羽曳野市学校教育情報セキュリティポリシー

令和８年３月

序章：羽曳野市学校教育情報セキュリティポリシーの構成

羽曳野市学校教育情報セキュリティポリシーとは、羽曳野市教育委員会（以下「教育委員会」という。）及び羽曳野市立小学校・中学校・義務教育学校（以下「学校」という。）が所掌する情報資産（以下「情報資産」という。）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を総称する。

羽曳野市学校教育情報セキュリティポリシーは、情報資産に関する業務に携わる職員等に浸透、普及、定着させるものであり、安定的な規範であることが要請される。また学校においては、児童生徒による教育情報システムの活用も進む中で、児童生徒も想定した情報セキュリティ対策を柔軟に講じる必要がある。

そのため、このポリシーは、本市セキュリティポリシー「基本方針」に準じて定めた教育委員会及び学校が所掌する情報資産の「基本方針」と学校を想定した「対策基準」の２階層に分けて策定することとする。

学校教育情報セキュリティポリシーの構成

文書名		内容
羽曳野市学校教育情報セキュリティポリシー	基本方針	羽曳野市情報セキュリティポリシーに準じた統一的かつ基本的な方針。
	対策基準	教育委員会及び学校を想定した情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
学校教育情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

第１章：羽曳野市学校教育情報セキュリティ基本方針

１．目的

教育委員会及び学校の各情報システムが取り扱う情報には、教職員等及び児童生徒の個人情報のみならず学校教育運営上重要な情報など、外部への漏洩等が発生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、情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、教職員等及び児童生徒のプライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが羽曳野市学校教育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、近年のいわゆる IT 革命の進展により、教育行政及び学校教育の DX などの実現が期待されるところである。教育委員会及び学校がこれらに積極的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、羽曳野市学校教育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)を整備するために羽曳野市学校教育情報セキュリティポリシーを定めることとし、このうち、教育情報セキュリティ基本方針については教育委員会及び学校の情報セキュリティ対策の基本的な方針として、学校教育情報セキュリティポリシーの対象、位置付け等を定めるものとする。

２．用語の定義

本ポリシーにおける用語は、以下のとおりとする。

用語	定義
機密性	認可された者だけが確実に情報にアクセスできることをいう。
完全性	情報及び処理の方法の正確さ及び完全である状態を安全防護することをいう。
可用性	許可された利用者が必要なときに情報にアクセスできることを確実にすることをいう。
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、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。
校務外部接続系情報（公開系情報）	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。
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。
校務用端末	校務系情報にアクセス可能な端末をいう。
学習者用端末	学習系情報にアクセス可能な端末で教職員および児童生徒が利用する端末をいう。
公会計システム用端末	公会計システムに接続可能な端末で、庁内端末と同等のセキュリティ設定が施された端末をいう。
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。
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。
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。
公会計システム	LGWAN ネットワークを利用した公会計情報を取り扱うシステムをいう。
校務系サーバ	校務系情報を取り扱うサーバをいう。
学習系サーバ	学習系情報を取り扱うサーバをいう。
教職員	学校の教職員（会計年度任用職員、非常勤職員、任期付き職員及び臨時的任用職員を含む。）をいう。
教職員等	教育委員会の職員及び学校の教職員をいう。
職員等	教職員並びに情報資産に関する業務に携わる外部委託事業者及び派遣労働者をいう。

３．学校教育情報セキュリティポリシーの位置付けと教職員及び職員等の義務

学校教育情報セキュリティポリシーは、教育委員会及び学校が所掌する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、学校教育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、羽曳野市教育長をはじめとして職員等は、学校教育情報セキュリティ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当たって学校教育情報セキュリティポリシー及び実施手順を遵守する義務を負うものとする。

４．学校教育情報セキュリティ管理体制

情報資産について、所属長及び学校長が率先して学校教育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。

５．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。

６．情報資産への脅威

学校教育情報セキュリティポリシーを策定するうえで、情報資産を脅かす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）部外者の侵入による機器又は情報資産の破壊・盗難、故意の不正アクセス又は不正操作による機器又は情報資産の破壊・盗聴・改ざん・消去等

（２）職員等による機器又は情報資産の持出、誤操作、アクセスのための認証情報又はパスワードの不適切管理、故意の不正アクセス又は不正行為による破壊・盗聴・改ざん・消去等、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏洩等

（３）コンピュータウイルス、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

７．学校教育情報セキュリティ対策

６．で示した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）物理セキュリティ対策

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、職員等に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切に保護するため、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、また、システム開発等の外部委託、ネットワークの監視、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。

また、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危機管理対策を講ずる。

８．学校教育情報セキュリティ対策基準の策定

学校教育の様々な情報資産について、上記７の情報セキュリティ対策を講ずるにあた

っては、遵守すべき行為及び判断等の基準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学校教育情報セキュリティ対策基準を策定するものとする。

９．学校教育情報セキュリティ実施手順の策定

学校教育情報セキュリティ対策基準を遵守して学校教育情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、教育委員会及び学校が所掌する情報資産の学校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、学校教育情報セキュリティ実施手順は、公にすることにより教育委員会及び学校の運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。

１０．学校教育情報セキュリティ監査の実施

学校教育情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施する。

（１）教育委員会は、情報セキュリティ対策の実効性を確保するため、情報セキュリティ監査を計画的に実施しなければならない。

（２）学校は、毎年度、学校教育情報セキュリティポリシー及び関連規程の遵守状況について自己点検を行い、その結果を教育委員会に報告しなければならない。

（３）監査及び自己点検は、情報資産管理、アクセス権限、物理的・人的・技術的対策、委託先管理、インシデント対応等の項目を含め、改善が必要な事項を明確化し、是正措置を講じることを目的とする。

（４）監査及び自己点検の結果は記録し、適切に保管するとともに、次回の監査計画及びセキュリティ対策の改善に反映しなければならない。

１１．評価及び見直しの実施

学校教育情報セキュリティ監査の結果等により、学校教育情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、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に、学校教育情報セキュリティポリシーの見直しを実施する。