京都市会情報セキュリティ基本方針

1　目的

本基本方針は、本市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

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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、以下の脅威を想定し、情報セキュリティ対策を実施する。

⑴　不正アクセス、ウイルス攻撃、サービス不能攻撃などのサイバー攻撃や部外者の侵入など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

⑵　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

⑶　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

⑷　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

⑸　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

⑴　適用範囲

本基本方針が適用される範囲は、本市会の議員及び補助職員、並びに市会事務局職員（会計年度任用職員を含む。）（以下「議員等」という。）とする。

⑵　情報資産の範囲

本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　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、業務の遂行に当たって本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。

なお、その対策等については、必要に応じて、京都市情報セキュリティ対策基準、京都市情報セキュリティ緊急時対応計画等を参考に行う。

⑴　組織体制

本市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。

最高情報セキュリティ責任者（ＣＩＳＯ）を置き、本市会の情報セキュリティ対策に関する最終的な責任を負う。

ＣＩＳＯを議長とし、情報セキュリティ対策の推進の状況を継続的に監理する情報セキュリティ監理者を市会事務局長、ＣＩＳＯを補佐する情報セキュリティ統括者を市会事務局次長、情報セキュリティ統括者を補佐する情報セキュリティ管理責任者を市会事務局総務課長、情報システムの構築及び運用に係る業務を主管する情報システム管理者並びに情報セキュリティを確保する情報セキュリティ管理者を市会事務局各課長とする。

⑵　情報資産の分類と管理

本市会の保有する情報資産を、機密性、完全性及び可用性を考慮したうえで、重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。また、電子計算機等の情報資産は、取り扱う電子情報等の重要性に基づき分類するものとし、重要性が異なる複数の電子情報等を取り扱う場合は、最高位の重要性の分類に基づくものとする。

⑶　物理的セキュリティ

サーバ、管理区域、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。

⑷　人的セキュリティ

情報セキュリティに関し、十分な周知及び啓発を行うことで人的な対策を講じる。

⑸　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。

⑹　運用

情報システムの監視、本基本方針の遵守状況の確認、業務委託を行う際のセキュリティ確保等を行う。

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等に迅速に対応する。

⑺　業務委託と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、必要に応じて契約上における措置を講じる。

クラウドサービスを利用する場合には、必要に応じて利用に係る規定を整備し対策を講じる。

⑻　運用の改善

定期的又は必要に応じて運用改善を行い、情報セキュリティの向上を図る。

7　情報セキュリティ監査及び自己点検の実施

本基本方針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　本基本方針の見直し

情報セキュリティ監査及び自己点検の結果、本基本方針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、本基本方針を見直す。

附　則

1　本基本方針は、令和８年４月１日から施行する。

2　京都市会事務局情報セキュリティポリシーは、廃止する。