美里町情報セキュリティポリシー

基本方針

平成31年３月１日

熊本県美里町

【改訂履歴】

| 施行年月日 | 版番号 | 改訂理由・内容 |
| --- | --- | --- |
| 平成18年1月10日 | 第1.0版 | 初版発行（平成18年1月10日） |
| 平成31年３月１日 | 第2.0版 | 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）」（一部改訂）及び「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）」（一部改訂）の発行による改訂 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

目　次

[はじめに 1](#_Toc501374584)

[１　目的 2](#_Toc501374585)

[２　定義 2](#_Toc501374586)

[３　対象とする脅威 3](#_Toc501374587)

[４　適用範囲 3](#_Toc501374588)

[５　職員等の遵守義務 4](#_Toc501374589)

[６　情報セキュリティ対策 4](#_Toc501374590)

[７　情報セキュリティ監査及び自己点検の実施 5](#_Toc501374591)

[８　情報セキュリティポリシーの見直し 5](#_Toc501374592)

[９　情報セキュリティ対策基準の策定 6](#_Toc501374593)

[10　情報セキュリティ実施手順の策定 6](#_Toc501374594)

[11　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の非公開 6](#_Toc501374595)

# はじめに

地方公共団体の情報システムが取り扱う情報には、住民の個人情報のみならず、行政運営上重要な情報等、外部への漏えい等が発生した場合には、極めて重大な結果を招く情報が多数含まれている。

さらに、社会保障・税番号法制度の導入により、各地方公共団体内で取り扱う情報は、より一層重要なものになっており、個人番号を含む特定個人情報の漏えいには、特に注意をしなければならない。

したがって、美里町の情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。

また、美里町が電子自治体を構築するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠である。

情報セキュリティ対策は、情報の保護の点では、個人情報保護対策と内容的に重なる部分も多く、また、自然災害による被災時の対応という点では、防災対策とも重なる部分があることから、関連部署が相互に連携し、それぞれの情報セキュリティ対策に取り組み、情報セキュリティに関する事故の未然防止のための計画、事故が発生した場合の拡大防止・迅速な復旧や再発防止対策を講じていくことが必要である。

そのため、美里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、美里町が実施する情報セキュリティ対策の整備を目的に、「美里町情報セキュリティポリシー」を制定するものである。

# １　目的

本基本方針は、美里町（以下「町」という。）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、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。

# ２　定義

（１）　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。

（２）　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。

（３）　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。

（４）　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。

（５）　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。

（６）　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。

（７）　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。

（８）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（９）　ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等ＬＧＷＡＮに接続された情報システム及びその情報システムで取り扱うデータをいう。

（10）　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及びその情報システムで取り扱うデータをいう。

（11）　通信経路の分割

接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（12）　無害化通信

ＬＧＷＡＮインターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

# 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）　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）　実施機関の範囲

本基本方針が適用される実施機関は、町長部局、教育委員会部局、選挙管理委員会事務局、農業委員会事務局、監査委員事務局、固定資産評価審査委員会事務局、議会事務局並びにその他町の情報資産及び情報システムを保有する機関とする。

（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、非常勤職員及び臨時職員（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、次の情報セキュリティ対策を講じる。

（１）　組織体制

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

町が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実施する。

（３）　情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）　物理的セキュリティ

サーバ等、電算室等、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）　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。

（６）　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。

（７）　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正に対応するため、緊急時対応計画を策定する。

（８）　外部サービスの利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（９）　評価・見直し

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し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

# 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。

# 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。

# 11　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の非公開

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、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。