令和8年3月23日

病院事業管理規程第2号

近江八幡市立総合医療センター
情報セキュリティ基本方針

令和８年３月

近江八幡市立総合医療センター

目　　次

（目的）

第１条　この方針は、近江八幡市立総合医療センター（以下「医療センター」という。）の保有する情報システムで取り扱う個人情報並びに運営上の情報の破壊、改ざん及び外部への漏洩が生じた場合の重大性を鑑み、情報セキュリティに関する基本的な事項について定め、情報資産の適切な管理を図り、もって市民の財産及びプライバシー等を守るとともに、医療センターにおける情報資産に関する事務の安定的な運営を確保することを目的とする。

（定義）

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

（１）ネットワーク

医療センターの内部又は関係機関の間を接続するための通信網、その構成機器及び記録媒体で構成され、処理を行う仕組み（医療センターの業務のために用いるものに限る。）をいう。

（２）情報システム

医療センターの電子計算機及び記録媒体で構成され、業務処理を行う仕組み（医療センターの業務のために用いるものに限る。）をいう。

（３）情報セキュリティポリシー

この方針及び第７条に規定する情報セキュリティ対策基準をいう。

（４）情報セキュリティ

情報資産の機密の保持、正確性及び完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（５）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。

（６）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。

（７）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。

（８）職員等

医療センターに勤務する正規職員、会計年度任用職員その他非常勤職員、委託業者、研修生をいう。

（９）医療情報システム系

電子カルテ他、医療業務に係る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。

（１０）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係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。

（対象とする脅威）

第３条　事業管理者は、次に掲げる事項を情報資産に対する脅威として想定し、情報セキュリティ対策を実施する。

（１）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、重要情報の搾取、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・広範囲にわたる疫病による要因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、水道供給の途絶等の提供サービスの障害からの波及等

（適用範囲）

第４条　本基本方針が適用される範囲は、次に掲げる範囲とする。

（１）機関の範囲　近江八幡市立総合医療センター

（２）情報資産の範囲

①　医療センターに係るネットワーク、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　医療センターに係る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　医療センターに係る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

（職員等の遵守義務）

第５条　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、業務の遂行にあたって情報セキュリティポリシー及び第８条に規定する情報セキュリティ実施手順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　事業管理者は、第３条各号に定める脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を行う。

（１）組織体制

医療センター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

医療センターの所有する情報資産を機密性、完全性、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）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　医療情報システム系においては、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、医療情報の流出を防ぐ。

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。

（４）物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、通信回線及び職員等のパソコン等の端末の管理、情報資産への損傷、妨害等から保護するため、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係る権限及び責任、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

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。

（７）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。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。

（８）外部サービスの利用

外部委託する場合には、外部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、外部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。

約款による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。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。

（情報セキュリティ対策基準の策定）

第７条　第６条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等を策定する。

なお、情報セキュリティ対策基準は、公にすることにより医療センター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。

（情報セキュリティ実施手順の策定）

第８条　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。

なお、情報セキュリティ実施手順は、公にすることにより医療センター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。

（情報セキュリティ監査の実施）

第９条　情報セキュリティポリシーの遵守状況を検証するために、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。

（評価および見直しの実施）

第１０条　前条に定めた監査及び自己点検の結果により、運用の改善を行い、情報セキュリティポリシーに定める事項および情報セキュリティ対策の実効性を評価するとともに、情報セキュリティに関する状況の変化に対応するため、情報セキュリティポリシーの見直しを実施する。