高等教育機関の情報セキュリティ対策のためのサンプル規程集

（2010 年版）

第Ⅱ分冊（手順・ガイドライン類）

2011 年 3 月 31 日

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

第 II 分冊　目次

（参考）第Ⅰ分冊　目次

A3100 情報システム運用・管理手順の策定に関する解説書

本書は、「A2101 情報システム運用・管理規程」を実際に適用する際に用いられる、情報セキュリティ対策を円滑に実施するための文書（手順、ガイドライン及びマニュアル等）の策定に関して、概要を解説するものである。

１．文書構成

情報システムの運用・管理に係る手順等（A3101～A3115）として、次に掲げる 15 の文書を用意した。

A3101 情報システムにおける情報セキュリティ対策実施手順（策定手引書）
A3102 例外措置手順書
A3103 インシデント対応手順
A3104 情報格付け取扱手順
A3105 情報システムリスク評価手順
A3106 セキュリティホール対策計画に関する様式（策定手引書）
A3107 ウェブサーバ設定確認実施手順（策定手引書）
A3108 電子メールサーバのセキュリティ維持手順（策定手引書）
A3109 人事異動の際に行うべき情報セキュリティ対策実施手順
A3110 機器等の購入における情報セキュリティ対策実施手順（策定手引書）
A3111 外部委託における情報セキュリティ対策実施手順
A3112 ソフトウェア開発における情報セキュリティ対策実施手順（策定手引書）
A3113 外部委託における情報セキュリティ対策に関する評価手順
A3114 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書
A3115 情報システムの構築等における ST 評価・ST 確認の実施に関する解説書

ポリシー及び関連する実施規程に従い、実際に情報システムを運用・管理する場合、情報セキュリティ維持のためにとるべき対策は多岐にわたる。そのためサンプル規程集では、個々の場面場面に応じて、そこで遵守すべき事項を複数の文書に定めることとした。これらの文書の他、さらに具体的な操作マニュアルとして、例えば次のような文書を整備することも考えられる。

・オペレーティング・システム設定手順（Windows®、Linux®、FreeBSD®等）
・ソフトウェア設定手順（DNS、SMTP、POP/IMAP、FTP、HTTP、SSL、SSH、VPN、IPFW 等）
・通信機器設定手順（ファイアウォール、ルータ、ハブ等）

あらかじめ詳細な手順を定めておくことで、情報システムを運用・管理する者が実施すべき事項が明確となり、情報セキュリティの向上につながる。ただし、実施規程や手順として定めた場

合、そこには当然強制力が働くため、実施規程・手順のレベルで定めるか、ガイドライン・マニュアルのレベルで定めるかについては、慎重に検討する必要がある。

２．情報システムの運用・管理に係る手順等（A3101～A3115）の概要

(1) A3101 情報システムにおける情報セキュリティ対策実施手順（策定手引書）

情報システムは、目的とする業務を円滑に遂行するため、情報システムのライフサイクルを通じて様々な要件を満たすことが必要となる。その要件の中には、情報システムのライフサイクルで発生する様々な脅威に対応するためのセキュリティの観点からの要件も含まれる。そして、セキュリティの要件を満足するためには、情報システムのライフサイクルを通じて適切な情報セキュリティ対策を実施し、実施した情報セキュリティ対策を PDCA サイクルによって、見直ししていかなければならない。ここでは、情報システムのライフサイクルの視点に立ち、情報システムのセキュリティ要件に基づいて、各段階において考慮すべき情報セキュリティ対策について定める。

(2) A3102 例外措置手順書

大学の業務を遂行するに当たって、ポリシー及び関連する実施規程・手順が業務の適正な遂行を著しく妨げる等の理由により、そこに規定された方法とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合がある。こうした場合において、情報セキュリティを維持しつつ柔軟に対応できるようにするための例外措置を定める。

(3) A3103 インシデント対応手順

災害等によるネットワーク設備の損壊、利用者等による規定違反や学外から学内への攻撃行為等により発生したインシデントへの対応について、具体的な対応手順を定める。インシデントが発生した場合、適切な対応によりインシデントの影響が拡大することを防ぐと共に復旧を図ることが必要である。対応を誤ると無用な被害の拡大を招くことが懸念されるため、インシデントの発見から対処にいたる手続きを定め、適切な対処を実施することが必要である。

(4) A3104 情報格付け取扱手順

情報システムで取り扱う情報は格付けされ、格付けに応じて適切に取り扱う必要がある。取扱いが不適切なため、機密性が求められる情報の漏えい、完全性が求められる情報の改ざん等が生じた場合には、大学活動の停止や社会的信用の失墜の要因となる可能性もある。このようなリスクを軽減するため、教職員等が情報を適切に取り扱うために必要な事項を定める。

(5) A3105 情報システムリスク評価手順

情報システムを適切に運用し管理するためには、情報システムに対するさまざまなリスクに応じて、適切かつ効率的、あるいは実現可能なセキュリティ対策を実施する必要がある。そうしたリスクを検討するための手順として、情報資産の洗い出し、脆弱性分析、資産価値判断、脅威の判断、リスク値の算出、対策の必要性判断について定める。

(6) A3106 セキュリティホール対策計画に関する様式（策定手引書）

セキュリティホール対策計画に関する様式を定める。セキュリティホール対策を行う者がこれを用いることにより、ポリシー及び実施規程の関係する規定を遵守し、セキュリティホールに対して効率よく対処できるようになるものである。

(7) A3107 ウェブサーバ設定確認実施手順（策定手引書）

ウェブサーバの設定確認を行う場合の手順書を策定するための手引書である。本書に基づいて策定される「ウェブサーバ設定確認実施手順」は、ウェブサーバの検収時における設定確認だけでなく、定期的なウェブサーバの設定確認にも用いられる。

(8) A3108 電子メールサーバのセキュリティ維持手順（策定手引書）

電子メールサーバのセキュリティ維持についての手順書を策定するための手引書である。電子メールは通信回線を介して提供されるサービスの中で最も普及しているサービスの一つであり、大学の業務を円滑に遂行するために不可欠なものになっている。その一方で、電子メールの送受信は情報のやりとりにほかならず、そのやりとりは様々な中継地点を経由して行われるため、その過程における情報の漏えい、改ざんのリスクがある。また、セキュリティホール対策や不正プログラム対策をおこたると、不正中継、ウイルス感染等、学内だけでなく学外にも迷惑をかけるおそれがある。このようなリスクを軽減するため、サーバ装置上で動作し、電子メールサービスにおいて利用されるアプリケーションソフトウェアのセキュリティを維持することが求められる。

(9) A3109 人事異動の際に行うべき情報セキュリティ対策実施手順

大学における情報セキュリティ対策は、それに係るすべての教職員・学生等が、その職制、職務及び立場に応じて与えられている権限と責務を理解した上で、ポリシー及び関連する実施規程・手順に基づき、負うべき責務を全うすることで適切に実施される。このため、それを実施するための基礎となる組織・体制については、教職員・学生等の採用・入学、退職・卒業、配置換え等が行われた際においても、適切に整備されている必要がある。さらに、適切に整備された組織・体制の下で、教職員・学生等に対する情報セキュリティに係る教育、権限の付与及び失効等を適時に行うことが情報セキュリティを確保する上で不可欠である。ここでは、人事異動等に伴い情報セキュリティの観点から行う手続について定める。

(10) A3110 機器等の購入における情報セキュリティ対策実施手順（策定手引書）

大学においてサーバ装置、端末、通信回線装置、ソフトウェアその他の機器等を購入して業務に使用する場合には、これらの機器等に情報を保有し、また機器等を介して利用者が大学の情報へアクセスすることとなるため、必要なセキュリティ機能が装備されていない場合や購入後に情報セキュリティ対策が継続的に行えない場合は、情報セキュリティが維持できなくなるおそれがある。このため、機器等の購入に当たっては、情報セキュリティ維持の観点から適切な機器等を選定することが求められる。ここでは、機器等の購入において情報セキュリティの観点から行うべき手続を定める。

(11) A3111 外部委託における情報セキュリティ対策実施手順

大学の情報処理業務の形態には、情報システムの構築、ソフトウェアの開発、情報システムの運用・保守・点検、情報の加工・処理及び情報の保存・運搬等がある。これらの情報処理業務を外部委託により行う場合には、当該業務の形態において、大学と委託先の業務分担、委託先に取り扱わせる情報、機器の設置場所（大学の施設内又は委託先の施設内）、委託先による業務の実施場所（大学の施設内又は委託先の施設内）等に関して様々な場合があり、それぞれの場合に応じて適切な情報セキュリティ対策を委託先に実施させるための管理が委託元である大学に求められる。ここでは、情報セキュリティを確保する観点から、情報処理業務を外部委託により行う場合に、委託元としての業務を行う者が遵守すべき事項を定める。

(12) A3112 ソフトウェア開発における情報セキュリティ対策実施手順（策定手引書）

ソフトウェアにおけるセキュリティの実現については、開発ライフサイクル（Software Development Life Cycle）である要件定義、設計、実装、テストの各工程におけるセキュリティ対策を的確に実施することが求められる。ここでは、情報セキュリティを確保する観点から、セキュリティの高いソフトウェアを開発するために実施すべき事項を定める。

(13) A3113 外部委託における情報セキュリティ対策に関する評価手順

大学が情報処理業務を外部委託により行う場合に、委託先の情報セキュリティの確保を目的として各種評価手法を大学において利用するための手引書である。大学において情報処理業務を外部委託により行う場合には、大学が求める情報セキュリティ水準が委託先において確保される必要がある。このため、大学では、情報セキュリティ関係規程の一つとして外部委託についても規程を定めることが想定されている。この規程に従い大学としての業務を行うに当たり、情報セキュリティマネジメントシステムに関する適合性評価制度、情報セキュリティ対策ベンチマーク及び情報セキュリティ監査の各評価手法を活用することができる。

(14) A3114 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書

大学が情報システムの構築またはソフトウェアの開発を行うにあたり、その構築を請け負う外部委託者等に対して示すセキュリティ要件やセキュリティ機能を検討する際の便宜を図るために提供される解説書である。本文書は内閣官房情報セキュリティセンター（NISC）が公開している同名の文書を参照する形で提供される。

(15) A3115 情報システムの構築等における ST 評価・ST 確認の実施に関する解説書

大学が重要なセキュリティ要件が含まれる情報システムを構築するにあたり、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価・ST 確認を受ける際の便宜を図るために提供される解説書である。本文書は内閣官房情報セキュリティセンター（NISC）が公開している同名の文書を参照する形で提供される。

３．情報システムの運用・管理に係る手順等（A3101～A3115）の使い方

これらの文書は、各大学が情報システムの運用・管理に係る実施手順等を作成する際の参考資料として提供されるものであり、実際の各大学の実施手順等がこれと同一の内容で作成されるものではない。各大学においては、サンプル規程集で定められた以上の情報セキュリティ確保を目標としながら、各大学の状況や特性を踏まえつつ、これらの文書を参考として実施手順等を策定する。文書の使い方として、本文書をそのまま取り込む、構成や表現を変えて盛り込む
等の方法がある。

４．事務情報セキュリティ対策基準との関係

サンプル規程集では、事務局管理の情報及び情報システムと、その他の大学の研究教育業務に係る情報及び情報システムとで、規程体系を二分している。すなわち、「A2101 情報システム運用・管理規程」には本文書及び A3101～A3115 の各手順が対応するのに対して、「A2501 事務情報セキュリティ対策基準」には「A3500 各種マニュアル類の策定に関する解説書」が対応する。事務情報システムに関連する文書（手順、ガイドライン及びマニュアル等）については、「A3500 各種マニュアル類の策定に関する解説書」を参照されたい。

A3101 情報システムにおける情報セキュリティ対策実施手順（策定手引書）

1. 本書の目的

本書は、本学において情報システムのライフサイクルにあわせて情報セキュリティ対策を実施する際に適用する規定（以下「情報システムにおける情報セキュリティ対策実施手順」という。）を整備するための手引書である。

本学においては、「A1000 情報システム運用基本方針」と「A1001 情報システム運用基本規程」（以下「ポリシー」という。）、及びそれらを具体化する実施規程と一連の手順群を整備することが求められている。「情報システムにおける情報セキュリティ対策実施手順」は、これらの手順の一つとして策定し、本学において情報システムに情報セキュリティ対策を実施する場合に適用するものである。すなわち、部局技術責任者がこれに従うことにより、ポリシーとそれに関係する規程を遵守することになるものである。

情報システムは、目的業務を円滑に遂行するため、情報システムのライフサイクルを通じて様々な要件を満たすことが必要となる。その要件の中には、情報システムのライフサイクルで発生する様々な脅威に対応するためのセキュリティの観点からの要件も含まれる。そして、セキュリティの要件を満足するためには、情報システムのライフサイクルを通じて適切な情報セキュリティ対策を実施し、実施した情報セキュリティ対策を PDCA サイクルによって、見直ししていかなければならない。

本書は、これらの背景の下で、「情報システムにおける情報セキュリティ対策実施手順」に含めるべき手順及び記述例を具体的に示し、もってポリシーへの準拠性、業務手順への適用性等において適切な規定の整備に資することを目的とする。

2. 規定に記載すべき事項

「情報システムにおける情報セキュリティ対策実施手順」には、以下の事項を具体化する手順等を記載すること。

2.1 「A2101 情報システム運用・管理規程」に定める情報システムにおける情報セキュリティ対策に係る遵守事項

A2101-31 （情報システムの計画・設計）
A2101-32 （情報システムの構築・運用・監視）
A2101-33 （情報システムの移行・廃棄）
A2101-34 （情報システムの見直し）

3. 文書構成例

「情報システムにおける情報セキュリティ対策実施手順」は、以下の文書構成で作成することが考えられる。

1 本手順の目的
2 本手順の対象

4. 策定する上での留意事項

「情報システムにおける情報セキュリティ対策実施手順」は、以下のことに留意して策定する。

(1) 「情報システムにおける情報セキュリティ対策実施手順」は、本学における全ての情報システムと部局技術責任者が広く適用できる記述とすると利用しやすいものとなる。
(2) 「情報システムにおける情報セキュリティ対策実施手順」は、情報システムのライフサイクルに沿って記述すると理解されやすいものとなる。

5. 参考資料

「情報システムにおける情報セキュリティ対策実施手順」の策定に際しては、以下の資料が参考となる。

5.1 国際規格及び諸外国を含む政府及び政府関係機関の資料

(1) ISO/IEC 17799「Information technology - Security techniques - Code of practice for information security management」(JIS X 5080)
(2) SLCP-JCF／共通フレーム 98（ISO/IEC 12207）
(3) 経済産業省「システム管理基準」
(4) IT セキュリティ評価及び認証制度 ISO/IEC 15408 「Common Criteria」 (JIS X 5070)
(5) 独立行政法人情報処理推進機構（IPA）IT セキュリティ評価及び認証制度（JISEC）

http://www.ipa.go.jp/security/jisec/index.html

5.2 政府以外の資料

なし。

6. 雛形の利用方法

別紙１の雛形を参考にして、「情報システムにおける情報セキュリティ対策実施手順」を策定すると効率的である。別紙１の雛形は、前記 2 の手順に記載すべき事項を、前記 3 の文書構成例の枠組みの中に記載したものである。

6.1 雛形において想定する前提

本雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 全学実施責任者又は部局総括責任者が手順を策定することを想定している。
- 部局技術責任者が手順を利用することを想定している。
- 大規模な情報システム等であり、情報システムのライフサイクルにおける業務を外部委託する場合、「外部委託におけるセキュリティ対策実施手順」に記載された事項を考慮するべきである。
- 個別の情報セキュリティ対策の適用に関する詳細については、別途情報セキュリティ関係手順を定め、これを遵守することを要求する必要がある。

6.2 手直しポイント

「情報システムにおける情報セキュリティ対策実施手順」を策定するに当たり、以下の点について手直しをする必要がある。

(1) 雛形において[・・・] 形式で示す設定値（担当者名、手順書名等）については、各大学内の定めに合わせる。
(2) 雛形において【・・・の場合】形式で示す記述については、想定される案を記したものであり、各大学の判断により適宜、選択又は修正する。
(3) 既存のガイドライン等との整合性を考慮し、適切に分割、統合、相互参照する。
(4) 雛形に情報セキュリティ対策の観点以外の一般的な記述について不足がある場合には、適宜、補う。

別紙１　A 大学情報システムにおける情報セキュリティ対策実施手順　雛形

本書の位置付け

本書は、情報システムにおける情報セキュリティ対策実施手順を作成する場合の雛形であり、「情報システムにおける情報セキュリティ対策実施手順 策定手引書」2 に示す手順に記載すべき事項を、同 3 に示す文書構成例の枠組みの中に盛り込み作成したものである。

本書の利用方法

本書において想定する前提

本雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 全学実施責任者又は部局総括責任者が手順を策定することを想定している。
- 部局技術責任者が手順を利用することを想定している。
- 大規模な情報システム等であり、情報システムのライフサイクルにおける業務を外部委託する場合、「外部委託におけるセキュリティ対策実施手順」に記載された事項を考慮する必要がある。
- 個別の情報セキュリティ対策の適用に関する詳細については、別途情報セキュリティ関係手順を定め、これを遵守することを要求する必要がある。

手直しポイント

「情報システムにおける情報セキュリティ対策実施手順」を策定するに当たり、以下の点について手直しをする必要がある。

(1) 雛形において*[・・・]* 形式で示す設定値（担当者名、手順書名等）については、各大学内の定めに合わせる。
(2) 雛形において【・・・の場合】形式で示す記述については、想定される案を記したものであり、各大学の判断により適宜、選択又は修正する。
(3) 既存のガイドライン等との整合性を考慮し、適切に分割、統合、相互参照する。
(4) 雛形に情報セキュリティ対策の観点以外の一般的な記述について不足がある場合には、適宜、補う。

1. 本手順の目的

情報システムは、目的業務を円滑に遂行するため、情報システムのライフサイクルを通じて様々な要件を満たすことが必要となる。その要件の中には、情報システムのライフサイクルで発生する様々な脅威に対応するための情報セキュリティの観点からの要件も含まれる。そして、セキュリティの要件を満足するためには、情報システムのライフサイクルを通じて適切な情報セキュリティ対策を実施し、実施した情報セキュリティ対策を PDCA サイクルによって、見直ししていかなければならない。

本手順は、情報システムのライフサイクルの視点に立ち、情報システムのセキュリティ要件に基づいて、各段階において考慮すべき情報セキュリティ対策について定めることを目的とする。

2. 本手順の対象

2.1 対象者

本手順は、部局技術責任者を対象とする。

3. 用語の定義

本手順において使用する用語の定義は次のとおりである。

(1) **「情報システム」とは、情報処理及び通信に係るシステムをいう。**

(2) **「機器等」とは、情報機器及びソフトウェアをいう。**

(3) **「情報システムのライフサイクル」とは、情報システムの「計画／設計／構築／運用／移行／廃棄」の過程をいう。**

(4) **「情報セキュリティ対策の PDCA サイクル」とは、情報セキュリティ対策の「計画（PLAN）／実施（DO）／点検（CHECK）／見直し（ACTION）」の過程をいう。**

4. 情報システムの計画

4.1 体制の確保

【手順策定者への解説】

情報システムのライフサイクル全般にわたってセキュリティを維持していく体制を確保するためには、十分な資源が必要となる。資源としては、一般的に下記のようなものが想定できる。

- セキュリティを維持するための人員（＝ヒト）
- セキュリティを維持するための予算（＝カネ）
- セキュリティを維持するための機器（＝モノ）

(1) **[部局技術責任者]は、セキュリティを維持するために人員、予算、機器等を必要とする場合は、[部局総括責任者]に申請すること。**

【手順利用者への補足説明】

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セキュリティを維持するために必要な措置に対して、部局総括責任者より十分な資源の提供を受けるべきである。

なお、情報システムのライフサイクルを通じてセキュリティを維持するために必要な措置とは、すなわち本項以降で説明されるすべての事項にほかならない。

【情報システムの分析を求める場合】

4.2 情報システムの分析

【手順策定者への解説】

情報システムのライフサイクル全般にわたってセキュリティを維持するためには、情報システムの状況に関する正確な調査・認識が必要であり、これは、稼動中のシステムであっても、開発中のシステムであっても同様である。

【システム構成図の作成を求める場合】

(1) [部局技術責任者]は、システムが提供するサービス、システムの構成、システムの関与者をまとめ、[システム構成図]を作成すること。

【手順利用者への補足説明】

情報システムのライフサイクル全般にわたってセキュリティを維持する作業を実施しやすくするために、情報システムの概要、情報システムの関与者、ネットワーク環境等について調査し、把握しておくべきである。

なお、大規模な組織においては、今後の作業を軽減するために、セキュリティ要件を判断する上で類似している情報システム、すなわち類似する構成、関与者、ネットワーク接続等、同一のセキュリティの条件を持った情報システムをグループ化しておくことが望ましい。

まとめた内容は、「システム構成図」等として整理しておくと脅威の洗い出し等の今後の作業が実施しやすい。

一般的に調査・把握しておくべき事項を以下に例示する。

(a) 情報システムの概要

- 適用業務
- 機能
- 設置場所
- [その他各本学が情報セキュリティ関係手順で定める事項]

(b) 情報システムの関与者

- サーバ担当者
- ネットワーク担当者
- ソフトウェア開発者
- 機器等の購入者
- 利用者
- 保守管理者

● [その他各本学が情報セキュリティ関係手順で定める者]

(c) ネットワーク環境

● ネットワーク接続
● インターネット等の外的環境との接続
● 外部システムとの連携
● [その他各本学が情報セキュリティ関係手順で定める事項]

【情報システムの構成要素の調査・把握を求める場合】

(2) **[部局技術責任者]は、情報セキュリティ対策の観点から情報システムの構成要素を調査し、把握すること。**

【手順利用者への補足説明】

情報システム運用・管理規程において、情報システムとは「情報処理及び通信に係るシステム」と定義され、具体的には、サーバ装置やクライアント PC 等のハードウェア、個別に開発した研究教育事務用アプリケーション、商用 OS や DBMS 等の製品ソフトウェア、通信回線及び通信回線装置等の複数の要素から構成される。この場合、情報システム全体のセキュリティ強度は、最も弱い部分のセキュリティ強度の影響を受ける。例えば、ウェブアプリケーションが極めて強固に作られていても、セキュリティホールを抱えるウェブサーバソフトウェアを使用していれば、情報システム全体としては脆弱となる。

情報システム全体のセキュリティ水準を高めるためには、各構成要素における情報セキュリティ対策を実施する必要があり、その前提として、情報システムの構成要素を調査し、把握しておくべきである。

一般的に調査・把握しておくべき事項を以下に例示する。

● アプリケーションソフトウェア（研究教育事務用アプリケーション等）
● OS、ミドルウェア（UNIX®系 OS、Linux®系 OS、Windows®系 OS、DBMS 等）
● サーバ装置（サーバ、ワークステーション等）
● 端末、周辺機器（デスクトップ PC、ノート PC、プリンタ、外部記録媒体等）
● 通信回線及び通信回線装置（LAN、インターネット、ルータ、モデム等）
● [その他本学が情報セキュリティ関係規程で定める事項]

【情報システムの台帳の作成を求める場合】

(3) **[部局技術責任者]は、情報システムの台帳を作成すること。**

【手順利用者への補足説明】

情報システムの分析の結果を本学の共通する様式の台帳等にまとめておくと、組織全体の情報セキュリティを管理する面で役立つ資料となる。

一般的に管理すべき項目を以下に例示する。

● 情報システムの一意的な名称

- 情報システムを管理する部局
- 用途の概要
- 用途の種別
- システムの種別
- サーバの有無
- 端末の有無
- アカウント数、インターネット接続
- 学外端末からの利用者
- [その他本学が情報セキュリティ関係規程で定める事項]

4.3 情報システムのセキュリティ要件

【手順策定者への解説】

セキュリティ要件とは、情報セキュリティに関する要求事項である。情報システムのセキュリティ要件を決定し、セキュリティ要件の重要性を判断する必要がある。

例えば、郵便を送る場合、その内容が秘匿すべきもので、かつ途中で盗み読まれる危険があるのであれば、封入封緘し、書留等の方法を用いるべきであるが、その内容が誰に読まれても構わない内容であるか、または盗み読まれる危険性がそもそもないのであれば、普通郵便で送るなど特に対策を採る必要がない。

なお、「A2101 情報システム運用・管理規程」では、本学において共通して対応を図るべき脅威として以下の対策を定めている。

- セキュリティホール対策［A2101-18］
- 不正プログラム対策［A2101-19］
- サービス不能攻撃対策［A2101-20］

【セキュリティ要件の決定に当たって、情報システムが取り扱う情報の抽出と格付けを要求する場合】

(1) **[部局技術責任者]は、情報システムが取り扱う情報のうち保護すべき情報を抽出し、抽出した情報資産に対して、機密性、完全性及び可用性の観点から情報の格付けを実施すること。**

【手順利用者への補足説明】

情報システムのセキュリティ要件を決定するために、情報システムが取り扱う情報のうち保護すべきものを抽出し、当該情報について、そのセキュリティ上の重要度を識別しておくため、情報の機密性、完全性、可用性の格付けを行う必要がある。

なお、情報の抽出に当たっては、例えば、情報システムで取り扱う情報を以下のように大別して作業を行うと効率的である。

- 一次情報資産（研究教育事務文書等）
- 二次情報資産（システム構成情報等）

一次情報資産とは、情報システムにて取り扱う研究教育事務情報そのものである。二次情報資産は、例えば、ソースコードやセッション ID 等の情報システムの構成情

報であり、一次情報資産を保護するために、間接的に重要な情報といえる。二次情報資産にどのようなものが含まれるかは、システムの仕様に左右されるが、新規開発の案件であれば、基本設計等の工程を経ることで明確化される。この分類は情報システムの開発が外部に委託される場合は、一次情報資産の洗い出しが発注者側の責務となり、二次情報資産の洗い出しが受注者側の責務となることが多いことから有効である。

【セキュリティ要件の決定に当たって、情報システムが取り扱う脅威の洗い出しを要求する場合】

(2) **[部局技術責任者]は、どのような攻撃者が、どの情報に対して、どのような攻撃を行う可能性があるかを検討し、情報システムに対する脅威を洗い出すこと。**

【手順利用者への補足説明】

情報システムに対する情報セキュリティの脅威とは、情報の機密性、完全性、可用性の侵害であり、例えば、機密性の侵害であれば、アカウントのない者によるデータへのアクセス、アカウントのある者によるアクセス、又は通信の盗聴等、様々な事由によって情報漏えいという事象として表面化する。

このため、脅威を検討するに当たっては、「どのような攻撃者が、どのデータに対して、どのような行いをする可能性があるか」を検討し、明確にする必要がある。

(3) **[部局技術責任者]は、情報システムのセキュリティ要件を決定すること。**

【情報システムのセキュリティ要件定義書の作成を要求する場合】

(4) **[部局技術責任者]は、決定したセキュリティ要件に基づいて、セキュリティ要件定義書を作成すること。**

【手順利用者への補足説明】

セキュリティ要件は、今後の作業のために「セキュリティ要件定義書」として文書化しておくことが望ましい。また、決定した情報システムのセキュリティ要件を各構成要素のセキュリティ要件として具体化するべきである。

なお、セキュリティ要件を決定する具体的な手順は、[情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書]を参考とできる。

4.4 情報システムにおける情報セキュリティ対策の選択

【手順策定者への解説】

情報システムにおける情報セキュリティ対策は、認証や暗号化等の情報セキュリティの機能についての対策、不正プログラムやサービス不能攻撃等の脅威への対策、情報システムの開発や購入等において必要な対策、ハードウェアや通信回線等の情報システムの構成要素についての対策等、情報システムのセキュリティ要件に応じ

て極めて多様な形態を取り得る。

「A2101 情報システム運用・管理規程」は、大学として最低限必要となる情報セキュリティ対策を定めるものである。それぞれの情報システムにおいては、情報システムにおける情報セキュリティ対策について、「A2101 情報システム運用・管理規程」が要求している遵守事項からセキュリティ要件を満足する有効かつ網羅的な情報セキュリティ対策を選択し、これを実施するべきである。

(1) **[部局技術責任者]は、情報システムのセキュリティ要件に基づいて、当該情報システムに関係する情報セキュリティ対策を[情報システム運用・管理規程]より選択し、これを実施すること。**

【手順利用者への補足説明】

それぞれの情報システムについて、情報システムのセキュリティ要件に基づいて必要となるセキュリティ対策を「A2101 情報システム運用・管理規程」より選択し、これを実施するべきである。

なお、 情報システムのセキュリティ要件を満足できない場合は、セキュリティ要件に基づいて、追加のセキュリティ対策を選択し、実施するべきである。

(2) **[部局技術責任者]は、情報システムのセキュリティ要件に基づいて、情報システムにおける脅威に適切に対抗する情報セキュリティ対策を漏れなく選択すること。**

【手順利用者への補足説明】

情報セキュリティ対策とは、「資産を脅威からどのように守るのか」という方法論である。脅威に対抗するための情報セキュリティ対策そのものに誤りや抜けがある場合、情報システムのセキュリティは維持できない。

例えば、「なりすまし」の脅威があるサーバに冗長化という対策を行ったとしても「なりすまし」を防ぐことはできない。また、外部の人間に厳重な認証を行っていながら、開発者が自由にアクセスできてしまう情報システムは、「開発者の悪意」という脅威に対しては無防備である。

したがって、情報システムのセキュリティ要件に基づいて、脅威に適切に対応した情報セキュリティ対策を漏れなく選択すべきである。

(3) **[部局技術責任者]は、情報システムのセキュリティ要件に基づいて、情報システムのライフサイクルを網羅する情報セキュリティ対策を選択すること。**

【手順利用者への補足説明】

情報システムに対する脅威は、情報システムのライフサイクルを通して存在している。

例えば、不正プログラムに対抗するために最新のアンチウイルスソフトウェアを購入しインストールしても、運用時の定義ファイルの更新に不備があれば、新たな

不正プログラムに対して無防備となる。また、情報システムの厳格な運用を行っていても、機器等が安易に廃棄されれば、機密情報が漏えいすることも考えられる。

したがって、情報システムのセキュリティ要件に基づいて、情報システムのライフサイクルを通して、網羅的な情報セキュリティ対策を実施するべきである。

5. 情報システムの設計・構築

5.1 設計・構築における情報セキュリティ対策

【手順策定者への解説】

情報システムのライフサイクルにおける設計・構築においては、情報システムのセキュリティ要件に基づいて、脅威に適切に対抗するセキュリティ機能を実装した情報システムを設計・構築し、設計・構築時におけるセキュリティ要件を満足していることを検証・確認した上で、運用環境に安全に導入する必要がある。

なお、重要なセキュリティ要件があると認めた情報システムについては、ST 評価、ST 確認と IT セキュリティ評価・認証制度を利用して、設計・構築を行うことが可能であり、これについては、本雛形の 9 章で示している。

(1) [部局技術責任者]は、脅威に対抗する情報システムのセキュリティ機能の設計と構成要素の構築を行うこと。

【手順利用者への補足説明】

情報システムの設計段階において、脅威に確実に対抗するために必要なセキュリティ機能を適切に選択すべきである。また、構成要素を適切に構築して、情報システムのセキュリティ機能を有効に動作させなければならない。

なお、情報システムの構築に際しては、機器等を購入したり、ソフトウェアを独自に開発したりする場合が想定される。

例えば、情報システムの構成要素の内、サーバ装置、端末等のハードウェア及び OS、ミドルウェア等のソフトウェアは、市販されている製品の購入、また、業務プログラム等は、業務仕様にあわせて開発することが想定される。

機器等の購入における情報セキュリティ対策については、[機器等の購入におけるセキュリティ対策実施手順]を、ソフトウェア開発における情報セキュリティ対策については、[ソフトウェア開発におけるセキュリティ対策実施手順]をあわせて参照されたい。

(2) [部局技術責任者]は、セキュリティ要件を満足する情報システムが設計・構築されたことを検証・確認すること。

【手順利用者への補足説明】

設計・構築時において、セキュリティ要件を満足する情報システムが設計・構築

されたことを検証・確認するための情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 設計・構築時におけるセキュリティのレビューとテスト
- セキュリティを考慮した設計・構築体制及び環境
- 評価・認証等を受けた製品

(3) **[部局技術責任者]は、誤った情報システムの導入及び運用環境と開発用資産へのセキュリティ侵害を防止するため、情報システムを運用環境に導入する手順及び環境に関するセキュリティの管理を行うこと。**

【手順利用者への補足説明】

脆弱性を発生させるような誤った情報システムの導入及び運用環境や開発用資産へのセキュリティ侵害を防止するため、導入のための手順及び環境を管理するための情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 運用の誤りを低減するためのガイダンスと教育（機能、設計、操作、保守、事故対応手順等）
- 脆弱性の混入を排除するための安全な導入の手順（配付・移送の保護、セキュリティを意識した設定等）
- セキュリティの保たれた運用環境への導入
- 運用環境へのセキュリティ侵害を防止する安全な移行の手順
- 開発に利用した機密性を有する情報資産の廃棄

(4) **[その他本学が必要と認めるセキュリティ対策]**

6. 情報システムの運用

6.1 運用における情報セキュリティ対策

【手順策定者への解説】

情報システムのライフサイクルにおける運用においては、情報システムのセキュリティ要件に基づいて、設計・構築したセキュリティ機能を適切に運用、維持することでセキュリティレベルの低下を慎重に防止することに加えて、運用時に発生するセキュリティの問題を想定し、これに適切に対処するための手順を整備しておく必要がある。

(1) **[部局技術責任者]は、情報資産へのセキュリティ侵害を防止するために、セキュリティ機能の適切な利用を行うこと。**

【手順利用者への補足説明】

強固なセキュリティ機能が実装されたとしても、その後適切な利用が行われなけ

れば情報システムのセキュリティは維持できない。例えば、ソフトウェアにマクロの自動実行を禁止する機能が実装されていたとしても、利用者がその機能を使用していない状態では、不正プログラムに感染する危険性は低減しない。

セキュリティ機能の誤った利用による情報資産へのセキュリティ侵害を防止するため、セキュリティ機能の適切な利用という観点からの情報セキュリティ対策を選択すべきである。

(2) **[部局技術責任者]は、法令や規制等の要求を満足するため、将来発生するかもしれない障害等の調査のため、又は情報セキュリティ対策の点検と改善に資するために、情報システムの運用を記録すること。**

【手順利用者への補足説明】

法令及び規制等の要請に応えるため、将来発生し得る障害等の調査のため、又は情報セキュリティ対策の点検と改善に資するため、情報システムの運用の記録という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 情報システムへのセキュリティ侵害に関する記録（適正な取得内容、時期、項目等）
- 記録へのセキュリティ侵害に対応するための保護（アクセス制御、暗号化、保存、廃棄等）

(3) **[部局技術責任者]は、セキュリティの侵害を検知するために、情報システムの運用を監視すること。**

【手順利用者への補足説明】

セキュリティの侵害を検知するため、情報システムの運用の監視という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 不正な変更やセキュリティレベルの低下を防止する情報システムの構成変更の監視
- 不正行為、不正利用に対する監視
- 性能、故障等の監視

(4) **[部局技術責任者]は、情報システムの障害等及び作業時における機密性、完全性の侵害から保護するために保守作業におけるセキュリティの管理を行うこと。**

【手順利用者への補足説明】

情報システムの障害等及び作業時における機密性、完全性の侵害から保護するために保守作業における情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 障害等を低減する適切な保守（適正な時期、回数、方法等）
- 障害等から情報システムを復旧させるための情報のバックアップ（適正な時期、回数、媒体、復元等）
- バックアップ情報への機密性、完全性侵害を防止するための保護（アクセス制御、暗号化等）
- 情報システムへの機密性、完全性の侵害を防止するための保守作業の管理（許可された担当者、暗号化された作業、機器等を敷地外に持ち出す場合の保護等）

(5) **[部局技術責任者]は、新たに発生する脅威から情報システムを保護するための脆弱性への対応を行うこと。**

【手順利用者への補足説明】

新たに発生するセキュリティホールや不正プログラムから情報システムを保護するため、脆弱性への対応という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 新たに発生する脆弱性に迅速かつ安全な対応を行うための手順（脆弱性情報の収集、対応計画、暫定対応、修正の試験、修正の配布方法等）

(6) **[部局技術責任者]は、障害等による被害拡大の防止と情報システムを迅速に回復するための対応を行うこと。**

【手順利用者への補足説明】

障害等による被害拡大を防止し、情報システムを迅速に回復するため、障害等に関する対応という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 障害等による被害拡大防止及び早期復旧のための手順（事故の定義、報告、対処、復旧、原因検証、再発防止、訓練等）

(7) **[その他本学が必要と認めるセキュリティ対策]**

7. 情報システムの移行・廃棄

7.1 移行・廃棄における情報セキュリティ対策

【手順策定者への解説】

情報システムのライフサイクルにおける移行・廃棄においては、情報システムのセキュリティ要件に基づいて、情報システムの記憶媒体に含まれる情報の適切な消去を行う必要がある。

(1) **[部局技術責任者]は、法令、規制等の要求を遵守し、かつ情報の漏えいを防止するために、**

記憶媒体に含まれる情報を消去すること。

【手順利用者への補足説明】

情報システムの記憶媒体に保存されている情報について、法令、規制等の要求を遵守し、かつ情報の漏えいを防止するために情報の消去という観点からの情報セキュリティ対策を選択すべきである。

以下の事項を考慮した対策を実施することが望ましい。

- 記憶媒体に保存された情報への機密性の侵害を防止するための情報の消去

(2) [**その他本学が必要と認めるセキュリティ対策**]

8. 情報セキュリティ対策の見直し

8.1 情報セキュリティ対策の見直し

【手順策定者への解説】

実施すべき情報セキュリティ対策は、状況や環境の変化によって影響を受ける。

例えば、ある時点で有効とされる情報セキュリティ対策が、新たな脅威の発生によって無効化されるおそれがあり、また組織が新たに重要な業務を受け持つようになったり、法令が改正される等の環境の変化があったりした場合は、既存の対策の十分性が失われる可能性がある。

こうしたことから、情報システムにおける情報セキュリティ対策は PDCA サイクルに基づいて、常に見直して、有効かつ効率的に機能しているかを検証し、最適な状態に維持し続けなければならない。

(1) [**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を必要に応じて見直すこと。**

【手順利用者への補足説明】

情報セキュリティ対策は下記の要因を踏まえて定期的又は必要に応じて見直し、最適化を進めていくべきである。

(a) 定期的な要因

- 自己点検の結果
- 監査の結果
- 情報システムの記録、監視の結果

(b) 非定期的な要因

- 組織の変更
- 技術の変化
- 情報セキュリティ関係規程の変更
- 脅威の変化
- 法的規制又は社会環境の変化

9. ST 評価・ST 確認と IT セキュリティ評価及び認証制度の活用

9.1 ST 評価・ST 確認の手続

【手順策定者への解説】

ST 評価・ST 確認は、情報システム及び製品のセキュリティ設計仕様書（ST：Security Target）が ISO/IEC15408 に適合していることを、第三者評価機関を使い評価・確認する制度である。セキュリティ機能の実装に当たって客観性の高い評価・確認を行いたい場合には、ST 評価・ST 確認を受けることを求めることができる。

(1) **[部局技術責任者]は、[情報システムの構築等における ST 評価・ST 確認の実施に関する解説書]に準じて、重要なセキュリティ要件がある情報システムについて、ST を作成し、評価機関・認証機関に申請を行い、ST 評価・ST 確認を受けたことを示す確認書を入手すること。なお、ST 評価・ST 確認は開発が終了するまでに終了すること。**

【手順利用者への補足説明】

セキュリティ機能の実装に当たって客観性の高い評価・確認を行いたい場合には、セキュリティ設計仕様書（ST：Security Target）に関する ST 評価・ST 確認を受けるべきである。

本学が自ら情報システムの構築又はソフトウェアの開発を行う場合には、本学が第三者機関に依頼して ST 評価・ST 確認を受けることを想定している。

情報システムの基本設計がまとまった時点で、ST の作成を開始し、ST 評価・ST 確認の申請を評価機関・認証機関に行い、ST 確認を実施する必要がある。また、ST 評価・ST 確認は、開発が終了するまでに終了している必要がある。

なお、手続の詳細については、[情報システムの構築等における ST 評価・ST 確認の実施に関する解説書]を参考とできる。

(2) **[部局技術責任者]は、ST 評価・ST 確認を行う場合、ST 評価・確認制度を運用する IPA（独立法人情報処理推進機構）の策定する要領に沿って ST を作成すること。**
[http://www.ipa.go.jp/security/jisec/apdx0504.html]

【手順利用者への補足説明】

ST に関する詳細は、ST 評価・確認制度を運用する IPA（独立法人情報処理推進機構）のホームページに記載されており、これに準じて作成する必要がある。

【IT セキュリティ評価・認証制度を利用する場合】

9.2 ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度の利用

【手順策定者への解説】

構築する情報システムの構成要素として調達する機器及びソフトウェアの選択に当たり、採用候補製品が複数ある場合に、ISO/IEC 15408 に基づく IT セキュリテ

ィ評価及び認証制度に基づく認証を取得している製品を選択する。IT セキュリティ評価・認証制度とは、IT 製品あるいはシステムのセキュリティ機能が、正確に実装され、想定されている脅威に有効に動作することを、認定された中立性の高い第三者（評価機関）が評価する制度である。

なお、本事項はサンプル規程集における強化遵守事項であって、採否は各大学が判断する。

(3) **[部局技術責任者]は、重要なセキュリティ要件がある情報システムについて、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能について、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合には、その中から当該セキュリティ機能に関して IT セキュリティ評価及び認証制度に基づく認証を取得している製品を情報システムの構成要素として選択すること。**

【手順利用者への補足説明】

情報システムの構築を行う場合には、[外部委託における情報セキュリティ対策実施手順 策定手引書及び同雛形]も参照されたい。

なお、手続の詳細については、「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」を参考とできる。

A3102 例外措置手順書

1. 目的

本学における大学業務を遂行するに当たって、ポリシー・実施規程・手順の適用が大学業務の適正な遂行を著しく妨げる等の理由により、ポリシー・実施規程・手順とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合がある。

こうした場合においても、あらかじめ定められた例外措置のための手続により、情報セキュリティを維持しつつ柔軟に対応できなければ、ポリシー・実施規程・手順の実効性を確保することは困難となる。

本書は、教職員等が例外措置の適用を希望する場合の手続を定め、もって例外措置において必要な情報セキュリティ水準を確保することを目的とする。

2. 本手順書の対象者

本書は、すべての教職員等を対象としている。

3. 定義

本書における用語の定義は次のとおりである。

(1) 「例外措置」とは、教職員等がその実施に責任を持つポリシー・実施規程・手順を遵守することが困難な状況で、大学業務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

(2) 「申請者」とは、例外措置の適用を申請する者をいう。

(3) 「許可権限者」とは、例外措置の適用を審査する者をいう。

(4) 「代替措置」とは、例外措置の適用に伴い発生するリスクを低減するためにポリシー・実施規程・手順が定める内容とは異なる代替のセキュリティ対策をいう。

4. 格付け及び取扱制限の手順

4.1 許可権限者

(1) ポリシー・実施規程・手順の遵守事項に対する例外措置の許可権限者を下記に定める。

申請者 （遵守義務を負うもの）		許可権限者	
		通常の場合	その他
全学総括責任者		全学情報システム運用委員会	ポリシー・実施規程・手順の遵守事項に被報告者、被届出者、被返還者、被許可者、承認者、判断者がある場合は当該者
全学情報システム運用委員会		全学総括責任者	
全学実施責任者		全学総括責任者	
情報セキュリティ監査責任者		全学総括責任者	
情報セキュリティ監査を実施する者		情報セキュリティ監査責任者	
部局総括責任者		全学実施責任者	
部局技術責任者		部局総括責任者	
部局技術担当者		部局技術責任者	
職場情報セキュリティ責任者(上司)		部局総括責任者	
教職員等	[情報セキュリティ要件の明確化に基づく対策と情報システムの構成要素についての対策]に係る事項	部局技術責任者	
	上記以外の事項	職場情報セキュリティ責任者(上司)	

（注）上記にかかわらず、必要がある場合は、当該許可権限者の上位を許可権限者とする。

5. 例外措置の申請

5.1 前提条件

(1) 申請者は、以下の場合に、例外措置の申請を行わなければならない。

- 部局固有の手順を作成するに当たって、ポリシー及び実施規程の遵守事項への準拠性を満足できない場合
- 情報、情報システムを取扱う業務を遂行するに当たって、ポリシー・実施規程・手順の遵守事項への準拠性を満足できない場合

(2) 申請者は、例外措置を申請する理由と例外措置の実施により想定される被害の大きさと影響を検討・分析した上で、例外措置の申請を行わなければならない。

5.2 事前申請の原則

例外措置の申請は、原則として事前に行わなければならない。

5.3 事前協議の原則

他の組織と関連のある事項は、事前に協議し、調整を行った上で例外措置の申請を行わなければならない。

5.4 例外措置の申請

申請者は、付録に示す例外措置申請書に以下の事項を記入し押印した上、許可権限者に提出する。

(1) 申請日

(2) 申請者の氏名、所属、連絡先

(3) 例外措置の適用を申請するポリシー・実施規程・手順の適用箇所（規程名と条項等）

(4) 例外措置の適用を申請する期間

(5) 例外措置の適用を申請する措置内容（講ずる代替手段等）

(6) 例外措置の適用を終了したときの報告方法

(7) 例外措置の適用を申請する理由

5.5 関係書類の添付

申請者は、申請内容を明確化するために参考資料が必要となる場合、これを添付する。またやむを得ない事情で、事後申請となった場合は、経緯書を添付する。

6. 例外措置の審査

6.1 例外措置の申請の受理

(1) 例外措置の申請を受理した許可権限者は、リスクを分析し、それに対する意見を記述する。

(2) 許可権限者は、必要がある場合は、例外措置申請書を上位の許可権限者に回付する。

6.2 審査の手続

(1) 当該例外措置申請に対する許可権限者は、速やかに審査手続を実施し、例外措置申請書に以下の事項を記載する。

- 申請を審査した者の情報（氏名、役割名、所属、連絡先）
- 審査決定日
- 審査結果の内容
  - 許可又は不許可の別（許可の場合、許可番号）
  - 許可又は不許可の理由
  - 例外措置の適用を許可したポリシー・実施規程・手順の適用箇所（規程名と条項等）
  - 例外措置の適用を許可した期間
  - 許可した措置内容（講ずるべき代替手段等）

○ 終了報告の方法

(2) 許可権限者は、例外措置申請書に対して疑義又は意見のある際は、その旨の意見書を添付する。

6.3 審査基準

許可権限者は、以下の条件をいずれも満たした場合に限り、例外措置の適用を許可すること。

(1) ポリシー・実施規程・手順の遵守事項を実施しないことについて、合理的理由があると認められるとき。

(2) ポリシー・実施規程・手順の遵守事項とは異なる代替の方法を採用する場合に、当該方法を採用した場合に想定される被害の大きさ・影響と採用しなかった場合の大学業務遂行への影響を比較、検討、分析した上で、その内容及び期間につき合理的理由があると認められるとき。

6.4 審査結果の通知

許可権限者は、例外措置申請書の副本を作成し、申請者に副本を返却して、審査結果を通知する。

6.5 例外措置の効力

例外措置は、例外措置の適用許可期間の開始日より効力を生ずる。ただし、承認された事項が次の各号のいずれかに該当した場合はその効力を失う。

(1) 適用を許可された期間を終了した場合

(2) 許可後、半年以内に実施できない場合

(3) 実施後、一時中断して、その中断期間が半年以上に及ぶ場合

7. 例外措置の適用

7.1 例外措置の関係者への周知

(1) 許可権限者は、適用した例外措置を、教職員等が参照可能な状態としておく。

7.2 例外措置の適用期間中のリスク管理

(1) 申請者は、例外措置によって行われる代替措置が暫定的な措置であることを認識し、その適用期間中におけるリスク管理に留意する。

8. 例外措置の修正

8.1 例外措置の修正

(1) 申請者は、許可された例外措置が以下に該当する場合は、速やかに許可権限者に例外措置申請書の修正申請を提出して承認を得る。

・許可された措置内容に大きな変更を加える場合

・例外措置の適用期間を延長する場合

(2) 申請者は、想定される被害の大きさと影響に変更がある場合は、必要に応じて別途の代替措置を適用し、速やかに許可権限者に例外措置申請書の修正申請を提出して承認を得る。

9. 例外措置の終了

9.1 終了の報告

申請者は、例外措置の適用終了時、速やかに許可権限者に付録に示す例外措置終了報告書を提出して確認を得る。ただし、許可権限者が報告を要しないとした場合は、この限りではない。

9.2 終了報告の確認

許可権限者は、例外措置の適用期間が終了した月の月末に例外措置終了報告書の提出の有無を確認する。ただし、報告を要しないとした場合は、この限りではない。

10. 例外措置の管理

10.1 例外措置の適用審査記録の管理

審査された例外措置申請書の正本は許可権限者が管理し、申請者に返却された副本は申請者が管理する。

10.2 例外措置の適用審査記録の提出

許可権限者は、毎月１回例外措置申請書の副本をもう一部作成し、全学総括責任者に提出する。

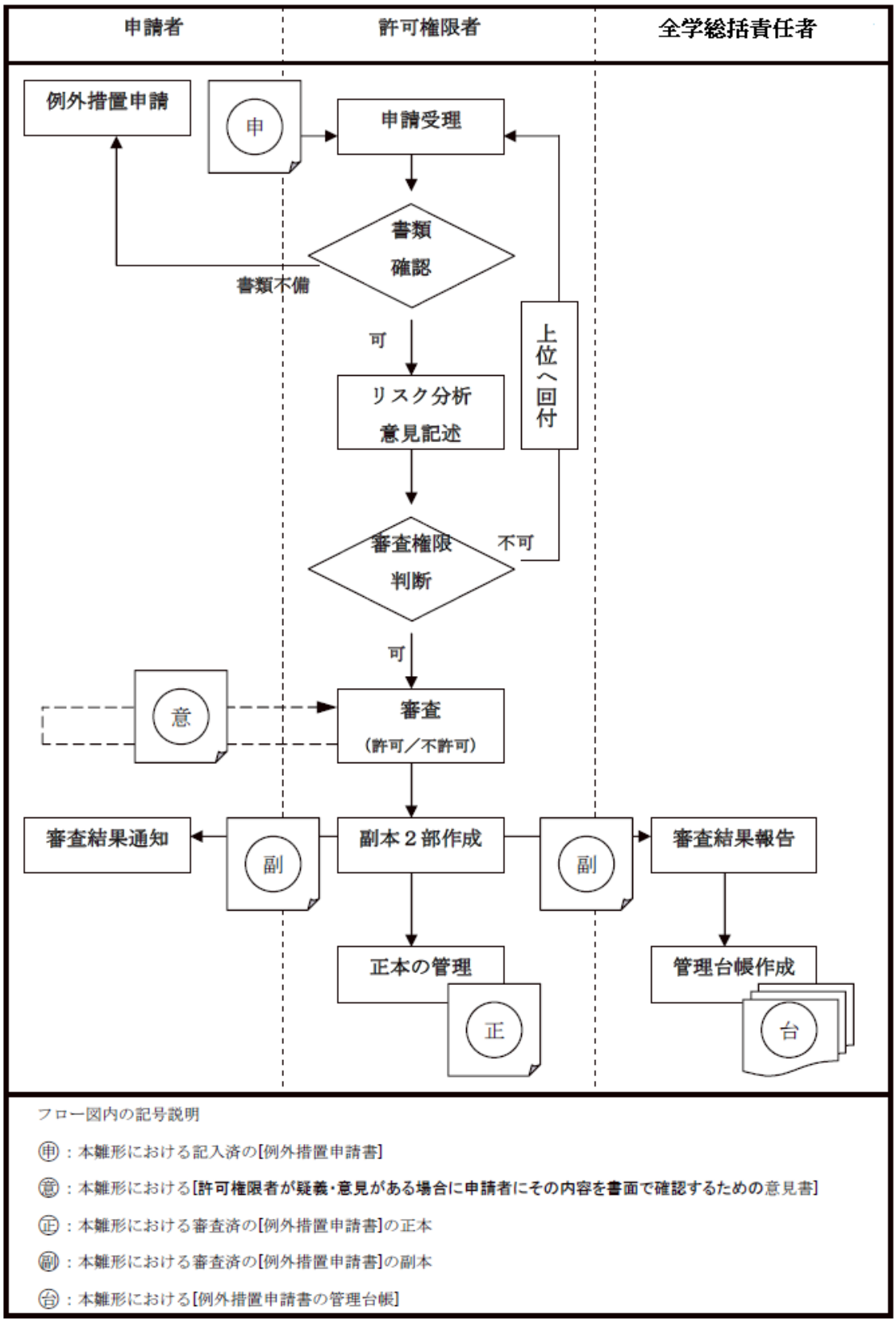
10.3 全学総括責任者による例外措置の適用審査記録の保管

全学総括責任者は、許可権限者から提出された例外措置申請書の副本を例外措置申請書の管理台帳として保管し、情報セキュリティ監査を実施する者からの申請に応じて閲覧を許可する。

11. 事務手続の代行

(1) 許可権限者は、書類の受付、書類の形式要件確認、書類の回付及び管理に関わる事務手続を、あらかじめ指定した総務担当者に行わせることができる。

付図 例外措置業務フロー



付録

例外措置申請・終了報告書

【申請・報告者記入欄】

申請・報告日 ※	年　月　日	**所属 ※**		印
適用開始希望日	年　月　日	**氏名 ※**		
適用終了希望日 ※	年　月　日	**連絡先 ※**	tel:　　mail:	
申請・報告の種別	(□新規　□延長　□修正　□終了報告)	**適用許可番号 ※**		
申請・報告対象規程	**規程名称 ※**			
	規程項番 ※			
申請・報告対象システム名 ※				
申請理由	【希望する例外措置終了時の報告方法 ：（□ 報告書提出　□ メール連絡　□ その他＿＿＿＿＿）】			
申請する代替措置の内容				

【許可権限者記入欄】

決定結果	（□許可　□不許可）	**所属・役割 ※**		印
適用許可期間	年　月　日～　年　月　日	**氏名 ※**		
適用許可番号		**連絡先 ※**	tel:　　mail:	
適用対象規程	**規程名称**			
	規程項番	**関係する手順の項番**		
許可対象システム名				
決定理由				
許可する代替措置の内容				
適用終了後の措置	**適用延長有無 ※**	（□有　□無）	**終了報告**	（□要　□否）
	適用終了日 ※	年　月　日	**報告方法**	（□報告書提出　□メール連絡　□ その他＿＿＿）

【申請書受理者記入欄】

本案件のリスク分析に対する意見

(注) 終了報告書として使用する場合は※欄について記載する。なお、適用終了日は「適用終了希望日」欄に記入。
　新規の申請の場合、申請者による「適用許可番号」の記入は不要。

許可権限者記入欄			
受付日	**審査決定日**	**申請書返却日**	**終了確認日 ※**
・　・	・　・	・　・	・　・

A3103 インシデント対応手順

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

1. 定義

(1) **物理的インシデント**

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

(2) **セキュリティインシデント**

ネットワークや情報システムの稼動を妨害し、またはデータの改ざんや消失を起こす行為及び利用行為の形態自体には問題は無いが、ネットワークの帯域やディスクや CPU の資源を浪費するなど、ネットワークやシステムの機能不全や障害または他の利用者の迷惑となる行為による情報セキュリティの確保が困難な事由の発生およびそのおそれを言い、下記原因によるものを含む。

- **大量のスパムメールの送信**
- **コンピュータウイルスの蔓延や意図的な頒布**
- **不正アクセス禁止法に定められた特定電子計算機のアクセス制御を免れる行為**
- **サービス不能攻撃その他部局総括責任者の要請に基づかずに管理権限のない情報システムのセキュリティ上の脆弱性を検知する行為**
- **利用規定により禁止されている形態での P2P ソフトウェアの利用**
- **禁止された方法による学外接続**
- **学内ネットワークへの侵入を許すようなアカウントを格納した PC の盗難・紛失**

(3) **コンテンツインシデント**

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

－電子掲示板、ブログやウェブページ等での名誉・信用毀損にあたる情報の発信
－他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信
－通信の秘密を侵害する行為
－他人の著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信
－秘密であるデータやプログラムの不正公開等守秘義務に違反する情報の発信
－児童ポルノやわいせつ画像の公開
－ネットワークを利用したねずみ講
－差別、侮辱、ハラスメントにあたる情報の発信
－営業ないし商業を目的とした本学情報システムの利用行為

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

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

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

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

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

(9) 運用･管理規程
「A2101 情報システム運用・管理規程」とそれにもとづく手順、命令、計画等を言う。

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

(11) 学外窓口
インシデントについて学外から連絡・通報を受け、学外への連絡・通報、対外クレームをするための窓口を言う。

(12) 利用規定

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

(13) 利用規定違反行為

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

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

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

2. インシデント通報窓口

(1) インシデント対応のための学外・学内の連絡・通報窓口は下記のとおりとする。

A．　学内窓口：情報メデイアセンター
B．　学外窓口：情報メデイアセンター／広報部門

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

Email: abuse@example.ac.jp

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

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

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

メーリングリストのアドレスあるいは自動転送をして関係者で同時に情報共有をすることなども考えられるが、いずれにしても一次対応する責任者を明確にしておく必要がある。

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

3. インシデントの対応判断のエスカレーション手順

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

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

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

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

① 部局内ネットワークに閉じた技術的問題か

i) **物理的インシデントまたはセキュリティインシデントの場合で、対外的インシデントでも体内的インシデントでも無く、部局内ネットワークにのみ影響が生じている場合、部局技術担当者に対策を指示し、対策結果を部局総括責任者に状況報告する。**

ii) **i)以外の場合、部局総括責任者を通じて全学実施責任者に状況報告をし、情報メディアセンターの支援を仰ぎながら、物理的インシデントまたはセキュリティインシデント対応のプロセスを実施する。**

② コンテンツインシデントか

i) **コンテンツインシデントの場合、加害者と被害者が部局内に閉じている場合であっても、法律的対策を講じる必要があるため、原則として部局総括責任者を通じて全学実**

施責任者に報告をし、情報メディアセンターの支援を仰ぎながら、ログの保全等、必要な技術的措置を取るものとする。

ii) **ただし、爆破予告・自殺予告など、生命・身体への危険等の緊急性がある場合で、部局内での対処が可能な場合は、コンテンツに関する緊急対応を実施の上、部局総括責任者と全学実施責任者に結果報告をする。**

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

(6) **部局技術責任者から報告を受けた部局総括責任者は、コンテンツインシデントについて、部局技術責任者・部局技術担当者を指揮監督する。セキュリティインシデント対応については、ポリシーに基づいて全学実施責任者に指示や承認を求める。また、法的判断を要する問題のうち、通報者への内容確認や定型回答文書の発信等、部局技術責任者や学外窓口に対して一定の一時的対応を指示または依頼する。**

(7) **学外クレームか、対外クレームか**

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

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

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

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

インシデントが発生した場合の報告･申請等の手続きに利用する様式および、当該様式を利用した報告・記録・申請・承認の要領については、「インシデント報告･承認要領」及び別紙を参照すること。

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

インシデントと影響範囲による役割・責任分担例

インシデントと影響範囲による責任分担

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

◎インシデント総括　○判断･技術支援　▲技術対応判断　△技術対応実施

4. 物理的インシデント発生時の対応

(1) 発生から緊急措置決定まで

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

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

(2) 被害拡大防止の応急措置の実施

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

(イ) 利用者等による対処が必要な場合には、その旨命令する。

(3) 緊急連絡及び報告

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

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

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

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

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

(4) 復旧計画

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

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

(5) 原因調査と再発防止策

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

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

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

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

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

5. セキュリティインシデント発生時の対応

⑴ 発生から緊急措置決定まで

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

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

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

⑵ 被害拡大防止の応急措置の実施

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

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

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

⑶ 緊急連絡及び報告

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

する。

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

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

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

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

(4) 復旧計画

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

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

(5) 原因調査と再発防止策

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

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

(ウ) 部局技術担当者と部局技術責任者は、インシデント対応作業の結果をまとめ、部局総括責任者は、再発防止策とともに全学実施責任者に報告するとともに、必要によりポリシーや実施規程の改善提案を行う。

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

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

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

・手順の確認
・作業記録の作成
・責任者、担当者への連絡
・事実の確認
・スナップショットの保存
・ネットワーク接続やシステムの遮断もしくは停止

・影響範囲の特定
・渉外、関係サイトへの連絡
・要因の特定
・システムの復旧
・再発防止策の実施
・監視体制の強化
・作業結果の報告
・作業の評価、ポリシー・運用体制・運用手順の見直し

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

6. コンテンツインシデントに関する緊急対応

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

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

(3) 部局総括責任者は、全学実施責任者に、学内緊急連絡についての指示を仰ぐ。その際、広報、保護者、警察への連絡等の学内規則に従う。

7. 学外クレーム対応

(1) 原則

(ア) 学外クレームを受けた場合で、請求の法律的な効果や指摘されたコンテンツや行為の違法性の判断を要するときは、あらかじめ対応手順が明確になっていない限り、必ず法律の専門家に相談するものとする。

(イ) 部局技術責任者は、学外クレームについては、部局総括責任者及び全学実施責任者に報告を行ものとする。

(ウ) 学外クレームについての報告を受けた全学実施責任者は、全学総括責任者の承認を仰ぎ必要に応じ非常時対策本部を設置するものとする。

(エ) 全学実施責任者または非常時対策本部は、攻撃先サイトや関係するサイトへの連絡、外部広報、及び JPCERT/CC への連絡などを指揮し、部局技術責任者及び部局技術担当者は、その指示に従うものとする。

(2) 利用者等のコンテンツの違法性を主張した送信中止・削除の要求

(ア) 発信元利用者等の特定

学外クレームが利用者等により不特定多数に宛て情報発信されたコンテンツの違法性

や情報発信による権利侵害を主張してコンテンツの送信中止や削除の要求が被害を主張する者またはその代理人からなされたものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。

(イ)（通常手続き）コンテンツを発信した利用者等への通知と削除

a. 指摘されたコンテンツの違法性の判断が困難な場合、プロバイダ責任制限法第 3 条第 2 項第 2 号に基づき利用者等に請求があった旨通知し、通知後 7 日以内に利用者等から反論がない場合は、送信中止あるいは削除を実施するものとする。

b. 有効と思われる反論があった場合は、その旨、削除請求者に伝えるとともに、当事者間での紛争解決を依頼する。

(ウ)（緊急手続き）利用者等への通知前の一旦保留

a. 指摘されたコンテンツの違法性が疑いもなく明らかと判断できる場合、一旦利用者等のコンテンツの送信を保留し、その旨利用者等に伝えるものとする。有効な反論があればコンテンツ送信を復活するものとする。

b. 本手続きの対象は、著名な音楽 CD の丸写しや個人の住所や電話の暴露等、権利侵害の疑いが濃厚である場合、緊急な救済の必要性がある場合のみとする。

c. 本緊急手続が適用されることもあることは具体的に利用規定として明示する等、利用者等に周知するものとする。

解説：「プロバイダ責任制限法ガイドライン等検討協議会」の各ガイドラインを参照。
http://www.telesa.or.jp/consortium/provider/index.htm

(3) 利用者等の発信したコンテンツの刑事的違法性の指摘及び送信中止・削除の要求

(ア) 利用者等の発信したコンテンツが刑事法上違法な可能性の高い旨指摘された場合で、名誉毀損や、著作権侵害等、被害者が存在する犯罪については、（２）と同様の手順を取るものとする。

(イ) わいせつ物陳列罪等、被害者のいない犯罪が外部クレームにより指摘された場合、

a. 部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。

b. 発信元利用者等に犯罪であるとする指摘があった旨通知し、7 日を経過しても利用者等から反論がない場合は、送信中止あるいは削除を実施する。

解説：情報内容についての刑事的な違法性判断は困難な場合が多く、基本的には、発信元利用者等の反論を待ってから送信防止措置を講ずることとする。

(4) 利用者等の行為（コンテンツ以外）の違法性を主張した送信中止・アカウント削除等の要求

i)（通常の対応）通信を発信した利用者等への通知とアカウント停止

- 学外クレームが利用者等による１対１の情報発信による権利侵害等による被害を主張して情報発信の中止を要求するものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。
- 事実確認を行い、特定できた利用者等に対し、問題の通信の発信を中止するよう通知する。これには再度行った場合には関連するアカウントを停止する旨警告することを含む。

- 利用者等から有効な反証があれれば、関連するアカウントの一時停止を解除する。
- 念書をとるなどの対応の後、アカウントの復活手続きを行う。
- 同様の手順を経て再発が確認できた場合には、Ａ大学の処罰の手順に移行する。

ii)（セキュリティインシデント対応）利用者等のアカウントの一時停止

- 学外クレームが利用者等による１対１の情報発信によるセキュリティインシデントによる被害を主張して情報発信の中止を要求するものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。
- 部局技術担当者は、事実を調査し、発信元利用者等を特定する。
- 部局技術担当者は、利用者等の行為がセキュリティインシデントの原因であると判断するのに十分な理由がある場合には、部局技術責任者に報告し、その判断を求めるものとする。
- 部局技術担当者からの報告を受けた部局技術責任者は、必要な場合、利用者等の関連するアカウントを一時停止するとともに、部局情報システム運用委員会に報告する。
- 請求者が連絡を要求しているときには一時停止した旨連絡する。
- アカウントを一時停止した旨利用者等に通知するとともに、再度行った場合には関連するアカウントを停止する旨警告する。
- 利用者等から有効な反証があれれば、関連するアカウントの一時停止を解除する。
- 念書をとるなどの対応の後、アカウントの復活手続きを行う。
- 同様の手順を経て再発が確認できた場合には、Ａ大学の処罰の手順に移行する。

解説：プロバイダ責任制限法第３条は、不特定の者により受信される通信（ウェブサイト、ブログや電子掲示板等によるいわゆる公然性を有する通信）を対象としており、インスタントメッセージやメールのような１対１の通信には適用されない。従って、脅迫メール、特定のメールボックスをターゲットにしたメール爆弾や、特定サーバへのクラッキング等、システムの機能障害を引き起こす通信やコンテンツが問題となる場合であっても特定の者相手の通信には適用がない。

しかし、プロバイダ責任制限法の適用範囲には入らず、免責の対象とはならないとはいえ、学内ネットワークの利用規定が、これらの行為についても手続きを明確にして利用規定違反とし、外部からの送信停止要求についても対応できるようにすることは法律上問題はない。これは学問の自由や表現の自由との関係においても問題が少ないと考えられる。

(5) 損害賠償請求等

（ア）利用者等の情報発信や学外でのネットワークを利用した行為について損害賠償請求や謝罪請求があった場合には、法律の専門家と相談の上、対応するものとする。

（イ）学外クレームに対して、法律的判断をせずに、謝罪することや、その他の約束をしてはならない。

（ウ）利用者等の発信者情報等、連絡先が特定できている場合、損害賠償を請求する相手方には、利用者等との自主的な紛争解決を依頼するものとする。

解説：利用者等の情報発信や学外でのネットワークを利用した行為について損害賠償

請求があった場合には、法律の専門家と共に対応する必要がある。

プロバイダ責任制限法第 3 条第 1 項により、損害賠償責任の免責を受けられる場合とそうでない場合がある。都立大学事件判決やニフティ事件第二審判決のように、最終的にネットワーク管理者としての損害賠償責任を負わないこととされた事例、ニフティ事件第一審判決や 2 ちゃんねる事件のように損害賠償責任を負うとされた事例が存在するため、慎重な判断が求められる。具体的な削除請求が事前または同時になされている場合には、上記(1)または(3)の手続きに従っていることにより作為義務違反が無いとされ、損害賠償責任を負わないとされる有力な根拠となり得る。

(6) **発信者情報の開示請求**

(ア) **プロバイダ責任制限法第 4 条に基づく場合**

a. **利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって、Web ページ等 1 対多の通信によるものの場合、プロバイダ責任制限法の規定に基づき専門家と共に対処するものとし、発信者が開示に同意している場合を除き、発信者情報の開示請求には慎重に対処するものとする。**

b. **電子メールアドレス等、事前に利用者等から開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼するものとする。**

解説：利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって、Web ページ等 1 対多の通信によるものの場合、プロバイダ責任制限法の規定に基づき専門家と共に対処する必要がある。プロバイダ責任制限法第 4 条に基づく手順としては、概ね下記の通りとなる。

（ア）発信者情報の保有の有無、技術的に特定できるかどうかの判断
開示できる発信者情報がなければその旨を請求者に通知する。

（イ）発信者情報開示請求の根拠の確認と違法性の判断
必ず法律の専門家に相談する。

（ウ）開示について発信者の意見を聞く。
発信者が開示に同意すれば開示してよい。

（エ）発信者情報開示をする法律要件を確実には満たしていないと判断すれば開示を拒否する旨通知する。不開示の判断に故意または重過失がなければ責任を問われないので、少しでも法律要件を満たさない事実があれば、不開示判断をすべきである。

（オ）発信者情報開示の要件に該当することが確実である場合には開示できる。しかし、開示判断を誤った場合には電気通信事業法や有線電気通信法上の通信の秘密侵害罪やプライバシー侵害による損害賠償責任からは免責されないため、慎重な判断を要する。発信者が開示に同意しない場合、特に慎重な判断を要する。

解説：「プロバイダ責任制限法ガイドライン等検討協議会」の発信者情報開示関係ガイドラインを参照。

http://www.telesa.or.jp/consortium/pdf/provider_070226_guideline.pdf

(7) プロバイダ責任制限法に基づかない発信者情報の照会（民事）

利用者等の情報発信や学外でのネットワークを利用した行為について発信者情報の照会があった場合であって、メール等 1 対 1 の通信によるものの場合、下記の手順をとるものとする。なお、警察官、検察官、検察事務官、国税職員、麻薬取締官、弁護士会、裁判所等の法律上照会権限を有する者から照会を受けた場合であっても、原則として発信者情報を開示してはならないので同様の手順となる。

i) 電子メールアドレス等、事前に開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼する。許諾を得ていない発信者情報の開示については発信者の意見を聴く。

ii) 発信者が開示に同意すれば開示してよい。発信者が開示に同意しない場合は、開示を拒絶する。その場合は、通信の秘密及びプライバシーの保護を理由とする。

iii) 発信者情報の保有の有無、技術的に特定できるか否かの判断をし、開示できる発信者情報がなければ、その旨を請求者に通知する。

(8) 強制捜査による発信者情報の差押え、提出命令等

(ア) 部局技術担当者は、発信者情報を含む情報の強制捜査の事前打診があった場合には、発信者情報その他の強制捜査対象の情報を印刷あるいは記憶媒体に出力できるよう準備をしておくものとする。

(イ) 部局総括責任者もしくは対外折衝事務担当者は、部局技術担当者の協力を得て、ネットワークの稼動への影響が最小限になるような方法で強制捜査に協力するものとする。

(ウ) 捜査当局から強制捜査の令状の呈示を受けた場合、令状の記載事項等を確認の上、立会いを求められたときは立会い、押収物があるときは押収目録の交付を受けるものとする。

8. 通常の利用規定違反行為の対応

(1) 発見または通報等による認知と事実確認（情報発信者の特定を含む）

部局技術担当者は発見あるいは通報により利用規定違反の疑いのある行為を知ったときは、すみやかに事実関係を調査し、発信元利用者等を特定した上で部局技術責任者に報告する。

(2) 利用規定違反の該当性判断

部局技術担当者の報告を受けた部局技術責任者は、通常の利用規定違反行為の対応手順にのせることが可能と考える場合は、その旨部局総括責任者に報告し、確認を得るものとする。

部局技術責任者は、技術的事項に関する利用規定違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置が必要であるかどうかを部局総括責任者に報告するものとする。

部局総括責任者は、技術的事項以外の利用規定違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置やアカウントの一時停止等、個別の情報発信の一時停止以上の措置が必要であるかを判断する。判断にあたっては、可能な限り当該行為を行

った者の意見を聴取するものとし、必要に応じて部局情報システム運用委員会の判断を求めるものとする。

(3) 情報発信の一時停止措置
部局技術担当者は、部局総括責任者または部局技術責任者の指示を受けて、利用規定違反に関係する情報発信の一次停止またはアカウントの一時停止措置等を実施する。

(4) 情報発信者に対する通知・注意・警告・当事者間紛争解決要請
部局技術責任者または部局総括責任者は、事案に応じて下記内容を発信者に通知するものとする。
- 利用規定違反の疑いがあること
- アカウントの一時停止措置等の利用を制約する措置を講じた場合は、そのこと、及びその理由・根拠
- 利用規定違反行為の是正、中止の要請
- 利用規定違反行為が是正、中止されなかった場合の効果（情報の削除やアカウントの停止、学内処分等）
- 反論を受け付ける期間とその効果
- 利用者等当事者間の紛争解決の要請

(5) 個別の情報発信またはアカウントの停止と復活

(6) 部局総括責任者または部局技術責任者は、(4) の措置を講じたときは、遅滞無く全学実施責任者にその旨を報告し、その後の利用者等の対応により、必要に応じ部局情報システム運用委員会の承認を得て、下記を実施するものとする。
- 個別の情報発信またはアカウントの停止と復活
- 有効な反論があった場合、または利用行為が是正された場合の個別の情報発信やアカウントの復活
- 利用行為が是正されなかった場合の情報の削除やアカウントの停止、学内処分の開始手続き-
- 利用者等の当事者間の紛争解決着手の有無の確認

9. 学内処分との関係

部局総括責任者は外部クレームの対象となった利用者等、利用規約違反をした利用者等につき、本学懲罰委員会への報告をすることができる。また、本学懲罰委員会による学内処分の検討に際し、アカウント停止処分やその他ネットワークやシステムの利用を制約する処分の必要性の有無について意見を述べることができる。

参考 1　インシデント対応手順にもとづくインシデント報告・承認要領

1. 本書の目的

インシデントが発生した場合、適切な対応によりインシデントの影響が拡大することを防ぐと共に復旧を図ることが必要である。このとき対応を誤ると無用な被害の拡大を招くことが懸念されるため、インシデントの発見から対処、さらには再発防止策の実施にいたる手続きを定め、適切な対処を実施することが必要である。

本書では、インシデントが発生した場合の報告･申請等の手続きに利用する様式を定め、様式を利用した報告・記録・申請・承認の要領を定めることによりＡ大学において必要とされるインシデントへの対処を適切に実施することを目的とする。

2. 本書の対象者

本書は、すべての情報システム運用関係者を対象としている。利用者には、インシデントが発生した場合の部局技術担当者や情報メディアセンター等の通報先を周知・徹底すること。

3. 承認権限者

(1) インシデントに対する対処方針の適否を審査等する者（**「インシデント対処承認権限者」**）は、部局技術責任者、部局総括責任者又は全学実施責任者とする。ただし、インシデントの内容に応じて必要がある場合は、その上位者を対処承認権限者とする。

(2) インシデントの再発防止策の適否を審査等する者（**「インシデント再発防止策承認権限者」**）は、部局総括責任者、全学実施責任者または全学総括責任者とする。

4. 障害等発生から再発防止策実施までの対応

4.1 障害等発生時における全般的な注意事項

(1) 全学実施責任者又は部局総括責任者は、インシデントが発生した場合において、緊急に対処が必要な場合の遅延を防止し、対処を円滑に実施するため、情報システム、組織等の状況を勘案し事前に詳細な手順を定め、関係者に周知すること。

(2) 部局技術担当者（外部からの通報の場合、情報メディアセンターまたは広報部門）は、緊急の対処が必要なインシデントが発生した場合において、報告、審査等の手続が遅延することにより、必要な対処の実施が遅れることのないようにすること。

(3) 緊急の対処が必要な場合は、報告書に代わって口頭での報告、審査等を先行することや、発見者に代わって報告受理者が報告書を記入しインシデントの発見者から内容確認を得ること等により、遅滞なく障害等に対する対処を実施する。ただし、このような場合であっても、速やかに報告書を作成して記録を残すこと。

【事業継続計画（BCP：Business Continuity Plan）が策定されている場合】

(4) 部局技術担当者は、BCP と情報セキュリティ関係規程が定める要求事項において事前に想定されていない不整合が生じた場合、その旨を部局技術責任者を通じて部局総括責任

者（必要により全学実施責任者）に報告し、指示を得ること。

4.2 インシデントの発見報告

(1) 自ら発見、または利用者等からの通報によりインシデントを認知した部局技術担当者（外部からの通報の場合、情報メディアセンターまたは広報部門）は、**別紙１**「インシデント発生・再発防止策に関する報告・申請書（様式○○）」（以下「**インシデント報告書**」）により、インシデントの内容に応じて部局技術責任者または部局総括責任者（「**インシデント報告受理者**」）に報告を行うこと。

(2) インシデントによる被害の拡大が懸念されるため、**インシデント報告受理者**の指示により部局技術担当者が応急措置を実施した場合には、すみやかにインシデント報告書に応急措置の内容を記録すること。

(3) **インシデント報告受理者**は、対処を実施する者を選び、対処の指示を与えること。なお、口頭により報告を受けた場合は、インシデント報告書のインシデントの詳細についてすみやかに記録させること。

(4) **インシデント報告受理者**は、報告された内容を確認し、必要に応じて abuse@example.ac.jp等の連絡網を活用し、部局総括責任者、全学実施責任者及び関係部署等に通知させること。また、通知先をインシデント報告書に記録させること。

(5) 全学実施責任者は、危機管理、利用者の意識向上に資するインシデント及びその対処の事例について、情報セキュリティ対策上支障のない範囲で学内の広報に努めること。

4.3 インシデントの対処

インシデントの対処を実施する者は、インシデントの対処方針を提案し、インシデント報告書によりインシデントの内容に応じて**対処承認権限者**の承認を得ること。ただし、部局総括責任者または全学実施責任者が定めた詳細な手順において、対処方針が規定されている場合には、承認を受けたものとみなす。なお、対処方針を決定する際には、必要に応じて通知先の関係部署と連携すること。

4.4 インシデントの再発防止

インシデントの対処を実施する者は、インシデントが発生する前の状態に復旧するだけでは再発するおそれがあると考える場合には、速やかに根本的な再発防止策を提案し、インシデントの内容に応じて、**再発防止策承認権限者**の承認を受け、記録すること。

別紙1

【機密性2】複製要許可

様式○○

インシデント発生・再発防止策に関する報告・申請書

インシデント管理番号:		受理者確認	□部局技術責任者　年　月　日 □部局総括責任者 □全学実施責任者 □その他　(氏名・役職・連絡先)
発見・通報日	年　月　日		
被害の範囲	□(　　)部局内 (部署名　　) □全学 □学外 (相手方名称・サイト)		
被害の有無：□有り　□無し（未遂）		発見者・通報者及び認知経路・発見方法	学外 (氏名、所属、連絡先*1) □情報メディアセンター 経由 □広報部門／学外窓口 経由 申告・請求内容
被害を受けた期間	年　月　日～　年　月　日		
被害対象	関連システム／ネットワークの名称・概要		学内 (氏名、所属、連絡先*1) □情報メディアセンター／非常時窓口 □部局技術担当者 □その他
機種	□IBM PC(含む互換機)　台 □Mac　台 □その他 (機種名:　　) 台		発見方法 □目視により発見 □アンチウィルスソフトで発見 (ソフト名:　　) □ツール類のログ (ツール名称:　　) □ その他疑いを持った状況
OS	□Windows-□3.1 □95 □98 □ME □NT □2000 □XP □Vista □Mac □Unix(名称・バージョン　　) □その他(　　)		
利用目的	□学術研究 □事務 □情報公開(Web等) □その他(　　)		
情報種別	□個人情報 (　　) □その他　要保護レベル: (　　)		
権利侵害・違法行為	□名誉・信用・プライバシー □著作権 □その他知的財産 (　　) □営業秘密・通信の秘密 □営業・業務妨害 □その他の犯罪・違法行為 (　　)	通知先	(氏名、所属、連絡先*1) □abuse@example.ac.jp □その他のML(　　@example.ac.jp) □情報メディアセンター／非常時窓口 □広報部門／学外窓口 □部局技術責任者 □部局総括責任者 □全学実施責任者 □全学総括責任者／非常時対策本部 □法律専門家 □その他 (保護者、警察等)
インシデント種別	□対外的 or □対内的 □物理的インシデント □セキュリティインシデント □コンテンツインシデント □その他利用規程違反 (違反内容　　)		
感染／攻撃経路・手口（推定）	実施していたセキュリティ対策 (　　) □国内 □海外 □不明 □電子メール □ダウンロードファイル □WEBサイト閲覧 □外部からの媒体、 □パスワード盗用 □セキュリティホール悪用・設定不備 (ソフト名・バージョン　　) □その他 (　　)	物理的被害状況	
被害状況（セキュリティ）	攻撃手法・ウイルス名称（不明な場合は症状） 攻撃（未遂）の種別： □ファイル／データ奪取、改竄、消去、破壊 □不正プログラムの埋め込み （トロイの木馬、ボット、バックドアなど） □権限取得　□踏み台 □サービス妨害 □資源利用（ファイル、ＣＰＵ使用） □メールの不正中継 □メールアドレス詐称 □その他（　　）	応急措置／日時	年　月　日　時　分 □パッチ・サービスパック適用 □アンチウイルスソフトで駆除または削除 (社名:　ソフト名:　　) □フリーの専用駆除ソフトで駆除 (ソフト名、またはダウンロード先のＵＲＬ等) □ファイル(メール)の削除 □初期化 □情報発信関連サーバ・BBS等の一時停止 □権利侵害・違法コンテンツ送信の一時停止 □権利侵害・違法コンテンツ送信の一時停止 □その他 (　　) ・回復に要した人日-(　)人・(　)日 (0.5日単位で記述)

A3103 **インシデント対応手順**

インシデントへの対処方針		対処方針の承認権限者承認*1 年 月 日
対処実施者	(役割、氏名、所属、日付、連絡先)	(役割、氏名、所属、連絡先)
対処区分	□緊急 □非常時対策本部の設置 □通常 □再現待ち □通常の利用規定違反	□部局技術責任者 □全学実施責任者 □全学総括責任者
方針の詳細	□情報機器・システム復旧計画 (内容:)	
	□学外クレームへの応答 □対外クレームの実施 (内容:) □個別システムの停止／ネットワークからの分離 □特定利用者アカウントの停止 □発信者である利用者への通知、注意、警告、当事者間紛争解決要請	

インシデントへの対処結果		対処結果の審査者確認*1 年 月 日
原因		(役割、氏名、所属、連絡先) □部局技術責任者 □全学実施責任者 □全学総括責任者
技術的対処	□パッチ・サービスパック適用 (パッチ・サービスパックの全てを列挙) □ソフトウェア・プログラム設定変更 (ソフトウエア・プログラムの名称、設定作業内容を明記) □ソフトウェア・プログラム更新・削除 (改竄されたものを回復した場合も含む。) (ソフトウエア・プログラムの名称を明記) □機器撤去 (永久使用しない場合のみ) □その他 (以下に詳細を明記)	
事務的対処	□利用者の懲罰委員会への報告 □外部機関への連絡・通報・届け出 (警察、JPCERT,IPA等) □民事訴訟他の民事手続きの提起・応訴等	

インシデント再発防止策		インシデント報告受理者確認 年 月 日
実施予定日 年 月 日		再発防止策許可者承認 年 月 日
実施者	(役割、氏名、所属、連絡先) □部局技術担当者 □部局技術責任者 □部局総括責任者 □全学実施責任者	(役割、氏名、所属、連絡先) □部局技術責任者 □部局総括責任者 □全学実施責任者 □全学総括責任者
インシデント再発防止策の詳細*1		

【報告・申請経路】インシデントの発見者→受理者 (インシデントの内容により部局技術責任者、部局総括責任者又は全学実施責任者がが受理) →対処実施者→対処方針の承認権限者者 (インシデントの内容により必要に応じて受理者より上位の承認権限者に回付) →対処結果の審査者 (対処方針を与えた者と承認した者と同一) →再発防止策実施者→インシデント報告実施者→再発防止策許可者→全学総括責任者

【注1】緊急の対処が必要なインシデントが発生した場合において、報告、審査等の手続により必要な対処が遅延することがないように留意すること。

【注2】記入欄に全てを書き込むことができない場合、適宜添付資料として通し番号を付すこと。

*1：複数の該当者がいる場合は、それぞれ記入する。

*2：再発防止の対処を暫定的な対処から段階的に実施する場合は、途中の段階における対処についても記入する。

参考 2　インシデント対応手順による学外クレーム対応時の留意点

1. コンテンツインシデントの権利者や被害者への返信の要否

学外クレームがあった際、A3103に基づき調査の上、対処するが、学外クレームを発した権利者や被害者への返信は不要な場合が多いことに留意する。

また、違法情報についての第三者からの指摘については、法的責任の観点からは、返信は不要である。ただし、地域コミュニティを無視している、等の風評を立てられることを回避するため、通報への謝辞（ご指摘ありがとう、学内ルールに基づき対処します、等）のみ記して返答するほうが良い場合もある。

権利者や被害者への返信が必要か望ましい場合は、以下のとおりのみ。。

(1) 法律で義務とされている場合
- プロバイダ責任制限法第4条の発信者情報開示請求の要件を満たす場合。

(2) 法律で義務とされていないが望ましい場合
- 発信者情報開示関係ガイドラインに基づき不開示決定を通知する場合
- 削除請求等のクレームに対して利用者等から有効と思われる反論があった場合
- クレーム者と利用者等との当事者間解決を依頼するのが適当な場合

(3) 法律専門家の判断による場合
- 対処結果を報告する等、連絡することで、その後の交渉ポジションを不利にしないために有用な場合。（海外からの請求の場合、通常はあてはまらない。）

2. 海外の権利者、被害者からのクレームの特徴と、対処時の留意点

(1) そもそも、正式な法的請求といえないものが多い。

(2) 海外の権利者・被害者からの場合、正式な法的請求をする場合は、弁護士名での書面で送付されるとのが普通

(3) 少なくとも海外からの訴状はメールでは送られてこない。

(4) 米国のDigital Milemium Copyright Act（デジタルミレニアム著作権法。以下、「DMCA」という。）に基づく削除請求は、様式や内容が定められており、電子署名のないメールでは様式を満たさない。

（参考）

http://en.wikipedia.org/wiki/Online_Copyright_Infringement_Liability_Limitation_Act

http://www.utsystem.edu/OGC/IntellectualProperty/dmcaisp.htm#top

http://www.chillingeffects.org/dmca512/faq.cgi

(5) DMCAに基づく削除請求にもとづき削除することにより、免責を受けられるが、返事するのは義務ではない。

(6) DMCAにもとづく旨、明記しているかどうかにかかわりなく、著作権侵害通知メールのほとんどは、機械的に発見した結果をとりこんで自動的に処理しているもので、まじめに読んだ相手方がさっさと削除等して、権利侵害が是正されれば儲け物というスタンス。削除結果等を回答することは実は期待されていない。

(7) なお、DMCAでは、アクセスプロバイダーはエンドユーザの（P2P）通信については免責。ただし、常習の権利侵害者の接続を切断する方針を実施する義務があるので、P2Pを利用した著作権侵害についての警告が累積した場合には、米国のISPは回線を切断している、とのこと。
(8) 削除等の対処がされない場合は、権利者、被害者側は、それを記録し、正式な要求をすることになった場合の有力な証拠の一つとすることになるが、国際的な裁判はコスト面でも準拠法や裁判管轄等の法的側面でも容易ではないので、これまでも裁判例は無い。
(9) 万が一、訴訟され反証せざるを得ない局面に備え、対利用者に対する警告、利用停止等の措置の記録はきちんと保存しておくほうが良い。

3. （特に海外からのクレームにおいて）返信をする場合のポイント

(1) 謝らない。故意の権利侵害を自認したことになる。
(2) 聞かれていないことには回答しない。
(3) 事実を正確に表現する。揚げ足をとられないように。

4. セキュリティインシデントの連絡への対処

(1) CERTや大学の機関からの連絡は、揚げ足をとるつもりは無いはずであるが、返信する場合は正確な表現ですべき。
(2) 法的権利を持っているわけではないが、ブラックリストに登録する権限をもった機関からの連絡は注意を要する。返信をするかどうかは別として、対処しない場合は、対象となるIPアドレスやホストをブラックリストに登録してしまうため、関連するサービス全体が巻き添えを食う恐れがある。（掲示板のアクセス制限も同様。同じアクセスポイントからの全アクセスを制限してしまうので、掲示板へのアクセスや書き込みを許す場合は、原因を取り除いた上で、アクセス制限の解除依頼をせざるを得ない。）
(3) 企業や個人が自営するメールサーバや、掲示板に対するSPAMや荒らし等の攻撃についての苦情も取扱いに注意を要するが、大学として故意にSPAMや業務妨害を行っていない限り、法的手段（訴訟や刑事告訴等）に訴えると脅されても攻撃の原因を取り除くことに集中し、淡々と対処してよい。

A3104 情報格付け取扱手順

1. 目的

情報システムで取り扱う情報は格付けされ、格付けに応じて適切に取り扱う必要がある。取扱いが不適切なため、機密性が求められる情報の漏えい、完全性が求められる情報の改ざん等が生じた場合には、大学活動の停止や社会的信用の失墜の要因となる可能性もある。

本書は、このようなリスクを軽減するため、教職員等が情報を適切に取り扱うために必要な事項を定めることを目的とする。

2. 本書の対象

本書は、情報を取り扱うすべての教職員等を対象とする。

3. 定義

本書における用語の定義は次のとおりである。

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

4. 情報の取扱いに関する全般的な注意事項

4.1 大学活動の遂行以外の目的での情報の作成、入手及び利用禁止

教職員等は、大学活動の遂行以外の目的で、情報の作成、入手又は利用を行わないよう努めること。

4.2 情報の格付け及び取扱制限に応じた取扱い

(1) 教職員等は、作成又は入手した情報について、格付け及び取扱制限を指定し、当該指定の結果を電磁的記録であるか書面であるかに応じて明示等すること。

(2) 教職員等は、取り扱う情報に明示等された格付けに従って、当該情報を本書が定めるとおりに取り扱うこと。格付けに加えて、取扱制限の明示等がなされている場合には、当該取扱制限の指示内容に従って当該情報を取り扱うこと。

5. 情報の格付け

5.1 格付け及び取扱制限の指定

教職員等は、情報の格付け及び取扱制限について、「付録A： 格付け及び取扱制限の判断基準」に基づき、格付け及び取扱制限の指定を行うこと。ただし、「付録A： 格付け及び取扱制限の判断基準」で規定されていない情報については、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限

の定義に基づき、要件に過不足が生じないように注意した上でその決定（取扱制限については必要性の有無を含む。）をし、決定した格付け及び取扱制限に基づき、その指定を行うこと。

5.2 格付け及び取扱制限の明示手順

(1) **教職員等は、書面の場合には、格付け及び取扱制限を各ページに明記すること。**

(2) **教職員等は、電磁的記録の場合には、参照、編集時に常に格付け及び取扱制限が分かるように、また印刷時に各ページに格付け及び取扱制限が印刷されるように、文章のヘッダ等において各ページに明記すること。ただし、電磁的記録の参照、編集等に利用するソフトウェアの制限等により、各ページに明記できない場合には、文章の先頭ページに明記すること。**

【格付け及び取扱制限をファイル名にも明記する場合】

(3) **教職員等は、電磁的記録の場合には、当該ファイルの内容を参照せずとも格付け及び取扱制限が分かるように、ファイル名に格付け及び取扱制限を明記すること。**

(4) **教職員等は、当該情報を取り扱う教職員等に格付け又は取扱制限の認識が周知徹底されているため、格付け又は取扱制限を明記する必要がないと情報システム運用委員会において定められた情報に関しては、格付け又は取扱制限を書面又は電磁的記録に明記する必要はない。なお、明記が不要な情報については、「付録B： 格付け及び取扱制限の明記不要な情報一覧」を参照すること。**

5.3 格付け及び取扱制限の変更手順

5.3.1 格付け及び取扱制限の再指定

(1) **教職員等は、元の情報への修正、追加、削除のいずれかにより、他者が指定した情報の格付け又は取扱制限を再指定する必要があると思料する場合には、「5.1 格付け及び取扱制限の指定」に従って、新たな格付け又は取扱制限を指定すること。**

【再指定した場合の指定者をこれを行った教職員等とする場合】

(2) **教職員等は、情報の格付け又は取扱制限を再指定した場合には、指定者の責任として、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け又は取扱制限とならないように努めること。**

5.3.2 格付け及び取扱制限の見直し

(1) **教職員等は、元の情報への修正、追加、削除のいずれもないが、元の情報の格付け又は取扱制限がその時点で不適当と考えるため、他者が指定した情報の格付け又は取扱制限そのものを見直す必要があると思料する場合には、その指定者又は同人が所属する上司に相談すること。**

(2) **被相談者は、指定した情報の格付け又は取扱制限の見直しの必要性を検討し、必要があると認めた場合には、当該情報に対して新たな格付け又は取扱制限を「5.1 格付け及**

び取扱制限の指定」に従って指定すること。ただし、「付録A： 格付け及び取扱制限の判断基準」に規定されていない情報の場合には、「5.1 格付け及び取扱制限の指定」に従って決定及び指定すること。

(3) 被相談者は、指定した情報の格付け又は取扱制限の見直しに際して、「付録A： 格付け及び取扱制限の判断基準」において決定されている情報の格付け又は取扱制限の見直しが必要と思料される場合には、上司に報告すること。

【見直した場合の指定者を元の格付け等を行った教職員等とする場合】

(4) 被相談者は、情報の格付け又は取扱制限を見直した場合には、指定者の責任として、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け及び取扱制限とならないように努めること。

6. 情報の作成・入手

6.1 情報を作成・入手する場合の注意事項

教職員等は、大学活動の遂行以外の目的で、情報を作成又は入手しないよう努めること。

6.2 情報を新規に作成した場合の格付け方法

教職員等は、情報を新規に作成した場合には、「5. 情報の格付け」に従って当該情報の格付け及び取扱制限を指定し、これを情報に明示等すること。

6.3 格付けされた情報を引用して情報を作成した場合の格付け方法

教職員等は、既に格付けされた情報を引用して情報を作成する場合には、引用した情報の格付け及び取扱制限と、「5. 情報の格付け」に従って指定した新規に作成した情報の格付け及び取扱制限とを比較した上で、より上位の格付けを行い、双方の取扱制限を併せた新たな取扱制限とし、これを情報に明示等すること。

6.4 格付け及び取扱制限が明示等されている情報を入手した場合の格付け方法

(1) 教職員等は、格付け又は取扱制限が明示等されている情報を入手した場合には、明示等されている格付け又は取扱制限を継承すること。

(2) 教職員等は、格付け又は取扱制限が明示等されている情報を入手した場合で、当該情報の継承すべき格付け又は取扱制限を変更する必要性があると思料するときは、「5 情報の格付け」に従って格付けを変更すること。

6.5 格付け及び取扱制限が明示等されていない情報を入手した場合の格付け方法

教職員等は、格付け又は取扱制限が明示等されていない情報を入手した場合には、「5 情報の格付け」に従って当該情報の格付け又は取扱制限を指定し、これを情報に明示等すること。

7. 情報の利用

7.1 情報の利用における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、情報を利用しないよう努めること。

(2) 教職員等は、取り扱う情報に明示等された格付けに従って、当該情報を取り扱うこと。格付けに加えて、取扱制限の明示等がなされている場合には、当該取扱制限の指示内容に従って当該情報を取り扱うこと。

