宮崎県議会情報セキュリティ基本方針

令和８年３月５日

１　目的

本基本方針は、本議会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) 議員用インターネット回線

議会が管理運用する議員専用のインターネット回線（Wi-Fi）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や紛失、無許可ソフトウェアの使用等の規定違反、操作・設定ミス、メンテナンス不備、内部監査機能の不備、外部委託管理の不備、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、火災等の災害並びに事故、電力供給及び通信回線の途絶等によるサービス及び業務の停止等

4　適用範囲

(1) 対象の範囲

本基本方針が適用される対象は、議会及び議会事務局とする。

ただし、知事部局が管理運用する情報システムの利用においては、知事部局の基本方針が適用される。

(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、知事部局が管理運用する情報システムの利用にかかる情報資産は、知事部局の基本方針が適用される。

ア　議会が管理運用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

イ　議会が管理運用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。）

ウ　議会が管理運用するネットワーク及び情報システムに係る全ての情報

5　議員等の遵守義務

議員（会派職員を含む）、事務局職員、非常勤職員、会計年度任用職員及び臨時的任用職員（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。

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

本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た重要性で分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 情報システムの強靭性の向上

議員用インターネット回線における不正通信の監視、適切な認証設定及び外部サービスにおける安全性確認等の必要な情報セキュリティ対策を講じる。

(4) 物理的セキュリティ

通信回線及び情報機器等の管理について、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する議員等の責務の明確化、研修及び啓発の実施など、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。

(7) 運用

ネットワーク等の監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保など、運用面の対策を講じる。また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講じる。

(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）については、取り扱う情報の重要性分類に基づき契約や運用における対策を講じる。

外部サービス（クラウドサービス）を利用する場合には、知事部局（デジタル推進課）の規程を準用する。

ソーシャルメディアサービスを利用する場合には、知事部局（秘書広報課広報戦略室）のガイドラインを準用する。

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、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評価及び見直し

情報セキュリティ監査及び自己点検の結果により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く

状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

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のうち、公にすることにより本議会の運営に重大な支障を及ぼすおそれがあるものについては非公開とする。

附　則

この基本方針は、令和８年４月１日から施行する。