岐阜県議会情報セキュリティ基本方針

（目的）

第１条　岐阜県議会情報セキュリティ基本方針（以下「基本方針」という。）は、岐阜県議会（以下「議会」という。）が保有する情報資産に関して機密性、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。

なお、本基本方針は、地方自治法（昭和２２年法律第６７号）第２４４条の６に基づく方針とする。

（用語の定義）

第２条　基本方針において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（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(ハードウエ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

基本方針及び第９条に規定する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。

（対象とする脅威）

第３条　議会は、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

（適用範囲）

第４条

１　機関

基本方針が適用される機関の範囲は、議会（議会事務局は除く。）とする。

２　情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

（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電磁的記録媒体

（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

（議員等の遵守義務）

第５条　議員及び委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、情報セキュリティポリシーを遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条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

議会が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・管理するための組織体制を確立する。

（２）情報資産の分類と管理

議会が保有する情報資産を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。

（３）物理的セキュリティ

情報システム及びその設置場所等の管理について、物理的な対策を講じる。

（４）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必要な人的な対策を講じる。

（５）技術的セキュリティ

コンピュータの管理、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な対策を講じる。

（６）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行うものとする。また、情報資産への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、緊急時対応計画を策定する。

（７）業務委託と外部サービスの利用

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。

（８）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、実施結果に基づき運用を改善することで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。

（情報セキュリティ監査及び自己点検の実施）

第７条　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。

（情報セキュリティポリシーの見直し）

第８条　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。

（情報セキュリティ対策基準の策定）

第９条　この方針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（以下「対策基準」という。）を策定する。なお、情報セキュリティ対策基準は、公にすることにより本県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。

（情報セキュリティ対策実施手順の策定）

第１０条　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対策実施手順を策定するものとする。なお、情報セキュリティ対策実施手順は、公にすることにより本県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。

附 則

この方針は、令和８年４月１日から施行する。