公立大学法人福島県立医科大学情報セキュリティ基本方針

（平成19年7月25日理事長制定）

1　趣旨及び目的

公立大学法人福島県立医科大学（以下「本学」という。）において、本学の理念に則り、教育、研究及び医療を推進していくうえで、情報システムやネットワークを整備し、これらを活用していくことは必要不可欠の要件である。

しかし、コンピュータウイルスや不正アクセスに代表される外部からの不正行為に加え、近年では、内部からの情報漏洩などが問題になっており、様々な情報セキュリティ上の対策を行う必要が生じている。

このため、本学は情報セキュリティ基本方針（以下「基本方針」という。）を定め、本学のすべての構成員の理解と協力により次の目標の達成に取り組む。

（1）　本学の情報資産[注1]に対する機密性[注2]、完全性[注3]及び可用性[注4]を損なう内外の脅威[注5]からの保護

（2）　学内外の情報セキュリティを損なう加害行為の防止と本学の社会的信用の保全

（3）　情報資産の重要度による分類とそれに見合った管理

（4）　情報セキュリティに関する教育及び情報取得の支援

（5）　情報セキュリティの定期的な評価と評価に基づく更新

2　定義

（1）　情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（2）　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(ハードウエア及びソフトウエア)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）　情報セキュリティポリシー

基本方針及び情報セキュリティ対策基準をいう。

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）　部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去等

（2）　情報資産の無断持ち出し、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、操作ミス、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サービス及び業務の停止等

4　適用範囲

（1） 対象組織

基本方針が対象とする組織は本学の全組織とする。

（2） 対象とする情報資産の範囲

基本方針が対象とする情報資産は、本学が管理するすべての情報資産及び本学が管理するネットワークに接続する本学管理以外のすべての情報システムとする。

(3) 対象者

本学の構成員のほか、対象とする情報資産に係わるすべての者とする。

5　遵守義務

対象者は、情報セキュリティの重要性について共通の認識を持ち、情報資産の利用にあたって、情報セキュリティポリシー、情報セキュリティ実施手順及び関連する法令等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。

ただし、これらの情報セキュリティ対策が、教育、研究及び医療上の活動を過剰に制限することのないようにしなければならない。

（1） 組織体制

本学の情報資産について、情報セキュリティ対策を推進する全学的な組織体制を確立する。

（2） 情報資産の分類と管理

本学の保有する情報資産を機密性、完全性及び可用性の観点から重要度に応じて分類し、リスク分析・評価[注6]を行ったうえで、その評価に基づく情報セキュリティ対策を行う。

（3） 物理的セキュリティ対策

情報資産に対する侵入、破壊、故障、停電及び災害等への物理的な対策を講じる。

（4） 人的セキュリティ対策

情報セキュリティに関し、対象者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。

（5） 技術的セキュリティ対策

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、コンピュータウイル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、情報セキュリティポリシーの遵守状況の確認、外部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、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

7　評価及び見直しの実施

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し、その結果に基づき情報セキュリティポリシーが定める事項について評価を行い、必要と認めるときは情報セキュリティポリシーの見直しを実施するものとする。

8　情報セキュリティ対策基準の策定

上記6及び7に規定する対策等を実施するために、本学内に共通かつ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別途策定するものとする。

9　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を別途策定するものとする。

１０　個人情報保護

対象者は、個人情報の保護に関する関係法令及び個人情報の取り扱いに関する各種ガイドライン等を遵守しなければならない。

１１　情報セキュリティに関する違反への対応

基本方針及び情報セキュリティ対策基準に違反した者については、その重大性、発生した事故等の状況等に応じて、本学の構成員にあっては懲戒処分等の対象とするほか、本学の構成員以外は法律的な措置を講ずるものとする。

（附．則）

この基本方針は、平成19年7月25日から施行する。

注１　情報資産

情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称

注２　機密性

アクセスを認可された者だけが情報にアクセスできることを確実にすること。

注３　完全性

情報及び処理方法が、正確であること及び完全であることを保護すること。

注４　可用性

認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

注５　脅威

情報資産に影響を与え、損失を発生させる直接の要因。不正アクセスによる情報の改ざんや破壊、ウイルスによる感染事故、自然災害による情報基盤の停止や過失による情報の漏えいや破壊などがある。

注６　リスク分析・評価

行うべきセキュリティ対策を決定するために、その情報資産に対する脅威と脆弱性[注7]からセキュリティリスクの発現可能性の分析を行い、影響度等の評価を行うこと。

注７　ぜい（脆）弱性

情報資産が脅威にさらされる要因で、情報資産の置かれている環境や運用状況の不備・欠陥のこと。脆弱性それ自体は脅威ではないが、その脆弱性があることで脅威が発現することになる。