四條畷市議会情報セキュリティ基本方針

1　目的

この基本方針は、四條畷市議会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、本市議会の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）情報資産

情報及び情報システム等の総称をいう。

（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）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。

（7)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含む。）をいう。

3　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

（1）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウィルス攻撃、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、外部委託管理の不備、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システム運用の機能不全等

（5）電力供給、通信、水道供給の途絶等の提供サービスの障害からの波及等

4　情報資産の範囲

本基本方針が対象とする情報資産は、本市議会が取り扱う以下の各号に掲げるものとする。

ただし、市長が議会事務局職員の使用に供する情報資産については、その取り扱いは、四條畷市情報セキュリティポリシーに従うものとし、本方針の適用範囲外とする。

（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

（2）ネットワーク及び情報システムで取り扱う情報(これらを印刷した文書を含む。)

（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

5　議員及び議会事務局職員の遵守義務

議員、議会事務局の全ての職員(以下、「職員等」という。)及び外部委託した業務の受託者等は、情報セキュリティの重要性について共通の認識をもつとともに、活動及び業務の遂行に当たって関係法令等及び四條畷市議会情報セキュリティ基本方針を遵守する義務を負うものとする。

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、次に掲げる情報セキュリティ対策を講じる。また、職員等は、この基本方針の実施に責任を負うとともに、その目的を十分理解し達成するため、情報セキュリティの重要性について共通の認識を持ち、この基本方針及び関連する法令を尊重かつ遵守し、行動しなければならない。

（1）組織体制

本市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を議会運営委員会とする。

（2）情報資産の分類及び管理

情報資産を安全に管理及び保護するため、情報資産の管理方法を定める。また、情報システムで取り扱う情報のうち、重要な情報を重点管理する考え方から、その重要性に応じた情報の分類の定義並びに情報の管理責任及び管理方法を定める。

（3）物理的セキュリティ対策

情報システムを設置する施設の管理について、物理的な対策を講じる。

（4）人的セキュリティ対策

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。

（5）技術的セキュリティ対策

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

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、緊急時対応計画を定める。**

（7）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。外部サービスを利用する場合は、利用に係る規定を整備し対策を講じる。

（8）評価・見直し

情報セキュリティ基本方針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視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。情報セキュリティ基本方針の見直しが必要な場合は、適宜情報セキュリティ基本方針の見直しを行う。

7　情報セキュリティ監査及び点検の実施

情報セキュリティ基本方針が遵守されていることを検証するため、必要に応じて、議会運営委員において情報セキュリティ監査及び点検を実施する。

8　情報セキュリティ基本方針の見直し

情報セキュリティ監査及び点検の結果、情報セキュリティ基本方針の見直しが必要に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、リスクを検討した上で、情報セキュリティ基本方針を見直す。

附則

この基本方針は令和８年４月１日から施行する。