筑西市選挙管理委員会サイバーセキュリティを確保するための方針

令和８年３月２日
筑西市選挙管理委員会

１　目的

筑西市選挙管理委員会サイバーセキュリティを確保するための方針（以下「本方針」という。）は、筑西市選挙管理委員会（以下「委員会」という。）が取り扱う住民の個人情報及び行政運営上重要な情報資産を破壊、改ざん、消去、持出し等の脅威から保護し、住民の財産及び個人のプライバシーを守り、安全かつ安定的な行政サービスを提供することを目的とする。

２　定義

⑴　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その構成機器（ハードウェア及びソフトウェア）をいう。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑴　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、改ざん及び消去、重要情報の詐取、内部不正等

⑵　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、内部及び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

⑶　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

⑷　大規模又は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

⑸　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障害による波及等

4　適用範囲

⑴　対象者の範囲

本方針は、委員会の委員及び事務局職員（以下「委員等」という。）並びに委員会が管理又は監督する業務を受託する事業者（以下「受託事業者」という。）に適用する。

⑵　情報資産の範囲

本方針が対象とする情報資産は、次のとおりとする。

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（これらを印刷した文書を含む。）

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文書

5　順守義務

委員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって本方針を順守しなければならない。

6　情報セキュリティ対策

情報資産に対する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じる。

⑴　組織体制

委員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確立する。

⑵　情報資産の分類と管理

委員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。

⑶　物理的セキュリティ対策

サーバ、情報システム室、通信回線及び委員等のパソコン等の管理について、物理的なセキュリティ対策を講じる。

⑷　人的セキュリティ対策

情報セキュリティに関し、委員等が順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セキュリティ対策を講じる。

⑸　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セキュリティ対策を講じる。

⑹　運用

情報システムの監視、本方針の順守状況の確認、業務委託を行う際のセキュリティ確保等、運用面のセキュリティ対策を講じる。

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。

⑺　業務委託

業務委託を行う場合には、受託事業者において適切なセキュリティ対策が確保されていることを確認し、情報セキュリティ要件を明記した契約を受託事業者と締結する。

また、契約締結後においても、受託事業者において契約に基づくセキュリティ対策が行われていることを確認し、必要に応じて措置を講じる。

⑻　外部サービス（クラウドサービス）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、利用に係る規程を整備し、セキュリティ対策を講じる。

⑼　ソーシャルメディアサービスの利用

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、発信できる情報、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。

⑽　評価

本方針の順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。

⑾　見直し

本方針の見直しが必要な場合は、適宜見直しを行う。