清水町情報セキュリティポリシー

2020年7月

第１編　情報セキュリティ基本方針

１　目的

この基本方針は、町の情報セキュリティ対策の基本を定めたもので、町が保有する個人情報及び行政運営上重要な情報等の情報資産を様々な脅威から保護し、機密性・完全性・可用性を維持することを目的とする。

２　用語の定義

本ポリシーにおける用語の定義は、次のとおりとする。

⑴　情報セキュリティ
　情報資産の機密性・完全性・可用性を維持すること。

⑵　機密性
　許可された者だけが情報にアクセスできること。

⑶　完全性
　情報が破壊、改ざん及び消去されていないこと。

⑷　可用性
　許可された者が必要なときに情報にアクセスできること。

⑸　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及びその構成機器

⑹　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等で構成され、これら全体で情報を処理する仕組み

⑺　ハードウェア
　本体、キーボードやマウス、スキャナ等の入力装置、ハードディスク等の記録媒体、ディスプレイ等の出力装置などのパソコンを構成する部品や装置

⑻　ソフトウェア
　パソコン等で動作するプログラム全般

３　対象とする脅威

⑴　ウイルス攻撃、サイバー攻撃、不正アクセス等の意図的な要因による情報の漏えい、改ざん、破壊、消去、搾取、内部不正等

⑵　無許可ソフトウェアの使用、情報システムの設計･操作ミス等の非意図的な要因による情報の漏えい、改ざん、破壊、消去等

⑶　災害等によるサービス及び業務の停止

⑷　電力供給、通信の途絶等インフラ障害による機能不全

４　適用範囲

⑴　行政機関の範囲
　本方針は、町長部局、教育委員会部局、議会事務局、公営企業、行政委員会に適用する。

⑵　情報資産の範囲
　ア　ネットワーク、情報システムに関する設備及び電磁的記録媒体
　イ　電磁的に記録された全ての情報及びその印刷物
　ウ　ネットワーク及び情報システムに関する仕様書等の関連文書

5　職員の遵守義務

職員（臨時職員及び嘱託職員含む。）は、情報資産の適切な管理の重要性について共通の認識を持ち、業務の際には、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6　情報セキュリティ対策

⑴　組織体制

情報セキュリティ対策を推進する全庁的な組織体制を確立する。

⑵　情報資産管理基準

町の情報資産を重要度に応じて分類し、その分類に基づき情報セキュリティ対策を行う。

⑶　物理的セキュリティ

パソコン及びモバイル端末（以下「パソコン等」という。）、サーバ、ネットワーク機器並びにサーバ室の管理等の物理的な対策を講じる。

⑷　人的セキュリティ

職員が遵守すべき事項を定め、教育・啓発等の人的な対策を講じる。

⑸　技術的セキュリティ

パソコン等の管理、アクセス制御、不正プログラム対策等の技術的な対策を講じる。

⑹　運用

情報セキュリティポリシーの遵守及び外部委託時のセキュリティ確保等の運用面での対策を講じる。

7　情報セキュリティ監査の実施

情報セキュリティポリシーの遵守及び情報セキュリティ対策について、定期的又は必要に応じて監査を行う。

8　情報セキュリティポリシーの見直し

情報セキュリティ監査の結果及び情報セキュリティを取り巻く状況の変化等を踏まえ、必要に応じて本ポリシーの見直しを行う。

9　情報セキュリティ対策基準の策定

情報セキュリティ対策の具体的な遵守事項及び判断基準を定めた情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策の具体的な手順を定めた情報セキュリティ実施手順（以下「実施手順」という。）を策定する。

なお、実施手順は公にすることで町政運営に重大な支障を及ぼすおそれがあるため非公開とする。