

大垣市民病院 情報セキュリティ基本方針

1 目的

本基本方針は、本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、本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。

なお、本基本方針については、地方自治法（昭和22年法律第67号）第244条の6第1項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

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

本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) 医療情報システム接続系

本院の医療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) オンライン資格確認等システム接続系

オンライン資格確認等の事務に関わる情報システム及びデータをいう。

(10) LGWAN接続系

LGWAN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。

(1) 本庁インターネット接続系

本庁敷設のインターネットメール等に関わる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。

(2) 院内インターネット接続系

本院敷設のインターネットメール等に関わる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。

(3) 通信経路の分割

医療情報システム接続系、オンライン資格確認等システム接続系、L G W A N接続系と院内インターネット接続系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。

(4) 無害化通信

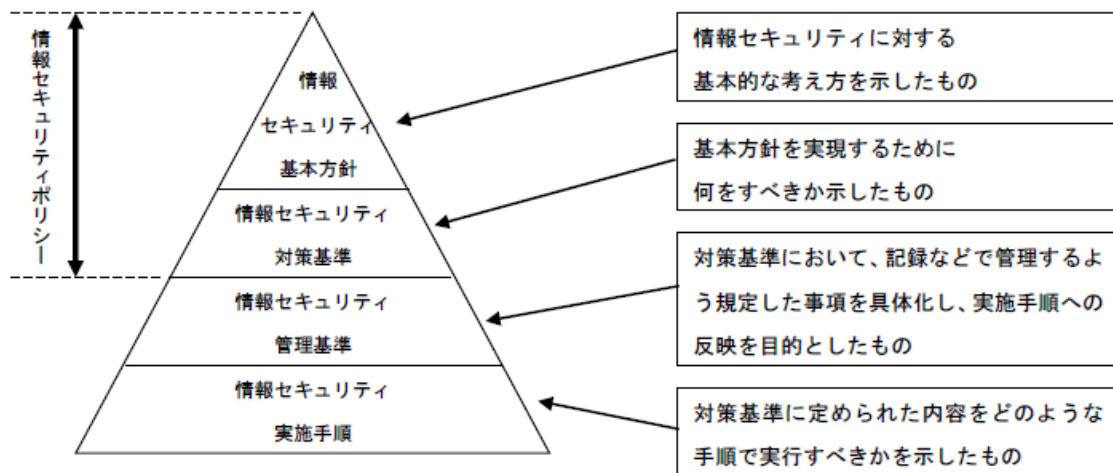
インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3 情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、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り、情報セキュリティ対策の頂点に位置するものである。

4 情報セキュリティポリシーの構成

情報セキュリティポリシーの構成は、一定の普遍性を備えた「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「情報セキュリティ対策基準」の二階層に分けて策定する。



5 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な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

6 適用範囲

(1) 組織の範囲

本基本方針は、本院の全ての組織に適用する。なお、事務局は、原則、大垣市情報セキュリティポリシーを適用するものとし、業務上、必要に応じて本基本方針を適用する。

(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 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

職員等が職務上作成し、又は取得した文書等

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器等
情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア（ウェブアプリケーションを含む）、クラウドサービス等

ネットワーク及び情報システムに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵記録媒体、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部記録媒体等
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等
職員等が職務上作成し、又は取得した文書等	申請書類、一覧のリスト、図画、写真等

7 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、情報セキュリティ管理基準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。

8 情報セキュリティ対策

前記5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

本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

本院の保有する情報資産をその重要度に応じて分類し、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靱性の向上

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 医療情報システム接続系及びオンライン資格確認等システム接続系においては、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等により、本院の医療情報の漏えいを防ぐ。
- ② LGWAN接続系においては、LGWANと接続する業務用システムと、本庁インターネット接続系の情報システムと通信経路の分割をする。なお、両システム間で通信する場合には、無害化通信を実施する。

③ 院内インターネット接続系においては、不正通信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

サーバ、サーバ室、通信回線等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（インシデント）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

業務委託を行う場合又は指定管理者に実施させる場合には、委託事業者を選定し、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情報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（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。

ソーシャルメディアサービスを利用する場合には、運用手順を定め、発信できる情報を規定し、サービスごとに責任者を定める。

(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な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の見直しを行う。

9 情報セキュリティ対策基準の策定

前記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 情報セキュリティ管理基準の策定

情報セキュリティ対策基準において、記録などで管理するよう規定した事項を具体化し、情報セキュリティ実施手順へ反映させることを目的として情報セキュリティ管理基準を策定する。

11 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、ネットワーク及び情報システム、個人番号及び特定個人情報並びにそれらに準ずるものの取扱いにおいて、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。

12 公開の範囲

情報セキュリティ対策基準、情報セキュリティ管理基準及び情報セキュリティ実施手順は、公にすることにより本院の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。

13 法令遵守

情報セキュリティに関する法令・ガイドライン等を遵守する。