公立大学法人三条市立大学
情報セキュリティポリシー

令和５年 11 月 13 日　策　　定

目　次

序章　情報セキュリティポリシーの構成

第１節　基本的な考え方

公立大学法人三条市立大学（以下「本法人」という。）の運営の多くは情報システムに依存しているところである。

本法人の各情報システムが取り扱う情報には、本法人の役員、教職員、学生、関係者及び関係団体（以下「教職員等」という。）の個人情報のみならず法人運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、教職員等の財産、プライバシー等を守るためにも、また、法人運営を安定的に継続するためにも必要不可欠である。

そのため、これらの脅威を組織共通の認識として一貫した方針の下、情報セキュリティ対策の実効性を高めるとともに、対策レベルを一層強化していくこととし、公立大学法人三条市立大学情報セキュリティポリシーを定めるものである。

第２節　情報セキュリティポリシーの構成

本法人が保有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを情報セキュリティポリシーとする。

情報セキュリティポリシーは、本法人が保有する情報資産に関する業務に携わる全ての教職員等に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを、一定の普遍性を備えた部分（基本方針）と情報セキュリティを取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、情報セキュリティ基本方針と情報セキュリティ対策基準の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする。

情報セキュリティポリシーの構成

文　書　名		内　　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全ての情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

情報資産の範囲

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器
情報システム	サーバ、ネットワーク、パソコン（机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいう。以下同じ。）、モバイル端末（業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。以下同じ。）、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	コンピュータ室、配電盤、電源ケーブル、通信ケーブル等
電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

第１章　情報セキュリティ基本方針

第１節　目的

本基本方針は、本法人が保有する情報資産の機密性、完全性及び可用性を維持するため、本法人が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

第２節　定義

⑴　情報資産

ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体（以下「記録媒体」という。）、ネットワーク及び情報システムで取り扱う情報並びに情報システムの仕様書、ネットワーク図等のシステム関連文書をいう。

⑵　ネットワーク

コンピュータ等を相互に接続するための通信回線、通信機器及び通信ソフトウェアをいう。

⑶　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑷　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。

⑸　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

⑹　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

⑺　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をいう。

⑻　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

⑼　データセンター

耐震性に優れた建物にシステムを収容して高速な通信回路を引き込み、空調設備や入退室管理、カメラによる監視等のセキュリティ対策を施した施設をいう。

⑽　クラウド

外部のデータセンター等でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念をいう。

第３節　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本法人の情報資産に関する情報セキュリティ対策の最上位に位置するものである。

第４節　適用範囲

本ポリシーの適用範囲は、本法人が管理する全ての情報資産とする。

本ポリシーの対象者は、教職員等とする。

第５節　教職員等の遵守義務

教職員等は、情報セキュリティの重要性について、共通の認識を持ち、情報セキュリティポリシーを遵守しなければならない。

第６節　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

⑴　意図的な脅威（故意）

不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃を始めとする部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

⑵　非意図的な脅威（過失）

情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・消去等

⑶　災害等による脅威

地震、落雷、火災等の災害によるサービス及び業務の停止等

⑷　必要資源の不足による脅威

大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

⑸　故障等による脅威

電力供給の途絶、通信の途絶、水道供給の途絶等のインフラ障害からの波及等

第７節　情報セキュリティ対策

上記第６節の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

⑴　組織体制

本法人の情報資産について、情報セキュリティ対策を推進する組織体制

を確立する。

⑵ 情報資産の分類と管理

本法人の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

⑶ 物理的セキュリティ対策

サーバ、コンピュータ室、通信回線、教職員等のパソコン及びモバイル端末等の管理について、物理的な対策を講じる。

⑷ 人的セキュリティ対策

情報セキュリティに関し、教職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

⑸ 技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

⑹ 運用におけるセキュリティ対策

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じる。

第８節　情報セキュリティ監査及び自己点検

情報セキュリティポリシーの遵守状況を検証するため、必要に応じて情報セキュリティ監査及び自己点検を実施する。

第９節　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合には、情報セキュリティポリシーを見直す。

第10節　情報セキュリティ対策基準の策定

上記第７節から第９節まで規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

第11節　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本法人の運営に重大な支障を及ぼすおそれがあることから非公開とする。

