地方独立行政法人北松中央病院情報セキュリティ基本方針

１．目的

この基本方針は、地方独立行政法人北松中央病院（以下「当院」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、当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

（１）情報　職員等が業務を遂行するために入手又は作成した「情報システムや記録媒体等に記録された情報」、「音声（会話、録音データ等）」、「映像・画像」、「画面に表示されたもの」、「情報システムから出力された情報（紙）」、「紙に印刷あるいは記載されたもの」の他、「業務上知り得た内容（記憶を含む）」等をいう。

（２）情報システム　情報システム機器やネットワークを利用し、情報処理や情報伝達を行う仕組みをいう。なお、情報システム機器とは、サーバ装置、パソコンやタブレット等の端末、通信回線装置、複合機、特定用途機器、ソフトウェア、記録媒体等が該当する。

（３）情報資産　情報及び情報システムをいう。

（４）機密性　許可された者だけが情報資産を利用できることをいう。

（５）完全性　情報資産を最新かつ正しい状態で維持することをいう。

（６）可用性　許可された者が必要なときに確実に情報資産を利用できることをいう。

（７）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。

（８）情報セキュリティ対策　情報セキュリティの実現を目的として実施する対策をいう。

（９）役員　理事長、副理事長、理事及び監事をいう。

（１０）職員等　当院の役員並びに当院に常時勤務する職員及び非常勤職員をいう。

（１１）業務委託　当院の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、当該業務において当院の情報を取り扱わせる場合に限る。

３．対象とする脅威

情報資産に対する脅威として、次に掲げる脅威を想定した、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、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、水道供給途絶等のインフラ障害からの波及等

４．適用範囲

この方針の適用範囲は、当院の情報資産に関わるすべての職員等とする。

５．職員等の遵守義務

職員等は、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。

６．情報セキュリティ対策

前３の脅威から情報資産を保護するために、次に掲げる各号の情報セキュリティ対策を講じる。

（１）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）当院の保有する情報資産を、機密性、完全性及び可用性に基づいた重要度に応じて分類し、その分類に応じた取扱いを整備し管理する。

（３）サーバ、サーバ室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（４）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）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）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、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じる。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、緊急時対応計画を整備する。

（７）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する。また、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することで、契約に基づいた措置を講じる。

（８）外部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。また、ソーシャルメディアサービスを利用する場合には、運用手順を定め、発信できる情報を規定する。

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。

８．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。

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当院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当院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

この方針は、令和７年１１月１日から施行する。