可児市教育情報セキュリティポリシー

可児市教育委員会

第1.1版

令和８年４月１日

改定履歴

版数	施行日	内容
―	令和 6 年 4 月 1 日	初版
第 1.1 版	令和 8 年 4 月 1 日	見直しによる一部改正

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、学校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ため、学校等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）教職員等

市内小中学校及びその他市教育委員会が設置又は管轄する施設（教育委員会事務局、教育支援センター等）において、教育、研究、学習支援、相談業務及び組織運営に従事する全ての者をいう。これには、教員（常勤・非常勤を問わず）、事務職、技術・技能職、外部専門職、教育委員、及びそれらに準ずる職種を含む。

（２）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。

（３）教育情報システム・校務系/学習系システム

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。校務系とは教職員等が事務等に使用するものをいう。学習系とは児童生徒が学習に使用するものをいう。

（４）情報資産

学校等が保有する電磁的記録や紙媒体のデータ、及びそれらを扱う情報システムをいう。

（５）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。

（６）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。

（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。

（９）教育情報セキュリティインシデント

情報漏えい、紛失、不正アクセス、ウイルス感染など、教育情報セキュリティ上の問題が発生した状態、またはそのおそれがある状態をいう。

(10) SaaS型パブリッククラウドサービス

インターネット経由で提供される、教育用アプリや外部ストレージなどのクラウドサービスをいう。

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、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情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）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、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）行政機関の範囲

本基本方針が適用される機関は、地方教育行政の組織及び運営に関する法律（以下「法」という。）第2条に規定する可児市教育委員会、法第17条に規定する事務局、及び法第30条に規定する教育機関のうち、市立小中学校、教育支援センターその他教育委員会が設置する施設とする。

（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。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③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．教職員等の順守義務

教職員等は、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

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

（２）情報資産の分類と管理

学校等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、当該分類に基づき教育情報セキュリティ対策を実施する。

（３）物理的セキュリティ

サーバ、通信回線及び教職員等のパソコン等の管理について、物理的な対策を講じる。

（4）人的セキュリティ

教育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、業務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。

（7）SaaS 型パブリッククラウドサービスの利用

利用する SaaS 型パブリッククラウドサービスの情報セキュリティ対策を確認し、約款による外部サービスの利用に係る規定の整備、ソーシャルメディアサービスの利用に係る運用手順を定めることで、教育情報セキュリティを確保するものとする。

（8）評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。教育情報セキュリティポリシーの見直しが必要な場合は、適宜教育情報セキュリティポリシーの見直しを行う。

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になった場合には、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。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本市の教育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の教育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。