タイトル	サイバーセキュリティを確保するための方針
説明	この方針は、地方自治法第２４４条の６、地方独立行政法人法第２４条の２及び総務大臣が示す指針「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針」に基づき、策定・変更し公表するものです。

本文

情報セキュリティ基本方針

1　目的

本基本方針は、当院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、当院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及びその構成機器（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) 医療情報システム

電子カルテシステム、電子カルテシステムと接続する各部門システム、各部門システムに接続する診療部等の接続機器、事務に関連するシステム及びファイル共有システム等の業務系で稼働する情報システムをいう。

(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

本基本方針及び情報セキュリティ対策基準をいう。

(6) 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。

(7) 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。

(8) 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。

(9) 業務系

イントラネットに接続された医療情報システム及びその情報システムで取扱うデータをいう。

(10) 情報系

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扱うデータをいう。

(11) 通信経路の分離

ある領域と他の領域との通信をできないようにすることをいう。

(12) 記録媒体

「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報処理の用に供されるものに係る記録媒体（以下「電磁的記録媒体」という。）がある。

(13) 外部サービス

一般の業者等の庁外の組織が情報システムの一部又は全部の機能を提供するクラウドサービス、ホスティングサービス、ハウジングサービス、ソーシャルメディアサービス等をいう。

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及び部外者の侵入等の意図的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、外部委託管理の不備、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

(1) 対象者

当院に勤務する役職者、職員及び有期雇用職員等全ての職員（以下「職員等」という。）とする。

(2) 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機器及び設備並びに電磁的記録媒体

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

エ　その他、２(13)に定める記録媒体及びそれに記録されている情報

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

当院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

当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・利便性を踏まえ、システム全体に対して、次の対策を講じる。

①　業務系と情報系とは、領域を分離することにより情報セキュリティの強化を図る。

②　業務系端末には、原則情報持ち出し不可設定を行い、患者情報の流出を防ぐ。

③　業務系において、オンライン資格確認用の通信については、その他業務系システムの通信とは異なるネットワーク体系とし、必要な通信だけ許可するようにしなければならない。

(4) 物理的セキュリティ

サーバ室、通信回線及び職員等のパソコン等の管理について、必要に応じ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、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、障害時対応計画を策定する。

(8) 委託業務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、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、必要に応じて措置を講じる。

外部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。

また、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、毎年度及び必要に応じて、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。

なお、情報セキュリティ対策基準は、情報セキュリティを確保するために公表すべきでない情報が含まれていることから非公開とする。

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当院の病院業務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。