東浦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) 情報セキュリティポリシー

本基本方針及び東浦町議会情報セキュリティ実施手順をいう。

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、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) 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　情報資産の範囲

(1) 対象機関の範囲

本基本方針が適用される範囲は、東浦町議会とする。

(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。

・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

・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。）

・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　町議会議員等の遵守義務

町議会議員等は、情報セキュリティの重要性について共通の認識を持ち、議会運営に当たって情報セキュリティポリシーを遵守しなければならない。

６　情報セキュリティ対策

項目３で示した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。

(1) 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。

(2) 物理的セキュリティ

町議会議員等のパソコン等の管理について、物理的な対策を講じる。

(3) 人的セキュリティ

情報セキュリティに関し、町議会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。

(4) 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。

(5) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認等、情報セキュリティポリシーの運用面の対策を講じるものとする。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。

(6) 評価・見直し

情報セキュリティポリシーの遵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。情報セキュリティポリシーの見直しが必要な場合は、適宜

情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵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する。

8　評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシー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、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

項目6、7及び8に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ実施手順を策定する。

第1版　令和8年4月1日