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

2007 年 2 月 15 日

国立情報学研究所 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

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

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、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。

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。

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

サンプル規程は、仮想の国立 A 大学における体制と規程を想定して検討した。A 大学の概要は以下の通りである。

- 文学部と理学部の２学部で構成され、両学部とも在学生 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る。なお、事務局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。

サンプル規程は、図１に示すような階層構造を有する。各階層において必要となるポリシー、実施規程及び手順の体系を図２に示す。

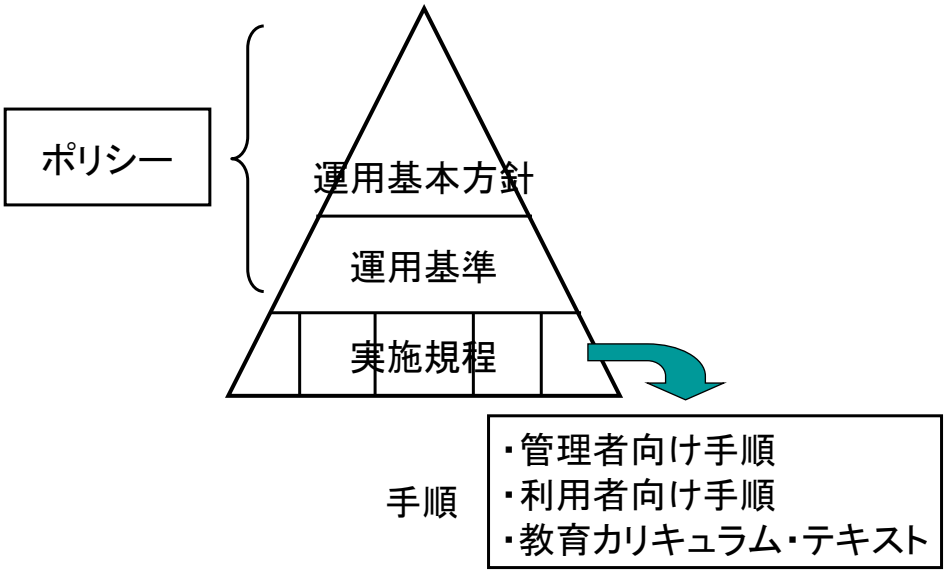
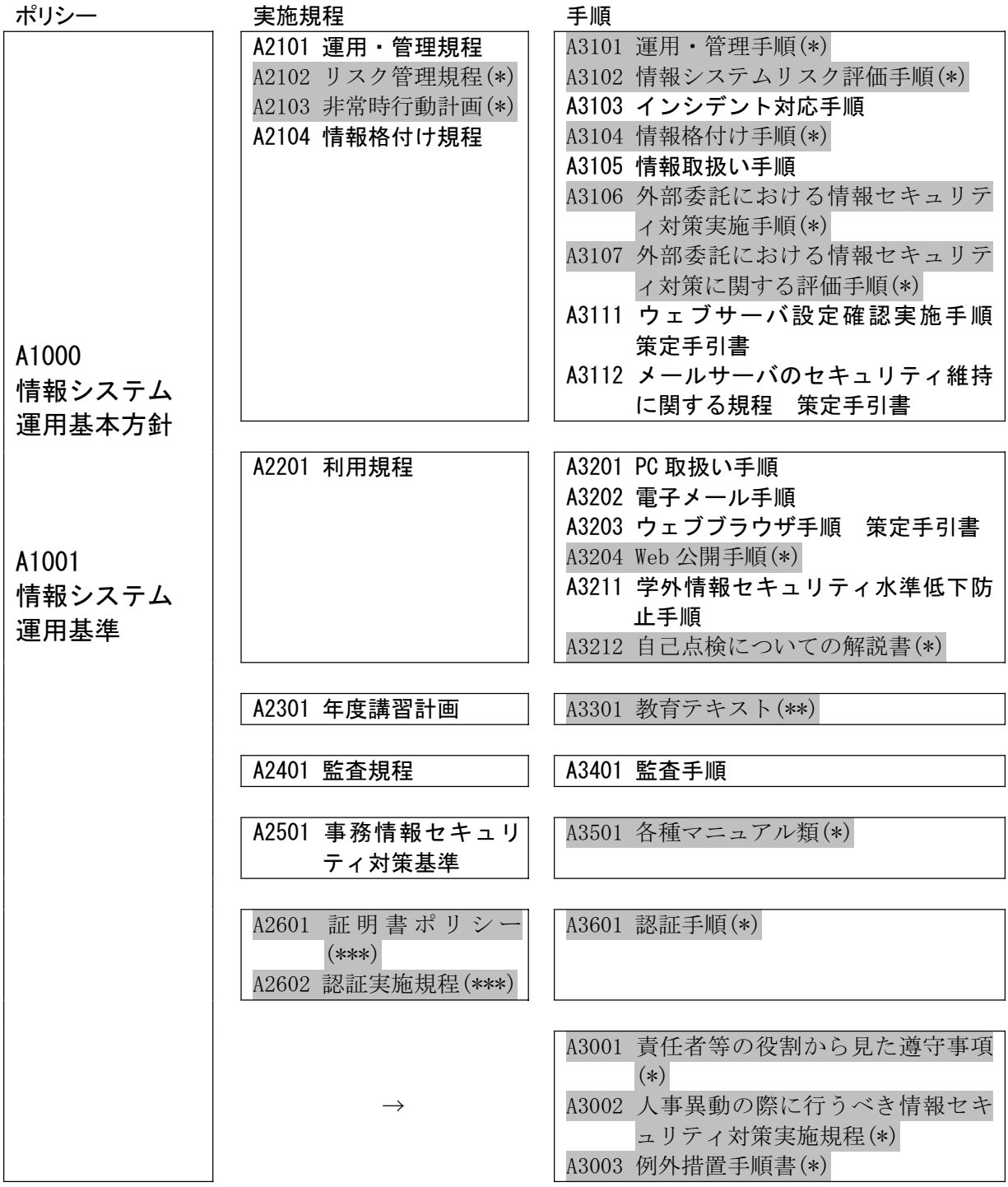


図1　運用ポリシー・実施規程・手順の位置付け



アミ掛け部分（明朝書体）は今年度の策定対象外とした文書。それぞれの対応状況は以下の通り：

(*) 2007 年度以降に整備する規程等

(**) 2006 年度はカリキュラムの項目名のみ

(***) UPKI イニシアティブにて策定中のものに準ずる方向で検討中

図２　ポリシー・実施規程・手順の体系

また、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。

なお、本ポリシー及び、実施規程、手順における管理態勢は、2005 年 12 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」の体制と表１のとおりに対応づけられるので参考にされたい。

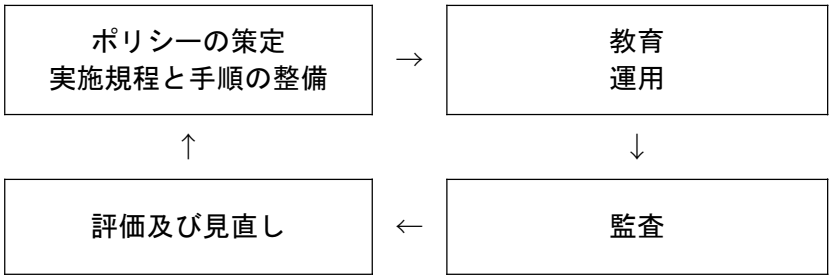


図３　ポリシーの評価及び見直し

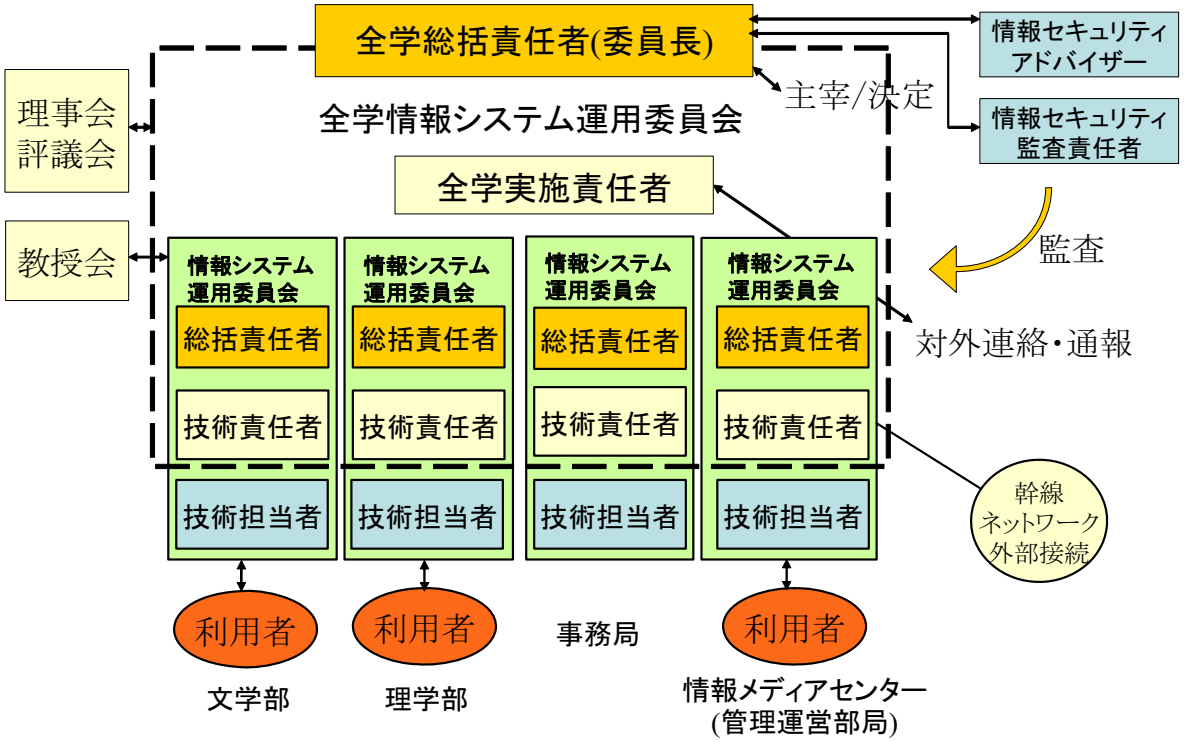


図４　情報システム運用管理体制

表 1　情報システム運用管理体制の対応

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

(注) 事務局においては課長又は室長を職場情報セキュリティ責任者として任命するが、この用語は研究室や学生にとってなじまないことから、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。

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「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）、
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（国立情報学研究所）、貴志武一（千葉大学）、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）、布施勇（東京工業大学）、
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）、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）

○領域幹事・幹事補佐

総論・体制：　幹事・冨士原裕文
ネットワーク運用：　幹事・金谷吉成、幹事補佐・丸橋透
認証運用：　幹事・岡部寿男、幹事補佐・高井昌彰
事務：　幹事・布施勇、幹事補佐・貴志武一
利用：　幹事・長谷川明生、幹事補佐・小川賢
教育・倫理：　幹事・中西通雄、幹事補佐・中野博隆

A1000 情報システム運用基本方針

A1000-01 （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。

A1000-02 （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、別に定める運用基準により、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：本学は、「研究と教育を通じて、社会の発展に資する」ことを基本理念とするものである。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

A1000-03 （利用者の義務）

第三条　本学情報システムを利用する者は、本方針及び運用基準に沿って利用し、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。

A1000-04 （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。

A1001 情報システム運用基準

第一条　Ａ大学（以下「本学」という。）における情報システムの運用については、この運用基準の定めるところによる。

A1001-02 （適用範囲）

第二条　この運用基準は、本学情報システムを運用・管理・利用するすべての者に適用する。

解説：来学中に利用する訪問者などの臨時利用者や業務委託者を含む。

A1001-03 （定義）

第三条　この運用基準において、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をいう。なお、事務処理に供され、事務局が運用責任を持つ情報システムを、研究・教育用の情報システムと区別するため、事務局情報システムと呼ぶ。

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。

二　情報ネットワーク

情報ネットワークには次のものを含む。

(1)　本学により、所有又は管理されている全ての情報ネットワーク

(2)　本学との契約あるいは他の協定に従って提供される全ての情報ネットワーク

解説：VPN などで学外に拡張されたネットワークも含む。

三　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。

四　事務局情報システム

本学情報システムの内、事務処理に供され、事務局が運用責任を持つ情報システムをいう。

五　ポリシー

本学が定めるＡ大学情報システム基本方針及び本運用基準をいう。

六　実施規程

ポリシーに基づいて策定される規程及び計画をいう。

七　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を指す

八　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。

九　教職員等

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）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、財団などの構成員を含む考え方もある。

十　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をいう。

十一　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：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。

十二　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。

十三　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：たとえば、コンピュータ内のハードディスクやメモリなどの内部記憶媒体と、取り外し可能な CD－ROM やメモリ、磁気カード、IC カードなどの外部記憶媒体が含まれる。コンピュータからの印刷出力、入力用に記入する伝票、フォームなどの帳票類はここでは含まれない。

十四　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。

A1001-04 （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　全学向け教育及び管理運営部局の部局技術担当者向け教育を統括する。

４　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。

５　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。

A1001-05 （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。

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制定及び改廃

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、年度計画を策定し、教育・啓発を実施する。

四　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　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システム監査規程として定める。

情報システムに係る監査の実施は、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。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。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　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。

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、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

A1001-06 （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

A1001-07 （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。

A1001-08 （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薦により学長が任命する。

A1001-09 （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。

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。

A1001-10 （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。

A1001-11 （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

A1001-12 （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。

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。

A1001-13 （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

A1001-14 （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

A1001-15 （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。

A1001-16 （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。

A1001-17 （部局技術担当者）

第十七条　部局技術責任者は、複数の技術担当者を任命して実務を担当させることができる。技術担当者は部局技術責任者が推薦し部局長が任命する。

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。

A1001-18 （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者又は許可者

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。その場合には、同じ承認又は許可をする役割を担う他者に申請し、承認又は許可を得る必要がある。

A1001-19 （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基準並びに格付け及び取扱制限を明示する手順を整備する。

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

A1001-20 （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　全学総括責任者は、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、全学総括責任者が、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・利用する者は、原則として、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・利用する者は、組織及び個人として措置を講ずることが重要である。

A1001-21 （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。

A1001-22 （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運用基準）に基づく手順に従って実施されていることを監査する。監査に際しては、別途定める監査規程に従う。

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。

A1001-23 （見直し）

第二十三条　ポリシー（情報システム運用基本方針及び本運用基準）、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・利用する者は、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・利用する者に求める事項である。

A2101 情報システム運用・管理規程

第一章　総則

A2101-01　（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運用及び管理に関する事項を定めることにより、本学の有する情報資産を適正に保護、活用し、並びに情報システムの信頼性、安全性及び効率性の向上に資することを目的とする。

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、「A1000 情報システム運用基本方針」及び「A1001 情報システム運用基準」（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

A2101-02　（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Ａ大学情報システム運用基本方針をいう。

二　運用基準　本学が定めるＡ大学情報システム運用基準をいう。

三　情報資産　情報システム、情報ネットワークに接続された情報ネットワーク機器並びに電子計算機、及びそこで取り扱われる情報をいう。ただし、別に定める場合を除き、情報は電磁的記録（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た記録をいう。）に限るものとする。

四　情報システム　情報処理及び通信に係るシステムをいう。

五　情報ネットワーク　通信回線を利用して、複数の電子計算機及び情報ネットワーク機器を接続し、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。

六　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。

七　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。

八　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。

九　利用者等　Ａ大学情報システム利用規程において定める利用者のほか、本学情報資産および情報システムを取扱う者をいう。

十　主体認証　識別符号（ユーザ ID）を提示した利用者等又は電子計算機が、情報システムにアクセスする正当な権限を有するか否かを検証することをいう。識別符号（ユーザ ID）とともに正しい方法で主体認証情報（パスワード）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利用者等又は電子計算機等を正当な権限を有するものとして認識する。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。

十一　識別符号（ユーザ ID）　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符号のうち、情報システムが利用者等又は電子計算機を特定して認識する符号をいう。代表的な識別符号として、ユーザ ID が挙げられる。

十二　主体認証情報（パスワード）　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。代表的な主体認証情報として、パスワードが挙げられる。

十三　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、利用者等又は電子計算機に付与された正当な権限をいう。また、狭義には、利用者等又は電子計算機に付与された識別符号（ユーザ ID）及び主体認証情報（パスワード）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。

十四　その他の用語の定義は、運用基本方針及び運用基準の定めるところによる。

解説：用語は、ポリシー・実施規程・手順を通して統一しておくこと。但し、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、利用者は、利用規程を読みこれを遵守しなければならないが、運用・管理規程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、読もうと思ったときに読めるように準備しておくことは必要である。

A2101-03　（適用範囲）

第三条　この規程は、情報資産及び情報システムを運用・管理する者に適用する。

解説：情報資産及び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

ゆるエンドユーザにあっても、本学の情報資産及び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。

A2101-04　（組織体制）

第四条　全学情報ネットワークの運用・管理は、運用基本方針及び運用基準に従い、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担当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　部局情報ネットワークの運用・管理は、運用基本方針並びに運用基準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　全学情報ネットワークと部局情報ネットワークとの調整及び対外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、「A1001 情報システム運用基準」を参照のこと。

A2101-05　（禁止事項）

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

一　情報資産の目的外利用

二　守秘義務に違反する情報の開示

三　部局総括責任者の許可なく情報ネットワーク上の通信を監視し、又は情報ネットワーク機器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　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

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。

第二章　情報システムのライフサイクル

解説：情報システムの設置時、運用時、運用終了時といった情報システムのライフサイクルに着目し、各段階において遵守すべき事項を定め、情報資産及び情報システムを保護するための対策を示す。

第一節　設置時

A2101-06　（セキュリティホール対策）（政府機関統一基準の対応項番 4.2.1(1)）

第六条　部局技術担当者は、電子計算機及び情報ネットワーク機器（公開されたセキュリティホールの情報がない電子計算機及び情報ネットワーク機器を除く。以下この項において同じ。）について、セキュリティホール対策に必要となる機器情報を収集し、書面として整備すること。

解説：セキュリティホール対策に必要となる機器情報の収集と書面整備を求める事項である。セキュリティホール対策に必要となる機器情報としては、例えば、ハードウェアの機種及びソフトウェアの種類並びにバージョン等が挙げられる。

２　部局技術担当者は、電子計算機及び情報ネットワーク機器の構築又は運用開始時に、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：情報システムの運用前までに、情報システムに係る機器の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。

A2101-07　（不正プログラム対策）（政府機関統一基準の対応項番 4.2.2(1)）

第七条　部局総括責任者は、不正プログラム感染の回避を目的とした利用者等に対する留意事項を含む日常的実施事項を定めること。

解説：不正プログラムとは、コンピュータウイルス、ワーム、スパイウェアなどの有害なプログラムをいう。不正プログラムは、これに感染した情報システムを破壊したり、情報を外部に漏えいさせたりすることの他、他の情報システムの再感染を引き起こすなど、セキュリティ脅威の原因となり得る。

利用者等に対する注意喚起としては、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、不審なホームページを閲覧しないこと等が考えられる。

また、日常的実施事項としては、例えば、不正プログラムに関する情報の収集や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検出等が挙げられる。

２　部局技術責任者は、不正プログラムから電子計算機（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。）を保護するため、アンチウイルスソフトウェアを導入する等の対策を実施すること。

解説：電子計算機には、原則としてアンチウイルスソフトウェア等を導入することが求められる。但し、電子計算機にアンチウイルスソフトウェアが存在しない場合はこの限りでない。

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のすべ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他、USB メモリーなどの外部記憶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。

A2101-08　（サービス不能攻撃対策）（政府機関統一基準の対応項番 4.2.3(1)）

第八条　部局技術責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける電子計算機、情報ネットワーク機器又は通信回線を有する情報システム。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情報ネットワーク機器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：サービス不能攻撃により情報システムの可用性が失われないよう、機器が備え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、サーバ装置における SYN Cookie、情報ネットワーク機器における SYN Flood 対策機能を有効にすることなどが挙げられる。

A2101-09　（安全区域）（政府機関統一基準の対応項番 5.1.1(1)）

第九条　部局技術責任者は、情報システムによるリスク（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、安全区域に施設及び環境面からの対策を実施すること。

解説：電子計算機及び情報ネットワーク機器において、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、安全区域を定めることが求められる。機器設置の際は、次の点に留意すること。

(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　部局技術責任者は、安全区域に不審者を立ち入らせない措置を講ずること。

解説：措置としては、身分を確認できる物の提示の義務化、安全区域の所在の表示の制限等が挙げられる。

３　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、電子計算機を安全区域に設置すること。ただし、モバイル PC 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。

４　部局技術責任者は、情報ネットワーク機器を安全区域に設置すること。

解説：情報ネットワーク機器や通信ケーブルに対する物理的なリスクへの対策を求める事項である。

A2101-10　（規定及び文書の整備）（政府機関統一基準の対応項番 5.2.1(1)、5.3.1(1)）

第十条　部局技術責任者は、電子計算機のセキュリティ維持に関する規定を整備すること。

２　部局技術責任者は、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規定を整備すること。

３　部局技術責任者は、すべての電子計算機に対して、電子計算機を管理する利用者等を特定するための文書を整備すること。

４　部局技術責任者は、電子計算機関連文書を整備すること。

５　部局技術責任者は、通信回線及び情報ネットワーク機器関連文書を整備すること。

解説：「電子計算機関連文書」とは、電子計算機の設計書、仕様書及び操作マニュアル等である。「通信回線及び通信回線装置関連文書」とは、通信回線の設計書、仕様書、通信回線の構成図、電子計算機の識別コード及び情報ネットワーク機器の設定が記載された文書等が挙げられる。これらは、書面ではなく電磁的記録媒体で整備していても差し支えない。

A2101-11　（主体認証と権限管理）（政府機関統一基準の対応項番 5.2.1(1)）

第十一条　部局技術責任者は、利用者等が電子計算機にログインする場合には主体認証を行うように電子計算機を構成すること。

解説：電子計算機を利用した者を特定するために行う事項である。サーバ装置や複数者で利用する共用 PC 等の端末の場合でも利用者に識別符号を個別に割り当て、本人性を確認することが望ましい。

２　部局技術責任者は、ログオンした利用者等の識別符号（ユーザ ID）に対して、権限管理を行うこと。

解説：識別符号ごとに必要となる権限のみを付与することを求める事項である。管理者権限は、最小限の識別符号に与える必要がある。

A2101-12　（電子計算機の対策）（政府機関統一基準の対応項番 5.2.2(1)）

第十二条　部局技術責任者は、電子計算機で利用可能なソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙、または両者を併用することができる。

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　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能力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、テスト等を実施し、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。

３　部局技術責任者は、要保護情報を取り扱うモバイル PC については、学外で使われる際にも、学内で利用される電子計算機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：学外で利用されるモバイル PC は、学内で利用される電子計算機と異なる条件下に置かれる（通常の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、学外でモバイル PC が利用される際の保護手段として、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。

A2101-13　（サーバ装置の対策）（政府機関統一基準の対応項番 5.2.3(1)）

第十三条　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、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、送受信される情報を暗号化すること。

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、通信の暗号化の対策が必要である。

２　部局技術責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。

解説：サーバ装置において、サービスの提供及びサーバ装置の運用・管理に必要となるソフトウェアを定めるための事項である。必要なソフトウェアを定める方法としては、サーバ装置の仕様書において定める、独立の文書として定める等が挙げられる。

3　部局技術責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動すること。

解説：不要なサーバアプリケーションの停止及び不要な機能の無効化により、サーバ装置から潜在的な脅威を排除するための事項である。

A2101-14　（通信回線の対策）（政府機関統一基準の対応項番 5.4.1(1)）

第十四条　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。例えば、部局技術責任者は、リスクを検討した結果、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。

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、通信回線及び情報ネットワーク機器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。通信回線の負荷に関して事前にテスト等を実施し、必要となる容量及び能力を想定し、それを備える。また、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。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、管理部署等から分類することをいう。

4　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情報ネットワーク機器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すべて確認した上で、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。

5　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、通信回線を用いて送受信され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：通信回線を用いて送受信され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、当該情報の暗号化の必要性を検討する必要がある。

6　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、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。本項は、要機密情報、要保全情報及び要安定情報のすべてを対象としている。

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。

7　部局技術責任者は、遠隔地から情報ネットワーク機器に対して、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：遠隔地からの情報ネットワーク機器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、識別符号及び主体認証情報（パスワード）による主体認証、接続する電子計算機の識別符号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。

8　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、契約を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。

9　部局技術責任者は、情報ネットワーク機器上で証跡管理を行う必要性を検討し、必要と認めた場合には実施すること。

解説：通信回線装置上で取得可能な証跡について、証跡管理を行うための事項である。管理として、取得する情報項目の設定、証跡の保存及び点検、分析並びに報告等が挙げられる。

A2101-15　（情報コンセント）

第十五条　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。

A2101-16　（VPN、無線 LAN、リモートアクセス）（政府機関統一基準の対応項番 5.4.2(3)）

第十六条　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、SoftEther 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。

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 接続方法の機密性の確保
八　無線 LAN に接続する電子計算機の管理

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。

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。

A2101-17　（学外通信回線との接続）（政府機関統一基準の対応項番 5.4.3(1)）

第十七条　全学実施責任者は、全学総括責任者の承認を得た上で、学内通信回線を学外通信回線と接続すること。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：学内通信回線と学外通信回線との接続に、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承認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。独立な通信回線の場合でも、遵守すべき対策規準は実施する必要がある。

A2101-18　（上流ネットワークとの関係）

第十八条　全学実施責任者は、本学情報ネットワークを構築し運用するにあたっては、本学情報ネットワークと接続される上流ネットワーク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プロバイダ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 に抵触しないよう利用規程等で定めるとともに、本学ネットワークの構築及び運用に携わる者は、上流ネットワークとの整合性を常に注意しなければならない。

第二節　運用時

A2101-19　（セキュリティホール対策）（政府機関統一基準の対応項番 4.2.1(2)）

第十九条　部局技術担当者は、電子計算機及び情報ネットワーク機器の構成に変更があった場合には、セキュリティホール対策に必要となる機器情報を記載した書面を更新すること。

解説：公開されたセキュリティホールに関連する情報との対応付けをするため、セキュリティホール対策に必要となる機器情報の最新化を求める事項である。

２　部局技術担当者は、管理対象となる電子計算機及び情報ネットワーク機器上で利用している

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。

3　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から、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作成すること。

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　対策テストの必要性

七　対策テストの方法

八　対策テストの実施予定

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、対策計画の作成を求める事項である。「対策テスト」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。

4　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。

5　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。

6　部局技術担当者は、信頼できる方法で対策用ファイルを入手すること。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媒体を利用して入手する方法が挙げられる。また、改ざんなど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。

7　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情報ネットワーク機器が確認された場合の対処を行うこと。

解説：電子計算機及び情報ネットワーク機器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、導入及び利用されているソフトウェアの種類、当該ソフトウェアの設定のことである。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。

8　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。

A2101-20　（不正プログラム対策）（政府機関統一基準の対応項番 4.2.2(2)）

第二十条　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など、日常から行われている不正プログラム対策では対応が困難と判断される場合が挙げられる。

2　部局総括責任者は、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：不正プログラム対策状況を適宜把握し、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。

A2101-21　（脆弱性診断）

第二十一条　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準）によるものとする。なお、脆弱性診断を行う者は、本規程第五条（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。

A2101-22　（規定及び文書の見直し、変更）（政府機関統一基準の対応項番 5.2.1(2) 、5.3.1(2)）

第二十二条　部局技術責任者は、適宜、電子計算機のセキュリティ維持に関する規定の見直しを行うこと。また、当該規定を変更した場合には、当該変更の記録を保存すること。

2　部局技術責任者は、適宜、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規定の見直しを行うこと。また、当該規定を変更した場合には、当該変更の記録を保存するこ

と。

解説：第一項と第二項は、電子計算機及び通信回線を介して提供するサービスのセキュリティ対策を適宜見直すことを求める事項である。セキュリティ対策は、想定するリスクに対して実施すべきであり、時間の経過によるリスクの変化に応じて、その見直しが必要になる。

3　部局技術責任者は、電子計算機を管理する利用者等を変更した場合には、当該変更の内容を、電子計算機を管理する利用者等を特定するための文書へ反映すること。また、当該変更の記録を保存すること。

4　部局技術担当者は、電子計算機の構成を変更した場合には、当該変更の内容を電子計算機関連文書へ反映すること。また、当該変更の記録を保存すること。

5　部局技術担当者は、通信回線の構成、情報ネットワーク機器の設定、アクセス制御の設定又は識別符号（ユーザ ID）を含む事項を変更した場合には、当該変更の内容を通信回線及び情報ネットワーク機器関連文書へ反映すること。また、当該変更の記録を保存すること。

解説：第三項乃至第五項は、部局技術担当者が行った変更を適宜関連文書に反映することで、それぞれの現状と関連文書との整合性を確保するための事項である。変更に関しては、記録を残し、後で参照できるようにしておく必要がある。

A2101-23　（運用管理）（政府機関統一基準の対応項番 5.2.1(2)、5.3.1(2)）

第二十三条　部局技術担当者は、電子計算機のセキュリティ維持に関する規定に基づいて、電子計算機の運用管理を行うこと。

2　部局技術担当者は、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規定に基づいて、日常的及び定期的に運用管理を実施すること。

解説：整備された規定に従っ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を求める事項である。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。

A2101-24　（接続の管理）

第二十四条　部局総括責任者は、情報ネットワークに関する接続の申請を受けた場合は、別途定める情報ネットワーク接続手順に従い、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ネットワーク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。たとえば、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、本学ネットワークと通信できないスタンドアローンのパソコンについては、接続申請は不要である。ただし、研究室のローカルネットワーク（本学ネットワークの一部ではない）に接続したパソコンからの通信が、VPN 接続により本学ネットワークを通過することも考えられるだろう。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。

A2101-25　（資源の管理）

第二十五条　部局技術責任者は、電子計算機の CPU 資源、ディスク資源並びに情報ネットワーク帯域資源等の利用を総合的かつ計画的に推進するため、これらの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。

A2101-26　（ネットワーク情報の管理）

第二十六条　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。

A2101-27　（サーバ装置の対策）（政府機関統一基準の対応項番 5.2.3(2)）

第二十七条　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、対応すること。

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応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保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理すること。

解説：バックアップを取得することにより情報の保護を目的とした事項である。バックアップの対象は、サーバ装置に保存されている情報から適宜選択すること。「安全に管理」とは、記録した媒体を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ことである。また、災害等を想定してバックアップを取得する場合には、媒体を遠隔地に保存することが望ましい。「定期的」とは、一日又は一週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。

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書面として残すための事項である。学内において、ある程度統一的な様式を作成する必要がある。

４　部局技術責任者は、サーバ装置上で証跡管理を行う必要性を検討し、必要と認めた場合には実施すること。

解説：サーバ装置上で取得可能な証跡について、証跡管理を行うための事項である。管理として、取得する情報項目の設定、証跡の保存及び点検、分析並びに報告等が挙げられる。

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、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。

A2101-28　（通信回線の対策）（政府機関統一基準の対応項番 5.4.1(2)）

第二十八条　部局技術担当者は、通信回線を利用する電子計算機の識別符号（ホスト ID）、電子計算機の利用者等と当該利用者等の識別符号（ユーザ ID）の対応、及び通信回線の利用部局を含む事項の管理を行うこと。

解説：通信回線の運用管理を行うことを求める事項である。

２　部局技術責任者は、定期的に通信回線の構成、情報ネットワーク機器の設定、アクセス制御の設定又は識別符号（ユーザ ID）を含む事項の変更を確認すること。また、当該変更によって生ずる通信回線のセキュリティへの影響を特定し、対応すること。

解説：通信回線の構成の不正な変更を定期的に確認し、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応することを求める事項である。

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ときに、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情報ネットワーク機器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情報ネットワーク機器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、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、及び情報ネットワーク機器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。

６　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、情報ネットワーク機器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構築した情報ネットワーク機器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。

A2101-29　（学外通信回線との接続）（政府機関統一基準の対応項番 5.4.3(2)）

第二十九条　全学実施責任者は、学内通信回線と学外通信回線の接続におい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ときに、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、通信回線の変更に際し及び定期的に、アクセス制御の設定の見直し行うこと。

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、三か月から六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、定期的に、学外通信回線から通信することが可能な学内通信回線及び情報ネットワーク機器のセキュリティホールを検査すること。

解説：定期的なセキュリティホール検査の実施を求める事項である。これによって、セキュリティレベルの低下、対策漏れ、アクセス制御の設定ミスがないかを確認する必要がある。

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。

第三節　運用終了時

A2101-30　（電子計算機の対策）（政府機関統一基準の対応項番 5.2.1(3)）

第三十条　部局技術責任者は、電子計算機の運用を終了する場合に、データ消去ソフトウェア若しくはデータ消去装置の利用、又は物理的な破壊若しくは磁気的な破壊等の方法を用いて、すべての情報を復元が困難な状態にすること。

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、すべ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消去されずに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すべ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。

A2101-31　（情報ネットワーク機器の対策）（政府機関統一基準の対応項番 5.4.1(3)）

第三十一条　部局技術責任者は、情報ネットワーク機器の利用を終了する場合には、情報ネットワーク機器の内蔵記録媒体のすべての情報を復元が困難な状態にすること。

解説：運用を終了した情報ネットワーク機器が再利用又は廃棄された後、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、情報の消去を求める事項である。

消去の方法としては、情報ネットワーク機器の初期化、内蔵記録媒体の物理的な破壊等の方法がある。

第四節　PDCA サイクル

A2101-32　（情報システムの計画・設計）（政府機関統一基準の対応項番 4.3.1(1)）

第三十二条　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、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開発・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、その中で重要とみなされる要求事項について対策を実施する対象を確定し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などのセキュリティに関する手順も含まれる。決定されたセキュリティ要件は、システム要件定義書や仕様書などの形式で明確化した上で、実装していくことが望ましい。

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。本規程の中から当該情報システムのセキュリティ対策として実施する遵守事項を選択した上でセキュリティ要件を満たしているかを検討し、満たしていないセキュリティ要件がある場合には、その対策も定めることが必要である。

４　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、教育やトラブル対応について手順を整備することを求める事項である。**

A2101-33　（情報システムの構築・運用・監視）（政府機関統一基準の対応項番 4.3.1(2)）

第三十三条　部局技術責任者は、情報システムの構築、運用及び監視に際しては、セキュリティ要件に基づき定めた情報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を実施し、情報システムを構築、運用及び監視することを求める事項である。

A2101-34　（情報システムの移行・廃棄）（政府機関統一基準の対応項番 4.3.1(3)）

第三十四条　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採ること。

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、情報の格付け等を考慮して、機器及び情報に関して廃棄、保存、消去等の適切な措置を採ることを求める事項である。

A2101-35　（情報システムの見直し）（政府機関統一基準の対応項番 4.3.1(4)）

第三十五条　部局技術責任者は、情報システムの情報セキュリティ対策について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：情報システムの情報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。

第三章　情報の格付けと取扱い

A2101-36　（情報の作成又は入手）（政府機関統一基準の対応項番 3.2.1(1)）

第三十六条　教職員等は、情報システムに係る情報を作成し又は入手する場合は、本学の研究教育事務の遂行の目的に十分留意すること。

解説：情報システムに係る情報の作成又は入手について、本学の研究教育事務の遂行の目的に留意す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、研究教育事務の遂行の目的以外の情報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程とすることは構わない。

A2101-37　（情報の作成又は入手時における格付けの決定と取扱制限の検討）（政府機関統一基準の対応項番 3.2.1(2)）

第三十七条　教職員等は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

解説：作成した情報について、以降、適切なセキュリティ管理が施されるように、機密性、完全性、可用性の格付け等を行うことを求める事項である。情報の格付けが適切に決定されていなかった、また、明示されていなかったことを一因として障害等が発生した場合には、障害等の直接の原因となった人物のほか、情報の格付け及び明示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、情報の格付けとその明示を確実に行うことは重要である。なお、教職員等は、情報の利用を円滑に行うため、格付けを必要以上に高くしないように配慮することも必要となる。あわせて、格付けに応じた情報の取扱いを確実にするための取扱制限の必要性の有無についても検討を行わなければならない。

２　教職員等は、学外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

解説：学外から入手した情報についても、格付けを行い、当該格付けに従った適正な管理を求める事項である。

A2101-38　（格付けと取扱制限の明示）（政府機関統一基準の対応項番 3.2.1(3)）

第三十八条　教職員等は、情報の格付けを、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し、必要に応じて取扱制限についても明示すること。

解説：作成者又は入手者によって格付けが行われた情報に対して、以降、他者が当該情報を利用する際に必要とされるセキュリティ対策レベルを示すため、情報の格付けの明示を行うことを求める事項である。また、取扱制限が必要な場合は、あわせてその明示も行わなければならない。

格付けと取扱制限の明示は、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、可搬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可搬記録媒体に、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、視認できる方法でそれぞれ行う必要がある。ただし、当該情報システムに保存されているすべての情報が同じ格付け、取扱制限であり、利用するすべての利用者等にてその認識が周知徹底されている場合は、この限りでない。しかし、格付けや取扱制限を認識していない利用者等に当該情報システムに保存されている情報を提供する必要が生じた場合は、当該情報に視認できるような明示を行った上で提供しなければならない。

また、既に書面として存在している情報に対して格付けや取扱制限を明示する場合には、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することも可能である。

なお、格付け及び取扱制限の明示とあわせて、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。

A2101-39　（格付けと取扱制限の継承）（政府機関統一基準の対応項番 3.2.1(4)）

第三十九条　教職員等は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。

解説：情報の作成者による情報の格付けと取扱制限を継承し、以降も同様のセキュリティ対策を維持することを求める事項である。

A2101-40　（格付けと取扱制限の変更）（政府機関統一基準の対応項番 3.2.1(5)）

第四十条　教職員等は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。

解説：情報を利用する利用者等が、当該情報の格付けを変更する場合に、当該情報の作成者又は入手者に相談し、了承を得ることを求める事項である。なお、自らが作成又は入手した場合も含まれる。当初の格付けが作成者又は入手者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、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を参照した者に対しても、当該情報の格付けを変更したことを周知させることが望ましい。なお、異動等の事由により、当該情報の作成者又は入手者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上司が相談を受け、その是非を検討することになる。

２　教職員等は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること。

解説：情報を利用する利用者等が、当該情報の取扱制限を変更する場合に、当該情報の作成者又は入手者に相談し、了承を得ることを求める事項である。なお、自らが作成又は入手した場合も含まれる。当初の取扱制限が作成者又は入手者によって不適正に設定されていれば、当該取扱制限を修正し、その旨を通知することによって、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を利用した者に対しても、当該情報の取扱制限を変更したことを周知させる必要がある。なお、異動等の事由により、当該情報の作成者又は入手者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上司が相談を受け、その是非を検討することになる。

A2101-41　（格付けに応じた情報の保存）（政府機関統一基準の対応項番 3.2.3(1)）

第四十一条　部局技術責任者は、電子計算機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：電子計算機に記録された情報に関して、機密性、完全性及び可用性の格付けに応じ、電子計算機の機能を活用して、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。

電子計算機におけるアクセス制御は、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。

2　部局技術責任者は、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、災害等への対策の必要性を検討し、必要があると認めたときは、同時被災等しないための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、遠隔地に保管することなどが考えられる。

第四章　主体認証

A2101-42　（主体認証機能の導入）（政府機関統一基準の対応項番 4.1.1(1)）

第四十二条　部局技術責任者は、すべ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性があると判断すること。

2　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。

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、主体認証情報（パスワード）を秘密にする必要がある場合には、当該主体認証情報（パスワード）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（パスワード）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（パスワード）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、利用者等に自らの主体認証情報（パスワード）を設定、変更、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。

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、利用者等に主体認証情報（パスワード）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

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、主体認証情報（パスワード）又は主体認証情報格納装置（IC カード）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（パスワード）若しくは主体認証情報格納装置（IC カード）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符号（ユーザ ID）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。

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（パスワード）を設定する機能

二　利用者等が設定した主体認証情報（パスワード）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

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、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、以下の要件について検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。また、用いる方式に応じて、以下を含む要件を定めること。

一　正当な主体以外の主体を誤って主体認証しないこと。（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できなくならないこと。（誤否の防止）

三　正当な主体が容易に他者に主体認証情報（パスワード）を付与及び貸与ができないこと。（代理の防止）

四　主体認証情報（パスワード）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　主体認証について業務遂行に十分な可用性があること。（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（パスワード）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（パスワード）を安全に再発行できること。（再発行の確保）

８　部局技術責任者は、生体情報による主体認証方式を用いる場合には、当該生体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。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。

９　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（パスワード）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。

第五章　アクセス制御

A2101-43　（アクセス制御機能の導入）（政府機関統一基準の対応項番 4.1.2(1)）

第四十三条　部局技術責任者は、すべ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。

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、アクセス制御を行う機能を設けること。

A2101-44　（利用者等による適正なアクセス制御）（政府機関統一基準の対応項番 4.1.2(2)）

第四十四条　部局技術責任者は、それぞれの情報システムに応じたアクセス制御の措置を講じるよう、利用者等に指示すること。

２　利用者等は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと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すること。

