湖西市情報セキュリティポリシー
（基本方針）

湖　　西　　市

第１章　情報セキュリティ基本方針

１．目的

本市が取り扱う情報資産には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産、情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。今後、ガバメントクラウドの利用を中心として、マイナンバー利用事務系の標準準拠システム等のクラウドサービスの利用が浸透することが想定されるため、外部サービス（クラウドサービス）上で標準準拠システム・関連システム等の業務システム（以下「標準準拠システム等」という。）を整備及び運用する場合の考え方とその対策基準を示す。

また、ICT 技術を活用した市民の利便性の向上や行政事務の効率化が求められている中、本市が電子自治体を構築するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

このため、本市の情報資産の機密性、完全性及び可用性を維持するための対策を整備するため、湖西市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

２．定義

（１）ネットワーク

本市における各部局、各行政委員会、地方公営企業（医療用ネットワークを除く）及び教育機関（教育用ネットワークを除く）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

業務系の電子計算機（業務系におけるネットワーク、ハードウェア及びソフトウェア）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。

（３）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。

（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）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）基幹系

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。

（９）インターネット系

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。

（１０）情報系

基幹系、インターネット系以外の総合行政ネットワーク（LGWAN）に接続された情報システム及びデータをいう。また、必要なセキュリティ対策を講じた上で外部のクラウドサービスと接続（ローカルブレイクアウト）を行うことが出来る。

（１１）通信経路の分割

情報系とインターネット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。

（１３）ISMAP 管理基準

クラウドサービス調達における政府が求めるセキュリティ基準のことをいう。また、評価基準を満たした業者を、審査結果に基づいて「ISMAP クラウドサービスリスト」に登録される。

３．情報セキュリティポリシーの位置付け

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、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

４．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

５．適用範囲

（１）行政機関の範囲

この情報セキュリティポリシーが対象とする範囲は、本市の保有する情報資産を利用するすべての部署を対象とする。

なお、統括情報セキュリティ責任者が指定し、各教育機関における教育のために用い、又は市立湖西病院における医療のために用いるネットワーク及び情報システム等は、この情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けるものとし、本情報セキュリティポリシーの対象としない。

（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。

ア．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

イ．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。）

ウ．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

６．職員等及び委託事業者の義務

職員等及び委託事業者は、業務遂行にあたり、情報セキュリティの重要性に対する統一された意識を持ち、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十分に理解し、遵守する義務を負うものとする。

７．情報セキュリティ対策

上記４の脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講ずる。

（１）組織体制

本市の保有する情報資産を保護するため、全庁的な情報セキュリティ管理体制を確立するものとする。

（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ずる。

ア．基幹系においては、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、住民情報等の流出を防ぐ。

イ．情報系においては、業務用システムとインターネット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、静岡県及び静岡県下の市町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対策

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、物理的な対策を講ずる。

（５）人的セキュリティ対策

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・啓発を行う等の人的な対策を講ずる。

（６）技術的セキュリティ対策

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ずる。

（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ずるものとする。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（クラウドサービス）の利用

業務委託する場合には、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ずる。

外部サービス（クラウドサービス）を利用する場合には、利用にかかわる規定を整備し対策を講ずる。

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。

８．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。

９．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。

１０．情報セキュリティ対策基準の策定

本市の様々な情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一することが必要となる。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

１１．情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、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、情報セキュリティ対策基準及び情報セキュリティ実施手順は、詳細なセキュリティ対策を示したものであるため、公にすることにより本市の行政運営に重大な支障を及ぼす恐れのある情報資産であることから組織外への公開は行わないものとする。