公立福生病院情報セキュリティ基本方針

平成17年５月26日告示第６号

公立福生病院情報セキュリティ基本方針

公立福生病院情報セキュリティ基本方針（平成17年告示第6号）の全部を改正する。

１　目的

ＩＴ社会の発展により、公立福生病院においても電子カルテシステム等の情報処理システムや情報通信ネットワークの活用は必要不可欠となっており、病院利用者等の個人の権利利益を守り、病院を安定的、継続的に運営するため、保有する情報資産を様々な脅威から守ることが責務となっている。

このため、公立福生病院情報セキュリティ基本方針は、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）　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）　公立福生病院セキュリティポリシー（以下「セキュリティポリシー」という。）

本基本方針及び公立福生病院情報セキュリティ対策基準（以下「セキュリティ対策基準」という。）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、必要な時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）　医療情報接続系（総合医療情報システム系）

診療に関わる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）　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。

（10）　通信経路の分割

医療情報接続系及びインターネット接続系の両環境間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。

（11）　無害化通信

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

3　対象とする脅威

情報資産に対する脅威として、次に掲げる脅威を想定し、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、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）　組織の範囲

本基本方針は、公立福生病院、福生病院企業団及び福生病院企業団議会に属する全ての組織に適用する。

（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。

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設備及び電磁的記録媒体

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

（３）　対象者

適用される情報資産に接する組織の職員（再任用職員、会計年度任用職員、福生病院企業団企業長、福生病院企業団議会の議員及び非常勤特別職の職員を含む。以下「職員等」という）とする。

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セキュリティポリシー及び情報セキュリティ実施基準を遵守しなければならない。

6　情報セキュリティ対策

前記３で示した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行うものとする。

（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及び管理するための体制を確立するものとする。

（２）　情報資産の分類と整理

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・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

ア　医療情報接続系においては、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、診療情報の流出を防ぐ。

イ　インターネット接続系においては、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、情報管理室、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、セキュリティポリシーの遵守状況の確認、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講じるものとする。この場合において、情報資産に対するセキュリティ侵害発生時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

ア　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ずる。

イ　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。

ウ　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

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。セキュリティポリシーの見直しが必要な場合は、適宜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

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　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、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、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ものとする。

10　情報セキュリティ実施基準の策定

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基準を策定するものとする。

なお、情報セキュリティ実施基準は、公にすることにより当院の運営に重大な支障を及ぼすお

それがある情報資産であることから、福生病院企業団情報公開条例（平成31年条例第１号）第７条第４号に基づき非公開とする。