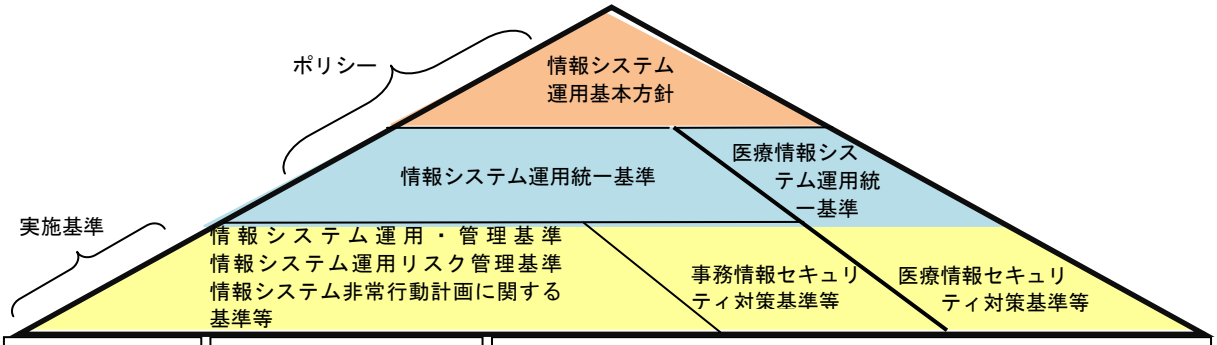
群馬大学情報セキュリティ体系



ポリシー	実施基準	手順ガイドライン等の事例
A1000 **情報システム運用基本方針**	A2101 **情報システム運用・管理基準** A2102 **情報システム運用リスク管理基準** A2103 **情報システム非常時行動計画に関する基準** A2104 **情報格付け基準**	A3100 **情報システム運用・管理手順に関する解説書** A3101 **情報システムにおけるセキュリティ対策実施手順** A3102 **例外措置手順** A3103 **インシデント対応手順** A3104 **情報格付け取扱手順** A3105 **情報システム運用リスク評価手順** 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 **電子メールサービス提供ソフトウェアのセキュリティ維持手順** 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** 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** 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**
A1001 **情報システム運用統一基準**	A2201 **情報システム利用基準**	A3200 **情報システム利用者向け文書に関する解説書** 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**
A1002 **医療情報システム運用統一基準**	A2301 **年度講習計画**	A3300 **教育テキストの策定に関する解説書** A3301 **教育テキスト作成ガイドライン（一般利用者向け）**
	A2401 **情報セキュリティ監査基準**	A3401 **情報セキュリティ監査実施手順**
	A2501 **事務情報セキュリティ対策基準等**	A3500 **各種マニュアル類の策定に関する解説書** A3501 **事務情報セキュリティポリシー実施手順書**
	A2601 証明書ポリシー A2602 認証実施規程	A3600 **認証手順の策定に関する解説書** A3601 **全学認証アカウント取得手順**
	A2901 医療情報セキュリティ対策基準等	A3901 医療情報セキュリティ関係各種マニュアル類の策定

国立大学法人群馬大学情報セキュリティポリシー

平成 20 年　9 月 18 日制定
平成 20 年 12 月 19 日改正

国立大学法人群馬大学情報システム運用基本方針

１　情報システムの目的

国立大学法人群馬大学（以下「本学」という。）情報システムは、本学の基本理念すなわち「意欲的・創造的で、国際的視野を持った人材の育成、最先端の創造的学術研究の推進、大学構成員の自主性・自律性の尊重、大学自治の確立、開かれた大学への改革」を実現するために、本学のすべての教育・研究活動及び運営の基盤として設置され、運用されるものである。

２　運用の基本方針

前項の目的を達するため、本学情報システムは、円滑で効果的な情報流通を図るために、別に定める運用統一基準により、優れた秩序と安全性をもって安定的かつ効率的に運用される。

なお、運用統一基準は「国立大学法人群馬大学情報システム運用統一基準」及び「国立大学法人群馬大学医療情報システム運用統一基準」からなる。

３　利用者の義務

本学情報システムを利用する者や運用の業務に携わる者は､本方針及び運用統一基準に沿って利用し、別に定める運用と利用に関する実施基準を遵守しなければならない。

４　罰則

本方針に基づく基準等に違反した場合の利用の制限及び罰則は、それぞれの基準に定めることができる。

A1001

国立大学法人群馬大学情報システム運用統一基準

平成 20 年　9 月 18 日制定
平成 20 年 12 月 19 日改正
平成 22 年　3 月 19 日改正

１　宣言

本統一基準は、国立大学法人群馬大学（以下「本学」という。）における医療情報システムを除く情報システムの運用について定める。

なお、医療情報システムについては、別に規定する A1002「国立大学法人群馬大学医療情報システム運用統一基準」に定める。

２　適用範囲

本統一基準は、本学情報システムを運用・管理及び利用するすべての者に適用する。

３　定義

本統一基準において、次の各項に掲げる用語は、それぞれ当該各号の定めるところによる。

３―１　情報システム

情報処理及び情報ネットワークに係わるシステムで、次のものをいい、本学情報ネットワークに接続する機器を含む。

（１）本学により、所有又は管理されているもの
（２）本学との契約あるいは他の協定に従って提供されるもの

３―２　情報ネットワーク

情報ネットワークには次のものを含む。

（１）本学により、所有又は管理されている全ての情報ネットワーク
（２）本学との契約あるいは他の協定に従って提供される全ての情報ネットワーク

３―３　情報

情報には次のものを含む。

（１）情報システム内部に記録された情報
（２）情報システム外部の電磁的記録媒体に記録された情報

（３）情報システムに関係がある書面に記載された情報

３―４　事務情報システム

本学情報システムのうち、事務処理に供され、事務局が運用責任を持つ情報システムをいう。但し、学務関係事務（教務関係事務、入試関係事務を含む。）は本文でいう事務処理には含まれない。

３―５　ポリシー

本学が定めるA1000「国立大学法人群馬大学情報システム運用基本方針」及びA1001「国立大学法人群馬大学情報システム運用統一基準」をいう。

３―６　実施基準

ポリシーに基づいて策定される基準及び計画をいう。

３―７　手順等

実施基準に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。

３―８　利用者

教職員、学生等で、利用許可を受けて本学情報システムを利用するものをいう。

３―９　教職員等

本学に勤務する常勤又は非常勤の教職員（派遣職員を含む。）その他部局（部門）情報化推進責任者又は全学総括責任者が認めた者をいう。

３―１０　学生等

本学学則及び大学院学則に定める学部学生、大学院学生、特別研究学生、特別聴講学生、科目等履修生、研究生、聴講生及び外国人留学生その他部局（部門）情報化推進責任者が認めた者をいう。

３―１１　臨時利用者

教職員、学生等以外の者で、臨時に利用許可を受けて本学情報システムを利用するものをいう。

３―１２　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

３―１３　電磁的記録

電子的方式､磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

３―１４　インシデント

情報セキュリティに関し、意図的又は偶発的に生じる、法令又は本学規程に反する事故あるいは事件をいう。

３―１５　明示等

情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。

３―１６　部局

本統一基準では次の組織を単独の部局とみなす。

・教育学部
・社会情報学部
・医学系研究科・医学部
・医学部附属病院
・工学研究科・工学部
・生体調節研究所
・総合情報メディアセンター
・大学教育・学生支援機構
・国際教育・研究センター
・重粒子線医学推進機構
・研究・産学連携戦略推進機構
・事務局

３―１７　部門

事務局・事務部のうち、学務事務（教務事務、入試関係事務を含む。）を扱う部署とそれ以外の部署はそれぞれ独立した部門として別に扱う｡部門は原則として部局に準じて扱う。

３―１８　地区

本統一基準においては、荒牧地区、昭和地区、桐生・太田地区を、それぞれ地区と呼ぶ。また、事務局・事務部（学務事務を除く。）と学務事務は部門として地区に準じて扱う。

４　全学総括責任者

本学情報システムの運用に責任を持つ者として、本学に全学総括責任者を置く。情報化統括責任者（ＣＩＯ）が全学総括責任者となる。

４―１　全学総括責任者は、ポリシー及びそれに基づく基準並びに手順等の決定や情報システム上での各種問題に対する最終責任を負う。

４―２　全学総括責任者は、全学向け教育及び管理運営部局の部局技術担当補佐向け教育を統括する。

４―３　全学総括責任者に事故あるときは、全学総括責任者があらかじめ指名した者が、その職務を代行する。

４―４　全学総括責任者は、原則として、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置く。

５　情報化推進室

本学情報システムの円滑な運用のための最終決定機関は情報化推進室とする。

５―１　情報化推進室は情報化推進室規程第２条に基づき、以下を実施する。

（１）ポリシー及び全学向け教育の実施ガイドラインの改廃
（２）情報システムの運用と利用、教育に係る規程、手順の制定及び改廃
（３）情報システムの運用と利用に関する教育の年度計画の制定及び改廃並びにその計画の実施状況の把握
（４）情報システム運用リスク管理基準の制定及び改廃並びにその実施状況の把握
（５）情報セキュリティ監査基準の制定及び改廃並びにその実施
（６）情報システム非常時行動計画の制定及び改廃並びにその実施
（７）インシデントの再発防止策の検討及び実施

５―２　情報化推進室は、地区情報システム運用委員会に対して、次の各項につき調査・検討を指示する。

（１）参加部局（部門）におけるポリシーの遵守状況
（２）参加部局（部門）におけるリスク管理、非常時行動計画の策定及び実施状況
（３）参加部局（部門）におけるインシデントの再発防止策の策定及び実施状況
（４）参加部局（部門）における技術担当補佐向け教育の計画と企画

５―３　情報化推進室は、５―２項の指示に対する地区情報システム運用委員会からの答申につき審議し、必要事項の実施を部局情報化推進責任者に対して命令する。

６　全学実施責任者

本学に全学実施責任者を置く。

６―１　全学実施責任者は、全学総括責任者の指示により、本学情報システムの整備と運用に関し、ポリシー及びそれに基づく基準並びに手順等の実施を行う。

６―２　全学実施責任者は、情報システムの運用に携わる者及び利用者に対して、情報システムの運用及び利用並びに情報システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく基準並びに手順等の遵守を確実にするための教育を実施する。

６―３　全学実施責任者は、本学の情報システムのセキュリティに関する連絡及び通報において本学情報システムを代表する。

６―４　全学実施責任者は、すべての部局（部門）技術担当者、部局（部門）技術担当補佐及び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。

６―５　全学実施責任者は、情報化推進室の室員の中から、全学総括責任者が任命する。なお、全学実施責任者は、地区情報システム運用委員会の委員長を兼務することができる。

７　情報セキュリティ監査責任者

全学総括責任者は、情報セキュリティ監査責任者を置く。

７―１　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。

８　管理運営部局

本学情報システムの管理運営部局は、本学の基幹ネットワークの管理運営、基幹ネットワークと外部ネットワークとの接続管理及び基幹ネットワークと部局ネットワークの接続管理を行う。

８―１　総合情報メディアセンターが管理運営部局となる。

９　管理運営部局の事務

管理運営部局の事務は事務局研究推進部総合情報メディアセンター課が所掌し、以下の各号に定める事務を行う。

（１）本学情報システムの運用及び利用におけるポリシーの実施状況の取りまとめ

（２）講習計画、リスク管理、非常時行動計画等の実施状況の取りまとめ

（３）本学の情報システムのセキュリティに関する連絡及び通報

１０　部局（部門）情報化推進責任者

各部局に情報化推進責任者を置く。部局長を部局の情報化推進責任者とする。

部局情報化推進責任者は、部局における運用方針の決定や情報システム上での各種問題に対する処置につき責任を持つ。部局情報化推進責任者が部局情報システム運用委員会の委員長を兼任することは妨げない。ただし、部門の情報システムにおいて部局のその他のシステムと異なった扱いをするときは、全学総括責任者は、当該部門情報システムに関して、部門情報化推進責任者を選任する。部門情報化推進責任者は、部局情報化推進責任者（部局長）に準じて扱う。部門情報化推進責任者は、部門情報システム運用委員会の委員長を兼任することができる。

１０―１　部局（部門）情報化推進責任者は、全学総括責任者の指示により、部局（部門）情報システムの整備と運用に関し、ポリシー及びそれに基づく基準並びに手順等の実施を行う。

１０―２　部局（部門）情報化推進責任者は、部局（部門）情報システムの運用に携わる者及び利用者に対して、情報システムの運用及び利用並びに情報システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく基準並びに手順等の遵守を確実にするための教育を実施する。

１１　部局（部門）情報化推進担当者

各部局に部局情報化推進担当者を置く。部局情報化推進担当者は、全学総括責任者が選任する。

１１―１　部局情報化推進担当者は、部局における運用方針の決定や情報システム上での各種問題に対する処置に関して部局情報化推進責任者を補佐する。

１１―２　部門の情報システムにおいて部局のその他のシステムと異なった扱いをするときは、全学統括責任者は、当該部門情報システムに関して、部門情報化推進担当者を選任する。

なお、部門情報化推進担当者は原則として部局情報化推進担当者に準じて扱う。

１２　地区（部門）情報システム運用委員会

全学総括責任者は、部局、部門等に対して、地区（部門）情報システム運用委員会の設置を指示する。各地区（部門）情報システム運用委員会を構成する部局、部門は全学総括責任者が決定する。

なお、単独部局で情報システム運用委員会を設置するときは、原則として地区（部門）情報システム運用委員会の規定を準用し、部局情報システム運用委員会の委員長は地区（部門）情報システム運用委員会の委員長に準じて扱う。

１２―１　地区（部門）情報システム運用委員会は以下の各号に掲げる事項につき調査検討し、検討結果を情報化推進室に答申する。

（１）参加部局（部門）におけるポリシーの遵守状況
（２）参加部局（部門）におけるリスク管理、非常時行動計画の策定及び実施状況
（３）参加部局（部門）におけるインシデントの再発防止策の策定及び実施状況
（４）参加部局（部門）における技術担当補佐向け教育の計画と企画

１２―２　複数部局で特定の情報システムを共有する場合は、関係部局の合意により管理責任者を選任する。管理責任者は部局（部門）情報化推進担当者に準じて扱う。管理責任者は必要があれば、技術担当者と技術担当補佐を選任することができる。当該技術担当者、技術担当補佐は、それぞれ部局技術担当者及び部局技術担当補佐に準じて扱う。

１２―３　管理運営部局は、単独で部局情報システム運用委員会を設置する。管理運営部局が他部局のネットワーク及び情報システムを運営するときは、管理運営部局が当該ネットワーク及び情報システムにつき、管理責任部局となる。

１２―４　事務局・事務部は、学務事務（教務事務、入試関係事務を含む。）を除いた事務に関して、事務情報システム運用委員会を設置する。

１２―５　学務事務部門は、学務事務（教務事務、入試関係事務を含む。）に関して他の部門とは別に学務事務情報システム運用委員会を設置する。

１３　地区（部門）情報システム運用委員会の構成員

地区（部門）情報システム運用委員会は、委員長及び次の各項に掲げる者を委員として組織する。

（１）部局（部門）情報化推進担当者

（２）部局技術担当者のうち若干人

（３）その他委員長が必要と認める者

１４　地区（部門）情報システム運用委員会の委員長

地区（部門）情報システム運用委員会の委員長は、情報化推進室の室員をもって充てる。

１５　部局（部門）技術担当者

部局に部局技術担当者を置く。部局技術担当者は、全学総括責任者が選任する。

１５―１　部局技術担当者は､部局情報システムの構成の決定や技術的問題に対する処置を担当する。

１５―２　部局技術担当者は、部局技術担当補佐に対して、ポリシー及びそれに基づく基準並びに手順等の遵守を確実にするための教育を実施する。

１５―３　部門の情報システムにおいて部局のその他のシステムと異なった扱いをする場合は、全学統括責任者は、当該部門情報システムに関して、部門技術担当者を選任する。

なお、部門技術担当者は原則として部局技術担当者に準じて扱う。

１６　部局（部門）技術担当補佐

部局技術担当補佐は部局技術担当者が推挙し、全学総括責任者が選任する。

１６―１　部局技術担当補佐は、部局技術担当者の指示により、部局の情報システム運用の技術的実務を補佐し、利用者への教育を補佐する。

１６―２　部門の情報システムにおいて部局のその他のシステムと異なった扱いをする場合は、全学統括責任者は、当該部門情報システムに関して、部門技術担当補佐を選任する。

なお、部門技術担当補佐は原則として部局技術担当補佐に準じて扱う。

１７　役割の分離

情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。

（１）承認又は許可事案の申請者とその承認者又は許可者

（２）監査を受ける者とその監査を実施する者

１８　一般基準と特別基準

１８―１　ポリシーを実施するために実施基準を定める。実施基準は、運用・管理、利用、教育、監査及び認証に関する一般基準と事務に関する特別基準から成る。

１８―２　事務に関する特別基準を事務情報セキュリティ対策基準とする。特別基準は、事務に対する一般基準の適用を排除するものではない。ただし、特別基準と一般基準の規定が重複する場合は、特別基準の規定を優先して適用するものとする。

１９　情報の格付け

情報化推進室は、情報システムで取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備する。

２０　情報セキュリティ水準の低下を招く行為の防止

２０―１　全学総括責任者は、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。

２０―２　本学情報システムを運用・管理・利用する者は、原則として、情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずる。

２１　情報システム運用の外部委託管理

全学総括責任者は、本学情報システムの運用業務のすべて又はその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

２２　情報セキュリティ監査

情報セキュリティ監査責任者は、情報システムのセキュリティ対策がポリシーに基づく手順に従って実施されていることを監査する。情報セキュリティ監査に際しては、別に定める情報セキュリティ監査基準に従う。

２３　見直し

２３―１　ポリシー、実施基準及び手順等を整備した者は、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。

２３―２　本学情報システムを運用・管理及び利用する者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。

A1002

国立大学法人群馬大学医療情報システム運用統一基準

平成 21 年 3 月 17 日制定
平成 22 年 3 月 19 日改正

１　宣言

本運用統一基準は、国立大学法人群馬大学医学部附属病院及び群馬大学重粒子線医学推進機構（以下「本部局」という。）における医療情報システムのセキュリティポリシーの運用について定める。

２　適用範囲

本運用統一基準は、本学医療情報システムを管理､運用及び利用する全ての者に適用する。

３　用語の定義

本運用統一基準において、次の各項に掲げる用語は、それぞれ当該各項の定めるところによる。

３－１　医療情報システム

本部局の診療にかかる情報処理を行うシステム、これを接続する情報ネットワーク等で、次のものをいう。

（１）本部局が管理する医事会計システム及び電子カルテシステム
（２）本部局が管理し、医事会計システム及び電子カルテシステムと接続するシステム
（３）医事会計システム又は電子カルテシステムと接続し、診療関連情報の送受信を必要とする医療機器類等

３－２　医療情報ネットワーク

医療情報システムの情報ネットワーク機能を構成する機器類及び通信ケーブルをいう。

３－３　医療情報

本部局の診療にかかる患者個人情報及びこれと関係付けられた情報（以下「診療関連個人情報」という。）並びに診療関連個人情報を保存・表示するシステム関連情報等からなり、次のものを含む。

（１）医療情報システム内部に記録された情報
（２）医療情報システム外部の電磁的記録媒体に記録された情報
（３）医療情報システムと入出力の関係にある書面に記載された情報

３－４　ポリシー

本学が定める A1000「国立大学法人群馬大学情報システム運用基本方針」及び本運用統一基準（以下「本ポリシー」という。）をいう。

３－５　実施基準、実施手順等

本部局が本ポリシーに基づいて策定する基準及び計画並びに運用・管理、利用、教育、監査及び認証に関する具体的な手順等をいう。

３－６　利用者

本部局において教育・研究・診療・その他業務に携わる者及び教育・研修のため許可を得て診療関連個人情報を扱う者で、許可を受けて本学医療情報システムを利用する者をいう。

３―７　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

３－８　情報インシデント

情報セキュリティに関し、意図的又は偶発的に生じる、法令又は本学の規程に反する事故あるいは事件をいう。

３―９　明示等

情報を取り扱うすべての者が当該医療情報の内容に従う格付けについて共通の認識となるように措置することをいう。

４　全学総括責任者

本学情報システムの運用に責任を持つ者として、本学に全学総括責任者を置く。情報化統括責任者（ＣＩＯ）が全学総括責任者となる。

４―１　全学総括責任者は、ポリシー及びそれに基づく基準並びに手順等の決定や情報システム上での各種問題に対する最終責任を負う。

４―２　全学総括責任者は、全学向け教育及び管理運営部局の部局技術担当補佐向け教育を統括する。

４―３　全学総括責任者に事故あるときは、全学総括責任者があらかじめ指名した者が、その職務を代行する。

４―４　全学総括責任者は、原則として、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置く。

５　情報化推進室

本学情報システムの円滑な運用のための最終決定機関は情報化推進室とする。

５―１　情報化推進室は情報化推進室規程第２条に基づき、以下を実施する。

（１）ポリシー及び全学向け教育の実施ガイドラインの改廃

（２）情報システムの運用と利用、教育に係る規程、手順の制定及び改廃

（３）情報システムの運用と利用に関する教育の年度計画の制定及び改廃並びにその計画の実施状況の把握

（４）情報システム運用リスク管理基準の制定及び改廃並びにその実施状況の把握

（５）情報セキュリティ監査基準の制定及び改廃並びにその実施

（６）情報システム非常時行動計画の制定及び改廃並びにその実施

（７）インシデントの再発防止策の検討及び実施

５―２　情報化推進室は、地区情報システム運用委員会に対して、次の各項につき調査・検討を指示する。

（１）参加部局（部門）におけるポリシーの遵守状況

（２）参加部局（部門）におけるリスク管理、非常時行動計画の策定及び実施状況

（３）参加部局（部門）におけるインシデントの再発防止策の策定及び実施状況

（４）参加部局（部門）における技術担当補佐向け教育の計画と企画

５―３　情報化推進室は、５―２項の指示に対する地区情報システム運用委員会からの答申につき審議し、必要事項の実施を部局情報化推進責任者に対して命令する。

６　全学実施責任者

本学に全学実施責任者を置く。

６―１　全学実施責任者は、全学総括責任者の指示により、本学情報システムの整備と運用に関し、ポリシー及びそれに基づく基準並びに手順等の実施を行う。

６―２　全学実施責任者は、情報システムの運用に携わる者及び利用者に対して、情報システムの運用及び利用並びに情報システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく基準並びに手順等の遵守を確実にするための教育を実施する。

６―３　全学実施責任者は、本学の情報システムのセキュリティに関する連絡及び通報において本学情報システムを代表する。

６―４　全学実施責任者は、すべての部局（部門）技術担当者、部局（部門）技術担当補佐及び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。

６―５　全学実施責任者は、情報化推進室の室員の中から、全学総括責任者が任命する。なお、全学実施責任者は、地区情報システム運用委員会の委員長を兼務することができる。

