

北海道情報大学情報セキュリティ対策基準

第1章 総 則

(趣 旨)

第1条 この基準は、北海道情報大学情報セキュリティ対策基本規程第9条の規定に基づき、北海道情報大学（以下「本学」という。）における適切な情報セキュリティ対策に関する基準について必要な事項を定めるものとする。

(適用対象)

第2条 この基準において適用対象とする者は、本学情報システムを運用・管理する全ての者並びに利用者及び臨時利用者とする。

2 この基準において適用対象とする情報は、北海道情報大学情報セキュリティ対策基本規程第2条第1項第1号に定めるものをいう。

3 この基準において適用対象とする情報システムは、北海道情報大学情報セキュリティ対策基本規程第2条第1項第2号に定めるものをいう。

(定 義)

第3条 この基準において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

- (1) IPv6 (Internet Protocol Version 6) 移行機構 物理的に一つのネットワークにおいて、IPv4 (Internet Protocol Version 4) 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、サーバ装置及び端末並びに通信回線装置が2つの通信プロトコルを併用するデュアルスタック機構や、相互接続性の無い2つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。
- (2) アクセス制御 情報又は情報システムへのアクセスを許可する主体を制限することをいう。
- (3) アプリケーション OS (Operating System) 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。
- (4) アプリケーション・コンテンツ アプリケーションプログラム、ウェブコンテンツ等の総称をいう。
- (5) アルゴリズム ある特定の目的を達成するための演算手順をいう。
- (6) 暗号化 第三者が容易に復元することができないよう、定められた演算を施しデータを変換することをいう。
- (7) 暗号化消去 情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化 (Windows の BitLocker 等)、ハードウェアによる暗号化 (自己暗号化ドライブ (Self-Encrypting Drive) 等) などがある。
- (8) 暗号モジュール 暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。
- (9) Web 会議サービス 専用のアプリケーションやウェブブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器同士で通信を行うもの (テレビ会議システム等) は含まれない。
- (10) ウェブクライアント ウェブページを閲覧するためのアプリケーション (いわゆるブラウザ) 及び付加的な機能を追加するためのアプリケーションをいう。
- (11) 運用監視暗号リスト CRYPTREC が発行する「電子政府における調達のために参照すべき暗号のリスト (CRYPTREC 暗号リスト)」において、危殆化等により推奨すべきではないが、互換性維持のために継続利用を容認するものをいう。
- (12) S/MIME (Secure/Multipurpose Internet Mail Extensions) 公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。
- (13) 学外通信回線 通信回線のうち、学内通信回線以外のものをいう。

- (14) 学内通信回線 本学が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、本学の管理下でないサーバ装置又は端末が論理的に接続されていないものをいう。学内通信回線には、専用線やVPN (Virtual Private Network) 等物理的な回線を本学が管理していないものも含むものとする。

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

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

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

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

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

- (18) 基本方針 本学が定める「北海道情報大学情報セキュリティ対策基本方針」をいう。

- (19) 基本規程 本学が定める「北海道情報大学情報セキュリティ対策基本規程」をいう。

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

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

- (21) 業務継続計画 本学が策定する発災時に非常時優先業務を実施するための計画をいう。広義には、平常時からの取組等や復旧に関する計画も含むものとする。

- (22) 共用識別コード 複数の主体が共用するために付与された識別コードをいう。原則として、一つの識別コードは一つの主体のみに対して付与されるものであるが、情報システム上の制約や利用状況等に応じて、識別コードを組織で共用する場合もある。このように共用される識別コードを共用識別コードという。

- (23) 国の行政機関 法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第二十号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。

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

- (25) CRYPTREC (Cryptography Research and Evaluation Committees) 電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。
- (26) 権限管理 主体認証に係る情報(識別コード及び主体認証情報を含む。)及びアクセス制御における許可情報を管理することをいう。
- (27) サービス不能攻撃 悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。
- (28) 最小限の特権機能 管理者権限を実行できる範囲を必要最小限に制限する機能をいう。
- (29) CYMAT (サイマツト) サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team (情報セキュリティ緊急支援チーム)の略。
- (30) 識別 情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。
- (31) 識別コード 主体を識別するために、情報システムが認識するコード(符号)をいう。代表的な識別コードとして、ユーザIDが挙げられる。
- (32) 主体 情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。
- (33) 主体認証 識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。
- (34) 主体認証情報 主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。
- (35) 主体認証情報格納装置 主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、ICカード等がある。
- (36) 情報の抹消 電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会(CRYPTREC)によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録媒体を物理的に破壊すること等も含む。ただし、削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。
- (37) 推奨候補暗号リスト CRYPTREC 暗号リストにおいて、安全性及び実装性能は確認されているが、利用実績や普及見込みが十分ではないものをいう。
- (38) セキュリティパッチ 発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。
- (39) ソーシャルメディアサービス インターネット上において、ブログ、ソーシャルネットワークワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していくものをいう。
- (40) ソフトウェア サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OSやOS上で動作するアプリケーションを含む広義の意味である。
- (41) 耐タンパ性 暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。
- (42) DNS サーバ 名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させるサーバ装置をいう。DNSサーバは、その機能によって、自らが管理するドメ

イン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の２種類に分けることができる。

- (４３) テレワーク 情報通信技術（ICT＝Information and Communication Technology）を活用した、場所や時間を有効に活用できる柔軟な働き方のことをいう。テレワークの形態は、業務を行う場所に応じて、自宅で業務を行う在宅勤務、主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務、モバイル端末等を活用して移動中や出先で業務を行うモバイル勤務に分類される。
- (４４) 電子署名 情報の正当性を保証するための電子的な署名情報をいう。
- (４５) 電子政府推奨暗号リスト CRYPTREC 暗号リストにおいて、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストをいう。
- (４６) 電子メールクライアント 電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。
- (４７) 電子メールサーバ 電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。
- (４８) 特定用途機器 テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は内蔵電磁的記録媒体を備えているものをいう。
- (４９) ドメインネームシステム（DNS：Domain Name System） クライアント等からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係について回答を行うシステムである。
- (５０) ドメイン名 国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.do-johodai.ac.jp というウェブサイトの場合は、do-johodai.ac.jp の部分がこれに該当する。
- (５１) 取扱制限 情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを利用者等に確実に行わせるための手段をいう。
- (５２) 名前解決 ドメイン名やホスト名と IP アドレスを変換することをいう。
- (５３) VPN（Virtual Private Network） 暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。
- (５４) 複合機 プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。
- (５５) 不正プログラム コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。
- (５６) 不正プログラム定義ファイル 不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。
- (５７) 踏み台 悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。
- (５８) MAC アドレス（Media Access Control address） 機器等が備える有線 LAN や無線 LAN のネットワークインタフェースに割り当てられる固有の認識番号である。識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割り当てる番号の組合せによって表される。
- (５９) 抹消 本条第３６号「情報の抹消」参照
- (６０) 無線 LAN IEEE802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ad、802.11ax 等の規格により、無線通信で情報を送受信する通信回線をいう。
- (６１) 明示等 情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

- (62) 要安定情報 可用性2情報をいう。
- (63) 要管理対策区域 機関等の管理下にある区域（機関等が外部の組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。
- (64) 要機密情報 機密性2情報及び機密性3情報をいう。
- (65) 要保護情報 要機密情報、要保全情報及び要安定情報に一つでも該当する情報をいう。
- (66) 要保全情報 完全性2情報をいう。
- (67) リスク 目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。
- (68) 利用者等 利用者及び臨時利用者のほか、本学の情報システムを取り扱う者をいう。
- (69) ルートヒントファイル 最初に名前解決を問い合わせる DNS コンテンツサーバ（以下「ルートDNS」という。）の情報をいう。ルートヒントファイルには、ルートDNSのサーバ名とIPアドレスの組が記載されており、ルートDNSのIPアドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC（Internet Network Information Center）のサイトから入手可能である。
- (70) 例外措置 利用者等がポリシー並びにそれに基づく規程及び手順等を遵守することが困難な状況で、教育研究事務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

第2章 導入・計画

第1節 対策推進計画の策定

（対策推進計画の策定）

第4条 総括責任者は、情報セキュリティ委員会における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めるものとする。

2 前項の対策推進計画には、本学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに次の各号に掲げる取組の方針・重点及びその実施時期を含めるものとする。

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

第3章 運用

第1節 情報セキュリティ関係規程の運用

（情報セキュリティ対策に関する実施手順の整備・運用）

第5条 情報センター長は、本学における情報セキュリティ対策に関する実施手順を整備（本規程で整備すべき者を別に定める場合を除く。）し、実施手順に関する事務を統括し、整備状況について総括責任者に報告するものとする。

2 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、終了及び人事異動時等（入学、卒業を含む。）に関する管理の規定を整備するものとする。

3 情報システム管理室長は、総括責任者が規定した情報セキュリティ対策推進体制の役割に応じた必要な事務を遂行するものとする。

4 部局責任者は、利用者等から情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、情報センター長に報告するものとする。

- 5 情報センター長は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて総括責任者にその内容を報告するものとする。

(違反への対処)

第6条 利用者等は、情報セキュリティ関係規程への重大な違反を知った場合は、部局責任者にその旨を報告するものとする。

- 2 部局責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、情報センター長を通じて、総括責任者に報告するものとする。

第2節 例外措置

(例外措置手続の整備)

第7条 総括責任者は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び審査手続を定めるものとする。

- 2 情報センター長は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めるものとする。

(例外措置の審査手続)

第8条 総括責任者は、例外措置について次の各号に掲げるものを含めた手続を定めるものとする。

- (1) 例外措置の許可権限者
- (2) 事前申請の原則その他の申請方法
- (3) 審査項目その他の審査方法
 - ・ 申請者の情報（氏名、所属、連絡先）
 - ・ 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
 - ・ 例外措置の適用を申請する期間
 - ・ 例外措置の適用を申請する措置内容（講ずる代替手段等）
 - ・ 例外措置により生じる情報セキュリティ上の影響と対処方法
 - ・ 例外措置の適用を終了した旨の報告方法
 - ・ 例外措置の適用を申請する理由

(例外措置の適用審査記録の台帳)

第9条 許可権限者は、例外措置の適用審査記録に次の各号に掲げる内容を記載し、適用審査記録の台帳として保管するとともに、情報センター長へ定期的に報告するものとする。

- (1) 審査した者の情報（氏名、役割名、所属、連絡先）
- (2) 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
- (3) 審査結果の内容
 - ・ 許可又は不許可の別
 - ・ 許可又は不許可の理由
 - ・ 例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等）
 - ・ 例外措置の適用を許可した期間
 - ・ 許可した措置内容（講ずるべき代替手段等）
 - ・ 例外措置を終了した旨の報告方法

(例外措置の運用)

第10条 例外措置の適用を受けたい利用者等は、定められた審査手続に従い、許可権限者に規定

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

- 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ものとする。
- 3 許可権限者は、例外措置の申請状況を台帳に記録し、情報センター長に報告するものとする。
- 4 情報センター長は、その必要に応じ、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行うものとし、その検討結果を総括責任者に報告するものとする。

第3節 教 育

(教育体制等の整備)

- 第11条 総括責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備するものとする。
- 2 総括責任者は、情報セキュリティの状況の変化に応じ、利用者等に対して新たに教育すべき事項が明らかになった場合には、教育実施計画を見直すものとする。

(教育のための資料の整備)

- 第12条 総括責任者は、利用者等の役割に応じて教育すべき内容を検討し、教育のための資料を整備するものとする。

(教育実施計画の策定)

- 第13条 総括責任者は、利用者等が毎年度最低1回は教育を受講できるように、教育実施計画を立案するとともに、その実施体制を整備するものとする。

(教育実施体制の整備)

- 第14条 総括責任者は、利用者等の入学、着任又は学外からの異動後、3か月以内に受講できるように、その実施体制を整備するものとする。

(教育の実施)

- 第15条 総括責任者は、利用者等に対して、情報セキュリティ関係規程に係る教育を適切に受講させるものとする。
- 2 利用者等は、教育実施計画に従って、適切な時期に教育を受講するものとする。
- 3 総括責任者は、CSIRTに属する職員に教育を適切に受講させなければならないものとする。
- 4 部局責任者は、教育の実施状況を記録し、総括責任者及び情報センター長に報告するものとする。
- 5 部局責任者は、教育の実施状況を分析・評価し、総括責任者に情報セキュリティ対策に関する教育の実施状況について報告するものとする。

第4節 情報セキュリティインシデントへの対処

(情報セキュリティインシデントに備えた事前準備)

- 第16条 情報センター長は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む本学関係者への報告手順を整備し、報告が必要な具体例を含め、利用者等に周知するものとする。
- 2 情報センター長は、情報セキュリティインシデントを認知した際の学外との情報共有を含む対処手順を整備するものとする。
- 3 情報センター長は、情報セキュリティインシデントの可能性に備え、教育研究事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備するものとする。
- 4 情報センター長は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、教育研究事務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備す

るものとする。

- 5 情報センター長は、情報セキュリティインシデントについて学外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を学外の者に明示するものとする。
- 6 情報センター長は、対処手順が適切に機能することを訓練等により確認するものとする。

(情報セキュリティインシデント発生時の対処と報告に係る対策)

- 第17条 情報センター長は、学校法人電子開発学園北海道情報大学学則第16章に定める図書館、学習支援センター、保健センター、情報センター、学生寮及び教育研究施設（以下「附属施設」という。）における情報セキュリティインシデント発生が報告された際にも、本学における情報セキュリティインシデントの場合と同様に、総括責任者や定められている関係機関に速やかに報告されるよう手順を定めるものとする。
- 2 情報センター長は、情報セキュリティインシデント発生時の対処手順のうち、意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等をあらかじめ定めておくものとする。
 - 3 情報センター長は、附属施設において発生した情報セキュリティインシデントについて、当該附属施設から報告・連絡を受ける窓口について定めるとともに、各機関にその窓口の連絡先を周知するものとする。

(情報セキュリティインシデントへの対処)

- 第18条 利用者等は、情報セキュリティインシデントの可能性を認知した場合には、本学の報告窓口に報告し、指示に従わなければならないものとする。
- 2 CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うものとする。
 - 3 CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、総括責任者に速やかに報告するものとする。
 - 4 CSIRT は、情報セキュリティインシデントに関係する部局責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行うものとする。
 - 5 部局情報システム管理責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、本学で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処するものとする。
 - 6 部局情報システム管理責任者は、認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処するものとする。
 - 7 CSIRT は、本学の情報システムについて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、予め定められている関係機関に連絡するものとする。
 - 7 CSIRT は、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うものとする。
 - 8 CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて対処全般に関する指示、勧告又は助言を行うものとする。
 - 9 CSIRT は、情報セキュリティインシデントに関する対処の内容を記録するものとする。
 - 10 CSIRT は、情報セキュリティインシデントに関して、本学を含む関係機関と情報共有を行うものとする。

(CSIRT における情報共有と役割分担に係る対策)

