令和元年 7 月 25 日
農場・演習林総務係

演習林におけるパソコンの学外持ち出しについて

パソコンの学外持ち出しに関する物品管理の取扱いについては、平成 27 年 5 月 14 日付農学研究院長決定で定められておりますが、演習林内における事務手続き等について、下記のとおり纏めましたので、よろしくお願いいたします。

記

1．演習林の教職員（技術職員含む）が、出張等においてパソコンを学外に持ち出す場合は、事前に演習林総務係に申請書を提出するものとします。

ただし煩雑になるため、日々の記録を研究室にて行い、翌月 10 日までに 1 カ月分をまとめて演習林総務係に提出することも可とします。

（例：６月分を７月１０日にまとめて提出）

（２）申請書は、研究室単位でまとめていただいても、先生お一人毎に作成いただいても結構です。

（３）持ち出しがない月については、特にご連絡いただく必要はありません。

2.「パソコン」に含まれる範囲は、デスクトップパソコン、ノートパソコン、タブレット型コンピュータ(iPad、iPadmini 等）とします。

3．持ち出しの範囲

（１）旅行命令による出張（例：北海道演習林への出張等）の場合、移動の際に学外で使用することも想定されるため、学外持ち出しに該当するものとします。

（２）本学の各キャンパスへの移動でも、旅行命令による出張の場合は学外持ち出しに該当するものとします。

農学部からの通知では、キャンパス間の移動は主な使用場所が学内のため、持ち出しに該当しない整理となっていますが、演習林間の移動の場合は旅行命令によるため、提出をお願いします。(教員の研修の際の移動も同様です。)

（３）旅行命令を発しない福岡市内のホテル等で開催される学会等に持ち出す場合でも、使用場所が学外の場合は持ち出しとして整理します。

なお、パソコン等に個人情報が含まれている場合は、データを暗号化するなど特に取り扱いにご注意願います。

また、持ち出したパソコンが、盗難、事故、災害等により紛失等した場合は、速やかに演習林総務係に連絡をお願いいたします。

九大農用第１７号
平成２７年5月１４日

教職員　各位

九州大学農学研究院長
平松　和昭　公印省略

物品の適正な管理について

先般の内部監査で、保有個人情報の管理体制の観点から、部局の実情を踏まえたパソコン等の外部への持ち出しルールを策定するよう指摘がなされたこと、また、農学部におけるパソコンの不適切な使用事例が発生したことを受けて、研究院長決定により「パソコンの学外持ち出しに関する物品管理の取扱いについて」を定めましたので、お知らせいたします。パソコンに関しては、当該決定により適正な管理をお願いいたします。

なお、パソコンだけでなく本学所有物品については、良好な状態で保管し、適切に使用することが求められており、教職員が故意又は重大な過失により物品を亡失した場合は、弁償責任が問われる場合があります。

物品の使用にあたっては、善良な管理者の注意をもってこれを行うと共に、やむを得ず学外に持ち出す場合は、大学の物品を所持していることに留意し、特に慎重な物品の管理を行っていただきますよう、お願いいたします。

担当　　農学部用度係
熊谷（2810）

パソコンの学外持ち出しに関する物品管理の取扱いについて

農学研究院長決定
平成２７年５月１４日

（目的）

第１条　この取扱いは、国立大学法人九州大学物品管理規程（平成１６年度九大会規第８号）第６条第４号の規定に基づき、農学研究院等における出張等の際のパソコン本体の学外持ち出しの取扱いについて必要な事項を定め、当該事務の適正な処理を図ることを目的とする。

（対象）

第２条　農学研究院等で使用されている、パソコン本体で、消耗品、少額備品及び有形固定資産を問わない。

（管理の方法）

第３条　管理の方法は、次の各号のとおりとする。

(1)　前条のパソコンを学外に持ち出す場合には、事前に所定の申請書を農学部事務部用度係（以下「用度係」という。）に提出するものとする。

(2)　用度係長は、原則月に１回、部局長に持ち出し状況について、所定の受付表にて報告するものとする。

(3)　持ち出したパソコンが、盗難、事故、災害等により紛失等した場合は、速やかに農学部事務部庶務係及び用度係に連絡するものとする。

（附記）

第４条　この取扱いは、平成２７年６月１日から適用する。

九州大学情報セキュリティポリシー

（第３版改定）

平成１４年１０月１８日 九州大学情報政策委員会決定
平成２３年　３月　１日 改定第２版（九州大学情報政策委員会決定）
平成２５年　３月　７日 改定（九州大学情報政策委員会決定）
平成２６年　９月　５日 改定第３版（九州大学情報政策委員会決定）
平成２７年　４月　１日 改定（九州大学情報政策委員会決定）

前　　文

現在、産官学の各組織体では、情報資産・個人情報の保護のための事業方針や規程を明確にすることが社会的に求められている。九州大学情報セキュリティポリシーは、九州大学情報倫理規程（平成 24 年九大規程第 73 号、平成 25 年 4 月 1 日施行）を具体的に補足し、教育・研究及び大学に求められる社会貢献に必要不可欠となった情報基盤の可用性と、外部からの脅威への対策及び内部のコンプライアンス確立のための統制という、互いにせめぎ合う問題を両立させ、社会に対しての説明責任をはたすために策定するものである。

