伊万里・有田地区医療福祉組合情報セキュリティ基本方針

（目的）

第 1 条　伊万里・有田地区医療福祉組合情報セキュリティ基本方針（以下、「本基本方針」という。）は、伊万里・有田地区医療福祉組合（以下、「組合」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、組合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。なお、組合事務局は議会に関する事務を兼務しているため、議会の情報セキュリティ基本方針を兼ねるものとする。

（定義）

第２条　本基本方針の用語の定義は、次の各号に掲げるとおりとする。

（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エア）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）医療情報システム

伊万里・有田地区医療福祉組合病院事業医療情報システム運用管理規程（以下「医療情報システム管理規程」という。）第２条に規定するシステムをいう。

（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。

（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。

（６）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。

（７）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。

（８）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情報を確保することをいう。

（９）マイナンバー利用事務

個人番号利用事務（職員等に係る社会保障に関する事務及び職員等に係る税に関する事務）をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、次の各号の脅威を想定し、情報セキュリティ対策を実施する。

（１）　不正アクセス、ウイルス攻撃及びサービス不能攻撃等のサイバー攻撃並びに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、重要情報の搾取及び内部不正等

（２）　情報資産の無断持ち出し、無許可ソフトウエアの使用、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及び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因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障害からの波及等

（適用範囲）

第４条　本基本方針が適用される機関は、組合事務局、老人ホーム事業及び病院事業とする。

２　本基本方針が対象とする情報資産は、次の各号に掲げるとおりとする。

（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）　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。）

（３）　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

（４）　医療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。）

３　本基本方針の適用の対象となる職員は、組合に勤務する全職員（雇用形態等は問わない。）とする。

（情報セキュリティ対策）

第５条　第３条に規定する脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講じる。

（１）　組織体制

組合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。医療情報システムの管理体制については、医療情報システム管理規程第４条のとおりとする。

（２）　情報資産の分類と管理

組合が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）　情報システム等の強靭化の向上

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、情報システム等に対し、次の対策を講じる。

① マイナンバー利用事務においては、原則として、社会保障及び税に関する事務担当者以外の利用を禁止する等取扱者を限定し、定期的又は必要に応じて点検を行い、個人情報の流出を防ぐ。

② インターネットを利用する事務においては、不正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。

（４） 物理的セキュリティ

サーバ、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、情報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、情報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。医療情報システムについては、医療情報システム管理規程第３条の規定に基づき、運用する。また、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切に対応するため、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じる。外部サービス（クラウドサービス）を利用する場合には、利用にかかる規程を整備し対策を講じる。

（９）情報セキュリティ監査及び自己点検の実施

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。

(10) 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には、情報セキュリティポリシーを見直す。

(11) 情報セキュリティ対策基準の策定

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を実施するにあたって必要となる基本的な要件を明記した情報セキュリティ対策基準を定める。

なお、情情報セキュリティ対策基準は、公にすることにより組合の運営に重大な支

障を及ぼす恐れがあることから非公開とする。

(12) 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手順を策定するものとする。なお、情報セキュリティ対策手順は、公にすることにより組合の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。

附則

この訓令は、令和８年２月１日から施行する。