地方独立行政法人大阪市民病院機構

情報セキュリティ管理要綱

直近改定：令和８年３月17日

制　定：平成28年４月１日

【目次】

第１条 目的

第２条 定義

（１）情報資産
（２）ネットワーク
（３）情報システム
（４）情報セキュリティ
（５）情報セキュリティポリシー
（６）機密性
（７）完全性
（８）可用性
（９）病院情報システム
（１０）病院事業ネットワークシステム
（１１）医学情報収集用ネットワークシステム
（１２）通信経路の分割
（１３）無害化通信

第３条 対象とする脅威

第４条 適用範囲

（１） 組織の範囲
（２） 情報資産の範囲

第５条 職員等の遵守義務

第６条 情報セキュリティ対策

（１） 組織体制
（２） 情報資産の分類と管理
（３） 情報システム全体の強靭性の向上
（４） 物理的セキュリティ
（５） 人的セキュリティ
（６） 技術的セキュリティ
（７） 運用
（８） 業務委託と外部サービスの利用
（９） 評価・見直し

第 7 条 情報セキュリティ監査及び自己点検の実施

第 8 条 情報セキュリティポリシーの見直し

第 9 条 情報セキュリティ対策基準の策定

第 10 条 情報セキュリティ実施手順の策定

（目的）

第１条　この要綱は、地方独立行政法人大阪市民病院機構（以下、「法人」という。）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、法人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　本要綱において、次に掲げる用語の意義は、当該各号に定めるところによる。

（１）情報資産

①　ネットワーク、パソコン、モバイル端末、電磁的記録媒体（USB、HDD 等）を含む情報システム及びこれらに関係する機器、設備

②　①で取扱う電子データ（紙媒体の文書を含む）

③　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

（２）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。

（３）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。

（４）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。

（５）情報セキュリティポリシー

組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書のことであり、本管理要綱及び情報セキュリティ対策基準をいう。

（６）機密性

情報資産にアクセスすることを認められた者だけが、アクセスできる状態を確保することをいう。

（７）完全性

情報資産が破壊、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。

（８）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、アクセスできる状態を確保することをいう。

（９）病院情報システム

電子カルテや部門システム等の患者情報を取り扱う情報システムをいう。

（１０）病院事業ネットワークシステム

病院事業の業務運営のためのネットワークシステムをいう。

（１１）医学情報収集用ネットワークシステム

医師向けに医学文献を検索するためのネットワークシステムをいう。

（１２）通信経路の分割

病院情報システム、病院事業ネットワークシステム、医学情報収集用ネットワークシステムは、それぞれ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。

（１４）外部サービス

外部の事業者が一般向けに提供する情報システム機能（ソーシャルメディアサービス、Web会議、検索、翻訳、クラウド等）を利用するサービスをいう。

（対象とする脅威）

第３条　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、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

（適用範囲）

第４条　適用範囲は次のとおりとする。

（１）組織の範囲

本要綱が適用される組織は、法人運営本部、大阪市立総合医療センター、大阪市立十三市民病院、大阪市立住之江診療所とする。

（２）情報資産の範囲

上記(1)の組織が保有する範囲とする。

（職員等の遵守義務）

第５条　法人の情報資産を取扱う役員および職員（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。

（情報セキュリティ対策）

第６条　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

法人の情報資産について、情報セキュリティ対策を推進する体制を確立する。

（２）情報資産の分類と管理

法人の保有する情報資産を情報セキュリティの３要素である機密性、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、次の対策を講じる。

①　病院情報システム（以下「ＨＩＳ」という。）においては、他の領域との通信を制限した上で、セキュリティソフトの導入、不正通信の監視、端末からの電子データ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情報流出を防ぎ、高度な情報セキュリティ対策を実施する。

②　病院事業ネットワークシステムにおいては、セキュリティソフトの導入、不正通信の監視、インターネット閲覧制限、ソフト・アプリインストールの制限、端末のポリシーの一括管理等により、高度な情報セキュリティ対策を実施する。

③　医学情報収集用ネットワークシステムにおいては、セキュリティソフトの導入、不正通信の監視、インターネット閲覧制限等により、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

情報システム室、通信回線及びパソコン等の情報資産の管理について、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。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）業務委託と外部サービスの利用

情報資産を取扱う業務委託を行う場合には、委託事業者選定の際、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いた措置を講じる。

ソーシャルメディアサービスを含む外部サービスを利用する場合には、サービスごとに責任者を定め、利用に係る規定や運用手順を整備し対策を講じる。

（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。

（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。

（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。

（情報セキュリティ対策基準の策定）

第9条　上記第6条、第7条及び第8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を策定する。

（情報セキュリティ実施手順の策定）

第10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。これは各部署が定めるマニュアルに該当し、公にすることにより法人の業務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

この対策基準は平成 28 年 4 月 1 日より施行する。

この改定対策基準は令和 8 年 3 月 17 日より施行する。