7.2 情報を利用する場合の保護方法

(1) 教職員等は、要保護情報が保存された外部記録媒体を利用する場合には、紛失及び盗難から保護するために、以下の措置を講ずること。

- 外部記録媒体の利用中に適切な保護が行えない場合には、当該外部記録媒体を放置せずに、施錠可能な保管庫、棚等に保管する。
- 外部記録媒体の利用が終了した場合には、当該外部記録媒体を机上、端末のドライブ内等に放置せずに、所定の場所に保管する。

(2) 教職員等は、要機密情報が記載された書面又は重要な設計書を利用する場合には、紛失及び盗難から保護するために、以下の措置を講ずること。

- 書面の利用中に適切な保護が行えない場合には、当該書面を放置せずに、施錠可能な保管庫、棚等に保管する。
- 書面の利用が終了した場合には、当該書面を机上等に放置せずに、所定の場所に保管する。
- プリンタ等で書面に印刷した場合には、出力トレイに当該書面を放置せずに、速やかに回収する。

(3) 教職員等は、機密性３情報が記載された書面又はこれが含まれる電磁的記録を必要以上に複製しないこと。

(4) 教職員等は、要機密情報が記載された書面又はこれが含まれる電磁的記録を必要以上に配付しないこと。

【書面に印刷された機密性３情報の所在を明らかにする場合（強化遵守事項）】

(5) 教職員等は、書面に印刷された機密性３情報には、一連番号を付し、その所在を[機密性３情報印刷書面管理表]の様式で明らかにしておくこと。

【機密性３情報に機密性３情報として取り扱う期間を明記する場合（強化遵守事項）】

(6) 教職員等は、機密性３情報には、機密性３情報として取り扱う期間を明記すること。

(7) 教職員等は、機密性３情報の格付けを下げた場合には、その旨を関係する教職員に通知するとともに、[機密性３情報印刷書面管理表]に記録すること。

8. 情報の保存・管理

8.1 情報の保存における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、要保護情報を電子計算機又は外部記録媒体に保存しないこと。

(2) 教職員等は、電子計算機又は外部記録媒体に保存された要保護情報について、保存の理由となった業務事務の遂行目的が達成された等、保存する理由が滅失した場合には、速やかに当該情報を削除すること。

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

(4) 教職員等は、保存期間が満了した情報に関して、保存期間を延長する必要がない場合は、速やかに当該情報を消去すること。

(5) 教職員等は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、滅失、消失又は改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、バックアップ又は複写を取得すること。ただし、部局技術担当者によりバックアップされているファイルサーバに保存している等、既にバックアップが行われている場合は、この限りでない。

(6) 教職員等は、バックアップ若しくは複写された情報又は当該情報が保存された電磁的記録媒体若しくは記載された書面を、バックアップ又は複写元の情報と同等に管理すること。

8.2 電子計算機へ情報を保存する場合の保護方法

(1) 教職員等は、要保護情報を電子計算機に保存する場合には、他の者が当該情報を参照、変更、削除等できないようにアクセス制御すること。

(2) 教職員等は、機密性３情報を端末に保存する場合には、アクセス制御に加え、当該情報を暗号化すること。

(3) 教職員等は、要保全情報を端末に保存する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与すること。

8.3 外部記録媒体へ情報を保存する場合の保護方法

(1) 教職員等は、要機密情報を外部記録媒体に保存する場合には、当該情報を暗号化すること。ただし、機密性２情報の場合には、パスワードを用いた保護で代替することができる。

(2) 教職員等は、要保全情報を外部記録媒体に保存する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与すること。

8.4 要保護情報が保存された外部記録媒体並びに記載された書面及び重要な設計書の保管方法

教職員等は、要保護情報が保存された外部記録媒体又は記載された書面若しくは重要な設計書を保管する場合には、施錠管理された保管庫、棚等に保管すること。

9. 情報の公表・提供

9.1 情報の公表・提供における注意事項

(1) 教職員等は、大学活動の遂行以外の目的で、情報を公表・提供しないよう努めること。

(2) 教職員等は、要機密情報を提供する場合には、「9.2 情報の公表・提供に関する手続」の手続に従い、提供する情報及び提供先を必要最小限にとどめること。

(3) 教職員等は、要保護情報を提供するために当該情報を移送する場合には、「11. 情報の移送」に従って移送すること。

(4) 電磁的記録には、プロパティ等に作成者名、組織名、作成履歴等の付加情報が含まれている可能性があり、当該付加情報から情報が漏えいする場合がある。教職員等は、電磁的記録を公表又は提供する場合には、当該情報の付加情報に不要な情報が含まれていないか確認し、不用意な情報漏えいを防止すること。

(5) 教職員等は、格付け及び取扱制限の明記が不要とされている情報を含む書面又は電磁的記録の提供については、提供先においても格付け及び取扱制限に応じた取扱いを確保するため、提供する前に、明記が不要とされている情報の格付け及び取扱制限を当該書面又は電磁的記録に明記すること。

(6) 教職員等は、要保護情報又は重要な設計書を学外の者に提供する場合には、提供先において、当該情報が、本学の付した情報の機密性の格付けに応じて適切に取り扱われるための措置として、取扱いに関する留意事項の伝達、適切な管理のための取決め等の措置を講ずること。

9.2 情報の公表・提供に関する手続

(1) 教職員等は、保有する情報を公表する場合には、当該情報が機密性１情報に格付けされるものであることを確認すること。

(2) 教職員等は、機密性１情報を公表する場合には、当該情報が法律の規定等で公表が禁じられていないことを確認すること。

(3) 教職員等は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を本学外の者に提供する場合には、[機密性３情報移送・提供許可申請書]の様式で上司に申請し、許可を得ること。

(4) 教職員等は、機密性２情報であって完全性１情報かつ可用性１情報である電磁的記録又は機密性２情報を記載した書面を本学外の者に提供する場合には、当該情報が機密性２情報に格付けされたものであることを確認し、秘密であると判断した情報を削除した

上で、提供すると同時に、上司に届け出ること。メールに添付して提供する場合は、上司にBCC:で送信しておくなどの方法が考えられる。ただし、上司が届出を要しないと定めた提供については、この限りでない。

10. 情報の持出し

10.1 情報の持出しにおける注意事項

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

(2) 教職員等は、大学活動の遂行の目的で、要保護情報を学外に持ち出す場合には、「10.2 情報の持出しに関する手続」の手続に従い、持ち出す情報及び持出先を必要最小限にとどめること。

(3) 教職員等は、要保護情報の持出しのため、当該情報を移送する場合には、「11. 情報の移送」に従って移送すること。

(4) 教職員等は、持出先においても学内と同様に情報を取り扱うこと。

10.2 情報の持出しに関する手続

(1) 教職員等は、大学活動の遂行の目的で、大学支給以外の情報システムにおける情報処理又は学外での情報処理を行うために、電子計算機、外部記録媒体、書面等で要保護情報（機密性２情報を除く。）を学外に持ち出す場合には、[要保護情報（機密性２情報を除く。）持出し許可申請書]の様式で部局技術責任者又は上司の許可を得ること。

(2) 教職員等は、要保護情報（機密性２情報を除く。）の持出しによる大学支給以外の情報システムにおける情報処理又は学外での情報処理が終了した場合には、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

11. 情報の移送

11.1 情報の移送に関する手続

教職員等は、機密性３情報、完全性２情報若しくは可用性２情報又は重要な設計書を移送する場合には、[機密性３情報移送・提供許可申請書]の様式で上司に申請し、許可を得ること。当該申請において、移送方法（送信又は運搬のいずれか）及び移送手段（電子メールの添付、郵送、職員による携行等）を届け出ること。

11.2 移送方法・手段の選択方法

情報の格付け、種類等に応じて移送方法・手段を選択する。

11.3 書面及び外部記録媒体を運搬する場合の保護方法

(1) 教職員等は、要機密情報が記載された書面又は保存された外部記録媒体を建屋外に運搬する場合には、安全確保のため、以下の措置を講ずること。

- 外見から機密性の高い情報であることが分からないようにする。
- 郵便、信書便等の場合には、親展で送付する。
- 携行の場合には、封筒、書類鞄等に収め、当該封筒、書類鞄等の盗難、置き忘れ等に注意する。

【機密性３情報の暗号化を必須とする場合】

(2) 教職員等は、要機密情報が保存された外部記録媒体を建屋外に運搬する場合には、書面又は保存された外部記録媒体を建屋外に運搬する場合の措置に加え、以下の方法を用いて当該記録媒体に保存された情報を保護すること。ただし、当該情報が機密性２情報の場合には、パスワードを用いた保護で代替することができる。

- 情報の暗号化

【秘密分散を利用する場合（強化遵守事項）】

- 秘密分散

(3) 教職員等は、要機密情報が記載された書面又は保存された外部記録媒体を建屋内で運搬する場合には、建屋外に運搬する場合の措置に準じて保護することが望ましい。

(4) 教職員等は、要保全情報が保存された外部記録媒体を建屋外に運搬する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与することが望ましい。

(5) 教職員は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めた時は、情報のバックアップを取得すること。

(6) 教職員は、要保全情報である電磁的記録を移送する場合には、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送するなどの措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。

11.4 電磁的記録を送信する場合の保護方法

【機密性３情報の暗号化を必須とする場合】

(1) 教職員等は、要機密情報である電磁的記録を学外に送信する場合には、以下の方法を用いて当該情報を保護すること。ただし、当該情報が機密性２情報の場合には、パスワードを用いた保護で代替することができる。

- 通信路の暗号化
- 電磁的記録の暗号化

【秘密分散を利用する場合（強化遵守事項）】

- 秘密分散

(2) 教職員等は、要機密情報である電磁的記録を学内に送信する場合には、学外に送信す

る場合の措置に準じて保護することが望ましい。

(3) 教職員等は、要保全情報である電磁的記録を　学外に送信する場合で、改ざんされるおそれが大きく、業務の遂行に影響を与える可能性が高いと判断されるときは、保存されている当該情報に電子署名を付与することが望ましい。

(4) 教職員は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めた時は、情報のバックアップを取得すること。

(5) 教職員は、要保全情報である電磁的記録を移送する場合には、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送するなどの措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。

12. 情報の消去

12.1 外部記録媒体及び書面の廃棄方法

【機密文書等の回収及び廃棄を外部委託している場合】

(1) 教職員等は、情報が保存された外部記録媒体を廃棄する場合には、専用の回収ボックスに投入すること。

(2) 教職員等は、要機密情報が記録された書面を廃棄する場合には、専用の回収ボックスに投入すること。

【細断機を利用する場合】

(1) 教職員等は、情報が保存された外部記録媒体を廃棄する場合には、細断機を利用して細断すること。

(2) 教職員等は、要機密情報が記録された書面を廃棄する場合には、細断機を利用して細断すること。

【外部記録媒体を教職員等が自身で処理する場合】

教職員等は、情報が保存された外部記録媒体を廃棄する場合には、以下のように外部記録媒体の物理的に破壊する等し、読取装置を利用して当該外部記録媒体から情報が読み出せないことを確認すること。ただし、物理的な破壊等により読取装置が利用できない場合に限り、確認を省くことができる。

- FD等の磁気媒体の場合には、当該媒体を折り曲げる、切断する等して情報を記録している内部の円盤を破壊する。
- CD-R/RW、DVD-R/RW等の光学媒体の場合には、カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する。

12.2 外部記録媒体を他者へ渡す場合の情報の消去方法

教職員等は、使用済みの外部記録媒体を他者へ渡す場合で、当該外部記録媒体に記録さ

れている情報を提供する必要がないときは、データ消去ソフトウェア又はデータ消去装置を用いて、当該外部記録媒体に保存されている情報を復元が困難な状態にし、残留する情報を最小限に保つこと。

【利用環境等により適宜情報を消去する必要がある場合（強化遵守事項）】

12.3 利用環境等の理由により適宜情報の消去が求められる場合の消去方法

教職員等は、外部記録媒体について、無人の執務室で利用される環境等、必要があると認められる場合は、適宜、データ消去ソフトウェアを用いて、当該外部記録媒体の要機密情報を復元が困難な状態にし、残留する要機密情報を最小限に保つこと。

13. 本書に関する相談窓口

(1) 教職員等は、緊急時の対応又は本書の内容を超えた対応が必要とされる場合には、部局技術責任者に相談し、指示を受けること。

(2) 教職員等は、本書の内容について不明な点又は質問がある場合には、部局技術担当者に連絡し、回答を得ること。

付録A： 格付け及び取扱制限の判断基準

格付けの区分

【ポリシーの格付け分類に準拠する場合】

機密性についての情報の格付け

格付けの区分	分類の基準
機密性３情報	本学情報システムで取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性２情報	本学情報システムで取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報
機密性１情報	機密性２情報又は機密性３情報以外の情報

完全性についての情報の格付け

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

可用性についての情報の格付け

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

取扱制限の種類

機密性についての取扱制限

取扱制限の種類	概要
○○禁止	○○で指定した行為を禁止する必要がある場合に指定する。 例）複製禁止、配付禁止、印刷禁止、転送禁止、転記禁止、再利用禁止、送信禁止
○○要許可	○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。 例）複製要許可、配付要許可、印刷要許可、転送要許可、転記要許可、再利用要許可、送信要許可
○○必須	○○で指定した行為を必須とする必要がある場合に指定する。また、必須とする際の条件を設定する必要がある場合には、当該条件を付与する。 例）暗号化必須、通信時暗号化必須
○○限り	提供する範囲を○○に限定する必要がある場合に指定する。 例）教職員限り、課内限り

完全性についての取扱制限

取扱制限の種類	概要
○○まで保存	○○の期日まで保存する必要がある場合に指定する。 例）平成１８年７月３１日まで保存
○○において保存	完全性が確保可能な○○の場所において保存する必要がある場合に指定する。 例）共有ファイルサーバにおいて保存
保存期間満了後要廃棄	指定した保存期日を越えた際に廃棄する必要がある場合に指定する。
○○禁止	○○で指定した行為を禁止する必要がある場合に指定する。 例）書換禁止、削除禁止
○○要許可	○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。 例）書換要許可、削除要許可

可用性についての取扱制限

取扱制限の種類	概要
○○以内復旧	復旧に要する時間として許容可能な時間を設定する必要がある場合に指定する。 例）１時間以内復旧
○○において保存	可用性が確保可能な○○の場所において保存する必要がある場合に指定する。 例）年度内保存文書用共有ファイルサーバにおいて保存

格付け及び取扱制限の判断例

情報類型	格付け	取扱制限
○○資料	機密性２情報 完全性２情報 可用性２情報	複製禁止、配付禁止
△△資料	機密性２情報 完全性２情報 可用性２情報	暗号化必須
□□資料	機密性２情報 完全性２情報 可用性２情報	教職員限り
●●資料	機密性１情報 完全性２情報 可用性２情報	３日以内復旧、バックアップ必須
▲▲報告書	機密性２情報 完全性２情報 可用性２情報	５年間保存
■■情報	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ａシステムにおいて保存、書換禁止、保存期間満了後要廃棄
…	…	…

【手順書策定者への補足説明】

※ 取扱制限の種類については、情報を取り扱う他の者が制限すべき事項を理解できる形式であれば、例示したものである必要はない。

※ 判断例の構成としては、文書の種類に基づくもの、特定文書に対応させたもの、本学活動の内容に基づくもの等があるため、適宜の方法を採用する。

付録B： 格付け及び取扱制限の明記不要な情報一覧

教職員等に当該情報に関する格付け及び取扱制限の認識が周知徹底されているため、格付け及び取扱制限を明記する必要がないと定められた情報は以下のとおりである。

- ○○資料
- ■■情報
- …

様式X　　別紙4－2

決裁欄
承認日：

機密性3情報移送・提供許可申請書

殿

［申請日］＿＿＿＿＿＿＿＿

［所属］＿＿＿＿＿＿＿＿

［氏名］＿＿＿＿＿＿＿＿

［連絡先］＿＿＿＿＿＿＿＿

［区分（複数選択可）］

□ 移送
□ 提供

移送にかかわる情報

移送日		移送先	(所属)　(氏名)
情報の名称			
移送方法	□ 送信 □ 運搬	移送手段	
移送目的			

保護対策	はい	いいえ	該当なし
・書面を移送する場合に、安全確保を行う。	□	□	□
・電磁的記録を移送する場合に、暗号化を行う。	□	□	□
・電磁的記録を移送する場合に、秘密分散を行う。	□	□	□

提供にかかわる情報（移送と同じ場合は「同上」と記入。）

提供日		提供先	(所属)　(氏名)
情報の名称			
提供目的			

保護対策	はい	いいえ	該当なし
・電磁的記録の付加情報を削除する。	□	□	□

様式X　　別紙2－2

機密性3情報印刷書面管理表

［記入日］＿＿＿＿＿＿＿＿

［所属］＿＿＿＿＿＿＿＿

［氏名］＿＿＿＿＿＿＿＿

［連絡先］＿＿＿＿＿＿＿＿

［区分］
□　印刷
□　入手

書面にかかわる情報

［印刷・入手日］＿＿＿＿＿＿＿＿

［情報名称］＿＿＿＿＿＿＿＿

［部数］＿＿＿＿＿＿＿＿

所在にかかわる情報（印刷・入手した部数に応じて記載する。）

番号	所在	管理者	廃棄	廃棄者
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	
			□	

A3105 情報システム運用リスク評価手順

情報資産の管理者が行うリスク評価は、次に掲げる方法によるものとする。

(1) 情報資産の洗い出し

「リスク分析票」(添付１)の中項目ごとに関係する情報資産をすべて洗い出す。例えば、「6.6.1 コンピュータの取外し可能な付属媒体」の場合、テープ、ディスク、カセット、MO、USB 媒体等、保有するすべての可搬媒体が該当する。これら情報資産を一つのセルに一つずつ記入する[1]。

(2) 脆弱性分析

「リスク分析票」(添付１)の安全対策項目と現状を比較し、脆弱性を数値で記入する。このとき、必要に応じ技術担当者の意見を取り入れ、現状を正確に把握する。脆弱性をあらわす数値は以下のとおりである。なお、未実施または即実施のものについては現在の状況を備考欄にメモしておくとよい。

数値	意味	判断基準
1	実施済み	関連のドキュメントが整理され、それに則った運用がなされている。
2	一部実施	関連のドキュメントが不足しているか、または運用が正確に行われていない。
3	未実施	ドキュメントもなく、運用もされていない。

(3) 資産価値判断

上記で洗い出した情報資産を機密性 (C)、完全性(I)、可用性(A)の観点で情報資産をリスク判断し、数値を記入する。判断基準は、これらの性格が損なわれたときに、その業務継続性に与える影響度から判断する。

・機密性(C)

３：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が著しく下がる。その結果、利用者や社会、本学情報システムの継続性など広範囲に影響が出る。

２：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が下がる。その結果、利用者や社会、本学情報システムの継続性など一部に影響が出る。

１：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が下がる危険性が低い。また、利用者や社会、本学情報システムの継続性などに影響は出ない。

・完全性(I)

[1] リスク分析票の安全対策項目は次を参照されたい。
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01_2.xls

３：情報資産に対し、基準となる安全性が確保されなかった場合、その情報の正確性または業務処理の正確な運用ができなくなる。その結果、利用者や社会、本学情報システムの継続性など広範囲に影響が出る。

２：情報資産に対し、基準となる安全性が確保されなかった場合、その情報の正確性または業務処理の正確な運用ができなくなる。その結果、利用者や社会、本学情報システムの継続性など一部に影響が出る。

１：情報資産に対し、基準となる安全性が確保されなくても、その情報の正確性または業務処理は継続可能である。その結果、利用者や社会または本学情報システム運用など、どの面にも影響が少ない。

・可用性(A)

３：情報資産に対し、基準となる安全性が確保されなかった場合、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスできなくなり、利用者や社会または本学情報システム運用など、広範囲に影響がある。

２：情報資産に対し、基準となる安全性が確保されなかった場合、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスできなくなり、利用者や社会または本学情報システム運用などの一部に影響がある。

１：情報資産に対し、基準となる安全性が確保されなくても、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスでき、利用者や社会または本学情報システム運用など、どの面にも影響が少ない。

(4) 脅威の判断

上記(2)で洗い出した情報資産について、脅威を判断する。脅威の判断は、CIA が損なわれる頻度によって判断する。

・機密性(C)

３：機密性が失われる危険が常にある。

２：機密性が失われる危険が週に一度程度ある。

１：機密性が失われる危険が年に一度程度ある。

・完全性(I)

３：情報の正確性や円滑な運用が失われる危険が常にある。

２：情報の正確性や円滑な運用が失われる危険が週に一度程度ある。

１：情報の正確性や円滑な運用が失われる危険が年に一度程度ある。

・可用性(A)

３：利用すべき立場にあるものが、利用不可能に陥る危険が常にある。

２：利用すべき立場にあるものが、利用不可能に陥る危険が週に一度程度ある。

１：利用すべき立場にあるものが、利用不可能に陥る危険が年に一度程度ある。

(5) リスク値の算出

脆弱性と資産価値と脅威の値を足しリスク値を算出する。

(6) **対策の必要性判断**

上記 5.の結果、リスク値が４以上のものについて、対策を実施する。対策を実施しないものについては、その理由を明確にし、全学総括責任者の承認を受ける。

添付１　リスク分析票（例）

大項目 No	中項目	安全対策項目	情報資産	脆弱性	資産価値		脅威	リスク値	備考
6.6 媒体の取扱い及びセキュリティ									
	6.6.1 コンピュータの取外し可能な付属媒体								
6.6.1.1		不要になったことで組織の管理外となる媒体が、再使用可能なものであるときは、それまでの内容を消去すること			C				
					I				
					A				
					C				
					I				
					A				
6.6.1.2		組織の管理外となる媒体のすべてについて、認可を必要とすること			C				
					I				
					A				
					C				
					I				
					A				
6.6.1.3		組織の管理外となる媒体の認可について、監査証跡維持のための記録を保管すること			C				
					I				
					A				
					C				
					I				
					A				
6.6.1.4		すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること			C				
					I				
					A				
					C				
					I				
					A				
6.6.1.5		コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書化すること			C				
					I				
					A				
					C				
					I				
					A				

A3106 セキュリティホール対策計画に関する様式（策定手引書）

第1条　本書の目的

本書は、セキュリティホール対策計画を作成する際に用いる様式を策定するための手引書であり、本学における当該様式の策定の参考に資することを目的とする。

様式を整備する者は、「セキュリティホール対策計画」に関する様式を策定する際に、本書を参考にすることによって、ポリシー及び実施規程により求められている様式を効率よく策定することができる。また、既存の様式を修正して利用する場合にも、項目等の過不足の確認に利用することができる。

第2条　計画に記載すべき事項

本書は、セキュリティホール対策計画についてポリシー及び実施規程により求められている手順のうち、本様式を以下の処理に用いることを前提として記述している。そのため、前提が異なる場合は、様式に盛り込む事項を適宜、修正又は追加する必要がある。

手順	項目	内容
対策計画の作成	関係者	作成者（部局技術責任者）
	処理内容	入手したセキュリティホールに関連する情報から、当該セキュリティホールが情報システムにもたらすリスクを分析し、その結果に基づいて、様式に記入する。
対策の実施	関係者	実施者（部局技術担当者）
	処理内容	作成された当該計画に基づいて、対策を実施する。
対策結果の記載	関係者	実施者（部局技術担当者）
	処理内容	実施したセキュリティホール対策の結果を記載する。

第3条　計画の基本情報

計画を設計するに当たって踏まえるべき情報システム運用・管理規程の遵守事項等を以下に示す。

なお、様式名は本学の状況に合わせて変更することが可能であるが、様式の内容が理解できる名称が望ましい。

関係する情報システム運用・管理規程遵守事項	A2101-18　セキュリティホール対策
様式名	セキュリティホール対策計画

第4条　様式に盛り込むべき項目

様式に盛り込むべき項目について以下に示す（実際の帳票のレイアウトイメージでないこ

とに留意）。

項目名		記入内容	記入者
作成にかかわる情報	作成日	作成した日付	作成者
	作成者	作成者の氏名	作成者
セキュリティホールにかかわる情報	影響のあるソフトウェア等	セキュリティホールによる影響があるソフトウェア、機器等の名称、バージョン情報	作成者
	概要	セキュリティホールの原因、影響、脅威等の情報（入手した情報の範囲で記入）	作成者
	参照先	セキュリティホール情報の参照先	作成者
対策の必要性	対策の必要性（有・無）	「有・無」のうち該当する方を選択	作成者
	対策しない理由	対策の必要性がないと判断した場合の具体的な理由	作成者
	参照先	セキュリティホール情報の参照先	作成者
対策の実施にかかわる情報	対策計画名	対策計画の名称	作成者
	対策の区分（解決策・回避策）	「解決策・回避策」のうち該当する区分を選択	作成者
	開始予定日時	対策を開始する予定の日時	作成者
	終了予定日時	対策が終了する予定の日時	作成者
	対象システム名	対策の実施対象となる情報システムの名称	作成者
	対象機器	対策の対象となる機器を特定できる情報（機器名称等）	作成者
	対象機器台数	対策の実施対象となる機器の台数	作成者
	実施者	対策を実施する責任者の氏名	作成者
	対策方法	対策の具体的な方法（回避策の場合には、解決策の実施予定を含む）	作成者
	対策用ファイルの入手方法	パッチ等の対策用ファイルを入手する方法	作成者
	情報システムへの影響	対策が情報システムへ与える影響	作成者
対策の実施における注意事項	対策用ファイルの完全性検証の必要性（有・無）	「有・無」のうち該当する方を選択	作成者
	対策用ファイルの完全性検証に関する備考	完全性検証の実施方法、必要性がないと判断した場合の具体的な理由等の情報	作成者
	システム停止の必要性（有・無）	「有・無」のうち該当する方を選択	作成者
	システム停止に関する備考	システムを停止した場合の影響、対応方法、必要性がないと判断した場合の具体的な理由等の情報	作成者
	関係者への周知の必要性（有・無）	「有・無」のうち該当する方を選択	作成者
	関係者への周知に関する備考	対策の関係者（情報システムの利用者を含む）への周知方法、周知範囲、必要性がないと判	作成者

項目名		記入内容	記入者
		断した場合の具体的な理由等の情報	
	その他	その他、必要と思われる注意事項	作成者
対策テストにかかわる情報	対策テストの必要性（有・無）	「有・無」のうち該当する方を選択	作成者
	開始予定日時	対策を開始する予定の日時	作成者
	終了予定日時	対策が終了する予定の日時	作成者
	実施者	対策テストを実施する責任者の氏名	作成者
	対策テスト環境	対策テストを実施するテスト環境	作成者
	対策テスト方法	対策テストの実施方法	作成者
対策テストの実施結果	対策テスト結果	対策テストの実施結果	実施者
	障害発生の有無	「有・無」のうち該当する方を選択	実施者
	障害内容		実施者
	障害対応方法		実施者
	障害対応結果		実施者
対策の実施結果	開始日時	対策を開始した日時	実施者
	終了日時	対策が終了した日時	実施者
	実施者	対策を実施した者の名前	実施者
	実施内容	対策実施の内容	実施者
	実施結果	対策実施の結果	実施者
	障害発生の有無	「有・無」のうち該当する方を選択	実施者
	障害内容		実施者
	障害対応方法		実施者
	障害対応結果		実施者

様式 X

[作成日]
[作成者]

セキュリティホール対策計画

セキュリティホールにかかわる情報（対策の必要性の有無に関係なく記述）

影響のあるソフトウェア等	
概要	
参照先	

[対策の必要性]
□ 有
□ 無

対策の必要性がないと判断した理由（対策の必要性がないと判断した場合に記述）

対策の実施にかかわる情報（対策の必要性があると判断した場合に記述）

対策計画名				
対策の区分	□ 解決策 □ 回避策			
開始予定日時		終了予定日時		
対象システム名				
対象機器(台数)				
実施者				
対策方法				
対策用ファイルの入手方法				
情報システムへの影響				
対策の実施における注意事項	有	無	備考	
・対策用ファイルの完全性検証の必要性	□	□	（完全性の検証方法が用意されている場合には検証を実施すること）	
・システム停止の必要性	□	□	（システム停止を伴う場合の影響、対応方法等の情報）	
・関係者への周知の必要性	□	□	（対策により影響のある者への通知方法、通知範囲等の情報）	
その他：（上記以外で注意すべき事項があれば記述）				

対策テストにかかわる情報（対策の必要性があると判断した場合に記述）

必要性	□ 有　□ 無		
開始予定日時		**終了予定日時**	
実施者			
対策テスト環境			
対策テスト方法			
対策テストの実施結果（対策テスト実施後に結果を記述）			
対策テスト結果			
障害発生の有無	□ 有　□ 無		
障害内容			
障害対応方法			
障害対応結果			

対策の実施結果（対策実施後に結果を記述）

開始日時		**終了日時**	
実施者			
実施内容			
実施結果			
障害発生の有無	□ 有　□ 無		
障害内容			
障害対応方法			
障害対応結果			

A3107 ウェブサーバ設定確認実施手順（策定手引書）

1. 本書の目的

本書は、本学ウェブサーバの設定確認を行う場合の手順書を策定するための手引書である。本書に基づいて策定される「ウェブサーバ設定確認実施手順」は、ウェブサーバの検収時における設定確認だけでなく、定期的なウェブサーバの設定確認における利用も想定される。また、定期的な設定確認の場合には、ユーザ認証やアクセス制御等の項目のみを部分的・重点的に確認する利用も想定される。手順書の整備を担当する者は、「ウェブサーバ設定確認実施手順」を策定する際に、本書を参考にすることによって、情報システム運用基本方針、情報システム運用基本規程及び情報システム運用・管理規程に準拠してこれを効率良く作成することができる。

2. 実施手順に記載すべき事項

「ウェブサーバ設定確認実施手順」には、以下の事項を具体化させて記載すること。

2.1 「A2101 情報システム運用・管理規程」に定める「ウェブサーバ設定確認実施手順」に係る遵守事項

A2101-06 （セキュリティホール対策）
A2101-07 （不正プログラム対策）
A2101-08 （サービス不能攻撃対策）
A2101-09 （踏み台対策）
A2101-11 （電子計算機の対策）
A2101-12 （サーバ装置の対策）
A2101-18 （セキュリティホール対策）
A2101-19 （不正プログラム対策）
A2101-20 （サービス不能攻撃対策）
A2101-21 （踏み台対策）
A2101-22 （脆弱性診断）
A2101-26 （サーバ装置の対策）
A2101-29 （電子計算機の対策）
A2101-57 （主体認証機能の導入）
A2101-58 （アクセス制御機能の導入）
A2101-59 （適正なアクセス制御）
A2101-60 （無権限のアクセス行為の対策）
A2101-61 （アカウント管理機能の導入）
A2101-62 （アカウント管理手続の整備）

A2101-70 （管理者権限を持つアカウントの利用）
A2101-71 （証跡管理機能の導入）
A2101-72 （証跡の取得と保存）
A2101-73 （取得した証跡の点検、分析及び報告）
A2101-74 （証跡管理に関する利用者等への周知）
A2101-75 （通信の監視）
A2101-76 （利用記録）
A2101-78 （利用者等が保有する情報の保護）
A2101-79 （暗号化機能及び電子署名機能の導入）
A2101-80 （暗号化及び電子署名に係る管理）
A2101-81 （暗号と電子署名に係る規定の整備）

2.2 セキュリティ確保に係るその他の留意事項

2.1 に示す遵守事項のほか、セキュリティ確保に係る留意事項として、以下の項目を考慮すべきである。

・システム領域とデータ領域との分離
・ウェブサーバアプリケーションに付属する不要なコンテンツの削除

3. 文書構成例

「ウェブサーバ設定確認実施手順」は、ウェブサーバアプリケーションの動作に関する設定及び運用並びに管理上必要となるアプリケーション（リモート管理、コンテンツ更新、パフォーマンス監視等）の設定等も含めた構成が有効である。文書構成の例を以下に示す。

1 本書の目的

2 本書の対象者
2.1 対象者

3 オペレーティングシステムに関する確認項目
3.1 ユーザ認証に関する項目
・アカウントの管理
・パスワードの管理
・認証の管理
・アカウントのロックアウト
・認証時のメッセージ表示
3.2 ユーザ権利の割り当てに関する項目
・システム管理に関する権利

- ログオンに関する権利
- 監査に関する権利

3.3 アクセス制御に関する項目

- ネットワークレベルでのアクセス制御
- ファイルシステムレベルでのアクセス制御
- システムリソースレベルでのアクセス制御
- デバイスレベルでのアクセス制御

3.4 サービスに関する項目

- サービスの停止
- 機能の無効化

3.5 ログ管理に関する項目

- 取得項目の選択
- ログファイルの保存方法及び管理
- 監査機能の設定

3.6 セキュリティホール対策に関する項目

- 既知アップデートの適用
- アップデート方法の設定

3.7 不正プログラム対策に関する項目

- アンチウイルスソフトウェアによる対策
- システム設定による対策

3.8 サービス不能攻撃対策に関する項目

- システムパラメータの調整
- ネットワークパラメータの調整

3.9 パフォーマンスに関する項目

- システムパラメータの調整
- ネットワークパラメータの調整

3.10 暗号及び電子署名に関する項目

- システム全般の暗号化設定

3.11 その他の項目

- 要機密情報の保護
- スクリーンセーバーの設定
- バックアップの設定

4 ウェブサーバアプリケーションに関する確認項目

4.1 コンテンツに関する項目

- パーティションの分割
- 不要なコンテンツの削除

- 公開コンテンツの格付け確認
- 私的なコンテンツの排除

4.2 機能に関する項目

- スクリプト／ファイル実行の制限
- アプリケーション／バージョン情報表示の制限
- ユーザドキュメントの公開の禁止
- インデックス表示の禁止
- WebDAV／FrontPage®等の機能制限

4.3 アクセス制御に関する項目

- ネットワークレベルでのアクセス制御
- ユーザレベルでのアクセス制御
- コンテンツレベルでのアクセス制御

4.4 ログ管理に関する項目

- 取得項目の選択
- ログファイルの保存方法及び管理

4.5 セキュリティホール対策に関する項目

- 既知アップデートの適用
- アップデート方法の設定

4.6 暗号に関する項目

- SSL/TLS の利用

5 リモート管理アプリケーションに関する確認項目

5.1 機能に関する項目

- リモート管理機能の設定
- セキュリティ機能の設定
- 機能の無効化

5.2 ユーザ認証に関する項目

- 認証方法の強化
- 認証時のメッセージ表示

5.3 アクセス制御

- ユーザレベルでのアクセス制御

5.4 ログ管理に関する項目

- 取得項目の選択
- ログファイルの保存方法及び管理

5.5 セキュリティホール対策に関する項目

- 既知アップデートの適用
- アップデート方法の設定

5.6 暗号に関する項目 ・暗号機能の強化

4. 作成する上での留意事項

「ウェブサーバ設定確認実施手順」は、以下のことに留意して作成する。

(1) オペレーティングシステム、ウェブサーバアプリケーション及び運用・管理上必要となるアプリケーションごとに確認すべき設定項目が異なるため、それぞれに特化した手順書を作成する。

(2) 確認及び結果の判断を的確に行うため、チェックシートの形式で作成し、確認すべき設定項目を具体的に記述する。

(3) 手順書の対象者として十分な技術を有する者を前提とした場合、確認手順を省略して確認すべき内容のみを簡潔に記載する。

(4) 文書構成例に記載された見出しは基本的なものであるため、ウェブサーバの利用目的、構成、環境等に応じた見出しの検討・追加を行い、必要な確認項目を網羅する。

(5) 文書構成例に記載された見出し及び検討・追加された見出しごとに、ソフトウェアの開発元が公開している情報を活用して確認項目を抽出する。

(6) ソフトウェアの開発元が公開している情報を活用する場合には、著作権に注意する。

(7) 手順書は、学内の担当者による検収時の又は定期的な設定確認としての利用が想定されているため、業者に公開せずに学内の総括責任者、技術責任者、技術担当者及び利用者に限り参照できる文書として取り扱う。

(8) 前記２に示す事項を「ウェブサーバ設定確認実施手順」に反映するに当たっては、当該事項の内容に応じて、以下のいずれかの方針で記述する。

[具体化]・・・「ウェブサーバ」に限定されず一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、これを「ウェブサーバ」に適用し、表現をより具体的に修正・追加する。

[転記]・・・・記述内容が具体性を持ち、変更が不要と思われる遵守事項については、これを転記する。

[詳細化]・・・記述内容が具体性を持っているが、利用者等の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、解説書等を参考に、これを詳細化する。

[背景]・・・・主にセキュリティ機能の実装に関する内容であり、これを背景として利用者等による注意義務が発生すると思われる遵守事項については、これをそれぞれの立場から解釈し直す。

[別立場]・・・利用者の立場ではなく、総括責任者側又は技術責任者並びに技術担当者側の立場から記述されている遵守事項については、これを利用者の立場から解釈し直す。

[参考引用]・・直接「ウェブサーバ」に関連した内容ではないが、利用者等の理解促進に寄与すると思われる遵守事項については、これを参考引用する。

[一般]・・・・直接「ウェブサーバ」に関連した内容ではないが、一般論として手順書に記載しておくことが望ましいと思われる遵守事項については、これを周辺知識として盛り込む。

5. 参考資料

「ウェブサーバ設定確認実施手順」の作成に際しては、以下のような資料が参考となる。

5.1 政府関係の資料

(1) 独立行政法人 情報処理推進機構(IPA)の「セキュアな Web サーバーの構築と運用」
URL: http://www.ipa.go.jp/security/fusei/ciadr.html

5.2 政府以外の資料

(1) マイクロソフト株式会社の「セキュリティガイダンスセンター」
URL: http://www.microsoft.com/japan/security/guidance/default.mspx

(2) マイクロソフト株式会社の「Windows Server. 2003 セキュリティ ガイド」
URL: http://www.microsoft.com/japan/technet/security/prodtech/windowsserver 2003/w2003hg/sgch00.mspx

(3) サン・マイクロシステムズ株式会社の「SunR BluePrints Security Publications」
URL: http://www.sun.com/software/security/blueprints/index.xml

(4) サン・マイクロシステムズ株式会社の「SolarisR Security Toolkit」
URL: http://www.sun.com/software/security/jass/

(5) 日本ヒューレット・パッカード株式会社の「ホワイトペーパー：ネットワーク&セキュリティ」
URL: http://h50146.www5.hp.com/products/software/oe/hpux/developer/setup/tips.html

(6) 日本ヒューレット・パッカード株式会社の「HP-UXR Bastille」
URL: http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA

(7) 「Bastille Linux®」
URL: http://www.bastille-linux.org/

A3108 電子メールサーバのセキュリティ維持手順（策定手引書）

1. 本書の目的

本書は、サーバ装置上で動作し、電子メールサービス提供のために利用しているソフトウェアのセキュリティ維持に関して、部局技術担当者等が遵守すべき規定（以下「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」という。）を部局技術責任者が整備するための手引書である。

本学においては、情報システム運用基本方針、情報システム運用基本規程に基づく情報システム運用・管理規程及び関係する規定を整備することが求められている。「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」は、これらの一つとして策定し、本学内において電子メールサービスを提供する場合に適用するものである。

電子メールは通信回線を介して提供されるサービスの中で最も普及しているサービスの一つであり、本学の研究教育事務を円滑に遂行するために不可欠なものになっている。その一方で、電子メールの送受信は情報のやりとりにほかならず、そのやりとりは様々な中継地点を経由して行われるため、その過程における情報の漏えい、改ざんのリスクがある。また、セキュリティホール対策や不正プログラム対策をおこたると、不正中継、ウイルス感染等、学内だけでなく学外にも迷惑をかけるおそれがある。このようなリスクを軽減するため、サーバ装置上で動作し、電子メールサービスにおいて利用されるアプリケーションソフトウェアのセキュリティを維持することが部局技術担当者等に求められる。

本書は、これらの背景の下で、「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」に含めるべき事項を具体的に示し、もって情報システム運用基本方針、情報システム運用基本規程及び情報システム運用・管理規程への準拠性、本学の研究教育事務への適用性等において適切な規定の整備に資することを目的とする。

2. 実施手順に記載すべき事項

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」には、以下の事項を具体化させて記載すること。

2.1 情報システム運用・管理規程に定める「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」に係る遵守事項

A2101-06 （セキュリティホール対策）
A2101-07 （不正プログラム対策）
A2101-08 （サービス不能攻撃対策）
A2101-09 （踏み台対策）
A2101-12 （サーバ装置の対策）

A2101-18 （セキュリティホール対策）
A2101-19 （不正プログラム対策）
A2101-20 （サービス不能攻撃対策）
A2101-21 （踏み台対策）
A2101-24 （資源の管理）
A2101-26 （サーバ装置の対策）
A2101-57 （主体認証機能の導入）
A2101-61 （アカウント管理機能の導入）
A2101-62 （アカウント管理手続の整備）
A2101-70 （管理者権限を持つアカウントの利用）
A2101-71 （証跡管理機能の導入）
A2101-72 （証跡の取得と保存）
A2101-73 （取得した証跡の点検、分析及び報告）
A2101-74 （証跡管理に関する利用者等への周知）
A2101-75 （通信の監視）
A2101-76 （利用記録）
A2101-78 （利用者等が保有する情報の保護）
A2101-84 （インシデントの発生に備えた事前準備）
A2101-85 （インシデントの原因調査と再発防止策）

2.2 セキュリティ確保に係るその他の留意事項

2.1 に示す遵守事項のほか、セキュリティ確保に係る留意事項として、以下の項目を考慮すべきである。

・迷惑メールの取扱い

3. 文書構成例

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」は、情報セキュリティ対策の観点を含めた一般的な利用手順書とすべきである。そのため、利用者等の行為に着目した構成が有効である。文書構成の例を以下に示す。

1 本手順の目的

2 本手順の対象者
2.1 対象者

3 定義
《 対象：部局技術担当者 》

4. 策定する上での留意事項

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」は、以下のことに留意して策定する。

(1) 電子メールサービス提供のために利用しているソフトウェアのセキュリティ維持に関して、部局技術担当者、権限管理を行う者、部局技術責任者、部局総括責任者ごとに遵守すべき規定を整理・分類する。各者に求められる役割は以下のとおりである。

(2) 部局技術担当者は、セキュリティ維持のための運用管理の主たる実施主体である。

(3) 権限管理を行う者は、電子メール送受信における主体の権限管理を行う主体である。

(4) 部局技術責任者は、セキュリティホール対策計画の作成、証跡管理における証跡の保護等の実施主体である。

(5) 部局総括責任者は、不正プログラム対策の見直し等の実施主体である。

(6) 規定の主語は、実施主体ごとに「部局技術担当者は」などに統一する。

(7) 前記 2 の実施手順に記載すべき事項を「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」に反映するに当たっては、当該事項の内容に応じて、以下のいずれかの方針で記述する。

[具体化]・・・「電子メールサービス」に限定されず一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、これを「電子メールサービス」に適用し、表現をより具体的に修正・追加する。

[転記]・・・・記述内容が具体性を持ち、変更が不要と思われる遵守事項については、これを転記する。

[詳細化]・・・記述内容が具体性を持っているが、利用者等の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、解説書等を参考に、これを詳細化する。

[背景]・・・・主にセキュリティ機能の実装に関する内容であり、これを背景として利用者等による注意義務が発生すると思われる遵守事項については、これをそれぞれの立場から解釈し直す。

[別立場]・・・利用者の立場ではなく、総括責任者側又は技術責任者並びに技術担当者側の立場から記述されている遵守事項については、これを利用者の立場から解釈し直す。

[参考引用]・・直接「電子メールサービス」に関連した内容ではないが、利用者等の理解促進に寄与すると思われる遵守事項については、これを参考引用する。

[一般]・・・・直接「電子メールサービス」に関連した内容ではないが、一般論として手順書に記載しておくことが望ましいと思われる遵守事項については、これを周辺知識として盛り込む。

5. 参考資料

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」の策定に際しては、以下のような資料が参考となる。

5.1 政府及び政府関係機関の資料

(1) 総務省の「迷惑メール対策」
URL: http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html

(2) 独立行政法人 情報処理推進機構(IPA)の「UBE（迷惑メール）中継対策」
URL: http://www.ipa.go.jp/security/ciadr/antirelay.html

(3) 独立行政法人 情報処理推進機構(IPA)の「電子メールのセキュリティ」の「電子商取引における電子メールに関するセキュリティ上の課題」
URL: http://www.ipa.go.jp/security/fy10/contents/over-all/email.html

5.2 政府・政府関係機関以外の資料

なし

6. 雛形の利用方法

別紙１の雛形を参考にして、「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」を策定すると効率的である。別紙１の雛形は、前記 2 の実施手順に記載すべき事項を、前記 3 の文書構成例の枠組みの中に記載したものである。

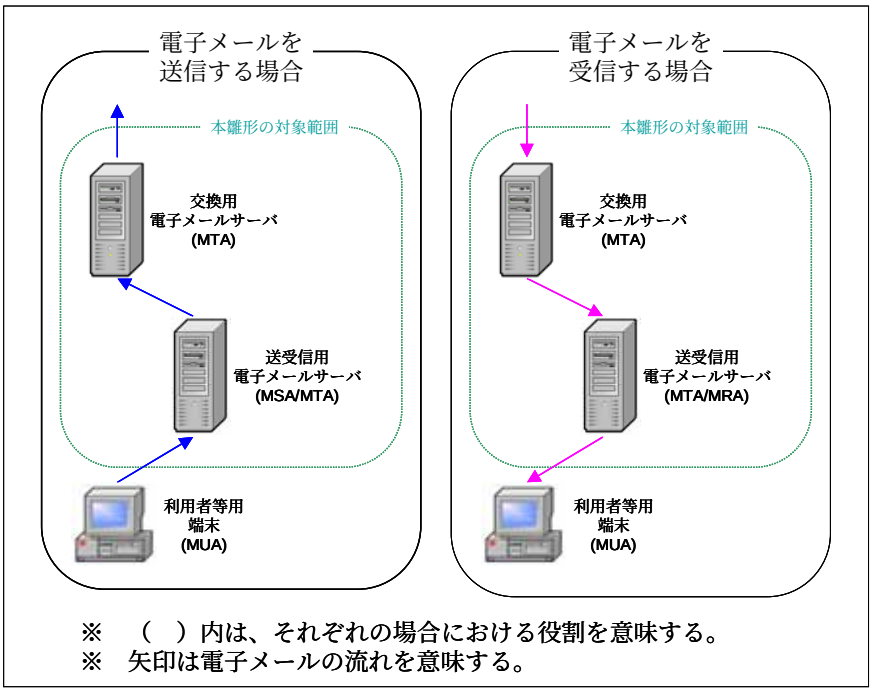
6.1 雛形において想定する前提

本雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 電子メールの送受信にかかわる電子メールサーバ及び端末の構成、電子メールの送受信の経路は、以下の図のとおりである。
- 交換用電子メールサーバにおいて、送受信する電子メールに対する不正プログラムのチェックが実施されている。
- MRA から電子メールを受信する際に行う利用認証は、知識による認証方式が利用されている。（MSA に電子メールを送信する際に利用認証を利用する場合も同様。）。
- 利用者等が、MRA から電子メールを受信する際の利用認証に利用するパスワードを、容易に変更できる機能が用意されている。（MSA に電子メールを送信する際に利用認証を利用する場合も同様。）
- MTA、MSA 及び MRA において、電子メール送受信、利用認証等の証跡が取得されてい

る。

図：サーバ及び端末の構成、電子メール送受信経路のイメージ



※　（　）内は、それぞれの場合における役割を意味する。
※　矢印は電子メールの流れを意味する。

6.2 手直しポイント

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する手順」を策定するに当たり、以下の点について手直しをする必要がある。

(1) **「通信回線を介して提供するサービス」に応じて内容を変更する必要がある。雛形は電子メールサービスを対象に記載されているが、例えば、ウェブサービスの場合には、HTTP 基本認証による利用認証、コンテンツのアクセス制御、SSL/TLS を利用した暗号化通信等に関する運用管理の実施手順について記述することとなる。**

(2) **メールアドレスを発行・削除を伴う人事異動等に関する情報の連絡経路について、「人事異動等における情報セキュリティ対策実施手順」に合わせる。**

(3) **雛形において、[・・・] 形式で示す設定値（期間等）については、本学の定めに合わせる。**

(4) **雛形において、【・・・の場合】形式で示す記述については、想定される複数の案を記したものであり、本学の判断により適宜、選択又は修正する。**

(5) **雛形と既存の実施手順書との整合性を考慮し、適切に分割、統合、相互参照する。特に、本雛形は電子メールに関連するアプリケーションソフトウェアのセキュリティ維持に関する規定を記載しているため、サーバ装置の運用管理手順書との、統合、相互参照をすると良い。**

(6) **部局技術担当者、部局技術責任者等の役割ごとに規定を記述しているため、既存の規定の構成に合わせて分割、統合すると良い。**

別紙１　電子メールサーバのセキュリティ維持手順　雛形

本書の位置付け

本書は、「電子メールサーバのセキュリティ維持手順」を策定する場合の雛形であり、「A3108 電子メールサーバのセキュリティ維持手順（策定手引書）」の 2.に示す実施手順に記載すべき事項を、同 3.に示す文書構成例の枠組みの中に記載したものである。

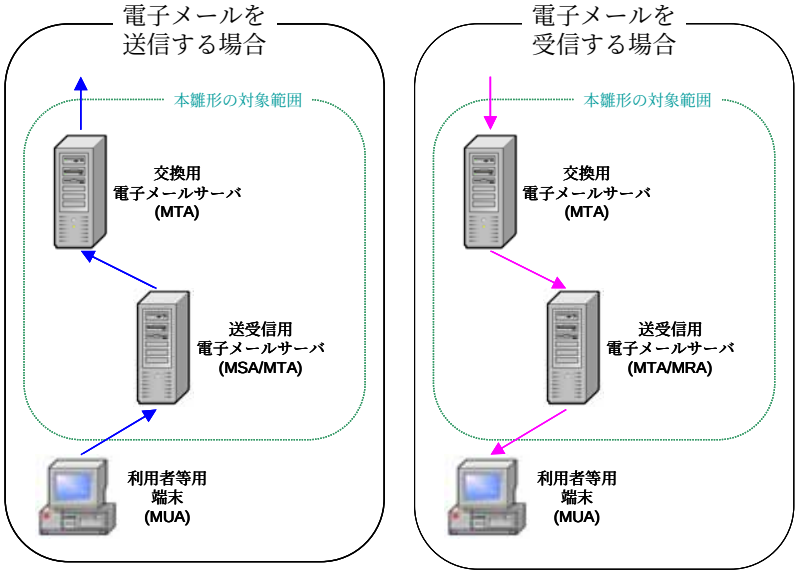
本書の利用方法

本書において想定する前提

本雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

・電子メールの送受信にかかわる電子メールサーバ及び端末の構成、電子メールの送受信の経路は、以下の図のとおりである。

図：サーバ及び端末の構成、電子メール送受信経路のイメージ



※　（　）内は、それぞれの場合における役割を意味する。
※　矢印は電子メールの流れを意味する。

・交換用電子メールサーバにおいて、送受信する電子メールに対する不正プログラムのチェックが実施されている。

・MRA から電子メールを受信する際に行う主体認証は、知識による認証方式が利用されている。（MSA に電子メールを送信する際に主体認証を利用する場合も同様。）。

・利用者等が、MRA から電子メールを受信する際の主体認証に利用するパスワードを、容易に変更できる機能が用意されている。（MSA に電子メールを送信する際に主体認証を利用する場合も同様。）

・MTA、MSA 及び MRA において、証跡が取得されている。

手直しポイント

「電子メールサーバのセキュリティ維持手順」を策定するに当たり、以下の点について手直しをする必要がある。

①「通信回線を介して提供するサービス」に応じて内容を変更する必要がある。雛形は電子メールサービスを対象に記載されているが、例えば、ウェブサービスの場合には、HTTP 基本認証による主体認証、コンテンツのアクセス制御、SSL/TLS を利用した暗号化通信等に関する運用管理の実施手順について記述することとなる。

②メールアドレスの発行・削除を伴う人事異動等に関する情報の連絡経路について、「A3109 人事異動の際に行うべき情報セキュリティ対策実施手順」に合わせる。

③雛形において、*[・・・]* 形式で示す設定値（期間等）については、各大学内の定めに合わせる。

④雛形において、【・・・の場合】形式で示す記述については、想定される複数の案を記したものであり、各大学の判断により適宜、選択又は修正する。

⑤雛形と既存の実施手順書との整合性を考慮し、適切に分割、統合、相互参照する。特に、本雛形は電子メールに関連するアプリケーションソフトウェアのセキュリティ維持に関する規定を記載しているため、サーバ装置の運用管理手順書との、統合、相互参照をすると良い。

⑥部局技術担当者、部局技術責任者等の役割ごとに規定を記述しているため、既存の規定の構成に合わせて分割、統合すると良い。

1. 本手順の目的

電子メールは通信回線を介して提供されるサービスの中で最も普及しているサービスの１つであり、本学の研究教育事務を円滑に遂行するために不可欠なものになっている。その一方で、電子メールの送受信は情報のやりとりにほかならず、そのやりとりは様々な中継地点を経由して行われるため、その過程における情報の漏えい、改ざんのリスクがある。また、セキュリティホール対策や不正プログラム対策をおこたると、不正中継、ウイルス感染等、学内だけでなく学外にも迷惑をかけるおそれがある。

本手順は、このようなリスクを軽減するため、サーバ装置上で動作し、電子メールサービスにおいて利用されるアプリケーションソフトウェアのセキュリティ維持に関する規定を提供することを目的とする。

2. 本手順の対象

2.1 対象者

本手順は、電子メールサービス提供ソフトェアのセキュリティ維持のため、日常的及び定期的に運用管理を実施することが求められているすべての情報システムの部局技術担当者等を対象とする。

3. 定義

本手順における用語の定義は次のとおりである。

(1) 「電子メールサービス提供ソフトェア」とは、電子メールの送受信のためにサーバ装置上で動作する MTA、MSA、MRA であって、部局技術担当者によって運用管理が行われているものをいう。

(2) 「MTA」とは、Mail Transfer Agent の略称であり、他のサーバから SMTP で受信した電子メール、又は MSA から渡された電子メールを、必要に応じて、SMTP で他のサーバへ転送したり、ローカルのメールボックスに格納するソフトウェアへ渡したりする処理を行うソフトウェアをいう。いわゆる SMTP サーバ等。

(3) 「MSA」とは、Mail Submission Agent の略称であり、MUA から SMTP で電子メールを受信し、当該電子メールを MTA に渡す処理を行うソフトウェアをいう。MTA の機能に含むとする考え方もある。

(4) 「MRA」とは、Mail Retrieval Agent の略称であり、メールボックスに格納された電子メールを、POP3、IMAP 等で MUA へ渡すソフトウェアをいう。いわゆる POP３サーバ、IMAP サーバ等。

(5) 「MUA」とは、Mail User Agent の略称であり、電子メールの読み書き、MSA 経由での電子メールの送信、MRA 経由での電子メールの受信、送受信した電子メールの管理を行うソフトウェアをいう。いわゆるメーラ等。

(6) 「エラーメール」とは、あて先のメールアドレスが存在しない場合等に、送信元のメールアドレス又は MTA の管理者用メールアドレスあてに送信不能を伝えるために、MTA によって自動的に送られる電子メールをいう。

(7) 「メールボックス」とは、あるメールアドレスあてに届いた電子メールを保管しておく電子メールサーバ上の領域をいう。メールボックスは、メールアドレスごとに存在し、メールアドレスあてに届いた電子メールは、当該メールアドレス専用のメールボックスに保管される。

(8) 「交換用電子メールサーバ」とは、他のドメインと電子メールを交換（送受信）するための電子メールサーバであり、DNS 情報において交換用であることが明示されている電子メールサーバであり、MTA が動作しているものをいう。いわゆる MX サーバ。

(9) 「送受信用電子メールサーバ」とは、電子メールを利用している利用者等のメールボックスが存在し、当該利用者等が MUA を利用して電子メールを送受信するために接続するための電子メールサーバであり、MTA、MSA、MRA が動作しているものをいう。

《対象：部局技術担当者 該当項目：4、5、6》

4. 電子メールサービス提供ソフトェアに共通のセキュリティ維持のための対策

4.1 主体認証

(1) 部局技術担当者は、電子メールを利用している利用者等からパスワードが他者に使用され又はその危険が発生したことの報告を受けた場合には、以下の措置を講ずること。

- 当該利用者等の識別符号（ユーザ ID）を一時的に無効にする。
- 新たなパスワードを設定し、他者に知られないように当該利用者等に連絡した上で、当該識別符号の一時無効を解除する。
- 証跡の分析により他者に使用された可能性を確認する。
- 部局総括責任者に状況を報告する。

【電子メールサービスにおいてパスワードの通信時に暗号化を行っていない場合】

(2) 部局技術担当者は、電子メールサービスを利用する利用者等に対して、以下の事項を通知すること。

- 電子メールサービスにおいて利用するパスワードは通信回線上を暗号化されずに送受信されるため、盗聴等により容易に漏えいする危険性があること。
- 他の情報システムで利用している重要なパスワードを電子メールサービスにおける主体認証に利用しないこと。

【電子メールサービスにおいてパスワードの保存時に暗号化を行っていない場合（多くの電子メールサービスにおいて該当しない。）】

(3) 部局技術担当者は、電子メールサービスを利用する利用者等に対して、以下の事項を通知すること。
- 電子メールサービスにおいて利用するパスワードは暗号化されずにサーバ装置上に保存されるため、不正侵入等により漏えいする危険性があること。
- 他の情報システムで利用している重要なパスワードを電子メールサービスにおける主体認証に利用しないこと。

4.2 証跡管理

(1) 部局技術担当者は、電子メールサービス提供ソフトェアにより取得される以下の証跡を記録すること。
- 電子メールの送受信に関する、送受信日時、メールアドレス、送受信の成否等の証跡（MTA、MSA により記録）

【電子メールの送信時に認証を行う場合（強化遵守事項）】
- MUA から電子メールを送信する際の主体認証の成功・失敗の証跡（MSA により記録）
- メールボックスから電子メールを取得する際の主体認証の成功・失敗の証跡（MRA により記録）
- メールボックスから電子メールを取得する際の取得日時、取得電子メール数、識別符号（ユーザ ID）等の証跡（MRA により記録）

(2) 部局技術担当者は、証跡が取得できなくなる事態を避けるため、電子メールサービス提供ソフトェアの証跡を記録しているファイルを*[1 ヶ月に１度]* 変更すること。また、証跡を改ざんから保護するとともに、証跡を記録したファイルにより記録装置の容量が圧迫されることを防止するため、当該ファイルを適宜外部記録媒体へ移動することが望ましい。

(3) 部局技術担当者は、電子メールサービス提供ソフトェアにより記録された証跡を*[○年間]* 保存すること。また、保存期間を延長する必要性がない場合には、速やかにこれを消去すること。

4.3 セキュリティホール対策

(1) 部局技術担当者は、電子メールサービス提供ソフトェアについて変更があった場合には、セキュリティホール対策に必要となる機器情報の文書に反映すること。
文書に記録すべき情報としては、以下の項目が想定される。
- 電子メールサービス提供ソフトェアの一覧（名称、種別、バージョン）

(2) 部局技術担当者は、電子メールサービス提供ソフトェアに関して、以下の方法で、セキュリティホールが発見されていないかどうかを*[毎日]* 確認すること。

【公表されているウェブサイト等を利用する場合】

・電子メールサービス提供ソフトェアの製造・開発・販売元、JVN(JP Vendor Status Notes)、JPCERT コーディネーションセンター等のセキュリティ関連機関等がウェブサイト、電子メール等で公表するセキュリティホール情報を収集し確認する。

【セキュリティホール情報提供サービスを利用する場合】

・セキュリティホール情報提供サービスにより提供される情報を確認する。

(3) 部局技術担当者は、電子メールサービス提供ソフトェアにセキュリティホールが発見されている場合には、当該セキュリティホールに関連する情報（原因、影響範囲、対策方法、攻撃ツールの有無等を含む。）を入手し、部局技術責任者に報告すること。

(4) 部局技術担当者は、部局技術責任者が作成したセキュリティホール対策計画に基づき、セキュリティホール対策を講ずること。

(5) 部局技術担当者は、セキュリティホール対策を実施する場合には、以下の事項に注意すること。

・対策の実施記録を部局技術責任者に報告すること。

・対策用ファイル（パッチ、アップデートファイル、最新バージョンのファイル等）に不正プログラムが含まれている可能性があるため、ソフトウェアの製造・開発・販売元からのダウンロード等の信頼できる方法で入手すること。

・対策用ファイルの完全性を検証する方法が用意されている場合には、その検証を実施すること。

(6) 部局技術担当者は、*[１年に１度]* 電子メールサービス提供ソフトェアに関して、以下の事項を確認、分析し、不適切な状態である場合には、是正措置を行うこと。是正措置は、セキュリティホール対策の注意事項に準じて行うこと。

・セキュリティホール対策の状況

・電子メールの中継に関わる設定の適切性（MTA 及び MSA の場合。詳細は「5.1 不正中継に関する対策」及び「6.1 メールボックスの管理」を参照すること。）

・VRFY、EXPN、ETRN、その他悪用されるおそれのある SMTP コマンドの無効化（MTA 又は MSA の場合）

・主体認証方式及びパスワードの安全性（MRA の場合）

【迷惑メール対策を実施している場合】

・迷惑メールの排除に関わる設定の適切性（MTA の場合。詳細は「5.3 迷惑メールに関する対策」を参照すること。）

【電子メールの送信時に認証を行う場合（強化遵守事項）】

・主体認証方法及びパスワードの安全性（MSA の場合）

【サービス不能攻撃対策として電子メールサービスを監視する場合（強化遵守事項）】

4.4 **サービス不能攻撃対策**

(1) **電子メールサービスは、大量の電子メール（エラーメールを含む。）を受信する攻撃により、通常の利用者が電子メールサービスを利用できなくなる可能性がある。部局技術担当者は、電子メールの配送状況、送受信数等を監視・記録し、平常時の状況を把握すること。**

(2) **部局技術担当者は、監視・記録された平常時と異なり、サービスの提供に問題が生じる状況を検出した場合には、部局技術責任者に報告すること。**

5. 交換用電子メールサーバにおけるセキュリティ維持のための対策

5.1 **不正中継に関する対策**

(1) **部局技術担当者は、電子メールの中継制御に関して、以下のような設定を、*[１年に１度]*確認すること。**

・MTA において、自ドメインあての電子メールのみを送受信用電子メールサーバに中継し、それ以外の電子メールを受信拒否とする設定

5.2 **電子メールに含まれる不正プログラムに関する対策**

(1) **部局技術担当者は、不正プログラムに関する情報の収集に努めること。**

(2) **部局技術担当者は、収集した情報について、以下のように特段の対処が必要な場合には、利用者等に注意喚起又は対応方法を周知徹底すること。**

・急激に感染を拡大する不正プログラムが報告されている場合

・交換用電子メールサーバ上で動作しているアンチウイルスソフトウェアで未対応の不正プログラムが報告されている場合

(3) **部局技術担当者は、交換用電子メールサーバ上で動作しているアンチウイルスソフトウェア、不正プログラム定義ファイル等を常に最新の状態に維持すること。**

(4) **部局技術担当者は、交換用電子メールサーバ上で MTA 及び MSA により取り扱われる電子メールに関して、電子メールの本文、添付ファイル等に対して不正プログラムのチェックを自動的に行う機能を有効にすること。**

(5) **部局技術担当者は、学内の端末から不正プログラムが含まれる電子メールが送信されていることを検知した場合には、当該電子メールを送信している端末を通信回線から隔離する等して不正プログラムが含まれる電子メールの送信を抑制し、部局総括責任者に感染の事実を報告すること。**

(6) **部局技術担当者は、学外から不正プログラムが含まれる電子メールが送信されているこ**

とを検知した場合には、送信元の MTA の管理者等にその旨を連絡し、対処を促すことが望ましい。

【迷惑メール対策を実施している場合】

5.3 迷惑メールに関する対策

(1) 部局技術担当者は、利用者等あての迷惑メールの排除基準及び取扱方法（受信拒否（恒久的エラー／一時的エラー）、受信後削除、受信等）に関する MTA の設定を適宜見直し、必要に応じて修正すること。

(2) 部局技術担当者は、MTA において設定されている排除基準及び取扱方法の修正により、迷惑メールに該当しない研究教育事務上必要な電子メールまでもが排除されることのないように配慮すること。

【記録装置の状態を監視し、容量の圧迫を検知する場合（強化遵守事項）】

5.4 電子メールキューの管理

(1) 部局技術担当者は、電子メールキュー（配送不能等の理由で再配送待ち状態の電子メールが保存される領域。）に、大量の再配送待ち電子メールが滞留し、記録装置の容量を圧迫していないかどうかを適宜確認すること。

(2) 部局技術担当者は、電子メールキューに大量の再配送待ち電子メールが滞留している場合で、当該電子メールが迷惑メールのときは、エラーメールにより学外の電子メールサーバに負荷をかけるおそれがあるため、当該電子メールを配送不能とせずに破棄すること。ただし、当該電子メールが迷惑メールでないときは、配送不能として送信元のメールアドレスにエラーメールを返すことが望ましい。

5.5 エラーメールの管理

(1) 部局技術担当者は、MTA・MSA の管理者用メールアドレス（postmaster 等）あてに届いているエラーメールを適宜確認し、電子メールの配送不能等の問題がないことを確認すること。

(2) 本学から送信したように送信元メールアドレスを詐称した迷惑メールが第三者によって送信された場合、配送不能で大量のエラーメールが管理者用メールアドレス又は利用者等のメールアドレスあてに届く場合がある。部局技術担当者は、多量のエラーメールが届いている場合には、エラーメールの内容を確認し、送信元メールアドレスを詐称した迷惑メールと判断できるときには、部局総括責任者に詐称の事実を報告すること。

(3) 部局技術担当者は、多量のエラーメールを受信することによって MTA が動作するサーバ装置のリソース（CPU、メモリ、HDD 等を含む。）が消費され、通常の電子メールの送受信に影響を及ぼすおそれがある場合には、受信拒否等の方法により影響を抑えること。

6. 送受信用電子メールサーバにおけるセキュリティ維持のための対策

6.1 不正中継に関する対策

(1) 部局技術担当者は、電子メールの中継制御に関して、以下のような設定を、*[１年に１度]* 確認すること。

・MTA において、自ドメインあての電子メールのみを受信した上で該当する電子メールアドレスのメールボックスに保存し、それ以外の電子メールを受信拒否とする設定

【電子メールの送信時に認証を行わない場合】

・MSA において、学内 LAN の端末からの接続により送信された電子メールのみを転送し、それ以外の電子メールを受信拒否とする設定

【電子メールの送信時に認証を行う場合（強化遵守事項）】

・MSA において、電子メール送信時に認証が行われた端末からの接続により送信された電子メールのみを転送し、それ以外の電子メールを受信拒否とする設定

6.2 メールボックスの管理

(1) 部局技術担当者は、メールボックスにより利用されている記録装置の容量を*[１ヶ月に１度]* 確認すること。

(2) 部局技術担当者は、メールボックスの容量がサーバ装置の運用に問題が生ずるほど大きい場合には、メールボックスの整理を行い、サーバ装置の正常な運用を確保すること。

《対象：アカウント管理を行う者 該当項目：7》

7. 電子メールサーバのセキュリティ維持のための対策

7.1 メールアドレス発行・削除に伴うアカウント管理

(1) アカウント管理を行う者は、部局技術責任者からメールアドレスの発行を指示された場合には、以下の事項に注意してメールアドレスを発行すること。なお、当該指示のないメールアドレスを発行しないこと。

・MRA が動作するサーバ装置上に、当該メールアドレスに対応するメールボックス、及び当該メールボックスから電子メールを取得するための識別符号（ユーザ ID）を作成し、当該識別符号に初期パスワードを設定すること。
また、設定する初期パスワードについて、以下の事項を考慮すること。
○８文字以上とすること。
○２以上のアルファベットと１つ以上の非アルファベットを含むこと。
○４つの異なる文字を含むこと。

○辞書にある言葉や一般的な言葉を単独で使用しないこと。

【電子メールの送信時に主体認証を行う場合（強化遵守事項）】

・MSA が動作するサーバ装置上に、当該メールアドレスに対応する電子メールを送信するための識別符号（ユーザ ID）を作成し、当該識別符号に初期パスワードを設定すること。
初期パスワードについては、MRA における考慮事項に準じて設定すること。
・当該識別符号及び初期設定のパスワードを、利用者等に連絡する際には、封書で直接手渡しする等、他の者に知られない安全な方法を用いること。

(2) アカウント管理を行う者は、メールアドレスを発行する際に、以下の事項を発行する利用者等に通知すること。
・共有識別符号（共有ユーザ ID）、共有ではない識別符号（共有ではないユーザ ID）の別。

【部局技術責任者が、初回ログイン時に初期パスワードを変更させると判断した場合】

・初期設定のパスワードを速やかに変更すること。

(3) アカウント管理を行う者は、部局技術責任者からメールアドレスの削除を指示された場合には、以下の事項に注意してメールアドレスを削除すること。
・MRA が動作するサーバ装置上に作成した、当該メールアドレスに対応する受信用識別符号（受信用ユーザ ID）及びメールボックスを削除すること。

【電子メールの送信時に主体認証を行う場合（強化遵守事項）】

・MSA が動作するサーバ装置上に作成した、当該メールアドレスに対応する送信用識別符号（送信用ユーザ ID）を削除すること。
・当該メールアドレスに関する転送等の設定を無効にすること。
・不要な識別符号（ユーザ ID）の有無を確認し、不要な識別符号が発見された場合には、当該識別符号を無効にすること。

(4) アカウント管理を行う者は、電子メールの受信時に行う主体に対して、識別符号（ユーザ ID）に対応した電子メールアドレスのメールボックスに限りアクセスできるようにすること。

【識別符号（ユーザ ID）の発行記録を取得する場合（強化遵守事項）】

(5) アカウント管理を行う者は、メールアドレスの発行に伴い利用者等に識別符号（ユーザ ID）を付与した場合には、当該利用者等及び当該メールアドレスを記録すること。当該

記録を消去する場合には、部局総括責任者から事前の承認を得ること。

【識別符号（ユーザ ID）の再利用を禁止する場合（強化遵守事項）】

(6) アカウント管理を行う者は、メールアドレスの発行に伴って利用者等に付与した識別符号（ユーザ ID）について、当該識別符号を削除した場合であっても、別の利用者等に対して同一の識別符号を発行しないこと。

《対象：部局技術責任者 該当項目：8、9》

8. 電子メールサーバのセキュリティ維持のための対策

8.1 主体認証

(1) 部局技術責任者は、当該電子メールサーバにおける主体認証において共有識別符号（共有ユーザ ID）の利用許可について、その必要性を判断すること。

(2) 部局技術責任者は、共有識別符号の必要性に関する判断の結果を、部局技術担当者に周知徹底すること。

8.2 証跡管理

(1) 部局技術責任者は、証跡を改ざん、漏えい、消去等から保護するため、以下の措置を講ずること。

- 証跡が保存されたファイルは電子メールサーバを管理する者しか参照できないように、アクセス制御する。
- 証跡が保存された外部記録媒体を施錠可能な棚等に保管し、当該棚等の鍵は部局技術責任者が管理する。

【取得した証跡の点検、分析及び報告を行う場合（強化遵守事項）】

(2) 部局技術責任者は、取得した証跡を*[３ヶ月に１度]* 点検及び分析し、その結果に応じて必要なセキュリティ対策を講じ、又は部局総括責任者に報告すること。

(3) 部局技術責任者は、証跡を点検及び分析する場合には、以下の事項を重点的に点検し、また通常と異なる状況が見られた場合には、より詳細に点検及び分析を行うこと。

- 不正中継による電子メール受信の拒否（MTA、MSA の証跡）
- パスワードクラックによる多数の主体認証の失敗（MRA の証跡）

【電子メールの送信時に主体認証を行う場合（強化遵守事項）】

- パスワードクラックによる多数の主体認証の失敗（MSA の証跡）

8.3 セキュリティホール対策

(1) 部局技術責任者は、部局技術担当者が入手したセキュリティホールに関連する情報から、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を作成すること。
- 対策の必要性
- 対策方法
- 対策方法が存在しない場合の一時的な回避方法
- 対策方法又は回避方法が情報システムに与える影響
- 対策の実施予定
- 対策テストの必要性
- 対策テストの方法
- 対策テストの実施予定

(2) 部局技術責任者は、作成したセキュリティホール対策計画に基づいて、部局技術担当者にセキュリティホール対策の実施を指示すること。

(3) 部局技術責任者は、入手したセキュリティホールに関連する情報に関して、必要に応じて、電子メールサービス提供ソフトェアを運用管理している他の部局技術責任者と共有すること。

8.4 サービス不能攻撃対策

(1) 部局技術責任者は、部局技術担当者からサービス不能攻撃を検出した旨の報告を受けた場合には、定められた手順に従って対処すること。

9. メールアドレスの発行・削除における注意事項

9.1 メールアドレス発行における注意事項

(1) 部局技術責任者は、*[教務又は庶務担当者]* から利用者等の入学・転入の連絡があり、当該利用者等にメールアドレスを発行する必要がある場合には、アカウント管理を行う者にメールアドレス発行に伴うアカウント管理の指示を出すこと。

(2) 部局技術責任者は、電子メールの送受信に関する証跡の取得、保存、点検及び解析を行う可能性があることを、メールアドレスを発行する利用者等にあらかじめ説明すること。

9.2 メールアドレス削除における注意事項

(1) 部局技術責任者は、*[教務又は庶務担当者]* から利用者等の卒業・転出の連絡があり、当該利用者等にメールアドレスを発行していた場合には、アカウント管理を行う者にメールアドレス削除に伴うアカウント管理の指示を出すこと。

《対象：部局総括責任者 該当項目：10》

10. 電子メールサーバのセキュリティ維持のための対策

10.1 不正プログラム対策

(1) **部局総括責任者は、電子メールサービスにおける不正プログラム対策の状況を適宜把握し、その見直しを行うこと。**

【外部の専門家の支援を受ける場合（強化遵守事項）】

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

A3109 人事異動の際に行うべき情報セキュリティ対策実施手順

1. 目的

本学における情報セキュリティ対策は、それに係るすべての教職員・学生等が、その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、ポリシー及び関連する実施規程・手順に基づき、負うべき責務を全うすることで適切に実施される。このため、それを実施するための基礎となる組織・体制については、教職員・学生等の採用・入学、退職・卒業、配置換え等が行われた際においても、適切に整備されている必要がある。さらに、適切に整備された組織・体制の下で、教職員・学生等に対する情報セキュリティに係る教育、権限の付与及び失効等を適時に行うことが情報セキュリティを確保する上で不可欠である。

本手順は、人事異動等に伴い情報セキュリティの観点から行う手続を定め、もって本学における情報セキュリティの確保に資することを目的とする。

2. 適用範囲

2.1 本手順の対象者

本手順は、全学総括責任者、全学実施責任者、部局総括責任者、部局技術責任者、部局技術担当者、職場情報セキュリティ責任者(以降、上司を含む)、権限管理を行う者、庶務担当者及びすべての教職員・学生等について、それぞれの役割において行うべき措置を定める。

補足：本手順においては、すべての教職員・学生等は原則として職場又は上司に属し、情報セキュリティ対策の実施について職場情報セキュリティ責任者等の支援を受けることができるものと想定している。このため、職場に属さない幹部等においては、支援を担当する職場情報セキュリティ責任者等を便宜的に定めた上で本手順を適用する必要がある。

2.2 本手順を適用する人事異動等の範囲

本手順は、人事異動発令に基づく採用、退職、配置換え等や学生等の入学、卒業における情報セキュリティ対策を定めるものである。

なお、本手順では、採用、他職場からの配置換え及び学生等の入学をあわせて「転入」といい、退職、他職場への配置換え及び学生等の卒業をあわせて「転出」といい、転入と転出をあわせて「人事異動等」という。

【手順利用者への補足説明】

大学の運用により、人事発令を伴わない職務の変更により、権限の付与及び失効その他の情報セキュリティ対策の実施が求められる状況が生ずる場合がある。このため、必要に応じて、職務の変更に係る情報を把握する者及び手順を追加又は変更し、大学の運用にあわせた手順とすること。

3. 人事異動等の把握と通知

(1) 人事異動等の情報は、各職場の庶務担当者が把握する。

(2) 各職場の庶務担当者ごとに、人事異動等の情報を通知する先の者を別表1のとおりに定める。

(3) 別表1は、全学実施責任者が作成し、常に最新の内容に維持する。

（別表1は各職場の庶務担当者ごとに人事異動等の情報を通知する先の者を一覧で示すものであるが、本雛形では省略している。全学総括責任者、全学実施責任者、部局総括責任者、部局技術責任者、部局技術担当者、職場情報セキュリティ責任者及び権限管理を行う者にもれなく通知されるように、庶務担当者ごとに通知先の者を定める。）

(4) 各職場の庶務担当者は、把握した教職員・学生等の人事異動等の情報を、速やかに別表1に記載する者全員に通知すること。

4. 人事異動等に伴う措置

人事異動等の情報の通知を受けた者は、以下の措置を採ること。

4.1 全学総括責任者が行う措置

4.1.1 特定の責任者等の転出に伴う措置

(1) 情報セキュリティ対策に係る体制の維持

全学総括責任者は、以下の者の転出に際して、後任者を指名すること。

- 情報セキュリティアドバイザー
- 全学情報システム運用委員会委員長及び委員
- 情報セキュリティ監査責任者
- 全学実施責任者、部局総括責任者
- 情報セキュリティに関する障害等に備えた体制に含まれる者

4.2 全学実施責任者が行う措置

4.2.1 特定の責任者等の転出に伴う措置

(1) 連絡網の維持

全学実施責任者は、部局総括責任者、部局技術責任者、部局技術担当者又は職場情報セキュリティ責任者の転出に際して、後任者を確認し、連絡網を更新すること。

(2) 緊急連絡網の維持

全学実施責任者は、特に重要と認めた情報システムについて整備している緊急連絡網に記載した部局技術責任者、部局技術担当者又はその他の者の転出に際して、後任者を確認し、緊急連絡網を更新すること。

4.3 部局総括責任者が行う措置

4.3.1 特定の責任者等の転出に伴う措置

(1) 情報セキュリティに係る体制の維持

部局総括責任者は、部局技術責任者又は職場情報セキュリティ責任者の転出に際して、後任者を指名すること。また、後任者を全学実施責任者に報告すること。

4.4 部局技術責任者が行う措置

4.4.1 教職員・学生等の転入に伴う措置

(1) 電子計算機を管理する教職員・学生等及び利用者を特定するための文書への登録

部局技術責任者は、転入する教職員・学生等に電子計算機を管理又は利用させるに際して、電子計算機を管理する教職員・学生等及び利用者を特定するための文書に必要な事項を反映し、また、当該変更の記録を保存すること。

【安全区域へ立ち入る者を承認する手続を整備している場合（強化遵守事項）】

(2) 安全区域立入者の登録

部局技術責任者は、安全区域へ立ち入る者を承認する手続を整備している場合であって、転入する教職員・学生等を安全区域に継続的に立ち入る者として承認するときは、氏名、所属、承認日、期間及び承認事由を含む事項を定められた書面に記録すること。

【安全区域へ立ち入る者及び当該区域から退出する者の主体認証を行うための措置を 講じている場合（強化遵守事項）】

（例えば、身分証明カードとセキュリティドアによる入退室管理を行っている場合）

(3) 安全区域の認証のための措置への登録

部局技術責任者は、安全区域へ立ち入る者又は当該区域から退出する者の主体認証を行うための措置を講じている場合であって、転入する教職員・学生等に安全区域への立入りを許可するときは、当該措置において立ち入りを許可する者として登録すること。

4.4.2 特定の責任者等及び教職員・学生等の転出に伴う措置

(1) 部局技術担当者の転出

部局技術責任者は、部局技術担当者の転出に際して、後任者を指名すること。また、後任者を全学実施責任者に報告すること。

(2) 権限管理を行う者の転出

部局技術責任者は、権限管理を行う者の転出に際して、後任者を指名すること。

(3) 電子計算機を管理する教職員・学生等及び利用者の登録削除

部局技術責任者は、電子計算機を管理する教職員・学生等又は利用者として登録された教職員・学生等の転出に際して、遅滞なく、電子計算機を管理する教職員・学生等及び利用者を特定するための文書に反映し、また、当該変更の記録を保存すること。

【安全区域へ立ち入る者を承認する手続を整備している場合（強化遵守事項）】

(4) 安全区域立入者の登録削除

部局技術責任者は、安全区域へ継続的に立ち入る者を承認する手続を整備している場合は、安全区域に継続的に立ち入る者として承認した教職員・学生等の転出に際して、遅滞なく、氏名、所属、承認日、期間及び承認事由を含む事項を記録した書面に必要な事項を反映し、当該変更の記録を保存すること。

【安全区域へ立ち入る者の主体認証を行うための措置を講じている場合（強化遵守事項）】

（例えば、身分証明カードとセキュリティドアによる入退室管理を行っている場合）

(5) 安全区域認証の登録削除

部局技術責任者は、安全区域へ立ち入る者の主体認証を行うための措置を講じている場合は、安全区域への立入りを許可している教職員・学生等の転出に際して、遅滞なく、当該措置における登録を削除すること。

(6) 本学外での情報処理のための機器の返却

部局技術責任者は、本学外での情報処理を行っている教職員・学生等の転出に際して、端末、媒体等の返却を含む当該情報処理を終了するときの手続に従った措置を講じさせること。

(7) 大学支給以外の情報システムによる情報処理に関する情報の消去

部局技術責任者は、大学支給以外の情報システムによる情報処理を行っている教職員・学生等の転出に際して、情報の消去を含む当該情報処理を終了するときの手続に従った措置を講じさせること。

4.5 部局技術担当者が行う措置

4.5.1 教職員・学生等の転入に伴う措置

(1) 通信回線の利用の管理

部局技術担当者は、教職員・学生等の転入に際して、当該教職員・学生等に通信回線を利用させる場合には、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードの対応、及び通信回線の利用部局を含む事項を管理するための文書に、当該転入に伴う変更を反映すること。

4.5.2 教職員・学生等の転出に伴う措置

(1) 通信回線の利用の管理

部局技術担当者は、教職員・学生等の転出に際して、当該教職員・学生等に通信回線を利用させていた場合には、通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードの対応、及び通信回線の利用部局を含む事項を管理するための文書に、当該転出に伴う変更を反映すること。

4.6 職場情報セキュリティ責任者が行う措置

4.6.1 教職員・学生等の転入に伴う措置

(1) 転入者への教育

職場情報セキュリティ責任者は、教職員・学生等の転入に際して、3か月以内に情報セキュリティ対策の教育を受講させること。

4.6.2 教職員・学生等の転出に伴う措置

(1) 本学外での情報処理のための機器の返却

職場情報セキュリティ責任者は、大学外での情報処理を行っている教職員・学生等の転出に際して、端末、媒体等の返却を含む当該情報処理を終了するときの手続に従った措置を講じさせること。

(2) 大学支給以外の情報システムによる情報処理に関する情報の消去

職場情報セキュリティ責任者は、大学支給以外の情報システムによる情報処理を行っている教職員・学生等の転出に際して、情報の消去を含む当該情報処理を終了するときの手続に従った措置を講じさせるここと。

4.7 権限管理を行う者が行う措置

4.7.1 教職員・学生等の転入に伴う措置

(1) 識別コード及び主体認証情報（パスワード等）の付与

権限管理を行う者は、教職員・学生等の転入に際して、利用させる電子計算機、アプリケーションソフトウェア等ごとに識別コード及び主体認証情報を発行すること。

(2) 主体認証情報格納装置の交付

権限管理を行う者は、教職員・学生等の転入に際して、主体認証情報格納装置を利用させる場合には、これを交付すること。

(3) アクセス制御の設定

権限管理を行う者は、教職員・学生等の転入に際して、必要最小限の範囲に限って情報システムにおけるアクセス制御に係る設定をすること。

【行政事務従事者と識別コードの対応の記録を保存する場合（強化遵守事項）】

(4) **教職員・学生等と識別コードの対応の記録**

権限管理を行う者は、教職員・学生等の転入に際して、当該教職員・学生等と付与した識別コードの対応を記録し、保存すること。

(5) **識別コード及びアクセス制御設定の見直し**

権限管理を行う者は、人事異動等その他識別コードを追加する機会に、不要な識別コード及び不適切なアクセス制御設定の有無を点検すること。

4.7.2 **教職員・学生等の転出に伴う措置**

(1) **識別コードの無効化**

権限管理を行う者は、教職員・学生等の転出に際して、利用させる電子計算機、アプリケーションソフトウェア等ごとに付与していた当該主体の識別コードを遅滞なく無効にすること。

(2) **主体認証情報格納装置の返還**

権限管理を行う者は、主体認証情報格納装置を交付していた教職員・学生等の転出に際して、当該主体認証情報格納装置を返還させること。

(3) **識別コード及びアクセス制御設定の見直し**

権限管理を行う者は、人事異動等その他識別コードを無効化する機会に、不要な識別コード及び不適切なアクセス制御設定の有無を点検すること。

4.8 **教職員・学生等が行う措置**

4.8.1 **自らの転入に伴う措置**

(1) **教育の受講**

教職員・学生等は、自らの転入に際して、情報セキュリティ対策の教育の受講方法について職場情報セキュリティ責任者に確認すること。

4.8.2 **自らの転出に伴う措置**

(1) **本学外での情報処理のための機器の返却**

本学外での情報処理を行っている教職員・学生等は、自らの転出に際して、大学外での情報処理を行っていた場合には、端末及び媒体等の返却を含む当該情報処理を終了するときの手続に従った措置を講ずること。

(2) **本学支給以外の情報システムによる情報処理に関する情報の消去**

本学支給以外の情報システムによる情報処理を行っている教職員・学生等は、自らの転出に際して、情報の消去を含む当該情報処理を終了するときの手続に従った措置を講

ずること。

5. 履行状況の確認

(1) 履行状況の確認

全学実施責任者は、前章までの規定の履行状況を定期的に確認すること。なお、当該確認は、自己点検の一部として行うことをもって代えることができる。

6. 本手順に関する相談窓口

(1) 本手順の対象者は、緊急時の対応又は本手順の内容を超えた対応が必要とされる場合には、情報セキュリティ体制の上位者に相談し、指示を受けること。

(2) 本手順の対象者は、本手順の内容について不明な点又は質問がある場合には、情報セキュリティ体制の上位者に連絡し、回答を得ること。

A3110 機器等の購入における情報セキュリティ対策実施手順（策定手引書）

1. 本書の目的

本書は、情報機器及びソフトウェア（以下機器等という。）の購入に伴う情報セキュリティ関係の手続を定める手順（以下「機器等の購入における情報セキュリティ対策実施手順」という。）を全学実施責任者が整備するための手引書である。

本学においては、ポリシー及び実施規程を整備することが求められている一方で、本学の研究教育業務を円滑に遂行するために必要な手順を具体的に示した実施手順の整備が望まれることから、当該実施手順に従い業務を行えば結果としてポリシー及び実施規程も遵守することとなる手順書を策定することが適切である。「機器等の購入における情報セキュリティ対策実施手順」は、これらの実施手順の一つとして策定し、機器等の購入における情報セキュリティ対策の実施に適用するものである。

本学においてサーバ装置、端末、通信回線装置、ソフトウェアその他の機器等を購入して業務に使用する場合には、これらの機器等に情報を保有し、また機器等を介して利用者が本学の情報へアクセスすることとなるため、必要なセキュリティ機能が装備されていない場合や購入後に情報セキュリティ対策が継続的に行えない場合は、情報セキュリティが維持できなくなるおそれがある。このため、機器等の購入に当たっては、情報セキュリティ維持の観点から適切な機器等を選定することが求められる。

本書は、これらの背景の下で、「機器等の購入における情報セキュリティ対策実施手順」に含めるべき事項を具体的に示し、もって適切な規定の整備に資することを目的とする。

2. 手順に記載すべき事項

「機器等の購入における情報セキュリティ対策実施手順」には、以下の事項を具体化して記載すること。

2.1 情報システム運用・管理規程に定める機器等の購入に係る遵守事項

なし。

2.2 セキュリティ確保に係るその他の留意事項

なし。

3. 文書構成例

「機器等の購入における情報セキュリティ対策実施手順」は、以下の文書構成で作成することが考えられる。

1 本手順の目的
2 本手順の対象者

4. 策定する上での留意事項

「機器等の購入における情報セキュリティ対策実施手順」は、以下のことに留意して策定する。

4.1 適用範囲

「機器等の購入における情報セキュリティ対策実施手順」は、本学における機器等の購入に適用するものとする。機器等とは、情報機器等及びソフトウェアをいう。

機器等の例：

- サーバ装置関連
  - ○ サーバ装置
  - ○ オペレーティングシステム（OS）
  - ○ ミドルウェア（DBMS、アプリケーションサーバ、グループウェア、運用管理ソフトウェア、セキュリティ対策ソフトウェア等）
  - ○ 汎用アプリケーションプログラム（ウェブサーバ、電子メールサーバ等）
  - ○ 業務プログラム
  - ○ その他
- 端末関連（PC を含む）
  - ○ 端末装置
  - ○ オペレーティングシステム（OS）
  - ○ ミドルウェア（運用管理ソフトウェア、セキュリティ対策ソフトウェア等）
  - ○ 汎用アプリケーションプログラム（ブラウザ、メーラ、文書処理プログラム等）
  - ○ 業務プログラム
  - ○ その他
- 通信回線装置
  - ○ ファイアウォール

- ○ ルータ、スイッチ
- ○ その他

● 複合機（印刷機能及びファクシミリ機能をあわせ持つ機器等）

4.2 求められる情報セキュリティ対策

機器等の購入においては以下の情報セキュリティ対策が求められるため、これらを機器等の選定基準に含めること。

(1) 当該機器が、求められるセキュリティ機能要件を満足するセキュリティ機能を持つこと。

(2) 情報セキュリティの維持のためセキュリティ修正（脆弱性を解消するための修正）を適用する必要がある機器等の場合には、以下の条件を満たすこと。

- 納品時に必要なセキュリティ修正が適用されていること。
- 納品後に必要なセキュリティ修正が継続的に提供され、適用できること。

(3) 情報セキュリティの維持に保守・点検等が必要な機器等の場合には、納品後に保守・点検等が購入先又は他の事業者により行われること。

4.3 情報システムとの関係

機器等は、情報システムの構成要素となる。情報システムにおけるセキュリティ要件の一部は個々の機器等に対するセキュリティ機能要件となるため、機器等の購入においては、当該セキュリティ機能要件を満足するセキュリティ機能を持つものを選定する必要がある。なお、情報システムにおけるセキュリティ要件の全体は、個々の機器等が有するセキュリティ機能のみによって満足されるわけではなく、機器等が保有する機能を利用すること並びに、安全区域等の物理的対策、組織及び人の運用による対策その他情報システムをとりまく様々な対策を実施することにより満足されることとなる。

情報システムの構築とは別に購入する機器等においても、ネットワークを通して情報システムに接続し、又は外部記録媒体により情報の移入・移出を行う等により情報システムの構成要素となるため、情報システムの観点から購入における情報セキュリティ対策の実施が求められる。

4.4 機器等の種類に応じた対策の適用

求められる情報セキュリティ対策及び選定基準については、当該対策の確実な実施及び事務の軽減を図るため、機器等の種類ごとに標準的なセキュリティ要件及び選定基準を示し、部局技術責任者の利用に供することが望ましい。

4.5 汎用製品等の選定における判断結果の記録

セキュリティ要件への対応については、必ずしも機器等の購入の都度判断する必要はない。多くの場合に過去の判断結果が有効であるため、判断結果の記録を残すことにより、事後の負担を軽減することができる。特に、汎用のサーバ装置、端末及びソフトウェアについては、過去の判断結果が参考になる場合が少なくないものと想定される。

5. 参考資料

「機器等の購入における情報セキュリティ対策実施手順」の策定に際しては、以下の資料が参考となる。

(1) IT セキュリティ評価及び認証制度に関する資料

独立行政法人情報処理推進機構（IPA）

http://www.ipa.go.jp/security/jisec/index.html

本参考資料は、IT 製品・システムにセキュリティ機能が実装されていることを国際的に合意された規格である ISO/IEC 15408 (Common Criteria) に基づき評価し、認証するための制度に関して解説したものである。

(2) 『情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書』

内閣官房情報セキュリティセンター、2006 年 6 月

本参考資料の「付録 C IT セキュリティ評価及び認証制度を活用した機器等の購入について」に、機器等の購入において IT セキュリティ評価及び認証制度及び認証製品リストを利用する際の考慮事項及び参考情報が記載されている。

6. 雛形の利用方法

別紙１の雛形を参考にして、「機器等の購入における情報セキュリティ対策実施手順」を策定すると効率的である。別紙１の雛形は、前記 2 の実施手順に記載すべき事項を、前記 3 の文書構成例の枠組みの中に記載したものである。

6.1 雛形において想定する前提

本雛形は、以下を前提として記述している。

機器等の購入においては求めるセキュリティ要件を満足するか否かを判断することになるが、必ずしも購入の都度判断する必要はなく、過去の判断を参考にしてよい場合が多い。このため、以下の方法により手続の簡略化を図っている。

(1) 機器等の種類ごとに標準的に求めるセキュリティ要件を府省庁において策定し、利用する。

(2) セキュリティ要件に照らした判断の結果を記録し、事後の参考とする。

6.2 手直しポイント

(1) 雛形において*[・・・]* 形式で示す設定値（組織名等）については、各大学内の定めに合わせる。

(2) 既存の調達関連その他の規定との整合性を考慮し、適切に統合、相互参照する。

別紙１　機器等の購入における情報セキュリティ対策実施手順　雛形

本書の位置付け

本書は、「機器等の購入における情報セキュリティ対策実施手順」を策定する場合の雛形であり、「機器等の購入における情報セキュリティ対策実施手順 策定手引書」の 2 に示す手順に記載すべき事項を、同 3 に示す文書構成例の枠組みの中に記載したものである。

本書の利用方法

本書において想定する前提

本雛形は、以下を前提として記述している。

- 機器等の購入においては求めるセキュリティ要件を満足するか否かを判断ことになるが、必ずしも購入の都度判断する必要はなく、過去の判断を参考にしてよい場合が多い。このため、以下の方法により手続の簡略化を図っている。
  - 機器等の種類ごとに標準的に求めるセキュリティ要件を本学において策定し、利用する（付録）。
  - セキュリティ要件に照らした判断の結果を記録し、事後の参考とする。

手直しポイント

「機器等の購入における情報セキュリティ対策実施手順」の策定に当たり、以下の点について手直しをする必要がある。

① 雛形において*[・・・]* 形式で示す設定値（組織名等）については、各大学の定めに合わせる。

② 既存の調達関連その他の規定との整合性を考慮し、適切に統合、相互参照する。

1. 本手順の目的

本学において情報機器及びソフトウェア（以下機器等という。）を購入して業務に使用する場合には、これらの機器に情報を保有し、また機器を介して利用者が本学の情報へアクセスすることとなるため、必要なセキュリティ機能が装備されていない場合や購入後に情報セキュリティ対策が継続的に行えない場合は、情報セキュリティが維持できなくなるおそれがある。このため、機器等の購入に当たっては、情報セキュリティ維持の観点から適切な機器等を選定することが求められる。

