国立大学法人長岡技術科学大学

情報セキュリティ管理運用の取扱い

令和５年４月

長岡技術科学大学　情報統合管理会議

目 次

■ 更新履歴

平成 30 年３月 30 日	制定
平成 31 年３月 31 日	機密区分に関する改正（平成 31 年４月１日施行）
令和３年３月３日	総合情報センターの設置に伴う改正（令和３年３月３日施行）
令和５年３月 23 日	取扱い全体に対する改正（令和５年４月１日施行）

第１章　総則

国立大学法人長岡技術科学大学（以下「本学」という。）は、本学の情報資産を利用する者及び管理・運用の業務に携わる者が国立大学法人長岡技術科学大学情報セキュリティ管理基本方針（以下「基本方針」という。）及び国立大学法人長岡技術科学大学情報セキュリティ管理基本規程（以下「基本規程」という。）に基づき実施すべき具体的な情報セキュリティ対策や実施手順を示すことを目的に、国立大学法人長岡技術科学大学情報セキュリティ管理運用の取扱い（本書、以下「運用の取扱い」という。）を定める。

本学は、下記規程群を国立大学法人長岡技術科学大学情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）と定める。

（１）基本方針
（２）基本規程
（３）運用の取扱い

第２章　適用対象

この運用の取扱いの適用対象者は、本学の情報資産を利用する者（以下「利用者」という。）及び管理・運用の業務に携わる者（以下「管理者」という。）とする。

対象とする情報は、本学基本方針第２条第２項に定めるものとする。

第３章　定義

この運用の取扱いにおける用語の定義は、本章の各条、基本方針第３条各号又は基本規程第２条各号又に定めるところによる。

３−１　主体認証　識別コードを提示した主体（情報システムの利用者等）が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。なお、主体認証情報とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報としてパスワード等がある。

３−２　識別コード　主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとしてユーザ ID があげられる。なお、識別とは、情報システムにアクセスする主体を当該情報システムにおいて特定することをいう。

３−３　モバイル端末　端末のうち、必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

第４章　法令等の遵守

本学の情報システムを利用した情報発信は、学内にとどまらず、社会へ広く伝達される可能性があることを自覚し、法令遵守等責任を持った行動がとられなければならない。

本学の情報システムの運用においては、第三者に対する誹謗中傷や名誉棄損、著作権

侵害等と判断された場合に基本方針第６条に基づき処罰することがある。

また、役職員等は自分自身のみならず、本学に勤務する教員、事務職員、技術職員（いずれも非常勤を含む。）その他本学の業務に従事し、組織責任者が認めた者、学生等の利用者に対して法令を遵守するよう指導しなければならない。

なお、主な関連法令については、付録２に例示する。

第５章　組織・体制

第１節　組織・体制

５－１　本学の情報セキュリティポリシー並びに対策推進計画の決定及び見直しは、基本方針及び基本規程に従い、最高情報セキュリティ責任者（Chief Information Security Officer 以下「CISO」という。）の下、国立大学法人長岡技術科学大学情報統合管理会議（以下「情報統合管理会議」という。）が執り行う。

５－２　本学の情報セキュリティ体制は、情報セキュリティ緊急時対応手順書に示す。

５－３　システム管理者及び利用者は、次に掲げる事項を行ってはならない。

（１）情報資産の目的外利用

（２）守秘義務に違反する情報の開示

（３）組織責任者の許可なく通信回線上を送受信される通信内容を監視し、又は通信回線装置及びサーバ装置の利用記録を採取する行為

（４）組織責任者の要請に基づかずにセキュリティ上の脆弱性を検知する行為

（５）法令又は学内規則に違反する情報の発信

（６）管理者権限を濫用する行為

（７）上記の行為を助長する行為

第２節　対策推進計画の策定

５－４　CISO は、情報統合管理会議における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定める。また、対策推進計画には、本学の業務、取扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含める。

（１）情報セキュリティに関する教育

（２）情報セキュリティ対策の自己点検

（３）情報セキュリティ監査

（４）情報システムに関する技術的な対策を推進するための取組

（５）前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

第６章　運用

第１節　情報セキュリティポリシー及び関係規程等の整備及び運用

６－１　CISO は、以下に示す情報セキュリティポリシー及び手順等を整備する。

（１）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

（２）情報セキュリティインシデント対応手順（緊急時対応手順）
（３）例外措置の適用手順（申請、審査及び承認手続）
（４）情報の取扱いに関する手順
（５）要管理対策区域の対策基準
（６）外部委託に係る規程（機器等の調達、機器等の納入時の確認・検査手続を含む）
（７）約款による外部サービスの利用に関する規程
（８）ソーシャルメディアサービスによる情報発信における情報セキュリティ対策に関する運用手順
（９）アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規程
(10) 要管理対策区域外で情報処理を行う際の安全管理措置に関する規程
(11) USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順
(12) 本学支給以外の端末による情報処理の実施手順
(13) 情報システムの管理規程の雛形
(14) 自己点検の実施手順
(15) 情報セキュリティ監査の実施手順

６－２　システム管理者及び利用者は、情報セキュリティポリシー及び手順等への重大な違反を知った場合は、組織責任者に報告する。

６－３　組織責任者は、情報セキュリティポリシー及び手順等への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、CISO に報告する。

６－４　組織責任者は、情報セキュリティポリシー及び手順等への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、速やかに調査を行い、事実を確認する。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取する。

６－５　組織責任者は、調査によって違反行為が判明したときには、次号に掲げる措置を講ずることができる。
（１）当該行為者に対する当該行為の中止命令
（２）当該行為に係る情報発信の遮断命令
（３）当該行為者のアカウント停止命令又は削除命令
（４）国立大学法人長岡技術科学大学職員の懲戒等に関する規程第５条及び国立大学法人長岡技術科学大学学生の懲戒に関する規程第２条に定める調査委員会への報告
（５）その他法令に基づく措置

６－６　組織責任者は、６－５項の措置を講じた場合には、CISO にその旨を報告する。

第２節　例外措置

6－7　CISO は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び審査手続を定める。

6－8　CISO は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求める。

6－9　CISO は、例外措置について以下を含む手順を定める。

（１）例外措置の許可権限者

（２）事前申請の原則その他の申請方法

（３）審査項目その他の審査方法

（ア）申請者の情報（氏名、所属、連絡先）

（イ）例外措置の適用を申請する情報セキュリティポリシー及び手順等の該当箇所
（規程名と条項等）

（ウ）例外措置の適用を申請する期間

（エ）例外措置の適用を申請する措置内容（講ずる代替手段等）

（オ）例外措置により生じる情報セキュリティ上の影響と対応方法

（カ）例外措置の適用を終了した旨の報告方法

（キ）例外措置の適用を申請する理由

6－10　許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、CISO へ定期的に報告する。

（１）審査した者の情報（氏名、役割名、所属、連絡先）

（２）申請内容

（ア）申請者の情報（氏名、所属、連絡先）

（イ）例外措置の適用を申請する情報セキュリティポリシー及び手順等の該当箇所
（規程名と条項等）

（ウ）例外措置の適用を申請する期間

（エ）例外措置の適用を申請する措置内容（講ずる代替手段等）

（オ）例外措置の適用を終了した旨の報告方法

（カ）例外措置の適用を申請する理由

（３）審査結果の内容

（ア）許可又は不許可の別

（イ）許可又は不許可の理由

（ウ）例外措置の適用を許可した情報セキュリティポリシー及び手順等の該当箇所
（規程名と条項等）

（エ）例外措置の適用を許可した期間

（オ）許可した措置内容（講ずるべき代替手段等）

（カ）例外措置を終了した旨の報告方法

6-11　システム管理者及び利用者は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請する。
ただし、教育研究事務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティポリシー及び手順等の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出る。

6-12　許可権限者は、申請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。

6-13　許可権限者は、例外措置の申請状況を台帳に記録し、CISO に報告する。

6-14　CISO は、情報統合管理会議において、例外措置の申請状況を踏まえた情報セキュリティポリシー及び手順等の追加又は見直しの検討を行う。

第３節　教育

6-15　CISO は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備する。

6-16　CISO は、情報セキュリティの状況の変化に応じ、システム管理者及び利用者に対して新たに教育すべき事項が明らかになった場合には、教育実施計画を見直す。

6-17　CISO は、システム管理者及び利用者の役割に応じて教育すべき内容を検討し、教育のための資料を整備する。

6-18　CISO は、システム管理者及び利用者が毎年度最低１回は教育を受講できるように、教育実施計画を立案するとともに、その実施体制を整備する。
教育の対象者には、役職員等、学生が含まれる。
教育実施の具体例を以下に示す。

（１）情報管理責任者への毎年の研修、説明会の実施及びその他の啓発活動を実施する。

（２）新規採用の役職員等に対して、業務で使用する財務会計システムや事務局 ICT システムの利用方法を説明する。

（３）学年始めのガイダンスにて、学部１年生、３年生及び修士課程１年生に対し、情報セキュリティビデオを利用して情報倫理教育を実施し、確認の問題を解いてもらうこと等で理解を深めてもらう。

（４）情報セキュリティ講習を受けたことがある役職員等に対しても再度講習を実施し、新しい事例等に関する知識を習得してもらう。また、必要に応じ、過去に教育した内容が習得できているか確認し、不足していた内容について対象者にフィードバックを行う。

6-19　CISO は、利用者等の入学、着任又は異動後に、３か月以内に受講できるように、その実施体制を整備する。

6-20　CISO は、CSIRT に属する役職員等に教育を適切に受講させること。

6-21　組織責任者は、システム管理者及び利用者に対して、情報セキュリティポリシ

一及び手順等に係る教育を適切に受講させる。

6-22　システム管理者及び利用者は、教育実施計画に従って、適切な時期に教育を受講する。

6-23　組織責任者は、教育の実施状況を記録し、CISO に報告する。

6-24　CISO は、教育の実施状況を分析、評価し、教育について継続的に見直しを行う。

第４節　情報セキュリティインシデントへの対応

6-25　CISO は、情報セキュリティインシデントの可能性を認知した際の報告を受付ける統一的な窓口（以下「統一的窓口」という。）の設置を含む本学関係者への報告手順を整備し、報告が必要な具体例を含め、システム管理者及び利用者に周知する。

6-26　CISO は、情報セキュリティインシデントを認知した際の学外との情報共有を含む対応手順を整備する。

6-27　CISO は、情報セキュリティインシデントの可能性に備え、教育研究事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備する。

6-28　CISO は、情報セキュリティインシデントへの対応の訓練の必要性を検討し、教育研究事務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備する。

6-29　CISO は、情報セキュリティインシデントについて学外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を学外の者に明示する。

6-30　CISO 及び組織責任者は、対応手順が適切に機能することを訓練等により確認する。

6-31　システム管理者及び利用者は、検知、発見、通報等により情報セキュリティインシデントの発生又はそのおそれを認知した場合は、基本規程に定める情報セキュリティ緊急時対応手順書のフローに従い、速やかに統一的窓口に報告し、その指示を仰ぐ。なお、紛失・盗難は、総務課にも報告を行う。

6-32　情報セキュリティインシデントの発生又はそのおそれの報告を受けた統一的窓口は、当該事案に関連する組織の情報セキュリティ専門部会員と連携し、以下の手順により事実関係を確認の上、ログの検査・分析等を行い、被害状況や影響範囲及び影響度など事態の全体像を把握し、情報セキュリティインシデントが発生したかどうかを判断する。

【事実関係の確認手順】

（１）学内からの通報受付

システム管理者又は利用者からインシデントの予兆・兆候等の連絡を受けた場合、当該システム管理者又は利用者へのヒアリング、学内 LAN や情報システムの状況確認（電源や LAN ケーブルの接続等の確認を含む。）を行う。また、システムベンダー等の外部委託事業者から学内 LAN や情

報システムの停止又は異常等を含むインシデントの予兆・兆候等の連絡を受けた場合は、ログ等の検査・分析を試みる。ログ等の検査・分析が難しいときは、セキュリティベンダー等の外部の専門家に協力の依頼又は要請を行う。

（2）学内システムから表示されたアラートやメッセージに関する通報受付

情報システムや OS から警報・警告、アラート、その他メッセージが表示されたとの通報があった場合（自動メール配信などを含む。）は、以下の確認を行う。

・警報・警告、アラート等を発した機器及びシステムを確認する。
・警報・警告、アラート等を発した機器及びシステムの運用、保守等を担当している外部委託事業者（システムベンダー等）を特定する。
・当該の外部委託事業者（システムベンダー等）へ問い合わせる。

（3）学外の第三者からの電話による通報受付

正式な通報であることを以下に留意して確認する。

・個人からの場合、折り返し確認させていただく旨を告げて、通報者の電話番号を控え、折り返しの電話により正式な通報であることを確認する。
・組織等の場合、相手先の正式名称および所属と氏名を確認の上、代表電話番号を探して電話を掛け(受信した電話番号には折り返さない。)、正式な通報であるか確認する。

正式な通報であることが確認されたら、通報受付の具体的な内容等について通報者にヒアリングを行う。

（4）学外の第三者からのメールでの通報受付

正式な通報であることを以下に留意して確認する。

・通報メールの添付ファイルは開かない。
・通報メールのリンクはクリックしない。
・発信元アドレス及び通報者の氏名（署名）の名前とドメイン名を確認する。
・不審点があれば通報メールは破棄する。
・通報者が個人の場合、通報メールに電話番号の記載があれば、その番号に電話を掛け、正式な通報であることを確認する。
・通報者が企業・団体等の場合、当該企業・団体等の代表番号を調べて電話を掛け（通報メールに記載されている電話番号には掛けない。)、正式な通報であるか確認する。

確認の結果、「なりすまし」等の場合、なりすまされた正規の発信元へ状況を説明し、なりすましの調査を依頼する。

正式な通報であることが確認された場合は､通報メールの具体的な内容、不明な点等について通報者にヒアリング等を行い、状況を確認する。

（5）マスコミからの通報受付

正式な通報であるかの確認は、学外の第三者からの電話での通報受付又は学外の第三者からのメールでの通報受付に準ずるが、以下の点に留意する。

・情報セキュリティインシデントに関連した質問には答えない。
・マスコミからの質問は、一言一句違わず記録するよう努める。

正式な通報であることが確認された場合、本学の広報担当者に、通報してきたマスコミへの対応と通報の具体的な内容等についてヒアリングを要請する。

（６）文部科学省、他大学、国立情報学研究所(NII)等からの通報受付

正式な通報であるかの確認は、学外の第三者からの電話での通報受付又は学外の第三者からのメールでの通報受付に準ずる。

正式な通報であることが確認された場合、通報の具体的な内容等について通報者にヒアリングを行う。

（７）クラウドサービス事業者からの通報受付

正式な通報であるかの確認は、学外の第三者からの電話での通報受付又は学外の第三者からのメールでの通報受付に準ずる。

正式な通報であることが確認されたら､通報の具体的な内容等について、クラウドサービス事業者に状況の報告を要請する。

【ログの検査・分析の実施手順】

（１）ログの収集・保全

検査・分析の対象とするログ（サーバ装置、通信回線装置、端末（モバイル端末を含む。）等）を特定し、その種類ごとに担当する外部委託事業者又は各機器を管理するシステム管理者にログの収集と提供を依頼する。

（２）ログの検査・分析

収集したログから事象の発生状況やその原因等を究明する。

情報システムへの不正侵入の有無を確認し、不正侵入があった場合は、侵入経路の特定を行う。

（３）検査・分析で必要となるログの種類と保管期間

検査・分析は、主に、DNS サーバ、プロキシサーバ、ファイアウォール及び各系で管理するサーバのログを対象として行うことを想定している。

具体的なログの種類及び保管期間は、実状に合わせ別途定める。

（４）統一的窓口の役割

統一的窓口は、ログの収集・保全、検査・分析作業がスムーズに行われるように、外部委託事業者と外部の専門家（セキュリティベンダー等）の間で必要な調整を行う。

また、サイバー攻撃（インターネットを経由して企業や団体等の情報システムを攻撃する行為をいう。）が疑われる場合の検査・分析は、サイバー攻撃の証跡のみならず、情報漏えいを示す証跡の有無も含め、できる限り詳細に実施する。

