伊豆市情報セキュリティポリシー（基本方針）

令和７年７月11日
伊豆市訓令第９号
教育委員会訓令第１号
企業管理訓令第１号
議会告示第２号

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　用語の定義

基本方針における用語の意義は、次の各号に定めるところによる。

（１）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。

（２）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。

（３）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。

（４）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。

（５）情報資産

情報や情報が保存された媒体及びハードウェア、ソフトウェア、ネットワーク等の情報システム等をいう。

（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）ネットワーク

市における本庁、各支所、外部施設及び関係機関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含む。）をいう。

（８）情報システム

業務処理の電子計算機（電子計算機におけるネットワーク、ハードウェア及びソフトウェアをいう。）及び電磁的記録媒体で構成され、処理を行う仕組みをいう。

（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）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。

⑽　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。）。

⑾　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。

⑿ 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。

⒀ 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。

⒁ 職員等

市に在職する正職員、非常勤職員及び会計年度任用職員とする。

⒂ 脅威

自然災害、不正行為、事故・故障、誤操作等情報資産に被害を与える要因をいう。

3　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

4　情報資産に対する脅威

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、風水害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

5　職員等の遵守義務

職員等は、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４の様々な脅威から情報資産を保護するために次のセキュリティ対策を講ずるものとする。

（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）情報資産の分類と整理

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。

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。

②ＬGWAN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、静岡県が整備する自治体情報セキュリティクラウドに参加する。

（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、物理的な対策を講じる。

（5）人的セキュリティ

情報セキュリティに関し、職員等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（クラウドサービス）を利用する場合には、利用に係る規定を整備し、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。

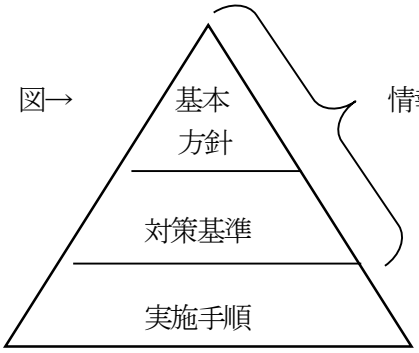
（9）評価・見直し

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。

7　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は、市の情報資産をさまざまな脅威から守るための基本的な考え方（基本方針）と、基本方針を実現するために遵守すべき行為及び判断などの基準（対策基準）から構成される。また、対策基準に基づいた具体的なセキュリティ対策のため、実施手順を定めるものとする。

図→



8　ポリシー、法令等の遵守

職務を遂行するに当たり、使用する情報資産について、情報セキュリティの重要性についての十分な認識を持ち、情報セキュリティポリシー及び関連する法令等を遵守し、これに従わなければならない。

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。

附　則

この訓令は、令和７年８月１日から施行する。