海田町情報セキュリティポリシー
基本方針

平成 15 年 3 月 3 日　　策定

令和 7 年 10 月 1 日　　改定

総務部　デジタル推進課

目次

はじめに

1　情報セキュリティポリシーの必要性

地方公共団体は，法令等に基づき，住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに，他に代替することができない行政サービスを提供している。

また，多くの業務が情報システムやネットワークに依存していることから，住民生活や地域の社会経済活動を保護するため，情報セキュリティ対策を講じて，その保有する情報を守り，業務を継続することが必要となる。

今後，各種手続のオンライン利用の本格化や，情報システムの高度化等，電子自治体の推進により，情報システムに障害が発生した場合，広範囲の業務が継続できなくなり，住民生活や地域の経済社会活動に重大な支障が生じる可能性は高まっている。

また，地方公共団体は，LGWAN（総合行政ネットワーク）等のネットワークで相互に接続されており，他の団体で発生した障害がネットワークを介して連鎖的に拡大する可能性は否定できない。

これらの事情から，全ての地方公共団体で，情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが重要となる。また，情報セキュリティの確保に絶対安全ということはなく，情報セキュリティに関する障害・事故及びシステム上の欠陥（以下，「情報セキュリティインシデント」という。）の未然防止のみならず，情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じることが急務である。

こうした背景をもとに本町では，情報セキュリティに関する基本的な考え方を明らかにするとともに，情報資産を保護するために必要な対策を講じるための基準として情報セキュリティポリシーを定め，組織的な対応を図る。

2　情報セキュリティポリシーの構成

情報セキュリティポリシーは，本町が保有する情報資産に関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を総称する。

また，情報セキュリティポリシーは，本町が保有する情報資産に関する業務に関わる職員，非常勤職員，嘱託職員及び臨時職員に浸透，普及，定着させ，安定的な規範として，共有する。一方では，技術の進歩等に伴う情報セキュリティを取り巻く急速な変化へ柔軟に対応する必要があることから，情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と，情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定する。

具体的には，情報セキュリティポリシーを，①情報セキュリティ基本方針及び②情報セキュリティ対策基準の２階層に分け，情報システムごとの具体的な実施手順として，情報セキュリティ実施手順を別途策定する。

基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
対策基準	基本方針を実行に移すため，全ての情報システムに共通する情報セキュリティ対策の基準
実施手順	情報システムごとに定める，対策基準に基づいた具体的なセキュリティ対策のためのマニュアル

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

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　マイナンバー利用事務系（個人番号利用事務系）（以下「K 系」という。）

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。

⑼　LGWAN 接続系（以下「L 系」という。）

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（K 系を除く。）。

⑽　インターネット接続系（以下「I 系」という。）

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。

⑾　通信経路の分割

L 系とＩ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。

⑿　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，次の脅威を想定し，情報セキュリティ対策を実施する。

⑴　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

⑵　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

⑶ 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

⑷ 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

⑸ 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

⑴ 行政機関の範囲

本基本方針が適用される行政機関は，海田町事務組織規則(平成 12 年海田町規則第 23 号。以下「事務組織規則」という。)に規定する本庁及び出先機関，附属機関，並びに行政委員会（教育委員会，選挙管理委員会，人事委員会（公平委員会），監査委員），議会事務局及び地方公営企業とする。

⑵ 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。ただし，教育委員会が所管する教育ネットワーク及び教育情報システムに係る情報資産を除く。

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

5 職員等の遵守義務

町の保有する情報資産に関する業務に携わるすべての職員（非常勤職員，嘱託職員及び臨時職員等を含む（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

第 3 項に規定する脅威から情報資産を保護するために，次の情報セキュリティ対策を講じる。

⑴ 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。

⑵ 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 K 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 L 系においては，LGWAN と接続する業務用システムと，I 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 I 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，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，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。

⑻　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，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。

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，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や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，すみやかに情報セキュリティポリシーを見直し，職員等へ情報共有する。

9　情報セキュリティ対策基準の策定

第6項，第7項及び第8項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定める。

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情報セキュリティ実施手順として定める。

なお，情報セキュリティ実施手順は，海田町情報公開条例（平成17年海田町条例第5号）第7条第1項第3号アに該当する情報として，非公開とする。