昭和病院企業団情報セキュリティ基本方針

平成２８年１０月１２日決定
改正　令和８年４月１日

（目的）

第１条　ＩＴ社会の発展により、昭和病院企業団　（以下「企業団」という。）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、企業団を安定的、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、昭和病院企業団情報セキュリティ基本方針を定め、総合的、体系的、積極的に情報セキュリティ対策を実施する。

（情報セキュリティ対策の体系）

第２条　情報セキュリティ基本方針に基づき、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を定める。

（１）情報セキュリティ対策基準

情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために、各情報システム共通の最低限必要な水準として、具体的な遵守事項及び判断基準等を定めるものである。

（２）情報セキュリティ実施手順

情報セキュリティ対策基準に基づき、情報システムごとに情報セキュリティ実施手順を策定し、これに基づき情報システム等を運用する。

なお、情報セキュリティ実施手順は、公にすることにより企業団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。

（用語の定義）

第３条

（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(ハードウエア及びソフトウエア) をいう。

（２）情報システム

コンピュータ、端末装置、通信回線等により、電子情報を処理するシステムをいう。

（３）情報資産

以下のものをいう。

ア　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（以下「情報システム等」という。）

イ　情報システム等で取り扱う電磁的な情報

ウ　情報システム等の仕様書及びネットワーク図等のシステム関連文書

（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。

ア　機密性とは、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。

イ　完全性とは、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。

ウ　可用性とは、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。

（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。

（適用範囲）

第３条の２　本基本方針は、昭和病院企業団、議会及び監査委員に属するすべての組織に適用する。

（対象とする脅威）

第４条　情報資産に対する脅威として、以下のものを想定し、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

（職員等の遵守義務）

第５条　職員、非常勤職員及び臨時職員は、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等を遵守しなければならない。

（外部委託事業者等への対策）

第６条　企業団の業務を受託する事業者及び派遣職員に当該業務等を行わせる場合においては、セキュリティ対策上遵守させるべき事項を契約または協定等において明記するとともに、本基本方針及び対策基準と同様の水準での情報セキュリティを確保で

きるよう、必要な措置をとるものとする。

（情報セキュリティ対策）

第７条　第４条に規定する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

企業団の情報資産について、総合的な情報セキュリティ対策を推進するため、全病院的な組織体制を確立する。

（２）　情報資産の分類と管理

企業団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行う。

（３）　物理的セキュリティ対策

サーバ、情報システム室、通信回線等及びパソコン等の情報処理機器類の管理について、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、情報セキュリティ対策基準等に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など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）　情報セキュリティポリシーの運用

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、外部委託等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運用上の対策を講じる。

また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

（７）　外部サービス（クラウドサービス）の利用

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、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。

（情報セキュリティ監査及び自己点検）

第８条　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する。

（情報セキュリティポリシーの見直し）

第９条　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への対応が必要となった場合には、情報セキュリティポリシーを見直す。