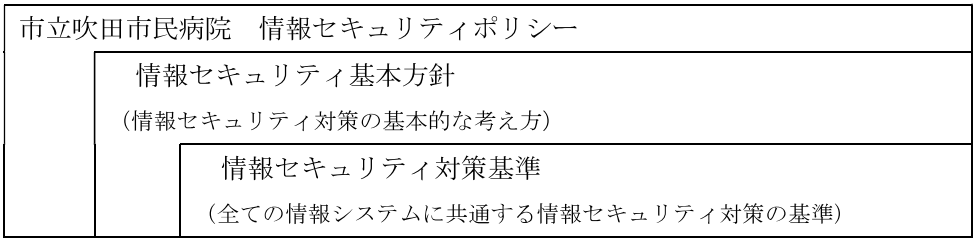
地方独立行政法人市立吹田市民病院

情報セキュリティポリシー

制　　定　平成２６年４月１日
最近改正　　令和６年９月１日

この情報セキュリティポリシーは、地方独立行政法人市立吹田市民病院（以下「当院」という。）が運用する情報システム及び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、情報セキュリティ基本方針及び情報セキュリティ対策基準で構成される。



Ⅰ　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情報セキュリティを維持するため、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、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）機密性

情報資産にアクセスすること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。

（5）完全性

情報資産が破壊、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。

（6）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、情報資産にアクセスできる状態を確保することをいう。

3　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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、重要情報の詐取、内部不正等の意図的な要因による脅威

（2）プログラム上の欠陥、操作、設定ミス、機器故障等の非意図的要因による脅威

（3）地震、落雷、火災、停電等の災害によるサービス、業務停止等の脅威

4　対象範囲

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、情報システム及びこれらに関する設備、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

（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

地方独立行政法人市立吹田市民病院正規職員、非常勤職員、アルバイト職員、再雇用職

員（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セキュリティポリシー、情報セキュリティに関連する規定等を順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、次の情報セキュリティ対策を実施する。

（１）組織体制

情報セキュリティ対策を強力に推進するため、その責任及び権限を明確にした院内全体的な管理体制を確立するものとする。

（２）情報資産の分類及び管理

当院の保有する情報資産を機密性、完全性、可用性の３つの側面から分析し、重要性に応じた分類に基づき情報セキュリティ対策を実施する。

（３）物理的なセキュリティ対策

情報処理機器、通信回線及びそれらを設置している施設等の管理について、物理的な対策を実施する。

（４）人的なセキュリティ対策

情報セキュリティに関する権限及び責任を明確にし、職員等が順守すべき事項を定めるとともに、セキュリティポリシーの意義を全ての職員等が理解できるように教育及び啓発に努める。

（５）技術的なセキュリティ対策

ネットワーク管理、外部及び内部からのアクセス制御、ウイルス対策等の技術面での対策を実施する。

（６）運用面におけるセキュリティ対策

情報システムの監視、セキュリティポリシーの順守状況の確認、外部委託を行う際のセキュリティ確保等、セキュリティポリシーの運用面の対策を実施する。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、迅速かつ適切に対応する。

7　情報セキュリティ監査及び自己点検

セキュリティポリシーの順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　評価及び見直し

情報セキュリティ監査及び自己点検による評価の結果、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、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

上記６、７及び８に規定する対策等を実施するために、具体的な順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。

なお、情報セキュリティ対策基準は、公にすることにより当院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、原則として非公開とする。

10　情報セキュリティ実施手順

セキュリティポリシーに基づき情報セキュリティ対策を実施するため、具体的な順守事項を明記した情報セキュリティ実施手順（以下「実施手順」という。）を策定する。

なお、実施手順は、公にすることにより当院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、原則として非公開とする。