、この検証鍵自体の真正性を保証するためには、大学の窓口での直接提供、信頼できる機関による電子証明書の発行、検証鍵に付随する固有の情報（フィンガープリント等）の公開等の方法がある。

なお、電子署名の正当性を検証するための情報又は手段については、当該電子署名が付与された情報が真正なものであることを証明する必要がある間、提供することとなる。例えば、電子署名の有効期限内にアルゴリズムの危殆化が発生し、又は有効期限を超えるため、別の電子署名を付与する場合にあっては、これら全ての電子署名の正当性を検証するための情報又は手段を提供する必要がある。

２　部局技術責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。

解説：様々な機関から提供されているアルゴリズムの危殆化に関する情報を適宜入手しておくことを求める事項である。

例えば、CRYPTREC を始めとする暗号技術の有識者による発表に関心を払うことが必要である。

第二章　情報セキュリティについての脅威

第一節　セキュリティホール対策

解説：セキュリティホールは、情報システムを構成する電子計算機及び通信回線装置上で利用しているソフトウェアに存在する可能性があり、そのセキュリティホ

ールを攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、不正プログラム感染の原因になる等、情報システム全体のセキュリティを維持する上で大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、本学の社会的な信用が失われるおそれがある。これらのリスクを回避するため、セキュリティホールへの対処は迅速かつ適切に行わなければならない。
これらのことを勘案し、本節では、セキュリティホールに関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

B2151-26　（情報システムの構築時）（政府機関統一技術基準の対応項番 2.2.2.1(1)）

第二十六条　部局技術責任者は、電子計算機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セキュリティホールの対策を実施すること。

解説：電子計算機及び通信回線装置の設置又は運用開始時に、その時点において、当該機器上で利用しているソフトウェアのセキュリティホール対策が完了していることを求める事項である。

2　部局技術責任者は、公開されたセキュリティホールの情報がない段階においても電子計算機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。

解説：公開されたセキュリティホールへの対策だけでなく、明らかになっていないセキュリティホールについても対策を求める事項である。
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。

B2151-27　（情報システムの運用時）（政府機関統一技術基準の対応項番 2.2.2.1(2)）

第二十七条　部局技術担当者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、公開されたセキュリティホールに関連する情報を適宜入手すること。

解説：セキュリティホールに関連する情報の収集を求める事項である。セキュリティホールに関連する情報とは、セキュリティホールの原因、影響範囲、対策方法、セキュリティホールを悪用するツールの公開の有無等が挙げられる。
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、定期的にセキュリティホール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、当該機能がない場合は、適時調査を行う必要がある。

2　部局技術責任者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、セキュリティホールに関連する情報を入手した場合には、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を策定すること。

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の一時的な回避方法
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

解説：セキュリティホールが情報システムにもたらすリスクを分析し、対策計画の策定を求める事項である。
「対策試験」とは、セキュリティホール対策の実施による情報システムへの影響の有無について、他の情報システムを用いて試験することをいう。

3　部局技術担当者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。

解説：セキュリティホール対策計画に基づいて対策が実施されることを求める事項である。

4　部局技術担当者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者を含む事項を記録すること。

解説：セキュリティホール対策の実施記録の様式は問わないが、実施日、実施内容及び実施者は必ず記録しなければならない必須事項である。これらの事項のほかに必要事項があれば、適宜追加する。

5　部局技術担当者は、信頼できる方法でパッチ又はバージョンアップソフトウェア等のセキュリティホール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。）を入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

解説：入手した対策用ファイルに悪意あるコードが含まれている可能性を考慮し、対策用ファイルを信頼できる方法で入手することを求める事項である。
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のダウンロード又は郵送された外部電磁的記録媒体を利用して入手する方法が挙げられる。また、改ざん等について検証することができる手段があれば、これを実行する必要がある。

6　部局技術担当者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。

解説：電子計算機及び通信回線装置上のセキュリティホール対策及びソフトウェア構成の状況を確認し、対策を担保するための事項である。
「セキュリティホール対策及びソフトウェア構成」とは、導入されているソフトウェアの種類及びこれらのセキュリティホール対策状況のことである。調査の間隔については、短いほど効果が高いため、可能な範囲で短くすることが望ましい。「不適切な状態」とは、パッチが適用されていない等、セキュリティホール対策が講じられていない状態のことである。

7　部局技術責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、他部局の部局技術責任者と共有すること。

解説：公開されたセキュリティホールに関連する情報の入手及びセキュリティホール対策を効果的に実施するために、部局技術責任者間の連携を求める事項である。

B2151-28　（脆弱性診断）

第二十八条　部局技術責任者及び部局技術担当者は、情報システムに関する脆弱性の診断を定期的に実施し、セキュリティの維持に努めること。

解説：脆弱性診断は、内部的に行うもの、外部機関に委託して行うものの両方が考えられる。また、脆弱性診断の範囲も、ソフトウェアによる簡単なテストから、機器の設置状況や物理的な管理状況の審査までさまざまな範囲があり得る。脆弱性診断の頻度や範囲をどのようにするかは、ポリシー（情報システム運用基本方針及び情報システム運用基本規程）によるものとする。なお、脆弱性診断を行う者は、「B2101 情報システム運用・管理規程」第 7 条（禁止事項）の内容を遵守し、管理者権限を濫用しないよう配慮すること。

第二節　不正プログラム対策

解説：不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の要機密情報を漏えいさせることから機密性に対する脅威ともなる。

さらに、不正プログラムに感染した情報システムは、他の情報システムの再感染を引き起こす危険性のほか、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危険性等他者に対するセキュリティ脅威の原因となり得る。

これらのことを勘案し、本節では、不正プログラムに関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

B2151-29　（情報システムの構築時）（政府機関統一技術基準の対応項番 2.2.2.2(1)）

第二十九条　部局技術責任者は、電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。以下この条において同じ。）にアンチウイルスソフトウェア等を導入すること。

解説：動作可能なアンチウイルスソフトウェア等が存在する電子計算機について、アンチウイルスソフトウェア等を導入することを求める事項である。

なお、多くのメインフレームシステム並びにオペレーティングシステム及びアプリケーションを搭載していない電子計算機については、動作可能なアンチウイルスソフトウェアが存在しないため、本遵守事項は適用されない。ただし、アンチウイルスソフトウェア等が新たにサポートを開始する場合には、速やかな導入が求められることから、部局技術責任者は、該当する電子計算機の把握を行っておくとともに、アンチウイルスソフトウェア等に関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。

なお、アンチウイルスソフトウェア等には、他社製品・技術だけでなく、同一社の製品でもアンチウイルスソフトウェアの他、パーソナルファイアウォールやスパイウェア対策ソフト等も含む。

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アンチウイルスソフトウェア等により不正プログラム対策を実施すること。

解説：電子計算機以外の想定される感染経路に対しても、不正プログラム対策の実施を求める事項である。

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、複数の感染経路を想定した対策が必要である。

3　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において、複数の種類のアンチウイルスソフトウェア等を組み合わせて導入する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：複数の種類のアンチウイルスソフトウェア等を導入することにより効果的な不正プログラム対策の実施を求める事項である。

アンチウイルスソフトウェア等は、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、アンチウイルス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が発生する可能性を低減させるため、感染経路において異なる製品や技術を組み合わせ、どれか１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必要がある。例えば、メールサーバに導入するアンチウイルスソフトウェアと端末に導入するアンチウイルスソフトウェアを異なるパターンファイルを用いた製品にすること等が考えられる。

4　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において、拡散を防止する措置の必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：ネットワーク及び外部電磁的記録媒体を経由した感染拡大を防止することを求める事項である。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、不正プログラム定義ファイル又はパッチ適用等が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情報システムや、通信に不正プログラムが含まれていることを検知すると、その通信を検知したネットワークからの通信を遮断する情報システムの導入等が挙げられる。また、外部電磁的記録媒体を経由した感染拡大の防止策としては、例えば、自動再生機能の無効化、外部電磁的記録媒体の電子計算機接続時の手動検索、及びアンチウイルスソフトウェアの自動検査機能の有効化等が挙げられる。

B2151-30　（情報システムの運用時）（政府機関統一技術基準の対応項番 2.2.2.2(2)）

第三十条　部局技術担当者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、利用者等にその対処の実施に関する指示を行うこと。

解説：不正プログラムに対し特段の対処が必要な場合に実施することを求める事項である。

「特段の対処が必要な場合」とは、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アンチウイルスソフトウェア等に用いる定義ファイルが配布されない等、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が挙げられる。

2　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、その見直しを行うこと。

解説：「B2101 情報システム運用・管理規程」第 93 条第 1 項の規定による全学実施

責任者が整備する規程に基づいた対策の状況及び本条の対策の状況を適宜把握し、問題点が発見された場合は改善することを求める事項である。

第三節　サービス不能攻撃対策

解説:インターネットを経由して外部に提供しているサービスを実現する電子計算機、並びにそのアクセスに利用される通信回線及び通信回線装置は、利用者が自由にアクセス可能である利便性を確保するために、サービス不能攻撃により、通常の利用者がサービスを利用できなくなるといった可用性に対するリスクがある。

このため、インターネットに接続しているサーバ装置、並びにそのアクセスに利用される通信回線及び通信回線装置については、高い可用性を維持するための対策が必要となる。

この対策については、ソフトウェアのセキュリティホールを悪用する攻撃に対するものと、大量のアクセスによる攻撃に対するものに大別され、両者とも実施する必要がある。

これらのことを勘案し、本節では、サービス不能攻撃に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

B2151-31　（情報システムの構築時）（政府機関統一技術基準の対応項番 2.2.2.3(1)）

第三十一条　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電子計算機、通信回線装置又は通信回線を有す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電子計算機及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。

解説：電子計算機や通信回線装置が設けている機能を有効にすることを求める事項である。

対策としては、例えば、3-way handshake 時のタイムアウトの短縮、各種 Flood 攻撃への防御機能、アプリケーションゲートウェイ機能、パケットフィルタリング機能を利用すること等が挙げられる。

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に影響が最小となるように情報システムを構築すること。

解説：要安定情報を取り扱う情報システムがサービス不能攻撃を受けた場合の影響を分析し、情報システムを構築することを求める事項である。影響としては、通信回線の帯域圧迫によるアクセス障害や、サーバの処理能力低下等が考えられる。このため、例えば、サービス不能攻撃を受けたことを検出した場合には、即座に情報システムを外部ネットワークより遮断する、通信回線の通信量に制限をかける等といった手段を有する情報システムを構築する必要がある。

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電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法及び監視記録の保存期間を定めること。

解説：サービス不能攻撃に関する監視対象の特定と監視方法及び監視記録の保存期間を定めることを求める事項である。

インターネットからアクセスされるサーバ装置、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サーバ装置、通信回線装置及び通信回線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、負荷の定量的な把握がある。監視方法は多種多様であるため、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。

4　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、電子計算機や通信回線装置における対策だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者と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こと。

解説：部局技術責任者が、電子計算機や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、学外へ接続する通信回線を提供している事業者へも対策の協力を依頼できる体制を整備することを求める事項である。

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については、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響を排除し、又は低減する措置の必要性の有無を検討し、必要と認めたときは、対策措置を講ずること。

解説：通信回線については、通信量の制限や通信の遮断が有効であり、サービス不能攻撃の影響を排除し、又は低減するために必要な装置の導入を求める事項である。例えば、巧みに偽装したパケットや正規の送信元アドレスを使用した巧妙な DDoS 攻撃を抑制するには、電子計算機及び通信回線装置が持つ既存のセキュリティ対策機能に加え、サービス不能攻撃に係る通信の遮断等、インターネットに接続している通信回線を提供している事業者による対策又はサービス不能攻撃の影響を排除し、又は低減することのできる専用の対策装置の導入が挙げられる。

なお、電子計算機や通信回線装置が設け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、インターネットに接続している通信回線を提供している事業者による対策又は対策装置を導入する必要性があると判断すること。

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については、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保することの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：大量のアクセスによる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における対処を効果的に実施するための事項である。

例えば、対処としては、サービス提供に利用している通信回線等がサービス不能攻撃により過負荷状態に陥っていても、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に設置されている対策装置を操作できる手段を確保することが挙げられる。より具体的には、管理者が当該

装置等を操作するための電子計算機及び通信回線等を、サービス提供に利用している電子計算機及び通信回線等とは別に用意すること等が挙げられる。

7　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、サービス提供に必要な電子計算機、通信回線装置又は通信回線を冗長構成にすることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：サービス不能攻撃が発生した場合、サービスを提供する電子計算機、通信回線装置及び通信回線を代替電子計算機、代替通信回線装置又は代替通信回線に切り替えることにより、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を求める事項である。

サービス不能攻撃の検知及び代替計算機等への切替えは短時間にできるようにすることが必要である。

B2151-32　（情報システムの運用時）（政府機関統一技術基準の対応項番 2.2.2.3(2)）

第三十二条　部局技術担当者は、要安定情報を取り扱う情報システムについては、監視方法が定められている場合は、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。

解説：電子計算機、通信回線装置及び通信回線の通常時の状態を記録し把握することを求める事項である。

電子計算機、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、季節変動を検討した上で記録を一定期間保存する。

第四節　踏み台対策

解説：インターネット等の学外の通信回線に接続された情報システムは、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として、意図しない用途に使われてしまうこと、いわゆる、踏み台とされてしまうおそれがある。踏み台とされた情報システムは、学外に迷惑をかけるだけにとどまらず、例えば、当該情報システムが提供していたサービスを利用者が利用できないという可用性に対する水準の低下や、学内の他の情報システムに対するセキュリティ脅威の原因ともなり得る。これらを防ぐためには、本学が意図しない目的で本学の情報システムが使われないようにすることが必要である。

これらのことを勘案し、本節では、踏み台防止に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

B2151-33　（情報システムの構築時）（政府機関統一技術基準の対応項番 2.2.2.4(1)）

第三十三条　部局技術責任者は、情報システム（インターネット等の学外の通信回線に接続される電子計算機、通信回線装置又は通信回線を有する情報システムに限る。以下この条において同じ。）が踏み台として使われることを防止するための措置を講ずること。

解説：電子計算機等に対し、踏み台になることを避けるための対処の実施を求める事項である。

対策としては、アンチウイルスソフトウェア等の導入、セキュリティホールの

対処、不要なサービスの削除、フィルタリング機能の有効化、不審なプログラムの実行禁止、アンチウイルスソフトウェア等で検出されないボットの通信の監視等が挙げられる。

2　部局技術責任者は、情報システムを踏み台として使われた場合の影響が最小となるように情報システムを構築すること。

解説：管理する情報システムを踏み台として使われた場合の影響を分析し、情報システムを構築することを求める事項である。影響としては、通信回線の帯域圧迫によるアクセス障害や、サーバの処理能力低下等が考えられる。このため、踏み台として使われたことを検出した場合には、即座に情報システムを外部ネットワークより遮断する、問題が発生している電子計算機のみ切り離す、等といった手段を有する情報システムを構築する必要がある。

3　部局技術責任者は、情報システムが踏み台になっているか否かを監視するための監視方法及び監視記録の保存期間を定める必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：踏み台に関する監視方法及び監視記録の保存期間を定めることを求める事項である。

「監視方法」については、意図しない稼動負荷やインターネットへの通信の有無の把握、電子計算機に意図しない処理を行わせる命令の有無の監視等がある。監視方法は多種多様であるため、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。

B2151-34　（情報システムの運用時）（政府機関統一技術基準の対応項番 2.2.2.4(2)）

第三十四条　部局技術担当者は、監視を行う情報システムについては、定められた監視方法に従って情報システムを監視し、その記録を保存すること。

解説：情報システムの通常稼働時の状態を記録し把握することを求める事項である。

情報システム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、季節変動を検討した上で記録を一定期間保存する。

第五節　標的型攻撃対策

解説：標的型攻撃は、複数の攻撃手法を組み合わせ、ソーシャルエンジニアリングにより特定の組織や個人を狙い執拗に行われる攻撃である。この攻撃を完全に検知及び防御することは困難であり、かつ、端末やサーバ装置への侵入後、情報システム内に潜伏し、バックドアの設置等の攻撃を行うものもある。

本学で管理している情報システムの内部に不正侵入された場合、組織内部の情報が漏えいする等により、本学の社会的な信用が失われるおそれがある。また、攻撃のあった組織から窃取された情報が学外への攻撃に利用される場合もある。そのため、本学の外部と内部の境界で攻撃を検知及び防御する対策だけでなく、本学の情報システム内の通信及び外部への通信の監視・制御等を行うことにより、情報システム内部からの攻撃の検知及び被害の拡大を防止するための対策

も講ずる必要がある。
これらのことを勘案し、本節では、標的型攻撃に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

B2151-35　（情報システムの構築時）（政府機関統一技術基準の対応項番 2.2.2.5(1)）
第三十五条　部局技術責任者は、情報システムについて標的型攻撃による不正プログラムの侵入及び感染拡大等を防止するための措置を講ずること。

解説：電子計算機等に対し、情報システムの構築時における標的型攻撃による不正プログラムの侵入及び感染拡大等への対処の実施を求める事項である。標的型攻撃への対策は、個々のサーバ装置や端末だけではなく、情報システムのネットワーク全体の通信要件も対象となる。そして、当該通信要件に従って、アクセス制御及び経路制御を含むネットワークシステム全体の対策を講ずる必要がある。
対策としては、例えば、以下のものが挙げられる。
（ア）通信回線における対策
・ファイアウォール等を利用した通信要件の制限
・侵入検知システム等による不正な通信の検知・遮断
・端末間、グループ化された電子計算機間の通信の制限
・学内通信回線上の端末から学外通信回線への通信はプロキシを経由させる等の経路制御　等
（イ）端末及びサーバ装置共通の対策
・管理者権限を持つ識別コードの個別の付与（管理者権限を持つ既定の識別コードの付与の禁止又は必要時以外の無効化）
・管理者権限を持つ識別コードの業務に必要な権限のみの付与
・指定回数以上の主体認証情報の誤入力後の、一定期間の当該識別コードの無効化
・主体認証情報を設定する時の、セキュリティ上の強度が指定以上となるように要求する機能の設置
・アンチウイルスソフトウェア等の導入
・不正プログラム定義ファイル利用型アンチウイルスソフトウェアとふるまい検知型アンチウイルスソフトウェアの併用
・不正プログラムの自動検査機能の有効化
・セキュリティホールの対処
・不要なサービスの削除
・不審なプログラムの実行禁止
・許可していない外部電磁的記録媒体及び端末の接続制限
・送信ドメイン認証等を利用した、受信した電子メールのなりすましの有無の確認
・ファイルの暗号化　等
（ウ）端末における対策
・パーソナルファイアウォールの導入　等

（エ）サーバ装置における対策
・重要な情報を保存しているサーバ装置へのログイン可能な端末の制限
・重要な情報を保存しているサーバ装置上のセキュリティ状態の監視等
なお、不正プログラムの自動検査機能の有効化といった不正プログラム感染防止のための日常的実施事項については「B2101 情報システム運用・管理規程」第 11 章第 8 節、セキュリティホールへの対処といったセキュリティホールについての対策については「B2151 情報セキュリティ要件の明確化に関する技術規程」第 2 章第 1 節、アンチウイルスソフトウェア等の導入といった不正プログラム対策については「B2151 情報セキュリティ要件の明確化に関する技術規程」第 2 章第 2 節、サーバ装置にログイン可能な端末の制限や不要なサービスの削除といったサーバ装置や端末に関する対策については「B2152 情報システムの構成要素に関する技術規程」第 2 章、電子メールに関する対策については「B2153 アプリケーションソフトウェアに関する技術規程」第 1 章及びファイアウォールや侵入検知システム等の導入といった通信回線に関する対策については「B2152 情報システムの構成要素に関する技術規程」第 3 章を参照すること。

2　部局技術責任者は、インターネット等の学外の通信回線に接続される情報システムについて標的型攻撃に利用されることを防止するための措置を講ずること。

解説：インターネット等の学外の通信回線に接続される電子計算機等に対し、標的型攻撃に利用されることへの対処の実施を求める事項である。
対策としては、送信ドメイン認証を利用した送信する電子メールの送信元ドメイン名のなりすまし防止、本学ドメイン名の利用及び学外に提供するソフトウェア等への電子証明書の付与、当該電子計算機が標的型攻撃に利用されているか否かの監視等が挙げられる。
なお、学外に提供するソフトウェア等への電子証明書の付与といった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対策については「B2101 情報システム運用・管理規程」第 11 章第 6 節、ドメイン名の使用に関する対策については「B2101 情報システム運用・管理規程」第 11 章第 7 節、当該電子計算機の監視といった踏み台対策については「B2151 情報セキュリティ要件の明確化に関する技術規程」第 2 章第 4 節及び電子メールに関する対策については「B2153 アプリケーションソフトウェアに関する技術規程」第 1 章を参照すること。

B2151-36　（情報システムの運用時）（政府機関統一技術基準の対応項番 2.2.2.5(2)）

第三十六条　部局技術責任者は、情報システムについて標的型攻撃による不正プログラムの侵入及び感染拡大等を防止するための措置を講ずること。

解説：電子計算機等に対し、情報システムの運用時における標的型攻撃による不正プログラムの侵入及び感染拡大等への対処の実施を求める事項である。
対策としては、例えば、以下のものが挙げられる。
（ア）通信回線における対策
・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の監視

・学内通信回線上の電子計算機同士で送受信される通信内容の監視
・アンチウイルスソフトウェア等で検出されないボットの通信の監視　等
（イ）端末及びサーバ装置共通の対策
・アンチウイルスソフトウェア等における不正プログラム定義ファイルの最新の状態の維持
・定期的な全ての電子ファイルに対する不正プログラムの有無の確認
・セキュリティホールに関連する情報の収集及びリスク分析した上での対策実施
・ログの取得及び解析　等
（ウ）その他
・標的型攻撃に関する訓練の実施
・送信ドメイン認証を利用した、送信する電子メールの送信元ドメイン名のなりすまし防止　等
なお、不正プログラム定義ファイルの最新の状態の維持や定期的な全ての電子ファイルに対する不正プログラムの有無の確認といった不正プログラム感染防止のための日常的実施事項については「B2101 情報システム運用・管理規程」第 11 章第 8 節、セキュリティホールに関する情報の収集といったセキュリティホールに関する対策については「B2151 情報セキュリティ要件の明確化に関する技術規程」第 2 章第 1 節、電子メールに関する対策については「B2153 アプリケーションソフトウェアに関する技術規程」第 1 章及び通信内容の監視といった通信回線に関する対策については「B2152 情報システムの構成要素に関する技術規程」第 3 章第 2 節を参照のこと。

B2152 情報システムの構成要素に関する技術規程

第一章　施設と環境

第一節　情報取扱区域のクラス別管理及び利用制限

解説：悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる設置環境にある場合においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改ざん等が行われるおそれがある。また、その他にも、設置環境に関する脅威としては、自然災害の発生による情報システムの損傷や情報の紛失等が発生するおそれもある。

このように施設全体や区域ごとに様々な脅威が考えられるため、それぞれの区域に応じた管理と想定される利用形態に応じた情報の取扱いを行う必要がある。これらのことを勘案し、本節では、情報取扱区域のクラス別管理及び利用制限の対策基準として、立ち入る者を制限するための管理対策、立ち入る者を許可する際の管理対策、訪問者がある場合の管理対策、設置する設備の管理対策、作業がある場合の管理対策、立ち入る者を制限するための利用制限対策、物品の持込み、持ち出し及び利用についての利用制限対策、荷物の受渡しについての利用制限対策並びに災害及び障害への対策に関する遵守事項を定める。

B2152-01　（立ち入る者を制限するための管理対策）（政府機関統一技術基準の対応項番 2.3.1.1(1)）

第一条　区域情報セキュリティ責任者は、立ち入る者を制限するための管理対策として、以下の事項について、別表１に従って、クラスの区分に応じた措置を講ずること。

一　不審者を立ち入らせない措置

解説：要管理対策区域への不審者の立入りを防止し、要管理対策区域のセキュリティを確保するための事項である。

措置としては、身分を確認できる物の提示の義務化、要管理対策区域の所在の表示の制限等が挙げられる。

二　要保護情報を取り扱う情報システムについては、物理的に隔離し、立入り及び退出を管理するための措置

解説：電子計算機及び通信回線装置が設置された区域を、物理的隔離及び立入り及び退出の管理によりセキュリティを確保するための事項である。

措置としては、壁、施錠可能な扉、パーティション等で囲むことで区域を隔離し、当該区域が無人になる際には扉を施錠する、当該鍵の貸し出しを管理するといった措置が挙げられる。なお、要管理対策区域では、扉を開放したまま無人の状態にしてはならない。

B2152-02　（立ち入る者を許可する際の管理対策）（政府機関統一技術基準の対応項番 2.3.1.1(2)）

第二条　区域情報セキュリティ責任者は、立ち入る者を許可する際の管理対策として、以下の事項について、別表１に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対

策を決定する場合は、当該個別管理についても講ずること。

一　要管理対策区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置

解説：要管理対策区域へ立ち入る者が立入りを許可された者であるかの確認を実施することで、許可されていない者の立入りを排除するための事項である。

なお、立入りを許可された者であるかの確認のために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等が望ましい。

二　要管理対策区域から退出する者が立入りを許可された者であるかの確認を行うための措置

解説：立ち入った者の退出を把握するための事項である。

三　立入りを許可された者が、立入りを許可されていない者を要管理対策区域へ立ち入らせ、及び当該区域から退出させない措置

解説：要管理対策区域の立入り及び退出時に立入りを許可された者であるかどうかの確認を確実に実施するための事項である。

対策としては、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。

四　継続的に立ち入る者を許可する手続の整備

解説：文書を整備することで、要管理対策区域へ継続的に立ち入る者を把握するための事項である。立入期間については、例えば、月又は年単位といった期間が考えられる。

なお、文書には、その者の氏名、所属、立入許可日、立入期間及び許可事由を含む事項を記載すること。

五　継続的に立入りを許可された者に変更がある場合の手続の整備

解説：立入りを許可された者に変更がある場合に変更手続をとることで、継続的に立ち入る者を把握するための事項である。変更の手続きには、変更の内容を前事項の文書へ反映することが挙げられる。

また、変更内容についての記録を保存し、後で参照できるようにしておく必要がある。

六　全ての者の要管理対策区域への立入り及び当該区域からの退出を記録し及び監視するための措置

解説：要管理対策区域への立入り及び当該区域からの退出の記録、監視を行い、区域のセキュリティが侵害された場合に追跡することができるようにするための事項である。

「記録し及び監視する」とは、警備員又は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。

B2152-03　（訪問者がある場合の管理対策）（政府機関統一技術基準の対応項番 2.3.1.1(3)）

第三条　区域情報セキュリティ責任者は、訪問者がある場合の管理対策として、以下の事項について、別表 1 に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

一　訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置

解説：訪問者の身元を確認するための事項である。

確認方法としては、例えば、訪問者に必要事項を記入させ、名刺又は社員証等と記入された内容とを照合する方法が挙げられる。

二　訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置

解説：訪問記録の作成を求める事項である。

三　訪問相手（情報システムを運用・管理する者をいう。以下同じ。）が訪問者の要管理対策区域への立入りについて審査するための手続の整備

解説：訪問者の要管理対策区域への立入りについて、訪問相手（情報システムを運用・管理する者をいう。以下同じ。）が審査するための手続を整備することを求める事項である。

手続としては、「警備員等が訪問相手に連絡し、訪問者の立入りについて審査する」、「訪問相手が、区域との境界線まで迎えに行き審査する」等の方法が挙げられる。なお、警備員等に対しては、必要に応じ、立入りの制限等について予め周知しておくこと等が考えられる。

四　訪問者の立ち入る区域を制限するための措置

解説：訪問者が許可されていない要管理対策区域へ立ち入らないようにすることを求める事項である。措置の例としては、扉を施錠し許可された者のみが開閉可能にすることや警備員による訪問者の確認等の方法が挙げられる。

五　訪問相手による訪問者に付き添う措置

解説：訪問者が許可されていない要管理対策区域へ立ち入らないように訪問相手が監視することを求める事項である。

六　訪問者と継続的に立入りを許可された者とを外見上判断できる措置

解説：継続的に立入りを許可された者と訪問者を区別するための事項である。

これにより、許可されていない要管理対策区域への訪問者の立入りが検知できる。対策としては、訪問者用の入館カードを作成し掲示を求める、訪問者の入館カード用ストラップの色を変える等が挙げられる。貸与した物は、訪問者の退出時に回収する必要がある。

B2152-04　（設置する設備の管理対策）（政府機関統一技術基準の対応項番 2.3.1.1(4)）

第四条　区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムについては、別表1 に従って、クラスの区分に応じて、設置及び利用場所が確定している電子計算機及び通信回線装置の盗難及び当該場所からの不正な持ち出しを防止するための措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

解説：設置場所が固定された電子計算機に関して、盗難及び不正な持ち出しを防止するための事項である。

「設置及び利用場所が確定している」とは、サーバ装置及び据置き型 PC のように、設置及び利用する場所が固定され、他の場所で利用することがないという意味である。

対策としては、端末であればセキュリティワイヤーによる固定、サーバ装置で

あればサーバラックへの設置及び当該サーバラックの施錠、施設からの退出時における持ち物検査等が挙げられる。
なお、重要システムを設置している場合やサーバ室に設置している複数のサーバラックの運用主体が異なる場合、サーバラックの鍵を適切に管理すること等が考えられる。
通信回線装置に係る対策としては、基幹の通信回線装置（ファイアウォール、ルータ、レイヤ３スイッチ、レイヤ２スイッチ等）であればサーバラックへの設置及び当該サーバラックの施錠、終端の通信回線装置（レイヤ２スイッチ等）であれば床下への埋設又は施錠できる場所への機器設置等が挙げられる。なお、学外通信回線と学内通信回線を結ぶルータを回線事業者が所有している場合は、契約等において不正な持ち出しを防止するための措置を講ずるよう求めることなどが考えられる。

２　区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置の設置に係る管理対策として、以下の事項について、別表１に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

一　電子計算機及び通信回線装置を設置する情報取扱区域を物理的に隔離するための措置

解説：電子計算機及び通信回線装置を設置する情報取扱区域が隣接する低いクラスと隔離されないことにより、安全性が確保できないことを防ぐための措置を求める事項である。

二　電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置

解説：電子計算機に接続されたディスプレイ、通信回線装置のメッセージ表示用ディスプレイ等を許可のない第三者に見られないように対策を実施することを求める事項である。
対策としては、偏光フィルタの利用等が挙げられる。

三　情報システムで利用する電源ケーブル及び通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置

解説：電源ケーブルの損傷及び通信ケーブルからの通信の盗聴等の脅威から、情報システムを保護するための事項である。
対策としては、ケーブルの床下への埋設、ケーブルのナンバリング等が挙げられる。

四　情報システムから放射される電磁波による情報漏えい対策の措置

解説：ディスプレイケーブル等から生ずる電磁波による情報漏えいのリスクについて対策を講ずるための事項である。
具体的には、電磁波軽減フィルタの利用等が挙げられる。

B2152-05　（作業がある場合の管理対策）（政府機関統一技術基準の対応項番 2.3.1.1(5)）

第五条　区域情報セキュリティ責任者は、別表１に従って、クラスの区分に応じて、要管理対策区域内での作業を監視するための措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

解説：要管理対策区域内での作業を監視するための事項である。

第三者による立会いや、監視カメラの導入等が挙げられる。

B2152-06　（立ち入る者を制限するための利用制限対策）（政府機関統一技術基準の対応項番 2.3.1.1(6)）

第六条　情報システムを運用・管理する者は、要管理対策区域内において、情報システムを運用・管理する者であることを常時視認することが可能な状態にすること。

解説：要管理対策区域に立ち入っている者が情報システムを運用・管理する者であることを外見上判断できるようにするために、身分証明書を着衣上に掲示すること等により常時視認できる状態にすることを求める事項である。

B2152-07　（物品の持込み、持ち出し及び利用についての利用制限対策）（政府機関統一技術基準の対応項番 2.3.1.1(7)）

第七条　区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムに関連する物品の持込み及び持ち出しに係る利用制限対策として、以下の事項について、別表 2 に従って、クラスの区分に応じた措置を講ずること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。

一　情報システムに関連する物品の持込み及び持ち出しを行う措置

解説：情報システムに関連する物品の持込み及び持ち出しによって生ずるリスクに対処するための事項である。

「情報システムに関連する物品」とは、要管理対策区域に存在する情報システムで利用するための物品が挙げられ、これにはハードウェア、ソフトウェア、電磁的記録媒体及び情報システムから出力された書面等が含まれる。

二　情報システムに関連する物品の持込み及び持ち出しに係る記録の保存

解説：情報システムに関連する物品の持込み及び持ち出しを記録し、追跡性を確保するための事項である。記録を取得する項目としては、持込み及び持ち出しを行う者の名前及び所属、日時、物品又は事由等が挙げられる。

三　情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の要管理対策区域への持込みについての制限

解説：情報漏えいの原因となる可能性のある電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の持込みを制限するための事項である。

2　情報システムを運用・管理する者は、撮影又は録音する場合は、別表 2 に従って、クラスの区分に応じて、区域情報セキュリティ責任者に撮影又は録音の許可を得、又は届け出ること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。

解説：動画及び写真の撮影並びに音声の録音に係る許可を得、又は届け出ることを求める事項である。

許可又は届出先となる主体は、当該区域を管理する区域情報セキュリティ責任者となるが、許可又は届出の窓口は担当の部局技術担当者が行うことが考えられる。

B2152-08　（荷物の受渡しについての利用制限対策）（政府機関統一技術基準の対応項番

2.3.1.1(8))

第八条　区域情報セキュリティ責任者は、受渡業者と物品の受渡しを行う際の対策として、別表2 に従って、クラスの区分に応じた措置を講ずること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。

解説：物品の受渡しを行う業者が要管理対策区域内に立ち入ることを制限するための事項である。

制限する措置としては、受渡しが認められる区域の決定並びに受渡しが認められない区域で、受渡しが必要な場合は、当該業者が該当区域内の電子計算機、通信回線装置及び記録媒体に触れることができない場所に限定し、情報システムを運用・管理する者が立ち会うようにすることが考えられる。「記録媒体」には電磁的記録媒体及び情報システムから出力された書面等の非電磁的な媒体が含まれる。

B2152-09　（災害及び障害への対策）（政府機関統一技術基準の対応項番 2.3.1.1(9)）

第九条　区域情報セキュリティ責任者は、要安定情報を取り扱う情報システムについては、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。

解説：地震、火災、水害、停電、爆発及び騒じょう等の災害から電子計算機及び通信回線装置を保護するための事項である。

対策としては、例えばサーバラックの利用のほか、

・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
・非常口及び非常灯

等の設置又は確保が挙げられる。

要安定情報を取り扱う情報システムについては、物理的損壊又は情報の漏えい若しくは改ざん等のリスク、自然災害による損傷のリスク等に備えるため、電子計算機及び通信回線装置を要管理対策区域に設置することが求められる。機器設置の際は、要管理対策区域に、次のような施設及び環境面からの対策を実施すること。

(1) 関係者以外の立ち入りを制限できる場所に設置すること。
(2) 停電及び過電流から保護されていることが望ましい。
(3) 故障防止のため、空調設備のあることが望ましい。
(4) 防塵及び防音のための設備のあることが望ましい。

２　区域情報セキュリティ責任者は、要安定情報を取り扱う情報システムについては、要管理対策区域内において災害又は障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。

解説：作業する者が災害等により要管理対策区域内に設置された電子計算機及び通信回線装置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

電子計算機及び通信回線装置の電源を遮断できるようにするための事項である。

第二章　電子計算機

第一節　電子計算機共通対策

解説：電子計算機の利用については、不正プログラム感染や不正侵入を受ける等の外部的要因により、保存されている情報の漏えい、改ざん又は当該電子計算機の機能停止等の被害に遭うおそれがある。また、利用者等の不適切な利用等の内部的要因による情報セキュリティの侵害も起こり得る。このように電子計算機の利用は、当該電子計算機及び当該電子計算機が取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本節では、電子計算機に関する対策基準として、電子計算機に関する設置時、運用時及び運用終了時についての遵守事項を定める。

B2152-10　（電子計算機の設置時）（政府機関統一技術基準の対応項番 2.3.2.1(1)）

第十条　部局技術責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を将来の見通しを含め検討し、確保すること。

解説：通常の運用において十分な性能を確保することを求める事項である。

例えば、電子計算機の負荷に関して事前に見積もり、試験等を実施し、必要となる処理能力及び容量を想定し、それを備える必要がある。また、将来にわたっても十分な性能を確保できるように、拡張性や余裕を持たせておく必要がある。

2　部局技術責任者は、要保護情報を取り扱う情報システムについては、電子計算機を要管理対策区域内に設置すること。ただし、モバイル端末について部局総括責任者の承認を得た場合は、この限りでない。

解説：電子計算機が設置される物理的環境における脅威への対策を求める事項である。

人為的な脅威としては建物内への侵入、部外者による操作、失火による火災又は停電等があり、環境的脅威としては地震、落雷又は風水害等がある。そのため、物理的な隔離、入退者の主体認証装置、消火設備、耐震設備又は無停電電源装置等を利用する必要がある。

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、サービス提供に必要な電子計算機を冗長構成にする必要性を検討し、必要と判断した場合には、その電子計算機を冗長構成にすること。

解説：障害・事故等が発生した場合、サービスを提供する電子計算機を代替電子計算機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を求める事項である。可用性を高めるためには、電子計算機本体だけでなく、ハードディスク等のコンポーネント単位で冗長構成にすることも考えられる。

なお、災害等を想定して冗長構成にする場合には、代替の電子計算機を遠隔地に設置することが望ましい。

4　部局技術責任者は、利用者等の離席時に、電子計算機を不正操作から保護するための措置を

講ずること。

解説：利用者等の離席時に、電子計算機を第三者による不正操作から保護するための事項である。

対策としては、例えば、スクリーンのロック等が挙げられる。スクリーンのロックについては、設定を義務付けるだけでなく、一定時間操作がないと自動的にロックする仕組み又は電子計算機のログインに利用する主体認証情報格納装置を事務室・研究室・教室等への立入りの許可の確認にも利用する方法等が考えられる。また、スクリーンのロックを設定できない電子計算機については、施錠管理可能な棚又はラック等に収納したり、キーボード、マウス及び USB ポート等を使用できないようにロックしたりする方法等が考えられる。

5　部局技術責任者は、電子計算機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：多様なソフトウェアを利用することによりセキュリティホール等の脅威が増大し、その対処が困難となる可能性があるため、電子計算機で利用するソフトウェアを制限することを求める事項である。

B2152-11　（電子計算機の運用時）（政府機関統一技術基準の対応項番 2.3.2.1(2)）

第十一条　教職員等は、研究教育事務の遂行以外の目的で電子計算機を利用しないよう努めること。

解説：電子計算機を研究教育事務目的以外に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電子計算機の利用を一切禁止しているが、大学の特性や実情を鑑みるに、実効的な運用を図るためには、研究教育事務の遂行以外の目的での電子計算機の利用を一切禁止することは困難と思われる。もちろん、サンプル規程集を利用する大学においては、本条より強固な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もあり得る。その場合は、例えば、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させられてしまうことから回避するため、研究教育事務目的外でのウェブサイトの閲覧を禁止すること等が求められる。

2　利用者等は、離席時に電子計算機を不正操作から保護するための措置を講ずること。

解説：利用者等が、離席時に電子計算機を第三者による不正操作から保護するために、スクリーンのロック、ログオフ又は施錠管理等の実施を求める事項である。

3　利用者等は、電子計算機で利用を禁止するソフトウェアに定められたものを利用しないこと。また、電子計算機で利用を認めるソフトウェアに定められたもの以外のソフトウェアを利用する必要がある場合には、部局技術責任者の承認を得ること。

解説：多様なソフトウェアを実行することによりセキュリティホール等の脅威が増大することから、利用を認めるソフトウェアに定められたもの以外のソフトウェアの利用を制限する事項である。

利用を認めるソフトウェアに定められたもの以外のソフトウェアを利用する必要がある場合には、承認を得る必要がある。部局技術責任者は、利用承認の申

請を受け付け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最低１回の手続きで済ませることができる。

4　部局技術責任者は、所管する範囲の電子計算機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電子計算機を検出等した場合には、当該不適切な状態の改善を図る必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：電子計算機で利用されている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場合にその改善を図ることを求める事項である。ただし、サーバ装置において利用を認めるソフトウェアに定められたもの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し、又は削除する必要がある。また、サーバ装置において利用を認めるソフトウェアに定められたものであっても、利用しない機能については無効化する必要がある。

「定期的」とは、１か月から６か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。

また、「不適切な状態」とは、利用を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、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等の状態のことをいう。

B2152-12　（電子計算機の運用終了時）（政府機関統一技術基準の対応項番 2.3.2.1(3)）

第十二条　部局技術責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体の全ての情報を抹消すること。

解説：電子計算機の運用を終了する場合に、当該電子計算機に内蔵される電磁的記録媒体から、全ての情報を抹消することを求める事項である。

「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。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、当該電磁的記録媒体に保存されている全ての情報を適切な方法で抹消する必要がある。

第二節　端末

解説：端末については、当該端末を利用する者が専門的知識を有していない場合が多いことから、当該利用者の過失による不正プログラム感染等のリスクが高い。また、可搬性の高い端末については、紛失又は盗難のリスクも高くなる。

このように端末の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本節では、端末に関する対策基準として、端末の設置時及び運用時についての遵守事項を定める。

B2152-13　（端末の設置時）（政府機関統一技術基準の対応項番 2.3.2.1(1)）

第十三条　部局技術責任者は、要保護情報を取り扱うモバイル端末については、要管理対策区域外で使われる際にも、要管理対策区域で利用される端末と同等の保護手段が有効に機能するように構成すること。

解説：要管理対策区域外で利用されるモバイル端末は、要管理対策区域で利用される端末と異なる条件下に置かれるため、要管理対策区域外で端末が利用される際の保護手段として、端末で動作するパーソナルファイアウォール等の具備を求める事項である。

例えば、モバイル端末が通常接続される通信回線で実施されているアクセス制御及び監視等は、他の通信回線では同等に実施されているとは限らないため、モバイル端末において実施する必要がある。

２　教職員等は、モバイル端末を利用する必要がある場合には、部局技術責任者に届け出ること。

解説：モバイル端末には様々なセキュリティ上のリスクが考えられるため、不必要にリスクを増大させないために、研究教育事務上必要なモバイル端末の利用にとどめるための事項である。

政府機関統一基準においては、モバイル端末を利用する必要がある場合には、情報システムセキュリティ責任者の承認が必要であるが、大学の特性や実情を鑑みるに、実効的な運用を図るためには、すべての場合に部局技術責任者の承認を得ることは困難と思われるため、サンプル規程集では部局技術責任者への届出を求めることとした。もちろん、サンプル規程集を利用する大学においては、本条より強固な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もあり得る。

３　部局技術責任者は、要機密情報を取り扱うモバイル端末については、電磁的記録媒体に保存される情報の暗号化を行う機能を設けること。

解説：モバイル端末が物理的に外部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、及びモバイル端末で利用していた外部電磁的記録媒体を他の電子計算機を利用して解読する等の攻撃によって要機密情報が読み取られる危険性がある。このような情報漏えいの対策として、端末に暗号化機能を装備することを求める事項である（ただし、当該モバイル端末で電磁的記録媒体に保存される情報の暗号化を行う機能が存在しない場合を除く。）。

なお、機密性３情報を取り扱う場合には、端末に暗号化機能を装備することが必要である。

４　部局技術責任者は、要保護情報を取り扱うモバイル端末については、盗難防止及び盗難後の被害を軽減するための措置を定めること。

解説：モバイル端末は容易に搬出することが可能なため盗難又は紛失に遭う可能性が高いことから、部局技術責任者にその対策を定めることを求める事項である。

対策としては、要管理対策区域においては、モバイル端末を入退出が管理される区域内に設置している場合においても端末の形状に応じて、固定物又は搬出が困難な物体と容易に切断できないセキュリティワイヤーでつなぐことや、帰宅時に施錠できるキャビネットに保存すること、常時所持又は携帯すること等が挙げられる。モバイル端末を要管理対策区域外に持ち出す場合は、常時所持又は携帯することや常に身近に置き目を離さないこと等が挙げられる。盗難後

の被害を軽減するための具体的な措置としては、例えば、遠隔データ消去機能等が挙げられる。

5　部局技術責任者は、利用者等が情報を保存できない端末を用いて情報システムを構築する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：端末から情報が漏えいすることを防ぐために、シンクライアント等の端末を利用することを求める事項である。

B2152-14　（端末の運用時）（政府機関統一技術基準の対応項番 2.3.2.2(2)）

第十四条　利用者等は、要保護情報を取り扱うモバイル端末を利用する場合には、盗難防止措置を行うこと。

解説：モバイル端末を利用する利用者等に対して、モバイル端末の盗難防止措置について、部局技術責任者が定めた手順に従い、措置を実施することを求める事項である。

2　利用者等は、要機密情報を取り扱うモバイル端末については、モバイル端末を要管理対策区域外に持ち出す場合に、当該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。

解説：モバイル端末で利用する電磁的記録媒体の紛失又は盗難により保存されている情報が漏えいすることを防ぐため、必要に応じて、ハードディスク、USB メモリ等に記録されている情報に対してファイル又は電磁的記録媒体全体を暗号化することを求める事項である。暗号化する方法としては、ハードディスク全体やファイルを暗号化するソフトウェアの導入や OS に標準装備されている暗号化機能の使用が挙げられる。

3　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端末を接続する必要がある場合には、部局技術責任者に届け出ること。

解説：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事項である。

政府機関統一基準においては、許可を得た通信回線以外に接続してはならず、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も接続許可を得る必要がある。しかし、大学の特性や実情を鑑みるに、実効的な運用を図るためには、許可を得た通信回線以外への接続を一切禁止することは困難と思われるため、サンプル規程集では部局技術責任者への届出を求めることとした。もちろん、サンプル規程集を利用する大学においては、本条より強固な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もあり得る。

4　部局技術担当者は、情報システムにおいて基準となる時刻に、端末の時刻を同期する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：情報システム内で同期されている基準となる時刻に、端末の時刻を同期させることを求める事項である。

情報セキュリティが侵害された際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えない。

第三節　サーバ装置

解説：サーバ装置については、当該サーバ装置の電磁的記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は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等を受けるリスクが高い。本学が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、社会における本学に対する信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。
このようにサーバ装置の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。
これらのことを勘案し、本節では、サーバ装置に関する対策基準として、サーバ装置の設置時及び運用時についての遵守事項を定める。

B2152-15　（サーバ装置の設置時）（政府機関統一技術基準の対応項番 2.3.2.3(1)）

第十五条　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場合は、通信を秘匿する必要性の有無を検討し、必要があると認めたときは、送受信される情報を秘匿するための機能を設けること。この場合、学外通信回線を経由する保守作業については、通信を秘匿する必要があると判断すること。

解説：通信回線を経由してサーバ装置の保守作業を行う際のセキュリティ強化を求める事項である。
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オ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、通信を秘匿する必要がある場合には、設置時に暗号化するための機能を設け、運用時に実際の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。

２　部局技術担当者は、要安定情報を取り扱うサーバ装置の内、サービス提供に必要なサーバ装置については、負荷を複数のサーバ装置に分散又はサーバ装置を冗長構成とする必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：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、複数のサーバ装置による負荷分散、負荷分散装置の設置、DNS による負荷分散又は冗長構成等の実施を求める事項である。

B2152-16　（サーバ装置の運用時）（政府機関統一技術基準の対応項番 2.3.2.3(2)）

第十六条　部局技術責任者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対処すること。

解説：サーバ装置のソフトウェア及びハードウェア等の構成が不正に変更されていないか定期的に確認し、また、変更によるセキュリティレベルの低下等が発生していないか検討し、変更状況に応じて対処することを求める事項である。

2　部局技術担当者は、要安定情報を取り扱うサーバ装置については、サーバ装置の運用状態を復元するために必要な措置を講ずること。

解説：サーバ装置の運用状態を復元するための必要な措置を講ずることによりサーバ装置に保存されている情報及びその情報を用いたサービスの可用性の担保を目的とした事項である。

サーバ装置の運用状態を復元するための必要な措置の例として、以下のようなものがある。

・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。

・前回内容からの変更部分の定期的なバックアップを実施する。

・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。

・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。

また、取得した情報を記録した電磁的記録媒体は、施錠された保管庫に保存等して、業務上の必要がある場合にこれらの情報を利用する部局技術担当者に限ってアクセスできるようにする。

なお、災害等を想定してバックアップを取得する場合には、記録媒体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ある施設に保存することが考えられる。その際には、情報を遠隔地に送信や移送する際のセキュリティ及び取得した情報の保管時のセキュリティを確保する必要がある。セキュリティを確保する措置の例としては、暗号や秘密分散技術を利用して情報の漏えいや改ざんを防止することが挙げられる。

3　部局技術担当者は、サーバ装置の運用管理について、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。

解説：運用管理作業の記録を文書として残すための事項である。

本学において、ある程度統一的な様式を作成する必要がある。

4　部局技術担当者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。

解説：情報システム内で同期されている基準となる時刻にサーバ装置を同期させることを求める事項である。

情報セキュリティが侵害された際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えない。

5　部局技術担当者は、サーバ装置のセキュリティ状態を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：サーバ装置のセキュリティ状態を監視するための事項である。

「セキュリティ状態を監視」するとは、サーバ装置上での不正な行為及び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ことである。

監視の方法の例としては、アクセスログを定期的に確認することや、侵入検知システム、アンチウイルスソフトウェア又はファイル完全性チェックツール等の利用が挙げられる。

なお、アクセスログを確認する際は、運用管理作業の記録若しくは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相関分析を行うことが考えられる。

6　部局技術担当者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、当該サーバ装置に関する障害等の発生を検知すること。

解説：日常的なサーバ装置のシステム状態について監視を行うことで、障害等の発生を早期に検出し、またこの影響の拡大を未然に防止するための事項である。

「システム状態を監視」するとは、サーバ装置の CPU、メモリ、ディスク入出力等の性能及び故障等を監視することである。監視方法は、状況に応じて、ツールの利用、手動から、適切な方法を選択することが可能である。

第三章　通信回線

第一節　通信回線共通対策

解説：通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本節では、通信回線に関する対策基準として、通信回線の構築時、運用時及び運用終了時についての遵守事項を定める。

B2152-17　（通信回線の構築時）（政府機関統一技術基準の対応項番 2.3.4.1(1)）

第十七条　部局技術責任者は、通信回線構築によるリスク（物理的損壊又は情報の漏えい若しくは改ざん等のリスクを含む。）を検討し、通信回線を構築すること。

解説：部局技術責任者は、通信回線構築によるリスクを考慮して、通信回線の構築及び運用開始を判断する必要がある。学外通信回線と接続する場合のリスク軽減措置としては、例えば、ファイアウォールやウェブアプリケーションファイアウォール（WAF）等を利用する方法が考えられる。リスクを検討した結果、部局技術責任者は、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か、通信回線を構築しない等の判断を行うことが望ましい。なお、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間の通信も同様に考慮すること。（「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きょう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。例えば、仮想化ソフトウェアを利用することが考えられる。なお、仮想化ソフトウェアとは、１つのハードウェアで複数のオペレーティングシステムを同時に実行する機能を有するソフトウェアをいう。以下同様。）

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、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。

解説：通常の運用において十分な通信回線の能力を確保し、情報の可用性を確保する

ための事項である。例えば、通信回線の負荷に関して事前に試験等を実施し、必要となる容量及び能力を想定する等の対策が考えられる。なお、将来にわたっても十分な容量及び能力を確保できるように、余裕を持たせておく必要がある。

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を定めること。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。

解説：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、セキュリティホール等の脅威への対処を確実なものとするために、通信回線装置が必要とするソフトウェアを定めておくことを求める事項である。

4　部局技術責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。

解説：電子計算機が接続されている通信回線の境界で効果的にアクセス制御するために、まず電子計算機をグループ化し通信回線上で分離することを求める事項である。学外通信回線と接続する学内通信回線の場合は、学外通信回線上の電子計算機は、学内通信回線に接続される電子計算機とは別のグループとし、分離する必要がある。

なお、「グループ化」とは、対象機器をその利用目的、求められるセキュリティレベル、管理部門等から分類することをいう。

分離方法として、通信回線の境界にルータ等の通信回線装置を置いて物理的に分離する方法のほか、通信回線装置に VLAN を設定して論理的に分離する方法がある。

5　部局技術責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用し、アクセス制御及び経路制御を行うこと。

解説：グループ化された電子計算機間の通信の制御を行うことで、セキュリティを確保するための事項である。部局技術責任者は、グループ化された電子計算機間で情報システムの運用上必要となる通信を全て確認した上で、通信要件を検討する必要がある。必要最小限のアクセスのみを許可するように、当該通信要件に従ってアクセス制御を行う。

6　部局技術責任者は、要機密情報を取り扱う情報システムについては、通信を秘匿する必要性の有無を検討し、必要があると認めたときは、通信を秘匿するための機能を設けること。

解説：通信における要機密情報を保護するための事項である。部局技術責任者は、通信回線上を要機密情報が送受信される場合には、当該情報の秘匿の必要性を検討して、運用時の暗号化に備えて構築時にそのための機能を設けておく必要がある。

また、通信路の暗号化は、情報の機密性だけでなく完全性を保護する上でも有用である。

なお、通信路の暗号化のために、例えば、IPsec、SSL 及び TLS 等を使用することも考えられる。

7　部局技術責任者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、適切な回線を選択すること。

解説：通信回線に利用する物理的な回線（例えば、有線 LAN における LAN ケーブル、

無線 LAN における伝搬路等の通信路）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措置が異なることから、適切な回線を選択することを求める事項である。
回線に応じたセキュリティ対策を実施する必要があるが、回線によってはセキュリティ対策を実施しても万全でない場合もあるので、回線の選択に当たっては十分に検討する必要がある。また、通信回線を仮想的に構築する場合には、物理的に同一の通信回線となる場合があることに注意する必要がある。

８　部局技術責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。

解説：遠隔地からの通信回線装置の保守や診断に利用するサービスのセキュリティを確保するための事項である。セキュリティ確保の方法として、識別コード及び主体認証情報（パスワード）による主体認証、接続する電子計算機の識別コードによるアクセス制御、通信の暗号化等の機密性の確保だけでなく、通信回線が利用できない状況での代替接続手段の確保等の可用性の確保も挙げられる。

９　部局技術責任者は、通信回線装置を要管理対策区域内に設置すること。

解説：通信回線装置及び通信ケーブルが設置される物理的環境における脅威への対策を求める事項である。
ただし、大学においては例えば廊下に棚を置きそこにハブを設置するなどの例もしばしば見られる。通信回線装置については要管理対策区域内への設置が求められるが、当該機器を含む情報システムにおいて取扱う情報の重要性や取り巻く脅威の大きさによっては、本項を削除し又は修正することもあり得る。遵守困難な事項を定める前に現状を適切に把握し、改善できる点は改善するよう努め、将来の規程の見直しにおいてあらためて規定することも可能である。

