第１章　情報セキュリティ基本方針

第１　目的

本基本方針は、本市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ことを目的とする。

第２　用語の定義

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　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　情報資産

（１）ネットワーク、情報システム及びこれらに関する設備、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。）

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　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。

６　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。

７　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。

８　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。

９　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。

10　LGWAN 接続系

人事給与、財務会計等 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。

11　インターネット接続系

インターネットメール、公共施設予約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。

12　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。

13　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。

14　職員等

地方公務員法第３条に定める本市の職員及び本市の小中学校等に勤務し、本市が管理する情報資産を職務で利用する者をいう。

15　外部委託者

契約に基づき操作等を認められた事業者をいう。

第３　情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は、次の各号に定めるものとする。

１　適用対象資産

適用対象資産は、本市が保有する情報資産とする。

２　適用対象者

適用対象者は、本市が保有する情報資産に接する職員等及び外部委託者とする。

第４　職員等及び外部委託者の義務

職員等及び外部委託者は、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。

第５　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６　情報セキュリティ対策

本市の情報資産を第５に規定する脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

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

⑴　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。

⑵　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。

⑶　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、県と市区町村のインターネット接続口を集約した上で、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対策

サーバ等、情報システム室等、通信回線等及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　人的セキュリティ対策

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対策

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、危機管理対策を講じる。

8　外部委託と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する等必要なセキュリティ対策を講じる。

第７　情報セキュリティ対策基準の策定

第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８　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。

第９　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されていることを検証するため、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。

第10　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になった場合には、情報セキュリティポリシーを見直す。