公立大学法人前橋工科大学情報セキュリティポリシー

公立大学法人前橋工科大学情報セキュリティポリシー（以下「本ポリシー」という。）は、地方自治法（昭和 22 年法律第 67 号）第 244 条の 6 及び地方独立行政法人法（平成 15 年法律第 118 号）第 24 条の 2 の規定並びに地方自治法の一部を改正する法律（令和 6 年法律第 65 号）による改正法の施行（令和 8 年 4 月 1 日）に対応し、総務大臣指針を踏まえて、公立大学法人前橋工科大学（以下「法人」という。）が情報セキュリティを確保するための方針として策定するものである。

また、本ポリシーは、法人が設置する前橋工科大学（以下「本学」という。）の情報資産を内外の脅威から適切に保護し、教育・研究・業務の継続性及び社会的信頼を確保することを目的とする。

なお、本ポリシーにおいて「情報セキュリティ」とは、サイバーセキュリティを含む情報資産の機密性、完全性及び可用性の確保に関する事項をいう。

Ⅰ　情報セキュリティ基本方針

本学は、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。そこで、法人及び本学（以下「大学」という。）は、サイバー攻撃、不正アクセス、情報漏えい、システム障害等のリスクから情報資産及び情報基盤を保護するため、情報セキュリティの確保を重要な経営課題として位置づけ、本ポリシーを定め、これに基づく必要な措置を講じるものとする。

1　基本方針

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の防止及び被害の最小化
②　サイバー攻撃その他の情報セキュリティを脅かす行為の抑止
③　情報資産の重要度に応じた適切な分類及び管理
④　情報セキュリティに関する意識向上及び体制強化

2　定　義

本ポリシーでの用語の定義については、内閣官房が示す「情報セキュリティポリシーに関するガイドライン」の定義を基本としつつ、最新の法令及び総務大臣指針に基づき、本学の運用に必要な補足定義を付録に示す。

3　情報セキュリティポリシーの構成

本ポリシーは、地方自治法第 244 条の 6 に基づくサイバーセキュリティ確保方針として、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き、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及び実施手順を別途定める。

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並びに、大学のネットワークに接続される大学管理外の機器、アウトソーシングしたシステム、ユーザー情報、加えてクラウドサービスや外部委託先が取り扱う情報資産等を含むものとする。

5　情報セキュリティ対策

(1) 組織・体制

法人は、地方独立行政法人としての責任のもと、情報セキュリティ委員会を設置し、情報セキュリティ対策を統括的に推進するための組織及び体制を明確にする。

(2) 情報資産の分類、管理等

情報資産をその内容及び重要性に応じて分類し、適切な情報セキュリティ対策を講じる。

(3) 物理的セキュリティ

サーバ、情報システム室、通信回線、端末等について、必要な物理的セキュリティ対策を講じる。

(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。また、本ポリシーは、地方自治法第 244 条の 6 第 3 項に基づき総務大臣が示す指針を踏まえ、必要に応じて見直しを行う。

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、サイバー攻撃を含む多様な脅威から大学の情報資産を保護するため、組織的、人的、物理的及び技術的対策を体系的に定めるものとする。

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(Plan)、運用(Do)、評価(Check)、見直し（Action）の PDCA サイクルを継続的に実施する。

６　公表

本ポリシーを策定又は変更した場合は、地方自治法第 244 条の 6 第 2 項に基づき、学内周知を行うとともに、Web サイト等により公表し、法人として説明責任を果たす。

附　則

このポリシーは、平成２５年４月１日から施行する。

附　則

このポリシーは、平成２８年１１月４日から施行する。

附　則

このポリシーは、令和８年４月１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

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。

・サイバーセキュリティ

ネットワーク・情報システム・クラウド環境等のサイバー空間に係る情報セキュリティをいう。情報セキュリティの一部であり、不正アクセス、マルウェア、サービス妨害等への対策を含む。

・機密性

認可された者のみが情報にアクセスできる状態を確保すること。

・完全性

情報及び処理方法の正確さ・完全性を保ち、改ざん・破壊・誤りを防止すること。

・可用性

許可された利用者が必要なときに情報・システムにアクセスできる状態を確保すること。

・情報資産

電磁的に記録された情報及びそれを蓄積・伝送・処理・表示するための仕組み全般。情報資産には、情報システム、その開発・運用・保守ドキュメント、クラウドサービス（SaaS／PaaS／IaaS 等）、外部委託先が取り扱う本学の情報資産を含む。

・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、ストレージ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、ログ、ネットワーク設定情報、構成情報、仕様書・設計書・運用手順等、情報システムの動作・管理に必要な設定情報及び技術文書。

・記録媒体

電磁的に情報を記録する媒体（例：HDD／SSD、USB メモリ、光学ディスク、磁気テープ、メモリーカード等）

・クラウドサービス

第三者が提供する計算資源・アプリケーション・プラットフォーム等をネットワーク経由で利用する形態（SaaS／PaaS／IaaS）。本学が契約・利用するクラウド上に保管・処理される本学の情報資産を含む。

・外部委託（アウトソーシング）

本学が業務やシステムの一部・全部を外部事業者へ委託すること。委託先が取り扱う本学の情報資産は本ポリシーの管理対象であり、契約におけるセキュリティ要件、監督、遵守確認の対象となる。

・脅威

情報資産の機密性・完全性・可用性を損なう可能性のある要因（例：不正アクセス、マルウェア、ランサムウェア、人的過誤、災害、設備故障、供給停止等）

・脆弱性

情報資産や管理プロセスに存在する弱点。脆弱性は脅威に悪用され得る。

・リスク

脅威と脆弱性の組合せにより発生し得る潜在的損害の大きさ。一般に発生確率×影響度等で評価する。

・情報セキュリティインシデント

情報資産の機密性・完全性・可用性を損なう事象、またはその疑い。（例：不正アクセス、情報漏えい、誤送信、マルウェア感染、媒体紛失等。）

・情報資産の分類

機密性・完全性・可用性の観点から重要度に応じて情報資産を区分すること。

・アクセス制御

認可された利用者・端末のみが、定められた権限で情報資産へアクセスできるように識別・認証・権限付与・ログ監視等を行う管理。

・ログ

システム・ネットワーク・アプリケーション等の動作・アクセス・変更履歴を記録したもの。保全・分析・監査の対象となる。

・個人情報

法令に定める、特定の個人を識別できる情報。漏えい・滅失・毀損の防止その他安全管理措置を要し、重大事案が生じた場合は関係機関への報告・本人通知を要する（個人情報保護法に基づく）。