第２章　情報セキュリティ対策基準

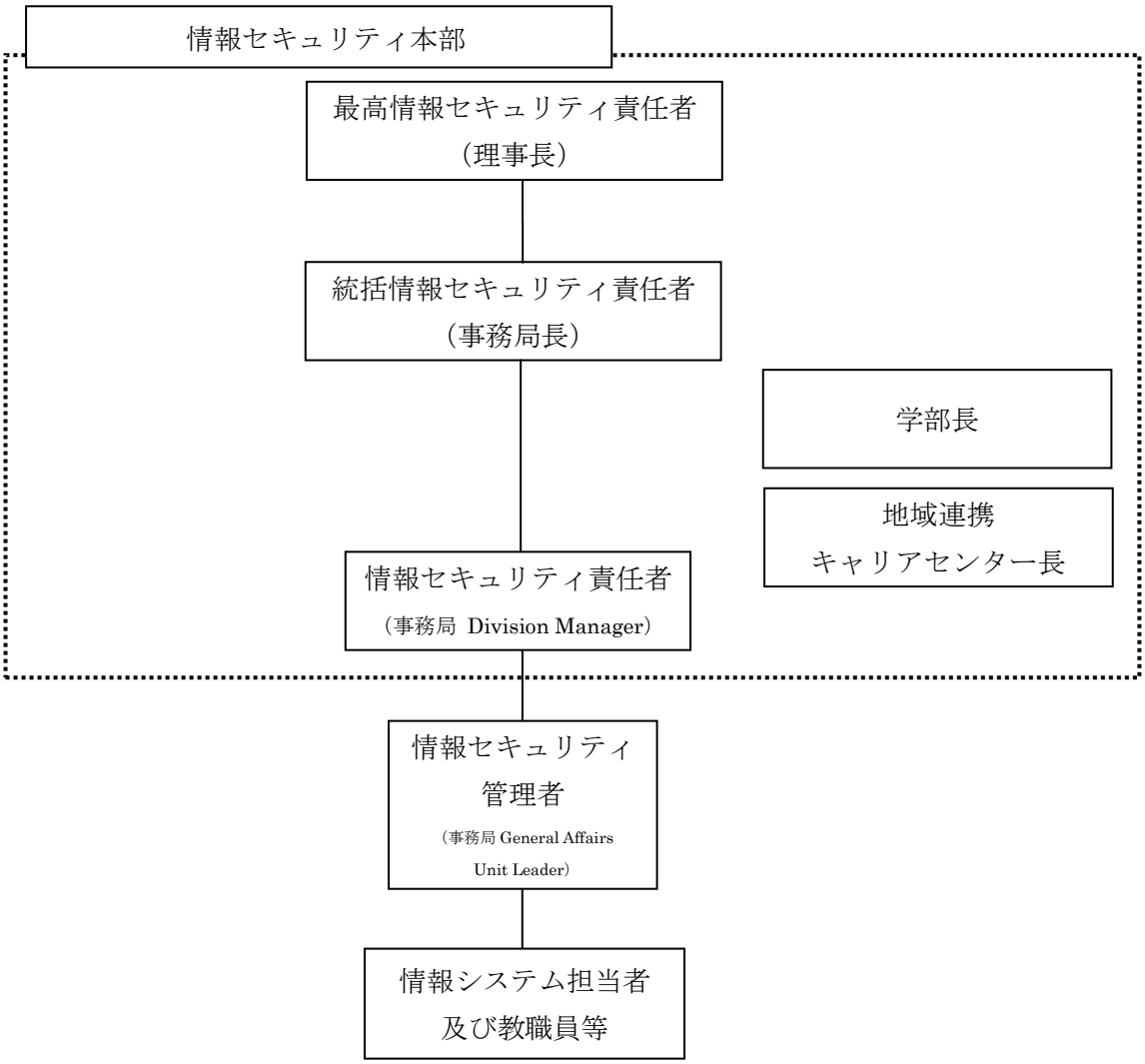
第１節　組織体制

１　組織体制

本法人の情報セキュリティ管理については、次の組織体制とする。（下図参照）

⑴　最高情報セキュリティ責任者
⑵　統括情報セキュリティ責任者
⑶　情報セキュリティ責任者
⑷　情報セキュリティ管理者
⑸　情報システム担当者
⑹　情報セキュリティ本部

組織体系図



２　権限及び責任

⑴　最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

理事長を、CISOとする。CISOは、本法人における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

⑵　統括情報セキュリティ責任者

①　事務局長を、統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISOを補佐しなければならない。

②　統括情報セキュリティ責任者は、次の事項に関する権限及び責任を有する。

ア　CISOが不在のとき、又は欠けたときは、自らの判断に基づき必要かつ十分な措置を行うこと。

イ　本法人の全てのネットワーク、情報システム等における情報セキュリティ対策に関すること。

ウ　本法人の全てのネットワーク、情報システム等における開発、設定の変更、運用、見直し等を行うこと。

エ　情報セキュリティ責任者、情報セキュリティ管理者に対して、情報セキュリティに関する指導及び助言を行うこと。

③　統括情報セキュリティ責任者は、緊急時にはCISOに報告を行うとともに、回復のための対策を講じなければならない。

⑶　情報セキュリティ責任者

①　事務局Division Managerを、情報セキュリティ責任者とする。

②　情報セキュリティ責任者は、次の事項に関する権限及び責任を有する。

ア　学部、事務局又は地域連携キャリアセンターの情報セキュリティ対策に関すること。

イ　学部、事務局又は地域連携キャリアセンターの情報システム等における開発、設定の変更、運用、見直し等を行うこと。

ウ　情報セキュリティ管理者に対して、情報セキュリティに関する指導及び助言を行うこと。

⑷　情報セキュリティ管理者

①　事務局General Affairs Unit Leaderを、情報セキュリティ管理者とする。

②　情報セキュリティ管理者は次の事項に関する権限を有する。

ア　情報セキュリティ対策に関すること。

イ　情報システム等における情報セキュリティ対策に関すること。

ウ　情報システムにおける開発、設定の変更、運用、見直し等を行うこ

と。この場合において、事前に統括情報セキュリティ責任者と協議すること。

エ　情報システム等を使用する教職員等に対して、情報セキュリティに関する指導及び助言を行うこと。

⑸　情報システム担当者

情報セキュリティ管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を、情報システム担当者とする。

⑹　情報セキュリティ本部

本法人の情報セキュリティ対策を統一的に行うため、情報セキュリティ本部において、情報セキュリティポリシーや緊急時対応計画の見直し等、情報セキュリティに関する重要な事項を決定する。

