町田市民病院

町田市民病院医療情報セキュリティ基本方針

、

－

町田市民病院医療情報セキュリティ対策基準及び実施手順については、
当面の間、町田市が策定したものを準用するものとする。

令和8年4月1日

町田市民病院医療情報セキュリティ基本方針

1. 目的

本基本方針は、町田市民病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。

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）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。

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）電力供給や通信の途絶、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）適用組織

町田市民病院の全ての部門とする。

（2）適用情報資産

本基本方針が対象とする情報資産は、次のとおりとする。

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本院が保有する情報

5 職員等の遵守義務

職員、臨時・非常勤職員等（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. 町田市民病院医療情報セキュリティポリシーの構成

医療情報セキュリティポリシーは、町田市民病院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、総合的かつ体系的に取りまとめたものであり、医療情報セキュリティ基本方針と医療情報セキュリティ対策基準によって構成する。

また、医療情報セキュリティポリシーに基づき、医療情報セキュリティ実施手順を策定することとする。

町田市民病院医療情報セキュリティポリシーの構成

文書名		内　容
医療情報セキュリティポリシー	医療情報セキュリティ基本方針	町田市民病院が保有する情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものであり、情報セキュリティ対策の最高位に位置するものとする。
	医療情報セキュリティ対策基準	基本方針に基づき、情報セキュリティ対策を実施するに当たっての遵守すべき事項及び判断等の統一的な基準として、医療情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。
医療情報セキュリティ実施手順		基本方針及び対策基準に基づき、情報セキュリティ対策を具体的に実施するために、医療情報セキュリティ実施手順（以下「実施手順」という。）を定めるものとする。

7. 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

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）物理的セキュリティ対策

サーバ、マシン室、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。

（４）人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な対策を講じる。

（５）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。

（６）運用

情報システムの監視及び情報セキュリティ対策の遵守状況の確認等について、運用面における必要な対策を講ずる。

（７）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。

8. 情報セキュリティ対策基準及び実施手順の非公表

基本方針は公表する。対策基準及び実施手順については、犯罪の予防、その他の公共の安全及び秩序の維持に支障を及ぼす恐れがあるため、公表はしない。

9. 情報セキュリティ対策の実施状況検証

医療情報セキュリティ対策が遵守されていることを確認するため、定期的に実施状況を検証するものとする。

附　則

（施行期日等）

１．この町田市民病院医療情報セキュリティ基本方針は、平成１９年４月１１日から施行する。

２．当面の間、情報セキュリティ対策基準及び情報セキュリティ実施手順は、町田市

の対策基準及び実施手順を準用する。

附　則

（施行期日等）

１．この町田市民病院医療情報セキュリティ基本方針は、令和４年４月１日に一部改正し、同日施行する。

２．当面の間、情報セキュリティ対策基準及び情報セキュリティ実施手順は、町田市の対策基準及び実施手順を準用する。

附　則

（施行期日等）

１．この町田市民病院医療情報セキュリティ基本方針は、令和８年４月１日に一部改正し、同日施行する。

２．当面の間、情報セキュリティ対策基準及び情報セキュリティ実施手順は、町田市の対策基準及び実施手順を準用する。