

## 春日井市議会情報セキュリティ基本方針

地方自治法（昭和 22 年法律第 67 号）第 244 条の 6 第 1 項に規定するサイバーセキュリティを確保するための方針として、春日井市議会情報セキュリティ基本方針（以下「基本方針」という）を定める。

### 1. 目的

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) 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。

#### (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。

#### (7) インターネット接続系

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、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

##### (1) 組織の範囲

基本方針が適用される組織は、本市議会とする。

##### (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。ただし、「春日井市情報セキュリティポリシー」で適用される情報資産を取り扱う場合は、その取り扱いは「春日井市情報セキュリティポリシー」に従うものとし、基本方針の適用除外とする。

- 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. 議員等の遵守義務

議員並びに議会事務局に属する職員及び再任用職員、会計年度任用職員等（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

本市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ための体

制を確立する。

(2) 情報資産の分類と管理

本市議会の保有する情報資産を重要性に応じて分類し、それに応じた情報セキュリティ対策を実施する。

(3) 情報システム全体の強靱性の向上

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、情報システム全体に対し、必要に応じたセキュリティ対策を講じる。

(4) 物理的セキュリティ

通信回線及び端末等の管理について、物理的な対策を講じる。

(5) 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、周知啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、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。

(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、利用に係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で発信できる情報を規定する等、運用手順を定める。

(8) 評価・見直し

基本方針の遵守状況を検証するため、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。基本方針の見直しが必要な場合は、適宜基本方針の見直しを行う。

7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティが確保されていることを検証するため、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、情報セキュリティを確保するための対策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、基本方針を見直す。