

島根県後期高齢者医療広域連合情報セキュリティ基本方針

(目的)

第1条 島根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「基本方針」という。)は、島根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。

(定義)

第2条 この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ並びにその周辺機器をいう。

(2) 電磁的記録媒体等

磁気ディスク、磁気テープ、光ディスク、USBメモリ等の電子データを記録することができる媒体及びこれに係る入出力帳票をいう。

(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(ハードウェア及びソフトウェア)をいう。

(4) 情報システム

電子計算機、電磁的記録媒体等及びネットワークで構成され、情報処理を行う仕組みをいう。

(5) 情報

職務の遂行に伴って情報システムに記録されたデータをいう。

(6) 情報資産

情報システム及び情報をいう。

(7) 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。

(8) 情報セキュリティポリシー

本基本方針及び第10条に規定する情報セキュリティ対策基準をいう。

(9) 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。

(10) 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。

(11) 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。

(12) 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。

(13) 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。

(14) 情報セキュリティインシデント

情報セキュリティに関する障害・事故及びシステム上の欠陥をいう。

（対象とする脅威）

第 3 条 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) 情報資産の無断持出し、無許可ソフトウェアの使用等の規程違反、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
（適用範囲）

第 4 条 本基本方針が適用される機関は、広域連合事務局、選挙管理委員会、監査委員及び議会とする。

2 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等
- (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
（職員の遵守義務等）

第 5 条 特別職及び臨時職員等を含むすべての職員（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つとともに、業務の遂行に当たっては、情報セキュリティ対策に関する法令及び情報セキュリティポリシー、情報セキュリティ実施手順を遵守しなければならない。

（情報セキュリティ対策）

第 6 条 情報資産を脅威から保護するために、次の各号に定める情報セキュリティ対策を講ずるものとする。

(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、情報システム室、通信回線、職員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、職員等及び委託業者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、緊急時対応計画を策定する。

(8) 業務委託と外部サービスの利用

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、情報セキュリティポリシーの見直しを行う。

(情報セキュリティ対策基準の策定)

第 7 条 本基本方針に基づき、広域連合における情報セキュリティ対策の統一基準となる具体的な遵守事項、判断基準等を定める情報セキュリティ対策基準(以下「対策基準」という。)を策定する。

(情報セキュリティ実施手順の策定)

第 8 条 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法及び手順を定めた情報セキュリティ実施手順(以下「実施手順」という。)を策定する。

(対策基準及び実施手順の取扱い)

第 9 条 対策基準及び実施手順の取扱いは、公にすることにより広域連合の情報セキュリティの確保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。

(義務違反者に対する措置)

第 10 条 情報セキュリティポリシーに違反した職員等は、地方公務員法(昭和 25 年法律第 261 号)等により懲戒処分の対象となる場合がある。

附 則

この基本方針は、平成 27 年 10 月 5 日から施行する。

この基本方針は、令和 4 年 4 月 1 日から施行する。

この基本方針は、令和 6 年 4 月 1 日から施行する。