豊田市情報セキュリティ基本方針

（目的）

第１条　本市は、市民の個人情報をはじめ、極めて重要な情報を多数保有している。これらの情報が、漏洩、改ざん、破壊された場合、市民の権利、財産を侵害し、取り返しのつかない影響を及ぼすおそれがある。

したがって、これらの情報やその情報を取り扱う情報システムを様々な脅威から防御することは、市民の権利・財産を守るため、また、行政事務の安定的な運営のためにも必要不可欠であり、信頼される市政の基礎となる。

そこで本市は、保有する情報や情報システムの安全性を維持向上するため、本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。

（定義）

第２条

（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当該通信網を構成す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、記録媒体及びプログラムで構成され、情報処理を行う仕組みをいう。

（３）データ

情報システムを構成するハードウェア、ソフトウェア及び情報システムで扱うことができる形にした文字、数値、記号、音声、静止画、動画等をいう。

（４）情報資産

情報システムを構成するハードウェア及びソフトウェア並びに情報システムで扱う全てのデータをいう。

（５）アクセス

情報システムに対して、物理的に、又はネットワークを介して、操作、記録、変更等の動作を行うことをいう。

（６）情報処理

データの入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれに類する行為をいう。

（７）情報処理装置

情報処理を行う装置をいう。ただし、ＡＥＤ、防犯カメラ、車載カメラ等の特定の場所に設置され、単独で特定の情報処理機能のみを持つ装置を除く。

（８）情報処理施設等

情報処理に関わる施設及び設備をいう。

（９）外部記録媒体

磁気ディスク、光化学ディスク、フラッシュメモリ、その他の情報処理装置の外部にデータを記録できる装置又は媒体をいう。

（１０）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。
（１１）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に関し実施すべき項目を網羅した文書をいう。
（１２）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。
（１３）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。
（１４）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。
（１５）マイナンバー利用事務系（個人番号利用事務系）
　特定個人情報（行政手続における特定の個人を識別するための番号の利用等に関する法律(平成２５年法律第２７号)第２条第 8 項に規定する特定個人情報をいう。）を取り扱う個人番号利用事務（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。
（１６）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。）。
（１７）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。
（１８）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。
（１９）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。
（２０）クラウドサービス
　データやアプリケーション等のコンピュータ資源をネットワーク経由で利用する仕組みのことをいう。

（対象とする脅威）
第３条　情報資産に関する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。
（１）サイバー攻撃を始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、設計又は開発の不備、プログラム上の欠陥、操作又は設定のミス、メンテナンスの不備、内部又は外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器の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）大規模かつ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　本基本方針は、市長、教育委員会、選挙管理委員会、監査委員、公平委員会、農業委員会、固定資産評価審査委員会、事業管理者、消防長、議会及び豊田市土地開発公社（以下「適用機関」という。）が所管する情報資産（適用機関が、適用機関以外のものに貸与し、専ら当該適用機関以外のものの業務を処理するための情報資産を除く。以下同じ。）並びに当該情報資産に接する全ての当該適用機関の職員（非常勤特別職員、会計年度任用職員及び適用機関が外郭団体に派遣した職員を含む。以下「職員等」という。）及び議員を適用範囲とする。

（職員等及び議員の順守義務）
第５条　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実施手順に定められた事項を遵守する義務を負うとともに、その役割と責任において、協力して豊田市全体の情報セキュリティの確保に努める。

（情報セキュリティ対策）
第６条　第３条に規定する脅威から情報資産を保護するために、次に掲げる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）物理的セキュリティ
　サーバ、情報システム室、通信回線、職員等及び議員のパソコン等の管理について、物理的な対策を講じる。
（４）人的セキュリティ
　情報セキュリティに関し、職員等及び議員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。
（５）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。

（６）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。

（７）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。

また、外部サービス（クラウドサービス）を利用する場合にも対策を講じる。

（８）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。

（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、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を見直す。

（対策基準の策定）

第９条　第６条、第７条及び第８条に規定する対策等を実施するために、情報セキュリティに関し実施すべき項目を網羅する文書を策定する。

（実施手順の策定）

第１０条 第９条で策定する文書に基づき、具体的な遵守事項及び判断基準並びに具体的対策を確実に実行するための実施手順を策定するものとする。

なお、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。

（基本方針の決定及び施行方法）

第１１条 本基本方針は、豊田市長及び豊田市議会議長の決定を以て、連名により施行する。