熊本県教育委員会情報セキュリティ基本方針

熊本県教育委員会
（令和３年３月制定　教育政策課）
（令和８年２月改訂　教育政策課）

熊本県教育委員会情報セキュリティ基本方針

目次

第１　目的

本基本方針は、熊本県教育委員会（以下「本委員会」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、本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。

第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。

①ハードウェア

電子的な回路等により構成され、情報処理を行う機器

②ソフトウェア

ハードウェアに一定単位の情報処理を指示するために作成された、動作制御の手順の総称

（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）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。

（４）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５）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。

（６）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。

（７）可用性

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。

（８）学習系

教員及び生徒が授業等で利用する情報システム及びデータをいう。

（９）校務系

教務及び校務情報システム及びその情報システムで取り扱うデータをいう。

（１０）通信経路の分割

学習系と校務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。

第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）情報資産の無断持出し、無許可ソフトウェアの仕様等の規定違反、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

第４　適用範囲

１　適用範囲

本基本方針が適用される機関は、教育委員会本庁各課、地方機関及び県立学校とする。ただし、教育委員会事務局については、本委員会が運用する情報システムを利用する所属のみとする。

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）ネットワーク及び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）ネットワーク及び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）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

第５　職員等の遵守義務

本委員会の保有する情報資産に関する業務に携わるすべての職員（臨時的任用教職員、非常勤講師を含めた教職員全員（以下「教職員等」という。）、事務局職員を含む。）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で規定するもののほか、関係

する法令を遵守しなければならない。

第６　情報セキュリティ対策

上記第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向上

情報システム全体に対し、次の対策を講じる。

①校務系においては、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や端末への多要素認証の導入等により、生徒情報等の流失を防ぐ。

②学習系においては、不適切なサイトへの接続を不可とするセキュリティ対策を実施する。

（４）物理的セキュリティ

サーバ、情報システム室、通信回線、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、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、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（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。

第７　情報セキュリティ監査及び自己点検の実施

情報セ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ュリティ監査及び自己点検を実施する。

第８　情報セキュリティポリシーの見直し

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に新たな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。

第９　情報セ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情報セキュリティ対策基準を策定する。

第１０　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、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより本委員会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。