また、組織的な情報セキュリティ保持は必要不可欠であるが、構成員個々の情報セキュリティに対する自己責任の醸成が最も重要である。

目　　次

1. 情報システム運用基本方針

1.1. 情報システムの目的

九州大学（以下「本学」という。）の情報システムは、九州大学教育憲章及び九州大学学術憲章に掲げる使命と理念を実現するため、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。

1.2. 運用の基本方針

1.1. で示した目的を達成し、円滑で効果的な情報流通を図るために、本学情報システムは、本情報セキュリティポリシー（以下「セキュリティポリシー」という。）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、全学で活用するものとする。

1.3. 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、セキュリティポリシーに沿って利用し、別に定める運用と利用に関する実施規程を遵守しなければならない。

1.4. 罰　則

セキュリティポリシーに基づく規程等に違反した場合の利用の制限及び罰則は、それぞれの規程に定めることができる。

1.5. 例　外

機器の設定等で、本学の依頼により事業者等が作業を行う場合や管理運営部局の許可を受けて一時的に本学のネットワークに接続する場合はこのセキュリティポリシーの適用外とする。

ただし、本学の指示の下に可能な限りセキュリティポリシー遵守に務めるものとする。

2. 定義等

2.1. 適用範囲

セキュリティポリシーは、病院情報ネットワーク（HIS）及びそれに接続されている情報システムを除く本学情報システムを運用・管理・利用するすべての者に適用する。

病院情報ネットワーク及びそれに接続されている情報システムに関するセキュリティポリシーは、別に定める。

2.2. 定 義

セキュリティポリシーにおいて、次の各号に掲げる用語は、それぞれ当該各号に定めるところによる。

(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、次のものをいう。

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協定に従って提供されるもの

③ 本学の情報ネットワークに接続されているもの

(2) 情報ネットワーク

本学の情報ネットワークは次のもので構成される。

① 本学により、所有又は管理されている全ての情報機器及びソフトウェア

② 本学との契約あるいは協定に従って提供される全ての情報機器及びソフトウェア

③ 本学の教職員等及び学生等が所有し、教育・研究用に必要な情報機器及びソフトウェア

(3) 情　報

セキュリティポリシーでいう「情報」とは，次のものをいう。

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

(4) 実施規程等

セキュリティポリシーに基づいて策定される規程・要項及び基準、計画をいう。

(5) 手　順

実施規程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。

(6) 情報システムの運用に携わる者

3.1.1 及び 3.1.2 に示す全学及び部局の管理担当者をいう。

(7) 教職員等

本学就業通則等に定める教職員及び派遣職員・研究者等で情報セキュリティ責任者(部局長等)が認めた者をいう。

(8) 学生等

本学学部通則及び大学院通則に定める学部学生、大学院学生、科目等履修生、聴講生、特別聴講学生、研究生、専修生、特別研究学生、その他、情報セキュリティ責任者(部局長等)が認めた者をいう。

(9) 利用者

教職員等及び学生等で、本学情報システムを利用する許可を受けて利用する者をいう。

(10) 全学共通 ID

学生等においては学生 ID 及び学生用 SSO-KID、教職員等においては教職員用 SSO-KID を指し、学内認証システムの ID となるコードをいう。

(11) 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。

(12) 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。

(13) 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、本学規程又は法令に反する事故あるいは事件をいう。

(14) 明示

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。

(15) 最高情報責任者（Chief Information Officer：ＣＩＯ）

「情報政策に係わる体制及び職務について（平成 26 年 5 月 13 日部局長会議決定)」に基づき、ＣＩＯとして指名された理事をいう。

(16) 副ＣＩＯ

「情報政策に係わる体制及び職務について（平成 26 年 5 月 13 日部局長会議決定)」に基づき、ＣＩＯから指名され、担当の分野に関してＣＩＯの職務を代行する者をいう。

(17) ＣＩＯ補佐官

「情報政策に係わる体制及び職務について（平成 26 年 5 月 13 日部局長会議決定)」に基づき、ＣＩＯから指名され、ＣＩＯ及び副ＣＩＯが行う情報化関連施策を補佐する者をいう。

(18) 最高情報セキュリティ責任者（Chief Information Security Officer：ＣＩＳＯ）

「情報政策に係わる体制及び職務について（平成 26 年 5 月 13 日部局長会議決定)」に基づきＣＩＯから指名されたＣＩＳＯをいう。

(19) 副ＣＩＳＯ

「情報政策に係わる体制及び職務について（(平成 26 年 5 月 13 日部局長会議決定)」に基づき、ＣＩＳＯが行う情報セキュリティ対策を補佐し、必要に応じてＣＩＳＯの職務を代行する者をいう。

(20) 情報政策委員会

情報政策委員会は、部局長会議規則（平成 16 年度九大規則第 14 号）第 7 条の定めにより情報政策を部局長会議から付託された全学的委員会である。

3. 組織・体制

3.1. 管理運営組織の構成

3.1.1. 全学体制

3.1.1.1 最高情報責任者（ＣＩＯ）の任務

全学の情報政策に関する最高責任者であり、情報セキュリティを含む情報戦略を立案するとともに、「情報政策に係わる体制及び職務について（平成 26 年 5 月 13 日部局長会議決定)」第 3 項に掲げる事項を統括し、本学の情報化を推進する。

