三原市議会情報セキュリティ基本方針

令和８年３月17日　制定

三原市議会情報セキュリティ基本方針　目次

三原市議会情報セキュリティ基本方針

1　目的

本基本方針は、三原市議会（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

(1)　電子計算機等

ハードウェア及びソフトウェアで構成するコンピュータ及び周辺機器（コンピュータに直接接続され一体として扱われるキーボード、マウス等をいう。）並びに電磁的記録媒体（電子的方式、磁気的方式その他人の知覚によっては認識できない方式で作られた記録を記録する媒体をいう。以下同じ。）をいう。

(2)　ネットワーク

電子計算機等を相互に接続するための通信網及びその接続に必要な機器（ソフトウェアを含む。）をいう。

(3)　情報システム

電子計算機等又は電子計算機等及びネットワークで構成され、情報処理を行う仕組みをいう。

(4)　情報

情報システムで取り扱う事務の執行に関する全てのデータをいう。

(5)　情報資産

情報システム及び情報をいう。

(6)　機密性

情報資産に接続することを認められた者のみが、情報資産に接続できる状態をいう。

(7)　完全性

情報資産が破壊、改ざん又は消去をされていない状態をいう。

(8)　可用性

必要なときに中断されることなく情報資産に接続できる状態をいう

(9)　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。

(10)　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

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からの

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、外部委託管理の不備、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、火災等の災害並びに事故、故障等によるサービス及び業務の停止

4　適用範囲

本基本方針が対象とする機関は、議会（職員、非常勤職員、嘱託職員及び臨時職員を除く。）とする。

5　議員の遵守義務

議会の情報資産に携わるすべての議員並びに受託事業者は、情報セキュリティの重要性について共通の認識を持ち、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6　情報セキュリティ対策

議会は、脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

(1)　組織体制

議会の保有する情報資産について、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ものとする。

(2)　情報資産の分類と管理

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行う。

(3)　物理的セキュリティ対策

情報システムを設置する施設への不正な立ち入りの防止や、パソコン等の機器及び電磁的記録媒体の適切な管理など、情報資産を損傷・妨害等から保護するために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する権限や責任を定め、議員に情報セキュリティポリシー及び情報セキュリティに関する法令等の内容を周知徹底する等、十分な研修及び啓発が講じられるように必要な対策を講ずる。

(5)　技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、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

各種対策の実施状況を確認するため、情報システムの監視、情報セキュリティポリシーの順守状況の確認、業務委託を行う際のセキュリティ確保などの運用面の対策を講じる。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、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・ソーシャルメディアサービス)の利用

業務委託を行う場合には、受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する等の必要な措置を講じる。また、外部サービス（クラウドサービス・ソーシャルメディアサービス）を利用する場合には、利用する際の留意事項を定め、周知する。

7　情報セキュリティ監査及び自己点検の実施

議会は、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する。

8　情報セキュリティポリシーの見直し

議会は、情報セキュリティ監査及び自己点検の実施による検証結果等を踏まえるとともに、情報セキュリティを取り巻く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のリスクを検討したうえで、情報セキュリティポリシー及び実施手順の見直しを適宜行い、都度議員に周知することとする。

9　情報セキュリティ対策基準の策定

議会は、上記６、７及び８に規定する対策など講じるに当たって、遵守すべき行為、判断等の基準を統一的に定めるため、必要となる基本的な要件を明記した対策基準を策定するものとする。

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、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情報セキュリティ実施手順を策定するものとする。