日南市議会情報セキュリティ対策基本方針

1　目的

本基本方針は、本市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、本市議会が独自に構築・運用する情報システム及びネットワーク、並びにこれらで扱う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、市から貸与されているパソコン等の端末及び接続するネットワークについては、市と市議会による共同策定の情報セキュリティ対策基本方針に準拠することとする。

2　定義

（1）　議会ネットワーク

議会活動及び事務の円滑な遂行を目的として、本市議会が独自に管理するインターネット接続環境をいう。

（2）　クラウドサービス

インターネットを通じて提供される外部サービスをいう（ペーパーレス会議システム、議会中継システム、その他将来的に導入される議会活動に資するサービスを含む)。

（3）　端末管理システム（MDM）

ネットワークに接続する端末の設定、利用制限、及び盗難・紛失時の遠隔消去等を一元的に管理する仕組みをいう。

（4）　情報資産

議会ネットワーク及び情報システムで取り扱うデータ、システム関連文書等をいう。

（5）　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。

（6）　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。

（7）　機密性

許可さ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。

（8）　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。

（9）　可用性

許可された者が、必要な時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。

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） 行政機関の範囲

議会ネットワークを利用する全ての議員、議会事務局職員、及び議会運営に関わる市職員とする。

（２） 情報資産の範囲

議会が管理するネットワーク、情報システム（タブレット端末等を含む）、及びこれらで取り扱うデータや文書とする。

5　議員等の遵守義務

本市議会の情報資産に接する全ての議員及び職員（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本基本方針を遵守しなければならない。

6　情報セキュリティ対策

議会ネットワーク及びクラウドサービスを安全に利用するため、以下の対策を講じる。

（１） 組織体制

情報セキュリティ対策を推進する組織体制を確立する。

① 最高情報セキュリティ責任者（ＣＩＳＯ：Chief Information Security Officer、以下「ＣＩＳＯ」という。）

（ア）議長をＣＩＳＯとする。ＣＩＳＯは、本市議会における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（イ）ＣＩＳＯは、本基本方針に定められた自らの担務を、情報セキュリティ責任者その他の本基本方針に定める責任者に担わせることができる。

② 情報セキュリティ責任者

（ア）議会事務局長をＣＩＳＯ直属の情報セキュリティ責任者とする。情報セキュリティ責任者は、ＣＩＳＯを補佐しなければならない。

（イ）情報セキュリティ責任者は、本市議会の情報セキュリティ対策、全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 情報セキュリティ・システム管理者

（ア）議会事務局次長を情報セキュリティ・システム管理者とする。

（イ）情報セキュリティ・システム管理者は、市議会の情報セキュリティ対策に関する権限及び

責任を有する。

（ウ）情報セキュリティ・システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

④　情報システム担当者

情報セキュリティ・システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

（２）　情報資産の分類と管理

本市議会が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

端末、サーバ、通信回線等について、物理的な対策を講じる。

（４）　人的セキュリティ

①　情報セキュリティに関し、本基本方針等を遵守し、必要な教育及び啓発を行う。

②　支給以外のパソコン、モバイル端末及び電磁的記録媒体等を議会ネットワークへ接続する場合は、情報セキュリティ責任者へ申請し許可を得なくてはならない。

（５）　技術的セキュリティ

ＭＤＭ（端末管理システム）による一元管理、アクセス制御、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（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、利用にかか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、定期的また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、運用改善を行い、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。

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、定期的また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、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は、公にすることにより本市議会の議会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。