3.1.1.2 最高情報セキュリティ責任者（ＣＩＳＯ）の任務

(1) ＣＩＳＯは、本学情報システムの情報セキュリティに責任を持つ。

(2) ＣＩＳＯは、ＣＩＯの指示のもとでセキュリティポリシー及びそれに基づく規程の制定や情報システム上でのセキュリティに関する各種問題に対する処置を行う。

(3) ＣＩＳＯは、情報セキュリティに関して全学向け教育及び管理運営部局のシステム管理者向け教育を統括する。

(4) ＣＩＳＯに事故があるときは、ＣＩＯがあらかじめ指名する者が、その職務を代行する。

(5) ＣＩＳＯは、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置くことができる。

3.1.1.3 副ＣＩＳＯの任務

ＣＩＯが行う情報セキュリティ対策を補佐するとともに必要に応じてＣＩＳＯの職務を代行する。

3.1.1.4　情報政策委員会の任務

情報政策委員会は、情報政策委員会規程（平成１６年度九大規程第１８９号）第２条第８号に定める情報システムのセキュリティに関し、次の各号に掲げる事項について審議し、又は実施する。

(1) セキュリティポリシー及び全学向け教育の実施ガイドラインの制定及び改廃
(2) 情報システムの運用と利用及び教育に係る規程及び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規程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規程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) 不正アクセス等の処置
(8) インシデントの再発防止策の検討及び実施
(9) その他委員長が必要と認めたこと

3.1.1.5　統括情報セキュリティ責任者（情報統括本部長）

(1) 本学に統括情報セキュリティ責任者を置き、情報統括本部長をもって充てる。統括情報セキュリティ責任者は、本学の情報システムのセキュリティに関する連絡と通報において責任を持つ。
(2) 情報統括本部長は、ＣＩＳＯの指示により、セキュリティポリシー及びそれに基づく規程並びに手順等に基づき本学情報システムの整備と運用を実施する。
(3) 情報統括本部長は、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、セキュリティポリシー並びにそれに基づく規程及び手順等の遵守を確実にするための教育を実施する。

3.1.1.6　情報セキュリティ対策室

(1) 情報統括本部の情報セキュリティ対策室は、全学の情報システムのセキュリティ管理を実施するとともに、情報統括本部長への情報セキュリティに関する技術的助言等を行う。
(2) 情報セキュリティ対策室の任務は、次のとおりとする。
　① 全学の情報システムが円滑に運用されるよう、情報セキュリティの保持と強化のための技術的な調査及び検討を行うとともに、総括的な連絡窓口となる。
　② 学内の定常的な情報セキュリティ管理の状況について、情報統括本部長へ報告する。
　③ 情報セキュリティを保持するために必要と判断したときは、関連する通信の遮断又は機器の切り離し等の緊急措置をとることができる。実施した緊急措置について、情報統括本部長へ報告する。
　④ 情報セキュリティの保持と強化のために必要な技術的措置を情報セキュリティ責任者(部局長等)に助言し、情報を提供するとともに、実施に関する協議を行う。

⑤　情報セキュリティ保持のため全学的な情報セキュリティ診断を定期的に行い、情報政策委員会に報告する。

3.1.1.7　情報セキュリティ監査責任者

(1) 本学に、情報セキュリティ監査責任者を置き、ＣＩＯが指名する副ＣＩＯをもって充てる。

(2) 情報セキュリティ監査責任者は、ＣＩＳＯの指示に基づき、管理運営部局が行う全学的情報サービスについて、ＩＳＭＳ（Information Security Management System：ＩＳＯ／ＩＥＣ２７００１）の要求事項に従い情報セキュリティの内部監査を企画、実施し、統括する。

3.1.1.8　管理運営部局

情報統括本部を、本学情報システムの管理運営部局として定め、情報統括本部長の指示により、以下の各号に定める事務を行うものとする。

(1) 情報政策委員会の運営に関する事務

(2) 本学情報システムの運用と利用におけるセキュリティポリシーの実施状況の取りまとめ

(3) 講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ

(4) 本学情報システムのセキュリティに関する連絡と通報

3.1.2.　部局の体制

3.1.2.1　情報セキュリティ責任者（部局長等）

(1) 各部局に情報セキュリティ責任者を置き、部局長等をもって充てる。

(2) 情報セキュリティ責任者(部局長等)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を担当する。

(3) 情報セキュリティ責任者(部局長等)は、部局における実施手順書等を制定した場合は、ＣＩＳＯに報告するものとする。

3.1.2.2　部局情報システム運用委員会

(1) 各部局に部局情報システム運用委員会を置く。

(2) 部局情報システム運用委員会は、各部局の教授会等で兼ねることができる。

(3) 部局情報システム運用委員会の委員長は、部局長等をもって充てる。

(4) 部局情報システム運用委員会は次の各号に掲げる事項について審議し、又は実施する。

①　部局における情報セキュリティ保持のための実施手順書等の制定及び改廃

②　部局におけるセキュリティポリシーの遵守状況の調査と周知徹底

③　部局におけるリスク管理及び非常時行動計画の策定及び実施

④　部局におけるインシデントの再発防止策の策定及び実施

⑤　部局におけるシステム管理者向け教育の企画及び実施

(4) 部局情報システム運用委員会を教授会とは別に設置した場合、部局長等は名称及び構成等をＣＩＳＯに報告するものとする。

3.1.2.3 システム管理者

(1) システム管理者は、個々の情報システムを維持管理する教職員で、セキュリティポリシーに基づいたパラメータの設定やセキュリティパッチの実施など情報セキュリティを維持するための責任を負う。

