千葉市議会のサイバーセキュリティを確保するための方針

第１ 目的

この方針は、千葉市議会のサイバーセキュリティ対策について、基本的な事項を定めることにより、市民の信頼に応える公的機関として、安全かつ適正な管理を確保することを目的とする。

第２ 定義

この方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) ネットワーク 通信回線及び通信回線装置で構成され、電子計算機、通信回線、通信回線装置、電磁的記録媒体及び周辺機器を相互に接続し情報を交換するための仕組みをいう。

(2) 情報システム 電子計算機、ネットワーク、電磁的記録媒体又は周辺機器で構成され、情報処理を行う仕組みをいう。

(3) 議員 千葉市議会議員をいう。

(4) 電子情報 情報システムで取り扱う情報をいう。

(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。

(8) サイバーセキュリティ 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。

(9) サイバーセキュリティ対策 サイバーセキュリティのための対策をいう。

第３ 適用範囲

この方針が適用されるのは、議員とする。

また、この方針が対象とする情報資産は、以下のとおりとする。

ア 情報システムを構成する機器、情報システムに関する設備、議会活動で取り扱う電子情報

イ 千葉市の執行部局、議会事務局及び各行政委員会等から提供された電子情報

第４ 議員の義務

議員は、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つとともに、この方針、その他サイバーセキュリティ対策及び法令を遵守する義務を負う。

第５ 組織及び体制

サイバーセキュリティ対策を推進するための組織及び体制を確立するものとする。

第６ 情報資産の管理

議員は、情報資産について、取得から廃棄に至るまでの各段階で適正に管理及びサイバーセキュリティ対策を実施するものとする。

ただし、情報資産のうち、公表情報等、一般に知り得る情報はこの限りではない。

第７ サイバーセキュリティへの脅威

議会は、次の各号に掲げるサイバーセキュリティに対する脅威について、抽出を行うものとする。

対象とする脅威は次の各号に掲げるものとする。

⑴ 不正アクセス、マルウェアによる攻撃、サービス不能攻撃等のサイバー攻撃、部外者の侵入、重要情報の詐取、内部不正等の意図的な要因に伴う情報資産の漏えい、破壊、改ざん、消去等の脅威

⑵ 情報資産の紛失、操作・設定ミス、ネットワークの誤接続、機器故障等の非意図的な要因に伴う情報資産の漏えい、破壊、改ざん、消去等の脅威

⑶ その他、情報システムを構成する機器及び情報システムに関する設備に対する脅威

第８ 脅威への対策

議会は、前項の抽出により明らかになった脅威に対して、以下のサイバーセキュリティ対策を実施するものとする。

⑴ 物理的な対策

重要な情報資産の保管場所への不正な立入り、窃盗、破壊等を防止する等の物理的な対策

⑵ 人的な対策

サイバーセキュリティに関する議員の権限及び責任の明確化、議員に対する教育及び啓発等の人的な対策

⑶ 技術的な対策

情報システム全体の強靭性の向上、情報資産を不正アクセス等から保護するためのアクセス制御、マルウェア対策等の技術的な対策

第９ サイバーセキュリティ監査及び自己点検の実施

サイバーセキュリティ対策の遵守状況を検証するため、必要に応じてサイバーセキュリティ監査及び自己点検を行うものとする。

第１０　千葉市議会のサイバーセキュリティを確保するための方針の見直し

この方針は、法令の改正、社会情勢の変化及び技術動向等を踏まえ、必要に応じて見直すものとする。

第１１　その他、必要な事項は議長が別に定めるものとする。

附 則

この方針は、令和８年４月１日から施行する。