兵庫県後期高齢者医療広域連合
情報セキュリティ基本方針

制定日：平成19年６月25日

改定日：令和８年３月31日

施行日：令和８年４月１日

兵庫県後期高齢者医療広域連合

改訂履歴

施行年月日	版番号	改訂理由・内容
平成１９年　６月　５日	第1.0版	初版発行
平成２７年１２月２８日	第2.0版	一部改正
令和　８年　４月　１日	第3.0版	全部改正（令和８年３月31日決裁）

目次

１．目的 1
２．定義 1
　２．１　ネットワーク 1
　２．２　情報システム 1
　２．３　データ 1
　２．４　情報セキュリティ 1
　２．５　情報セキュリティポリシー 1
　２．６　機密性 1
　２．７　完全性 1
　２．８　可用性 2
　２．９　マイナンバー利用事務系（個人番号利用事務系） 2
　　２．９．１　標準システム系 2
　　２．９．２　国保連合会システム系 2
　　２．９．３　中間サーバ系 2
　２．１０　事務処理系 2
　２．１１　通信経路の分離 2
　２．１２　システム利用団体 2
３．情報セキュリティポリシーの位置付け及び構成 2
４．対象とする脅威 3
５．適用範囲 3
　５．１　組織の範囲 3
　５．２　情報資産の範囲 3
　５．３　情報資産の対象 3
６．職員等の遵守義務 4
　６．１　システム利用団体の情報セキュリティポリシーとの関係 4
７．情報セキュリティ対策 4
　７．１　情報セキュリティ管理体制 4
　７．２　情報セキュリティ管理体制 4
　７．３　情報システム全体の強靭性の向上 4
　７．４　物理的セキュリティ 5
　７．５　人的セキュリティ 5
　７．６　技術的セキュリティ 5
　７．７　運用 5
　７．８　業務委託等及び外部サービス（クラウドサービス）の利用 5

８．情報セキュリティ監査及び自己点検の実施 5
９．情報セキュリティポリシーの見直し 5
１０．情報セキュリティ対策基準の策定 6
１１．情報セキュリティ個別基準の策定 6
１２．情報セキュリティ実施手順の策定 6

１．目的

当広域連合の情報システムが取り扱う情報には、住民の個人情報や行政運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

このため、当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ことを目的として兵庫県後期高齢者医療広域連合情報セキュリティ基本方針を定める。兵庫県後期高齢者医療広域連合の情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものである。

２．定義

２．１　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。

２．２　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。

２．３　データ

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、光ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

２．４　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。

２．５　情報セキュリティポリシー

兵庫県後期高齢者医療広域連合情報セキュリティ基本方針（以下「情報セキュリティ基本方針」という及び兵庫県後期高齢者医療広域連合情報セキュリティ対策基準（以下「情報セキュリティ対策基準」という）をいう。

２．６　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。

２．７　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。

２．８　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。

２．９　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（社会保障に関する事務）に関わる情報システム及びデータをいう。

２．９．１　標準システム系

マイナンバー利用事務系のうち、後期高齢者医療標準システム（当広域連合で独自開発した機能を含む）及びデータをいう。

２．９．２　国保連合会システム系

マイナンバー利用事務系のうち、兵庫県国民健康保険団体連合会（以下、「国保連合会」という）が管理運営する情報システム及びデータをいう。

２．９．３　中間サーバ系

マイナンバー利用事務系のうち、医療保険者等向け中間サーバ等に接続するための情報システム及びデータをいう。

２．１０　事務処理系

マイナンバー利用事務系以外の情報システム及びデータをいう。

２．１１　通信経路の分離

マイナンバー利用事務系と事務処理系の通信環境を分離する。

当広域連合事務局内では、標準システム系、国保連合会システム系、中間サーバ系の、それぞれの通信環境を分離する。マイナンバー利用事務系と中間サーバ系相互間の通信は、必要最小限の通信のみを許可する。

２．１２　システム利用団体

広域連合の情報システムを利用する兵庫県内の全ての市町をいう。

３．情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは、当広域連合が保有する情報資産に関する情報セキュリティ対策について総合的かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり、情報セキュリティ基本方針及び情報セキュリティ対策基準から構成される。

