

南大東村情報セキュリティ基本方針

(第 4.0 版)

制定日：平成 15 年 9 月

改正日：令和 8 年 3 月 31 日

施行日：令和 8 年 4 月 1 日

南大東村

改訂履歴

施行年月日	版番号	改訂理由・内容
平成 15 年 9 月	第 1.0 版	初版発行
平成 30 年 10 月	第 2.0 版	情報セキュリティガイドライン改訂に伴う機微修正
令和 4 年 2 月	第 3.0 版	情報セキュリティガイドライン改訂に伴う機微修正
令和 8 年 3 月 31 日	第 4.0 版	情報セキュリティガイドライン改訂に伴う見直し。昨今の IT 情勢に合わせて定義追加、セキュリティポリシーの位置付けを章内に組み込み
年 月 日		
年 月 日		
年 月 日		

目次

- 1 目的
- 2 定義
- 3 情報セキュリティポリシーの位置付け及び構成
- 4 対象とする脅威
- 5 適用範囲
- 6 職員等の順守義務
- 7 情報セキュリティ対策
- 8 情報セキュリティ監査及び自己点検の実施
- 9 情報セキュリティポリシーの見直し
- 10 情報セキュリティ対策基準の策定
- 11 情報セキュリティ実施手順の策定

1 目的

本村の情報システムが取り扱う情報には、住民の個人情報や行政運営上の重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等の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る。

このために、本村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ことを目的として南大東村情報セキュリティ基本方針を定める。南大東村の情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものである。

2 定義

用語	定義
電子計算機	ハードウェア及びソフトウェアで構成するコンピュータをいう。また、電子計算機のうち、職員等が情報処理を行うために直接操作する機器を端末といい、そのうち、必要に応じて移動させて使用することを目的として導入したものをモバイル端末という。また、モバイル端末のうち、庁舎内と同様の汎用的業務を庁舎外で行うために使用するものをテレワーク端末という。
ネットワーク	電子計算機等を相互に接続するための通信回線及びその構成機器（ハードウェア及びソフトウェア）をいう。
情報システム	電子計算機、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。 情報システムが接続するネットワークには、マイナンバー（個人番号）利用事務系ネットワーク、LGWAN接続系ネットワーク、インターネット接続系ネットワークがある。
電磁的記録媒体	電子計算機に使用される磁気ディスク、磁気テープ、光ディスク、フラッシュメモリその他これらに類する媒体をいう。また、記録媒体のうち、取り外し可能で持ち出しが可能なものを外部記録媒体という。
データ	電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、光ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。
マイナンバー利用事務系ネットワーク	個人番号利用事務（社会保障、地方税も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。

LGWAN 接続系ネットワーク	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）。
インターネット接続系ネットワーク	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。
情報資産	本村の行政事務の執行に関わる情報で、情報システムで取り扱うものをいう。（入出力帳票及び情報システム仕様書及びネットワーク図等を含む。） ただし、情報資産を外部へ提供した場合や IC カード等に情報資産を記録したものを住民に交付する等により、当該情報の管理責任が本村から離れたものを除く。
特定用途機器	テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵の記録媒体を備えているものをいう。
RPA	ロボティック・プロセス・オートメーション（以下「RPA」という。）はこれまで人間が行ってきた定型的な処理等をソフトウェアのロボットにより自動化するものをいう。
外部サービス	外部サービスとは、外部の事業者が提供するサービスの総称であり、調達の形態が利用料金の有料・無料を問わず、以下のものをいう。 ア 委託による外部サービス ・本村の業務を外部の事業者に委託することにより調達する外部サービスのことをいう。 ・事業者が定める約款（利用規約等）への同意のみによって利用可能となるサービスのことをいう。 イ 約款に特約等を付して調達する外部サービス ・事業者が定める約款に取扱う行政情報の保護に関する特約等を付加し、利用するサービスのことをいう。 ウ 国や LGWAN-ASP により提供される外部サービス ・国が提供するサービスのほか、地方公共団体情報システム機構（以下、J-LIS という。）等が

