北村山公立病院組合情報セキュリティ基本方針

令和８年３月策定

1　目的

本基本方針は、北村山公立病院組合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、本組合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

本基本方針において、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。

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、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。

⑶　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。

⑷　機密性

情報にアクセスすることが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。

⑸　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。

⑹　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。

⑺　診療ネットワーク系

電子カルテや部門システム等に接続された情報システム及びその情報システムで取り扱うデータをいう。

⑻　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

⑼　通信経路の分割

診療ネットワーク系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

⑽　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウィルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

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。

⑴　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

⑵　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

⑶　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

⑷　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

⑸　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　適用範囲

⑴　適用機関の範囲

本基本方針が適用される機関は、北村山公立病院組合、北村山公立病院、監査委員（以下「病院組合等」という。）とする。なお、組合議会については、東根市議会の基本方針を準用する。

⑵　情報資産の範囲

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　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

5　職員等の遵守義務

職員（会計年度任用職員等を含む。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方針及び情報システムに関する規程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。

⑴　組織体制

病院組合等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。

⑵　情報資産の分類及び管理

病院組合等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実施する。

⑶　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

①　診療ネットワーク系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、情報の流出を防ぐ。

②　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

⑷　物理的セキュリティ

サーバ室への不正な立入り、情報資産への損傷・妨害等を防ぐため、物理的な対策を講じる。

⑸　人的セキュリティ

情報セキュリティに関する権限や職員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が講じられるように必要な対策を講じる。

⑹　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、不正プログラム対策、不正アクセス対策等の技術面の対策を講じる。

⑺　運用

情報システムの監視、情報セキュリティ方針の遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティ方針の運用面の対策を講じるものとする。

また、緊急事態が発生した場合に迅速な対応を可能とするための対策を講じる。

⑻　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者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。

外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じる。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティ方針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。

8　情報セキュリティ方針の見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティ方針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、情報セキュリティ方針を見直す。

９　情報セキュリティ対策基準の策定

上記６、７及び８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組合等の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。

10　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。

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組合等の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。

附　則

この基本方針は、令和８年４月１日から施行する。