地方独立行政法人京都市立病院機構
情報セキュリティポリシー

【情報セキュリティ基本方針】

制定日：令和８年２月２４日
施行日：令和８年４月　１日

情報セキュリティポリシーの構成（基本方針と対策基準）

地方独立行政法人京都市立病院機構情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、地方独立行政法人 京都市立病院機構（以下「機構」という。）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る。

情報セキュリティポリシーは、本機構が所掌する情報資産を取り扱う本機構職員及び本機構の運営業務に携わる者（以下「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。
しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

以上のことから、情報セキュリティポリシーを、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層に分け、それぞれを策定することとする。

なお、機構では別に定める「京都市立病院機構情報セキュリティガイドライン」と「地方独立行政法人京都市立病院機構医療情報管理規程」が「情報セキュリティ対策基準」に該当する。

1　目的

本基本方針は、機構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、機構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等で構成され、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) 情報資産

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情報システム関連の機密文書

(5) 機密性

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

(6) 完全性

情報資産が破壊、改ざん又は欠落なく、常に正常で最新の状態を確保することをいう。

(7) 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。

(8) 電子カルテ接続系

電子カルテや部門システム等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。

(9) インターネット接続系

イントラネット等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。

(10) 通信経路の分割

電子カルテ接続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。

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、通信の途絶等の公共インフラの障害からの波及等

4　適用範囲

本基本方針を適用する組織は、京都市立病院及び京都市立京北病院の各部署とする。

5　職員等の遵守義務

職員等は、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

機構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体的な組織体制を確立する。

(2) 情報資産の分類と管理

機構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、各接続系について次の対策を講じる。

ア　電子カルテ接続系

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、患者情報の流出を防ぐ。

イ　インターネット接続系

必要に応じて、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。

(4) 物理的セキュリティ対策

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的対策を講じる。

(5) 人的セキュリティ対策・組織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、十分な教育及び啓発を行う等の人的・組織的対策を講じる。

(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、緊急時の対応計画を策定する。

(8) 業務委託と外部サービス（クラウドサービス）の利用

ア　業務委託を行う場合には、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じる。

イ　外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ウ　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、情報セキュリティの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。なお、情報セキュリティポリシーの見直しが必要な場合は、適宜それを行う。

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、情報セキュリティの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

情報セキュリティの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、保有する情報及び利用する情報システム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、リスクを検討したうえで、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

(1) 上記の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。

(2) 機構の情報セキュリティ対策基準は、「京都市立病院機構情報セキュリティガイドライン」と「地方独立行政法人京都市立病院機構医療情報管理規程」とし、これらを公開することにより機構の行政運営に重大な支障を及ぼす恐れがあると機構の理事長が判断した場合は、非公開とする。

10　情報セキュリティ実施手順の策定

(1) 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。

(2) 情報セキュリティ実施手順は、具体的な各手順書やマニュアルとし、これらを公開することにより機構の行政運営に重大な支障を及ぼす恐れがあると機構の理事長が判断した場合は、非公開とする。

附　則

本基本方針は令和８年４月１日より施行する。