○公立藤田総合病院情報セキュリティポリシー

第１章　情報セキュリティ基本方針

１　目的

本基本方針は、公立藤田総合病院（以下「当院」という。）が地域医療の中核を担う公立病院として、患者及び地域住民から寄せられる信頼に応えるため、当院が保有する情報資産を様々な脅威から保護し、情報セキュリティを確保することを目的とする。

また、当院の業務の継続性を確保するとともに、個人情報及び診療情報の適正な管理を行うことにより、安全で質の高い医療サービスの提供を維持することを目的とする。

２　定義

（１）情報資産

電子データ、紙媒体の文書、情報システム、ネットワーク、記録媒体、及びこれらを処理又は保存するための機器等、当院の業務において利用されるすべての情報及びそれを取り扱うための資源をいう。

（２）個人情報

個人情報の保護に関する法律及び当院の個人情報保護規程に基づき定義される、特定の個人を識別できる情報をいう。

（３）医療情報システム

診療情報を取り扱う情報システム（ハードウェア及びソフトウェアを含む。）並びにこれらの情報を電子的に記録する媒体等により構成される、医療業務を処理するための仕組みをいう。

（４）ネットワーク

情報システム及び情報機器が相互に通信するための通信網及び通信機器の総体をいう。

（５）病院情報システム系ネットワーク

電子カルテシステム、医事会計システム、部門システム等の患者情報を含む個人情報を取り扱う情報システム及びそのネットワークをいう。

（６）部門システムネットワーク

各部門において独自に構築された情報システム及びそれらを接続するネットワークをいう。

（7）情報系ネットワーク

インターネットに接続された情報システム及びそのネットワークをいう。

（8）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。

① 機密性

情報資産にアクセスすることを認められた者のみが情報資産にアクセスできる状態を確保すること。

② 完全性

情報資産が破壊、改ざん又は消失していない状態を確保すること。

③ 可用性

情報資産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資産にアクセスできる状態を確保すること。

3　対象とする脅威

当院の情報資産に対する主な脅威として、次の事項を想定する。

① 不正アクセス、マルウェア感染、サービス不能攻撃等のサイバー攻撃
② 外部者の侵入、内部不正等による情報漏えい、改ざん、破壊又は消失
③ 情報資産の無断持ち出し、無許可ソフトウェアの利用等の規程違反
④ 設定ミス、操作ミス、システム障害等による情報資産の損失
⑤ 地震、落雷、火災等の災害による業務停止
⑥ 大規模感染症の流行等による要員不足
⑦ 電力、通信等のインフラ障害によるシステム停止

4　適用範囲

本基本方針は、当院の職員（正規職員及び会計年度任用職員）、派遣職員、研修医、実習生、及び業務委託先の従業員等、当院の情報資産を取り扱うすべての者（以下「全職員等」という。）に適用する。

また、院内ネットワーク、医療情報システム、電子カルテシステム、医事会計システム、各部門システム、及びこれらで取り扱う電子データ並びに紙媒体の書類等、当院が管理するすべての情報資産を対象とする。

5　職員等の遵守義務

全職員等は、地方公務員法に定める守秘義務を遵守するとともに、本基本方針及び関連規程を理解し、情報資産を適切に取り扱わなければならない。

6　情報セキュリティ対策

上記４の脅威から情報資産を保護するため、以下の情報セキュリティ対策を講じる。

（１）組織体制

情報セキュリティ対策を推進するための体制を整備し、責任及び権限を明確にする。

（２）情報資産の分類と管理

情報資産を機密性、完全性及び可用性の観点から分類し、その重要度に応じた適切な管理を行う。

（３）情報システム全体の強靱性の向上

業務の効率性及び利便性を考慮しつつ、情報システム全体の安全性を確保するため、以下の対策を講じる。

① 病院情報システム系ネットワーク

原則として他のネットワーク領域との通信を制限するとともに、端末からの情報持ち出し制御等により患者情報の漏えい防止を図る。

② 部門システムネットワーク

病院情報システム系ネットワーク及び情報系ネットワークとの通信経路を適切に分離し、必要に応じてファイアウォールや中間サーバ等を設置する。

③ 情報系ネットワーク

不正通信の監視機能の強化等、必要な情報セキュリティ対策を実施する。

（４）人的セキュリティ

情報セキュリティに関する権限及び責任を明確にするとともに、職員等に対して教育及び啓発を実施する。

（５）物理的セキュリティ

情報システム機器の設置場所への不正な立入り、機器の盗難、破壊等を防止するための物理的対策を講じる。

（６）技術的セキュリティ

アクセス制御、認証、暗号化、ネットワーク管理等の技術的対策を講じ、不正アクセス及び情報漏えいを防止する。

（７）運用管理

情報システムの監視及び情報セキュリティ対策の遵守状況の確認を行うとともに、情報セキュリティインシデント発生時には迅速な対応を行う。

（８）業務委託及び外部サービスの利用

業務委託を行う場合は、委託事業者の選定にあたり情報セキュリティ対策の実施状況を確認し、必要な情報セキュリティ要件を契約に明記する。

また、クラウドサービス等の外部サービスを利用する場合には、関係規程を整備し、適切な安全管理措置を講じる。

7　情報セキュリティ監査及び自己点検

情報セキュリティポリシーの遵守状況を確認するため、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並びに社会情勢、技術動向等の変化を踏まえ、必要に応じて情報セキュリティポリシーの見直しを行う。

9　情報セキュリティ対策基準の策定

上記7、8及び9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。

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本組合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

この規程は、令和8年4月1日から施行する。