情報セキュリティ基本方針

目　　次

１．はじめに

八千代町が取扱う情報には、町民の個人情報や行政情報等、厳重管理が必要な情報資産が数多く含まれている。これらの情報資産は、町民の財産及びプライバシーの保護、また、安全かつ継続的なサービスを提供するため、故意や過失による情報漏えいや改ざん、システムの故障及び停止、自然災害による被災等の様々な脅威から確実に保護しなければならない。

今後、各種手続のオンライン化や効率的で利便性の高い情報システムの利用など、町民が安心して利用できる電子自治体を構築するため、情報セキュリティに関する事件・事故を未然に防止するとともに、事件・事故又は被災等による被害の最小化・局所化、さらにはこれらの再発防止等、情報資産保護を包括した情報セキュリティポリシーを定め、情報セキュリティの確保に最大限取組むこととする。

２．目的

本基本方針は、八千代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、八千代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。

３．用語の定義

（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だけが、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。

４．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）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、無許可ソフトウエ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、機能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提供サービスの障害からの波及等

５．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、内部部局、行政委員会、議会事務局及び地方公営企業とする。

（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

６．職員等の遵守義務

職員、非常勤職員及び臨時職員（以下「職員」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。

７．情報セキュリティ対策

上記４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

八千代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

八千代町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行う。

（３）物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職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。

（４）人的セキュリティ

情報セキュリティに関し、職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。

（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。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

８．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。

９．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。

１０．情報セキュリティ対策基準の策定

上記７、８及び９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対策基準を策定する。

１１．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八千代町の行政運営に重大な支障を及ぼすおそれのあることから**非公開**とする。