情報セキュリティポリシー

制定：平成１９年１２月
改定：令 和 ４ 年 ３ 月

第１章　情報セキュリティポリシーの必要性と構成

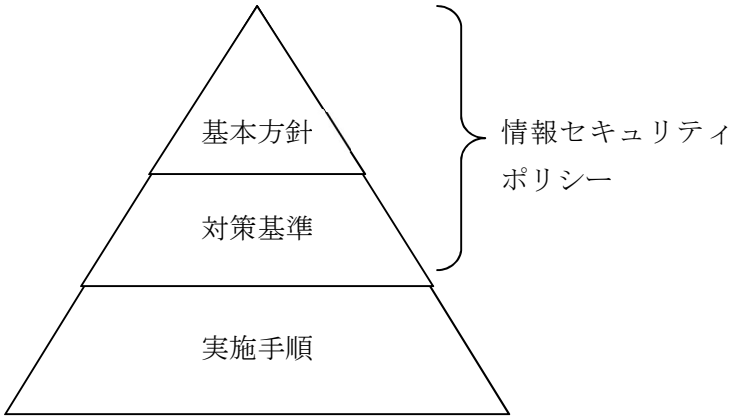
大阪府後期高齢者医療広域連合（以下「広域連合」という。）においては、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには広域連合外に設置され後期高齢者医療制度に係る業務を行う市町村の窓口（以下「庁外窓口」という。）と広域連合とが意思統一し、明文化された文書として、情報セキュリティポリシーを定めなければならない。

なお、行政手続等における情報通信の技術の利用に関する法律（平成 14 年法律第 151 号）第 9 条第 1 項は、「地方公共団体は、地方公共団体に係る申請、届出その他の手続における情報通信の技術の利用の推進を図るため、この法律の趣旨にのっとり、当該手続に係る情報システムの整備及び条例又は規則に基づく手続について必要な措置を講ずること」に努めなければならないと規定しており、条例等に基づく手続については、同法第 8 条第 2 項（安全性及び信頼性の確保）の趣旨にのっとり、広域連合は情報セキュリティポリシーの策定や見直しを行うことが求められている。広域連合では平成 19 年度に情報セキュリティポリシーを制定し運用を開始した。平成 29 年度には外部環境の変化及び後期高齢者医療制度関係事務における個人番号を含む個人情報（特定個人情報）の利用を考慮し、情報セキュリティポリシーの見直しを実施した。

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。

広域連合の情報セキュリティ対策における基本的な考え方を定めるものが、「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。具体的なシステムや手順、手続に個別の実施事項を定めるものが「実施手順」である。

このように、情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、広域連合長をはじめ、広域連合の職員、会計年度任用職員及び臨時的任用職員（以下「広域連合職員等」という。）並びに庁外窓口の職員、会計年度任用職員及び臨時的任用職員（以下「庁外窓口職員等」という。）並びに外部委託事業者は、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負う。



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

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状態を確保することをいう。

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） 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、プログラム上の欠陥、操作ミス、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

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、庁外窓口、選挙管理委員会、監査委員、公平委員会及び議会とする。

（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、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 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　広域連合職員等及び庁外窓口職員等の遵守義務

広域連合職員等及び庁外窓口職員等は、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。

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）物理的セキュリティ

サーバ等、情報システム室等、通信回線等並びに広域連合職員等及び庁外窓口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。

（４）人的セキュリティ

情報セキュリティに関し、広域連合職員等及び庁外窓口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。

（５）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。

（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、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。また、情報資産への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。

２．７　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。

２．８　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。

２．９　情報セキュリティ対策基準の策定

上記２．６、２．７及び２．８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。

２．１０　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非公開とする。