C2501 事務情報セキュリティ対策基準

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

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年2月15日  A2501 | 統一基準（全体版初版）をもとに新規作成 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2007年10月31日  A2501 | 統一基準（第２版）に対応した修正 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2011年3月31日  A2201 | 統一基準（第４版）をもとに全面改定 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2013年7月5日  B2501/B2551 | 統一基準（平成24年度版）をもとに全面改定  （管理基準と技術基準に分割） | 高等教育機関における情報セキュリティポリシー推進部会事務局 |
| 2015年10月9日  C2501 | 統一基準（平成26年度版）をもとに全面改定 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |

（注）統一基準＝政府機関の情報セキュリティ対策のための統一基準

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

目　次

[第1部　総則 280](#_Toc431830384)

[1.1 本基準の目的・適用範囲 280](#_Toc431830385)

[1.2 情報の格付の区分・取扱制限 281](#_Toc431830386)

[1.3 用語定義 282](#_Toc431830387)

[第2部　情報セキュリティ対策の基本的枠組み 286](#_Toc431830388)

[2.1 導入・計画 286](#_Toc431830389)

[2.2 運用 290](#_Toc431830390)

[2.3 点検 295](#_Toc431830391)

[2.4 見直し 297](#_Toc431830392)

[第3部　情報の取扱い 298](#_Toc431830393)

[3.1 情報の取扱い 298](#_Toc431830394)

[3.2 情報を取り扱う区域の管理 303](#_Toc431830395)

[第4部　外部委託 306](#_Toc431830396)

[4.1 外部委託 306](#_Toc431830397)

[第5部　情報システムのライフサイクル 313](#_Toc431830398)

[5.1 情報システムに係る文書等の整備 313](#_Toc431830399)

[5.2 情報システムのライフサイクルの各段階における対策 316](#_Toc431830400)

[5.3 情報システムの運用継続計画 323](#_Toc431830401)

[第6部　情報システムのセキュリティ要件 324](#_Toc431830402)

[6.1 情報システムのセキュリティ機能 324](#_Toc431830403)

[6.2 情報セキュリティの脅威への対策 331](#_Toc431830404)

[6.3 アプリケーション・コンテンツの作成・提供 337](#_Toc431830405)

[第7部　情報システムの構成要素 340](#_Toc431830406)

[7.1 端末・サーバ装置等 340](#_Toc431830407)

[7.2 電子メール・ウェブ等 347](#_Toc431830408)

[7.3 通信回線 353](#_Toc431830409)

[第8部　情報システムの利用 359](#_Toc431830410)

[8.1 情報システムの利用 359](#_Toc431830411)

[8.2 本学支給以外の端末の利用 364](#_Toc431830412)

## 第1部　総則

### 1.1 本基準の目的・適用範囲

##### (1) 本基準の目的

情報セキュリティの基本は、高等教育機関で取り扱う情報の重要度に応じた「機密性」・「完全性」・「可用性」を確保することであり、それぞれの高等教育機関が自らの責任において情報セキュリティ対策を講じていくことが原則である。しかし、高等教育機関共通のIT環境の利用、本学間の情報流通の現状を踏まえると、高等教育機関全体の統一的な枠組みを構築し、それぞれの高等教育機関の情報セキュリティ水準の斉一的な引上げを図ることが必要である。

「事務情報セキュリティ対策基準」（以下､「本基準」という。）は、国立大学法人A大学（以下､「本学」という。）の事務局管理の情報及び情報システムの情報セキュリティ強化のための基準である。本基準は、「政府機関の情報セキュリティ対策のための統一基準」（平成26年5月19日付情報セキュリティ政策会議決定。以下､「政府機関統一基準」という。）に基づいて作成したものであり、各国立大学法人が､政府機関統一基準を踏まえた情報セキュリティポリシーの策定ならびに見直しを行う際に、検討のたたき台として活用いただくための標準版である。検討の参考にしていただければ幸いである。

また、政府機関統一基準は、定期的に見直しを行い、その適用性を将来にわたり維持する方針であるため、本基準は、政府機関統一基準の改訂に対応できるよう、構成をほぼ同様にしていることを申し添える。

##### (2) 本基準の適用範囲

###### (a) 本基準において適用範囲とする者は、全ての事務従事者とする。

###### (b) 本基準において適用範囲とする情報は、以下の情報とする。

(ア) 事務従事者が職務上使用することを目的として本学が調達し、又は開発した情報システム若しくは外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

(イ) その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、事務従事者が職務上取り扱う情報

(ウ) (ア)及び(イ)のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報

###### (c) 本基準において適用範囲とする情報システムは、本基準の適用範囲となる情報を取り扱う全ての情報システムとする。

##### (3) 本基準の改訂

情報セキュリティ水準を適切に維持していくためには、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。

このため、情報技術の進歩に応じて、本基準を定期的に点検し、必要に応じ規定内容の追加・修正等の見直しを行う。

##### (4) 法令等の遵守

情報及び情報システムの取扱いに関しては、本基準のほか法令及び基準等（以下「関連法令等」という。）を遵守しなければならない。なお、これらの関連法令等は情報

セキュリティ対策にかかわらず当然に遵守すべきものであるため、本基準では、あえて関連法令等の遵守について明記していない。また、情報セキュリティを巡る状況に応じて策定される政府決定等についても同様に遵守すること。

##### (5) 対策項目の記載事項

本基準では、本学が行うべき対策について、目的別に部、節及び項の３階層にて対策項目を分類し、各項に対して目的、趣旨及び遵守事項を示している。遵守事項は、事務情報セキュリティ対策基準において必ず実施すべき対策事項である。本学が別途整備する事務情報セキュリティ対策基準策定のためのガイドライン及び関連規程等において規定する統一基準の遵守事項に対応した個別具体的な対策実施要件、対策の実施例や解説等も参照し、事務情報セキュリティ対策基準を策定する必要がある。

### 1.2 情報の格付の区分・取扱制限

##### (1) 情報の格付の区分

情報について、機密性、完全性及び可用性の３つの観点を区別し、本基準の遵守事項で用いる格付の区分の定義を示す。

本学において格付の定義を変更又は追加する場合には、それぞれの高等教育機関の対策基準における格付区分と遵守事項との関係が本基準での関係と同等以上となるように準拠しなければならない。また、他本学へ情報を提供する場合は、自身の格付区分と本基準における格付区分の対応について、適切に伝達する必要がある。

機密性についての格付の定義

|  |  |
| --- | --- |
| 格付けの区分 | 分類の基準 |
| 機密性３情報 | 本学で取り扱う情報のうち、秘密文書に相当する機密性を要する情報 |
| 機密性２情報 | 本学で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報 |
| 機密性１情報 | 公表済みの情報、公表しても差し支えない情報等、機密性２情報又は機密性３情報以外の情報 |

なお、機密性２情報及び機密性３情報を「要機密情報」という。

完全性についての格付の定義

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

なお、完全性２情報を「要保全情報」という。

可用性についての格付の定義

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

なお、可用性２情報を「要安定情報」という。また、要機密情報、要保全情報及び要安定情報を「要保護情報」という。

##### (2) 情報の取扱制限

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを事務従事者に確実に行わせるための手段をいう。

事務従事者は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。本学は、取り扱う情報について、機密性、完全性及び可用性の３つの観点から、取扱制限に関する基本的な定義を定める必要がある。

### 1.3 用語定義

事務情報セキュリティ対策基準において次の各号に掲げる用語の定義は、当該各号に定めるところによる。

【あ】

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

【か】

* 「外部委託」とは、本学の情報処理業務の一部又は全部について、契約をもって学外の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。
* 「学外通信回線」とは、通信回線のうち、学内通信回線以外のものをいう。
* 「学内通信回線」とは、一つの本学が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該高等教育機関の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。学内通信回線には、専用線やVPN等物理的な回線を本学が管理していないものも含まれる。
* 「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。
* 「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R等の外部電磁的記録媒体がある。

【さ】

* 「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。
* 「」とは、本学において発生した情報セキュリティインシデントに対処するため、当該高等教育機関に設置された体制をいう。Computer Security Incident Response Teamの略。
* 「実施手順」とは、事務情報セキュリティ対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。
* 「事務従事者」とは、本学において高等教育機関の事務に従事している国家公務員その他の高等教育機関の指揮命令に服している者であって、本学の管理対象である情報及び情報システムを取り扱う者をいう。事務従事者には、個々の勤務条件にもよるが、例えば、派遣労働者等も含まれている。
* 「事務情報セキュリティ対策基準」とは、本学における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。
* 「情報」とは、「1.1(2) 本基準の適用範囲」の(b)に定めるものをいう。
* 「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理及び通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。
* 「情報セキュリティインシデント」とは、JIS Q 27001:2006における情報セキュリティインシデントをいう。
* 「情報セキュリティ関係規程」とは、事務情報セキュリティ対策基準及び実施手順を総称したものをいう。
* 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

【た】

* 「端末」とは、情報システムの構成要素である機器のうち、事務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。
* 「通信回線」とは、複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。
* 「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。
* 「特定用途機器」とは、テレビ会議システム、IP電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。

【は】

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

【ま】

* 「抹消」→「情報の抹消」を参照。
* 「明示等」とは、情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。
* 「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

* 「約款による外部サービス」とは、民間事業者等の学外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。
* 「要管理対策区域」とは、本学が管理する施設等（外部の組織から借用している施設等を含む。）本学の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。

## 第2部　情報セキュリティ対策の基本的枠組み

### 2.1 導入・計画

#### 2.1.1 組織・体制の整備

目的・趣旨

情報セキュリティ対策は、それに係る全ての事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。特に全学総括責任者は、情報セキュリティ対策を着実に進めるために、自らが組織内を統括し、組織全体として計画的に対策が実施されるよう推進しなければならない。

なお、全学総括責任者は、その権限に属する事務の一部を統一基準に定める各責任者に委任することができる。

遵守事項

##### (1) 全学総括責任者の設置

###### (a) 本学は、本学における情報セキュリティに関する事務を統括する全学総括責任者１人を置くこと。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学総括責任者は、次に掲げる事務を統括すること。   1. 情報セキュリティ対策推進のための組織・体制の整備 2. 事務情報セキュリティ対策基準の決定、見直し 3. 対策推進計画の決定、見直し 4. 情報セキュリティインシデントに対処するために必要な指示その他の措置 5. 前各号に掲げるもののほか、情報セキュリティに関する重要事項 |

##### (2) 全学情報システム運用委員会の設置

###### (a) 全学総括責任者は、事務情報セキュリティ対策基準等の審議を行う機能を持つ組織として、本学の情報セキュリティを推進する部局及びその他高等教育機関の事務を実施する部局の代表者を構成員とする全学情報システム運用委員会を置くこと。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 全学情報システム運用委員会の委員長及び委員は、全学総括責任者が情報セキュリティを推進する部局及びその他の高等教育機関の事務を実施する部局の代表者から指名すること。  (2)-2 全学情報システム運用委員会は、次に掲げる事項を審議すること。   1. 事務情報セキュリティ対策基準 2. 対策推進計画 3. 前各号に掲げるもののほか、情報セキュリティに関し必要な事項 |