A2101-45　（無権限のアクセス対策）

第四十五条　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。

第六章　アカウント管理

A2101-46　（アカウント管理機能の導入）（政府機関統一基準の対応項番 4.1.3(1)）

第四十六条　部局技術責任者は、すべての情報システムについて、アカウント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、アカウント管理を行う必要があると判断すること。

解説：アカウント管理を行う前提として、部局技術責任者は、各情報システムについて、アクセスする主体のアカウント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、アカウントとは、主体に付与される許可のことをいい、アカウント管理とは、主体に対する許可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。

２　部局技術責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理を行う機能を設けること。

A2101-47　（アカウント管理手続の整備）（政府機関統一基準の対応項番 4.1.3(2)）

第四十七条　部局技術責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理について、以下の事項を含む手続を明確にすること。

一　主体からの申請に基づいてアカウント管理を行う場合には、その申請者が正当な主体であることを確認するための手続

二　主体認証情報（パスワード）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

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

解説：アカウントの管理においては、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利用規程において定める。

なお、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。

A2101-48　（共用アカウント）

第四十八条　部局技術責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、共用アカウント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。

２　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウントを発行する際に、それが共用アカウントか、共用ではないアカウントかの区別を利用者等に通知すること。ただし、共用アカウントは、部局技術責任者が、その利用を認めた情報システムでのみ付与することができる。

A2101-49　（アカウントの発行）

第四十九条　アカウント管理を行う者は、利用者等からのアカウント発行申請を受理したときは、申請者が第六十五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。

２　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、情報システムを利用する許可を得た主体に対してのみ、アカウントを発行すること。

３　アカウント管理を行う者は、アカウントを発行するにあたっては、期限付きの仮パスワードを発行する等の措置を講じることが望ましい。

４　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、管理者権限を持つアカウントを、業務又は業務上の責務に即した場合に限定して付与すること。

５　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、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アクセス制御に係る設定をすること。

A2101-50　（アカウント発行の報告）

第五十条　アカウント管理を行う者は、アカウントを発行したときは、速やかにその旨を部局総括責任者に報告すること。

２　全学総括責任者は、必要により部局総括担当者にアカウント発行の報告を求めることができる。

A2101-51　（アカウントの有効性検証）

第五十一条　アカウント管理を行う者は、発行済のアカウントについて、次号に掲げる項目を一か月毎に確認すること。

一　利用資格を失ったもの

二　部局総括責任者が指定する削除保留期限を過ぎたもの

三　パスワード手順に違反したパスワードが設定されているもの

四　六か月以上使用されていないもの

２　アカウント管理を行う者は、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、利用規程やパスワード基準に定める。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。

A2101-52　（アカウントの削除）

第五十二条　アカウント管理を行う者は、第五十条第一項第一号及び第二号に該当するアカウントを発見したとき、又は第六十五条第二項第三号よる削除命令を受けたときは、速やかにそのアカウントを削除し、その旨を部局総括責任者に報告すること。
２　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等のアカウントを削除し、その旨を部局総括責任者に報告すること。
３　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等に交付した主体認証情報格納装置（IC カード）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。

A2101-53　（アカウントの停止）
第五十三条　アカウント管理を行う者は、第五十条第一項第三号及び第四号に該当するアカウントを発見したとき、第六十五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（パスワード）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。

A2101-54　（アカウントの復帰）
第五十四条　アカウントの停止を受けた利用者等がアカウント停止からの復帰を希望するときは、その旨を部局総括責任者に申し出させること。
２　部局総括責任者は、前項の申し出を受けたときは、アカウント管理を行う者に当該アカウントの安全性の確認及びアカウントの復帰を指示すること。
３　アカウント管理を行う者は、前項の指示に従い当該アカウントの安全性を確認した後、速やかにアカウントを復帰させること。

A2101-55　（管理者権限を持つアカウントの利用）（政府機関統一基準の対応項番 4.1.1(2)）
第五十五条　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。

第七章　証跡管理

A2101-56　（証跡管理機能の導入）（政府機関統一基準の対応項番 4.1.4(1)）
第五十六条　部局技術責任者は、すべ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。
2　部局技術責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。
3　部局技術責任者は、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、事象を証跡として記録するに当たり、事象ごとに必要な情報項目を記録するように情報システムの設定をすること。
4　部局技術責任者は、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針を整備し、必要に応じ、これらの場合に対応するための機能を情報システムに設けること。
5　部局技術責任者は、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、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い、外部記録媒体等その他の装置・媒体に記録した証跡についてはこれを適正に管理すること。

A2101-57　（部局技術担当者による証跡の取得と保存）（政府機関統一基準の対応項番 4.1.4(2)）
第五十七条　部局技術担当者は、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、部局技術責任者が情報システムに設けた機能を利用して、証跡を記録すること。
2　部局技術担当者は、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、取得した証跡の保存期間を定め、当該保存期間が満了する日まで証跡を保存し、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。
3　部局技術担当者は、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、定められた対処を行うこと。

A2101-58　（証跡管理に関する利用者等への周知）（政府機関統一基準の対応項番 4.1.4(4)）
第五十八条　部局総括責任者又は部局技術責任者は、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、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。

A2101-59　（通信の監視）
第五十九条　利用者等によるネットワークを通じて行われる通信の傍受を禁止すること。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。

5　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。運用・管理規程において、どのような場合に誰に何をさせ何をさせないかを定めるとともに、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。

運用・管理規程の策定にあたっては、これらのことに十分配慮するとともに、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。運用・管理規程や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。

A2101-60　（利用記録）

第六十条　複数の者が利用する情報機器の管理者は、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採取することができる。当該目的との関連で必要性の認められない利用記録を採取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　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。

４　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。

５　第一項の規定により情報機器の利用を記録しようとする者は、第二項の目的、これによって採取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。

６　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。

A2101-61　（個人情報の取得と管理）

第六十一条　電子的に個人情報の提供を求める場合は、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。

A2101-62　（利用者等が保有する情報の保護）

第六十二条　利用者等が保有する情報は、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採取が、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。

第八章　暗号と電子署名

A2101-63　（暗号化機能及び電子署名の付与機能の導入）（政府機関統一基準の対応項番 4.1.6(1)）

第六十三条　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。

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。

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、電子署名の付与を行う機能を付加する必要性の有無を検討すること。

４　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は、電子署名の付与を行う機能を設けること。

５　部局技術責任者は、暗号化又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、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズム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から選択すること。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つをそれらのリストの中から選択すること。

解説：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、電子署名やサーバ証明書を用いた確認を行わなければならない。なお、サーバ証明書には SSL による暗号化通信も含む。

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。

A2101-64　（暗号化及び電子署名の付与に係る管理）（政府機関統一基準の対応項番 4.1.6(2)）

第六十四条　部局技術責任者は、暗号化又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、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、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応手順等を定めること。

２　部局技術責任者は、暗号化又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、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、鍵の保存媒体及び保存場所を定めること。

３　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。

第九章　違反と例外措置

A2101-65　（違反への対応）（政府機関統一基準の対応項番 2.1.3(1)）

第六十五条　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、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及び上記の措置を講じた場合は、遅滞無く全学総括責任者にその旨を報告すること。

A2101-66　（例外措置）（政府機関統一基準の対応項番 2.1.3(2)）

第六十六条　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「許可権限者」という。）を定め、審査手続を整備すること。

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

・例外措置の適用を許可した期間

・許可した措置内容（講ずるべき代替手段等）

・例外措置を終了した旨の報告方法

３　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、必要な対応を講ずること。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。

第十章　インシデント対応

A2101-67　（インシデントの発生に備えた事前準備）（政府機関統一基準の対応項番 2.2.2(1)）

第六十七条　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（故障を含む。以下第六十七条までにおいて同じ。）が発生した場合、被害の拡大を防ぐとともに、インシデントから復旧するための体制を整備すること。

２　全学実施責任者は、インシデントについて利用者等から部局総括責任者への報告手順を整備し、当該報告手段をすべての利用者等に周知すること。

３　全学実施責任者は、インシデントが発生した際の対応手順を整備すること。

４　全学実施責任者は、インシデントに備え、本学の研究教育事務の遂行のため特に重要と認めた情報システムについて、その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、連絡内容を含む緊急連絡網を整備すること。

５　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。

A2101-68　（インシデントの原因調査と再発防止策）（政府機関統一基準の対応項番 2.2.2(3)）

第六十八条　部局総括責任者は、インシデントが発生した場合には、インシデントの原因を調査し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。

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。

第十一章　本学支給以外の情報システム

A2101-69　（本学支給以外の情報システムにかかる安全管理措置の整備）（政府機関統一基準の対応項番 6.2.2(1)）

第六十九条　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。

A2101-70　（本学支給以外の情報システムの利用許可及び届出の取得及び管理）（政府機関統一基準の対応項番 6.2.2(2)）

第七十条　部局技術責任者及び部局技術担当者は、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。

２　部局技術責任者及び部局技術担当者は、要保護情報（機密性２情報を除く。）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、対応を講ずること。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。

３　部局技術責任者及び部局技術担当者は、機密性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、対応を講ずること。

第十二章　学外の情報セキュリティ水準の低下を招く行為の禁止

A2101-71　（学外の情報セキュリティ水準の低下を招く行為の防止）（政府機関統一基準の対応項番 6.3.1(1)）

第七十一条　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：「A3211 学外情報セキュリティ水準低下防止手順」を参照のこと。

第十三章　教育・研修

A2101-72　（情報セキュリティ対策の教育）（政府機関統一基準の対応項番 2.2.1(1)）

第七十二条　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。

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、教育啓発対象者に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。

３　全学実施責任者は、教育啓発対象者が毎年度最低一回、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、立案するとともに、その実施体制を整備すること。

４　全学実施責任者は、教育啓発対象者の入学時、着任時、異動時に三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、立案し、その体制を整備すること。

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。

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、当該教育啓発対象者の所属する部局の部局総括責任者に通知すること。

７　部局総括責任者は、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。

８　全学実施責任者は、毎年度一回、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。

９　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内容及び体制を整備すること。

１０　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。

１１　その他、教育・研修に関する事項については、講習計画に定めること。

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。

A2101-73　（教育の主体と客体）

第七十三条　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。

第十四章　評価

A2101-74　（自己点検に関する年度計画の策定）（政府機関統一基準の対応項番 2.3.1(1)）
第七十四条　全学総括責任者は、年度自己点検計画を策定すること。

A2101-75　（自己点検の実施に関する準備）（政府機関統一基準の対応項番 2.3.1(2)）
第七十五条　部局総括責任者は、職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。

A2101-76　（自己点検の実施）（政府機関統一基準の対応項番 2.3.1(3)）
第七十六条　部局総括責任者は、全学総括責任者が定める年度自己点検計画に基づき、職務従事者に対して、自己点検の実施を指示すること。
２　職務従事者は、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。

A2101-77　（自己点検結果の評価）（政府機関統一基準の対応項番 2.3.1(4)）
第七十七条　部局総括責任者は、職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。
２　全学総括責任者は、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。

A2101-78　（自己点検に基づく改善）（政府機関統一基準の対応項番 2.3.1(5)）
第七十八条　職務従事者は、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。
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。

A2101-79　（監査）
第七十九条　部局総括責任者その他の関係者は、全学総括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。

A2104 情報格付け規程

１．目的

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。

解説：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。

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。

【規程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	本学情報システム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	本学情報システム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、直ちに一般に公表することを前提としていない情報
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：ここで言う機密性の格付けに対して、行政機関の保有する情報の公開に関する法律（情報公開法）で言う開示・不開示の区別は一致しにくいものである。

現状の政府機関統一基準では、機密性２が公開を前提としないものとされているので、機密性１は公開を前提とすると解釈されてしまい、結果として、取扱注意情報は、機密性２に格付けするしかなくなる。しかし、審議中の文書などいわゆる取扱注意文書が、機密性２の遵守事項の対象となると、外部への提供に際して届出が必要となったりするなど、多くの遵守事項の対象となるため運用が煩雑になる。

これを回避するために、このサンプル規程集では以下の解釈を推奨する。

機密性２及び３＝基準の遵守事項による機密保護の対象とする情報。

機密性２と３の違い＝３はすべて非開示情報、２は開示について個々に検討する情報。

機密性１＝遵守事項による機密保護の対象としない情報。公開を前提とはしなくても、情報公開法による開示請求を受けた場合には原則として開示する情報と考えられるが、別に「部外秘」などの取扱制限を指定することによって何らかの保護をすべき情報として扱うことも可能である。

これまで「取扱注意」とされてきた情報について、機密性１（以上）の格付けは必須であると考えられるが，上記の解釈により、機密性２または１を選択することになる。

(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	本学情報システムで取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

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	本学情報システムで取り扱う情報（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。

【規程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

【規程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。
- 「〇〇限り」 当該情報について、参照先を〇〇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	〇〇まで保存
保存場所について	〇〇において保存
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

【規程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	〇〇以内復旧
保存場所について	〇〇において保存

【規程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決定

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。

【規程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。

【規程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

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すること。

【規程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」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。

【規程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

【規程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。

【規程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。

【規程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。

【規程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。

【規程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

【規程利用者への補足説明】

本学における情報システム運用基準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。

【規程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、バックアップ必須
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

A2201 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。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。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）のアカウントと共通である。A大学とは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、教務・事務用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、「事務システム利用規程」や「事務執行手順書」に従う必要がある。

なお、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、学籍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。

A2201-01　（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。

A2201-02　（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　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　運用基準　本学が定める A 大学情報システム運用基準をいう。

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　その他の用語の定義は、基本方針及び運用基準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。

A2201-03　（適用範囲）

第三条　この規程は本学情報システム及びそれにかかわる情報を利用するすべての者に適用する。
2　本規程の情報システムには、A大学ネットワークおよびA大学内のすべてのコンピュータシステムが含まれる。ただし、教務・事務用のシステムについては「事務システム利用規程」および「事務執行手順書」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。原則として私物を使わせないという方針もあり得る。なお、「事務システム利用規程」および「事務執行手順書」は本サンプル規程集における本年度の策定対象外である。

A2201-04　（全学アカウントの申請）

第四条　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得なければならない。

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。

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、A1001 情報システム運用基準の A1001-06（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。

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（認証ネットワーク）な場合は、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のためにインターネット・カフェや学外のホットスポットからの大学情報システムへのアクセスを禁止している。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。

A2201-05　（ID とパスワードによる認証の場合）

第五条　利用者は、アカウントの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、自分のユーザアカウントを他の者に使用させたり、他の者のユーザアカウン

トを使用したりしてはならない。
二　利用者は、パスワードとして、容易に推測できるような文字列を設定してはならない
三　利用者は、セキュリティを確保するためのパスワードの定期的な変更を怠ってはならない。
四　利用者は、他の者の認証情報を聞き出したり使用したりしてはならない。
五　利用者は、自己のパスワードを厳重に管理しなければならない。
六　利用者は、他の者にパスワードを教えたり、不注意でパスワードが他の者に知られたりしてしまうことがないよう最大限の注意を払わなければならない。
七　利用者は、使用中のコンピュータをロックし、あるいはログアウト（ログオフ）せずに長時間自らの席を離れてはならない。
八　学外のインターネットカフェなどに設置されているような不特定多数の人が操作（利用）可能な端末を用いての学内情報システムへのアクセスを行ってはならない。
九　利用者は、アカウントを他者に使用され又はその危険が発生した場合には、直ちに全学実施責任者にその旨を報告しなければならない。
十　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。

A2201-05-2　（IC カードを用いた認証の場合）
第五条の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。

A2201-06　（遵守事項）
第六条　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。

A2201-07　（利用者による情報セキュリティ対策教育の受講義務）
第七条　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。

A2201-08　（自己点検の実施）

第八条　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。

A2201-09　（情報の格付け）

第九条　教職員等は、情報格付け規程に従って、情報の格付け及び取扱いを行わなければならない。

解説：電子化された情報について、政府統一基準は、格付け（いわゆるラベリング）を実施して、保護レベルを決め管理することとしている。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、情報格付け規程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く、学生が格付けされた情報に触れる機会はない。

A2201-10　（禁止事項）

第十条　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　差別、名誉毀損、侮辱、ハラスメントにあたる情報の発信

三　個人情報やプライバシーを侵害する情報の発信

四　守秘義務に違反する情報の発信

五　著作権等の財産権を侵害する情報の発信

六　通信の秘密を侵害する行為

七　営業ないし商業を目的とした本学情報システムの利用

八　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

九　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、またはこれに類する行為

十　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
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　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
十三　上記の行為を助長する行為
十四　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
十五　利用者は、Ｐ２Ｐソフトウェアについては、教育・研究目的以外にこれを利用してはならない。Ｐ２Ｐソフトウェアを教育・研究目的に利用する場合は全学実施責任者の許可を得なければならない。

解説：利用に際しての禁止条項を上記で条文化している。A大学では、構成員による知的財産権侵害を防ぐために P2P ソフトウェアの利用を原則として禁止している。

A2201-11　（違反行為への対処）

第十一条　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。

A2201-12　（PC 取扱手順）

第十二条　利用者は、様々な情報の作成、利用、保存等のための PC の利用にあたっては、別途定める PC 取扱手順に従い、これらの情報及び端末の適切な保護に注意しなければならない。

A2201-13　（電子メール手順）

第十三条　利用者は、電子メールの利用にあたっては、別途定める電子メール手順に従い、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。

A2201-14　（ウェブブラウザ手順）

第十四条　利用者は、ウェブサイトの閲覧にあたっては、別途定めるウェブブラウザ手順に従って、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、不正プログラムの感染、情報の漏えい、誤った相手への情報の送信等の脅威だけでなく、業務時間中における私的目的でのウェブの閲覧、掲示板への無断書き込みその他業務効率の低下や本学の社会的信用を失わせることのないよう注意しなければならない。

2　部局情報システム運営委員会に許可を得た場合にウェブページを作成し、公開することができる。公開にあたって、Web 公開手順に従わなければならない。

3　サーバを運用する場合は、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。

A2201-15　（モバイル PC 利用手順）

第十五条　利用者は、以下の手順にしたがってモバイル PC を利用しなければならない。

一　事務処理に用いる PC を学外に持ち出してはならない。

二　データの持ち出しには、保護レベルに応じた管理が必要である。

三　学外に持ち出す可能性のある PC は可能な限り強固な認証システムを備えていなければならない。

四　PC を盗難の可能性のある箇所に放置してはならない。

五　PC の電源を入れたまま放置してはならない。

六　学外から本学内のシステムに接続する場合には、あらかじめ全学実施責任者の許可を得た手順以外の方法を利用してはならない。

七　学外に持ち出した PC を本学情報ネットワークに接続する場合は、アンチウィルスソフトウエア等でスキャンを実行し、問題のあるソフトウェアが検出されないことをあらかじめ確認しなければならない。（モバイル PC の接続申請および許可は済んでいるものとする。）

解説：大学において、教員や学生に対してモバイル PC の利用に厳しい制限を課すことは困難である。ただし、ここでいうモバイル PC には、事務処理用 PC を含めない。

A2201-16　（安全管理義務）

第十六条　利用者は、自己の管理するコンピュータについて、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、次の各号に定めるように、悪意あるプログラムを導入しないように注意しなければならない。

一　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る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。

二　アンチウイルスソフトウェア等にかかわ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。

三　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しなければならない。

四　アンチウイルスソフトウェア等により定期的にすべての電子ファイルに対して、不正プ

ログラムの有無を確認すること。

五　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。

六　ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。

2　利用者は、本学情報ネットワークおよび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、「情報システムインシデント対応手順」に従って行動するものとする。

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 PC 手順に記載することとしてもよいであろう。

A2201-17　（接続の許可）

第十七条　利用者は、本学情報システムに新規に情報システム（コンピュータ）を接続しようとする場合は、事前に部局技術責任者と協議し、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、情報コンセントからの本学情報システムへの一時的な接続はこの限りではない。）

解説：機器をネットワークに接続して利用開始にあたっての手続き等を規定する。大学の実情に合わせて、ネットワーク利用規程と情報システム利用規程を分離することも考えられる。ただし書きの部分について、一時接続についても認証を行うといった対策が推奨される。認証を実施しない場合でも、その接続についての直接的責任が明確になるような手続きを規定すべきである。

A2301 年度講習計画

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）

解説：関連規程: A1001-5 第五条、A1001-08 第八条、A2201-07 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、実施時期に応じた区分として、以下の３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。

(a) 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
(b) 定期講習：すでに(a)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
(c) 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・倫理なども含めて実施するもの

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 (A3301 教育テキスト参照)

A2401 監査規程

A2401-01 （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。

A2401-02 （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。

A2401-03 （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。

A2401-04 （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

A2401-05 （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。

A2401-06 （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。

A2401-07 （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。

A2501 事務情報セキュリティ対策基準

目　次

第１部　総則

1.1 位置付け

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「国立Ａ大学事務情報セキュリティ対策基準」（以下、本基準という。）は、平成 17 年 12 月 13 日に制定された「政府機関の情報セキュリティ対策のための統一基準」（以下、「政府統一基準」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、政府統一基準を踏まえて情報セキュリティ水準の見直しを行う際に、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、政府統一基準の改訂に対応できるよう、構成を同様にしていることを申し添える。

1.2 目的

本基準は、本学事務局管理の情報及び情報システムに関する情報セキュリティ対策に必要な遵守事項を明確にすることにより、機密性、可用性、完全性の観点から安全なシステム運用を確保することを目的とする。

1.3 適用対象（情報の定義と対象者）

本基準が適用される対象範囲を以下のように定める。

（a）本基準は、「情報」を守ることを目的に作成されている。本基準において「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、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる。

（b）本基準は、教職員等のうち、事務局管理の情報及び情報システムを取り扱う者に適用される。なお、本基準中、特に断りがないものを除き、「教職員等」とは、事務局管理の情報及び情報システムを取り扱う教職員等をいう。

1.4 全体構成

本基準は、部、節及び項の３つの階層によって構成される。

本基準は、情報セキュリティ対策を「組織と体制の構築」、「情報についての対策」、「セキュリティ要件の明確化に基づく対策」、「情報システムについての対策」、「個別事項についての対策」に部として分類し、さらに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。

(a)「組織と体制の構築」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、違反や例外措置などの組織として構築すべき課題を取り上げ、組織としての運用に関係する各教職員等の権限と責務を明確にする。

(b)「情報についての対策」では、情報の作成、利用、保存、移送、提供及び消去等といった情報のライフサイクルに着目し、各段階において遵守すべき事項を定め、各教職員等が業務の中で常に実施する情報保護の対策を示す。

(c)「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など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遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。

(d)「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、それぞれ遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。

(e)「個別事項についての対策」では、調達・開発や学外での情報処理等の、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、それぞれ遵守すべき事項を定める。

1.5 対策レベルの設定

情報セキュリティ対策においては、対象となる情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一様ではない。また、該当する情報システム及び業務の特性に応じて、各対策項目で適切な強度の対策を実施すべきである。したがって、本基準においては、各対策項目で対策の強度に段階を設け、採るべき遵守事項を定めている。この段階を「対策レベル」と呼び、以下のように定義する。

(a)「基本遵守事項」は、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

(b)「強化遵守事項」は、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、各国立大学法人において、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

以上より、各国立大学法人は、基本遵守事項以上の対策を実施することとなるが、当該情報システム及び業務の特性を踏まえ、リスクを十分に勘案した上で、対策項目ごとに適切な対策レベルを選択しなければならない。

1.6 用語の定義

【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。
- 「安全区域」とは、電子計算機及び通信回線装置を設置した事務室又はサーバルーム等の内部であって、部外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。
- 「委託先」とは、情報システムに関する企画、開発、保守及び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。
- 「受渡業者」とは、安全区域内で職務に従事する教職員等との物品の受渡しを目的とした者のことで、安全区域へ立ち入る必要のない者をいう。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】

- 「外部委託」とは、情報システムに関する企画、開発、保守及び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。
- 「外部記録媒体」とは、情報機器から取り外しすることが可能な記録装置（磁気テープ、磁気ディスク、光ディスク、カセットテープ、MO、フロッピーディスク及びUSBメモリ等）をいう。
- 「学外」とは、本学が管理する組織又は大学施設の外をいう。
- 「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、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」とは、本学の管理部外で職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。
- 「学内」とは、本学が管理する組織又は施設の内をいう。
- 「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、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」とは、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することをいう。
- 「可用性１情報」とは、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」とは、職務で取り扱う情報（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、研究・教育活動等に支障を及ぼす又は職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。
- 「完全性１情報」とは、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」とは、職務で取り扱う情報（書面を除く。）のうち、その改ざん、誤びゅう又は破損により、大学の運営に支障を及ぼす又は職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をいう。
- 「機密性１情報」とは、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２情報」とは、職務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、直ちに一般に公表することを前提としていない情報をいう。
- 「機密性３情報」とは、職務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。
- 「教職員等」とは、本学教職員及び本学の指示に服している者のうち、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。
- 「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。
- 「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。）の付与及びアクセス制御における許可情報の付与を管理することをいう。
- 「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、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等が該当する。

【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、管理者権限を持つ識別コードを付与された者が、管理者としての業務遂行時に限定してその識別コードを利用させる機能をいう。
- 「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。

- 「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」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、磁気テープカードやＩＣカード等がある。
- 「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、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外部記録媒体、PC 及び書面を運搬することをいう。
- 「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】

- 「対策用ファイル」とは、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をいう。
- 「端末」とは、端末を利用する教職員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。
- 「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」とは、回線の接続のために設置され、電子計算機により通信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、読後廃棄等をいう。

【は】
- 「複数要素（複合）主体認証（multiple factors authentication / composite authentication）方式」とは、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」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。
- 「付与」（主体認証に係る情報、アクセス制御における許可情報等に関して）とは、発行、更新及び変更することをいう。
- 「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、本学支給以外の情報システムを用いて職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】
- 「明示」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に含むものとする。
- 「モバイル PC」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ノート型 PC は、モバイル PC に含まれない。

【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、教職員等がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、職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２部　組織と体制の構築

2.1　導入

2.1.1 組織･体制の確立

趣旨（必要性）

情報セキュリティ対策は、それに係るすべての教職員等が、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・体制を確立する必要がある。

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。

遵守事項

(1)　全学総括責任者の設置

【基本遵守事項】

(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定めた事項である。
情報セキュリティ対策の実現には、教職員等一人一人の意識の向上や責務の遂行はもちろんのこと、組織的な取組み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、本基準で規定する各役割については図４（本書ｖページ）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、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。

(c) 全学総括責任者は、必要に応じ、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。
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。

(2) 全学情報システム運用委員会の設置

【基本遵守事項】

(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。A1001 情報システム運用基準では、全学総括責任者を委員長とし、全学実施責任者、部局総括責任者、部局技術責任者、およびその他全学総括責任者が必要と認める者で構成することとしている。あるいは部局長会議と兼ねることが考えられるが、委員長と議長の整合性に問題が生じ、あるいは構成メンバーが異なる可能性がある。
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学内で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。
（参照：A1001 情報システム運用基準　A1001-05 （全学情報システム運用委員会）第五条～第七条）

(b) 全学情報システム運用委員会は、情報セキュリティに関する対策基準を策定し、全学総括責任者に承認を得ること。

解説：大学全体として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

【基本遵守事項】

(a) 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定めた事項である。
情報セキュリティ監査責任者は、たとえば監事とすることが考えられるが、その場合には、規程の中で規定しておくか、あるいは情報担当理事ではなく学長が任命することが必要になると考えられる。
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、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、学内及び学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。

(b) 情報セキュリティ監査責任者は、監査に関する事務を統括すること。

(4) 全学実施責任者の設置

【基本遵守事項】

(a) 全学総括責任者は、全学実施責任者を置くこと。

(b) 全学実施責任者は、部局総括責任者が実施する事務を統括すること。

(c) 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策定し、全学総括責任者の承認を得ること。

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、人事担当課又は各職場から、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、職員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、鍵や ID カード、通行証の発行から失効及び返却までの管理、古いアカウントの閉鎖等、情報システムへのアクセス権の変更の管理も含まれる。

(5) 部局総括責任者の設置

【基本遵守事項】

(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。管理を行う単位を全学情報システム運用委員会の各情報システム運用委員会とし、部局総括責任者は、部局情報システム運用委員会の各総括責任者とすること。

解説：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定めることによる組織内での役割の明確化に関して定めた事項である。
「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、すべての教職員等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) 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。

(c) 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。

(d) 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。

(e) 全学実施責任者は、すべての部局総括責任者に対する連絡網を整備すること。

(6) 部局技術責任者の設置

【基本遵守事項】

(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置くこと。部局技術責任者は、各情報システム運用委員会の技術責任者とすること。

解説：各情報システムにおいて、企画、開発、運用、保守等のライフサイクル全般を通じて必要となる情報セキュリティ対策の責任者を定めた事項である。

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、その他本学のすべての情報システムを、情報システム単位に情報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。

「所管する単位における情報システムごとに」と記載しているが、所管する単位ごとに１人あるいは情報システムごとに１人に限るものではなく、所管する単位内に複数の部局技術責任者を置いてもよいし、複数の情報システム群をまとめて、部局技術責任者を置いてもよい。

(b) 部局技術責任者は、所管する情報システムに対する情報セキュリティ対策の管理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、すべての部局技術責任者に対する連絡網を整備すること。

(7) 部局技術担当者の設置

【基本遵守事項】

(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情報セキュリティ対策の実施を管理する者を定めた事項である。

企画、開発、運用、保守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、すべての部局技術担当者に対する連絡網を整備すること。

(8) 職場情報セキュリティ責任者の設置
【基本遵守事項】
(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、所管する事務や職員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ものであり、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 名任命し、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、すべ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。

2.1.2 役割の分離

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。

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職務の分離に関する対策基準を定める。

遵守事項

(1) 兼務を禁止する役割の規定
【基本遵守事項】
(a) 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。
(ア)承認又は許可事案の申請者とその承認者又は許可者
(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。その場合には、同じ承認又は許可をする役割を担う他者に申請し、承認又は許可を得る必要がある。

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、適切に対応する必要がある。

また、情報セキュリティ関係規程の適用が職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、あらかじめ定められた例外措置のための手続により、情報セキュリティを維持しつつ柔軟に対応できるものでなければ、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を定める。

遵守事項

(1) 違反への対応

【基本遵守事項】

(a) 教職員等は、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。

(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採らせること。

解説：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を回復するとともに、情報セキュリティ対策の適切な実施を再度徹底するために、違反者及び当該規定の実施に責任を持つ者を含む必要な者に情報セキュリティ維持のための措置を採ることを求める事項である。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ていれば、これを早急に解決し、問題の拡大を防止する必要がある。情報セキュリティ関係規

程を知らずに違反を犯したのであれば、違反者及び当該規定の実施に責任を持つ者を含む必要な者にこれを知らせ、情報セキュリティを維持するための措置を採らせる必要がある。

(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

【基本遵守事項】

(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「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) 教職員等は、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、職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許可を得ること。教職員等は、申請の際に以下の事項を含む項目を明確にすること。

(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適用箇所（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ときの報告方法

(カ) 例外措置の適用を申請する理由

解説：例外措置を教職員等の独断で行わせないための事項である。

教職員等は、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、職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。

教職員等は、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。

(c) **許可権限者は、教職員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整備し、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適用箇所（規程名と条項等）**
- **例外措置の適用を許可した期間**
- **許可した措置内容（講ずるべき代替手段等）**
- **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職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、該当する申請をすべて把握し、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、許可権限者のいずれかを記載する。

(d) **教職員等は、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、それを終了したときに、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、許可を受けた教職員等が、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、必要な対応を講ずること。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。必要な対応としては、許可を受けた者が報告を怠っているのであればそれを催促すること、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を実施する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などの対応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。

2.2 運用

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正に策定されたとしても、教職員等にその内容が周知されず、教職員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、すべての教職員等が、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、本項では、情報セキュリティ対策の教育に関する対策基準を定める。

遵守事項

(1) 教職員等に対する情報セキュリティ対策教育の実施

【基本遵守事項】

(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、教職員等に対し、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、教職員等に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：全学実施責任者が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、教職員等が対策内容を十分に理解できるものとする必要がある。

(c) **全学実施責任者は、教職員等が毎年度最低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、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など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。

(d) **全学実施責任者は、教職員等の着任時、異動時に新しい職場等で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、立案し、その体制を整備すること。**

解説：着任、異動した教職員等に対して、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、教職員等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など、

教育をしないことについて合理的な理由がある場合は、対象から除外され得る。

(e) 全学実施責任者は、教職員等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し、教職員等への教育を促すことを求める事項である。

(f) 全学実施責任者は、教職員等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：定めら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職員等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、教職員等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。教職員等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、定められた教育を受講しない教職員等は、その遵守違反について責任を問われることになる。

(h) 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、教職員等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。

【強化遵守事項】

(i) 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必要に応じ、全学実施責任者は、情報セキュリティ関係規程について、教職員等に対する情報セキュリティ対策の訓練の内容及び体制を整備すること。

解説：模擬的な状況において実際に情報セキュリティ対策のための事務を行うことにより、その知識・技能等の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。

訓練の内容については、本学の実情に合わせて幅広い角度から検討し、教職員等が対策内容を十分に理解できるものとする必要がある。

(2) 教職員等による情報セキュリティ対策教育の受講義務

【基本遵守事項】

(a) 教職員等は、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：教職員等が、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) **教職員等は、着任時、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、異動した教職員等が、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。

職場情報セキュリティ責任者への確認がなされない場合は、職場情報セキュリティ責任者において、受講日程を連絡することが望ましい。

(c) **教職員等は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではないと思われる場合には、その理由について、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、定められた教育を受講しない場合には、教職員等は、その遵守違反について責任を問われることになる。

【強化遵守事項】

(d) **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必要に応じ、教職員等は、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：教職員等が、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。

2.2.2 障害等の対応

趣旨（必要性）

情報セキュリティに関する障害等が発生した場合には、早急にその状況を検出し、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、障害等の影響や範囲を定められた責任者へ報告し、障害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ことが重要である。

これらのことを勘案し、本項では、障害等の発生時に関する対策基準を定める。

遵守事項

(1) 障害等の発生に備えた事前準備

【基本遵守事項】

(a) **全学総括責任者は、情報セキュリティに関する障害等（インシデント及び故障を含む。以下「障害等」という。）が発生した場合、被害の拡大を防ぐとともに、障害等から復旧するための体制を整備すること。**

解説：全学総括責任者に障害等に対する体制の整備を求める事項である。本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が求められる。

なお、情報セキュリティに関する障害等とは、機密性、完全性、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、ISO/IEC 17799 におけるインシデントと同意である。

(b) 全学実施責任者は、障害等について教職員等から部局総括責任者への報告手順を整備し、当該報告手段をすべての教職員等に周知すること。

解説：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などして、緊急時に教職員等がすぐに参照できるようにすることが必要である。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。

(c) 全学実施責任者は、障害等が発生した際の対応手順を整備すること。

解説：対応手順として障害等の発生時における緊急を要する対応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。対応する者に、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。そのようなことがないよう検討すること。
対応手順において、障害等の発生日及び内容、障害等への対応の内容及び対応者等を教職員等が記録すべきことを定めることも考えられる。

(d) 全学実施責任者は、障害等に備え、職務の遂行のため特に重要と認めた情報システムについて、その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、連絡内容を含む緊急連絡網を整備すること。

解説：全学実施責任者は、すべ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（統一基準 2.1.1）が、これは「緊急」連絡網を加えて整備することを定める事項である。

【強化遵守事項】

(e) 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必要に応じ、全学実施責任者は、障害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) 障害等の発生時における報告と応急措置

【基本遵守事項】

(a) 教職員等は、障害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、部局総括責任者にその旨を報告すること。

解説：障害等が発生した場合に、教職員等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等への対応を開始することができるように求める事項である。

(b) 教職員等は、障害等が発生した際の対応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：教職員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、障害等への対応手順に従うことを求める事項である。なお、対応手順は、より具体的に整備するとともに、対応の体制を速やかに整え、組織的な対応を実施することが重要である。

(c) 教職員等は、障害等が発生した場合であって、当該障害等について対応手順がないとき及びその有無を確認できないときは、その対応についての指示を受けるまで、障害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：対応手順が想定していない障害等が発生した場合、教職員等は対応の指示を受けるまでの間も障害等の拡大防止に努めることを求める事項である。

(3) 障害等の原因調査と再発防止策

【基本遵守事項】

(a) 部局総括責任者は、障害等が発生した場合には、障害等の原因を調査し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て、障害等の原因を究明し、それに基づき障害等の再発防止策を策定すること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。

2.3 評価

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、それに係るすべての教職員等が、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、すべ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、本項では、自己点検に関する対策基準を定める。

遵守事項

(1) 自己点検に関する年度計画の策定

【基本遵守事項】

(a) 全学総括責任者は、年度自己点検計画を策定すること。

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、当初はすべ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。

(2) 自己点検の実施に関する準備

【基本遵守事項】

(a) 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。

(3) 自己点検の実施

【基本遵守事項】

(a) 部局総括責任者は、全学総括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。

(b) 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

【基本遵守事項】

(a) 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、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/対策実施数などの準拠率の把握が挙げられる。

(b) 全学総括責任者は、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、全学総括責任者が評価することを求める事項である。

(5) 自己点検に基づく改善

【基本遵守事項】

(a) 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すべ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。

(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。

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、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、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、教職員等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監査を実施する必要である。

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を定める。

遵守事項

(1) 監査計画の策定

【基本遵守事項】

(a) 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こと。

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こと。

(2) 情報セキュリティ監査の実施に関する指示

【基本遵守事項】

(a) 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こと。

解説：年度情報セキュリティ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こと。

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、学内及び、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。

(3) 個別の監査業務における監査実施計画の策定

【基本遵守事項】

(a) 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

・監査の実施担当者及び割当て

・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

(4) 情報セキュリティ監査を実施する者の要件

【基本遵守事項】

(a) 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こと。

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。

(b) 情報セキュリティ監査責任者は、必要に応じて、教職員等以外の者に監査の一

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、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。

(5) 情報セキュリティ監査の実施

【基本遵守事項】

(a) 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こと。

解説：情報セキュリティ監査を実施する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を実施する者は、本基準の導入に当たって実施手順が作成されている場合には、それらが本基準に準拠しているか否かを確認すること。

解説：本学の実施手順が本基準に準拠して設計されているか否かの確認を求める事項である。

(c) 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情報セキュリティ関係規程に準拠しているか否かを確認すること。

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定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。

(d) 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こと。

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。

(e) 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) 情報セキュリティ監査結果に対する対応

【基本遵守事項】

(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、指摘事案に対する対応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応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、報告すること。

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。

(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、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、既存の情報セキュリティ関係規程の更新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。

2.4 見直し

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

【基本遵守事項】

(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、自己点検及び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情報セキュリティ関係規程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情報セキュリティ関係規程を見直した者は、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情報セキュリティ関係規程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。

(b) 教職員等は、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こと。

解説：情報セキュリティ関係規程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、その見直しを教職員等に求める事項である。

第３部　情報についての対策

3.1　情報の格付け

3.1.1 情報の格付け

趣旨（必要性）

職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、情報の格付けが必要となる。

これらのことを勘案し、本項では、情報の格付けに関する対策基準を定める。

遵守事項

(1)　情報の格付け

【基本遵守事項】

(a) 全学情報システム運用委員会は、職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基準並びに格付け及び取扱制限を明示する手順を整備すること。

解説：職務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。

3.2 情報の取扱い

3.2.1 情報の作成と入手

趣旨（必要性）

職務においては、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、すべ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

【基本遵守事項】

(a) 教職員等は、職務の遂行以外の目的で、情報システムに係る情報を作成し又は入手しないこと。

解説：職務の遂行以外の目的で、情報システムに係る情報については、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けの決定と取扱制限の検討

【基本遵守事項】

(a) 教職員等は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

解説：作成した情報について、以降、適切なセキュリティ管理が施されるように、機密性、完全性、可用性の格付け等を行うことを求める事項である。情報の格付けが適切に決定されていなかった、また、明示されていなかったことを一因として障害等が発生した場合には、障害等の直接の原因となった人物のほか、情報の格付け及び明示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、情報の格付けとその明示を確実に行うことは重要である。なお、教職員等は、情報の利用を円滑に行うため、格付けを必要以上に高くしないように配慮することも必要となる。あわせて、格付けに応じた情報の取扱いを確実にするための取扱制限の必要性の有無についても検討を行わなければならない。

(b) 教職員等は、教職員等以外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

解説：外部から入手した情報についても、格付けを行い、当該格付けに従った適正な管理を求める事項である。

(c) 教職員等は、未定稿の情報を決定稿にする際には、当該情報の格付けと取扱制

限について、その妥当性の有無を再確認し、妥当でないと思われる場合には、これを行った者に相談することに努めること。相談された者は、格付けと取扱制限の見直しを行う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と取扱制限を決定すること。

