邑南町立学校教育情報セキュリティポリシー

令和 7 年 12 月

邑南町教育委員会

第１　目的

GIGA スクール構想第 1 期では、全国的にひとり 1 台端末の整備とクラウドサービスの導入が一気に進み、邑南町立小学校及び中学校(以下「学校」という。)においても、令和元年度以降、この構想に基づくひとり 1 台端末の更新やデジタル利活用支援員の配置など、公立小中学校のデジタル環境の充実により「主体的・対話的で深い学び」の実現に不可欠なツールとして端末利用が定着している。

その過程で蓄積された児童生徒の学習データ、教職員の人事情報、学校運営データなど、多様な情報資産をクラウド環境で安全に管理するためには、セキュリティに関するルールづくりや運用体制の整備が昨今の急激な変化に追い付いていない現状がある。

また、企業や公共機関での情報漏えいやサイバー攻撃のニュースが頻繁に報じられ子どもたちの大切な情報を扱う教育現場も例外ではない状況となっており、従来の「校内ネットワーク内は安全」という前提は通用せず、すべてのアクセスを検証・認証する新しいセキュリティモデルへの対応がこれまで以上に必要となっている。

この現状を踏まえ、令和 7 年 3 月、文部科学省による「教育情報セキュリティポリシーに関するガイドライン」が第 3 版に改定がなされた。この改定は単なる内容更新ではなく、教育現場のデジタル化が急速に進む中で、各教育委員会が直面している現実的な課題への対応策を示すものであり、今後展開される GIGA 第 2 期、そして次世代校務 DX でのクラウド環境とゼロトラスト環境がシステム構築の基盤となることを踏まえた新たなセキュリティポリシーの整備が各自治体に求められている。

それを受けて邑南町教育委員会(以下「教育委員会」という。)において、文部科学省の「教育情報セキュリティポリシーに関するガイドライン(令和 7 年 3 月版)」を参考に、児童生徒の学習データ、教職員の人事情報、学校運営データなど、多様な情報資産をクラウド環境で安全に管理するには、これまで以上に詳細で実効性のあるセキュリティポリシーが不可欠であるため、「邑南町立学校教育情報セキュリティポリシー」(以下「このポリシー」という。)を策定するものとする。

第２　構成

このポリシーは、学校で扱う情報資産(校務系情報、学習系情報)に対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、学校が保有する情報資産を取扱う全教職員に浸透、定着させるものであることから、安定した統一的な規範であることが求められる。

一方、情報処理や通信技術の進歩による急速な環境の変化に柔軟に対応することも必要であることから、教育情報セキュリティ対策における統一的な規範として基本的な考え方を定める「教育情報セキュリティ基本方針」と、情報資産を取り巻く環境の変化に柔軟に対応していくための「教育情報セキュリティ対策基準」の 2 部構成として策定する。

なお、学校に敷設されている行政系ネットワークの取扱いについては、「行政手続における特定の個人を識別するための番号の利用等に関する法律」(平成 25 年法律第 27 号)、「邑

南町個人情報保護条例」（平成 16 年邑南町条例第 17 号）、その他の関係法令及び邑南町情報セキュリティポリシーに準拠するものとする。

第 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. サイバー攻撃

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・消去等

2. 内部からの脅威

内部不正、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則違反、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. 情報資産の漏えい、破壊、改ざん、消去

意図的あるいは過失によるもの、重要情報の搾取等

4. 物理的要因

地震、落雷、火災等の災害によるサービス及び業務の停止、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、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 4　対象範囲及び用語説明

1. 行政機関等の範囲

このポリシーが適用される行政機関等は、学校及び教育委員会とする。

2. 情報資産の範囲

このポリシーが対象とする情報資産は、以下のとおりとする。

（1）教育ネットワーク、教育情報システム、これらに関する施設・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扱う情報
（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

情報資産の種類	情報資産の例
教育ネットワーク	情報資産を扱う通信回線、ルータ等の通信機器
教育情報システム	情報資産を扱うサーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア、クラウドサービス等
教育ネットワーク及び教育情報システムに関する施設・設備	情報資産を扱うコンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
電磁的記録媒体	情報資産を扱うサーバ装置(クラウドサービスを除く)、端末、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ、SD カード等の外部電磁的記録媒体

教育ネットワーク及び教育情報システムで取扱う情報	教育ネットワーク、教育情報システムで取扱うデータ(これらを印刷した文書を含む。)
教育情報システム関連文書	教育情報システム関連のシステム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図、クラウドサービス契約関連文書等

第5　教育情報セキュリティ対策

情報資産を脅威「第1章 教育情報セキュリティ基本方針 第3 対象とする脅威」から保護するため、以下に定める教育情報セキュリティ対策を立てるものとする。

1. 管理体制

情報資産を管理し、機密性、完全性及び可用性を維持するための体制を確立する。

2. 情報資産の分類と管理

学校の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

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・盗難等から保護するために施設整備等の物理的な対策を立てるよう努める。

4. 人的セキュリティ

教育情報セキュリティに関する権限や責任を定めるとともに、全教職員等にこのポリシーを周知徹底させるための教育及び啓発を行う等の必要な対策を立てるよう努める。

5. 技術的セキュリティ

情報資産を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、不正プログラム対策ソフトウェアの導入等の技術面における対策を立てるよう努める。

6. 運用

(1) 情報システムの監視、このポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、このポリシーの運用面の対策を立てるよう努める。

(2) 情報セキュリティが侵害される事態が発生した場合に、被害の拡大防止、復旧等を迅速かつ的確に実施するため、緊急時対応計画を整備する。また、侵害に備えた対応訓練の定期的な実施等の対策をとるよう努める。

7. 外部サービスの利用

(1) 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とるよう努める。

(2) 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立てるよう努める。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、利用できるソーシャルメディアごとの責任者を定める。

第６　監査及び自己点検

このポリシーの遵守状況を検証するため、必要に応じて監査を受け、定期的に点検を実施する。

第７　評価及び見直しの実施

監査又は点検の結果等により、このポリシーに定める事項、及び教育情報セキュリティ対策の評価を行うとともに、情報システムの変更や新たな脅威の発生等、状況の変化に迅速かつ的確に対応するため、必要に応じてこのポリシーの見直しを実施する。