東久留米市教育情報セキュリティポリシー

（情報セキュリティ基本方針）

東　久　留　米　市

令　和　５　年　４　月

（令和８年３月改定）

目次

1 目的

本基本方針は、東久留米市（以下「本市」という。）の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、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

（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

本基本方針及び教育情報セキュリティ対策基準をいう。

（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。

（8）インターネット接続系システム

インターネットメール等に関わるインターネットに接続された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。

（9）校務系情報

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。

（１０）校務外部接続系情報
　ネットワーク分離による対策を講じたシステム構成において、インターネット接続を前提として、校務で利用される情報校務系情報をいう。

（１１）学習系情報
　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。

（１２）校務用端末
　校務系情報にアクセス可能な端末をいう。

（１３）校務外部接続用端末
　ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報にアクセス可能な端末をいう。

（１４）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。

（１５）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。

（１６）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及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステムをいう。

（１７）校務外部接続系システム
　ネットワーク分離による対策を講じたシステム構成において、校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）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。

（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及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステムをいう。

（１９）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を合わせた総称をいう。

（２０）校務外部接続系サーバ
　ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報を取り扱うサーバをいう。

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）行政機関等の範囲

本基本方針が適用される行政機関等は、本市の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学校における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学校における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 教職員等の遵守義務

教職員、再任用職員及び会計年度任用職員等（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

学校が保有する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

学校が保有する情報資産について、情報セキュリティ対策を推進する教育委員会の組織体制を確立する。

（2）情報資産の分類と管理

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

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）一人一台端末におけるセキュリティ

GIGA スクール構想における一人一台端末の整備に伴い、学校内外で利用する学習者用端末に対してのセキュリティ対策を講じる。

（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、必要に応じて自己点検を実施し、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・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 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教育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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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

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の教育情報セキュリティ運営に重大な支障を及ぼす恐れがあることから非公開とする。