(2) システム管理者は、学生等にシステム管理業務を補助させることができるが、その場合においてもシステム管理者が最終的な責任を負う。

(3) システム管理者は、情報セキュリティ対策室、情報セキュリティ責任者(部局長等)、支線ＬＡＮ管理者等から情報セキュリティ維持管理のために協力を依頼された場合にはそれに応じなければならない。

3.1.2.4 支線ＬＡＮ管理者

(1) 支線ＬＡＮ管理者は、九州大学総合情報伝達システム運用規則第８条に定める部局において支線ＬＡＮの管理及び運用を担当する者をいう。

(2) 支線ＬＡＮ管理者は、支線ＬＡＮに障害が発生した場合には情報セキュリティ対策室と協力して復旧に努めなければならない。

(3) 支線ＬＡＮ管理者は、システム管理者と協力して支線ＬＡＮ内の情報セキュリティ管理を行わなければならない。

3.1.3. 役割の分離

情報セキュリティ対策の運用において、同一人は以下の役割を兼務してはならない。

(1) 承認又は許可事案の申請者とその承認者又は許可者
承認する立場にあるものが申請を行う場合は、セキュリティ対策室又は、情報セキュリティ責任者(部局長等)が認めた者の審査を受け、その記録を保存しなければならない。

(2) 監査を受ける者とその監査を実施する者

3.1.4. その他

情報政策委員会及び情報セキュリティ対策室は、その責務を効率的に遂行するため、次の事項に留意するものとする。

(1) 組織の管理運用の単位（部局）と、サブネットワークの構成等、情報ネットワークの管理単位を一致させる。

(2) 複数部局で１つのサブネットワークを共有するのは避ける。

(3) 情報ネットワークの管理階層を深くしすぎないよう、できるだけ単純構成にする。

(4) 病院情報ネットワーク、事務用 LAN 等については、それぞれ別に管理体制を整え、情報セキュリティ対策室との連携を図る。

(5) 情報セキュリティ対策室は、学内情報ネットワークの常時運用と情報セキュリティ確保のための緊急時対応への全学的支援を行う。

3.2. 本学外の情報セキュリティに悪影響を及ぼす行為の防止及び処置

3.2.1. 防止のための措置等

(1) ＣＩＳＯは、本学外の情報セキュリティに悪影響を及ぼす行為の防止に関する措置についての規定を整備しなくてはならない。

(2) 本学の情報システムを運用・管理・利用する者は、原則として、本学外の情報セキュリティに悪影響を及ぼす行為の防止に関する措置を講じなくてはならない。

3.2.2. 不正アクセス等への処置

(1) ＣＩＳＯは、学内から学外のシステムへの不正アクセス等が発生し、本学外の情報セキュリティの水準低下を招くおそれがある場合は、不正アクセス等を行う当該情報システム又はそれを継続する情報ネットワークについて定常的な利用の停止などの抑止措置をとり、情報政策委員会に報告しなくてはならない。

(2) 情報政策委員会は、教職員等及び学生等が不正アクセス等を行った場合、教授会、評議会等に対し違反行為の報告を行う。

3.3. 事故及び障害の報告

(1) 教職員等及び学生等は、情報セキュリティに関する事故、情報システムの不審な動作、情報の改ざん、情報システム上の障害及び誤動作等を発見した場合には、情報セキュリティ責任者(部局長等)、支線ＬＡＮ管理者又はシステム管理者に直ちに報告しなければならない。

(2) 上記の報告を受けた情報セキュリティ責任者(部局長等)等は、報告のあった事故等について必要な措置を直ちに講じ、情報セキュリティ対策室に通知しなければならない。必要があれば、その措置について情報セキュリティ対策室に指示又は支援を要請する。

(3) 上記の報告を受けた情報セキュリティ対策室は必要に応じて情報システム部情報企画課に連絡するものとする。情報システム部情報企画課は、ＣＩＳＯの指示に従い文部科学省大臣官房政策課への報告及びＩＰＡセキュリティセンター不正アクセス対策室への届出並びに警察のネットワーク犯罪担当部署への相談等を行う。

(4) 情報統括本部長は、副ＣＩＳＯと連携し発生したすべての情報セキュリティ上の事故等を検証し、必要に応じて情報政策委員会に報告するとともに記録を一定期間保存し、重大な事故に対しては再発防止のための迅速な対策を当該部局等に講じさせなければならない。

