萩市
情報セキュリティ基本方針

制定日：令和５年２月１日
施行日：令和５年３月１日

萩市

目　次

第１章 情報セキュリティ基本方針

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。

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) 基幹系システム

自治体の業務に係る必要不可欠な情報システムをいう。具体的には、住民情報関連システム、税務関連システム、人事給与システム、会計システム等のことをいう。

(4) サブシステム

基幹系システムのうち、税務関連システムにおける市県民税、固定資産税等や介護福祉関連システムにおける心身障碍者手帳、介護保険等の各業務システムをいう。

(5) 情報資産

自治体の業務に係る紙の資料や電磁的記録媒体、サーバ等に保管されている情報全てのことを言う。

(6) 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。

(7) 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。

(8) 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。

(9) 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。

(10) 可用性

情報にアクセスすることを認められた者だけが、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。

(11) 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）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。

(12) 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）。

(13) 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。

(14) 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。

(15) 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。

(16) クラウドサービス

民間事業者等がインターネット上で不特定多数の利用者に対して提供する電子メール、ファイルストレージ、グループウェア、プラットフォーム等のサービスを指す。有料、無料に関らず、約款や利用規約等への同意、簡易なアカウントの登録等により利用可能なサービスは「クラウドサービス」となる。

(17) 職員

萩市の情報資産を取り扱う、任用形態、職種及び勤務地を問わない萩市の全職員をいう。

(18) 外部委託事業者

業務委託先社員（システム開発業務を委託する外部業者等）等、契約に基づいて市の機関で作業する者の総称をいう。

(19) 特権

サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常の利用者権限よりもシステムに対するより高いレベルでの操作が可能な権限をいう。

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)　行政機関の範囲

本基本方針が適用される行政機関は、市長部局、行政委員会、議会事務局、消防本部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、本市の保有する全ての情報資産とする。

５．職員の遵守義務

職員は、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の体系

本市の情報セキュリティの管理・運用で使用する文書・記録の体系は以下のとおりとする。

(1)　情報セキュリティ基本方針

情報セキュリティ基本方針は、文書体系の最上位に位置し、本書は情報セキュリティ管理・運用を実現するための基本方針を定める。

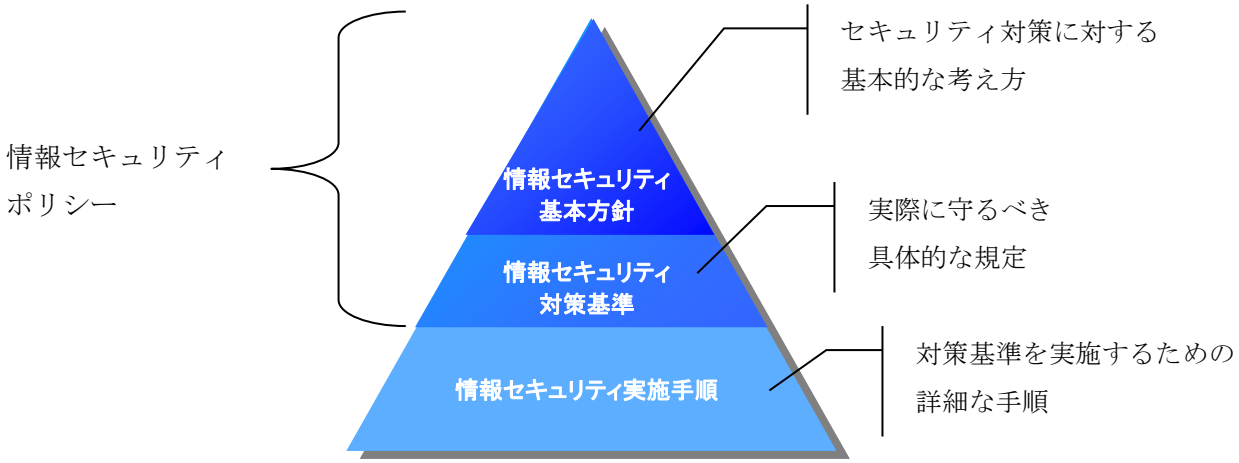
(2)　情報セキュリティ対策基準

情報セキュリティ対策基準は、情報セキュリティ基本方針に基づき、情報セキュリティ対策を実施するにあたって、準拠すべき管理策を定める。

(3)　情報セキュリティ実施手順

情報セキュリティ実施手順は、情報セキュリティ対策基準で定める管理策に基づき、情報セキュリティ管理・運用に関する具体的な内容・方式・手続・様式等を定める。

なお、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当市の活動に重大な支障を及ぼすおそれのある情報資産であることから、非公開とする。



７．情報セキュリティ対策

上記３条の脅威から情報資産を保護するために、以下のセキュリティ対策を講じる。

(1) 組織体制

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

本市の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。

（ア）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。

（イ）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。

（ウ）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、通信回線及び職員のパソコン等の管理について、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

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) 外部サービスの利用

外部委託する場合には、外部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、外部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。

約款による外部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。

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) 情報セキュリティポリシーの評価・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。

８．関連法令の遵守

職員は、情報セキュリティポリシーのみならず、関連する法律・条例等についてもこれを遵守しなければならない。

９．情報セキュリティに関する違反への対応

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、その他の関連法令に違反した場合は、地方公務員法に基づき、当該違反により生じた結果の重大性及び当該違反の悪質性等の状況に応じて、懲戒処分等の対象とする場合がある。

１０．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。