解説：未定稿を決定稿にする際に、未定稿の情報が作成又は入手されたときにおける格付けと取扱制限が適切に行われていたかを再確認することにより、情報の格付けと取扱制限の決定の妥当性を、より確実にするための事項である。

当初の格付けと取扱制限が作成者又は入手者によって不適正に設定されていれば、当該格付けと取扱制限を修正し、その旨を通知することによって、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を利用した者に対しても、当該情報の格付けと取扱制限を変更したことを周知させる必要がある。

なお、異動等の事由により、当該情報の作成者又は入手者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が相談を受け、その是非を検討することになる。

ただし、当該情報の格付けと取扱制限を適切に行うことは、本来は未定稿の時点から求められているため、未定稿に不適切な格付けと取扱制限がされていた場合の責任は、それを行った者である。したがって、未定稿を決定稿にする者の遵守事項は、再確認等を「すること」ではなく、これらを「することに努めること」とした。

(3) 格付けと取扱制限の明示

【基本遵守事項】

(a) 教職員等は、情報の格付けを、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し、必要に応じて取扱制限についても明示すること。

解説：作成者又は入手者によって格付けが行われた情報に対して、以降、他者が当該情報を利用する際に必要とされるセキュリティ対策レベルを示すため、情報の格付けの明示を行うことを求める事項である。また、取扱制限が必要な場合は、あわせてその明示も行わなければならない。

格付けと取扱制限の明示は、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、可搬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可搬記録媒体に、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、視認できる方法でそれぞれ行う必要がある。ただし、当該情報システムに保存されているすべての情報が同じ格付け、取扱制限であり、利用するすべての教職員等にてその認識が周知徹底されている場合は、この限りでない。しかし、格付けや取扱制限を認識していない教職員等に当該情報システムに保存されている情報を提供する必要が生じた場合は、当該情報に視認できるような明示を行った上で提供しなければならない。

また、既に書面として存在している情報に対して格付けや取扱制限を明示する場合には、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することも可能である。

なお、格付け及び取扱制限の明示とあわせて、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。

(4) 格付けと取扱制限の継承

【基本遵守事項】

(a) 教職員等は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。

解説：情報の作成者による情報の格付けと取扱制限を継承し、以降も同様のセキュリティ対策を維持することを求める事項である。

(5) 格付けと取扱制限の変更

【基本遵守事項】

(a) 教職員等は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。

解説：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、当該情報の作成者又は入手者に相談し、了承を得ることを求める事項である。なお、自らが作成又は入手した場合も含まれる。当初の格付けが作成者又は入手者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、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を参照した者に対しても、当該情報の格付けを変更したことを周知させることが望ましい。

なお、異動等の事由により、当該情報の作成者又は入手者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が相談を受け、その是非を検討することになる。

(b) 教職員等は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること。

解説：情報を利用する教職員等が、当該情報の取扱制限を変更する場合に、当該情報の作成者又は入手者に相談し、了承を得ることを求める事項である。なお、自らが作成又は入手した場合も含まれる。当初の取扱制限が作成者又は入手者によって不適正に設定されていれば、当該取扱制限を修正し、その旨を通知することによって、作成者又は入手者への教育的効果も期待できる。また、それまでその情報を利用した者に対しても、

当該情報の取扱制限を変更したことを周知させる必要がある。
なお、異動等の事由により、当該情報の作成者又は入手者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が相談を受け、その是非を検討することになる。

3.2.2 情報の利用

趣旨（必要性）

職務においては、その事務の遂行のために多くの情報を取り扱うが、情報システムの利用者の認識不足等による情報の不適切な利用や、情報システムの管理者によるセキュリティホールの対策及び不正プログラム対策の不備等の問題により、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ある。情報を不適切に利用すると、情報の漏えい、改ざん、不当な消去、不当な持出し等によって、情報セキュリティを損なうリスクが増大し、本学に何らかの損害を与えることが考えられる。それらのリスクに対応するため、情報を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を定める。

遵守事項

(1) 業務以外の利用の禁止

【基本遵守事項】

(a) 教職員等は、職務の遂行以外の目的で、情報システムに係る情報を利用しないこと。

解説：職務の遂行以外の目的で、情報システムに係る情報については、利用しないことを求める事項である。

(2) 格付け及び取扱制限に従った情報の取扱い

【基本遵守事項】

(a) 教職員等は、利用する情報に明示された格付けに従って、当該情報を適切に取り扱うこと。格付けに加えて取扱制限の明示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：情報に明示された格付け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) 要保護情報の取扱い

【基本遵守事項】

(a) 教職員等は、職務の遂行以外の目的で、要保護情報を学外に持ち出さないこと。

解説：情報の漏えい、改ざん、破損、紛失等を未然に防ぐため、教職員等が職務の遂行以外の目的で要保護情報を学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) 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。
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などを徹底する必要がある。

(c) 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) 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。

【強化遵守事項】

(e) 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必要に応じ、教職員等は、機密性３情報には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付けを下げる必要性があると思料される場合には、格付けの変更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ときは、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) 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必要に応じ、教職員等は、書面に印刷された機密性３情報には、一連番号を付し、その所在を明らかにしておくこと。

解説：書面に印刷された機密性３情報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。

3.2.3 情報の保存

趣旨（必要性）

職務においては、その事務の継続性を確保するなど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を定める。

遵守事項

(1) 格付けに応じた情報の保存

【基本遵守事項】

(a) 部局技術責任者は、電子計算機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：電子計算機に記録された情報に関して、機密性、完全性及び可用性の格付けに応じ、電子計算機の機能を活用して、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。
電子計算機におけるアクセス制御は、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。

(b) 教職員等は、情報の格付けに応じて、情報が保存された外部記録媒体を適切に管理すること。

解説：外部記録媒体に関して、機密性、完全性及び可用性の格付けに応じて、適切に管理することを求める事項である。
例えば、機密性の格付けに応じて、外部記録媒体を施錠のできる書庫・保管庫に保存し、不正な持出しや盗難を防ぐことが考えられる。
外部記録媒体が主体認証情報（パスワード）によるロック機能を持つ場合は、アクセス制御が可能であるが、ロック機能を持たない外部記録媒体も多く、保存する情報に応じた外部記録媒体を選択する必要がある。

(c) 教職員等は、情報システムに入力された情報若しくは情報システムから出力した情報を記載した書面のうち要機密情報を記載した書面、又は重要な設計書を適切に管理すること。

解説：情報を記載した書面の適切な管理を求める事項である。
例えば、必要なく情報の参照等をさせないために、書面を施錠のできる

書庫に保存するなどの措置が考えられる。

(d) **教職員等は、要機密情報を電子計算機又は外部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：電子計算機又は外部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、ファイル又は外部記録媒体の紛失・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。

(e) **教職員等は、要保全情報を電子計算機又は外部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：要保全情報を電子計算機又は外部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。

(f) **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。障害等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、バックアップ情報を記録した媒体の紛失・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) **部局技術責任者は、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、災害等への対策の必要性を検討し、必要があると認めたときは、同時被災等しないための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、遠隔地に保管することなどが考えられる。

(2) 情報の保存期間

【基本遵守事項】

(a) **教職員等は、電子計算機又は外部記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、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：情報の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、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。

3.2.4 情報の移送

趣旨（必要性）

職務においては、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記録媒体の運搬及び PC、紙面に記載された情報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を定める。

遵守事項

(1) 情報の移送に関する許可及び届出

【基本遵守事項】

(a) 教職員等は、機密性３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、あらかじめ手続を定めておくことが望ましい。

(b) 教職員等は、機密性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に届け出ること。

解説：機密性２情報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、あらかじめ手続を定めておくことが望ましい。

(2) 情報の送信と運搬の選択

【基本遵守事項】

(a) 教職員等は、要機密情報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決定し、職場情報セキュリティ責任者に届け出ること。

解説：要機密情報の安全確保に留意した移送を求める事項である。

(3) 移送手段の選択

【基本遵守事項】

(a) 教職員等は、要機密情報を移送する場合には、安全確保に留意して、当該要機密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。

解説：多種多様な移送手段の中から要機密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、部局総括責任者があらかじめ指定する運送サービス及び職員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。

(4) 書面に記載された情報の保護対策

【基本遵守事項】

(a) 教職員等は、要機密情報が記載された書面を運搬する場合には、情報の格付けに応じて、安全確保のための適切な措置を講ずること。

解説：要機密情報が記載された書面を運搬する場合におけるセキュリティ対策を求める事項である。

教職員等は、書面を運搬する場合には、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

【基本遵守事項】

(a) 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。

(b) 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。

なお、暗号化された通信路を用いて情報を送信する場合は、この限りでない。

【強化遵守事項】

(c) 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必要に応じ、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、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-ROM 等の媒体で郵送する方法が挙げられる。

3.2.5 情報の提供

趣旨（必要性）

職務においては、その事務の遂行のために教職員等以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を定める。

遵守事項

(1) 情報の公表

【基本遵守事項】

(a) 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情報に格付け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、保有する情報をホームページ等により広く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けの適正さを再度検討し、必要に応じて格付けの変更等を行った上で、当該情報が機密性１情報に格付けされるものであることを確認する必要がある。
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) 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採ること。

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において作成者名、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又は作成履歴が残っていることがないように消去等をすることが考えられる。

(2) 他者への情報の提供

【基本遵守事項】

(a) 教職員等は、機密性３情報を教職員等以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情報を教職員等以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) 教職員等は、機密性２情報を教職員等者以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。

解説：機密性２情報を教職員等以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。

(c) 教職員等は、要機密情報を教職員等以外の者に提供する場合には、提供先において、当該要機密情報が、本学の付した情報の機密性の格付けに応じて適切に取り扱われるための措置を講ずること。

解説：要機密情報を教職員等以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。

要機密情報を教職員等以外の者に提供する場合には、提供先において当該要機密情報が適切に取り扱われるように、情報の機密性の格付けを含む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要機密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。

(d) 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採ること。

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又は作成履歴が残っていることがないように消去等をすることが考えられる。

3.2.6 情報の消去

趣旨（必要性）

職務において利用した電子計算機、通信回線装置及び外部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、情報の消去を行っていたつもりでも、適切な措置が採られていなければ、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を定める。

遵守事項

(1) 電磁的記録の消去方法

【基本遵守事項】

(a) **教職員等は、電子計算機、通信回線装置及び外部記録媒体を廃棄する場合には、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊などの方法を用いて、すべての情報を復元が困難な状態にすること。**

解説：電子計算機、通信回線装置及び外部記録媒体を廃棄する場合に、すべ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消去されずに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、当該記録媒体に記録されているすべ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。

(b) **教職員等は、電子計算機、通信回線装置及び外部記録媒体を他の者へ提供する場合には、これらに保存された情報を復元が困難な状態にする必要性の有無を検討し、必要があると認めたときは、データ消去ソフトウェア又はデータ消去装置を用いて、当該電子計算機等の要機密情報を復元が困難な状態にし、残留する要機密情報を最小限に保つこと。**

解説：電子計算機、通信回線装置及び外部記録媒体に保存された情報を、必要に応じて、復元が困難な状態にすることを求める事項である。

長期にわたり利用された電子計算機、通信回線装置及び外部記録媒体には、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、外部記録媒体等を用いて教職員等以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、別の業務に当該機器等が利用されることが想定される場合には、データ消去ソフトウェア又はデータ消去装置を利用し、残留する要機密情報を最小限に保つことが必要である。

【強化遵守事項】

(c) **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必要に応じ、教職員等は、電子計算機、通信回線装置及び外部記録媒体について、設置環境等から必要があると認められる場合は、データ消去ソフトウェアを用いて、当該電子計算機等の要機密情報を復元が困難な状態にし、残留する要機密情報を最小限に保つこと。**

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記録媒体など、安全といえない環境で利用される電子計算機等に残留する要機密情報を最小限にすることを求める事項である。教職員等は、適宜、データ消去ソフトウェアを用いて、要機密情報が記録された電子ファイルの消去又は空き領域に残留する情報の消去を行うこと。

(2) 書面の廃棄方法

【基本遵守事項】

(a) **教職員等は、要機密情報が記録された書面を廃棄する場合には、復元が困難な状態にすること。**

解説：電磁的記録の消去と同様に、書面に記載された情報が不要となった場合には、シュレッダーによる細断処理、焼却又は溶解などにより、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などの理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃棄処理証明書の取得などにより、書面が確実に廃棄されていることを確認するとよい。

第４部　情報セキュリティ要件の明確化に基づく対策

4.1　情報セキュリティについての機能

4.1.1 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、本来アクセス権限のない者が、悪意又は過失により、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、主体認証に関する対策基準を定める。

なお、本学が有する各情報システムの利用者は、教職員等のほか、それ以外の者がいる。例えば、学生や学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、教職員等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、教職員等以外の者は本基準の適用範囲ではない。しかし、それらの者に対し、これを保護するよう注意喚起することが望ましい。

遵守事項

(1)　主体認証機能の導入

【基本遵守事項】

(a) 部局技術責任者は、すべ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性があると判断すること。

解説：主体認証を行う前提として、部局技術責任者は、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。

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 カードや磁気テープカード等、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。なお、本項における解説としてはそれら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。

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、そのような場合の職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などについて考慮するとよい。

(b) 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。

(c) 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、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、これ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など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。」などの警告を表示するようにすることが必要である。

(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、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。

その機能を自動化することが望ましいが、技術的に困難な場合においては、運用によって対処する必要がある。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。

(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、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などの対策を講ずること。

(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、運用上の理由など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、仮に悪意ある者によってそのシステム管理者権限を奪取されてしまった場合に、す

べ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などにより、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。

(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、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、以下の要件について検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。また、用いる方式に応じて、以下を含む要件を定めること。

(ア)正当な主体以外の主体を誤って主体認証しないこと。(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できなくならないこと。(誤否の防止)

(ウ)正当な主体が容易に他者に主体認証情報を付与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)主体認証について業務遂行に十分な可用性があること。(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なども考慮の上、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、必ずしもすべ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。

具体例：知識、所有、生体情報による主体認証方式以外の方法の具体例としては、ＧＰＳ受信装置を用いた位置による認証方式などがある。

(h) 部局技術責任者は、生体情報による主体認証方式を用いる場合には、当該生体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。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。

解説:利用者の指紋情報など、主体認証情報として生体情報を取り扱う場合に、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を求める事項である。

【強化遵守事項】

(i) 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必要に応じ、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、複数要素（複合）主体認証方式で主体認証を行う機能を設けること。

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、生体情報などのうち、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。

(j) 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必要に応じ、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、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を設けること。

解説：仮に、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は、その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、本人が不正な使用に気付く機会を得られるようにする。

(k) 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必要に応じ、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、不正にログオンしようとする行為を検知し、又は防止する機能を設けること。

解説：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。

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の2点を達成できることが望ましい。

(l) 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必要に応じ、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を設けること。

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、刑法の処罰対象となること

(m) 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必要に応じ、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、以前に設定した主体認証情報と同じものを再設定することを防止する機能を設けること。

解説：一度使用した主体認証情報（パスワードなど）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。

(n) 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必要に応じ、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、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を設けること。

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ションシステムが Unix 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) 教職員等における識別コードの管理

【基本遵守事項】

(a) 教職員等は、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、他者の許可を得て、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、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。

(b) 教職員等は、自己に付与された識別コードを他者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。

(c) 教職員等は、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。

(d) 教職員等は、職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、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、あらかじめ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、教職員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、人事異動など、大規模に識別コードの教職員等が変更となる場合や、その変更を部局技術担当者が教職員等自らからの届出によらずして把握できる場合には、教職員等自らの届出は不要とすることができる。

【強化遵守事項】

(e) 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必要に応じ、管理者権限を持つ識別コードを付与された者は、管理者としての業務遂行時に限定して、当該識別コードを利用すること。

解説：この遵守事項は、最少特権機能（least privilege 機能）と呼ばれている。

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。

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、最少特権機能が容易に操作できるような環境が整えば、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事項を選択されたい。

(3) 教職員等における主体認証情報の管理

【基本遵守事項】

(a) 教職員等は、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：教職員等は、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。

(b) 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の報告を受けた部局技術責任者又は部局技術担当者は、必要な措置を講ずること。

解説：報告を受けた者が、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) 教職員等は、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。

(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：教職員等は、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。

(イ) 自己の主体認証情報を他者に教えないこと。

解説：教職員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、証跡管理その他の情報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、「教えない」、「聞かない」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。

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設計・運用すべきである。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が望ましい。

(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、更に特殊記号など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)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などの運用によって対処することでも差し支えない。

(d) 教職員等は、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。

(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、紛失などで、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。

4.1.2 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を定める。

遵守事項

(1) アクセス制御機能の導入

【基本遵守事項】

(a) 部局技術責任者は、すべ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.bits.go.jp/inquiry/pdf/secure_os_2004.pdf

(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、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：DAC）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。

【強化遵守事項】

(c) 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必要に応じ、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、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の機能を追加すること。

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。

・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

(d) **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必要に応じ、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、強制アクセス制御機能を設けること。**

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。
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。

(2) **教職員等による適正なアクセス制御**

【基本遵守事項】

(a) **教職員等は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと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すること。**

解説：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、当該情報の格付けと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を求める事項である。
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。
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。

4.1.3 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を定める。

遵守事項

(1) **権限管理機能の導入**

【基本遵守事項】

(a) **部局技術責任者は、すべ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、部局技術責任者は、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。

(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。

【強化遵守事項】

(c) 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必要に応じ、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、最少特権機能を設けること。

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。

(d) 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必要に応じ、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、主体認証情報の再発行を自動で行う機能を設けること。

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により、安全性を強化することができる。

(e) 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必要に応じ、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、デュアルロック機能を設けること。

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

【基本遵守事項】

(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。

(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明確にすること。

(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。

(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：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。

(d) 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、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発行することが重要である。そのため、初期付与に関する本人確認や、識別コード及び主体認証情報の初期付与方法について厳格な方法を採ることを求める事項である。

(e) 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、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。ただし、共用識別コードは、部局技術責任者が、その利用を認めた情報システムでのみ付与することができる。

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。

(f) 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、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与すること。

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。

(g) 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、教職員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、当該教職員等の識別コードを無効にすること。また、人事異動等、識別コードを追加又は削除する時に、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。

(h) 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、教職員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、当該教職員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、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。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。

(i) 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、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アクセス制御に係る設定をすること。また、人事異動等、識別コード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：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限のみを付与することを求める事項である。

【強化遵守事項】

(j) 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必要に応じ、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、単一の情報システムにおいては、１人の教職員等に対して単一の識別コードのみを付与すること。

解説：デュアルロック機能を備えた情報システムでは、１人の**教職員等**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いことから、１人の教職員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。

(k) 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必要に応じ、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、付与した識別コードをどの主体に付与していたかの記録について、保存すること。当該記録を消去する場合には、部局総括責任者からの事前の承認を得ること。

解説：識別コードは将来の障害等の原因調査に備えて長期保存を原則とし、削除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、適切な承認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。

(l) 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必要に応じ、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、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しないこと。

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。ただし、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など、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、識別コードを再利用しても構わないが、その際、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。なお、識別コードを以前使用していた同一の主体に対する再利用を認めるか、認めないかについては、部局総括責任者による判断に従うものとする。

(3) 識別コードと主体認証情報における代替措置の適用

【基本遵守事項】

(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教職員等から、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教職員等においては、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、申請者が正当な教職員等であること及び許可申請の理由が妥当であることを確認した上で、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などが想定されるが、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教職員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、適正な代替手段をあらかじめ準備しておくこと。
なお、代替手段の実施に当たっては、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の報告を受けた場合には、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：不正使用の報告を受けた場合には、他の基準項目で定められている障害等の対応に係る遵守事項とともに、本事項の対応を実施する。
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、すべ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べきである。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べきである。

4.1.4 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を定める。

遵守事項

(1) **証跡管理機能の導入**

【基本遵守事項】

(a) **部局技術責任者は、すべ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、部局技術責任者に、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。

(b) **部局技術責任者は、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：利用者の行動等の事象を証跡として記録する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。
情報セキュリティは、様々な原因で損なわれることがある。クラッカー

等の部外者による不正アクセス、不正侵入、操作員の誤操作又は不正操作、学内及び学外の情報システム利用者の誤操作又は不正操作などがその原因となる。また、職務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り、そのために不正アクセス、不正侵入等の事象、操作員及び利用者の行動を含む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。部局技術責任者は、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。

記録事項には、以下の記録を含めることが考えられる。

・利用者による情報システムの操作記録

・操作員、監視要員及び保守要員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

(c) 部局技術責任者は、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、事象を証跡として記録するに当たり、事象ごとに必要な情報項目を記録するように情報システムの設定をすること。

解説：証跡を取得する場合に、取得する情報項目を適切に選択す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：

・事象の主体である人又は機器を示す識別コード

・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

・操作員、監視要員及び保守要員等への通知の内容

(d) 部局技術責任者は、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針を整備し、必要に応じ、これらの場合に対応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応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員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、整備した対処方針を実現するために必要な場合に限られる。

(e) 部局技術責任者は、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、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い、外部記録媒体等その他の装置・媒体に記録した証跡についてはこれを適正に管理すること。

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、適切な格付けを与えてこれを管理することを求める事項である。証跡の格付けは、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、部局技術担当者及び操作員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。

なお、「適正に管理する」とは、「3.2.3 情報の保存」に準拠して管理することをいう。

【強化遵守事項】

(f) 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必要に応じ、部局技術責任者は、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、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。

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、報告書を生成するなどにより、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。

(g) 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必要に応じ、部局技術責任者は、取得した証跡管理情報の内容により、情報セキュリティ侵害の可能性を示す事象を検知した場合に、監視要員等にその旨を即時に通知する機能を情報システムに設けること。

解説：セキュリティ侵害の可能性を示す事象が発生した場合に、迅速な対応を可能とするために、監視要員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など、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) 部局技術担当者による証跡の取得と保存

【基本遵守事項】

(a) 部局技術担当者は、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、部局技術責任者が情報システムに設けた機能を利用して、証跡を記録すること。

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記録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、定められた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を定め、当該保存期間が満了する日まで証跡を保存し、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。保存期間は、学外にアクセスする情報システムにおいては３ヶ月以上とし、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。

解説：取得した証跡を適正に保存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、事後追跡に必要であると考えられる保存期間をあらかじめ定め、その間証跡を保存する必要がある。証跡を保存する期間は、１つの情報システムの各所で取得する証跡により異なることもあり得る。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すべて保有できるファイル容量としたり、証跡を適宜外部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、定められた対処を行うこと。

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応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、あらかじめ定められた操作を行うことが求められる。定められた操作とは、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。

(3) 取得した証跡の点検、分析及び報告

【強化遵守事項】

(a) 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必要に応じ、部局総括責任者又は部局技術責任者は、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、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又はそれぞれ全学実施責任者若しく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、そのすべ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。

(b) 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必要に応じ、監視要員等は、セキュリティ侵害の可能性を示す事象を検知した旨の通知を受けた場合には、あらかじめ定められた措置を採ること。

解説：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これを監視要員等に即時に通知する機能を持つ情報システムにおいて、通知を受けた監視要員等に対して、あらかじめ定められた措置を採ることを求める事項である。あらかじめ定められた措置とは、操作手順の実行、特定の者への報告等が想定される。

(4) 証跡管理に関する利用者への周知

【基本遵守事項】

(a) 部局総括責任者又は部局技術責任者は、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、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。

4.1.5 保証のための機能

趣旨（必要性）

本基準では、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、これらの機能のこれらの機能による情報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。

遵守事項

(1) 保証のための機能の導入

【基本遵守事項】

(a) 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の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。

(b) 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。

情報が適切な状態にあることを保証するための「保証のための機能」としては、例えば、アクセスする情報に対して、主体認証、アクセス制御、権限管理、証跡管理の各機能が有効に実施されていることを確認するための上位の機能などが挙げられるが、それに限ることなく、多種多様な

機能が考えられる。
また、「保証のための機能」とは、主体認証機能等の各項のような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項の遵守事項を達成することができる。

4.1.6 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の付与が有効とされている。

これらのことを勘案し、本項では、暗号化及び電子署名の付与に関する対策基準を定める。

遵守事項

(1) 暗号化機能及び電子署名の付与機能の導入

【基本遵守事項】

(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の程度から電子署名の付与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、電子署名の付与を行う機能を設けること。

解説：情報の完全性の程度から電子署名の付与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を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズム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から選択すること。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つをそれらのリストの中から選択すること。**

解説：行政情報システム関係課長連絡会議では、「必要とされる安全性及び信頼性などに応じ、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとする」こととされており、これに基づく措置を求める事項である。暗号化又は電子署名の付与に用いるアルゴリズムを選択するに当たっては、その暗号強度、利用条件、効率性等について多角的な検討を行うことが求められる。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。

【強化遵守事項】

(f) **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必要に応じ、部局技術責任者は、暗号化又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、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。**

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。

(g) **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必要に応じ、部局技術責任者は、暗号化又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、複数のアルゴリズムを選択可能とすること。**

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。

(h) **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必要に応じ、部局技術責任者は、暗号化又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、選択したアルゴリズムが、ソフトウェアやハードウェアへ適切に実装されているか否かを確認すること。**

解説：アルゴリズムの実装状況について確認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う。

(i) 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必要に応じ、部局技術責任者は、暗号化又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、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を、第三者による物理的な攻撃から保護するために、耐タンパー性を有する暗号モジュールへ格納すること。

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。

(2) 暗号化及び電子署名の付与に係る管理

【基本遵守事項】

(a) 部局技術責任者は、暗号化又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、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、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応手順等を定めること。

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応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、あらかじめ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。

(b) 部局技術責任者は、暗号化又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、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、鍵の保存媒体及び保存場所を定めること。

解説：鍵の保存媒体及び保存場所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、あらかじめ鍵の保存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。

(c) 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。

【強化遵守事項】

(d) 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必要に応じ、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おいて、暗号化された情報の復号に用いる鍵のバックアップの取得方法又は鍵の預託方法を定めること。

解説：暗号化された情報の復号に用いる鍵の紛失及び消去に備え、鍵のバックアップの取得方法又は鍵の預託方法を定めることを求める事項である。

例えば、復号に用いる鍵を紛失又は消去した場合には、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、又は信頼できる第三者へ鍵情報を預託する等の対策が必要である。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。

(e) 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必要に応じ、部局技術責任者は、暗号化又は電子署名の付与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。

また、CRYPTREC による発表に関心を払うことが必要である。

(3) 暗号化機能及び電子署名の付与機能の利用

【基本遵守事項】

(a) 教職員等は、要機密情報を移送する場合又は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：要機密情報を移送する場合又は電磁的記録媒体に保存する場合、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。

(b) 教職員等は、要保全情報を移送する場合又は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：要保全情報を移送する場合又は電磁的記録媒体に保存する場合、その改ざんに係るリスクを勘案し、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。

(c) 教職員等は、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、これを他者に知られないように自己管理すること。

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、教職員等による鍵情報の保護を求める事項である。

(d) 教職員等は、暗号化された情報の復号に用いる鍵について、機密性、完全性、可用性の観点から、バックアップの必要性の有無を検討し、必要があると認めたときは、そのバックアップを取得し、オリジナルの鍵と同等の安全管理をすること。

解説：鍵の書換え、紛失、消去等により、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。その観点からは、鍵のバックアップを取得することが望まれるが、一方でバックアップを取得することによって鍵が露呈する危険性が増大し、その機密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自体の機密性、完全性が損なわれる可能性もある。そのため、バックアップを取得する場合には、その機密性、完全性、可用性の観点から十分に検討することを求める事項である。

4.2 情報セキュリティについての脅威

4.2.1 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、ウイルス感染等の脅威の発生原因になるなど、情報システム全体のセキュリティの大きな脅威となる。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応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を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

(a) 部局技術担当者は、電子計算機及び通信回線装置（公開されたセキュリティホールの情報がない電子計算機及び通信回線装置を除く。以下この項において同じ。）について、セキュリティホール対策に必要となる機器情報を収集し、書面として整備すること。

解説：セキュリティホール対策に必要となる機器情報の収集及び書面整備を求める事項である。セキュリティホール対策に必要となる機器情報としては、例えば、電子計算機及び通信回線装置の機種並びに当該電子計算機及び通信回線装置が利用しているソフトウェアの種類及びバージョン等が挙げられる。

また、公開されたセキュリティホール情報がない電子計算機及び通信回線装置についても、同様に情報収集等に努めることが望ましい。

(b) 部局技術担当者は、電子計算機及び通信回線装置の構築又は運用開始時に、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構築又は運用開始時に、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。

【強化遵守事項】

(c) 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必要に応じ、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、セキュリティホール対策中にサービス提供が中断しないように、電子計算機及び通信回線装置を冗長構成にすること。

解説：セキュリティホール対策を実施する際に電子計算機及び通信回線装置を

停止する場合に、サービス提供を中断させないための措置を求める事項である。

サービス提供を中断できない情報システムでは、電子計算機及び通信回線装置を冗長構成にすることで、セキュリティ対策を実施する際の可用性を高めることが必要である。

(d) 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必要に応じ、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いない段階においても電子計算機及び通信回線装置上でその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が挙げられる。

(2) 情報システムの運用時

【基本遵守事項】

(a) 部局技術担当者は、電子計算機及び通信回線装置の構成に変更があった場合には、セキュリティホール対策に必要となる機器情報を記載した書面を更新すること。

解説：公開されたセキュリティホールに関連する情報との対応付けをするため、セキュリティホール対策に必要となる機器情報の最新化を求める事項である。

(b) 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連する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。

(c) 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から、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作成すること。

(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)対策テストの必要性
(キ)対策テストの方法
(ク)対策テストの実施予定

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、対策計画の作成を求める事項である。

「対策テスト」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。

(d) 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。

(e) 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。

(f) 部局技術担当者は、信頼できる方法で対策用ファイルを入手すること。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媒体を利用して入手する方法が挙げられる。また、改ざんなど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。

(g) 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、導入及び利用されているソフトウェアの種類、当該ソフトウェアの設定のことである。

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。

(h) 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。

4.2.2 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、主体認証情報等の秘密情報や業務上の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など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を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

(a) 部局総括責任者は、不正プログラム感染の回避を目的とした教職員等に対する留意事項を含む日常的実施事項を定めること。

解説：日常的に不正プログラム対策のために実施する事項の明文化を求める事項である。

「教職員等に対する留意事項」とは、アンチウイルスソフトウェア等が現存する不正プログラムをすべて検知できるとは限らないため、教職員等に対して注意喚起を行う事項であり、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、不審なホームページを閲覧しないこと等である。

「日常的実施事項」とは、不正プログラムに関する情報の収集や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検出等が挙げられる。

これらの事項については、不正プログラム対策の実施単位ごとに定めることが原則であるが、複数の不正プログラム対策の実施単位において共通して運用できる場合には、複数の実施単位で内容を整備する等状況に応じていずれかの方法を選択することが可能である。

(b) 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、本事項は適用されない。

(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のすべ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。

【強化遵守事項】

(d) 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必要に応じ、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、異なる業者のアンチウイルスソフトウェア等を組み合わせ、導入すること。

解説：複数の業者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、これらは現存するすべ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、感染経路において複数の製品や技術を組み合わせ、どれか１つの不具合で、その環境のすべ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。

(e) 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必要に応じ、部局技術責任者は、不正プログラムが通信により拡散することを防止するための対策を実施すること。

解説：不正プログラムが短時間かつ大規模に感染を拡大する場合には通信を利用することが多いため、その防止策の導入を求める事項である。

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。

(2) 情報システムの運用時

【基本遵守事項】

(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、教職員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など、日常から行われている不正プログラム対策では対応が困難と判断される場合が挙げられる。

(b) 教職員等は、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る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、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る実行ファイル等の実行を禁止する事項である。

(c) 教職員等は、アンチウイルスソフトウェア等にかかわ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(d)～(f)の事項は、部局総括責任者が適切な方法を選択すること。

(d) 教職員等は、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。

(e) 教職員等は、アンチウイルスソフトウェア等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、定期的にすべての電子ファイルを検査する必要がある。

(f) **教職員等は、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。

(g) **教職員等は、ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。**

解説：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感染を防ぐ、といった個別のアプリケーションごとに設定することが可能な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。オペレーティングシステムに不正プログラムに対応する機能がある場合には、当該機能を利用しても差し支えない。

(h) **部局総括責任者は、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：不正プログラム対策状況を適宜把握し、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。

【強化遵守事項】

(i) **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必要に応じ、部局総括責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておくこと。**

解説：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等、新種の不正プログラム等に対応した不正プログラム定義ファイルがアンチウイルスソフトウェア等の製造業者から提供されるより前に、不正プログラムに感染した場合等において、外部から支援を受けられるように準備しておくことを求める事項である。

4.2.3 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。また、インターネットに

接続しているサーバ装置及び端末は、不正プログラム感染又は不正侵入等により、管理者が意図しないにもかかわらず他者へサービス不能攻撃を行ってしまうおそれがある。

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。

これらのことを勘案し、サービス不能攻撃に関する対策基準を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

(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。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、サーバ装置における SYN Cookie、通信回線装置における SYN Flood 対策機能等を有効にすること等が挙げられる。

【強化遵守事項】

(b) 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必要に応じ、部局技術責任者は、サービス不能攻撃を受けた場合、通信回線装置や通信回線を共用している他サービスや内部からのインターネットへのアクセスにも影響が及ぶことを考慮して通信回線装置及び通信回線の構築を行うこと。

解説：管理する情報システムと通信回線装置や通信回線を共有している他の情報システムとの関係も考慮した上で、サービス不能攻撃の影響を分析し、通信回線装置、通信回線の構築を行うことを求める事項である。

(c) 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必要に応じ、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の整備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。また、不正プログラムの感染又は不正侵入等を受けることにより、管理する電子計算機から他者にサービス不能攻撃を行ってしまうおそれがあるため、当該電子計算機等を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り、サービス不能攻撃に利用されることに関する監視には、電子計算機からインターネットへの通信の監視のほか、電子計算機にサービス不能攻撃を行わせる命令の有無の監視がある。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。

(d) 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必要に応じ、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、又は低減する対策装置を導入すること。

解説：電子計算機及び通信回線装置における対策については、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。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。

(e) 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必要に応じ、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しておくこと。

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などが挙げられる。

(f) 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必要に応じ、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。

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。

(g) 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必要に応じ、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定めておくこと。

解説：部局技術責任者が、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。

(2) 情報システムの運用時

【強化遵守事項】

(a) 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必要に応じ、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。

(b) 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必要に応じ、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、前事項の記録をサービス不能攻撃の検知技術の向上に反映すること。

解説：前事項で把握した情報をサービス不能攻撃による異常発生の検知精度向上及び検知時間の短縮等の検知技術の向上に活用することを求める事項である。

(c) 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必要に応じ、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、定期的にサービス不能攻撃の対策の見直しを行うこと。

解説：サービス不能攻撃の動向や電子計算機等への対策を運用した結果に応じて、定期的に対策を見直すことを求める事項である。

4.3 情報システムのセキュリティ要件

4.3.1 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、設計、構築、運用、監視、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情報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) 情報システム計画・設計

【基本遵守事項】

(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開発・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。

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、その中で重要とみなされる要求事項について対策を実施する対象を確定し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などのセキュリティに関する手順も含まれる。決定されたセキュリティ要件は、システム要件定義書や仕様書などの形式で明確化した上で、実装していくことが望ましい。

(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：本項は、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。本基準から当該情報システムのセキュリティ対策として実施する遵守事項を選択した上でセキュリティ要件を満たしているかを検討し、満たしていないセキュリティ要件がある場合には、その対策も定めることが必要である。

(d) 部局技術責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムの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・ST 確認を受けること。ただし、情報システムを更改する場合であって、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情報システムについては、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・ST 確認を行うことを求める事項である。「ST 評価・ST 確認を受けること」とは、ST 評価・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。情報システム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・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開発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、情報システムの構築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・ST 確認を受けさせることになる。

(e) 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、教育やトラブル対応について手順を整備することを求める事項である。

【強化遵守事項】

(f) 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必要に応じ、部局技術責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合には、その中から当該セキュリティ機能に関して IT セキュリティ評価及び認証制度に基づく認証を取得している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、より信頼度の高い情報システムが構築できる。

(2) 情報システムの構築・運用・監視

【基本遵守事項】

(a) 部局技術責任者は、情報システムの構築、運用及び監視に際しては、セキュリティ要件に基づき定めた情報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を実施し、情報システムを構築、運用及び監視することを求める事項である。

(3) 情報システムの移行・廃棄

【基本遵守事項】

(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採ること。

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、情報の格付け等を考慮して、機器及び情報に関して廃棄、保存、消去等の適切な措置を採ることを求める事項である。

(4) 情報システムの見直し

【基本遵守事項】

(a) 部局技術責任者は、情報システムの情報セキュリティ対策について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：情報システムの情報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５部　情報システムの構成要素についての対策

5.1 施設と環境

5.1.1 電子計算機及び通信回線装置を設置する安全区域

趣旨（必要性）

電子計算機及び通信回線装置の設置環境について、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状況においては、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が行われるおそれがある。また、設置環境に関する脅威としては、自然災害の発生により情報システムが損傷する等のおそれもある。

これらのことを勘案し、本項では、安全区域に関する対策基準を定める。

遵守事項

(1) 立入り及び退出の管理

【基本遵守事項】

(a) 部局技術責任者は、安全区域に不審者を立ち入らせない措置を講ずること。

解説：安全区域への不審者の立入りを防止し、安全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、安全区域の所在の表示の制限等が挙げられる。

【強化遵守事項】

(b) 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必要に応じ、部局技術責任者は、安全区域をセキュリティレベルが異なる区域から物理的に隔離し、立入り及び退出が可能な場所を制限する措置を講ずること。

解説：安全区域を壁及び施錠することが可能な扉等によりセキュリティレベルが異なる区域から隔離し、安全区域へ立ち入る者の主体認証を行うことが可能な管理された箇所からのみ立入り及び退出できるようにするための事項である。

(c) 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必要に応じ、部局技術責任者は、安全区域へ立ち入る者の主体認証を行うための措置を講ずること。

解説：安全区域へ立ち入る者の主体認証を実施することで、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、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。

(d) 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必要に応じ、部局技術責任者は、安全区域から退出する者の主体認証を行うための措置を講ずること。

解説：立ち入った者の退出を把握するための事項である。

(e) 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必要に応じ、部局技術責任者は、主体認証を経た者が、主体認証を経ていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。

解説：安全区域の立入り及び退出時における主体認証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。

(f) 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必要に応じ、部局技術責任者は、安全区域へ継続的に立ち入る者を承認する手続を整備すること。また、その者の氏名、所属、立入承認日、立入期間及び承認事由を含む事項を記載した書面を整備すること。

解説：書面を整備することで、安全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。

(g) 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必要に応じ、部局技術責任者は、安全区域へ立入りが承認された者に変更がある場合には、当該変更の内容を前事項の書面へ反映させること。また、当該変更の記録を保存すること。

解説：変更の内容を前事項の書面へ反映することで安全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。

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。

(h) 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必要に応じ、部局技術責任者は、安全区域へのすべての者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を講ずること。

解説：安全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、安全区域のセキュリティが侵害された際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、安全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。

(2) 訪問者及び受渡業者の管理

【強化遵守事項】

(a) 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必要に応じ、部局技術責任者は、安全区域への訪問者がある場合には、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を講ずること。

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、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。

(b) 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必要に応じ、部局技術責任者は、安全区域への訪問者がある場合には、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

るための措置を講ずること。

解説：訪問記録の作成を求める事項である。

(c) 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必要に応じ、部局技術責任者は、安全区域への訪問者がある場合には、訪問相手の教職員等が訪問者の安全区域への立入りについて審査するための手続を整備すること。

解説：訪問者の安全区域への立入りについて、訪問相手の教職員等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教職員等に連絡し、訪問者の立入りについて審査する」、「訪問相手の教職員等が、安全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。

(d) 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必要に応じ、部局技術責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。

解説：訪問者が許可されていない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。訪問者に主体認証情報格納装置は貸与しない又は貸与する場合には最小限の権限を持った装置とする方法等が挙げられる。

(e) 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必要に応じ、部局技術責任者は、安全区域内において訪問相手の教職員等が訪問者に付き添うための措置を講ずること。

解説：訪問者が許可されていない区域へ立ち入らないように教職員等が監視することを求める事項である。

(f) 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必要に応じ、部局技術責任者は、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講ずること。

解説：継続的に立入りが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。

(g) 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必要に応じ、部局技術責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。

(ア)安全区域外で受渡しを行うこと。

(イ)業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、外部記録媒体、書面に触れることができない場所に限定し、教職員等が立ち会うこと。

解説：安全区域内の教職員等と物品の受渡しを行う業者の立入りを制限するための事項である。

(3) 電子計算機及び通信回線装置のセキュリティ確保

【強化遵守事項】

(a) 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必要に応じ、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、電子計算機及び通信回線装置を他の情報システムから物理的に隔離し、安全区域を共用しないこと。