##### (3) 情報セキュリティ監査責任者の設置

###### (a) 全学総括責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くこと。

|  |
| --- |
| 【 基本対策事項 】  (3)-1 情報セキュリティ監査責任者は、命により次の事務を統括すること。   1. 監査実施計画の策定 2. 監査実施体制の整備 3. 監査の実施指示及び監査結果の全学総括責任者への報告 4. 前各号に掲げるもののほか、情報セキュリティの監査に関する事項 |

##### (4) 全学実施責任者・部局総括責任者等の設置

###### (a) 全学総括責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、部局総括責任者１人を置くこと。そのうち、部局総括責任者を統括し、全学総括責任者を補佐する者として、全学実施責任者１人を選任すること。

###### (b) 部局総括責任者は、遵守事項3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者1人を置くこと。

###### (c) 部局総括責任者は、課室ごとに情報セキュリティ対策に関する事務を統括する職場情報セキュリティ責任者1人を置くこと。

###### (d) 部局総括責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、部局技術責任者を、当該情報システムの企画に着手するまでに選任すること。

|  |
| --- |
| 【 基本対策事項 】  (4)-1 全学実施責任者は、命を受け、次の事務を統括すること。   1. 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定 2. 情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務のとりまとめ 3. 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備 4. 例外措置の適用審査記録の台帳整備等 5. 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等 6. 前各号に掲げるもののほか、情報セキュリティ対策に係る事務   (4)-2 部局総括責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括すること。   1. 定められた区域ごとの区域情報セキュリティ責任者の設置 2. 課室の職場情報セキュリティ責任者の設置 3. 情報システムごとの部局技術責任者の設置 4. 情報セキュリティインシデントの原因調査、再発防止策等の実施 5. 情報セキュリティに係る自己点検計画の策定及び実施手順の整備 6. 前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務   (4)-3 区域情報セキュリティ責任者は、命を受け、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を統括すること。  (4)-4 職場情報セキュリティ責任者は、命を受け、課室における情報の取扱いその他の情報セキュリティ対策に関する事務を統括すること。  (4)-5 部局技術責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。  (4)-6 部局技術責任者は、所管する情報システムの管理業務において必要な単位ごとに**部局技術担当者**を置くこと。 |

##### (5) 情報セキュリティアドバイザーの設置

###### (a) 全学総括責任者は、情報セキュリティについて専門的な知識及び経験を有する者を情報セキュリティアドバイザーとして置き、自らへの助言を含む情報セキュリティアドバイザーの業務内容を定めること。

|  |
| --- |
| 【 基本対策事項 】  (5)-1 全学総括責任者は、以下を例とする情報セキュリティアドバイザーの業務内容を定めること。   1. 本学全体の情報セキュリティ対策の推進に係る全学総括責任者への助言 2. 情報セキュリティ関係規程の整備に係る助言 3. 対策推進計画の策定に係る助言 4. 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援 5. 情報システムに係る技術的事項に係る助言 6. 情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言 7. 事務従事者に対する日常的な相談対応 8. 情報セキュリティインシデントへの対処の支援 9. 前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援 |

##### (6) 情報セキュリティインシデントに備えた体制の整備

###### (a) 全学総括責任者は、CSIRTを整備し、その役割を明確化すること。

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

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

|  |
| --- |
| 【 基本対策事項 】  (6)-1 全学総括責任者は、以下を含むCSIRTの役割を規定すること。   1. 報告窓口からの情報セキュリティインシデントの報告の受付 2. 情報セキュリティインシデントの全学総括責任者等への報告 3. 文部科学省及び内閣サイバーセキュリティセンターへの連絡 4. 被害の拡大防止を図るための応急措置の指示又は勧告   (6)-2 全学総括責任者は、CSIRTの代表者（PoC（Point of Contact））を置くこと。 |

##### (7) 兼務を禁止する役割

###### (a) 事務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

(ア) 承認又は許可（以下、本項において「承認等」という。）の申請者と当該承認等を行う者（以下、本項において「承認権限者等」という。）

(イ) 監査を受ける者とその監査を実施する者

###### (b) 事務従事者は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。

#### 2.1.2 事務情報セキュリティ対策基準・対策推進計画の策定

目的・趣旨

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

遵守事項

##### (1) 事務情報セキュリティ対策基準の策定

###### (a) 全学総括責任者は、全学情報システム運用委員会における審議を経て、統一基準に準拠した事務情報セキュリティ対策基準を定めること。

##### (2) 対策推進計画の策定

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

(ア) 情報セキュリティに関する教育

(イ) 情報セキュリティ対策の自己点検

(ウ) 情報セキュリティ監査

(エ) 情報システムに関する技術的な対策を推進するための取組

(オ) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

### 2.2 運用

#### 2.2.1 情報セキュリティ関係規程の運用

目的・趣旨

本学は、事務情報セキュリティ対策基準に定められた対策を実施するため、具体的な実施手順を定める必要がある。

実施手順が整備されていない、又はそれらの内容に漏れがあると、対策が実施されないおそれがあることから、全学総括責任者は、全学実施責任者に実施手順の整備を指示し、その結果について定期的に報告を受け、状況を適確に把握することが重要である。

遵守事項

##### (1) 情報セキュリティ対策に関する実施手順の整備・運用

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

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

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

##### (2) 違反への対処

###### (a) 事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合は、部局総括責任者にその旨を報告すること。

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

#### 2.2.2 例外措置

目的・趣旨

情報セキュリティ関係規程の適用が高等教育機関の事務の適正な遂行を著しく妨げるなどの理由により、規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合がある。このような場合に対処するために、例外措置の手続を定めておく必要がある。

遵守事項

##### (1) 例外措置手続の整備

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

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

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学総括責任者は、例外措置について以下を含む手順を定めること。   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   (1)-2 許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、全学実施責任者へ定期的に報告すること。   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 |

##### (2) 例外措置の運用

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

###### (b) 許可権限者は、事務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。

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

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

#### 2.2.3 教育

目的・趣旨

情報セキュリティ関係規程が適切に整備されているとしても、その内容が事務従事者に周知されず、これが遵守されない場合には、情報セキュリティ水準の向上を望むことはできない。このため、全ての事務従事者が、情報セキュリティの教育を通じ、情報セキュリティ関係規程への理解を深め、情報セキュリティ対策を適切に実施することが求められる。

遵守事項

##### (1) 教育体制等の整備

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

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、事務従事者の役割に応じて**教育すべき内容を検討**し、教育のための資料を整備すること。  (1)-2 全学実施責任者は、**事務従事者が毎年度最低１回は教育を受講**できるように、教育実施計画を立案するとともに、その実施体制を整備すること。  (1)-3 全学実施責任者は、事務従事者の着任又は異動後に、**３か月以内に受講**できるように、その実施体制を整備すること。 |

##### (2) 教育の実施

###### (a) 職場情報セキュリティ責任者は、事務従事者に対して、情報セキュリティ関係規程に係る教育を適切に受講させること。

###### (b) 事務従事者は、教育実施計画に従って、適切な時期に教育を受講すること。

###### (c) 職場情報セキュリティ責任者は、CSIRTに属する職員に教育を適切に受講させること。

###### (d) 全学実施責任者は、全学総括責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。

#### 2.2.4 情報セキュリティインシデントへの対処

目的・趣旨

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

遵守事項

##### (1) 情報セキュリティインシデントに備えた事前準備

###### (a) 全学実施責任者は、情報セキュリティインシデント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、事務従事者に周知すること。

###### (b) 全学実施責任者は、情報セキュリティインシデントを認知した際の学外との情報共有を含む対処手順を整備すること。

###### (c) 全学実施責任者は、情報セキュリティインシデントに備え、高等教育機関の事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

###### (d) 全学実施責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、高等教育機関の事務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備すること。

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

##### (2) 情報セキュリティインシデントの認知時における報告・対処

###### (a) 事務従事者は、情報セキュリティインシデントを認知した場合には、本学の報告窓口に報告し、指示に従うこと。

###### (b) CSIRT責任者は、情報セキュリティインシデントを認知した場合にはその状況を確認し、情報セキュリティインシデントについて全学総括責任者に速やかに報告すること。

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

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

###### (e) 部局技術責任者は、認知した情報セキュリティインシデントが複数の本学で共通的に使用する情報システム（一本学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。以下「基盤となる情報システム」という。）に関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処すること。

###### (f) 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、文部科学省及び内閣サイバーセキュリティセンターに連絡すること。また、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。さらに、国民の生活、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態等においては、「大規模サイバー攻撃等への初動対処について（平成22年3月19日内閣危機管理監決裁）」に基づく報告も行うこと。

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

###### (h) CSIRTは、学外事業者等による情報セキュリティ関連サービスの支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うこと。

##### (3) 情報セキュリティインシデントの原因調査・再発防止

###### (a) 部局総括責任者は、CSIRTの指示を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として全学総括責任者に報告すること。

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

### 2.3 点検

#### 2.3.1 情報セキュリティ対策の自己点検

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ関係規程の遵守状況等を点検し、その結果を把握・分析することが必要である。

自己点検は、事務従事者が自らの役割に応じて実施すべき対策事項を実際に実施しているかどうかを確認するだけではなく、組織全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要である。

また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

遵守事項

##### (1) 自己点検計画の策定・手順の準備

###### (a) 全学実施責任者は、対策推進計画に基づき年度自己点検計画を策定すること。

###### (b) 部局総括責任者は、事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。

##### (2) 自己点検の実施

###### (a) 部局総括責任者は、年度自己点検計画に基づき、事務従事者に自己点検の実施を指示すること。

###### (b) 事務従事者は、部局総括責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。

##### (3) 自己点検結果の評価・改善

###### (a) 全学実施責任者及び部局総括責任者は、事務従事者による自己点検結果を分析し、評価すること。全学実施責任者は評価結果を全学総括責任者に報告すること。

###### (b) 全学総括責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、全学実施責任者及び部局総括責任者に改善を指示すること。

#### 2.3.2 情報セキュリティ監査

目的・趣旨

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

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

遵守事項

##### (1) 監査実施計画の策定

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

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

|  |
| --- |
| 【 基本対策事項 】  (1)-1 情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする**監査実施計画**を策定すること。   1. 監査の目的（例：自己点検の適切性を監査すること等） 2. 監査の対象（例：監査の対象となる組織、情報システム、業務等） 3. 監査の方法（例：自己点検結果を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、事務情報セキュリティ対策基準及び実施手順とする） 4. 監査の実施体制（例：監査責任者、監査実施者の所属、氏名） 5. 監査の実施時期（例：対象ごとの実施時期） |

##### (2) 監査の実施

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

(ア) 事務情報セキュリティ対策基準に統一基準を満たすための適切な事項が定められていること

(イ) 実施手順が事務情報セキュリティ対策基準に準拠していること

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

|  |
| --- |
| 【 基本対策事項 】  (2)-1 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、**被監査部門から独立した者**から選定し、情報セキュリティ監査実施者に指名すること。  (2)-2 情報セキュリティ監査責任者は、組織内における監査遂行能力が不足等している場合には、**学外の者に監査の一部を請け負わせる**こと。 |

