
野洲市教育委員会
教育情報セキュリティポリシー基本方針

教育情報セキュリティポリシー基本方針

1. 目的	1
2. 定義	1
3. 対象とする脅威	1
4. 適用範囲	2
5. 教職員の遵守義務	2
6. 教育情報セキュリティ対策	2
7. 教育情報セキュリティ監査及び自己点検の実施	3
8. 教育情報セキュリティポリシーの見直し	3
9. 教育情報セキュリティ対策基準の策定	3
10. 教育情報セキュリティ実施手順の策定	3

教育情報セキュリティポリシー基本方針

1. 目的

本基本方針は、市が教育情報資産に対し、基本方針及び基本方針に基づいた対策基準を定め、教育情報資産の機密性、完全性及び可用性を維持することにより、職員や児童生徒の教育情報資産に対する脅威から守ることを目的とする。

2. 定義

(1) 教育ネットワーク

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) 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ポリシー対策基準をいう。

(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、重要情報の搾取、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因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) 教育機関等の範囲

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任用職員等を含む。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 教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体
- ② 教育ネットワーク及び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. 教職員等の遵守義務

臨時的任用教職員、非常勤講師を含めたすべての教職員及び教育委員会所属職員、市が任用した職員（以下「教職員等」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

3に規定する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、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靱性の向上

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、情報システム課サーバ室等、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

外部委託する場合には、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、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に、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実施の結果、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

この基本方針に基づき、教育情報セキュリティ対策を実施するために、具体的な遵守事項、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ものとする。

10. 教育情報セキュリティ実施基準の策定

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。