報告第７２号

東広島市教育情報セキュリティポリシーの策定について

１　教育情報セキュリティポリシーとは

学校が保有する情報資産を、漏えいや不正アクセス、データの改ざん、情報の滅失などの脅威から守るための方針や対策をまとめたもの。

２　目　的

学校が保有する情報資産を様々な脅威から守るとともに、対策の導入や運用を通して、情報管理に係る組織体制の見直しや情報セキュリティに対する教職員の意識向上につなげる。

３　経　緯

本市では、これまで「東広島市情報システム等管理運営規程」及び「東広島教育委員会情報ネットワークシステム運用管理要綱」に基づき、教育情報システム等の運用管理を行ってきたが、ＧＩＧＡスクール構想の推進に伴い、１人１台端末を活用するために必要なセキュリティ対策やクラウドサービスを利用する際の課題に対応する必要が生じた。

これらに対応するため、文部科学省から、地方公共団体の教育情報セキュリティポリシーの策定や見直しの指針として、「教育情報セキュリティポリシーに関するガイドライン」が示された。

この流れを受け、この度「東広島市教育情報セキュリティポリシー」を新規に策定した。

今回の「東広島市教育情報セキュリティポリシー」の策定に伴い、「東広島市教育委員会情報ネットワークシステム運用管理要綱」は廃止する予定としている。

東広島市教育情報セキュリティ基本方針

1　目的

東広島市教育委員会及び市立小・中学校において各情報システムで取り扱う情報には、児童生徒の個人情報のみならず、学校運営に関する情報など、校外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、児童生徒、保護者等の財産、プライバシー等を守るため、事務の安定的な運営のために必要不可欠であり、ひいては、このことが本市教育行政に対する市民からの信頼の維持向上に寄与するものである。

また、児童生徒の学習の多様化（ＩＣＴを活用した自宅学習、個別最適化された学び等）や、その実現に向けた教職員の働き方改革など、Society5.0 時代における社会構造や雇用環境の変化に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、学校関係の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために東広島市教育情報セキュリティポリシーを定めることとする。このうち情報セキュリティ基本方針については、学校関係の情報資産においても、本市全体の基本方針と同一のものであるとの認識から、東広島市情報セキュリティポリシーを準用するものとする。

2　定義

(1) 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。

(2) 機密性(confidentiality)
　情報にアクセスすることを認可された者だけが、情報にアクセスできることを確保することをいう。

(3) 完全性(integrity)
　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(availability)
　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) 教職員
　学校教育法（昭和 22 年法律第 26 号）第 37 条及び第 49 条に規定する者で、市立小・中学校に従事する職員、並びにその他の支援員等をいう。

(6) 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、教職員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒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。

(7) 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。

(8) 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、かつ当該情報に教職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。

(9) 校務用端末
　校務系情報にアクセス可能な端末をいう。

(10) 校務外部接続用端末
　校務外部接続系情報にアクセス可能な端末をいう。

(11) 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。

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

(13) 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。

(14) 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、ホームページ管理サーバ（CMS)、市民ポータルサイト（CRM）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をいう。
(15) 学習系システム
学習系ネットワーク、学習系サーバ及び学習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。
(16) 教育ネットワーク
市立小・中学校の各室、本庁舎及びデータセンターの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。
(17) 教育情報システム
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の総称をいう。
(18) 通信経路の分割
校務系システム、校務外部接続系システム、学習系システムの各環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。
(19) 無害化通信
インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3　適用範囲
(1) 行政機関の範囲
東広島市教育情報セキュリティポリシーが適用される行政機関は、本市教育委員会学校教育部及び市立小・中学校とする。
(2) 情報資産の範囲
東広島市教育情報セキュリティポリシー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、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
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

4　東広島市教育情報セキュリティポリシーの位置付けと教職員等の義務
東広島市教育情報セキュリティポリシーは、学校関係の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、学校における情報セキュリティ対策の頂点に位置するものである。
したがって、教育委員会の長及び職員、教職員及び外部委託事業者（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の「対策基準」を遵守する義務を負うものとする。

5　情報セキュリティ管理体制
学校関係の情報資産について、管理職が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

6　情報資産の分類
情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

7　情報資産への脅威
東広島市教育情報セキュリティポリシーを策定する上で、情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。
(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、外部委託管理の不備、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、火災等の災害並びに事故、故障等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

8　情報セキュリティ対策

上記７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ずるものとする。

(1) 物理的セキュリティ対策

教育情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

(2) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての教職員等に教育情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

(3) 技術的及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適正に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、システム開発等の外部委託、ネットワークの監視、教育情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。その他、緊急事態が発生した際に迅速な対応を可能とするための緊急時対応計画を策定する。

(4) 教育情報システム全体の強靭性の向上

教育情報システム全体に対し、次の二段階の対策を講じる。

① 校務系システム、校務外部接続系システム、学習系システムの各情報システムとの通信経路を分割する。なお、各システム間で通信する場合には、無害化通信を実施する。

② 校務外部接続系システム、学習系システムにおいては、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。

(5) 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。

9　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、定期的また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。

10　評価及び見直しの実施

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を取り巻く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の見直しを実施する。

11　教育情報セキュリティ対策基準の策定

上記８、９及び 10 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統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した教育情報セキュリティ対策基準を策定するものとする。

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学校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。

12　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学校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。

令和３年１１月１７日　策定
東広島市長