小国町情報セキュリティーポリシー
情報セキュリティ基本方針

第３版

令和７年３月改訂

平成１５年３月初版

目　　次

１　目的

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、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、近年のいわゆるＩＴ革命の進展により、電子政府や電子自治体の実現が期待されている中で、マイナンバー制度に伴う特定個人情報の保護等を実現するためには、ネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件となる。

このため、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を整備することを目的として、小国町情報セキュリティポリシーを定め、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、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。

２　用語の定義

（１）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、及び周辺機器をいう。

（２）ネットワーク

電子計算機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）庁内ネットワーク

ネットワークのうち、町役場本庁、出先機関、各委員会、議会事務局、教育機関、福祉施設、医療機関等で使用される電子計算機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。

（４）部署ネットワーク

庁内ネットワークのうち、特定の部署のみで使用されるネットワークをいう。

（５）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。

（６）情報システム

町の各種電子計算機（ネットワーク、ハードウェア及びソフトウェア）及び

電磁的記録媒体で構成され、処理を行う仕組みをいう。

（７）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。

（８）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。

（９）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。

（１０）完全性

情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

（１１）可用性

許可された利用者が必要なときに情報にアクセスできることを確実にすること。

（１２）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。

（１３）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。)。

（１４）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。

（１５）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。

（１６）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。

（１７）サイバーセキュリティ

サイバーセキュリティ基本法（平成２６年法律第１０４号）第２条に規定されるサイバーセキュリティをいう。

（１８）職員

地方公務員法で規定された特別職、一般職の中で、町に勤務する者の総称を

いう。
（１９）関係機関の職員等
　各委員会、議会、福祉施設、広域組合、医療機関に勤務し、町が管理する情報資産を職務で利用する者の総称をいう。
（２０）職員等
　町が管理する情報資産を職務で利用する職員及び関係機関の職員であって、それぞれ非常勤職員及び会計年度任用職員等を含む職員の総称をいう。
（２１）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、契約に基づいて町の機関で作業する者の総称をいう。
（２２）公共端末
　町の情報資産のうち、町の施設等に設置され、町民などが自由に操作する端末の総称をいう。
（２３）部外者
　職員等及び外部委託者以外の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　情報セキュリティポリシーの位置付け
　情報セキュリティポリシーは、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、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。また、サイバーセキュリティ基本法第５条に規定される地方公共団体の責務、その他の法令の規定に基づき地方公共団体が実施すべき施策を町において実施するための拠り所と位置付けられるものである。

４　情報資産への脅威
　情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。
（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

５　情報セキュリティポリシーの対象範囲

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）適用資産

情報セキュリティポリシーの適用対象資産は、小国町の行政機関における全ての情報資産とする。

（２）行政機関の範囲

情報セキュリティポリシーが適用される行政機関は、内部部局、行政委員会、議会、消防小国分署、地方公営企業とする。

（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、第１号に規定する適用資産に接する全ての職員等とする。

６　職員等の遵守事項

町が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託者は、情報セキュリティの重要性について共通の認識をもつとともに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するものとする。

７　情報セキュリティ対策

小国町の情報資産を４に示した脅成から保護するために、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

町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・管理するための体制を確立する。

（２）情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行う。

（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。

② 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。

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、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対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（５）人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めるとともに、全ての職員等及び外部委託者に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、啓発等を実施する。

（６）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理、不正プログラム対策等を実施する。

（７）運用

情報セキュリティポリシーの実効性を確保するため、また、不正なアクセス等から適切に保護するため、システム開発等の外部委託、システムの管理、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面における必要な措置を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

（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。

８　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的又は必要に応じて監査及び自己点検を実施する。

９　評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

１０情報セキュリティ対策基準の策定

町の様々な情報資産について、７、８及び９の情報セキュリティ対策を講ずるに当たっては、職員等が遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した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を遵守して情報セキュリティ対策を実施するために、情報セキュリティ対策基準の基本的な要件に基づき、情報セキュリティ実施手順を策定する。

１２情報セキュリティポリシーの情報公開

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町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。