【A】

羽村市教育委員会	教育情報セキュリティ基本方針（第４版）

羽村市立学校
教育情報セキュリティ基本方針

制定	2010 年 4 月	最終改定	2026 年 4 月

【A】

羽村市教育委員会	教育情報セキュリティ基本方針（第４版）

目　　次

制定	2010 年 4 月	最終改定	2026 年 4 月

羽村市立学校教育情報セキュリティ基本方針

１　目的

羽村市立学校教育情報セキュリティ基本方針（以下「基本方針」という。）は、羽村市情報セキュリティ基本方針に基づき、羽村市教育委員会及び羽村市立学校が保有する教育情報に関する情報資産を様々な脅威から組織的、体系的かつ継続的に保護するための統一的な方針並びに情報資産の安全管理対策を実践するにあたっての基本的な考え方及び方策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意義は、当該各号に定めるところによる。

(1)　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及びその構成機器（ハードウェア及びソフトウェア）をいう。

(2)　教育情報システム

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)　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。

(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

インターネットに接続された教育情報システム及びその教育情報システムで取り扱うデータをいう。

(9)　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　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、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

この基本方針は、羽村市立学校の教育情報を取り扱う羽村市教育委員会職員及び、羽村市立学校に所属する職員（以下これらを「職員等」という。）に適用する。

５　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、教育情報システム、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。） 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

６　職員等の責務

職員等は、教育情報セキュリティ対策の重要性について共通の認識をもつとともに、業務の遂行において、基本方針を遵守しなければならない。

７　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
教育情報セキュリティ対策を推進及び管理するための組織体制を整備する。

(2) 情報資産の分類と管理
情報資産を価値等により分類し、当該分類に基づき情報資産の適切な管理を実施する。

(3) 物理的セキュリティ対策

サーバ、電子計算室、通信回線及び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) 人的セキュリティ対策

教育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) 技術的セキュリティ対策

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) 外部委託管理

事務事業を委託した場合における教育情報セキュリティを確保するため、外部委託管理を実施する。

８　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。

９　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教育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、リスクを検討した上で、教育情報セキュリティポリシーを見直す。

１０　教育情報セキュリティ対策基準の策定

上記７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。

１１　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。