# 松島町情報セキュリティ基本方針

令和８年４月１日施行

松島町長　　櫻井　公一
松島町議会議長　髙橋　利典

## 第１章 総則

### 第１　（目的）

この基本方針は、地方自治法その他関係法令の規定に基づき、松島町（以下「本町」という。）の議会及び長その他の執行機関（以下「各機関」という。）が管理する情報システムの利用にあたって、サイバーセキュリティを確保するための基本的な方針を定めることにより、町民の個人情報をはじめとする重要な情報資産を保護し、行政サービスの安定的な提供を実現することを目的とする。

### 第２　（適用範囲）

１　適用対象者

本基本方針は、次に掲げる者（以下、職員等という）に適用する。

(1) 本町の議員及び職員（会計年度任用職員等を含む。）
(2) 本町の情報システム及び情報資産を利用する全ての者
(3) 本町から業務を受託し、又は本町と共同で業務を行う事業者及びその従業員
(4) その他各機関が指定する者

２　適用対象機関

本基本方針は、本町の全ての執行機関（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、公営企業管理者）及び議会事務局に適用する。

３　適用対象となる情報資産

本基本方針が対象とする情報資産は、次に掲げるものとする。

(1) 情報システム（ハードウェア、ソフトウェア、ネットワーク機器等）
(2) 電磁的記録（電子データ、電子メール等）
(3) 紙媒体の情報（文書、図面等）
(4) その他の情報資産

### 第３　（定義）

本基本方針の語句の定義は、次のとおりとする。

(1) 情報資産

本町が保有する情報及び情報システムのすべてをいう。

(2) 情報システム

コンピュータ、ネットワーク機器、ソフトウェア等により構成され、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

情報へのアクセスを認められた者だけが、その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、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。

(6) 可用性

情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる状態を確保することをいう。

(7) 情報セキュリティインシデント

情報資産の機密性、完全性又は可用性を脅かす事象をいう。

(8) サイバー攻撃

情報システムに対する不正アクセス、コンピュータウイルスの感染、サービス妨害攻撃等の悪意ある行為をいう。

(9) クラウドサービス

インターネット等のネットワークを経由して、情報システムの機能を利用するサービスをいう。

第4　(基本的な考え方)

1　情報セキュリティの重要性

本町は、住民情報、税情報、福祉情報等の重要な個人情報を保有し、これらの情報を活用して行政サービスを提供している。これらの情報資産が漏えい、改ざん、滅失等の被害を受けた場合、住民の権利利益を侵害し、行政運営に重大な支障を及ぼすおそれがある。

このため、本町は、情報セキュリティの確保を最重要課題の一つと位置づけ、組織的、人的、物理的、技術的な対策を総合的に実施する。

2　総務省ガイドラインへの準拠

本基本方針は、総務省「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」に準拠して策定する。

3　継続的な改善

情報セキュリティを取り巻く環境は常に変化しており、新たな脅威が日々発生している。本町は、情報セキュリティ対策を継続的に評価・見直し、改善を図る。

## 第2章 情報セキュリティ対策の基本方針

第5　(組織・体制)

1　情報セキュリティ対策本部の設置

本町は、情報セキュリティ対策を統括的に推進するため、副町長を本部長とする「松島町情報セキュリティ対策本部」を設置する。

2　最高情報セキュリティ責任者（CISO）の設置

本町は、情報セキュリティ対策を統括管理する最高情報セキュリティ責任者（CISO）を置く。CISO は企画調整課長をもって充てる。

3　情報セキュリティ責任者の設置

各課等に情報セキュリティ責任者を置き、当該課等における情報セキュリティ対策を統括する。

4　情報セキュリティ管理者の設置

情報システムごとに情報セキュリティ管理者を置き、当該情報システムの情報セキュリティ対策を管理する。ただし、小規模なシステムについては、情報セキュリティ責任者が兼務することができる。

