

# 情報セキュリティ基本方針

中播衛生施設事務組合

令和8年3月 策定

# 中播衛生施設事務組合 情報セキュリティ基本方針

## 第1条（目的）

本基本方針は、中播衛生施設事務組合（以下「本組合」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確保し、し尿処理施設の安定運転、住民の生活環境保全及び本組合に対する信頼を維持するため、情報セキュリティ対策の基本事項を定めることを目的とする。

併せて、個人情報保護法及び関係条例を遵守し、適切な情報管理を行うことを基本とする。

## 第2条（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及び構成機器をいう。
- 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、情報セキュリティ対策基準及び実施手順をいう。
- 5 機密性：認められた者のみが情報にアクセスできる状態を確保すること。
- 6 完全性：情報及び処理方法が正確かつ完全であり、破壊・改ざん・消去されていない状態を確保すること。
- 7 可用性：認められた者が必要ときに中断なく情報にアクセスできる状態を確保すること。
- 8 マイナンバー利用事務系：個人番号利用事務に関わる情報システム及びデータをいう。
- 9 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情報システム及びデータをいう。
- 10 無害化通信：インターネットメール本文のテキスト化や画面転送等により、安全が確保された通信をいう。
- 11 情報セキュリティインシデント：情報資産の漏えい、滅失、き損、不正利用、サービス停止等、情報セキュリティに影響を及ぼす事象をいう。

## 第3条（対象とする脅威）

本組合は、リスク分析に基づき、情報資産に対する以下の脅威を想定し、必要な対策を講じる。

- 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及び内部不正
- 2 情報資産の無断持出し、無許可ソフト使用、委託管理の不備、機器故障等の非意図的要因
- 3 地震、落雷、火災等の災害による業務停止
- 4 大規模疾病等による要員不足
- 5 電力・通信・水道等インフラ障害
- 6 し尿処理施設の設備停止や処理機能低下に伴う衛生上の影響及び住民生活への支障

## 第4条（適用範囲）

- 1 本組合及び本組合が管理する施設に適用する。
- 2 本組合の職員（常勤・非常勤・会計年度任用職員等）及び業務に従事する委託業者に適用する。
- 3 対象となる情報資産は、ネットワーク、情報システム、関連設備、電磁的記録媒体及びシステム関連文書とする。

## 第5条（職員等の遵守義務）

職員等は、情報セキュリティの重要性を認識し、本ポリシー及び関連する基準・手順を遵守しなければならない。

## 第6条（情報セキュリティ対策）

### 1 組織体制

情報セキュリティ責任者を置き、必要に応じて情報セキュリティ委員会を設置する。小規模組織であることを踏まえ、実効性を重視した体制とする。

### 2 情報資産の分類と管理

情報資産台帳を整備し、重要度に応じた適切な管理を行う。特に、施設運転に関わる情報は可用性確保を最優先とする。

### 3 情報システム強靱化

- (1) マイナンバー利用事務系は他領域と分離し、国のガイドラインに基づく多要素認証、持出し制限等の対策を講じる。
- (2) インターネット接続系は不正通信監視機能を強化し、必要に応じて無害化通信を導入する。
- (3) 無線 LAN を利用する場合は、クライアント証明書による認証等、ガイドラインが求める強固な認証方式を採用する。

### 4 物理的セキュリティ

施設、端末及び媒体の入退室管理、施錠管理及び適切な保管を徹底する。特に、し尿処理施設の運転設備に関わる情報機器については、誤操作や不正利用を防止するための管理を行う。

### 5 人的セキュリティ

職員に対し、情報セキュリティに関する教育・研修・啓発を定期的実施する。委託契約には情報セキュリティ条項を明記し、委託先の遵守状況を確認する。

### 6 技術的セキュリティ

アクセス制御、ウイルス対策、不正アクセス防止、暗号化等の技術的対策を実施する。ログ（アクセスログ、操作ログ等）を適切に取得・保管し、必要に応じて監視する。小規模組織であることを踏まえ、外部専門機関のサービスも適宜活用する。

### 7 運用管理

監視、遵守状況の確認、委託時のセキュリティ確保を行う。情報セキュリティインシデントが発生した場合は、速やかに報告・連絡・初動対応を行う体制を整備する。緊急時対応計画及び事業継続計画（BCP）を策定し、施設運転に支障が生じた場合の対応手順を明確にする。

### 8 業務委託・外部サービス利用

契約にセキュリティ要件を明記し、クラウドサービス等を利用する場合は、データ所在、暗号化、可用性、委託先の管理体制等を含む安全性評価を行う。必要に応じてソーシャルメディア運用規定を整備する。

### 9 評価・改善

監査及び自己点検を定期的実施し、PDCA サイクルにより継続的に改善する。

#### 第7条（情報セキュリティ監査及び自己点検）

本組合は、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。小規模組織であることを踏まえ、外部監査や専門家の助言を活用することができる。

#### 第8条（情報セキュリティポリシーの見直し）

監査結果、技術動向、法令改正及び環境変化に応じてリスク分析を行い、必要に応じて本ポリシーを見直す。

#### 第9条（情報セキュリティ対策基準の策定）

本基本方針に基づき、遵守事項及び判断基準を定めた情報セキュリティ対策基準を策定する。

#### 第10条（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、具体的な実施手順を策定する。なお、行政運営に重大な支障を及ぼすおそれがあるため、実施手順は非公開とする。