高知県・高知市病院企業団情報セキュリティ基本方針

令和８年４月１日

（趣旨）

第１条　高知県・高知市病院企業団情報セキュリティ基本方針（以下「基本方針」という。）は、高知県・高知市病院企業団（以下「企業団」という。）が管理する情報資産を適切に取り扱い、企業団の情報セキュリティを確保するための基本的な方針を定めるものとする。

なお、企業団議会及び企業団監査委員においても、必要な範囲でこれを準用するものとする。

（定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）　院内ネットワーク　院内の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る、情報を処理するための仕組みをいう。

（３）　情報資産　院内ネットワーク並びに情報システム（これに付随する開発、運用及び保守のための資料等を含む。）及び当該情報システムで利用される情報（これらの内容を印刷した文書を含む。）をいう。

（４）　情報セキュリティポリシー　この基本方針及び情報セキュリティ対策基準をいう。

（５）　情報セキュリティ対策基準　情報セキュリティに関する対策等を実施するため、具体的な遵守事項、判断基準等を定めたものをいう。

（６）　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定める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まとめたものをいう。

（７）　機密性　情報にアクセスすることを認められた者だけが、情報にアクセスすることができる状態を確保することをいう。

（８）　完全性　情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

（９）　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、情報にアクセスすることができる状態を確保することをいう。

(10)　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。

(11)　診療系　電子カルテシステム、部門システム及び接続機器など患者の診療に関する情報を取り扱う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。

(12)　LGWAN系　LGWANに接続された情報システム及び当該情報システムで取り扱うデータをいう。

(13)　インターネット系　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当該情報システムで取り扱うデータをいう。

（情報資産に対する脅威）

第３条　情報資産を管理し、又は利用する所属の長は、情報資産に対する脅威として、次に掲げる脅威を想定し、第７条の規定による情報セキュリティ対策を行うものとする。

（１）　不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成１１年法律第

１２８号）第２条第４項に規定する不正アクセス行為をいう。第７条第４号において同じ。）による情報資産の漏えい、破壊、改ざん又は消去、重要な情報の詐取、内部不正等

（２） 情報資産の無断での持ち出し、許可を得ていないソフトウェアの使用、設計又は開発の不備、プログラムの欠陥、操作又は設定の誤り、メンテナンスの不備、内部又は外部による監査機能の不備、委託業者による管理の不備、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、改ざん又は消去等

（３） 地震、落雷、火災等の災害によるサービス又は業務の停止等

（４） 大規模又は広範囲にわたる疾病等により、作業要員が不足すること等に伴うシステム運用の機能不全等

（５） 電力若しくは水道の供給若しくは通信の途絶等又はインフラの障害等に伴うシステム運用の機能不全等

（職員の責務）

第４条 職員（会計年度任用職員、臨時的任用職員及び非常勤職員を含む。以下同じ。）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は、法令、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、情報資産の適切な管理に努めなければならない。

２ 職員は、情報資産を取り扱う事務の全部又は一部を事業者に委託する場合は、法令、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させるために必要な措置を講ずるものとする。

（情報セキュリティ委員会）

第５条 情報セキュリティ対策を総合的に推進し、情報セキュリティ対策に関する調整を行うため、情報セキュリティ委員会を置く。

２ 前項の規定により置かれる情報セキュリティ委員会（以下「情報セキュリティ委員会」という。）に関し必要な事項は、情報セキュリティ対策基準によるものとする。

（情報資産の分類）

第６条 情報資産を管理し、又は利用する所属の長は、情報セキュリティ対策基準 に定めるとおりその管理する情報資産を分類し、その分類に応じた情報セキュリティ対策を行うものとする。

（情報セキュリティ対策の実施）

第７条 情報資産を管理し、又は利用する所属の長は、情報資産に対する脅威（第３条各号に掲げる脅威をいう。第１号イにおいて同じ。）から情報資産を保護するため、次に掲げる情報セキュリティ対策を行わなければならない。

（１） 情報システム全体の強靭性を向上するため、院内ネットワークに接続する情報システム全体を次に掲げる区分に領域を分離し、それぞれ次に掲げる情報セキュリティ対策を講ずること。

ア 診療系 原則として、他の領域と分離し、必要な場合は安全性を確保した通信経路を用いて接続すること。端末からの情報の持出しを不可能とする設定、端末への多要素認証の導入等により、情報の流出を防ぐこと。

イ LGWAN系 当該LGWAN系とインターネット系との通信経路 を分割することを基本とし、両者の間で通信を行う場合には、無害化通信（情報資産に対する脅威を無害化した通信をいう。）により行うものとすること。

ウ インターネット系 不正な通信の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こと。

（２） サーバ、情報システム室、通信回線、職員のパソコン等の管理について、物理的な対策を講ずること。

（３） 情報セキュリティに関し、職員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ずること。

（４） 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、不正アクセス行為の対策等の技術的対策を講ずること。

（５） 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、業務委託をする場合のセキュリティの確保等、情報セキュリティポリシーの運用面の対策を講ずること。

（６） 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、ITシステムにおける事業継続計画（IT-BCP）を策定すること。

（７） 業務委託をする場合又は外部サービス（クラウドサービス）を利用する場合は、次に掲げる情報セキュリティ対策を行うこと。

ア 業務委託をする場合は、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、必要に応じて当該契約に基づき必要な措置を講ずること。

イ 外部サービス（クラウドサービス）を利用する場合は、利用に係る規定を整備し、対策を講ずること。

ウ ソーシャルメディアサービスを利用する場合は、ソーシャルメディアサービスの運用方針を定め、発信することができる情報を規定し、利用するサービスごとの管理者を定めること。

（情報セキュリティ対策基準の策定）

第８条 情報セキュリティ委員会の副委員長は、前条の規定による情報セキュリティ対策の実施のため、情報セキュリティ対策基準を定めるものとする。

（情報セキュリティ実施手順の作成等）

第９条 情報システムを管理する者は、自らが管理する情報システムについて、情報セキュリティ対策基準に定める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まとめた情報セキュリティ実施手順を作成しなければならない。

２ 情報システムを管理する者は、情報セキュリティを確保するため、情報セキュリティ対策の実施状況の点検を行い、必要に応じて情報セキュリティ実施手順の見直しを行うものとする。

３ 情報システムを管理する者は、情報セキュリティ実施手順を公表しないものとする。

（情報セキュリティの監査及び自己点検の実施の指示）

第10条 情報セキュリティ委員会の委員長は、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の監査及び自己点検の実施を指示し、運用改善を行い、情報セキュリティの向上を図るものとする。

（情報セキュリティポリシーの見直し）

第11条 前条の規定による情報セキュリティの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又は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な対策が必要になった場合は、情報セキュリティ委員会において情報セキュリティポリシーの見直しを行うものとする。

（委任）

第12条 この規程の施行に関し必要な事項は、企業長が別に定める。

附 則

この基本方針は、令和８年４月１日から施行する。