本手順は、機器等の購入において情報セキュリティの観点から行うべき手続を定め、もって本学における情報セキュリティの確保に資することを目的とする。

2. 本手順の対象者

本手順は、購入する機器等を構成要素とすることとなる情報システムの部局技術責任者を対象とする。

3. 本手順を適用する機器等の購入の範囲

(1) 本手順は、本学における機器等の購入に適用する。
(2) 本手順における機器等の購入には、リース契約等、売買契約以外の方法による機器等の調達を含む。
(3) 本手順における機器等の購入には、情報システムの構築を外部委託により行う場合であって、当該委託にあわせて機器等を購入する場合を含む。

4. 機器等に求めるセキュリティ要件

4.1 求めるセキュリティ要件の原則

購入する機器等は、原則として、情報セキュリティの観点から以下のセキュリティ要件を満たすものであること。

(1) 求められるセキュリティ機能を持つこと

当該機器等に求められるセキュリティ機能要件を満足するセキュリティ機能を持つこと。

【手順利用者への補足説明】

機器等は、情報システムの構成要素となる。情報システムにおけるセキュリティ要件の一部は、個々の機器等に対するセキュリティ機能要件となるため、機器等の購入においては、当該セキュリティ機能要件を満足するセキュリティ機能を持つものを選定する必要がある。なお、情報システムにおけるセキュリティ要件の全体は、個々の機器等が有するセキュリティ機能のみによって満足されるわけではなく、機器等が保有する機能を利用すること並びに、安全区域等の物理的対策、組織及び人の運用による対策その他当該情報システムをとりまく様々な対策を実施することにより満足されることとなる。

(2) セキュリティ修正が提供されること

情報セキュリティの維持のためセキュリティ修正（脆弱性を解消するための修正）を適用する必要がある機器等の場合には、以下の条件を満たすこと。

- 納品時に必要なセキュリティ修正が適用されていること。
- 納品後に必要なセキュリティ修正が継続的に提供され、適用できること。

UNIX®、Windows®を含むオープン系システムではなく、メインフレームシステム等で稼動するソフトウェアについては、その脆弱性が指摘されることは一般にないため、セキュリティ修正の提供は求める必要がない。

(3) その他の保守・点検等が行われること

以下の保守・点検等のうち、部局技術責任者が情報セキュリティの確保に必要と認めるものが適用可能であること。

- ハードウェアの保守・点検等
- ソフトウェア及びファームウェアの修正及び更新の提供
- 部局技術責任者が必要と認めた機器等の脆弱性検査その他の保守・点検等

4.2 標準的に求めるべきセキュリティ要件

前節の原則に基づき、機器等に標準的に求めるセキュリティ要件を「機器等に標準的に求めるセキュリティ要件」のとおりに定める。本要件は、全学実施責任者が定め、維持する。「機器等に標準的に求めるセキュリティ要件」については、付録を参照されたい。

なお、「5 機器等の選定」の手続において本要件を満たすものと確認した機器等について確認したことの記録を本要件とあわせて維持し、事後の利用に供することも、手続の簡略化に有効である。

4.3 機器等に求めるセキュリティ要件の決定

部局技術責任者は、機器等の選定に当たり、以下の手順で当該機器等に求めるセキュリティ要件を定めること。

① 当該機器等の利用方法に照らして、「機器等に標準的に求めるセキュリティ要件」を採用することが適切であるか否かを判断すること。

② 「機器等に標準的に求めるセキュリティ要件」を採用しない場合には、以下の手続を踏むこと。

- 同表中「(1) セキュリティ機能を持つこと」の内容を採用しない場合には、当該機器等に求めるセキュリティ機能要件を定めた上で、これに基づき求めるセキュリティ機能を定めること。
- 同表中「(2) セキュリティ修正が提供されること」の内容を採用しない場合には、それに代わるセキュリティ要件を定めること。

- 同表中「(3) その他の保守・点検等が行われること」の内容を採用しない場合には、それに代わるセキュリティ要件を定めること。

5. 機器等の選定

① 部局技術責任者は、「4.3 機器等に求めるセキュリティ要件の決定」で定めたセキュリティ要件を情報セキュリティ以外の要件に加味して機器等を選定すること。
なお、「機器等に標準的に求めるセキュリティ要件」を採用した場合で、当該要件を満たすものであると確認した機器等について確認したことの記録を残し、事後の利用に供することは、手続の簡略化に有効である。

② 部局技術責任者は、機器等について満足すべきセキュリティ要件があり、それを実現するためのセキュリティ機能の要求仕様がある場合であって、総合評価落札方式により購入を行うときは、当該要求仕様への対応について IT セキュリティ評価・認証制度による認証を取得しているかどうかを評価項目として活用すること。

- IT セキュリティ評価・認証制度とは、IT 製品・システムにセキュリティ機能が実装されていることを国際的に合意された規格である ISO/IEC 15408 (Common Criteria) に基づき評価し、認証するための制度であり、独立行政法人情報処理推進機構（IPA）が運営している。
  http://www.ipa.go.jp/security/jisec/index.html
  認証を取得している場合には、製品名等製品を特定する情報及び認証番号を購入先の事業者に報告させること。認証取得は、上記ウェブページにある認証製品リストで確認することができる。
  認証取得の範囲が、当該機器等に求めるセキュリティ機能要件と合致していることを確認する必要がある。

  なお、IT セキュリティ評価及び認証制度に基づく認証の取得を製品の選択に利用することについては、以下の資料もあわせて参照されたい。
  1. 「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」（内閣官房情報セキュリティセンター、2006 年 6 月）

6. 機器等の納入時の確認

(1) 部局技術責任者は、機器等の納入を受けるに際して、当該機器等に求めるセキュリティ要件を満たしていることを必要に応じて確認し、その結果を納品検査における判断に加えること。確認する事項は、以下に挙げるもののうち必要と認めるものとすること。

- 求めるセキュリティ機能が装備されていることを、納入される仕様書の査閲、機器等の操作等により確認する。
- セキュリティ修正が最近のものまで適用されていることを、納入される仕様書の査

閲等により確認する。

- 保守・点検等が行われることを、納入される仕様書の査閲等により確認する。

7. 機器等の保守・点検等

① 部局技術責任者は、情報セキュリティ対策に関する保守・点検等が必要であると認めた場合には、機器等の購入先又は他の事業者に保守・点検を行わせること。
当該手続は、学内において行うこととした事項を除き、[「外部委託における情報セキュリティ対策実施手順」]に従うこと。

8. 本手順に関する相談窓口

(1) 部局技術責任者は、緊急時の対応又は本手順の内容を超えた対応が必要とされる場合には、統括情報セキュリティ責任者に相談し、指示を受けること。
(2) 部局技術責任者は、本手順の内容について不明な点又は質問がある場合には、統括情報セキュリティ責任者に連絡し、回答を得ること。

付録　機器等に標準的に求めるセキュリティ要件

「4.2 標準的に求めるべきセキュリティ要件」の内容を以下のとおりに定める。表中の(1)、(2)及び(3)の意味については「4.1 求めるセキュリティ要件の原則」を参照されたい。

	機器等の種別		(1) セキュリティ機能をもつこと	(2) セキュリティ修正が提供されること	(3) その他の保守・点検等が行われること
1	サーバ装置関連	サーバ装置（ハードウェア）	―	―	保守・点検等がなされること。
2		オペレーティングシステム（OS）	当該ソフトウェアについて「取り扱う情報」「管理者」及び「利用者」に着目した、 ①主体認証機能、 ②アクセス制御機能、 ③権限管理機能及び ④証跡管理機能 を持つこと。 なお、UNIX®系OS（Linux®を含む。）及びWindows®は、これらの機能を持つものと認められる。	必要 ただし、メインフレームシステム等、オープン系システム以外のものには適用しない。	ソフトウェアの修正及び更新が提供されること。
3		ミドルウェア（DBMS、アプリケーションサーバ、グループウェア、運用管理ソフトウェア、セキュリティ対策ソフトウェア等）			
4		汎用アプリケーションプログラム（メールサーバ、ウェブサーバ等）			
5		業務プログラム	当該プログラムごとに判断すること。	個別に必要性を判断すること。	個別に必要性を判断すること。
6	端末関連	端末（ハードウェア）	―	―	保守・点検等がなされること。
7		オペレーティングシステム（OS）	当該ソフトウェアについて「取り扱う情報」「管理者」及び「利用者」に着目した、 ①主体認証機能、 ②アクセス制御機能、 ③権限管理機能及び ④証跡管理機能 を持つこと。 UNIX®系OS（Linux®を含む。）及びWindows®は、これらの機能を持つものと認められる。	必要	ソフトウェアの修正及び更新が提供されること。
		ミドルウェア（運用管理ソフトウェア、セキュリティ対策ソフトウェア等）		必要	
8		汎用アプリケーションプログラム（ブラウザ、メーラ、文書処理プログラム等）		必要	
9		業務プログラム	当該プログラムごとに判断すること。	個別に必要性を判断すること。	
10	通信回線装置	ファイアウォール	上記「サーバ装置関連」のミドルウェアと同じ。	必要	ソフトウェア及びファームウェアの修正及び更新が提供されること。
		ルータ、スイッチ等	装置ごとに必要なセキュリティ機能を判断する必要がある。	個別に必要性を判断すること。通信プログラムを取り扱うファームウェア等に関して修正が必要になる場合がある。	
11	複合機（印刷機能及びファクシミリ機能をあわせ持つ機器等）		省庁内LANを外部ネットワークに接続することとなる可能性に留意し、要求仕様を策定すること。	個別に必要性を判断すること。汎用のOSを搭載している場合等に必要になり得る。	個別に必要性を判断すること。

A3111 外部委託における情報セキュリティ対策実施手順

第Ⅰ部 実施手順

1. 目的

本学において情報処理業務を外部委託により行う場合には、委託先における業務の遂行を委託元が直接に指揮命令することがなく、また当該業務に必要な情報を委託元から提供して委託先に取り扱わせるため、情報セキュリティを確保する観点から、委託元としての業務を行う者が委託先による業務の遂行を契約等により適切に管理する必要がある。

本書は、情報処理業務を外部委託により行う場合に、委託元としての業務を行う部局技術責任者が遵守すべき事項を定め、もって外部委託により行う情報処理業務の遂行において必要な情報セキュリティ水準を確保することを目的とする。

2. 本書の対象

本書は、委託元としての業務を行う部局技術責任者を対象としている。

なお、情報の加工・処理（「3.3 情報の加工・処理の外部委託」を参照。）及び情報の保存・運搬（「3.4 情報の保存・運搬の外部委託」）は、職場情報セキュリティ責任者の責任の下で行う場合がある。これらを外部委託により行う場合には、本書において部局技術責任者に求める事項を、職場情報セキュリティ責任者に求めることとなる。

3. 外部委託を行う業務の形態

本書においては、外部委託により行う業務を以下のとおりに分類している。なお、部局技術責任者は、これ以外の業務形態についても、本書の内容に準じて委託元としての業務を行うこと。

3.1 情報システム等の構築・開発の外部委託

情報システムの構築又はソフトウェアの開発（これらをあわせて「情報システム等の構築・開発」という。）を外部委託により行う場合である。

3.2 情報システムの運用・保守・点検の外部委託

情報システムの運用、保守又は点検を外部委託により行う場合であり、運用のみの外部委託、保守・点検の外部委託、運用・保守及び点検をあわせて外部委託する形態等がある。具体的には、次のようなものが想定される。

① 委託先が、本学内で、そこに設置された情報システムの運用・保守・点検を行う。いわゆる「オンサイトサービス」の利用である。

② 委託先の事業所から回線等を経由して本学内に設置した情報システムに接続し、委託先がその運用・保守・点検を行う。いわゆる「リモートサービス」の利用である。委託先が情報システムの運用を行うリモート運用サービス、情報システムやネットワークの稼動監視を行うリモート監視サービス、及びインターネットを通した不正アクセスを監視するセキュリティ監視サービス等がある。

③ 委託先の事業所内に本学の情報システムを設置し、委託先がその運用・保守・点検を行う。いわゆる「データセンター」の利用である。情報システムを構成する資産を本学が所有する場合と、委託先が所有する場合の両方を含む。

④ 委託先が提供する情報サービスを本学が利用する。いわゆる「アプリケーションサービスプロバイダ（ASP）」のサービスの利用である。レンタルウェブサーバの利用は、この一例である。

⑤ 委託先の事業所内に本学の情報システムを設置し、建屋の維持、入退室管理等の物理的管理と通信回線の維持を委託先に行わせ、情報システムのその他の運用・保守・点検の業務は本学が行う。いわゆる「ハウジングサービス」の利用である。

3.3 情報の加工・処理の外部委託

統計処理、集計処理、データエントリー及び媒体変換を含む情報の加工・処理を外部委託により行う場合である。

3.4 情報の保存・運搬の外部委託

バックアップデータ及び業務情報を含む情報の保存・運搬を外部委託により行う場合である。この場合には、委託先の事業者は、通常は倉庫又は運送に係る事業者である。

4. 外部委託における情報セキュリティ確保に関係する手続

情報処理業務を外部委託により行おうとする部局技術責任者は、以下の手続に従うこと。

(1) 外部委託により情報処理業務を行うことの可否の判断

外部委託により行う候補の情報処理業務がある場合に、情報セキュリティ確保の観点から、これを外部委託により行うことの可否を判断する。詳細は「5 外部委託により情報処理業務を行うことの可否の判断」を参照されたい。

(2) 調達における手続

調達において示す調達条件、委託先の選定基準、及び、当該業務の実施において委託先に行わせる事項に、情報セキュリティ確保のための事項を含める。詳細は「6 調達における手続」を参照されたい。

(3) 契約における手続

契約において定める委託元及び委託先双方の義務に、情報セキュリティ確保のための事項を含める。詳細は「7 契約における手続」を参照されたい。

(4) 委託先における情報処理業務実施中の手続
外部委託した情報処理業務の実施中に、契約で定めた情報セキュリティ確保のための義務を、委託元及び委託先双方で履行する。詳細は「8 委託先における情報処理業務実施中の手続」を参照されたい。

(5) 納品・検収における手続
外部委託した業務の終了時に、納品に関する検収手続において、契約で定めた情報セキュリティ確保のための義務を委託先が履行したことを確認する。詳細は「9 納品・検収における手続」を参照されたい。

5. 外部委託により情報処理業務を行うことの可否の判断

5.1 外部委託の可否の原則

(1) 重要な情報を取り扱う情報処理業務（付録1 を参照。）を外部委託により行うことは、情報漏えい等のリスクにかんがみ、これを原則として禁止する。
- 重要な情報とは、これが不適切に取り扱われた場合に、利用者の権利利益に重大な損害を与え、あるいは、利用者及び本学の安全に重大な懸念が生ずる情報をいう。

(2) 重要な情報を取り扱わない情報処理業務（付録1 を参照。）は、外部委託により行うことができる。この場合には、次章以降の規定に従うこと。

(3) 部局技術責任者は、付録1 に掲載されていない情報処理業務を外部委託により行うことを望む場合には、当該情報処理業務及び取り扱う情報について部局総括責任者に説明し、重要な情報を取り扱う情報処理業務に該当するか否かの判断を得ること。

(4) 部局総括責任者は、(3)項の判断の結果を全学実施責任者に報告し、付録1 の更新を求めること。全学実施責任者は、必要に応じて付録1 を更新すること。

(5) 部局技術責任者は、重要な情報を取り扱う情報処理業務を外部委託により行うことを特に望む場合には、想定される脅威及び実施可能な対策の有効性に基づくリスク分析を行うこと。その結果リスクが十分に低減できると判断する場合には、部局総括責任者に判断及びその根拠を報告し、当該情報処理業務を外部委託により行うことにつき許可を求めることができる。部局総括責任者の許可を得た場合には、指示された対策の実施を条件に、例外として、重要な情報を取り扱う情報処理業務を外部委託により行うことができる。

5.2 脅威及び対策の検討における留意事項

部局総括責任者及び部局技術責任者は、前節により情報処理業務が重要な情報を取り扱うものであるか否かを判断又は検討する場合には、以下の事項を考慮すること。

(1) 当該情報処理業務において、委託先に提供する情報及び委託先によるアクセスを認める情報を洗い出し、重要な情報に該当するか否かを判断すること。

(2) 委託先による重要な情報の取扱いを不要とするために、外部委託の対象とする情報処理業務の範囲を検討すること。

(3) 情報システム等の構築・開発を委託先の事業所で行う限りにおいては重要な情報を取り扱わない場合であっても、当該情報システム等の導入作業において、既存の情報システムとの接続作業及び既存の情報システムが稼動している区域での設置作業に伴い、既存の情報システムが保有する重要な情報へのアクセスが可能となる場合があること。

(4) 情報システムの運用・保守・点検を行う者は、当該業務の遂行に必要なアクセス

権を付与されることにより、一般に、当該情報システムで保有するすべての情報にアクセスし得ること。

6. 調達における手続

6.1 委託先の選定基準及び委託先が具備すべき要件

(1) 部局技術責任者は、委託先の選定において、委託する情報処理業務の実施に求められる安定性を有すると認められる事業者を選定すること。

(2) 部局技術責任者は、委託先に実施を求める情報セキュリティ対策等を調達仕様に含め、委託先候補による提案を評価することにより、適格な事業者を選定すること。求める情報セキュリティ対策等は、表１を目安として部局技術責任者が適切に定めること。

表１．調達仕様において委託先に求める情報セキュリティ対策等

委託する業務の分類 ＼ 情報セキュリティ対策等	情報システム等の構築・開発	情報システムの運用					情報システムの保守・点検	情報の加工・処理	情報の保存・運搬
		オンサイトサービス	リモート運用サービス	データセンター	ASPサービス	ハウジングサービス			
(1)情報セキュリティを確保するための体制の整備	○	○	○	○	○	○	○	○	※
(2)取り扱う府省庁の情報の秘密保持等	○	○	○	○	○	○	○ 物理的対策	○	△
(3)セキュリティ機能の装備	○	×	×	×	×	×	×	×	×
(4)運用・保守・点検における情報セキュリティ対策の実施	×	△	△	△	※	×	△	×	×
(5)脆弱性対策の実施	○	△	△	△	※	×	△	×	×
(6)情報セキュリティ対策のサービスレベルに関する事項	×	△	△	△	△	△	△	×	×
(7)情報セキュリティが侵害された場合の対処	△	△	△	△	△	△	△	△	※
(8)情報セキュリティ監査の実施	△	△	△	△	△	△	△	△	△
(9)情報セキュリティ対策の履行が不十分であると思われる場合の対処	△	△	△	△	△	△	△	△	※
(10)再請負に関する事項（7.5項）	○	△	△	△	△	△	△	○	△
(11)国際規格を踏まえた委託先の情報セキュリティ水準の評価（6.2節）	△	△	△	△	△	△	△	△	△

○：必要 △：選択（当該対策等の実施を委託先に求めるか否かについて調達ごとに選択するもの、及び当該対策等の実施を委託先に求めるが委託先の選定後に契約に含めれば足りると判断する場合があるもの）

×：非該当又は不必要 ※：一般にサービスに含まれている

本表の区分は一般的な目安であり、調達仕様に記載する事項は案件ごとに判断すること。

「情報セキュリティ対策等」の(1)～(9)の各項目については「付録2 情報セキュリティ対策等」を参照されたい。

6.2 国際規格を踏まえた委託先の情報セキュリティ水準の評価

委託先の選定における前節の手続に加えて、選定の厳格性を向上させる場合に、委託先の候補者における情報セキュリティ水準を以下に示す国際規格等を踏まえて評価するこ

と。目的に適した制度を利用する必要がある。

- 情報セキュリティマネジメントシステムに関する適合性評価制度
- 情報セキュリティ対策ベンチマーク
- 情報セキュリティ監査制度

6.2.1 情報セキュリティマネジメントシステムに関する適合性評価制度の活用

(1) 部局技術責任者は、情報処理業務を外部委託により行う場合であって、委託先候補における情報セキュリティマネジメントに関して客観性の高い評価基準に基づく評価を行う必要があると判断したときは、第三者機関（審査登録機関）による適合性評価に基づく認証の取得有無を、委託先候補の評価の要素として活用すること。

我が国においては、情報セキュリティマネジメントシステムに関する適合性評価制度として、財団法人日本情報処理開発協会（JIPDEC）が「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」を運営している。

本制度の利用方法については、「付録3 組織における情報セキュリティ水準の評価に関する制度」及び次の資料を参照されたい。

「外部委託における情報セキュリティ対策に関する評価手法の利用の手引」（内閣官房情報セキュリティセンター、2006 年5 月）の資料1「外部委託におけるISMS 適合性評価制度の利用方法」（JIPDEC）

(2) 部局技術責任者は、情報セキュリティマネジメントシステムに関する適合性評価に基づく認証の取得有無を委託先候補の評価の要素として活用する場合には、委託先候補の事業者に対して登録証及び適用範囲定義書の提示を求め、登録範囲及び適用範囲が委託する情報処理業務に合致することを確認すること。

6.2.2 情報セキュリティ対策ベンチマークの活用

(1) 部局技術責任者は、情報処理業務を外部委託により行う場合であって、委託先候補における情報セキュリティマネジメントの評価を委託先の自己評価により行う必要があると認めたときは、情報セキュリティ対策ベンチマークを委託先候補の評価の要素として活用すること。

本制度の利用方法については、「付録3 組織における情報セキュリティ水準の評価に関する制度」及び次の資料を参照されたい。

「外部委託における情報セキュリティ対策に関する評価手法の利用の手引」（内閣官房情報セキュリティセンター、2006 年5 月）の資料2「外部委託における情報セ

キュリティ対策ベンチマークの利用方法」（経済産業省）

(2) 部局技術責任者は、情報セキュリティ対策ベンチマークを委託先候補の評価の要素として活用する場合には、委託先候補の事業者に、情報セキュリティ対策ベンチマークの結果を提出させ、その内容について以下の点に留意して評価すること。

・ベンチマークの結果は、事業者自身が行ったものであり第三者による確認・認証の結果ではないため、不明確な事項があれば、事業者に質問する等により結果の客観性を高めること。

6.2.3 情報セキュリティ監査の活用

(1) 部局技術責任者は、情報処理業務を外部委託により行う場合であって、委託先候補における情報セキュリティ水準について客観性の高い評価を行う必要があると認めたときは、委託先候補の事業者が過去に実施した情報セキュリティ監査の結果を委託先候補の評価の要素として活用すること。

情報セキュリティ監査については、「情報セキュリティ監査基準」及び「情報セキュリティ管理基準」を含む事項を定めた「情報セキュリティ監査制度」がある。当制度の利用方法については、「付録3 組織における情報セキュリティ水準の評価に関する制度」及び次の資料を参照されたい。

「外部委託における情報セキュリティ対策に関する評価手法の利用の手引」（内閣官房情報セキュリティセンター、2006 年5 月）の資料3「外部委託における情報セキュリティ監査の利用方法」（特定非営利活動法人日本セキュリティ監査協会）

(2) 部局技術責任者は、情報セキュリティ監査の結果を委託先候補の評価の要素として活用する場合には、委託先候補の事業者に監査報告書を提出させ、監査の対象が委託する情報処理業務に合致することを確認した上で、評価すること。

6.3 委託先に求める事項の周知

6.3.1 委託先に実施させる情報セキュリティ対策の内容の周知

(1) 部局技術責任者は、外部委託に係る業務の遂行に際して委託先に実施させる情報セキュリティ対策の内容を、調達仕様として委託先候補に周知すること。委託先に実施させる情報セキュリティ対策の範囲は、「6.1 委託先の選定基準及び委託先が具備すべき要件」の「表１ 調達仕様において委託先に求める情報セキュリティ対策等」の(1)～(7)に示す事項を原則として、外部委託する業務に即して部局技術責任者が定めること。

調達仕様の記述例は、「第Ⅱ部 調達仕様における情報セキュリティ関連事項の記述例」を参照されたい。

6.3.2 情報セキュリティが侵害された場合の対処手順の周知

(1) **部局技術責任者は、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処手順（表１(7)）を、調達仕様に記載することにより委託先候補に周知すること。**

調達仕様の記述例は、「第Ⅱ部 調達仕様における情報セキュリティ関連事項の記述例」を参照されたい。

6.3.3 情報セキュリティ対策の履行状況の確認等に関する事項の周知

(1) **部局技術責任者は、調達仕様、契約及び確認書において実施を求める情報セキュリティ対策が委託先において履行されていることを確認するための評価基準を策定すること。例えば、情報セキュリティ対策項目を定めてその履行状況を委託先から適宜又は定期的に報告させ、対策が履行されていることを確認すること。**

(2) **部局技術責任者は、委託先における情報セキュリティ対策の履行状況の確認にあたり、必要に応じて、情報セキュリティ監査を行うこと（表１(8)）。具体的には、当該業務及び取り扱わせる情報の重要度、当該業務の実施場所、実施期間、委託金額等を考慮し、必要性の判断を行うこと。[2] 以下に例示する場合等には情報セキュリティ監査を適用することが特に望ましい。**

- **利用者の安全及び権利保護の観点から情報の機密性・完全性の維持が強く求められる情報処理業務**
- **大学の信用維持のために可用性及び機密性の確保が求められる情報処理業務**

(3) **委託先における情報セキュリティ対策の履行状況の確認を情報セキュリティ監査により行う場合には、その内容及び方法等を、調達仕様に記載することにより委託先候補に周知すること。**

(4) **部局技術責任者は、委託先において情報セキュリティ対策の履行が不十分である場合の対処手順（表１(9)）を、調達仕様として委託先候補に周知すること。**

調達仕様の記述例は、「第Ⅱ部 調達仕様における情報セキュリティ関連事項の記述例」を参照されたい。

6.4 委託先の選定における手続の遵守

[2] 情報処理業務を委託先において行う場合には、学内において行う場合と比べ、情報の機密性、完全性、可用性が損なわれるリスクが増大すること、及び当該業務が長期に渡るほど情報セキュリティ上の問題が発生しやすいことに留意し、リスクを評価すること。ただし、実施期間が短い、委託金額が少ない場合等、必ずしも委託先に対する情報セキュリティ監査の活用が合理的でないことがあり得ることから、監査の実施可能性も考慮した上で、監査の必要性を判断すること。

(1) 部局技術責任者は、「6.1 委託先の選定基準及び委託先が具備すべき要件」の定めに従い委託先を選定すること。

7. 契約における手続

7.1 外部委託に係る契約における情報セキュリティの考慮

(1) 部局技術責任者は、委託先に行わせる情報セキュリティ対策等を契約又はその付属書に含めて明示すること。委託先に行わせる情報セキュリティ対策等の範囲は、表２を原則として、外部委託する業務に即して部局技術責任者が定めること。

表２ 契約において委託先に行わせるものとする情報セキュリティ対策等

委託する業務の分類 / 情報セキュリティ対策等	情報システム等の構築・開発	情報システムの運用					情報システムの保守・点検	情報の加工・処理	情報の保存・運搬
		オンサイトサービス	リモート運用サービス	データセンター	ASPサービス	ハウジングサービス			
(1)情報セキュリティを確保するための体制の整備	○	○	○	○	○	○	○	○	※
(2)取り扱う府省庁の情報の秘密保持等	○	○	○	○	○	○	○ 物理的対策	○	○
(3)セキュリティ機能の装備	○	×	×	×	×	×	×	×	×
(4)運用・保守・点検における情報セキュリティ対策の実施	×	△	△	△	※	×	△	×	×
(5)脆弱性対策の実施	○	△	△	△	※	×	△	×	×
(6)外部委託する業務以外の情報資産の保全	△	△	×	×	×	×	△	×	×
(7)情報セキュリティ対策のサービスレベルに関する事項	△	△	△	△	△	△	△	△	※
(8)情報セキュリティが侵害された場合の対処	○	○	○	○	○	○	○	○	※
(9)情報セキュリティ対策の履行状況の確認	○	○	○	○	○	○	○	○	※
(10)情報セキュリティ監査の実施	△	△	△	△	△	△	△	△	△
(11)情報セキュリティ対策の履行が不十分であると思われる場合の対処	○	○	○	○	○	○	○	○	※
(12)確認書に委任する事項	△	△	△	△	△	△	△	△	×
(13)再請負に関する事項	○	△	△	△	△	△	△	○	△

○：必要 △：選択 ×：非該当又は不必要

※：一般にサービスに含まれている

本表は一般的な目安を示すものであり、契約に含める事項は案件ごとに判断すること。

契約の記述例は、「第III部 契約における情報セキュリティ関連事項の記述例」を参照されたい。

「情報セキュリティ対策等」の各項目については「付録2 情報セキュリティ対策等」を参照されたい。

7.2 外部委託に係る確認書における情報セキュリティの考慮

(1) 部局技術責任者は、委託先に情報処理を行わせるに当たり、契約において定めた委託先に行わせる情報セキュリティ対策等に関して、双方の責任の明確化と合意の形成を行い、合意した事項を確認書として委託先の責任者から提出させ、あるいは、契約の付属書とすること（以降、付属書に記載する事項も含めて契約という。）。

(2) 確認書又は契約の付属書には、情報セキュリティ対策等を実施する体制を含めること。例えば、情報セキュリティ対策等の実施における双方の責任者及び技術担当者を記載することが考えられる。

(3) 確認書又は契約の付属書には、必要に応じて次の事項を含めること。

- 委託先が実施する情報セキュリティ対策等の具体的な取組内容
- 当該外部委託に係る業務を行う者の特定とそれ以外の者による当該業務の禁止

(4) 確認書及び契約の付属書は、契約に加えて取り交わす必要がない場合には、省略することができる。

7.3 外部委託の継続における注意

(1) 部局技術責任者は、外部委託契約を継続する場合には、「6.1 委託先の選定基準及び委託先が具備すべき要件」に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。外部委託契約の継続には、特に、次の場合を含む。

- 情報システムの構築において、設計を外部委託により行い、その終了後に当該設計に基づく実装を外部委託により行う場合
- 情報システムの構築を外部委託により行い、その終了後に当該情報システムの運用、保守又は点検を外部委託により行う場合
- 情報システムの運用、保守又は点検を外部委託により行い、その後の当該情報システムの運用、保守又は点検も新たな契約の下で外部委託により行う場合

7.4 外部委託における実施内容の変更に関する注意

(1) 部局技術責任者は、契約及び確認書において委託先が行うものと定めた事項の変更を委託先が希望する場合には、情報セキュリティを維持する観点から、契約及び確認書、並びに委託先の選定において適用した選定手続、選定基準及び委託先が具備すべき要件に基づき、その可否を審査すること。

7.5 再請負の原則禁止

(1) 再請負による情報処理業務の遂行は、委託先に行わせる場合に比べ、脅威が増大し、対策は困難になる傾向がある。このため、部局技術責任者は、委託先が外部委託を受けた業務の全部又は一部を第三者に再請負により行わせることを原則として禁止すること。

(2) 部局技術責任者は、委託先が業務の全部又は一部を第三者に再請負により行わせることを認めない場合には、その旨を調達仕様に含めること。

(3) 部局技術責任者は、委託先が外部委託を受けた業務の一部を再請負により行うことを望む場合には、再請負の可否及び条件を検討し、部局総括責任者の判断を得ること。判断基準の例を以下に示す。

- 再請負を行うことに合理的な理由があると認められる場合にのみ、これを認めることができる。事業者の専門性にかんがみ、当該業務が再請負により技術的に可能となること及び適正な費用で実施可能となることは、合理的な理由として認められ得る。
- 委託先自体が当該一部の業務を実施する場合に求めるべき水準と同等の情報セキュリティ水準を再請負においても確保させるための情報セキュリティ対策を委託先が再請負先に契約に基づき行わせることを求め、以下の措置を採ること。
  - ○ 当該求めを委託元と委託先の契約において定めること。
  - ○ 再請負先において採る情報セキュリティ対策について委託先から報告させ、これが十分なものであることを確認すること。
  - ○ 委託先が再請負先に情報セキュリティ対策を行わせた結果を委託元が確認する方法を定め、確認すること。

8. 委託先における情報処理業務実施中の手続

8.1 取り扱う府省庁の情報の秘密保持等

(1) 部局技術責任者は、外部委託により情報処理を行う場合に、委託先に提供する情報を必要最小限の範囲に限定すること。

(2) 部局技術責任者は、委託先に情報を提供する場合には、その都度、提供の記録を採ること。

(3) 部局技術責任者は、委託先に要機密情報を提供する場合には、その移送における情報漏洩対策を施すこと。情報漏洩対策として、書面の不要部分のマスキング、媒体中の情報を暗号化した上での郵送、暗号化通信等、安全な方法を採ること。

(4) 部局技術責任者は、提供した情報が外部委託した業務の終了等により委託先において不要となった場合に、これを返却、消去又は廃棄させること。委託先において情報を消去又は廃棄した場合には、その旨を委託先から報告させること。

(5) 部局技術責任者は、提供した情報の返却を受け、若しくは消去又は廃棄の報告を受けた場合には、その都度、その記録を取ること。

(6) 委託先における府省庁の情報の取扱規則を策定し、これを遵守させること。本規則には、取り扱う府省庁の情報等に応じて以下に例示する事項等を選択して含めること。

- 取り扱う情報は外部委託した情報処理業務にのみ使用し、他の目的には使用しないこと。
- 取り扱う情報は外部委託した情報処理業務を行う者以外には秘密とすること。
- 取り扱う情報は指定した場所から持ち出さないこと。
- 取り扱う情報は委託元の許可なく複製しないこと。

8.2 情報セキュリティ対策の履行状況の確認

(1) 部局技術責任者は、「7.1 外部委託に係る契約における情報セキュリティの考慮」に従い契約又は確認書に含めた委託先に実施させる情報セキュリティ対策の履行状況を確認すること。

(2) 部局技術責任者は、委託先に実施させる情報セキュリティ対策の履行状況の確認を情報セキュリティ監査により行う旨契約において定めた場合には、定められた内容及び方法に従いこれを実施すること。

9. 納品・検収における手続

(1) 部局技術責任者は、外部委託の終了時に、委託先が行った情報セキュリティ対策を契約及び確認書の内容に照らして確認し、その結果を納品検査における合否の判断に加えること。確認する情報セキュリティ対策は、重要性を判断して選択してよい。

10. 国際規格を踏まえたセキュリティ機能の設計及び実装の評価

10.1 情報システム等の構築・開発におけるセキュリティ機能の設計及び実装の評価

(1) 部局技術責任者は、情報システム等の構築・開発を外部委託により行う場合であって、当該構築又は開発について重要なセキュリティ要件があると認めるときには、委託先に、セキュリティ機能の設計についてセキュリティ設計仕様書（ST: Security Target）の評価（以下「ST 評価」という。）及び同確認（以下「ST 確認」という。）を受けさせること。ただし、情報システム等を更改する場合であって、重要なセキュリティ要件の変更が軽微であると認めたときは、この限りではない。

(2) 部局技術責任者は、委託先から、セキュリティ機能の設計に係るST 評価・ST 確認を受けたことを示す確認書を納品までに提示させること。

(3) 部局技術責任者は、ST 評価・ST 確認は第三者機関が行うものであること等にかんがみ、委託先の責任によらず確認書が納品までに提出されないおそれがあると考えられる場合には、納品後に当該文書が提出される場合の取扱いを委託先と協議して決定すること。例えば、まず情報システムの構築又はソフトウェアの開発の成果物について納品・検収を行い、別途ST 評価・ST 確認の結果について納品・検収を行う方法がある。

委託先にST 評価･ST 確認を行わせる場合には､以下の資料もあわせて参照されたい。

- 「情報システムの構築等におけるST評価・ST確認の実施に関する解説書」内閣官房情報セキュリティセンター、2006年6月

10.2 情報システムの構築に伴い調達する機器等のセキュリティ機能の評価

(1) 部局技術責任者は、構築する情報システムに重要なセキュリティ要件があると認める場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定めること。

(2) 部局技術責任者は、情報システムの構築に係る委託先からの調達に限ることなく当該情報システムの構成要素とする機器及びソフトウェアを調達する場合であって、(1)に従い定めたセキュリティ機能及びその他の要求条件を満たす採用候補製品が複数あるときには、その中から当該セキュリティ機能に関してIT セキュリティ評価及び認証制度に基づく認証を取得している製品を選択すること。

(3) 部局技術責任者は、情報システムの構築に係る委託先から当該情報システムの構成要素とする機器又はソフトウェアを調達する場合には、委託先の評価・選定基準に、当該機器又はソフトウェアが(1)に定めたセキュリティ機能についてIT セキュリティ評価及び認証制度に基づく認証を取得しているか否かを加味すること。

IT セキュリティ評価及び認証制度に基づく認証の取得を製品の選択に利用する場合には、以下の資料もあわせて参照されたい。

- 「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」内閣官房情報セキュリティセンター、2006年6月

11. 本書に関する相談窓口

(1) 部局技術責任者は、緊急時の対応又は本書の内容を超えた対応が必要な場合には、全学実施責任者に相談し、指示を受けること。

(2) 部局技術責任者は、本書の内容について不明な点又は質問がある場合には、全学実施責任者に連絡し、回答を得ること。

第Ⅱ部 調達仕様における情報セキュリティ関連事項の記述例

第Ⅱ部では、情報処理業務を外部委託により行う場合に、情報セキュリティの観点から調達仕様に含める事項の例を示す。

1. 情報システム等の構築・開発の場合

(1) 情報セキュリティを確保するための体制の整備

・本調達に係る業務を行う事業者は、当該業務の実施において情報セキュリティを確保するための体制を整備すること。

(2) 取り扱う府省庁の情報の秘密保持等

・本調達に係る業務の実施のために本学から提供する情報その他当該業務の実施において知り得た情報については、その秘密を保持し、また当該業務の目的以外に利用しないこと。

(3) セキュリティ機能の装備

【セキュリティ要求仕様を提示し、応札においてセキュリティ機能の提案を求める場合】

・本調達に係る［情報システム／ソフトウェア］において取り扱う情報の保護を目的として、［付属文書（セキュリティ要求仕様）］に基づき、応札においてセキュリティ機能を提案すること。

【セキュリティ要求仕様を提示し、セキュリティ機能の装備を求める場合】

・本調達に係る［情報システム／ソフトウェア］において取り扱う情報の保護を目的として、［付属文書（セキュリティ要求仕様）］に基づきセキュリティ機能を設計し、実装すること。

【セキュリティ機能の概要を提示し、その装備を求める場合】

・本調達に係る情報システムにおいて以下のセキュリティ機能を具体化し、実装すること。

【情報システムの構築の場合】

○ 本調達に係る情報システムへのアクセスを業務上必要な者に限るための機能

○ 本調達に係る情報システムに対する不正アクセス、ウイルス・不正プログラ

ム感染等、インターネットを経由する攻撃、不正等への対策機能

○ 本調達に係る情報システムにおけるセキュリティ事故及び不正の原因を事後に追跡するための機能

【ソフトウェアの開発の場合】

○ 本調達に係るソフトウェアへのアクセスを業務上必要な者に限るための機能

○ 本調達に係るソフトウェアの不正な利用を防止するために、不正な入力及び出力を防止する機能

○ 本調達に係るソフトウェアに関連するセキュリティ事故及び不正の原因を事後に追跡するための機能

【ST 評価・ST 確認を求める場合】

・本調達に係る［情報システム／ソフトウェア］において取り扱う情報の保護を目的として、ISO/IEC 15408に基づき必要なセキュリティ機能を設計し、実装すること。当該設計において策定するセキュリティ設計仕様書（ST: Security Target）についてST評価・ST確認を受け、その結果を［納品までに／○○○○年○○月○○日までに］提出すること。

【情報システムの構築で、構成ソフトウェアに関してIT セキュリティ評価及び認証制度に基づく認証取得を考慮する場合】

・本調達に係る情報システムを構成する○○機能を有するソフトウェアについて、取り扱う情報の保護を目的とするセキュリティ機能について、ITセキュリティ評価及び認証制度に基づく認証を取得しているか否かを情報システムに係る提案の評価の要素とする。当該認証を取得している場合は、提案において報告すること。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

(4) 脆弱性対策の実施

【情報システムの構築の場合】

・本調達に係る情報システムの構築における以下の脆弱性対策を提案すること。

○ 構築する情報システムを構成する機器及びソフトウェアの中で、脆弱性対策を実施するものを適切に決定すること。

○ 脆弱性対策を行うとした機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。

○ 把握した脆弱性情報について、対処の要否、可否を判断すること。

対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を納品時に委託元に報告すること。

【情報セキュリティが侵害された場合の対処を明示する場合】

(5) 情報セキュリティが侵害された場合の対処

・本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、速やかに委託元に報告すること。これに該当する場合には、以下の事象を含む。

○ 委託先に提供し、又は委託先によるアクセスを認める本学の情報の外部への漏えい及び目的外利用

○ 委託先の者による本学のその他の情報へのアクセス

(6) 情報セキュリティ対策の履行状況の確認等に関する事項の通知

・本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、委託先に対して以下の報告を求める場合がある。

【委託先に求める情報セキュリティ対策全般につき報告を求める場合】

○ 本調達仕様の［(1)～(5)の各項］において求める情報セキュリティ対策の実績

【委託先に取り扱わせる情報の秘密保持等に係る報告を求める場合】

○ 委託先に取り扱わせる府省庁の情報の秘密保持等に係る管理状況

【情報セキュリティ監査を行う場合】

(7) 情報セキュリティ監査の実施

・本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、添付「情報セキュリティ監査仕様書」に示す仕様に基づき情報セキュリティ監査を行う。委託先は、応札において、情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「監査対応計画書」により提示すること。（情報セキュリティ監査仕様書において、監査内容、対象範囲、実施者等を提示する。）

【情報セキュリティ対策の履行が不十分な場合の対処を明示する場合】

(8) 情報セキュリティ対策の履行が不十分な場合の対処

・本調達に係る業務の遂行において、委託先における情報セキュリティ対策の履行が不十分である可能性を委託元が認める場合には、委託先の責任者は、委託元の求めに応じこれと協議を行い、合意した対応を採ることとする

(9) 再請負に関する事項

【再請負を禁止する場合】

・本調達に係る業務は、その全部又は一部を他の事業者に再請負により行わせてはならない。

【再請負を認める場合】

・本調達に係る業務の一部を他の事業者に再請負により行わせる場合には、委託先は、委託元が委託先に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再請負先に行わせること。再請負先に行わせた情報セキュリティ対策及びこれを行わせた結果に関する報告を、委託先に求める場合がある。

【国際規格を踏まえた委託先の情報セキュリティ水準の評価を行う場合】

(10) 国際規格を踏まえた委託先の情報セキュリティ水準の評価

【ISMS 認証取得を考慮する場合】

・本調達に係る業務を行おうとする事業者又はその部門において、情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

【情報セキュリティ対策ベンチマークの結果を考慮する場合】

・本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提示すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が［n］以上であるか否かを、提案に関する評価の要素とする。

（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

【ISMS 認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】

・本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同

等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

・ただし、ISMS認証及びこれと同等の認証を取得していない事業者又はその部門においては、情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提出すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が4以上であるか否かを、提案に関する評価の要素とする。

（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

2. 情報システムの運用・保守・点検の場合

(1) 情報セキュリティを確保するための体制の整備

・本調達に係る業務を行う事業者は、当該業務の実施において情報セキュリティを確保するための体制を整備すること。

(2) 取り扱う大学の情報の秘密保持等

・本調達に係る業務の実施のために本学から提供する情報その他当該業務の実施において知り得た情報については、その秘密を保持し、また当該業務の目的以外に利用しないこと。

【運用・保守・点検における情報セキュリティ対策の実施を求める場合】

(3) 運用・保守・点検における情報セキュリティ対策の実施

・（稼働状況の監視、バックアップの取得等、委託先に実施を求める情報セキュリティ対策を具体的に記述する。これらは、委託先に実施を求める運用・保守・点検の業務に含めて記述することも考えられる。）

【脆弱性対策を外部委託する場合】

(4) 脆弱性対策の実施

・本調達に係る情報システムの運用における以下の脆弱性対策を提案すること。

○ 別紙○（略）に掲げる機器及びソフトウェアについて、公表される脆弱性情報を常時把握すること。

【対処の要否、可否の判断を委託先にさせる場合】

○ 把握した脆弱性情報について、対処の要否、可否を判断すること。

対処したものに関して対処方法、対処しなかったものに関してその理由、代

替措置及び影響を委託元に報告すること。

【対処の要否、可否の判断に委託元も加わる場合】

○ 把握した脆弱性情報について、対処の要否、可否につき委託元と協議し、決定すること。決定した対処又は代替措置を実施すること。

【情報セキュリティ対策のサービスレベルに関する事項を求める場合】

(5) **情報セキュリティ対策のサービスレベルに関する事項**

・(求めるサービスレベルの例に、使用するソフトウェアに関してセキュリティ修正がベンダーから提供された後にこれを適用するまでの期間、インターネット接続に関して外部からの攻撃等の異常を検知してから委託元に報告するまでの時間等がある。情報セキュリティ対策のサービスレベルは、情報システムの運用・保守・点検におけるサービスレベルの一部として記述することも考えられる。)

【情報セキュリティが侵害された場合の扱いを明示する場合】

(6) **情報セキュリティが侵害された場合の対処**

・本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、速やかに委託元に報告すること。これに該当する場合には、以下の事象を含む。

○ 委託先に提供し、又は委託先によるアクセスを認める本学の情報の外部への漏えい及び目的外利用

○ 委託先の者による本学のその他の情報へのアクセス

【情報システムの運用を外部委託する場合】

○ 外部の者による不正アクセス、不正プログラム感染等の情報セキュリティ侵害

(7) **情報セキュリティ対策の履行状況の確認等に関する事項の通知**

・本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、委託先に対して以下の報告を求める場合がある。

【委託先に求める情報セキュリティ対策全般につき報告を求める場合】

○ 本調達仕様の［(1)〜(6)の各項］において求める情報セキュリティ対策の実績

【委託先に取り扱わせる情報の秘密保持等に係る報告を求める場合】

○ 委託先に取り扱わせる大学の情報の秘密保持等に係る管理状況

【情報セキュリティ監査を行う場合】

(8) **情報セキュリティ監査の実施**

- **本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、添付「情報セキュリティ監査仕様書」に示す仕様に基づき情報セキュリティ監査を行う。委託先は、応札において、情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「監査対応計画書」等により提示すること。（情報セキュリティ監査仕様書において、監査内容、対象範囲、実施者等を提示する。）**

【情報セキュリティ対策の履行が不十分な場合の対処を明示する場合】

(9) **情報セキュリティ対策の履行が不十分な場合の対処**

- **本調達に係る業務の遂行において、委託先における情報セキュリティ対策の履行が不十分である可能性を委託元が認める場合には、委託先の責任者は、委託元の求めに応じこれと協議を行い、合意した対応を採ること。**

(10) **再請負に関する事項**

【再請負を禁止する場合】

- **本調達に係る業務は、その全部又は一部を他の事業者に再請負により行わせてはならない。**

【再請負を認める場合】

- **本調達に係る業務の一部を他の事業者に再請負により行わせる場合には、委託先は、委託元が委託先に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再請負先に行わせること。再請負先に行わせた情報セキュリティ対策及びこれを行わせた結果に関する報告を、委託先に求める場合がある。**

【国際規格を踏まえた委託先の情報セキュリティ水準の評価を行う場合】

(11) **国際規格を踏まえた委託先の情報セキュリティ水準の評価**

【ISMS 認証取得を考慮する場合】

- **本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同**

等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

【情報セキュリティ対策ベンチマークの結果を考慮する場合】

・本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提出すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が［n］以上であるか否かを、提案に関する評価の要素とする。

（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

【ISMS 認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】

・本調達に係る業務を行おうとする事業者又はその部門において情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はこれと同等の認証を取得しているか否かを、提案に関する評価の要素とする。（評価式は調達ごとに定めることとなるため、本雛形では省略している。）

・ただし、ISMS認証及びこれと同等の認証を取得していない事業者又はその部門においては、情報セキュリティ対策ベンチマークを実施し、その結果を書式1（本雛形では省略している。）により提出すること。情報セキュリティ対策ベンチマークに基づく平均成熟度が4以上であるか否かを、提案に関する評価の要素とする。

（情報セキュリティ対策ベンチマークに関する説明を、付録3から引用する。）

3. 情報の加工・処理の場合

(1) 情報セキュリティを確保するための体制の整備

・本調達に係る業務を行う事業者は、当該業務の実施において情報セキュリティを確保するための体制を整備すること。

(2) 取り扱う大学の情報の秘密保持等

・本調達に係る業務の実施のために本学から提供する情報その他当該業務の実施において知り得た情報については、その秘密を保持し、また当該業務の目的以外に利用しないこと。

【情報セキュリティが侵害された場合の対処を明示する場合】

(3) 情報セキュリティが侵害された場合の対処

・本調達に係る業務の遂行において委託先に提供し、又は委託先によるアクセスを

認める情報について外部への漏えい、目的外利用等、情報セキュリティ侵害が起き又はそのおそれがある場合には、速やかにこれを委託元に報告すること。

(4) 情報セキュリティ対策の履行状況の確認等に関する事項の通知

・本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、委託先対して以下の報告を求める場合がある。

【委託先に求める情報セキュリティ対策全般につき報告を求める場合】

○ 本調達仕様の［(1)～(3)の各項］において求める情報セキュリティ対策の実績

【委託先に取り扱わせる情報の秘密保持等に係る報告を求める場合】

○ 委託先に取り扱わせる府省庁の情報の秘密保持等に係る管理状況

【情報セキュリティ監査を行う場合】

(5) 情報セキュリティ監査の実施

・本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、添付「情報セキュリティ監査仕様書」に示す仕様に基づき情報セキュリティ監査を行う。委託先は、応札において、情報セキュリティ監査を受け入れる部門、場所、時期等を「監査対応計画書」等により提示すること。（情報セキュリティ監査仕様書において、監査内容、対象範囲、実施者等を提示する。）

【情報セキュリティ対策の履行が不十分な場合の対処を明示する場合】

(6) 情報セキュリティ対策の履行が不十分な場合の対処

・本調達に係る業務の遂行において、委託先における情報セキュリティ対策の履行が不十分である可能性を委託元が認める場合には、委託先の責任者は、委託元の求めに応じこれと協議を行い、合意した対応を採ること。

(7) 再請負に関する事項

【再請負を禁止する場合】

・本調達に係る業務は、その全部又は一部を他の事業者に再請負により行わせてはならない。

【再請負を認める場合】

・本調達に係る業務の一部を他の事業者に再請負により行わせる場合には、委託先

は、委託元が委託先に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再請負先に行わせること。再請負先に行わせた情報セキュリティ対策及びこれを行わせた結果に関する報告を、委託先に求める場合がある。

【ISMS 認証取得等を委託先の選定において考慮する場合】

(8) 国際規格を踏まえた委託先の情報セキュリティ水準の評価

・【ISMS認証取得を考慮する場合】

「1 情報システム等の構築・開発の場合」と同じ。

・【情報セキュリティ対策ベンチマークの結果を求める場合】

「1 情報システム等の構築・開発の場合」と同じ。

・【ISMS認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】

「1 情報システム等の構築・開発の場合」と同じ。

4. 情報の保存・運搬の場合

(1) 取り扱う大学の情報の秘密保持等

・本調達において［保存／運搬］を委託する本学の情報について、その漏洩及び毀損を防止するための十分な安全管理を行うこと。

【情報の保存に関して委託先の情報セキュリティ監査を行う場合】

(2) 情報セキュリティ監査の実施

・本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、委託元は、添付「情報セキュリティ監査仕様書」に示す仕様に基づき情報セキュリティ監査を行う。委託先は、応札において、情報セキュリティ監査を受け入れる部門、場所、時期等を「監査対応計画書」等により提示すること。（情報セキュリティ監査仕様書において、監査内容、対象範囲、実施者等を提示する。）

【情報の保存に関してISMS 認証取得等を委託先の選定において考慮する場合】

(3) 国際規格を踏まえた委託先の情報セキュリティ水準の評価

・【ISMS認証取得を考慮する場合】

「1 情報システム等の構築・開発の場合」と同じ。

・【情報セキュリティ対策ベンチマークの結果を考慮する場合】

「1 情報システム等の構築・開発の場合」と同じ。

・【ISMS認証取得及び情報セキュリティ対策ベンチマークの結果を考慮する場合】

「1 情報システム等の構築・開発の場合」と同じ。

（情報の保存・運搬を外部委託により行う場合には、物品を安全に保存・運搬すること自体が委託先の提供するサービスの内容であることに留意して調達仕様に記載する事項を定める必要がある。

以下の各事項は、適切なサービスを利用すれば実質的に達成されるものであり、通常は調達仕様に含めない。

・情報セキュリティを確保するための体制の整備

・情報セキュリティが侵害された場合の対処

・情報セキュリティ対策の履行状況が不十分であると思われる場合の対処

第III部 契約における情報セキュリティ関連事項の記述例

第III部では、情報処理業務を外部委託により行う場合に、情報セキュリティの観点から契約に含める事項の例を示す。

1. 情報システム等の構築・開発の場合

(1) 情報セキュリティを確保するための体制の整備

【情報セキュリティの確保のために体制を整備する場合】

- ［乙］は、本契約に係る業務の実施における情報セキュリティ確保のための体制を整備し、［甲］に報告するものとする。

【外部委託を受けた業務を実施する体制を情報セキュリティ確保の体制ともする場合】

- ［乙］は、第○条に基づき整備する実施体制において、情報セキュリティの確保に努めるものとする。
- ［乙］は、本契約に係る業務の実施体制を整備し、［甲］に報告するものとする。

（当該体制については、委託元、委託先の両者で協議し、合意した結果を別途確認書として取り交わすこととなる。）

(2) 取り扱う大学の情報の秘密保持等

契約における通常の秘密保持条項が該当する。以下の内容が含まれていることを確認し、必要に応じ記述を加えること。

- ［乙］は、本契約に係る業務に関して［甲］から提供された情報その他知り得た情報を実施体制に定めた者以外の者には秘密とし、また、当該業務の遂行以外の目的に使用しないこと。
- ［乙］は、本契約に係る業務に関して［甲］から提供された情報を、当該業務の終了時に委託元に返却するか、消去又は廃棄してその旨を書面で報告すること。
- ［乙］は、本契約に係る業務に関して委託元から提供、貸与等された情報その他知り得た情報を当該業務の終了後においても他者に漏えいしないこと。
- ［乙］は、本契約に係る業務に関して［甲］から提供された情報その他アクセスを認められた府省庁の情報を、別途定める規則に従い取り扱うこと。

（別途定める規則には、取り扱う大学の情報等に応じて、以下に例を示す事項等を

選択して含めること。

○ 取り扱う情報は外部委託した情報処理業務にのみ使用し、他の目的には使用しないこと。

○ 取り扱う情報は外部委託した情報処理業務を行う者以外には秘密とすること。

○ 取り扱う情報を指定した場所から持ち出さないこと。

○ 当該情報を委託元の許可なく複製しないこと。

○ 当該情報は、当該委託の終了時に、委託元への返却若しくは消去又は廃棄を確実に行うこと。）

(3) **セキュリティ機能の装備**

【情報システムの構築の場合】

【調達において提示したセキュリティ要求仕様と提案を受けたセキュリティ機能を付属文書で示し、当該セキュリティ機能の装備を求める場合】

・[乙] は、[付属文書（セキュリティ要求仕様及びセキュリティ機能)] に示すセキュリティ機能を構築する情報システムに装備すること。

（本雛形では、付属文書は省略している。）

【調達において提示したセキュリティ要求仕様を付属文書で示し、必要なセキュリティ機能を設計した上でその装備を求める場合】

・[乙] は、[付属文書（セキュリティ要求仕様)] に示すセキュリティ要求仕様に基づき、必要なセキュリティ機能を設計し、装備すること。

（本雛形では、付属文書は省略している。）

【契約でセキュリティ機能の概要を提示する場合】

・[乙] は、構築する情報システムに以下のセキュリティ機能を持たせること。

○ 構築する情報システムへのアクセスを業務上必要な者に限るための機能

○ 構築する情報システムに対する不正アクセス、ウイルス・不正プログラム感染等、インターネットを経由する攻撃、不正等への対策機能

○ 構築する情報システムにおけるセキュリティ事故及び不正の原因を事後に追跡するための機能

【ソフトウェアの開発の場合】

【調達において提示したセキュリティ要求仕様と提案を受けたセキュリティ機能を付属文書で示し、当該セキュリティ機能の装備を求める場合】

・[乙]は、[付属文書（セキュリティ要求仕様及びセキュリティ機能)]に示すセキュリティ機能を開発するソフトウェアに装備すること。

（本雛形では、付属文書は省略している。）

【調達において提示したセキュリティ要求仕様を付属文書で示し、必要なセキュリティ機能を設計した上でその装備を求める場合】

・[乙]は、[付属文書（セキュリティ要求仕様)]に示すセキュリティ要求仕様に基づき、必要なセキュリティ機能を設計し、装備すること。

（本雛形では、付属文書は省略している。）

【契約でセキュリティ機能の概要を提示する場合】

・[乙]は、開発する情報システムに以下のセキュリティ機能を持たせること。

○ 開発するソフトウェアへのアクセスを業務上必要な者に限るための機能

○ 開発するソフトウェアに対する不正アクセス、ウイルス・不正プログラム感染等、インターネットを経由する攻撃、不正等への対策機能

○ 開発するソフトウェアにおけるセキュリティ事故及び不正の原因を事後に追跡するための機能

【ST 評価・ST 確認を求める場合】

(4) セキュリティ機能の設計に関する確認

【ST 評価・ST 確認の結果を納品時に提出する場合】

・[乙]は、[構築する情報システム／開発するソフトウェア]に関して、取り扱う情報の保護を目的として、ISO/IEC 15408に基づき必要なセキュリティ機能を設計及び実装すること。当該設計において策定するセキュリティ設計仕様書（ST: Security Target）についてST評価・ST確認を受け、その結果を納品までに［甲］に提出すること。

【ST 評価・ST 確認の結果を納品後に提出する場合】

・[乙]は、[構築する情報システム／開発するソフトウェア]に関して、取り扱う

情報の保護を目的として、ISO/IEC 15408に基づき必要なセキュリティ機能を設計及び実装すること。当該設計において策定するセキュリティ設計仕様書（ST: Security Target）についてST評価・ST確認を受け、その結果を○○○○年○月○○日までに［甲］に提出すること。ST評価・ST確認を受けるために納品物に追加・変更が必要となった場合には、当該追加・変更は［乙］の責任においてこれを行うものとする。

【情報システムの構築の場合】

(5) 脆弱性対策の実施

・［乙］は、構築する情報システムに関して次の脆弱性対策を実施すること。

○ 構築する情報システムを構成する機器及びソフトウェアの中で、脆弱性対策を実施するものを適切に決定すること。

○ 脆弱性対策を行うとした機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。

○ 把握した脆弱性情報について、対処の要否、可否を判断すること。

対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を納品時に［甲］に報告すること。

【外部委託する業務以外の情報資産の保全を明示する場合】

(6) 外部委託する業務以外の情報資産の保全

・（略）

【サービスレベルを契約で定める場合】

(7) 情報セキュリティ対策のサービスレベルに関する事項

・（略）

(8) 情報セキュリティが侵害された場合の対処

・［乙］は、本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、これを速やかに［甲］に報告すること。これに該当する場合には、以下の事象を含む。

○ ［乙］に提供し、又は［乙］によるアクセスを認める［甲］の情報の外部への漏えい及び目的外利用

○ ［乙］の者による［甲］のその他の情報へのアクセス

(9) 情報セキュリティ対策の履行状況の確認

・（定期的に報告を求める等、情報セキュリティ対策の履行状況の確認として行う事項及び方法を列挙する。）

【情報セキュリティ監査を行う場合】

(10) 情報セキュリティ監査を行う事項及び方法

・（情報セキュリティ監査に関して、調達及び応札において確認した事項及び方法を記述する。）

(11) 情報セキュリティ対策の履行が不十分であると思われる場合の対処

・［乙］による情報セキュリティ対策の履行が不十分である可能性を［甲］が認める場合には、［乙］の責任者は、［甲］の求めに応じこれと協議を行い、合意した対応を採るものとする

【確認書を求める場合】

(12) 確認書に委任する事項

・（略）

(13) 再請負に関する事項

【再請負を禁止する場合】

・［乙］は、本契約に係る業務を再請負により第三者に行わせないこと。

【再請負を認める場合】

・［乙］は、［甲］が［乙］に求める情報セキュリティ対策と同水準の情報セキュリティ対策を再請負先に行わせること。

・［乙］は、再請負先に行わせた情報セキュリティ対策及びその結果を［適宜確認し、／監査し、］［甲］に報告すること。

2. 情報システムの運用・保守・点検の場合

(1) 情報セキュリティを確保するための体制の整備

「1 情報システム等の構築・開発の場合」と同じ。

(2) 取り扱う大学の情報の秘密保持等

「1 情報システム等の構築・開発の場合」と同じ。

(3) 運用・保守・点検における情報セキュリティ対策の実施

・（略）

【脆弱性対策を委託する場合】

(4) 脆弱性対策の実施

・［乙］は、情報システムの［運用／保守／点検］のにおいて、次の脆弱性対策を実施すること。

○ 別途定める脆弱性対策を行うものとする機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。

○ 把握した脆弱性情報について、対処の要否、可否を［［甲］と協議し、］判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を随時に［甲］に報告すること。

【外部委託する業務以外の情報資産の保全を明示する場合】

(5) 外部委託する業務以外の情報資産の保全

・（略）

(6) 情報セキュリティ対策のサービスレベルに関する事項

・（略）

(7) 情報セキュリティが侵害された場合の対処

・［乙］は、本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、これを速やかに［甲］に報告すること。これに該当する場合には、以下の事象を含む。

① ［乙］に提供し、又は［乙］によるアクセスを認める［甲］の情報の外部への漏えい及び目的外利用

② ［乙］の者による［甲］のその他の情報へのアクセス

③ ［甲］の者、［乙］の者又は外部の者による当該情報システムからの情報漏えい及び情報の目的外利用

④ 当該情報システムへの不正アクセスによる情報漏えい、サービス停止、情報の改ざん

⑤ 当該情報システムへのサービス不能攻撃によるサービス停止

⑥ 当該情報システムにおける不正プログラムの感染による情報漏えい、サービス停止、情報の改ざん

・［甲］及び［乙］は、上記④、⑤及び⑥その他被害が短時間に拡大する情報セキュリティ侵害については、別途定める緊急時対策を実施すること。

（別途定める緊急時対策は、契約の付属文書とすることが想定される。本雛形では省略している。）

(8) 情報セキュリティ対策の履行状況の確認

・（定期的に報告を求める等、情報セキュリティ対策の履行状況の確認として行う事項及び方法を列挙する。）

【情報セキュリティ監査を行う場合】

(9) 情報セキュリティ監査を行う事項及び方法

・（情報セキュリティ監査に関して、調達及び応札において確認した事項及び方法を記述する。）

(10) 情報セキュリティ対策の履行が不十分であると思われる場合の対処

・［乙］による情報セキュリティ対策の履行が不十分である可能性を［甲］が認める場合には、［乙］の責任者は、［甲］の求めに応じこれと協議を行い、合意した対応を採るものとする

【確認書を求める場合】

(11) 確認書に委任する事項

・（略）

3. 情報の加工・処理の場合

(1) 情報セキュリティを確保するための体制の整備

「1 情報システム等の構築・開発の場合」と同じ。

(2) 取り扱う大学の情報の秘密保持等

「1 情報システム等の構築・開発の場合」と同じ。

(3) 情報セキュリティが侵害された場合の対処

・[乙]は、本調達に係る業務の遂行において［乙］に提供し、又は［乙］によるアクセスを認める［甲］の情報の外部への漏えい若しくは目的外利用が認められ又はそのおそれがある場合には、これを速やかに［甲］に報告すること。

(4) 情報セキュリティ対策の履行状況の確認

・(情報セキュリティ対策の履行状況の確認として行う事項及び方法を列挙する。)

【情報セキュリティ監査を行う場合】

(5) 情報セキュリティ監査を行う事項及び方法

・(情報セキュリティ監査に関して、調達及び応札において確認した事項及び方法を記述する。)

(6) 情報セキュリティ対策の履行が不十分であると思われる場合の対処

・[乙]による情報セキュリティ対策の履行が不十分である可能性を［甲］が認める場合には、［乙］の責任者は、［甲］の求めに応じこれと協議を行い、合意した対応を採るものとする

【確認書を求める場合】

(7) 確認書に委任する事項

・(略)

(8) 再請負に関する事項

【再請負を禁止する場合】

・[乙]は、本契約に係る業務を再請負により第三者に行わせないこと。

【再請負を認める場合】

・[乙]は、［甲］が［乙］に求める情報セキュリティ対策と同水準の情報セキュリティ対策を再請負先に行わせること。

4. 情報の保存・運搬の場合

(1) 取り扱う大学の情報の秘密保持等

・［乙］は、本調達に係る業務の遂行において［甲］が［保存／運搬］を委託する情報について、その漏洩及び毀損を防止するための十分な安全管理を行うこと。

【情報セキュリティ監査を行う場合】

(2) 情報セキュリティ監査を行う事項及び方法

・（情報セキュリティ監査に関して、調達及び応札において確認した事項及び方法を記述する。）

（情報の保存・運搬を外部委託により行う場合には、物品を安全に保存・運搬すること自体が委託先の提供するサービスの内容であることに留意して契約に記載する事項を定める必要がある。以下の各事項については、利用するサービスの契約に実質的に含まれる場合には個々に記載する必要はない。

・情報セキュリティを確保するための体制の整備

・情報セキュリティが侵害された場合の対処

・情報セキュリティ対策の履行状況が不十分であると思われる場合の対処）

付録1 重要な情報を取り扱う情報処理業務及び取り扱わない情報処理業務

1. 重要な情報を取り扱う情報処理業務

以下の情報処理業務は重要な情報を取り扱うものであり、原則として外部委託の対象としてはならない。

(1) ×××システムの構築及び運用

(2) △△△システムの構築に伴う導入

（既存システムとの接続確認及びシステムの設置において既存のxxx システムに保有する重要な情報へアクセスすることが可能となるため）

(3) △△△システムの運用

(4) □□□情報の統計処理

2 重要な情報を取り扱わない情報処理業務

以下の情報処理業務は重要な情報を取り扱わないものであり、外部委託の対象としてよい。

(1) △△△システムの構築（既存システムとの接続確認及びシステムの設置を除く）

(2) ○○○システムの構築及び運用

(3) ◎◎◎情報の統計処理

付録2 情報セキュリティ対策等

[「策定手引書」の「9.3.1 外部委託に係る契約」にある情報セキュリティ対策等の説明記事を引用することができる。本雛形では省略している。]

付録3 組織における情報セキュリティ水準の評価に関する制度

組織における情報セキュリティ水準の評価に活用できる制度に、「情報セキュリティマネジメントシステムに関する評価制度」、「情報セキュリティ対策ベンチマーク」及び「情報セキュリティ監査制度」がある。

(1) 情報セキュリティマネジメントシステムに関する適合性評価制度

委託先における情報セキュリティマネジメントシステムに関して、第三者機関（審査登録機関）による適合性評価に基づく認証を取得していることを委託先の選定の要素に含めることができる。

我が国においては、財団法人日本情報処理開発協会（JIPDEC）が「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」を運営している。

http://www.isms.jipdec.jp/

(2) 情報セキュリティ対策ベンチマーク

情報セキュリティ対策ベンチマークは、事業者が自らの情報セキュリティ対策を評価するための制度であり、評価項目は、対策の取組状況を把握するための評価項目（25 項目）と、企業プロフィールに関する評価項目（15 項目）からなる。本制度に基づく評価結果を委託先の選定の要素に含めることができる。

本制度は、経済産業省が「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」の「参考資料 情報セキュリティ対策ベンチマーク」として公表している。

http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

http://www.meti.go.jp/policy/netsecurity/downloadfiles/1_benchmark.pdf

また、これを独立行政法人情報処理推進機構（IPA）が、ウェブページ上で使える自動化ツールにして提供している。

http://www.ipa.go.jp/security/benchmark/

以上の制度の特徴は、以下の表のとおりである。

これらの両制度の特徴を踏まえ、委託先の情報セキュリティ水準の評価方法を定める。例えば、JIPDEC による「ISMS 適合性評価制度」等情報セキュリティマネジメントシステムに関する適合性評価制度の認証取得を評価の要素に含め、認証を取得していない事業者については情報セキュリティ対策ベンチマークの結果を評価の要素に含めることが考えられる。

	情報セキュリティマネジメントシステムに関する適合性評価制度	情報セキュリティ対策ベンチマーク
概要	組織における情報セキュリティマネジメントに関する評価・認証制度	組織における情報セキュリティマネジメントに関する自己評価のための仕組み
認証基準 及び 管理基準	認証基準：JIS Q 27001:2006 管理策：JIS Q 27002:2006	「情報セキュリティ対策ベンチマーク評価項目」 「ISMS認証基準Ver.2.0」の詳細管理策(JIS X5080:2002(ISO/IEC 17799:2000))に基づき25項目に集約
評価対象の範囲	業務・事業所等、事業者が評価対象の範囲を定める。	事業者全体を対象とすることを想定しているが、業務・事業所等、事業者が範囲を定めて利用することもできる。
評価項目の選択	管理策に基づきリスク評価を実施して評価項目を選択するため、任意性は実質的にない。	定められた一般的に求められる項目
評価の継続性	内部監査及びマネジメントレビューを年1回以上実施する。また、認証登録の継続のため、年1回以上のサーベイランス（維持審査）及び3年ごとの更新審査を受ける。	（評価の継続性を確保する仕組みは定めていない。）
評価の信頼性	認定機関により認定された審査登録機関により客観的な評価・認証が行われるため、信頼性は高い。	自己評価であるため、評価の客観性、信頼性は高くない。
確認できる事項	情報セキュリティマネジメントの維持・改善の第三者機関による評価結果が確認できる。	情報セキュリティマネジメントの維持・改善の自己評価結果が確認できる。 望ましい水準と現在の水準を比較することもできる。
適用性・費用等	情報セキュリティマネジメントシステムに関する認証取得は、現状では限定的。また、認証取得には、費用及び時間を要する。	自己評価であるため簡便に実施でき、費用及び時間について負担が小さい。
委託先の選定における利用手順	委託先候補があらかじめ取得している認証を、登録証及び適用範囲定義書の確認を通じて評価する。	調達手続において情報セキュリティ対策ベンチマークを実施し、その結果を提出することを委託先候補に求める。

(3) 情報セキュリティ監査

将来的に、以下の場合には、上記の制度に替えて情報セキュリティ監査を利用することも考えられる。

① 継続業務である等、直近において同様の情報処理業務を委託しており、情報セキュリティ監査を実施している場合

② 直近において、第三者による情報セキュリティ監査等の手段により、委託元と同等の情報セキュリティ水準にあることが確認できる場合

情報セキュリティ監査は、「情報セキュリティ監査制度」に基づき行うことができる。本制度で定めている「情報セキュリティ管理基準」（経済産業省告示）はISO/IEC 17799:2000 (JIS X 5080:2002) に基づくものであり、この点は、ISMS適合性評価制度の「ISMS 認証基準 Ver2.0」と同様である。

http://www.meti.go.jp/policy/netsecurity/audit.htm

なお、監査主体を選定する際の参考に資するよう、任意登録制の「情報セキュリティ監査企業台帳」が整備されている。

http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html

また、本制度については、特定非営利活動法人日本情報セキュリティ監査協会（JASA）が普及促進に係る活動を行っている。

http://www.jasa.jp/index.html

A3112 ソフトウェア開発における情報セキュリティ対策実施手順(策定手引書)

1. 本書の目的

本書は、本学において利用される「ソフトウェア開発手順書」にセキュリティに関する事項を追加し、改善するための参考文書（以下「ソフトウェア開発における情報セキュリティ対策実施手順」という。）を整備するための手引書である。

本学においては、ポリシー並びに実施手順及びそれらを具体化する一連の実施手順群を整備することが求められている。「ソフトウェア開発における情報セキュリティ対策実施手順」は、これらの実施手順の一つとして策定し、学内でソフトウェアを開発する場合に適用するものである。すなわち、本学においてソフトウェア開発に携わる者がこれに従うことにより、ポリシー及び実施規程の関係する規定を遵守することとなるものである。

ソフトウェアにおけるセキュリティの実現については、開発ライフサイクル（Software Development Life Cycle）である要件定義、設計、実装、テストの各工程におけるセキュリティ対策を的確に実施することが求められる。

本書は、これらの背景の下で、「ソフトウェア開発における情報セキュリティ対策実施手順」に含めるべき手順及び記述例を具体的に示し、もってポリシー及び実施規程への準拠性、業務手順への適用性等において適切な規定の整備に資することを目的とする。

2. 実施手順に記載すべき事項

「ソフトウェア開発における情報セキュリティ対策実施手順」には、以下の事項を具体化させて記載すること。

2.1 情報システム運用・管理規程に定める「ソフトウェア開発における情報セキュリティ対策実施手順」に係る遵守事項

なし。

3. 文書構成例

「ソフトウェア開発における情報セキュリティ対策実施手順」は、セキュリティの高いソフトウェア開発を行うにあたって必要となるセキュリティ対策の観点を解説しつつ、最終的にソフトウェア開発手順書に統合できる構成とすべきである。文書構成の例を以下に示す。

1 本書の背景と目的
 1.1 本書の背景
 1.2 本書の目的

4. 作成する上での留意事項

「ソフトウェア開発における情報セキュリティ対策実施手順」は、以下のことに留意して作成する。

(1) ポリシー及び実施規程はセキュリティの視点から遵守事項を記載している。これに対し「ソフトウェア開発における情報セキュリティ対策実施手順」は、ソフトウェア開発のライフサイクルに沿って記述すると既存のソフトウェア開発手順書に統合しやすく、かつ理解されやすいものとなる。

(2) 解説を補足するための図や実際に使用している帳票を使用し、個々のフェーズごとに具体的に説明を加えると理解されやすいものとなる。

(3) セキュリティの高いソフトウェアを開発するに当たって実施すべき標準的な事項を記述し、ソフトウェア開発を外部委託している場合においても、他の情報セキュリティ関係規程と併用することで、発注者として外部委託事業者を適切に管理するための資料として有効に活用されやすいものとなる。

(4) 2 章に示す事項を「ソフトウェア開発における情報セキュリティ対策実施手順」に反映するに当たっては、当該事項の内容に応じて、以下のいずれかの方針で記述するとよい。

[具体化]・・・一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、表現をより具体的に修正・追加することにより盛り込む。

[転記]・・・・記述内容がそのまま具体性を持ち、そのままの形で十分と思われる遵守事項については、これを転記することにより盛り込む。

[詳細化]・・・記述内容がそのまま具体性を持っているが、利用者の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、これを詳細化して盛り込む。

5. 参考資料

「ソフトウェア開発における情報セキュリティ対策実施手順」の作成に際しては、以下のような資料が参考となる。

5.1 国際規格及び諸外国を含む政府及び政府関係機関の資料

(1) ISO/IEC 15408 「Common Criteria」 (JIS X 5070)
(2) ISO/IEC 27002「Information technology - Security techniques - Code of practice for information security management」(JIS Q 27002)
(3) IPA「セキュア・プログラミング講座」
（http://www.ipa.go.jp/security/awareness/vendor/programming/）
(4) IPA：「セキュアな Web サーバーの構築と運用」
（http://www.ipa.go.jp/security/awareness/administrator/secure-web/）
(5) IPA：「消費者向け電子商取引サイトにおける注意点」
（http://www.ipa.go.jp/security/vuln/20050304_ec_security.html）
(6) IPA：「脆弱性関連情報に関する届け出状況」
（http://www.ipa.go.jp/security/vuln/20050304_ec_security.html）
(7) SLCP-JCF／共通フレーム 98（ISO/IEC 12207）
(8) NIST Special Publication 800-53 「Recommended Security Controls for Federal Information Systems」
(9) NIST Special Publication 800-64「Security Considerations in the Information System Development Life Cycle」

5.2 政府・政府関係機関以外の資料

(1) Microsoft：「信頼できるコンピューティングのセキュリティ開発ライフサイクル」
（http://www.microsoft.com/japan/msdn/security/general/sdl.asp）
(2) Microsoft：「Web アプリケーション セキュリティ強化」

（http://www.microsoft.com/japan/msdn/security/guidance/secmod71.mspx）

6. 雛形の利用方法

別紙１の雛形を参考にして、「ソフトウェア開発における情報セキュリティ対策実施手順」を策定すると効率的である。別紙１の雛形は、前記 2 の実施手順に記載すべき事項を、前記 3 の文書構成例の枠組みの中に記載したものである。

6.1 雛形において想定する前提

本雛形は、以下を前提として記述している。

- 標準化されたソフトウェアの開発手順書が存在している。

そのため、使用する環境が上記の前提と異なる場合には、適宜、修正、追加又は削除する必要がある。

6.2 手直しポイント

各大学においてポリシー及び実施規程におけるセキュリティの遵守事項を盛り込んだソフトウェア開発手順書を作成するには、大別して、新規で作成する場合と既存の文書を修正する場合とがあるが、そのどちらの場合でも、以下の事項を踏まえて作業を行う必要がある。

(1) ソフトウェアは、その開発規模、開発期間、予算的制約等によって、最適な開発方法が異なることから、雛形の全要求事項を画一的に適用することは好ましくない。特に、比較的小規模なソフトウェアについては本書の要求事項の適用が現実的ではない場合が多い。このため、適用させる前に要求事項に所要の変更を加える必要性の有無を検討する必要がある。なお、雛形では、要求事項を箇条書きにして「●」記号を付加している。各大学においては、自組織における業務の内容とポリシー及び実施規程にかんがみ、適宜、要求事項を追記又は削除する。また修正が必要となる箇所等には、以下の記号を付加している。

(a) 雛形中に、*[・・・]* 形式で明記される部分（大学名、担当者等）については、各大学内の定めに合わせる。

(b) 雛形中に、【・・・の場合】形式で明記される記述については、想定される案を記したものであり、各大学の判断により適宜、選択又は修正する。

(c) ≪図・・・≫は、開発手順書の策定者向けの解説資料であり、適宜判断の上、修正又は削除する必要がある。

(d) ≪参考文献≫は、セキュリティの高いソフトウェアを開発するための参考資料であり、適宜判断の上、修正する必要がある。

(2) ソフトウェア開発における役割分担については、組織や開発プロジェクトによって様々であるため、各大学の開発手順書では、自組織の構成や各担当者のソフトウェア開発に

関する責務を考慮した上で、主語の追記又は変更を検討する。

(3) 雛形において使用しているソフトウェア開発に関わる用語等については、大学において既に用いられている用語と平仄を揃える。例えば、ソフトウェア開発の工程を意味する「要件定義」「設計」という用語等は共通化された呼称ではなく、組織やプロジェクトによって定義や利用方法が異なっているため、必要に応じて修正を加える。

(4) 既存の情報セキュリティ関係規程との整合性を考慮し、適切な分割、統合、相互参照を検討する。

(5) 情報セキュリティ対策の観点以外の一般的な記述について、雛形の内容では不足があると思われる場合には、適宜、補う。

別紙１　ソフトウェア開発における情報セキュリティ対策実施手順　雛形

【本書の利用に当たって】

ソフトウェアにおけるセキュリティの実現については、開発ライフサイクル（SDLC: Software Development Life Cycle)におけるセキュリティ対策が重要な意味を持つ。このことから本書では、学内でソフトウェア開発を行う場合の「ポリシー及び実施規程」の遵守事項の実装手法について解説する。

なお、ソフトウェアは、開発規模、開発期間、予算的制約等の相違によって、開発手法も多様化している。このため、本書が想定している開発手法ではなく、それぞれの組織がこれまで利用してきた開発手法を用いる方が適切な場合もあり得る。よって、この場合は本書に記載されたソフトウェア開発におけるセキュリティ対策実施手順を整理し、組織独自の開発手法の中に統合する必要がある。

本書に記載する要件は、完全かつ網羅的なものではないが、高いセキュリティが求められるソフトウェアを開発する際の出発点、及び ISO/IEC15408（Common Criteria）導入の事前準備として有効に利用できる。また、ソフトウェア開発ライフサイクルにおいて考慮すべきセキュリティに関する事項について理解を深める際に役立つ参考文献を、本書中でその出所を記した上で紹介している。参考文献は、国際標準、又はインターネットにおいて入手が比較的容易であるものを優先して掲載している。

なお、本書においては、別途作成される策定手引書及び参考文献との併用を意図していることから、以下の内容に関する詳細な説明は本文に含めていない。

・情報の格付けに関する事項
・コーディングに関するセキュリティ事項
・ソフトウェア開発を委託する場合の調達・契約に関するセキュリティ事項
・セキュリティ設計仕様書（Security Target）の評価、確認に関する事項

本書の位置付け

本書は、各大学のソフトウェア開発手順書にセキュリティに関する事項を追加し、改善を促すための手引書の雛形であり、「ソフトウェア開発におけるセキュリティ対策実施手順 策定手引書」の２に示す実施手順に記載すべき事項を、同３に示す文書構成例の枠組みの中に盛り込み作成したものである。

手直しポイント

各大学においてポリシー及び実施規程で規定する遵守事項を盛り込んだソフトウェア開発手順書を作成するには、大別して、新規で作成する場合と既存の手順書を修正する場合とがあるが、そのどちらの場合でも、以下の事項を踏まえて作業を行う必要がある。

(1) **ソフトウェアは、その開発規模、開発期間、予算的制約等によって、最適な開発方法が異なることから、雛形の全要求事項を画一的に適用することは好ましくない。特に、比較的小規模なソフトウェアについては本書の要求事項の適用が現実的ではない場合が多い。このため、適用させる前に要求事項に所要の変更を加える必要性の有無を検討する必要がある。なお、雛形では、要求事項を箇条書きにして「●」記号を付加している。各大学においては、自組織における業務の内容とポリシー及び実施規程にかんがみ、適宜、要求事項を追記又は削除する。また修正が必要となる箇所等には、以下の記号を付加している。**

(a) **雛形中に、*[・・・]* 形式で明記される部分（大学名、担当者等）については、各大学内の定めに合わせる。**

(b) **雛形中に、【・・・の場合】形式で明記される記述については、想定される案を記したものであり、各大学の判断により適宜、選択又は修正する。**

(c) **≪図・・・≫は、開発手順書の策定者向けの解説資料であり、適宜判断の上、修正又は削除する必要がある。**

(d) **≪参考文献≫は、セキュリティの高いソフトウェアを開発するための参考資料であり、適宜判断の上、修正する必要がある。**

(2) **ソフトウェア開発における役割分担については、組織や開発プロジェクトによって様々であるため、各大学の開発手順書では、自組織の構成や各担当者のソフトウェア開発に関する責務を考慮した上で、主語の追記又は変更を検討する。**

(3) **雛形において使用しているソフトウェア開発に関わる用語等については、大学において既に用いられている用語と平仄を揃える。例えば、ソフトウェア開発の工程を意味する「要件定義」「設計」という用語等は共通化された呼称ではなく、組織やプロジェクトによって定義や利用方法が異なっているため、必要に応じて修正を加える。**

(4) **既存の情報セキュリティ関係規程との整合性を考慮し、適切な分割、統合、相互参照を検討する。**

(5) **情報セキュリティ対策の観点以外の一般的な記述について、雛形の内容では不足があると思われる場合には、適宜、補う。**

商標について

本資料に記載されている会社名、製品名は、それぞれの会社の登録商標又は商標です。

1. 本書の背景と目的

1.1 本書の背景

近年、業務全体のうち、何らかのソフトウェアを用いるものが占める比重は増大しており、これに比例するようにソフトウェアは大規模化、複雑化の一途をたどっている。これに伴いソフトウェアの品質を確保することが困難となったことから、この課題を解決する様々なソフトウェア開発の方法論が検証され、その標準化が進められている。代表的なものとして、ソフトウェアのライフサイクルの観点から検討された共通フレーム 98 や CMMI、あるいはマネジメントの観点のから検討された PMBOK や ISO9001 などが挙げられる。

また、一時代前においてはソフトウェアが満足すべき品質の一要素でしかなかったセキュリティは、高度化する情報通信ネットワークへの業務の依存度が著しく増大したことによって、リスクマネジメントの観点から、コストや納期、又は保守性や操作性といった品質に優先して組織が取り組むべき最優先の課題へと押し上げられることとなった。こうしたことから、ソフトウェア開発において、『セキュリティを考慮した開発方法論』が必要とされてきている。

セキュリティ面からのソフトウェア開発へのアプローチとしては、代表的なものとして、IT 関連製品のセキュリティ評価手法である ISO/IEC15408（Common Criteria：CC）が存在する。しかしながら、CC は高い網羅性を持つ万能のセキュリティ標準として作成されていることから、一般のセキュリティ管理者にとっては、個々の情報システムに適用させるのが難解であるという一面もあるため、十分に普及しているとはいえない状況である。

1.2 本書の目的

本書は、セキュリティの高いソフトウェアを開発するために、*[○○大学]*で採用しているソフトウェア開発手順を、ポリシー及び実施規程が定めるセキュリティの観点から補完し、改善を促すことを目的としている。

セキュリティの高いソフトウェアを開発するために実施すべき事項を概観すると、以下のとおりとなる。

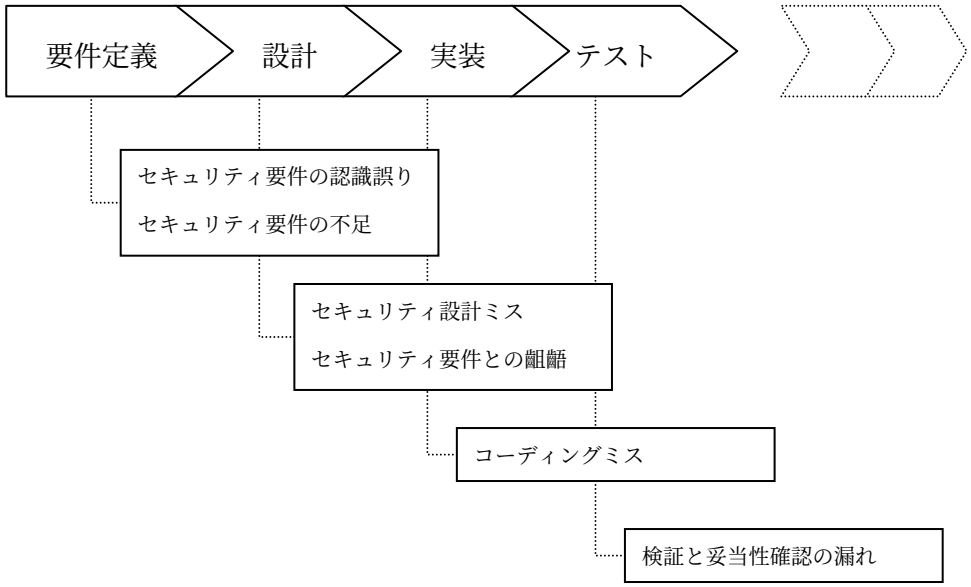
(1) 開発作業、場所、情報資産、要員に関する適切なセキュリティの管理
(2) 適切なセキュリティ機能の設計及び実装
(3) セキュリティの脆弱性の排除

そして、これらの事項を達成するためには、組織のソフトウェア開発手法をセキュリティの観点から修正し、セキュリティを確実に実現できる開発手法に改善する必要がある。

具体的には、ソフトウェア開発のライフサイクル（要件定義、設計、実装、テスト）の各工程について、混入されるおそれのある脆弱性を排除し、セキュリティの品質を向上させる

ために実施すべき対策を開発手法に含めることにより、これを実現する。

≪図 1-1：ソフトウェア開発ライフサイクルにおいて混入する脆弱性≫



本書はセキュリティの高いソフトウェアを開発するに当たって実施すべき標準的な事項を*[○○大学]*内部でソフトウェアを開発する場合を想定して記載したものである。この趣旨から、外部委託によりソフトウェアを開発する場合においても、[情報システムにおける情報セキュリティ対策実施手順及び外部委託における情報セキュリティ対策実施手順と併用することで]発注者として外部委託事業者を適切に管理するための資料として有効に活用できる。

≪参考文献≫

- SLCP-JCF／共通フレーム 98（ISO/IEC 12207）
  ソフトウェア開発及び取引を明確化し、利用者と開発者が共通の尺度を持つための枠組みを解説したもの。ソフトウェア構築時の作業手順や役割分担を明確化すること、契約時の相互の認識の不一致を防止することを目的として策定されている。
- NIST Special Publication 800-64「Security Considerations in the Information System Development Life Cycle」
  情報システムの開発ライフサイクル(System Development Life Cycle)においてセキュリティを確保するための枠組みを解説したもの。
- Microsoft：「信頼できるコンピューティングのセキュリティ開発ライフサイクル
  （http://www.microsoft.com/japan/msdn/security/general/sdl.asp）
  重大な脅威にさらされるソフトウェア向けにマイクロソフト社が採用しているセキュリティ開発ライフサイクル(Security Development Lifecycle)を示したもの。

2. 本書の対象者

本書は、セキュリティの立場からソフトウェア開発に携わる*[部局技術責任者]*を対象とする。

3. 開発体制の構築及びソフトウェア・情報資産の保護

【趣旨】
セキュリティの高いソフトウェアを開発するためには、そのために必要となる措置を確実に実現できる体制の確保が必須である。
また、開発されるソフトウェア及び開発において使用される情報を適切に保護するためには、開発に用いる施設や環境、開発に要する情報資産に関するセキュリティの管理も考慮しておく必要がある。
本項では、セキュリティを実現するためのソフトウェア開発における体制の構築やこれに係る情報資産の保護について解説する。

3.1 開発体制に係るセキュリティ

開発担当者にセキュリティに関する責務が正式に割り当てられていなかったり、担当者の能力が不足している場合、セキュリティの高いソフトウェアの開発は不可能である。セキュリティの高いソフトウェアを開発するために必要とされる作業を明確化した上で、専門的な知識を持った要員の配置や当該要員に対する教育等、セキュリティにかかわる対策事項を満たすことが可能な開発体制を構築しなければならない。

(1) ソフトウェア開発に係る役割の明確化

- ソフトウェア開発の責任者に対して、セキュリティの高いソフトウェアを開発するために必要となる作業を特定し、十分な人員を割り当てることを要求すること。

セキュリティの高いソフトウェア開発を確実に実現するために、ソフトウェアのセキュリティ要件に応じて必要な各作業（要件定義→設計→実装→テスト）についてその担当者を明確にし、その的確な実施を求めなければならない。

(2) 開発担当者へのセキュリティ教育

- ソフトウェア開発の責任者に対して、開発担当者に対する適切なセキュリティ教育を行うことを要求すること。

ソフトウェアを開発する作業を行う担当者に、割り当てられたセキュリティに関する役割を確実に達成させるために、知識や能力を向上させるためのセキュリティ教育を求めなければならない。

3.2 ソフトウェア・情報資産の保護

開発場所の入退室管理や開発に要する情報資産の管理に不備があれば、開発に関する機密性の高い情報が外部に流出したり、不正なプログラムがソフトウェアに埋め込まれるおそれなどが高まる。このため、セキュリティの高いソフトウェアを開発する前提として開発を行う場所や開発に要する情報資産に係るセキュリティを確保しておかなければならない。

(1) 施設と環境のセキュリティ

- ポリシー及び実施規程に準拠して、ソフトウェア開発を行う施設と環境を安全区域として保護すること。

【運用中の情報システムとの分離が必要な場合】

- 運用環境とは物理的・論理的に分離された環境で、ソフトウェアの開発・試験を実施すること。また、開発担当者が運用環境において作業を行う場合は、責任者の承認を受け、作業内容を記録すること。

悪意のある者が容易に接触できる状況においては、セキュリティを維持しつつソフトウェアを開発することが困難である。このため、重要なセキュリティ要件を持つソフトウェア開発を行う施設については、ポリシー及び実施規程に準拠して、入退室管理を含めた安全区域の物理的管理を実施する必要がある。また、運用中の情報システムへの悪影響を防ぐため、開発・試験環境と運用環境は物理的・論理的に分離し、開発者の運用環境へのアクセスを制限しなければならない。

(2) 開発に要する情報資産のセキュリティ

- ソフトウェア開発時に必要となる要保護情報及び関連する情報資産は、責任者の承認を受けた上で利用し、利用状況を記録すること。また、利用が許可された情報等は適切に保護すること。
- コンパイラ、エディタ、その他ユーティリティ等の開発に要する資産は、責任者の承認を受けた上で利用し、利用状況を記録すること。また、利用が許可された資産等は適切に保護すること。
- 本番運用データは原則テストデータとして使用しないこと。やむを得ず使用する際は要機密情報を消去した上で使用すること。
- ソースコードついて、許可された利用者以外のアクセス（閲覧・変更）を制限し、滅失、き損等に備えたバックアップの取得を行うこと。

ソフトウェア開発の担当者は、*[○○大学]*の所有する要保護情報及び関連する情報資産の取扱いを任され、当該情報等を通常とは異なった運用に用いることになる。このような場合においては、情報資産を盗難、改ざん、滅失等から防ぐために使用に際しての申請、承認及び記録並びに使用後の返却及び消去を徹底するなど、当該情報等について厳格な管理を行わなければならない。

【セキュリティ要件を明確にする必要がある場合】

4. セキュリティの要件定義

【趣旨】
要保全情報を取り扱い、不特定多数の人間が接続するインターネット上で利用されるソフトウェアについては、外部からの攻撃等による改ざんが生じないセキュリティ品質が要求される。また、要機密情報を取り扱うソフトウェアについては、情報の漏えいが生じないセキュリティ品質も要求される。このように、個々のソフトウェアの重要性や利用環境に応じて必要とされる要求事項は異なるため、それぞれの場合について、情報資産を守るために求められるセキュリティの要求事項が何であるかを検討しなければならない。この要求事項を「セキュリティ要件」と呼ぶ。
本項では、ソフトウェアのセキュリティ要件について解説する。

4.1 セキュリティ要件の定義

ソフトウェアのセキュリティ要件は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果、及び当該ソフトウェアにおいて取扱う情報の格付けに応じて決定される。セキュリティ機能の必要性を認めた場合、セキュリティ要件をセキュリティ要件定義書として文書化する。

(1) セキュリティ要件定義書の作成

- **ソフトウェアのセキュリティ要件定義書を作成し、これに基づきセキュリティの設計と実装を行うこと。**

ソフトウェアのセキュリティ要件について、共通の認識を持ち、組織としてセキュリティに取り組むためには、要件定義書として文書化しなければならない。セキュリティ要件定義書はセキュリティ機能の設計と実装を求めるための根拠となる。

なお、セキュリティ要件定義書の作成に当たっては、開発対象となるソフトウェアのセキュリティを確保する観点のみならず、直接・間接に結びついた他の情報システムへの影響も

考慮に入れておく必要がある。これは、例えば対象となるソフトウェア自体の重要度が低い場合であっても、不正侵入の脅威が大きい環境に設置されるのであれば、踏み台にされ、他の情報システムを脅威にさらす可能性があるからである。

(2) **ポリシー及び実施規程の遵守との整合性**

- **ポリシー及び実施規程と整合性を持つセキュリティ要件定義書を作成すること。**

***[○○大学]*が遵守すべきルールや前提条件に準拠したソフトウェアを開発するため、セキュリティの要件定義書は、*[○○大学]*のセキュリティの遵守事項をまとめたポリシー及び実施規程と整合性を持つ必要がある。**

【セキュリティ機能が必要な場合】

5. セキュリティ機能の設計・実装・構成管理

【趣旨】
「ソフトウェアが行うべきこと（What）」を定めたセキュリティの要件定義に則って、「ソフトウェアが行う方法(How)」を設計し、この設計に基づいて確実な実装を行わなければならない。
また、ソフトウェアの大規模化、複雑化が進むにつれて、開発の初期段階において要件や設計を完全に定義することは困難となり、仕様の変更は避けられない事象となりつつある。こうした変更は、セキュリティの脆弱性を生じさせる原因となるおそれがあるため、適切な構成管理が重要である。
本項では、セキュリティ機能の設計と実装及び構成管理について解説する。