解説：他の情報システムと共用の安全区域に設置した場合であって、セキュリティが確保できないときに、物理的に隔離することを求める事項である。

(b) 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必要に応じ、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、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を所定の設置場所から移動できない措置を講ずること。

解説：設置場所が固定された電子計算機及び通信回線装置に関して、盗難及び教職員等による許可されない持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等が挙げられる。

(c) 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必要に応じ、部局技術責任者は、教職員等が離席時に電子計算機及び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：教職員等の離席時に、電子計算機及び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、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の主体認証にも利用する方法等が挙げられる。

(d) 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必要に応じ、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、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を講ずること。

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。

(e) 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必要に応じ、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、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を講ずること。

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。

(f) 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必要に応じ、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、電磁波による情報漏えい対策の措置を講ずること。

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。

(4) 安全区域内のセキュリティ管理

【基本遵守事項】

(a) 教職員等は、安全区域内において、身分証明書を他の職員から常時視認することが可能な状態にすること。

解説：安全区域への立入りを許可されていることを外見上判断できるようにするための事項である。

【強化遵守事項】

(b) 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必要に応じ、教職員等は、要保護情報を取り扱う情報システムについては、部局技術責任者の承認を得た上で、情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しを行うこと。

解説：情報システムに関連する物品の持込み及び持出しによって生ずるリスクに対応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、安全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、外部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。

(c) 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必要に応じ、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、安全区域への持込み及び安全区域からの持出しについて、持込み及び持出しに係る記録を取得すること。

解説：情報システムに関連する物品の持込み及び持出しを記録し、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。

(d) 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必要に応じ、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、情報システムに関連しない電子計算機、通信回線装置、外部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。）の安全区域への持込みについて制限すること。

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、外部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。

(e) **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必要に応じ、部局技術責任者は、安全区域内での作業を監視するための措置を講ずること。**

解説：安全区域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、監視カメラの導入などが挙げられる。

(5) 災害及び障害への対策

【強化遵守事項】

(a) **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必要に応じ、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、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、サーバラックの利用のほか、ハロゲン化物消火設備、無停電電源装置等の設備、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) **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必要に応じ、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、安全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安全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。

5.2 電子計算機

5.2.1 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、ウイルス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若しくは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、職員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を定める。

遵守事項

(1) 電子計算機の設置時

【基本遵守事項】

(a) 部局技術責任者は、電子計算機のセキュリティ維持に関する規定を整備すること。

解説：電子計算機に関する対策について定めることを求める事項である。

「電子計算機のセキュリティ維持に関する規定」とは、主体認証、アクセス制限及び情報システムの保守に関する目的、対象とする機器の範囲、管理する教職員等及び利用者の役割及び責任のほか、端末の利用許可、モバイル PC の持出許可、利用者の識別コードの管理方法及び主体認証情報の管理方法並びに接続可能通信回線及びセキュリティ設定等の手順を整備する規定である。部局技術責任者の所管する単位ごとに規定を整備することが原則であるが、当該規定の内容を変更する必要がない場合には複数の実施単位で共通に整備する等状況に応じていずれかの方法を選択することが可能である。

(b) 部局技術責任者は、すべての電子計算機に対して、電子計算機を管理する教職員等及び利用者を特定するための文書を整備すること。

解説：電子計算機の管理状況の確認等を容易にするとともに、盗難及び紛失等を防止する責任の所在を明確にすることを目的とした事項である。

(c) 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能力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、テスト等を実施し、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。

(d) 部局技術責任者は、利用者が電子計算機にログインする場合には主体認証を行

うように電子計算機を構成すること。

解説：電子計算機を利用した者を特定するために行う事項である。

サーバ装置及び複数者で利用する共用PC等の端末の場合でも利用者に識別コードを個別に割り当て、各識別コードに対応する主体認証情報（パスワード）を用いた主体認証等、本人性を確認することが可能な主体認証技術を用いる必要がある。

(e) 部局技術責任者は、ログオンした利用者の識別コードに対して、権限管理を行うこと。

解説：識別コードごとに必要となる権限のみを付与することを求める事項である。管理者権限は、最小限の識別コードに与える必要がある。

(f) 部局技術責任者は、電子計算機上で動作するオペレーティングシステム及びアプリケーションに存在する公開されたセキュリティホールから電子計算機（公開されたセキュリティホールの情報がない電子計算機を除く。）を保護するための対策を講ずること。

解説：セキュリティホール対策を行うことで、電子計算機のセキュリティが確保された状態にするための事項である。

なお、多くのメインフレームシステムのように、電子計算機に搭載しているオペレーティングシステムによっては、セキュリティホールがまれにしか報告されないものもあるが、これらについても、公開されている通信プロトコルに関してセキュリティホールが報告された場合等においては、これと関連するソフトウェアに関して措置を講ずる必要がある。

当該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端末については、セキュリティホールが報告されることはないため、本事項は適用されない。

(g) 部局技術責任者は、不正プログラムから電子計算機（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ものを除く。）を保護するための対策を講ずること。

解説：ウイルス及びワーム等の不正プログラムから電子計算機を保護するための事項である。

セキュリティホール対策だけでなく、アンチウイルスソフトウェア等の導入等を実施する必要がある。

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端末については、不正プログラムが送り込まれることは実質的にないため、本事項は適用されない。

(h) 部局技術責任者は、電子計算機関連文書を整備すること。

解説：電子計算機と関連文書の整合性を確保するための事項である。

「電子計算機関連文書」とは、電子計算機の設計書、仕様書及び操作マニュアル等である。書面ではなく電磁的記録媒体で整備していても差し支えない。

(i) 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

機を安全区域に設置すること。ただし、モバイル PC 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、利用者による誤操作、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。

【強化遵守事項】

(j) 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必要に応じ、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こと。

解説：障害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。災害等を想定して冗長構成にする場合には、電子計算機を遠隔地に設置することが望ましい。

(2) 電子計算機の運用時

【基本遵守事項】

(a) 部局技術担当者は、電子計算機のセキュリティ維持に関する規定に基づいて、電子計算機の運用管理を行うこと。

解説：整備された規定に従っ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を求める事項である。

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。

(b) 部局技術責任者は、適宜、電子計算機のセキュリティ維持に関する規定の見直しを行うこと。また、当該規定を変更した場合には、当該変更の記録を保存すること。

解説：電子計算機のセキュリティ対策を適宜見直すことを求める事項である。

セキュリティ対策は、想定するリスクに対して実施すべきであり、時間の経過によるリスクの変化に応じて、その見直しが必要になる。

(c) 教職員等は、職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。

本学が所管する電子計算機への不正アクセスを禁止する意味を含んでいる。

(d) 部局技術責任者は、電子計算機を管理する教職員等及び利用者を変更した場合には、当該変更の内容を、電子計算機を管理する教職員等及び利用者を特定するための文書へ反映すること。また、当該変更の記録を保存すること。

解説：電子計算機を管理する教職員等及び利用者を変更した場合に、現状を反映するように管理することを求める事項である。

また、変更に関して記録を残し、後で参照できるようにしておく必要がある。

(e) 部局技術責任者は、電子計算機のセキュリティレベルを維持するため、公開されたセキュリティホールから電子計算機を保護するための対策を講ずること。

解説：電子計算機の運用中、公開されたセキュリティホールに対応することにより、電子計算機のセキュリティレベルを維持するための事項である。

例えば、対策としては、公開されたセキュリティホールに対処するための対策計画の検討及び実施を意味し、対策計画を検討する初期の段階では、「直接解決する対策方法がないため代替案を実施する」、「リスクが大きくないので対策しない」といった計画で差し支えない。その判断は各実施単位に委ねられる。

なお、多くのメインフレームシステムのように、電子計算機に搭載しているオペレーティングシステムによっては、公開されたセキュリティホールがまれにしか報告されないものもあるが、これらについても、公開されている通信プロトコルに関してセキュリティホールが報告された場合等においては、これと関連するソフトウェアに関して対処する必要がある。

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端末については、セキュリティホールが報告されることはないため、本事項は適用されない。

(f) 部局技術責任者は、電子計算機のセキュリティレベルを維持するため、不正プログラムから電子計算機を保護するための対策を講ずること。

解説：電子計算機の運用中に公開された不正プログラムに対応することにより、電子計算機のセキュリティレベルを維持するための事項である。

対策とは、不正プログラム対策の責任体制の整備、アンチウイルスソフトウェア等を利用した対策等を意味する。

なお、多くのメインフレームシステムのように、電子計算機に搭載しているオペレーティングシステムによっては、公開された不正プログラムがまれにしか報告されないものもあるが、報告された場合等においては、これと関連するソフトウェアに関して対処する必要がある。

(g) 部局技術担当者は、電子計算機の構成を変更した場合には、当該変更の内容を電子計算機関連文書へ反映すること。また、当該変更の記録を保存すること。

解説：部局技術担当者が行った変更の内容を適宜関連文書に反映することで、電子計算機と関連文書の整合性を確保するための事項である。

【強化遵守事項】

(h) 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必要に応じ、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すべ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した場合には、当該不適切な状態の改善を図ること。

解説：電子計算機で利用されているソフトウェアのセキュリティホールの対処

状況及び不正なソフトウェアの存在確認等を定期的に調べ、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。
なお、「不適切な状態」とは、パッチが適用されていない、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等の状態のことをいう。

(3) 電子計算機の運用終了時

【基本遵守事項】

(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、データ消去ソフトウェア若しくはデータ消去装置の利用、又は物理的な破壊若しくは磁気的な破壊等の方法を用いて、すべての情報を復元が困難な状態にすること。

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、すべ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消去されずに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すべ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。

5.2.2 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ウイルス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を定める。

遵守事項

(1) 端末の設置時

【基本遵守事項】

(a) 部局技術責任者は、端末で利用可能なソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙、または両者を併用することができる。

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、端末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。

(b) 部局技術責任者は、要保護情報を取り扱うモバイル PC については、学外で使われる際にも、学内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：学外で利用されるモバイル PC は、学内で利用される端末と異なる条件下に置かれるため、学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 PC 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 PC において実施する必要がある。

(c) 教職員等は、モバイル PC 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 PC 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 PC の利用にとどめるための事項である。

(d) 部局技術責任者は、要機密情報を取り扱うモバイル PC については、内蔵記録媒体に保存される情報の暗号化を行う機能を付加すること。

解説：モバイル PC が物理的に外部の者の手に渡った場合には、モバイル PC から取り外された内蔵記録媒体を他の電子計算機に取り付け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。

(e) 部局技術責任者は、要保護情報を取り扱うモバイル PC については、盗難を防止するための措置を定めること。

解説：モバイル PC 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求める事項である。

対策としては、学内においては、モバイル PC を安全区域内に設置している場合においても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、学外においては、常に身近に置き目を離さないこと等が挙げられる。

【強化遵守事項】

(f) 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必要に応じ、部局技術責任者は、教職員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こと。

解説：端末から情報が漏えいすることを防ぐために、内蔵記録媒体又は外部記録媒体を装備しない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

【基本遵守事項】

(a) 教職員等は、端末での利用可能と定められたソフトウェアを除いて、ソフトウェアを利用してはならない。

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増大することから、定められたソフトウェア以外の利用を禁止する事項である。

(b) モバイル PC を利用する教職員等は、要保護情報を取り扱うモバイル PC については、盗難防止措置を行うこと。

解説：モバイル PC を利用する教職員等に対して、モバイル PC 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。

(c) 教職員等は、要機密情報を取り扱うモバイル PC については、モバイル PC を学外に持ち出す場合に、当該モバイル PC の内蔵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 PC の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、ハードディスク内の情報に対してファイル又はハードディスク全体を暗号化する必要性を検討すること。学外に持ち出す場合、紛失又は盗難等のリスクが高まるため、可能な限り暗号化する必要がある。暗号化に準ずる方法としては、秘密分散等の情報保護措置の実施が挙げられる。

(d) 教職員等は、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 PC を学外に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。

【強化遵守事項】

(e) 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必要に応じ、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。

5.2.3 サーバ装置

趣旨（必要性）

サーバ装置については、当該サーバ装置の内蔵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、ウイルス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、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を定める。

遵守事項

(1) サーバ装置の設置時

【基本遵守事項】

(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、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、送受信される情報を暗号化すること。

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、通信の暗号化の対策が必要である。

(b) 部局技術責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。

解説：サーバ装置において、サービスの提供及びサーバ装置の運用管理に必要となるソフトウェアを定めるための事項である。必要なソフトウェアを定める方法としては、サーバ装置の仕様書において定める、独立の文書として定める等が挙げられる。

(c) 部局技術責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動すること。

解説：不要なサーバアプリケーションの停止及び不要な機能の無効化により、サーバ装置から潜在的な脅威を排除するための事項である。

【強化遵守事項】

(d) 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必要に応じ、部局技術責任者は、利用が定められたソフトウェアに該当しないソフトウェアをサーバ

装置から削除すること。

解説：利用が定められたソフトウェアに該当しないものが導入されている場合、利用を禁止していても不正侵入した攻撃者等に悪用される可能性があるため、当該ソフトウェアをサーバ装置から削除することを求める事項である。

(2) サーバ装置の運用時

【基本遵守事項】

(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、対応すること。

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応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保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理すること。

解説：バックアップを取得することにより情報の保護を目的とした事項である。バックアップの対象は、サーバ装置に保存されている情報から適宜選択すること。「安全に管理」とは、記録した媒体を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ことである。また、災害等を想定してバックアップを取得する場合には、媒体を遠隔地に保存することが望ましい。「定期的」とは、1 日又は 1 週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。

(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書面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) 部局技術責任者は、サーバ装置上で証跡管理を行う必要性を検討し、必要と認めた場合には実施すること。

解説：サーバ装置上で取得可能な証跡について、証跡管理を行うための事項である。管理として、取得する情報項目の設定、証跡の保存及び点検、分析並びに報告等が挙げられる。

(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、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。

【強化遵守事項】

(f) 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必要に応じ、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し、不正行為及び不正利用を含む事象の発生を検知すること。

解説：サーバ装置上での不正行為及び不正利用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要機密情報へのアクセス等の不正利用の発生を監視することである。

監視の方法としては、侵入検知システム、アンチウイルスソフト又はファイル完全性チェックツール等が利用できる。

(g) 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必要に応じ、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し、当該サーバ装置に関するトラブル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、トラブル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。

(h) 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必要に応じ、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、サービス提供に必要なサーバ装置の負荷を複数のサーバ装置に分散すること。

解説：障害や過度のアクセス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サーバ装置群の負荷を分散させることにより、サービスが中断しないように、負荷分散装置の設置、DNS による負荷分散等の実施を求める事項である。

5.3 アプリケーションソフトウェア

5.3.1 通信回線を介して提供するアプリケーション共通対策

趣旨（必要性）

IP ネットワークの技術は一般的に普及していること等の理由により、通信回線を介して提供するサービスには、セキュリティ脅威全般に係るリスクが考えられる。これらのリスクを回避するためには、情報システムのライフサイクル全般に対して適切な対策を施すことが必要である。

これらのことを勘案し、本項では、通信回線を介して提供するアプリケーションに関する対策基準を定める。

遵守事項

(1) アプリケーションの導入時

【基本遵守事項】

(a) 部局技術責任者は、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規定を整備すること。

解説：通信回線を介して提供するサービスに関するセキュリティ維持のための対策について定めることを求める事項である。

「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規定」とは、例えば、サービスを利用する者及び電子計算機の主体認証、アクセス制御、権限管理及び証跡管理の手順等である。

(2) アプリケーションの運用時

【基本遵守事項】

(a) 部局技術担当者は、サービスのセキュリティ維持に関して整備した規定に基づいて、日常的及び定期的に運用管理を実施すること。

解説：整備された規定に従った運用管理を行い、担当者による個別判断で運用管理を実施しないことを求める事項である。

(b) 教職員等は、通信回線を介して提供されるサービスを私的な目的のために利用しないこと。

解説：教職員等に対して私的な目的でのサービス利用を禁止する事項である。

5.3.2 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教職員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を定める。

遵守事項

(1) 電子メールの導入時

【基本遵守事項】

(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。

【強化遵守事項】

(b) 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必要に応じ、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送受信時における教職員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主体認証を行うことを定めた事項である。

(2) 電子メールの運用時

【基本遵守事項】

(a) 教職員等は、業務遂行にかかわる情報を含む電子メールを送受信する場合には、本学が運営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：教職員等以外の者が提供する電子メールサービスを、業務遂行にかかわ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」が含まれているところであり、特に自動転送については当該電子メールに含まれる情報の格付け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背反しないようにも留意する必要がある。

(b) 教職員等は、受信した電子メールを電子メールクライアントにおいてテキストとして表示すること。

解説：HTML メールの表示により、偽のホームページ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及び不正なスクリプトが実行されること等を防ぐことを定めた事項である。
なお、「テキスト」には、リッチテキストが含まれる。また、本項は、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。しかしながら、ウェブメールにおいても、同様の脅威が想定されることから、テキスト表示の設定が不可能なウェブメールは利用しないことが望ましい。

5.3.3 ウェブ

趣旨（必要性）

ウェブにおいては、様々なアプリケーション、データを組み合わせた情報を送受信すること、また IP ネットワークにおいて標準的に利用されるシステムとして一般的に普及していること等の理由により、セキュリティ脅威全般に係るリスクが考えられる。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施すことが必要である。

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を定める。

遵守事項

(1) ウェブの導入時

【基本遵守事項】

(a) 部局技術責任者は、ウェブサーバを用いて提供するサービスが利用者からの文字列等の入力を受ける場合には、特殊文字の無害化を実施すること。

解説：特殊文字を無害化することを求める事項である。

特殊文字は不正侵入等の攻撃に用いられるため、すべての入力されるデータに対して特殊文字列が含まれていないかを確認する必要がある。

(b) 部局技術責任者は、ウェブサーバからウェブクライアントに攻撃の糸口になり得る情報を送信しないように情報システムを構築すること。

解説：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、攻撃を試みる者に攻撃の糸口に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、不必要な情報を送信しないことを求める事項である。

(c) 部局技術責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバを用いて提供するサービスにおいて、通信の盗聴から保護すべき情報を特定し、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：通信時に盗聴により第三者へ漏えいすることを防止するための事項である。

「通信の盗聴から保護すべき情報」とは、例えば、ウェブで提供するサービスの運営に関わる要機密情報を指し、サービスの利用者から受け取る個人情報等も含む。

【強化遵守事項】

(d) **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必要に応じ、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。
あらかじめすべての利用者が利用等することが想定されているデータを除き、特定の利用者のみが利用等するデータ等を、ウェブサーバに保存しないことが必要である。

(e) **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必要に応じ、部局技術責任者は、ウェブサーバの正当性を保証するために電子証明書を利用すること。**

解説：電子証明書による検証により、利用者がウェブサーバの正当性を確認できるようにウェブサーバを構築することを求める事項である。

(2) ウェブの運用時

【基本遵守事項】

(a) **教職員等は、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：ダウンロードするソフトウェアを電子署名により配布元を確認したソフトウェアに限定することを求める事項である。

【強化遵守事項】

(b) **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必要に応じ、部局技術責任者は、教職員等が閲覧することが可能な学外のホームページを制限し、定期的にその見直しを行うこと。**

解説：ウェブで閲覧したホームページからの不適切なソフトウェアのダウンロードや私的なホームページ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。

5.4 通信回線

5.4.1 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を定める。

遵守事項

(1) 通信回線の構築時

【基本遵守事項】

(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。例えば、部局技術責任者は、リスクを検討した結果、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。

(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。通信回線の負荷に関して事前にテスト等を実施し、必要となる容量及び能力を想定し、それを備える。また、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、通信回線及び通信回線装置関連文書を整備すること。

解説：通信回線及び通信回線装置と関連文書の整合性を確保するための事項である。「通信回線及び通信回線装置関連文書」とは、通信回線の設計書、仕様書、通信回線の構成図、電子計算機の識別コード及び通信回線装置の設定が記載された文書等が挙げられる。書面ではなく電磁的記録媒体で整備していても差し支えない。

(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、管理部署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すべて確認した上で、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、通信回線を用いて送受信され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：通信回線を用いて送受信され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、当該情報の暗号化の必要性を検討する必要がある。

(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、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。

(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、通信回線装置に存在する公開されたセキュリティホールから通信回線装置を保護するための対策を講ずること。

解説：セキュリティホール対策を行うことで、通信回線装置をセキュリティが確保された最新の状態にするための事項である。対策には、パッチ適用だけでなく、設定等での回避も含まれる。

(j) 部局技術責任者は、通信回線装置を安全区域に設置すること。

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。

(k) 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、契約を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。

(l) 部局技術責任者は、通信回線装置上で証跡管理を行う必要性を検討し、必要と認めた場合には実施すること。

解説：通信回線装置上で取得可能な証跡について、証跡管理を行うための事項である。管理として、取得する情報項目の設定、証跡の保存及び点検、分析並びに報告等が挙げられる。

【強化遵守事項】

(m) 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必要に応じ、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。

(n) 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必要に応じ、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こと。

解説：障害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。災害等を想定して冗長構成にする場合には、被災時にも冗長構成のうち少なくとも一系統が存続可能な構成にすることが望ましい。

(2) 通信回線の運用時

【基本遵守事項】

(a) 部局技術担当者は、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の対応、及び通信回線の利用部局を含む事項の管理を行うこと。

解説：通信回線の運用管理を行うことを求める事項である。部局技術担当者は、通信回線を利用する電子計算機の識別コード及び電子計算機を利用する者と当該利用者の識別コードの対応並びに通信回線の利用部局を含む事

項の管理を行う必要がある。

(b) **部局技術担当者は、通信回線の構成、通信回線装置の設定、アクセス制御の設定又は識別コードを含む事項を変更した場合には、当該変更の内容を通信回線及び通信回線装置関連文書へ反映すること。また、当該変更の記録を保存すること。**

解説：部局技術担当者が行った変更を適宜関連文書に反映することで、通信回線及び通信回線装置と関連文書の整合性を確保するための事項である。

(c) **部局技術責任者は、定期的に通信回線の構成、通信回線装置の設定、アクセス制御の設定又は識別コードを含む事項の変更を確認すること。また、当該変更によって生ずる通信回線のセキュリティへの影響を特定し、対応すること。**

解説：通信回線の構成の不正な変更を定期的に確認し、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応することを求める事項である。

(d) **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ときに、他の情報システムを保護するための事項である。

(e) **教職員等は、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。

(f) **部局技術責任者は、通信回線装置のセキュリティレベル維持のため、公開されたセキュリティホールから通信回線装置を保護するための対策を講ずること。**

解説：通信回線及び通信回線装置の運用中に公開されたセキュリティホールに対応することにより、電子計算機のセキュリティレベルを維持するための事項である。対策を検討する初期の段階では、「直接解決する対策方法がないため代替案を実施する」、「リスクが大きくないので対策しない」といった計画で差し支えない。その判断は各組織に委ねられる。

(g) **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構築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。

(3) 通信回線の運用終了時

【基本遵守事項】

(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、通信回線装置の内蔵記録媒体のすべての情報を復元が困難な状態にすること。

解説：運用を終了した通信回線装置が再利用又は廃棄された後、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、情報の消去を求める事項である。

消去の方法としては、通信回線装置の初期化、内蔵記録媒体の物理的な破壊等の方法がある。

5.4.2 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を定める。

遵守事項

(1) 学内通信回線の構築時

【強化遵守事項】

(a) 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必要に応じ、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ための措置を講ずること。

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

【強化遵守事項】

(a) 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必要に応じ、部局技術責任者は、通信要件の変更に際し及び定期的に、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) **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必要に応じ、部局技術責任者は、定期的に、通信回線及び通信回線装置のセキュリティホールを検査すること。**

解説：定期的なセキュリティホール検査の実施を求める事項である。「定期的」とは、１か月から３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。これによって、セキュリティレベルの低下、対策漏れ、アクセス制御の設定ミスがないかを確認する必要がある。

(c) **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必要に応じ、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) **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必要に応じ、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。

(3) 回線の対策

【基本遵守事項】

(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、SoftEther 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。
(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 接続方法の機密性の確保
(ク)無線 LAN に接続する電子計算機の管理
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。

(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。

5.4.3 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
【基本遵守事項】

(a) 部局技術責任者は、部局総括責任者の承認を得た上で、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承認の可否を判断する必要がある。

(b) 部局総括責任者は、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。独立な通信回線の場合でも、遵守すべき対策規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

【基本遵守事項】

(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ときに、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、通信回線の変更に際し及び定期的に、アクセス制御の設定の見直し行うこと。

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) 部局技術責任者は、定期的に、学外通信回線から通信することが可能な学内通信回線及び通信回線装置のセキュリティホールを検査すること。

解説：定期的なセキュリティホール検査の実施を求める事項である。これによって、セキュリティレベルの低下、対策漏れ、アクセス制御の設定ミスがないかを確認する必要がある。

(d) 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。

(e) 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６部　個別事項についての対策

6.1　調達・開発にかかわる情報セキュリティ対策

6.1.1 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情報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情報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明確にする必要がある。

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)　学内における情報セキュリティ確保の仕組みの整備

【基本遵守事項】

(a) 全学実施責任者は、機器等の選定基準及び機器等が具備すべき要件を整備し、適時見直すこと。

解説：機器等の選定に先立って整備すべき基準や具備すべき要件に関する事項を定めたものである。

全学実施責任者は、機器等の選定基準や要件の整備に当たっては、機器等が本学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、機器等が本学基準の該当項目を満たし、本学のセキュリティレベルを一定水準以上に保つために、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、選定基準や要件は、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、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。

確認・検査手続としては、必要なセキュリティ機能の実装の確認（機器等に最新のパッチが適用されているかどうか、ウイルス対策ソフトウェアが最新の脆弱性に対応しているかどうか等にも留意）を、購入先から

の報告で確認すること等が挙げられる。

(2) 機器等の購入の実施における手続の遵守

【基本遵守事項】

(a) 部局技術責任者は、機器等の選定時において、選定基準及び具備すべき要件に対する機器等の適合性を確認し、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及び具備すべき要件に従って、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、納入された機器等が選定基準及び具備すべき要件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こと。

解説：納入された機器等が選定基準及び具備すべき要件を満たすことを確認・検査することを求める事項である。

(c) 部局技術責任者は、機器等の納入後の情報セキュリティ対策に関する保守・点検等の必要性の有無を検討し、必要と認めた場合には、実施条件を明確にし、それらの実施者である機器等の購入先又は他の事業者との間で、その内容に関する契約を取り交わすこと。

解説：機器等の購入先又は他の事業者との間で、納入後の情報セキュリティに関する保守・点検等の実施者及び実施条件を明確にし、その内容を文書で取り交わす必要性を定めた事項である。なお、機器等の購入先以外の事業者が保守・点検等を行う場合の手続については 6.1.2 外部委託によるものとなる。

(d) 部局技術責任者は、機器等の購入において、満足すべきセキュリティ要件があり、それを実現するためのセキュリティ機能の要求仕様がある場合であって、総合評価落札方式により購入を行う場合には、これについて、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。

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、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ものを優遇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、より信頼度の高い情報システムが構築できる。

6.1.2 外部委託

趣旨（必要性）

教職員等以外の者に情報処理業務を委託する場合には、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明確にする必要がある。

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。

適用範囲

本項は、会計法第 29 条に規定する貸借、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、例えば次に掲げるものに適用する。

- 統計、集計、データエントリー、媒体変換を含む情報の加工・処理
- 情報システムの構築（ソフトウェア開発、運用、ASP サービス、保守、改修等含む。）
- その他調査・研究
- 物品等の賃貸借（機器増設、保守、レンタルサーバ、ハウジング等含む）

遵守事項

(1) 学内における情報セキュリティ確保の仕組みの整備

【基本遵守事項】

(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。

(b) 全学実施責任者は、委託先の選定手続、選定基準及び委託先が具備すべき要件（委託先職員に対する情報セキュリティ対策の実施を含む。）を整備すること。

解説：委託先の選定において整備すべき基準や要件に関して定めた事項である。

全学実施責任者は、委託先の選定基準や要件の整備に当たっては、当該委託先が、事業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、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確立すること、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、本学のセキュリティレベルを一定水準以上に保つために、委託先職員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、本基準や要件は、法制度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。

【強化遵守事項】

(c) 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必要に応じ、全学実施責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法を整備すること。

解説：委託先の候補者の情報セキュリティ水準を確認するための評価方法を整備することを求める事項である。

評価方法の整備には、ISO/IEC 17799 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セルフチェックベースのツール等の応用が考えられる。

(d) 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必要に応じ、全学実施責任者は、前事項の評価方法に従って、求める情報セキュリティ要件に対する委託先の候補者の情報セキュリティ水準を確認し、委託先の選定基準の一要素として利用すること。

解説：前事項の評価方法に従って委託先候補者のセキュリティ水準を確認し、これを委託先の選定基準の一要素として利用することを求める事項である。

(2) 委託先に適用する情報セキュリティ対策の整備

【基本遵守事項】

(a) 部局技術責任者は、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整備し、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の整備に関して定めた事項である。

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整備及び周知しておくことが重要である。

(b) 部局技術責任者は、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手順を整備し、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侵害発生時の対処手順を本学として整備することを定めた事項である。請負内容における情報セキュリティ侵害の影響度の大きさや可用性に対する要求度に応じて、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評価基準を策定し、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手順に関して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履行が不十分である場合に対する措置に関し、対象となる情報システムや業務に応じて決定、事前通知すべき事項を定めたものである。

また、部局技術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) 外部委託先の選定における手続の遵守

【基本遵守事項】

(a) **部局技術責任者は、整備されている選定手続、選定基準及び委託先が具備すべき要件に基づき、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。

(4) 外部委託の実施における手続の遵守

【基本遵守事項】

(a) **部局技術責任者は、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。）、情報セキュリティ侵害発生時の対処手順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手順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、以下の事項を含めること。**

(ア)情報セキュリティ監査を受け入れること。

(イ)提供されるサービスレベルに関して委託先に保証させること。

解説：外部委託を実施する際の手続の遵守に関して定めた事項である。

機密の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。

委託先への監査の実施に際しては、提出させる各種ログの監査レベルや提出範囲等を決定し、事前に合意しておくことが重要である。また、当該業務の重要度により、立入監査の実施、重点項目のみ立入監査、委託先による内部監査報告の監査等を適切に選択することが必要である。

委託先から提供を受け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手順、事故発生時の対応手順等を決定し、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。

(b) **部局技術責任者は、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に含めること。**

(ア)遵守すべき情報セキュリティ対策を実現するために、委託先における所属職員が実施する具体的な取組内容

(イ)外部委託した業務の作業に携わる者の特定とそれ以外の者による作業の禁止

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の入手に関し定めた事項である。

特に、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。

また、開発委託の終了後の運用におけるセキュリティパッチの適用等、情報セキュリティの維持に関する責任の所在に関しては、外部委託の実施時に明確化しておく必要がある。

(c) 部局技術責任者は、外部委託契約の継続に関しては、選定手続、選定基準及び委託先が具備すべき要件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、都度審査することの重要性を定めた事項である。

また、部局技術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) 部局技術責任者は、委託先の提供するサービス（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、選定手続、選定基準及び委託先が具備すべき要件に基づき、その是非を審査すること。

解説：委託契約の実施中及び変更時における委託先のサービス変更の管理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) 部局技術責任者は、委託先がその請負内容の全部又は一部を第三者に再請負させることを禁止すること。ただし、委託先からの申請を受け、再請負させ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が担保されると部局総括責任者が判断する場合は、その限りではない。

解説：請負内容に関する第三者への再請負の原則禁止を定めた事項である。

一般的に、委託先が多階層化されるとセキュリティレベルが下がることが懸念されるため、再請負をするべきではない。ただし、委託先から申請を受け、再請負を行うことが合理的であると認められる場合には、再請負させ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が担保されることを条件に再請負を認めるものとする。情報セキュリティを十分に確保するためには、委託先を選定する場合と同一観点から再請負先が委託契約の内容を遵守できる者であることを部局総括責任者が確認し、再請負先に行わせる内容に応じて、委託先自体が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実施させることを契約等に盛り込むよう委託先に求めることが必要である。

部局技術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。

(f) 教職員等は、委託先に提供する情報を必要最低限とし、委託先が要機密情報を取り扱う場合、以下の実施手順に従うこと。

(ア) 委託先に情報を移送する場合は、不要部分のマスキングや暗号化等安全な受渡方法により実施し、移送した記録を保存すること。

(イ) 外部委託の業務終了等により情報が不要になった場合には、確実に返却させ、又は廃棄させること。

解説：委託契約開始から終了に至るまでの当事者間での情報の授受に関する実施手順遵守の徹底に関して定めた事項である。委託先の選定基準や情報セキュリティ侵害時の対処手順等の仕組みを整備した上で、当事者間の情報の授受において実施手順に従うことによりセキュリティレベルを確保することが重要である。

(5) 外部委託終了時の手続の遵守

【基本遵守事項】

(a) 部局技術責任者は、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。

「納品検査」とは、会計法第 29 条の 11 第 2 項に規定されている「その受ける給付の完了の確認をするため必要な検査」のことであり、本項の適用範囲すべてを対象とする。

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。

6.1.3 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（設計及びコーディング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を定める。

遵守事項

(1) ソフトウェア開発体制の確立時

【基本遵守事項】

(a) **部局技術責任者は、ソフトウェア開発について、セキュリティにかかわる対策事項（本項(2)から(5)の遵守事項）を満たすことが可能な開発体制の確保を、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開発体制（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開発・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、ソフトウェア開発を外部委託する場合には、委託先が実施すべき対策事項（本項(2)から(5)の遵守事項）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かかわる要件を選択し、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。

(2) ソフトウェア開発の開始時

【基本遵守事項】

(a) **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かかわ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、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、「環境」とは、例えば、ドキュメント、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、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。

(b) 部局技術責任者は、ソフトウェアの開発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開発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。

(3) ソフトウェアの設計時

【基本遵守事項】

(a) 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、及び当該ソフトウェアにおいて取り扱う情報の格付けに応じて、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開発する場合はもとより、すべ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、不正侵入、DoS 攻撃、なりすまし等の脅威を分析する必要がある。

(b) 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かかわる機能、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。

(c) 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。

(d) 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 タグやスクリプトなど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など、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。

(e) 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・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・ST 確認を受ける場合、又はソフトウェアを更改する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・ST 確認を行うことを求める事項である。

「ST 評価・ST 確認を受けること」とは、ST 評価・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・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開発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・ST 確認を受けさせることになる。

(4) ソフトウェアの作成時

【基本遵守事項】

(a) 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及びバックアップの取得を行うこと。

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。

(b) 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。

【強化遵守事項】

(c) 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必要に応じ、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、市中製品を組み込む場合など、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。

(5) ソフトウェアの試験時

【基本遵守事項】

(a) 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、統合試験など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。

(b) 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の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。

6.2 個別事項

6.2.1 学外での情報処理の制限

趣旨（必要性）

職務においては、その事務の遂行のため、学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、学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、教職員等は、学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、学外での情報処理の制限に関する対策基準を定める。

遵守事項

(1) 安全管理措置の整備

【基本遵守事項】

(a) 全学実施責任者は、要保護情報について学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、学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。学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、関与する学内及び学外の者等に応じて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学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、学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

【基本遵守事項】

(a) 教職員等は、要保護情報（機密性２情報を除く。）について学外で情報処理を行う場合には、部局技術責任者又は職場情報セキュリティ責任者の許可を得ること。

解説：要保護情報（機密性２情報を除く。）に係る情報処理を学外で行う場合に、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を求める事項である。情報システムに係る事項は部局技術責任者の、情報に係る事項は職場情報セキュリティ責任者の許可を得ることとなる。

(b) 教職員等は、機密性２情報について学外で情報処理を行う場合には、部局技術責任者又は職場情報セキュリティ責任者に届け出ること。

解説：学外で機密性２情報の情報処理を行う場合に、部局技術責任者又は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。

(c) 部局技術責任者及び職場情報セキュリティ責任者は、学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：学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、要保護情報（機密性２情報を除く。）について学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、対応を講ずること。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：学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、対応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、教職員等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情報について学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、対応を講ずること。

解説：機密性２情報について学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教職員等に改めて届出をさせる等の対応を講ずることを求める事項である。

(f) 教職員等は、要保護情報について学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：情報セキュリティ侵害のおそれを低減するために、要保護情報を学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) 教職員等は、要保護情報（機密性２情報を除く。）を取り扱う情報システムを学外に持ち出す場合には、部局技術責任者又は職場情報セキュリティ責任者の許可を得ること。

解説：要保護情報（機密性２情報を除く。）を学外に持ち出す教職員等に、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を求める事項である。情報システムに係る事項は部局技術責任者の、情報に係る事項は職場情報セキュリティ責任者の許可を得ることとなる。

(h) 教職員等は、機密性２情報を取り扱う情報システムを学外に持ち出す場合には、部局技術責任者又は職場情報セキュリティ責任者に届け出ること。

解説：機密性２情報を学外に持ち出す教職員等に、部局技術責任者又は職場情

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。

(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学外への持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学外への持出しに係る記録を取得し、保存することを求める事項である。

「持出しに係る記録」には、持出しの実施者、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、要保護情報（機密性２情報を除く。）を取り扱う情報システムを学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、対応を講ずること。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：情報システムを学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、教職員等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情報を取り扱う情報システムを学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、対応を講ずること。

解説：届出期間が長期にわたるなど、必要に応じて、学外への持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、教職員等に改めて届出をさせること。

(l) 教職員等は、要保護情報を取り扱う情報システムを学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出しにとどめること。

解説：情報セキュリティ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学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

【基本遵守事項】

(a) 教職員等は、要保護情報について学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：教職員等に対して、学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) 教職員等は、要保護情報（機密性２情報を除く。）について学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：教職員等に対して、学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) 教職員等は、要保護情報を取り扱う情報システムの学外への持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：教職員等に対して、情報システムの学外への持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ァイ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) 教職員等は、要保護情報（機密性２情報を除く。）を取り扱う情報システムを学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：教職員等に対して、学外へ情報システムの持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。

6.2.2 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）

職務においては、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を定める。

遵守事項

(1) 安全管理措置の整備

【基本遵守事項】

(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：教職員等が所有する個人の PC など、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情報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。

(2) 許可及び届出の取得及び管理

【基本遵守事項】

(a) 教職員等は、要保護情報（機密性２情報を除く。）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、部局技術責任者又は職場情報セキュリティ責任者の許可を得ること。

解説：要保護情報（機密性２情報を除く。）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、許可を得ることを求める事項である。情報システムに係る事項は部局技術責任者の、情報に係る事項は職場情報セキュリティ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要保護情報（機密性２情報を除く。）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、教職員等に改めて許可を得るようにさせること。

(b) 教職員等は、機密性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、部局技術責任者又は職場情報セキュリティ責任者に届け出ること。

解説：本学支給以外の情報システムによる機密性２情報の情報処理を行う場合に、部局技術責任者又は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。

(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し、保存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、要保護情報（機密性２情報を除く。）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、対応を講ずること。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、教職員等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、対応を講ずること。

解説：届出期間が長期にわたる場合など、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、教職員等に改め

て届出をさせること。

(3) 安全管理措置の遵守

【基本遵守事項】

(a) 教職員等は、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、原則として、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：**教職員等**が所有する個人の PC など、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情報セキュリティ対策を施す必要があるため、**教職員等**に安全管理措置を講ずることを求める事項である。

(b) 教職員等は、要保護情報（機密性２情報を除く。）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：教職員等が要保護情報（機密性２情報を除く。）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。

6.3 その他

6.3.1 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を定める。

遵守事項

(1) 措置の整備

【基本遵守事項】

(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) 措置の遵守

【基本遵守事項】

(a) 教職員等は、原則として、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。教職員等は、組織及び個人として措置を講ずることが重要である。

6.3.2 業務継続計画(BCP)との整合的運用の確保

趣旨（必要性）

本学においては、事業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、当該事態への対応計画を業務継続計画（BCP：Business Continuity Plan）として策定することが考えられる。他方では、BCP 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採られることとなる。この場合､BCP 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、BCP と情報セキュリティ対策の整合的運用の確保に関する対策基準を定める。

遵守事項

(1) 本学における BCP 整備計画の把握

【基本遵守事項】

(a) 全学総括責任者は､本学における BCP の整備計画について全学実施責任者を通じ全学情報システム運用委員会が適時に知ることができる体制を構築すること。

解説：全学総括責任者が、本学が整備する BCP の内容や状況について、全学情報システム運用委員会が適時に情報を入手できるような体制を構築することを求める事項である。

BCP に変更がある場合などにも、必要な情報が継続的に得られるようにしなければならない。

(b) 全学実施責任者は、本学において BCP の整備計画を把握した場合は、その内容を全学情報システム運用委員会並びに必要に応じて部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者に連絡すること。

解説：全学情報システム運用委員会並びに必要に応じて部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者が本学における BCP の整備計画を知ることができるために、全学実施責任者に対して、把握した BCP 整備計画の内容を連絡することを求める事項である。