【トリアージ】

統一的窓口は、情報セキュリティインシデントの発生又はそのおそれの報告について上記【事実関係の確認手順】及び【ログの検査・分析の実施手順】に従い調査等を行い、以下に示す影響度から情報セキュリティインシデントとして対応する必要の有無を判断する。

※情報セキュリティインシデントの種別ごとのトリアージ実施手順を別表１に示す。

【影響度の判定基準】

事実関係の確認、ログの検査・分析の結果等を踏まえ、下表の判定基準

に照らして影響度を判定する。

影響度	判定基準	事案（例）
レベル３	当該事案の発生が学生や大学運営に重大な影響を与える場合	・学内 LAN 等に接続した情報機器がウイルス感染し、広範な情報機器に感染又は感染のおそれがある場合 ・長期間に渡り学内 LAN 又は情報システムを停止する必要がある場合 ・個人情報、研究情報の漏えいの可能性がある場合　等
レベル２	当該事案の影響が一部に限定される場合	・学内 LAN 等に接続している端末がウイルス感染したが、他の情報システムや端末に影響しない場合 ・CD、DVD、USB メモリ等の外部電磁的記録媒体を介したウイルス感染又はそのおそれがあるが、拡大範囲が限定される場合　等
レベル１	当該事案の影響が軽微な場合	・スタンドアロンで利用している端末へのウイルス感染又はそのおそれがある場合 ・外部電磁的記録媒体内のウイルス感染又はそのおそれがあるが、拡大する見込みがない場合　等

※影響度がレベル３の事案は、情報セキュリティインシデントの発生と判断する。

※影響度がレベル２又はレベル１の事案は、情報セキュリティインシデントとは判断しないが、必要な措置を講じた上で、情報セキュリティ専門部会長に報告を行い、必要に応じて再発防止策を講じる。

※情報セキュリティインシデントの種別ごとの影響度の判定基準を別表２に示す。

6-33　情報セキュリティインシデントの定義は、次の各事項のとおりとする。

（１）ネットワーク系インシデント

学外第三者又は悪意のある内部者が通信回線装置や情報システムの稼動を妨害し、又はデータの漏えい、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、通信回線の帯域やディスクや CPU の資源を浪費するなど、通信回線装置や情報システムの機能不全や障害又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及びそのおそれをいい、下記原因によるものを含む。

（ア）大量のスパムメールの送信

（イ）不正プログラム等のマルウェアの蔓延や意図的な配布

【具体例】

・ワーム、トロイの木馬、ランサムウェア

（ウ）発信者を偽った電子メールへのファイル添付や偽装した URL 又は URI への誘導などにより、利用者の環境に利用者の意図しないアプリケーションのインストール、不正プログラムの侵入、又は不正に情報を窃取する行為

【具体例】

・標的型攻撃、なりすまし、ワンクリック詐欺

(エ)情報システムの脆弱性や利用者による不適切なアカウント管理等を利用することにより、通信回線装置や情報システムのセキュリテ

ィに影響を及ぼす行為

【具体例】

・SQL インジェクション脆弱性、OS コマンドインジェクション脆弱性、クロスサイトスクリプティング脆弱性、クリックジャッキング脆弱性、バッファオーバーフロー及び整数オーバーフロー脆弱性

(オ)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

【具体例】

・標的型攻撃、辞書攻撃、ブルートフォース攻撃

(カ) サービス不能攻撃

【具体例】

・DoS 攻撃、DDoS 攻撃

(キ)管理者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

(ク) Peer to Peer (P2P) ソフトウェアの利用

(ケ) 不正アクセスによる学外接続

【具体例】

・標的型攻撃、なりすまし、辞書攻撃、ブルートフォース攻撃

(コ)学内 LAN への侵入を許すようなアカウントを格納した端末の盗難・紛失

(サ) アクセス権限設定の不備等の管理上の過失による秘密情報(個人情報を含む)の漏えい、データの消失又は改ざん

(2) 物理的インシデント

地震等の天災、火災、事故、盗難等及び悪意のある内部者による通信回線装置、サーバ装置、端末等の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通信回線装置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及びそのおそれをいう。

【具体例】

・落雷を原因とする停電による通信回線の障害に伴う全学的な学内 LAN・情報システムの停止

・工事中の事故を原因とする学内の一部通信回線の障害に伴う一部学内の学内 LAN・情報システムの停止

・情報システムを構成する一部の通信回線装置の盗難を原因とする通信回線の滅失に伴う情報システムの機能不全

・通信回線の設備、サーバ、端末等の物理的損壊や滅失

・悪意のある内部者による損壊

(3) 盗難・紛失インシデント

学外第三者または、悪意のある内部者により大学が管理する重要な情報(例 学生情報、研究情報、技術情報等)またはこれらが格納された機器、

書類の盗難・紛失の発生又はそのおそれをいう。

・学内 LAN への侵入を許すようなアカウントを格納した端末の盗難・紛失
・学生の要配慮情報等が記載された書類の紛失
・未公表の研究情報の盗難
・悪意のある内部者による窃盗

（4）外部（クラウド）サービスインシデント

学外第三者または、悪意のある内部者が、データセンターへの不正な攻撃を行い、本学が利用しているサービスの妨害、又はデータセンターに保管している本学のデータ漏えい・き損等により情報セキュリティの確保が困難な事由の発生及びそのおそれをいう。

なお、クラウドにおけるハードウェア障害の場合は、クラウド事業者の責任により対応・復旧を行うこととなるため、本学 CSIRT では対象としない。

・アカウントハイジャック
・データ喪失、データ侵害
・悪用、乱用、不正使用
・ID、認証情報、アクセス管理不備
・改ざん、漏洩、データ滅失

6-34　統一的窓口は、情報セキュリティインシデントが発生したと判断した場合、直ちに CISO へ報告する。報告を受けた CISO は、情報統合管理会議を招集し、CSIRT の発動を指示する。CSIRT は、情報セキュリティ緊急時対応手順書に基づく対応を行う。

6-35　発生した事案について、統一的窓口が情報セキュリティインシデントと判断しなかった場合は、組織責任者又はシステム管理者が定める通常の障害対応等の手順に従い対応する。なお、注意喚起等が必要と考えられる事案については、関係する者に情報共有を行うものとする。

6-36　CSIRT 責任者は、国、新潟県、警察等の関係機関への連絡が必要と判断した場合は、速やかに連絡を行う。認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるもので、当該情報セキュリティインシデントが犯罪に該当する場合及び盗難・紛失の場合は、必ず警察への通報・連絡を行う。

6-37　CSIRT 責任者は、情報セキュリティインシデントに関する対応内容を記録・報告させ、対応状況を把握する。また、必要に応じて対応全般に関する指示又は助言を行う。

6-38　CSIRT は、情報セキュリティインシデントの原因を調査するとともに再発防止策計画を策定し、CISO に報告する。

6-39　CSIRT 責任者は、情報セキュリティインシデント対応の結果から得られた教訓を CISO、情報セキュリティ専門部会、関係するシステム管理者等に共有する。

第７章　点検

第１節　情報セキュリティ対策の自己点検

7－1　CISO は、対策推進計画に基づき年度自己点検計画を策定する。

7－2　CISO は、システム管理者及び利用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。

7－3　CISO は、情報セキュリティの状況の変化に応じ、システム管理者及び利用者に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直す。

7－4　組織責任者は、年度自己点検計画に基づき、システム管理者及び利用者に自己点検の実施を指示する。

7－5　システム管理者及び利用者は、組織責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施する。

7－6　自己点検は、年に 1 回以上実施する。

7－7　CISO 及び組織責任者は、システム管理者及び利用者による自己点検結果を分析し、評価する。

7－8　CISO は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について､組織責任者に改善を指示し､改善結果の報告を受ける。

第２節　情報セキュリティ監査

7－9　情報セキュリティ監査責任者は、情報セキュリティポリシーの遵守状況について監査を行い、その結果を学長に報告する。
監査を行う者は、十分な専門的知識を有するものでなければならない。

7-10　学長は、監査結果を情報セキュリティポリシーの評価・見直しに反映させる。

【監査の実施手順例（監査基準の設定に基づく監査)】

いつ	情報統合管理会議が必要と認めた時期
だれが	情報統合管理会議監査部会
方法	（１）監査計画の立案（監査体制の確認及び日時・期間、範囲、対象、項目、役員会・教育研究評議会等への説明） （２）各系等・事務局への説明及び監査の実施 （３）各系等・事務局から実施調書提出受付 （４）調書の取りまとめ、情報統合管理会議への報告 （５）学長、CIS0 及び関係部署へ報告、規程群の更新案の提出 （６）必要に応じて、情報統合管理会議から各系等・事務局へフォローアップ

7-11　監査業務を外部委託する場合は、第 10 章第 1 節に基づき、実施する。

第８章　評価・見直し

第１節　情報セキュリティ管理の評価

８－１　情報統合管理会議は、監査の結果等も踏まえながら、情報セキュリティ管理のレベルを定期的又は臨時に評価し、その高度化を図るものとする。

第２節　情報セキュリティ対策の見直し

８－２　CISO は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報統合管理会議の審議を経て、情報セキュリティポリシー及び関係規程等について必要な見直しを行う。

８－３　CISO は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について報告させる。

８－４　CISO は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報統合管理会議の審議を経て、対策推進計画について定期的な見直しを行う。

第９章　情報の取扱い

第１節　情報の格付けの区分

９－１　情報の格付けの区分は、機密性、完全性、可用性について、それぞれ以下のとおりとする。

９－２　機密性についての格付けの定義（具体例は、別表３に示す。）

格付けの区分	区分の基準
機密性３情報	本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報

機密性２B 情報	本学で取り扱う機密性３以外の情報のうち、独立行政法人の保有する情報の公開に関する法律（平成 13 年 12 月５日法律第 140 号。以下、「独立行政法人等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、その漏えいにより本学の情報資産を利用する者のうち、学内外を含む多数の者の権利が侵害され、又は本学の活動の遂行に支障を及ぼすおそれがある情報
機密性２A 情報	本学で取り扱う機密性３以外の情報のうち、独立行政法人等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性が高い情報を含む情報であって、その漏えいにより本学の情報資産を利用する者のうち、特に学内の役職員等や学生の権利が侵害され、又は役職員等の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３情報、機密性２B 情報又は機密性２A 情報以外の情報

なお、機密性２A 情報、機密性２B 情報及び機密性３情報を「要機密情報」という。

９－３　完全性についての格付けの定義（具体例は、別表３に示す。）

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

なお、完全性２情報を「要保全情報」という。

９－４　可用性についての格付けの定義（具体例は、別表３に示す。）

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

可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。

また、要機密情報、要保全情報及び要安定情報を「要保護情報」という。

第２節　情報の取扱制限

9－5　「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを役職員等に確実に行わせるための手段をいう。具体例を別表４に示す。

9－6　役職員等は、格付けに応じた情報の取扱いを適切に行うため、機密性、完全性及び可用性の３つの観点から、取扱制限を定める。

第３節　情報の取扱い

9－7　CISO は、以下を含む情報の取扱いに関する規定を整備し、システム管理者及び利用者に周知する。

（１）情報の格付け及び取扱制限についての定義

（２）情報の格付け及び取扱制限の明示等についての手続

（３）情報の格付け及び取扱制限の継承、見直しに関する手続

9－8　CISO は、情報の取扱いに関する規定として、以下の手順を整備する。

（１）情報のライフサイクル全般にわたり必要な手順（教育研究事務の遂行以外の目的で情報を利用等しないよう努めること等）

（２）情報の入手・作成時の手順

（３）情報の利用・保存時の手順

（４）情報の提供・公表時の手順

（５）情報の運搬・送信時の手順

（６）情報の消去時の手順

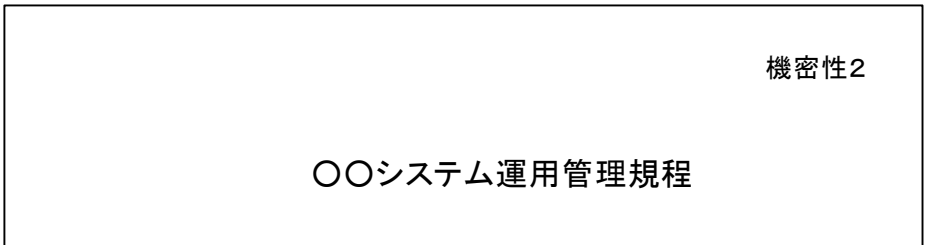
（７）情報のバックアップ時の手順

9－9　CISO は、情報の格付け及び取扱制限の明示の方法について、規定を整備する。

【明示例】

（１）電磁的記録として取扱われる情報に明示する場合

（ア）電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載



（イ）電磁的ファイル等の取扱単位ごとにファイル名自体へ記載

例）【機密性２】○○システム運用管理規程.docx

（ウ）フォルダ単位等で取扱う情報は、フォルダ名に記載
例）【機密性２】○○システム運用管理記録フォルダ

（エ）電子メールで取扱う情報は、メール本文又はメール件名に記載
例）件名：【機２】○○システムの運用支援見積書作成の依頼

（２）外部電磁的記録媒体に保存して取扱う情報に明示する場合
（ア）保存する電磁的ファイル又は文書等の単位ごとに記載
（イ）外部電磁的記録媒体本体に記載

（３）書面に印刷されることが想定される場合
（ア）書面のヘッダ部分等に記載
（イ）冊子等の単位で取扱う場合は、冊子の表紙、裏表紙等に記載

（４）既に書面として存在している情報に対して格付けや取扱制限を明示する場合
（ア）手書きによる記入
（イ）スタンプ等による押印

9-10　情報の加工時、複製時等における格付け及び取扱制限の継承、見直しは、以下に示すとおりとする。

（１）情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付け及び取扱制限を継承する。

（２）既存の情報に、より機密性の高い情報を追加するときは、格付け及び取扱制限を見直す。

（３）機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付け及び取扱制限を見直す。

（４）情報を複製する場合には、元となる情報の機密性に係る格付け及び取扱制限を継承する。

（５）完全性及び可用性については、作成時又は複製時に適切な格付けを決定する。

（６）他者が決定した情報の格付け及び取扱制限を見直す必要がある場合には、その決定者（決定について引き継いだ者を含む。）又はその上司に確認を求める。

9-11　役職員等は、自らが担当している教育研究事務の遂行以外の目的で、情報を利用等しないよう努めること。

9-12　役職員等は、情報の作成時及び学外の者が作成した情報を入手したことに伴う管理の開始時に、格付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し、明示等すること。

9-13　役職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付け及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付け及び取扱制限を継承すること。

9-14　役職員等は、修正、追加、削除その他の理由により、情報の格付け及び取扱制

限を見直す必要があると考える場合には、情報の格付け及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司に確認し、その結果に基づき見直すこと。

9-15　役職員等は、利用する情報に明示等された格付け及び取扱制限に従い、当該情報を適切に取扱うこと。

9-16　役職員等は、機密性 3 情報について要管理対策区域外で情報処理を行う場合は、組織責任者の許可を得ること。

9-17　役職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。

9-18　役職員等は、保存する情報にアクセス制限を設定するなど、情報の格付け及び取扱制限に従って情報を適切に管理すること。

9-19　役職員等は、USB メモリ等の外部電磁的記録媒体は原則として利用しない。利用する場合は、定められた利用手順に従うこと。

9-20　役職員等は、情報の格付け及び取扱制限に応じて、情報を以下のとおり取扱うこと。

（1）要保護情報を放置しない。

（2）要機密情報を必要以上に複製しない。

（3）電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。

（4）電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。

（5）情報の保存方法を変更する場合には、格付け、取扱制限及び記録媒体の特性に応じて必要な措置を講ずる。

9-21　役職員等は、入手した情報の格付け及び取扱制限が不明な場合には、情報の作成元又は入手元への確認を行うこと。

9-22　役職員等は、情報を公表する場合には、当該情報が機密性 1 情報に格付けされるものであることを確認すること。

9-23　役職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付け及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付け及び取扱制限に応じて適切に取扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。

