南部町情報セキュリティポリシー

南　部 町

令和８年３月３１日　一部改定

改定履歴

制定／改定	施行年月日	改定内容	
改定	平成２０年９月１日	改定	
改定	令和４年２月２日	改定	
改定	令和６年３月３１日	一部改定	
改定	令和８年３月３１日	一部改定	
	年　月　日		
	年　月　日		
	年　月　日		
	年　月　日		
	年　月　日		
	年　月　日		
	年　月　日		
	年　月　日		

はじめに

○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、南部町が所掌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、体系的及び具体的に取りまとめたものを総称する。情報セキュリティポリシーは、南部町が所掌する情報資産に関する業務に携わる全職員（会計年度任用職員を含む。以下「職員等」という。）に浸透、普及及び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（以下「情報セキュリティ基本方針」という。）と情報資産を取り巻く状況の変化に依存する部分（以下「情報セキュリティ対策基準」という。）に分けて策定することとした。また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の「情報セキュリティ実施手順」を策定することとする。

情報セキュリティポリシーの構成

文書名		内容
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全ての情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

第１章　情報セキュリティ基本方針

１．目的

本基本方針は、本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、本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。本町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上重要な情報など、外部に漏えい等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。したがって、これらの情報及び当該情報を取り扱う情報システムを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。ひいては、このことが、本町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。また、デジタル社会の進展に伴い、行政サービスの提供が情報システムやネットワークに強く依存している現状を踏まえ、本町が管理しているすべての情報システムが高度な安全性を有することは、住民生活や地域の社会経済活動を保護するための不可欠な前提条件である。そのため、本町の情報資産の機密性、完全性及び可用性を維持するための対策(以下「情報セキュリティ対策」という。）をするため、南部町情報セキュリティポリシーを定めることとする。

このうち、情報セキュリティ基本方針においては、本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ものとする。さらに、本町はサイバー攻撃、内部不正、災害、システム障害、外部委託先の不備その他の脅威に対応し、行政サービスの継続性を確保するため、国の統一基準群の改定や技術動向を踏まえつつ、必要な情報セキュリティ対策を継続的に強化するものとする。

なお、本基本方針は、地方自治法第244条の6第3項の規定に基づき策定される「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」に沿ったものとして位置付ける。

また、本基本方針は、南部町の執行機関及び議会が共同して策定するものである。

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（ハードウェア及びソフトウェア）、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、改ざんまた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。
（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）また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
　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。）。
(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
　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。
(12) 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。

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）行政機関の対象範囲
　本基本方針が適用される行政機関は、町長部局、内部部局、行政委員会（教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会）及び地方公営企業とする。なお、議会は執行機関ではないが、本基本方針の適用対象とする。
（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。
　ア　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電磁的記録媒体
　イ　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。）

ウ　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

（３）対象とする主体

本基本方針は、町長部局、議会事務局、教育委員会事務局、選挙管理委員会、監査委員事務局、農業委員会事務局、固定資産評価審査委員会及び地方公営企業に適用する。また、業務委託先、指定管理者及び再委託先についても、本町と同等の情報セキュリティ対策を講じることを求める。また、本基本方針は、これらの機関に属する職員、会計年度任用職員、非常勤職員に加え、議員及び各種委員（教育委員、選挙管理委員、監査委員、農業委員、固定資産評価審査委員等）にも適用する。

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、本基本方針、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を遵守しなければならない。また、議員及び各種委員（教育委員、選挙管理委員、監査委員、農業委員、固定資産評価審査委員等）も、執行機関としての責務に基づき、本基本方針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

本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

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。

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。

イ　LGWAN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。

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。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、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、緊急時における連絡体制や対応手順等の整備に努める。さらに、情報セキュリティインシデントが発生した場合には、被害の拡大防止、速やかな復旧及び再発防止のための措置を講じるものとする。

（８）業務委託と外部サービス（クラウドサービス）の利用

業務委託する場合には、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。また、再委託（二以上の段階にわたる委託を含む。）が行われる場合においても、委託事業者を通じて適切な監督及び指導を行うものとする。

外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し適切な設定及び管理を行うなど、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、定期的または必要に応じて、外部の視点を取り入れた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。また、監査及び自己点検の結果を踏まえ、必要に応じて情報セキュリティポリシー及び関連規程の不断の見直しを行うものとする。

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、定期的また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。監査及び自己点検の結果は、必要に応じて本基本方針及び情報セキュリティ対策基準の見直しに反映するものとする。

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（国の動向、最新の技術や脅威、DXの進展等）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ものとし、不断の改善に努める。

９．方針の公表

本基本方針を策定又は変更した際は、情報セキュリティ対策の実効性や透明性の

維持・向上を図るため、速やかに町民に公表するものとする。

１０．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。

１１．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。