山陽小野田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》（案）

策定　令和８年３月１日

山陽小野田市教育委員会

教育情報セキュリティ基本方針

1　目的

本基本方針は、本市の学校教育に係る情報資産の機密性、完全性及び可用性を維持するために実施する教育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) 教育ネットワーク

本市の学校教育において使用される校務系システム、校務外部接続系システム及び学習系システムのネットワークをいう。

(2) 教育情報システム

本市の学校教育において使用されるコンピュータ、ネットワーク及び電磁的記録媒体等で構成され、情報処理を行う仕組み（クラウドサービス等を含む）をいう。

(3) 教育情報セキュリティ

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、その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、その情報にアクセスできる状態を確保することをいう。

(8) 職員等

教職員等及び教育委員会事務局職員をいう。

なお、教職員等は、臨時的任用教職員、非常勤講師を含む教職員全員を、教育委員会事務局職員は、教育ネットワークを利用して学校等が保有する情報にアクセスできる者をいう。

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、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

4　適用範囲

(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、教育委員会及び学校（本市内小学校及び中学校）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　教育ネットワーク、教育情報システム、これらに関する設備、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ネットワーク構成図等のシステム関連文書

5 職員等の遵守義務

職員等は、教育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 教育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、以下の教育情報セキュリティ対策を講じる。

(1) 組織体制

教育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

本市の学校教育に係る情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき教育情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等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

教育情報セキュリティに関し、職員等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

教育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。

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切に対応するため、緊急時対応計画を策定する。

(7) 外部委託

外部委託を行う場合には、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、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。

(8) SaaS 型パブリッククラウドサービスの利用

クラウドサービスの利用に当たり、サービス提供事業者に要求するセキュリティ対策の項目等を定めるとともに、約款による外部サービスの利用及びソーシャルメディアサービスの利用基準等を設ける。また、当該サービスの要件基準を確認し、これを満たすネットワーク設計等に留意する。

7　教育情報セキュリティ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を検証するため、定期的又は必要に応じて教育情報セキュリティ監査及び自己点検を実施する。

8　教育情報セキュリティポリシーの見直し

教育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教育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。

9　教育情報セキュリティ対策基準の策定

上記６に規定する教育情報セキュリティ対策を実施するため、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。

10　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。

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。

11　その他

職員等が、本基本方針で定める情報資産以外のネットワーク、情報システム等を取り扱う際には、本市の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に基づき、適切にセキュリティ対策を講じる。