9-24　役職員等は、機密性 3 情報を閲覧制限の範囲外の者に提供する場合には、組織責任者の許可を得ること。

9-25　役職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずること。

9-26　役職員等は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。

9-27　役職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保のための適切な措置を講ずること。

9-28　役職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付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。

9-29　役職員等は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬すること。

9-30　役職員等は、要機密情報である電磁的記録を要管理対策区域外に運搬又は学外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下の対策を講ずること。

（1）運搬又は送信する情報を暗号化する。

（2）運搬又は送信を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬または送信する。

（3）主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。

9-31　役職員等は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。

（1）本学管理の通信回線を用いて送信する。

（2）信頼できる通信回線を使用して送信する。

（3）VPN を用いて送信する。

（4）S/MIME 等の暗号化された電子メールを使用して送信する。

（5）本学独自で運用するなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。

9-32　役職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。

9-33　役職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、すべての情報を復元できないように抹消すること。

9-34　役職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

9-35　役職員等は、情報の格付けに応じて、適切な方法で情報のバックアップを実施すること。

9-36　役職員等は、取得した情報のバックアップについて、格付け及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。

9-37　役職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。

9-38　役職員等は、要保全情報又は要安定情報である電磁的記録又は重要な設計書

について、バックアップを取得すること。

9-39　役職員等は、要保全情報、要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップの保管について、災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定すること。

第４節　情報を取扱う区域の管理

9-40　CISO は、要管理対策区域の範囲を定めること。

9-41　CISO は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。

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

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

9-42　CISO は、要管理対策区域の安全性を確保するための段階的な対策の水準（以下「クラス」という。）を下表のとおり三段階のクラスに定める。

クラス	説明
クラス３	一部の限られた者以外の者の立入りを制限する必要があるなど、クラス２より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス２	役職員等以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス１	クラス３、クラス２以外の要管理対策区域

※便宜上、要管理対策区域外の区域はクラス０と呼び、クラス０＜クラス１＜クラス２＜クラス３の順位を設ける。すなわち、クラス０が最も下位のクラス、クラス３が最も上位のクラスとなる。

9-43　CISO は、クラス１の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定める。

（１）不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。

（２）不特定の者が容易に立ち入らないように、立ち入る者の身元、訪問目的等の確認を行うための措置を講ずること。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。

（３）クラス２以上の区域に不正に立ち入った者を容易に判別することができるように、以下を含む措置を講ずること。

（ア）役職員等は、身分証明書等を着用、明示する。クラス２及びクラス３の区域においても同様とする。

（イ）一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス２及びクラス３の区域においても同様とする。この際、一時

的に立ち入った者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。

9-44　CISOは、クラス２の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定める。

（１）クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。ただし、窓口のある教室、研究室、事務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は役職員等が窓口を常に目視できるような措置を講ずること。

（２）クラス２の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠すること。

（３）クラス２の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。

9-45　CISOは、クラス３の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定める。

（１）クラス３の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分すること。

（２）クラス３の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。

（３）クラス３の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにすること。

（４）一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずること。業者が作業を行う場合は立会いや監視カメラ等により監視するための措置を講ずること。

9-46　CISOは、クラスの割当ての基準を以下のように定める。

（１）サーバ室や日常的に機密性が高い情報を取扱う研究室、事務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス３を割り当てる。

（２）一般的な研究室、事務室や会議室には、役職員等及び関係の学生以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス２を割り当てる。

9-47　組織責任者は、CISOが定めた対策の基準を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定める。

9-48　組織責任者は、管理する区域について、CISO が定めた対策の基準と、周辺環境や当該区域で行う教育研究事務の内容、取扱う情報等を勘案し、当該区域において実施する対策を決定する。

9-49　組織責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う教育研究事務の内容、取扱う情報等を勘案し、当該区域において実施する対策を決定する。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定する。

9-50　組織責任者は、管理する区域に対して定めた対策を実施すること。利用者等が実施すべき対策については、利用者等が認識できる措置を講ずる。

9-51　組織責任者は、災害から要安定情報を取扱う情報システムを保護するために物理的な対策を講ずる。

9-52　システム管理者及び利用者は、利用する区域について組織責任者が定めた対策に従って利用すること。また、利用者等が学外の者を立ち入らせる際には、当該学外の者にも当該区域で定められた対策に従って利用させる。

9-53　組織責任者は、管理する区域について、以下の利用手順等を整備し、当該区域を利用する利用者等に周知する。

（1）扉の施錠及び開閉に関する利用手順

（2）一時的に立ち入る者が許可された者であることを確認するための手順

（3）一時的に立ち入る者を監視するための手順

第 10 章　外部委託

第 1 節　外部委託

10-1　CISO は、外部委託に係る以下の内容を含む規定を整備する。

（1）委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準

（2）委託先の選定基準

10-2　組織責任者又はシステム管理者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含める。

（1）委託先に提供する情報の委託先における目的外利用の禁止

（2）委託先における情報セキュリティ対策の実施内容及び管理体制

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

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

（5）情報セキュリティインシデントへの対応方法

（６）情報セキュリティ対策その他の契約の履行状況の確認方法

（７）情報セキュリティ対策の履行が不十分な場合の対応方法

10-３　組織責任者又はシステム管理者は、委託する業務において取扱う情報の格付け等を勘案し、必要に応じて以下の内容を仕様に含める。

（１）情報セキュリティ監査の受入れ

（２）サービスレベルの保証

10-４　組織責任者又はシステム管理者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、10-２及び 10-３の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本学に提供し、本学の承認を受けるよう、仕様内容に含める。

10-５　組織責任者又はシステム管理者は、以下の内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させる。また、変更があった場合は、速やかに再提出させる。

（１）当該委託業務に携わる者の特定

（２）当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

10-６　組織責任者又はシステム管理者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取扱う。

10-７　組織責任者又はシステム管理者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認する。

10-８　組織責任者又はシステム管理者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を利用者等より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく必要な措置を講じさせる。

10-９　組織責任者又はシステム管理者は、委託した業務の終了時に、委託先において取扱われた情報が確実に返却、又は抹消されたことを確認する。

10-10　組織責任者又はシステム管理者は、委託先への情報の提供等において、以下の事項を遵守する。

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

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

（３）委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかにシステム管理者に報告すること。

第２節　約款による外部サービスの利用

10-11　CISO は、以下を含む約款による外部サービスの利用に関する規定を整備する

こと。また、当該サービスの利用において要機密情報が取扱われないよう規定する。

（１）約款による外部サービスを利用してよい業務の範囲

（２）業務に利用する約款による外部サービス

（３）利用手続及び運用手順

10-12　組織責任者又はシステム管理者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定める。

10-13　CISO は、本学において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定めること。

（１）利用申請の許可権限者

（２）利用申請時の申請内容

（ア）利用する組織名

（イ）利用するサービス

（ウ）利用目的（業務内容）

（エ）利用期間

（オ）利用責任者（利用アカウントの責任者）

（３）サービス利用中の安全管理に係る運用手順

（ア）サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認

（イ）情報の滅失、破壊等に備えたバックアップの取得

（ウ）利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等）

（４）情報セキュリティインシデント発生時の連絡体制

10-14　組織責任者又はシステム管理者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用する。

第３節　ソーシャルメディアサービスによる情報発信

10-15　CISO は、本学が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定める。また、当該サービスの利用において要機密情報が取扱われないよう規定する。

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

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

10-16　組織責任者又はシステム管理者は、本学において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定める。

10-17　組織責任者又はシステム管理者は、要安定情報の一般利用者への提供にソーシャルメディアサービスを用いる場合は、本学の自己管理ウェブサイトに当該情報を掲載して参照可能とする。

10-18　CISO は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定める。

（１）アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

（２）URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等､その使用が避けられない場合を除き、原則使用しない。

10-19　CISO は、本学のアカウントによる情報発信が実際の本学のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定める。

（１）本学からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、本学が運用していることを利用者に明示すること。

（２）本学からの情報発信であることを明らかにするために､「nagaokaut.ac.jp」で終わるドメイン名（以下「本学ドメイン名」という。）を用いて管理しているウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

（３）運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページの URL を記載すること。

（４）ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

10-20　CISO は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う､いわゆる｢アカウント乗っ取り｣を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定める。

（１）パスワードを適切に管理すること。具体的には、ログインパスワードは十分な長さと複雑さを持たせ、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

（２）二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

（３）ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭

ったりした場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行うこと。

（４）ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。

10-21　CISO は、なりすましや不正アクセスを確認した場合の対応として、以下を含む対応手順を定める。

（１）自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。

（２）アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、CSIRT に報告するなど、適切な対応を行うこと。

第４節　クラウドサービスの利用

10-22　組織責任者又はシステム管理者は、クラウドサービス（民間事業者が提供するものに限らず、政府等が提供するものを含む。以下同じ。）を利用するに当たり、取扱う情報の格付け及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する。

10-23　組織責任者又はシステム管理者は、クラウドサービスで取扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定する。

10-24　組織責任者又はシステム管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とする。

10-25　組織責任者又はシステム管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める。

10-26　組織責任者又はシステム管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断する。

10-27　組織責任者又はシステム管理者は、クラウドサービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下のセキュリティ対策を実施することをクラウドサービスの選定条件とし、仕様内容にも含める。

（１）取扱う情報の可用性区分の格付けに応じた、サービス中断時の復旧要件

（２）取扱う情報の可用性区分の格付けに応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

10-28　組織責任者又はシステム管理者は、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティ対策を構築すること。また、対策を実現するために、以下のセキュリティ要件をクラウドサービスに求め、契約内容にも含める。

特に、運用段階で委託先が変更となる場合、開発段階等で設計したクラウドサービスのセキュリティ要件のうち継承が必須なセキュリティ要件について、変更後の委託先における維持・向上の確実性を事前に確認する。

（１）クラウドサービスに係るアクセスログ等の証跡の保存及び提供

（２）インターネット回線とクラウド基盤の接続点の通信の監視

（３）クラウドサービスの委託先による情報の管理・保管の実施内容の確認

（４）クラウドサービス上の脆弱性対策の実施内容の確認

（５）クラウドサービス上の情報に係る復旧時点目標（RPO）等の指標

（６）クラウドサービス上で取扱う情報の暗号化

（７）利用者の意思によるクラウドサービス上で取扱う情報の確実な削除・廃棄

（８）利用者が求める情報開示請求に対する開示項目や範囲の明記

第 11 章　情報システムに係る文書等の整備

第１節　情報システムに係る台帳等の整備

11-１　CISO は、すべての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備する。

11-２　組織責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について CISO に報告する。

11-３　CISO は、以下の内容を含む台帳を整備する。

（１）情報システム名

（２）管理する職場

（３）当該情報システムのシステム管理者の氏名及び連絡先

（４）システム構成

（５）接続する学外通信回線の種別

（６）取扱う情報の格付け及び取扱制限に関する事項

（７）当該情報システムの設計・開発、運用・保守に関する事項

11-４　CISO は、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備する。

（１）情報処理サービス名

（２）契約事業者

（３）契約期間

（４）情報処理サービスの概要

（５）ドメイン名（インターネット上で提供される情報処理サービスを利用する場合）

（６）取扱う情報の格付け及び取扱制限に関する事項

11-５　システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備する。

（１）情報システムを構成するサーバ装置及び端末関連情報

（２）情報システムを構成する通信回線及び通信回線装置関連情報

（３）情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

（４）情報セキュリティインシデントを認知した際の対応手順

11-６　システム管理者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備する。

（１）サーバ装置及び端末を管理する役職員等及び利用者を特定する情報

（２）サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン

（３）サーバ装置及び端末で利用するソフトウェアを動作させるために用いられる他のソフトウェアであって、以下を含むものの種類及びバージョン

（ア）動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの

（イ）フレームワーク等、ソフトウェアを実行するための実行環境となるもの

（ウ）プラグイン等、ソフトウェアの機能を拡張するもの

（エ）静的リンクライブラリ等、本学がソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの

（オ）インストーラー作成ソフトウェア等、本学がソフトウェアを開発する際に開発を支援するために使用するもの

（４）サーバ装置及び端末の仕様書又は設計書

11-７　システム管理者は、11-６（２）及び（３）の情報を収集するため、自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェアを導入するなどにより、これら情報を効率的に収集する手法を決定すること。

11-８　システム管理者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、以下を含む文書を整備すること。

（１）通信回線及び通信回線装置を管理する役職員等を特定する情報

（２）通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン

（３）通信回線及び通信回線装置の仕様書又は設計書

（４）通信回線の構成

（５）通信回線装置におけるアクセス制御の設定

（６）通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応

（７）通信回線の利用部門

11-９　システム管理者は、所管する情報システムについて、情報システム構成要素ごとのセキュリティ維持に関する以下を含む手順を定める。

（１）サーバ装置及び端末のセキュリティの維持に関する手順

（２）通信回線を介して提供するサービスのセキュリティの維持に関する手順

（３）通信回線及び通信回線装置のセキュリティの維持に関する手順

第２節　機器等の調達に係る規定の整備

11-10　CISO は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を本学が確認できることを加える。

11-11　CISO 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。

11-12　CISO は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を例に規定する。

（１）調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、本学と調達先が連携して原因を調査・排除できる体制を整備していること。

11-13　CISO は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408 に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定める。

11-14　CISO は、機器等の納入時の確認・検査手続には以下を含む事項を確認できる手続を定める。

（１）調達時に指定したセキュリティ要件の実装状況

（２）機器等に不正プログラムが混入していないこと

第 12 章　情報システムのライフサイクルの各段階における対策

第１節　情報システムの企画・要件定義

12-１　システム管理者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者（総合情報センター長）に求める。

12-２　システム管理者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する本学が定める運用管理規程等に応じた体制の確保を、CISO に求める。

12-３　CISO は 12-２で求められる体制の確保に際し、情報システムを統括する責任

者（総合情報センター長）の協力を得ることが必要な場合には、総合情報センター長に当該体制の全部又は一部の整備を求める。

12-4　システム管理者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取扱われる情報の格付け等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定する。

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

（２）情報システム運用時の監視等の運用管理機能要件（監視するデータが暗号化されている場合は、必要に応じて復号すること）

（３）情報システムに関連する脆弱性についての対策要件

12-5　システム管理者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定する。

12-6　システム管理者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト（独立行政法人情報処理推進機構）」（以下「IT 製品の調達におけるセキュリティ要件リスト」という。）の最新版を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定する。

12-7　システム管理者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定する。

12-8　システム管理者は、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（内閣官房 内閣サイバーセキュリティセンター）」の最新版を活用し、情報システムが提供する業務及び取扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定する。

12-9　システム管理者は、開発する情報システムが運用される際に想定される脅威の分析結果並びに当該情報システムにおいて取扱う情報の格付け及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書等に明記する。

12-10　システム管理者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、ST 確認を受ける。

12-11　システム管理者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、以下を含む措置を実施する。

（１）情報システム運用時に情報セキュリティ確保のために必要となる管理機

能を仕様書等に明記すること。

（２）情報セキュリティインシデントの発生を監視する必要があると認めた場合には、監視のために必要な機能について、以下を例とする機能を仕様書等に明記すること。

（ア）学外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能

（イ）不正プログラム感染や踏み台に利用されること等による学外への不正な通信を監視する機能

（ウ）学内 LAN への端末の接続を監視する機能

（エ）端末への外部電磁的記録媒体の挿入を監視する機能

（オ）サーバ装置等の機器の動作を監視する機能

12-12　システム管理者は、開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を含む対策を仕様書等に明記する。

（１）既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

（２）開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針。

（３）セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。

（４）ソフトウェアのサポート期間又はサポート打ち切り計画に関する本学への情報提供。

12-13　システム管理者は、構築する情報システムの構成要素のうち製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施する。

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

（２）IT 製品の調達におけるセキュリティ要件リストに掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定すること。

