

三種町議会情報セキュリティ基本方針

1 目的

本基本方針は、本町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するため、本町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。
- (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、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

(1) 議事機関の範囲 本基本方針が適用される議事機関は、議会及び議会事務局とする。

(2) 情報資産の範囲 本基本方針が対象とする情報資産は、次のとおりとする。ただし、議員の私的な情報システムであって、本町議会や本町が保有する情報資産に影響を及ぼすおそれがないものは除く。

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 議員等の遵守義務

議員及び職員等（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ち、業務の遂行に当たって本基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

上記3の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について検討する。

(1) 組織体制 本町議会の情報資産について、情報セキュリティ対策を推

進する組織体制を確立する。

(2) 情報資産の分類と管理 本町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。

(4) 物理的セキュリティ 通信回線及び議員等のタブレット等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ 情報セキュリティに関し、議員等が遵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対策を講じる。

(6) 技術的セキュリティ 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対策を講じる。

(7) 運用 情報システムの監視、本基本方針の遵守状況の確認等、本基本方針の運用面の対策を講じるものとする。

(8) 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。

(9) 評価・見直し 本基本方針の遵守状況を検証するため、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し、運用改善を行い、情報セキュリティの向上を図る。本基本方針の見直しが必要な場合は、適宜本基本方針の見直しを行う。

7 情報セキュリティ監査及び自己点検の実施

本基本方針の遵守状況を検証するため、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。

8 本基本方針の見直し

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、リスクを検討したうえで、本基本方針を見直す。