##### (3) 監査結果に応じた対処

###### (a) 全学総括責任者は、監査報告書の内容を踏まえ、指摘事項に対する対処計画の策定等を部局総括責任者に指示すること。

###### (b) 部局総括責任者は、監査報告書等に基づいて全学総括責任者から改善を指示されたことについて、対処計画を策定し、報告すること。

|  |
| --- |
| 【 基本対策事項 】  (3)-1 全学総括責任者は、監査報告書の内容を踏まえ監査を受けた部門以外の部門においても同種の課題又は問題点がある可能性が高く、並びに緊急に同種の課題又は問題点があることを確認する必要があると判断した場合には、他の部門の部局総括責任者に対しても、同種の課題又は問題点の有無を確認するように指示すること。 |

### 2.4 見直し

#### 2.4.1 情報セキュリティ対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、本学の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、実際の運用において生じた課題、自己点検、監査の結果等を踏まえて、適時見直しを行う必要がある。

また、自己点検、監査等の結果を総合的に評価して、情報セキュリティに係る取組をより一層推進するために、取組を見直すことも重要である。

遵守事項

##### (1) 情報セキュリティ関係規程の見直し

###### (a) 全学総括責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、全学情報システム運用委員会の審議を経て、事務情報セキュリティ対策基準について必要な見直しを行うこと。

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

##### (2) 対策推進計画の見直し

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

## 第3部　情報の取扱い

### 3.1 情報の取扱い

#### 3.1.1 情報の取扱い

目的・趣旨

高等教育機関の事務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下、本項において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての事務従事者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、事務従事者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

遵守事項

##### (1) 情報の取扱いに係る規定の整備

###### (a) 全学実施責任者は、以下を含む情報の取扱いに関する規定を整備し、事務従事者へ周知すること。

(ア) 情報の格付及び取扱制限についての定義

(イ) 情報の格付及び取扱制限の明示等についての手続

(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、情報の取扱いに関する規定として、以下を例とする手順を整備すること。   1. 情報のライフサイクル全般にわたり必要な手順（高等教育機関の事務の遂行以外の目的での情報の利用等の禁止等） 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   (1)-2 全学実施責任者は、情報の格付及び取扱制限の**明示の方法**について、以下を例に、規定を整備すること。   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   (1)-3 全学実施責任者は、情報の格付及び取扱制限の**明示を省略**する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、規定を整備すること。  (1)-4 全学実施責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例に、規定を整備すること。   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。 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。 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。 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。 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。 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（以下本項において「決定者等」という。）に確認を求める。 |

##### (2) 情報の目的外での利用等の禁止

###### (a) 事務従事者は、自らが担当している高等教育機関の事務の遂行のために必要な範囲に限って、情報を利用等すること。

##### (3) 情報の格付及び取扱制限の決定・明示等

###### (a) 事務従事者は、情報の作成時及び学外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。

###### (b) 事務従事者は、情報を機密性３情報と決定した場合には、機密性３情報として取り扱う期間を明示等すること。

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

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

##### (4) 情報の利用・保存

###### (a) 事務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。

###### (b) 事務従事者は、機密性３情報について要管理対策区域外で情報処理を行う場合は、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。

###### (c) 事務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。

###### (d) 事務従事者は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。

###### (e) 事務従事者は、USBメモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。

|  |
| --- |
| 【 基本対策事項 】  (4)-1 事務従事者は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱うこと。   1. 要保護情報を**放置しない**こと。 2. 機密性３情報を**必要以上に複製しない**こと。 3. 要機密情報を必要以上に配布しないこと。 4. 閲覧可能範囲の制限が指定されている情報については、制限範囲外の者に情報の参照等をさせないために、施錠のできる書庫・保管庫に保存する。 5. 書面に機密性３情報を出力する場合は、書面ごとに一連番号を付与し、その所在を明らかにしておく。 6. 電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行う。 7. 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する。 8. 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。 9. 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。 10. 情報の格付又は取扱制限が明示等されていない場合には、情報の作成元への確認を行う。 |

##### (5) 情報の提供・公表

###### (a) 事務従事者は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。

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

###### (c) 事務従事者は、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、職場情報セキュリティ責任者の許可を得ること。

###### (d) 事務従事者は、電磁的記録を提供又は公表する場合には、当該電磁的記録の付加記録（更新の履歴、文書のプロパティ等をいう。）等からの不用意な情報漏えいを防止するための措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (5)-1 事務従事者は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。 |

##### (6) 情報の運搬・送信

###### (a) 事務従事者は、機密性３情報、要保全情報又は要安定情報を、要管理対策区域外に持ち出し他の場所に運搬する場合又は学外通信回線を使用して送信する場合には、職場情報セキュリティ責任者の許可を得ること。

###### (b) 事務従事者は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。ただし、他本学の要管理対策区域であって、全学実施責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域と見なすことができる。

###### (c) 事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (6)-1 事務従事者は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、**セキュアな運送サービス**を提供する運送事業者により運搬すること。  (6)-2 事務従事者は、要機密情報である電磁的記録を要管理対策区域外に運搬又は学外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。   1. 運搬又は送信する情報を暗号化する。 2. 運搬又は送信を**複数の情報に分割して**それぞれ異なる経路及び手段を用いる。 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。   (6)-3 事務従事者は、要保全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、情報の改ざんを防止するため、以下を例とする措置を講ずること。   1. 電子署名を付与する。 2. あらかじめバックアップを取得しておく。   (6)-4 事務従事者は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。   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. 本学独自で運用するなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。 |

##### (7) 情報の消去

###### (a) 事務従事者は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。

###### (b) 事務従事者は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。

###### (c) 事務従事者は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

##### (8) 情報のバックアップ

###### (a) 事務従事者は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。

###### (b) 事務従事者は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。

###### (c) 事務従事者は、保存期間を過ぎた情報のバックアップについては、本項(7)の規定に従い、適切な方法で消去、抹消又は廃棄すること。

|  |
| --- |
| 【 基本対策事項 】  (8)-1 事務従事者は、要保全情報又は要安定情報である電磁的記録又は重要な設計書について、バックアップを取得すること。  (8)-2 事務従事者は、要保全情報、要安定情報である電磁的記録のバックアップ又は**重要な設計書**のバックアップの保管について、災害等により生ずる業務上の支障を考慮し、**適切なバックアップの手段又は保管場所**を選定すること。 |

### 3.2 情報を取り扱う区域の管理

#### 3.2.1 情報を取り扱う区域の管理

目的・趣旨

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

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

遵守事項

##### (1) 要管理対策区域における対策の基準の決定

###### (a) 全学実施責任者は、要管理対策区域の範囲を定めること。

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

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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、以下を例とする、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を定めること。   1. 下表のとおり、３段階のクラスを定める。  |  |  | | --- | --- | | クラス | 説明 | | クラス３ | 一部の限られた者以外の者の立入りを制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域 | | クラス２ | 事務従事者以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域 | | クラス１ | クラス３、クラス２以外の要管理対策区域 |   ※便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。  (1)-2 全学実施責任者は、クラス１の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。   1. 不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。 2. 不特定の者が容易に立ち入らないように、**立ち入る者の身元、訪問目的等の確認を行うための措置**を講ずること。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。 3. クラス２以上の区域に不正に立ち入った者を容易に判別することができるように、以下を含む措置を講ずること。    * 事務従事者は、身分証明書等を着用、明示する。クラス２及びクラス３の区域においても同様とする。    * 一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス２及びクラス３の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。   (1)-3 全学実施責任者は、クラス２の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。   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こと。ただし、窓口のある執務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は事務従事者が窓口を常に目視できるような措置を講ずること。 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こと。 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**を講ずること。   (1)-4 全学実施責任者は、クラス３の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。   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こと。 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**を講ずること。 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こと。 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こと。業者が作業を行う場合は立会いや監視カメラ等により監視するための措置を講ずること。   (1)-5 全学実施責任者は、以下を例とする、区域への**クラスの割当ての基準**を定めること。   1. クラスの割当ての基準を以下のように定める。    * サーバ室や日常的に機密性が高い情報を取り扱う執務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス３を割り当てる。    * 一般的な執務室や執務室内の会議室には、事務従事者以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス２を割り当てる。 |

##### (2) 区域ごとの対策の決定

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

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

|  |
| --- |
| 【 基本対策事項 】  (2)-1 区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に**割り当てるクラスを決定する**とともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う高等教育機関の事務の内容、取り扱う情報等を勘案し、**当該区域において実施する対策を決定する**こと。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する**個別の対策**を含め決定すること。 |

##### (3) 要管理対策区域における対策の実施

###### (a) 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。事務従事者が実施すべき対策については、事務従事者が認識できる措置を講ずること。

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

###### (c) 事務従事者は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、事務従事者が学外の者を立ち入らせる際には、当該高等教育機関外の者にも当該区域で定められた対策に従って利用させること。

|  |
| --- |
| 【 基本対策事項 】  (3)-1 区域情報セキュリティ責任者は、管理する区域について、以下を例とする利用手順等を整備し、当該区域を利用する事務従事者に周知すること。   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4部　外部委託

### 4.1 外部委託

#### 4.1.1 外部委託

目的・趣旨

学外の者に、情報システムの開発、アプリケーションプログラムの開発等を委託する際に、事務従事者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において事務情報セキュリティ対策基準に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

外部委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任等様々であるが、いずれの場合においても外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお、民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等、1.5節において「約款による外部サービス」として定義するものを利用し、高等教育機関の事務を遂行する場合も外部委託の一つの形態と考えられるが、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、その際は本項に代えて4.1.2項「約款による外部サービスの利用」を適用してもよい。

＜外部委託の例＞

* 情報システムの開発及び構築
* アプリケーションプログラムやウェブコンテンツ等（以下｢アプリケーション・コンテンツ」という。）の開発
* 情報システムの運用
* パブリッククラウド等外部サービス利用による情報処理役務
* 業務運用支援業務（統計、集計、データ入力、媒体変換等）
* プロジェクト管理支援業務等
* 調査・研究業務（調査、研究、検査等）
* 情報システム、データセンター、通信回線等の賃貸借

遵守事項

##### (1) 外部委託に係る規定の整備

###### (a) 全学実施責任者は、外部委託に係る以下の内容を含む規定を整備すること。

(ア) 外部委託を認める情報システムの範囲並びに委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準

(イ) 委託先の選定基準

##### 2) 外部委託に係る契約

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

(ア) 委託先に提供する情報の委託先における目的外利用の禁止

(イ) 委託先における情報セキュリティ対策の実施内容及び管理体制

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

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

(オ) 情報セキュリティインシデントへの対処方法

(カ) 情報セキュリティ対策その他の契約の履行状況の確認方法

(キ) 情報セキュリティ対策の履行が不十分な場合の対処方法

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

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

###### (c) 部局技術責任者又は職場情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(a)(b)の措置の実施を委託先に担保させること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者又は職場情報セキュリティ責任者は、以下の内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させること。また、変更があった場合は、速やかに再提出させること。   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)-2 部局技術責任者又は職場情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む**情報の取扱手順**について委託先と合意し、定められた手順により情報を取り扱うこと。 |

