春日市議会におけるサイバーセキュリティを確保するための方針

第１章 総則

（目的）

第１条　本方針は、地方自治法第 244 条の 6 に基づき、議会が管理する情報システムの利用に当たってのサイバーセキュリティの確保を図ることを目的とするとともに、巧妙化かつ深刻化するサイバー攻撃の脅威に対し、情報資産の機密性、完全性及び可用性を確保することで、議会活動の円滑な運営に資する強靭性の向上を目指す。

（定義）

第２条　本方針における用語の定義は、次に掲げるものとする。

(1)　情報資産　行政文書(春日市情報公開条例(平成 12 年条例第 40 号)第 2 条第 2 号に規定する行政文書をいう。以下同じ。)及び行政文書に記録された情報並びに行政文書を作成し、及び行政文書に記録された情報を処理するための情報システム及びその関連機器をいう。

(2)　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及びその構成機器(ハードウェア及びソフトウェア)をいう。

(3)　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。

(4)　サイバーセキュリティ　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)　サイバーセキュリティポリシー　この方針及び春日市議会サイバーセキュリティ対策基準（以下「サイバーセキュリティ対策基準」という。)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に限り、当該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、改ざん又は消去を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当該情報にアクセスできる状態を確保することをいう。

（対象とする脅威）

第３条　本方針は、情報資産の機密性、完全性又は可用性に影響を及ぼすサイバー攻撃及びそれに起因する脅威を対象とする。これには、外部からのサイバー攻撃（標的型攻撃、不正プログラムの感染等をいう。)、内部不正、情報漏えい等が含まれる。

（適用範囲）

第４条　本方針は、春日市議会を構成する議員、議会事務局の職員その他議会が管理する情報資産を利用するすべての者（会計年度任用職員、業務委託先の従業者等を含む。）を適用範囲とする。

２　本方針は、次に掲げる議会が管理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を適用範囲とする。

(1)　議員に議案等を提供するために議会が運用するクラウドシステム

(2)　議会に係る手続のオンライン化システム

(3)　議員向けに提供される議会棟内の Wi-Fi 等の通信回線及び通信回線装置
(4)　議会等が管理するネットワークに接続される議員の私物端末

（職員等の遵守義務）
第５条　適用されるすべての議員及び職員等は、本方針、これに基づき策定されるサイバーセキュリティ対策基準及び実施手順を遵守しなければならない。また、サイバーセキュリティ意識の向上に努め、情報資産を議員活動を含む業務以外の目的で使用してはならない。

第２章 サイバーセキュリティ対策の実施

（組織体制の確立、情報資産の分類・管理、セキュリティ対策）
第６条　議会は、サイバーセキュリティ対策を確実に実施するため、一元的な組織体制を整備し、必要な措置を講じる。
(1)　組織体制の確立は次に掲げるものとする。
ア　最高サイバーセキュリティ責任者（CISO）を設置し、サイバーセキュリティ対策の推進に関する役割、権限及び責任を明確化する。
イ　サイバーセキュリティインシデント（侵害）に対処するため、緊急時対応体制（CSIRT）を整備し、迅速な被害の拡大防止及び復旧に努める。
(2)　情報資産の分類・管理は次に掲げるものとする。
ア　議会が保有する情報資産を、その機密性、完全性、可用性の観点から分類する。
イ　情報資産の分類に応じた取扱いを定め、情報資産のライフサイクルの全段階を通じて適切な管理を行う。
(3)　サイバーセキュリティ対策の実施
議会は、次に掲げる分野において、サイバーセキュリティ対策基準を定め、必要な対策を講じる。
ア　人的セキュリティ対策　議員及び職員に対し、サイバーセキュリティポリシーの遵守やセキュリティ意識向上を図るための定期的な研修及び訓練（緊急時対応訓練を含む。）を実施する。
イ　技術的セキュリティ対策　コンピュータ及びネットワークの管理、不正プログラム対策（ランサムウェア等）、不正アクセス対策（内部の不正、標的型攻撃等）、アクセス制御を講じる。セキュリティ情報を収集し、脆弱性のある箇所を突かれないよう、最新の対策を適用する。
ウ　運用管理対策　サイバーセキュリティポリシーの遵守状況を確認する。インシデント発生時は、総務省等の関係機関へ報告する。
エ　業務委託・外部サービス対策　業務を外部に委託する場合、又はクラウドサービス等の外部サービスを利用する場合は、委託先や外部サービスの特性とリスクを十分に評価し、セキュリティ要件を契約条件に明記する。
(4)　対策基準及び実施手順の策定
本方針に基づき、本方針を実践するための具体的な規則として「サイバーセキュリティ対策基準」及び具体的な手順書として「実施手順」を策定することとする。

第３章 評価及び見直し

（サイバーセキュリティ監査・自己点検の実施）
第７条　サイバーセキュリティ対策の実効性を評価するため、被監査部門から独立した監査人による客

観的な監査、又は自己点検を定期的に実施する。監査や自己点検の結果は、サイバーセキュリティポリシーの見直しに反映させる。

（サイバーセキュリティポリシーの見直し）
第８条　本方針、サイバーセキュリティ対策基準及び関係規定等について、サイバーセキュリティに関する環境の変化が発生した場合等、必要に応じ評価を行い、見直し、改善を行う。

（公表）
第９条　本方針を策定又は変更した際は、速やかに公表する。