- 第19条 CSIRT は、情報セキュリティインシデントではないと評価した場合であっても、注意喚起が必要と考えられるものについては、関係する者に情報共有を行わなければならない。
- 2 CSIRT 責任者は、認知した情報セキュリティインシデントの種類や規模、影響度合い等を勘案し、必要に応じて、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局の役割分担を見直すものとする。

(情報セキュリティインシデントの再発防止・教訓の共有)

- 第20条 部局責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止

策を検討し、それを報告書として総括責任者に報告するものとする。

- 2 総括責任者は、部局責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示するものとする。
- 3 CSIRT 責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、情報センター長、関係する部局責任者等に共有するものとする。

第4章 点 検

第1節 情報セキュリティ対策の自己点検

(自己点検計画の策定・手順の準備)

第21条 情報センター長は、対策推進計画に基づき年度自己点検計画を策定するものとする。

- 2 情報システム管理室長は、利用者等ごとの自己点検票及び自己点検の実施手順を整備するものとする。
- 3 情報センター長は、情報セキュリティの状況の変化に応じ、利用者等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直すものとする。

(自己点検の実施)

第22条 情報システム管理室長は、年度自己点検計画に基づき、利用者等に自己点検の実施を指示するものとする。

- 2 利用者等は、情報システム管理室長から指示された自己点検票及び自己点検の手順を用いて自己点検を実施するものとする。

(自己点検結果の評価・改善)

第23条 情報センター長及び情報システム管理室長は、利用者等による自己点検結果を分析・評価し、情報センター長は、その評価結果を総括責任者に報告するものとする。

- 2 総括責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、情報センター長及び情報システム管理室長に改善を指示し、改善結果の報告を受けものとする。

第5章 見直し

第1節 情報セキュリティ対策の見直し

(情報セキュリティ関係規程の見直し)

第24条 総括責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、本基準を含むポリシー及びそれに基づく規程等について必要な見直しを行わなければならない。

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

(対策推進計画の見直し)

第25条 総括責任者は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について定期的な見直しを行うものとする。

第6章 情報の取扱い

第1節 情報の取扱い

(情報の取扱いに係る規定の整備)

第26条 総括責任者は、次の各号に掲げるものを含む情報の取扱いに関する規定を整備し、教職員等へ周知するものとする。

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

(情報の取扱いに係る手順の整備)

第27条 情報センター長は、情報の取扱いに関し定めるため、次の各号に掲げるものを例とする手順を整備するものとする。

- (1) 情報のライフサイクル全般にわたり必要な手順（教育研究事務の遂行以外の目的で情報を利用等しないよう努めること等）
- (2) 情報の入手・作成時の手順
- (3) 情報の利用・保存時の手順
- (4) 情報の提供・公表時の手順
- (5) 情報の運搬・送信時の手順
- (6) 情報の消去時の手順
- (7) 情報のバックアップ時の手順

(格付と取扱制限の明示に係る規定の整備)

第28条 情報センター長は、情報の格付及び取扱制限の明示の方法について、次の各号に掲げるものを例とする規定を整備するものとする。

- (1) 電磁的記録として取り扱われる情報に明示する場合
 - ・ 電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載
 - ・ 電磁的ファイル等の取扱単位ごとにファイル名自体へ記載
 - ・ フォルダ単位等で取り扱う情報は、フォルダ名に記載
 - ・ 電子メールで取り扱う情報は、メール本文又はメール件名に記載
- (2) 外部電磁的記録媒体に保存して取り扱う情報に明示する場合
 - ・ 保存する電磁的ファイル又は文書等の単位ごとに記載
 - ・ 外部電磁的記録媒体本体に記載
- (3) 書面に印刷されることが想定される場合
 - ・ 書面のヘッダ部分等に記載
 - ・ 冊子等の単位で取り扱う場合は、冊子の表紙、裏表紙等に記載
- (4) 既に書面として存在している情報に対して格付や取扱制限を明示する場合
 - ・ 手書きによる記入
 - ・ スタンプ等による押印

2 情報センター長は、情報の格付及び取扱制限の明示を省略する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、規定を整備するものとする。

(格付と取扱制限の継承、見直しに係る規定の整備)

第29条 情報センター長は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、次の各号に掲げるものを例に、規定を整備するものとする。

- (1) 情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付及び取扱制限を継承するものとする。
- (2) 既存の情報に、より機密性の高い情報を追加するときは、格付及び取扱制限を見直すものとする。
- (3) 機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直すものとする。
- (4) 情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承するものとする。

- (5) 完全性及び可用性については、作成時又は複製時に適切な格付を決定するものとする。
- (6) 他者が決定した情報の格付及び取扱制限を見直す必要がある場合には、その決定者（決定について引き継いだ者を含む。）又はその上司に確認を求めるものとする。

（情報の目的外での利用等の制限）

第30条 教職員等は、自らが担当している教育研究事務の遂行以外の目的で、情報を利用等しないよう努めなければならない。

（情報の格付及び取扱制限の決定・明示等）

第31条 教職員等は、情報の作成時及び学外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等するものとする。

- 2 教職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承するものとする。
- 3 教職員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司に確認し、その結果に基づき見直すものとする。

（情報の利用・保存）

第32条 教職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱わなければならない。

- 2 教職員等は、機密性3情報について要管理対策区域外で情報処理を行う場合は、部局情報システム管理責任者及び総括責任者の許可を得なければならない。
- 3 教職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講じなければならない。
- 4 教職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理するものとする。なお、機密性3情報を機器等に保存する際、以下の措置を講じなければならない。
 - (1) 機器等に保存する場合は、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用すること。
 - (2) 当該情報に対し、暗号化による保護を行うこと。
 - (3) 当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずること。
- 5 教職員等は、USBメモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従わなければならない。

（格付と取扱制限に応じた情報の取扱い）

第33条 教職員等は、情報の格付及び取扱制限に応じて、情報を次の各号に掲げるとおり取り扱わなければならない。

- (1) 要保護情報を放置しないこと。
 - (2) 要機密情報を必要以上に複製しないこと。
 - (3) 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずること。
 - (4) 電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずること。
 - (5) 情報の保存方法を変更する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずること。
- 2 教職員等は、入手した情報の格付及び取扱制限が不明な場合には、情報の作成元又は入手元への確認を行わなければならない。

（情報の提供・公表）

第34条 教職員等は、情報を公表する場合には、当該情報が機密性1情報に格付されるものであ

ることを確認するものとする。

- 2 教職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従わなければならない。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱上の留意事項を確実に伝達するなどの措置を講じなければならない。
- 3 教職員等は、機密性3情報を閲覧制限の範囲外の者に提供する場合には、総括責任者の許可を得なければならない。
- 4 教職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講じなければならない。

(電磁的記録媒体の第三者提供)

第35条 教職員等は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消するものとする。

(情報の運搬・送信)

第36条 教職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずるものとする。教職員等が機密性3情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、総括責任者が指定する方法により運搬するものとする。ただし、他機関等の要管理対策区域であって、総括責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。

- 2 教職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずるものとする。教職員等が、機密性3情報を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、総括責任者が指定する方法により送信するものとする。ただし、大学等において、機密性3情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができるものとする。

(情報の運搬を第三者に依頼する場合の対策)

第37条 教職員等は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬するものとする。

(情報漏えいの防止、情報の改ざんの防止)

第38条 教職員等は、要機密情報である電磁的記録を要管理対策区域外に運搬又は学外通信回線を使用して送信する場合には、情報漏えいを防止するため、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) 運搬又は送信する情報を暗号化すること。
- (2) 要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬又は送信すること。
- (3) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用すること。

(情報の送信に係る対策)

第39条 教職員等は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、次の各号に掲げるものを例に当該情報の送信の手段を決定するものとする。

- (1) 本学管理の通信回線を用いて送信する。
- (2) 信頼できる通信回線を使用して送信する。
- (3) VPNを用いて送信する。
- (4) S/MIME等の暗号化された電子メールを使用して送信する。
- (5) 本学独自で運用しているあるいは主体となって契約したセキュリティが十分確保されているウェブメールサービス又はオンラインストレージ環境を利用する。

(情報の消去)

第40条 教職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去するものとする。

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

3 教職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にしなければならない。

(リース契約で調達した端末等における情報の消去)

第41条 教職員等は、端末やサーバ装置等をリース契約で調達する場合は、契約終了に伴う返却時の情報の抹消方法及び履行状況の確認手段について、次の各号に掲げるものを例とする対策を行うものとする。

(1) リース契約の調達仕様書に記載し、契約内容にも含めること。

(2) リース契約終了に伴う情報の抹消について、役務提供契約を別途締結する本学管理の通信回線を用いて送信すること。

(情報のバックアップ)

第42条 教職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施するものとする。

2 教職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理するものとする。

3 教職員等は、保存期間を過ぎた情報のバックアップについては、第40条及び第41条の規定に従い、適切な方法で消去、抹消又は廃棄するものとする。

(要保全情報又は要安定情報のバックアップの取得)

第43条 教職員等は、要保全情報又は要安定情報である電磁的記録又は重要な設計書について、バックアップを取得するものとする。

(要保全情報又は要安定情報のバックアップの保管)

第44条 教職員等は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップの保管について、災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定するものとする。

第2節 情報を取り扱う区域の管理

(要管理対策区域における対策の基準の決定)

第45条 統括責任者は、要管理対策区域の範囲を定めるものとする。

2 統括責任者は、要管理対策区域の特性に応じて、次の各号に掲げる観点を含む対策の基準を定めるものとする。

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

(2) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策

(要管理対策区域における対策)

第46条 統括責任者は、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）として、次に掲げる3段階のクラスを定めるものとする。

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

	するための対策を実施する必要がある区域
クラス1	クラス3、クラス2以外の要管理対策区域

- ※ 便宜上、要管理対策区域外の区域はクラス0と呼び、クラス0<クラス1<クラス2<クラス3の順位を設ける。クラス0が最も下位のクラス、クラス3が最も上位のクラスとなる。
- 2 統括責任者は、クラス1の区域について、次の各号に掲げるものを含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めるものとする。
- (1) クラス1の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。
 - (2) クラス1の区域への立入りを許可されていない者が容易に立ち入らないように、立ち入る者の身元、訪問目的等の確認を行うための措置を講ずること。また、出入口が無になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。
 - (3) 要管理対策区域に不正に立ち入った者を容易に判別することができるように、次に掲げるものを含む措置を講ずること。
 - ・ 教職員等は、身分証明書等を着用、明示する。クラス2及びクラス3の区域においても同様とする。
 - ・ 一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス2及びクラス3の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。
- 3 統括責任者は、クラス2の区域について、次の各号に掲げるものを含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めるものとする。
- (1) クラス2の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分するものとする。ただし、窓口のある教室、研究室、事務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は教職員等が窓口を常に目視できるような措置を講ずるものとする。
 - (2) クラス2の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠するものとする。
 - (3) クラス2の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずるものとする。
- 4 統括責任者は、クラス3の区域について、次の各号に掲げるものを含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めるものとする。
- (1) クラス3の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分するものとする。
 - (2) クラス3の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずるものとする。
 - (3) クラス3の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにするものとする。
 - (4) 一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずるものとし、業者が作業を行う場合は、立会いや監視カメラ等により監視するための措置を講ずるものとする。
- 5 統括責任者は、区域へのクラスの割当ての基準を次の各号に掲げるものを含め定めるものとする。
- (1) サーバ室や日常的に機密性が高い情報を取り扱う研究室、事務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス3を割り当てる。
 - (2) 一般的な研究室、事務室や会議室には、教職員等及び関係の学生等以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること

と等を防止するために、クラス2を割り当てる。

(区域ごとの対策の決定)

第47条 部局責任者は、統括責任者が定めた対策の基準を踏まえ、施設及び教育研究事務の執務環境に係る対策を行う単位ごとの区域を定めるものとする。

2 部局責任者は、管理する区域について、情報センター長が定めた対策の基準と、周辺環境や当該区域で行う教育研究事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定するものとする。

(区域ごとに実施する対策)

第48条 部局責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と周辺環境や当該区域で行う教育研究事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定するものとする。この場合において、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定するものとする。

(要管理対策区域における対策の実施)

第49条 部局責任者は、管理する区域に対して定めた対策を実施するものとし、利用者等が実施すべき対策については、利用者等が認識できる措置を講ずるものとする。

2 部局責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずるものとする。

3 利用者等は、利用する区域について部局責任者が定めた対策に従って利用し、利用者等が学外の者を立ち入らせる際には、当該学外の者にも当該区域で定められた対策に従って利用するものとする。

(要管理対策区域における利用手順等の整備)

第50条 部局責任者は、管理する区域について、次の各号に掲げるものを例とする利用手順等を整備し、当該区域を利用する利用者等に周知するものとする。

(1) 扉の施錠及び開閉に関する利用手順

(2) 一時的に立ち入る者が許可された者であることを確認するための手順

(3) 一時的に立ち入る者を監視するための手順

第7章 業務委託

第1節 業務委託

(業務委託に係る規定の整備)

第51条 情報センター長は、業務委託に係る次の各号に掲げる内容を含む規定を整備するものとする。

(1) 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準

(2) 委託先の選定基準

(業務委託に係る契約)

第52条 部局責任者は、委託判断基準に従って業務委託を実施しなければならない。

2 部局責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定し、次の各号に掲げる内容を含む情報セキュリティ対策を実施することを委託先の選定条件として、仕様内容にも含めなければならない。

(1) 委託先に提供する情報の委託先における目的外利用の禁止

(2) 委託先における情報セキュリティ対策の実施内容及び管理体制

(3) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者によって、本学の意図しない変更が加えられないための管理体制

(4) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門

性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

- (5) 情報セキュリティインシデントへの対処方法
 - (6) 情報セキュリティ対策その他の契約の履行状況の確認方法
 - (7) 情報セキュリティ対策の履行が不十分な場合の対処方法
- 3 部局責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて次の各号に掲げる内容を仕様を含めるものとする。
- (1) 情報セキュリティ監査の受入れ
 - (2) サービスレベルの保証
- 4 部局責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、第2項及び前項の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本学に提供し、本学の承認を受けるよう、仕様内容に含めるものとする。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断するものとする。

（業務委託に係る対策）

- 第53条 部局責任者は、次の各号に掲げる内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させるものとし、変更があった場合は、速やかに再提出させるものとする。
- (1) 当該委託業務に携わる者の特定
 - (2) 当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容
- 2 部局責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱うものとする。

（業務委託における対策の実施）

- 第54条 部局責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認するものとする。
- 2 部局責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を利用者等から受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせるものとする。
- 3 部局責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却又は抹消されたことを確認するものとする。

（業務委託における情報の取扱い）

- 第55条 利用者等は、委託先への情報の提供等において、次の各号に掲げる事項を遵守するものとする。
- (1) 委託先に要保護情報を提供する場合は、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。
 - (2) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。
 - (3) 委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに部局責任者に報告すること。

