公立大学法人敦賀市立看護大学情報セキュリティ基本方針

平成３０年９月２６日
（理　事　長）

１　目的

公立大学法人敦賀市立看護大学（以下「本学」という。）の情報資産には、個人情報、実習や研究等における対象者の情報、論文等の知的財産など、漏洩、破壊、改ざん、詐取等が発生した場合には重大な結果を招く情報が多数含まれている。

公立大学法人敦賀市立看護大学情報セキュリティ基本方針(以下「基本方針」という。)は、情報資産を不正アクセスや災害、事故等の様々な脅威から防御するとともに、人為的過誤による情報漏洩等の防止策を含め、情報資産の適切な管理・運用を図るために本学が実施する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　適用者

基本方針は、情報資産を取り扱う役員、職員（非常勤職員を含む)、外部委託事業者、学生その他本学の許可を受け情報資産を取り扱う者（以下、総称して「利用者」という。）に適用する。

３　用語の定義

基本方針における次の各号の用語の意義については、当該各号に定めるところによる。

（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、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。

（５）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。

（６）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。

（7）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。

4　利用者の責務

利用者は、情報セキュリティの重要性を常に意識して行動するとともに、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（以下「ポリシー等」という。）を遵守しなければならない。

5　違反への対応

ポリシー等に違反する行為及び違反者には、厳正に対応する。

6　情報資産の範囲

基本方針が対象とする情報資産は、次の各号に定めるところによる。

（1）本学のネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体（契約あるいは他の協定に従って提供されるものを含む。以下同じ。）

（2）本学の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）本学の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

7　対象とする脅威

情報資産に対する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）悪意のある攻撃

不正アクセス、マルウェア、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洩、破壊、改ざん、消去、詐取、内部不正等

（2）情報システムの欠陥、管理・設定の不備、故障等

設計・開発の不備、プログラム上の欠陥、メンテナンス不備、外部委託管理の不備、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洩、破壊、消去等

（3）災害等

地震、落雷、火災、水害その他事故等によるサービス及び業務の停止等

（4）人為的過誤等

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、コンピュータ及び情報システム等の誤操作及び設定ミス、メールの誤送信、パスワードの脆弱性、紛失等による情報の消去、漏洩等

８ 情報セキュリティ対策

情報資産を脅威から防御するために、次の情報セキュリティ対策を実施する。

（１）組織体制の確立

情報セキュリティ対策を実施・推進する組織体制を確立する。

（２）情報資産の分類と管理

情報資産を機密性、完全性及び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

情報資産を悪意のある攻撃、災害等から防御するための物理的対策を実施する。

（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、利用者に対する教育、啓発、情報提供等の人的対策を実施する。

（５）技術的セキュリティ

コンピュータ等の動作管理、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実施する。

（６）運用

ポリシー等の遵守状況の確認、外部委託を行う際のセキュリティ確保等、運用面の対策を実施する。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切に対応するため、緊急時の対応について定める。

９　情報セキュリティの評価及び情報セキュリティポリシーの見直し

情報セキュリティに関する状況の変化に対応するため、必要に応じて、情報セキュリティの評価及び情報セキュリティポリシーの見直しを実施する。

１０　情報セキュリティ対策基準の策定

基本方針に基づく情報セキュリティ対策を実施するために、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を策定する。

１１　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策定する。

なお、情報セキュリティ実施手順は、非公開とする。