##### (3) 外部委託における対策の実施

###### (a) 部局技術責任者又は職場情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。

###### (b) 部局技術責任者又は職場情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を事務従事者より受けた場合は、当該サービスの利用を中止するなど、必要な措置を講じ、委託先に契約に基づく必要な措置を講じさせること。

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

##### (4) 外部委託における情報の取扱い

###### (a) 事務従事者は、委託先への情報の提供等において、以下の事項を遵守すること。

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

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

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

#### 4.1.2 約款による外部サービスの利用

目的・趣旨

外部委託により高等教育機関の事務を遂行する場合は、原則として4.1.1項「外部委託」にて規定する事項について、委託先と特約を締結するなどし、情報セキュリティ対策を適切に講ずる必要がある。しかしながら、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合には、民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等、1.5節において「約款による外部サービス」として定義するものを利用することも考えられる。

このような「約款による外部サービス」をやむを得ず利用する場合には、リスクを十分踏まえた上で利用を判断し、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

##### (1) 約款による外部サービスの利用に係る規定の整備

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

(ア) 約款による外部サービスを利用してよい業務の範囲

(イ) 業務に利用する約款による外部サービス

(ウ) 利用手続及び運用手順

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

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、本学において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定めること。   1. 利用申請の**許可権限者** 2. 利用申請時の申請内容    * 利用する組織名    * 利用するサービス    * 利用目的（業務内容）    * 利用期間    * **利用責任者（利用アカウントの責任者）** 3. サービス利用中の安全管理に係る運用手順    * サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認    * 情報の滅失、破壊等に備えたバックアップの取得    * 利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等） 4. 情報セキュリティインシデント発生時の連絡体制 |

##### (2) 約款による外部サービスの利用における対策の実施

###### (a) 事務従事者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

#### 4.1.3 ソーシャルメディアサービスによる情報発信

目的・趣旨

インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していく様々なソーシャルメディアサービスが普及している。本学においても、積極的な広報活動等を目的に、こうしたサービスが利用されるようになっている。しかし、ソーシャルメディアサービスを使うには、約款による外部サービスを利用せざるを得ず、A大学ドメイン名を使用することもできないため、本学になりすましたアカウントが現れる可能性を避けらない。また、本学のアカウントを乗っ取られる場合や、利用しているソーシャルメディアサービスが予告なくサービス停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報等の重要な情報を広く提供する際には、本学の自己管理ウェブサイトに当該情報を掲載した上でソーシャルメディアサービスを併用するなど、当該情報を必要とする利用者等が一次情報源を確認できる形での情報発信が必要である。加えて、虚偽情報により利用者等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。

このようなソーシャルメディアサービスは機能拡張やサービス追加等の技術進展が激しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。

遵守事項

##### (1) ソーシャルメディアサービスによる情報発信時の対策

###### (a) 全学実施責任者は、本学が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。

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

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

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

###### (c) 事務従事者は、要安定情報の学外への提供にソーシャルメディアサービスを用いる場合は、本学の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定めること。   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ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。 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。   (1)-2 全学実施責任者は、本学のアカウントによる情報発信が実際の本学のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定めること。   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、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。 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、本学がA大学ドメイン名を用いて管理しているウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。 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。   (1)-3 全学実施責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定めること。   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る。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。   (1)-4 全学実施責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定めること。   1. 自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。 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、自己管理ウェブサイト等で周知を行うとともに、自組織のCSIRTや文部科学省、内閣サイバーセキュリティセンターに報告するなど、適切な対処を行うこと。 |

## 第5部　情報システムのライフサイクル

### 5.1 情報システムに係る文書等の整備

#### 5.1.1 情報システムに係る台帳等の整備

目的・趣旨

本学が所管する情報システムの情報セキュリティ水準を維持するとともに、情報セキュリティインシデントに適切かつ迅速に対処するためには、本学が所管する情報システムの情報セキュリティ対策に係る情報を情報システム台帳で一元的に把握するとともに、情報システムの構成要素に関する調達仕様書や設定情報等が速やかに確認できるように、日頃から文書として整備しておき、その所在を把握しておくことが重要である。

遵守事項

##### (1) 情報システム台帳の整備

###### (a) 全学実施責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。

###### (b) 部局技術責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について全学実施責任者に報告すること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、以下の内容を含む台帳を整備すること。   1. 情報システム名 2. 管理課室 3. 当該部局技術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**   また、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備すること。   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（インターネット上で提供される情報処理サービスを利用する場合） 6. 取り扱う情報の格付及び取扱制限に関する事項   (1)-2 部局技術責任者は、**政府情報システム管理データベースの登録対象となるシステム**については、当該データベースに必要な情報を記録すること。 |

##### (2) 情報システム関連文書の整備

###### (a) 部局技術責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備すること。

(ア) 情報システムを構成するサーバ装置及び端末関連情報

(イ) 情報システムを構成する通信回線及び通信回線装置関連情報

(ウ) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

(エ) 情報セキュリティインシデントを認知した際の対処手順

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備すること。   1. サーバ装置及び端末を**管理する事務従事者**及び利用者を特定する情報 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の**仕様書又は設計書**   (2)-2 部局技術責任者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、以下を含む文書を整備すること。   1. 通信回線及び通信回線装置を**管理する事務従事者**を特定する情報 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   (2)-3 部局技術責任者は、所管する情報システムについて、情報システム構成要素ごとの**セキュリティ維持に関する以下を含む手順**を定めること。   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 |

#### 5.1.2 機器等の調達に係る規定の整備

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。

これらの課題に対応するため、事務情報セキュリティ対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

##### (1) 機器等の調達に係る規定の整備

###### (a) 全学実施責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を本学が確認できることを加えること。

###### (b) 全学実施責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を例に規定すること。   1. 調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、本学と調達先が連携して原因を調査・排除できる体制を整備していること。   (1)-2 全学実施責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、**ISO/IEC 15408に基づく認証**を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定めること。  (1)-3 全学実施責任者は、機器等の納入時の確認・検査手続には以下を含む事項を確認できる手続を定めること。   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 |

### 5.2 情報システムのライフサイクルの各段階における対策

#### 5.2.1 情報システムの企画・要件定義

目的・趣旨

情報システムのライフサイクル全般を通じて、情報セキュリティを適切に維持するためには、情報システムの企画段階において、情報システムの情報セキュリティの維持が実施可能な体制の整備、情報システムのライフサイクルに応じた様々な情報セキュリティリスクに対する要件定義が求められる。

セキュリティ要件の曖昧さや過不足は、過剰な情報セキュリティ対策に伴うコスト増加のおそれ、要件解釈のばらつきによる提案内容の差異からの不公平な競争入札、設計・開発工程での手戻り、運用開始後の情報セキュリティインシデントの発生といった不利益が生じる可能性が考えられる。

そのため、情報システムが対象とする業務、業務において取り扱う情報、情報を取り扱う者、情報を処理するために用いる環境・手段等を考慮した上で、当該情報システムにおいて想定される脅威への対策を検討し、必要十分なセキュリティ要件を仕様に適切に組み込むことが重要となる。

加えて、構築する情報システムへの脆弱性の混入を防止するための対策も、構築前の企画段階で考慮することが重要となる。

また、情報システムの構築、運用・保守を外部委託する場合については、4.1.1項「外部委託」についても併せて遵守する必要がある。

遵守事項

##### (1) 実施体制の確保

###### (a) 部局技術責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者に求めること。

###### (b) 部局技術責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し、運用管理する本学が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めること。

##### (2) 情報システムのセキュリティ要件の策定

###### (a) 部局技術責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、以下の事項を含む情報システムのセキュリティ要件を策定すること。

(ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

(イ) 情報システム運用時の監視等の運用管理機能要件

(ウ) 情報システムに関連する脆弱性についての対策要件

###### (b) 部局技術責任者は、学外利用者・企業と本学との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定すること。

###### (c) 部局技術責任者は、機器等を調達する場合には、「IT製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

###### (d) 部局技術責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、「**情報システムに係る政府調達におけるセキュリティ要件策定マニュアル**」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定すること。  (2)-2 部局技術責任者は、**開発する情報システム**が運用される際に想定される脅威の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書等に明記すること。  (2)-3 部局技術責任者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、**ST確認**を受けること。  (2)-4 部局技術責任者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、以下を含む措置を実施すること。   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、以下を例とする機能を仕様書等に明記すること。    * 学外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能    * 不正プログラム感染や踏み台に利用されること等による学外への不正な通信を監視する機能    * 学内通信回線への端末の接続を監視する機能    * 端末への外部電磁的記録媒体の挿入を監視する機能    * サーバ装置等の機器の動作を監視する機能   (2)-5 部局技術責任者は、開発する情報システムに関連する**脆弱性への対策**が実施されるよう、以下を含む対策を仕様書等に明記すること。   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。   (2)-6 部局技術責任者は、構築する情報システムの構成要素のうち製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施すること。   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。 |

##### (3) 情報システムの構築を外部委託する場合の対策

###### (a) 部局技術責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させること。

(ア) 情報システムのセキュリティ要件の適切な実装

(イ) 情報セキュリティの観点に基づく試験の実施

(ウ) 情報システムの開発環境及び開発工程における情報セキュリティ対策

|  |
| --- |
| 【 基本対策事項 】  (3)-1 部局技術責任者は、情報セキュリティの観点に基づく試験の実施について、以下を含む事項を実施させること。   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。   (3)-2 部局技術責任者は、**開発工程における情報セキュリティ対策**として、以下を含む事項を実施させること。   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、き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。 |

##### (4) 情報システムの運用・保守を外部委託する場合の対策

###### (a) 部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。

|  |
| --- |
| 【 基本対策事項 】  (4)-1 部局技術責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を含む要件を調達仕様書に記載するなどして、適切に実施させること。   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 |

#### 5.2.2 情報システムの調達・構築

目的・趣旨

情報システムを調達・構築する際には、策定したセキュリティ要件に基づく情報セキュリティ対策を適切に実施するために、選定基準に適合した機器等の調達や、情報システムの開発工程での情報セキュリティ対策の実施が求められる。

また、機器等の納入時又は情報システムの受入れ時には、整備された検査手続に従い、当該情報システムが運用される際に取り扱う情報を保護するためのセキュリティ機能及びその管理機能が、適切に情報システムに組み込まれていることを検査することが必要となる。

遵守事項

##### (1) 機器等の選定時の対策

###### (a) 部局技術責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用すること。

##### (2) 情報システムの構築時の対策

###### (a) 部局技術責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。

###### (b) 部局技術責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、情報システムの構築において以下を含む**情報セキュリティ対策**を行うこと。   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、き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)-2 部局技術責任者は、情報システムの運用保守段階へ移行するに当たり、以下を含む情報セキュリティ対策を行うこと。   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 |

##### (3) 納品検査時の対策

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

#### 5.2.3 情報システムの運用・保守

目的・趣旨

情報システムの運用段階に移るに当たり、企画又は調達・構築時に決定したセキュリティ要件が適切に運用されるように、人的な運用体制を整備し、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を実施する必要がある。