BCP に変更がある場合にも、当該連絡を行わなければならない。

(2) BCP と情報セキュリティ対策の整合性の確保

【基本遵守事項】

(a) 全学情報システム運用委員会は、本学において BCP 又は本基準の整備計画がある場合には、BCP と本基準との整合性の確保のための検討を行うこと。

解説：BCP と本基準は、特定の事態に対して、それぞれの体系において定められることがあり得る。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 BCP 及び本基準のそれぞれで定める対策に矛盾があると、双方の遵守を求められる本学組織及び職員は、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、BCP と本基準の間であらかじめ整合性を確保するよう検討を行うことが必要である。

例えば、全学情報システム運用委員会は、「情報の格付け及び取扱制限の基準」の整備について、本基準の 3.1.1 項で求められている。その整備の際に、本学が BCP 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、BCP の整備計画を担当する者と協議し双方の定めを調整する必要がある。また、BCP 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、その変更が当該基準に影響するかどうかを確認し、必要があれば、当該基準の改訂を行うなどして、BCP との整合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 BCP の整備計画がある場合には、すべての情報システムについて、当該 BCP との関係の有無を検討すること。

解説：BCP と情報セキュリティ関係規程と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、BCP 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 BCP の整備計画がある場合には、当該 BCP と関係があると認めた情報システムについて、以下に従って、BCP と本基準に基づく共通の実施手順を整備すること。

(ア) 通常時において BCP と本基準の共通要素を整合的に運用するため、情報セキュリティの枠内で必要な見直しを行うこと。

(イ) 事態発生時において BCP と本基準の実施に障害となる可能性のある情報セキュリティ対策の遵守事項の有無を把握し、整合的運用が可能となるよう事態発生時の規定の整備を行うこと。

解説：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に、BCP と自らが担当する実施手順の整合性の確保を求める事項である。

整合性を確保するための対応には、通常時の運用において実施するものと、事態発生時に実施するものがある。事態発生への対応として、BCP 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策を実施手順において具体的に定める等が想定される。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要員計画も整備対象となり得る。

これらの目標及び対策を BCP 及び情報セキュリティ関係規程の双方で定めることとなるため、相互の整合性を確保するための規定の整備が必要となる。

(3) BCP と情報セキュリティ関係規程の不整合の報告

【基本遵守事項】

(a) 教職員等は、本学において BCP の整備計画がある場合には、BCP と情報セキュリティ関係規程が定める要求事項との違いなどにより、実施の是非の判断が困難な場合には、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、BCP と情報セキュリティ関係規程が定める要求事項との整合性については、上記(1)及び(2)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、BCP 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。BCP 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。

A3103 インシデント対応手順

解説：災害等によるネットワーク設備の損壊、利用者等による規定違反や学外から学内への攻撃行為等により発生したインシデントへの対応については、あらかじめ実施要領や対応マニュアルに具体的な手順を明記しておかなければならない。各高等教育機関においては、それぞれの実情に即して対応手順を個別に定めることになるだろう。具体的な対応については、以下のとおり物理的インシデント・セキュリティインシデント・コンテンツインシデントとで分けて考えるべきである。また、部局内の対応と全学の対応の分担と当事者の権限を明確にし、迅速な対処と、慎重な検討とを両立させることが必要である。なお、ネットワークをめぐる問題は多種多様であり、すべての対応を網羅的に定めることは難しいかもしれない。ポリシーの見直しが行われる際は、規定違反行為等への対応についても、実際の運用経験を反映させた見直しが行われるべきである。

１ 定義

(1) 物理的インシデント

地震等の天災、火災、事故、盗難等によるネットワークを構成する機器や回線の物理的損壊や滅失及びその他の物理的原因による情報システムやネットワークの機能不全や障害等、情報セキュリティの確保が困難な事由の発生およびそのおそれを言う。

(2) セキュリティインシデント

ネットワークや情報システムの稼動を妨害し、またはデータの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

(3) コンテンツインシデント

ネットワークを利用した情報発信内容（以下「コンテンツ」という）が著作権侵害等の他人の権利侵害や児童ポルノ画像の公開等の違法行為または公序良俗違反である行為(及びその旨主張する被害者等からの請求）による事故を言い、下記原因を含む。

－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

(4) インシデント

物理的インシデント、セキュリティインシデントまたはコンテンツインシデントを言う。

(5) 対外的インシデント

インシデントのうち、利用者等による行為であって、外部ネットワークにおけるあるいは外部のシステムに対して行われた行為による事故、事件を言う。

(6) 対内的インシデント

インシデントのうち、外部のネットワークから内部に向かって行われた行為による事故、事件を言う。

(7) 学外クレーム

学内の利用者等による情報発信行為（本学の業務としてなされたものを除く）の問題を指摘しての連絡・通報及び学外(学内の者が、弁護士等の代理人を立てる場合も含む)からの発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び証拠、証言の収集や犯罪捜査等にかかわる協力要請や強制的命令を言う。

(8) 対外クレーム

対内的インシデントに対し、学外の発信者に対して連絡・通報し、または発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び当局に犯罪捜査の告訴・告発をすることを言う。

(9) 運用･管理規程

A2101　A 大学情報システム運用・管理規程とそれにもとづく手順、命令、計画等を言う。

(10) 緊急連絡網

運用・管理規程に基づき整備された［インシデント/障害等]に備え、特に重要と認めた情報システムについて、その部局技術責任者及び部局技術担当者の緊急連絡先、連絡手段、連絡内容を含む連絡網を言う。

(11) 学外窓口

障害等について学外から連絡・通報を受け、学外への連絡・通報、対外クレームをするための窓口を言う。

(12) 利用規定

A2201 大学情報システム利用規程とそれにもとづく手順、その他本学の情報ネットワークや情報システムの利用上のルールを言う。

(13) 利用規定違反行為

インシデントに係わるかどうかに限らず、利用規程に違反する行為を言い、下記を含む。

１　情報システム及び情報について定められた目的以外の利用
２　電子掲示板、ブログやウェブページ等での名誉・信用毀損にあたる情報の発信

３　差別、侮辱、ハラスメントにあたる情報の発信
４　他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信
５　守秘義務に違反する情報の発信
６　他人の著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信
７　通信の秘密を侵害する行為
８　営業ないし商業を目的とした本学情報システムの利用
９　部局総括責任者の許可（業務上の正当事由）なくネットワーク上の通信を監視し、又は情報機器の利用情報を取得する行為
１０　不正アクセス禁止法に定められたアクセス制御を免れる行為及びそれを助長する行為
１１　部局総括責任者の要請に基づかずに管理権限のないシステムのセキュリティ上の脆弱性を検知する行為
１２　サービス不能攻撃等、故意に過度な負荷を情報システムに与えることにより本学の円滑な情報システムの運用を妨げる行為
１３　その他法令に基づく処罰の対象となり、又は損害賠償等の民事責任を発生させる情報の発信
１４　上記の行為を助長する行為
１５　管理者の許可をえず、ソフトウェアのインストールやコンピュータの設定の変更を行う行為

解説：規定違反行為の内容とその対処方針は、明確に規定されている必要がある。何が規定違反に該当するかを明確にし、利用者等の予見性を高めることによりネットワークの適切な利用が促進されるからである。

２ インシデント通報窓口

(1) インシデント対応のための学外・学内の連絡・通報窓口は下記のとおりとする。
A.　学内窓口：メデイアセンター
B.　学外窓口：メデイアセンター／広報部門

(2) 学外窓口への学外からの e-mail による連絡手段は、[緊急連絡網参加者全員が受信可能とする]以下のメーリングリストとし、公表するものとする。
Email: abuse@a-univ.ac.jp

(3) 学外への連絡・通報、対外クレームに当たっては、本学[広報部門]との連絡を密にし、無断で行わないものとする。

解説：問題発生時の対処を迅速・確実に行うためネットワーク運用と利用の問題についての学外・学内の連絡・通報窓口を設定しておくことが必要である。

連絡窓口は部署別あるいは機能別に複数設置してもよいが、問題の切り分けが効率的にできるならば、一箇所に集中して設け、関連部門の技術責任者や部局技術担当者等、学内への連絡網を整備し情報を配布することでも対応できよう。対外的連絡・通報については、全学広報部門との役割分担を明確にし、情報共有と意思疎通を密接にする必要がある。

メーリングリストのアドレスあるいは自動転送をして関係者で同時に情報共

有をすることなども考えられるが、いずれにしても一次対応する責任者を明確にしておく必要がある。

特に、利用者等により違法行為がなされたおそれがあるとする被害者との対応や関連する捜査や取材の対応については、慎重にする必要がある。

3 インシデントの対応判断のエスカレーション手順

(1) メディアセンター／広報部門は、インシデントを発見し、または、学外クレームによりインシデントを認知した場合は、緊急連絡網その他所定の連絡網により、適宜、全学総括責任者、全学実施責任者、部局総括責任者、部局技術責任者、部局技術担当者にインシデントの初期対応を連絡するものとする。

(2) メディアセンターは、全学ネットワークに関るインシデントについては、必要に応じて自ら技術的対応をするものとし、部局ネットワークにのみ関連するインシデントについては、部局技術責任者を支援するものとする。

(3) 部局技術担当者は、インシデントを発見し、またはメディアセンター等を通じて内部・外部からの通報を受けることにより認知した場合、ただちに部局技術責任者に状況報告するものとする。

(4) 部局技術責任者は、インシデントを自ら認知するか部局技術担当者から状況報告を受けた場合、下記の基準により一次切り分け判断を行うものとする。

① 部局内ネットワークに閉じた技術的問題か

1. 物理的インシデントまたはセキュリティインシデントの場合で、対外的インシデントでも体内的インシデントでも無く、部局内ネットワークにのみ影響が生じている場合、部局技術担当者に対策を指示し、対策結果を部局総括責任者に状況報告する。
2. １.以外の場合、部局総括責任者を通じて全学実施責任者に状況報告をし、メディアセンターの支援を仰ぎながら、物理的インシデントまたはセキュリティインシデント対応のプロセスを実施する。

② コンテンツインシデントか

1. コンテンツインシデントの場合、加害者と被害者が部局内に閉じている場合であっても、法律的対策を講じる必要があるため、原則として部局総括責任者を通じて全学総括責任者に報告をし、メディアセンターの支援を仰ぎながら、ログの保全等、必要な技術的措置を取るものとする。
2. ただし、爆破予告・自殺予告など、生命・身体への危険等の緊急性がある場合で、部局内での対処が可能な場合は、コンテンツに関する緊急対応を実施の上、部局総括責任者と全学実施責任者に結果報告をする。

(5) 部局技術責任者は、あらかじめ定められた手順に従って、緊急な技術的対応が必要なときは部局技術担当者に指示を与え、部局総括責任者に対応結果を報告する。法的に慎重な判断を要する場合は、対応を実施する前に必ず部局総括責任者に報告し、指示を受けることとする。

(6) 部局技術責任者から報告を受けた部局総括責任者は、コンテンツインシデントについて、部局技術責任者・部局技術担当者を指揮監督する。セキュリティインシデント対応につい

ては、ポリシーに基づいて全学総括責任者に指示や承認を求める。また、法的判断を要する問題のうち、通報者への内容確認や定型回答文書の発信等、部局技術責任者や学外窓口に対して一定の一時的対応を指示または依頼する。

(7) 学外クレームか、対外クレームか

① 全学実施責任者は、学外クレームにより認知したインシデントの場合、学外クレーム対応プロセスを併せて実施する。

② 全学実施責任者は、法律専門家に相談しながら、必要に応じて対外クレームを実施するものとする。

③ 学内問題として処理可能であるインシデントは、通常の技術的対応または利用規定違反対応とする。

解説：インシデントについて、部局技術責任者が発見あるいは通報によって認知した場合の対応手順は、あらかじめ管理者向けマニュアルに明示しておかなければならない。

インシデントと影響範囲による役割・責任分担例

インシデントと影響範囲による責任分担

インシデント分類	物理／セキュリティ		コンテンツ	
影響範囲	対外・全学	部局	対外・全学	部局
全学総括責任者（非常時対策本部）	◎▲	----------	◎▲	◎（定形以外）
メディアセンター（非常時窓口）	○	○	○	○（定形以外）
部局総括責任者		◎		○(定形のみ◎)
部局技術責任者	△	▲（定形のみ◎）	△	△（定形のみ▲）
部局技術担当者	△	△	△	△

◎インシデント総括　○判断・技術支援　▲技術対応判断　△技術対応実施

コンテンツインシデントについては、慎重な法的判断を要することが多く、また通信の秘密あるいはプライバシー保護の観点から、部局技術責任者と部局技術担当者が立ち入ることが適当でない場合が少なくないため、部局技術責任者がコンテンツインシデントと信じた場合は、部局総括責任者に一次判断を求めるものとする。一方、セキュリティインシデントに関する問題については、利用規定違反の判断が比較的容易であること、被害の拡大防止のために緊急の技術的対応が必要となる場合も少なくないことなどから、部局技術責任者と部局技術担当者の一次判断が重要となる。

4 物理的インシデント発生時の対応

(1) 発生から緊急措置決定まで

(ア) 通報・発見等で物理的インシデントの可能性を認知した部局技術担当者は、事実を確認するとともに部局技術責任者に報告し、被害拡大防止のための緊急措置の必要性について判断を求めるものとする。

(イ) 部局技術担当者は、後日の調査に備え、物理的インシデント発生時の状況に関する記録を作成し、ネットワーク運用に影響があるおそれがある場合、バックアップデータの作成、ハードディスクのイメージの保存等を行う。

(2) 被害拡大防止の緊急措置の実施

(ア) 部局技術責任者は、個別システムの停止やネットワークからの遮断、機器の交換、ネットワークの迂回等の緊急措置の必要性を判断し、実施を部局技術担当者に指示する。

(イ) 利用者等による対処が必要な場合には、その旨命令する。

(3) 緊急連絡及び報告

(ア) 部局技術責任者は、緊急の被害拡大防止措置を実施する場合は、部局総括責任者に報告する。

(イ) 部局総括責任者は、被害拡大防止措置が全学ネットワークに影響が及ぶと判断するときは学内窓口を通じて全学総括責任者に報告する。

(ウ) 全学総括責任者は学内窓口に指示して、緊急措置の実施により影響を受ける利用者等へ連絡するとともに、必要に応じ非常時対策本部を組織する。

(エ) 学外窓口は総括責任者または非常時対策本部の指示に基づき、関係するネットワークへの連絡、外部広報などを行う。

(オ) 非常時対策本部が設置された場合、部局総括責任者、部局技術責任者及び部局技術担当者は、その指示に従うものとする。

(4) 復旧計画

(ア) 部局技術担当者は、物理的インシデントによる被害や緊急措置の影響を特定し、システムやネットワークの復旧計画を立案する。

(イ) 部局技術責任者は、復旧計画を検討し、部局総括責任者の承認を得て実施する。

(5) 原因調査と再発防止策

(ア) 部局技術担当者は、物理的インシデント発生の要因を特定し、再発防止策を立案する。

(イ) 部局技術責任者は、利用者等への注意喚起等を含めた再発防止策を検討し、部局総括責任者は検討結果に基づき再発防止策を策定する。

(ウ) 部局技術担当者と部局技術責任者は、インシデント対応作業の結果をまとめ、部局総括責任者は、再発防止策とともに全学情報システム運用委員会に報告するとともに、必要によりポリシーや実施手順の改善提案を行う。

(エ) 全学総括責任者は、部局総括責任者から物理的インシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずる。

解説：セキュリティインシデント発生時の対応に準ずる一方、全学の災害等における非常時行動計画と整合性をとる必要がある。

５ セキュリティインシデント発生時の対応

(1) 発生から緊急措置決定まで

(ア) 監視システムによるセキュリティインシデントの可能性を示す事象の検知や、通報等でセキュリティインシデントの可能性を認知した部局技術担当者は、事実を確認するとともに部局技術責任者に報告し、被害拡大防止のための緊急措置の必要性について判断を求めるものとする。

(イ) 部局技術担当者は、後日の調査に備え、セキュリティインシデント発生時の状況、例えばログイン状況、ネットワーク接続や手順の稼働状況に関する記録を作成し、バックアップデータの作成、ハードディスクのイメージの保存等を行う。

(ウ) セキュリティインシデントが、外部からの継続している攻撃等であって攻撃元ネットワークの管理主体等への対処依頼が必要な場合、部局総括責任者の承認を得て部局技術責任者から相手方サイトへの対処依頼を行う。

⑵ 被害拡大防止の緊急措置の実施

(ア) 部局技術責任者は、個別システムの停止やネットワークからの遮断（他の情報システムと共有している学内通信回線又は学外通信回線から独立した閉鎖的な通信回線に構成を変更する等）等の緊急措置の必要性を判断し、実施を部局技術担当者に指示する。

(イ) 部局総括責任者および部局技術責任者は、情報システムのアカウントの不正使用の報告を受けた場合には、直ちに当該アカウントによる使用を停止させるものとする。

(ウ) 部局技術責任者は、利用者等による対処が必要な場合には、その旨命令する。

⑶ 緊急連絡及び報告

(ア) 部局技術責任者は、緊急の被害拡大防止措置を実施する場合は、部局総括責任者に報告する。

(イ) 部局総括責任者は、被害拡大防止措置が全学ネットワークに影響する場合は、部局総括責任者は学内窓口を通じて全学総括責任者に連絡する。

(ウ) 全学総括責任者は、学内窓口に指示して、緊急措置の実施により影響を受ける利用者等に被害拡大防止措置を連絡するとともに、必要に応じ非常時対策本部を組織する。

(エ) 学外窓口は、総括責任者または非常時対策本部の指示に基づき、攻撃元サイトや関係するサイトへの連絡、外部広報、及び JPCERT/CC への連絡などを指揮する。

(オ) 非常時対策本部が設置された場合、部局技術責任者及び部局技術担当者は、その指示に従うものとする。

⑷ 復旧計画

(ア) 部局技術担当者は、セキュリティインシデントの被害や緊急措置の影響を特定し、システムやネットワークの復旧計画を立案する。

(イ) 部局技術責任者は、復旧計画を検討し、部局総括責任者（全学ネットワークに影響する場合は全学総括責任者）の承認を得て実施する。

(5) 原因調査と再発防止策

(ウ) 部局技術担当者は、セキュリティインシデント発生の要因を特定し、再発防止策を立案する。

(エ) 部局技術責任者は、利用者等への注意喚起等を含めた再発防止策を検討し、部局総括責任者（全学ネットワークに影響する場合は全学総括責任者）の承認を得て実施する。

(オ) 部局技術担当者と部局技術責任者は、インシデント対応作業の結果をまとめ、部局総括責任者は、再発防止策とともに全学総括責任者に報告するとともに、必要によりポリシ

一や実施規程の改善提案を行う。

(カ) 全学総括責任者は、部局総括責任者からセキュリティインシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずる。

解説：セキュリティインシデントに対して、技術的対応とともに重要となるのが、事後の対応による見直しである。組織においていかに技術的対応を強固にしても、組織をインターネットに接続する限り常に情報セキュリティ上の脅威は存在しているのであって、潜在的かつ必然的にインシデントに対応しなければならない状況にあることをまず理解しなければならない。

JPCERT/CC によるセキュリティインシデントの対応手順の例は以下の通りである。

・手順の確認
・作業記録の作成
・責任者、担当者への連絡
・事実の確認
・スナップショットの保存
・ネットワーク接続やシステムの遮断もしくは停止
・影響範囲の特定
・渉外、関係サイトへの連絡
・要因の特定
・システムの復旧
・再発防止策の実施
・監視体制の強化
・作業結果の報告
・作業の評価、ポリシー・運用体制・運用手順の見直し

JPCERT/CC 技術メモ－コンピュータセキュリティインシデントへの対応
JPCERT-ED-2002-0002 (Ver. 04)
http://www.jpcert.or.jp/ed/2002/ed020002.txt を参照のこと。

６ コンテンツインシデントに関する緊急対応

(1) 部局技術担当者は、生命・身体への危険の可能性を示唆するコンテンツ（殺人、爆破、自殺の予告等）を発見し、または通報等により認知した場合、部局技術責任者の指示によりコンテンツの情報発信元を探知し、その結果を部局技術責任者に報告するものとする。

(2) 部局技術責任者は、部局総括責任者にコンテンツの情報発信元の探知結果を報告し、学内緊急連絡についての指示を求める。

(3) 部局総括責任者は、全学総括責任者に、学内緊急連絡についての指示を仰ぐ。その際、広報、保護者、警察への連絡等の学内規則に従う。

７ 学外クレーム対応

(1)　原則

(ア) 学外クレームを受けた場合で、請求の法律的な効果や指摘されたコンテンツや行為の違法性の判断を要するときは、あらかじめ対応手順が明確になっていない限り、必ず法律の専門家に相談するものとする。
(イ) 部局技術責任者は、学外クレームについては、部局総括責任者及び全学総括責任者に報告を行ものとする。
(ウ) 学外クレームについての報告を受けた全学総括責任者は、必要に応じ非常時対策本部を設置するものとする。
(エ) 全学実施責任者または非常時対策本部は、攻撃先サイトや関係するサイトへの連絡、外部広報、及び JPCERT/CC への連絡などを指揮し、部局技術責任者及び部局技術担当者は、その指示に従うものとする。

(2) 利用者等のコンテンツの違法性を主張した送信中止・削除の要求
(ア) 発信元利用者等の特定
学外クレームが利用者等により不特定多数に宛て情報発信されたコンテンツの違法性や情報発信による権利侵害を主張してコンテンツの送信中止や削除の要求が被害を主張する者またはその代理人からなされたものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。

(イ)（通常手続き）コンテンツを発信した利用者等への通知と削除
a. 指摘されたコンテンツの違法性の判断が困難な場合、プロバイダ責任制限法第 3 条第 2 項第 2 号に基づき利用者等に請求があった旨通知し、通知後 7 日以内に利用者等から反論がない場合は、送信中止あるいは削除を実施するものとする。
b. 有効と思われる反論があった場合は、その旨、削除請求者に伝えるとともに、当事者間での紛争解決を依頼する。
(ウ)（緊急手続き）利用者等への通知前の一旦保留
a. 指摘されたコンテンツの違法性が疑いもなく明らかと判断できる場合、一旦利用者等のコンテンツの送信を保留し、その旨利用者等に伝えるものとする。有効な反論があればコンテンツ送信を復活するものとする。
b. 本手続きの対象は、著名な音楽 CD の丸写しや個人の住所や電話の暴露等、権利侵害の疑いが濃厚である場合、緊急な救済の必要性がある場合のみとする。
c. 本緊急手続が適用されることもあることは具体的に利用規定として明示する等、利用者等に周知するものとする。
解説：「プロバイダ責任制限法ガイドライン等検討協議会」の各ガイドラインを参照。
http://www.telesa.or.jp/consortium/provider/index.htm

(3) 利用者等の発信したコンテンツの刑事的違法性の指摘及び送信中止・削除の要求
（ア） 利用者等の発信したコンテンツが刑事法上違法な可能性の高い旨指摘された場合で、名誉毀損や、著作権侵害等、被害者が存在する犯罪については、（２）と同様の手順を取るものとする。
（イ） わいせつ物陳列罪等、被害者のいない犯罪が外部クレームにより指摘された場合、

a. 部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。
b. 発信元利用者等に犯罪であるとする指摘があった旨通知し、7 日を経過しても利用者等から反論がない場合は、送信中止あるいは削除を実施する。

解説：情報内容についての刑事的な違法性判断は困難な場合が多く、基本的には、発信元利用者等の反論を待ってから送信防止措置を講ずることとする。

(4) 利用者等の行為（コンテンツ以外）の違法性を主張した送信中止・アカウント削除等の要求

(1)（通常の対応）通信を発信した利用者等への通知とアカウント停止
- 学外クレームが利用者等による１対１の情報発信による権利侵害等による被害を主張して情報発信の中止を要求するものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。
- 事実確認を行い、特定できた利用者等に対し、問題の通信の発信を中止するよう通知する。これには再度行った場合には関連するアカウントを停止する旨警告することを含む。
- 利用者等から有効な反証があれれば、関連するアカウントの一時停止を解除する。
- 念書をとるなどの対応の後、アカウントの復活手続きを行う。
- 同様の手順を経て再発が確認できた場合には、Ａ大学の処罰の手順に移行する。

(2)（セキュリティインシデント対応）利用者等のアカウントの一時停止
- 学外クレームが利用者等による１対１の情報発信によるセキュリティインシデントによる被害を主張して情報発信の中止を要求するものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。
- 部局技術担当者は、事実を調査し、発信元利用者等を特定する。
- 部局技術担当者は、利用者等の行為がセキュリティインシデントの原因であると判断するのに十分な理由がある場合には、部局技術責任者に報告し、その判断を求めるものとする。
- 部局技術担当者からの報告を受け、部局技術責任者は、必要な場合、利用者等の関連するアカウントを一時停止するとともに、部局情報システム運用委員会に報告する。
- 請求者が連絡を要求しているときには一時停止した旨連絡する。
- アカウントを一時停止した旨利用者等に通知するとともに、再度行った場合には関連するアカウントを停止する旨警告する。
- 利用者等から有効な反証があれれば、関連するアカウントの一時停止を解除する。
- 念書をとるなどの対応の後、アカウントの復活手続きを行う。
- 同様の手順を経て再発が確認できた場合には、Ａ大学の処罰の手順に移行する。

解説：プロバイダ責任制限法第３条は、不特定の者により受信される通信（ウェブサイト、ブログや電子掲示板等によるいわゆる公然性を有する通信）を対象としており、インスタントメッセージやメールのような１対１の通信には適用されない。従って、脅迫メール、特定のメールボックスをターゲットにしたメール爆弾や、特定サーバへのクラッキング等、システムの機能障害を引き起こす通信やコンテンツが問題となる場合であっても特定の者相手の通信には適用がな

い。

しかし、プロバイダ責任制限法の適用範囲には入らず、免責の対象とはならないとはいえ、学内ネットワークの利用規定が、これらの行為についても手続きを明確にして利用規定違反とし、外部からの送信停止要求についても対応できるようにすることは法律上問題はない。これは学問の自由や表現の自由との関係においても問題が少ないと考えられる。

(5) 損害賠償請求等

（ア） **利用者等の情報発信や学外でのネットワークを利用した行為について損害賠償請求や謝罪請求があった場合には、法律の専門家と相談の上、対応するものとする。**

（イ） **学外クレームに対して、法律的判断をせずに、謝罪することや、その他の約束をしてはならない。**

（ウ） **利用者等の発信者情報等、連絡先が特定できている場合、損害賠償を請求する相手方には、利用者等との自主的な紛争解決を依頼するものとする。**

解説：利用者等の情報発信や学外でのネットワークを利用した行為について損害賠償請求があった場合には、法律の専門家と共に対応する必要がある。

プロバイダ責任制限法第 3 条第 1 項により、損害賠償責任の免責を受けられる場合とそうでない場合がある。都立大学事件判決やニフティ事件第二審判決のように、最終的にネットワーク管理者としての損害賠償責任を負わないこととされた事例、ニフティ事件第一審判決や２ちゃんねる事件のように損害賠償責任を負うとされた事例が存在するため、慎重な判断が求められる。具体的な削除請求が事前または同時になされている場合には、上記(1)または(3)の手続きに従っていることにより作為義務違反が無いとされ、損害賠償責任を負わないとされる有力な根拠となり得る。

(6) 発信者情報の開示請求

（ア） **プロバイダ責任制限法第 4 条に基づく場合**

a. **利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって、Web ページ等 1 対多の通信によるものの場合、プロバイダ責任制限法の規定に基づき専門家と共に対処するものとし、発信者が開示に同意している場合を除き、発信者情報の開示請求には慎重に対処するものとする。**

b. **電子メールアドレス等、事前に利用者等から開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼するものとする。**

解説：利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって、Web ページ等 1 対多の通信によるものの場合、プロバイダ責任制限法の規定に基づき専門家と共に対処する必要がある。（通信事業者団体がガイドラインを公表していれば参考とする。）プロバイダ責任制限法第 4 条に基づく手順としては、概ね下記の通りとなる。

(ア) 発信者情報の保有の有無、技術的に特定できるかどうかの判断
開示できる発信者情報がなければその旨を請求者に通知する。
(イ) 発信者情報開示請求の根拠の確認と違法性の判断
必ず法律の専門家に相談する。
(ウ) 開示について発信者の意見を聞く。
発信者が開示に同意すれば開示してよい。
(エ) 発信者情報開示をする法律要件を確実には満たしていないと判断すれば開示を拒否する旨通知する。不開示の判断に故意または重過失がなければ責任を問われないので、少しでも法律要件を満たさない事実があれば、不開示判断をすべきである。
(オ) 発信者情報開示の要件に該当することが確実である場合には開示できる。しかし、開示判断を誤った場合には電気通信事業法や有線電気通信法上の通信の秘密侵害罪やプライバシー侵害による損害賠償責任からは免責されないため、慎重な判断を要する。発信者が開示に同意しない場合、特に慎重な判断を要する。

(7) プロバイダ責任制限法に基づかない発信者情報の照会（民事）

利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の照会があった場合であって、メール等１対１の通信によるものの場合、下記の手順をとるものとする。なお、警察官、検察官、検察事務官、国税職員、麻薬取締官、弁護士会、裁判所等の法律上照会権限を有する者から照会を受けた場合であっても、原則として発信者情報を開示してはならないので同様の手順となる。

(a) 電子メールアドレス等、事前に開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼する。許諾を得ていない発信者情報の開示については発信者の意見を聴く。
(b) 発信者が開示に同意すれば開示してよい。発信者が開示に同意しない場合は、開示を拒絶する。その場合は、通信の秘密及びプライバシーの保護を理由とする。
(c) 発信者情報の保有の有無、技術的に特定できるか否かの判断をし、開示できる発信者情報がなければ、その旨を請求者に通知する。

(8) 強制捜査による発信者情報の差押え、提出命令等

(ア) 部局技術担当者は、発信者情報を含む情報の強制捜査の事前打診があった場合には、発信者情報その他の強制捜査対象の情報を印刷あるいは記憶媒体に出力できるよう準備をしておくものとする。
(イ) 部局総括責任者もしくは対外折衝事務担当者は、部局技術担当者の協力を得て、ネットワークの稼動への影響が最小限になるような方法で強制捜査に協力するものとする。
(ウ) 捜査当局から強制捜査の令状の呈示を受けた場合、令状の記載事項等を確認の上、立会いを求められたときは立会い、押収物があるときは押収目録の交付を受けるものとする。

8 通常の利用規定違反行為の対応

(1) 発見または通報等による認知と事実確認（情報発信者の特定を含む）
部局技術担当者は発見あるいは通報により利用規定違反の疑いのある行為を知ったときは、すみやかに事実関係を調査し、発信元利用者等を特定した上で部局技術責任者に報告する。

(2) 利用規定違反の該当性判断
部局技術担当者の報告を受けた部局技術責任者は、通常の利用規定違反行為の対応手順にのせることが可能と考える場合は、その旨部局総括責任者に報告し、確認を得るものとする。
部局技術責任者は、技術的事項に関する利用規定違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置が必要であるかどうかを部局総括責任者に報告するものとする。
部局総括責任者は、技術的事項以外の利用規定違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置やアカウントの一時停止等、個別の情報発信の一時停止以上の措置が必要であるかを判断する。判断にあたっては、可能な限り当該行為を行った者の意見を聴取するものとし、必要に応じて部局情報システム運用委員会の判断を求めるものとする。

(3) 情報発信の一時停止措置
部局技術担当者は、部局総括責任者または部局技術責任者の指示を受けて、利用規定違反に関係する情報発信の一次停止またはアカウントの一時停止措置等を実施する。

(4) 情報発信者に対する通知・注意・警告・当事者間紛争解決要請
部局技術責任者または部局総括責任者は、事案に応じて下記内容を発信者に通知するものとする。
- 利用規定違反の疑いがあること
- アカウントの一時停止措置等の利用を制約する措置を講じた場合は、そのこと、及びその理由・根拠
- 利用規定違反行為の是正、中止の要請
- 利用規定違反行為が是正、中止されなかった場合の効果（情報の削除やアカウントの停止、学内処分等）
- 反論を受け付ける期間とその効果
- 利用者等当事者間の紛争解決の要請

(5) 個別の情報発信またはアカウントの停止と復活
(6) 部局総括責任者または部局技術責任者は、(4) の措置を講じたときは、遅滞無く全学総括責任者にその旨を報告し、その後の利用者等の対応により、必要に応じ部局情報システム運用委員会の承認を得て、下記を実施するものとする。

- 個別の情報発信またはアカウントの停止と復活
- 有効な反論があった場合、または利用行為が是正された場合の個別の情報発信やアカウントの復活
- 利用行為が是正されなかった場合の情報の削除やアカウントの停止、学内処分の開始手続き-
- 利用者等の当事者間の紛争解決着手の有無の確認

９ 学内処分との関係

部局総括責任者は外部クレームの対象となった利用者等、利用規約違反をした利用者等につき、本学懲罰委員会への報告をすることができる。また、本学懲罰委員会による学内処分の検討に際し、アカウント停止処分やその他ネットワークやシステムの利用を制約する処分の必要性の有無について意見を述べることができる。

A3105 情報取扱い手順

１．目的

情報システムで取り扱う情報は格付けされ、格付けに応じて適切に取り扱う必要がある。取扱いが不適切なため、機密性が求められる情報の漏えい、完全性が求められる情報の改ざん等が生じた場合には、大学活動の停止や社会的信用の失墜の要因となる可能性もある。

本書は、このようなリスクを軽減するため、教職員等が情報を適切に取り扱うために必要な事項を定めることを目的とする。

２．本書の対象

本書は、情報を取り扱うすべての教職員等を対象とする。

３．定義

本書における用語の定義は次のとおりである。

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

４．情報の取扱いに関する全般的な注意事項

4.1 大学活動の遂行以外の目的での情報の作成、入手及び利用禁止

教職員等は、大学活動の遂行以外の目的で、情報の作成、入手又は利用を行わないよう努めること。

4.2 情報の格付け及び取扱制限に応じた取扱い

(1) 教職員等は、作成又は入手した情報について、格付け及び取扱制限を指定し、当該指定の結果を電磁的記録であるか書面であるかに応じて明示すること。

(2) 教職員等は、取り扱う情報に明示された格付けに従って、当該情報を本書が定めるとおりに取り扱うこと。格付けに加えて、取扱制限の明示がなされている場合には、当該取扱制限の指示内容に従って当該情報を取り扱うこと。

５．情報の格付け

5.1 格付け及び取扱制限の指定

教職員等は、情報の格付け及び取扱制限について、「付録A： 格付け及び取扱制限の判断基準」に基づき、格付け及び取扱制限の指定を行うこと。ただし、「付録A： 格付け及び取扱制限の判断基準」で規定されていない情報については、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定（取扱制限については必要性の有無を含む。）をし、決定した格付け及び取扱制限に基づき、その指定を行

うこと。

5.2 格付け及び取扱制限の明示手順

(1) 教職員等は、書面の場合には、格付け及び取扱制限を各ページに明記すること。

(2) 教職員等は、電磁的記録の場合には、参照、編集時に常に格付け及び取扱制限が分かるように、また印刷時に各ページに格付け及び取扱制限が印刷されるように、文章のヘッダ等において各ページに明記すること。ただし、電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記すること。

【格付け及び取扱制限をファイル名にも明記する場合】

(3) 教職員等は、電磁的記録の場合には、当該ファイルの内容を参照せずとも格付け及び取扱制限が分かるように、ファイル名に格付け及び取扱制限を明記すること。

(4) 教職員等は、当該情報を取り扱う教職員等に格付け又は取扱制限の認識が周知徹底されているため、格付け又は取扱制限を明記する必要がないと情報システム運用委員会において定められた情報に関しては、格付け又は取扱制限を書面又は電磁的記録に明記する必要はない。なお、明記が不要な情報については、「付録B： 格付け及び取扱制限の明記不要な情報一覧」を参照すること。

5.3 格付け及び取扱制限の変更手順

5.3.1 格付け及び取扱制限の再指定

(1) 教職員等は、元の情報への修正、追加、削除のいずれかにより、他者が指定した情報の格付け又は取扱制限を再指定する必要があると思料する場合には、「5.1 格付け及び取扱制限の指定」に従って、新たな格付け又は取扱制限を指定すること。

【再指定した場合の指定者をこれを行った教職員等とする場合】

(2) 教職員等は、情報の格付け又は取扱制限を再指定した場合には、指定者の責任として、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け又は取扱制限とならないように努めること。

5.3.2 格付け及び取扱制限の見直し

(1) 教職員等は、元の情報への修正、追加、削除のいずれもないが、元の情報の格付け又は取扱制限がその時点で不適当と考えるため、他者が指定した情報の格付け又は取扱制限そのものを見直す必要があると思料する場合には、その指定者又は同人が所属する上司に相談すること。

(2) 被相談者は、指定した情報の格付け又は取扱制限の見直しの必要性を検討し、必要があると認めた場合には、当該情報に対して新たな格付け又は取扱制限を「5.1 格付け及び取扱制限の指定」に従って指定すること。ただし、「付録A： 格付け及び取扱制限の判断基準」に規定されていない情報の場合には、「5.1 格付け及び取扱制限の指定」に

従って決定及び指定すること。

(3) 被相談者は、指定した情報の格付け又は取扱制限の見直しに際して、「付録A： 格付け及び取扱制限の判断基準」において決定されている情報の格付け又は取扱制限の見直しが必要と思料される場合には、上司に報告すること。

【見直した場合の指定者を元の格付け等を行った教職員等とする場合】

(4) 被相談者は、情報の格付け又は取扱制限を見直した場合には、指定者の責任として、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け及び取扱制限とならないように努めること。

6. 情報の作成・入手

6.1 情報を作成・入手する場合の注意事項

教職員等は、大学活動の遂行以外の目的で、情報を作成又は入手しないよう努めること。

6.2 情報を新規に作成した場合の格付け方法

教職員等は、情報を新規に作成した場合には、「5. 情報の格付け」に従って当該情報の格付け及び取扱制限を指定し、これを情報に明示すること。

6.3 格付けされた情報を引用して情報を作成した場合の格付け方法

教職員等は、既に格付けされた情報を引用して情報を作成する場合には、引用した情報の格付け及び取扱制限と、「5. 情報の格付け」に従って指定した新規に作成した情報の格付け及び取扱制限とを比較した上で、より上位の格付けを行い、双方の取扱制限を併せた新たな取扱制限とし、これを情報に明示すること。

6.4 格付け及び取扱制限が明示されている情報を入手した場合の格付け方法

(1) 教職員等は、格付け又は取扱制限が明示されている情報を入手した場合には、明示されている格付け又は取扱制限を継承すること。

(2) 教職員等は、格付け又は取扱制限が明示されている情報を入手した場合で、当該情報の継承すべき格付け又は取扱制限を変更する必要性があると思料するときは、「5 情報の格付け」に従って格付けを変更すること。

6.5 格付け及び取扱制限が明示されていない情報を入手した場合の格付け方法

教職員等は、格付け又は取扱制限が明示されていない情報を入手した場合には、「5 情報の格付け」に従って当該情報の格付け又は取扱制限を指定し、これを情報に明示すること。

7. 情報の利用

7.1 情報の利用における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、情報を利用しないよう努めること。

(2) 教職員等は、取り扱う情報に明示された格付けに従って、当該情報を取り扱うこと。格付けに加えて、取扱制限の明示がなされている場合には、当該取扱制限の指示内容に従って当該情報を取り扱うこと。

7.2 情報を利用する場合の保護方法

(1) 教職員等は、要保護情報が保存された外部記録媒体を利用する場合には、紛失及び盗難から保護するために、以下の措置を講ずること。

- 外部記録媒体の利用中に適切な保護が行えない場合には、当該外部記録媒体を放置せずに、施錠可能な保管庫、棚等に保管する。
- 外部記録媒体の利用が終了した場合には、当該外部記録媒体を机上、端末のドライブ内等に放置せずに、所定の場所に保管する。

(2) 教職員等は、要機密情報が記載された書面又は重要な設計書を利用する場合には、紛失及び盗難から保護するために、以下の措置を講ずること。

- 書面の利用中に適切な保護が行えない場合には、当該書面を放置せずに、施錠可能な保管庫、棚等に保管する。
- 書面の利用が終了した場合には、当該書面を机上等に放置せずに、所定の場所に保管する。
- プリンタ等で書面に印刷した場合には、出力トレイに当該書面を放置せずに、速やかに回収する。

(3) 教職員等は、機密性３情報が記載された書面又はこれが含まれる電磁的記録を必要以上に複製しないこと。

(4) 教職員等は、要機密情報が記載された書面又はこれが含まれる電磁的記録を必要以上に配付しないこと。

【書面に印刷された機密性３情報の所在を明らかにする場合（強化遵守事項）】

(5) 教職員等は、書面に印刷された機密性３情報には、一連番号を付し、その所在を[機密性３情報印刷書面管理表]の様式で明らかにしておくこと。

【機密性３情報に機密性３情報として取り扱う期間を明記する場合（強化遵守事項）】

(6) 教職員等は、機密性３情報には、機密性３情報として取り扱う期間を明記すること。

(7) 教職員等は、機密性３情報の格付けを下げた場合には、その旨を関係する教職員に通知するとともに、[機密性３情報印刷書面管理表]に記録すること。

８．情報の保存・管理

8.1 情報の保存における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、要保護情報を電子計算機又は外部記録媒体に保存しないこと。

