＜平塚市民病院情報セキュリティ基本方針＞

令和7年3月１日
（令和7年8月１日　改正）

1　目的

本院の取り扱う情報資産には、患者の個人情報のみならず行政運営上重要な情報など、外部への漏洩や破壊等が発生した場合には極めて重大な被害を招く情報が数多く含まれている。したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、患者の財産やプライバシーを守り、また、行政サービスの安全かつ安定した実施のためにも必要不可欠である。ひいては、このことが本院に対する市民・患者からの信頼の維持に寄与するものである。

よって、本院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、平塚市民病院情報セキュリティ基本方針（以下「基本方針」という）を定める。

本基本方針は、本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

この基本方針において、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）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（2）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。

（3）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。

（4）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。

（5）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、その構成機器（ハードウェア及びソフトウェア）をいう。

（6）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。

（7）情報資産

ネットワーク、情報システム及びこれらで取り扱う情報をいう。

（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。

（９）医療情報システム系

診療等に関わ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）LGWAN接続系

デジタル推進課が整備するLGWAN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（マイナンバー利用事務系を除く。）。

（１１）インターネット接続系

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。

（１２）通信経路の分割

医療情報システム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。

（１３）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、コンピュータウイ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。

（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、委託管理者の不備、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、水道供給等のインフラの障害からの波及等

４　適用範囲

（1）適用範囲

本基本方針は、平塚市民病院が保有するすべての情報システムを適用範囲とする。ただし、事務局職員が利用する LGWAN 系端末に保存された情報資産は、平塚市情報セキュリティ基本方針の適用対象となるため、本基本方針の対象外とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、本院が保有する情報資産とする。

5　職員等の遵守義務

一般職員、定年前再任用短時間職員、暫定再任用職員、任期付職員及びパートタイム会計年度任用職員、派遣職員、委託職員（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。

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。

（1）組織体制

本院の情報資産について、情報セキュリティ対策を推進する全院的な組織体制を確立する。

（2）情報資産の分類と管理

本院の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、次の三段階の対策を講じる。

ア　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、診療情報の流出を防ぐ。

イ　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。。

ウ　ＬＧＷＡＮ接続系においては、医療情報システム系、インターネット系と分離した独立したネットワークを構築し、他の領域との通信をできないようにする。

（4）物理的セキュリティ

サーバ、情報システム室、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。

（5）人的セキュリティ

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

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、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ものとする。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）業務委託とクラウドサービスの利用

業務委託を行う場合には、選定し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した上で、情報セキュリティ要件を明記した契約を締結し、必要に応じて契約に基づいた措置を講じる。

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。

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。

（9）　評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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本院の政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本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。