# 高島市情報セキュリティ基本方針

滋賀県高島市

# 目　次



| 版数 | 年月日 |
|---|---|
| 初版 | 2008/04/01 |
| 改訂 | 2016/12/01 |
| 改訂 | 2020/04/01 |
| 改訂 | 2026/04/01 |
| | |

## 1. 目 的

高島市情報セキュリティ基本方針（以下「基本方針」という。）は、本市が保有する情報資産の機密性、完全性および可用性を維持するため、本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しています。

## 2. 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します。

| 情報セキュリティ対策において脅威となる事象・要因 | |
|---|---|
| 情報セキュリティインシデント<br>（市の情報資産に対する攻撃、システム障害、個人情報の漏えい、紛失および盗難など、市の情報セキュリティを脅かす事象） | 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 |
| | 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、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 |
| | 地震、落雷、火災等の災害によるサービスおよび業務の停止等 |
| | 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 |
| | 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 |

## 3. 対象範囲

本基本方針が適用される組織の対象範囲は、次のとおりです。

| 対　　象　　範　　囲 | | |
|---|---|---|
| 組 織 | ①市の全機関 | 市長部局（各支所、出先機関を含む）、各行政委員会、消防本部（署等の機関を含む）、地方公営企業（病院医療職を除く）、各教育機関（出先機関、各小中学校を含む）および議会事務局 |
| | ②その他 | 本市と業務委託契約を結んでいる企業や各種団体 等 |

| | | |
|---|---|---|
| 人 | | 上記組織における本市の情報資産の利用者 |
| 情報資産 | ①機器類 | ネットワーク、情報システム、これらに関する施設・設備および電磁的記録媒体 |
| | ②文書類 | ネットワークおよび情報システムで取り扱う情報（印刷した文書を含む）、設計書、仕様書および構成図等のシステム関連文書 |

## 4. 文書体系

本市の情報セキュリティ対策を実施するため、明文化する規程、基準等の文書体系を定めます。

| セキュリティ規程等 | |
|---|---|
| 高島市情報セキュリティ基本方針 | 本基本方針のことで、本市の情報セキュリティ対策に関する基本的な考え方をまとめたもの |
| 高島市情報セキュリティポリシー | 本基本方針および本市の情報セキュリティ対策基準（以下「セキュリティポリシー」）をいう。 |
| 高島市教育情報セキュリティポリシー | 本基本方針および本市の教育情報セキュリティ対策基準（以下「セキュリティポリシー」）をいう。 |
| 高島市情報システム管理運営規程 | セキュリティポリシーに基づき、本市の情報システムの管理方法や運用について定めたもの |
| 実施手順書 | セキュリティポリシーに基づき、本市の情報セキュリティ対策について具体的に定めた実施マニュアル |
| 運用基準 | 各情報システム管理者が所管システムの運用について定めた取り決め |

| 委員会 | |
|---|---|
| 情報化推進委員会 | 本市の情報化の総合調整、セキュリティ審議およびセキュリティ監査を行うために設置される機関（副市長を委員長とする部長級等職員で構成） |
| 情報システム運営委員会 | 本市の情報システムの整備および利用に係る計画等の策定や情報システムの開発などの検討をおこなうための機関（情報セキュリティ責任者等で構成） |

## 5. 職員等の遵守義務

市の職員、会計年度任用職員および臨時の職員（以下「職員等」）は、各々が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セキュリティポリシーや各種規程類を遵守しなければなりません。

## 6. 情報セキュリティ対策

本市の情報資産を上記の脅威から保護するため、以下の情報セキュリティ対策を実施します。

| 情報セキュリティ対策 | |
|---|---|
| 組織体制 | 本市の情報セキュリティ対策を推進するため、副市長を最高情報セキュリティ責任者（ＣＩＳＯ）とする全庁横断的な組織管理・責任体制を整備します。 |
| 情報資産の分類と管理 | 本市の保有する情報資産を機密性、完全性およ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します。 |
| 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ます。 |
| | 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ぎます。 |
| | 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、無害化通信を実施します。 |
| | 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、都道府県およ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します。 |
| 物理的セキュリティ | サーバ、情報システム室、通信回線およ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ます。 |

| | |
|---|---|
| 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、十分な教育および啓発を行う等の人的な対策を講じます。 |
| 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ます。 |
| 運用 | 情報システムの監視､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ます。 |
| 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ます。 |
| | 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ます。 |
| | 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ます。 |
| 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、定期的または必要に応じて情報セキュリティ監査およ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います。 |

## 7. 情報セキュリティ監査および自己点検の実施

セキュリティポリシー､各種情報関係規程､実施手順書等の遵守状況を確認するため、定期的または必要に応じて自己点検および情報セキュリティ監査を実施します。

## 8. 事故等緊急時の対応

情報資産への侵害､事故･災害等によるシステム障害が発生した場合に迅速かつ適切に対応するため､緊急時対応計画を策定し､原因分析･再発防止対策を実施します。

## 9. セキュリティポリシーの見直し

情報セキュリティ監査および自己点検の結果、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およ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、保有する情報および利用する情報システムに係る脅威の発生の可能性および発生時の損失等を分析し、リスクを検討したうえで、セキュリティポリシーおよび教育情報セキュリティポリシーの見直しを行います。

## 10. 情報セキュリティ対策基準の策定

情報セキュリティ対策を実施するため、具体的な遵守事項および統一的な判断基準等を定めた情報セキュリティ対策基準（セキュリティポリシーおよび教育情報セキュリティポリシーのこと）を策定します。

## 11. 情報セキュリティ実施手順書の策定など

セキュリティポリシーに基づき、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書を策定します。

また、セキュリティポリシー、教育情報セキュリティポリシー、実施手順書、運用基準、各マニュアル類、緊急時対応計画は、本市の情報セキュリティの具体的な対策を記述したものであることから、外部への公開は行わないものとします。