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生することが大半であることから、適宜情報システムの情報セキュリティ対策の実効性を確認するために、情報システムの運用状況を監視することも重要である。

また、情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても、事務情報セキュリティ対策基準に基づく情報セキュリティ対策について適切に措置を講ずることが求められる。

遵守事項

##### (1) 情報システムの運用・保守時の対策

###### (a) 部局技術責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。

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

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

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、情報システムのセキュリティ監視を行う場合は、以下の内容を含む監視手順を定め、適切に監視運用すること。   1. 監視するイベントの種類 2. 監視体制 3. 監視状況及び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 4. 監視運用における情報の取扱い（機密性の確保）   (1)-2 部局技術責任者は、情報システムに実装された**セキュリティ機能が適切に運用されていること**を確認すること。  (1)-3 部局技術責任者は、情報システムにおいて取り扱う情報について、**当該情報の格付及び取扱制限が適切に守られていること**を確認すること。  (1)-4 部局技術責任者は、運用中の情報システムの**脆弱性の存在が明らかになった場合**には、情報セキュリティを確保するための措置を講ずること。 |

#### 5.2.4 情報システムの更改・廃棄

目的・趣旨

情報システムの更改・廃棄において、情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。

情報システムに機密性の高い情報が記録されている場合や、格付や取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講ずることが必要となる。

遵守事項

##### (1) 情報システムの更改・廃棄時の対策

###### (a) 部局技術責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。

(ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策

(イ) 情報システム廃棄時の不要な情報の抹消

#### 5.2.5 情報システムについての対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、新たに発生した脅威等に的確に対応しない場合には、情報セキュリティ水準を維持できなくなる。このため、情報システムの情報セキュリティ対策を定期的に見直し、さらに外部環境の急激な変化等が発生した場合は、適時見直しを行うことが必要となる。

遵守事項

##### (1) 情報システムについての対策の見直し

###### (a) 部局技術責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

### 5.3 情報システムの運用継続計画

#### 5.3.1 情報システムの運用継続計画の整備・整合的運用の確保

目的・趣旨

業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、非常時でも継続させる必要があり、本学においては業務継続計画を策定し運用している。

一方、非常時に情報システムの運用を継続させる場合には、非常時における情報セキュリティに係る対策事項を検討し、定めることが重要となる。

なお、業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。

遵守事項

##### (1) 情報システムの運用継続計画の整備・整合的運用の確保

###### (a) 全学実施責任者は、本学において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討すること。

###### (b) 全学実施責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認すること。

## 第6部　情報システムのセキュリティ要件

### 6.1 情報システムのセキュリティ機能

#### 6.1.1 主体認証機能

目的・趣旨

情報又は情報システムへのアクセス権のない者による情報の漏えいや滅失、情報システムの停止等の情報セキュリティインシデントを防止するために、主体認証機能の導入が求められる。

また、本学の情報システムの利用者は、例えば一般向けのサービスを提供する場合等、事務従事者に限られるものではない。識別コードと主体認証情報については、このような利用者の別にかかわらず保護すべきであり、利用者に対する注意喚起等の対策が求められる。

遵守事項

##### (1) 主体認証機能の導入

###### (a) 部局技術責任者は、情報システムや情報へのアクセスを管理するため、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、識別及び主体認証を行う機能を設けること。

###### (b) 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、主体認証は、以下を例とする主体認証方式を決定すること。   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等、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   (1)-2 部局技術責任者は、主体認証を行う情報システムにおいて、知識による主体認証方式を用いる場合には、以下の機能を設けること。   1. 利用者が自ら主体認証情報を設定する機能や、利用者以外の者が主体認証情報を設定する場合に、利用者へ**安全な方法で主体認証情報を割り当てる**機能 2. 利用者が主体認証情報としてパスワードを設定する際に、以下の要素を考慮して、セキュリティ上の強度が指定以上となるよう、情報システムに要求する機能    * パスワードに用いる文字の種類とその組み合わせ    * パスワードの桁数    * パスワードの有効期間    * 大規模な辞書を用いたパスワード解析への耐性   (1)-3 部局技術責任者は、主体認証を行う情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下の機能を設けること。   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   (1)-4 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下を例とする方法を用いて適切に管理すること。   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。 2. 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**よう注意を促す。 3. 主体認証情報に対するアクセス制限を設ける。   (1)-5 部局技術責任者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に利用され、又は利用されるおそれを認識した場合に当該主体認証情報を用いた不正アクセスが行われないよう、当該主体認証による情報システムの利用を停止する機能を設けること。 |

#### 6.1.2 アクセス制御機能

目的・趣旨

複数の主体が情報システムを利用する場合、特定の情報へのアクセスは、当該情報を業務上知る必要がある主体のみに限定される必要がある。したがって、情報システムにおいては、どの主体がどの情報にアクセスすることが可能なのかに関し、アクセス制御が適切に実施されるよう、留意する必要がある。

遵守事項

##### (1) アクセス制御機能の導入

###### (a) 部局技術責任者は、情報システムが取り扱う情報へのアクセスを、主体によって制御する必要がある場合、当該情報システムにアクセス制御を行う機能を設けること。

###### (b) 部局技術責任者は、アクセス制御機能の導入に当たり、情報セキュリティの強度や利便性を考慮の上、利用者及び所属するグループの属性に基づくアクセス制御だけでなく、利用時間帯や利用端末ごとの制御等、アクセス制御機能に求める情報セキュリティ上の要件を定めること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、以下を例とするアクセス制御機能の要件を定めること。   1. **情報システム利用者やそのグループ属性に基づくアクセス制御** 2. 利用時間や利用時間帯によるアクセス制御 3. 同時利用者数によるアクセス制御 4. 同一IDによる複数アクセスの禁止 5. IPアドレスによる端末の制限 |

##### (2) 適正なアクセス制御の実施

###### (a) 部局技術責任者は、事務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付及び取扱制限に従い、適正にアクセス制御を行うこと。

#### 6.1.3 権限管理機能

目的・趣旨

情報システムの管理機能として、一般的に管理者権限にはあらゆる操作が許可される特権が付与されている。当該特権が悪意ある第三者等に入手された場合、主体認証情報等の漏えい、改ざん又は情報システムに係る設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念される。

したがって、限られた主体のみに管理者権限が付与され、不正に利用されないよう、権限管理機能を導入することが必要となる。

遵守事項

##### (1) 権限管理機能の導入

###### (a) 部局技術責任者は、情報システムを利用する主体に対して、主体認証を行う必要がある場合、情報システムの管理を実現するための権限に係る管理の機能を設けること。

###### (b) 部局技術責任者は、情報システムに権限管理機能を導入するに当たり、管理者権限の特権を悪意ある第三者等によって、不正に窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、権限管理を行う情報システムにおいて、以下を含めた機能を導入すること。   1. **最小限の特権機能** 2. **内部からの不正操作や誤操作の防止機能** |

##### (2) 識別コード・主体認証情報の付与管理

###### (a) 部局技術責任者は、情報システムを利用する主体に対して、全ての識別コード及び主体認証情報を適切に付与し、適切に管理するための措置を講ずること。

|  |
| --- |
| (2)-1 部局技術責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）すること。  (2)-2 部局技術責任者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。  (2)-3 部局技術責任者は、識別コードは、情報システムを利用する主体ごとに個別に付与すること。ただし、部局技術責任者の判断の下、やむを得ず、複数の主体で共用する識別コード（以下「**共用識別コード**」という。）を付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。  (2)-4 部局技術責任者は、**管理者権限を持つ識別コード**を付与する場合は、以下の措置を講ずること。   1. 業務上必要な場合に限定する。 2. 初期設定の識別コードを変更できる場合には、識別コードを初期設定以外のものに変更する。 3. 初期設定の主体認証情報を変更できる場合には、主体認証情報を初期設定以外のものに変更する。 4. **ネットワーク経由のログインを制限する**。   (2)-5 部局技術責任者は、主体が情報システムを利用する必要がなくなった場合には、以下の措置を講ずること。   1. 当該主体の**識別コードを無効にする**。 2. 識別コードを追加又は削除する時に、不要な識別コードの有無を点検する。 3. 主体認証情報の不正な利用を防止するために、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。   (2)-6 部局技術責任者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス権を与えるようにアクセス制御を設定すること。また、人事異動等により、識別コードを追加又は削除する時に、不適切なアクセス制御設定の有無を点検すること。  (2)-7 部局技術責任者は、その他、識別コードの付与に当たっては、以下を例とする**措置**を講ずること。   1. 単一の情報システムにおいては、事務従事者１人に対する単一の識別コードのみの付与 2. 事務従事者への識別コードの付与に関する記録及び当該記録を消去する場合の部局総括責任者からの事前の許可 3. ある主体に付与した識別コードを別の主体に対して付与することの禁止 |

#### 6.1.4 ログの取得・管理

目的・趣旨

情報システムにおけるログとは、システムの動作履歴、利用者のアクセス履歴、その他必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の情報セキュリティインシデント（その予兆を含む。）を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

遵守事項

##### (1) ログの取得・管理

###### (a) 部局技術責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行う必要がある場合、ログを取得すること。

###### (b) 部局技術責任者は、情報システムにおいて、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。

###### (c) 部局技術責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の**時刻を同期**させ、ログに時刻情報も記録されるよう、設定すること。  (1)-2 部局技術責任者は、以下を例とする、ログとして取得する情報項目を定め、管理すること。   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. 利用者による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   (1)-3 部局技術責任者は、ログの**保存期間**を定めること。  (1)-4 部局技術責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。  (1)-5 部局技術責任者は、**ログが取得できなくなった場合の対処方法**を定めること。  (1)-6 部局技術責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入すること。   1. ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の**自動化** |

#### 6.1.5 暗号・電子署名

目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用するアルゴリズムが適切であること、運用時に当該アルゴリズムが危殆化した場合の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

遵守事項

##### (1) 暗号化機能・電子署名機能の導入

###### (a) 部局技術責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。

(ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

###### (b) 部局技術責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム及び運用方法について、以下の事項を含めて定めること。

(ア) 事務従事者が暗号化及び電子署名に対して使用するアルゴリズムについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」又は、本学における検証済み暗号リストがあればその中に記載されたアルゴリズムを採用すること。

(ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合を想定した緊急対応手順を定めること。

(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

###### (c) 部局技術責任者は、本学における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）又は○○が発行している場合は、それを使用するように定めること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。   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。 2. **複数のアルゴリズムを選択**することが可能な構成とする。 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た製品であって、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ひも付く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前提とするため、「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。 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。 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。 |

##### (2) 暗号化・電子署名に係る管理

###### (a) 部局技術責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。

(ア)電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。

(イ)暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化に関する情報を定期的に入手し、必要に応じて、事務従事者と共有を図ること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とすること。   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** |

### 6.2 情報セキュリティの脅威への対策

#### 6.2.1 ソフトウェアに関する脆弱性対策

目的・趣旨

本学の情報システムに対する脅威としては、第三者が情報システムに侵入し本学の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させるなどの攻撃を受けることが想定される。特に、一般向けに提供するサービスが第三者に侵入され、個人情報の漏えい等が発生した場合、本学に対する社会的な信用が失われる。