12-14　システム管理者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させる。

（１）情報システムのセキュリティ要件の適切な実装

（２）情報セキュリティの観点に基づく試験の実施

（３）情報システムの開発環境及び開発工程における情報セキュリティ対策

12-15　システム管理者は、情報セキュリティの観点に基づく試験の実施について、以下を含む事項を実施させる。

（１）ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離すること。

（２）情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。

（３）情報セキュリティの観点から実施した試験の実施記録を保存すること。

12-16　システム管理者は、開発工程における情報セキュリティ対策として、以下を含む事項を実施させる。

（１）ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。

（ア）ソースコードの変更管理

（イ）ソースコードの閲覧制限のためのアクセス制御

（ウ）ソースコードの滅失、き損等に備えたバックアップの取得

（２）情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

（３）セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること。

12-17　システム管理者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させる。

12-18　システム管理者は、情報システムの運用・保守を外部委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させる。

12-19　システム管理者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を含む要件を調達仕様書に記載するなどして、適切に実施させる。

（１）情報システムの運用環境に課せられるべき条件の整備

（２）情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

（３）情報システムの保守における情報セキュリティ対策

（４）運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

第２節　情報システムの調達・構築

12-20　システム管理者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用する。

12-21　システム管理者は、情報システムの構築において、情報セキュリティの観点か

ら必要な措置を講ずる。

12-22　システム管理者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずる。

12-23　システム管理者は、情報システムの構築において以下を含む情報セキュリティ対策を行う。

（１）情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対応するために開発環境を整備すること。

（２）セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。

（３）情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。

（４）セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施すること。

（５）脆弱性検査を含む情報セキュリティの観点での試験を実施すること。

12-24　システム管理者は、情報システムの運用保守段階へ移行するに当たり、以下を含む情報セキュリティ対策を行う。

（１）情報セキュリティに関わる運用保守体制の整備

（２）運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

（３）情報セキュリティインシデントを認知した際の対応方法の確立

12-25　システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認する。

12-26　システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認する。

第３節　情報システムの運用・保守

12-27　システム管理者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用する。

12-28　システム管理者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し、運用管理する本学との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用する。

12-29　システム管理者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理する。

12-30　システム管理者は、情報システムのセキュリティ監視を行う場合は、以下の内容を含む監視手順を定め、適切に監視運用する。

（１）監視するイベントの種類

（２）監視体制

（３）監視状況の報告手順

（４）情報セキュリティインシデントを認知した場合の報告手順

（５）監視運用における情報の取扱い（機密性の確保）

12-31　システム管理者は、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認する。

12-32　システム管理者は、情報システムにおいて取扱う情報について、当該情報の格付け及び取扱制限が適切に守られていることを確認する。

12-33　システム管理者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずる。

第４節　情報システムの更改・廃棄

12-34　システム管理者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付け及び取扱制限を考慮した上で、以下の措置を適切に講ずる。

（１）情報システム更改時の情報の移行作業における情報セキュリティ対策

（２）情報システム廃棄時の不要な情報の抹消

第５節　情報システムについての対策の見直し

12-35　システム管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずる。

第 13 章　情報システムの運用継続計画

第１節　情報システムの運用継続計画の整備・整合的運用の確保

13-１　CISO は、本学において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討する。

13-２　CISO は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認する。

第 14 章　情報システムのセキュリティ機能

第１節　主体認証機能

14-１　システム管理者は、情報システムや情報へのアクセスを管理するため、主体を

特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設ける。

14-2　システム管理者は、外部機関との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定する。

14-3　システム管理者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずる。

14-4　システム管理者は、利用者が正当であることを検証するための主体認証機能を設けるに当たっては、以下を例とする主体認証方式を決定し、導入する。この際、認証の強度として2つ以上の方式を組み合わせる主体認証方式（多要素主体認証方式）が求められる場合には、これを用いる。

（1）知識（パスワード等、利用者本人のみが知り得る情報）による認証

（2）所有（電子証明書を格納する IC カード又はワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証

（3）生体（指紋や静脈等、本人の生体的な特徴）による認証

14-5　システム管理者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、文字の種類や組合せ、桁数等のパスワード設定条件を利用者に守らせる機能を設ける。

14-6　システム管理者は、主体認証を行う情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下を例とする機能を設ける。

（1）利用者が定期的に変更しているか否かを確認する機能

（2）利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

（3）利用者が主体認証情報を変更する際に、以前に設定した主体認証情報の再設定を防止する機能

14-7　システム管理者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下を含む方法を用いて適切に管理する。

（1）主体認証情報を送信又は保存する場合には、その内容を暗号化する。

（2）主体認証情報に対するアクセス制限を設ける。

14-8　システム管理者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に利用され、又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設ける。

（1）当該主体認証情報及び対応する識別コードの利用を停止する機能

（2）主体認証情報の再設定を利用者に要求する機能

14-9　システム管理者は、情報システムにアクセスするすべての主体に対して、識別

コード及び主体認証情報を適切に付与し、管理するための措置を講ずる。

14-10　システム管理者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずる。

14-11　システム管理者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）する。

14-12　システム管理者は、識別コードの付与に当たっては、以下を例とする措置を講ずる。

（１）単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

（２）主体への識別コードの付与に関する記録を消去する場合のシステム管理者からの事前の許可

14-13　システム管理者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずる。

14-14　システム管理者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促す。

14-15　システム管理者は、知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促す。

14-16　システム管理者は、情報システムを利用する主体ごとに識別コードを個別に付与する。ただし、システム管理者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与する。

14-17　システム管理者は、主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、以下を例とする措置を講ずる。

（１）当該主体の識別コードを無効にする。

（２）当該主体に交付した主体認証情報格納装置を返還させる。

（３）無効化した識別コードを他の主体に新たに発行することを禁止する。

第２節　アクセス制御機能

14-18　システム管理者は、情報システムの特性、情報システムが取扱う情報の格付け及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設ける。

14-19　システム管理者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用する。

14-20　システム管理者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、必要に応じて、以下を例とするアクセス制御機能の要件を定める。

（１）利用時間や利用時間帯によるアクセス制御

（２）同一主体による複数アクセスの制限

（３）IP アドレスによる端末の制限

（４）ネットワークセグメントの分割によるアクセス制御

第３節　権限の管理

14-21　システム管理者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずる。

14-22　システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずる。

14-23　システム管理者は、権限管理を行う情報システムにおいて、以下を含めた機能を導入する。

（１）業務上必要な場合に限定する

（２）必要最小限の権限のみ付与

（３）管理者権限を行使できる端末をシステム管理者等の専用の端末とする

第４節　ログの取得・管理

14-24　システム管理者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得する。

14-25　システム管理者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対応方法等について定め、適切にログを管理する。

14-26　システム管理者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施する。

14-27　システム管理者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定する。

14-28　システム管理者は、所管する情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理する。

（１）事象の主体（人物又は機器等）を示す識別コード

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

14-29　システム管理者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定める。

14-30　システム管理者は、ログが取得できなくなった場合の対応方法を定める。

14-31　システム管理者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入する。
（１）ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化

第４節の二　通信の監視

14-32　システム管理者及び利用者は、通信回線を通じて行われる通信を傍受してはならない。ただし、CISO 又は当該通信回線を管理するシステム管理者は、セキュリティ確保のため、あらかじめ指定した者に、通信回線を通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

14-33　CISO 又は情報システムを統括する責任者（総合情報センター長）は、監視の範囲をあらかじめ具体的に定めておかなければならない。ただし、不正アクセス行為又はこれに類する重大なセキュリティ侵害に対応するために特に必要と認められる場合、CISO 又は組織責任者は、セキュリティ侵害の緊急性、内容及び程度に応じて、対応のために不可欠と認められる情報について、監視を行うよう命ずることができる。

14-34　監視を行う者は、監視によって知った通信の内容又は個人情報を、他の者に伝達してはならない。ただし、14-33 ただし書きに定める情報については、CISO 並びに組織責任者及び情報統合管理会議に伝達することができる。

14-35　監視によって採取された記録（以下「監視記録」という。）は、要機密情報、要保全情報、要安定情報とし、監視を行わせる者を情報の作成者とする。

14-36　監視を行わせる者は、監視を行う者に対して、監視記録を保存する期間をあらかじめ指示する。監視を行う者は、指示された期間を経過した監視記録を直ちに破棄しなければならない。ただし、監視記録から個人情報に係る部分を削除して、通信回線運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存する。

14-37　監視を行う者及び監視記録の伝達を受けた者は、通信回線運用・管理のために

必要な限りで、これを閲覧し、かつ、保存することができる。監視記録を不必要に閲覧してはならない。不必要となった監視記録は、直ちに破棄しなければならない。監視記録の内容を、法令に基づく場合等を除き、他の者に伝達してはならない。

14-38　複数の者が利用する情報機器を管理するシステム管理者は、当該機器に係る利用記録（以下「利用記録」という。）をあらかじめ定めた目的の範囲でのみ取得することができる。当該目的との関連で必要性の認められない利用記録を取得することはできない。

14-39　14-38 に規定する目的は、法令の遵守、情報セキュリティの確保、課金その他当該情報機器の利用に必要なものに限られる。個人情報の取得を目的とすることはできない。

14-40　利用記録は要機密情報、要保全情報とし、当該情報機器のシステム管理者を情報の作成者とする。

14-41　当該情報機器のシステム管理者は、第一項の目的のために必要な限りで、利用記録を閲覧することができる。他人の個人情報及び通信内容を不必要に閲覧してはならない。

14-42　当該情報機器のシステム管理者は、14-39 に規定する目的のために必要な限りで、利用記録を他の者に伝達することができる。

14-43　当該情報機器のシステム管理者は、14-39 の目的、これによって取得しようとする利用記録の範囲及び前項により利用記録を伝達する者を、あらかじめ組織責任者に申告し、かつ、当該機器の利用者に開示しなければならない。組織責任者は、申告の内容を不適切と認めるときは、これを修正させるものとする。

14-44　当該情報機器のシステム管理者又は利用記録の伝達を受けた者は、14-38 の目的のために必要な限りで、これを保有することができる。不要となった利用記録は、直ちに破棄しなければならない。ただし、当該情報機器のシステム管理者は、利用記録から個人情報に係る部分を削除して、通信回線運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

14-45　電子的に個人情報の提供を求めようとする者は、提供を求める情報の範囲、利用の目的、その情報が伝達される範囲を、あらかじめ相手方に示さなければならない。

14-46　14-45 の個人情報は、当人の請求により開示、訂正又は削除をしなければならない。また、そのための手続を示さなければならない。

14-47　複数の者が利用する情報機器を管理するシステム管理者は、利用者が保有する情報を通信回線運用に不可欠な範囲又は情報セキュリティインシデントへの対応に不可欠な範囲において、閲覧、複製又は提供することができる。

第５節　暗号・電子署名

14-48　システム管理者は、情報システムで取扱う情報の漏えいや改ざん等を防ぐた

め、以下の措置を講ずる。

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

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

14-49　システム管理者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）（以下「CRYPTREC 暗号リスト」という。）」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定める。

（１）利用者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、CRYPTREC 暗号リストに記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

（２）情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、CRYPTREC 暗号リストに記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

（３）暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

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

14-50　システム管理者は、本学における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を UPKI 電子証明書発行サービスが発行している場合は、それを使用するように定める。

14-51　システム管理者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずる。

（１）情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。

（２）複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。

（３）選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護される製品を利用することを確実にするため、「暗号モジュール試験及び認証制度(JCMVP)」に基づく認証を取得している製品を選択する。

（４）暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。

（５）機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のある暗号プロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

14-52　システム管理者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずる。

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

（２）暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、利用者等と共有を図ること。

14-53　システム管理者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下の方法により、当該情報の提供を可能とする。

（１）信頼できる機関による電子証明書の提供

（２）本学の窓口での電子証明書の提供

第 15 章　情報システムの脅威への対策

第１節　ソフトウェアに関する脆弱性対策

15-１　システム管理者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施する。

15-２　システム管理者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施する。

15-３　システム管理者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認する。

15-４　システム管理者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずる。

15-５　システム管理者は、対象となるソフトウェアの脆弱性に関して、以下を含む情報を適宜入手する。

（１）脆弱性の原因

（２）影響範囲

（３）対策方法

（４）脆弱性を悪用する不正プログラムの流通状況

15-６　システム管理者は、利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しない。

15-7　システム管理者は、以下を例とする手段で脆弱性対策の状況を確認する。

（1）構成要素ごとにソフトウェアのバージョン等を把握し、当該ソフトウェアの脆弱性の有無を確認する。

（2）脆弱性診断を実施する。

15-8　システム管理者は、脆弱性対策の状況を確認する間隔を、可能な範囲で短くする。

15-9　システム管理者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項について判断する。

（1）対策の必要性

（2）対策方法。この際、自動でソフトウェアを更新する機能を有するIT資産管理ソフトウェアを導入するなどにより、効率的に脆弱性対策を実施する手法を予め決定すること

（3）対策方法が存在しないゼロデイと呼ばれる状態の場合又は対策が完了するまでの期間に対する一時的な回避方法

（4）対策方法又は回避方法が情報システムに与える影響

（5）対策の実施予定時期

（6）対策試験の必要性

（7）対策試験の方法

（8）対策試験の実施予定時期

15-10　システム管理者は、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認する。

15-11　システム管理者は、脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録する。

（1）実施日

（2）実施内容

（3）実施者

15-12　システム管理者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル(以下「対策用ファイル」という。)は、信頼できる方法で入手する。

第2節　不正プログラム対策

15-13　システム管理者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入する。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

15-14　システム管理者は、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、不正プログラム対策ソフトウェア等により対策を講ずる。

15-15　システム管理者は、不正プログラム対策の状況を適宜把握し、必要な対応を行う。

15-16　システム管理者は、不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるよう構成する。

15-17　システム管理者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しない。

15-18　システム管理者は、不正プログラム対策ソフトウェア等は、定期的にすべてのファイルを対象としたスキャンを実施するよう構成する。

15-19　システム管理者は、想定されるすべての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行う。

15-20　システム管理者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対応を行う。

（１）不正プログラム対策ソフトウェア等の導入状況

（２）不正プログラム対策ソフトウェア等の定義ファイルの更新状況

第３節　サービス不能攻撃対策

15-21　システム管理者は、要安定情報を取扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下この条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行う。

15-22　システム管理者は、要安定情報を取扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築する。

15-23　システム管理者は、要安定情報を取扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視する。

15-24　システム管理者は、サーバ装置、端末及び通信回線装置について、以下を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対応する。

（１）パケットフィルタリング機能

（２）３-way handshake 時のタイムアウトの短縮

（３）各種 Flood 攻撃への防御

（４）アプリケーションゲートウェイ機能

15-25　システム管理者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築する。

15-26　システム管理者は、サーバ装置、端末及び通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合

には、以下を例とする対策を検討する。

（１）インターネットに接続している通信回線の提供元となる事業者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策

（２）サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入

（３）サーバ装置、端末及び通信回線装置及び通信回線の冗長化

15-27　システム管理者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対応を効率的に実施できる手段の確保について検討する。

15-28　システム管理者は、特定した監視対象について、監視方法及び監視記録の保存期間を定める。

15-29　システム管理者は、監視対象の監視記録を保存すること。

第４節　標的型攻撃対策

15-30　システム管理者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずる。

15-31　システム管理者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対応する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対応する対策（内部対策）を講ずる。

15-32　システム管理者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下を例とする対策を行う。

（１）不要なサービスについて機能を削除又は停止する。

（２）不審なプログラムが実行されないよう設定する。

（３）パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

15-33　システム管理者は、USB メモリ等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下を例とする対策を行う。

（１）原則として外部電磁的記録媒体を学内 LAN 上の端末に接続させず、クラウドサービスを利用させること。

（２）外部電磁的記録媒体を接続する場合は、暗号化機能を有するものとし、事前に特定しておく。

（３）外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。

（４）サーバ装置及び端末について、自動再生（オートラン）機能を無効化する。

（５）サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする。

（６）サーバ装置及び端末について、使用を想定しない USB ポートを無効化する。

（７）学内 LAN 上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。

15-34　システム管理者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を例とする対策を行う。

（１）重要サーバについては、学内 LAN を複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。

（２）認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずる。

15-35　システム管理者は、端末の管理者権限アカウントについて、以下を例とする対策を行う。

（１）不要な管理者権限アカウントを削除する。

（２）管理者権限アカウントのパスワードは、容易に推測できないものに設定する。

15-36　システム管理者は、重点的に守るべき業務・情報を取扱う情報システムについては、高度サイバー攻撃対応のためのリスク評価等のガイドラインに従って、対策を講ずる。

