

豊山町情報セキュリティ基本方針

改訂履歴

年月日	改定内容等
令和8年4月1日	初版改訂（令和8年4月1日施行）

豊山町情報セキュリティ基本方針

(目的)

第1条 豊山町情報安全対策指針（以下「指針」という。）は、本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ることにより、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ことを目的とする。

(定義)

第2条 指針において、次の各号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) 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。

(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) 情報資産 指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等を含む。）

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

(4) 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。

(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、改ざん又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) LGWAN 地方公共団体を相互に接続する行政専用の総合行政ネットワークをいう。

(9) 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、地方税又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。

(10) 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）。

(11) 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。

(12) 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。

(13) 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。

(14) クラウドサービス 事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

(15) LGWAN-ASP 行政専用のセキュアなネットワークであるLGWANを利用して、高度な品質のサービス及びリソースを地方公共団体間で共同利用することにより、地方公共団体のIT化の促進、IT活用格差等の解消、システムの導入及び運用の経済性を実現する各種行政事務サービスを提供するものをいう。

(16) 情報セキュリティインシデント 望ましくない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(17) 情報セキュリティ事象 指針への違反若しくは管理策の不具合の可能性又はセ

セキュリティに関係し得る未知の状況を示すシステム、サービス又はネットワークの状態に関連する事象をいう。

(18) 電磁的記録媒体 コンピュータによる情報処理に使用する電子的又は電磁的な記録方式により作成された記録を保持するための媒体。ハードディスク、CD、DVD、USBメモリ、SDカード、コンパクトフラッシュ、フロッピーディスク、磁気テープ類等をいう。

(19) 電算室 重要な情報システム及びネットワークの基幹機器を設置し、当該機器等の管理並びに運用を行うための部屋をいう。

(20) 部局等の長 豊山町部設置条例(昭和61年豊山町条例第5号)で定める部の長、豊山町教育委員会事務局組織規則及び豊山町議会事務局処務規程(平成19年豊山町議会訓令第1号)で定める事務局長をいう。

(21) 課等の長 豊山町行政組織規則及び豊山町会計課設置規則で定める課長及び出先機関の長をいう。

(22) 外部 第4条に規定する適用範囲以外をいう。

(23) 個人情報 豊山町個人情報の保護に関する法律施行条例(令和5年条例第17号)第2条第2号に規定する個人情報をいう。

(24) 特定個人情報 豊山町個人情報の保護に関する法律施行条例(令和5年条例第17号)第2条第2号に規定する特定個人情報をいう。

(対象とする脅威)

第3条 情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施するものとする。

(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、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、設計又は開発の不備、プログラム上の欠陥、操作又は設定ミス、メンテナンス不備、内部又は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、機器故障等の非意図的な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) 大規模又は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(適用範囲)

第4条 指針が適用される範囲は、次のとおりとする。町長、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議会とする。ただし、豊山町立学校設置条例(昭和45年豊山町条例第15号)第2条に規定する小学校、中学校(以下「学校」という。)については、第1章のみを適用し、第2章以降については適用しない。

(職員等の遵守義務)

第5条 職員、会計年度任用職員等(以下「職員等」という。)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指針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条に規定する脅威から情報資産を保護するため、次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 本町の保有する情報資産について、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) 情報資産の分類及び管理 本町の保有する情報資産を重要性分類に応じて分類及び管理を行い、当該分類及び管理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、次の3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「知識」「所持」「存在」のうち二つ以上の要素を併用する認証（以下「多要素認証」という。）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の分割を行う。なお、両システム間で通信する場合は、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行う。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行う。

（４） 物理的セキュリティ サーバ及び通信機器、電算室、通信回線等の管理について、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、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な対策を講じる。

（７） 運用 情報システムの監視、指針の遵守状況の確認、業務委託を行う際のセキュリティ確保等、指針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 業務委託する場合は、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。

（９） 評価・見直し 指針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。情報セキュリティの見直しが必要な場合は、適宜指針の見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第7条 指針の遵守状況を検証するため、適時に情報セキュリティ監査及び自己点検を実施するものとする。

（指針の見直し）

第8条 情報セキュリティ監査及び自己点検の結果、指針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となった場合は、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、指針を見直す。

（実施手順の策定）

第9条 指針に基づき、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。