田原本町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

令和５年４月

田原本町教育委員会

＜目　次＞

１　目的

本基本方針は、田原本町教育委員会（以下「本教育委員会」という。）並びに田原本町が設置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、教育情報セキュリティ対策に関する基本的な事項を定めることを目的とする。

２　定義

（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）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）サーバ等

ネットワーク上で情報を処理し、接続されたパソコン等の端末機に情報を提供するコンピュータ（ホストコンピュータを含む。）をいう。

（４）端末

ネットワークを通じてサーバに接続されたパソコン等の端末機をいう。

（５）電子情報

情報システム並びに情報システムの開発、保守及び運用に係る全ての電子情報（電子的、磁気的、その他人の知覚によって認識することができない方式で作られた記録をいい、プログラム等のソフトウェアを含む。）をいう。

（６）記録媒体

電子情報を保管する記録装置のうち、取りはずして使用することが可能な外部記憶装置（USBメモリ、SDカード等）、光ディスク（CD、DVD等）、光磁気ディスク（MO等）、磁気ディスク（FD等）、磁気テープその他これらに類するものをいう。

（７）アクセス

電子情報を保管する記録装置に対して、データの書き込み、読み出しを行うこと。

（８）情報資産

ネットワーク及び情報システムで取り扱う電子情報（紙等の有体物に出力された情報も含む。）をいう。

（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、必要な時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。

3　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、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、風水害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等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

４　適用範囲

（１）本基本方針が適用される実施機関等は、本教育委員会及び学校とする。ただし、田原本町情報システムの適用範囲については除くものとする。

（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教育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

５　遵守義務

教職員等（教職員、非常勤教職員及び臨時教職員をいう。以下同じ。）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。

６　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

本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

本教育委員会及び学校の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（３）物理的セキュリティ

サーバ、情報システム室、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。

（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）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。

クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用し、クラウド事業者において情報セキュリティポリシー等の遵守を担保する管理体制が整備されているかを確認する。

７　教育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教育情報セキュリティ監査及び自己点検を実施する。

８　教育情報セキュリティポリシーの見直し

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。

９　教育情報セキュリティ対策基準の策定

上記６、７及び８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。

10　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町の学校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。