【NBIS-R-01】

新潟県病院局情報セキュリティポリシー
【基本方針】

令和８年３月　日制定

目　次

【基本方針】

新潟県病院局情報セキュリティ基本方針

第１　目的

新潟県病院局（以下「病院局」という。）は、病院事業の運営に必要な多数の情報を保有しており、これらの情報や情報を取り扱うネットワーク及び情報システム等を、災害、事故、故意及び過失等の様々な脅威から防御することは、病院事業の安定的・継続的な運営のために必要不可欠である。

本基本方針は、病院局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ため、病院局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。

第２　定義

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　情報資産

(1)　ネットワーク、情報システム及びこれらに関する設備、モバイル端末、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。

(3)　ネットワーク構成図及び情報システムの仕様書等のシステム関連文書。

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　情報セキュリティ対策

情報セキュリティを確保するための対策をいう。

６　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

７　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。

８　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。

９　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。

10　情報セキュリティインシデント

情報セキュリティに関する障害・事故及び欠陥のことをいう。

第３　対象とする脅威

情報資産に対する脅威として以下のものを想定し、情報セキュリティ対策を実施する。

１　意図的要因

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な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　非意図的要因

情報資産の無断持ち出し、無許可ソフトウェアの使用や端末接続等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、認証情報又はパスワードの不適切管理、搬送中の事故等による情報資産の盗難・紛失、機器の故障等による情報資産の漏えい・破壊・消去等。

３　災害等による要因

地震、落雷、火災等の災害や電力供給、通信の途絶等のインフラの障害によるサービス及び業務の停止等。

第４　適用範囲

１　適用機関

新潟県病院局組織規程（昭和 36 年新潟県病院局管理規程第 3 号）に定める局本庁及び施設とする。

２　適用情報資産

適用機関が所管する情報資産とする。ただし、新潟県知事が管理運営する情報資産は本ポリシーの適用範囲外とする。

３　適用対象者

適用情報資産に接する全ての職員（常勤又は非常勤の別を問わない全ての職員。以下「職員」という。）とする。

第５　情報セキュリティ対策

病院局が所管する情報資産を上記第３に規定する脅威から保護するために、以下の情報セキュリティ対策を講ずる。

１　組織体制

病院局の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

２　情報資産の分類と管理

病院局が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行う。

３　物理的セキュリティ

サーバ、情報システム室、通信回線及びパソコン等の管理について、物理的な対策を講じる。

４　人的セキュリティ

情報セキュリティに関し、職員等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

パソコン等の管理、アクセス制御、不正プログラム対策及び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、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。

第６　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、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。

第７　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティ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、情報セキュリティポリシーを見直す。

第８　情報セキュリティ対策基準の策定

上記第５から第７までに規定する対策等を実施するために、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。

なお、情報セキュリティ対策基準は、公にすることにより病院局の病院事業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。

第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策定するものとする。この情報セキュリティ実施手順は、業務ごと又は情報システムごとに策定することを基本とする。

なお、情報セキュリティ実施手順は、公にすることにより病院局の病院事業運営に重大な

支障を及ぼすおそれがあることから非公開とする。

第 10　職員等の遵守義務

職員は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって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を遵守しなければならない。また、契約等により病院局の情報資産の利用を認められた外部の事業者及び派遣等により病院局の業務に従事する者についても、業務内容に応じた情報セキュリティを確保させなければならない。

第 11　法令等の遵守

職員等は、職務の遂行において、情報セキュリティ関連法令等を遵守しなければならない。