

地方独立行政法人新小山市民病院

情報セキュリティポリシー

【第1章抜粋版】

制定日：令和5年4月1日

第1章 情報セキュリティ基本方針

1 基本的な考え方

情報セキュリティ基本方針は、地方独立行政法人新小山市市民病院（以下「病院」という。）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 定義

この情報セキュリティポリシーにおいて、次に掲げる用語の意義は、当該各号に定めるところによる。

（1）情報資産

本基本方針が対象とする情報資産は、次のとおりとする。

- ① 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
- ② 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 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

（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（ハードウェア及びソフトウェア）をいう。

（3）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のことで、病院の所有であるかを問わず、病院の所掌する事務に使用するものすべてをいう。

（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）情報セキュリティポリシー

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（confidentiality）

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（integrity）

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（availability）

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。

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) 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、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) 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の障害からの波及等

4 職員等の遵守義務

職員、契約職員、及び委託職員（以下「職員等」という。）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。

5 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。

(1) 組織体制

病院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。

(3) 人的セキュリティ対策

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。

(4) 物理的セキュリティ対策

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

(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) 外部サービスの利用

外部委託や約款による外部サービス、ソーシャルメディアサービスを利用する場合は、外部事業者等において必要なセキュリティ対策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。

(8) 評価・見直し

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、運用改善を行い情報セキュリティの向上を図る。

情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

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、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。

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。

8 情報セキュリティ対策基準の策定

上記5、6及び7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（本書第2章のとおり）。

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本書とは別に策定するものとする。

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。