<平塚市教育情報セキュリティポリシー>

＜平塚市教育情報セキュリティ基本方針＞

令和４年４月１日

１　目的

本市では、本市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、「平塚市情報セキュリティ基本方針（平成２７年１月１日）」を定めているが、学校（市立小学校、中学校を言う。以下同じ。）においては、コンピュータを活用した学習活動の実施など、教職員はもとより、児童・生徒が日常的に情報システムにアクセスする機会がある。このことは、平塚市情報セキュリティ基本方針の適用範囲である行政機関（市長部局、行政委員会等事務局、消防及び市民病院事務局）の行政事務とは異なる特徴である。

よって、本市教育委員会及び学校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、平塚市教育情報セキュリティ基本方針（以下「基本方針」という。）を定める。

本基本方針は、本市教育委員会及び学校が実施する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

この基本方針において、次の各号に掲げる用語の定義はそれぞれ当該各号に定めるところによる。

（１）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。

（２）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。

（３）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。

（４）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。

（５）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。

（６）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。

（７）教育情報システム

本市教育委員会及び学校が、学校教育に資する目的で導入・管理する情報システムのことをいい、校務系情報システム及び教育系情報システムの総称をいう。

（８）情報資産

ネットワーク、情報システム及びこれらで取り扱う情報をいう。

（９）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。

（１０）校務系

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ための情報を取

り扱う校務支援システムに関わる情報システム及びその情報システムで取り扱うデータをいう。

（１１）教育系

学校の授業で用いる教材、児童・生徒が作成したワークシート及び作品など、教育活動において活用するための情報を取り扱う教育用の情報システム及びその情報システムで取り扱うデータをいう。

（１２）通信環境の分離

校務系と教育系の通信環境を分離することをいう。

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、重要情報の搾取、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、外部委託管理者の不備、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行政機関は、本市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、本市教育委員会及び学校が保有する情報資産とする。

５　教職員等の遵守義務

本市教育委員会の一般職員、再任用職員、任期付職員、パートタイム会計年度任用職員及び学校の教職員（非常勤職員や臨時的任用職員も含む）（以下「教職員等」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、業務の遂行にあ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　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

本市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組織体制を確立する。

（2）情報資産の分類と管理

本市教育委員会と学校が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）情報システム全体の強靭性の向上

情報システム全体に対し、次の対策を講じる。

ア　校務系と教育系においては、相互通信ができないようにする。

イ　校務系及び教育系においては、不正通信の監視機能の強化等の高度な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、情報システム室等、通信回線等及び教職員等のパソコンの管理について、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

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、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

外部委託等をする場合（クラウドサービス利用を含む）には、選定した外部委託事業者等において、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たうえで、委託契約を締結又はサービス利用契約等を締結する。

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教育委員会及び学校の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、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教育委員会及び学校の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。