松江市議会情報セキュリティ基本方針

1. 目的

本基本方針は、松江市議会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、松江市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

（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、その構成機器（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。

（3）情報資産：松江市議会が保有する情報資産で、以下のものをいう。
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

（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、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、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。

（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

本基本方針は、松江市議会が保有する情報資産について適用する。

5. 議員及び職員等の遵守義務

議員並びに議会事務局の職員及び会計年度任用職員は、情報セキュリティの重要性について共通の認識を持ち、職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

（1）上記3の脅威から情報資産を保護するため、松江市情報セキュリティ基本方針に準じ、情報セキュリティを推進する組織体制を確立するとともに、物理的セキュリティ、人的セキュリティ、技術的セキュリティを講じる。

（2）業務委託を行う場合には、委託業者を選定し、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。

7. 情報セキュリティ監査等の実施

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又は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又は自己点検の結果、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、本基本方針を見直す。

9. 情報セキュリティ対策基準及び実施手順の作成

上記6、7及び8に規定する対策等を実施するため、必要に応じて情報セキュリティ対策基準及び情報セキュリティ実施手順を策定する。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより本市議会の運営に重大な支障を及ぼすおそれがあることから原則非公開とする。

10. 附則

本基本方針は、令和８年４月１日から施行する。