第２節　情報資産の分類と管理方法

１　情報資産の分類

本法人における情報資産は、重要性により次のとおり分類し、当該分類に基づき適切に管理するものとする。

分類	分類基準
非公開情報	本法人が保有する情報資産のうち、個人番号、特定個人情報及び個人情報並びに重要度が高く、かつ漏えいした場合、著しく本法人の信用や利益を損なうもの
限定公開情報	本法人が保有する情報資産のうち、教職員等の限定された者のみに開示すべきもの
公開情報	本法人が保有する情報資産のうち、内外を問わず不特定多数の者に開示できるもの（ホームページや広報誌等を通じて積極的に発信する情報等を含む。）

２　情報資産の管理責任

⑴　情報セキュリティ管理者は、情報資産について管理責任を有するものとする。

⑵　情報資産が複製された場合には、当該情報資産の複製物も１の分類に基づき管理しなければならない。

３　情報資産の分類の表示

教職員等は、情報資産について、必要に応じてファイル名、格納する電磁的記録媒体のラベル等に情報資産の分類を表示する等、適切に管理しなければならない。

４　情報の作成

⑴　教職員等は、業務上必要のない情報を作成してはならない。

⑵　情報を作成する者は、作成途中の情報についても、紛失や流出等を防

止しなければならない。また、情報の作成途中で不要になった場合は、当該情報を消去しなければならない。

５　情報資産の利用

⑴　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

⑵　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

⑶　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

６　情報資産の保管

⑴　情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

⑵　個人番号及び特定個人情報をインターネットに接続されているネットワークには保管してはならない。

⑶　限定公開以上の情報を本法人の内部共有ファイル以外に保管してはならない。ただし、やむを得ず保管しようとする場合は、セキュリティへの影響度を詳細に調査した上で、暗号化又はパスワードの設定を行わなければならない。

⑷　情報セキュリティ管理者は、重要な情報を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

⑸　情報セキュリティ管理者は、限定公開情報以上の情報を記録した電磁的記録媒体を保管する場合は、施錠可能な場所に保管しなければならない。

７　情報資産の送信

原則として、電子メール等により限定公開情報以上の情報を送信してはならない。ただし、やむを得ない理由により送信する必要がある場合は、暗号化及びパスワードの設定を行わなければならない。

８　情報資産の運搬

車両等により限定公開情報以上の情報資産を運搬する者は、原則として、鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

９　情報資産の提供・公表

⑴　限定公開情報以上の情報資産を外部に提供する者は、原則として、暗号化及びパスワードの設定を行わなければならない。

⑵　限定公開情報以上の情報資産を外部に提供する者は、統括情報セキュリティ責任者の許可を得なければならない。

⑶　情報セキュリティ管理者は、外部に公開する情報資産について、完全性

を確保しなければならない。

10　情報資産の廃棄

⑴　限定公開情報以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

⑵　限定公開情報以上の情報資産を廃棄する者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

⑶　限定公開情報以上の情報資産を記録している電磁的記録媒体を廃棄する者は、統括情報セキュリティ責任者の許可を得なければならない。

⑷　限定公開情報以上の情報資産を取り扱う情報システムを廃止する者は、統括情報セキュリティ責任者の許可を得なければならない。

第３節　物理的セキュリティ

１　サーバ等の管理

⑴ 機器の取付け

統括情報セキュリティ責任者は、サーバ等の機器の取付けを行う場合、火災、水害、ほこり、振動、温度及び湿度等の影響を可能な限り排除した場所に設置し、安易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

⑵　サーバの冗長化

①　統括情報セキュリティ責任者は、重要情報を格納しているサーバ、セキュリティサーバに冗長化等の対策を講じ、情報資産への脅威が発生した場合に、システムの運用が停止しないよう努めなければならない。

②　統括情報セキュリティ責任者は、冗長化を行っている場合であってメインサーバに障害が発生したときは、速やかにセカンダリサーバを起動し、システム運用停止時間を最小限にしなければならない。

⑶　機器の電源

①　統括情報セキュリティ責任者は、施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②　統括情報セキュリティ責任者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

⑷　通信ケーブル等の配線

①　統括情報セキュリティ責任者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用

する等、必要な措置を講じなければならない。

② 統括情報セキュリティ責任者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③ 統括情報セキュリティ責任者は、ネットワーク接続口（ハブのポート等をいう。）を他者が容易に接続できない場所に設置する等、適切に管理しなければならない。

④ 統括情報セキュリティ責任者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

⑸ 機器の保守及び修理

① 統括情報セキュリティ責任者は、限定公開情報以上の情報資産を取り扱うサーバ等の機器の保守を実施しなければならない。

② 統括情報セキュリティ責任者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。ただし、内容を消去できない場合、統括情報セキュリティ責任者は、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

⑹ 大学外への機器の設置

統括情報セキュリティ管理者は、大学外にサーバ等の機器を設置する場合、CISOの承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

⑺ 機器の廃棄等

統括情報セキュリティ責任者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

２　管理区域の管理

⑴ 管理区域の構造等

① 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「サーバ室」という。）又は電磁的記録媒体の保管庫で、統括情報セキュリティ責任者が指定したものをいう。

② 統括情報セキュリティ責任者は、原則として管理区域を１階以下に設けてはならない。

また、原則として外部からの侵入が容易にできないように無窓の外壁にしなければならない。

③ 統括情報セキュリティ責任者は、施設管理部門と連携して、管理区

域から外部に通ずるドアは必要最小限とし、鍵等によって許可されていない立入りを防止しなければならない。

④　統括情報セキュリティ責任者は、原則としてサーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤　統括情報セキュリティ責任者は、管理区域に配置する消化薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

