

高千穂町
情報セキュリティ基本方針

平成 27 年 9 月

高千穂町

序 高千穂町情報セキュリティポリシーの構成

高千穂町情報セキュリティポリシーとは、高千穂町が所掌する情報資産に関するセキュリティ対策について、総合的、体系的かつ具体的にとりまとめたものである。

高千穂町情報セキュリティポリシーは、本町の情報資産を取り扱う全職員、非常勤及び臨時職員（以下「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかし、一方では、情報の処理技術や通信技術等の進展に伴う情報管理を取り巻く急速な状況の変化に、柔軟に対応することも必要である。

このようなことから、高千穂町情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の2階層からなるものとして策定することとする。また、情報セキュリティ対策基準に基づき、情報システム毎に、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。

高千穂町情報セキュリティポリシーの構成

文書名		内容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための、全ての情報資産に共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報システム毎に定める、情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策基準

1. 目的

高千穂町の情報システムが取り扱う情報には、町民の個人情報や行政運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等様々な脅威から防御することは、町民の財産、プライバシーを守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも不可欠である。

このため、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ことを目的として高千穂町情報セキュリティ基本方針（以下「情報セキュリティ基本方針」という）を定める。高千穂町の情報資産に関する情報セキュリティ対策の基本的な考え方や方針を規定するものである。

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) 情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

(4) データ

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、パンチカードその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

(5) 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。

(6) 情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

(7) 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。

(8) 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。

(9) 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、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な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) 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

5. 職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、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。

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を講ずるものとする。

(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切に対応するため危機管理対策を講ずる。

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. 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。

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等を定める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を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に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、公開することにより高千穂町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。