

# 情報セキュリティ方針

本文書は、「情報セキュリティ基本方針」に従って、本法人が保有する情報資産を改竄、破壊、漏洩等から保護するためのガイドラインをまとめたものである。

## 1 定義

情報セキュリティ方針で使用する用語の定義は、次のとおりとする。

### (1) 情報システム

本法人が管理するハードウェア、ソフトウェア、ネットワーク、記録媒体で構成され、その処理を行う仕組みをいう。

### (2) 情報

情報システムで扱うデータをいう。

### (3) 情報資産

情報システム(これらに付随する開発、運用及び保守のための資料等を含む)並びに情報をいう。

### (4) 情報セキュリティ

情報資産の機密性<sup>注1</sup>、完全性<sup>注2</sup>及び可用性<sup>注3</sup>を維持すること並びに定められた範囲での利用可能な状態を維持することをいう。

## 2 趣旨及び位置づけ

ポリシーは、次の目的を持って策定され、情報システムを利用して情報を扱うにあたって遵守しなければならない最低限の事項をまとめたものである。詳細は、関連法令<sup>注4</sup>、本法人の各種規程及び内規等に従うものとする。

### (1) 本法人の情報セキュリティに対する侵害の阻止

### (2) 本法人内外の情報セキュリティを損ねる加害行為の抑止

### (3) 情報資産の分類と管理

### (4) 情報セキュリティの評価と更新

## 3 対象範囲ならびに対象者

本法人におけるポリシーの対象範囲は、ハードウェア、ソフトウェア、記録媒体等の情報システム等及びすべての情報のうち、情報システムに電磁的に記録される情報とする。ポリシーの対象者は、本法人の情報資産を利用する教育職員、事務職員、臨時職員、事務補助職員、非常勤講師、委託業者、大学院生、大学生、短期大学生、科目等履修生等の本法人学生及び研究会等で来学した者等、本学の情報資産を利用するすべての者（以下、「対象者」という。）とする。

## 4 ポリシーの公開対象者

基本方針及び方針は、学内外に公開する。対策基準は、機密文書として取り扱い、原則として学外に公開してはならない。ただし、公開しなければ職務を遂行できない場合には、機密保持契約を締結した上で公開を認める場合がある。

## 5 情報セキュリティ管理体制

本法人が所有するすべての情報資産の情報セキュリティを保護・管理するために情報セキュリティ最高責任者（以下「C I O」という。）を置き、C I Oの下に情報セキュリティ対策を推進し、管理するための体制を確立するものとする。

## 6 情報資産の分類と管理

情報資産をその内容に応じて分類し、管理責任を明確にするとともに、情報セキュリティ対策基準において定める重要性に応じた情報セキュリティ対策を行うものとする。

## 7 情報資産への脅威

情報セキュリティ対策を推進する上で、特に情報資産への脅威は、その発生度合いや発生した場合の影響を考慮すると、次のとおりである。

- (1) 大学構成員以外の者による故意の不正アクセスまたは不正操作によるデータやプログラムの持出し、傍受、改変若しくは消去、及び機器若しくは媒体の盗難等。
- (2) 学構成員による意図しない操作または故意の不正アクセス若しくは不正操作によるデータやプログラムの持出し、盗難、改変または消去、及び機器または媒体の盗難、規格外の端末接続によるデータの漏洩等。
- (3) 地震、落雷、火災等の災害、事故、故障等によるサービス又は業務の停止。

## 8 情報セキュリティ対策

第7に掲げる脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じるものとする。

### (1) 物理的セキュリティ対策

ネットワーク及び情報システムを設置する施設への不正な立入りならびに情報資産への損傷、妨害等から保護するために必要な物理的な対策

### (2) 人的セキュリティ対策

情報セキュリティ対策に関する権限や責任を定め、すべての大学構成員等にポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるために必要な対策。

### (3) 技術及び運用におけるセキュリティ対策

情報資産を外部または内部からの不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策及びシステム開発等の外部委託、ネットワークの監視、ポリシー遵守状況確認等の運用面の対策。  
緊急事態が発生した際に、迅速な対応を可能とするための対策。

## 9 情報セキュリティ対策基準の策定

学内の様々な情報資産について、第8の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為、判断等の基準を統一的な水準で定める必要があるため、C I Oは、情報セキュリティ対策を行ううえで必要となる基本的な基準を明記した学校法人松山大学情報セキュリティ対策基準（以下「対策基準」という。）を別途策定するものとする。

#### 10 情報セキュリティ実施手順の策定

情報システム管理者（情報資産を所掌する部・課(室を含む)の長をいう）は、情報資産に対する脅威および情報資産の重要性に対応して、対策基準に定める基本的な基準に基づき、その所掌する情報資産について、情報セキュリティ対策の実施手順を策定するものとする。

#### 11 情報資産の利用制限等

C I Oは、本学が管理する情報資産を利用する者のうち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に違反した者に対して、本学の職員及び学生であるなしに関わらず情報資産の利用を制限することがある。また、違反した本学の職員又は学生については、別に定めるところにより懲戒の対象となる場合がある。

#### 12 評価及び見直しの実施

C I Oは、ポリシーが遵守されていることを検証するため、定期的に監査を実施したうえで、その結果に基づきポリシーに定める事項及び情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応させるため、必要であると認めるときはポリシーの見直しを実施するものとする。

注釈

※<sup>1</sup> 機密性：情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。

※<sup>2</sup> 完全性：情報及び処理方法の正確さ並びに完全である状態を安全防護すること。

※<sup>3</sup> 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。

※<sup>4</sup> 関連法令：主な情報セキュリティ関連法

- 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律
- 行政機関の保有する情報の公開に関する法律
- 個人情報の保護に関する法律
- 民法
- プロバイダー責任制限法
- 刑法
- 不正アクセス行為の禁止等に関する法律
- 犯罪捜査のための通信傍受に関する法律
- 著作権法
- 不正競争防止法