山　辺　町
情報セキュリティポリシー

（地方自治法第244条の6に基づくサイバーセキュリティを確保するための方針）

策定　平成２０年　４　月　１　日
改定　令和　８　年　３　月１３日

山　辺　町

改定履歴

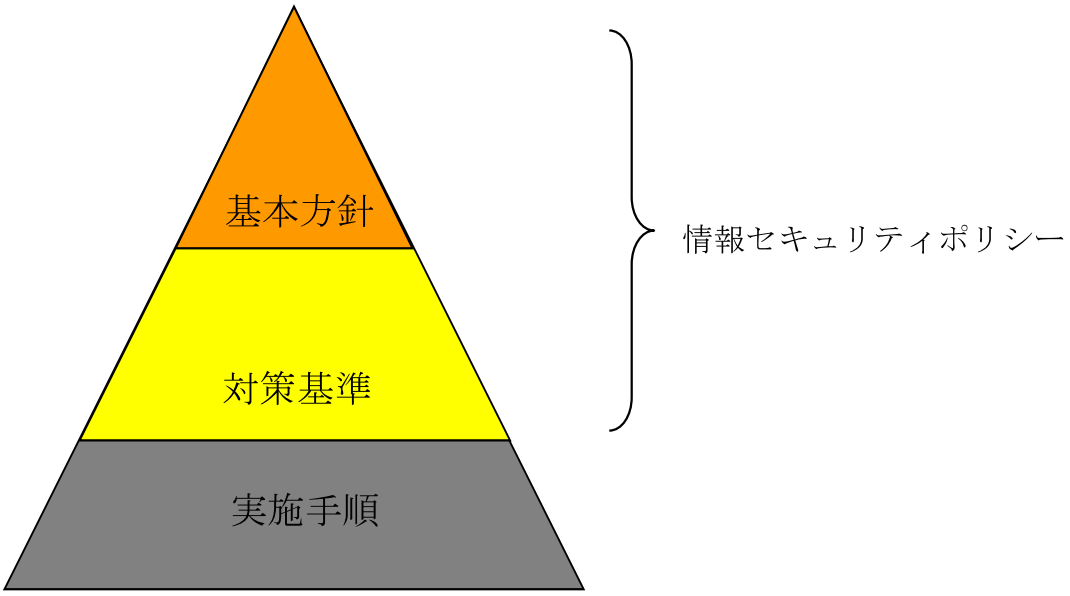
版数	改定日	改定内容の概要
第 1 版	平成 20 年 4 月 1 日	新規策定
第 2 版	平成 29 年 11 月 6 日	情報セキュリティ対策基準、共通実施手順改定
第 3 版	令和 8 年 3 月 13 日	地方自治法第 244 条の 6 に基づく全面改定

情報セキュリティポリシーの構成

情報セキュリティポリシーとは、山辺町が所掌するコンピュータや情報通信ネットワークといった情報システム（以下「情報資産」という。）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を総称する。情報セキュリティポリシーは、山辺町が所掌する情報資産に関する業務に携わる全職員、非常勤及び会計年度任用職員（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。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。
具体的には、情報セキュリティポリシーを、①情報セキュリティ基本方針及び②情報セキュリティ対策基準の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順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（下図参照）。

情報セキュリティポリシーの構成



山　辺　町
情報セキュリティ基本方針

策定　平成２０年４月１日
改定　令和８年３月１３日

山　辺　町

● 目　次

情報セキュリティ基本方針

１　目的

２　定義

（１）ネットワーク

（２）情報システム

（３）情報セキュリティ

（４）情報セキュリティポリシー

（５）機密性

（６）完全性

（７）可用性

（８）サイバーセキュリティ

（９）情報セキュリティインシデント

３　対象とする脅威

（１）意図的な要因による脅威

（２）非意図的な要因による脅威

（３）災害等による物理的脅威

（４）サイバー攻撃による脅威（高度化・巧妙化）

（５）サプライチェーンの弱点を悪用した脅威

（６）標的型攻撃メール等による脅威

（７）内部不正行為による脅威

４　適用範囲

（１）行政機関の範囲

（２）情報資産の範囲

（３）委託先等の範囲

５　職員等の遵守義務

６　情報セキュリティ対策

（１）組織体制

（２）情報資産の分類と管理

（３）物理的セキュリティ

（４）人的セキュリティ

（５）技術的セキュリティ

（６）運用

７　情報セキュリティ監査及び自己点検の実施

８　情報セキュリティポリシーの見直し

９　情報セキュリティ対策基準の策定

１０　情報セキュリティ実施手順の策定

１１　公表

情報セキュリティ基本方針

１　目的

本基本方針は、山辺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とともに、サイバー攻撃その他の脅威から町の情報システム及び業務を保護し、住民サービスの安定的な提供を確保することを目的とする。