７　情報セキュリティ監査責任者

全学総括責任者は、情報セキュリティ監査責任者を置く。

７―１　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。

８　本学医療情報システムの管理運営部署

本学医療情報システム管理運営部署は医療情報部とし、本学医療情報システム及び医療情報ネットワークの管理運営を担当する。

９　情報化推進責任者

本部局に情報化推進責任者を置き、病院長をもって充てる。

９－１　情報化推進責任者は、医療情報システムの整備、運用方針の決定及び情報セキュリティ上の各種問題に対する処置につき責任を持つ。

９－２　情報化推進責任者は、本ポリシー及びそれに基づく実施基準・手順等の実施、これに必要な教育・研修を利用者に対し企画実行する責任を持つ。

９－３　情報化推進責任者は、他の部局（部門）情報システムと関連するセキュリティ上の問題及び情報セキュリティ監査により指摘された問題などに関し、全学総括責任者の指示に従い適切な措置を行う。

１０　情報化推進担当者

本部局に情報化推進担当者を置く。情報化推進担当者は、情報化推進責任者が選任する。

１０－１　情報化推進担当者は、本部局における運用方針の決定や情報システム上での各種問題に対する処置に関して情報化推進責任者を補佐する。

１０－２　情報化推進担当者は、医療情報システム並びに周辺の医療機器類の調達、構築内容及び利用者の構成について検討し情報化推進責任者に報告する。

１１　情報化技術担当者

本部局に情報化技術担当者を置く。情報化技術担当者は、情報化推進責任者が選任する。

１１－１　情報化技術担当者は、医療情報システムの構成の決定や技術的問題に対する処置を担当する。

１１－２　情報化技術担当者は、利用者に対して、本ポリシー及びそれに基づく基準並びに手順等の遵守を確実にするための教育を実施する。

１２　情報化技術担当補佐

本部局に情報化技術担当補佐を置く。情報化技術担当補佐は、情報化推進責任者が選任する。

１２－１　情報化技術担当補佐は、情報化技術担当者を補佐し医療情報システムの技術的問題に対する処置を担当する。

１３　医療情報システム運用委員会

本部局に医療情報システム運用委員会を設置する。

医療情報システム運用委員会は次のことを行う。

１３－１　本部局に生じた情報セキュリティ上の諸問題について審議し、本ポリシーに従った実施基準、実施手順等を策定する。

１３－２　昭和地区情報システム運用委員会と情報セキュリティ上の諸問題について調整を行う。

１３－３　以下の各号に掲げる事項につき調査検討し、検討結果を情報化推進室に答申する。

（１）本部局における情報セキュリティポリシーの遵守状況
（２）本部局におけるリスク管理、非常時行動計画の策定及び実施状況
（３）本部局における情報インシデントの収集と再発防止策の策定及び実施状況
（４）本部局における情報セキュリティ水準低下行為の適宜調査
（５）本部局における職員向け広報と教育の計画と企画
（６）その他、部局（部門）情報システム間に起こる諸問題

１４　医療情報システム運用委員会の構成員

医療情報システム運用委員会は、委員長及び次の各項に掲げる者を委員として組織する。

（１）本部局の情報化推進担当者
（２）本部局の情報化技術担当者
（３）医療情報部運営委員会の委員
（４）昭和地区情報システム運用委員会の委員のうち、本運用委員会の委員長が指名する者

（５）総合情報メディアセンターの教員
（６）その他委員長が必要と認める者

１５　医療情報システム運用委員会の委員長

医療情報システム運用委員会の委員長は情報化推進室の室員をもって充てる。

１６　役割の分離

情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。
（１）承認又は許可事案の申請者とその承認者又は許可者
（２）監査を受ける者とその監査を実施する者

１７　実施基準の制定

１７－１　本ポリシーを実施するために、実施基準を定める。
１７－２　実施基準は、医療情報システムの変更、ネットワーク・機器類等周辺環境の変化及び社会情勢の変化に応じて見直しをする。

１８　情報の格付けと明示

本部局は、医療情報の社会的・倫理的特殊性を考慮し、医療情報の内容に従う格付け基準を設け、取扱制限の規程を整備し、これを明示する。

１９　情報セキュリティ水準の低下を招く行為の防止

１９－１　全学総括責任者は、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、規程を整備する。
１９－２　本学医療情報システムを運用、管理及び利用するものは、情報セキュリティ水準の低下を招く行為の防止に関する措置をする。

２０　情報システム運用の外部委託管理

情報化推進責任者は、医療情報システム及びネットワークを介して医療情報システムに接続する医療機器類の一部又は全部の保守管理を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう適切な措置をする。

２１　情報セキュリティ監査

２１－１　情報セキュリティ監査責任者は、医療情報システムのセキュリティ対策が本ポリシーに基づく手順に従って実施されていることを監査する。情報セキュリティ監査に際しては、別途定める情報セキュリティ監査基準に従う。
２１－２　情報化推進責任者は、本学の情報セキュリティ監査と併せて、他大学の医療情報システムを担当する専門的な職員等に情報セキュリティの監査を依頼し、監査結果を運用改善に結びつけるよう措置することができる。

２２　利用の制限

情報化推進責任者は、利用者が本ポリシー、実施基準、実施手順等に違反する行為を行った場合は、当該者が医療情報を利用する権限を制限することができる。

２３　見直し

本ポリシー、実施基準、実施手順等は、医療情報システムと周辺機器類の調達整備の都度、及び医療情報システムの運用環境が社会情勢に即応しなくなった時、速やかに見直しを行う。

２４　その他

本ポリシーに定めるもののほか医療情報の取扱いに関し必要な事項は、「群馬大学医学部附属病院診療情報管理規程」（平成 20 年 10 月 14 日制定）、「群馬大学医学部附属病院の保有する診療関連個人情報管理規程」（平成 21 年 1 月 13 日制定）等で別に定める。

A2101

国立大学法人群馬大学情報システム運用・管理基準

平成２０年９月１８日制定
平成２１年３月１７日改正

第１章　総則

１　目的

この基準は、国立大学法人群馬大学（以下「本学」という。）における情報システムの運用及び管理に関する事項を定めることにより、本学の有する情報資産を適正に保護、活用し、並びに情報システムの信頼性、安全性及び効率性の向上に資することを目的とする。

２　定義

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

（１）　運用基本方針　本学が定める「国立大学法人群馬大学情報システム運用基本方針」をいう。

（２）　運用統一基準　　本学が定める「国立大学法人群馬大学情報システム運用統一基準」をいう。

（３）　情報資産　情報システム、情報ネットワークに接続された情報ネットワーク機器並びに電子計算機、及びそこで取り扱われる情報をいう。ただし、別に定める場合を除き、情報は電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。）に限るものとする。

（４）　情報ネットワーク機器　情報ネットワークの接続のために設置され、電子計算機により情報ネットワーク上を送受信される情報の制御を行うための装置（ファイアウォール、ルータ、ハブ、情報コンセント又は無線ネットワークアクセスポイントを含む。）をいう。

（５）　電子計算機　コンピュータ全般のことを指し、オペレーティングシステム、接続される周辺機器を含むサーバ装置及び端末をいう。

（６）　安全区域　電子計算機及び情報ネットワーク機器を設置した事務室、研究室、教室又はサーバルーム等の内部であって、利用者等以外の者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。

（７）　利用者等　情報システム利用基準において定める利用者のほか、本学情報資産及び情報システムを取扱う者をいう。

（８）　主体認証　識別符号（ユーザ ID）を提示した利用者等又は電子計算機が、情報システムにアクセスする正当な権限を有するか否かを検証することをいう。識別符号（ユーザ ID）とともに正しい方法で主体認証情報（パスワード）が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した利用者等又は電子計算機等を正当な権限を有するものとして認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、この基準における「主体認証」については、公的又は第三者による証明に限るものではない。

（９）　識別符号（ユーザ ID）　主体認証を行うために、利用者等又は電子計算機が提示する符号のうち、情報システムが利用者等又は電子計算機を特定して認識する符号をいう。代表的な識別符号として、ユーザ ID が挙げられる。

（１０）　主体認証情報（パスワード）　主体認証を行うために、利用者等又は電子計算機が提示する情報のうち、情報システムが利用者等又は電子計算機を正当な権限を有するものとして認識する情報をいう。代表的な主体認証情報として、パスワードが挙げられる。

（１１）　アカウント　主体認証を行う必要があると認めた情報システムにおいて、利用者等又は電子計算機に付与された正当な権限をいう。また、狭義には、利用者等又は電子計算機に付与された識別符号（ユーザ ID）及び主体認証情報（パスワード）の組み合わせ、又はそれらのいずれかを指して「アカウント」という。

（１２）　その他の用語の定義は、運用基本方針及び運用基準の定めるところによる。

３　適用範囲

この基準は、情報資産及び情報システムを運用・管理する者に適用する。

４　組織体制

４―１　全学情報システムの運用・管理は、運用基本方針及び運用統一基準に従い、全学総括責任者の下、全学実施責任者、部局情報化推進担当者等からなる情報化推進室が執り行うものとする。

４―２　部局情報システムの運用・管理は、運用基本方針並びに運用統一基準及び情報化推進室の運用方針に従い、部局情報化推進責任者（部局長）の指揮の下、部局情報化推進担当者、部局技術担当者、部局技術担当補佐が執り行うものとする。

４―３　全学情報ネットワークと部局情報ネットワークとの調整及び対外接続に関する事項は、管理運営部局が執り行うものとする。

５　禁止事項

部局技術担当者及び部局技術担当補佐は、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）　部局情報化推進責任者の許可なく情報ネットワーク上の通信を監視し、又は情報ネットワーク機器及び電子計算機の利用記録を採取する行為

（４）　部局情報化推進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）　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

（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章　情報システムのライフサイクル

第１節　設置時

１　セキュリティホール対策

１―１　部局技術担当補佐は、電子計算機及び情報ネットワーク機器（公開されたセキュリティホールの情報がない電子計算機及び情報ネットワーク機器を除く。以下この項において同じ。）について、セキュリティホール対策に必要となる機器情報を収集し、書面として整備すること。

１―２　部局技術担当補佐は、電子計算機及び情報ネットワーク機器の構築又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。

２　不正プログラム対策

２―１　部局情報化推進責任者は、不正プログラム感染の回避を目的とした利用者等に対する留意事項を含む日常的実施事項を定めること。

２―２　部局技術担当者は、不正プログラムから電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。以下この項において同じ。）を保護するため、アンチウイルスソフトウェアを導入する等の対策を実施すること。

２―３　部局技術担当者は、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。

３　サービス不能攻撃対策

部局技術担当者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける電子計算機、情報ネットワーク機器又は通信回線を有する情報システム。以下この項において同じ。）については、サービス提供に必要な電子計算機及び情報ネットワーク機器が装備している機能をサービス不能攻撃対策に活用すること。

４　安全区域

４―１　部局技術担当者は、情報システムによるリスク（物理的損壊又は情報の漏えい若しくは改ざん等のリスクを含む。）を検討し、安全区域に施設及び環境面からの対策を実施すること。

４―２　部局技術担当者は、安全区域に不審者を立ち入らせない措置を講ずること。

４―３　部局技術担当者は、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 について部局情報化推進責任者の承認を得た場合は、この限りでない。

４―４　部局技術担当者は、情報ネットワーク機器を安全区域に設置すること。

５　規程及び文書の整備

５―１　部局技術担当者は、電子計算機のセキュリティ維持に関する規定を整備すること。

５―２　部局技術担当者は、通信回線を介して提供するサービスのセキュリティ維持に関する規定を整備すること。

５―３　部局技術担当者は、すべての電子計算機に対して、電子計算機を管理する利用者等を特定するための文書を整備すること。

５―４　部局技術担当者は、電子計算機関連文書を整備すること。

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

６　主体認証と権限管理

６―１　部局技術担当者は、利用者等が電子計算機にログインする場合には主体認証を行うように電子計算機を構成すること。

６―２　部局技術担当者は、ログオンした利用者等の識別符号（ユーザ ID）に対して、権限管理を行うこと。

７　電子計算機の対策

７―１　部局技術担当者は、電子計算機で利用可能なソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙、または両者を併用することができる。

７―２　部局技術担当者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。

７―３　部局技術担当者は、要保護情報を取り扱うモバイル PC については、学外で使われる際にも、学内で利用される電子計算機と同等の保護手段が有効に機能するように構成すること。

８　サーバ装置の対策

８―１　部局技術担当者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報を暗号化すること。

８－２　部局技術担当者は、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。

８－３　部局技術担当者は、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。

９　通信回線の対策

９－１　部局技術担当者は、通信回線構築によるリスク（物理的損壊又は情報の漏えい若しくは改ざん等のリスクを含む。）を検討し、通信回線を構築すること。

９－２　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、通信回線及び情報ネットワーク機器に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保すること

９－３　部局技術担当者は、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。

９－４　部局技術担当者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って情報ネットワーク機器を利用しアクセス制御及び経路制御を行うこと。

９－５　部局技術担当者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

９－６　部局技術担当者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、選択すること。

９－７　部局技術担当者は、遠隔地から情報ネットワーク機器に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。

９－８　部局技術担当者は、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。

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

１０　情報コンセント

部局技術担当者は、情報コンセントを設置する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

（１）　利用開始及び利用停止時の申請手続の整備
（２）　通信を行う電子計算機の識別又は利用者等の主体認証
（３）　主体認証記録の取得及び管理
（４）　情報コンセント経由でアクセスすることが可能な通信回線の範囲の制限

（５）　情報コンセント接続中に他の通信回線との接続の禁止
（６）　情報コンセント接続方法の機密性の確保
（７）　情報コンセントに接続する電子計算機の管理

１１　VPN、無線 LAN、リモートアクセス

１１―１　部局技術担当者は、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。
（１）　利用開始及び利用停止時の申請手続の整備
（２）　通信内容の暗号化
（３）　通信を行う電子計算機の識別又は利用者等の主体認証
（４）　主体認証記録の取得及び管理
（５）　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
（６）　VPN 接続方法の機密性の確保
（７）　VPN を利用する電子計算機の管理

１１－２　部局技術担当者は、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。
（１）　利用開始及び利用停止時の申請手続の整備
（２）　通信内容の暗号化
（３）　通信を行う電子計算機の識別又は利用者等の主体認証
（４）　主体認証記録の取得及び管理
（５）　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
（６）　無線 LAN に接続中に他の通信回線との接続の禁止
（７）　無線 LAN 接続方法の機密性の確保
（８）　無線 LAN に接続する電子計算機の管理

１１－３　部局技術担当者は、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。
（１）　利用開始及び利用停止時の申請手続の整備
（２）　通信を行う者又は発信者番号による識別及び主体認証
（３）　主体認証記録の取得及び管理
（４）　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
（５）　リモートアクセス中に他の通信回線との接続の禁止
（６）　リモートアクセス方法の機密性の確保

（７）　リモートアクセスする電子計算機の管理

１２　学外通信回線との接続

１２－１　全学実施責任者は、全学総括責任者の承認を得た上で、学内通信回線を学外通信回線と接続すること。利用者等による、学内通信回線と学外通信回線との接続を禁止すること。

１２―２　全学実施責任者は、学内通信回線を学外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している学内通信回線又は学外通信回線から独立した通信回線として学内通信回線を構築すること。

１３　上流ネットワークとの関係

全学実施責任者は、本学情報ネットワークを構築し運用するにあたっては、本学情報ネットワークと接続される上流ネットワークとの整合性に留意すること。

第２節　運用時

１　セキュリティホール対策

１－１　部局技術担当補佐は、電子計算機及び情報ネットワーク機器の構成に変更があった場合には、セキュリティホール対策に必要となる機器情報を記載した書面を更新すること。

１－２　部局技術担当補佐は、管理対象となる電子計算機及び情報ネットワーク機器上で利用しているソフトウェアに関連する公開されたセキュリティホールに関連する情報を適宜入手すること。

１－３　部局技術担当者は、入手したセキュリティホールに関連する情報から、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を作成すること。

（１）　対策の必要性
（２）　対策方法
（３）　対策方法が存在しない場合の一時的な回避方法

（４）　対策方法又は回避方法が情報システムに与える影響
（５）　対策の実施予定
（６）　対策テストの必要性
（７）　対策テストの方法
（８）　対策テストの実施予定

１－４　部局技術担当補佐は、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。
１－５　部局技術担当補佐は、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。

１－６　部局技術担当補佐は、信頼できる方法で対策用ファイルを入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

１－７　部局技術担当補佐は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び情報ネットワーク機器が確認された場合の対処を行うこと。

１－８　部局技術担当者は、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、他の部局技術担当者と共有すること。

２　不正プログラム対策

２－１　部局技術担当補佐は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、利用者等にその対処の実施に関する指示を行うこと。

２－２　部局情報化推進責任者は、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。

３　脆弱性診断

部局技術担当者及び部局技術担当補佐、は、情報システムに関する脆弱性の診断を定期的に実施し、セキュリティの維持に努めること。

４　規定及び文書の見直し、変更

４－１　部局技術担当者は、適宜、電子計算機のセキュリティ維持に関する規定の見直しを行うこと。また、当該規定を変更した場合には、当該変更の記録を保存すること。
４－２　部局技術担当者は、適宜、通信回線を介して提供するサービスのセキュリティ維持に関する規定の見直しを行うこと。また、当該規定を変更した場合には、当該変更の記録を保存すること。

４－３　部局技術担当者は、電子計算機を管理する利用者等を変更した場合には、当該変更の内容を、電子計算機を管理する利用者等を特定するための文書へ反映すること。また、当該変更の記録を保存すること。

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

４－５　部局技術担当補佐は、通信回線の構成、情報ネットワーク機器の設定、アクセス制御の設定又は識別符号（ユーザ ID）を含む事項を変更した場合には、当該変更の内容を通信回線及び情報ネットワーク機器関連文書へ反映すること。また、当該変更の記録を保存すること。

５　運用管理

５－１　部局技術担当補佐は、電子計算機のセキュリティ維持に関する規定に基づいて、電子計算機の運用管理を行うこと。

５－２　部局技術担当補佐は、通信回線を介して提供するサービスのセキュリティ維持に関する規定に基づいて、日常的及び定期的に運用管理を実施すること。

６　接続の管理

地区総括責任者は、情報ネットワークに関する接続の申請を受けた場合は、別途定める情報ネットワーク接続手順に従い、申請者に対して接続の諾否を通知し必要な指示を行うこと。

７　資源の管理

部局技術担当者は、電子計算機の CPU 資源、ディスク資源並びに情報ネットワーク帯域資源等の利用を総合的かつ計画的に推進するため、これらの資源を利用者等の利用形態に応じて適切に分配し管理すること。

８　ネットワーク情報の管理

部局技術担当者は、部局情報ネットワークで使用するドメイン名や IP アドレス等のネットワーク情報について、情報化推進室から割り当てを受け、利用者等からの利用形態に応じて適切に分配し管理すること。

９　サーバ装置の対策

９－１　部局技術担当者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対応すること。

９－２　部局技術担当補佐は、要安定情報を取り扱うサーバ装置に保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理すること。

９－３　部局技術担当補佐は、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。

９－４　部局技術担当者は、サーバ装置上で証跡管理を行う必要性を検討し、必要と認めた場合には実施すること。

９－５　部局技術担当補佐は、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。

１０　通信回線の対策

１０－１　部局技術担当補佐は、通信回線を利用する電子計算機の識別符号（ホスト ID）、電子計算機の利用者等と当該利用者等の識別符号（ユーザ ID）の対応、及び通信回線の利用部局を含む事項の管理を行うこと。

１０－２　部局技術担当者は、定期的に通信回線の構成、情報ネットワーク機器の設定、アクセス制御の設定又は識別符号（ユーザ ID）を含む事項の変更を確認すること。また、当該変更によって生ずる通信回線のセキュリティへの影響を特定し、対応すること。

１０－３　部局技術担当者は、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。

１０－４　部局技術担当補佐は、部局技術担当者の許可を受けていない電子計算機及び情報ネットワーク機器を通信回線に接続させないこと。

１０－５　部局技術担当補佐は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測又は検知すること。

１０－６　部局技術担当補佐（及び地区技術担当者）は、情報システムにおいて基準となる時刻に、情報ネットワーク機器の時刻を同期すること。

１１　学外通信回線との接続

１１－１　全学実施責任者は、学内通信回線と学外通信回線の接続において情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している学内通信回線又は学外通信回線から独立した通信回線に構成を変更すること。

１１－２　全学実施責任者は、通信回線の変更に際し及び定期的に、アクセス制御の設定の見直し行うこと。

１１－３　全学実施責任者は、定期的に、学外通信回線から通信することが可能な学内通信回線及び情報ネットワーク機器のセキュリティホールを検査すること。

１１－４　全学実施責任者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視すること。

第３節　運用終了時

１　電子計算機の対策

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

２　情報ネットワーク機器の対策

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

第４節　PDCA サイクル

１　情報システムの計画・設計

１－１　部局技術担当者は、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。

１－２　部局技術担当者は、情報システムのセキュリティ要件を決定すること。

１－３　部局技術担当者は、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。

１－４　部局技術担当者は、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。

２　情報システムの構築・運用・監視

部局技術担当者は、情報システムの構築、運用及び監視に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行うこと。

３　情報システムの移行・廃棄

部局技術担当者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を採ること。

４　情報システムの見直し

部局技術担当者は、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。

第３章　情報の格付けと取扱い

１　情報の作成又は入手

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

２　情報の作成又は入手時における格付けの決定と取扱制限の検討

２－１　教職員等は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

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

３　格付けと取扱制限の明示

教職員等は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示し、必要に応じて取扱制限についても明示すること。

４　格付けと取扱制限の継承

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

５　格付けと取扱制限の変更

５－１　教職員等は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。

５－２　教職員等は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること。

６　格付けに応じた情報の保存

６－１　部局技術担当者は、電子計算機に保存された要保護情報について、適切なアクセス制御を行うこと。

６－２　部局技術担当者は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書の複写の保管について、災害等への対策の必要性を検討し、必要があると認めたときは、同時被災等しないための適切な措置を講ずること。

第４章　主体認証

１　主体認証機能の導入

１－１　部局技術担当者は、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。

１－２　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、識別及び主体認証を行う機能を設けること。

１－３　部局技術担当補佐は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報（パスワード）を秘密にする必要がある場合には、当該主体認証情報（パスワード）が明らかにならないように管理すること。
（１）　主体認証情報（パスワード）を保存する場合には、その内容の暗号化を行うこと。
（２）　主体認証情報（パスワード）を通信する場合には、その内容の暗号化を行うこと。
（３）　保存又は通信を行う際に暗号化を行うことができない場合には、利用者等に自らの主体認証情報（パスワード）を設定、変更、提供（入力）させる際に、暗号化が行われない旨を通知すること。

１－４　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、利用者等に主体認証情報（パスワード）の定期的な変更を求める場合には、利用者等に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。
（１）　利用者等が定期的に変更しているか否かを確認する機能
（２）　利用者等が定期的に変更しなければ、情報システムの利用を継続させない機能

