八女市議会
情報セキュリティポリシー

≪基本方針≫

令和８年４月１日施行

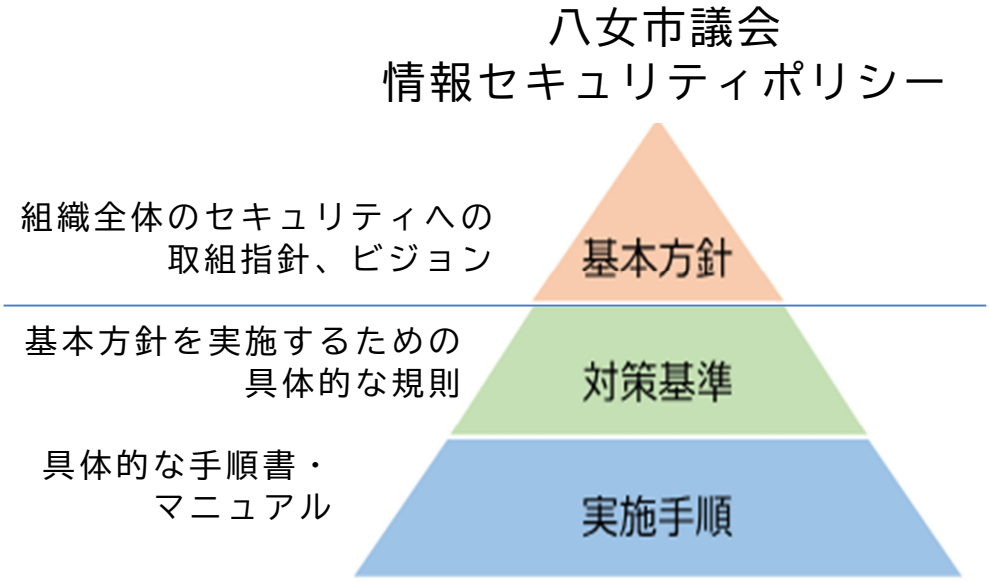
■情報セキュリティポリシーとは

組織において実施する情報セキュリティ対策の方針や行動指針のことである。

現在、情報通信技術の発展や高速インターネットへのアクセスが利用しやすくなったことにより、いつでもどこでもインターネットが利用できる環境が進み、生活のデジタル化も加速しつつある。

情報通信技術の発展が進む一方で、不正アクセスやコンピュータウイルス等によるデータの破壊や改ざん、情報漏えい、さらには災害や事故等さまざまなセキュリティ脅威に対処する対策の必要性が一層高まっている。

そこで、このような脅威から議会が保有する情報資産を組織として守るために、対策の方針や規定等を「八女市議会情報セキュリティポリシー」として定め、自ら取り組んでいくこととする。



八女市議会情報セキュリティポリシー

≪基本方針≫

１　目的

この基本方針は、八女市議会（以下、「市議会」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、市議会が実施する情報セキュリティ対策の基本的な事項を定めることを目的とする。特に、市議会で導入しているタブレット端末等及び関連アプリケーションの適正な利用を通じ、円滑な議会運営とセキュリティ確保の両立を図るものとする。

２　定義

八女市議会情報セキュリティポリシーにおける用語の定義は、次の各号に定めるところによる。

（１）情報資産

議会活動に伴い作成、取得又は保有する情報（電磁的記録を含む。）及びこれらを処理するための情報システムをいう。

（２）ネットワーク

タブレット端末等電子機器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。

（３）議会タブレット端末及びアプリケーションサービス

市議会が貸与するタブレット端末及び議会活動等で使用するアプリケーションサービス（管理者が許可したアプリケーションサービス等）やソフトウェアをいう。

（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

基本方針及び基本方針に基づいた情報セキュリティ対策基準及び実施手順等をいう。

（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。

（９）ＢＹＯＤ（Ｂｒｉｎｇ　Ｙｏｕｒ　Ｏｗｎ　Ｄｅｖｉｃｅ）

個人所有のスマートフォン端末等を議会活動や業務に利用する形態のことをいう。

３　対象とする脅威

議会タブレット端末、アプリケーションサービス及び外部サービス（インターネット経由によるサービスを含む）の利用特性を踏まえ、以下の脅威を重点的な対策の対象とする。

（１）不正アクセス、ウイルス攻撃、偽サイトへの誘導による認証情報の詐取、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・内部不正等

（２）情報資産の無断持ち出し、無許可アプリケーションサービスやソフトウェアの使用等の規定違反、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）議会タブレット端末本体の紛失や盗難による端末内データの流出及び不正利用

４　適用範囲

（１）使用者の範囲

議会タブレット端末及びアプリケーションサービスを使用することができる者は、八女市議会議員及び八女市職員（以下「使用者」という。）とし、本情報セキュリティポリシーは、議会タブレット端末及びアプリケーションサービスを使用する全ての者に適用する。

（２）情報資産の範囲

議会タブレット端末及びアプリケーションサービスで取り扱う全ての情報を範囲とする。

５　使用者の遵守義務

使用者は、情報セキュリティの重要性について共通の認識を持ち、議会タブレット端末及び情報資産を扱う際には、本情報セキュリティポリシー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、以下の対策を講じるものとする。

（１）組織体制の確立

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・管理

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実施する。

（３）物理的セキュリティ

議会タブレット端末及び通信回線について、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、使用者が遵守すべき事項を定めるとともに、十分な啓発及び教育を行う等の人的な対策を講じる。

（５）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策及び不正アクセス対策等の技術的対策を講じる。

（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講じるものとする。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（インターネット経由でのサービスを含む）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、利用にかかる規定を整備し対策を講じる。

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。

９　情報セキュリティ対策基準・実施手順の策定

上記６、７及び８に規定する対策等を実施するために、別途「対策基準・実施手順」等として定めるものとする。