中之条町
情報セキュリティポリシー

平成15年９月16日	策定
平成27年８月４日	全部改定
令和４年２月28日	全部改定
令和４年７月25日	一部改定
令和５年５月25日	一部改定
令和７年３月３日	一部改定
令和７年12月１日	一部改定

地域共創課

序　文

中之条町情報セキュリティポリシーとは、町が保有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る。

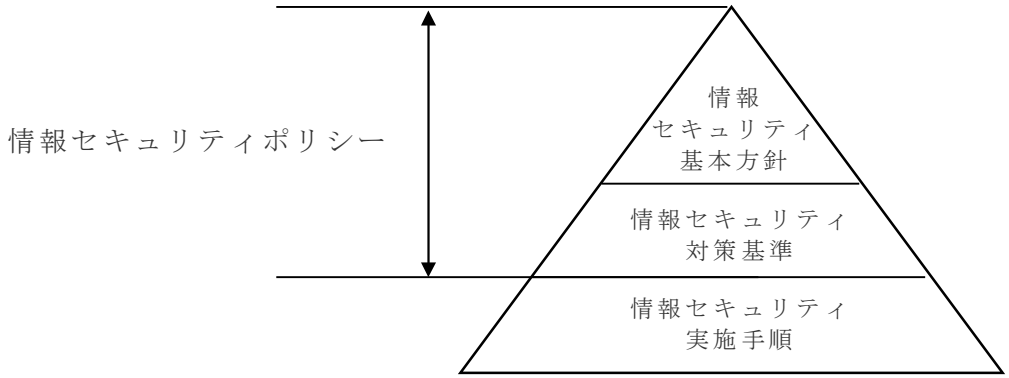
情報セキュリティポリシーは、町が保有する情報資産に携わる職員、委託事業者等にも浸透、普及、定着されるものであり、安定的な規範であることが求められ、一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーは、町の情報セキュリティ対策に関する統一的かつ基本的な方針を定めた「情報セキュリティ基本方針」（以下「基本方針」という。）と、基本方針を実行に移すための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である「情報セキュリティ対策基準」の２階層で構成し策定するものとする。

また、具体的な手順を定めた「実施手順」を、必要により、別途、策定するものとする。

中之条町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	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	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



中之条町情報セキュリティ基本方針

（目的）

第１条　中之条町（以下「町」という。）においては、効率的で効果的な町政を実現するため、情報通信技術を活用した多様な情報システムを活用しており、さらに今後は行政のオンラインサービス化も増加していく見込みである。これらの各情報システムが取り扱う情報には、行政運用上の情報や町民の個人情報などの重要な情報などが含まれている。したがって、これらの情報及び各情報システムを人的、災害その他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、また、行政事務の安定的な運営のためにも必要不可欠である。

そのため、町が実施する情報セキュリティ対策に関する基本的な事項を定め、サイバー攻撃等の様々な脅威から、町が保有する情報資産の機密性、安全性及び可用性を維持することを中之条町情報セキュリティ基本方針（以下「基本方針」という。）の目的とする。

また、全ての職員は、町が保有する情報資産に対する脅威への対応が重大かつ喫緊の課題であることを改めて認識し、町における情報セキュリティ対策の推進に積極的に取り組むこととする。

本基本方針は、地方自治法に規定する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である。

（定義）

第２条

（１）　コンピュータ

パソコン、サーバ、ストレージ等の機器をいう。

（２）　ネットワーク

コンピュータ等の電子計算機器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）をいう。

（３）　情報システム

町の運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュー

タのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記憶媒体等の仕組みをいう。

（４） 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。

（５） 完全性

情報が破壊、改ざん消去又は不正なデータがない状態を維持し、データの正当性、正確性、一貫性等を確保した完全な状態のことをいう。

（６） 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、対象の情報にアクセスできる状態を確保することをいう。

（７） 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。

（８） 情報セキュリティポリシー

基本方針及び情報セキュリティ対策基準をいう。

（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。以下「マイナンバー法」という。）第２条に規定する、個人番号をその内容に含む個人情報をいう。

(10) マイナンバー利用事務系（個人番号利用事務）

マイナンバー法に定められている個人番号利用事務（社会保障、地方税又は防災に関する特定の事務）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

マイナンバー利用事務系を除いた、ＬＧＷＡＮに接続された情報システム及び情報システムで取り扱うデータをいう。

(12) インターネット接続系

ＬＧＷＡＮ接続系を除いた、電子メール、Ｗｅｂサイト管理システム、内部事務を取り扱う情報システム等の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ない等、安全が確保された通信をいう。

(15)　ソーシャルメディアサービス

インターネット上で展開される情報メディアであって、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアである、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のサービスをいう。

（対象とする脅威）

第３条　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ほか、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応する。

（１）　人による脅威（故意）

不正アクセス、ウイルス攻撃、ランサムウェア攻撃、サービス不能攻撃等のサイバー攻撃、機器の盗難、対象の情報資産の不正な操作や持ち出し等の故意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、サービス及び業務停止の他、内部管理の欠陥など職員による不正行為等

（２）　人による脅威（過失）

情報資産の管理不備、無許可ソフトウェアの使用等の規定違反、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、委託管理の不備、マネジメントの欠陥、機器故障、メールの誤送信等の過失による情報資産の漏えい・破壊・消去、重要情報の詐取、サービス及び業務の停止、不正行為等

（３） 災害による脅威

地震、落雷、火災、水害等の災害によるサービス及び業務の停止、情報資産の消失等

（４） 必要資源の不足、故障等による脅威

災害の影響又はその他の原因による電力、通信、水道の途絶、交通機能のまひや大規模・広範囲にわたる疾病のまん延による要員不足、機器の故障等によるサービスや業務の停止、システム運用の機能不全等

（適用範囲）

第４条　行政機関の適応範囲

基本方針が適用される行政機関は、町長部局、教育委員会（小・中学校を除く。）、議会、選挙管理委員会、農業委員会、固定資産評価審査委員会、監査委員及び地方公営企業とする。

２　情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

（１） ネットワーク及び情報システム並びにこれらに関する設備及び磁気的記録媒体

（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

（職員の遵守義務）

第５条　職員（常勤職員、再任用時短勤務職員及び会計年度任用職員並びに労働者派遣事業により町の事務に関わる者をいう。以下同じ。）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。

（情報セキュリティ対策）

第６条　第３条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

を講じるものとする。

（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、当該分類に基づく情報セキュリティ対策を講じる。

（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、業務の効率化・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

ア　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出来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。

イ　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する業務システムと、インターネット接続系の情報システムとの通信経路の分割する。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。

ウ　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。また、高度なセキュリティ対策として、都道府県及び市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

サーバ等、情報システムの設置箇所、通信回線及び職員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及び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及び外部委託を行う際の情報セキュリティの確保等、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、町の業務の根幹となる住民情報や特定個人情報ファイルを取り扱うシステム等、特に重要な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、基幹システム及び特定個人情報を取り扱うシステム等について、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）を利用する場合においても、利用にかかる規定の整備等、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。

（９） ソーシャルメディアの活用

ソーシャルメディアサービスを利用する場合には、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。

(10) 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実施する。

（情報セキュリティ監査及び自己点検の実施）

第７条 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。

（情報セキュリティポリシーの見直し）

第８条　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。

（情報セキュリティ対策基準の策定）

第９条　第６条から前条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。なお、情報セキュリティ対策基準は、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恐れがあることから非公開とする。また、委託事業者の契約等により情報セキュリティ対策基準の遵守を求める場合は開示するものとする。

（情報セキュリティ実施手順の策定）

第10条　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。