(5) 情報セキュリティ対策室は必要に応じて教職員等及び学生等に対して情報セキュリティ上の事故及び障害等を速やかに通知しなければならない。

(6) 学内からの不正アクセス等によって学外に被害が及び、その事実関係の説明を被害者又は第三者から求められた場合は、ＣＩＳＯが対応する。

3.4. 緊急時の対応

(1) 情報セキュリティ対策室は、緊急時に備えなければならない。

(2) 情報セキュリティ対策室が行った緊急措置に対する報道機関や警察等への対応は、ＣＩＳＯが行う。

(3) 部局における緊急措置は、情報セキュリティ責任者(部局長等)の責任において行うことができる。

4. 情報の格付け、分類と管理

4.1. 情報の格付け及び取扱い制限のルール

(1) ＣＩＳＯ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しなければならない。

(2) 情報セキュリティ責任者(部局長等)は、部局におけるすべての電磁的に記録された情報を重要度と目的により分類し、利用権限を定めるとともに、情報の管理方法と管理責任を明確にしなければならない。情報を共有あるいは公開する場合は、その範囲と権限を明確にしなければならない。

(3) ネットワークに係る次の各号の情報は，情報セキュリティ確保のために保護されるべき秘密情報として区分する。

① ネットワーク機器の IP アドレス，サブネットマスク

② ネットワークの重要な機器であるルータの機器名

③ 重要なネットワーク機器の設置場所

④ LAN 管理者に関する情報（所属，氏名，メールアドレス　など）

4.2. 情報の分類と利用権限

(1) 情報には、情報システムを稼動させるためのシステムプログラムやシステム設定情報、情報システムを利用するための管理情報、情報システムの利用者が作成する情報等がある。また、利用者が作成する情報には、教育研究情報、保健医療情報、事務情報等がある。

(2) 情報の利用者には、情報の所有者と作成者、所有者と作成者が所属するグループあるいは組織（例えば、経理系事務限定、研究室内限定等)、それ以外の学内の教職員等及び学生等、並びに学外の不特定者等がある。

(3) 情報の利用権限には、作成、参照、更新、削除等がある。

(4) 各部局で情報の管理に責任を持つ者は、情報の内容に応じて分類し、その利用者と利用権限を定めなければならない。

4.3. 情報の管理

システム管理者は、自ら管理する情報を、不特定多数の者がアクセス可能な公開情報、アクセスが制限されている限定公開情報、開示を行わない非公開情報とに分類し、それぞれ適正に管理しなければならない。特に、非公開情報の保存場所（どの情報システム上のどこに保持するのか）と、その情報システムを設置する物理的な場所等に配慮しなければならない。

4.3.1. 情報の公開・非公開に関する分類

(1) 公開情報

一般に公開する情報をいう。

(2) 限定公開情報

特定の利用者にのみ開示する情報をいう。

(3) 非公開情報

開示を行わず、作成者及び特定の権限を有するものだけが取り扱うことができる情報をいう。

4.3.2. アクセス制限

システム管理者は、情報の利用者とその利用権限を定めなければならない。さらに、情報を利用するための手段を適切に設定し、許可されることがない情報へのアクセスができないようにしなければならない。

4.3.3. 公開情報の管理

公開情報は任意の場所からアクセス可能な性質を持つため、情報の改ざんや偽情報の流布に対し、4.6 に掲げる防止策を講じなければならない。

4.3.4. 限定公開情報の管理

情報の中には、特定の利用者に特定の情報を開示する必要があるものがある。例えば、成績情報に対する担当教員又は学生のアクセスがこれに該当する。このような特定の利用者に情報の登録を許可し、情報を公開、開示する場合の取り扱いは次の各号による。

(1) システム管理者は、情報の登録及び閲覧は、許可された者が許可された操作だけを行えるように、認証及びアクセス制御機能を設けなければならない。

(2) システム管理者は、不正な登録や閲覧が行われていないか、定期的に状況を確認しなければならない。

(3) システム管理者は、教職員等及び学生等に対してのみ情報の登録を許可し、又は情報の開示を行う場合は、IP アドレスを用いた判定ではなく、全学共通 ID による認証を行った上で行うことを原則とする。

(4) システム管理者は、教職員等及び学生等に対して、機密性の高い情報の登録を許可し、又は機密性の高い情報の開示を行う場合は、全学共通 ID による認証に加えてより高度な認証を行うことが望ましい。

(5) システム管理者は、情報システムを運用するために必要な物品や役務等の調達、共同研究、委託研究等の手続の際に情報を提示する場合には、公開情報と非公開情報を厳密に分類し、非公開情報の提示が必要となった場合には非公開情報を分離し、相手方との秘密保持契約（Non-disclosure agreement : NDA）等を行った上で非公開情報を開示しなければならない。

(6) 外部組織との契約等により情報セキュリティインシデントに関する限定公開情報及び非公開情報の開示、共有等の取り決めを行う場合には、事前にＣＩＳＯに報告し許可を得なければならない。

4.3.5. 非公開情報の管理

(1) 非公開情報は、システム管理者が許可した場所以外に保管してはならない。

(2) システム管理者は、同一の情報システム上に非公開情報と公開情報を保持する場合は、情報を保持する場所を明確に分離し、非公開情報が誤って公開されることがないようにしなければならない。

