鯖江市情報セキュリティ基本方針

１　目的

鯖江市が保有する情報資産の機密性、完全性および可用性を維持するため、本市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およびその構成機器（ハードウェアおよびソフトウェア）をいう。

（２）情報システム

コンピュータ、ネットワークおよ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、完全性およ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

本基本方針およ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ことを確保することをいう。

（６）完全性

情報が破壊、改ざんまた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（個人番号利用事務系）

個人番号利用事務（社会保障、地方税または防災に関する事務）または戸籍事務等にかかわる情報システムおよびデータをいう。

（９）LGWAN 接続系

人事給与、財務会計および文書管理等 LGWAN に接続された情報システムおよ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およびその情報システムで取り扱うデータをいう。

（１１）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。

（１２）無害化通信

インターネットメール本文のテキスト化や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無い等、安全が確保された通信をいう。

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、機械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および業務の停止等

（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　適用範囲

（１）行政機関等の範囲

本基本方針が適用される行政機関等は、市長部局、各行政委員会、議会、地方公営企業、教育委員会事務局、監査委員事務局、鯖江・丹生消防組合消防本部、福井県丹南広域組合事務局、鯖江広域衛生施設組合事務局および公立丹南病院組合事務局の一部（共通の情報システムを利用する範囲）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。

ア　ネットワーク、情報システムならびにこれらに関する設備および電磁的記録媒体

イ　ネットワークおよ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）

ウ　情報システムの仕様書およびネットワーク図等のシステム関連文書

５　職員等および外部委託事業者の遵守義務

市が所掌する情報資産に関する業務に携わる全ての職員等および外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当た

って情報セキュリティポリシーおよ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。

６　情報セキュリティ対策

上記の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、管理するための全庁的な体制を確立する。

（２）情報資産の分類と管理

本市の保有する情報資産をその内容に応じて分類し、その重要度に応じた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

情報システム全体に対し、次の三段階の対策を講じる。

ア　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。

イ　LGWAN 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。

ウ　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、県および県内市町のインターネット接続口を集約した、自治体情報セキュリティクラウドに接続するものとする。

（４）物理的セキュリティ

サーバ等、情報システム室等、通信回線等および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、全ての職員等および外部委託事業者が遵守すべき事項を定めるとともに、十分な教育および啓発を行う等の人的な対策を講ずる。

（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ずる。

（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の利用

委託をする場合には、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ガイドラインを定め、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順守状況を検証するため、定期的または必要に応じて情報セキュリティ監査およ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、情報セキュリティポリシーの見直しを行う。

７　情報セキュリティ監査および自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査および自己点検を実施する。

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および自己点検の結果、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およ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、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記７、８および９に規定する対策等を実施するために、具体的な遵守事項およ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。

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。