山ノ内町行政情報セキュリティポリシー

目次

平成 16 年制定	
平成 28 年改訂	
令和 6 年 6 月改訂	
令和 8 年 3 月改訂	

序　山ノ内町行政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、山ノ内町の情報資産に対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文書を総称する。情報セキュリティポリシーは、山ノ内町の情報資産に関する業務に携わる職員等、及び外部委託業者に浸透、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。

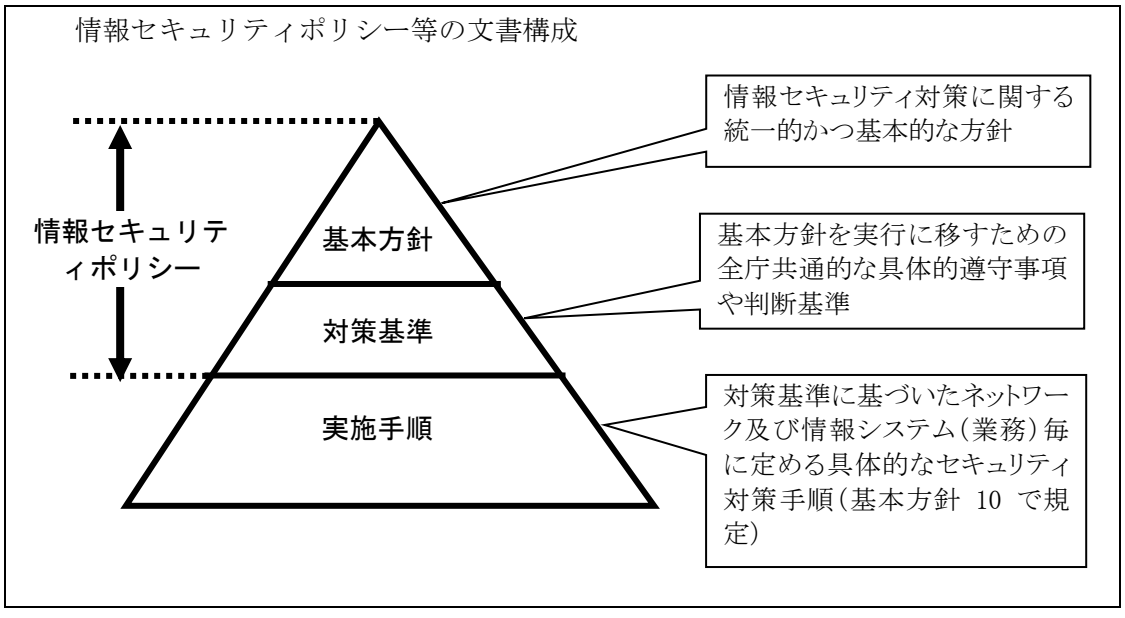
このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）の 2 階層に分けて策定することとした。

（1）　情報セキュリティ基本方針

山ノ内町としての情報セキュリティ対策に関する取り組み姿勢及び統一的な方針。

（2）　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山ノ内町におけるすべてのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。



第１章　情報セキュリティ基本方針

１　目的

山ノ内町の情報資産には、町民の個人情報をはじめ行政運営に必要な情報など、部外に漏洩、あるいは滅失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。これらの情報資産を人的脅威や災害、事故等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必要不可欠であり、ひいては、行政に対する町民からの信頼の維持向上に寄与するものである。

このため、山ノ内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の対策を整備することを目的として、山ノ内町行政情報セキュリティポリシー（以下、情報セキュリティポリシーという。）を定め、情報セキュリティの確保に最大限取り組むものである。

このうち情報セキュリティ基本方針は、山ノ内町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるとともに、総務省が策定した「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又は変更に関する指針（案)」を踏まえて、山ノ内町のサイバーセキュリティを確保するための方針として定めるものとする。

２　用語の定義

（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）　庁内ネットワーク

ネットワークのうち、山ノ内町役場、出先機関等の事務室等で使用されるコンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

（３）　外部ネットワーク

ネットワークのうち、庁内ネットワーク以外のものをいう。

（４）　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。

（５）　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並びに業務で使用する書類、帳票等をいう。

（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）　機密性

情報にアクセスすることを認められた者だけがアクセスできること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。

（１０）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。

（１１）LGWAN 接続系

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（マイナンバー利用事務系を除く。）。

（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及びその情報システムで取り扱うデータをいう。

（１３）通信経路の分割

LGWAN 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。

（１４）無害化通信

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。

（１５）情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、行政事務の運営を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

（１６）職員

地方公務員法で規定された特別職、一般職の中で、山ノ内町役場に勤務する者（非常勤職員及び臨時職員等を含む。）の総称をいう。

（１７）関係機関の職員等

各種委員会、議会事務局、福祉施設等に勤務し、山ノ内町が管理する情報資産を職務で利用する者（非常勤職員及び臨時職員等を含む。）の総称をいう。

（１８）職員等

山ノ内町が管理する情報資産を職務で利用する職員、臨時・非常勤職員等の総称をいう。

（１９）外部委託者

職務委託先社員（地方自治法（昭和 22 年法律第 67 号）第 244 条の 2 第 3 項に規定する指定管理者を含む。）等、契約に基づいて山ノ内町の機関で作業する者の総称をいう。

（２０）部外者

職員等及び外部委託者以外の山ノ内町の情報資産に接することが認められていない者の総称をいう。

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、水道水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

情報セキュリティポリシーの適用範囲は、次の各号に定めるものとする。

（１）　行政機関の範囲

情報セキュリティポリシーの適用対象機関は下記のとおりとする。

① 町長の事務部局
② 議会、議会事務局
③ 公営企業
④ 教育委員会
⑤ 選挙管理委員会
⑥ 監査委員
⑦ 農業委員会
⑧ 固定資産評価審査委員会

（２）　適用資産の範囲

情報セキュリティポリシーの適用対象資産は、山ノ内町役場、出先機関等の事務室等における全ての情報資産とする。

（３）　適用対象者

情報セキュリティポリシーの適用対象者は、前項に規定する適用資産に接する全ての職員等とする。

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

山ノ内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

山ノ内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実施する。

（３）　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、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、都道府県及び市区町村のインターネットとの通信を集約した上で、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、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、物理的な対策を講ずる。

（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、全ての職員等に対して情報セキュリティポリシーの内容を周知徹底する等、教育、訓練、啓発等を実施し、外部委託者に対して情報セキュリティポリシーの内容のうち必要となる部分を周知徹底する。

（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、業務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）　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、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、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。

外部サービス（クラウドサービス）を利用する場合には、利用に係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、適宜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ものとする。

なお、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山ノ内町の行政運営に重大な支障を及ぼすおそれのある情報であることから非公開とする。