高座清掃施設組合 情報セキュリティ基本方針

令和８年４月１日決定

１ 目的

本基本方針は、高座清掃施設組合（以下「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維持するため、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）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。

（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）クラウドサービス

インターネットを通じて提供されるコンピューティングリソース（サーバ、ストレージ、アプリケーション等）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。

（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、Web閲覧、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当該情報システムで取り扱うデータをいう。

３ 対象とする脅威

組合は、情報資産に対する以下の脅威を想定し、適切な情報セキュリティ対策を実施する。

（１）意図的な要因による脅威

インターネット経由の不正アクセス、コンピュータウイルス攻撃、サービス不能攻撃（DoS攻撃）等のサイバー攻撃、標的型メール等による重要情報の詐取、部外者の侵入、並びに内部不正による情報資産の漏えい・破壊・改ざん・消去等。

（２）非意図的な要因による脅威

情報資産の無断持ち出し、無許可ソフトウェア・クラウドサービスの使用（シャドーIT）等の規定違反、設定ミスや操作ミス、プログラム上の欠陥、メンテナンス不備、機器の故障、並びに委託管理の不備による情報資産の漏えい・破壊・消去等。

（３）サービス利用に起因する脅威（クラウド等）

将来導入するクラウドサービスにおいて、サービス提供事業者の瑕疵やシステム障害、通信経路の遮断等により、業務が停止又は情報の可用性が損なわれること。

（4）災害・疾病等による物理的・組織的脅威

地震、落雷、火災、風水害等の自然災害による設備破壊、並びに大規模な感染症の流行等に伴う要員不足により、システム運用や施設管理機能が不全に陥ること。

（5）社会インフラの障害による脅威

電力供給の途絶、通信回線の切断等の外部インフラの障害が、情報システムの稼働や施設の運営に波及すること。

4 適用範囲

（1）組織の範囲

本基本方針は、組合の全ての組織（事務局及び各施設等）に適用する。

（2）情報資産の範囲

① 組合が管理するサーバ、コンピュータ端末、ネットワーク機器、通信回線、並びにクラウドサービス上のシステム。

② 上記で取り扱う電子データ（メール、業務データ等）、及びそれらを印刷した文書・図面等の紙媒体。

③ 情報システムの仕様書、ネットワーク図、運用マニュアル等のシステム関連文書。

（3）対象者の範囲

組合の全ての職員、会計年度任用職員、及び派遣職員（以下「職員等」という。）に適用する。また、外部委託事業者の作業員等についても、契約に基づき本方針の遵守を求める。

5 情報セキュリティ対策

（1）組織体制

情報セキュリティ対策を推進する責任者を明確に定め、事故発生時の報告体制や意思決定を迅速に行うための組織体制を確立する。

（2）情報資産の分類と管理

保有する情報資産を重要度に応じて分類し、適切なアクセス制限や保管期限の設定など、適切な管理を実施する。

（3）情報システムの強靭性の向上

不正アクセスの防止（多要素認証の検討等)、メールセキュリティの強化及びクラウド利用における安全性確保（暗号化通信等）を講じる。

（4）物理的セキュリティ

サーバ、通信機器、及び端末の盗難・損傷を防ぐため、設置場所の施錠管理や入退室制限等の物理的な対策を講じる。

（5）人的セキュリティ

職員等が遵守すべき行動指針を定めるとともに、定期的な教育や訓練を行い、セキュリティ意識の向上を図る。

（6）技術的セキュリティ

OS等の最新化、ウイルス対策ソフトの導入、アクセスログの記録、及び外部媒体（USBメモリ等）の使用制限等の技術的対策を講じる。

6 運用、業務委託及び外部サービスの利用

（1）運用管理と緊急時対応

システムの監視と方針の遵守状況を確認する。また、事故発生時に迅速に対応するための緊急時対応計画を策定する。

（２）業務委託

委託先を選定する際はセキュリティ要件を明記した契約を締結し、対策の実施状況を定期的に確認する。

（３）外部サービス（クラウド等）の利用

クラウドサービスを利用する場合は、利用に係る規定を整備し、安全性を確認した上で導入する。

（４）ソーシャルメディアの利用

SNS等を利用する場合は、運用手順を定め、発信情報の範囲や責任者を明確にする。

７ 評価・見直し及び策定

（１）監査及び自己点検の実施

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、運用の改善を図る。

（２）情報セキュリティポリシーの見直し

監査結果や環境の変化、新たな脅威に対応するため、リスク分析を行った上で本方針を適宜見直す。

（３）対策基準及び実施手順の策定

本方針に基づき、具体的な遵守事項を定める「情報セキュリティ対策基準」及び、具体的な操作手順を定めた「情報セキュリティ実施手順」を策定する。なお、実施手順は原則として非公開とする。