一般的に、このような攻撃では、情報システムを構成するサーバ装置、端末及び通信回線装置のソフトウェアの脆弱性を悪用されることが想定される。したがって、本学の情報システムにおいては、ソフトウェアに関する脆弱性について、迅速かつ適切に対処することが求められる。

なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2項「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。

遵守事項

##### (1) ソフトウェアに関する脆弱性対策の実施

###### (a) 部局技術責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。

###### (b) 部局技術責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。

###### (c) 部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。

###### (d) 部局技術責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む**情報を適宜入手**すること。   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   (1)-2 部局技術責任者は、利用するソフトウェアは**サポート期間を考慮**して選定し、サポート期間を過ぎたソフトウェアは原則として利用しないこと。  (1)-3 部局技術責任者は、構成要素ごとに**ソフトウェアのバージョン等を把握**し、**脆弱性対策の状況を確認**すること。  (1)-4 部局技術責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項について判断すること。   1. 対策の必要性 2. 対策方法 3. 対策方法が存在しない場合の**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 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   (1)-5 部局技術責任者は、脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。   1. 実施日 2. 実施内容 3. 実施者   (1)-6 部局技術責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「**対策用ファイル**」という。）は、信頼できる方法で入手すること。  (1)-7 部局技術責任者は、脆弱性対策の状況を確認する間隔は、可能な範囲で短くすること。 |

#### 6.2.2 不正プログラム対策

目的・趣旨

情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼすおそれがある。このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

遵守事項

##### (1) 不正プログラム対策の実施

###### (a) 部局技術責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

###### (b) 部局技術責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

###### (c) 部局技術責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるよう構成すること。  (1)-2 部局技術責任者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。  (1)-3 部局技術責任者は、不正プログラム対策ソフトウェア等は、定期的に全てのファイルを対象としたスキャンを実施するよう構成すること。  (1)-4 部局技術責任者は、想定される全ての**感染経路を特定**し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による**感染拡大の防止**等の必要な対策を行うこと。  (1)-5 部局技術責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。   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 |

#### 6.2.3 サービス不能攻撃対策

目的・趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、本学の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。

遵守事項

##### (1) サービス不能攻撃対策の実施

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

###### (b) 部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。

###### (c) 部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、サーバ装置、端末及び通信回線装置について、以下を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。   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   (1)-2 部局技術責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築すること。  (1)-3 部局技術責任者は、サーバ装置、端末及び通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、以下を例とする対策を検討すること。   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**   (1)-4 部局技術責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、**攻撃への対処を効率的に実施できる手段**の確保について検討すること。  (1)-5 部局技術責任者は、特定した監視対象について、**監視方法及び監視記録の保存期間**を定めること。  (1)-6 部局技術責任者は、監視対象の**監視記録を保存**すること。 |

#### 6.2.4 標的型攻撃対策

目的・趣旨

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。

したがって、標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

遵守事項

##### (1) 標的型攻撃対策の実施

###### (a) 部局技術責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。

###### (b) 部局技術責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下を例とする対策を行うこと。   1. 不要なサービスについて機能を削除又は停止する。 2. 不審なプログラムが実行されないよう設定する。 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。   (1)-2 部局技術責任者は、USBメモリ等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下を例とする対策を行うこと。   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。接続する外部電磁的記録媒体を事前に特定しておく。 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。 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。 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。 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。 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。   (1)-3 部局技術責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を例とする対策を行うこと。   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。また、インターネットに直接接続しない。 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。   (1)-4 部局技術責任者は、端末の管理者権限アカウントについて、以下を例とする対策を行うこと。   1. 不要な管理者権限アカウントを削除する。 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。   (1)-5 部局技術責任者は、重点的に守るべき業務・情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って、対策を講ずること。 |

### 6.3 アプリケーション・コンテンツの作成・提供

#### 6.3.1 アプリケーション・コンテンツの作成時の対策

目的・趣旨

本学では、情報の提供、行政手続、意見募集等の行政サービスのためにアプリケーション・コンテンツを用意し、広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に、利用者端末の情報セキュリティ水準の低下を招いてしまうことは避けなければならない。本学は、アプリケーション・コンテンツの提供に際しても、情報セキュリティ対策を講じておく必要がある。

また、アプリケーション・コンテンツの開発・提供を外部委託する場合については、4.1.1項「外部委託」についても併せて遵守する必要がある。

遵守事項

##### (1) アプリケーション・コンテンツの作成に係る規定の整備

###### (a) 全学実施責任者は、アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること。

##### (2) アプリケーション・コンテンツのセキュリティ要件の策定

###### (a) 部局技術責任者は、学外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含めること。

(ア) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

(イ) 提供するアプリケーションが脆弱性を含まないこと。

(ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

(エ) 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

(オ) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのOSやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

(カ) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

###### (b) 事務従事者は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前号に掲げる内容を調達仕様に含めること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を含む対策を行うこと。   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. 外部委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。   (2)-2 部局技術責任者は、提供するアプリケーション・コンテンツにおいて、学外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTMLソースを表示させるなどして確認すること。**必要があって当該機能を含める場合**は、当該高等教育機関外へのアクセスが情報セキュリティ上安全なものであることを確認すること。  (2)-3 部局技術責任者は、提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない**学外へのアクセスを自動的に発生させる機能**を含めないこと。  (2)-4 部局技術責任者は、文書ファイル等のコンテンツの提供において、当該コンテンツが改ざん等なく真正なものであることを確認できる手段がない場合は、**「https://」で始まるURLのウェブページから当該コンテンツをダウンロードできるように提供**すること。  (2)-5 部局技術責任者は、改ざん等がなく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。 |

#### 6.3.2 アプリケーション・コンテンツ提供時の対策

目的・趣旨

本学では、情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサイト等を用意し、一般利用者等の利用に供している。これらのサービスは通常インターネットを介して利用するものであるため、一般利用者等にとっては、そのサービスが実際の本学のものであると確認できることが重要である。また、本学になりすましたウェブサイトを放置しておくと、本学の信用を損なうだけでなく、利用者等が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講ずる必要がある。

遵守事項

##### (1) A大学ドメイン名の使用

###### (a) 部局技術責任者は、学外向けに提供するウェブサイト等が実際の本学提供のものであることを利用者が確認できるように、.example.ac.jpで終わるドメイン名（以下「A大学ドメイン名」という。）を情報システムにおいて使用するよう仕様に含めること。ただし、4.1.3項に掲げる場合を除く。

###### (b) 事務従事者は、学外向けに提供するウェブサイト等の作成を外部委託する場合においては、前号と同様、A大学ドメイン名を使用するよう調達仕様に含めること。

##### (2) 不正なウェブサイトへの誘導防止

###### (a) 部局技術責任者は、利用者が検索サイト等を経由して本学のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、学外向けに提供するウェブサイトに対して、以下を例とする**検索エンジン最適化措置（SEO対策）**を講ずること。   1. **クローラからのアクセスを排除しない**。 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**。 3. **適切なタイトルを設定する**。 4. **不適切な誘導を行わない**。   (2)-2 部局技術責任者は、学外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、**不審なサイトへのアクセスを防止するための対策**を講ずること。 |

##### (3) 学外のアプリケーション・コンテンツの告知

###### (a) 事務従事者は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、以下の対策を講ずること。

(ア) 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。

(イ) 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。

(ウ) 電子メールの送信により告知する場合には、告知内容についての問合わせ先としてA大学ドメイン名による電子メールアドレスを明記するか又は告知する電子メールにA大学ドメイン名による電子署名を付与する。

## 第7部　情報システムの構成要素

### 7.1 端末・サーバ装置等

#### 7.1.1 端末

目的・趣旨

端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等のおそれがある。また、事務従事者の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。モバイル端末の利用に当たっては、盗難・紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1項「ソフトウェアに関する脆弱性対策」、6.2.2項「不正プログラム対策」、7.3.2項「IPv6通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

遵守事項

##### (1) 端末の導入時の対策

###### (a) 部局技術責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

###### (b) 部局技術責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。

###### (c) 部局技術責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、モバイル端末を除く端末について、**原則としてクラス２以上の要管理対策区域に設置する**こと。  (1)-2 部局技術責任者は、端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。   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。 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。   (1)-3 部局技術責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。   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。 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。   (1)-4 部局技術責任者は、第三者により情報窃取されることを防止するために、以下を例とする、端末に保存される情報を**暗号化**するための機能又は利用者が端末に情報を保存できないようにするための機能を設けること。   1. 端末に、ハードディスク等の電磁的記録媒体全体を暗号化する機能を設ける。 2. 端末に、ファイルを暗号化する機能を設ける。 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**を活用したリモートアクセス環境を構築する。 4. **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。 5. **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。 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消去する機能（**遠隔データ消去機能**）を設ける。   (1)-5 部局技術責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。   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 |

##### (2) 端末の運用時の対策

###### (a) 部局技術責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

###### (b) 部局技術責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

##### (3) 端末の運用終了時の対策

###### (a) 部局技術責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

#### 7.1.2 サーバ装置

目的・趣旨

電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に本学が有するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、学外からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1項「ソフトウェアに関する脆弱性対策」、6.2.2項「不正プログラム対策」、6.2.3項「サービス不能攻撃対策」、7.3.2項「IPv6通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。また、特に電子メールサーバ、ウェブサーバ、DNSサーバについては、本項での共通的な対策に加え、それぞれ7.2節「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。

遵守事項

##### (1) サーバ装置の導入時の対策

###### (a) 部局技術責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

###### (b) 部局技術責任者は、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、将来の見通しも考慮し、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。

###### (c) 部局技術責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

###### (d) 部局技術責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、要保護情報を取り扱うサーバ装置については、**クラス２以上の要管理対策区域に設置する**こと。  (1)-2 部局技術責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。   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。   (1)-3 部局技術責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。   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。   (1)-4 部局技術責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため要安定情報を取り扱う情報システムについては、将来の見通しも考慮し、以下を例とする対策を講ずること。   1. 複数のサーバ装置の設置による負荷分散 2. 負荷分散装置の設置による負荷分散 3. DNSラウンドロビン方式を利用した負荷分散 4. 同一システムを２系統で構成することによる**冗長化**   (1)-5 部局技術責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。   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 |

##### (2) サーバ装置の運用時の対策

###### (a) 部局技術責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

###### (b) 部局技術責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図ること。

###### (c) 部局技術責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を監視する措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

###### (d) 部局技術責任者は、要安定情報を取り扱うサーバ装置について、情報のバックアップを取得するなど、サーバ装置を正常な運用状態に復元することが可能になるよう、必要な措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。  (2)-2 部局技術責任者は、サーバ装置上での不正な行為及び無許可のアクセス等の意図しない事象の発生を監視するために、以下を例とする対策を講ずること。   1. **アクセスログ等を定期的に確認する**。 2. IDS/IPSを設置する。 3. 不正プログラム対策ソフトウェアを利用する。 4. ファイル完全性チェックツールを利用する。 5. CPU、メモリ、ディスクI/O等のシステム状態を確認する。   (2)-3 部局技術責任者は、要安定情報を取り扱うサーバ装置については、運用状態を復元するために以下を例とする対策を講ずること。   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。 2. 定期的な**バックアップ**を実施する。 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。 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。 |

