富士吉田市教育情報セキュリティポリシー

教育情報セキュリティ基本方針
第 1.0 版

令和 2 年 3 月

富士吉田市教育委員会

改訂履歴

版	日付	区分	理由及び内容
第 1.0 版	令和 2 年 3 月 31 日	新規制定	

1　目的

情報技術の進歩により、多くの業務が情報システムに依存するようになっており、学校の教育活動における ICT の積極的な活用は、今後、ますます求められることが見込まれる。その中でコンピュータウィルスやシステムへの不正侵入など外部からの攻撃や、組織内部の者や委託事業者による人為的なミスでの情報漏洩や盗難が考えられ、情報に対してのリスクは高まる一方である。

これらの問題に有効かつ効果的に対応するために、教育情報セキュリティ対策に取り組むための体制を確立すると共に、富士吉田市としての方針を明確にした教育情報セキュリティポリシーを策定し、これに基づく総合的・体系的な情報セキュリティ対策を図る必要がある。

2　用語の定義

(1)　教育情報システム

情報を取り扱うシステム（ ハードウェア、ソフトウェア、通信機器、記録媒体）

(2)　ICT

情報通信技術

(3)　情報処理設備

サーバー及びその周辺装置　（主要な通信機器を含む ）

(4)　LAN

限られた範囲を結ぶネットワーク 。Local Area Network

(5)　コンピュータウィルス

第 三 者 の プ ロ グラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能のいずれか一つ以上を有するもの。

(6)　システムファイル

システムライブラリ。ＯＳや業務プログラムの実行形式ファイルやその設定情報などが格納されているファイルまたはライブラリ。

(7)　不正アクセス

不正アクセス禁止法第３ 条第２ 項に規定する不正アクセス行為その他のものが行うアクセスまたは用者が行う権限外のアクセス。

(8)　不正アクセス禁止法

不正アクセス行為の禁止等に関する法律（ 平成１１年法律第１　２　８号）

(9)　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。

(10)　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。

(11)　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。

(12)　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。

(13)　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。

(14)　校務系情報

児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校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、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報をいう。

(15)　校務外部接続系情報

校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報を想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報をいう。

(16)　学習系情報

児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校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することが想定されている情報をいう。

(17)　通信経路の分割

校務系と学習系の両環境間の通信環境を分離し、かつ、校務系と校務外部接続系の両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をいう。

(18)　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3　教育情報セキュリティポリシーの公開

富士吉田市の教育情報セキュリティに対する姿勢と一定の対策を実施していることを示す意味において、教育情報セキュリティ基本方針は公開できるものとする。

しかし、実際の取り組み内容を具体的に記載した教育情報セキュリティ対策基準、実施手順などセキュリティレベルや脆弱性の判断に活用できる文書については、情報セキュリティ対策の一環として公開しないものとする。

4　適用範囲

(1)　対象の範囲

本基本方針が適用される行政機関等は、学校（小学校、中学校をいう。以下同じ。）及び、学校が利用するネットワークに接続する機器を利用する組織とする。

(2)　情報資産の範囲

①　教育系ネットワーク、教育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　教育系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

5　指針

情報セキュリティ事故の発生を防ぐとともに、発生してしまった場合の対策も定める。また、情報資産の変化や新たな脅威に対して継続的に対策を講じていくために、運営の体制を整えるとともに、定期的に見直しについても定めるものとする。

上記内容及び「教育情報セキュリティ基本方針」を受けて、管理すべき事項についての指針を以下の通り定める。

(1)　法律上及び契約上の要求事項への適合

関連法規を明確にして遵守する。及び、契約で取り交わした内容を遵守する。

(2)　教職員等の遵守義務

全ての教職員等は、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基本方針、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を遵守する。

(3)　情報セキュリティ教育の実施

教育情報セキュリティポリシーを遵守する上で必要となる教育、訓練を実施する。

(4)　教育情報システム全体の強靭性の向上

教育情報システム全体に対し、次の三段階の対策を講じる。

①　マイナンバーを利用する事務においては、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、端末からの情報持ち出し不可設定等を実施し、教職員等の個人情報の流出を防ぐ。

②　校務系システム及び校務外部接続系システム、学習系システムにおいては、原則として、通信経路の物理的又は理論的に分離し、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定により、児童生徒及び教職員等の個人情報等の流出を防ぐ。

③　校務系システムと校務外部接続系システム及び学習系システムの間で通信する場合には、無害化通信を実施する。

④　インターネットに接続する通信においては、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。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、教育情報セキュリティクラウドの導入等を実施する。

(5)　悪意のあるソフトウェアの検出及び予防

コンピュータウィルス及び他の悪意のあるソフトウェアの検出の予防対策を実施する。

(6)　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、利用にかか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、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。

(7)　緊急時対応計画

情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。

(8)　事業継続管理

災害など対策しえない事項による事象が発生した場合に、事業を継続していくための計画を策定する。

(9)　報告責任

情報セキュリティの事件・事故について報告を行うことを義務付ける。

(10) 評価と見直し

教育情報セキュリティポリシーは普遍的な理念を除き、外部要因の変化や情報資産の変更を受けて定期的に見直しを行う。

また、ポリシーに従った運営が継続していること及び、情報セキュリティに対しての効果の状況を評価し改善を実施する。