第8章 外部サービスの利用

第1節 要機密情報を取り扱う場合

（外部サービスの利用に係る規定の整備）

- 第56条 情報センター長は、次の各号に掲げるものを含む外部サービス（要機密情報を取り扱う場合）の利用に関する規定を整備し、当該サービスの利用においては要機密情報が取り扱われないよう規定するものとする。
- (1) 外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下本節において「外部サービス利用判断基準」という。）

- (2) 外部サービス提供者の選定基準
- (3) 外部サービスの利用申請の許可権限者と利用手続
- (4) 外部サービス管理者の指名と外部サービスの利用状況の管理

(外部サービスの利用に係る規定の整備)

第57条 情報センター長は、第51条第1項第2号で整備を求めている「委託先の選定基準」と同等の規定となるよう外部サービス提供者の選定基準を策定するものとする。また、クラウドサービス選定における外部サービス提供者の選定基準は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」（以下「ISMAP」という。）の管理基準に従い策定するものとする。

2 総括責任者は、本学において要機密情報を取り扱う場合の外部サービスの利用手続を、次に掲げるものを例に定めるものとする。

- (1) 利用申請の許可権限者
- (2) 申請内容
 - ・外部サービスの名称（必要に応じて機能名までを含む）
 - ・外部サービスの種類（クラウドサービスか否か）
 - ・外部サービス提供者の名称
 - ・利用目的（業務内容）
 - ・取り扱う情報の格付
 - ・利用期間
 - ・利用申請者（所属・氏名）
 - ・利用者の範囲（学内に限る、部局内に限る など）
 - ・選定時の確認結果

3 総括責任者は、本学において要機密情報を取り扱う場合の外部サービスの利用手続を、次の各号に掲げるものを例に定めるものとする。

- (1) 利用申請の許可権限者は、申請ごとに外部サービスの管理者を指名すること。
- (2) 利用承認した外部サービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新の外部サービスの利用状況を把握できるようにすること。記録する際は、次に掲げるものを例に項目を記録し、学内で共有すること。
 - ・外部サービスの名称（必要に応じて機能名までを含む）
 - ・外部サービスの種類（クラウドサービスか否か）
 - ・外部サービス提供者の名称
 - ・利用目的（業務内容）
 - ・取り扱う情報の格付
 - ・利用期間
 - ・利用申請者（所属・氏名）
 - ・利用者の範囲（学内に限る、部局内に限る など）
 - ・外部サービスの管理者（所属・氏名）

(外部サービスの選定（クラウドサービスの場合）)

第58条 部局責任者又は部局情報システム管理責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討するものとする。

2 部局責任者又は部局情報システム管理責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定するものとする。また、業務に特有のリスクが存在する場合には、必要な情報セキュリティ対策を外部サービス提供者の選定条件に含めるものとする。

3 部局責任者又は部局情報システム管理責任者は、取り扱う情報の格付及び取扱制限並びに外部サービスとの情報セキュリティに関する役割及び責任の範囲を踏まえてセキュリティ要件を定め、外部サービスを選定するものとする。

(クラウドサービスのセキュリティ要件策定)

第59条 部局責任者又は部局情報システム管理責任者は、クラウドサービスのセキュリティ要件策定に当たっては、ISMAP 管理基準の管理策基準が求める対策と同等以上の水準を求めるものとする。

(外部サービスの選定(クラウドサービス以外の場合))

第60条 部局責任者又は部局情報システム管理責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討するものとする。

2 部局責任者又は部局情報システム管理責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定するものとする。また、次の各号に掲げる内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めるものとする。

- (1) 外部サービスの利用を通じて本学が取り扱う情報の外部サービス提供者における目的外利用の禁止
- (2) 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制
- (3) 外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本学の意図しない変更が加えられないための管理体制
- (4) 外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報提供
- (5) 情報セキュリティインシデントへの対処方法
- (6) 情報セキュリティ対策その他の契約の履行状況の確認方法
- (7) 情報セキュリティ対策の履行が不十分な場合の対処方法

3 部局責任者又は部局情報システム管理責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めるものとする。

4 部局責任者又は部局情報システム管理責任者は、外部サービスの利用を通じて本学が取り扱う情報の格付等を勘案し、必要に応じて次の各号に掲げる内容を外部サービス提供者の選定条件に含めるものとする。

- (1) 情報セキュリティ監査の受入れ
- (2) サービスレベルの保証

5 部局責任者又は部局情報システム管理責任者は、外部サービスの利用を通じて本学が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本学の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めるものとする。

6 部局責任者又は部局情報システム管理責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本学に提供し、本学の承認を受けるよう、外部サービス提供者の選定条件に含めるものとする。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断するものとする。

7 部局責任者又は部局情報システム管理責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定するものとする。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めるものとする。

8 部局責任者又は部局情報システム管理責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めるものとする。

9 部局責任者又は部局情報システム管理責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断するものとする。

(外部サービスの選定(クラウドサービス以外の場合))

第61条 部局責任者又は部局情報システム管理責任者は、外部サービス提供者との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について外部サービス提供者と合意し、定められた手順により情報を取り扱うものとする。

2 部局責任者又は部局情報システム管理責任者は、外部サービスを利用するに当たり、サービス

の中断や終了時に際し、円滑に業務を移行するための対策として、次の各号に掲げるものを例とするセキュリティ対策を実施することを外部サービスの選定条件とし、仕様内容にも含めるものとする。

- (1) 取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件
- (2) 取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

3 部局責任者又は部局情報システム管理責任者は、外部サービス部分を含む情報の流通経路全般にわたるセキュリティ対策を構築するものとする。また、対策を実現するために、次の各号に掲げるものを例とするセキュリティ要件を外部サービスに求め、契約内容にも含めるものとする。

- (1) 外部サービスに係るアクセスログ等の証跡の保存及び提供
- (2) 外部サービスのインターネット回線とクラウド基盤の接続点の通信の監視
- (3) 外部サービス提供者による情報の管理・保管の実施内容の確認
- (4) 外部サービス上の脆弱性対策の実施内容の確認
- (5) 外部サービス上の情報に係る復旧時点目標（RPO）等の指標
- (6) 外部サービス上で取り扱う情報の暗号化
- (7) 外部サービス利用者の意思による外部サービス上で取り扱う情報の確実な削除・廃棄
- (8) 外部サービス利用者が求める情報開示請求に対する開示項目や範囲の明記

（外部サービスの利用に係る調達・契約）

第62条 部局責任者又は部局情報システム管理責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様にも含めるものとする。

2 部局責任者又は部局情報システム管理責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約にも含めるものとする。

（外部サービスにおける役割及び責任の範囲の明確化）

第63条 部局責任者又は部局情報システム管理責任者は、調達仕様の内容を契約にも含める際、外部サービス提供者との情報セキュリティに関する役割及び責任の範囲が明確になっていることを確認するものとする。

（外部サービスの利用承認）

第64条 部局責任者又は部局情報システム管理責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うものとする。

- 2 利用申請の許可権限者は、教職員等による外部サービスの利用申請を審査し、利用の可否を決定するものとする。
- 3 利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名するものとする。

（外部サービスを利用した情報システムの導入・構築時の対策）

第65条 情報センター長は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、次の各号に掲げるものを含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定するものとする。

- (1) 不正なアクセスを防止するためのアクセス制御
- (2) 取り扱う情報の機密性保護のための暗号化
- (3) 開発時におけるセキュリティ対策
- (4) 設計・設定時の誤りの防止

2 外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録するものとする。

（外部サービスを利用した情報システムの導入・構築時の対策）

第66条 情報センター長は、構築時におけるアクセス制御に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 外部サービスを利用する際に外部サービス提供者が付与又は外部サービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理
 - (2) 外部サービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御
 - (3) 外部サービスを利用する情報システムの管理者特権を保有する外部サービス利用者に対する強固な認証技術の利用
 - (4) 外部サービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことの確認
 - (5) 外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御できることの確認
 - (6) 外部サービス利用者による外部サービスに多大な影響を与える操作の特定と誤操作の抑制
 - (7) 外部サービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施
 - (8) インターネット等の学外通信回線から学内通信回線を経由せずに外部サービス上に構築した情報システムにログインすることの可否の判断と認める場合の適切なセキュリティ対策の実施
- 2 情報センター長は、構築時における暗号化に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。
- (1) 外部サービス内及び通信経路全般における暗号化の確認
 - (2) 利用する情報システムに係る法令や規則に対する暗号化方式の遵守度合い
- 3 情報センター長は、構築時における開発に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。
- (1) 情報システムの構築において外部サービスを利用する場合の外部サービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用
 - (2) 情報システムの構築において、外部サービス上に他ベンダーが提供するソフトウェア等を導入する場合のそのソフトウェアの外部サービス上におけるライセンス規定
- 4 情報センター長は、構築時における設計・設定に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。
- (1) 外部サービス上に情報システムを構築する際の外部サービス提供者への設計、構築における知見等の情報の要求とその活用
 - (2) 外部サービス上に情報システムを構築する際の設定の誤りを見いだすための対策
 - (3) 外部サービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視
 - (4) 利用する外部サービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測
 - (5) 利用する外部サービス上で要安定情報を取り扱う場合の可用性を考慮した設計
 - (6) 外部サービス内における時刻同期の方法の確認

(外部サービスを利用した情報システムの運用・保守時の対策)

第67条 情報センター長は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次の各号に掲げるものを含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定するものとする。

- (1) 外部サービス利用方針の規定
 - (2) 外部サービス利用に必要な教育
 - (3) 取り扱う資産の管理
 - (4) 不正アクセスを防止するためのアクセス制御
 - (5) 取り扱う情報の機密性保護のための暗号化
 - (6) 外部サービス内の通信の制御
 - (7) 設計・設定時の誤りの防止
 - (8) 外部サービスを利用した情報システムの事業継続
- 2 部局責任者又は部局情報システム管理責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備するものとする。
- 3 部局情報システム管理責任者は、前各項において定める規定に対し、運用・保守時に実施状況

を定期的に確認・記録するものとする。

(外部サービスを利用した情報システムの運用・保守時の対策)

第68条 情報センター長は、運用・保守時における利用方針に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 責任分界点を意識した外部サービスの利用
- (2) 利用承認を受けていない外部サービスの利用禁止
- (3) 外部サービス提供者に対する定期的なサービスの提供状態の確認
- (4) 利用する外部サービスに係る情報セキュリティインシデント発生時の連絡体制

2 情報センター長は、運用・保守時における教育に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 外部サービス利用のための規定及び手順について
- (2) 外部サービス利用に係る情報セキュリティリスクとリスク対応について
- (3) 外部サービス利用に関する適用法令や関連する規制等について

3 情報センター長は、運用・保守時における資産管理に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 外部サービス上で利用する IT 資産の適切な管理
- (2) 外部サービス上に保存する情報に対する適切な格付・取扱制限の明示
- (3) 外部サービスの機能に対する脆弱性対策について、外部サービス利用者の責任範囲の明確化と対策の実施

4 情報センター長は、運用・保守時におけるアクセス制御に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 管理者権限を外部サービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録
- (2) 外部サービス利用者に割り当てたアクセス権限に対する定期的な見直し
- (3) 外部サービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限
- (4) 利用する外部サービスの不正利用の監視

5 情報センター長は、運用・保守時における暗号化に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 暗号化に用いる鍵の管理者と鍵の保管場所
- (2) 鍵管理機能を外部サービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価
- (3) 鍵管理機能を外部サービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

6 情報センター長は、運用・保守時における通信に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 利用する外部サービスのネットワーク基盤が他のネットワークと分離されていることの確認

7 情報センター長は、運用・保守時における設計・設定に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 外部サービスの設定を変更する場合の設定の誤りを防止するための対策
- (2) 外部サービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施

8 情報センター長は、運用・保守時における事業継続に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施又は外部サービス提供者が提供する機能を利用する場合は、その実施の確認
- (2) 要安定情報を外部サービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施
- (3) 外部サービス提供者からの変更通知の内容確認と復旧手順の確認
- (4) 外部サービスで利用しているデータ容量、性能等の監視

9 部局責任者は、運用・保守時におけるインシデント対応に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 外部サービス上での情報セキュリティインシデント、情報の目的外利用等を認知した場合の部局情報システム管理責任者への報告
- (2) 部局情報システム管理責任者がインシデント報告を受けた場合の対応

(外部サービスを利用した情報システムの更改・廃棄時の対策)

第69条 情報センター長は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次の各号に掲げるものを含む外部サービスの利用を終了する際のセキュリティ対策を規定するものとする。

- (1) 外部サービス利用終了時における対策
 - (2) 外部サービスで取り扱った情報の廃棄
 - (3) 外部サービスの利用のために作成したアカウントの廃棄
- 2 外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録するものとする。

(外部サービスを利用した情報システムの更改・廃棄時の対策)

第70条 情報センター長は、更改・廃棄時における利用終了手順に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。

- (1) 外部サービスの利用を終了する場合の移行計画書若しくは終了計画書の作成
 - (2) 移行計画書若しくは終了計画書の外部サービス利用者への事前通知
- 2 情報センター長は、更改・廃棄時における情報の廃棄に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。
- (1) 情報の廃棄方法
 - (2) 基盤となる物理機器の廃棄
- 3 情報センター長は、更改・廃棄時におけるアカウントの廃棄に係る規定を策定する場合、次の各号に掲げるものを含む内容を規定するものとする。
- (1) 作成された外部サービス利用者アカウントの削除
 - (2) 利用した外部サービス管理者アカウントの削除・返却と再利用の確認
 - (3) 外部サービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

第2節 要機密情報を取り扱わない場合

(外部サービスの利用に係る規定の整備)

第71条 情報センター長は、次の各号に掲げるものを含む外部サービス（要機密情報を取り扱わない場合）の利用に関する規定を整備するものとする。

- (1) 外部サービスを利用可能な業務の範囲
- (2) 外部サービスの利用申請の許可権限者と利用手続
- (3) 外部サービス管理者の指名と外部サービスの利用状況の管理
- (4) 外部サービスの利用の運用手続

(外部サービスの利用に係る利用手続の整備)

第72条 情報センター長は、本学において要機密情報を取り扱わない前提下で外部サービスを業務に利用する場合は、次の各号に掲げるものを例に利用手続を定めるものとする。

- (1) 利用申請の許可権限者
 - (2) 利用申請時の申請内容
 - ・外部サービスの名称（必要に応じて機能名までを含む）
 - ・外部サービス提供者の名称
 - ・利用目的（業務内容）
 - ・取り扱う情報の格付
 - ・利用期間
 - ・利用申請者（所属・氏名）
 - ・利用者の範囲（学内に限る、部局内に限る など）
 - ・選定時の確認結果
- 2 利用申請の許可権限者は、本学における要機密情報を取り扱わない場合の外部サービスの利用

