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

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。

第１章　総則

１．目的

情報セキュリティ基本方針は、伊賀市（以下、「本市」という）の情報セキュリティに関し、包括的な対策を図ることにより、本市が保有する情報資産を適切に保護す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。

③ 機密性

アクセスを許可された者だけが情報にアクセスできることを確実にすることをいう。

④ 完全性

情報及び、情報処理方法が、正確であること及び完全であることを保護することをいう。

⑤ 可用性

許可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にする事をいう。

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、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

職員とは、本市に在職する市長をはじめとする全ての職員を示す。

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」を示す。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。

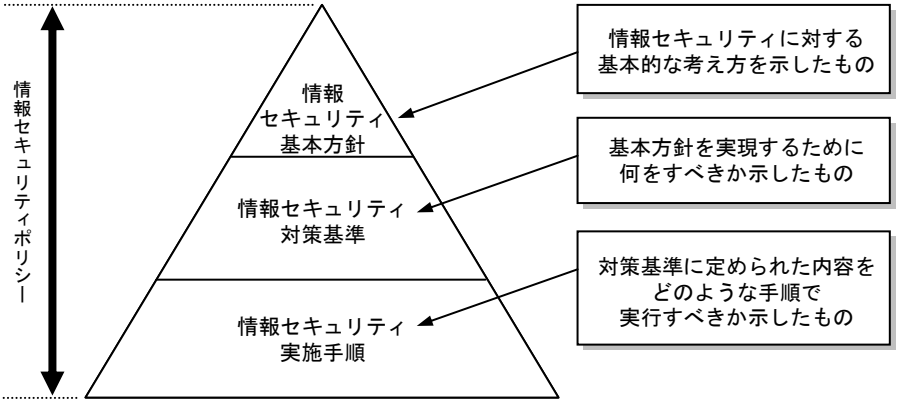
⑲　情報サービス

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。

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、伊賀市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、基本方針を公開とし、他の文書は公開してはならない。

５．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、次の通りとする。

① 本市が管理する情報資産（消防本部、市民病院及び教育委員会が個別に管理する情報資産は除く）及び情報資産を取扱う者（職員及び委託先事業者の従事者）全てに適用する。

② 前項に係わる業務を外部委託する場合には、この対策基準に準拠した契約を締結し、委託先事業者に対してもこの基準を適用する。

第２章　基本方針

１．情報セキュリティ組織運営

情報セキュリティの推進及び向上のため、情報セキュリティ組織体制の確立及び情報セキュリティポリシーの周知徹底に必要な教育等を実施する。

２．行政情報の管理

行政情報を適切に取扱うため、情報の重要度に応じた分類を行い、情報の管理責任及び取扱い方法を明確化する。

３．情報セキュリティ行動基準

職員による、市の保有するコンピュータの取扱い、パスワードの管理、電子メールの利用、インターネットの利用等に関し、情報セキュリティの確保に必要な対策を講ずる。

４．環境・機器・設備管理

情報システムを設置する施設への不正な立入、盗難、自然災害等から、情報資産を適切に保護するために、入退室管理等の必要な対策を講ずる。

５．情報システム管理

情報システムの運用に関し、情報資産を不正アクセス等から適切に保護するため、コンピュータ管理、アクセス管理、コンピュータウイルス対策等の必要な対策を講ずる。

６．ネットワーク管理

ネットワークを経由した不正なアクセス等から、情報資産を適切に保護するため、ネットワーク構成管理、ネットワークアクセス制御等の必要な対策を講ずる。

７．情報システム開発

情報システムの企画、設計、開発及び導入に関し、情報セキュリティの確保に必要な対策を講ずる。

８．外部委託

本基準は、情報サービスを外部委託等する場合、委託先事業者の選任に関し、情報セキュリティを確保するために必要な事項を定めるものとする。

９．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ものとする。

１０．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ものとする。

１１．情報セキュリティの評価・見直し

情報セキュリティポリシーの遵守状況を定期的に監査し、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の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、情報セキュリティポリシーの見直しを実施するものとする。

１２．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に従うものとする。

１３．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ものとする。