奈良市教育委員会
教育情報セキュリティポリシー

奈良市教育委員会　教育情報セキュリティポリシーについて

奈良市教育委員会　教育情報セキュリティポリシーは、本市が保有する教育情報資産に関する教育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定めたものである。

この教育情報セキュリティポリシーの目的は、教育情報セキュリティを確保するための考え方、体制、組織、運用等を規定することによって業務の安定的な運用を図ること、そして本市が保有する個人情報、教育情報資産を守ることである。

教育情報セキュリティポリシーとして、本市の教育情報セキュリティに対する基本的な考え方を示した「奈良市教育委員会　教育情報セキュリティ基本方針」と、その対策基準を基に個々の教育情報セキュリティ対策を規定した「奈良市教育委員会　教育情報セキュリティ対策基準」を策定することとする。これらは、常に水準の向上を図るため、継続的な評価・見直しを実施する。

そして、「奈良市教育委員会　教育情報セキュリティ基本方針」及び「奈良市教育委員会　教育情報セキュリティ対策基準」に基づき、各情報システムの具体的な教育情報セキュリティ対策の実施手順を策定することとする。

第一章

教育情報セキュリティ基本方針

改訂履歴

バージョン	改定日	改定内容
1.0	令和５年５月２日	初版発行

第１章 教育情報セキュリティ基本方針

1. 目的

本基本方針は、本市が保有する教育情報資産の機密性、完全性及び可用性を維持するため、本市が実施する教育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を目的とする。

2. 定義

(1) 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、その構成機器（ハードウェア及びソフトウェア）をいう。

(2) 教育情報システム

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。

(3) 教育情報セキュリティ

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。

(4) 教育情報セキュリティポリシー

本基本方針及び教育情報セキュリティ対策基準をいう。

(5) 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。

(6) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 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。

3. 対象とする脅威

教育情報資産に対する脅威として以下の脅威を想定し、教育情報セキュリティ対策を実施する。

(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教育情報資産の漏えい・破壊・改ざん・消去、重要情報の許取、内部不正等

(2) 教育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、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による教育情報資産の漏えい・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の停止等

(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

4. 適用範囲

(1) 行政機関等の範囲

本市が保有する教育情報資産及びこの情報資産に接する職員（会計年度任用職員及び臨時的職員等を含む。以下同じ。）及び外部委託事業者等に適用する。

(2) 教育情報資産の範囲

本基本方針が対象とする教育情報資産は、次のとおりとする。

① 教育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 教育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 教育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. 教職員の遵守義務

常勤・非常勤を問わずすべての教職員（以下「教職員」という。）は、教育情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって教育情報セキュリティポリシー及び教育情報セキュリティ実施手順を遵守しなければならない。

6. 教育情報セキュリティ対策

上記３の脅威から教育情報資産を保護するために、以下の教育情報セキュリティ対策を講じる。

(1) 組織体制

本市の教育情報資産について、教育情報セキュリティ対策を推進する本市及び教育委員会事務局内で組織体制を確立する。

(2) 教育情報資産の分類と管理

本市の保有する教育情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき教育情報セキュリティ対策を実施する。

(3) 教育情報システム全体の強靭性の向上

教育情報システム全体に対し、次の対策を講じる。

①不正通信の監視機能の強化等の高度な教育情報セキュリティ対策を実施する。

(4) 物理的セキュリティ

サーバ等、教育情報システム室等、通信回線等及び教職員のパソコン等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

教育情報セキュリティに関し、教職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

教育情報システムの監視、教育情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、教育情報セキュリティポリシーの運用面の対策を講じるものとする。また、教育情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8) 外部サービスの利用

外部委託を行う場合には、外部委託事業者を選定し、教育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、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、利用にかかる規定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手順を定め、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。

7. 教育情報セキュリティ監査及び自己点検の実施

教育情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて教育情報セキュリティ監査及び自己点検を実施する。

8. 教育情報セキュリティポリシーの見直し

教育情報セキュリティ監査及び自己点検の結果、教育情報セキュリティポリシーの見直しが必要となった場合及び教育情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合には、教育情報セキュリティポリシーを見直す。

9. 教育情報セキュリティ対策基準の策定

上記６，７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める教育情報セキュリティ対策基準を策定する。教育情報セキュリティ対策基準は、公にすることにより本市教育委員会事務局の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

10. 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、教育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教育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本市教育委員会事務局の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。