１０　部局技術責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。

解説：学内通信回線同士を専用線で接続する場合に、当該専用線のサービスレベルを確保するための事項である。
部局技術責任者自身が契約を行わない場合には、セキュリティレベル及びサービスレベルを含む事項の取決めについて、契約する者に対して依頼すること。なお、セキュリティレベル及びサービスレベルが約款に記述されていれば、それで代替することが可能である。

１１　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、サービス提供に必要な通信回線又は通信回線装置を冗長構成にする必要性を検討し、必要と判断した場合には、その通信回線又は通信回線装置を冗長構成にすること。

解説：障害・事故等によりサービスを提供できない状態が発生した場合、サービスを提供する通信回線又は通信回線装置を代替通信回線又は代替通信回線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を求める事項である。また、災害等を想定して冗長構成にする場合には、その通信回線及び代替通信回線がそれぞれ別の経路となることが望ましい。

１２　部局技術責任者は、通信を行う電子計算機の主体認証を行う必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：通信を行う電子計算機の主体認証を行うことで、通信相手の電子計算機が正しい相手であることを確認するための事項である。

B2152-18　（通信回線の運用時）（政府機関統一技術基準の対応項番 2.3.4.1(2)）

第十八条　部局技術担当者は、通信回線装置のソフトウェアを変更する場合には、部局技術責任者の許可を得ること。

解説：通信回線装置のソフトウェアは機能の改善等を目的に変更を行う必要が生ずる場合がある。この変更の必要性が生じた時に、部局技術担当者は、独断での変更は行わず、部局技術責任者の許可を得てから行う事を求める事項である。

2　部局技術担当者は、通信回線及び通信回線装置の運用管理について、作業日、作業を行った通信回線及び通信回線装置並びに作業内容及び作業者を含む事項を記録すること。

解説：運用管理作業の記録を文書として残すための事項である。
本学において、ある程度統一的な様式を作成することが望ましい。

3　部局技術責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している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こと。

解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生した時に、他の情報システムを保護するための事項である。

4　部局技術担当者は、部局技術責任者の許可を受けていない電子計算機及び通信回線装置を通信回線に接続させないこと。

解説：通信回線に無断で電子計算機及び通信回線装置を接続された場合に生ずるリスクを防止するための事項である。

5　部局技術担当者は、情報システムにおいて基準となる時刻に、通信回線装置の時刻を同期すること。

解説：情報システム内で同期されている共通の時刻に設置した通信回線装置の時刻を同期させることを求める事項である。
情報セキュリティが侵害された際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えないものとする。

6　部局技術担当者は、要安定情報を取り扱う情報システムについては、通信回線装置の運用状態を復元するために必要な措置を講ずること。

解説：障害・事故等によりサービスを提供できない状態が発生した場合に、サービスの可用性を担保することを目的とした事項である。対策としては、通信回線装置の設定情報を作成又は変更した際に、設定情報のバックアップを実施することが挙げられる。
なお、災害等を想定してバックアップを取得する場合には、取得した情報を記録した電磁的記録媒体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ある施設に保存することが考えられる。

7　部局技術責任者は、所管する範囲の通信回線装置が動作するために必要な全てのソフトウェアの状態を定期的に調査する必要性の有無を検討し、必要と認めたときは、当該措置を講じ、

不適切な状態にある通信回線装置を検出した場合には、当該不適切な状態の改善を図ること。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。

解説：通信回線装置における不正なソフトウェアの存在確認等を定期的に行い、対処がなされていない場合にその改善を図ることを求める事項である。

「定期的」とは、1 か月から 6 か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、調査する必要性については、一般的には、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検討することが考えられる。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必要性が高い機器として考えられる。ただし、必要性が低いと判断された機器についても、ソフトウェア等にぜい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。

なお、「不適切な状態」とは、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、定められた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等の状態のことをいう。

8　部局技術担当者は、通信回線装置を不正操作から保護するための措置を講ずること。

解説：部局技術担当者が通信回線装置を第三者による不正操作から保護するための事項である。対策としては、主体認証を行う通信回線装置については、コンソールターミナル等での作業終了後の確実なログアウト、施錠可能なラック内への設置等が挙げられる。

B2152-19　（通信回線の運用終了時）（政府機関統一技術基準の対応項番 2.3.4.1(3)）

第十九条　部局技術責任者は、通信回線装置の利用を終了する場合には、通信回線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：運用を終了した通信回線装置が再利用され、又は廃棄された後、終了前に保存していた情報が漏えいすることを防ぐために、情報の抹消を求める事項である。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。

B2152-20　（端末の学内通信回線への接続の管理）

第二十条　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。

B2152-21　（電子計算機及び情報ネットワーク資源の管理）
第二十一条　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。

B2152-22　（ネットワーク情報の管理）
第二十二条　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。

第二節　学内通信回線の管理

解説：学内通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。また、利用する回線により想定される脅威及びリスクが異なる。
これらのことを勘案し、本節では、学内通信回線に関する対策基準として、学内通信回線の構築時及び運用時、回線の対策についての遵守事項を定める。

B2152-23　（学内通信回線の構築時）（政府機関統一技術基準の対応項番 2.3.4.2(1)）
第二十三条　部局技術責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続することを許可されたものであることを確認する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：通信回線に接続する電子計算機の確認を行うことを求める事項である。
当該措置を実施するための技術としては、電子計算機固有の情報による主体認証、IEEE 802.1x 等が挙げられる。

B2152-24　（学内通信回線の運用時）（政府機関統一技術基準の対応項番 2.3.4.2(2)）
第二十四条　部局技術責任者は、通信要件の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。

解説：適正なアクセス制御の維持を求める事項である。通信要件については、組織、情報システム又はサービスの変更等により変化するため、当該変更等に応じてアクセス制御の設定も見直す必要がある。「定期的」とは、6 か月から 12 か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保

に効果的である。また、必ずしも当該変更等が適時連絡されるとは限らないので、部局技術責任者は定期的にアクセス制御の設定の見直しを行う。

2　部局技術担当者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析する必要性の有無を検討し、必要と認めたときは、当該措置を講じ、通信回線の性能低下及び異常を推測し、又は検知すること。

解説：確保している性能では適正な運用が困難な状態及び通信回線装置等の故障により通信不能な状態等により、情報の可用性を損なう事態を回避するため、通信回線の利用状況及び状態の確認を求める事項である。問題の発生を推測でき、又は検知できた場合には、事前に対策を行うことが求められる。

3　部局技術担当者は、学内通信回線上を送受信される通信内容を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：通信回線上を送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正な行為及び無許可のアクセス等の意図しない事象の発生がないかを監視することが挙げられる。

B2152-25　（回線の対策）（政府機関統一技術基準の対応項番 2.3.4.2(3)）

第二十五条　部局技術責任者は、VPN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

一　利用開始及び利用停止時の申請手続の整備
二　通信内容の暗号化
三　通信を行う電子計算機の識別又は利用者等の主体認証
四　主体認証記録の取得及び管理
五　VPN 経由でアクセスすることが可能な通信回線の範囲の制限
六　VPN 接続方法の機密性の確保
七　VPN を利用する電子計算機の管理

解説：VPN を利用して論理的な学内通信回線を構築する場合に、セキュリティを確保することを求める事項である。「VPN」には、インターネット VPN、IP-VPN、SSL-VPN 等が挙げられる。

2　部局技術責任者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。この場合、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を行う必要性があると判断すること。

一　利用開始及び利用停止時の申請手続の整備
二　通信内容の暗号化
三　通信を行う電子計算機の識別又は利用者等の主体認証
四　主体認証記録の取得及び管理
五　無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限
六　無線 LAN に接続中に他の通信回線との接続の禁止
七　無線 LAN に接続する電子計算機及び通信回線装置の管理

解説：無線 LAN を利用して論理的な学内通信回線を構築する場合に、セキュリティを確保することを求める事項である。無線 LAN を利用する場合は、構築する

環境に応じて措置を講ずることが望ましい。

第二号については、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。なお、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を求めているが、WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信の妨害を発生させることができたりするという脆弱性が報告されており、また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。この場合、暗号化については、暗号と電子署名の標準手順に従わなければならない。

なお、無線 LAN の方式には、通信内容の暗号化と同時にアクセス制限のための利用者認証を行うものが多いが、共有鍵を用いるのではなく、個人認証により利用者を特定して接続を認可することが望ましい。また、MAC アドレスによる接続制限は、認証の目的での有効性が確実ではない。

暗号化方式には AES などがあり、また利用者認証方式には WPA、WPA2、IEEE 802.1x などがあるが、所定の組合せ（WPA2-AES など）から選択して設定することが多い。暗号化の共有鍵を用いる場合には、適切な文字列の長さ及び複雑さを持つように設定する必要がある。

暗号化の強弱は方式によって異なり、暗号化技術の進歩があるので、常に最新の情報を確認して運用する必要がある。初期の暗号化方式として WEP や WPA-TKIP が広く使われたが、暗号化の強度が十分ではなくなったためにセキュリティ対策の効果が期待できなくなったので、Wi-Fi 認定機器では 2011 年から 2014 年までに段階的に禁止される。

参考：岡田仁志編著『ヒカリ＆つばさの情報セキュリティ 3 択教室』第 10 話（国立情報学研究所，2009 年）

第三号については、例えば、通信回線上における主体認証の方式である IEEE 802.1x（クライアント認証及びサーバ認証）を導入し、適切に設定することが考えられる。

第五号については、例えば、利用者等が利用する学内通信回線と学外の者向けに提供する学内通信回線を分離することが考えられる。

第六号については、例えば、無線 LAN に接続中に同時に有線 LAN と接続することを禁止することが考えられる。

第七号については、例えば、無線 LAN に接続する電子計算機及び通信回線装置（無線 LAN アクセスポイント等）の機能で、以下のような管理を行うことが考えられる。

・出力・チャンネル管理等による電波監理

・IEEE 802.1x 等による管理外の無線 LAN アクセスポイント及び電子計算機の検出及び除去

・IPS（Intrusion Prevention System）機能等によるサービス不能攻撃の防御

・MAC アドレス等による接続管理　等

これらは、通信回線装置を要管理対策区域内に設置しても、第三者が区域外から不正に接続してくる可能性があることに注意して、設定する必要がある。

なお、学外の者向けに通信回線を提供する場合は、例えば、事前共有鍵等を利用した暗号化及び認証を行うことや VPN を利用することが考えられる。
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－実践編」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin00.htm）にある、「安全な無線 LAN の利用」のページの解説、及び各府省情報化統括責任者（CIO）補佐官等連絡会議の「無線 LAN セキュリティ要件の検討」（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou.pdf）を適宜参照。

3　部局技術責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

一　利用開始及び利用停止時の申請手続の整備
二　通信を行う者又は発信者番号による識別及び主体認証
三　主体認証記録の取得及び管理
四　リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限
五　リモートアクセス中に他の通信回線との接続の禁止
六　リモートアクセス方法の機密性の確保
七　リモートアクセスする電子計算機の管理

解説：公衆電話網を経由してリモートアクセスを利用する場合に、セキュリティを確保することを求める事項である。

B2152-26　（情報コンセント）

第二十六条　部局技術責任者は、情報コンセントを設置する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

一　利用開始及び利用停止時の申請手続の整備
二　通信を行う電子計算機の識別又は利用者等の主体認証
三　主体認証記録の取得及び管理
四　情報コンセント経由でアクセスすることが可能な通信回線の範囲の制限
五　情報コンセント接続中に他の通信回線との接続の禁止
六　情報コンセント接続方法の機密性の確保
七　情報コンセントに接続する電子計算機の管理

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。

第三節　学外通信回線との接続

解説：学内通信回線と学外通信回線との接続については、学外通信回線に接続された電子計算機からの不正アクセス、サービス不能攻撃等のほか、学外通信回線に送受信される情報の漏えい、改ざん又は破壊等、学外通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本節では、学外通信回線と接続する場合の学内通信回線に関する対策基準として、学内通信回線と学外通信回線との接続時及び運用時についての遵守事項を定める。

B2152-27　（学内通信回線と学外通信回線との接続時）（政府機関統一技術基準の対応項番 2.3.4.3(1)）

第二十七条　全学実施責任者は、全学総括責任者の許可を得た上で、学内通信回線を学外通信回線と接続すること。また、全学実施責任者は、利用者等による学内通信回線と学外通信回線との接続を禁止すること。

解説：学内通信回線を学外通信回線と接続するとリスクの増大を招くので、全学総括責任者の判断を得ることを求める事項である。全学総括責任者は、様々なリスクを検討した上で許可の可否を判断する必要がある。

２　全学実施責任者は、学内通信回線を学外通信回線と接続することにより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通信回線として学内通信回線を構築すること。

解説：学内通信回線に接続している情報システムを、学外からの脅威から保護するための事項である。セキュリティの確保が困難な情報システムについては、他の情報システムと共有している学内通信回線から独立した通信回線として構成するか、学外通信回線から切断した通信回線として構築することになる。独立した通信回線の場合でも、遵守すべき対策基準は実施する必要がある。

B2152-28　（学外通信回線と接続している学内通信回線の運用時）（政府機関統一技術基準の対応項番 2.3.4.3(2)）

第二十八条　全学実施責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、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通信回線に構成を変更すること。

解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生した時に、他の情報システムを保護するための事項である。

２　全学実施責任者は、通信回線の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。

解説：適正なアクセス制御の維持を求める事項である。通信要件については、組織、情報システム又はサービスの変更等により変化するため、当該変更等に応じてアクセス制御の設定を見直す必要がある。「定期的」とは、3 か月から 6 か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、必ずしも当該変更等が適時連絡されるとは限らないので、全学実施責任者は定期的にアクセス制御の設定の見直しを行う。

３　全学実施責任者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。

解説：確保している性能では適正な運用が困難な状態及び通信回線装置等の故障により通信不能な状態等により、情報の可用性を損なう事態を回避するため、通信

回線の利用状況及び状態の確認を求める事項である。問題の発生を推測でき、又は検知できた場合には、事前に対策を行うことが求められる。

4　全学実施責任者は、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こと。

解説：学外通信回線と送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正アクセス等の行為がないかを監視することが挙げられる。

B2152-29　（上流ネットワークとの関係）

第二十九条　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「B2201 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。

第四編　個別事項についての対策

第一節　情報システムへの IPv6 技術の導入における対策

解説：多くの高等教育機関では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 通信プロトコルは IPv4 通信プロトコル環境下と同様にセキュリティ上のリスクがあるとともに、グローバル IP アドレスによる直接通信の利用等に際し考慮すべきリスクも考えられる。また 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いても、新旧の規格が共存することから、十分に検討し、適切な措置を講じないと、情報システムのセキュリティを損なうおそれがある。さらに、昨今、電子計算機及び通信回線装置には IPv6 技術を利用する通信機能が標準で備わっているものが増えていることから、意図せず IPv6 技術を利用する通信機能が動作している可能性がある。このため、それぞれの環境を前提として、対策を講ずる必要がある。

なお、IPv6 に関する最新の動向については、引き続き状況の変化が予想されるため、本学においても、IPv6 のセキュリティ対策に関する動向を十分に注視し、適切に対応していく必要がある。これらのことを勘案し、本節では、IPv6 技術

を利用する情報システム、IPv4 技術を利用する通信と IPv6 技術を利用する通信が共存する情報システムのセキュリティ確保に関する対策基準を定める。

B2152-30　（IPv6 通信がもたらす脆弱性対策）（政府機関統一技術基準の対応項番 2.4.1.1(1)）

第三十条　部局技術責任者は、IPv6 技術を利用する通信（以下「IPv6 通信」という。）を想定して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及びソフトウェアについて、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に IPv6 Ready Logo Program に基づく Phase-2 準拠製品がある場合には、当該製品を情報システムの構成要素として選択すること。

解説：IPv6 に対応する機器等の購入において、一定水準以上のセキュリティ機能を有する製品を選択することを求める事項である。国際的な IPv6 に関する標準プログラムである IPv6 Ready Logo Program による客観的な基準に準拠する製品を選択することにより、安全性の高い情報システムの構築が期待できる。

2　部局技術責任者は、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 アドレスによる直接の到達性における脅威を防止するための措置を講ずること。

解説：IPv6 で新たに導入された通信制御機構や、IPv6 の特徴である外部ネットワークとの直接接続の容易さに起因する各種攻撃への対策を求める事項である。
対策としては、不正な機器からの経路調査コマンド（traceroute　等）及び ICMP エコー要求等に応答しない、サービス不能攻撃への対策、並びに認可した宛先からのみアクセスを可能にする等が挙げられる。

3　部局技術責任者は、IPv6 通信を想定して構築する情報システムにおいて、不正な通信を制限するフィルタリングを適切に行うこと。

解説：IPv6 の特徴として、アドレスが長い、アドレスの省略形が複数パターン存在し一意に定まらない、端末が複数の IP アドレスを持つ等が挙げられる。このような複雑なアクセス制御が設定の不備等を招き不正アクセス等に繋がるリスクが高まるため、フィルタリングを適切に実施することを求める事項である。
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。

4　部局技術責任者は、情報システムに IPv6 通信の機能を導入する場合には、IPv6 移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。

解説：IPv4 技術を利用する通信と IPv6 通信の両方を共存させることを可能とする IPv6 移行機構の選定と利用に当たり、必要な措置を求める事項である。
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電子計算機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、学内のネットワークが外部から攻撃される危険性がある。管理された電子計算機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等、不適切な IPv6 通信を制御する対策が必要である。

5　部局技術責任者は、IPv6 通信を想定して構築する情報システムにおいて、IPv6 に対応していない機器及びソフトウェアの利用によるセキュリティの問題がないように措置を講ずること。

解説：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のセキュリティ上のリスクに対する対策を求める事項である。

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等が挙げられる。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。

B2152-31　（意図しない IPv6 通信の抑止と監視）（政府機関統一技術基準の対応項番 2.4.1.1(2)）

第三十一条　部局技術責任者は、学内のみで利用する情報システムについて、IPv6 通信を想定していない通信回線に接続される全ての電子計算機及び通信回線装置に対して、IPv6 通信を抑止するための措置を講ずること。

解説：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措置を求める事項である。

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侵入検知システム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 通信が可能な電子計算機においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該電子計算機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、電子計算機と外部のネットワークとの間に利用者や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電子計算機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、学外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 通信を抑止するための措置を講ずることが必要である。

2　部局技術責任者は、学内のみで利用する情報システムについて、IPv6 通信を想定していない通信回線を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を講ずること。

解説：意図しない IPv6 通信が情報システムに与える脅威から情報システムを守るための事項である。
IPv6 技術にはアドレスの自動構成機構が提供されている。電子計算機から送出されるアドレスの自動構成を要求する通信パケットや、ルータから送出されるアドレスの自動構成を提供する通信パケットが学内通信回線を流れている場合には、管理者や利用者が気付かないうちに IPv6 技術のアドレス自動構成機構が利用されていることを示唆している。また、IPv6 通信を想定していない学内通信回線において、IPv6-IPv4 トンネル機構で使用する通信パケットが検知された場合は、IPv6 技術を使った悪意のある通信がなされているおそれがある。学内通信回線を管理する者は、このような通信の有無を監視して、IPv6 通信が検知された場合は、当該通信の遮断等の措置を講ずる必要がある。
なお、学外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 通信を遮断するための措置を講ずることが必要である。

別表1　情報取扱区域のクラス別管理

行番号	遵守事項	対策例		備考	クラス0	クラス1	クラス2	クラス3
1	〔凡例〕クラス0～クラス3までの列に記載している内容は、それぞれのクラスにおいて、各欄の左側に記載された措置・対策・実施に対して、以下のとおり。 **要**：必要、**不要**：不要、**可**：使用可能又は設定可能、**禁**：禁止（許可（届出）申請が必要）、**対象外**：対象外							
2	（1）立ち入る者を制限するための管理対策							
3	（ア）不審者を立ち入らせない措置 2.3.1.1(1)(a)(ア)	所在の表示（案内板の表示等）	クラス0の表示		対象外	可		
4			クラス1の表示	・例）学校名、学部等の名称	可			
5			クラス2の表示	・例）部局名、会議室名	可			
6			クラス3の表示	（※1） サーバ室は非表示	可（※1）			
7	（イ）要保護情報を取り扱う情報システムについては、区域間を物理的に隔離し、立入り及び退出を管理するための措置 2.3.1.1(1)(a)(イ)	入退出可能な下位区域との接続	クラス0との接続		対象外	不可		
8			クラス1との接続		対象外		可	
9			クラス2との接続		対象外			可
10			クラス3との接続		対象外			
11		下位の区域との分離方法	天井を突き抜ける壁		対象外	可		
12			天井と接する固定式パーティション、壁		対象外	可		
13			天井と接しない固定式パーティション		対象外	可		禁
14			可動式パーティション		対象外	可		禁
15		管理方法	立入り及び退出の管理方法		対象外	・セキュリティゲート ・警備員等による立ち番	・施錠可能な扉、間仕切り等。ただし、ドアガラス等で中が見えても良い。	・施錠可能な扉等。中が見えないこと。
16			全員不在時に制限	（制限方法例） ・扉等を施錠 ・出入口に警備員等を配置し、入退出する者を確認	対象外	要		
17			常に制限		対象外			要
18	（2）立ち入る者を許可する際の管理対策							
19	（ア）立ち入る者の確認 2.3.1.1(2)(a)(ア)			「立ち入る」とは、「下位のクラスの区域から上位のクラスの区域への立入り」を指す。	対象外	要		
20	（イ）退出する者の確認 2.3.1.1(2)(a)(イ)			「退出」とは、「上位のクラスの区域から下位のクラスの区域への退出」を指す。	対象外	不要		
21	（ウ）許可されていない者の立入り及び退出を制限する措置 2.3.1.1(2)(a)(ウ)				対象外	要		

別表1　情報取扱区域のクラス別管理

行番号	遵守事項		対策例		備考	クラス0	クラス1	クラス2	クラス3
22	(エ) 継続的に立ち入る者を許可する手続 2.3.1.1(2)(a)(エ)					対象外	要		
23	(オ) 継続的に立入りを許可された者に変更がある場合の手続 2.3.1.1(2)(a)(オ)					対象外	要		
24	(カ) 立入り及び退出の記録及び監視 2.3.1.1(2)(a)(カ)				・例) 警備員又は防犯カメラ等の導入	対象外	不要		要
25	(3) 訪問者がある場合の管理対策								
26	(ア) 訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置 2.3.1.1(3)(a)(ア)		登録申請(訪問者の身元確認)	事前貸与者(※2)	・学外施設等、本学で管理対策を講ずることが出来ない場合は、当該施設等に対策状況を確認するなどして、管理対策を決定する。 (※2) ・「事前貸与者」とは、事前に識別カードを貸与されている者を指す。(学外の者で、継続的に立入りを許可された者) ・「訪問者」とは、事前に識別カードを貸与されていない者を指す。 ・「事前に識別カードを貸与されている」とは、民間事業者等に、継続的な立入りのために本学のセキュリティゲートを通過可能な識別カードを貸与している場合を指す。 (※3) ・クラス0からクラス1へ進入する際の確認・審査で代替とすることも可能	不要			要
27				訪問者(※2)		不要	要	要 (※3)	
28	(イ) 訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置 2.3.1.1(3)(a)(イ)		訪問記録	事前貸与者(※2)		不要			要
29				訪問者(※2)		不要			要
30	(ウ) 訪問相手の事務従事者が訪問者の情報取扱区域への立入りについて審査するための手続の整備 2.3.1.1(3)(a)(ウ)		登録申請(訪問者の立入り時の審査)	事前貸与者(※2)		不要			要
31				訪問者(※2)		不要	要	要 (※3)	
32	(エ) 訪問者の立ち入る区域を制限するための措置 2.3.1.1(3)(a)(エ)			事前貸与者(※2)		不要			要
33				訪問者(※2)		不要	不要		要
34	(オ) 訪問相手の事務従事者による訪問者に付き添う措置 2.3.1.1(3)(a)(オ)		事務従事者の帯同、エスコート	事前貸与者(※2)		不要			要
35				訪問者(※2)		不要	不要		要
36	(カ) 訪問者と継続的に立入りを許可された者とを外見上判断できる措置 2.3.1.1(3)(a)(カ)		・訪問者と継続的に立入りを許可された者との外見上の区別			不要	要		
37	(4) 設置する設備の管理対策								
38	要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している電子計算機及び通信回線装置の盗難及び当該場所からの不正な持ち出しを防止するための措置 2.3.1.1(4)(a)	端末	・セキュリティワイヤーによる固定		(※4) 当該クラスへの立入りの際に立ち入る者の確認を行う等の措置をとり、入退出者を制限できる場合は、部屋全体の施錠管理にて対策を講ずることも考えられる。	対象外	要	要(※4)	
39		サーバ装置	・機器扉付きラック等で施錠管理 ・セキュリティワイヤーによる固定			対象外	要	要(※4)	
40		通信回線装置 (装置への主体認証が必要なもの)	・機器扉付きラック等で施錠管理			対象外	要	要(※4)	
41		通信回線装置 (装置への主体認証が不要なもの)				対象外	要	要(※4)	
42	要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置の設置に係る対策 2.3.1.1(4)(b)	(ア) 他の区域との物理的な隔離				対象外	不要	要	
43		(イ) 表示用デバイスの盗み見防止				対象外	不要		要
44		(ウ) 電源ケーブル及び通信ケーブルの損傷及び盗聴防止	・ケーブルの床下への埋設 ・ケーブルのナンバリング			対象外	不要		要

別表1　情報取扱区域のクラス別管理

行番号	遵守事項		対策例		備考	クラス0	クラス1	クラス2	クラス3
45		(エ) 電磁波による情報漏えい対策	・電磁波軽減フィルタの利用			対象外	不要		
46	(5) 作業がある場合の管理対策								
47		当該区域内での作業を監視するための措置 2.3.1.1(5)(a)	事務従事者の作業の立会、監視	・当該作業に関係する他の事務従事者による同行、立会		対象外	不要		
48				・監視カメラ等による監視		対象外	不要		要
49			業者の作業の立会、監視	・担当の事務従事者による同行、立会		対象外	不要		要
50				・監視カメラ等による監視		対象外	不要		要

別表2　情報取扱区域のクラス別利用制限

行番号	遵守事項		対策例	備考	クラス0	クラス1	クラス2	クラス3
1	（凡例） 許可：（部局技術責任者及び職場情報セキュリティ責任者からの）許可が必要、 届出：（部局技術責任者及び職場情報セキュリティ責任者への）届出が必要（部局技術責任者及び職場情報セキュリティ責任者が届出不要と判断した場合は、不要）、 禁止：原則禁止（許可を求める場合は、例外措置の適用の申請が必要（事務情報セキュリティ対策管理基準に定める許可権限者の承認が必要））、 要：必要、不要：許可又は届出が不要、可：設置可能、対象外：対象外							
2	（1）立ち入る者を制限するための利用制限対策							
3	事務従事者であることを常時視認することが可能な状態にすること 2.3.1.1(6)(a)		識別カードの着用、明示（学外の者も含む）		不要	要		
4	（2）物品の持込み、持ち出し及び利用についての利用制限対策							
5	要保護情報を取り扱う情報システムに関連する物品の持込み及び持ち出しに係る対策 2.3.1.1(7)(a)	（ア）持込み及び持ち出しを行う措置			対象外	不要		
6		（イ）記録の保存			対象外	不要		
7		（ウ）情報システムに関連しない電子計算機等の持込みの制限	荷物検査		対象外	不要		
8	事務従事者の所持する府省庁支給以外の情報システム（モバイル端末及び記録装置）の持込みの制限等 2.3.1.1(7)(a)	（ウ）情報システムに関連しない電子計算機等の持込みの制限		・荷物の持込を許可しない場合は、荷物の預りを可能にする環境構築が必要。	対象外	不要		不要
9			起動・利用 （学内LAN未接続、要保護情報は取り扱わない場合）	・「起動・利用」は「持込」が前提 （※1） 学内通信回線への接続を認める場合は、学内のすべての情報にアクセスできる可能性があるリスクを考慮すること。	対象外	不要		
10		モバイル端末の起動・利用 1.4.2.2(2)(a) （機密性3情報、完全性2情報又は可用性2情報を取り扱う場合）			許可(※1)			
11		モバイル端末の起動・利用 1.4.2.2(2)(b) （機密性2情報であって完全性1情報かつ可用性1情報を取り扱う場合）			届出(※1)			
12	学外の者の所持するモバイル端末及び記録装置の持込みの制限等 2.3.1.1(7)(a)、 1.2.5.3(3)(b)	（ウ）情報システムに関連しない電子計算機等の持込みの制限		・荷物の持込を許可しない場合は、荷物の預りを可能にする環境構築が必要。	対象外	不要		要
13			起動・利用 （学内LAN未接続）	・「起動・利用」は「持込」が前提	対象外	不要		
14	事務従事者による写真撮影、録音 2.3.1.1(7)(b)			（※2） 許可又は届出先となる主体は、当該区域を管理する区域情報セキュリティ責任者となるが、許可又は届出の窓口は担当の事務従事者が行うことが考えられる。	対象外	不要		
15	学外の者による写真撮影、録音 2.3.1.1(7)(b)、1.2.5.3(3)(b)				対象外	不要	要（※2）	

別表2　情報取扱区域のクラス別利用制限

行番号	遵守事項	対策例		備考	クラス0	クラス1	クラス2	クラス3
16	(3) 荷物の受渡しについての利用制限対策							
17	受渡し管理 2.3.1.1(8)(a)	宅配便、荷物			不要		要	
18		要保護情報又は機密性1情報			不要			
19	(4) 情報処理の制限							
20	要管理対策区域外での情報処理の制限 1.4.2.1(2)(a)(b)	機密性2情報について情報処理を行う場合			届出	対象外		
21		機密性1情報並びに完全性2情報又は可用性2情報について情報処理を行う場合			許可	対象外		
22		機密性3情報について情報処理を行う場合			許可	対象外		
23	(5) 設備の設置							
24	端末の設置 2.3.2.1(1)(b)			・追加で設置する場合 ・モバイル端末について部局総括責任者の承認を得た場合は、この限りでない。	禁	可	可	
25	通信回線装置の設置 2.3.4.1(1)(i)				禁	可	可	
26	サーバ装置の設置 2.3.2.1(1)(b)				禁	禁	可	
27	(6) ネットワークの接続							
28	通信回線構築によるリスクを検討し、通信回線を構築すること 2.3.4.1(1)(a) 無線LAN環境を構築する場合に、必要に応じて措置を講ずること 2.3.4.2(3)(b)	学内LAN	クラス0のLANとの接続	・追加で設置する場合	対象外	(学外通信回線との接続に準じる)		
29			クラス1のLANとの接続		(学外通信回線との接続に準じる)	可	不可	
30			クラス2のLANとの接続			不可	可	
31			クラス3のLANとの接続				可	
32		無線LAN	クラス0の無線LANとの接続	・追加で設置する場合 ・他の区域との接続制限の例：MACアドレス、IEEE802.1x等による接続制限	対象外	(学外通信回線との接続に準じる)		
33			クラス1の無線LANとの接続		(学外通信回線との接続に準じる)	可	不可	
34			クラス2の無線LANとの接続			不可	可	可
35			クラス3の無線LANとの接続				可	可
36		学内から本学管理外のネットワーク経由でのインターネット直接接続		・学内通信回線（学内LAN）へは、接続禁止が前提 ・「本学管理外のネットワーク」とは、Wi-fiルータ（学外通信回線へ直接接続可能な通信回線装置）等の利用によるインターネットへの直接接続を想定	対象外	不可		

B2153 アプリケーションソフトウェアに関する技術規程

第一章　電子メール（政府機関統一技術基準の対応項番 2.3.3.1）

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等の機密性に対するリスクがある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれる等の可用性に対するリスクがある。この他、内容を偽ったメールによるいわゆるフィッシング詐欺等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。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要である。

これらのことを勘案し、本章では、電子メールサーバの管理及び電子メールの利用に関する対策基準として、電子メールの導入時及び運用時についての遵守事項を定める。

B2153-01　（電子メールの導入時）（政府機関統一技術基準の対応項番 2.3.3.1(1)）

第一条　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。

解説：迷惑メールの送信等に使われることを回避するために、電子メールを不正に中継しないように電子メールサーバを設定することを求める事項である。

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利用者等の主体認証を行う機能を備えること。

解説：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 認証等の主体認証を行うことを定めた事項である。

３　部局技術責任者は、電子メールの送信元について、なりすましの防止策を講ずること。

解説：電子メールの送信時及び受信時において、なりすましを防止することを求める事項である。

「なりすましの防止策」には、平時から行う防止策、電子メールの送信時に行う防止策及び電子メールの受信時に行う防止策等がある。これらの防止策は、第３レベルのドメインだけでなく、第４レベル以上のドメインについても、考慮する必要がある。

（ア）平時から行うなりすましの防止策として、Sender Policy Framework（以下「SPF」という。）、SenderID 及び DomainKeys Identified Mail（以下「DKIM」という。）を利用した送信側における送信ドメイン認証等が挙げられる。（なお、「SenderID」及び「DKIM」は、それぞれ送信ドメイン認証の１つである。）これらは、電子メールで使用するドメインを管理する DNS サーバに、電子メールサーバの情報や署名で使用する公開鍵の登録・公開を行う。なお、SPF や SenderID における DNS サーバへの電子メールサーバ情報の登録では、次の事項に留意する必要がある。

・電子メールを利用していないドメインは、その情報を登録する必要があること。

・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、若しくは将来にわたって利用の予定のないドメインについては、なりすましの防止策を講ずるか、又はドメイン名の登録を廃止すること。
・SPF レコードについては、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こと。（なお、「SPF レコード」とは、SPF や SenderID において、DNS サーバの TXT レコードに記述される送信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”を記述すること。
・電子メールサーバを外部委託先において運用している場合には、外部委託先のグローバルIPアドレスを本学のものとしてSPFレコードに登録することは、同じ IP アドレスを民間業者も共用し、なりすましのおそれがあること。このため、外部委託先には、同じサーバの他の利用者によるなりすまし防止策を講じたり、本学ドメイン名を使用する機関向けに民間業者と共用しない専用の IP アドレスを割り振られたりした場合を除き、外部委託先のグローバル IP アドレスを SPF レコードに登録することは認められない。
（イ）電子メールの送信時に行うなりすましの防止策として、S/MIME や DKIM を利用した送信メール（メールマガジンを含む）への電子署名の添付等が挙げられる。
（ウ）電子メールの受信時に行うなりすましの防止策として、電子署名の検証及び受信側における SPF の検証（具体的には、受信時に通信を行った送信側の電子メールのサーバと、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電子メールサーバの情報との比較によるなりすましの判定）等が挙げられる。

B2153-02　（電子メールの運用時）（政府機関統一技術基準の対応項番 2.3.3.1(2)）

第二条　部局技術責任者は、電子メールの運用につき、教職員等及び利用者等に次の事項を遵守させること。

一　教職員等は、業務遂行に係る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。ただし、本学支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。

解説：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以外の電子メールサービス（以下「本学以外の電子メールサービス」という。）を、業務遂行に係る情報を含む電子メールの送受信に利用することを禁ずる事項である。なお、上記の「送受信」には電子メールの「転送」が含まれている。したがって、本学以外の電子メールサービスの電子メールアドレスに業務遂行に係る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、要機密情報の移送についての遵守事項に違反しないようにも留意する必要がある。

２　利用者等は、受信した電子メールにより、スクリプトが電子計算機で実行されないように電

子メールの内容を表示させること。

解説：例えば HTML メールの表示により、偽のウェブサイトに誘導するために表示が偽装されること、意図しないファイルが外部から取り込まれること等の不正なスクリプトが実行されることを防ぐことを定めた事項である。

「スクリプト」とは、ここでは JavaScript 等の電子計算機にて簡易的に実行することができるプログラムをいう。

「スクリプトが電子計算機で実行されないように表示させる」とは、表示をテキスト形式のみに設定して表示することや端末でスクリプトの実行を禁止された情報システムを用いて表示することが挙げられる。

そのため、情報システムの管理者により、利用者等が使用する電子メールクライアントの設定が上述のとおり適切に行われ、かつ、利用者等が電子メールクライアントの設定を勝手に変更しないよう制限することにより対策を実施することも考えられる。

なお、本遵守事項は、スクリプトが電子計算機で実行されないのであれば、電子メールの文字装飾や画像の表示を禁止するものではない。

また、本遵守事項は、端末等にインストールされる電子メールクライアントを対象としているため、ウェブブラウザにより読み書きする電子メール（いわゆるウェブメール）は対象外となる。

第二章　ウェブ（政府機関統一技術基準の対応項番 2.3.3.2）

解説：ウェブを利用するに当たっては、サーバにおいて、OS 等既成のソフトウェアや開発したウェブアプリケーション等の複数の要素で構成されていること、一方で、クライアントにおいてもサーバと同様に情報処理が行われていることから、様々な脅威が考えられる。

これらのリスクを回避するためには、システムのライフサイクル全般に対して適切な対策を組み合わせて実施することが必要である。

これらのことを勘案し、本章では、ウェブに関する対策基準として、ウェブサーバの導入、ウェブアプリケーションの開発、ウェブの運用についての遵守事項を定める。

なお、ウェブサーバの導入及び運用については、本章に加えて、「B2152 情報システムの構成要素に関する技術規程」第 2 章第 3 節にて定めたサーバ装置に係る対策基準を、また、サービス不能攻撃等のウェブにおける脅威への対策としては、「B2151 情報セキュリティ要件の明確化に関する技術規程」第 2 章第 3 節にて定めた情報セキュリティについての脅威に係る対策基準を参照する必要がある。

B2153-03　（ウェブサーバの導入時）（政府機関統一技術基準の対応項番 2.3.3.2(1)）

第三条　部局技術責任者は、情報セキュリティが確保されるよう適切にウェブサーバのセキュリティ設定をすること。適切なセキュリティ設定として、以下に挙げる事項を含む措置を講ずること。

一　ウェブサーバの機能を適切に制限すること。

二　ウェブサーバに保存された情報へのアクセス制限を適切に設定すること。
三　識別コードを適切に管理すること。
四　通信時の盗聴による情報漏えいのリスクを検討し、必要と判断した場合には、暗号化と電子証明書による認証の機能を設けること。

解説：ウェブサーバの導入時の設定に関して以下の項目を適切に行うことにより、セキュリティを確保することを求める事項である。
第一号は、ウェブサーバで提供する機能の内、不要な機能を停止又は制限することを求めている。例えば、スクリプトやファイル実行の制限や保存場所の限定、インデックス表示の禁止、ホームページ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の制限等が挙げられる。
第二号は、情報の漏えいやウェブページの改ざんを防ぐために、情報へのアクセス権限を適切に設定することを求めている。例えば、ウェブコンテンツファイルへのアクセス権限は、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、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等が挙げられる。
第三号は、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の適切な管理を求めている。これらの識別コードはブルートフォース（総当たり）攻撃の標的になるリスクがあるため、その必要性を確認して、不要なものは削除することが重要である。また、初期状態で用意されるサンプルのページ、プログラム等も削除するといった注意が必要である。
第四号は、通信時の盗聴による第三者への情報漏えいの防止及びウェブサーバの詐称を利用者が検知できるようにするための事項である。第三者への漏えいを防止する必要のある情報には、例えば、サービスの利用者の個人情報等が挙げられる。ウェブサーバにおいてこれらを解決するための機能としては、例えば、SSL 及び TLS が挙げられる。この機能を設けることにより、通信内容の暗号化が可能になるとともに、ウェブサーバの利用者は、ウェブサーバの電子証明書を参照することでその正当性を確認することができる。
なお、本学のウェブサーバに電子署名を付与する必要があると認めたときの SSL 及び TLS に用いる電子証明書は、全国大学共同電子認証基盤（UPKI）で発行したものを使用することが望ましい。

2　部局技術責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバに保存する情報を特定し、当該サーバに特定した情報以外の要機密情報が含まれないことを確認すること。

解説：万が一、不正侵入等が発生した場合であっても、当該サーバから要機密情報が漏えいしないよう、被害範囲の限定を図るための事項である。利用が想定されていないデータ等を、ウェブサーバに保存しないことが必要である。

B2153-04　（ウェブアプリケーションの開発時）（政府機関統一技術基準の対応項番 2.3.3.2(2)）
第四条　部局技術責任者は、情報セキュリティが適切に確保されるようにウェブアプリケーションの開発においてセキュリティ対策機能を組み込むこと。適切なセキュリティ機能として、以

下に挙げる事項を含む措置を講ずること。

一　利用者による URL の確認を妨げないこと。

二　主体認証と情報へのアクセス制御を適切に行うこと。

三　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限定すること。

四　不正な入力データを排除すること。

五　不正な出力データを排除すること。

六　安全なセッション管理を行うこと。

解説：ウェブアプリケーションの開発を行う場合に、以下のセキュリティ機能を実装することにより、セキュリティを確保することを求める事項である。

なお、セキュリティ機能の実装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「セキュアプログラミング講座」（http://www.ipa.go.jp/security/awareness/vendor/programming/index.html）の「Web アプリケーション編」または、「安全なウェブサイトの作り方」（http://www.ipa.go.jp/security/vuln/websecurity.html）を適宜参照することが望ましい。

第一号は、利用者が URL（ウェブアドレス）を確認できない場合、攻撃者が用意した危険なサイト（フィッシングサイト等）に誘導される可能性があることから、それを避けることを求めるものである。この対策としては、例えば、アドレスバーを隠さない、右クリックを無効にしない等が挙げられる。

第二号は、主体認証を行うウェブアプリケーションにおいて、パスワード等の漏えいによる利用者のなりすまし防止や主体認証後の利用者のファイルへのアクセスについて適切に制御することを求めるものである。ユーザ ID とパスワードによって主体認証を行う場合、例えば、パスワードの設定時にその文字列に適切な条件を課す、利用者本人がパスワードを変更できるようにする、入力されたパスワードは隠し文字にして表示しない等の対策が挙げられる。また、利用者が設定したパスワードはハッシュ関数を用いて復元できない形にすることも重要である。ファイルへのアクセス制御については、ウェブサイトでどの主体がどの情報にアクセスする必要があるのかについて検討し、それに基づきアクセス制御を設計・実装することが重要である。特に、主体認証後にのみ参照可能なファイルが主体認証前に参照できてしまうことがないよう、適切にアクセス制御を行うことが求められる。

第三号は、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と、公開を想定しないファイルが参照されるリスクがあり、これを防止することを求めるものである。この対策としては、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のが安全だが、これができない場合は、例えば、ファイルにアクセスする前に入力されたパラメータの検査を行う、ファイルのディレクトリと識別子を固定の文字列にしてアクセスする等の方法が挙げられる。

第四号は、ウェブサーバを用いて提供するサービスにおいて、利用者から文字列等の入力を受ける場合には、不当な入力データを排除することによって、バッファオーバフロー攻撃や SQL インジェクション等の攻撃を防ぐことを求め

るものである。対策としては、例えば、ウェブアプリケーションへの入力を正しく定義し、不正なデータが渡されないよう、入力されたパラメータの長さや内容を検査し、無害化する機能を設ける等が挙げられる。
第五号は、ウェブアプリケーションが出力する画面や OS の関数、SQL コマンド等の呼び出しといった出力情報に不正なデータの混入を排除することにより、クロスサイトスクリプティングや SQL インジェクション等の攻撃を防止することを求めるものである。対策としては、例えば、HTML に埋め込むデータを全て検査してエスケープ処理する、外部プログラムを呼び出す際のプログラム名、オプション、パラメータ等はできる限り固定の文字列にする等が挙げられる。また、ウェブアプリケーション又はデータベース等から発信されるエラーメッセージ、稼動している製品名及びそのバージョン、登録されているユーザ ID 等は、攻撃を試みる者に対し攻撃の糸口となり得る情報を与えてしまう危険性がある。これらのことを回避するため、不必要な情報は出力しない措置を講ずることが求められる。
第六号は、セッション管理の不備により利用者になりすましてアクセスされることを防止するため、適切なセション管理を求めるものである。対策としては、例えば、セション ID の有効期間を主体認証直後のレスポンスからログアウトまでに限定する、推測困難なセッション ID を設定する、セッション ID を URL パラメータに格納しない、Cookie に入れる情報はセッション ID 以外に必要最小限とする、SSL を使用する Cookie は secure 属性にする等が挙げられる。

B2153-05　（ウェブの運用時）（政府機関統一技術基準の対応項番 2.3.3.2(3)）

第五条　部局技術責任者は、ウェブの運用につき、利用者等に次の事項を遵守させること。

一　利用者等は、情報セキュリティの確保がなされるよう適切にウェブクライアントのセキュリティ設定をすること。

解説：利用者等が意図しない悪意のあるソフトウェアが電子計算機において実行されること等により、情報が漏えいしてしまうことや他の電子計算機を攻撃してしまうこと等を防止するため、ウェブクライアントのセキュリティ設定を適切に行うことを求める事項である。
具体的には、閲覧するウェブサイトの信頼性やウェブクライアントが動作する電子計算機にて扱う情報の機密性等に応じて、以下のようなセキュリティ設定項目について適切な値を選択すること。

・ActiveX コントロールの実行
・JavaScript の実行
・Java の実行
・Cookie の保存　等

そのため、情報システムの管理者がウェブクライアントのセキュリティ設定を上述のとおり行い、かつ、利用者等が当該設定を勝手に変更しないよう制限することにより対策を実施することも考えられる。

二　利用者等は、ウェブクライアントが動作する電子計算機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。

解説：ソフトウェアをダウンロードする場合は、電子署名により配布元の正当性を確認することを求める事項である。

三　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。

イ　送信内容が暗号化されること。

解説：主体認証情報等を入力して送信する場合には、情報漏えいを防止するため、ブラウザの鍵アイコンの表示を確認する等により、SSL や TLS 等の暗号通信が使用されていること等の手段を限定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を使用する際に主体認証情報等を入力すること等を指す。

ロ　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：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かを確認することにより、当該情報の送信先を限定することを求める事項である。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ないかを確認することが必要である。

2　部局技術責任者は、利用者等が閲覧することが可能な学外のウェブサイトを制限する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、定期的にその見直しを行うこと。

解説：ウェブサイトからの不適切なソフトウェアのダウンロードや私的なウェブサイトの閲覧を制限するため、コンテンツフィルタ等により閲覧することが可能な範囲の制限を定める事項である。

部局技術責任者は、制限を実施する方法として、ウェブクライアント、ウェブプロキシ及びその他の装置の設定等、状況に応じて、適切な方法を選択することが可能である。

第三章　ドメインネームシステム（DNS）（政府機関統一技術基準の対応項番 2.3.3.3）

解説：ドメインネームシステム（DNS：Domain Name System）は、クライアント等からの問い合わせを受けて、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インターネットの基盤をなすサービスである。DNS 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 DNS 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、クライアント等が悪意あるサーバに接続させられる等の被害にあう可能性がある。このようなリスク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。

これらのことを勘案し、本章では、DNS に関する対策基準として、DNS の導入時及び運用時についての遵守事項を定める。

B2153-06　（DNS の導入時）（政府機関統一技術基準の対応項番 2.3.3.3(1)）

第六条　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、名前解決を停止させないための措置を講ずること。

解説：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、名前解決を停止させないために、求められる可用性の度合いに応じた措置を求める事項である。

DNS の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等、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、冗長化による措置の例である。あるいは、悪意ある者からのサービス不能攻撃に備え、ソフトウェアや通信回線装置で適切なアクセス制御を実施しておくことも重要である。

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。

2　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を運用管理するための手続を定めること。

解説：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（ゾーン情報）を運用管理するための手続を定めることを求める事項である。

「管理するドメインに関する情報を運用管理するための手続」では、例えば、管理するドメインに関する情報の設定や更新、正確性の維持等の手順や管理するドメインの構成範囲を明確化しておくことが考えられる。

3　部局技術責任者は、DNS の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。

解説：DNS のキャッシュサーバの第三者による不正利用やキャッシュ情報の汚染等を防ぐための措置を講ずることを求める事項である。キャッシュサーバにおいては、学外からの名前解決の要求には応じず、学内からの名前解決の要求のみに回答を行うように措置を講ずる必要がある。キャッシュサーバを動作させる場合は、サーバの設定やファイアウォール等でアクセス制御を行うことが重要である。

また、適正な名前解決の代行を維持するために、ルートヒントファイルの更新の有無を定期的に確認し、最新のものに維持する必要がある。「定期的」とは、3 ヶ月に一度程度実施することを想定している。

4　部局技術責任者は、DNS の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、当該情報が外部に漏えいしないための措置を講ずること。

解説：DNS の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、本学の利用者等以外の者が内部のみで使用している名前情報を取得できないようにすることを求める事項である。例えば、内部向けの名前解決を提供するコンテンツサーバを外部向けのコンテンツサーバとは別々に設置し、サーバの設定やファイアウォール等でアクセス制御を行う等の方法が考えられる。

5　部局技術責任者は、情報システムに対し名前解決を提供する DNS サーバにおいて、コンテン

ツサーバによるドメイン名の情報提供時には電子署名を付与し、キャッシュサーバによる名前解決時には電子署名を検証する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：電子署名によって DNS のコンテンツサーバのなりすましや同サーバからの提供情報の改ざんを DNS のキャッシュサーバで検出できるようにすることを求める事項である。その対策としては、DNSSEC の利用等が挙げられる。

DNSSEC は、公開鍵暗号技術を用いて改ざん等を防止するため、その導入には情報の提供側である DNS のコンテンツサーバと情報の問い合わせ側である DNS のキャッシュサーバの双方に対応が必要となる。

社会への信頼できるサービスの提供と、学内の情報セキュリティ向上の観点から、本学ドメインを管理する DNS のコンテンツサーバ、及び本学の DNS 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。

B2153-07　（DNS の運用時）（政府機関統一技術基準の対応項番 2.3.3.3(2)）

第七条　部局技術担当者は、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。

解説：複数台の DNS のコンテンツサーバが保有し管理するドメインに関する情報について、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の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の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 の利用等が考えられる。

2　部局技術担当者は、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を運用管理するための手続に基づいて、当該情報が正確であることを適宜確認すること。

解説：管理するドメインに関する情報が正確であるかどうかを確認することを求める事項である。管理するドメインに関する情報の設定ミスや不正な改ざん等が発生していないかを確認する必要がある。管理するドメインに関する情報の具体例として、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 レコード等がある。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。

B2201 情報システム利用規程

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（B2201-12、B2201-13、B2201-14 および B2201-15）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。

B2201-01　（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。

B2201-02　（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「B1000 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「B1001 大学情報システム運用基本規程」をいう。

三　全学アカウント　本学の全学統一認証に対応した情報システムの利用に当たって用いるアカウントをいう。

四　三に加え、本学が契約し外部委託したシステムおよびサービス利用のためのアカウントも含むものとする。

五　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。

B2201-03　（適用範囲）

第三条　この規程は本学構成員および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。

２　本学情報システムとは、A 大学が設置もしくは契約により使用もしくは提供をうけているネットワーク、情報機器および情報サービスのことである。ただし、事務情報システムについては「B2501 事務情報システム対策管理基準」「B2551 事務情報システム対策技術基準」および「B3501 各種マニュアル類」に別途定める。

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 CNISD-K303-101-1C（案）(http://www.nisc.go.jp/active/general/pdf/K303-101-1C_draft.pdf)等を参考に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、「B3501 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。

B2201-04　（遵守事項）

第四条　本学情報システムの利用者は、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。

B2201-05　（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、「A 大学情報システム利用申請書」を管理運営部局に提出し、全学実施責任者から全学アカウントの交付を受けなければならない。

２　学会等での訪問者によるネットワーク等の臨時的利用について全学アカウントが必要である。会合等の主催者は臨時に全学アカウントの取得および来訪者による利用をさせた場合には来訪者に本規程を遵守させなければならない．臨時のアカウントは不要になった場合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、「B1001 情報システム運用基本規程」の B1001-08（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。

B2201-06　（ID とパスワードによる認証の場合）

第六条　利用者は、アカウント管理に際して次の各号を遵守しなければならない。

一　利用者は、自己のアカウントを他の者に使用させ、または他の者に開示してはならない。

二　利用者は、他の者のアカウントを聞き出し、または使用してはならない。

三　利用者は、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。また、全学アカウントの漏えいが発生しないよう管理しなければならない。

四　利用者は、全学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。

五　利用者は、システムを利用する必要がなくなった場合は、遅滞なく全学実施責任者に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、あらかじめ全学実施責任者が定めている場合は、この限りでない。

六　利用者は、アカウントを「B3205 アカウント管理ガイドライン」に従って適切に管理しなければならない。

B2201-06-2　（IC カードを用いた認証の場合）

第六条の２　利用者は、IC カードの管理を以下のように徹底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 カードを他者に付与及び貸与しないこと。

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。

四　IC カードを利用する必要がなくなった場合には、遅滞なく、これを全学実施責任者に返還しなければならない。

（五　IC カード使用時に利用する PIN 番号を他に教えたりしてはならない。）

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。

B2201-07　（情報機器の利用）

第七条　利用者は、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したがわなければならない。

一　利用者は、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　情報機器は認証システムおよびログ機能を備えている場合には、それらの機能が設定され動作していなければならない。不正ソフトウェア対策機能が提供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可能でなければならない。

四　情報機器は脆弱性を持たないよう可能な限り最新の状態でなければならない。
五　利用者は、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「B3201 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、「B2501 事務情報セキュリティ対策管理基準」1.6 の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。**

B2201-08　（利用者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（利用者）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（利用者）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。全利用者に受講義務があるが、学生は講義等で一括受講すると考えられるので、第七条２項および３項は教職員等（利用者）として区別している。

B2201-09　（自己点検の実施）

第九条　利用者は、本学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。

解説：政府機関統一基準によれば、大学で整備された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。自己点検の範囲・対象や報告義務については、自己点検基準に記載されているので、規程としては自己点検実施義務を記載しておけば十分である。

B2201-10　（情報の取り扱い）

第十条　利用者は、格付けされた情報について、情報格付け取扱手順（B3104）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：B1001-19 にしたがって B2104 および B3104 が策定され、教職員等は B2104 および B3104 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 B3104 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。

B2201-11 （制限事項）

第一一条　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。

B2201-12 （禁止事項）

第十二条　利用者は、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「B1001 情報システム運用基本規程」第三条九号「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。

B2201-13　（違反行為への対処）

第一三条　利用者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（第十二条～十四条）の条文は、利用者が守るべき手順書を示している。

B2201-14　（電子メールの利用）

第十四条　利用者は、電子メールの利用にあたっては、別途定める「B3252 電子メール利用ガイドライン」および「B3201 学外情報セキュリティ水準低下防止手順」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。

B2201-15　（ウェブの利用および公開）

第一五条　利用者は、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　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、「B3203 ウェブブラウザ利用ガイドライン」および「B3211 学外情報セキュリティ水準低下防止手順」に従わなければならない。

二　利用者は、部局情報システム運営委員会に許可を得て、「B3204 ウェブ公開ガイドライン」および「B3201 学外情報セキュリティ水準低下防止手順」に従いウェブページを作成し、公開することができる。

