

浅口市議会情報セキュリティ基本方針

1. 目的

本基本方針は、浅口市議会（以下「本市議会」という。）が保有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

(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。

(4) 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。

(5) 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。

(6) 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の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) 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、「浅口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、「浅口市情報セキュリティポリシー」を遵守するものとする。

(2) 情報資産の範囲

本市議会が保有又は管理するネットワーク、情報システム、及びこれらで取り扱うデータや文書を対象とする。

5. 遵守義務

本市議会議員及び議会事務局職員は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって本基本方針及び「浅口市議会タブレット端末等使用基準」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。

(1) 組織体制

議長を最高責任者とし、本市議会における情報セキュリティ対策を推進する体制を確立する。

(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

本市議会から貸与されている端末及び記録媒体等の管理について、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、本市議会議員及び議会事務局職員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

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、本基本方針や個別基準の遵守状況の確認、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備する。

(7) 業務委託と外部サービスの利用

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。

外部サービスを利用する場合には、利用にかかる規約等の確認を行う等の対策を講じる。

ソーシャルメディアサービスを利用する場合には、発信できる情報及び利用するサービスごとの責任者を定める。

(8) 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

本基本方針や個別基準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. 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、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、適宜本基本方針を見直す。

附則

本基本方針は、令和8年4月1日から施行する。