

| | |
|-----|------------|
| 改訂日 | |
| 制定日 | 令和8年 4月 1日 |

鈴鹿市議会情報セキュリティ基本方針

令和8年4月1日

鈴鹿市議会

目次

| | | |
|----|----------------------|---|
| 1 | はじめに | 1 |
| 2 | 情報セキュリティ基本方針の目的 | 1 |
| 3 | 情報セキュリティ基本方針の適用範囲 | 1 |
| 4 | 情報セキュリティ基本方針の遵守義務者 | 1 |
| 5 | 情報セキュリティ推進体制 | 2 |
| 6 | 情報資産の取扱い | 2 |
| 7 | 情報資産への脅威 | 2 |
| 8 | 情報セキュリティ対策の実施 | 2 |
| 9 | 情報セキュリティ意識の向上 | 3 |
| 10 | 情報セキュリティ問題への対応 | 3 |
| 11 | 情報セキュリティ監査及び自己点検の実施 | 4 |
| 12 | 情報セキュリティ基本方針の評価及び見直し | 4 |
| 13 | 用語の定義 | 4 |

鈴鹿市議会情報セキュリティ基本方針

1 はじめに

地方自治法（昭和 22 年法律第 67 号）第 244 条の 6 第 1 項の規定に基づき、鈴鹿市議会情報セキュリティ基本方針（以下「基本方針」という。）を定める。

2 情報セキュリティ基本方針の目的

基本方針は、鈴鹿市議会が取り扱う情報資産を盗難や不正アクセス等の様々な脅威から適正に保護し、情報資産の機密性・完全性・可用性を維持していくことを目的とする。

3 情報セキュリティ基本方針の適用範囲

3.1 適用組織の範囲

鈴鹿市議会

3.2 情報資産の範囲

基本方針が対象とする情報資産は次のとおりとする。

- 1 議会が管理する情報システム（業務委託により利用するものを含む。）
- 2 議会が管理する情報システムにおいて取り扱う電子データ（印刷した紙文書を含む。）
- 3 情報システム利用時の認証に関する情報
- 4 議員が議会活動及び政務活動を行う過程で取得・保持する個人情報・機密情報・公開情報
- 5 上記 1 から 4 を管理するために必要な設備及び電磁的記録媒体（ルーター、wi-fi 機器、パソコン、タブレット、USB メモリなど）

4 情報セキュリティ基本方針の遵守義務者

鈴鹿市議会が保有する情報資産に携わる議員、議会事務局職員及び業務委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては基本方針を遵守しなければならない。

5 情報セキュリティ推進体制

基本方針に基づき、情報セキュリティ対策を組織的かつ効果的に管理する体制を確立するため、議長を最高責任者とし、セキュリティ推進体制を構築する。

6 情報資産の取扱い

情報資産を適切に取り扱うため、情報セキュリティ対策を実施する。

7 情報資産への脅威

鈴鹿市議会の情報資産に対する脅威の発生度合い及び発生した場合の影響から、認識すべき脅威は次のとおりとする。

- 7.1 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、盗難、盗聴、改ざん、消去、重要情報の許取、内部不正等
- 7.2 議会事務局職員、議員又は業務委託事業者による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の要因による情報資産の漏えい、破壊、消去等
- 7.3 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
- 7.4 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
- 7.5 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

8 情報セキュリティ対策の実施

情報資産を脅威から保護するため、次のセキュリティ対策を実施するものとする。

- 8.1 情報システムを設置する場所（施設）への不正な立入り、情報資産を損傷・妨害、災害等から保護するための物理的なセキュリティ対策
- 8.2 情報資産へのアクセス制御、コンピュータウイルスからの保護、ネットワーク管理等の技術面のセキュリティ対策、また外部へのシステム開発等の業務委託を行う際のセキュリティの確保等や、ネットワークの監視、基本方針の遵守状況の確認等の運用面のセキュリティ対策
- 8.3 情報セキュリティに関する権限及び責任を定め、議会事務局職員、議員及び業務委託事業者の基本方針の内容を周知徹底し、必要に応じたセキュリティ教育の実施又はパスワードの適切な設定・管理、作業内容の記録、業務委託時の守秘義務契約締結等の人的なセキュリティ対策
- 8.4 緊急事態が発生した際に迅速な対応を可能とするための危機管理対策
- 8.5 業務委託と外部サービス（クラウドサービス）の利用
 - ①業務委託する場合には、業務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、業務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た上で、必要に応じて契約に基づき措置を講じる。
 - ②約款による外部サービス（クラウドサービス）を利用する場合には、利用に係る規定等を整備し、対策を講じる。
 - ③ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用方針等を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

9 情報セキュリティ意識の向上

議員及び議会事務局職員に対し情報セキュリティの浸透を図り、議員及び議会事務局職員自らが情報セキュリティに関する意識の向上に努めるため、情報セキュリティに関する教育を定期的実施する。

10 情報セキュリティ問題への対応

情報セキュリティ問題等が発生した場合は、速やかに必要な措置をとるとともに、原因等を分析し、再発防止策を講じるものとする。

11 情報セキュリティ監査及び自己点検の実施

基本方針が有効的に実施され、かつ遵守されていることを検証するため、定期的に監査及び自己点検を実施する。

12 情報セキュリティ基本方針の評価及び見直し

基本方針に定める事項及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化や、基本方針の遵守状況などを踏まえ、基本方針がその実効性を維持するよう、評価及び見直しを定期的、又は必要に応じ適宜行うものとする。

13 用語の定義

(1) 情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(2) 情報

職務遂行上に作成、取得した紙等の有体媒体上の記録及び電磁的記録をいう。単体では意味をなさなくても、ソフトウェア等により意味をなす場合はこれに該当する。

(3) 情報システム

電子計算機及び業務処理用アプリケーション（ソフトウェアを含む）で構成され、情報処理する仕組みをいう。ネットワークもこれを含む。

(4) 情報資産

情報（紙等の有体物に出力された情報を含む）及び情報システムをいう。

(5) ネットワーク

情報システムを相互に接続するための通信網及びその構成機器（ソフトウェアを

含む) で構成され、情報処理を行う仕組みをいう。

(6) 個人情報

個人情報の保護に関する法律（平成 15 年法律第 57 号）第 2 条第 1 項第 1 号に規定する個人情報をいう。

(7) 業務委託事業者

鈴鹿市議会から業務の委託を受けている事業者をいう。

(9) 機密性 (Confidentiality)

情報にアクセスすることを許可された者だけがアクセスできることを確実にすることをいう。

(10) 完全性 (Integrity)

情報及び処理の方法の正確さ及び完全である状態を安全防護することをいう。

(11) 可用性 (Availability)

許可された利用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ことを確実にすることをいう。