鈴鹿市情報セキュリティ基本方針

第10版

平成３１年２月２６日

鈴　鹿　市

目　　次

情報セキュリティ基本方針

1　はじめに

鈴鹿市情報化推進体制の整備に関する規則（平成27年鈴鹿市規則第53号）第13条の規定により，情報セキュリティポリシーを定める。

なお，情報セキュリティポリシーを普遍性の部分である基本方針と，基本方針を実現するために実施しなければならない行動を示す対策基準に分けて策定する。

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鈴鹿市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，次のような体系で構成し，各々を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

鈴鹿市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）

(2)情報セキュリティ対策基準

情報セキュリティ基本方針に基づき，すべての情報資産に共通の情報セキュリティ対策を実施する上での統一的な対策基準

3.2　関連規則

(1)情報セキュリティ実施手順

情報セキュリティ対策基準に基づき，情報セキュリティ対策を実施するための具体的な実施手順書

4　情報セキュリティポリシーの適用範囲

4.1　適用組織の範囲

情報セキュリティポリシーを適用する組織は，市長部局，上下水道局，消防本部，教育委員会事務局，鈴鹿市立小中学校，議会事務局，監査委員事務局，選挙管理委員会事務局，農業委員会事務局，固定資産評価審査委員会事務局及び公平委員会事務局とする。

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。ただし，教育委員会事務局及び鈴鹿市立小中学校が保有する情報資産を除く。

①　鈴鹿市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　鈴鹿市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　鈴鹿市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

4.3　適用管理策

管理策	内　容
直接適用する管理策	適用した管理策を鈴鹿市が直接マネジメント及びコントロールする管理策
守秘契約に基づき委託する管理策	適用した管理策を鈴鹿市がマネジメントするが直接コントロールできない管理策
守秘義務に基づき依存する管理策	国，県及び関係団体等が適用した管理策が鈴鹿市にも適用されているが鈴鹿市がマネジメントできない管理策

5　情報セキュリティポリシーの遵守義務者

鈴鹿市が保有する情報資産に携わる職員及び外部委託事業者は，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情報セキュリティポリシーを維持するための実施手順を遵守しなければならない。

情報セキュリティポリシー又は情報セキュリティ実施手順の違反者に対しては，違反の程度に応じて懲戒処分等の対象とする。

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組織的かつ効果的に管理する体制を確立するため，情報統括監を中心としたＩＣＴ推進本部及び情報統括監補佐官，各部局の主管課長等で構成するＩＣＴ推進委員会により，統一した情報セキュリティ対策を推進する。

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

鈴鹿市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　外部からの故意のネットワークへの不正アクセス，不正操作，コンピュータウィルスの侵入，建物への不正侵入等による情報資産の漏えい，破壊，盗難，盗聴，改ざん等

8.2　職員による誤操作，設計仕様の誤り，情報資産の不適切管理による漏えい，改ざん，消去等の意図しないミス及び情報資産の破壊，持ち出し，盗聴，漏えい，改ざん等の内部犯罪

8.3　外部委託事業者による情報資産の持ち出し，誤操作，不適切管理による破壊，漏えい，盗難，消去等

8.4　地震，落雷等の災害，火災等の事故，故障等によるサービス，業務停止等

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，職員及び外部委託事業者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，外部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

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　情報システム全体の強靭性向上対策（次の三段階の対策）

① マイナンバー利用事務系においては，原則として，他の領域との通信をできないようにした上で，端末からの情報持ち出し不可設定や端末への多要素認証の導入等により，住民情報の流出を防ぐ。

② LGWAN 接続系においては，LGWAN と接続する業務用システムと，インターネット接続系の情報システムとの通信経路を分割する。なお，両システム間で通信する場合には，無害化通信等を実施する。

③ インターネット接続系においては，三重県自治体情報セキュリティクラウドに参加し，インターネット接続口を集約した上で，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実施する。

10　外部サービスの利用

外部委託する場合には，外部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，外部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。

約款による外部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。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。

11　情報セキュリティ対策基準の策定

鈴鹿市の情報資産についてセキュリティ対策を実施するに当たり，遵守すべき事項及び判断の基準を統一的なレベルで定めるため，セキュリティ対策を行う上での基本的な要求を明記した情報セキュリティ対策基準を策定するものとする。

12　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守し，セキュリティ対策を確実に実施するため，個々の情報資産に関する対策手順等を具体的に定めておく必要がある。情報資産に対する脅威及び情報資産の重要度に対応する対策基準の要求に基づき，それぞれの情報資産の情報セキュリティ実施手順を策定するものとする。

なお，情報セキュリティ対策基準及び情報セキュリティ実施手順で具体的な対策を定めた部分は，本市の情報セキュリティ対策に重大な支障を及ぼす恐れがある情報を含むことから非公開とする。

13　情報セキュリティ意識の向上

職員に対し情報セキュリティの浸透を図り，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に実施する。

14　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。

15　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。

16　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。

17　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

鈴鹿市個人情報保護条例（平成 15 年鈴鹿市条例第 36 号）第２条第１号に規定する個人情報をいう。

(7) 職員

鈴鹿市の職員で地方公務員法（昭和 25 年法律第 261 号）第 2 条に規定する職員をいう。

(8) 外部委託事業者

鈴鹿市から業務の委託を受けている事業者をいう。

(9) 脅威

情報資産の価値を失わせる事象をいう。不正アクセス等の意図的脅威，入力ミス等の偶発的脅威，災害時の環境的脅威等を指す。

(10) 管理策

情報資産のセキュリティリスクに対し，脆弱性を減らし情報セキュリティを保護するための具体的な対策をいう。

(11) 機密性（Confidentiality）

情報にアクセスすることが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。

（12）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。
（13）可用性（Availability）
許可された利用者が必要なときに情報にアクセスできることを確実にすることをいう。
（14）マイナンバー利用事務系（個人番号利用事務系）
個人番号利用事務（社会保障，地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。
（15）LGWAN 接続系
人事給与,財務会計及び文書管理等 LGWAN 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。
（16）インターネット接続系
インターネットメール,ホームページ管理システム等に関わる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。
（17）通信経路の分割
LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で，安全が確保された通信だけを許可できるようにすることをいう。
（18）無害化通信
インターネットメール本文のテキスト化や端末への画面転送等により,コンピュータウイルス等の不正プログラムの付着が無い等，安全が確保された通信をいう。