○つくばみらい市情報セキュリティ基本方針

（目的）

第１条　この訓令は、本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、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ことを目的とする。

（定義）

第２条　この訓令において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）　実施機関　市長(水道事業及び下水道事業の管理者の権限を行う市長を含む。)、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会をいう。

（２）　職員等　次のいずれかに該当する者をいう。

ア　地方公務員法(昭和25年法律第261号)第3条第2項に規定する一般職に属する職員及び同条第3項に規定する特別職に属する職員

イ　市が委託契約、請負契約その他の契約を締結している者が行う当該契約に基づく業務に従事する者

ウ　地方自治法(昭和22年法律第67号)第244条の2第3項の規定により市が指定した者が行う市の公の施設の管理業務に従事する者

（３）　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及びその構成機器（ソフトウェアを含む。）をいう。

（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　この訓令及びつくばみらい市情報セキュリティ対策基準をいう。

（７）　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。

（８）　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。

（９）　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。

（１０）　マイナンバー利用事務系　個人番号利用事務、戸籍事務等に関わる情報システム及びデータをいう。

（１１）　ＬＧＷＡＮ接続系　総合行政ネットワーク（以下「ＬＧＷＡＮ」という。）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）　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。

（１３）　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うえで、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。

（１４）　無害化通信　インターネットメール本文のテキスト化、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。

（情報資産の範囲）

第３条　この訓令における情報資産とは、次のとおりとする。

（１）　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体等

（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、ネットワーク図等のシステム関連文書

（対象とする脅威）

第４条　実施機関は、情報資産に対する脅威として、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ものとする。

（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、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、改ざん及び消去、重要情報の詐取並びに内部不正

（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、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及び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

（４）　大規模及び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

（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

（職員等の遵守事項）

第５条　職員等は、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共通実施手順を遵守しなければならない。

（情報セキュリティ対策）

第６条　実施機関は、第４条に規定する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講ずるものとする。

（１）　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）　本市が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のため、次に掲げる対策を講ずる。

ア　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うえで、端末からの情報持ち出し不可設定、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　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する情報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ものとし、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

キュリティ対策として、都道府県及び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）　サーバ、サーバ室、通信回線、職員等のパソコン等の管理について、物理的な対策を講ずる。

（５）　情報セキュリティに関し、職員等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）　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ずる。

（７）　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、外部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とともに、情報資産に対するセキュリティ侵害が発生した場合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

ア　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ずる。

イ　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じる。

ウ　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。

（監査及び自己点検）

第７条　実施機関は、情報セキュリティポリシーの遵守状況を検証するため、定期に又は必要に応じて随時に情報セキュリティ監査及び自己点検を実施するものとする。

（情報セキュリティポリシーの見直し）

第８条　実施機関は、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又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に対策が必要になった場合は、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行うものとする。

（対策基準の策定）

第９条　実施機関は、前３条に規定する対策等を実施するため、具体的な遵守事項、判断基準等を定める情報セキュリティ対策基準（以下「対策基準」という。）を策定するものとする。

２　対策基準は、つくばみらい市情報公開条例（平成１８年つくばみらい市条例第９号）第７条第７号の規定により、非公開とする。

（共通実施手順の策定）

第１０条　実施機関は、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共通実施手順（以下「共通実施手順」という。）を策定するものとする。

２　共通実施手順は、つくばみらい市情報公開条例第７条第７号の規定により、非公開とする。

（補則）

第１１条　この訓令に定めるもののほか、情報セキュリティ対策に関し必要な事項は、市長が別に定める。

附　則

この訓令は、令和８年４月１日から施行する。