伊仙町情報セキュリティポリシー

平成２７年１０月　１日　策定

令和　２年　２月　１日　改定

令和　７年　11月　１日　改定

伊　仙　町

〈　目　　次　〉

第１編

第２編
第１章　情報セキュリティ基本方針

第１編

伊仙町サイバーセキュリティを確保するための方針

伊仙町サイバーセキュリティを確保するための方針

１．目的

本方針は、伊仙町（以下「町」という。）が管理・運用する情報システム及び情報資産の安全を確保し、町民サービスの継続的提供と町民の信頼を維持することを目的とする。町は、サイバー攻撃、災害、事故等による被害の防止および軽減を図り、迅速な復旧と再発防止を実現する体制を整備する。

２．基本的考え方

ア　町は、サイバーセキュリティの確保を行政運営の基盤と位置付け、全職員が一体となって取り組む。

イ　情報資産の機密性、完全性及び可用性を確保し、行政サービスの安定運用を維持する。

ウ　個人情報及び機微情報を適正に管理し、町民の信頼を損なうことのないよう努める。

エ　関係機関、他自治体、専門機関と連携し、最新の脅威や対策に対応する。

３．組織体制

ア　町長は、サイバーセキュリティ確保に関する最高責任者として、本方針の実施及び推進に関する最終的な責任を負う。

イ　副町長は、町の CISO（Chief Information Security Officer：情報セキュリティ統括責任者）として、具体的な方針の運用及び監督を行う。

ウ　総務課は、サイバーセキュリティ対策の企画・実施・点検を統括し、必要に応じて各課に対する指導・支援を行う。

エ　町は、必要に応じて CSIRT（Computer Security Incident Response Team）を設置し、インシデント対応及び再発防止策を実施する。

４．取組方針

ア　組織的対策：責任体制の明確化、監査・点検の実施、継続的改善。

イ　技術的対策：ネットワーク分離、アクセス制御、多要素認証、ログ監視、ウイルス対策等を適切に実施する。

ウ　人的対策：全職員及び委託事業者に対して情報セキュリティ教育を行い、意識の向上を図る。

エ　委託・外部連携対策：システム開発・運用等の委託先に対し、契約等によりセキュリティ遵守を義務付ける。

オ　インシデント対応・復旧：インシデント発生時の報告・初動・復旧手順を定め、迅速な対応を行う。

カ　評価・見直し：年１回以上の見直しを行い、必要に応じて方針及び関連規程を改定する。

５．公表・周知

・本方針は町の公式ウェブサイト等により公表する。

・職員及び委託事業者に対して本方針を周知し、遵守を徹底する。

・町民に対しても、サイバーセキュリティに関する理解促進を図る情報発信に努める。

６．附則

１　本方針は、令和７年４月１日から施行する。

２　本方針の別冊資料として、伊仙町情報セキュリティポリシーを掲載する。

地方自治法第２４４条の６第１項において、「普通地方公共団体の議会及び長その他の執行機関は、それぞれその管理する情報システムの利用に当たってのサイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない。」と規定されています。

それを踏まえ、本町では「伊仙町情報セキュリティポリシー情報セキュリティ基本方針」を、地方自治法第２４４条の６第１項に示されている「サイバーセキュリティを確保するための方針」に位置づけるとともに、同法に基づき関係機関との共同による方針を公表する観点から、伊仙町サイバーセキュリティを確保するための方針を策定し、さらなるセキュリティ確保を図ってまいります。

令和７年４月１日

伊仙町長

伊仙町教育委員会教育長

伊仙町議会議長

伊仙町選挙管理委員会委員長

伊仙町農業委員会会長

（本方針は、上記関係機関の連携・協議の下で策定したものであり、伊仙町長が最終責任を負う。）

第２編

第１章

情報セキュリティ基本方針

〈　目　　次　〉

第１章　情報セキュリティ基本方針

第１章　情報セキュリティ基本方針

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

（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）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。

（５）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。

（６）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。

（７）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。

（８）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。※NewTRY-X/Ⅱ等利用回線及び端末等。

（９）ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等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。

(10) 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。

(11) 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。

(12) 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

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、各行政委員会、議会事務局及び地方公営企業とし、各教育機関（事務室及び職員室を除く）は対象外とする。

なお、各教育機関における教育のために用いるシステム等は，この情報セキュリティポリシーの対象となるシステムと物理的に分離しなければならない。

（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、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。）

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、非常勤職員及び臨時職員・会計年度任用職員（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

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、都道府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

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。

（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の向上を図る。情報セキュリティポリシーの見直しが必要な場合は、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、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。