解説：総合情報処理センターの public_html の下までは含めないような規程にすると使い勝手がよい。クラウドやアウトソースへの配慮が B3204 に必要になる。

三　利用者は、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。サーバは「B3152 ウェブサーバ設定確認実施書（策定手引書）」に従って設定しなければならない。業者によるウェブサービス等を利用する場合には、B3152 に合致するサービスを選定すること。

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。

B2201-16　（学外からの本学情報システムの利用）

第一六条 利用者は、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　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。B2201-07 に集約することが可能と思われる。

B2201-18　（安全管理義務）

第一八条　利用者は、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。

B2201-19 (インシデント対応)

第一九条　利用者は、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、「B3103 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。

解説：すべての大学にある情報システムおよびネットワークに接続する機器の利用にあたってセキュリティ確保上実施しなければならない項目を規定している。詳細まで明文化する方法もあるが、詳細を「B3201 情報機器取扱ガイドライン」に記載することとしてもよいであろう。

B2202 認証基盤利用規程

解説：本規程は、A 大学の学内ネットワークの管理運営部局である情報メディアセンターが提供する認証基盤を、情報メディアセンターが提供しないサービスにおいて利用する場合に必要となる管理手続きについて定めるものである。認証以外の利用に関わる規定事項については、B2201（情報システム利用規程）を参照されたい。

B2202-01　（目的）

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２項第二号に基づき、Ａ大学（以下「本学」という。）における全学認証基盤の適切な運用及び管理について必要な事項を定めることを目的とする。

B2202-02　（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「B1000 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「B1001 情報システム運用基本規程」をいう。

三　運用・管理規程　本学が定める「B2201 情報システム運用・管理規程」をいう。

四　利用規程　本学が定める「B2201 情報システム利用規程」をいう。

五　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。

六　特定部局情報システム　部局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。

七　利用者端末　学内・学外に関らず利用者等が全学情報システム及び特定部局情報システムを特定利用（第十七号に定めるもの）するために用いる情報機器（全学情報システム又は特定部局情報システムを除く）をいう。

八　教職員等　役員及び本学が定める就業規則に基づき雇用されている教職員をいう。

九　学生等　学部学生及び大学院学生、外国学生、委託生、科目等履修生、聴講生、研究生、研修員等その他本学規程に基づき受け入れる研究者等をいう。

十　利用者　教職員等及び学生等で、全学情報システム又は特定部局情報システムを利用する者をいう。

十一　全学情報システム臨時利用者　教職員等及び学生等以外の者で、情報メディアセンター長の許可を受けて、全学情報システムを利用（運用・管理等の業務において取り扱うことを含む。以下同じ）する者をいう。

十二　特定部局情報システム臨時利用者　教職員等及び学生等以外の者で、特定部局情報システムについて、当該部局の長又は部局情報セキュリティ技術責任者の許可を受けて利用する者をいう。

十三　利用者等　利用者及び全学情報システム臨時利用者並びに特定部局情報システム臨時利用者をいう。

十四　主体認証　次号に定める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。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する際には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。識別コード符号と共に正しい方法で主体認証情報が提示された際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。

十五　識別コード　主体認証を行うために、利用者等又は電子計算機が提示する情報のうち、情報システムが利用者等又は電子計算機を正当な権限を有するものとして認識する情報をいう。代表的な識別コードとして、ID 等がある。

十六　主体認証情報　主体認証を行うために、利用者等又は電子計算機が提示する情報のうち、情報システムが利用者等又は電子計算機を正当な権限を有するものとして認識する情報をいう。代表的な主体認証情報として、パスワードがある。

十七　特定利用　本学情報ネットワークへの接続者又は利用者等による全学情報システムの利用（運用・管理等の業務において取り扱うことを含む。以下同じ）、並びに利用者等による全学アカウントによる主体認証を伴っての全学情報システム又は特定部局情報システムの利用をいう。

B2202-03　（適用範囲）

第三条 本規則は教職員等のほか、すべての利用者等に適用する。

２　本規則は、以下の情報システムを対象とする。

一　全学情報システム

二　特定部局情報システム

三　利用者端末（特定利用に用いられているときに限る）

B2202-04　（全学アカウントの申請と交付）

第四条 全学情報システム又は特定部局情報システムを、全学アカウントによる主体認証を伴って利用する利用者等は、情報メディアセンター長が別途定める手続きにより、申請を行い情報メディアセンターから全学アカウントを取得しなければならない。

B2202-05　（全学情報システム臨時利用者及び特定部局情報システム臨時利用者への許可）

第五条 情報メディアセンター長は、教職員等及び学生等以外の者について、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、全学情報システム臨時利用者として、全学情報システムの利用の許可を与えるものとする。

一　部局情報セキュリティ責任者より臨時利用の目的・範囲・期間等を明示して申請があったとき

二　その他情報メディアセンター長が特に必要があると認めたとき

２　部局情報セキュリティ責任者又は部局情報セキュリティ技術責任者は、教職員等及び学生等以外の者について、必要があると認めるときは、部局の定める手続きに従って、特定部局情報システムの利用の許可を与えるものとする。

３　部局情報セキュリティ責任者は、第１項第一号に基づき情報メディアセンター長に全学情報システム臨時利用者の利用を申請し許可された際、許可された全学情報システム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、許可された全学情

報システム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全学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　情報メディアセンター長は、第１項第二号に基づき全学情報システムの利用を許可した際、許可した全学情報システム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、許可した全学情報システム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全学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。

5　部局情報セキュリティ責任者又は部局情報セキュリティ技術責任者は、第２項に基づき、特定部局情報システムの利用を許可した際、許可した特定部局情報システム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、許可した特定部局情報システム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全学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。

B2202-06　（全学アカウント利用の遵守すべき事項）

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を遵守しなければならない。

（1）　自分の全学アカウントを他の者に使用させたり、他の者の全学アカウントを使用したりしてはならない。

（2）　他の者の主体認証情報(パスワード)を聞き出したり使用したりしてはならない。

（3）　主体認証情報（パスワード）は、B3205 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。

(4) 利用者等は、主体認証を伴って全学情報システム又は特定部局情報システムへアクセス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。

（5）　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情報システム並びに特定部局情報システムへの全学アカウントによる主体認証を伴ってのアクセスを行ってはならない。

（6）　全学アカウントを他の者に使用され又はその危険が発生した際には、直ちに情報メディアセンター長にその旨を報告しなければならない。

（7）　姓名の変更等全学アカウントの変更が必要になった際は、遅滞なく情報メディアセンターに届け出なければならない。

（8）　全学情報システムの利用資格を喪失した際又は利用する必要がなくなった際は、遅滞なく情報メディアセンターに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、あらかじめ情報メディアセンターが定めている場合は、この限りでない。

B2202-07　（全学アカウントの一時停止と復帰）

第七条 情報メディアセンター長は、第７条及び第８条第１号、第２号、第３号に該当する全学アカウントを発見したとき、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、全学アカウントにより主体認証を行っている全学情報システム並びに本学認証基盤と接続されている部局情報システムの全部又は一部へのアクセス制限を行い、その旨を該当する全学アカウント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 全学アカウントの一時停止あるいはアクセス制限を受けた利用者等が、全学アカウントの復帰を希望するときは、その旨を情報メディアセンター長に申し出るものとする。

４ 情報メディアセンター長は、前項の申し出を受けたときは、当該の全学アカウントの確認を行った後、速やかに全学アカウントの復帰を行うものとする。

B2202-08 （本学認証基盤への特定部局情報システム接続及び利用の許可と停止）

第九条 部局情報セキュリティ技術責任者は、本学認証基盤に対して、特定部局情報システムを接続する際、利用目的及び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、情報メディアセンター長に申請し許可を得なければならない。なお、情報メディアセンター長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 部局情報セキュリティ技術責任者は、前項の接続を行った際には、部局情報セキュリティ責任者に報告しなければならない。

３ 情報メディアセンター長は、前項の申請で許可した接続又はあらかじめ指定する範囲の接続において、個人情報が提供される場合には、当該特定部局情報システムと個人情報の利用目的について、対象となる利用者等に通知又は公表しなければならない。

４ 部局情報セキュリティ技術責任者は、本学認証基盤の接続について、その必要がなくなった際、遅滞なく情報メディアセンター長にその旨を届けなければならない。

５ 部局情報セキュリティ技術責任者は、本学認証基盤の接続によって特定部局情報システムに提供された情報の利用の範囲が、接続の申請時に示した利用目的及び情報の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。

B2301 年度講習計画

解説：「B2101 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:「B1001 情報システム運用基本規程」B1001-5（第五条）、B1001-08（第八条）、「B2201 情報システム利用規程」B2201-07（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 ・メール転送、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（「B3302 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。「B3303 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。

B2401 情報セキュリティ監査規程

B2401-01 （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。

B2401-02 （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。

B2401-03 （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。

B2401-04 （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

B2401-05 （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。

B2401-06 （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。

B2401-07　（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。

B2501 事務情報セキュリティ対策管理基準

目　次

第 1.1 部　総則

1.1.1.1 本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準の位置付け

「事務情報セキュリティ対策管理基準」及び「事務情報セキュリティ対策技術基準」（以下、この２つの文書を総称して「本基準」という。）は、国立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、平成 24 年 4 月 26 日に決定された「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」（以下、この２つの文書を総称して「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。解説部分も含めて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。

1.1.1.2 本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準の使い方

(1) 全体構成

本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準は、部、節及び項の 3 つの階層によって構成される。

本事務情報セキュリティ管理基準は、組織全体で情報セキュリティ対策を推進する組織・体制の整備、情報のライフサイクルの各段階における情報セキュリティ対策、情報システムに関連のある規程類の整備等について遵守すべき事項を定めており、事務情報セキュリティ技術基準は技術的な内容であり改訂頻度が高いものとして情報システムに求められるセキュリティ要件等について遵守すべき事項を定めている。

本事務情報セキュリティ管理基準では、「総則」、「組織と体制の整備」、「情報についての対策」、「情報処理についての対策」、「情報システムについての基本的な対策」を、事務情報セキュリティ技術基準では、「情報セキュリティ要件の明確化に基づく対策」、「情報システムの構成要素についての対策」、「個別事項についての対策」をそれぞれ部として分類している。

さらにそれぞれの部において、内容に応じて節として対策項目に分け、その下に項として対策基準を定めている。具体的には以下のとおり。

(a) 第 1.1 部 総則

(b) 第 1.2 部 組織と体制の整備

「組織と体制の整備」では、組織全体として情報セキュリティ対策を実施するに当たり、実施体制や評価手順、違反や例外措置等、組織としての運用に関係する各事務従事者の権限と責務を明確にするために整備すべき事項を本事務情報セキュリティ管理基準において定めている。

(c) 第 1.3 部 情報についての対策

「情報についての対策」では、情報の作成、利用、保存、移送、提供、消去等といった

情報のライフサイクルに着目し、各段階において各事務従事者が情報を保護するために業務の中で常に実施すべき事項を本事務情報セキュリティ管理基準において定めている。

(d) 第 1.4 部 情報処理についての対策

「情報処理についての対策」では、情報システムの利用において実施すべき事項と、要管理対策区域外での情報処理及び本学支給以外の情報システムによる情報処理において制限すべき事項を本事務情報セキュリティ管理基準において定めている。

(e) 第 1.5 部 情報システムについての基本的な対策

「情報システムについての基本的な対策」では、事務情報セキュリティ技術基準で定められる遵守事項が適切に実施されるように、情報システムの計画、構築、運用、移行、廃棄及び見直しといった情報システムのライフサイクルの各段階において実施すべき事項と、情報システムに係る情報セキュリティを確保するために規定として整備すべき事項を本事務情報セキュリティ管理基準において定めている。

(f) 第 2.1 部 総則

(g) 第 2.2 部 情報セキュリティ要件の明確化に基づく対策

「情報セキュリティ要件の明確化に基づく対策」では、情報システムにおいて、アクセス制御の観点等、導入すべきセキュリティ機能を示すとともに、セキュリティホール、不正プログラム及びサービス不能攻撃等の脅威を防ぐために、情報システムにおいて実施すべき事項を事務情報セキュリティ技術基準において定めている。

(h) 第 2.3 部 情報システムの構成要素についての対策

「情報システムの構成要素についての対策」では、電子計算機及び通信回線等の個別の情報システムの特性及びライフサイクルの観点から、情報システムにおいて実施すべき事項を事務情報セキュリティ技術基準において定めている。

(i) 第 2.4 部 個別事項についての対策

「個別事項についての対策」では、新たな技術の導入等に際し特に情報セキュリティ上の配慮が求められる個別事象に着目し、遵守すべき事項を事務情報セキュリティ技術基準において定めている。

(2) 対策項目の記載事項

本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準では、本学が行うべき対策について、対策項目ごとに遵守事項を示す。

(3) 「対策レベルの設定」に係る変更点

「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（2011 年版）」（平成 23 年 3 月 31 日公開）までは、各対策項目で対策の強度に段階を設けていた。この段階を「対策レベル」と呼び、採るべき遵守事項を「基本遵守事項」又は「強化遵守事項」としていた。

そして、「基本遵守事項」を「保護すべき情報とこれを取り扱う情報システムにおいて、必須として実施すべき対策事項」、「強化遵守事項」を「特に重要な情報とこれを取り扱う情報システムにおいて、本学が、その事項の必要性の有無を検討し、必要と認められるときに選択して実施すべき対策事項」と定義し、「強化遵守事項」については、本学において本基準の策定時に、本学の情報システム及び業務の特性を踏まえ、本基準への採用を選択することとしていた。

今後は、従来の「基本遵守事項」及び「強化遵守事項」の区分を廃止して「遵守事項」と

する。「遵守事項」は、本基準において、保護すべき情報とこれを扱うシステムにおいて、必須として実施すべき対策事項とする。なお、必要性の有無を検討し、必要があると判断した際に実施する対策事項については、実施の必要性の有無の検討を必須とし、対策の実施については本学の判断とする。

1.1.1.3 情報の格付の区分及び取扱制限の種類

(1) 格付及び取扱制限

高等教育機関の事務で取り扱う情報については、その目的や用途により、取扱いに慎重を要する度合いは様々であり、その重要性に応じた適切な措置を講じ、確実に情報セキュリティを確保するために、情報の格付の区分及び取扱制限の種類を定めるものとする。

情報の格付及び取扱制限は、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とから、適切に実施される必要がある。

また、情報の格付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及び取扱制限の判断を行い、情報を取り扱うたびに格付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ため、事務従事者にその内容を理解し遵守するように周知すること。

解説：情報の格付及び取扱制限の実施方法については、「行政機関の保有する情報の公開に関する法律」（以下「情報公開法」という。）に基づき本学において定めている「処分に係る審査基準」や文書管理規程等を参考に決めるとよい。なお、情報の格付及び取扱制限については、本学における情報セキュリティ対策基準の施行日以後に作成又は入手した全ての情報について適用するものであり、施行日前に作成又は入手した情報について一括して処理することを求めているものではない。しかし、施行日前に作成又は入手した情報についても、適宜その決定を行うことが望ましいことから、当該情報を施行日以後取り扱う際に、格付及び取扱制限を行う必要がある。

(2) 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、それぞれにつき格付の区分の定義を示す。

格付としては、以下に記載のものを本事務情報セキュリティ管理基準の遵守事項で用いるが、本学において、適宜変更又は追加して構わない。しかし、変更又は追加する場合には、本学の対策基準における格付区分と遵守事項との関係が本事務情報セキュリティ管理基準及び事務情報セキュリティ技術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、変更又は追加した場合には、他の高等教育機関等との情報のやり取りをする際に、自身の格付区分が本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準で用いた格付区分とどのように対応するかを伝達する方法について定めなければならない。例えば、他の高等教育機関に情報を提供する際に、本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準で用いた格付区分を記載する方法が考えられる。

(a) 情報の格付の区分は、機密性、完全性及び可用性について、それぞれ以下のとおりとする。

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、秘密文書に相当する機密性を要する情報
機密性２情報	本学で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報
機密性１情報	機密性２情報又は機密性３情報以外の情報

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。

解説：機密性の格付については、文書管理規程上の秘密文書に相当する機密性を要する情報であり、事務従事者のうち、特定の者だけがアクセスできる状態を厳密に確保されるべき情報は機密性３情報に、秘密文書には相当しないが、情報公開法に基づく処分に係る審査基準で不開示情報に該当すると考えられる情報等、事務従事者以外がアクセスできない状態を最低限確保されるべき情報は機密性２情報に、それ以外の情報は、機密性１情報に決定することを基本とする。例えば、従来「取扱注意」等と表示されてきたような資料は、機密性２情報に決定することが考えられるが、その内容によっては、機密性１情報に決定した上で取扱制限を決定することで十分な場合も考えられる。

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。

解説：完全性の格付については、情報が改ざん、誤びゅう又は破損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情報に決定することを基本とする。例えば、原本に相当する情報を完全性２情報に、複製に相当する情報（例えば、電子メールに添付されるファイル等）を完全性１情報に決定すること等が考えられる。

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、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。

解説：可用性の格付については、情報が滅失又は紛失されていない状態並びに情報及び関連資産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情報に決定することを基本とする。なお、可用性２情報に決定した場合には、取扱制限を併用して、どの程度の可用性が必要かを決定することが望ましい。

(3) 取扱制限の種類

情報について、機密性、完全性及び可用性の３つの観点から区別し、それぞれにつき取扱制限の種類について基本的な定義を定める。「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。

(a) 情報の取扱制限の種類は、機密性、完全性及び可用性について、それぞれ定めるものとする。なお、取扱制限の種類については適宜定めることができる。

1.1.1.4 情報取扱区域における管理及び利用制限

(1) 情報取扱区域

情報セキュリティを確保するためには、適切な対策が講じられている区域で高等教育機関の事務を行うことが必要不可欠である。そのため、執務室や会議室、サーバ室等の管理に当たっては、それらの区域でどのような高等教育機関の事務が行われるのかを想定し、それに応じて必要となる管理対策を決定し、適切な措置を講ずる必要がある。

また、それらの区域の利用に当たっては、用途や施されている管理対策に応じて、必要な制限を利用者に求めることも情報セキュリティを確保する上で必要となる。さらに、このような対策を有効なものとするためには、高等教育機関の事務を行う者が、それらの区域に求められる管理対策及び利用の制限について正しく認識でき、取り扱う情報の重要性に応じて適切な区域を選択できるようにする必要がある。

これらのことから、本学の内外において情報を取り扱う区域を「情報取扱区域」とし、それらの区域のうち、求める対策の観点から「クラス」の区分を定めるものとする。

(2) 情報取扱区域のクラスの決定

情報取扱区域について、求める対策の基準ごとに「クラス」の区分を定める。

(a) 情報取扱区域におけるクラス及びクラスにおける区分の基準を、それぞれ以下のとおりとする。

クラス	区分の基準
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
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
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
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

なお、クラス １以上の区域を「要管理対策区域」という。

(3) 情報取扱区域のクラス別管理及び利用制限

本学は、定めた情報取扱区域について、クラス ０からクラス ３の区域においてクラス別に講ずる管理対策（以下「クラス別管理」という。）及び対策が講じられた区域におけるクラス別の利用制限対策（以下「クラス別利用制限」という。）を決定し、それらに基づいて適切に対策を講ずるものとする。

なお、事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準において定めるクラス別管理及び利用制限は、最低限の管理対策及び利用制限対策であるため、本学において、名称の変更、クラスの追加並びに実施する管理対策及び利用制限対策の変更又は追加を適宜実施して構わない。ただし、変更又は追加する場合には、本学の対策基準で求める情報取扱区域における情報セキュリティ水準が、本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準において求める情報セキュリティ水準と同等以上となるように準拠しなければならない。

(4) 情報取扱区域の個別管理及び個別利用制限

情報取扱区域について、決定したクラスの区分において必要な対策が不足していると認められる区域、又はクラスとは別の区分で対策を講ずる必要のある区域があるときは、求める情報セキュリティ水準を確保又は向上させるため、定められたクラス別管理及び利用制限にかかわらず、当該区域ごとに個別の管理対策（以下「個別管理」という。）及び個別の利用制限対策（以下「個別利用制限」という。）を決定することができる。

1.1.1.5 用語定義

【あ】

- 「アクセス制御」とは、主体によるアクセスを許可する客体を制限することをいう。
- 「移送」→「情報の移送」を参照。
- 「委託先」とは、情報システムに関する計画、構築、運用等の情報処理業務の一部又は全部を請け負った者をいう。

【か】

- 「外部委託」とは、情報システムに関する計画、構築、運用等の情報処理業務の一部又は全部を学外の者に請け負わせることをいう。

- 「学外」とは、事務従事者の各々が所属する高等教育機関が管理する組織又は庁舎の外をいう。
- 「学外通信回線」とは、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、事務従事者の各々が所属する高等教育機関が管理していない電子計算機が接続され、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。
- 「学内」とは、事務従事者の各々が所属する高等教育機関が管理する組織又は庁舎の内をいう。
- 「学内通信回線」とは、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、事務従事者の各々が所属する高等教育機関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。
- 「可用性」とは、情報及び関連資産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、情報及び関連資産にアクセスできる状態を確保することをいう。
- 「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。
- 「機器等」とは、情報機器等及びソフトウェアをいう。
- 「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状態を確保することをいう。
- 「共用識別コード」とは、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、利用状況等を考慮して、１つの識別コードを複数の主体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。
- 「記録媒体」とは、情報が記録され、又は記載されるものをいう。なお、記録媒体には、書面、書類その他文字、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、電子計算機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、電子計算機や通信回線装置に内蔵される内蔵電磁的記録媒体と外付けハードディスク、CD-R、DVD、MO、USB メモリ、フラッシュメモリ等の外部電磁的記録媒体がある。
- 「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」とは、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。
- 「最少特権機能」とは、管理者権限を実行できる範囲を管理作業に必要な最少の範囲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。

- 「事務従事者」とは、本学教職員（本学において高等教育機関の事務に従事している者）及び本学の指揮命令に服している者（個々の勤務条件にもよるが、例えば、派遣労働者等）のうち、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。
- 「重要な設計書」とは、情報システムに関する設計書のうち、当該情報システムの適切な管理に必要なものであり、その紛失、漏えい等により、高等教育機関の事務の遂行に支障を及ぼすものをいう。情報の格付では、要機密情報に相当する。
- 「主体」とは、情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。
- 「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。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、本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準における「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。
- 「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。
- 「本基準」とは、事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準に準拠した、本学における全ての情報資産に適用する情報セキュリティ対策の基準をいう。
- 「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。したがって、作業途上の文書も適用対象であり、書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面又は情報システムから出力した情報を記載した書面をいう。）及び情報システムに関する設計書が含まれる。
- 「情報システム」とは、情報処理及び通信に係るシステムをいう。
- 「情報セキュリティ関係規程」とは、本基準及び本基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた実施手順をいう。
- 「情報の移送」とは、要管理対策区域外に、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」とは、廃棄した情報が漏えいすることを防止するために、全ての情報を復元が困難な状態にすることをいう。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態ではない。

- 「ソフトウェア」とは、電子計算機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、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。

【た】

- 「端末」とは、事務従事者が直接操作を行う電子計算機（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。）であり、いわゆる PC のほか、PDA 等も該当する。
- 「通信回線」とは、これを利用して複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みであり、物理的なものと論理的なものがある。
- 「通信回線装置」とは、回線の接続のために設置され、電子計算機により回線上を送受信される情報の制御を行うための装置をいう。いわゆるリピータハブ、スイッチングハブ及びルータのほか、ファイアウォール等も該当する。
- 「電子計算機」とは、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。
- 「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、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。

【は】

- 「不正プログラム」とは、コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。
- 「不正プログラム定義ファイル」とは、アンチウイルスソフトウェア等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。
- 「本学支給以外の情報システム」とは、本学が支給する情報システム以外の情報システムをいう。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情報システムも含むものとする。
- 「本学支給以外の情報システムによる情報処理」とは、本学が支給する情報システム以外の情報システムを用いて高等教育機関の事務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことであり、例えば、本学の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。

【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措置することをいう。なお、情報ごとに格付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、当該情報の格付に係る認識が共通となる措置については、明示等に含むものとする。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を規定等に明記し、当該情報システムを利用する全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とする。

【や】

- 「要安定情報」とは、可用性２情報をいう。

- 「要機密情報」とは、機密性２情報及び機密性３情報をいう。
- 「要管理対策区域」とは、施設及び環境に係る管理対策が講じられている区域であって、情報取扱区域におけるクラス １以上の区域をいう。
- 「要管理対策区域外」とは、情報取扱区域におけるクラス 0 の区域をいう。
- 「要管理対策区域外での情報処理」とは、事務従事者が情報取扱区域におけるクラス 0 の区域において高等教育機関の事務の遂行のための情報処理を行うことをいう。なお、オンラインで学外から本学の情報システムに接続して、情報処理を行う場合だけではなく、オフラインで行う場合も含むものとする。
- 「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。
- 「要保全情報」とは、完全性２情報をいう。

【ら】

- 「例外措置」とは、事務従事者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、高等教育機関の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。
- 「ログイン」とは、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。
- 「ログオン」とは、ログインの結果により、主体認証を要求した主体が正当であることが情報システムに確認された状態をいう。

第 1.2 部　組織と体制の整備

1.2.1 導入

1.2.1.1 組織・体制の整備

趣旨（必要性）

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。

これらのことを勘案し、本項では、情報セキュリティ対策に係る組織・体制に関する対策基準を定める。具体的には、

・全学総括責任者の設置とその役割
・全学情報システム運用委員会の設置とその役割
・情報セキュリティ監査責任者の設置とその役割
・部局総括責任者の設置とその役割
・部局技術責任者の設置とその役割
・部局技術担当者の設置とその役割
・職場情報セキュリティ責任者の設置とその役割
・区域情報セキュリティ責任者の設置とその役割
・情報セキュリティアドバイザーの設置とその役割

についての遵守事項を定めるものである。

遵守事項

(1)　全学総括責任者の設置

(a)　全学総括責任者を 1 人置くこと。

解説：本学における情報セキュリティ対策の最高責任者を置くことを定めた事項である。情報セキュリティ対策の実現には、事務従事者一人一人の意識の向上や責務の遂行はもちろんのこと、組織的な取組の推進や幹部の責任を持った関与が必須であり、本学における最高責任者の設置とその役割の明確化が重要である。なお、本事務情報セキュリティ管理基準で規定する各役割についてはイメージ図（本書別添資料 A.1.1）を参考にされたい。

(b) 全学総括責任者は、本学における情報セキュリティ対策に関する事務を統括すること。

解説：全学総括責任者は、本学内における情報セキュリティ対策の推進体制が十分機能するように管理するとともに、本基準の決定や評価結果による見直しに関する承認等を行う。

(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、全学情報システム運用委員会を設置し、委員長及び委員を置くこ

と。

解説：本学における本基準の策定等を行う機能を持つ組織の設置について定めた事項である。情報セキュリティ対策の運用を円滑に進めるには、委員会を設置し組織全体で取り組むことが重要である。全学総括責任者は、委員長を兼務することが可能である。なお、実務を担当する下位委員会を設置し、又は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等して、部門横断的な連携の仕組みを確立することが望まれる。

(b) 全学情報システム運用委員会は、事務情報セキュリティ管理基準に準拠して、情報セキュリティに関する対策基準を策定し、全学総括責任者の承認を得ること。

解説：全部門的に定めるべき本基準策定に関する全学情報システム運用委員会の役割を定めた事項である。

(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、情報セキュリティ監査責任者を１人置くこと。

解説：本学において策定した本基準に基づき監査を行う責任者を置くこと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、部局総括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。情報セキュリティ監査責任者は、本学内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、本学の内部及び外部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。なお、本学において、監査責任者を補佐する立場として監査副責任者等を独自に設置することを妨げるものではない。

(b) 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こと。

(4) 部局総括責任者の設置

(a) 全学総括責任者は、情報セキュリティ対策の運用に係る管理を行う単位を定め、その単位ごとに部局総括責任者を置くこと。そのうち、部局総括責任者を統括する者として全学実施責任者を１人置くこと。

解説：組織内での役割の明確化のため、情報セキュリティ対策の運用について管理を行う単位を決めることを定めた事項である。「管理を行う単位」は、部、局（外局、地方支分局等含む。）ごとや情報システムごと等が挙げられる。部局総括責任者は、本学の実施手順を策定するとともに、組織内での情報セキュリティ対策の運用実態を十分踏まえ、実務レベルでの管理の仕組みを確立し、全ての事務従事者への責務の周知や教育を行う等、個別対策を機能させる環境を整備することが重要である。

(b) 全学実施責任者は、全学総括責任者の指示に基づき、事務情報セキュリティ技術基準に準拠して、情報セキュリティに関する対策基準における技術的側面の基準を策定すること。なお、当該基準の策定については、全学総括責任者が指定した者に委任することができる。

解説：全部門的に定めるべき本基準における技術的側面の基準策定に関する全学実施責任者の役割を定めた事項である。また、当該基準の策定については、全学総括責任者が指定した者に委任することができる。なお、部局総括責任者等が委任に基づき技術基準を策定する場合は、全学総括責任者及び全学実施責任者に報告することが望ましい。

(c) 部局総括責任者は、所管する単位における情報セキュリティ対策に関する事務を統括すること。

(d) 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、終了及び人事異動等に関する管理の規定を整備すること。

解説：「雇用の開始、終了及び人事異動等に関する管理の規定」とは、現実の人事配置状況と情報システム上のアクセス権の付与状況等の不整合や、採用及び異動時等における適切な教育の不十分さを原因とする情報セキュリティの侵害を回避することを目的とする規定のことである。具体的には、

・人事担当課又は各課室から、情報システム所管課に人事異動に関する情報が提供される連絡体制

・人事異動の情報に基づき、アクセス権の変更、事務従事者の教育等の情報セキュリティ関係業務を適切に実施するための手順

等を整備することが求められる。

これには、転出に伴うアカウントの失効、情報システムへのアクセス権の変更の管理等も含まれる。

(e) 部局総括責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動等に関する管理の規定に従った運用がなされていることを定期的に確認すること。

(f) 全学総括責任者は、部局総括責任者を置いた時及び変更した時は、全学実施責任者にその旨を連絡すること。

(g) 全学実施責任者は、全ての部局総括責任者に対する連絡網を整備すること。

(5) 部局技術責任者の設置

(a) 部局総括責任者は、所管する単位における情報システムごとに部局技術責任者を、当該情報システムの計画段階までに置くこと。

解説：各情報システムにおいて、計画、構築、運用等のライフサイクル全般を通じて必要となるセキュリティ対策の責任者を置くことを定めた事項である。情報システムのセキュリティ要件は計画段階において決定されることから、部局技術責任者は新規の情報システムについては計画段階までに置かなければならない。学内 LAN システムのような全部門的なシステム、特定部門における個別業務システム、その他本学の全ての情報システムを、情報システム単位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。なお、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こと。

(b) 部局技術責任者は、所管する情報システムに対するセキュリティ対策に関する事務を統括すること。

(c) 部局総括責任者は、部局技術責任者を置いた時及び変更した時は、全学実施責任者に

その旨を報告すること。

(d) 全学実施責任者は、全ての部局技術責任者に対する連絡網を整備すること。

(6) 部局技術担当者の設置

(a) 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：各情報システムにおいて、その管理業務ごとのセキュリティ対策の実施を管理する者を置くことを定めた事項である。計画、構築、運用等の情報システムのライフサイクルやサーバ、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設置する必要がある。部局技術担当者は、部局総括責任者によって定められた手順や判断された事項に従い、対策を実施する。

(b 部局技術担当者は、所管する管理業務における情報セキュリティ対策を実施すること。

(c) 部局技術責任者は、部局技術担当者を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。

(d) 全学実施責任者は、全ての部局技術担当者に対する連絡網を整備すること。

(7) 職場情報セキュリティ責任者の設置

(a) 部局総括責任者は、各職場に職場情報セキュリティ責任者を 1 人置くこと。

解説：職場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、所管する事務や事務従事者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、課室長若しくはそれに相当する者であることが望ましい。部局総括責任者が各職場で 1 人任命し、全学実施責任者に報告するものである。

本文中「職場」と記載されている箇所を、「課室」と書き換えて基準を定めても構わない。

(b) 職場情報セキュリティ責任者は、職場における情報セキュリティ対策に関する事務を統括すること。

(c) 部局総括責任者は、職場情報セキュリティ責任者を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。

(d) 全学実施責任者は、全ての職場情報セキュリティ責任者に対する連絡網を整備すること。

(8) 区域情報セキュリティ責任者の設置

(a) 全学実施責任者は、要管理対策区域について、情報セキュリティ対策の運用に係る管理を行う区域の単位を定め、その単位ごとに区域情報セキュリティ責任者を置くこと。

解説：要管理対策区域について、情報セキュリティ対策の運用に係る管理を行う単位を決め、区域ごとの情報セキュリティ対策を実施する者を置くことを定めた事項である。

要管理対策区域には、執務室やサーバ室だけでなく、ロビーや庁舎内の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。

「管理を行う区域の単位」は、当該区域の利用用途や設置環境等を勘案して、例えば、

・部局又は課室単位で管理している執務室又は会議室ごと
・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、上記以外の要管理対策区域（ロビー、廊下等）を一つの区域とする場合も考えられる。
なお、区域情報セキュリティ責任者は、当該区域の利用用途や設置環境等を勘案して、部局総括責任者、職場情報セキュリティ責任者、部局技術責任者又は本学施設等の管理に関する部門の責任者等の中から定めることが考えられる。定める単位としては、例えば、
・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
・複数の課室が利用する執務室及び会議室を管理する場合は、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
・執務室又はサーバ室以外の要管理対策区域（ロビー、廊下等）を管理する場合は、本学施設等の管理に関する部門の責任者
等を区域情報セキュリティ責任者として定めることが考えられる。

(b) 区域情報セキュリティ責任者は、所管する単位における区域ごとの情報セキュリティ対策に関する事務を統括すること。

(c) 全学実施責任者は、全ての区域情報セキュリティ責任者に対する連絡網を整備すること。

(9) 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こと。

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、本基準の策定・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。
情報セキュリティアドバイザーについては、内部人材を充てることもできる。またこの場合、情報セキュリティアドバイザーは部局総括責任者等の各責任者を兼務することができる。
なお、CIO（情報化統括責任者）補佐官は情報セキュリティアドバイザーを兼務することができる。この場合、CIO 補佐官に情報セキュリティ担当を設けることが望ましい。

(b) 全学総括責任者は、情報セキュリティ対策等の実施において情報セキュリティアドバイザーが行う業務の内容について定めること。

解説：情報セキュリティアドバイザーの業務を明確化するため、全学総括責任者に、情報セキュリティアドバイザーの業務の内容について定めることを求める事項である。

情報セキュリティアドバイザーの業務として、情報セキュリティ対策に係る様々な事務への助言等が想定されるが、その事務として例えば、
・情報セキュリティ施策の全般的な計画策定
・情報セキュリティ教育の計画立案、教材開発及び実施
・各種規定の整備
・情報システムに係る技術的事項
・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
・事務従事者に対する日常的な相談対応
・緊急時対応
・自己点検の計画立案と実施
・情報セキュリティの監査の計画立案と実施
等が想定される。
これらの事務を行う全学総括責任者、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、職場情報セキュリティ責任者等が定められた事項を遂行するために、情報セキュリティアドバイザーが専門的な知識及び経験に基づき行う助言等の内容を定める。

1.2.1.2 役割の割当て

趣旨（必要性）

情報セキュリティ対策に係る組織において、承認する者と承認される者が同一である場合や、監査する者と監査される者が同一である場合は、情報セキュリティが確保されていることが確認、証明されたことにはならない。情報セキュリティを確立するためには、兼務してはいけない役割が存在する。また、承認や許可事案においては、情報セキュリティ対策に係る組織体制に加えて、職務上の権限等から、当該組織体制上の承認等を行う者の上司が承認等をすべき場合がある。

これらのことを勘案し、本項では、情報セキュリティ対策に係る役割の割当てに関する対策基準として、兼務を禁止する役割、上司による承認・許可についての遵守事項を定める。

遵守事項

(1) 兼務を禁止する役割の規定

(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。）

(イ) 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) 上司による承認・許可

(a) 事務従事者は、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と。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。

(b) 事務従事者は、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、措置を講ずること。

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、要管理対策区域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等が求められる。

1.2.1.3 違反と例外措置

趣旨（必要性）

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は、万一違反があった場合に、定められた手続に従って、適切に対処する必要がある。

また、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等の理由により、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についても、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るものでなければ、当該規程の実効性を確保することが困難となる。

これらのことを勘案し、本項では、違反と例外措置に関する対策基準として、違反への対処方法及び例外措置の適用方法についての遵守事項を定める。

遵守事項

(1) 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には、各規定の実施に責任を持つ部局総括責任者にその旨を報告すること。

解説：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。本学においては、例規への違反を知った者に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。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来すもの又はその可能性のあるものをいう。

(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こと。

解説：情報セキュリティ関係規程への違反があった場合に、違反者及び当該規程の実施に責任を持つ者を含む必要な者に対して、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ことを求める事項である。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、問題の早期解決、拡大防止の必要がある。例えば、情報セキュリティ関係規程について再度周知する方法が考えられる。

(c) 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、全学総括責任者にその旨を報告すること。

解説：情報セキュリティ関係規程への違反があった場合に、違反の事実を、その内容、結果、業務への影響、社会的評価等を含めて、全学総括責任者に報告することを求める事項である。

(2) 例外措置

(a) 全学情報システム運用委員会は、例外措置の適用の申請を審査する者（以下本項において「許可権限者」という。）を定め、審査手続を整備すること。

解説：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ための事項である。緊急を要して申請される場合は、遂行に不要の遅滞を生じさせずに審査を速やかに実施する必要がある。そのため、申請の内容に応じ、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、部局技術担当者又は職場情報セキュリティ責任者の中から許可権限者を定めておくことが重要である。

(b) 事務従事者は、例外措置の適用を希望する場合には、定められた審査手続に従い、許可権限者に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する等の場合であって、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、事後速やかに申請し許可を得ること。事務従事者は、申請の際に以下の事項を含む項目を明確にすること。

(ア) 申請者の情報（氏名、所属、連絡先）
(イ) 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）
(ウ) 例外措置の適用を申請する期間
(エ) 例外措置の適用を申請する措置内容（講ずる代替手段等）
(オ) 例外措置の適用を終了した旨の報告方法
(カ) 例外措置の適用を申請する理由

解説：例外措置を事務従事者の独断で行わせないための事項である。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。ただし、高等教育機関の事務の遂行に緊急を要する等の場合であって、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を実施しないことが不可避のときは、事後速やかに申請して許可を得ること。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場合の被害の大きさと影響を検討、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、リスク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。

(c) 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。また、決定の際に、以下の項目を含む例外措置の適用審査記録を作成し、全学総括責任者に報告すること。

(ア) 決定を審査した者の情報（氏名、役割名、所属、連絡先）

(イ) 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

(ウ) 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：許可権限者に、例外措置の適用の申請を適切に審査させるための事項である。審査に当たっては、例外措置の適用を許可した場合のリスク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。例外措置の適用審査記録の報告を受け、全学総括責任者は適用審査記録の台帳を整備することとなるが、これは、将来、許可をさかのぼって取り消す場合に、該当する申請を全て把握し、一貫性をもって取り消すために必要となる。（ア）の「役割名」には、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、部局技術担当者又は職場情報セキュリティ責任者のいずれかを記載する。

(d) 事務従事者は、例外措置の適用について許可を受け、例外措置を適用した場合には、それを終了した時に、当該例外措置の許可権限者にその旨を報告すること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

解説：例外措置の適用の終了を確認するための事項である。例外措置の適用期間が終了した場合及び期間終了前に適用を終了する場合には、許可を受けた事務従事者が、許

可権限者に終了を報告しなければならない。

(e) 許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な措置を講ずること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

解説：例外措置の適用期間を、許可を受けた者に遵守させるための事項である。必要な措置としては、許可を受けた者が報告を怠っているのであればそれを督促すること、許可を受けた者が例外措置の適用を継続している場合にはその延長について申請させそれについて審査すること、が挙げられる。

(f) 全学総括責任者は、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査責任者からの求めに応ずること。

解説：全学総括責任者に、例外措置の適用審査記録の台帳を維持・整備することを求める事項である。例外措置の適用を許可したとしても、それが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採用すること又は遵守事項を実施していないことに変わりはない。もしも、例外措置を適用していることにより重大な情報セキュリティの侵害が発生した場合には、同様の例外措置を適用している者に対して、情報セキュリティの侵害発生の予防について注意を喚起したり、例外措置適用の許可について見直しをしたりする等の対処を検討する必要がある。そのためには、例外措置を適用している者や情報システムの現状について、最新の状態のものを集中して把握する必要がある。

1.2.2 運用

1.2.2.1 情報セキュリティ対策の教育

趣旨（必要性）

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、事務従事者にその内容が周知されず、事務従事者がこれを遵守しない場合には、情報セキュリティ対策の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、情報セキュリティ対策の教育を通じて、情報セキュリティ関係規程に関する理解を深め、情報セキュリティ対策を適切に実践できるようにすることが必要である。

これらのことを勘案し、本項では、情報セキュリティ対策の教育に関する対策基準として、全学実施責任者及び職場情報セキュリティ責任者による教育体制の整備に係る規程及び事務従事者による教育の受講についての遵守事項を定める。

遵守事項

(1) 情報セキュリティ対策の教育の実施

(a) 全学実施責任者は、情報セキュリティ関係規程について、事務従事者に対し、その啓発をすること。

解説：全学実施責任者に情報セキュリティ対策の啓発の実施を求める事項である。

(b) 全学実施責任者は、情報セキュリティ関係規程について、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。

解説：全学実施責任者に情報セキュリティ対策の教育のための資料を整備することを求める事項である。教育の内容については、本学の実情に合わせて幅広い角度から検討し、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る。そのためには、本学の情報セキュリティに係る網羅的な資料ではなく、受講する者が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。すなわち、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、受講する者が遵守する必要がない事項は極力含まないように配慮する必要がある。なお、遵守すべき事項以外であっても、教育内容に含めることが望ましい情報セキュリティ対策の例として、違反の監視機能に係る説明が挙げられる。これは、当該機能の存在を周知することで、その違反についての抑止効果を期待できる場合があるためである。

(c) 全学実施責任者は、事務従事者の役割に応じて毎年度最低１回、受講できるように、情報セキュリティ対策の教育に係る計画を企画及び立案するとともに、その実施体制を整備すること。

解説：情報セキュリティ対策の教育の最低限の受講回数等について定めた事項である。なお、情報セキュリティ事案の発生等、情報セキュリティ環境の変化に応じて、適宜、教育を行うことが重要である。計画の作成に際しては、関係する教育計画を参照し、効率性に注意するとともに人材育成にも留意すること。

(d) 全学実施責任者は、事務従事者の着任時又は異動時に、その役割に応じて新しい職場等で３か月以内に受講できるように、情報セキュリティ対策の教育を企画及び立案するとともに、その実施体制を整備すること。

解説：着任、異動した事務従事者に対して、早期に情報セキュリティ対策の教育を受講させることによって、当該事務従事者の情報セキュリティ対策の適正な実施を求める事項である。なお、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等、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。

(e) 全学実施責任者は、事務従事者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備すること。

解説：情報セキュリティ対策の教育の受講状況について把握できる仕組みを整備することを求める事項である。

(f) 全学実施責任者は、事務従事者の情報セキュリティ対策の教育の受講状況について、職場情報セキュリティ責任者に通知すること。

解説：計画された教育の実施に向けて、情報セキュリティ対策の教育を受講していない事務従事者を職場情報セキュリティ責任者に通知することを定めた事項である。

(g) 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こと。

解説：職場情報セキュリティ責任者が、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について定めた事項である。なお、例えば、受講時間を確保する等の事務従事者が受講できるための環境を整備することも必要である。

(h) 職場情報セキュリティ責任者は、事務従事者の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告すること。事務従事者が当該勧告に従わない場合には、全学実施責任者にその旨を報告すること。

解説：情報セキュリティ対策の教育を受講しない者への対策を定めた事項である。なお、計画された教育を受講しない事務従事者は、その遵守違反について責任を問われることになる。

(i) 全学実施責任者は、毎年度１回、全学総括責任者及び全学情報システム運用委員会に対して、事務従事者の情報セキュリティ対策の教育の受講状況について報告すること。

解説：全学総括責任者及び全学情報システム運用委員会に情報セキュリティ対策の教育の受講状況を報告することを求める事項である。

(j) 全学実施責任者は、情報セキュリティ関係規程について、事務従事者に対する情報セキュリティ対策の必要性を検討し、必要と判断した場合には、その訓練の内容及び体制を整備すること。

解説：実際に情報セキュリティ対策のための模擬的に事務を行うことにより、情報セキュリティ関係規程に係る知識・技能等を習得するために実施する訓練の内容及び体制を整備することを求める事項である。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。

(2) 情報セキュリティ対策の教育の受講

(a) 事務従事者は、毎年度最低１回、情報セキュリティ対策の教育に関する計画に従って、情報セキュリティ対策の教育を受講すること。

解説：事務従事者が、情報セキュリティ対策の教育に関する計画に従って、これを受講することを求める事項である。

(b) 事務従事者は、着任時又は異動時に新しい職場等で、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。

解説：着任、異動した事務従事者が、確実に情報セキュリティ対策の教育を受講するための事項である。

(c) 事務従事者は、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場合には、その理由について、職場情報セキュリティ責任者を通じて、全学実施責任者に報告すること。

解説：情報セキュリティ対策の教育を受講できない理由についての報告をしないままで、計画された教育を受講しない場合には、事務従事者は、その遵守違反について責任を問われることになる。

(d) 事務従事者は、情報セキュリティ対策の訓練に関する規定が定められている場合には、当該規定に従って情報セキュリティ対策の訓練に参加すること。

解説：事務従事者が、情報セキュリティ対策の訓練に関する規定に従って、これを受講することを求める事項である。

1.2.2.2 障害・事故等の対処

趣旨（必要性）

情報セキュリティに関する障害・事故等が発生又はそのおそれがある場合には、早急にその状況を検出又は確認し、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、その際には、障害・事故等の影響や範囲に関する責任者への報告及び学内外の関係部門との情報共有により、障害・事故等の発生現場の混乱や誤った指示の発生等を最小限に抑えるとともに、被害の拡大防止策や再発防止策を講ずることが重要である。これらのことを勘案し、本項では、障害・事故等の発生時に関する対策基準として、障害・事故等の発生に備えた事前準備、発生時における報告と対処の流れ、原因調査と再発防止策についての遵守事項を定める。

遵守事項

(1) 障害・事故等の発生に備えた事前準備

(a) 全学総括責任者は、情報セキュリティに関する障害・事故等（インシデント及び故障を含む。以下「障害・事故等」という。）の発生に対応するために以下の役割及び機能を有する体制を整備すること。

(ア) 障害・事故等に対応する責任者の決定
(イ) 障害・事故等の発生の報告
(ウ) 障害・事故等の発生報告の受付
(エ) 関係する部門への障害・事故等の発生に関する速やかな連絡
(オ) 応急措置の実施（被害の拡大防止）
(カ) 障害・事故等からの復旧
(キ) 原因調査の実施
(ク) 再発防止策の策定及び実施
(ケ) 再発防止策の実施の確認

解説：全学総括責任者に障害・事故等に対する体制の整備を求める事項である。本遵守事項が効果的に機能するように他の規程との整合性に配意することも必要である。障害・事故等に対する体制を整備するに当たっては、複数の部門で機能を分担することも考えられる。「障害・事故等に対応する責任者」とは、障害・事故等が発生した場合の対応に係る責任者であり、その役割としては、障害・事故等に関する全般的な対応が求められる。また、全学総括責任者が自ら障害・事故等への対応に当たる場合は、その指揮監督の下で必要な対応を行うこととなる。障害・事故等に対応する責任者は、情報セキュリティ対策に関する事務を総括する部門の責任者がその役割を担うことが考えられるが、全学実施責任者又は各部門の部局総括責任者がその役割を担うことも考えられる。その場合は、障害・事故等に関係する部門及び情報セキュリティ対策に関する事務を総括する部門との間で速やかな連絡ができる体制にすることが望ましい。「関係する部門への障害・事故等の発生に関する速やかな連絡」には、学内だけでなく、学外の関係部門への連絡も含まれる。なお、障害・事故等の発生時に、学外の関係部門へ速やかに連絡するためには、学外の関係部門と日常的な情報共有等の連携を図る必要がある。その場合、障害・事故等の発生時の

連絡と日常的な連携を複数の部門で分担することも考えられる。ただし、機能を分担する場合は、互いの部門間で、障害・事故等に関する情報や日常的な連携で得られた情報を共有する必要がある。なお、情報セキュリティに関する障害・事故等とは、機密性、完全性及び可用性が侵害されるものを対象としており、可用性等に影響を及ぼさない程度の故障等は対象としていない。また、「インシデント」とは、JIS Q 27002:2006（ISO/IEC 17799:2005）及び ISO/IEC 27035:2010 における情報セキュリティインシデントと同意である。

(b) 全学実施責任者は、障害・事故等について報告手順を整備し、当該報告手段を全ての事務従事者に周知すること。

解説：報告手順として、障害・事故等の発生を知った事務従事者から報告を受け、障害・事故等に対応する責任者が、全学総括責任者に報告するまでの具体的な手順や決定された障害・事故等に対応する責任者に対し、確実に報告ができる連絡手段等について明記する必要がある。また、報告手順の中には、例えば、全学総括責任者に障害・事故等の報告を集約するための窓口を設けることが考えられる。窓口についての周知は、情報セキュリティ対策の教育の中で行うとともに、窓口の連絡先を執務室内に掲示する等して、緊急時に事務従事者がすぐに参照できるようにする必要がある。なお、情報システムが利用不能となる状況も想定して、複数の連絡手段の導入を検討すること。窓口は、情報セキュリティ対策に関する事務を総括する部門に設置することが考えられるが、別の部門に窓口を設ける場合は、当該部門から障害・事故等に関係する部門への連絡や情報セキュリティ対策に関する事務を総括する部門への報告が速やかに実施される体制にすることが望ましい。

(c) 全学実施責任者は、障害・事故等が発生した際の学内及び学外との情報共有を含む対処手順を整備すること。

解説：対処手順として障害・事故等の発生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措置の承認手続を設けることもあわ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。対処手順は、より具体的に整備することが重要である。例えば、対処手順において、障害・事故等の発生日及び内容、障害・事故等への対処の内容及び対処者等を事務従事者が記録すべきこと並びに学内外の関係部門への障害・事故等の情報共有を行うまでの目標時間を定めること等も考えられる。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）等で定めた連絡連携体制を利用すること。

(d) 全学実施責任者は、障害・事故等に備え、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。

解説：全学実施責任者は、全ての部局技術責任者及び部局技術担当者の連絡網を整備しているものである（事務情報セキュリティ管理基準 1.2.1.1）が、障害･事故等が発生した場合に速やかに対応するため、「緊急」連絡網を加えて整備することを定める事

項である。緊急連絡網には、1.2.1.1 において整備を求める連絡網とは異なり、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、この場合、それぞれの連絡網の取扱いが異なることに注意する必要がある。なお、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、大規模な障害・事故等に備えて全学総括責任者も含める必要がある。

(e) 全学実施責任者は、障害・事故等への対処の訓練の必要性を検討し、必要と判断した場合には、その訓練の内容及び体制を整備すること。

解説：実際に障害・事故等への対処を模擬的に行うことにより、対応力を強化す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。訓練には、情報システム部門だけでなく、障害・事故等の報告の窓口となる部門や情報セキュリティ対策に関する事務を総括する部門も参加することが望ましい。この場合、障害・事故等の報告の窓口となる部門や情報セキュリティ対策に関する事務を総括する部門では、障害・事故等への専門的な対処を行う必要があるため、必要となる知識もより高度になる。そのため、訓練の一部として、障害・事故等の対処に関する教育を受講したり、外部から情報セキュリティに関する情報を適宜収集したりする必要がある。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。

(f) 事務従事者は、障害・事故等への対処の訓練に関する規定が定められている場合には、当該規定に従って、障害・事故等への対処の訓練に参加すること。

解説：事務従事者が、障害・事故等への対処の訓練に関する規定に従って、これに参加することを求める事項である。

(g) 全学実施責任者は、障害・事故等について学外から報告を受けるための窓口を設置し、その窓口への連絡手段を学外に公表すること。

解説：本学における情報セキュリティ対策の不備について外部の者が発見したり、本学において管理する電子計算機がサービス不能攻撃を外部に行った場合等、本学を取り巻く外部に対して、関連業務に支障を生じさせたり、情報セキュリティ上の脅威を与えたりした際に、その連絡を外部から受ける体制についても整備し、連絡先を本学の外部に公表することを求める事項である。

(2) 障害・事故等の発生時における報告と対処の流れ

(a) 事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、全学実施責任者が定めた報告手順により、障害・事故等に対応する責任者、及び障害・事故等に対応する責任者を通じて全学総括責任者にその旨を報告すること。ただし、緊急やむを得ない事情により、障害・事故等に対応する責任者に報告することができない場合は、定められた報告手順に従って、全学総括責任者に報告すること。

解説：障害・事故等が発生した場合に、事務従事者から速やかに関係者に連絡し、連絡を受けた者が当該障害・事故等への対処を開始すること、及び障害・事故等が発生したことについて事務従事者から障害・事故等に対応する責任者に報告され、障害・事故等に対応する責任者が速やかに全学総括責任者に報告することにより、全学総括責任者が状況を把握し、適切に対処することができるようにすることを求める事

項である。なお、連絡又は報告については、その内容により必要に応じて定められた受理者よりも上位の者に対して行う場合も考えられる。また、障害・事故等に対応する責任者に報告することができない場合は、他の手順により全学総括責任者に確実に報告される必要がある。

(b) 障害・事故等に対応する責任者は、被害の拡大防止等を図るための応急措置の実施及び障害・事故等からの復旧に係る指示又は勧告を行うこと。

解説：障害・事故等に対応する責任者に対し、報告を受けた障害・事故等に係る必要な措置を講ずることを求める事項である。応急措置や復旧に当たっては、障害・事故等が発生している情報システムの停止又は隔離について、障害・事故等に対応する責任者の判断で指示又は勧告ができるようにする必要がある。なお、障害・事故等に対応する責任者の役割を情報セキュリティ対策に関する事務を総括する部門の責任者が担う場合は、当該部門の責任者が応急措置及び復旧に関する具体的な指示又は勧告を行うこととなるが、全学実施責任者又は各部門の部局総括責任者が担う場合についても情報セキュリティ対策に関する事務を総括する部門が、具体的な指示又は勧告の取りまとめを支援する体制にすることが望ましい。