5.1 セキュリティの設計

ソフトウェアのセキュリティ要件定義により明確にされた要求事項を満たすソフトウェアを開発するためには、その要求を満たすための具体的な機能を設計しなければならない。この際、セキュリティの実装の段階で齟齬が発生しないように、設計書を正確に具体化していく必要がある。

また、あらゆる脅威を想定し、それらに対して完全な措置を講ずることは、実際には困難であることから、セキュリティが侵害された場合の対策をあらかじめ設計をしておく必要がある。

(1) **セキュリティの設計**

- **ポリシー及び実施規程とセキュリティの要件定義に準拠してセキュリティの設計を行うこと。**

セキュリティの要件定義を精査した上でセキュリティに関する設計を行う。セキュリティの設計は、セキュリティ要件定義を満たす網羅的な構成を取る必要がある。

加えて、セキュリティの設計は本学が遵守すべきセキュリティ事項を網羅しているポリシー及び実施規程を前提条件とした内容となっていることを確認しなければならない。これによって、強力な認証やアクセス制御、妥当性の検証など、強固なセキュリティの設計を行う必要がある。また、客観性や網羅性を保つ観点から、ポリシー及び実施規程に加えて、その他の信頼できる文献を併用することも有益である。

≪参考文献≫

- ISO/IEC 15408 Common Criteria (JIS X 5070)
  IT 製品及びシステムのセキュリティ機能の開発を対象とした評価規格を示したもの。概説（Part1）、セキュリティ機能要件（Part2）、セキュリティ保証要件（Part3）の三部から構成される。CC の Part2 は、セキュリティ機能要件のセットであり、セキュリティ設計・実装の参考書として有効に活用できる。
- ISO/IEC 27002（JIS Q 27002）
  組織の情報セキュリティマネジメントに基づいて推奨されるべきセキュリティコントロールを体系的に定めた規格を示したもの。
- NIST Special Publication 800-53「Recommended Security Controls for Federal Information Systems」
  米政府の各省庁における情報システムの分類された結果（Low/Moderate/High）に基づき実施すべきセキュリティコントロールのベースラインセットを示したもの。

(2) 設計書におけるセキュリティ機能の具体化

- セキュリティの設計を設計書において具体化し、記述すること。

ソフトウェアの設計は、作業段階に応じて基本設計から詳細設計へと具体化され、設計書として文書化される。

ソフトウェアの開発規模、複雑性等によって、どのレベルまで詳細な設計書を必要とするかは異なるが、実装段階での齟齬を防止するため、セキュリティ機能を具体化し、明確に記述しておく必要がある。

【セキュリティ機能として、セキュリティの管理機能が必要な場合】

(3) セキュリティの管理機能の設計

- 開発するソフトウェアが運用される際に利用されるセキュリティ機能の管理機能を設計すること。

「管理機能」とは、真正確認、権限管理等のセキュリティ機能を管理するための機能のほか、証跡保全の機能等の故障、事故、障害等の発生時に行う対処及び復旧にかかわる機能等を指す。これらの機能をソフトウェアのセキュリティ要件に応じて、セキュリティの管理機能をソフトウェアに組み込む必要がある。

【開発するソフトウェアに重要なセキュリティ要件がある場合】

(4) ST 評価・ST 確認の実施

- 重要なセキュリティ要件があるソフトウェアに対して、セキュリティ設計仕様書（Security Target）の評価・確認を実施すること。

開発するソフトウェアに重要なセキュリティ要件があると判断されたソフトウェアについては、セキュリティ要件定義の結果を受けて、セキュリティ設計仕様書（Security Target）を策定し、セキュリティ機能の設計において、第三者機関による ST 評価・ST 確認を受ける必要がある。

【権限管理の設計が必要な場合】

5.2 設計のポイント - 権限管理

ソフトウェアにおいて要機密情報の漏えいなどを防止する手法のうち一般的なものとして、権限管理機能がある。『権限管理』とは、識別と真正確認の結果である『認証』に対して、『アクセス制御』すなわち、権限の割当てや制限を強制することである。

(1) 権限管理対象とする情報の識別

- ソフトウェアで権限管理を行うべき情報を識別すること。

ソフトウェアのセキュリティ要件を定義する際に実施した当該ソフトウェアで取り扱う情報の格付けの結果に基づき、「権限管理」すべき情報を識別しなければならない。その上で、必要とされる権限管理の強度を慎重に判断する必要がある。

この際、ソフトウェアが取り扱う行政事務情報以外の重要な情報にも注意する必要がある。特に識別子、パスワード、暗号鍵、ソースコード、パラメータ、セッション情報、監査ログ等のシステム構成情報については、慎重な検討を要する。

(2) 権限管理の設計

- ポリシー及び実施規程に準拠して、ソフトウェアのセキュリティ要件に応じた識別（特定された一意の識別子など）、認証（知識・所有・生体による認証）に基づいた権限管理機能及びそれを支援するための暗号、電子署名、証跡管理等の機能を設計すること。

- ポリシー及び実施規程に準拠して、識別された要保護情報に適切な権限管理を行うこと。
- ポリシー及び実施規程に準拠して、プログラムが所有する特権を特定し、必要最小限の権限に制限すること。

権限管理対象の識別結果に基づいて、権限管理の設計を行う。この際、情報システム運用・管理規程「第七章　アカウント管理」に準拠した十分な強度の権限管理を設計し、識別された情報を保護する必要がある。特に、システム構成情報はソフトウェアのセキュリティにかかわる情報であり、システム構成情報のセキュリティが侵害された場合、セキュリティ機能が迂回されたり、無力化される可能性があるため、慎重な権限管理の設計が必要である。

また、権限管理の設計においては、必要な情報に適切な権限管理を行い、不要な権限を割り当てないことが重要である。

【情報の妥当性の検証に係る設計が必要な場合】

5.3 設計のポイント - 情報の妥当性の検証

ソフトウェアは、入力された情報を正確に処理し、その結果を出力することをその基本的な目的としている。この目的を確実に達成するため、妥当性の検証によって、処理の誤りや悪用される可能性のある情報などから、情報と処理方法の完全性を保護する必要がある。

特に悪意のある情報の入力によってソフトウェアの完全性を侵害する攻撃は、現在ソフトウェアに対する最も重大なセキュリティ脅威となりつつあり、その対応に注意が必要である。

(1) 妥当性検証を行うべき情報の識別

- ソフトウェアで妥当性検証を行うべき情報を識別すること。
- 利用者及び外部プログラムとやり取りするものを含めてすべての入力される情報について、悪意ある情報が含まれると仮定した上で、妥当性の検証を行うこと。

「妥当性の検証」を行うべき情報を識別しなければならない。

この際、特にソフトウェアに「入力」される情報には注意を払う必要がある。入力される情報は常に信頼できるものとは限らない。すべての入力される情報には悪意ある情報が含まれると仮定した上で、識別子、パスワード、入力フォームといった開発者が「入力を想定している情報」だけではなく、「入力を許可している情報」に対しても識別を行わなければならない。

なお、外部の利用者による入力だけでなく、当該ソフトウェア以外の外部のプログラム等とやり取りされる情報についても、ソフトウェアの内部で検証を行う必要がある。

(2) 情報の排除

- 悪用される可能性のある情報を識別し、排除すること。

情報の排除とは、悪用される可能性のある情報の型等を定義し、当該情報が含まれる場合に不正な部分の除去、置換等の処理を行う手法である。

悪用される可能性のある情報としては、プログラム内部や最終的な出力において特別な意味を有する特殊文字がある。情報の排除は、可能な限り手作業を排し、自動化されたプロセスを実装することが望ましい。

なお、処理を OS やミドルウェアなど外部のプログラムに引き渡す場合は、情報を使用するプログラムと検証するプログラムが異なることから、作業漏れが発生しやすい。こうした場合においても悪用される可能性のある情報を確実に排除しておく必要がある。

(3) 入力の制限

- 入力を許可する情報の型等を定義して、合致した情報のみの入力を許可すること。
- 悪用される可能性のある情報の型等を定義して、その定義に合致する情報の入力を拒否すること。
- 許可されない入力に対しては、リスクを想定して適切なエラー処理を実施すること。

入力の制限とは、許可した情報以外の入力を拒絶し、リスクに応じて適切なエラーの処理（再確認、終了、警告等）を行う手法である。

これには、入力を許可する情報の型等を定義して、その定義に合致した情報のみの入力を許可する手法と悪用される可能性のある情報の型等を定義し、その定義に合致した情報の入力を拒否する手法がある。これらのうち、適切な手法について検討し、実施する必要がある。

5.4 セキュリティの実装を支援するための枠組み

セキュリティの実装は、個々のプログラマのスキルによって差異が生じがちである。責任者の視点から重要な点は、プログラマ個々の知識に依存せず、コーディング規約の統一等によって開発方法を標準化することで、実装時に混入する脆弱性を最小限に抑制する点にある。

(1) コーディング規約におけるセキュリティ

- 最新のセキュリティ技術を反映したセキュアコーディングに関する注意事項を記載したコーディング規約を作成すること。
- セキュアコーディングに関する注意事項について、定期的にプログラマに教育を実施し、その浸透を図ること。

プログラミング作業の品質と保守性を向上させるために、「コーディング規約」を作成する。「コーディング規約」は命名、スタイル、コメント、改行・インデント、関数・クラス・変

数の取扱い等、様々な事項をルールとして網羅的に定めたものである。

ソフトウェアを開発する組織は、実装段階における脆弱性の混入を防ぐため、コーディング規約にセキュリティに関する注意事項を記載し、教育などを通してその運用を徹底し、個々のプログラマの知識に依存しない仕組みを確立することによって、確実なセキュリティの実装を図る必要がある。

組織がコーディング規約を策定する際のセキュリティ事項については、文献を参考にできるが、参考文献のみでは最新の攻撃手法に対応することが難しいため、外部の専門家の支援や専用ツールの購入などの手法で、コーディング規約を更新していくことも必要である。

≪参考文献≫

・ IPA「セキュア・プログラミング講座」
（http://www.ipa.go.jp/security/awareness/vendor/programming/）
セキュリティの脆弱性を発生させないようなプログラミングテクニックを示したもの。

5.5 構成の管理

不十分な構成管理は、開発者によるバックドアや隠れチャネルの埋め込みなどのセキュリティ上の深刻な問題を引き起こす原因となる。また、現在のソフトウェア開発においては、開発の過程で、仕様の変更が発生することが多い。これらの問題に対処するため、ソフトウェアの構成要素の変更、追加、削除を管理し、ソフトウェアの完全性を確保するための手続である構成管理を適正に実施する必要がある。

(1) 構成要素の識別

- ソフトウェア開発に関する構成要素を識別した上で、各構成要素を一意に識別し、バージョン番号を付与し管理すること。

セキュリティの高いソフトウェアを開発するためには、各工程において作成される仕様書、ソースコードその他管理の対象とすべき構成要素のセキュリティを保護しなければならない。

こうしたソフトウェアの各構成要素は、一覧を作成する等の手法で明確に識別して、バージョン管理を行う必要がある。また、識別された構成要素に対して、アクセス制御やバックアップの取得などの十分な保護対策を実施しなければならない。構成要素として、下記のようなものが想定できる。

(a) 開発プロジェクトの計画関連のドキュメント
(b) 実装関連ドキュメント
(c) 要件・設計ドキュメント
(d) テスト関連ドキュメント

(e) **運用ガイダンス**

(f) **構成管理ツール**

(2) **構成変更の管理**

- **構成要素の変更管理を行う前提として、開発関係者の合意の結果をベースラインとして定義し、許可された利用者以外のアクセス（閲覧・変更）から保護すること。**
- **ベースラインの設定以降に構成要素の変更を行う場合には、正式な変更申請手続を行うこと。変更作業の内容は記録として保持すること。**
- **構成要素の変更申請に対して、ソフトウェア開発を行う責任者はその影響を検証すること。変更作業は、緊急時も含めて承認された後に実行すること。**

ソフトウェアの開発過程における仕様変更や発見された欠陥に対処するためのプログラム・モジュール構成の修正又は当該修正に伴うドキュメントからの乖離は、セキュリティの脆弱性を発生させる原因となる。

このため、各構成要素について、ある時点での開発関係者の合意の結果をベースラインとして定義し、ベースラインが設定された以降の変更は、正式な手続を通して厳格に管理する必要がある。

なお、変更が発生する要因としては、仕様が変更された場合と欠陥が発見された場合の修正が考えられる。仕様変更は、さらに要求変更、設計変更、実装変更に分類することができる。ソフトウェア開発を行う責任者はこうした変更の必要性と影響を検証した上で変更内容を承認し、かつ修正に関する記録を残しておかなければならない。

(3) **構成管理の自動化**

- **構成管理ツール等の利用により、正確かつ効率的な構成管理を行うこと。**

構成変更は、開発するソフトウェアの規模が大きく複雑になると、大量に発生する可能性がある。また、特定の構成要素の修正によって、他の構成要素に変更が生ずることも想定される。

このようなことに対処し、構成管理作業の正確性や効率性を確保するために、構成管理ツール等を利用しなければならない。

6. セキュリティの検証と妥当性確認

【趣旨】

ソフトウェアは、その開発ライフサイクルの各工程で的確な作業がなされることで、本来求められるセキュリティをはじめて確保することができる。そして、各工程での作業の的確性を判断し、ソフトウェアの脆弱性を可能な限り減少させるためには、厳格な検証と妥当性確認が不可欠である。
本項では、セキュリティの視点からの検証と妥当性確認、及びその際のポイントとなる既知の攻撃手法について解説する。

6.1 セキュリティの検証と妥当性確認

高い品質のソフトウェアを開発するためには、各工程が前の工程の成果物を受けて正しい作業が行われているかを検証し、かつ各工程の作業結果が、上流工程で定められた目的や要件に合致しているかの妥当性の確認を徹底する必要がある。この検証と妥当性確認は、セキュリティの品質を保証する意味でも、中核的な位置付けとなる作業である。

(1) 開発工程へのセキュリティの検証と妥当性確認の組込み

- **セキュリティの検証と妥当性確認を開発工程に組み込むこと。**

ウォーターフォールモデルでもスパイラルモデルでも基本的な開発の流れは「要件定義→設計→実装→テスト」の順序で進行する。いずれのモデルを採用するにせよ、各工程にセキュリティの検証と妥当性確認を計画的に組み込む必要がある。

【セキュリティの専門家による確認が必要と判断した場合】

(2) セキュリティの専門家による検証と妥当性確認

- **セキュリティの検証と妥当性確認を行うための専門家が、開発者による設計や実装作業が適正であるかどうかを確認すること。**

脆弱性は、開発者の思いこみや盲点を原因として発生する場合が多い。この対策として、セキュリティの検証と妥当性確認を行う専門の担当者を配置する必要がある。
なお、検証と妥当性確認を行う担当者（レビューを行うレビュアとテストを担当するテスタ）は、セキュリティに関する十分な知識、経験を備えた専門家として、開発者による設計や実装作業が適正であるかどうかをセキュリティ面から確認する必要がある。

【セキュリティベンダのサービスの利用が必要と判断した場合】

(3) セキュリティベンダを利用した検証と妥当性確認

- **セキュリティ検証と妥当性確認のために外部のセキュリティベンダによるサービスを利用すること。**

本来は、自組織内でセキュリティの専門家を育成し、配置することが望ましい。しかし、現実的には十分なスキルを持つ専門家を自組織内で配置することは極めて困難である。このような場合においては、必要に応じて外部のセキュリティベンダを利用することも有効な解決策となり得る。

セキュリティベンダによる検証と妥当性確認は、自組織内での作業では不足することが想定される検査項目の網羅性や最新技術への対応が期待できることから、ソフトウェアのセキュリティ要件に応じて、実施の是非を検討する必要がある。

【ツールの利用が必要と判断した場合】

(4) セキュリティツールを利用した検証と妥当性確認

- コード検査ツール等の利用により、正確かつ効率的なセキュリティの検証と妥当性確認を行うこと。

セキュリティの検証を全部手作業で実施すると、膨大な時間を要すると同時に作業ミスも発生しやすくなる。このため、検証と妥当性確認の作業は、セキュリティツール等の利用によって可能な限り自動化すべきである。

例えば、ソースコードを検査するツールの中には、危険な関数や変数の利用をスキャンし、不具合を修正する機能等を有するものがあり、高いセキュリティ品質を備えたソフトウェアの開発において不可欠となりつつある。また、最新の攻撃手法等を使用して脆弱性を検査するツールもある。

ただし、こうしたツールは技術的に発展途上の状態にあり、誤検出等のおそれも高いことから、十分に熟練した開発者の作業を支援する手段として利用する必要がある。

6.2 セキュリティに関するレビューとテスト

ソフトウェアの検証と妥当性確認を行うための方法論はレビューとテストであり、セキュリティのレビューとテストの徹底によって脆弱性は減少する。

レビューは、テストに比して軽微な工数で済むとされ、効率的な欠陥予防・除去の観点から、極めて重要なプロセスである。しかし、レビューのみではすべての欠陥を排除することは難しいため、実際にプログラムを動かして確認するテストを実施する必要がある。

なお、ソフトウェア開発における一般的な動作確認のレビューやテストが、「想定される行動が行われた際に要求された機能が確実に動作する点」に比重を置くのと対照的に、セキュリティのレビューやテストは、「想定外の行動が行われた際に問題のある動作が発生しない点」に重点を置いている。本項では、セキュリティのレビューとテストについて解説する。

(1) セキュリティに関するレビュー

- 実装を開始する前に*[定められた各工程の開発関係者]*において、セキュリティの設計

に関するドキュメント（要件定義書、基本設計書、詳細設計書等）のレビューを実施し、セキュリティ要件定義に基づく設計が行われていることを確認し、その合意した内容について記録すること。

- 実装を終了する前に*[定められた各工程の開発関係者]*において、セキュリティの実装ドキュメント（ソースコード等）に関するレビューを実施し、セキュリティ設計に基づく実装が行われていることを確認し、その合意した内容について記録すること。
- 各セキュリティドキュメント（要件定義書、基本設計書、詳細設計書、ソースコード等）間における要件の対応関係を明確化し、セキュリティ要件が正確かつ完全に具体化されていることを確認すること。

レビューとは、各工程の成果物としてのドキュメント（要件定義書、基本設計書、詳細設計書、ソースコード等）について開発関係者間の合意を得る手続であり、セキュリティ面からのレビューも実施する必要がある。レビューの手法は、インスペクション、ピアレビュー、ウォークスルー等が一般的である。

ソフトウェア開発は、下流工程に進むにつれて、要件の抜けや認識の誤り等の齟齬が発生することが多い。特に実際の開発作業のスタートラインである要件定義から基本設計までの工程でミスや抜けが生じていた場合は、多大な手戻り工数が発生してしまう可能性があることに留意し、上流工程におけるレビューは特に慎重に実施する必要がある。

【セキュリティテストが必要な場合】

(2) セキュリティに関するテスト

【ホワイトボックス形式でのセキュリティテストが必要な場合】

- セキュリティ問題を想定し、それに対する対策を実践できるセキュリティ知識を備えたテスタが、ホワイトボックス検査によるセキュリティテストを行うこと。

【ブラックボックス形式でのセキュリティテストが必要な場合】

- 使用するプログラミング言語に対する既知の攻撃手法を熟知し、それに対して新たな脆弱性を発見できるセキュリティ知識を備えたテスタがブラックボックス検査によるセキュリティテストを行うこと。

テストとは、作成したプログラムを実際に稼働させ、その処理の結果が想定したものと一致しているかどうか等を検証・確認する手続であり、単体テスト、結合テスト、統合テストといった工程において、性能、信頼性、負荷テスト等に加え、セキュリティ面からのテストも実施する必要がある。

テストの手法は、ホワイトボックス検査とブラックボックス検査に大別される。このうち、ホワイトボックス検査は、主に単体テストや結合テストで使用される手法であり、プログラムの内部構造が開示された状態で検査を行うことから、入力に対するプログラムの挙動を確実に把握することができる。一方、ブラックボックス検査は、主に統合テストで使用される

手法であり、プログラムの内部構造を確認せずに仕様やインタフェースに基づきテストを行う。これらのうち、適切な手法について検討し、実施する必要がある。

【セキュリティテストが必要な場合】

6.3 既知の攻撃

既知の攻撃を想定した脆弱性の検証は、セキュリティのレビューとテストの効果を高める重要な要素となる。なぜなら、多くの攻撃が同様の手法によって行われるからである。加えて、既知の攻撃を想定した脆弱性の検証は、レビューとテストに客観性をもたらし、作業漏れを防止する効果もある。

なお、攻撃手法は一定ではないため、常に最新の動向を把握しておくことが重要である。本項では、例示として代表的な攻撃手法の概要について解説する。

【アクセス制限の回避に関するテストを実施する場合】

(1) アクセス制限の回避

- アクセス制限の回避に関する脆弱性の検証を行うこと。

攻撃者は、識別や認証、アクセスコントロールの抜けや誤りによって生ずる権限管理の脆弱性を突いて、機密性の高い情報に許可されないアクセスを行う可能性がある。

【パスワード推測に関するテストを実施する場合】

(2) パスワード推測

- パスワード推測に関する脆弱性の検証を行うこと。

知識による認証であるパスワードは、十分な時間さえあれば理論的には解読は可能である。パスワード推測の手法としては、予測され得るパスワードを推測する辞書攻撃、トライアンドエラーを繰り返す総当たり（Brute force）攻撃などが代表的である。

攻撃者は、パスワードを自動で推測するツール等を利用することで、権限管理の脆弱性を突いて、パスワードを不正に取得する可能性がある。

【権限昇格に関するテストを実施する場合】

(3) 権限昇格

- 権限昇格に関する脆弱性の検証を行うこと。

攻撃者は、アプリケーションにアクセスを行った後、権限管理の脆弱性を突いて、一般利用者権限から管理者権限への昇格を試みる可能性がある。権限を昇格させた攻撃者はソフトウェアの完全な制御が可能となる。

【パラメータの改ざんに関するテストを実施する場合】

(4) パラメータの改ざん

- パラメータの改ざんに関する脆弱性の検証を行うこと。

攻撃者は、ソフトウェアと利用者との間で送受信されるパラメータの権限管理や情報の妥当性の検証の脆弱性を突いて、パラメータを改ざんし、ソフトウェアの誤動作を発生させる可能性がある。代表的な例として、電子商取引サイトでの価格の改ざんやパラメータを使ってファイルをオープンするプログラムにおけるパラメータ改ざんによるディレクトリトラバーサル攻撃等がある。

【セッション管理への攻撃に関するテストを実施する場合】

(5) セッション管理への攻撃

- セッション管理への攻撃に関する脆弱性の検証を行うこと。

ウェブアプリケーションでは、アプリケーションレベルでセッション管理を行っているものがある。攻撃者は、セッション情報の権限管理の脆弱性を突いて、利用者のセッション情報を取得することで、利用者と同レベルの権限でアクセスを行う可能性がある。代表的な例として、利用者とアプリケーションとのセッション情報を盗聴や推測によって強奪するセッションハイジャック等がある。

【コマンドインジェクションに関するテストを実施する場合】

(6) コマンドインジェクション

- コマンドインジェクションに関する脆弱性の検証を行うこと。

攻撃者は、入力データを利用したコマンド処理を実行しているアプリケーションにおいて、情報の妥当性の検証の脆弱性を突いて悪意あるコマンドを混入し、アプリケーションの背後にあるデータベースやシェルなどを不正に操作する可能性がある。代表的な例として、SQL インジェクション、OS コマンドインジェクション等がある。

【クロスサイトスクリプティングに関するテストを実施する場合】

(7) クロスサイトスクリプティング

- クロスサイトスクリプティングに関する脆弱性の検証を行うこと。

攻撃者は、入力データを外部に出力する処理を実行しているアプリケーションにおいて、情報の妥当性の検証の脆弱性を突いて、悪意あるスクリプトを利用者の Web ブラウザ上で実行する可能性がある。これによって正規の利用者のセッション情報を盗んだり、偽のページ

を表示させてフィッシング詐欺等に利用することがある。

【バッファオーバフローに関するテストを実施する場合】

(8) バッファオーバフロー

- バッファオーバフローに関する脆弱性の検証を行うこと。

攻撃者は、不適切なデータ長の定義によって生ずる情報の妥当性の検証の脆弱性を突いて、確保したメモリ領域を超えてデータを入力することで、データをあふれさせてプログラムを暴走させ、開発者の意図しない動作を実行させる可能性がある。この代表的な例として、スタックオーバフロー、ヒープオーバフロー等がある。

【エラー処理からの情報の取得に関するテストを実施する場合】

(9) エラー処理からの情報の取得

- エラー処理からの情報の取得に関する脆弱性の検証を行うこと。

権限管理や情報の妥当性の検証の処理において、許可されないデータについては可能な限り入力を拒否し、エラー処理を返す必要があるが、その際、ソフトウェアの内部処理が露呈する可能性がある情報をエラーメッセージとして通知すると、攻撃者は、当該エラーメッセージを利用して、機密情報を取得したり、攻撃に関する有用な手掛かりを得る可能性がある。

≪参考文献≫

・ IPA：「脆弱性関連情報に関する届け出状況」
（http://www.ipa.go.jp/security/vuln/report/press.html）
ソフトウェアの脆弱性関連情報に関する最新の届け出状況をまとめたもの。

【セキュリティテストが必要な場合】

6.4 セキュリティテストの計画と管理

問題のある副作用や誤動作が発生しないことを網羅的に検証するためにセキュリティに関するテストでは、適正なテスト計画の準備が極めて重要となる。

また、テストにおいて発見された脆弱性は、速やかに改善されなければならないが、その過程で従来存在していたセキュリティ機能が弱められたり、新たな脆弱性を発生させる可能性があるため、改善の実施状況を適切に管理する必要がある。

(1) セキュリティのテスト項目

- セキュリティテストに当たって、既知の脆弱性やコーディング規約をベースとしたテスト項目を作成し、テストを実施すること。

網羅的かつ効率的なテストのためにはテストのスケジュールや体制、テスト項目や検証手法等に関するテスト計画の作成が重要である。テスト計画には、ソフトウェアのセキュリティ要件に応じて、必要なセキュリティのテスト項目を記載しなければならない。

セキュリティのテスト項目は、ソフトウェアの設計や実装に応じて、既知の攻撃手法やコーディング規約などをベースに作成しなければならない。

≪参考文献≫

- IPA：「消費者向け電子商取引サイトにおける注意点」
  （http://www.ipa.go.jp/security/vuln/20050304_ec_security.html）
  電子商取引サイトにおいて発生しうるけるセキュリティ上の問題点とそれらの対策方法をまとめたもの。
- IPA：「セキュアな Web サーバーの構築と運用」
  （http://www.ipa.go.jp/security/awareness/administrator/secure-web/）
  Web サーバを構築、運用するにあたってのセキュリティ対策の手引き
- Microsoft：「Web アプリケーション セキュリティ強化」
  （http://www.microsoft.com/japan/msdn/security/guidance/secmod71.mspx）
  セキュリティ保護された ASP.NET Web アプリケーションを構築する際のガイドラインを示したもの。

(2) セキュリティテストの管理

- セキュリティテストにおける項目、実施結果、実施時に判明した不具合及び当該不具合の修正内容等を記載した記録を作成し、管理すること。
- セキュリティテストの終了後に、テスタはテスト報告書を作成し、責任者はテスト報告書の内容を検証した上で承認すること。
- セキュリティテストの終了後に脆弱性の修正を行う場合、原因や修正内容などを検討し、関係者に連絡すること。連絡を受けた責任者は、この内容を検証し、妥当と認めた場合にこれを承認すること。
- 責任者の承認を得た後に修正を行うこと。また、責任者は修正された結果について、再度検証を行うこと。
- テストドキュメント（報告書やテスト用ソフトウェア等）について適切に保護し、保存期間終了後は直ちに廃棄すること。
- セキュリティテストの終了後に、仕様の変更、又は脆弱性の修正をした場合、コードレビューや回帰テスト（リグレッションテスト）を実施すること。

重大な脆弱性を見逃すことがないように、また運用業務において発生するトラブルの原因究明及び保守業務作業に備えるため、テストの実施状況を管理しなければならない。

具体的には、試験項目、実施結果、不具合、修正結果等を記載したセキュリティテストの記録を作成する。作成するテストの記録は、その実施数、正常終了数、修正数などをまとめ、作業の進捗状況を確認する必要がある。

また、セキュリティテストの結果、要件定義書、設計、プログラム等に欠陥が発見された場合は修正を行う必要がある。上流工程において修正が行われた場合は、脆弱性が正しく修正されていること及び修正による副作用（新たなバグの発生）が発生していないことを確認するため、コードの再レビューや回帰テスト（リグレッションテスト）を実施する必要がある。

7. 運用環境への移行におけるセキュリティ

【趣旨】
検証と妥当性確認の結果が良好であれば、ソフトウェアを開発環境から運用環境に切り替えることが可能となる。
本項では、検証と妥当性確認を終了した新規開発ソフトウェアを実運用環境に移行する作業に関するセキュリティ面からの留意事項を解説する。

7.1 運用ガイダンスにおけるセキュリティの考慮

運用環境とは、実際の業務が行われている環境であり、移行作業におけるセキュリティ上のリスクは可能な限り極小化される必要がある。このため、開発されたソフトウェアの適切な運用を行うためのガイダンスの準備が必要である。

【運用ガイダンスの作成が必要な場合】

(1) 運用ガイダンスにおけるセキュリティの考慮

- 運用ガイダンスにおいて、セキュリティ機能の特質、設計及び実装を含めたソフトウェアの構成及び機能運用について明確に記述すること。
- 運用ガイダンスにおいて、管理者及び利用者がセキュリティ面で正しい運用を行うことを支援するための操作手順について明確に記述すること。
- 運用ガイダンスにおいて、セキュリティ上の留意事項を含む保守運用体制、インストール及びアンインストール方法について明確に記述すること。
- 運用ガイダンスにおいて、脅威に基づいたセキュリティインシデント定義、インシデント発生時の連絡先及び一次対応手順、予兆検知のためのログの収集・解析方法等を含めた事故・障害の対応手順について明確に記述すること。
- 運用ガイダンスにおいて、セキュリティに関する一般的問い合わせとそれに対する回答（FAQ）について明確に記述すること。

運用ガイダンスとは、ソフトウェアの確実かつ効率的な運用を支援するため、ソフトウェアの機能・設計、操作方法、導入・保守の手順、事故・トラブル対応を説明したドキュメントである。ガイダンスには、セキュリティ面からの考慮事項を併せて記載しておく必要がある。

運用ガイダンスは、管理者向けと一般利用者向けに分けて作成されるのが一般的であり、運用環境への移行前に完成しておくことが望ましい。

7.2 導入におけるセキュリティの考慮

移行作業は切替えの方法によっては、旧システムの情報の変換や利用者側の業務停止等を伴うことがあり、業務継続の観点を重視して慎重な作業を行わなければならない。ただし、業務継続や効率性を優先するあまり、ソフトウェアの導入・移行においてセキュリティが見落とされ、脆弱性が混入されないようにしなければならない。

【導入手順の作成が必要な場合】

(1) 導入手順におけるセキュリティの考慮

- 運搬によって、ソフトウェアの配付を行う場合、安全な配送方法や開梱検出シール等で改ざんの危険性を低減すること。
- 通信によって、ソフトウェアの配付を行う場合、コード署名・ハッシュ関数等で改ざんの危険性を低減すること。
- 本番環境にコンパイルする際、デバッグモードの利用を禁止すること。
- 導入に当たって、開発時に使用した不要な識別子、認証情報、ソースコード、ユーティリティ、テストデータ、サンプルプログラム等を運用環境から除去すること。
- 本番環境への導入前に、アンチウイルスソフトウェア等によって、不正なプログラムが残留していないかを確認すること。
- 本番環境で稼働させる前にセキュリティ機能の設定を完了すること。

開発したソフトウェアを指定された運用環境に配付・移送する際は、ポリシー及び実施規程に則り、適切な安全管理措置を行う必要がある。

また、導入されるソフトウェアには、テスト効率などの観点から開発者が作り込んだバックドアやデバッグコード、不要なテスト用ツール等が残留している状態であったり、セキュリティ機能が未設定である可能性がある。

このため、導入の事前段階でこうした点について検証した上で、安全な導入作業を行わなければならない。

【移行計画・移行手順の作成が必要な場合】

(2) 移行計画・移行手順におけるセキュリティ

- 開発者の本番環境へのアクセス及び変更作業について、正式な申請・承認・記録の手順を作成すること。
- 本番環境におけるコンパイラ、エディタ等の利用について、正式な申請・承認・記録の手順を作成すること。
- 移行前に既存システムのソースプログラムやマスターファイルなどを記録媒体に記録し、一定期間保存すること。
- 運用に使用しない開発用のデータ、ドキュメント、ソフトウェア（試作品や不良品を含む。）類は、開発終了後、廃棄すること。ただし、以降の保守・運用・復旧作業に必要になる資産については、管理責任を明確化し、適切に保護すること。

移行時には、確実かつ効率的な移行を行うことを目的として、移行対象とする資産、移行に要する期間、要員計画等を明確化した移行計画、及び移行方法、作業手順、利用者教育等を明確化した移行手順を策定する。この際、セキュリティ面からの管理を十分に考慮しておく必要がある。

具体的には、移行作業は多くの担当者が関与する状況であり、作業の管理が困難であることから、作業についての正式な申請、承認、記録の手順を作成させたり、障害等の予期しないトラブルを想定して、移行前の環境を適切に保存させる等の対策が必要となる。

また、移行を終了し、確認期間を終了した時点で、運用に使用しない開発用の情報、関連する情報資産、及び開発に要する資産は適切に廃棄しなければならない。

A3113 外部委託における情報セキュリティ対策に関する評価手順

1. 目的

本書は、大学が情報処理業務を外部委託により行う場合に、委託先の情報セキュリティの確保を目的として各種評価手法を大学において利用するための手引書である。

大学において情報処理業務を外部委託により行う場合には、大学が求める情報セキュリティ水準が委託先において確保される必要がある。このため、大学では、情報セキュリティ関係規程の一つとして外部委託についても手順を定めることが想定されている。この手順に従い大学としての業務を行うに当たり、情報セキュリティマネジメントシステムに関する適合性評価制度、情報セキュリティ対策ベンチマーク及び情報セキュリティ監査の各評価手法を活用することができる。

本書は、大学で情報処理業務の外部委託に責任を持つ部局技術責任者及び調達担当者に対してこれらの制度を適切に利用するための情報を提供し、もって情報処理業務の外部委託における情報セキュリティの確保に資することを目的とする。

2. 情報セキュリティ確保の枠組み

情報処理業務を外部委託により行う場合には、以下の枠組みにより情報セキュリティの確保を図ることとなる。

(1) 外部委託の可否の判断

対象情報処理業務について、これに係る情報システム及び情報に照らして、情報セキュリティ確保の観点から、これを外部委託により行うことの可否を判断すること。

(2) 委託先の選定

調達において、委託先候補の事業の安定性と情報セキュリティ対策の遂行能力を検討の上、委託先を選定すること。

(3) 実施する情報セキュリティ対策に関する合意

当該外部委託に係る情報処理業務において委託先が実施すべき情報セキュリティ対策に関して、大学及び委託先が合意し、契約に含めること。

(4) 情報セキュリティ対策の実施

委託先が、当該業務の遂行において、合意した情報セキュリティ対策を実施すること。

(5) 情報セキュリティ対策の履行状況の確認

委託先における情報セキュリティ対策の履行状況について、大学による確認がなされること。

(6) 是正措置

委託先における情報セキュリティ対策の履行状況の確認の結果、必要であればこれが是正されること。

3. 各種制度と利用場面

外部委託において利用できる評価手法として、主に以下の3つの制度がある。

・情報セキュリティマネジメントシステムに関する適合性評価制度

・情報セキュリティ対策ベンチマーク

・情報セキュリティ監査

「(2) 委託先の選定」においては、委託先候補が情報セキュリティマネジメントシステムに関する適合性評価制度に基づく認証を取得していること、又は情報セキュリティ対策ベンチマークの結果が求める成熟度に達していることを、選定における評価の要素に含めることができる。また、将来的には、情報セキュリティ監査の結果を選定における評価の要素に含めることも想定される。

「(5) 履行状況の確認」においては、業務における定常的な確認に加えて、委託先における当該情報処理業務を対象にした情報セキュリティ監査が活用できる。

これらの制度はそれぞれの特徴に応じて適切な場面で有効に活用することが重要であることから、本書添付の各資料において利用方法を説明している。

なお、情報セキュリティマネジメントシステムに関する適合性評価制度については、我が国において財団法人日本情報処理開発協会(JIPDEC)が運営している「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」を基に説明することとする。

4. 参考文献

ISMS 適合性評価制度、情報セキュリティ対策ベンチマーク及び情報セキュリティ監査の各制度については、専門的な知見に基づく説明書の必要性が高いことから、制度を運用しているそれぞれの組織が作成した資料を内閣官房が取りまとめた以下の資料を参照されたい。内容については経済産業省、特定非営利活動法人日本セキュリティ監査協会 (JASA)、財団法人日本情報処理開発協会及び内閣官房情報セキュリティセンターがタスクフォースを構成して共同で検討し、その成果を各資料に反映している。

（所在 URL　http://www.nisc.go.jp/active/general/pdf/dm6-06-061_manual.pdf）

資料 1

「外部委託における ISMS 適合性評価制度の利用方法」

財団法人 日本情報処理開発協会、2006 年 5 月

資料 2

「外部委託における情報セキュリティ対策ベンチマークの利用方法」

経済産業省、2006 年 5 月

資料 3

「外部委託における情報セキュリティ監査の利用方法」

特定非営利活動法人 日本セキュリティ監査協会、2006 年 5 月

利用の際の参考として、各資料を大学に適用する際に行うべき用語の置換例について下表に示す。

表　用語対応表

内閣官房情報セキュリティセンター（NISC）発行文書における用語	本サンプル規程集における用語置換例
府省庁	大学
情報システムセキュリティ責任者	部局技術責任者
省庁基準	ポリシー、実施規程
実施手順	手順
○○省	○○大学または○○学部

A3114 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書

情報システムの構築またはソフトウェアの開発を行う際には、その情報システム等が満たすべき情報セキュリティ上の条件を「セキュリティ要件」としてまとめ、構築を請け負う者にその実現を求める必要がある。また、セキュリティ要件を実現させる手段が具体的な機能として定まっている場合は、これを「セキュリティ機能」として情報システム等に関する仕様書に反映させることもある。情報システム等が備えるべきセキュリティ要件やセキュリティ機能は、その情報システム等で扱う情報の性質やシステムを取り巻く環境などによって異なるため、情報システム等の発注者において個々に検討する必要がある。しかしながら、情報システム等に対する脅威とこれを防ぐための対策はたえず変化している上に、確保すべき情報セキュリティの水準と必要となる費用とのバランスなどは情報セキュリティの専門家でなければ適切に判断できないことも多い。このとき、学内に専門家がいない場合は外部委託先の提案に委ねることにもなりがちであるが、情報セキュリティの確立の上では大学等が主体的にセキュリティ要件を定めることが重要であることは言うまでもない。

内閣官房情報セキュリティセンター（NISC）では政府機関におけるこうしたセキュリティ要件の検討の便宜を図るため、本文書と同名称の文書を以下の URL で公開している。

DM6-07 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書

http://www.nisc.go.jp/active/general/pdf/dm6-07-061_manual.pdf

この文書は独立行政法人情報処理推進機構に設置された「政府機関における機器等の購入ガイドラインに関する研究会」がとりまとめた「政府機関調達者向けのセキュリティ要件作成マニュアル」（2006 年 3 月）に NISC が政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））に関係する内容を加筆の上公開したものである。政府機関向けであるが、大学等高等教育機関が情報システムの構築等を外部委託する場合においても有用な内容であるので、セキュリティ要件やセキュリティ機能を検討する際の参考とすることが望ましい。

A3115 情報システムの構築等における ST 評価・ST 確認の実施に関する解説書

内閣官房情報セキュリティセンター（NISC）が公開している「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））」（政府機関統一基準）は、重要なセキュリティ要件が含まれる情報システムを構築する場合に、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価・ST 確認を受けることを求めている（本サンプル規程集における「A2501 事務情報セキュリティ対策基準」の 4.3.1(1)(d)、6.1.3(3)(e)の記述に対応）。NISC では、政府機関におけるこうした ST 評価・ST 確認の実施の便宜を図るため、本文書と同名称の文書を以下の URL で公開している。

DM6-08 情報システムの構築等における ST 評価・ST 確認の実施に関する解説書
http://www.nisc.go.jp/active/general/pdf/dm6-08-061_manual.pdf

この文書は独立行政法人情報処理推進機構に設置された「政府機関における機器等の購入ガイドラインに関する研究会」がとりまとめた「政府機関調達者向けのセキュリティ要件作成マニュアル」（2006 年 3 月）に NISC が政府機関統一基準に関係する内容を加筆の上公開したものである。政府機関向けであるが、大学等高等教育機関においても有用な内容であるので、ST 評価・ST 確認の実施の際の参考とすることが望ましい。

A3200 情報システム利用者向け文書の策定に関する解説書

この文書は、以下の文書の利用に際しての注意点について述べたものである。

A3201　PC 取扱ガイドライン
A3202　電子メール利用ガイドライン
A3203　ウェブブラウザ利用ガイドライン
A3204　ウェブ公開ガイドライン
A3205　利用者パスワードガイドライン
A3211　学外情報セキュリティ水準低下防止手順
A3212　自己点検の考え方と実務への準備に関する解説書

文書 A3201－A3204 は、「A2201 情報システム利用規程」の解説でも触れたが、内規や手順としてではなく、ガイドラインとして提示されている。これらのガイドラインには、昨今の教育環境の変化により、やむなく主観が入り込む余地のある道徳的条項が盛り込まれている。その結果として、これらの文書は手順や内規ではなくガイドラインとした。

ガイドラインではなく手順や内規として本ひな形を参考にする場合には、何が違反となるかを明確になるように文書を作成するとともに、「A2201 情報システム利用規程」を修正しなければならない。

「A3211 学外情報セキュリティ水準低下防止手順」は、本学のシステムの利用が学外システムの可用性の低下や学外システムのセキュリティ水準に影響を与えないためにどうすべきかを示した文書である。学外への情報提供等に関して提供先のセキュリティ低下をきたさないために守るべき事項を定めている。

「A3212 自己点検の考え方と実務への準備に関する解説書」は、自己点検の適切な実施のため、関係する遵守事項を解説した文書である。あわせて、年度計画や実施手順書の雛形を示している。

A3201 情報機器取扱ガイドライン

解説：A2201（情報システム利用規程）で指定した情報機器の利用手順に関して述べている。ここでいう情報機器とは、利用者が相対して操作する端末等を想定している。サーバ機能やルータ機能を持つコンピュータは対象としていない。ただし、大学外からこれら情報機器へのリモートアクセスを可能にするためのサーバ機能は例外である。利用手順に倫理条項を含んでいるが、一般端末の利用手順の雛形としての利用を想定したためである。

1. 一般利用者向け利用手順

解説：ここでいう一般利用者は、計算機の特権利用者（Windows®であればAdministrator、UNIX®であればrootなど）以外の利用者を指し、特権利用があらかじめ用意したアカウントを利用する利用者である。一般利用者は計算機の設定（個人環境に関するものを除く）変更や、アプリケーションのインストールはできないものとしている。大学の場合は、演習室や図書館等に設置されている共用端末を利用する一般学生等が対象となる。もちろん、特権利用者も本項目に書かれている事項は遵守する必要がある。

1.1 利用者は以下に掲げる行為をはじめとする、端末等の設備を物理的に損傷する可能性のある行為をしてはならない。

(a) **演習室等における飲食。ただし、管理者が別途許可する場合を除く。**
(b) **コネクタ等を引き抜いたり、キーボードやマウス等周辺機器を取り外す行為**
(c) **フロッピーディスクドライブ等、開口部に異物を詰める行為**
(d) **キーボードの乱打、USB メモリ等の乱暴な抜き差しをする行為**

解説：主として大学内の共用スペースに設置する共同利用端末に関して、端末設備を物理的に破損する行為等を禁止する。飲食等についてはカフェテリア等に設置する場合もあり、状況に応じて規定を設ける。これら端末を損傷する行為に対する対策は、規定等による対策の他に、管理者による適切な監視体制の整備等も重要である。それら対策が困難である場合には、シンクライアント端末の導入や、タッチパッド等の採用も考慮すべきである。

1.2 利用者は以下に掲げる行為をはじめとする、他の利用者の利用を妨げる行為をしてはならない。

(a) **共用端末の占有行為。端末をロックして長時間離席する行為も含む。ただし、講義等で特に許可された場合を除く。**
(b) **演習室で大声で騒ぐ行為や、ごみを放置する行為。**
(c) **プリンタの紙詰まりや紙切れ、トナー切れを放置する行為。**

解説：ここに掲げられている事項の他に、ディスク記憶領域や、計算能力、メモリ等の占有行為の禁止が必要になる場合があるかもしれない。しかし、これらの計算機資源の占有が危惧される場合には、クォータ等、システム側で対応を考えた方がよい。
また、ライセンス上、同時起動数が制限されているようなアプリケーションを導入している場合は、同様の規定が必要であろう。
さらに、前項と同様、管理者による監視体制の整備や、プリンタのトラブル等に迅速に対応できる体制作りも重要である。

1.3 **利用者は以下に掲げる行為をはじめとするネットワーク帯域を占有する行為をしてはならない。**

(a) **大きなサイズのファイルの転送**
(b) **大きなサイズのメール送信**
(c) **高い頻度で問い合わせパケット等を送出するアプリケーションの使用**

解説：基本的には、1.2 項の規定に含まれるとも考えられるが、場合によっては、広範囲に影響が及ぶため独立した項目としている。「大きなサイズ」等の具体値をネットワーク性能等に応じて示す方がよい。

1.4 **利用者がアプリケーションをインストール、使用する場合には、以下の各号を遵守しなければならない。**

(a) **教育・研究目的、およびそれらを支援する目的に合致しないアプリケーションをインストール、使用してはならない。**
(b) **インストール、使用しようとするアプリケーションの利用条件に従って利用すること。**
(c). **アプリケーションをインストールする前に、ウイルスチェックソフトウェア等により、ウイルスやスパイウェア等、有害ソフトウェアが含まれていないことを確認すること。**
(d) **出所の定かでないソフトウェアをインストール、使用しないこと。**

解説：アプリケーションのインストールに関しては、管理者が行うべきものであり、利用者が共通領域にインストールできるようなシステム構築はセキュリティ上、

極力避けるべきである。しかし、その場合でも、利用者権限で利用者用領域にインストール可能なソフトウェアも存在するので、本項目を設けている。
なお、利用者用ディスク容量の制約が厳しい場合等は、利用者がインストールしてほしいアプリケーションを管理者に申請できるような仕組みを設けることも考えられる。

1.5 **利用者は、情報格付け規定において規定されている要管理情報や、その他重要なデータの取り扱いに関して以下の各号を遵守しなければならない。**

(a) **要管理情報を PC 内部、あるいは外部記憶メディアに保管する場合は、暗号化するものとし、その暗号化鍵を適切に管理すること。**
ただし、暗号化以外に十分な保護対策が採られていると管理者が認める場合はこの限りでない。
(b) **要管理情報を電子メール等を用いて送信する場合は暗号化するものとし、その暗号化鍵は別途安全な手段を用いて送信すること。**

解説：個人情報等、重要な情報の保管、送信時の暗号化の必要性について述べている。
(a)の但し書きは、バックアップ用メディア等で、暗号化すると著しく利便性が損なわれるような場合に、メディアを厳重に管理することで暗号化に代えられるとしたもの。

1.6 **利用者は、CD-ROM やフロッピーディスク、USB メモリ等の外部記憶メディアを利用する場合には、以下の各号を遵守しなければならない。**

(a) **利用者のファイルを保存した外部記憶メディアを放置しないこと。**
(b) **放置してある、または出所が定かでない外部記憶メディアを端末に挿入しアクセスしてはならない。そのような媒体を発見した場合は、管理者に届け出ること。**
(c) **使用済みの外部記憶メディアを譲渡、または廃棄する場合には、記録されていたデータが復元されることのないように、専用ツールを用いて消去するか、メディアを物理的に破壊すること。**

解説：CD-ROM の内容を自動実行する設定にしている場合には、メディアを挿入するだけでソフトウェアが実行され、悪意のあるソフトウェアがインストールされる可能性に留意すること。
メディアを廃棄、譲渡する場合は、OS 上でファイルを消去しただけでは、記録情報が復元される可能性に注意すること。なお、データ破壊に関しては、「要管理情報等の重要な情報」を記録した外部記憶メディアに対象を限定するとい

う考え方もある。

1.7 **利用者は、演習室等、共用スペースに設置してある PC 端末を利用する場合は、以下の各号を遵守しなければならない。**

(a) **端末を操作中に一時的に離席する場合は、端末をロックすること。**
(b) **演習室等の扉や窓を開放しないこと。また、空調機の設定温度を変更しないこと。ただし、管理者が別途指示する場合はこの限りでない。**
(c) **使用後の端末等の電源を切ること。ただし、管理者が別途指示する場合はこの限りでない。**
(d) **プリンターで無駄な印刷をしないこと。**

解説：(b)は、PC 端末の正常動作（温度、ほこり等）の保証と、PC 端末の盗難防止を目的とするものなので、これらの懸念がない場合は必要ない。
(c)についても、利用者に電源を切らせずに、管理者が電源を切る運用をしている場合は必要ない。
(d)に関しては、システム上で利用者毎に印刷枚数を制限する方法も考えられる。

1.8 **利用者は、以下に掲げる各事項を発見したときは、すみやかに管理者に連絡をするとともに、「情報システムインシデント対応手順」に従って行動すること。**

(a) **端末の OS やアプリケーション、あるいは、大学内に設置されているホストコンピュータやネットワーク機器等について、セキュリティ上の脆弱性など不具合を見つけた場合。**
(b) **大学内のホスト上に、著作権を侵害しているおそれのあるコンテンツや、機密情報、個人情報等が公開されていることを見い出した場合。**
(c) **大学外のホストで、大学の機密情報や、構成員の個人情報等が公開されている、または、大学が権利を有するコンテンツが無断で使用されていることを見い出した場合。**

解説：ネットワークや PC 端末の管理業務をしていない一般利用者であっても本項目に掲げるような脆弱性等を発見した場合に報告させることで、構成員のセキュリティや知的財産に関する意識を向上させるとともに、管理業務の効率化をはかることができる。もちろん、管理側では、これら報告に対処する体制作りが必要である。

1.9 **利用者は、大学外のネットワークから大学内の情報システム（不特定多数に公開されているもの（Web サービスなど）を除く）にアクセスする場合は以下の各号を遵守しなければならない。**

(a) **アクセスの際に必要となる認証情報（パスワードや秘密鍵）が漏洩しないように細心の注意を払うこと。万一、認証情報が漏洩した場合、またはその可能性がある場合は、迅速に管理者に報告し、その指示を仰ぐこと。**
(b) **信頼性が保障できない端末（ネットカフェの端末等）からのアクセスは禁止する。**

解説：本項は、利用者が、大学内の PC 端末やゲートウェイサーバ等にリモートアクセス可能な場合に必要な規定である。リモートアクセスのための認証情報が漏洩した場合には、単にメールを読むためのパスワード等が漏洩した場合に比較して、より深刻な被害をもたらす可能性が高いことを利用者が十分に理解していることが大切である。

2. 特権利用者向け利用手順

解説：特権利用者は、PC 端末を管理する権限を持つ特権利用者（Windows®であれば Administrator、UNIX®であれば root）を指している。具体的には、演習室や図書館等に設置されている PC 端末を管理するセンター職員や、個人で PC 端末を管理する教員や事務職員、研究室に導入されている PC 端末を管理する大学院生等が含まれる。学生等の私物 PC を学内ネットワークに接続することを許可している場合は、その私物 PC の所有者も含まれる。

2.1 特権利用者は、自らが管理する端末が、ウイルス、ワーム等に感染しないように、以下に掲げる規定を遵守しなければならない。

(a) **利用している OS、アプリケーションの脆弱性情報をはじめとする情報に留意し、ソフトウェアの不具合を迅速に修正すること。**
(b) **ウイルス対策ソフトウェアをインストールするとともに、ウイルス情報データベースを常に最新に保っておくこと。**

解説：主として利用される OS、アプリケーションに関しては、具体的なチェック方法、修正方法を示しておくことが望ましい。
また、ウイルス対策ソフトウェアをサイトライセンスにより導入している場合、学内からのみデータベースの更新が可能な場合がある。この場合、休暇中等に自宅で感染してしまう可能性があるので注意が必要。場合によっては検疫ネットワークの導入等も検討する。

2.2 特権利用者は、自らが管理する端末に、アプリケーションをインストールし、利用する際に

は、1.4 項に掲げる規定の他、以下に掲げる規定を遵守しなければならない。ただし、研究・教育目的およびそれらを支援する目的であって、対象となるネットワークの管理者が許可する場合にはこの限りでない。

(a) **ネットワーク帯域を極度に圧迫するアプリケーションをインストール、利用してはならない。**
(b) **自端末宛以外のパケットを傍受するアプリケーション（パケットスニファ）をインストール、利用してはならない。**
(c) **P2P ファイル交換ソフトウェアをインストール、利用してはならない。**
(d) **その他、情報システム利用規程、その他の本学ネットワークの利用に係わる規定等に反するネットワークアプリケーションをインストール、利用してはならない。**

解説：1.4 項の規定の他に、主にネットワークに関連するアプリケーションのインストールについて規定している。(a)ではネットワーク資源の浪費、(b)では通信の秘密、(c)では著作権侵害等に関して問題が生じそうなアプリケーションを原則禁止している。大学の実態に応じて、これらの問題に関する教育を十分に行った上で、届出制等の形で利用を認めることも考えられる。
なお、情報システム利用規程には、ファイルのダウンロード（第十五条一号）、ソフトウェアを取り込む場合（第十七条五号）のように、関連する規定があるので参照のこと。

2.3.**特権利用者は、自らが管理する端末に関して、以下の各規定を遵守すること。**

(a) **利用者が当該端末を認証なしで利用できるようにしてはならない。**
端末が認証機能を有さない場合には、あらかじめ許可された者のみが利用できるように別途手段を講じること。
アカウントの発行状況や利用状況（利用者識別の設定できないシステムにあっては、利用状況が把握できるもの）について部局責任者に定期的に報告すること。
(b) **ネットワークを経由して、不特定多数の第三者が端末にアクセスできないようにすること。**
(c) **当該端末にアカウントを有さない者に端末を使用させないこと。**
ただし、教育・研究上必要な場合など、管理者が特に認める場合を除く。
(d) **デスクトップ型端末においては、アカウントを有さない者が端末に物理的にアクセスできないように設置場所に施錠等の措置をとるとともに、必要に応じて、端末機器にワイヤーロック等の盗難防止措置をとること。**
(e) **移動可能な端末においては、短時間であっても端末を放置しないこと。**
保管時は施錠可能な場所に保管すること。

(f) **管理権限をもたない者によって CD、DVD 等、外部記憶メディアから起動されないように BIOS を設定し、BIOS パスワードを設定すること。**

(g) **端末を廃棄、あるいは譲渡する場合は、内部ハードディスクや不揮発性メモリに、要管理情報やその他重要な情報が残留することのないように、専用ツールを用いて完全に消去するか、物理的に破壊すること。**

解説：PC 端末への許可されていない者のアクセスや端末機器自体の盗難等を防止するための規定である。(f)は、管理者権限を有さない利用者が管理者権限を得る危険性を排除するためである。(g)は、1.6 項(c)と同様に、PC 端末から重要情報や認証情報が漏洩する危険性を排除するためである。リースおよびレンタルの機器に関してはデータの完全削除をソフトウェア的に実施すること。なお、データ破壊に関しては、「要管理情報等の重要な情報」を記録した端末に対象を限定するという考え方もある。

2.4 **特権利用者は、自らが管理する端末に関して、利用者が大学外のネットワークから当該端末にアクセスできるようにする場合は、以下の各規定を遵守すること。**

(a) **アクセスに使用するポート番号、VPN ソフトウェア名等をセンターに届け出ること。**

(b) **通信内容は全て暗号化されるようにすること。**

(c) **パスワードのみ（ワンタイムパスワードを除く）による認証方式は原則として避けること。パスワードによる認証を用いる場合は、パスワードの選定に関して利用者に十分な教育を行うこと。**

(d) **特権アカウント（root など）によるリモートアクセスは原則として行えないように設定すること。**

(e) **大学が提供するネットワーク以外（電話回線など）の方法でアクセスできるようにしてはならない。教育・研究目的等で、特に必要な場合には、センターの許可を得ること。**

解説：1.9 項の規定に加えて、特権利用者が、VPN サーバソフトウェア等をインストール、運用する場合の注意点を述べている。
(c)は、通信が暗号化されていても、認証パスワードが脆弱であれば不正侵入を許してしまう可能性を考慮したもの。また、リモートアクセスのパスワードとメール受信（POP/IMAP）のパスワードが共通になっている場合、メール受信は SSL/TLS を必須とする等の対策が必要である。

2.5 **特権利用者は、自らが管理する端末に関して、情報セキュリティ監査実施手順書に従って情報セキュリティ監査を実施すること。**

A3202 電子メール利用ガイドライン

1. 本書の目的

電子メールは日々の学習・教育・研究活動において必要不可欠なものになっている。そのため、電子メールは、ルールやマナーを守った安全な方法で使用しなければ、多くの利用者に迷惑をかけることになる。その上、誤った方法による使用は学習・教育・研究活動の停止や社会的信用を失わせる要因となる可能性もある。

本書は、このようなリスクを軽減し、情報資産を保護し、電子メールを安全に利用するための手順を提供する。

2. 本書の対象者

本書は、A大学が整備・提供する電子メールを利用するすべての利用者を対象とする。

3. 電子メールソフトの設定

3.1 電子メール受信に係る設定

(1)利用者は、受信した電子メールをテキスト（リッチテキストを含む。）として表示することとし、偽のホームページへの誘導や不正なスクリプトの実行を未然に防ぐ目的からHTMLメールの利用は原則として認めない。

［操作手順］　各大学の電子メール利用環境に則した説明を記述する。
なお、HTMLメールの利用を許可する場合には、注意事項、許可に要する手続等についても記述する。

(2)利用者は、アンチウイルスソフトウェアに加えて、電子メールソフトウェア側においてもウイルス対策が設定可能であれば、これを実施すること。

［操作手順］　各大学の電子メール利用環境に則した説明を記述する。

【参考：プレビュー機能を停止することを求める場合】

(3)利用者は、HTMLメールのプレビュー機能を停止すること。

［操作手順］　各大学の電子メール利用環境に則した説明を記述する。

3.2 電子メール送信に係る設定

(1) 利用者は、原則として、HTML形式の電子メールを送信しないこと。これは、当方よりHTML形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

［操作手順］　各大学の電子メール利用環境に則した説明を記述する。

4. 電子メールに係る全般的な注意事項

4.1 電子メールの私的利用の禁止

(1) 利用者は、電子メールシステムを、学習・教育・研究活動を遂行する上で必要な場合のみ使用することとし、私的目的のために使用しないこと。

4.2 電子メールの自動転送の禁止

(1) 利用者は、原則として要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送することを禁止する。

(2) 利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要がある場合には、メール転送先・理由・期間・セキュリティ対策などを明確にした上で事前に電子メールシステムの部局技術担当者及び上司の了解を得ること。

(3) 利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要性がなくなった場合には、その旨を電子メールシステムの部局技術担当者及び上司に報告すること。

4.3 大学が整備した電子メールシステム以外の情報システム利用の禁止

(1) 利用者は、学習・教育・研究活動遂行にかかわる情報を含む電子メールを送受信する場合には、大学が整備した電子メールシステムを利用することを原則とする。

(2) 利用しようとする電子メールシステムの利用規程等で、明示的に許可されている場合を除き、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、電子メールシステムの部局技術担当者及び上司の許可を得ること。

(3) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、セキュリティ対策ソフトを導入するなど安全管理措置を講ずること。

(4) 利用者は、大学が整備した電子メールシステム以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要性がなくなった場合には、その旨を電子メールシステムの部局技術担当者及び上司に報告すること。

解説：利用者は、利用しようとするシステムの利用規程等で外部への転送や大学が整備した以外の情報システム（個人所有の PC 等）でのメールの送受信が許可されている場合、部局責任者や上司の許可を必要としない。学生の連絡先が携帯メールで、情報システムの運用で、携帯メールのアドレスや ISP のメールアドレスの登録が許可されている場合も同様である。システムの利用規程で IMAP、POP やウェブメールおよび VPN を介してモバイル PC 等による電子メールシステムへのアクセスを許可している場合も個別の許可を要しない。セキュリティ担当者の緊急連絡先として携帯電話等の外部の情報システムを登録することは広く行われていることであるが、送付する内容や外部情報システムのトラブル、設定ミス等での情報漏洩のリスクを考えると情報セキュリティ責任者が転送内容等について把握しておく必要がある。
研究室等の単位でアウトソースした場合のシステムは「大学が整備したシステム」とみなす。

4.4 電子メールの監視

(1) **電子メールシステムの適正な利用のため、その利用状況（あて先、内容、添付ファイル等）について証跡の取得、保存、点検及び分析が行われる可能性がある。利用者は、その趣旨を理解の上、電子メールの内容に関するモニタリング及び監査を実施していることを認識すること。**

4.5 電子メールID及び電子メールアドレスの管理

(1) **利用者は、他人の電子メールID（電子メールサーバへのログインID。以下同じ。）及び電子メールアドレスを使用しないこと。**

(2) **利用者は、電子メールID及び電子メールアドレスを他人と共用しないこと。**

(3) **利用者は、自己に付与された電子メールIDを、それを知る必要のない者に知られるような状態で放置しないこと。**

(4) **利用者は、電子メールを利用する必要がなくなった場合は、電子メールシステムの部局技術担当者へ届け出ること。**

(5) **特定のサービス、職位、部門単位に付与される電子メールID及び電子メールアドレスのように、電子メールID及び電子メールアドレスを複数の関係者で共用する、あるいは担当者が引き継いで使用する必要がある場合には、利用者はその許可及び設定について電子メールシステムの部局技術担当者に相談すること。**

4.6 ニュースグループ、メーリングリスト等の発信機関への電子メールID登録の制限

(1) 利用者は、ニュースグループ、メーリングリスト等(メールマガジン、Webマガジン、フリーメール)への電子メールID登録は、情報セキュリティ情報のメール配信サービスなど、学習・教育・研究活動上必要なものに限定すること。

5. パスワードの管理

5.1 クライアントPCのログイン管理・電源管理

(1) 利用者は、クライアントPCのログインパスワードを設定すること。

(2) 利用者は、クライアントPCを利用しない時にはクライアントPCの電源を切ること。

(3) 利用者は、離席時には、各自が利用しているクライアントPCをロックすること。また、ロックし忘れた場合に備えて、パスワード・スクリーンセーバが自動起動するように設定すること。

5.2 電子メールパスワードの管理

(1) 利用者は、パスワードを設定すること。

(2) 利用者は、パスワードの管理にあたっては「A3205 利用者パスワードガイドライン」にしたがうこと。

(3) 利用者は、パスワードを電子メールソフトに永続的に保存しないこと。ただし、電子メールの受信のたびにパスワード入力を行うことが過度に煩雑である場合には、電子メールソフトに一時保存し、クライアントPC起動後のみパスワード入力とする仕組みを利用してもよい。

(4) 利用者は、パスワードを電子メールソフトに一時保存する場合には、当該パスワードを一時保存するクライアントPCを「主体認証情報格納装置」とみなして、以下の点に配慮して安全に取り扱うこと。

- パスワードを保存したクライアントPCを本人が意図せずに使用されることのないように安全措置を講じること。
- パスワードを保存したクライアントPCを他者に付与及び貸与しないこと。
- パスワードを保存したクライアントPCを紛失しないように管理すること。紛失した場合には、直ちに電子メールシステムの部局技術担当者又は部局技術担当者にその旨を報告すること。

6. 電子メールの受信

6.1 電子メールの受信確認

(1) 利用者は、定期的に、電子メールの受信確認を行うこと。

6.2 電子メール添付ファイルのウイルスチェック

(1) 利用者は、アンチウイルスソフトウェアによる自動ウイルスチェックを実施すること。

(2) 利用者は、電子メールシステムの部局技術担当者が自動的にウイルスチェックを実施するように設定している場合又は自動的にウイルスチェック最新データを更新するように設定している場合は、当該設定を変更しないこと。

(3) 利用者は、受信した電子メールの添付ファイルに対して、随時、ウイルスチェックを行うこと。これは、新種のウイルスに対応したパターンファイルの提供が間に合わず、ファイル受信時のウイルスチェックにおいてウイルスが発見されなかった場合を考慮し、最新のパターンファイルを用いて過去に受信した電子メールの添付ファイルに対してもウイルスの有無を確認するための対策である。

(4) 利用者は、緊急時対応が必要な時には、電子メールシステムの部局技術担当者からの指示に従うこと。

6.3 あて先間違いの電子メールを受信したときの対処

(1) 利用者は、あて先間違いの電子メールを受信し、送信者から正しい受信者へ再度送信する必要がある場合には、可能な範囲で送信者へあて先が間違っていたことを通知すること。

(2) 利用者は、あて先間違いの電子メールを受信した場合には、これを削除すること。

6.4 不審な電子メールを受信したときの対処

(1) 利用者は、不審な電子メールを受信した場合には、電子メールを開かず、電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

(2) 利用者は、電子メールに不審なファイルが添付されていた場合には、当該ファイルを開くことなく電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

6.5 ウイルスに感染したときの対処

(1) 利用者は、クライアントPCがウイルスに感染した場合、又は感染したと疑われる場合には、更なる感染を未然に防止するため直ちに当クライアントPCをネットワークから分離し、電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。
ネットワークからの分離は、具体的には、ネットワークケーブル、無線LANカード、USB

キー型無線LANアダプタなどを取り外す。または、無線LANアダプタがPCに内蔵されている場合には無線LAN機能を停止させる。

6.6 迷惑メールの対処

(1) 利用者は、必要以上に電子メールアドレスを公表し又は通知しないこと。

(2) 利用者は、ネットワークを経由して電子メールアドレスを開示し又は通知する場合には、アドレスを自動収集されないように、工夫を施すことが望ましい。（画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等）

(3) 利用者は、送信される迷惑メールに対しては、これを無視することが望ましい。送信者へ停止要求を出した場合、その電子メールアドレスが使用されている事実を伝えてしまう結果となり、かえって迷惑メールが増加してしまう可能性もあるからである。

7. 電子メールの作成

7.1 To、Cc及び Bccの制限

(1) 利用者は、To（あて先）、Cc（カーボンコピー）及びBcc（ブラインドカーボンコピー）の総あて先件数は必要最低限とすること。

- 使用するネットワークリソースは、電子メール１件の使用リソース×総あて先件数である。

(2) 利用者は、同時に多数の人へ電子メールを送信する場合、Bccを利用するか、あるいは各自に個別送信する等配慮すること。これは、その場合に電子メールアドレスをTo、Ccに列記してしまうと、当該電子メールを受信した者に、他の者の電子メールアドレスが露呈することになるからである。

7.2 電子メール１件当たりのファイル容量の制限

(1) 利用者は、電子メール本体と添付するファイルを含めた総容量が■■Mbyteを超えないこと。

- 本電子メールシステムでは、送信の際の容量制限を■■MByteとしている。

(2) 利用者は、電子メール本体と添付するファイルを含めた総容量が■■Mbyteを超える場合、別手段による情報提供や分割送信などについて検討の上、電子メールシステムの部局技術担当者に相談し、指示を仰ぐこと。

7.3 電子メールの形式の制限

(1) 利用者は、原則として、HTML形式の電子メールを送信しないこと。これは、当方より

HTML形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

7.4 電子メールの内容

(1) 利用者は、要機密情報を電子メールで送信する場合は別途定められた安全措置を講ずること。

- •利用者は、機密性3情報を電子メールで送信する場合には、電子メールシステムの部局技術担当者及び上司の許可を得ること。
- •利用者は、機密性2情報を電子メールで送信する場合には、電子メールシステムの部局技術担当者及び上司に届け出ること。
- •利用者は、要機密情報を電子メールで送信する場合には、安全確保に留意して送信手段を決定すること。例えば以下の手段が挙げられる。
  - ○ 外部を経由しないネットワーク(専用線等)
  - ○ 暗号化された通信路(VPN等)
  - ○ 暗号メール(S/MIME等)
- •利用者は、検討の上決定された送信手段について電子メールシステムの部局技術担当者及び上司へ届け出ること。
- •利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、以下の保護対策の必要性を検討し、必要があると認めたときには、これを実施すること。
  - ○ 添付ファイルに対するパスワード保護
  - ○ 添付ファイルの暗号化(暗号化ソフトの使用等)

(2) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

(3) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

(4) 利用者は、他人になりすまして電子メールを作成しないこと。

(5) 利用者は、電子メールを転送する際に、作成者の許可なく内容の変更をしないこと。

(6) 利用者は、個人情報やプライバシーの保護を考慮すること。

(7) 利用者は、次の事項に該当する電子メールの送信を行わないこと。

- 機密保護違反（■■方針・規程を遵守）
- 権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）
- セクシャルハラスメント及び人種問題に関わる内容

- 無礼及び誹謗中傷
- ねずみ講に相当する内容
- 脅迫、個人的な儲け話や勧誘に相当する内容

7.5 ネチケット

(1) 利用者は、チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わないこと。

(2) 利用者は、スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール）、ジャンクメール（役に立たない情報が書かれている電子メール）等を送信しないこと。

(3) 利用者は、電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。

(4) 利用者は、俗語的表現やあらかじめ定められていない省略語を使用しないこと。

(5) 利用者は、機種依存文字コードを使用しないこと。

•利用者が判断できない場合には、電子メールシステムの部局技術担当者に相談し、指示を仰ぐこと。

(6) 利用者は、電子メールを作成する際、各行とも全角30～35文字程度で改行を入れること。

(7) 利用者は、ToとCcとの使い分けを意識し、送信する電子メールに対する返事を要求する時には、To（あて先）を使用すること。

8. 電子メールの送信

8.1 送信時の注意

(1) 利用者は、To（受信者）の記述に誤りがないかを確認してから送信すること。

(2) 利用者は、電子メールにファイルを添付し送信する際に、当該ファイルのウイルスチェックを行うこと。

8.2 電子メールの暗号化

(1) 利用者は、要機密情報を電子メールで送信する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

•暗号メール(S/MIME等)

•添付ファイルの暗号化(暗号化ソフトの使用等)

［操作手順］　電子メール（S/MIME）の暗号化手順（Outlook® Express の場合）
Outlook® Express の新規メール作成画面の[ツール]メニューから [S/MIME暗号]を選択の上、送信する。 なお、送信に先立ち、送り先相手の電子証明書の取得は完了しているものとする。

(2) 利用者は、暗号化された情報の復号に用いる鍵を適切に管理すること。

(3) 利用者は、暗号化された情報の復号に用いる鍵のバックアップを取得しておくこと。

8.3 添付ファイルのパスワード保護

(1) 利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、添付ファイルにパスワードを設定すること。

［操作手順］　文書ファイルのパスワードのかけ方（Word®の場合）
Word®の[ファイル]メニューから[名前を付けて保存]を選択した後、[ツール]から[セキュリティオプション]を選択し、[読み取りパスワード]を設定する。
あるいは、[ツール]メニューから[オプション]を選択し、[セキュリティ]タブの画面からも同様の設定が可能である。

(2) 利用者は、保護に用いたパスワードについては、あらかじめ受信者と合意した文字列を用いるかあるいは、電子メールで送信せずに電話などの別手段を用いて伝達すること。

8.4 電子メール送信時における情報漏えい防止の確認事項

(1) 利用者は、添付ファイルを電子メールで送信する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないか確認すること。

- 「プロパティ」に作成者や修正者等の個人情報が残っていないか
- 一見すると表示されていない部分（「非表示」の設定箇所、非表示としたコメント、裏に隠れたシート等）に要機密情報が含まれていないか
- 変更履歴が必要以上に保存されていないか

8.5 電子メールへの署名付与

(1) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

［操作手順］　電子メール (S/MIME) の暗号化手順（Outlook® Express の場合）

Outlook® Express の新規メール作成画面の[ツール]メニューから [S/MIME暗号]を選択の上、送信する。 なお、送信に先立ち、送り先相手の電子証明書の取得は完了しているものとする。

(2) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

8.6 電子メール送信時の受信確認機能の使用制限

(1) 利用者は、トラフィック増を防止するため、電子メール送信時の受信確認は必要最低限の使用とすること。

8.7 電子メールを誤って送信したときの対処

(1) 利用者は、電子メールを誤って送信した場合、相手先（受信者）へのフォローは発信者責任で実施すること。

8.8 ウイルスを送信したときの対処

(1) 利用者は、誤ってウイルスを送信したことが判明した場合、直ちに電子メールシステムの部局技術担当者に連絡・相談し、指示を仰ぐこと。

9. 電子メールの保存・削除

9.1 メールボックス（サーバ側）における電子メールの保存・削除

(1) 利用者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、メールボックスから不要な電子メールを削除すること。

- サーバ側の個人別メールボックスに格納される電子メールの最大容量は、■■Mbytesに設定されている。

(2) 利用者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、クライアントPCへの保存を行うこと。

- サーバ側の個人別メールボックスに格納される電子メールの保存期限は、■か月に設定されている。

9.2 メールボックス（クライアントPC側）における電子メールの保存・削除

(1) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを保存する場合には、暗号化等の措置を講じた上で保存することが望ましい。

(2) 利用者は、本文や添付ファイルに要保全情報が含まれている電子メールについては、適宜バックアップすること。

(3) 利用者は、不要なメッセージは速やかにクライアントPCから削除すること。

(4) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを削除する場合には、その機密性に配慮し、復元が困難な状態にすること。

10. 本手順に関する相談窓口

(1) 利用者は、緊急時の対応及び本書の内容を超えた対応が必要とされる場合には、電子メールシステムの部局技術担当者に相談し、指示を受けること。

(2) 利用者は、本書の内容について不明な点及び質問がある場合には、電子メールシステムの部局技術担当者に連絡し、回答を得ること。

A3203 ウェブブラウザ利用ガイドライン

解説：本ガイドラインの対象者は、行政事務従事者を除く一般利用者である。

1. 本書の目的

ウェブは、情報の伝達や共有に必要不可欠なツールとなっている。一方で、私的目的でのウェブの閲覧、掲示板への無断書き込み等は、大学の社会的信用を失わせる要因となる可能性もある。本書は、このようなリスクを軽減し、情報資産を保護し、利用者がウェブを安心・安全に利用するために必要な事項を定めることを目的とする。なお、ウェブブラウザを利用する PC 端末にはウィルス対策ソフトウェアが導入されているものとする。ウィルス対策ソフトウェアが導入されていない PC 端末でのウェブ閲覧は原則として禁止する。

2. 本書の対象者

2.1 対象者

本書は、ウェブブラウザを教育や研究目的で利用するすべての教員学生（以下利用者と呼ぶ。）を対象とする。 行政事務従事者は、事務手順書のブラウザ手順に従うものとする。

3. ウェブの利用に係る全般的な注意事項

ウェブブラウザを利用したウェブサイトの閲覧、各種情報システムの利用等、ウェブの利用において、利用者の安全性を確保するために、ウェブの利用に係る全般的な注意事項を記述する。

3.1 目的外利用の禁止

(1) 利用者は研究や教育および教育支援等、大学で活動する上で必要な範囲でウェブサイトを閲覧するものとし、それ以外で閲覧しないこと。営利目的でのネットワーク利用は禁止する。

(2) 利用者は学内から任意のウェブサイトを閲覧することにより、閲覧先のサーバに本学のドメイン名及び IP アドレス等が記録されることに留意すること。記録された情報をもとに、サーバ管理者により本学に対して不当な要求が行われるとか、閲覧者の個人情報の開示をサーバ管理者が要求する場合がある。また、掲示板等に名前やメールアドレスを記入して場合、不正請求をされることもある。

【閲覧可能なウェブサイトをコンテンツフィルタリング等により制限する場合（強化遵守事項）】

3.2 閲覧可能なウェブサイトの制限

(1) 適正なウェブ利用を維持するため、コンテンツフィルタリング等により閲覧可能なウェブ

サイトを制限している。利用者は、閲覧したいウェブサイトが閲覧制限されている可能性に留意すること。

(2) 利用者は、コンテンツフィルタリング等による閲覧制限がなされていないウェブサイトであっても、当該ウェブサイトの閲覧が許可されているわけではない点に留意すること。

(3) 利用者は、制限されているウェブサイトの閲覧が必要な場合には、部局技術管理者に連絡・相談すること。

3.3 プラグイン等の導入・利用の禁止

(1) 利用者は、部局技術責任者が端末で利用可能と定めていないプラグイン（ウェブブラウザの機能を拡張するためのソフトウェア）等の、端末への導入、利用を行わないこと。

(2) 利用者は、部局技術責任者が端末で利用可能と定めていないプラグイン等の導入、利用が必要な場合には、部局技術管理者に連絡・相談すること。

3.4 外部のウェブサイトで提供されているサービスの利用等の注意事項

(1) 利用者は、学外の掲示板、ブログ等への書き込み、ウェブメールの利用等にあたっては、情報漏えいの可能性に十分に注意すること。

(2) 公序良俗に反する不適切な書き込みや利用を行わないこと。掲示板等への単純な書き込みであっても、内容によっては本学や本学構成員の良識が疑われる場合がある。特に、他人への誹謗中傷と誤解されるような記事やプライバシーや著作権等の侵害と疑われかねない書き込みをしてはならない。

(3) 不正なサイトへの誘導を狙ったリンクやウィルス等の不正なソフトウェアをダウンロードさせることを目的としたリンクはインターネット上に多数存在する。有名なサイトであっても決して安全ではないので、不用意にリンクをクリックしないこと。

3.5 ウェブサイト閲覧の監視

(1) 適正なウェブ利用を維持するため、その利用状況（いつ、誰が、どのウェブサイトを閲覧したか等）について監査証跡の取得、保存、点検及び分析を行う可能性がある。利用者は、その趣旨を理解の上、自身のウェブサイトの閲覧がモニタリング及び監査されていることを認識すること。

4. ウェブサイトの閲覧

ウェブサイトの閲覧に使用するウェブブラウザの利用方法、ウェブサイトを閲覧する場合に想定される脅威を回避するための注意事項等について記述する。

4.1 ウェブサイト閲覧時の一般的な注意事項

(1) 利用者は、ウェブサイトを閲覧する場合には、以下の事項に留意すること。

- ウェブサイトの情報には、正しい情報だけでなく偽情報や誤情報が含まれている可能性があるので、ウェブサイトの情報を検討せずそのまま採り入れないこと。
- 目的とするウェブサイトの閲覧には、URI を直接入力すること。データ入力に中継サイトを利用するとデータの詐取やクロスサイトスクリプティングの危険性がある。また、認証を求められるページへ入って後で、そのページから張られたページへのリンクの参照は、認証情報が不正利用されることがあるので注意が必要である。
- ウェブページの再読み込みを短時間に繰り返すと、サービス不能攻撃（DoS 攻撃、サービスに不要な通信をおこさせて、サービスの質の低下を狙った攻撃）と見なされる可能性があるので注意すること。 サイトによっては、当該ドメインや当該 IP アドレスからのアクセスがブロックされる可能性がある。オンラインジャーナルの大量一時ダウンロードによっても、アクセスブロック等の問題が発生することがある。
- 検索サイトでは、検索結果に有害なウェブサイトへのリンクが含まれている可能性があるので、安易に検索結果のリンク先を閲覧しないこと。また、検索結果リストの表示の順番は重要度とか参照頻度といった特別な意味があるわけではない。先頭に表示されるからといって、正しいということはない。
- 有名で広く知られているサイトであっても、バナー広告等を安易にクリックしないこと。有害なサイトやウィルスダウンロードサイトがリンクされていることがある。
- 電子メールで送られてきた HTML メール内のリンクを安易にクリックしないこと。成りすましサイトやワンクリック詐欺サイトへの誘導、phishing 被害につながることがある。次ページに phishing サイトの例を示す。画面上で URI に見える部分は見せかけのテキストで、ID とパスワードを詐取するためのサイトへのリンクになっている。
- ウェブページ閲覧時に、見かけないセキュリティ警告表示とともにソフトウェアのダウンロードを求められてもダウンロードしないこと。ウィルスや不正なソフトウェアをインストールさせられる可能性がある。

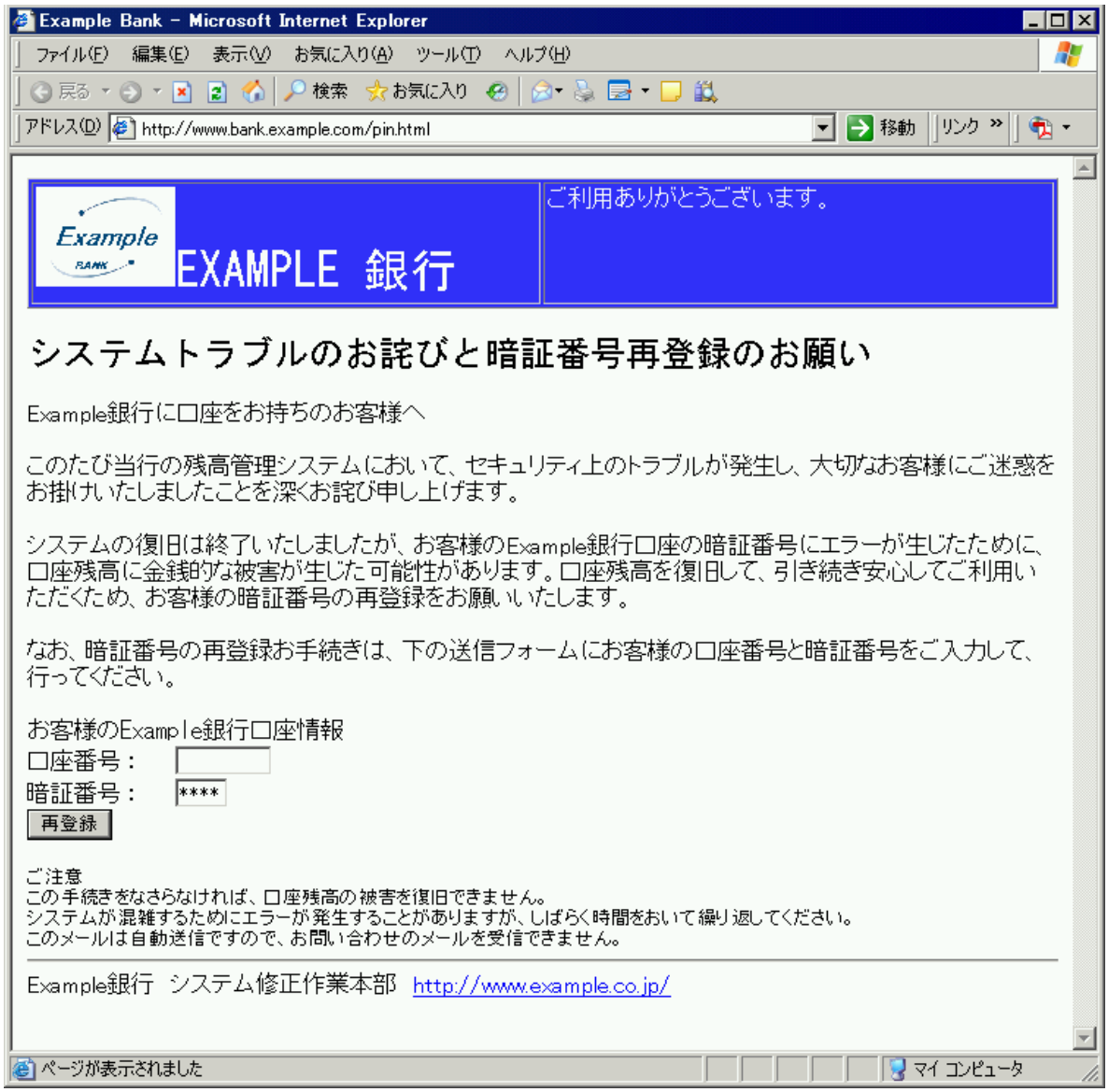


図１　金融機関からの連絡を装って暗証番号を盗み出そうとするサイトの例（説明用に作成）[3]

4.2 SSL/TLS 通信の確認

(1) **SSL/TLS 通信とは、通信内容の暗号化及び通信相手のなりすまし対策がなされた安全な通信であり、重要な情報等を送受信するウェブサイトで標準的に利用されている技術である。利用者は、閲覧しているウェブサイトと個人情報、重要な情報等を送受信する可能性がある場合には、SSL/TLS 通信が利用されていることを確認すること。また、その際提示される証明書が正当なものであることを確認すること。証明書によっては、次ページの図のような画面が表示される。このような場合には注意が必要である。**

[3] 図１～図４では、Microsoft Corporation のガイドラインに従って画面写真を使用しています。Windows® Internet Explorer® は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

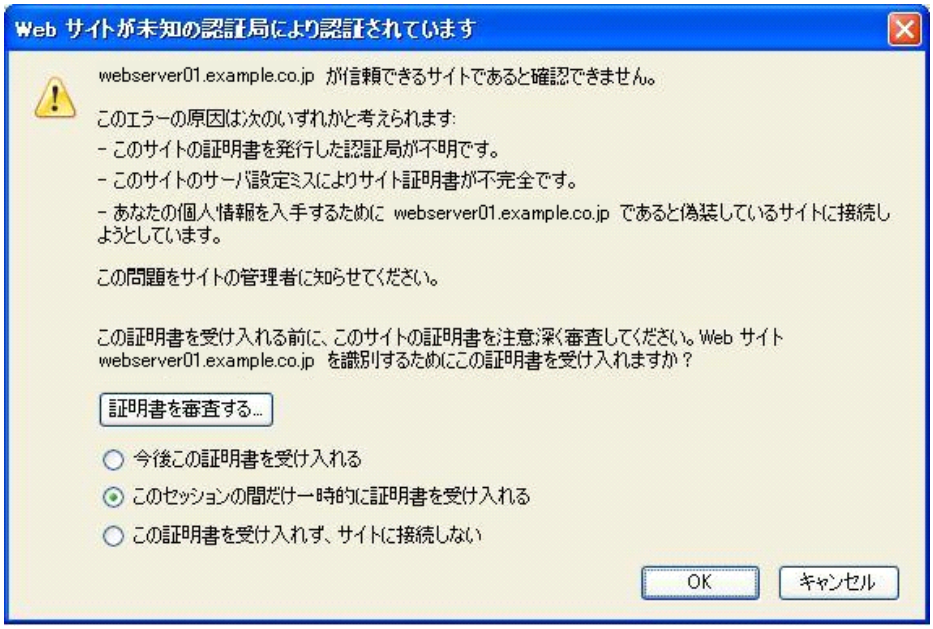


図２　注意を要する証明書への警告表示の例（１）

また、以下のような警告が表示されることもある。

図３　注意を要する証明書への警告表示の例（２）

SSL を利用している場合には、下図のような錠前が表示されることが多い。

図４　SSL を利用していることを示す表示

ただしウェブサーバ証明書は誰でも取得できるものであることを 理解しておかなければならない。

【ウェブブラウザの設定によりダイアログを表示する設定にしている場合】

4.3 確認・警告等のダイアログへの対応

(1) セキュリティ機能に係る設定等により確認のためのダイアログ等が表示される可能性がある。当該ダイアログに関して安易に ActiveX®、Java®等のスクリプトの実行を許可すると、不正プログラムの感染、情報漏えい等の危険性があるため、利用者は、確認のためのダイアログが表示された場合には、中身を確認せずに安易に実行を許可してはいけない。

4.4 ウェブブラウザの設定変更を要求するウェブサイトの閲覧

(1) 利用者は、ウェブサイトから閲覧のためにプラグイン、スクリプト等の実行に関するウェブブラウザの設定変更を要求された場合であっても、ウェブブラウザのセキュリティレベルが低下し不正プログラムに感染する危険性等があるため、当該要求に従ってウェブブラウザの設定を安易に変更しないこと。

5. ウェブサイトへの情報送信（フォームへ入力した情報の送信、ファイルのアップロード等）

送信する情報の盗聴、なりすましによる誤った通信相手への情報送信その他ウェブサイトに情報を送信する場合に想定される脅威を回避するための注意事項等について記述する。

(1) 重要な情報のやりとりには SSL/TLS 等の安全な通信を利用すること。その際、証明書の正当性を確認すること。

(2) 情報の書き込みにあたっては、クロスサイトスクリプティング等の危険性に留意すること。入力の必要なページは、ポータル等を経由せずに参照すること。

6. ファイルのダウンロード

不正プログラムの感染その他ウェブサイトからダウンロードしたファイルを実行又は開く場合に想定される脅威を回避するための注意事項等について記述する。

6.1 ウェブブラウザから直接的に、実行ファイルを実行する行為及び文書ファイル等を開く行為の制限

(1) ウェブブラウザから実行ファイルを直接的に実行した場合でもアンチウイルスソフトウェア等の自動検査機能によりウイルスを検出することが可能であるが、利用者は、実行ファイルをダウンロードする場合には、電子署名及び不正プログラムの有無を確認し、また問題が生じた場合に原因となったファイルの特定を容易にするため、ウェブブラウザから直接実行するのではなく、端末上に一旦ダウンロードすることが望ましい。

(2) ウェブブラウザから文書ファイルを直接的に開いた場合でもアンチウイルスソフトウェア等の自動検査機能によりウイルスを検出することが可能であるが、利用者は、ウェブサイト上にある文書ファイル等を開こうとする（利用しようとする）場合には、不正プログ

ラムの有無を確認し、また問題が生じた場合に原因となったファイルの特定を容易にするため、ウェブブラウザから直接開くのではなく、端末上に一旦ダウンロードすることが望ましい。ただし、信頼できるウェブサイト上にある文書ファイル等を開こうとする（利用しようとする）場合、この限りではない。

(3) 利用者は、ダウンロードした実行ファイルが部局技術責任者により定められた利用可能なソフトウェアに含まれていない場合には、導入、利用しないこと。

6.2 保存したファイルに対する不正プログラムの有無の確認

(1) 利用者は、保存したファイルを実行又は特定のソフトウェアにより開く前に、不正プログラムの有無の確認を行うこと。

(2) 利用者は、保存したファイルに不正プログラムが含まれていることが判明した場合には、当該ファイルを実行せずに又は特定のソフトウェアにより開かずに、部局技術管理者に連絡・相談し、指示を仰ぐこと。

6.3 保存した実行ファイルの電子署名の確認

(1) 利用者は、保存した実行ファイルについて電子署名により配布元が確認できる場合には、配布元が適切な組織であることを確認すること。

6.4 不正プログラムに感染した時の対処

(1) 利用者は、ダウンロードしたファイルを実行し又は開いたことにより、不正プログラムに感染したか又は感染の疑いがある場合には、直ちに LAN ケーブルを抜くことにより当該 PC をネットワークから分離し、部局技術管理者に連絡・相談し、指示を仰ぐこと。

7. 本手順に関する相談窓口

(1) 利用者は、緊急時の対応又は本書の内容を超えた対応が必要とされる場合には、部局技術責任者に相談し、指示を受けること。

(2) 利用者は、本書の内容について不明な点又は質問がある場合には、部局技術管理者に連絡し、回答を得ること。

用語集

- URI（Universal Resource Identifier）
  http://wwww.example.com/のようなウェブサイトをアクセスするためのキーとなる情報。URL（Universal Resource Locator）と呼ぶこともも普通におこなわれている。
- クロスサイトスクリプティング（CSS、XSS の脆弱性）
  クロスサイトスクリプティングとは、入力データの正当性検査の甘いウェブサイトの利用者を狙った攻撃で、データ入力の際に悪意のあるサイトを経由すると、そこでスクリプトと呼ぶプ

ログラムが入力データに挿入される。挿入されたスクリプトは、入力データをチェックしていないサーバで利用者入力データとともにブラウザに送り返される。スクリプトはブラウザの画面には表示されないが、スクリプト実行を制限していないブラウザでは解釈実行されてしまい、重要な情報が盗み取られたりする。
（IPA セキュリティセンターによる解説）
http://www.ipa.go.jp/security/awareness/vendor/programming/a01_02.html

- phishing（フィッシング）
  phising とは、たとえばオークションサイトと類似の画面を持ったなりすましサイトに利用者を誘導し ID やパスワードを盗み出すような行為である。ニセのサイトには、電子メール等で HTML メールのリンクから誘導する。

A3204 ウェブ公開ガイドライン

1. 本ガイドラインの目的

A大学（以下、本学）からウェブによって情報発信を行うことはもはや必要不可欠といえる。一方で、各種権利侵害を伴うようなウェブコンテンツの公開や掲示板等の開設は、その為のトラブル対応による業務効率の低下や、本学の社会的信用を失わせる要因となる可能性もある。

本ガイドラインは、このようなリスクを軽減し、情報資産を保護し、利用者がウェブを用いて各種コンテンツや情報を、正確かつ、安心・安全に公開するために必要な事項を定めることを目的とする。

解説：本ガイドラインは、学生個人や研究室単位でのウェブサーバの公開を主に想定したものである。それ故、公開コンテンツの内容の多様さとそれに伴う注意事項を中心としたガイドラインとなっている。
その際にまず何より重要なことは、その発信される情報の内容が、正確かつ公開者・利用者にとって安全なものでなければならない。
なお大学や学部の公式ウェブページの運用のための指針は、学内の広報規則等に別途定めてあるので、そちらの規則にまず従うことが前提となっている。

2. 本ガイドラインの対象者

本ガイドラインは、学内よりウェブページを用いて情報発信を行うすべての者を対象とする。

また外部業者に委託する場合も、コンテンツの中身に関する責任は本学にも帰するので注意が必要である。

3. ウェブの公開に係る全般的な注意事項

ウェブを用いて各種情報を公開する際には、各種法令を遵守することはもちろんのこと、契約ISPの利用規約や、関連の学内規則をも守らなければならない。

また公序良俗に反する行為や社会通念上してはならないことは、ウェブ公開の際にも同様に行ってはならない。

解説：ウェブによる各種情報の公開の際に、利用者の安全性を確保し、権利侵害などを防止し、また業務効率を向上させるために、全般的な注意事項を以下に記述する。特にコンプライアンスの精神が必要であることは言うまでもない。

参考として、以下にSINETの加入規約の一部を記載する。全文はSINETのページ（http://www.sinet.ad.jp/）を参照のこと。

第７条（加入にあたっての遵守事項）
加入者は、次の各号に掲げる事項を遵守しなければならない。
一　研究・教育並びにその支援のための管理業務以外の目的にネットワークを利用しないこと。
二　営利を目的とした利用を行わないこと。
三　通信の秘密を侵害しないこと。
四　ネットワークの運用に支障を及ぼすような利用をしないこと。
五　ネットワーク及び接続するコンピュータに対する不正行為等が発生しないように最善の努力を払うこと。
六　その他所長が別に定める事項

ウェブを用いた情報公開には大きなメリットがある反面、様々な危険やリスクを伴うことも承知しなければならない。情報発信者の責任として、その意義と危険性についての十分な認識が求められる。ウェブに限らず、ネットワークの世界も現実の世界同様、自己責任の原則によって成り立っていることを忘れてはならない。