##### (3) サーバ装置の運用終了時の対策

###### (a) 部局技術責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。

#### 7.1.3 複合機・特定用途機器

目的・趣旨

本学においては、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器（以下「複合機」という。）が利用されている。複合機は、学内通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、本学においては、テレビ会議システム、IP電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。

したがって、複合機や特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずることが重要である。

遵守事項

##### (1) 複合機

###### (a) 部局技術責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。

###### (b) 部局技術責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。

###### (c) 部局技術責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、**「IT製品の調達におけるセキュリティ要件リスト」を参照**するなどし、複合機が備える機能、設置環境及び取り扱う情報の格付及び取扱制限に応じ、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記すること。  (1)-2 部局技術責任者は、以下を例とする運用中の複合機に対する、情報セキュリティインシデントへの対策を講ずること。   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。 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。 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。 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。 5. 複合機をインターネットに直接接続しない。 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。 7. **利用者ごとに許可される操作**を適切に設定する。   (1)-3 部局技術責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消すること。当該機能を備えていない複合機については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの**別の手段で対策を講ずる**こと。 |

##### (2) 特定用途機器

###### (a) 部局技術責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、特定用途機器の特性に応じて、以下を例とする対策を講ずること。   1. 特定用途機器について、利用環境に応じた適切なセキュリティ設定を実施する。 2. 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。 3. 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。 4. インターネットに接続されている特定用途機器についてソフトウェアに関する脆弱性が存在しないか確認し、脆弱性が存在する場合、**バージョンアップやセキュリティパッチの適用**、アクセス制御等の対策を講ずる。 5. 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。 |

### 7.2 電子メール・ウェブ等

#### 7.2.1 電子メール

目的・趣旨

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する事務従事者が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本項の遵守事項のほか、7.1.2項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

##### (1) 電子メールの導入時の対策

###### (a) 部局技術責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

###### (b) 部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

###### (c) 部局技術責任者は、電子メールのなりすましの防止策を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする事務従事者の主体認証を行う機能を備えること。   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。   (1)-2 部局技術責任者は、以下を例とする電子メールのなりすましの防止策を講ずること。   1. SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）等の**送信ドメイン認証技術**による**送信側の対策**を行う。 2. SPF、DKIM等の送信ドメイン認証技術による**受信側の対策**を行う。 3. S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用する。 |

#### 7.2.2 ウェブ

目的・趣旨

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ（ウェブページとして公開している情報）が改ざんされたり、ウェブサーバが利用不能にされたり、又はウェブサーバが侵入されるなどの被害が想定されるため、適切な対策を組み合わせて実施することが求められる。

なお、本項の遵守事項のほか、7.1.2項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

##### (1) ウェブサーバの導入・運用時の対策

###### (a) 部局技術責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずること。

(ア) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

(イ) ウェブコンテンツの編集作業を担当する主体を限定すること。

(ウ) 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。

(エ) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。

(オ) サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。

###### (b) 部局技術責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、不要な機能の停止又は制限として、以下を例とするウェブサーバの管理や設定を行うこと。   1. **CGI機能**を用いるスクリプト等は必要最低限のものに限定し、CGI機能を必要としない場合は設定でCGI機能を使用不可とする。 2. **ディレクトリインデックスの表示を禁止する**。 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**。 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。   (1)-2 部局技術責任者は、ウェブコンテンツの編集作業を担当する主体の限定として、以下を例とするウェブサーバの管理や設定を行うこと。   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。 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。   (1)-3 部局技術責任者は、公開してはならない又は無意味なウェブコンテンツが公開されないよう管理することとして、以下を例とするウェブサーバの管理や設定を行うこと。   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。 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。   (1)-4 部局技術責任者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行うこと。   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。 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。 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。   (1)-5 部局技術責任者は、通信時の盗聴による第三者への情報の漏えいの防止及び正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を例とするウェブサーバの実装を行うこと。   1. **SSL（TLS）機能を適切に用いる**。 2. SSL（TLS）機能のために必要となるサーバ証明書には、**利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局**（証明書発行機関）により発行された電子証明書を用いる。 |

##### (2) ウェブアプリケーションの開発時・運用時の対策

###### (a) 部局技術責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、以下を含むウェブアプリケーションの脆弱性を排除すること。   1. **SQLインジェクション脆弱性** 2. **OSコマンドイ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** |

#### 7.2.3 ドメインネームシステム（DNS）

目的・趣旨

ドメインネームシステム（DNS：Domain Name System）は、端末等のクライアント（DNSクライアント）からの問合わせを受けて、ドメイン名やホスト名とIPアドレスとの対応関係等について回答を行うネットワークの基盤をなすものである。DNSの可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また、DNSが提供する情報の完全性が損なわれ、誤った情報を提供した場合は、端末等のDNSクライアントが悪意あるサーバに接続させられるなどの被害に遭う可能性がある。さらに、DNSが管理するドメインをアドレスとして利用する電子メールのなりすまし対策の一部はDNSで行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNSサーバの適切な管理が必要である。

なお、本項の遵守事項のほか、7.1.2項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

##### (1) DNSの導入時の対策

###### (a) 部局技術責任者は、要安定情報を取り扱う情報システムの名前解決を提供するDNSのコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。

###### (b) 部局技術責任者は、DNSのキャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。

###### (c) 部局技術責任者は、DNSのコンテンツサーバにおいて、本学のみで使用する名前の解決を提供する場合、当該情報が外部に漏えいしないための措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、要安定情報を取り扱う情報システムの名前解決を提供するDNSのコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講ずること。   1. DNSのコンテンツサーバを**冗長化**する。 2. 通信回線装置等で、DNSのコンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。   (1)-2 部局技術責任者は、DNSのキャッシュサーバにおいて、以下を例とする**名前解決の要求への適切な応答をするための措置**を講ずること。   1. 学外からの名前解決の要求には応じず、学内からの名前解決の要求のみに回答を行うように措置を講ずる。 2. キャッシュサーバの設定、ファイアウォール等でアクセス制御を行う。 3. 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。   (1)-3 部局技術責任者は、学内のみで使用する名前の解決を提供するDNSのコンテンツサーバにおいて、以下を例とする**当該情報が外部に漏えいしないための措置**を講ずること。   1. 内部向けの名前解決を提供するコンテンツサーバを外部向けのコンテンツサーバとは別々に設置し、コンテンツサーバの設定、ファイアウォール等でアクセス制御を行う。 |

##### (2) DNSの運用時の対策

###### (a) 部局技術責任者は、DNSのコンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。

###### (b) 部局技術責任者は、DNSのコンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。

### 7.3 通信回線

#### 7.3.1 通信回線

目的・趣旨

サーバ装置やクライアント端末への不正アクセスやサービス不能攻撃等は、当該サーバ装置や端末に接続された通信回線及び通信回線装置を介して行われる場合がほとんどであることから、通信回線及び通信回線装置に対する情報セキュリティ対策については、情報システムの構築時からリスクを十分検討し、必要な対策を実施しておく必要がある。通信事業者の公衆回線や本学専用の通信回線の運用主体又は有線回線や無線LAN回線等の物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。

また、情報システムの運用開始時と一定期間運用された後とでは、通信回線の構成や接続される情報システムの条件等が異なる場合があり、攻撃手法の変化も想定されることから、情報システムの構築時に想定した対策では十分でなくなる可能性がある。そのため、通信回線の運用時においても、継続的な対策を実施することが重要である。

遵守事項

##### (1) 通信回線の導入時の対策

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

###### (b) 部局技術責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。

###### (c) 部局技術責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。

###### (d) 部局技術責任者は、事務従事者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。

###### (e) 部局技術責任者は、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。

###### (f) 部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。

###### (g) 部局技術責任者は、学内通信回線にインターネット回線、公衆通信回線等の学外通信回線を接続する場合には、学内通信回線及び当該高等教育機関内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。

###### (h) 部局技術責任者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視するための措置を講ずること。

###### (i) 部局技術責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

###### (j) 部局技術責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。

###### (k) 部局技術責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくこと。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 部局技術責任者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じて、以下を例とする通信経路の分離を行うこと。   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。 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。 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。   (1)-2 部局技術責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、SSL（TLS）、IPsec等による暗号化を行うこと。また、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。  (1)-3 部局技術責任者は、学内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずること。   1. 情報システムの機器番号等により接続機器を識別する。 2. クライアント証明書により接続機器の認証を行う。   (1)-4 部局技術責任者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講ずること。   1. 通信回線装置を施錠可能なラック等に設置する。 2. 施設内に敷設した通信ケーブルを物理的に保護する。 3. 通信回線装置の操作ログを取得する。   (1)-5 部局技術責任者は、要安定情報を取り扱う情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずること。   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。 2. **通信回線及び通信回線装置を冗長構成にする**。   (1)-6 部局技術責任者は、学内通信回線に、インターネット回線や公衆通信回線等の学外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講ずること。   1. ファイアウォール、WAF（Web Application Firewall）、リバースプロキシ等により通信制御を行う。 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。 3. IDS/IPSにより不正アクセスを検知及び遮断する。   (1)-7 部局技術責任者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、以下を例とする対策を講ずること。   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。 2. 主体認証によりアクセス制御する。 3. 通信内容の暗号化により秘匿性を確保する。 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。 |

##### (2) 通信回線の運用時の対策

###### (a) 部局技術責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずること。

###### (b) 部局技術責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。

###### (c) 部局技術責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。

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

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管すること。  (2)-2 部局技術責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。 |

##### (3) 通信回線の運用終了時の対策

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

##### (4) リモートアクセス環境導入時の対策

###### (a) 部局技術責任者は、VPN回線を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。

###### (b) 部局技術責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (4)-1 部局技術責任者は、VPN回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。   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   (4)-2 部局技術責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。   1. 利用開始及び利用停止時の申請手続の整備 2. 利用者の認証又は発信者番号による識別及び認証 3. 主体認証ログの取得及び管理 4. アクセス可能な情報システムの制限 5. リモートアクセス中の他の通信回線との接続禁止 |

##### (5) 無線LAN環境導入時の対策

###### (a) 部局技術責任者は、無線LAN技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (5)-1 部局技術責任者は、無線LAN技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、**以下を含む措置**を講ずること。   1. 無線LAN回線利用申請手続の整備 2. **無線LAN通信の暗号化** 3. 通信を行う端末の識別又は認証 4. 利用者の認証 5. **主体認証ログ**の取得及び管理 6. 無線LAN経由でアクセス可能な情報システムの明確化 7. 無線LANに接続する端末及び**通信回線装置の管理** 8. **不正プログラム感染を認知した場合の対処手順** |

#### 7.3.2 IPv6通信回線

目的・趣旨

本学において、インターネットの規格であるIPv6通信プロトコルに対応するための取組が進められているが、IPv6通信プロトコルを採用するに当たっては、グローバルIPアドレスによるパケットの直接到達性やIPv4通信プロトコルからIPv6通信プロトコルへの移行過程における共存状態等、考慮すべき事項が多数ある。

