常滑市
教育情報セキュリティポリシー
＜基本方針＞

令和８年３月 31 日　初版

常滑市教育委員会

改版履歴

版数	策定（改定）日	備考
初版	令和８年３月 31 日	

目次

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

基本方針

１．目的

本基本方針は、常滑市教育委員会及び学校（小学校、中学校をいう。以下同じ。）が保有する情報資産の機密性、完全性及び可用性を維持し、ICT を安全かつ効果的に教育活動へ活用できる環境を整えるため、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）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

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）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、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人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障害からの波及等

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、教育委員会及び学校とする。

（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 教育ネットワーク及び教育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 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．職員等の遵守義務

教育委員会及び学校に属するすべての教職員、非常勤職員及び会計年度任用職員等（以下「職員等」という。）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及び実施手順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、以下のセキュリティ対策を講じる。

（１）組織体制

教育委員会及び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ための組織体制を確立する。

（２）情報資産の分類と管理

本市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）物理的セキュリティ

サーバ、サーバ室、通信回線、教職員用端末及び児童生徒用端末の管理について、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、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）児童生徒に対する情報セキュリティ対策

児童生徒に対して、ICT の利用に伴う責任や情報モラル、情報セキュリティの重要性について、発達段階に応じた指導及び啓発を行う。

（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、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。また、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の危機管理対策を講じる。

（８）業務委託と外部サービスの利用

① 業務委託

業務委託を行う場合には、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。

② クラウドサービス

学習系システムや校務系システム等においてクラウドサービスを利用する場合には、情報の格付けに応じた適切なセキュリティレベルが確保されたサービスを選定するとともに、利用にかかる設定や運用規定を整備し、対策を講じる。

③ ソーシャルメディアサービス

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、責任者を定める。

④ 生成 AI サービス

生成 AI サービスを利用する場合には、教育委員会が別途定めるガイドライン等を遵守し、適切に利用するものとする。

（９）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．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に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の見直しを行う。

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、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学校毎に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、非公開とする。