１－５　部局技術担当者は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報（パスワード）又は主体認証情報格納装置（IC カード）を他者に使用され又は使用される危険性を認識した場合に、直ちに当該主体認証情報（パスワード）若しくは主体認証情報格納装置（IC カード）による主体認証を停止する機能又はこれに対応する識別符号（ユーザ ID）による情報システムの利用を停止する機能を設けること。

１－６　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、知識による主体認証方式を用いる場合には、以下の機能を設けること。
（１）　利用者等が、自らの主体認証情報（パスワード）を設定する機能
（２）　利用者等が設定した主体認証情報（パスワード）を他者が容易に知ることができないように保持する機能

１－７　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、知識、所有、生体情報以外の主体認証方式を用いる場合には、以下の要件について検証

した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。また、用いる方式に応じて、以下を含む要件を定めること。
（１）　正当な主体以外の主体を誤って主体認証しないこと。（誤認の防止）
（２）　正当な主体が本人の責任ではない理由で主体認証できなくならないこと。（誤否の防止）
（３）　正当な主体が容易に他者に主体認証情報（パスワード）を付与及び貸与ができないこと。（代理の防止）
（４）　主体認証情報（パスワード）が容易に複製できないこと。（複製の防止）
（５）　部局技術担当補佐の判断により、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）
（６）　主体認証について業務遂行に十分な可用性があること。（可用性の確保）
（７）　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）
（８）　主体に付与した主体認証情報（パスワード）を使用することが不可能になった際に、正当な主体に対して主体認証情報（パスワード）を安全に再発行できること。（再発行の確保）

１－８　部局技術担当者は、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。

１－９　部局情報化推進責任者は、セキュリティ侵害又はその可能性が認められる場合、主体認証情報（パスワード）の変更を求め又はアカウントを失効させることができる。

第５章　アクセス制御

１　アクセス制御機能の導入

１－１　部局技術担当者は、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。
１－２　部局技術担当者は、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。

２　利用者等による適正なアクセス制御

２－１　部局技術担当者は、それぞれの情報システムに応じたアクセス制御の措置を講じるよう、利用者等に指示すること。
２－２　利用者等は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。

３　無権限のアクセス対策

３－１　部局技術担当者及び部局技術担当補佐は、無権限のアクセス行為を発見した場合は、速やかに部局情報化推進責任者に報告すること。部局情報化推進責任者は、上記の報告を受けたときは、遅滞なく全学総括責任者にその旨を報告すること。
３－２　全学総括責任者及び部局情報化推進責任者は、前項の報告を受けた場合は、新たな防止対策等必要な措置を講じること。

第６章　アカウント管理

１　アカウント管理機能の導入

１－１　部局技術担当者は、すべての情報システムについて、アカウント管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アカウント管理を行う必要があると判断すること。
１－２　部局技術担当者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理を行う機能を設けること。

２　アカウント管理手続の整備

２－１　部局技術担当者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理について、以下の事項を含む手続を明確にすること。
（１）　主体からの申請に基づいてアカウント管理を行う場合には、その申請者が正当な主体であることを確認するための手続
（２）　主体認証情報（パスワード）の初期配布方法及び変更管理手続

（３）　アクセス制御情報の設定方法及び変更管理手続

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

３　共用アカウント

３－１　部局技術担当者は、アカウント管理を行う必要があると認めた情報システムにおいて、共用アカウントの利用許可については、情報システムごとにその必要性を判断すること。

３－２　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウントを発行する際に、それが共用アカウントか、共用ではないアカウントかの区別を利用者等に通知すること。ただし、共用アカウントは、部局技術担当者が、その利用を認めた情報システムでのみ付与することができる。

４　アカウントの発行

４－１　アカウント管理を行う者は、利用者等からのアカウント発行申請を受理したときは、申請者が第９章１－２項第３号による処分期間中である場合を除き、遅滞無くアカウントを発行すること。

４－２　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、情報システムを利用する許可を得た主体に対してのみ、アカウントを発行すること。

４－３　アカウント管理を行う者は、アカウントを発行するにあたっては、期限付きの仮パスワードを発行する等の措置を講じることが望ましい。

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

４－５　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス制御に係る設定をすること。

５　アカウント発行の報告

５－１　アカウント管理を行う者は、アカウントを発行したときは、速やかにその旨を部局情報化推進責任者に報告すること。

５－２　全学総括責任者は、必要により部局情報化推進責任者にアカウント発行の報告を求めることができる。

６　アカウントの有効性検証

６－１　アカウント管理を行う者は、発行済のアカウントについて、次号に掲げる項目を一か月毎に確認すること。
（１）　利用資格を失ったもの
（２）　部局情報化推進責任者が指定する削除保留期限を過ぎたもの
（３）　パスワード手順に違反したパスワードが設定されているもの
（４）　六か月以上使用されていないもの
６－２　アカウント管理を行う者は、人事異動等、アカウントを追加又は削除する時に、不適切なアクセス制御設定の有無を点検すること。

７　アカウントの削除

７－１　アカウント管理を行う者は、６－１項第１号及び第２号に該当するアカウントを発見したとき、又は第９章１－２項第３号による削除命令を受けたときは、速やかにそのアカウントを削除し、その旨を部局情報化推進責任者に報告すること。
７－２　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等のアカウントを削除し、その旨を部局情報化推進責任者に報告すること。
７－３　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等に交付した主体認証情報格納装置（IC カード）を返還させ、その旨を部局情報化推進責任者に報告すること。
７－４　部局情報化推進責任者は、７－１項乃至７－３項の報告を受けたときは、速やかにその旨を利用者等に通知すること。ただし、電話、郵便、電子メール等の伝達手段によっても通知ができない場合はこの限りでない。
７－５　全学総括責任者は、必要により部局情報化推進責任者にアカウント削除の報告を求めることができる。

８　アカウントの停止

８－１　アカウント管理を行う者は、６－１項第３号及び第４号に該当するアカウントを発見したとき、第９章１－２項第３号による停止命令を受けたとき、又は主体認証情報（パスワード）が他者に使用され若しくはその危険が発生したことの報告を受けたときは、速やかにそのアカウントを停止し、その旨を部局情報化推進責任者に報告すること。

８－２　部局情報化推進責任者は、前項の措置の報告を受けたときは、速やかにその旨を利用者等に通知すること。ただし、電話、郵便、電子メール等の伝達手段によっても通知ができない場合はこの限りでない。
８－３　全学総括責任者は、必要により部局情報化推進責任者にアカウント停止の報告を求めることができる。

９　アカウントの復帰

９－１　アカウントの停止を受けた利用者等がアカウント停止からの復帰を希望するときは、その旨を部局情報化推進責任者に申し出させること。
９－２　部局情報化推進責任者は、前項の申し出を受けたときは、アカウント管理を行う者に当該アカウントの安全性の確認及びアカウントの復帰を指示すること。
９－３　アカウント管理を行う者は、前項の指示に従い当該アカウントの安全性を確認した後、速やかにアカウントを復帰させること。

１０　管理者権限を持つアカウントの利用

管理者権限を持つアカウントを付与された者は、管理者としての業務遂行時に限定して、当該アカウントを利用すること。

第７章　証跡管理

１　証跡管理機能の導入

１－１　部局技術担当者は、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。
１－２　部局技術担当者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。
１－３　部局技術担当者は、証跡を取得する必要があると認めた情報システムにおいては、事象を証跡として記録するに当たり、事象ごとに必要な情報項目を記録するように情報システムの設定をすること。
１－４　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、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方針

を整備し、必要に応じ、これらの場合に対応するための機能を情報システムに設けること。

１－５　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、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行い、外部記録媒体等その他の装置・媒体に記録した証跡についてはこれを適正に管理すること。

２　部局技術担当補佐による証跡の取得と保存

２－１　部局技術担当補佐は、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、部局技術担当者が情報システムに設けた機能を利用して、証跡を記録すること。

２－２　部局技術担当補佐は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間を定め、当該保存期間が満了する日まで証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。

２－３　部局技術担当補佐は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処を行うこと。

３　証跡管理に関する利用者等への周知

部局情報化推進責任者又は部局技術担当者は、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、部局技術担当補佐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。

４　通信の監視

４－１　利用者等によるネットワークを通じて行われる通信の傍受を禁止すること。ただし、全学総括責任者又は当該ネットワークを管理する部局情報化推進責任者は、セキュリティ確保のため、あらかじめ指定した者に、ネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

４－２　全学総括責任者又は部局情報化推進責任者は、監視の範囲をあらかじめ具体的に定めておかなければならない。ただし、不正アクセス行為又はこれに類する重大なセキュリティ侵害に対処するために特に必要と認められる場合、全学総括責任者又は部局情報化推進責任者は、セキュリティ侵害の緊急性、内容及び程度に応じて、対処のために不可欠と認められる情報について、監視を行うよう命ずることができる。

４－３　監視を行う者は、監視によって知った通信の内容又は個人情報を、他の者に伝達してはならない。ただし、前項ただし書きに定める情報については、全学総括責任者並びに部局情報化推進責任者、及び、情報化推進室並びに地区（部門）情報システム運用委員会に伝達することができる。
４－４　監視を行わせる者は、監視を行う者に対して、監視記録を保存する期間をあらかじめ指示するものとする。監視を行う者は、指示された期間を経過した監視記録を直ちに破棄しなければならない。ただし、監視記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。
４－５　監視を行う者及び監視記録の伝達を受けた者は、ネットワーク運用・管理のために必要な限りで、これを閲覧し、かつ、保存することができる。監視記録を不必要に閲覧してはならない。不必要となった監視記録は、直ちに破棄しなければならない。監視記録の内容を、法令に基づく場合等を除き、他の者に伝達してはならない。

５　利用記録

５－１　複数の者が利用する情報機器の管理者は、当該機器に係る利用記録（以下「利用記録」という。）をあらかじめ定めた目的の範囲でのみ採取することができる。当該目的との関連で必要性の認められない利用記録を採取することはできない。
５－２　前項に規定する目的は、法令の遵守、情報セキュリティの確保、課金その他当該情報機器の利用に必要なものに限られる。個人情報の取得を目的とすることはできない。
５－３　当該情報機器の管理者は、５－１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。
５－４　当該情報機器の管理者は、５－２項に規定する目的のために必要な限りで、利用記録を他の者に伝達することができる。
５－５　５－１項の規定により情報機器の利用を記録しようとする者は、５－２項の目的、これによって採取しようとする利用記録の範囲及び前項により利用記録を伝達する者を、あらかじめ部局情報化推進責任者に申告し、かつ、当該機器の利用者等に開示しなければならない。部局情報化推進責任者は、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。
５－６　当該情報機器の管理者又は利用記録の伝達を受けた者は、５－１項の目的のために必要な限りで、これを保有することができる。不要となった利用記録は、直ちに破棄しなければならない。ただし、当該情報機器の管理者は、利用記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

６　個人情報の取得と管理

６－１　電子的に個人情報の提供を求める場合は、提供を求める情報の範囲、利用の目的、その情報が伝達される範囲を、あらかじめ相手方に示さなければならない。
６－２　前項の個人情報は、当人の請求により開示、訂正又は削除をしなければならない。また、そのための手続を示さなければならない。

７　利用者等が保有する情報の保護

利用者等が保有する情報は、ネットワーク運用に不可欠な範囲又はインシデント対応に不可欠な範囲において、閲覧、複製又は提供することができる。

第８章　暗号と電子署名

１　暗号化機能及び電子署名の付与機能の導入

１－１　部局技術担当者は、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。
１－２　部局技術担当者は、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。
１－３　部局技術担当者は、要保全情報を取り扱う情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討すること。
１－４　部局技術担当者は、電子署名の付与を行う必要があると認めた情報システムには、電子署名の付与を行う機能を設けること。
１－５　部局技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リスト又は、本学における検証済み暗号リストがあればその中から選択すること。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つをそれらのリストの中から選択すること。

２　暗号化及び電子署名の付与に係る管理

２－１　部局技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対応手順等を定めること。
２－２　部局技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の保存媒体及び保存場所を定めること。
２－３　部局技術担当者は、電子署名の付与を行う必要があると認めた情報システムにおいて、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供すること。

第９章　違反と例外措置

１　違反への対応

１－１　部局情報化推進責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、速やかに調査を行い、事実を確認すること。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取すること。
１－２　部局情報化推進責任者は、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）　部局技術担当者に対する当該行為に係る情報発信の遮断命令
（３）　部局技術担当者に対する当該行為者のアカウント停止命令、または削除命令
（４）　本学の懲罰委員会への報告
（５）　その他法令に基づく措置
１－３　部局情報化推進責任者は、前項第２号及び第３号については、情報化推進室を通じて、他部局の部局情報化推進責任者に同等の措置を依頼することができる。
１－４　部局情報化推進責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合及び上記の措置を講じた場合は、遅滞無く全学総括責任者にその旨を報告すること。

２　例外措置

２－１　情報化推進室は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）を定め、審査手続を整備すること。
２－２　許可権限者は、利用者等による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。また、決定の際に、以下の項目を含む例外措置の適用審査記録を整備し、全学総括責任者に報告すること。
（１）　決定を審査した者の情報（氏名、役割名、所属、連絡先）
（２）　申請内容
・申請者の情報（氏名、所属、連絡先）
・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
・例外措置の適用を申請する期間
・例外措置の適用を申請する措置内容（講ずる代替手段等）
・例外措置の適用を終了した旨の報告方法
・例外措置の適用を申請する理由
（３）　審査結果の内容
・許可又は不許可の別
・許可又は不許可の理由
・例外措置の適用を許可した情報セキュリティ関係規程の適用箇所（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
２－３　許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な対応を講ずること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

第１０章　インシデント対応

１　インシデントの発生に備えた事前準備

１－１　全学総括責任者は、情報セキュリティに関するインシデント（故障を含む。以下第２項までにおいて同じ。）が発生した場合、被害の拡大を防ぐとともに、インシデントから復旧するための体制を整備すること。

１－２　全学実施責任者は、インシデントについて利用者等から部局情報化推進責任者への報告手順を整備し、当該報告手段をすべての利用者等に周知すること。
１－３　全学実施責任者は、インシデントが発生した際の対応手順を整備すること。
１－４　全学実施責任者は、インシデントに備え、本学の研究教育事務の遂行のため特に重要と認めた情報システムについて、その部局技術担当者及び部局技術担当補佐の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。
１－５　全学実施責任者は、インシデントについて学外から報告を受けるための窓口を設置し、その窓口への連絡手段を学外に公表すること。

２　インシデントの原因調査と再発防止策

２－１　部局情報化推進責任者は、インシデントが発生した場合には、インシデントの原因を調査し再発防止策を策定し、その結果を報告書として全学総括責任者に報告すること。
２－２　全学総括責任者は、部局情報化推進責任者からインシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずること。

第１１章　本学支給以外の情報システム

１　本学支給以外の情報システムにかかる安全管理措置の整備

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。

２　本学支給以外の情報システムの利用許可及び届出の取得及び管理

２－１　部局技術担当者及び部局技術担当補佐は、本学支給以外の情報システムによる要保護情報の情報処理に係る記録を取得すること。
２－２　部局技術担当者及び部局技術担当補佐は、要保護情報（機密性２情報を除く。）について本学支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

２－３　部局技術担当者及び部局技術担当補佐は、機密性２情報について本学支給以外の情報システムによる情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。

第１２章　学外の情報セキュリティ水準の低下を招く行為の禁止

１　学外の情報セキュリティ水準の低下を招く行為の防止

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。

第１３章　教育・研修

１　情報セキュリティ対策の教育

１－１　全学実施責任者は、情報セキュリティ関係基準について、部局情報化推進責任者部局技術担当者、部局技術担当補佐及び利用者等（以下「教育啓発対象者」という。）に対し、その啓発をすること。
１－２　全学実施責任者は、情報セキュリティ関係基準について、教育啓発対象者に教育すべき内容を検討し、教育のための資料を整備すること。
１－３　全学実施責任者は、教育啓発対象者が毎年度最低一回、受講できるように、情報セキュリティ対策の教育に係る計画を企画、立案するとともに、その実施体制を整備すること。
１－４　全学実施責任者は、教育啓発対象者の入学時、着任時、異動時に三か月以内に受講できるように、情報セキュリティ対策の教育を企画、立案し、その体制を整備すること。
１－５　全学実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備すること。
１－６　全学実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況について、当該教育啓発対象者の所属する部局の部局情報化推進責任者に通知すること。

１－７　部局情報化推進責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告すること。教育啓発対象者が当該勧告に従わない場合には、全学実施責任者にその旨を報告すること。
１－８　全学実施責任者は、毎年度一回、全学総括責任者及び情報化推進室に対して、教育啓発対象者の情報セキュリティ対策の教育の受講状況について報告すること。
１－９　全学実施責任者は、情報セキュリティ関係基準について、教育啓発対象者に対する情報セキュリティ対策の訓練の内容及び体制を整備すること。
１－１０　全学情報システム運用委員会及び部局情報システム運用委員会は、利用者等からの情報セキュリティ対策に関する相談に対応すること。
１－１１　その他、教育・研修に関する事項については、講習計画に定めること。

２　教育の主体と客体

２－１　地区（部門）情報システム運用委員会は、部局情報化推進責任者、部局技術担当者及び部局技術担当補佐に対して、情報セキュリティ対策の教育を実施すること。
２－２　部局技術担当者及び部局技術担当補佐は、利用者等に対して、講習計画の定める講習を実施すること。

第１４章　評価

１　自己点検に関する年度計画の策定

全学総括責任者は、年度自己点検計画を策定すること。

２　自己点検の実施に関する準備

部局情報化推進責任者は、職務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。

３　自己点検の実施

３－１　部局情報化推進責任者は、全学総括責任者が定める年度自己点検計画に基づき、職務従事者に対して、自己点検の実施を指示すること。
３－２　職務従事者は、部局情報化推進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。

４　自己点検結果の評価

４－１　部局情報化推進責任者は、職務従事者による自己点検が行われていることを確認し、その結果を評価すること。
４－２　全学総括責任者は、部局情報化推進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。

５　自己点検に基づく改善

５－１　職務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、部局情報化推進責任者にその旨を報告すること。
５－２　全学総括責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には部局情報化推進責任者に改善を指示すること。

６　監査

部局情報化推進責任者その他の関係者は、全学総括責任者の行う監査の適正かつ円滑な実施に協力すること。

A2102

国立大学法人群馬大学情報システム運用リスク管理基準

平成２０年９月１８日制定
平成２１年３月１７日改正

１　目的

この基準は、国立大学法人群馬大学情報システム運用基本方針及び国立大学法人群馬大学情報システム運用統一基準（以下「ポリシー」という。）に基づき本学情報システムの運用におけるリスクを分析し、必要な対策を立て、情報セキュリティを確保することを目的とする。

２　定義

この基準において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。
（１）　機密性(Confidentiality)　アクセス権を持つ者だけが、情報にアクセスできることを確実にすること。
（２）　完全性(Integrity)　情報及び処理方法が正確であること及び完全であることを保護すること。
（３）　可用性(Availability)　認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。
（４）　その他の用語の定義はポリシーの定めるところによる。

３　リスク評価手順

全学総括責任者は、情報資産の価値と脅威、脆弱性を評価するための情報システム運用リスク評価手順を定める。

４　リスク管理

全学総括責任者は、全学実施責任者を含む各情報資産の管理者に対して、少なくとも年に一回、リスク管理を次の各号に従って実施し、その結果を報告するよう指示する。
（１）　当該管理者は、自らが扱う情報資産について情報システム運用リスク評価手順に基づきリスク評価を行う。
（２）　当該管理者は、評価結果に従い、リスクに対する事前の対策を必要とするものについてその具体策を定め、あるいはトラブルが発生した場合の具体的な対応について当該情報資産についてのインシデント対応手順を定める。対策を施さないと判断したものについても報告する。
（３）　全学総括責任者は、報告に基づいて、ポリシー及び実施基準等の見直しを行う。

A2103

国立大学法人群馬大学情報システム非常時行動計画に関する基準

平成２０年９月１８日制定
平成２１年３月１７日改正

１　目的

この基準は、国立大学法人群馬大学（以下、本学という）情報システムの運用において非常事態が発生した場合の行動を非常時行動計画として事前に定め、早期発見・早期対応により、事件・事故の影響を最小限に抑え、早急な情報システムの復旧と再発防止に努めるために必要な措置を講じることを定めることを目的とする。

２　定義

この基準において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。
（１）　運用基本方針　本学が定める国立大学法人群馬大学情報システム運用基本方針をいう。
（２）　運用基準　本学が定める国立大学法人群馬大学情報システム運用基準をいう。
（３）　非常事態　本学情報システムの運用に関するインシデントのうち特に緊急性を要するものをいう。
（４）　その他の用語の定義は、運用基本方針及び運用基準で定めるところによる。

３　危機管理規程の適用

本学情報システムの運用において非常事態が発生した場合には、本学危機管理規則に従う。

４　非常事態の報告

４－１　全学実施責任者は、インシデントについての報告または通報を学内または学外から受けつけ、迅速に情報を集約する手段を整備し、周知・公表する。
４－２　全学実施責任者は、報告または通報を受けたインシデントのうち、非常事態の発生またはそのおそれがある場合には、全学総括責任者へ報告する。

５　非常時対策本部

全学総括責任者は、非常事態が発生しまたは発生するおそれが特に高いと認められる場合には、被害の拡大防止、被害からの早急な復旧その他非常事態の対策等を実施するために危機管理規則に従って、学長に対して危機対策本部の設置を進言する。

６　非常時連絡網

本学情報システムの運用における非常事連絡網は、本学危機管理規則に従う。

７　インシデント対応手順

７－１　具体的なインシデント対応は、別途定める「A3103 インシデント対応手順」に基づき対処する。

７－２　非常事態においては、危機対策本部の指示がインシデント対応手順に優先する。

８　再発防止策の検討

全学総括責任者は、危機対策本部の報告書をもとに再発防止策の実施を図る。

A2104

国立大学法人群馬大学情報格付け基準

平成２０年９月１８日制定
平成２１年３月１７日改正

1　目的

情報の格付けは、本学におけるポリシー及び実施基準に沿った対策を適正に実施するための基礎となる重要な事項である。

情報の格付け及び取扱制限は、その作成者又は入手者が、当該情報をどのように取り扱うべきと考えているのかを他の者に認知させ、当該情報の重要性や講ずべき情報セキュリティ対策を明確にするための手段である。このため、情報の格付け及び取扱制限が適切に行われなければ、当該情報の取扱いの重要性が認知されず、必要な対策が講じられないこととなる。

また、情報の格付け及び取扱制限を実施することで、情報の利用者に対し、日々の情報セキュリティ対策の意識を向上させることができる。具体的には、情報を作成又は入手するたびに格付け及び取扱制限の判断を行い、情報を取り扱うたびに格付け及び取扱制限に従った対策を講ずることで、情報と情報セキュリティ対策が不可分であるとの認識を継続的に維持する効果も期待できる。

