坂戸、鶴ヶ島下水道組合
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６年１月策定

令和８年３月最終改正

坂戸、鶴ヶ島下水道組合

目次

1　目 的

本基本方針は、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　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、磁気的方式その他人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絶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、本組合の情報資産（議会事務及び監査事務として取り扱う情報資産を含む。以下同じ。）を取り扱う全ての職員（管理者、副管理者、定年前再任用短時間勤務職員、会計年度任用職員等を含む。以下同じ）に適用~~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 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　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

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

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靭性の向上

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、次の対策を講じる。

① 基幹系ＬＡＮ

原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、機密情報の流出を防止する。

② インターネット系ＬＡＮ

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。

（4）物理的セキュリティ

サーバ室、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、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、緊急時対応計画を策定する。

（8）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。

③ ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用する

④ ソーシャルメディアサービスごとの責任者を定める。

7　情報セキュリティ自己点検の実施

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　情報セキュリティポリシーの見直し

情報セキュリティ自己点検の結果、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応するため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。

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、情報セキュリティ自己点検及び必要に応じて情報セキュリティポリシーの見直しを実施するために、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、公にすることにより組合の運営に重大な支障を及ぼすおそれがあることから非公開とする。

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は、公にすることにより本組合の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。