小林市教育情報セキュリティ基本方針

令和８年３月30日　制定

小林市教育委員会

はじめに

情報セキュリティとは

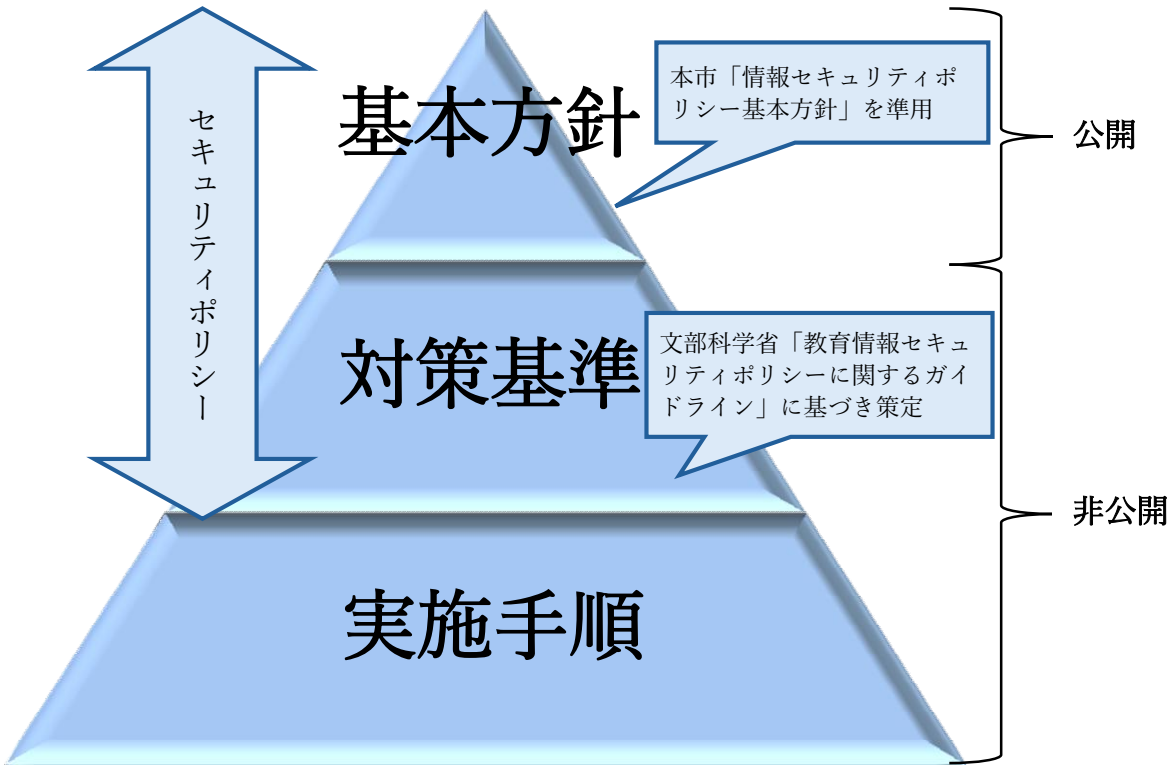
市民サービス向上に向けて、市民の個人情報を含む、学校園で保持している様々な情報資産を保護すること。

そのためには、①機密性、②完全性、③可用性を維持する必要がある。

セキュリティポリシーの構成

セキュリティポリシーは、情報セキュリティ対策に関する基本的な考え方をまとめた「基本方針」と、この基本方針に基づき、全ての学校に共通の情報セキュリティ対策の基準を定める「対策基準」から構成される。「基本方針」については、地方自治体が策定したものを準用するとされる。

さらに、対策基準を実際のシステムに当てはめ、個別の実施事項など具体的な内容を定めた「実施手順」については、教育委員会が策定したひな形を基に各学校で策定・見直しをすることが求められる。



１．目的

小林市が保有する教育ネットワーク、教育情報システム及び情報資産について、教育情報セキュリティ対策の基本的な考え方を定めることにより、市内小・中学校の教育活動の推進と児童生徒、保護者及び職員等、学校に関わる全ての者の財産、プライバシー等を保護し学校の安定的な運営を図ることを目的とする。

２．位置づけ

教育情報セキュリティ基本方針は、学校の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かかる情報セキュリティ対策を総合的、体系的かつ具体的に取りまとめたものであり、学校における情報セキュリティ対策を実施するうえで基礎となるものである。

３．定義

（１） コンピュータ

パーソナルコンピュータ（一人一台端末含む)、サーバ、ストレージ等の機器をいう。

（２） ネットワーク

コンピュータ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、小林市教育委員会が設置する小・中学校、市庁舎内部所属で利用するネットワークを特に教育ネットワークという。

（３） 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。

（４） 情報資産

情報システムで取り扱う情報で、開発及び運用に係るものを含むすべての情報をいう。なお、それらを紙等に出力した文書も含む。

（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） 情報セキュリティポリシー

組織が所管する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、本基本方針及び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) 校務系情報