	LGWAN を通じて地方公共団体向けに提供するサービスのことをいう。
クラウドサービス	データやソフトウェアをネットワーク経由でサービスとして利用者に提供するものをいい、主に仮想化技術により実現されているものをいう。
仮想化技術	サーバなどのハードウェア資源（CPU、メモリ、ディスクなど）を抽象化し、物理的な制限にとらわれず、ソフトウェア的に統合・分割できるようにする技術のことをいう。
テレワーク	情報通信技術（ICT = Information and Communication Technology）を活用した、勤務場所にとらわれない柔軟な働き方のことをいう。
情報セキュリティ	情報資産の機密性、完全性及び可能性を維持することという。
情報セキュリティポリシー	南大東村情報セキュリティ基本方針（以下「情報セキュリティ基本方針」という）及び南大東村情報セキュリティ対策基準（以下「情報セキュリティ対策基準」という）をいう。
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という。
完全性	情報及び処理の方法の正確さ、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という。
可用性	情報にアクセスすることを認められた者が、必要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という。
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という。
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。
ソーシャルメディア	ブログ、ソーシャルネットワーキングサービス（SNS）、動画共有サイト等、利用者が情報を発信し、形成していくメディアのことをいう。

3 情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは、本村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かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり、情報セキュリティ基本方針及び情報セキュリティ対策基準から構成される。

情報セキュリティ対策基準は、情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために最低限必要な水準として、職員、再任用職員、任期付職員、臨時的任用職員、会計年度任用職員、特別職非常勤職員、労働者派遣契約等により本村業務に従事する者（以下「職員等」という。）が順守すべき事項及び判断基準をまとめたものである。本村では、組織等の状況に合わせた情報セキュリティ対策基準を策定する。

また、情報セキュリティポリシーに基づく具体的な手順を示す「情報セキュリティ実施手順」として全庁的に共通する情報資産の取扱いを定める実施手順と、管理する情報システム毎の取扱いを定める実施手順を策定するものとする。

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に基づき、情報セキュリティ対策を実施するための、全ての情報資産に共通の遵守事項・判断基準。
情報セキュリティ実施手順		全庁的に共通する情報資産の取扱いを定める実施手順と、管理する情報システム毎の取扱いを定める実施手順。

4 対象とする脅威

情報セキュリティ対策を講じるうえでは、情報資産に対する脅威の発生度合いや発生した場合の影響度を考慮するものとする。特に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、業務委託等の管理の不備、マネジメントの欠陥、機器故障等の非意図的の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、洪水、津波等の災害によるサービス及び業務の停止等

- (4) 大規模・広範囲によ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

5 適用範囲

(1) 組織の範囲

村長(南大東村課設置条例(平成8年条例第7号)第1条に規定する課及び会計課)、教育委員会、監査委員、選挙管理委員会、農業委員会、固定資産評価審査委員会、議会事務局及び公営企業管理者等とする。

(2) 情報資産の範囲

本村のネットワーク、情報システム並びにこれらに関する設備、電磁的記録媒体及び情報資産をいう。

6 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つとともに、情報資産の利用及び業務の遂行にあたっては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。

7 情報セキュリティ対策

上記4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) 情報セキュリティ管理体制

本村の情報資産について、適切に情報セキュリティ対策を推進・管理するため、全庁的な組織体制を確立する。必要な体制、役割、権限等については情報セキュリティ対策基準にて定める。

(2) 情報資産の分類と整理

本村の保有する情報資産の機密性、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講じる。

(3) 情報システム全体の強靱性の向上

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、情報資産の分類に応じた情報セキュリティ対策を講じるとともに、次の対策も併せて講じる。

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、無害化通信を行う。

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

電子計算機室等への入退室、サーバ等の管理、通信回線及び端末等への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、十分な研修・訓練及び啓発を実施するなど人的な対策を講じる。

(6) 技術的セキュリティ

電子計算機等の管理、アクセス制御、コンピュータウイルス等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、業務委託等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切に対応するため、緊急時対応計画を策定する。

(8) 業務委託等及び外部サービス（クラウドサービス）の利用

業務委託等をする場合には、業務委託事業者等を選定し、情報セキュリティ要件を明記した契約を締結し、業務委託事業者等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。

8 情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況を評価するため、定期的及び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。

9 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な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。

10 情報セキュリティ対策基準の策定

上記、7、8及び9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村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。