本基準は、情報の格付け及び取扱制限の意味とその運用について教職員等が正しく理解することを目的とする。

2　本基準の対象者

本基準は、情報を取り扱うすべての教職員等を対象とする。

3　格付けの区分及び取扱制限の種類の定義

3-1 格付けの区分

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

【基準利用者への補足説明】

情報について、機密性（情報に関して、アクセスを認可された者だけがこれにアクセスできる状態を確保すること）、完全性（情報が破壊、改ざん又は消去されていない状態を確保すること）、可用性（情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること）の３つの観点を区別し、それぞれにつき格付けの区分の定義を示す。

(2) 機密性についての格付けの定義

格付けの区分	分類の基準
機密性３情報	本学情報システムで取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性２情報	本学情報システムで取り扱う情報のうち、秘密文書に相当する機密性は要しないが、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

なお、機密性２情報及び機密性３情報を「要機密情報」という。

(3) 完全性についての格付けの定義

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

なお、完全性２情報を「要保全情報」という。

(4) 可用性についての格付けの定義

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

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

3-2 取扱制限の種類

情報の取扱制限の種類は、機密性、完全性、可用性について、それぞれ以下のとおりとする。

【基準利用者への補足説明】
情報について、機密性、完全性、可用性の３つの観点を区別し、それぞれにつき取扱制限の種類の定義を行う。「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。

3-2-1 機密性についての取扱制限

機密性についての取扱制限の定義

取扱制限の種類	指定方法
複製について	複製禁止、複製要許可
配付について	配付禁止、配付要許可
暗号化について	暗号化必須、保存時暗号化必須、通信時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り

【基準利用者への補足説明】
上記の指定方法の意味は以下のとおり。
・「○○禁止」 当該情報について、○○で指定した行為を禁止する必要がある場合に指定する。
・「○○要許可」 当該情報について、○○で指定した行為をするに際して、許可を得る必要がある場合に指定する。

・「暗号化必須」 当該情報について、暗号化を必須とする必要がある場合に指定する。また、保存時と通信時の要件を区別するのが適当な場合には、例えば、「保存時暗号化」「通信時暗号化」など、情報を取り扱う者が分かるように指定する。
・「○○限り」 当該情報について、参照先を○○に記載した者のみに制限する必要がある場合に指定する。例えば、「部局内限り」「委員会出席者限り」など、参照を許可する者が分かるように指定する。

3-2-2 完全性についての取扱制限

完全性についての取扱制限の定義

取扱制限の種類	指定方法
保存期間について	○○まで保存
保存場所について	○○において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

【基準利用者への補足説明】
保存期間の指定の方法は、以下のとおり。
保存を要する期日である「年月日」又は期日を特定できる用語に「まで保存」を付して指定する。
例）平成１８年７月３１日まで保存
例）平成１８年度末まで保存
完全性の要件としては保存期日や保存方法等を明確にすることであるが、実際の運用においては、保存先とすべき情報システムを指定することで、結果的に完全性を確実にすることができる。例えば、以下のように指定する。
例）年度内保存文書用共有ファイルサーバに保管
例）３カ年保存文書用共有ファイルサーバに保管

3-2-3 可用性についての取扱制限

可用性についての取扱制限の定義

取扱制限の種類	指定方法

復旧までに許容できる時間について	**〇〇以内復旧**
保存場所について	**〇〇において保存**

【基準利用者への補足説明】
復旧許容時間の指定の方法は以下のとおり。
復旧に要するまでの時間として許容できる時間を記載し、その後に「以内復旧」を付して指定する。
例）１時間以内復旧
例）３日以内復旧
可用性の要件としては復旧許容期間等を明確にすることであるが、実際の運用においては、必要となる可用性対策を講じてある情報システムを指定することで、結果的に可用性を確実にすることができる。例えば、各自 PC のファイルについては定期的にバックアップが実施されておらず、部局共有ファイルサーバについては毎日バックアップが実施されている場合には、以下のような指定が考えられる。
例）部局共有ファイル保存必須
例）各自 PC 保存可

4　格付け及び取扱制限の手順

4-1 格付け及び取扱制限の決定

4-1-1 決定

部局情報化推進責任者（部局長）が決定を行う場合：
(1) 部局情報化推進責任者は、教職員等による格付けの適正性を確保するため、格付け及び取扱制限の定義に基づき、当該部局情報化推進責任者が所掌する事務で取り扱う情報について、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、これが格付け及び取扱制限の定義のいずれに分類されるものであるのかを例示した表（以下「格付け及び取扱制限の判断例」という。）を作成し、当該情報の格付け及び取扱制限を決定する（取扱制限の必要性の有無を含む。）こと。

教職員等が個々に決定を行う場合：
(2) 教職員等は、情報の作成時又は情報を入手しその管理を開始する時に、当該情報について、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、その決定を行う（取扱制限の必要性の有無を含む。）こと。

【基準利用者への補足説明】
情報の格付け及び取扱制限を行うとは、情報の格付け及び取扱制限を決定し、指定することである。すなわち、情報システムで取り扱う情報について、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、当該情報が、どのように取り扱われるべきか、どのような対策が講じられるべきかを検討して、それぞれの定義のいずれに分類されるものであるのかを決定し、決定された格付け及び取扱制限を指定することが、格付け及び取扱制限の本質である。
決定に当たっての考え方を以下に例示する。
・機密性の格付けについては、秘密文書に相当する機密性を要する情報であり、[教職員等のうち、特定の者だけがアクセスできる状態を確保されるべき]情報は機密性３情報に、[教職員等以外がアクセスできない状態を確保されるべきであるが、特定の者に限定する必要がない]情報は機密性２情報に、それ以外の情報には、機密性１情報に決定する。
・完全性の格付けについては、情報が破壊、改ざん又は消去されていない状態を確保されるべき情報は完全性２情報に、それ以外の情報は、完全性１情報に決定する。
・可用性の格付けについては、情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保されるべき情報は可用性２情報に、それ以外の情報は可用性１情報に決定する。

4-1-2 決定に当たっての注意事項

部局情報化推進責任者が決定を行う場合：
(1) 部局情報化推進責任者は、格付け及び取扱制限の決定に当たっては、要件に過不足が生じないように注意すること。

教職員等が個々に決定を行う場合：
(2) 教職員等は、格付け及び取扱制限の決定に当たっては、要件に過不足が生じないように注意すること。

【基準利用者への補足説明】
格付け及び取扱制限として決定する要件が不十分であると、そのための情報セキュリティ対策が不十分となり、情報が適切に保護されなくなる。逆に、過度の要件を求めると、情報の保護が必要以上に厳しくなり、情報の利便性や有用性が損なわれる。そのため、

格付け及び取扱制限の決定をする際は、要件に過不足が生じないように注意しなければならない。
機密の情報（例えば、本来要機密情報とする情報）を要機密情報に格付けないことは不適切であるが、逆に、機密ではない情報（例えば、公開しても差し支えない情報）をむやみに要機密情報に格付けることも不適切であることに注意すること。

4-2 格付け及び取扱制限の指定

部局情報化推進責任者が決定を行う場合：
(1) 教職員等は、情報の作成時又は情報を入手しその管理を開始する時に、部局情報化推進責任者が策定した格付け及び取扱制限の判断例に基づき、格付け及び取扱制限の指定を行うこと。ただし、格付け及び取扱制限の判断例で規定されていない情報については、当該情報の作成時又は当該情報を入手しその管理を開始する時に、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、要件に過不足が生じないように注意した上でその決定をし、決定した格付け及び取扱制限に基づき、その指定を行うこと。

教職員等が個々に決定を行う場合：
(2) 教職員等は、決定した格付け及び取扱制限に基づき、その指定を行うこと。

4-3 格付け及び取扱制限の明示等

教職員等は、情報の格付け及び取扱制限を指定した場合には、それを認識できる方法を用いて明示等すること。

【基準利用者への補足説明】
情報の格付け及び取扱制限を指定した者が、当該情報に対して行う格付け及び取扱制限の明示等についての考え方は以下のとおり。
① 格付け及び取扱制限の明示の簡便化
「明示等」とは、情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示等に含むものとする。
② 取扱制限の明示を簡便化した場合における取扱制限の追加・変更

例えば、機密性３情報の取扱制限について事前に規定しておくことで、取扱制限の明記を省いて運用する方法を用いる場合、特定の機密性３情報について取扱制限を追加するときは、当該追加する取扱制限のみを明記し、逆に取扱制限を解除するときは、当該解除する取扱制限を「送信可」「印刷可」と明記することが想定される。
したがって、当該情報システムに記録される情報の格付け及び取扱制限を規定等により明記し、当該情報システムを利用するすべての者に当該規定が周知されていない場合（特に他大学に情報を提供等する場合）は、格付け及び取扱制限について記載しなければならない。
なお、記載が必須でない場合も、記載することによる問題がない限り、記載することが望ましい。

4-4 格付け及び取扱制限の継承

教職員等は、情報を作成する際に、参照した情報又は入手した情報が既に格付け又は取扱制限の指定がなされている場合には、元となる格付け及び取扱制限を継承すること。

【基準利用者への補足説明】
作成の際に参照した情報又は入手した情報が既に格付け又は取扱制限の指定がされている場合には、元となる格付け及び取扱制限を継承し、同一情報について一貫した対策を実施する必要がある。

4-5 格付け及び取扱制限の変更

【基準利用者への補足説明】
情報の格付け及び取扱制限は、情報システム運用基準に沿った対策を適正に実施するための基礎となる重要な事項であることについては、前記のとおりである。このため、これらを変更するに当たっても適正な手続により実施する必要がある。情報の格付け及び取扱制限の変更には、大別して再指定と見直しがあり、以下において、それぞれにつきその手順を示す。

4-5-1 格付け及び取扱制限の再指定

教職員等は、元の情報の修正、追加、削除のいずれかにより、他者が指定した情報の格付け及び取扱制限を再指定する必要があると思料する場合には、決定と指定の手順に従って処理すること。

【基準利用者への補足説明】
元の情報の修正、追加、削除のいずれかにより、格付け又は取扱制限を変更する必要が生じた場合には、格付け及び取扱制限の変更を行う必要がある。
　例えば、以下のような場合が考えられる。
・機密性の低い情報に機密性の高い情報を追加したことによって、情報の機密性が上がる場合
・機密性の高い情報から機密に該当する部分を削除したことによって、情報の機密性が下がる場合

4-5-2 格付け及び取扱制限の見直し

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

【基準利用者への補足説明】
元の情報への修正、追加、削除のいずれもないが、元の格付け又は取扱制限がその時点で不適当と考える場合には、格付け及び取扱制限の変更を行う必要がある。
　例えば、以下のような場合が考えられる。
・作成時には非公開だった情報が正規の手続によって公開されることで機密性が失われた場合（時間の経過により変化した場合）
・格付け及び取扱制限を決定したときの判断が不適切であったと考えられる場合
・取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合
・取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合

(2) 相談者又は被相談者は、情報の格付け及び取扱制限について見直しを行う必要性の有無を検討し、必要があると認めた場合には、当該情報に対して新たな格付け及び取扱制限を決定又は指定すること。
(3) 相談者又は被相談者は、情報の格付け及び取扱制限を見直した場合には、それ以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け及び取扱制限とならないように努めること。

(4) 教職員等は、自らが指定した格付け及び取扱制限を変更する場合には、その以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け及び取扱制限とならないように努めること。

【基準利用者への補足説明】
いずれの理由であっても、適正な格付け及び取扱制限がなされていない場合は、情報セキュリティ対策が適正に実施されないおそれが生ずるため、情報を利用する教職員等が、当該情報の格付けを変更する場合に、その指定者等に相談した上、妥当な格付けに変更する必要がある。なお、当初の格付けが指定者等によって不適正に設定されていれば、当該格付けを修正し、その旨を通知することによって、指定者等への教育的効果も期待できる。また、同一の情報が異なる格付け及び取扱制限とならないように、変更以前に当該情報を参照した者に対しても、格付け及び取扱制限が変更された旨を周知させることに努める必要がある。
なお、異動等の事由により、当該情報の指定者等と相談することが困難である場合においては、引継ぎを受けた者又は職場情報セキュリティ責任者に相談し、その是非を検討することになる。

4-5-3 変更後の指定者

情報の格付け及び取扱制限を変更する者は、変更後の格付け及び取扱制限の指定者について、変更前の指定者が継続するのか、変更者が新たに指定者となるのかについて明確にすること。

【基準利用者への補足説明】
変更後の格付け及び取扱制限の指定者は、再指定の場合には再指定をした者、見直しの場合には元の指定者が継続することを原則とするが、それ以外の場合には変更時点で明確にしておく必要がある。

5 既存の情報についての措置

5-1 既存の情報について

【基準利用者への補足説明】

本学における情報システム運用基準の施行日より以前の情報については、格付けと取扱制限は適宜実施することとしており、それらをすべて処理することは求めていない。
(1) 教職員等は、本基準の施行日以前に作成又は入手した情報を取り扱う場合には、当該情報の格付けを行うこと。
(2) 教職員等は、本基準の施行日以前に作成又は入手した情報を取り扱う場合には、取扱制限の必要性の有無を検討し、必要と認めるときは、それを行うこと。

【基準利用者への補足説明】
情報の格付け及び取扱制限の指定については、本学におけるポリシー及び実施基準の施行日以後に作成又は入手したすべての情報について適用するものであるが、施行日以前に作成又は入手した情報についても、適宜その指定を行うことが望ましい。
なお、施行日以前に作成又は入手した情報にあっては、これを取り扱う場合には、格付け及び取扱制限の指定を行う必要がある。

【付表】
文書の種類に基づく分類例

情報類型	格付け	取扱制限
公開前会議資料	機密性２情報 完全性２情報 可用性２情報	複製禁止、配付禁止
各部局協議	機密性２情報 完全性２情報 可用性２情報	暗号化必須
勉強会・研修会資料	機密性２情報 完全性２情報 可用性２情報	教職員等限り
ＨＰ掲載資料	機密性１情報 完全性２情報 可用性２情報	３日以内復旧、バックアップ必須
情報セキュリティ検査結果とりまとめ報告書	機密性２情報 完全性２情報 可用性２情報	５年間保存
個人等の秘密を侵害し、又は名誉、信用を損なうおそれのある情報	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ａシステムにおいて保存、書換禁止、保存期間満了後要廃棄

特定文書に対応させた分類例

文書類型	格付け	取扱制限
個人情報を含むパブリックコメント受領文書	機密性２情報 完全性２情報 可用性２情報	パブリックコメント終了後３年間保存
ポリシー及び実施基準	機密性１情報 完全性２情報 可用性２情報	作成後５年
未実施の各種試験問題案	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ｂシステムにおいて保存、書換禁止、削除禁止

大学活動の内容に基づく分類例

事務類型	格付け	取扱制限
○○○に関する事務において知り得た○○○の情報	機密性２情報 完全性２情報 可用性２情報	
非公開の会議において知り得た非公知の情報	機密性２情報 完全性２情報 可用性２情報	配付禁止、暗号化必須、書換禁止、削除禁止、関係者限り
未実施の各種試験問題作成に関する事務において知り得た情報	機密性３情報 完全性２情報 可用性２情報	複製禁止、配付禁止、暗号化必須、転送禁止、再利用禁止、送信禁止、関係者限り、Ｂシステムにおいて保存、書換禁止、削除禁止

A2201

国立大学法人群馬大学情報システム利用基準

平成２０年９月１８日制定
平成２１年３月１７日改正

１　目的

この基準は、国立大学法人群馬大学（以下「本学」という。）における情報システムの利用に関する事項を定め、情報セキュリティの確保と円滑な情報システムの利用に資することを目的とする。

２　定義

この基準において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

（１）　運用基本方針　本学が定めるA1000「 国立大学法人群馬大学情報システム運用基本方針」をいう。

（２）　運用統一基準　本学が定めるA1001「 国立大学法人群馬大学情報システム運用統一基準」をいう。

（３）　全学アカウント　本学の全学認証に対応した情報システムの利用に当たって用いるアカウントをいう。

（４）　その他の用語の定義は、運用基本方針及び運用統一基準で定めるところによる。

３　適用範囲

３－１　この基準は本学情報システム及びそれにかかわる情報を利用するすべての者に適用する。

３－２　本基準の情報システムには、本学ネットワークおよび本学内のすべてのコンピュータシステムが含まれる。ただし、事務情報システムについてはA2501「 事務情報セキュリティ対策基準」および事務情報システムに関するA3501 「各種マニュアル類の策定」に別途定める。

４　遵守事項

本学情報システムの利用者は、この基準及び本学情報システムの利用に関する手順及び本学個人情報保護規程を遵守しなければならない。

５　アカウントの申請

管理運営部局が運用する全学認証に対応する情報システムを利用する者は､情システム利用申請書を管理運営部局に提出し､アカウントの交付を受けなくてはならない｡全学認証に対応しない情報システムの利用者は､各情報システムの管理者からアカウントの交付を受ける｡

６　IDとパスワードによる認証の場合

利用者は、アカウントの管理に際して次の各号を遵守しなければならない。

（１）　利用者は、自分のユーザアカウントを他の者に使用させたり、他の者のユーザアカウントを使用したりしてはならない。

（２）　利用者は、他の者の認証情報を聞き出したり使用したりしてはならない。

（３）　利用者は、パスワードをA3205「 利用者パスワードガイドライン」に従って適切に管理しなければならない。

（４）　利用者は、使用中のコンピュータをロックあるいはログアウト（ログオフ）せずに長時間自らの席を離れてはならない。

（５）　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。

（６）　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｡ただし､全学認証システムに対応しない情報システムの利用者は、当該情報システムの管理者に報告する。

（７）　利用者は、システムを利用する必要がなくなった場合は、遅滞なく全学実施責任者に届け出なければならない｡ただし､個別の届出が必要ないと､あらかじめ全学実施責任者が定めている場合は、この限りでない。

全学認証システムに対応しない情報システムの利用者は当該情報システムの管理者に届け出る｡ただし､個別の届け出が必要ないと定められている場合は、この限りではない。

７　ICカードを用いた認証の場合

利用者は、ICカードの管理を以下のように徹底しなければならない。

（１）　ICカードを本人が意図せずに使われることのないように安全措置を講じて管理しなければならない。

（２）　ICカードを他者に付与及び貸与しないこと。

（３）　IC カードを紛失しないように管理しなければならない。紛失した場合には、直ちに全学実施責任者にその旨を報告しなければならない。但し、全学認証システムに対応しない情報システムの場合は当該 IC カードの発行者にその旨報告する。
（４）　IC カードを利用する必要がなくなった場合には、遅滞なく、これを全学実施責任者あるいは当該カードの発行者に返還しなければならない。
（５）　IC カード使用時に利用する PIN 番号を他に教えたりしてはならない。）

８　利用者による情報セキュリティ対策教育の受講義務

８－１　利用者は、毎年度１回は、年度講習計画に従って、本学情報システムの利用に関する教育を受講しなければならない。
８－２　教職員等（利用者）は、着任時、異動時に新しい職場等で、本学情報システムの利用に関する教育の受講方法について部局情報化推進責任者（部局長）に確認しなければならない。
８－３　教職員等（利用者）は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではないと思われる場合には、その理由について、部局情報化推進責任者（部局長）を通じて、全学実施責任者に報告しなければならない。
８－４　利用者は、情報セキュリティ対策の訓練に参加しなければならない。

９　自己点検の実施

利用者は、本学自己点検基準に基づいて自己点検を実施しなければならない。

１０　情報の格付け

教職員等は、情報格付け基準に従って、情報の格付け及び取扱いを行わなければならない。

１１　禁止事項

利用者は、本学情報システムについて、次の各号に定める行為を行ってはならない。
（１）　当該情報システム及び情報について定められた目的以外の利用
（２）　差別、名誉毀損、侮辱、ハラスメントにあたる情報の発信
（３）　個人情報やプライバシーを侵害する情報の発信
（４）　守秘義務に違反する情報の発信

（５）　著作権等の財産権を侵害する情報の発信
（６）　通信の秘密を侵害する行為
（７）　営業ないし商業を目的とした本学情報システムの利用
（８）　部局情報化推進責任者の許可（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
（９）　不正アクセス禁止法に定められたアクセス制御を免れる行為、またはこれに類する行為
（10）　部局情報化推進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
（11）　過度な負荷等により本学の円滑な情報システムの運用を妨げる行為
（12）　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
（13）　上記の行為を助長する行為
（14）　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
（15）　利用者は、ファイルの自動公衆送信機能を持ったP2Pソフトウェアについては、教育・研究目的以外にこれを利用してはならない。このようなP2Pソフトウェアを教育・研究目的に利用する場合は全学実施責任者の許可を得なければならない。

１２　違反行為への対処

１２－１　利用者の行為が前条に掲げる事項に違反すると被疑される行為と認められたときは、部局情報化推進責任者は速やかに調査を行い、事実を確認するものとする。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取しなければならない。
１２－２　部局情報化推進責任者は、上記の措置を講じたときは、遅滞無く全学総括責任者にその旨を報告しなければならない。
１２－３　調査によって違反行為が判明したときは、部局情報化推進責任者は全学総括責任者を通じて次の各号に掲げる措置を講ずること依頼することができる。
（１）　当該行為者に対する当該行為の中止命令
（２）　管理運営部局に対する当該行為に係る情報発信の遮断命令
（３）　管理運営部局に対する当該行為者のアカウント停止、または削除命令
（４）　本学懲罰委員会への報告
（５）　本学学則および就業規則に定める処罰
（６）　その他法令に基づく措置

１３　PC の利用

利用者は、様々な情報の作成、利用、保存等のための PC の利用にあたっては、別途定める A3201「 PC 取扱ガイドライン」に従い、これらの情報及び端末の適切な保護に注意しなければならない。

１４　電子メールの利用

利用者は、電子メールの利用にあたっては、別途定める A3202「 電子メール利用ガイドライン」および A3211「 学外情報セキュリティ水準低下防止手順」に従い、規則の遵守のみならずマナーにも配慮しなければならない。

１５　ウェブの利用および公開

１５－１　利用者は、ウェブブラウザを利用したウェブサイトの閲覧、情報の送信、ファイルのダウンロード等を行う際には、別途定める A3203「 ウェブブラウザ利用ガイドライン」および A3211「 学外情報セキュリティ水準低下防止手順」に従って、不正プログラムの感染、情報の漏えい、誤った相手への情報の送信等の脅威に注意するだけでなく、業務時間中における私的目的でのウェブの閲覧、掲示板への無断書き込みその他業務効率の低下や本学の社会的信用を失わせることのないよう注意しなければならない。

１５－２　利用者は、情報化推進室に許可を得た場合にウェブページを作成し、公開することができる。ウェブページの公開にあたって、A3204「 ウェブ公開ガイドライン」および A3211「 学外情報セキュリティ水準低下防止手順」に従いセキュリティや著作権等の問題および本学の社会的信用を失わせることのないように配慮しなければならない。