(c) 事務従事者は、障害・事故等が発生した際の対処手順の有無を確認し、それを実施できる場合には、その手順に従うこと。

解説：事務従事者の判断による被害拡大防止策が常に適切なものであるとは限らないため、障害・事故等への対処手順に従うことを求める事項である。

(d) 事務従事者は、障害・事故等が発生した場合であって、当該障害・事故等について対処手順がないとき及びその有無を確認できないときは、その対処についての指示を受けるまで、障害・事故等による被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。

解説：対処手順が想定していない障害・事故等が発生した場合、事務従事者は対処の指示を受けるまでの間も障害・事故等の拡大防止に努めることを求める事項である。

(e) 全学総括責任者は、報告を受けた障害・事故等について、定められた対処手順に従って、学内外の関係部門と情報共有を行うこと。

解説：障害・事故等が発生した場合に、学内外の関係部門と情報を共有することで、被害の拡大防止策及び再発防止策が講じられるようにすることを求める事項である。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）等で定めた連絡連携体制を利用すること。

(3) 障害・事故等の原因調査と再発防止策

(a) 部局総括責任者は、障害・事故等が発生した場合には、障害・事故等に対応する責任者が実施した内容も踏まえ、障害・事故等の原因を調査するとともに再発防止策を策定し、その結果を報告書として全学総括責任者に報告すること。

解説：部局総括責任者に対し、障害・事故等に対応する責任者が把握している障害・事故等の状況や実施した応急措置・復旧等の内容も踏まえて、障害・事故等の原因を究明し、それに基づき障害・事故等の再発防止策の策定を求める事項である。

(b) 全学総括責任者は、部局総括責任者から障害・事故等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こと。

解説：障害・事故等の再発防止策を講ずることを、全学総括責任者に求める事項である。

(4) 障害・事故等の発生するおそれがある場合の対処

(a) 全学総括責任者、全学実施責任者、部局総括責任者又は障害・事故等に対応する責任者は、障害・事故等の発生するおそれがある場合においては、本項の各遵守事項に準じて、必要な措置を講ずること。

解説：攻撃予告等により、インシデント等の発生するおそれがある場合については、それぞれの役割の者が、本項の各遵守事項に準じて必要な措置を講ずることを求める事項である。

(b) 事務従事者は、障害・事故等の発生するおそれがある場合においては、前事項による報告手順や対処手順等に基づき、適切な措置を講ずること。

解説：攻撃予告等により、インシデント等の発生するおそれがある場合において、事務従事者は、前事項（1.2.2.2(4)(a)）の規定に基づいて整備された報告手順や対処手順等に従い、適切な措置を講ずることを求める事項である。

1.2.3 評価

1.2.3.1 情報セキュリティ対策の自己点検

趣旨（必要性）

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、各自の役割を確実に行うことで実効性が担保されるものであることから、全ての事務従事者自らが情報セキュリティ関係規程に準拠した運用を行っているか否かについて点検することが重要である。また、自己点検の結果に基づき、それぞれの当事者又はその管理者がその責任において、必要となる改善策を実施する必要がある。

これらのことを勘案し、本項では、自己点検に関する対策基準として、自己点検に関する年度計画の策定とその実施に関する準備、自己点検の実施、結果の評価及び自己点検に基づく改善についての遵守事項を定める。

遵守事項

(1) 自己点検に関する年度計画の策定

(a) 全学実施責任者は、年度自己点検計画を策定し、全学総括責任者の承認を得ること。

解説：自己点検を実施するに当たり、その実施頻度、実施時期、確認及び評価の方法、実施項目の選択等に関する年度自己点検計画を策定することを求める事項である。実施頻度については、自己点検は年に２度以上実施することが望ましいが、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等、様々な選択肢が考えられる。実施時期については、例えば、当初は毎月 10 項目ずつ自己点検し、事務従事者の意識が高まった後、半年に一度、全項目を実施するように変更する等、様々な選択肢が考えられる。確認及び評価の方法については、例えば、単純に実施したことを確認するほか、遵守率を確認する

等、数値評価により客観性を持った評価とすることが望ましく、様々な選択肢が考えられる。実施項目の選択については、例えば、当初は全ての事務従事者が容易に遵守できる項目のみを自己点検し、事務従事者の意識が高まった後、遵守率が低いと想定される項目を実施するように変更する等、様々な選択肢が考えられる。なお、事務従事者自らが行う自己点検を原則とするが、システム的な仕組みを用いてパッチやパターンファイルの更新状況を把握したり、実際の文書を確認することによりその整備状況を把握する等、自己点検と同等以上の信頼性を有する方法が存在する場合には、代替方法としてそれを採用しても良い。

(2) 自己点検の実施に関する準備

(a) 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。

解説：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を求める事項である。

(3) 自己点検の実施

(a) 部局総括責任者は、全学実施責任者が定める年度自己点検計画に基づき、事務従事者に対して、自己点検の実施を指示すること。

解説：年度自己点検計画に基づき、部局総括責任者自らも含めた事務従事者に対して、自己点検の実施に関し指示することを求める事項である。

(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実施手順を用いて自己点検を実施すること。

解説：情報セキュリティに関わる事務従事者に対して、自己点検を実施し、自らが実施すべき対策事項について、実施の有無を確認することを求める事項である。

(4) 自己点検結果の評価

(a) 部局総括責任者は、事務従事者による自己点検が行われていることを確認し、その結果を評価すること。

解説：事務従事者による自己点検の結果について、部局総括責任者が評価することを求める事項である。なお、評価においては、自己点検が正しく行われていること、本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、自己点検実施率や、本基準遵守率、要改善対策数 /対策実施数等の準拠率の把握が挙げられる。

(b) 全学実施責任者は、部局総括責任者による自己点検が行われていることを確認し、その結果を評価すること。

解説：部局総括責任者による自己点検が適切に行われていることを、全学実施責任者が評価することを求める事項である。

(c) 全学実施責任者は、自己点検の結果を全学総括責任者へ報告すること。

解説：全学実施責任者は、自己点検の結果を全学総括責任者へ報告することを求める事項

である。

(5) 自己点検に基づく改善

(a) 事務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、部局総括責任者にその旨を報告すること。

解説：自己の権限の範囲で改善可能である問題点については、情報セキュリティに関わる全ての事務従事者自らが自己改善することを求める事項である。

(b) 全学総括責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には部局総括責任者に改善を指示すること。

解説：自己点検の結果により明らかとなった問題点について、全学総括責任者が部局総括責任者に対して改善することを求める事項である。

1.2.3.2 情報セキュリティ対策の監査

趣旨（必要性）

情報セキュリティの確保のためには、本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準に準拠して本基準が適切に策定され、かつ、情報セキュリティ関係規程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、その準拠性と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、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。

これらのことを勘案し、本項では、情報セキュリティ対策の監査に関する対策基準として、監査計画の策定とその実施に関する指示、個別の監査業務における監査実施計画の策定、監査の実施に係る準備、監査の実施及びその結果に対する対処についての遵守事項を定める。

遵守事項

(1) 監査計画の策定

(a) 情報セキュリティ監査責任者は、年度監査計画を策定し、全学総括責任者の承認を得ること。

解説：監査の基本的な方針として、年度監査計画を策定し、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、不正アクセス防止等）
・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、年度監査計画に盛り込むこと。

(2) 監査の実施に関する指示

(a) 全学総括責任者は、年度監査計画に従って、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こと。

解説：年度監査計画に従って監査を実施することを求める事項である。

(b) 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、年度監査計画で計画されたこと以外の監査の実施を指示すること。

解説：年度監査計画において実施する監査以外に、学内外における注目すべき事案の発生又は情報セキュリティ対策の実施内容について重大な変更が生じた場合に、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。

(3) 個別の監査業務における監査実施計画の策定

(a) 情報セキュリティ監査責任者は、年度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こと。

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

・監査の実施場所

・監査実施者及び担当職務の割当て

・準拠性監査（情報セキュリティ関係規程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情報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

なお、被監査部門に対し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に関して、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。

また、本事務情報セキュリティ管理基準においては、監査業務に対して監査を別途実施することを必須とはしてない。しかし、監査実施者が監査過程で被監査者を監査すること以外のことを実施した場合には、その実施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、監査実施計画を策定する際は、監査実施者が実施することが情報セキュリティ対策の向上になり得ることや、何らかの作業を効率的に行えるとしても、それを安易に監査実施計画の中に取り込むべきではない。

(4) 監査の実施に係る準備

(a) 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。

解説：情報セキュリティ監査責任者に、本学において監査業務を実施するに当たり、必要となる者を情報セキュリティ監査実施者に指名することを求める事項である。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は、当該情報システムの構築をした者は、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。

(b) 情報セキュリティ監査責任者は、学外の者に監査の一部を請け負わせる必要性を検討し、必要と判断した場合には、学外の者に監査の一部を請け負わせること。

解説：情報セキュリティ監査責任者に、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、学内の情報システム部門に加えて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等を考慮することが望ましい。

(5) 監査の実施

(a) 情報セキュリティ監査実施者は、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こと。

解説：情報セキュリティ監査実施者が適切に監査を実施することを求める事項である。

(b) 情報セキュリティ監査実施者は、本基準が事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準に準拠していることを確認すること。

解説：本基準が事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準に準拠して設計されていることの確認を求める事項である。

(c) 情報セキュリティ監査実施者は、実施手順が本基準に準拠していることを確認すること。

解説：本学における実施手順が本基準に準拠して設計されていることの確認を求める事項である。

(d) 情報セキュリティ監査実施者は、自己点検の適正性の確認を行う等により、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を確認すること。

解説：被監査部門における実際の運用が、本学の情報セキュリティ関係規程に準拠して実施されていること（運用の準拠性）の確認を求める事項である。運用の準拠性の確認は、自己点検の適正性の確認によることが実効性の高い方法であると考えられる。監査に当たっては、自己点検結果に基づく担当者への質問、記録文書の査閲、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の妥当性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脆弱性検査、侵入検査等のその他の方法によっても確認することができる。

(e) 情報セキュリティ監査実施者は、監査調書を作成すること。

解説：監査報告書の根拠となる監査調書を適切に作成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綴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。

(f) 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こと。

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、本基準が事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準に準拠しているか、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。

(6) 監査結果に対する対処

(a) 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、指摘されたことに対する対処の実施を指示すること。

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処実施の指示を求める事項である。

(b) 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、他の部門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こと。

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。

(c) 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、対処計画を策定し、報告すること。

解説：監査報告書や監査調書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、対処計画の策定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処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、提示された対処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。

(d) 全学総括責任者は、監査の結果を踏まえ、既存の情報セキュリティ関係規程の妥当性を評価し、必要に応じてその見直しを指示すること。

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、課題とその改善に対する助言意見等の指摘を受けた場合には、既存の情報セキュリティ関係規程の見直しを検討することを求める事項である。検討の結果、情報セキュリティ関係規程の見直しを行わない場合には、その理由について明確化すること。

1.2.4 見直し

1.2.4.1 情報セキュリティ対策の見直し

趣旨（必要性）

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、情報セキュリティレベルは維持できなくなる。このため、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、作成、導入、運用、評価の各段階において、適時見直しを行う必要がある。これらのことを勘案し、本項では、情報セキュリティ対策の見直しに関する対策基準について定める。

遵守事項

(1) 情報セキュリティ対策の見直し

(a) 情報セキュリティ関係規程を整備した者は、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こと。

解説：情報セキュリティ関係規程を整備した者は、新たなセキュリティ脅威の出現、自己点検及び監査の評価結果等を踏まえつつ、情報セキュリティ対策に支障が生じないように見直しを行う時期を判断する必要がある。情報セキュリティ関係規程を見直した者は、他部門へも影響があると思われる場合、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。

(b) 事務従事者は、情報セキュリティ関係規程に課題及び問題点が認められる場合には、情報セキュリティ関係規程を整備した者に相談すること。

解説：事務従事者自らが整備したものではない情報セキュリティ関係規程について、課題及び問題点が認められる場合には、情報セキュリティ関係規程を整備した者に相談することを求める事項である。

(c) 情報セキュリティ関係規程を整備した者は、情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合は、必要な措置を講ずること。

解説：情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合に、その是非を検討し、必要な措置を講ずることを求める事項である。例えば、事務従事者からの相談が妥当であると思料する場合に情報セキュリティ関係規程の見直しを行ったり、逆に事務従事者の理解不足が原因であると思料する場合は、再教育の措置を講ずること等が考えられる。

1.2.5 その他

1.2.5.1 外部委託

趣旨（必要性）

学外の者に情報処理業務を委託する場合（外部の設備を利用した役務提供も含む）には、本学が委託先を直接管理することができないため、学内で行う場合と比べ、情報の機密性、

完全性及び可用性が損なわれるリスクが増大する。

このリスクに対応するため、情報処理業務を外部委託する際は、委託先においても本基準と同等の対策を実施させるべく、委託先への要求事項を定める必要がある。

これらのことを勘案し、本項では、外部委託に関する対策基準を定める。具体的には、

・情報セキュリティ確保のための学内共通の仕組みの整備
・委託先に実施させる情報セキュリティ対策の明確化
・委託先の選定
・外部委託に係る契約
・外部委託の実施における手続
・外部委託終了時の手続

についての遵守事項を定めるものである。

適用範囲

本項は、本学による貸借、請負その他の契約に基づき提供される役務のうち、情報処理に係る業務であって、例えば次に掲げる営業品目に該当するものに適用する。

- ソフトウェア開発（プログラム作成、システム開発等）
- 情報処理（統計、集計、データエントリー、媒体変換等）
- 賃貸借
- 調査・研究（調査、研究、検査等）

遵守事項

(1) 情報セキュリティ確保のための学内共通の仕組みの整備

(a) 全学実施責任者は、外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準を整備すること。

解説：外部委託の対象としてよい範囲としてはいけない範囲を判断する基準を本学として整備することを定めた事項である。学内の情報システム及び関連する業務に関し、網羅性を確保しつつ統一的な基準で当該範囲を設定することが重要である。また、データの所在については、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切とな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。例えば、「行政機関の保有する個人情報の保護に関する法律」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判断すること等が考えられる。

(b) 全学実施責任者は、委託先の選定基準及び選定手続を整備すること。

解説：委託先の選定において整備すべき手続や基準に関して定めた事項である。全学実施責任者は、委託先の選定基準の整備に当たっては、当該委託先が、事業の継続性を有し存続可能であり、本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、例えば、委託先が本基準の該当項目を遵守し得る者であること、本基準と同等の情報セキュリティ管理体制を整備すること、本基準と同等の情報セキュリティ対策の教育を実施す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 等に基づく認証制度の活用や、国際規格を踏まえ、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（http://www.jisc.go.jp/mss/other.html）」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が望ましい。なお、本基準は、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、外部委託の実施に反映することが必要である。

(2) 委託先に実施させる情報セキュリティ対策の明確化

(a) 部局技術責任者又は職場情報セキュリティ責任者は、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容を定め、委託先候補に事前に周知すること。

解説：委託先に実施させる情報セキュリティ対策の内容を具体的に定めることを求める事項である。外部委託に係る業務において納入される成果物（特に情報システム）に関しては、委託先における情報セキュリティ対策が適切に実施されていることがその後の情報システム等の運用におけるセキュリティレベルの維持及び向上の前提となることから、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容を定め、周知しておくことが重要である。なお、職場情報セキュリティ責任者が外部委託に係る業務について責任を負う場合には、例えば、課室において保有する情報の加工・処理を外部委託により行う場合がある。

(b) 部局技術責任者又は職場情報セキュリティ責任者は、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処方法を整備し、委託先候補に事前に周知すること。

解説：委託先に請け負わせる業務における情報セキュリティの侵害発生時の対処方法を本学として整備することを定めた事項である。情報セキュリティの侵害の業務に対する影響度の大きさや機密性、完全性及び可用性の要求度に応じて、対処の緊急性等を考慮することが重要である。

(c) 部局技術責任者又は職場情報セキュリティ責任者は、委託先におけ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及び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を整備し、委託先候補に事前に周知すること。

解説：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ること、及び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ことにかんがみ、これらのための方法の整備を求める事項である。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。周知す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で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、本学及び委託先が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こと。

(3) 委託先の選定

(a) 部局技術責任者又は職場情報セキュリティ責任者は、選定基準及び選定手続に基づき、委託先を選定すること。

(4) 外部委託に係る契約

解説:委託先の選定時における手続等の遵守に関して定めた事項である。

(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、委託先に請け負わせる業務における情報セキュリティ対策、機密保持(情報の目的外利用の禁止を含む。)、情報セキュリティの侵害発生時の対処方法、情報セキュリティ対策の履行状況の確認方法及び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を含む外部委託に伴う契約を取り交わすこと。また、必要に応じて、以下の事項を当該契約に含めること。

(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

解説:情報セキュリティの観点から、外部委託に係る契約に含めるべき事項を定めた事項である。機密保持に関する条項は、要機密情報が委託範囲に含まれるか否かにかかわらず、請け負った業務及びその業務の遂行により知り得る情報を守るべきであることから、これを記載する必要がある。情報セキュリティ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を契約に含める。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、事故発生時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。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こと。なお、国の安全に関する重要な情報を委託先に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を当該契約に含めること。

(b) 部局技術責任者又は職場情報セキュリティ責任者は、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書等を提出させること。また、必要に応じて、以下の事項を当該確認書等に含めさせること。

(ア) 当該委託業務に携わる者の特定

(イ) 遵守すべき情報セキュリティ対策を実現するために、当該者が実施する具体的な取組内容

解説：外部委託に係る契約者双方の責任の明確化と合意形成に基づく委託先からの確認書等の提出に関し定めた事項である。必要に応じて、当該委託業務に携わる委託先の者の特定や、当該者が実施する取組内容を、委託先に確認することが重要になる。特に、情報システムの構築及びソフトウェア開発等の外部委託の場合には、成果物における情報セキュリティ対策の実施が、その作成プロセスと不可分であることが想定されるため、遂行される業務全体の責任者を報告させることが重要である。

(c) 部局技術責任者又は職場情報セキュリティ責任者は、外部委託契約の継続に関しては、選定基準及び選定手続に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。

解説：外部委託契約の継続、特に随意契約に関し、都度審査することを定めた事項である。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こと。

(d) 部局技術責任者又は職場情報セキュリティ責任者は、委託先の提供する役務（情報セキュリティ基本方針、実施手順、管理策の維持及び改善を含む。）の変更に関しては、選定基準及び選定手続に基づき、その是非を審査すること。

解説：委託契約の実施中の契約変更に関して定めた事項である。変更がある場合にはその是非を審査し、必要に応じて、契約変更をする等の対応が必要である。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こと。

(e) 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措置を委託先に担保させること。

解説：委託先がその委託内容を再委託することは、セキュリティレベルの低下を招くことが懸念されることから原則として避けるべきである。一方、委託先がその委託内容を再委託する場合には、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措置を委託先に担保させることを定めた事項である。情報セキュリティを十分に確保するためには、委託先自体が業務を実施する場合に求めるべき水準と同一水準の情報セキュリティ対策を再委託先においても確保させる必要がある。

(5) 外部委託の実施における手続

(a) 事務従事者は、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、以下の措置を講ずること。

(ア) 委託先に情報を提供する場合は、安全な受渡し方法によりこれを実施し、提供した記録を取得すること。

(イ) 外部委託の業務終了等により提供した情報が委託先において不要になった場合には、これを確実に返却させ、又は廃棄させ、若しくは抹消（全ての情報を復元が困難な状態にすることをいう。以下同じ。）させること。

解説：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を必要最小限に止め、また、提供に伴う要保護情報の漏えいや滅失等を防止するための措置の実施を求める事項である。委託先への情報の提供における遵守事項は、本事務情報セキュリティ管理基準の「1.3.1.4 情報の移送」及び「1.3.1.5 情報の提供」の定めに準ずるが、例えば機密性３情報を提供する場合には、当該外部委託について責任を負う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、また、機密性２情報を提供する場合には、これらの者のいずれかに届け出ることが必要となる。委託先の選定基準や情報セキュリティの侵害時の対処方法を整備した上で、当事者間の情報の授受において上記の措置に従うことにより情報セキュリティを確保することが重要である。

(b) 部局技術責任者又は職場情報セキュリティ責任者は、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、取り交わした契約の対処方法に従い、委託先に必要な措置を講じさせること。

解説：請け負わせた業務の実施中に情報セキュリティの侵害が発生した場合に、契約に記載した対処方法に従い、委託先に必要な措置を講じさせること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事項である。

(c) 部局技術責任者又は職場情報セキュリティ責任者は、取り交わした契約の対処方法に従い、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。

解説：委託先に請け負わせた業務の実施中に、契約に記載した方法に従い、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事項である。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、契約に記載し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。

(6) 外部委託終了時の手続

(a) 部局技術責任者又は職場情報セキュリティ責任者は、外部委託の終了時に、委託先に請け負わせた業務において行われた情報セキュリティ対策を確認し、その結果を納品検査における確認の判断に加えること。

解説：外部委託に係る業務の終了時における情報セキュリティ対策の確認に関して定めた事項である。委託先に請け負わせた業務において情報セキュリティ対策が契約に従い適切に実施されていることが、その後の運用におけるセキュリティレベルの維持及び向上の前提となる。このため、部局技術責任者又は職場情報セキュリティ責任者は、委託先において実施された情報セキュリティ対策を確認し、その結果を納品検査の判断に加えることが重要である。

1.2.5.2 業務継続計画及び情報システム運用継続計画との整合的運用の確保

趣旨（必要性）

本学においては、「中央省庁業務継続ガイドライン第１版」（平成 19 年 6 月、内閣府）に

基づき、業務の継続に重大な支障を来す可能性が想定される事態を特定し、当該事態に対応する計画を業務継続計画として策定することが想定されている。また、「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」（平成 23 年 3 月、内閣官房情報セキュリティセンター）を活用し、必要な情報システムについて、運用を継続するために必要な計画（以下「情報システム運用継続計画」という。）を策定することが求められる。他方、業務継続計画及び情報システム運用継続計画の対象とする事態は、多くの場合に情報セキュリティを損なうものともなり、本学の情報セキュリティ関係規程に基づく対策も講じられることとなる。この場合、業務継続計画及び情報システム運用継続計画の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要である。

これらのことを勘案し、本項では、業務継続計画及び情報システム運用継続計画と情報セキュリティ対策との間の整合性の確保並びに情報セキュリティ関係規程との間の不整合の報告に関する対策基準を定める。

遵守事項

(1) 業務継続計画及び情報システム運用継続計画と情報セキュリティ対策との間の整合性の確保

(a) 全学情報システム運用委員会は、本学において業務継続計画、情報システム運用継続計画又は本基準を整備する場合には、業務継続計画及び情報システム運用継続計画と本基準との間の整合性の確保のための検討を行うこと。

解説：業務継続計画、情報システム運用継続計画及び本基準は、それぞれの目的を達成するために、特定の事態に対して異なる対応が定められることも考えられる。当該事態の例として、情報システムの稼動を損なう地震及び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、並びに情報機器の故障等が想定される。これらの事態に対して業務継続計画、情報システム運用継続計画及び本基準のそれぞれで定める対策に矛盾があると、それぞれの遵守を求められる本学組織及び事務従事者は、日常及び事態発生時に一貫性のある適切な行動をとることができない。このため、業務継続計画及び情報システム運用継続計画と本基準との間で整合性を確保するよう検討を行うことが必要である。本事務情報セキュリティ管理基準の 1.2.1.1 項で全学情報システム運用委員会は本基準の策定を求められているが、その策定及び見直しの際に、本学が業務継続計画及び情報システム運用継続計画で定め、又は定めることが予定されている要求事項を全学情報システム運用委員会が把握した上で、業務継続計画及び情報システム運用継続計画の整備を担当する者と協議しそれぞれが定める内容を調整する必要がある。また、業務継続計画及び情報システム運用継続計画に変更が生じ、又は生ずることが予定されている場合には、その変更が本基準に影響するかどうかを確認し、必要があれば、本基準の改訂を行う等して、業務継続計画及び情報システム運用継続計画との整合性の確保に努めなければならない。

(b) 全学実施責任者、部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者は、本学において業務継続計画及び情報システム運用継続計画を整備する場合には、全ての情報システムについて、当該業務継続計画及び情報システム運用継続計画との

関係の有無を検討すること。

解説：業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間の整合性を確保する前提として、本学の情報システムのうち、業務継続計画及び情報システム運用継続計画と関係のある情報システムを特定することを求める事項である。

(c) 全学実施責任者、部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者は、本学において業務継続計画及び情報システム運用継続計画を整備する場合には、当該業務継続計画及び情報システム運用継続計画と関係があると認めた情報システムについて、業務継続計画及び情報システム運用継続計画との整合性を考慮し、必要な措置を講ずること。

(ア) 通常時において業務継続計画及び情報システム運用継続計画と本基準との整合的運用が可能となるよう必要な措置を講ずること。

解説：例えば、事態発生時には、業務の継続以外の対応として、本学の施設の一部を帰宅困難者や救命等が必要な外来者の退避場所として使用する場合等も考えられる。このような場合を想定した対策を講じていないと、不特定者の出入りによって通常時と比べてセキュリティレベルの確保に支障を来すおそれがある。このため、セキュリティ確保の面で配慮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、施設全体の入館管理だけでなく、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、通常時から不特定者の出入りを想定した対策を講ずる必要がある。また、事態発生時にも利用することを想定している情報システムについては、事態発生時に確実に利用できるように、通常時において耐震対策等の物理的な対策を講ずる必要がある。

(イ) 事態発生時において業務継続計画、情報システム運用継続計画及び本基準との整合的運用が可能となるよう実施手順の整備等の必要な措置を講ずること。

解説：事態発生への対応として、業務継続計画、情報システム運用継続計画及び本基準のそれぞれにおいて事態発生時における情報システムの稼動水準及び復旧までの所要時間の目標を定め、その達成を図る様々な対応を実施手順において具体的に定めることとなるため、相互の整合性を確保するための実施手順の整備が必要となる。この場合、対策として、例えば、施設の耐災害性確保、施設・情報システムの地理的分散及び冗長化、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用等がある。また、事態発生時の対応体制及び担当者の指名も整備対象となり得る。また、事態発生時には、情報システムの主体認証情報（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。しかしながら、個人が管理しているパスワードの共用（共用識別コードに係るものを除く。）は、そもそも情報セキュリティ対策の観点では厳に禁止されるべきものである上、事態発生時には、パスワードを聞き出す者についての本人確認等が不十分となることも想定される。このような事態発生時の手順については、業務継続計画及び情報システム運用継続計画で安易に定めるのではなく、事態発生時においても必要な情報セキュリティを確保するために、本基準において事態発生時の実施手順として整備する必要がある。手順の一例としては、

起動のためのパスワードを通常時には使用者だけが主として管理するような端末の管理者権限アカウントについては、本人が設定するアカウントのほかに、事態発生時用のアカウントをあらかじめ設定しておく方法が考えられる。この方法を用いる場合は、まず、その事態発生時用のアカウントのパスワードを人が記憶困難な文字列で設定し、設定内容を記載した紙面を施錠された安全な保管場所で保管しておく。そして、事態発生時には、その紙面を参照し事態発生時用のアカウントで起動する。このような手順を採用することで、パスワードの聞き出しや事態発生時以外の共用を回避することができる。また、設定内容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の確認が可能となる。なお、このような手順の方が、事態発生時に本人に連絡して聞き出すよりも、迅速に対応ができるものと思われる。

(2) 業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程との間の不整合の報告

(a) 事務従事者は、本学において業務継続計画及び情報システム運用継続計画と整備する場合であって、業務継続計画、情報システム運用継続計画及び情報セキュリティ関係規程が定める要求事項との違い等により、実施の是非の判断が困難なときは、関係者に連絡するとともに、全学実施責任者が整備した障害・事故等が発生した際の報告手順により、部局総括責任者にその旨を報告して、指示を得ること。

解説：本来、業務継続計画及び情報システム運用継続計画と情報セキュリティ関係規程が定める要求事項との間の整合性については、上記(1)の遵守事項を適正に実施することで担保されるものである。しかしながら、情報セキュリティ関係規程との間では、業務継続計画及び情報システム運用継続計画の対象となる状況においては、事前に想定していなかった様々な不整合が発生すると考えられる。業務継続計画の重要性を考慮すると、万が一、不整合について、全学情報システム運用委員会等が事前に想定できなかった場合にも、それを迅速に改善できるようにしておくべきである。

1.2.5.3 情報取扱区域

趣旨（必要性）

悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる設置環境にある場合においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改ざん等が行われるおそれがある。また、その他にも、設置環境に関する脅威としては、自然災害の発生による情報システムの損傷や情報の紛失等が発生するおそれもある。

このように施設全体や区域ごとに様々な脅威が考えられるため、それぞれの区域に応じた管理と想定される利用形態に応じた情報の取扱いを行う必要がある。

これらのことを勘案し、本項では、情報取扱区域にクラスの区分を設け、クラスに応じた管理及び利用を行うための対策基準として、情報取扱区域のクラス、管理及び利用制限の決定、情報取扱区域の管理並びに情報取扱区域における利用制限についての遵守事項を定める。

遵守事項

(1) 情報取扱区域のクラス、管理及び利用制限の決定

(a) 全学実施責任者は、情報取扱区域にクラスの区分を定め、クラスに応じた管理対策及び利用制限対策を決定すること。なお、決定する内容は、事務情報セキュリティ技術基準 2.3.1.1（別表 1 及び別表 2 を含む。）に定める。

解説：情報取扱区域にクラスの区分を設け、各クラスの利用用途に応じたセキュリティの確保を求めるための事項である。

(b) 部局総括責任者は、要管理対策区域については、当該区域を管理又は利用する事務従事者がクラスについて認識できる措置を講ずること。

解説：決定された情報取扱区域のクラス区分について共通の認識となるように措置することで、クラスに応じた管理対策及び利用制限対策が講じられるようにするための事項である。「認識できる措置」には、A.1.5 情報取扱区域のクラスと区域例の内容を参考に本学で定めた内容を周知する、区域ごとにクラスを掲示する、若しくは当該区域で情報を取り扱う際に必要な利用制限対策を掲示又は周知する等が考えられる。なお、関係者限りで管理及び利用する区域については、関係者のみにクラスを周知することでも構わない。

(c) 区域情報セキュリティ責任者は、個別の管理対策及び利用制限対策を決定する必要性の有無を検討し、必要と認めた場合は、当該対策を決定し、全学実施責任者に報告すること。

解説：決定したクラスの区域において、必要な対策が不足していると認められる区域、又は定められたクラスとは別の区分で対策を講ずる必要がある区域があるときは、求める情報セキュリティ水準を確保又は向上させるために、定められたクラス別管理及び利用制限にかかわらず、当該区域ごとに個別に管理対策及び利用制限対策を決定することを求める事項である。

(2) 情報取扱区域の管理

(a) 区域情報セキュリティ責任者は、要管理対策区域を管理する場合には、全学実施責任者が定めた当該区域のクラスを確認し、事務情報セキュリティ技術基準 2.3.1.1（別表 1 を含む。）に定める管理対策を講ずること。また、個別の管理対策を決定している場合には、同様に対策を講ずること。

解説：区域情報セキュリティ責任者が要管理対策区域を管理する場合に、当該区域で求められる管理対策を講ずることを求める事項である。個別の管理対策については、A.1.6 情報取扱区域の個別管理及び利用制限の付表例を参照。

(3) 情報取扱区域における利用制限

(a) 区域情報セキュリティ責任者は、全学実施責任者が定めた情報取扱区域のクラスを確認し、事務情報セキュリティ技術基準 2.3.1.1（別表 2 を含む。）に定める利用制限対策を講ずること。なお、個別に利用制限対策を決定している場合には、同様に講ずること。

解説：区域情報セキュリティ責任者が当該区域で求められる利用制限対策を講ずることを求める事項である。

(b) 事務従事者は、情報を取り扱う場合には、全学実施責任者が定めた情報取扱区域のク

ラスを確認し、事務情報セキュリティ技術基準 2.3.1.1（別表 2 を含む。）に定める利用制限対策に従って利用すること。なお、個別の利用制限対策を決定している場合には、同様に従うこと。

解説：事務従事者が要管理対策区域を利用する場合に、当該区域で求められる利用制限対策に従って利用することを求める事項である。なお、事務従事者が学外の者を立ち入らせる際に、当該区域で求められる利用制限対策に従って利用させることも含まれる。個別の利用制限対策については、A.1.6 情報取扱区域の個別管理及び利用制限の付表例を参照。

第 1.3 部　情報についての対策

1.3.1 情報の取扱い

1.3.1.1 情報の作成と入手

趣旨（必要性）

高等教育機関の事務においては、その事務の遂行のために複数の者が共通の情報を利用する場合がある。この際、利用者により当該情報の取扱いに関する認識が異なると、当該情報に応じた適切な情報セキュリティ対策が採られないおそれがあるため、情報を作成し、又は入手した段階で、全ての利用者において認識を合わせるための措置が必要となる。

これらのことを勘案し、本項では、情報の作成及び入手に関する対策基準として、業務以外の情報の作成又は入手の禁止、情報の作成又は入手時における格付と取扱制限の決定、格付と取扱制限の明示等、格付と取扱制限の加工時における継承についての遵守事項を定める。

遵守事項

(1) 業務以外の情報の作成又は入手の禁止

(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、情報を作成し、又は入手しないこと。

解説：高等教育機関の事務の遂行以外の目的で、情報を作成し、又は入手しないことを求める事項である。

(2) 情報の作成又は入手時における格付と取扱制限の決定

(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すること。

解説：作成又は入手した情報について、以降、適切な情報セキュリティ対策が実施されるように、機密性、完全性及び可用性の格付及び取扱制限を決定することを求める事項である。情報の格付が適切に決定されていなかった、また、明示等されていなかったことを一因として障害・事故等が発生した場合には、障害・事故等の直接の原因となった人物のほか、情報の格付及び明示等を適切に行わなかった情報の作成者にも責任が及ぶことがある。その観点からも、事務従事者が、情報の格付及び取扱制限とその明示等を確実に行うことは重要である。なお、格付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十分注意しなければならない。格付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って事務が繁雑になり、情報の利便性や有用性が損なわれたり、事務の繁雑さを事務従事者が煩わしく思うことで適切な管理が行われなくなったりするおそれがある。特に、格付及び取扱制限を必要以上に高くしないように配慮することも、情報の利用を円滑に行うために注意が必要である。例え

ば、本来要機密情報とする情報を要機密情報に決定しないことは不適切であるが、逆に、本来要機密情報ではない情報（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決定することも不適切であることに注意すること。また、取扱制限については必要性の有無を検討し、その結果指定しないという決定を行っても差し支えない。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、格付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、決定した格付及び取扱制限に基づき、その指定を行うこと。なお、本遵守事項に基づき、情報セキュリティ確保の観点から、取扱制限として保存期間を指定する場合も考えられる。

(b) 事務従事者は、元の情報の修正、追加、削除のいずれかにより、他者が決定した情報の格付及び取扱制限を変更する必要があると思料する場合には、前項に従って再決定すること。

解説：元の情報の修正、追加、削除のいずれかにより、格付又は取扱制限を変更する必要が生じた場合には、格付及び取扱制限の再決定を行う必要がある。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

なお、情報の格付及び取扱制限は、本基準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。情報の格付及び取扱制限の変更には、大別して再決定と見直しがある。再決定した場合には、再決定後の新たな格付等の決定者は再決定した者となる。見直しについては、1.3.1.2 情報の利用(4)を参照のこと。

(3) 格付と取扱制限の明示等

(a) 事務従事者は、情報の格付及び取扱制限を決定（再決定を含む。以下同じ。）した際に、当該情報の参照が許されている者が認識できる方法を用いて明示等すること。

解説：作成者又は入手者によって格付及び取扱制限が決定された情報に対して、以降、他者が当該情報を利用する際に必要とされる情報セキュリティ対策の内容を示すため、情報の格付及び取扱制限の明示等を行うことを求める事項である。「明示等」とは、情報を取り扱う全ての者が当該情報の格付及び取扱制限について共通の認識となるように措置することをいい、情報ごとの格付の区分及び取扱制限の種類を当該情報に記載することによる明示を原則とする。なお、格付の区分及び取扱制限の種類を記載していたとしても、当該ファイルを参照する者が、その内容を参照する際に格付の区分及び取扱制限の種類を特段の手順なく視認することができない状態（例えば、文書ファイルのプロパティ設定に格付の区分を記載することや、文章閲覧時に画面表示はされず印刷しかされないヘッダ部分に記載すること等）については、記載しても明示に当たらない。格付及び取扱制限の明示等は、当該情報が、電磁的フ

ファイルとして取り扱われることが想定される場合にはファイル名自体又は情報内容の中に、外部電磁的記録媒体に保存して取り扱うことが想定される場合には外部電磁的記録媒体に、書面に印刷されることが想定される場合には書面のヘッダ部分等に、それぞれ記載する必要がある。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等する場合には、手書きによる記入又はスタンプ等による押印が必要である。なお、原則として各書面それぞれに明示等すべきであるが、取り扱う単位がフォルダ単位や冊子単位の時には、その単位ごとに明示等することも可能である。なお、格付及び取扱制限の明示等とあわせて、情報の作成者又は入手者の氏名、所属、連絡先等を記載することも有益である。

明示等を行うに当たっては、格付の区分及び取扱制限の種類を記載することによる明示が原則であるが、以下のような場合に明示等を簡便化してもよい。

① 格付及び取扱制限の明示等を簡便化できる場合

特定の情報（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）の格付及び取扱制限を規定等により明記し、当該情報にアクセスする全ての者に当該規定を周知している場合は、格付の区分及び取扱制限の種類について記載することを省略することができる。具体的な例としては、次のような場合が考えられる。

・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の区分及び取扱制限を規定等により明記し、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。

・取り扱う情報の格付が機密性１、完全性１及び可用性１の場合には、記載による明示を簡便化できることを規定等により周知している場合。

ただし、格付及び取扱制限の明示等を簡便化した場合には、以下の事項に注意する必要がある。

格付及び取扱制限の明示等を簡便化した場合の注意事項

① 格付及び取扱制限の決定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の種類が記載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、他の公用教育機関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の種類を記載した上で提供しなければならない。

② 取扱制限の明示等を簡便化した場合における取扱制限の追加・変更例えば、簡便化に係る規定等により、特定の文書ファイルについて、取扱制限の種類の記載を省略している場合において、当該ファイルのうち一部のファイルについて取扱制限を追加するときは、追加する取扱制限の種類のみを記載すること。また、取扱制限を解除する場合は、当該解除する取扱制限を「送信可」「印刷可」等のように記載することが考えられる。

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。

(4) 格付と取扱制限の加工時における継承

(a) 事務従事者は、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又は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。

解説：作成の際に参照した情報又は入手した情報が既に機密性に係る格付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維持することを求める事項である。なお、完全性及び可用性については、引用した新たな情報において適切な格付及び取扱制限を決定すること。

1.3.1.2 情報の利用

趣旨（必要性）

高等教育機関の事務においては、その遂行のために多くの情報を利用するが、利用者の認識不足等により情報を不適切に取り扱うと、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれがある。このリスクに対応するため、高等教育機関の事務の遂行において、情報は、格付等に応じて定められた手続に従い、適切に利用しなければならない。これらのことを勘案し、本項では、情報の利用に関する対策基準として、業務以外の利用の禁止、格付及び取扱制限に従った情報の取扱い、格付及び取扱制限の複製時における継承、格付及び取扱制限の見直し、要保護情報の取扱いについての遵守事項を定める。

遵守事項

(1) 業務以外の利用の禁止

(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、情報を利用しないこと。

解説：高等教育機関の事務の遂行以外の目的で、情報を利用しないことを求める事項である。

(2) 格付及び取扱制限に従った情報の取扱い

(a) 事務従事者は、利用する情報に明示等された格付に従って、当該情報を適切に取り扱うこと。格付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取り扱うこと。

解説：情報に明示等された格付及び取扱制限に従って、適切に取り扱うことを求める事項である。

(3) 格付及び取扱制限の複製時における継承

(a) 事務従事者は、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こと。

解説：複製の際に元となる情報が既に機密性に係る格付又は取扱制限の明示等がされている場合には、元となる格付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維持することを求める事項である。なお、完全性及び可用性については、複製した新たな情報において適切な格付及び取扱制限を決定すること。

(4) 格付及び取扱制限の見直し

(a) 事務従事者は、情報を利用する場合に、元の格付又は取扱制限がその時点で不適切と考えるため、他者が決定した情報の格付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（以下この項において「決定者等」という。）に相談すること。

解説：利用する元の情報への修正、追加、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同人の上司に相談し、その是非を検討することになる。ただし、元の決定者等のいずれかによる再決定がない限り、当該情報の利用者がそれらの者に無断で、格付又は取扱制限を変更することは許されない。見直しにより元の決定者等に相談することが必要となる例として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）

・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

相談を受けた決定者等は、次項 (b)に基づいて所要の措置を講ずることになる。

(b) 事務従事者は、自らが格付及び取扱制限の決定者等である情報に対して、見直しの必要があると認めた場合には、当該情報の格付又は取扱制限を再決定し、それを明示等すること。また、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すること。

解説：いずれの理由であっても、適切な格付又は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、適切な格付又は取扱制限に変更することを求める事項である。また、同一の情報が異なる格付又は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、格付又は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。当該情報を直接提供した相手やそれを参照したと思われる者を特定することが困難な場合には、わかる範囲で構わない。

(5) 要保護情報の取扱い

(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、要保護情報を要管理対策区域外に持ち出さないこと。

解説：情報の漏えい、改ざん、破損、紛失等を未然に防ぐため、事務従事者が高等教育機関の事務の遂行以外の目的で要保護情報を要管理対策区域外へ持ち出すことを禁止する事項である。なお、これを徹底させる手段として、「持出禁止」の取扱制限の明示等が挙げられる。

(b) 事務従事者は、要保護情報を放置しないこと。

解説：第三者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ーを起動するあるいはログオフして、画面に情報を表示しないこと、また、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。

(c) 事務従事者は、機密性３情報を必要以上に複製しないこと。

解説：不必要な複製によって情報漏えいの危険性が高くなることを考慮し、必要以上に機密性３情報を複製しないことを求める事項である。なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ）第 6 項では、「「極秘」の文書の複製は、絶対に行なわないこと。「秘」の文書は、指定者の承認をうけて複製することができること。」と定めている。なお、これを徹底させる手段として、「複製禁止」の取扱制限の明示等が挙げられる。

(d) 事務従事者は、要機密情報を必要以上に配付しないこと。

解説：情報漏えいを未然に防ぐため、要機密情報の配付は最小限にとどめることを求める事項である。なお、これを徹底させる手段として、「配付禁止」の取扱制限の明示等が挙げられる。

(e) 事務従事者は、情報を機密性３情報と決定した場合には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付を下げる又は取扱制限を緩和する必要性があると思料される場合には、格付及び取扱制限の見直しに必要な処理を行うこと。

解説：秘密としての管理を求められる期間を明記することにより、必要以上の秘密管理を防止するための事項である。なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ）第 5 項では、「秘密文書には、秘密にしておく期間を明記し、その期間が経過した時は、秘密の取扱いは、解除されたものとする。ただし、その期間中秘密にする必要がなくなったときは、その旨を通知して秘密の解除を行うものとすること。」と定めている。

(f) 事務従事者は、情報を機密性３情報と決定した書面のうち、必要なものには、一連番号を付し、その所在を明らかにしておくこと。

解説：機密性３情報である書面に一連番号を付与し、個別に所在管理を行うことを求める事項である。配付時に一連番号を付与することによって、当該機密性３情報を受領した者に、一定の管理義務を要請する効果も期待できる。なお、「秘密文書等の取扱いについて」（昭和 40.4.15 事務次官等会議申合せ）第 4 項では、「「極秘」の文書には、必ず一連番号を付し、その所在を明らかにしておくこと。」と定めている。

1.3.1.3 情報の保存

趣旨（必要性）

高等教育機関の事務においては、その事務の継続性を確保する等の必要性から情報を保存する場合があるが、情報の保存を続ける限り、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれも継続する。これらのことを勘案し、本項では、情報の保存に関する対策

基準として、格付に応じた情報の保存及び保存期間における取扱い又は保存期間満了後の取扱期間についての遵守事項を定める。

遵守事項

(1) 格付に応じた情報の保存

(a) 事務従事者は、情報の格付及び取扱制限に応じて、情報を適切に保存すること。

解説：電磁的記録媒体に保存された情報、書面に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、適切に保存することを求める事項である。例えば、事務従事者が書面を保存する場合は、要管理対策区域内の棚に保存したり、必要なく情報の参照等をさせないために、施錠のできる書庫・保管庫に保存すること等が考えられる。ここで、外部電磁的記録媒体に情報を保存する場合は、主体認証情報（パスワード）によるロック機能を利用して、当該媒体の利用を防止することが可能であるが、ロック機能を持たない外部電磁的記録媒体も多く、保存する情報に応じた外部電磁的記録媒体を選択する必要がある。一方、事務従事者が要保護情報に関する情報処理を行う場合は、例えば、要管理対策区域内に設置された情報システム上に保存すること等が考えられる。また、事務従事者が許可を得て、個人で利用するASP・SaaS サービスの外部の情報システムを用いて、要保護情報に関する情報処理を行う場合は、本基準と同等の情報セキュリティ対策が実施される場所に保存する必要がある。なお、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切とな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。

(b) 事務従事者は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うこと。

解説：電磁的記録媒体に保存された情報に関して、機密性、完全性及び可用性の格付及び取扱制限に応じ、必要のない者に情報へアクセスさせないためのアクセス制御を可能な範囲で実施することを求める事項である。電磁的記録媒体に保存された情報には電子計算機等を利用してアクセスすることになるため、アクセス制御は、電子計算機、オペレーティングシステム、アプリケーション及びファイル等を単位として行うことができ、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。情報システムに事務従事者自らがアクセス制御設定を行う機能が装備されている場合には、事務従事者は、当該情報の格付及び取扱制限の指示内容に従って、必要なアクセス制御の設定を行うこと。例えば、要機密情報であれば、不適当な者から参照されないよう、読取制限の属性を付与し、完全性２情報であれば、不適当な者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。例えば、上書き禁止の属性を付与する方法としては、ファイルに対する書込権限者の制限、又はファイルのセキュリティ設定でパスワード設定した上での読取専用の設定等がある。ただし、複製禁止の取扱制限がされていたとしても、情報システムに複製禁止とする機能がなければ、そのアクセス制御の設定をすることはできない。その場合には、情報システムが備えていない機能については、事務従事者が取扱上注意することで、その指示を遵守することになる。

(c) 事務従事者は、要機密情報を電磁的記録媒体に保存する場合には、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、情報にパスワードを設定すること。

解説：電磁的記録媒体に保存された情報の機密性を確保するために、要機密情報を容易に参照できないようにするため、パスワードによって保護することを求める事項である。方法としては、文書作成アプリケーションによるパスワード保護オプション、圧縮・解凍ソフトによるパスワード保護オプションの利用等が挙げられる。なお、パスワードは、適切な文字列の長さ及び複雑さを持つように設定する必要がある。

(d) 事務従事者は、要機密情報を電磁的記録媒体に保存する場合には、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。

解説：電磁的記録媒体に保存された情報の機密性を確保するために、その暗号化を行うことを求める事項である。暗号化を行うと情報の復号ができる者を限定することとなり、学内において情報の機密性を高めるために有効である。また、万一 PC、光ディスク、USB メモリ等の紛失・盗難が発生しても、暗号が解読されない限り、情報の漏えいは防ぐことができる。情報を暗号化する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。

(e) 事務従事者は、要保全情報を電磁的記録媒体に保存する場合には、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は、情報に電子署名を付与すること。

解説：要保全情報を電磁的記録媒体に保存する場合、その改ざんのおそれを勘案し、必要に応じて電子署名を付与することを求める事項である。情報に電子署名を付与する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。

(f) 事務従事者は、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、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。

解説：情報のバックアップ又は複写の取得を求める事項である。バックアップは、その取得頻度が復元の手順及び所要時間に関係することも考慮して、頻度を定める。障害・事故等に備えて適切な頻度で復元の演習も行い、事務従事者に習熟させる。なお、バックアップした記録媒体の紛失・盗難により情報が漏えいするおそれがあるため、必要に応じて、その情報を暗号化することが望ましい。

(g) 事務従事者は、要保全情報若しくは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複写の保管について、災害等により生ずる支障の有無を検討し、支障があると認めたときは、適切な措置を講ずること。

解説：バックアップ又は複写の適切な保管を求める事項である。例えば、バックアップ又は複写を防火金庫に保管することや、同時被災に備えて遠隔地に保管すること等が考えられる。

(2) 情報の保存期間

(a) 事務従事者は、電磁的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し、保存期間を延長する必要性がない場合は、速やかに消去すること。

解説：電磁的記録媒体に保存された情報に関して、情報セキュリティ確保の観点から保存期間を定めている場合に、当該保存期間に従って管理することを求める事項である。事務従事者は、情報セキュリティ上、必要な期間は確実に情報を保存するとともに、その期間を経過した場合には当該情報を速やかに消去してリスクの増大を回避する必要がある。また、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等して移管するものとする。その際、本事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準における遵守事項に従いつつ、例えば、事務従事者でパスワードを設定していた場合は、解除する等して移管先がその内容を参照できるように配慮すること。

1.3.1.4 情報の移送

趣旨（必要性）

高等教育機関の事務においては、その事務の遂行のために他者又は自身に情報を移送する場合がある。移送の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部電磁的記録媒体及び PC の運搬、書面の運搬等の方法が挙げられるが、いずれの方法を用いるにせよ、情報の移送により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになる。

これらのことを勘案し、本項では、情報の移送に関する対策基準として、情報の移送に関する許可及び届出、情報の送信と運搬の選択、移送手段の決定、記録媒体及び電磁的記録の保護対策についての遵守事項を定める。

遵守事項

(1) 情報の移送に関する許可及び届出

(a) 事務従事者は、機密性３情報、完全性２情報又は可用性２情報を移送する場合には、職場情報セキュリティ責任者の許可を得ること。

解説：機密性３情報、完全性２情報又は可用性２情報を移送する際に職場情報セキュリティ責任者の許可を求める事項である。なお、機密性３情報、完全性２情報又は可用性２情報を定常的に移送する必要がある場合には、送信又は運搬の別、移送手段、情報の保護対策に関して、手続を定めておくことが望ましい。

(b) 事務従事者は、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情報である書面を移送する場合には、職場情報セキュリティ責任者に届け出ること。ただし、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

解説：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情報である書面を移送する際に職場情報セキュリティ責任者に届け出ることを求める事項である。なお、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情報である書面を定常的に移送する必要がある場合には、送信又は運搬の別、移送手段、情報の保護対策に関して、手続を定めておくことが

望ましい。また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(2) 情報の送信と運搬の選択

(a) 事務従事者は、要保護情報である電磁的記録を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを選択し、職場情報セキュリティ責任者に届け出ること。ただし、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の移送であり、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

解説：要保護情報の安全確保に留意した移送を求める事項である。届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(3) 移送手段の決定

(a) 事務従事者は、要保護情報を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、職場情報セキュリティ責任者に届け出ること。ただし、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情報である書面の移送であり、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。

解説：多種多様な移送手段の中から要保護情報を安全に移送するための手段の選択を求める事項である。「移送手段」とは、送信については学内通信回線、信頼できるプロバイダ、 VPN 及び暗号メール(S/MIME)等、運搬については信頼できる運送業者や、部局総括責任者が指定する運送役務及び事務従事者自らによる携行等が挙げられる。なお、「S/MIME（Secure Multipurpose Internet Mail Extensions）」とは、電子メールの暗号化の方式の１つである。また、届出を必要としない移送を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(4) 記録媒体の保護対策

(a) 事務従事者は、要機密情報が記録又は記載された記録媒体を運搬する場合には、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。

解説：要機密情報が記録又は記載された記録媒体を運搬する場合における情報セキュリティ対策を求める事項である。事務従事者は、外部電磁的記録媒体、 PC、書面等を運搬する場合には、例えば、外見ではその内容が要機密情報であると知られないこと、送付先において適切な取扱いがなされるように二重封筒とすること、「親展」の指定を行うこと、専用ケースに保存して施錠すること等、安全確保のための適切な措置を講ずる必要がある。

(5) 電磁的記録の保護対策

(a) 事務従事者は、要機密情報である電磁的記録を移送する場合には、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、情報にパスワードを設定すること。

解説：移送手段の種別を問わず、受取手以外の者が要機密情報を容易に参照できないようにするため、パスワードによって保護することを求める事項である。方法としては、文書作成アプリケーションによるパスワード保護オプション及び圧縮・解凍ソフト

によるパスワード保護オプションの利用等が挙げられる。なお、パスワードは、適切な文字列の長さ及び複雑さを持つように設定する必要がある。

(b) 事務従事者は、要機密情報である電磁的記録を移送する場合には、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。

解説：要機密情報を移送する場合、その漏えいに係るリスクを勘案し、必要に応じて暗号化することを求める事項である。情報を暗号化する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。

(c) 事務従事者は、要保全情報である電磁的記録を移送する場合には、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は、情報に電子署名を付与すること。

解説：要保全情報を移送する場合、必要に応じて電子署名の付与を行うことを求める事項である。情報に電子署名を付与する際は、1.5.2.4 暗号と電子署名の標準手順の定めに従うこと。

(d) 事務従事者は、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ときは、情報のバックアップを取得すること。

解説：要保全情報を移送する場合、必要に応じてバックアップを取得することを求める事項である。

(e) 事務従事者は、要安定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等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。

解説：要安定情報を移送する場合、必要に応じて所要の措置を講ずることを求める事項である。

(f) 事務従事者は、電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いる必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：情報を分割し、これを異なる経路で移送することを求める事項である。要機密情報を移送する場合には、当該要機密情報が情報量的に解読不能となるように、分割して移送を行うこと。この考え方は、専門用語で秘密分散技術といわれ、例えば、1個の電子情報についてファイルを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 CD-R、DVD、MO、USB メモリ、フラッシュメモリ等の外部電磁的記録媒体で郵送する方法が挙げられる。

1.3.1.5 情報の提供

趣旨（必要性）

高等教育機関の事務においては、その事務の遂行のために学外の者に情報を提供する場合があるが、提供先における情報の不適切な取扱いにより、当該情報の漏えい又は不適切な利用等が発生するおそれがある。これらのことを勘案し、本項では、情報の提供に関する対策基準

として、情報の公表及び他者への情報の提供についての遵守事項を定める。

遵守事項

(1) 情報の公表

(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。

解説：公表すべきでない情報の公表を防止することを求める事項である。本学の業務においては、保有する情報をウェブサイト等により広く本学外の人々に提供する場合がある。この場合には、公表しようとする情報に対する格付の適正さを再度検討し、必要に応じて格付の変更等を行った上で、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必要がある。なお、情報セキュリティ関係規程の定めによらず、当該情報が法律の規定等で公表が禁じられたものでないことは別途確認する必要がある。

