# ふじみ野市議会情報セキュリティ基本方針

## 1　目的

この基本方針は、ふじみ野市議会（以下「議会」という。）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、議会の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。なお、ふじみ野市議会議員（以下「議員」という。）個人が、議員活動の中で取得した情報資産は、基本方針の対象外とする。

## 2　定義

(1) 情報資産

議会が保有し又は管理する情報及びこれを取り扱うための設備、システム、その他一切の資源をいう。

(2) 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（ハードウェア及びソフトウェア）をいう。

(3) 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。

(4) 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。

(5) 機密性

情報にアクセスすることを認められた者だけが、その情報にアクセスできる状態を確保することをいう。

(6) 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。

(7) 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、その情報にアクセスできる状態を確保することをいう。

(8) 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。

## 3　対象とする脅威

議会は、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。

(1) 不正アクセス、コンピュータウイルス攻撃、サービス不能攻撃等のサイバー攻撃及び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業務の停止等
(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等
(5) 電力供給、水道供給、通信の途絶等のインフラの障害からの波及等

## 4　情報資産の範囲

この基本方針が対象とする情報資産は、次に掲げるとおりとする。

ただし、市長が議会事務局職員の使用に供する情報資産については、その取扱いはふじみ野市情報セキュリティポリシーに従うものとし、本方針の適用範囲外とする。

(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　議員等の遵守義務

議員、議会事務局職員及び部外受託者など（以下、「議員等」という。）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、関係法令及び情報セキュリティ基本方針を遵守しなければならない。

なお、議会事務局職員は、市長部局が管理する情報システムを利用して業務を行うことから、本基本方針に加えて、ふじみ野市情報セキュリティ基本方針、同対策基準、同実施手順及び関連規程を遵守する。

## 6　情報セキュリティ対策

議会は、上記３の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

議会の情報資産について、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) 情報システム全体の強靭性の向上

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。

(3) 物理的セキュリティ

サーバ、通信回線、議員等の使用する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、議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など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、情報セキュリティ基本方針の遵守状況の確認、業務委託を行う際のセキュリティ確保等について情報セキュリティ基本方針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。

(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。

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。

(8) 評価・見直し

情報セキュリティ基本方針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。情報セキュリティ基本方針の見直しが必要な場合は、適宜情報セキュリティ基本方針の見直しを行う。

## 7　情報セキュリティ監査及び自己点検の実施

情報セキュリティ基本方針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　情報セキュリティ基本方針の見直し

情報セキュリティ監査及び自己点検の結果において、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、情報セキュリティ基本方針を見直す。

## ９　情報セキュリティ対策基準の策定

議会は上記６から８までに規定する対策等を実施するために、必要に応じ、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の議会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。

## １０　情報セキュリティ実施手順の策定

議会は、情報セキュリティ対策基準に基づき、必要に応じ、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の議会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。

附　則

この基本方針は、令和８年４月１日から施行する。