大阪市会サイバーセキュリティを確保するための方針

1　目的

この方針は、地方自治法（昭和 22 年法律第 67 号）第 244 条の 6 に基づき、大阪市会（以下「市会」という。）が実施するサイバーセキュリティの確保に関する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)　情報資産

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（認証情報（ID、パスワード、多要素認証情報等）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情報

(4)　サイバーセキュリティ

ネットワーク及び情報システムに対する不正又は有害な行為による被害の予防、検知、対応及び復旧に関する措置を講じ、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)　機密性

情報にアクセスすることを認められた者だけが、その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、その情報にアクセスできる状態を確保することをいう。

(8)　インターネット接続系

インターネットメール、大阪市会文書共有システム、議員在席等表示システム等に関わる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、サイバー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

この方針は、市会において適用する。

5　遵守義務

(1)　大阪市会議員及び市会事務局職員（以下「議員等」という。）は、サイバーセキュリティの重要性について共通の認識を持ち、職務の遂行に当たってこの方針を遵守しなければならない。
(2)　議員等が、市会以外の機関又は団体（国、大阪市、他の地方公共団体その他の機関又は団体をいう。）が管理運用するネットワーク及び情報システムを利用する場合は、当該ネットワーク又は情報システムの管理者が定めるサイバーセキュリティに関する規程（情報セキュリティに関する規程を含む。）、基準、手順等を遵守しなければならない。

6　サイバーセキュリティ対策

上記３の脅威から情報資産を保護するために、以下の対策を講じるものとする。

なお、その対策については、必要に応じて、大阪市情報セキュリティ対策基準を参考に実施するものとする。

(1)　組織体制

サイバーセキュリティ対策を推進する組織体制を確立する。

①　市会にサイバーセキュリティ責任者を置き、市会のサイバーセキュリティ対策を統括し、必要な指揮監督を行う。
②　サイバーセキュリティ責任者は大阪市会議長をもって充てる。
③　市会に副サイバーセキュリティ責任者を置き、サイバーセキュリティ責任者を補佐する。
④　副サイバーセキュリティ責任者は大阪市会副議長をもって充てる。

(2) サイバーセキュリティの強化

業務の効率性・利便性の観点を踏まえ、インターネット接続系においては、不正通信の監視機能の強化等の高度なサイバーセキュリティ対策を実施する。

(3) 物理的セキュリティ

市会が保有する情報資産の管理について、物理的な対策を講じるものとする。

(4) 人的セキュリティ

サイバー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ものとする。

(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ものとする。

(6) 緊急時の対応

市会が保有する情報資産に漏えい、滅失、き損、改ざん等のセキュリティ事故（その疑いがある場合を含む。）が発生した場合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) 業務委託と外部サービス（クラウドサービス）の利用

市会が保有する情報資産を取り扱う業務を委託する場合には、委託事業者が確保すべき情報資産のセキュリティに関する要件（情報資産へのアクセスに関すること、従業員に対する教育の実施、セキュリティ事故発生時の報告・対応等）を業務委託契約書等に明記し、委託事業者において当該事項が遵守され、かつ必要な対策が講じられていることを確認するなど、情報資産を適切に管理するために必要な措置を講じるものとする。

なお、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ものとする。

(8) 評価・見直し

この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監査及び自己点検を実施する。

また、監査及び自己点検の結果、この方針の見直しが必要となった場合及びサイバー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、市会が保有する情報資産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たうえで、この方針を見直すものとする。

附　則

この方針は、令和８年４月１日から施行する。