福生市議会サイバーセキュリティ基本方針

（目的）

第１条　本方針は、地方自治法（昭和 22 年法律第 67 号）第 244 条の６に基づき、福生市議会（以下「市議会」という。）が講ずべきサイバーセキュリティ対策に関する基本的事項を定め、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し、サイバー攻撃等の様々な脅威から情報資産を守ることにより、議会運営の安定的・継続的な遂行を実現することを目的とする。

２　福生市議会議員（以下「議員」という。）及び福生市議会事務局の職員（以下「事務局職員」という。）等は、サイバーセキュリティの重要性を認識し、市議会におけるサイバーセキュリティ対策の推進に積極的に取り組むものとする。

３　市議会が保有する個人情報の漏えい、滅失又は毀損の防止その他の安全管理措置については、福生市議会の個人情報の保護に関する条例（令和４年条例第 29 号。以下「条例」という。）第９条、本方針等に基づいて実施されるものとする。

（定義）

第２条　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

コンピュータを相互に接続するための通信網及び構成機器で構成され、情報処理を行う仕組みをいう。

（２）　情報システム

コンピュータ及びネットワークにより業務処理を行う仕組みをいう。

（３）　情報資産

次のいずれかに該当するものをいう。

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（出力した文書も含む。）

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

（４）　機密性

情報にアクセスすることを認められた者のみが、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。

（７）　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。

（８）　サイバーセキュリティ

デジタル環境における情報の機密性、完全性及び可用性を維持するための包括的な取組をいう。

（９）　受託事業者

市議会から情報資産の取扱いを委託された者又は市議会から情報資産の取扱いを請け負う者をいう。

(10)　議員及び事務局職員等

議員、事務局職員及び市の職員（受託事業者、再委託先従事者を含む。）であって、市議会固有の情報システム及びネットワークを利用し、又は市議会の情報資産に接するものをいう。

(11)　端末機

会議用システム（会議用アプリケーションソフトウエア及びサーバを一体化させたシステムで、資料の共有等を行うものをいう。）等を使用するためのタブレット型コンピュータをいう。

(12)　情報セキュリティインシデント

予期しない単独又は一連の情報セキュリティ事象であって、会議等の遂行を危うくし、情報セキュリティを脅かす可能性の高いものをいう。

(13)　個人情報漏えい等

条例第 11 条に規定する個人情報の漏えい、滅失、毀損その他の保有個人情報の安全の確保に係る事態であって、個人の権利利益を害するおそれが大きいものをいう。

（対象とする脅威）

第３条　次に掲げる市議会の情報資産に対する脅威を想定し、サイバーセキュリティ対策を実施する。この場合において、新たな脅威の発生に備え、最新

の脅威動向を確認するなど、適切に対応する。

（１）　不正アクセス、ウイルス攻撃、ランサムウェア攻撃、サービス不能攻撃等のサイバー攻撃及び侵入等の意図的要因による市議会の情報資産の漏えい、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、無許可ソフトウエ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、外部委託管理の不備、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会議等の停止等

（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障害からの波及等

（適用範囲）

第４条　この方針が適用される範囲は、議員及び事務局職員等とする。

２　この方針が対象とする情報資産は、次のとおりとする。

（１）　情報システム及びネットワーク

（２）　個人情報のほか、情報システム等で取り扱うデータ

（３）　情報システム等に関するシステム設計書、ネットワーク図等のシステム関連文書

（議員及び事務局職員等の遵守義務）

第５条　議員及び事務局職員等は、市議会が保有する情報資産に対する脅威への対応の重要性について共通の認識を持ち、会議等の遂行に当たって、本方針を遵守しなければならない。

（サイバーセキュリティ対策）

第６条　市議会は、第３条に規定する脅威から情報資産を保護するため、次のサイバーセキュリティ対策を講じる。

（１）　組織体制の確立

市議会の情報資産について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。

（２）　情報資産の分類と管理

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、適切なセキュリティ対策を講じる。

（３）　物理的セキュリティ対策

サーバ、通信回線及び端末機等の管理について、不正な立入り及び盗難、損傷、破壊、自然災害等から情報資産を保護するため、必要な物理的対策を講じる。

（４）　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、議員及び事務局職員等に対する十分な教育及び啓発が講じられるように必要な対策を講じる。

（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、ネットワーク管理、コンピュータウイルス対策その他の必要な技術的対策を講じる。

（６）　運用面での対策

情報システムの監視及び本方針等の遵守状況の確認のほか、次号の業務委託及びクラウドサービスを利用する際のセキュリティ確保等の本方針等の運用面での対策を講じるものとする。この場合において、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、緊急時対応体制を整備する。

（７）　業務委託及びクラウドサービス利用に係る対策

業務委託及びクラウドサービス等の外部サービス利用に当たり、委託事業者の選定時に情報セキュリティ要件を明示し、個人情報の目的外利用禁止、秘密保持義務、情報の返却・廃棄等の事項を契約に明記するものとする。この場合において、委託期間中は委託事業者等における情報セキュリティ対策の履行状況を定期的に確認し、改善指導を行うとともに、情報セキュリティインシデント発生時は直ちに報告を求め適切に対処し、クラウドサービス等の外部サービスを利用する場合は、サービス提供者のセキュリティ水準、個人情報保護体制、情報の保存地域、廃棄方法等を事前に確認し、取り扱う情報の分類に応じて利用承認を得た上で、委託終了時には、提供した情報を確実に返却・廃棄させ、その処理内容を記録・保管するものとする。

（８）　個人情報保護対策

市議会が保有する個人情報について、条例第９条に基づき、安全管理措置を講じ、情報セキュリティインシデントにより個人情報漏えい等が発生

した場合は、原則として本人に対する通知を行う。

（自己点検及びセキュリティ監査の実施）

第７条　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、自己点検及びセキュリティに関する監査を実施する。

（本方針等の見直し）

第８条　自己点検及びセキュリティに関する監査の結果、本方針等の見直しが必要となった場合又は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となった場合には、本方針等の見直しを実施し、議会運営委員会にて審議するものとする。

附　則

この方針は、令和８年４月１日から施行する。