仁淀川町教育情報セキュリティポリシー

仁淀川町教育委員会

令和８年４月

仁淀川町教育情報セキュリティポリシーの策定について

１．目的

仁淀川町教育委員会及び学校が取り扱う情報には、児童、生徒、保護者、職員等の個人情報のみならず、学校運営上重要な情報など、外部に漏えいした場合に極めて重大な結果を招く情報が多数含まれている。

従って、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、プライバシーを守るためにも、また、事務の安定的な運営のためにも必要不可欠である。

また、学校教育においては、文部科学省の「GIGA スクール構想の実現」に基づき、児童生徒１人１台タブレット端末の整備が進み、情報活用能力の育成やプログラミング教育等を実施することとなっているなど、より一層の教育の情報化が求められている。学校がこれら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前提条件となる。

そのため、仁淀川町教育委員会及び学校が取り扱う情報資産をさまざまな脅威から保護し、機密性、完全性及び可用性を維持するための情報セキュリティ対策を整備するために、仁淀川町教育情報セキュリティポリシー（以下「教育情報セキュリティポリシー」という。）を定めることとする。

なお、行政機関には、町長部局が策定した仁淀川町情報セキュリティポリシーも適用されることから、当該セキュリティポリシーが適用される範囲においては当該セキュリティポリシーも遵守しなければならない。

２．構成

教育情報セキュリティポリシーは、教育行政機関が保有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る。

教育情報セキュリティポリシーは、教育行政機関が保有する情報資産を取り扱う全ての職員に浸透、普及及び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。一方で、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に対し柔軟に対応することも必要である。

このようなことから、教育情報セキュリティポリシーは、一定の普遍性を備えた部分としての「仁淀川町教育情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に対応する部分としての「仁淀川町教育情報セキュリティ対策基準」から構成する。

【教育情報セキュリティポリシーの構成】

文書名	内容	
教育情報セキュリティポリシー	仁淀川町教育情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	仁淀川町教育情報セキュリティ対策基準	仁淀川町教育情報セキュリティ基本方針を実行に移すための全ての情報システムに共通の情報セキュリティ対策の基準

また、本ポリシーに基づき、具体的な情報セキュリティ対策の実施手順として「情報セキュリティポリシー実施手順」を策定する。

仁淀川町教育情報セキュリティ基本方針（公開）

第１ 趣旨

仁淀川町教育委員会及び町立学校が管理する情報資産を適切に取り扱い、情報セキュリティを確保するための基本的な方針を定めるものとする。

第２ 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、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、水害、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

第３ 職員の責務

職員は、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は、法令、教育情報セキュリティポリシー及び情報セキュリティ実施手順を遵守し、情報資産の適切な管理に努めなければならない。

また、職員は、情報資産を取り扱う事務の全部又は一部を事業者に委託する場合は、法令、教育情報セキュリティポリシー及び情報セキュリティ実施手順を遵守させるために必要な措置を講ずるものとする。

第４ 情報セキュリティ管理体制

情報セキュリティ対策を推進、管理するための体制及び役割を定めるものとする。

第５ 情報資産の分類

情報資産は、その重要性に応じて分類し、適正な管理を行うこととする。

第６ 情報セキュリティ対策の実施

情報資産を管理し、又は利用する所属の長は、情報資産に対する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を行わなければならない。

（１）物理的セキュリティ対策

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講ずる物理的な対策をいう。

（２）人的セキュリティ対策

情報セキュリティに関する職員の責務を定め、職員等に情報セキュリティ対策を周知徹底する等、十分な教育及び啓発を行うために講じる人的な対策をいう。

（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の、コンピュータ等の管理、アクセス制御、マルウェア対策、不正アクセス対策等の技術的対策をいう。

また、ネットワーク管理等の技術面の対策及び情報システム開発等の外部委託、外部サービスの利用、

情報セキュリティ対策の実施状況を確認する等の運用面における対策をいう。

（４）障害時におけるセキュリティ対策

情報セキュリティに係る障害が発生した場合に迅速な対応を可能とするために講じる緊急時の対策をいう。

第７ 情報セキュリティ対策基準の策定

情報セキュリティ対策を講ずるにあたり、遵守すべき行為及び判断等の基準を明らかにするため、「教育情報セキュリティ対策基準」を定めるものとする。

第８ 情報セキュリティ実施手順書の作成等

情報システムを管理する者は、自らが管理する情報システムについて、教育情報セキュリティ対策基準に定める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まとめた、情報セキュリティ実施手順を作成しなければならない。

また、情報システムを管理する者は、情報セキュリティを確保するため、情報セキュリティ対策の実施状況の点検を行い、必要に応じて情報セキュリティ実施手順の見直しを行うものとする。

なお、情報セキュリティ実施手順は公表しないものとする。

第９ 情報セキュリティの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について、必要に応じて点検又は監査を実施する。

第10 教育情報セキュリティポリシーの見直し

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又は、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な対策が必要になった場合は、教育情報セキュリティポリシーの見直しを行うものとする。

附則

（施行期日）

１ この基本方針は、令和８年４月１日から施行する。