小牧市教育委員会

教育情報セキュリティポリシー
(基本方針)

小　牧　市　教　育　委　員　会

小牧市教育委員会情報セキュリティ基本方針

１　目的

教育委員会が管理する教育情報システムが取り扱う情報には、児童生徒等の個人情報のみならず、学校経営上重要な情報など、外部に漏えい等をした場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う教育情報システムを様々な脅威から防御することは、児童生徒の生命、財産、プライバシー等を守るため、また、教育委員会の情報処理業務の安定的な運営のために必要不可欠であり、ひいては、このことが教育委員会に対する信頼の維持向上に寄与するものである。

そのため、教育委員会が所掌する情報資産の機密性、完全性及び可用性（※注）を維持するための情報セキュリティ対策を整備するため、教育情報セキュリティポリシーを定める。このうち、情報セキュリティ基本方針については、教育委員会の情報セキュリティ対策の基本的な事項を定めるものとする。

（※注）国際標準化機構（ＩＳＯ）が定めるもの（ＩＳＯ７４９８－２：１９８９）

機密性（confidentiality）：情報にアクセスすることを認可された者だけがアクセスできる状態を確保すること。

完全性（integrity）：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性（availability）：許可された利用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ことを確実にすること。

２　定義

（１）ネットワーク

教育委員会が所掌する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（ハードウエア及びソフトウエア）をいう。

（２）教育情報システム

教育委員会が所掌するコンピュータ（ハードウエア・ソフトウエア）、ネットワーク、クラウドサービス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）情報資産

教育委員会が所掌する教育ネットワーク及び教育情報システムの開発と運用に係るすべての情報並びにネットワーク及び教育情報システムで取り扱うすべての情報（これらを印刷した文書を含む。）をいう。

また、小中学校においては、名簿や成績などの情報自体に加えて、それらを記載したファイルや電子メールなどのデータ、データが保存されているパソコンやサーバ、ＣＤ－ＲＯＭ、ＵＳＢメモリなどの電磁的記録媒体も情報資産に含まれる。

（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）教育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。

（６） 情報セキュリティインシデント

情報セキュリティに関する事故やシステム上の欠陥、並びにその原因や結果。教育委員会内外の情報の漏えい（教職員等の規定違反に起因するものを含む）や、教育情報システムに対するサイバー攻撃等をいう。

３　情報資産への脅威

情報資産に対する脅威として、次の事項を想定し、情報セキュリティ対策を実施する。

- 内部の者による情報資産の窃取・改ざん等
- 自然災害等による情報資産の滅失等
- 児童生徒のいたずら等による情報資産の窃取・改ざん等
- 悪意のある外部の者による情報資産の窃取・改ざん等
- 教職員等の過失による情報資産の漏えい・紛失等
- 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
- 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　対象範囲

（１） 教育機関の範囲

本基本方針が適用される機関は、小牧市教育委員会ネットワーク（以下「教育ネットワーク」という。）に接続できる機関（以下「適用機関」という。）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、教育委員会が所掌する次のものとする。

ア　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及び電磁的記録媒体

イ　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。）

ウ　教育情報セキュリティポリシー、教育情報セキュリティ実施手順、教育情報システムの仕様書及びネットワーク図等の教育情報システム関連文書

５　教育情報セキュリティポリシーの位置付けと職員等の遵守義務

教育情報セキュリティポリシーは、情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、情報資産に関する業務に携わる全ての職員は、情報セキュリティの重要性について共通の認識を持つとともに、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する義務を負うものとする。

６　情報セキュリティ対策

上記３で示した脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講ずるものとする。

（１） 組織体制の確立

教育委員会の情報資産について、情報セキュリティ対策を推進及び管理するための組織体制を確立するものとする。

（２） 情報資産の分類と管理

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

（３） 教育ネットワークの分離

校務系情報について、インターネットから侵入する脅威への情報セキュリティ対策を一層強化するため、また、児童生徒による不正アクセスを防止するため、教育ネットワークを児童生徒の個人情報等を取り扱う「校務系」、学校ホームページの編集、保護者メールの送信などインターネット接続が必要な校務や教育活動において教職員が利用する「校務外部接続系」、教育活動において主に児童生徒が利用する「学習系」に分離する対策を講じる。

（４） 人的セキュリティ対策

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） 物理的セキュリティ対策

教育情報システム装置、管理区域、ネットワーク接続及び職員等の端末等の管理について、物理的な対策を講ずる。

（６） 技術的セキュリティ対策

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。

（７） 運用面での対策

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の運用面の対策を講じる。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の緊急時対応計画を策定する。

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が遵守されていることを検証するため、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の実施

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を取り巻く状況の変化に対応するために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の見直しを実施する。

９　情報セキュリティ対策基準の策定

様々な情報資産について、上記６、７及び８の情報セキュリティ対策を実施するために、遵守すべき行為及び判断等の基準を具体的に定める情報セキュリティ対策基準を策定するものとする。

１０　教育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個々の情報資産における情報セキュリティ対策を実施するため、別途、教育情報セキュリティポリシーに基づく具体的な教育情報セキュリティ実施手順（以下「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の学校経営に重大な支障を及ぼす恐れのある情報であることから非公開とする。