近年では、サーバ装置、端末及び通信回線装置等にIPv6技術を利用する通信（以下「IPv6通信」という。）を行う機能が標準で備わっているものが多く出荷され、運用者が意図しないIPv6通信が通信ネットワーク上で動作している可能性があり、結果として、不正アクセスの手口として悪用されるおそれもあることから、必要な対策を講じていく必要がある。

なお、IPv6技術は今後も技術動向の変化が予想されるが、一方で、IPv6技術の普及に伴い情報セキュリティ対策技術の進展も期待されることから、本学においても、IPv6の情報セキュリティ対策に関する技術動向を十分に注視し、適切に対応していくことが重要である。

遵守事項

##### (1) IPv6通信を行う情報システムに係る対策

###### (a) 部局技術責任者は、IPv6技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Programに基づくPhase-2準拠製品を、可能な場合には選択すること。

###### (b) 部局技術責任者は、IPv6通信の特性等を踏まえ、IPv6通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

(ア) グローバルIPアドレスによる直接の到達性における脅威

(イ) IPv6通信環境の設定不備等に起因する不正アクセスの脅威

(ウ) IPv4通信とIPv6通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

(エ) アプリケーションにおけるIPv6アドレスの取扱い考慮漏れに起因する脆弱性の発生

##### (2) 意図しないIPv6通信の抑止・監視

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

## 第8部　情報システムの利用

### 8.1 情報システムの利用

#### 8.1.1 情報システムの利用

目的・趣旨

事務従事者は、業務の遂行のため、端末での事務処理のほか電子メール、ウェブ等様々な情報システムを利用している。これらを適切に利用しない場合、情報セキュリティインシデントを引き起こすおそれがある。

このため、情報システムの利用に関する規定を整備し、事務従事者は規定に従って利用することが求められる。

遵守事項

##### (1) 情報システムの利用に係る規定の整備

###### (a) 全学実施責任者は、本学の情報システムの利用のうち、情報セキュリティに関する規定を整備すること。

###### (b) 全学実施責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。

###### (c) 全学実施責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、本学の情報システムの利用のうち、情報セキュリティに関する規定として、**以下を例とする実施手順を定める**こと。   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   (1)-2 全学実施責任者は、要管理対策区域外にて情報処理を行う際の安全管理措置として、以下を例とする措置を規定し、事務従事者に遵守させること。   1. モバイル端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化 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**（不要な情報をモバイル端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど） 4. 利用する場所や時間の限定 5. 端末及び外部電磁的記録媒体等についての盗難・紛失が発生した際の緊急対応手順   (1)-3 全学実施責任者は、要管理対策区域外にて事務従事者が情報処理を行う際の許可等の手続として、以下を例とする手続を規定し、事務従事者に遵守させること。   1. 許可権限者の決定（部局技術責任者又は職場情報セキュリティ責任者が想定される。） 2. 利用時の許可申請手続 3. 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線の接続形態等） 4. **利用期間満了時の手続** 5. 許可権限者による手続内容の記録   (1)-4 全学実施責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順として以下の事項を含めて定めること。   1. 本学支給の外部電磁的記録媒体を使用する（私物や出所不明の媒体を使用しない）。 2. 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。 3. 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。 4. 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行う。 |

##### (2) 情報システム利用者の規定の遵守を支援するための対策

###### (a) 部局技術責任者は、事務従事者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。

|  |
| --- |
| 【 基本対策事項 】  (2)-1 部局技術責任者は、学外のウェブサイトについて、事務従事者が閲覧できる範囲を制限する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。   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)-2 部局技術責任者は、事務従事者が不審なメールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。   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メールクライアントの導入 |

##### (3) 情報システムの利用時の基本的対策

###### (a) 事務従事者は、高等教育機関の事務の遂行以外の目的で情報システムを利用しないこと。

###### (b) 事務従事者は、部局技術責任者が接続許可を与えた通信回線以外に本学の情報システムを接続しないこと。

###### (c) 事務従事者は、学内通信回線に、部局技術責任者の接続許可を受けていない情報システムを接続しないこと。

###### (d) 事務従事者は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、部局技術責任者の承認を得ること。

###### (e) 事務従事者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。

###### (f) 事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。

###### (g) 事務従事者は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、部局技術責任者又は職場情報セキュリティ責任者の許可を得ること。

|  |
| --- |
| 【 基本対策事項 】  (3)-1 事務従事者は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下を例とする措置を講ずること。   1. スクリーンロックの設定 2. 利用後のログアウト徹底 3. 利用後に情報システムを鍵付き保管庫等に格納し施錠 |

##### (4) 電子メール・ウェブの利用時の対策

###### (a) 事務従事者は、要機密情報を含む電子メールを送受信する場合には、それぞれの高等教育機関が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。

###### (b) 事務従事者は、学外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名にA大学ドメイン名を使用すること。ただし、当該高等教育機関外の者にとって、当該事務従事者が既知の者である場合は除く。

###### (c) 事務従事者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。

###### (d) 事務従事者は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。

###### (e) 事務従事者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

###### (f) 事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。

(ア) 送信内容が暗号化されること

(イ)当該ウェブサイトが送信先として想定している組織のものであること

##### (5) 識別コード・主体認証情報の取扱い

###### (a) 事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。

###### (b) 事務従事者は、自己に付与された識別コードを適切に管理すること。

###### (c) 事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。

###### (d) 事務従事者は、自己の主体認証情報の管理を徹底すること。

|  |
| --- |
| 【 基本対策事項 】  (5)-1 事務従事者は、自己に付与された識別コードを適切に管理するため、以下を含む措置を講ずること。   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**。 2. **他者が主体認証に用いるために付与及び貸与しない**。 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**。   (5)-2 事務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。   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。 2. **自己の主体認証情報を他者に教えない**。 3. **主体認証情報を忘却しないように努める**。 4. 主体認証情報を設定するに際しては、**容易に推測されないもの**にする。 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**。 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。（シングルサインオンの場合を除く。） 7. 部局技術責任者から**主体認証情報を定期的に変更する**ように指示されている場合は、その指示に従って定期的に変更する。   (5)-3 事務従事者は、所有による主体認証情報を用いる場合には、以下の管理を徹底すること。   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。 2. 主体認証情報格納装置を他者に付与及び貸与しない。 3. 主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する。 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、これを部局技術責任者に返還する。 |

##### (6) 暗号・電子署名の利用時の対策

###### (a) 事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。

###### (b) 事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。

###### (c) 事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

##### (7) 不正プログラム感染防止

###### (a) 事務従事者は、不正プログラム感染防止に関する措置に努めること。

###### (b) 事務従事者は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずること。

|  |
| --- |
| 【 基本対策事項 】  (7)-1 事務従事者は、不正プログラム対策ソフトウェアを活用し、不正プログラム感染を回避するための以下措置に努めること。   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**実行ファイルを実行しない**。また、データファイルをアプリケーション等で読み込まない。 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**。 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**。 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**。   (7)-2 事務従事者は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。  (7)-3 事務従事者は、不正プログラムに感染するリスクを低減する情報システムの利用方法として、以下のうち実施可能な措置を講ずること。   1. 不審なウェブサイトを閲覧しない。 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。 3. プログラム及びスクリプトの実行機能を無効にする。 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。 |

### 8.2 本学支給以外の端末の利用

#### 8.2.1 本学支給以外の端末の利用

目的・趣旨

高等教育機関の事務の遂行においては、本学から支給された端末を用いて高等教育機関の事務を遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず本学支給以外の端末を利用して情報処理を行う必要が生じる場合がある。この際、当該端末は本学が支給したものではないという理由で、事務従事者へ情報セキュリティ対策の実施を求めなかった場合、当該端末で取り扱われる情報セキュリティ水準が、事務情報セキュリティ対策基準を満たさないおそれがある。

したがって、そのような可能性がある場合は、本学支給以外の端末を事務従事者が安全に利用するための手続や安全管理措置の規定をあらかじめ整備し、本学における厳格な管理の下で利用させることが必要である。

また、本学支給以外の端末であっても、本学から支給されるモバイル端末と同等の情報セキュリティ水準の確保が求められることから、7.1.1項「端末」も参照し、同等の安全管理が実施されるよう、規定を整備し、事務従事者に安全管理措置を講じさせる必要がある。

遵守事項

##### (1) 本学支給以外の端末の利用規定の整備・管理

###### (a) 全学実施責任者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。

###### (b) 全学実施責任者は、要機密情報について本学支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。

###### (c) 部局総括責任者は、本学支給以外の端末による高等教育機関の事務に係る情報処理に関する安全管理措置の実施状況を管理する責任者を定めること。

###### (d) 前号で定める責任者は、要機密情報を取り扱う本学支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、事務従事者に適切に安全管理措置を講じさせること。

|  |
| --- |
| 【 基本対策事項 】  (1)-1 全学実施責任者は、以下を例に本学支給以外の端末を利用する際の許可等の手続に関する手順を整備し、事務従事者に周知すること。   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）    * 利用する端末の機種名    * 利用目的、取り扱う情報の概要、機密性３情報の利用の有無等    * 主要な利用場所    * 利用する主要な通信回線サービス    * **利用する期間** 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. **許可権限者**（遵守事項8.2.1(1)(c)において定める、本学支給以外の端末の安全管理措置の実施状況を管理する責任者（以下、この項において「端末管理責任者」という。））   (1)-2 全学実施責任者は、本学支給以外の端末により要機密情報を取り扱う場合は、事務従事者が講ずるべき**安全管理措置**の実施手順について、以下を例に整備すること。   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. 遠隔データ消去機能の設定 5. **要機密情報の暗号化等による秘匿性の確保** 6. 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） 7. 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） 8. 以下を例とする禁止事項の遵守    * **端末、OS、アプリケーション等の改造行為**    * **安全性が確認できないアプリケーション**のインストール及び利用    * **利用が禁止されているソフトウェア**のインストール及び利用    * **許可されない通信回線サービスの利用**（利用する回線を限定する場合）    * **第三者への端末の貸与**   (1)-3 部局技術責任者は、本学支給以外の端末により要機密情報を取り扱う本学の情報システムにリモートアクセスする環境を構築する場合、基盤となる情報システムにより各高等教育機関に提供されるリモートアクセス環境が利用可能であれば活用し、端末の盗難・紛失や不正プログラム感染等により情報窃取されることを防止するために、以下を例とする対策を講ずること。   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。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。 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。 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**を活用したリモートアクセス環境を構築する。利用者は専用のアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。 |

##### (2) 本学支給以外の端末の利用時の対策

###### (a) 事務従事者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合には、遵守事項8.2.1(1)(c)で定める責任者の許可を得ること。

###### (b) 事務従事者は、要機密情報を本学支給以外の端末で取り扱う場合は、職場情報セキュリティ責任者の許可を得ること。

###### (c) 事務従事者は、本学支給以外の端末により高等教育機関の事務に係る情報処理を行う場合には、本学にて定められた手続及び安全管理措置に関する規定に従うこと。

###### (d) 事務従事者は、情報処理の目的を完了した場合は、要機密情報を本学支給以外の端末から消去すること。