第 16 章　アプリケーション・コンテンツの作成・提供

第１節　アプリケーション・コンテンツ作成時の対策

16-１　CISO は、アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備する。

16-２　システム管理者は、学外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含める。

（１）提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

（２）提供するアプリケーションが脆弱性を含まないこと。

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

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

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

（６）サービス利用に当たって必須ではない、サービス利用者その他の者に関

する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

16-3　システム管理者は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前号に掲げる内容を調達仕様に含める。

16-4　システム管理者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を含む対策を行う。

（1）アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

（2）外部委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。

16-5　システム管理者は、提供するアプリケーション・コンテンツにおいて、学外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、当該学外へのアクセスが情報セキュリティ上安全なものであることを確認する。

16-6　システム管理者は、提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない学外へのアクセスを自動的に発生させる機能を含めない。

16-7　システム管理者は、文書ファイル等のコンテンツの提供において、当該コンテンツが改ざん等なく真正なものであることを確認できる手段がない場合は、「https://」で始まる URL のウェブページから当該コンテンツをダウンロードできるように提供する。

16-8　システム管理者は、改ざん等がなく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、国立情報学研究所 UPKI 電子証明書発行サービスの利用が可能である場合は、国立情報学研究所 UPKI 電子証明書発行サービスにより発行された電子証明書を用いて署名を施す。

第２節　アプリケーション・コンテンツ提供時の対策

16-9　システム管理者は、学外向けに提供するウェブサイト等が実際の本学提供のものであることを利用者が確認できるように、本学ドメイン名を情報システムにおいて使用するよう仕様に含める。ただし、ソーシャルメディアサービスによる情報発信は除く。

16-10　システム管理者は、学外向けに提供するウェブサイト等の作成を外部委託する場合においては、前号と同様、本学ドメイン名を使用するよう調達仕様に含める。

16-11　システム管理者は、利用者が検索サイト等を経由して本学のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずる。

16-12　システム管理者は、学外向けに提供するウェブサイトに対して、以下を例とす

る検索エンジン最適化措置（SEO 対策）を講ずる。

（１）クローラからのアクセスを排除しない。

（２）cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする。

（３）適切なタイトルを設定する。

（４）不適切な誘導を行わない。

16-13　システム管理者は、学外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、不審なサイトへのアクセスを防止するための対策を講ずる。

16-14　アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずる。

16-15　システム管理者及び利用者は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つ。

16-16　システム管理者及び利用者は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示する。また、短縮 URL を用いないこと。

16-17　システム管理者及び利用者は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示する。

16-18　システム管理者及び利用者は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知する URL 等の有効性を保つために以下の措置を講ずる。

（１）告知するアプリケーション・コンテンツを管理する組織名を明記する。

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

第 17 章　端末・サーバ装置等

第１節　端末

17-１　システム管理者は、要保護情報を取扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずる。

17-２　システム管理者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める。

17-３　システム管理者は、モバイル端末を除く端末について、原則としてクラス２以上の要管理対策区域に設置する。

17-４　システム管理者は、端末の盗難及び不正な持ち出しを防止するために、以下の対策を講ずる。

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

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

17-５　システム管理者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下の対策を講ずる。

（１）一定時間操作が無いと自動的にスクリーンロックするよう設定する。

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

17-６　システム管理者は、以下を考慮した上で、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める。

（１）ソフトウェアベンダ等のサポート状況

（２）ソフトウェアと外部との通信の有無及び通信する場合はその通信内容

（３）インストール時に同時にインストールされる他のソフトウェア

（４）その他、ソフトウェアの利用に伴う情報セキュリティリスク

17-７　システム管理者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行う。

17-８　システム管理者は、所管する範囲の端末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端末を検出等した場合には、改善を図る。

17-９　システム管理者は、端末の運用を終了する際に、端末の電磁的記録媒体のすべての情報を抹消する。

17-10　システム管理者は、要機密情報を取扱う本学が支給する端末（要管理対策区域外で使用する場合に限る）及び本学支給以外の端末について、以下の安全管理措置に関する規定を整備する。

（１）盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置

（２）本学支給以外の端末において不正プログラムの感染等により情報窃取されることを防止するための利用時の措置

17-11　組織責任者は、本学支給以外の端末を用いた本学の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者（以下「端末管理責任者」という。）を定める。

17-12　次の各号に掲げる責任者は、利用者等が当該各号に定める端末を用いて要機密情報を取扱う場合は、当該端末について 17-10 の安全管理措置を講ずる。

（１）組織責任者
本学が支給する端末（要管理対策区域外で使用する場合に限る）
（２）端末管理責任者
本学支給以外の端末

17-13　端末管理責任者は、要機密情報を取扱う本学支給以外の端末について、前項の規定にかかわらず 17-10（１）に定める安全管理措置のうち自ら講ずることができないもの 17-10（２）に定める安全管理措置を利用者に講じさせる。

17-14　利用者は、要機密情報を取扱う本学支給以外の端末について、17-13 において 16-10（１）に定める安全管理措置のうち端末管理責任者が講ずることができないもの及び 16-10（２）に定める安全管理措置を講ずる。

17-15　CISO は、要機密情報を取扱う本学が支給する端末（要管理対策区域外で使用する場合に限る）及び本学支給以外の端末について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を設ける。
（１）シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。
（２）セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。
（３）ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。
（４）端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。
（５）上記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。
（６）ハードディスク等電磁的記録媒体に保存されている情報を遠隔からの命令等により消去する機能を設ける。ただし、この場合は上記（３）から（５）を例とする暗号化の機能を組み合わせること。

17-16　CISO は、要機密情報を取扱う本学支給以外の端末について、以下を例に、利用者等が講ずるべき利用時の実施手順に係る安全管理措置を設ける。
（１）パスワード等による端末ロックの常時設定
（２）OS やアプリケーションの最新化
（３）不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（本学として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）
（４）端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取扱う情報のバックアップ手順を別途考慮する必要がある）
（５）本学提供の業務専用アプリケーションの利用（専用アプリケーションを

提供する場合のみ）

（６）以下を例とする禁止事項の遵守

（ア）端末、OS、アプリケーション等の改造行為

（イ）安全性が確認できていないアプリケーションのインストール及び利用

（ウ）利用が禁止されているソフトウェアのインストール及び利用

（エ）許可されていない通信回線サービスの利用（利用する回線を限定する場合）

（オ）第三者への端末の貸与

第２節　サーバ装置

17-17　システム管理者は、要保護情報を取扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずる。

17-18　システム管理者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保する。

17-19　システム管理者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める。

17-20　システム管理者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずる。

17-21　システム管理者は、要保護情報を取扱うサーバ装置については、クラス２以上の要管理対策区域に設置する。

17-22　システム管理者は、サーバ装置の盗難及び不正な持ち出しを防止するため、以下の対策を講ずる。

（１）施錠可能なサーバラックに設置して施錠する。

（２）容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

17-23　システム管理者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下の対策を講ずる。

（１）一定時間操作が無いと自動的にスクリーンロックするよう設定する。

17-24　システム管理者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため要安定情報を取扱う情報システムについては、将来の見通しも考慮し、必要に応じて以下の対策を講ずる。

（１）負荷分散装置、DNS ラウンドロビン方式等による負荷分散

（２）同一システムを 2 系統で構成することによる冗長化

17-25　システム管理者は、以下を考慮した上で、利用を認めるソフトウェア及び利用

を禁止するソフトウェアをバージョンも含め定める。

（1）ソフトウェアベンダのサポート状況

（2）ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容

（3）インストール時に同時にインストールされる他のソフトウェア

（4）その他、ソフトウェアの利用に伴う情報セキュリティリスク

17-26　システム管理者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行う。

17-27　システム管理者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図る。

17-28　システム管理者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずる。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

17-29　システム管理者は、要安定情報を取扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講ずる。

17-30　システム管理者は、所管する範囲内のサーバ装置の構成やソフトウェアの状態を定期的に確認する場合は、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録する。

17-31　システム管理者は、サーバ装置への無許可のアクセス等の不正な行為を監視するために、以下の対策を講ずる。

（1）アクセスログ等を定期的に確認する。

（2）IDS/IPS、WAF 等を設置する。

（3）不正プログラム対策ソフトウェアを利用する。

（4）ファイル完全性チェックツールを利用する。

（5）CPU、メモリ、ディスク I/O 等のシステム状態を確認する。

17-32　システム管理者は、要安定情報を取扱うサーバ装置については、運用状態を復元するために以下の対策を講ずる。

（1）サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。

（2）定期的なバックアップを実施する。

（3）サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。

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

17-33　システム管理者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体のすべての情報を抹消する。

第３節　複合機・特定用途機器

17-34　システム管理者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取扱う情報の格付け及び取扱制限に応じ、適切なセキュリティ要件を策定する。

17-35　システム管理者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずる。

17-36　システム管理者は、複合機の運用を終了する際に、複合機の電磁的記録媒体のすべての情報を抹消する。

17-37　システム管理者は、IT 製品の調達におけるセキュリティ要件リストを参照するなどし、複合機が備える機能、設置環境及び取扱う情報の格付け及び取扱制限に応じ、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記する。

17-38　システム管理者は、以下を例とする運用中の複合機に対する、情報セキュリティインシデントへの対策を講ずること。

（１）複合機について、利用環境に応じた適切なセキュリティ設定を実施する。

（２）複合機が備える機能のうち利用しない機能を停止する。

（３）印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用する。

（４）学内 LAN とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする。

（５）複合機をインターネットに直接接続しない。

（６）リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

（７）利用者ごとに許可される操作を適切に設定する。

17-39　システム管理者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消する。当該機能を備えていない複合機については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずる。

17-40　システム管理者は、特定用途機器について、取扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずる。

17-41　システム管理者は、特定用途機器の特性に応じて、以下を含む対策を講ずる。ただし、使用している特定用途機器の機能上の制約により講ずることができない対策を除く。

（１）特定用途機器について、主体認証情報を初期設定から変更した上で、適切に管理する。

（２）特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理する。

（３）特定用途機器が備える機能のうち利用しない機能を停止する。

（４）インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットやインターネットに接点を有する情報システムに接続しない。

（５）特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

（６）特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。

（７）特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。

（８）特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されているすべての情報を抹消する。

第 18 章　電子メール・ウェブ等

第 1 節　電子メール

18-１　システム管理者は、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。

18-２　システム管理者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備える。

18-３　システム管理者は、電子メールのなりすましの防止策を講ずる。

18-４　システム管理者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずる。

18-５　システム管理者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする利用者等の主体認証を行う機能を備える。

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

18-６　システム管理者は、以下を例とする電子メールのなりすましの防止策を講ずる。

（１）SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain- based Message Authentication, Reporting & Conformance）等の送信ドメイン認証技術による送信側の対策を行う。

（２）SPF、DKIM、DMARC 等の送信ドメイン認証技術による受信側の対策を行う。

（３）S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用する。

18-７　利用者は、要保護情報を電子メールで送信する場合、情報漏えい防止のため、CISO の定めた方式によりデータを暗号化する。
電子メールで送信したデータの復号方法又は復号情報（パスワード等）は、電子メール以外の手段で送信先に伝える。

18-８　利用者は、電子メールアドレスの漏えい防止のため、宛先、CC、BCC を使い分ける。

18-９　利用者は、電子メールの誤送信防止のため、送信前に宛先、CC、BCC のそれぞれについて、送信先アドレスに誤りがないか再確認を行う。

18-10　利用者は、電子メールにデータを添付して送信する場合、添付するデータが間違っていないか再確認を行う。

第２節　ウェブ

18-11　システム管理者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずる。

（１）ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

（２）ウェブコンテンツの編集作業を担当する主体を限定すること。

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

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

（５）インターネットを介して転送される情報の盗聴及び改ざんの防止のため、すべての情報に対する暗号化及び電子証明書による認証の対策を講じること。

18-12　システム管理者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。

18-13　システム管理者は、不要な機能の停止又は制限として、以下を例とするウェブサーバの管理や設定を行う。

（１）CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする。

（２）ディレクトリインデックスの表示を禁止する。

（３）ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する。

（４）ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。

18-14　システム管理者は、ウェブコンテンツの編集作業を担当する主体の限定として、以下を例とするウェブサーバの管理や設定を行う。

（１）ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテ

ンツの作成や更新に必要な者以外に更新権を与えない。

（２）OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。

18-15　システム管理者は、公開してはならない又は無意味なウェブコンテンツが公開されないよう管理することとして、以下を例とするウェブサーバの管理や設定を行う。

（１）公開を想定していないファイルをウェブ公開用ディレクトリに置かない。

（２）初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。

18-16　システム管理者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行う。

（１）ウェブコンテンツの更新の際は、専用の端末を使用して行う。

（２）ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する。

（３）ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行う。

18-17　システム管理者は、通信時の盗聴による第三者への情報の漏えいの防止及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を含むウェブサーバの実装を行う。

（１）TLS（SSL）機能を適切に用いる。

（２）TLS（SSL）機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局(証明書発行機関)により発行された電子証明書を用いる。

（３）暗号技術検討会及び関連委員会（CRYPTREC）により作成された「SSL/TLS 暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する。

18-18　システム管理者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対応を行う。

18-19　システム管理者は、以下を含むウェブアプリケーションの脆弱性を排除する。

（１）SQL インジェクション脆弱性

（２）OS コマンドインジェクション脆弱性

（３）ディレクトリトラバーサル脆弱性

（４）セッション管理の脆弱性

（５）アクセス制御欠如と認可処理欠如の脆弱性

（６）クロスサイトスクリプティング脆弱性

（７）クロスサイトリクエストフォージェリ脆弱性

（８）クリックジャッキング脆弱性

（９）メールヘッダインジェクション脆弱性

（10）HTTP ヘッダインジェクション脆弱性

（11）eval インジェクション脆弱性

（12）レースコンディション脆弱性

（13）バッファオーバーフロー及び整数オーバーフロー脆弱性

第３節　ドメインネームシステム（DNS）

18-20　システム管理者は、要安定情報を取扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずる。

18-21　システム管理者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずる。

18-22　システム管理者は、コンテンツサーバにおいて、本学のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずる。

18-23　システム管理者は、要安定情報を取扱う情報システムの名前解決を提供するコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講ずる。

（１）コンテンツサーバを冗長化する。

（２）通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。

18-24　システム管理者は、学外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は必要であれば学内からの名前解決の要求のみに応答をするよう、以下を例とする措置を講ずる。

（１）キャッシュサーバの設定でアクセス制御を行う。

（２）ファイアウォール等でアクセス制御を行う。

18-25　システム管理者は、DNS キャッシュポイズニング攻撃から保護するため、以下を例とする措置を講ずること。

（１）ソースポートランダマイゼーション機能を導入する。

（２）DNSSEC を利用する。

18-26　システム管理者は、学内のみで使用する名前の解決を提供するコンテンツサーバにおいて、以下を例とする当該コンテンツサーバで管理する情報の漏えいを防止するための措置を講ずる。

（１）外部向けのコンテンツサーバと別々に設置する。

（２）ファイアウォール等でアクセス制御を行う。

18-27　システム管理者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持する。

18-28　システム管理者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認する。

18-29　システム管理者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずる。

18-30　システム管理者は、キャッシュサーバにおいて、ルートヒントファイル（DNSルートサーバの情報が登録されたファイル）の更新の有無を定期的（３か月に一度程度）に確認し、最新のDNSルートサーバの情報を維持する。

