情報セキュリティポリシー　基本方針

１　目的

本基本方針は、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　定義

本情報セキュリティポリシーで使用する用語に関して、以下のように定義する。

【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。

【記録媒体】

情報を記録するために用いる電磁的記録媒体をいう。

【情報】

職員等が職務上作成し、又は取得した全ての文書等のうち電磁的に記録されたもの及び電磁的記録の出力に用いる紙等の有体物

【情報資産】

川島町が保有する、住民・行政に関する情報、及びそれらの情報を管理する仕組み（業務システムやシステム運用・保守のマニュアル、資料等を含む）の総称。

【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。

【情報セキュリティ】

情報資産の機密性、完全性、可用性を維持することをいう。

・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。
・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。
・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。

【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。

【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）又は住民基本情報や戸籍事務等に関わる情報システム及びデータをいう。

【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）

【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。

【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。

【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・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、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　適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、地方公営企業とする。

（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　職員等の遵守義務

職員、会計年度任用職員及び臨時的任用職員（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。

職員等の情報セキュリティポリシーに対する違反が判明した場合、その内容を町長に報告する。又、地方公務員法をはじめとする各関連法令に基づき、懲戒等の処分の対象となる場合がある。

６　情報セキュリティ対策

上記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。詳細内容は、第２章情報セキュリティポリシー対策基準で定める。

（１）組織体制

本町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のもと行うものとする。

（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化の向上

情報セキュリティの強化を目的とし、次の対策を講じる。

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している。高度な情報セキュリティ対策として、都道府県と市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している。

（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

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、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。

（８）外部委託

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を講じる。

（９）評価・見直し

情報セキュリティポリシーを遵守するため､必要に応じて情報セキュリティ監査の実施等を行い、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。