諏訪中央病院組合_情報セキュリティ基本方針を次のように定める

令和８年４月１日

組合長　今井　敦

諏訪中央病院組合 情報セキュリティ基本方針

（目的）

第１条　この基本方針は、情報資産の機密性、完全性及び可用性を確保し、及び維持するため、当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。

（定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)　実施機関:組合立諏訪中央病院、リバーサイドクリニック、北山診療所、介護老人保健施設やすらぎの丘、介護老人福祉施設特別養護老人ホームふれあいの里、諏訪中央病院訪問看護ステーションいろは、諏訪中央病院看護専門学校をいう。

(2)　ネットワーク：コンピュータ等の端末機器（以下「端末」という。）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。

(3)　情報システム：端末、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。

(4)　情報資産：端末及びネットワーク（仕様書、図等のシステム関連情報を含む。）並びに情報システムで作成され、及び保存された情報（これらを印刷した文書を含む。）をいう。

(5)　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確保し、及び維持することをいう。

(6)　情報セキュリティポリシー：この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：情報資資産を利用することを認めた者だけが，当該情報資産を利用できる状態を確保することをいう。

(8)　完全性：情報資産が破壊、改ざん又は廃棄されていなく、処理の方法が正確かつ完全な状態を確保することをいう。

(9)　可用性：情報資産を利用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、当該情報資産を利用できる状態を確保することをいう。

(10)　電子カルテシステム接続系：完全に他のネットワークと分離された電子カルテに係る情報システムをいう。

(11)　閉域ネットワーク接続系：信州メディカルネット，メドコム、総合行政ネットワーク（「LGWAN ネットワーク」という。）等閉域網に接続された情報システムをいう（電子カルテシステム接続系を除く。）。
(12)　インターネット接続系（SCHPnet）：インターネットを経由するメール、ホームページ管理システムその他のインターネットに接続された情報システムをいう。
(13)　通信経路の分割：閉域ネットワーク接続系とインターネット接続系と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することをいう。
(14)　無害化通信：インターネットを経由するメール本文のテキスト化、端末への画面転送、ゼロトラスト導入、無線認証等を行うことにより、コンピュータウイルス等の不正プログラム等を排除し、安全を確保した通信をいう。

（対象とする脅威）
第３条　この基本方針が対象とする情報資産に対する脅威は、次に掲げるものとする。
(1)　不正アクセス、コンピュータウイルス攻撃、サービス不能攻撃等によるサイバー攻撃及び部外者の侵入、内部不正等の意図的な要因による情報資産の漏えい、破壊、改ざん、詐取、廃棄等
(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、設計又は開発の不備、プログラム上の欠陥、操作又は設定の誤り、メンテナンス不備、内部又は外部の監査機能の不備、委託管理の不備、管理体制の欠陥、機器故障等の非意図的な要因による情報資産の漏えい、破壊、改ざん、詐取、廃棄等
(3)　地震、落雷、火災等の災害による情報システムの停止等
(4)　大規模かつ広範囲にわたる疾病等による要員の不足に伴う情報システムの運用の機能不全等
(5)　電力、通信等の社会生活基盤の途絶に伴う情報システムの運用の機能不全等

（適用の範囲）
第４条　この基本方針を適用する情報資産の範囲は、実施機関が保有する情報資産とする。

（職員等の遵守義務）
第５条　常勤の職員、非常勤の職員、派遣職員及び委託請負業者職員（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。

２　職員等は、情報資産の利用及び管理に当たり、個人情報の保護に関する法律（平成 15 年法律第 57 号）等の関連する法令等を遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条に規定する脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

(1)　組織体制：情報資産について、情報セキュリティ対策を推進する全組合的な組織体制を確立する。

(2)　情報資産の分類と管理：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)　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、業務の効率性及び利便性の観点を踏まえ、次の対策を講じる。

①　電子カルテシステム接続系においては、原則として、インターネット接続系等の他の領域との通信を不可能とする設定を行った上で、端末からの情報の持ち出しを不可能とする設定、端末への多要素認証の導入その他対策を講じる。

②　閉域ネットワーク接続系においては、通信経路の分割を行う。この場合において、インターネット接続系との間の通信に当たっては、無害化通信の使用その他対策を講じる。

③　インターネット接続系においてはゼロトラストの導入等セキュリティ強化の対策を講じる。

(4)　物理的セキュリティ対策：サーバ、情報システム室、通信回線及び職員等の端末等の管理について、物理的な対策を講じる。

(5)　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。

(6)　技術的セキュリティ対策：情報資産の管理、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。

(7)　運用：情報システムの監視、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の遵守状況の検証、業務委託を行う際の情報セキュリティの確保等の運用における対策を講じる。この場合において、情報資産の脅威となる事案が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画をあらかじめ策定する。

(8)　業務委託、外部サービス（外部の事業者が運営するサーバを利用したクラウドサービス等をいう。）又はソーシャルメディアサービス(インターネットを利用し、個人又は法人が情報を発信し、相互に情報のやり取りを行うことができるサービスをいう。)の利用においては、次の措置を講じる。

①　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。

② 外部サービスを利用する場合には、利用に係る規定を整備し、必要な対策を講じる。

③ ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（情報セキュリティ監査及び自己点検の実施）

第７条　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の遵守状況を検証するため、定期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。

（情報セキュリティポリシーの見直し）

第８条　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及び情報セキュリティ実施手順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に新たな対策が必要になった場合においては、情報資産に係る脅威の発生の可能性及び発生時の損失等を分析し、その影響を検討した上で、直ちに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見直す。

（情報セキュリティ対策基準の策定）

第９条　第６条から前条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別に定める。

（情報セキュリティ実施手順の策定）

第 10 条　前条の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別に定める。

２　前項の情報セキュリティ実施手順は、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。