第４節　データベース

18-31　システム管理者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行う。

18-32　システム管理者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずる。

18-33　システム管理者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずる。

18-34　システム管理者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずる。

18-35　システム管理者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化を行う。

18-36　システム管理者は、必要に応じて情報システムの管理者とデータベースの管理者を別にする。

18-37　システム管理者は、データベースに格納されているデータにアクセスする必要のない利用者に対して、データへのアクセス権を付与しないこと。

18-38　システム管理者は、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずる。

18-39　システム管理者は、業務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずる。

（１）一定数以上のデータの取得に関するログを記録し、警告を発する。

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

18-40　システム管理者は、データベースにアクセスする機器上で動作するプログラムに対して、SQLインジェクションの脆弱性を排除する。

18-41　システム管理者は、データベースにアクセスする機器上で動作するプログラムに対してSQLインジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討する。

（１）ウェブアプリケーションファイアウォールの導入

（２）データベースファイアウォールの導入

18-42　システム管理者は、格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実

施する。

第 19 章　通信回線

第 1 節　通信回線

19-1　システム管理者は、通信回線構築時に、当該通信回線に接続する情報システムにて取扱う情報の格付け及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずる。

19-2　システム管理者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設ける。

19-3　システム管理者は、要機密情報を取扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずる。

19-4　システム管理者は、利用者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずる。

19-5　システム管理者は、通信回線装置を要管理対策区域に設置する。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにする。

19-6　システム管理者は、要安定情報を取扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずる。

19-7　システム管理者は、学内 LAN にインターネット回線、公衆通信回線等の学外通信回線を接続する場合には、学内 LAN 及び当該学内 LAN に接続されている情報システムの情報セキュリティを確保するための措置を講ずる。

19-8　システム管理者は、学内 LAN と学外通信回線との間で送受信される通信内容を監視するための措置を講ずる。

19-9　システム管理者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備する。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。

19-10　システム管理者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保する。

19-11　システム管理者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておく。

19-12　システム管理者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取扱う情報の格付け及び取扱制限に応じて、以下を例とする通信

経路の分離を行う。

（1）外部との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離する。

（2）業務目的や取扱う情報の格付け及び取扱制限に応じて情報システムごとに VLAN により通信経路を分離し、それぞれの通信制御を適切に行う。

（3）他の情報システムから独立した専用の通信回線を構築する。

19-13　システム管理者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設ける。通信回線の秘匿性確保の方法として、TLS（SSL）、IPsec 等による暗号化を行う。また、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定する。

19-14　システム管理者は、学内 LAN への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずる。

（1）情報システムの機器番号等により接続機器を識別する。

（2）クライアント証明書により接続機器の認証を行う。

19-15　システム管理者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、以下の措置を講ずる。

（1）通信回線装置を施錠可能なラック等に設置する。

（2）施設内に敷設した通信ケーブルを物理的に保護する。

（3）通信回線装置の操作ログを取得する。

19-16　システム管理者は、要安定情報を取扱う情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずる。

（1）通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。

（2）通信回線及び通信回線装置を冗長構成にする。

19-17　システム管理者は、学内 LAN に、インターネット回線や公衆通信回線等の学外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講ずる。

（1）ファイアウォール、WAF（Web Application Firewall）、リバースプロキシ等により通信制御を行う。

（2）通信回線装置による特定の通信プロトコルの利用を制限する。

（3）IDS/IPS により不正アクセスを検知及び遮断する。

19-18　システム管理者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、以下を例とする対策を講ずる。

（1）リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う。

（2）主体認証によりアクセス制御する。

（3）通信内容の暗号化により秘匿性を確保する。

（４）ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにする。

19-19　システム管理者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずる。

19-20　システム管理者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行う。

19-21　システム管理者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図る。

19-22　システム管理者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更する。

19-23　システム管理者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、総合情報センターネットワークインフラ部門に申請し、許可を得る。また、組織責任者は、情報セキュリティインシデント発生時の調査対応のために作業記録を作成し、保管する。

19-24　システム管理者は、要安定情報を取扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し、保管する。

19-25　システム管理者は、通信回線装置の運用を終了する場合には、総合情報センターネットワークインフラ部門に報告する。
組織責任者は、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されているすべての情報を抹消するなど適切な措置を講ずる。

19-26　システム管理者は、VPN 回線を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずる。

19-27　システム管理者は、利用者等の業務遂行を目的としたリモートアクセス環境を、学外通信回線を経由して本学の情報システムへリモートアクセスする形態により構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずる。

19-28　システム管理者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、総合情報センターネットワークインフラ部門に申請して許可を得たうえで以下の対策を講ずる。

（１）利用開始及び利用停止時の申請手続の整備

（２）通信を行う端末の識別又は認証

（３）利用者の認証

（４）通信内容の暗号化
（５）主体認証ログの取得及び管理
（６）リモートアクセスにおいて利用可能な公衆通信網の制限
（７）アクセス可能な情報システムの制限
（８）リモートアクセス中の他の通信回線との接続禁止

19-29　システム管理者は、無線 LAN 技術を利用して学内 LAN を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずる。

19-30　システム管理者は、無線 LAN 技術を利用して学内 LAN を構築する場合は、通信回線の構築時共通の対策に加えて、以下を例とする対策を講ずる。
（１）SSID の隠蔽
（２）無線 LAN 通信の暗号化
（３）MAC アドレスフィルタリングによる端末の識別
（４）802.1X による無線 LAN へのアクセス主体の認証
（５）無線 LAN 回線利用申請手続の整備
（６）無線 LAN 機器の管理手順の整備
（７）無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対応手順の整備

19-31　システム管理者は、情報コンセントを設置する場合は、以下を例とする対策を講ずる。
（１）利用開始及び利用停止時の申請手続の整備
（２）通信を行う端末の識別又は認証
（３）利用者の認証
（４）主体認証ログの取得及び管理
（５）情報コンセント経由でアクセス可能な情報システムの明確化
（６）情報コンセント接続中の他の通信回線との接続禁止
（７）情報コンセント接続方法の機密性の確保
（８）情報コンセントに接続する端末及び通信回線装置の管理

19-32　システム管理者は、端末の学内 LAN への接続の申請を受けた場合は、別途定める接続手順に従い、申請者に対して接続の諾否を通知し必要な指示を行う。

19-33　システム管理者は、サーバ装置及び通信回線装置の利用を総合的かつ計画的に推進するため、サーバ装置の CPU 資源及びディスク資源並びに通信回線帯域資源を利用者等の利用形態に応じて適切に分配し管理する。

19-34　システム管理者は、所管組織の通信回線装置で使用するドメイン名や IP アドレス等の情報について、総合情報センターネットワークインフラ部門から割り当てを受け、利用者からの利用形態に応じて適切に分配し管理する。

19-35　CISO は、学内 LAN を構築し運用するにあたっては、学内 LAN の上流ネット

ワークとなる学外通信回線との整合性に留意する。

第２節　IPv6 通信回線

19-36　システム管理者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択する。

19-37　システム管理者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずる。

（１）グローバル IP アドレスによる直接の到達性における脅威

（２）IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

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

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

19-38　システム管理者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正な IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずる。

第 20 章　情報システムの利用

20-１　CISO は、本学の情報システムの利用のうち、情報セキュリティに関する規定を整備する。

20-２　CISO は、利用者が本学の支給する端末（要管理対策区域外で使用する場合に限る）及び本学支給以外の端末を用いて要保護情報を取扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定める。

20-３　CISO は、要管理対策区域外において学外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で学内 LAN に接続することについての可否を判断した上で、可と判断する場合は、当該端末（支給外端末を含む）から学内 LAN を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定める。

20-４　CISO は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定める。当該手順には、以下の事項を含める。

（１）利用者等は、国の行政機関、独立行政法人若しくは指定法人が支給する外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により本学との間で取り決めた学外の組織から受け取った外部電磁的記録媒体を使用すること。

（２）自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずること。

20-５　CISO は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続を定める。

20-６　CISO は、本学の情報システムの利用における情報セキュリティに関する規定として、以下を例とする実施手順を定める。

（１）情報システムの基本的な利用のうち、情報セキュリティに関する手順

（２）電子メール及びウェブの利用のうち、情報セキュリティに関する手順

（３）識別コードと主体認証情報の取扱手順

（４）暗号と電子署名の利用に関する手順

（５）不正プログラム感染防止の手順

（６）アプリケーション・コンテンツの提供時に学外の情報セキュリティ水準の低下を招く行為の防止に関する手順

（７）ドメイン名の使用に関する手順

20-７　CISO は、利用者が本学の支給する端末（要管理対策区域外で使用する場合に限る）及び本学支給以外の端末を用いて要保護情報を取扱う場合の利用手順を、以下を例として定める。

（１）端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化

（２）盗み見に対する対策（のぞき見防止フィルタの利用等）

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

（４）利用する場所や時間の限定

（５）端末の盗難・紛失が発生した際の緊急対応手順

20-８　CISO は、利用者等が本学の支給する端末（要管理対策区域外で使用する場合に限る）及び本学支給以外の端末を用いて要保護情報を取扱う場合について、以下を含む許可手続を定める。

（１）利用時の許可申請手続

（２）手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線の接続形態等）

（３）利用期間満了時の手続

（４）許可権限者（システム管理者）による手続内容の記録

20-９　CISO は、要管理対策区域外にて学外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で学内 LAN に接続することの許可手続として、以下を含む手続を規定し、利用者等に遵守させる。

（１）利用時の許可申請手続

（２）手続内容（利用者、目的、利用する情報、端末等）

（３）利用期間満了時の手続

（４）許可権限者（システム管理者）による手続内容の記録

20-10　CISO は、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順として以下の事項を含めて定める。

（１）原則として USB メモリ等の外部電磁的記録媒体は利用せず、クラウドサービスを始めとした情報システムを利用する。

（２）主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。

（３）要機密情報は保存される必要がなくなった時点で速やかに削除する。

（４）外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行う。

（５）外部電磁的記録媒体の利用者が利用内容を貸出簿等に記録する。

20-11　CISO は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続として、以下を含む手続を規定し、利用者等に遵守させること。

（１）利用時の許可申請手続

（２）手続内容（利用者、利用期間、主たる利用場所、目的、記録する情報、機器名）

（３）利用期間満了時の手続

（４）許可権限者（システム管理者）による手続内容の記録

20-12　システム管理者は、利用者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。

20-13　システム管理者は、学外のウェブサイトについて、利用者等が閲覧できる範囲を制限する機能を情報システムに導入する。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

（１）ウェブサイトフィルタリング機能

（２）事業者が提供するウェブサイトフィルタリングサービスの利用

20-14　システム管理者は、利用者等が不審なメールを受信することによる被害をシステム的に抑止する機能を情報システムに導入する。具体的には、以下を例とする機能を導入する。また、当該機能に係る設定や条件について定期的に見直す。

（１）受信メールに対するフィルタリング機能

（２）受信メールをテキスト形式で表示する機能

（３）スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがないメールクライアントの導入

（４）受信メールに添付されている実行プログラム形式のファイルを削除することで実行させない機能

20-15　利用者は、研究教育事務の遂行以外の目的で情報システムを利用しないよう努めること。

20-16　利用者は、組織責任者が接続許可を与えた通信回線以外に本学の情報システムを接続しないこと。

20-17　利用者は、学内 LAN に、組織責任者の接続許可を受けていない情報システムを接続しないこと。

20-18　利用者は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを研究教育事務上の必要により利用する場合は、組織責任者の承認を得ること。

20-19　利用者は、接続が許可されていない機器等を情報システムに接続しないこと。

20-20　利用者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。

20-21　利用者は、本学が支給する端末（要管理対策区域外で使用する場合に限る）及び本学支給以外の端末を用いて要保護情報を取扱う場合は、定められた利用手順に従うこと。

20-22　利用者は、次の各号に掲げる端末を用いて当該各号に定める情報を取扱う場合は、組織責任者の許可を得ること。

（１）本学が支給する端末（要管理対策区域外で使用する場合に限る）
　　機密性３情報、要保全情報又は要安定情報

（２）本学支給以外の端末
　　要保護情報

20-23　利用者は、要管理対策区域外において学外通信回線に接続した端末（支給外端末を含む）を要管理対策区域外において学内 LAN に接続する場合は、定められた安全管理措置を講ずること。

20-24　利用者は、要管理対策区域外において学外通信回線に接続した端末（支給外端末を含む）を要管理対策区域外において学内 LAN に接続する場合は、組織責任者の許可を得ること。

20-25　利用者は、機密性３情報、要保全情報又は要安定情報が記録された USB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、システム管理者の許可を得ること。

20-26　利用者は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下の措置を講ずること。

（１）スクリーンロックの設定

（２）利用後のログアウト徹底

（３）利用後に情報システムを鍵付き保管庫等に格納し施錠

20-27　利用者は、要機密情報を含む電子メールを送受信する場合には、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。

20-28　利用者は、学外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に本学ドメイン名を使用すること。ただし、電子メールを受信する学外の者が、本学の利用者等から送信された電子メールであることを認知できる場合（本学ドメイン名が使用できない場合に限る。）。

20-29　利用者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対応すること。

20-30　利用者は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。

20-31　利用者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

20-32　利用者は、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。

（１）送信内容が暗号化されること

（２）当該ウェブサイトが送信先として想定している組織のものであること

20-33　利用者は、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。

20-34　利用者は、自己に付与された識別コードを適切に管理すること。

20-35　利用者は、管理者権限を持つ識別コードを付与された場合には、システム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。

20-36　利用者は、自己の主体認証情報の管理を徹底すること。

20-37　利用者は、自己に付与された識別コードを適切に管理するため、以下を含む措置を講ずること。

（１）知る必要のない者に知られるような状態で放置しない。

（２）他者が主体認証に用いるために付与及び貸与しない。

（３）識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止する。

20-38　利用者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。

（１）自己の主体認証情報を他者に知られないように管理する。

（２）自己の主体認証情報を他者に教えない。

（３）主体認証情報を忘却しないように努める。

（４）主体認証情報を設定するに際しては、容易に推測されないものにする。

（５）異なる識別コードに対して、共通の主体認証情報を用いない。

（６）異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない。（シングルサインオンの場合を除く。）

（７）組織責任者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更する。

20-39　利用者は、所有による主体認証情報を用いる場合には、以下の管理を徹底すること。

（１）主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する。

（２）主体認証情報格納装置を他者に付与及び貸与しない。

（３）主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する。

（４）主体認証情報格納装置を利用する必要がなくなった場合には、これをシステム管理者に返還する。

20-40　利用者は、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。

20-41　利用者は、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。

20-42　利用者等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。

20-43　利用者は、不正プログラム感染防止に関する措置に努めること。

20-44　利用者は、情報システム（支給外端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずること。

20-45　利用者は、不正プログラム対策ソフトウェアを活用し、不正プログラム感染を回避するための以下措置に努めること。

（１）不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しない。また、検知されたデータファイルをアプリケーション等で読み込まない。

（２）不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持する。

（３）不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にする。

（４）不正プログラム対策ソフトウェア等により定期的にすべてのファイルに対して、不正プログラムの検査を実施する。

20-46　利用者は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

20-47　利用者は、不正プログラムに感染するリスクを低減する情報システムの利用方法として、以下のうち実施可能な措置を講ずること。

（１）不審なウェブサイトを閲覧しない。

（２）アプリケーションの利用において、マクロ等の自動実行機能を無効にす

る。

（３）プログラム及びスクリプトの実行機能を無効にする。

（４）安全性が確実でないプログラムをダウンロードしたり実行したりしない。

第 21 章　本学支給以外の端末の利用

21-１　CISO は、本学支給以外の端末の利用について、取扱うことになる情報の格付け及び取扱制限、本学が講じる安全管理措置、当該端末の管理は本学ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、本学における本学支給以外の端末の利用の可否を判断する。

