

# 青森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 6 月 28 日 策定

令和 8 年 6 月 29 日 一部改正

青森県後期高齢者医療広域連合

## 目 次

### 第1章 情報セキュリティ基本方針

|    |                             |   |
|----|-----------------------------|---|
| 1  | 目的・・・・・・・・・・・・・・・・・・・・・・・・  | 1 |
| 2  | 定義・・・・・・・・・・・・・・・・・・・・・・・・  | 1 |
| 3  | 対象とする脅威・・・・・・・・・・・・・・・・     | 2 |
| 4  | 適用範囲・・・・・・・・・・・・・・・・・・・・    | 3 |
| 5  | 職員等の遵守義務・・・・・・・・・・・・        | 3 |
| 6  | 情報セキュリティ対策・・・・・・・・・・・・      | 3 |
| 7  | 情報セキュリティ監査及び自己点検の実施・・・・・・・・ | 4 |
| 8  | 情報セキュリティポリシーの見直し・・・・・・・・    | 5 |
| 9  | 情報セキュリティ対策基準の策定・・・・・・・・     | 5 |
| 10 | 情報セキュリティ実施手順の策定・・・・・・・・     | 5 |
| 11 | 情報セキュリティポリシーの公開・・・・・・・・     | 5 |

## 第1章 情報セキュリティ基本方針

### 1 目的

本基本方針は、青森県後期高齢者医療広域連合（以下「本広域連合」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、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

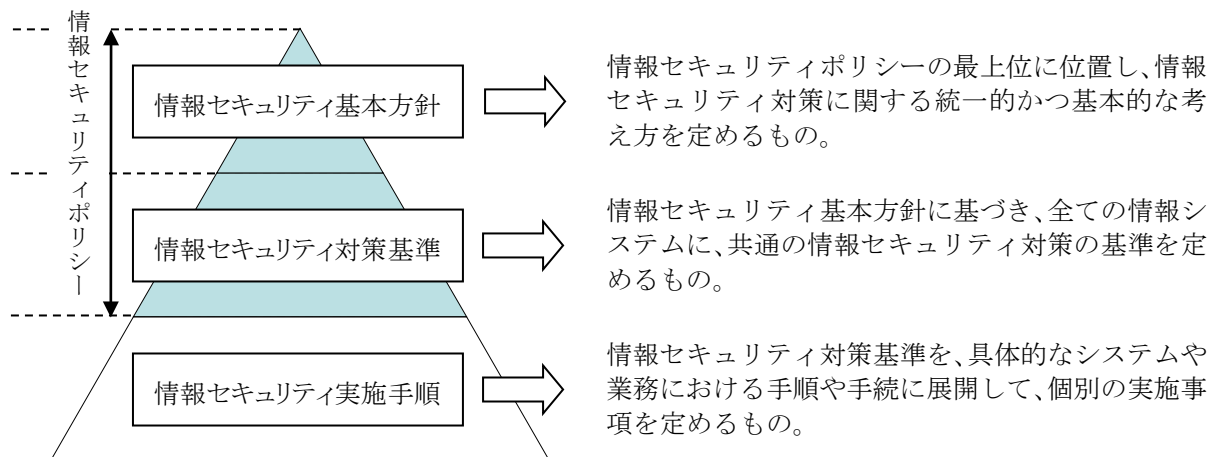
コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

#### （3）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

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) 個人情報

氏名、住所、生年月日、性別等の個人を特定できる情報または他の情報と組合せて個人を特定できる情報を含む情報及び特定個人情報をいう。特定個人情報とは、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報を指す。なお、法令の定める業務範囲の手続きにおいて、個人番号の記入欄のある様式を用いて得られた情報については、様式に個人情報の記入がない個人情報も特定個人情報と同様に取り扱う。

(9) 情報資産

ネットワークおよ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い、情報システムで取り扱う電子情報だけでなく、情報システムへ入力する前の紙媒体の情報や、職員の履歴書等全ての個人情報を含む。

(10) 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、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(11) 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。

### 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) 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

## 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、本広域連合事務局、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

## 5 職員等の遵守義務

職員、非常勤職員及び会計年度任用職員（以下「職員等」という。）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。

## 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) 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、次の二段階の対策を講じる。

- 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

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。

#### (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正に対応するため、緊急時対応マニュアルを策定する。

#### (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、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。

### 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となった場合には、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。

## 9 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。

## 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。

## 11 情報セキュリティポリシーの公開

情報セキュリティポリシーには、公開することにより本広域連合の運営に重大な支障を及ぼすおそれがある内容が含まれることから、本基本方針のみ公開するものとし、情報セキュリティ対策基準及び情報セキュリティ実施手順については、公開しないものとする。