石岡市議会
情報セキュリティ基本方針

石岡市議会

目次

１　目的

本基本方針は、石岡市議会（以下「議会」という。）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、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。

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

ネットワーク及び情報システムの開発と運用に係るすべての情報並びにネットワーク及び情報システムで取り扱う情報をいう。

（4）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。

（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。

３　対象とする脅威

議会は、情報資産に対する脅威として次に掲げるものを想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃及びサービス不能攻撃等のサイバー攻撃並びに部外者の侵入、内部不正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、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サービス及び業務の停止等

（４）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

本基本方針の適用範囲は、議会が取り扱う情報資産とし、石岡市行政情報セキュリティポリシー（平成15年策定）の適用を受ける情報資産の取扱いは本基本方針の適用範囲外とする。

５　議員及び議会事務局職員の遵守義務

議員、議会事務局の全ての職員(以下、「議員等」という。)及び外部委託事業者に属する者等は、情報セキュリティの重要性について共通の認識を持ち、活動及び業務の遂行に当たって本基本方針を遵守する義務を負うものとする。

６　組織体制

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議会内に確立するため、最高情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ担当者を置く。

（１）最高情報セキュリティ責任者

最高情報セキュリティ責任者は、議長をもって充て、議会における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（２）情報セキュリティ責任者

情報セキュリティ責任者は、議会事務局長をもって充て、最高情報セキュリティ責

任者を補佐するとともに、情報セキュリティ管理者に対し情報セキュリティに関する事項に関して指示及び指導を行う。

また、石岡市情報管理組織に関する規則（平成17年石岡市規則第21号）第３条第１項に規定する統括情報管理者が招集する石岡市情報化推進会議において決定した事項について、必要に応じて議会の情報セキュリティ対策を講じる。

（３）情報セキュリティ管理者

情報セキュリティ管理者は、庶務議事課長をもって充て、情報セキュリティ対策を実施するとともに、情報セキュリティ担当者に対し情報セキュリティに関する事項に関して指示及び指導を行う。

情報資産に関するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者及び最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰ぐ。

（４）情報セキュリティ担当者

情報セキュリティ担当者は、庶務議事課係長をもって充て、情報セキュリティ管理者のもと、情報資産の適正な維持管理を実施するとともに、本基本方針の周知、推進を行う。

７　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、以下の情報セキュリティ対策を講じる。

（１）情報システムを設置した場所への不正な立ち入り又は情報資産の持ち出し若しくは破壊等の物理的な侵害から情報資産を保護するための物理的なセキュリティ対策

（２）情報セキュリティ対策に関する実施体制の整備及び周知徹底をはじめとした情報資産を取り扱う議員等に対する教育等の人的なセキュリティ対策

（３）情報資産に対する不正アクセスの防止、ウイルス対策及びインターネットの利用に伴うリスクに対する接続点の限定等の技術的なセキュリティ対策

８　情報セキュリティ監査及び自己点検の実施

本基本方針が遵守されていることを検証するため、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。監査については、客観性を確保するために、外部の専門知識・見解を有する者の協力を得て実施することができる。

９　情報セキュリティ基本方針の見直し

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に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、リスクを検討した上で、本基本方針を見直す。

附則

この基本方針は、令和８年４月１日から施行する。