１５－３　利用者は、研究室等でウェブサーバを運用しようとする場合は、事前に情報化推進室に申請し、許可を得ていなければならない。

１５－４　利用者はウェブサーバを運用し情報を学外へ公開する場合は、A3107「 ウェブサーバ設定確認実施書(策定手引書)」に従ってサーバを設定しなければならない。

１５－５　ウェブページやウェブサーバ運用に関して、基準やガイドラインに違反する行為が認められた場合には、情報化推進室は公開の許可の取り消しやウェブコンテンツの削除を行うことがある。

１６　モバイル PC の利用

利用者は、モバイル PC その他の情報システムの学外の利用にあたっては以下の手順を遵守しなければならない。

（１）　要保護情報および要安定情報を記録したモバイル PC 等の情報システムを全学実施責任者、あるいは部局情報化推進責任者の許可なく学外に持ち出してはならない。これらの情報の持ち出しには、保護レベルに応じた管理（暗号化、パスワード保護、作業中の覗き見防止等）が必要である。

（２）　モバイル PC は可能な限り強固な認証システムを備え、ログ機能を持っていなければならない。また、それらの機能が設定され動作していなければならない。アンチウィルス・ソフトウェアが提供されているシステムでは、その機能が最新の状態でシステムを保護可能でなければならない。

（３）　モバイル PC の画面を他者から見える状態で利用してはならない。また、当該システムを他者が支配もしくは操作可能な状態にしてはならない。（不正操作、情報漏洩および盗難防止）

（４）　モバイル PC を本学情報システムに再接続する場合は、接続に先だってアンチウィルス・ソフトウェア等でスキャンを実行し、問題のあるソフトウェアが検出されないことを確認しなければならない。

（５）　モバイル PC 等の情報システムの紛失および盗難は、部局技術担当補佐に報告すること。

１７　学外の情報システムの持込および学外の情報システムからの利用

利用者は、学外の情報システムからの本学情報システムへのアクセスおよび学外の情報システムの本学ネットワークへの接続において、以下の手順を遵守しなければならない。

（１）　利用者は、学外の情報システムを用いての公開のウェブ以外の学内情報システムへのアクセスや学外の情報システムの本学ネットワークの接続にあたって、事前に全学実施責任者の許可を得なければならない。

（２）　これらの目的に利用する学外の情報システムは可能な限り強固な認証システムを備え、ログ機能を持っていなければならない。また、それらの機能が設定され動作していなければならない。アンチウィルス・ソフトウェアが提供されているシステムでは、その機能が最新の状態であって、システムを保護可能でなければならない。

（３）利用者は、これらの情報システムを許可された者以外に利用させてはならない。また、当該システムを他者が支配もしくは操作可能な状態にしてはならない。（不正操作、情報漏洩および盗難防止）
（４）　全学実施責任者の許可なく、これらの情報システムに要保護情報および要安定情報を複製保持してはならない。
（５）　これらの情報システムで動作するソフトウェアは正規のライセンスを受けたものでなければならない。

１８　安全管理義務

１８－１　利用者は、自己の管理するコンピュータについて、本学情報ネットワークとの接続状況に関わらず、安全性を維持する一次的な担当者となることに留意し、次の各号に定めるように、悪意あるプログラムを導入しないように注意しなければならない。
（１）　アンチウィルス・ソフトウェア等により不正プログラムとして検知される実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。
（２）　アンチウィルス・ソフトウェア等にかかわるアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。
（３）　アンチウィルス・ソフトウェア等による不正プログラムの自動検査機能を有効にしなければならない。
（４）　アンチウィルス・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。
（５）　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。
（６）　ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。
１８－２　利用者は、本学情報ネットワークおよびシステムの利用に際して、インシデントを発見したときは、A3103「インシデント対応手順」に従って行動するものとする。

１９　接続の許可

１９－１　利用者は、本学情報システムに新規に情報システム（コンピュータ）を接続しようとする場合は、事前に部局技術担当者と協議し、接続を行おうとする部局の部局情報化推進責任者に接続の許可を得なければならない。（ただし、情報コンセントからの本学情報システムへの一時的な接続はこの限りではない。）
１９－２　利用者は、本学基幹ネットワークを経由しないで、外部ネットワークと接続する場合には、全学実施責任者の許可を得なくてはならない。

１９－３　利用者は、VPN 等により本学ネットワークを通過し、外部ネットワークと接続する場合は、全学実施責任者の許可を得なくてはならない。

A2301

国立大学法人群馬大学情報セキュリティ年度講習計画

平成２０年９月１８日制定
平成２１年３月１７日改正

１　適用範囲

本文書は、以下の目的で実施される講習の年度計画について規定するものである。なお、いずれの講習とも、情報セキュリティ対策教育を単独で行う必要はなく、関連分野と合わせた講習の中で実施する形で差し支えない。

(1) 新たに大学の情報システムを利用することとなった学生、教職員等を対象とした、情報セキュリティ対策の基礎知識習得のための講習（以下、「基礎講習」と表記）

(2) (1)以外の利用者（教職員、学生等）を対象とした、最新状況への対応法等からなる情報セキュリティ対策の基礎知識習得のための講習（以下、「定期講習」と表記）

(3) 情報システム管理者を対象とした、運用に必要な情報セキュリティ対策の応用知識習得のための講習（以下、「システム管理者講習」と表記）

(4) 学長、全学総括責任者（CIO）、部局（部門）情報化推進責任者（部局長等）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理解するための講習（以下、「役職者講習」と表記）

なお、臨時職員、臨時利用者等、一時的に大学の設備を利用する利用者への教育については、本文書によらず、各利用者の利用条件に応じて必要かつ簡潔な教育を実施するものとし、本文書の適用範囲としない。

２　年度講習計画

年度講習計画を策定する場合には､対象者と実施時期に応じて以下の４種類を区別し、それぞれの区分について実施時期と教育する内容を定めること。

(1) 基礎講習：学生の場合は入学・編入学後の関連講義の初回、もしくは利用者講習会において、また教職員については着任後の講習会において、情報システムを利用する際の事故やトラブルの発生を予防するために､事前に理解しておくべき知識を集中的に教育するもの

(2) 定期講習：すでに(1)を習得済みの利用者に対し、習得状況の維持・確認や最新動向の教育などを目的として実施するもの

(3) システム管理者講習: 情報システムの管理者に対して、技術面を中心として、法令なども含めて実施するもの
(4) 役職者講習：本学における情報セキュリティの状況と、大学運営における情報セキュリティのあり方について実施するもの

３　計画例

(1) 基礎講習

情報セキュリティ対策の基礎知識だけでなく、法令、マナー、学内関連諸規程について併せて教育を実施する。

講習時期	講習内容	備考
4月～5月、および10月	A. 導入事項 ①事故から身を守るための知識 ・事故例と対策の必要性（導入として） ②利用規則と罰則 ・目的外利用の禁止 ・大学設備・環境の損壊、重大な影響を及ぼす行為の禁止 ・他利用者への迷惑行為の禁止 ・パスワード等の適正管理 ③学内情報システムの基本理念 ・言論の自由、学問の自由 ・他者の生命、安全、財産を侵害しない ・他者の人格の尊重 B. 情報セキュリティの基礎的知識 ・Internet のしくみ（IP address, URL, https） ・virus と worm（感染兆候と予防対策+事後対策） ・spyware（予防対策） ・情報発信(個人情報、責任、Accessibility) ・迷惑メール（対策） ・phishing、架空請求（しくみと注意喚起、	新入学生の情報倫理教育（「情報処理入門」授業の一環として実施）、中途入学者のための情報倫理教育、教職員の新規採用時教育としてA、B、C、Dについて実施する。

	対策） ・ファイル交換（情報漏洩、著作権） C. マナー・関連法令 ①法令の遵守 ・個人情報・秘密情報の保護 ・不正アクセス行為の禁止 ・著作権・肖像権 ②利用上のマナー ・社会慣行の尊重 ・ネットワーク利用のマナーの理解と尊重 ・運用への協力 ・ネット中毒 D. 便利な使い方 ・メール転送、Web メール ・学外から学内へのアクセス手段	

(2) 定期講習

最新の情報セキュリティ動向を教育するためのテキストを配布する。

講習時期	講習内容	備考
6 月～7 月	・最近の脅威の動向 ・主要な情報セキュリティ対策の確認	ｅラーニング形式により実施

(3) システム管理者講習

講義および、必要に応じて実習形式にて実施する。

講習時期	講習内容	備考
4 月～5 月	・システム管理の重要性 ・最低限知っておくべきセキュリティ対策 （各回カリキュラムによる）	e-ラーニング形式により実施

(4) 役職者講習

簡単な資料を用いてe-ラーニングあるいは短時間の報告により実施する。以下の計画のほか、重大インシデント発生の際には臨時で実施する。

役職	講習時期	講習内容	備考
学長	着任時及び年1回	・CIOによる本学の情報セキュリティ状況の報告（体制・対策、事例） ・テキスト：状況報告資料	学長への状況報告は、詳細状況よりも、統計及び重大インシデントの発生事例に重点を置く
全学総括責任者(CIO)	着任時及び必要のある場合随時	・大学運営における情報セキュリティのあり方 (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） ・重大インシデントの詳細な分析 (2) 情報セキュリティ対策に必要な措置 ・情報セキュリティ対策の必要性 ・情報セキュリティの責任体制 (3) 情報システムの構築・運用・インシデント対応 ・体制整備に関する課題 ・体制整備の方法 ・テキスト：メディアセンター教員が進講。A3303「 教育テキスト作成ガイドライン（CIO/役職者向け）」を参照	情報化推進室の会議、あるいはその打ち合わせ等の際に随時行うことによって代替することができる。
部局(部門)情報化推進責任者	着任時及び年1回	・部局（部門）情報化推進担当者が進講。総合情報メディアセンター教員が状況報告を補佐することができる。 ・テキスト：状況報告資料	状況報告にはケーススタディと統計がある。状況報告は必要に応じて秘密扱いとする。

A2401

国立大学法人群馬大学情報セキュリティ監査基準

平成２０年９月１８日制定
平成２１年３月１７日改正

１　目的

独立性を有する者による情報セキュリティ監査の実施基準を定めることにより、本学ポリシー、実施基準、及びそれに基づく手順が確実に遵守され、問題点が改善されることを目的とする。

２　監査計画の策定

情報セキュリティ監査責任者は、年度情報セキュリティ監査計画を策定し、全学総括責任者の承認を得る。

３　情報セキュリティ監査の実施に関する指示

３－１　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、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。
３－２　全学総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、情報セキュリティ監査責任者に対して、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示する。

４　個別の監査業務における監査実施計画の策定

情報セキュリティ監査責任者は、年度情報セキュリティ監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を策定する。

５　情報セキュリティ監査を実施する者の要件

５－１　情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した情報セキュリティ監査を実施する者に対して、監査の実施を依頼する。
５－２　情報セキュリティ監査責任者は、必要に応じて、本学外の者に監査の一部を請け負わせる。

６　情報セキュリティ監査の実施

６－１　情報セキュリティ監査を実施する者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施する。
６－２　情報セキュリティ監査を実施する者は、実施手順が作成されている場合には、それらが本ポリシーに準拠しているか否かを確認する。
６－３　情報セキュリティ監査を実施する者は、被監査部門における実際の運用が本ポリシー及び実施基準に基づく手順に準拠しているか否かを確認する。
６－４　情報セキュリティ監査を実施する者は、監査調書を作成し、あらかじめ定められた期間保存する。
６－５　情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、全学総括責任者へ提出する。

７　情報セキュリティ監査結果に対する対応

７－１　全学総括責任者は、監査報告書の内容を踏まえ、被監査部門の部局情報化推進責任者（部局長）に対して、指摘事案に対する対応の実施を指示する。
７－２　全学総括責任者は、監査報告書の内容を踏まえ、監査を受けた部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、他の部局の部局情報化推進責任者に対しても、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。
７－３　部局情報化推進責任者は、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。
７－４　全学総括責任者は、監査の結果を踏まえ、本ポリシー及び実施基準に基づく既存の手順の妥当性を評価し、必要に応じてその見直しを指示する。

A2501

国立大学法人群馬大学事務情報セキュリティ対策基準

平成２０年９月１８日制定
平成２１年３月１７日改正

目　次

第１部　総則

1-1 位置付け

国立大学法人群馬大学（以下、「本学」という。）の事務局管理の情報及び情報システムの情報セキュリティ強化のための基準である「国立大学法人群馬大学事務情報セキュリティ対策基準」（以下、本基準という。）は、平成 17 年 12 月 13 日に制定された「政府機関の情報セキュリティ対策のための統一基準」（以下、「政府統一基準」という。）に基づいて作成したものである。

1-2 目的

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

1-3 適用対象（情報の定義と対象者）

本基準が適用される対象範囲を以下のように定める。

（a）本基準は、「情報」を守ることを目的に作成されている。本基準において「情報」とは、情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。したがって、作業途上の文書も適用対象であり、書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる。

(b) 本基準は、事務局・事務部が扱う行政事務に関する特別規程である。教職員等のうち、事務局管理の行政事務に関する情報及び情報システムを取り扱う者に適用される。なお、本規程中と、一般規程が重複する場合は、本規程を優先する。

1-6 用語の定義

【あ】

＊「アクセス制御」とは、主体によるアクセスを許可する客体を制限することをいう。

＊「安全区域」とは、電子計算機及び通信回線装置を設置した事務室又はサーバルーム等の内部であって、部外者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。

＊「委託先」とは、情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を請け負った者をいう。

＊「受渡業者」とは、安全区域内で職務に従事する教職員等との物品の受渡しを目的とした者のことで、安全区域へ立ち入る必要のない者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

【か】

＊「外部委託」とは、情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を学外の者に請け負わせることをいう。

＊「外部記録媒体」とは、情報機器から取り外しすることが可能な記録装置（磁気テープ、磁気ディスク、光ディスク、カセットテープ、MO、フロッピーディスク及びUSBメモリ等）をいう。

＊「学外」とは、本学が管理する組織又は大学施設の外をいう。

＊「学外通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び本学管理又は他組織管理）及び通信回線装置を問わず、本学が管理していない電子計算機が接続され、当該電子計算機間の通信に利用する論理的な通信回線をいう。

＊「学外での情報処理」とは、本学の管理部外で職務の遂行のための情報処理を行うことをいう。なお、オンラインで学外から本学の情報システムに接続して、情報処置を行う場合だけではなく、オフラインで行う場合も含むものとする。

＊「学内」とは、本学が管理する組織又は施設の内をいう。

＊「学内通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び本学管理又は他組織管理）及び通信回線装置を問わず、本学が管理する電子計算機を接続し、当該電子計算機間の通信に利用する論理的な通信回線をいう。

＊「可用性」とは、情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。

＊「可用性１情報」とは、可用性２情報以外の情報（書面を除く。）をいう。

＊「可用性２情報」とは、職務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、研究・教育活動等に支障を及ぼす又は職務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
＊「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。
＊「完全性１情報」とは、完全性２情報以外の情報（書面を除く。）をいう。
＊「完全性２情報」とは、職務で取り扱う情報（書面を除く。）のうち、その改ざん、誤びゅう又は破損により、大学の運営に支障を及ぼす又は職務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
＊「機器等」とは、情報機器等及びソフトウェアをいう。
＊「機密性」とは、情報に関して、アクセスを認可された者だけがこれにアクセスできる状態を確保することをいう。
＊「機密性１情報」とは、機密性２情報又は機密性３情報以外の情報をいう。
＊「機密性２情報」とは、職務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報をいう。
＊「機密性３情報」とは、職務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報をいう。
＊「教職員等」とは、本学教職員及び本学の指示に服している者のうち、本学の管理対象である情報及び情報システムを取り扱う者をいう。
＊「共用識別コード」とは、複数の主体が共用することを想定した識別コードをいう。原則として、１つの識別コードは１つの主体のみに対して付与されるものであるが、情報システム上の制約や、利用状況などを考慮して、１つの識別コードを複数の主体で共用する場合もある。このように共用される識別コードを共用識別コードという。
＊「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）の付与及びアクセス制御における許可情報の付与を管理することをいう。
＊「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造・提供元等から公表されたセキュリティホール、セキュリティ関連機関から公表されたセキュリティホール等が該当する。

【さ】
＊「サービス」とは、サーバ装置上で動作しているアプリケーションにより、接続してきた電子計算機に対して提供される単独又は複数の機能で構成される機能群をいう。
＊「最少特権機能」とは、管理者権限を持つ識別コードを付与された者が、管理者としての業務遂行時に限定してその識別コードを利用させる機能をいう。
＊「識別」とは、情報システムにアクセスする主体を特定することをいう。

＊「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。
＊「主体」とは、情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。
＊「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、本基準における「主体認証」については、公的又は第三者による証明に限るものではない。
＊「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。
＊「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。
代表的な主体認証情報格納装置として、磁気テープカードやＩＣカード等がある。
＊「情報システム」とは、情報処理及び通信に係るシステムをいう。
＊「情報セキュリティ関係規程」とは、本基準及び本基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた実施手順をいう。
＊「情報の移送」とは、学外に、電磁的に記録された情報を送信すること並びに情報を記録した外部記録媒体、PC 及び書面を運搬することをいう。
＊「ソフトウェア」とは、電子計算機を動作させる手順及び命令を電子計算機が理解できる形式で記述したものをいう。オペレーティングシステム、オペレーティングシステム上で動作するアプリケーションを含む広義の意味である。

【た】
＊「対策用ファイル」とは、パッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイルをいう。
＊「端末」とは、端末を利用する教職員等が直接操作を行う電子計算機（オペレーティングシステム及び接続される周辺機器を含む。）であり、いわゆる PC のほか、PDA 等も該当する。
＊「通信回線」とは、これを利用して複数の電子計算機を接続し、所定の通信様式に従って情報を送受信するための仕組みをいう。回線及び通信回線装置の接続により構成さ

れた通信回線のことを物理的な通信回線といい、物理的な通信回線上に構成され、電子計算機間で所定の通信様式に従って情報を送受信可能な通信回線のことを論理的な通信回線という。
＊「通信回線装置」とは、回線の接続のために設置され、電子計算機により通信回線上を送受信される情報の制御を行うための装置をいう。いわゆるリピータハブ、スイッチングハブ及びルータのほか、ファイアウォール等も該当する。
＊「電子計算機」とは、コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。
＊「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄等をいう。

【は】
＊「複数要素（複合）主体認証（multiple factors authentication / composite authentication）方式」とは、知識、所有、生体情報などのうち、複数の方法の組合せにより主体認証を行う方法である。
＊「不正プログラム」とは、コンピュータウイルス、スパイウェア等の電子計算機を利用する者が意図しない結果を電子計算機にもたらすソフトウェアの総称をいう。
＊「不正プログラム定義ファイル」とは、アンチウイルスソフトウェア等が不正プログラムを判別するために利用するデータをいう。
＊「付与」（主体認証に係る情報、アクセス制御における許可情報等に関して）とは、発行、更新及び変更することをいう。
＊「本学支給以外の情報システム」とは、本学が支給する情報システム以外の情報システムをいう。いわゆる私物の PC のほか、本学への出向者に対して出向元組織が提供する情報システムも含むものとする。
＊「本学支給以外の情報システムによる情報処理」とは、本学支給以外の情報システムを用いて職務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことであり、例えば、本学の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。

【ま】
＊「明示」とは、情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により

明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示に含むものとする。
＊「モバイル PC」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動する端末をいう。特定の設置場所だけで利用するノート型 PC は、モバイル PC に含まれない。

【や】
＊「要安定情報」とは、可用性２情報をいう。
＊「要機密情報」とは、機密性２情報及び機密性３情報をいう。
＊「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。
＊「要保全情報」とは、完全性２情報をいう。

【ら】
＊「例外措置」とは、教職員等がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、職務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。
＊「ログイン」とは、何らかの主体が主体認証を要求する行為をいう。ログインの後に主体認証が行われるため、ログインの段階ではその主体が正当であるとは限らない。
＊「ログオン」とは、ログインの結果により、主体認証を要求した主体が正当であることが情報システムに確認された状態をいう。

第２部　組織と体制の構築

2-1　導入

2-1-1 組織・体制の確立

趣旨（必要性）

情報セキュリティ対策は、それに係るすべての教職員等が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を確立する必要がある。

これらのことを勘案し、本項では、情報セキュリティ対策に係る組織・体制に関する対策基準を定める。

【基本遵守事項】

(1) 全学総括責任者、情報化推進室、全学実施責任者、運用委員会、部門情報化推進担当者、情報セキュリティ監査責任者については情報システム運用基本規程に従う。

(5) 部門情報化推進責任者の設置

【基本遵守事項】

(a) 全学総括責任者は、情報セキュリティ対策の運用に係る管理を行う単位を定める。管理を行う単位を情報化推進室の部門情報システム運用委員会とし､情報化推進室員の中から部門運用委員会の委員長を選任する｡部門情報化推進責任者が部門情報システム運用委員会の委員長を兼ねることは妨げない。

(b) 部門情報化推進責任者は、所管する単位における情報セキュリティ対策に関する事務を統括すること。

(c) 部門情報化推進責任者は、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。

(6)部門技術担当者の設置

【基本遵守事項】

(a)部門情報化推進責任者は、所管する単位における情報システムごとに部門技術担当者を置くこと。部門技術担当者は、部門情報システム運用委員会の委員とする。

(b)部門技術担当者は、所管する情報システムに対する情報セキュリティ対策の管理に関する事務を統括すること。

(c)部門情報化推進責任者は、部門技術担当者を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。

(d) 全学実施責任者は、すべての部門技術担当者に対する連絡網を整備すること。

(7)部門技術担当補佐の設置

【基本遵守事項】

(a)部門技術担当者は、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門技術担当補佐を置くこと。

(b)部門技術担当補佐は、所管する管理業務における情報セキュリティ対策を実施すること。

(c)部門技術担当者は、部門技術担当補佐を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。

(d) 全学実施責任者は、すべての部門技術担当補佐に対する連絡網を整備すること。

(8) 職場情報セキュリティ責任者の設置

【基本遵守事項】

(a)部門情報化推進責任者は、各職場に職場情報セキュリティ責任者を1人置くこと。

(b) 職場情報セキュリティ責任者は、職場における情報セキュリティ対策に関する事務を統括すること。

(c)部門情報化推進責任者は、職場情報セキュリティ責任者を置いた時及び変更した時は、全学実施責任者にその旨を報告すること。

(d) 全学実施責任者は、すべての職場情報セキュリティ責任者に対する連絡網を整備すること。

2-1-2 役割の分離

趣旨（必要性）

情報セキュリティ対策に係る組織において、承認する者と承認される者が同一である場合や、監査する者と監査される者が同一である場合は、情報セキュリティが確保されていることが確認、証明されたことにはならない。情報セキュリティを確立するためには、兼務してはいけない役割が存在する。

