上田市議会情報セキュリティ基本方針

１　目的

上田市議会は、議会活動等で得た行政情報や議会運営上重要な情報を多数保有し、取り扱っている。保有する情報資産を紛失、盗難、不正使用、破壊等の脅威から防御することは、市民の権利、利益を守るためにも、また、議会の安定的、継続的な運営のためにも必要不可欠である。

上田市議会情報セキュリティ基本方針（以下「基本方針」という。）は、地方自治法の一部を改正する法律（令和６年法律第６５号）による改正後の地方自治法第２４４条の６第１項で定めるサイバーセキュリティを確保するための方針に位置付けるものであり、議会が保有する情報資産を守るため、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) 機密性

情報を利用することを認められた者だけが、情報を利用できる状態を確保することをいう。

(5) 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。

(6) 可用性

情報を利用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、情報を利用できる状態を確保することをいう。

(7) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

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　適用の範囲

(1) 行政機関の範囲

基本方針が適用される行政機関は、保有する情報を取り扱う議会及び議会事務局とする。

(2) 情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

① 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
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

５　遵守義務

議員及び事務局職員（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基本方針及び「上田市議会タブレット端末運用基準」、「上田市議会議員ソーシャルメディア運用ガイドライン（以下「ガイドライン」という。」等の議会で策定した基準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

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、完全性及び可用性を踏まえて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ、情報システム室、通信回線及び議員等のパソコン等の管理について、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、基本方針や議会で策定した基準の遵守状況の確認、業務委託を行う際のセキュリティ確保等、運用面の対策を講じるものとする。また、情報資産に対する脅威が発生した場合に迅速かつ適切に対応するため、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、ガイドラインを遵守し、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

基本方針や議会で策定した基準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し、運用改善を行い、情報セキュリティの向上を図るとともに、見直しが必要な場合は、適宜見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

基本方針や議会で策定した基準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　基本方針等の見直し

情報セキュリティ監査及び自己点検の結果、基本方針や議会で策定した基準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、基本方針や議会で策定した基準を見直す。

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必要に応じて策定する。

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必要に応じて策定する。

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。