岡山市教育情報セキュリティポリシー
（抜粋版）

平成３１年３月

（令和３年２月改定）

岡山市教育委員会事務局

第１章 教育情報セキュリティ基本方針

１ 目的

教育情報セキュリティポリシーは、市立学校が所掌する情報資産に係る機密性、完全性及び可用性を維持するための対策の基準を定めることにより、学校関係者等の市民のプライバシー、財産等を保護するとともに、学校業務及び学習活動の適正な運営に資す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並びにその構成機器（ハードウェア及びソフトウェア）をいう。

（２）教育ネットワーク

教育委員会事務局が管理するネットワークであり、各市立学校において校務支援システムやインターネットの利用、学校ホームページの公開等を行うためのネットワークをいう。

（３）外部ネットワーク

インターネットや他団体が管理しているネットワークなどの本市が管理していないネットワークの総称をいう。

（４）ウェブサイト

インターネット上に公開された、文字、画像、動画等から成るホームページの集まりをいう。

（５）学校外

その学校の建物や敷地以外の場所で、当該学校が管理していない場所をいう。

（６）教育情報

岡山市情報公開条例第２条第２号に規定する「公文書」と同義とし、教職員等が職務上作成し、又は取得した文書、図画、写真、フィルム、テープ及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作成された記録をいう。以下同じ。）であって、当該学校の教職員等及び教育委員会事務局の職員等が組織的に用いるものとして、当該学校及び教育委員会事務局が保有しているものをいう。ただし、次に掲げるものを除く。

ア 官報、白書、新聞、雑誌、書籍その他不特定多数の者に販売することを目的として発行されるもの

イ 図書館その他の施設において一般の利用に供することを目的として管理されているもの

ウ 実施機関において歴史的若しくは文化的な資料又は学術研究用の資料として特別の管理がなされているもの

（７）情報システム

コンピュータ（ハードウェア及びソフトウェア）、ネットワーク及び電磁的記録媒体で構成された、情報処理を行う仕組みをいう。

（８）校務系情報
　児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報をいう。

（９）校務系サーバ
　校務系情報を取り扱うサーバをいう。

(10) 校務用端末
　校務系情報にアクセス可能な端末をいう。

(11) 校務系ネットワーク
　校務系サーバと校務用端末の通信及びインターネット接続を取り扱うネットワークをいう。

(12) 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をいう。

(13) 学習系情報
　児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それらの情報を学校における教育活動において活用することを想定しており、かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報をいう。

(14) 学習系サーバ
　学習系情報を取り扱うサーバをいう。

(15) 学習者用端末
　学習系情報にアクセス可能な端末で、児童生徒が利用する端末をいう。

(16) 指導者用端末
　学習系情報にアクセス可能な端末で、教員のみが利用可能な端末をいう。

(17) 学習系ネットワーク
　学習系サーバと学習者用端末・指導者用端末の通信及びインターネット接続を取り扱うネットワークをいう。

(18) 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をいう。

(19) 校務外部接続系情報
　校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報をいう。

(20) 校務外部接続系サーバ

校務外部接続系情報を取り扱うサーバをいう。

(21) 校務外部接続系システム
メールサーバ、ホームページ運用サーバ及び校務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

(22) 教育情報システム
教育ネットワーク及び校務系システム、校務外部接続系システム及び学習系システムを併せた総称をいう。

(23) NAS (Network Attached Storage)
ハードディスクとコントローラから構成され、ネットワークに接続して複数の端末でファイルを共有するためのストレージ機器をいう。

(24) 公開系システム
情報システムの中で、ウェブサーバ等外部ネットワークへの公開を目的としたシステムをいう。

(25) 情報資産
教育情報システム及び教育情報システムで取り扱う教育情報をいう。

(26) 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。

(27) 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。

(28) 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。

(29) 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。

(30) 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。

(31) 情報セキュリティ事故（情報セキュリティインシデント）
不正アクセス、ウイルス感染、ハードウェア・ソフトウェア障害、人為的ミス等により、情報資産の漏えい・破壊・改ざん・消去や情報システムのサービス停止等が発生することをいう。

(32) 全庁ネットワーク管理者
庁内LANの運用管理の統括及び総合調整を行う情報システム管理者であり、総務局総務部情報システム課長をもって充てる。

（33）情報セキュリティ推進本部
「岡山市情報セキュリティ推進本部設置規程」第１条に基づき、情報セキュリティ対策を組織的かつ継続的に推進していくために設置する組織をいう。

（34）最高情報セキュリティ責任者（副市長（総務局担当））
最高情報セキュリティ責任者（CISO：Chief Information Security Officer、以下「CISO」という。）は、本市における全ての情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（35）情報セキュリティインシデント統括窓口（CSIRT）
情報セキュリティ事故に関する統一的な窓口として、CISO補佐（最高情報セキュリティ責任者補佐：総務局長）の下に置かれる組織をいう。

（36）岡山市情報セキュリティポリシー（平成25年6月策定）
市長事務部局及び区役所、他部局を適用範囲とし、本市が所掌する情報資産について、セキュリティの脅威から機密性、完全性及び可用性を維持するための対策基準等をいう。

３ 対象とする脅威

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

（１）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃、内部不正等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、サービス停止等

（２）無許可のハードウェア、不正な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、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、機器故障等の偶発的要因による情報資産の漏えい・破壊・消去等

４ 適用範囲

（１）行政機関等の範囲
本基本方針が適用される行政機関等は、市立学校（小学校、中学校、高等学校をいう。以下同じ。）及び教育委員会事務局（教育情報システムの利用や開発、管理等に関すること）とする。

（２）情報資産の範囲
本基本方針が対象とする情報資産は、次のとおりとする。

ア 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
イ 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。）
ウ 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

教職員等（教職員、非常勤教職員及び臨時教職員をいう。以下同じ。）は、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を遵守しなければならない。

６ 情報セキュリティ対策

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

（１）組織体制

市立学校の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（２）情報資産の分類と管理

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行う。

（３）物理的セキュリティ

サーバ、情報システム室、通信回線、LANケーブル及び教職員等、児童生徒が利用するパソコン等の端末並びに情報資産を取り扱うその他の設備及び機器の管理について、物理的な対策を講じる。

（４）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。

（５）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。

（６）運用

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、情報セキュリティ事故が発生した場合等に迅速かつ適切に対応するため、緊急時対応手順を策定する。

（７）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、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 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

情報セキュリティ自己点検等の結果、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又は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。

１０ 教育情報セキュリティ実施手順の策定

情報セキュリティに関する対策の具体的な実施手順は、教育情報セキュリティポリシーで定める教育情報セキュリティ対策基準に基づき、学校共通の実施手順として策定及び必要に応じて見直しを行うものとする。

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情報セキュリティ事故を誘発する可能性があり、また、業務等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。

附 則

この基本方針は、平成３１年３月１日から施行する。

この基本方針は、令和３年２月１日から施行する。