三田市情報セキュリティポリシー

第１章　情報セキュリティ基本方針（サイバーセキュリティを確保するための方針）

１　目的

本基本方針は、本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、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する。

本市が保有する情報システムが取り扱う情報には、市民等の個人情報や行政運営上重要な情報等、外部へ漏えい又は流出した場合には、重大な事態を招くおそれのある情報が多く含まれており、情報資産を様々な脅威から防御することは、市民の生命、財産、プライバシー等を守るためにも、また、継続的かつ安定的な行政サービスを実施するためにも必要不可欠である。

このため、本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、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 とともに、地方自治法（昭和 22 年法律第 67 号）第 244 条の６第１項を踏まえて、本市のサイバーセキュリティを確保するための方針として定めるものである。

２　定義

(1) ネットワーク

ハードウェア（電子計算機、端末機、通信装置、通信回線、周辺機器及び電磁的記録媒体等から構成されるもの）を相互に接続するための通信網及びその仕組みをいう。

(2) 情報システム

ハードウェア、ソフトウェア（コンピュータを動作させる手順及び命令をコンピュータが理解できる形式で記述したもの）及びネットワークにより業務処理を行う仕組みをいう。

(3) 情報資産

情報資産は、次のとおりとする。

① ア　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② イ　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 ウ　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

(4) 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。

(5) 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。

(6) 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。

(7) 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。

(8) 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。

(9) 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等）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。

(10) ＬＧＷＡＮ接続系

LGWAN に接続することができる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。）。

(11) 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。

(12) 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。

(13) 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、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、ウィルス攻撃、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、重要情報の搾取、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、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

(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

情報セキュリティポリシー基本方針は、部等 及び課等が保有する情報資産並びに当該情報資産に接する全ての職員等について適用する。

(1) 行政機関の範囲

本基本方針が適用される行政機関は、市長、議会（事務局に限る）、行政委員会（事務局含む）及び水道事業管理者とする。

(2) 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、各行政機関が独自に定める基本方針において対象とされる情報資産は本基本方針の対象外とする。

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

本市の情報資産に関する業務に携わる全ての職員・委員等（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

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずる。

(1) 情報セキュリティ管理体制

本市の情報資産について、情報セキュリティ対策を推進、管理するための全庁的な組織体制を確立する。

(2) 情報の分類と管理

情報資産である情報（以下「情報」という。）をその機密性、完全性及び可用性から重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 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。

(4) 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、物理的な対策を講ずる。

(5) 人的セキュリティ

情報セキュリティに関する権限及び責任を定め、全ての職員等に情報セキュリティポリシーの内容を周知徹底するため、教育及び啓発を行う等の人的な対策を講ずる。

(6) 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ずる。

(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、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ずるものとする。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。

(8) 業務委託と外部サービス（クラウドサービス）の利用

① 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。

② 外部サービス（クラウドサービス） を利用する場合には、利用にかかる規定を整備し対策を講じる。

③ 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。

(9) 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、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。

８　情報セキュリティポリシーの評価及び見直し

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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

本市の情報資産について、上記６、７及び８の情報セキュリティ対策を講ずるに当たっては、職員等及び委託事業者が遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定する。

なお、情報セキュリティ対策基準は、公にすることにより本市の行政運営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。

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を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要がある。そのため、各課等の長はその所管する情報資産に対する情報セキュ

リティ実施手順を策定するものとする。

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市の行政運営に重大な支障を及ぼすおそれのある情報資産でがあることから非公開とする。