情報セキュリティ基本方針

第１　目的

本基本方針は、本町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。

第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　本基本方針及び情報セキュリティ対策基準をいう。

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。

第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、ウィルス攻撃、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、内部点検・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

第４　適用範囲

１　行政機関の範囲

本基本方針が適用される行政機関は、町長部局、教育委員会部局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。

(1)　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

(2)　ネットワーク及び情報システムで取扱う情報（これらを印刷した文書を除く。）

(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

第５　職員の遵守義務

職員（非常勤職員及び臨時職員を含む。以下同じ。）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。

第６　情報セキュリティ対策

上記第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を講じる。

(1)　組織体制　本町の情報資産について、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。

(2)　情報資産の分類と管理　本町が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行う。

(3)　物理的セキュリティ　サーバ等、サーバ室、通信回線等及び職員のパソコン等の管理について、物理的な対策を講じる。

(4)　人的セキュリティ　情報セキュリティに関し、職員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。

(5)　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。

(6)　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、外部委託を行う際のセキュリティ確保等、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。

第７　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、定期的に監査及び自己点検を実施する。

第８　情報セキュリティポリシーの見直し

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、情報セキュリティポリシーを見直す。

第９　情報セキュリティ対策基準の策定

上記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を定める情報セキュリティ対策基準を策定する。

第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を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより本町の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。