

中遠広域事務組合情報セキュリティポリシー

第1版

令和8年3月

中遠広域事務組合

< 改 版 履 歴 >

版 数	作成年月日	作成改訂理由
第 1 版	令和 8 年 3 月 31 日	新規制定

序章 はじめに.....	- 3 -
1 序文.....	- 3 -
2 定義.....	- 4 -
第1章 情報セキュリティ基本方針.....	- 6 -
1 目的.....	- 6 -
2 適用範囲.....	- 6 -
3 対象とする脅威.....	- 6 -
4 職員等の遵守義務.....	- 6 -
5 情報セキュリティ対策.....	- 6 -
6 情報セキュリティ監査及び自己点検の実施.....	- 7 -
7 情報セキュリティポリシーの見直し.....	- 7 -

序章 はじめに

1 序文

中遠広域事務組合情報セキュリティポリシーとは、中遠広域事務組合（以下「本組合」という。）が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。

情報セキュリティポリシーは、本組合が所掌する情報資産に関する業務に携わる全ての職員に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

情報セキュリティインシデントが多発する現状や、標準準拠システム等のクラウドサービス利用に対応した情報セキュリティ対策、外部委託先管理の運用面に関するセキュリティ対策、昨今のサイバー攻撃の情報セキュリティ対策に対応するために、情報セキュリティポリシーを新規制定した。

表 1 中遠広域事務組合情報セキュリティポリシーの構成

文 書 名	内 容
情報セキュリティポリシー	情報セキュリティ基本方針
情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針

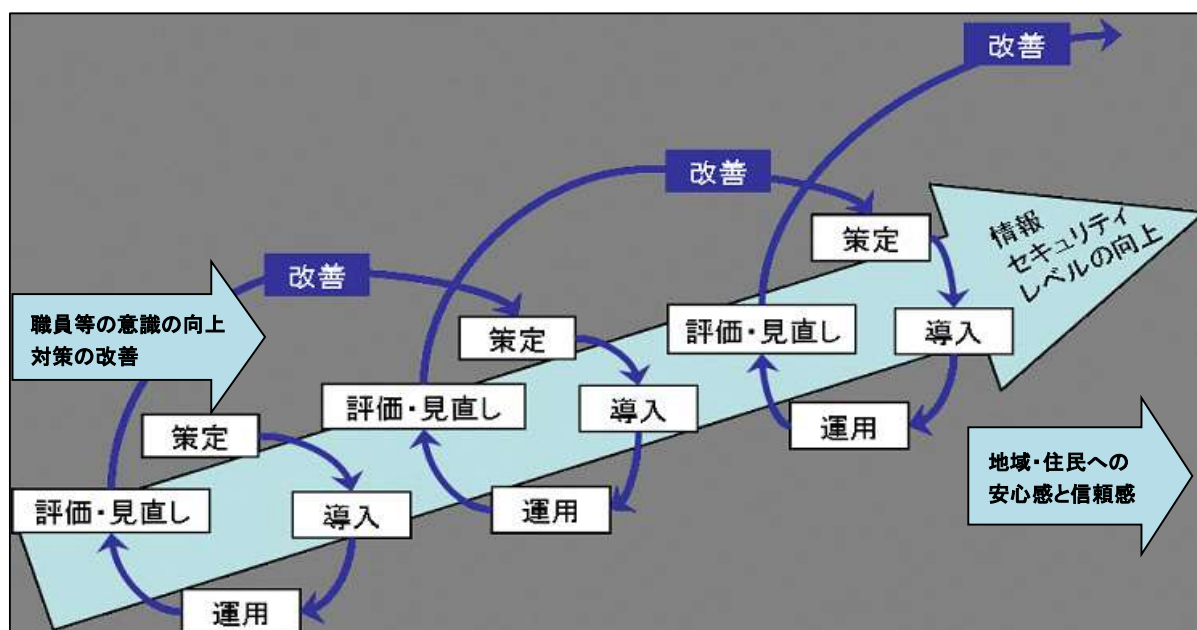


図 1 情報セキュリティレベルの向上とマネジメントサイクル

2 定義

(1) 行政情報

行政事務の執行にかかわる情報をいう。

(2) 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。

(3) パソコン等

データの入出力などの操作を行う装置のことをいう。

(4) 記録媒体

ハードディスク、USBメモリ、CD-R、DVD-Rなど情報を記憶するための媒体(メディア)をいう。

(5) 情報システム

コンピュータ、ソフトウェア、ネットワーク及び記録媒体で構成され、行政情報を処理するための仕組みをいう。

(6) 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。

(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) 不正プログラム(マルウェア)

コンピュータを不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なプログラムの総称で、コンピュータウイルス、スパイウェア、トロイの木馬などをいう。

(11) 職員等

本組合の情報資産に接する正規職員、会計年度任用職員及び非常勤職員をいう。

(12) モバイル端末

スマートフォンやタブレット型端末など、持ち運びが可能な携帯情報機器のことをいう。

(13) ソーシャルメディア

インターネットを利用してユーザが情報を発信し、あるいは相互に情報をやり取りする情報の伝達手段のことをいう。

(14) ISMS適合性評価制度

情報セキュリティマネジメントシステム適合性評価制度のことをいう。

(15) ITSMS適合性評価制度

ITサービスマネジメントシステム適合性評価制度のことをいう。

(16) プライバシーマーク制度

個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、プライバシーマークを付与し、その使用を認める制度のことをいう。

(17) 事務局

中遠広域事務組合事務局のことをいう。

(18) 情報セキュリティインシデント

ウイルス感染、不正アクセス、USBメモリなど記録媒体の紛失等、事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故及びセキュリティ上好ましくない事象・事態のことをいう。

(19) LGWAN接続系

庶務事務、財務会計及び文書管理等LGWAN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。

(20) インターネット接続系

ホームページ閲覧、ASPサービス利用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。

(21) 外部サービス

事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。クラウドサービス、Web会議サービス、ソーシャルメディア、オンラインストレージサービス、検索サービス、翻訳サービス、地図サービス、ホスティングサービス等をいう。

第1章 情報セキュリティ基本方針

1 目的

情報セキュリティ基本方針は、地方自治法（昭和22年法律第67号）第244条の6第1項の規定に基づき、本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、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 適用範囲

情報セキュリティ基本方針は、本組合の全ての情報資産を適用範囲とする。

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) 情報資産の無断持出、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因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 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を遵守する。

5 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 LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

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。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

情報システム、通信回線及び職員等のパソコン等の管理等について、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な対策を講じる。

(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。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

6 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。

7 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や情報セキュリティに関する状況の変化により、新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行う。