(3) 非公開情報を扱う情報ネットワークは、一般の情報ネットワークと論理的に異なるよう設置し、物理的に異なる回線を利用することが望ましい。

(4) 一般の情報ネットワークと非公開情報ネットワークの間で通信する必要がある場合は、両情報ネットワークの接続点を最小限とし、非公開情報ネットワーク側からのみ通信可能としておかなければならない。さらに、必要なとき以外は両情報ネットワーク間の通信は遮断しておくことが望ましい。

(5) 利用者は、利用を許可された場所から外部に非公開情報を持ち出してはならない。同様に、盗聴防止のため、インターネット等の公衆回線を介して非公開情報にアクセスする必要がある場合には、不特定の者が傍受不可能な方式でアクセスしなければならない。

(6) 外注等のため、非公開情報を限定された第三者に開示する必要がある場合は、外注等にかかる契約の主体者は、守秘義務を明記した契約を結ばなければならない。

4.4. 情報の開示

非公開情報及び限定公開情報を含む文書、データ等を開示する場合は、個人情報の漏洩、プライバシーや著作権の侵害、情報セキュリティの保護に十分注意しなければならない。

4.5. 情報改ざん及び偽情報流布の防止

(1) システム管理者は、情報の重要度を考慮して、CD-ROM/CD-R 等の書き換え不能な記憶媒体に保存するなどにより情報の原本性を保証しなければならない。

(2) システム管理者は、自ら管理する情報システムの公開情報が改ざんを受けた場合の速やかな回復機構を備えなければならない。

(3) システム管理者は、公開情報（Web での掲示情報やメールマガジンによる情報発信を含む）の複製・編集等による情報の発信者の偽造及び偽情報の流布を防止するための対策を講じることが望ましい。

4.6. 情報システム及び記憶媒体の処分

情報システム及び記憶媒体を破棄する場合は、次のような方法で処分しなければならない。

(1) 磁気記憶媒体

ハードディスク、磁気テープ、フロッピーディスク等の磁気記憶媒体は、通常の消去操作では管理情報のみが消去されるだけで情報そのものは消去されないこと、また、数回の上書き消去でも残留磁気情報の読み出しによって情報を復元できるため、媒体自体の破壊または専用の磁気消去装置を利用する必要がある。

(2) フラッシュメモリ製品

SSD（Solid State Drive）、USB メモリ、SD カード等のフラッシュメモリを搭載した記憶媒体は、搭載されたメモリチップを破壊するか、効果が確認されている記録消去ソフトを利用する。

(3) 光メディア

CD、DVD、ブルーレイディスク等の光メディアはディスク自体を破壊する。

(4) その他の記憶媒体

(1)～(3)以外の新たな記憶媒体が現れた場合は、完全に記録を消去する方法について配慮しなければならない。

(5) 業者への廃棄委託

業者に委託して情報機器の交換及び機器の撤去を行う場合は、記憶媒体の処理法についても十分配慮しなけれ

ばならない。

5. 物理的セキュリティ保護の方針

5.1. 情報ネットワーク運用方針

5.1.1. 情報ネットワーク設計、機器導入及び設定

(1) 情報ネットワーク設計

新たな情報ネットワークの設計及び構築にあたっては、教育研究、保健医療、事務等の目的の異なる情報ネットワークトラフィックを論理的に混在させてはならない。さらに、物理的に混在させないことが望ましい。

(2) 情報ネットワーク機器

システム管理者は、機器障害や権限のないアクセスによって機器の構成や制御機能が損なわれないように情報ネットワーク機器を管理しなければならない。また、機器のファームウェアを最新のものに更新しておかなければならない。

(3) 情報セキュリティ機器及びその運用情報セキュリティ責任者(部局長等)は、ファイアウォール及び情報ネットワーク侵入検知システムその他の必要と思われる情報セキュリティ機器を導入することが望ましい。

5.1.2. 情報ネットワークサービス選択

情報セキュリティ責任者(部局長等)は、利用可能な情報ネットワークサービスと利用形態を決定し、定められた以外のサービスを提供しないよう管理しなければならない。

5.1.3. 情報ネットワーク接続の管理

(1) 情報システムを情報セキュリティ責任者(部局長等)の許可なく情報ネットワーク機器（公共情報端末や情報コンセントを含む）に接続してはならない。

(2) バックドア（ＰＰＰサーバ、コンピュータに接続する公衆回線、ＶＰＮ装置及びソフトウェア等大学構内以外からあたかも構内からの接続であるように見せることができる設備、以下「学外からのＬＡＮ接続」という。）を設置し、接続することを原則的に禁止する。

(3) 前項の規定にかかわらず、教育・研究上必要な場合は、ＣＩＳＯの承認を得て前項の機器等を設置し本学の情報ネットワークに接続することができる。この場合においては、次のように取り扱う。

① 学外からのＬＡＮ接続が承認された場合においても、地理的に学外から利用が禁じられているもの（学内の特定の情報サービス）や、インターネットへの接続をすることはできない。

② 管理運営部局は学内の情報サービスを運用するために必要と認められた場合は、その時点で最も安全であると判断される認証方法を用いて学外からの接続サービスを本学構成員に対して提供することができ、このサービスを利用する場合はインターネットへの接続も利用できるものとする。

③ システム管理者は、管理運営部局が提供する学外からのＬＡＮ接続サービスを利用したアクセスが不適当であると判断した場合は管理するシステムへのアクセスを拒否することができる。

