第１章　情報セキュリティ基本方針

１　目的

当町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上重要な情報など、部外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う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、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが当町に対する町民からの信頼の維持向上に寄与するものである。

また、個人番号（マイナンバー）制度により、当町としても個人番号を含む特定個人情報を取り扱うことから、より強固な情報セキュリティが求められている。

そのため、当町の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を強化するために西伊豆町情報セキュリティポリシーを国のガイドラインに沿って策定することとする。このうち、情報セキュリティ基本方針については当町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

当町の情報セキュリティポリシーは、下記の要求事項を確実に遵守することを目的とする。

ア　保有する情報資産を、不正な第三者からのアクセスから保護すること。
イ　保有する情報資産を、不正な第三者により故意又は不注意な行為により開示されないこと。
ウ　保有する情報資産を、不正な第三者による改ざんから保護すること。
エ　許可された者が必要なときに情報が利用できること。
オ　法規制上の要求事項を遵守すること。

２　定義

情報セキュリティポリシーで使用される用語の定義については、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省　平成 13 年３月 30 日策定／平成 30 年９月 25 日一部改定／令和２年 12 月 28 日一部改定／令和４年３月 25 日／令和５年３月 28 日一部改定）、国際標準規格（ISO/IEC27001：2005 等）及び各種公的な規格に準じ、以下のとおり定める。

(1) 情報

当町の業務遂行に伴って取り扱う全ての情報（紙及び電磁的記録媒体に記録されたもの、会話等を含む）をいう。

(2) 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。

(3) 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。

(4) 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。

(5) 情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

(6) 資産

組織にとって価値を持つもの。

(7) 情報資産

当町における情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料など）の総称。ネットワーク及び情報システム。またその情報システム上で取り扱う電磁的に記録されたデータ。

(8) 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。

(9) 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。

(10) 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。

(11) マイナンバー利用事務系（番号系）

「行政手続における特定の個人を識別するための番号の利用等に関する法律」に規定された個人番号利用事務（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。

(12) ＬGWAN接続系（情報系）

一般行政事務に使用することを目的とし、総合行政ネットワーク（以下「ＬGWAN」という。）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。）

(13) 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。

(14) 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。

(15) 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、委託管理の不備、マネージメントの欠陥、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障害からの波及等。

4　対象の範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、町長部局、行政委員会事務局、議会事務局、教育委員会事務局（小学校及び中学校の教職員及びその教職員の担当する業務を除く）、地方公営企業及び町長が特に定める機関を対象とする。

（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

（3）対象者

上記（1）に定める組織に属する職員（非常勤職員及び会計年度任用職員を含む。以下「職員等」という。）及び上記（2）に定める対象となる情報の取扱いを委託された者（以下「委託事業者」という。）とする。

5　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及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。

（1）組織体制

当町の情報資産について、情報セキュリティ対策を推進・管理する全庁的な組織体制を確立する。

（2）情報資産の分類と管理

当町が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

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。

②ＬGWAN接続系においては、ＬGWANと接続する業務システムと、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。高度なセキュリティ対策として、静岡県及び市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

サーバー、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

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、業務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(クラウドサービス)の利用

業務委託を行う場合には、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(クラウドサービス)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運用手順を定め、ソーシャルメディアサービスで発言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。

(9) 評価・見直し

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し、運用改善を行い情報セキュリティ向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜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。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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６、７及び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。

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当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。