福島県後期高齢者医療広域連合情報セキュリティポリシー

平成１９年７月１日策定

情報セキュリティポリシーの構成

福島県後期高齢者医療広域連合（以下、「本広域連合」という。）情報セキュリティポリシーとは、本広域連合が所有する情報資産に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。本広域連合情報セキュリティポリシーは、本広域連合の情報資産に関する業務に携わる全ての職員、非常勤職員及び臨時職員（以下、「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが求められる。

また、業務の電算化による行政サービスの効率化、インターネット接続環境の整備や電子自治体に向けた取組み等、情報システムへのアクセスの機会が増えており、情報セキュリティ対策は、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応することが必要である。

このようなことから、本広域連合情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層から成るものとして策定することとする。

また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。

福島県後期高齢者医療広域連合情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための、全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
情報セキュリティ実施手順		情報システム毎に定める、情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策手順

情報セキュリティ基本方針

１　目的

本広域連合の各情報システムが取り扱う情報資産には、住民の個人情報を始めとし行政運営上重要な情報など、部外に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う情報システムを人的脅威や災害、事故等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。ひいては、このことが住民からの信頼の維持向上に寄与するものである。

また、電子政府や電子自治体の実現が推進されており、本広域連合がこれらに積極的な対応をするためには、本広域連合の管理するすべての情報システムが高度な安全性を有していなければならない。

そのため、本広域連合の情報資産の機密性、完全性及び可用性を維持するための対策を整備することを目的として、本広域連合情報セキュリティポリシーを定めて、情報セキュリティ対策に取り組むこととする。

このうち情報セキュリティ基本方針は、本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。

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）情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。また、情報の重要性に照らし、紙文書等の情報も

含む。

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）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、無許可ソフトウェ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

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、本広域連合及び構成市町村とする。

（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。

ア　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

イ　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。）

ウ　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

エ　個人情報に関連する庶務一般文書

なお、構成市町村における適用範囲及び対象とする情報資産は別に定める。

5　職員等の遵守義務

本広域連合が管理する情報資産に関する業務に携わる職員等は、情報セキュリティポリシー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

本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組織体制を確立する。

（2）情報資産の分類と管理

本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。

（4）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。

（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。

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

本広域連合の情報資産について、上記６、７及び８に規定する情報セキュリティ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。

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を遵守し情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準に基づき、情報資産の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本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。