(4) 本学の IP アドレスは、本学の教職員等及び学生等のみが利用可能である。

(5) 本学の IP アドレスは、地理的に本学のキャンパス（遠隔地施設を含む）以外の場所においても本学の教職員等及び学生等教職員等が必要に応じて利用できる。

5.1.4. 情報ネットワークの運用

(1) システム管理者は、ログを定期的にチェックし、一定期間保存しなければならない。
(2) システム管理者は、ルータやソフトウェア設定可能なハブ等の情報ネットワーク機器や情報ネットワークサービスを提供する機器を設置するに当たっては、施錠などによって物理的に隔離された区域に設置することが望ましい。
(3) 情報統括本部長は、基幹部分を構成する機器など、特に重要と思われる情報ネットワーク機器については、原則としてその設置場所を限られたシステム管理者以外に公開してはならない。

5.2. 対外接続の基本方針

本学では、外部情報ネットワークとの接続点にファイアウォール等の管理装置を設置し情報セキュリティの保持を行う対外接続を原則とする。

そのために、以下の各号の方針に従って運用を行う。

(1) 情報統括本部長は、安全性及び信頼性を向上させるため、対外接続点にファイアウォール等の管理装置を設置し、外部からの攻撃を防御するとともに、外部への攻撃・著作権侵害等を抑制する設定を行う。
(2) システム管理者や利用者は、自己責任を自覚し、情報セキュリティ管理につとめなければなければならない。
(3) システム管理者や利用者は、教育・研究のための正当な理由がある場合は対外接続点のファイアウォールの設定変更について情報統括本部長に依頼することができる。

5.2.1. 例外的な対外接続と自己責任による情報セキュリティ保持

支線ネットワークが管理装置を回避した対外接続を行う場合には、情報セキュリティ対策室に申請の上、承認を得なければならない。また、その支線ネットワークを運用するものは、自己のネットワークで発生する危険のあるセキュリティインシデントに対して学内外へ与える影響を慎重に考慮し、対外接続形態を選択しなければならない。

5.3. コンピュータ等の運用に関する方針

5.3.1. 基本方針

(1) 情報セキュリティ責任者(部局長等)は、情報ネットワークに接続する機器の情報セキュリティ対策として、セキュリティポリシーに従って、その用途あるいは機器の種類ごとに実施手順書を別途策定する。システム管理者及び利用者は、実施手順書に合わない機器を情報ネットワークに接続してはならない。
(2) システム管理者は、常に最新の情報セキュリティに関する情報に注意を払い、コンピュータシステムを安全に運用するように努力しなければならない。
(3) システム管理者は、情報統括本部長又は情報セキュリティ責任者(部局長等)の要請があった場合、ログ等の運

用に関する情報を提供しなければならない。

(4) 情報セキュリティ責任者(部局長等)は、情報システムを把握し、求めに応じて情報セキュリティ対策室に報告しなければならない。

5.3.2. 情報システムを運用する際の遵守事項

(1) システム管理者は、コンピュータシステムを情報ネットワークに接続する場合、設定作業（情報セキュリティ対策を含む）の完了していない機器を情報ネットワークに接続してはならない。

(2) システム管理者は、認証機能を持たない機器を情報ネットワークに接続してはならない。それ自身で認証機能を持たない機器を利用する必要がある場合は、物理的な手段又は他の機器との組み合わせにより認証機能を確保しなければならない。

(3) システム管理者は、機器の利用者を把握しなければならない。

(4) 情報セキュリティ責任者(部局長等)は、コンピュータシステムとＩＰアドレスの整合を定期的に検査しなければならない。

6. 情報システムを取り扱う者の留意事項

6.1. セキュリティポリシーの遵守

(1) 教職員等及び学生等は、セキュリティポリシーを遵守しなければならない。

(2) 教職員等及び学生等は、システム管理者から情報セキュリティ維持管理のために協力の要請があった場合は、それに応じなければならない。

6.2. 利便性の配慮

(1) 教職員等及び学生等は、情報セキュリティ対策によって利便性を著しく損なう場合や遵守することが困難な場合は、情報セキュリティ責任者(部局長等)に対してセキュリティポリシー及び実施手順書等の改善を求めることができる。

(2) 教職員等及び学生等は、システム管理者の許可を得ずにコンピュータシステム等を設置場所から持ち出してはならない。ただし、携帯可能な機器（ノートパソコンや携帯情報端末等）は、部局等の管理規定に従った手続きを行った上でこれを持ち出すことができる。

(3) システム管理者は、教職員等及び学生等以外の者に学内の情報システム（公共情報端末や情報コンセントを含む）を一時的に使用させる場合は、セキュリティポリシーを遵守させなければならない。

6.3. 教育及び研修

(1) 情報政策委員会は、情報セキュリティ責任者(部局長等)、支線ＬＡＮ管理者及びシステム管理者に対し、必要な技能を修得するための研修を実施する。

(2) 情報政策委員会は、各部局等で行う教職員等向けのセキュリティポリシーに関する研修の支援をしなければならない。また、教員が行う学生等向けのセキュリティポリシーに関するオリエンテーション又は講義に協力しなければならない。