状況を次の各号に掲げるものを例に管理するものとする。

- (1) 利用申請の許可権限者は、申請ごとに外部サービス管理者を指名するものとする。
 - (2) 利用承認した外部サービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新の外部サービスの利用状況を把握できるようにするものとする。記録する際は、次に掲げるものを例とする項目を記録し学内で共有するものとする。
 - ・外部サービスの名称（必要に応じて機能名までを含む）
 - ・外部サービス提供者の名称
 - ・利用目的（業務内容）
 - ・取り扱う情報の格付
 - ・利用期間
 - ・利用申請者（所属・氏名）
 - ・利用者の範囲（学内に限る、部局内に限る など）
 - ・外部サービス管理者（所属・氏名）
- 3 情報センター長は、本学において要機密情報を取り扱わない前提で外部サービスを業務に利用する場合は、次の各号に掲げるものを例に運用手順を定めるものとする。
- (1) サービス利用中の安全管理に関する運用手順
 - ・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
 - ・情報の滅失、破壊等に備えたバックアップの取得
 - ・利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等）
 - (2) 情報セキュリティインシデント発生時の連絡体制

（外部サービスの利用における対策の実施）

第73条 教職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で要機密情報を取り扱わない場合の外部サービスの利用を申請するものとする。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずるものとする。

- 2 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定するものとする。また、承認した外部サービスを記録するものとする。

第9章 情報システムに係る文書等の整備

第1節 情報システムに係る台帳等の整備

（情報システム台帳の整備）

第74条 情報センター長は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備するものとする。

- 2 部局責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について情報センター長に報告するものとする。

（情報システム台帳の記載事項）

第75条 情報センター長は、次の各号に掲げる内容を含む台帳を整備するものとする。

- (1) 情報システム名
 - (2) 部局
 - (3) 当該部局責任者の氏名及び連絡先
 - (4) システム構成
 - (5) 接続する学外通信回線の種別
 - (6) 取り扱う情報の格付及び取扱制限に関する事項
 - (7) 当該情報システムの設計・開発、運用・保守に関する事項
- 2 情報センター長は、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、次の各号に掲げるものを含む内容を台帳として整備するものとする。
- (1) 情報処理サービス名

- (2) 契約事業者
- (3) 契約期間
- (4) 情報処理サービスの概要
- (5) ドメイン名
- (6) 取り扱う情報の格付及び取扱制限に関する事項

(情報システム関連文書の整備)

第76条 部局責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、次の各号に掲げるものを網羅した情報システム関連文書を整備するものとする。

- (1) 情報システムを構成するサーバ装置及び端末関連情報
- (2) 情報システムを構成する通信回線及び通信回線装置関連情報
- (3) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
- (4) 情報セキュリティインシデントを認知した際の対処手順

(情報システム関連文書の記載事項)

第77条 部局責任者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、次の各号に掲げるものを含む文書を整備するものとする。

- (1) サーバ装置及び端末を管理する教職員等及び利用者を特定する情報
- (2) サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン
- (3) サーバ装置及び端末で利用するソフトウェアを動作させるために用いられる他のソフトウェアであって、次のものを含むものの種類及びバージョン
 - ・ 動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの
 - ・ フレームワーク等、ソフトウェアを実行するための実行環境となるもの
 - ・ プラグイン等、ソフトウェアの機能を拡張するもの
 - ・ 静的リンクライブラリ等、本学がソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの
 - ・ インストーラー作成ソフトウェア等、本学がソフトウェアを開発する際に開発を支援するために使用するもの
- (4) サーバ装置及び端末の仕様書又は設計書

2 部局責任者は、前項第二号及び第三号の情報を収集するため、自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェアを導入するなどにより、これら情報を効率的に収集する手法を決定するものとする。

3 部局責任者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、次の各号に掲げるものを含む文書を整備するものとする。

- (1) 通信回線及び通信回線装置を管理する教職員等を特定する情報
- (2) 通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン
- (3) 通信回線及び通信回線装置の仕様書又は設計書
- (4) 通信回線の構成
- (5) 通信回線装置におけるアクセス制御の設定
- (6) 通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応
- (7) 通信回線の利用部門

4 部局責任者は、所管する情報システムについて、情報システム構成要素ごとのセキュリティ維持に関し、次の各号に掲げるものを含む手順を定めるものとする。

- (1) サーバ装置及び端末のセキュリティの維持に関する手順
- (2) 通信回線を介して提供するサービスのセキュリティの維持に関する手順
- (3) 通信回線及び通信回線装置のセキュリティの維持に関する手順

第2節 機器等の調達に係る規定の整備

(機器等の調達に係る規定の整備)

第78条 情報センター長は、機器等の選定基準を整備し、必要に応じて、機器等の開発等のライ

フサイクルで不正な変更が加えられない管理が行われ、その管理を本学が確認できることを選定基準の一つとして加えるものとする。

- 2 情報センター長は、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ものとする。

(機器等の選定基準)

第79条 情報センター長は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、本学と調達先が連携して原因を調査・排除できる体制を整備していることを例に規定するものとする。

- 2 情報センター長は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定めるものとする。

(納品時の確認・検査手続)

第80条 情報センター長は、機器等の納入時の確認・検査手続には、次の各号に掲げるものを含む事項を確認できる手続を定めるものとする。

- (1) 調達時に指定したセキュリティ要件の実装状況
- (2) 機器等に不正プログラムが混入していないこと

第10章 情報システムのライフサイクルの各段階における対策

第1節 情報システムの企画・要件定義

(実施体制の確保)

第81条 部局情報システム管理責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を部局責任者に求めるものとする。

- 2 部局情報システム管理責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する本学が定める運用管理規程等に応じた体制の確保を総括責任者に求めるものとする。

(情報システムのセキュリティ要件の策定)

第82条 部局情報システム管理責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットやインターネットに接点を有する情報システム（外部サービスを含む。）から分離することの可否を判断した上で、次の各号に掲げるものを含む情報システムのセキュリティ要件を策定するものとする。

- (1) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件
- (2) 情報システム運用時の監視等の運用管理機能要件（監視するデータが暗号化されている場合は、必要に応じて復号すること。）
- (3) 情報システムに関連する脆弱性についての対策要件

- 2 部局情報システム管理責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定するものとする。
- 3 部局情報システム管理責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定するものとする。
- 4 部局情報システム管理責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリテ

ィ要件を適切に策定するものとする。

(情報システムのセキュリティ要件に係る対策)

第83条 部局情報システム管理責任者は、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定するものとする。

- 2 部局情報システム管理責任者は、開発する情報システムが運用される際に想定される脅威の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書等に明記するものとする。
- 3 部局情報システム管理責任者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書(ST: Security Target)を作成し、ST 確認を受けるものとする。
- 4 部局情報システム管理責任者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、次の各号に掲げるものを含む措置を実施するものとする。

- (1) 情報システム運用時に情報セキュリティ確保のために必要となる管理機能を仕様書等に明記すること。
 - (2) 情報セキュリティインシデントの発生を監視する必要があると認めた場合には、監視のために必要な機能について、次に掲げるものを例とする機能を仕様書等に明記すること。
 - ・ 学外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能
 - ・ 不正プログラム感染や踏み台に利用されること等による学外への不正な通信を監視する機能
 - ・ 端末等の学内ネットワークの末端に位置する機器及びサーバ装置において不正プログラムの挙動を監視する機能
 - ・ 学内通信回線への端末の接続を監視する機能
 - ・ 端末への外部電磁的記録媒体の挿入を監視する機能
 - ・ サーバ装置等の機器の動作を監視する機能
 - (3) 暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を仕様書等に明記すること。
- 5 部局情報システム管理責任者は、開発する情報システムに関連する脆弱性への対策が実施されるよう、次の各号に掲げるものを含む対策を仕様書等に明記するものとする。
- (1) 既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。
 - (2) 開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針。
 - (3) セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。
 - (4) ソフトウェアのサポート期間又はサポート打ち切り計画に関する本学への情報提供。

(情報システムのセキュリティ要件に係る対策)

第84条 部局情報システム管理責任者は、構築する情報システムの構成要素のうち、製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、次の各号に掲げるものを含む事項を実施するものとする。

- (1) 「IT 製品の調達におけるセキュリティ要件リスト」を参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とすること。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。
- (2) 「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定すること。

(情報システムの構築を外部委託する場合の対策)

第85条 部局情報システム管理責任者は、情報システムの構築を外部委託する場合は、次の各号に掲げるものを含む委託先に実施させる事項を調達仕様書に記載するなどして、適切に実施させるものとする。

- (1) 情報システムのセキュリティ要件の適切な実装
- (2) 情報セキュリティの観点に基づく試験の実施
- (3) 情報システムの開発環境及び開発工程における情報セキュリティ対策

(情報セキュリティの観点に基づく試験の実施)

第86条 部局情報システム管理責任者は、情報セキュリティの観点に基づく試験の実施について、次の各号に掲げるものを含む事項を実施させるものとする。

- (1) ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離すること。
- (2) 情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。
- (3) 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。

(情報システムの開発環境及び開発工程における情報セキュリティ対策)

第87条 部局情報システム管理責任者は、開発工程における情報セキュリティ対策として、次の各号に掲げるものを含む事項を実施させるものとする。

- (1) ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。
 - ・ ソースコードの変更管理
 - ・ ソースコードの閲覧制限のためのアクセス制御
 - ・ ソースコードの滅失、毀損等に備えたバックアップの取得
- (2) 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。
- (3) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること。

(情報システムの運用・保守を業務委託する場合の対策)

第88条 部局情報システム管理責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させるものとする。

- 2 部局情報システム管理責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させるものとする。

(情報システムの運用・保守を外部委託する場合の対策)

第89条 部局情報システム管理責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、次の各号に掲げるものを含む要件を調達仕様書に記載するなどして、適切に実施させるものとする。

- (1) 情報システムの運用環境に課せられるべき条件の整備
- (2) 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法
- (3) 情報システムの保守における情報セキュリティ対策
- (4) 運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

第2節 情報システムの調達・構築

(機器等の選定時の対策)

第90条 部局情報システム管理責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用するものとする。

(情報システムの構築時の対策)

第91条 部局情報システム管理責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずるものとする。

2 部局情報システム管理責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずるものとする。

(情報システムの構築時の対策事項)

第92条 部局情報システム管理責任者は、情報システムの構築において次の各号に掲げるものを含む情報セキュリティ対策を行うものとする。

- (1) 情報システム構築の工程で扱う要保護情報への不正アクセス、滅失及び毀損等に対処するために開発環境を整備すること。
- (2) セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。
- (3) 情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。
- (4) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために設計レビューやソースコードレビュー等を実施すること。

(5) 脆弱性検査を含む情報セキュリティの観点での試験を実施すること。

2 部局情報システム管理責任者は、情報システムの運用保守段階へ移行するに当たり、次の各号に掲げるものを含む情報セキュリティ対策を行うものとする。

- (1) 情報セキュリティに関わる運用保守体制の整備
- (2) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施
- (3) 情報セキュリティインシデントを認知した際の対処方法の確立

(納品検査時の対策)

第93条 部局情報システム管理責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認するものとする。

2 部局情報システム管理責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に情報セキュリティ対策に必要な内容が含まれていることを確認するものとする。

第3節 情報システムの運用・保守

(情報システムの運用・保守時の対策)

第94条 部局情報システム管理責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用するものとする。

2 部局情報システム管理責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し、運用管理する本学との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用するものとする。

3 部局情報システム管理責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理するものとする。

(情報システムの運用・保守時の対策事項)

第95条 部局情報システム管理責任者は、情報システムのセキュリティ監視を行う場合は、次の各号に掲げる内容を含む監視手順を定め、適切に監視運用するものとする。

- (1) 監視するイベントの種類
- (2) 監視体制
- (3) 監視状況の報告手順

- (4) 情報セキュリティインシデントを認知した場合の報告手順
- (5) 監視運用における情報の取扱い（機密性の確保）
- 2 部局情報システム管理責任者は、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認するものとする。
- 3 部局情報システム管理責任者は、情報システムにおいて取り扱う情報について、当該情報の格付及び取扱制限が適切に守られていることを確認するものとする。
- 4 部局情報システム管理責任者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずるものとする。

第4節 情報システムの更改・廃棄

（情報システムの更改・廃棄時の対策）

第96条 部局情報システム管理責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、次の各号に掲げるものを適切に講ずるものとする。

- (1) 情報システム更改時の情報の移行作業における情報セキュリティ対策
- (2) 情報システム廃棄時の不要な情報の抹消

第5節 情報システムについての対策の見直し

（情報システムについての対策の見直し）

第97条 部局情報システム管理責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずるものとする。

第11章 情報システムの運用継続計画

（情報システムの運用継続計画の整備・整合的運用の確保）

第98条 情報センター長は、本学において非常時優先業務を支える情報システムの運用継続計画を整備する必要がある場合は、非常時における情報セキュリティに係る対策事項を検討するものとする。

- 2 情報センター長は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認するものとする。

第12章 情報システムのセキュリティ機能

第1節 主体認証機能

（主体認証機能の導入）

第99条 部局情報システム管理責任者は、情報システムや情報へのアクセスを管理するため、主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けるものとする。

- 2 部局情報システム管理責任者は、外部機関との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定するものとする。
- 3 部局情報システム管理責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずるものとする。

（主体認証に係る対策）

第100条 部局情報システム管理責任者は、利用者が正当であることを検証するための主体認証機能を設けるに当たっては、次の各号に掲げるものを例とする主体認証方式を決定し、導入する

ものとする。この際、認証の強度として2つ以上の方式を組み合わせる主体認証方式（多要素主体認証方式）が求められる場合には、これを用いるものとする。

- (1) 知識（パスワード等、利用者本人のみが知り得る情報）による認証
 - (2) 所有（電子証明書を格納する IC カード又はワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証
 - (3) 生体（指紋や静脈等、本人の生体的な特徴）による認証
- 2 部局情報システム管理責任者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、強固なパスワードに必要な桁数や複雑さを利用者には守らせる機能を設けるものとする。

（不正行為を防止するための措置）

第101条 部局情報システム管理責任者は、主体認証を行う情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、次の各号に掲げるものを例とする機能を設けるものとする。

- (1) 利用者が定期的に変更しているか否かを確認する機能
 - (2) 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
 - (3) 利用者が主体認証情報を変更する際に、以前に設定した主体認証情報の再設定を防止する機能
- 2 部局情報システム管理責任者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、次の各号に掲げるものを含む方法を用いて適切に管理するものとする。
- (1) 主体認証情報を送信又は保存する場合には、その内容を暗号化すること。
 - (2) 主体認証情報に対するアクセス制限を設けること。
- 3 部局情報システム管理責任者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に利用され、又は利用されるおそれを認識した場合の対策として、次の各号に掲げるものを例とする機能を設けるものとする。
- (1) 当該主体認証情報及び対応する識別コードの利用を停止する機能
 - (2) 主体認証情報の再設定を利用者に要求する機能

（識別コード及び主体認証情報の管理）

第102条 部局情報システム管理責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずるものとする。

- 2 部局情報システム管理責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずるものとする。

（識別コード及び主体認証情報の管理に係る対策）

第103条 部局情報システム管理責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下この条において同じ。）するものとする。

