地方独立行政法人香取おみがわ医療センター情報セキュリティ基本方針

１．目的

本基本方針は、地方独立行政法人香取おみがわ医療センター（以下「法人」という。）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、法人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

本基本方針において用いる用語の定義は、以下のとおりとする。

（１）情報資産

法人が業務上取り扱う情報及びその情報を処理・保存・伝送するための仕組みをいう。

なお、情報資産には、次のものを含むものとする。

① 情報（電子データ、記録媒体、音声、映像、画像、画面表示、紙媒体、記憶によるものを含む。）

② 医療情報（診療録、検査結果、放射線画像、処方情報、医療機器から取得されるデータ等）

③ 個人情報（特に要配慮個人情報を含む。）

④ 情報システム（コンピュータ、ネットワーク、サーバ、端末、記録媒体等）

⑤ 医療機器（ネットワーク接続機器）

（２）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。

（３）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。

（４）役員

法人の理事長、副理事長、理事及び監事をいう。

（５）職員等

役員及び法人に勤務する全職員（雇用形態、職位等を問わない。）をいう。

（６）利用者

情報資産にアクセスする職員等、外部委託業者、医療機器保守担当者及び香取おみがわ医療センター附属看護専門学校等の学生をいう。

（７）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。

（８）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。

（９）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。

(10) クラウドサービス

インターネットを通じて提供される情報処理サービスであり、データの保存、処理、通信等を外部事業者の設備で行うサービスをいう。

(11) 情報セキュリティインシデント

情報漏えい、不正アクセス、マルウェア感染、システム障害、医療機器の誤作動等、情報資産の機密性・完全性・可用性に影響を及ぼす事象をいう。

(12) リスクアセスメント

情報資産に対する脅威と脆弱性の組み合わせにより、発生する可能性のある損害の程度を評価し、必要な対策を検討するプロセスをいう。

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）意図的な要因による脅威

サイバー攻撃、不正アクセス、マルウェア感染、脆弱性の悪用、内部不正、部外者の侵入等の意図的な要因により、情報資産が受ける漏えい・破壊・改ざん・消去等

（２）非意図的な要因による脅威

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な要因により発生する情報資産の漏えい・破壊・消去等

（３）災害による脅威

地震、落雷、火災、洪水等の災害による業務の停止

（４）人的・社会的要因による脅威

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）インフラ障害による脅威

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

本基本方針の適用範囲は、法人の情報資産に関わるすべての利用者とする。

５．利用者の遵守義務

利用者は、情報資産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．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

情報資産の管理及び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

情報資産を機密性、完全性及び可用性に応じて分類し、リスクアセスメントを実施した上で、当該分類に基づき適切な管理及び対策を実施する。

（３）物理的セキュリティ

サーバ、ネットワーク機器、医療機器、端末等の物理的な管理について対策を講じる。

（4）人的セキュリティ

情報資産を取り扱う利用者が遵守すべき事項を定めるとともに、教育及び啓発を行う。

（5）技術的セキュリティ

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、情報セキュリティポリシーの遵守状況の確認、業務委託及び再委託におけるセキュリティ確保等、運用面の対策を講じる。また、情報セキュリティインシデント発生時には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。

（7）業務委託とクラウドサービスの利用

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する。

クラウドサービスを利用する場合には、利用者とクラウド事業者との責任分界点（責任共有モデル）を明確化し、契約書に明記する。

ソーシャルメディアサービスを利用する場合には、運用手順を定め、発信可能な情報を規定し、責任者を定める。

（8）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、リスクの変化に応じて見直し、必要な改善を行う。

7．情報セキュリティ監査及び自己点検の実施

情報資産の管理状況及び情報セキュリティ対策の実施状況について、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．情報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、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に対応するため新たに対策が必要になった場合には、情報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の策定

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。

10．情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報資産を適切に管理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手順を策定する。

なお、情報セキュリティ実施手順は、公にすることにより法人の業務運営に重大な支障を及ぼす恐れがあることから非公開とする。