(2) 教職員等は、電子計算機又は外部記録媒体に保存された要保護情報について、保存の理由となった業務事務の遂行目的が達成された等、保存する理由が滅失した場合には、速やかに当該情報を削除すること。

(3) 教職員等は、電子計算機又は外部記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存すること。

(4) 教職員等は、保存期間が満了した情報に関して、保存期間を延長する必要がない場合は、速やかに当該情報を消去すること。

(5) 教職員等は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、滅失、消失又は改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、バックアップ又は複写を取得すること。ただし、部局技術担当者によりバックアップされているファイルサーバに保存している等、既にバックアップが行われている場合は、この限りでない。

(6) 教職員等は、バックアップ若しくは複写された情報又は当該情報が保存された電磁的記録媒体若しくは記載された書面を、バックアップ又は複写元の情報と同等に管理すること。

8.2 電子計算機へ情報を保存する場合の保護方法

(1) 教職員等は、要保護情報を電子計算機に保存する場合には、他の者が当該情報を参照、変更、削除等できないようにアクセス制御すること。

(2) 教職員等は、機密性３情報を端末に保存する場合には、アクセス制御に加え、当該情報を暗号化すること。

(3) 教職員等は、要保全情報を端末に保存する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与すること。

8.3 外部記録媒体へ情報を保存する場合の保護方法

(1) 教職員等は、要機密情報を外部記録媒体に保存する場合には、当該情報を暗号化すること。ただし、機密性２情報の場合には、パスワードを用いた保護で代替することができる。

(2) 教職員等は、要保全情報を外部記録媒体に保存する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与すること。

8.4 要保護情報が保存された外部記録媒体並びに記載された書面及び重要な設計書の保管方法

教職員等は、要保護情報が保存された外部記録媒体又は記載された書面若しくは重要な設計書を保管する場合には、施錠管理された保管庫、棚等に保管すること。

９．情報の公表・提供

9.1 情報の公表・提供における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、情報を公表・提供しないよう努めること。

(2) 教職員等は、要機密情報を提供する場合には、「9.2 情報の公表・提供に関する手続」の手続に従い、提供する情報及び提供先を必要最小限にとどめること。

(3) 教職員等は、要保護情報を提供するために当該情報を移送する場合には、「11. 情報の移送」に従って移送すること。

(4) 電磁的記録には、プロパティ等に作成者名、組織名、作成履歴等の付加情報が含まれている可能性があり、当該付加情報から情報が漏えいする場合がある。教職員等は、電磁的記録を公表又は提供する場合には、当該情報の付加情報に不要な情報が含まれていないか確認し、不用意な情報漏えいを防止すること。

(5) 教職員等は、格付け及び取扱制限の明記が不要とされている情報を含む書面又は電磁的記録の提供については、提供先においても格付け及び取扱制限に応じた取扱いを確保するため、提供する前に、明記が不要とされている情報の格付け及び取扱制限を当該書面又は電磁的記録に明記すること。

(6) 教職員等は、要機密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、本学の付した情報の機密性の格付けに応じて適切に取り扱われるための措置として、取扱いに関する留意事項の伝達、適切な管理のための取決め等の措置を講ずること。

9.2 情報の公表・提供に関する手続

(1) 教職員等は、保有する情報を公表する場合には、当該情報が機密性１情報に格付けされるものであることを確認すること。

(2) 教職員等は、機密性１情報を公表する情報には、当該情報が法律の規定等で公表が禁じられていないことを確認すること。

(3) 教職員等は、機密性３情報を本学外の者に提供する場合には、[機密性３情報移送・提供許可申請書]の様式で上司に申請し、許可を得ること。

(4) 教職員等は、機密性２情報を本学外の者に提供する場合には、当該情報が機密性２情報に格付けされたものであることを確認し、秘密であると判断した情報を削除した上で、提供すると同時に、上司に届け出ること。メールに添付して提供する場合は、上司にBCC:で送信しておくなどの方法が考えられる。

１０．情報の持出し

10.1 情報の持出しにおける注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、要保護情報を学外に持ち出さないこと。

(2) 教職員等は、大学活動の遂行の目的で、要保護情報を学外に持ち出す場合には、「10.2 情報の持出しに関する手続」の手続に従い、持ち出す情報及び持出先を必要最小限にと

どめること。

(3) 教職員等は、要保護情報の持出しのため、当該情報を移送する場合には、「11. 情報の移送」に従って移送すること。

(4) 教職員等は、持出先においても学内と同様に情報を取り扱うこと。

10.2 情報の持出しに関する手続

(1) 教職員等は、大学活動の遂行の目的で、大学支給以外の情報システムにおける情報処理又は学外での情報処理を行うために、電子計算機、外部記録媒体、書面等で要保護情報（機密性２情報を除く。）を学外に持ち出す場合には、[要保護情報（機密性２情報を除く。）持出し許可申請書]の様式で部局技術責任者又は上司の許可を得ること。

(2) 教職員等は、要保護情報（機密性２情報を除く。）の持出しによる大学支給以外の情報システムにおける情報処理又は学外での情報処理が終了した場合には、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

１１．情報の移送

11.1 情報の移送に関する手続

教職員等は、機密性３情報を移送する場合には、[機密性３情報移送・提供許可申請書]の様式で上司に申請し、許可を得ること。当該申請において、移送方法（送信又は運搬のいずれか）及び移送手段（電子メールの添付、郵送、職員による携行等）を届け出ること。

11.2 移送方法・手段の選択方法

情報の格付け、種類等に応じて移送方法・手段を選択する。

11.3 書面及び外部記録媒体を運搬する場合の保護方法

(1) 教職員等は、要機密情報が記載された書面又は保存された外部記録媒体を建屋外に運搬する場合には、安全確保のため、以下の措置を講ずること。

- 外見から機密性の高い情報であることが分からないようにする。
- 郵便、信書便等の場合には、親展で送付する。
- 携行の場合には、封筒、書類鞄等に収め、当該封筒、書類鞄等の盗難、置き忘れ等に注意する。

【機密性３情報の暗号化を必須とする場合】

(2) 教職員等は、要機密情報が保存された外部記録媒体を建屋外に運搬する場合には、書面又は保存された外部記録媒体を建屋外に運搬する場合の措置に加え、以下の方法を用いて当該記録媒体に保存された情報を保護すること。ただし、当該情報が機密性２情報の場合には、パスワードを用いた保護で代替することができる。

・ 情報の暗号化

【秘密分散を利用する場合（強化遵守事項）】

・ 秘密分散

(3) 教職員等は、要機密情報が記載された書面又は保存された外部記録媒体を建屋内で運搬する場合には、建屋外に運搬する場合の措置に準じて保護することが望ましい。

(4) 教職員等は、要保全情報が保存された外部記録媒体を建屋外に運搬する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与することが望ましい。

11.4 電磁的記録を送信する場合の保護方法

【機密性３情報の暗号化を必須とする場合】

(1) 教職員等は、要機密情報である電磁的記録を学外に送信する場合には、以下の方法を用いて当該情報を保護すること。ただし、当該情報が機密性２情報の場合には、パスワードを用いた保護で代替することができる。

・ 通信路の暗号化

・ 電磁的記録の暗号化

【秘密分散を利用する場合（強化遵守事項）】

・ 秘密分散

(2) 教職員等は、要機密情報である電磁的記録を学内に送信する場合には、学外に送信する場合の措置に準じて保護することが望ましい。

(3) 教職員等は、要保全情報である電磁的記録を　学外に送信する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与することが望ましい。

１２．情報の消去

12.1 外部記録媒体及び書面の廃棄方法

【機密文書等の回収及び廃棄を外部委託している場合】

(1) 教職員等は、情報が保存された外部記録媒体を廃棄する場合には、専用の回収ボックスに投入すること。

(2) 教職員等は、要機密情報が記録された書面を廃棄する場合には、専用の回収ボックスに投入すること。

【細断機を利用する場合】

(1) 教職員等は、情報が保存された外部記録媒体を廃棄する場合には、細断機を利用して細断すること。

(2) 教職員等は、要機密情報が記録された書面を廃棄する場合には、細断機を利用して細断すること。

【外部記録媒体を教職員等が自身で処理する場合】

教職員等は、情報が保存された外部記録媒体を廃棄する場合には、以下のように外部記録媒体の物理的に破壊する等し、読取装置を利用して当該外部記録媒体から情報が読み出せないことを確認すること。ただし、物理的な破壊等により読取装置が利用できない場合に限り、確認を省くことができる。

- 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。
- 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。

12.2 外部記録媒体を他者へ渡す場合の情報の消去方法

教職員等は、使用済みの外部記録媒体を他者へ渡す場合で、当該外部記録媒体に記録されている情報を提供する必要がないときは、データ消去ソフトウェア又はデータ消去装置を用いて、当該外部記録媒体に保存されている情報を復元が困難な状態にし、残留する情報を最小限に保つこと。

【利用環境等により適宜情報を消去する必要がある場合（強化遵守事項）】

12.3 利用環境等の理由により適宜情報の消去が求められる場合の消去方法

教職員等は、外部記録媒体について、無人の執務室で利用される環境等、必要があると認められる場合は、適宜、データ消去ソフトウェアを用いて、当該外部記録媒体の要機密情報を復元が困難な状態にし、残留する要機密情報を最小限に保つこと。

１３．本書に関する相談窓口

(1) 教職員等は、緊急時の対応又は本書の内容を超えた対応が必要とされる場合には、部局技術責任者に相談し、指示を受けること。

(2) 教職員等は、本書の内容について不明な点又は質問がある場合には、部局技術担当者に連絡し、回答を得ること。

付録A： 格付け及び取扱制限の判断基準

格付けの区分

【ポリシーの格付け分類に準拠する場合】

機密性についての情報の格付け

格付けの区分	分類の基準
機密性３情報	本学情報システム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	本学情報システム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、直ちに一般に公表することを前提としていない情報
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

完全性についての情報の格付け

格付けの区分	分類の基準
完全性２情報	本学情報システムで取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

可用性についての情報の格付け

格付けの区分	分類の基準
可用性２情報	情報システムで取り扱う情報（書面を除く。）のうち、滅失、紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

取扱制限の種類

機密性についての取扱制限

取扱制限の種類	概要
○○禁止	○○で指定した行為を禁止する必要がある場合に指定する。 例）複製禁止、配付禁止、印刷禁止、転送禁止、転記禁止、再利用禁止、送信禁止
○○要許可	○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。 例）複製要許可、配付要許可、印刷要許可、転送要許可、転記要許可、再利用要許可、送信要許可
○○必須	○○で指定した行為を必須とする必要がある場合に指定する。また、必須とする際の条件を設定する必要がある場合には、当該条件を付与する。 例）暗号化必須、通信時暗号化必須
○○限り	提供する範囲を○○に限定する必要がある場合に指定する。 例）行政事務従事者限り、課内限り

完全性についての取扱制限

取扱制限の種類	概要
○○まで保存	○○の期日まで保存する必要がある場合に指定する。 例）平成１８年７月３１日まで保存
○○において保存	完全性が確保可能な○○の場所において保存する必要がある場合に指定する。 例）共有ファイルサーバにおいて保存
保存期間満了後要廃棄	指定した保存期日を越えた際に廃棄する必要がある場合に指定する。
○○禁止	○○で指定した行為を禁止する必要がある場合に指定する。 例）書換禁止、削除禁止
○○要許可	○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。 例）書換要許可、削除要許可

可用性についての取扱制限

取扱制限の種類	概要

○○以内復旧	復旧に要する時間として許容可能な時間を設定する必要がある場合に指定する。 例） １時間以内復旧
○○において保存	可用性が確保可能な○○の場所において保存する必要がある場合に指定する。 例）年度内保存文書用共有ファイルサーバにおいて保存

格付け及び取扱制限の判断例

情報類型	格付け	取扱制限
○○資料	機密性２情報 完全性２情報 可用性２情報	複製禁止、配付禁止
△△資料	機密性２情報 完全性２情報 可用性２情報	暗号化必須
□□資料	機密性２情報 完全性２情報 可用性２情報	行政事務従事者限り
●●資料	機密性１情報 完全性２情報 可用性２情報	３日以内復旧、バックアップ必須
▲▲報告書	機密性２情報 完全性２情報 可用性２情報	５年間保存
■■情報	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ａシステムにおいて保存、書換禁止、保存期間満了後要廃棄
…	…	…

【手順書策定者への補足説明】

※ 取扱制限の種類については、情報を取り扱う他の者が制限すべき事項を理解できる形式であれば、例示したものである必要はない。

※ 判断例の構成としては、文書の種類に基づくもの、特定文書に対応させたもの、本学活動の内容に基づくもの等があるため、適宜の方法を採用する。

付録B： 格付け及び取扱制限の明記不要な情報一覧

教職員等に当該情報に関する格付け及び取扱制限の認識が周知徹底されているため、格付け及び取扱制限を明記する必要がないと定められた情報は以下のとおりである。

- ○○資料
- ■■情報
- …

様式X　　別紙4－2

決裁欄
承認日：

機密性3情報移送・提供許可申請書

殿

[申請日]＿＿＿＿＿＿＿＿

[所属]＿＿＿＿＿＿＿＿
[氏名]＿＿＿＿＿＿＿＿
[連絡先]＿＿＿＿＿＿＿＿

[区分(複数選択可)]
☐ 移送
☐ 提供

移送にかかわる情報

移送日		移送先	(所属)　(氏名)
情報の名称			
移送方法	☐ 送信 ☐ 運搬	移送手段	
移送目的			

保護対策	はい	いいえ	該当なし
・書面を移送する場合に、安全確保を行う。	☐	☐	☐
・電磁的記録を移送する場合に、暗号化を行う。	☐	☐	☐
・電磁的記録を移送する場合に、秘密分散を行う。	☐	☐	☐

提供にかかわる情報(移送と同じ場合は「同上」と記入。)

提供日		提供先	(所属)　(氏名)
情報の名称			
提供目的			

保護対策	はい	いいえ	該当なし
・電磁的記録の付加情報を削除する。	☐	☐	☐

様式X　　別紙2－2

機密性3情報印刷書面管理表

［記入日］

［所属］
［氏名］
［連絡先］

［区分］
□ 印刷
□ 入手

書面にかかわる情報

［印刷・入手日］
［情報名称］
［部数］

所在にかかわる情報（印刷・入手した部数に応じて記載する。）

番号	所在	管理者	廃棄	廃棄者
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	

A3111 ウェブサーバ設定確認実施手順　策定手引書

1　本書の目的

本書は、本学ウェブサーバの設定確認を行う場合の手順書を策定するための手引書である。本書に基づいて策定される「ウェブサーバ設定確認実施手順」は、ウェブサーバの検収時における設定確認だけでなく、定期的なウェブサーバの設定確認における利用も想定される。また、定期的な設定確認の場合には、ユーザ認証やアクセス制御等の項目のみを部分的・重点的に確認する利用も想定される。手順書の整備を担当する者は、「ウェブサーバ設定確認実施手順」を策定する際に、本書を参考にすることによって、情報システム運用基本方針、情報システム運用基準及び情報システム運用・管理規程に準拠してこれを効率良く作成することができる。

2　実施手順に記載すべき事項

「ウェブサーバ設定確認実施手順」には、以下の事項を具体化させて記載すること。

2.1　情報システム運用・管理規程に定める「ウェブサーバ設定確認実施手順」に係る遵守事項

A2101-06　（セキュリティホール対策）
A2101-07　（不正プログラム対策）
A2101-08　（サービス不能攻撃対策）
A2101-10　（規定及び文書の整備）
A2101-11　（主体認証と権限管理）
A2101-13　（サーバ装置の対策）
A2101-19　（セキュリティホール対策）
A2101-20　（不正プログラム対策）
A2101-22　（規定及び文書の見直し、変更）
A2101-23　（運用管理）
A2101-27　（サーバ装置の対策）
A2101-30　（電子計算機の対策）
A2101-41　（格付けに応じた情報の保存）
A2101-42　（主体認証機能の導入）
A2101-43　（アクセス制御機能の導入）
A2101-44　（利用者等による適正なアクセス制御）
A2101-46　（アカウント管理機能の導入）
A2101-47　（アカウント管理手続の整備）
A2101-55　（管理者権限を持つアカウントの利用）
A2101-56　（証跡管理機能の導入）
A2101-57　（部局技術担当者による証跡の取得と保存）

A2101-58　（証跡管理に関する利用者等への周知）
A2101-59　（通信の監視）
A2101-60　（利用記録）
A2101-62　（利用者等が保有する情報の保護）
A2101-63　（暗号化機能及び電子署名の付与機能の導入）
A2101-64　（暗号化及び電子署名の付与に係る管理）

2.2　セキュリティ確保に係るその他の留意事項

2.1 に示す遵守事項のほか、セキュリティ確保に係る留意事項として、以下の項目を考慮すべきである。

・システム領域とデータ領域との分離
・ウェブサーバアプリケーションに付属する不要なコンテンツの削除

3　文書構成例

「ウェブサーバ設定確認実施手順」は、ウェブサーバアプリケーションの動作に関する設定及び運用並びに管理上必要となるアプリケーション（リモート管理、コンテンツ更新、パフォーマンス監視等）の設定等も含めた構成が有効である。文書構成の例を以下に示す。

1 本書の目的

2 本書の対象者
  2.1 対象者

3 オペレーティングシステムに関する確認項目
  3.1 ユーザ認証に関する項目
    ・アカウントの管理
    ・パスワードの管理
    ・認証の管理
    ・アカウントのロックアウト
    ・認証時のメッセージ表示
  3.2 ユーザ権利の割り当てに関する項目
    ・システム管理に関する権利
    ・ログオンに関する権利
    ・監査に関する権利
  3.3 アクセス制御に関する項目
    ・ネットワークレベルでのアクセス制御
    ・ファイルシステムレベルでのアクセス制御
    ・システムリソースレベルでのアクセス制御
    ・デバイスレベルでのアクセス制御
  3.4 サービスに関する項目

・サービスの停止
・機能の無効化
3.5 ログ管理に関する項目
・取得項目の選択
・ログファイルの保存方法及び管理
・監査機能の設定
3.6 セキュリティホール対策に関する項目
・既知アップデートの適用
・アップデート方法の設定
3.7 不正プログラム対策に関する項目
・アンチウイルスソフトウェアによる対策
・システム設定による対策
3.8 サービス不能攻撃対策に関する項目
・システムパラメータの調整
・ネットワークパラメータの調整
3.9 パフォーマンスに関する項目
・システムパラメータの調整
・ネットワークパラメータの調整
3.10 暗号及び電子署名に関する項目
・システム全般の暗号化設定
3.11 その他の項目
・要機密情報の保護
・スクリーンセーバーの設定
・バックアップの設定

4 ウェブサーバアプリケーションに関する確認項目
4.1 コンテンツに関する項目
・パーティションの分割
・不要なコンテンツの削除
・公開コンテンツの格付け確認
・私的なコンテンツの排除
4.2 機能に関する項目
・スクリプト／ファイル実行の制限
・アプリケーション／バージョン情報表示の制限
・ユーザドキュメントの公開の禁止
・インデックス表示の禁止
・WebDAV／FrontPage®等の機能制限
4.3 アクセス制御に関する項目
・ネットワークレベルでのアクセス制御
・ユーザレベルでのアクセス制御

・コンテンツレベルでのアクセス制御
4.4 ログ管理に関する項目
・取得項目の選択
・ログファイルの保存方法及び管理
4.5 セキュリティホール対策に関する項目
・既知アップデートの適用
・アップデート方法の設定
4.6 暗号に関する項目
・SSL/TLS の利用

5 リモート管理アプリケーションに関する確認項目
5.1 機能に関する項目
・リモート管理機能の設定
・セキュリティ機能の設定
・機能の無効化
5.2 ユーザ認証に関する項目
・認証方法の強化
・認証時のメッセージ表示
5.3 アクセス制御
・ユーザレベルでのアクセス制御
5.4 ログ管理に関する項目
・取得項目の選択
・ログファイルの保存方法及び管理
5.5 セキュリティホール対策に関する項目
・既知アップデートの適用
・アップデート方法の設定
5.6 暗号に関する項目
・暗号機能の強化

4　作成する上での留意事項

「ウェブサーバ設定確認実施手順」は、以下のことに留意して作成する。

(1) オペレーティングシステム、ウェブサーバアプリケーション及び運用・管理上必要となるアプリケーションごとに確認すべき設定項目が異なるため、それぞれに特化した手順書を作成する。
(2) 確認及び結果の判断を的確に行うため、チェックシートの形式で作成し、確認すべき設定項目を具体的に記述する。
(3) 手順書の対象者として十分な技術を有する者を前提とした場合、確認手順を省略して確認すべき内容のみを簡潔に記載する。
(4) 文書構成例に記載された見出しは基本的なものであるため、ウェブサーバの利用目的、構成、環境等に応じた見出しの検討・追加を行い、必要な確認項目を網羅する。

(5) 文書構成例に記載された見出し及び検討・追加された見出しごとに、ソフトウェアの開発元が公開している情報を活用して確認項目を抽出する。
(6) ソフトウェアの開発元が公開している情報を活用する場合には、著作権に注意する。
(7) 手順書は、学内の担当者による検収時の又は定期的な設定確認としての利用が想定されているため、業者に公開せずに学内の総括責任者、技術責任者、技術担当者及び利用者に限り参照できる文書として取り扱う。
(8) 前記２に示す事項を「ウェブサーバ設定確認実施手順」に反映するに当たっては、当該事項の内容に応じて、以下のいずれかの方針で記述する。

[具体化]・・・「ウェブサーバ」に限定されず一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、これを「ウェブサーバ」に適用し、表現をより具体的に修正・追加する。

[転記]・・・・記述内容が具体性を持ち、変更が不要と思われる遵守事項については、これを転記する。

[詳細化]・・・記述内容が具体性を持っているが、利用者等の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、解説書等を参考に、これを詳細化する。

[背景]・・・・主にセキュリティ機能の実装に関する内容であり、これを背景として利用者等による注意義務が発生すると思われる遵守事項については、これをそれぞれの立場から解釈し直す。

[別立場]・・・利用者の立場ではなく、総括責任者側又は技術責任者並びに技術担当者側の立場から記述されている遵守事項については、これを利用者の立場から解釈し直す。

[参考引用]・・直接「ウェブサーバ」に関連した内容ではないが、利用者等の理解促進に寄与すると思われる遵守事項については、これを参考引用する。

[一般]・・・・直接「ウェブサーバ」に関連した内容ではないが、一般論として手順書に記載しておくことが望ましいと思われる遵守事項については、これを周辺知識として盛り込む。

5　参考資料

「ウェブサーバ設定確認実施手順」の作成に際しては、以下のような資料が参考となる。

5.1　政府関係の資料

(1) 独立行政法人 情報処理推進機構(IPA)の「セキュアな Web サーバーの構築と運用」
URL: http://www.ipa.go.jp/security/fusei/ciadr.html

5.2　政府以外の資料

(1) マイクロソフト株式会社の「セキュリティガイダンスセンター」
URL: http://www.microsoft.com/japan/security/guidance/default.mspx

(2) マイクロソフト株式会社の「Windows Server. 2003 セキュリティ ガイド」
URL: http://www.microsoft.com/japan/technet/security/prodtech/
windowsserver 2003/w2003hg/sgch00.mspx
(3) サン・マイクロシステムズ株式会社の「SunR BluePrints Security Publications」
URL: http://www.sun.com/software/security/blueprints/index.xml
(4) サン・マイクロシステムズ株式会社の「SolarisR Security Toolkit」
URL: http://www.sun.com/software/security/jass/
(5) 日本ヒューレット・パッカード株式会社の「ホワイトペーパー：ネットワーク&セキュリティ」
URL: http://h50146.www5.hp.com/products/software/oe/hpux/
developer/setup/tips.html
(6) 日本ヒューレット・パッカード株式会社の「HP-UXR Bastille」
URL: http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/
displayProductInfo.pl?productNumber=B6849AA
(7) 「Bastille Linux®」
URL: http://www.bastille-linux.org/

A3112 メールサーバのセキュリティ維持に関する規程　策定手引書

1　本書の目的

本書は、サーバ装置上で動作し、電子メールサービス提供のために利用しているソフトウェアのセキュリティ維持に関して、部局技術担当者等が遵守すべき規定（以下「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」という。）を部局技術責任者が整備するための手引書である。

本学においては、情報システム運用基本方針、情報システム運用基準に基づく情報システム運用・管理規程及び関係する規定を整備することが求められている。「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」は、これらの一つとして策定し、本学内において電子メールサービスを提供する場合に適用するものである。

電子メールは通信回線を介して提供されるサービスの中で最も普及しているサービスの一つであり、本学の研究教育事務を円滑に遂行するために不可欠なものになっている。その一方で、電子メールの送受信は情報のやりとりにほかならず、そのやりとりは様々な中継地点を経由して行われるため、その過程における情報の漏えい、改ざんのリスクがある。また、セキュリティホール対策や不正プログラム対策をおこたると、不正中継、ウイルス感染等、学内だけでなく学外にも迷惑をかけるおそれがある。このようなリスクを軽減するため、サーバ装置上で動作し、電子メールサービスにおいて利用されるアプリケーションソフトウェアのセキュリティを維持することが部局技術担当者等に求められる。

本書は、これらの背景の下で、「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」に含めるべき事項を具体的に示し、もって情報システム運用基本方針、情報システム運用基準及び情報システム運用・管理規程への準拠性、本学の研究教育事務への適用性等において適切な規定の整備に資することを目的とする。

2　実施手順に記載すべき事項

「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」には、以下の事項を具体化させて記載すること。

2.1　情報システム運用・管理規程に定める「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」に係る遵守事項

A2101-06　（セキュリティホール対策）
A2101-07　（不正プログラム対策）
A2101-08　（サービス不能攻撃対策）
A2101-10　（規定及び文書の整備）
A2101-11　（主体認証と権限管理）
A2101-13　（サーバ装置の対策）

A2101-19　（セキュリティホール対策）
A2101-20　（不正プログラム対策）
A2101-22　（規定及び文書の見直し、変更）
A2101-23　（運用管理）
A2101-27　（サーバ装置の対策）
A2101-42　（主体認証機能の導入）
A2101-46　（アカウント管理機能の導入）
A2101-47　（アカウント管理手続の整備）
A2101-55　（管理者権限を持つアカウントの利用）
A2101-56　（証跡管理機能の導入）
A2101-57　（部局技術担当者による証跡の取得と保存）
A2101-58　（証跡管理に関する利用者等への周知）
A2101-59　（通信の監視）
A2101-60　（利用記録）
A2101-62　（利用者等が保有する情報の保護）
A2101-67　（インシデントの発生に備えた事前準備）
A2101-68　（インシデントの原因調査と再発防止策）

2.2　セキュリティ確保に係るその他の留意事項

2.1 に示す遵守事項のほか、セキュリティ確保に係る留意事項として、以下の項目を考慮すべきである。

・迷惑メールの取扱い

3　文書構成例

「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」は、情報セキュリティ対策の観点を含めた一般的な利用手順書とすべきである。そのため、利用者等の行為に着目した構成が有効である。文書構成の例を以下に示す。

1 本規程の目的

2 本規程の対象者
　2.1 対象者

3 定義
　《 対象：部局技術担当者 》

4 電子メールサービス提供ソフトェアに共通のセキュリティ維持のための対策
　4.1 利用認証
　4.2 証跡管理
　4.3 セキュリティホール対策
　4.4 サービス不能攻撃対策

5 交換用電子メールサーバにおけるセキュリティ維持のための対策
5.1 不正中継に関する対策
5.2 電子メールに含まれる不正プログラムに関する対策
5.3 迷惑メールに関する対策
5.4 電子メールキューの管理
5.5 エラーメールの管理

6 送受信用電子メールサーバにおけるセキュリティ維持のための対策
6.1 不正中継に関する対策
6.2 メールボックスの管理
《 対象：権限管理を行う者 》

7 電子メールサーバのセキュリティ維持のための対策
7.1 メールアドレス発行・削除に伴う権限管理
《 対象：部局技術責任者 》

8 電子メールサーバのセキュリティ維持のための対策
8.1 利用認証
8.2 証跡管理
8.3 セキュリティホール対策
8.4 サービス不能攻撃対策

9 メールアドレスの発行・削除における注意事項
9.1 メールアドレス発行における注意事項
9.2 メールアドレス削除における注意事項
《 対象：部局総括責任者 》

10 電子メールサーバのセキュリティ維持のための対策
10.1 不正プログラム対策

4　策定する上での留意事項

「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」は、以下のことに留意して策定する。

(9) 電子メールサービス提供のために利用しているソフトウェアのセキュリティ維持に関して、部局技術担当者、権限管理を行う者、部局技術責任者、部局総括責任者ごとに遵守すべき規定を整理・分類する。各者に求められる役割は以下のとおりである。

(10)部局技術担当者は、セキュリティ維持のための運用管理の主たる実施主体である。

(11)権限管理を行う者は、電子メール送受信における主体の権限管理を行う主体である。

(12)部局技術責任者は、セキュリティホール対策計画の作成、証跡管理における証跡の保護等の実施主体である。
(13)部局総括責任者は、不正プログラム対策の見直し等の実施主体である。
(14)規定の主語は、実施主体ごとに「部局技術担当者は」などに統一する。
(15)前記 2 の実施手順に記載すべき事項を「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」に反映するに当たっては、当該事項の内容に応じて、以下のいずれかの方針で記述する。

[具体化]・・・「電子メールサービス」に限定されず一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、これを「電子メールサービス」に適用し、表現をより具体的に修正・追加する。

[転記]・・・・記述内容が具体性を持ち、変更が不要と思われる遵守事項については、これを転記する。

[詳細化]・・・記述内容が具体性を持っているが、利用者等の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、解説書等を参考に、これを詳細化する。

[背景]・・・・主にセキュリティ機能の実装に関する内容であり、これを背景として利用者等による注意義務が発生すると思われる遵守事項については、これをそれぞれの立場から解釈し直す。

[別立場]・・・利用者の立場ではなく、総括責任者側又は技術責任者並びに技術担当者側の立場から記述されている遵守事項については、これを利用者の立場から解釈し直す。

[参考引用]・・直接「電子メールサービス」に関連した内容ではないが、利用者等の理解促進に寄与すると思われる遵守事項については、これを参考引用する。

[一般]・・・・直接「電子メールサービス」に関連した内容ではないが、一般論として手順書に記載しておくことが望ましいと思われる遵守事項については、これを周辺知識として盛り込む。

5　参考資料

「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」の策定に際しては、以下のような資料が参考となる。

5.1　政府及び政府関係機関の資料

(1) 総務省の「迷惑メール対策」
URL: http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html
(2) 独立行政法人 情報処理推進機構(IPA)の「UBE（迷惑メール）中継対策」
URL: http://www.ipa.go.jp/security/ciadr/antirelay.html
(3) 独立行政法人 情報処理推進機構(IPA)の「電子メールのセキュリティ」の「電子商取引における電子メールに関するセキュリティ上の課題」

URL: http://www.ipa.go.jp/security/fy10/contents/over-all/email.html

5.2　政府・政府関係機関以外の資料

なし

6　雛形の利用方法

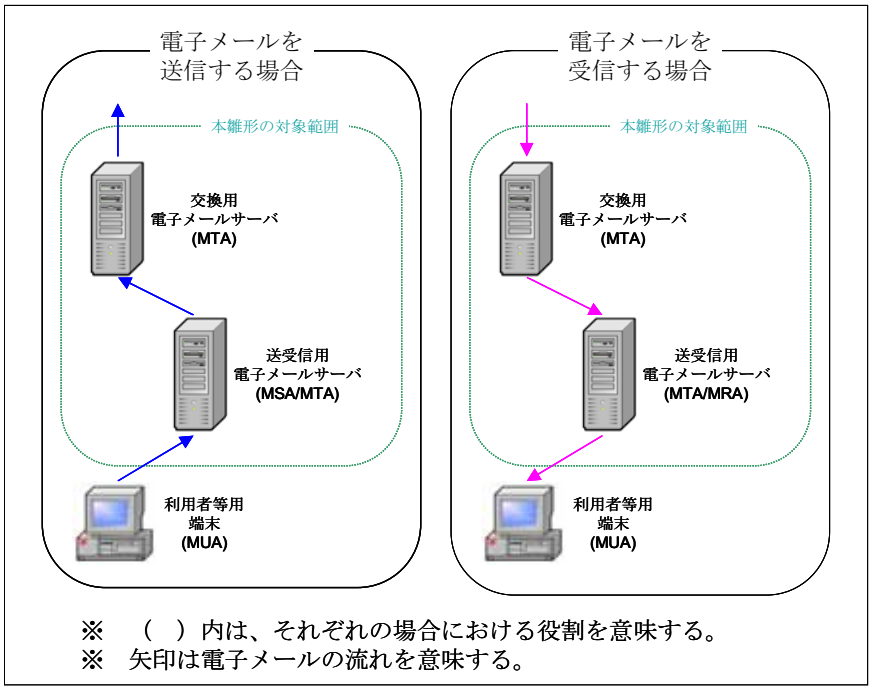
別紙１の雛形を参考にして、「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」を策定すると効率的である。別紙１の雛形は、前記 2 の実施手順に記載すべき事項を、前記 3 の文書構成例の枠組みの中に記載したものである。

6.1　雛形において想定する前提

本雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

・ 電子メールの送受信にかかわる電子メールサーバ及び端末の構成、電子メールの送受信の経路は、以下の図のとおりである。

図：サーバ及び端末の構成、電子メール送受信経路のイメージ



※　（　）内は、それぞれの場合における役割を意味する。
※　矢印は電子メールの流れを意味する。

・ 交換用電子メールサーバにおいて、送受信する電子メールに対する不正プログラムのチェックが実施されている。
・ MRA から電子メールを受信する際に行う利用認証は、知識による認証方式が利用されている。（MSA に電子メールを送信する際に利用認証を利用する場合も同様。）。
・ 利用者等が、MRA から電子メールを受信する際の利用認証に利用するパスワード

を、容易に変更できる機能が用意されている。（MSA に電子メールを送信する際に利用認証を利用する場合も同様。）

・ MTA、MSA 及び MRA において、電子メール送受信、利用認証等の証跡が取得されている。

6.2　手直しポイント

「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」を策定するに当たり、以下の点について手直しをする必要がある。

(1) 「通信回線を介して提供するサービス」に応じて内容を変更する必要がある。雛形は電子メールサービスを対象に記載されているが、例えば、ウェブサービスの場合には、HTTP 基本認証による利用認証、コンテンツのアクセス制御、SSL/TLS を利用した暗号化通信等に関する運用管理の実施手順について記述することとなる。

(2) メールアドレスを発行・削除を伴う人事異動等に関する情報の連絡経路について、「人事異動等における情報セキュリティ対策実施規程」に合わせる。

(3) 雛形において、[・・・] 形式で示す設定値（期間等）については、本学の定めに合わせる。

(4) 雛形において、【・・・の場合】形式で示す記述については、想定される複数の案を記したものであり、本学の判断により適宜、選択又は修正する。

(5) 雛形と既存の実施手順書との整合性を考慮し、適切に分割、統合、相互参照する。特に、本雛形は電子メールに関連するアプリケーションソフトウェアのセキュリティ維持に関する規定を記載しているため、サーバ装置の運用管理手順書との、統合、相互参照をすると良い。

(6) 部局技術担当者、部局技術責任者等の役割ごとに規定を記述しているため、既存の規定の構成に合わせて分割、統合すると良い。

A3201 PC 取扱い手順

解説：大学内で使用される PC 端末の利用手順に関して述べている。ここでいう PC 端末は、利用者がデスクトップ環境等を用いて相対して操作する端末を想定している。サーバ機能やルータ機能を持つコンピュータは対象としていない。ただし、大学外からこれら PC 端末へのリモートアクセスを可能にするためのサーバ機能は例外である。利用手順に倫理条項を含んでいるが、一般端末の利用手順の雛形としての利用を想定したためである。

1. 一般利用者向け利用手順

解説：ここでいう一般利用者は、計算機の特権利用者（Windows であれば Administrator、UNIX であれば root など）以外の利用者を指し、特権利用があらかじめ用意したアカウントを利用する利用者である。一般利用者は計算機の設定（個人環境に関するものを除く）変更や、アプリケーションのインストールはできないものとしている。大学の場合は、演習室や図書館等に設置されている共用端末を利用する一般学生等が対象となる。もちろん、特権利用者も本項目に書かれている事項は遵守する必要がある。

1-1.利用者は以下に掲げる行為をはじめとする、端末等の設備を物理的に損傷する可能性のある行為をしてはならない。

1-1-a.演習室等における飲食。ただし、管理者が別途許可する場合を除く。
1-1-b.コネクタ等を引き抜いたり、キーボードやマウス等周辺機器を取り外す行為
1-1-c.フロッピーディスクドライブ等、開口部に異物を詰める行為
1-1-d.キーボードの乱打、USB メモリ等の乱暴な抜き差しをする行為

解説：主として大学内の共用スペースに設置する共同利用端末に関して、端末設備を物理的に破損する行為等を禁止する。飲食等についてはカフェテリア等に設置する場合もあり、状況に応じて規定を設ける。これら端末を損傷する行為に対する対策は、規定等による対策の他に、管理者による適切な監視体制の整備等も重要である。それら対策が困難である場合には、シンクライアント端末の導入や、タッチパッド等の採用も考慮すべきである。

1-2.利用者は以下に掲げる行為をはじめとする、他の利用者の利用を妨げる行為をしてはならない。

1-2-a.共用端末の占有行為。端末をロックして長時間離席する行為も含む。
ただし、講義等で特に許可された場合を除く。
1-2-b.演習室で大声で騒ぐ行為や、ごみを放置する行為。
1-2-c.プリンタの紙詰まりや紙切れ、トナー切れを放置する行為。

解説：ここに掲げられている事項の他に、ディスク記憶領域や、計算能力、メモリ等の占有行為の禁止が必要になる場合があるかもしれない。しかし、これらの計算機資源の占有が危惧される場合には、クォータ等、システム側で対応を考えた方がよい。
また、ライセンス上、同時起動数が制限されているようなアプリケーションを導入している場合は、同様の規定が必要であろう。
さらに、前項と同様、管理者による監視体制の整備や、プリンタのトラブル等に迅速に対応できる体制作りも重要である。

1-3.利用者は以下に掲げる行為をはじめとするネットワーク帯域を占有する行為をしてはならない。

1-3-a.大きなサイズのファイルの転送
1-3-b.大きなサイズのメール送信
1-3-c.高い頻度で問い合わせパケット等を送出するアプリケーションの使用

解説：基本的には、1-2 の規定に含まれるとも考えられるが、場合によっては、広範囲に影響が及ぶため独立した項目としている。「大きなサイズ」等の具体値をネットワーク性能等に応じて示す方がよい。

1-4.利用者がアプリケーションをインストール、使用する場合には、以下の各号を遵守しなければならない。

1-4-a.教育・研究目的、およびそれらを支援する目的に合致しないアプリケーションをインストール、使用してはならない。
1-4-b.インストール、使用しようとするアプリケーションの利用条件に従って利用すること。
1-4-c.アプリケーションをインストールする前に、ウイルスチェックソフトウェア等により、ウイルスやスパイウェア等、有害ソフトウェアが含まれていないことを確認すること。
1-4-d.出所の定かでないソフトウェアをインストール、使用しないこと。

解説：アプリケーションのインストールに関しては、管理者が行うべきものであり、利用者が共通領域にインストールできるようなシステム構築はセキュリティ上、極力避けるべきである。しかし、その場合でも、利用者

権限で利用者用領域にインストール可能なソフトウェアも存在するので、本項目を設けている。
なお、利用者用ディスク容量の制約が厳しい場合等は、利用者がインストールしてほしいアプリケーションを管理者に申請できるような仕組みを設けることも考えられる。

1-5.利用者は、情報格付け規定において規定されている要管理情報や、その他重要なデータの取り扱いに関して以下の各号を遵守しなければならない。

1-5-a.要管理情報を PC 内部、あるいは外部記憶メディアに保管する場合は、暗号化するものとし、その暗号化鍵を適切に管理すること。
ただし、暗号化以外に十分な保護対策が採られていると管理者が認める場合はこの限りでない。

1-5-b.要管理情報を電子メール等を用いて送信する場合は暗号化するものとし、その暗号化鍵は別途安全な手段を用いて送信すること。

解説：個人情報等、重要な情報の保管、送信時の暗号化の必要性について述べている。1-5-a の但し書きは、バックアップ用メディア等で、暗号化すると著しく利便性が損なわれるような場合に、メディアを厳重に管理することで暗号化に代えられるとしたもの。

