地方独立行政法人市立東大阪医療センター
情報セキュリティ基本方針

目次

1 目的

地方独立行政法人市立東大阪医療センター情報セキュリティ基本方針（以下「基本方針」という。）は、当センター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、地方独立行政法人市立東大阪医療センター（以下「法人」という。）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

(1) 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。

(2) 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。

(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

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) 医療情報システム

電子カルテシステムや部門システム等の患者の診療情報を取り扱うシステム及びネットワークの総称ことをいう。

(9) 事務系システム

病院事業の運営のためのネットワーク及びシステムの総称をいう。

(10) 通信経路の分割

病院情報システム、事務系システムの各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。

(11) 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ない等、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、標的型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、セキュリティ設定管理の不備、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、通信の途絶等のインフラの障害からの波及等

4 適用範囲

(1) 施設の範囲

基本方針が適用される施設は、地方独立行政法人市立東大阪医療センターとする。

(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。

① 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並びに電磁的記録媒体

② ネットワーク、情報システム及び電磁的記録媒体で取り扱う情報

③ 情報システムの仕様書、ネットワーク図等のシステム関連文書

④ その他、当センターの保有する情報

5 職員等の遵守義務

法人の業務に従事するすべての者（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医療情報システム管理規定を遵守しなければならない。

6 情報セキュリティ対策

想定される上記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全病院的な組織体制を確立する。

(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、次の対策を講じる。

① 医療情報システムにおいては、他の領域との通信をできないようにした上で、セキュリティソフトの導入、不正通信の監視、端末からの情報持ち出しの不可設定や端末ログイン時の2要素認証の導入により、情報漏洩を防ぎ高度な情報セキュリティ対策を実施する。また、年に2回Windows Server Update Servicesを用いた更新プログラムを展開する。

②事務系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、インターネットの閲覧制限、メール添付ファイルの無害化、ソフトウエア・アプリケーションのインストール制限や端末ポリシーの一元管理等により、高度な情報セキュリティ対策を実施する。特にインターネット接続においては、無害化通信等の対策を講じるものとする。

(4) 物理的セキュリティ

サーバー、電算機室、サーバー室、通信回線、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、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ものとする。また、情報資産に対する情報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、IT-BCP（事業継続計画別紙）を策定する。

(8) 業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、本基本方針を示した上で契約を締結し、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じる。

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。

(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、情報資産に係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、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、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。

制定日：令和8年1月23日

制定者：病院情報システム検討委員会