議案第 14 号
に関する資料

門真市教育情報セキュリティポリシー

情報セキュリティ基本方針

令和５年３月20日　制定

令和８年　月　日　改定

＜改定履歴＞

版数	制定／改定年月日	制定／改定	制定／改定内容
01	令和５年３月20日	新規制定	新規制定
02	令和７年３月31日	改定	文部科学省セキュリティポリシーに関するガイドラインの改定及び門真市セキュリティポリシー改定に伴う見直し
03	令和８年４月　日	改定	門真市セキュリティポリシー基本方針の改定に伴う基本方針の一部改定 情報セキュリティ基本方針の表紙・目次追加

目次

情報セキュリティ基本方針

１．目 的

教育現場における ICT 環境整備は、学習環境の多様化、教職員の働き方改革の実現等に向け、クラウドサービスの利用も含め、教育課題に対する改善の手段として効果的に進めることが求められている。

一方で、教育情報通信システムが取り扱う情報には、指導要録、答案用紙、生徒指導等の記録、進路希望調査票、児童生徒等の住所録等児童生徒のみならず学校運営上重要な情報など、外部への漏洩等が発生した場合には極めて重大な結果を招く重要性が高い情報が多数保管されている。

また、児童生徒の育成においては、学校教育に直接関わる複数の関係者により、児童生徒に関する情報が多目的で活用される。学習においても、教職員や他の児童生徒と協働学習活動を実践する際、児童生徒が生み出す情報は本人の思考の記録であるとともに学習評価の材料となり、必要に応じて他児童生徒に開示する等多目的に活用される。

さらには、令和５年３月には国において「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」が取りまとめられ、今後の教育情報システムのあるべき姿として校務系ネットワークと学習系ネットワークの統合及びパブリッククラウド環境を前提とした次世代の校務 DX の姿を示されるとともに、パブリッククラウド上で学習系・校務系情報を取り扱うに当たってこれまでの境界防御型セキュリティに代わって、強固なアクセス制御による対策を前提とするセキュリティの考え方が導入されたところであり、本市においても転換を図ったところである。

このように、学校教育においては、児童生徒の存在及び取り扱う情報の多様性・多目的性等を考慮した情報セキュリティ対策を講ずる必要があり、学校が保有する情報資産及び情報資産を取り扱うネットワーク及び教育情報通信システムを様々な脅威から防御することは、児童生徒の財産、プライバシー等を守るためにも、事務の安定的な運営のためにも極めて重要である。こうした背景を踏まえつつ、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた教育情報セキュリティポリシーを定め、明確化することにより、市民からの信頼の維持向上に寄与するものである。

２．教育情報セキュリティポリシーの構成と位置付け

教育情報セキュリティポリシーとは、門真市教育委員会及び学校が所有する情報資産について、その機密性・ 完全性・可用性を維持するための対策について、総合的、体系的に取りまとめたものである。

門真市教育委員会及び学校が所有する情報資産に係る業務については、教育情報セキュリティポリシーに即して実施することとし、教職員等及び外部委託事業者が遵守するよう浸透、普及、定着を図るものとする。

教育情報セキュリティポリシーは一定の普遍性を備えた部分（情報セキュリティ基本方針）と情報資産を取り巻く状況の変化に対応する部分（情報セキュリティ対策基準）から構成する。これらに基づき、情報通信システム毎に具体的な情報セキュリティ対策の実施手順を策定することとする。（下表参照）

教育情報セキュリティポリシーの構成

文　　書　　名		内　　容
教育情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報通信システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

３．定義

教育情報セキュリティポリシーにおける用語の意義は、次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、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　情報資産

業務遂行の過程で生み出される価値のあるものを言い､以下の切り口で抽出する。

①　直接的情報資産：データベース、データファイル、手順書、監査証跡など

②　ソフトウェア資産：業務用ソフトウェア、システムソフトウェア、開発用ツールなど

③　物理的情報資産：コンピュータ装置、通信装置、電磁的記録媒体など

④　サービス資産：ユーティリティ（空調、電源、照明）など

⑤　人的資産：資格、技能、経験など

⑥　無形資産：組織の評判、イメージなど

⑷　電磁的記録媒体

　情報システムでデータ等を記録するための磁気ディスク、磁気テープ、フロッピーディスク等をいう。

⑸　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。

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。

4　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。

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、アクセスのための認証情報又はパスワードの不適切管理、故意の不正アクセス又は不正行為による破壊盗聴・改ざん・消去等、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏洩､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

5．情報セキュリティ対策

上記4の脅威から情報資産を保護するため、以下の情報セキュリティ対策を講じる。

⑴　物理的セキュリティ対策

　サーバ、通信回線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。

⑵　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。

⑶　技術的セキュリティ対策

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。

⑷　運用

不正なアクセス等から情報セキュリティが侵害されることを防ぐため、ネットワーク監視等の運用における対策を講ずるとともに、緊急事態の発生に備えた危機管理体制を講じる。

⑸　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、利用規約及びセキュリティに関する規程の確認等、必要な対策を講じる

６．適用範囲

⑴　機関の範囲

教育情報セキュリティポリシーが適用される機関は、教育委員会、学校（門真市立学校設置条例（昭和39年６月15日条例第21号）の規定に基づく学校を言う。以下、同じ）とする。

⑵　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　教育ネットワーク、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　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。）

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

⑶　教職員等の範囲

情報セキュリティポリシーが適用される教職員等の範囲は、教育委員会に常時勤

務する職員、非常勤職員、臨時的任用職員及びこれらの職員に準じて情報資産を取り扱う特別職の職員、並びに、臨時的任用教職員、非常勤講師を含めた学校に勤務する教職員全員（本教育情報セキュリティポリシーにおいて「教職員等」という。）とする。

７．情報セキュリティ管理体制

情報資産について、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

８．教職員等の遵守義務

教職員等は、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情報セキュリティ実施手順を遵守しなければならない。

９．情報セキュリティ監査の実施

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。

10．違反に対する措置

教育情報セキュリティポリシー及びこれを受けて規定する情報セキュリティ実施手順に違反した者については、当該違反と過失の重大性に応じて、懲戒処分の対象とする。

11．教育情報セキュリティポリシーの評価・見直し

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

12．情報セキュリティ対策基準の策定

基本方針で定める情報セキュリティ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。

13. 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本市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。