小矢部市教育情報セキュリティポリシー

≪教育情報セキュリティ基本方針≫

小矢部市教育委員会

令 和 ８ 年 ３ 月

（目　次）

１　目的・・・・・・・・・・・・・・・・・・・・・・・・２

２　定義・・・・・・・・・・・・・・・・・・・・・・・・２

３　対象とする脅威・・・・・・・・・・・・・・・・・・３

４　適用範囲・・・・・・・・・・・・・・・・・・・・・３

５　教職員等の遵守義務・・・・・・・・・・・・・・・・４

６　情報セキュリティ対策・・・・・・・・・・・・・・・４

７　教育情報セキュリティ対策基準の策定・・・・・・・５

８　教育情報セキュリティ実施手順の策定・・・・・・・５

９　情報セキュリティ監査及び自己点検・・・・・・・・５

10　教育情報セキュリティポリシーの見直し・・・・・・５

11　教育情報セキュリティポリシー等の公開・・・・・・５

1　目的

この基本方針は、本市教育委員会及び市立学校が保有する情報資産の機密性、完全性及び可用性を維持するため、本市教育委員会が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2　定義

本基本方針においては、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) 情報資産

ネットワーク、情報システムやこれらに関する設備、電磁記録媒体やこれらの開発と運用に係る全ての情報、ネットワーク及び情報システムで取り扱う全ての情報（紙等の有体物に出力された情報を含む。）をいう。

(2) 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

本基本方針及び教育情報セキュリティ対策基準をいう。

(4) 情報システム

ネットワーク、ハードウェア、ソフトウェア（アプリケーションを含む。）及び電磁記録媒体で構成され、情報処理を行う仕組みをいう。

(5) ネットワーク

コンピュータ等の機器が互いに通信し合うために必要な仕組みをいう。

(6) ハードウェア

コンピュータ本体や周辺機器など、物理的な実体を伴う装置や機器をいう。

(7) ソフトウェア

コンピュータを制御するためのプログラムや命令を出すものをいう。

(8) 機密性

情報にアクセスすることを認められた者のみが、情報にアクセスできる状態を確保することをいう。

(9) 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。

(10) 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。

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による機器の盗難や情報資産の漏えい・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又は持ち出しによる紛失、不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、水害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
(4) 大規模・広範囲にわたる疾病のまん延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、通信の途絶等のインフラの障害からの波及等

４　適用範囲

本基本方針が適用される範囲は、次に定めるところによる。

(1) 行政機関等の範囲

本基本方針が適用される行政機関等は、本市教育委員会が設置する施設のうち、学校の管理運営に係る事務を担う執行機関（以下「学校管理運営事務担当課」という。）、小矢部市立学校設置条例（昭和 39 年小矢部市条例第 41 号）に規定する小中学校とする。

(2) 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 ネットワーク、情報システム及びこれらに関する設備並びに電磁記録媒体
② 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。）
③ 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　教職員等の遵守義務

教職員、非常勤職員及び臨時職員等（以下「教職員等」という。）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、業務の遂行に当たっては教育情報セキュリティポリシー及び実施手順を遵守しなければならない。

なお、教育委員会事務局職員は本市情報セキュリティポリシーを遵守すること。

６　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、次の各号に掲げる情報セキュリティ対策を講じるものとする。

(1)　組織体制

学校管理運営事務担当課及び学校における情報資産について、市長部局と連携しつつ、適切に情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

(2)　情報資産の分類及び管理

学校管理運営事務担当課及び学校が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講じる。

(3)　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物理的な対策を講じる。

(4)　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等を定め、職員に情報セキュリティポリシー及び情報セキュリティに関する法令等の内容を周知徹底する等、十分な教育及び啓発が行われるよう必要な対策を講じる。

(5)　技術的セキュリティ対策

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、不正プログラム対策、不正アクセス対策、ネットワーク管理等の技術面の対策を講じる。

(6)　運用におけるセキュリティ対策

情報システムの監視、情報セキュリティ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、情報セキュリティポリシーの運用面の対策を講じる。また、情報資産に対するセキュリティ侵害等の緊急事態が発生した場合に迅速かつ適切な対応を可能とするための危機管理対策を講じる。

７　教育情報セキュリティ対策基準の策定

上記６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等の基準を明らかにする教育情報セキュリティ対策基準を別に策定するものとする。

８　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、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別に策定するものとする。

９　情報セキュリティ監査及び自己点検

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情報セキュリティ監査及び自己点検を実施する。

10　教育情報セキュリティポリシーの見直し

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、教育情報セキュリティポリシーを見直す。

11　教育情報セキュリティポリシー等の公開

本基本方針は、原則公開とする。ただし、教育情報セキュリティ対策基準及び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。