愛知県後期高齢者医療広域連合情報セキュリティ基本方針

１　目的

本基本方針は、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とともに、広域連合のサイバーセキュリティを確保するための方針として位置付けることを目的とする。

２　定義

（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及びその構成機器（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、情報処理を行う仕組みをいう。

（３）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。

（４）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。

（５）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。

（６）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。

（７）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。

（８）情報セキュリティインシデント

情報資産に対する脅威が顕在化し、情報資産の機密性、完全性及び可用性が侵害される又は侵害されるおそれがある事態をいう。

（９）脅威

情報セキュリティインシデントが発生する原因をいう。

（１０）リスク

特定の脅威に関する情報セキュリティインシデントの発生確率及び発生した際の被害の程度の組合せをいう。

（１１）マイナンバー利用事務系

広域連合が行う個人番号利用事務（後期高齢者医療事務）に関わる情報システム及びデータをいう。

（１２）インターネット接続系

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。

（１３）職員等

広域連合が保有する情報資産に関する業務に携わる職員、非常勤職員及び臨時職員等をいう。

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）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、外部委託管理の不備、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

４　適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関等は、広域連合長、議会、選挙管理委員会及び監査委員とする。

（２）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 広域連合が所管するネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② 広域連合が所管する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・転記した文書や入力・参照のために用いる文書を含む。）

③ 広域連合が所管する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

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

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・管理するための体制を確立するものとする。

（２）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）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、次の二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不可設定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 インターネット接続系においては、不正通信の監視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対策

広域連合が保有する情報資産について、盗難防止や災害対策等、脅威への物理的な対策を行う。

（５）人的セキュリティ対策

情報セキュリティに関する職員等の権限、責任及び遵守事項を明確化し、職員等に対する十分な教育及び啓発を行う等、脅威への人的対策を行う。

（６）技術的セキュリティ対策

情報システムやネットワークの管理、アクセス制御、不正プログラム対策、不正アクセス対策等、脅威への技術的対策を講じる。

（７）運用

情報システムやネットワークの監視、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。また、情報セキュリティインシデントが発生した場合等に迅速かつ適切に対応するため、統一的な対応窓口である情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team）を設置し、インシデント対応計画を策定する。

（８）業務委託と外部サービス（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）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。

（９）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。

７　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。

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。

なお、情報セキュリティ対策基準は、公にすることにより広域連合の行政運営に重大な支障を及ぼすおそれがあることから原則非公開とする。

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、情報セキュリティ実施手順は、公にすることにより広域連合の行政運営に重大な支障を及ぼすおそれがあることから原則非公開とする。

附則

この基本方針は、令和８年４月１日から施行する。