# 江津市教育委員会サイバーセキュリティを確保するための方針

（江津市教育情報セキュリティポリシー）

令和８年３月

江津市教育委員会

（目次）

1　目的

小・中学校が取り扱う情報には、児童・生徒の個人情報のみならず保護者、教職員、その他地域住民に関する情報等学校運営に欠かせない重要な情報等が数多く含まれ、外部への情報漏えい等が発生した場合には、極めて重大な結果を招くおそれがある。

したがって、本市の教育情報ネットワークにおいて、個人情報を始めとする情報資産を漏えいや改ざん、コンピュータウイルスによるシステム障害、災害や事故等の様々な脅威から防御することは、保護者や地域住民等から信頼される安心・安全な学校づくりには必要不可欠なことである。

こうしたことから、市立小・中学校における情報セキュリティ対策を総合的、体系的かつ具体的に整備することを目的に、教育情報セキュリティポリシーを定めることとする。

このうち基本方針は、各小・中学校が所管する教育情報資産においても、本市全体の基本方針と共通のものであるとの認識の上に立ち、江津市サイバーセキュリティを確保するための方針を準用するものとする。

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) 教育情報システム

本市の学校教育において使用されるコンピュータ、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) 教育情報資産

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

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

(4) 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。

(5) 教育情報セキュリティポリシー

本方針及び教育情報セキュリティ対策基準をいう。

(6) 教職員

学校教育法（昭和22年法律第26号）第37条及び第49条に規定する者で、市長が設

置する小・中学校に従事する職員並びにその他の支援員等をいう。

(7) 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。

(8) 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。

(9) 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。

(10) マイナンバー利用事務系(個人番号利用事務系)

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(11) LGWAN接続系

LGWANに接続された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（マイナンバー利用事務系を除く。）。

(12) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された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。

(13) 通信経路の分割

LGWAN接続系とインターネット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。

## 3 対象とする脅威

教育情報資産に対する脅威として、以下の脅威を想定し、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外部進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、重要情報の搾取、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、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

(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障害からの波及等

4　適用範囲

(1)行政機関の範囲

本基本計画が適用される行政機関は、教育委員会、学校等の所管するものとする。

(2)情報資産の範囲

本方針が対象とする情報資産は、教育委員会及び学校等が所管する個人情報をはじめとする次に掲げる資産とする。

①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次期的記録媒体

②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 教育情報セキュリティポリシーの位置付けと教職員等の義務

教育情報セキュリティポリシーは、本市が所管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り、教育情報セキュリティ対策の頂点に位置するものである。

したがって、本市の全ての教職員、教育情報資産に係る業務に携わる教育委員会事務局の職員、指定管理者及び外部委託事業者に属する者（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つとともに、業務の遂行に当たって、教育情報セキュリティポリシーを遵守する義務を負うものとする。

6 教育情報セキュリティ対策

３で示した脅威から教育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ずる。

(1) 組織体制

本市の教育情報資産について、教育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) 教育情報資産の分類と管理

本市の保有する教育情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき教育情報セキュリティ対策を実施する。

(3) 教育情報システム全体の強靭性の向上

教育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、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マイナンバー利用事務系においては、原則として、他の領域との通信をできない

ようにしたうえで、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、住民情報の流出を防ぐ。

②LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、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、都道府県及び市区町村のインターネットとの通信を集約したうえで、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

サーバ、電算室、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

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の確認、業務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、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

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し、運用改善を行い、情報セキュリティの向上を図る。教育情報セキュリティポリシーの見直しが必要な場合は、

適宜教育情報セキュリティポリシーの見直しを行う。

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となった場合には、保有する情報及び利用する情報システムに係る教委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、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

本市の様々な教育情報資産について、7の教育情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。このため、教育情報セキュリティ対策を行う上で必要となる基本的な要件を明記した教育情報セキュリティ対策基準を策定する。

なお、教育情報セキュリティ対策基準は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがある情報資産であることから非公開とする。

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を遵守して情報セキュリティ対策を実施するために、情報資産ごとに実施手順等をそれぞれ定めていく必要がある。このため、情報資産に対する脅威及び情報資産の重要度に対応する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、教育情報資産の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市の行政運営に重大な支障を及ぼすおそれがある情報資産であることから非公開とする。