愛西市議会情報セキュリティ基本方針

1　目的

本基本方針は、愛西市議会（以下「本市議会」という。）が保有し、又は管理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

本基本方針において使用する用語の意義は、次の各号に定めるところによる。

（１）情報

職務上作成し、又は取得した文書、図面、写真、電磁的記録その他の記録をいう。

（２）記録媒体

電磁的記録媒体及び紙媒体をいう。

（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、その構成機器（ハードウェア及びソフトウェア）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）情報資産

本市議会が保有し、又は管理する情報、情報システム、ネットワーク及びこれらに関する設備並びに記録媒体をいう。

（６）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。

（７）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。

（８）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。

（９）情報セキュリティポリシー

本市議会における情報資産の機密性、完全性及び可用性を維持するために定める基本方針及び対策基準その他の規程の総称をいう。

（１０）公文書

本市議会議員及び市議会事務局職員（以下「市議会議員等」という。）が職務上作成し、又は取得した文書、図面、フィルム、写真及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）であって、市議会議員等が組織的に用いるものとして、本市議会が保有しているものをいう。

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、重要情報の搾取、内部不正等

（2） 情報資産の無断持ち出し、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、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活動・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）組織の範囲

本基本方針が適用される組織は、本市議会及び本市議会事務局とする。

ただし、「愛西市情報セキュリティポリシー」で適用される情報資産を取扱う場合は、同ポリシーを遵守するものとする。

（2）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。

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器
情報システム	パソコン、モバイル端末、プリンター、オペレーションシステム、ソフトウェア等

ネットワーク・情報システムに関する施設・設備	電源ケーブル、通信ケーブル等
電磁的記録媒体	端末、通信回線装置等に内蔵される内蔵電磁式記録媒体、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体等
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等
公文書	市議会議員等が職務上作成し、又は取得した文書、図面、フィルム、写真及び電磁的記録

5　情報セキュリティ管理体制

本市議会における情報セキュリティ対策を総括するため、議長を情報セキュリティ責任者とし、必要な管理体制を整備するものとする。

6　市議会議員等の遵守義務

市議会議員等並びに本市議会の情報資産を取り扱う委託事業者その他本市議会の情報資産を取り扱う者は、情報セキュリティの重要性について共通の認識をもつとともに、活動及び業務の遂行にあたって関係法令等及び情報セキュリティ基本方針を遵守する義務を負うものとする。

7　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、以下の情報セキュリティ対策を講じる。

（１） 組織体制

本市議会の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立する。

（２） 情報資産の分類と管理

本市議会の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） 物理的セキュリティ対策

通信回線及び端末等への物理的な対策を講じる。

（４） 人的セキュリティ対策

情報セキュリティに関し、市議会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。

（５） 技術的セキュリティ対策

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、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の体制を整える。

（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、利用に係る規定を整備し対策を講じる。

（８） 評価・見直し

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。情報セキュリティポリシー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。

８　情報セキュリティインシデントへの対応

情報資産に対する不正アクセス、情報漏えいその他の情報セキュリティ侵害が発生し、又は発生するおそれがある場合には、速やかに報告し、被害の拡大防止及び原因の究明並びに再発防止のための措置を講じるものとする。

９　情報セキュリティ監査及び点検の実施

情報セキュリティポリシーが遵守されていることを検証するため、必要に応じて、議長の指示に基づき、議会運営委員会において情報セキュリティ監査及び点検を実施するものとする。

１０　情報セキュリティポリシーの見直し

情報セキュリティ監査及び点検の結果、情報セキュリティポリシーの見直しが必要に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、リスクを検討した上で、情報セキュリティポリシーを見直す。

１１　情報セキュリティ対策基準の策定

本基本方針に基づき、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。

付則

この基本方針は、令和８年４月１日から施行する。