# 湖南市サイバーセキュリティを確保するための方針

# （湖南市情報セキュリティポリシー）

令和８年３月

湖南市

# 目次

# 序　サイバーセキュリティを確保するための方針と情報セキュリティポリシーについて

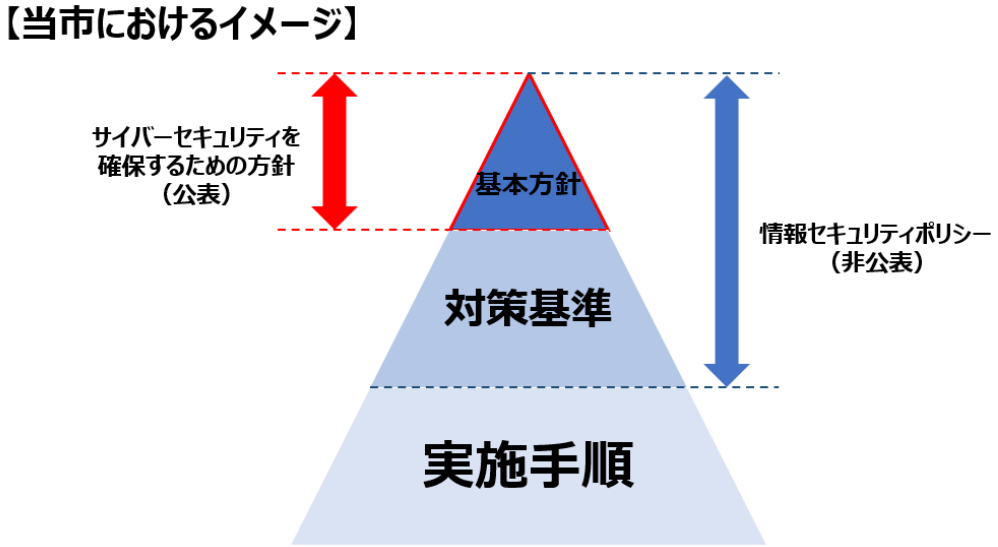
令和６年６月に地方自治法が改正され、地方自治体はサイバーセキュリティの確保について方針を定め、必要な措置を講じなければならないものとされた。また、方針の策定又は変更については、総務大臣が指針を示すこととされ、令和７年４月に「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針（案）」（以下「指針」という。）が示された。

当市では、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化してくことを目的に、現行の情報セキュリティポリシーのうち「情報セキュリティ基本方針」について指針を踏まえて見直しを行い、地方自治法第 244 条の６第１項に規定する「サイバーセキュリティを確保するための方針」に位置付けることとした。

なお、情報セキュリティポリシーは、当市の情報資産に対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文書を総称し、当市の情報資産に関する業務に携わる職員、行政機関委員及び外部委託事業者は、業務の遂行にあたり情報セキュリティポリシーを遵守する義務を負う。

情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層で構成されている。「情報セキュリティ基本方針」は地方自治法における方針と位置づけ公表する（地方自治法第 244 条の６第２項）。ただし、「情報セキュリティ対策基準」以下はセキュリティ確保のため公表はしないこととする。

当市における各方針のイメージを次に示す。



# 第１章　情報セキュリティ基本方針

## 1.1　目的

市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、住民の財産やプライバシー等を守るとともに、行政内部事務の安定的な運営のためにも必要不可欠である。このことが市行政に対する住民の信頼度、満足度を向上させるのに寄与するものである。

また、近年のいわゆるＩＴ革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなってきている状況下、市がこれらに対応するために、全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となるところである。

以上のことを踏まえ、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(以下「情報セキュリティ対策」という。)を整備するために「湖南市情報セキュリティポリシー」を策定し、市が実施する情報セキュリティ対策についての基本的な事項を定めることを目的とする。

## 1.2　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、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、ネットワーク及び記録媒体で構成され、情報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、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(Confidentiality)

情報にアクセスすることが認可された者だけが、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(Integrity)

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(Availability)

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．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。）。

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。

## 1.3　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．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、重要情報の搾取、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・広範囲にわたる疫病による要因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、水道供給の途絶等の提供サービスの障害からの波及等

## 1.4　適用範囲

１．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市の機関の範囲は、以下の組織（以下

「本市組織」という。）の情報資産に関連する人的・物理的・環境的資源とする。

⑴　市長（総合政策部、総務部、健康福祉部、こども未来応援部、都市建設部、環境経済部、教育部）

⑵　議会事務局、出納局、監査委員、公平委員会、固定資産評価審査委員会、選挙管理委員会、農業委員会、上下水道事業所

⑶　教育委員会（市の内部情報システムが及ぶ小中学校の事務室又は職員室を含む）

２.情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

⑴　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記録媒体

⑵　ネットワーク及び情報システム

⑶　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

## 1.5　職員等の遵守義務

職員、行政機関委員及び外部委託事業者（以下「職員等」という。）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、業務の遂行にあたって情報セキュリティポリシーを遵守しなければならない。

## 1.6　情報セキュリティ対策

上記１．３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

本市の所有する情報資産を機密性、完全性、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行う。

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。高度な情報セキュリティ対策として、滋賀県及び本市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、情報システム室、通信回線及び職員等のパソコン等の端末の管理について、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（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じる。

９．外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じる。

10．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。

11．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。

## 1.7　情報セキュリティ対策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に、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する。

## 1.8　情報セキュリティ対策基準の策定

上記1.6及び1.7に規定する対策等を実施するために、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。

なお、情報セキュリティ対策基準は、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おそれがあることから非公開とする。

## 1.9　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行政運営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。

## 1.10　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となった場合には、情報セキュリティポリシーを見直す。