金沢市教育委員会サイバーセキュリティ基本方針

令和８年３月

1. 目的

金沢市教育委員会（以下「教育委員会」という。）が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和 22 年法律第 67 号)第 244 条の６第１項に規定するサイバーセキュリティを確保するための方針として、教育委員会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ことを目的に金沢市教育委員会サイバーセキュリティ基本方針（以下「基本方針」という。）を定める。

2. 用語の定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(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。

(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) 教職員等

臨時的任用教職員、非常勤講師を含めた教職員全員をいう。

(4) 教育委員会事務局職員

教育ネットワークを利用して、学校が所管する情報にアクセスできる教育委員会事務局職員をいう。

(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) 校務系システム

児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・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取り扱うシステムをいう。

(9) 学習系システム

児童生徒のワークシート、作品など、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取り扱うシステムをいう。

(10) 校務外部接続系システム

校務系情報のうち、保護者メールや学校ホームページ等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取り扱うシステムをいう。

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、サイバー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

この基本方針が対象とする情報資産の範囲は、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. サイバーセキュリティ対策

上記３に定める脅威から情報資産を保護するために、以下のサイバーセキュリティ対策を講じる。

(1) 組織体制

教育委員会の保有する情報資産について、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

教育委員会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、当該分類に基づきサイバーセキュリティ対策を実施する。

(3) 情報システム全体構成上の対策

情報システム全体を校務系システム、校務外部接続系システム、学習系システムの３つに分類し、取り扱う情報に応じて、接続するネットワークの分離または強固なアクセス制御等により安全対策を講じる。

(4) 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員のパソコン等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

サイバーセキュリティに関し、職員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。

(6) 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。

(7) 運用

情報システムの監視、サイバー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、サイバー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、緊急時対応体制を整備する。

(8) 業務委託と外部サービス（クラウドサービス）の利用

① 業務委託を行う場合には、委託事業者を選定し、サイバー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。

② 外部サービス（ クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

③ 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。

(9) 評価・見直し

サイバー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サイバー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、サイバーセキュリティの向上を図る。サイバーセキュリティポリシーの見直しが必要な場合は、適宜サイバーセキュリティポリシーの見直しを行う。

6. サイバーセキュリティ監査及び自己点検の実施

サイバー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サイバーセキュリティ監査及び自己点検を実施する。

7. サイバーセキュリティポリシーの見直し

サイバーセキュリティ監査及び自己点検の結果、サイバー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サイバー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、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、リスクを検討したうえで、サイバーセキュリティポリシーを見直す。

8. サイバーセキュリティ対策基準の策定

上記５、６及び７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サイバーセキュリティ対策基準を策定する。なお、サイバーセキュリティ対策基準は、公にすることにより教育委員会の教育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。

9. サイバーセキュリティ実施手順の策定

サイバーセキュリティ対策基準に基づき、サイバー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サイバーセキュリティ実施手順を策定するものとする。なお、サイバーセキュリティ実施手順は、公にすることにより教育委員会の教育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。