3.1 著作権等の知的財産権の遵守

他人が保有する知的財産権を侵害してはならない。特に、ウェブ公開時には著作権侵害が発生しやすいので、十分に注意すること。

解説：およそ他人がつくった作品には著作権が存在する。よって自分の作ったコンテンツ以外は原則として許諾なしには掲載してはいけない。
また、ウェブに公開することを著作権者が許諾する「公衆送信権（送信可能化権）」は、通常の複製を許諾する「複製権」とは別の支分権でありこれらは別個に許諾を受ける必要がある。その為、複製の許諾を受けたからと言って公衆送信も出来るわけではないことに注意が必要である。
同様に、著作権法第 35 条が規定している「学校その他の教育機関における複製等」の権利制限も、あくまで“複製”に対してのみ及ぶのであって、複製以外には適用されないので注意が必要である。
ただし「引用」など、条件を満たせば“著作権の制限”の一つとして、許諾なしでの利用を行うことができる場合もある。

解説：（著作物の保護期間）
著作権の保護期間は、原則、作者の死後 50 年（法人著作の場合は公表後 50 年）である。よって、明治期から戦前期などのものに関しては、著作権が消滅しているかどうか十分に確認すること。また、映像著作物に関しては保護期間が 70

年となったので注意すること。

解説：（引用が成立する条件）

引用は、例外的に著作権者の許諾なく行うことができる。

> ***著作権法 32 条：公表された著作物は、引用して利用することができる。この場合において、その引用は、公正な慣行に合致するものであり、かつ、報道、批評、研究その他の引用の目的上正当な範囲内で行われるものでなければならない。***

判例では引用が成立するためには次のような条件が必要とされている。

- 正当性　→　それがその場所に引用するに相当する理由が必要である。前後の繋がりのないものをいきなり持ってきても引用とはならない。
- 明瞭区分性　→　自己の文章と引用文との違いが明確に分かる必要がある。通常の論文であればカギ括弧で括るなどするのが普通であるが、ウェブ上で表現する場合は、境界線を引いたり、フォントの字体や色などを変えるというやり方でもよいであろう。
- 出典元の明記　→　出典先は単なる書物名だけでなく、何ページからの引用なのかもできるだけ詳細に記載する必要がある。他のウェブ上から引用する場合は、URL 等を記載しておくと良いだろう。また、ウェブからの引用の場合は状況に応じて参照した年月日を記載しておくとよい。
- 自分の文章が主たる物であり、引用先の文章が従たる物であること　→　引用はあくまで自己の著作を補完するものである必要がある。分量的にも、相手先の文章が自己の文章よりも多い場合には引用と認められない。

など。

解説：（著作人格権（特に “ 同一性保持権 ”））

作者は著作物の同一性を保持する権利を有している。日本の著作権法は、作者の意に反する改変を認めてはいない（これは人格権として一身専属の権利であり、売買や譲渡もできない）。そこで、許諾を得て他人の著作物をウェブ公開する際や、きちんと条件を守って引用をする際であっても、その著作物を掲載する際は改変せずにそのまま載せる必要がある。

解説：（著作権が存在しないもの）

単なるファクトデータ（経済指数や気象統計など）には著作権は存在しない。ただし、これらの他人が制作したファクトデータをそのままコピーして新たなデータベース（いわゆる「創作性のないデータベース」）を作成した場合には、

他の法律によって処罰または損害賠償の対象になることがあるので注意すること。例えば、不正競争防止法や民法の不法行為(709 条)などに問われることがある。この件に関しては、自動車の性能情報等一覧データベースに関する判例「翼システム 対 システムジャパン」（東京地裁　平成 13 年 5 月 25 日）が参考になる。

○ネット上での著作権の扱いに関して参考となる URL:
・著作権情報センター（CLIC）： http://www.cric.or.jp/
・メディア教育開発センター（NIME）： http://www.nime.ac.jp/

3.2 肖像権・パブリシティー権などを侵害してはならない

解説：人は各々、人格権的な権利として、肖像権を有すると考えられている。そこで、他人の顔が写っている写真等を掲載する際には、「肖像権」に十分注意すること。原則、本人の許諾なしに写真を掲載するべきではないだろう。
また著名人の場合は一般人よりは肖像権が制限されると考えられているが、その分、彼らは顧客吸引力という経済的利益を有するので、「パブリシティー権」という権利を持つと考えられている。よって芸能人やスポーツ選手などの写真は無許諾で掲載してはならない。

3.3 他人に迷惑をかけるような情報発信の禁止

ウェブ上で情報発信する際は、他人に迷惑をかけるような情報を発信してはならない。
他人に迷惑をかけるような情報としては、
・人を誹謗中傷する内容のもの
・他者のプライバシーを侵害するような情報
などがある。

解説：他人への誹謗中傷は、自身のウェブページ上ではもちろんのこと、掲示板上などにも書き込んではいけない。こういった行為は名誉毀損に問われる可能性がある。名誉毀損は、民法上の損害賠償の対象となるだけではなく、場合によっては刑法上の名誉毀損罪（刑法 230 条）となり刑事罰（３年以下の懲役もしくは禁錮、または五〇万円以下の罰金）が科される場合があるので、注意が必要である。
また、他人のプライバシーに関する情報を自分のウェブページなどに掲載する場合には十分な注意が必要となる。プライバシーは一般的には、他人に知られたくない情報、いわゆるセンシティブ情報だとされているが、プライバシーの概念は判例や法律で厳格に規定されたものでないが故、その判断が難しい。よ

って他人の情報の取扱に関しては、その掲載がその人に何らかの影響をあたえる可能性がある場合は、掲載するべきではない。(たとえ本人がよかれと思ってやっても、当事者からしてみれば望まぬ結果になる可能性もあるので、悪影響だけではなく、単に影響を与える可能性がある場合でも掲載すべきではない。)

3.4 研究成果や研究途中の情報を掲載する際の注意

研究成果や研究途中の情報を掲載する際には、公開に問題がないか十分留意すること。

解説：民間企業や他の研究者との共同研究の場合には、守秘義務契約等に違反していないか留意する必要がある。また、特許等の取得を考えている場合も、先にウェブに公開してしまうと公知の事実となり、特許取得の条件である新規性が失われるので注意が必要である。

3.5 企業名やロゴなどの扱い

学会やシンポジウム等で協賛企業のロゴを貼るときは、事前に相手側と協議すること。

3.6 顔写真の掲載によるリスク

自身の肖像写真を掲載する場合にも、顔を露出する際のリスクを十分に考慮すること。

解説：自分の名前や顔をウェブに公開することは、そのメリット・デメリットを十分に考える必要がある。場合によっては、他人から謂われのない迫害や誹謗中傷を受けたり、発言に対する揚げ足とりや横やりなどが入ることがある。また、ストーカー被害などに遭うといったことも十分考えられるので、注意が必要である。

研究室構成員の紹介や集合写真などを掲載する場合は、自分一人分だけを掲載するときよりもさらなる注意をすること。原則的には学生の顔は掲載しないことが望ましい。どうしても必要な場合は、写真を似顔絵やイラストなどで代用する方法もある。

さらに、指導教員は学生が各自でウェブページを持つ場合などにおいて十分に注意を促す必要がある。

3.7 その他（公序良俗に反する情報発信の禁止など）

違法な情報はもちろんのこと、公序良俗に反する情報や有害情報を発信してはならない。

解説：わいせつな文書・図画などのほかに、有害情報としては、次のようなものがある。

・情報自体から、違法行為を誘引するような情報（銃器や爆発物、禁止薬物や

麻薬の情報など）
・人を自殺に勧誘・誘引する情報
・ネズミ講やマルチ商法の勧誘
・ハラスメントに関する記述を伴うような情報
など。
有害情報や違法情報に関する具体例は、「インターネットホットラインセンター」（http://www.internethotline.jp/）などの運用ガイドラインに詳しいので、詳細はこちらを参考にすると良い。

4. デジタルアーカイブを行う際の注意事項

古典資料などのデジタルアーカイブをウェブで公開する際には、各種権利処理が済んでいるかをきちんと確認すること。

解説：古典資料においては、通常、著作権は消滅しているが（＊著作権は、原則、作者の死後 50 年をもって消滅する）、それ以外にも、物件としての所有権やアーカイブ時（デジタル化時）の費用負担者などとの間での様々な利害関係がある場合があるので、様々な方面からの検討が必要である。
例えば、大学所蔵の古典資料などに関しては、その昔、単に地元の旧家などから保管を委託されただけのものである可能性もありえるし、ウェブ公開をしないことを条件に所有者がデジタル化を許諾したものでないかなども確認すること。
また判例では、「およそ正当な手段を持って入手された著作権の切れたコンテンツの複製物を公表する際には、その原版所有者の許諾は不要である」とされているが(*)、実務では、このような場合にでも、何らかの金銭的支払いを行うこともある。また、事後に資料提供者（デジタルアーカイブ化協力者）との間で、ウェブ上での公開の仕方を巡ってトラブルとなる場合が多いので、事前にできるかぎり詳細な打ち合わせを行っておくことが望ましい。この際に、口頭での取り決めのみしか行わなかった場合、事後にトラブルや遺恨を残すこともあるので、明文化した書類を取り交わしておくべきである。

(*) 顔真卿自書建中告身帖（がんしんけいじしょけんちゅうしんこくしんちょう）事件　最高裁判所昭和５９年１月２０日判決
顔真卿は唐代の有名な書家である。その顔真卿の書である自書告身帖を複写した写真乾板を所有する出版社がその書集を出版したところ、その原書の所有者から出版の差し止め及び廃棄を求められた事件。その写真乾板はもちろん正当なる手段によって入手されたものである（つまり、盗品、盗撮品で

はない)。

最高裁は、「美術の著作物の原作品に対する所有権は、その有体物の面に対する排他的支配権能でとどまる」とし、複製された写真にまでは及ばないとした。また、「博物館や美術館において、著作権が現存しない著作物の原作品の観覧や写真撮影について料金を徴収し、あるいは写真撮影に許可を要するとしているのは、原作品の所有権に縁由するもので、一見、所有権者が無体物である著作物の複製等を許諾する権利を専有するようにみえるが、それは、所有者が無体物である著作物 を体現している有体物としての原作品を所有していることから生じる反射的効果にすぎない。」との見解を示している。

3.1 で前述した、著作権情報センターの FAQ にも本事件の解説がある。(http://www.cric.or.jp/qa/sodan/sodan7_qa.html)

5. リンクの際の留意点

ウェブページを公開する者は、リンクの設定に関して注意をすること。

5.1 自らリンクを張る際

リンクの設定自体は、慣習上、相手の許諾を得ることなしに自由に行えるものとされている。しかし、トップページ以外の他の階層に直接リンクを張る場合においては、必ずしもその限りではないので注意すること。よってリンクはトップページに設定するように心がけること。

解説:海外ではディープリンクの可否について争った事例がいくつか存在する。バナー広告を表示させないようにしたり、他者のコンテンツの本質部分(ニュース記事本文)などがあたかも自分のページのオリジナルコンテンツであるかのように思わせるようなリンクの張り方をした場合は問題ありとの判断がなされる場合がある。

6. 各種利用規程の遵守と目的外利用の禁止

6.1 目的外利用の禁止

ウェブ公開者は、本ガイドライン以外にも、関連の情報システムの利用に関する規程や規約を守らなければならない。また本学の定めるネットワーク利用目的や、SINET が定める目的以外の利用をしてはならない。

本学の情報設備および SINET は、もっぱら教育・研究の推進と職務・支援業務遂行のために提供されている。そのため、情報発信者は、公用と私用の区別を意識して、設置目的にそぐわない情報を公開しないように注意することが求められる。目的外利用の典型は、本学の情報設備を研

究目的ではなくもっぱら利益を上げる商業目的で利用するというような場合である。

解説：目的外利用の一例として、学生が以下のような行為をウェブ上で行う事は好ましくない。
・自身のページで家庭教師等のアルバイトの宣伝をすること
・アフェリエイトなどの運営　など
教員が自著を紹介する際も注意が必要である。本の紹介や学生へのテキスト販売などに必要な情報を超えての、書物の宣伝・販売行為は、学術ネットワークの目的を超えた利用と見なされる可能性がある。

6.2 **本学では、個人ページや各研究室サーバからの政治や宗教に関する情報の発信はこれを禁止する。**

解説：6.2 は「このような記述もあり得る」というサンプル規定である。
政治や宗教に絡む情報に関しては、その扱い方や考え方に様々な基準が考えられる。そこでこれらの情報発信に対する基準をあらかじめ明文化しておくことが大事である。その際の運営方針の一つとして、宗教や政治に関するものを全面的に禁止してしまう方式のポリシーもある。むろん大学や学部の性質によってはこれらに関する情報発信が必要な場合も逆に存在しうるであろう。重要なことは、いずれの場合にでも、その為のガイドラインをきちんと明文化しておくことである。

7. システムの安全性の確保

7.1.セキュリティの確保

ウェブページを作成するときは、セキュリティの確保に十分注意する。特に OS **や各種ソフトウェアなどは修正パッチなどを充て、恒常的に最新の情報を保つこと。**

ページの作成を外部の業者に委託するときも同様である。

解説：サーバシステムを可能な限り安全な状態にしておくことは言うまでもない。ウェブコンテンツを外部の業者に発注するときは、デザインや見栄え、アクセシビリティだけではなく、必ずセキュリティ技術も契約の要件とし、セキュリティ確保分に関しても、相応の投資をすること。外部業者に委託した場合でも、その責任は本学にも帰するので注意が必要である。

7.2 CGI **の禁止、**SSL/TLS **通信の使用**

7.2.1 **本学ではウェブページ内における** CGI **の使用を全面的に禁止する。**

7.2.2 パスワードや個人情報を入力するページにおいては、必ず SSL/TLS などで保護された通信を用いること。

解説：7.2 は「このような記述もあり得る」というサンプル規定である。
ポップアップや CGI などを使うページはセキュリティレベルが下がるので、その扱いにおいては、できるだけ使用させないような方向で、統一した基準を設けておくことが望ましい。この場合、禁止としてしまうやり方、あらかじめ大学側が許可したものについてだけ使用を許可するやり方などが考えられる。
またパスワードの入力や個人情報などの入力を求める場合は、必要に応じて SSL/TLS などで保護された通信を用いること。

7.3 隠しディレクトリに関する注意

公開すべきでない情報は、たとえ隠しディレクトリであっても決して蔵置してはならない。

解説：公開ウェブページから直接リンクを張っていない、いわゆる「隠しディレクトリ」や「隠しファイル」であっても、検索エンジンのロボットはこれらの情報も取得していくので、広く一般の人の目に触れて困る情報は、public_html の下に置いてはならない。このやり方は、一部のメンバーだけに情報を提供する際などによく使われるが、どうしても必要な場合は、期間を限定する、Basic 認証を行うなどの手段を用いること。現実に、聴講生だけに成績を通知しようとして隠しディレクトリに成績をおいたまま放置しておいたが故に、それが検索エンジンに収集され学外に流失した事例がある。
いずれの場合においても、前述の通り、そもそも外部の人の目に触れると不都合な情報はウェブサーバ上においてはならない。
また、日付やファイル名をそのまま URL に使うことによって容易に想像されてしまうようなアドレスは、たとえトップページからのリンクを張っていなくても、他人がそれを入力してしまい情報を事前に入手してしまうことがあるので、決してそのようなことはやってはならない。現実に、過去にこのようなやり方を取ってしまったが故に、事前に合格者番号などが漏洩してしまった事例がある。

7.4 公開掲示板（BBS）等の開設の禁止

本学では、研究室サーバや個人のサーバで公開掲示板（BBS）等の開設を禁止する。

解説：7.4 は「このような記述もあり得る」というサンプル規定である。
誰でも自由に書き込める掲示板などは、様々な権利侵害やトラブルの原因となりやすいので、特別の事情がない限り立ち上げない方が望ましい。開設を許可

する際も、その基準を明確にしておくことが望ましい。(1)全面禁止、(2)許可が必要、(3)自粛、(4)研究室内メンバーなどの限られた範囲でパスワード等の認証を用いて利用者制限を行う場合のみ許可、などの方針が考えられる。

7.5 十分なサーバ容量やネットワーク資源の確保

ウェブページを公開するためのサーバを設置する際には、そのマシンやネットワークが十分なアクセスに対応しうるものとすること。

解説：大規模な学会やシンポジウムの準備の為に、研究室内のサーバを使う場合などがよくあるが、そういった場合には、システムダウンが起こりやすいので十分注意すること。
特に、大容量のファイル等をやり取りする場合は、自身のサーバだけでなく、その上流のシステムの容量にも十分に配慮しなければならない。
これは、大学や学部の公式サーバで、大学入試の合格者発表を行う際も同様である。

8. ウェブサーバや掲示板の管理者等の責任の及ぶ範囲

サーバ管理者は、学内的にも学外的にもそれなりの責任と義務を負うことを十分承知して運用すること。
特に「プロバイダ責任制限法」は、ウェブサイトや掲示板の管理者も「特定電気通信役務提供者」と見している。よってこれらの管理を行う者は、同法上の責任と義務を負うので十分に注意すること。

解説：「プロバイダ責任制限法」は、「特定電気通信役務提供者」に対して、損害賠償責任の制限と発信者情報の開示について定めたものである。ウェブサイトや掲示板の管理者も「特定電気通信役務提供者」とみなしている。

8.1 権利侵害があった場合

本学では、自己の管理するサーバやネットワーク内で権利侵害があることが明らかである場合、管理者は、別途定める書式を用い、可及的速やかにその情報を削除させるか、あるいは削除するものとする。

解説：8.1 は「このような記述もあり得る」というサンプル規定である。
自らが管理するウェブ上で、他人の書き込みにより権利侵害（人権侵害や知的財産権侵害）が行われていることを知った場合、管理者は削除義務を負うとされ、削除義務があるにもかかわらず、ただちに削除しなければ、（プロバイダ責

任制限法以前から）権利者／被害者に対して損害賠償責任を負う可能性がある。ただし、「プロバイダ責任制限法の手順に従って権利侵害情報を削除すれば、発信者への損害賠償責任を免れる」とされている。

⇒また、プロバイダ責任制限法ガイドライン等協議会の各種ガイドラインの手続きに準拠する場合には、裁判所も権利者／被害者に対する責任を認めないことが期待できる。詳細は、以下を参照のこと。
http://www.telesa.or.jp/consortium/provider/index.htm

（警告文の例）

警　告

年　　月　　日

＿＿＿＿＿＿＿＿＿＿＿＿殿

A大学○○学部　部局総括責任者
山田　太郎

あなたの開設するウェブページに掲載されている下記の情報の流通により他者への権利侵害が発生していると認められ、加えて被害者自らが被害の回復予防を図ることが諸般の事情を総合考慮して困難と認められますので、直ちに当該情報の送信を防止する措置を講じて下さい。

○○日までに送信防止措置がなされない場合、こちら側でコンテンツを削除させていただきます。

掲載されている場所：　※URL や情報の特定に必要な情報を記載
掲載されている情報：　※権利侵害の行われている情報の種類などを記載
プライバシーに関わる情報の掲載
他人の知的財産権の侵害など

なお、上記「プロバイダ責任制限法ガイドライン等協議会」のガイドラインのページにも各種文例があるので参照のこと。

8.2 発信者情報の開示

本学では、権利者（あるいは、権利者と称する者）または捜査機関から、発信者情報の開示請求があった場合は、法的拘束力のある書類（裁判所の令状など）がない限り、これに応じないこととする。

解説：8.2 は「このような記述もあり得る」というサンプル規定である。
自らが管理するウェブ上で「権利侵害が行われているので発信者情報を開示しろ」との要求が権利者を名乗る人物からあったが、権利侵害の事実が明白とは言えない場合、すぐに発信者情報を開示する義務は無い。
捜査機関からの問い合わせに関しても同様であり、令状を伴わない捜査協力依頼の段階ではまだ情報を開示する義務はない。もちろん、この段階で情報開示をすることを、大学としての方針としても構わない。重要なことは、どのようなどのような場合においても、発信者情報開示の際の基準を同一にしておき、振らさないことである。

⇒その他、発信者情報開示の判断に当たっては、上記プロバイダ責任制限法ガイドライン等協議会の発信者情報開示関係ガイドライン（8.1 解説）を参照のこと。

9. 本ガイドラインに関する相談窓口

ウェブ管理者は、緊急時の対応および本書の内容を超えた対応が必要とされる場合には、部局総括責任者に報告・相談し、指示を受けること。

解説：研究室レベルのウェブサーバの場合、その管理者が学生や大学院生である場合もある。そのため、彼らが直接判断することが困難な場合に直接相談できる窓口を作っておく必要がある。

A3205 利用者パスワードガイドライン

1. 本ガイドラインの目的

本ガイドラインは、本学情報システムのアカウントを利用する際のパスワードに関し、利用者が予め理解しておくべき事項を示すことを目的とする。

2. パスワードに係る全般的な注意事項

2.1 初期パスワードの変更

利用者は、アカウントが発行されたら速やかに初期パスワードを自己のものに変更すること。初期パスワードのまま情報システムの利用を継続してはならない。

2.2 パスワードに使用する文字列

利用者が設定するパスワード文字列は、以下の条件を全て満足するものでなければならない。

- 最低限６文字以上の長さを持つ。
- 以下ア～エの文字集合から各最低１文字以上を含む。
  - ア）英大文字（A～Z）
  - イ）英小文字（a～z）
  - ウ）数字（0～9）
  - エ）システムで使用可能な特殊文字（@!#$%&=-+*/.,:;[]|）

また、以下の文字列は容易に推察可能であるため、パスワードとして設定してはならない。

- 利用者のアカウント情報から容易に推測できる文字列（名前、ユーザ ID 等）
- 上記を並べ替えたもの、上記に数字や記号を追加したもの
- 辞書の見出し語
- 著名人の名前等

2.3 パスワードの定期的な変更

利用者は、アカウント発行者（全学アカウントに関しては情報メディアセンター、個別システムについてはシステム管理者）からパスワードの変更の指示を受けた場合には遅滞なくパスワードを変更しなければならない。変更後のパスワードは変更前のパスワードと類似のものであってはならない。

解説：パスワード漏えいによる不正利用やパスワード破りによるリスクを減らす手段として、パスワードの定期的な変更には一定の効果があるという考えもある。パスワードの有効期間やパスワード文字列構成検査および世代管理が可能なシステムでは、パスワードポリシーを強制することも可能である。一方で、強固なパスワードを設定し、変更しない方がよいという考え方もある。ここでは、

後者の考えを基本に、パスワード漏えいによる不正利用の可能性をシステム管理者が検知したり、一般的なパスワード検査ツールで容易に解読されるようなパスワードの利用者を発見した場合に、システム管理者がパスワードの変更を要求するというモデルを想定している。

2.4 パスワードの管理

利用者は、自己のパスワードを厳重に管理しなければならない。パスワードをメモしたり、端末にそのメモを貼り付けたりしてはならない。利用者は、他の者にパスワードを教えたり、不注意でパスワードが他の者に知られたりしてしまうことがないよう最大限の注意を払わなければならない。

2.5 パスワードの詐取の可能性のある場所での利用の禁止

パスワードやアカウントを詐取される可能性があるので、学外のインターネットカフェなどに設置されているような不特定多数の人が操作（利用）可能な端末を用いての学内情報システムへのアクセスを行ってはならない。

2.6 パスワードによるロックの励行

利用者は、使用中のコンピュータにログインしたまま離席する場合は、他者が画面を閲覧したり操作することができないよう、画面のロック操作を行わなければならない。

3. パスワードに関する各種手続き

解説：本項で扱う事項は実施手順等で別途定めておくべき内容であるが、利用者の便宜を図るためにガイドラインにおいて手続きを説明している。

3.1 パスワードを失念した場合

利用者がパスワードを忘れた場合には、発行部局に対して、所定の様式で、身分証（学生証もしくは職員証等）を持参し、パスワードのリセットを申請しなければならない。パスワードのリセットを受けた場合には、速やかに新しいパスワードに変更すること。

3.2 パスワードの事故の報告

利用者は、アカウントを他者に使用され又はその危険が発生した場合には、直ちに全学実施責任者にその旨を報告しなければならない。

A3211 学外情報セキュリティ水準低下防止手順

1. 目的

本学は、本学内の情報セキュリティ水準の低下を招くような行為を防止するだけでなく、本学外の情報セキュリティ水準の低下を招くような行為をしないことは当然である。また、本学外のセキュリティ水準を低下させることは、本学を取り巻く情報セキュリティ環境を悪化させることにもなる。

本手順は、情報セキュリティ対策の適所において講ずべき措置を定め、もって本学外の情報セキュリティ水準の低下を招く行為を防止することを目的とする。

2. 適用範囲

「A1001 情報システム運用基本規程」と同じとする。

3. 本学外の情報セキュリティ水準の低下を招く行為の防止

3.1 措置の整備

(1) 全学実施責任者は、本学外の情報セキュリティ水準の低下を招く行為を防止するための具体的措置を例示すること。なお、例示にあたっては、インターネット、PC、ソフトウェア等の環境の変化、技術の進歩、安全に関する意識の向上等によって変わることに留意すること。

(2) 部局総括責任者は、所管する部局において、本学外の情報セキュリティ水準の低下を招く行為を防止するために、部局技術責任者に対して、防止に必要な措置を検討し、実施手順書等に盛り込むように指示すること。

(3) 部局技術責任者は、所管する情報システムにおいて、全学実施責任者が例示した具体的措置をもとにして、本学外の情報セキュリティ水準の低下を招く行為を防止するための措置を検討し、実施手順書等に盛り込むこと。

3.2 措置の実施

本学情報システムを運用・管理・利用する者は、実施手順書等に従い、本学外の情報セキュリティ水準の低下を招かないように行動すること。

付録： 本学外の情報セキュリティ水準の低下を招く行為を防止するための措置の例示

部局技術責任者は、所管する情報システムにとってリスクと感じる本学外の者による行為は、本学から本学外に対しても行わないことが望ましい。このような視点から、本学外の情報セキュリティ水準の低下を招く行為を防止するための措置として、以下のような注意事項が想定される。

(1) 提供する電磁的記録の内容、形式等による影響

本学外へ電磁的記録を提供する際に、当該電磁的記録の内容、形式等によって、本学外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

- 提供する電磁的記録が不正プログラムを含まないこと。
- 実行プログラムの形式以外に電磁的記録を提供する手段がない限り、実行プログラムの形式で電磁的記録を提供しないこと。
- 提供する電磁的記録に改ざん等がないことを知りえる機会を、提供先の者に与えること。
- 提供先の者が警告等に慣れて無視しないように、提供する電磁的記録の参照時に警告等が出ないようにすること。

具体的には以下のような事項が想定される。

- 本学のウェブサイト、電子メールの添付ファイル、外部記録媒体等でファイルを提供する場合には、アンチウイルスソフトウェア等を利用して不正プログラムの有無を確認すること。
  - ○不正プログラムに感染したファイルを本学外に送らないようにするため。
- 本学のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利用して圧縮したファイルを提供する場合には、自己解凍形式を利用しないこと。
  - ○自己解凍形式で圧縮されたファイルは実行可能形式のファイルとなり、当該ファイルを入手した者に不正プログラムの可能性を不必要に想起させ、解凍する際に安全性の確認が必要になるため。
- 本学のウェブサイトにおいて、電子署名されていない実行モジュール（Java®アプレット、ActiveX®コントロール等）を提供しないこと。
  - ○実行モジュールを悪用することで、不正プログラムの感染、情報の漏えい等の被害が発生する可能性がある。そのような悪意のある実行モジュールではなく、安全な実行モジュールであることを正しい電子署名により保証するため。
- 本学のウェブサイトにおいて、実行モジュールを電子署名して提供する場合に、

有効でない証明書を利用しないこと。

○安全な実行モジュールであることを保証できないだけでなく、当該モジュールを入手した者が、有効でないことを示す警告等に慣れてしまい、他の警告等に対しても危険性を感じとれなくなる可能性があるため。

(2) 提供する電磁的記録を処理することによる直接的な影響

本学外へ提供した電磁的記録を提供先の者が参照等する際に、利用する端末等の設定変更を要求することによって、本学外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

・本学外の者が利用している端末のオペレーティングシステム、ソフトウェア等のセキュリティ設定変更を不用意に指示しないこと。

・やむを得ずセキュリティ設定変更を指示する場合には、後に元の設定に戻す方法を、参照しやすい形式で紹介すること。

具体的には以下のような事項が想定される。

・本学のウェブサイトのコンテンツを参照するために、訪問者のブラウザのセキュリティ設定を変更するよう要求しないこと。

○ウェブウザのセキュリティ設定の変更要求に従った結果、ブラウザのセキュリティレベルが低下し、悪意を持ったウェブサイト等を参照した際に不正プログラムに感染するおそれがあるため。

・本学のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利用して提供するファイルを参照するために、安全性の確認が困難なライセンスフリーの専用ソフトウェア等のインストールを要求しないこと。

○ソフトウェアのインストールにより、利用可能なソフトウェアの制限の変更又は違反を生じさせるため。また、当該ソフトウェアに脆弱性が発見された場合に、脆弱性を悪用した攻撃の被害にあうおそれがあるため。

(3) 提供する電磁的記録を処理することによる間接的な影響

本学外へ提供した電磁的記録を提供先の者が参照等する際に、明示的に利用する端末等の設定変更を要求するわけでないが、電磁的記録を参照できる設定であることを想定することは、暗黙に設定変更を指示したと考えられる。暗黙に指示した設定変更により、本学外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

・本学外の者にセキュリティ上の問題を生じさせるような設定変更を暗黙に指示する電磁的記録を不用意に提供しないこと。

・やむを得ず当該電磁的記録を提供する場合には、後に元の設定に戻す方法を、参

照しやすい形式で紹介すること。

具体的には以下のような事項が想定される。

・本学のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利用して、マクロ等を含んだファイルを提供しないこと。

○マクロ等を含んだファイルを提供することは、提供先の者に対してセキュリティ設定の変更を明示的に指示することではないが、当該提供先の者がマクロを実行できるような設定にしていることを想定した行為であり、暗黙に設定変更を指示したことと考えることができる。マクロ等には、不正プログラムに感染する問題があり、暗黙に指示した設定変更により、提供先の者に当該問題が生じるおそれがあると考えられるため。

・HTML形式での電子メールを送信しないこと。

○HTML形式の電子メールを送信することは、受信者に対してセキュリティ設定の変更を明示的に指示することではないが、当該受信者がHTMLを判読できるような設定にしていることを想定した行為であり、暗黙に設定変更を指示したことと考えることができる。HTML形式の電子メールには、フィッシング（本物に似せた偽のウェブサイトへ誘導し、入力情報を詐取する手法）、ウェブビーコン（メールを開いた事実、日時等を確認する手法）等のセキュリティ上の問題があり、暗黙に指示した設定変更により、受信者に当該問題が生じるおそれがあると考えられるため。

A3212 自己点検の考え方と実務への準備に関する解説書

1. 本解説書の目的

国立大学においては、「A2501 事務情報セキュリティ対策基準」に基づき、自己点検を実施することが求められている。しかしながら、自己点検については、これまで各大学に取り入れられていないものであることから、その計画策定及び準備は入念に行う必要がある。

本解説書は、自己点検の考え方と実務への準備を中心に、関係する遵守事項を詳細に解説するとともに、年度計画や実施手順書等の雛形を示したものであり、もって自己点検の適切な実施に資することを目的とする。

2. 自己点検の概要

2.1 自己点検の趣旨

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

［「A2501 事務情報セキュリティ対策基準」1.2.3.1 情報セキュリティ対策の自己点検より引用］

2.2 自己点検の基本的な考え方

自己点検は、各遵守事項の実施主体となる本人が行うべき情報セキュリティ対策を適切に実施しているかを点検するものである。このため、「実施主体による自己点検」が自己点検の中心として位置付けられるが、その進捗状況の管理や集計をする体制を構築することが重要となる。したがって、事務情報セキュリティ対策基準 1.2.3.1 項に示す自己点検における実施及び確認・評価は、本人による点検及び部局総括責任者等による進捗管理・集計、そして全学総括責任者によるとりまとめの 3 つの過程により行う。（図１参照）

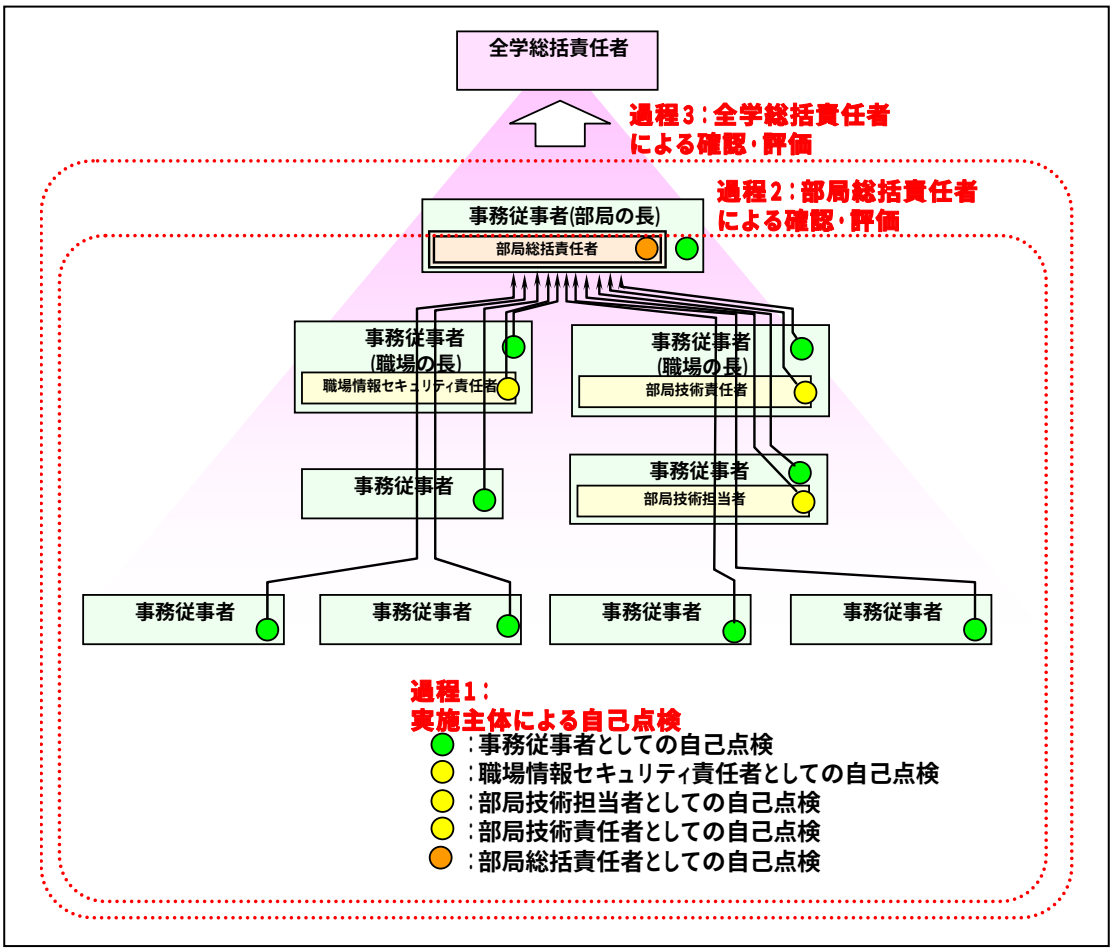


図 1. 自己点検の実施及び確認・評価における３つの過程

(1) 過程１：実施主体による自己点検

「実施主体による自己点検」とは、情報セキュリティ関係規程に定められたセキュリティ対策条項における主語、すなわちその対策の実施主体本人による自己点検である。例えば、情報セキュリティ関係規程において「すべての事務従事者は、・・・すること」と記載がある場合の実施主体は、「すべての事務従事者」となり、「職場情報セキュリティ責任者（又は上司）、・・・すること」と記載がある場合のそれは、「職場情報セキュリティ責任者（又は上司）」となる。

そのため、部局総括責任者、部局技術責任者、部局技術担当者、職場情報セキュリティ責任者（又は上司）その他情報セキュリティ管理の職務にある者は、当該職務者としての自己点検に加えて、事務従事者（利用者）としての自己点検の両方が求められることになる。また、複数の情報システムを取り扱う場合には、それぞれの情報セキュリティの管理単位に応じて、自己点検が実施されることとなる。すなわち、一人の事務従事者に注目した場合、取り扱う情報システムごと、及びその役割（利用者、責任者）ごとに自己点検が実施されることとなる。

なお、実施主体による回答結果は、部局総括責任者があらかじめ指定する者を経由して集約する。

(2) **過程２：部局総括責任者による確認・評価**

「部局総括責任者による確認・評価」とは、所管する単位における情報セキュリティ対策全体を通して、実施主体による自己点検が適切に行われていることについて進捗の状況を確認し、その本人による自己点検結果の記載内容に不備がないかを評価することである。すなわち、実施主体から提出された回答結果を閲覧し、記入ミスや記入漏れの有無の確認をした上で、全実施主体が計画した期限内に自己点検を完了するための進捗状況（自己点検実施率）を管理する。必要に応じて、実施主体に対して進捗状況を確認したり、予定より遅れていれば実施の催促をする。実施主体による自己点検が終了したら、数値評価（事務情報セキュリティ対策基準準拠率や要改善対策数/対策実施数など）による集計を行う。また、必要に応じて、以前実施された自己点検方法における指摘事項が適切に改善されていること等を評価する。その上で、所管する単位における確認・評価の結果を報告書として全学総括責任者へ提出する。

なお、作業の効率性や自己点検結果の正確性を向上させることを目的として、確認・評価に係る作業の一部を、大学事務の管理責任を有する者や、情報セキュリティ対策の管理責任を有する者（職場情報セキュリティ責任者、部局技術責任者、部局技術担当者等）に委任してもよい。

(3) **過程３：全学総括責任者による確認・評価**

「全学総括責任者による確認・評価」とは、部局総括責任者からの自己点検結果の報告書の提出状況などを踏まえ、全学総括責任者が大学全体での自己点検が適切に行われていることを確認・評価することである。

2.3 自己点検に係る作業の全体像

自己点検に係る作業は、前節で示した 3 つの過程（実施及び確認・評価）を核とし、「導入」、「実施指示」及び「改善」を含めた以下の作業から構成される。

(1) **実施及び確認・評価の前段階である「導入」においては、全学総括責任者が策定した年度自己点検計画を踏まえて各部局総括責任者は、自らの所管する範囲の情報システムに係る自己点検を実施するために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。**
(2) **「実施指示」においては、上記の導入準備が完了した後、部局総括責任者が自己点検票及び自己点検の実施手順（提出先、提出期限などを含む。）を提示し、自己点検の実施を指示する。**
(3) **「実施及び確認・評価」においては、前述のとおり、まず実施主体による自己点検が行われ、その結果を部局総括責任者が確認・評価し、さらにその結果を全学総括責任者が確認・評価する。**
(4) **自己点検は、本人による対策実施を自己点検することが目的であるが、事務情報セキュリティ対策基準** 1.2.3.1 (5) **「自己点検に基づく改善」においては、自己点検で気付いた問題点ですぐに改善できることがあれば、自己点検結果の集計や監査結果を必ず**

しも待たなくとも、適宜改善することが望ましいことを示している。
「改善」においては、事務従事者自身による自己改善と、全学総括責任者による改善指示に大別される。前者は、ボトムアップ的なものであり、自己点検の結果に基づいて自己の権限の範囲で改善できると判断した事項へ対処するものである。後者は、トップダウン的なものであり、全学総括責任者が情報システムの自己点検結果を評価し、必要があると判断した場合には部局総括責任者に改善を指示するものである。

実施及び確認・評価を含め、自己点検に係る作業の全体像を図２に示す。

		導入		実施指示	実施及び確認・評価			改善	
					過程 1	過程 2	過程 3		
		計画	準備		実施主体による自己点検	部局総括責任者による確認・評価	全学総括責任者による確認・評価	自己改善	改善指示
職位・役割	全学総括責任者	年度計画の策定					自己点検の確認・評価		改善指示
	部局総括責任者(※1)		自己点検票及び実施手順の整備	実施の指示		自己点検の確認・評価		自己の権限の範囲で改善	
	事務従事者（実施主体）(※2)				自己点検の実施			自己の権限の範囲で改善	
事務情報セキュリティ対策基準における項番		1.2.3.1 (1)(a)	1.2.3.1 (2)(a)	1.2.3.1 (3)(a)	1.2.3.1 (3)(b)	1.2.3.1 (4)(a)	1.2.3.1 (4)(b)	1.2.3.1 (5)(a)	1.2.3.1 (5)(b)
本手引書における解説		6 章	7 章	8 章		9 章		10 章	

※１：ここで、部局総括責任者とは、自己点検の確認・評価を実施する者としての部局総括責任者を指す。

※２：ここで、事務従事者（実施主体）とは、実施主体としての部局総括責任者、部局技術責任者、部局技術担当者、職場情報セキュリティ責任者等を含む。

図２. 自己点検に係る作業の全体像

自己点検と監査の違いとは？

自己点検は、事務従事者自らがその情報セキュリティ対策を実施しているかを点検するものである。一方、監査は、情報セキュリティ対策の実施者とは独立性を有した者が客観性、専門性を持って監査を行うものである。

また、自己点検は、原則としてすべての情報セキュリティ対策を対象とするものである。一方、監査は、実際の運用が情報セキュリティ関係規程に準拠しているか否かを監査するに当たっては、すべての情報セキュリティ対策を直接監査することが困難なこともある。そのため、自己点検の結果等を踏まえて、自己点検が適切に実施されているかをサンプリング調査によって確認することが可能な場合もある。

以下に、自己点検と監査との主な相違点を示す。

	自己点検	監査
実施者	情報セキュリティ対策の実施主体自ら実施する。	情報セキュリティ対策の実施者とは独立性を有した者が実施する。
報告先	自己点検の実施者は、回答結果を部局総括責任者へ提出する。部局総括責任者は、その確認・評価の結果を全学総括責任者へ提出する。	監査責任者は、監査調書に基づき監査報告書を作成し、全学総括責任者へ提出する。
実施頻度	遵守事項に応じて、日常的に実施されるべきものから、年一度程度の実施でよいものまで様々である。	主たる監査は年度末に実施されるが、自己点検に応じて随時するという実施計画を策定しても構わない。
対象の選定	実施主体が自ら行うものであり、原則として、すべての実施主体がすべての対策項目について実施する。	監査対象をサンプリングし、母集団の統計的性質を推定することができる場合もある。
評価の観点	実際の運用が情報セキュリティ関係規程を遵守しているかを点検する。(遵守性の観点)	実際の運用が情報セキュリティ関係規程を遵守しているかという観点のほか、それら関係規程が事務情報セキュリティ対策基準に準拠しているか、作成された実施手順が関係規程に準拠しているかについても監査を行う。(準拠性と遵守性の観点)
評価の手法	情報セキュリティ対策の実施主体によって自己申告された回答を原票として、それを評価する。	規定文書等の確認を行って準拠性を評価し、また、被監査部門への質問・査閲・観察・点検により遵守性を評価する。
改善プロセス	全学総括責任者から改善指示があった場合の対処のほか、事務従事者の自己の権限の範囲で改善できると判断した事項は自ら対処を行う。	全学総括責任者から改善指示があった場合には、部局総括責任者は対応計画を作成し、報告する。

図 3. 自己点検と監査

自己点検結果の取扱い

全学総括責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には部局総括責任者に改善の指示を出すことが義務付けられている[事務情報セキュリティ対策基準の 1.2.3.1 (5)(b)]。なお、自己点検の結果は、監査を実施するに当たって、すべての事務従事者における情報セキュリティ対策の実態を把握するための重要な資料となるだけでなく、監査の方向性や重点領域を定める際の参考ともなる。

3. 自己点検に関する年度計画の策定　（ 1.2.3.1 (1) ）

自己点検は、各部局総括責任者の責任において、所管する単位で実施されるものである。全学総括責任者は、それぞれの情報システムにおける自己点検を効率的かつ整合的に実施するため、大学全体としての年度自己点検計画を定める必要がある。

> **事務情報セキュリティ対策基準　　1.2.3.1 情報セキュリティ対策の自己点検**
> (1) (a) 全学総括責任者は、年度自己点検計画を策定し、全学総括責任者の承認を得ること。
> 【基本遵守事項】

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

3.1 「年度自己点検計画」の位置付けと策定目的

(1) 「年度自己点検計画」は、各大学における自己点検を適切に実施するため、中長期的な視点から当該年度のテーマを定めた上で、様々な考慮事項、制約事項を勘案し、実施スケジュール（実施頻度及び実施時期）、確認及び評価の方法（委任する場合の責任範囲含む。）、実施項目の選択等を定めたものである。なお、自己点検はすべての実施主体が行うものであることから、「年度自己点検計画」については、事務従事者がこれを共有する必要がある。
(2) 「年度自己点検計画」は、全学総括責任者によって策定される。この「年度自己点検計画」に基づき、部局総括責任者は、自身の管理する情報セキュリティ対策の単位における自己点検について詳細スケジュールを策定し、自己点検票及び自己点検の実施手順を整備する。

3.2 「年度自己点検計画」を策定する際の考慮事項と制約事項

(1) 大学における情報セキュリティ関係規程の整備状況及びその遵守状況を踏まえること。特に、新たなセキュリティ対策を施す場合には、その施行に至るまでの準備期間や移行期間を考慮して計画することが求められる。
(2) 自己点検の実施に関与する特定の組織、特定の役職、特定の事務従事者に負荷が集中しないように負荷を平滑化すること。例えば、対象システムをいくつかの機能に分割した上で順次実施する、実施対象者をいくつかのグループに分割した上で順次実施する、自己点検一度当たりの質問数を分割する等の配慮が必要である。
(3) 実施時期の検討に当たっては、他の事務処理へ配慮すること。例えば、年度末や予算編成期などの繁忙期を避ける等の配慮が必要である。

(4) 実施時期の検討に当たっては、「自己点検の随時実施」を検討することが重要である。
一般的には、実施者が一定期間に行った遵守事項の実施状況を確認するため、年度末などの特定の時期に、自己点検の対象期間に係る実施状況について自己点検を行うことになる。例えば、事務情報セキュリティ対策基準の第 1.3 部にある「情報の作成又は入手時における格付けと取扱制限の決定」などのように必要の都度、実施者が判断するものが該当する。
しかしながら、事務情報セキュリティ対策基準の第 1.4 部及び第 1.5 部の遵守事項並びに第 2 編の一部の遵守事項については、情報システムのライフサイクルに沿って構成してあることから、それら遵守事項の中には、情報システムのライフサイクルの各段階において、１度しか実施しないものもある。例えば、事務情報セキュリティ対策基準の第 2.1 部にある「アクセス制御の必要性の有無の検討の実施」などのように情報システムの設計時に実施する事項が該当する。
このような事項については、その実施後、一定期間を経過してから自己点検をするよりも、実施後、速やかに自己点検を済ませてしまう方が、実施者にとっての負担が少ないばかりではなく、自己点検結果の精度も高いものとなる。例えば、情報システムの設計時に注意すべき遵守事項について、設計作業をする傍らに自己点検票を用意して作業チェックリストのように用いることにより、作業とともに自己点検を完了することができる。この結果、事後に時間が経過してから自己点検をするよりも、事実関係に係る誤記入が防げることに加え、失念により遵守事項の実施を怠るということも防ぐことができる。
このため、情報システム対策に関係する遵守事項のうち、その都度に済ませる対策については、それを実施する際に自己点検票を作業チェックリストのように用いることで、作業時に自己点検を随時済ませていくことが効果的である。また、期間を通じての対策も、それが特定期間であれば、その期間終了後に速やかに自己点検をすることが効果的である。各大学における情報セキュリティ対策基準に基づく自己点検作業のうち、上記の趣旨に該当するものについては、随時の実施をすることが効率及び精度を向上させることができる。
(5) 自己点検結果に基づく改善活動についても考慮した実施スケジュールとすること。

年度自己点検計画の雛形を付録１に示す。

4. 自己点検の実施に関する準備 （ 1.2.3.1 (2) ）

自己点検は、情報セキュリティの管理単位ごとに、それに係るすべての事務従事者が実施するものであること、事務従事者の役割によって実施内容に追加があること、実施主体による回答結果を部局総括責任者へ提出するに当たっては複数の関係者を経由する可能性があること、部局総括責任者による確認・評価が別の者に委任される可能性があること等をかんがみ、自己点検票及び自己点検の実施手順を整備することが求められる。

> **事務情報セキュリティ対策基準　　1.2.3.1 情報セキュリティ対策の自己点検**
> (2) (a) 部局総括責任者は、事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。
> 【基本遵守事項】

各事務従事者が自己点検を実施するに当たっては、各自の業務における情報の取扱方法や、実施すべき情報セキュリティ対策上の役割が異なるため、それぞれの職務内容に即した自己点検票が必要となる。そのため、部局総括責任者は、事務従事者ごとの自己点検票を作成するとともに、自己点検の正確性を高めるために詳細な実施手順を準備することを求める事項である [解説書より抜粋]。

自己点検票及び自己点検の実施手順を整備するには、以下に示す手順(Step A から Step G)に従って実施すると効率的である。

- Step A : **情報セキュリティ関係規程の整備**　(4.1)
- Step B : **自己点検項目の整備**　(4.2)
- Step C : **集約ルートの検討**　(4.3)
- Step D : **確認・評価の委任**　(4.4)
- Step E : **自己点検票への展開**　(4.5)
- Step F : **事務従事者ごとに再構成**　(4.6)
- Step G : **実施環境の整備**　(4.7)

また、これらの準備は、部局総括責任者が、自身の所管する単位について行うものであるが、大学において共通的に準備することが効率的と思われる事務については、全学総括責任者や他の部局総括責任者と相談の上で準備するとよい。

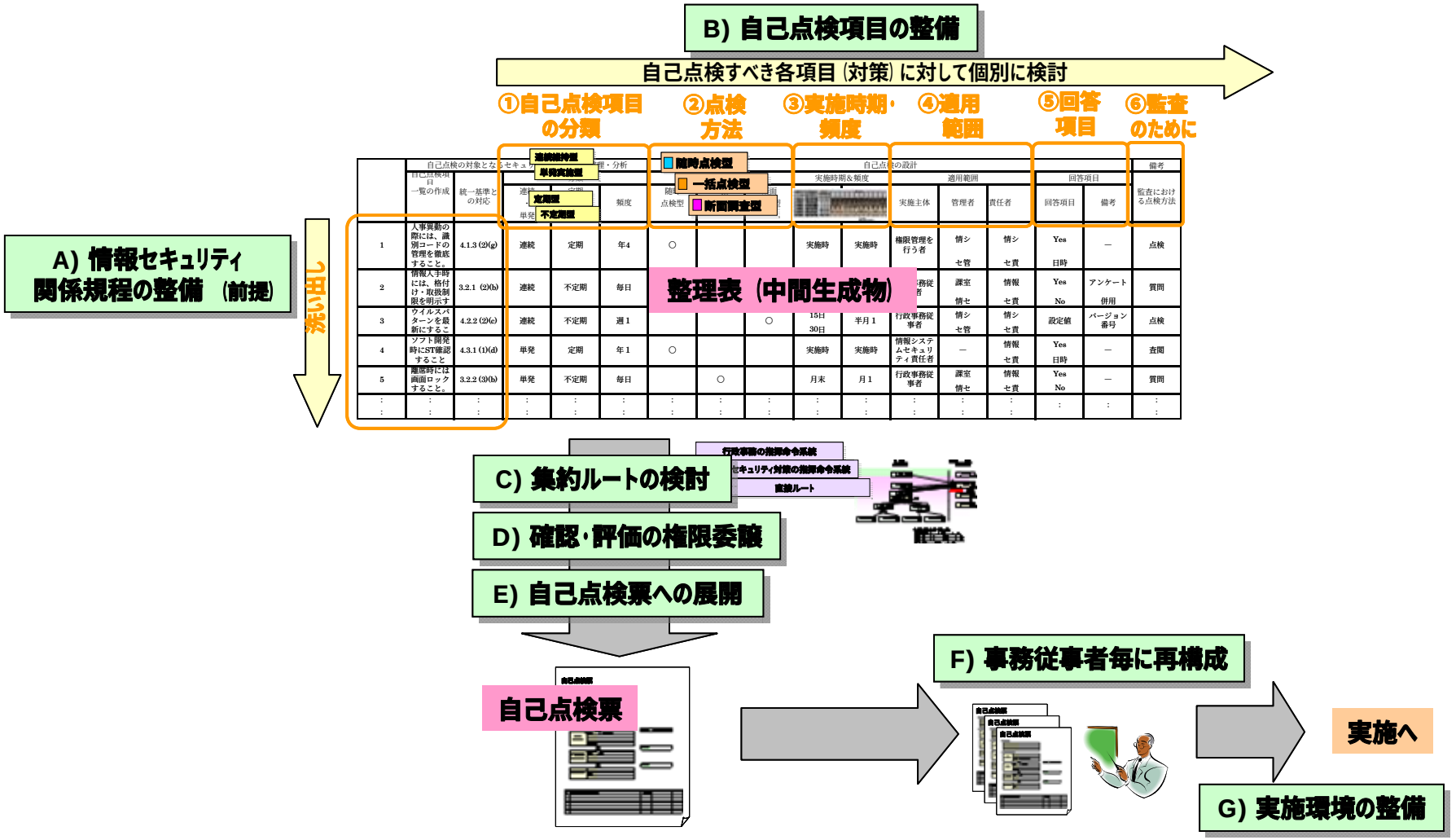


図 4. 自己点検実施の準備の全体像

4.1 情報セキュリティ関係規程の整備 (Step A)

自己点検は、各大学で定めた情報セキュリティ関係規程に従った運用が行われていることを確認するものである。そのため、部局総括責任者は、自己点検票及び自己点検の実施手順を整備するに先立ち、まずは実施主体（事務従事者、部局技術責任者、部局技術担当者、職場情報セキュリティ責任者、部局総括責任者等）が実施すべき情報セキュリティ対策を明確にした情報セキュリティ関係規程の整備が求められる。

(1) **まず、「高等教育機関の情報セキュリティ対策のためのサンプル規程集」の事務情報セキュリティ対策基準を各大学の事務情報セキュリティ対策基準へ反映させる**(Step A-1)**ことが必要である。事務情報セキュリティ対策基準への反映については、策定時に実施されているところであるが、今後の事務情報セキュリティ対策基準の改訂や、情報セキュリティを取り巻く環境の変化、対策の改善などに応じて、今後も継続的に事務情報セキュリティ対策基準を見直す必要がある。なお、大学全体のセキュリティポリシーである事務情報セキュリティ対策基準の見直しに当たって、部局総括責任者がその責務を負っていない場合には、全学総括責任者と相談の上、適宜対応すること。**

(2) **次に、必要に応じて実施手順を整備する**(Step A-2)**ことが必要である。部局総括責任者は、事務情報セキュリティ対策基準の導入に当たって実施手順が必要であると判断した場合には、これを整備することが求められる。当該情報システムにセキュリティ対策を講ずるための実施手順は、誰が（実施主体）何をすべきか、自己点検において評価可能な程度まで具体的に記述されている必要がある。**

(3) **つづいて、自己点検項目一覧を作成する**(Step A-3)**ことが必要である。情報セキュリティ関係規程を元に、当該情報システムの自己点検を行う項目を選別し、一覧を作成する。**

(4) **さらに、事務情報セキュリティ対策基準との対応関係を明確化する**(Step A-4)**ことが必要である。自己点検項目一覧に記載されたそれぞれの項目に対して、それが事務情報セキュリティ対策基準のどの遵守事項に対応するものであるかを明らかにするため、対応関係を明確化する。これは、自己点検の実施に直接必要となるものではないが、後に自己点検結果を分析・評価した場合に有用であるとともに、事務情報セキュリティ対策基準に対する運用状況等の報告を求められた場合に有用となる情報である。**

4.2 自己点検項目の整備 (Step B)

事務従事者が業務において遵守すべき情報セキュリティ関係規程の項目が記載された自己点検票を作成することが必要となる。その手順を Step B から Step E において説明する。

効果的かつ効率的な自己点検を実施するためには、情報セキュリティ関係規程に定められている情報セキュリティ対策の特質を反映した自己点検票の作成が必要となる。Step B では情報セキュリティ対策の特質を検討・分類し、自己点検票を作成するための整理表を作成するところまでを説明する。

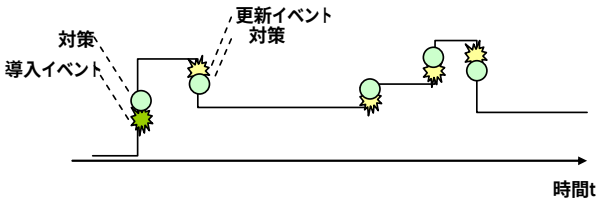
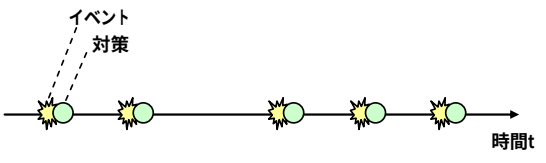
情報セキュリティ対策の特質を検討する際には、次の５つの観点から行うとよい。

(1) 自己点検項目の分類	セキュリティ対策を実施するタイミングで自己点検をするか定期的に自己点検を実施するかを決定するために、情報セキュリティ対策の点検項目の特性を、「連続維持型」か「単発実施型」か、対策実施時期を「定期型」か「不定期型」かに分類する。
(2) 点検方法	情報セキュリティ対策の特性及び実施時期に応じた点検方法として、点検方法を「随時点検型」、「一括点検型」又は「断面調査型」に分類する。
(3) 実施時期・頻度	セキュリティ対策の重要性や点検方法に応じて実施時期及び頻度を決める。
(4) 適用範囲	セキュリティ対策の点検実施者を決める。
(5) 回答項目	回答項目（実施したか否か）、設定値などを決める。

(1) **自己点検項目の分類** (Step B-1)

自己点検における点検方法を検討するに当たり、情報セキュリティ対策の特質を以下の観点から分類するとよい。

- **対策された状態の維持性による分類**

タイプ	概説
連続維持型	**実施されたセキュリティ対策について、それ以降もその対策状態が連続的に維持されるもの。すなわち、初期導入した後、その対策状態が保持され、セキュリティ対策の更新が必要と思われる事象の発生に応じて、対策状況の更新が行われる対策。** **例えば、以下の対策が挙げられる。** **・責任者、管理者の設置及び担当変更** **・ウイルスパターン定義ファイルの更新** **・情報入手時の格付け/取扱制限の明示** **イメージ図** 
単発実施型	**実施されたセキュリティ対策について、それ以降もその対策状態が必ずしも継続されないもの。すなわち、対策の初期導入を伴わず、セキュリティ対策が必要と思われる事象の発生に応じて、その都度実施される対策。** **例えば、以下の対策が挙げられる。** **・各種の報告や申請処理** **・各種の確認処理** **（例：公開時の機密度チェック）** **・離席時の画面ロック** **イメージ図** 

- 対策時期の定期・予測可能 / 不定期・予測困難　による分類

タイプ	概説
定期型 （時期予測可能型を含む）	セキュリティ対策が必要と思われる事象が定期的に発生する、又はその発生時期が予測可能なもの。 例えば、以下の対策が挙げられる。 ・識別コードの管理（人事異動反映） ・定期報告、年度計画策定 ・毎日帰宅時に書類の施錠保管 ・ソフトウェア開発における ST 確認
不定期型 （時期予測困難型を含む）	セキュリティ対策が必要と思われる事象が不定期的に発生する、又はその発生時期が予測困難なもの。 例えば、以下の対策が挙げられる。 ・ウイルスパターン定義ファイルの更新 ・情報入手時の格付け/取扱制限の明示 ・障害報告、例外申請処理

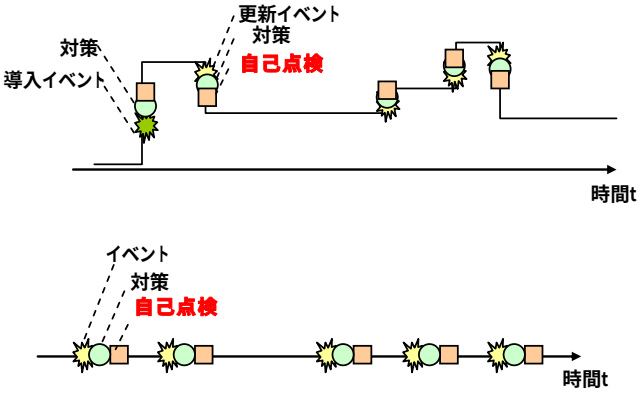
なお、定期型/不定期型ともに、対策実施の頻度は、自己点検の実施時期及び実施頻度を検討する上で重要な要素である。以下に「頻度」及び「該当する遵守事項」の分類例を示す。

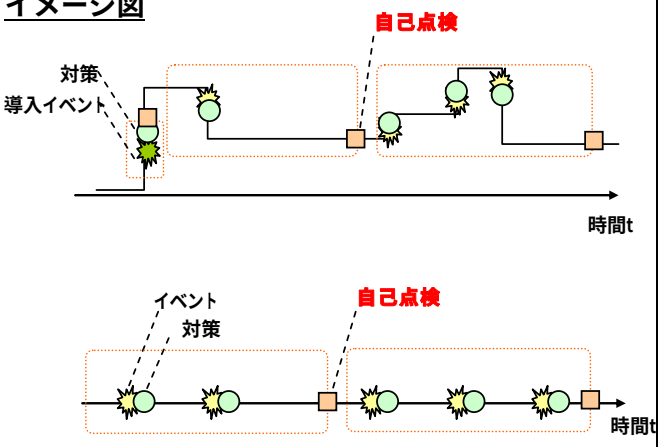
頻度	該当する遵守事項
年に一回 程度	・年度計画の策定 ・責任者、管理者の設置及び担当変更 ・ソフトウェア開発における ST 確認
6 ヶ月に一回 程度	・定期報告（上期・下期）
3 ヶ月に一回 程度	・識別コードの管理（人事異動反映） ・パスワードの変更
月に一回 程度	・Microsoft® Windows® Update
半月に一回 程度	・機密性 3 情報を移送する場合の許可申請
週に一回 程度	・ウイルスパターン定義ファイルの更新
一日に一回 程度	・毎日帰宅時に書類の施錠保管
一日に数回 程度	・離席時の画面ロック
頻度不明	・障害報告、例外申請処理

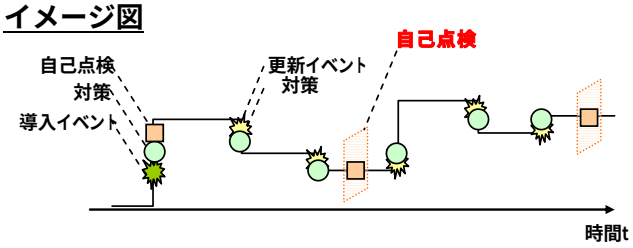
上記表内の「頻度」や「該当する遵守事項」はすべて例示であり、各大学におけるセキュリティ対策の対象や、各大学における対策状況を踏まえ、適宜定める。

(2) **点検方法の検討** (Step B-2)

自己点検項目一覧に記載されたそれぞれの項目に対して、点検方法を検討する。自己点検については、原則として実施主体における自己申告形式となるので、自己点検を実施するタイミングとその内容によって、主に以下の３つの点検方法が考えられる。

点検方法		概説
Yes/No 回答型	随時点検型	セキュリティ対策が必要と思われる事象が発生した際に、その対策を実施した旨(Yes)を、随時、自己点検して報告する。 イメージ図  長所 ・対策が実施された事実を部局総括責任者が即座に把握することができる。 短所 ・事象ごとに自己点検が発生するため、頻度が高い場合には、実施主体側、集約する側ともに負荷が大きい。 ・対策を忘れた場合には、回答もされない可能性が高いため、対策実態を把握しにくい。 ・提出期限を設定することが難しく、実施主体の自発的な申告となるため、申告忘れが懸念される。 この点検方法が適している遵守事項 ・発生頻度が低い事象に対する対策

	一括点検型	あらかじめ設定された期間内において、セキュリティ対策が必要と思われる事象に対する対応状況(実施した(Yes)/実施しなかった(No)等)を自己点検して報告する。 イメージ図  長所 ・設定期間内における対策状況をまとめて申告することができる。 ・提出期限を設定することにより、部局総括責任者が統制することができる。 短所 ・設定期間内における対策状況について、実施主体が記憶しておく必要がある。 ・対策実施とその自己点検に時間差が発生するため、即時把握が難しい。 ・設定期間内に、セキュリティ対策を実施すべき事象が発生しない場合であっても申告する必要が発生する。 この点検方法が適している遵守事項 ・発生頻度が高い事象に対する対策 ・不定期に発生する事象に対する対策
実態 回答型	断面調査型	連続維持型の対策に対して、ある時点でのセキュリティ対策状態をスナップショット的に調査して報告する。「対策を実施した事実」の確認ではなく、調査時点での対策実態を自己申告するものであり、

		設定値等を合せて提出する。 **イメージ図**  **長所** ・対策実態を把握することが可能 ・提出期限を設定することにより、部局総括責任者が統制することができる。 **短所** ・調査時点での対策状況のみが申告対象であるため、過去の対策経緯や履歴は不明。 **この点検方法が適している遵守事項** ・連続維持型の対策であって、常に最新の状態であることが期待されるセキュリティ対策

自己点検項目一覧に記載された対策項目に対して自己点検方法を決定するに当たっては、自己点検項目の分類(Step B-1)や、それぞれの点検方法の長所及び短所を踏まえ、上記３つの点検方法を基本として適宜検討することが望ましい。上記３つの点検方法のいずれかを選択するほか、例えば、対策実施の都度、その記録を取得した上で、定期的に一括点検し、併せて過去の実施状況を再確認する等、点検方法を複合的に使うことも可能であれば検討すべきである。

なお、連続維持型、単発実施型のそれぞれについて、[定期型/不定期型]及び[対策実施の頻度]を考慮して自己点検項目を比較検討した場合における適切と思われる自己点検方法は、概ね以下の図 5 に示すような領域となる。

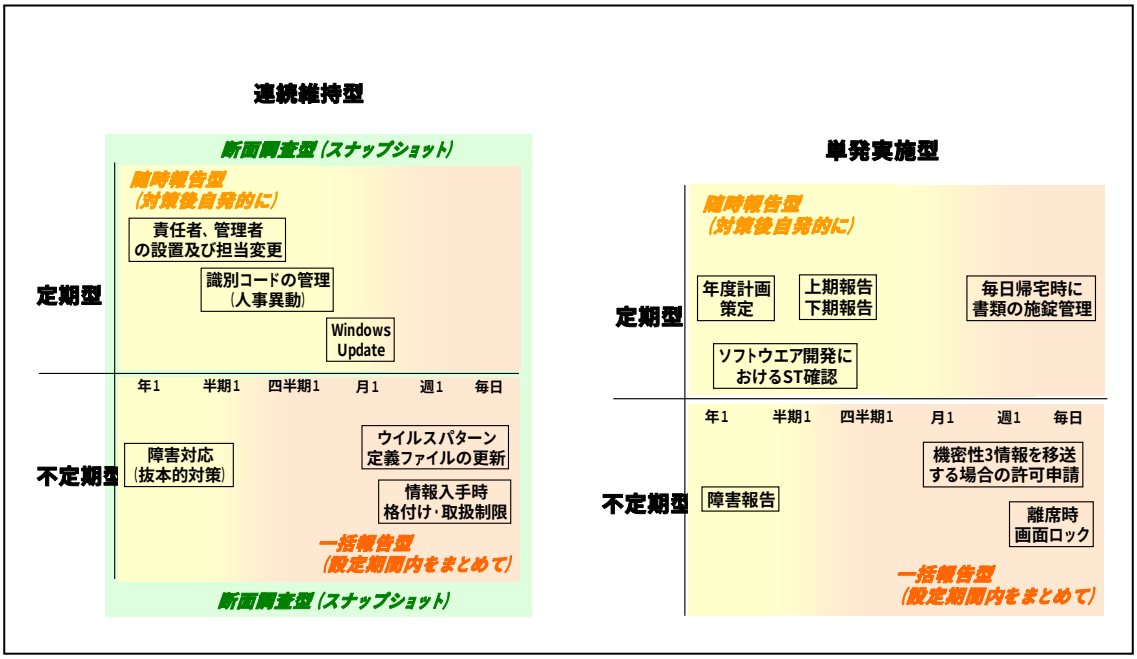


図 5. 点検方法の検討（例）

(3) 実施時期及び実施頻度の検討 (Step B-3)

自己点検項目一覧に記載されたそれぞれの項目に対して、一括点検型又は断面調査型による自己点検方法を選択した場合には、実施時期及び実施頻度に関する検討が必要である。自己点検の実施時期及び実施頻度を検討するに当たっては、全学総括責任者が定める年度自己点検計画を踏まえる必要がある。また、自己点検は、原則としてすべての情報セキュリティ対策項目についてすべての実施主体が行うものであることから、当該セキュリティ対策自体の発生頻度のほか、実施主体（回答者）による作業負荷、部局総括責任者による確認・評価に係る作業負荷、全学総括責任者による確認・評価に係る作業負荷なども考慮する必要がある。

負荷軽減・効率化のために例えば以下のような工夫をするとよい。

- 自己点検の実施時期及び実施頻度は、当該情報セキュリティ対策項目の発生時期や発生頻度に応じて適切に決定されるべきであるが、発生時期や発生頻度に過剰に即して個別に設定された場合には、自己点検に係る者に過大な負荷を強いるおそれがある。そのため、自己点検の実施時期及び実施頻度は、ある程度グループ化した上で、同一グループに属する情報セキュリティ対策項目は同時に自己点検する方が効率的である。以下の図6に示す例では、毎月末に１ヶ月分、毎半期末に半期分、毎年度末に一年分の3つの異なるサイクルで自己点検を実施するモデルである。

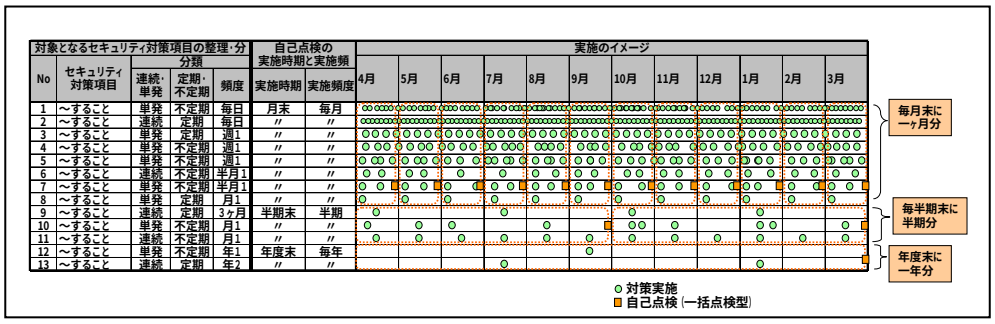


図6. 自己点検の実施時期及び実施頻度の検討

- ある特定の時期（例：月末）に負荷が集中するおそれがある場合には、実施時期をずらすなどの工夫が必要である。

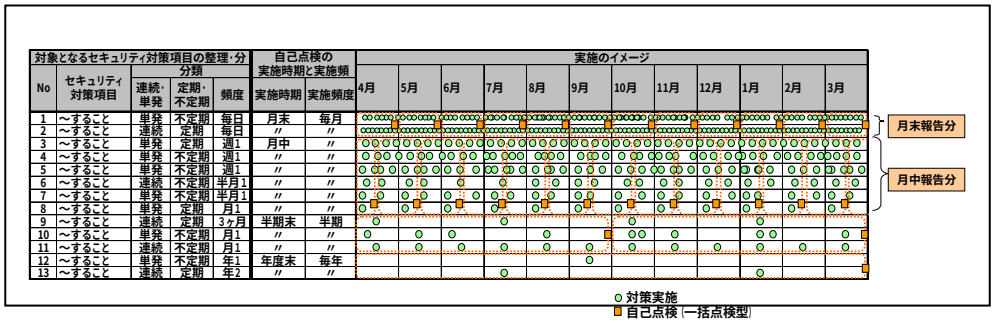


図7. 自己点検の実施時期及び実施頻度の検討

- 実施頻度と実施項目のバランスを考慮すべきである。すなわち、頻繁に実施する自己点検項目については、その実施項目の数を過度に増やさないようにする必要がある。そのためには、以下に示すように、実施されたすべての対策を限定した上で、対象時期と自己点検項目を順次ずらすなどの工夫が必要である。

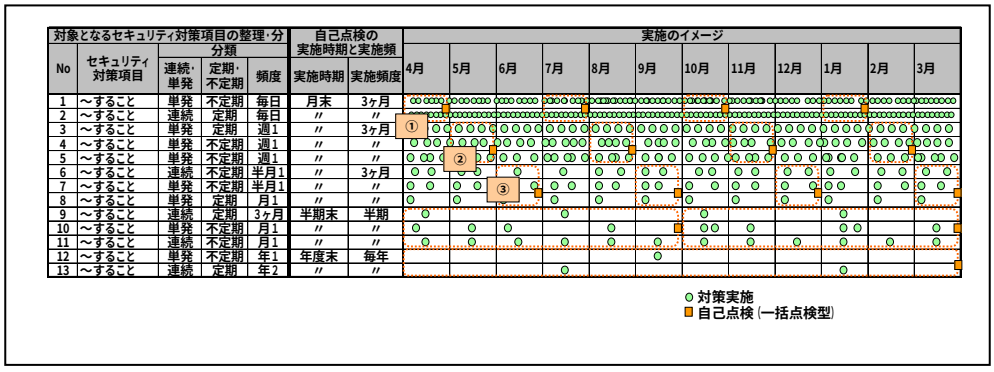


図8. 自己点検の実施時期及び実施頻度の検討

(4) **適用範囲の整理** (Step B-4)

自己点検項目一覧に記載されたそれぞれの項目に対して、その実施主体（情報セキュリティ関係規程の「主語」）、管理者、責任者などを明確にする。なお、この情報は、自己点検結果の集約ルートを決定する際に必須となる。

また、後に自己点検結果を分析・評価した場合に有用と思われる属性を追加しておくことが望ましい。例えば、対象となるシステム（例：全システムが対象、モバイル PC が対象、メールシステムが対象等）や、ライフサイクル（例：システム開発時に適用、情報の保存時に適用等）などが挙げられる。

(5) **自己点検の回答項目の作成** (StepB-5)

実施主体における自己点検は、原則として当該実施主体による自己申告形式であるが、その回答項目は、Step B-2 において検討を行った自己点検方法（随時点検型/一括点検型/断面調査型）の区別により異なったものとなる。

(I)**随時点検型の場合には、その回答は対策実施した事実とその日時を回答することが基本となる。**

(II)**一括点検型の場合には、その回答は実施状況、すなわち実施した**(Yes)**又は実施しなかった**(No)**による回答が基本となる。ただし、実施状況や遵守できていない場合の理由等をより詳細に把握し、今後の改善に結び付けていくため、あるいは、実施すべき対策についての認識が不十分である等の理由により自己点検の実施によって教育的な効果も期待する場合には、以下のようなアンケート形式の選択肢も有効である。**

- **適切に実施している**（Yes）
- **通常実施しているが、今回は実施していない**（No）
  - **今回実施できなかった合理的な理由があるため**（自由記入）
  - **たまたま実施することを忘却してしまったため**
  - **毎回実施することは現実的には困難であるため**（自由記入）
  - **その他**（自由記入）
- **恒常的に実施していない**（No）
  - **恒常的に実施していない合理的な理由があるため**（自由記入）
  - **遵守事項を守ることは現実的には困難であるため**（自由記入）
  - **遵守事項が抽象的であり、どう実施してよいか判断が難しいため**
  - **遵守事項の存在を認識していなかったため**
  - **その他**（自由記入）
- **該当しない**(NA)
  - **既に例外承認済みであるため**
  - **現在、例外申請中であるため**
  - **そもそも対象外であるため**
  - **当該セキュリティ対策を必要とする事象が発生しなかったため**
  - **その他**（自由記入）

(III)断面調査型の場合には、その回答は調査時点でのセキュリティ対策状態を回答することが基本となる。例えば、ウイルスパターン定義ファイルの最新化を求める対策の場合には、ウイルスパターン定義ファイルのバージョン番号を、適切なアクセス制御を求める対策の場合には、その Access Control List （アクセス制御に関する設定ファイル）の提出を求めるものである。

なお、自己点検は、その情報セキュリティ対策実施状況を忠実に自己申告することが大前提であり、回答者が虚偽の申告（No であることを隠して Yes と回答する等）を行ったり、不適切な申告（自己点検項目の中身を理解せず全部 Yes と回答する等）を行ったりすることのないようにする必要がある。すなわち、忠実に自己申告することを実施手順書において改めて確認するとともに、No と回答した場合の対応手順を明確にしたり、システム化によって回答者の負荷を軽減したり明確な質問として回答しやすくする等の配慮が求められる。

(6) 情報セキュリティ監査における調査方法 (Step B-6)

なお、本解説書の範囲外ではあるが、自己点検結果を踏まえて実施される情報セキュリティ監査における調査方法も合わせて検討しておくと効率的である。情報セキュリティ監査における調査方法としては、主に以下のものがある。詳細は、セキュリティ監査に関するマニュアル類を参照のこと。

- 質問
- 査閲
- 観察
- 点検

以上、自己点検項目の整備(Step B)を行うに当たっては、以下の図 9 に示すような整理表を用いて作業を行うとよい。

	自己点検の対象となるセキュリティ対策項目の整理・分析					自己点検の設計										備考
	自己点検項目一覧の作成	事務情報セキュリティ対策基準との対応	分類			点検方法			実施時期＆頻度		適用範囲			回答項目		監査における調査方法
			連続・単発	定期・不定期	頻度	随時点検型	一括点検型	断面調査型	自己点検の実施時期	自己点検の実施頻度	実施主体	管理者	責任者	回答項目	備考	
1	人事異動の際には、識別コードの管理を徹底すること。	2.1.1.3 (2)(g)	連続	定期	年 4	○			実施時	実施時	権限管理を行う者	情シセ管	情シセ責	Yes 日時	—	点検
2	情報入手時には、格付け・取扱制限を明示すること。	1.3.1.1 (2)(a)	連続	不定期	毎日		○		月末	月１	事務従事者	課室情セ	情報セ責	Yes No	アンケート併用	質問
3	ウイルスパターンを最新にすること。	1.5.2.7 (1)(a)	連続	不定期	週１			○	15 日 30 日	半月１	事務従事者	情シセ管	情シセ責	設定値	バージョン番号	点検
4	ソフト開発時に ST 確認すること	1.5.1.1 (1)(d)	単発	定期	年１	○			実施時	実施時	部局技術責任者	—	情報セ責	Yes 日時	—	査閲
5	離席時には画面ロックすること。	1.3.1.2 (5)(b)	単発	不定期	毎日		○		月末	月１	事務従事者	課室情セ	情報セ責	Yes No	—	質問
：	：	：	：	：	：	：	：	：	：	：	：	：	：	：	：	：
	Step A-3	StepA-4	Step B-1			Step B-2			Step B-3		Step B-4			Step B-5		Step B-6

注：本検討例では、自己点検の対象となるセキュリティ対策項目の例として典型的な５つの対策を列記したが、実際には、これらを所管する部局総括責任者が必ずしも一致するものではない。

図 9. 自己点検項目の整備(Step B)における整理表の例

4.3 自己点検票の集約ルートの検討 (Step C)

実施主体によって記入された自己点検票は、部局総括責任者へ集約し、最終的に自己点検の結果を全学総括責任者に集約することが必要となる。

自己点検票を集約するに当たっては、概ね以下の３つの集約ルートが想定されるところ、部局総括責任者は、自己点検の規模、指揮命令系統の構造、確認・評価の実施方法などをかんがみ、適切な集約ルートを選択する必要がある。

(1) 大学事務の指揮命令系統を軸とした集約ルート（図 10 参照）

実施主体は、大学事務遂行上の指揮命令系統における上司に当たる者へ自己点検票を提出し、順次、この指揮命令系統に沿って回収し、最終的に部局総括責任者へ集約するルートである。この集約ルートでは、大学事務遂行上の指揮命令系統における上司を経由させることによって、統制機能が作用し、対策の実態をより適切に反映した回答を得ることが期待できる。また上司による改善指導も期待できる。そのため、実施主体（回答者）が行うべきセキュリティ対策について、上司が十分認識している場合には有効な方法である。

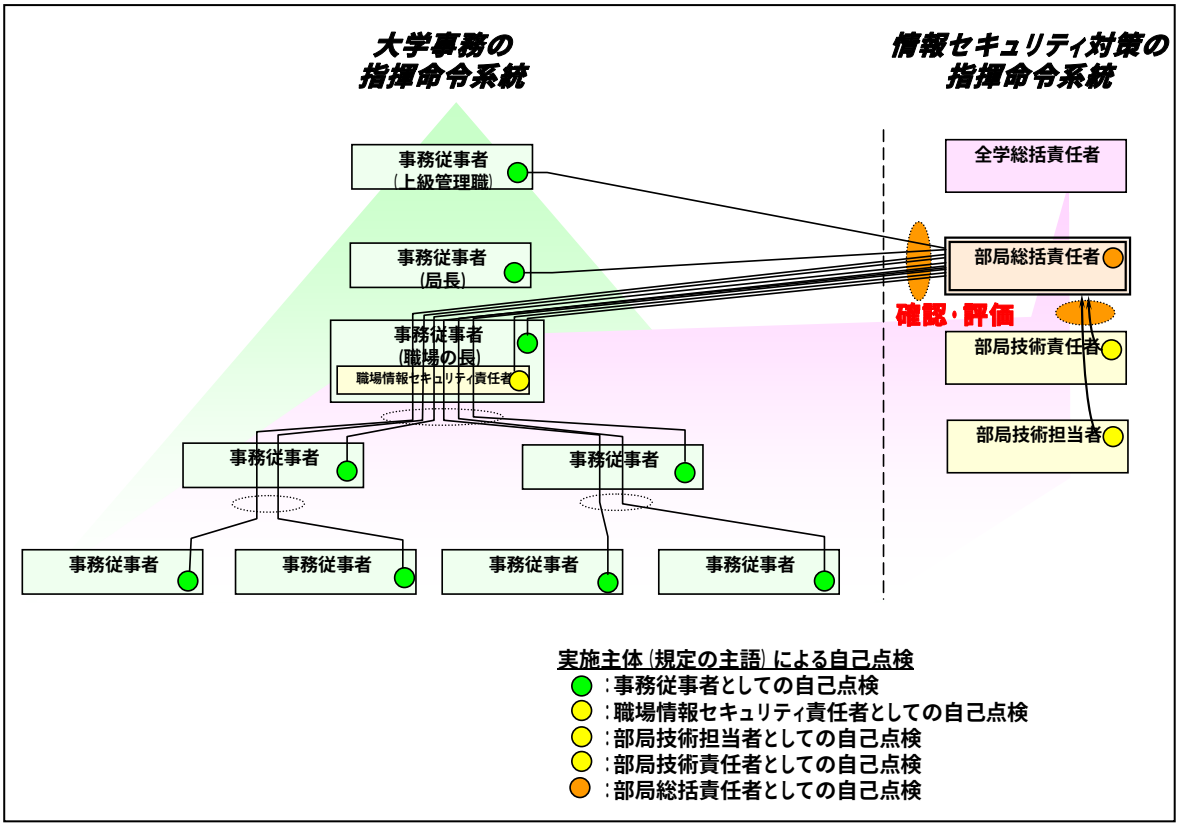


図 10. 大学事務の指揮命令系統を軸とした集約ルート

(2) 情報セキュリティ対策の指揮命令系統を軸とした集約ルート（図 11 参照）

実施主体は、情報セキュリティマネジメント上の本来の集約ルートである部局技術担当者に自己点検票を提出し、部局技術責任者を経由して部局総括責任者へ集約するルートである。この集約ルートでは、情報セキュリティ対策の責任分担が明確化されているため、部局技術責任者や部局技術担当者が、各実施主体（回答者）との面識がある場合など、適切な意思疎通が可能な場合には有効な方法である。

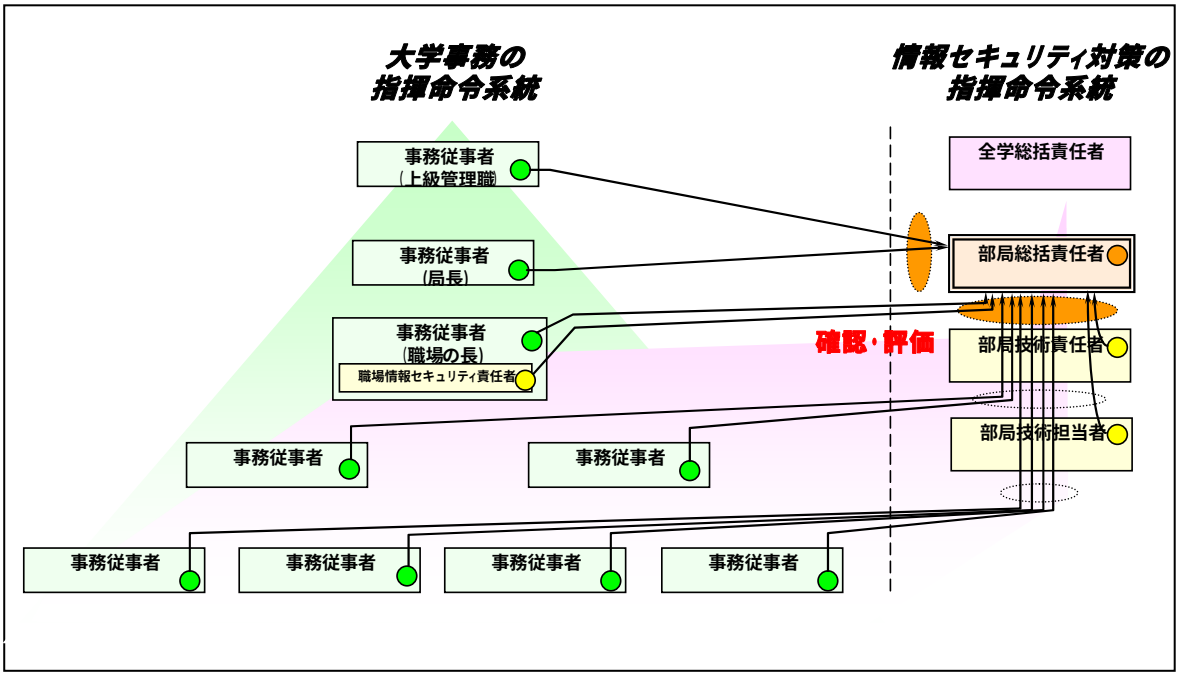


図 11 情報セキュリティ対策の指揮命令系統を軸とした集約ルート

(3) 部局総括責任者へ直接提出する集約ルート（図 12 参照）

最も簡素な（オーバーヘッドの少ない）集約ルートであり、自己点検を実施する範囲が小規模な場合には有効な方法である。

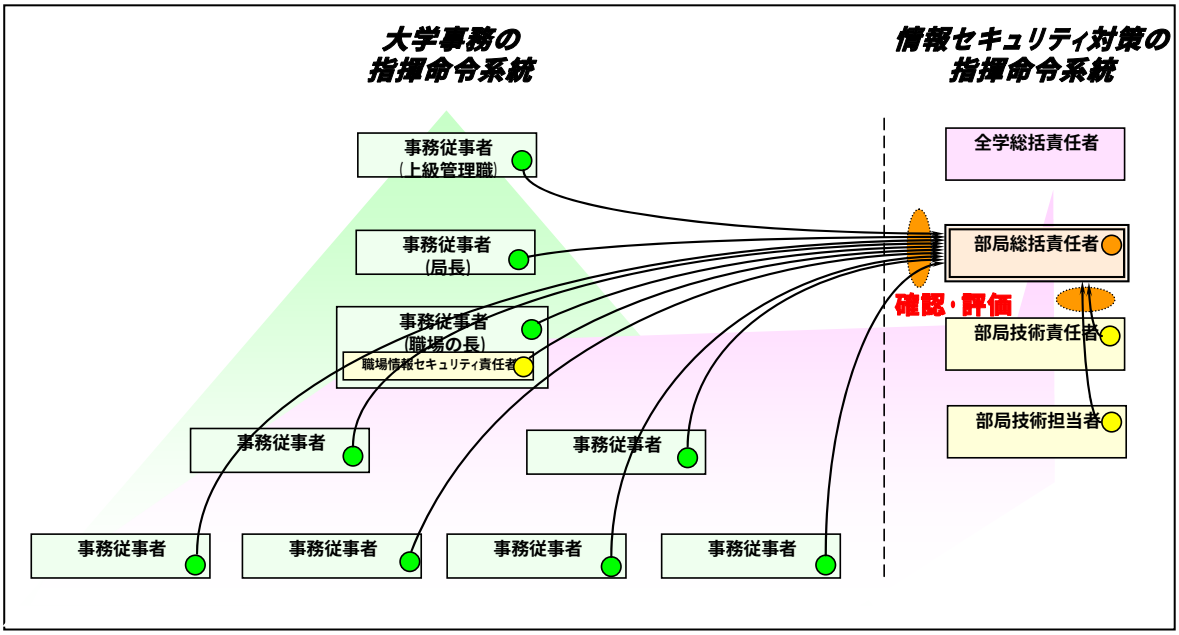


図 12. 部局総括責任者へ直接提出する集約ルート

4.4 自己点検の確認・評価に関する委任の検討 (Step D)

自己点検の回答結果については、本来、部局総括責任者がそれを確認・評価するものであるが、大規模な自己点検を実施する場合には、部局総括責任者にその負荷が集中する可能性がある。そのため、作業の効率性や自己点検結果の正確性を向上させることを目的として、確認・評価に係る作業の一部を、大学事務の管理責任を有する者や、情報セキュリティ対策の管理責任を有する者（職場情報セキュリティ責任者、部局技術責任者、部局技術担当者等）に委任することができる。

自己点検票の確認・評価に係る作業の一部を委任する場合には、自己点検の実施準備の段階で十分な検討を行い、委任される者に対して確認・評価の実施手順書を作成した上で事前に説明する必要がある。

図 10 に示した「大学事務の指揮命令系統を軸とした集約ルートの場合」について、部局総括責任者が行うべき確認・評価の一部を大学事務における管理責任者へ委任した例を図 13 に示す。この例は、事務従事者の記入内容をその上席者が「一次確認」し、その結果について職場情報セキュリティ責任者が「二次確認及び評価」を実施するモデルである。

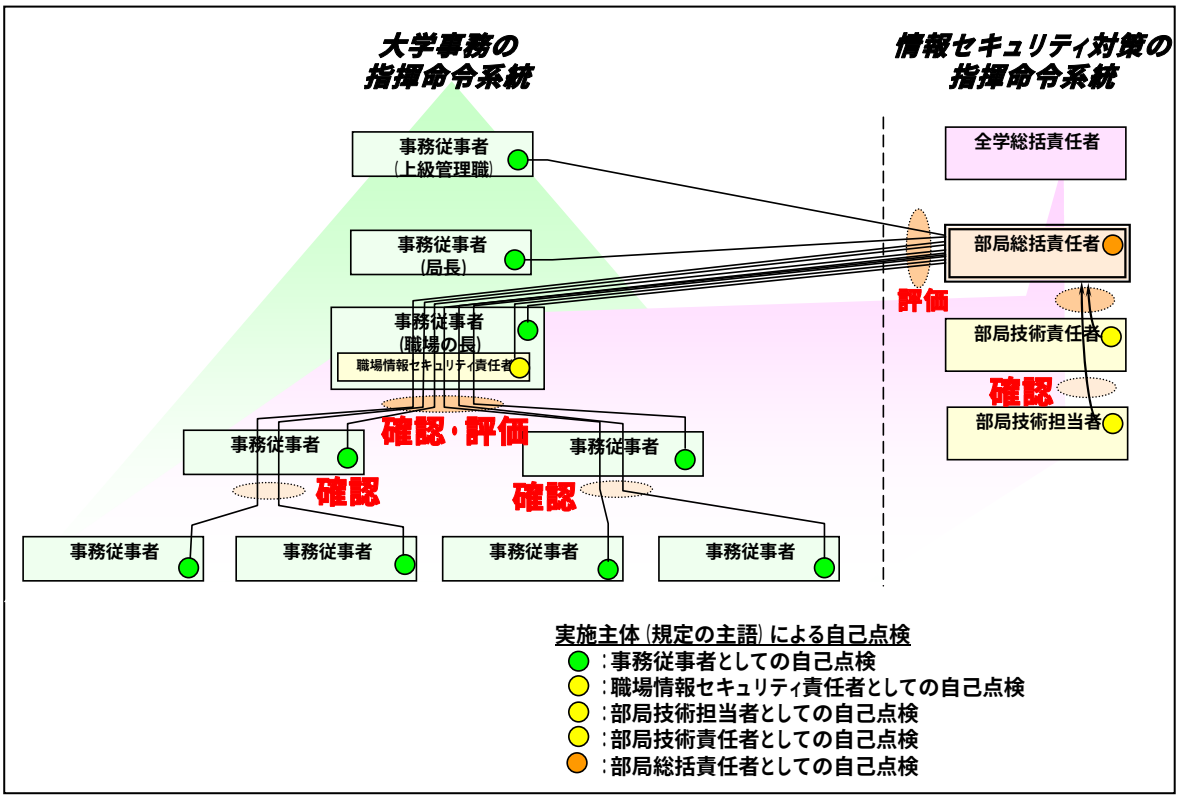


図 13. 確認・評価を委任した例

確認・評価の委託に係る留意事項は以下のとおりである。

- 実施主体から提出された自己点検票は必ずしも部局総括責任者に送付し、同人において保管する必要はないが、参照が求められた際に迅速に提示できるよう適切に管理するとともに、あらかじめ定められた期間、適切に保管する必要がある。例えば、物理的な保管場所の確保の観点から、すべての自己点検票を部局総括責任者へ集めることが困難であると予想される場合には、その確認・評価を行った者が分散してこれらを保管することが望ましい。
- 確認・評価に係る作業の一部を委任した場合であっても、確認・評価の最終的な責任は部局総括責任者が有することに注意すること。

4.5 自己点検票への展開 (Step E)

Step B で作成された整理表をもとに、職位・職階・役割ごとに自己点検票への展開を行う。

(1) 実施主体の職位・職階・役割を考慮して自己点検票への展開(Step E-1)

実施主体となる職位・職階・役割ごと（すべての事務従事者、部局総括責任者、職場情報セキュリティ責任者、部局技術担当者等）に、それぞれ実施すべき自己点検項目を抽出して自己点検票の原票を作成する。なお、一括点検型の自己点検については、その実施時期及び実施頻度に応じて、複数種類の自己点検票を準備する必要がある。（図 14 参照）

