市立湖西病院　情報セキュリティポリシー
（基本方針）

市立湖西病院

第１章　情報セキュリティ基本方針

1. 目的

市立湖西病院(以下「湖西病院」)が取り扱う情報資産には、患者の生体情報など、機微性の高い要配慮個人情報等極めて慎重な取り扱いが求められる情報が多数含まれている。

また、マイナ保険証制度の導入や医療機器等における医療システムの DX 化に伴い、各種情報連携システムは、医療機関や行政機関、地方公共団体、医療保険者等が保有する個人情報を安全かつ効率的に連携・共有するための基盤であり、これを保護するため、技術的な対策だけでなく組織的・人的・物理的な観点から多層的なセキュリティ対策が必要である。

情報資産を取り扱うネットワーク及び情報システムを、サイバー攻撃や災害、内部不正などの様々な脅威から防御することは、患者の生命・健康・プライバシー等を守るために必要不可欠であり、医療サービスの安定的な提供の確保につながるものである。

このことから、情報資産の機密性、完全性及び可用性を維持するための対策整備を目的とした市立湖西病院情報セキュリティポリシーを定めることとし、情報セキュリティ基本方針については湖西市情報セキュリティポリシーに準拠し、対策の基本方針として情報セキュリティポリシーの対象、位置付け等を定めるものとする。

2. 定義

（1）ネットワーク

湖西病院における各部門及び部門間、各委託業者間において用いられる情報通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

（2）情報システム

業務系の電子計算機(業務系におけるネットワーク、ハードウェア及びソフトウェア)及び電磁的記録媒体で構成され、処理を行う仕組みをいう。

（3）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。

（4）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。

（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）基幹系

電子カルテ、オーダリング、医事会計及び連動する部門システムに関わる情報システム及びデータをいう。

（9）情報系

事務部門に配置される行政用基幹系、インターネット系以外の総合行政ネットワーク(LGWAN)に接続された情報システム及びデータをいう。また、必要なセキュリティ対策を講じた上で外部のクラウドサービスと接続(ローカルブレイクアウト)を行うことが出来る。

（１０）インターネット系

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。

３．情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、湖西病院が保有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

４．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、水道供給の途絶等のインフラの障害からの波及等

５．適用範囲

（１）医療機関の範囲

この情報セキュリティポリシーが対象とする範囲は、湖西病院が保有する情報資産を利用する全ての部署を対象とする。

なお、一部事務職が取り扱う湖西市の情報資産においては、湖西市情報セキュリティポリシーを適

用し、市立湖西病院情報セキュリティポリシーと分けるものとするが、資産情報の内容や性質に応じて相互の基準に依るものとする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア．ネットワーク及び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

イ．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。）

ウ．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

６．職員等及び委託事業者の遵守義務

職員等及び委託事業者は、業務遂行にあたり、情報セキュリティの重要性に対する統一された意識を持ち、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十分に理解し、遵守する義務を負うものとする。

７．情報セキュリティ対策

情報資産を脅威から保護するために、次に掲げる情報セキュリティ対策を講ずる。

（１）組織体制

市立湖西病院医療情報システム運用管理規定により、情報セキュリティ管理体制を確立する。

（２）情報資産の分類と管理

湖西病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・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ずる。

ア．基幹系においては、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、端末からの情報の持ち出し制限や端末への認証導入等により、情報等の流出を防ぐ。

イ．情報系においては、部門業務用システムと基幹系システムとの通信経路を限定制御する。

ウ．インターネット系においては、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。

エ．その他、事務職が取り扱う行政システムについては湖西市情報セキュリティポリシーに依る。

（４）物理的セキュリティ対策

サーバ、情報システム室、通信回線及び職員のパソコン等の管理について物理的な対策を講ずる。

（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・啓発を行う等の人的な対策を講ずる。

（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ずる。

（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ずるものとする。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（事業継続計画）を策定する。

（8）業務委託と外部サービス（クラウドサービス）の利用

業務委託する場合には、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ずる。外部サービス(クラウドサービス)を利用する場合には、利用にかかわる規定を整備し対策を講ずる。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、ソーシャルメディアサービスで発信できる情報を規定する。

（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。

８．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システムセキュリティ監査及び自己点検を実施する。

９．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。

１０．情報セキュリティ対策基準の策定

湖西病院の保有する情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、遵

守すべき行為及び判断等の基準を統一することが必要となる。そのため、情報セキュリティ対策を行う上で 必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

１１．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を遵守して情報セキュリティ対策を実施するために、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、情報セキュリティ対策基準及び情報セキュリティ実施手順は、詳細なセキュリティ対策を示したものであるため、公にすることにより重大な支障を及ぼす恐れのある情報資産であることから組織外への公開は行わないものとする。