

鳥取市教育情報セキュリティポリシー

鳥取市教育情報セキュリティ基本方針

制定 令和3年4月

改定 令和7年4月

鳥取市教育委員会

改定履歴

版	改定日	施行日	改定箇所	改定内容
初	令和3年4月1日	令和3年4月1日	全章	初版発行
2	令和7年4月1日	令和7年4月1日	全章	文部科学省「教育情報セキュリティポリシーに関するガイドライン」（令和6年1月）改定及び鳥取県学校教育情報セキュリティポリシー改定（令和6年4月）、鳥取市情報セキュリティポリシー改定（令和6年4月）に伴う改定など
3				

目次

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

1 目的

鳥取市立小学校、中学校及び義務教育学校（以下「学校」という。）が学校教育の情報化を進めるにあたっては、児童・生徒、その保護者、教職員及びその他の関係者の個人情報情報を情報システムにより取り扱う機会が増大することから、個人情報を含む教育情報資産の一層適切な管理・運用が求められる。

そのため、学校が管理・運用する教育情報資産の機密性、完全性、及び可用性を確保するため、様々な脅威に対する抑止、予防、検知及び回復について、組織的かつ体系的に取り組むための統一的な方針並びに教育情報資産の安全管理対策を実施するに当たっての基本的な考え方及び方策を定めることを目的に、教育情報セキュリティポリシーを定めることとする。

2 用語の定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- (1) 教育情報ネットワーク 本市立学校で使用される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 本市立学校で使用されるコンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
- (3) 記録媒体 磁気式、光学式、半導体メモリ等、電子データとして情報を記録する媒体（ハードディスク、ソリッドステートドライブ、USBメモリ、SDカード、CD-ROM、DVD-ROM等）をいう。
- (4) 教職員等 校長、教頭、教員、任期付職員、非常勤職員、会計年度任用職員、臨時職員など、学校が保有する教育情報資産に関する業務に携わる全ての職員をいう。
- (5) 情報セキュリティ 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をいう。
- (6) 教育情報セキュリティポリシー 本基本方針及び鳥取市教育情報セキュリティ対策基準をいう。
- (7) 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。
- (8) 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。
- (9) 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。
- (10) LGWAN系ネットワーク LGWANに接続されたネットワークをいう。
インターネット系ネットワーク インターネットに接続されたネットワークをいう。
- (11) 校務系システム

校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム

(12) 校務外部接続系システム

校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ(CMS)及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム

(13) 学習系システム

学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム

3 教育情報セキュリティポリシーの位置づけ及び構成

教育情報セキュリティポリシーは、本市立学校が保有する情報資産について、総合的かつ体系的に取りまとめた教育情報セキュリティ対策の基本となるものであり、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から構成される。

教育情報セキュリティ対策基準は、教育情報セキュリティ基本方針に基づき、教育情報セキュリティ対策等を実施するために最低限必要な水準として、教職員が遵守すべき事項及び判断基準をまとめたものである。本市では、組織等の状況に合わせた教育情報セキュリティ対策基準を策定する。

4 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、ウィルス攻撃、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機器又は教育情報資産の漏えい・破壊・改ざん・消去等、重要情報の詐取、内部不正等
- (2) 機器又は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、設定・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、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、機器故障や規定外パソコン接続等の非意図的的要因による情報漏えい・破壊・消去等、アクセスのための認証情報又はパスワードの不適切管理
- (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

5 適用範囲

(1) 鳥取市教育情報セキュリティポリシーの適用範囲

鳥取市教育情報セキュリティポリシーは、鳥取市立小学校、中学校、義務教育学校及び教育委員会事務局並びに教育委員会事務局が業務を委託した外部委託事業者に適用する。ただし、市長部局が管理する情報システム（LGWAN系ネットワーク）については、市長事務局が定める情報セキュリティポリシーを適用する。

(2) 教育情報資産の範囲

教育情報セキュリティポリシーが対象とする教育情報資産は、次のとおりとする。

- ① 教育情報ネットワーク、教育情報システム及びこれらに関する設備、記録媒体
- ② 教育情報ネットワーク及び教育情報システムで取り扱う情報（印刷した文書を含む。）
- ③ 教育情報システムの仕様書及び教育情報ネットワーク図等のシステム関連文書

6 教職員等の遵守義務

教職員及び外部委託者は、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教育情報セキュリティポリシーを遵守しなければならない。

7 情報セキュリティ対策

上記4の脅威から教育情報資産を保護するため、以下のセキュリティ対策を実施するものとする。

(1) 組織体制

教育情報セキュリティにおける責任者を明確にし、その責任者に教育情報セキュリティに関する全ての権限を与える。また、専門組織を設置すると共に、組織横断的なセキュリティ推進体制を確立し、技術的対策のみならず、情報資産を取り扱う教職員への教育やセキュリティ事故発生時の対応等の教育情報セキュリティ対策を円滑に推進・管理する。

(2) 情報資産の分類と管理

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

(3) 情報システム全体の強靱性の向上

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。

(4) 物理的セキュリティ

サーバ等、通信回線等及び教職員等の端末等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、教職員等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

情報システムの監視、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、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) 業務委託と外部サービス（クラウドサービス）の利用

業務委託する場合には、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、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。

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。

(9) 評価・見直し

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情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

8 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。

9 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には、保有する情報及び利用する情報システムに係る教委の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、教育情報セキュリティポリシーを見直す。

10 教育情報セキュリティ対策基準の策定

上記7、8及び9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。

1 1 教育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本市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。