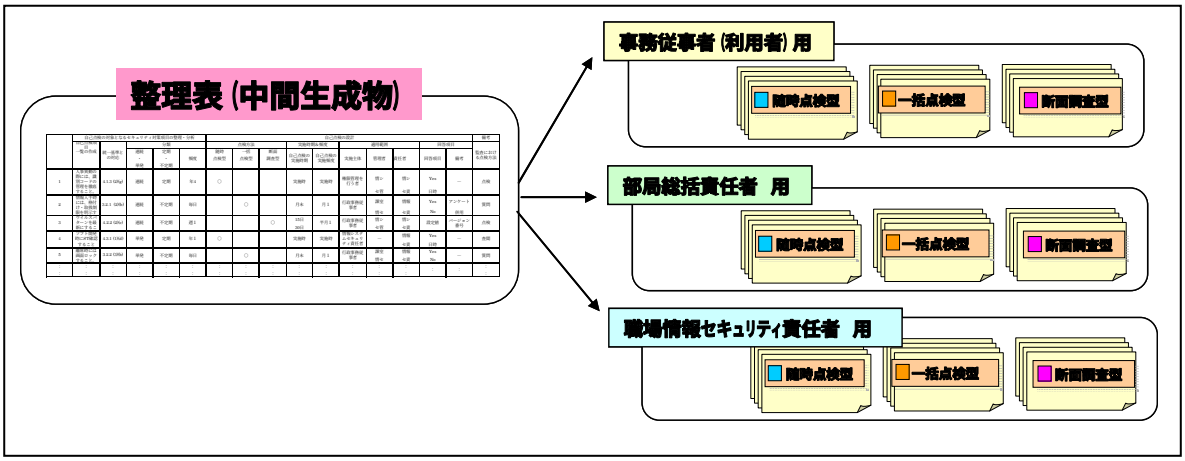


図 14. 自己点検票への展開

(2) 関連する情報の付加(Step E-2)

上記で作成された自己点検票の原票に対して、以下の関連情報を付加する。（図 15 参照）

- シートの種別（シート番号）
- 対象システム
- 想定する記入者
- 自己点検方法の種別
  - ○ 一括調査型
  - ○ 随時点検型
  - ○ 断面調査型
- 集約ルートと提出期限
- 記入者の所属、役職、氏名、連絡先
- 提出日

自己点検票 sample

シートの種別

シート番号	大学LAN-大学-一括-1-1
対象システム	○○大学 大学LANシステム
想定する記入者	事務従事者 用
自己点検方法の種別	一括点検型 (一ヶ月分)
対象期間	2011/3/1 ～2011/3/31

所属・役職・氏名・連絡先の具体名は、予め個別に入力してから配布しても良いし、当事者へ記入してもらっても良い。

集約ルートと提出期限

記入者 (実施主体)	所属	××局△△課
	役職	主査
	氏名	大学太郎
	連絡先	taro@example.ac.jp
	提出期限	2011年4月1日
上席者 (確認者)	所属	××局△△課
	役職	課長補佐
	氏名	大学次郎
	連絡先	jiro@example.ac.jp
	提出期限	2011年4月15日
職場情報セキュリティ責任者 (一次評価者)	所属	××局△△課
	役職	課長
	氏名	大学三郎
	連絡先	saburo@example.ac.jp
	提出期限	2011年5月1日
部局総括責任者 (最終評価者)	所属	××局
	役職	局長
	氏名	大学花子
	連絡先	hanako@example.ac.jp

記入者が記入

提出日	要記入

受領者が記入

提出日	要記入

次の受領者が記入

提出日	要記入

集約ルート及び確認・評価の権限委譲は、情報セキュリティ責任者が指定

No	セキュリティ対策項目	回答 (記入者が記入)	備考	確認 (確認者が記入)
1	離席時には画面ロックすること	要記入		要記入
2	情報入手時には、格付け・取扱制限を明記すること	要記入		要記入
3	毎日帰宅時にはクリアデスクを徹底すること	要記入		要記入
4	機密性3情報を移送する場合には許可申請すること	要記入		要記入
5	パスワードを変更する場合には推定されにくい文字列とすること	要記入		要記入
6	機密性3情報を府省庁外の者に提供する場合には許可申請すること	要記入		要記入
7	外部記憶媒体を他の者へ提供する場合にはデータ消去を徹底すること	要記入		要記入

図 15. 自己点検票の例

4.6 事務従事者ごとに再構成 (Step F)

実施主体となる職位・職階・役割ごとに作成された自己点検票をもとに、それを実際の事務従事者ごとに再構成する。

(1) 事務従事者ごとの再構成 (Step F-1)

実際の運用においては、一人の事務従事者が、システムの利用者としての立場のほかに、管理者あるいは責任者等の複数の立場で情報セキュリティ対策を実施する場合がある。そのため、自己点検の実施対象となるすべての事務従事者のそれぞれに対して、その情報セキュリティ対策上の立場を個別に考慮して、必要とされる自己点検項目を、統合・再構成する必要がある。以下の図 16 に、事務従事者の A さんが職場情報セキュリティ責任者としての自己点検及び事務従事者（利用者）としての自己点検を実施する場合の例を示す。

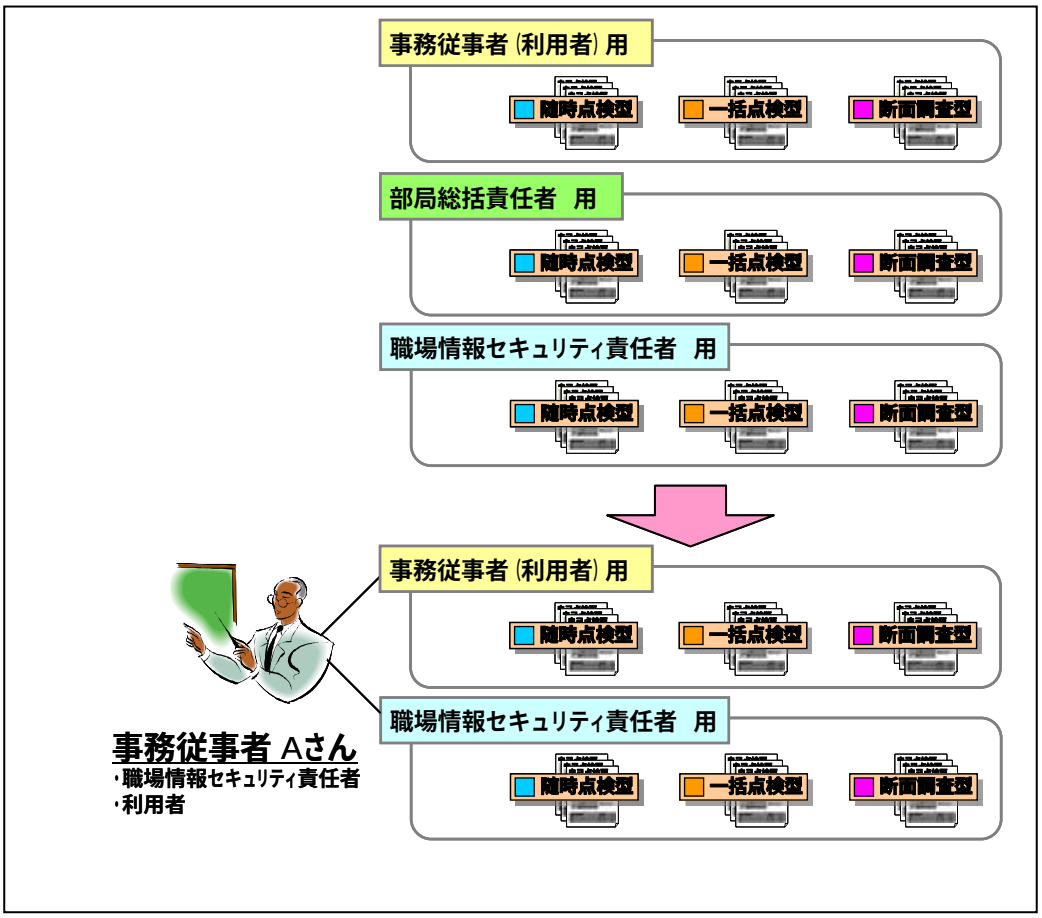


図 16. 自己点検実施の例

なお、複数の情報システムを取り扱う場合には、それぞれの情報システムに、それぞれの情報セキュリティ対策上の立場から要請される自己点検を行うことが求められる。

4.7 自己点検の実施環境の整備 (Step G)

自己点検は、情報セキュリティの管理単位ごとに、それに係るすべての事務従事者が実施するものであること、事務従事者ごとに実施内容が異なるものであること、実施主体による回答結果を部局総括責任者へ提出するに当たっては複数の関係者を経由する可能性があること、部局総括責任者による確認・評価が別の者に委任される可能性があること等をかんがみ、その実施環境を整備しておくことが望ましい。

部局総括責任者の所管する単位が小規模であれば、紙媒体による回答用紙の配布、記入、回覧、分析が可能であるが、より効率的に自己点検を実施する必要がある場合や当該単位が大きい場合には、電子メールの添付ファイルによる回答用紙の送付のほか、ワークフロー環境（電子決裁システム等）の利用、Web フォームによる回答・集約、自動集計、自動分析などの環境を整備することが望ましい。

5. 自己点検の実施 （ 1.2.3.1 (3) ）

5.1 部局総括責任者による実施の指示

> **事務情報セキュリティ対策基準　　1.2.3.1 情報セキュリティ対策の自己点検**
> (3) (a) 部局総括責任者は、全学総括責任者が定める年度自己点検計画に基づき、事務従事者に対して、自己点検の実施を指示すること。
> 【基本遵守事項】

全学総括責任者が定める年度自己点検計画は、大学全体の自己点検計画であり、情報セキュリティ対策の運用に係る単位、すなわち部局総括責任者の所管する単位ごとに実施される自己点検の集合体として整合的に構成される。そのため、各部局総括責任者は、年度自己点検計画に基づき、自らの所管する情報セキュリティの運用単位の自己点検を実施することが求められる。また、自己点検の実施に当たって、部局総括責任者は、当該運用単位に関与するすべての実施主体（事務従事者のほか、部局総括責任者を含む。）に対して自己点検の実施を指示する必要がある。

(1) 情報セキュリティ対策の実施主体に対しては、以下の内容を提示し、自己点検の実施を指示する。

- 自己点検を実施する対象（システム名称等）と自己点検項目
- 自己点検の記入方法や留意事項
- 自己点検結果の提出先及び提出方法
  提出方法の例：
  - ○ 部局総括責任者に直接提出
  - ○ 大学事務の指揮命令系統に沿って提出
  - ○ 情報セキュリティ対策の指揮命令系統に沿って提出
  - ○ 統一窓口へ提出
  - ○ 紙面による提出
  - ○ ワークフローの活用
  - ○ Webフォーム入力
- 自己点検結果の提出期限

実施手順の雛形を付録２に示す。

また、部局総括責任者は、実施主体による自己点検結果の確認・評価の一部を、大学事務の管理責任を有する者又は情報セキュリティ対策の管理責任を有する者に委任することができる。その場合には、自己点検結果の確認・評価の一部を委任された者に対してもその指示をする必要がある。

(2) 自己点検結果の確認・評価の一部を委任された者に対しては、以下の内容を提示し、確認・評価の代行を指示する。

- 自己点検を実施する対象（システム名称等）と自己点検項目
- 確認・評価の対象となる実施主体（事務従事者）の一覧
- 実施主体による自己点検結果の入手方法（能動的に取得するのか、通知があるのか等）
- 確認・評価方法や留意事項
- 確認・評価結果の提出先及び提出方法
  提出方法の例：
  - 確認・評価結果の提出先部局総括責任者に直接提出
  - 大学事務の指揮命令系統に沿って提出
  - 情報セキュリティ対策の指揮命令系統に沿って提出
  - 統一窓口へ提出
  - 紙面による提出
  - ワークフローの活用
  - Webフォーム入力
- 確認・評価結果の提出期限

なお、一人の事務従事者が、情報セキュリティ対策の実施主体として自己点検を実施すると同時に、他の事務従事者による自己点検結果の確認・評価を実施する場合がある。その場合には、それぞれの実施指示が不明確であると事務従事者の混乱を招くことから、実施指示を明確に行うよう配慮する必要がある。

実施手順の雛形を付録３示す。

5.2 事務従事者（実施主体）による実施

> **事務情報セキュリティ対策基準　　1.2.3.1 情報セキュリティ対策の自己点検**
> (3) (b) 事務従事者は、部局総括責任者から指示された自己点検票及び自己点検の実施手順を用いて自己点検を実施すること。
> 【基本遵守事項】

情報セキュリティ関係規程に定められたセキュリティ対策条項の実施主体本人による自己点検を実施する。その回答結果は、情報セキュリティ対策を把握する際の基本的な資料となる。このため、その実施においては、部局総括責任者の指示に事務従事者が従って自己点検することが重要である。

5.3 部局総括責任者による実施状況の確認

各事務従事者に対して、自己点検結果の提出期限を示して、自己点検を指示したのであるから、期限に従って提出することは、事務従事者の責任である。

しかし、部局総括責任者が所管する運用単位における、すべての自己点検が遅滞なく完了することについては、部局総括責任者も責任を担う。

そのためには、多くの事務従事者が関わることから、かれらの実施状況の進捗度合いを管理することが重要である。最終的な期限になる前に、途中の進捗などを随時確認し、予定よりも遅れている者がいれば期限の再周知や実施の催促をするなどして、実施状況の確認と必要な対応を取ることが重要である。

6. 自己点検結果の評価　（ 1.2.3.1 (4) ）

実施主体によって実施された自己点検の結果について、部局総括責任者による確認・評価が行われる。さらに、部局総括責任者による自己点検が適切に行われているかを、全学総括責任者が確認・評価する。

6.1 部局総括責任者による確認・評価

> **事務情報セキュリティ対策基準　　1.2.3.1 情報セキュリティ対策の自己点検**
> (4) (a) 部局総括責任者は、事務従事者による自己点検が行われていることを確認し、その結果を評価すること。
> 【基本遵守事項】

部局総括責任者は、所管する情報セキュリティ対策運用の単位全体について、自己点検が適切に行われていることを確認し、その結果を評価する必要がある。

(1) 部局総括責任者による確認・評価においては、主に以下の観点からの確認・評価を行う。

- 事務従事者による自己点検が実施されたかを確認する。すなわち、全員が自己点検を実施したかを確認する。
- 回答の不備（記入ミス（期待する回答形式と異なる回答をしている）や記入漏れ（回答すべきところに回答がされていない））の有無を確認する。回答の不備を発見した場合には、実施主体に対して回答の再提出を指示すること。なお、回答の不備の検出については、システム的な仕組みを構築するなどして、作業負荷を軽減することも検討すべきである。
- 必要に応じて、事務従事者へ内容を確認する。実施主体の回答結果に矛盾があると思われる内容を発見した場合には、実施主体又はその管理責任者に対して、その内容を確認する。たとえば、情報システムの対策において、求められた機能の導入がされていないのに当該機能の運用がされているという場合には、あるはずのない機能が運用されていることになる。そのような場合には、回答内容について確認をして適切な回答にする必要がある。
- 数値評価による集計を行う。対策の所管単位における実施率を把握するために、対策実施確認数 / 対策実施対象数　を求めたり、準拠率を把握するために、事務情報セキュリティ対策基準遵守率や要改善対策数 / 対策実施数　を求めたりするとよい。

(2) 個々の回答を受領した段階で随時点検するのか、回答をすべて受領した段階で一括して点検するのか等は任意であり、実施主体による自己点検の実施時期及び実施頻度と必ずしも一致させる必要はない。しかしながら、全学総括責任者が定める年度自己点検計画のスケジュールに整合するよう、確認・評価を実施しなければならない。

(3) 部局総括責任者は、自己点検結果に関する報告書を作成し、全学総括責任者へ提出する。

なお、部局総括責任者による確認・評価の一部を委任するに当たっては、事務作業のみの委任、事務作業及び判断作業の委任など様々な選択肢があるが、状況に応じて適切に判断すること。ただし、確認・評価の最終的な責任は部局総括責任者が有することに注意すること。

6.2 全学総括責任者による確認・評価

事務情報セキュリティ対策基準　　1.2.3.1 情報セキュリティ対策の自己点検

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

【基本遵守事項】

全学総括責任者は、部局総括責任者による自己点検が適切に行われていることを確認し、現状の情報セキュリティ対策状況を評価することが求められる。

(1) 全学総括責任者による確認・評価においては、主に以下の観点から確認・評価を行う。

- 部局総括責任者による自己点検が実施されたかを確認する。すなわち、全員が自己点検を実施したかを確認する。
- 提出内容の不備の有無を確認する。提出内容の不備を発見した場合には、部局総括責任者に対して提出内容の再提出を指示すること。
- 必要に応じて、部局総括責任者へ内容を確認する。部局総括責任者の提出内容に矛盾があると思われる内容を発見した場合には、部局総括責任者に対して、その内容を確認する。
- 数値評価による集計を行う。対策の大学全体としての実施率を把握するために、対策実施確認数 / 対策実施対象数　を求めたり、準拠率を把握するために、事務情報セキュリティ対策基準遵守率や要改善対策数 / 対策実施数　を求めたりするとよい。

7. 自己点検に基づく改善 （ 1.2.3.1 (5) ）

自己点検は、本人による対策実施を自己点検することが目的であるが、事務情報セキュリティ対策基準 1.2.3.1 (5) 「自己点検に基づく改善」においては、自己点検で気付いた問題点ですぐに改善できることがあれば、自己点検結果の集計や監査結果を必ずしも待たなくとも、適宜改善することが望ましいことを示している。

自己点検結果に基づく改善では、事務従事者自身による自己改善と、全学総括責任者による改善指示の２つの方法が挙げられる。

前者は、ボトムアップ的な改善であり、自己点検の結果に基づき、自己の権限の範囲で改善できると判断した事項へ対処するものである。事務情報セキュリティ対策基準 1.2.3.1 (5)(a)に記す遵守事項がこれに相当する。

後者は、トップダウン的な改善であり、全学総括責任者が情報システムの自己点検結果を評価し、必要があると判断した場合には部局総括責任者に改善を指示するものである。事務情報セキュリティ対策基準 1.2.3.1 (5)(b)に記す遵守事項がこれに相当する。

7.1 事務従事者自身による自己改善

> **事務情報セキュリティ対策基準　1.2.3.1 情報セキュリティ対策の自己点検**
> (5) (a) 事務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、部局総括責任者にその旨を報告すること。
> 【基本遵守事項】

事務従事者自身による自己改善には、実施主体の自発によるものと、部局総括責任者の指導によるものがある。

(1) 実施主体は、自己点検によって実施していないセキュリティ対策を認識した際に、それを自己の権限の範囲で改善できると判断した場合は、それを適時改善する必要がある。以下に例を示す。

- 遵守事項について失念していただけで、直ちにそれを実施することができる場合。
- 遵守事項の方法について正しく理解しておらず、異なる方法を実施しており、自己点検によってその方法では遵守したことにならないと知ったが、正しい方法について直ちに実施することができる場合。
- 遵守事項の方法について正しく理解しておらず、異なる方法を実施しており、自己点検によってその方法では遵守したことにならないと知ったが、正しい方法の実施が困難で現状の方法を続けるために例外措置の手続きを取る場合。

なお、そもそも情報セキュリティ関係規程の定める遵守事項が現実的ではない等の理由により、情報セキュリティ関係規程自体を改訂すべきと思われる場合については、まず事務情報セキュリティ対策基準 1.2.1.3 (2) (b) により例外措置の適用を申請した上で、情報セキュリティ対策における管理責任者又は部局総括責任者へ相談すること。

遵守事項を実施できない合理的理由がある場合は、例外措置の適用を申請することで、遵守事項が求める対策を実施せずとも遵守事項違反にはならない。しかし、例外措置の適用を申請することなく、遵守事項が求める対策を実施しないことは、違反となることに注意すること。

(2) 部局総括責任者（委任された者等を含む。）は、その所管する範囲で違反を発見した場合には、どのような理由によって実施主体が遵守事項を実施できなかったのかを十分調査した上で、管理責任者として部下への改善指導を行う。

- 違反した実施主体への直接指導
- 違反した実施主体の管理責任者への指導

(3) 事務従事者は自己改善を行った場合には、以下の事項について部局総括責任者への報告を行うこと。

- 違反した情報セキュリティ関係規程
- 違反した理由・背景
- 改善事項
- その他

7.2 全学総括責任者による改善指示

事務情報セキュリティ対策基準　　1.2.3.1 情報セキュリティ対策の自己点検

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

【基本遵守事項】

全学総括責任者が自己点検の結果を全体として評価し、必要に応じて部局総括責任者に改善を指示するに当たっては、以下の観点が考えられる。

(1) 当該情報システムに関する自己点検の結果を踏まえ、改善する必要があることが明らかになった事項（当該情報システムに閉じた範囲で分かる改善点であり、自己点検報告書に記載があるもの）について改善の指示を行う。
(2) 他の情報システムに関する自己点検の結果を踏まえ、それらとの総合的な分析に基づいて明らかになった事項について改善の指示を行う。また、他の情報システムに関す

る自己点検の結果を踏まえ、他の情報システムにおいても同種の課題及び問題点がある可能性が高い場合には、併せて改善の指示を行う。

また、改善するに当たっては、どのような理由によって遵守事項が実施されていないのかを十分調査した上で対応方法を検討する必要がある。以下に改善指示の例を示す。

- 実施主体（事務従事者）による遵守を徹底
- システム的な仕組みの整備により、実施主体（事務従事者）の負荷を軽減
- 情報セキュリティ関係規程における記述の詳細化・具体化
- 情報セキュリティに関する教育の見直し
- 情報セキュリティ関係規程の見直し、事務情報セキュリティ対策基準へのフィードバック
- 例外措置の申請

付録編

雛形の利用方法

雛形において想定する前提

これらの雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 情報セキュリティ対策の運用に係る単位が定められ、その単位ごとに部局総括責任者が設置されている。
- 当該運用単位において、部局総括責任者以下、部局技術責任者、部局技術担当者、職場情報セキュリティ責任者が設置されている。
- 「高等教育機関の情報セキュリティ対策のためのサンプル規程集」の事務情報セキュリティ対策基準が各大学の事務情報セキュリティ対策基準へ適切に反映されており、また、必要に応じて実施手順が整備されている。すなわち、当該運用単位における情報セキュリティ関係規程が整備されており、情報セキュリティ対策を実施するに当たって事務従事者自らが実施すべき具体的な対策項目が明確になっている。

手直しポイント

「高等教育機関の情報セキュリティ対策のためのサンプル規程集」の事務情報セキュリティ対策基準に基づき策定された各大学の事務情報セキュリティ対策基準に準拠した「年度自己点検計画」及び「自己点検の実施手順」を策定する手順には、以下の事項を踏まえて作業を行う必要がある。

(1) 各大学において所有する情報システムの数及び規模、それに係る事務従事者の数、各大学における情報セキュリティ対策状況や情報セキュリティ対策体制等を踏まえ、実効的な実施手順とすること。特に、自己点検に係る者に過度の作業負荷を強いることのないよう配慮する。
(2) 実施手順（雛形）において/・・・/形式で示す設定値（システム名称、担当者名、文書名等）については、各大学内の定めに合わせる。
(3) 実施手順（雛形）において【・・・の場合】形式で示す記述については、想定される複数の案を記したものであり、各大学の判断により適宜、選択又は修正する。
(4) 自己点検や情報セキュリティ監査に関してマニュアル、ガイドライン等を作成する場合には、それらとの整合性を考慮し、適切に分割、統合、相互参照する。

付録１：年度自己点検計画の雛形

作成日：*[○○年○月○日]*

全学総括責任者

[氏 名]

[○○年度] [×××大学] 自己点検計画

1. 本自己点検計画の位置付け

本自己点検計画は、各部局総括責任者が所管する単位で自己点検を行うに当たり、大学全体として効率的かつ整合的に実施するための計画である。

2. 自己点検の実施方針

本年度の自己点検は、以下の方針で実施する。

2.1 実施頻度

(1) 自己点検は、各点検項目について、年間を通じて*最低[1]回以上* 実施する。
(2) ただし、情報システムの運用に係る点検項目については、年間を通じて*最低[2]回以上* 実施する。

2.2 実施時期

(1) 部局総括責任者は、*[10 月 31 日]* までに自己点検の確認・評価結果を全学総括責任者へ提出すること。
(2) 事務従事者（実施主体）による自己点検の実施時期は、自己点検項目それぞれの実施頻度や上記の提出期限を考慮の上、部局総括責任者が定めること。通年で日々実施するような対策以外の特定の時点や期間に実施する対策については、対策実施後遅滞することなく随時自己点検を実施すること。

2.3 確認及び評価の方法

(1) 事務従事者による自己点検が実施されたか（全員が自己点検を実施したか）を確認する。
(2) 以下の数値評価を行う。

- 対策実施率（＝対策実施確認数 / 対策実施対象数）
- 事務情報セキュリティ対策基準遵守率

3. 自己点検の全体スケジュール

（詳細を別紙で添付する）

付録２：自己点検の実施指示書の雛形

[○○○号]

[平成□年□月□日]

[○○システムの全利用者] 殿

[○○システム] 部局総括責任者

[○○局長　　大学太郎]

[○○システム] の自己点検実施について

1. 自己点検の実施

（自己点検を実施する趣旨を記述する。）

2. 自己点検の対象者

2.1 対象者

【利用者を対象者とする場合の記述例】

本指示書は、*[○○システム]*を利用するすべての事務従事者を対象とする。

【部局技術責任者及び部局技術担当者を対象者とする場合の記述例】

本指示書は、*[○○システム]*における部局技術責任者及び部局技術担当者を対象とする。

3. 自己点検の対象システム及び関係規程

3.1 自己点検を実施する対象システム

本指示書は、*[○○システム]* に関する自己点検を対象とする。

3.2 対象となる情報セキュリティ関係規程

本指示書は、以下に示す情報セキュリティ関係規程に記載されたセキュリティ対策項目に対する自己点検を対象とする。

- *[○○システム運用管理規定 ver1.3]*
- *[○○システム利用者の手引 ver2.2]*

4. 自己点検票（一式）の入手方法

【本実施指示書に添付する場合】

対象者は、本通達に添付された自己点検票を使用すること。

【自己点検に関する HomePage からダウンロードする場合】

対象者は、以下 URL より自身の自己点検票をダウンロードして使用すること。

[http://○○.example.ac.jp/security/self-check/index.html]

5. 自己点検票（一式）の構成

シート No	シート名称	自己点検方法	対象者（実施主体）	
[○○-11]	*[○○]*	*[一括点検型]*	*[職場情報セキュリティ責任者]*	
[○○-12]	*[○○]*	*[一括点検型]*	*[利用者]*	*[○]*
[○○-13]	*[○○]*	*[一括点検型]*	*[利用者]*	*[○]*
[○○-14]	*[○○]*	*[随時報告型]*	*[職場情報セキュリティ責任者]*	
[○○-15]	*[○○]*	*[随時報告型]*	*[利用者]*	*[○]*

【利用者を対象者とする場合の記述例】

これらの自己点検票（一式）のうち、利用者を実施対象とした自己点検票（上表右列の○を付した自己点検票）を用いること。

6. 自己点検票の記入時の留意事項

(1) 対象者は、虚偽の申告（実施していない事実を隠して「実施した」と回答）をしないこと。
(2) 対象者は、不正確な申告（自己点検項目の中身を理解せず「実施した」と回答）をしないこと。

7. 自己点検結果の提出先

【本実施指示書において明示する場合】

自己点検結果の提出先は、以下のとおりとする。

シート No	シート名称	自己点検方法	提出先
[○○-12]	*[○○]*	*[一括点検型]*	*[職場情報セキュリティ責任者]*
[○○-13]	*[○○]*	*[一括点検型]*	*[職場情報セキュリティ責任者]*

[○○-15]	*[○○]*	*[随時報告型]*	*[職場情報セキュリティ責任者]*

【自己点検票において明示する場合】
自己点検結果の提出先は、各自己点検票の記載のとおりとする。

8. 自己点検結果の提出期限

【本実施指示書において明示する場合】
自己点検結果の提出期限は、以下のとおりとする。

シート No	シート名称	自己点検方法	提出期限
[○○-12]	*[○○]*	*[一括点検型]*	*[2011 年 4 月 30 日]*
[○○-13]	*[○○]*	*[一括点検型]*	*[2011 年 5 月 30 日]*
[○○-15]	*[○○]*	*[随時報告型]*	*[随時報告]*

【自己点検票において明示する場合】
自己点検結果の提出期限は、各自己点検票に記載のとおりとする。

9. 自己点検に基づく改善

9.1 対象者による自己改善

(1) 対象者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善すること。

- 遵守事項について失念していただけで、直ちにそれを実施することができる場合。
- 遵守事項の方法について正しく理解しておらず、異なる方法を実施しており、自己点検によってその方法では遵守したことにならないと知ったが、正しい方法について直ちに実施することができる場合。
- 遵守事項の方法について正しく理解しておらず、異なる方法を実施しており、自己点検によってその方法では遵守したことにならないと知ったが、正しい方法の実施が困難で現状の方法を続けるために例外措置の手続きを取る場合。

なお、そもそも情報セキュリティ関係規程の定める遵守事項が現実的ではない等の理由により、情報セキュリティ関係規程自体を改訂すべきと思われる場合については、まず事務情報セキュリティ対策基準 1.2.1.3 (2) (b) により例外措置の適用を申請した上で、情報セキュリティ対策における管理責任者又は部局総括責任者へ相談すること。

遵守事項を実施できない合理的理由がある場合は、例外措置の適用を申請することで、遵守事項が求める対策を実施せずとも遵守事項違反にはならない。しかし、例外措置の適用を申請することなく、遵守事項が求める対策を実施しないことは、

違反となることに注意すること。

(2) 対象者は、自己改善を行った場合には、以下の事項について部局総括責任者への報告を行うこと。

- 違反した情報セキュリティ関係規程
- 違反した理由・背景
- 改善事項
- その他

9.2 全学総括責任者による改善指示

全学総括責任者から情報セキュリティ対策の改善指示があった場合には、その趣旨を理解の上これに従うこと。

10. 参考資料

【本実施指示書に添付する場合】

自己点検の概要について、*[別紙○]* に示す。

【自己点検に関する HomePage で公開する場合】

自己点検の概要について、以下 URL を参照のこと。

[http://○○.example.ac.jp/security/self-check/index.html]

付録３：確認・評価の委任指示の雛形

[○○○号]

[平成□年□月□日]

[○○システムの部局技術責任者] 殿

[○○システム] 部局総括責任者

[○○局長　　大学太郎]

[○○システム] の自己点検結果の確認・評価の委任について

1. 自己点検結果の確認・評価の実施

（自己点検結果の確認・評価を実施する趣旨を記述する。）

2. 自己点検結果の確認・評価を行う者

2.1 対象者

【職場情報セキュリティ責任者を対象者とする場合の記述例】

本指示書は、*[○○システム]*における職場情報セキュリティ責任者を対象とする。

【部局技術責任者及び部局技術担当者を対象者とする場合の記述例】

本指示書は、*[○○システム]*における部局技術責任者及び部局技術担当者を対象とする。

3. 自己点検結果の確認・評価の対象システム及び関係規程

3.1 自己点検を実施する対象システム

本指示書は、*[○○システム]* に関する自己点検結果を対象とする。

3.2 対象となる情報セキュリティ関係規程

本指示書は、以下に示す情報セキュリティ関係規程に記載されたセキュリティ対策項目に対する自己点検結果を対象とする。

- *[○○システム運用管理規定 ver1.3]*
- *[○○システム利用者の手引 ver2.2]*

4. 自己点検結果の確認・評価の対象者

4.1 対象者一覧の入手方法

【本実施指示書に添付する場合】

本指示書に添付する対象者一覧を参照すること。

【自己点検に関する HomePage からダウンロードする場合】

以下の URL より対象者一覧をダウンロードして使用すること。

[http://○○.example.ac.jp/security/self-check/index.html]

5. 実施主体による自己点検結果の入手方法

【本実施指示書に添付する場合】

本指示書に添付された自己点検結果を使用すること。

【自己点検に関する HomePage からダウンロードする場合】

通知メールを受領した後、以下の URL より自己点検結果をダウンロードして使用すること。

[http://○○.example.ac.jp/security/self-check/index.html]

6. 自己点検票の構成

シート No	シート名称	自己点検方法	対象者（実施主体）	
[○○-11]	*[○○]*	*[一括点検型]*	*[職場情報セキュリティ責任者]*	
[○○-12]	*[○○]*	*[一括点検型]*	*[利用者]*	*[○]*
[○○-13]	*[○○]*	*[一括点検型]*	*[利用者]*	*[○]*
[○○-14]	*[○○]*	*[随時報告型]*	*[職場情報セキュリティ責任者]*	
[○○-15]	*[○○]*	*[随時報告型]*	*[利用者]*	*[○]*

これらの自己点検票のうち、本確認・評価の対象となるシートは、○を付した自己点検票である。

7. 自己点検票の確認・評価方法及び留意事項

(1) 対象者全員が自己点検を実施したかを確認すること。

(2) 回答の不備（記入ミス（期待する回答形式と異なる回答をしている）や記入漏れ（回答すべきところに回答がされていない））の有無を確認する。回答の不備を発見した場合には、実施主体に対して回答の再提出を指示すること。なお、回答の不備の検出

については、システム的な仕組みを構築するなどして、作業負荷を軽減することも検討すべきである。

(3) 必要に応じて、事務従事者へ内容を確認する。実施主体の回答結果に矛盾があると思われる内容を発見した場合には、実施主体又はその管理責任者に対して、その内容を確認する。たとえば、情報システムの対策において、求められた機能の導入がされていないのに当該機能の運用がされているという場合には、あるはずのない機能が運用されていることになる。そのような場合には、回答内容について確認をして適切な回答にする必要がある。

【数値評価を実施する場合】

(4) 以下の数値評価を実施すること。

- *[対策実施確認数 / 対策実施対象数]*
- *[要改善対策数 / 対策実施数]*

8. 確認・評価結果の提出先

【本実施指示書において明示する場合】

自己点検の確認・評価結果の提出先は、以下のとおりとする。

シート No	シート名称	自己点検方法	提出先
[○○-12]	*[○○]*	*[一括点検型]*	*[部局総括責任者]*
[○○-13]	*[○○]*	*[一括点検型]*	*[部局総括責任者]*
[○○-15]	*[○○]*	*[随時報告型]*	*[部局総括責任者]*

【自己点検票において明示する場合】

自己点検の確認・評価結果の提出先は、各自己点検票に記載のとおりとする。

9. 確認・評価結果の提出期限

【本実施指示書において明示する場合】

確認・評価結果の提出期限は、以下のとおりとする。

シート No	シート名称	自己点検方法	提出期限
[○○-12]	*[○○]*	*[一括点検型]*	*[2006 年 4 月 30 日]*
[○○-13]	*[○○]*	*[一括点検型]*	*[2006 年 5 月 30 日]*
[○○-15]	*[○○]*	*[随時報告型]*	*[随時報告]*

【自己点検票において明示する場合】

確認・評価結果の提出期限は、各自己点検票に記載のとおりとする。

10. 自己点検に基づく改善

10.1 事務従事者自身による自己改善

(1) 実施主体から自己改善を行った旨の報告を受けた場合には、以下の事項について部局総括責任者へ報告を行うこと。

- 違反した情報セキュリティ関係規程
- 違反した理由・背景
- 改善事項
- その他

11. 参考資料

【本実施指示書に添付する場合】

自己点検の概要について、*[別紙○]* に示す。

【自己点検に関する HomePage で公開する場合】

自己点検の概要について、以下 URL を参照のこと。

[http://○○.example.ac.jp/security/self-check/index.html]

A3300 教育テキストの策定に関する解説書

解説：本書では、このサンプル規程集に収められている教育テキスト(A3301～A3303)を参照する場合の、各大学における策定について説明する。

１．大学における情報セキュリティに関する教育の必要性

情報セキュリティは、一般論として、組織とその事業の運営にとって質や継続性に重大な影響を及ぼしかねない要素である。大学の組織運営においてもそれはあてはまる。さらに、教育機関である大学にとって、学生に対して情報セキュリティに関する教育を行い、情報を取り扱うために必要な資質を習得させることも欠かせない。

大学では多くの場合に、コンピュータのネットワーク接続やシステム設定のような管理業務を、「情報部」のような部署が一元的に行うのではなく、部局や研究室、事務室ごとにいわゆる「管理者」を定めて委ねていることが多いと考えられる。したがって、情報セキュリティの維持のために多くの「管理者」への教育も欠かせない。

２．大学における情報セキュリティ教育の種別

前節で述べた必要性に基づいて、A 大学が行うべき情報セキュリティに関する教育の対象者や内容などの事項を「A2301 年度講習計画」で定めている。これは、学内規程と同様に、大学として遵守すべきものである。

A 大学では、情報セキュリティ教育を次のように３つの種別に分けた。

(1) 一般利用者向け教育

これは、情報処理演習で情報教育システムや情報ネットワークを利用する立場の学生や、事務情報システムを端末や PC から利用する一般職員などを想定している。これらの対象者には、それらの利用に関して法律や学内規程によって定められている順守事項や許諾範囲、あるいはマナーや心がけるべきことがあることを理解させることができるように、教育しなければならない。

これらの対象者は情報システムやネットワークの設定操作や運用のような管理について権限をもたず、それに関する責任もないと考えられるので、管理に関する教育は必要がない。ただし、規定されている内容を利用者が理解するための最低限の技術的な知識も教育内容に含まれる。

一般利用者向けの教育は、学生の入学あるいは教職員の採用のときのように、新たな利用者に加わった者を対象として実施する「基礎講習」が基本である。これは、1 年生の情報処理演習の講義や、あるいは新規採用者講習の中で実施することも考えられる。そのほかに、定期的な再教育と、技術面や法律・制度面の最新知識を習得させるために「定期講習」も行う。

(2) システム管理者向け教育

A 大学には、全学的な情報システムを設置し運用する情報メディアセンターのほかに、部局や研究室でウェブサーバや電子メールサーバなどの情報システムを運用することがある。そのいずれのケースでも、情報セキュリティを高いレベルで維持できるように運用管理しなければならない。したがって、その管理を担当するシステム管理者に対して、情報セキュリティ対策の応用知

識を定期的に教育する必要がある。

情報メディアセンター以外の一般の部局におけるシステム管理者に対しては、部局における運用に必要な技術や状況などの知識を習得させるために「部局管理者」向けの教育を講習会などのスタイルで情報メディアセンターが実施する。

システム管理者のうち、情報メディアセンターの教職員については、とくに専門的分野に携わっていることから、他の部局の管理者と分けて教育を実施することが適当と考えられる。これは情報メディアセンターが内部的に実施するものであるが、学外のセミナー等を利用する方法もとりうる。

なお、たとえば PC 一台ごと、ネットワーク機器一台ごとについて適切なシステム管理が必要であって、PC やネットワークを設置する者には管理者責任を負えるような専門的知識の教育をなすべきであるという考え方があり、あるいは PC やネットワーク機器の設置を何らかの有資格者に限定すべきであるというような考え方もあり、厳密にはそうしなければならない。しかし一方で、専門的知識を習得した管理者をすべての PC について割り当てることは、多くの大学において現実的ではないことが考えられ、たとえば一般利用者とシステム管理者の中間的な位置づけの教育を実施する考え方もありうる。

(3) CIO/役職者向け教育

大学の運営、とくに業務遂行とそのための予算配分と人員配置に責任のある執行部（理事会、事務局長、CIO など）を対象とする教育は、情報セキュリティ対策の必要性と課題について理解を得るためのものである。その内容は、技術などの各論的知識ではなく、情報セキュリティのためのコスト（人と予算）の理解を得て、また、状況を的確に把握して、必要な対策を指揮できるように備えておくことである。

3. 大学における情報セキュリティ教育のテキスト

情報セキュリティ教育のそれぞれの種別について、教育を実施する際のテキスト（あるいは教材）が必要である。一般利用者を対象とする教育のうち、一般論については市販の教科書（情報処理演習の一部としているものを含む）を利用することもありうる。しかし、いずれの種別の教育でも各大学の情報セキュリティポリシーや情報システムサービスなどによって具体的な情報に関する内容が異なるので、その情報についてテキストを独自に準備することが必要になる。とくに、CIO/役職者向け教育はその大学における情報セキュリティの状況を説明することが重要であるから、そのときの状況を取り入れた説明資料を情
報メディアセンターにおいて作成することが必要になる。

このサンプル規程集に収めた３つの教育テキストは、講習計画に沿って教育すべき内容の概要を示しつつ、各大学の状況によって教育テキストを作成するためのガイドラインとして示した。

A3301 教育テキスト作成ガイドライン（一般利用者向け）

解説：本文書は独立した形で利用可能な、一般利用者向けの教育テキストである。内容はできるかぎり正確な記述とするよう心がけたが、記述の簡潔さを優先したために一部不十分な表現になっていたり、逆に記述が重複しているところもある。また、自習用のテキストではなく、講師が一般利用者の立場やスキルに応じて適切な助言を行いつつ講義を行うことを前提として、その講習用テキストとして作成してあることに留意されたい。

このテキストは、「A2301 年度講習計画」に従って、60 分ないし 90 分の基礎講習用として作成したものです。受講対象は、本学情報システムを新たに利用することとなった学生・教職員です。テキストの内容は、本学情報セキュリティポリシー（の各規程）に基づいて、できるだけ具体的にわかりやすい形で説明しています[4]。

1. はじめに

1.1 情報システムの目的

本学情報システムは、本学の理念である「研究と教育を通じて、社会の発展に資する」ことを実現するために、本学のすべての教育・研究活動および運営の基盤として設置され、運営されています。したがって、情報システムを秩序と安全性をもって安定的かつ効率的に運用することが不可欠です。このためには、本学情報システムを利用するすべての人が、本学のセキュリティポリシー（基本方針、運用基本規程）や利用に関する規則を遵守せねばなりません。

1.2 情報システム利用者の心構え

「コンピュータ教室で、ログインされたままのパソコンを何者かが操作して、いたずらメールを送信した。」、「他人の著作物を無許可でウェブサーバに置いて公開し、著作権者から注意を受けた。」、「新しいパソコンをネットワークに接続して、OS のアップデートをしている間にウイルスに感染してしまった。」、「研究室のウェブサーバがフィッシングに利用された。」などの事件が発生しています。法令に違反しないことは当然ながら、本学の情報システムを円滑に運用するためには、各利用者が本学構成員の一員であるという認識をもって、十分な注意を払ってコンピュータを操作することが必要です。まず、このことをよく理解してください。

1.3 利用についての原則

（利用の精神）

(1) 本学情報システムの利用にあたっては、つぎのことに留意するとともに、基本的な社会常識に従い、他の利用者や通信先に対する配慮をもって利用してください。

- **言論の自由、学問の自由**

[4] 教育を担当される教員の方へ：学生に対して「情報リテラシー」などの講義の中で実施する場合には，一回ですべてを教えてしまうのではなく，毎回の講義の中で関連する部分をとりあげていくのがよいでしょう(マイクロインサーション)。例えば，個人のウェブサイト作成の授業ときに著作権に関することを教えるなどして，工夫してください。

- 他者の生命、安全、財産を侵害しない
- 他者の人権、人格の尊重
- 公共の福祉、公の秩序

（法令の遵守）

(2) 法令の遵守

本学情報システムでの行為は治外法権ではありません。日本国内においては日本国内法が適用されます。場合によっては海外の法律の適用をうける可能性もあります。法令や公序良俗に反する行為を行ってはなりません。

（目的外利用の禁止）

(3) 本学情報システムは、教育・研究活動および運営の基盤として設置・運営されているものです。これらの目的に該当する範囲で利用してください。

（利用規程と罰則）

(4) 「A2201 情報システム利用規程」に違反する行為をした場合には、警告、利用制限、所属部局への通報などの措置がとられることがあります。また、不正利用の発生とその対処について、利用者の氏名を含め公表されることがあります。なお、個々の部局等ネットワークの利用については、それぞれ規則が定められていますので、個別のルールに従ってください。

以下、2 章で具体的に説明しますが、最初の２つは本学情報システムに限らず一般の広域ネットワークの利用でも共通する事項であることに留意してください。

2. 法令および利用規則の遵守

2.1 法令および利用規則に違反する行為

関連する法令としては、憲法はもちろんのこと、刑法、民法、商法をはじめとして、不正アクセス禁止法、著作権法、プロバイダ責任制限法、その他多くのものがあります。また、外国に影響を及ぼすときは外国法の適用を受ける可能性があることにも留意せねばなりません。例えば、次のような行為をしてはなりません。また、他人の犯罪行為の手伝いをしてはなりません。幇助罪または従犯として処罰されることがあります。

(1) 基本的人権・プライバシーの侵害

本学情報システムの利用に限らず、基本的人権を尊重せねばなりません。人種・性別・思想信条などに基づく差別的な発言をネットワークで公開すると、基本的人権の侵害となることがあります。誹謗中傷は名誉毀損で訴えられることがあります。

本学情報システム利用者のプライバシーは尊重されますが、利用者は他人のプライバシーも尊重しなければなりません。他人のプライバシーを勝手に公開してはなりません。私信の無断開示などもそれにあたります。

(2) 利用権限の不正使用

利用権限は正しく使用せねばなりません。また、パスワードを盗まれて不正行為が行われないようにするため、パスワードを厳格に管理することは、システム管理者および利用者の責務です。利用者は、以下のような行為をしてはなりません。

(a) 他者のアカウントを使う

利用者は、他者のログイン名を用いてログインしてはいけません。この行為は不正アクセス禁止法で犯罪とされています。また、利用者は、自分の利用権限(アカウント)を他人に使わせてはなりません。本人のログイン名で他者に本学情報ネットワークを使用させたり、ファイル格納領域などの資源を他者に使わせることもこれに含まれます。

(b) 他者の名前やログイン名をかたって、電子メールを送ったり掲示板に書き込みを行う。

(3) 他組織への侵入

セキュリティホール等を利用してコンピュータシステムに侵入する行為も不正アクセス行為です。本学情報システムの内外を問わず、利用資格のないコンピュータを使用してはなりません。本学情報システムから他組織の情報システムへ不正に侵入した場合、本学全体が外部のネットワークとの接続を切られるだけなく、場合によっては国際問題に発展する可能性があります。また、他組織への侵入を試みるようなことも絶対にしてはなりません。

自分で不正アクセスをしなくても、他人に不正アクセスをさせるような行為をしてもいけません。たとえば、電子掲示板に他人の ID とパスワードを載せるような行為や、友人に自分の ID とパスワードを貸し与える行為などがあてはまります。また、コンピュータウイルスの中には、感染すると他のコンピュータへの不正侵入を試みるものもあります。感染したコンピュータの所有者が知らないうちに、不正侵入や攻撃が行われることになりますので注意が必要です。

(4) 知的財産権の侵害[5]

知的財産権は、人間の知的創作活動について創作者に権利保護を与えるものです。絵画・小説・ソフトウェアなどの著作物、デザインの意匠などを尊重することに心がけて下さい。 著作物の無断複製や無断改変はしてはなりません。例えば、本・雑誌・ウェブページなどに提供されている文章・図・写真・映像・音楽などを、無許可で複製あるいは改変して、自分のウェブページで公開したり、ネットニュースに投稿したりしてはいけません。他人の肖像や芸能人の写真については、肖像権や・パブリシティ権の侵害になることがあります。

(a) 著作権

著作物（小説、音楽、絵画、動画、写真、プログラム、データベース等）には著作権があります。著作権は、著作物の作者が自分の作品を勝手に公開されたり改変されたりすることで気

[5] 引用や，私的利用の場合の例外については，講義時間に余裕がある場合は触れておくのがよいでしょう。特に，引用については，ウェブによる情報発信方法の講義や，レポートの書き方の講義で説明すべきです。

分を害されることのないようにするという働き（著作者人格権）と、著作物を勝手にコピーされたりして作品の価値が下がってしまうということのないようにする働きがあります。ただし、著作物の利用を永久に禁止すると、文化の普及や発展に悪影響を及ぼしますので、一定期間経過後は自由に利用してもよいことになっています。

著作権のある著作物を著作権者の許可なくコピーして他人に渡したり、ウェブページなどで公開すると、著作権法によって罰せられるだけでなく、著作権者から損害賠償を要求されることもあります。著作物の一部を利用したり、改変、翻訳、編曲、翻案することも、著作権者に無断で行ってはいけません[6]。

意識的に公開したつもりがなくても、コンピュータがウイルスに感染していたり、ファイル共有ソフトウェアの設定によっては、著作物が外部に公開・共有されてしまうことがありますので、ファイル共有ソフトを使ってはいけません[7]。また、ディジタル著作物には、コピーできないように制限がかかっているものもありますが、その制限を無効にしてコピーができるようにする装置やソフトウェアを販売したり配布すると、たとえ自らはコピーや公開をしていなくても罰せられることがあります。

(b) 肖像権、パブリシティ権

他人の写真を本人に無断で写真に撮ったりインターネットに公開してはいけません。写真を撮られたり公開されることで、嫌悪感をもつことも多く、人格権の侵害であると考えられるからです。このような行為をすると、肖像権の侵害として訴えられ損害賠償を請求されることがあります。

また、タレントやスポーツ選手など有名人の写真は、それだけで経済的な価値がありますので、パブリシティ権の侵害として、経済的な損失について賠償請求されることになります。

(5) 個人情報・機微(センシティブ)情報の保護

以下に挙げるような、個人情報や機微(センシティブ)情報をパソコンで取り扱う場合は、これらの情報が不必要に流出しないように細心の注意を払う必要があります。

(a) 氏名、住所、生年月日、電話番号、メールアドレスなど、個人を特定できる情報
(b) 病歴、持病、血液型などの医療情報
(c) 家族・親族関係や出身地などの情報
(d) 個人の趣味や嗜好などに関する情報
(e) 借金の有無や残高などに関する情報
(f) 銀行口座番号やクレジットカード番号、健康保険証番号など

(6) 有害情報の発信

違法な情報はもちろんのこと、公序良俗に反する情報や有害情報を発信してはいけません。本学情報システムを用いてわいせつな文書・図画などを公開してはいけません。また、それらへのリンクを提供してはいけません。このほか、次のような情報の公開も、研究上必要な場合を除き、

[6] 受講対象者によっては，著作権法違反になりうる具体例を挙げて説明するのもよいでしょう。
[7] 「利用規程」(A2201)の第十条十五項で、教育研究目的以外での P2P ソフトウェアの利用は禁止されています。

禁止します[8]。詳しくは、「A3204 ウェブ公開ガイドライン」を参考にしてください。

- 情報自体から違法行為を誘引するような情報（銃器や爆発物などの情報、禁止薬物や麻薬の情報など）
- 人を自殺等に勧誘・誘引する情報
- ネズミ講やマルチ商法の勧誘
- セクハラ、アカハラに関する記述を伴うような情報

(7) 本学情報システムのセキュリティ保持に協力する

上記(1)〜(6)のほかに、セキュリティを保持するために、利用者自身が注意すべきことがあります。例えば、コンピュータウイルスを持ち込まない、不信な発信元からのメールを開かない、自分の管理しているコンピュータにウイルス対策ソフトを導入しウイルス検知パターンを常に最新状態に保つ、本学情報システムの故障や異常を見つけたら速やかに管理者に通報するなどが、これに該当します。

大学のネットワークは、多くの管理者によって支えられています。ネットワークでは、一部の利用者の自分勝手な行為や心無い行為によって、ネットワークの利用が著しく制限されたり、大学全体の信用が失われたりすることがあります。ひとりひとりのネットワーク運用への協力が、よりよい教育・研究環境の構築につながることを自覚しましょう。ネットワークの利用中に、ネットワークの安定運用に関わる問題点に気づいたら定められた窓口に報告してください。

2.2 教育・研究目的に反する行為

本学情報システムは、教育・研究活動および運営の基盤として設置されています。教育、研究および運営という設置目的から逸脱する以下のような行為は、利用の制限や処分の対象になることがあります。

(1) 政治・宗教活動

本ネットワークは国立大学法人の財産ですから、特定の団体に利便を供するような活動に用いてはいけません。

(2) 営利活動の禁止

広告・宣伝・販売などの営利活動のためにウェブページや電子メールを用いてはいけません。塾のプリントを作成したりすることもこれに含まれます。

(3) 運用妨害

物的な加害の有無に関わらず、本学情報システムの運用を妨害する行為は禁止します。例えば、本学情報システムに悪影響を与えたり、他の利用者に迷惑をかけるような過剰な利用は避けねばなりません。

[8] 各大学で発信する情報をどこまで禁止しているかに依存します。

(4) 目的外のデータの保持

個人に与えられたファイル領域やウェブページ領域に、教育・研究の目的に合致しないものを置くべきではありません。

3. マナーの遵守

3.1 ネットワークを快適に利用するために

法令や公序良俗に反せず、教育研究目的に合致した利用であっても、注意すべきことがいくつかあります。ここでは簡単に触れておきます。

(1) 品位をもって利用する

本学の構成員としての品位を保って利用すべきことは言うまでもありません。品位に欠けるメッセージの発信は謹んで下さい。

(2) 他人を思いやって利用する

大量のデータを送受信したりすると、本学情報システムを利用している他人に迷惑をかけることになりますから、十分注意してください。メールソフトで、メールの到着状態を調べる時間間隔を極端に短くするなども、そのシステムを共有している利用者への迷惑になりますし、運用妨害になることもあります。また、情報メディアセンターのように共同で利用するコンピュータ設備は、ネットサーフィンやゲームで占有したりせずに、他人に対する思いやりをもって利用してください。

(3) パスワードを適正に管理する

パスワードはあなたが正規の利用者であることを確認するために大切なものです。自分のパスワードを友人に教えたり、友人のパスワードを使ってコンピュータを用いてはいけません。パスワードを教えた人、教えてもらって利用した人の双方が責任を負うことになります。
パスワードの文字列を自分なりに工夫して、自分の頭の中だけに覚えておいて、パスワードを他人がわかるような状態で手帳や携帯電話機などにメモしないことです。他人がパスワードを入力するときには、顔をそむけるという配慮もよく行われています。

アカウントを盗用されても、直接的な経済的不利益は被らないかもしれません。しかし、例えば、パスワードを知られたために、自分のアカウントから他人を侮辱する内容の電子メールが発信された場合、あなたが侮辱行為者として扱われます。また、あなたのアカウントを利用して他の計算機への侵入行為が行われた場合(これを踏台アタックと呼びます)、アカウントを盗用された被害者が、まず最初に犯人として疑われるのです。

強い(破られにくい)パスワードの例：パスワードには、辞書に載っているような単語を避けること、および、英小文字だけでなく、英大文字・数字・記号を含めるようにしてください[9]。

[9] これらの文字を含まないようなパスワードは設定させないようにしているシステムもあります。

(4) 個人情報やプライバシー情報を守る

共用のサーバコンピュータに置かれたファイルには、他の利用者から読まれないようにアクセス権限を設定できることが多いので、適切に設定しましょう。誰からも読める、または誰からも書き込めるという状態は非常に危険です。また、他人のファイルが読めるようになっていたとしても、無断でその内容を見ることはやめましょう。ウェブページ・ニュース・掲示板などに、個人情報やプライバシー情報を提供することも危険につながります。

ウェブページやブログ等に書いて公開すること以外に、情報を保存してあるパソコンやメモリカードなどを放置したり紛失することで、意図せずに情報が流出することがあります。同様に、ファイル共有ソフトウェアを使用している場合に、これらの重要な情報が外部に対して公開されてしまっていることもあります。

懸賞応募のウェブページ等に個人情報を入力する際は十分に注意する必要があります。懸賞を口実に個人情報の収集を行っている場合があり、後日大量の迷惑メールが届くようになってしまうこともあります。

また、パソコンのセキュリティ対策が不十分であると、コンピュータウイルスなどの悪性プログラムに感染し、これらによって情報が自動的に外部に送信されたり、ファイル共有ソフトウェアで共有されることがあります。

いずれにしても、いったん流出した情報は、たとえ後で公開を取りやめたとしても、既に第三者にコピーされていることが多く、回収することは困難です。自分自身の個人情報や秘密情報を流出させてしまった場合には、自分自身に、肉体的、精神的、金銭的な被害が生じますし、他人の個人情報や機微(センシティブ)情報を流出させてしまった場合には､法的に訴えられる可能性が生じますので、十分な注意が必要です[10]。

3.2 メールの利用に関して[11]

・メールの信頼性を過信しないようにしましょう

電子メールは、複数のコンピュータを中継して配送されますので、相手に届かないこともまれですがあり得ます。また、宛て先アドレスが変更になっていたり、迷惑メールと間違われて配送されないこともあります。重要な用件をメールのみに頼るのは避けて、状況に応じて他の手段を併用しましょう。

・あいさつ、自己紹介など、手紙としてのマナーを守りましょう

親しい友人へのメールであれば、用件のみを伝えることもありますが、そうでない人へのメールは、あいさつや自己紹介などを忘れないようにしましょう。

・宛て先を間違えないようにしましょう

メールの宛て先を間違えると、メールシステムに余計な負担をかけ、管理者に迷惑をかけることがあります。また、大切なメールが意図しない人に届き、個人情報などが漏洩すること

[10] ここでは，主に個人的なレベルの個人情報の取り扱いに関する注意を述べています。業務として，一定規模以上の個人情報を収集し取り扱う場合は，個人情報保護法（国立大学法人の場合は、独立行政法人等個人情報保護法）の規定や，本学情報格付け規定に従う必要があります。

[11] 詳細は、A3202 電子メール利用ガイドラインを参照のこと。

もあります。メーリングリスト等で届いたメールに対して返事を出すと、メーリングリストの登録者全員にメールが届いてしまうことがあります。メールを送信する前に宛て先を確認するようにしましょう。

・Cc、Bcc の使い方

本来の宛て先ではない人にメールのコピーを送っておきたいときには Cc (Carbon Copy)や Bcc (Blind Carbon Copy) を使います。メールの返事を書くときは、Cc に書いてある人にも返事を出す必要があるかどうかを考えましょう。メールの宛て先(To)や Cc に書いたアドレスは、メールが届いた人全員が見ることができます。他に誰に出したメールか知られたくない場合は、Bcc に宛て先を書きましょう。

・サブジェクト（題名もしくは件名）をつけましょう

多くのメールが届く人は、サブジェクトを見てメールを整理します。内容を簡潔に表すサブジェクトを付けるようにしましょう。

・機種依存文字、HTML メールに関する注意

記号や罫線、絵文字等の中には、特定の機種でしか表示できないものがあります（ローマ数字（時計文字）や、丸数字（マルの中に数字）など)。また、いわゆる半角カナも使用してはいけません。HTML 形式のメールは、原則として使ってはいけません。これは、受信した側のセキュリティ水準の低下を招くおそれがあるからです。

・添付ファイルに関する注意

添付ファイルを使用する場合は、ウイルス等と間違われないように、どのようなファイルを添付するのか、必ず本文中で説明をするようにしましょう。また、特にサイズの大きな添付ファイルは、メール配送システムに大きな負担をかけます。他の方法がないか検討し、相手先に確認をしてから送りましょう。

・チェーンメール (chain mail)、デマメールの禁止

複数人へのメールの転送を求めるチェーンメール（不幸の手紙などのように、同じ内容を別の人に転送するように要請するもの）は、メールの配送システムに大きな負担をかけ、システム管理者にも迷惑をかけますので、加担してはいけません。メールの内容が重要かつ緊急を要すると思われてもデマの可能性もありますので、よく確認をして、必要であればマスコミ等、他の手段での伝達を考えるようにします。

・迷惑メールやフィッシングメールへの対策

迷惑メールやフィッシングメールが届いても、配送中止の依頼も含めて返事を出してはいけません。メールが確実に届いていることを相手に知らせることになります。迷惑メールやフィッシングメールの本文には特定のサイトへのリンクが設定されていることが多いですが、それらをクリックしてはいけません[12]。また、自分のメールアドレスをウェブや掲示板に掲

[12] フィッシングメールは，その内容が非常に巧妙なものもあり，利用者がフィッシングメールであることに気づ

載すると、迷惑メールが多く届くようになりますから、メールアドレスの取り扱いは慎重に行いましょう。

・PC のメールと携帯電話のメールとの違い

PC のメールでは携帯電話のメールと異なり、すぐに返事ができるとは限りません。たとえ、すぐに返事が来なくても、怒ったりしてはいけません。

・メールアドレスの扱い

メールのアドレスはウェブなどで不用意に公開しないことが望ましいでしょう。しかし、講演会の連絡先等のために公開する必要が生じることもあります。そのような場合には、次のような方法をとるのがよいでしょう。

(i) メールアドレスをロボットで機械的に収集されないように、メールアドレスの全部あるいは一部を画像にしたり、アドレスの一部の@記号を --atmark-- のように別の文字列に置換したりしてウェブに掲載する。

(ii) 講演会への参加申し込みなどのように、掲載期間が限定されている場合は、申込み専用の時限アドレスを使用する。

3.3 掲示板、SNS (Social Networking Service) などの利用

・誹謗・中傷をしない

実名の場合はもちろん、匿名の掲示板であるからといって、誹謗・中傷をしてはいけません。名誉毀損などで訴えられることがあります。相手が特定できなくても、人種差別など許されない発言があります。一般社会で許されないことはネットワークでも許されません[13]。

・フレーミング（炎上）に注意

ネットワークでは、些細なことから議論が白熱し、誹謗中傷の応酬や水掛け論になってしまうことがよくあります。冷静かつ誠実な対応を心掛けましょう。

・掲示板毎のルールに従う

掲示板や、SNS（mixi など）には、そのコミュニティ毎に個別のルールが設けられていることがよくあります。いくつかの記事を読んで雰囲気を理解してから、発言するのがよいでしょう。

3.4 ネットワークの過度の利用による悪影響

パソコンや携帯電話によるネットワーク利用は便利ですが、長時間にわたって過度な利用をすると、以下にあげるように心身面に様々な影響が生じることが指摘されています。十分な休息と適度な運動を心掛けましょう。

・対人関係などコミュニケーション能力の阻害

かずに対応してしまう危険性もあるので，必要に応じて具体例をあげて解説を行うとよいでしょう。

[13] 匿名の掲示板等であっても，捜査機関等からの要請があれば，ログ情報から利用者が特定されます。

・学業成績の低下
・生活リズムが不規則になることによる心身障害
・姿勢や視力への悪影響

4. 情報セキュリティの基礎的知識

4.1 インターネットのしくみ（IP アドレス、URL、HTTP）

(1) IP アドレス

PC をインターネットに接続して利用するためには、その PC をインターネット上で一意に識別できるよう、住所や電話番号に相当する「アドレス」が必要となります。インターネットでは、「IP アドレス」と呼ばれるアドレス体系を利用します。具体的には 32 桁の 2 進数で表現されますが、それでは分かりづらいのでこれを 8 ビット毎に切って 10 進数で表現します[14]。つまり、「192.168.0.1」のように 0～255 までの数字を 4 つ、ピリオドで区切って並べたものになります（図１参照）。

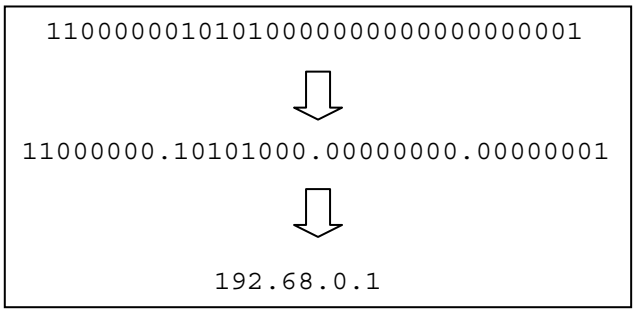


図１：IP アドレスの例

このような IP アドレスは基本的にインターネット上で固有のものでなければなりませんが、様々な理由から「プライベート IP アドレス」と呼ばれるものも利用されています。

インターネットにおいて、データは「パケット」という形式により共有回線上でやりとりされます（パケット交換方式）。パケットは、元々送信しようとしていたデータ（例えば電子メールのデータ）にヘッダ（小包の表書きのようなもの）等を加えたものです。

すべてのパケットについて、ヘッダに発信元および宛先の IP アドレスが書き込まれます。従って、基本的にインターネットにおける通信は匿名ではないと考えるべきです。また、たとえどのような暗号化を行ったとしても、「どのコンピュータから情報が発信されたか」「どのコンピュータ宛てに情報が送信されたか」という記録は残ります。暗号化しなければ基本的に万人が観察可能な状態で通信が行われますので、インターネットは安全であることを仮定することができない通信手段ということができます。電子メールにしてもウェブにしても、せいぜいはがき程度の秘匿性しか持ち合わせていません。機密性の高い情報は必ず暗号を利用するべきです。

[14] IPv4 の場合。

(2) ドメイン名

さて、このような IP アドレスは覚えるのが面倒です。1 個なら覚えることができるかもしれませんが、必要な数だけ覚えるのは実用的ではありません。そこで、コンピュータにニックネームを与え、そのニックネームを IP アドレスに変換してやるシステムを考えます。これを DNS（Domain Name System）と呼びます。これにより、例えば www.kantei.go.jp という「ドメイン名」を IP アドレスに変換することができます。ドメイン名は階層的な構造を持っており、ある程度類推をすることもできるといった特徴があります。

このドメイン名は安全なウェブの利用で重要なポイントとなりますので、どのドメイン名がどの企業や大学等の組織（のサービス）のものであるか、重要なものについては覚えておくようにしましょう。特に金銭や個人情報等の取り扱いに注意が必要な情報のやり取りを伴うサイト、つまり銀行等の金融機関、ショッピングサイトなどについては重要です。

(3) URL と HTTP

ウェブでは、URL（Uniform Resource Locator）という形式で情報の入手元を指定します。これは、図２のような構造を持ちます。

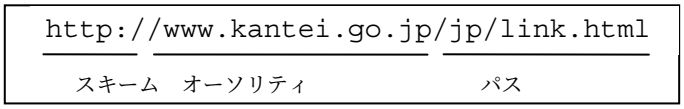


図２：URL の構造

一番左の「http://」が「スキーム」で、情報（正確にはリソースといいます）にアクセスするための方法を指定します。次が「オーソリティ」で、そのリソースを管理しているコンピュータを指定します。オーソリティにはドメイン名や IP アドレスを利用することができます。最後がパスで、そのオーソリティのどこにリソースがあるのかを指定します。ここでは「jp」というディレクトリ（フォルダ）の中にある「link.html」というファイルを指定しています。

ここで利用されているスキームは HTTP（Hyper Text Transfer Protocol）です。これは文字通り「転送」のためのプロトコル（決まり事）です。ウェブブラウザは URL に書かれているオーソリティにアクセスし、パスをたどってファイルを取得して表示等を行います。つまり、ウェブブラウザは基本的にダウンロードのためのシステムであるということができます。ここは重要なポイントです。ウェブはテレビ放送のように一方的に送りつけられている情報を受動的に画面に映しているわけではなく、あくまでも自分でリクエストした情報をダウンロードしているのです。IP アドレス等の情報がリクエスト先に残りますし、自分が望まないデータ（コンピュータウイルスなど）をダウンロードしてしまうこともあり得るのです。

HTTP では、ダウンロードだけでなく情報を送信することもできます。これによって、通信が双方向となり、より様々なサービスを受けることが可能になりますが、逆に言えばウェブを通じた自覚・無自覚の情報漏洩というものも起こりえます。特にオンライン・プライバシーについては、「あなたのオンライン・プライバシーを守る 12 の方法[15]」を参照して自衛を心がけてください。

[15] http://www.eff.org/Privacy/eff_privacy_top_12_jp.html

4.2 コンピュータウイルスとワーム、Spyware（感染兆候と予防対策、事後対策）

ソフトウェアは人間に役立つように設計されているものですが、一般的に害を及ぼすことを目的に作成されたソフトウェアをマルウェア（malware）と呼びます。マルウェアにはコンピュータウイルス、ワーム、スパイウェア、アドウェアなど、広範な種類のソフトウェアが含まれます。

コンピュータウイルスは、自己伝染機能（自己を複製し他のコンピュータに感染を広げる機能）、潜伏機能（特定の条件がそろうまで活動を待機する機能）、発病機能（データの破壊・システムを不安定にする・バックドアを作成するなどの機能）を特徴としたプログラムです。コンピュータウイルスには、ウイルス、トロイの木馬、ボットなどがあります。

ウイルスは宿主となるプログラムに寄生するのが特徴で、様々な不利益（ハードディスクを消去するなど）をもたらします。トロイの木馬は一見有益ないし無害に見えるプログラムが、実は不正な動作をするというものです。スパイウェアは、トロイの木馬とほとんど同じですが、特にユーザに関する情報を収集するのに利用されるものをいいます。

ボットは、メールやネットワークを通じて感染範囲を広げ、感染したコンピュータにバックドア（正規の手続きを踏まずに内部に入る事が可能な侵入口）を仕掛けるというものです。このバックドアにより感染したコンピュータは不正に操られ、著名なサイトなどを（数千、数万台の PC から）一斉攻撃するのに利用されます。

ワームは独立したプログラムであって宿主を必要としないところがウイルスとは異なるとされていますが、ネットワークを媒介として増殖し、コンピュータやネットワークに過大な負荷をかけます。

いずれにしても感染経路、ファイルの種類（アプリケーション、Microsoft Office のファイル、ウェブ Cookie など）、被害など、どのような側面で切ってもマルウェアには様々なものがあり、この対策だけ取っていればよいということはありません[16]。ここでは IPA（情報処理推進機構）による「パソコンユーザのためのウイルス対策 7 箇条[17]」を紹介しておきます。

最も重要なのは、アンチウイルスソフトウェア（ウイルス対策ソフトウェア）を導入しておく、ということです。アンチウイルスソフトウェアには、無償で利用することができるものもあります。次の 3 種類のソフトウェアを紹介しておきますので、検討して「自分の」パソコンに導入しておきましょう(無料で利用できる条件として、非営利の条件がついているものもありますので注意)。

- avast! [18]
- Google™ Pack[19]
- AVG® Anti-virus Free Edition[20]

これらのソフトウェアを導入しても、ウイルス検出のパターンファイルなどを定期的に更新しなければ意味がありません。これらのソフトウェアはいずれも自動でパターンファイルを更新す

---

[16] マルウェア(malware, malicious software）とは，悪意的なソフトウェアという意味の造語で、ネットワークやコンピュータに何らかの被害をもたらすように作られたソフトウェアの総称。

[17] http://www.ipa.go.jp/security/antivirus/7kajonew.html

[18] http://www.avast.com/jpn/download-avast-home.html

[19] http://pack.google.com/intl/ja/pack_installer.html （Norton Security Scan および Spyware Doctor™ スターターエディションをインストールすること）

[20] http://free.grisoft.com/

るように設定することができますので、良く確認しておきましょう。

4.3 フィッシング、架空請求等

フィッシング（phishing）は「釣り」の fishing にかけた言葉ですが、ウェブや電子メールを利用した詐欺の一種です。典型的には、「ユーザアカウントの有効期限が近づいています」であるとか「登録情報の確認をしてください」などといった電子メールが届きます。電子メールにあるリンクをクリックすると本物そっくりのサイトが表示されるのですが、実際にはそれは犯罪者が仕立てたニセのサイトで、そこで銀行の口座番号や ID、パスワード、クレジットカードの番号等の情報を収集しているというものです。

ポータルサイトと呼ばれる統合的なサービスを提供しているサイトでは、オークションや小口決済機能を 1 つの ID で統合しているケースもあり、ID やパスワードを盗まれることで何重にも被害に遭い、また間接的に加害者になるケースもあるようです。

また、電子メールで利用してもいないサービスについて料金を請求されたり、またその請求が恐喝的な手口で行われることもあるようです。

このようなフィッシングや架空請求への対応は、次のようなものを挙げることができます。

1. ウェブブラウザのフィッシング詐欺対策機能を有効にすること
2. 正しい電子メールの知識を持ち、HTML メールを利用しない、リンクを安易にクリックしないこと
3. ウェブページの URL（特にオーソリティのドメイン名）を良く確認すること

フィッシング詐欺は様々な手口で行われていますが、最終的にはウェブを通じて情報収集が行われることが多いため、ウェブの安全な利用が鍵となります。この点については、産業技術総合研究所の情報セキュリティ研究センターによる「安全なウェブサイト利用の鉄則[21]」を参照してください。ショッピングや銀行等だけでなく、ウェブを利用していて個人情報を入力しなければならないような場合は、とにかく慎重になる必要があります。

インターネットが普及するにつれ、インターネット上の経済活動も活発に行われるようになっており、それにともなって犯罪者もまたインターネットを活動の場にするようになっています。

4.4 ファイル交換（情報漏洩、著作権）

Winny などのファイル交換ソフトウェアを通じた情報流出は、もはやニュースになっても驚かなくなるほど一般的になりました。問題の背景にあるのがコンピュータを利用する者の知識と注意の不足、そしてなによりも意識の欠如であるのは明らかです。

驚くべきことに、「Winny そのものは悪くない」「刃物で殺傷事件があっても刃物が悪者扱いされないのと同様に…」といった議論が一部で行われているようです。しかし、Winny ネットワークに一度流出した情報は、完全に消去するのが非常に難しい構造になっており、それはユーザが増えれば増えるほど難しい構造になっています。Winny ネットワークに参加するということは、すなわち著作権侵害に加担することと言ってもいいのが現状であり、それが学問の府から行われて良いはずがありません。P2P そのものは有望なフレームワークであると考えられますが、Winny そのものについて利用を正当化する理由は１つたりとも存在しないことを知るべきです。

[21] http://www.rcis.aist.go.jp/special/websafety2007/

なお、Winny には「Antinny」や「山田オルタナティブ」その他の、Winny を狙ったウイルスが存在する他、Winny そのものにもバッファオーバーフローという基本的な脆弱性が存在します[22]。Winny の開発が止まっている以上、Winny を使い続ける理由はありません。

Winny 以外のファイル共有ソフトウェアであっても同じことで、その利用には常に著作権侵害と情報漏洩がつきまといます。本学では、利用規程で Winny などの P2P ソフトウェアの利用を禁じていますので、それらのソフトウェアを利用してはなりません。

4.5 情報発信

インターネットは、だれもが気軽に情報発信ができるのがその特徴の 1 つです。以前から気軽に行うことのできた情報発信ですが、ブログや Wiki、匿名掲示板などの普及によって、敷居の高さはより低くなっています。

インターネットへの情報発信として注意しなければならないのは、それが不特定多数への情報発信であることが多く、またコンピュータを利用しているため情報の再利用が簡単である、ということです。特定少数への発信であったとしても、一度自分の手を離れた情報がどのように再利用されるかコントロールするのは難しいですから、情報の発信にあたっては、特に慎重になってください。

特に慎重を期すべきなのは、個人情報です。自分の個人情報以上に、他者の個人情報の扱いについては、極めて慎重に行ってください。

また、文字のみのコミュニケーションでは真意が伝わらずに嫌な思いをすることもあるでしょう。基本的には情報の送り手としては真意が伝わるよう厳密に、誠意を持って対応し、情報の受け手としてはおおらかな気持ちで接するのが基本です。インターネット上のコミュニケーションで嫌な思いをしたら、相手が誰であれ、誹謗や中傷をやり返すのではなく、単にその場から離れるのが良いでしょう。

なお、近年の傾向として、インターネット上の情報発信について責任を問われるケースが増えています。インターネット上のソーシャルネットワーキングサイトの mixi で、学生が飲酒運転を告白、社会的に非難を浴びたのは記憶に新しいところです。真実かどうか別として、無責任あるいは反社会的な言説については社会的な制裁が加えられる可能性が高くなっています。またそうなった場合に、インターネットは発信者を特定するのがそれほど難しくないことから、民事や刑事上の責任すら負う可能性があることを自覚しておく必要があります。

インターネットというすばらしい道具を得て、私たちの情報空間はこれまでとは桁違いに広いものとなりました。この広大な情報空間にどのように対応していくのかということを、技術的な面から、また社会的な面からも学ぶ必要があるのです。

[22] http://jvn.jp/jp/JVN%2374294680/index.html
http://www.ipa.go.jp/security/vuln/documents/2006/JVN_74294680_winny.html

A3302 教育テキスト作成ガイドライン（システム管理者向け）

セキュリティ関連教育は、大学の特性を踏まえて行う必要があります。本文書では教育テキスト作成ガイドラインとして、システム管理者が踏まえるべき大学の特性とセキュリティ関連教育事項の関係を必要最小限の項目に絞って述べます。さらに、部局や情報センター内にいるシステム管理者が情報サービスの維持・運用・管理も行う場合に必要な心構えや学習項目についても言及しています。なお部局での情報セキュリティ管理は、専門の担当部署や担当者が部門総括責任者や部門技術責任者として担当する場合と、システム管理者がこれらの役割を兼務する場合とがあります。このガイドラインの内容は部門技術責任者の役割を兼ねる可能性のあるシステム管理者を対象としたものですが、情報セキュリティ管理上の役割に応じて必要となる知識は変わってくることに留意してください。

解説：教育項目としての諸規程については、高等教育機関の情報セキュリティ対策のためのサンプル規程集（以下、本サンプル規程集：国立情報学研究所 ネットワーク運営・連携本部国立大学法人等における情報セキュリティポリシー策定作業部会と電子情報通信学会 ネットワーク運用ガイドライン検討ワーキンググループ）そのものが最良のテキスト例である。必要に応じて参照願いたい。

第１章　概論

1.1 概要

大学の使命は、学生に質の高い教育を提供することと、学問における未知の問題の解決に取り組むことです。その目的を果たすために、大学には多くの資産があります。ここで資産というのは、建物や実験設備に代表される物理的なもの、教員や職員といった人材、そして、大学が所有するさまざまな情報のことを指します。ここでは、情報資産について考えてみたいと思います。大学が所有する情報資産には、例えば次のようなものがあります。

- ● 成り立ちが大学に属するもの
  - ○ 教員、大学院学生の研究・教育内容
  - ○ 学生、教員、職員の個人情報（氏名、住所、成績、履歴、業績など）
- ● 購入やライセンスの取得により使用できるもの
  - ○ 図書館や各研究室にある書籍
  - ○ コンピュータルームにある PC に内蔵されているソフトウェア

現在、大学の情報資産の多くはコンピュータで取り扱うことができるようになっていて、その中のいくつかはインターネットを通じて外部に公開されています。しかし、公開に適さない情報資産は逆に、インターネットでは入手できないようになっています。もし、大学の情報資産の消去や、外部に提供することが禁止されている情報資産を誰かが誤って提供してしまうと、大学の運営に支障を来すことがあります。このようなことは、情報以外の資産と同じように考えてください。大学の情報資産を不正に消したり書き換えたりすることは、大学に備え付けられている備

品を破壊したり、私用にすることと同じで、犯罪です。

本大学の教員、および職員は国立大学法人の就業規定にしたがって大学の資産を管理する必要があります。そこでは、大学の資産が外部に流出したり、消失したりしないように、細心の注意を怠ってはいけないといえます。

法律や公序良俗に反する行為以外にも避けるべき行為があります。例えば、コンピュータやネットワークの正常な運用を阻害する行為を避けるべきです。但し、個々の環境によって、避けるべき行為は様々です。

学内に設置してある各種の情報機器ネットワーク機器および通信網は、大学という教育・研究機関に所属するものです。また、大学から利用資格として通知されたアカウントも、本学における教育・研究目的に必要不可欠であるからこそ全員に付与されています。したがって本学の教育・研究目的に著しく反するような形で、これらを利用すべきではありません。

近年、インターネットを始めとする情報技術の発達に伴い、大学が保有する情報資産の利用・流通にも変化が現われています。たとえば従来では、紙の学生証による本人確認によって交付されていたさまざまな証明書が、IC カードなどを利用した学生証によって本人宛に交付されるようになり、また、データベースの活用のおかげで、そのデータの正確性も確保されるようになりました。

電子情報の特徴の一つとして、「複製の容易さ」と「複雑な解釈」を挙げることができます。前者は、情報漏洩や著作物の不正複製の際は「悪い特徴」として捉えられます。一方、後者は暗号などの仕組みを利用した解釈を成立させる「よい特徴」として捉えることができます。

そして今後も、暗号技術、ネットワーク技術などさまざまな情報技術が高度に発展していくことが見込まれます。情報技術の発展は、システム管理者にとっては防護技術の進化に寄与しますが、一方でネットワーク犯罪者にとっては犯罪技術の進化に寄与しています。

情報に関する技術が、他の技術ともっとも異なる様相を見せるのは、変化の速さです。ドッグイヤー・マウスイヤーという言葉があるように、情報技術は他の技術の数倍の速さで変化します。新しく開発された技術も、わずか数カ月で全く役にたたなくなることがあります。

システム管理者は、このように、犯罪防御も、犯罪行為も技術革新によって日々変化していて、そのなかで、安全な情報サービスの提供に努めるために何ができるかを考える必要がある、ということができます。

1.2 大学で守るべき情報

大学にある情報資産を、事務部門と教育研究部門の２つに分けて考えてみます。

事務部門には、教職員や学生の個人情報があります。個人情報には、氏名や住所などの基本的な個人情報の他に、研究活動・学習活動に伴う個人評価、健康状態、給与・学費の状況なども含まれます。また、独立行政法人として契約や調達に関わる情報を保有しています。

一方、教育研究部門としては、大学が持つ研究情報資産、具体的には未公開の特許情報や、大学として企画した著作物などの知的所有権・知的財産があります。各部門の管理責任者は、自らの部門にどのような情報資産があるかを把握しておく必要があります。

1.3 大学において守るべき事項と特徴

研究のみを目的として成立している研究機関と異なり、大学の場合は、教育機関としての側面を同時に持ち合わせています。研究を行う教員と学生、教育を受ける学生、研究に参画する企業の研究者など、大学にはさまざまな立場の人間が出入りします。また、頻繁な人事異動、入学・卒業があります。そのため、大学にはさまざまな人が自由に出入りし、その状況調査も簡単ではありません。一方で、歴史的な経緯で、大学には学問の自由、自治権があり、また、大学の研究成果は広く公表されるべきだという考え方もあります。

このような状況を前提にして、情報資産を適切に運用するには、大学情報の機密性を十分に確保する必要があります。すでに述べたように、最新の暗号技術を利用して、多彩な情報閲覧権限・編集権限を設定する必要があります。

システム管理者は、自部局の情報閲覧権限や編集権限を十分調査し、適切に設定を行う必要があります。

なお、インターネットに接続をして、さまざまな情報を流通させる場合には、ネットワークセキュリティについて注意する必要があります。この場合の注意点は、大学の特殊性はありません。サーバ攻撃（DOS、ポートスキャン、不正侵入、ホームページ書き換え）、ウイルス・迷惑メール、P2P ファイル交換ソフトなどの不正アプリケーション使用による情報漏洩、踏み台、物理的脅威（盗聴、侵入、操作ミス、不正）などの対策が必要です。

1.4 大学のセキュリティ対策の特徴

セキュリティ維持の基本として大学全体のセキュリティポリシーが定められます。さらに大規模大学で部局ごとに運用組織があるようなケースでは、各部局の事情に応じて部局毎に実施規程等として詳細化されることがあります。部局総括責任者にとって、セキュリティポリシーおよび実施規程間の矛盾に配慮することは重要です。全学のポリシーと、ある部局の実施規程等が矛盾することのないように、全学ポリシーの作成作業には全部局の部局総括責任者が参加すべきです。部局総括責任者は部局間の実施規程等の違いを部局の事情とともに理解し、それに起因する問題の解決に向けて努力すべきです。さらに、全学と各部局で実施規程等が異なる原因について検討する必要があります。多くの場合は、部局技術責任者の役割を担うシステム管理者のスキルに差が大きいため、スキルを身に付けた部局の提案が全学のポリシーに反映される傾向があります。また、附属機関として病院などがある部局と、そうでない部局では、利用者の個人情報の取扱が異なることがあります。このようなセキュリティポリシーが適用される環境の差を認識し、全学の情報セキュリティポリシーに、部局毎の事情を矛盾なく追加できるようにしておく必要があります。

このような努力を有効なものとするため、セキュリティインシデントに対応できる全学の組織を予め整えておくことが重要です。組織を整えておかない場合にはインシデントに対する迅速な対応が困難となることもあります。本学では全学総括責任者のもと関連組織が整備されています。

また、大学のように、最先端の情報技術を利用しようという組織の場合、潜在的な脅威となる項目を発見することが困難であり、さらに、研究開発においては、リスクのように確定していない(未知の)脅威に対する対策費用を計上することも簡単ではありません。求められるのは、情報技術に対する正しい理解と、技術が原因で発生した脅威には、(経費ではなく)技術をもって対応する

という姿勢です。

なお、大学では、学問の自由・教員の研究に関するプライバシーの確保があるために、学内のパソコンをインターネットに接続する際も、ファイアウォールの設置を嫌う傾向があります。その結果として、管理が行き届いていないパソコンがインターネットに直接接続され、ウイルス感染などの問題を引きおこします。学問の自由と、ネットワークにおけるパケットフィルタリングの違いについても、システム管理者は知っておく必要があるといえます。

ここで、情報セキュリティポリシーを作成する際に必要となる情報リスクマネジメントの注意事項を記します。

1. まず、情報セキュリティの確保を行う目的と場所を明らかにすることです。その際には、学内にある情報資産をすべて調べあげ、どのような脅威がどの程度の確率で発生するかを予想することが必要です。また、脅威に対する被害を予想することも必要です。これをアセスメントといいます。
2. 次に目的に応じた手法を計画(Plan)し、計画通りに実施(Do)し、そして実施がうまく出来ているかを監査(Check)する必要があります。この流れを PDC と呼びます。
3. 一度 PDC を実行したら、再び PDC を行います。これを繰り返していくことで、日々の情報セキュリティの確保を行えるようになります。

各項目においては、制度・組織の見直し、技術的な解決、教育(研修)による対応などを同時に進める必要があります。また、予算確保や、規約・規則作成も行う必要があります。

規約・規則の項目を作成する場合も、

a. インシデント（事故）を防ぐための項目
   例: 鎖錠、パスワード設定、フィルタリング
b. インシデントがあっても復旧可能にするための準備項目
   例: バックアップ、暗号化、予備電源
c. インシデント発生時の対応項目
   例: 緊急連絡網、倉庫在庫との交換
d. インシデント発生後の始末項目
   例: 報告(お詫び)、被害算出、保険の検討、規則改正

のすべてを考える必要があります。

なお、近年、大学同士で図書館利用や単位互換、連合大学院、入試問題の共通利用なども行われています。また、大学においては企業との共同研究が活発化しています。そのため、情報セキュリティポリシーを作成した場合は、他機関や企業との矛盾点をうまく解決できるようにしておくべきであるといえます。

システム管理者が情報セキュリティポリシーについて学ばなければならない項目を、別の観点で整理してみます。現実の人間社会では、匿名性を確保することは簡単ではありませんでした。会えば必ず顔がわかり、電話をかければ声が聞こえ、文字を書けば筆跡をたどることができました。しかし、個人の情報がデータとして簡単に複製・加工可能になった現在、私たちは簡単に匿名性を確保することができます。その結果、匿名性を利用したさまざまな犯罪行為が行われるようになりました。

社会において人々が行為の自由を権利として行使できるのは、自由が、その行為に伴う責任と不可分であるからです。ところが、匿名性は、行為と責任を切り離します。情報セキュリティポリシーは、このような匿名性を支える技術の使用を禁止することで、本当の意味での自由な行動

を保証するということができます。具体的には、情報資産利用の目的を明らかにし、ID の貸し借り、パスワードの共用、盗用などを禁止する情報セキュリティポリシーを作成する必要があります。大学は学術研究の場所です。商業的な利益に左右されることなく、真実・科学のために活動をすることが許されている場所であるともいえます。だからこそ、おかしな商業主義や、科学的な検証をうけていない態度に惑わされることなく、活動を行うことができます。情報セキュリティ教育についても同じです。情報セキュリティ教育が目指すべき学問的な健全さを追求し、他の組織の見本となる活動を行うべきであるといえます。

また、工学・経営学・教育学の研究者が関わることが可能ならば、その観点からも情報セキュリティ教育を評価し、改善するべきでしょう。システム管理者は、自身として教育者である場合と、自身は教育者でない場合があります。前者の場合は、自らが利用者(おもに学生)への教育に関わることになりますが、後者の場合は、自らが利用者教育を担当することはありません。しかし、後者の場合であっても、利用者とのやり取りの中で情報セキュリティ教育に相当する行為を行わざるを得ない場合があります。

そこで、利用者教育を担当する人(おもに情報リテラシー系の授業担当者)と連絡をとり、大学・各部局における情報セキュリティ教育の内容に、各部局固有の事情・内容・制限を反映させることが必要となります。

ある時にある仕組みや制度が成立しても、情報技術の変化は大変激しいので、その仕組み・制度が急速に陳腐化し利用されなくなる、ということがよく起こります。システム管理者は、情報技術・情報通信技術などに関する様々な内容を、

「技能」
　時間とともに変化する、商品知識的な内容。

「技術」
　時間とともに変化することは少ないが永遠の真実とはいえない内容。

「科学」
　時間とともに変化することがほとんどない内容。
　その知識が直接、情報セキュリティに役に立つことはないが、
　情報セキュリティの根幹をなす原理・原則である。

に分類しておき、それぞれを必要に応じて点検する計画を立てる必要があります。また、その中でも技能として分類される内容は時間とともに変化するため、その詳細を学ぶことが常に必要となります。ちょうど、携帯電話の新機種を購入すると、たいていの場合は使用方法が大きく変わっていて、そのため、取り扱い説明書をよく読まなければならなくなるのと同じです。

第１章では、情報セキュリティに関する概論を述べました。その内容は、上位の役割を兼ねる可能性のあるシステム管理者を想定し、情報セキュリティに関して知っておくべき知識と態度について、「科学の立場・教育学の立場」から述べたものです。ここでいう「科学の立場・教育学の立場」とは、情報科学のことではなく、「情報セキュリティの学習」という作業全体を科学的に分析した結果から得られた内容ということです。すなわち、「情報セキュリティを学ぶということはどのようなことか」「情報セキュリティを身に付けるとはどのようなことか」という内容を科学的に考察したものといえます。

個々の内容については、続く第２章以降で取り扱います。

第２章　ネットワークサービス・システム

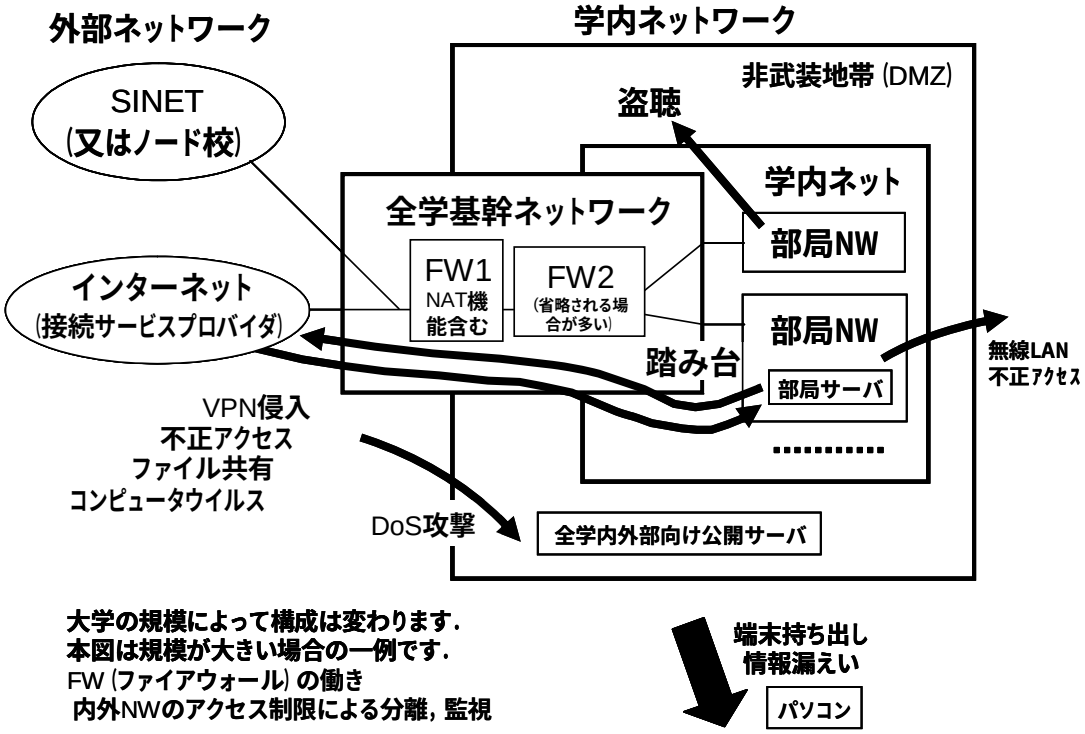


図1　大学ネットワークの構成例

図１に大学ネットワークの構成例を示します。図１は大規模な場合の例ですが、大学の規模によってネットワーク構成は変わってきます。小規模な場合には部局が直接インターネット（プロバイダ）と接続する場合もあります。ある規模以上では多くの場合、部局内ネットワークと全学基幹ネットワークの２階層構成になります。

基幹ネットワーク、部局ネットワークの入り口にはセキュリティを確保するためのファイアウォールが置かれます。大学から外部への接続は、インターネット（SINET または SINET 配下のノード校への接続を含む）によってなされます。

高いセキュリティレベルを持つ学内ネットワークと外部ネットワークの間に内外共用向けサーバ等をおく中間的なセキュイリティレベルを設ける場合があります（非武装地帯)。中小大学では十分なグローバル IP アドレスを持たないため、アドレス変換(NAT)機能を持ったファイアウォールを用いることが一般的です。このような大学ネットワークに対するセキュリティ攻撃は、例えば次のような多様な形で行われます。

- ネットワークの物理的盗聴
- 媒体、端末を経由した情報漏洩、ウイルス感染
- ガードの緩い無線 LAN への不正アクセス
- 外部向けサーバでは簡易なパスワードの走査（スキャン）に発見とその利用
- ファイル共有ソフトによる情報漏洩
- メールについているウイルスを介した攻撃

2.1 コンピュータネットワークの構成

大学におけるコンピュータネットワークは、通常以下の要素によって構成されます。

1) LAN: イーサネットハブ、無線基地局とそれに接続するサーバ・クライアント等から構成
2) 部局ネットワーク: 1 つ以上の LAN をルータで接続したネットワーク
3) 全学基幹ネットワーク: 学内の部局ネットワークと学外のインターネットを接続するネットワーク

大学ネットワークのセキュリティを維持するためには、ネットワークに接続する各機器においてセキュリティを確保すると共に、ネットワークを相互に接続するルータにおいてファイアウォールによりセキュリティポリシーに応じたアクセス制限が必要です。

地域交流センタ、後援会、宿舎、インキュベーションセンタなどの大学外部の関連者がネットワークを利用する場合、学内ネットワークとの接続にファイアウォールを設置することにより、学内利用者と異なるアクセス制限が可能となります。

2.2 ファイアウォール

ファイアウォールはネットワークセキュリティ維持に欠かせない要素です。システム管理者はファイアウォールの設置箇所、ファイアウォールのアクセス制限ルールを適切に設定しなければなりません。必要に応じて、ネットワーク間を接続するルータにファイアウォールを設定します。ファイアウォールでは、学内ネットワークへの攻撃を防ぐと共に、学外ネットワークへの意図しない通信 (学外への攻撃、迷惑メールの発信、P2P ファイル共有ソフト等) を防ぐ必要があります。また、IP アドレス詐称による攻撃を防ぐために、Reverse Path Filtering (RPF) を行うことも考慮すべきです。

Network Address Translation（NAT）は外部のグローバルアドレスネットワークから内部のプライベートアドレスネットワークへ直接通信できなくするために、簡易ファイアウォールとして機能しますが、NAT 越え技術、外部への意図しない通信には対応できないため、注意が必要です。

2.3 DMZ（Demilitarized Zone: 非武装地帯）

学内ネットワークと学外ネットワークの間に DMZ を設けて、そこに学外公開サーバを設置することがあります。DMZ から学内へのアクセス制限を適切に運用することで、例えば学外公開サーバが攻撃者に乗っ取られた場合においても学内ネットワークを守ることが可能となります。

