

知立市議会情報セキュリティポリシー

知立市議会

令和8年4月1日策定

<目次>

第1章 議会情報セキュリティ基本方針

1 目的	2
2 定義	2
3 対象とする脅威	3
4 適用範囲	3
5 議員等の遵守義務	4
6 情報セキュリティ対策	4
7 情報セキュリティに関する自己点検の実施	5
8 議会情報セキュリティポリシーの見直し	5
9 議会情報セキュリティ対策基準の策定	5
10 議会情報セキュリティ実施手順の策定	5
11 違反等に対する対応	6
12 準用規定	6

序 議会情報セキュリティポリシーの構成

議会情報セキュリティポリシーとは、議会が取り扱う情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的にとりまとめたものを総称する。併せて、市の情報セキュリティポリシーとの整合を図りつつ、議会の特性を踏まえた情報の取扱いに関する基本的な考えを示すものである。

議会情報セキュリティポリシーについては、一定の普遍性を備えた部分『基本方針』と情報資産を取り巻く状況の変化に依存する部分『対策基準』に分けて策定することとした。具体的には、第1章に定める『議会情報セキュリティ基本方針』及び、第2章に規定する『議会情報セキュリティ対策基準』の2階層に分けることとする。また、議会情報セキュリティポリシーに基づき、具体的な情報セキュリティ対策の実施手順として『議会情報セキュリティ実施手順』を策定することとする。

なお、本ポリシー（基本方針）は、地方自治法第244条の6第1項に規定する「地方公共団体におけるサイバーセキュリティを確保するための方針」に位置付けることとし、同第2項の規定により、これを公表するものとする。

情報セキュリティの構成

文書名		内容
議会情報セキュリティポリシー	第1章 議会情報セキュリティ基本方針	情報セキュリティ対策に関する統一かつ基本的な方針
	第2章 議会情報セキュリティ対策基準	議会情報セキュリティ基本方針を実行に移すための情報セキュリティ対策の基準
議会情報セキュリティ実施手順		議会情報セキュリティ対策基準に基づいた具体的な実施手順

第1章 議会情報セキュリティ基本方針

1 目的

この基本方針は、知立市議会（以下「議会」という。）が保有し、又は議会活動において取り扱う情報資産を、議員及び議会事務局職員（以下「議員等」という。）が適切に管理するための基本的な事項を定めることにより、円滑な議会運営を維持し、議会に対する市民の信頼を確保することを目的とする。

2 定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(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

情報を処理するためのハードウェア、ソフトウェア、ネットワーク、クラウドサービス等の一体的な仕組みをいう。

(3) 情報資産

議会事務局の事務及び議員の公務としての職務に関連して取得、作成又は保有する情報（電磁的記録及び紙媒体）並びにこれらを取り扱うための情報システムをいう。

(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。

ア 機密性：情報資産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。

イ 完全性：情報資産が破壊、改ざん又は消去されていない状態を確保すること。

ウ 可用性：情報資産にアクセスすることを認められた者が、必要など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。

(5) 議会情報セキュリティポリシー

議会情報セキュリティ基本方針及び議会情報セキュリティ対策基準をいう。

(6) インターネット接続系

インターネットメール、ホームページ管理システム等インターネットに接続された情報システム

及びその情報システムで取り扱うデータをいう。

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、業務委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な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

この基本方針の適用範囲については、次のとおりとする。

(1) 人的範囲

- ア 全ての議員
- イ 議会事務局職員（以下「事務局職員」という。）

(2) 情報資産の範囲

- ア ネットワーク、情報システム及びこれらに関する設備
- 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システム関連文書

(3) 物的範囲

- ア 議会が管理し、議員に貸与するタブレット端末
- イ 議会が管理し、各会派等に配布するコンピュータ
- ウ ア及びイに使用する電磁的記録媒体
- エ アからウの利用に際して使用する周辺機器

(4) 事務局職員に対する適用

事務局職員については、知立市情報セキュリティポリシー（以下「市ポリシー」という。）を適用することを原則とする。ただし、市ポリシーに定めのない事項については、本方針を適用する。

5 議員等の遵守義務

議員等は、情報セキュリティの重要性について共通の認識を持ち、公務の遂行に当たって本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に、以下の情報セキュリティ対策を講じるものとする。

(1) 組織・体制の連携

本市の最高情報セキュリティ責任者（CISO）及びインシデント対応チーム（CSIRT）と連携し、議会事務局を通じて迅速な情報共有を行う体制を確立する。

(2) 情報資産の分類と管理

議会等が取り扱う情報資産の重要度に応じ、機密性、完全性及び可用性の観点から分類するとともに、適切な管理を行う。

(3) 物理的セキュリティ

情報資産を取り扱う端末や電磁的記録媒体の管理について、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な対策を講じる。

(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に、その被害の拡大を防止し、迅速な復旧を図るため、市のインシデント対応チーム（CSIRT）と連携し、被害拡大の防止、原因特定、および復旧に向けた措置を講じる。

(7) 業務委託及び外部サービス(クラウドサービス)等の利用

① 業務委託

業務委託を行う場合には、委託内容に応じて情報セキュリティ上十分な管理体制を有する事業者を選定し、情報セキュリティ要件を明記した契約を締結する。また、委託期間中においては、委託事業者(再委託事業者を含む。)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定期的を確認し、必要に応じて契約に基づき是正等の措置を講じる。

② 外部サービス(クラウドサービス)

外部サービス(クラウドサービス)を利用する場合には、利用に係る規定を整備し、情報の格付や取扱制限に応じたリスク評価を行い、適切な情報セキュリティ対策を講じる。

③ ソーシャルメディアサービス等の利用

ソーシャルメディアサービスその他の情報発信手段により外部に発信する場合においては、非公開情報、個人情報及び機密性を有する情報などの取扱いに十分留意し、議会の信用を損なう行為を行わないよう努めるものとする。

7 情報セキュリティ自己点検の実施

情報セキュリティ対策が適切に運用されているかを検証するため、定期的又は必要に応じて情報セキュリティ自己点検を実施する。

8 議会情報セキュリティポリシーの見直し

(1) 本ポリシーについて、定期的又は必要に応じて見直しを行うものとする。

(2) 見直しにあたっては、保有する情報資産に係るリスクを評価・検討した上で、その要否及び内容を判断する。

9 議会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議会情報セキュリティ対策基準(以下「議会对策基準」という。)を策定する。

10 議会情報セキュリティ実施手順の策定

(1) 議会情報セキュリティ実施手順(以下「議会実施手順」という。)は、議会对策基準に基づき、議員等が公務において情報セキュリティ対策を実行するための具体的な手順を定めたマニュアルであり、議会において策定するものとする。

(2) 議会実施手順は、必要に応じて柔軟に見直しを行う。

(3) 議会実施手順は、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。

11 違反等に対する対応

議会は、本ポリシーに反するおそれのある行為又は情報セキュリティ上不適切な取扱いが確認された場合には、事実関係を確認の上、必要に応じて議会として適切な対応を行うものとする。なお、事務局職員においては、市ポリシーに規定する処分の対象とする。

12 準用規定

本ポリシーに定めのない事項については、市ポリシーを準用する。