(b) 事務従事者は、電磁的記録を公表する場合には、当該情報の付加情報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：事務従事者が意図せず情報を漏えいすることを防止するための事項である。例えば、公開する文書ファイルの作成者名、組織名その他の記録に使用できる「プロパティ」と呼ぶ部分に個人情報が残っている又は文書に作成履歴が残っていることがないように除去することが考えられる。また、電子ファイル上でアプリケーションの機能を用いて特定の部分の情報を黒塗りしたとしても、当該部分の情報の閲覧が可能となる場合があることに留意し、黒塗りされた部分の情報そのものの削除や置換えを行うことも検討する必要がある。

(2) 他者への情報の提供

(a) 事務従事者は、機密性３情報、完全性２情報又は可用性２情報を学外の者に提供する場合には、職場情報セキュリティ責任者の許可を得ること。

解説：機密性３情報、完全性２情報又は可用性２情報を学外の者に提供する際に職場情報セキュリティ責任者の許可を得ることを求める事項である。

(b) 事務従事者は、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情報である書面を学外の者に提供する場合には、職場情報セキュリティ責任者に届け出ること。ただし、職場情報セキュリティ責任者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。

解説：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情報である書面を学外の者に提供する際に職場情報セキュリティ責任者に届け出ることを求める事項である。届出を必要としない提供を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(c) 事務従事者は、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、当該情報に付された情報の格付及び取扱制限に応じて適切に取り扱われるための措置を講ずること。

解説：要保護情報を学外の者に提供する場合において遵守すべきことを定める事項である。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、情報の格付及び取扱制限の取扱上の留意事項を提供先へ確実に伝達し、必要に応じ、提供先における当該情報の適切な管理のために必要な措置及び情報の利用目的を協議の上、決定する必要がある。
確実に伝達する方法として、提供先が事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準に準じた組織の場合には、事務情報セキュリティ管理基準及び事務情報セキュリティ技術基準による情報の格付及び取扱制限を用いて示す方法が考えられる。それ以外の場合には、格付の区分だけを示すのでは不十分である。なぜなら、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が認識できないからである。格付の区分（例えば、「機密性２」と記載する）で示すのであれば、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か、格付の区分で示す以外の方法としては、提供する情報にそれを適切に管理するために必要な措置が具体的にわかるように示す（例えば、「委員以外への再配布を禁止する」と記載する）等をする必要がある。また、提供した情報が提供先の別の者によって取り扱われる際にも、それが適切に取り扱われることを確実にするため、必要な措置について口頭による伝達ではなく記載する等の方法によって伝達する必要がある。
事務従事者は、格付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及び取扱制限に従っ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。

(d) 事務従事者は、電磁的記録を提供する場合には、当該記録の付加情報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：事務従事者が意図せず情報を漏えいすることを防止するための事項である。例えば、提供する文書ファイルの作成者名、組織名その他の記録に使用できる「プロパティ」と呼ぶ部分に個人情報が残っている又は文書に作成履歴が残っていることがないように除去することが考えられる。

1.3.1.6 情報の消去

趣旨（必要性）

高等教育機関の事務において利用した電子計算機、通信回線装置及び外部電磁的記録媒体については、不要となった後、適切に処分されずに放置された場合には、盗難や紛失により、記録されている情報が漏えいするおそれがある。また、情報を消去する際に、適切な措置が講じられていなければ、復元ツールや復元サービス等を用いて当該情報を復元することが可能であり、情報漏えいのおそれは払拭されない。

これらのことを勘案し、本項では、情報の消去に関する対策基準として、電磁的記録の消去方法及び書面の廃棄方法についての遵守事項を定める。

遵守事項

(1) 電磁的記録の消去方法

(a) 事務従事者は、電磁的記録媒体を廃棄する場合には、全ての情報を抹消すること。

解説：電磁的記録媒体を廃棄する場合に、全ての情報を復元が困難な状態にすることを求める事項である。「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。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、内蔵電磁的記録媒体及び外部電磁的記録媒体に記録されている全ての情報を適切な方法で復元が困難な状態にする必要がある。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）によりファイルを個々に抹消する方法

・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

なお、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。

・FD 等の磁気媒体の場合には、当該媒体を折り曲げる、切断する等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方法

(b) 事務従事者は、電磁的記録媒体を他の者へ提供する場合には、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：電磁的記録媒体に保存された不要な情報を抹消することを求める事項である。長期にわたり利用された内蔵電磁的記録媒体及び外部電磁的記録媒体には、要機密情報が断片的に残留した状態となっているおそれがある。そのため、電磁的記録媒体を用いて学外の者に情報を提供する場合や、担当者間による業務の引継ぎを伴わず、別の業務に機器等を引き継ぐことが想定される場合には、データを抹消する必要がある。

(c) 事務従事者は、電磁的記録媒体について、設置環境等から要機密情報を抹消する必要性の有無を検討し、必要と認めたときは、当該電磁的記録媒体の要機密情報を抹消すること。

解説：無人の執務室に設置されていたり、設置場所及び利用場所が確定していない電子計算機、通信回線装置及び外部電磁的記録媒体等、安全といえない環境で利用される電子計算機等に要機密情報を残留させないことを求める事項である。事務従事者は、要機密情報が保存された電子ファイル又は空き領域に残留する情報を抹消すること。

(2) 書面の廃棄方法

(a) 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。

解説：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、焼却又は溶解等により、復元が困難な状態にすることを求める事項である。なお、廃棄すべき書類が大量である等の理由により、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。

第 1.4 部　情報処理についての対策

1.4.1 情報システムの利用

1.4.1.1 情報システムの利用

趣旨（必要性）

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。これらのことを勘案し、識別コード及び主体認証情報の管理等に関する対策基準として、識別コードと主体認証情報の管理及び付与管理、代替手段等の適用についての遵守事項を定める。

なお、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する判断基準を、事務情報セキュリティ技術基準 2.2.1.1~2.2.1.5 においても各機能の導入等に関する対策基準を定めている。

遵守事項

(1) 識別コードの管理

(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。

解説：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、なりすまし行為であることを認識する必要がある。仮に、悪意がない行為であっても、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、安易に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利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使って行おうとしている業務について、他者へ代行処理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、当該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用いて、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。また、業務の継続のために、他者の識別コードを用いることが不可避の場合には、例外措置の承認を行う際に本人の事前の了解に加えて、部局技術担当者の了解を得ることが最低限必要である。極めて緊急性が高い場合には、他者の識別コードを利用していた期間とアクセスの内容を、事後速やかに、部局技術担当者に報告しなければならない。部局技術担当者は、その理由と利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のが望ましい。

いずれの場合も、用い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

別コードを用いて、情報システムを利用することは禁止されるべきである。
遵守事項に「主体認証の際に」とあるのは、主体認証以外の目的で他者の識別コードを使用することを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、電子メール送信先のアドレスとして他者の識別コードを指定してメール送信のための情報システムを利用することについては問題がない。

(b) 事務従事者は、自己に付与された識別コードを他者が主体認証に用いるために付与及び貸与しないこと。

解説：共用する識別コードについても部局技術担当者から各本人に個別に付与されるものであり、付与された者がそれを他者に付与、貸与してはならない。また、部局技術担当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。遵守事項に「主体認証に用いるために」とあるのは、主体認証に用いる目的以外で他者に知らせることを除くためである。例えば、識別コードとして電子メールアドレスが使用されている場合に、自分宛の電子メールアドレスとして知らせることについては問題がない。

(c) 事務従事者は、自己に付与された識別コードを、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。

解説：ほとんどの場合には、識別コード自体は必ずしも秘密ではないが、積極的に公開したり、公然となるような放置はしないようにすることを求める事項である。本来、主体認証のためには、主体認証情報が用いられるが、識別コード自体も秘密にすることによって、不正に主体認証される可能性をより低くすることが可能となる。そのため、識別コードについても適切に管理することが求められる。

(d) 事務従事者は、高等教育機関の事務のために識別コードを利用する必要がなくなった場合は、その旨を部局技術担当者に届け出ること。ただし、個別の届出が必要ないと、部局技術責任者が定めている場合は、この限りでない。

解説：識別コードを利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担当者へ届け出ることを求める事項である。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担当者が事務従事者自らからの届出によらずして把握できる場合等、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良い。

(e) 部局技術責任者は、管理者権限を持つ識別コードを付与された事務従事者に、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させる必要性の有無を検討し、必要と認めたときは、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させること。

解説：事務従事者に、管理者権限を持つ識別コードを管理者としての業務遂行時に限定して、利用させることを求める事項である。
なお、本遵守事項は、実際には事務従事者が繁雑な操作を必要とする場合があるため、最少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、当該情報システムで取り扱う情報の重要性等を勘案し、必要に応じて選択されたい。

(f) 事務従事者は、管理者権限を持つ識別コードを付与され、かつ部局技術責任者が求めた場合には、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。

解説：管理者権限を持つ識別コード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ティングシステムが Windows であれば、administrator 権限を付与された場合であって、PC の設定変更等をしないときには、administrator 権限なしの識別コードを使用し、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。

(2) 主体認証情報の管理

(a) 事務従事者は、主体認証情報が他者に使用され、又はその危険が発生した場合には、直ちに部局技術責任者又は部局技術担当者にその旨を報告すること。

解説：事務従事者は、自らの主体認証情報自体の露呈や主体認証情報に関連する情報の露呈又はそれらが露呈した可能性がある場合には、直ちに部局技術責任者又は部局技術担当者へ報告することを求める事項である。

(b) 部局技術責任者又は部局技術担当者は、主体認証情報が他者に使用され、又はその危険が発生したことを知った場合には、必要な措置を講ずること。

解説：自らが発見したり、報告を受けたりして、主体認証情報の他者使用又は危険発生を知った部局技術責任者又は部局技術担当者が、必要な措置を講ずることを求める事項である。必要な対策としては、例えば、主体認証情報の変更や別の主体認証方式の併用、当該識別コードによるログオン制限等がある。

(c) 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。

(ア) 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こと。

解説：事務従事者は、例えば自己の主体認証情報を内容が分かる状態で付箋に記入して貼付するようなことを行ってはならず、主体認証情報を入力する際に周囲からの盗み見に注意を払ったり、管理者を名乗って主体認証情報を聞き出す行為に注意したりする等、他者に知られないように管理すること。
また、主体認証情報を、容易に他者に知られてしまう状態で、主体認証を行う情報システムとは異なる情報システムに記憶させないこと。

(イ) 自己の主体認証情報を他者に教えないこと。

解説：事務従事者が他者に処理代行させるために自己の主体認証情報を教示しないことを求める事項である。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連があいまいとなる可能性があり、アクセス制御、権限管理、証跡管理その他のセキュリティ対策の基礎が崩壊する可能性がある。また、教示された側にとっても、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。

(ウ) 主体認証情報を忘却しないように努めること。

解説：他者が容易に見ることができないような措置（施錠して保存する等）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、メモを取ることそのものを禁ずるものではない。むしろ、忘れることのないようにもしなければならない。

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）する場合に備えて、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。

(エ) 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こと。

解説：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、更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。

(オ) 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こと。

解説：事務従事者が付与された複数の識別コードで共通の主体認証情報を用いていると、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ため、共通の主体認証情報を用いないことを求める事項である。複数の識別コードの権限レベルが異なっていたり、複数の識別コードを用いる情報システムのセキュリティレベルが異なっていたりする場合、低いレベルの主体認証情報の漏えいにより、高いレベルの権限や高いセキュリティレベルの情報システムが正規の主体認証方式を用いて容易に不正アクセスされないようにすることを求めている。対象となる識別コードには、本学支給の情報システムだけでなく、本学支給以外の情報システムで使用している識別コードも含める必要がある。

なお、シングルサインオンシステム等、一組の識別コード及び主体認証情報を用いて複数のシステムの利用を可能とするシステムは、当該複数システム間のそれぞれの主体認証情報が異なっていれば、本項目が想定する脅威は存在しないため、共通の主体認証情報を用いたことにはならない。

(カ) 部局技術担当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こと。

解説：定期的な変更の要求を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等の運用によって対処することでも差し支えない。

なお、例えば、主体認証やその後の情報システムにおける処理を自動的に行うと、定期的な変更の際に、それらの処理をその都度修正する必要があることに注意すること。

(d) 事務従事者は、所有による主体認証を用いる場合には、以下の管理を徹底すること。

(ア) 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こと。

(イ) 主体認証情報格納装置を他者に付与及び貸与しないこと。

(ウ) 主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに部局技術責任者又は部局技術担当者にその旨を報告すること。

(エ) 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

又は部局技術担当者に返還すること。

解説：所有による主体認証方式では、それを取得した者が正当な主体として主体認証されることになるため、他者に使用されることがないように、また、紛失等で、その可能性がある場合の報告を徹底する必要がある。異動等により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、これを返却する必要がある。

(e) 部局技術責任者は、主体認証のために取得した情報を本人から事前に同意を得た目的以外の目的で使用しないこと。

解説：利用者の指紋情報等、主体認証情報として生体情報を取り扱う場合には、個人のプライバシーに配慮し、個人情報として厳格な管理が求められる。管理方法としては、元の生体情報が再現できないように保存すること等が考えられる。

(3) 識別コードと主体認証情報の付与管理

(a) 部局技術責任者は、権限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、利用状況等を考慮して、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。

(b) 部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、以下の事項を含む手続を定めること。

(ア) 主体からの申請に基づいて権限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

(イ) 主体認証情報の初期配布方法及び変更管理手続

(ウ) アクセス制御情報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、確実にアクセス権を設定するため、関連手続を明確に定めることを求める事項である。

(c) 部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。

解説：権限の管理については、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、権限管理を行う者を定める事項である。

(4) 識別コードと主体認証情報における代替手段等の適用

(a) 部局技術担当者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった事務従事者から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。

解説：情報システムを利用する事務従事者においては、何らかの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合が想定される。例えば、知識による主体認証方式であれば主体認証情報（パスワード）を忘れた場合、所有による主体認証方式であれば携帯するのを忘れた場合、指紋による主体認

証方式であれば指を怪我した場合等が挙げられる。
それらの理由により、付与された識別コードに対する主体認証情報を提示することが困難である場合には、代替手段の使用に関する許可申請をすることができる。部局技術担当者は、その申請を受理した時には、その申請が正当な利用者からの許可申請であること及び許可申請の理由が妥当であること等を確認した上で、その必要性を判断し代替手段を提供することを求める事項である。なお、代替手段としては、例えば、当日限り有効とした暫定的な識別コード及び主体認証情報の提供や、当該情報システムから切り離された代替 PC の提供、情報システムを利用しない業務環境の提供等が想定されるが、部局技術担当者が情報セキュリティ保護の観点に加えて事務従事者本人による業務執行の緊急性、効率性、利便性及び当該情報システムの可用性等も考慮して、適正な代替手段を準備しておくこと。
なお、代替手段の提供に当たっては、その申請理由と使用期間、使用者等を記録として残すことが望ましい。

(b) 部局技術責任者及び部局技術担当者は、権限管理を行う必要があると認めた情報システムにおいて、識別コードの不正使用を知った場合には、直ちに当該識別コードによる使用を停止させること。

解説：自らが発見したり、報告を受けたりして、識別コードの不正使用を知った場合には、他の項目で定められている障害・事故等の対処に係る遵守事項とともに、本遵守事項の対処を実施する。なお、不正使用による被害が甚大であると予想される場合には、例えば、全ての使用を停止した上で、状況把握、原因特定及び証拠保全のためにバックアップを取得することが望ましい。その後、不正使用に対する対策を講じた上で、使用を再開する場合には、改めて主体認証情報を再発行することが望ましい。

1.4.2 情報処理の制限

1.4.2.1 要管理対策区域外での情報処理の制限

趣旨（必要性）

高等教育機関の事務においては、その事務の遂行のため、要管理対策区域外において情報処理を実施する必要が生ずる場合がある。この際、要管理対策区域外での実施では物理的な安全対策を講ずることが比較的困難になることから、事務従事者は、要管理対策区域内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。

これらのことを勘案し、本項では、要管理対策区域外での情報処理の制限に関する対策基準として、安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項を定める。

遵守事項

(1) 安全管理措置についての規定の整備

(a) 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の情報処理を行う場合の安全管理措置についての規定を整備すること。

解説：全学実施責任者が、要管理対策区域外において情報処理を行う場合の安全管理措置についての規定を整備することを求める事項である。ただし、情報処理の種類により個別の規定を設けても構わない。要管理対策区域外において情報処理を行う場合を具体的に想定し、情報処理の内容と取り扱う情報、実施場所、回線を通した通信の形態、関与する学内外の者等に応じた措置を示した規定を整備する必要がある。

(b) 全学実施責任者は、要保護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の安全管理措置についての規定を整備すること。

解説：全学実施責任者が、要管理対策区域外に要保護情報を取り扱う情報システムを持ち出す場合の安全管理措置についての規定を整備することを求める事項である。持ち出す情報システム及び持ち出し先等を具体的に想定して規定を整備する必要がある。

(2) 許可及び届出の取得及び管理

(a) 事務従事者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外で情報処理を行う場合には、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。

解説：機密性３情報、完全性２情報又は可用性２情報に係る情報処理を要管理対策区域外で行う場合に、部局技術責任者と職場情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については職場情報セキュリティ責任者の、当該情報処理の安全性については部局技術責任者の許可を得ることとなる。

なお、「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

(b) 事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外で情報処理を行う場合には、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。

解説：要管理対策区域外で機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、部局技術責任者と職場情報セキュリティ責任者の両方に届け出ることを求める事項である。また、部局技術責任者又は職場情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない要管理対策区域外での情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(c) 部局技術責任者及び職場情報セキュリティ責任者は、要管理対策区域外での要保護情報の情報処理に係る記録を取得すること。

解説：要管理対策区域外での要保護情報の情報処理に係る記録を取得することを求める事項である。

「情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

(d) 部局技術責任者及び職場情報セキュリティ責任者は、機密性３情報、完全性２情報又

は可用性２情報について要管理対策区域外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：要管理対策区域外での情報処理を行うことを許可した期間が終了した時に報告の有無を確認し、措置を講ずること等を求める事項である。状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、事務従事者に改めて許可を得るようにさせること。

(e) 部局技術責任者及び職場情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

解説：機密性２情報であって完全性１情報かつ可用性１情報である情報について要管理対策区域外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、期間の延長が必要な状況であれば事務従事者に改めて届出をさせる等の措置を講ずることを求める事項である。

(f) 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には、業務の遂行に必要最小限の情報処理にとどめること。

解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を要管理対策区域外で情報処理することを最小限にとどめることを求める事項である。

(g) 事務従事者は、機密性３情報、完全性２情報又は可用性２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、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。

解説：機密性３情報、完全性２情報又は可用性２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事務従事者に、部局技術責任者と職場情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該持ち出しの業務上の必要性については職場情報セキュリティ責任者の、当該持ち出しの安全性については部局技術責任者の許可を得ることとなる。

(h) 事務従事者は、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、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。

解説：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事務従事者に、部局技術責任者と職場情報セキュリティ責任者の両方に届け出ることを求める事項である。また、部局技術責任者又は職場情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない要管理対策区域外への持ち出しを定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(i) 部局技術責任者及び職場情報セキュリティ責任者は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しに係る記録を取得すること。

解説：要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しに係る記録を取得することを求める事項である。「持ち出しに係る記録」には、持ち出しの実施者、端末、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

(j) 部局技術責任者及び職場情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２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ことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：情報システムを要管理対策区域外に持ち出すことを許可した期間が終了した時に報告の有無を確認すること等を求める事項である。

状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告をさせる。期間の延長が必要な状況であれば、事務従事者に改めて許可を得るようにさせること。

(k) 部局技術責任者及び職場情報セキュリティ責任者は、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ことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

解説：届出期間が長期にわたる場合等、必要に応じて、要管理対策区域外への持ち出しの状況を確認することを求める事項である。状況を確認した際に、期間の延長が必要な状況であれば、事務従事者に改めて届出をさせること。

(l) 事務従事者は、要保護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、業務の遂行に必要最小限の情報システムの持ち出しにとどめること。

解説：情報セキュリティの侵害のおそれを低減するために、要保護情報を取り扱うシステムを要管理対策区域外に持ち出すことを最小限にとどめることを求める事項である。

(3) 安全管理措置の遵守

(a) 事務従事者は、要保護情報について要管理対策区域外での情報処理について定められた安全管理措置を講ずること。

解説：事務従事者に対して、要管理対策区域外での情報処理について定められた安全管理措置を講ずることを求める事項である。

(b) 事務従事者は、機密性３情報、完全性２情報又は可用性２情報について要管理対策区域外での情報処理を行うことを終了した時に、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。

解説：事務従事者に対して、要管理対策区域外での情報処理が終了したことを、その許可を与えた者に報告することを求める事項である。

(c) 事務従事者は、要保護情報を取り扱う情報システムの要管理対策区域外への持ち出しについて定められた安全管理措置を講ずること。

解説：事務従事者に対して、情報システムの要管理対策区域外への持ち出しについて定められた安全管理措置を講ずることを求める事項である。定められた安全管理措置の

内容としては、例えば、盗難及び亡失の防止に十分に注意すること、操作や画面の盗み見を防止するために、スクリーンに覗き見防止フィルターを貼ることや、スクリーンセーバーの機能を利用し、操作を実施できなくすること等が考えられる。

(d) 事務従事者は、機密性３情報、完全性２情報又は可用性２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ことを終了した時に、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。

解説：事務従事者に対して、要管理対策区域外へ情報システムの持ち出しが終了したことを、その許可を与えた者に報告することを求める事項である。

1.4.2.2 本学支給以外の情報システムによる情報処理の制限

趣旨（必要性）

高等教育機関の事務においては、その遂行のため、本学支給以外の情報システムを利用する必要が生じる場合がある。この際、当該情報システムが、本学が支給したものでないという理由で対策を講じなかった場合、当該情報システムで取り扱われる情報のセキュリティは確保できない。

これらのことを勘案し、本項では、本学支給以外の情報システムによる情報処理の制限に関する対策基準として、安全管理措置についての規定の整備、許可及び届出の取得及び管理、安全管理措置の遵守についての遵守事項を定める。

遵守事項

(1) 安全管理措置についての規定の整備

(a) 全学実施責任者は、要保護情報について本学支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備すること。

解説：事務従事者が所有する個人の PC 等を用いて要保護情報に関する情報処理を行う場合であっても、本学支給の情報システムと同程度のセキュリティ対策を施す必要があるため、その安全管理措置についての規定を整備することを求める事項である。ただし、情報システムの種類により個別の規定を設けても構わない。

(2) 許可及び届出の取得及び管理

(a) 事務従事者は、機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムにより情報処理を行う必要がある場合には、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。

解説：機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムにより情報処理を行う必要がある場合に、部局技術責任者と職場情報セキュリティ責任者の両方の許可を得ることを求める事項である。当該情報処理の業務上の必要性については職場情報セキュリティ責任者の、当該情報処理の安全性については部局技術責任者の許可を得ることとなる。

本学支給以外の情報システムによる機密性３情報、完全性２情報又は可用性２情報の情報処理を許可する場合は、その期間については、最長で１年間にすることが望

ましい。ただし、期間の延長が必要な状況であれば、事務従事者に改めて許可を得るようにさせること。

(b) 事務従事者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について本学支給以外の情報システムにより情報処理を行う必要がある場合には、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。

解説：本学支給以外の情報システムによる機密性２情報であって完全性１情報かつ可用性１情報である情報の情報処理を行う場合に、部局技術責任者と職場情報セキュリティ責任者の両方に届け出ることを求める事項である。また、部局技術責任者又は職場情報セキュリティ責任者が、各々の責任の範囲において届出を必要としない本学支給以外の情報システムによる情報処理を定める際には、届出をしないことにより発生するリスクを充分に検討する必要がある。

(c) 部局技術責任者及び職場情報セキュリティ責任者は、本学支給以外の情報システムによる要保護情報の情報処理に係る記録を取得すること。

解説：本学支給以外の情報システムによる要保護情報の情報処理に係る記録を取得することを求める事項である。「本学支給以外の情報システムによる情報処理に係る記録」には、情報処理の実施者、内容、期間及び理由並びに許可事案の場合の終了時の報告の有無等を含めることが考えられる。

(d) 部局技術責任者及び職場情報セキュリティ責任者は、機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

解説：本学支給外の情報システムによる情報処理を行うことを許可した期間が終了した時に、報告の有無を確認すること等を求める事項である。

状況を確認した際に、終了の報告をしていない理由が報告漏れである場合には、報告させる。期間の延長が必要な状況であれば、事務従事者に改めて許可を得るようにさせること。

(e) 部局技術責任者及び職場情報セキュリティ責任者は、機密性２情報であって完全性１情報かつ可用性１情報である情報について本学支給以外の情報システムによる情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。

解説：届出期間が長期にわたる場合等、必要に応じて、本学支給以外の情報システムによる情報処理の状況を確認することを求める事項である。状況を確認した際に、期間の延長が必要な状況であれば、事務従事者に改めて届出をさせること。

(3) 安全管理措置の遵守

(a) 事務従事者は、要保護情報について本学支給以外の情報システムによる情報処理を行う場合には、当該情報システムについて定められた安全管理措置を講ずること。

解説：事務従事者が所有する個人の PC 等、本学支給以外の情報システムを用いて要保護情報に関する情報処理を行う場合であっても、本学支給の情報システムと同程度の

セキュリティ対策を施す必要があるため、事務従事者に安全管理措置を講ずることを求める事項である。

(b) 事務従事者は、機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムによる情報処理を終了した時に、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。

解説：事務従事者が機密性３情報、完全性２情報又は可用性２情報について本学支給以外の情報システムによる情報処理を終了した時に、その報告を求める事項である。

本学支給以外の情報システムの利用許可を与えた者は、その終了報告を受け、本学支給以外の情報システムによる情報処理の状況を把握することが可能となる。その結果、本学支給以外の情報システムを、本来必要とされる期間を超えて利用している場合には、これを検知し、利用実態を是正することが可能となる。

(c) 部局技術責任者は、要保護情報を取り扱う本学支給以外の情報システムについて、定められた安全管理措置が適切に講じられていることを定期的に確認すること。

解説：部局技術責任者に対して、許可又は届出を受理した要保護情報を取り扱う本学支給以外の情報システムについて、本学支給の情報システムと同程度のセキュリティ対策が施されていることの確認を求める事項である。

確認する頻度は、情報処理の開始時や一定期間経過後等、本学の特性に応じて設定することが望ましい。また、当該情報システムが固定されている等の理由で、情報システムの運搬が不可能な場合には、当該情報システムが設置されている現地に赴いて確認することが望ましい。

なお、あらかじめ部局技術責任者が認めた場合には、部局技術責任者が指定した者に確認させることも考えられる。その際には、部局技術責任者は、指定した者より適宜報告を受けることが望ましい。

第 1.5 部　情報システムについての基本的な対策

1.5.1 情報システムのセキュリティ要件

1.5.1.1 情報システムのセキュリティ要件

趣旨（必要性）

情報システムは、目的業務を円滑に遂行するため、その計画、構築、運用、移行、廃棄及び見直しのライフサイクルを通じて様々な要件を満たすことが必要である。その要件の中にはセキュリティの観点からの要件も含まれ、情報システムのライフサイクルにあわせてセキュリティ対策を実施する必要がある。

これらのことを勘案し、本項では、情報システムのライフサイクルの視点に立ち、各段階において考慮すべき情報セキュリティの対策基準を定める。

遵守事項

(1) 情報システムの計画

(a) 部局技術責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ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。

解説：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。なお、「情報システムを統括する責任者」とは、情報システムのライフサイクルの全般にわたって情報システムの構築・運用等に責任を持ち、その責務を全うするために人員、機器、予算等の資源を確保する者を想定している。

(b) 部局技術責任者は、情報システムのセキュリティ要件を決定すること。この場合、「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を行った上で決定すること。また、本学外の人々・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」に基づき決定すること。

解説：情報システムに求められる要求事項のうち、セキュリティに関わる要求事項について検討し、その中で必要と判断する要求事項を当該情報システムのセキュリティ要件として決定することを求める事項である。

「情報システムのセキュリティ要件」には、情報システムを構成するハードウェア、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。

具体的なセキュリティ要件については、本基準において事務情報セキュリティ技術基準に対応して定められた事項、本事務情報セキュリティ管理基準の「 1.5.2 情報

システムに係る規定の整備と遵守」に対応するものも含めた本学の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件を考慮して決める必要がある。この実施においては、「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、これを踏まえてセキュリティ要件を決定すること。

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。

また、ASP・SaaS サービス等の外部の情報システムを利用する場合は、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発生しないようにすること。

なお、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も同様に考慮すること。「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、仮想的・論理的に分割させた状態の情報システムをいう。例えば、仮想化技術を利用することが考えられる。

(c) 部局技術責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。

解説：情報システムのセキュリティ要件を満たすために必要な対策を定めることを求める事項である。

情報システムにおいて必要な対策としては、本基準において事務情報セキュリティ技術基準に対応して定められた事項、本事務情報セキュリティ管理基準の「 1.5.2 情報システムに係る規定の整備と遵守」に対応するものも含めた本学の情報セキュリティ関係規程内の事項及び当該情報システムの業務、取り扱う情報又は利用・運用の環境等の要因による当該情報システム固有の要件に基づく対策がある。

(d) 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及びソフトウェアについて、IT セキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性については、「IT セキュリティ評価及び認証制度に基づく認証取得製品分野リスト」を参照し、必要があると認めた場合には、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、当該製品を情報システムの構成要素として選択すること。

解説：情報セキュリティ機能が重要である機器等の購入において、要求する機能を有する製品に選択肢がある場合、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による認証を取得しているものを選択することを求める事項である。第三者による情報セキュリティ機能の客観的な評価によって、安全性の高い情報システムの構築が期待できる。

製品分野として当該認証を取得する必要性の判断については、「IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」に則ることが望ましい。なお、

国際承認アレンジメント（CCRA）参加国における ISO/IEC 15408 に基づく認証取得製品又は実質的に CC 認証取得製品とセキュリティ機能上同等であると確認されている製品（上記のリストを参照）を活用することが考えられる。

(e) 部局技術責任者は、情報システムについて、情報セキュリティの侵害又はそのおそれのある事象の発生を監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定めること。

解説：情報システムの計画において、情報セキュリティの侵害又はそのおそれのある事象の監視のために必要な措置を定めることを求める事項である。情報セキュリティの侵害とは、要保護情報について機密性、完全性又は可用性が損なわれること及び情報セキュリティ関係規程への違反をいう。監視する必要性の有無を検討するとは、情報システム及び取り扱う情報等を考慮して、情報システムの各所において監視する必要性の有無を検討することをいう。なお、監視の対象には、本学の外部から通信回線を通してなされる不正アクセス、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又は不正操作、サーバ装置等機器の動作、及び、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。

また、監視のために必要な措置を定めるとは、例えば以下の事項が考えられる。

（1）設ける監視機能を定める。監視機能には、以下の例がある。

・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（侵入検知システム等による）

・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 PC の接続を監視する機能

・PC への外部記録媒体の挿入を監視する機能

・サーバ装置等の機器の正常な動作を監視する機能

・要管理対策区域への入退出を監視する機能

（2）監視を行う運用時の体制を定める。情報システムの運用を行う体制において監視も行うことも考えられる。

（3）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、当該事務従事者等への説明について定める。

(f) 部局技術責任者は、構築した情報システムを運用段階へ導入するに当たって、情報セキュリティの観点から実施する導入のための手順及び環境を定めること。

解説：部局技術責任者に、セキュリティの観点での試験等の実施により当該情報システムがセキュリティ要件を満たすことを確認し、運用段階への導入の方法、体制、作業手順、スケジュール、期間、教育やトラブル対処について手順を整備することを求める事項である。

(2) 情報システムの構築及び運用

(a) 部局技術責任者は、情報システムの構築、運用に際しては、セキュリティ要件に基づき定めたセキュリティ対策を行うこと。

解説：情報システムのセキュリティ要件に基づき機器等の購入及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティにつ

いての脅威への対策、並びに情報システムについての対策及び監視を実施し、情報システムを構築、運用することを求める事項である。

(3) 情報システムの移行及び廃棄

(a) 部局技術責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を講ずること。

解説：情報システムの移行及び廃棄を行う場合に、情報システムを構成する機器の扱い、情報の格付等を考慮して、機器及び情報に関して廃棄、保存、消去等の適切な措置を講ずることを求める事項である。

(4) 情報システムの見直し

(a) 部局技術責任者は、情報システムのセキュリティ対策について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い、必要な措置を講ずること。

解説：情報システムのセキュリティ対策について、必要に応じて見直しとそれに必要な措置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、運用、監視等の状況により判断する必要がある。

1.5.2 情報システムに係る規定の整備と遵守

1.5.2.1 情報システムに係る文書及び台帳整備

趣旨（必要性）

本学の情報システムにおいて、適切なセキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うためには、情報システムの管理のために必要な情報を文書として整備する必要がある。また、本学全体としてセキュリティレベルを維持するとともに、より大規模な障害・事故等に対処するためには、本学が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備し、維持管理していく必要がある。

これらのことを勘案し、本項では、本学における情報システムに係る文書整備及び台帳整備に関する情報セキュリティの対策基準を定める。

遵守事項

(1) 情報システムの文書整備

(a) 部局技術責任者は、所管する情報システムについて以下の事項を記載した文書を整備すること。

(ア) 当該情報システムを構成する電子計算機関連事項

- 電子計算機を管理する事務従事者及び利用者を特定する情報
- 電子計算機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
- 電子計算機の仕様書又は設計書

(イ) 当該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事項

- 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

- 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
- 通信回線及び通信回線装置の仕様書又は設計書
- 通信回線の構成 ・通信回線装置におけるアクセス制御の設定
- 通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応 ・通信回線の利用部門

(ウ) 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

- 電子計算機のセキュリティ維持に関する手順
- 通信回線を介して提供するサービスのセキュリティ維持に関する手順
- 通信回線及び通信回線装置のセキュリティ維持に関する手順

(エ) 障害・事故等が発生した際の対処手順

解説：所管する情報システムにおいて、適切なセキュリティ対策を行い、また、障害・事故等が発生した際に適切な対処を行うために、情報システムの管理のために必要な情報を把握し、文書として整備することを定めた遵守事項である。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、文書は書面ではなく電磁的記録媒体として整備しても差し支えない。

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。電子計算機、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セキュリティホール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、速やかにセキュリティホール対策を行う等、適切に対処するために必要な事項である。

電子計算機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・事故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。

通信回線の構成、通信回線装置におけるアクセス制御の設定、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応、及び通信回線の利用部門の記載は、通信回線の管理状況を把握するために必要な事項である。

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。

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るべき手順であり、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、権限管理並びに証跡管理の設定・変更等の手順が挙げられる。

障害・事故等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。
・障害・事故等の内容・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・事故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
・障害・事故等から復旧等を行うための情報システムの構成要素ごとの対処に関する事項
・アンチウイルスソフトウェア等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（1.2.2.2(1)(c)を参照）により、上記のとおり整備されているならば、情報システム個別に整備しなくても構わない。

(b) 部局技術担当者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理においてセキュリティ対策を行うこと。

解説：所管する情報システムの運用管理において、適切なセキュリティ対策を行うことを求める遵守事項である。

(2) 情報システムの台帳整備

(a) 全学実施責任者は、全ての情報システムに対して、当該情報システムに係る以下の事項を記載した台帳を整備すること。

(ア) 情報システム名
(イ) 管理課室、当該部局技術責任者の氏名及び連絡先
(ウ) システム構成
(エ) 接続する学外通信回線の種別
(オ) 取り扱う情報の格付及び取扱制限に関する事項
(カ) 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、情報処理業務を外部に委託する場合は、以下の事項を記載した台帳を整備すること。
(キ) 役務名
(ク) 管理課室、当該部局技術責任者の氏名及び連絡先
(ケ) 契約事業者
(コ) 契約期間
(サ) 役務概要
(シ) ドメイン名（インターネット上で提供されるサービス等を利用する場合）
(ス) 取り扱う情報の格付及び取扱制限に関する事項

解説：本学全体としてセキュリティレベルを維持するとともに、より大規模な障害・事故等に対処するため、本学が所管する情報システムに係る情報のうち重要なものを一元的に把握し管理するための台帳を整備することを求める事項である。
情報システム名、管理課室及び当該部局技術責任者の氏名・連絡先の記載は、本学が所管する全ての情報システムを把握し、当該情報システムに係る管理責任を把握するために必要な事項である。
システム構成の記載は、情報システムを構成する電子計算機、通信回線及び通信回線装置に関する事項である。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。
接続する学外通信回線の種別、取り扱う情報の格付及び取扱制限に関する事項の記載は、当該情報システムを設置し、また運用管理することによるセキュリティ上のリスクを本学として把握するために必要な事項である。なお、取り扱う情報の格付及び取扱制限に関する事項については、情報システムを構成する電子計算機等について機器別又は機器の形態・目的別に記載することが望ましい。
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、実施責任者若しくは実施担当組織、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。
また、情報処理業務を外部委託する場合は、役務名、管理課室及び当該部局技術責任者の氏名・連絡先、契約事業者、契約期間、役務概要、ドメイン名（インターネット上で提供される役務等を利用する場合）、取り扱う情報の格付及び取扱制限に関する事項を記載した決裁に係る書類を集約し、容易に参照できるようにすることで、台帳の代替とすることも可能である。
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台帳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。

(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、当該情報システムの台帳の記載事項について全学実施責任者に報告すること。

解説：本学の各情報システムを所管する部局技術責任者が、情報システムに係る台帳に記載の事項について全学実施責任者に報告することを求める事項である。
台帳における網羅性の維持のため、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、台帳の最新性の維持のため、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、その報告の方法やタイミングについては、本学にて定めることが望ましい。

1.5.2.2 機器等の購入

趣旨（必要性）

機器等を購入（購入に準ずるリース等を含む。）する際に、当該機器等に必要なセキュリティ機能が装備されていない場合及び購入後にセキュリティ対策が継続的に行えない場合には、既存の情報システム又は購入する機器等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。

この課題に対応するため、機器等を購入する際は、本基準に準拠した機器等の購入を行うべく、購入先への要求事項を定める必要がある。

これらのことを勘案し、本項では、機器等の購入に関する対策基準として、全学実施責任者による機器等の購入に係る規定の整備、部局技術責任者による当該規定の遵守についての遵

守事項を定める。

適用範囲

本項は、機器等の購入（購入に準ずるリース等を含む。以下同じ。）に適用する。

遵守事項

(1) 機器等の購入に係る規定の整備

(a) 全学実施責任者は、機器等の選定基準を整備すること。

解説：機器等の選定に先立って、機器等の選定基準を整備することを求める事項である。

全学実施責任者は、機器等の選定基準の整備に当たっては、機器等が本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、機器等が本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。なお、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、機器等の購入に反映することが必要である。

(b) 全学実施責任者は、機器等の購入において、セキュリティ機能の要求仕様があり、総合評価落札方式により購入を行う際には、IT セキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用することを選定基準として定めること。

解説：機器等の購入において、セキュリティ機能の要求仕様があり、総合評価落札方式により購入を行う際に、当該機能を有する製品の中でも ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による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を求める事項である。

第三者による情報セキュリティ機能の客観的な評価のある製品を選定することによって、より信頼度の高い情報システムが構築できる。

(c) 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：機器等の納入時の確認・検査に関する手続を定めるものである。特に、確認・検査手続では、納入された機器等が定められた選定基準を満たすことを確認し、その結果を納品検査における確認の判断に加える手続を組み込む必要がある。

具体的な確認・検査の方法として、必要なセキュリティ機能の実装状況（機器等に最新のパッチが適用されているかどうか、アンチウイルス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）及び機器等に不正プログラムが混入していないことを、購入先からの報告で確認すること等が挙げられる。

(2) 機器等の購入に係る規定の遵守

(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候補の選定における判断の一要素として活用すること。

解説：整備された選定基準に従って、機器等に必要なセキュリティ機能が実装されていること等を確認し、これを機器等の選定における判断の一要素として利用することを求める事項である。

(b) 部局技術責任者は、機器等の納入時において、定められた確認・検査手続に従って、納品検査を実施すること。

解説：情報セキュリティ対策の視点を加味して定められた納入時の確認・検査手続に準拠して、納入された機器等の納品検査を行うことを求める事項である。

1.5.2.3 ソフトウェア開発

趣旨（必要性）

ソフトウェアを開発する際には、効果的なセキュリティ対策を実現するため、当該ソフトウェアが運用される際に関連する情報資産に対して想定される脅威を分析し、その分析に基づいて脅威から情報資産を保護するためのセキュリティ機能（真正確認、アクセス制御、権限管理、証跡管理等）及びその管理機能を適切にソフトウェアに組み込む必要がある。

加えて、開発するソフトウェアの処理に対するセキュリティホールの混入（設計及び作成時のミス等によりセキュリティホールが埋め込まれてしまうこと、不正なコードが開発者により意図的に埋め込まれること等）についての防止対策も必要となる。

これらのことを勘案し、本項では、ソフトウェアを開発する際の対策基準として、全学実施責任者によるソフトウェア開発に係る規定の整備、部局技術責任者による当該規定の遵守についての遵守事項を定める。

遵守事項

(1) ソフトウェア開発に係る規定の整備

(a) 全学実施責任者は、ソフトウェア開発について、セキュリティに係る以下の対策事項を部局技術責任者に求めるための規定を整備すること。

解説：本遵守事項では、全学実施責任者が部局技術責任者に求める規定を整備することとしているが、別途規定を整備することとはせずに、本基準内において部局技術責任者に対する遵守事項として（ア）～（セ）の事項を直接定める方法も可能である。ただし、後者の方法では、自己点検の対象が全学実施責任者ではなく部局技術責任者となることに留意すること。

(ア) 部局技術責任者は、セキュリティに係る対策事項（本項(1)(a)(ウ)から(セ)の遵守事項をいう。）を満たすことが可能な開発体制を確保すること。

解説：ソフトウェア開発を実施する体制が、セキュリティ維持の側面からも実施可能な開発体制（人員、機器、予算等）を確保することを求める事項である。

なお、開発体制の確保に当たっては、情報システムを統括する責任者に要求することとなる。ここで、情報システムを統括する責任者とは、情報システムのライフサイクルの全般にわたって情報システムの構築・運用等に責任を持ち、その責務を全うするために人員、機器、予算等の資源を確保する者を指す。

(イ) 部局技術責任者は、ソフトウェア開発を外部委託する場合には、セキュリティに係る対策事項（本項(1)(a)(ウ)から(セ)の遵守事項をいう。）の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。

解説：ソフトウェア開発を委託先に行わせる場合には、ソフトウェア開発を実施する者に実施の責任を負わせるセキュリティに係る要件を選択し、それを委託先に保証させることを求める事項である。「委託先に実施について保証させる」手段は、契約（付随する確認書等を含む。）によることとなる。

(ウ) 部局技術責任者は、ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。

解説：ソフトウェア開発に係る情報資産を保護するための手順及び環境を定めることを求める事項である。「手順」とは、例えば、仕様書及びソースコード等の成果物に対してソフトウェア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を指し、「環境」とは、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、開発に利用する電子計算機の設置場所及びアクセス制御の方法等を指す。

なお、ソフトウェア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。

(エ)部局技術責任者は、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と分離する必要性の有無を検討し、必要と認めたときは分離すること。

解説：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ことにより、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を求める事項である。これは運用中の情報システム全体ではなく一部だけの場合も同様である。例えば、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こと等も含まれる。

(オ) 部局技術責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。

解説：開発するソフトウェアに必要となるセキュリティ機能について、その設計を適切に行うとともに、設計書に明確に記録することを求める事項である。

なお、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、外部から察知される脅威（例えば、SQL インジェクション、バッファオーバーフロー等）は存在するため、開発するソフトウェアの機能、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。

(カ) 部局技術責任者は、開発するソフトウェアが運用される際に利用されるセキュリティ機能についての管理機能の必要性の有無を検討し、必要と認めたときは、管理機能を適切に設計し、設計書に明確に記述すること。

解説：「管理機能」とは、真正確認及び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、故障、事故及び障害等の発生時に行う対処及び復旧に係る機能、事故発

生時の証跡保全の機能等を指し、これらの必要性をソフトウェアの設計時から検討することにより、必要がある場合にはソフトウェアに組み込むことを求める事項である。

(キ) 部局技術責任者は、ソフトウェアの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。

解説：ソフトウェアの設計について、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を求める事項である。

一般にソフトウェア開発における設計レビューには、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。

(ク) 部局技術責任者は、開発するソフトウェアにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要と認めたときは、その方法を適切に設計し、設計書に明確に記述すること。

解説：ソフトウェアの内部及び入出力するデータについて、処理の誤りや意図的な改ざん等を検出するための機能、又はセキュリティホールの原因となり得る不正な入出力データを排除する機能等を組み込むことを求める事項である。

「データの妥当性」とは、例えば、HTML タグや JavaScript、SQL 文等として機能する不正な文字列や通信過程において生じたデータ誤り等、適切なデータ処理の障害になる情報がデータ内に含まれない状態であることを意味している。データの妥当性を確認する方法として、不正な文字列を変換し、又は削除する機能（いわゆるサニタイジング）の付加、チェックデジット（検査数字）による処理の正当性を確認する機能の付加等がある。

(ケ) 部局技術責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価及び ST 確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書の ST 評価及び ST 確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

解説：重要なセキュリティ要件があるソフトウェアについては、セキュリティ機能が確実に実装されることを目的として、ISO/IEC 15408 に基づきセキュリティ設計仕様書の ST 評価及び ST 確認を行うことを求める事項である。

「ST 評価及び ST 確認を受けること」とは、ST 評価及び ST 確認がなされた状態になることを意味し、具体的な手続としては、申請と確認書入手がなされることである。ソフトウェアの開発が終了するまでにセキュリティ設計仕様書について、ST

評価及び ST 確認済みとなっている必要があるが、セキュリティ設計仕様が適切であると判断できた上で設計段階から作成段階に移るべきであることから、申請行為は設計段階のうちに行われていることが通常の手順である。

なお、ソフトウェア開発を外部委託する場合には、契約時に条件として含め納品までに ST 評価及び ST 確認を受けさせることになる。

(コ) 部局技術責任者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスから保護するとともに、バックアップを取得すること。

解説：ソフトウェア開発者が悪意を持って脆弱性を持つソースコードを組み込んでしまうことを防ぐための変更管理や、ソースコードが流出することを防ぐための閲覧制限のためのアクセス制御、ソースコードの滅失及びき損等に備えたバックアップの取得等を求める事項である。

(サ) 部局技術責任者は、情報セキュリティの観点からコーディングに関する規定を整備すること。

解説：ソフトウェア開発者が意図せずに脆弱性の存在するソフトウェアを作成してしまわないように、ソフトウェア開発者が実施するコーディングに関する規定を定めるように求める事項である。

「コーディングに関する規定」とは、コードの可読性の向上や記述ミスの軽減のため、ソフトウェア開発担当者間のコードの記述スタイルのガイドラインとして、使用を控える構文、使用禁止語等を定めたいわゆるコーディング規約に相当する規定を指す。例えば、バッファオーバーフローによる情報の改ざんを防ぐために、データを更新する処理を実行する場合には、そのデータ量が適正であることを確認する処理を付加することを義務付ける等の規定が挙げられる。

(シ) 部局技術責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの必要性の有無を検討し、必要と認めたときは、ソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。

解説：ソースコードレビューの範囲及び方法について定めることを求める事項である。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、これらについては静的解析ツール、又はソースコードレビュー等による検証が挙げられる。なお、ソースコードレビューについては、開発するソフトウェア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。

(ス) 部局技術責任者は、セキュリティの観点から実施する試験の必要性の有無を検討し、必要と認めたときは実施する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。

解説：セキュリティの観点から必要な試験がある場合にその試験の項目及び試験方法を定めることを求める事項である。攻撃が行われた際にソフトウェア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、バッファオーバーフローが発生しないか、想定の範囲外のデータの入力を拒否できるか、DoS 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、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、ソフトウェアの試験計画全般について、セキュリティホールの有無、必要なチェック機能の欠如等について、単体試験、結合試験、統合試験等の複数の試験を通じて、必要な試験が網羅されるよう留意することが望ましい。

(セ) 部局技術責任者は、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：「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、セキュリティホールを発見した場合の対処に利用できるようにすることを求める事項である。

(2) ソフトウェア開発に係る規定の遵守

(a) 部局技術責任者は、ソフトウェア開発に係る規定に基づいて、ソフトウェアの開発を行うこと。

解説：ソフトウェア開発を行う部局技術責任者が、本学で整備したソフトウェア開発に係る規定を遵守して、ソフトウェアの開発を行うことを定めた事項である。

1.5.2.4 主体認証・アクセス制御・権限管理・証跡管理・保証等の標準手順

趣旨（必要性）

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

一方、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。また、主体認証情報の機密性と完全性、及びアクセス制御情報の完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。

これらのことを勘案し、本項では、主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準として、全学実施責任者による主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備、部局総括責任者及び部局技術責任者による当該規定の遵守、部局技術責任者による取得した証跡の点検、分析及び報告についての遵守事項を定める。

なお、1.4.1.1 において識別コードと主体認証情報の管理等に関する判断基準を、事務情報セキュリティ技術基準 2.2.1.1~2.2.1.5 においても主体認証・アクセス制御・権限管理・証跡管理・保証等の導入等に関する対策基準を定めている。

遵守事項

(1) 主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の整備

(a) 全学実施責任者は、本学における主体認証・アクセス制御・権限管理・証跡管理・保

証等の必要性判断に関する規定を、以下の事項を含めて定めること。

解説：本遵守事項では、全学実施責任者が部局総括責任者及び部局技術責任者に求める規定を整備することとしているが、別途規定を整備することはせずに、本基準内において部局総括責任者及び部局技術責任者に対する遵守事項として（ア）～（カ）の事項を直接定める方法も可能である。

ただし、後者の方法では、自己点検の対象が全学実施責任者ではなく部局総括責任者及び部局技術責任者となることに留意すること。

(ア) 部局技術責任者は、全ての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要があると判断すること。

解説：主体認証を行う前提として、部局技術責任者に、各情報システムについて、アクセスする主体の主体認証を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、主体認証を行う必要があると判断すること。

(イ) 部局技術責任者は、全ての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。

解説：アクセス制御を行う前提として、部局技術責任者は、各情報システムについて、アクセス制御を行う必要性の有無を検討しなければならない。要保護情報を取り扱う情報システムにおいては、アクセス制御を行う必要があると判断すること。

なお、アクセス制御方式やセキュリティに配慮した OS に関する用語の解説については、内閣官房情報セキュリティセンターによる「電子政府におけるセキュリティを配慮した OS を活用した情報システム等に関する調査研究」を参照のこと。

http://www.nisc.go.jp/inquiry/pdf/secure_os_2004.pdf

(ウ) 部局技術責任者は、全ての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。

解説：権限管理を行う前提として、部局技術責任者に、各情報システムについて、アクセスする主体の権限管理を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、権限管理を行う必要があると判断すること。

なお、アクセス制御は、主体から客体へのアクセス条件を制限することで客体に対してのアクセス許可を管理することである。それに対して、権限とは、主体に付与（発行、更新及び変更を含む。以下この項において同じ。）される許可のことをいい、権限管理とは、主体に対する許可情報を管理することである。その主体が情報システムの管理を担う場合には、その主体に対して管理者権限を与える場合もある。

(エ) 部局総括責任者は、全ての情報システムについて、証跡管理を行う必要性の有無を検討すること。

解説：証跡管理を行う前提として、部局総括責任者に、情報システムについて、証跡管理を行う必要性の有無を検討することを求める事項である。

情報セキュリティは、本学の内部及び外部からの不正アクセス、不正侵入、誤操作又は不正操作等の様々な原因により損なわれることがある。また、高等教育機関の事務の遂行以外の目的でウェブの閲覧や電子メールの送受信がなされるおそれもある。万一問題が発生した場合にはその実行者を特定する必要があるため、一連の事象を情報システムで証跡として取得し、保存する必要がある。

証跡として多くの情報を取得すれば、事後追跡及び事前抑止の効果は高まる。その反面、多くの証跡を取得する場合には、情報システムの処理能力及び記憶容量を多く消費することになる。部局総括責任者は、この両面に配慮し、また情報システムの重要度や取り扱う証跡管理情報の機密性も考慮して、証跡として取得する情報と、証跡を取得する箇所を決定する必要がある。

証跡には、以下のような管理記録が考えられる。

・識別コードの発行等の管理履歴

・各識別コードへのアクセス権設定の管理履歴

それらの権限管理者の許認可そのものの管理履歴また、証跡として、上記の他に以下のような利用記録や監視記録等を含めることも考えられる。

・利用者による情報システムの操作記録

・操作する者、監視する者及び保守する者等による情報システムの操作記録

・ファイアウォール、侵入検知システム（ Intrusion Detection System）等通信回線装置の通信記録

・プログラムの動作記録

なお、証跡管理を行う必要性の有無の判断に当たっては、情報システムの側面だけではなく、組織的な側面からの検討も必要であるため、部局総括責任者によるものとしている。

(オ)部局総括責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡として取得する情報項目及び証跡の保存期間を定めること。

解説：証跡を取得する場合に、取得する情報項目及び証跡の保存期間を適切に定めることを求める事項である。以下に示す例は一般的に取得すべき基本的な情報項目であるが、限られた情報量で実効性のある証跡を取得するように設計することが重要である。証跡に含める情報項目の例：

・事象の主体である者又は機器を示す識別コード等

・事象の種類（ウェブサイトへのアクセス、ログオン及びログアウト、ファイルへのアクセス、アプリケーションの起動及び終了、特定の操作指令等）

・事象の対象（アクセスした URL（ウェブアドレス）、ログオンしたアプリケーション、アクセスしたファイル、起動及び終了したアプリケーション、操作指令の対象等）

・日付、時刻

・成功、失敗の区別、事象の結果

・電子メールのヘッダ情報、通信内容

・通信パケットの内容

・操作する者、監視する者及び保守する者等への通知の内容

また、保存期間は、１つの情報システムであっても取得する箇所や情報項目により異なることもあり得る。

情報セキュリティに関する問題を事後に追跡し、また事前に抑止するという証跡管理の目的に照らして、保存期間を定めることになる。

(カ) 部局技術責任者は、証跡を取得する必要があると認められた情報システムにおいては、部局技術担当者及び利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。

解説：証跡の取得等について、あらかじめ部局技術担当者及び利用者等に対して説明を行うことを求める事項である。取得、保存する証跡には、情報システムの管理者、操作員及び利用者等の行動に関する情報が記録される。そのため、証跡を取得、保存し、事後に参照、点検、分析する可能性があることを、利用者に説明する必要がある。なお、証跡を証拠として活用する際の正当性を高めるためにも周知することが望ましい。

(キ) 部局技術責任者は、要保護情報を取り扱う情報システムについて、保証のための対策を行う必要性の有無を検討すること。

解説：要保護情報を取り扱う情報システムについて、情報が適切な状態であることを保証するための対策の必要性の有無を検討することを求める事項である。

(2) 主体認証・アクセス制御・権限管理・証跡管理・保証等に係る規定の遵守

(a) 部局総括責任者及び部局技術責任者は、本学における主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定に基づいて、情報システムの導入を行うこと。

