鳴沢村情報セキュリティポリシー

平成 29 年２月１日策定
令和元年６月 12 日改定
令和８年４月１日改定

第１章 情報セキュリティ基本方針

１　方針の目的

本基本方針は、「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」及び「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針」に基づき、鳴沢村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、鳴沢村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。また、前提として本村は三層分離モデルのαモデルを採用している。

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。

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、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

この基本方針が適用される行政機関は、内部部局、行政委員会（(選挙管理委員会・公平委員会・監査委員・農業委員会・固定資産評価審査委員会・その他委員会等）以下同じ。)、議会事務局、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、非常勤職員、臨時的任用職員、再任用職員、若しくは会計年度任用職員等（以下「職員等」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。

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じる。

（１） 組織体制

鳴沢村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

鳴沢村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、緊急時対応計画を策定する。

（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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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鳴沢村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。

～第２章情報セキュリティ対策基準の項番１～９に関しては非公開とする～

１０　評価・見直し

（１）　監査

①　実施方法

統括情報セキュリティ責任者は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

②　監査を行う者の要件

（ア）情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

（イ）監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

③　監査実施計画の立案及び実施への協力

（ア）情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

（イ）被監査部門は、監査の実施に協力しなければならない。

④　委託事業者に対する監査

事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

⑤　報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、鳴沢村情報セキュリティ委員会に報告する。

⑥　保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

⑦　監査結果への対応

統括情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する情報セ

キュリティ責任者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ責任者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

統括情報セキュリティ責任者は、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

⑧ 情報セキュリティポリシー及び関係規程等の見直し等への活用

鳴沢村情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（2） 自己点検

① 実施方法

（ア）統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

（イ）情報セキュリティ責任者は、情報セキュリティ責任者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

② 報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、鳴沢村情報セキュリティ委員会に報告しなければならない。

③ 自己点検結果の活用

（ア）職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

（イ）鳴沢村情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活

用しなければならない。

（３） 情報セキュリティポリシー及び関係規程等の見直し

鳴沢村情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示し、措置の結果についてCISO に報告しなければならない。

１１　改版履歴

改版履歴	日時	内容
初版	平成 29 年2月1日	
1.1 版	平成 29 年９月 30 日	副村長設置による CISO の変更（村長→副村長）
1.2 版	令和元年６月 12 日	職員等の中に会計年度任用職員を令和 ２ 年度を見越して追記。上職者不在時の対応を追記。
2.0 版	令和８年４月１日	総務省の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(令和７年３月版）及び地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針に基づいた内容の見直し。