

# 桶川市議会情報セキュリティ基本方針

## 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

この方針において使用する用語の意義は、次のとおりとする。

### (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。

### (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) 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。

### (5) 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。

### (6) 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。

### (7) 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。

### 3 対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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又は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又は機器故障等の非意図的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) 対象範囲

次に掲げる者（以下「議員等」という。）に適用する。

ア 桶川市議会議員

イ 桶川市議会事務局設置条例（昭和34年桶川市条例第5号）に規定する事務局に所属する職員（会計年度任用職員、臨時的任用職員等を含む。）

ウ その他議会の情報資産を取り扱う者で議長が認めた者

## (2) 情報資産の範囲

本基本方針の対象とする情報資産は、次のとおりとする。ただし、桶川市が管理運営する情報資産は除くものとする。

- ア 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
- 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、ネットワーク図等のシステム関連文書
- エ 議会活動に関連する情報資産を取り扱うために使用される情報機器であって、議会事務局が貸与するもの及び議員が私的に所有するもの

## 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つとともに、業務の遂行に当たっては情報セキュリティポリシー及び情報セキュリティ実施手順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に規定する脅威から情報資産を保護するために、次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組織体制を確立する。

### (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

サーバ、情報システム室、通信回線、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、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とともに、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、外部サービス（クラウドサービス）等の利用

ア 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するとともに、必要に応じて契約に基づき措置を講じる。

イ 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。

ウ 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、定期的又は

必要に応じて情報セキュリティ監査又は自己点検を実施して運用改善を行うことにより情報セキュリティの向上を図るとともに、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 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又は自己点検の結果、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又は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、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进行分析し、リスクを検討した上で見直しを行う。

#### 9 情報セキュリティ対策基準の策定

上記6から8まで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。当該情報セキュリティ対策基準及び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。

### 附 則

この方針は、令和 8 年 4 月 1 日から施行する。