解説：部局総括責任者及び部局技術責任者が、本学で主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断に関する規定を遵守して、情報システムの導入を行うことを定めた事項である。

(3) 取得した証跡の点検、分析及び報告

(a) 部局技術責任者は、証跡を取得する必要があると認められた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析することの必要性の有無を検討し、必要と認めたときは、当該措置を講じ、その結果に応じて必要な情報セキュリティ対策を講じ、又は部局総括責任者に報告すること。

解説：取得した証跡を用いて、定期的に又は何らかの兆候を契機に点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講ずることにより、情報セキュリティを維持し、あるいはその侵害を早期に検知することを求める事項である。

取得した証跡は、その全てを定期的に精査することは一般には困難であり、その一部を重点あるいは指標として点検及び分析することが有効である。重点項目の内容と証跡の量を定期的に点検し、その範囲で通常とは異なる状況が見られた場合に更に詳細な点検及び分析を行うことも考えられる。

証跡の点検、分析及び報告を支援するための自動化機能が設けられていれば、これを利用することにより、作業を効率的かつ確実に行うことができる。

情報セキュリティの侵害が特定された場合は、復旧及び再発防止のために必要な対策を採らなければならない。

1.5.2.5 暗号と電子署名の標準手順

趣旨（必要性）

情報システムの利用において、当該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には、情報の暗号化及び電子署名を行うことが有効な対策となりうるが、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップについては、様々な選択肢があり得ることから、事務従事者による個別判断で選択されることのないよう、本学で標準となる手順を定めることが重要である。

これらのことを勘案し、本項では、暗号化及び電子署名のアルゴリズム、方法、鍵管理、鍵保存並びに鍵バックアップの標準手順に関する対策基準として、全学実施責任者による暗号と電子署名に係る規定の整備、事務従事者による当該規定の遵守についての遵守事項を定める。

なお、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する判断基準を、事務情報セキュリティ技術基準 2.2.1.1~2.2.1.5 においても各機能の導入等に関する対策基準を定めている。

遵守事項

(1) 暗号と電子署名に係る規定の整備

(a) 全学実施責任者は、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を、以下の事項を含めて定めること。

(ア) 電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。

(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、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を使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。

解説：学内の情報システムにおける暗号化及び電子署名について、使用を認めるアルゴリズム及び方法を全学実施責任者が定めることを求める事項である。アルゴリズム及び方法は、暗号及び電子署名の使用場面等に応じて整備することも可能である。例えば、電子メールの暗号化に関してアルゴリズムを定めるとともにその方法を S/MIME とし、ウェブサーバとブラウザの通信の暗号化に関してアルゴリズムを定めるとともに方法を SSL とする。他に、データベースのデータ暗号化や、電子申請における電子署名等についても、アルゴリズム及び方法を定めることが考えられる。事務従事者は、文書の作成、電子メールの送受信等に汎用のソフトウェアを日常的に使用しているが、これらのソフトウェアでは、暗号化及び電子署名について、複数のアルゴリズムを用意し、設定画面等で利用者が選択できるようにしている場合がある。そのような場合には、事務従事者は、（ア）にもとづき電子政府推奨暗号リストに記載されたアルゴリズムを選択して使用することになる。

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、部局技術責任者は、本遵守事項に基づき全学実施責任者が定めたアルゴリズム及び方法を使用する。なお、本学における検証済み暗号リストを作成する場合には、安全性も含めたその理由を明確にしておくことや誰がそのように判断したかについても明確にしておく必要がある。

暗号化又は電子署名を行う特定の箇所について見ると、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、複数のアルゴリズムを実装し、使用可能とする場合がある。この場合には、共通鍵暗号、公開鍵暗号及びハッシュ関数のそれぞれについて、電子政府推奨暗号リストに記載されたアルゴリズムを少なくとも一つ含めることを求める。

(ウ) アルゴリズムが危殆化した場合の緊急対応計画の必要性の有無を検討し、必要と認めたときは、緊急対応計画を定めること。

解説：アルゴリズムが危殆化した場合に備えて、情報システムの停止等の緊急避難的な対応計画を策定することを求める事項である。対象となるアルゴリズムは、用途に応じて変わることに留意すること。

(b) 全学実施責任者は、暗号化された情報（書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の（ア）から（ウ）の手順（以下「鍵の管理手順等」という。）を定めること。

(ア) 鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等

解説：鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等を定めることによって、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の適正な管理を求める事項である。

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、その適切な運用管理が重要である。なお、オペレーティングシステムに標準搭載されている暗号化又は電子署名付与の機能を使用する場合や、パッケージソフトを使用する場合に、鍵の生成手順や有効期限等が定められている時は、安全性を検討の上、これを準用することが可能である。また、電子署名の有効期限については、当該有効期限満了までの間、その正当性を検証可能なものとする必要がある。

(イ) 鍵の保存手順

解説：鍵の保存手順を保存方法及び保存場所を含めて定めることによって、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の適正な管理を求める事項である。

鍵の保存方法としては、電磁的記録媒体に保存することが考えられるが、それをどのように保存するかの方法や、保存する際に電磁的記録媒体以外の記録媒体と併用することの是非等についても定める必要がある。

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、その適切な運用管理が重要である。なお、オペレーティングシステムに標準搭載されている暗号化又は電子署名付与の機能を使用する場合や、パッケージソフトを使用する場合に、鍵を保存する電磁的記録媒体や保存場所が定められている時は、安全性を検討の上、これを

準用することが可能である。
情報システム共通として鍵の保存手順を定める場合には、全学実施責任者が直接それを定めることが考えられる。あるいは、情報システムごとに鍵の保存手順を個別に定めるのであれば、各部局技術責任者にそれを定めさせることについて、定めるという方法でもよい。

(ウ) 鍵のバックアップ手順

解説：暗号化された情報の復号に用いる鍵の紛失及び消失に備え、鍵のバックアップ手順等を定めることを求める事項である。
鍵のバックアップ手順については、バックアップが必要な鍵とバックアップしてはならない鍵の区別を明確にし、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預託手順等を定める。
例えば、復号に用いる鍵を紛失し、又は消失した場合には、それ以前に暗号化した情報を復号できなくなる。そのため、鍵情報のバックアップを取得したり、信頼できる第三者へ鍵情報を預託したりする等の鍵のバックアップ対策が必要である。ただし、鍵情報の複製は、その漏えいに係るリスクを増大させる可能性があるため、最小限にとどめること。
なお、本遵守事項における鍵のバックアップ手順は、前事項の鍵の管理手順等に含めて整備することも可能である。
なお、バックアップしてはならない鍵のタイプについては、例えば、乱数を生成するために用いられる鍵や暗号化に用いる鍵の共有を目的として一度だけ使用される鍵等が考えられる。また、米国国立標準技術研究所（NIST）が発行している文書「SP800-57」を参考とすることも考えられる。

(c) 全学実施責任者は、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政府認証基盤（GPKI）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：情報システムにおいて電子署名を生成するに当たり、当該電子署名の検証に使用可能な電子証明書を GPKI が発行している場合には、それを使用することを求める事項である。このような電子証明書には、サーバ証明書、コード署名証明書等がある。
なお、GPKI 以外で使用している電子証明書が有効期限内の場合、次期更新時には、GPKI で発行している電子証明書を使用するように求めることも考えられる。

(2) 暗号と電子署名に係る規定の遵守

(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。

解説：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、本学で定めたアルゴリズム及び方法を遵守することを求める事項である。

(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。

解説：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が露呈した場合、暗号化された情報の漏えいや電子署名の偽造等のおそれがある。そのため、事務従事者による鍵情報の保護を求める事項である。

(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。

解説：鍵の書換え、紛失、消失等により、その完全性、可用性が侵害された場合には、暗号化により保護されている情報を復号することが困難となり、可用性が損なわれる可能性がある。そのため、事務従事者による鍵のバックアップを求める事項である。

1.5.2.6 学外の情報セキュリティ水準の低下を招く行為の防止

趣旨（必要性）

本学が、学外の情報セキュリティ水準の低下を招くような行為をすることは、学外に対して適切な行為でないことは当然であって、その行為が他者の情報セキュリティ水準を低下させることによって、本学を取り巻く情報セキュリティ環境を悪化させるため、本学にとっても好ましくない。これらのことを勘案し、本項では、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対策基準として、全学実施責任者による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の整備、事務従事者による当該規定の遵守についての遵守事項を定める。

遵守事項

(1) 措置についての規定の整備

(a) 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こと。

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可能性のある行為としては、例えば、以下のものが挙げられる。

（ア）不適切なソフトウェア及びサービスの使用要求：情報サービス（例えば、本学のウェブによるコンテンツの提示等を言う。以下同じ。）を利用するために、脆弱性の問題が指摘されているソフトウェア及びサービスの使用（脆弱性の問題が指摘されているソフトウェア及びサービスのインストールや脆弱性の問題が指摘されているバージョンへの変更による使用を言うが、脆弱性の問題が改善されているソフトウェア及びサービスへの変更ができないことによる使用継続を含む。）を暗黙又は明示的に要求する行為。

（イ）ソフトウェアの不適切な設定要求：情報サービスを利用するために、利用者の環境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、クライアント PC の OS やウェブブラウザ等）以下同じ。）について、セキュリティ設定の下方修正を暗黙又は明示的に要求する行為。

（ウ）ソフトウェア等の不適切な削除要求：本学のウェブのコンテンツを利用するために、利用者のセキュリティ対策に必要なソフトウェアやハードウェア等の無効化や削除を暗黙又は明示的に要求する行為。

「明示的に要求する行為」とは、「『このような設定を変更してください。』等のよう

に明記すること」であるが、「暗黙に要求する行為」とは、「『このサービスを利用するためには、このような設定が必要です。』と婉曲に記載すること」だけではなく、何も記載しなくとも「結果的にそのような設定変更をしないと利用を継続できないような状態でサービスを提供すること」も含む。
以下のような場合に、暗黙の要求になることがあるので、注意する必要がある。
・ソフトウェアを実行させる場合：情報サービスのためのソフトウェアを実行させる場合に注意する必要がある。それらを大別すると、単独実行型（例えば、Windowsの「.exe」ファイル等）、ランタイム環境実行型（例えば、Java アプレットや Windows の ActiveX ファイル等）、クライアントソフト内実行型（例えば、JavaScript やファイル中のマクロ等）があるが、これらの全てを含む。
・HTML メール等を送信する場合：本学から HTML メール等（利用者がセキュリティ上の理由から受信側のメールサーバやメールクライアントで処理を制限していることが想定されるメール文書形式を用いたメールのこと。）を送信する場合に注意する必要がある。

これらの場合については、結果的に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。実行させるソフトウェアの提供については、オンラインによる提供（ウェブへの掲載、メールの添付等）について特に注意して規定を整備する必要がある。その際に大別した種類ごとに整備しても構わない。例えば、単独実行型ファイルについてはオンライン提供の原則禁止、ランタイム環境実行型については電子署名を付けることの義務付け、HTML メール等の送信については受信者の事前同意を得た場合のみの送信と不同意者への別方式の送信手段の提供の義務付け等が考えられる。
やむをえず、単独実行型ファイルをオンライン提供する必要が生じた場合は、電子署名を付けることを義務付けること。また、オンラインによる提供だけでなく、外部電磁的記録媒体を介したオフラインによる提供の場合も同様に考慮する必要がある。

ソフトウェアを提供する者は、ソフトウェアの動作や脆弱性に十分注意して署名を付与する必要がある。
また、オンライン又はオフラインでソフトウェアを提供する際に、ソフトウェアに対する署名（コード署名）が必要な場合には、政府認証基盤（GPKI）で発行したコード署名証明書を利用することが望ましい。
なお、正当な署名が付与されたソフトウェアに対しては、ユーザの確認なしに、端末上の機能が当該ソフトウェアに利用される場合があることに注意すること。
（ア）（イ）については、当該情報サービスの準備をした時点では、脆弱性の問題が指摘されていなくても、運用開始後に指摘される場合もある。そのような場合にも脆弱性を回避するための選択を利用者ができるように努めなければならない。回避に必要な当該情報サービスで用いるウェブのコンテンツやアプリケーション等の是正を容易にできるような準備や設計について規定を整備する必要がある。「容易にで

きる」とは、追加の予算措置を講じなくてもよい程度であり、運用担当者による変更ができるか、是正開発作業を保守費用の範囲に含める等の方法を考えることができる。
例えば、電子行政用ウェブのアプリケーションを利用するために、利用者の PC 上にあらかじめ標準的にインストールされているソフトウェアがバージョンＡであったとする。その後、そのソフトウェアの最新バージョンがＢに更新され、また、バージョンＡについて脆弱性が公開された場合には、バージョンＢで当該アプリケーションを利用できるようにしなければならない。このとき、当該アプリケーションがそのソフトウェアのバージョンＡだけで動作するような設計では、利用者に脆弱性のあるバージョンＡを利用することを暗黙に要求してしまうことになる。そのような場合に適切な対処（バージョンＢでも当該アプリケーションを利用できるようにする等）を容易に実施できるように、設計内容又は業者との保守契約内容等について検討しておくことが重要である。
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で動作するように、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等、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。

(2) 措置についての規定の遵守

(a) 事務従事者は、学外の情報セキュリティ水準の低下を招く行為の防止の規定に基づいて、必要な措置を講ずること。

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本学の役割を定めた事項である。事務従事者は、組織及び個人として措置を講ずることが重要である。

1.5.2.7 ドメイン名の使用についての対策

趣旨（必要性）

本学では、行政に係る情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサーバ、電子メール等を用意し、本学外の人々の利用に供している。これらのサービスはインターネットを介して利用するものであるため、本学外の人々にとっては、そのサービスが実際の本学のものであると信頼できることが重要である。一方、インターネット上のサービスの特定はドメイン名（例えば、nisc.go.jp のこと。）が重要な役割を果たしており、本学において一貫したドメイン名を使用することにより、万一本学以外の者による悪用や詐称がなされた場合にも本学外の人々が気付くための条件を整備する必要がある。

これらのことを勘案し、本項では、本学におけるドメイン名の使用に関する対策基準として、全学実施責任者によるドメイン名の使用についての規定の整備、事務従事者による当該規定の遵守についての遵守事項を定める。

遵守事項

(1) ドメイン名の使用についての規定の整備

(a) 全学実施責任者は、ドメインネームシステムによるドメイン名（以下「ドメイン名」と言う。）の使用について、以下の事項を事務従事者に求める規定を整備すること。

解説：本遵守事項では、全学実施責任者が事務従事者に求める規定を整備することとしているが、別途規定を整備することとはせずに、本基準内において事務従事者に対する遵守事項として（ア）～（ウ）の事項を直接定める方法も可能である。ただし、後者の方法では、自己点検の対象が全学実施責任者ではなく事務従事者となることに留意すること。

(ア) 事務従事者は、学外の者（国外在住の者を除く。以下本項において同じ。）に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、以下の政府機関のドメイン名であることが保証されるドメイン名（以下「政府ドメイン名」という。）を使用すること。

- go.jp で終わるドメイン名

ただし、電子メール送信又は政府ドメイン名のウェブページでの掲載に限り以下の条件を満たす場合には、政府ドメイン名以外のドメイン名を本学以外のものとして告知してもよい。

具体的には、電子メールの送信においては以下の条件を全て満たすことが必要である。

- 告知内容についての問い合わせ先として政府ドメイン名による電子メールアドレスを明記しているか、又は政府ドメイン名による電子署名をしていること。
- 告知するドメイン名を管理する組織名を明記すること。
- 告知するドメイン名の有効性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していること。

また、政府ドメイン名のウェブページでの掲載においては以下の条件を全て満たすことが必要である。

- 告知するドメイン名を管理する組織名を明記すること。
- 告知するドメイン名の有効性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していること。

解説：「.go.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、日本国の政府機関、各省庁所管研究所、独立行政法人、特殊法人（特殊会社を除く）とされている。

アクセスさせることを目的にドメイン名を告知するとは、ウェブサイト（例えば、http://www.nisc.go.jp/）や FTP サーバ（例えば、ftp://ftp.nisc.go.jp/）等へのアクセスを促すことをいう。上記には、ウェブページの閲覧に必要なソフトウェア（プ

ラグインを含む）を入手できる政府ドメイン名以外のウェブサイトを告知する場合も含む。また、送信させることを目的にドメイン名を告知するとは、電子メールの宛先（例えば、null@nisc.go.jp）への送信等を促すことをいう。

本遵守事項における告知にあたる場合とは、情報提供のきっかけが本学側にある場合で、告知にあたらない場合とは、情報提供のきっかけが本学側にない場合である。例えば、学外の者からの問い合わせに回答する場合は、問い合わせがきっかけであるので、告知にはあたらず、本遵守事項の対象とはならない。なお、いずれの場合についても媒体の種類（郵送、電話、電子メール送信、ウェブ掲載、ポスター掲示等）を問わない。

「告知する場合に」としているが、実際には「告知内容を検討する際に告知するドメイン名を決める時点で」実施しなければならない遵守事項である。

なお、在外公館のように国外在住の者を対象とし、かつ、現地のルールに従うことが適切であると考えられる場合には、この限りではない。これらドメイン名の使用については、外務省ウェブサイト等において確認できるよう措置されることが適当である。

政府ドメイン名以外のドメイン名を告知してもよい条件を満たす記載の例としては、以下のようなものが考えられる。

（例）

・この告知についてのお問い合わせは、null@nisc.go.jp までご連絡ください。

・この告知で案内しているウェブサイトは○○○協会が運営しており、内閣官房が運営しているものではありません。

・この告知で案内しているウェブサイトのアドレスについては、2007 年 12 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。

(イ) 事務従事者は、学外の者に対して、送信に使用する電子メールのドメイン名は、政府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、当該事務従事者が既知の者である場合を除く。

解説：送信に使用する電子メールのドメイン名として政府ドメインの使用を求める遵守事項である。また、電子メールの送信元として政府ドメイン名を使用するに当たっては、その送信に用いる電子メールサーバは、当該政府ドメイン名にかかる DNS サーバの MX レコードで指定している IP アドレスのサーバである必要がある。なお、送信元として使われる電子メールアドレスを外部に告知する場合には、適切なドメイン名で告知するように、事前に準備する必要がある。

(ウ) 事務従事者は、学外の者に対して、アクセスさせることを目的として情報を保存するためにサーバを使用する場合には、政府ドメイン名のサーバだけを使用すること。

解説：学外の者にアクセスさせることを目的として情報を保存するサーバとは、主としてウェブサーバのことをいう。

（ア）により政府ドメイン名以外のドメイン名を告知することを禁止しているが、告知していなくとも、政府機関としての情報を政府ドメイン名以外のドメイン名の

ウェブサーバに保存していると、インターネット上の検索サービス等により表示される場合がある。そのような場合には、なりすましをしようとする者が、政府機関からの情報を装った内容を保存したウェブを作成して、検索されるのを待ち伏せするという方法によるなりすましが考えられる。普段から政府ドメイン名のウェブサーバだけを使うことで、検索結果が政府ドメイン名以外である場合に、そこに保存されている情報の真偽について学外以外の者が注意を心がけやすくできる。

なお、既存のウェブサーバ等においてこれら以外のドメイン名のサーバの使用が避けられない場合には、本遵守事項に対する例外措置を必要な期間に限り適用し、かつ、政府ドメイン名のサイトから当該ドメイン名を案内することにより、新規に告知するドメイン名について（ア）を遵守すること。

また、政府ドメイン名以外のウェブサーバの使用を停止した後も、当該ドメイン名を不正に利用されないように管理することに注意しなければならない。具体的には、そのような用途に使用した当該ドメイン名については、使用後も登録管理を一定期間維持することを求める規定を設ける必要がある。

(2) ドメイン名の使用についての規定の遵守

(a) 事務従事者は、ドメイン名の使用についての規定に基づいて、必要な措置を講ずること。

解説：全ての事務従事者が、インターネットを経由した行政サービスの提供に当たり、本学で整備したドメイン名の使用についての規定を遵守して、政府ドメイン名等のドメイン名を適切に使用することを定めた事項である。

なお、ウェブサイトの構築・管理等の「ドメイン名の使用」を伴う業務を外部委託する場合は、事務従事者が委託先への要求事項に含める必要がある。

そのような業務の外部委託は、情報システム部門以外の者が担当となる場合があるため、それらの者にも本遵守事項を周知すること。

1.5.2.8 不正プログラム感染防止のための日常的実施事項

趣旨（必要性）

不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の要機密情報を漏えいさせることから機密性に対する脅威ともなる。不正プログラムへの感染を防止するためには、情報システムを利用する全ての事務従事者が、アンチウイルスソフトウェア等を活用して不正プログラムの検知・除去に努めるほか、ファイルの閲覧や実行、外部ファイルの取り込み等において十分な注意を払う必要がある。

これらのことを勘案し、本項では、不正プログラム感染の回避を目的とした対策基準として、全学実施責任者による不正プログラム対策に係る規定の整備、事務従事者による当該規定の遵守について遵守事項を定める。

遵守事項

(1) 不正プログラム対策に係る規定の整備

(a) 全学実施責任者は、不正プログラム感染の回避を目的として、以下の措置を事務従事者に求める規定を整備すること。

解説：本事項では、全学実施責任者が事務従事者に求める規定を整備することとしているが、別途規定を整備することとせずに、本基準内において直接に事務従事者に対する遵守事項として（ア）～（キ）の事項を定める方法も可能である。ただし、後者の方法では、自己点検の対象が全学実施責任者ではなく事務従事者となることに留意すること。

(ア) 事務従事者は、アンチウイルス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ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

解説：不正プログラムに感染したソフトウェア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、復旧に労力を要するため、不正プログラムとして検知された実行ファイル等の実行を禁止する事項である。

なお、アンチウイルスソフトウェア等が全ての現存する不正プログラムを検知できるとは限らないことに留意し、あわせて必要な予防措置を行うことが望ましい。予防措置とは、例えば、差出人が不明な電子メールに添付された不審なファイルを実行しないこと、ウェブクライアントのセキュリティ設定を不必要に低下させないこと、不審なウェブサイトを閲覧しないこと等である。

(イ) 事務従事者は、アンチウイルス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こと。

解説：アンチウイルス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最新化することで、不正プログラム等の検知漏れによる感染を回避することを求める事項である。

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。ただし、利用に当たってはアンチウイルスソフトウェア等を自動更新する情報システムが提供するサービスの内容、当該アンチウイルスソフトウェア等に不具合が含まれていた場合に影響が及ぶ範囲、自動更新しない場合に不正プログラムに感染するリスクが高まること等を勘案すべきである。

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、部局総括責任者が適切な方法を選択すること。同様に（ウ)～(オ)の事項は、部局総括責任者が適切な方法を選択すること。

(ウ) 事務従事者は、アンチウイルス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こと。

解説：人為による対策の漏れや遅れを回避するために、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を求める事項である。

ファイルの作成、参照等のたびに検査を自動的に行う機能をオンに設定し、その機能をオフにしないことが必要である。

(エ) 事務従事者は、アンチウイルスソフトウェア等により定期的に全ての電子ファイルに対して、不正プログラムの有無を確認すること。

解説：定期的に不正プログラムの有無を確認することを求める事項である。前事項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、定期的に全ての電子ファイルを検査する必要がある。

(オ) 事務従事者は、外部からデータやソフトウェアを電子計算機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。

解説：外部とやり取りするデータやソフトウェアには、ウェブの閲覧やメールの送受信等のネットワークを経由したもののほか、 USB メモリや CD-ROM 等の外部電磁的記録媒体によるものも含む。不正プログラムの自動検査による確認ができていればそれで差し支えない。

(カ) 事務従事者は、不正プログラム感染の予防に努めること。

解説：不正プログラム感染の予防に役立つ措置の実施を求める事項である。アンチウイルスソフトウェア等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に注意して、例えば、アプリケーションでマクロの自動実行を無効にすることによりマクロウイルスの実行を防ぐことや、ソフトウェアのセキュリティ設定により読み込まれるプログラムやスクリプトの実行を無効にすること、安全性が確実では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こと等がある。

(キ) 事務従事者は、不正プログラムに感染したおそれのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講ずること。

解説：不正プログラムに感染したおそれがある電子計算機については、他の電子計算機への感染等の被害の拡大を防ぐために、当該電子計算機が通信回線に接続している場合には、それを切断して、必要な措置を講ずることを求める事項である。切断後に必要となる措置としては、例えば、不正プログラムの有無を検知して駆除することや、「1.2.2.2 障害・事故等の対処」に定められた連絡等をすることが挙げられる。

(2) 不正プログラム対策に係る規定の遵守

(a) 事務従事者は、定められた不正プログラム対策に係る規定に基づいて、不正プログラムの感染を防止するための対策を行うこと。

解説：全ての事務従事者が、不正プログラム対策に係る規定に基づき、不正プログラムの感染を防止するための対策を行うことを定めた事項である。

B2551 事務情報セキュリティ対策技術基準

目　次

第 2.1 部　総則

2.1.1.1 本事務情報セキュリティ技術基準の位置付け

事務情報セキュリティ管理基準に準じる。

2.1.1.2 本事務情報セキュリティ技術基準の使い方

(1) 全体構成

事務情報セキュリティ管理基準に準じる。

(2) 対策項目の記載事項

事務情報セキュリティ管理基準に準じる。

(3) 「対策レベルの設定」に係る変更点

事務情報セキュリティ管理基準に準じる。

2.1.1.3 情報の格付の区分及び取扱制限の種類

(1) 格付及び取扱制限

事務情報セキュリティ管理基準に準じる。

(2) 格付の区分

事務情報セキュリティ管理基準に準じる。

(3) 取扱制限の種類

事務情報セキュリティ管理基準に準じる。

2.1.1.4 情報取扱区域における管理及び利用制限

(1) 情報取扱区域

事務情報セキュリティ管理基準に準じる。

(2) 情報取扱区域のクラスの決定

事務情報セキュリティ管理基準に準じる。

(3) 情報取扱区域のクラス別管理及び利用制限

事務情報セキュリティ管理基準に準じる。

(4) 情報取扱区域の個別管理及び個別利用制限

事務情報セキュリティ管理基準に準じる。

2.1.1.5 用語定義

事務情報セキュリティ管理基準に準じる。以下は、本事務情報セキュリティ技術基準で初出の用語。

【あ】

- 「受渡業者」とは、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。

【か】

- 「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造・提供元等から公表されたセキュリティホール、又は JPCERT コーディネーションセンター等のセキュリティ関連機関から公表されたセキュリティホールが該当する。

【は】

- 「複数要素（複合）主体認証（multiple factors authentication）方式」とは、複数の方法の組合せにより主体認証を行う方法である。

【ま】

- 「モバイル端末」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用する端末は、モバイル端末に含まれない。

第 2.2 部　情報セキュリティ要件の明確化に基づく対策

2.2.1 情報セキュリティについての機能

2.2.1.1 主体認証機能

趣旨（必要性）

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権のない者が、故意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

これらのことを勘案し、本項では、主体認証機能の導入に関する対策基準を定める。

また、政府機関が有する各情報システムの利用者は、事務従事者に限られるものではない。例えば、学生や社外利用者向けのサービスを提供する情報システムの利用者は、事務従事者以外の者である場合がある。識別コードと主体認証情報については、このような利用者の別にかかわらず保護すべきであるが、事務従事者以外の者は事務情報セキュリティ管理基準及び本事務情報セキュリティ技術基準の適用範囲ではないため、それらの者に対しては、これを保護するよう注意喚起することが望ましい。

なお、事務情報セキュリティ管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) 主体認証機能の導入

(a) 部局技術責任者は、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、識別及び主体認証を行う機能を設けること。

解説：識別のための機能を設けることが技術的にできない情報システム（識別コード自体が存在せず、主体認証情報（パスワード）の設定のみ可能であるような装置等）は、例外措置として判断されることになる。その場合には、識別されないことによる影響について勘案し、必要に応じて代替あるいは追加の措置を講ずる必要がある。

主体認証の方式として、知識、所有、生体情報の３つの方法が代表的である。「知識」による主体認証とは、パスワード等、本人のみが知り得る情報を提示することにより、検証する方法である。「所有」による主体認証とは、IC カード等、本人のみが所有する機器等を主体認証処理に介在させることにより、検証する方法である。「生体情報」による主体認証とは、指紋や虹彩等、本人の生体的な特徴により、検証する方法である。

生体情報による主体認証を用いる場合には、その導入を決定する前に、この方式特有の誤認率と誤否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。この方式では、正当な本人に対して、本人の非によらない理由で、主体認証が正しくできなくなる場合があることを想定し、そのような場合の高等教育機関の事務の遂行への影響について検討してから導入を決定すること。

機微な情報へのアクセスであれば、本人であっても主体認証が解決できるまでアクセス不可能でよいとするか、あるいは、別の方式と組み合わせる等について考慮するとよい。なお、具体的な主体認証機能の設計に当たっては、当該情報システムに対して決定したセキュリティ要件（1.5.1.1(1)(b)を参照）を満たす必要がある。

(b) 部局技術担当者は、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、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。

(ア) 主体認証情報を保存する場合には、その内容の暗号化を行うこと。

(イ) 主体認証情報を通信する場合には、その内容の暗号化を行うこと。

(ウ) 保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更及び提供（入力）させる際に、暗号化が行われない旨を通知すること。

解説：主体認証情報の保存や通信を行う際に暗号化できない場合には、利用者は他の情報システムで用いていない主体認証情報を設定すべきである。その旨を利用者が判断できるように通知しなければならない。

保存又は通信を行う際に主体認証情報を暗号化できない情報システムでは、主体認証情報が漏えいする危険性がある。もしも、そのような問題が生じた場合に、そこで使われていた主体認証情報と同じものが他の情報システムでも使われた場合には、暗号化できる情報システムにおいても、不正に使われてしまうという二次被害を招きかねない。その危険性を低減するため、暗号化されない情報システムでの主体認証情報については、他の情報システムで用いていないものを利用者が設定する等の回避策をとる必要がある。そのため、利用者が暗号化されない旨を知る機会を得られるようにしておかなければならない。

したがって、暗号化できない情報システムにおいて、主体認証情報を入力させる際には、例えば、「この情報システムでは入力される情報が暗号化されません。他の情報システムで使用している主体認証情報（パスワード）を入力しないようにしてください。」等の警告を表示するようにすることが必要である。

(c) 部局技術責任者は、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、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、以下のいずれかの機能を設けること。

(ア) 利用者が定期的に変更しているか否かを確認する機能

(イ) 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

解説：定期的な変更を遵守事項とする場合には、それが実施されているか否かを確認できる機能を用意しておく必要がある。その機能によって確認作業を自動化することが技術的に困難な場合は、例外措置の手続を実施した上で、管理者が定期的にパスワードの変更を促すメールを利用者に送信し、利用者がこれに従ってパスワードを変更した旨を返信することで確認するといった代替措置の適用も考えられる。なお、

生体情報による主体認証方式のように、利用者本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。

(d) 部局技術責任者は、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、主体認証情報又は主体認証情報格納装置を他者に使用され、又は使用される危険性を認識した場合に、直ちに当該主体認証情報若しくは主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けること。

解説：主体認証情報自体の露呈、主体認証情報に関連する情報の露呈又はそれらが露呈した可能性について報告を受けた場合には、主体認証の停止、識別コードによる情報システムの利用停止のほか、主体認証情報の変更や別の主体認証方式の併用等の対策を講ずること。

(e) 部局技術責任者は、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、知識による主体認証方式を用いる場合には、以下の機能を設けること。

(ア) 利用者が、自らの主体認証情報を設定する機能

解説：知識による主体認証方式の場合には、本人による設定を可能にすることによって、以下の利点が期待できる。

・他者に設定された主体認証情報に比べ、本人が設定した主体認証情報の方が容易に記憶できる。

・本人以外の者が主体認証情報を設定する場合には、その設定者によるなりすましが懸念されるが、本人自身が設定することにより、そのおそれが少なくなる。

なお、例えば、運用上の理由等で他者による再設定を認めた場合には、同様に本人になりすますことは可能であるため、主体認証情報（パスワード）変更の通知機能によって、本人に設定が変更されたことについて通知することが望ましい。

(イ) 利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能

解説：部局技術責任者であっても、他者の主体認証情報を知ることができないようにする必要がある。部局技術責任者に悪意がなくとも、悪意のある第三者によってその管理者権限が奪取されてしまった場合には、全ての利用者の主体認証情報を知られてしまうおそれがあるため、不可逆の暗号化を用いる等により、部局技術責任者自らも、他者の主体認証情報を知ることができないような措置を講ずる必要がある。

(ウ) 主体認証情報を設定する時は、セキュリティ上の強度が指定以上となるように要求する機能

解説：安易な主体認証情報（パスワード）を設定すると、悪意のある第三者によって解読されてしまうため、必要なセキュリティ上の強度を持つようにする必要がある。

セキュリティ上の強度の指定については、次の要素を考慮する必要がある。

・パスワードに用いる文字の種類

・パスワードの桁数

・パスワードの有効期間

・アカウントをロックする方法

・アカウントのロックを解除する方法

・当該情報システムを利用する人数
・当該情報システムへログインする方法
・当該情報システムに保存される情報の格付　等
なお、本学外の人々・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、パスワード等のセキュリティ上の強度に関する設定例について記載があるため、参考にされたい。

(f) 部局技術責任者は、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、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項のうちその特性に応じて適用可能な要件を全て満たす主体認証方式を導入すること。
(ア) 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）
(イ) 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）
(ウ) 正当な主体が容易に他者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）
(エ) 主体認証情報が容易に複製できないこと。（複製の防止）
(オ) 部局技術担当者の判断により、ログオンを個々に無効化できる手段があること。（無効化の確保）
(カ) 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）
(キ) 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）
(ク) 主体に付与した主体認証情報を使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）
解説：代表的な方式である、知識、所有、生体情報による主体認証方式以外の方法を用いる場合の検討事項を列挙している。セキュリティ上の求められる強度や利便性等も考慮の上、方式を決定することを求める事項である。なお、これらの要件は、必ずしも全て充足することを求めるものではない。例えば、主体認証情報（パスワード）等による「知識」方式の場合には、要件（ウ)や(エ)を技術的に充足する必要はない。
また、上記の（ア）～（ク）以外に気づいた事項があれば、適宜追加することが望ましい。

(g) 部局技術責任者は、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、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。
(ア) 複数要素（複合）主体認証方式で主体認証を行う機能
解説：複数要素（複合）による主体認証方式を用いることにより、より強固な主体認証が可能となる。
これは、単一要素（単一）主体認証方式（「単一要素（単一）主体認証（single factor

authentication / single authentication）方式」とは、知識、所有、生体情報等のうち、単一の方法により主体認証を行う方式である。）の場合には、何らかの理由によって主体認証情報が露呈してしまった際には、不正にログオンされる可能性が非常に高くなってしまうが、複数要素（複合）主体認証方式の場合には、仮に一方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、不正にログオンされる可能性は依然低いと考えられるからである。

(イ) ログオンした利用者に対して、前回のログオンに関する情報を通知する機能

解説：識別コードによる前回のログオンに関する情報（日時や装置名等）を通知することで、本人の識別コードが他者によって不正に使われた場合に、本人が気付く機会を得られるようにすることを求める事項である。

(ウ) 不正にログオンしようとする行為を検知し、又は防止する機能

解説：通知によって本人が知る機会を得ること及び組織が状況を管理できること等が考えられる。例えば、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、その旨を本人に通知する、あるいは、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（アカウントをロックする）機能の付加が挙げられる。

なお、OS といった一般的に主体認証機能を有する機器やソフトウェア等を調達する場合には、当該機能を有する機器やソフトウェア等を選択することが望ましい。

(エ) 利用者が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能

解説：通知メッセージの例としては、以下のようなものがある。

・利用者が政府機関の情報システムへアクセスしようとしていること
・情報システムの使用が監視、記録される場合があり、監査対象となること
・情報システムの不正使用は禁止されており、刑法の罰則対象となること

(オ) 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、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

解説：一度使用した主体認証情報（パスワード等）の再利用を禁止することを求める事項である。なお、生体情報による主体認証方式のように、利用者本人であっても変更できない情報を用いる場合には、定期的に変更する必要はない。

(カ) 管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能

解説：管理者権限を有した識別コードを管理者グループで共用した場合には、そのログオン記録だけでは、共用している管理者のうち、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。そのため、管理者個人を特定することを目的として、非管理者権限の識別コードを本人に付与した上、その識別コードで最初にログオンした後に限り、管理者権限を有する共用識別コードに切り替えて管理者作業を実施することを可能とする必要がある。

なお、当該情報システムのオペレーティングシステムが Unix 系の場合には、一般利用者でログオンした後に 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 によるログオ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。

2.2.1.2 アクセス制御機能

趣旨（必要性）

主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。

これらのことを勘案し、本項では、アクセス制御に関する対策基準として、アクセス制御機能の導入、適正なアクセス制御についての遵守事項を定める。

なお、事務情報セキュリティ管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

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、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設けること。

解説：情報システムの利用者やそのグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式（任意アクセス制御）を利用すること。なお、「任意アクセス制御（DAC：Discretionary Access Control）」とは、主体が客体に設定したアクセス制御について、その設定がそれ以後継承されるかが任意である方式であり、この方式では、その客体にアクセス許可されている主体が別の客体を作成し複製等する際に、元のアクセス制御を新しい客体のアクセス制御として継承するかは当該主体の任意であり、変更が可能である。

(b) 部局技術責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。

(ア) 利用者及び所属するグループの属性以外に基づくアクセス制御機能の追加

解説：情報システムの利用者や所属するグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式のほか、情報システムの利用者やそのグループの属性以外に基づくアクセス制御を追加すること。

情報システムの利用者やそのグループの属性に基づくアクセス制御としては、例えば以下の方式が挙げられる。

・アクセス・コントロール・リスト（ＡＣＬ）制御

情報システムの利用者やそのグループの属性以外に基づくアクセス制御としては、例えば以下の方式が挙げられる。

・利用時間による制御

・利用時間帯による制御

・同時利用者数による制限
・同一ＩＤによる複数アクセスの禁止
・IP アドレスによる端末制限

(イ) 強制アクセス制御機能

解説：強制アクセス制御機能（MAC)の組み込みを導入することを求める事項である。
強制アクセス制御機能を備えたものとして、トラステッドＯＳやセキュアＯＳ等で実装したものもある。
なお、強制アクセス制御機能の組み込みを導入した場合、任意アクセス制御機能の組み込みができなくなるが、強制アクセス制御機能の方がより強力な機能のため、2.2.1.2(1)(a)を遵守していると考えられる。

(2) 適正なアクセス制御

(a) 部局技術責任者は、事務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付及び取扱制限に従って、アクセス制御を行うこと。

解説：共有ファイルサーバのアクセス制御のように、情報システムを事務従事者が利用する際に、自らがアクセス制御を行うことができない場合、情報システムの導入時及び運用時にアクセス制御を行うことを求めた事項である。例えば、要機密情報であれば、不適当な者から参照されないよう、読み取り制限の属性を付与し、完全性２情報であれば、不適当な者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。
また、事務従事者自らがアクセス制御を行うことが出来る場合、1.3.1.3(1)(b)の規程に基づき対策を行うこと。

2.2.1.3 権限管理機能

趣旨（必要性）

主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。

これらのことを勘案し、本項では、権限管理に関する対策基準として、権限管理機能の導入、識別コードと主体認証情報の付与管理についての遵守事項を定める。

なお、事務情報セキュリティ管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) 権限管理機能の導入

(a) 部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。

解説：権限管理を行う機能を設ける必要性があると認められた場合に、当該機能を情報シ

ステムに設けることを求める事項である。

(b) 部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を設けること。

(ア) 最少特権機能

解説：管理者権限を持つ識別コードを付与された者が、管理作業をする時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最少特権機能を、情報システムに設けることを求める事項である。

(イ) 主体認証情報の再発行を自動で行う機能

解説：情報システムの利用を開始している主体が、主体認証情報の再発行を要求した場合には、当該情報システムにおいて、その主体により重要な情報が既に作成されている可能性があることから、再発行する主体認証情報を他の者が知り得ないように、新規に主体認証情報を発行する場合に比べて、一層安全な機能を設けることを求める事項である。なお、再発行を自動化して他の者による操作を必要とすることなく主体認証情報を再発行することは、管理者による不正な操作が発生する機会を減らし、安全性を強化することができる。

(ウ) デュアルロック機能

解説：不正操作及び誤操作を防止するために、情報システムにデュアルロック機能を設けることを求める事項である。デュアルロック機能とは、行為に対して、少なくとも2名の者が操作しなければその行為を完遂できない方式のことである。

(2) 識別コードと主体認証情報の付与管理

(a) 権限管理を行う者は、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発行すること。

解説：情報システムにおける識別コード及び主体認証情報は、情報システムを利用する許可を得た主体に対してのみ、本人確認の上で初期発行することが重要である。また、識別コード及び主体認証情報の安全な初期配布方法について求める事項である。

(b) 権限管理を行う者は、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。

解説：識別コードを利用者に発行する際に共用識別コードか共用ではない識別コードかの別について通知することにより、それらの区別を利用者が独自に判断するようなことを防ぐための事項である。ただし、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。

(c) 権限管理を行う者は、管理者権限を持つ識別コードを付与（発行、更新及び変更を含む。以下この項において同じ。）する場合は、以下の措置を講ずること。

(ア) 業務又は業務上の責務に則した場合に限定すること

(イ) 初期設定の識別コードを変更できる場合には、識別コードを初期設定以外のものに変更すること

(ウ) 初期設定の主体認証情報を変更できる場合には、主体認証情報を初期設定以外のものに変更すること

(エ) ネットワークからのログインを制限すること

解説：管理者権限を持つ識別コードの取扱いは、情報システムのセキュリティ対策上、非常に重要な事項である。そのため、管理者権限を持つ識別コードは、業務又は業務上の責務に即して最小限の者へ付与すること。必要以上の者に過大な管理者権限を付与しないこと。また、管理者権限に係る識別コード及び主体認証情報の取扱いについては、2.2.1.1 の識別コード及び主体認証情報に係る遵守事項も踏まえること。なお、管理者権限を持つ識別コードについては、初期設定の識別コードの使用を禁止し、又は必要時以外は無効化することが望ましい。

「ネットワークからのログインを制限する」こととしては、例えば、電子証明書による端末認証、IP アドレス、MAC アドレス等により制限することが考えられる。

(d) 権限管理を行う者は、事務従事者が情報システムを利用する必要がなくなった場合には、当該事務従事者の識別コードを無効にすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不要な識別コードの有無を点検すること。

解説：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、これを無効にすることを求める事項である。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、無効の設定漏れを最小限にとどめることが期待できる。

(e) 権限管理を行う者は、事務従事者が情報システムを利用する必要がなくなった場合には、当該事務従事者に交付した主体認証情報格納装置を返還させること。

解説：識別コードの付与を最小限に維持し、かつ主体認証情報の不当な使用を防止するために、退職等により不要になった主体認証情報格納装置の回収を求める事項である。

(f) 権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与えるようにアクセス制御の設定をすること。また、人事異動等により、識別コードを追加し、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：業務又は業務上の責務に即して、必要となる者に限り、当該者の業務遂行に必要となるアクセス権のみを付与することを求める事項である。

(g) 権限管理を行う者は、以下のそれぞれの措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

(ア) 単一の情報システムにおいては、１人の事務従事者に対して単一の識別コードのみの付与

解説：１人の事務従事者に対して単一の識別コードのみを付与することを求める事項である。例えば、デュアルロック機能を備えた情報システムにおいては、１人の事務従事者に複数の識別コードでの主体認証を許してしまうと、デュアルロック機能による強化が万全とならなくなる。

(イ) 識別コードをどの主体に付与したかについての記録及び当該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

解説：識別コードの付与に係る記録は将来の障害・事故等の原因調査に備えて、不用意に消去しないことを求める事項である。その情報システムへの将来の調査が不要になったものについては、消去することになるが、その場合には、許可を得た上で消去しなければならない。情報システムの関係者だけの判断で、識別コードをどの主体

に付与したかを知るための記録を消去してはならない。

(ウ) ある主体に付与した識別コードをその後別の主体に対して付与することの禁止

解説：ある主体に付与した識別コードを再利用して別の主体に付与することを禁ずる事項である。このため、職位等に対応する識別コードが存在し、それを担当者が引き継いで使用する場合等、やむを得ずある主体に付与した識別コードをその後別の主体に対して付与する場合には、例外措置を申請する必要がある。そして、当該申請を許可するときは、その主体認証情報を新たに設定し、以前に使用していた主体による使用を禁ずるとともに、任意の時点で識別コードの利用主体を特定できるように、履歴を管理することが求められる。

なお、当該例外措置は、どの識別コードを誰が使用しているかを管理する ID マネジメントに係る重要事項であるため、部局総括責任者が許可・不許可を判断することが望ましい。

2.2.1.4 証跡管理機能

趣旨（必要性）

情報システムの利用においては、当該情報システムの制御及び管理の実効性を高め、また情報セキュリティに関する問題が発生した場合にこれに適切に対処するために、当該情報システムの動作及びその他必要な事象を記録し、事後にこれを調査する証跡管理を行う必要がある。また、証跡管理により、外部又は内部の者による不正利用又は過失行為を事前に抑止し、また事後に追跡することが可能となる。

これらのことを勘案し、本項では、証跡管理に関する対策基準として、証跡管理機能の導入、証跡の取得と保存についての遵守事項を定める。

なお、事務情報セキュリティ管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) 証跡管理機能の導入

(a) 部局技術責任者は、証跡を取得する必要があると部局総括責任者が認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。

解説：証跡を取得する機能を設ける必要があると認められた場合に、当該機能を情報システムに設けることを求める事項である。

(b) 部局技術責任者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。

解説：証跡の取得ができなくなった場合及び取得できなくなるおそれがある場合に対処する機能を情報システムに設けることを求める事項である。設けるべき機能としては、用意したファイル容量を使い切った場合に証跡の取得を中止する機能、古い証跡に

上書きをして取得を継続する機能、ファイル容量を使い切る前に操作する者に通知して対処をさせる機能等が考えられる。

なお、「必要に応じ」とは、定めた対処方法を実現するために必要な場合に限られる。

(c) 部局技術責任者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。

解説：不正アクセス、不正操作若しくは職務外利用又は誤操作を行った者にとって、その証跡は自己に不利益をもたらすものであることも考慮し、証跡が不当に消去、改ざんされることのないように、適切な格付を与えてこれを管理することを求める事項である。証跡の格付は、多くの場合に、機密性２情報又は機密性３情報で、要保全情報となるものと考えられる。

証跡は、訴訟において証拠として利用されることがある。その適切な取扱いを組織として定め、かつこれを遵守していることが、証跡に証拠力が認められる前提となることにも留意する必要がある。

また、証跡には情報システムを利用する者の行為が記録されるため、業務上の必要なくこれにアクセスすべきではない。

これらの理由で、証跡は、部局技術担当者を含む利用者が不当に消去、改ざん又はアクセスすることのないように、証跡を保存したファイルに適切なアクセス制御を適用する必要がある。

また、証跡として利用記録や監視記録を含めた場合には、対象となる利用者のプライバシーを侵害しないことにも配慮する必要があるため、アクセスできる者を制限することが重要になる。

(d) 部局技術責任者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、以下のそれぞれの機能を設けることの必要性の有無を検討し、必要と認めたときは、当該機能を情報システムに設けること。

(ア) 証跡の点検、分析及び報告を支援するための自動化機能

解説：取得した証跡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、その作業を自動化する機能を設けることを求める事項である。

証跡は、その量が膨大になるため、証跡の内容をソフトウェア等により集計し、時系列表示し、報告書を生成する等により、効率的かつ確実な点検、分析及び報告が可能となる。規模の大きい情報システムにおいては、複数のサーバ装置で取得した証跡をあわせた点検、分析及び報告の作業を支援する自動化も、必要に応じて導入する。

(イ) 情報セキュリティの侵害の可能性を示す事象を検知した場合に、監視する者等にその旨を即時に通知する機能

解説：情報セキュリティの侵害の可能性を示す事象が発生した場合に、迅速な対処を可能とするために、監視する者等に即時に通知する機能を設けることを求める事項である。

学外からの不正侵入の可能性、本学における持込み PC の情報システムへの接続等、通知すべき事象を定め、これを通知する機能を情報システムに組み込む。必要に応

じ、情報システムの利用者に即時に注意を促す仕組みを設けることも考えられる。

(2) 証跡の取得と保存

(a) 部局技術担当者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、情報システムに設けられた機能を利用して、証跡を取得すること。

解説：情報システムの運用中に、利用者の行動等の事象を証跡として取得することを求める事項である。部局技術担当者は、証跡を取得するために、必要な操作を行う必要がある。

(b) 部局技術担当者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。

解説：取得した証跡を適正に保存し、又は消去することを求める事項である。部局技術担当者は、証跡の保存期間が満了するまで当該証跡を保存する必要がある。

必要な期間にわたり証跡を保存するために、当該期間に取得する証跡を全て保有できるファイル容量としたり、証跡を適宜外部電磁的記録媒体に退避したりする方法がある。

なお、法令の規定により保存期間が定められている場合には、これにも従うこと。

(c) 部局技術担当者は、証跡を取得する必要があると部局総括責任者が認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処方法に基づいて対処すること。

解説：証跡の取得ができない場合又は取得できなくなるおそれがある場合の対処を定める事項である。

これらの場合には、部局技術担当者は、対処方法に定められた操作を行うことが求められる。対処方法に定められた操作としては、用意したファイル容量の残りが少ないことを通知された場合に、ファイルの切替えと証跡の退避を指示する操作等が想定される。

2.2.1.5 保証のための機能

趣旨（必要性）

事務情報セキュリティ管理基準及び本事務情報セキュリティ技術基準では、基本的なセキュリティ機能として、主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能の各項で具体的に遵守事項を規定している。しかし、情報が適切な状態であることを保証するためには、これらの機能によるセキュリティ対策より上位の機能やそれ以外の機能等による対策全般についても導入の必要性を検討することが重要である。こうした対策は、限られた情報システムに導入されることになると考えるが、基本的な対策ではないからといって最初から除外するのではなく、必要性の有無を確認し選択的に導入するという対応が適切である。

これらのことを勘案し、本項では、保証のための機能に関する対策基準を定める。

なお、事務情報セキュリティ管理基準 1.4.1.1 において識別コードと主体認証情報の管理等に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) 保証のための機能の導入

(a) 部局技術責任者は、保証のための対策を行う必要があると認めた情報システムにおいて、保証のための機能を設けること。

解説：保証のための対策を行う必要性があると認めた場合に、保証のための機能を情報システムに設けることを求める事項である。保証のための機能とは、2.2.1.1～2.2.1.4で示した遵守事項に限らない情報及び情報システムの安全性をより確実にするための機能のことをいう。これには大きく分けて以下の２つのものがある。

（ア）2.2.1.1～2.2.1.4 の機能とは異なる観点での保護を高めるための機能：

2.2.1.1～2.2.1.4 の機能は、主として情報及び情報システムの機密性、完全性及び可用性を保護することを目的とした機能である。これに加えて、情報及び情報システムの真正性（ Authenticity）の保護、否認防止（Non-Repudiation）のための機能等を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。

真正性の保護及び否認防止のための機能としては、例えば、電子署名及びタイムスタンプが挙げられる。

（イ）2.2.1.1～2.2.1.4 の機能及び上の（ア）の機能の動作が適正であることを確認するための機能：

2.2.1.1～2.2.1.4 の機能及び上の（ア）の機能は情報及び情報システムを保護するための機能といえる。それに対して（イ）は、それらの機能を監視して、異常やその兆候を検知し、検知された問題を解決する対処をすることによって、それらの機能の回復に備えるための機能である。これらの機能を設けることの必要性を、対象とする情報及び情報システムに対して検討し、必要な措置を講ずることによって、安全性をより確実にすることができる。

（イ）の機能としては、例えば、侵入検知システムやネットワーク監視等が挙げられる。

また、保証のための機能は、主体認証機能等のように個別のものではなく、複数の機能であったり、それら複数のものを組み合わせた機能であったりする場合もある。情報セキュリティをより高めるために必要となる機能を設けることで本遵守事項を達成することができる。

2.2.1.6 暗号と電子署名（鍵管理を含む）

趣旨（必要性）

情報システムの利用においては、当該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に、情報の暗号化及び電子署名が有効とされている。この際、あらかじめ定めた暗号アルゴリズム及び方法に基づき、暗号及び電子署名を適切な状況で利用する必要がある。

これらのことを勘案し、本項では、暗号化及び電子署名に関する対策基準として、暗号化機能及び電子署名機能の導入、暗号化及び電子署名に係る管理についての遵守事項を定める。

なお、事務情報セキュリティ管理基準 1.4.1.1 において識別コードと主体認証情報の管理等

に関する対策基準を、1.5.2.4 において主体認証・アクセス制御・権限管理・証跡管理・保証等の必要性判断等に関する対策基準を定めている。

遵守事項

(1) 暗号化機能及び電子署名機能の導入

(a) 部局技術責任者は、要機密情報（書面を除く。以下この項において同じ。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。

解説：暗号化を行う機能を情報システムに付加する前提として、部局技術責任者は、各情報システムについて、取り扱う情報の機密性の程度から暗号化を行う機能を付加する必要性の有無を検討しなければならない。

(b) 部局技術責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。

解説：情報の機密性の程度から暗号化を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項である。

(c) 部局技術責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与及び検証を行う機能を付加する必要性の有無を検討すること。

解説：電子署名の付与及び検証を行う機能を情報システムに付加する前提として、部局技術責任者は、各情報システムについて、取り扱う情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与及び検証を行う機能を付加する必要性の有無を検討しなければならない。

(d) 部局技術責任者は、電子署名の付与又は検証を行う必要があると認めた情報システムには、電子署名の付与又は検証を行う機能を設けること。

解説：情報の完全性及び情報提供者の真正性確認の程度から電子署名の付与又は検証を行う機能を付加する必要性が認められる場合に、当該機能を情報システムに設けることを求める事項である。

(e) 部局技術責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、以下のそれぞれの措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

(ア) 暗号モジュールの交換可能なコンポーネント化による構成

解説：選択したアルゴリズムが危殆化した場合を想定し、暗号モジュールを交換可能なコンポーネントとして構成するため、設計段階からの考慮を求める事項である。そのためには、暗号モジュールのアプリケーションインターフェイスを統一しておく等の配慮が必要である。

(イ) 複数のアルゴリズムを選択可能にする構成

解説：選択したアルゴリズムが危殆化した場合を想定し、設定画面等によって、当該アルゴリズムを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等を、情報システムに設けることを求める事項である。

(ウ) 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、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主体認証情報等が安全に保護された製品を使用するため、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の選択

解説：アルゴリズムの実装状況及び鍵等の保護状況を確認するに当たり、ISO/IEC 19790に基づく暗号モジュール試験及び認証制度による認証を取得している製品を選択することを求める事項である。

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ずる等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ずる等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。

なお、「適切に実装されている」とは、アルゴリズム自体の安全性だけではなく、疑似乱数の推測、鍵情報の一部露呈等の脅威に対応して実装していることをいい、その確認には、独立行政法人 情報処理推進機構（IPA)により運用されている暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）等が利用可能である。

