鴻巣市学校情報セキュリティ基本方針

1　目的

小・中学校は、児童・生徒及び保護者の個人情報や学校運営上重要な情報等、多くの情報資産を蓄積・保有している。これらの情報資産は児童・生徒及びその保護者の生命、財産及びプライバシーを守るためにも、また、継続的かつ安全な学校運営を行うためにも、故意や過失による情報の改ざんや漏えい、情報システムの故障や不具合、自然災害による被災等から確実に保護しなければならない。また、校内のみならず、学校外での交流など広く情報通信技術を活用した情報教育を推進するためには、高度な安全性を有したネットワークや情報システムの構築及び運用が必要となる。

このようなことから、学校セキュリティ基本方針を定め、小・中学校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教育委員会及び小・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(ハードウエア及びソフトウェア)をいう。

(2)　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、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。

3　対象とする脅威

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

(1)　不正アクセス、マルウェア、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、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因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障害からの波及等

4　適用範囲

(1)　対象者の範囲

本基本方針が適用される対象者は、小・中学校が保有する情報資産を取り扱うすべての教職員等及び外部委託事業者とする。

(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。

ア　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

イ　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。）

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関連文書

5　教職員等の遵守義務

教職員等は、情報セキュリティの重要性について共通の認識を持ち、職務の遂行に当たって学校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

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

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

情報資産を重要性分類に応じて分類し、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、重要機能室、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

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

コンピュータ等の一元管理、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、学校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、学校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正に対応するため、緊急時対応計画を策定する。

(7)　外部委託

外部委託する場合には、外部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、外部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。

約款によ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。

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毎の責任者を定める。

クラウドサービスを利用する場合には、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する。

(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。学校セキュリティポリシーの見直しが必要な場合は、学校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

学校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、学校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、新たに対策が必要となった場合には、学校セキュリティポリシーを見直す。

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各学校において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学校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。