⑵　管理区域の入退室管理等

①　統括情報セキュリティ責任者は、サーバ室への入退室を許可された者のみに制限し、入退室管理簿の記載等による入退室管理を行わなければならない。

②　教職員等は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③　統括情報セキュリティ責任者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立入区域を制限した上で、管理区域への入退室を許可された教職員等が付き添うものとし、外見上教職員等と区別できる措置を講じなければならない。

④　統括情報セキュリティ責任者は、サーバ室に本法人の情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

⑶　機器等の搬入出

①　統括情報セキュリティ責任者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ教職員等又は委託した事業者に確認を行わせなければならない。

②　統括情報セキュリティ責任者は、サーバ室の機器等の搬入出について、教職員等を立ち会わせなければならない。

３　通信回線及び通信回線装置の管理

⑴　構内の通信回線等の適切な管理

統括情報セキュリティ責任者は、構内の通信回線及び通信回線装置を適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

⑵　外部へのネットワーク接続の限定措置

統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最小限に限定し、できる限り接続ポイントを減らさなければならない。

⑶　通信回線に利用する回線の選択等

統括情報セキュリティ責任者は、限定公開情報以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準

を検討の上、適切な回線を選択しなければならない。また、原則として、送受信される情報の暗号化を行わなければならない。

⑷ 回線の十分なセキュリティ対策の実施

統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途中に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑸ 回線の継続性の確保

統括情報セキュリティ責任者は、限定公開以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じて、回線を冗長構成にする等の措置を講じなければならない。

４　教職員等のパソコン等の管理

⑴ パソコン等の盗難防止措置

統括情報セキュリティ責任者は、盗難防止のため、業務で使用するときを除き、施錠保管等の物理的措置を講じなければならない。また、電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

⑵ 情報システムへのログインパスワードの設定等

統括情報セキュリティ責任者は、情報システムへのログインについて、パスワード、生体認証等の認証情報の入力を必要とするように設定する等、本人以外のログインを防止する措置を講じなければならない。

第４節　人的セキュリティ

１　教職員等の遵守事項

⑴ 教職員等の遵守事項

① 教職員等は、情報セキュリティポリシーを遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

② 教職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③ 教職員等は、統括情報セキュリティ責任者が指定したパソコン以外に個人番号及び特定個人情報を記録してはならない。

④ 教職員等は、統括情報セキュリティ責任者が指定する内部ネットワークの共有フォルダ以外に個人情報、人事記録等の特定の教職員等しか取り扱えないデータを記録してはならない。ただし、やむを得ず保管しようとする場合は、セキュリティへの影響度を詳細に調査した上

で、統括情報セキュリティ責任者の許可を得た上、暗号化又はパスワードの設定を行わなければならない。

⑤　教職員等は、本法人から支給されたパソコン、モバイル端末及び電磁的記録媒体等以外を原則業務利用してはならない。

⑥　教職員等は、本法人から支給されたパソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を統括情報セキュリティ責任者の許可なく変更してはならない。

⑦　教職員等は、パソコン、モバイル端末及び電磁的記録媒体等について、第三者に使用されること又は閲覧されることがないように、離席時のパソコン及びモバイル端末のロック、並びに電磁的記録媒体等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

⑧　教職員等は、人事異動及び退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。

また、その後も業務上知り得た情報を漏らしてはならない。

⑵　情報セキュリティポリシーの供覧

統括情報セキュリティ責任者は、教職員等が常に情報セキュリティポリシーを閲覧できるようにしなければならない。

⑶　外部委託事業者に対する説明

統括情報セキュリティ責任者は、本法人の情報資産を取り扱う業務を外部委託事業者（外部委託事業者から再委託を受ける事業者及び指定管理者を含む。以下同じ。）に委託する場合、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

２　研修及び訓練

⑴　情報セキュリティに関する研修及び訓練

統括情報セキュリティ責任者は、必要に応じて情報セキュリティに関する研修及び訓練を実施しなければならない。

⑵　研修の実施

①　統括情報セキュリティ責任者は、教職員等及び学生に対する情報セキュリティに関する研修を必要に応じて実施しなければならない。

②　研修は、教職員等それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑶　緊急時対応訓練

統括情報セキュリティ責任者は、緊急時対応を想定した訓練を必要に応じて実施しなければならない。訓練は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を定め、また、効果的に実施できるようにしなければならない。

⑷　研修及び訓練への参加

教職員等は、定められた研修及び訓練に参加しなければならない。

３　情報セキュリティインシデントの報告

⑴　事故等の報告

①　教職員等は、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下「情報セキュリティインシデント」という。）を認知した場合、速やかに情報セキュリティ管理者に報告しなければならない。

②　報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び統括情報セキュリティ責任者に報告しなければならない。

③　統括情報セキュリティ責任者は、必要に応じてCISOに報告しなければならない。

⑵　住民等外部からの事故等の報告

①　教職員等は、本法人が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、速やかに情報セキュリティ管理者に報告しなければならない。

②　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

③　統括情報セキュリティ責任者は、必要に応じてCISOに報告しなければならない。

⑶　情報セキュリティインシデント原因の究明・記録、再発防止等

①　情報セキュリティ責任者は、情報セキュリティ管理者と連携し、情報セキュリティインシデント原因を究明し、記録を保存しなければならない。

②　情報セキュリティ責任者は、情報セキュリティインシデントの原因究明の結果及び再発防止策を統括情報セキュリティ責任者に報告しなければならない。また、情報セキュリティインシデントのうち重要なものについて、統括情報セキュリティ責任者は、その原因究明の結果及び再発防止策をCISOに報告しなければならない。