2.4 VPN （Virtual Private Network）

大学が複数拠点にあり、拠点毎のネットワークがインターネット経由で接続されている場合があります。この場合、拠点間に VPN **を設定することにより、拠点間通信が拠点内通信と同様のセキュリティで提供できます。また、学外にいる組織構成員が** VPN **を使用することにより、安全に学内サービスを利用することができます。ただし、**VPN **のセキュリティを維持するために、システム管理者は** VPN **接続鍵の有効期限設定、紛失時の無効化設定等を行う必要があります。**

第３章 ネットワークを構成する要素技術

ネットワークセキュリティを維持するためには、ネットワークを構成する技術要素を理解することが必要です。ここでは、基礎的なネットワーク技術要素の項目を列挙します。詳細な内容については、それぞれの技術要素の文献を参照してください。ネットワーク技術は進歩の激しい分野ですので、最新技術の動向を常に把握する必要があります。

なお、ここに示した要素技術についての教科書や文献は豊富に提供されていますので、詳細はそれぞれの教科書・参考書を参照してください。

3.1 IP アドレス体系

IP アドレス体系を構成するための技術要素の例を以下に示します。IP アドレスの確保や管理は大学内の情報資産管理の一環として重要です。IP アドレスにおけるクラスの概念などを熟知しておく必要があります。

- IPv4 / IPv6
- グローバルアドレス / プライベートアドレス / リンクローカルアドレス
- Classless Inter-Domain Routing (CIDR) / Variable Length Subnet Masks (VLSM)
- well known port

3.2 パケットフィルタリング

パケットフィルタリングを構成するための技術要素の例を以下に示します。パケットフィルタリングはアクセス制御に使われる重要な概念です。

- アクセスコントロールリスト (ACL)
- IP アドレスフィルタリング
- Reverse Path Filtering (RPF)
- ICMP
- プロトコル・ポート番号フィルタリング
- IP フラグメント
- ステートレスフィルタリング / ステートフルフィルタリング
- 流量制限

3.3 NAT と NAT 越え（超え）

NAT を構成するための技術要素の例を以下に示します。NAT は大学外部向けの IP アドレスであるグローバル IP アドレスと、大学内部向けの IP アドレスであるプライベート IP アドレスを変換する機能です。グローバル IP を持たないものが、サーバ機能を外部に提供する場合や P2P 通信を行う場合などに「NAT 越え」が必要となります。NAT 越えは大変便利な機能ですが、セキュリティホールを招く恐れもあります。したがってネットワークの管理者・システム管理者は、利用実態、関連インシデントなどに気を配る必要があります。また、NAT をおく場合には、インシデント対応を容易とするためセッションログをとるようにするのが好ましいと言えます。

- Network Address Translation (NAT)
- Network Address Port Translation (NAPT) / IP マスカレード
- NAT 越え
  - 静的マッピングテーブル
  - Universal Plug and Play (UPnP)
  - TCP connection reversal
  - UDP hole punching

3.4 MAC（Media Access Control）アドレス

MAC アドレスはイーサネットワークを構成する機器に付けられたユニークなアドレスであり、機器管理の基本情報の一つです。ネットワークの管理者・システム管理者は概念を熟知する必要があります。MAC セキュリティの例を以下に示します。

- MAC アドレス
- MAC アドレス認証

3.5 無線 LAN

無線 LAN を構成するための技術要素の例を以下に示します。安易に無線 LAN を設定することは、ネットワークにおけるセキュリティホールを生じさせる原因となります。ネットワークの管理者・システム管理者は利用実態、関連インシデントなどに注意する必要があります。

- 無線 LAN の標準規格
- 認証・暗号化
- ESS-ID
- WEP / WPA / IEEE802.1x / IEEE802.1i
- RADIUS 認証

第４章　セキュリティサービス・システム

大学においてもセキュリティに対する脅威が拡大し、情報通信システムのセキュリティ強化が必須となっています。セキュリティを危うくする原因（以下、セキュリティホールと称す）はあらゆる所に存在するため、セキュリティの維持はあらゆる観点から行われる必要があります。情報通信システムを中心に考えると、利用者の意識の低さ、利用組織・体制の不備、物理媒体を含めた情報管理の不備、組織情報通信システムを囲う物理環境の脆弱性、情報通信システムとしての論理的な脆弱性などが全て関連します。どこかにセキュリティホールがあれば、一部だけ強固なセキュリティを維持しても意味がありません。このことを念頭に置きつつ、以下では情報通信システムとしての論理的な安全性を確保することについて述べます。

システムとしての論理的な安全性を確保するために必要な対策（及び関連技術）は以下の通りです。それぞれの対策はそれぞれに対応する最新の技術に立脚しなければなりません。

①自己を正しく識別し正しく情報を伝え、他者を正しく識別し正しい情報を受け取るための対策

（成りすまし防止、改竄防止、事後否認防止、盗聴防止、電子証明書）

②迷惑を受けないための対策

（フィッシング防止、ウイルス防止、迷惑メール防止）

③他者に迷惑をかけないための対策

（踏み台防止、情報漏洩防止、ウイルス防止）

これらの中で基本となる対策は、大学構成員の正しい識別（ID の管理）です。大学構成員の多様化に伴い、ID の管理が分散化する場合が見受けられます。このような分散を避け、情報インフラとしての ID 管理と認証システムの確立がセキュリティ維持のための第一歩であるといえます。

インシデントの大規模化に伴い、予防措置の重要性が増しています。ここでは、様々な予防措置の中から、侵入検知、監査、アンチウイルス、アンチスパムについて述べます。

4.1 大学構成員の識別

大学構成員に付与する識別子（ID: Identifier）は情報システムの運用に欠かせない要素です。一般的に、学生は学生証番号、教職員は職員番号が付与されますが、これらの ID 体系は独立であることが多いようです。学生証番号は新学期に一括発行されます。情報通信システムログインのための ID は、これらの ID（またはそれから派生した ID）が流用されるか、新規に付けられることになります。システムログインのための ID には有効期限、再発行処理、パスワードの紛失対応などを行うネットワークの管理者が必要です。

解説：ID の種類ごとに管理元が分かれる場合がある。

［構成員例（管理元例）］

ａ）学生（学務部）

ｂ）常勤職員（人事部）

ｃ）非常勤職員（学科）

このため同一人物でも所属により ID が変わる場合がある。例えば、部局生か

ら大学院生になる時、学生証番号が更新される。
以下に ID 種別例を示す。
ａ）管理元に対応した ID として、組織構成員に付与する ID
ｂ）組織横断的に個人に付与する ID（個人ＩＤ）
ｃ）臨時に付与する ID

4.2 ID 管理の統一と ID を用いたアクセス制御

付与した ID およびその ID に与えられたパスワードを用いて、学内サービスへのアクセス制御を行うことが広く行われています。パスワード設定ポリシーを定義しておくことにより、安易なパスワードの付与を避けることができます。

地域交流センタ、後援会、宿舎、インキュベーションセンタなどの大学外部の関連者に ID を付与する場合はその属性を分け、完全なアクセス管理ができるようにしておく必要があります。

中小大学では ID の管理元が一元化され、その結果 ID 付与体系の一元化に問題が起こらないのが一般的です。しかしながら大規模な大学になると、システム毎に ID が与えられることもあります。このような ID を統一するには、ID を組織横断的に個人に付与し、個人の属性として所属部局、アクセス許可サービスなどを登録するようにすることになります。ただし、組織毎の ID から個人 ID への移行には、組織別の ID 付与ポリシーの統一に関する問題をクリアしなければなりません。さらに、パスワード付与ポリシーも統一する必要があります。

解説：認証を要求される通信（高信頼な情報交換）には 2 者間の認証を用いることもできるが、多くの利用者種別とサービスが存在する場合には、公開鍵基盤（PKI: Public Key Infrastructure）による電子証明書を使うことにより、認証コストを削減できる。電子証明書では信頼のおける機関（以下、信頼点）を介して認証する。信頼点として、外部に開かれた公的なレベル（パブリック）と大学学内に閉じる私的なレベル（プライベート）がある。ブラウザには信頼できる認証局（パブリック）の電子証明書（ルート証明書）が組み込まれている。
大学におけるパブリックな証明書の利用シーンは、
①大学情報公開時のサーバ認証、
②電子商取引における個人認証、
③大学間で交換する情報の認証、
④物理トークンを用いた VPN へのアクセス制御
などである。
ID とパスワードの併用に比較した PKI の利点は、見破りやすいパスワード利用の害がない（セキュリティが高い）、リアルシーンでの利用を含め多く応用シーンがある等であるが、サービス開始時のコストは高い。
大学間の PKI 利用を促進する動きとして、大学間連携のための全国共同認証基盤（UPKI）がある。UPKI イニシアティブが推進する。用途、目的、特徴は以下の通りである。
用途：大学間相互認証、ネットワークローミング、

グリッドコンピューティング
目的：学生・教員流動化への対応、導入・開発コストの削減、
国際連携への展開
特徴：パブリックとも連携

4.3 統一した ID とその応用（SSO アクセス制御管理）

ID を使ったアクセス制御方式には、システム毎に設計する個別アクセス制御方式と一回の認証で多くのサービスへのアクセスを可能とする SSO（シングルサインオン）アクセス制御方式とがあります。SSO アクセス制御方式は利用者にとっては便利ですが、高度な機能（SSO アプリケーション）が必要になります。SSO アプリケーションがサービス毎の ID とパスワードを記憶しておく方式もありますが、システム間で統一した ID を用いると、SSO アクセス制御を大幅に効率化できます。大学内の情報サービスが多様化すると、統一 ID（ID 管理ポリシーの統一を含む）を用いた SSO アクセス制御による管理コストの節約とサービス性の向上が有効になると考えられます。

解説：統一 ID を用いたシステム構成例を図 2（シングルサインオンシステム構成例）に示す。 SSO サーバの機能は、①利用者のアクセス制御を個別サーバ（サービス）に代わって行い、②必要とする利用者属性を個別サーバに渡す。さらに、③オンラインによる SSO アクセス制御を行わないサーバ（サービス）のために、ID とその利用者属性を供給する役目も果たす、場合もある。
利用者属性を納めるデータベースをディレクトリデータベースと称す。ディレクトリデータベースにアクセスするプロトコルの一種に LDAP（Lightweight Directory Access Protocol）がある。

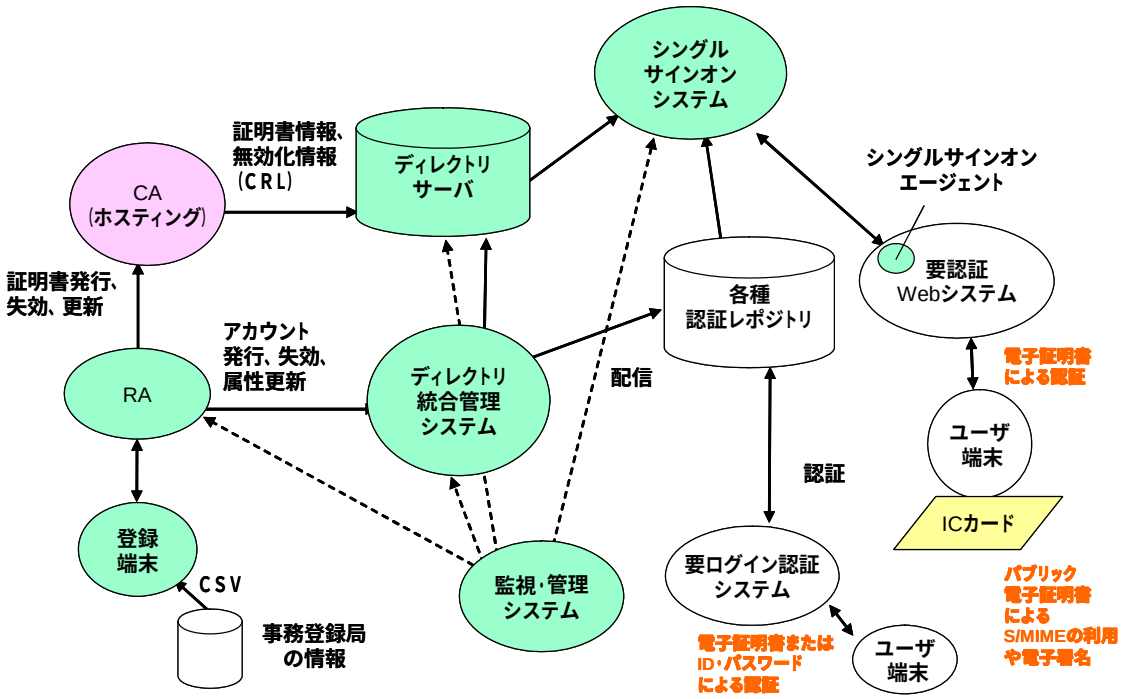


図2，シングルサインオンシステム構成例

4.4 セキュリティインシデントの予防措置

大規模化するインシデント、複雑化するセキュリティ攻撃に対して、予防措置の重要性が高まっています。予防は物理・論理的にインシデントを防ぐだけではなく、利用者の意識向上ももたらします。

1）トラヒックパターンによるネットワーク侵入検知

特定の IP アドレス・ポートに対する集中的なアクセスなどトラヒックパターンの観察によりネットワークに対する侵入を検知するセキュリティサービスです。特徴的なトラヒックパターンを伴う侵入の試みを検知することができます。攻撃を受ける場合にも、踏み台となって外部サーバを攻撃してしまう場合にも有効です。ただし、攻撃を受ける場合はファイアウォールで防御しておき、外部又は内部への意図しない攻撃の検知に用いられる場合が一般的です。欠点は誤認識があることです。

大学では侵入検知後のアクションを予め確立しておくことが重要です。例えば、大学のサーバが踏み台となって外部サーバを攻撃してしまった場合、踏み台とされたサーバの管理者による迅速な分析・対応が不可欠です。アクションを予め確立しておかないと、迅速な対応ができません。

コストはかかりますが、大学の情報システム維持に有効なサービスといえるでしょう。

2）サーバ監査（脆弱性評価）

サーバの管理者の了解のもと、仮想的なアタックやサーバの分析（セキュリティホールの発見）を行います。評価コストを抑えるため、対象サーバが主要なサーバに限定されることもあります。セキュリティホールの種類としては、①OS、アプリの既知の脆弱性、②見破られやすいパスワー

ドの存在、③回線、サーバの物理的状態など多岐にわたります。実施頻度は実情に応じて設定されます。評価結果はリスクのランクと伴にサーバの管理者に通知され、対処が求められます。運用なども含めた総合的評価を行うことが一般的です。

安易に設定されたパスワードによるインシデントが後を絶たないなかで、その抑止力ともなります。

３）ウイルスとアンチウイルス処理

他のソフト（宿主）の一部として自己を複製し、拡散させていくソフトのことをウイルスと呼びます。これに対して、独立したソフトの形態をとるのがワームです。特定の条件が揃うまで活動を抑制する場合があり、被害を拡大する一因となります。情報システムに様々な悪影響を及ぼしますが、具体的には、システム不安定・停止、バックドア（踏み台）などの原因になります。利用者が気づかないうちに感染が広がることがあるので、他者にも多大な迷惑（損害）をかけることになります。

こうしたウイルスやワームに対しては、しっかりした知識に基づき、感染予防、拡散予防に努めなければなりません。ウイルス発生に関する情報を常にチェックし、必要な対策をとることが重要です。不審なページへのアクセスや不審なソフトをダウンロードしないなどの日常オペレーションにおける注意、ネットワークの入り口での対策、汚染された端末を持ち込まないなどの物理的対策が同時に必要となります。アンチウイルスソフトウェア(ウイルス対策ソフトウェア)を用いることも重要な対策であり、利用促進指導が必要です。また、キャンパス全体で対応しないと感染が収束しにくいものです。

解説：ウイルスの種類

ワーム型：単独で活動できるプログラムを指す。宿主のファイルが必要な場合のみをウイルスと定義する場合もある。

トロイの木馬型：感染後、一見正常なプログラムとして利用者情報の不正持ち出しなどを行う。

ボット型：ロボットに因んだ命名。侵入後、端末が第３者の意思のままに動作するようになる。このようになると悪意の集団行動に知らぬうちに加担させられてしまう。

解説：感染経路と対策

ウイルスの特徴を表すデータ（パターンデータ）を用いて検出するのが一般的である。新しいウイルスの出現に対して、パターンデータをいち早く更新することが重要である。メールの添付ファイルなどネットワーク経由で侵入する場合が多い。このため、大学ネットワークの入り口でウイルス侵入を防ぐ必要があるが、媒体経由、持ち込み PC 経由などでも感染するため、端末毎の対策も不可欠である。WEB 閲覧中にセキュリティホールを突いて感染する場合もある。

解説：予防措置と対応組織の確立

予防措置の実施においては異常時に即応できるよう、対応する大学の組織を整

えることが重要です。政府機関の情報セキュリティ対策のための統一基準（内閣官房情報セキュリティセンター）や本サンプル規程集に従うことで、しっかりした組織を整備することができます。

4.5 迷惑メールと対策

各大学とも迷惑メールが急激に増加しており、対応に苦慮しているのが現状です。完全な対応方法はありませんが、①メールアドレスの使い分け、②メールアドレスの公開を制限、③簡単に見破られないメールアドレスの利用などがあります。ネットワーク入り口での対処と、端末における対処を併用する場合もあります。

解説：迷惑メール対策法には、ホワイトリスト方式、グレーリスト方式、ブラックリスト方式がある。図３（迷惑メール対策方式）に各方式の概要を示す。ホワイトリストは非迷惑メールのリスト、ブラックリストは迷惑メールのリストである。グレーリストは初めて受信するメールをリスト化したもので、このメールはいったん受信拒否される。ランダムに送りつけられる迷惑メールは殆どの場合は再送されないが、非迷惑メールは再送される。再送されたメールは正常受信させホワイトリストに移行させる。メールの識別は送信元 IP アドレス、本文中の送受信者の表示名などを使って行われる。

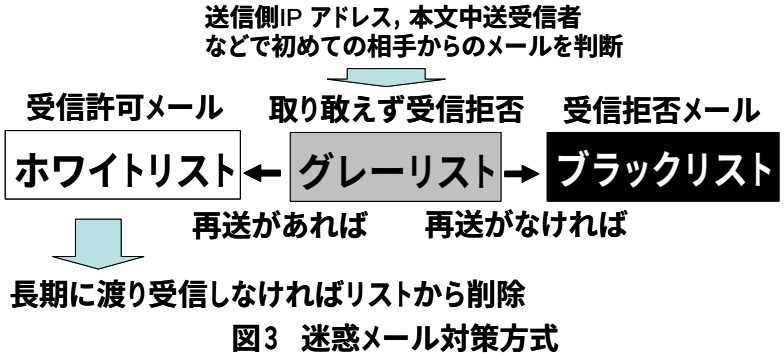


図3　迷惑メール対策方式

プロバイダの中には極めて優秀な迷惑メールフィルタを持つものがある。ただし、迷惑メールを含むメールを大量に特定のプロバイダに送りこのフィルタを使い過ぎると、大学ドメイン全体が迷惑サイトとなることがあるため、注意が必要である。

本文中に存在する特定の単語群をもとにベイズフィルタを応用して、迷惑メールの確率を予想する方法もある。本文内容に基づく判断が可能であり、学習により判断精度を向上できる。

4.6 IC カード

実験室の入退出、図書館の入退館・貸出しなど、多くのカードがアプリケーション毎に使われていることがあります。アプリケーション毎に使われるカードは個別に管理されますが、統一 IC カードを用いることにより、個別管理のコストを削減することができます。さらに、統一 IC カードを応用した高度なサービスを提供できるようになります。即ち、統一 IC カードは高度に情報化された大学の情報インフラとなることが期待されます。

解説：統一 IC カードの用途を図４（統一 IC カードの用途）に示す。その用途は、職員証、学生証、パブリック証明書（PKI）格納などが想定されている。

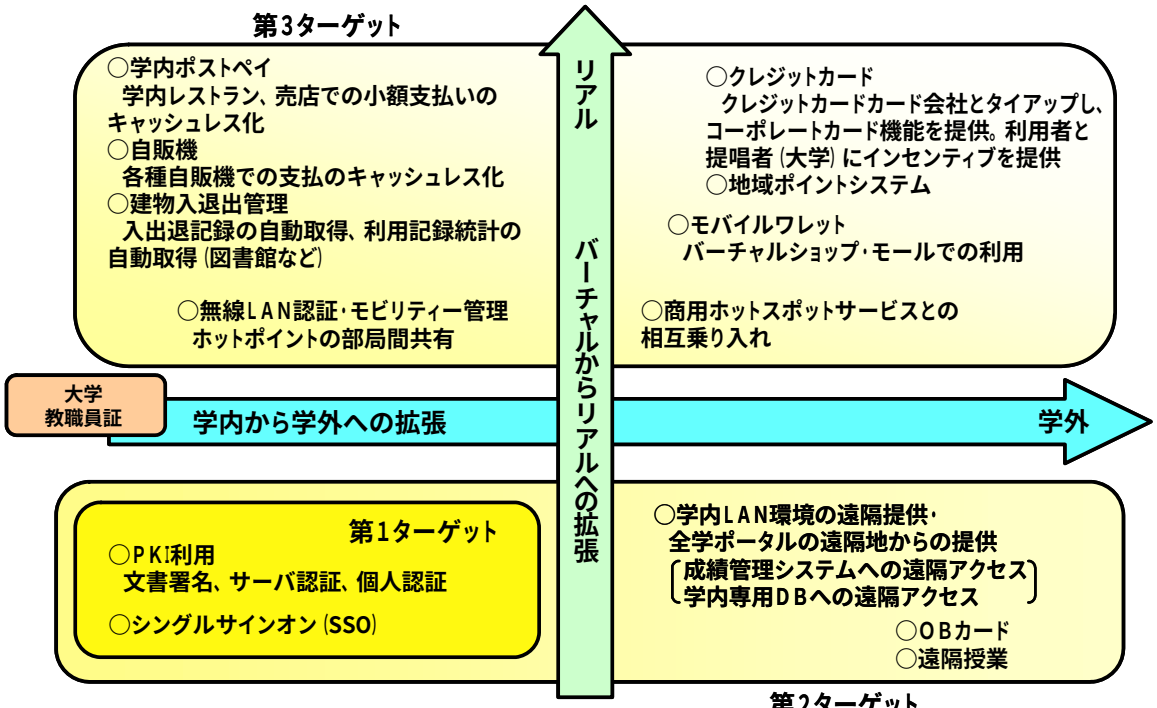


図４　統一ICカードの用途

第５章　セキュリティサービス・システムを構成する要素技術

セキュリティサービス・システムを構成するための要素技術の例を以下に示します。教科書や文献の豊富な分野です。詳細はそれぞれの教科書・参考書を参照してください。

１）公開鍵暗号による電子署名
２）認証・認可
３）暗号（秘匿）
４）改竄検出
５）セキュリティプロトコル

第６章　サーバ（アプリケーション，OS）のセキュリティ

サーバ（アプリケーション、OS）のセキュリティの例を以下に示します。教科書や文献の豊富な分野です。詳細はそれぞれの教科書・参考書を参照してください。

１）WEB サーバ
２）電子メールサーバ
３）DNS サーバ
４）OS のセキュリティ
　　UNIX®
　　Linux®
　　Windows®

第７章　法令・基準

情報セキュリティに関連する法令として、内閣官房情報セキュリティセンター(http://www.nisc.go.jp/law/index.html) から、下記の概要と本文が紹介されています。

１）不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
２）電子署名及び認証業務に関する法律（平成１２年法律第１０２号）
３）高度情報通信ネットワーク社会形成基本法（IT 基本法）（平成１２年法律第１４４号）

この他に、

４）個人情報の保護に関する法律
５）著作権法

が、情報セキュリティ周辺に関係する法令として重要です。本セキュリティポリシーにおいても関連法令と大学の著作権法の関係が解説されています(「A3204 ウェブ公開ガイドライン」参照)。

システム管理者は一通りの知識を持つことが望まれます。

A3303 教育テキスト作成ガイドライン（CIO/役職者向け）

本書は、役職者（学長、事務局長、全学総括責任者（CIO）、学部長（部局総括責任者））を対象とした大学運営における情報セキュリティ対策の基本的知識を習得するための講習テキストの必要項目を示すものである。

解説：対象は、ＣＩＯや大学執行部、経営陣。情報セキュリティの常識と事例を中心に、教育する。情報セキュリティのためのコスト（人、予算）を理解させる。情報セキュリティ対策はコストがかかるものであり効果が直ちに見えないこともあるので、予防的な対処は理解が得られにくいことがある。しかし、セキュリティ対策をあらかじめ施さないままにインシデント被害が発生すると、原因の特定や対処が困難になり、その困難な対応を直ちに短期間で実施することを迫られて、結果的に割高なコストがかかりがちで非効率的である。また、大学の評価が低下することに起因する副次的な被害につながることもあるので、「保険」のような必要コストであるという理解もありうる。

１．本学における情報セキュリティ状況

- インシデント発生状況の詳細情報（扱い件数の統計）
- 重大インシデント（学外に対して重大な被害を与え、あるいは報道・苦情など問題化したもの）の詳細な分析

2. 情報セキュリティ対策に必要な措置

2.1 情報セキュリティ対策の必要性

- ふだんから情報セキュリティ対策をきちんとしておかないと、インシデント発生時に業務遂行に支障が生じ、また対応にコストがかかって、労力と費用が失われる。情報セキュリティ対策にも労力と費用を要するので、合理的な労力および費用について考察して実施する。
- 情報セキュリティは、大学の存亡にかかわりかねない重大な問題である。情報セキュリティ対策を怠ったがために、重大インシデントが起こった場合の影響を考えてみる。この場合、直接的に業務遂行に支障が生じるだけでなく、大学の評価が低下する。例えば、研究データの管理能力や研究成果の正当性が疑われるために、研究活動に困難が生じるとともに、共同研究が拒否される。さらに、社会的評価の低下は、受験生の減少にもつながる。共同研究先や受験生が減少する結果、大学経営が厳しくなって情報セキュリティ対策の実施が困難になり、さらに重大インシデントを呼び込むことになる。その結果、大学経営に非常に重大な影響を及ぼしかねない。
- 大学における情報セキュリティ対策の中でも、とくに事務情報と医療情報については、特別な配慮を要する。事務情報には、学籍や職員に関する個人情報、財務情報、調達情報などがあり、適切な格付けに基づいた取り扱いを要する。また、医学部を有しない本学においても、学生の保健管理、あるいは人に係わる研究において医療情報をもつことがありうる。

・研究の成果は、やがて公表するものであっても、研究成果発表のプライオリティ維持のため、あるいは特許取得のため、情報管理が必要とされる。学生が実験で得た結果もその対象に含まれる。企業等との共同研究であれば、さらに厳密な管理が求められる。

2.2 情報セキュリティの責任体制

・情報セキュリティ対策の有効化のために、情報システム運用管理体制を整備することが必要である。
・「A2101 情報システム運用・管理規程」にもとづき、情報セキュリティ対策の最終責任は全学総括責任者にある。
・情報セキュリティ対策のために、通常業務として情報メディアセンター（管理運営部局）が整備、運用、監視を行う。
・インシデント発生時の判断と対応は、「A3103 インシデント対応手順」に従い、法務と技術の両面から遺漏のなく行うことが必要である。広報も重要である。必要に応じて情報セキュリティ分野の法務について実務経験のある弁護士等の助言を得ることが望ましい。

3. 情報システムの構築・運用・インシデント対応

3.1 体制の整備に関する課題

・情報セキュリティは情報システムの運用と利用のための安全保障である。
情報システムの構築時から、しっかり設備と体制をつくることが、セキュリティ対策上および TCO 削減のうえからも有効である。セキュリティ対策は、投資（労力と費用）効率を考慮すべきである。
情報セキュリティ規程を制定しても、実効的な設備および体制を構築しなければ、情報セキュリティ対策にならない。現実的な労力と費用において実施することができない情報セキュリティ規程を制定した場合、インシデントが発生すればその規程を制定した責任が問われる。

・情報セキュリティのため、通常運用の体制とインシデント対応のための体制の二つを整備することが必要である。
通常業務体制のために、情報メディアセンター（管理運営部局）の情報セキュリティ体制を整備する。すなわち、体制構築のための人員および必要な予算を確保する。
インシデント対応の体制のために、インシデント対応手順に合わせて、学内の法務と技術、広報等に関係する部署により体制を整備する。必要に応じて専門の弁護士等と契約する。

3.2 体制の整備の方法

・情報セキュリティの体制を整える際に、要員は学外への業務委託や派遣などのアウトソーシングも選択肢になりうる。情報セキュリティ対策のための設備、あるいはその運用と監視もアウトソーシングの対象になる。インシデント対応のアウトソーシングについては、大学運営を勘案した判断を要する面に十分に考慮すべきである。アウトソーシングには、臨機応変に最適化できることや長期的人件費を削減できるメリットがあるが、継続的な取り組みも含めて、費用対効果を十分に検討して判断する。

・情報セキュリティの体制を全学的に整備していなくても、各部局ごと、あるいは PC 一台ごとに既に対策ソフトを導入したり監査を実施したりしているようなケースも考えられる。しかし、一般的に多数でまとめたほうが経費や手数が効率的になり、費用対効果が良くなると期待できるので、全学的な取り組みに改めることが望ましい。教育の効果や実施の徹底のためにも、全学レベルで取り組む姿勢を示すことは有意義である。

4. ケーススタディ

解説：以下はあくまでも例なので、最新の事例を収集する。

4.1 不正侵入の事例

不正侵入の事件が発生した結果、外部から苦情が届き、不正侵入されたサーバの修復に加えて広報などの対応も必要になって、大きな労力を費やし、大学の社会的評判を落とすことになった例がある。被害者から損害賠償を請求された例もある。

・ウェブサーバが不正侵入されて、ホームページを改ざんされた大学の例。

・不正侵入された結果、踏み台となって、スパムサーバや不正アクセスに利用された例。同様に、フィッシングサイトを置かれた例。インターネットの掲示板に不適切な発言を書き込むアクセスの踏み台として悪用された例。

4.2 情報漏えいの事例

大学がもつ情報が漏えいした場合、社会的信頼を損なうほか、個人情報である場合などに損害賠償責任が生じる例がある。

・学生の成績情報が漏えいした大学の例。

・職員が使用するパソコンがウイルス（暴露ウイルスと呼ばれる種類）に感染し、取扱注意の情報が漏えいした大学や官公庁の例。

4.3 体制ができてない事例

情報システムや情報セキュリティの体制が整備されていない場合に、業務に多大な支障が生じた例がある。

・大学院生が主体になって仕様書を作成し、システムを構築した。その後、リプレイスのとき、その大学院生は卒業したため誰も仕様書を書けなかった大学の例。

・ネットワーク担当の教授が主体となってシステムを構築した後に定年退職となり、システムを理解する人が学内に皆無になったという大学の例。

・ネットワーク運用を学生（あるいは非常勤教員）に依存していたところ、その人が卒業（任期切れ）になった後、だれもネットワーク管理ができなくなり、安定運用ができず業務に支障をきたしたという大学の例。

4.4 著作権侵害の事例

・学生がインターネット規模のファイル交換システム上で長期間にわたって商用ソフトウェア

（あるいは、音楽や映画）を配布した結果、多額の損害賠償が問題になったという例。

- 商用ソフトウェアについて、許諾されるライセンスを大幅に超えて利用し続けた結果、損害賠償を支払った大学の例。

4.5 その他の事例

- 学生が学内からインターネットの掲示板に名誉毀損を疑われる発言を書き込んだ結果、訴えられた例。同様に、インターネットオークションに海賊版ソフトウェアを出品した例。

A3401 情報セキュリティ監査実施手順

1. 目的

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

本書は、本学における監査の適切な実施のための手順を定めることによって、情報セキュリティ対策の実効性を確保することを目的とする。

2. 本書の対象者

本書は、情報セキュリティ監査責任者及び情報セキュリティ監査を実施する者（以下「監査実施者」という。）を含む本学内における監査に携わる者（以下「学内監査関係者」という。）を対象とする。

3. 監査の概要

3.1 監査とは

本学における監査とは、本学ポリシーに従い、被監査部門とは独立性を有した組織又は者が行う情報セキュリティに関する確認行為（独立的評価）をいい、本学における自己点検結果等をサンプリングし、その確認・評価を行い、確認・評価の結果を全学総括責任者に報告することにより学内のセキュリティレベルの向上に資するものである。

一般的に、監査には「保証型監査」と「助言型監査」があり、これらは監査対象により使い分けられることになる。本学における監査では、ポリシー、実施規程及びそれに基づく手順については準拠性に対する保証型監査を行い、情報セキュリティ対策の運用については準拠性及び妥当性に対する助言型監査を行う。

3.2 基本的考え方

(1) 監査の実施は、本学ポリシーに根拠を置く。

(2) 監査の実施に係る本学内規定等を作成し、監査業務及び手続に関する学内での位置付けを明確化する。

(3) 監査は、年度情報セキュリティ監査計画に基づき、全学総括責任者の指示により実施する。

(4) 監査の客観性、実効性を確保するために、監査責任者は以下のことに配慮する。

- 専任の監査実施者の確保が困難であることを考慮し、監査業務を通常業務とは独立した業務として行うよう、監査実施者に指示する。
- 監査実施者の任命に当たっては、所属する上司等と協議をした上で、学内から

広く選定することとし、原則として任期は【2年】とする。

- 監査責任者及び監査実施者で、本学内における監査チーム等の組織を編成することを検討する。
- 監査実施者には、自らが直接担当している業務やシステムの監査を実施させない。
- 監査実施者に対して、監査で知りえたことをその業務以外では利用しないよう、周知徹底する。
- 適宜必要性に応じて、外部監査の活用を合わせて検討する。

(5) 監査調書又は監査報告書を含む監査関連文書は、学内の文書規定及び監査の重要性等をかんがみて、情報の格付けの実施等適切な取扱いを行うとともに、決定した保管方法、保管者、保存期間等に従い適切に保管する。

3.3 監査の目的及び位置付け

3.3.1 準拠性監査（保証意見及び助言意見）

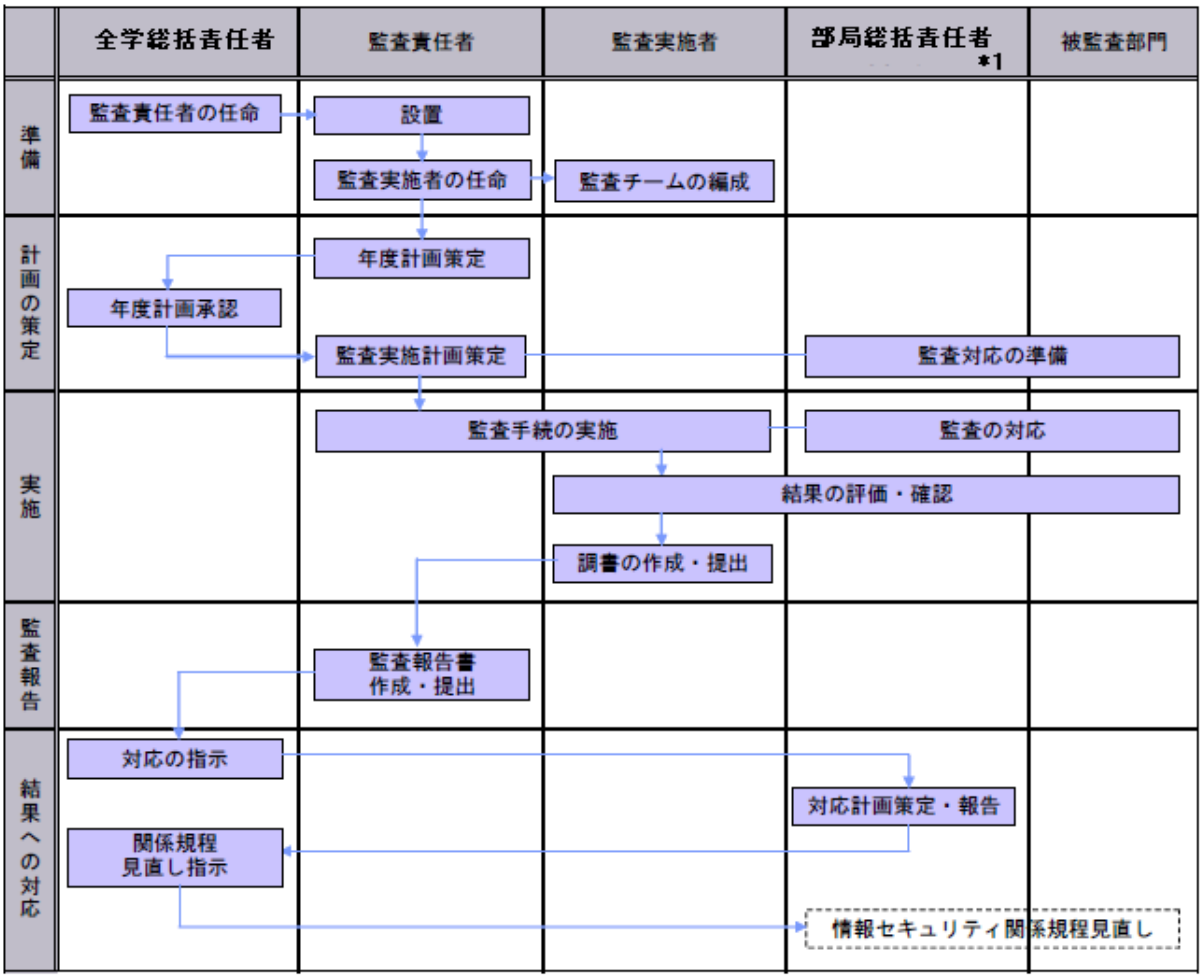
(1) 本学の実施手順が本学ポリシーに準拠しているかを確認・評価する。

(2) 本学における情報セキュリティ対策の運用がポリシー、実施規程及びそれに基づく手順に準拠しているかについて、自己点検結果等をもとに確認・評価する。

3.3.2 妥当性監査（助言意見）

本学のポリシー、実施規程及びそれに基づく手順が実効性のあるものになっているか、情報セキュリティ対策が妥当であるか又は有効に機能しているかについて、自己点検結果等をもとに確認し、改善提案等の助言を行う。

3.4 監査業務の全体像



＊1：被監査部門以外の部局総括責任者を含む場合がある。

4. 監査実施に当たっての前提及び準備

4.1 監査責任者の役割及び権限

(1) 監査責任者は、全学総括責任者の指示に基づき、監査に関する事務を統括する。

(2) 監査責任者は、年度情報セキュリティ監査計画及び監査実施計画（以下「監査計画」という。）を策定し、監査を実施する。

(3) 監査責任者は、監査実施者を任命【し、監査チームを編成】する。

(4) 監査責任者は、監査調書に基づき、監査の結果を監査報告書として作成し、全学総括責任者に報告する。

- 監査責任者は、準拠性監査の結果を保証する。
- 監査責任者は、妥当性監査の結果に基づき、改善提案等の助言を行う。

(5) 監査責任者は、監査計画の立案、監査マニュアルの整備及び監査調書のレビュー等

のプロセスを通じて、監査業務の品質を管理する。

(6) 監査責任者は、情報システム運用委員会への出席や各部局総括責任者へのヒヤリング等により、継続的に情報セキュリティ関係規程の整備状況や対策の実施状況、情報セキュリティ事案や違反の発生状況等の情報収集に努める。

4.2 監査実施体制の確立及び監査実施者の任命

(1) 監査責任者は、監査の客観性を確保することを考慮し、監査実施者を学内から広く選定し、監査実施体制を確立する。

(2) 監査責任者は監査実施者を任命する際に、監査責任者自らの所管する部局又は学内の各部局からメンバーを選定する。監査責任者は、必要に応じ監査実施者に対する兼務発令や業務指示を発効する。

(3) 監査責任者は、必要に応じ、監査責任者と監査実施者等で構成する監査チームを編成する。

(4) 監査責任者は、監査対象となる情報システムや業務、情報資産の運用に直接携わる者に、当該情報システム等の監査を実施させないものとする。

(5) 監査責任者又は監査実施者は、必要に応じて、監査対象システムの詳細情報を有する組織、学内の情報システム部門等の専門家の支援を受ける。

(6) 監査責任者は、監査の一部業務を外部に委託した場合でも、学内に相当程度の監査実施者を確保する必要があることに留意の上、監査実施体制を検討する。

(7) 監査責任者は、組織内に監査を実施する者又は監査遂行能力が不足していると判断した場合、必要に応じて監査の一部業務の外部委託を検討する。

(8) 監査責任者は、外部委託をする場合、委託先の選定に当り、被監査部門との独立性及び監査遂行能力を有している者を選択する。

4.3 情報収集及び状況の理解

監査責任者は、監査計画の策定及び監査の実施に当たり、事前に部局総括責任者等へのヒヤリングや学内の組織及び所管業務に関する情報収集を行い、学内のセキュリティ関連状況に関する理解に努める。

5. 年度情報セキュリティ監査計画の策定

5.1 目的及び位置付け

(1) 監査責任者は、学内監査関係者と情報を共有することにより、学内における監査業務を円滑に実施することを目的とし、継続的かつ定期的に行うべく当該年度における監査の年度計画を策定する。

(2) 監査責任者は、当該年度の監査計画の策定に当り、必要に応じて、3ヵ年程度以上の

中・長期計画を策定し、重点監査対象の年度展開及び当該年度に　実施すべき監査の水準・詳細度等を設定する。

5.2 概要

(1) 監査責任者は、【毎年2月末日】までに翌年度の「年度情報セキュリティ監査計画」を策定する。

(2) 策定した「年度情報セキュリティ監査計画」は、全学総括責任者の承認をもって、【当該年度4月1日より】発効する。

(3) 監査責任者は、監査実施計画の修正で適応しきれないほどのリスクの変動があった場合には、適宜本計画を修正し、全学総括責任者の承認を得る。

(4) 監査責任者は、当該年度に実施する監査の位置付けや目的、目標を明確化する。

(5) 中・長期計画を策定している場合は、当該中・長期計画に沿って当該年度における監査計画を策定する。

(6) 監査責任者は、当該年度計画の監査対象を明確化し、学内監査関係者に周知する。

(7) 監査責任者は、実施時期の調整や内容の重複の回避などを配慮し、会計検査や特定業務の監査等、恒常的に行われている通常の監査業務との連携を視野に入れて年度計画を策定する。

(8) 監査責任者は、年度情報セキュリティ監査計画に次の事項を記載する。

- 監査方針
- 監査の目的
- 監査対象（業務、システム、段階等）及び監査対象に係る監査目標（例えば、機密性、情報漏えい防止、不正アクセス防止等）
- 監査の想定カバー率
- 監査スケジュール
- 監査業務の管理体制
- 外部委託による監査及び外部専門家の活用の必要性及び範囲
- リソース管理（監査予算、人材育成計画等）

6. 監査実施計画の策定

6.1 目的及び位置付け

(1) 監査責任者は、年度情報セキュリティ監査計画で対象とした個別業務、システム等に応じて、具体的な監査方法及び監査時期等を計画する。

(2) 監査責任者は、学内における監査を円滑に実施することを目的とし、監査実施計画の内容を被監査部門及び当該部門の所属職員に対し事前に通知する。

6.2 概要

(1) 監査責任者は、年度情報セキュリティ監査計画及び情報セキュリティの状況の変化に応じた全学総括責任者からの実施指示に基づき、個別の監査対象ごとの監査実施計画を策定する。

(2) 監査責任者は、過年度の監査の実施状況その他過去の経験、事前の質問、世の中の状況等を勘案し、監査対象ごとの監査実施計画を策定する。

(3) 監査責任者は、監査実施計画に次の事項を記載する。

- 監査目的
- 背景（直前の情報セキュリティの状況認識）
- 監査対象
- 被監査部門及びその責任者
- 監査実施責任者及び実施担当者
- 監査の実施時期
- 監査の実施場所
- 監査の想定カバー率
- 実施する監査手続の概要（監査要点、評価方法の種類等）
- 監査の進捗管理手段
- 外部委託先との役割分担（外部委託を行う場合）

7. 監査の実施

7.1 監査の実施の指示

(1) 全学総括責任者は、年度情報セキュリティ監査計画に従って、監査責任者に対して、監査の実施を指示する。

(2) 全学総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、監査責任者に対して、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示する。監査責任者は監査実施計画を修正し、実施する。

(3) 監査責任者は、被監査部門から独立した監査実施者に対して、監査の実施を指示する。

- 情報システムを監査する場合、当該情報システムを構築又は開発した者はその

監査を担当しない。

- 情報資産の運用状況を監査する場合、当該情報資産を運用している者はその監査を担当しない。

7.2 監査の実施における留意事項

(1) 監査実施者は、監査計画に基づいて、十分かつ適切な監査証拠を入手し評価する。

(2) 監査実施者は、学内基準等の規定文書の内容確認を行った上で、被監査部門への質問を基本とする。さらに、別途文書による裏づけをとったり（査閲）、実際に行っている作業を観察したり（観察）、自らが実際に行って点検したり（点検）することにより、質問への回答を検証する。

(3) 監査実施者は、対策の実施状況を効率的に確認するために、自己点検票及び自己点検結果を活用する。

(4) 入手した資料は、その入手元及び入手時の状況等を勘案して、監査証拠として採用するかについて、それらが有する信用性及び証明力の程度を慎重に判断する。

(5) 被監査部門から提出された資料、監査実施者自らが入手した資料、自らが行ったテスト結果等を総合的に勘案して、相互に矛盾があるか、異常性を示す兆候があるかを評価する。

7.3 実施結果の評価

7.3.1 準拠性に関する保証意見

(1) 監査実施者は、ポリシー、実施規程及びそれに基づく手順の間に矛盾、相違点、不足がなければ、準拠しているものと判断する。

(2) 監査実施者は、遵守事項違反がなければ、準拠しているものと判断する。

7.3.2 妥当性に関する助言意見

(1) 助言意見は、想定するリスクと比較して、対策が妥当であるかについての意見とする。

(2) 監査実施者は、将来の遵守事項違反につながる可能性のある事象について助言を行う。

(3) 監査実施者は、助言意見を検討するに当たり、実施すべき対策の実現可能性についてまでは考慮せず、原則を指摘することを役割とし、実現可能性についての検討は被監査部門の部局総括責任者が行う。

(4) 被監査部門の部局総括責任者は、実施すべき対策の実現可能性について、監査報告書に基づく全学総括責任者からの指示により検討する。

7.3.3 監査業務において発見された問題点・違反等の取扱い

(1) 監査実施者及び被監査部門の部局総括責任者は、発見された問題点に関する事実関係について、事実誤認等がないかを含め合意をしておく。

(2) 監査実施者は、準拠性に関する違反について、重大な違反と軽微な違反に区分して報告する。

7.4 監査調書の作成

(1) 監査実施者は、実施した監査業務ごとに、監査実施の過程を監査報告書作成の基礎とするため記録した監査業務の実施記録であり、監査意見表明の根拠となる監査証拠集である監査調書を作成し、監査責任者に報告する。

(2) 監査実施者は、参照符号等を整備して、監査の結論に至った経過が秩序整然と分かるように作成する。

(3) 監査実施者は、被監査部門から提出された資料や組織の外部の第三者から入手した資料を監査調書に添付する。

(4) 監査責任者は、監査調書の保管場所や保管責任者を決定し、情報漏えいや紛失等を考慮した上で、あらかじめ定められた期間保存する。

(5) 監査実施者は、監査調書に次の事項を記載する。

- 表題（何を確認したか、何を証明したいか）
- 監査実施者氏名・署名
- 実施期間
- 被監査部門及び責任者
- 発見された問題点（重大な違反、軽微な違反）
- 意見（保証意見、助言意見）
- 確認した遵守項目
- 確認した対策の内容
- サンプルの件数及び抽出方法
- 評価方法及び結果
- 監査証拠としての形態（文書か口頭か）
- 監査証拠の入手元（被監査部門から提出された資料か、監査実施者が直接入手した資料か、第三者から入手した資料か）
- 関連資料番号（チェックした項目をマーキングし、資料として添付する。）

8. 監査報告

8.1 監査報告書の作成と提出

(1) 監査責任者は、監査調書に基づき、監査報告書を作成し、全学総括責任者に報告する。

(2) 監査責任者は、監査報告書において、準拠性監査については、当該監査対象の準拠性に関する保証を行うとともに、違反を改善するための助言を行う。また、妥当性監査については、助言を行い、学内PDCAサイクルの実施により改善につなげる。

(3) 監査責任者は、監査報告書の読み手が全学総括責任者であることを意識し、全学総括責任者が報告内容の重要性や指摘事項の緊急性等を理解し、部局総括責任者等への指示すべき内容が明瞭になるように記述する。

(4) 監査責任者は、助言意見を述べるに際して、監査人の自由裁量ではなく、ポリシーや当該契約書等の監査の基準に照らして検出された課題及び問題点の指摘と改善提言とするものとし、保証を付与するかのような誤解を与える表現を用いないようにする。

(5) 監査責任者は、監査報告書の正本を全学総括責任者に提出、写を自らが保管する。

(6) 監査責任者は、監査報告書に次の事項を記載する。

- 報告書の名称
- 報告書の日付
- 報告書の宛名
- 監査人の署名、又は記名押印
- 監査実施期間
- 監査対象範囲（組織、システム、業務機能等）
- 監査の基準（判断の尺度）とした管理基準等
- 総合的所見
- 監査意見（違反の有無、課題及び問題点等）
- 監査人の独立性に関する事項 【独立性の例】
  - ○ 過去一度も当該監査対象業務に従事していない
  - ○ 過去2年の間、当該監査対象業務に従事していない
  - ○ 過去1年の間、当該監査対象業務に従事していなく、それ以前に当該業務に係る規定の整備又はシステムの設定等現在に影響の及ぶ行為をしていない
- 運用状況の準拠性に関する監査を実施した旨及びその結果（準拠性監査の場合）
- 遵守事項の整備状況の妥当性及び運用状況の準拠性に関する監査を実施した旨

及びその結果（妥当性監査の場合）

- 監査報告書の取扱い（利用及び利用者の制限事項等）
- 添付資料（個別業務ごとの監査調書等）

9. 監査結果に対する対応

9.1 監査報告書の内容の分析及び評価

(1) 全学総括責任者は、報告内容を分析し、全体像の把握と課題及び問題点の整理を行う。

(2) 全学総括責任者は、監査報告書において、改善提案等の助言があった場合、その内容の妥当性及び実現可能性等を検討する。

(3) 全学総括責任者は、同種の課題及び問題点が他の部門にもあり得るかの検討及び対策の見直し等の緊急性の検討を行う。

9.2 部局総括責任者への改善指示

(1) 全学総括責任者は、監査報告書の内容を踏まえ、被監査部門の部局総括責任者に対して、指摘事案に対する対応を指示する。

(2) 全学総括責任者は、被監査部門における課題及び問題点が他の部門にも発生する可能性があると判断した場合、他の部局総括責任者に確認する。

(3) 全学総括責任者は、(1)(2)に掲げるもののほか必要な事項について、該当する部局総括責任者に対応を指示する。

9.3 対応計画の作成及び報告

(1) 部局総括責任者は、監査報告書に基づいて全学総括責任者から改善を指示された事案について、対応計画を作成し、報告する。

(2) 部局総括責任者は、指示された改善が困難であることについて正当な理由がある場合には、リスク軽減策を示した上で、達成可能な対応目標を提示する。

(3) 部局総括責任者は、指示された改善内容が教育・訓練により解決すべき課題であると判断した場合には、全学実施責任者と相談の上、教育計画及び資料に反映する。

9.4 情報セキュリティ関係規程の見直しの指示

(1) 全学総括責任者は、監査報告書において情報セキュリティ対策の妥当性に関した改善提案を受けた場合、ポリシー、実施規程及びそれに基づく手順の妥当性を評価し、当該規定を整備した者に対して必要に応じてその見直しを指示する。

(2) 全学総括責任者は、改善提案を受けた場合であって、ポリシー、実施規程及びそれに基づく手順の見直しの必要がないと判断したときは、その理由を明確にする。

A大学情報セキュリティ監査手順解説

本解説は、「A3401 情報セキュリティ監査手順」の各項における用語や例を示すものであり、本書における項番号は「A3401 情報セキュリティ監査手順」の項番号に対応させている。

3. 監査の概要

【手順策定者への補足説明：保証型監査と助言型監査の比較】

特定非営利活動法人 日本セキュリティ監査協会「情報セキュリティ監査制度利用促進等事業 実施報告書」より抜粋

	保証型監査	助言型監査	コンサルティング（参考）
保証	与える	与えない	
意見	述べる		
提言	しない	する	
客観的基準	存在することが前提		ない
実施者の独立性	必須		必須ではない
提言のフォローアップ	なし	あり	なし

4. 監査実施に当たっての前提及び準備

【手順策定者への補足説明：監査業務の品質とは】

実施された監査が、本学ポリシーや外部委託に係る契約書等の監査の基準に準拠して適切に行われているかという監査業務の信頼性及び有効性のこと。

【手順策定者への補足説明：監査実施者に求められる一般的な要件】

- 高い倫理観
- 監査対象業務についての知識・理解
- 情報セキュリティについての知識・技術
- 情報システムについての知識・技術
- 監査についての知識・技術

【手順策定者への補足説明：監査チーム編成における配慮事項】

- 各監査実施者の通常業務と監査業務の負荷バランス
- 監査実施者間の相互チェック機能の確保
- 適切な職務の分担による監査対象からの独立性の確保

【手順策定者への補足説明：監査に必要な人的リソースの目安】

監査対象とする項目やシステム、業務の数及び実施する監査の方法により、必要となる監査実施者の人数や能力は異なるが、10～20名程度／大学、人年換算をすると５～10名程度の体制が目安と考えられる。

この一部の人員を外部委託することにより確保した場合でも、学内にかなりの人的リソースを確保しなければならないことに留意の上、計画を立てることが重要である。

【手順策定者への補足説明：監査遂行能力とは】

監査遂行能力とは、監査に関する能力や経験と監査対象業務及び情報セキュリティに対する知識・技術等からなる。

【手順策定者への補足説明：監査業務の委託先の選定に関する配慮事項】

委託先の選定に当たっては、情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の参画を考慮することが望ましい。

【手順策定者への補足説明：収集する情報の例】

- 学内の組織図及び情報セキュリティ関係の体制図
- 学内の情報セキュリティ関係規程（ポリシー、実施規程、実施手順等）
- 各組織及び各情報セキュリティ関係の責任者の一覧
- 各組織の業務内容
- 各業務で取り扱う情報の種別
- 保有している情報システムの一覧
- ネットワーク図等の情報システムに関する情報
- 以前に実施した監査に関する計画及び報告書等の監査結果

5. 年度情報セキュリティ監査計画の策定

【中・長期計画を策定する場合の例】

- 初年度 ：学内情報セキュリティ対策の実施状況の把握及び評価
- 2年度目：情報セキュリティ対策実施に関する日常業務への浸透
- 3年度目：情報セキュリティ対策実施の定着化及び学内セキュリティレベルの底上げ

【手順策定者への補足説明：監査対象選定のための観点の例】

- 自己点検が適切に行われているかを確認するための観点
- 遵守できていない（と思われる）ところを重点的に監査する観点
- 毎年同様の監査を実施し、対策状況の進捗や成熟度を経年で確認・評価する観　点（定点観測的に経年で確認・評価する観点）
- 環境の変化や監査時点での情報セキュリティ事案の動向・トピックス、体制・規定の変更等をかんがみ、年度別の重点監査対象の項目や重点システムを評価する観点（当該年度重点監査対象の選定）
- 導入段階、定常的運用段階等業務のライフサイクルに応じて確認する観点
- 以前実施した監査結果で明らかになった課題及び問題点の改善状況を確認する観点

【年度情報セキュリティ監査計画の雛形】

作成日：○○年4月1日

（情報セキュリティ監査責任者）

氏 名

○○年度 ××××大学情報セキュリティ監査計画書

１．監査方針

本年度は、本学内における情報セキュリティ関係の体制構築及び対策の実施状況を網羅的に把握・評価する。来年度以降の対策レベル向上に向けた基盤整備を行う。

２．監査の目的

本学内における情報セキュリティ関係の状況を網羅的に把握することにより、現在の情報セキュリティ関係規程(ポリシー、実施規程、手順等)の妥当性を評価し、来年度以降の対策レベル向上に向けた情報収集・分析を行う。

３．監査対象及び監査対象に係る監査目標

(1) 重点監査対象

① 実施規程及び手順の準拠性監査（監査目標：○○○）
② 情報セキュリティ管理体制の構築の監査（監査目標：○○○）
③ 情報の格付け業務の監査（監査目標：○○○）
④ 学内LANの運用状況の監査（監査目標：○○○）

(2) その他の監査対象

① インターネット接続口に設置されているサーバ群のセキュリティ設定の監査

４．監査の想定カバー率

(1) 対象となる責任者、管理者、利用者（対象となる者/全員）

(2) 対象となるシステム（対象システム数/全システム数）

(3) 対象となる端末（対象端末数/全端末数）

５．監査スケジュール：別紙のとおり

６．監査業務の管理体制：別紙のとおり

７．外部委託による監査の範囲及び必要性

(1) 外部委託の範囲及び必要性

① 範囲 インターネット接続口に設置されているサーバ群のセキュリティ設定の監査
② 必要性 脆弱性スキャン、システム侵入テスト等専門的技術を要するため

(2) 委託契約の必要性の要否：要

８．リソース管理

(1) 監査予算：別紙のとおり

(2) 人材育成計画：詳細別紙のとおり 目標：監査スキルの向上と要員の確保

① 監査業務基礎講座：4月１日～4月30日の2週間程度
② 情報セキュリティ基礎講座：5月1日～5月30日の2週間程度

別紙

●監査業務の管理体制

（体制図の挿入）

●監査スケジュール

監査対象	作業フェーズ	2月	3月	4月	5月	6月	7月	・・・	10月	11月	12月	1月	2月	3月
年度計画策定								・・・						
本学基準及び実施手順の準拠性監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
体制の構築の監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
情報の格付けの監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
学内ＬＡＮの運用の監査	実施計画策定							・・・						
	被監査部門への周知							・・・						
	監査の実施							・・・						
・								・・・						
・								・・・						
・								・・・						

●監査予算

予算項目	項目概要	予算費目	金額	実施時期	実施担当者
出張費					
宿泊費					
外部委託費					
・・・					

●　人材育成計画

育成内容	実施時期	実施方法	対象者	実施担当者
監査業務基礎講座	4/1～4/30	座学	利用者	○○○
・・・				

6. 監査実施計画の策定

【手順策定者への補足説明：監査実施計画策定上の配慮事項】

- 本学のシステム、業務、組織等の特性を分析した上で、影響度や脆弱性から判別し、リスクが高いと思われる領域を抽出する。
  - ○ 事件の発生可能性が高いと思われる領域（対策を実施していなければ事故の発生可能性が高い領域、対策が不十分と思われる領域、対策が十分に行われているか不明な領域等）
  - ○ 事件が発生した場合の影響が大きいと思われる領域（機密性の高い情報を取り扱っている領域、完全性の確保が必要となる情報・システムを取り扱っている領域、可用性の確保が必要となる情報・システムを取り扱っている領域等）
- 自己点検が終了している等、監査の受入れが十分と考えられる領域を選定する。
- 監査が円滑に実施できるように考慮する。
  - ○ 人的リソースや予算の状況
  - ○ 監査対象部門の負荷状況
  - ○ システムの運用状況（負荷の多い日、時間帯を避ける等）
- システムをカテゴリー分けし、監査頻度を決定する。

  【例】

  カテゴリーＡ：2回／年で監査を実施

  カテゴリーＢ：1回／年で監査を実施

  カテゴリーＣ：1回／3年で監査を実施

【監査実施計画の雛形】

作成日：○○年○○月○○日

（情報セキュリティ監査実施者）

氏 名

○○年度 ××××大学情報セキュリティ管理体制の構築に関する監査実施計画書

１．監査目的

本学ポリシー、実施規程及びそれに基づく手順で定めた情報セキュリティ管理体制の構築状況に関し、体制図・設置規定等の文書及び当該責任者への質問により確認する。

２．背景

平成18年12月に国立大学法人等における情報システム運用ポリシーが策定され、本学でも従来のセキュリティポリシーを改訂し、新たに本学ポリシーを策定したところ、昨今、情報漏えい事案も頻発しており、本学における情報管理体制の再確認が必要である。

３．監査対象：本学情報セキュリティ管理体制の監査

４．被監査部門及び責任者：××××

５．監査実施責任者：△△△△

６．監査の実施時期：7月1日～9月30日の各月末の週（計15日間）

７．監査の実施場所：本学内執務室

８．監査の想定カバー率

対象となる責任者、管理者および利用者（対象となる者/全員）

対象となるシステム（対象システム数/全システム数）

対象となる端末（全端末数/全端末数）

９．実施する監査手続の概要：別紙のとおり

１０．監査の進捗管理手段：別紙のとおり

別紙

●監査手続の概要

遵守事項	対策内容	評価方法	実施時期	実施担当者
部局技術責任者の設置	設置	体制図の確認	・・・	・・・
		質問	・・・	・・・
	連絡網の整備	体制図の確認	・・・	・・・

●監査の進捗管理手段

１．定期報告の実施

２．・・・

7. 監査の実施

【手順策定者への補足説明：情報セキュリティ状況の変化の例】

- 新しいシステムが開発又は導入されたとき
- 新たに他のシステム又はネットワーク等と接続したとき
- 学内における大きな人事異動や組織改編があったとき
- 学内外を問わず重大なセキュリティ侵害があったとき
- 本学ポリシー等が改訂又は追加されたとき

【手順利用者への補足説明：監査証拠の十分かつ適切な入手方法例】

- 関連書類の査閲
- 担当者への質問
- 現場への視察
- システムテストへの立会い
- テストデータによる検証
- 脆弱性スキャン、システム侵入テスト

【手順策定者への補足説明：評価方法の解説】

- 質問：講じた対策、行為
- 査閲：規程類、設定文書（設計書等の設定一覧等）、記録文書、文書証拠
- 観察：日常の行為
- 点検：物理的状態、システム上のセキュリティ設定

【手順利用者への補足説明：点検による評価における配慮事項】

　点検という手法を採用する場合には、システム運用を停止させること等がないように配慮し、実際の操作は部局技術担当者等に行ってもらうことが望ましい。

【手順利用者への補足説明：自己点検票の利用等チェックリストによる監査実施における配慮事項】

　事前に監査チェックリスト等を用意して監査を実施することは、監査業務の経験の浅い監査実施者が行う場合等に有効であるが、通常、監査の最終段階で監査手続が網羅的に行われたかをチェックするために使用することが効果的とされており、以下のことに留意して行うことが望ましい。

- 効率性確保の観点 リスト上のチェック項目の意味や重要性をかんがみ、上から下に順

番に行ったり、同じような質問を繰り返したりしない。

- 有効性検討の観点 チェック項目の内容が現実に合っているかを考慮しながら監査を実施する。
- 網羅性確保の観点 チェックリストに記載されていない重要な項目がないか検討する。

【自己点検票の活用例】

	自己点検の対象となるセキュリティ対策項目の整理・分析					自己点検の実施										備考
			分類			点検方法			実施時期&頻度		適用範囲			回答項目		
	自己点検項目一覧の作成	本学基準との対応	連続・単発	定期・不定期	頻度	随時点検型	一括点検型	断面調査型	自己点検の実施時期	自己点検の実施頻度	実施主体	管理者	責任者	回答項目	備考	監査における評価方法
1	人事異動の際には、識別コードの管理を徹底すること。	4.1.3 (2) (g)	連続	定期	年4	○			実施時	実施時	権限管理を行う者	部局技術管理者	部局技術責任者	Yes 日時	—	点検
2	情報入手時には、格付け・取扱制限を明示す	3.2.1 (2) (b)	連続	不定期	毎日		○		月末	月1	部局技術責任者	上司	部局総括責任者	Yes No	アンケート併用	質問
3	ウイルスパターンを最新にするこ	4.2.2 (2) (c)	連続	不定期	週1			○	15日 30日	半月1	利用者	部局技術管理者	部局技術責任者	設定値	バージョン番号	点検
4	ソフト開発時にST確認すること	4.3.1 (1) (d)	単発	定期	年1	○			実施時	実施時	利用者	—	部局総括責任者	Yes 日時	—	査閲
5	離席時には画面ロックすること。	3.2.2 (3) (b)	単発	不定期	毎日		○		月末	月1	利用者	上司	部局総括責任者	Yes No	—	質問
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
	Step 1-1	Step1-2	Step 1-3			Step 1-4			Step 1-5		Step 1-6			Step 1-7		Step 1-8

【準拠性判断の基準例（最大逸脱率が9%であることを90%の信頼度で確認する場合）】

- 25件のサンプルのうち、1件も遵守事項違反がなければ、準拠しているものとする。
- 25件のサンプルのうち、1件の遵守事項違反があっても、追加で20件のサンプルを選び、1件も遵守事項違反がなければ準拠しているものとする。
- それ以外は準拠していないものとする。

【手順策定者への補足説明：重大な違反と軽微な違反の定義例】

- 重大な違反とは、その違反単独で、又は他の違反と複合することにより、重大なリスクの発生を引き起こす可能性のあるものをいう。
- 軽微な違反とは、重大な違反以外のものをいう。

【監査調書の雛形】

○○年○○月○○日

情報セキュリティ監査責任者 殿

（監査実施者）

署名

情報セキュリティ管理体制構築に係る情報セキュリティ監査の報告

平成○○年度情報セキュリティ管理体制の構築に関する監査実施計画に基づき、情報セキュリティ管理体制の構築状況を対象として監査を実施したので、以下のとおり報告する。

1．実施期間：××年××月××日から○○年○○月○○日まで

2．被監査部門及び責任者：・・・・・・

3．発見された問題点

(1) 重大な違反 ・・・・・・

(2) 軽微な違反 ・・・・・・

(3) 課題及び問題点等 ・・・・・・

4．意見

(1) 準拠性に関する保証意見 ・・・・・・

(2) 妥当性に関する助言意見 ・・・・・・

5．実施内容：別紙のとおり

別紙

順守事項	対策内容	評価方法	評価結果	サンプル		監査証拠		関連資料番号
				件数	抽出方法	形態	入手元	
部局技術責任者の設置	・・・	・・・	・・・	50/200	無作為	文書	第三者	001
	・・・	・・・	・・・	・・・	・・・	口頭	直接入手	-

8. 監査報告

【手順利用者への補足説明：監査報告書記載上の配慮事項】

- **要約と詳細を分ける**
- **指摘事項等の対象となる部門や責任者をわかりやすく記述**
- **準拠性の違反等の事実と妥当性の助言意見については、分けて記述**
- **違反の事実については、重要性により区分けをし、記述**

【監査報告書の雛形】

- **準拠性監査報告書の雛形**

○○年○○月○○日

全学総括責任者 殿

（情報セキュリティ監査責任者）

署 名

○○年度 ××××大学情報セキュリティ監査報告書

（準拠性監査報告）

平成○○年度情報セキュリティ監査計画に基づき、情報セキュリティの状況について準拠性監査を実施したところ、以下のとおり報告する。

1. **監査実施期間：××年××月××日から○○年○○月○○日まで**
2. **監査対象範囲**
   ・・・・・・
   ・・・・・・
3. **監査の基準：本学ポリシー及び当該請負契約書**
4. **総合的所見：・・・・・・・・**
5. **監査意見**
   ⑴ **違反の有無**
      ① 重大な違反 ・・・・・・
      ② 軽微な違反 ・・・・・・
   ⑵ **課題及び問題点 ・・・・・・**
   ⑶ **助言意見 ・・・・・・**
6. **添付資料**
   ⑴ **平成○○年度×××に係る情報セキュリティ監査の報告**
   ⑵ **・・・**

なお、本職は、今回の監査対象の業務の実施には直接携わっておらず、十分な独立性を有しており、監査手続を実施した結果に基づいて、以上のとおり意見を表明するものである。

また、本報告書の利用は、本学における全学総括責任者及び部局総括責任者に限る。

- **妥当性監査報告書の雛形**

○○年○○月○○日

全学総括責任者 殿

（情報セキュリティ監査責任者）

署 名

○○年度 ××××大学情報セキュリティ監査報告書

（妥当性監査報告）

平成○○年度情報セキュリティ監査計画に基づき、情報セキュリティの状況について妥当性監査を実施したところ、以下のとおり報告する。

1. **監査実施期間：××年××月××日から○○年○○月○○日まで**
2. **監査対象範囲**

・・・・・・

・・・・・・

3. **監査の基準：本学ポリシー及び当該請負契約書**
4. **総合的所見：・・・・・・・・**
5. **監査意見**

(1) **課題及び問題点 ・・・・・・**

(2) **助言意見 ・・・・・・**

6. **添付資料**

(1) **平成○○年度×××に係る情報セキュリティ監査の報告**

(2) **・・・**

なお、本職は、今回の監査対象の業務の実施には直接携わっておらず、十分な独立性を有しており、監査手続を実施した結果に基づいて、以上のとおり意見を表明するものである。

また、本報告書の利用は、本学における全学総括責任者及び部局総括責任者に限る。

A3500 各種マニュアル類の策定に関する解説書

1. 本書の目的

「高等教育機関の情報セキュリティ対策のためのサンプル規程集」(以下サンプル規程集)では、「A2501 事務情報セキュリティ対策基準」に基づいた情報セキュリティ対策実施手順書の雛形として「A3501 各種マニュアル類」を策定することとしている。「A2501 事務情報セキュリティ対策基準」は、「政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版(全体版初版))」(以下政府機関統一基準)を基にしており、その内容は用語の違いをのぞき、多くの部分で共通である。政府機関統一基準に準拠した実施手順書の雛形としては、「政府機関統一基準適用個別マニュアル群」(以下統一基準マニュアル群)と呼ばれる文書群が整備されている。よって事務情報セキュリティ対策基準に基づいた「A3501 各種マニュアル類」の作成に当たっては、統一基準マニュアル群を基とすることが適切である。

一方、2007 月 6 月に政府機関統一基準は改定を受けており、現在は「政府機関の情報セキュリティ対策のための統一基準(第二版)」(以下政府機関統一基準第二版)に置き換えられている。このため、事務情報セキュリティ対策基準は、政府統一基準第二版に準拠したものに改訂することが適当である。一方、統一基準マニュアル群は政府機関統一基準第二版での変更点への反映が 2007 年 7 月時点では完了していない。政府機関統一基準と同第二版の差異は表現上の違いを除くと小さいが、統一基準マニュアル群の内容には確実に影響するため今後改訂が進むと考えられる。そこで本文書は、将来統一基準マニュアル群が改訂・追加された場合に備え、一般に統一基準マニュアル群中の文書を基に「A3501 各種マニュアル類」を作成する際の手順および注意事項について記したものである。

2. 「A3501 各種マニュアル類」作成にあたっての基本的な考え方

本文書で述べる「A3501 各種マニュアル類」とは、「A1001 情報システム運用基本規程」第三条四に定義された事務情報システムの運用にあたり、「A2501 事務情報セキュリティ対策基準」を満たした情報システムの操作もしくは電子化された情報資産の取り扱いを、各業務を担当する教職員等が容易に理解し実行できるようにまとめたものである。その基となる統一基準マニュアル群の構成は 2007 年 7 月現在、表1のようになっている。各文書に付されている文書番号の先頭 DM に続く数字は、政府統一対策基準内の対応する部の番号を表している(例えば DM2 で始まる文書は第2部に対応している)。

一方、「A2501 事務情報セキュリティ対策基準」は政府機関統一基準および同第二版と同じ章立てになっており、部の番号も完全に対応している。よって、例えば統一基準マニュアル群「DM5-01 庁舎内における PC 利用手順」を基に各大学の事務情報システム利用者の PC 利用手順を作成するには、A2501 を基に作成した各大学の事務情報セキュリティ対策基準の第2部を参照しながら作成するとよい。

表 1　政府機関統一基準適用個別マニュアル群の構成

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

「A3501 各種マニュアル類」作成の基本的な手順

既に述べたように、政府機関統一基準と「A2501 事務情報セキュリティ対策基準」は用語の違いをのぞいて多くの部分が共通であるため、統一基準マニュアル群の各文書に対し以下のような作業を行うことにより、効率的に「A3501 各種マニュアル類」等を作成することができる。

2.1. 用語の置換

政府機関統一基準と「A2501 事務情報セキュリティ対策基準」の間には表 2 のような用語の差異があるため、統一基準マニュアル群の各文書内の対応する用語を置き換えることによってある程度機械的に各種マニュアル類の雛形を作成することができる。ただし完全に機械的な置換を行うと表現が崩れる部分があるため、適宜修正する必要がある。また、表 2 中にない政府機関特有の用語が今後統一基準マニュアル群に表れる可能性もある。

表 2　政府機関統一基準と A2501 の主な用語の対応

	政府機関統一基準 (府省庁等対象)	A2501 事務情報セキュリティ対策基準 (高等教育機関対象)
役職名等	最高セキュリティ責任者	全学総括責任者
	最高セキュリティ監査責任者	情報セキュリティ監査責任者
	最高情報セキュリティアドバイザー	情報セキュリティアドバイザー
	総括情報セキュリティ責任者	全学実施責任者
	情報セキュリティ責任者	部局総括責任者
	情報システムセキュリティ責任者	部局技術責任者
	情報システムセキュリティ管理者	部局技術担当者
	課室情報セキュリティ責任者	職場情報セキュリティ責任者
	情報セキュリティ委員会	全学情報システム運用委員会　または　部局情報システム運用委員会
利用者･関係者	行政事務従事者	教職員等
	国民	学生や学外利用者
	職員	本学構成員
組織･施設	政府機関	本学
	(各) 府省庁	本学　または　(各) 部局
	庁内または庁舎内	学内
業務	行政事務	事務
	行政職務	職務
その他	国民の権利が侵害され	大学の運営に支障を及ぼす

2.2. 強化遵守事項の扱い

政府機関統一基準内で明示的に強化遵守事項となっている部分については、「A2501 事務情報セキュリティ対策基準」内では「特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ」という文を補っている。各種マニュアル類においては、この強化遵守事項を含む対策を実施するか否かを、判断基準となるリスク評価結果等の基準もしくは責任者の判断とともに加えるべきである。

2.3. 情報セキュリティ対策基準の構成の違いに起因する修正

政府機関統一基準は府省庁においては最上位に位置する規程であるが、「A2501 事務情報セキュリティ対策基準」には上位規程として「A1001 情報システム運用基本規程」があり、事務情報以外を取り扱う情報システムに関する他の規程も並列に存在するため、それらとの整合性を取るこ

とが必要である。特に事務情報以外を取り扱う情報システムに関するマニュアル等が作成された場合には、情報システム利用者が遵守するべきマニュアル等は事務情報システムにかかるものになるか否かで異なってくるため、利用者が混乱しないような工夫が求められる。例えば事務情報システムに関連するマニュアルを他の情報システムに関連するマニュアル内の対策基準全てを含むように記述し、事務情報システムを利用する可能性のある者には事務情報システム向けの各種マニュアル等で代替可能にするなどの措置が考えられる。現時点では、サンプル規程集中で事務情報システム以外に対応する実施手順書類である A3100 番台の文書はその多くが統一基準マニュアル群を基に作成されているため、「A2501 事務情報セキュリティ対策基準」にも対応しており、流用・共用が可能である場合も多い。

2.4. その他各大学固有の事情に応じた修正

その他、各大学で「A2501 事務情報セキュリティ対策基準」を基に施した修正等に関しては各種マニュアル類にも反映させる必要がある。

A3502 責任者等の役割から見た遵守事項

1. 本書の目的

本書は、「A2501 事務情報セキュリティ対策基準」に記載されてある遵守事項を役割（例えば、全学総括責任者）単位で整理したものである。

各大学において、事務情報セキュリティ対策基準に定められている役割に当該大学の役職者等を充て、又は情報セキュリティを確保するための体制を整備する際の参考にすることを目的とする。

2. 本書の利用方法及び補足説明

ポリシー、実施規程及び手順を策定又は運用する者は、当該大学の組織、役職、権限等の状況を考慮し、当該大学内に情報セキュリティを確保するための体制を整備するものとする。

体制を整備するに当たっては、事務情報セキュリティ対策基準に定められている「1.2.1.2 役割の割当て」を遵守した上で、当該大学の実態に合わせて例えば以下のように運用することが可能である。

①対象となる情報システムや業務量が大きい場合、責任の所在を明確化した上で役割を分担すること。

②自らが所管する情報システムや業務において、各々の規模が小さいなどの理由により情報セキュリティを確保することが可能であると判断した場合、一人の役職者等が事務情報セキュリティ対策基準に定められている責任者や管理者の役割を兼務すること。

③役割を担うべき役職者等が責任を持ち、かつ実効性を確保した上で、所管する職員にその 実務の一部を委任すること。

なお、体制の整備においては、形式的に役職者を充てる又は当該大学の業務実態と乖離した役割を担わせる等を行わず、実効性を確保すること。

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
第1編 基本編																		
第1.2部 組織と体制の整備																		
1.2.1 導入																		
1.2.1.1 組織・体制の整備																		
(1) 全学総括責任者の設置																		
1.2.1.1(1)(a)	基本	全学総括責任者を1人置くこと。	学長(A1001-04)															
1.2.1.1(1)(b)	基本	全学総括責任者は、本学における情報セキュリティ対策に関する事務を統括すること。	全学総括責任者	○														
(2) 全学情報システム運用委員会の設置																		
1.2.1.1(2)(a)	基本	全学総括責任者は、全学情報システム運用委員会を設置し、委員長及び委員を置くこと。	全学総括責任者	○														
1.2.1.1(2)(b)	基本	全学情報システム運用委員会は、情報セキュリティに関する対策基準を策定し、全学総括責任者の承認を得ること。ただし、あらかじめ全学総括責任者が認めた場合は、一部の技術的な事項について、指定した者に委任することができる。	全学情報システム運用委員会								○							
(3) 情報セキュリティ監査責任者の設置																		
1.2.1.1(3)(a)	基本	全学総括責任者は、情報セキュリティ監査責任者を1人置くこと。	全学総括責任者	○														
1.2.1.1(3)(b)	基本	情報セキュリティ監査責任者は、全学総括責任者の指示に基づき、監査に関する事務を統括すること。	情報セキュリティ監査責任者									○						
(4) 全学実施責任者の設置																		
1.2.1.1(4)(a)	基本	全学総括責任者は、全学実施責任者を置くこと。	全学総括責任者	○														
1.2.1.1(4)(b)	基本	全学実施責任者は、部局総括責任者が実施する事務を統括すること。	全学実施責任者		○													
1.2.1.1(4)(c)	基本	全学実施責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動等に関する管理の規定を策定し、全学総括責任者の承認を得ること。	全学実施責任者		○													
(5) 部局総括責任者の設置																		
1.2.1.1(5)(a)	基本	全学総括責任者は、情報セキュリティ対策の運用に係る管理を行う単位を定め、その単位ごとに部局総括責任者を置くこと。管理を行う単位を全学情報システム運用委員会の各情報システム運用委員会とし、部局総括責任者は、部局情報システム運用委員会の各総括責任者とすること。	全学総括責任者	○														
1.2.1.1(5)(b)	基本	部局総括責任者は、所管する単位における情報セキュリティ対策に関する事務を統括すること。	部局総括責任者			○												
1.2.1.1(5)(c)	基本	部局総括責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動等に関する管理の規定に従った運用がなされていることを定期的に確認すること。	部局総括責任者			○												
1.2.1.1(5)(d)	基本	全学総括責任者は、部局総括責任者を置いた時及び変更した時は、全学実施責任者にその旨を連絡すること。	全学総括責任者	○														
1.2.1.1(5)(e)	基本	全学実施責任者は、すべての部局総括責任者に対する連絡網を整備すること。	全学実施責任者		○													
(6) 部局技術責任者の設置																		
1.2.1.1(6)(a)	基本	部局総括責任者は、所管する単位における情報システムごとに部局技術責任者を、当該情報システムの計画段階までに置くこと。	部局総括責任者			○												
1.2.1.1(6)(b)	基本	部局技術責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務を統括すること。	部局技術責任者				○											
1.2.1.1(6)(c)	基本	部局総括責任者は、部局技術責任者を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。	部局総括責任者			○												
1.2.1.1(6)(d)	基本	全学実施責任者は、すべての部局技術責任者に対する連絡網を整備すること。	全学実施責任者		○													
(7) 部局技術担当者の設置																		
1.2.1.1(7)(a)	基本	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。	部局技術責任者				○											
1.2.1.1(7)(b)	基本	部局技術担当者は、所管する管理業務における情報セキュリティ対策を実施すること。	部局技術担当者					○										
1.2.1.1(7)(c)	基本	部局技術責任者は、部局技術担当者を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。	部局技術責任者				○											
1.2.1.1(7)(d)	基本	全学実施責任者は、すべての部局技術担当者に対する連絡網を整備すること。	全学実施責任者		○													
(8) 職場情報セキュリティ責任者の設置																		
1.2.1.1(8)(a)	基本	部局総括責任者は、各職場に職場情報セキュリティ責任者を1人置くこと。	部局総括責任者			○												
1.2.1.1(8)(b)	基本	職場情報セキュリティ責任者は、職場における情報セキュリティ対策に関する事務を統括すること。	職場情報セキュリティ責任者						○									
1.2.1.1(8)(c)	基本	部局総括責任者は、職場情報セキュリティ責任者を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。	部局総括責任者			○												
1.2.1.1(8)(d)	基本	全学実施責任者は、すべての職場情報セキュリティ責任者に対する連絡網を整備すること。	全学実施責任者		○													
(9) 情報セキュリティアドバイザーの設置																		
1.2.1.1(9)(a)	基本	全学総括責任者は、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置くこと。	全学総括責任者	○														
1.2.1.1(9)(b)	基本	全学総括責任者は、情報セキュリティ対策等の実施において情報セキュリティアドバイザーが行う業務の内容について定めること。	全学総括責任者	○														
1.2.1.2 役割の割当て																		
(1) 兼務を禁止する役割の規定																		
1.2.1.2(1)(a)	基本	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。	事務従事者							○								
(2) 上司による承認・許可																		

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.2.1.2(2)(a)	基本	事務従事者は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可（以下「承認等」という。）の可否の判断を行うことが不適切と認められる場合には、当該承認権限者等の上司に承認等の申請をすること。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。	事務従事者							○								
1.2.1.2(2)(b)	基本	事務従事者は、前事項の場合において承認等を与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずること。	事務従事者							○								
1.2.1.3 違反と例外措置																		
(1) 違反への対処																		
1.2.1.3(1)(a)	基本	事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合には、各規定の実施に責任を持つ部局総括責任者にその旨を報告すること。	事務従事者							○								
1.2.1.3(1)(b)	基本	部局総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせること。	部局総括責任者			○												
1.2.1.3(1)(c)	基本	部局総括責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、全学総括責任者にその旨を報告すること。	部局総括責任者			○												
(2) 例外措置																		
1.2.1.3(2)(a)	基本	全学情報システム運用委員会は、例外措置の適用の申請を審査する者（以下、本項において「許可権限者」という。）を定め、審査手続を整備すること。	全学情報システム運用委員会								○							
1.2.1.3(2)(b)	基本	事務従事者は、例外措置の適用を希望する場合には、定められた審査手続に従い、許可権限者に例外措置の適用を申請すること。ただし、大学事務の遂行に緊急を要する等の場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定を実施しないことが不可避のときは、事後速やかに申請し許可を得ること。事務従事者は、申請の際に以下の事項を含む項目を明確にすること。	事務従事者							○								
1.2.1.3(2)(b)(ア)		申請者の情報（氏名、所属、連絡先）																
1.2.1.3(2)(b)(イ)		例外措置の適用を申請する情報セキュリティ関係規程の適用箇所（規程名と条項等）																
1.2.1.3(2)(b)(ウ)		例外措置の適用を申請する期間																
1.2.1.3(2)(b)(エ)		例外措置の適用を申請する措置内容（講ずる代替手段等）																
1.2.1.3(2)(b)(オ)		例外措置の適用を終了したときの報告方法																
1.2.1.3(2)(b)(カ)		例外措置の適用を申請する理由																
1.2.1.3(2)(c)	基本	許可権限者は、事務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。また、決定の際に、以下の項目を含む例外措置の適用審査記録を作成し、全学総括責任者に報告すること。	許可権限者												○			
1.2.1.3(2)(c)(ア)		決定を審査した者の情報（氏名、役割名、所属、連絡先）																
1.2.1.3(2)(c)(イ)		申請内容 ・申請者の情報（氏名、所属、連絡先） ・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等） ・例外措置の適用を申請する期間 ・例外措置の適用を申請する措置内容（講ずる代替手段等） ・例外措置の適用を終了した旨の報告方法 ・例外措置の適用を申請する理由																
1.2.1.3(2)(c)(ウ)		審査結果の内容 ・許可又は不許可の別 ・許可又は不許可の理由 ・例外措置の適用を許可した情報セキュリティ関係規程の適用箇所（規程名と条項等） ・例外措置の適用を許可した期間 ・許可した措置内容（講ずるべき代替手段等） ・例外措置を終了した旨の報告方法																
1.2.1.3(2)(d)	基本	事務従事者は、例外措置の適用について許可を受け、例外措置を適用した場合には、それを終了したときに、当該例外措置の許可権限者にその旨を報告すること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。	事務従事者							○								
1.2.1.3(2)(e)	基本	許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な措置を講ずること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。	許可権限者												○			
1.2.1.3(2)(f)	基本	全学総括責任者は、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査責任者からの求めに応ずること。	全学総括責任者	○														
1.2.2 運用																		
1.2.2.1 情報セキュリティ対策の教育																		
(1) 情報セキュリティ対策の教育の実施																		
1.2.2.1(1)(a)	基本	全学実施責任者は、情報セキュリティ関係規程について、事務従事者に対し、その啓発をすること。	全学実施責任者		○													
1.2.2.1(1)(b)	基本	全学実施責任者は、情報セキュリティ関係規程について、事務従事者に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。	全学実施責任者		○													
1.2.2.1(1)(c)	基本	全学実施責任者は、事務従事者が毎年度最低1回、受講できるように、情報セキュリティ対策の教育に係る計画を企画、立案するとともに、その実施体制を整備すること。	全学実施責任者		○													
1.2.2.1(1)(d)	基本	全学実施責任者は、事務従事者の着任時、異動時に新しい職場等で3か月以内に受講できるように、情報セキュリティ対策の教育を企画、立案するとともに、その実施体制を整備すること。	全学実施責任者		○													
1.2.2.1(1)(e)	基本	全学実施責任者は、事務従事者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備すること。	全学実施責任者		○													

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.2.2.1(1)(f)	基本	全学実施責任者は、事務従事者の情報セキュリティ対策の教育の受講状況について、職場情報セキュリティ責任者に通知すること。	全学実施責任者		○													
1.2.2.1(1)(g)	基本	職場情報セキュリティ責任者は、事務従事者の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告すること。事務従事者が当該勧告に従わない場合には、全学実施責任者にその旨を報告すること。	職場情報セキュリティ責任者						○									
1.2.2.1(1)(h)	基本	全学実施責任者は、毎年度1回、全学総括責任者及び全学情報システム運用委員会に対して、事務従事者の情報セキュリティ対策の教育の受講状況について報告すること。	全学実施責任者		○													
1.2.2.1(1)(i)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、全学実施責任者は、情報セキュリティ関係規程について、事務従事者に対する情報セキュリティ対策の訓練の内容及び体制を整備すること。	全学実施責任者		○													
(2) 情報セキュリティ対策の教育の受講																		
1.2.2.1(2)(a)	基本	事務従事者は、毎年度最低1回、情報セキュリティ対策の教育に関する計画に従って、情報セキュリティ対策の教育を受講すること。	事務従事者							○								
1.2.2.1(2)(b)	基本	事務従事者は、着任時、異動時に新しい職場等で、情報セキュリティ対策の教育の受講方法について職場情報セキュリティ責任者に確認すること。	事務従事者							○								
1.2.2.1(2)(c)	基本	事務従事者は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではないと思われる場合には、その理由について、職場情報セキュリティ責任者を通じて、全学実施責任者に報告すること。	事務従事者							○								
1.2.2.1(2)(d)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、事務従事者は、情報セキュリティ対策の訓練に関する規定が定められている場合には、当該規定に従って、情報セキュリティ対策の訓練に参加すること。	事務従事者							○								
1.2.2.2 障害・事故等の対処																		
(1) 障害・事故等の発生に備えた事前準備																		
1.2.2.2(1)(a)	基本	全学総括責任者は、情報セキュリティに関する障害・事故等（インシデント及び故障を含む。以下「障害・事故等」という。）が発生した場合、被害の拡大を防ぐとともに、障害・事故等から復旧するための体制を整備すること。	全学総括責任者	○														
1.2.2.2(1)(b)	基本	全学実施責任者は、障害・事故等について事務従事者から部局総括責任者への報告手順を整備し、当該報告手段をすべての事務従事者に周知すること。	全学実施責任者		○													
1.2.2.2(1)(c)	基本	全学実施責任者は、障害・事故等が発生した際の対処手順を整備すること。	全学実施責任者		○													
1.2.2.2(1)(d)	基本	全学実施責任者は、障害・事故等に備え、大学事務の遂行のため特に重要と認めた情報システムについて、その部局技術責任者及び部局技術担当者の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。	全学実施責任者		○													
1.2.2.2(1)(e)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、全学実施責任者は、障害・事故等について学外から報告を受けるための窓口を設置し、その窓口への連絡手段を学外に公表すること。	全学実施責任者		○													
(2) 障害・事故等の発生時における報告と応急措置																		
1.2.2.2(2)(a)	基本	事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、全学実施責任者が定めた報告手順により、部局総括責任者にその旨を報告すること。	事務従事者							○								
1.2.2.2(2)(b)	基本	事務従事者は、障害・事故等が発生した際の対処手順の有無を確認し、それを実施できる場合には、その手順に従うこと。	事務従事者							○								
1.2.2.2(2)(c)	基本	事務従事者は、障害・事故等が発生した場合であって、当該障害・事故等について対処手順がないとき及びその有無を確認できないときは、その対処についての指示を受けるまで、障害・事故等による被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。	事務従事者							○								
(3) 障害・事故等の原因調査と再発防止策																		
1.2.2.2(3)(a)	基本	部局総括責任者は、障害・事故等が発生した場合には、障害・事故等の原因を調査し再発防止策を策定し、その結果を報告書として全学総括責任者に報告すること。	部局総括責任者			○												
1.2.2.2(3)(b)	基本	全学総括責任者は、部局総括責任者から障害・事故等についての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずること。	全学総括責任者	○														
1.2.3 評価																		
1.2.3.1 情報セキュリティ対策の自己点検																		
(1) 自己点検に関する年度計画の策定																		
1.2.3.1(1)(a)	基本	全学実施責任者は、年度自己点検計画を策定し、全学総括責任者の承認を得ること。	全学実施責任者		○													
(2) 自己点検の実施に関する準備																		
1.2.3.1(2)(a)	基本	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。	部局総括責任者			○												
(3) 自己点検の実施																		
1.2.3.1(3)(a)	基本	部局総括責任者は、全学実施責任者が定める年度自己点検計画に基づき、事務従事者に対して、自己点検の実施を指示すること。	部局総括責任者			○												
1.2.3.1(3)(b)	基本	事務従事者は、部局総括責任者から指示された自己点検票及び自己点検の実施手順を用いて自己点検を実施すること。	事務従事者							○								
(4) 自己点検結果の評価																		
1.2.3.1(4)(a)	基本	部局総括責任者は、事務従事者による自己点検が行われていることを確認し、その結果を評価すること。	部局総括責任者			○												
1.2.3.1(4)(b)	基本	全学実施責任者は、部局総括責任者による自己点検が行われていることを確認し、その結果を評価すること。	全学実施責任者		○													
1.2.3.1(4)(c)	基本	全学実施責任者は、自己点検の結果を全学総括責任者へ報告すること。	全学実施責任者		○													
(5) 自己点検に基づく改善																		

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.2.3.1(5)(a)	基本	事務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、部局総括責任者にその旨を報告すること。	事務従事者							○								
1.2.3.1(5)(b)	基本	全学総括責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には部局総括責任者に改善を指示すること。	全学総括責任者	○														
1.2.3.2 情報セキュリティ対策の監査																		
(1) 監査計画の策定																		
1.2.3.2(1)(a)	基本	情報セキュリティ監査責任者は、年度監査計画を策定し、全学総括責任者の承認を得ること。	情報セキュリティ監査責任者									○						
(2) 監査の実施に関する指示																		
1.2.3.2(2)(a)	基本	全学総括責任者は、年度監査計画に従って、情報セキュリティ監査責任者に対して、監査の実施を指示すること。	全学総括責任者	○														
1.2.3.2(2)(b)	基本	全学総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、情報セキュリティ監査責任者に対して、年度監査計画で計画されたこと以外の監査の実施を指示すること。	全学総括責任者	○														
(3) 個別の監査業務における監査実施計画の策定																		
1.2.3.2(3)(a)	基本	情報セキュリティ監査責任者は、年度監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を策定すること。	情報セキュリティ監査責任者									○						
(4) 監査の実施に係る準備																		
1.2.3.2(4)(a)	基本	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。	情報セキュリティ監査責任者									○						
1.2.3.2(4)(b)	基本	情報セキュリティ監査責任者は、必要に応じて、教職員等以外の者に監査の一部を請け負わせること。	情報セキュリティ監査責任者									○						
(5) 監査の実施																		
1.2.3.2(5)(a)	基本	情報セキュリティ監査実施者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施すること。	情報セキュリティ監査実施者															
1.2.3.2(5)(b)	基本	情報セキュリティ監査実施者は、実施手順が本基準に準拠していることを確認すること。	情報セキュリティ監査実施者															
1.2.3.2(5)(c)	基本	情報セキュリティ監査実施者は、自己点検の適正性の確認を行う等により、被監査部門における実際の運用が情報セキュリティ関係規程に準拠していることを確認すること。	情報セキュリティ監査実施者															
1.2.3.2(5)(d)	基本	情報セキュリティ監査実施者は、監査調書を作成すること。	情報セキュリティ監査実施者															
1.2.3.2(5)(e)	基本	情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、全学総括責任者へ提出すること。	情報セキュリティ監査責任者									○						
(6) 監査結果に対する対処																		
1.2.3.2(6)(a)	基本	全学総括責任者は、監査報告書の内容を踏まえ、被監査部門の部局総括責任者に対して、指摘されたことに対する対処の実施を指示すること。	全学総括責任者	○														
1.2.3.2(6)(b)	基本	全学総括責任者は、監査報告書の内容を踏まえ、監査を受けた部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、他の部門の部局総括責任者に対しても、同種の課題及び問題点の有無を確認するように指示すること。	全学総括責任者	○														
1.2.3.2(6)(c)	基本	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。	部局総括責任者			○												
1.2.3.2(6)(d)	基本	全学総括責任者は、監査の結果を踏まえ、既存の情報セキュリティ関係規程の妥当性を評価し、必要に応じてその見直しを指示すること。	全学総括責任者	○														
1.2.4 見直し																		
1.2.4.1 情報セキュリティ対策の見直し																		
(1) 情報セキュリティ対策の見直し																		
1.2.4.1(1)(a)	基本	情報セキュリティ関係規程を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行うこと。	情報セキュリティ関係規程を整備した者														○	
1.2.4.1(1)(b)	基本	事務従事者は、情報セキュリティ関係規程に課題及び問題点が認められる場合には、情報セキュリティ関係規程を整備した者に相談すること。	事務従事者							○								
1.2.4.1(1)(c)	基本	情報セキュリティ関係規程を整備した者は、情報セキュリティ関係規程に課題及び問題点が認められる旨の相談を受けた場合は、必要な措置を講ずること。	情報セキュリティ関係規程を整備した者														○	
1.2.5 その他																		
1.2.5.1 外部委託																		
(1) 情報セキュリティ確保のための学内共通の仕組みの整備																		
1.2.5.1(1)(a)	基本	全学実施責任者は、外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準を整備すること。	全学実施責任者		○													
1.2.5.1(1)(b)	基本	全学実施責任者は、委託先の選定基準及び選定手続を整備すること。	全学実施責任者		○													
1.2.5.1(1)(c)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、全学実施責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法を整備すること。	全学実施責任者		○													
(2) 委託先に実施させる情報セキュリティ対策の明確化																		
1.2.5.1(2)(a)	基本	部局技術責任者又は職場情報セキュリティ責任者は、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容を定め、委託先候補に事前に周知すること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.1(2)(b)	基本	部局技術責任者又は職場情報セキュリティ責任者は、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処方法を整備し、委託先候補に事前に周知すること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.1(2)(c)	基本	部局技術責任者又は職場情報セキュリティ責任者は、委託先における情報セキュリティ対策の履行状況を確認するための方法及び情報セキュリティ対策の履行が不十分である場合の対処方法を整備し、委託先候補に事前に周知すること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
(3) 委託先の選定																		

