伊賀市
情報セキュリティポリシー
（基本方針）

平成１８年　４月　１日
平成２０年　４月　１日改定
平成３１年　４月　１日改定
令和　３年　４月　１日改定
令和　７年　４月　１日改定

序文

伊賀市（以下、「本市」という。）が取り扱う情報には、住民の個人情報のみならず、行政運営上重要な情報等、外部への漏えい等が生じた場合は、極めて重大な結果を招く情報が多数含まれている。そのため、情報の重要性を認識し、住民の利便性を向上させつつ、厳格な管理運用により情報を保護するとともに、安全性を追求する必要がある。

本市では、情報セキュリティを保持するため、「伊賀市情報セキュリティポリシー」を策定し、本市の職員等がこれに関与し、その対策が有効に機能するよう、これを遵守することとする。

伊賀市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）は総務省が策定した「地方公共団体における情報セキュリティポリシーに関するガイドライン」に準拠し、本市の情報セキュリティの基本的な考え方（基本方針）とこれを実現するために遵守すべき行為、判断等の基準（対策基準）から構成される。

１．目的

情報セキュリティ基本方針は、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

基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

① 情報

紙、音声、電子データ等、あらゆる形式で保存されている事物、出来事などの内容、様子をいう。

② 情報セキュリティ

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ことをいう。

③ 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。

④ 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。

⑤ 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、情報及び関連する資産にアクセスできる状態を確保することをいう。

⑥ 情報システム

コンピュータ、ソフトウェア、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

⑦ 情報資産

情報と情報システム並びにそれらが正当に保護され使用及び機能するために必要な要件をいう。情報資産は、データ資産、ソフトウェア資産、物理的資産、サービスに分類される。

⑧ データ資産

文書、公開情報、仕様書、図面、マニュアル、データベース及びデータファイル等の電子データ、記録保管された情報等をいう。

⑨ ソフトウェア資産

アプリケーションソフトウェア、オペレーティングシステム、ユーティリティプログラム、開発ツール等をいう。

⑩ 物理的資産

コンピュータ（汎用コンピュータ、サーバ、端末、パーソナルコンピュータ等）、通信装置（電話、電話交換機、ＦＡＸ、ルータ等）、付帯設備（ＵＰＳ、発電機、

空調機等）等をいう。

⑪　サービス

情報処理サービス、電力サービス、通信サービス等をいう。

⑫　行政情報

行政事務の執行に係わる情報（個人情報を含む）をいう。又、一時的に記録されたメモ等の情報も含む。

⑬　脆弱性

情報資産が保有するセキュリティの弱い部分や、セキュリティを弱める環境等により、脅威を発生し易くさせる要因をいう。

⑭　脅威

自然災害や悪意のある行為等、情報資産に被害を与える要因をいう。

⑮　職員

本市に在職する市長をはじめとする全ての職員をいう。

⑯　委託先事業者

本市との契約に基づいて、本市が保有・管理する情報資産を取扱う事業者の社員等をいう。

⑰　記録媒体

情報を保存した電子媒体及び情報が記録された紙媒体、写真のフィルム等を示す。

⑱　情報セキュリティインシデント

「コンピュータセキュリティに関連した事件、出来事、事象」をいう。例えば、情報資産の不正使用、業務妨害行為、データの破壊、意図しない情報の開示や、更にそれらに至るための行為（事象）等をいう。

⑲　情報サービス

市民への行政サービス及び内部業務を行うために必要な情報の提供及び情報システム処理の提供をいう。

⑳　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。

㉑　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。

㉒　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。）。

㉓　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。

㉔　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。

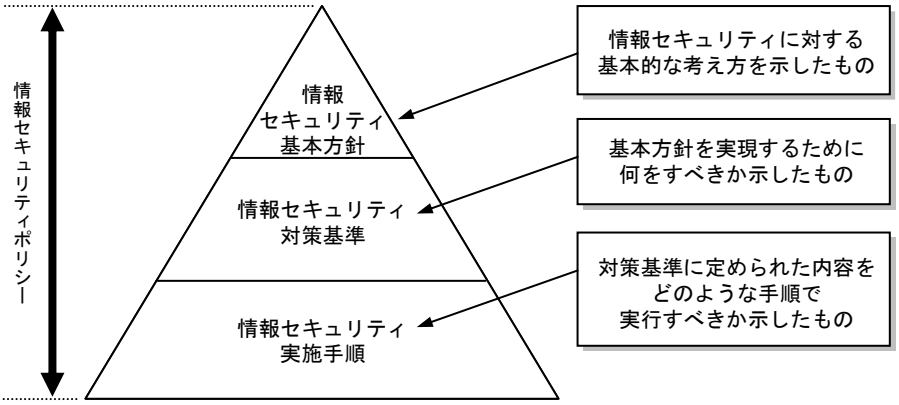
㉕　無害化通信

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．情報セキュリティポリシーの構成

情報セキュリティポリシーとは、本市の情報セキュリティの対策について、総合的、体系的かつ具体的に取りまとめたものである。

情報セキュリティに関する文書は、以下の３つの階層に分けて策定、管理するものとし、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から構成される。



３．１　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、情報セキュリティポリシーの最上位に位置する文書である。

この文書は、情報セキュリティの対策に関する基本的な方針を記述した文書である。

３．２　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、情報システム及び業務で遵守すべき対策の基準を記述した文書である。

３．３　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に基づき、各情報システム又は業務における具体的な実施手順を記述した文書である。

４．情報セキュリティポリシーの公開

情報セキュリティポリシーには、本市のセキュリティ上の脆弱性に関する内容が含まれており、情報セキュリティの確保の観点から、基本方針及び対策基準は公開し、実施手順は非公開とする。

５．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、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

６．情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は、次のとおりとする。

① 本市が管理する情報資産及び情報資産を取扱う者（職員及び委託先事業者等の従事者）全てに適用する。

② 前項に係わる業務の外部委託等をする場合は、情報セキュリティポリシーに準拠した契約を締結し、委託先事業者等に対しても本市の情報セキュリティ対策を適用する。

７．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。

８．情報セキュリティ対策

上記５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。

⑴ 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。

⑵ 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。

⑶ 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。

④ 物理的セキュリティ

情報システムを設置する施設、サーバ、通信回線及び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、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　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。

９．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。

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。

１１．情報セキュリティインシデント対応

情報セキュリティインシデントの発生に備え、事前に対応策や再発防止に関する事項を定める。

１２．行政業務継続

行政業務の継続性を高めるため、情報サービスの可用性や代替手段を確保するための行政業務継続計画に関し、必要な事項を定める。

１３．法令等の遵守

情報セキュリティポリシーの運用については、関連法令及び本市条例等に従う。

１４．違反への対応

情報セキュリティポリシーの遵守状況の確認及び遵守違反を発見した場合の報告義務並びに違反への対応に関し、必要な事項を定める。