5　各機関の体制

教育委員会、議会、選挙管理委員会その他の執行機関は、それぞれの機関において情報セキュリティ責任者を置き、本基本方針に基づく情報セキュリティ対策を実施する。

第 6　（情報資産の分類と管理）

1　情報資産の分類

本町は、保有する情報資産を機密性、完全性及び可用性の観点から重要度に応じて分類し、分類に応じた適切な管理を行う。情報資産の機密性分類は、次のとおりとする。

(1) 機密性 3：マイナンバー利用事務系情報、住民基本台帳情報等、特に厳格な管理が必要な情報

(2) 機密性 2：機密性 3 以外の個人情報、内部管理情報等

(3) 機密性 1：公開情報等

2　情報資産の管理責任

すべての情報資産には管理責任者を定め、適切な管理を行う。

3　情報資産のライフサイクル管理

情報資産の取得、利用、保管、廃棄に至るまでの各段階において、適切なセキュリティ対策を実施する。

第 7　（物理的セキュリティ）

1　施設の安全管理

サーバ室等の重要な施設については、入退室管理、施錠管理等により、物理的な安全を確保する。

2　機器の安全管理

情報システムの機器については、盗難、破壊、不正操作等を防止するための物理的な対策を実施する。

3　執務環境の安全管理

執務室における情報資産の管理について、離席時の画面ロック、書類の施錠保管等の対策を実施し、関係者以外の立ち入りを原則禁止する。

第８　（人的セキュリティ）

1　職員等の責務

職員等は、情報セキュリティの重要性を認識し、本基本方針及び関連規程を遵守しなければならない。

2　教育・研修

本町は、職員等に対し、情報セキュリティに関する教育・研修を定期的に実施する。教育・研修は、e-ラーニング等の効率的な方法により実施することができる。

3　誓約書の提出

職員等は、情報セキュリティに関する誓約書を提出しなければならない。

4　懲戒処分等

本基本方針及び関連規程に違反した職員等に対しては、松島町職員の懲戒処分の基準に関する規程（平成 19 年 12 月 11 日訓令第 30 号）に照らし、懲戒処分その他の措置を講ずる。

第９　（技術的セキュリティ）

1　アクセス制御

情報システムへのアクセスは、業務上必要な範囲に限定し、適切なアクセス制御を実施する。

2　認証

情報システムへのアクセスにあたっては、利用者の認証を行う。重要な情報システムについては、多要素認証等の強固な認証方式を段階的に導入する。

3　ネットワークセキュリティ

ネットワークについては、適切な分離、ファイアウォールの設置等により、不正アクセスやサイバー攻撃から保護する。

4　マルウェア対策

すべての端末及びサーバにマルウェア対策ソフトウェアを導入し、常に最新の状態に保つ。

5　暗号化

重要な情報を電子メールで送信する場合や、可搬記録媒体に保存する場合は、暗号化を行う。

6　ログの取得・保存

情報システムの利用状況を記録するログを取得し、適切に保存・管理する。ログの分析は、自動分析ツール等の効率的な方法により実施することができる。

第 10　（運用）

1　情報システムの開発・導入

情報システムの開発・導入にあたっては、企画段階から情報セキュリティ対策を組み込む。

2　情報システムの運用・保守

情報システムの運用・保守にあたっては、適切なセキュリティ対策を実施する。

3　バックアップ

重要な情報資産については、定期的にバックアップを取得し、災害等に備える。バックアップは、クラウドサービスの自動バックアップ機能等の効率的な方法により実施することができる。

4　脆弱性対策

情報システムの脆弱性については、速やかに修正プログラムを適用する等の対策を実施する。

5　変更管理

情報システムの変更にあたっては、セキュリティへの影響を評価し、適切な手続きを経て実施する。

第 11　（外部サービスの利用）

1　クラウドサービス

クラウドサービスを利用する場合は、サービス提供事業者のセキュリティ対策を評価し、適切なサービスを選定する。また、契約において情報セキュリティに関する事項を明確にする。

2　可搬記録媒体

可搬記録媒体(USB メモリ、外付けハードディスク等)の利用については、適切なセキュリティ対策を実施することとする。

3　外部委託

情報システムの運用や業務を外部に委託する場合は、委託先のセキュリティ対策を評価し、契約において情報セキュリティに関する事項を明確にする。また、委託先の履行状況を定期的に確認する。

