公立大学法人新潟県立看護大学情報セキュリティポリシー

（平成31年1月 22 日制定）
（令和8年3月11日全部改正）

第 1 章　情報セキュリティ基本方針

1　目的

公立大学法人新潟県立看護大学（以下「法人」という。）が保有・管理する情報資産を利用し、情報を適切かつ有効に取り扱うことにより、教育及び研究の充実に資するためには、安全かつ信頼される情報セキュリティを確保することが不可欠である。

法人の情報の保護及び活用並びに適切な情報セキュリティ対策を図ることを目的として、情報セキュリティポリシー（以下「ポリシー」という。）を定める。

2　定義

ポリシーにおいて、次の各号に掲げる用語の定義は、それぞれ当該各号のとおりとする。

(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及びその構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

ハードウェア及びソフトウェアから成るシステム及びクラウドサービス並びに有線又は無線のネットワークであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、法人が調達又は開発するもの（管理を外部委託しているシステムを含む。）若しくは法人の情報ネットワークに接続されるものをいう。

(3) 情報資産

法人が業務を遂行するうえで入手及び作成した情報並びにその情報を管理するシステム全般をいう。

(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) ポリシー

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。

(9) 職員

法人の役員及び常勤又は非常勤の教職員をいう。

(10) クライアント機器

学内で使用される情報機器等（個人が所有するものを含む。）あって、学内ネットワークに接

続可能な装置をいう。

(11) ログ情報

法人が管理する情報システム及びネットワーク機器等において自動的又は手動で生成・収集される記録であって、認証ログ、アクセスログ、操作ログ、セキュリティ機器ログその他これに準ずるものをいう。

(12) 第三者機関

警察・検察等の捜査機関、裁判所、監督官庁その他の行政機関等、及び法令に基づき法人に対して情報提出を求め得る機関をいう。

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

(3) 地震、落雷、火災等の災害による業務の停止や情報資産の漏えい・破壊・消去等

(4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラ障害からのシステム運用の機能不全等

4 適用範囲

(1) 情報資産の範囲

ポリシーの適用対象とする情報は、次のとおりとする。

ア 職員が職務上使用することを目的として法人または職員が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報(当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)

イ その他の情報システム又は外部電磁的記録媒体に記録された情報(当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)であって、職員が職務上取り扱う情報

ウ ア及びイのほか、法人または職員が調達し、又は開発した情報システムの設計又は運用管理に関する情報

(2) 情報システムの範囲

ポリシーの適用対象となる情報を取り扱うすべての情報システムとする。

(3) 適用対象者

職員、学生、研究員、委託業者など法人の情報資産を利用するすべての者とする。

5 利用者の遵守義務

すべての利用者は情報セキュリティの重要性を認識し、ポリシーを遵守し、各種規程等に従って適切に情報資産を利用しなければならない。

6　情報セキュリティ対策

上記3に掲げる脅威から情報資産を保護するため、次に掲げる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ための組織体制を確立する。

(2)　情報資産の分類と管理

法人の保有する情報資産を機密性、完全性、可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3)　物理的セキュリティ

情報システムの設置場所について安全性を保ち、不正な立ち入りを阻止する対策を講じる。また、持ち運びを前提とした情報資産を保護するための対策にも配慮する。

(4)　人的セキュリティ

情報セキュリティに関し、利用者が遵守すべき事項を定めるとともに、教育・啓発を行う等の人的対策を講じる。

(5)　技術的セキュリティ

コンピュータ及びネットワークの管理、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、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、運用面の対策を講じる。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。

(7)　業務委託と外部サービス(クラウドサービス等)の利用

ア　業務委託を行う場合には、委託業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託業者において必要なセキュリティ対策基準が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

イ　外部サービス(クラウドサービス等)を利用する場合には、利用に係る規程を整備し、対策を講じる。

(8)　ソーシャルメディアサービスの利用

別途、運用手順(ガイドライン等)を定めるものとする。

7　情報セキュリティ監査及び自己点検の実施

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　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、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、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、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」を策定する。なお、「情報セキュリティ対策基準」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。

10　情報セキュリティ実施手順の策定

上記 9 により策定された「情報セキュリティ対策基準」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定めた情報セキュリティ実施手順（ガイドライン・要領等を含む。）（以下「実施手順」という。）を策定するものとする。なお、実施手順は、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。