21-２　CISO は、利用者等が本学支給以外の端末を用いて研究教育事務に係る情報処理を行う場合の許可等の手続を定める。

21-３　CISO は、本学支給以外の端末を利用する際に、以下を含む許可等の手続を整備し、利用者等に周知する。

（１）以下を含む本学支給以外の端末利用時の申請内容

（ア）申請者の氏名、所属、連絡先

（イ）利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）

（ウ）利用する端末の機種名

（エ）利用目的、取扱う情報の概要、要機密情報の利用の有無等

（オ）主要な利用場所

（カ）利用する主要な通信回線サービス

（キ）利用する期間

（２）利用許諾条件

（３）申請手順

（４）利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順

（５）利用期間満了時の利用終了又は利用期間更新の手続方法

（６）許可権限者（端末管理責任者）

21-４　利用者は、本学支給以外の端末を用いて研究教育事務に係る情報処理を行う場合には、端末管理責任者の許可を得ること。

21-５　利用者は、情報処理の目的を完了した場合は、要機密情報を本学支給以外の端末から消去すること。

以上

別表1　情報セキュリティインシデントの種別ごとのトリアージ実施手順（第6章6-32関連）

情報セキュリティインシデント種別	実施事項	実施手順
ネットワーク系インシデント	1　ログの収集、保全	・保全、調査するサーバ（ログ）の種類ごとに担当する外部委託事業者又は、各サーバを管理する担当者へログの収集依頼を行う。 （通常は、検査・分析に際して必要となる、各情報システム及び機器の操作・設定は、各サーバを導入・設定した外部委託事業者が行う。） 【検査・分析で必要となるログの種類と保管期間】 ・主に、DNSサーバ、プロキシサーバ、ファイアウォール及び各系で管理するサーバのログを収集し、検査・分析に用いる。 ・具体的なサーバ毎のログの種類及び保管期間は、実状に合わせ別途定める。
	2　ログの検査・分析	・収集したログを用いてインシデントの調査、原因究明を行う。 ・ログを過去に遡って、情報システムへの侵入を確認し、経路の特定を行う。
	3　検査・分析結果の報告	・当該部署の情報セキュリティ専門部会員及び統一的窓口は、インシデント予兆等の検査・分析結果及び影響度判定結果について、情報セキュリティインシデント報告書（様式1）に、報告時点までに判明している事項を記載し、情報セキュリティ専門部会長に報告する。
		・報告を受けた情報セキュリティ専門部会長は、影響度判定の結果、当該事案がレベル3に該当すると判断された場合、情報セキュリティ専門部会長（CSIRT責任者）に報告する。
		・報告を受けた情報セキュリティ専門部会長（CSIRT責任者）は、CISOへの報告を行う。 なお、影響度がレベル2又は1の場合は、学内で必要な措置及び報告を行い、必要に応じて再発防止策を検討の上、対策を講じる。
		・情報セキュリティインシデントの判定報告を受けたCISOは、情報統合管理会議を招集し、CSIRTの発動を指示する。
	【統一的窓口の役割】	統一的窓口は、保全、調査、検査・分析作業がスムーズに行われるように、外部委託事業者と外部の専門家（セキュリティベンダー等）の間で必要な調整を行う。 また、「サイバー攻撃」が疑われる場合の検査・分析では、サイバー攻撃の証跡のみならず、情報漏えいを示す情報の有無も含めてできうる限り詳細に実施する。
物理的インシデント	1　検査・分析	・ハードウェア又はソフトウェアが停止している場合には、システム停止の日時及び停止に至るプロセスの異常の有無をログ情報により確認する。
		・ネットワークの経路上にあるネットワーク機器及びサブシステムやミドルウェアの稼働状況も併せて確認する。
		・ネットワークを構成する経路上の全ての構成要素が正常に稼働している場合には、稼働の不具合の原因となる情報をシステムから提供されるログから確認する。
		・統一的窓口は、保全、調査、検査・分析作業がスムーズに行われるように、外部委託事業者と外部の専門家（セキュリティベンダー等）の間で必要な調整を行う。
	2　検査・分析結果の報告	・当該部署の情報セキュリティ専門部会員及び統一的窓口は、インシデント予兆等の検査・分析結果及び影響度判定結果について、情報セキュリティインシデント報告書（様式1）に、報告時点までに判明している事項を記載し、情報セキュリティ専門部会長に報告する。
		・報告を受けた情報セキュリティ専門部会長は、影響度判定の結果、当該事案がレベル3に該当すると判断された場合、情報セキュリティ専門部会長（CSIRT責任者）に報告する。
		・報告を受けた情報セキュリティ専門部会長（CSIRT責任者）は、CISOへの報告を行う。 なお、影響度がレベル2又は1の場合は、学内で必要な措置及び報告を行い、必要に応じて再発防止策を検討の上、対策を講じる。
		・情報セキュリティインシデントの判定報告を受けたCISOは、情報統合管理会議を招集し、CSIRTの発動を指示する。
	【統一的窓口の役割】	統一的窓口は、保全、調査、検査・分析作業がスムーズに行われるように、外部委託事業者と外部の専門家（セキュリティベンダー等）の間で必要な調整を行う。

別表1　情報セキュリティインシデントの種別ごとのトリアージ実施手順（第6章6-32関連）

情報セキュリティインシデント種別	実施事項	実施手順
盗難・紛失インシデント	1　調査・分析	・時期、重要度、経緯、情報の内容、データ量等について、検査・分析する。 ア）発生した時期の特定 イ）データの重要度 ウ）当該記録媒体の所在確認 ※媒体が届けられている場合は、媒体自体が物的な証拠であることに留意し、保全の手配をする。 エ）外部メディアの不正利用 オ）情報機器（PC、携帯端末、DVD、USB等）の置き忘れ、盗難 カ）WEBメール等を利用したデータの不正送信 キ）データのダウンロード ク）個人情報の盗難・紛失か ケ）情報システムへの不正アクセスを可能とする情報か コ）暗号化の有無 サ）データ量など被害の規模
		・学内での発生である場合、必要に応じて監視画像等も調査する。
		・データを記録した媒体の貸出記録なども検査・分析対象とする。
	2　検査・分析結果の報告	・当該部署の情報セキュリティ専門部会員及び統一的窓口は、インシデント予兆等の検査・分析結果及び影響度判定結果について、情報セキュリティインシデント報告書（様式1）に、報告時点までに判明している事項を記載し、情報セキュリティ専門部会長に報告する。
		・報告を受けた情報セキュリティ専門部会長は、影響度判定の結果、当該事案がレベル3に該当すると判断された場合、情報セキュリティ専門部会長（CSIRT責任者）に報告する。
		・報告を受けた情報セキュリティ専門部会長（CSIRT責任者）は、CISOへの報告を行う。 なお、影響度がレベル2又は1の場合は、学内で必要な措置及び報告を行い、必要に応じて再発防止策を検討の上、対策を講じる。
		・情報セキュリティインシデントの判定報告を受けたCISOは、情報統合管理会議を招集し、CSIRTの発動を指示する。
	【統一的窓口の役割】	統一的窓口は、保全、調査、検査・分析作業がスムーズに行われるように、外部委託事業者と外部の専門家（セキュリティベンダー等）の間で必要な調整を行う。
外部（クラウド）サービスインシデント	1　調査・分析	・CSIRT管理者は、クラウド事業者に対し下記事項を速やかに報告するよう要請する。 ア）発生した時期の特定 イ）情報資産の種類、データ量 ウ）個人情報の漏えい・き損か エ）暗号化の有無 オ）データ量など被害の規模
		・情報セキュリティ専門部会長（CSIRT責任者）は、クラウド事業者からの情報と学内で保有する情報からインシデントの影響度を分析する。 ア）インシデント対象のデータの重要度、暗号化有無 イ）関係部署と連携し漏えい・き損による影響範囲を特定する。
		・CISOは、必要に応じて学生への対応等について指示を行う。
	2　検査・分析結果の報告	・当該部署の情報セキュリティ専門部会員及び統一的窓口は、インシデント予兆等の検査・分析結果及び影響度判定結果について、情報セキュリティインシデント報告書（様式1）に、報告時点までに判明している事項を記載し、情報セキュリティ専門部会長に報告する。
		・報告を受けた情報セキュリティ専門部会長は、影響度判定の結果、当該事案がレベル3に該当すると判断された場合、情報セキュリティ専門部会長（CSIRT責任者）に報告する。
		・報告を受けた情報セキュリティ専門部会長（CSIRT責任者）は、CISOへの報告を行う。 なお、影響度がレベル2又は1の場合は、学内で必要な措置及び報告を行い、必要に応じて再発防止策を検討の上、対策を講じる。
		・情報セキュリティインシデントの判定報告を受けたCISOは、情報統合管理会議を招集し、CSIRTの発動を指示する。
	【統一的窓口の役割】	統一的窓口は、保全、調査、検査・分析作業がスムーズに行われるように、外部委託事業者と外部の専門家（セキュリティベンダー等）の間で必要な調整を行う。

別表2　情報セキュリティインシデントの種別ごとの影響度判定基準（第6章6-32関連）

情報セキュリティインシデント種別	影響度	判定基準	事案（例）
ネットワーク系インシデント	レベル 3	情報セキュリティインシデントが学生や大学運営に重大な影響を与える場合	ネットワーク接続の情報機器にウイルス感染し、広範な情報機器に感染又は感染のおそれがある場合
			長期間にわたりシステム又はネットワークを停止する必要がある場合
			個人情報、研究情報の漏えいの可能性がある場合　等
	レベル 2	情報セキュリティインシデントの影響が一部に限定されている場合	ネットワーク接続している端末にウイルス感染したが他のシステム、端末に影響していないもの
			CD、DVD、USB等の記録媒体を介して、ウイルス感染が限定的に拡大するおそれがある場合　等
	レベル 1	情報セキュリティインシデントの影響が軽微な場合	スタンドアロンで利用している端末へのウイルス感染
			記録媒体内のウイルス感染
物理的インシデント	レベル 3	情報セキュリティインシデントが学生や大学運営に重大な影響を与える場合	基幹ネットワークの重大な障害
			サーバ、ネットワーク等の障害で、他の情報資産に影響を及ぼす可能性のある重大な障害
			長期間に渡りシステム又はネットワークを停止する必要がある重大な障害
			広範にわたる停電
			全建屋又は地域的に長時間の停電
	レベル 2	情報セキュリティインシデントの影響が一部に限定されている場合	一部部署のネットワーク機器の障害
			サーバ、ネットワーク、端末機等の障害で、他の情報資産に影響を及ぼすことがない一時的な障害
			フロア又は建物全体の電源障害
			一部の電源系統の障害　等
	レベル 1	情報セキュリティインシデントの影響が軽微な場合	端末機の障害
			システムの一時的な障害
			ネットワーク障害で、通信回線業者側の一時的な障害
			機器の電源障害

別表2　情報セキュリティインシデントの種別ごとの影響度判定基準（第6章6-32関連）

情報セキュリティインシデント種別	影響度	判定基準	事案（例）
			コンセントの接続ミス
			ブレーカ遮断　等

別表2　情報セキュリティインシデントの種別ごとの影響度判定基準（第6章6-32関連）

情報セキュリティインシデント種別	影響度	判定基準	事案（例）
盗難・紛失インシデント	レベル 3	情報セキュリティインシデントが学生や大学運営に重大な影響を与える場合	暗号化等がされていない個人情報、研究情報を保管している情報機器又は記録媒体の盗難、紛失
			広範なシステム又はネットワークの稼動に影響がある機器の盗難、紛失
			重要なシステム又はネットワークの設計書等の漏えい
	レベル 2	情報セキュリティインシデントの影響が一部に限定されている場合	暗号化等がされている情報機器又は記録媒体の盗難、紛失
			一部のシステム又はネットワークの稼動に影響がある機器の盗難、紛失
	レベル 1	情報セキュリティインシデントの影響が軽微な場合	情報を保管していない情報機器又は記録媒体の盗難、紛失
			システム又はネットワークの稼動に影響が軽微な機器の盗難、紛失
			重要でない情報であるが知る必要のない教職員等がアクセスできる状況が判明
			重要でない情報を含んだ記録媒体の持ち出し
			重要でない情報を含んだ記録媒体の持ち出し
外部（クラウド）サービスインシデント	レベル 3	情報セキュリティインシデントが学生や大学運営に重大な影響を与える場合	暗号化等がされていない研究情報の漏えい・き損
			特定個人情報、要配慮個人情報の漏えい・き損
			暗号化等がされていない特定個人情報、要配慮個人情報以外の個人情報の漏えい・き損
	レベル 2	情報セキュリティインシデントの影響が一部に限定されている場合	暗号化等がされている研究情報の漏えい・き損
			暗号化等がされている特定個人情報、要配慮個人情報以外の個人情報の漏えい・き損の漏えい
	レベル 1	情報セキュリティインシデントの影響が軽微な場合	個人情報、研究情報以外の重要性が低い情報の漏えい・き損
			インシデントからの復旧が直ちに行われる場合
			インシデントからの復旧が直ちに行われる場合

別表3　情報の格付け区分の具体例（第9章第1節9-2、9-3、9-4関連）

機密性

格付けの区分	区分の基準	具体例
機密性3情報	本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年4月1日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報	(・全学的に影響のある情報） ・学生の成績 ・学位記 ・役職員及び学生の個人番号及び特定個人情報 ・学生の健康情報（ドック、健康診断の結果等） ・実施前の入学試験問題 ・入学試験業務用資料 ・入開札実施前の予定価額 ・本学の経営情報のうち、学長が関係者外秘に指定した情報
機密性2B情報	本学で取り扱う機密性3以外の情報のうち、独立行政法人の保有する情報の公開に関する法律（平成13年12月5日法律第140号。以下、「独立行政法人等情報公開法」という。）第5条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、その漏えいにより本学の情報資産を利用する者のうち、学内外を含む多数の者の権利が侵害され、又は本学の活動の遂行に支障を及ぼすおそれがある情報	・学生及び教職員名簿 ・非公開の研究情報 ・営業秘密やそれに係る技術情報 ・人事、給与、共済組合関係記録情報 ・本学のネットワーク、情報システムの構成等に関する情報 ・情報セキュリティ監査結果報告書 ・関係省庁への報告
機密性2A情報	本学で取り扱う機密性3以外の情報のうち、独立行政法人等情報公開法第5条各号における不開示情報に該当すると判断される蓋然性が高い情報を含む情報であって、その漏えいにより本学の情報資産を利用する者のうち、特に学内の役職員等や学生の権利が侵害され、又は役職員等の活動の遂行に支障を及ぼすおそれがある情報	・非公開の会議において知り得た情報 ・勉強会、研修会資料 ・財務会計システムにおいて発行可能な伝票等 ・公開前会議資料 ・公式ホームページ内の学内限定ページ掲載資料 ・事務局からのお知らせ及び事務に係るもの ・情報セキュリティ管理運用の取扱い ・法人文書ファイル管理簿に係る業務に関する情報
機密性1情報	機密性3情報、機密性2B情報又は機密性2A情報以外の情報	・大学戦略課、総務課、入試課等から発表される報道機関向け情報 ・研究室等から一般に告知される情報 ・公式ホームページ掲載資料（機密性2A情報を除く） ・学生・保護者向け情報

完全性

格付けの区分	区分の基準	具体例
完全性2情報	本学で取扱う情報（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	・学生の成績 ・実施前の入学試験問題 ・人事・給与・共済組合関係記録情報
完全性1情報	完全性2情報以外の情報（書面を除く。）	・公式ホームページ掲載資料（入学試験情報等）

可用性

格付けの区分	区分の基準	具体例
可用性2情報	本学で取扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。	・学生の成績 ・実施前の入学試験問題 ・人事・給与・共済組合関係記録情報
可用性1情報	可用性2情報以外の情報（書面を除く。）	・電子メール、グループウェア等の情報システム及び当該システムで取扱う情報

