近江八幡市情報セキュリティポリシー

令和５年３月

近江八幡市

目　　次

第１章　情報セキュリティ基本方針

1.1　目的

この方針は、本市の管理する情報システムで取り扱う個人情報並びに行政運営上の情報の破壊、改ざん及び外部への漏洩が生じた場合の重大性を鑑み、情報セキュリティに関する基本的な事項について定め、情報資産の適切な管理を図り、もって市民の財産及びプライバシー等を守るとともに、本市における情報資産に関する事務の安定的な運営を確保することを目的とする。

1.2　定義

（１）　ネットワーク　実施機関の内部又は相互間を接続するための通信網、その構成機器及び記録媒体で構成され、処理を行う仕組み（地方公営企業の業務のために用いるもの及び小・中学校、コミュニティセンター等において専ら教育・研修のために用いるものを除く。）をいう。

（２）　情報システム　実施機関の電子計算機及び記録媒体で構成され、業務処理を行う仕組み（地方公営企業の業務のために用いるもの及び小・中学校、コミュニティセンター等において専ら教育・研修のために用いるものを除く。）をいう。

（３）　情報セキュリティポリシー　この方針及び第７条に規定する情報セキュリティ対策基準をいう。

（４）　情報セキュリティ　情報資産の機密の保持、正確性及び完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（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）　マイナンバー利用事務系　個人番号利用事務、戸籍事務等に係る情報システム及びデータをいう。

（９）　LGWAN 接続系　総合行政ネットワーク（以下「LGWAN」という。）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。

（１０）　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係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。

（１１）　無害化通信　インターネットメール本文のテキスト化、端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がないこと等の安全が確保された

通信をいう。

1.3　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）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、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・広範囲にわたる疫病による要因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、水道供給の途絶等の提供サービスの障害からの波及等

1.4　適用範囲

（１）機関の範囲

本基本方針が適用される機関は、近江八幡市議会、近江八幡市長、近江八幡市教育委員会、近江八幡市選挙管理委員会とする。

（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

1.5　職員等の遵守義務

職員、非常勤職員、臨時職員等及びその他市にかかる業務に従事する者（以下「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、業務の遂行にあ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。

1.6　情報セキュリティ対策

上記１．３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

本市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

本市の所有する情報資産を機密性、完全性、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行う。

（３）情報システム全体の強靭性の向上

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、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、滋賀県及び本市のインターネットとの通信を集約した上で、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、情報システム室、通信回線及び職員等のパソコン等の端末の管理について、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、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）外部サービスの利用

外部委託する場合には、外部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、外部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。

約款による外部サービスを利用する場合には、利用にかか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。

1.7　情報セキュリティ監査及び自己点検の実施

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、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。

1.8　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新たに対策が必要となった場合には、情報セキュリティポリシーを見直す。

1.9　情報セキュリティ対策基準の策定

上記１．６、１．７及び１．８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等を策定する。

1.10　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ことから非公開とする。