松江市上下水道局
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３月　初版

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. 職員の遵守義務 3
6. 情報セキュリティ対策 3
7. 情報セキュリティ監査及び自己点検の実施 4
8. 情報セキュリティポリシーの見直し 4
9. 情報セキュリティ対策基準の策定 4
10. 情報セキュリティ実施手順の策定 4

1.　目的

本基本方針は、松江市上下水道事業（以下「上下水道事業」という。）における松江市上下水道局（以下「本局」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、本局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により、情報資産を適切に管理し、上下水道事業の円滑な業務運営に資することを目的とする。

なお、水道事業は国民にとっての重要インフラとして定義されており、水道事業者は、サイバーセキュリティ基本法が規定する重要インフラ事業者（重要社会基盤事業者）として、「任務保証の考え方」を踏まえ、水道事業における重要インフラサービスの継続性を維持するため、サイバーセキュリティ確保に取り組むことが重要であると定義されている。

2.　定義

(1)　情報資産

上下水道事業の運営、施設の運用及び保守に係わる全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

(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)　情報システム

コンピュータ、ネットワークおよび記録媒体で構成され、情報処理を行う仕組みをいう。

(4)　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。

(5)　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。なお、報セキュリティ対策基準は非公開。

(6)　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。

(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。

(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。

(10)　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）等に関わる情報システム

及びデータをいう。

(11)　ソーシャルメディア

インターネットを利用して誰でも手軽に情報を発信し、相互のやりとりができる双方向のメディア。ソーシャルメディアには、SNS（Social Networking Service）、電子掲示板、ブログ、投稿サイトなどの様々なものが含まれる。

(12)　業務委託

本局の業務の一部又は全部（情報システムの運用に関する業務を含む。）について、契約をもって外部の者に実施させることをいう。

(13)　IT（Information Technology）

情報技術。コンピュータやネットワークを利用して、「データや情報の処理・管理・伝達を行うための技術」のこと。「顧客管理システム」。「請求システム」及び業務用のシステム等がこれにあたる。

(14)　OT（Operation Technology）

工場やインフラなどの現場において、「物理的な装置やプロセスを制御・運用するための技術」のこと。「浄水場の監視制御システム」、「ポンプ場の運転システム」及び「排水処理システム」等がこれにあたる。

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の波及等

4.　適用範囲

本情報セキュリティポリシーが適用される範囲は、本局が保有する情報資産並びに情報資産を取り扱う全職員及び外部委託者に適用し、情報資産の範囲は、次のとおりとする。

(1)　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
（IT 領域のみならず OT 領域を含む）

(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

5.　職員の遵守義務

正規職員、任期付任用職員、再任用職員及び会計年度任用職員等の松江市上下水道局職員（以下「職員等」という。）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と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

上記「3.対象とする脅威」から情報資産を保護するために、次の情報セキュリティ対策を講ずる。

(1)　組織体制

本局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

本局の保有する情報資産を機密性、完全性、可用性及びそれに応じて重要性を分類し、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

インターネット接続系において、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

サーバー等、通信回線等、職員のパソコン等の管理について、物理的な対策を講ずる。

(5)　人的セキュリティ

情報セキュリティに関し、職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ずる。

(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ずる。

(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ずるものとする。また、情報資産に対するインシデント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の利用

①　業務委託

業務委託する場合には、ISMS の取得状況等を確認したうえで適切な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じる。

② 外部サービスの利用

一般的な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 クラウドサービスの利用

クラウド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。

④ ソーシャルメディア

ソーシャルメディアを利用する場合には、ソーシャルメディアの運用手順を定め、ソーシャルメディアで発信できる情報を規定し、利用するソーシャルメディアごとの責任者を定める。

(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、定期的に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応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驚異の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、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

上記 6，7 及び 8 に規定する対策等を実施するために、具体的な遵守事項及び判断基準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本局の運営に重大な 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局の運営に重大な支障を及ぼす恐れがあることから非公開とする。