公立大学法人神戸市看護大学情報セキュリティ基本方針

2019年４月１日

１　目的

公立大学法人神戸市看護大学（以下「法人」という。）の情報システムが取り扱う情報には，役員，職員，派遣労働者及び学生の個人情報や法人及び大学の運営上重要な情報が多数含まれている。これらの情報資産を人的脅威や災害，事故等様々な脅威から防御することは，プライバシー保護，質の高い教育研究活動及び適切な大学運営を確保するために必要不可欠である。

このため，法人が保有する情報資産の機密性，完全性及び可用性を維持することを目的として公立大学法人神戸市看護大学情報セキュリティ基本方針(以下「情報セキュリティ基本方針」という。）を定める。

２　用語の定義

⑴　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。

⑵　情報システム

コンピュータ及びネットワークで構成され，情報処理を行う仕組みをいう。

⑶　データ

電子計算機処理に係る入出力帳票，磁気テープ，磁気ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

⑷　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いう。

⑸　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。

⑹　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。

⑺　可用性

情報にアクセスすることを認められた者だけが，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。

⑻　構成員

役員，職員，派遣労働者及び学生など法人において情報資産を取り扱う全ての者をいう。

３ 情報セキュリティ基本方針の位置付け

情報セキュリティ基本方針は，法人が保有する情報資産に関して総合的かつ体系的にまとめた情報セキュリティ対策の基本となるものであり，本方針の下に「公立大学法人神戸市看護大学情報セキュリティ対策基準」（以下「情報セキュリティ対策基準」という。）を定める。

情報セキュリティ基本方針は，情報セキュリティ対策基準とともに情報セキュリティポリシーを構成する。

4　情報セキュリティ基本方針の適用範囲

情報セキュリティ基本方針の適用範囲は，法人における情報資産及び情報資産に接する構成員，法人の委託業者，来学者等法人の情報資産を利用する全ての者とする。

また，情報資産の範囲は次のとおりとする。

⑴　物理資産

コンピュータ，ネットワーク，記録媒体等物理的な形状を有する資産であり，かつ，情報を利用するのに必要な資産

⑵　データ資産

データ及び情報システムの設計等に関する情報

⑶　ソフトウェア資産

コンピュータ等の情報機器において稼動するプログラム

⑷　サービス資産

電源，メールサービス等契約により提供される情報システムに関連する業務

5　構成員の義務

構成員は，情報セキュリティの重要性について共通の認識を持つとともに，情報資産の利用に当たっては情報セキュリティ基本方針を遵守するものとする。

6　情報セキュリティ管理体制

法人の情報資産について，適切に情報セキュリティ対策を推進し，管理するための体制を確立するものとする。

必要な体制，役割，権限等については，情報セキュリティ対策基準にて定める。

7　情報資産への脅威

情報セキュリティ対策を講じる上では，情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に次の脅威については，十分な措置を講じるものとする。

⑴　部外者による不正アクセス又は不正操作によるデータやプログラムの持ち出し，盗聴，改ざん及び消去，機器及び媒体の盗難等

⑵　構成員及び部外委託者による以下に記す行為

ア　意図しない操作，不正アクセス又は不正操作によるデータやプログラムの持ち出し，盗聴，改ざん又は消去

イ　機器及び媒体の盗難

ウ　規定外の端末接続によるデータ漏えい

エ　その他上記に類する行為

⑶　地震，落雷，火災等の災害，事故，故障等によるサービス及び業務の停止

8　情報セキュリティ対策

情報資産に対する脅威から情報資産を保護するため，以下の情報セキュリティ対策を講じるものとする。

⑴　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こととする。

⑵　物理的セキュリティ

コンピュータの設置場所への入退室，サーバ等の管理，通信回線及び端末等への物理的な対策を講じる。

⑶　人的セキュリティ

情報セキュリティに関し，全ての構成員が遵守すべき事項を定めるとともに，十分な研修，訓練及び啓発を実施するなど人的な対策を講じる。

⑷　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，コンピュータウィルス等不正アクセス対策等の技術的対策を講じる。

⑸　運用面のセキュリティ

情報システムに関し，情報セキュリティ基本方針の遵守状況の確認等，情報セキュリティ基本方針の運用面の対策を講じる。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。

9　情報セキュリティ個別基準の策定

情報セキュリティ基本方針を補完するために必要な内容に関して，具体的な内容を定める情報セキュリティ個別基準を策定するものとする。

10　情報セキュリティ実施手順の周知

情報セキュリティ基本方針及び情報セキュリティ個別基準に基づき，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周知するものとする。

11　情報セキュリティ自己点検及び監査の実施

情報セキュリティ対策の実施状況を評価するため，定期的及び必要に応じて情報セキュリティ自己点検及び監査を実施する。

12　情報セキュリティ基本方針の見直し

情報セキュリティ自己点検及び監査の結果，情報セキュリティに関する状況の変化等を踏まえ，必要に応じ適宜情報セキュリティ基本方針の見直しを行う。

附　則

この情報セキュリティ基本方針は，2019年４月１日から施行する。