

坂戸、鶴ヶ島下水道組合監査委員  
情報セキュリティポリシー  
(情報セキュリティ基本方針)

令和8年5月策定  
坂戸、鶴ヶ島下水道組合

# 目次

1	目的	1
2	定義	1
3	対象とする脅威	2
4	適用範囲	2
5	監査委員の遵守義務	2
6	情報セキュリティ対策	3
7	監査委員セキュリティ自己点検の実施	3
8	監査委員セキュリティ基本方針の見直し	3

## 1 目的

本基本方針は、坂戸、鶴ヶ島下水道組合監査委員（以下「監査委員」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、監査委員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) 情報セキュリティ

情報資産を脅威（自然災害、機器障害、悪意のある行為等の損失を発生させる直接の要因をいう。）から保護し、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。

### (2) 情報資産

情報システム及び情報通信ネットワークで取り扱う情報並びに情報システム及び情報通信ネットワークに関する設備又はその仕様書等の関連文書のことをいう。

### (3) 情報システム

コンピュータ、ソフトウェア及び電磁的記録媒体で構成された情報処理を行う仕組みのことをいう。

### (4) 情報通信ネットワーク

コンピュータを通信回線、ルータ等の通信装置で接続し、情報を伝達するための仕組みのことをいう。

### (5) 電磁的記録媒体

電子的方式、磁氣的方式その他の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものに係る記録媒体のことをいう。

### (6) 機密性

情報に接続することを認められた者だけが、情報に接続できる状態を確保することをいう。

### (7) 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。

### (8) 可用性

情報に接続することが認められた者が、必要なときに中断されることなく、情報に接続できる状態を確保することをいう。

### (9) 基幹系LAN

インターネットから隔離された財務会計システム等で取り扱うデータが使用する情報通信ネットワークのことをいう。

### (10) インターネット系LAN

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等で取り扱うデータが使用する情報通信ネットワークのことをいう。

### (11) 通信経路の分割

基幹系LAN及びインターネット系LANのそれぞれの情報通信ネットワークを分離したうえで、安全が確保された通信だけを許可できるようにすることをいう。

#### (12) 無害化通信

インターネットメール本文のテキスト化等により、コンピュータウイルス等の不正プログラムの付着を防止するなどの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、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員不足に伴うシステム運用の機能不全等
- (5) 電力供給、通信、水道供給等の途絶等のインフラ障害からの波及等

### 4 適用範囲

#### (1) 適用機関の範囲

本基本方針が適用される機関は、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。

ただし、管理者が監査事務に従事する組合職員の使用に供する情報資産については、その取扱いは坂戸、鶴ヶ島下水道組合情報セキュリティポリシーに従うものとし、基本方針の適用範囲外とする。

- ① 情報システム及び情報通信ネットワーク並びにこれらに関する設備及び電磁的記録媒体
- ② 情報システム及び情報通信ネットワークで取り扱う情報（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情報通信ネットワーク図等のシステム関連文書

### 5 監査委員の遵守義務

監査委員は、情報セキュリティの重要性について共通の認識を持ち、活動及び業務の遂行に当たって関係法令及び情報セキュリティ基本方針を遵守する義務を負うものとする。

## 6 情報セキュリティ対策

対象とする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

監査委員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、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。

### (3) 物理的セキュリティ

情報システムを設置する施設の管理について、物理的な対策を講じる。

### (4) 人的セキュリティ

情報セキュリティに関し、監査委員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。

### (5) 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。

### (6) 運用

情報システムの監視、基本方針の遵守状況の確認、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、危機管理対策を講じるよう努める。

### (7) 外部サービスの利用

- ① 外部委託する場合には、外部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、外部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。
- ② 約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

## 7 情報セキュリティ自己点検の実施

基本方針の遵守状況を検証するため、必要に応じて情報セキュリティ自己点検を実施、運用改善を行い、情報セキュリティの向上を図る。

## 8 情報セキュリティ基本方針の見直し

情報セキュリティ自己点検の結果、基本方針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、基本方針を見直す。