

# 神川町情報セキュリティポリシー

## 情報セキュリティ基本方針

(令和8年4月1日改定版)

神 川 町

<改定履歴>

	改定日	改定内容	文書取扱
1	平成 14 年度	策定	まちづくり政策課
2	平成 18 年度	全部改定	総合政策課
3	平成 27 年 12 月 24 日	番号制度改正等に伴う一部改定	総合政策課
4	平成 30 年 4 月 1 日	総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 27 年 3 月版）」の改定及び情報セキュリティ強靱化の実施に伴う全部改定	総合政策課
5	令和 2 年 4 月 1 日	総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 30 年 9 月版）」の改定並びに地方公務員法及び地方自治法の一部を改正する法律の施行等に伴う一部改定	総合政策課
6	令和 8 年 4 月 1 日	地方自治法の一部を改正する法律の施行に伴う一部改定	総合政策課

## 目 次

総則.....	4
第1 目的.....	5
第2 定義.....	5
第3 適用範囲.....	6
第4 職員等の遵守義務.....	6
第5 対象とする脅威.....	6
第6 情報セキュリティ対策.....	7
第7 情報セキュリティ監査の実施及び自己点検の実施.....	7
第8 情報セキュリティポリシーの見直し.....	7
第9 情報セキュリティ対策基準の策定.....	8
第10 情報セキュリティ実施手順の策定.....	8
第11 懲戒処分等.....	8
第12 補則.....	8

## 総則

本町は、町民の個人情報や行政運営上重要な情報などを多数取り扱うとともに、ほかに代替えすることができない行政サービスを提供している。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。

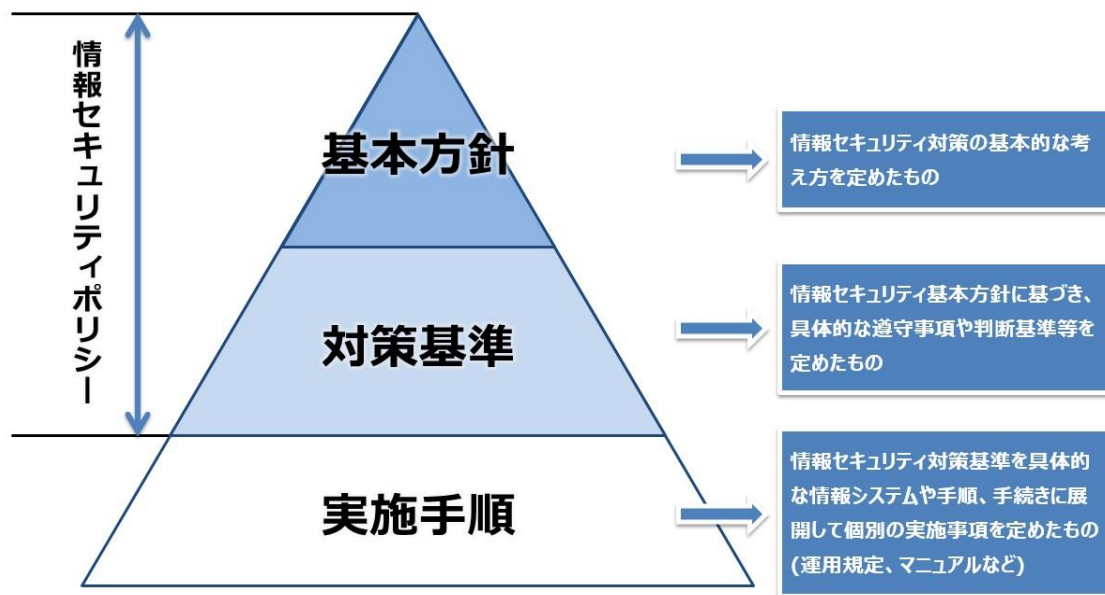
したがって、これらの情報資産を様々な脅威から防御することは、町民の財産、プライバシー等を守るためにも、また、安定的な行政運営を行うためにも必要不可欠である。

このため、本町の情報資産の機密性、完全性及び可用性を維持するため、神川町情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

神川町情報セキュリティポリシーとは、本町が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

このうち本町の情報セキュリティ対策の基本的な考え方を定めたものが「情報セキュリティ基本方針」である。この基本方針に基づき、情報セキュリティ対策の基準を定めたものが「情報セキュリティ対策基準」である。この対策基準を具体的な情報システムや手順、手続きに展開して個別の実施事項を定めたものが「情報セキュリティ実施手順」である。

神川町情報セキュリティポリシー体系図



## 第1 目的

この基本方針は、本町が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産について、情報セキュリティ対策に関する基本的な事項を定めることにより、町民の財産、プライバシー等の保護及び安定的な行政事務の運営を図り、もって町民からの信頼の維持向上に寄与することを目的とする。

## 第2 定義

### (1) コンピュータ

パーソナルコンピュータ（以下「パソコン」という。）、サーバ及び情報を長期的に保存しておくことを目的としたハードディスク等の補助記録装置（ストレージ）等の機器をいう。

### (2) 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。

### (3) 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<sup>1</sup>で構成され、情報処理を行う仕組みをいう。

### (4) 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と入出力される帳票・文書をいう。

### (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) 機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

### (7) 完全性

情報資産が破壊、改ざん、消去又は不正なデータがない状態を確保することをいう。

### (8) 可用性

情報資産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、情報資産にアクセスできる状態を確保することをいう。

---

<sup>1</sup> 電磁的記録媒体

パソコンやサーバ等に内蔵されているハードディスク等の内蔵記録媒体や外付けハードディスク、CD、DVD、MO、FD、USBメモリ等の外部記録媒体。

(9) 特定個人情報

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）第 2 条に規定する個人番号（以下「マイナンバー」という。）をその内容に含む個人情報をいう。

(10) 個人番号利用事務系（マイナンバー利用事務系）

個人番号利用事務又は戸籍事務等に関わる情報システムをいう。

(11) LGWAN 接続系

財務会計等 LGWAN（総合行政ネットワーク）に接続された情報システムをいう。

(12) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システムをいう。

### 第 3 適用範囲

この基本方針の適用範囲は、本町の保有する情報資産、その情報資産に関する業務に携わる全ての職員、非常勤職員及び会計年度任用職員（以下、「職員等」という。）並びに外部委託事業者とする。

### 第 4 職員等の遵守義務

本町の保有する情報資産、その情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに、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 5 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) ウイルス攻撃、不正アクセス、サービス不能攻撃、標的型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の要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害並びに事故、故障等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、通信の途絶その他のインフラ（社会基盤）障害による機能不全等

## 第6 情報セキュリティ対策

本町の情報資産を第5に示した脅威から保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

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重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3) 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。

(4) 物理的セキュリティ

サーバ等、サーバ室等、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。

(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な対策を講じる。

(6) 運用

情報システム及びネットワークの監視、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の確保等、運用面の対策を講じる。

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、緊急時対応策を講じる。

## 第7 情報セキュリティ監査の実施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。

## 第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、新たに対策が必要となった場合には、情報セキュリティポリシーの見直しを行う。

## 第9 情報セキュリティ対策基準の策定

上記第6、第7及び第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。

## 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。

## 第11 懲戒処分等

情報セキュリティポリシーに違反した職員等は、その重大性、発生した事案の状況等に応じ、地方公務員法の規定による懲戒処分の対象とする。

## 第12 補則

情報セキュリティ対策基準及び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恐れがあることから非公開とする。