③　CISOは、統括情報セキュリティ責任者から情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

４　ID、パスワード等の管理

⑴　IDの取扱い

①　情報セキュリティ管理者は、業務を遂行する上で必要となる教職員等にIDを配布しなければならない。

②　教職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

ア　自己が利用しているIDを他者に利用させないこと。

イ　共用IDを利用する場合は、共用IDの利用者以外に利用させないこと。

⑵ パスワードの取扱い

教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① パスワードを他者に知られないように管理すること。

② パスワードを秘密にし、パスワードの照会等には一切応じないこと。

③ 原則として、パスワードは次のとおり設定すること。

ア　最低８文字以上とすること。

イ　英字大文字、英字小文字、数字の３種類を組み合わせること。

ウ　記号（！“＃＄％＆‘() @～？＜＞,.：;）は使用しないこと。

④ パスワードが流失したおそれがある場合には、情報システム管理者に速やかに報告し、パスワードを速やかに変更すること。

⑤ パスワードを定期的に変更すること。ただし、有効日数は設定しない。

⑥ 複数の情報システムを扱う場合には、同一のパスワードをシステム間で用いないこと。

⑦ 仮のパスワードがある場合は、最初のログイン時点で変更すること。

⑧ パソコン及びモバイル端末等にパスワードを記憶させないこと。

⑨ 原則として、パスワードを共有しないこと。

第５節　技術的セキュリティ

１　コンピュータ及びネットワークの管理

⑴ ファイル共有サーバの設定等

① 統括情報セキュリティ責任者は、教職員等が使用できるファイル共有サーバの容量を設定し、教職員等に周知しなければならない。

② 統括情報セキュリティ責任者は、ファイル共有サーバを部門等の単位で構成し、教職員等が他の部門等のフォルダ及びファイルを閲覧及び使用できないように設定しなければならない。

③ 統括情報セキュリティ責任者は、個人情報、人事記録等、特定の教職員等しか取り扱えないデータについて、別途フォルダを作成する等の措置を講じ、同一部門であっても担当教職員等以外の教職員等が閲覧及び使用できないようにしなければならない。

⑵ バックアップの実施

情報セキュリティ管理者は、サーバ等に記録された情報について、必要に応じて定期的にバックアップを実施しなければならない。

⑶ 他団体との情報システムに関する情報等の交換

情報セキュリティ管理者は、他団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定

め、統括情報セキュリティ責任者の許可を得なければならない。

⑷　システム管理記録及び作業の確認

①　情報セキュリティ管理者は、情報システムにおいて、システムの変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

②　情報セキュリティ管理者、情報システム担当者又は契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

⑸　情報システム仕様書等の管理

情報セキュリティ管理者は、情報システム仕様書及びネットワーク構成図について、業務上必要とする者以外の者による閲覧、紛失等がないよう、適切に管理しなければならない。

⑹　ログの取得等

①　情報セキュリティ管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。ただし、教職員等が開発した簡易ツール等で、ログ確保ができないものはこの限りではない。

②　情報セキュリティ管理者は、ログとして取得する項目、保存期間、取得方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③　情報セキュリティ管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

⑺　障害記録

情報セキュリティ管理者は、教職員等からのシステム障害の報告、システム障害に対する対処結果等を、障害記録として記録し、適切に保存しなければならない。

⑻　ネットワークの接続制御、経路制御等

①　統括情報セキュリティ責任者は、接続制御（フィルタリングをいう。）及び経路制御（ルーティングをいう。）について、設定の不整合が発生しないように、ファイアウォール、ルータ等を設定しなければならない。

②　統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑼　外部の者が利用できるシステムの分離等

統括情報セキュリティ責任者は、外部の者が利用できるシステムについて、必要に応じて他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

⑽　外部ネットワークとの接続制限等

①　情報セキュリティ管理者は、ネットワークを外部ネットワークと接続しようとする場合には、統括情報セキュリティ責任者の許可を得なければならない。

②　情報セキュリティ管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を調査し、構内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③　情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん、システムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④　情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑾　複合機のセキュリティ管理

①　情報セキュリティ管理者は、複合機（プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。以下同じ。）を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

②　情報セキュリティ管理者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③　情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

⑿　特定用途機器のセキュリティ管理

情報セキュリティ管理者は、特定用途機器（テレビ会議システム、IP電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものをいう。以下同じ。）について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

⒀　無線LAN及びネットワークの盗聴対策

①　統括情報セキュリティ責任者は、無線LANの利用を認める場合、解読

が困難な暗号化及び認証技術の使用を義務付けなければならない。

② 統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、必要に応じて暗号化等の措置を講じなければならない。

⑭ 電子メールのセキュリティ管理

統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、電子メールの運用を停止しなければならない。

⑮ 電子メールの利用制限

① 教職員等は、業務上必要のない送信先に電子メールを送信してはならない。

② 教職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

③ 教職員等は、限定公開情報以上の情報の電子メールを誤送信した場合は、情報セキュリティ管理者に速やかに報告しなければならない。

⑯ 無許可ソフトウェアの導入等の禁止

① 教職員等は、支給されたパソコンやモバイル端末等に無断でソフトウェアを導入してはならない。

② 教職員等は、業務上の必要がある場合に限り、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者は、ソフトウェアのライセンスを管理しなければならない。

