

安芸地区衛生施設管理組合
情報セキュリティポリシー
(基本方針)

令和8年3月

1 目的

本情報セキュリティポリシーは、安芸地区衛生施設管理組合（以下「本組合」という。）が所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、本組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

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) 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（リスク管理等）の欠陥、機器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) 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、本組合とする。

(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対策基準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、以下の対策を講じる。

(1) 組織体制

本組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

本組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、当該分類に基づき管理する。

(3) 情報システム全体の強靱性の向上

インターネット接続系（各業務システムを含む。）においては、高度な不正通信の監視機能の強化等を実施する。

(4) 物理的セキュリティ

サーバ、OA室、通信回線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、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、緊急時対応体制を構築する。

(8) 業務委託と外部サービスの利用

情報システムに関する業務委託を行う場合には、委託事業者と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。

利用可能な外部サービスは、原則、業務等に関連して必要となる次のサービスのみとする。その他のサービスを利用する場合には、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づき、利用に係る規定を整備し対策を講じる。ただし、総務省所管の『自治体の行政手続きのオンライン化』に関連するサービスについては、この限りではない。

- ① オンライン研修（講習）会で指定される Zoom 又は業務説明会で使用される Webex 等のウェブ（ビデオ）会議サービス及びこれに関連して必要となるオンライン手続き
- ② 指定金融機関（収納代理金融機関を含む。）のデータ伝送サービス及び取引用回線接続サービス
- ③ 例規及び法制等データベース検索・支援システム等の自治体法務サービス
- ④ インターネット回線接続サービス
- ⑤ メール運用・管理に係るホスティングサービス

なお、上記①から⑤に掲げるような民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、セキュリティ対策やデータの取扱いなどについて本組合への特別な扱いを求めることができない場合が多く、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできない。

(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、適宜運用改善を行い、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又は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、情報システムへの脅威等を精査し、リスクを検討した上で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および自己点検の実施

情報セキュリティポリシー遵守状況を検証するため、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 情報セキュリティ対策基準の策定

上記6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。