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

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、本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。

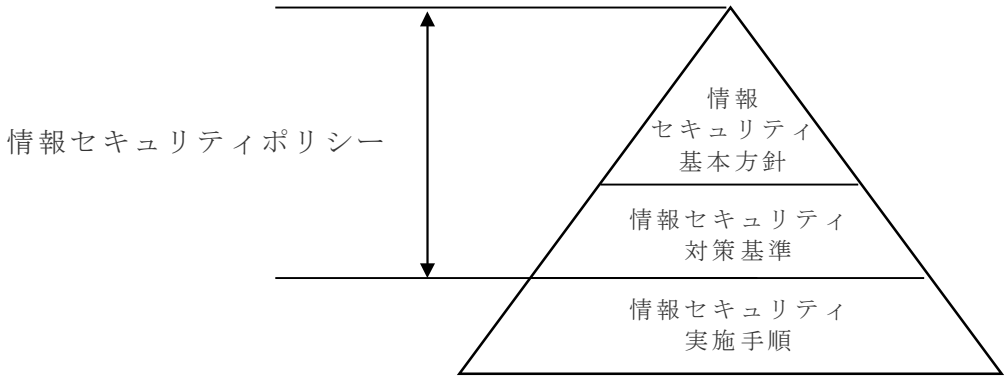
情報セキュリティポリシーは、本町が保有する情報資産に携わる職員、委託事業者等にも浸透、普及、定着されるものであり、安定的な規範であることが求められ、一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーは、本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　中之条町情報セキュリティ基本方針（以下「基本方針」という。）は、本町が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産（以下「対象資産」という。）について、本町が実施する情報セキュリティに関する基本的な事項を定めることを目的とする。

（定義）

第２条　基本方針において、次に掲げる用語の意義は、当該各号に定めるところによる。

（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。

（３）　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。

（４）　情報資産

情報システムで取り扱う情報で、開発及び運用に係るものを含め全ての情報をいう。

（５）　情報セキュリティ

対象資産の機密性、完全性及び可用性を維持することをいう。

（６）　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。

（７）　機密性

対象資産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。

（８） 完全性

対象資産が破壊、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、一貫性等を確保することをいう。

（９） 可用性

対象資産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、対象資産にアクセスできる状態を確保することをいう。

(10) 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）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。

(11) 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。

(12) 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。）

(13) インターネット接続系　インターネットメールや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。

(14) 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。

(15) 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。

（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。

（１）　人による脅威（故意）

不正アクセスやウイルス攻撃等のサイバー攻撃、機器の盗難、対象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、内部不正等

（２）　人による脅威（過失）

対象資産の管理不備、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、機器故障等の過失による情報資産の漏えい・破壊・消去等

（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　基本方針の適用範囲は、本町が保有する対象資産、対象資産に関する事務に携わる全ての職員（会計年度任用職員や労働者派遣事業により本町の事務に携わる者を含む。）（以下「職員等」という。）及び委託事業者とする。

（職員等の遵守義務）

第５条　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。

（情報セキュリティ対策）

第６条　第３条の脅威から対象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

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

（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、当該分類に基づく情報セキュリティ対策

（３） 情報システム全体の強じん性の向上

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は、原則として他の領域との通信不可。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

イ ＬＧＷＡＮ接続系は、インターネット接続系との通信経路の分割。両システム間で通信する場合には、無害化通信を実施

ウ インターネット接続系は、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。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する自治体情報セキュリティクラウドの導入等を実施

（４） 物理的セキュリティ

対象資産の設置方法又は保管施設の管理について物理的な対策

（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

（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

（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、対象資産へ侵害が発生した場合等に、迅速かつ適切に対応するための

緊急時対応計画を策定

（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、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。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、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

（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、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選定

(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、情報セキュリティの向上、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

（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。

（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。

（公開）

第11条　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。