第 12　（情報セキュリティインシデントへの対応）

1　インシデント対応体制（CSIRT）

本町は、情報セキュリティインシデントが発生した場合に迅速かつ適切に対応するための体制（CSIRT：Computer Security Incident Response Team）を整備する。CSIRT は、CISO、情報セキュリティ責任者及び CISO が指定する職員により構成し、兼務体制とすることができる。

2　インシデントの報告

職員等は、情報セキュリティインシデントを認知した場合、直ちに情報セキュリティ責任者に報告しなければならない。

3　インシデントへの対応

情報セキュリティインシデントが発生した場合、被害の拡大防止、原因究明、復旧、再発防止等の措置を迅速に実施する。

4　関係機関との連携

重大な情報セキュリティインシデントが発生した場合、警察、総務省、宮城県等の関係機関と連携して対応する。

第 13　（事業継続管理）

1　事業継続計画の策定

本町は、災害やサイバー攻撃等により情報システムが停止した場合でも、重要な業務を継続できるよう、事業継続計画（BCP）を策定する。

2　復旧計画

情報システムが停止した場合の復旧手順を定め、定期的に訓練を実施する。訓練は、机上訓練等の効率的な方法により実施することができる。

第 14　（評価・監査）

1　自己点検

各課等は、情報セキュリティ対策の実施状況について、定期的に自己点検を実施する。

2　内部監査

本町は、情報セキュリティ対策の実施状況について、定期的に内部監査を実施する。ただし、自己点検を適切に実施している場合は、自己点検の結果を確認することにより、内部監査に代えることができる。

3　外部監査

本町は、3 年に 1 回以上、外部の専門機関による監査を実施する。

第 15　（見直し・改善）

1　継続的な見直し

本町は、情報セキュリティを取り巻く環境の変化、新たな脅威の出現、法令の改正等に応じて、本基本方針及び関連規程を継続的に見直す。

2　PDCA サイクル

本町は、Plan（計画）、Do（実施）、Check（評価）、Act（改善）のサイクルにより、情報セキュリティ対策を継続的に改善する。

## 第 3 章　対策基準・実施手順

第 16　（対策基準・実施手順の策定）

1　対策基準の策定

本基本方針に基づき、情報セキュリティ対策を実施するための具体的な基準として「松島町情報セキュリティ対策基準」を策定する。

2　実施手順の策定

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として「松島

町情報セキュリティ実施手順」を策定する。

3　非公開

対策基準及び実施手順は、公にすることにより本町の情報セキュリティ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。

## 第 4 章 法令遵守

### 第 17　（法令等の遵守）

本町は、情報セキュリティに関する法令、国の指針、県の方針等を遵守する。主な関連法令等は次のとおりである。

(1) 地方自治法（昭和 22 年法律第 67 号）
(2) 個人情報の保護に関する法律（平成 15 年法律第 57 号）
(3) 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（平成 25 年法律第 27 号）
(4) 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
(5) サイバーセキュリティ基本法（平成 26 年法律第 104 号）
(6) 電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）
(7) 総務省『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』（令和 7 年 3 月 28 日一部改定）
(8) その他関連法令等

## 第 5 章 その他

### 第 18　（適用除外）

特別の事情により本基本方針の適用が困難な場合は、CISO と協議の上、当該機関の情報セキュリティ責任者(又は当該機関の長)の承認を得て、適用を除外することができる。ただし、この場合においても、代替的なセキュリティ対策を実施しなければならない。

### 第 19　（委任）

本基本方針の実施に関し必要な事項は、各機関が別に定める。ただし共通事項は、情報セキュリティ対策本部で調整する。

## 附則

（施行期日）

この基本方針は、令和 8 年 4 月 1 日から施行する。

（経過措置）

この基本方針の施行前に策定された「松島町情報セキュリティポリシー（令和 5 年 6 月 30 日改定)」は、この基本方針の施行をもって廃止する。ただし、この基本方針に基づく対策基準及び実施手順が整備されるまでの間は、従前のポリシーを準用する。

（各機関における決定）

　各機関は、この基本方針を採用する旨の決定を行うものとする。

（採用決定の記録）

　各機関は、前項の決定について、決定日、決定方法(会議の議決、委員長決定その他これに準ずる方法をいう。)その他必要な事項を記録し、保管するものとする。