これらのことを勘案し、本項では、情報セキュリティ対策に係る職務の分離に関する対策基準を定める。

遵守事項

(1) 兼務を禁止する役割の規定

【基本遵守事項】

(a) 情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。

（ア）承認又は許可事案の申請者とその承認者又は許可者

（イ）監査を受ける者とその監査を実施する者

2-1-3 違反と例外措置

趣旨（必要性）

本学において情報セキュリティを継続的に維持するためには、万一違反があった場合に、定められた手続に従って、適切に対応する必要がある。

また、情報セキュリティ関係規程の適用が職務の適正な遂行を著しく妨げる等の理由により、情報セキュリティ関係規程の規定とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合についても、あらかじめ定められた例外措置のための手続により、情報セキュリティを維持しつつ柔軟に対応できるものでなければ、当該規程の実効性を確保することが困難となる。

これらのことを勘案し、本項では、違反と例外措置に関する対策基準を定める。

遵守事項

(1) 違反への対応

【基本遵守事項】

(a) 教職員等は、情報セキュリティ関係規程への重大な違反を知った場合には、各規定の実施に責任を持つ部門情報化推進責任者にその旨を報告すること。

(b) 部門情報化推進責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を採らせること。

(c) 部門情報化推進責任者は、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。

(2) 例外措置

【基本遵守事項】

(a)情報化推進室は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）を定め、審査手続を整備すること。

(b) 教職員等は、例外措置の適用を希望する場合には、定められた審査手続に従い、許可権限者に例外措置の適用を申請すること。ただし、職務の遂行に緊急を要する等の場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定を実施しないことが不可避のときは、事後速やかに申請し許可を得ること。教職員等は、申請の際に以下の事項を含む項目を明確にすること。

（ア） 申請者の情報（氏名、所属、連絡先）

（イ）例外措置の適用を申請する情報セキュリティ関係規程の適用箇所（規程名と条項等）

（ウ） 例外措置の適用を申請する期間

（エ） 例外措置の適用を申請する措置内容（講ずる代替手段等）

（オ） 例外措置の適用を終了したときの報告方法

（カ） 例外措置の適用を申請する理由

(c) 許可権限者は、教職員等による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。また、決定の際に、以下の項目を含む例外措置の適用審査記録を整備し、全学総括責任者に報告すること。

（ア） 決定を審査した者の情報（氏名、役割名、所属、連絡先）

（イ） 申請内容

＊ 申請者の情報（氏名、所属、連絡先）

＊ 例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）

＊ 例外措置の適用を申請する期間

＊ 例外措置の適用を申請する措置内容（講ずる代替手段等）

＊ 例外措置の適用を終了した旨の報告方法

＊ 例外措置の適用を申請する理由

（ウ） 審査結果の内容

＊ 許可又は不許可の別

＊ 許可又は不許可の理由

＊ 例外措置の適用を許可した情報セキュリティ関係規程の適用箇所（規程名と条項等）

＊ 例外措置の適用を許可した期間

＊ 許可した措置内容（講ずるべき代替手段等）

＊ 例外措置を終了した旨の報告方法

(d) 教職員等は、例外措置の適用について許可を受け、例外措置を適用した場合には、それを終了したときに、当該例外措置の許可権限者にその旨を報告すること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

(e) 許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な対応を講ずること。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

(f) 全学総括責任者は、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査を実施する者からの求めに応ずること。

2-2　運用

2-2-1 情報セキュリティ対策の教育

趣旨（必要性）

情報セキュリティ関係規程が適正に策定されたとしても、教職員等にその内容が周知されず、教職員等がこれを遵守しない場合には、情報セキュリティ対策の水準の向上を望むことはできない。このため、すべての教職員等が、情報セキュリティ対策の教育を通じて、情報セキュリティ関係規程に関する理解を深め、情報セキュリティ対策を適切に実践できるようにすることが必要である。

これらのことを勘案し、本項では、情報セキュリティ対策の教育に関する対策基準を定める。

遵守事項

(1) 教職員等に対する情報セキュリティ対策教育の実施

【基本遵守事項】

(a) 全学実施責任者は、情報セキュリティ関係規程について、教職員等に対し、その啓発をすること。

(b) 全学実施責任者は、情報セキュリティ関係規程について、教職員等に教育すべき内容を検討し、教育のための資料を整備すること。

(c) 全学実施責任者は、教職員等が毎年度最低１回、受講できるように、情報セキュリティ対策の教育に係る計画を企画､立案するとともに､その実施体制を整備すること。

(d) 全学実施責任者は、教職員等の着任時、異動時に新しい職場等で３か月以内に受講できるように、情報セキュリティ対策の教育を企画、立案し、その体制を整備すること。

(e) 全学実施責任者は、教職員等の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備すること。

(f) 全学実施責任者は、教職員等の情報セキュリティ対策の教育の受講状況について、職場情報セキュリティ責任者に通知すること。

(g) 職場情報セキュリティ責任者は、教職員等の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告すること。教職員等が当該勧告に従わない場合には、全学実施責任者にその旨を報告すること。

(h) 全学実施責任者は、毎年度１回、全学総括責任者及び情報化推進室に対して、教職員等の情報セキュリティ対策の教育の受講状況について報告すること。

【強化遵守事項】
(i) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、全学実施責任者は、情報セキュリティ関係規程について、教職員等に対する情報セキュリティ対策の訓練の内容及び体制を整備すること。

(2) 教職員等による情報セキュリティ対策教育の受講義務
【基本遵守事項】
(a) 教職員等は、毎年度最低１回、情報セキュリティ対策の教育に関する計画に従って、情報セキュリティ対策の教育を受講すること。

(b) 教職員等は、着任時、異動時に新しい職場等で、情報セキュリティ対策の教育の受講方法について職場情報セキュリティ責任者に確認すること。

(c) 教職員等は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではないと思われる場合には、その理由について、職場情報セキュリティ責任者を通じて、全学実施責任者に報告すること。

【強化遵守事項】

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、教職員等は、情報セキュリティ対策の訓練に関する規定が定められている場合には、当該規定に従って、情報セキュリティ対策の訓練に参加すること。

2-2-2 障害等の対応

趣旨（必要性）

情報セキュリティに関する障害等が発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、障害等の影響や範囲を定められた責任者へ報告し、障害等の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。

これらのことを勘案し、本項では、障害等の発生時に関する対策基準を定める。

遵守事項

(1) 障害等の発生に備えた事前準備

【基本遵守事項】

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

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

(c) 全学実施責任者は、障害等が発生した際の対応手順を整備すること。

(d) 全学実施責任者は、障害等に備え、職務の遂行のため特に重要と認めた情報システムについて、その部門技術担当者及び部門技術担当補佐の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

【強化遵守事項】

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、全学実施責任者は、障害等について学外から報告を受けるための窓口を設置し、その窓口への連絡手段を学外に公表すること。

(2) 障害等の発生時における報告と応急措置

【基本遵守事項】

(a) 教職員等は、障害等の発生を知った場合には、それに関係する者に連絡するとともに、全学実施責任者が定めた報告手順により、部門情報化推進責任者にその旨を報告すること。

(b) 教職員等は、障害等が発生した際の対応手順の有無を確認し、それを実施できる場合には、その手順に従うこと。

(c) 教職員等は、障害等が発生した場合であって、当該障害等について対応手順がないとき及びその有無を確認できないときは、その対応についての指示を受けるまで、障害等による被害の拡大防止に努めること。指示があった場合には、その指示に従うこと。

(3) 障害等の原因調査と再発防止策

【基本遵守事項】

(a) 部門情報化推進責任者は、障害等が発生した場合には、障害等の原因を調査し再発防止策を策定し、その結果を報告書として全学総括責任者に報告すること。

(b) 全学総括責任者は、部門情報化推進責任者から障害等についての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずること。

2-3　評価

2-3-1 情報セキュリティ対策の自己点検

趣旨（必要性）

情報セキュリティ対策は、それに係るすべての教職員等が、各自の役割を確実に行うことで実効性が担保されるものであることから、すべての教職員等自らが情報セキュリティ関係規程に準拠した運用を行っているか否かについて点検することが重要であ

る。また、自己点検の結果に基づき、それぞれの当事者又はその管理者がその責任において、必要となる改善策を実施する必要がある。

これらのことを勘案し、本項では、自己点検に関する対策基準を定める。

遵守事項

(1) 自己点検に関する年度計画の策定

【基本遵守事項】

(a) 全学総括責任者は、年度自己点検計画を策定すること。

(2) 自己点検の実施に関する準備

【基本遵守事項】

(a) 部門情報化推進責任者は、教職員等ごとの自己点検票及び自己点検の実施手順を整備すること。

(3) 自己点検の実施

【基本遵守事項】

(a) 部門情報化推進責任者は、全学総括責任者が定める年度自己点検計画に基づき、教職員等に対して、自己点検の実施を指示すること。

(b) 教職員等は、部門情報化推進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。

(4) 自己点検結果の評価

【基本遵守事項】

(a) 部門情報化推進責任者は、教職員等による自己点検が行われていることを確認し、その結果を評価すること。

(b) 全学総括責任者は、部門情報化推進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。

(5) 自己点検に基づく改善

【基本遵守事項】

(a) 教職員等は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、部門情報化推進責任者にその旨を報告すること。

(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門情報化推進責任者に改善を指示すること。

2-3-2 情報セキュリティ対策の監査

趣旨（必要性）

情報セキュリティの確保のためには、情報セキュリティ関係規程が適切に運用されることによりその実効性を確保することが重要であって、実効性及び対策の妥当性の有無が確認されなければならない。そのためには、教職員等による自己点検だけでなく、独立性を有する者による情報セキュリティ監査を実施する必要である。

これらのことを勘案し、本項では、情報セキュリティ対策の監査に関する対策基準を定める。

遵守事項

(1) 監査計画の策定

【基本遵守事項】

(a) 情報セキュリティ監査責任者は、年度情報セキュリティ監査計画を策定し、全学総括責任者の承認を得ること。

(2) 情報セキュリティ監査の実施に関する指示

【基本遵守事項】

(a) 全学総括責任者は、年度情報セキュリティ監査計画に従って、情報セキュリティ監査責任者に対して、監査の実施を指示すること。

(b) 全学総括責任者は、情報セキュリティの状況の変化に応じて必要と判断した場合、情報セキュリティ監査責任者に対して、年度情報セキュリティ監査計画で計画された事案以外の監査の実施を指示すること。

(3) 個別の監査業務における監査実施計画の策定

【基本遵守事項】

(a) 情報セキュリティ監査責任者は、年度情報セキュリティ監査計画及び情報セキュリティの状況の変化に応じた監査の実施指示に基づき、個別の監査業務ごとの監査実施計画を策定すること。

(4) 情報セキュリティ監査を実施する者の要件

【基本遵守事項】

(a) 情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した情報セキュリティ監査を実施する者に対して、監査の実施を依頼すること。

(b) 情報セキュリティ監査責任者は、必要に応じて、教職員等以外の者に監査の一部を請け負わせること。

(5) 情報セキュリティ監査の実施

【基本遵守事項】

(a) 情報セキュリティ監査を実施する者は、情報セキュリティ監査責任者の指示に基づき、監査実施計画に従って監査を実施すること。

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

(c) 情報セキュリティ監査を実施する者は、被監査部門における実際の運用が情報セキュリティ関係規程に準拠しているか否かを確認すること。

(d) 情報セキュリティ監査を実施する者は、監査調書を作成し、あらかじめ定められた期間保存すること。

(e) 情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、全学総括責任者へ提出すること。

(6) 情報セキュリティ監査結果に対する対応

【基本遵守事項】

(a) 全学総括責任者は、監査報告書の内容を踏まえ、被監査部門の部門情報化推進責任者に対して、指摘事案に対する対応の実施を指示すること。

(b) 全学総括責任者は、監査報告書の内容を踏まえ、監査を受けた部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、他の部門の部門情報化推進責任者に対しても、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。

(c) 部門情報化推進責任者は、監査報告書に基づいて全学総括責任者から改善を指示された事案について、対応計画を作成し、報告すること。

(d) 全学総括責任者は、監査の結果を踏まえ、既存の情報セキュリティ関係規程の妥当性を評価し、必要に応じてその見直しを指示すること。

2-4　見直し

2-4-1 情報セキュリティ対策の見直し

趣旨（必要性）

情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティレベルは維持できなくなる。このため、情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、作成、導入、運用、評価の各段階において、適時見直しを行う必要がある。

これらのことを勘案し、本項では、情報セキュリティ対策の見直しに関する対策基準について定める。

遵守事項

(1) 情報セキュリティ対策の見直し

【基本遵守事項】

(a) 情報セキュリティ関係規程を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行うこと。

(b) 教職員等は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行うこと。

第３部　情報についての対策

3-1　情報の格付け

3-1-1 情報の格付け

趣旨（必要性）

職務で取り扱う情報については、その目的や用途により、取扱いに慎重を要する度合いは様々であり、その重要性に応じた適切な措置を講じ、確実に情報セキュリティを確保するために、情報の格付けが必要となる。

これらのことを勘案し、本項では、情報の格付けに関する対策基準を定める。

遵守事項

(1) 情報の格付け

【基本遵守事項】

(a) 情報化推進室は、職務で取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順を整備すること。

3-2　情報の取扱い

3-2-1 情報の作成と入手

趣旨（必要性）

職務においては、その事務の遂行のために複数の者が共通の情報を利用する場合がある。この際、利用者により当該情報の取扱いに関する認識が異なると、当該情報に応じた適切な情報セキュリティ対策が採られないおそれがあるため、情報を作成し又は入手した段階で、すべての利用者において認識を合わせるための措置が必要となる。

これらのことを勘案し、本項では、情報の作成及び入手に関する対策基準を定める。

遵守事項

(1) 業務以外の情報の作成又は入手の禁止

【基本遵守事項】

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

(2) 情報の作成又は入手時における格付けの決定と取扱制限の検討

【基本遵守事項】

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

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

(c) 教職員等は、未定稿の情報を決定稿にする際には、当該情報の格付けと取扱制限について、その妥当性の有無を再確認し、妥当でないと思われる場合には、これを行った者に相談することに努めること。相談された者は、格付けと取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな格付けと取扱制限を決定すること。

(3) 格付けと取扱制限の明示

【基本遵守事項】

(a) 教職員等は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示し、必要に応じて取扱制限についても明示すること。

(4) 格付けと取扱制限の継承

【基本遵守事項】

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

(5) 格付けと取扱制限の変更

【基本遵守事項】

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

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

3-2-2 情報の利用

趣旨（必要性）

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

これらのことを勘案し、本項では、情報の利用に関する対策基準を定める。

遵守事項

(1) 業務以外の利用の禁止

【基本遵守事項】

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

(2) 格付け及び取扱制限に従った情報の取扱い

【基本遵守事項】

(a) 教職員等は、利用する情報に明示された格付けに従って、当該情報を適切に取り扱うこと。格付けに加えて取扱制限の明示がなされている場合には、当該取扱制限の指示内容に従って取り扱うこと。

(3) 要保護情報の取扱い

【基本遵守事項】

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

(b) 教職員等は、要保護情報を放置しないこと。

(c) 教職員等は、機密性３情報を必要以上に複製しないこと。

(d) 教職員等は、要機密情報を必要以上に配付しないこと。

【強化遵守事項】

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、教職員等は、機密性３情報には、機密性３情報として取り扱う期間を明記すること。また、その期間中であっても、情報の格付けを下げる必要性があると思料される場合には、格付けの変更に必要な処理を行うこと。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、教職員等は、書面に印刷された機密性３情報には、一連番号を付し、その所在を明らかにしておくこと。

3-2-3 情報の保存

趣旨（必要性）

職務においては、その事務の継続性を確保するなどの必要性から情報を保存する場合があるが、情報の保存を続ける限り、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれも継続する。

これらのことを勘案し、本項では、情報の保存に関する対策基準を定める。

遵守事項

(1) 格付けに応じた情報の保存

【基本遵守事項】

(a) 部門技術担当者は、電子計算機に保存された要保護情報について、適切なアクセス制御を行うこと。

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

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

(d) 教職員等は、要機密情報を電子計算機又は外部記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

(e) 教職員等は、要保全情報を電子計算機又は外部記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。

(f) 教職員等は、要保全情報若しくは要安定情報である電磁的記録又は重要な設計書について、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること。

(g) 部門技術担当者は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書の複写の保管について、災害等への対策の必要性を検討し、必要があると認めたときは、同時被災等しないための適切な措置を講ずること。

(2) 情報の保存期間

【基本遵守事項】

(a) 教職員等は、電子計算機又は外部記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること。

3-2-4 情報の移送

趣旨（必要性）

職務においては、その事務の遂行のために他者又は自身に情報を移送する場合がある。移送の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部記録媒体の運搬及びPC、紙面に記載された情報の運搬等の方法が挙げられるが、いずれの方法を用いるにせよ、情報の移送により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになる。

これらのことを勘案し、本項では、情報の移送に関する対策基準を定める。

遵守事項

(1) 情報の移送に関する許可及び届出

【基本遵守事項】

(a) 教職員等は、機密性３情報を移送する場合には、職場情報セキュリティ責任者の許可を得ること。

(b) 教職員等は、機密性２情報を移送する場合には、職場情報セキュリティ責任者に届け出ること。

(2) 情報の送信と運搬の選択

【基本遵守事項】

(a) 教職員等は、要機密情報を移送する場合には、安全確保に留意して、送信又は運搬のいずれによるかを決定し、職場情報セキュリティ責任者に届け出ること。

(3) 移送手段の選択

【基本遵守事項】

(a) 教職員等は、要機密情報を移送する場合には、安全確保に留意して、当該要機密情報の移送手段を決定し、職場情報セキュリティ責任者に届け出ること。

(4) 書面に記載された情報の保護対策

【基本遵守事項】

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

(5) 電磁的記録の保護対策

【基本遵守事項】

(a) 教職員等は、要機密情報である電磁的記録を移送する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、情報にパスワードを設定すること。

(b) 教職員等は、要機密情報である電磁的記録を移送する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

【強化遵守事項】

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、教職員等は、要機密情報である電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いること。

3-2-5 情報の提供

趣旨（必要性）

職務においては、その事務の遂行のために教職員等以外の者に情報を提供する場合があるが、提供先における情報の不適切な取扱いにより、当該情報の漏えい又は不適切な利用等が発生するおそれがある。

これらのことを勘案し、本項では、情報の提供に関する対策基準を定める。

遵守事項

(1) 情報の公表

【基本遵守事項】

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

(b) 教職員等は、電磁的記録を公表する場合には、当該情報の付加情報等からの不用意な情報漏えいを防止するための措置を採ること。

(2) 他者への情報の提供

【基本遵守事項】

(a) 教職員等は、機密性３情報を教職員等以外の者に提供する場合には、職場情報セキュリティ責任者の許可を得ること。

(b) 教職員等は、機密性２情報を教職員等者以外の者に提供する場合には、職場情報セキュリティ責任者に届け出ること。

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

(d) 教職員等は、電磁的記録を提供する場合には、当該記録の付加情報等からの不用意な情報漏えいを防止するための措置を採ること。

3-2-6 情報の消去

趣旨（必要性）

職務において利用した電子計算機、通信回線装置及び外部記録媒体については、不要となった後、適切に処分されずに放置された場合には、盗難や紛失により、記録されている情報が漏えいするおそれがある。また、情報の消去を行っていたつもりでも、適切な措置が採られていなければ、復元ツールや復元サービス等を用いて当該情報を復元することが可能であり、情報漏えいのおそれは払拭されない。

これらのことを勘案し、本項では、情報の消去に関する対策基準を定める。

遵守事項

(1) 電磁的記録の消去方法

【基本遵守事項】

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

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

【強化遵守事項】

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

(2) 書面の廃棄方法

【基本遵守事項】

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

第４部　情報セキュリティ要件の明確化に基づく対策

4-1　情報セキュリティについての機能

4-1-1 主体認証機能

趣旨（必要性）

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権限のない者が、悪意又は過失により、情報の参照、改ざん又は消去を行うおそれがある。また、各主体及び情報システムにアクセスする者が各主体の識別と主体認証に関する情報の適切な取扱いに努めなければ、同様のおそれを招くことになる。

これらのことを勘案し、本項では、主体認証に関する対策基準を定める。

なお、本学が有する各情報システムの利用者は、教職員等のほか、それ以外の者がいる。例えば、学生や学外利用者向けのサービスを提供する情報システムの利用者は、教職員等以外の者である場合がある。識別コードと主体認証情報については、このような利用者の別にかかわらず保護すべきであるが、教職員等以外の者は本基準の適用範囲ではない。しかし、それらの者に対し、これを保護するよう注意喚起することが望ましい。

遵守事項

(1) 主体認証機能の導入

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、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、識別及び主体認証を行う機能を設けること。

(c) 部門技術担当補佐は、主体認証を行う必要があると認めた情報システムにおいて、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。
(ア) 主体認証情報を保存する場合には、その内容の暗号化を行うこと。
(イ) 主体認証情報を通信する場合には、その内容の暗号化を行うこと。
(ウ) 保存又は通信を行う際に暗号化を行うことができない場合には、利用者に自らの主体認証情報を設定、変更、提供（入力）させる際に、暗号化が行われない旨を通知すること。

(d) 部門技術担当者は、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、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。
(ア) 利用者が定期的に変更しているか否かを確認する機能
(イ) 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

(e) 部門技術担当者は、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。

(f) 部門技術担当者は、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、知識による主体認証方式を用いる場合には、以下の機能を設けること。
(ア) 利用者が、自らの主体認証情報を設定する機能

(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

(g) 部門技術担当者は、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、知識、所有、生体情報以外の主体認証方式を用いる場合には、以下の要件について検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たすこと。また、用いる方式に応じて、以下を含む要件を定めること。
(ア) 正当な主体以外の主体を誤って主体認証しないこと。（誤認の防止）

（イ）正当な主体が本人の責任ではない理由で主体認証できなくならないこと。（誤否の防止）
（ウ）正当な主体が容易に他者に主体認証情報を付与及び貸与ができないこと。（代理の防止）
（エ）主体認証情報が容易に複製できないこと。（複製の防止）
（オ）部門技術担当補佐の判断により、ログオンを個々に無効化できる手段があること。（無効化の確保）
（カ）主体認証について業務遂行に十分な可用性があること。（可用性の確保）
（キ）新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。（継続性の確保）
（ク）主体に付与した主体認証情報を使用することが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できること。（再発行の確保）

(h) 部門技術担当者は、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。

【強化遵守事項】
（i）特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、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。

（j）特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、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。

(k) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、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。

（l）特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、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。

(m) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、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。

(n) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、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。

(2) 教職員等における識別コードの管理

【基本遵守事項】

(a) 教職員等は、自己に付与された識別コード以外の識別コードを用いて、情報システムを利用しないこと。

(b) 教職員等は、自己に付与された識別コードを他者に付与及び貸与しないこと。

(c) 教職員等は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと。

(d) 教職員等は、職務のために識別コードを利用する必要がなくなった場合は、部門技術担当補佐に届け出ること。ただし、個別の届出が必要ないと、あらかじめ部門技術担当者が定めている場合は、この限りでない。