- 2 部局情報システム管理責任者は、識別コードの付与に当たっては、次の各号に掲げるものを例とする措置を講ずるものとする。
- (1) 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止
 - (2) 主体への識別コードの付与に関する記録を消去する場合の部局責任者からの事前の許可
- 3 部局情報システム管理責任者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずるものとする。
- 4 部局情報システム管理責任者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すものとする。
- 5 部局情報システム管理責任者は、知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促すものとする。
- 6 部局情報システム管理責任者は、情報システムを利用する主体ごとに識別コードを個別に付与

するものとする。ただし、部局責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与するものとする。

7 部局情報システム管理責任者は、主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、次の各号に掲げるものを例とする措置を講ずるものとする。

- (1) 当該主体の識別コードを無効にすること。
- (2) 当該主体に交付した主体認証情報格納装置を返還させること。
- (3) 無効化した識別コードを他の主体に新たに発行することを禁止すること。

第2節 アクセス制御機能

(アクセス制御機能の導入)

第104条 部局情報システム管理責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けるものとする。

2 部局情報システム管理責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用するものとする。

(アクセス制御に係る対策)

第105条 部局情報システム管理責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めるものとし、必要に応じて、次の各号に掲げるものを例とするアクセス制御機能の要件を定めるものとする。

- (1) 利用時間や利用時間帯によるアクセス制御
- (2) 同一主体による複数アクセスの制限
- (3) IPアドレスによる端末の制限
- (4) ネットワークセグメントの分割によるアクセス制御
- (5) ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御
- (6) 主体の操作に対する常時アクセス判断・許可アーキテクチャでの制御

第3節 権限の管理

(権限の管理)

第106条 部局情報システム管理責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずるものとする。

2 部局情報システム管理責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び内部からの不正操作や誤操作を防止するための措置を講ずるものとする。

(権限管理に係る対策)

第107条 部局情報システム管理責任者は、主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するため、次の各号に掲げるものを例とする措置を講ずるものとする。

- (1) 業務上必要な場合に限定すること。
- (2) 必要最小限の権限のみ付与すること。
- (3) 管理者権限を行使できる端末をシステム管理者等の専用の端末とすること。

第4節 ログの取得・管理

(ログの取得・管理)

第108条 部局情報システム管理責任者は、情報システムにおいて、情報システムが正しく利用

されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得するものとする。

- 2 部局情報システム管理責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理するものとする。
- 3 部局情報システム管理責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施するものとする。

（ログの取得に係る対策）

第109条 部局情報システム管理責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう設定するものとする。

（ログの管理に係る対策）

第110条 部局情報システム管理責任者は、所管する情報システムの特性に応じてログを取得する目的を設定し、次の各号に掲げるものを例とするログとして取得する情報項目を定め、管理するものとする。

- (1) 事象の主体（人物又は機器等）を示す識別コード
- (2) 識別コードの発行等の管理記録
- (3) 情報システムの操作記録
- (4) 事象の種類
- (5) 事象の対象
- (6) 正確な日付及び時刻
- (7) 試みられたアクセスに関わる情報
- (8) 電子メールのヘッダ情報及び送信内容
- (9) 通信パケットの内容
- (10) 操作する者、監視する者、保守する者等への通知の内容

- 2 部局情報システム管理責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含むログ情報の保全方法を定めるものとする。
- 3 部局情報システム管理責任者は、ログが取得できなくなった場合の対処方法を定めるものとする。

（ログの分析・点検に係る対策）

第111条 部局情報システム管理責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を作成するなどの作業の自動化を例とする当該作業を支援する機能を導入するものとする。

第5節 通信の観測

（通信傍受の禁止）

第112条 情報システムを運用・管理する者及び利用者等は、ネットワークを通じて行われる通信を傍受してはならない。ただし、総括責任者又は当該ネットワークを管理する部局責任者は、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セキュリティ確保目的の観測（以下「観測」という。）を行わせることができるものとする。

- 2 総括責任者又は部局責任者は、観測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、総括責任者又は部局責任者は、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、観測を行うよう命ずることができるものとする。
- 3 観測を行う者は、観測によって知った通信の内容又は個人情報等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、総括責任者並びに部局責任者及び情報セ

セキュリティ委員会に伝達することができるものとする。

- 4 観測によって採取された記録（以下「観測記録」という。）は、要機密情報、要保全情報及び要安定情報とし、観測を行わせる者を情報の作成者とする。
- 5 観測を行わせる者は、観測を行う者に対して、観測記録を保存する期間をあらかじめ指示するものとし、観測を行う者は、指示された期間を経過した観測記録を直ちに破棄するものとする。ただし、観測記録から個人情報に係る部分を削除して、セキュリティ確保のための資料とすることができ、その資料は、体系的に整理し、常に活用できるよう保存するものとする。
- 6 観測を行う者及び観測記録の伝達を受けた者は、セキュリティ確保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ものとする。
- 7 監視記録を不必要に閲覧してはならない。不必要となった観測記録は、直ちに破棄するものとし、観測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。

第6節 暗号・電子署名

（暗号化機能・電子署名機能の導入）

第113条 部局情報システム管理責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、次の各号に掲げる事項を例とした措置を講ずるものとする。

- (1) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。
- (2) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。
- 2 部局情報システム管理責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、次の各号に掲げるものを含めて定めるものとする。
 - (1) 利用者等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。
 - (2) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。
 - (3) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。
 - (4) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。
- 3 部局情報システム管理責任者は、本学における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ、適用可能な電子証明書を UPKI 電子証明書発行サービスが発行している場合は、それを使用するように定めるものとする。

（暗号化・電子署名に係る対策）

第114条 部局情報システム管理責任者は、暗号化又は電子署名を行う情報システムにおいて、次の各号に掲げるものを例とする措置を講ずるものとする。

- (1) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とすること。
- (2) 複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とすること。
- (3) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護される製品を利用することを確実にするため「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択すること。
- (4) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納すること。
- (5) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあ

る暗号プロトコルを選択し、長期的な秘匿性を保証する観点を考慮すること。

(暗号化・電子署名に係る管理)

第115条 部局情報システム管理責任者は、暗号及び電子署名を適切な状況で利用するため、次の各号に掲げる措置を講ずるものとする。

- (1) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。
- (2) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、利用者等と共有を図ること。

(電子署名に係る検証)

第116条 部局情報システム管理責任者は、署名検証者が電子署名の正当性を容易に検証するための情報を入手できるよう、次の各号に掲げるものを例とする方法により、当該情報の提供を可能にするものとする。

- (1) 信頼できる機関による電子証明書の提供
- (2) 本学の窓口での電子証明書の提供

第13章 情報セキュリティの脅威への対策

第1節 ソフトウェアに関する脆弱性対策

(ソフトウェアに関する脆弱性対策の実施)

第117条 部局情報システム管理責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施するものとする。

- 2 部局情報システム管理責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施するものとする。
- 3 部局情報システム管理責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認するものとする。
- 4 部局情報システム管理責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずるものとする。

(ソフトウェアに関する脆弱性対策)

第118条 部局情報システム管理責任者は、対象となるソフトウェアの脆弱性に関して、次の各号に掲げるものを含む情報を適宜入手するものとする。

- (1) 脆弱性の原因
- (2) 影響範囲
- (3) 対策方法
- (4) 脆弱性を悪用する不正プログラムの流通状況
- 2 部局情報システム管理責任者は、利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しないものとする。
- 3 部局情報システム管理責任者は、次の各号に掲げるものを例とする手段で脆弱性対策の状況を確認するものとする。
 - (1) 構成要素ごとにソフトウェアのバージョン等を把握し、当該ソフトウェアの脆弱性の有無を確認すること。
 - (2) 脆弱性診断を実施すること。
- 4 部局情報システム管理責任者は、脆弱性対策の状況を確認する間隔を、可能な範囲で短くするものとする。

- 5 部局情報システム管理責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、次の各号に掲げる事項について判断するものとする。
- (1) 対策の必要性
 - (2) 対策方法。この際、自動でソフトウェアを更新する機能を有する IT 資産管理ソフトウェアを導入するなどにより、効率的に脆弱性対策を実施する手法を予め決定すること。
 - (3) 対策方法が存在しないゼロデイと呼ばれる状態の場合又は対策が完了するまでの期間に對する一時的な回避方法
 - (4) 対策方法又は回避方法が情報システムに与える影響
 - (5) 対策の実施予定時期
 - (6) 対策試験の必要性
 - (7) 対策試験の方法
 - (8) 対策試験の実施予定時期
- 6 部局情報システム管理責任者は、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認するものとする。
- 7 部局情報システム管理責任者は、脆弱性対策を実施する場合には、少なくとも次の各号に掲げる事項を記録し、これらの事項のほかに必要な事項があれば適宜記録するものとする。
- (1) 実施日
 - (2) 実施内容
 - (3) 実施者
- 8 部局情報システム管理責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイルは、信頼できる方法で入手するものとする。

第2節 不正プログラム対策

(不正プログラム対策の実施)

- 第119条 部局情報システム管理責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入するものとする。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除くものとする。
- 2 部局情報システム管理責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずるものとする。
- 3 部局情報システム管理責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うものとする。

(不正プログラム対策ソフトウェア等に係る対策)

- 第120条 情報センター長は、不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入するものとする。
- 2 情報センター長は、不正プログラム対策ソフトウェア等が、常に最新の状態となるように構成するものとする。
- 3 情報センター長は、不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成するものとする。
- 4 不正プログラム対策ソフトウェア等の設定変更権限については、情報システム管理室が一括管理し、システム利用者に当該権限を付与しないものとする。
- 5 情報センター長は、不正プログラム対策ソフトウェア等は、定期的に全てのファイルを対象としたスキャンを実施するよう構成するものとする。

(想定される不正プログラムの感染経路の全てにおける対策)

- 第121条 部局情報システム管理責任者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行うものとする。

(不正プログラム対策の状況の把握)

- 第122条 部局情報システム管理責任者は、不正プログラム対策の実施を徹底するため、次の各

号に掲げるものを例とする不正プログラム対策に関する状況を把握し、必要な対処を行うものとする。

- (1) 不正プログラム対策ソフトウェア等の導入状況
- (2) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況

第3節 サービス不能攻撃対策

(サービス不能攻撃対策の実施)

第123条 部局情報システム管理責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下この条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うものとする。

- 2 部局情報システム管理責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築するものとする。
- 3 部局情報システム管理責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視するものとする。

(サービス不能攻撃への対策)

第124条 部局情報システム管理責任者は、サーバ装置、端末及び通信回線装置について、次の各号に掲げるものを例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処するものとする。

- (1) パケットフィルタリング機能
- (2) 3-way handshake 時のタイムアウトの短縮
- (3) 各種 Flood 攻撃への防御
- (4) アプリケーションゲートウェイ機能

(サービス不能攻撃を受けた場合を想定した対策)

第125条 部局情報システム管理責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築するものとする。

- 2 部局情報システム管理責任者は、サーバ装置、端末及び通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、次の各号に掲げるものを例とする対策を検討するものとする。
 - (1) インターネットに接続している通信回線の提供元となる事業者が別途提供するサービス不能攻撃に係る通信の遮断等の対策
 - (2) サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入
 - (3) サーバ装置、端末及び通信回線装置及び通信回線の冗長化
 - (4) コンテンツデリバリーネットワーク (CDN) サービスの利用
- 3 部局情報システム管理責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討するものとする。

(サービス不能攻撃を受けることに関する監視)

第126条 部局情報システム管理責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定めるものとする。

- 2 部局情報システム管理責任者は、監視対象の監視記録を保存するものとする。

第4節 標的型攻撃対策

(標的型攻撃対策の実施)

第127条 部局情報システム管理責任者は、情報システムにおいて標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずるものとする。

- 2 部局情報システム管理責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講ずるものとする。

（標的型攻撃に係る入口対策）

第128条 部局情報システム管理責任者は、サーバ装置及び端末について組織内部への侵入を低減するため、次の各号に掲げるものを例とする対策を行うものとする。

- （1） 不要なサービスについて機能を削除又は停止すること。
- （2） 不審なプログラムが実行されないよう設定すること。
- （3） パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限すること。

2 部局情報システム管理責任者は、USB メモリ等の外部電磁的記録媒体を利用した組織内部への侵入を低減するため、次の各号に掲げるものを例とする対策を行うものとする。

- （1） 出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させないとともに、接続する外部電磁的記録媒体を事前に特定しておくこと。
- （2） 外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査すること。
- （3） サーバ装置及び端末について、自動再生（オートラン）機能を無効化すること。
- （4） サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とすること。
- （5） サーバ装置及び端末について、使用を想定しないUSB ポートを無効化すること。
- （6） 組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入すること。

（標的型攻撃に係る内部対策）

第129条 部局情報システム管理責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される認証サーバやファイルサーバ等の重要なサーバについて、次の各号に掲げるものを例とする対策を行うものとする。

- （1） 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定するとともに、インターネットに直接接続しないこと。
- （2） 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずること。

2 部局情報システム管理責任者は、端末の管理者権限アカウントについて、次の各号に掲げるものを例とする対策を行うものとする。

- （1） 不要な管理者権限アカウントを削除すること。
- （2） 管理者権限アカウントのパスワードは、容易に推測できないものに設定すること。

3 部局情報システム管理責任者は、重点的に守るべき業務・情報を取り扱う情報システムについては、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」に従って、対策を講ずるものとする。

第14章 アプリケーション・コンテンツの作成・提供

第1節 アプリケーション・コンテンツ作成時の対策

（アプリケーション・コンテンツの作成に係る規定の整備）

第130条 情報センター長は、アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備するものとする。

（アプリケーション・コンテンツのセキュリティ要件の策定）

第131条 部局情報システム管理責任者は、学外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて次の各号に掲げる内容を仕様

めるものとする。

- (1) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。
 - (2) 提供するアプリケーションが脆弱性を含まないこと。
 - (3) 実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しないこと。
 - (4) 電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えること。
 - (5) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を OS やソフトウェア等の利用者に要求することがないように、アプリケーション・コンテンツの提供方式を定めて開発すること。
 - (6) サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能がアプリケーション・コンテンツに組み込まれることがないように開発すること。
- 2 教職員等は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項に掲げる内容を調達仕様に含めるものとする。

(アプリケーション・コンテンツのセキュリティ要件に係る対策)

第132条 部局情報システム管理責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、次の各号に掲げるものを含む対策を行うものとする。

- (1) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。
 - (2) 業務委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。
- 2 部局情報システム管理責任者は、提供するアプリケーション・コンテンツにおいて、学外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを HTML のソースを表示させるなどして確認するものとし、必要があつて当該機能を含める場合は、当該学外へのアクセスが情報セキュリティ上安全なものであることを確認するものとする。
- 3 部局情報システム管理責任者は、提供するアプリケーション・コンテンツに本来のサービス提供に必要な学外へのアクセスを自動的に発生させる機能を含めないものとする。
- 4 部局情報システム管理責任者は、文書ファイル等のコンテンツの提供において、当該コンテンツが改ざん等なく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、国立情報学研究所 UPKI 電子証明書発行サービス (UPKI) の利用が可能である場合は、当該サービスにより発行された電子証明書を用いて署名を施すものとする。

