令和８年４月１日策定

川西市議会情報セキュリティ基本方針

１．方針の目的

本基本方針は、川西市議会（以下「議会」という。）が議会活動及び政務活動（以下「議会活動等」という。）を行う上で取り扱う情報資産の機密性、完全性及び可用性を維持するとともに、議会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。また、本基本方針を地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定するサイバーセキュリティを確保するための方針として位置付ける。

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

情報資産を様々な脅威から守り、その価値を維持することをいう。

（４）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。

（５）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。

（６）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。

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、操作・設定ミ

ス、監査機能の不備、委託管理の不備、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、通信の途絶等のインフラの障害からの波及等

４．適用範囲
（１）機関の範囲
本基本方針が適用されるのは、本市の議会（議員及び議会事務局を含む。以下同じ。）とする。
（２）情報資産の範囲
本基本方針が対象とする情報資産は、次のとおりとする。
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（本市が管理するネットワーク又は情報システムに接続して利用する私物端末等を含む。）
② ネットワーク及び情報システムで取り扱う情報

５．議員等の遵守義務
議員、議会事務局職員等（以下「議員等」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、本基本方針を遵守し、責任をもって行動しなければならない。
なお、本市が管理する情報資産に対しては、川西市情報セキュリティに関する規則ほか市が定める規定等（以下「市規則等」という。）を遵守しなければならない。

６．情報セキュリティ対策
第３項に規定する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
議会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
議会の保有する情報資産をその重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。
（３）物理的セキュリティ
議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。
（４）人的セキュリティ
情報セキュリティに関し、議員等が遵守すべき事項を定めるとともに、教育及び啓発を行う等の人的な対策を講じる。
（５）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。

（６）運用

本市のシステム運用・保守に関する基準、ＩＣＴ業務継続計画等を準用し、情報システムの監視、本方針の遵守状況の確認、業務委託を行う際のセキュリティ確保等、本方針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は市規則等を準用し、迅速かつ適正に対応する。

（７）業務委託（外部サービス（クラウドサービス）の利用を含む。）

議会活動等において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。

（８）評価・見直し

本基本方針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。本基本方針の見直しが必要な場合は、適宜本基本方針の見直しを行う。

７．情報セキュリティ監査・自己点検の実施

本基本方針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する。

８．本基本方針の見直し

情報セキュリティ監査及び自己点検の結果、本基本方針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脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、本基本方針を見直す。