所沢市情報セキュリティ基本方針（サイバーセキュリティを確保するための方針）

１．　目的

本基本方針は、所沢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、所沢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。

２．　定義

（１）コンピュータ

① パーソナルコンピュータ（以下「パソコン」という。）

② モバイル端末（スマートフォン・タブレット等）

業務上の必要に応じて移動させて使用することを目的とした端末

③ サーバ

④ その他類似・周辺機器等（IoT 機器を含む）

（２）ネットワーク

コンピュータ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。また、全庁で利用するネットワークを特に全庁ネットワークという。

（３）電磁的記録媒体

① コンピュータに内蔵される電磁的記録媒体

② 外付けストレージ（ハードディスクドライブ、SSD 等）

③ USB メモリ

④ 光学記憶媒体（CD-R、DVD-R、BD-R 等）

⑤ 磁気テープ

⑥ その他類似する電磁的記録媒体

（４）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。

（５）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。

（６）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。

（７）情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務遂行を危うくする確率及び情報セキュリティを脅かす確率の高いものをいう。

（８）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。

（９）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。

（１０）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。

（１１）基幹系（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。

（１２）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）。

（１３）インターネット接続系

ホームページ閲覧、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。

（１４）通信経路の分割

情報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。

（１５）無害化通信

電子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。

（１６）委託事業者

業務委託契約等により、所沢市の業務執行を受託した事業者をいう。所沢市情報セキュリティポリシーにおいては、業務委託サービス（（１７）にて定義）の提供者を含む。

（１７）業務委託サービス

事業者等の庁外の組織が所沢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サービスのことをいう。ただし、クラウドサービスは含まない。例として、ホスティングサービスや回線接続サービス等が該当する。

（１８）業務委託サービス管理者

業務委託サービスの利用における利用申請の許可権限者から利用承認時に指名された当該業務委託サービスに係る管理を行う者をいう。

（１９）クラウドサービス

インターネット等のネットワークを経由して、コンピュータやデータ、ソフトウェア等を利用できるサービスをいう。クラウドサービスの例としては、SaaS（Software as a Service)、PaaS（Platform as a Service)、IaaS（Infrastructure as a Service）等が存在する。

（２０）クラウドサービス提供者

クラウドサービスを提供する事業者をいう。なお、委託事業者等が他社のクラウドサービスを利用して所沢市にサービスを提供する場合、当該他社のクラウドサービスの事業者と所沢市は直接契約締結や約款同意を行わないのでクラウドサービス提供者には含めない。

（２１）クラウドサービス管理者

クラウドサービスの利用における利用申請の許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う者をいう。

（２２）Web 会議サービス

専用のアプリケーションや Web ブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行えるクラウドサービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）や、閉域のネットワーク環境で構築したものは含まれない。

（２３）ソーシャルメディアサービス

インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持った Web サイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

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）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

本基本方針が適用される行政機関は、市長の事務部局、教育委員会、市議会事務局及び各行政委員会並びに上下水道事業の部局、病院事業の部局とする（但し、市立小・中学校における教育のために用いるネットワーク及び情報システム等、また医療センター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除く）。

（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（これらを印刷した文書を含む。）

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

５．　職員等及び委託事業者の遵守義務

職員、会計年度任用職員、臨時的任用職員、非常勤の特別職員（以下「職員等」という。）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ち、業務の遂行に当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しなければならない。

６．　情報セキュリティ対策

上記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

所沢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

所沢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じる。

① 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。

② 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。

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、埼玉県及び所沢市を含む市区町村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、コンピュータ機械室、通信回線及び職員等のコンピュータの管理について、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。

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。

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。

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、リスクを検討した上で、情報セキュリティポリシーを見直す。

９．　情報セキュリティ対策基準の策定

上記６、７及び８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所沢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、所沢市情報公開条例第７条４号及び６号の規定により一部を除き非公開とする。

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所沢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、所沢市情報公開条例第７条４号及び６号の規定により非公開とする。