大垣市議会情報セキュリティポリシー

第1版　令和　8年　3月17日　策　定
令和　8年　4月　1日　施　行

大垣市議会

目次

第１章　情報セキュリティ基本方針

１　目　　的

本基本方針は、大垣市議会（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

本基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

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。

⑷ 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。

⑸ 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。

⑹ 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。

⑺ 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。

⑻ 情報セキュリティインシデント

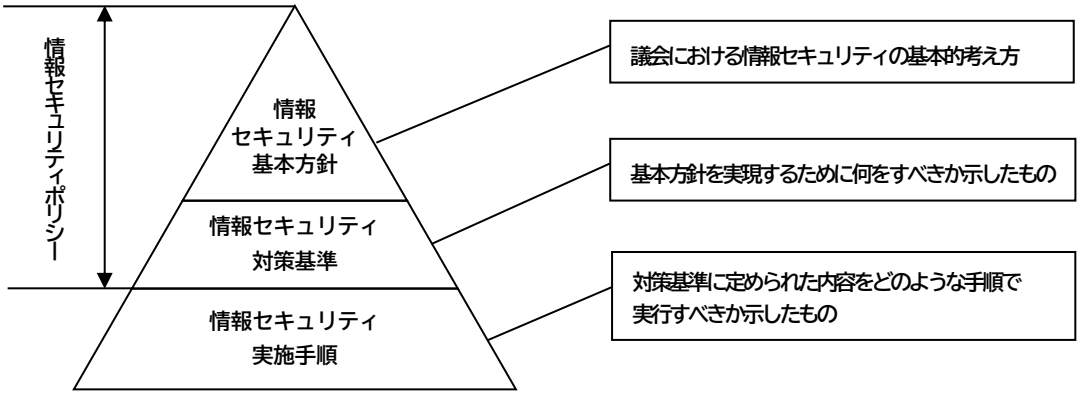
情報資産の管理上の脅威となる確率が高い現象や事案をいう。具体的には、ウイルス感染、第三者からの不正アクセス※による侵害、情報システム上の欠陥や誤動作による情報漏えい※及び議会の議員（以下、「議員」という）による情報紛失等がある。

３　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

４　情報セキュリティポリシーの構成

情報セキュリティポリシーの構成は、一定の普遍性を備えた「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する「情報セキュリティ対策基準」の二階層に分けて策定する。



５　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

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

(3) 地震、落雷、火災等の災害によるサービス及び議会活動の停止等

(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

６　適用範囲

(1) 適用機関

本基本方針は、議会に適用する。

(2) 情報資産の範囲

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 議員が議会活動において作成し、又は取得した文書等

情報資産の分類	情報資産の具体例
ネットワーク	通信回線、ルータ等の通信機器等
情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム※、ソフトウェア（ウェブアプリケーション※を含む。）、クラウドサービス※等
ネットワーク及び情報システムに関する設備	電源ケーブル、通信ケーブル等
記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵記録媒体、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記録媒体等
システム関連文書	仕様書、マニュアル、ネットワーク構成図等
議員が議会活動において作成し、又は取得した文書等	議会に関する書類、一覧のリスト、図画、写真等

７　議員の遵守義務

議員は、情報セキュリティの重要性について共通の認識を持ち、議会活動の遂行に当たって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。

８　情報セキュリティ対策

前記５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組織体制を確立する。

⑵ 情報資産の分類と管理

議会の保有する情報資産をその重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

⑶ 物理的セキュリティ

通信回線及び議員の端末等の管理について、物理的な対策を講じる。

⑷ 人的セキュリティ

情報セキュリティに関し、議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。

⑸ 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。

⑹ 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認等、情報セキュリティポリシー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、緊急時（インシデント）の対応を定める。

９　情報セキュリティ監査・自己点検の実施

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。

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自己点検の結果、情報セキュリティポリシーの見直しが必要な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、情報セキュリティポリシーの見直しを行う。

１１　情報セキュリティ対策基準の策定

前記８に規定する対策等を実施するために、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。

１２　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、ネットワーク及び情報システム並びにそれらに準ずるものの取扱いにおいて、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定めた情報セキュリティ実施手順を策定する。

１３　公開の範囲

情報セキュリティ対策基準、情報セキュリティ実施手順は、公にすることにより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非公開とする。

１４　法令等の遵守

情報セキュリティに関する法令・ガイドライン等を遵守する。

１５　問い合わせ先

大垣市議会事務局　電話　0584-47-8073