京都府公立大学法人情報セキュリティ基本方針

令和８年４月１日

１　目的

本基本方針は、京都府公立大学法人（以下「法人」という。）が保有する機密性、完全性及び可用性を維持するための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。

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）情報資産

法人が利用する情報システム及び情報システムで取り扱うすべてのデータをいう。

（４）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。

（５）情報セキュリティポリシー

本基本方針並びに京都府立医科大学（以下「医科大学」という。）及び京都府立大学（以下「府立大学」という。）が策定した情報セキュリティ対策に係る基準等をいう。

（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

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

（１）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や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

（２）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、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要因による情報資産の漏えい・破壊・消去等

４　適用範囲

（１）組織の範囲

本基本方針が適用されるのは、法人本部、医科大学及び府立大学とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

５　教職員、学生及び委託事業者等の遵守義務

法人が設置するネットワーク及び情報システムを利用する教職員、学生及び情報システムの操作を伴う業務の委託事業者（派遣労働者及び機器のリースを行う者を含む。以下「委託事業者等」という。）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、業務の遂行に当たって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を遵守しなければならない。

６　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）組織体制

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。

（２）物理的セキュリティ

サーバ、情報システム室、通信回線、教職員のパソコン等の管理について、物理的な対策を講じる。

（３）人的セキュリティ

情報セキュリティに関し、教職員、学生及び委託事業者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。

（４）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。

（５）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、業務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ものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（６）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は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。

８　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になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記６、７及び８に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等を医科大学及び府立大学において策定する。

10　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に係る基準等に基づき、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医科大学及び府立大学において策定するものとする。

なお、具体的な内容は、公にすることにより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。