第2節 アプリケーション・コンテンツ提供時の対策

(大学ドメイン名の使用)

第133条 部局情報システム管理責任者は、学外向けに提供するウェブサイト等が実際の本学提供のものであることを利用者が確認できるように大学ドメイン名を情報システムにおいて使用するように仕様に含めるものとする。ただし、次の各号に掲げる場合を除くものとする。

- (1) 政府ドメイン名を使用する場合
 - (2) 第18章第2節に掲げるソーシャルメディアサービスによる情報発信を行う場合
- 2 教職員等は、学外向けに提供するウェブサイト等の作成を業務委託する場合は、前項各号列記以外の部分、同項第1号の規定に則り本学に適するドメイン名を使用するように調達仕様に含めるものとする。

(不正なウェブサイトへの誘導防止)

第134条 部局情報システム管理責任者は、利用者が検索サイト等を経由して本学のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずるものとする。

(検索サイトに係る対策)

第135条 部局情報システム管理責任者は、学外向けに提供するウェブサイトに対して次の各号に掲げるものを例とする検索エンジン最適化措置（SEO 対策）を講ずるものとする。

- (1) クローラからのアクセスを排除しないこと。
- (2) cookie 機能を無効に設定したブラウザでも正常に閲覧可能とすること。
- (3) 適切なタイトルを設定すること。
- (4) 不適切な誘導を行わないこと。

2 部局情報システム管理責任者は、学外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、不審なサイトへのアクセスを防止するための対策を講ずるものとする。

(学外のアプリケーション・コンテンツの告知)

第136条 利用者等は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずるものとする。

2 利用者等は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つものとする。

(アプリケーション・コンテンツの告知に係る対策)

第137条 利用者等は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示するものとする。この場合において、短縮 URL は、用いないものとする。

2 利用者等は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示するものとする。

3 利用者等は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つために次の各号に掲げる措置を講ずるものとする。

- (1) 告知するアプリケーション・コンテンツを管理する組織名を明記すること。
- (2) 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記すること。

第15章 端末・サーバ装置等

第1節 端 末

(端末の導入時の対策)

第138条 情報センター長は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作及び表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずるものとする。

2 情報センター長は、多様なソフトウェアを利用することにより脆弱性が存在する可能性を増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めるものとする。

(物理的な脅威から保護するための対策)

第139条 情報センター長は、モバイル端末を除く端末について、原則としてクラス2以上の要管理対策区域に設置するものとする。

2 情報センター長は、端末の盗難及び不正な持ち出しを防止するために、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定するものとする。

(2) モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意するものとする。

3 情報センター長は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、次の各号に掲げるものを例とする対策を講ずるものとする。

(1) 一定時間操作が無いと自動的にスクリーンロックするよう設定すること。

(2) 要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付けること。

(端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアに係る対策)

第140条 情報センター長は、次の各号に掲げるものを考慮した上で、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めるものとする。

(1) ソフトウェアベンダ等のサポート状況

(2) ソフトウェアと外部との通信の有無及び通信する場合はその通信内容

(3) インストール時に同時にインストールされる他のソフトウェア

(4) その他ソフトウェアの利用に伴う情報セキュリティリスク

(端末の運用時の対策)

第141条 情報センター長は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うものとする。

2 情報センター長は、端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図るものとする。

(端末の運用終了時の対策)

第142条 情報センター長は、端末の運用を終了する際に端末の電磁的記録媒体の全ての情報を抹消するものとする。

(本学が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用時の対策)

第143条 情報センター長は、教職員等が本学が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めるものとする。

2 情報センター長は、要機密情報を取り扱う本学が支給する端末（要管理対策区域外で使用する場合に限る）について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する規定を整備するものとする。

3 情報センター長は、要管理対策区域外において学外通信回線に接続した本学が支給する端末を学内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から学内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めるものとする。

4 部局責任者は、教職員等が本学が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要機密情報を取り扱う場合は、当該端末について本条第2項の技術的な措置を講ずるものとする。

(本学が支給する端末（要管理対策区域外で使用する場合に限る）の対策)

第144条 情報センター長は、利用者等が本学が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合の利用手順を、次の各号に掲げるものを例として定めるものとする。

(1) 端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化

(2) 盗み見に対する対策（のぞき見防止フィルタの利用等）

(3) 盗難・紛失に対する対策（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）

(4) 利用する場所や時間の限定

(5) 端末の盗難・紛失が発生した際の緊急対応手順

2 総括責任者は、利用者等が本学が支給する端末（要管理対策区域外で使用する場合に限る）を

用いて要保護情報を取り扱う場合について、次の各号に掲げるものを含む許可手続を定めるものとする。

- (1) 利用時の許可申請手続
 - (2) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等）
 - (3) 利用期間満了時の手続
 - (4) 部局責任者による手続内容の記録
- 3 情報センター長は、要機密情報を取り扱う本学が支給する端末（要管理対策区域外で使用する場合に限る）について、次の各号に掲げるものを例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を設けるものとする。
- (1) シンククライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンククライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスすること。
 - (2) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスすること。
 - (3) ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入すること。
 - (4) 端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設けること。
 - (5) 上記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設けること。
 - (6) ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設けること。
 - (7) 高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等を使用すること。
- 4 情報センター長は、要管理対策区域外において学外通信回線に接続した本学が支給する端末を要管理対策区域で学内通信回線に接続することの許可手続として、次の各号に掲げるものを含む手続を規定し、利用者等に遵守させるものとする。
- (1) 利用時の許可申請手続
 - (2) 手続内容（利用者、目的、利用する情報、端末等）
 - (3) 利用期間満了時の手続
 - (4) 学内通信回線への接続時の手続（端末の事前検疫等）
 - (5) 部局責任者による手続内容の記録

（本学支給以外の端末の導入及び利用時の対策）

第145条 情報センター長は、本学支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、本学が講じる安全管理措置、当該端末の管理は本学ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、本学における本学支給以外の端末の利用の可否を判断するものとする。

- 2 情報センター長は、利用者等が本学支給以外の端末を用いて本学の業務に係る情報処理を行う場合の許可等の手続を定めるものとする。
- 3 情報センター長は、利用者等が本学支給以外の端末を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めるものとする。
- 4 情報センター長、要機密情報を取り扱う本学支給以外の端末について、次の各号に掲げるものを含む安全管理措置に関する規定を整備するものとする。
 - (1) 盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置
 - (2) 不正プログラムの感染等により情報窃取されることを防止するための利用時の措置
- 5 情報センター長は、要管理対策区域外において学外通信回線に接続した本学支給以外の端末を学内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から学内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めるものとする。

- 6 総括責任者は、本学支給以外の端末を用いた本学の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者（以下「端末管理責任者」という。）を定めるものとする。
- 7 端末管理責任者は、利用者等が本学支給以外の端末を用いて要機密情報を取り扱う場合は、当該端末について第4項第1号の安全管理措置を講ずるものとする。
- 8 端末管理責任者は、要機密情報を取り扱う本学支給以外の端末について、前項の規定にかかわらず第4項第1号に定める安全管理措置のうち、自ら講ずることができないもの及び第4項第2号に定める安全管理措置を利用者等に講じさせるものとする。
- 9 利用者等は、要機密情報を取り扱う本学支給以外の端末について、前項において第4項第1号に定める安全管理措置のうち、端末管理責任者が講ずることができないもの及び第4項第2号に定める安全管理措置を講ずるものとする。
- 10 利用者等は、本学支給以外の端末を用いて本学の業務に係る情報処理を行う場合には、端末管理責任者の許可を得るものとする。
- 11 利用者等は、情報処理の目的を完了した場合は、要保護情報を本学支給以外の端末から消去するものとする。

（本学支給以外の端末の導入及び利用時の対策）

第146条 情報センター長は、本学支給以外の端末を利用する際に、次に掲げるものを含む許可等の手続を整備し、教職員に周知するものとする。

- (1) 以下を含む本学支給以外の端末利用時の申請内容
 - ・申請者の氏名、所属、連絡先
 - ・利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）
 - ・利用する端末の製造企業名、機種名、OSの種類及びバージョン
 - ・利用目的、取り扱う情報の概要、要機密情報の利用の有無等
 - ・主要な利用場所
 - ・利用する主要な通信回線サービス
 - ・利用する期間
 - (2) 利用許諾条件
 - (3) 申請手順
 - (4) 利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順
 - (5) 利用期間満了時の利用終了又は利用期間更新の手続方法
 - (6) 部局責任者
- 2 情報センター長は、利用者等が本学支給以外の端末を用いて要保護情報を取り扱う場合の利用手続を、次の各号に掲げるものを例として定めるものとする。
- (1) 端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化
 - (2) 盗み見に対する対策（のぞき見防止フィルタの利用等）
 - (3) 盗難・紛失に対する対策（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）
 - (4) 利用する場所や時間の限定
 - (5) 端末の盗難・紛失が発生した際の緊急対応手順
- 3 情報センター長は、利用者等が本学支給以外の端末を用いて要保護情報を取り扱う場合について、以下を含む許可手続を定めるものとする。
- (1) 利用時の許可申請手続
 - (2) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等）
 - (3) 利用期間満了時の手続
 - (4) 部局責任者による手続内容の記録
- 4 情報センター長は、要機密情報を取り扱う本学支給以外の端末について、次の各号に掲げるものを例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を設けるものとする。
- (1) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築すること。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスすること。

- (2) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築すること。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスすること。
 - (3) ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入すること。
 - (4) 端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設けること。
 - (5) 上記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設けること。
 - (6) ハードディスク等電磁的記録媒体に保存されている情報を遠隔からの命令等により消去する機能を設けること。
 - (7) 高度なセキュリティ機能を備えた OS を搭載するスマートフォンやタブレット端末等を使用すること。
- 5 情報センター長は、要機密情報を取り扱う本学支給以外の端末について、次の各号に掲げるものを例に、利用者等が講ずるべき利用時の実施手順に係る安全管理措置を設けるものとする。
- (1) パスワード等による端末ロックの常時設定
 - (2) OS やアプリケーションの最新化
 - (3) 不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（本学として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）
 - (4) 端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）
 - (5) 本学提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）
 - (6) 次に掲げるものを例とする禁止事項の遵守
 - ・ 端末、OS、アプリケーション等の改造行為
 - ・ 安全性が確認できていないアプリケーションのインストール及び利用
 - ・ 利用が禁止されているソフトウェアのインストール及び利用
 - ・ 許可されていない通信回線サービスの利用（利用する回線を限定する場合）
 - ・ 第三者への端末の貸与

第2節 サーバ装置

（サーバ装置の導入時の対策）

- 第147条 部局情報システム管理責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作及び表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずるものとする。
- 2 部局情報システム管理責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保するものとする。
 - 3 部局情報システム管理責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めるものとする。
 - 4 部局情報システム管理責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずるものとする。

（物理的な脅威から保護するための対策）

- 第148条 部局情報システム管理責任者は、要保護情報を取り扱うサーバ装置については、クラス2以上の要管理対策区域に設置するものとする。
- 2 部局情報システム管理責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、次の各号に掲げるものを例とする対策を講ずるものとする。
 - (1) 施錠可能なサーバラックに設置して施錠する。
 - (2) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

- 3 部局情報システム管理責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、一定時間操作が無いと自動的にスクリーンロックするよう設定するなどの対策を講ずるものとする。

(可用性を確保するための対策)

第149条 部局情報システム管理責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため要安定情報を取り扱う情報システムについては、将来の見通しも考慮し、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) 負荷分散装置、DNS ラウンドロビン方式等による負荷分散
- (2) 同一システムを2系統で構成することによる冗長化

(サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアに係る対策)

第150条 部局情報システム管理責任者は、次の各号に掲げるものを考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めるものとする。

- (1) ソフトウェアベンダのサポート状況
- (2) ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容
- (3) インストール時に同時にインストールされる他のソフトウェア
- (4) その他ソフトウェアの利用に伴う情報セキュリティリスク

(サーバ装置の運用時の対策)

第151条 部局情報システム管理責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うものとする。

- 2 部局情報システム管理責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には、改善を図るものとする。
- 3 部局情報システム管理責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずるものとする。ただし、サーバ装置の利用環境等から不要と判断できる場合は、この限りではない。
- 4 部局情報システム管理責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講ずるものとする。

(サーバ装置の運用管理作業の記録に係る対策)

152条 部局情報システム管理責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認する場合は、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録するものとする。

(サーバ装置の監視に係る対策)

第153条 部局情報システム管理責任者は、サーバ装置への無許可のアクセス等の不正な行為を監視するために、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) アクセスログ等を定期的に確認すること。
- (2) IDS (Intrusion Detection System) /IPS (Intrusion Prevention System)、WAF (Web Application Firewall) 等を設置すること。
- (3) 不正プログラム対策ソフトウェアを利用すること。
- (4) ファイル完全性チェックツールを利用すること。
- (5) CPU、メモリ、ディスク I/O 等のシステム状態を確認すること。

(サーバ装置の復元に係る対策)

第154条 部局情報システム管理責任者は、要安定情報を取り扱うサーバ装置については、運用状態を復元するために次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) サーバ装置の運用に必要なソフトウェアの原本を別に用意しておくこと。
- (2) 定期的なバックアップを実施すること。
- (3) サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施すること。

- (4) バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施すること。

(サーバ装置の運用終了時の対策)

第155条 部局情報システム管理責任者は、サーバ装置の運用を終了する際にサーバ装置の電磁的記録媒体の全ての情報を抹消するものとする。

第3節 複合機・特定用途機器

(複合機)

第156条 部局情報システム管理責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定するものとする。

- 2 部局情報システム管理責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずるものとする。
- 3 部局情報システム管理責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消するものとする。

(複合機の導入時の対策)

第157条 部局情報システム管理責任者は、「IT 製品の調達におけるセキュリティ要件リスト」を参照するなどし、複合機が備える機能、設置環境及び取り扱う情報の格付及び取扱制限に応じ、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記するものとする。

(複合機の運用時の対策)

第158条 部局情報システム管理責任者は、次の各号に掲げるものを例とする運用中の複合機に対する情報セキュリティインシデントへの対策を講ずるものとする。

- (1) 複合機について、利用環境に応じた適切なセキュリティ設定を実施すること。
- (2) 複合機が備える機能のうち、利用しない機能を停止すること。
- (3) 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用すること。
- (4) 学内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにすること。
- (5) 複合機をインターネットに直接接続しないこと。
- (6) リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行うこと。
- (7) 利用者ごとに許可される操作を適切に設定すること。

(複合機の運用終了時の対策)

第159条 部局情報システム管理責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消するものとし、当該機能を備えていない複合機については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを契約内容に含むなど別の手段で対策を講ずるものとする。