(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の耐タンパー性を有する暗号モジュールへの格納

解説：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、技術的な対策等に加え、物理的対策を講ずることを求める事項である。鍵を格納する電磁的記録媒体が盗難され、鍵が開封される等しても、鍵情報が外部へ漏えいしない仕組みが必要である。

この場合、耐タンパー性を有するとは、例えば、 JIS X 19790:2007 7.5 物理的セキュリティ（ISO/IEC 19790:2006）の規定に照らし合わせると、他のセキュリティ対策との組み合わせによりレベル２以上を選択することが可能であるが、他の組み合わせがない場合、レベル３以上が相当する。

(2) 暗号化及び電子署名に係る管理

(a) 部局技術責任者は、電子署名の付与を行う必要があると認めた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提供すること。

解説：電子署名の付与を実効的に機能させるために、付与された電子署名を受け取った者が、その電子署名の正当性を容易に検証できるようにすることを求める事項である。

通常、付与された電子署名を検証するためには、署名時に使用した署名鍵に対応する検証鍵が必要であるが、この検証鍵自体の真正性を保証するためには、本学の窓口での直接提供、信頼できる機関による電子証明書の発行、検証鍵に付随する固有の情報（フィンガープリント等）の公開等の方法がある。

なお、電子署名の正当性を検証するための情報又は手段については、当該電子署名が付与された情報が真正なものであることを証明する必要がある間、提供することとなる。例えば、電子署名の有効期限内にアルゴリズムの危殆化が発生し、又は有効期限を超えるため、別の電子署名を付与する場合にあっては、これら全ての電子署名の正当性を検証するための情報又は手段を提供する必要がある。

(b) 部局技術責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。

解説：様々な機関から提供されているアルゴリズムの危殆化に関する情報を適宜入手しておくことを求める事項である。
例えば、CRYPTREC を始めとする暗号技術の有識者による発表に関心を払うことが必要である。

2.2.2 情報セキュリティについての脅威

2.2.2.1 セキュリティホール対策

趣旨（必要性）

セキュリティホールは、情報システムを構成する電子計算機及び通信回線装置上で利用しているソフトウェアに存在する可能性があり、そのセキュリティホールを攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、不正プログラム感染の原因になる等、情報システム全体のセキュリティを維持する上で大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、政府の社会的な信用が失われるおそれがある。これらのリスクを回避するため、セキュリティホールへの対処は迅速かつ適切に行わなければならない。

これらのことを勘案し、本項では、セキュリティホールに関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1) 情報システムの構築時

(a) 部局技術責任者は、電子計算機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セキュリティホールの対策を実施すること。

解説：電子計算機及び通信回線装置の設置又は運用開始時に、その時点において、当該機器上で利用しているソフトウェアのセキュリティホール対策が完了していることを求める事項である。

(b) 部局技術責任者は、公開されたセキュリティホールの情報がない段階においても電子計算機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。

解説：公開されたセキュリティホールへの対策だけでなく、明らかになっていないセキュリティホールについても対策を求める事項である。
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。

(2) 情報システムの運用時

(a) 部局技術担当者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、公開されたセキュリティホールに関連する情報を適宜入手すること。

解説：セキュリティホールに関連する情報の収集を求める事項である。セキュリティホールに関連する情報とは、セキュリティホールの原因、影響範囲、対策方法、セキュ

リティホールを悪用するツールの公開の有無等が挙げられる。
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、定期的にセキュリティホール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、当該機能がない場合は、適時調査を行う必要がある。

(b) 部局技術責任者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、セキュリティホールに関連する情報を入手した場合には、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を策定すること。
(ア) 対策の必要性
(イ) 対策方法
(ウ) 対策方法が存在しない場合の一時的な回避方法
(エ) 対策方法又は回避方法が情報システムに与える影響
(オ) 対策の実施予定
(カ) 対策試験の必要性
(キ) 対策試験の方法
(ク) 対策試験の実施予定

解説：セキュリティホールが情報システムにもたらすリスクを分析し、対策計画の策定を求める事項である。「対策試験」とは、セキュリティホール対策の実施による情報システムへの影響の有無について、他の情報システムを用いて試験することをいう。

(c) 部局技術担当者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。

解説：セキュリティホール対策計画に基づいて対策が実施されることを求める事項である。

(d) 部局技術担当者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者を含む事項を記録すること。

解説：セキュリティホール対策の実施記録の様式は問わないが、実施日、実施内容及び実施者は必ず記録しなければならない必須事項である。これらの事項のほかに必要事項があれば、適宜追加する。

(e) 部局技術担当者は、信頼できる方法でパッチ又はバージョンアップソフトウェア等のセキュリティホール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。）を入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

解説：入手した対策用ファイルに悪意あるコードが含まれている可能性を考慮し、対策用ファイルを信頼できる方法で入手することを求める事項である。
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のダウンロード又は郵送された外部電磁的記録媒体を利用して入手する方法が挙げられる。また、改ざん等について検証することができる手段があれば、これを実行する必要がある。

(f) 部局技術担当者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。

解説：電子計算機及び通信回線装置上のセキュリティホール対策及びソフトウェア構成の状況を確認し、対策を担保するための事項である。
「セキュリティホール対策及びソフトウェア構成」とは、導入されているソフトウェアの種類及びこれらのセキュリティホール対策状況のことである。調査の間隔については、短いほど効果が高いため、可能な範囲で短くすることが望ましい。「不適切な状態」とは、パッチが適用されていない等、セキュリティホール対策が講じられていない状態のことである。

(g) 部局技術責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、他の部局技術責任者と共有すること。

解説：公開されたセキュリティホールに関連する情報の入手及びセキュリティホール対策を効果的に実施するために、部局技術責任者間の連携を求める事項である。

2.2.2.2 不正プログラム対策

趣旨（必要性）

不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の要機密情報を漏えいさせることから機密性に対する脅威ともなる。

さらに、不正プログラムに感染した情報システムは、他の情報システムの再感染を引き起こす危険性のほか、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危険性等他者に対するセキュリティ脅威の原因となり得る。

これらのことを勘案し、本項では、不正プログラムに関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1) 情報システムの構築時

(a) 部局技術責任者は、電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。以下この項において同じ。）にアンチウイルスソフトウェア等を導入すること。

解説：動作可能なアンチウイルスソフトウェア等が存在する電子計算機について、アンチウイルスソフトウェア等を導入することを求める事項である。なお、多くのメインフレームシステム並びにオペレーティングシステム及びアプリケーションを搭載していない電子計算機については、動作可能なアンチウイルスソフトウェアが存在しないため、本遵守事項は適用されない。ただし、アンチウイルスソフトウェア等が新たにサポートを開始する場合には、速やかな導入が求められることから、部局技術責任者は、該当する電子計算機の把握を行っておくとともに、アンチウイルスソフトウェア等に関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。
なお、アンチウイルスソフトウェア等には、他社製品・技術だけでなく、同一社の製品でもアンチウイルスソフトウェアの他、パーソナルファイアウォールやスパイウェア対策ソフト等も含む。

(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アンチウイルスソフトウェア等により不正プログラム対策を実施すること。

解説：電子計算機以外の想定される感染経路に対しても、不正プログラム対策の実施を求める事項である。

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、複数の感染経路を想定した対策が必要である。

(c) 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において、複数の種類のアンチウイルスソフトウェア等を組み合わせて導入する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：複数の種類のアンチウイルスソフトウェア等を導入することにより効果的な不正プログラム対策の実施を求める事項である。

アンチウイルスソフトウェア等は、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、アンチウイルス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が発生する可能性を低減させるため、感染経路において異なる製品や技術を組み合わせ、どれか１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必要がある。例えば、メールサーバに導入するアンチウイルスソフトウェアと端末に導入するアンチウイルスソフトウェアを異なるパターンファイルを用いた製品にすること等が考えられる。

(d) 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において、拡散を防止する措置の必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：ネットワーク及び外部電磁的記録媒体を経由した感染拡大を防止することを求める事項である。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、不正プログラム定義ファイル又はパッチ適用等が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情報システムや、通信に不正プログラムが含まれていることを検知すると、その通信を検知したネットワークからの通信を遮断する情報システムの導入等が挙げられる。また、外部電磁的記録媒体を経由した感染拡大の防止策としては、例えば、自動再生機能の無効化、外部電磁的記録媒体の電子計算機接続時の手動検索、及びアンチウイルスソフトウェアの自動検査機能の有効化等が挙げられる。

(2) 情報システムの運用時

(a) 部局技術担当者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、事務従事者にその対処の実施に関する指示を行うこと。

解説：不正プログラムに対し特段の対処が必要な場合に実施することを求める事項である。

「特段の対処が必要な場合」とは、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アンチウイルスソフトウェア等に用いる定義ファイルが配布されない等、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が挙げられる。

(b) 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、その見直しを行うこと。

解説：1.5.2.8(1)(a)の規定による全学実施責任者が整備する規程に基づいた対策の状況及び本項の対策の状況を適宜把握し、問題点が発見された場合は改善することを求める事項である。

2.2.2.3 サービス不能攻撃対策

趣旨（必要性）

インターネットを経由して外部に提供しているサービスを実現する電子計算機、並びにそのアクセスに利用される通信回線及び通信回線装置は、利用者が自由にアクセス可能である利便性を確保するために、サービス不能攻撃により、通常の利用者がサービスを利用できなくなるといった可用性に対するリスクがある。

このため、インターネットに接続しているサーバ装置、並びにそのアクセスに利用される通信回線及び通信回線装置については、高い可用性を維持するための対策が必要となる。この対策については、ソフトウェアのセキュリティホールを悪用する攻撃に対するものと、大量のアクセスによる攻撃に対するものに大別され、両者とも実施する必要がある。

これらのことを勘案し、本項では、サービス不能攻撃に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1) 情報システムの構築時

(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電子計算機、通信回線装置又は通信回線を有す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電子計算機及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。

解説：電子計算機や通信回線装置が設けている機能を有効にすることを求める事項である。対策としては、例えば、3-way handshake 時のタイムアウトの短縮、各種 Flood 攻撃への防御機能、アプリケーションゲートウェイ機能、パケットフィルタリング機能を利用すること等が挙げられる。

(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に影響が最小となるように情報システムを構築すること。

解説：要安定情報を取り扱う情報システムがサービス不能攻撃を受けた場合の影響を分析し、情報システムを構築することを求める事項である。影響としては、通信回線の帯域圧迫によるアクセス障害や、サーバの処理能力低下等が考えられる。このため、例えば、サービス不能攻撃を受けたことを検出した場合には、即座に情報システムを外部ネットワークより遮断する、通信回線の通信量に制限をかける等といった手段を有する情報システムを構築する必要がある。

(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電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法及び監視記録の保存期間を定めること。

解説：サービス不能攻撃に関する監視対象の特定と監視方法及び監視記録の保存期間を定めることを求める事項である。

インターネットからアクセスされるサーバ装置、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サーバ装置、通信回線装置及び通信回線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、負荷の定量的な把握がある。監視方法は多種多様であるため、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。

(d) 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、電子計算機や通信回線装置における対策だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者と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こと。

解説：部局技術責任者が、電子計算機や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、学外へ接続する通信回線を提供している事業者へも対策の協力を依頼できる体制を整備することを求める事項である。

(e) 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、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響を排除し、又は低減する措置の必要性の有無を検討し、必要と認めたときは、対策措置を講ずること。

解説：通信回線については、通信量の制限や通信の遮断が有効であり、サービス不能攻撃の影響を排除し、又は低減するために必要な装置の導入を求める事項である。例えば、巧みに偽装したパケットや正規の送信元アドレスを使用した巧妙な DDoS 攻撃を抑制するには、電子計算機及び通信回線装置が持つ既存のセキュリティ対策機能に加え、サービス不能攻撃に係る通信の遮断等、インターネットに接続している通信回線を提供している事業者による対策又はサービス不能攻撃の影響を排除し、又は低減することのできる専用の対策装置の導入が挙げられる。

なお、電子計算機や通信回線装置が設け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、インターネットに接続している通信回線を提供している事業者による対策又は対策装置を導入する必要性があると判断すること。

(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については、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保することの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：大量のアクセスによる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における対処を効果的に実施するための事項である。

例えば、対処としては、サービス提供に利用している通信回線等がサービス不能攻撃により過負荷状態に陥っていても、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に設置されている対策装置を操作できる手段を確保することが挙げられる。より具体的には、管理者が当該装置等を操作するための電子計算機及び通信回線等を、サービス提供に利用している電子計算機及び通信回線等とは別に用意すること等が挙げられる。

(g) 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、サービス提供に必要な電子計算機、通信回線装置又は通信回線を冗長構成にすることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：サービス不能攻撃が発生した場合、サービスを提供する電子計算機、通信回線装置及び通信回線を代替電子計算機、代替通信回線装置又は代替通信回線に切り替えることにより、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を求める事項である。

サービス不能攻撃の検知及び代替計算機等への切替えは短時間にできるようにすることが必要である。

(2) 情報システムの運用時

(a) 部局技術担当者は、要安定情報を取り扱う情報システムについては、監視方法が定められている場合は、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。

解説：電子計算機、通信回線装置及び通信回線の通常時の状態を記録し把握することを求める事項である。

電子計算機、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、季節変動を検討した上で記録を一定期間保存する。

2.2.2.4 踏み台対策

趣旨（必要性）

インターネット等の学外の通信回線に接続された情報システムは、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として、意図しない用途に使われてしまうこと、いわゆる、踏み台とされてしまうおそれがある。踏み台とされた情報システムは、学外に迷惑をかけるだけにとどまらず、例えば、当該情報システムが提供していたサービスを利用者が利用できないという可用性に対する水準の低下や、学内の他の情報システムに対するセキュリティ脅威の原因ともなり得る。これらを防ぐためには、本学が意図しない目的で本学の情報システムが使われないようにすることが必要である。

これらのことを勘案し、踏み台防止に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1) 情報システムの構築時

(a) 部局技術責任者は、情報システム（インターネット等の学外の通信回線に接続される電子計算機、通信回線装置又は通信回線を有する情報システムに限る。以下この項に

おいて同じ。）が踏み台として使われることを防止するための措置を講ずること。

解説：電子計算機等に対し、踏み台になることを避けるための対処の実施を求める事項である。

対策としては、アンチウイルスソフトウェア等の導入、セキュリティホールの対処、不要なサービスの削除、フィルタリング機能の有効化、不審なプログラムの実行禁止、アンチウイルスソフトウェア等で検出されないボットの通信の監視等が挙げられる。

(b) 部局技術責任者は、情報システムを踏み台として使われた場合の影響が最小となるように情報システムを構築すること。

解説：管理する情報システムを踏み台として使われた場合の影響を分析し、情報システムを構築することを求める事項である。影響としては、通信回線の帯域圧迫によるアクセス障害や、サーバの処理能力低下等が考えられる。このため、踏み台として使われたことを検出した場合には、即座に情報システムを外部ネットワークより遮断する、問題が発生している電子計算機のみ切り離す、等といった手段を有する情報システムを構築する必要がある。

(c) 部局技術責任者は、情報システムが踏み台になっているか否かを監視するための監視方法及び監視記録の保存期間を定める必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：踏み台に関する監視方法及び監視記録の保存期間を定めることを求める事項である。

「監視方法」については、意図しない稼動負荷やインターネットへの通信の有無の把握、電子計算機に意図しない処理を行わせる命令の有無の監視等がある。監視方法は多種多様であるため、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。

(2) 情報システムの運用時

(a) 部局技術担当者は、監視を行う情報システムについては、定められた監視方法に従って情報システムを監視し、その記録を保存すること。

解説：情報システムの通常稼働時の状態を記録し把握することを求める事項である。

情報システム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、季節変動を検討した上で記録を一定期間保存する。

2.2.2.5 標的型攻撃対策

趣旨（必要性）

標的型攻撃は、複数の攻撃手法を組み合わせ、ソーシャルエンジニアリングにより特定の組織や個人を狙い執拗に行われる攻撃である。この攻撃を完全に検知及び防御することは困難であり、かつ、端末やサーバ装置への侵入後、情報システム内に潜伏し、バックドアの設置等の攻撃を行うものもある。

本学で管理している情報システムの内部に不正侵入された場合、組織内部の情報が漏えい

する等により、本学の社会的な信用が失われるおそれがある。また、攻撃のあった部局から窃取された情報が学外への攻撃に利用される場合もある。

そのため、本学の外部と内部の境界で攻撃を検知及び防御する対策だけでなく、本学の情報システム内の通信及び外部への通信の監視・制御等を行うことにより、情報システム内部からの攻撃の検知及び被害の拡大を防止するための対策も講ずる必要がある。

これらのことを勘案し、本項では、標的型攻撃に関する対策基準として、情報システムの構築時及び運用時についての遵守事項を定める。

遵守事項

(1) 情報システムの構築時

(a) 部局技術責任者は、情報システムについて標的型攻撃による不正プログラムの侵入及び感染拡大等を防止するための措置を講ずること。

解説：電子計算機等に対し、情報システムの構築時における標的型攻撃による不正プログラムの侵入及び感染拡大等への対処の実施を求める事項である。標的型攻撃への対策は、個々のサーバ装置や端末だけではなく、情報システムのネットワーク全体の通信要件も対象となる。そして、当該通信要件に従って、アクセス制御及び経路制御を含むネットワークシステム全体の対策を講ずる必要がある。

対策としては、例えば、以下のものが挙げられる。

（ア）通信回線における対策

・ファイアウォール等を利用した通信要件の制限

・侵入検知システム等による不正な通信の検知・遮断

・端末間、グループ化された電子計算機間の通信の制限

・学内通信回線上の端末から学外通信回線への通信はプロキシを経由させる等の経路制御　等

（イ）端末及びサーバ装置共通の対策

・管理者権限を持つ識別コードの個別の付与（管理者権限を持つ既定の識別コードの付与の禁止又は必要時以外の無効化）

・管理者権限を持つ識別コードの業務に必要な権限のみの付与

・指定回数以上の主体認証情報の誤入力後の、一定期間の当該識別コードの無効化

・主体認証情報を設定する時の、セキュリティ上の強度が指定以上となるように要求する機能の設置

・アンチウイルスソフトウェア等の導入

・不正プログラム定義ファイル利用型アンチウイルスソフトウェアとふるまい検知型アンチウイルスソフトウェアの併用

・不正プログラムの自動検査機能の有効化

・セキュリティホールの対処

・不要なサービスの削除

・不審なプログラムの実行禁止

・許可していない外部電磁的記録媒体及び端末の接続制限

・送信ドメイン認証等を利用した、受信した電子メールのなりすましの有無の確認

等

（ウ）端末における対策

・パーソナルファイアウォールの導入　等

（エ）サーバ装置における対策

・重要な情報を保存しているサーバ装置へのログイン可能な端末の制限

・重要な情報を保存しているサーバ装置上のセキュリティ状態の監視　等

なお、不正プログラムの自動検査機能の有効化といった不正プログラム感染防止のための日常的実施事項については 1.5.2.8、セキュリティホールへの対処といったセキュリティホールについての対策については 2.2.2.1、アンチウイルスソフトウェア等の導入といった不正プログラム対策については 2.2.2.2、サーバ装置にログイン可能な端末の制限や不要なサービスの削除といったサーバ装置や端末に関する対策については 2.3.2.1～2.3.2.3、電子メールに関する対策については 2.3.3.1 及びファイアウォールや侵入検知システム等の導入といった通信回線に関する対策については 2.3.4.1～2.3.4.3 を参照すること。

(b) 部局技術責任者は、インターネット等の学外の通信回線に接続される情報システムについて標的型攻撃に利用されることを防止するための措置を講ずること。

解説：インターネット等の学外の通信回線に接続される電子計算機等に対し、標的型攻撃に利用されることへの対処の実施を求める事項である。

対策としては、送信ドメイン認証を利用した送信する電子メールの送信元ドメイン名のなりすまし防止、政府ドメイン名の利用及び学外に提供するソフトウェア等への電子証明書の付与、当該電子計算機が標的型攻撃に利用されているか否かの監視等が挙げられる。

なお、学外に提供するソフトウェア等への電子証明書の付与といった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対策については 1.5.2.6、ドメイン名の使用に関する対策については 1.5.2.7、当該電子計算機の監視といった踏み台対策については 2.2.2.4 及び電子メールに関する対策については 2.3.3.1 を参照すること。

(2) 情報システムの運用時

(a) 部局技術責任者は、情報システムについて標的型攻撃による不正プログラムの侵入及び感染拡大等を防止するための措置を講ずること。

解説：電子計算機等に対し、情報システムの運用時における標的型攻撃による不正プログラムの侵入及び感染拡大等への対処の実施を求める事項である。

対策としては、例えば、以下のものが挙げられる。

（ア）通信回線における対策

・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の監視

・学内通信回線上の電子計算機同士で送受信される通信内容の監視

・アンチウイルスソフトウェア等で検出されないボットの通信の監視　等

（イ）端末及びサーバ装置共通の対策

・アンチウイルスソフトウェア等における不正プログラム定義ファイルの最新の状態の維持

・定期的な全ての電子ファイルに対する不正プログラムの有無の確認
・セキュリティホールに関連する情報の収集及びリスク分析した上での対策実施
・ログの取得及び解析　等
（ウ）その他
・標的型攻撃に関する訓練の実施
・送信ドメイン認証を利用した、送信する電子メールの送信元ドメイン名のなりすまし防止　等
なお、不正プログラム定義ファイルの最新の状態の維持や定期的な全ての電子ファイルに対する不正プログラムの有無の確認といった不正プログラム感染防止のための日常的実施事項については 1.5.2.8、セキュリティホールに関する情報の収集といったセキュリティホールに関する対策については 2.2.2.1、電子メールに関する対策については 2.3.3.1 及び通信内容の監視といった通信回線に関する対策については 2.3.4.2 を参照のこと。

第 2.3 部　情報システムの構成要素についての対策

2.3.1 施設と環境

2.3.1.1 情報取扱区域のクラス別管理及び利用制限

趣旨（必要性）

悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる設置環境にある場合においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改ざん等が行われるおそれがある。また、その他にも、設置環境に関する脅威としては、自然災害の発生による情報システムの損傷や情報の紛失等が発生するおそれもある。

このように施設全体や区域ごとに様々な脅威が考えられるため、それぞれの区域に応じた管理と想定される利用形態に応じた情報の取扱いを行う必要がある。

これらのことを勘案し、本項では、情報取扱区域のクラス別管理及び利用制限の対策基準として、立ち入る者を制限するための管理対策、立ち入る者を許可する際の管理対策、訪問者がある場合の管理対策、設置する設備の管理対策、作業がある場合の管理対策、立ち入る者を制限するための利用制限対策、物品の持込み、持ち出し及び利用についての利用制限対策、荷物の受渡しについての利用制限対策並びに災害及び障害への対策に関する遵守事項を定める。

遵守事項

(1) 立ち入る者を制限するための管理対策

(a) 区域情報セキュリティ責任者は、立ち入る者を制限するための管理対策として、以下の事項について、別表 1 に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

(ア) 不審者を立ち入らせない措置

解説：要管理対策区域への不審者の立入りを防止し、要管理対策区域のセキュリティを確保するための事項である。

措置としては、身分を確認できる物の提示の義務化、要管理対策区域の所在の表示の制限等が挙げられる。

(イ) 要保護情報を取り扱う情報システムについては、物理的に隔離し、立入り及び退出を管理するための措置

解説：電子計算機及び通信回線装置が設置された区域を、物理的隔離及び立入り及び退出の管理によりセキュリティを確保するための事項である。

措置としては、壁、施錠可能な扉、パーティション等で囲むことで区域を隔離し、当該区域が無人になる際には扉を施錠する、当該鍵の貸し出しを管理するといった措置が挙げられる。なお、要管理対策区域では、扉を開放したまま無人の状態にしてはならない。

(2) 立ち入る者を許可する際の管理対策

(a) 区域情報セキュリティ責任者は、立ち入る者を許可する際の管理対策として、以下の事項について、別表 1 に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

(ア) 要管理対策区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置

解説：要管理対策区域へ立ち入る者が立入りを許可された者であるかの確認を実施することで、許可されていない者の立入りを排除するための事項である。

なお、立入りを許可された者であるかの確認のために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等が望ましい。

(イ) 要管理対策区域から退出する者が立入りを許可された者であるかの確認を行うための措置

解説：立ち入った者の退出を把握するための事項である。

(ウ) 立入りを許可された者が、立入りを許可されていない者を要管理対策区域へ立ち入らせ、及び当該区域から退出させない措置

解説：要管理対策区域の立入り及び退出時に立入りを許可された者であるかどうかの確認を確実に実施するための事項である。

対策としては、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。

(エ) 継続的に立ち入る者を許可する手続の整備

解説：文書を整備することで、要管理対策区域へ継続的に立ち入る者を把握するための事項である。立入期間については、例えば、月又は年単位といった期間が考えられる。

なお、文書には、その者の氏名、所属、立入許可日、立入期間及び許可事由を含む事項を記載すること。

(オ) 継続的に立入りを許可された者に変更がある場合の手続の整備

解説：立入りを許可された者に変更がある場合に変更手続をとることで、継続的に立ち入る者を把握するための事項である。変更の手続きには、変更の内容を前事項の文書へ反映することが挙げられる。

また、変更内容についての記録を保存し、後で参照できるようにしておく必要がある。

(カ) 全ての者の要管理対策区域への立入り及び当該区域からの退出を記録し及び監視するための措置

解説：要管理対策区域への立入り及び当該区域からの退出の記録、監視を行い、区域のセキュリティが侵害された場合に追跡することができるようにするための事項である。

「記録し及び監視する」とは、警備員又は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。

(3) 訪問者がある場合の管理対策

(a) 区域情報セキュリティ責任者は、訪問者がある場合の管理対策として、以下の事項について、別表１に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

(ア) 訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置

解説：訪問者の身元を確認するための事項である。確認方法としては、例えば、訪問者に必要事項を記入させ、名刺又は社員証等と記入された内容とを照合する方法が挙げられる。

(イ) 訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置

解説：訪問記録の作成を求める事項である。

(ウ) 訪問相手の事務従事者が訪問者の要管理対策区域への立入りについて審査するための手続の整備

解説：訪問者の要管理対策区域への立入りについて、訪問相手の事務従事者が審査するための手続を整備することを求める事項である。

手続としては、「警備員等が訪問相手の事務従事者に連絡し、訪問者の立入りについて審査する」、「訪問相手の事務従事者が、区域との境界線まで迎えに行き審査する」等の方法が挙げられる。なお、警備員等に対しては、必要に応じ、立入りの制限等について予め周知しておくこと等が考えられる。

(エ) 訪問者の立ち入る区域を制限するための措置

解説：訪問者が許可されていない要管理対策区域へ立ち入らないようにすることを求める事項である。措置の例としては、扉を施錠し許可された者のみが開閉可能にすることや警備員による訪問者の確認等の方法が挙げられる。

(オ) 訪問相手の事務従事者による訪問者に付き添う措置

解説：訪問者が許可されていない要管理対策区域へ立ち入らないように事務従事者が監視することを求める事項である。

(カ) 訪問者と継続的に立入りを許可された者とを外見上判断できる措置

解説：継続的に立入りを許可された者と訪問者を区別するための事項である。

これにより、許可されていない要管理対策区域への訪問者の立入りが検知できる。

対策としては、訪問者用の入館カードを作成し掲示を求める、訪問者の入館カード用ストラップの色を変える等が挙げられる。貸与した物は、訪問者の退出時に回収する必要がある。

(4) 設置する設備の管理対策

(a) 区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムについては、別表１に従って、クラスの区分に応じて、設置及び利用場所が確定している電子計算機及び通信回線装置の盗難及び当該場所からの不正な持ち出しを防止するための措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

解説：設置場所が固定された電子計算機に関して、盗難及び不正な持ち出しを防止するための事項である。

「設置及び利用場所が確定している」とは、サーバ装置及び据置き型 PC のように、設置及び利用する場所が固定され、他の場所で利用することがないという意味である。

対策としては、端末であればセキュリティワイヤーによる固定、サーバ装置であればサーバラックへの設置及び当該サーバラックの施錠、施設からの退出時における持ち物検査等が挙げられる。なお、重要システムを設置している場合やサーバ室に設置している複数のサーバラックの運用主体が異なる場合、サーバラックの鍵を適切に管理すること等が考えられる。

通信回線装置に係る対策としては、基幹の通信回線装置（ファイアウォール、ルータ、レイヤ３スイッチ、レイヤ２スイッチ等）であればサーバラックへの設置及び当該サーバラックの施錠、終端の通信回線装置（レイヤ２スイッチ等）であれば床下への埋設又は施錠できる場所への機器設置等が挙げられる。なお、学外通信回線と学内通信回線を結ぶルータを回線事業者が所有している場合は、契約等において不正な持ち出しを防止するための措置を講ずるよう求めることなどが考えられる。

(b) 区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置の設置に係る管理対策として、以下の事項について、別表１に従って、クラスの区分に応じた措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

(ア) 電子計算機及び通信回線装置を設置する情報取扱区域を物理的に隔離するための措置

解説：電子計算機及び通信回線装置を設置する情報取扱区域が隣接する低いクラスと隔離されないことにより、安全性が確保できないことを防ぐための措置を求める事項である。

(イ) 電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置

解説：電子計算機に接続されたディスプレイ、通信回線装置のメッセージ表示用ディスプレイ等を許可のない第三者に見られないように対策を実施することを求める事項である。

対策としては、偏光フィルタの利用等が挙げられる。

(ウ) 情報システムで利用する電源ケーブル及び通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置

解説：電源ケーブルの損傷及び通信ケーブルからの通信の盗聴等の脅威から、情報システムを保護するための事項である。

対策としては、ケーブルの床下への埋設、ケーブルのナンバリング等が挙げられる。

(エ) 情報システムから放射される電磁波による情報漏えい対策の措置

解説：ディスプレイケーブル等から生ずる電磁波による情報漏えいのリスクについて対策を講ずるための事項である。

具体的には、電磁波軽減フィルタの利用等が挙げられる。

(5) 作業がある場合の管理対策

(a) 区域情報セキュリティ責任者は、別表１に従って、クラスの区分に応じて、要管理対

策区域内での作業を監視するための措置を講ずること。なお、個別の管理対策を決定する場合は、当該個別管理についても講ずること。

解説：要管理対策区域内での作業を監視するための事項である。
第三者による立会いや、監視カメラの導入等が挙げられる。

(6) 立ち入る者を制限するための利用制限対策

(a) 事務従事者は、要管理対策区域内において、事務従事者であることを常時視認することが可能な状態にすること。

解説：要管理対策区域に立ち入っている者が事務従事者であることを外見上判断できるようにするために、身分証明書を着衣上に掲示すること等により常時視認できる状態にすることを求める事項である。

(7) 物品の持込み、持ち出し及び利用についての利用制限対策

(a) 区域情報セキュリティ責任者は、要保護情報を取り扱う情報システムに関連する物品の持込み及び持ち出しに係る利用制限対策として、以下の事項について、別表 2 に従って、クラスの区分に応じた措置を講ずること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。

(ア) 情報システムに関連する物品の持込み及び持ち出しを行う措置

解説：情報システムに関連する物品の持込み及び持ち出しによって生ずるリスクに対処するための事項である。
「情報システムに関連する物品」とは、要管理対策区域に存在する情報システムで利用するための物品が挙げられ、これにはハードウェア、ソフトウェア、電磁的記録媒体及び情報システムから出力された書面等が含まれる。

(イ) 情報システムに関連する物品の持込み及び持ち出しに係る記録の保存

解説：情報システムに関連する物品の持込み及び持ち出しを記録し、追跡性を確保するための事項である。記録を取得する項目としては、持込み及び持ち出しを行う者の名前及び所属、日時、物品又は事由等が挙げられる。

(ウ) 情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の要管理対策区域への持込みについての制限

解説：情報漏えいの原因となる可能性のある電子計算機、通信回線装置、電磁的記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の持込みを制限するための事項である。

(b) 事務従事者は、撮影又は録音する場合は、別表 2 に従って、クラスの区分に応じて、区域情報セキュリティ責任者に撮影又は録音の許可を得、又は届け出ること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。

解説：動画及び写真の撮影並びに音声の録音に係る許可を得、又は届け出ることを求める事項である。
許可又は届出先となる主体は、当該区域を管理する区域情報セキュリティ責任者となるが、許可又は届出の窓口は担当の事務従事者が行うことが考えられる。

(8) 荷物の受渡しについての利用制限対策

(a) 区域情報セキュリティ責任者は、受渡業者と物品の受渡しを行う際の対策として、別

表 2 に従って、クラスの区分に応じた措置を講ずること。なお、個別の利用制限対策を決定する場合は、当該個別利用制限を講ずること。

解説：物品の受渡しを行う業者が要管理対策区域内に立ち入ることを制限するための事項である。

制限する措置としては、受渡しが認められる区域の決定並びに受渡しが認められない区域で、受渡しが必要な場合は、当該業者が該当区域内の電子計算機、通信回線装置及び記録媒体に触れることができない場所に限定し、事務従事者が立ち会うようにすることが考えられる。「記録媒体」には電磁的記録媒体及び情報システムから出力された書面等の非電磁的な媒体が含まれる。

(9) 災害及び障害への対策

(a) 区域情報セキュリティ責任者は、要安定情報を取り扱う情報システムについては、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。

解説：地震、火災、水害、停電、爆発及び騒じょう等の災害から電子計算機及び通信回線装置を保護するための事項である。対策としては、例えばサーバラックの利用のほか、

・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
・非常口及び非常灯

等の設置又は確保が挙げられる。

(b) 区域情報セキュリティ責任者は、要安定情報を取り扱う情報システムについては、要管理対策区域内において災害又は障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。

解説：作業する者が災害等により要管理対策区域内に設置された電子計算機及び通信回線装置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電子計算機及び通信回線装置の電源を遮断できるようにするための事項である。

2.3.2 電子計算機

2.3.2.1 電子計算機共通対策

趣旨（必要性）

電子計算機の利用については、不正プログラム感染や不正侵入を受ける等の外部的要因により、保存されている情報の漏えい、改ざん又は当該電子計算機の機能停止等の被害に遭うおそれがある。また、事務従事者の不適切な利用等の内部的要因による情報セキュリティの侵害も起こり得る。このように電子計算機の利用は、当該電子計算機及び当該電子計算機が

取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、電子計算機に関する対策基準として、電子計算機に関する設置時、運用時及び運用終了時についての遵守事項を定める。

遵守事項

(1) 電子計算機の設置時

(a) 部局技術責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を将来の見通しを含め検討し、確保すること。

解説：通常の運用において十分な性能を確保することを求める事項である。

例えば、電子計算機の負荷に関して事前に見積もり、試験等を実施し、必要となる処理能力及び容量を想定し、それを備える必要がある。また、将来にわたっても十分な性能を確保できるように、拡張性や余裕を持たせておく必要がある。

(b) 部局技術責任者は、要保護情報を取り扱う情報システムについては、電子計算機を要管理対策区域内に設置すること。ただし、モバイル端末について部局総括責任者の承認を得た場合は、この限りでない。

解説：電子計算機が設置される物理的環境における脅威への対策を求める事項である。

人為的な脅威としては建物内への侵入、部外者による操作、失火による火災又は停電等があり、環境的脅威としては地震、落雷又は風水害等がある。そのため、物理的な隔離、入退者の主体認証装置、消火設備、耐震設備又は無停電電源装置等を利用する必要がある。

(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、サービス提供に必要な電子計算機を冗長構成にする必要性を検討し、必要と判断した場合には、その電子計算機を冗長構成にすること。

解説：障害・事故等が発生した場合、サービスを提供する電子計算機を代替電子計算機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を求める事項である。可用性を高めるためには、電子計算機本体だけでなく、ハードディスク等のコンポーネント単位で冗長構成にすることも考えられる。

なお、災害等を想定して冗長構成にする場合には、代替の電子計算機を遠隔地に設置することが望ましい。

(d) 部局技術責任者は、事務従事者の離席時に、電子計算機を不正操作から保護するための措置を講ずること。

解説：事務従事者の離席時に、電子計算機を第三者による不正操作から保護するための事項である。

対策としては、例えば、スクリーンのロック等が挙げられる。スクリーンのロックについては、設定を義務付けるだけでなく、一定時間操作がないと自動的にロックする仕組み又は電子計算機のログインに利用する主体認証情報格納装置を事務室への立入りの許可の確認にも利用する方法等が考えられる。また、スクリーンのロックを設定できない電子計算機については、施錠管理可能な棚又はラック等に収納したり、キーボード、マウス及び USB ポート等を使用できないようにロックしたりする方法等が考えられる。

(e) 部局技術責任者は、電子計算機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：多様なソフトウェアを利用することによりセキュリティホール等の脅威が増大し、その対処が困難となる可能性があるため、電子計算機で利用するソフトウェアを制限することを求める事項である。

(2) 電子計算機の運用時

(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電子計算機を利用しないこと。

解説：電子計算機を業務目的以外に利用することを禁止する事項である。例えば、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させられてしまうことから回避するため、業務目的外でのウェブサイトの閲覧を禁止すること等が求められる。

(b) 事務従事者は、離席時に電子計算機を不正操作から保護するための措置を講ずること。

解説：事務従事者が、離席時に電子計算機を第三者による不正操作から保護するために、スクリーンのロック、ログオフ又は施錠管理等の実施を求める事項である。

(c) 事務従事者は、電子計算機で利用を禁止するソフトウェアに定められたものを利用しないこと。また、電子計算機で利用を認めるソフトウェアに定められたもの以外のソフトウェアを利用する必要がある場合には、部局技術責任者の承認を得ること。

解説：多様なソフトウェアを実行することによりセキュリティホール等の脅威が増大することから、利用を認めるソフトウェアに定められたもの以外のソフトウェアの利用を制限する事項である。

利用を認めるソフトウェアに定められたもの以外のソフトウェアを利用する必要がある場合には、承認を得る必要がある。部局技術責任者は、利用承認の申請を受け付け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最低１回の手続きで済ませることができる。

(d) 部局技術責任者は、所管する範囲の電子計算機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電子計算機を検出等した場合には、当該不適切な状態の改善を図る必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：電子計算機で利用されている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場合にその改善を図ることを求める事項である。ただし、サーバ装置において利用を認めるソフトウェアに定められたもの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し、又は削除する必要がある。また、サーバ装置において利用を認めるソフトウェアに定められたものであっても、利用しない機能については無効化する必要がある。

「定期的」とは、１か月から ６か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。

また、「不適切な状態」とは、利用を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、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等の状態のことをいう。

(3) 電子計算機の運用終了時

(a) 部局技術責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体の全ての情報を抹消すること。

解説：電子計算機の運用を終了する場合に、当該電子計算機に内蔵される電磁的記録媒体から、全ての情報を抹消することを求める事項である。

「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。また、ファイルの情報自体へ別の情報を上書きした場合であっても残留磁気により復元される可能性があることが指摘されている。したがって、当該電磁的記録媒体に保存されている全ての情報を適切な方法で抹消する必要がある。

2.3.2.2 端末

趣旨（必要性）

端末については、当該端末を利用する者が専門的知識を有していない場合が多いことから、当該利用者の過失による不正プログラム感染等のリスクが高い。また、可搬性の高い端末については、紛失又は盗難のリスクも高くなる。

このように端末の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、端末に関する対策基準として、端末の設置時及び運用時についての遵守事項を定める。

遵守事項

(1) 端末の設置時

(a) 部局技術責任者は、要保護情報を取り扱うモバイル端末については、要管理対策区域外で使われる際にも、要管理対策区域で利用される端末と同等の保護手段が有効に機能するように構成すること。

解説：要管理対策区域外で利用されるモバイル端末は、要管理対策区域で利用される端末と異なる条件下に置かれるため、要管理対策区域外で端末が利用される際の保護手段として、端末で動作するパーソナルファイアウォール等の具備を求める事項である。

例えば、モバイル端末が通常接続される通信回線で実施されているアクセス制御及び監視等は、他の通信回線では同等に実施されているとは限らないため、モバイル端末において実施する必要がある。

(b) 事務従事者は、モバイル端末を利用する必要がある場合には、部局技術責任者の承認を得ること。

解説：モバイル端末には様々なセキュリティ上のリスクが考えられるため、不必要にリスクを増大させないために、業務上必要なモバイル端末の利用にとどめるための事項である。

(c) 部局技術責任者は、要機密情報を取り扱うモバイル端末については、電磁的記録媒体に保存される情報の暗号化を行う機能を設けること。

解説：モバイル端末が物理的に外部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、及びモバイル端末で利用していた外部電磁的記録媒体を他の電子計算機を利用して解読する等の攻撃によって要機密情報が読み取られる危険性がある。このような情報漏えいの対策として、端末に暗号化機能を装備することを求める事項である（ただし、当該モバイル端末で電磁的記録媒体に保存される情報の暗号化を行う機能が存在しない場合を除く。）。

なお、機密性 3 情報を取り扱う場合には、端末に暗号化機能を装備することが必要である。

(d) 部局技術責任者は、要保護情報を取り扱うモバイル端末については、盗難防止及び盗難後の被害を軽減するための措置を定めること。

解説：モバイル端末は容易に搬出することが可能なため盗難又は紛失に遭う可能性が高いことから、部局技術責任者にその対策を定めることを求める事項である。

対策としては、要管理対策区域においては、モバイル端末を入退出が管理される区域内に設置している場合においても端末の形状に応じて、固定物又は搬出が困難な物体と容易に切断できないセキュリティワイヤーでつなぐことや、帰宅時に施錠できるキャビネットに保存すること、常時所持又は携帯すること等が挙げられる。モバイル端末を要管理対策区域外に持ち出す場合は、常時所持又は携帯することや常に身近に置き目を離さないこと等が挙げられる。盗難後の被害を軽減するための具体的な措置としては、例えば、遠隔データ消去機能等が挙げられる。

(e) 部局技術責任者は、事務従事者が情報を保存できない端末を用いて情報システムを構築する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：端末から情報が漏えいすることを防ぐために、シンクライアント等の端末を利用することを求める事項である。

(2) 端末の運用時

(a) 事務従事者は、要保護情報を取り扱うモバイル端末を利用する場合には、盗難防止措置を行うこと。

解説：モバイル端末を利用する事務従事者に対して、モバイル端末の盗難防止措置について、部局技術責任者が定めた手順に従い、措置を実施することを求める事項である。

(b) 事務従事者は、要機密情報を取り扱うモバイル端末については、モバイル端末を要管理対策区域外に持ち出す場合に、当該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。

解説：モバイル端末で利用する電磁的記録媒体の紛失又は盗難により保存されている情報が漏えいすることを防ぐため、必要に応じて、ハードディスク、USB メモリ等に記録されている情報に対してファイル又は電磁的記録媒体全体を暗号化することを求める事項である。暗号化する方法としては、ハードディスク全体やファイルを暗号化するソフトウェアの導入や OS に標準装備されている暗号化機能の使用が挙げら

れる。

(c) 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端末を接続しないこと。

解説：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事項である。

学内通信回線でも許可を得た通信回線以外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も接続許可を得る必要がある。

(d) 部局技術担当者は、情報システムにおいて基準となる時刻に、端末の時刻を同期する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：情報システム内で同期されている基準となる時刻に、端末の時刻を同期させることを求める事項である。

情報セキュリティが侵害された際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えない。

2.3.2.3 サーバ装置

趣旨（必要性）

サーバ装置については、当該サーバ装置の電磁的記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は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等を受けるリスクが高い。政府機関が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、本学外の人々からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。

このようにサーバ装置の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、サーバ装置に関する対策基準として、サーバ装置の設置時及び運用時についての遵守事項を定める。

遵守事項

(1) サーバ装置の設置時

(a) 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場合は、通信を秘匿する必要性の有無を検討し、必要があると認めたときは、送受信される情報を秘匿するための機能を設けること。この場合、学外通信回線を経由する保守作業については、通信を秘匿する必要があると判断すること。

解説：通信回線を経由してサーバ装置の保守作業を行う際のセキュリティ強化を求める事項である。

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オンして作業

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、通信の秘匿する必要がある場合には、設置時に暗号化するための機能を設け、運用時に実際の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。

(b) 部局技術担当者は、要安定情報を取り扱うサーバ装置の内、サービス提供に必要なサーバ装置については、負荷を複数のサーバ装置に分散又はサーバ装置を冗長構成とする必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：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、複数のサーバ装置による負荷分散、負荷分散装置の設置、DNS による負荷分散又は冗長構成等の実施を求める事項である。

(2) サーバ装置の運用時

(a) 部局技術責任者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対処すること。

解説：サーバ装置のソフトウェア及びハードウェア等の構成が不正に変更されていないか定期的に確認し、また、変更によるセキュリティレベルの低下等が発生していないか検討し、変更状況に応じて対処することを求める事項である。

(b) 部局技術担当者は、要安定情報を取り扱うサーバ装置については、サーバ装置の運用状態を復元するために必要な措置を講ずること。

解説：サーバ装置の運用状態を復元するための必要な措置を講ずることによりサーバ装置に保存されている情報及びその情報を用いたサービスの可用性の担保を目的とした事項である。

サーバ装置の運用状態を復元するための必要な措置の例として、以下のようなものがある。

・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。

・前回内容からの変更部分の定期的なバックアップを実施する。

・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。

・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。

また、取得した情報を記録した電磁的記録媒体は、施錠された保管庫に保存等して、業務上の必要がある場合にこれらの情報を利用する部局技術担当者に限ってアクセスできるようにする。

なお、災害等を想定してバックアップを取得する場合には、記録媒体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ある施設に保存することが考えられる。その際には、情報を遠隔地に送信や移送する際のセキュリティ及び取得した情報の保管時のセキュリティを確保する必要がある。セキュリティを確保する措置の例としては、暗号や秘密分散技術を利用して情報の漏えいや改ざんを防止することが挙げられる。

(c) 部局技術担当者は、サーバ装置の運用管理について、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。

解説：運用管理作業の記録を文書として残すための事項である。本学において、ある程度

統一的な様式を作成する必要がある。

(d) 部局技術担当者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。

解説：情報システム内で同期されている基準となる時刻にサーバ装置を同期させることを求める事項である。

情報セキュリティが侵害された際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えない。

(e) 部局技術担当者は、サーバ装置のセキュリティ状態を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：サーバ装置のセキュリティ状態を監視するための事項である。

「セキュリティ状態を監視」するとは、サーバ装置上での不正な行為及び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ことである。監視の方法の例としては、アクセスログを定期的に確認することや、侵入検知システム、アンチウイルスソフトウェア又はファイル完全性チェックツール等の利用が挙げられる。

なお、アクセスログを確認する際は、運用管理作業の記録若しくは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相関分析を行うことが考えられる。

(f) 部局技術担当者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、当該サーバ装置に関する障害等の発生を検知すること。

解説：日常的なサーバ装置のシステム状態について監視を行うことで、障害等の発生を早期に検出し、またこの影響の拡大を未然に防止するための事項である。

「システム状態を監視」するとは、サーバ装置の CPU、メモリ、ディスク入出力等の性能及び故障等を監視することである。監視方法は、状況に応じて、ツールの利用、手動から、適切な方法を選択することが可能である。

2.3.3 アプリケーションソフトウェア

2.3.3.1 電子メール

趣旨（必要性）

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等の機密性に対するリスクがある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれる等の可用性に対するリスクがある。この他、内容を偽ったメールによるいわゆるフィッシング詐欺等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。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要である。

これらのことを勘案し、本項では、電子メールサーバの管理及び電子メールの利用に関する対策基準として、電子メールの導入時及び運用時についての遵守事項を定める。

遵守事項

(1) 電子メールの導入時

(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。

解説：迷惑メールの送信等に使われることを回避するために、電子メールを不正に中継しないように電子メールサーバを設定することを求める事項である。

(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事務従事者の主体認証を行う機能を備えること。

解説：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 認証等の主体認証を行うことを定めた事項である。

(c) 部局技術責任者は、電子メールの送信元について、なりすましの防止策を講ずること。

解説：電子メールの送信時及び受信時において、なりすましを防止することを求める事項である。

「なりすましの防止策」には、平時から行う防止策、電子メールの送信時に行う防止策及び電子メールの受信時に行う防止策等がある。これらの防止策は、第３レベルのドメインだけでなく、第４レベル以上のドメインについても、考慮する必要がある。

（ア）平時から行うなりすましの防止策として、Sender Policy Framework（以下「SPF」という。）、SenderID 及び DomainKeys Identified Mail（以下「DKIM」という。）を利用した送信側における送信ドメイン認証等が挙げられる。（なお、「SenderID」及び「DKIM」は、それぞれ送信ドメイン認証の１つである。）これらは、電子メールで使用するドメインを管理する DNS サーバに、電子メールサーバの情報や署名で使用する公開鍵の登録・公開を行う。なお、SPF や SenderID における DNS サーバへの電子メールサーバ情報の登録では、次の事項に留意する必要がある。

・電子メールを利用していないドメインは、その情報を登録する必要があること。

・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、若しくは将来にわたって利用の予定のないドメインについては、なりすましの防止策を講ずるか、又はドメイン名の登録を廃止すること。

・SPF レコードについては、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こと。（なお、「SPF レコード」とは、SPF や SenderID において、DNS サーバの TXT レコードに記述される送信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”を記述すること。

・電子メールサーバを外部委託先において運用している場合には、外部委託先のグローバル IP アドレスを自組織のものとして SPF レコードに登録することは、同じ IP アドレスを民間業者も共用し、なりすましのおそれがあること。このため、外部委託先には、同じサーバの他の利用者によるなりすまし防止策を講じたり、政府ドメイン名を使用する機関向けに民間業者と共用しない専用の IP アドレスを割り振られたりした場合を除き、外部委託先のグローバル IP アドレスを SPF レコードに登録することは認められない。

（イ）電子メールの送信時に行うなりすましの防止策として、S/MIME や DKIM を利用した送信メール（メールマガジンを含む）への電子署名の添付等が挙げられる。
（ウ）電子メールの受信時に行うなりすましの防止策として、電子署名の検証及び受信側における SPF の検証（具体的には、受信時に通信を行った送信側の電子メールのサーバと、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電子メールサーバの情報との比較によるなりすましの判定）等が挙げられる。

(2) 電子メールの運用時

(a) 事務従事者は、業務遂行に係る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。ただし、本学支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。

解説：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以外の電子メールサービス（以下「本学以外の電子メールサービス」という。）を、業務遂行に係る情報を含む電子メールの送受信に利用することを禁ずる事項である。なお、上記の「送受信」には電子メールの「転送」が含まれている。したがって、本学以外の電子メールサービスの電子メールアドレスに業務遂行に係る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、要機密情報の移送についての遵守事項に違反しないようにも留意する必要がある。

(b) 事務従事者は、受信した電子メールにより、スクリプトが電子計算機で実行されないように電子メールの内容を表示させること。

解説：例えば HTML メールの表示により、偽のウェブサイトに誘導するために表示が偽装されること、意図しないファイルが外部から取り込まれること等の不正なスクリプトが実行されることを防ぐことを定めた事項である。
「スクリプト」とは、ここでは JavaScript 等の電子計算機にて簡易的に実行することができるプログラムをいう。
「スクリプトが電子計算機で実行されないように表示させる」とは、表示をテキスト形式のみに設定して表示することや端末でスクリプトの実行を禁止された情報システムを用いて表示することが挙げられる。
そのため、情報システムの管理者により、事務従事者が使用する電子メールクライアントの設定が上述のとおり適切に行われ、かつ、事務従事者が電子メールクライアントの設定を勝手に変更しないよう制限することにより対策を実施することも考えられる。
なお、本遵守事項は、スクリプトが電子計算機で実行されないのであれば、電子メールの文字装飾や画像の表示を禁止するものではない。
また、本遵守事項は、端末等にインストールされる電子メールクライアントを対象としているため、ウェブブラウザにより読み書きする電子メール（いわゆるウェブメール）は対象外となる。

2.3.3.2 ウェブ

趣旨（必要性）

ウェブを利用するに当たっては、サーバにおいて、OS 等既成のソフトウェアや開発したウェブアプリケーション等の複数の要素で構成されていること、一方で、クライアントにおいてもサーバと同様に情報処理が行われていることから、様々な脅威が考えられる。

これらのリスクを回避するためには、システムのライフサイクル全般に対して適切な対策を組み合わせて実施することが必要である。

これらのことを勘案し、本項では、ウェブに関する対策基準として、ウェブサーバの導入、ウェブアプリケーションの開発、ウェブの運用についての遵守事項を定める。

なお、ウェブサーバの導入及び運用については、本項に加えて、2.3.2.3 にて定めたサーバ装置に係る対策基準を、また、サービス不能攻撃等のウェブにおける脅威への対策としては、2.2.2.3 にて定めた情報セキュリティについての脅威に係る対策基準を参照する必要がある。

遵守事項

(1) ウェブサーバの導入時

(a) 部局技術責任者は、情報セキュリティが確保されるよう適切にウェブサーバのセキュリティ設定をすること。適切なセキュリティ設定として、以下に挙げる事項を含む措置を講ずること。

(ア) ウェブサーバの機能を適切に制限すること。

(イ) ウェブサーバに保存された情報へのアクセス制限を適切に設定すること。

(ウ) 識別コードを適切に管理すること。

(エ) 通信時の盗聴による情報漏えいのリスクを検討し、必要と判断した場合には、暗号化と電子証明書による認証の機能を設けること。

解説：ウェブサーバの導入時の設定に関して以下の項目を適切に行うことにより、セキュリティを確保することを求める事項である。

（ア）は、ウェブサーバで提供する機能の内、不要な機能を停止又は制限することを求めている。例えば、スクリプトやファイル実行の制限や保存場所の限定、インデックス表示の禁止、ホームページ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の制限等が挙げられる。

（イ）は、情報の漏えいやウェブページの改ざんを防ぐために、情報へのアクセス権限を適切に設定することを求めている。例えば、ウェブコンテンツファイルへのアクセス権限は、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、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等が挙げられる。

（ウ）は、 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の適切な管理を求めている。これらの識別コードはブルートフォース (総当たり)攻撃の標的になるリスクがあるため、その必要性を確認して、不要なものは削除することが重要である。また、初期状態で用意されるサンプルのページ、プログラム等も削除するといった注意が必要である。

（エ）は、通信時の盗聴による第三者への情報漏えいの防止及びウェブサーバの詐称を利用者が検知できるようにするための事項である。第三者への漏えいを防止する必要のある情報には、例えば、サービスの利用者の個人情報等が挙げられる。ウェブサーバにおいてこれらを解決するための機能としては､例えば、SSL 及び TLS が挙げられる。この機能を設けることにより、通信内容の暗号化が可能になるとともに、ウェブサーバの利用者は、ウェブサーバの電子証明書を参照することでその正当性を確認することができる。

なお、政府機関のウェブサーバに電子署名を付与する必要があると認めたときの SSL 及び TLS に用いる電子証明書は、政府認証基盤（GPKI）で発行したものを使用することが望ましい。

(b) 部局技術責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバに保存する情報を特定し、当該サーバに特定した情報以外の要機密情報が含まれないことを確認すること。