(3) 教職員等及び学生等は、セキュリティポリシーを遵守するため、研修会や説明会又は講義等に出席しセキュリティポリシー及び実施手順書等の理解に努めなければならない。

6.4. パスワード管理及びログ管理

6.4.1. 利用者の遵守事項

(1) 自己のパスワードは秘密としなければならない。また、情報セキュリティを維持できるよう、自己のパスワードの設定及び変更に配慮しなければならない。

(2) 他の利用者のパスワードを聞き出したり、アカウントを使用してはならない。

(3) システムの管理権限を有する者からのパスワードの聞き取りに対しても応じてはならない。

(4) 情報セキュリティ責任者(部局長等)、支線ＬＡＮ管理者又はシステム管理者がパスワードの変更を求めた場合、利用者はその指示に従わなければならない。

6.4.2. システム管理者の遵守事項

(1) 情報システムの利用資格者の規定を定めなければならない。

(2) 規定に基づく利用資格を有する者以外にコンピュータシステムのアカウントを発行してはならない。また、利用資格を失った利用者のアカウントは、直ちに削除しなければならない。

(3) 利用者のアカウントを管理権限のない第三者に漏洩してはならない。また、利用者からパスワードを聞き出してはならない。

(4) ログ情報及び通信内容の解析等にあたっては、利用者のプライバシーに配慮し、部局情報システム運用委員会等において閲覧解析を認める場合の要件と手続きを定めなければならない。

6.5. 非常勤教職員及び臨時職員並びに外部委託業者の留意事項

6.5.1. セキュリティポリシーの理解及び遵守

非常勤教職員及び臨時職員を雇用する者並びに外部事業者との契約を行い業務委託する者は、採用及び契約での派遣の際、従事者に守るべきセキュリティポリシーの内容を理解させ、遵守させなければならない。

6.5.2. 情報システムの開発及び保守管理業務の委託における遵守事項

情報システムの開発及び保守管理業務を外部事業者に委託する場合は、下請として受託する業者を含めて、セキュリティポリシーのうち遵守すべき内容を明記した契約を行わなければならない。具体的には以下のような点を契約書に明記しなければならない。

(1) パスワードやシステム設定情報などの非公開情報の開示に係わる守秘義務

(2) 責任所在の境界及びセキュリティポリシーが遵守されなかった場合の罰則規定

7. セキュリティポリシーの実施、評価及び見直し

7.1. セキュリティポリシーの実施

セキュリティポリシーの実施に当たって、ＣＩＳＯ及び情報セキュリティ責任者(部局長等)は、全学又は部局ごとに予めセキュリティを保持するための実施手順書を定め、その上でセキュリティポリシーを実施しなければならない。

7.2. セキュリティポリシーの運用実態の把握

ＣＩＳＯは、セキュリティポリシーの運用実態等を把握しなければならない。

7.2.1. 情報セキュリティ監査

(1) 管理運営部局を含む各部局は、監事及び本学が契約した監査法人が実施する情報セキュリティに関する監査に協力し、指摘事項に対して真摯に対応しなければならない。

(2) 情報セキュリティ監査責任者は、部局から部局情報システムに関する情報セキュリティ監査への協力を要請された場合、協力することができる。

(3) 情報セキュリティ監査責任者は、管理運営部局が実施する全学的情報サービスについての情報セキュリティ対策が確実に実施されているかについて内部監査を実施しなければならない。

7.2.2. 利用者意見の収集

ＣＩＳＯは、教職員等及び学生等からセキュリティポリシーに関する意見を収集、分析、整理しなければならない。また、情報セキュリティ責任者(部局長等)は、部局におけるセキュリティポリシーの運用実態を把握しなければならない。

7.2.3. 情報セキュリティ対策費の把握

ＣＩＳＯ及び情報セキュリティ責任者(部局長等)は、情報セキュリティ対策に要した直接的経費を把握しなければならない。直接的経費には、情報セキュリティ対策室及び情報セキュリティ責任者(部局長等)が不正アクセス等の検出のために購入した装置（ハードウェア、ソフトウェア、ソフトウェアのバージョンアップを含む)、支線ＬＡＮ管理者及びシステム管理者が購入したウィルス対策ソフトウェア、外注した情報セキュリティ診断及び監査などに要した費用等が含まれる。

7.3. 情報セキュリティレベルの向上策

情報政策委員会は、ＣＩＳＯの報告に基づき、セキュリティポリシーに沿った対策がどの程度実施されているかを把握するとともに、情報セキュリティレベルの向上に必要な措置を検討しなければならない。

7.3.1. セキュリティポリシーの評価及び見直し

情報政策委員会は、7.2 の結果に基づきセキュリティポリシーの実効性を少なくとも年１回評価し、必要な部分を見直して内容の変更及び実施時期の検討を行うとともに、より情報セキュリティレベルの高い、かつ、遵守可能なセキュリテ

ィポリシーへの更新を審議しなければならない。

7.3.2. 情報セキュリティ計画及び予算案の作成

情報政策委員会は評価及び見直しの結果を踏まえ、次年度の情報セキュリティ計画及び予算案を作成しなければならない。

7.3.3. 評価及び見直しの報告

情報政策委員会は評価及び見直しの結果の要約を全学の教職員等及び学生等に提示しなければならない。