(IoT 機器を含む特定用途機器)

第160条 部局情報システム管理責任者は、特定用途機器について、取り扱う情報、利用方法及び通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずるものとする。

(特定用途機器の運用時の対策)

第161条 部局情報システム管理責任者は、特定用途機器の特性に応じて、次の各号に掲げるものを含む対策を講ずるものとする。ただし、使用している特定用途機器の機能上の制約により講

することができない対策は除くものとする。

- (1) 特定用途機器について、主体認証情報を初期設定から変更した上で、適切に管理すること。
- (2) 特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理すること。
- (3) 特定用途機器が備える機能のうち、利用しない機能を停止すること。
- (4) インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットやインターネットに接点を有する情報システムに接続しないこと。
- (5) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行うこと。
- (6) 特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずること。
- (7) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視すること。
- (8) 特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消すること。

第16章 電子メール・ウェブ等

第1節 電子メール

(電子メールの導入時の対策)

第162条 部局情報システム管理責任者は、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ものとする。

- 2 部局情報システム管理責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えるものとする。
- 3 部局情報システム管理責任者は、電子メールのなりすましの防止策を講ずるものとする。
- 4 部局情報システム管理責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずるものとする。

(電子メールの受信時及び送信時の主体認証)

第163条 部局情報システム管理責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、次に掲げるものを例とする利用者等の主体認証を行う機能を備えるものとする。

- (1) 電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入すること。

(電子メールのなりすましの防止)

第164条 部局情報システム管理責任者は、次の各号に掲げるものを例とする電子メールのなりすましの防止策を講ずるものとする。

- (1) SPF (Sender Policy Framework)、DKIM (DomainKeys Identified Mail)、DMARC (Domain-based Message Authentication, Reporting & Conformance) 等の送信ドメイン認証技術による送信側の対策を行うこと。
 - (2) SPF、DKIM、DMARC 等の送信ドメイン認証技術による受信側の対策を行うこと。
 - (3) S/MIME 等の電子メールにおける電子署名の技術を利用すること。
- 2 部局情報システム管理責任者は、次の各号に掲げるものを例とする盗聴及び改ざんの防止策を講ずるものとする。
- (2) SMTP によるサーバ間通信を TLS により保護する。
 - (3) S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用すること。

第2節 ウェブ

(ウェブサーバの導入・運用時の対策)

第165条 部局情報システム管理責任者は、ウェブサーバの管理や設定において、次の各号に掲げるものを含む情報セキュリティ確保のための対策を講ずるものとする。

- (1) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。
- (2) ウェブコンテンツの編集作業を担当する主体を限定すること。
- (3) 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。
- (4) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。
- (5) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講ずること。

2 部局情報システム管理責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要な情報がウェブサーバに保存されないことを確認するものとする。

(ウェブサーバの管理や設定)

第166条 部局情報システム管理責任者は、不要な機能の停止又は制限として、次の各号に掲げるものを例とするウェブサーバの管理や設定を行うものとする。

- (1) CGI (Common Gateway Interface) 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とすること。
- (2) ディレクトリインデックスの表示を禁止すること。
- (3) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム (CMS) 等における不要な機能を制限すること。
- (4) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持すること。

2 部局情報システム管理責任者は、ウェブコンテンツの編集作業を担当する主体の限定として、次の各号に掲げるものを例とするウェブサーバの管理や設定を行うものとする。

- (1) ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えないこと。
- (2) OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除すること。

3 部局情報システム管理責任者は、公開してはならない又は無意味なウェブコンテンツが公開されないよう管理することとして、次の各号に掲げるものを例とするウェブサーバの管理や設定を行うものとする。

- (1) 公開を想定していないファイルをウェブ公開用ディレクトリに置かないこと。
- (2) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除すること。

4 部局情報システム管理責任者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、次の各号に掲げるものを例とするウェブサーバの管理や設定を行うものとする。

- (1) ウェブコンテンツの更新の際は、専用の端末を使用して行うこと。
- (2) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限すること。
- (3) ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行うこと。

5 部局情報システム管理責任者は、通信時の盗聴による第三者への情報の漏えいの防止及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、次の各号に掲げるものを含むウェブサーバの実装を行うものとする。

- (1) TLS 機能を適切に用いること。
- (2) TLS 機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局 (証明書発行機関) により発行された電子証明書を用いること。
- (3) 暗号技術検討会及び関連委員会 (CRYPTREC) により作成された「TLS 暗号設定ガイドライン」に従って、TLS サーバを適切に設定すること。

(ウェブアプリケーションの開発時・運用時の対策)

第167条 部局情報システム管理責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずるものとし、運用時においてもこれらの対策に漏れが無いことを定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うものとする。

(ウェブアプリケーションの脆弱性の排除)

第168条 部局情報システム管理責任者は、次の各号に掲げるものを含むウェブアプリケーションの脆弱性を排除するものとする。

- (1) SQL インジェクション脆弱性
- (2) OS コマンドインジェクション脆弱性
- (3) ディレクトリトラバーサル脆弱性
- (4) セッション管理の脆弱性
- (5) アクセス制御欠如と認可処理欠如の脆弱性
- (6) クロスサイトスクリプティング脆弱性
- (7) クロスサイトリクエストフォージェリ脆弱性
- (8) クリックジャッキング脆弱性
- (9) メールヘッダインジェクション脆弱性
- (10) HTTP ヘッダインジェクション脆弱性
- (11) eval インジェクション脆弱性
- (12) レースコンディション脆弱性
- (13) バッファオーバーフロー及び整数オーバーフロー脆弱性

第3節 ドメインネームシステム (DNS)

(DNS の導入時の対策)

第169条 部局情報システム管理責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずるものとする。

- 2 部局情報システム管理責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずるものとする。
- 3 部局情報システム管理責任者は、コンテンツサーバにおいて、本学のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずるものとする。

(コンテンツサーバに係る対策)

第170条 部局情報システム管理責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、次の各号に掲げるものを例とする名前解決を停止させないための措置を講ずるものとする。

- (1) コンテンツサーバを冗長化すること。
- (2) 通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行うこと。

(キャッシュサーバに係る対策)

第171条 部局情報システム管理責任者は、学外からの名前解決の要求に応じる必要性について検討し、必要性がないと判断される場合は必要であれば学内からの名前解決の要求のみに応答をするよう、次の各号に掲げるものを例とする措置を講ずるものとする。

- (1) キャッシュサーバの設定でアクセス制御を行うこと。
- (2) ファイアウォール等でアクセス制御を行うこと。

(DNS キャッシュポイズニング攻撃に係る対策)

第172条 部局情報システム管理責任者は、DNS キャッシュポイズニング攻撃から保護するため、次の各号に掲げるものを例とする措置を講ずるものとする。

- (1) ソースポートランダム化機能を導入すること。

(2) DNSSEC を利用すること。

(学内のみで使用する名前の解決を提供するコンテンツサーバに係る対策)

第173条 部局情報システム管理責任者は、学内のみで使用する名前の解決を提供するコンテンツサーバにおいて、次の各号に掲げるものを例とする当該コンテンツサーバで管理する情報の漏えいを防止するための措置を講ずるものとする。

(1) 外部向けのコンテンツサーバと別々に設置すること。

(2) ファイアウォール等でアクセス制御を行うこと。

(DNS の運用時の対策)

第174条 部局情報システム管理責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持するものとする。

2 部局情報システム管理責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認するものとする。

3 部局情報システム管理責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずるものとする。

(キャッシュサーバに係る対策)

第175条 部局情報システム管理責任者は、キャッシュサーバにおいて、ルートヒントファイル(DNS ルートサーバの情報が登録されたファイル)の更新の有無を定期的(3か月に一度程度)に確認し、最新のDNS ルートサーバの情報を維持するものとする。

第4節 データベース

(データベースの導入・運用時の対策)

第176条 部局情報システム管理責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うものとする。

2 部局情報システム管理責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずるものとする。

3 部局情報システム管理責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずるものとする。

4 部局情報システム管理責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずるものとする。

5 部局情報システム管理責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をするものとする。

(データベースの管理者権限に係る対策)

第177条 部局情報システム管理責任者は、必要に応じて情報システムの管理者とデータベースの管理者を別にするものとする。

2 部局情報システム管理責任者は、データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しないものとする。

3 部局情報システム管理責任者は、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずるものとする。

(データベースの操作ログに係る対策)

第178条 部局情報システム管理責任者は、業務を遂行するに当たって不必要なデータの操作を検知できるよう、次の各号に掲げるものを例とする措置を講ずるものとする。

(1) 一定数以上のデータの取得に関するログを記録し、警告を発すること。

(2) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発すること。

(データベースにおける脆弱性に係る対策)

第179条 部局情報システム管理責任者は、データベースにアクセスする機器上で動作するプロ

グラムに対して、SQL インジェクションの脆弱性を排除するものとする。

- 2 部局情報システム管理責任者は、データベースにアクセスする機器上で動作するプログラムに対して SQL インジェクションの脆弱性の排除が不十分であると判断した場合、次の各号に掲げるものを例とする対策の実施を検討するものとする。

- (1) ウェブアプリケーションファイアウォールの導入
- (2) データベースファイアウォールの導入

(データベースにおける暗号化に係る対策)

- 第180条 部局情報システム管理責任者は、格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施するものとする。

第17章 通信回線

第1節 通信回線

(通信回線の導入時の対策)

- 第181条 部局情報システム管理責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずるものとする。

- 2 部局情報システム管理責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けるものとする。
- 3 部局情報システム管理責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考えられる場合は、通信内容の秘匿性を確保するための措置を講ずるものとする。
- 4 部局情報システム管理責任者は、利用者等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずるものとする。学内通信回線へ本学支給以外の端末を接続する際も同様とする。
- 5 部局情報システム管理責任者は、通信回線装置を要管理対策区域に設置するものとする。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにするものとする。
- 6 部局情報システム管理責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずるものとする。
- 7 部局情報システム管理責任者は、学内通信回線にインターネット回線、公衆通信回線等の学外通信回線を接続する場合には、学内通信回線及び当該学内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずるものとする。
- 8 部局情報システム管理責任者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視するための措置を講ずるものとする。
- 9 部局情報システム管理責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備するものとする。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。
- 10 部局情報システム管理責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保するものとする。
- 11 部局情報システム管理責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくものとする。

(通信経路の分離に係る対策)

- 第182条 部局情報システム管理責任者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じて、次の各号に掲げるものを例とする通信経路の分離を行

うものとする。

- (1) 外部との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離すること。
- (2) 業務目的や取り扱う情報の格付及び取扱制限に応じて情報システムごとに VLAN により通信経路を分離し、それぞれの通信制御を適切に行うこと。
- (3) 他の情報システムから独立した専用の通信回線を構築すること。

(通信回線の秘匿性確保に係る対策)

第183条 部局情報システム管理責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けるものとし、通信回線の秘匿性確保の方法として、TLS 及び IPsec 等による暗号化を行い、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し、決定するものとする。

(通信回線への情報システムの接続に係る対策)

第184条 部局情報システム管理責任者は、学内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) 情報システムの MAC アドレス等の端末を一意に識別できる情報により接続機器を識別すること。
- (2) クライアント証明書により接続機器の認証を行うこと。

(通信回線及び通信回線装置の保護に係る対策)

第185条 部局情報システム管理責任者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、次の各号に掲げるものを例とする措置を講ずるものとする。

- (1) 通信回線装置を施錠可能なラック等に設置すること。
- (2) 施設内に敷設した通信ケーブルを物理的に保護すること。
- (3) 通信回線装置の操作ログを取得すること。

(要安定情報を取り扱う情報システムが接続される通信回線に係る対策)

第186条 部局情報システム管理責任者は、要安定情報を取り扱う情報システムが接続される通信回線を構築する場合は、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設けること。
- (2) 通信回線及び通信回線装置を冗長構成にすること。

(学内通信回線と学外通信回線との接続に係る対策)

第187条 部局情報システム管理責任者は、学内通信回線に、インターネット回線や公衆通信回線等の学外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) ファイアウォール、WAF、リバースプロキシ等により通信制御を行うこと。
- (2) 通信回線装置による特定の通信プロトコルの利用を制限すること。
- (3) IDS/IPS により不正アクセスを検知及び遮断すること。

(遠隔地から通信回線装置に対して行われるリモートアクセスに係る対策)

第188条 部局情報システム管理責任者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行うこと。
- (2) 主体認証によりアクセス制御すること。
- (3) 通信内容の暗号化により秘匿性を確保すること。
- (4) ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにすること。

(通信回線の運用時の対策)

第189条 部局情報システム管理責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずるものとする。

2 部局情報システム管理責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うものとする。

3 部局情報システム管理責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図るものとする。

4 部局情報システム管理責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更するものとする。

(作業記録・設定情報等のバックアップの取得と保管)

第190条 部局情報システム管理責任者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管するものとする。

2 部局情報システム管理責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管するものとする。

(通信回線の運用終了時の対策)

第191条 部局情報システム管理責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずるものとする。

(無線 LAN 環境導入時の対策)

第192条 部局情報システム管理責任者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずるものとする。

(無線 LAN 環境導入時の対策)

第193条 部局情報システム管理責任者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、次の各号に掲げるものを例とする対策を講ずるものとする。

- (1) 無線 LAN 通信の暗号化
- (2) IEEE802.1X による無線 LAN へのアクセス主体の認証
- (3) 無線 LAN 回線利用申請手続の整備
- (4) 無線 LAN 機器の管理手順の整備
- (5) 無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対処手順の整備
- (6) 来訪者等に提供する無線 LAN によるインターネット接続回線と業務で使用する本学 LAN の分離

第2節 IPv6 通信回線

(IPv6 通信を行う情報システムに係る対策)

第194条 部局情報システム管理責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択するものとする。

2 部局情報システム管理責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、次の各号に掲げるものを含む脅威又は脆弱性に対する検討を行い、必要な

措置を講ずるものとする。

- (1) グローバル IP アドレスによる直接の到達性における脅威
- (2) IPv6 通信環境の設定不備等に起因する不正アクセスの脅威
- (3) IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生
- (4) アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

(意図しない IPv6 通信の抑止・監視)

第 195 条 部局情報システム管理責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずるものとする。

第 18 章 情報システムの利用

第 1 節 情報システムの利用

(情報システムの利用に係る規定の整備)

第 196 条 情報センター長は、本学の情報システムの利用のうち、情報セキュリティに関する規定を整備するものとする。

2 情報センター長は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定め、当該手順には、次の各号に掲げる事項を含めるものとする。

- (1) 利用者等は、国の行政機関、独立行政法人もしくは指定法人が支給する外部電磁的記録媒体又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により本学との間で取り決めた学外の組織から受け取った外部電磁的記録媒体を使用すること。
- (2) 自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずること。

3 情報センター長は、機密性 3 情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続を定めるものとする。

(情報システムの利用に係る実施手順の整備)

