第1章　セキュリティ基本方針

１　基本方針の目的

本基本方針は、本町情報セキュリティポリシーの体系及び本町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、本町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。

２　用語の定義

（１）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。

（２）情報資産

情報システム及びネットワークで取り扱われる全ての情報（電磁的に記録されている情報及び出力した媒体を含む。）をいう。

（３）情報システム

電子計算機及び電磁的記録媒体で構成され、情報を処理するための仕組みをいう。

（４）ネットワーク

本町の情報システム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。

（５）装置

本町の情報システムに関わる装置をいう。

（６）端末

職員等が、個別に情報システムの情報を処理する装置をいう。

（７）職員等

雇用関係にある職員（常勤の特別職、一般職、再任用職員、会計年度任用職員、臨時的任用職員をいう。）をいい、雇用関係にない者は含まれない。

（８）第三者

職員等に該当しない者をいう。

（９）情報処理施設

装置（情報機器、サーバ等）が設置されている建物や部屋をいう。

(10) サーバ設置区画

重要な情報資産を保護する目的で設置された高いセキュリティが保たれたサーバ等が設置されている区画をいう。

(11) セキュリティ事故

本町の情報資産の正常な運営や維持がセキュリティ上の問題や不正な攻撃等によって妨げられる事象をいう。

(12) 脅威

情報資産の価値を失わせる事象（不正アクセス等の意図的脅威、入力ミス等

の偶発的脅威、災害等の環境的脅威等）をいう。

(13) 機密性

許可された者のみが情報にアクセスできることを確実にすることをいう。

(14) 完全性

情報及び処理方法が正確であること及び完全であることを保護することをいう。

(15) 可用性

許可された者が必要なときに情報にアクセスできることを確実にすることをいう。

(16) 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。

(17) 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）。

(18) 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。

(19) 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。

(20) 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。

(21) 情報セキュリティインシデント

望まないあるいは予期しない単独もしくは一連の情報セキュリティに関する事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。具体的にはサイバー攻撃、意図的な要因による情報漏えい、破壊、改ざん、機器故障等の非意図的な要因による情報漏えい、破壊、改ざん等をいう。

(22) CSIRT (Computer Security Incident Response Team)

コンピュータやネットワーク上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査を行ったりする組織の総称。

3　情報セキュリティポリシーの文書体系

情報セキュリティポリシーを下記に定め、各々を明文化するものとする。

（１）情報セキュリティ基本方針

本町の情報セキュリティ対策に関する基本的な方針（本基本方針）をいう。

（２）情報セキュリティ対策基準

情報セキュリティ基本方針に基づき情報セキュリティ対策を実施する上での統一的な対策基準をいう。

4　適用範囲

（１）適用機関の範囲

本基本方針が適用される行政機関は、町長部局、教育委員会事務局、議会事務局及びその他関係機関とする。

（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。）

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

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

6　職員等の遵守義務

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情報セキュリティポリシーを遵守しなければならない。

7　情報セキュリティ対策の実施

情報資産を脅威から保護するため、以下のセキュリティ対策を実施するものとする。

（１）組織体制

情報セキュリティポリシーに基づき、情報セキュリティ対策を推進するため、副町長を最高責任者とする組織横断的なセキュリティ推進体制を確立する。

（２）情報資産の分類と管理

本町の保有する情報資産を重要度分類基準に従って分類し、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。

②　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。

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、県及び町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端末等の管理について、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、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。

8　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、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。

9　情報セキュリティポリシーの評価及び見直し

情報セキュリティを取り巻く状況、環境の変化や、情報セキュリティポリシーの遵守状況等を考慮し、情報セキュリティポリシーがその実効性を維持するよう、評価及び見直しを行うものとする。