富山県後期高齢者医療広域連合

情報セキュリティ基本方針

平成 19 年　4 月　1 日	策定
平成 27 年 12 月 28 日	一部改定
平成 29 年　6 月 30 日	一部改定
平成 30 年 12 月 28 日	一部改定
令和　3 年　3 月　1 日	一部改定
令和　5 年　2 月　28 日	一部改定
令和　7 年 10 月　1 日	一部改定

富山県後期高齢者医療広域連合

目　次

情報セキュリティ基本方針

1. 目的

本基本方針は、富山県後期高齢者医療広域連合（以下、「広域連合」という。）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

（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）広域連合システム

情報システムのうち、厚生労働省から配布される後期高齢者医療広域連合電算処理システムと、広域連合が当該システムに関する業務について委託した事業者に委託して独自に開発したシステムとを合わせた、後期高齢者医療制度を運営するためのシステムの総称をいう。

（4）中間サーバシステム

情報システムのうち、厚生労働省が運営する医療保険者等向け中間サーバ等に接続し、個人番号を利用した情報連携の業務を行うためのシステムのことをいう。

（5）広域連合システム等

情報システムのうち、広域連合システム及び中間サーバシステムのことをいう。

（6）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。

(7)内部事務系システム

情報システムのうち、後期高齢者医療制度を運営するため、個々の被保険者の情報を扱わない一般的事務を行うためのシステムのことをいう。

（8）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。

（9）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。

（10）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。

（11）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。

（12）情報セキュリティ対策基準
本基本方針に定められた事項を遵守するための、具体的な事項及び判断基準等をいう。

（13）情報セキュリティ実施手順
情報セキュリティ対策基準に定められた事項を、広域連合での業務に係る事務に即した形にした、より具体的な事項及びより明確な判断基準等をいう。

（14）情報セキュリティポリシー
本基本方針及び各情報セキュリティ対策基準をいう。

（15）広域連合職員等
広域連合の職員及び非常勤職員のことをいう。

（16）市町村職員等
富山県内市町村（以下、「市町村」という。）で広域連合システムの運用に従事する職員及び非常勤職員のことをいう。

（17）業務委託事業者職員等
広域連合から、情報システムに関する業務を委託された事業者で情報システムの運用等に従事する社員及び非常勤社員のことをいう。

（18）職員等
広域連合職員等、市町村職員等及び業務委託事業者職員等の総称をいう。

3. 適用範囲
（1）団体・事業者の範囲
本基本方針が適用される組織は、広域連合、市町村、国保連合会及び広域連合等が業務委託した事業者（再委託事業者等含む。）など、広域連合に関係する団体・事業者の全ての人とする。

（2）情報資産の範囲
本基本方針が対象とする情報資産は、広域連合で管理する以下のものとする。ただし、広域連合で管理するもののうち、市町村、国保連合会及び広域連合等が業務委託した事業者（以下、「市町村等」と言う。）に管理を委託しているものは別途定めるものとし、本基本方針の対象範囲外とする。
・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
・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。）
・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. 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

5. 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。

(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) マイナンバー利用事務系の強靭性の向上

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、端末への多要素認証の導入等により、住民情報の流出を防ぐ。

(4) 物理的セキュリティ

サーバ、情報システム室、通信回線及び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。

(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、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、緊急時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、利用に係る規定を整

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ポリシーを定め、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。

6. 情報セキュリティ対策基準の策定

職員等が広域連合の情報資産を扱ううえで、前述3、4及び5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「富山県後期高齢者医療広域連合情報セキュリティ対策基準」を策定する。

7. 情報セキュリティ実施手順の策定

職員等が前述６に規定する情報セキュリティ対策基準を広域連合での業務に係る事務に即した形で実施するために、より具体的な手順を定めた「富山県後期高齢者医療広域連合情報セキュリティ実施手順」を策定するものとする。

なお、「富山県後期高齢者医療広域連合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事業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。

8. 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。

9. 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。

10. 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。

以 上