小牧岩倉衛生組合情報セキュリティ基本方針

令和６年３月２９日制定

令和８年３月３１日改正

小牧岩倉衛生組合情報セキュリティ基本方針

1　目的

この基本方針は、小牧岩倉衛組合（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

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（ハードウエア及びソフトウエア）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。

(4) 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。

(5) 情報セキュリティインシデント

情報セキュリティに関する事故やシステム上の欠陥、並びにその原因や結果。組合内外の情報の漏えい（職員等の規定違反に起因するものを含む）や、情報システムに対するサイバー攻撃等をいう。

(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) 一般事務系

組合事務に係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)プラント制御系

ごみ処理施設のプラント設備における情報システム（分散型制御システム等）及びその情報システムで取り扱うデータをいう。

3　情報資産への脅威

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) 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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) 情報資産の無断持出、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、操作ミス、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) 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　情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は、組合の行政機関（管理者部局、議会事務局等）が保有するすべての情報資産並びに当該情報資産に接するすべての職員（特別職、非常勤職員及び臨時職員を含む。以下「職員等」という。）及び委託事業者とする。

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

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

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

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

情報システム全体に対し、次の対策を講じるものとする。

ア　一般事務系においては、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。

イ　プラント制御系においては、原則として、インターネット及び組合内の他のネットワークとの通信をできないようにした上で、端末へのＵＳＢメモリ等の記録媒体の接続を制限し、情報システムへの不正プログラムの侵入等を防ぐものとする。なお、一般事務系と通信を行う必要がある場合は、中継端末により通信環境を分離した上で、安全が確保された通信だけを送受信できるようにする。

(4) 物理的セキュリティ対策

サーバ、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) 人的セキュリティ対策

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セキュリティホールへの迅速な対応等の技術的対策を講じる。

(7) 運用面での対策

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切に対応するため、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

業務委託を行う場合には、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。

外部サービス（クラウドサービス等）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、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の実施

情報セキュリティポリシー自己点検の結果、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の見直しを実施する。

9　情報セキュリティ対策基準の策定

組合の情報資産について、上記６、７及び８に規定する対策等を実施するために、遵守すべき行為及び判断等の基準を定める情報セキュリティ対策基準を策定するものとする。

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。