

太子町教育情報セキュリティ基本方針

令和6年3月26日 制定

(目次)

1	目的	1
2	対象とする脅威	1
3	適用範囲	1
4	教職員等の遵守義務	1
5	情報セキュリティ対策	2
6	情報セキュリティ監査及び自己点検の実施	3
7	教育情報セキュリティポリシーの見直し	3
8	情報セキュリティ対策基準の策定	3
9	情報セキュリティ実施手順の策定	3

教育情報セキュリティポリシーにおける用語一覧

附則

1 目的

本基本方針は、太子町教育委員会事務局及び太子町立小学校・中学校（以下「学校等」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、学校等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。なお、本基本方針に含まれない範囲については、「太子町情報セキュリティ基本方針」により定めるものとする。

2 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

3 適用範囲

(1) 適用組織の範囲

本基本方針が適用される組織は、学校等とする。

(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。

- ① 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
- ② ネットワーク及び情報システムで取扱う情報（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

4 教職員等の遵守義務

教職員（再任用教職員等を含む）、非常勤教職員及び臨時的任用教職員、会計年度任用職員等（以下「教職員等」という。）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。

5 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
学校等の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。
- (2) 情報資産の分類と管理
学校等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) 情報システム全体の強靱性の向上
情報システム全体に対し、次の段階の対策を講じる。
 - ① 校務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持出し不可設定や端末への多要素認証の導入等により、個人情報流出を防ぐよう努める。
 - ② インターネット接続においては、インターネット接続口を集約した上で、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施するよう努める。
- (4) 物理的セキュリティ
サーバ等、情報システム室等、通信回線等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。
- (5) 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、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、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よう努める。
- (8) 外部サービスの利用
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、その運用手順を定め、利用する範囲を規定し、利用する約款による外部サービスごとに責任者を定める。

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。

(9) 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、教育情報セキュリティポリシーの見直しを行う。

6 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。

7 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、教育情報セキュリティポリシーを見直す。

8 情報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情報セキュリティ対策基準を策定する。

9 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等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。

教育情報セキュリティポリシーにおける用語一覧

用語	用語の解説・定義
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）
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
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

校務系	児童生徒の成績などの個人情報など、学校等が保有する情報資産のうち、それら情報を学校・学級の管理運営や各種指導に活用するため、教職員のみがアクセスできる情報システム及びデータ
教育系	児童生徒の成果物など、学校等が保有する情報資産のうち、それら情報を学校等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できる情報システム及びその情報システムで取扱うデータ
通信経路の分割	それぞれの環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすること
校務用端末	校務系情報にアクセス可能な端末
学習者用端末	教育系(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
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
教育系システム	教育系ネットワーク、教育系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
教育情報システム	校務系、教育系システムを合わせた総称。
強固なアクセス制御	インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、利用者認証(多要素認証)、端末認証、アクセス 3 経路の監視・制御等を組み合わせたセキュリティ対策

※その他用語については、「太子町情報セキュリティ基本方針」及び別紙用語一覧参照のこと。

附 則

(施行期日)

- 1 この基本方針は、令和6年3月26日から施行する。