相模原市情報セキュリティ基本方針

（目的）

第１条　この方針は、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、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。なお、この方針は、地方自治法に基づくサイバーセキュリティを確保するための方針として定めるものである。

（定義）

第２条　この方針において、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）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並びにその構成機器である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）クラウドサービス　ソフトウェア、データ、サーバその他のコンピュータシステムの一部をインターネットを経由して提供するサービスをいう。

（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）情報セキュリティポリシー　この方針及び情報セキュリティ対策基準をいう。

（６）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。

（７）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。

（８）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。

（９）基幹系　個人番号（社会保障、地方税若しくは防災に関する事務に係るものに限る。）を取り扱う情報システム、共通基盤システムと連携する情報システム及び個人や法人の特定に利用する番号を有する情報システム及びデータをいう。

(10) 情報系（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（基幹系を除く。）。

(11) インターネット接続系　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。

(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ない等、安全が確保された通信をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、以下の要因を想定し、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・設定のミス、メンテナンスの不備、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

（適用範囲）

第４条　この方針が適用される組織及び情報資産は、次のとおりとする。

（１）本基本方針が適用される組織は、議会の事務局、市長の事務部局、市選挙管理委員会の事務局、区選挙管理委員会の事務局、監査委員の事務局、消防機関、人事委員会の事務局、農業委員会の事務局並びに教育委員会の事務局及び学校以外の教育機関とする。

（２）この方針が適用される情報資産は、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

（職員の遵守義務）

第５条　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、業務の遂行において、情報セキュリティに関する法令等を遵守しなければならない。

２　職員は、契約により市の事務事業の委託を受けた事業者、派遣労働者（労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和６０年法律第８８号）第２６条第１項に規定する労働者派遣契約に基づき市に派遣され、市の事務事業に従事する者をいう。）その他市の事務事業に従事する者に対して、事業執行に当たりこの方針を遵守するよう周知し、及び徹底しなければならない。

（情報セキュリティ対策）

第６条　第３条に挙げた脅威から情報資産を保護するため、以下の情報セキュリティ対策を講じる。

（１）組織体制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）情報セキュリティの強化を目的として、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。

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、住民情報の流出を防ぐ。

イ　情報系においては、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。

ウ　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、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として、サーバ、管理区域、通信回線及び職員のパソコン等

の管理について、必要な対策を講じる。

（５）人的セキュリティ対策として、情報セキュリティに関する遵守事項を定めるとともに、十分な教育及び啓発を行う等の必要な対策を講じる。

（６）技術的セキュリティ対策として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必要な対策を講じる。

（７）情報セキュリティ対策の運用における対策として、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、業務委託やクラウドサービス利用時のセキュリティ確保等の対策を講じる。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）業務委託を実施する場合は、委託事業者が守るべき情報セキュリティ要件を明記した契約を締結する。また、必要な情報セキュリティ対策が確保されていることを確認し、契約に基づき必要な措置等を講じる。

（９）クラウドサービスを利用する場合は、利用に係る規定を整備し必要な対策を講じる。

(10) ソーシャルメディアサービスを利用する場合は、目的及び効果を十分に検討した上で、運用手順を定め、必要な対策を講ずる。

（情報セキュリティ監査及び自己点検の実施）

第７条　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。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティ監査及び自己点検の結果、または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な対策が必要になった場合には、情報資産に関わるリスクを分析・検討した上で、情報セキュリティポリシーを見直す。

（情報セキュリティ対策基準の策定）

第９条　この方針に基づく情報セキュリティ対策を実施するため、具体的な遵守事項及び判断基準等を定めた情報セキュリティ対策基準を策定する。

（情報セキュリティ実施手順の策定）

第１０条　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。

附　則

この方針は、令和８年４月１日から施行する。