

奈良県立医科大学サイバーセキュリティ基本方針

1 目的

本基本方針は、公立大学法人奈良県立医科大学（以下「本学」という。）が保有し、又は管理するデータ資産について、その機密性、完全性及び可用性を維持し、教育・研究・診療及び法人運営を安定的に継続するため、サイバーセキュリティを確保するための基本的な考え方及び方針を定めることを目的とする。

2 定義

(1) 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網、その構成機器（ハードウェア及びソフトウェア）をいう。

(2) 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。

(3) データ資産

本学が所管する電子情報、紙情報及びフィルム情報の総称をいう。

(4) 情報セキュリティ

データ資産の機密性、完全性及び可用性を維持することをいう。

(5) 情報セキュリティポリシー

本学が策定した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をいう。

(6) 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。

(7) 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。

(8) 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。

3 対象とする脅威

本学は、データ資産に対する脅威として、次に掲げる事項を想定し、情報セキュリティ対策を講じるものとする。

- (1) 不正アクセス、マルウェア感染、サービス不能攻撃等のサイバー攻撃
- (2) 内部不正、人的過失、設定ミス等による情報の漏えい、滅失又はき損
- (3) 災害、事故、機器故障その他の非意図的要因による業務の阻害

4 適用範囲

本基本方針は、次に掲げる範囲に適用する。

- (1) 本学のすべての組織
- (2) 本学のデータ資産を取り扱う役員、教職員、学生、研修生及び委託事業者等
- (3) 本学が管理又は利用するすべての情報システム及びネットワーク

5 遵守義務

本学のデータ資産及び情報システムを利用する者は、情報セキュリティの重要性を十分に認識し、本基本方針、情報セキュリティポリシー及び情報セキュリティに関する実施手順書等を遵守しなければならない。

6 情報セキュリティ対策の基本

本学は、3に定める脅威からデータ資産を保護するため、次に掲げる観点から情報セキュリティ対策を講じるものとする。

- (1) 組織的対策
- (2) 人的対策
- (3) 物理的対策
- (4) 技術的対策
- (5) 運用面における対策
- (6) 情報セキュリティ侵害発生時の迅速かつ適切な対応

7 評価及び見直し

本学は、本基本方針及び情報セキュリティポリシーの遵守状況について、定期的又は必要に応じて監査及び自己点検を行い、その結果を踏まえ、情報セキュリティ水準の向上を図るものとする。

8 対策基準及び実施手順書

本学は、本基本方針に基づき、具体的な遵守事項、判断基準及び運用方法を定めるため、情報セキュリティポリシー及び実施手順書等を別途定めるものとする。

なお、当該情報セキュリティポリシー及び実施手順書等は、学内運用上必要な詳細を含むため、公表しないものとする。

9 基本方針の見直し

本学は、情報セキュリティを取り巻く環境の変化、法令の改正その他必要が生じた場合には、本基本方針の内容について見直しを行うものとする。

附 則

この基本方針は、令和8年4月1日から施行する。