情報セキュリティ対策基準は、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等を実施するために最低限必要な水準として、職員、再任用職員、任期付職員、臨時的任用職員、会計年度任用職員、特別職非常勤職員、労働者派遣契約等により当広域連合

業務に従事する者（以下「職員等」という。）が遵守すべき事項及び判断基準をまとめたものである。当広域連合では、組織等の状況に合わせた情報セキュリティ対策基準を策定する。

４．対象とする脅威

情報セキュリティ対策を講じるうえでは、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に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、業務委託等の管理の不備、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

５．適用範囲

５．１　組織の範囲

兵庫県後期高齢者医療広域連合事務分掌規則（平成 19 年 2 月 1 日規則第 1 号）第２条に規定する広域連合長の事務局の内部組織、及び、システム利用団体において後期高齢者医療業務を担当する組織とする。

５．２　情報資産の範囲

情報セキュリティ基本方針が対象とする情報資産は次のとおりとする。

(1) ネットワーク及び及び情報システム並びにこれらに関する設備４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

５．３　情報資産の対象

当広域連合が実施する業務で扱う情報資産を当広域連合の情報資産として本基本方針の対象とする。

６．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つとともに、業務の遂行にあたっては情報セキュリティポリシーを遵守しなければならない。

６．１　システム利用団体の情報セキュリティポリシーとの関係

当広域連合の情報セキュリティポリシーとシステム利用団体における情報セキュリティポリシーの規定が異なる場合、当該システム利用団体の職員等が遵守すべき規定は、次のとおりとする。

(1) 当広域連合が定める情報セキュリティポリシーに規定がなく、システム利用団体が定める情報セキュリティポリシーに規定がある事項については、システム利用団体が定める情報セキュリティポリシーを遵守する。

(2) システム利用団体が定める情報セキュリティポリシーに規定がなく、当広域連合が定める情報セキュリティポリシーに規定がある事項については、当広域連合が定める情報セキュリティポリシーを遵守する。

(3) 当広域連合が定める情報セキュリティポリシーの規定と、システム利用団体が定める情報セキュリティポリシーの規定が、異なる場合は、後期高齢者医療制度の業務を行うにあたっては、原則として、当広域連合が定める情報セキュリティポリシーを遵守する。

７．情報セキュリティ対策

上記４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。

７．１　情報セキュリティ管理体制

当広域連合の情報資産について、適切に情報セキュリティ対策を推進・管理するため、事務局長を情報セキュリティ最高責任者とし、その下に全庁的な組織体制を確立する。必要な体制、役割、権限等については情報セキュリティ対策基準にて定める。

７．２　情報セキュリティ管理体制

当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講じる。

７．３　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、情報資産の分類に応じた情報セキュリティ対策を講じるとともに、次の対策も併せて講じる。

(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)事務系においては、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、機密情報の流出を防ぐ。

７．４　物理的セキュリティ

コンピュータ設置場所への入室、サーバ等の管理、通信回線及び端末等への物理的な対策を講じる。

７．５　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、十分な研修・訓練及び啓発を実施するなど人的な対策を講じる。

７．６　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、コンピュータウイルス等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。

７．７　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、業務委託等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、情報セキュリティインシデント発生時の対応手順書を策定する。

７．８　業務委託等及び外部サービス（クラウドサービス）の利用

業務委託等をする場合には、業務委託事業者等を選定し、情報セキュリティ要件を明記した契約を締結し、業務委託事業者等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。

クラウドサービスを利用する場合には、外部サービス（クラウドサービス）利用基準を整備し対策を講じる。

８．情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況を評価するため、定期的及び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。

９．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、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。

１０．情報セキュリティ対策基準の策定

上記７、８及び９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。

１１．情報セキュリティ個別基準の策定

情報セキュリティ対策基準を補完するために必要な内容に関して、具体的な内容を定める情報セキュリティ個別基準を策定するものとする。なお、情報セキュリティ個別基準は、公にすることにより当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。

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及び情報セキュリティ個別基準に基づき、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当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。