箕面市議会情報セキュリティ基本方針

制定　令和８年（2026 年）４月１日

１　目的

箕面市議会情報セキュリティ基本方針（以下「本基本方針」という。）は、議会が保有又は管理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、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。

２　用語の定義

本基本方針において使用する用語の定義は、次に掲げるところによる。

（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及びその構成機器（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）機密性

情報にアクセスすることを認められた者のみ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）インターネット接続系

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。

３　対象とする脅威

情報資産に対する脅威として、次に掲げる事項を想定し、必要な情報セキュリティ対策を講ずるものとする。

（１）不正アクセス、ウイルス感染、サービス妨害攻撃等のサイバー攻撃又は部外者の侵入等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、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、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

（１）本基本方針が適用される機関

箕面市議会（議会事務局を除く。）

（２）情報資産の範囲

本基本方針が対象とする議会が議会活動のため保有する情報資産は、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
②ネットワーク及び情報システムで取り扱う情報（これらを印字した文書を含む。）
③情報システムの仕様書及びネットワーク図等の関連文書

５　議員の遵守義務

議員は、情報セキュリティの重要性を認識し、業務の遂行にあたっては、関係法令等及び本基本方針を遵守しなければならない。

６　職員等の遵守義務

事務局職員及び会計年度任用職員は、箕面市情報システムの管理運営に関する条例施行規則（令和４年箕面市規則第４４号）を遵守しなければならない。

７　組織体制

議会の情報セキュリティ対策を推進するため議会の組織体制を確立する。

８　情報システム全体の強靭性の向上

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講じる。

９　物理的セキュリティ対策

端末及び記録媒体等について、盗難防止措置等の物理的対策を講じる。

１０　人的セキュリティ対策

議員に対し、情報セキュリティ対策に関する教育及び啓発を行う等の人的な対策を講じる。

１１　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。

１２　運用及び緊急時対応

情報システムの監視、本基本方針の遵守状況の確認等の運用管理を実施するとともに、情報資産に対するセキュリティ侵害が発生した場合には、速やかに議長へ報告し対応する。

１３　業務委託の利用

業務委託を行う場合には、委託業者を選定し、情報セキュリティ要件を明記した契約を締結し、必要に応じて契約に基づき措置を講じる。

１４　外部サービスの利用

外部サービス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。

１５　情報セキュリティ監査及び自己点検

（１）本基本方針の遵守状況を確認するため、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。

（２）情報セキュリティ監査については議会事務局が実施し、結果について、議長が指定する組織に報告する。

１６　評価・見直し

情報セキュリティ監査及び自己点検の結果又は社会情勢・技術環境の変化により、必要があると認めるときは、本基本方針を見直すものとする。

１７　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となった場合には、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、本基本方針を見直すものとする。