くれさか環境事務組合
情報セキュリティ基本方針

令和８年３月策定

1　目的

本基本方針は、くれさか環境事務組合が保有する情報資産の機密性、完全性及び可能性を維持するため、くれさか環境事務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) 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) 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。

(6) 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。

(7) 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。

(8) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務に関わる情報システム及びデータをいう。

(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) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、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、ウィルス攻撃、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因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

(1) 本基本方針が適用される行政機関は、内部部局、議会事務局及び本組合管理の施設に適用する。

(2) 情報資産の範囲は、ネットワーク、情報システム、関連施設、電磁的記録媒体及びシステム関連文書とする。

5　職員等の遵守義務

本組合が保有する情報資産を取扱う職員（再任用職員、会計年度任用職員を含む。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

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) 情報システムの強靭化の向上

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、他領域との通信をできないようにした上で、端末からの情報持出し不可設定や端末への多要素認証の導入により流出を防ぐ。

② インターネット接続系は不正通信監視機能を強化し、必要に応じて無害化通信を導入する。

③ 無線 LAN を利用する場合は、ガイドラインが求める強固な認証方式等を導入する。

(4) 物理的セキュリティ

サーバ、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、業務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) 業務委託とクラウドサービスの利用

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書を締結した上で、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、必要に応じて契約書に基づき措置を講じる。クラウドサービスを利用する場合には、運用手順を定めることにより、利用する範囲を規定する。必要に応じてソーシャルメディア運用規定を整備する。

(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。又、見直しが必要な場合は適宜情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ対策基準の策定

上記 6 に規定する対策を実施するために、具体的な遵守事項及び判断基準を定めた情報セキュリティ対策基準を策定する。

8　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。尚、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恐れがあることから非公開とする。