岐阜市議会情報セキュリティ基本方針

（令和８年３月２６日
議会運営委員会決定）

（目的）

第１　この方針は、岐阜市議会（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。

（定義）

第２　この方針において、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。

(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)　情報資産　次に掲げるものをいう。

①　ネットワーク、情報システム、ネットワーク及び情報システムに関する設備並びに電磁的記録媒体

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

(4)　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。

(5)　情報セキュリティポリシー　この方針及び情報セキュリティ対策基準をいう。

(6)　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。

(7)　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。

(8)　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　情報資産に対する情報セキュリティ対策の実施に当たり、対象とする脅威は、次の各号に掲げるとおりとする。

(1)　サイバー攻撃（不正アクセス、ウイルス攻撃、サービス不能攻撃等をいう。）、部外者の侵入その他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、設計又は開発の不備、プログラム上の欠陥、操作又は設定の不備、メンテナンスの不備、監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障その他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、火災その他の災害による業務の停止等

(4)　重大な感染症のまん延等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、水道供給の途絶その他のインフラの障害からの波及等

（適用範囲）

第４　この方針の適用範囲は、次の各号に掲げる区分に応じ、当該各号に定めるとおりとする。

(1)　機関の範囲　この方針の適用を受ける機関は、議会とする。

(2)　情報資産の範囲　この方針の適用を受ける情報資産の範囲は、議会が管理する情報資産とする。ただし、議会事務局の常勤職員及び会計年度任用職員が、岐阜市情報セキュリティポリシーの適用を受ける情報資産を取り扱う場合については、岐阜市情報セキュリティポリシーを遵守するものとする。

（議員等の遵守義務）

第５　議員並びに議会事務局の常勤職員及び会計年度任用職員（以下「議員等」という。）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、業務の遂行に当たっては、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　第３に規定する脅威から情報資産を保護するために講じる情報セキュリティ対策は、次の各号に掲げる区分に応じ、当該各号に定めるとおりとする。

(1)　組織体制　議会の情報資産について、議会全体で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　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講じる。

(3)　物理的セキュリティ　サーバ、通信回線及び端末等の管理について、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、議員等が遵守すべき事項を定めるとともに、十分な周知啓発を行う等の人的な対策を講じる。

(5)　技術的セキュリティ　情報システムの管理、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その他の情報セキュリティポリシーの運用面における対策を講じる。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、緊急時対応体制を整備する。

(7)　業務委託等に伴う措置　業務委託、クラウドサービス及びソーシャルメディアサービスの利用に伴う措置は、次に掲げるとおりとする。

①　業務委託により、業務において議会が保有する情報資産を議員等以外の者に利用させる場合は、情報セキュリティポリシーと同等以上の水準での情報セキュリティを確保できるよう、契約等において必要な措置

を講じるものとする。

② 業務委託により、業務において議会が保有する情報資産を利用する議員等以外の者は、当該業務の範囲において情報セキュリティポリシーを遵守するものとする。

③ クラウドサービスを利用する場合は、利用に係る規定を整備し対策を講じるものとする。

④ ソーシャルメディアサービスを利用する場合は、運用手順、発信可能な情報及び利用するサービスごとの責任者を定めるものとする。

（情報セキュリティ監査及び自己点検の実施）

第７ 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ものとする。

（情報セキュリティポリシーの見直し）

第８ 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は、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）

第９ 第６、第７及び第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ものとする。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。