飯能市教育情報セキュリティポリシー

飯能市教育委員会

令和５年１月２６日

目次

第1章　総則

第2章　教育情報セキュリティ基本方針

第１章　総則

飯能市教育情報セキュリティポリシーとは、飯能市教育委員会が保有する教育ネットワーク、教育情報システムの情報資産に関する情報セキュリティを確保するための方針、体制、対策等を包括的に定めたものである。情報セキュリティ対策を徹底するためには、対策を組織的に統一して推進することが必要となり、そのためには組織として意思統一し、明文化された文書を定める必要がある。

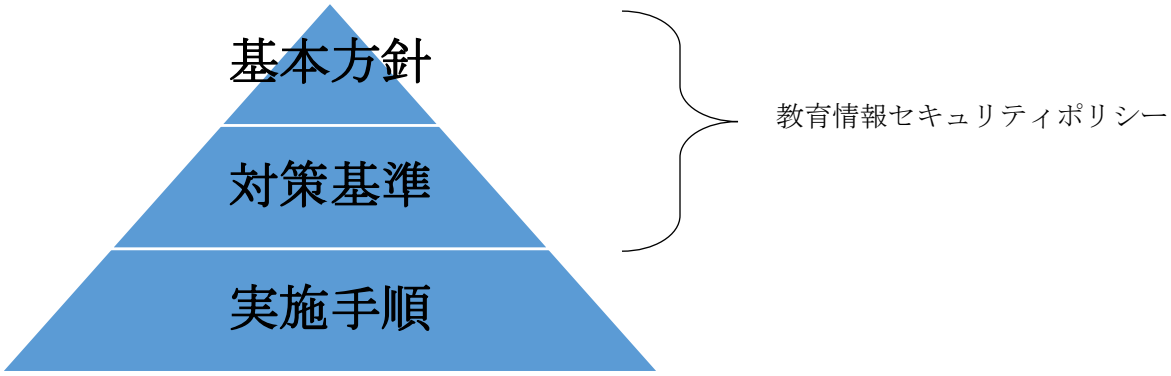
飯能市の教育情報セキュリティ対策における基本的な考え方を定めたものが、「基本方針」である。この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めたものを「対策基準」という。この「基本方針」と「対策基準」を総称して、「教育情報セキュリティポリシー」という。

また、「対策基準」を具体的なシステムや手順、手続きに展開して個別の実施事項を定めるものを「実施手順」という。

飯能市教育情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、全ての教職員及び委託事業者は、業務の遂行にあたって本情報セキュリティポリシーを遵守する義務を負う。

情報セキュリティポリシーの体系は、図１に示すとおりとする。

図 1



第２章　教育情報セキュリティ基本方針

１　目的

本基本方針は、本市が保有する教育ネットワーク及び情報資産の機密性、完全性及び可用性を維持するため、市立幼稚園、小学校及び中学校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。また、飯能市教育委員会が設置する幼稚園・小学校及び中学校、教育センター、市庁舎内部所属で利用するネットワークを教育ネットワークという。

（２）情報システム

コンピュータ、ネットワーク、電磁的記録媒体及びソフトウェアで構成され、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）情報セキュリティポリシー

本基本方針及び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）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（９）コンピュータ

パーソナルコンピュータ（以下「パソコン」という。）

モバイル端末

業務上の必要に応じて移動させて使用することを目的としたタブレット端末等

サーバ・ストレージ

その他類似・周辺機器等

(10) 電磁的記録媒体

①内蔵電磁的記録媒体

コンピュータ、通信回線装置等に内蔵される電磁的記録媒体

②外部電磁的記録媒体

USB メモリ・外付けハードディスクドライブ

SD カード・DVD-R・カードリーダー

その他類似する電磁的記録媒体

(11) 委託事業者

業務委託契約等により、飯能市教育委員会の業務執行を受託した業者をいう。

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、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、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）行政機関の範囲

本基本方針が適用される行政機関は、教育委員会（幼稚園・小学校及び中学校を含む。）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ネットワーク及び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

教職員及び委託事業者は、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

本市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実施する。

（３）物理的セキュリティ

サーバ、教育情報システムを設置する施設、通信回線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、教職員及び委託事業者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

情報システム及びネットワークの監視、情報セキュリティポリシーの遵守状況の確認、業務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切に対応するため、緊急時対応計画を策定する。

（７） 業務委託と外部サービスの利用

業務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。

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。

（８） 評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

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　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、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、情報セキュリティポリシーの見直しを行う。

９　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共通の判断基準等を定める情報セキュリティ対策基準を策定する。

１０　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。

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市の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。