③ 教職員等は、不正にコピーしたソフトウェアを利用してはならない。

⑰ 機器構成の変更の制限

① 教職員等は、支給されたパソコンやモバイル端末等に対し機器の改造、増設及び交換を行ってはならない。

② 教職員等は、業務上、パソコンやモバイル端末等に対し機器の改造、増設及び交換を行う必要がある場合には、統括情報セキュリティ責任者の許可を得なければならない。

⑱ 無許可でのネットワーク接続の禁止

教職員等は、統括情報セキュリティ責任者の許可なくパソコンやモバイル端末等を本法人の内部ネットワークに接続してはならない。

⑲ 業務以外の目的でのウェブ閲覧の禁止

① 教職員等は、業務以外の目的でウェブを閲覧してはならない。

② 情報セキュリティ管理者は、教職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合、統括情報セキュリティ責任者及び情報セキュリティ責任者に通知し適切な措置を求めなければならない。

２　アクセス制御

⑴　アクセス制御等

統括情報セキュリティ責任者は、ネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなければならない。

⑵　利用者IDの取扱い

①　情報セキュリティ管理者は、利用者IDの取扱いについて、次の事項を措置しなければならない。

ア　利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向又は退職に伴う利用者IDの取扱い等の方法を定めること。

イ　利用されていない利用者IDが放置されないように点検すること。

②　情報セキュリティ管理者は、業務上必要がなくなった場合は、利用者登録を抹消するようにしなければならない。

⑶　特権を付与されたIDの管理等

統括情報セキュリティ責任者は、特権を付与されたIDの管理等について、次の事項を措置しなければならない。

①　管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理すること。

②　特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせないこと。

③　特権を付与されたID及びパスワードについて、定期変更、入力回数制限等のセキュリティ機能を、他よりも強化すること。

⑷　外部からのアクセス等の制限

①　教職員等、外部委託事業者等が外部から本法人内のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者の許可を得なければならない。

②　統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③　統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④　統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途中の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤　統括情報セキュリティ責任者は、外部からのアクセスに利用するパソコンやモバイル端末等を教職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥　教職員等は、外部から持ち帰った又は持ち込んだパソコンやモバイル端末等を本法人内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

⑦　統括情報セキュリティ責任者は、公衆通信回線（公衆無線LAN等）の構外の通信回線を本法人内ネットワークに接続することは原則として、禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のID及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ICカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

⑸　自動識別の設定

情報セキュリティ管理者は、ネットワークで使用される機器について、必要に応じて機器固有情報によって、端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

⑹　ログイン時の表示等

情報セキュリティ管理者は、必要に応じてログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員等がログインしたことを確認することができるようシステムを設定しなければならない。

⑺　パスワードに関する情報の管理

①　パスワードに関する情報は各自で厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

②　情報セキュリティ管理者は、教職員等に対してパスワードを発行する場合は、必要に応じて仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

⑻　特権による接続時間の制限

統括情報セキュリティ責任者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

３　システム開発、導入、保守等

⑴　情報システムの調達

①　情報セキュリティ管理者は、情報システム開発、導入、保守等の調達並びに機器及びソフトウェアの調達に当たっては、統括情報セキュリティ責任者に協議しなければならない。

②　情報セキュリティ管理者は、情報システム開発、導入、保守等の調達

に当たっては、統括情報セキュリティ責任者と協議の上、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

③　情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、統括情報セキュリティ責任者と協議の上、当該製品のセキュリティ機能を調査し、情報セキュリティ上の問題がないことを確認しなければならない。

⑵　情報システムの開発

①　情報セキュリティ管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

②　情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発用IDを削除しなければならない。

③　情報セキュリティ管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

④　情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

⑤　情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

⑶　情報システムの導入

①　情報セキュリティ管理者は、システム開発、保守及びテスト環境とシステム運用環境を可能な限り分離しなければならない。

②　情報セキュリティ管理者は、システム開発、保守及びテスト環境からシステム運用環境への移行について、システム開発及び保守計画の策定時に手順を明確にしなければならない。

③　情報セキュリティ管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

④　情報セキュリティ管理者は、導入するシステム及びサービスの可用性が確保されていることを確認した上で導入しなければならない。

⑤　情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼動している情報システムに接続する前に十分な試験を行わなければならない。

⑥　情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

⑦　情報セキュリティ管理者は、個人情報、特定個人情報及び機密性の高い実際のデータを、テストデータに使用してはならない。

⑧　情報セキュリティ管理者は、開発したシステムについて受け入れテ

ストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

⑷　システム開発及び保守に関連する資料等の整備・保管

①　情報セキュリティ管理者は、システム開発及び保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

②　情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

③　情報セキュリティ管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

⑸　情報システムにおける入出力データの正確性の確保

①　情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②　情報セキュリティ管理者は、故意若しくは過失により情報が改ざんされる、又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③　情報セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

⑹　情報システムの変更管理

情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

⑺　開発及び保守用のソフトウェアの更新等

情報セキュリティ管理者は、開発及び保守用のソフトウェア等を更新する場合、他の情報システムとの整合性を確認しなければならない。

⑻　システム更新又は統合時の検証等

情報セキュリティ管理者は、システム更新又は統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新又は統合後の業務運営体制の検証を行わなければならない。

4　不正プログラム対策

⑴　情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、不正プログラム対策として、次の事項を措置しなければならない。

①　サーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させること。

②　不正プログラム対策ソフトウェア及びそのパターンファイルを、常に最新の状態に保つこと。

③　本法人の情報システムにおいて電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、本法人の許可を受けた電磁的記録媒体以外を教職員等に利用させないこと。

④　業務で利用するソフトウェアは、原則として、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。ただし、やむを得ず利用しようとする場合は、セキュリティへの影響度を詳細に調査した上で判断すること。

