東松山市情報セキュリティポリシー

（令和３年１０月版）

平成１５年３月２７日　策定
平成１９年４月　１日　一部改正
平成２８年３月　１日　全部改定
令和３年１０月　５日　一部改正

東松山市

第１章　情報セキュリティ基本方針

１．目的

本基本方針は、東松山市が所有する情報資産の機密性[1]、完全性[2]及び可用性[3]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。

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、その構成機器（ハードウェア及びソフトウェア）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をいう。

(3)　情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

(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)　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）または戸籍事務等に係る情報システム及びデータをいう。

(6)　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。）。

(7)　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係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。

国際標準化機構（ISO）が定めるもの（ISO7498-2：1989）

機密性[1]　情報にアクセスすることが認可された者だけがアクセスできることを確実にする。

完全性[2]　情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性[3]　許可された利用者が必要なときに情報にアクセスできることを確実にすること。

(8)　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。

(9)　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ない等、安全が確保された通信をいう。

３．職員及び外部委託事業者の遵守義務

情報セキュリティポリシーは、東松山市が所掌するネットワーク、情報システム及び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である。

従って、東松山市が所掌する情報資産に関する業務に携わる全ての職員及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては情報セキュリティポリシーを遵守する義務を負うものとする。

４．情報セキュリティ管理体制

東松山市の情報資産について、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

５．情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

６．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洩・破壊・改ざん・消去、重要情報の搾取、機器及び媒体の盗難等

(2)　職員及び外部委託者によるデータやプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難及び承認されていない端末接続によるデータ漏洩等

(3)　情報通信技術を使用しないパスワード等の重要情報の盗み見、なりすまし等

(4)　地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

(5)　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

(6)　電力供給、通信及び水道供給の途絶等、インフラの障害による機能不全等

７．適用範囲

(1)　行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企業とする。

(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。

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

８．情報セキュリティ対策

情報資産を認識すべき脅威から保護するために、以下の情報セキュリティ対策を講ずるものとする。

(1)　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、サーバ・パソコン・通信回線等の情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

(2)　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が行われるように必要な対策を講ずる。

(3)　技術及び運用におけるセキュリティ対策

コンピュータ等の管理、情報資産を外部からの不正アクセス、不正プログラム等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の外部委託のセキュリティ管理、ネットワークの監視、情報セキュリティポリシーの遵守状況を確認する等の運用面の対策を講ずる。

併せて、緊急事態が発生した際に迅速な対応を可能とするための緊急時対応計画を策定する。

９．情報セキュリティ対策基準の策定

東松山市で情報セキュリティ対策を講ずるに当たっては、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ものとする。

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基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産に応じた対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対する情報セキュリティ対策基準の基本的な要件に基づき、東松山市が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

11. 情報セキュリティ対策基準等の非公開

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は、公にすることにより東松山市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。ただし、公開しなければ業務を遂行できない場合には、機密保持契約を締結した上で、公開を認める場合もある。

12. 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が遵守されていることを検証するため、定期的または必要に応じて情報セキュリティ監査及び自己点検を実施する。

13. 評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティ対策及び情報セキュリティポリシーの見直しを実施する。