高浜町情報セキュリティ基本方針

平成 15 年 9 月 30 日　　策定
平成 29 年 4 月 1 日　一部改正
令和 3 年 4 月 1 日　一部改正

高浜町

はじめに

電子自治体をはじめとする行政の情報化の進展に伴い、情報通信ネットワークや情報システムを利用する業務が拡大し、高浜町の第４次総合計画のリーディングプロジェクト「地域でくるむ　暮らしよさ実感プロジェクト」、「多様な関わりでつなぐ　新たな連携・交流促進プロジェクト」、「魅力を高めてかがやく　賑わい創出・産業再生プロジェクト」、また基本計画１３分野の実現のためにも、情報化の一層の推進は不可欠である。

しかしながら、情報の取扱いの多様化に伴い、住民の個人情報等の自治体が保有している機密情報の流出・漏えい等の事故、情報システムを利用した不正アクセスやコンピュータウイルスの被害、組織内部の者による意図しない操作や不正操作等が、以前より容易に発生する危険性もある。これらが発生した場合、住民の利益や自治体活動への信頼に甚大な損失が発生する。

このことをすべての関係者は深く考え、高浜町が保有している個人情報や重要な行政情報等の情報資産を適切に管理するため、ここに情報セキュリティポリシー（注）を策定し、運用・維持するものである。

（注）：高浜町のすべての情報資産に対する情報セキュリティ対策について、総合的、体系的かつ、具体的に取りまとめたものの総称

（目的）

第１条　高浜町情報セキュリティ基本方針（以下「基本方針」という。）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。

（用語の定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 情報
　職務の遂行に伴ってコンピュータまたは記録媒体に記録されたデータ及び文書をいう。

(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) 情報資産
　情報及び情報システムをいう。

(4) 脅威
　自然の脅威（地震、火災、風水害等）、情報システムの脅威（情報システムの故障、誤動作等）及び人的な脅威（不正行為、誤操作等）をいう。

(5) 情報セキュリティ
　脅威から町が管理する情報資産を保護し、情報資産の「機密性」、「完全性」及び「可用性」を確保することをいう。
- 「機密性」：権限のない者への情報の漏えいを防止すること
- 「完全性」：情報の改ざん、破壊による被害を防止すること
- 「可用性」：権限のある者に対し、いつでも情報の利用を可能とすること

(6) 情報セキュリティポリシー
　基本方針及び情報セキュリティ対策基準をいう。

(7) 情報セキュリティ対策
　情報セキュリティを維持するための管理策をいう。

(8) 職員等
　地方公務員法で規定された特別職、一般職、会計年度任用職員の中で町に勤務する者の総称をいう。

(9) 外部要員
　職務委託先社員（システム開発業務を委託する外部業者等）等、契約に基づいて町の依頼により作業する者の総称をいう。

(10) 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。

(11) 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。）。

(12) 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。

(13) 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。

(14) 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。

（対象とする脅威）

第３条　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、重要情報の詐取及び内部不正等

(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、外部委託管理の不備、マネジメントの欠陥及び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、落雷及び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

(5) 電力供給の途絶、通信の途絶及び水道供給の途絶等のインフラの障害からの波及等

（適用範囲）

第４条　この基本方針が適用される行政機関は、町長、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、議会及び地方公営企業とする。

２　この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情報通信ネットワーク図等のシステム関連文書

（職員等の遵守義務）

第５条　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。

２　職員等は、次に掲げる義務を負うものとする。

(1) この基本方針を遵守し、情報セキュリティ対策を有効に機能させなければならない。

(2) 職務上知り得た秘密を漏らしてはならない。その職を退いた後も同様とする。

（関係機関の職員等の参加）

第６条　関係機関の職員等は、情報資産の利用範囲に応じて、第４条と同様の義務が生じ得るものとし、町が実施する情報セキュリティ対策に積極的に関与するものとする。

（外部要員の管理）

第７条　町は、外部要員を使用する場合、契約等に基づき、第５条と同様の内容を外部要員に対しても義務づけ、管理するものとする。

（情報セキュリティ対策）

第８条　町は、第３条で定める脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

⑴ 組織体制

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。

⑵ 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。

⑶ 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、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。

⑷ 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パソコン等の管理について、物理的な対策を講じる。

⑸ 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。

⑹ 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及び不正アクセス対策等の技術的対策を講じる。

⑺ 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。

⑻ 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。

⑼ 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、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ対策基準）
第９条　町における情報セキュリティ対策の統一基準となる情報セキュリティ対策基準（以下「対策基準」という。）を定め、想定される脅威に対応するための対策要件を規定する。

（情報セキュリティ実施手順）
第１０条　この基本方針及び対策基準に従い、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（以下「実施手順」という。）を作成するものとする。
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恐れのあることから非公開とする。

（情報資産の分類）
第１１条　町が管理する情報資産は、その重要度に応じて分類し、その分類に応じた情報セキュリティ対策を講ずるものとする。必要な情報分類の定義及び分類に応じた情報セキュリティ対策の要件を、別に定める情報セキュリティ対策基準に規定するものとする。

（情報セキュリティ管理体制）
第１２条　この基本方針及び対策基準に規定された情報セキュリティ対策の推進・管理のための組織・体制を置き、管理体制を確立するものとする。

（情報セキュリティ監査及び自己点検の実施 ）
第１３条　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。

（情報セキュリティポリシーの見直し）
第１４条　次の場合において、情報セキュリティポリシーを見直すものとする。
⑴ 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になった場合
⑵ 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

（法令等の遵守）

第１５条　すべての適用対象者は、職務遂行において、関連法令等に従わなければならない。