⑵　教職員等の遵守事項

教職員等は、不正プログラム対策として、次の事項を遵守しなければならない。

①　パソコンやモバイル端末等において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しないこと。

②　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行うこと。

③　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除すること。

④　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施すること。

⑤　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行うこと。

⑥　コンピュータウイルス等の不正プログラムに感染した場合、又は感染が疑われる場合は、LANケーブルの即時取り外しを行うこと。また、無線LAN又は公衆通信回線を利用していた場合は、直ちに利用を中止し、通信を行わない設定への変更を行うこと。

５　不正アクセス対策

⑴　措置

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

①　不要なサービスについて、機能の削除又は停止すること。

②　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、指定する教職員等へ通報するよう設定すること。

③　統括情報セキュリティ責任者は、情報セキュリティ責任者と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

⑵　攻撃の予告

CISO、統括情報セキュリティ責任者及び情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。

また、関係機関と連絡を密にして情報の収集に努めなければならない。

⑶ 記録の保存

CISO、統括情報セキュリティ責任者及び情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成11年法律第128号）違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

⑷ 内部からの攻撃

情報セキュリティ管理者は、教職員等及び外部委託事業者が使用しているパソコンやモバイル端末等からの本法人内のサーバ等に対する攻撃及び外部のサイトに対する攻撃を監視しなければならない。

⑸ 教職員等による不正アクセス

情報セキュリティ管理者は、教職員等による不正アクセスを発見した場合は、統括情報セキュリティ責任者及び情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

⑹ サービス不能攻撃

情報セキュリティ管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

⑺ 標的型攻撃

情報セキュリティ管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

６　セキュリティ情報の収集

⑴ セキュリティホールに関する情報の収集及び共有、ソフトウェアの更新等

情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じて関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

⑵ 不正プログラム等のセキュリティ情報の収集及び周知

情報セキュリティ管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じて対応方法について、教職員等に周知しなければならない。

⑶ 情報セキュリティに関する情報の収集及び共有

情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じて関係者間で共有しなければならない。また、情報セキュリティに関する社会環境、技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を講じなければならない。

第６節　運用

１　情報システムの監視

⑴　情報システムの監視

情報セキュリティ責任者は、情報セキュリティに関する事案を検知するため、情報システム（外部に接続して利用するものを含む。）を必要に応じて監視しなければならない。

⑵　サーバの正確な時刻設定等の措置

情報セキュリティ責任者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を可能な限り講じなければならない。

２　情報セキュリティポリシーの遵守状況の確認

⑴　遵守状況の確認及び対処

①　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について、必要に応じて確認を行い、問題を認めた場合には、速やかに統括情報セキュリティ責任者に報告しなければならない。

②　統括情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

③　統括情報セキュリティ責任者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、必要に応じて確認を行い、問題が発生していた場合には、適切かつ速やかに対処しなければならない。

⑵　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

統括情報セキュリティ責任者は、不正アクセス、不正プログラム等の調査のために、教職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

⑶　教職員等の報告義務

①　教職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者に報告しなければならない。

②　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性が

あると統括情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

３　情報セキュリティ実施手順の策定

⑴　情報セキュリティ実施手順の策定

①　統括情報セキュリティ責任者は、本法人の情報システムに共通する事項について、情報セキュリティポリシーに基づく情報セキュリティ対策を実施するための具体的な手順を定めた実施手順（以下「情報セキュリティ実施手順」という。）を策定しなければならない。

②　情報セキュリティ責任者は、情報システムについて、情報セキュリティ実施手順を策定しなければならない。

③　情報セキュリティ責任者は、情報セキュリティ実施手順の策定に当たって、統括情報セキュリティ責任者の承認を得なければならない。

⑵　情報セキュリティ実施手順の見直し

情報セキュリティ責任者は、情報セキュリティを取り巻く状況の変化、組織体制の変動等に応じて、情報セキュリティ実施手順を見直さなければならない。

４　侵害時の対応

⑴　緊急時対応計画の策定

CISO又は情報セキュリティ本部は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は侵害の発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

⑵　緊急時対応計画に盛り込むべき内容

緊急時対応計画を策定する際には、次の内容を定めなければならない。

①　関係者の連絡先

②　発生した事案に係る報告すべき事項

③　発生した事案への対応措置

④　再発防止措置の策定

⑶　緊急時対応計画の見直し

CISO又は情報セキュリティ本部は、情報セキュリティを取り巻く状況の変化、組織体制の変動等に応じて、緊急時対応計画を見直さなければならない。

５　例外措置

⑴　例外措置の許可

情報セキュリティ管理者及び情報システム担当者は、情報セキュリティ関係規定を遵守することが困難な状況で、事務の適正な遂行を継続す

るため、遵守事項とは異なる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な理由がある場合には、統括情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

⑵　緊急時の例外措置

情報セキュリティ管理者及び情報システム担当者は、事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに統括情報セキュリティ責任者に報告しなければならない。

⑶　例外措置の申請書の管理

情報セキュリティ管理者は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

６　法令遵守

教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

①　著作権法（昭和45年法律第48号）
②　不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
③　個人情報の保護に関する法律（平成15年法律第57号）
④　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）
⑤　サイバーセキュリティ基本法（平成26年法律第104号）
⑥　三条市情報公開条例（平成17年三条市条例第10号）
⑦　三条市個人情報保護法施行条例（令和４年三条市条例第23号）

７　懲戒処分等

⑴　懲戒処分

情報セキュリティポリシーに違反した教職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて懲戒処分の対象とする。

