嵐山町教育情報セキュリティポリシー

令和６年４月策定
令和８年３月改訂
嵐山町教育委員会

目　次

嵐山町教育情報セキュリティ基本方針

嵐山町教育情報セキュリティ基本方針

1　目的

本基本方針は、嵐山町情報セキュリティポリシー（平成２７年３月３１日策定）に準拠するほか、本町教育委員会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に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）情報資産

情報資産及び教育情報システムをいう。

（２）情報

教育委員会(教育総務課)、町立小・中学校及び幼稚園が保有する情報（電磁的記録）をいう。

（３）教育ネットワーク

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。

（４）教育情報システム

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

（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。

（６）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。

（７）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。

（８）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。

（９）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。

(10) 冗長化

システムの一部に何らかの障害が発生した場合に備えて、障害発生後でもシステ

ム全体の機能を維持し続けられるように、予備装置を平常時からバックアップとして配置し運営しておくことをいう。

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、情報セキュリティ対策を実施する。

（1）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、通信等の途絶等の提供サービスの障害からの波及等

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、内部部局、教育委員会（教育総務課）、町立小・中学校及び幼稚園とする。

（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、教育情報システム及び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図等のシステム関連文書

5　教職員等の遵守義務

教職員、臨時教職員、会計年度任用職員等関係職員（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ち、業務の遂行に当たって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

本町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

本町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行う。

（３）物理的セキュリティ

サーバ・サーバ室等及び教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

情報セキュリティに関し、教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ものとする。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応マニュアルを策定する。

（７）クラウドサービスにおけるセキュリティ

クラウドサービスの利用に関して遵守すべき事項を定め、対策を講じる。

（８）１人１台端末におけるセキュリティ

学習用端末のセキュリティ対策及び児童生徒の ID、パスワード等の管理について遵守すべき事項を定め、対策を講じる。

７　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

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は、教育情報セキュリティポリシーの見直しを行う。

なお、本セキュリティポリシーに定めのない事項や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（平成 29 年 10 月 18 日策定）（以下「ガイド

ライン」という。）の一部改正等については、本セキュリティポリシーを改定することなくガイドラインに準ずる。

９　教育情報セキュリティ対策基準の策定

上記６、７及び８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町の行政運営及び本町の教育機関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　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情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本町の行政運営及び本町の教育機関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。