久喜市情報セキュリティポリシー
情報セキュリティ基本方針

令和８年４月１日

１　目的

本基本方針は、市が所有する情報資産の機密性、完全性及び可用性を的確に維持するため、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、本方針は、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」として位置付けるものとする。

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、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）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。（情報を許可された者だけが利用できること）

（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。（情報が正確で完全であること）

（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。（情報を必要な時に利用できること）

（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。

３　対象となる脅威

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

４　適用範囲

（１）行政機関の範囲

本基本方針が対象とする行政機関の範囲は、市長部局（上下水道部及び小・中学校（財務会計システム端末）を含む。）、議会及び各行政委員会とする。

（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（これらの印刷文書を含む）

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（設計ドキュメント、運用のためのドキュメント及び操作研修のためのドキュメント等）

５　情報セキュリティポリシーの位置付と職員等の義務

情報セキュリティポリシーは、市が所掌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。

したがって、情報資産に関する業務に携わる全ての職員等及び委託事業者は、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、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する義務を負うものである。

６　情報セキュリティ対策

３の脅威から、情報資産を保護するためには、安全性と利便性のバランスをとることが必要であり、これらを踏まえて、以下の情報セキュリティ対策を講ずる。

（１）組織体制

市の情報資産について、幹部（市長、副市長、教育長（校務部分を除く）及び部長級の職員）が、率先して情報セキュリティ対策を推進・管理するための組織体制を確立する。

（２）情報資産の分類と管理

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、次の三段階の措置を講ずる。

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。

② 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。

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、埼玉県及び市のインターネットとの通信を集約したうえで、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、情報システムを設置する管理区域、通信回線及び職員等のコンピュータ等の管理について、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、職員等及び委託事業者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ずる。

（６）技術的セキュリティ対策

コンピュータ等管理、情報資産へのアクセス制御、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）運用におけるセキュリティ対策

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。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

業務委託を行う場合には、委託事業者と情報セキュリティ要件を明記した契約を締結する。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定期的に確認し、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ずる。

ソーシャルメディアサービスを利用する場合には、その運用手順や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実施する。

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、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､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の見直しを実施する。

９　情報セキュリティ対策基準の策定

市の様々な情報資産について、６の情報セキュリティ対策を講ずるにあたっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。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。

10　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に、個々のシステム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。

なお、情報セキュリティ実施手順は、各情報資産に関するシステム運用・保守に関する実施手順をまとめたもので、公にすることにより市の行政運営に重大な支障を及ぼす恐れのあることから非公開とする。