

茨城県後期高齢者医療広域連合 情報セキュリティポリシー【基本方針】

茨城県後期高齢者医療広域連合

制定：平成 19 年 10 月

改定：令和 7 年 11 月

目 次

情報セキュリティ基本方針

1	目的	1
2	情報セキュリティポリシーの構成	1
	(1) 情報セキュリティ基本方針	
	(2) 情報セキュリティ対策基準	
	(3) 情報セキュリティ実施手順	
3	定義	2
	(1) コンピュータ	
	(2) 電磁的記録媒体	
	(3) ネットワーク	
	(4) 情報システム	
	(5) 情報セキュリティ	
	(6) 情報セキュリティポリシー	
	(7) マイナンバー利用事務系（個人番号利用事務系）	
	(8) LGWAN 接続系	
	(9) インターネット接続系	
	(10) 通信経路の分割	
	(11) 無害化通信	
	(12) 職員等	
	(13) 行政情報	
	(14) 情報資産	
4	対象とする脅威	3
5	適用範囲	3
	(1) 行政機関の範囲	
	(2) 情報資産の範囲	
6	職員等の遵守義務	4
7	情報セキュリティ対策	4
	(1) 組織体制	
	(2) 情報資産の分類と管理	
	(3) 情報システム全体の強靱性の向上	

(4)	物理的セキュリティ	
(5)	人的セキュリティ	
(6)	技術的セキュリティ	
(7)	運用	
(8)	業務委託と外部サービス（クラウドサービス）の利用	
(9)	評価・見直し	
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	5
11	情報セキュリティ実施手順の策定	6
12	市町村等の対応	6

情報セキュリティ基本方針

1 目的

茨城県後期高齢者医療広域連合（以下「広域連合」という。）の情報システムが取り扱う情報には、被保険者等の個人情報及び業務運営上の重要な情報が多数含まれている。広域連合が保有する情報資産を、人的脅威、災害及び事故等の様々な脅威から防御することにより、被保険者等の個人情報及びプライバシー等を保護することになる。また、広域連合が、継続的に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。

この情報セキュリティ基本方針は、上記のことを踏まえ、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総合的、体系的な基本方針を定めることを目的として制定するものである。

2 情報セキュリティポリシーの構成

広域連合の情報セキュリティ対策については、下図に示す階層構造から成り立つものである。それぞれの概要については以下のとおりであり、このうち「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」の2つを、「情報セキュリティポリシー」と総称するものである。

(1) 情報セキュリティ基本方針

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である。

(2) 情報セキュリティ対策基準

情報セキュリティ基本方針に基づき、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ものである。

(3) 情報セキュリティ実施手順

情報セキュリティ対策を確実に実施していくため、情報セキュリティ対策基準に基づき、情報システム又は業務における具体的な対策の手順及び手続を定めるものである。

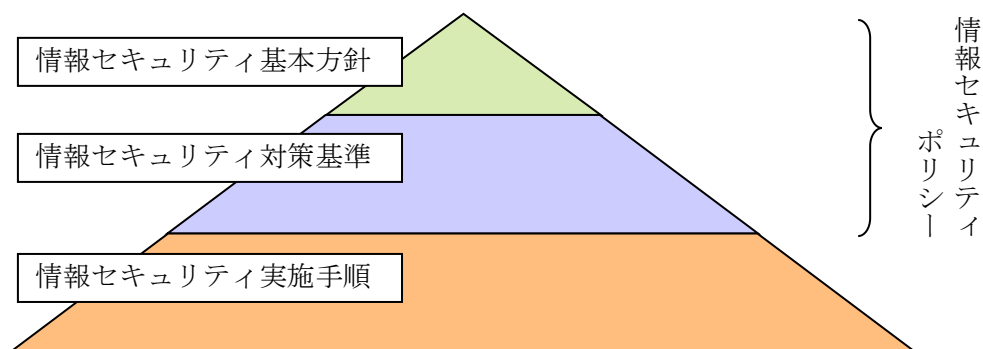


図 情報セキュリティポリシーに関する体系図

3 定義

(1) コンピュータ

ハードウェア及びソフトウェアで構成する電子計算機、周辺機器及び記録媒体等で構成する集合体をいう。

(2) 電磁的記録媒体

コンピュータで使用されるハードディスク、CD-ROM、USB メモリ、その他これらに類する電子情報を記録するための記録媒体をいう。

(3) 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（ソフトウェアを含む。）をいう。

(4) 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た情報処理を行う仕組みをいう。

(5) 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。

ア 機密性 (confidentiality)

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。

イ 完全性 (integrity)

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。

ウ 可用性 (availability)

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。

(6) 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。

(7) 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。

(8) LGWAN 接続系

LGWAN 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（マイナンバー利用事務系を除く。）。

(9) 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。

(10) 通信経路の分割

LGWAN 接続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。

(11) 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。

(12) 職員等

広域連合に常勤する職員及び会計年度任用職員をいう。

(13) 行政情報

広域連合の行政事務の執行に係わる情報で、かつ、情報システムで取り扱うものをいう。

(14) 情報資産

情報システム及び行政情報をいう。

4 対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃又は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、操作ミス・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の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

(1) 行政機関の範囲

本基本方針が適用される機関は、広域連合事務局、議会事務局、監査委員事務局、選挙管理委員会及び公平委員会等とする。

(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

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に関する法令等を遵守しなければならない。

7 情報セキュリティ対策

情報資産に対する上記4の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じるものとする。

(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体制を確立する。

(2) 情報資産の分類と管理

広域連合の情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 情報システム全体の強靱性の向上

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、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

各市町村及び広域連合のサーバ、通信回線、並びに職員のパソコン等の管理について、物理的対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、職員等に情報セキュリティポリシー等を周知徹底する等、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

コンピュータ等の情報資産の管理、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正に対応するための措置を講じる。

(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手順を定め、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。

(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、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。

8 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシー遵守状況を検証するため、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となった場合には、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6、7及び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。

なお、情報セキュリティ対策基準は、公開することにより広域連合の運営に重大かつ深刻な支障を及ぼすおそれがあるため、非公開とする。

11 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の実施における具体的な手順を定めるため、情報セキュリティ実施手順を策定する。

なお、情報セキュリティ実施手順は、公開することにより広域連合の運営に重大かつ深刻な支障を及ぼすおそれがあるため、非公開とする。

12 市町村等の対応

広域連合を構成する市町村等において、後期高齢者医療の事務を行う場合、各自で定めている情報セキュリティポリシーに基づき、適切に対応するものとする。