⑵　違反時の対応

教職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

①　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は情報セキュリティ責任者に通知し、適切な措置を求めなければならない。
②　情報セキュリティ管理者等が違反を確認した場合、違反を確認した者は速やかに統括情報セキュリティ責任者及び情報セキュリティ責任者に通知し、適切な措置を求めなければならない。
③　情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該教職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後

速やかに、統括情報セキュリティ責任者は、教職員等の権利を停止あるいは剥奪した旨をCISOに報告しなければならない。

第７節　外部サービスの利用

１　外部委託

⑴　外部委託の実施

情報セキュリティ管理者は、情報システムの外部委託の実施に当たって、外部委託の実施の可否、外部委託事業者の選定基準等を統括情報セキュリティ責任者に協議しなければならない。

⑵　外部委託先の選定基準

①　情報セキュリティ管理者は、外部委託事業者の選定に当たり、選定基準を定めなければならない。

②　情報セキュリティ管理者は、外部委託事業者の選定に当たり、業務内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

③　情報セキュリティ管理者は、クラウドによるシステムを利用する場合、外部委託先がサービス内容に応じた十分な情報セキュリティ対策を確保していることを確認しなければならない。

④　情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

⑶　契約項目

情報セキュリティ管理者は、本法人の情報資産を取り扱う業務を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

①　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

②　次の法令及び関係法令の遵守

ア　著作権法（昭和45年法律第48号）

イ　不正アクセス行為の禁止等に関する法律（平成11年法律第128号）

ウ　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）

エ　三条市個人情報保護法施行条例（令和４年三条市条例第23号）

③　外部委託事業者の責任者、委託内容、作業者及び作業場所の特定

④　提供されるサービスレベルの保証

⑤　外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法

⑥　外部委託事業者の従業員に対する教育の実施

⑦　提供された情報の目的外利用及び受託者以外への提供の禁止

⑧　業務上知り得た情報の守秘義務
⑨　再委託に関する制限事項の遵守
⑩　委託業務終了時の情報資産の返還、廃棄等
⑪　委託業務の定期報告及び緊急時報告義務
⑫　本法人による監査又は検査
⑬　本法人による情報セキュリティインシデント発生時の公表
⑭　情報セキュリティインシデント等に対する損害賠償等の規定

⑷　クラウドによるシステム利用時の契約項目

情報セキュリティ管理者は、クラウドによるシステムを利用する場合には、上記⑶の契約項目に合わせて次の情報セキュリティ要件を明記した契約を締結しなければならない。

①　本店所在地、データセンター及びデータバックアップ先が日本国内にあること。
②　準拠法は日本の法律であり、裁判所も日本国内の裁判所であること。
③　データセンターは十分な情報セキュリティ対策、災害対策を確保していること。

⑸　遵守状況の確認及び是正

①　情報セキュリティ管理者は、外部委託事業者における情報セキュリティ対策の遵守状況について、必要に応じて確認を行い、違反行為を認めた場合には、速やかに是正させなければならない。
②　情報セキュリティ管理者は、外部委託事業者の違反行為が、情報セキュリティ上重大な影響を及ぼす可能性があると判断した場合は、情報セキュリティ責任者、統括情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

２　約款による外部サービスの利用

⑴　約款による外部サービスの利用に係る規程の整備

統括情報セキュリティ責任者は、次の事項を含む約款による外部サービスの利用に関する規程を整備しなければならない。また、原則として、当該サービスの利用において、限定公開情報以上の情報が取り扱われないように規定しなければならない。

①　約款によるサービスを利用してよい範囲
②　業務により利用する約款による外部サービス
③　利用手続及び運用手順

⑵　約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

３　ソーシャルメディアサービスの利用

⑴ 統括情報セキュリティ責任者は、本法人が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

① 本法人のアカウントによる情報発信が、実際の本法人のものであることを明らかにするために、本法人の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

② パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

⑵ 教職員等は、限定公開情報以上の情報はソーシャルメディアサービスで発信してはならない。

⑶ 統括情報セキュリティ責任者は、利用するソーシャルメディアサービスごとの責任者を定めなければならない。

第８節　評価及び見直し

１　監査

⑴ 監査の実施

情報セキュリティ責任者は、情報システムにおける情報セキュリティポリシーの遵守状況について、必要に応じて監査を行わなければならない。

⑵ 監査を行う者の要件

監査を行う者は、原則として、監査及び情報セキュリティに関する専門知識を有する者を基本とする。

⑶ 外部委託事業者に対する監査

情報セキュリティ責任者は、外部委託先に業務を委託している場合、再委託先を含め、外部委託事業者における情報セキュリティポリシーの遵守状況について、必要に応じて監査を行わなければならない。

⑷ 監査結果の報告

情報セキュリティ責任者は、監査の結果を情報セキュリティポリシーの見直し等に活用するため、当該監査結果を取りまとめ、統括情報セキュリティ責任者に報告しなければならない。

２　自己点検

⑴ 自己点検の実施

情報セキュリティ責任者は、情報セキュリティポリシーの遵守状況について、必要に応じて自己点検を行わなければならない。

⑵　自己点検結果の報告

情報セキュリティ責任者は、自己点検の結果を情報セキュリティポリシーの見直し等に活用するため、当該自己点検結果を取りまとめ、統括情報セキュリティ責任者に報告しなければならない。

３　情報セキュリティポリシーの見直し

統括情報セキュリティ責任者は、監査及び自己点検の結果、情報セキュリティに関する状況の変化、組織体制の変動等に応じて、情報セキュリティポリシーの見直しを行うものとする。