中央区教育情報セキュリティ基本方針

令和8年 10 月
中央区教育委員会

目次

1 目的 3
2 定義 3
3 対象とする脅威 4
4 適用範囲 4
5 教職員等及び教育委員会事務局職員の義務 4
6 情報セキュリティ対策 4
7 情報セキュリティ監査及び自己点検の実施 5
8 教育情報セキュリティポリシーの見直し 6
9 教育情報セキュリティ対策基準の策定 6
10 教育情報セキュリティ実施手順の策定 6

1 目的

本基本方針は、中央区立学校（宇佐美学園を含む。）及び中央区立幼稚園（以下「学校」という。）並びに中央区教育委員会（以下「教育委員会」という。）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、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

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

⑴ 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及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑵ 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。

⑶ 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。

⑷ 教育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。

⑸ 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障害・事故及びシステム上の欠陥をいう。

⑹ 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。

⑺ 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。

⑻ 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。

⑼ 約款による外部サービス

民間事業者等がインターネット上で不特定多数の利用者（主に一般消費者）に対して提供（有料、無料に関わらず）する、画一的な約款や利用規約等への同意、簡易なアカウントの登録（登録が不要な場合もある）等により利用可能なサービスをいう。システム開発保守業者と業務委託契約を締結し、受託者がシステムの機密性・完全性・可用性についての必要な対策を講じた上で、システム構成の一部に上記のサービスを利用する場合は、約款による外部サービスとして扱わない。

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、情報セキュリティ対策を講じる。

⑴ 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

⑵ 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

⑶ 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

⑷ 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

⑸ 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

⑴ 本基本方針が対象とする範囲は、学校及び教育委員会とする。

⑵ 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 教育ネットワーク及び教育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 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 教職員等及び教育委員会事務局職員の義務

教職員等（臨時的任用教員や時間講師等も含めた教職員全員をいう。以下同じ。）及び教育委員会事務局職員は、情報セキュリティの重要性について共通の認識を持ち、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。

⑴ 組織体制

教育委員会及び学校が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。

⑵ 情報資産の分類と管理

教育委員会及び学校が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講じる。

⑶ 物理的セキュリティ

設置されたネットワーク機器及び通信回線については、関係者以外の立入り制限又は物理的な保護措置を講ずることにより、破壊又は不正接続からその安全を確保するものとする。一

方、教職員等が利用する情報端末及び認証デバイスについては、校内外を問わずその所在に応じた盗難又は紛失の防止策を講ずるものとする。あわせて、クラウドサービス基盤については、高度な物理的セキュリティが担保された環境を適切に選定及び管理することで、情報資産全体の安全性を確保するものとする。

⑷ 人的セキュリティ

情報セキュリティに関し、教職員等及び教育委員会事務局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などの人的な対策を講じる。

⑸ 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。

⑹ 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、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。

⑺ 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、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。

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た対策を講じる。

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ごとの責任者を定める。

⑻ 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。

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、リスクを検討した上で、教育情報セキュリティポリシーを見直す。

9 教育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講じるために、具体的な遵守事項及び判断基準等を定める教育情報セキュリティ対策基準を策定する。

なお、本基準は、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ことから非公開とする。

10 教育情報セキュリティ実施手順の策定

教育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教育情報セキュリティ実施手順を策定する。

なお、本手順は、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ことから非公開とする。