第 197 条 情報センター長は、本学の情報システムの利用のうち、情報セキュリティに関する規定として、次の各号に掲げるものを例とする実施手順を定めるものとする。

- (1) 情報システムの基本的な利用のうち、情報セキュリティに関する手順
- (2) 電子メール及びウェブの利用のうち、情報セキュリティに関する手順
- (3) 識別コードと主体認証情報の取扱手順
- (4) 暗号と電子署名の利用に関する手順
- (5) 不正プログラム感染防止の手順
- (6) アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為の防止に関する手順
- (7) ドメイン名の使用に関する手順
- (8) Web 会議サービス利用時の手順

(USB メモリ等の外部電磁的記録媒体を用いる場合の対策)

第 198 条 情報センター長は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順として、次の各号に掲げるものを含め、定めるものとする。

- (1) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用すること。
- (2) 要機密情報は保存される必要がなくなった時点で速やかに削除すること。
- (3) 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる

検疫・駆除を行うこと。

- (4) 外部電磁的記録媒体の利用者が利用内容を貸出簿等に記録すること。
- 2 情報センター長は、機密性3情報、要保全情報又は要安定情報が記録されたUSBメモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続として、次の各号に掲げるものを含む手続を規定し、利用者等に遵守させるものとする。
 - (1) 利用時の許可申請手続
 - (2) 手続内容（利用者、利用期間、主たる利用場所、目的、記録する情報、機器名）
 - (3) 利用期間満了時の手続
 - (4) 部局責任者による手続内容の記録

（情報システム利用者の規定の遵守を支援するための対策）

- 第199条 部局情報システム管理責任者は、利用者等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築するものとする。

（情報システム利用者の規定の遵守を支援するためのウェブサイト及び電子メールに係る対策）

- 第200条 情報センター長は、学外のウェブサイトについて、利用者等が閲覧できる範囲を制限する機能を情報システムに導入するものとする。この場合においては、次の各号に掲げるものを例とする機能を導入するものとし、当該機能に係る設定や条件については、定期的に見直すものとする。
- (1) ウェブサイトフィルタリング機能
 - (2) 事業者が提供するウェブサイトフィルタリングサービスの利用
- 2 情報センター長は、利用者等が不審なメールを受信することによる被害を抑止する機能を情報システムに導入するものとする。この場合においては、次の各号に掲げるものを例とする機能を導入するものとし、当該機能に係る設定や条件について定期的に見直すものとする。
- (1) 受信メールに対するフィルタリング機能
 - (2) 受信メールをテキスト形式で表示する機能
 - (3) スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがない電子メールクライアントの導入
 - (4) 受信メールに添付されている実行プログラム形式のファイルを削除することで実行させない機能

（情報システムの利用時の基本的対策）

- 第201条 利用者等は、教育研究事務の遂行以外の目的で情報システムを利用しないよう努めなければならない。
- 2 利用者等は、情報センター長が接続許可を与えた通信回線以外に本学の情報システムを接続しないものとする。
 - 3 利用者等は、学内通信回線に情報センター長の接続許可を受けていない情報システムを接続しないものとする。
 - 4 利用者等は、情報システムで利用を禁止するソフトウェアを利用しないものとし、情報システムで利用を認めるソフトウェア以外のソフトウェアを教育研究事務上の必要により利用する場合は、情報センター長の承認を得るものとする。
 - 5 利用者等は、接続が許可されていない機器等を情報システムに接続しないものとする。
 - 6 利用者等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずるものとする。
 - 7 利用者等は、本学が支給する端末（要管理対策区域外で使用する場合に限り）及び本学支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うものとする。
 - 8 利用者等は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、部局責任者の許可を得るものとする。
 - (1) 本学が支給する端末（要管理対策区域外で使用する場合に限り） 機密性3情報、要保全情報又は要安定情報
 - (2) 本学支給以外の端末 要保護情報
 - 9 利用者等は、要管理対策区域外において学外通信回線に接続した端末（本学支給以外の端末を

含む)を要管理対策区域外において学内通信回線に接続する場合は、定められた安全管理措置を講ずるものとする。

- 10 利用者等は、要管理対策区域外において学外通信回線に接続した端末(本学支給以外の端末を含む)を要管理対策区域外において学内通信回線に接続する場合は、情報センター長の許可を得るものとする。
- 11 利用者等は、機密性3情報、要保全情報又は要安定情報が記録されたUSBメモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、部局責任者の許可を得るものとする。

(電子メール・ウェブの利用時の対策)

- 第202条 利用者等は、要機密情報を含む電子メールを送受信する場合には、本学が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用するものとする。
- 2 利用者等は、学外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に大学ドメイン名を使用するものとする。ただし、電子メールを受信する学外の者が、本学の利用者等から送信された電子メールであることを認知できる場合(大学ドメイン名が使用できない場合に限る。)を除く。
 - 3 利用者等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処するものとする。
 - 4 利用者等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないものとする。
 - 5 利用者等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認するものとする。
 - 6 利用者等は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、次の各号に掲げるものを確認するものとする。
 - (1) 送信内容が暗号化されること。
 - (2) 当該ウェブサイトが送信先として想定している組織のものであること。

(識別コード・主体認証情報の取扱い)

- 第203条 利用者等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないものとする。
- 2 利用者等は、自己に付与された識別コードを適切に管理するものとする。
 - 3 利用者等は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用するものとする。
 - 4 利用者等は、自己の主体認証情報の管理を徹底するものとする。

(識別コードの適切な管理に係る対策)

- 第204条 利用者等は、自己に付与された識別コードを適切に管理するため、次の各号に掲げるものを含む措置を講ずるものとする。
- (1) 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。
 - (2) 他者が主体認証に用いるために付与及び貸与しないこと。
 - (3) 識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止すること。

(主体認証情報の適切な管理に係る対策)

- 第205条 利用者等は、知識による主体認証情報を用いる場合には、次の各号に掲げるものの管理を徹底するものとする。
- (1) 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。
 - (2) 自己の主体認証情報を他者に教えないこと。
 - (3) 主体認証情報を忘却しないように努めること。
 - (4) 主体認証情報を設定するに際しては、推測されないものにすること。
 - (5) 異なる識別コードに対して、共通の主体認証情報を用いないこと。
 - (6) 異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いないこと。(シングルサインオンの場合を除く。)
 - (7) 情報センター長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。

2 利用者等は、所有による主体認証情報を用いる場合には、次の各号に掲げるものの管理を徹底するものとする。

- (1) 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。
- (2) 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。
- (3) 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、定められた報告手続に従い、直ちにその旨を報告すること。
- (4) 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、これを部局責任者に返還すること。

(暗号・電子署名の利用時の対策)

第206条 利用者等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うものとする。

- 2 利用者等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理するものとする。
- 3 利用者等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うものとする。

(不正プログラム感染防止)

第207条 利用者等は、不正プログラム感染防止に関する措置に努めるものとする。

- 2 利用者等は、情報システム（本学支給以外の端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずるものとする。

(不正プログラム感染防止に係る対策)

第208条 利用者等は、不正プログラム対策ソフトウェアを活用し、不正プログラム感染を回避するため、次の各号に掲げる措置に努めるものとする。

- (1) 不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しないこと。また、検知されたデータファイルをアプリケーション等で読み込まないこと。
 - (2) 不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。
 - (3) 不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にすること。
 - (4) 不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施すること。
- 2 利用者等は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認するものとする。
 - 3 利用者等は、不正プログラムに感染するリスクを低減する情報システムの利用方法として、次の各号に掲げるもののうち、実施可能な措置を講ずるものとする。
 - (1) 不審なウェブサイトを閲覧しないこと。
 - (2) アプリケーションの利用において、マクロ等の自動実行機能を無効にすること。
 - (3) プログラム及びスクリプトの実行機能を無効にすること。
 - (4) 安全性が確実でないプログラムをダウンロードしたり実行したりしないこと。

(Web 会議サービスの利用時の対策)

第209条 利用者等は、本学の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施するものとする。

- 2 利用者等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずるものとする。

(Web 会議サービスの利用時の対策)

第210条 利用者等は、Web 会議サービスの利用に当たり、次の各号に掲げる情報セキュリティ対策を実施するものとする。

- (1) 原則として、本学が支給する端末を利用すること。
 - (2) 原則として、本学が利用を許可した Web 会議サービスを利用すること。
 - (3) 利用する Web 会議サービスのソフトウェアが、最新の状態であることを確認すること。
 - (4) 要機密情報を取り扱う場合は、可能な限りエンドツーエンド (E2E) の暗号化を行うこと。
 - (5) 要機密情報を取り扱う場合は、Web 会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2E の暗号化を利用できなくなる機能を可能な限り使用しないこと。
- 2 利用者等は、会議に無関係な者を会議に参加させないために、次の各号に掲げるものを例とする対策を行うものとする。
- (1) 会議室にアクセスするためのパスワード等をかけること。
 - (2) 会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知すること。
 - (3) 待機室を設けて参加者と確認できた者だけを会議室に入室させること。
 - (4) なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させること。

第2節 ソーシャルメディアサービスによる情報発信

(ソーシャルメディアサービスによる情報発信時の対策)

第211条 情報センター長は、本学が管理するアカウントでソーシャルメディアサービスを利用することを前提として、次の各号に掲げるものを含む情報セキュリティ対策に関する運用手順等を定めるとともに、当該サービスの利用において要機密情報が取り扱われないよう規定するものとする。

- (1) 本学のアカウントによる情報発信が実際の本学のものであることを明らかにするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずるものとする。
 - (2) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずるものとする。
- 2 部局責任者は、本学において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めるものとする。
- 3 利用者等は、要安定情報の一般利用者への提供にソーシャルメディアサービスを用いる場合は、本学の公式ウェブサイト当該情報を掲載して参照可能なものとする。

(ソーシャルメディアサービスによる情報発信時の対策の手順)

第212条 情報センター長は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、次の各号に掲げるものを含む対策を手順として定めるものとする。

- (1) アカウント運用ポリシー (ソーシャルメディアポリシー) を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている本学の公式ウェブサイト上のページにアカウント運用ポリシーを掲載し、特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示するものとする。
 - (2) URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しないものとする。
- 2 情報センター長は、本学のアカウントによる情報発信が実際の本学のものであると認識できるようにするためのなりすまし対策として、次の各号に掲げるものを含む対策を手順として定めるものとする。
- (1) 本学からの情報発信であることを明らかにするために、大学ドメイン名を用いて管理しているウェブサイト内において、利用するソーシャルメディアのサービス名及びそのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

- (2) 本学からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、本学が運用していることを利用者に明示すること。
 - (3) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている本学の公式ウェブサイト上のページの URL を記載すること。
 - (4) ソーシャルメディアの提供事業者がアカウント管理者を確認し、それを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。
- 3 情報センター長は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、次の各号に掲げるものを含む管理手順を定めるものとする。
- (1) パスワードを適切に管理すること。具体的には、ログインパスワードは十分な長さとし、複雑さを持たせ、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。
 - (2) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。
 - (3) ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭ったりした場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行うこと。
 - (4) ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり端末に保存されたパスワードが窃取されたりする可能性があり、これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。
- 4 情報センター長は、なりすましや不正アクセスを確認した場合の対処として、次の各号に掲げるものを含む対処手順を定めるものとする。
- (1) 本学の公式ウェブサイト、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行うとともに、信用できる機関やメディアを通じて注意喚起を行うこと。
 - (2) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、本学の公式ウェブサイト等で周知を行うとともに、CSIRT に報告するなど、適切な対処を行うこと。

第3節 テレワーク

(実施規程の整備)

第213条 総括責任者は、テレワーク実施時の情報セキュリティ対策に係る規定を整備し、原則としてテレワークは本学が支給する端末で行うよう定めるものとする。

(実施規程の整備)

第214条 総括責任者は、次の各号に掲げるものを例とする項目について、既に本学において整備されている規定に不足があれば、新たに規定を整備するものとする。

- (1) テレワークの実施申請及び承認並びにテレワークの実施報告
- (2) テレワークで取り扱うことができる情報の格付
- (3) テレワークで取り扱う情報の保存場所
- (4) 要管理対策区域外での要機密情報の取扱手続
- (5) テレワークに使用する端末に必要な情報セキュリティ対策
- (6) 本学が支給する端末の持出手続
- (7) 例外的に本学支給以外の端末の利用を認める場合
- (8) 本学支給以外の端末の利用許可手続及び安全管理措置
- (9) テレワーク実施可能な場所
- (10) テレワークに利用可能なネットワーク

(実施環境における対策)

第215条 情報センター長は、テレワークの実施により学外通信回線を経由して本学の情報システムへリモートアクセスする形態となる情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対するセキュリティを確保するものとする。

2 情報センター長は、リモートアクセスに対し多要素主体認証を行うものとする。

3 情報センター長は、リモートアクセスする端末を許可された端末に限定する措置を講じるものとする。

4 情報センター長は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定するものとする。

(実施環境における対策)

第216条 情報センター長は、VPN回線を整備してリモートアクセス環境を構築する場合は、次の各号に掲げるものを例とする対策を講ずるものとする。

(1) 利用開始及び利用停止時の申請手続の整備

(2) 通信を行う端末の識別又は認証

(3) 利用者の認証

(4) 通信内容の暗号化

(5) 主体認証ログの取得及び管理

(6) リモートアクセスにおいて利用可能な公衆通信網の制限

(7) アクセス可能な情報システムの制限

(8) リモートアクセス中の他の通信回線との接続禁止

2 情報センター長は、リモートアクセスする端末が、許可されたものであるかどうかを確認するために、次の各号に掲げるものを例とする対策を行うものとする。

(1) 証明書による端末確認

(2) ソフトウェア認証による端末確認

3 情報センター長は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定するために、次の各号に掲げるものを例とする対策を行うものとする。

(1) 検疫ネットワークの整備

(2) IT資産管理の自動化

(実施時における対策)

第217条 総括責任者は、テレワーク実施前及び実施後に利用者等がチェックすべき項目を定め、利用者等に当該チェックを実施させるものとする。

2 利用者等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定するものとする。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意するものとする。

3 利用者等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な学外通信回線を利用してテレワークを行わないものとする。

(実施時における対策)

第218条 利用者等は、第139条第3項に示した対策のほか、次の各号に掲げる項目を例とする画面ののぞき見や盗聴から発生する情報漏えい対策を講じるものとする。

(1) 背後に人が立たないように背後に通路がない場所で壁を背にする位置に座りテレワークを行うこと。

(2) Web会議等、音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。

(3) 同居する者に対し知り得た情報を他人に漏らさないよう協力を求めること。

2 利用者等は、テレワークに情報セキュリティ対策の状況が不明又は不十分な学外通信回線を利用しないために、次の各号に掲げるものを例とする対策を行うこと。

(1) 公衆無線LANを利用しないこと。

(2) 宿泊施設等が提供する無料ネットワークを利用しないこと。

附 則

この基準は、令和5年12月25日から施行する。

附 則
この基準は、令和 7 年 4 月 1 日から施行する。