

廿日市市立学校教育情報セキュリティポリシー基本方針

(目的)

第1条 廿日市市立学校教育情報セキュリティポリシー基本方針（以下「基本方針」という。）は、廿日市市立学校設置条例（昭和39年条例第18号）に規定する小学校及び中学校（以下「学校」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、学校が実施する教育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。

(定義)

第2条 この基本方針において、次に掲げる用語の意義は、それぞれ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) 教育情報システム 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) 教育情報セキュリティ 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) 教育情報セキュリティポリシー この基本方針及び教育情報セキュリティポリシー対策基準をいう。
- (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。

(対象とする脅威)

第3条 情報資産に対する脅威として、次に掲げる脅威を想定し、教育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
- (情報資産の範囲)

第4条 基本方針において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
 - (2) 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。）
 - (3) 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
- (教職員の遵守義務)

第5条 教職員は、教育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を遵守しなければならない。

(教育情報セキュリティ対策)

第6条 第3条の脅威から情報資産を保護するために、次に掲げる教育情報セキュリティ対策を講じる。

- (1) 組織体制 学校における教育情報セキュリティ対策を推進し、及び管理するための組織体制を整備する。
- (2) 情報資産の分類と管理 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、当該分類に基づき教育情報セキュリティ対策を講じる。
- (3) 教育情報システム全体の強靱性の向上 教育情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、教育情報システム全体に対し不正通信の監視機能の強化等の教育情報セキュリティ対策を実施する。
- (4) 物理的セキュリティ サーバ、通信回線及び教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 教育情報セキュリティに関し、教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 教育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とともに、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、緊急時に対応可能な体制を構築する。
- (8) 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合は、委託事業者を選定し、教育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こととし、外部サービス（クラウドサービス）を利用する場合は、利用に係る規定を整備し対策を講じる。
- (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教育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、教育情報セキュリティの向上を図り、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。

(教育情報セキュリティ監査及び自己点検の実施)

第7条 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教育情報セキュリティ監査及び自己点検を実施する。

(教育情報セキュリティポリシーの見直し)

第8条 教育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教育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教育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、教育情報セキュリティポリシーを見直す。

(教育情報セキュリティポリシー対策基準の策定)

第9条 第6条から第8条まで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教育情報セキュリティポリシー対策基準を策定する。

(教育情報セキュリティポリシー実施手順の策定)

第10条 教育情報セキュリティポリシー対策基準に基づき、教育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ものとする。

(教育情報セキュリティポリシー等の公開)

第11条 基本方針は、原則公開とする。ただし、教育情報セキュリティ対策基準及び教育情報セキュリティ実施手順は、公にすることにより市の学校運営に支障を及ぼす恐れがあることから非公開とする。

附 則

この基本方針は、令和8年4月1日から施行する。