1-6.利用者は、CDROM やフロッピーディスク、USB メモリ等の外部記憶メディアを利用する場合には、以下の各号を遵守しなければならない。

1-6-a.利用者のファイルを保存した外部記憶メディアを放置しないこと。

1-6-b.放置してある、または出所が定かでない外部記憶メディアを端末に挿入しアクセスしてはならない。そのような媒体を発見した場合は、管理者に届け出ること。

1-6-c.使用済みの外部記憶メディアを譲渡、または廃棄する場合には、記録されていたデータが復元されることのないように、専用ツールを用いて消去するか、メディアを物理的に破壊すること。

解説：CD-ROM の内容を自動実行する設定にしている場合には、メディアを挿入するだけでソフトウェアが実行され、悪意のあるソフトウェアがインストールされる可能性に留意すること。メディアを廃棄、譲渡する場合は、OS 上でファイルを消去しただけでは、記録情報が復元される可能性に注意すること。

1-7.利用者は、演習室等、共用スペースに設置してある PC 端末を利用する場合は、以下の各号を遵守しなければならない。

1-7-a.端末を操作中に一時的に離席する場合は、端末をロックすること。
1-7-b.演習室等の扉や窓を開放しないこと。また、空調機の設定温度を変更しないこと。ただし、管理者が別途指示する場合はこの限りでない。
1-7-c.使用後の端末等の電源を切ること。ただし、管理者が別途指示する場合はこの限りでない。
1-7-d.プリンターで無駄な印刷をしないこと。

解説：1-7-b は、PC 端末の正常動作（温度、ほこり等）の保証と、PC 端末の盗難防止を目的とするものなので、これらの懸念がない場合は必要ない。
1-7-c についても、利用者に電源を切らせずに、管理者が電源を切る運用をしている場合は必要ない。
1-7-d に関しては、システム上で利用者毎に印刷枚数を制限する方法も考えられる。

1-8.利用者は、以下に掲げる各事項を発見したときは、すみやかに管理者に連絡をするとともに、「情報システムインシデント対応手順」に従って行動すること。

1-8-a.端末の OS やアプリケーション、あるいは、大学内に設置されているホストコンピュータやネットワーク機器等について、セキュリティ上の脆弱性など不具合を見つけた場合。
1-8-b.大学内のホスト上に、著作権を侵害しているおそれのあるコンテンツや、機密情報、個人情報等が公開されていることを見い出した場合。
1-8-c.大学外のホストで、大学の機密情報や、構成員の個人情報等が公開されている、または、大学が権利を有するコンテンツが無断で使用されていることを見い出した場合。

解説：ネットワークや PC 端末の管理業務をしていない一般利用者であっても本項目に掲げるような脆弱性等を発見した場合に報告させることで、構成員のセキュリティや知的財産に関する意識を向上させるとともに、管理業務の効率化をはかることができる。もちろん、管理側では、これら報告に対処する体制作りが必要である。

1-9.利用者は、大学外のネットワークから大学内の情報システム（不特定多数に公開されているもの（Web サービスなど）を除く）にアクセスする場合は以下の各号を遵守しなければならない。

1-9-a.アクセスの際に必要となる認証情報（パスワードや秘密鍵）が漏洩しないように細心の注意を払うこと。万一、認証情報が漏洩した場合、またはその可能性がある場合は、迅速に管理者に報告し、その指示を仰ぐこと。
1-9-b.信頼性が保障できない端末（ネットカフェの端末等）からのアクセスは禁止する。

解説：本項は、利用者が、大学内の PC 端末やゲートウェイサーバ等にリモートアクセス可能な場合に必要な規定である。リモートアクセスのための認証情報が漏洩した場合には、単にメールを読むためのパスワード等が漏洩した場合に比較して、より深刻な被害をもたらす可能性が高いことを利用者が十分に理解していることが大切である。

2. 特権利用者向け利用手順

解説：特権利用者は、PC 端末を管理する権限を持つ特権利用者（Windows であれば Administrator、UNIX であれば root）を指している。具体的には、演習室や図書館等に設置されている PC 端末を管理するセンター職員や、個人で PC 端末を管理する教員や事務職員、研究室に導入されている PC 端末を管理する大学院生等が含まれる。学生等の私物 PC を学内ネットワークに接続することを許可している場合は、その私物 PC の所有者も含まれる。

2-1.特権利用者は、自らが管理する端末が、ウイルス、ワーム等に感染しないように、以下に掲げる規定を遵守しなければならない。

2-1-a.利用している OS、アプリケーションの脆弱性情報をはじめとする情報に留意し、ソフトウェアの不具合を迅速に修正すること。

2-1-b.ウイルス対策ソフトウェアをインストールするとともに、ウイルス情報データベースを常に最新に保っておくこと。

解説：主として利用される OS、アプリケーションに関しては、具体的なチェック方法、修正方法を示しておくことが望ましい。
また、ウイルス対策ソフトウェアをサイトライセンスにより導入している場合、学内からのみデータベースの更新が可能な場合がある。この場合、休暇中等に自宅で感染してしまう可能性があるので注意が必要。場合によっては検疫ネットワークの導入等も検討する。

2-2.特権利用者は、自らが管理する端末に、アプリケーションをインストールし、利用する際には、1-4 項に掲げる規定の他、以下に掲げる規定を遵守しなければならない。ただし、研究・教育目的およびそれらを支援する目的であって、対象となるネットワークの管理者が許可する場合にはこの限りでない。

2-2-a.ネットワーク帯域を極度に圧迫するアプリケーションをインストール、利用してはならない。

2-2-b.自端末宛以外のパケットを傍受するアプリケーション（パケットスニファ）をインストール、利用してはならない。
2-2-c.P2P ファイル交換ソフトウェアをインストール、利用してはならない。
2-2-d.その他、本学 LAN 利用規定に反するネットワークアプリケーションをインストール、利用してはならない。

解説：1-4 項の規定の他に、主にネットワークに関連するアプリケーションのインストールについて規定している。ネットワーク資源の浪費(2-2-a)、通信の秘密(2-2-b)、著作権侵害(2-2-c)等に関して問題が生じそうなアプリケーションを原則禁止している。大学の実態に応じて、これらの問題に関する教育を十分に行った上で、届出制等の形で利用を認めることも考えられる。

2-3.特権利用者は、自らが管理する端末に関して、以下の各規定を遵守すること。

2-3-a.利用者が当該端末を認証なしで利用できるようにしてはならない。
端末が認証機能を有さない場合には、あらかじめ許可された者のみが利用できるように別途手段を講じること。
アカウントの発行状況や利用状況（利用者識別の設定できないシステムにあっては、利用状況が把握できるもの）について部局責任者に定期的に報告すること。
2-3-b.ネットワークを経由して、不特定多数の第三者が端末にアクセスできないようにすること。
2-3-c.当該端末にアカウントを有さない者に端末を使用させないこと。
ただし、教育・研究上必要な場合など、管理者が特に認める場合を除く。
2-3-d.デスクトップ型端末においては、アカウントを有さない者が端末に物理的にアクセスできないように設置場所に施錠等の措置をとるとともに、必要に応じて、端末機器にワイヤーロック等の盗難防止措置をとること。
2-3-e.移動可能な端末においては、短時間であっても端末を放置しないこと。
保管時は施錠可能な場所に保管すること。
2-3-f.CDROM 等、外部記憶メディアから起動できないように BIOS を設定し、BIOS パスワードを設定すること。
2-3-g.端末を廃棄、あるいは譲渡する場合は、内部ハードディスクや不揮発性メモリに、要管理情報やその他重要な情報が残留することのないように、専用ツールを用いて完全に消去するか、物理的に破壊すること。

解説：PC 端末への許可されていない者のアクセスや端末機器自体の盗難等を防止するための規定である。2-3-f は、管理者権限を有さない利用者が管理者権限を得る危険性を排除するためである。2-3-g は、1-6-c と同様に、PC 端末から重要情報や認証情報が漏洩する危険性を排除するためであ

る。特に、学生が所有するノート PC を中古市場に出す場合など注意が必要。

2-4.特権利用者は、自らが管理する端末に関して、利用者が大学外のネットワークから当該端末にアクセスできるようにする場合は、以下の各規定を遵守すること。

2-4-a.アクセスに使用するポート番号、VPN ソフトウェア名等をセンターに届け出ること。

2-4-b.通信内容は全て暗号化されるようにすること。

2-4-c.パスワードのみ（ワンタイムパスワードを除く）による認証方式は原則として避けること。パスワードによる認証を用いる場合は、パスワードの選定に関して利用者に十分な教育を行うこと。

2-4-d.特権アカウント(root など)によるリモートアクセスは原則として行えないように設定すること。

2-4-e.大学が提供するネットワーク以外（電話回線など）の方法でアクセスできるようにしてはならない。教育・研究目的等で、特に必要な場合には、センターの許可を得ること。

解説：1-9 の規定に加えて、特権利用者が、VPN サーバソフトウェア等をインストール、運用する場合の注意点を述べている。

2-4-c は、通信が暗号化されていても、認証パスワードが脆弱であれば不正侵入を許してしまう可能性を考慮したもの。また、リモートアクセスのパスワードとメール受信(POP/IMAP)のパスワードが共通になっている場合、メール受信は SSL/TLS を必須とする等の対策が必要である。

2-5.特権利用者は、自らが管理する端末に関して、監査手順書に従って監査を実施すること。

A3202 電子メール手順

1 本書の目的

電子メールは日々の学習・教育・研究活動において必要不可欠なものになっている。そのため、電子メールは、ルールやマナーを守った安全な方法で使用しなければ、多くの利用者に迷惑をかけることになる。その上、誤った方法による使用は学習・教育・研究活動の停止や社会的信用を失わせる要因となる可能性もある。

本書は、このようなリスクを軽減し、情報資産を保護し、電子メールを安全に利用するための手順を提供する。

2 本書の対象者

本書は、Ａ大学が整備・提供する電子メールを利用するすべての利用者を対象とする。

3 電子メールソフトの設定

3.1 電子メール受信に係る設定

(1)利用者は、受信した電子メールをテキスト（リッチテキストを含む。）として表示することとし、偽のホームページへの誘導や不正なスクリプトの実行を未然に防ぐ目的からHTMLメールの利用は原則として認めない。

[操作手順]　各大学の電子メール利用環境に則した説明を記述する。

なお、HTMLメールの利用を許可する場合には、注意事項、許可に要する手続等についても記述する。

(2)利用者は、アンチウイルスソフトに加えて、電子メールソフト側においてもウイルス対策が設定可能であれば、これを実施すること。

[操作手順]各大学の電子メール利用環境に則した説明を記述する。

【参考：プレビュー機能を停止することを求める場合】

(3)利用者は、プレビュー機能を停止すること。

[操作手順]各大学の電子メール利用環境に則した説明を記述する。

3.2 電子メール送信に係る設定

(1) 利用者は、原則として、HTML形式の電子メールを送信しないこと。これは、当方よりHTML形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

[操作手順]　各大学の電子メール利用環境に則した説明を記述する。

4 電子メールに係る全般的な注意事項

4.1 電子メールの私的利用の禁止

(1) 利用者は、電子メールシステムを、学習・教育・研究活動を遂行する上で必要な場合のみ使用することとし、私的目的のために使用しないこと。

4.2 電子メールの自動転送の禁止

(1) 利用者は、原則として要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送することを禁止する。

(2) 利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要がある場合には、メール転送先・理由・期間・セキュリティ対策などを明確にした上で事前に電子メールシステムの部局技術担当者及び上司の了解を得ること。

(3) 利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要性がなくなった場合には、その旨を電子メールシステムの部局技術担当者及び上司に報告すること。

4.3 大学が整備した電子メールシステム以外の情報システム利用の禁止

(1) 利用者は、学習・教育・研究活動遂行にかかわる情報を含む電子メールを送受信する場合には、大学が整備した電子メールシステムを利用することを原則とする。

(2) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、電子メールシステムの部局技術担当者及び上司の許可を得ること。

(3) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、セキュリティ対策ソフトを導入するなど安全管理措置を講ずること。

(4) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要性がなくなった場合には、その旨を電子メールシステムの部局技術担当者及び上司に報告すること。

4.4 電子メールの監視

(1) 電子メールシステムの適正な利用のため、その利用状況（あて先、内容、添付ファイル等）について証跡の取得、保存、点検及び分析が行われる可能性がある。利用者は、その趣旨を理解の上、電子メールの内容に関するモニタリング及び監査を

実施していることを認識すること。

4.5 電子メールID及び電子メールアドレスの管理

(1) 利用者は、他人の電子メールID (メールサーバへのログインID。以下同じ。) 及び電子メールアドレスを使用しないこと。

(2) 利用者は、電子メールID及び電子メールアドレスを他人と共用しないこと。

(3) 利用者は、自己に付与された電子メールIDを、それを知る必要のない者に知られるような状態で放置しないこと。

(4) 利用者は、電子メールを利用する必要がなくなった場合は、電子メールシステムの部局技術担当者へ届け出ること。

(5) 特定のサービス、職位、部門単位に付与される電子メールID及び電子メールアドレスのように、電子メールID及び電子メールアドレスを複数の関係者で共用する、あるいは担当者が引き継いで使用する必要がある場合には、利用者はその許可及び設定について電子メールシステムの部局技術担当者に相談すること。

4.6 ニュースグループ、メーリングリスト等の発信機関へのID登録の制限

(1) 利用者は、ニュースグループ、メーリングリスト等(メールマガジン、Webマガジン、フリーメール)へのＩＤ登録は、情報セキュリティ情報のメール配信サービスなど、学習・教育・研究活動上必要なものに限定すること。

5 パスワードの管理

5.1 クライアントＰＣのログイン管理・電源管理

(1) 利用者は、クライアントＰＣのログインパスワードを設定すること。

(2) 利用者は、クライアントＰＣを利用しない時にはクライアントＰＣの電源を切ること。

(3) 利用者は、離席時には、各自が利用しているクライアントＰＣをロックすること。また、ロックし忘れた場合に備えて、パスワード・スクリーンセーバが自動起動するように設定すること。

5.2 電子メールパスワードの管理

(1) 利用者は、パスワードを設定すること。

(2) 利用者は、パスワードを容易に推定されないように、設定時には以下の事項を考慮すること。

・ ８文字以上とすること。

・ ２つ以上のアルファベットと１つ以上の非アルファベットを含むこと。

・４つの異なる文字を含むこと。

・辞書にある言葉や一般的な言葉を単独で使用しないこと。

(3) 利用者は、パスワードを他人に知られないように管理すること。

・内容が分かる状態で付箋に記入して貼付しないこと。

・パスワード入力時には周囲からの盗み見に注意すること。

・管理者を名乗ってパスワードを聞き出す等の行為に注意すること。

・付与された初期パスワードは速やかに変更すること。

(4) 利用者は、代行処理などのためにパスワードを他人に教えないこと。

(5) 利用者は、パスワードを忘却しないように努めること。

・他者が容易に閲覧することができないような措置(施錠して保存する等)をとること。

・他者が見ても分からないような措置（独自の暗号方式、変換ルール等）をとること。

(6) 利用者は、定期的に（■か月に１回）パスワードを変更すること。

(7) 利用者は、パスワードが漏えいしたり、電子メールを他者に使用された場合（その危険性がある場合を含む。）には、直ちに電子メールシステムの部局技術担当者又は部局技術担当者に連絡すること。

(8) 利用者は、パスワードを忘れた場合には、学生証又は職員証を提示の上、電子メールシステムの部局技術担当者に相談すること。

(9) 利用者は、パスワードを電子メールソフトに永続的に保存しないこと。ただし、電子メールの受信のたびにパスワード入力を行うことが過度に煩雑である場合には、電子メールソフトに一時保存し、クライアントPC起動後のみパスワード入力とする仕組みを利用してもよい。

(10) 利用者は、パスワードを電子メールソフトに一時保存する場合には、当該パスワードを一時保存するクライアントＰＣを「主体認証情報格納装置」とみなして、以下の点に配慮して安全に取り扱うこと。

・パスワードを保存したクライアントＰＣを本人が意図せずに使用されることのないように安全措置を講じること。

・パスワードを保存したクライアントＰＣを他者に付与及び貸与しないこと。

・パスワードを保存したクライアントＰＣを紛失しないように管理すること。紛失した場合には、直ちに電子メールシステムの部局技術担当者又は部局技術担当者にその旨を報告すること。

6 電子メールの受信

6.1 電子メールの受信確認

(1) 利用者は、定期的に、電子メールの受信確認を行うこと。

6.2 電子メール添付ファイルのウイルスチェック

(1) 利用者は、アンチウイルスソフトによる自動ウイルスチェックを実施すること。

(2) 利用者は、電子メールシステムの部局技術担当者が自動的にウイルスチェックを実施するように設定している場合又は自動的にウイルスチェック最新データを更新するように設定している場合は、当該設定を変更しないこと。

(3) 利用者は、受信した電子メールの添付ファイルに対して、随時、ウイルスチェックを行うこと。これは、新種のウイルスに対応したパターンファイルの提供が間に合わず、ファイル受信時のウイルスチェックにおいてウイルスが発見されなかった場合を考慮し、最新のパターンファイルを用いて過去に受信した電子メールの添付ファイルに対してもウイルスの有無を確認するための対策である。

(4) 利用者は、緊急時対応が必要な時には、電子メールシステムの部局技術担当者からの指示に従うこと。

6.3 あて先間違いの電子メールを受信したときの対処

(1) 利用者は、あて先間違いの電子メールを受信し、送信者から正しい受信者へ再度送信する必要がある場合には、可能な範囲で送信者へあて先が間違っていたことを通知すること。

(2) 利用者は、あて先間違いの電子メールを受信した場合には、これを削除すること。

6.4 不審な電子メールを受信したときの対処

(1) 利用者は、不審な電子メールを受信した場合には、電子メールを開かず、電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

(2) 利用者は、電子メールに不審なファイルが添付されていた場合には、当該ファイルを開くことなく電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

6.5 ウイルスに感染したときの対処

(1) 利用者は、クライアントＰＣがウイルスに感染した場合、又は感染したと疑われる場合には、更なる感染を未然に防止するため直ちに当クライアントＰＣをネットワークから分離（ネットワークケーブル又は無線ＬＡＮカードを取り外す。）し、電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

6.6 迷惑メールの対処

(1) 利用者は、必要以上に電子メールアドレスを公表し又は通知しないこと。

(2) 利用者は、ネットワークを経由して電子メールアドレスを開示し又は通知する場合には、アドレスを自動収集されないように、工夫を施すことが望ましい。（画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等）

(3) 利用者は、送信される迷惑メールに対しては、これを無視することが望ましい。送信者へ停止要求を出した場合、その電子メールアドレスが使用されている事実を伝えてしまう結果となり、かえって迷惑メールが増加してしまう可能性もあるからである。

7 電子メールの作成

7.1 To、Cc及び Bccの制限

(1) 利用者は、To（あて先）、Cc（カーボンコピー）及びBcc（ブラインドカーボンコピー）の総あて先件数は必要最低限とすること。

・ 使用するネットワークリソースは、電子メール１件の使用リソース×総あて先件数である。

(2) 利用者は、同時に多数の人へ電子メールを送信する場合、Bccを利用するか、あるいは各自に個別送信する等配慮すること。これは、その場合に電子メールアドレスをTo、Ccに列記してしまうと、当該電子メールを受信した者に、他の者の電子メールアドレスが露呈することになるからである。

7.2 電子メール１件当たりのファイル容量の制限

(1) 利用者は、電子メール本体と添付するファイルを含めた総容量が■■Mbyteを超えないこと。

・ 本電子メールシステムでは、送信の際の容量制限を■■MByteとしている。

(2) 利用者は、電子メール本体と添付するファイルを含めた総容量が■■Mbyteを超える場合、別手段による情報提供や分割送信などについて検討の上、電子メールシステムの部局技術担当者に相談し、指示を仰ぐこと。

7.3 電子メールの形式の制限

(1) 利用者は、原則として、HTML形式の電子メールを送信しないこと。これは、当方よりHTML形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

7.4 電子メールの内容

(1) 利用者は、要機密情報を電子メールで送信する場合は別途定められた安全措置を講ずること。

・利用者は、機密性3情報を電子メールで送信する場合には、電子メールシステムの部局技術担当者及び上司の許可を得ること。

・利用者は、機密性2情報を電子メールで送信する場合には、電子メールシステムの部局技術担当者及び上司に届け出ること。

・利用者は、要機密情報を電子メールで送信する場合には、安全確保に留意して送信手段を決定すること。例えば以下の手段が挙げられる。

〇 外部を経由しないネットワーク(専用線等)
〇 暗号化された通信路(VPN等)
〇 暗号メール(S/MIME等)

・利用者は、検討の上決定された送信手段について電子メールシステムの部局技術担当者及び上司へ届け出ること。

・利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、以下の保護対策の必要性を検討し、必要があると認めたときには、これを実施すること。

〇 添付ファイルに対するパスワード保護
〇 添付ファイルの暗号化(暗号化ソフトの使用等)

(2) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

(3) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

(4) 利用者は、他人になりすまして電子メールを作成しないこと。

(5) 利用者は、電子メールを転送する際に、作成者の許可なく内容の変更をしないこと。

(6) 利用者は、個人情報やプライバシーの保護を考慮すること。

(7) 利用者は、次の事項に該当する電子メールの送信を行わないこと。

・ 機密保護違反（■■方針・規程を遵守）

・ 権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）

・ セクシャルハラスメント及び人種問題に関わる内容

・ 無礼及び誹謗中傷

・ ねずみ講に相当する内容

・ 脅迫、個人的な儲け話や勧誘に相当する内容

7.5 ネチケット

(1) 利用者は、チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わないこと。

(2) 利用者は、スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール）、ジャンクメール（役に立たない情報が書かれている電子メール）等を送信しないこと。

(3) 利用者は、電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。

(4) 利用者は、俗語的表現やあらかじめ定められていない省略語を使用しないこと。

(5) 利用者は、機種依存文字コードを使用しないこと。

- 利用者が判断できない場合には、電子メールシステムの部局技術担当者に相談し、指示を仰ぐこと。

(6) 利用者は、電子メールを作成する際、全角30文字以内に改行を入れること。

(7) 利用者は、ToとCCとの使い分けを意識し、送信する電子メールに対する返事を要求する時には、To（あて先）を使用すること。

8 電子メールの送信

8.1 送信時の注意

(1) 利用者は、To（受信者）の記述に誤りがないかを確認してから送信すること。

(2) 利用者は、電子メールにファイルを添付し送信する際に、当該ファイルのウイルスチェックを行うこと。

8.2 電子メールの暗号化

(1) 利用者は、要機密情報を電子メールで送信する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

- 暗号メール(S/MIME等)
- 添付ファイルの暗号化(暗号化ソフトの使用等)

[操作手順] 電子メール（S/MIME）の暗号化手順（Outlook® Express の場合）
Outlook® Express の新規メール作成画面の[ツール]メニューから [S/MIME暗号]を選択の上、送信する。 なお、送信に先立ち、送り先相手の電子証明書の取得は完了しているものとする。

(2) 利用者は、暗号化された情報の復号に用いる鍵を適切に管理すること。

(3) 利用者は、暗号化された情報の復号に用いる鍵のバックアップを取得しておくこと。

8.3 添付ファイルのパスワード保護

(1) 利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、添付ファイルにパスワードを設定すること。

[操作手順] 文書ファイルのパスワードのかけ方（Word®の場合）
Word®の[ファイル]メニューから[名前を付けて保存]を選択した後、 [ツール]から[セキュリティオプション]を選択し、[読み取りパスワード]を設定する。あるいは、[ツール]メニューから[オプション]を選択し、[セキュリティ]タブの画面からも同様の設定が可能である。

(2) 利用者は、保護に用いたパスワードについては、あらかじめ受信者と合意した文字列を用いるかあるいは、電子メールで送信せずに電話などの別手段を用いて伝達すること。

8.4 電子メール送信時における情報漏えい防止の確認事項

(1) 利用者は、添付ファイルを電子メールで送信する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないか確認すること。

- 「プロパティ」に作成者や修正者等の個人情報が残っていないか
- 一見すると表示されていない部分（「非表示」の設定箇所、非表示としたコメント、裏に隠れたシート等）に要機密情報が含まれていないか
- 変更履歴が必要以上に保存されていないか

8.5 電子メールへの署名付与

(1) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

[操作手順] 電子メール (S/MIME) の暗号化手順（Outlook® Express の場合）
Outlook® Express の新規メール作成画面の[ツール]メニューから [S/MIME暗号]を選択の上、送信する。 なお、送信に先立ち、送り先相手の電子証明書の取得は完了しているものとする。

(2) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

8.6 電子メール送信時の受信確認機能の使用制限

(1) 利用者は、トラフィック増を防止するため、電子メール送信時の受信確認は必要最低限の使用とすること。

8.7 電子メールを誤って送信したときの対処

(1) 利用者は、電子メールを誤って送信した場合、相手先（受信者）へのフォローは発信者責任で実施すること。

8.8 ウイルスを送信したときの対処

(1) 利用者は、誤ってウイルスを送信したことが判明した場合、直ちに電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

9 電子メールの保存・削除

9.1 メールボックス（サーバ側）における電子メールの保存・削除

(1) 利用者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、メールボックスから不要な電子メールを削除すること。

・ サーバ側の個人別メールボックスに格納される電子メールの最大容量は、■■Mbytesに設定されている。

(2) 利用者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、クライアントＰＣへの保存を行うこと。

・ サーバ側の個人別メールボックスに格納される電子メールの保存期限は、■か月に設定されている。

9.2 メールボックス（クライアントＰＣ側）における電子メールの保存・削除

(1) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを保存する場合には、暗号化等の措置を講じた上で保存することが望ましい。

(2) 利用者は、本文や添付ファイルに要保全情報が含まれている電子メールについては、適宜バックアップすること。

(3) 利用者は、不要なメッセージは速やかにクライアントＰＣから削除すること。

(4) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを削除する場合には、その機密性に配慮し、復元が困難な状態にすること。

10 本手順に関する相談窓口

(1) 利用者は、緊急時の対応及び本書の内容を超えた対応が必要とされる場合には、電子メールシステムの部局技術担当者に相談し、指示を受けること。

(2) 利用者は、本書の内容について不明な点及び質問がある場合には、電子メールシステムの部局技術担当者に連絡し、回答を得ること。

A3203 ウェブブラウザ手順　策定手引書

1 本書の目的

ウェブは、Ａ大学（以下、本学）における業務システムの利用、情報の伝達や共有だけでなく、学外のニュースサイトや検索サイトの活用等業務の円滑な遂行に必要不可欠なツールとなっている。一方で、私的目的でのウェブの閲覧、掲示板への無断書き込み等が、業務効率の低下や本学の社会的信用を失わせる要因となる可能性もある。

本書は、このようなリスクを軽減し、情報資産を保護するため、ウェブを利用するにあたって利用者が遵守すべき事項を定めることを目的とする。

2 本書の対象者

本書は、ウェブブラウザを利用するすべての利用者に向けた利用手順書を策定しようとする者を対象とする。

3 ウェブの利用に係る全般的な注意事項

ウェブブラウザを利用した学外のウェブサイトの閲覧、学内の情報システムの利用等、ウェブの利用において、利用者の安全性を確保し、業務効率を向上させるために、ウェブの利用に係る全般的な注意事項を記述する。

3.1 目的外利用の禁止

文書構成の例を以下に示す。

（文書構成例）

本学の情報設備は、もっぱら教育・研究の推進と職務・支援業務遂行のために提供されています。そのため、利用者には、公用と私用の区別を意識して、設置目的にそぐわない利用（目的外利用）をしないように注意することが求められます。

目的外利用の典型は、本学の情報設備を使って外部からデータ入力やプログラム開発業務を受注し、もっぱら利益を上げる商業目的で利用するというような場合です。しかし、目的外の利用の形態や態様はさまざまなので、この心得では、利用者を学生・大学院生、教職員に分けて、目的外利用と考えられる事例についての注意情報を提供しています。

学生・大学院生用注意事例(抜粋)

・私的なアルバイトのために掲示板等を利用することは、適切ではありません。
・本学の情報設備を用いて、外部の計算機やデータの保守を、利益をあげる目的で行うことは原則として認められません。

教職員用注意事例
・学会出張等のための航空券等の手配といった職務を遂行する上で必要な取引のために本学の情報設備を用いることは、適正使用です。
・研究目的でやむえない場合を除き、本学の設備や電子メールアドレス、ドメイン名等を利用しネットオークションをしてはいけません。なお、研究目的でやむを得ず利用する場合は、事前の許可が必要です。
・自分の書物を宣伝・販売するために本学の情報設備を利用することは不適切です。
・著作リストの掲示や講義を受講する本学の学生へのテキスト販売に必要な情報は問題のない範囲です。

3.2 ウェブサイト閲覧の監視

適正なウェブ利用を維持するため、その利用状況（いつ、誰が、どのウェブサイトを閲覧したか等）について監査証跡の取得、保存、点検及び分析を行う可能性がある。利用者に対して、その趣旨を理解の上、自身のウェブサイトの閲覧がモニタリング及び監査されていることを認識すべきであることを記述する。

4 ウェブサイトの閲覧

ウェブサイトの閲覧に使用するウェブブラウザの利用方法、ウェブサイトを閲覧する場合に想定される脅威を回避するための注意事項等について記述する。

4.1 ウェブサイトを閲覧する方法

ウェブブラウザの基本的な利用方法を示す。（省略）

4.2　A 大学内の主要なウェブサイト

A 大学で利用できる情報システムの URL と概要を記述。（省略）

4.3 ウェブサイト閲覧時の一般的な注意事項

(1) 利用者は、学外のウェブサイトを閲覧する場合には、以下の事項に留意すべきであることを示す。
・ウェブサイトの情報（特に個人が作成しているウェブサイト）には、正しい情報だけでなく偽情報や誤情報が含まれている可能性があるので、ウェブサイトの情報を検討せずそのまま採り入れないこと。
・ウェブページの再読み込みを短時間に繰り返す（「F5」キーを連打する。）と、サービス不能攻撃と見なされる可能性があるので、注意すること。
・検索サイトでは検索に利用するキーワードによっては、検索結果に有害なウェブサイトへのリンクが含まれている可能性があるので、安易に検索結果のリンク先を閲覧しないこと。

（文書構成例）

利用者がインターネットその他で情報を受信する場合、情報の提供者・発信者が良心的であるとは限りません。利用者には、コンピュータウィルスなど多くの危険の存在を意識して、適切な行動をとることが求められます。 不適切な Web ページにアクセスするとセキュリティ上危険なソフトウェアを実行させられたり、自動認証等に利用する情報（一般にクッキーと呼ばれます。）が漏れたりする可能性があります。

(2) 利用者は、学内のウェブサイトを閲覧する場合には、以下の事項に留意すべきであることを示す。

・（省略）学内のウェブサイトを閲覧する場合の注意事項

4.4 SSL/TLS 通信の確認

SSL/TLS 通信とは、通信内容の暗号化及び通信相手のなりすまし対策がなされた安全な通信であり、重要な情報等を送受信するウェブサイトで標準的に利用されている技術である。利用者に対し、閲覧している学外のウェブサイトと個人情報、重要な情報等を送受信する可能性がある場合には、SSL/TLS 通信が利用されていることを確認すべきであることを示す。

5 ウェブサイトへの情報送信（フォームへ入力した情報の送信、ファイルのアップロード等）

送信する情報の盗聴、なりすましによる誤った通信相手への情報送信その他ウェブサイトに情報を送信する場合に想定される脅威を回避するための注意事項等について記述する。

5.1 フォームに入力した情報の保護方法

利用者は、閲覧しているページに表示されているフォームに機密性の高い情報（パスワード、要機密情報等）を入力してウェブサイトに送信する場合には、情報漏えいを防止するため、SSL/TLS 通信が利用されているのを確認すべきであることを記述する。

（文書構成例）

金融機関等からの電子メールと装って、クレジットカード番号や暗証番号を盗み出すサイトに誘導し、入力させるフィッシング詐欺が広がっています。

６．情報発信

利用者が電子掲示板等に情報を発信する際の注意事項に関する文書構成の例を、以下に示す。

（文書構成例）

１）情報発信者の責任

本学では、さまざまな情報設備・情報資源を活用して、利用者が比較的容易に情報発信のできる環境を提供しています。有意義な情報発信には、大きな社会的メリットがありますが、その一方で予想外の紛争を国の内外で引き起こす危険も含んでいます。利用者には、情報発信の意義と危険について十分な認識が求められます。

２）プライバシー侵害

Web ページは、原理的には世界中の人が閲覧することのできるものです。そのため、他人のプライバシーに関する情報を自分の Web ページなどに掲載する場合には、適切な判断が求められます。電子メールによる情報発信についても同様の配慮が必要です。

３）誹謗中傷

インターネット上の掲示板などを用いて他人を誹謗中傷してはいけません。

インターネットを利用した「チャット」などでは、言葉の行き違いから、議論が感情的なけんかになりがちです。また、匿名で行われるチャットは、参加者以外にも公開されていることが少なくなく、結果的に他人についての誹謗中傷を広く公開する結果になることに十分注意すべきです。

自分とは異なる立場を表明する他人の Web ページに対して意見を述べたり、コメントする場合には、誠実で節度を持った行動が必要です。

４）ストーカー

掲示板等で、特定の人をつけまわすことなどの行為は、不適切です。

５）目的外利用

物や情報の販売を目的にして、大学の情報設備を用いて情報発信することは、原則として認められません。

本学の情報設備や情報資源を物品や情報の販売に利用することはできません。

商品やサービスを販売する目的で、本学の情報設備を使って広告等を掲示・発信することはできません。

本学の情報設備や情報資源を使って、商取引の仲介をすることはできません。

もっぱら政治活動や宗教活動に本学の情報設備を利用することはできません。

６）その他

その他、公序良俗に反する情報を発信してはいけません。

自殺の方法や爆弾の製造方法に関する情報の表示と配布をしてはいけません。

A3211 学外情報セキュリティ水準低下防止手順

１．目的

本学は、本学内の情報セキュリティ水準の低下を招くような行為を防止するだけでなく、本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しないことは当然である。また、本学外のセキュリティ水準を低下させることは、本学を取り巻く情報セキュリティ環境を悪化させることにもなる。

本手順は、情報セキュリティ対策の適所において講ずべき措置を定め、もって本学外の情報セキュリティ水準の低下を招く行為を防止することを目的とする。

２．適用範囲

A1001 情報システム運用基準と同じとする。

３．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

3.1 措置の整備

(1) 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を防止するための具体的措置を例示すること。なお、例示にあたっては、インターネット、ＰＣ、ソフトウェア等の環境の変化、技術の進歩、安全に関する意識の向上等によって変わることに留意すること。

(2) 部局総括責任者は、所管する部局において、本学外の情報セキュリティ水準の低下を招く行為を防止するために、部局技術責任者に対して、防止に必要な措置を検討し、実施手順書等に盛り込むように指示すること。

(3) 部局技術責任者は、所管する情報システムにおいて、全学実施責任者が例示した具体的措置をもとにして、本学外の情報セキュリティ水準の低下を招く行為を防止するための措置を検討し、実施手順書等に盛り込むこと。

3.2 措置の実施

本学情報システムを運用・管理・利用する者は、実施手順書等に従い、本学外の情報セキュリティ水準の低下を招かないように行動すること。

付録： 本学外の情報セキュリティ水準の低下を招く行為を防止するための措置の例示

部局技術責任者は、所管する情報システムにとってリスクと感じる本学外の者による行為は、本学から本学外に対しても行わないことが望ましい。このような視点から、本学外の情報セキュリティ水準の低下を招く行為を防止するための措置として、以下のような注意事項が想定される。

(1) 提供する電磁的記録の内容、形式等による影響

本学外へ電磁的記録を提供する際に、当該電磁的記録の内容、形式等によって、本学外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

・提供する電磁的記録が不正プログラムを含まないこと。

・実行プログラムの形式以外に電磁的記録を提供する手段がない限り、実行プログラムの形式で電磁的記録を提供しないこと。

・提供する電磁的記録に改ざん等がないことを知りえる機会を、提供先の者に与えること。

・提供先の者が警告等に慣れて無視しないように、提供する電磁的記録の参照時に警告等が出ないようにすること。

具体的には以下のような事項が想定される。

・本学のウェブサイト、電子メールの添付ファイル、外部記録媒体等でファイルを提供する場合には、アンチウイルスソフトウェア等を利用して不正プログラムの有無を確認すること。

〇不正プログラムに感染したファイルを本学外に送らないようにするため。

・本学のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利用して圧縮したファイルを提供する場合には、自己解凍形式を利用しないこと。

〇自己解凍形式で圧縮されたファイルは実行可能形式のファイルとなり、当該ファイルを入手した者に不正プログラムの可能性を不必要に想起させ、解凍する際に安全性の確認が必要になるため。

・本学のウェブサイトにおいて、電子署名されていない実行モジュール（Java®アプレット、ActiveX®コントロール等）を提供しないこと。

〇実行モジュールを悪用することで、不正プログラムの感染、情報の漏えい等の被害が発生する可能性がある。そのような悪意のある実行モジュールではなく、安全な実行モジュールであることを正しい電子署名により保証するため。

・本学のウェブサイトにおいて、実行モジュールを電子署名して提供する場

合に、有効でない証明書を利用しないこと。

〇安全な実行モジュールであることを保証できないだけでなく、当該モジュールを入手した者が、有効でないことを示す警告等に慣れてしまい、他の警告等に対しても危険性を感じとれなくなる可能性があるため。

(2) 提供する電磁的記録を処理することによる直接的な影響

本学外へ提供した電磁的記録を提供先の者が参照等する際に、利用する端末等の設定変更を要求することによって、本学外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

・本学外の者が利用している端末のオペレーティングシステム、ソフトウェア等のセキュリティ設定変更を不用意に指示しないこと。

・やむを得ずセキュリティ設定変更を指示する場合には、後に元の設定に戻す方法を、参照しやすい形式で紹介すること。

具体的には以下のような事項が想定される。

・本学のウェブサイトのコンテンツを参照するために、訪問者のブラウザのセキュリティ設定を変更するよう要求しないこと。

〇ウェブウザのセキュリティ設定の変更要求に従った結果、ブラウザのセキュリティレベルが低下し、悪意を持ったウェブサイト等を参照した際に不正プログラムに感染するおそれがあるため。

・本学のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利用して提供するファイルを参照するために、安全性の確認が困難なライセンスフリーの専用ソフトウェア等のインストールを要求しないこと。

〇ソフトウェアのインストールにより、利用可能なソフトウェアの制限の変更又は違反を生じさせるため。また、当該ソフトウェアに脆弱性が発見された場合に、脆弱性を悪用した攻撃の被害にあうおそれがあるため。

(3) 提供する電磁的記録を処理することによる間接的な影響

本学外へ提供した電磁的記録を提供先の者が参照等する際に、明示的に利用する端末等の設定変更を要求するわけでないが、電磁的記録を参照できる設定であることを想定することは、暗黙に設定変更を指示したと考えられる。暗黙に指示した設定変更により、本学外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

・本学外の者にセキュリティ上の問題を生じさせるような設定変更を暗黙に指示する電磁的記録を不用意に提供しないこと。

・やむを得ず当該電磁的記録を提供する場合には、後に元の設定に戻す方法を、参照しやすい形式で紹介すること。

具体的には以下のような事項が想定される。

・本学のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利用して、マクロ等を含んだファイルを提供しないこと。

〇マクロ等を含んだファイルを提供することは、提供先の者に対してセキュリティ設定の変更を明示的に指示することではないが、当該提供先の者がマクロを実行できるような設定にしていることを想定した行為であり、暗黙に設定変更を指示したことと考えることができる。マクロ等には、不正プログラムに感染する問題があり、暗黙に指示した設定変更により、提供先の者に当該問題が生じるおそれがあると考えられるため。

・HTML形式での電子メールを送信しないこと。

〇HTML形式の電子メールを送信することは、受信者に対してセキュリティ設定の変更を明示的に指示することではないが、当該受信者がHTMLを判読できるような設定にしていることを想定した行為であり、暗黙に設定変更を指示したことと考えることができる。HTML形式の電子メールには、フィッシング（本物に似せた偽のウェブサイトへ誘導し、入力情報を詐取する手法）、ウェブビーコン（メールを開いた事実、日時等を確認する手法）等のセキュリティ上の問題があり、暗黙に指示した設定変更により、受信者に当該問題が生じるおそれがあると考えられるため。

A3301 教育テキスト

―情報システム管理者（技術責任者・技術担当者）を対象とした情報セキュリティ対策の教育テキストの必要項目―

1. はじめに

大学等におけるセキュリティポリシーの浸透を意図して、情報セキュリティ対策教育を行う必要がある。教育の対象としては、教員、職員、学生などのさまざまな対象が考えられるが、本文書では、情報システム運用・管理規程第三条で規定された「情報資産及び情報システムを運用管理する者」を対象とする。

2. 項目の構成

情報セキュリティ教育に必要な項目を標準セットとする。その中で、「導入教育」を除いた項目数は次の通りである。

13 大分類
66 中分類
99 小分類
364 項目

ここでは、大分類と主な内容について解説をする。

2.1 導入教育

この項目は、管理者になるための前提知識となる導入部分である。従って、上記の項目数には含まれていない。内容は、LAN の構成や、ネットワーク共有の仕組み、OSI モデルなどの基本知識と、ユビキタス社会の影響などである。

2.2 ネットワークインフラセキュリティ

ここでは、ネットワーク設計技術のなかでも、特に IPV4、IPV6、VPN などの仕組み、装置管理、ルーティングや運用・管理、また、パケットフィルタリングや無線 LAN、PKI を扱う。

2.3 セキュリティアーキテクチャ

ここでは、コンピュータネットワークの基本構造と、セキュリティ確保のためのトポロジー、また、システム保護やシステム更新計画、開発管理などを扱う。

2.4　アプリケーションセキュリティ（全般）

ここでは、サーバ上および組織で管理するクライアントマシン上の、アプリケーションソフトに関するセキュリティの問題を一般的に取り扱う。

2.5　アプリケーションセキュリティ（web）

ここでは、web サーバと web ブラウザの両方について、セキュリティに関する問題を取り扱う。具体的には、Web サーバ管理者としての基礎知識、設定、Web アプリケーション設計に関する事項日々行うべきセキュリティ対策と、クライアントマシン管理者として知っているべきブラウザの特性と、ユーザが陥りやすい事例(スパイウエア、フィッシング)についての対策を含んでいる。

2.6　アプリケーションセキュリティ（電子メール）

ここでは、電子メールシステムのセキュリティについて、MTA, MUA のそれぞれを取り上げ、それぞれの対応方法を取り扱う。特に問題化する不正中継に関する事項とその対処についても重点的な項目とする。

2.7　アプリケーションセキュリティ（DNS）

ここでは、DNS を支えるシステムに関するセキュリティを取り扱う。特にサーバのゾーン転送を取り扱う。

2.8　OS セキュリティ（Unix）

ここでは、Unix（および互換 OS）に関するセキュリティの問題を取り扱う。特にデーモンの起動やポートの取り扱いが重要である。

2.9　OS セキュリティ（Windows）

ここでは、MS Windows に関するセキュリティの問題を取り扱う。特にパッチ管理やライセンスポリシーが重要である。

2.10　OS セキュリティ（Trusted OS）

ここでは、Trusted OS ないしはセキュア OS と呼ばれる OS について取り上げる。

2.11　ファイアーウォール

ここでは特にファイアーウォール技術に固有のセキュリティ問題を取り扱う。特に NAT や DMZ の仕組みが重要である。

2.12　侵入検知

ここでは、侵入検知システムについて取り扱う。特に、運用体制の構築や、検出アルゴリズムについて知ることが重要である。

2.13　コンピュータウイルス

ここでは、コンピュータウイルスについて扱う。特に、予防の方法と感染発見方法、駆除方法などを取り扱う。

2.14　運用

ここでは、人的、設備的な運用について取り扱う。また、定常時と異常時や、システム更新に関わるセキュリティ問題を取り扱う。

ここには関連法規と情報倫理を含む. 情報倫理教育では, 単なる知識の詰め込みでなく, 理念に基づいた行動を取らせるまで理解させることが大切である.

