加古川市情報セキュリティポリシー

令和７年６月１日

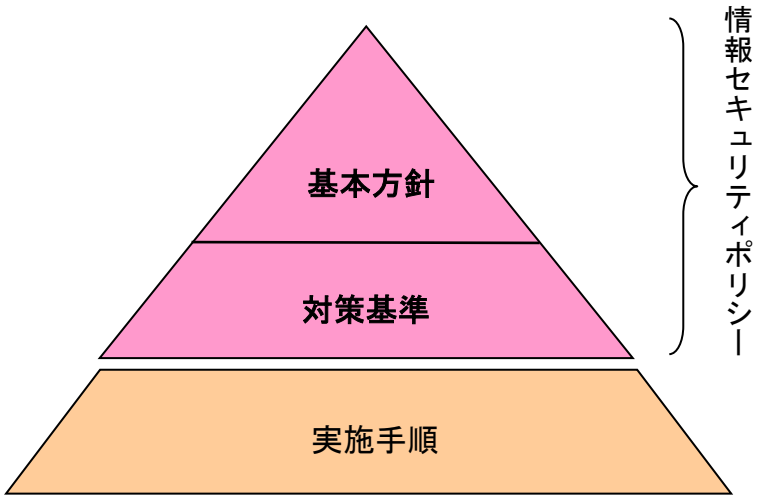
加古川市

－ 目次 －

序　章　加古川市情報セキュリティポリシーの位置付け及び構成

加古川市情報セキュリティポリシーは、本市が保有する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、体系的に取りまとめた情報セキュリティ対策の頂点に位置するものであり、情報セキュリティ基本方針及び情報セキュリティ対策基準により構成される。

【情報セキュリティポリシー体系図】



基本方針	本市の情報セキュリティ対策について、基本的な方針を定めたもの。
対策基準	情報セキュリティ対策を実施するための共通の基準を定めたもの。
実施手順	対策基準に基づき、情報セキュリティ対策を具体的に実施するために必要な事項を定めたもの。

第１章　情報セキュリティ基本方針

１．目的

本市が取り扱っている情報には、市民の個人情報や行政運営上重要な情報が多数含まれており、情報資産を適切に保護し、責任を持って管理することは、市民の財産及びプライバシーを守り、継続的かつ安定的な行政事務運営を確保するためにも必要不可欠である。

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及びその構成機器（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）個人情報

個人情報の保護に関する法律（平成 15 年法律第 57 号）第 2 条第 1 項第 1 号に規定する個人情報をいう。

（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）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。

（６）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。

（７）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。

（８）マイナンバー利用事務系

個人番号利用事務（社会保障、地方税又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。

（９）ＬGWAN接続系

ＬGWANに接続された情報システム並びに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。）。

（１０）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。

（１１）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。

（１２）無害化通信

インターネットメール本文のテキスト化、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．情報資産への脅威

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）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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な要因による情報資産の漏えい、破壊、改ざん、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．対象範囲

（１）対象機関の範囲

本基本方針の対象となる機関は、市長、教育委員会（学校を除く）、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、上下水道事業管理者、消防長及び議会とする。

（２）情報資産の範囲

本基本方針の対象となる情報資産は、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

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

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つとともに、業務の遂行にあたっては、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

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ずる。

（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。

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、端末からの情報の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、都道府県及び市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、サーバ室、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、委託を行う際のセキュリティ確保、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、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、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。

７．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。

８．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並びに、情報セキュリティに関する状況の変化等を踏まえ、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

９．情報セキュリティ対策基準の策定

情報セキュリティ対策を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

１０．情報セキュリティ実施手順の策定

情報セキュリティポリシーに基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の情報セキュリティ対策に重大な支障を及ぼすおそれがあることから非公開とする。