

# 浜田市情報セキュリティポリシー

《情報セキュリティ基本方針》

《情報セキュリティ対策基準》

令和8年3月

浜田市情報セキュリティ委員会

**第 1 部 情報セキュリティ基本方針**

序文 .....	1
1 目的 .....	2
2 定義 .....	2
3 対象とする脅威 .....	3
4 適用範囲 .....	3
5 職員等の遵守義務 .....	3
6 情報セキュリティ対策 .....	3
7 情報セキュリティ監査及び自己点検の実施 .....	5
8 情報セキュリティポリシーの見直し .....	5
9 情報セキュリティ対策基準の策定 .....	5
10 実施手順の策定 .....	5
11 情報セキュリティポリシー等の公開 .....	5

# 第1部 情報セキュリティ基本方針

## 序文

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

本市は、市民の個人情報や行政運営上重要な情報を多数取り扱っている。また、電子自治体の構築が進み、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。したがって、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。また、本市には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。

これらの状況を鑑み、本市における情報資産に対する安全対策を推進し、市民からの信頼を確保し、さらに地域に貢献するため、以下に積極的に取り組むことを宣言する。

- (1) 情報セキュリティ対策に取り組むための全庁的な体制を確立する。
- (2) 情報セキュリティ対策の基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。
- (3) 本市の保有する情報資産を適切に管理する。
- (4) 職員等に情報セキュリティ対策の重要性を認識させ、当該対策を適切に実施するために、職員等に対して必要な教育を実施する。
- (5) 情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を策定する。
- (6) 情報セキュリティ対策の実施状況の自己点検等を通して、定期的に当該対策の見直しを実施する。
- (7) 全ての職員等に情報セキュリティの重要性について共通の認識を持たせ、業務の遂行に当たって情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守させる。
- (8) 地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献する。

令和8年3月31日

浜田市長

## 1 目的

この基本方針は、浜田市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、浜田市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及び通信装置（ハードウェア及びソフトウェア）のことをいう。

### (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のことをいう。

### (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の総称のことをいう。

### (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）

個人情報等利用事務（社会保障、地方税又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。

### (9) 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。）。

### (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。

#### (1 2) 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。

#### (1 3) 個人情報等

市が保有する個人情報及び特定個人情報（個人番号を含んだ個人情報）のことをいう。

### 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、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な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) 組織の範囲

- ① 本庁、支所、消防本部及び出先機関（学校を除く。）
- ② 上記に勤務する職員（会計年度任用職員・派遣等を含む。（以下「職員等」という。））

#### (2) 情報資産の範囲

- ① ネットワーク、情報システム及びこれらに関する施設、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、業務の遂行にあたっては、情報セキュリティポリシー及び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、以下の対策を講じる。

#### (1) 組織体制

庁内に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

浜田市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行う。

(3) 情報システム全体の強靱性の向上

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。

(4) 物理的セキュリティ

情報資産を収容する施設・設備及び職員等が使用するパソコンやモバイル端末等（以下「パソコン等」という。）の情報機器の管理について、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

情報システムの管理、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。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(8) 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。

## 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、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 実施手順の策定

情報セキュリティ対策基準に基づいて情報セキュリティ対策を実施するための具体的手順を定めた実施手順を策定する。

## 11 情報セキュリティポリシー等の公開

- ①情報セキュリティ基本方針は、浜田市ホームページにおいて公開し、浜田市の情報セキュリティマネジメントの取り組み方を外部に表明する。
- ②情報セキュリティ対策基準及び実施手順は、情報セキュリティの脆弱性を顕在化させるおそれがあることから非公開とする。