3. 具体的な教材の作成に向けて

ここに上げられた項目は、情報セキュリティを確保するために、当面必要となるであろう項目のリストである。本リストも完全ではなく、時代時代に応じて適宜更新が必要である。

A3401 監査手順

1. 目的

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

本書は、本学における監査の適切な実施のための手順を定めることによって、情報セキュリティ対策の実効性を確保することを目的とする。

2. 本書の対象者

本書は、情報セキュリティ監査責任者及び情報セキュリティ監査を実施する者（以下「監査実施者」という。）を含む本学内における監査に携わる者（以下「学内監査関係者」という。）を対象とする。

3. 監査の概要

3.1 監査とは

本学における監査とは、本学ポリシーに従い、被監査部門とは独立性を有した組織又は者が行う情報セキュリティに関する確認行為（独立的評価）をいい、本学における自己点検結果等をサンプリングし、その確認・評価を行い、確認・評価の結果を全学総括責任者に報告することにより学内のセキュリティレベルの向上に資するものである。

一般的に、監査には「保証型監査」と「助言型監査」があり、これらは監査対象により使い分けられることになる。本学における監査では、ポリシー、実施規程及びそれに基づく手順については準拠性に対する保証型監査を行い、情報セキュリティ対策の運用については準拠性及び妥当性に対する助言型監査を行う。

3.2 基本的考え方

(1) 監査の実施は、本学ポリシーに根拠を置く。
(2) 監査の実施に係る本学内規定等を作成し、監査業務及び手続に関する学内での位置付けを明確化する。
(3) 監査は、年度情報セキュリティ監査計画に基づき、全学総括責任者の指示により実施する。
(4) 監査の客観性、実効性を確保するために、監査責任者は以下のことに配慮する。
  - 専任の監査実施者の確保が困難であることを考慮し、監査業務を通常業務とは独立した業務として行うよう、監査実施者に指示する。
  - 監査実施者の任命に当たっては、所属する上司等と協議をした上で、学

内から広く選定することとし、原則として任期は【2年】とする。

- 監査責任者及び監査実施者で、本学内における監査チーム等の組織を編成することを検討する。
- 監査実施者には、自らが直接担当している業務やシステムの監査を実施させない。
- 監査実施者に対して、監査で知りえたことをその業務以外では利用しないよう、周知徹底する。
- 適宜必要性に応じて、外部監査の活用を合わせて検討する。

(5) 監査調書又は監査報告書を含む監査関連文書は、学内の文書規定及び監査の重要性等をかんがみて、情報の格付けの実施等適切な取扱いを行うとともに、決定した保管方法、保管者、保存期間等に従い適切に保管する。

3.3 監査の目的及び位置付け

3.3.1 準拠性監査（保証意見及び助言意見）

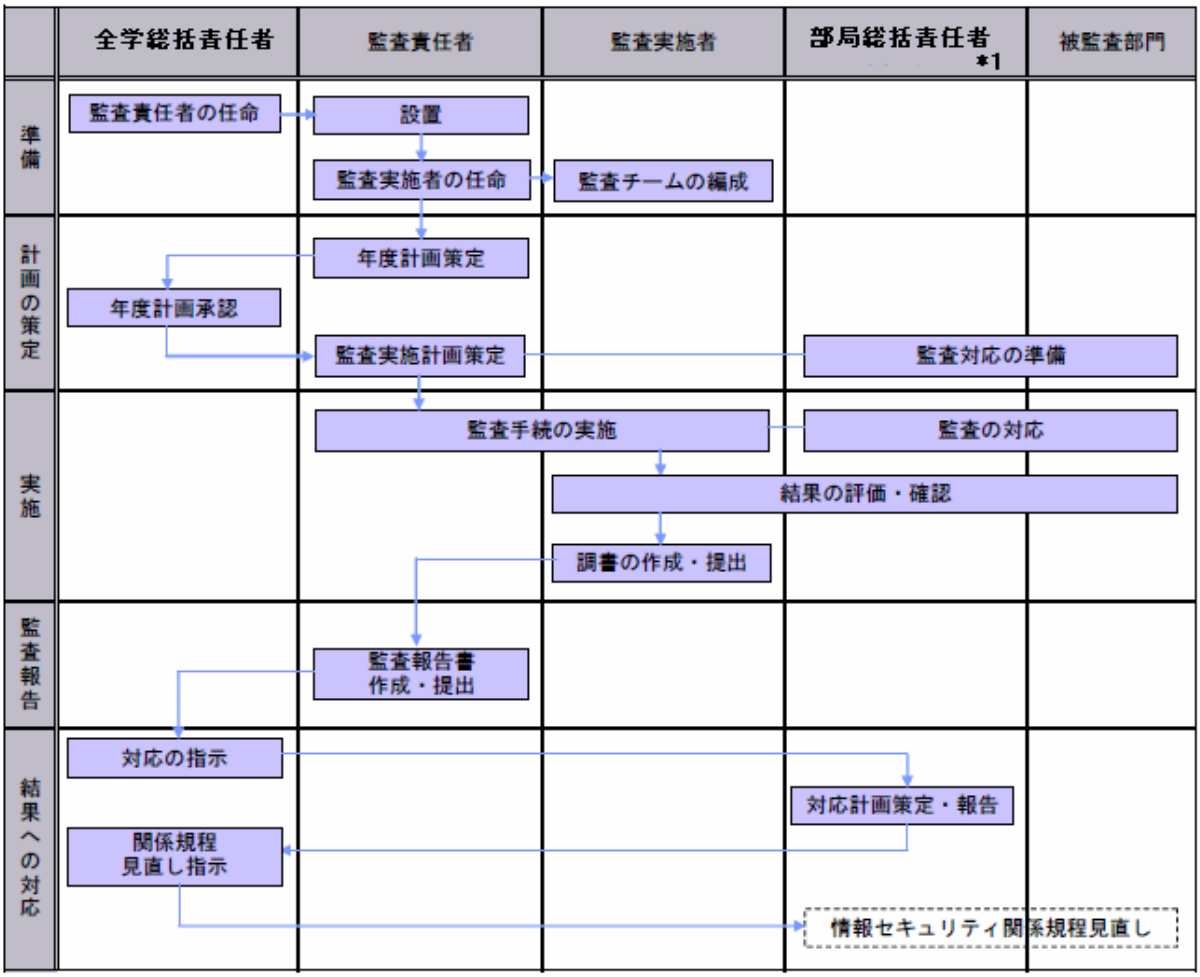
(1) 本学の実施手順が本学ポリシーに準拠しているかを確認・評価する。

(2) 本学における情報セキュリティ対策の運用がポリシー、実施規程及びそれに基づく手順に準拠しているかについて、自己点検結果等をもとに確認・評価する。

3.3.2 妥当性監査（助言意見）

本学のポリシー、実施規程及びそれに基づく手順が実効性のあるものになっているか、情報セキュリティ対策が妥当であるか又は有効に機能しているかについて、自己点検結果等をもとに確認し、改善提案等の助言を行う。

3.4 監査業務の全体像



＊1：被監査部門以外の部局総括責任者を含む場合がある。

4. 監査実施に当たっての前提及び準備

4.1 監査責任者の役割及び権限

(1) 監査責任者は、全学総括責任者の指示に基づき、監査に関する事務を統括する。

(2) 監査責任者は、年度情報セキュリティ監査計画及び監査実施計画（以下「監査計画」という。）を策定し、監査を実施する。

(3) 監査責任者は、監査実施者を任命【し、監査チームを編成】する。

(4) 監査責任者は、監査調書に基づき、監査の結果を監査報告書として作成し、全学総括責任者に報告する。

・ 監査責任者は、準拠性監査の結果を保証する。

・ 監査責任者は、妥当性監査の結果に基づき、改善提案等の助言を行う。

(5) 監査責任者は、監査計画の立案、監査マニュアルの整備及び監査調書のレビュー等のプロセスを通じて、監査業務の品質を管理する。

(6) 監査責任者は、情報システム運用委員会への出席や各部局総括責任者へのヒヤリング等により、継続的に情報セキュリティ関係規程の整備状況や対策の実施状況、情報セキュリティ事案や違反の発生状況等の情報収集に努める。

4.2 監査実施体制の確立及び監査実施者の任命

(1) 監査責任者は、監査の客観性を確保することを考慮し、監査実施者を学内から広く選定し、監査実施体制を確立する。

(2) 監査責任者は監査実施者を任命する際に、監査責任者自らの所管する部局又は学内の各部局からメンバーを選定する。監査責任者は、必要に応じ監査実施者に対する兼務発令や業務指示を発効する。

(3) 監査責任者は、必要に応じ、監査責任者と監査実施者等で構成する監査チームを編成する。

(4) 監査責任者は、監査対象となる情報システムや業務、情報資産の運用に直接携わる者に、当該情報システム等の監査を実施させないものとする。

(5) 監査責任者又は監査実施者は、必要に応じて、監査対象システムの詳細情報を有する組織、学内の情報システム部門等の専門家の支援を受ける。

(6) 監査責任者は、監査の一部業務を外部に委託した場合でも、学内に相当程度の監査実施者を確保する必要があることに留意の上、監査実施体制を検討する。

(7) 監査責任者は、組織内に監査を実施する者又は監査遂行能力が不足していると判断した場合、必要に応じて監査の一部業務の外部委託を検討する。

(8) 監査責任者は、外部委託をする場合、委託先の選定に当り、被監査部門との独立性及び監査遂行能力を有している者を選択する。

4.3 情報収集及び状況の理解

監査責任者は、監査計画の策定及び監査の実施に当たり、事前に部局総括責任者等へのヒヤリングや学内の組織及び所管業務に関する情報収集を行い、学内のセキュリティ関連状況に関する理解に努める。

5. 年度情報セキュリティ監査計画の策定

5.1 目的及び位置付け

(1) 監査責任者は、学内監査関係者と情報を共有することにより、学内における監査業務を円滑に実施することを目的とし、継続的かつ定期的に行うべく当該

年度における監査の年度計画を策定する。

(2) 監査責任者は、当該年度の監査計画の策定に当り、必要に応じて、3ヵ年程度以上の　中・長期計画を策定し、重点監査対象の年度展開及び当該年度に実施すべき監査の水準・詳細度等を設定する。

5.2 概要

(1) 監査責任者は、【毎年2月末日】までに翌年度の「年度情報セキュリティ監査計画」を策定する。

(2) 策定した「年度情報セキュリティ監査計画」は、全学総括責任者の承認をもって、【当該年度4月1日より】発効する。

(3) 監査責任者は、監査実施計画の修正で適応しきれないほどのリスクの変動があった場合には、適宜本計画を修正し、全学総括責任者の承認を得る。

(4) 監査責任者は、当該年度に実施する監査の位置付けや目的、目標を明確化する。

(5) 中・長期計画を策定している場合は、当該中・長期計画に沿って当該年度における監査計画を策定する。

(6) 監査責任者は、当該年度計画の監査対象を明確化し、学内監査関係者に周知する。

(7) 監査責任者は、実施時期の調整や内容の重複の回避などを配慮し、会計検査や特定業務の監査等、恒常的に行われている通常の監査業務との連携を視野に入れて年度計画を策定する。

(8) 監査責任者は、年度情報セキュリティ監査計画に次の事項を記載する。

- 監査方針
- 監査の目的
- 監査対象（業務、システム、段階等）及び監査対象に係る監査目標（例えば、機密性、情報漏えい防止、不正アクセス防止等）
- 監査の想定カバー率
- 監査スケジュール
- 監査業務の管理体制
- 外部委託による監査及び外部専門家の活用の必要性及び範囲
- リソース管理（監査予算、人材育成計画等）

6. 監査実施計画の策定

6.1 目的及び位置付け

(1) 監査責任者は、年度情報セキュリティ監査計画で対象とした個別業務、システム等に応じて、具体的な監査方法及び監査時期等を計画する。

(2) 監査責任者は、学内における監査を円滑に実施することを目的とし、監査実施計画の内容を被監査部門及び当該部門の所属職員に対し事前に通知する。

6.2 概要

(1) 監査責任者は、年度情報セキュリティ監査計画及び情報セキュリティの状況の変化に応じた全学総括責任者からの実施指示に基づき、個別の監査対象ごとの監査実施計画を策定する。

(2) 監査責任者は、過年度の監査の実施状況その他過去の経験、事前の質問、世の中の状況等を勘案し、監査対象ごとの監査実施計画を策定する。

(3) 監査責任者は、監査実施計画に次の事項を記載する。

- 監査目的
- 背景（直前の情報セキュリティの状況認識）
- 監査対象
- 被監査部門及びその責任者
- 監査実施責任者及び実施担当者
- 監査の実施時期
- 監査の実施場所
- 監査の想定カバー率
- 実施する監査手続の概要（監査要点、評価方法の種類等）
- 監査の進捗管理手段
- 外部委託先との役割分担（外部委託を行う場合）

7. 監査の実施

7.1 監査の実施の指示

(1) 全学総括責任者は、年度情報セキュリティ監査計画に従って、監査責任者に対して、監査の実施を指示する。

(2) 全学総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、監査責任者に対して、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示する。監査責任者は監査実施計画を修正し、実施

する。

(3) 監査責任者は、被監査部門から独立した監査実施者に対して、監査の実施を指示する。

・情報システムを監査する場合、当該情報システムを構築又は開発した者はその監査を担当しない。

・情報資産の運用状況を監査する場合、当該情報資産を運用している者はその監査を担当しない。

7.2 監査の実施における留意事項

(1) 監査実施者は、監査計画に基づいて、十分かつ適切な監査証拠を入手し評価する。

(2) 監査実施者は、学内基準等の規定文書の内容確認を行った上で、被監査部門への質問を基本とする。さらに、別途文書による裏づけをとったり（査閲）、実際に行っている作業を観察したり（観察）、自らが実際に行って点検したり（点検）することにより、質問への回答を検証する。

(3) 監査実施者は、対策の実施状況を効率的に確認するために、自己点検票及び自己点検結果を活用する。

(4) 入手した資料は、その入手元及び入手時の状況等を勘案して、監査証拠として採用するかについて、それらが有する信用性及び証明力の程度を慎重に判断する。

(5) 被監査部門から提出された資料、監査実施者自らが入手した資料、自らが行ったテスト結果等を総合的に勘案して、相互に矛盾があるか、異常性を示す兆候があるかを評価する。

7.3 実施結果の評価

7.3.1 準拠性に関する保証意見

(1) 監査実施者は、ポリシー、実施規程及びそれに基づく手順の間に矛盾、相違点、不足がなければ、準拠しているものと判断する。

(2) 監査実施者は、遵守事項違反がなければ、準拠しているものと判断する。

7.3.2 妥当性に関する助言意見

(1) 助言意見は、想定するリスクと比較して、対策が妥当であるかについての意見とする。

(2) 監査実施者は、将来の遵守事項違反につながる可能性のある事象について助言を行う。

(3) 監査実施者は、助言意見を検討するに当たり、実施すべき対策の実現可能性についてまでは考慮せず、原則を指摘することを役割とし、実現可能性についての検討は被監査部門の部局総括責任者が行う。

(4) 被監査部門の部局総括責任者は、実施すべき対策の実現可能性について、監査報告書に基づく全学総括責任者からの指示により検討する。

7.3.3 監査業務において発見された問題点・違反等の取扱い

(1) 監査実施者及び被監査部門の部局総括責任者は、発見された問題点に関する事実関係について、事実誤認等がないかを含め合意をしておく。

(2) 監査実施者は、準拠性に関する違反について、重大な違反と軽微な違反に区分して報告する。

7.4 監査調書の作成

(1) 監査実施者は、実施した監査業務ごとに、監査実施の過程を監査報告書作成の基礎とするため記録した監査業務の実施記録であり、監査意見表明の根拠となる監査証拠集である監査調書を作成し、監査責任者に報告する。

(2) 監査実施者は、参照符号等を整備して、監査の結論に至った経過が秩序整然と分かるように作成する。

(3) 監査実施者は、被監査部門から提出された資料や組織の外部の第三者から入手した資料を監査調書に添付する。

(4) 監査責任者は、監査調書の保管場所や保管責任者を決定し、情報漏えいや紛失等を考慮した上で、あらかじめ定められた期間保存する。

(5) 監査実施者は、監査調書に次の事項を記載する。

- 表題（何を確認したか、何を証明したいか）
- 監査実施者氏名・署名
- 実施期間
- 被監査部門及び責任者
- 発見された問題点（重大な違反、軽微な違反）
- 意見（保証意見、助言意見）
- 確認した遵守項目
- 確認した対策の内容
- サンプルの件数及び抽出方法

・評価方法及び結果

・監査証拠としての形態（文書か口頭か）

・監査証拠の入手元（被監査部門から提出された資料か、監査実施者が直接入手した資料か、第三者から入手した資料か）

・関連資料番号（チェックした項目をマーキングし、資料として添付する。）

8. 監査報告

8.1 監査報告書の作成と提出

(1) 監査責任者は、監査調書に基づき、監査報告書を作成し、全学総括責任者に報告する。

(2) 監査責任者は、監査報告書において、準拠性監査については、当該監査対象の準拠性に関する保証を行うとともに、違反を改善するための助言を行う。また、妥当性監査については、助言を行い、学内PDCAサイクルの実施により改善につなげる。

(3) 監査責任者は、監査報告書の読み手が全学総括責任者であることを意識し、全学総括責任者が報告内容の重要性や指摘事項の緊急性等を理解し、部局総括責任者等への指示すべき内容が明瞭になるように記述する。

(4) 監査責任者は、助言意見を述べるに際して、監査人の自由裁量ではなく、ポリシーや当該契約書等の監査の基準に照らして検出された課題及び問題点の指摘と改善提言とするものとし、保証を付与するかのような誤解を与える表現を用いないようにする。

(5) 監査責任者は、監査報告書の正本を全学総括責任者に提出、写を自らが保管する。

(6) 監査責任者は、監査報告書に次の事項を記載する。

・報告書の名称

・報告書の日付

・報告書の宛名

・監査人の署名、又は記名押印

・監査実施期間

・監査対象範囲（組織、システム、業務機能等）

・監査の基準（判断の尺度）とした管理基準等

・総合的所見

・監査意見（違反の有無、課題及び問題点等）

・監査人の独立性に関する事項 【独立性の例】

〇 過去一度も当該監査対象業務に従事していない

〇 過去2年の間、当該監査対象業務に従事していない

〇 過去1年の間、当該監査対象業務に従事していなく、それ以前に当該業務に係る規定の整備又はシステムの設定等現在に影響の及ぶ行為をしていない

・運用状況の準拠性に関する監査を実施した旨及びその結果（準拠性監査の場合）

・遵守事項の整備状況の妥当性及び運用状況の準拠性に関する監査を実施した旨及びその結果（妥当性監査の場合）

・監査報告書の取扱い（利用及び利用者の制限事項等）

・添付資料（個別業務ごとの監査調書等）

9. 監査結果に対する対応

9.1 監査報告書の内容の分析及び評価

(1) 全学総括責任者は、報告内容を分析し、全体像の把握と課題及び問題点の整理を行う。

(2) 全学総括責任者は、監査報告書において、改善提案等の助言があった場合、その内容の妥当性及び実現可能性等を検討する。

(3) 全学総括責任者は、同種の課題及び問題点が他の部門にもあり得るかの検討及び対策の見直し等の緊急性の検討を行う。

9.2 部局総括責任者への改善指示

(1) 全学総括責任者は、監査報告書の内容を踏まえ、被監査部門の部局総括責任者に対して、指摘事案に対する対応を指示する。

(2) 全学総括責任者は、被監査部門における課題及び問題点が他の部門にも発生する可能性があると判断した場合、他の部局総括責任者に確認する。

(3) 全学総括責任者は、(1)(2)に掲げるもののほか必要な事項について、該当する部局総括責任者に対応を指示する。

9.3 対応計画の作成及び報告

(1) 部局総括責任者は、監査報告書に基づいて全学総括責任者から改善を指示さ

れた事案について、対応計画を作成し、報告する。

(2) 部局総括責任者は、指示された改善が困難であることについて正当な理由がある場合には、リスク軽減策を示した上で、達成可能な対応目標を提示する。

(3) 部局総括責任者は、指示された改善内容が教育・訓練により解決すべき課題であると判断した場合には、全学実施責任者と相談の上、教育計画及び資料に反映する。

9.4 情報セキュリティ関係規程の見直しの指示

(1) 全学総括責任者は、監査報告書において情報セキュリティ対策の妥当性に関した改善提案を受けた場合、ポリシー、実施規程及びそれに基づく手順の妥当性を評価し、当該規定を整備した者に対して必要に応じてその見直しを指示する。

(2) 全学総括責任者は、改善提案を受けた場合であって、ポリシー、実施規程及びそれに基づく手順の見直しの必要がないと判断したときは、その理由を明確にする。

Ａ大学監査手順解説

本解説は、「A3401 監査手順」の各項における用語や例を示すものであり、本書における項番号は「監査手順」の項番号に対応させている。

3. 監査の概要

【手順策定者への補足説明：保証型監査と助言型監査の比較】

特定非営利活動法人 日本セキュリティ監査協会「情報セキュリティ監査制度利用促進等事業 実施報告書」より抜粋

	保証型監査	助言型監査	コンサルティング（参考）
保証	与える	与えない	
意見	述べる		
提言	しない	する	
客観的基準	存在することが前提		ない
実施者の独立性	必須		必須ではない
提言のフォローアップ	なし	あり	なし

4. 監査実施に当たっての前提及び準備

【手順策定者への補足説明：監査業務の品質とは】

実施された監査が、本学ポリシーや外部委託に係る契約書等の監査の基準に準拠して適切に行われているかという監査業務の信頼性及び有効性のこと。

【手順策定者への補足説明：監査実施者に求められる一般的な要件】

・ 高い倫理観

・ 監査対象業務についての知識・理解

・ 情報セキュリティについての知識・技術

・ 情報システムについての知識・技術

・ 監査についての知識・技術

【手順策定者への補足説明：監査チーム編成における配慮事項】

・各監査実施者の通常業務と監査業務の負荷バランス

・監査実施者間の相互チェック機能の確保

・適切な職務の分担による監査対象からの独立性の確保

【手順策定者への補足説明：監査に必要な人的リソースの目安】

監査対象とする項目やシステム、業務の数及び実施する監査の方法により、必要となる監査実施者の人数や能力は異なるが、10～20名程度／大学、人年換算をすると５～10名程度の体制が目安と考えられる。

この一部の人員を外部委託することにより確保した場合でも、学内にかなりの人的リソースを確保しなければならないことに留意の上、計画を立てることが重要である。

【手順策定者への補足説明：監査遂行能力とは】

監査遂行能力とは、監査に関する能力や経験と監査対象業務及び情報セキュリティに対する知識・技術等からなる。

【手順策定者への補足説明：監査業務の委託先の選定に関する配慮事項】

委託先の選定に当たっては、情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の参画を考慮することが望ましい。

【手順策定者への補足説明：収集する情報の例】

・学内の組織図及び情報セキュリティ関係の体制図

・学内の情報セキュリティ関係規程（ポリシー、実施規程、実施手順等）

・各組織及び各情報セキュリティ関係の責任者の一覧

・各組織の業務内容

・各業務で取り扱う情報の種別

・保有している情報システムの一覧

・ネットワーク図等の情報システムに関する情報

・以前に実施した監査に関する計画及び報告書等の監査結果

5. 年度情報セキュリティ監査計画の策定

【中・長期計画を策定する場合の例】

- 初年度 ：学内情報セキュリティ対策の実施状況の把握及び評価
- 2年度目：情報セキュリティ対策実施に関する日常業務への浸透
- 3年度目：情報セキュリティ対策実施の定着化及び学内セキュリティレベルの底上げ

【手順策定者への補足説明：監査対象選定のための観点の例】

- 自己点検が適切に行われているかを確認するための観点
- 遵守できていない（と思われる）ところを重点的に監査する観点
- 毎年同様の監査を実施し、対策状況の進捗や成熟度を経年で確認・評価する観点（定点観測的に経年で確認・評価する観点）
- 環境の変化や監査時点での情報セキュリティ事案の動向・トピックス、体制・規定の変更等をかんがみ、年度別の重点監査対象の項目や重点システムを評価する観点（当該年度重点監査対象の選定）
- 導入段階、定常的運用段階等業務のライフサイクルに応じて確認する観点
- 以前実施した監査結果で明らかになった課題及び問題点の改善状況を確認する観点

【年度情報セキュリティ監査計画の雛形】

作成日：〇〇年4月1日

（情報セキュリティ監査責任者）

氏 名

〇〇年度 ××××大学情報セキュリティ監査計画書

１．監査方針

本年度は、本学内における情報セキュリティ関係の体制構築及び対策の実施状況を網羅的に把握・評価する。来年度以降の対策レベル向上に向けた基盤整備を行う。

２．監査の目的

本学内における情報セキュリティ関係の状況を網羅的に把握することにより、現在の情報セキュリティ関係規程(ポリシー、実施規程、手順等)の妥当性を評価し、来年度以降の対策レベル向上に向けた情報収集・分析を行う。

３．監査対象及び監査対象に係る監査目標

⑴ 重点監査対象

① 実施規程及び手順の準拠性監査（監査目標：〇〇〇）
② 情報セキュリティ管理体制の構築の監査（監査目標：〇〇〇）
③ 情報の格付け業務の監査（監査目標：〇〇〇）
④ 学内LANの運用状況の監査（監査目標：〇〇〇）

⑵ その他の監査対象

① インターネット接続口に設置されているサーバ群のセキュリティ設定の監査

４．監査の想定カバー率

⑴ 対象となる責任者、管理者、利用者（対象となる者/全員）

⑵ 対象となるシステム（対象システム数/全システム数）

⑶ 対象となる端末（対象端末数/全端末数）

５．監査スケジュール：別紙のとおり

６．監査業務の管理体制：別紙のとおり

７．外部委託による監査の範囲及び必要性

⑴ 外部委託の範囲及び必要性

① 範囲 インターネット接続口に設置されているサーバ群のセキュリティ設定の監査
② 必要性 脆弱性スキャン、システム侵入テスト等専門的技術を要するため

⑵ 委託契約の必要性の要否：要

８．リソース管理

⑴ 監査予算：別紙のとおり

⑵ 人材育成計画：詳細別紙のとおり 目標：監査スキルの向上と要員の確保

① 監査業務基礎講座：4月１日～4月30日の2週間程度

② 情報セキュリティ基礎講座：5月1日～5月30日の2週間程度

別紙

●監査業務の管理体制

（体制図の挿入）

●監査スケジュール

監査対象	作業フェーズ	2月	3月	4月	5月	6月	7月	・・・	10月	11月	12月	1月	2月	3月
年度計画策定								・・・						
本学基準及び実施手順の準拠性監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
体制の構築の監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
情報の格付けの監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
学内ＬＡＮの運用の監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
・								・・・						
・								・・・						
・								・・・						

●監査予算

予算項目	項目概要	予算費目	金額	実施時期	実施担当者
出張費					
宿泊費					
外部委託費					
・・・					

●　人材育成計画

育成内容	実施時期	実施方法	対象者	実施担当者
監査業務基礎講座	4/1～4/30	座学	利用者	○○○
・・・				

6. 監査実施計画の策定

【手順策定者への補足説明：監査実施計画策定上の配慮事項】

・本学のシステム、業務、組織等の特性を分析した上で、影響度や脆弱性から判別し、リスクが高いと思われる領域を抽出する。

○ 事件の発生可能性が高いと思われる領域（対策を実施していなければ事故の発生可能性が高い領域、対策が不十分と思われる領域、対策が十分に行われているか不明な領域等）

○ 事件が発生した場合の影響が大きいと思われる領域（機密性の高い情報を取り扱っている領域、完全性の確保が必要となる情報・システムを取り扱っている領域、可用性の確保が必要となる情報・システムを取り扱っている領域等）

・自己点検が終了している等、監査の受入れが十分と考えられる領域を選定する。

・監査が円滑に実施できるように考慮する。

○ 人的リソースや予算の状況

○ 監査対象部門の負荷状況

○ システムの運用状況（負荷の多い日、時間帯を避ける等）

・システムをカテゴリー分けし、監査頻度を決定する。

【例】

カテゴリーＡ：2回／年で監査を実施

カテゴリーＢ：1回／年で監査を実施

カテゴリーＣ：1回／3年で監査を実施

【監査実施計画の雛形】

作成日：〇〇年〇〇月〇〇日

（情報セキュリティ監査実施者）

氏 名

〇〇年度 ××××大学情報セキュリティ管理体制の構築に関する監査実施計画書

１．監査目的

本学ポリシー、実施規程及びそれに基づく手順で定めた情報セキュリティ管理体制の構築状況に関し、体制図・設置規定等の文書及び当該責任者への質問により確認する。

２．背景

平成18年12月に国立大学法人等における情報システム運用ポリシーが策定され、本学でも従来のセキュリティポリシーを改訂し、新たに本学ポリシーを策定したところ、昨今、情報漏えい事案も頻発しており、本学における情報管理体制の再確認が必要である。

３．監査対象：本学情報セキュリティ管理体制の監査

４．被監査部門及び責任者：××××

５．監査実施責任者：△△△△

６．監査の実施時期：7月1日～9月30日の各月末の週（計15日間）

７．監査の実施場所：本学内執務室

８．監査の想定カバー率

対象となる責任者、管理者および利用者（対象となる者/全員）

対象となるシステム（対象システム数/全システム数）

対象となる端末（全端末数/全端末数）

９．実施する監査手続の概要：別紙のとおり

１０．監査の進捗管理手段：別紙のとおり

別紙

●監査手続の概要

遵守事項	対策内容	評価方法	実施時期	実施担当者
部局技術責任者の設置	設置	体制図の確認	・・・	・・・
		質問	・・・	・・・
	連絡網の整備	体制図の確認	・・・	・・・

●監査の進捗管理手段

１．定期報告の実施

２．・・・

7. 監査の実施

【手順策定者への補足説明：情報セキュリティ状況の変化の例】

・新しいシステムが開発又は導入されたとき

・新たに他のシステム又はネットワーク等と接続したとき

・学内における大きな人事異動や組織改編があったとき

・学内外を問わず重大なセキュリティ侵害があったとき

・本学ポリシー等が改訂又は追加されたとき

【手順利用者への補足説明：監査証拠の十分かつ適切な入手方法例】

・関連書類の査閲

・担当者への質問

・現場への視察

・システムテストへの立会い

・テストデータによる検証

・脆弱性スキャン、システム侵入テスト

【手順策定者への補足説明：評価方法の解説】

・質問：講じた対策、行為

・査閲：規程類、設定文書（設計書等の設定一覧等）、記録文書、文書証拠

・観察：日常の行為

・点検：物理的状態、システム上のセキュリティ設定

【手順利用者への補足説明：点検による評価における配慮事項】

点検という手法を採用する場合には、システム運用を停止させること等がないように配慮し、実際の操作は部局技術担当者等に行ってもらうことが望ましい。

【手順利用者への補足説明：自己点検票の利用等チェックリストによる監査実施における配慮事項】

事前に監査チェックリスト等を用意して監査を実施することは、監査業務の経験の浅い監査実施者が行う場合等に有効であるが、通常、監査の最終段階で監査手続が網羅的に行われたかをチェックするために使用することが効果的とされており、以下のことに留意して行うことが望ましい。

・効率性確保の観点 リスト上のチェック項目の意味や重要性をかんがみ、上から

下に順番に行ったり、同じような質問を繰り返したりしない。

・ 有効性検討の観点 チェック項目の内容が現実に合っているかを考慮しながら監査を実施する。

・ 網羅性確保の観点 チェックリストに記載されていない重要な項目がないか検討する。

【自己点検票の活用例】

	自己点検の対象となるセキュリティ対策項目の整理・分析					自己点検の設計										備考
	自己点検項目一覧の作成	本手順書との対応	分類			点検方法			実施時期&頻度		適用範囲			回答項目		監査における評価方法
			連続・単発	定期・不定期	頻度	随時点検型	一括点検型	断面調査型	自己点検の実施時期	自己点検の実施頻度	実施主体	管理者	責任者	回答項目	備考	
1	人事異動の際には、識別コードの管理を徹底すること。	4.1.3 (2) (g)	連続	定期	年4	○			実施時	実施時	権限管理を行う者	部局技術管理者	部局技術責任者	Yes 日時	—	点検
2	情報入手時には、格付け・取扱制限を明示す	3.2.1 (2) (b)	連続	不定期	毎日		○		月末	月1	部局技術責任者	上司	部局総括責任者	Yes No	アンケート併用	質問
3	ウイルスパターンを最新にするこ	4.2.2 (2) (c)	連続	不定期	週1			○	15日 30日	半月1	利用者	部局技術管理者	部局技術責任者	設定値	バージョン番号	点検
4	ソフト開発時にST確認すること	4.3.1 (1) (d)	単発	定期	年1	○			実施時	実施時	利用者	—	部局総括責任者	Yes 日時	—	質問
5	離席時には画面ロックすること。	3.2.2 (3) (b)	単発	不定期	毎日		○		月末	月1	利用者	上司	部局総括責任者	Yes No	—	質問
：	：	：	：	：	：	：	：	：	：	：	：	：	：	：	：	：
	Step 1-1	Step1-2	Step 1-3			Step 1-4			Step 1-5		Step 1-6			Step 1-7		Step 1-8

【準拠性判断の基準例（最大逸脱率が9%であることを90%の信頼度で確認する場合）】

・ 25件のサンプルのうち、1件も遵守事項違反がなければ、準拠しているものとする。

・ 25件のサンプルのうち、1件の遵守事項違反があっても、追加で20件のサンプルを選び、1件も遵守事項違反がなければ準拠しているものとする。

・ それ以外は準拠していないものとする。

【手順策定者への補足説明：重大な違反と軽微な違反の定義例】

・ 重大な違反とは、その違反単独で、又は他の違反と複合することにより、重大なリスクの発生を引き起こす可能性のあるものをいう。

・ 軽微な違反とは、重大な違反以外のものをいう。

【監査調書の雛形】

〇〇年〇〇月〇〇日

情報セキュリティ監査責任者 殿

（監査実施者）

署名

情報セキュリティ管理体制構築に係る情報セキュリティ監査の報告

平成〇〇年度情報セキュリティ管理体制の構築に関する監査実施計画に基づき、情報セキュリティ管理体制の構築状況を対象として監査を実施したので、以下のとおり報告する。

１．実施期間：××年××月××日から〇〇年〇〇月〇〇日まで

２．被監査部門及び責任者：・・・・・・

３．発見された問題点

(1) 重大な違反 ・・・・・・

(2) 軽微な違反 ・・・・・・

(3) 課題及び問題点等 ・・・・・・

４．意見

(1) 準拠性に関する保証意見 ・・・・・・

(2) 妥当性に関する助言意見 ・・・・・・

５．実施内容：別紙のとおり

別紙

順守事項	対策内容	評価方法	評価結果	サンプル		監査証拠		関連資料番号
				件数	抽出方法	形態	入手元	
部局技術責任者の設置	・・・	・・・	・・・	50/200	無作為	文書	第三者	001
	・・・	・・・	・・・	・・・	・・・	口頭	直接入手	－

8. 監査報告

【手順利用者への補足説明：監査報告書記載上の配慮事項】

・ 要約と詳細を分ける

・ 指摘事項等の対象となる部門や責任者をわかりやすく記述

・ 準拠性の違反等の事実と妥当性の助言意見については、分けて記述

・ 違反の事実については、重要性により区分けをし、記述

【監査報告書の雛形】

・準拠性監査報告書の雛形

〇〇年〇〇月〇〇日

全学総括責任者 殿

（情報セキュリティ監査責任者）

署 名

〇〇年度 ××××大学情報セキュリティ監査報告書

（準拠性監査報告）

平成〇〇年度情報セキュリティ監査計画に基づき、情報セキュリティの状況について準拠性監査を実施したところ、以下のとおり報告する。

1. 監査実施期間：××年××月××日から〇〇年〇〇月〇〇日まで
2. 監査対象範囲
   ・・・・・・
   ・・・・・・
3. 監査の基準：本学ポリシー及び当該請負契約書
4. 総合的所見：・・・・・・・・
5. 監査意見
   (1) 違反の有無
      ① 重大な違反 ・・・・・・
      ② 軽微な違反 ・・・・・・
   (2) 課題及び問題点 ・・・・・・
   (3) 助言意見 ・・・・・・
6. 添付資料
   (1) 平成〇〇年度×××に係る情報セキュリティ監査の報告
   (2) ・・・

なお、本職は、今回の監査対象の業務の実施には直接携わっておらず、十分な独立性を有しており、監査手続を実施した結果に基づいて、以上のとおり意見を表明するものである。

また、本報告書の利用は、本学における全学総括責任者及び部局総括責任者に限る。

・妥当性監査報告書の雛形

〇〇年〇〇月〇〇日

全学総括責任者 殿

（情報セキュリティ監査責任者）

署 名

〇〇年度 ××××大学情報セキュリティ監査報告書

（妥当性監査報告）

平成〇〇年度情報セキュリティ監査計画に基づき、情報セキュリティの状況について妥当性監査を実施したところ、以下のとおり報告する。

1. 監査実施期間：××年××月××日から〇〇年〇〇月〇〇日まで
2. 監査対象範囲

・・・・・・

・・・・・・

3. 監査の基準：本学ポリシー及び当該請負契約書
4. 総合的所見：・・・・・・・・
5. 監査意見
   (1) 課題及び問題点 ・・・・・・
   (2) 助言意見 ・・・・・・
6. 添付資料
   (1) 平成〇〇年度×××に係る情報セキュリティ監査の報告
   (2) ・・・

なお、本職は、今回の監査対象の業務の実施には直接携わっておらず、十分な独立性を有しており、監査手続を実施した結果に基づいて、以上のとおり意見を表明するものである。

また、本報告書の利用は、本学における全学総括責任者及び部局総括責任者に限る。