また、本基本方針は、地方自治法第 244 条の 6 に基づく「サイバーセキュリティを確保するための方針」として位置付ける。

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、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。

（８）サイバーセキュリティ

サイバー攻撃その他の脅威から情報システム及び業務を保護し、安定的な行政サービスを確保するための取組をいう。

（９）情報セキュリティインシデント

不正アクセス、マルウェア感染、情報漏えい、システム障害その他、情報資産の機密性・

完全性・可用性に影響を及ぼす事象又はそのおそれをいう。

３　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

（１）意図的な要因による脅威

外部からの不正アクセス、標的型攻撃メール、ランサムウェア等のサイバー攻撃による情報の窃取、改ざん、破壊及びシステム停止。また、部外者の侵入、盗難、破壊行為のほか、職員等による情報資産の不正持ち出し、不正利用等の内部不正行為。

（２）非意図的な要因による脅威

職員等の操作ミス、設定ミス、知識不足による情報の紛失、誤送信、誤廃棄。情報システムの故障、不具合、メンテナンス不備によるサービス停止。また、生成 AI 等の新たな技術の不適切な利用に伴う情報漏えい。

（３）災害等による物理的脅威

地震、落雷、火災、水害、その他の自然災害や事故、広域的な停電等による、情報システムの物理的な損壊及び長期間の停止。

（４）サイバー攻撃による脅威（高度化・巧妙化）

特定の個人や組織を狙い、マルウェアを感染させて情報を奪う標的型攻撃や、データを暗号化して金銭を要求するランサムウェア攻撃など、行政サービスの継続を困難にする攻撃。

（５）サプライチェーンの弱点を悪用した脅威

本町の業務に関わる外部委託先、指定管理者、又はクラウドサービス提供者等のセキュリティ対策の不備を突いた攻撃、及び提供されるソフトウェアやハードウェアへの不正なプログラムの混入。

（６）標的型攻撃メール等による脅威

特定の組織や個人を標的とし、業務に関係する内容を装ったメールによってマルウェアに感染させ、情報の窃取、改ざん、又はランサムウェア等によるデータの暗号化及びシステム停止を引き起こす脅威。

（７）内部不正行為による脅威

職員等（委託先職員等を含む。）が、権限を悪用して情報資産を不正に持ち出す行為、データの改ざん、又は情報の目的外利用を行うことによる機密情報の流出及び行政への信頼失墜。

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、町長の事務部局に属する各課並びに議会、委員会及び監査委員の事務部局（以下「各課等」という。）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。

ア　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

イ　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）

ウ　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

（３）委託先等の範囲

本基本方針は、山辺町が締結する委託契約に基づき業務を行う事業者、指定管理者、クラウドサービス提供者等が取り扱う情報資産にも適用する。

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。

また、委託事業者及び指定管理者は、本基本方針及び契約に定める情報セキュリティ要件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、次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。

町は、情報セキュリティインシデント発生時に迅速な初動対応・連絡・復旧を行うため、必要な体制を整備する。

（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、情報システム室、通信回線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。

職員等に対し、定期的な情報セキュリティ研修及び訓練（フィッシング訓練等）を実施する。

（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。

ア 脆弱性管理（パッチ適用、設定管理）を適切に行う。

イ 多要素認証の導入を推進する。

ウ ログの取得・保存・監視を適切に行う。

エ クラウドサービス利用時は、セキュリティ要件（認証方式、ログ取得、データ保管場所等）を確認する。

（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し、情報セキュリティインシデントが発生した場合には、初動対応、関係機関への報告、復旧、再発防止を迅速に行う。

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。

また、情報セキュリティ対策の実効性を確保するため、PDCA サイクルに基づき継続的な改善を行う。

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、又は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ものとする。

また、本基本方針は、社会情勢、技術動向、法令改正、インシデント発生状況等を踏まえ、必要に応じて見直すものとする。さらに、概ね３年を目安として定期的に見直しを行うもの

とする。

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。

１１　公表

本基本方針を策定し、又は変更したときは、地方自治法第 244 条の 6 第 2 項に基づき、遅滞なく公表しなければならない。