

宮崎市議会情報セキュリティポリシー

令和8年3月12日

宮崎市議会

目 次

宮崎市議会情報セキュリティポリシーについて.....	1
議会情報セキュリティ基本方針.....	2
1. 目的.....	2
2. 定義.....	2
3. 対象とする脅威.....	2
4. 情報資産の範囲.....	2
5. 議員等の遵守義務.....	2
6. 情報セキュリティ対策.....	3
7. 情報セキュリティ監査及び自己点検の実施.....	3
8. 情報セキュリティポリシーの見直し.....	3
9. タブレット端末、SIDE BOOKS及びLINE WORKS 実施手順書の策定.....	3

宮崎市議会情報セキュリティポリシーについて

宮崎市議会情報セキュリティポリシー（以下「情報セキュリティポリシーという。）とは、宮崎市議会が管理する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として、宮崎市議会における情報セキュリティ対策の頂点に位置するものであり、宮崎市議会が管理する情報資産に関する業務に携わる議員及び議会事務局職員（会計年度任用職員を含む。以下「議員等」という。）並びに委託事業者に対し、浸透・普及・定着させるべきものである。

情報セキュリティポリシーは、情報セキュリティ基本方針（一定の普遍性を備えた部分）と情報セキュリティ対策基準（情報資産を取り巻く状況の変化に依存する部分）により構成される。なお、本セキュリティポリシーを補完するため、宮崎市議会が議員等に貸与するタブレット端末、SIDE BOOKS及びLINE WORKSの利用及び運用に係る実施手順書を策定する。

情報セキュリティ対策基準及び当該実施手順書については、公にすることにより宮崎市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。

なお、宮崎市が保有する情報資産を議会事務局が使用する場合は、宮崎市情報セキュリティポリシーが適用される。

情報セキュリティ基本方針

1 目的

情報セキュリティ基本方針（以下「本基本方針」という。）は、宮崎市議会が保有する情報資産の機能性、完全性及び可用性を維持するため、宮崎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及びその構成機器（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な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 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。

- (1) 市議会が貸与するタブレット端末
- (2) SIDE BOOKS及びLINE WORKSで取り扱う情報（USB等の記憶媒体に保存した文書及び印刷した文書を含む。）
- (3) 議員等がSIDE BOOKS及びLINE WORKSを利用するために使用する全ての情報端末
- (4) 議事堂に整備されたWi-Fi

5 議員等の遵守義務

議員等は、情報セキュリティの重要性について共通の認識を持ち、業務遂行に当たっては、情報セキュリティポリシー並びにタブレット端末、SIDE BOOKS及びLINE WORKSの実施手順書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、次の情報セキュリティ対策を講じる。

(1)組織体制

宮崎市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。

(2)情報資産の分類と管理

宮崎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行う。

(3)情報システム全体の強靱性の向上

議会運営を支える情報システム及びネットワークについては、その特性に応じた適切な分離及び防御措置を講じるものとする。また、不正通信の監視体制を強化するとともに、継続的なセキュリティ評価（監査）を実施することで、情報セキュリティインシデントの未然防止及び早期発見に努めるものとする。

(4)物理的セキュリティ

議員等のタブレット端末等の管理について、MDM等により、紛失・盗難等を防止するための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ずる。

(6)技術的セキュリティ

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ずる。

(7)運用

情報セキュリティポリシーの遵守状況の確認、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ずるものとする。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切に対応するため、緊急時対応計画を策定する。

(8)業務委託とクラウドサービスの利用

業務委託を行う場合は、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するとともに、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ずる。

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、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や、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を見直す。

9 その他の事項

本情報セキュリティポリシーに定めのない事項又は解釈に疑義が生じた場合には、協議により解決を図るものとする。