益田市教育情報セキュリティ基本方針（R7.1.1）

１ 目的

この基本方針は、益田市教育委員会（以下「市教育委員会」）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、様々な脅威に対する抑止、予防、検知及び回復について、組織的かつ計画的に取り組むための統一的な方針であり、その基本的な考え方及び方策を定めることを目的とする。

２ 定義

（１） ネットワーク

市教育委員会が教育の情報化の充実を目的として、市立学校及び教育機関の情報の共有化を図るために整備した通信網、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

電子計算機(ネットワーク、ハードウェア及びソフトウェア)及び 記録媒体で構成され、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

本基本方針及び教育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。

（８） 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。

３ 対象とする脅威

教育情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生頻度や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（1）　不正アクセス、ウイルス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、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

4　適用する職員の範囲

本基本方針を適用する職員の範囲は次のとおりとする。益田市教育委員会事務局（以下「事務局」という。）職員、市立学校の県費負担教職員及び市費負担職員（以下「教職員等」という。会計年度職員及び非常勤職員を含む。）並びに外部委託事業者とする。

5　適用範囲

（1）　行政機関の範囲

本対策基準が適用される行政機関の範囲は、市教育委員会及び益田市立小学校及び中学校設置条例（昭和 39 年益田市条例第 21 号）第 2 条に規定する小学校及び第 3 条に規定する中学校（以下「学校」）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。

・ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

・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。）

・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　教職員等の遵守義務

教職員等は、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。

また、外部委託事業者に業務を行わせようとする場合は、契約又は別途取決めを行うことにより、教育情報セキュリティポリシーを守らせるために必要な措置を講じなければならない。

7　統一的な情報セキュリティの確保

統一的な情報セキュリティの確保のため、最高教育情報セキュリティ責任者（CISO）、統括教育情報セキュリティ責任者及び教育情報セキュリティ責任者をおく。

８ 情報の分類及び管理

統括教育情報セキュリティ責任者は、情報資産について、情報の機密性、完全性、可用性等を踏まえた分類を行うとともに、適切な管理が行われるよう、教育情報セキュリティ管理者（事務局の所属長及び市立学校長をいう。）及び教育情報システム管理者（情報システム所管課長をいう。）に対して指導又は助言を行う。

９ 情報セキュリティ対策

上記３で示した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ずるものとする。

（１） 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。

（２） 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。

（３） 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。

（４） 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等、情報セキュリティポリシーの運用面の対策を講じる。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、緊急時対応策を講じる。

10 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責任者は、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。

11 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。

12 教育情報セキュリティ対策基準の策定

上記９、10 及び 11 の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。そのため、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ものとする。

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、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、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、教職員等が所掌する情報資産の情報セキュリティ実施手順を別途策定するものとする。 なお、教育情報セキュリティ対策基準及び教育情報セキュリティ実施手順は、公にすることにより学校の運営に重大な支障を及ぼすおそれのある情報資産であることから、非公開とする。