姶良市議会情報セキュリティポリシー

制定：令和8年3月19日

施行：令和8年4月1日

姶良市議会

目次

第１章　議会情報セキュリティ基本方針

１ 目的

本基本方針は、姶良市議会（以下「本市議会」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、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）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。

（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。

（8）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（9）無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

（10）議員

本市議会の議員をいう。

（11）職員等

議会事務局に所属する職員及び会計年度任用職員等をいう。

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

（1）対象者の範囲

本基本方針が適用される対象者は、議員及び議会事務局職員等とする。

（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。ただし、議員が公務ではなく議員個人の政治活動等を通じて取得した情報であって、本市議会が管理する情報システムに保存されていないものは対象外とする。

① 本市議会が管理する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 本市議会が管理する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 本市議会が提供・貸与する情報端末、及び本市議会のネットワークに接続して利用する私物端末（BYOD）
④ 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

5 議員及び職員等の遵守義務

議員及び職員等その他議会の業務に従事する者は、情報セキュリティの重要性を十分に認識し、本市議会の活動及び業務の遂行に当たり、この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。

議員及び職員等その他議会の業務に従事する者が「姶良市情報セキュリティポリシー」の適用対象となる情報資産を取り扱う場合には、当該情報資産については、同ポリシーを遵守するものとする。

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

本市の情報資産について、情報セキュリティ対策を推進する本市議会における組織体制を確立する。

（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、さらにクラウドサービス等の利用環境における脅威やリスクを検討したうえで、当該分類に基づき、適切な水準の情報セキュリティ対策を実施する。

（3）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し対策を講じる。

① 議員が使用する情報システムがインターネット空間のクラウドサービス等に配置される場合、取り扱う情報資産の重要度（機密性等）に応じて、多要素認証等の高い水準の認証方式を導入するなど、適切なセキュリティ対策を講じる。

（4）物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（5）人的セキュリティ

情報セキュリティに関し、議員及び議会事務局職員等が遵守すべき事項を定めるとともに、全員に対して十分な教育及び啓発を行う等の人的な対策を講じる。

（6）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。本市議会のネットワークやシステムに私物端末（BYOD）を接続させる場合は、他の情報システムと同水準のセキュリティ対策を講じるものとする。

（7）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、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、公費で購入し議員へ貸与する端末等については、原則として議会事務局が把握・管理できる範囲内で運用する。さらに、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、議員及び議会事務局職員等を含めた緊急時対応計画を策定する（市長部局と共通で策定する場合を含む）。

（8）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。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの 運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用する ソーシャルメディアサービスごとの責任者を定める。

（9）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ポリシーの見直しを行う。

7 情報セキュリティ監査及び自己点検の実施

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

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、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、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9 情報セキュリティ対策基準の策定

上記6、7及び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。

10 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、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ものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政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。