公立大学法人前橋工科大学情報セキュリティポリシー

Ⅰ　情報セキュリティ基本方針

公立大学法人前橋工科大学（以下「法人」という。）の設置する前橋工科大学（以下「本学」という。）は、理念「自然と人との共生ならびに持続可能な循環型社会の構築に貢献する知的基盤の創造を推進することによって、文化的で健康な市民生活の実現に寄与し、地域と社会の発展と福祉に貢献する工学を追究する」を掲げている。この理念のもと、学生、教員、職員及び本学関係者は、自由でかつ便利に情報の収集、格納、伝達及び報告といった手段を情報基盤に依存している。そのため、不断の努力の基に情報資産を保全しなければならない。そこで、法人及び本学（以下「大学」という。）の情報基盤を利用する者は、情報のセキュリティポリシーを遵守する責任があり、大学の情報資産を内外から保全し、教育・研究・環境をより質の高いものにするため、情報セキュリティポリシーを整備し実施する責任がある。

１　目　的

大学において情報基盤の整備とそれに関する必要なセキュリティを確保することは、大学の円滑な活動に不可欠である。大学は、情報セキュリティポリシーを定め、大学の全ての構成員の理解と協力により次に揚げる目標の達成に取り組む。

①　大学の情報資産に対する侵害を阻止
②　大学内外の情報セキュリティを侵害する行為の抑止
③　情報資産の重要度による分類と管理
④　情報セキュリティに関する情報取得の支援

２　定　義

本ポリシーでの用語の定義については、内閣官房情報セキュリティ対策推進室がとりまとめた「情報セキュリティポリシーに関するガイドライン」に定める定義を基本とし、付録に示す。

３　情報セキュリティポリシーの構成

情報セキュリティポリシーは、情報セキュリティ基本方針及び情報セキュリティ対策基準から構成する。また、情報セキュリティ対策基準に基づいて、情報資産のセキュリティ対策に関する具体的な運用方針を別途定める。

４　対象範囲

(1) 本ポリシーの対象者は、教員、非常勤教員、事務職員、委託業者、大学院生、

大学生、研究生、来学者その他関係する者全てとする。

(2) 対象となる情報資産は、大学が保有する全ての情報資産及び大学のネットワークに接続される大学管理以外のシステム機器並びにアウトソーシングしたシステム情報及びユーザー情報とする。

5　情報セキュリティ対策

(1) 組織・体制

情報セキュリティ委員会を置き、情報セキュリティ対策を推進する。そのための組織・体制を明確にする。

(2) 情報資産の分類、管理等

情報資産をその内容に応じて分類し、その重要性に応じた情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、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。

(5) 技術的セキュリティ

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。

(6) 運用

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及び情報セキュリティポリシーの運用面の対策を講じるとともに、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため緊急時対応計画を策定するものとする。

(7) 評価及び更新

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評価及び自己点検並びに情報セキュリティ監査を実施する。

情報セキュリティ監査の結果等により、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になった場合には、情報セキュリティポリシーを見直す。

6　本ポリシーの改訂及び運用方針の策定

本ポリシーの改訂及び運用方針の策定は､情報セキュリティ委員会で協議の上、

理事長の議決を経なければならない

Ⅱ　情報セキュリティ対策基準

情報セキュリティ対策基準は、基本方針に定められた情報セキュリティを実施するために遵守すべき行為及び判断等の基準とし、下記１から５までに定めるとおりとする。

１　組織・体制

本ポリシーに基づき大学の情報セキュリティを管理するために、情報セキュリティ委員会を設置し、情報セキュリティ最高責任者、情報セキュリティ管理責任者、情報セキュリティ管理者、ネットワーク管理者及び情報システム管理者を置く。

２　情報資産の分類、管理等

(1) 情報資産の分類

大学の情報資産の適切な保護を維持するため、機密性、完全性、可用性等の観点から情報資産を重要度により分類する。

(2) 情報資産の管理

情報資産の管理方法及び管理責任を規定し、重要度に応じた情報セキュリティ対策を行う。

(3) リスク分析・評価

情報資産の重要性並びに情報資産に対する脅威及び現状における対策の脆弱性からリスク（潜在する損害の大きさ）を評価し、その評価に基づく効果的な情報セキュリティ対策を行う。

３　情報セキュリティ対策の実施

(1) 大学の情報セキュリティに対する侵害の阻止

情報セキュリティ管理責任者は、外部又は内部からの不正アクセスが検出された場合には、関連する通信の遮断又は該当する情報機器の切り離しを実施する。

不正アクセスが継続する場合には、該当情報機器又はそれを接続する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ることができる。

(2) 学内外の情報セキュリティを損ねる加害行為の抑止

学内外を問わず、あらゆる研究・教育機関、企業、組織団体、個人等の情報

資産を侵害してはならない。また、本ポリシーその他の情報セキュリティに関連する法令及び本学が定める規程等を遵守しなければならない。

(3) 情報セキュリティ実施手順等

(1)、(2)に掲げたセキュリティ対策を実施するため、物理的、人的及び技術的な情報セキュリティ実施手順を具体的に定め、実施しなければならない。また、本ポリシーの全ての対象者に、それぞれに応じた教育、研修、啓発等を行い、情報セキュリティの重要性を理解させなければならない。

4　情報セキュリティポリシーの運用

情報セキュリティ最高責任者は、情報セキュリティ管理者等からの情報セキュリティに関する情報の収集及び分析並びに情報資産の運用状況に対する情報セキュリティ診断及び情報セキュリティ監査を実施し、これらの結果を情報セキュリティ委員会に報告しなければならない。

5　情報セキュリティポリシーの評価及び更新

情報セキュリティを取り巻く状況の変化などに対応して有効性を維持するため、定期的又は必要に応じて情報セキュリティポリシーの評価を実施し、その更新を図る。

なお、情報セキュリティポリシーは、策定、導入、運用、評価及び更新を循環的に行う。

附　則

この規程は、平成２５年４月１日から施行する。

附　則

この規程は、平成２８年１１月４日から施行する。

付録　用語の定義

・情報セキュリティポリシー（以下「ポリシー」ともいう。）
大学が所有する情報資産の情報セキュリティ対策について、大学が総合的・体系的かつ具体的にとりまとめたもの．どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定．情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。

・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。

・機密性
情報にアクセスすることを認可された者だけがアクセスできることを確実にすること。

・完全性
情報及び処理方法の正確さ及び安全である状態を完全防護すること。

・可用性
許可された利用者が必要なときに情報にアクセスできることを確実にすること。

・情報資産
情報（電磁的に記録されたもの）及び情報を管理（蓄積・伝送・処理等）する仕組み。情報を管理する仕組みには、情報システム及び情報システムの開発・運用・保守のためのドキュメント類が含まれる。

・情報システム
基盤システム及びそれにつながる全部分システム並びにアウトソーシングシステムがあり、システム機器、ソフトウェア、システム情報及び記録媒体で構成され、これらで情報を管理し業務処理を行うもの。

・システム機器
ネットワーク機器、サーバ、教育用端末、ＰＣ、プリンター等の情報システムを動作させるハードウェアのこと。

・システム情報
パスワードファイル、アクセス記録、ネットワーク設定情報等の情報システムを動作及び管理するために必要な設定情報及び仕様書・設計書のこと。

・記録媒体
情報を電磁的に記録した媒体のこと。