滋賀県後期高齢者医療広域連合

情報セキュリティポリシー

（基本方針）

令和６年４月１日施行
（令和８年６月１日一部改定）

【 目　　次 】

第１章　情報セキュリティ基本方針

１　目的

情報セキュリティ基本方針（以下「本基本方針」という。）は、広域連合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、広域連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。

２　定義

⑴　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ェア）をいう。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　完全性

情報が破壊、改ざん又は消去されてない状態を確保することをいう。

⑺　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状態を確保することをいう。

⑻　情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

⑼　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務に関わる情報システム及びデータをいう。

⑽　標準システム接続系

滋賀県後期高齢者医療広域連合電算処理システム（以下「標準システム」という。）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（マイナンバー利用事務系を除く）。

⑾　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。

⑿　通信経路の分割

標準システム接続系と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。

⒀　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、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、以下の脅威を想定し、情報セキュリティ対策を実施する。

⑴　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、情報資産の詐取、内部不正等

⑵　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、業務委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・消去等

⑶　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

⑷　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

⑸　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

⑴　行政機関の範囲

本基本方針が適用される行政機関は、広域連合、選挙管理委員会、監査委員、公平委員会及び議会並びに構成市町とする。

⑵　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。

①　ネットワーク及び情報処理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

⑶　取扱者の範囲

広域連合の情報資産に関わる全ての職員（会計年度任用職員及び特別職職員並びに広域連合の業務の受託業者を含む。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、 情報セキュリティに関する関係法令及び情報セキュリティポリシーを遵守しなければならない。

6　組織体制

広域連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。

7　情報資産の分類と管理

広域連合の保有する情報資産を機密性、完全性及び可用性を鑑み、重要性に応じた分類とし、当該分類に基づき情報セキュリティ対策を行う。

8　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、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し制限や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

② 標準システム接続系においては、標準システムと、インターネット接続系の情報システムとの通信経路を分割する。

③ インターネット接続系においては、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。

９ 物理的セキュリティ

広域連合が保有、管理するサーバ、パソコン端末等機器類（広域連合が保有、管理する機器類のうち市町に設置する端末及び市町が保有、管理する機器類で標準システムのネットワークに接続する端末等機器類を含む。）及び通信回線、広域連合電算室等の管理について、物理的な対策を講じる。

10 人的セキュリティ

情報セキュリティに関し、職員等に情報セキュリティポリシー及び同実施手順を周知徹底し、十分な教育及び啓発を行う等の人的な対策を講じる。

11 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。

12 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、情報セキュリティインシデントの報告及び対応、業務委託を行う際のセキュリティ確保等の情報セキュリティポリシーの運用面の対策を講じる。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正に対応するため、緊急時対応計画を策定する。

13 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、以下「クラウドサービス」という。）を利用する場合には、利用にかか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。

14 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、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

15　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、中期計画を策定したうえで情報セキュリティ監査及び自己点検を実施する。

16　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に対策が必要になった場合には、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、情報セキュリティポリシーを見直すものとする。

17　情報セキュリティ対策基準の策定

上記の情報セキュリティ対策等を実施するための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。

18　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。

なお、情報セキュリティ実施手順は、公にすることにより広域連合の制度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。

19　構成自治体の対応等

広域連合を構成する市町等において、後期高齢者医療の事務を行う場合、本基本方針のほか、市町等において定めている情報セキュリティポリシーに基づき、適切に対応するものとする。