真庭市議会情報セキュリティ基本方針

１．目的

本基本方針は、本市議会が保有、管理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、本市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。

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、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サービス及び業務の停止等

（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

４．適用範囲

（1） 対象範囲

本基本方針は、本市議会が保有する情報資産の利用者（以下「利用者」という。）に適用する。

なお、議会事務局職員については、原則として市長部局が策定する情報セキュリティポリシーの適用を受けるものとする。

ただし、議会固有の業務に従事し、議会が整備するネットワークや情報システム等を利用する場合には、本基本方針の適用対象とする。

（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。

ア 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 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 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

５．利用者の遵守事項

利用者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たり、以下の事項を遵守しなければならない。

・個人情報及び機密情報を適切に取り扱うこと
・議会タブレット端末等（議長が議員又は議会事務局職員に貸与するタブレット端末及び真庭市議会会議規則第 157 条の２の規定に基づき議長が許可した情報通信端末機器をいう。以下同じ。）を適切に管理すること
・議会が整備したネットワーク及びシステムには、上記端末のみを接続すること
・生成 AI などの技術を利用する際は、個人情報や機密情報を入力せず、出力内容の正確性を確認すること

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

本市議会における情報セキュリティ対策の最高責任者（CISO）を議長とし、実務責任者を議会事務局長とする。情報資産の分類と管理

（２） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、不正通信の監視機能の強化等の高度な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等及びの管理については、真庭市議会タブレット端末の使用等に関する規程（平成 30 年議会訓令第２号）に準ずる。

（４） 人的セキュリティ

情報セキュリティに関し、利用者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、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に当たっては、市長部局の情報セキュリティ統括部門（CSIRT）と協議し、その確認を受けた上で必要な対策を講じる。また、情報資産に対するセキュリティ侵害等の緊急事態が発生した場合には、市長部局の最高情報セキュリティ責任者（CISO）に直ちに報告し、関連部局と連携・協力のうえ、市長部局が定める緊急時対応計画に則り迅速かつ適切な対応を行うものとする。

（7） 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）を利用する場合には、真庭市の定める情報セキュリティ対策基準に準じて対策を講じる。

ソーシャルメディアサービスを利用する場合には、情報セキュリティの重要性を十分に認識し、許可されていない議会情報、個人情報、機密情報などを発信しないこと。

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。

令和８年４月１日

真庭市議会　議長　長尾　修