鈴鹿亀山地区広域連合情報セキュリティポリシー

（情報セキュリティ基本方針）

平成 28 年 3 月 30 日

（令和 8 年 3 月 26 日改正）

鈴鹿亀山地区広域連合

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	平成 28 年 3 月 30 日	初版制定	平成 28 年 3 月 30 日制定 同日施行
2 版	令和 6 年 3 月 13 日	ガイドラインの改正による改訂	令和 6 年 3 月 13 日改正 同日施行
3 版	令和 8 年 3 月 26 日	ガイドラインの改正による改訂	令和 8 年 3 月 26 日改正 同日施行

目次

情報セキュリティポリシー

情報セキュリティ基本方針

情報セキュリティポリシー

1　はじめに

情報セキュリティポリシーとは、鈴鹿亀山地区広域連合の情報資産をどのような脅威からなぜ保護しなければならないかを明確にした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である。

行政事務の電子化に伴い、あらゆる情報が不正アクセスや改ざん又は漏えい等の被害を受ける可能性が増大していることから、個人情報や機密情報等の情報に対する保護のあり方がより厳しく求められるようになってきている。様々な脅威から情報資産を防御するため、当広域連合における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。

情報セキュリティポリシーは、鈴鹿亀山地区広域連合が取り扱う情報資産に携わる職員及び委託事業者に普及、浸透させ定着させるものである。

2　目的

情報セキュリティポリシーの目的は、盗難や不正アクセス等の様々な脅威から鈴鹿亀山地区広域連合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である。「鈴鹿亀山地区広域連合情報セキュリティポリシー」に定める統一的な情報セキュリティ対策を実施することで、行政サービスの提供に不可欠な情報資産の管理を徹底し、圏域住民からの信頼の維持向上に努めるものとする。

3　体系

情報セキュリティポリシーは、次のような体系で構成し、各々を明文化するものとする。

（1）　情報セキュリティ基本方針

鈴鹿亀山地区広域連合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、全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

情報セキュリティ基本方針

１　基本方針

鈴鹿亀山地区広域連合の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するための情報セキュリティポリシーのうち、情報セキュリティ基本方針については、情報セキュリティ対策の基本的な事項について定めることとする。

２　適用範囲

情報セキュリティポリシーの適用範囲は、鈴鹿亀山地区広域連合の行政サービスとし、適用する組織、サイト、資産及び管理策について、次のように定める。

（１）　組織の範囲

鈴鹿亀山地区広域連合事務局、議会事務局、監査委員事務局、選挙管理委員会事務局、公平委員会事務局職員

（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、次のとおりにする。

ただし、議会及びその他の執行機関において定める情報セキュリティに係る方針等の適用範囲を除く。

① 鈴鹿亀山地区広域連合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 鈴鹿亀山地区広域連合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 鈴鹿市亀山地区広域連合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

３　遵守義務者

鈴鹿亀山地区広域連合が保有する情報資産に携わる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情報セキュリティポリシー及び情報セキュリティ実施手段を遵守しなければならない。

情報セキュリティポリシー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。

４　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、情報セキュリティ対策委員会を設置し、統一した情報セキュリティ対策を実施する。

5　情報資産の取扱い

情報資産を適正に取り扱うため、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。

6　情報資産への脅威

鈴鹿亀山地区広域連合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。

（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

（2）　職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

7　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。

（1）　情報システムを設置する場所（施設）への不正な立入り、情報資産の損傷・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

（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

（3）　情報セキュリティに関する権限及び責任を定め、職員及び業務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、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

（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

（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。

８　情報セキュリティ対策基準の策定

鈴鹿亀山地区広域連合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。

９　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ことから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情報セキュリティ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、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。

１０　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。

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講じるとともに、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等を踏まえ、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内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、情報処理する仕組みをいう。

（６）サイト

事務所等の情報資産を設置、取り扱い又は保管する建物及びその附属施設並びにこれらの敷地をいう。

（７）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。以下「個人情報保護法」という。）第２条第１項第１号に規定する個人情報をいう。

（８）業務委託事業者

鈴鹿亀山地区広域連合から業務の委託を受けている事業者をいう。

（９）機密性

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

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

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。

（１２）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）に関わる情報システム及びデータをいう。

（１３）LGWAN 接続系

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（マイナンバー利用事務系を除く。）。

（１４）インターネット接続系

インターネットメール、ウェブサイト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。