第１章　　教育情報セキュリティ基本方針

（目的）

第1条　本基本方針は、東吾妻町教育委員会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、東吾妻町教育委員会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。

（定義）

第2条　本基本方針における用語は、以下のとおりとする。

（ア）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。

（イ）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。

（ウ）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。

（エ）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。

（オ）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。

（カ）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。

（キ）強固なアクセス制御

「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～」(令和５年３月８日)p.18 にて示されている、インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、利用者認証(多要素認証)、端末認証、アクセス経路の監視・制御等を組み合わせたセキュリティ対策

https://www.mext.go.jp/content/20230308-mxt_jogai01-000027984_001.pdf

（ク）SaaS 型パブリッククラウドサービス

Google Workspace や Microsoft365 等、教職員等が直接利用するサービス。利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の

機能、開発系の機能、セキュリティ系の機能等がサービスとして提供されるもの。

（ケ）IaaS ,PaaS 型クラウド

AWS や Azure 等、教育情報システムの構築時に、利用されるサービス。利用者に、CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。利用者は、そのリソース上に OS や任意機能（情報セキュリティ機能を含む。）を構築することが可能である。

（コ）BYOD(Bring Your Own Device)

会社や学校等で、従業員や学生が、個人で所有する端末を利用すること

（対象とする脅威）

第3条　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。

（ア）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

（イ）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要因による情報資産の漏えい・破壊・消去等

（ウ）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

（エ）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

（オ）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

（行政機関等の範囲）

第4条　本基本方針が適用される行政機関等は、教育委員会事務局及び学校(小学校、中学校、義務教育学校、高等学校、中等教育学校、特別支援学校を言う。以下同じ。)とする。

（情報資産の範囲）

第5条　本基本方針が対象とする情報資産は、次のとおりとする。

（ア）教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

（イ）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。)

（ウ）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

（エ）上記以外の情報資産については、情報通信技術の利用における安全性及び信頼性の確

保に関する基本要綱（東吾妻町情報セキュリティポリシー）を適用することとする。

（教職員等の遵守義務）

第6条　教職員、非常勤教職員及び臨時的任用教職員、教育委員会事務局職員(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。

（情報セキュリティ対策）

第7条　上記第 3 条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

本教育委員会の情報資産について、情報セキュリティ対策を推進する全庁的な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実施する。

3 情報システム全体の強靭性の確保

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、情報システム全体に対し、次の対策を講じる。

（ア）強固なアクセス制御による対策を講じたうえで、県域のパブリッククラウドサービスを利用することを基本とする。

（イ）SaaS 型パブリッククラウドサービスの利用にあたり、クラウドサービスを学習用途と校務用途で使い分けるよう、適切に運用しなければならない。

（ウ）教育情報システムを構築するにあたり、強固なアクセス制御による対策を講じたシステム構成の場合は、各システムにおけるアクセス権管理の徹底をしなければならない。

（エ）教育情報システムを構築するにあたり、ネットワーク分離による対策を講じたシステム構成の場合は、校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報(特に校務系)を論理的又は物理的に分離をしなければならない。

4 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、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、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正に対応するため、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、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。

9　評価・見直し

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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第8条　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。

（情報セキュリティポリシーの見直し）

第9条　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、情報セキュリティポリシーを見直す。

（対策基準の策定）

第10条　上記第 7 条、第 8 条及び第 9 条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対策基準を策定する。

なお、対策手順は、公にすることにより本教育委員会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し、業務委託先等へ開示の際は、秘密保持条項の締結を前提とする。

（情報セキュリティ実施手順の策定）

第11条　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教育委員会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し、業務委託先等へ開示の際は、秘密保持条項の締結を前提とする。