■個人情報データベース等

「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。

一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

別表4　情報の格付け区分に応じた取扱方法の具体例（第9章第2節9-5関係）

凡例　○：必ず行う　△：必要に応じて行う　空欄：行う必要なし

情報の取扱の種類	取扱方法例	機密性の格付け				完全性の格付け		可用性の格付け	
		機密性3	機密性2B	機密性2A	機密性1	完全性2	完全性1	可用性2	可用性1
表示	格付け区分の表示	○	○	△		○			
	保存・保管期間の表示	○	○	△					
	保存・保管場所の表示	○	○	△	△				
	表示色（黒色以外）	○	△						
	格付け区分有効期限の表示	○	○						
保存・保管	保存・保管期間の設定	○	○	△		○		○	
	保存・保管場所の設定	○	○	△	△	○			
	保存・保管場所の施錠	○	○	△		○			
	電子ファイルの暗号化による保存・保管	○	△	△		○			
アクセス	アクセス権限者の決定・設定	○	○	○		○			
	アクセス権限者のリスト作成・保管	○	○	○		△			
	アクセス権限者の可用性確認								
	アクセス制限範囲（※業務等で情報を取り扱う者のみ）	○	○	△		○			
	アクセス制限範囲（※学内者のみ）	○	○	○		○			
	アクセス権限・制限範囲の変更確認	○	○	○		△			
	アクセス権限・制限範囲の誤謬・改ざん確認	○	○	○		○			
	アクセス許可手続き	○	○			△			
	アクセス記録の作成・管理	○	△	△	△	△			
情報変更	情報管理責任者による情報変更	○	○	○	○	○		○	
	情報管理責任者から管理権限を委任または継承した者による情報変更	○	○	○	○	○		○	
情報削除	情報管理責任者による情報削除	○	○	○	○	○		○	
	情報管理責任者から管理権限を委任または継承した者による情報削除	○	○	○	○	○		○	
複製・複写	複製・複写禁止	○	△			△			
	印刷禁止	△	△			△			
持ち出し	持ち出し禁止	○	△			△			
	持ち出し記録	○				△			
配布・通信・メール送信	情報管理責任者による配布・通信・メール送信の許可	○	○						
	手渡しの徹底	○	△						
	文書の郵送禁止	○	△						
	文書のFAX送信禁止	○	△						
	電子ファイルのネットワーク通信禁止	○	△						
	電子ファイル暗号化による配布・通信・メール送信	○	△	△					
	配布・通信・メール送信記録の作成・管理	○	○			△			
廃棄処分	シュレッダーまたはメディアシュレッダーによる廃棄処分	○	○			△			
	廃棄処分の委託禁止	○	△						
	配布先における廃棄処分	○	△						
情報開示	情報管理責任者による情報開示許可	○	○	○		△		○	
	機密保持契約の締結	○	○	△		△			
復旧期限	復旧までに許容できる期限の設定					○		○	
格付け区分変更	情報管理責任者による格付け区分変更	○	○	○	○	○		○	

別表4　情報の格付け区分に応じた取扱方法の具体例（第9章第2節9-5関係）

凡例　○：必ず行う　△：必要に応じて行う　空欄：行う必要なし

情報の取扱の種類	取扱方法例	機密性の格付け				完全性の格付け		可用性の格付け	
		機密性3	機密性2B	機密性2A	機密性1	完全性2	完全性1	可用性2	可用性1
	情報管理責任者から管理権限を委任または継承した者による格付け区分変更	○	○	○	○	○		○	
記憶	守秘義務（離職後も含む）の徹底	○	○	○		△			

付録1　用語の定義

基本方針、基本規程及び運用の取扱いにおいて、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

項番	用語	定義
1	ハードウェア	機器（通信回線装置、サーバ装置、端末）の総称。機器本体、キーボードやマウス、スキャナー等の入力装置、ハードディスク等の記憶装置、ディスプレー等の出力装置等で構成される。ハードウェアはソフトウェアによって制御される。
2	通信回線	複数の情報システム又は情報システムの構成要素である機器（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。
3	通信回線装置	通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。
4	サーバ装置	情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む）で、原則として本学が調達又は開発するものをいい、通信回線及び通信回線装置を介して学内LANに接続されるものとする。
5	端末	情報システムの構成要素である機器のうち、本学の情報及び情報システムを利用する者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む）で、本学が調達又は開発するもの及び学内ネットワークに接続する本学支給以外のものをいう。
6	学内LAN	複数の情報システム又は情報システムの構成要素である機器の間で所定の方式に従って情報通信を行うための仕組みのうち、本学の情報システム又は情報システムの構成要素である機器において利用され、かつ、総合情報センターネットワークインフラ部門により通信回線が管理されているもので、原則として有線又は無線接続が可能なものをいう。
7	ソフトウェア	サーバ装置及び端末を動作させる手順及び命令をサーバ装置及び端末が理解できる形式で記述したものをいい、オペレーティングシステム（Windows、macOS等）、オペレーティングシステム上で動作するアプリケーション（ウェブブラウザ、メールソフトウェア、ソーシャルメディアサービス、クラウドサービス、Microsoft Office等）を含む。
8	クラウドサービス	ソフトウェア又はハードウェアのうち、共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセス可能なウェブサービスとして事業者によって提供され、本学の情報及び情報システムを利用する者によって自由にリソースの設定及び管理が可能であって、かつ、情報セキュリティに関する必要な設定ができるものをいう。
9	情報システム	非電子化情報を含むすべての情報の処理、蓄積及び通信を行うハードウェア並びにこれに用いられるソフトウェアであって、本学の教育、研究及び事務処理に使用するもので、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。
10	外部委託	本学の情報処理業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。
11	情報機器	情報システムの構成要素の総称をいう。
12	情報資産	情報及び情報システムをいう。
13	記録媒体	情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（書面）と、電子的方式、磁気的方式そのほか人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（電磁的記録）に係る記録媒体（電磁的記録媒体）がある。なお、電磁的記録媒体には、次に掲げるものがある。 ア　情報機器や端末に内蔵されるもの（内蔵電磁的記録媒体） イ　情報機器や端末の外部に接続することによって情報の記録又は記載が可能な記録媒体（USBメモリ、外付けハードディスクドライブ、DVD-R等）（外部電磁的記録媒体）
14	組織責任者	系長、センター長及び共同研究等の事業におけるプロジェクトの長、事務局における事務局長、事務局次長、課長、室長並びに技術長をいう。
15	役職員等	本学の役員のほか、本学に勤務する教員、事務職員、技術職員（いずれも非常勤を含む。）その他本学の業務に従事し、組織責任者が認めた者をいう。

項番	用語	定義
16	学生	本学学則に定める学部学生、大学院学生、研究生、聴講生、科目等履修生、外国人留学生等をいう。
17	アクセス	情報を使用すること（閲覧を含む。）及び情報の利用手段を使用することをいう。
18	アクセス権限	アクセスできる権限をいう。
19	アクセス権限者	アクセス権限を有する者をいう。
20	機密性	アクセスを許可されていない者が情報にアクセスできないことをいう。
21	完全性	情報が正確であり、かつ不備がないことをいう。
22	可用性	必要な場合、確実に情報にアクセスできることをいう。
23	情報セキュリティ	情報の機密性、完全性、可用性を維持すること。
24	情報セキュリティ管理	情報資産の環境を適切に管理することにより、情報セキュリティの維持・改善・向上を図ることをいう。
25	情報セキュリティインシデント	本学の情報資産に対する望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。
26	CISO（シーアイエスオー）	本学の情報セキュリティに関する事務を統括する最高情報セキュリティ責任者をいう。Chief Information Security Officerの略。
27	要管理対策区域	本学の管理下にある区域（学外組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。
28	CSIRT（シーサート）	本学において発生した情報セキュリティインシデントに対応するため、本学に設置された体制をいう。Computer Security Incident Response Teamの略。
29	要管理対策区域	本学の管理下にある区域（学外組織から借用している施設等における区域を含む。）であって、取扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。
30	主体認証	識別コードを提示した主体（情報システムの利用者等）が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。なお、主体認証情報とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報としてパスワード等がある。
31	識別コード	主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとしてユーザID があげられる。なお、識別とは、情報システムにアクセスする主体を当該情報システムにおいて特定することをいう。
32	モバイル端末	端末のうち、必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

付録2 主な関連法令（第3章関係）

（1）特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成13年法律第137号：通称プロバイダ責任制限法）

この法律は、インターネット上における情報の流通によって権利の侵害があった場合、プロバイダ等の損害賠償責任の制限及び発信者情報の開示を請求する権利を定めたものである。ここでいうプロバイダには、大学等の機関も含まれる。

次に例示するような場合は、不作為の責任を負うことがあるので注意すること。

- 他人の権利を侵害する情報が流通していることを現実に認識していた場合
- 私人のプライバシー情報（住所、電話番号等）、公共の利害に関する事実でないこと及び公益目的でないことが明らかであるような誹謗中傷を内容とする情報等の流通を認識できたと認められる場合
- 他人を誹謗中傷する情報について、その流通径路が分からないまま権利侵害に該当するか否かについての連絡があったが、その裏付けが取れないまま侵害行為が行われている場合

【罰則】 3年以下の懲役若しくは禁錮又は50万円以下の罰金（刑法における名誉毀損罪の適用）

（2）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：通称不正アクセス禁止法）

この法律は、不正アクセス行為等を禁止し、ネットワークを通じて行われるコンピューター犯罪の防止とアクセス制御機能により実現される電気通信に関する秩序を維持するものである。

アクセス制御機能による利用制限を免れて特定電子計算機を特定利用できる状態にする次に例示するような行為を禁止する。

- 他人のID、パスワードを無断で入力する行為
- ID、パスワード以外の情報・指令を入力する行為
- 特殊な情報・指令を入力して、本来はID、パスワードを入力しなければ行うことができないことが、それなしに行うことができる状態にする行為
- 他人のID、パスワードをどの特定電子計算機に対してであるかを明らかにすること、又はこれを知っている者の求めに応じて、アクセス管理者や利用権者に無断で第三者に提供する助長行為

【罰則】 1年以下の懲役又は50万円以下の罰金

（3）不正競争防止法（平成5年法律第47号）

この法律は、公正な競争とこれに関する約束の的確な実施を確保するため、不正競争の防止と不正競争にかかわる損害賠償に関する措置を規定し、次に例示するような不正競争について規制している。

- 窃取、詐欺、強迫その他の不正な手段により営業秘密（秘密として管理されており、事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの）を取得する行為及び不正取得行為により取得した営業秘密を使用・開示する行為
- 不正取得行為の有無にかかわらず、営業秘密を取得する行為又はその取得した営業秘密を使用・開示する行為
- 営業秘密の保有者から営業秘密を示された場合、不正の競業その他の不正の利益を得る目的又はその保有者に損害を加える目的で、その営業秘密を使用・開示する行為
- 営業秘密について不正開示行為が介在したことを知っていたか否かにかかわらず営業秘密を取得する行為又はその取得した営業秘密を使用・開示する行為

【罰則】 10年以下の懲役若しくは3億円以下の罰金

（4）個人情報の保護に関する法律（平成15号：通称個人情報保護法）

個人情報の適正な取り扱いに関し基本となる事項を定め、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人の権利利益を保護する。大学も個人情報取扱事業者に当たる。個人情報の取り扱いについて次に例示するような義務を課している。

- 個人情報を取り扱うに当たり、その利用の目的をできる限り特定する
- 偽り等の不正の手段により個人情報を取得しない
- 法令に基づく場合等を除き、あらかじめ本人の同意を得ないで、第三者に提供してはならない
- 個人情報の取り扱いに関する苦情に対して、適切で迅速な対応をする
- 個人情報を利用する場合は、特定した利用目的を超えてはならず、超える場合（利用目的の変更・追加をする場合）は、原則としてあらかじめ本人から同意を得る

【罰則】　行為者：1年以下の懲役又は50万円以下の罰金
法人等：1億円以下の罰金

【参考】

個人情報とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

二　個人識別符号（※）が含まれるもの

※次のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。

- 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの
- 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

（5）特定電子メールの送信の適正化等に関する法律（平成14年法律第26号：通称迷惑メール防止法）

一時に多数の者に対してされる特定電子メールの送信等による電子メールの送受信上の支障を防止する必要性が生じたため、送信の適正化のための措置等が定められ、次に例示するような行為が禁止されている。

- 相手の承諾がないまま「一度でも」宣伝用メールを送信する行為
- 送信拒否の通知をした者に対して、再び特定電子メールを送信する行為
- 架空電子メールアドレスをそのあて先とする電子メールの送信行為
- 送信者情報を偽り送信する行為

【罰則】 1年以下の懲役若しくは3,000万円以下の罰金、又はこれの併科

（6）著作権法（昭和45年法律第48号）

思想・感情を創作的に表現したものであって、文芸・学術・美術・音楽の範囲に属する文化的な創作物を保護の対象とする法律である。次に例示するような行為は、著作権者の承諾・補償金の支払が必要となる。

- 著作物をデジタル方式の機器等を使い複製する行為（私的複製も含む）

・ コピープロテクション等技術的保護手段の回避装置を使い、複製する行為（私的複製も含む）
・ 営利を目的とした著作物の複製（非営利でも著作権者の了解が必要）
・ 授業を除いて、学内の資料として、新聞・雑誌の記事等を複写して配布する行為
・ ホームページ等へアニメキャラクターを掲載する行為
・ PCソフトメーカー（著作権者）の了解がない（海賊版）ソフトウェアの使用
・ いわゆる「ファイル交換ソフト」を使って、著作権者の了解なしに複製・送信する行為
・ 著作権者の了解がないまま、音楽ＣＤ等をネットワーク上で再生できる状態にする行為

【罰則】 10年以下の懲役若しくは1,000万円以下の罰金、又はこれの併科

（7）サイバーセキュリティ基本法（平成26年法律第104号）

ネットワークや情報通信技術等の進展に伴い世界的規模で生じているサイバーセキュリティに対する脅威の深刻化等に伴い、サイバーセキュリティに関する施策等を定めた法律である。次に例示するような行為が禁止されている。

・ サイバーセキュリティに関する対策の基準に基づく監査に係る事務、又は発生したサイバーセキュリティに関する重大な事象の原因究明のための調査に係る事務の委託を受けた職員等が、正当な理由がなく、当該委託に係る事務に関して知り得た秘密を漏らし、又は盗用する行為

【罰則】 1年以下の懲役又は50万円以下の罰金

付録3　今すぐできる情報セキュリティ対策

○機密性が高い（機密性3、2B、2A）ファイル

- パスワードを設定する。例えば、Word/EXCELのパスワード機能を使う。
- パスワードを使い分ける。
- 暗号化する。
- 学外に持ち出さない。

○PCの取り扱い

- ログインパスワードを設定するとともに、部屋は施錠してから離れる。
- 離席中に不正に操作されないように画面ロック設定を適用する。
- ファイル交換ソフトは導入しない。
  ■ ファイル交換ソフトの例
  Amoeba（アモエバ）， BitTorrent（ビットトレント）， Freenet（フリーネット）， Gnutella（グヌーテラ）
  Perfect Dark（パーフェクトダーク），， Share（シェア）， Winny（ウィニー）， WinMX（ウィンエムエックス） など
- OSやプログラムは最新に保ち、不正プログラム対策のためにセキュリティソフトウェアを導入する。

○個々人の情報の管理責任

- 機密区分・有効期限の設定、適切なアクセス権限の設定並びに使用目的を明確にする。
- 必要とする者にのみ当該情報へのアクセス権限を付与する。
- 許可者のみ、正しい情報を、必要なときにいつでも利用できるように維持管理する。

○不審なメールの見分け方

- 添付ファイルを開く前、または実行する前に不審点を見つけること。
- 送信者のメールアドレスが署名と異なっている。
- 言い回しが不自然である。
- 日本語では使用されない漢字（繁体字、簡体字）やカタカナが使用されている。
- 正式名称を一部に含むような不審なURLまたはURIへのアクセスを指示するものである。
- HTMLメールであり、表示と実際のURLまたはURIが異なるウェブリンクを使用している。
- 署名の記載内容が不自然であり、存在しない部門の名称を使用している。
- ショートカットファイル（.lnk、.pif、.url等）が添付されている。
- 添付されたファイルが実行形式であるが、文書ファイルやフォルダのアイコンを使用している。
- ファイル名が不審である
- 拡張子が二重に表示されている。
  ー ファイル拡張子の前に大量の空白文字が挿入されている。
  ー 文字列が左右反転している。
  ー 圧縮ファイルを実行せずにエクスプローラで表示すると、ファイル名が文字化けしている。

詳細は、下記の資料を参照すること。
IPA J-CRAT標的型攻撃メールの傾向と見分け方 ～サイバーレスキュー隊(J-CRAT)の活動を通して～
https://www.ipa.go.jp/files/000052612.pdf（参照：2018-02-21）