能勢町教育委員会
教育情報セキュリティポリシー

令和７年10月

はじめに 「能勢町教育委員会 教育情報セキュリティポリシー」について

能勢町教育委員会 教育情報セキュリティポリシーとは、能勢町教育委員会および義務教育学校が保有する教育情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

教育情報セキュリティポリシーは、教育情報資産のセキュリティを確保するための考え方、体制、組織、運用等を規定し、業務の安定的な運用を図るものである。また、教育情報資産に関する業務に携わる教育委員会の全職員および学校の全ての教職員に浸透、普及、定着させ、個人情報、教育情報資産を守ることを目的としている。さらに、技術の進歩や社会情勢によりセキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要であるため、これらは常に水準の向上を図り、継続的な評価・見直しを実施する。

また、ICT 機器の管理に関しては、令和元年 12 月施行の「能勢町立小・中学校における ICT 機器等の管理に関する要綱」に定めるところではあるが、GIGA スクール構想の実現に向けて、令和 5 年 3 月の「GIGA スクール構想の下での校務 DX について」の中で「教育情報セキュリティポリシーに関するガイドラインの改訂」が文部科学省より示されたことから、「能勢町立小・中学校における ICT 機器等の管理に関する要綱」を廃し、ICT 機器の管理に加え、その運用やセキュリティに関する事項を加え、「能勢町教育委員会 教育情報セキュリティポリシー」として改めて定めることとした。

以上を踏まえ、上記ガイドライン及び「能勢町情報セキュリティポリシー（令和 5 年 12 月改定)」に照らし、「能勢町教育委員会 教育情報セキュリティ基本方針」に基づき、各情報システムの具体的な「能勢町教育委員会 教育情報セキュリティ対策基準」を策定する。

改定履歴

・令和 7 年 10 月　初版発行

参考資料

文部科学省

「教育情報セキュリティポリシーに関するガイドライン」令和 7 年 3 月

https://www.mext.go.jp/content/20250325-mxt_jogai01-100003157_1.pdf

目次

第１章　教育情報セキュリティ基本方針

1.　目的

本基本方針は、能勢町が保有する教育情報資産の機密性、完全性及び可用性を維持するためのものである。

IT 技術の進歩等により、教育行政及び学校教育の DX（※定義は下記を参照）の実現が期待されている一方で、学校教育で取り扱う情報には、職員及び児童生徒の個人情報など、部外に漏洩等した場合に極めて重大な結果を招くものが多数含まれている。情報及び情報を取り扱う情報システムを様々な脅威から防御することで、職員及び町民のプライバシーを守るとともに、全てのネットワーク及び情報システムに高度な安全性を確保することで、各種業務の安定的かつ柔軟な運用を図る。そのために、教育委員会及び学校の情報セキュリティ対策の基本的な事項を定めることを目的とする。

2.　用語の定義

能勢町教育委員会 教育情報セキュリティ基本方針における用語の定義は、それぞれ下表に定める。

用語	定義
情報資産	組織が所有している情報や、それらを管理するシステムや機器などを指す。
機密性	情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。
完全性	情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
可用性	許可された利用者が必要な時にアクセスできることを確実にすること。
DX	デジタルトランスフォーメーション。デジタル技術を活用して業務プロセスを改善していくだけでなく、ネットとリアルの両面から業務モデルや組織文化や風土そのものを変革すること。
不正アクセス	悪意ある第三者が詐欺行為や個人情報の取得などを目的に、他人のＩＤやパスワードを使用しサービスを悪用することや、不正にコンピュータに侵入する犯罪。
ウイルス攻撃 サイバー攻撃	ネットワークを介してウイルスを送りこむなどして、サーバやパソコンなどの情報端末に対して、金銭や個人情報を盗んだり、システムの機能を停止させたりすることを目的とした攻撃。
クラウド サービス	従来は利用者が手元のコンピュータで利用していたデータやソフトウェアをネットワーク経由で、サービスとして利用者に提供するものをいう。これまで機材の購入やシステムの構築、管理などにかかるとされていた様々な手間や時間の削減をはじめとして、業務の効率化やコストダウンを図れるというメリットがあるといわれている。
教育情報 システム	教育情報を扱う各種サービスを指す。校務支援システム、グループウェアツール、各種授業支援アプリケーションなど。

3. 職員及び教職員の遵守義務

教育委員会及び学校が保有する情報資産に関する業務に携わるすべての職員等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって、関係法令、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。

4. 対象とする脅威

教育情報資産に対する脅威として以下の５項目を想定し、教育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教育情報資産の漏洩・破壊・改竄・消去、重要情報の許取、内部不正等。

（２）教育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教育情報資産の漏洩・破壊・消去等。

（３）災害等による電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害及びサービス、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）クラウドサービスのサービス遅延や停止、回線障害等の外部サービスに依存した情報システムを利用した業務の停止。

5. 適用範囲

（１）行政機関等の範囲

能勢町が保有する教育情報資産及びこの情報資産に接する職員及び外部委託事業者等に適用する。

（２）教育情報資産の範囲

本基本方針が対象とする教育情報資産は、次のとおりとする。

① 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 教育情報システムで取り扱う情報（そ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。

6. 教育情報セキュリティ対策

上記４に示す脅威から教育情報資産を保護するために、以下の教育情報セキュリティ対策を講じる。

（１）物理的セキュリティ

情報システムを設置する施設等への不正な立入り、通信回線等及び教職員の情報機器の管理について、物理的な対策を講じる。

（２）人的セキュリティ

教育情報セキュリティに関し、教職員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対策を講じる。

（3）技術的セキュリティ

教育情報資産へのアクセス制御、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。

（4）運用

教育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、運用面の対策を講じるものとする。また、教育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は、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。

7. 教育情報セキュリティ対策基準の策定

上記6に規定する対策等を実施するにあたり、具体的な遵守事項およ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。教育情報セキュリティ対策基準は、公にすることにより能勢町の行政運営に重大な支障を及ぼすおそれがあることから、原則として非公開とする。

8. 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を遵守して教育情報セキュリティ対策を実施するために、具体的な手順を定めていく必要がある。そのため、教育情報セキュリティ対策基準の基本的な要件に基づき、所属長及び学校長等が教育情報資産の教育情報セキュリティ実施手順を作成するものとする。教育情報セキュリティ実施手順は、公にすることにより能勢町の行政運営及び学校運営に重大な支障を及ぼすおそれがあることから、原則として非公開とする。

9. 監査および自己点検による見直しの実施

情報セキュリティを取り巻く状況の変化への対応や、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に、必要に応じて学校教育情報セキュリティポリシーの監査及び自己点検を実施する。

第1章までを公開し、第2章以降は非公開とする