新潟市議会情報セキュリティ基本方針

1　目的

新潟市議会情報セキュリティ基本方針（以下「本方針」という。）は、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。

なお、本方針は地方自治法に基づくサイバーセキュリティを確保するための方針として定めるものである。

2　用語の定義

(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（ハードウエア及びソフトウエア）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、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、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。

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、通信の途絶等のインフラの障害からの波及等

4　適用範囲

本方針は、本市議会が保有する情報資産のうち、次の各号に定める情報資産について適用する。

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及びネットワーク図等のシステム関連文書

5　議員等の義務

議員及び職員（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つとともに、新潟市議会が所掌する情報資産を取り扱う際には、不正アクセス行為の禁止等に関する法律や著作権法等の情報セキュリティに関連する法令並びに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

３に掲げた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ずる。

(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次の各号のとおり確立する。

ア 議長を最高情報セキュリティ責任者（CISO: Chief Information Security Officer）とする。CISO は情報資産を保護するための総括的な権限及び責任を有し、情報セキュリティに関する最終決定権限及び責任を有する。

また、副議長を最高情報セキュリティ副責任者とする。最高情報セキュリティ副責任者は CISO を補佐するとともに、CISO に事故あるとき、または CISO が欠けたときは、その職務を代行する。

イ 議会事務局長を統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は CISO 及び最高情報セキュリティ副責任者を補佐するとともに、その保有する情報資産を保護するための権限及び責任、所管するネットワーク及び情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

ウ 新潟市議会事務局規程（昭和 34 年 10 月 1 日議会規程第 1 号）第１条の２に定める課長の職にある者を情報セキュリティ管理者とする。情報セキュリティ管理者は、所属における情報セキュリティに関する権限及び責任、並びに所管する情報システムにおける開発、設定の変更、運用、見直しに関する権限及び責任を有する。

エ 情報セキュリティ管理者の指名を受け、その指示等に従って情報セキュリティ管理者の補佐及び関係事務、並びに情報システムの開発、設定の変更、運用、更新等の作業及び委託業者への指示を行う者を情報セキュリティ担当者とする。

(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対策

議会棟の諸室、通信回線及び議員等の使用する公費導入パソコン等の管理について、物理的な対策を講じる。

(4)人的セキュリティ対策

情報セキュリティに関し、議員等が遵守すべき事項を次の各号のとおり定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

ア 情報資産の利用や持ち出しは、業務目的に限るものとする。

イ 情報セキュリティインシデントを発見した場合は、速やかに定められた窓口へ報告する義務を負う。

(5)技術的セキュリティ対策

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ずる。

(6)運用

情報システムの監視、本方針等の遵守状況の確認、業務委託を行う際のセキュリティ確保等、本方針等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)外部サービス（クラウドサービス）等の利用

外部サービス（クラウドサービス）を利用する場合には、利用にかか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

本方針等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し、運用改善を行い、情報セキュリティの向上を図るとともに、本方針等の見直しが必要な場合は、適宜これを行う。

7　情報セキュリティ監査及び自己点検の実施

本方針等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　本方針等の見直し

　情報セキュリティ監査及び自己点検の結果、本方針等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に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害等を分析し、リスクを検討したうえで、本方針等を見直す。

９　その他

　本方針に定めるもののほか、情報セキュリティ対策の実施について必要な事項は、議長が別に定める。

附　則

（施行期日）

　本方針は、令和８年４月１日から施行する。