第１章　情報セキュリティ基本方針

第１　目的

本町の情報システムで取り扱われる情報には、町民の個人情報や行政運営上重要な情報など、外部に漏えいした場合に極めて重大な被害をもたらすおそれがある情報が多数含まれていることから、情報資産、情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、町民の財産及びプライバシーを守るため、かつ、事務の安定的な運営のために必要不可欠であり、本町に対する町民からの信頼の向上に寄与するものである。そのため、本ポリシーのうち、情報セキュリティ基本方針では、本ポリシーの対象範囲、情報資産の取扱いその他情報セキュリティ対策の基本的な事項について定めるものとする。

第２　定義

(1) ネットワーク

町が管理しているコンピュータを相互に接続するための通信網並びにその通信網を構成する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。

(4) 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。

(5) 完全性

情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

(6) 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。

(7) 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、地方税又は防災に関する事務をいう。）又は戸籍事務等に関わる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。

(8) LGWAN接続系

マイナンバー利用事務系を除く、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。

(9) 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の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。

(10)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。

(11)無害化通信

インターネットメール本文のテキスト化又は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等、安全が確保された通信をいう。

第３　情報資産への脅威

情報資産への脅威として、次に掲げる事項が想定されるため、６の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、重要情報の詐取又は内部不正

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用その他情報資産の取扱いに関する規定違反、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、委託管理の不備、マネジメントの欠陥、機器故障の非意図的要因による情報資産の漏えい・破壊・消去

(3) 地震、落雷、火災その他の災害によるサービス及び業務の停止

(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

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等による波及

第４　適用範囲

１　組織の範囲

情報セキュリティ基本方針が適用される組織は、松前町行政手続等における情報通信の技術の利用に関する条例（平成18年条例第１号）第２条第３号に規定する町の機関及び伊予消防事務組合（本町の情報システムを利用する部署に限る。）とする。

２　情報資産の範囲

情報セキュリティ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並び

(2) に電磁的記録媒体

(2) ネットワーク及び情報システムで取り扱う情報（これらを印刷した書面を含む。）

(3) 情報システムの仕様書、ネットワーク図等のシステム関連文書

第５　職員等の義務

職員等（地方公務員法に規定する一般職及び特別職のすべての職員並びに本庁と労働派遣契約等により従事するものをいう。以下同じ。）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、本ポリシーを遵守する義務を負うものとする。

第６　情報セキュリティ対策

３に掲げる脅威から、４に定める情報資産を保護するため、次の対策を講ずるものとする。

(1) 組織体制

情報資産について、情報セキュリティ対策を推進する体制を確立するものとする。

(2) 情報資産の分類と管理

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行うものとする。

(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、業務の効率性及び利便性の観点を踏まえつつ、情報システム全体に対し次の対策を講ずるものとする。

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、端末からの情報の持ち出しを不可とする設定及び端末へログインする際の多要素認証の導入により、情報の流出を防ぐ。

イ　LGWAN接続系においては、通信経路の分割を行い、LGWAN接続系とインターネット接続系の両システム間で通信を行う場合にあっては、無害化通信を行う。

ウ　インターネット接続系においては、通信経路の分割を行い、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として、都道府県及び市区町村のインターネットとの通信を集約し、自治体情報セキュリティクラウドを導入する。

(4) 物理的セキュリティ対策

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明確に定めるとともに、職員等に対し、十分な教育、啓発及び訓練を行えるよう人的な対策を講ずるものとする。

(6) 技術的セキュリティ対策

情報資産へのアクセス制御、ネットワーク管理及び不正プログラム対策、不正アクセス対策等の技術的な対策を講ずるものとする。

(7) 運用

ア　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その他の情報セキュリティの運用面の対策を講ずるものとする。

イ　情報資産に対するセキュリティ侵害が発生した場合に迅速かつ適切に対応するため、情報セキュリティインシデント発生時の対応手順書を策定するものとする。

(8) 業務委託及び外部サービス（クラウドサービス）の利用

ア　業務委託を行う場合には、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情報セキュリティ対策が確保されているかどうかを確認の上、必要に応じて当該契約に基づく措置を講ずるものとする。

イ　外部サービス（クラウドサービス）を利用する場合には、利用するサービスの約款等を確認し、必要な情報セキュリティ対策を講ずるものとする。

ウ　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。

第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が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ものとする。

第８　評価及び見直しの実施

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又は情報資産を取り巻く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の見直しを行うものとする。

第９　情報セキュリティ対策基準の策定

６から８までに規定する情報セキュリティ対策等を実施するため、具体的な遵守事項及び判断基準を明記した情報セキュリティ対策基準を策定するものとする。

第 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。ただし、情報セキュリティ実施手順については、公にすることにより本町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。