改版日	
制定日	令和８年　４月　１日

鈴鹿市監査委員
情報セキュリティ基本方針

令和８年４月１日

鈴鹿市監査委員

制　定・改　訂　履　歴

版	制 改 訂 年 月 日	制　改　訂 理　　由	制　　改　　訂 内　　　　容
初版	令和８年４月１日	初版制定	令和８年４月１日制定 同日施行

目次

情報セキュリティ基本方針

1　はじめに

鈴鹿市監査委員情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、鈴鹿市監査委員及び鈴鹿市監査委員事務局（以下「監査委員等」という。）が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。

2　情報セキュリティポリシーの目的

情報セキュリティポリシーは、盗難や不正アクセス等の様々な脅威から監査委員等の情報資産を適正に保護し、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　情報セキュリティポリシーの体系

情報セキュリティポリシー及び関連する規則は、次の体系で構成し、明文化するものとする。

3.1　情報セキュリティポリシー

(1) 情報セキュリティ基本方針

監査委員等の情報セキュリティ対策に関する統一的かつ基本的な方針（本基本方針）

4　情報セキュリティポリシーの適用範囲

4.1　組織の範囲

情報セキュリティポリシーを適用する範囲は、監査委員及び監査委員事務局とする。

4.2　情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

① 監査委員等が管理するネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② 監査委員等が管理する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 監査委員等が管理する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　情報セキュリティポリシーの遵守義務者

監査委員及び監査委員事務局の職員並びに業務委託事業者（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つとともに、業務の遂行に当たっては情報セキュリティポリシーを遵守しなければならない。

6　情報セキュリティ推進体制

情報セキュリティポリシーに基づき、情報セキュリティ対策を推進する組織的かつ効果的に管理する体制を確立する。

7　情報資産の取扱い

情報資産を適切に取り扱うため、情報資産を情報資産の重要度に応じて分類し、分類レベルに応じた情報セキュリティ対策及び管理体制を定めるものとする。

8　情報資産への脅威

監査委員等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。

8.1　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

8.2　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

8.3　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

8.4　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

8.5　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

9　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。

9.1　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

9.2　情報資産へのアクセス制御、コンピュータウィルスからの保護、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、情報セキュリティポリシーの遵守状況の確認等の運用面のセキュリティ対策

9.3　情報セキュリティに関する権限及び責任を定め、職員等に情報セキュリティポリシー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、業務時の守秘義務契約締結等の人的なセキュリティ対策

9.4　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

9.5　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。

10　情報セキュリティ意識の向上

職員等に対し情報セキュリティの浸透を図り、職員等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に実施する。

11　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。

12　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシー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。

13　情報セキュリティポリシーの評価及び見直し

情報セキュリティポリシー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、情報セキュリティ監査、情報セキュリティポリシーの遵守状況などを踏まえ、情報セキュリティポリシー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。

14　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に含む。

(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) 職員

地方公務員法（昭和 25 年法律第 261 号）第３条に規定する職員をいう。

(8) 業務委託事業者

監査委員等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。