解説：万が一、不正侵入等が発生した場合であっても、当該サーバから要機密情報が漏えいしないよう、被害範囲の限定を図るための事項である。利用が想定されていないデータ等を、ウェブサーバに保存しないことが必要である。

(2) ウェブアプリケーションの開発時

(a) 部局技術責任者は、情報セキュリティが適切に確保されるようにウェブアプリケーションの開発においてセキュリティ対策機能を組み込むこと。適切なセキュリティ機能として、以下に挙げる事項を含む措置を講ずること。

(ア) 利用者による URL の確認を妨げないこと。

(イ) 主体認証と情報へのアクセス制御を適切に行うこと。

(ウ) 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限定すること。

(エ) 不正な入力データを排除すること。

(オ) 不正な出力データを排除すること。

(カ) 安全なセッション管理を行うこと。

解説：ウェブアプリケーションの開発を行う場合に、以下のセキュリティ機能を実装することにより、セキュリティを確保することを求める事項である。

なお、セキュリティ機能の実装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「セキュアプログラミング講座」（http://www.ipa.go.jp/security/awareness/vendor/programming/index .html）の「Web アプリケーション編」または、「安全なウェブサイトの作り方」（http://www.ipa.go.jp/security/vuln/websecurity.html）を適宜参照することが望ましい。

（ア）は、利用者が URL（ウェブアドレス）を確認できない場合、攻撃者が用意した危険なサイト（フィッシングサイト等）に誘導される可能性があることから、それを避けることを求めるものである。この対策としては、例えば、アドレスバーを隠さない、右クリックを無効にしない等が挙げられる。

（イ）は、主体認証を行うウェブアプリケーションにおいて、パスワード等の漏えいによる利用者のなりすまし防止や主体認証後の利用者のファイルへのアクセスに

ついて適切に制御することを求めるものである。ユーザ ID とパスワードによって主体認証を行う場合、例えば、パスワードの設定時にその文字列に適切な条件を課す、利用者本人がパスワードを変更できるようにする、入力されたパスワードは隠し文字にして表示しない等の対策が挙げられる。また、利用者が設定したパスワードはハッシュ関数を用いて復元できない形にすることも重要である。ファイルへのアクセス制御については、ウェブサイトでどの主体がどの情報にアクセスする必要があるのかについて検討し、それに基づきアクセス制御を設計・実装することが重要である。特に、主体認証後にのみ参照可能なファイルが主体認証前に参照できてしまうことがないよう、適切にアクセス制御を行うことが求められる。

（ウ）は、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と、公開を想定しないファイルが参照されるリスクがあり、これを防止することを求めるものである。この対策としては、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のが安全だが、これができない場合は、例えば、ファイルにアクセスする前に入力されたパラメータの検査を行う、ファイルのディレクトリと識別子を固定の文字列にしてアクセスする等の方法が挙げられる。

（エ）は、ウェブサーバを用いて提供するサービスにおいて、利用者から文字列等の入力を受ける場合には、不当な入力データを排除することによって、バッファオーバフロー攻撃や SQL インジェクション等の攻撃を防ぐことを求めるものである。対策としては、例えば、ウェブアプリケーションへの入力を正しく定義し、不正なデータが渡されないよう、入力されたパラメータの長さや内容を検査し、無害化する機能を設ける等が挙げられる。

（オ）は、ウェブアプリケーションが出力する画面や OS の関数、SQL コマンド等の呼び出しといった出力情報に不正なデータの混入を排除することにより、クロスサイトスクリプティングや SQL インジェクション等の攻撃を防止することを求めるものである。対策としては、例えば、 HTML に埋め込むデータを全て検査してエスケープ処理する、外部プログラムを呼び出す際のプログラム名、オプション、パラメータ等はできる限り固定の文字列にする等が挙げられる。また、ウェブアプリケーション又はデータベース等から発信されるエラーメッセージ、稼動している製品名及びそのバージョン、登録されているユーザ ID 等は、攻撃を試みる者に対し攻撃の糸口となり得る情報を与えてしまう危険性がある。これらのことを回避するため、不必要な情報は出力しない措置を講ずることが求められる。

（カ）は、セッション管理の不備により利用者になりすましてアクセスされることを防止するため、適切なセション管理を求めるものである。対策としては、例えば、セション ID の有効期間を主体認証直後のレスポンスからログアウトまでに限定する、推測困難なセッション ID を設定する、セッション ID を URL パラメータに格納しない、Cookie に入れる情報はセッション ID 以外に必要最小限とする、SSL を使用する Cookie は secure 属性にする等が挙げられる。

(3) ウェブの運用時

(a) 事務従事者は、情報セキュリティの確保がなされるよう適切にウェブクライアントの

セキュリティ設定をすること。

解説：事務従事者が意図しない悪意のあるソフトウェアが電子計算機において実行されること等により、情報が漏えいしてしまうことや他の電子計算機を攻撃してしまうこと等を防止するため、ウェブクライアントのセキュリティ設定を適切に行うことを求める事項である。

具体的には、閲覧するウェブサイトの信頼性やウェブクライアントが動作する電子計算機にて扱う情報の機密性等に応じて、以下のようなセキュリティ設定項目について適切な値を選択すること。

・ActiveX コントロールの実行
・JavaScript の実行
・Java の実行
・Cookie の保存 等

そのため、情報システムの管理者がウェブクライアントのセキュリティ設定を上述のとおり行い、かつ、事務従事者が当該設定を勝手に変更しないよう制限することにより対策を実施することも考えられる。

(b) 事務従事者は、ウェブクライアントが動作する電子計算機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。

解説：ソフトウェアをダウンロードする場合は、電子署名により配布元の正当性を確認することを求める事項である。

(c) 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。

解説：主体認証情報等を入力して送信する場合には、情報漏えいを防止するため、ブラウザの鍵アイコンの表示を確認する等により、SSL や TLS 等の暗号通信が使用されていること等の手段を限定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を使用する際に主体認証情報等を入力すること等を指す。

(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。

解説：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かを確認することにより、当該情報の送信先を限定することを求める事項である。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ないかを確認することが必要である。

(d) 部局技術責任者は、事務従事者が閲覧することが可能な学外のウェブサイトを制限する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、定期的にその見直しを行うこと。

解説：ウェブサイトからの不適切なソフトウェアのダウンロードや私的なウェブサイトの閲覧を制限するため、コンテンツフィルタ等により閲覧することが可能な範囲の制限を定める事項である。

部局技術責任者は、制限を実施する方法として、ウェブクライアント、ウェブプロキシ及びその他の装置の設定等、状況に応じて、適切な方法を選択することが可能である。

2.3.3.3 ドメインネームシステム（DNS）

趣旨（必要性）

ドメインネームシステム（DNS：Domain Name System）は、クライアント等からの問い合わせを受けて、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インターネットの基盤をなすサービスである。DNS 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 DNS 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、クライアント等が悪意あるサーバに接続させられる等の被害にあう可能性がある。このようなリスク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。

これらのことを勘案し、本項では、DNS に関する対策基準として、DNS の導入時及び運用時についての遵守事項を定める。

遵守事項

(1) DNS の導入時

(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 DNS の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。

解説：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、名前解決を停止させないために、求められる可用性の度合いに応じた措置を求める事項である。

DNS の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等、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、冗長化による措置の例である。あるいは、悪意ある者からのサービス不能攻撃に備え、ソフトウェアや通信回線装置で適切なアクセス制御を実施しておくことも重要である。

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。

(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を運用管理するための手続を定めること。

解説：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（ゾーン情報）を運用管理するための手続を定めることを求める事項である。

「管理するドメインに関する情報を運用管理するための手続」では、例えば、管理するドメインに関する情報の設定や更新、正確性の維持等の手順や管理するドメインの構成範囲を明確化しておくことが考えられる。

(c) 部局技術責任者は、DNS の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。

解説：DNS のキャッシュサーバの第三者による不正利用やキャッシュ情報の汚染等を防ぐための措置を講ずることを求める事項である。キャッシュサーバにおいては、学外からの名前解決の要求には応じず、学内からの名前解決の要求のみに回答を行うように措置を講ずる必要がある。キャッシュサーバを動作させる場合は、サーバの設定やファイアウォール等でアクセス制御を行うことが重要である。

また、適正な名前解決の代行を維持するために、ルートヒントファイルの更新の有無を定期的に確認し、最新のものに維持する必要がある。「定期的」とは、3 ヶ月に一度程度実施することを想定している。

(d) 部局技術責任者は、DNS の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、当該情報が外部に漏えいしないための措置を講ずること。

解説：DNS の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、学内の事務従事者以外の者が内部のみで使用している名前情報を取得できないようにすることを求める事項である。例えば、内部向けの名前解決を提供するコンテンツサーバを外部向けのコンテンツサーバとは別々に設置し、サーバの設定やファイアウォール等でアクセス制御を行う等の方法が考えられる。

(e) 部局技術責任者は、情報システムに対し名前解決を提供する DNS サーバにおいて、コンテンツサーバによるドメイン名の情報提供時には電子署名を付与し、キャッシュサーバによる名前解決時には電子署名を検証する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：電子署名によって DNS のコンテンツサーバのなりすましや同サーバからの提供情報の改ざんを DNS のキャッシュサーバで検出できるようにすることを求める事項である。その対策としては、DNSSEC の利用等が挙げられる。

DNSSEC は、公開鍵暗号技術を用いて改ざん等を防止するため、その導入には情報の提供側である DNS のコンテンツサーバと情報の問い合わせ側である DNS のキャッシュサーバの双方に対応が必要となる。

本学外の人々への信頼できるサービスの提供と、政府機関内の情報セキュリティ向上の観点から、政府ドメインを管理する DNS のコンテンツサーバ、及び政府機関の DNS 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。

(2) DNS の運用時

(a) 部局技術担当者は、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。

解説：複数台の DNS のコンテンツサーバが保有し管理するドメインに関する情報について、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の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の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 の利用等が考えられる。

(b) 部局技術担当者は、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を運用管理するための手続に基づいて、当該情報が正確であることを適宜確認すること。

解説：管理するドメインに関する情報が正確であるかどうかを確認することを求める事項である。管理するドメインに関する情報の設定ミスや不正な改ざん等が発生していないかを確認する必要がある。管理するドメインに関する情報の具体例として、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 レコード等がある。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。

2.3.4 通信回線

2.3.4.1 通信回線共通対策

趣旨（必要性）

通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、通信回線に関する対策基準として、通信回線の構築時、運用時及び運用終了時についての遵守事項を定める。

遵守事項

(1) 通信回線の構築時

(a) 部局技術責任者は、通信回線構築によるリスクを検討し、通信回線を構築すること。

解説：部局技術責任者は、通信回線構築によるリスクを考慮して、通信回線の構築及び運用開始を判断する必要がある。学外通信回線と接続する場合のリスク軽減措置としては、例えば、ファイアウォールやウェブアプリケーションファイアウォール(WAF)等を利用する方法が考えられる。リスクを検討した結果、部局技術責任者は、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か、通信回線を構築しない等の判断を行うことが望ましい。なお、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間の通信も同様に考慮すること。（「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きょう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。例えば、仮想化ソフトウェアを利用することが考えられる。なお、仮想化ソフトウェアとは、１つのハードウェアで複数のオペレーティングシステムを同時に実行する機能を有するソフトウェアをい

う。以下同様。）

(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、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。

解説：通常の運用において十分な通信回線の能力を確保し、情報の可用性を確保するための事項である。例えば、通信回線の負荷に関して事前に試験等を実施し、必要となる容量及び能力を想定する等の対策が考えられる。なお、将来にわたっても十分な容量及び能力を確保できるように、余裕を持たせておく必要がある。

(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を定めること。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。

解説：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、セキュリティホール等の脅威への対処を確実なものとするために、通信回線装置が必要とするソフトウェアを定めておくことを求める事項である。

(d) 部局技術責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。

解説：電子計算機が接続されている通信回線の境界で効果的にアクセス制御するために、まず電子計算機をグループ化し通信回線上で分離することを求める事項である。学外通信回線と接続する学内通信回線の場合は、学外通信回線上の電子計算機は、学内通信回線に接続される電子計算機とは別のグループとし、分離する必要がある。なお、「グループ化」とは、対象機器をその利用目的、求められるセキュリティレベル、管理部門等から分類することをいう。

(e) 部局技術責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用し、アクセス制御及び経路制御を行うこと。

解説：グループ化された電子計算機間の通信の制御を行うことで、セキュリティを確保するための事項である。部局技術責任者は、グループ化された電子計算機間で情報システムの運用上必要となる通信を全て確認した上で、通信要件を検討する必要がある。必要最小限のアクセスのみを許可するように、当該通信要件に従ってアクセス制御を行う。

(f) 部局技術責任者は、要機密情報を取り扱う情報システムについては、通信を秘匿する必要性の有無を検討し、必要があると認めたときは、通信を秘匿するための機能を設けること。

解説：通信における要機密情報を保護するための事項である。部局技術責任者は、通信回線上を要機密情報が送受信される場合には、当該情報の秘匿の必要性を検討して、運用時の暗号化に備えて構築時にそのための機能を設けておく必要がある。

また、通信路の暗号化は、情報の機密性だけでなく完全性を保護する上でも有用である。なお、通信路の暗号化のために、例えば、IPsec、SSL 及び TLS 等を使用することも考えられる。

(g) 部局技術責任者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、適切な回線を選択すること。

解説：通信回線に利用する物理的な回線（例えば、有線 LAN における LAN ケーブル、無線 LAN における伝搬路等の通信路）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措置が異なることから、適切な回線を選択することを求める事項である。

回線に応じたセキュリティ対策を実施する必要があるが、回線によってはセキュリティ対策を実施しても万全でない場合もあるので、回線の選択に当たっては十分に検討する必要がある。また、通信回線を仮想的に構築する場合には、物理的に同一の通信回線となる場合があることに注意する必要がある。

(h) 部局技術責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。

解説：遠隔地からの通信回線装置の保守や診断に利用するサービスのセキュリティを確保するための事項である。セキュリティ確保の方法として、識別コード及び主体認証情報（パスワード）による主体認証、接続する電子計算機の識別コードによるアクセス制御、通信の暗号化等の機密性の確保だけでなく、通信回線が利用できない状況での代替接続手段の確保等の可用性の確保も挙げられる。

(i) 部局技術責任者は、通信回線装置を要管理対策区域内に設置すること。

解説：通信回線装置及び通信ケーブルが設置される物理的環境における脅威への対策を求める事項である。

(j) 部局技術責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。

解説：学内通信回線同士を専用線で接続する場合に、当該専用線のサービスレベルを確保するための事項である。

部局技術責任者自身が契約を行わない場合には、セキュリティレベル及びサービスレベルを含む事項の取決めについて、契約する者に対して依頼すること。なお、セキュリティレベル及びサービスレベルが約款に記述されていれば、それで代替することが可能である。

(k) 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、サービス提供に必要な通信回線又は通信回線装置を冗長構成にする必要性を検討し、必要と判断した場合には、その通信回線又は通信回線装置を冗長構成にすること。

解説：障害・事故等によりサービスを提供できない状態が発生した場合、サービスを提供する通信回線又は通信回線装置を代替通信回線又は代替通信回線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を求める事項である。また、災害等を想定して冗長構成にする場合には、その通信回線及び代替通信回線がそれぞれ別の経路となることが望ましい。

(l) 部局技術責任者は、通信を行う電子計算機の主体認証を行う必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：通信を行う電子計算機の主体認証を行うことで、通信相手の電子計算機が正しい相手であることを確認するための事項である。

(2) 通信回線の運用時

(a) 部局技術担当者は、通信回線装置のソフトウェアを変更する場合には、部局技術責任

者の許可を得ること。

解説：通信回線装置のソフトウェアは機能の改善等を目的に変更を行う必要が生ずる場合がある。この変更の必要性が生じた時に、部局技術担当者は、独断での変更は行わず、部局技術責任者の許可を得てから行う事を求める事項である。

(b) 部局技術担当者は、通信回線及び通信回線装置の運用管理について、作業日、作業を行った通信回線及び通信回線装置並びに作業内容及び作業者を含む事項を記録すること。

解説：運用管理作業の記録を文書として残すための事項である。
本学において、ある程度統一的な様式を作成することが望ましい。

(c) 部局技術責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している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こと。

解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生した時に、他の情報システムを保護するための事項である。

(d) 事務従事者は、部局技術責任者の許可を受けていない電子計算機及び通信回線装置を通信回線に接続しないこと。

解説：通信回線に無断で電子計算機及び通信回線装置を接続された場合に生ずるリスクを防止するための事項である。

(e) 部局技術担当者は、情報システムにおいて基準となる時刻に、通信回線装置の時刻を同期すること。

解説：情報システム内で同期されている共通の時刻に設置した通信回線装置の時刻を同期させることを求める事項である。
有事の際に、時刻が同期していないとログの解析等が困難になる。標準時との同期が望ましいが、情報システム内で同期が取られていれば差し支えないものとする。

(f) 部局技術担当者は、要安定情報を取り扱う情報システムについては、通信回線装置の運用状態を復元するために必要な措置を講ずること。

解説：障害・事故等によりサービスを提供できない状態が発生した場合に、サービスの可用性を担保することを目的とした事項である。対策としては、通信回線装置の設定情報を作成又は変更した際に、設定情報のバックアップを実施することが挙げられる。
なお、災害等を想定してバックアップを取得する場合には、取得した情報を記録した電磁的記録媒体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ある施設に保存することが考えられる。

(g) 部局技術責任者は、所管する範囲の通信回線装置が動作するために必要な全てのソフトウェアの状態を定期的に調査する必要性の有無を検討し、必要と認めたときは、当該措置を講じ、不適切な状態にある通信回線装置を検出した場合には、当該不適切な状態の改善を図ること。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。

解説：通信回線装置における不正なソフトウェアの存在確認等を定期的に行い、対処がな

されていない場合にその改善を図ることを求める事項である。「定期的」とは、1 か月から 6 か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、調査する必要性については、一般的には、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検討することが考えられる。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必要性が高い機器として考えられる。ただし、必要性が低いと判断された機器についても、ソフトウェア等にぜい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。

なお、「不適切な状態」とは、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、定められた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等の状態のことをいう。

(h) 部局技術担当者は、通信回線装置を不正操作から保護するための措置を講ずること。

解説：部局技術担当者が通信回線装置を第三者による不正操作から保護するための事項である。対策としては、主体認証を行う通信回線装置については、コンソールターミナル等での作業終了後の確実なログアウト、施錠可能なラック内への設置等が挙げられる。

(3) 通信回線の運用終了時

(a) 部局技術責任者は、通信回線装置の利用を終了する場合には、通信回線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：運用を終了した通信回線装置が再利用され、又は廃棄された後、終了前に保存していた情報が漏えいすることを防ぐために、情報の抹消を求める事項である。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。

2.3.4.2 学内通信回線の管理

趣旨（必要性）

学内通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。また、利用する回線により想定される脅威及びリスクが異なる。

これらのことを勘案し、本項では、学内通信回線に関する対策基準として、学内通信回線の構築時及び運用時、回線の対策についての遵守事項を定める。

遵守事項

(1) 学内通信回線の構築時

(a) 部局技術責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続することを許可されたものであることを確認する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるこ

と。

解説：通信回線に接続する電子計算機の確認を行うことを求める事項である。当該措置を実施するための技術としては、電子計算機固有の情報による主体認証、IEEE 802.1x 等が挙げられる。

(2) 学内通信回線の運用時

(a) 部局技術責任者は、通信要件の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。

解説：適正なアクセス制御の維持を求める事項である。通信要件については、組織、情報システム又はサービスの変更等により変化するため、当該変更等に応じてアクセス制御の設定も見直す必要がある。「定期的」とは、６か月から１２か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、必ずしも当該変更等が適時連絡されるとは限らないので、部局技術責任者は定期的にアクセス制御の設定の見直しを行う。

(b) 部局技術担当者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析する必要性の有無を検討し、必要と認めたときは、当該措置を講じ、通信回線の性能低下及び異常を推測し、又は検知すること。

解説：確保している性能では適正な運用が困難な状態及び通信回線装置等の故障により通信不能な状態等により、情報の可用性を損なう事態を回避するため、通信回線の利用状況及び状態の確認を求める事項である。問題の発生を推測でき、又は検知できた場合には、事前に対策を行うことが求められる。

(c) 部局技術担当者は、学内通信回線上を送受信される通信内容を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

解説：通信回線上を送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正な行為及び無許可のアクセス等の意図しない事象の発生がないかを監視することが挙げられる。

(3) 回線の対策

(a) 部局技術責任者は、VPN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備

(イ) 通信内容の暗号化

(ウ) 通信を行う電子計算機の識別又は利用者の主体認証

(エ) 主体認証記録の取得及び管理

(オ) VPN 経由でアクセスすることが可能な通信回線の範囲の制限

(カ) VPN 接続方法の機密性の確保

(キ) VPN を利用する電子計算機の管理

解説：VPN を利用して論理的な学内通信回線を構築する場合に、セキュリティを確保することを求める事項である。「VPN」には、インターネット VPN、IP-VPN、SSL-VPN 等が挙げられる。

(b) 部局技術責任者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む措

置の必要性の有無を検討し、必要と認めたときは措置を講ずること。この場合、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を行う必要性があると判断すること。

(ア) 利用開始及び利用停止時の申請手続の整備
(イ) 通信内容の暗号化
(ウ) 通信を行う電子計算機の識別又は利用者の主体認証
(エ) 主体認証記録の取得及び管理
(オ) 無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限
(カ) 無線 LAN に接続中に他の通信回線との接続の禁止
(キ) 無線 LAN に接続する電子計算機及び通信回線装置の管理

解説：無線 LAN を利用して論理的な学内通信回線を構築する場合に、セキュリティを確保することを求める事項である。無線 LAN を利用する場合は、構築する環境に応じて措置を講ずることが望ましい。

（イ）については、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。なお、要機密情報を取り扱う無線 LAN 環境については、通信内容の暗号化を求めているが、WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信の妨害を発生させることができたりするという脆弱性が報告されており、また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。この場合、暗号化については、暗号と電子署名の標準手順に従わなければならない。

（ウ）については、例えば、通信回線上における主体認証の方式である IEEE 802.1x（クライアント認証及びサーバ認証）を導入し、適切に設定することが考えられる。

（オ）については、例えば、事務従事者が利用する学内通信回線と学外の者向けに提供する学内通信回線を分離することが考えられる。

（カ）については、例えば、無線 LAN に接続中に同時に有線 LAN と接続することを禁止することが考えられる。

（キ）については、例えば、無線 LAN に接続する電子計算機及び通信回線装置（無線 LAN アクセスポイント等）の機能で、以下のような管理を行うことが考えられる。

・出力・チャンネル管理等による電波監理
・IEEE 802.1x 等による管理外の無線 LAN アクセスポイント及び電子計算機の検出及び除去
・IPS（Intrusion Prevention System）機能等によるサービス不能攻撃の防御
・MAC アドレス等による接続管理　等

これらは、通信回線装置を要管理対策区域内に設置しても、第三者が区域外から不正に接続してくる可能性があることに注意して、設定する必要がある。

なお、学外の者向けに通信回線を提供する場合は、例えば、事前共有鍵等を利用した暗号化及び認証を行うことや VPN を利用することが考えられる。

参考：総務省「本学外の人々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－実践編」
（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin00.htm）にある、「安全な無線 LAN の利用」のページの解説、及び各府省情報化統括責任者（CIO）補佐官等連絡会議の「無線 LAN セキュリティ要件の検討」（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai65/65lan_kentou. pdf）を適宜参照。

(c) 部局技術責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備
(イ) 通信を行う者又は発信者番号による識別及び主体認証
(ウ) 主体認証記録の取得及び管理
(エ) リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限
(オ) リモートアクセス中に他の通信回線との接続の禁止
(カ) リモートアクセス方法の機密性の確保
(キ) リモートアクセスする電子計算機の管理

解説：公衆電話網を経由してリモートアクセスを利用する場合に、セキュリティを確保することを求める事項である。

2.3.4.3 学外通信回線との接続

趣旨（必要性）

学内通信回線と学外通信回線との接続については、学外通信回線に接続された電子計算機からの不正アクセス、サービス不能攻撃等のほか、学外通信回線に送受信される情報の漏えい、改ざん又は破壊等、学外通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、学外通信回線と接続する場合の学内通信回線に関する対策基準として、学内通信回線と学外通信回線との接続時及び運用時についての遵守事項を定める。

遵守事項

(1) 学内通信回線と学外通信回線との接続時

(a) 部局技術責任者は、部局総括責任者の許可を得た上で、学内通信回線を学外通信回線と接続すること。

解説：学内通信回線を学外通信回線と接続するとリスクの増大を招くので、部局総括責任者の判断を得ることを求める事項である。
部局総括責任者は、様々なリスクを検討した上で許可の可否を判断する必要がある。

(b) 部局技術責任者は、学内通信回線を学外通信回線と接続することにより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通信回線として学内通信回線を構築

すること。

解説：学内通信回線に接続している情報システムを、学外からの脅威から保護するための事項である。セキュリティの確保が困難な情報システムについては、他の情報システムと共有している学内通信回線から独立した通信回線として構成するか、学外通信回線から切断した通信回線として構築することになる。独立した通信回線の場合でも、遵守すべき対策基準は実施する必要がある。

(2) 学外通信回線と接続している学内通信回線の運用時

(a) 部局技術責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、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通信回線に構成を変更すること。

解説：他の情報システムと通信回線を共有している場合であって、情報システムのセキュリティの確保が困難な事由が発生した時に、他の情報システムを保護するための事項である。

(b) 部局技術責任者は、通信回線の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。

解説：適正なアクセス制御の維持を求める事項である。通信要件については、組織、情報システム又はサービスの変更等により変化するため、当該変更等に応じてアクセス制御の設定を見直す必要がある。「定期的」とは、３か月から６か月ごとに実施することを想定しており、短い期間で実施するとセキュリティ確保に効果的である。また、必ずしも当該変更等が適時連絡されるとは限らないので、部局技術責任者は定期的にアクセス制御の設定の見直しを行う。

(c) 部局技術担当者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。

解説：確保している性能では適正な運用が困難な状態及び通信回線装置等の故障により通信不能な状態等により、情報の可用性を損なう事態を回避するため、通信回線の利用状況及び状態の確認を求める事項である。問題の発生を推測でき、又は検知できた場合には、事前に対策を行うことが求められる。

(d) 部局技術担当者は、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こと。

解説：学外通信回線と送受信される情報から不正アクセス行為を検知するための事項である。「通信内容を監視する」とは、侵入検知システム等を利用して、通信される情報から不正アクセス等の行為がないかを監視することが挙げられる。

第 2.4 部　個別事項についての対策

2.4.1 その他

2.4.1.1 情報システムへの IPv6 技術の導入における対策

趣旨（必要性）

政府機関では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 通信プロトコルは IPv4 通信プロトコル環境下と同様にセキュリティ上のリスクがあるとともに、グローバル IP アドレスによる直接通信の利用等に際し考慮すべきリスクも考えられる。また 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いても、新旧の規格が共存することから、十分に検討し、適切な措置を講じないと、情報システムのセキュリティを損なうおそれがある。さらに、昨今、電子計算機及び通信回線装置には IPv6 技術を利用する通信機能が標準で備わっているものが増えていることから、意図せず IPv6 技術を利用する通信機能が動作している可能性がある。このため、それぞれの環境を前提として、対策を講ずる必要がある。

なお、IPv6 に関する最新の動向については、引き続き状況の変化が予想されるため、本学においても、IPv6 のセキュリティ対策に関する動向を十分に注視し、適切に対応していく必要がある。これらのことを勘案し、本項では、IPv6 技術を利用する情報システム、IPv4 技術を利用する通信と IPv6 技術を利用する通信が共存する情報システムのセキュリティ確保に関する対策基準を定める。

遵守事項

(1) IPv6 通信がもたらす脆弱性対策

(a) 部局技術責任者は、IPv6 技術を利用する通信（以下「IPv6 通信」という。）を想定して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及びソフトウェアについて、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に IPv6 Ready Logo Program に基づく Phase-2 準拠製品がある場合には、当該製品を情報システムの構成要素として選択すること。

解説：IPv6 に対応する機器等の購入において、一定水準以上のセキュリティ機能を有する製品を選択することを求める事項である。国際的な IPv6 に関する標準プログラムである IPv6 Ready Logo Program による客観的な基準に準拠する製品を選択することにより、安全性の高い情報システムの構築が期待できる。

(b) 部局技術責任者は、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 アドレスによる直接の到達性における脅威を防止するための措置を講ずること。

解説：IPv6 で新たに導入された通信制御機構や、IPv6 の特徴である外部ネットワークとの直接接続の容易さに起因する各種攻撃への対策を求める事項である。

対策としては、不正な機器からの経路調査コマンド（traceroute 等）及び ICMP エ

コー要求等に応答しない、サービス不能攻撃への対策、並びに認可した宛先からのみアクセスを可能にする等が挙げられる。

(c) 部局技術責任者は、IPv6 通信を想定して構築する情報システムにおいて、不正な通信を制限するフィルタリングを適切に行うこと。

解説：IPv6 の特徴として、アドレスが長い、アドレスの省略形が複数パターン存在し一意に定まらない、端末が複数の IP アドレスを持つ等が挙げられる。このような複雑なアクセス制御が設定の不備等を招き不正アクセス等に繋がるリスクが高まるため、フィルタリングを適切に実施することを求める事項である。

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。

(d) 部局技術責任者は、情報システムに IPv6 通信の機能を導入する場合には、IPv6 移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。

解説：IPv4 技術を利用する通信と IPv6 通信の両方を共存させることを可能とする IPv6 移行機構の選定と利用に当たり、必要な措置を求める事項である。

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電子計算機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、学内のネットワークが外部から攻撃される危険性がある。管理された電子計算機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等、不適切な IPv6 通信を制御する対策が必要である。

(e) 部局技術責任者は、IPv6 通信を想定して構築する情報システムにおいて、IPv6 に対応していない機器及びソフトウェアの利用によるセキュリティの問題がないように措置を講ずること。

解説：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のセキュリティ上のリスクに対する対策を求める事項である。

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等が挙げられる。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。

(2) 意図しない IPv6 通信の抑止と監視

(a) 部局技術責任者は、高等教育機関相互間及び学内のみで利用する情報システムについて、IPv6 通信を想定していない通信回線に接続される全ての電子計算機及び通信回線装置に対して、IPv6 通信を抑止するための措置を講ずること。

解説：高等教育機関相互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措置を求める事項である。

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侵入検知システム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 通信が可能な電子計算機においては、IPv4 ネットワークに接続している時でも IPv6 通信による当該電子計算機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、電子計算機と外部のネットワークとの間に利用者や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電子計算機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 通信を抑止するための措置を講ずることが必要である。

(b) 部局技術責任者は、高等教育機関相互間及び学内のみで利用する情報システムについて、IPv6 通信を想定していない通信回線を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずるとともに、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を講ずること。

解説：意図しない IPv6 通信が情報システムに与える脅威から情報システムを守るための事項である。

IPv6 技術にはアドレスの自動構成機構が提供されている。電子計算機から送出されるアドレスの自動構成を要求する通信パケットや、ルータから送出されるアドレスの自動構成を提供する通信パケットが学内通信回線を流れている場合には、管理者や利用者が気付かないうちに IPv6 技術のアドレス自動構成機構が利用されていることを示唆している。また、IPv6 通信を想定していない学内通信回線において、IPv6-IPv4 トンネル機構で使用する通信パケットが検知された場合は、IPv6 技術を

使った悪意のある通信がなされているおそれがある。学内通信回線を管理する者は、このような通信の有無を監視して、IPv6 通信が検知された場合は、当該通信の遮断等の措置を講ずる必要がある。
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 通信を遮断するための措置を講ずることが必要である。

別表1　情報取扱区域のクラス別管理

行番号	遵守事項	対策例		備考	クラス0	クラス1	クラス2	クラス3
1	(凡例) クラス0～クラス3までの列に記載している内容は、それぞれのクラスにおいて、各欄の左側に記載された措置・対策・実施に対して、以下のとおり。 **要**：必要、**不要**：不要、**可**：使用可能又は設定可能、**禁**：禁止 (許可 (届出) 申請が必要)、**対象外**：対象外							
2	(1) 立ち入る者を制限するための管理対策							
3	(ア) 不審者を立ち入らせない措置 2.3.1.1(1)(a)(ア)	所在の表示 (案内板の表示等)	クラス0の表示		対象外	可		
4			クラス1の表示	・例) 学校名、学部等の名称	可			
5			クラス2の表示	・例) 部局名、会議室名	可			
6			クラス3の表示	(※1) サーバ室は非表示	可(※1)			
7	(イ) 要保護情報を取り扱う情報システムについては、区域間を物理的に隔離し、立入り及び退出を管理するための措置 2.3.1.1(1)(a)(イ)	入退出可能な下位区域との接続	クラス0との接続		対象外	不可		
8			クラス1との接続		対象外		可	
9			クラス2との接続		対象外			可
10			クラス3との接続		対象外			
11		下位の区域との分離方法	天井を突き抜ける壁		対象外	可		
12			天井と接する固定式パーティション、壁		対象外	可		
13			天井と接しない固定式パーティション		対象外	可		禁
14			可動式パーティション		対象外	可		禁
15		管理方法	立入り及び退出の管理方法		対象外	・セキュリティゲート ・警備員等による立ち番	・施錠可能な扉、間仕切り等。ただし、ドアガラス等で中が見えても良い。	・施錠可能な扉等。中が見えないこと。
16			全員不在時に制限	(制限方法例) ・扉等を施錠 ・出入口に警備員等を配置し、入退出する者を確認	対象外	要		
17			常に制限		対象外			要
18	(2) 立ち入る者を許可する際の管理対策							
19	(ア) 立ち入る者の確認 2.3.1.1(2)(a)(ア)			「立ち入る」とは、「下位のクラスの区域から上位のクラスの区域への立入り」を指す。	対象外	要		
20	(イ) 退出する者の確認 2.3.1.1(2)(a)(イ)			「退出」とは、「上位のクラスの区域から下位のクラスの区域への退出」を指す。	対象外	不要		
21	(ウ) 許可されていない者の立入り及び退出を制限する措置 2.3.1.1(2)(a)(ウ)				対象外	要		

別表1　情報取扱区域のクラス別管理

行番号	遵守事項		対策例		備考	クラス0	クラス1	クラス2	クラス3
22	(エ) 継続的に立ち入る者を許可する手続 2.3.1.1(2)(a)(エ)					対象外	要		
23	(オ) 継続的に立入りを許可された者に変更がある場合の手続 2.3.1.1(2)(a)(オ)					対象外	要		
24	(カ) 立入り及び退出の記録及び監視 2.3.1.1(2)(a)(カ)				・例) 警備員又は防犯カメラ等の導入	対象外	不要		要
25	(3) 訪問者がある場合の管理対策								
26	(ア) 訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置 2.3.1.1(3)(a)(ア)		登録申請(訪問者の身元確認)	事前貸与者(※2)	・学外施設等、本学で管理対策を講ずることが出来ない場合は、当該施設等に対策状況を確認するなどして、管理対策を決定する。 (※2) ・「事前貸与者」とは、事前に識別カードを貸与されている者を指す。(学外の者で、継続的に立入りを許可された者) ・「訪問者」とは、事前に識別カードを貸与されていない者を指す。 ・「事前に識別カードを貸与されている」とは、民間事業者等に、継続的な立入りのために本学のセキュリティゲートを通過可能な識別カードを貸与している場合を指す。 (※3) ・クラス0からクラス1へ進入する際の確認・審査で代替とすることも可能	不要			要
27				訪問者(※2)		不要	要	要 (※3)	
28	(イ) 訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置 2.3.1.1(3)(a)(イ)		訪問記録	事前貸与者(※2)		不要			要
29				訪問者(※2)		不要			要
30	(ウ) 訪問相手の事務従事者が訪問者の情報取扱区域への立入りについて審査するための手続の整備 2.3.1.1(3)(a)(ウ)		登録申請(訪問者の立入り時の審査)	事前貸与者(※2)		不要			要
31				訪問者(※2)		不要	要	要 (※3)	
32	(エ) 訪問者の立ち入る区域を制限するための措置 2.3.1.1(3)(a)(エ)			事前貸与者(※2)		不要			要
33				訪問者(※2)		不要	不要		要
34	(オ) 訪問相手の事務従事者による訪問者に付き添う措置 2.3.1.1(3)(a)(オ)		事務従事者の帯同、エスコート	事前貸与者(※2)		不要			要
35				訪問者(※2)		不要	不要		要
36	(カ) 訪問者と継続的に立入りを許可された者とを外見上判断できる措置 2.3.1.1(3)(a)(カ)		・訪問者と継続的に立入りを許可された者との外見上の区別			不要	要		
37	(4) 設置する設備の管理対策								
38	要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している電子計算機及び通信回線装置の盗難及び当該場所からの不正な持ち出しを防止するための措置 2.3.1.1(4)(a)	端末	・セキュリティワイヤーによる固定		(※4) 当該クラスへの立入りの際に立ち入る者の確認を行う等の措置をとり、入退出者を制限できる場合は、部屋全体の施錠管理にて対策を講ずることも考えられる。	対象外	要	要(※4)	
39		サーバ装置	・機器扉付きラック等で施錠管理 ・セキュリティワイヤーによる固定			対象外	要	要(※4)	
40		通信回線装置 (装置への主体認証が必要なもの)	・機器扉付きラック等で施錠管理			対象外	要	要(※4)	
41		通信回線装置 (装置への主体認証が不要なもの)				対象外	要	要(※4)	
42	要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置の設置に係る対策 2.3.1.1(4)(b)	(ア) 他の区域との物理的な隔離				対象外	不要	要	
43		(イ) 表示用デバイスの盗み見防止				対象外	不要		要
44		(ウ) 電源ケーブル及び通信ケーブルの損傷及び盗聴防止	・ケーブルの床下への埋設 ・ケーブルのナンバリング			対象外	不要		要

別表1　情報取扱区域のクラス別管理

行番号	遵守事項		対策例		備考	クラス0	クラス1	クラス2	クラス3
45		(エ) 電磁波による情報漏えい対策	・電磁波軽減フィルタの利用			対象外	不要		
46	(5) 作業がある場合の管理対策								
47	当該区域内での作業を監視するための措置 2.3.1.1(5)(a)		事務従事者の作業の立会、監視	・当該作業に関係する他の事務従事者による同行、立会		対象外	不要		
48				・監視カメラ等による監視		対象外	不要		要
49			業者の作業の立会、監視	・担当の事務従事者による同行、立会		対象外	不要		要
50				・監視カメラ等による監視		対象外	不要		要

別表2　情報取扱区域のクラス別利用制限

行番号	遵守事項		対策例	備考	クラス0	クラス1	クラス2	クラス3
1	（凡例） 許可：（部局技術責任者及び職場情報セキュリティ責任者からの）許可が必要、 届出：（部局技術責任者及び職場情報セキュリティ責任者への）届出が必要（部局技術責任者及び職場情報セキュリティ責任者が届出不要と判断した場合は、不要）、 禁止：原則禁止（許可を求める場合は、例外措置の適用の申請が必要（事務情報セキュリティ対策管理基準に定める許可権限者の承認が必要））、 要：必要、不要：許可又は届出が不要、可：設置可能、対象外：対象外							
2	（1）立ち入る者を制限するための利用制限対策							
3	事務従事者であることを常時視認することが可能な状態にすること 2.3.1.1(6)(a)		識別カードの着用、明示（学外の者も含む）		不要	要		
4	（2）物品の持込み、持ち出し及び利用についての利用制限対策							
5	要保護情報を取り扱う情報システムに関連する物品の持込み及び持ち出しに係る対策 2.3.1.1(7)(a)	（ア）持込み及び持ち出しを行う措置			対象外	不要		
6		（イ）記録の保存			対象外	不要		
7		（ウ）情報システムに関連しない電子計算機等の持込みの制限	荷物検査		対象外	不要		
8	事務従事者の所持する府省庁支給以外の情報システム（モバイル端末及び記録装置）の持込みの制限等 2.3.1.1(7)(a)	（ウ）情報システムに関連しない電子計算機等の持込みの制限		・荷物の持込を許可しない場合は、荷物の預りを可能にする環境構築が必要。	対象外	不要		不要
9			起動・利用 （学内LAN未接続、要保護情報は取り扱わない場合）	・「起動・利用」は「持込」が前提 （※1） 学内通信回線への接続を認める場合は、学内のすべての情報にアクセスできる可能性があるリスクを考慮すること。	対象外	不要		
10		モバイル端末の起動・利用 1.4.2.2(2)(a) （機密性3情報、完全性2情報又は可用性2情報を取り扱う場合）			許可(※1)			
11		モバイル端末の起動・利用 1.4.2.2(2)(b) （機密性2情報であって完全性1情報かつ可用性1情報を取り扱う場合）			届出(※1)			
12	学外の者の所持するモバイル端末及び記録装置の持込みの制限等 2.3.1.1(7)(a)、 1.2.5.3(3)(b)	（ウ）情報システムに関連しない電子計算機等の持込みの制限		・荷物の持込を許可しない場合は、荷物の預りを可能にする環境構築が必要。	対象外	不要		要
13			起動・利用 （学内LAN未接続）	・「起動・利用」は「持込」が前提	対象外	不要		
14	事務従事者による写真撮影、録音 2.3.1.1(7)(b)			（※2） 許可又は届出先となる主体は、当該区域を管理する区域情報セキュリティ責任者となるが、許可又は届出の窓口は担当の事務従事者が行うことが考えられる。	対象外	不要		
15	学外の者による写真撮影、録音 2.3.1.1(7)(b)、1.2.5.3(3)(b)				対象外	不要	要（※2）	

別表2　情報取扱区域のクラス別利用制限

行番号	遵守事項	対策例		備考	クラス0	クラス1	クラス2	クラス3
16	(3) 荷物の受渡しについての利用制限対策							
17	受渡し管理 2.3.1.1(8)(a)	宅配便、荷物			不要		要	
18		要保護情報又は機密性1情報			不要			
19	(4) 情報処理の制限							
20	要管理対策区域外での情報処理の制限 1.4.2.1(2)(a)(b)	機密性2情報について情報処理を行う場合			届出	対象外		
21		機密性1情報並びに完全性2情報又は可用性2情報について情報処理を行う場合			許可	対象外		
22		機密性3情報について情報処理を行う場合			許可	対象外		
23	(5) 設備の設置							
24	端末の設置 2.3.2.1(1)(b)			・追加で設置する場合 ・モバイル端末について部局総括責任者の承認を得た場合は、この限りでない。	禁	可	可	
25	通信回線装置の設置 2.3.4.1(1)(i)				禁	可	可	
26	サーバ装置の設置 2.3.2.1(1)(b)				禁	禁	可	
27	(6) ネットワークの接続							
28	通信回線構築によるリスクを検討し、通信回線を構築すること 2.3.4.1(1)(a) 無線LAN環境を構築する場合に、必要に応じて措置を講ずること 2.3.4.2(3)(b)	学内LAN	クラス0のLANとの接続	・追加で設置する場合	対象外	(学外通信回線との接続に準じる)		
29			クラス1のLANとの接続		(学外通信回線との接続に準じる)	可	不可	
30			クラス2のLANとの接続			不可	可	
31			クラス3のLANとの接続				可	
32		無線LAN	クラス0の無線LANとの接続	・追加で設置する場合 ・他の区域との接続制限の例：MACアドレス、IEEE802.1x等による接続制限	対象外	(学外通信回線との接続に準じる)		
33			クラス1の無線LANとの接続		(学外通信回線との接続に準じる)	可	不可	
34			クラス2の無線LANとの接続			不可	可	可
35			クラス3の無線LANとの接続				可	可
36		学内から本学管理外のネットワーク経由でのインターネット直接接続		・学内通信回線（学内LAN）へは、接続禁止が前提 ・「本学管理外のネットワーク」とは、Wi-fiルータ（学外通信回線へ直接接続可能な通信回線装置）等の利用によるインターネットへの直接接続を想定	対象外	不可		

B2651 証明書ポリシー（CP）

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。

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）

B2652 認証実施規程（CPS）

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。

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）

用語集

	用 語	説 明
あ	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。
	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。また、狭義には、利用者等に付与されたユーザ ID（識別コード）とパスワード（主体認証情報）の組み合わせ、又はそれらのいずれかを指して「アカウント」という。
	アクセス制御	主体によるアクセスを許可する客体を制限することをいう。
	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。
	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。
	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。
	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ハードウェア、ソフトウェア、ファームウェア及びそれらの組合せをいう。
	安全区域	電子計算機及び情報ネットワーク機器を設置した事務室、研究室、教室又はサーバルーム等の内部であって、利用者等以外の者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。
い	委託先	情報システムに関する計画、構築、運用等の情報処理業務の一部又は全部を請け負った者をいう。
	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。
	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。
う	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	安全区域内で職務に従事する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。
え	ST 確認	評価機関による ST 評価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。
	ST 評価	セキュリティ設計仕様書(ST:Security Target)がITセキュリティ評価基準(ISO/IEC 15408)に適合していることを IT セキュリティ評価方法 CEM（Common Methodology for Information Technology Security Evaluation）に則って、ST の評価を行うことが可能な機関が評価することをいう。
	MRA	Mail Retrieval Agent の略称であり、メールボックスに格納された電子メールを、POP3、IMAP 等で MUA へ渡すソフトウェアをいう。いわゆる POP3 サーバ、IMAP サーバ等。
	MSA	Mail Submission Agent の略称であり、MUA から SMTP で電子メールを受信し、当該電子メールを MTA に渡す処理を行うソフトウェアをいう。MTA の機能に含むとする考え方もある。
	MTA	Mail Transfer Agent の略称であり、他のサーバから SMTP で受信した電子メール、又は MSA から渡された電子メールを、必要に応じて、SMTP で他のサーバへ転送したり、ローカルのメールボックスに格納するソフトウェアへ渡したりする処理を行うソフトウェアをいう。いわゆる SMTP サーバ等。

	用 語	説 明
	MUA	Mail User Agent の略称であり、電子メールの読み書き、MSA 経由での電子メールの送信、MRA 経由での電子メールの受信、送受信した電子メールの管理を行うソフトウェアをいう。いわゆるメーラ等。
	エラーメール	あて先のメールアドレスが存在しない場合等に、送信元のメールアドレス又は MTA の管理者用メールアドレスあてに送信不能を伝えるために、MTA によって自動的に送られる電子メールをいう。
か	外部委託	情報システムに関する計画、構築、運用等の情報処理業務の一部又は全部を教職員等以外の者に請け負わせることをいう。
	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。
	学外通信回線	物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び府省庁管理又は他組織管理）及び通信回線装置を問わず、本学が管理していない電子計算機が接続され、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。
	学外での情報処理	本学の管理部外で大学事務の遂行のための情報処理を行うことをいう。なお、オンラインで学外から本学の情報システムに接続して、情報処置を行う場合だけではなく、オフラインで行う場合も含むものとする。
	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。
	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。
	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。
	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、情報及び関連資産にアクセスできる状態を確保することをいう。
	可用性1情報	可用性2情報以外の情報（書面を除く。）をいう。
	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。
	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をいう。
	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。
	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。
き	機器等	情報機器等及びソフトウェアをいう。
	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状態を確保することをいう。
	機密性1情報	機密性2情報又は機密性3情報以外の情報をいう。
	機密性3情報	本学で取り扱う情報のうち、秘密文書に相当する機密性を要する情報をいう。

	用 語	説 明
	機密性2情報	本学で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、利用者等の権利が侵害され又は本学の活動の遂行に支障を及ぼすおそれがある情報をいう。
	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。
	強制アクセス制御（MAC：Mandatory Access Control）	主体が客体(情報、ファイル等)に設定したアクセス制御について、その設定の継承を情報システムが強制的に行う方式をいう。強制アクセス制御の機能を備えた情報システムでは、主体が客体を保護すべき対象とした場合には、アクセスを許可された者であっても、それを保護すべき対象ではないものとすることはできない。すなわち、主体が設定したアクセス制御の継承は、任意ではなく強制されることになる。
	業務継続計画	中央省庁業務継続ガイドライン第1版（平成19年6月、内閣府）に基づき府省庁において策定するBCP（Business Continuity Plan: 事業継続計画）をいう。
	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。
	記録媒体	情報が記録され、又は記載されるものをいう。なお、記録媒体には、書面、書類その他文字、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、電子計算機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、電子計算機や通信回線装置に内蔵される内蔵電磁的記録媒体と外付けハードディスク、CD-R、DVD、MO、USBメモリ、フラッシュメモリ等の外部電磁的記録媒体がある。
	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。
く	クロスサイトスクリプティング	クロスサイトスクリプティングとは、入力データの正当性検査の甘いウェブサイトの利用者を狙った攻撃で、データ入力の際に悪意のあるサイトを経由すると、そこでスクリプトと呼ぶプログラムが入力データに挿入される。挿入されたスクリプトは、入力データをチェックしていないサーバで利用者入力データとともにブラウザに送り返される。スクリプトはブラウザの画面には表示されないが、スクリプト実行を制限していないブラウザでは解釈実行されてしまい、重要な情報が盗み取られたりする。 （IPAセキュリティセンターによる解説） http://www.ipa.go.jp/security/awareness/vendor/programming/a01_02.html
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。
こ	公開されたセキュリティホール	誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造・提供元等から公表されたセキュリティホール、セキュリティ関連機関から公表されたセキュリティホールが該当する。
	交換用電子メールサーバ	他のドメインと電子メールを交換（送受信）するための電子メールサーバであり、DNS情報において交換用であることが明示されている電子メールサーバであり、MTAが動作しているものをいう。いわゆるMXサーバ。

	用 語	説 明
	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
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。
	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。
	最少（最小）特権機能	管理者権限を実行できる範囲を管理作業に必要な最少の範囲に制限する機能をいう。
し	識別	情報システムにアクセスする主体を特定することをいう。
	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。
	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。
	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
	事務情報システム	事務情報を扱う情報システムをいう。
	重要な設計書	情報システムに関する設計書のうち、当該情報システムの適切な管理に必要なものであり、その紛失、漏えい等により、大学事務の遂行に支障を及ぼすものをいう。
	主体	情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。
	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、本統一基準における「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。
	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。

	用 語	説 明
	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、磁気ストライプカードやICカード等がある。
	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
	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。
	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
	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。
	情報セキュリティ関係規程	情報システム運用基本方針及び同方針に定められた内容に基づき定めた規程、基準、実施手順をいう。
	情報ネットワーク機器	情報ネットワークの接続のために設置され、電子計算機により情報ネットワーク上を送受信される情報の制御を行うための装置（ファイアウォール、ルータ、ハブ、情報コンセント又は無線ネットワークアクセスポイントを含む。）をいう。
	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。
せ	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の蔓延や意図的な頒布 －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
	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	本学の全学統一認証に対応した情報システムの利用に当たって用いるアカウントをいう。これに加え、本学が契約し外部委託したシステムおよびサービス利用のためのアカウントも含むものとする。
そ	送受信用電子メールサーバ	電子メールを利用している利用者等のメールボックスが存在し、当該利用者等が MUA を利用して電子メールを送受信するために接続するための電子メールサーバであり、MTA、MSA、MRA が動作しているものをいう。
	ソフトウェア	電子計算機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、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。

	用 語	説 明
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。
	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。
	耐タンパー性	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。
	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。
	端末	利用者等が直接操作を行う電子計算機（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。）であり、いわゆる PC のほか、PDA 等も該当する。
つ	通信回線	これを利用して複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みをいう。回線及び通信回線装置の接続により構成された通信回線のことを物理的な通信回線といい、物理的な通信回線上に構成され、電子計算機間で所定の通信様式に従って情報を送受信可能な通信回線のことを論理的な通信回線という。
	通信回線装置	回線の接続のために設置され、電子計算機により回線上を送受信される情報の制御を行うための装置をいう。いわゆるリピータハブ、スイッチングハブ及びルータのほか、ファイアウォール等も該当する。
て	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。
	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。
	デュアルロック	行為に対して、少なくとも 2 名の者が操作しなければその行為を完遂できない方式のことをいう。
	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。
	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。
	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。
	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並びにそのアプリケーションを動作させる電子計算機をいう。
	電子メールサービス提供ソフトェア	電子メールの送受信のためにサーバ装置上で動作する MTA、MSA、MRA であって、部局技術担当者によって運用管理が行われているものをいう。
と	ドメインネームシステム（DNS）	ドメイン名やホスト名と IP アドレスとの対応関係を管理するデータベースシステムである。
	ドメイン名	サーバ装置や通信回線装置に付与した IP アドレスを、扱いやすいように英数字および一部の記号を用いて表したものをいう。たとえば、sample.ac.jp のこと。
	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。
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。

	用 語	説 明
は	パッチ	発見された問題点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、パッチ、ホットフィクス、サービスパック等名称が異なる。
ひ	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。
	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。
ふ	フィッシング (phishing)	たとえばオークションサイトと類似の画面を持ったなりすましサイトに利用者を誘導し ID やパスワードを盗み出すような行為である。ニセのサイトには、電子メール等で HTML メールのリンクから誘導する。
	VPN (Virtual Private Network)	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。
	複数要素 (複合) 主体認証	知識、所有、生体情報などのうち、複数の方法の組合せにより主体認証を行う方法である。
	不正プログラム	コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。
	不正プログラム定義ファイル	アンチウイルスソフトウェア等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。
	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。
	踏み台	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。
ほ	ポリシー	本学が定める「B1000 情報システム運用基本方針」及び「B1001 情報システム運用基本規程」をいう。
	本学支給以外の情報システムによる情報処理	本学支給以外の情報システムを用いて大学事務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことであり、例えば、本学の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。
	本学支給以外の情報システム	本学が支給する情報システム以外の情報システムをいう。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情報システムも含むものとする。
む	無線 LAN	無線通信で情報を送受信する通信回線をいう。無線 LAN の規格としては、802.11a、802.11b、802.11g、802.11n、Bluetooth 等が挙げられる。
め	明示等	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る認識が共通となる措置については、明示等に含むものとする。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とする。
	メールボックス	あるメールアドレスあてに届いた電子メールを保管しておく電子メールサーバ上の領域をいう。メールボックスは、メールアドレスごとに存在し、メールアドレスあてに届いた電子メールは、当該メールアドレス専用のメールボックスに保管される。

	用 語	説 明
も	モバイル PC	端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用するノート型 PC は、モバイル PC に含まれない。
ゆ	URI (Universal Resource Identifier)	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。
よ	要安定情報	可用性2情報をいう。
	要機密情報	機密性2情報及び機密性3情報をいう。
	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。
	要保全情報	完全性2情報をいう。
り	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
	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。
	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扱う者をいう。
	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。
れ	例外措置	事務従事者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。
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。
	ログオン	ログインの結果により、主体認証を要求した主体が正当であることが情報システムに確認された状態をいう。

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）ページ番号の書式の意味は以下の通りである。

太字：用語を定義しているページ

斜字：事務情報システムのみが対象の規程等の内部で用語を定義・解説しているページ