鈴鹿市教育情報セキュリティ基本方針

平成30年７月13日策定
令和４年２月18日改定
令和８年３月30日改定

１　目的

この基本方針は、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定する方針として鈴鹿市教育委員会（以下「教育委員会」という。）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により、教育委員会等が保有する情報資産の機密性、完全性及び可用性を維持することを目的とする。

２　用語の定義

（１）教育委員会等

教育委員会（その権限に属する事務を補助執行する職員が属する市長の補助機関を含む。）及び教育委員会の所管に属する学校その他の教育機関をいう。

（２）学校

教育委員会の所管に属する学校をいう。

（３）教育委員会事務局職員等

教育委員会事務局の職員（教育委員会の権限に属する事務を補助執行する職員を含む。）及び教育委員会の所管に属する学校以外の教育機関の職員（臨時又は非常勤の職員を含む。）をいう。

（４）教職員

学校に勤務する教職員（臨時又は非常勤の教職員を含む。）をいう。

（５）児童生徒

学校に就学する児童及び生徒をいう。

（６）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。）をいう。

（７）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。

（８）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。

（９）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保

することをいう。

(10) 完全性

情報が破壊、改ざん又は消去をされていない状態を確保することをいう。

(11) 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。

(12) 教育情報セキュリティポリシー

教育情報セキュリティ基本方針及び教育情報セキュリティ対策基準をいう。

3　対象とする情報資産への脅威

情報資産への脅威として、次の脅威を想定する。

（1）外部からの故意の不正アクセス、不正操作、コンピュータウイルスの侵入、建物への不正侵入等による情報資産の漏えい、破壊、盗難、改ざん等のリスク

（2）誤操作、不適切管理又は意図的な不正操作等による情報資産の漏えい、持ち出し、盗聴、改ざん、消去等のリスク

（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のリスク

（4）大規模かつ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のリスク

（5）電力供給の途絶、通信の途絶等の提供サービスの障害からの波及等のリスク

（6）組織的又は人的な脆弱性に起因するリスク

（7）重要度の高い情報資産を保管する際のセキュリティリスク

（8）児童生徒が重要度の高い情報資産にアクセスするリスク

（9）インターネット利用におけるセキュリティリスク

(10) 外部への情報資産の持ち出しリスク

(11) パブリッククラウドサービスのサービス事業者側のセキュリティリスク

4　適用範囲

（1）この基本方針を適用する機関は、教育委員会等とする。

（2）この基本方針を適用する情報資産は、次のとおりとする。

ア　ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体

イ　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、及び複製したものを含む。）

ウ　ネットワーク構成図及び情報システムの仕様書等のシステム関連文書

5　教育委員会事務局職員等及び教職員の遵守義務

教育委員会事務局職員等及び教職員は、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法令及び教育情報セキュリティポリシーを遵守し、情報資産を適切に保護しなければならない。

6　情報セキュリティ対策の管理体制

教育委員会等の情報資産の運用に関して、情報セキュリティ対策を推進し、及び管理するための体制を確立するものとする。

7　情報資産の分類及び管理

情報資産を適切に取り扱うため、教育委員会等が取り扱う情報資産を洗い出し、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　情報セキュリティ対策

情報資産を脅威から保護するため、次に定める情報セキュリティ対策を実施する。

（1）地震、落雷、火災等の災害、大規模かつ広範囲にわたる疾病、電力供給の途絶等が発生した場合における「鈴鹿市業務継続計画（鈴鹿市ＢＣＰ）」に準じた対応

（2）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

（3）情報資産へのアクセス制御、不正プログラム対策、コンピュータウイルスからの保護、ネットワーク管理、ネットワーク分離、情報漏えい対策等の技術的なセキュリティ対策

（4）情報システムの監視、教育情報セキュリティポリシー遵守状況の確認、外部委託を行う際の情報セキュリティの確保等、教育情報セキュリティポリシーの運用面のセキュリティ対策

（5）情報セキュリティに関する権限及び責任の明確化、教育委員会事務局職員等及び教職員に対するセキュリティ教育の実施並びにパスワードの適切な設定、管理等の人的なセキュリティ対策

（6）情報資産への侵害等の緊急事態が発生した際に迅速かつ適切な対応を可能とするための危機管理対策

9　情報セキュリティ意識の向上

教育委員会事務局職員等及び教職員に対し情報セキュリティの浸透を図り、教育委員会事務局職員等及び教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。

10　情報セキュリティ問題への対応

情報セキュリティに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　監査及び自己点検

教育情報セキュリティポリシーが遵守されていることを検証するため、定期的又は必要に応じて監査及び自己点検を実施する。

12　評価及び見直し

教育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、情報セキュリティ監査、教育情報セキュリティポリシーの遵守状況等を踏まえ、教育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て行うものとする。

13　教育情報セキュリティ対策基準の策定

教育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として、教育情報セキュリティ対策基準を策定する。

なお、教育情報セキュリティ対策基準は、公にすることにより教育委員会等の運営に支障を及ぼす恐れがあることから非公開とする。

14　教育情報セキュリティ実施手順の策定

教育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手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、教育情報セキュリティ実施手順は、公にすることにより教育委員会等の運営に支障を及ぼす恐れがあることから非公開とする。