資料 No.7-2

つくば市長、つくば市教育委員会、つくば市選挙管理委員会、つくば市等公平委員会、つくば市監査委員、つくば市農業委員会、つくば市固定資産評価審査委員会及びつくば市議会は、地方自治法（昭和 22 年法律第 67 号）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、つくば市情報セキュリティ基本方針を共同で定める。

令和８年４月１日

つくば市長
つくば市教育委員会
つくば市選挙管理委員会
つくば市等公平委員会
つくば市監査委員
つくば市農業委員会
つくば市固定資産評価審査委員会
つくば市議会

つくば市情報セキュリティ基本方針（案）

１　目的

つくば市（以下「本市」という。）は、市民の個人情報や非公開情報など、外部への漏えいやデータの改ざん等の被害を受けた場合に極めて重大な結果を招く情報資産を多数保有している。

したがって、サイバー攻撃等の不正アクセスや災害等によるシステム停止など、

様々な脅威から本市の情報資産を守ることは、市民の財産やプライバシーを保護するとともに、組織の安定的な運営を図るために必要不可欠である。

つくば市情報セキュリティ基本方針（以下「本方針」という。）は、本市が保有する情報資産の機密性・完全性・可用性を維持する対策として、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。

2　用語の定義

本方針において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1) 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。

ア　機密性　情報にアクセスすることを許可された者だけが、確実に情報にアクセスできることをいう。

イ　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。

ウ　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。

(2) 端末　パーソナルコンピュータのほか、スマートフォンその他これらに類する機能を持つ機器のことをいう。

(3) 電磁的記録媒体　USBメモリ、SD カード、ハードディスク、SSD、CD、DVD 及び Blu-ray Disc 等の電子情報を記録可能な媒体をいう。

(4) 外部デバイス　電磁的記録媒体以外のものであって、プリンタ、スキャナその他端末に接続して使用する機器（マウス、キーボード、ディスプレイ、Webカメラ、ヘッドセット及びこれらに類するものを除く。）をいう。

(5) ネットワーク　端末を相互に接続するための通信網及びその構成機器（ハー

ドウェア及びソフトウェア）をいう。

(6) 情報システム　端末、ネットワーク及び電磁的記録媒体で構成されるものであって、情報処理を行う仕組みをいう。

(7) 情報資産　情報システム及び情報システムで取り扱う情報をいう。

(8) 外部サービス　外部組織が情報システムの一部又は全部の機能を提供するサービスをいう。

3　対象とする脅威

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。

(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) 機関の範囲

本方針が適用される機関は、市長、教育委員会、選挙管理委員会、公平委員

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とする。

(2)情報資産の範囲

本方針が対象とする情報資産は、次に掲げるものとする。

ア　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、電磁的記録媒体及び外部デバイス

イ　ネットワーク及び情報システムで取り扱うデータ

ウ　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　対策基準・実施手順の策定

各機関は、本方針の目的を達成するため、必要に応じて具体的な対策基準又は運用ルール等の規程及び実施手順（以下「対策基準等」という。）を定めるものとする。対策基準等については、公にすることにより、本市の運営に重大な支障を及ぼす恐れがあることから非公開とすることができるものとする。

6　遵守義務

各機関に所属する者は、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、業務の遂行に当たって本方針及び対策基準等を遵守しなければならない。

7　情報セキュリティ対策

各機関は、3の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対策基準等により必要に応じて実施するものとする。

(1) 組織体制　情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理　本市が保有する情報資産の分類については、「地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）」で規定する機密性・完全性・可用性の概念を参考とし、当該分類に基づ

き、情報セキュリティ対策を講じる。

(3)物理的セキュリティ　端末、ネットワークの管理について、物理的な対策を講じる。

(4) 技術的セキュリティ　情報システム等の管理、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。

(5) 人的セキュリティ　情報セキュリティに関し、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) 運用　情報システムの監視、対策基準等の遵守状況の確認、業務委託を行う際のセキュリティ確保等、運用面の対策を講じる。

(7) 業務委託と外部サービスの利用　業務委託する場合には、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。

(8) 評価・見直し　対策基準等の遵守状況を検証するため、定期的又は必要に応じて自己点検及び情報セキュリティ監査を実施し、必要な場合には、運用改善及び対策基準等の見直しを行い、情報セキュリティの向上を図る。

8　見直し

情報セキュリティに対する状況の変化に対応する等の理由により、本方針の見直しが必要となった場合は、これを行うものとする。