下妻市教育委員会
教育情報セキュリティポリシー

第２版

制改定履歴

制定 改正	施行年月日	改正内容
制定	令和５年２月１５日	
改正	令和８年４月１日	地方自治法改正に則した運用のための改正
	年　月　日	
	年　月　日	
	年　月　日	
	年　月　日	
	年　月　日	
	年　月　日	
	年　月　日	
	年　月　日	
	年　月　日	

目次

教育情報セキュリティ基本方針.....1
1 目的.....1
2 対象とする脅威.....1
3 適用範囲.....1
4 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 教育情報セキュリティ対策基準の策定.....3
9 教育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基本方針

１．目的

本基本方針は、本市教育委員会及び市立学校（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、本市教育委員会及び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．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、業務委託管理の不備、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

３．適用範囲

(1) 実施機関の範囲

本基本方針が適用される実施機関は、本市教育委員会及び学校とする。

(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

４．職員等の遵守義務

本市教育委員会及び学校に勤務する常勤職員、非常勤職員及び臨時職員（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２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

本市教育委員会及び学校の情報資産について、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

本市教育委員会及び学校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行う。

(3) 情報システム全体の強靭性の向上

業務の効率性・利便性の観点を踏まえ、各ネットワーク系の用途に適した対策を講じる。

①校務系ネットワークにおいては、児童生徒の機微な情報や教職員等の個人情報を扱うことから、端末からの情報持ち出し制限や本人認証を確実に行う対策を講じ、情報の流出を防ぐ。また、外部からアクセスする際の認証対策の強化やインターネットの接続を前提することから、ウェブページの閲覧制限により安全なインターネット利用環境を保つ。

②学習系ネットワークにおいては、教育活動において教員等及び児童生徒が学習用情報資産にアクセスするものであり、ウェブページの閲覧制限に加えて、学習用タブレット端末の盗難や紛失時の情報漏洩対策を実施する。

(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、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、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切に対応するため、緊急時対応計画を策定する。

(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、発信する情報や利用用途により、運用手順や発信できる情報の規定及び利用における責任者を定めるなど必要な対策を講じること。

(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、適宜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．教育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教育情報セキュリティ対策基準を策定する。

９．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ものとする。

なお、教育情報セキュリティ実施手順は、公にすることにより本市教育委員会及び学校の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。