

秋田県後期高齢者医療広域連合情報セキュリティ基本方針

令和 8 年 3 月 1 6 日 策定

1 目的

本基本方針は、秋田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。

なお、本基本方針は、地方自治法（昭和 22 年法律第 67 号）第 244 条の 6 第 1 項に定めるサイバーセキュリティを確保するための方針に位置付けるものである。

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

情報資産の機密性及び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) 標準システム系

秋田県後期高齢者医療広域連合電算処理システムに関わる情報システム及びデータをいう。

(9) 内部情報系

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、ウィルス攻撃、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、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、通信、水道等の基幹インフラにおける供給途絶、その他障害からの波及による影響等

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、本広域連合の長、議会、選挙管理委員会及び監査委員とする。

(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
- イ ネットワーク及び情報システムで取り扱う電子情報（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

(3) 職員等の範囲

本基本方針が適用される職員等は、行政機関の事務部局において常時勤務する一般職の職員、臨時的任用職員及び会計年度任用職員並びにそれらに準じて情報資産を取り扱う特別職とする。

5 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。

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全庁的な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。

ア 標準システム系においては、原則として、他の領域との通信をできないようにしたうえで、端末からの情報持ち出し不可設定や端末への生体認証の導入等により、被保険者情報の流出を防ぐ。

イ 内部情報系においては、不正な挙動の監視機能強化等、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、通信回線及び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及び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に関する必要な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（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、その結果に基づき運用改善を行い情報セキュリティの向上を図る。また、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になった場合には、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、本広域連合の長が所管する情報資産について、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、専ら議会、選挙管理委員会及び監査委員の所管に属する情報資産で、本広域連合の長が整備するネットワークと論理的又は物理的に分離されている情報資産については、当該情報資産を所管する行政機関が必要に応じて個別に情報セキュリティ対策基準を策定するものとする。

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、必要に応じて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 情報セキュリティ対策基準及び実施手順の秘匿

情報セキュリティ対策基準及び実施手順は、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。