

西秋川衛生組合情報セキュリティ基本方針

令和8年3月

西秋川衛生組合

(目次)

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

1 目的

本基本方針は、当組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、当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考え方を定めることを目的とする。

2 定義

(1) 情報

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。）、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をいう。

(2) 情報資産

情報及び情報システムをいう。

(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

コンピュータ、ネットワーク及び記録媒体で構成され、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。

(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) 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。

(8) 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。

(9) 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。

(10) インターネット接続系

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。

(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。

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・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波及等

4 適用範囲

(1) 情報資産の範囲

本基本方針が対象とする情報資産は、当組合が保有する次の情報資産とする。

- 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

(2) 対象者の範囲

本基本方針の対象者の範囲は、任用形態又は勤務形態にかかわらず、当組合が保有する情報資産を取り扱う全ての職員とする。

当組合の情報資産に係る業務を外部に委託する場合は、当該業務の受託者に対しても本ポリシーを遵守させるための措置を講ずるものとする。

5 職員等の遵守義務

職員は、情報セキュリティの重要性について共通認識を持ち、業務の遂行に当たり、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

情報資産を脅威から保護するために、以下の情報セキュリティ対策を講ずる。

(1) 組織体制

当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組織体制を確立する。

(2) 情報資産の分類と管理

当組合の保有する情報資産をその重要性に応じて分類し、適切な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、必要に応じて対策を講ずる。

(4) 物理的セキュリティ対策

情報システムの設置場所への不正な立入りの防止等、情報資産を保護するために物理的な対策を講ずる。

(5) 人的セキュリティ対策

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、教育及び啓発

を行う等の人的な対策を講ずる。

(6) 技術的セキュリティ対策

情報資産を不正アクセス等から保護するために、情報資産へのアクセス制御やネットワーク管理等の技術的対策を講ずる。

(7) 運用面における情報セキュリティ対策

情報システム監視、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情報セキュリティの確保等、情報セキュリティポリシーの運用面の対策を講ずるものとする。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）の利用における情報セキュリティ対策

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ずる。

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ずる。

(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

情報セキュリティ対策基準を実施するために、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、原則として非公開とする。

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、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。なお、情報セキュリティ実施手順についても原則として非公開とする。