那珂市小中学校情報セキュリティポリシー

那珂市教育委員会

第１章（情報セキュリティ基本方針）

１　目的

現在、那珂市立小中学校（以下「学校」という。）においては、那珂市学校情報化推進計画「那珂市Edtech プラン」に基づき、小中一貫教育による９年間の系統的・連続的な学びを通して児童生徒一人一人が情報活用能力等のこれからの時代に必要な資質・能力の育成と、学校教育のＤＸを進めている。

その中で学校が取り扱う情報には、児童生徒の個人情報のみならず、保護者、職員などの個人情報及び学校運営の情報などの重要な情報が数多く含まれており、外部へ情報漏洩等が発生した場合には極めて重大な結果を招く恐れがある。

したがって、教育情報ネットワークにおいて、個人情報をはじめとする教育情報資産を漏洩や改ざん、コンピューターウイルスによるシステム障害、災害や事故等の様々な脅威から防御することは、学校の財産、プライバシーを守るために必要不可欠であり、保護者や地域住民から信頼される安心・安全な学校づくりに寄与するものである。

以上より、児童生徒、保護者、職員などの個人情報及び学校教育上の重要な情報を保護し、適切に管理・運営するための対策を整備するために、那珂市小中学校情報セキュリティポリシーを定める。

２　定義

このポリシーにおける用語の定義は、次に定めるところによる。

（１）電磁的記録媒体

サーバ装置、端末（ノートＰＣ、タブレットＰＣ等）、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，磁気テープ等の外部電磁的記録媒体をいう。

（２）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。

（３）情報システム

コンピュータ等で構成され、情報処理を行う仕組みをいう。具体的には、ネットワーク及び記録媒体等（ハードウェア、クラウドサービス等）を指す。

（４）情報資産

本対策基準が対象とする教育情報資産は、次のとおりとする。

ア　ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

イ　ネットワーク及び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）

ウ　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）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。

３　情報セキュリティポリシーの位置づけと対象範囲

情報セキュリティポリシーは、学校が所管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、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、情報セキュリティポリシーの対象範囲は、学校に勤務する全ての職員、教育委員会事務局の職員、外部委託事業者に属する者に適用される。

４　職員等の義務

職員等は、情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用に当たっては情報セキュリティポリシーを遵守するものとする。

５　情報セキュリティ管理体制

本市の情報資産について、適切に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。

６　情報資産の分類

情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行うものとする。

７　情報資産への脅威

情報セキュリティポリシーを講ずる上で、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。

特に認識すべき脅威は以下のとおりである。

（１）権限外者による故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、聞き及び電磁的記録媒体の盗難等

（２）職員及び外部委託者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び電磁的記録媒体の盗難、規定外の情報システムの機器操作によるデータ漏洩等

（３）地震、落雷、火災等の災害や事故、故障等によるサービス及び業務の停止

８　情報セキュリティ対策

本市の情報資産を上記７の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

（１）人的セキュリティ対策

職員の情報セキュリティに関する権限や責任等を定めるとともに、全ての職員に情報セキュリティポリシーの内容を周知徹底するため、教育・訓練を行う。

（２）物理的セキュリティ対策

情報システムを設置する施設等への不正な立入り、情報資産への損傷・妨害等から保護するため、物理的な対策を講ずる。

（３）技術的セキュリティ対策

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等を実施する。

（４）運用におけるセキュリティ対策

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報処理システムに対して被害を及ぼすことを防ぐため、ネットワークの監視、セキュリティポリシーの遵守状況確認等の必要な措置を講ずる。また、障害及び緊急事態が発生した際の迅速な対応を可能とするための対策を講ずる。

９　教育情報セキュリティ実施手順の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定するものとする。

１０　評価・見直し

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、情報システムの変更、新た

な脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティ対策基準の見直しを実施するものとする。