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.2.5.1(3)(a)	基本	部局技術責任者又は職場情報セキュリティ責任者は、選定基準及び選定手続に基づき、委託先を選定すること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.1(3)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者又は職場情報セキュリティ責任者は、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法に従って、委託先の候補者の情報セキュリティ水準を確認し、委託先の選定における評価の一要素として利用すること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
(4) 外部委託に係る契約																		
1.2.5.1(4)(a)	基本	部局技術責任者又は職場情報セキュリティ責任者は、外部委託を実施する際に、委託先に請け負わせる業務における情報セキュリティ対策、機密保持(情報の目的外利用の禁止を含む。)、情報セキュリティの侵害発生時の対処方法、情報セキュリティ対策の履行状況の確認方法及び情報セキュリティ対策の履行が不十分である場合の対処方法を含む外部委託に伴う契約を取り交わすこと。また、必要に応じて、以下の事項を当該契約に含めること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.1(4)(a)(ア)		情報セキュリティ監査の受入れ																
1.2.5.1(4)(a)(イ)		サービスレベルの保証																
1.2.5.1(4)(b)	基本	部局技術責任者又は職場情報セキュリティ責任者は、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書等を提出させること。また、必要に応じて、以下の事項を当該確認書等に含めさせること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.1(4)(b)(ア)		当該委託業務に携わる者の特定																
1.2.5.1(4)(b)(イ)		遵守すべき情報セキュリティ対策を実現するために、当該者が実施する具体的な取組内容																
1.2.5.1(4)(c)	基本	部局技術責任者又は職場情報セキュリティ責任者は、外部委託契約の継続に関しては、選定基準及び選定手続に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.1(4)(d)	基本	部局技術責任者又は職場情報セキュリティ責任者は、委託先の提供するサービス(情報セキュリティ基本方針、実施手順、管理策の維持及び改善を含む。)の変更に関しては、選定基準及び選定手続に基づき、その是非を審査すること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.1(4)(e)	基本	部局技術責任者又は職場情報セキュリティ責任者は、委託先がその請負内容の全部又は一部を第三者に再請負させることを禁止すること。ただし、委託先からの申請を受け、再請負させることにより生ずる脅威に対して情報セキュリティが十分に確保される措置が担保されると判断する場合は、その限りでない。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
(5) 外部委託の実施における手続																		
1.2.5.1(5)(a)	基本	事務従事者は、委託先に要保護情報又は重要な設計書を提供する場合、提供する情報を必要最小限とし、以下の措置を講ずること。	事務従事者							○								
1.2.5.1(5)(a)(ア)		委託先に情報を提供する場合は、安全な受渡方法によりこれを実施し、提供した記録を取得すること。																
1.2.5.1(5)(a)(イ)		外部委託の業務終了等により提供した情報が委託先において不要になった場合には、これを確実に返却させ、又は廃棄させ、若しくは抹消させること。																
1.2.5.1(5)(b)	基本	部局技術責任者又は職場情報セキュリティ責任者は、請け負わせた業務の実施において情報セキュリティの侵害が発生した場合に、定められた対処方法に従い、委託先に必要な措置を講じさせること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.1(5)(c)	基本	部局技術責任者又は職場情報セキュリティ責任者は、定められた方法に従い、委託先における情報セキュリティ対策の履行状況を確認すること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
(6) 外部委託終了時の手続																		
1.2.5.1(6)(a)	基本	部局技術責任者又は職場情報セキュリティ責任者は、外部委託の終了時に、委託先に請け負わせた業務において行われた情報セキュリティ対策を確認し、その結果を納品検査における確認の判断に加えること。	部局技術責任者又は職場情報セキュリティ責任者				○		○									
1.2.5.2 業務継続計画との整合的運用の確保																		
(1) 業務継続計画と情報セキュリティ対策の整合性の確保																		
1.2.5.2(1)(a)	基本	全学情報システム運用委員会は、本学において業務継続計画又は本基準を整備する場合には、業務継続計画と本基準との整合性の確保のための検討を行うこと。	全学情報システム運用委員会								○							
1.2.5.2(1)(b)	基本	全学実施責任者、部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者は、本学において業務継続計画の整備計画がある場合には、すべての情報システムについて、当該業務継続計画との関係の有無を検討すること。	全学実施責任者、部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者		○	○	○		○									
1.2.5.2(1)(c)	基本	全学実施責任者、部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者は、本学において業務継続計画の整備計画がある場合には、当該業務継続計画と関係があると認めた情報システムについて、以下に従って、業務継続計画と本基準に基づく共通の実施手順を整備すること。	全学実施責任者、部局総括責任者、部局技術責任者及び職場情報セキュリティ責任者		○	○	○		○									
1.2.5.2(1)(c)(ア)		通常時において業務継続計画と本基準の共通要素を整合的に運用するため、情報セキュリティの枠内で必要な見直しを行うこと。																
1.2.5.2(1)(c)(イ)		事態発生時において業務継続計画と本基準の実施に障害となる可能性のある情報セキュリティ対策の遵守事項の有無を把握し、整合的運用が可能となるよう事態発生時の規定を整備すること。																
(2) 業務継続計画と情報セキュリティ関係規程の不整合の報告																		
1.2.5.2(2)(a)	基本	事務従事者は、本学において業務継続計画の整備計画がある場合であって、業務継続計画と情報セキュリティ関係規程が定める要求事項との違いなどにより、実施の是非の判断が困難なときは、関係者に連絡するとともに、全学実施責任者が整備した障害・事故等が発生した際の報告手順により、部局総括責任者にその旨を報告して、指示を得ること。	事務従事者							○								
第1.3部 情報についての対策																		
1.3.1 情報の取扱い																		
1.3.1.1 情報の作成と入手																		

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
(1) 業務以外の情報の作成又は入手の禁止																		
1.3.1.1(1)(a)	基本	事務従事者は、大学事務の遂行以外の目的で、情報を作成し、又は入手しないこと。	事務従事者							○								
(2) 情報の作成又は入手時における格付けと取扱制限の決定																		
1.3.1.1(2)(a)	基本	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け及び取扱制限の定義に基づき、格付け及び取扱制限を決定すること。	事務従事者							○								
1.3.1.1(2)(b)	基本	事務従事者は、元の情報の修正、追加、削除のいずれかにより、他者が決定した情報の格付け及び取扱制限を変更する必要があると思料する場合には、前項に従って再決定すること。	事務従事者							○								
1.3.1.1(2)(c)		事務従事者は、未定稿の情報を決定稿にする際には、当該情報の格付けと取扱制限について、その妥当性の有無を再確認し、妥当でないと思われる場合には、これを行った者に相談することに努めること。相談された者は、格付けと取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな格付けと取扱制限を決定すること。	事務従事者							○								
(3) 格付けと取扱制限の明示等																		
1.3.1.1(3)(a)	基本	事務従事者は、情報の格付け及び取扱制限を決定（再決定を含む。以下同じ。）した際に、当該情報の参照が許されている者が認識できる方法を用いて明示等すること。	事務従事者							○								
(4) 格付けと取扱制限の加工時における継承																		
1.3.1.1(4)(a)	基本	事務従事者は、情報を作成する際に、参照した情報又は入手した情報が既に格付け又は取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付け及び取扱制限を継承すること。	事務従事者							○								
1.3.1.2 情報の利用																		
(1) 業務以外の利用の禁止																		
1.3.1.2(1)(a)	基本	事務従事者は、大学事務の遂行以外の目的で、情報を利用しないこと。	事務従事者							○								
(2) 格付け及び取扱制限に従った情報の取扱い																		
1.3.1.2(2)(a)	基本	事務従事者は、利用する情報に明示等された格付けに従って、当該情報を適切に取り扱うこと。格付けに加えて取扱制限の明示等がなされている場合には、当該取扱制限の指示内容に従って取り扱うこと。	事務従事者							○								
(3) 格付け及び取扱制限の複製時における継承																		
1.3.1.2(3)(a)	基本	事務従事者は、情報を複製する場合には、元となる情報の機密性に係る格付け及び取扱制限を継承すること。	事務従事者							○								
(4) 格付け及び取扱制限の見直し																		
1.3.1.2(4)(a)	基本	事務従事者は、情報を利用する場合に、元の格付け又は取扱制限がその時点で不適切と考えるため、他者が決定した情報の格付け又は取扱制限そのものを見直す必要があると思料する場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下、この項において「決定者等」という。）に相談すること。	事務従事者							○								
1.3.1.2(4)(b)	基本	事務従事者は、自らが格付け及び取扱制限の決定者等である情報に対して、見直しの必要があると認めた場合には、当該情報の格付け又は取扱制限を再決定し、それを明示等すること。また、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知すること。	事務従事者							○								
(5) 要保護情報の取扱い																		
1.3.1.2(5)(a)	基本	事務従事者は、大学事務の遂行以外の目的で、要保護情報を学外に持ち出さないこと。	事務従事者							○								
1.3.1.2(5)(b)	基本	事務従事者は、要保護情報を放置しないこと。	事務従事者							○								
1.3.1.2(5)(c)	基本	事務従事者は、機密性3情報を必要以上に複製しないこと。	事務従事者							○								
1.3.1.2(5)(d)	基本	事務従事者は、要機密情報を必要以上に配付しないこと。	事務従事者							○								
1.3.1.2(5)(e)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、事務従事者は、機密性3情報には、機密性3情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付けを下げる又は取扱制限を緩和する必要性があると思料される場合には、格付け及び取扱制限の見直しに必要な処理を行うこと。	事務従事者							○								
1.3.1.2(5)(f)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、事務従事者は、機密性3情報である書面には、一連番号を付し、その所在を明らかにしておくこと。	事務従事者							○								
1.3.1.3 情報の保存																		
(1) 格付けに応じた情報の保存																		
1.3.1.3(1)(a)	基本	事務従事者は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うこと。	事務従事者							○								
1.3.1.3(1)(b)	基本	事務従事者は、情報の格付け及び取扱制限に応じて、情報が保存された電磁的記録媒体を適切に管理すること。	事務従事者							○								
1.3.1.3(1)(c)	基本	事務従事者は、情報システムに入力された情報若しくは情報システムから出力した情報を記載した書面のうち要機密情報である書面、又は重要な設計書を適切に管理すること。	事務従事者							○								
1.3.1.3(1)(d)	基本	事務従事者は、要機密情報を電磁的記録媒体に保存する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。	事務従事者							○								
1.3.1.3(1)(e)	基本	事務従事者は、要機密情報を電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。	事務従事者							○								
1.3.1.3(1)(f)	基本	事務従事者は、要保全情報を電磁的記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。	事務従事者							○								
1.3.1.3(1)(g)	基本	事務従事者は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。	事務従事者							○								

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.3.1.3(1)(h)	基本	事務従事者は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書の複写の保管について、災害等により生ずる支障の有無を検討し、支障があると認めたときは、適切な措置を講ずること。	事務従事者							○								
(2) 情報の保存期間																		
1.3.1.3(2)(a)	基本	事務従事者は、電磁的記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること。	事務従事者							○								
1.3.1.4 情報の移送																		
(1) 情報の移送に関する許可及び届出																		
1.3.1.4(1)(a)	基本	事務従事者は、機密性3情報、完全性2情報若しくは可用性2情報又は重要な設計書を移送する場合には、職場情報セキュリティ責任者の許可を得ること。	事務従事者							○								
1.3.1.4(1)(b)	基本	事務従事者は、機密性2情報であって完全性1情報かつ可用性1情報である電磁的記録又は機密性2情報である書面を移送する場合には、職場情報セキュリティ責任者に届け出ること。ただし、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。	事務従事者							○								
(2) 情報の送信と運搬の選択																		
1.3.1.4(2)(a)	基本	事務従事者は、要保護情報である電磁的記録を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを選択し、職場情報セキュリティ責任者に届け出ること。ただし、機密性2情報であって完全性1情報かつ可用性1情報である電磁的記録の移送であり、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。	事務従事者							○								
(3) 移送手段の決定																		
1.3.1.4(3)(a)	基本	事務従事者は、要保護情報又は重要な設計書を移送する場合には、安全確保に留意して、当該情報の移送手段を決定し、職場情報セキュリティ責任者に届け出ること。ただし、機密性2情報であって完全性1情報かつ可用性1情報である電磁的記録又は機密性2情報である書面の移送であり、職場情報セキュリティ責任者が届出を要しないと定めた移送については、この限りでない。	事務従事者							○								
(4) 書面の保護対策																		
1.3.1.4(4)(a)	基本	事務従事者は、要機密情報である書面又は重要な設計書を運搬する場合には、情報の格付け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。	事務従事者							○								
(5) 電磁的記録の保護対策																		
1.3.1.4(5)(a)	基本	事務従事者は、要機密情報である電磁的記録を移送する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。	事務従事者							○								
1.3.1.4(5)(b)	基本	事務従事者は、要機密情報である電磁的記録を移送する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。	事務従事者							○								
1.3.1.4(5)(c)	基本	事務従事者は、要保全情報である電磁的記録を移送する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。	事務従事者							○								
1.3.1.4(5)(d)	基本	事務従事者は、要保全情報である電磁的記録を移送する場合には、バックアップを行う必要性の有無を検討し、必要があると認めたときは、情報のバックアップを取得すること。	事務従事者							○								
1.3.1.4(5)(e)	基本	事務従事者は、要安定情報である電磁的記録を移送する場合には、移送中の滅失、紛失、移送先への到着時間の遅延等により支障が起こるおそれに対し、同一の電磁的記録を異なる移送経路で移送するなどの措置を講ずる必要性の有無を検討し、必要があると認めたときは、所要の措置を講ずること。	事務従事者							○								
1.3.1.4(5)(f)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、事務従事者は、要機密情報である電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いること。	事務従事者							○								
1.3.1.5 情報の提供																		
(1) 情報の公表																		
1.3.1.5(1)(a)	基本	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情報に格付けされるものであることを確認すること。	事務従事者							○								
1.3.1.5(1)(b)	基本	事務従事者は、電磁的記録を公表する場合には、当該情報の付加情報等からの不用意な情報漏えいを防止するための措置を講ずること。	事務従事者							○								
(2) 他者への情報の提供																		
1.3.1.5(2)(a)	基本	事務従事者は、機密性3情報、完全性2情報若しくは可用性2情報又は重要な設計書を教職員等以外の者に提供する場合には、職場情報セキュリティ責任者の許可を得ること。	事務従事者							○								
1.3.1.5(2)(b)	基本	事務従事者は、機密性2情報であって完全性1情報かつ可用性1情報である電磁的記録又は機密性2情報である書面を教職員等以外の者に提供する場合には、職場情報セキュリティ責任者に届け出ること。ただし、職場情報セキュリティ責任者が届出を要しないと定めた提供については、この限りでない。	事務従事者							○								
1.3.1.5(2)(c)	基本	事務従事者は、要保護情報又は重要な設計書を学外の者に提供する場合には、提供先において、当該情報に付された情報の格付け及び取扱制限に応じて適切に取り扱われるための措置を講ずること。	事務従事者							○								
1.3.1.5(2)(d)	基本	事務従事者は、電磁的記録を提供する場合には、当該記録の付加情報等からの不用意な情報漏えいを防止するための措置を講ずること。	事務従事者							○								
1.3.1.6 情報の消去																		
(1) 電磁的記録の消去方法																		
1.3.1.6(1)(a)	基本	事務従事者は、電磁的記録媒体を廃棄する場合には、すべての情報を復元が困難な状態にする（以下「抹消する」という。）こと。	事務従事者							○								

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.3.1.6(1)(b)	基本	事務従事者は、電磁的記録媒体を他の者へ提供する場合には、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。	事務従事者							○								
1.3.1.6(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、事務従事者は、電磁的記録媒体について、設置環境等から必要があると認められる場合は、当該電磁的記録媒体の要機密情報を抹消すること。	事務従事者							○								
(2) 書面の廃棄方法																		
1.3.1.6(2)(a)	基本	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。	事務従事者							○								
第1.4部 情報処理についての対策																		
1.4.1 情報処理の制限																		
1.4.1.1 学外での情報処理の制限																		
(1) 安全管理措置についての規定の整備																		
1.4.1.1(1)(a)	基本	全学実施責任者は、要保護情報について学外での情報処理を行う場合の安全管理措置についての規定を整備すること。	全学実施責任者		○													
1.4.1.1(1)(b)	基本	全学実施責任者は、要保護情報を取り扱う情報システムを学外に持ち出す場合の安全管理措置についての規定を整備すること。	全学実施責任者		○													
(2) 許可及び届出の取得及び管理																		
1.4.1.1(2)(a)	基本	事務従事者は、機密性3情報、完全性2情報又は可用性2情報について学外で情報処理を行う場合には、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。	事務従事者							○								
1.4.1.1(2)(b)	基本	事務従事者は、機密性2情報であって完全性1情報かつ可用性1情報である情報について学外で情報処理を行う場合には、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。	事務従事者							○								
1.4.1.1(2)(c)	基本	部局技術責任者及び職場情報セキュリティ責任者は、学外での要保護情報の情報処理に係る記録を取得すること。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
1.4.1.1(2)(d)	基本	部局技術責任者及び職場情報セキュリティ責任者は、機密性3情報、完全性2情報又は可用性2情報について学外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
1.4.1.1(2)(e)	基本	部局技術責任者及び職場情報セキュリティ責任者は、機密性2情報であって完全性1情報かつ可用性1情報である情報について学外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
1.4.1.1(2)(f)	基本	事務従事者は、要保護情報について学外で情報処理を行う場合には、業務の遂行に必要最小限の情報処理にとどめること。	事務従事者							○								
1.4.1.1(2)(g)	基本	事務従事者は、機密性3情報、完全性2情報又は可用性2情報を取り扱う情報システムを学外に持ち出す場合には、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。	事務従事者							○								
1.4.1.1(2)(h)	基本	事務従事者は、機密性2情報であって完全性1情報かつ可用性1情報である情報を取り扱う情報システムを学外に持ち出す場合には、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。	事務従事者							○								
1.4.1.1(2)(i)	基本	部局技術責任者及び職場情報セキュリティ責任者は、要保護情報を取り扱う情報システムの学外への持出しに係る記録を取得すること。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
1.4.1.1(2)(j)	基本	部局技術責任者及び職場情報セキュリティ責任者は、機密性3情報、完全性2情報又は可用性2情報を取り扱う情報システムを学外に持ち出すことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
1.4.1.1(2)(k)	基本	部局技術責任者及び職場情報セキュリティ責任者は、機密性2情報であって完全性1情報かつ可用性1情報である情報を取り扱う情報システムを学外に持ち出すことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
1.4.1.1(2)(l)	基本	事務従事者は、要保護情報を取り扱う情報システムを学外に持ち出す場合には、業務の遂行に必要最小限の情報システムの持出しにとどめること。	事務従事者							○								
(3) 安全管理措置の遵守																		
1.4.1.1(3)(a)	基本	事務従事者は、要保護情報について学外での情報処理について定められた安全管理措置を講ずること。	事務従事者							○								
1.4.1.1(3)(b)	基本	事務従事者は、機密性3情報、完全性2情報又は可用性2情報について学外での情報処理を行うことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。	事務従事者							○								
1.4.1.1(3)(c)	基本	事務従事者は、要保護情報を取り扱う情報システムの学外への持出しについて定められた安全管理措置を講ずること。	事務従事者							○								
1.4.1.1(3)(d)	基本	事務従事者は、機密性3情報、完全性2情報又は可用性2情報を取り扱う情報システムを学外に持ち出すことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。	事務従事者							○								
1.4.1.2 本学支給以外の情報システムによる情報処理の制限																		
(1) 安全管理措置についての規定の整備																		
1.4.1.2(1)(a)	基本	全学実施責任者は、要保護情報について本学支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備すること。	全学実施責任者		○													
(2) 許可及び届出の取得及び管理																		
1.4.1.2(2)(a)	基本	事務従事者は、機密性3情報、完全性2情報又は可用性2情報について本学支給以外の情報システムにより情報処理を行う必要がある場合には、部局技術責任者及び職場情報セキュリティ責任者の許可を得ること。	事務従事者							○								

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.4.1.2(2)(b)	基本	事務従事者は、機密性2情報であって完全性1情報かつ可用性1情報である情報について本学支給以外の情報システムにより情報処理を行う必要がある場合には、部局技術責任者及び職場情報セキュリティ責任者に届け出ること。ただし、部局技術責任者又は職場情報セキュリティ責任者が届出を要しないとした場合は、この限りでない。	事務従事者							○								
1.4.1.2(2)(c)	基本	部局技術責任者及び職場情報セキュリティ責任者は、本学支給以外の情報システムによる要保護情報の情報処理に係る記録を取得すること。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
1.4.1.2(2)(d)	基本	部局技術責任者及び職場情報セキュリティ責任者は、機密性3情報、完全性2情報又は可用性2情報について本学支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、措置を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
1.4.1.2(2)(e)	基本	部局技術責任者及び職場情報セキュリティ責任者は、機密性2情報であって完全性1情報かつ可用性1情報である情報について本学支給以外の情報システムによる情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、措置を講ずること。	部局技術責任者及び職場情報セキュリティ責任者				○		○									
(3) 安全管理措置の遵守																		
1.4.1.2(3)(a)	基本	事務従事者は、要保護情報について本学支給以外の情報システムによる情報処理を行う場合には、当該情報システムについて定められた安全管理措置を講ずること。	事務従事者							○								
1.4.1.2(3)(b)	基本	事務従事者は、機密性3情報、完全性2情報又は可用性2情報について本学支給以外の情報システムによる情報処理を終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。	事務従事者							○								
第1.5部 情報システムについての基本的な対策																		
1.5.1 情報システムのセキュリティ要件																		
1.5.1.1 情報システムのセキュリティ要件																		
(1) 情報システムの計画																		
1.5.1.1(1)(a)	基本	部局技術責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、情報システムを統括する責任者に求めること。	部局技術責任者				○											
1.5.1.1(1)(b)	基本	部局技術責任者は、情報システムのセキュリティ要件を決定すること。	部局技術責任者				○											
1.5.1.1(1)(c)	基本	部局技術責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。	部局技術責任者				○											
1.5.1.1(1)(d)	基本	部局技術責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST評価・ST確認を受けること。ただし、情報システムを更改し、又は構築中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。	部局技術責任者				○											
1.5.1.1(1)(e)	基本	部局技術責任者は、情報システムについて、情報セキュリティの侵害又はそのおそれのある事象の発生を監視する必要性の有無を検討し、必要があると認めた場合には、監視のために必要な措置を定めること。	部局技術責任者				○											
1.5.1.1(1)(f)	基本	部局技術責任者は、構築した情報システムを運用段階へ導入するに当たって、情報セキュリティの観点から実施する導入のための手順及び環境を定めること。	部局技術責任者				○											
1.5.1.1(1)(g)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、構築する情報システムの構成要素については、重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合であって、その中に当該セキュリティ機能に関してITセキュリティ評価及び認証制度に基づく認証を取得している製品がある場合には、当該製品を情報システムの構成要素として選択すること。	部局技術責任者				○											
(2) 情報システムの構築・運用																		
1.5.1.1(2)(a)	基本	部局技術責任者は、情報システムの構築、運用に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行うこと。	部局技術責任者				○											
(3) 情報システムの移行・廃棄																		
1.5.1.1(3)(a)	基本	部局技術責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を講ずること。	部局技術責任者				○											
(4) 情報システムの見直し																		
1.5.1.1(4)(a)	基本	部局技術責任者は、情報システムの情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。	部局技術責任者				○											
1.5.2 情報システムに係る規定の整備と遵守																		
1.5.2.1 情報システムに係る文書及び台帳整備																		
(1) 情報システムの文書整備																		
1.5.2.1(1)(a)	基本	部局技術責任者は、所管する情報システムについて以下の事項を記載した文書を整備すること。	部局技術責任者				○											
1.5.2.1(1)(a)(ア)		当該情報システムを構成する電子計算機関連事項 ・電子計算機を管理する事務従事者及び利用者を特定する情報 ・電子計算機の機種並びに利用しているソフトウェアの種類及びバージョン ・電子計算機の仕様書又は設計書																

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.5.2.1(1)(a)(イ)		当該情報システムを構成する通信回線及び通信回線装置関連事項 ・通信回線及び通信回線装置を管理する事務従事者を特定する情報 ・通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン ・通信回線及び通信回線装置の仕様書又は設計書 ・通信回線の構成 ・通信回線装置におけるアクセス制御の設定 ・通信回線を利用する電子計算機の識別コード、電子計算機の利用者と当該利用者の識別コードとの対応 ・通信回線の利用部署																
1.5.2.1(1)(a)(ウ)		情報システムの構成要素のセキュリティ維持に関する手順 ・電子計算機のセキュリティ維持に関する手順 ・通信回線を介して提供するサービスのセキュリティ維持に関する手順 ・通信回線及び通信回線装置のセキュリティ維持に関する手順																
1.5.2.1(1)(a)(エ)		障害・事故等が発生した際の対処手順																
1.5.2.1(1)(b)	基本	部局技術担当者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理において情報セキュリティ対策を行うこと。	部局技術担当者					○										
(2) 情報システムの台帳整備																		
1.5.2.1(2)(a)	基本	全学実施責任者は、すべての情報システムに対して、当該情報システムに係る以下の事項を記載した台帳を整備すること。	全学実施責任者		○													
1.5.2.1(2)(a)(ア)		情報システム名、管理課室及び管理責任者の氏名・連絡先																
1.5.2.1(2)(a)(イ)		システム構成																
1.5.2.1(2)(a)(ウ)		接続する学外通信回線の種別																
1.5.2.1(2)(a)(エ)		取り扱う情報の格付け及び取扱制限に関する事項																
1.5.2.1(2)(a)(オ)		当該情報システムの設計・開発、運用、保守に関する事項																
1.5.2.1(2)(b)	基本	部局技術責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システムの台帳の記載事項について全学実施責任者に報告すること。	部局技術責任者				○											
1.5.2.2 機器等の購入																		
(1) 機器等の購入に係る規定の整備																		
1.5.2.2(1)(a)	基本	全学実施責任者は、機器等の選定基準を整備すること。	全学実施責任者		○													
1.5.2.2(1)(b)	基本	全学実施責任者は、機器等の購入において、セキュリティ機能の要求仕様があり、総合評価落札方式により購入を行う際には、ITセキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用することを選定基準として定めること。	全学実施責任者		○													
1.5.2.2(1)(c)	基本	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。	全学実施責任者		○													
(2) 機器等の購入に係る規定の遵守																		
1.5.2.2(2)(a)	基本	部局技術責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の候補の選定における判断の一要素として活用すること。	部局技術責任者				○											
1.5.2.2(2)(b)	基本	部局技術責任者は、機器等の納入時において、定められた確認・検査手続に従って、納品検査を実施すること。	部局技術責任者				○											
1.5.2.3 ソフトウェア開発																		
(1) ソフトウェア開発に係る規定の整備																		
1.5.2.3(1)(a)	基本	全学実施責任者は、ソフトウェア開発について、セキュリティに係る以下の対策事項を部局技術責任者に求めるための規定を整備すること。	全学実施責任者		○													
1.5.2.3(1)(a)(ア)		部局技術責任者は、セキュリティに係る対策事項（本項(ウ)から(セ)の遵守事項）を満たすことが可能な開発体制を確保すること。	部局技術責任者				○											
1.5.2.3(1)(a)(イ)		部局技術責任者は、ソフトウェア開発を外部委託する場合には、セキュリティに係る対策事項（本項(ウ)から(セ)の遵守事項）の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。	部局技術責任者				○											
1.5.2.3(1)(a)(ウ)		部局技術責任者は、ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。	部局技術責任者				○											
1.5.2.3(1)(a)(エ)		部局技術責任者は、ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムと分離する必要性の有無を検討し、必要と認めたときは分離すること。	部局技術責任者				○											
1.5.2.3(1)(a)(オ)		部局技術責任者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果並びに当該ソフトウェアにおいて取り扱う情報の格付け及び取扱制限に応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときは、セキュリティ機能を適切に設計し、設計書に明確に記述すること。	部局技術責任者				○											
1.5.2.3(1)(a)(カ)		部局技術責任者は、開発するソフトウェアが運用される際に利用されるセキュリティ機能についての管理機能の必要性の有無を検討し、必要と認めたときは、管理機能を適切に設計し、設計書に明確に記述すること。	部局技術責任者				○											
1.5.2.3(1)(a)(キ)		部局技術責任者は、ソフトウェアの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。	部局技術責任者				○											
1.5.2.3(1)(a)(ク)		部局技術責任者は、開発するソフトウェアにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要と認めたときは、その方法を適切に設計し、設計書に明確に記述すること。	部局技術責任者				○											
1.5.2.3(1)(a)(ケ)		部局技術責任者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST評価・ST確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書のST評価・ST確認を受ける場合、又はソフトウェアを更改し、若しくは開発中に仕様変更が発生した場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。	部局技術責任者				○											

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.5.2.3(1)(a)(コ)		部局技術責任者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスから保護するとともに、バックアップを取得すること。	部局技術責任者				○											
1.5.2.3(1)(a)(サ)		部局技術責任者は、情報セキュリティの観点からコーディングに関する規定を整備すること。	部局技術責任者				○											
1.5.2.3(1)(a)(シ)		部局技術責任者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの必要性の有無を検討し、必要と認めたときは、ソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。	部局技術責任者				○											
1.5.2.3(1)(a)(ス)		部局技術責任者は、セキュリティの観点から実施する試験の必要性の有無を検討し、必要と認めたときは実施する試験項目及び試験方法を定め、これに基づいて試験を実施すること。	部局技術責任者				○											
1.5.2.3(1)(a)(セ)		部局技術責任者は、情報セキュリティの観点から実施した試験の実施記録を保存すること。	部局技術責任者				○											
(2) ソフトウェア開発に係る規定の遵守																		
1.5.2.3(2)(a)	基本	部局技術責任者は、ソフトウェア開発に係る規定に基づいて、ソフトウェアの開発を行うこと。	部局技術責任者				○											
1.5.2.4 暗号と電子署名の標準手順																		
(1) 暗号と電子署名に係る規定の整備																		
1.5.2.4(1)(a)	基本	全学実施責任者は、本学における暗号化及び電子署名のアルゴリズム及び方法を、以下の事項を含めて定めること。	全学実施責任者		○													
1.5.2.4(1)(a)(ア)		電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること。																
1.5.2.4(1)(a)(イ)		情報システムの新規構築又は更新に伴い暗号化又は電子署名を導入する場合には、電子政府推奨暗号リスト又は、本学における検証済み暗号リストがあればその中に記載されたアルゴリズムを使用すること。ただし、使用するアルゴリズムを複数のアルゴリズムの中から選択可能とするよう暗号化又は電子署名を実装する箇所においては、当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。																
1.5.2.4(1)(b)	基本	全学実施責任者は、暗号化された情報（書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵について、以下の（ア）及び（イ）の手順（以下「鍵の管理手順等」という。）を定めること。	全学実施責任者		○													
1.5.2.4(1)(b)(ア)		鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対処手順等																
1.5.2.4(1)(b)(イ)		鍵の保存手順																
1.5.2.4(1)(c)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、全学実施責任者は、暗号化された情報の復号に用いる鍵のバックアップの取得手順又は鍵の預託手順（以下「鍵のバックアップ手順等」という。）を定めること。	全学実施責任者		○													
(2) 暗号と電子署名に係る規定の遵守																		
1.5.2.4(2)(a)	基本	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。	事務従事者							○								
1.5.2.4(2)(b)	基本	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。	事務従事者							○								
1.5.2.4(2)(c)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、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、定められた鍵のバックアップ手順等に従い、そのバックアップを取得すること。	事務従事者							○								
1.5.2.5 学外の情報セキュリティ水準の低下を招く行為の防止																		
(1) 措置についての規定の整備																		
1.5.2.5(1)(a)	基本	全学実施責任者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備すること。	全学実施責任者		○													
(2) 規定の遵守																		
1.5.2.5(2)(a)	基本	事務従事者は、学外の情報セキュリティ水準の低下を招く行為の防止の規定に基づいて、必要な措置を講ずること。	事務従事者							○								
1.5.2.6 ドメイン名の使用についての対策																		
(1) ドメイン名の使用についての規定の整備																		
1.5.2.6(1)(a)	基本	全学実施責任者は、ドメインネームシステムによるドメイン名（以下「ドメイン名」と言う。）の使用について、以下の事項を事務従事者に求める規定を整備すること。	全学実施責任者		○													
1.5.2.6(1)(a)(ア)		事務従事者は、学外の者（国外在住の者を除く。以下、本項において同じ。）に対して、アクセスや送信させることを目的としてドメイン名を告知する場合に、以下のA大学及びA大学を運営する国立大学法人のドメイン名であることが保証されるドメイン名（以下「A大学ドメイン名」という。）を使用すること。																
1.5.2.6(1)(a)(イ)		事務従事者は、教職員等以外の者に対して、電子メールの送信元としてドメイン名を使用する場合には、A大学ドメイン名を使用すること。ただし、当該教職員等以外の者にとって、当該事務従事者が既知の者である場合を除く。																
1.5.2.6(1)(a)(ウ)		事務従事者は、教職員等以外の者に対して、アクセスさせることを目的として情報を保存するためにサーバを使用する場合には、A大学ドメイン名のサーバだけを使用すること。																
(2) ドメイン名の使用についての規定の遵守																		
1.5.2.6(2)(a)	基本	事務従事者は、ドメイン名の使用についての規定に基づいて、必要な措置を講ずること。	事務従事者							○								
1.5.2.7 不正プログラム感染防止のための日常的実施事項																		
(1) 不正プログラム対策に係る規定の整備																		
1.5.2.7(1)(a)	基本	全学実施責任者は、不正プログラム感染の回避を目的として、以下の措置を事務従事者に求める規定を整備すること。	全学実施責任者		○													
1.5.2.7(1)(a)(ア)		事務従事者は、アンチウイルスソフトウェア等により不正プログラムとして検知された実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。								○								

管理番号		基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
1.5.2.7(1)(a)(イ)			事務従事者は、アンチウイルスソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。								○								
1.5.2.7(1)(a)(ウ)			事務従事者は、アンチウイルスソフトウェア等による不正プログラムの自動検査機能を有効にすること。								○								
1.5.2.7(1)(a)(エ)			事務従事者は、アンチウイルスソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること。								○								
1.5.2.7(1)(a)(オ)			事務従事者は、外部からデータやソフトウェアを電子計算機等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。								○								
1.5.2.7(1)(a)(カ)			事務従事者は、不正プログラム感染の予防に努めること。								○								
1.5.2.7(1)(a)(キ)			事務従事者は、不正プログラムに感染した恐れのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講じること。								○								
(2) 不正プログラム対策に係る規定の遵守																			
1.5.2.7(2)(a)		基本	事務従事者は、定められた不正プログラム対策に係る規定に基づいて、不正プログラムの感染を防止するための対策を行うこと。	事務従事者							○								
第2編 情報システム編																			
第2.1部 情報セキュリティ要件の明確化に基づく対策																			
2.1.1 情報セキュリティについての機能																			
2.1.1.1 主体認証機能																			
(1) 主体認証機能の導入																			
2.1.1.1(1)(a)		基本	部局技術責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断すること。	部局技術責任者				○											
2.1.1.1(1)(b)		基本	部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、識別及び主体認証を行う機能を設けること。	部局技術責任者				○											
2.1.1.1(1)(c)		基本	部局技術担当者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。	部局技術担当者					○										
2.1.1.1(1)(c)(ア)			主体認証情報を保存する場合には、その内容の暗号化を行うこと。																
2.1.1.1(1)(c)(イ)			主体認証情報を通信する場合には、その内容の暗号化を行うこと。																
2.1.1.1(1)(c)(ウ)			保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更、提供(入力)させる際に、暗号化が行われない旨を通知すること。																
2.1.1.1(1)(d)		基本	部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。	部局技術責任者				○											
2.1.1.1(1)(d)(ア)			利用者が定期的に変更しているか否かを確認する機能																
2.1.1.1(1)(d)(イ)			利用者が定期的に変更しなければ、情報システムの利用を継続させない機能																
2.1.1.1(1)(e)		基本	部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報又は主体認証情報格納装置を他者に使用され、又は使用される危険性を認識した場合に、直ちに当該主体認証情報若しくは主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けること。	部局技術責任者				○											
2.1.1.1(1)(f)		基本	部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識による主体認証方式を用いる場合には、以下の機能を設けること。	部局技術責任者				○											
2.1.1.1(1)(f)(ア)			利用者が、自らの主体認証情報を設定する機能																
2.1.1.1(1)(f)(イ)			利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能																
2.1.1.1(1)(g)		基本	部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、その要件を定めるに際して、以下の事項が適用可能かどうかを検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。	部局技術責任者				○											
2.1.1.1(1)(g)(ア)			正当な主体以外の主体認証を受諾しないこと。(誤認の防止)																
2.1.1.1(1)(g)(イ)			正当な主体が本人の責任ではない理由で主体認証を拒否されないこと。(誤否の防止)																
2.1.1.1(1)(g)(ウ)			正当な主体が容易に他者に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。)及び貸与ができないこと。(代理の防止)																
2.1.1.1(1)(g)(エ)			主体認証情報が容易に複製できないこと。(複製の防止)																
2.1.1.1(1)(g)(オ)			部局技術担当者の判断により、ログオンを個々に無効化できる手段があること。(無効化の確保)																
2.1.1.1(1)(g)(カ)			必要時に中断することなく主体認証が可能であること。(可用性の確保)																
2.1.1.1(1)(g)(キ)			新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。(継続性の確保)																
2.1.1.1(1)(g)(ク)			主体に付与した主体認証情報を使用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。(再発行の確保)																
2.1.1.1(1)(h)		基本	部局技術責任者は、生体情報による主体認証方式を用いる場合には、当該生体情報を本人から事前に同意を得た目的以外の目的で使用しないこと。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。	部局技術責任者				○											
2.1.1.1(1)(i)		強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、複数要素(複合)主体認証方式で主体認証を行う機能を設けること。	部局技術責任者				○											

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.1.1.1(1)(j)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、ログオンした利用者に対して、前回のログオンに関する情報を通知する機能を設けること。	部局技術責任者				○											
2.1.1.1(1)(k)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、不正にログオンしようとする行為を検知し、又は防止する機能を設けること。	部局技術責任者				○											
2.1.1.1(1)(l)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者が情報システムにログインする前に、当該情報システムの利用に関する通知メッセージを表示する機能を設けること。	部局技術責任者				○											
2.1.1.1(1)(m)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、以前に設定した主体認証情報と同じものを再設定することを防止する機能を設けること。	部局技術責任者				○											
2.1.1.1(1)(n)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、主体認証を行う必要があると認めた情報システムにおいて、管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンすることが必要となる機能を設けること。	部局技術責任者				○											
(2) 識別コードの管理																		
2.1.1.1(2)(a)	基本	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。	事務従事者							○								
2.1.1.1(2)(b)	基本	事務従事者は、自己に付与された識別コードを他者に主体認証に用いる目的のために付与及び貸与しないこと。	事務従事者							○								
2.1.1.1(2)(c)	基本	事務従事者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。	事務従事者							○								
2.1.1.1(2)(d)	基本	事務従事者は、大学事務のために識別コードを利用する必要がなくなった場合は、その旨を部局技術担当者に届け出ること。ただし、個別の届出が必要ないと、部局技術責任者が定めている場合は、この限りでない。	事務従事者							○								
2.1.1.1(2)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、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。	事務従事者							○								
(3) 主体認証情報の管理																		
2.1.1.1(3)(a)	基本	事務従事者は、主体認証情報が他者に使用され、又はその危険が発生した場合には、直ちに部局技術責任者又は部局技術担当者にその旨を報告すること。	事務従事者							○								
2.1.1.1(3)(b)	基本	部局技術責任者又は部局技術担当者は、主体認証情報が他者に使用され、又はその危険が発生したことの報告を受けた場合には、必要な措置を講ずること。	部局技術責任者又は部局技術担当者				○	○										
2.1.1.1(3)(c)	基本	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。	事務従事者							○								
2.1.1.1(3)(c)(ア)		自己の主体認証情報を他者に知られないように管理すること。																
2.1.1.1(3)(c)(イ)		自己の主体認証情報を他者に教えないこと。																
2.1.1.1(3)(c)(ウ)		主体認証情報を忘却しないように努めること。																
2.1.1.1(3)(c)(エ)		主体認証情報を設定するに際しては、容易に推測されないものにすること。																
2.1.1.1(3)(c)(オ)		部局技術担当者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更すること。																
2.1.1.1(3)(d)	基本	事務従事者は、所有による主体認証を用いる場合には、以下の管理を徹底すること。	事務従事者							○								
2.1.1.1(3)(d)(ア)		主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理すること。																
2.1.1.1(3)(d)(イ)		主体認証情報格納装置を他者に付与及び貸与しないこと。																
2.1.1.1(3)(d)(ウ)		主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに部局技術責任者又は部局技術担当者にその旨を報告すること。																
2.1.1.1(3)(d)(エ)		主体認証情報格納装置を利用する必要がなくなった場合には、これを部局技術責任者又は部局技術担当者に返還すること。																
2.1.1.2 アクセス制御機能																		
(1) アクセス制御機能の導入																		
2.1.1.2(1)(a)	基本	部局技術責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。	部局技術責任者				○											
2.1.1.2(1)(b)	基本	部局技術責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設けること。	部局技術責任者				○											
2.1.1.2(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、利用者及び所属するグループの属性以外に基づくアクセス制御の機能を追加すること。	部局技術責任者				○											
2.1.1.2(1)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、強制アクセス制御機能を設けること。	部局技術責任者				○											
(2) 適正なアクセス制御																		
2.1.1.2(2)(a)	基本	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け及び取扱制限に従って、アクセス制御を行うこと。	部局技術責任者				○											
2.1.1.3 権限管理機能																		
(1) 権限管理機能の導入																		

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.1.1.3(1)(a)	基本	部局技術責任者は、すべての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。	部局技術責任者				○											
2.1.1.3(1)(b)	基本	部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。	部局技術責任者				○											
2.1.1.3(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、最少特権機能を設けること。	部局技術責任者				○											
2.1.1.3(1)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、主体認証情報の再発行を自動で行う機能を設けること。	部局技術責任者				○											
2.1.1.3(1)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、デュアルロック機能を設けること。	部局技術責任者				○											
(2) 識別コードと主体認証情報の付与管理																		
2.1.1.3(2)(a)	基本	部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、共用識別コードの利用許可については、情報システムごとにその必要性を判断すること。	部局技術責任者				○											
2.1.1.3(2)(b)	基本	部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理について、以下の事項を含む手続を定めること。	部局技術責任者				○											
2.1.1.3(2)(b)(ア)		主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続																
2.1.1.3(2)(b)(イ)		主体認証情報の初期配布方法及び変更管理手続																
2.1.1.3(2)(b)(ウ)		アクセス制御情報の設定方法及び変更管理手続																
2.1.1.3(2)(c)	基本	部局技術責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う者を定めること。	部局技術責任者				○											
2.1.1.3(2)(d)	基本	権限管理を行う者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を発行すること。	権限管理を行う者											○				
2.1.1.3(2)(e)	基本	権限管理を行う者は、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。	権限管理を行う者											○				
2.1.1.3(2)(f)	基本	権限管理を行う者は、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与（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。	権限管理を行う者											○				
2.1.1.3(2)(g)	基本	権限管理を行う者は、事務従事者が情報システムを利用する必要がなくなった場合には、当該事務従事者の識別コードを無効にすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不要な識別コードの有無を点検すること。	権限管理を行う者											○				
2.1.1.3(2)(h)	基本	権限管理を行う者は、事務従事者が情報システムを利用する必要がなくなった場合には、当該事務従事者に交付した主体認証情報格納装置を返還させること。	権限管理を行う者											○				
2.1.1.3(2)(i)	基本	権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与えるようにアクセス制御の設定をすること。また、人事異動等により、識別コードを追加し、又は削除する時に、不適切なアクセス制御設定の有無を点検すること。	権限管理を行う者											○				
2.1.1.3(2)(j)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、単一の情報システムにおいては、1人の事務従事者に対して単一の識別コードのみを付与すること。	権限管理を行う者											○				
2.1.1.3(2)(k)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、識別コードをどの主体に付与したかについて記録すること。当該記録を消去する場合には、部局総括責任者からの事前の承認を得ること。	権限管理を行う者											○				
2.1.1.3(2)(l)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。	権限管理を行う者											○				
(3) 識別コードと主体認証情報における代替手段等の適用																		
2.1.1.3(3)(a)	基本	部局技術担当者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった事務従事者から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。	部局技術担当者					○										
2.1.1.3(3)(b)	基本	部局技術責任者及び部局技術担当者は、権限管理を行う必要があると認めた情報システムにおいて、識別コードの不正使用の報告を受けた場合には、直ちに当該識別コードによる使用を停止させること。	部局技術責任者及び部局技術担当者				○	○										
2.1.1.4 証跡管理機能																		
(1) 証跡管理機能の導入																		
2.1.1.4(1)(a)	基本	部局技術責任者は、すべての情報システムについて、証跡管理を行う必要性の有無を検討すること。	部局技術責任者				○											
2.1.1.4(1)(b)	基本	部局技術責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。	部局技術責任者				○											
2.1.1.4(1)(c)	基本	部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡として取得する情報項目及び証跡の保存期間を定めること。	部局技術責任者				○											
2.1.1.4(1)(d)	基本	部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方法を定め、必要に応じ、これらの場合に対処するための機能を情報システムに設けること。	部局技術責任者				○											
2.1.1.4(1)(e)	基本	部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行うこと。	部局技術責任者				○											
2.1.1.4(1)(f)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡の点検、分析及び報告を支援するための自動化機能を情報システムに設けること。	部局技術責任者				○											

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.1.1.4(1)(g)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、取得した証跡の内容により、情報セキュリティの侵害の可能性を示す事象を検知した場合に、監視する者等にその旨を即時に通知する機能を情報システムに設けること。	部局技術責任者				○											
(2) 証跡の取得と保存																		
2.1.1.4(2)(a)	基本	部局技術担当者は、証跡を取得する必要があると認めた情報システムにおいては、部局技術責任者が情報システムに設けた機能を利用して、証跡を記録すること。	部局技術担当者					○										
2.1.1.4(2)(b)	基本	部局技術担当者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間が満了する日まで当該証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。保存期間は、学外にアクセスする情報システムにおいては3ヶ月以上とし、特に重要な情報を取り扱う情報システムにおいては1年以上として定めること。	部局技術担当者					○										
2.1.1.4(2)(c)	基本	部局技術担当者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処方法に基づいて対処すること。	部局技術担当者					○										
(3) 取得した証跡の点検、分析及び報告																		
2.1.1.4(3)(a)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又は部局総括責任者に報告すること。	部局技術責任者				○											
(4) 証跡管理に関する利用者への周知																		
2.1.1.4(4)(a)	基本	部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、部局技術担当者及び利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。	部局技術責任者				○											
2.1.1.5 保証のための機能																		
(1) 保証のための機能の導入																		
2.1.1.5(1)(a)	基本	部局技術責任者は、要保護情報を取り扱う情報システムについて、保証のための対策を行う必要性の有無を検討すること。	部局技術責任者				○											
2.1.1.5(1)(b)	基本	部局技術責任者は、保証のための対策を行う必要があると認めた情報システムにおいて、保証のための機能を設けること。	部局技術責任者				○											
2.1.1.6 暗号と電子署名(鍵管理を含む)																		
(1) 暗号化機能及び電子署名機能の導入																		
2.1.1.6(1)(a)	基本	部局技術責任者は、要機密情報(書面を除く。以下この項において同じ。)を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。	部局技術責任者				○											
2.1.1.6(1)(b)	基本	部局技術責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。	部局技術責任者				○											
2.1.1.6(1)(c)	基本	部局技術責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与及び検証を行う機能を付加する必要性の有無を検討すること。	部局技術責任者				○											
2.1.1.6(1)(d)	基本	部局技術責任者は、電子署名の付与又は検証を行う必要があると認めた情報システムには、電子署名の付与又は検証を行う機能を設けること。	部局技術責任者				○											
2.1.1.6(1)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。	部局技術責任者				○											
2.1.1.6(1)(f)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、複数のアルゴリズムを選択可能とすること。	部局技術責任者				○											
2.1.1.6(1)(g)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択すること。	部局技術責任者				○											
2.1.1.6(1)(h)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵を、第三者による物理的な攻撃から保護するために、耐タンパー性を有する暗号モジュールへ格納すること。	部局技術責任者				○											
(2) 暗号化及び電子署名に係る管理																		
2.1.1.6(2)(a)	基本	部局技術責任者は、電子署名の付与を行う必要があると認めた情報システムにおいて、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供すること。	部局技術責任者				○											
2.1.1.6(2)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。	部局技術責任者				○											
2.1.2 情報セキュリティについての脅威																		
2.1.2.1 セキュリティホール対策																		
(1) 情報システムの構築時																		
2.1.2.1(1)(a)	基本	部局技術責任者は、電子計算機及び通信回線装置(公開されたセキュリティホールの情報がない電子計算機及び通信回線装置を除く。以下この項において同じ。)の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。	部局技術責任者				○											

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.1.2.1(1)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、セキュリティホール対策中にサービス提供が中断しないように、電子計算機及び通信回線装置を冗長構成にすること。	部局技術責任者				○											
2.1.2.1(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、公開されたセキュリティホールの情報がない段階においても電子計算機及び通信回線装置上で採り得る対策を実施すること。	部局技術責任者				○											
(2) 情報システムの運用時																		
2.1.2.1(2)(a)	基本	部局技術担当者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、公開されたセキュリティホールに関連する情報を適宜入手すること。	部局技術担当者					○										
2.1.2.1(2)(b)	基本	部局技術責任者は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関して、セキュリティホールに関連する情報を入手した場合には、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を策定すること。	部局技術責任者				○											
2.1.2.1(2)(b)(ア)		対策の必要性																
2.1.2.1(2)(b)(イ)		対策方法																
2.1.2.1(2)(b)(ウ)		対策方法が存在しない場合の一時的な回避方法																
2.1.2.1(2)(b)(エ)		対策方法又は回避方法が情報システムに与える影響																
2.1.2.1(2)(b)(オ)		対策の実施予定																
2.1.2.1(2)(b)(カ)		対策試験の必要性																
2.1.2.1(2)(b)(キ)		対策試験の方法																
2.1.2.1(2)(b)(ク)		対策試験の実施予定																
2.1.2.1(2)(c)	基本	部局技術担当者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。	部局技術担当者					○										
2.1.2.1(2)(d)	基本	部局技術担当者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者を含む事項を記録すること。	部局技術担当者					○										
2.1.2.1(2)(e)	基本	部局技術担当者は、信頼できる方法でパッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイル（以下、「対策用ファイル」という。）を入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。	部局技術担当者					○										
2.1.2.1(2)(f)	基本	部局技術担当者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び通信回線装置が確認された場合の対処を行うこと。	部局技術担当者					○										
2.1.2.1(2)(g)	基本	部局技術責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、他の部局技術責任者と共有すること。	部局技術責任者				○											
2.1.2.2 不正プログラム対策																		
(1) 情報システムの構築時																		
2.1.2.2(1)(a)	基本	部局技術責任者は、電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。以下この項において同じ。）にアンチウイルスソフトウェア等を導入すること。	部局技術責任者				○											
2.1.2.2(1)(b)	基本	部局技術責任者は、想定される不正プログラムの感染経路のすべてにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。	部局技術責任者				○											
2.1.2.2(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、想定される不正プログラムの感染経路において、複数の種類のアンチウイルスソフトウェア等を組み合わせ、導入すること。	部局技術責任者				○											
2.1.2.2(1)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、不正プログラムが通信により拡散することを防止するための対策を実施すること。	部局技術責任者				○											
(2) 情報システムの運用時																		
2.1.2.2(2)(a)	基本	部局技術担当者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、事務従事者にその対処の実施に関する指示を行うこと。	部局技術担当者					○										
2.1.2.2(2)(b)	基本	部局技術責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。	部局技術責任者				○											
2.1.2.3 サービス不能攻撃対策																		
(1) 情報システムの構築時																		
2.1.2.3(1)(a)	基本	部局技術責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける電子計算機、通信回線装置又は通信回線を有する情報システムに限る。以下この項において同じ。）については、サービス提供に必要な電子計算機及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。	部局技術責任者				○											
2.1.2.3(1)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、情報システムがサービス不能攻撃を受けた場合に影響が最小となるように情報システムを構築すること。	部局技術責任者				○											
2.1.2.3(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受ける電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法及び監視記録の保存期間を定めること。	部局技術責任者				○											
2.1.2.3(1)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、電子計算機、通信回線装置又は通信回線に対するサービス不能攻撃の影響を排除し、又は低減する対策装置を導入すること。	部局技術責任者				○											
2.1.2.3(1)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合に攻撃への対処を効果的に実施できる手段を確保しておくこと。	部局技術責任者				○											
2.1.2.3(1)(f)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機、通信回線装置又は通信回線を冗長構成にすること。	部局技術責任者				○											

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.1.2.3(1)(g)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、電子計算機や通信回線装置における対策だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し、インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を整備すること。	部局技術責任者				○											
(2) 情報システムの運用時																		
2.1.2.3(2)(a)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術担当者は、要安定情報を取り扱う情報システムについては、監視方法に従って電子計算機、通信回線装置及び通信回線を監視し、その記録を保存すること。	部局技術担当者					○										
2.1.2.4 踏み台対策																		
(1) 情報システムの構築時																		
2.1.2.4(1)(a)	基本	部局技術責任者は、情報システム（インターネット等の学外の通信回線に接続される電子計算機、通信回線装置又は通信回線を有する情報システムに限る。以下この項において同じ。）が踏み台として使われることを防止するための措置を講ずること。	部局技術責任者				○											
2.1.2.4(1)(b)	基本	部局技術責任者は、情報システムを踏み台として使われた場合の影響が最小となるように情報システムを構築すること。	部局技術責任者				○											
2.1.2.4(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、情報システムが踏み台になっているか否かを監視するための監視方法及び監視記録の保存期間を定めること。	部局技術責任者				○											
(2) 情報システムの運用時																		
2.1.2.4(2)(a)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術担当者は、定められた監視方法に従って情報システムを監視し、その記録を保存すること。	部局技術担当者					○										
第2.2部 情報システムの構成要素についての対策																		
2.2.1 施設と環境																		
2.2.1.1 電子計算機及び通信回線装置を設置する安全区域																		
(1) 立入り及び退出の管理																		
2.2.1.1(1)(a)	基本	部局技術責任者は、安全区域に不審者を立ち入らせない措置を講ずること。	部局技術責任者				○											
2.2.1.1(1)(b)	基本	部局技術責任者は、要保護情報を取り扱う情報システムについては、安全区域を物理的に隔離し、立入り及び退出を管理するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域へ立ち入る者が立入りを許可された者であるかの確認を行うための措置を講ずること。	部局技術責任者				○											
2.2.1.1(1)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域から退出する者が立入りを許可された者であるかの確認を行うための措置を講ずること。	部局技術責任者				○											
2.2.1.1(1)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、立入りを許可された者が、立入りを許可されていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。	部局技術責任者				○											
2.2.1.1(1)(f)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域へ継続的に立ち入る者を許可する手続を整備すること。また、その者の氏名、所属、立入許可日、立入期間及び許可事由を含む事項を記載するための文書を整備すること。	部局技術責任者				○											
2.2.1.1(1)(g)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域へ立入りを許可された者に変更がある場合には、当該変更の内容を前事項の文書へ反映させること。また、当該変更の記録を保存すること。	部局技術責任者				○											
2.2.1.1(1)(h)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域へのすべての者の立入り及び当該区域からの退出を記録し及び監視するための措置を講ずること。	部局技術責任者				○											
(2) 訪問者及び受渡業者の管理																		
2.2.1.1(2)(a)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属を確認するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(2)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的、訪問相手の氏名及び所属、訪問日並びに立入り及び退出の時刻を記録するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(2)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域への訪問者がある場合には、訪問相手の事務従事者が訪問者の安全区域への立入りについて審査するための手続を整備すること。	部局技術責任者				○											
2.2.1.1(2)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、訪問者の立ち入る区域を制限するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(2)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域内において訪問相手の事務従事者が訪問者に付き添うための措置を講ずること。	部局技術責任者				○											
2.2.1.1(2)(f)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、訪問者と継続的に立入りを許可された者とを外見上判断できる措置を講ずること。	部局技術責任者				○											
2.2.1.1(2)(g)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。	部局技術責任者				○											
2.2.1.1(2)(g)(ア)		安全区域外で受渡しを行うこと。																

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.2.1.1(2)(g)(イ)		業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、記録媒体に触れることができない場所に限定し、事務従事者が立ち会うこと。																
(3) 電子計算機及び通信回線装置のセキュリティ確保																		
2.2.1.1(3)(a)	基本	部局技術責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している電子計算機の盗難及び当該場所からの不正な持出しを防止するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(3)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要保護情報を取り扱う情報システムについては、電子計算機及び通信回線装置を他の情報システムから物理的に隔離し、安全区域を共用しないこと。	部局技術責任者				○											
2.2.1.1(3)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している通信回線装置の盗難及び当該場所からの不正な持出しを防止するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(3)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、事務従事者が離席時に電子計算機及び通信回線装置を不正操作から保護するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(3)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要機密情報を取り扱う情報システムについては、電子計算機及び通信回線装置の表示用デバイスを盗み見から保護するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(3)(f)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要保護情報を取り扱う情報システムについては、情報システムで利用する電源ケーブル及び通信ケーブルを含む配線を、損傷及び盗聴を含む脅威から保護するための措置を講ずること。	部局技術責任者				○											
2.2.1.1(3)(g)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要機密情報を取り扱う情報システムについては、電磁波による情報漏えい対策の措置を講ずること。	部局技術責任者				○											
(4) 安全区域内のセキュリティ管理																		
2.2.1.1(4)(a)	基本	事務従事者は、安全区域内において、身分証明書を他の職員から常時視認することが可能な状態にすること。	事務従事者							○								
2.2.1.1(4)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、事務従事者は、部局技術責任者の許可を得た上で、要保護情報を取り扱う情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しを行うこと。	事務従事者							○								
2.2.1.1(4)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要保護情報を取り扱う情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しに係る記録を取得すること。	部局技術責任者				○											
2.2.1.1(4)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要機密情報を取り扱う情報システムについては、情報システムに関連しない電子計算機、通信回線装置、電磁的記録媒体及び記録装置(音声、映像及び画像を記録するものを含む。)の安全区域への持込みについて制限すること。	部局技術責任者				○											
2.2.1.1(4)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、安全区域内での作業を監視するための措置を講ずること。	部局技術責任者				○											
(5) 災害及び障害への対策																		
2.2.1.1(5)(a)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、自然災害及び人為的災害から電子計算機及び通信回線装置を保護するための物理的な対策を講ずること。	部局技術責任者				○											
2.2.1.1(5)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、安全区域内において災害又は障害が発生している場合には、作業する者の安全性を確保した上で必要な場合に電子計算機及び通信回線装置の電源を遮断できる措置を講ずること。	部局技術責任者				○											
2.2.2 電子計算機																		
2.2.2.1 電子計算機共通対策																		
(1) 電子計算機の設置時																		
2.2.2.1(1)(a)	基本	部局技術責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を将来の見通しを含め検討し、確保すること。	部局技術責任者				○											
2.2.2.1(1)(b)	基本	部局技術責任者は、要保護情報を取り扱う情報システムについては、電子計算機を安全区域に設置すること。ただし、モバイルPCについて部局総括責任者の承認を得た場合は、この限りでない。	部局技術責任者				○											
2.2.2.1(1)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機を冗長構成にすること。	部局技術責任者				○											
(2) 電子計算機の運用時																		
2.2.2.1(2)(a)	基本	事務従事者は、大学事務の遂行以外の目的で電子計算機を利用しないこと。	事務従事者							○								
2.2.2.1(2)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、所管する範囲の電子計算機で利用されているすべてのソフトウェアの状態を定期的に調査し、不適切な状態にある電子計算機を検出した場合には、当該不適切な状態の改善を図ること。	部局技術責任者				○											
(3) 電子計算機の運用終了時																		
2.2.2.1(3)(a)	基本	部局技術責任者は、電子計算機の運用を終了する場合に、電子計算機の電磁的記録媒体のすべての情報を抹消すること。	部局技術責任者				○											
2.2.2.2 端末																		
(1) 端末の設置時																		

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.2.2.2(1)(a)	基本	部局技術責任者は、端末で利用可能なソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙し、又は両者を併用することができる。	部局技術責任者				○											
2.2.2.2(1)(b)	基本	部局技術責任者は、要保護情報を取り扱うモバイルPCについては、学外で使われる際にも、学内で利用される端末と同等の保護手段が有効に機能するように構成すること。	部局技術責任者				○											
2.2.2.2(1)(c)	基本	事務従事者は、モバイルPCを利用する必要がある場合には、部局技術責任者の承認を得ること。	事務従事者							○								
2.2.2.2(1)(d)	基本	部局技術責任者は、要機密情報を取り扱うモバイルPCについては、電磁的記録媒体に保存される情報の暗号化を行う機能を設けること。	部局技術責任者				○											
2.2.2.2(1)(e)	基本	部局技術責任者は、要保護情報を取り扱うモバイルPCについては、盗難を防止するための措置を定めること。	部局技術責任者				○											
2.2.2.2(1)(f)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、事務従事者が情報を保存できない端末を用いて情報システムを構築すること。	部局技術責任者				○											
(2) 端末の運用時																		
2.2.2.2(2)(a)	基本	事務従事者は、端末で利用可能と定められたソフトウェアを除いて、ソフトウェアを利用しないこと。	事務従事者							○								
2.2.2.2(2)(b)	基本	事務従事者は、要保護情報を取り扱うモバイルPCを利用する場合には、盗難防止措置を行うこと。	事務従事者							○								
2.2.2.2(2)(c)	基本	事務従事者は、要機密情報を取り扱うモバイルPCについては、モバイルPCを学外に持ち出す場合に、当該モバイルPCで利用する電磁的記録媒体に保存されている要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。	事務従事者							○								
2.2.2.2(2)(d)	基本	事務従事者は、部局技術責任者が接続許可を与えた通信回線以外に端末を接続しないこと。	事務従事者							○								
2.2.2.2(2)(e)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術担当者は、情報システムにおいて基準となる時刻に、端末の時刻を同期すること。	部局技術担当者					○										
2.2.2.3 サーバ装置																		
(1) サーバ装置の設置時																		
2.2.2.3(1)(a)	基本	部局技術責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報を暗号化するための機能を設けること。	部局技術責任者				○											
2.2.2.3(1)(b)	基本	部局技術責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。	部局技術責任者				○											
2.2.2.3(1)(c)	基本	部局技術責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動すること。	部局技術責任者				○											
2.2.2.3(1)(d)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、利用が定められたソフトウェアに該当しないソフトウェアをサーバ装置から削除すること。	部局技術責任者				○											
2.2.2.3(1)(e)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術担当者は、要安定情報を取り扱うサーバ装置の内、サービス提供に必要なサーバ装置については、負荷を複数のサーバ装置に分散又はサーバ装置を冗長構成とすること。	部局技術担当者					○										
(2) サーバ装置の運用時																		
2.2.2.3(2)(a)	基本	部局技術責任者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対処すること。	部局技術責任者				○											
2.2.2.3(2)(b)	基本	部局技術担当者は、要安定情報を取り扱うサーバ装置については、サーバ装置の運用状態を復元するために必要な措置を講ずること。	部局技術担当者					○										
2.2.2.3(2)(c)	基本	部局技術担当者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。	部局技術担当者					○										
2.2.2.3(2)(d)	基本	部局技術担当者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。	部局技術担当者					○										
2.2.2.3(2)(e)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術担当者は、サーバ装置のセキュリティ状態を監視し、不正行為及び不正利用を含む事象の発生を検知すること。	部局技術担当者					○										
2.2.2.3(2)(f)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術担当者は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視し、当該サーバ装置に関する障害等の発生を検知すること。	部局技術担当者					○										
2.2.3 アプリケーションソフトウェア																		
2.2.3.1 電子メール																		
(1) 電子メールの導入時																		
2.2.3.1(1)(a)	基本	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。	部局技術責任者				○											
2.2.3.1(1)(b)	基本	部局技術責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に事務従事者の主体認証を行う機能を備えること。	部局技術責任者				○											
(2) 電子メールの運用時																		
2.2.3.1(2)(a)	基本	事務従事者は、業務遂行に係る情報を含む電子メールを送受信する場合には、本学が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。ただし、本学支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。	事務従事者							○								
2.2.3.1(2)(b)	基本	事務従事者は、受信した電子メールにより、スクリプトが電子計算機で実行されないように電子メールの内容を表示させること。	事務従事者							○								
2.2.3.2 ウェブ																		
(1) ウェブの導入時																		

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.2.3.2(1)(a)	基本	部局技術責任者は、ウェブサーバを用いて提供するサービスが利用者からの文字列等の入力を受ける場合には、特殊文字の無害化を実施すること。	部局技術責任者				○											
2.2.3.2(1)(b)	基本	部局技術責任者は、ウェブサーバからウェブクライアントに攻撃の糸口になり得る情報を送信しないように情報システムを構築すること。	部局技術責任者				○											
2.2.3.2(1)(c)	基本	部局技術責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバを用いて提供するサービスにおいて、通信の盗聴から保護すべき情報を特定し、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化する機能を設けること。	部局技術責任者				○											
2.2.3.2(1)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要機密情報を取り扱う情報システムについては、ウェブサーバに保存する情報を特定し、当該サーバに要機密情報が含まれないことを確認すること。	部局技術責任者				○											
2.2.3.2(1)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、ウェブサーバの正当性を保証するために電子証明書を利用すること。	部局技術責任者				○											
(2) ウェブの運用時																		
2.2.3.2(2)(a)	基本	事務従事者は、情報セキュリティの確保がなされるよう適切にウェブクライアントのセキュリティ設定をすること。	事務従事者							○								
2.2.3.2(2)(b)	基本	事務従事者は、ウェブクライアントが動作する電子計算機にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。	事務従事者							○								
2.2.3.2(2)(c)	基本	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。	事務従事者							○								
2.2.3.2(2)(c)(ア)		送信内容が暗号化されること。																
2.2.3.2(2)(c)(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。																
2.2.3.2(2)(d)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、事務従事者が閲覧することが可能な学外のホームページを制限し、定期的にその見直しを行うこと。	部局技術責任者				○											
2.2.3.3 ドメインネームシステム（DNS）																		
(1) DNSの導入時																		
2.2.3.3(1)(a)	基本	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。	部局技術責任者				○											
2.2.3.3(1)(b)	基本	部局技術責任者は、DNSのコンテンツサーバにおいて管理するドメインに関する情報を運用管理するための手続を定めること。	部局技術責任者				○											
2.2.3.3(1)(c)	基本	部局技術責任者は、DNSのキャッシュサーバにおいて、学外からの名前解決の要求には応じず、府省庁内からの名前解決の要求のみに回答を行うための措置を講ずること。	部局技術責任者				○											
2.2.3.3(1)(d)	基本	部局技術責任者は、DNSのコンテンツサーバにおいて、学内のみで使用する名前の解決を提供する場合、当該情報が外部に漏えいしないための措置を講ずること。	部局技術責任者				○											
2.2.3.3(1)(e)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、重要な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、管理するドメインに関する情報に電子署名を付与すること。	部局技術責任者				○											
(2) DNSの運用時																		
2.2.3.3(2)(a)	基本	部局技術担当者は、DNSのコンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。	部局技術担当者					○										
2.2.3.3(2)(b)	基本	部局技術担当者は、DNSのコンテンツサーバにおいて管理するドメインに関する情報を運用管理するための手続に基づいて、当該情報が正確であることを適宜確認すること。	部局技術担当者					○										
2.2.4 通信回線																		
2.2.4.1 通信回線共通対策																		
(1) 通信回線の構築時																		
2.2.4.1(1)(a)	基本	部局技術責任者は、通信回線構築によるリスクを検討し、通信回線を構築すること。	部局技術責任者				○											
2.2.4.1(1)(b)	基本	部局技術責任者は、要安定情報を取り扱う情報システムについては、通信回線及び通信回線装置に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。	部局技術責任者				○											
2.2.4.1(1)(c)	基本	部局技術責任者は、通信回線装置が動作するために必要なソフトウェアを定めること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。	部局技術責任者				○											
2.2.4.1(1)(d)	基本	部局技術責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。	部局技術責任者				○											
2.2.4.1(1)(e)	基本	部局技術責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って通信回線装置を利用しアクセス制御及び経路制御を行うこと。	部局技術責任者				○											
2.2.4.1(1)(f)	基本	部局技術責任者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化するための機能を設けること。	部局技術責任者				○											
2.2.4.1(1)(g)	基本	部局技術責任者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、適切な回線を選択すること。	部局技術責任者				○											
2.2.4.1(1)(h)	基本	部局技術責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。	部局技術責任者				○											
2.2.4.1(1)(i)	基本	部局技術責任者は、通信回線装置を安全区域に設置すること。	部局技術責任者				○											
2.2.4.1(1)(j)	基本	部局技術責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。	部局技術責任者				○											

A3502 責任者等の役割から見た遵守事項

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.2.4.1(1)(k)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、通信を行う電子計算機の主体認証を行うこと。	部局技術責任者				○											
2.2.4.1(1)(l)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要な通信回線又は通信回線装置を冗長構成にすること。	部局技術責任者				○											
(2) 通信回線の運用時																		
2.2.4.1(2)(a)	基本	部局技術担当者は、通信回線装置のソフトウェアを変更する場合には、部局技術責任者の許可を得ること。	部局技術担当者					○										
2.2.4.1(2)(b)	基本	部局技術担当者は、通信回線及び通信回線装置の運用管理について、作業日、作業を行った通信回線及び通信回線装置並びに作業内容及び作業者を含む事項を記録すること。	部局技術担当者					○										
2.2.4.1(2)(c)	基本	部局技術責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更すること。	部局技術責任者				○											
2.2.4.1(2)(d)	基本	事務従事者は、部局技術責任者の許可を受けていない電子計算機及び通信回線装置を通信回線に接続しないこと。	事務従事者							○								
2.2.4.1(2)(e)	基本	部局技術担当者は、情報システムにおいて基準となる時刻に、通信回線装置の時刻を同期すること。	部局技術担当者					○										
2.2.4.1(2)(f)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、所管する範囲の通信回線装置が動作するために必要なすべてのソフトウェアの状態を定期的に調査し、不適切な状態にある通信回線装置を検出した場合には、当該不適切な状態の改善を図ること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。	部局技術責任者				○											
(3) 通信回線の運用終了時																		
2.2.4.1(3)(a)	基本	部局技術責任者は、通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体のすべての情報を抹消すること。	部局技術責任者				○											
2.2.4.2 学内通信回線の管理																		
(1)学内通信回線の構築時																		
2.2.4.2(1)(a)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、通信回線装置に物理的に接続した電子計算機を、通信回線に論理的に接続する前に、当該電子計算機が通信回線に接続することを許可されたものであることを確認するための措置を講ずること。	部局技術責任者				○											
(2) 学内通信回線の運用時																		
2.2.4.2(2)(a)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、通信要件の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。	部局技術責任者				○											
2.2.4.2(2)(b)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術担当者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。	部局技術担当者					○										
2.2.4.2(2)(c)	強化	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術担当者は、学内通信回線上を送受信される通信内容を監視すること。	部局技術担当者					○										
(3) 回線の対策																		
2.2.4.2(3)(a)	基本	部局技術責任者は、VPN環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。	部局技術責任者				○											
2.2.4.2(3)(a)(ア)		利用開始及び利用停止時の申請手続の整備																
2.2.4.2(3)(a)(イ)		通信内容の暗号化																
2.2.4.2(3)(a)(ウ)		通信を行う電子計算機の識別又は利用者の主体認証																
2.2.4.2(3)(a)(エ)		主体認証記録の取得及び管理																
2.2.4.2(3)(a)(オ)		VPN経由でアクセスすることが可能な通信回線の範囲の制限																
2.2.4.2(3)(a)(カ)		VPN接続方法の機密性の確保																
2.2.4.2(3)(a)(キ)		VPNを利用する電子計算機の管理																
2.2.4.2(3)(b)	基本	部局技術責任者は、無線LAN環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。この場合、要機密情報を取り扱う無線LAN環境については、通信内容の暗号化を行う必要性があると判断すること。	部局技術責任者				○											
2.2.4.2(3)(b)(ア)		利用開始及び利用停止時の申請手続の整備																
2.2.4.2(3)(b)(イ)		通信内容の暗号化																
2.2.4.2(3)(b)(ウ)		通信を行う電子計算機の識別又は利用者の主体認証																
2.2.4.2(3)(b)(エ)		主体認証記録の取得及び管理																
2.2.4.2(3)(b)(オ)		無線LAN経由でアクセスすることが可能な通信回線の範囲の制限																
2.2.4.2(3)(b)(カ)		無線LANに接続中に他の通信回線との接続の禁止																
2.2.4.2(3)(b)(キ)		無線LAN接続方法の機密性の確保																
2.2.4.2(3)(b)(ク)		無線LANに接続する電子計算機の管理																
2.2.4.2(3)(c)	基本	部局技術責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。	部局技術責任者				○											
2.2.4.2(3)(c)(ア)		利用開始及び利用停止時の申請手続の整備																
2.2.4.2(3)(c)(イ)		通信を行う者又は発信者番号による識別及び主体認証																
2.2.4.2(3)(c)(ウ)		主体認証記録の取得及び管理																
2.2.4.2(3)(c)(エ)		リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限																
2.2.4.2(3)(c)(オ)		リモートアクセス中に他の通信回線との接続の禁止																
2.2.4.2(3)(c)(カ)		リモートアクセス方法の機密性の確保																
2.2.4.2(3)(c)(キ)		リモートアクセスする電子計算機の管理																
2.2.4.3 学外通信回線との接続																		
(1) 学内通信回線と学外通信回線との接続時																		
2.2.4.3(1)(a)	基本	部局技術責任者は、部局総括責任者の承認を得た上で、学内通信回線を学外通信回線と接続すること。	部局技術責任者				○											

管理番号	基本または強化	遵守事項	実施者	全学総括責任者	全学実施責任者	部局総括責任者	部局技術責任者	部局技術担当者	職場情報セキュリティ責任者	事務従事者	全学情報システム運用委員会	情報セキュリティ監査責任者	情報セキュリティ監査を実施する者	権限管理を行う者	許可権限者	管理者権限を持つ識別コードを付与された者	情報セキュリティ関係規程を整備した者	監視要員等
2.2.4.3(1)(b)	基本	部局技術責任者は、学内通信回線を学外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している学内通信回線又は学外通信回線から独立した通信回線として学内通信回線を構築すること。	部局技術責任者				○											
(2) 学外通信回線と接続している学内通信回線の運用時																		
2.2.4.3(2)(a)	基本	部局技術責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している学内通信回線又は学外通信回線から独立した通信回線に構成を変更すること。	部局技術責任者				○											
2.2.4.3(2)(b)	基本	部局技術責任者は、通信回線の変更の際及び定期的に、アクセス制御の設定の見直しを行うこと。	部局技術責任者				○											
2.2.4.3(2)(c)	基本	部局技術担当者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測し、又は検知すること。	部局技術担当者					○										
2.2.4.3(2)(d)	基本	部局技術担当者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視すること。	部局技術担当者					○										
第2.3部 個別事項についての対策																		
2.3.1 その他																		
2.3.1.1 情報システムへのIPv6技術の導入における対策																		
(1) IPv6移行機構がもたらす脆弱性対策																		
2.3.1.1(1)(a)	基本	部局技術責任者は、情報システムにIPv6技術を利用する通信（以下「IPv6通信」という。）の機能を導入する場合には、IPv6移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。	部局技術責任者				○											
(2) 意図しないIPv6通信の抑止と監視																		
2.3.1.1(2)(a)	基本	部局技術責任者は、IPv6通信を想定していない通信回線に接続されるすべての電子計算機及び通信回線装置に対して、IPv6通信を抑止するための措置を講ずること。	部局技術責任者				○											
2.3.1.1(2)(b)	**強化**	特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部局技術責任者は、IPv6通信を想定していない通信回線を監視し、IPv6通信が検知された場合には通信している装置を特定し、IPv6通信を遮断するための措置を講ずること。	部局技術責任者				○											

A3600 認証手順の策定に関する解説書

この文書は、「A2201 情報システム利用規程」A2201-05（全学アカウントの申請）に定める全学アカウントの申請と交付の手順の雛形として使われることを想定している。A大学では、IDとパスワードによる全学統一認証方式を採用し、ネットワークを含めて、全学統一認証に対応した情報システムの利用にあたって全学アカウントを用いている。これに基づき以下の４文書を雛形として示す。

(1) A 大学情報システムアカウント取得手順（「A3601 情報システムアカウント取得手順」に相当）
アカウントの申請・交付の手順として、学生、教職員それぞれに対して公開する文書。

(2) A 大学情報メディアセンターにおける全学アカウントに係る個人情報の保護
（「A3601 情報システムアカウント取得手順」別紙１に相当）
利用者からの全学アカウントの交付申請・登録などに際して収集した個人情報の取扱について、利用者に対して示す文書。

(3) A 大学情報システム利用申請書（「A3601 情報システムアカウント取得手順」別紙２に相当）
全学アカウントの申請書様式（複写式）。「A 大学情報システム利用心得」を示し、それを遵守することについての誓約書に署名させるようになっている。

(4) A 大学情報システム全学アカウント交付申請区分（「A3601 情報システムアカウント取得手順」別紙３に相当）
申請者の身分ごとに本人確認手順、更新手続きなどの認証手続きを定めた内部文書。原則非公開。年度ごとの手順の見直しが必要。

全学アカウントは、全学実施責任者（管理運営部局である情報メディアセンター長）から交付を受けなければならない。A大学では、利用の申請と承認は全学情報システム運用委員会が処理をするが、利用承認とアカウント指定を行うのは全学実施責任者なので、申請宛先も全学実施責任者としている。アカウントの発行に際しては原則として写真付身分証による対面での本人確認を義務付けている。また学生については全学アカウントの発行に際して講習会の受講を義務付けている。学生・教職員以外の者の申請に当たっては、関係部局長（来学中に利用する訪問者などの臨時利用者を受け入れた部局の長など）名での受入証明書の提出を要件とする。

なお、A 大学では身分証は IC カード化されていないが、身分証が IC カード化され PKI による利用者認証が可能になっている場合には、アカウントは電子申請によりオンラインで発行を受けることが可能である。ただしその場合には身分証の交付手順が CP（証明書ポリシー）／CPS（認証局実施規程）に基づくものでなければならない。

実際の運用にあたっては以下のような点についても検討が必要である。

- 医学部、歯学部、獣医学部、薬学部のような 6 年制の学部の学生に対して、卒業まで 6 年間有効のアカウントを発行してよいか、他の学部と合わせて 4 年＋2 年の更新とするか。博士課程 5 年一貫教育の場合も同様。
- 名誉教授に対するアカウントを発行するか、年度ごとの更新処理は必要か。

- 卒業生に対するアカウントを発行するか、有効期限の設定、利用者との契約をどうするか
- 産学連携施設など大学内に制度的に整備された施設で研究を行う、大学外の身分の研究者等にアカウントを発行するか。その場合の契約をどうするか。
- 本人死亡に伴うアカウント失効処理手順をどうするか。知財の継承のほか労災の認定などにおいてもデータの保全が求められることがある。

A3601 情報システムアカウント取得手順

【全学アカウントの取得手順（学生等用)】

全学アカウント交付のための利用者講習会（情報セキュリティ基礎講習を含む）を受講してください。その際、学生証と筆記用具を持参してください。全学アカウント交付のための利用者講習会は、年度初めを中心に開催しています。都合の良い機会に、早めに受講してください。

講習会の実施日については、 情報メディアセンターのトップページにある 「イベント等のお知らせ」あるいは情報メディアセンター事務室前の掲示等を参照してください。

既に全学アカウントを取得している方で、転学部、進学等に伴い身分変更が生じた際には、手続きが必要となる場合があります。手続きが必要となる方には、例年メールでお知らせしています。詳しくは、情報メディアセンター事務室までお問い合わせください。

【全学アカウントの取得手順（教職員等用)】

1. **手続き**

登録に必要な仮パスワードを発行しますので、職員証または大学が発行する身分証を持って、申請受付場所までお越しください。

- **情報メディアセンター事務室**
- **図書館事務室**

新規利用登録以外の申請は、情報メディアセンター以外では受付していない場合があります。

2. **申請用紙**

所定の利用登録申請書（新規登録用）をご利用ください。

なお､情報メディアセンター､図書館については窓口に複写式の申請用紙を用意してあります。

3. **注意**

情報メディアセンター窓口以外での申請分については、当日中の仮パスワード発行ができませんので、当日中の発行をご希望の方はセンター事務室での申請をお願い致します。

また、常勤教職員以外の方は、年度が変わった時点で利用延長の手続きが必要です。新年度になりましたら情報メディアセンター電子メールシステムのメールアドレス宛に、利用延長の手続きの案内を送ります。手続きの案内を受け取った後、継続して利用を希望される場合には、新年度継続して勤務していることを証明する書類を持って、手続きにお越しください。

4. **その他**

全学アカウント取得後速やかに、年度講習計画に定める情報セキュリティ基礎講習を受講してください｡また毎年度１回は年度講習計画に従い情報セキュリティ定期講習を受講してください。

別紙１　情報メディアセンターにおける全学アカウントに係る個人情報の保護

1. 個人情報について

利用者からの本学情報システムの全学アカウントの交付申請・登録などに際して収集した特定の個人を識別しうる情報を対象とします。情報メディアセンターは個人情報の保護に関して「独立行政法人等の保有する個人情報の保護に関する法律」及び関係法令ならびに「A 大学個人情報保護規程」等の A 大学の定める個人情報保護の方針に則って業務を行います。

2. 全学アカウントの交付等申請時に取得する個人情報の利用目的

本学情報システムの全学アカウントの交付、継続、停止、再開などの申請時に取得する個人情報の利用目的は以下のとおりです。

- A 大学ネットワークや情報処理演習システムなど情報メディアセンターで提供しているサービスのご利用に関しての利用者ご本人への連絡（学部、研究科等 A 大学各部局の保有する個人情報と結合することにより連絡先を得て利用することがあります。）
- 全学アカウントなどのご本人自身による照会に際してのご本人の確認
- 統計データの作成

3. 全学アカウントとパスワードの利用目的

本学情報システムの全学アカウントとパスワードは、本学が提供する教育研究その他業務のためのサービスにおいて、これらの組み合わせにより利用者個人を認証するために利用します。利用者個人の認証に際しては、サービスの必要に応じ氏名など利用者個人を特定する情報と結合することがあります。

4. 利用記録の取得とその利用目的

利用者による全学アカウントを用いた本学情報システムの利用に関して以下の事項について利用コードおよび時刻情報を含めて利用記録を取得します。

- A 大学ネットワークならびに全学統一認証方式を用いる A 大学内のすべての情報システムにおける、全学アカウントとパスワードを用いて行われる利用者の認証記録
- 情報メディアセンターの電子メールシステムにおける電子メールの送信と受信
- 情報メディアセンターの情報処理演習システムの端末からの Web サイトのアクセス

これらの利用記録は以下の目的のために利用します。

(1)利用者自身のご利用上の問題解決の支援
(2)情報メディアセンターの情報システムの運用の改善
(3)関係法令、本学関係規程ならびに情報システム利用心得遵守の確認のため
(4)統計データ

5. 個人情報の安全確保、利用、提供、開示、訂正並びに利用停止

収集した個人情報の安全確保、利用、提供、開示、訂正並びに利用停止については「A 大学個人情報保護規程」に則して取り扱います。

別紙２　A 大学情報システム利用申請書

情報メディアセンター提出用

A 大学情報システム利用申請書

A 大学情報システム利用規程第四条に基づき、全学アカウントの交付を申請します。

申請日 application date					年 Year			月 Month			日 Day

氏名/Name(Last,First)	フリガナ/Name in Kana	利用申請者の区分/ Current Status
		1．学部学生/undergraduate 2．大学院生/graduate 3．常勤教職員/permanent staff 4．非常勤教職員/part time staff 5．名誉教授/emeritus 6．研究生/research student 7．その他/other （　　） ・該当する番号に○印 ・その他の方は括弧内に区分を記入
所属部局・学科等/Faculty・Department	学生証、職員証、身分証の番号（左詰）/ ID Number(left-align)	
連絡先電話番号/Telephone Number	誕生日/Date of Birth	
	月 Month / 日 Day	

A 大学情報システム利用心得

1．A 大学情報システムの全学アカウントの交付を受けた者（以下、利用者という）は利用に際して、関連法令を遵守しなければならない。利用者は、本学情報システム運用基本方針、本学情報システム運用基本規程、本学情報システム利用規程（以下、利用規程という）および本学個人情報保護規程を遵守しなければならない。
2．利用者は、利用規程第五条に定めるアカウントの管理に関する規定を遵守しなければならない。
利用者は利用に際して、当該システムを管理する部局の担当職員および当該部局がコンピュータシステムの管理を委託した者の指示に従わなければならない。
3．利用者は、毎年度1回は、本学が定める年度講習計画に従って、本学情報システムの利用に関する教育を受講しなければならない。利用者は、本学が定める自己点検基準に基づいて自己点検を実施しなければならない。
4．利用者は利用に際して、利用規程第十条に定める禁止事項に該当する行為を行ってはならない。
利用者は利用に際して、利用規程第十二条に定める PC 取扱ガイドライン、利用規程第十三条に定める電子メール利用ガイドライン、利用規程第十四条に定めるウェブブラウザ利用ガイドラインおよびウェブ公開ガイドライン、利用規程第十五条に定めるモバイル PC の利用手順を遵守しなければならない。
利用者は利用に際して、他人のプライバシーおよび人格を尊重しなければならない。
利用者は利用に際して、他人の著作権およびその他の知的財産権を尊重しなければならない。
利用者は利用に際して、A 大学の定めるセクシャルハラスメント等に関する方針を遵守しなければならない。
利用者は利用に際して、A 大学の定める大学における言論に関する方針を遵守しなければならない。
5．利用者は利用に際して、本学情報システムを構成する計算機のハードウェア、ソフトウェアおよび装置を毀損、破壊または改変してはならない。
利用者は利用に際して、利用規程第十七条に定める安全管理に関する義務を負う。
6．本学情報システムの利用にあたり故意または過失により本学情報システムを構成する計算機組織に損害を生じさせた利用者は、それによって生じた損害を賠償する責任を負う。本学情報システムによるサービス提供を妨害した利用者は、それによって生じた損害を賠償する責任を負う。

誓　約　書

A 大学情報メディアセンター長　殿

A 大学情報システム利用規程及び情報システム利用心得を遵守して、本学情報システムを利用することに同意します。これらに違反した場合、センター長が、私のアカウントを取り消すこと、あるいは私のアカウントの利用を一時停止すること、又は私のアカウントの権限により作成された本学情報システム上の電子情報ファイルの一部ないし全部を放棄させることに異議はありません。

（　　）年/Year　（　　）月/Month　（　　）日/Day

自署/Signature（　　）

申請者控（利用期間中は確実に保管のこと）

A 大学情報システム利用申請書(控)

A 大学情報システム利用規程第四条に基づき、全学アカウントの交付を申請します。

申請日 application date	年 Year	月 Month	日 Day

氏名/Name(Last,First)	フリガナ/Name in Kana	利用申請者の区分/ Current Status
		1．学部学生/undergraduate 2．大学院生/graduate 3．常勤教職員/permanent staff 4．非常勤教職員/part time staff 5．名誉教授/emeritus 6．研究生/research student 7．その他/other （　　） ・該当する番号に○印 ・その他の方は括弧内に区分を記入
所属部局・学科等/Faculty・Department	学生証、職員証、身分証の番号（左詰）/ ID Number(left-align)	
連絡先電話番号/Telephone Number	誕生日/Date of Birth	
	月 Month / 日 Day	

この用紙にはパスワードは書き込まないでください。
Don't write your password on this sheet!

全学アカウント/User ID	メールアドレス/e-mail address
	＿＿＿＿＿＿＿＿＿＿＿＿ @ mail.example.ac.jp

A 大学情報システム利用心得

1．A 大学情報システムの全学アカウントの交付を受けた者（以下、利用者という）は利用に際して、関連法令を遵守しなければならない。利用者は、本学情報システム運用基本方針、本学情報システム運用基本規程、本学情報システム利用規程（以下、利用規程という）および本学個人情報保護規程を遵守しなければならない。
2．利用者は、利用規程第五条に定めるアカウントの管理に関する規定を遵守しなければならない。
利用者は利用に際して、当該システムを管理する部局の担当職員および当該部局がコンピュータシステムの管理を委託した者の指示に従わなければならない。
3．利用者は、毎年度1回は、本学が定める年度講習計画に従って、本学情報システムの利用に関する教育を受講しなければならない。利用者は、本学が定める自己点検基準に基づいて自己点検を実施しなければならない。
4．利用者は利用に際して、利用規程第十条に定める禁止事項に該当する行為を行ってはならない。
利用者は利用に際して、利用規程第十二条に定める PC 取扱ガイドライン、利用規程第十三条に定める電子メール利用ガイドライン、利用規程第十四条に定めるウェブブラウザ利用ガイドラインおよびウェブ公開ガイドライン、利用規程第十五条に定めるモバイル PC の利用手順を遵守しなければならない。
利用者は利用に際して、他人のプライバシーおよび人格を尊重しなければならない。
利用者は利用に際して、他人の著作権およびその他の知的財産権を尊重しなければならない。
利用者は利用に際して、A 大学の定めるセクシャルハラスメント等に関する方針を遵守しなければならない。
利用者は利用に際して、A 大学の定める大学における言論に関する方針を遵守しなければならない。
5．利用者は利用に際して、本学情報システムを構成する計算機のハードウェア、ソフトウェアおよび装置を毀損、破壊または改変してはならない。
利用者は利用に際して、利用規程第十七条に定める安全管理に関する義務を負う。
6．本学情報システムの利用にあたり故意または過失により本学情報システムを構成する計算機組織に損害を生じさせた利用者は、それによって生じた損害を賠償する責任を負う。本学情報システムによるサービス提供を妨害した利用者は、それによって生じた損害を賠償する責任を負う。

誓　約　書

A 大学情報メディアセンター長　殿

A 大学情報システム利用規程及び情報システム利用心得を遵守して、本学情報システムを利用することに同意します。これらに違反した場合、センター長が、私のアカウントを取り消すこと、あるいは私のアカウントの利用を一時停止すること、又は私のアカウントの権限により作成された本学情報システム上の電子情報ファイルの一部ないし全部を放棄させることに異議はありません。

（　　）年/Year　（　　）月/Month　（　　）日/Day

自署/Signature（　　）

別紙３　ID 交付申請区分

<table>
<tr><th></th><th colspan="3">身　　分</th><th>講習会受講</th><th>更新手続き</th><th>備　　考</th></tr>
<tr><td rowspan="3">一 学生等</td><td>学部学生
大学院学生</td><td>学生証
(学生部発行･顔写真あり)</td><td rowspan="5">「学生証」「職員証」等の大学発行の身分証を提示、顔写真付のものについては対面にて確認</td><td rowspan="2">必要</td><td>必要
(身分変更が生じた年度のみ)</td><td>10 月入学生については所定の年限の 9 月末で失効</td></tr>
<tr><td>研究生
研究員
研修員
研究者
他</td><td>学生証
(部局発行･顔写真なし)</td><td>必要
(毎年度)</td><td>アカウントの有効期限は身分証の有効期限と年度末の早い方まで</td></tr>
<tr><td rowspan="3">二 教職員等</td><td>常勤教職員
特定有期雇用教職員</td><td>職員証
(人事部発行･顔写真あり)</td><td rowspan="2"></td><td>着任早々で身分証を未取得の場合は「人事異動通知書」の提示。身分証番号を所属人事又は総務担当より入手。さらに以下のいずれかの方法で顔写真を確認する。1) 公的機関発行の顔写真付身分証の提示　2)1ヶ月以内に顔写真付職員証を持参して再確認</td></tr>
<tr><td>時間雇用職員
有期雇用職員
　事務補佐員
　技術補佐員
他</td><td rowspan="2">身分証 (職員証等)
(部局発行･顔写真なし)</td><td rowspan="2">必要
(毎年度)</td><td rowspan="2">着任早々で身分証を未取得の場合は「労働条件通知書」または「受入証明書」の提示。身分証番号を所属人事又は総務担当より入手。</td></tr>
<tr><td>外国人研究員
外国人教師
客員教員
招聘外国人学者
派遣職員
他</td></tr>
<tr><td>三 臨時利用者</td><td>訪問者
受託業務従事者
他</td><td>身分証
(受入証明書に記載の所属機関発行)</td><td>受入部局長名で受入証明書等の提出</td><td>必要
(学生のみ)</td><td>必要
(毎年度)</td><td>個別に情報メディアセンター全学アカウント担当へ問い合わせる。</td></tr>
</table>

参考資料等

1. 大学の情報セキュリティポリシーに関連するもの

(1) 高等教育機関のための情報セキュリティポリシー策定支援ポータル
http://www.uispp.jp/
本サンプル規程集の活用に関する各種情報の提供を行っているほか、情報セキュリティポリシーを公開している大学へのリンク等がある。

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

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

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

(5) UPKI イニシアティブ
https://upki-portal.nii.ac.jp/
本サンプル規程集における「A2601 証明書ポリシー（CP）」や「A2602 認証実施規程（CPS）」は本サイトで公開されている「キャンパス PKI CP/CPS ガイドライン」に相当する。

2. 情報セキュリティや著作権保護に関するもの

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

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

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

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

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

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

(7) 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）
http://www.jnsa.org/
企業向けの情報セキュリティポリシーのサンプル等を活動成果として公開。

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

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

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

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

用語索引

本索引は用語の定義もしくは解説を行っているページのみを対象としている。用語が出現しているページすべてを参照しているわけではないので留意されたい。また、特定の文書内に限定して用語を用いている例もあるので注意のこと。

（注）ページ番号の書式の意味は以下の通りである。

太字：用語を定義しているページ

斜字：事務情報システムのみが対象の規程等の内部で用語を定義・解説しているページ