情報セキュリティポリシー

制定：平成１９年１２月
改定：令 和 ５ 年 ３ 月

大阪府後期高齢者医療広域連合

目次

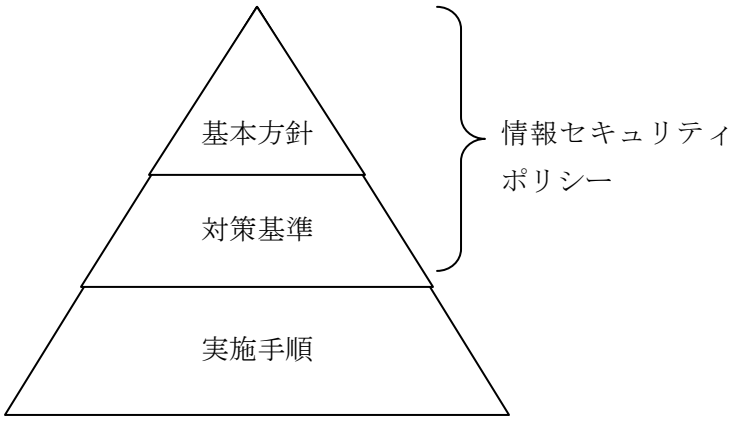
内容

第１章　情報セキュリティポリシーの必要性と構成

大阪府後期高齢者医療広域連合（以下「広域連合」という。）においては、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、明文化された文書として、情報セキュリティポリシーを定める。

情報セキュリティポリシーの体系は、図表１に示す階層構造となっている。

情報セキュリティ対策における基本的な事項を定めるものが、「基本方針」である。この基本方針に基づき、すべての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。また、「対策基準」を実施するための具体的な手順を定めるものが「実施手順」である。



図表１　情報セキュリティポリシーに関する体系図

第２章　情報セキュリティ基本方針

２．１ 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ことを目的とする。

２．２ 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、その構成機器(ハードウエア及びソフトウエア）をいう。このうち、物理的又は論理的に広域連合が占有するネットワーク以外を外部ネットワークという。

（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） 情報システム室

広域連合の事務所内にあり、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋をいう。

（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

情報セキュリティ基本方針及び対策基準をいう。

（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状態を確保することをいう。

（９）マイナンバー利用事務系（個人番号利用事務系）

①医療保険者等向け中間サーバ等に専用ネットワークで接続された端末及びその情報システ

ムで取り扱うデータをいう。

②広域連合及び市町村に設置した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。）端末と標準システムサーバを専用ネットワークで接続した標準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

（１０）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。

（１１）通信経路の分割

マイナンバー利用事務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。

（１２）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。

２．３ 対象とする脅威

情報資産に対する脅威として、以下の脅威とそれによるリスクを想定し、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、重要情報の搾取、内部不正等

（２） 情報資産の無断持ち出し、無許可ソフトウエ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、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、水道共有の途絶等のインフラの障害からの波及等

２．４ 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は、広域連合内部部局、選挙管理委員会、監査委員、公平委員会及び議会事務局とする。

なお、 標準システムを利用する範囲において関係市町村の担当部局（以下「関係市町村」という。）についても、これに準じるものとする。

（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 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 その他、後期高齢者医療制度の運営に関する情報と広域連合内部の運営に関する情報

２．５ 職員の遵守義務

職員（臨時的任用職員、任期付職員、会計年度任用職員、定年前再任用短時間勤務職員及び暫定再任用職員を含む）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。

なお、 標準システムを利用する範囲において関係市町村の窓口部局の職員についても、これに準じるものとする。

２．６ 情報セキュリティ対策

上記２．３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する全庁的な組織体制を確立する。

（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、インターネット接続系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、情報システム室、通信回線並びに職員のパソコンやモバイル端末等の管理について、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、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、情報資産への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。

（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

２．７ 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。

２．８ 情報セキュリティ対策基準の策定

上記２．６及び２．７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。

２．９ 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非公開とする。