公立大学法人奈良県立大学情報セキュリティポリシー

１　目的

このセキュリティポリシー（以下「本ポリシー」という。）は、高度情報通信ネットワーク社会の到来に伴い増大する情報への脅威に的確に対応するとともに、個人情報等の情報資産の機密性、完全性及び可用性を維持するため、必要な事項を定めることを目的とする。

２　定義

（１）情報ネットワーク

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、電磁的記録媒体等で構成され、情報処理を行う仕組みをいう。

（３）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。

（４）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。

（５）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。

（６）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）情報システムの障害（利用不能、データ喪失　等）

情報システムの障害により、情報が利用できない、情報の一部を喪失したなどの事故。主に誰が、どの様に復旧作業を行うかが焦点となる。

（２）情報システムへの攻撃（ウイルス感染、不正アクセス、改ざん　等）

情報システムがウイルス感染や不正アクセス、改ざんなどの攻撃を受けた事故。意図的な犯行に対して法的措置を検討するかどうかや、どの様に復旧するかが焦点となる。

（３）情報漏えい（可能性も含む。）

紛失や盗難、または原因が不明な情報漏えい事故をいう。情報漏えいを起こした人物が分かっているかどうかにより対応が分かれ、意図的な犯行に対しては、法的措置の検討や情報漏えいの被害者に対する対外対応などが焦点となる。

４　適用する情報資産の範囲

（１）ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

（２）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。）

（３）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　対象者

法人の役職員（法人と雇用契約にある者を含む。）、研究活動を行う学術研究員等、学生、附属高等学校生徒及び法人の情報資産を利用するすべての者とする。

６　組織体制

情報セキュティに関する管理体制を整備するため、情報セキュリティに関する権限と責任を有する最高情報セキュリティ責任者を置く。また、最高情報セキュリティ責任者を補佐し、情報管理の実施及び緊急等の対応等にあたるため、情報セキュリティ管理者を置く。

（１）最高情報セキュリティ責任者は、副理事長をもって充て、法人の情報セキュリティ対策を実施する。

（２）情報セキュリティ管理者は、法人及び大学においては事務局長、附属高等学校においては校長をもって充て、以下の事務を所掌する。

（ア）情報セキュリティ事故対策マニュアルを作成し、又は改正すること。

（イ）情報セキュリティ対策が適正かつ円滑に行われるよう、役職員、学生及び生徒に対し、情報セキュリティポリシー及び情報セキュリティ事故対策マニュアルの研修及び周知を図ること。

（３）情報セキュリティ担当者は、法人及び大学においては総務課員、附属高等学校においては教頭をもって充て、情報セキュリティ管理者の指示を受け、その業務を補助する。

７　守られるべき財産と権利

情報ネットワークや情報システムなどの資源は、適正な利用によって保護されなければならない。

情報ネットワークや情報システムのデータを保護するため、情報セキュリティの保

護、適切な情報セキュリティ機器の導入、システムの監視など適切な対応をおこなわなければならない。
　ただし、私的利用によって生じたいかなる損失や障害についての責任は負わない。

８　情報セキュリティ侵害・加害行為の防止
　法人は、不正アクセスを高い確率で常時感知出来る監視システムを導入するとともに、外部または内部からの不正アクセスを検出した場合には速やかに対応し、適切な対策を施さなければならない。
　本ポリシーの対象となる者は、法人内外を問わず、あらゆる研究・教育機関、組織団体、個人等の情報資産を侵害してはならない。また、本ポリシーの他、情報セキュリティに関する法令、知的財産権に関連する法令、個人情報の保護に関する法令及び法人が定める規程等を遵守しなければならない。

９　違反行為への対応
　本ポリシーに違反した役職員が、故意または重大な過失により法人に損害を与えた場合には、公立大学法人奈良県立大学職員就業規則等により処分を行う場合がある。
　同様に本ポリシーに違反した学生及び生徒に対しては、学則等により処分を行う場合がある。

10　事故への対応
　情報セキュリティにかかる重大な事故等に対しては、最高情報セキュリティ責任者及び情報セキュリティ管理者は、公立大学法人奈良県立大学情報セキュリティ事故対策マニュアルに基づき迅速な対策の実施及び再発防止のための対策を講じなければならない。

11　情報の管理
　情報の漏えいを防止するため、情報機器及び記録媒体を持ち込み、持ち出し、交換、破棄する場合は、適切な処置をしなければならない。また、マルウェアを検出した場合にも、適切な処置をしなければならない。

12　情報資産の利用
情報資産を利用する者は、下記以外の目的に当該情報資産を利用しないこと。
（１）　業務
（２）　学術研究
（３）　授業又は自習
（４）　就職活動

（５） その他事務局長または校長が特に必要と認めたもの

13　情報資産の廃棄

情報資産を廃棄する場合は、記録媒体の破壊、磁気処理による消去等、情報を復元できないように処置した上で廃棄すること。

14　ソーシャルメディアサービスの利用について

ソーシャルメディアサービスの利用については、公立大学法人奈良県立大学ソーシャルメディア利用に関するガイドライン及び公立大学法人奈良県立大学公式アカウント等取り扱い要領に基づき適切に対応すること。

15　本ポリシーの見直し

本ポリシーは、情報セキュリティに関する状況の変化等を踏まえ、必要があると認めた場合、改訂を行うものとする。

附則

このポリシーは令和５年４月１日より施行する。