門真市議会情報セキュリティ基本方針

1　目的

本基本方針は、門真市議会（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

⑴　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、その構成機器（ハードウェア及びソフトウェア）をいう。

⑵　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。

⑶　情報資産

業務遂行の過程で生み出される価値のあるものを言い、以下の切り口で抽出する。

ア　直接的情報資産：データベース、データファイル、手順書、監査証跡など

イ　ソフトウェア資産：業務用ソフトウェア、システムソフトウェア、開発用ツールなど

ウ　物理的情報資産：コンピュータ装置、通信装置、記録媒体など

エ　サービス資産：ユーティリティ（空調、電源、照明）など

オ　人的資産：資格、技能、経験など

カ　無形資産：組織の評判、イメージなど

⑷　電磁的記録媒体

情報通信システムでデータ等を記録するための磁気ディスク､磁気テープ、フロッピーディスク等をいう。

⑸　情報セキュリティ

情報資産の機密性及び完全性及び可用性を維持することをいう。

⑹　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。

⑺　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。

⑻　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。

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。

⑴　不正アクセス、ウィルス攻撃、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

⑵　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

⑶　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

⑷　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

⑸　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

⑴　機関の範囲

本基本方針が適用される機関は、議会及び議会事務局とする。

⑵　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。ただし、市長が定める「門真市情報セキュリティポリシー」が適用される情報資産を取り扱う場合は、本基本方針の適用範囲外とする。

①　議会の職務に関する事務に係る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　議会の職務に関する事務に係るネットワーク及び情報システムで取り扱う電子情報（これらを印刷した文書を含む。）

③　議会の職務に関する事務に係る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

⑶　議員等の範囲

本基本方針が適用される議員等の範囲は、議員並びに議会事務局の常勤職員及び非常勤職員（本基本方針において「議員等」という。）とする。

5　議員等の遵守義務

議員等は、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本基本方針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。

⑴　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ための体制を確立する。

⑵　物理的セキュリティ

サーバ、通信回線及び議員等の情報端末等の管理について、物理的な対策を講じる。

⑶　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等の人的な対策を講じる。

⑷　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。

⑸　運用

情報システムの監視、本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、本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、緊急事態の発生に備えた危機管理体制を講じる。

⑹　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、利用規約及びセキュリティに関する規程の確認等、必要な対策を講じる。

⑺　評価・見直し

本基本方針の遵守状況を検証するため、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。本基本方針の見直しが必要な場合は、適宜本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

本基本方針の遵守状況を検証するため、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　本基本方針の見直し

情報セキュリティ監査及び自己点検の結果、本基本方針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、本基本方針を見直す。

附　則

この方針は、令和８年４月1日から施行する。