地方独立行政法人福岡市立病院機構
情報セキュリティ基本方針

令和８年４月

地方独立行政法人福岡市立病院機構　情報セキュリティ基本方針

（目次）

１．目的

本基本方針(以下「基本方針」という。)は、地方独立行政法人福岡市立病院機構(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。

２．定義

この方針において、次の各号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)情報セキュリティ

情報資産の機密を保持し、情報資産の正確性及び完全性を維持し、並びに情報資産を定められた範囲で利用可能な状態で維持することをいう。

(２)情報資産

ネットワーク及び情報システム、これらに関する設備、これらで取り扱う情報、これらを印刷した文書、電磁的記録媒体並びにシステム構成図等の関連する文書をいう。

(３)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並びにその構成機器であるハードウェア及びソフトウェアをいう。

(４)情報システム

コンピュータ、ネットワーク、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。

(５)病院等

福岡市立こども病院、福岡市民病院並びに運営本部をいう。

(６)職員

法人に雇用される全ての職員(役員及び有期職員含む。以下同じ)をいう。

(７)派遣労働者

労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律(昭和 60 年法律第 88 号)第 26 条第１項に規定する労働者派遣契約に基づき法人に派遣され、法人の業務に従事している者をいう。

(８)脅威

情報資産に何らかの障害又は影響を与える原因となるものをいう。

(９)インターネット接続系

インターネットメール、ホームページ管理システム等に係るインターネットに接続された情報システム及び当該情報システムで取り扱うデータをいう。

(10)市全庁 OA システム(FINE)接続系

福岡市の全庁 OA システムに接続された端末及び当該情報システムで取り扱うデータをいう。

(11)事務人事給与業務システム系

法人の人事給与システム及び当該情報システムで取り扱うデータをいう。

(12)医療情報システム接続系

電子カルテシステム等の医療情報システム、人事評価システム、労務管理システム及び当該情報システムで取り扱うデータをいう。

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

４．適用範囲

この方針は、法人の病院等が所管する情報資産を利用する全ての職員及び派遣労働者（以下「職員等」という。）に適用する。

（１）法人の範囲

本基本方針が適用される組織は、福岡市立こども病院、福岡市民病院、運営本部とする。

（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及び電磁的記録媒体

②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。)

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

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の情報セキュリティに関する対策（以下「情報セキュリティ対策」という。）は、次に掲げるとおりとする。

（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、次の三段階の対策を講じる。

①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。

②市全庁 OA システム(FINE)接続系においては、他の領域と通信できないようにする。

③事務人事給与業務システム系においては、他の領域を通信できないようにする。
また、 記録媒体による端末からの情報持ち出しができないように設定するとともに、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医療情報システム系における対策は、各病院の「医療情報システム運用管理規定」等において定める。

（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）業務委託と外部サービス(クラウドサービス)の利用

①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。

②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。

③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、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

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。

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共通実施手順を策定するものとする。 なお、情報セキュリティ共通実施手順は、公にすることによって、法人の病院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。