東御市教育情報セキュリティポリシー

第１章　総則

１　目的

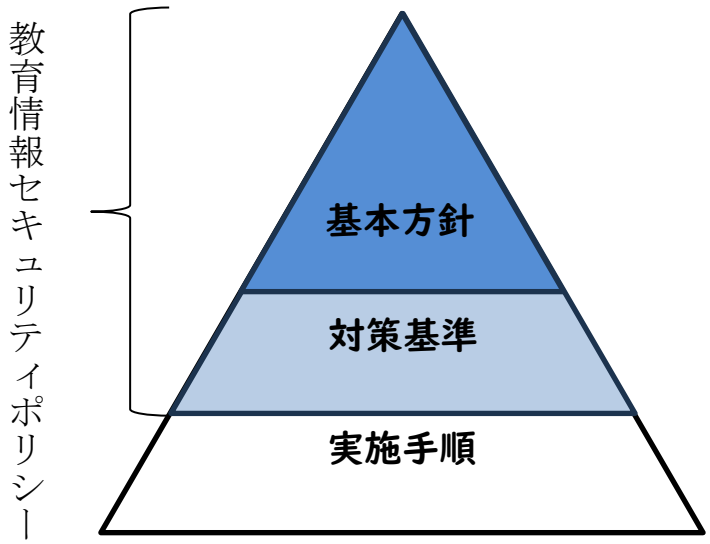
情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。東御市においても東御市情報セキュリティポリシーが策定している一方で、市内小学校及び中学校（以下「学校」という。）においては、地方公共団体とは異なる特徴を有することから、学校現場の特徴を踏まえた「教育情報セキュリティポリシー」を定めることが求められる。

本ポリシーは、教育委員会が保有・利用する教育情報資産に対し、情報セキュリティ対策を組織的かつ計画的に行うため、情報セキュリティ対策の基本となる事項を定めることにより情報資産を保護することを目的とする。

２　構成

本ポリシーは、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る「東御市教育情報セキュリティ基本方針（以下「基本方針」という。）」と、基本方針に基づき全ての教育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る「東御市教育情報セキュリティ対策基準（以下「対策基準」という。）」の二つから構成される。

情報セキュリティポリシーの構成図



第２章　基本方針

１　目的

基本方針は、東御市教育委員会が保有する教育情報資産の機密性、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) 教育情報資産

教育活動に必要となる情報及びその情報を生成・保管・流通する媒体（紙、ネットワーク、サーバ、校務用端末、学習用端末等）をいう。

(2) ネットワーク

教育情報資産を扱う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。

(3) 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、教育情報資産の情報処理を行う仕組みをいう。

(4) 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

(5) 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。

(6) 機密性

情報にアクセスすることが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。

(7) 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。

(8) 可用性

情報にアクセスすることが認められた者だけが、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

教育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教育情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2) 教育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教育情報資産の漏えい・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

教育情報セキュリティポリシーが適用される行政機関等は、教育委員会及び学校とする。

(2) 教育情報資産の範囲

ア　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

イ　ネットワークおよ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。）

ウ　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に関連する文書

5　教職員等及び外部委託事業者の遵守義務

校長、教頭、教員、職員（以下「教職員等」という。）及び外部委託事業者は、情報セキュリティの重要性について共通認識を持ち、業務の遂行にあたって、関係法令及び教育情報セキュリティポリシーを遵守しなければならない。

6　情報セキュリティ対策

「3　対象とする脅威」に示す脅威から教育情報資産を保護するため、以下の情報セキュリティ対策項講じる。

(1) 組織体制

情報セキュリティ対策を推進する教育委員会及び学校での組織体制を確立する。

(2) 教育情報資産の分類と管理

教育委員会の保有する教育情報資産を機密性、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

教育情報資産及びネットワークの管理について、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

技術的な対策を講じる。

(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、業務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、教育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、緊急時対応計画を策定する。

(7) 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、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たうえで、必要に応じて契約に基づいた措置を講じる。

外部サービス（クラウドサービス）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。

教育委員会及び学校において、ソーシャルメディアサービスを利用する場合にはソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで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。

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等の見直し

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に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となった場合には、教育情報セキュリティポリシーを見直す。

9　対策基準の策定

情報セキュリティ対策を実施するために、具体的な遵守事項及び判断基準等を定めた対策基準を策定する。

なお、対策基準は公にすることにより教育委員会及び学校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　実施手順の策定

対策基準に基づき、情報セキュリティに関する対策を実施するための具体的な手順を定めた実施手順を策定するものとする。

なお、実施手順は公にすることにより教育委員会及び学校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。