第１章 情報セキュリティ基本方針

第１節 基本的な考え方

ICT（Information and Communication Technology：情報通信技術）の進展による情報のネットワーク化は、その利便性・効率性により急速な普及を遂げている。さいたま市においても、いまや情報システムは業務遂行に必要不可欠なものとなり、また、情報化を推進するにあたり、ICT の利活用はさらに期待されているところである。

しかし、ICT の利便性・効率性が注目される一方で、不正アクセスや情報漏えい等の情報の安全性を侵害する問題が発生している。市が取り扱う情報には、市民の個人情報（特定個人情報を含む）をはじめとする重要な情報が多数含まれており、適切な使用を怠った場合には、「業務継続の中断」や「信用の失墜」等行政運営の根幹にかかわる極めて重大な結果を招くことになる。

市は、これらの脅威を組織共通の認識として一貫した方針のもと情報セキュリティ対策を行うこととし、その指針として「さいたま市情報セキュリティポリシー」を定める。職員は、これを遵守して情報セキュリティの確保に取り組み、「情報資産の安定活用」及び「行政活動の基本である住民の信頼」の維持・向上に努めなければならない。

第２節 定義

さいたま市情報セキュリティポリシー（以下「ポリシー」という。）で使用する用語の定義は、次のとおりとする。

(1) 情報セキュリティ

情報資産の機密性(注)、完全性及び可用性を確保し、維持することをいう。

（注）国際標準化機構（ISO）が定めるもの（ISO 7498－2：1989）。

機密性（confidentiality）：情報にアクセスすることが許可された者だけがアクセスできることを確実にすること。

完全性（integrity）：情報及び処理の方法の正確さ及び完全である状態を完全防護すること。

可用性（availability）：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

(2) 行政情報

さいたま市の業務の執行上、作成又は取得した情報で、情報システムに電磁的に記録されたもの及び入出力帳票等をいう。

(3) 情報システム

ハードウエア、ソフトウエア、ネットワーク、記録媒体等で構成され、これら一部又は全体で業務処理を行う仕組み（構成又は仕様に関する資料等を含む。）をいう。

(4) ネットワーク

情報の共有等を目的として通信回線、通信機器等で構成された通信網をいう。

(5) 記録媒体

行政情報の記録・管理に使用される磁気ディスク、磁気テープ、光ディスク等をいう。

(6) 情報資産

行政情報及び情報システムをいう。

(7) 業務用パソコン

職員等が業務で使用するコンピュータをいう。これには、タブレットやスマートフォン等のモバイル端末も含む。

(8) 私物パソコン

職員等が所有するコンピュータをいう。これには、タブレットやスマートフォン等のモバイル端末も含む。

(9) 業者パソコン

業者等が所有するコンピュータをいう。これには、タブレットやスマートフォン等のモバイル端末も含む。

(10) 職員等

職員、臨時職員、非常勤職員等の任用形態、職位及び勤務地を問わず、さいたま市の全職員をいう。

(11) クラウドサービス

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。このクラウドサービスの形態としては、SaaS（Software as a Service）、PaaS（Platform as aService）、IaaS（Infrastructure as a Service）が存在する。クラウドサービスの例としては、Web 会議サービス、SNS、検索サービス、翻訳サービス、地図サービス、ファイル転送サービス等が存在する。ただし、電話やメール等の電気通信サー

ビス、郵便、運送サービス等は除く。

(12) 業務委託サービス

事業者等の庁外の組織がさいたま市向けに重要情報を取り扱う情報システムの一部の機能を提供するものをいう。業務委託サービスの例としては、ホスティングサービス、インターネット回線接続サービス等が存在する。ただし、クラウドサービスを除く。

第３節 ポリシーの位置付けと構成

ポリシーは、さいたま市の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とりまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

ポリシーは、次の二階層で構成する。

(1) 情報セキュリティ基本方針（以下「基本方針」という。）

ポリシーの上位層に位置付けられるもので、情報セキュリティに対する基本的な考え方や方針を示すものである。

(2) 情報セキュリティ対策基準（以下「対策基準」という。）

基本方針を実行に移すために遵守すべき事項及び判断等の統一的基準を示すものである。

また、基本方針に基づき個々の情報資産に対し、どのような手順に従って情報セキュリティ対策を実行していくのかを具体的に定めるとともに、対策基準に基づいたセキュリティ実施手順（以下「実施手順」という。）を策定することとする。

第４節 対象範囲

ポリシーの対象範囲は、市長及び市長の補助機関（地方公営企業を含む。）並びにその他の執行機関の事務局、その他法律に基づき本市に置かれる機関の事務局等とする。

詳細は、情報セキュリティポリシー付属適用範囲表において定める。

第５節 責務

職員等は、情報セキュリティの確保を共通の認識とするとともに、情報資産を保護し、かつ、適切に使用するためにポリシー及び関連する法令等を遵守しなければ

ならない。

また、情報資産を取り扱う委託事業者、指定管理者(注)、外郭団体、クラウドサービス提供者等（以下「委託業者等」という。）に対しても、契約等を通じて、又は別途取り決めを行うことにより、ポリシーを遵守させるための措置を講じなければならない。

（注）指定管理者：地方自治法（昭和２２年法律第６７号）第２４４条の２第３項に規定する指定管理者をいう。

第６節 情報セキュリティ管理方針

次に掲げる各事項を情報セキュリティに関する管理方針とする。

第１項 組織・体制の確立

情報セキュリティ対策を推進、管理するため、組織・体制を確立し、責任、権限等を定める。

第２項 情報資産の分類と管理

適切かつ効果的な情報セキュリティ対策を実施するために、情報資産の分類及び管理方法について定める。

第３項 情報セキュリティ対策

情報資産を脅威(注)から保護するため、脆弱性(注)を排除又は低減させる対策を定める。

（注）脅威：情報資産に損失を発生させる要因をいう。主な脅威を以下に示す。

ア　侵入、破壊、故障、停電、災害等

イ　不正アクセス、盗聴、コンピュータウイルス、改ざん・消去、なりすまし等

ウ　誤操作、持ち出し、不正行為等

（注）脆弱性：脅威を顕在化させる要因をいう。主な脆弱性を以下に示す。

ア　入退室管理の不備、保守の不備、予備電源の不備等

イ　情報システムの設定ミス、コンピュータウイルス対策の不備、認証情報の管理不備等

ウ　教育や周知徹底の不備、契約内容の不備等

第４項 ポリシーの運用管理

ポリシーの実効性を確保するため、情報システムの稼動監視及び職員等のポリシー遵守状況の確認事項等を定めるとともに、情報セキュリティを侵害する事案

が発生した場合において、迅速な対応を実施するために必要な事項等を定める。

第５項 評価・見直し

情報セキュリティ水準の向上のため、監査及び点検、ポリシー及び情報セキュリティ対策の評価、これらに基づくポリシーの見直しについて定める。

第７節　情報セキュリティに関する違反への対応

職員等がポリシー及び関連する実施手順に定められた事項に違反した場合は、その重大性に応じて地方公務員法をはじめとする各関連法令の罰則の対象となり得る。