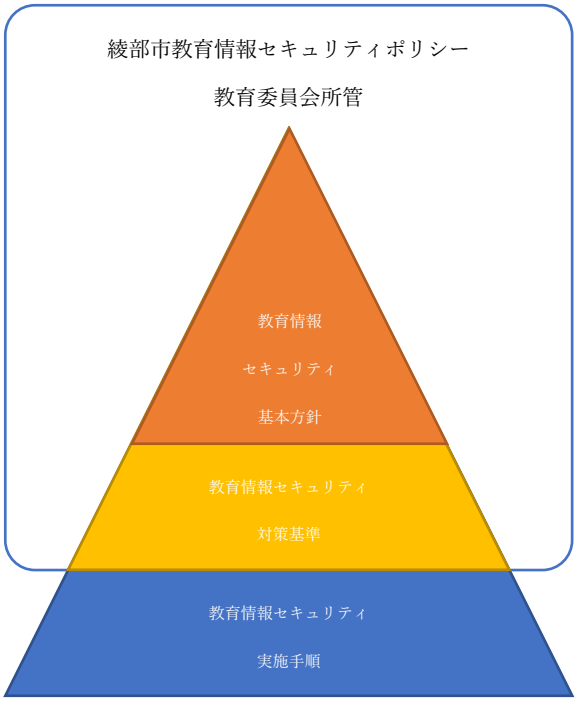
綾部市教育情報セキュリティポリシー

令和３年９月２８日　策定
令和８年３月４日　改訂
綾部市教育委員会最高情報セキュリティ責任者（CISO）承認

序　綾部市教育情報セキュリティポリシーの構成

綾部市教育委員会は教育機関の運用に準じた教育情報セキュリティ基本方針、教育情報セキュリティ対策基準から構成される綾部市教育情報セキュリティポリシーを定める。

本セキュリティポリシーは本市の教育委員会が管轄する範囲における情報セキュリティ対策の最上位の指針を示すものである。



綾部市教育情報セキュリティ基本方針

1.　　目的

本基本方針は、本市教育委員会及び本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

(1)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、その構成機器(ハードウェア及びソフトウェア)をいう。

(2)情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3)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。

(4)教育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。

(5)機密性

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

(6)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。

(7)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。

(8)校務系

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システム及びデータをいう。

(9)学習系

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システム及びデータをいう。

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、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、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
(6)児童生徒から秘匿すべき情報の誤表示・誤共有等

4. 適用範囲

(1)行政機関の範囲

本基本方針が適用される行政機関は、教育委員会及び学校(小学校、中学校、幼稚園を言う。以下同じ。)とする。なお教育委員会及び幼稚園については、所管する教育情報システムに関する部分のみを対象とする。

(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 教育情報システム並びにこれらに関する設備及び電磁的記録媒体
② 教育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 教育情報システムの仕様書及び基幹情報ネットワーク図等のシステム関連文書

5. 教職員の遵守義務

教職員、非常勤教職員及び臨時教職員等(以下「教職員」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ち、業務の遂行に当たって教育情報セキュリティポリシー及び教育情報セキュリティ実施手順を遵守しなければならない。

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、以下の情報セキュリティ対策を講じる。

(1)組織体制

本市教育委員会及び本市立学校の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2)情報資産の分類と管理

本市教育委員会の保有する情報資産を重要性に応じて分類し、当該分類に基づき教育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

サーバ、情報システム室、通信回線及び教職員のパソコン等の管理について、物理的な対策を講じる。

(4)人的セキュリティ

情報セキュリティに関し、教職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(5)技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6)運用

情報システムの監視、教育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、教育情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を必要に応じて策定する。

(7)外部サービスの利用

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講じる。

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には運用手順を定め、発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(8)評価・見直し

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教育委員会による情報セキュリティ遵守状況の確認及び学校での自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。教育情報セキュリティポリシーの見直しが必要な場合は、適宜教育情報セキュリティポリシーの見直しを行う。

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基準等を定める教育情報セキュリティ対策基準を策定する。なお、教育情報セキュリティ対策基準は、公にすることにより本市教育委員会の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。

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策定するものとする。なお、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教育委員会の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。