学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報をいう。

(11) 校務外部接続系情報

校務系情報のうち、保護者メールや学校ホームページ等の外部とインターネット接続を前提とした校務で利用される情報をいう。

(12) 学習系情報

学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教職員及び児童生徒がアクセスすることが想定されている情報をいう。

(13) 校務用端末

校務系情報全てにアクセス可能な端末をいう。

(14) 学習者用端末

学習系情報にアクセス可能な端末で、児童生徒が利用する端末をいう。

(15) 指導者用端末

学習系情報にアクセス可能な端末で、教職員のみが利用可能な端末をいう。

(16) 教育情報システム

情報資産を扱うハードウェア、ソフトウェア、クラウドサービス等をいう。

(17) 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問題としてとらえられる事象（障害、事件、事故、欠陥、攻撃、侵害等）をいう。

(18) 記録媒体

情報システムでデータ等を記録するための媒体（メディア）。サーバ、各端末機、デジタルカメラ、デジタルビデオカメラ、外付けハードディスク、ＣＤ－ＲＯＭ、ＤＶＤ－Ｒ、ＵＳＢメモリ、ＳＤカード等の外部電磁的記録媒体をいう。

(19) 無線ＬＡＮ

電波等を利用してデータの送受信を行う構内通信網システムをいう。

(20) クラウドサービス

学校外、庁舎外でプログラムやデータベースを管理し、インターネットなどのコンピューターネットワークを経由し、情報システム等の利用をサービスの形で提供され

る利用形態をいう。

(21)　ソーシャルメディアサービス

インターネット上における、ホームページ、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等をいう。

(22)　外部委託事業者

業務委託契約等により、小林市教育委員会の業務執行を受託した業者をいう。

4．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、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、水害、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

（6）　その他、本市教育委員会の情報資産の機密性、完全性及び可用性を脅かす脅威

5．適用範囲

教育情報セキュリティポリシーの適用範囲は、以下に示すものとする。

（1）　組織の範囲

学校の内部のすべての組織及びクラウドサービスを利用・管理する教育委員会。さらに、委託契約により学校の業務を受託し情報資産を取り扱う外部事業者等及びクラウドサービス提供事業者を含む。ただし、学校事務で使用しているLGWAN接続系ネットワークに接続された情報システムは、小林市情報セキュリティポリシーの対象範囲に属するため、これを除く。

（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

（3）　対象者

上記（2）の情報資産に接する組織の職員（会計年度任用職員、臨時的任用職員を

含む。）及び受託事業者等職員に準じる者（以下、「職員等」という。）とする。

６．教育情報セキュリティポリシー及び関連法令等の順守

（１） 職員等の責務

① 職員等は、情報セキュリティの重要性を認識し、業務の遂行に当たっては教育情報セキュリティポリシーを順守する義務を負う。また、情報資産の利用や保管等を行う際は、情報セキュリティ実施手順等を順守しなければならない。

② 教育情報セキュリティポリシーに違反した職員等は、生じた結果の重大性及び違反の悪質性等の状況に応じて、地方公務員法等に基づき懲戒処分等の対象になることがある。

（２） 外部事業者への対応

学校は、業務を委託する外部事業者・団体等に対しても情報セキュリティの重要性を認識させるため、契約書等において教育情報セキュリティポリシーへの順守事項及び違反した場合の責任等についても明確にするものとする。

（３） 児童生徒への対応

学校は、児童生徒に対しても、情報モラル教育の観点から情報セキュリティの重要性を認知させる等、指導、監督するものとする。

（４） クラウドサービスの利用

クラウドサービスを利用・管理する学校及び教育委員会は、クラウドサービスの特性に起因する留意点を踏まえ、教育情報セキュリティポリシーに基づきクラウドサービスを利用する上での安全性の確保に努めるものとする。

７．情報セキュリティ対策

上記４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

情報資産を管理し、機密性、完全性及び可用性を維持するための体制を確立する。

（２） 情報資産の分類と管理

学校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、情報システム室、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

教育情報セキュリティに関する権限や責任、教職員等が遵守すべき事項を定めるとともに、このポリシーを周知徹底させるための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の確保等、この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、緊急的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、委託事業者に選定し、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。

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、利用できるソーシャルメディアごとの責任者を定める。

（８） 評価・見直し

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

８．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。

９．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に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で教育情報セキュリティポリシーを見直す。

10．情報セキュリティ対策基準の策定

上記７、８及び９に規定する対策等を実施するために、職員等が順守すべき事項や判断の基準等を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を実施する上で必要となる一定の基準を示した情報セキュリティ対策基準を策定するものとする。

11. 情報セキュリティ実施手順の策定

各学校が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手順を策定するものとする。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより学校運営に重大な支障を及ぼす恐れがあるため、非公開とする。