【強化遵守事項】

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、管理者権限を持つ識別コードを付与された者は、管理者としての業務遂行時に限定して、当該識別コードを利用すること。

(3) 教職員等における主体認証情報の管理

【基本遵守事項】

(a) 教職員等は、主体認証情報が他者に使用され又はその危険が発生した場合には、直ちに部門技術担当者又は部門技術担当補佐にその旨を報告すること。

(b) 主体認証情報が他者に使用され又はその危険が発生したことの報告を受けた部門技術担当者又は部門技術担当補佐は、必要な措置を講ずること。

(c) 教職員等は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。
（ア）自己の主体認証情報を他者に知られないように管理すること。

（イ）自己の主体認証情報を他者に教えないこと。

（ウ）主体認証情報を忘却しないように努めること。

（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。

（オ）部門技術担当補佐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。

(d) 教職員等は、所有による主体認証を用いる場合には、以下の管理を徹底すること。
（ア）主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理すること。
（イ）主体認証情報格納装置を他者に付与及び貸与しないこと。
（ウ）主体認証情報格納装置を紛失しないように管理すること。紛失した場合には、直ちに部門技術担当者又は部門技術担当補佐にその旨を報告すること。
（エ）主体認証情報格納装置を利用する必要がなくなった場合には、これを部門技術担当者又は部門技術担当補佐に返還すること。

4-1-2 アクセス制御機能

趣旨（必要性）

主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。

これらのことを勘案し、本項では、アクセス制御に関する対策基準を定める。

遵守事項

(1) アクセス制御機能の導入

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、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。

【強化遵守事項】

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(2) 教職員等による適正なアクセス制御

【基本遵守事項】

(a) 教職員等は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。

4-1-3 権限管理機能

趣旨（必要性）

主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになる。

これらのことを勘案し、本項では、権限管理に関する対策基準を定める。

遵守事項

(1) 権限管理機能の導入

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、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、権限管理を行う機能を設けること。

【強化遵守事項】

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、最少特権機能を設けること。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、主体認証情報の再発行を自動で行う機能を設けること。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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、デュアルロック機能を設けること。

解説：不正操作及び誤操作を防止するために、情報システムにデュアルロック機能を設けることを求める事項である。デュアルロック機能とは、行為に対して、少なくとも 2 名の者が操作しなければその行為を完遂できない方式のことである。

(2) 識別コードと主体認証情報の付与管理

【基本遵守事項】

(a) 部門技術担当者は、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、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。

(b) 部門技術担当者は、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、権限管理について、以下の事項を含む手続を明確にすること。

（ア）主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続
（イ）主体認証情報の初期配布方法及び変更管理手続
（ウ）アクセス制御情報の設定方法及び変更管理手続

(c) 部門技術担当者は、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、権限管理を行う者を定めること。

(d) 権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を発行すること。

(e) 権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、識別コードを発行する際に、それが共用識別コードか、共用ではない識別コードかの区別を利用者に通知すること。ただし、共用識別コードは、部門技術担当者が、その利用を認めた情報システムでのみ付与することができる。

(f) 権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、管理者権限を持つ識別コードを、業務又は業務上の責務に即した場合に限定して付与すること。

(g) 権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、教職員等が情報システムを利用する必要がなくなった場合には、当該教職員等の識別コードを無効にすること。また、人事異動等、識別コードを追加又は削除する時に、不要な識別コードの有無を点検すること。

(h) 権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、教職員等が情報システムを利用する必要がなくなった場合には、当該教職員等に交付した主体認証情報格納装置を返還させること。

(i) 権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス制御に係る設定をすること。また、人事異動等、識別コードを追加又は削除する時に、不適切なアクセス制御設定の有無を点検すること。

【強化遵守事項】

(j) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、単一の情報システムにおいては、１人の教職員等に対して単一の識別コードのみを付与すること。

解説：デュアルロック機能を備えた情報システムでは、１人の教職員等に複数の識別コードでの主体認証を許してしまうと、デュアルロック機能による強化が万全とならないことから、１人の教職員等に対して単一の識別コードのみを付与することを求める事項である。

(k) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードをどの主体に付与していたかの記録について、保存すること。当該記録を消去する場合には、部門情報化推進責任者からの事前の承認を得ること。

(l) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、権限管理を行う者は、権限管理を行う必要があると認めた情報システムにおいて、ある主体に付与した識別コードをその後別の主体に対して付与しないこと。

(3) 識別コードと主体認証情報における代替措置の適用

【基本遵守事項】

(a) 部門技術担当補佐は、権限管理を行う必要があると認めた情報システムにおいて、付与した識別コードが使用できなくなった教職員等から、代替手段の使用に関する許可申請を受けた場合には、その申請者が正当な利用者であることを確認した上で、その必要性の有無を検討し、必要があると認めたときは、代替手段を提供すること。

(b) 部門技術担当者及び部門技術担当補佐は、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。

4-1-4 証跡管理機能

趣旨（必要性）

情報システムの利用においては、当該情報システムの制御及び管理の実効性を高め、また情報セキュリティに関する問題が発生した場合にこれに適切に対処するために、当該情報システムの動作及びその他必要な事象を記録し、事後にこれを調査する証跡管理を行う必要がある。また、証跡管理により、外部又は内部の者による不正利用又は過失行為を事前に抑止し、また事後に追跡することが可能となる。

これらのことを勘案し、本項では証跡管理に関する対策基準を定める。

遵守事項

(1) 証跡管理機能の導入

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。

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

(d) 部門技術担当者は、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、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方針を整備し、必要に応じ、これらの場合に対応するための機能を情報システムに設けること。

(e) 部門技術担当者は、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、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行い、外部記録媒体等その他の装置・媒体に記録した証跡についてはこれを適正に管理すること。

【強化遵守事項】

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、取得した証跡管理情報の内容により、情報セキュリティ侵害の可能性を示す事象を検知した場合に、監視要員等にその旨を即時に通知する機能を情報システムに設けること。

(2) 部門技術担当補佐による証跡の取得と保存

【基本遵守事項】

(a) 部門技術担当補佐は、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、部門技術担当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。

(b) 部門技術担当補佐は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間を定め、当該保存期間が満了する日まで証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。保存期間は、学外にアクセスする情報システムにおいては３ヶ月以上とし、特に重要な情報を取り扱う情報システムにおいては１年以上として定めること。

(c) 部門技術担当補佐は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処を行うこと。

(3) 取得した証跡の点検、分析及び報告

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門情報化推進責任者又は部門技術担当者は、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、取得した証跡を定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講じ、又はそれぞれ全学実施責任者若しくは部門情報化推進責任者に報告すること。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、監視要員等は、セキュリティ侵害の可能性を示す事象を検知した旨の通知を受けた場合には、あらかじめ定められた措置を採ること。

(4) 証跡管理に関する利用者への周知

【基本遵守事項】

(a) 部門情報化推進責任者又は部門技術担当者は、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、部門技術担当補佐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。

4-1-5 保証のための機能

趣旨（必要性）

本基準では、基本的なセキュリティ機能として、主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能の各項で具体的に遵守事項を規定している。しかし、情報が適切な状態であることを保証するためには、これらの機能のこれらの機能による情報セキュリティ対策より上位の機能やそれ以外の機能等による対策全般についても導入の必要性を検討することが重要である。こうした対策は、限られた情報システムに導入されることになると考えるが、基本的な対策ではないから最初から除外するのではなく、必要性の有無を確認し選択的に導入するという対応が適切である。

これらのことを勘案し、本項では、保証のための機能に関する対策基準を定める。

遵守事項

(1) 保証のための機能の導入

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、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。

4-1-6　暗号と電子署名（鍵管理を含む）

趣旨（必要性）

情報システムの利用においては、当該情報システムで取り扱う情報の漏えいや改ざん等を防ぐために、情報の暗号化及び電子署名の付与が有効とされている。

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

遵守事項

(1) 暗号化機能及び電子署名の付与機能の導入

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、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。

(c) 部門技術担当者は、要保全情報を取り扱う情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討すること。

(d) 部門技術担当者は、電子署名の付与を行う必要があると認めた情報システムには、電子署名の付与を行う機能を設けること。

(e) 部門技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リスト又は、本学における検証済み暗号リストがあればその中から選択すること。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つをそれらのリストの中から選択すること。

【強化遵守事項】

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号モジュールを、交換ができるようにコンポーネント化して構成すること。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、複数のアルゴリズムを選択可能とすること。

(h) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、選択したアルゴリズムが、ソフトウェアやハードウェアへ適切に実装されているか否かを確認すること。

(i) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報（書面を除く。以下この項において同じ。）の復号又は電子署名の付与に用いる鍵を、第三者による物理的な攻撃から保護するために、耐タンパー性を有する暗号モジュールへ格納すること。

(2) 暗号化及び電子署名の付与に係る管理

【基本遵守事項】

(a) 部門技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対応手順等を定めること。

(b) 部門技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の保存媒体及び保存場所を定めること。

(c) 部門技術担当者は、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。

【強化遵守事項】

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、暗号化を行う必要があると認めた情報システムにおいて、暗号化された情報の復号に用いる鍵のバックアップの取得方法又は鍵の預託方法を定めること。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、暗号化又は電子署名の付与を行う必要があると認めた場合、当該情報システムにおいて選択されたアルゴリズムの危殆化に関する情報を適宜入手すること。

(3) 暗号化機能及び電子署名の付与機能の利用

【基本遵守事項】

(a) 教職員等は、要機密情報を移送する場合又は電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

(b) 教職員等は、要保全情報を移送する場合又は電磁的記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること。

(c) 教職員等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、これを他者に知られないように自己管理すること。

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

4-2　情報セキュリティについての脅威

4-2-1 セキュリティホール対策

趣旨（必要性）

セキュリティホールは、情報システムを構成する電子計算機及び通信回線装置上で利用しているソフトウェアに存在する可能性があり、そのセキュリティホールを攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、ウイルス感染等の脅威の発生原因になるなど、情報システム全体のセキュリティの大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、本学の社会的な信用が失われるおそれがある。これらのリスクを回避するため、セキュリティホールへの対応は迅速かつ適切に行わなければならない。

これらのことを勘案し、本項では、セキュリティホールに関する対策基準を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

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

(b) 部門技術担当補佐は、電子計算機及び通信回線装置の構築又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施すること。

【強化遵守事項】
(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、公開されたセキュリティホールの情報がいない段階においても電子計算機及び通信回線装置上でその対策を実施すること。

(2) 情報システムの運用時
【基本遵守事項】
(a) 部門技術担当補佐は、電子計算機及び通信回線装置の構成に変更があった場合には、セキュリティホール対策に必要となる機器情報を記載した書面を更新すること。

(b) 部門技術担当補佐は、管理対象となる電子計算機及び通信回線装置上で利用しているソフトウェアに関連する公開されたセキュリティホールに関連する情報を適宜入手すること。

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

（カ）対策テストの必要性
（キ）対策テストの方法
（ク）対策テストの実施予定

(d) 部門技術担当補佐は、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。

(e) 部門技術担当補佐は、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。

(f) 部門技術担当補佐は、信頼できる方法で対策用ファイルを入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

(g) 部門技術担当補佐は、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。

(h) 部門技術担当者責任者は、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、他の部門技術担当者責任者と共有すること。

4-2-2　不正プログラム対策

趣旨（必要性）

不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の秘密情報や業務上の機密情報を漏えいさせることから機密性に対する脅威ともなる。

さらに、不正プログラムに感染した情報システムは、他の情報システムの再感染を引き起こす危険性のほか、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される危険性など他者に対するセキュリティ脅威の原因となり得る。

これらのことを勘案し、本項では、不正プログラムに関する対策基準を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

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

(b) 部門技術担当者責任者は、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。

(c) 部門技術担当者責任者は、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。

【強化遵守事項】

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者責任者は、想定される不正プログラムの感染経路において、異なる業者のアンチウイルスソフトウェア等を組み合わせ、導入すること。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者責任者は､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。

(2) 情報システムの運用時

【基本遵守事項】

(a) 部門技術担当補佐は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、教職員等にその対処の実施に関する指示を行うこと。

(b) 教職員等は、アンチウイルスソフトウェア等により不正プログラムとして検知される実行ファイルを実行せず､データファイルをアプリケーション等で読み込まないこと。

(c) 教職員等は、アンチウイルスソフトウェア等にかかわるアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。

(d) 教職員等は、アンチウイルスソフトウェア等による不正プログラムの自動検査機能を有効にすること。

(e) 教職員等は、アンチウイルスソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること。

(f) 教職員等は、外部からデータやソフトウェアを電子計算機等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

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

(h) 部門情報化推進責任者は、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。

【強化遵守事項】

(i) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門情報化推進責任者は、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。

4-2-3 サービス不能攻撃対策

趣旨（必要性）

インターネットを経由して外部に提供しているサービスを実現する電子計算機、並びにそのアクセスに利用される通信回線及び通信回線装置は、利用者が自由にアクセス可能である利便性を確保するために、サービス不能攻撃により、通常の利用者がサービスを利用できなくなるといった可用性に対するリスクがある。また、インターネットに接続しているサーバ装置及び端末は、不正プログラム感染又は不正侵入等により、管理者が意図しないにもかかわらず他者へサービス不能攻撃を行ってしまうおそれがある。

このため、インターネットに接続しているサーバ装置、並びにそのアクセスに利用される通信回線及び通信回線装置については、高い可用性を維持するための対策が必要となる。

これらのことを勘案し、サービス不能攻撃に関する対策基準を定める。

遵守事項

(1) 情報システムの構築時

【基本遵守事項】

(a) 部門技術担当者責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける電子計算機、通信回線装置又は通信回線を有する情報システム。以下この項において同じ。）については、サービス提供に必要な電子計算機及び通信回線装置が装備している機能をサービス不能攻撃対策に活用すること。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者責任者は、サービス不能攻撃を受けた場合、通信回線装置や通信回線を共用している他サービスや内部からのインターネットへのアクセスにも影響が及ぶことを考慮して通信回線装置及び通信回線の構築を行うこと。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受ける電子計算機、通信回線装置又は通信回線から監視対象を特定し、監視方法を定めること。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、電子計算機や通信回線装置だけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し､インター

ネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を定めておくこと。

(2) 情報システムの運用時

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当補佐は、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。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、前事項の記録をサービス不能攻撃の検知技術の向上に反映すること。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、定期的にサービス不能攻撃の対策の見直しを行うこと。

4-3　情報システムのセキュリティ要件

4-3-1 情報システムのセキュリティ要件

趣旨（必要性）

情報システムは、目的業務を円滑に遂行するため、その計画、設計、構築、運用、監視、移行、廃棄及び見直しのライフサイクルを通じて様々な要件を満たすことが必要である。その要件の中にはセキュリティの観点からの要件も含まれ、情報システムのライフサイクルにあわせて情報セキュリティ対策を実施する必要がある。

これらのことを勘案し、本項では、情報システムのライフサイクルの視点に立ち、各段階において考慮すべき情報セキュリティの対策基準を定める。

遵守事項

(1) 情報システム計画・設計

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、情報システムのセキュリティ要件を決定すること。

(c) 部門技術担当者は、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。

(d) 部門技術担当者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価・ST 確認を受けること。ただし、情報システムを更改する場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

(e) 部門技術担当者は、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。

【強化遵守事項】

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該機能及びその他の要求条件を満たす採用候補製品が複数ある場合には、その中から当該セキュリティ機能に関して IT セキュリティ評価及び認証制度に基づく認証を取得している製品を情報システムの構成要素として選択すること。

(2) 情報システムの構築・運用・監視

【基本遵守事項】

(a) 部門技術担当者は、情報システムの構築、運用及び監視に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行うこと。

(3) 情報システムの移行・廃棄

【基本遵守事項】

(a) 部門技術担当者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を採ること。

(4) 情報システムの見直し

【基本遵守事項】

(a) 部門技術担当者は、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。

第５部　情報システムの構成要素についての対策

5-1　施設と環境

5-1-1 電子計算機及び通信回線装置を設置する安全区域

趣旨（必要性）

電子計算機及び通信回線装置の設置環境について、悪意を持った者が電子計算機及び通信回線装置に物理的に接触できる状況においては、なりすまし、物理的な装置の破壊のほか、情報の漏えい又は改ざんが行われるおそれがある。また、設置環境に関する脅威としては、自然災害の発生により情報システムが損傷する等のおそれもある。

これらのことを勘案し、本項では、安全区域に関する対策基準を定める。

遵守事項

(1) 立入り及び退出の管理

【基本遵守事項】

(a) 部門技術担当者は、安全区域に不審者を立ち入らせない措置を講ずること。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、安全区域をセキュリティレベルが異なる区域から物理的に隔離し、立入り及び退出が可能な場所を制限する措置を講ずること。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、安全区域へ立ち入る者の主体認証を行うための措置を講ずること。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、安全区域から退出する者の主体認証を行うための措置を講ずること。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、主体認証を経た者が、主体認証を経ていない者を安全区域へ立ち入らせ、及び安全区域から退出させない措置を講ずること。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、安全区域へ継続的に立ち入る者を承認する手続を整備すること。また、その者の氏名、所属、立入承認日、立入期間及び承認事由を含む事項を記載した書面を整備すること。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、安全区域へ立入りが承認された者に変更がある場合には、当該変更の内容を前事項の書面へ反映させること。また、当該変更の記録を保存すること。

(h) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(2) 訪問者及び受渡業者の管理

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、安全区域への訪問者がある場合には、訪問相手の教職員等が訪問者の安全区域への立入りについて審査するための手続を整備すること。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、安全区域内において訪問相手の教職員等が訪問者に付き添うための措置を講ずること。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講ずること。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、受渡業者と物品の受渡しを行う場合には、以下に挙げるいずれかの措置を講ずること。
(ア) 安全区域外で受渡しを行うこと。
(イ) 業者が安全区域へ立ち入る場合は、当該業者が安全区域内の電子計算機、通信回線装置、外部記録媒体、書面に触れることができない場所に限定し、教職員等が立ち会うこと。

(3) 電子計算機及び通信回線装置のセキュリティ確保
【強化遵守事項】
(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要保護情報を取り扱う情報システムについては、設置及び利用場所が確定している電子計算機及び通信回線装置を所定の設置場所から移動できない措置を講ずること。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、教職員等が離席時に電子計算機及び通信回線装置を不正操作から保護するための措置を講ずること。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(4) 安全区域内のセキュリティ管理

【基本遵守事項】

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

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、教職員等は、要保護情報を取り扱う情報システムについては、部門技術担当者の承認を得た上で、情報システムに関連する物品の安全区域への持込み及び安全区域からの持出しを行うこと。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要保護情報を取り扱う情報システムについては、安全区域への持込み及び安全区域からの持出しについて、持込み及び持出しに係る記録を取得すること。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要機密情報を取り扱う情報システムについては、情報システムに関連しない電子計算機、通信回線装置、外部記録媒体及び記録装置（音声、映像及び画像を記録するものを含む。）の安全区域への持込みについて制限すること。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(5) 災害及び障害への対策

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

5-2 電子計算機

5-2-1 電子計算機共通対策

趣旨（必要性）

電子計算機の利用については、ウイルス感染や不正侵入を受ける等の外部的要因により、保存されている情報の漏えい若しくは改ざん又は当該電子計算機の機能停止等の被害に遭うおそれがある。また、職員の不適切な利用等の内部的要因による情報セキュリティの侵害も起こり得る。このように電子計算機の利用は、当該電子計算機及び当該電子計算機が取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、電子計算機に関する対策基準を定める。

遵守事項

(1) 電子計算機の設置時

【基本遵守事項】

(a) 部門技術担当者は、電子計算機のセキュリティ維持に関する規定を整備すること。

解説：電子計算機に関する対策について定めることを求める事項である。

「電子計算機のセキュリティ維持に関する規定」とは、主体認証、アクセス制限及び情報システムの保守に関する目的、対象とする機器の範囲、管理する教職員等及び利用者の役割及び責任のほか、端末の利用許可、モバイル PC の持出許可、利用者の識別コードの管理方法及び主体認証情報の管理方法並びに接続可能通信回線及びセキュリティ

設定等の手順を整備する規定である。部局技術責任者の所管する単位ごとに規定を整備することが原則であるが、当該規定の内容を変更する必要がない場合には複数の実施単位で共通に整備する等状況に応じていずれかの方法を選択することが可能である。

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

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

(c) 部門技術担当者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見通しを含め検討し、確保すること。

(d) 部門技術担当者は、利用者が電子計算機にログインする場合には主体認証を行うように電子計算機を構成すること。

(e) 部門技術担当者は、ログオンした利用者の識別コードに対して、権限管理を行うこと。

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

(g) 部門技術担当者は、不正プログラムから電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しないものを除く。）を保護するための対策を講ずること。

(h) 部門技術担当者は、電子計算機関連文書を整備すること。

解説：電子計算機と関連文書の整合性を確保するための事項である。
「電子計算機関連文書」とは、電子計算機の設計書、仕様書及び操作マニュアル等である。書面ではなく電磁的記録媒体で整備していても差し支えない。

(i) 部門技術担当者は、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 について部門情報化推進責任者の承認を得た場合は、この限りでない。

【強化遵守事項】

(j) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

(2) 電子計算機の運用時

【基本遵守事項】

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

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

(c) 教職員等は、職務の遂行以外の目的で電子計算機を利用しないこと。

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

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

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

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

【強化遵守事項】

(h) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は､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。

(3) 電子計算機の運用終了時

【基本遵守事項】

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

5-2-2 端末

趣旨（必要性）

端末については、当該端末を利用する者が専門的知識を有していない場合が多いことから、当該利用者の過失によるウイルス感染等のリスクが高い。また、可搬性の高い端末については、紛失又は盗難のリスクも高くなる。

このように端末の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、端末に関する対策基準を定める。

遵守事項

(1) 端末の設置時

【基本遵守事項】

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

(b) 部門技術担当者は、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。

(c) 教職員等は、モバイル PC を利用する必要がある場合には、部門技術担当者の承認を得ること。

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

(e) 部門技術担当者は、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。

【強化遵守事項】
(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、教職員等が情報を保存できない端末を用いて情報システムを構築すること。

(2) 端末の運用時

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

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

(c) 教職員等は、要機密情報を取り扱うモバイル PC については、モバイル PC を学外に持ち出す場合に、当該モバイル PC の内蔵記録媒体に保存されている要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

(d) 教職員等は、部門技術担当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。

【強化遵守事項】
(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当補佐は、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。

5-2-3 サーバ装置

趣旨（必要性）

サーバ装置については、当該サーバ装置の内蔵記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は改ざんによる影響も端末と比較して大きなものとなる。

また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、ウイルス感染や不正侵入等を受けるリスクが高い。本学が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、学外の人々からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。

このようにサーバ装置の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、サーバ装置に関する対策基準を定める。

