那覇市・南風原町環境施設組合
情報セキュリティ基本方針

令和８年３月２６日制定

那覇市・南風原町環境施設組合 情報セキュリティ基本方針

1 目的

那覇市･南風原町環境施設組合情報セキュリティ基本方針(以下｢基本方針｣という。)は、那覇市・南風原町環境施設組合（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

この基本方針における用語の定義は下記のとおり定める。

（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）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。

① 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。

② 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。

③ 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。

（4）情報セキュリティポリシー

基本方針及び情報セキュリティ対策基準をいう。

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、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等の停止等

（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

情報セキュリティポリシーの適用範囲は、以下の範囲とする。

（１）組織

本組合の執行機関、議会、監査機関

（２）情報資産

① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（印刷文書等を含む。）

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

（３）対象者

本組合の職員（会計年度任用職員を含む。以下「職員等」という。）並びに、本組合の管理者・副管理者・会計管理者、本組合の議員及び監査委員、並びに本組合から業務を受託し情報資産に接する委託事業者（指定管理者を含む。）とする。

５ 職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たり情報セキュリティポリシーを遵守しなければならない。また、本組合の管理者・副管理者・会計管理者、本組合の議員及び監査委員、並びに本組合から業務を受託し情報資産に接する委託事業者（指定管理者を含む。）も、同様に本ポリシー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の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行う。

（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、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域と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、個人情報等の流出を防ぐ。

② LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③ インターネット接続系においては、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。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を検討する。

（4）物理的セキュリティ

サーバ機器、通信回線及び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、情報資産への侵害が発生した場合等に迅速かつ適切な初動対応を行い、関係機関（国、県、情報セキュリティ関連機関等）との連携のもとで被害の最小化と早期復旧を図る。

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、必要に応じて情報セキュリティ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、新たに対策が必要となった場合には、情報セキュリティポリシーを見直す。