# 四国中央市議会情報セキュリティ基本方針

令和８年３月　策定

四 国 中 央 市 議 会

## １　目的

本基本方針は、四国中央市議会（以下「本市議会」という。）における議会活動、議員活動及び議会事務局業務において取り扱う情報資産を適切に保護し、その機密性・完全性・可用性を確保することを目的とする。

特に、議員が私物端末や外部クラウドサービスを利用する機会が多いという議会特有のリスクを踏まえ、情報漏えい等の事故を防止するために必要な情報セキュリティ対策を定める。

なお、本基本方針は議員の自由な政治活動を不当に制限するものではなく、議会情報の適切な管理を目的とする。

## 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る情報処理の仕組みをいう。

（３）情報セキュリティ

情報資産の機密性・完全性・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

情報にアクセスを認められた者のみがアクセスできる状態をいう。

（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いう。

（７）可用性

情報にアクセスを認められた者が必要なときに中断なく利用できる状態をいう。

（８）議員端末

本市議会が貸与するタブレット端末等をいう。

（９）私物端末

議員が所有し、議会情報の閲覧・保存・送受信等に利用するスマートフォン、PC、タブレット等をいう。家族共有端末は含まない。

（１０）クラウドサービス

外部事業者が提供するオンラインサービスをいう（例:OneDrive、Google Drive、Dropbox 等)。

（１１）公開情報

議案、議事録、委員会資料等、公開を前提とした情報をいう。

（１２）限定公開情報

議員のみが閲覧できる情報（議会運営情報、調整資料、非公開会議資料等）をいう。

（１３）非公開情報

個人情報、行政機密情報、議会内部の非公開資料等、漏えいした場合に重大な影響を及ぼす情報をいう。

## ３　対象とする脅威

本市議会は、情報資産に対する脅威を以下のとおり整理し、必要な対策を講じる。

（１）技術的脅威（不正アクセス、ウイルス感染、ランサムウェア、サービス不能攻撃等）

（２）人的脅威（操作ミス、設定ミス、無断持ち出し、無許可ソフト利用、内部不正、家族等による誤使用）

（３）物理的脅威（盗難、紛失、覗き見、災害、設備故障）

（４）社会的脅威（大規模感染症等による要員不足、新たな攻撃手法の出現）

（５）外部サービス利用に伴う脅威（クラウドサービスや各種メディアを通じた情報漏えい、誤投稿、外部事業者の障害等）

## ４　適用範囲

（１）実施機関

本基本方針は、本市議会の議員及び議会事務局職員に適用する。ただし、議会事務局職員は市情報セキュリティポリシーに準ずる。

（２）情報資産

本基本方針の対象は以下の情報資産とする。

① 議員端末

② 私物端末で扱う場合の議会関連情報

③ 議会ネットワーク

④ 議会資料（紙・電子）

⑤ 議会中継・録画データ

⑥ クラウドサービス上の議会関連データ

⑦ SNS アカウントで扱う議会関連情報

## ５　議員等の遵守義務

議員等は以下を遵守する。

（１） 議員配付端末にパスコード・生体認証等を設定し、紛失時は 30 分以内に議会事務局へ報告する。

（２）私物端末で議会情報を扱う場合は、以下を必須とする。

① 画面ロック設定

② OS・アプリの最新化

③ 家族共有禁止

④ 非公開情報の保存禁止

（３）各種メディアで非公開情報・限定公開情報を発信しない。

（４）クラウドサービス利用時は、非公開情報を保存しない。

（５）情報漏えい等のインシデント発生時は速やかに議会事務局へ報告する。

（６）年１回の情報セキュリティ研修を受講する。

## ６　情報セキュリティ対策

本市議会は、情報資産を適切に保護するため、以下の対策を講じる。

（１）組織的対策

議長を情報セキュリティ最高責任者、議会事務局長を統括責任者とする。

（２）情報資産の分類と管理

公開情報・限定公開情報・非公開情報に分類し、分類に応じた管理基準を適用する。

（３）情報システムの強靭性確保

議会端末はインターネット接続系で運用し、不正通信監視、マルウェア対策、アクセス制御等を実施する。

（４）物理的セキュリティ

議会フロア等での端末施錠管理、覗き見防止、紙資料の適切な廃棄を徹底する。

（５）人的セキュリティ

議員及び議会事務局職員に対し、情報セキュリティ教育・研修を定期的に実施する。

（６）技術的セキュリティ

端末のウイルス対策ソフト導入、OS・アプリ更新、アクセスログ管理等を実施する。

（７）運用管理

インシデント発生時の初動手順、連絡体制、復旧手順を整備する。

（８）業務委託・外部サービス利用

委託契約には情報セキュリティ要件を明記し、委託先の管理状況を確認する。クラウドサービス利用時は利用基準に基づき適切に管理する。SNS 利用時は運用手順に従う。

（９）継続的改善

情報セキュリティ対策の有効性を定期的に評価し、必要に応じて改善する。

## ７　情報セキュリティ監査及び自己点検の実施

本市議会は、情報セキュリティポリシーの遵守状況を確認するため、年１回以上の自己点検を実施する。また、必要に応じて外部又は市内部の監査機関による情報セキュリティ監査を実施し、改善が必要な事項については速やかに是正措置を講じる。監査結果は議長及び議会運営委員会に報告し、必要に応じて議員へ周知する。

## ８　情報セキュリティポリシーの見直し

本市議会は、情報技術の進展、社会情勢の変化、新たな脅威の発生、監査結果等を踏まえ、情報セキュリティポリシーが現状に適合しているかを定期的に検証する。必要がある場合には、情報資産に係るリスクを分析し、適切な対策を追加・修正する形で見直しを行う。見直し後のポリシーは議長が決裁し、議員及び議会事務局に周知する。

## ９　情報セキュリティ対策基準の策定

本基本方針に基づき、情報資産の分類、アクセス管理、端末管理、クラウドサービス利用、SNS 利用、インシデント対応等に関する具体的な遵守事項及び判断基準を定めた「情報セキュリティ対策基準」を策定する。対策基準は、議会特有の運用実態を踏まえ、実効性のある内容とする。

## 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（インシデント発生時の初動、端末紛失時の対応、クラウド利用手順等）を定めた「情報セキュリティ実施手順」を策定する。実施手順は、公開することで本市議会の情報資産の保護に支障を及ぼすおそれがあるため非公開とする。ただし、議員が遵守すべき事項については、必要な範囲で周知する。