遵守事項

(1) サーバ装置の設置時

【基本遵守事項】

(a) 部門技術担当者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報を暗号化すること。

(b) 部門技術担当者は、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。

(c) 部門技術担当者は、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。

【強化遵守事項】

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(2) サーバ装置の運用時

【基本遵守事項】

(a) 部門技術担当者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対応すること。

(b) 部門技術担当補佐は、要安定情報を取り扱うサーバ装置に保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理すること。

(c) 部門技術担当補佐は、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。

(d) 部門技術担当者は、サーバ装置上で証跡管理を行う必要性を検討し、必要と認めた場合には実施すること。

(e) 部門技術担当補佐は、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。

【強化遵守事項】

(f) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当補佐は、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。

(g) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当補佐は、要安定情報を取り扱うサーバ装置について、当該サーバ装置のシステム状態を監視し、当該サーバ装置に関するトラブルの発生を検知すること。

(h) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当補佐は、要安定情報を取り扱うサーバ装置について、サービス提供に必要なサーバ装置の負荷を複数のサーバ装置に分散すること。

5-3　アプリケーションソフトウェア

5-3-1 通信回線を介して提供するアプリケーション共通対策

趣旨（必要性）

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

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

遵守事項

(1) アプリケーションの導入時

【基本遵守事項】

(a) 部門技術担当者は、通信回線を介して提供するサービスのセキュリティ維持に関する規定を整備すること。

(2) アプリケーションの運用時

【基本遵守事項】

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

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

5-3-2 電子メール

趣旨（必要性）

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいする等の機密性に対するリスクがある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれる等の可用性に対するリスクがある。この他、内容を偽ったメールによるいわゆるフィッシング詐欺等に電子メールを利用する教職員等が巻き込まれるリスクもある。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要である。

これらのことを勘案し、本項では、電子メールサーバの管理及び電子メールの利用に関する対策基準を定める。

遵守事項

(1) 電子メールの導入時

【基本遵守事項】

(a) 部門技術担当者は、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。

【強化遵守事項】

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、電子メールクライアントから電子メールサーバへの電子メールの送受信時における教職員等の主体認証を行う機能を備えること。

(2) 電子メールの運用時

【基本遵守事項】

(a) 教職員等は、業務遂行にかかわる情報を含む電子メールを送受信する場合には、本学が運営又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。ただし、本学支給以外の情報システムによる情報処理について許可を得ている者については、この限りでない。

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

5-3-3 ウェブ

趣旨（必要性）

ウェブにおいては、様々なアプリケーション、データを組み合わせた情報を送受信すること、また IP ネットワークにおいて標準的に利用されるシステムとして一般的に普及していること等の理由により、セキュリティ脅威全般に係るリスクが考えられる。これらのリスクを回避するためには、システムのライフサイクル全般に対して適切な対策を施すことが必要である。

これらのことを勘案し、本項では、ウェブに関する対策基準を定める。

遵守事項

(1) ウェブの導入時

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、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。

(c) 部門技術担当者は、要機密情報を取り扱う情報システムについては、ウェブサーバを用いて提供するサービスにおいて、通信の盗聴から保護すべき情報を特定し、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

【強化遵守事項】
(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(e) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(2) ウェブの運用時
【基本遵守事項】
(a) 教職員等は、ウェブクライアントが動作する電子計算機にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

【強化遵守事項】
(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、教職員等が閲覧することが可能な学外のホームページを制限し、定期的にその見直しを行うこと。

5-4　通信回線

5-4-1 通信回線共通対策

趣旨（必要性）

通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、通信回線に関する対策基準を定める。

遵守事項

(1) 通信回線の構築時

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

(c) 部門技術担当者は、通信回線及び通信回線装置関連文書を整備すること。

(d) 部門技術担当者は、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。

(e) 部門技術担当者は、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。

(f) 部門技術担当者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

(g) 部門技術担当者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、選択すること。

(h) 部門技術担当者は、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。

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

(j) 部門技術担当者は、通信回線装置を安全区域に設置すること。

(k) 部門技術担当者は、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。

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

【強化遵守事項】

(m) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、通信を行う電子計算機の主体認証を行うこと。

(n) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、要安定情報を取り扱う情報システムについては、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。

(2) 通信回線の運用時

【基本遵守事項】

(a) 部門技術担当補佐は、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門を含む事項の管理を行うこと。

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

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

(d) 部門技術担当者は、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。

(e) 教職員等は、部門技術担当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。

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

(g) 部門技術担当補佐は、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。

(3) 通信回線の運用終了時

【基本遵守事項】

(a) 部門技術担当者は、通信回線装置の利用を終了する場合には、通信回線装置の内蔵記録媒体のすべての情報を復元が困難な状態にすること。

5-4-2 学内通信回線の管理

趣旨（必要性）

学内通信回線の利用については、当該通信回線の不正利用、これに接続された電子計算機又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。また、利用する回線により想定される脅威及びリスクが異なる。

これらのことを勘案し、本項では、学内通信回線に関する対策基準を定める。

遵守事項

(1) 学内通信回線の構築時

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、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。

(2) 学内通信回線の運用時

【強化遵守事項】

(a) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、通信要件の変更に際し及び定期的に、アクセス制御の設定の見直しを行うこと。

(b) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、定期的に、通信回線及び通信回線装置のセキュリティホールを検査すること。

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当補佐は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測又は検知すること。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当補佐は、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。

(3) 回線の対策

【基本遵守事項】

(a) 部門技術担当者は、VPN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備

(イ) 通信内容の暗号化

(ウ) 通信を行う電子計算機の識別又は利用者の主体認証

(エ) 主体認証記録の取得及び管理

(オ) VPN 経由でアクセスすることが可能な通信回線の範囲の制限

(カ) VPN 接続方法の機密性の確保

(キ) VPN を利用する電子計算機の管理

(b) 部門技術担当者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

(ア) 利用開始及び利用停止時の申請手続の整備

(イ) 通信内容の暗号化

(ウ) 通信を行う電子計算機の識別又は利用者の主体認証

(エ) 主体認証記録の取得及び管理

(オ) 無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限

(カ) 無線 LAN に接続中に他の通信回線との接続の禁止

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

(c) 部門技術担当者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、以下に挙げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。
（ア）利用開始及び利用停止時の申請手続の整備
（イ）通信を行う者又は発信者番号による識別及び主体認証
（ウ）主体認証記録の取得及び管理
（エ）リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限
（オ）リモートアクセス中に他の通信回線との接続の禁止
（カ）リモートアクセス方法の機密性の確保
（キ）リモートアクセスする電子計算機の管理

5-4-3 学外通信回線との接続

趣旨（必要性）

学内通信回線と学外通信回線との接続については、学外通信回線に接続された電子計算機からの不正アクセス、サービス不能攻撃等のほか、学外通信回線に送受信される情報の漏えい、改ざん又は破壊等、学外通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。

これらのことを勘案し、本項では、学外通信回線と接続する場合の学内通信回線に関する対策基準を定める。

遵守事項

(1) 学内通信回線と学外通信回線との接続時

【基本遵守事項】

(a) 部門技術担当者は、部門情報化推進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。

(b) 部門情報化推進責任者は、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。

(2) 学外通信回線と接続している学内通信回線の運用時

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、通信回線の変更に際し及び定期的に、アクセス制御の設定の見直し行うこと。

(c) 部門技術担当者は、定期的に、学外通信回線から通信することが可能な学内通信回線及び通信回線装置のセキュリティホールを検査すること。

(d) 部門技術担当補佐は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測又は検知すること。

(e) 部門技術担当補佐は、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。

第６部　個別事項についての対策

6-1　調達・開発にかかわる情報セキュリティ対策

6-1-1 機器等の購入

趣旨（必要性）

機器等を購入（購入に準ずるリース等を含む。）する際に、当該機器等に必要な情報セキュリティ機能が装備されていない場合及び購入後に情報セキュリティ対策が継続的に行えない場合には、既存の情報システム又は購入する機器等で取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。

この課題に対応するため、機器等を購入する際は、本学基準に準拠した機器等の購入を行うべく、購入先への要求事項を明確にする必要がある。

これらのことを勘案し、本項では、機器等の購入に関する対策基準を定める。

適用範囲

本項は、機器等の購入（購入に準ずるリース等を含む。以下同じ。）に適用する。

遵守事項

(1) 学内における情報セキュリティ確保の仕組みの整備

【基本遵守事項】

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

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

(2) 機器等の購入の実施における手続の遵守

【基本遵守事項】

(a) 部門技術担当者は、機器等の選定時において、選定基準及び具備すべき要件に対する機器等の適合性を確認し、機器等の候補の選定における判断の一要素として活用すること。

(b) 部門技術担当者は、機器等の納入時において、納入された機器等が選定基準及び具備すべき要件を満たすことを確認し、その結果を納品検査における確認の判断に加えること。

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

(d) 部門技術担当者は、機器等の購入において、満足すべきセキュリティ要件があり、それを実現するためのセキュリティ機能の要求仕様がある場合であって、総合評価落札方式により購入を行う場合には、これについて、IT セキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用すること。

6-1-2 外部委託

趣旨（必要性）

教職員等以外の者に情報処理業務を委託する場合には、本学が委託先を直接管理することができないため、学内で行う場合と比べ、情報の機密性、完全性及び可用性が損なわれるリスクが増大する。

このリスクに対応するため、情報処理業務を外部委託する際は、委託先においても本基準と同等の対策を実施させるべく、委託先への要求事項を明確にする必要がある。

これらのことを勘案し、本項では、外部委託に関する対策基準を定める。

適用範囲

本項は、会計法第 29 条に規定する貸借、請負その他の契約に基づき提供される役務のうち、情報処理に係る業務であって、例えば次に掲げるものに適用する。

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

遵守事項

(1) 学内における情報セキュリティ確保の仕組みの整備

【基本遵守事項】

(a) 全学実施責任者は、外部委託の対象としてよい情報システムの範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準を整備すること。

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

【強化遵守事項】

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、全学実施責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法を整備すること。

(d) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、全学実施責任者は、前事項の評価方法に従って、求める情報セキュリティ要件に対する委託先の候補者の情報セキュリティ水準を確認し、委託先の選定基準の一要素として利用すること。

(2) 委託先に適用する情報セキュリティ対策の整備

【基本遵守事項】

(a) 部門技術担当者は、外部委託に係る業務遂行に際して委託先に実施させる情報セキュリティ対策の内容を整備し、委託先候補に事前に周知すること。

(b) 部門技術担当者は、委託先に請け負わせる業務において情報セキュリティが侵害された場合の対処手順を整備し、委託先候補に事前に周知すること。

(c) 部門技術担当者は、委託先における情報セキュリティ対策の履行状況を確認するための評価基準を策定し､情報セキュリティ対策の履行が不十分である場合の対処手順に関して委託先候補に事前に周知すること。

(3) 外部委託先の選定における手続の遵守

【基本遵守事項】

(a) 部門技術担当者は、整備されている選定手続、選定基準及び委託先が具備すべき要件に基づき、委託先を選定すること。

(4) 外部委託の実施における手続の遵守

【基本遵守事項】

(a) 部門技術担当者は、外部委託を実施する際に、委託先に請け負わせる業務における情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む。）、情報セキュリティ侵害発生時の対処手順及び情報セキュリティ対策の履行が不十分である場合の対処手順を含む外部委託に伴う契約を取り交わすこと。また、必要に応じて、以下の事項を含めること。

（ア）情報セキュリティ監査を受け入れること。

（イ）提供されるサービスレベルに関して委託先に保証させること。

(b) 部門技術担当者は、外部委託に係る契約者双方の責任の明確化と合意の形成を行い､委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書を提出させること。また、必要に応じて、以下の事項を当該確認書に含めること。

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

（イ）外部委託した業務の作業に携わる者の特定とそれ以外の者による作業の禁止

(c) 部門技術担当者は、外部委託契約の継続に関しては、選定手続、選定基準及び委託先が具備すべき要件に基づきその都度審査するものとし、安易な随意契約の継続をしないこと。

(d) 部門技術担当者は、委託先の提供するサービス（情報セキュリティ基本方針、実施手順、管理策の維持及び改善を含む。）の変更に関しては、選定手続、選定基準及び委託先が具備すべき要件に基づき、その是非を審査すること。

(e) 部門技術担当者は、委託先がその請負内容の全部又は一部を第三者に再請負させることを禁止すること。ただし、委託先からの申請を受け、再請負させることにより生ずる脅威に対して情報セキュリティが十分に確保される措置が担保されると部門情報化推進責任者が判断する場合は、その限りではない。

(f) 教職員等は、委託先に提供する情報を必要最低限とし、委託先が要機密情報を取り扱う場合、以下の実施手順に従うこと。
（ア）委託先に情報を移送する場合は、不要部分のマスキングや暗号化等安全な受渡方法により実施し、移送した記録を保存すること。
（イ）外部委託の業務終了等により情報が不要になった場合には、確実に返却させ、又は廃棄させること。

(5) 外部委託終了時の手続の遵守

【基本遵守事項】

(a) 部門技術担当者は、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。

6-1-3 ソフトウェア開発

趣旨（必要性）

ソフトウェアを開発する際には、効果的なセキュリティ対策を実現するため、当該ソフトウェアが運用される際に関連する情報資産に対して想定される脅威を分析し、その分析に基づいて脅威から情報資産を保護するためのセキュリティ機能（真正確認、ア

クセス制御、権限管理、証跡管理等）及びその管理機能を適切にソフトウェアに組み込む必要がある。

加えて、開発するソフトウェアの処理に対するセキュリティホールの混入（設計及びコーディングのミス等によりセキュリティホールが埋め込まれてしまうこと、不正なコードが開発者により意図的に埋め込まれること等）についての防止対策も必要となる。

これらのことを勘案し、本項では、ソフトウェアを開発する際の対策基準を定める。

遵守事項

(1) ソフトウェア開発体制の確立時

【基本遵守事項】

(a) 部門技術担当者は、ソフトウェア開発について、セキュリティにかかわる対策事項（本項(2)から(5)の遵守事項）を満たすことが可能な開発体制の確保を、情報システムを統括する責任者に求めること。

(b) 部門技術担当者は、ソフトウェア開発を外部委託する場合には、委託先が実施すべき対策事項（本項(2)から(5)の遵守事項）の中から必要な事項を選択し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること。

(2) ソフトウェア開発の開始時

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、ソフトウェアの開発及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムと分離する必要性の有無を検討し、必要と認めたときは分離すること。

(3) ソフトウェアの設計時

【基本遵守事項】

(a) 部門技術担当者は、開発するソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果、及び当該ソフトウェアにおいて取り扱う情報の格付けに応じて、セキュリティ機能の必要性の有無を検討し、必要と認めたときはセキュリティ機能を適切に設計し、設計書に明確に記述すること。

(b) 部門技術担当者は、開発するソフトウェアが運用される際に利用されるセキュリティ機能についての管理機能の必要性の有無を検討し、必要と認めたときは適切に設計し、設計書に明確に記述すること。

(c) 部門技術担当者は、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。

(d) 部門技術担当者は、開発するソフトウェアにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要と認めたときは、その方法を設計し、設計書に明確に記述すること。

(e) 部門技術担当者は、開発するソフトウェアに重要なセキュリティ要件がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST評価・ST確認を受けること。ただし、当該ソフトウェアを要素として含む情報システムについてセキュリティ設計仕様書のST評価・ST確認を受ける場合、又はソフトウェアを更改する場合であって見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

(4) ソフトウェアの作成時

【基本遵守事項】

(a) 部門技術担当者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスから保護及びバックアップの取得を行うこと。

(b) 部門技術担当者は、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。

【強化遵守事項】

(c) 特に重要な情報とこれを取り扱う情報システムにおいて必要に応じ、部門技術担当者は、作成されたソースコードについて、その情報セキュリティに関する妥当性を確認するためのソースコードレビューの範囲及び方法を定め、これに基づいてソースコードレビューを実施すること。

(5) ソフトウェアの試験時

【基本遵守事項】

(a) 部門技術担当者は、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。

(b) 部門技術担当者は、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。

6-2　個別事項

6-2-1 学外での情報処理の制限

趣旨（必要性）

職務においては、その事務の遂行のため、学外において情報処理を実施する必要が生ずる場合がある。この際、学外での実施では物理的な安全対策を講ずることが比較的困難になることから、教職員等は、学内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。

これらのことを勘案し、本項では、学外での情報処理の制限に関する対策基準を定める。

遵守事項

(1) 安全管理措置の整備

【基本遵守事項】

(a) 全学実施責任者は、要保護情報について学外での情報処理を行う場合の安全管理措置についての規定を整備すること。

(b) 全学実施責任者は、要保護情報を取り扱う情報システムを学外に持ち出す場合の安全管理措置についての規定を整備すること。

(2) 許可及び届出の取得及び管理

【基本遵守事項】

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

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

(c) 部門技術担当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。

(d) 部門技術担当者及び職場情報セキュリティ責任者は、要保護情報（機密性２情報を除く。）について学外での情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

(e) 部門技術担当者及び職場情報セキュリティ責任者は、機密性２情報について学外での情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。

(f) 教職員等は、要保護情報について学外で情報処理を行う場合には、業務の遂行に必要最小限の情報処理にとどめること。

(g) 教職員等は、要保護情報（機密性２情報を除く。）を取り扱う情報システムを学外に持ち出す場合には、部門技術担当者又は職場情報セキュリティ責任者の許可を得ること。

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

(i) 部門技術担当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。

(j) 部門技術担当者及び職場情報セキュリティ責任者は、要保護情報（機密性２情報を除く。）を取り扱う情報システムを学外に持ち出すことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

(k) 部門技術担当者及び職場情報セキュリティ責任者は、機密性２情報を取り扱う情報システムを学外に持ち出すことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。

(l) 教職員等は、要保護情報を取り扱う情報システムを学外に持ち出す場合には、業務の遂行に必要最小限の情報システムの持出しにとどめること。

(3) 安全管理措置の遵守

【基本遵守事項】

(a) 教職員等は、要保護情報について学外での情報処理について定められた安全管理措置を講ずること。

(b) 教職員等は、要保護情報（機密性２情報を除く。）について学外での情報処理を行うことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

(c) 教職員等は、要保護情報を取り扱う情報システムの学外への持出しについて定められた安全管理措置を講ずること。

(d) 教職員等は、要保護情報（機密性２情報を除く。）を取り扱う情報システムを学外に持ち出すことを終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

6-2-2 本学支給以外の情報システムによる情報処理の制限

趣旨（必要性）

職務においては、その遂行のため、本学支給以外の情報システムを利用する必要が生じる場合がある。この際、当該情報システムが、本学が支給したものでないという理由で対策を講じなかった場合、当該情報システムで取り扱われる情報のセキュリティは確保できない。

これらのことを勘案し、本項では、本学支給以外の情報システムによる情報処理の制限に関する対策基準を定める。

遵守事項

(1) 安全管理措置の整備

【基本遵守事項】

(a) 全学実施責任者は、要保護情報について本学支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備すること。

(2) 許可及び届出の取得及び管理

【基本遵守事項】

(a) 教職員等は、要保護情報（機密性２情報を除く。）について本学支給以外の情報システムにより情報処理を行う必要がある場合には、部門技術担当者又は職場情報セキュリティ責任者の許可を得ること。

(b) 教職員等は、機密性２情報について本学支給以外の情報システムにより情報処理を行う必要がある場合には、部門技術担当者又は職場情報セキュリティ責任者に届け出ること。

(c) 部門技術担当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。

(d) 部門技術担当者及び職場情報セキュリティ責任者は、要保護情報（機密性２情報を除く。）について本学支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずること。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。

(e) 部門技術担当者及び職場情報セキュリティ責任者は、機密性２情報について本学支給以外の情報システムによる情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずること。

(3) 安全管理措置の遵守

【基本遵守事項】

(a) 教職員等は、要保護情報について本学支給以外の情報システムによる情報処理を行う場合には、原則として、当該情報システムについて定められた安全管理措置を講ずること。

(b) 教職員等は、要保護情報（機密性２情報を除く。）について本学支給以外の情報システムによる情報処理を終了した時に、その許可を与えた者に対して、その旨を報告すること。ただし、許可を与えた者から報告を要しないとされた場合は、この限りでない。

6-3　その他

6-3-1 学外の情報セキュリティ水準の低下を招く行為の防止

趣旨（必要性）

本学が、学外の情報セキュリティ水準の低下を招くような行為をすることは、学外に対して適切な行為でないことは当然であって、その行為が他者の情報セキュリティ水準を低下させることによって、本学を取り巻く情報セキュリティ環境を悪化させるため、本学にとっても好ましくない。

これらのことを勘案し、本項では、学外の情報セキュリティ水準の低下を招く行為の防止に関する対策基準を定める。

遵守事項

(1) 措置の整備

【基本遵守事項】

(a) 全学実施責任者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備すること。

(2) 措置の遵守

【基本遵守事項】

(a) 教職員等は、原則として、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずること。

6-3-2 業務継続計画（BCP）との整合的運用の確保

趣旨（必要性）

本学においては、事業の継続に重大な支障を来す可能性が想定される事態を特定し、当該事態への対応計画を業務継続計画（BCP：Business Continuity Plan）として策定することが考えられる。他方では、BCP の対象とする事態は、多くの場合に情報セキュ

リティを損なうものともなり、本学の情報セキュリティ関係規程に基づく対策も採られることとなる。この場合、BCP の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要である。

これらのことを勘案し、本項では、BCP と情報セキュリティ対策の整合的運用の確保に関する対策基準を定める。

遵守事項

(1) 本学における BCP 整備計画の把握

【基本遵守事項】

(a) 全学総括責任者は、本学における BCP の整備計画について全学実施責任者を通じ情報化推進室が適時に知ることができる体制を構築すること。

(b) 全学実施責任者は、本学において BCP の整備計画を把握した場合は、その内容を情報化推進室並びに必要に応じて部門情報化推進責任者、部門技術担当者及び職場情報セキュリティ責任者に連絡すること。

(2) BCP と情報セキュリティ対策の整合性の確保

【基本遵守事項】

(a) 情報化推進室は、本学において BCP 又は本基準の整備計画がある場合には、BCP と本基準との整合性の確保のための検討を行うこと。

(b) 全学実施責任者、部門情報化推進責任者、部門技術担当者及び職場情報セキュリティ責任者は本学において BCP の整備計画がある場合には、すべての情報システムについて、当該 BCP との関係の有無を検討すること。

(c) 全学実施責任者、部門情報化推進責任者、部門技術担当者及び職場情報セキュリティ責任者は、本学において BCP の整備計画がある場合には、当該 BCP と関係があると認めた情報システムについて、以下に従って、BCP と本基準に基づく共通の実施手順を整備すること。

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

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

【基本遵守事項】

(a) 教職員等は、本学においてBCPの整備計画がある場合には、BCPと情報セキュリティ関係規程が定める要求事項との違いなどにより、実施の是非の判断が困難な場合には、関係者に連絡するとともに、全学実施責任者が整備した障害等が発生した際の報告手順により、部門情報化推進責任者にその旨を報告して、指示を得ること。