山北町

情報セキュリティポリシー

情報セキュリティ基本方針

令和８年４月１日

山北町

１ 目的

本基本方針は、本町が保有する行政情報の機密性、完全性及び可用性を維持し、安全で安心できる町の情報基盤の構築及び情報資産の維持・管理・運用を行うために実施する情報セキュリティ対策について定めることを目的とする。

２ 定義

（１）行政情報

①職員及び臨時職員（以下「職員等」という。）並びに外部委託事業者が職務上作成、取得した文書、図面及び電磁的記録等のデータファイル。

（２）ネットワーク

①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)。

（３）情報システム

①コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組み及びその構成機器(ハードウェア及びソフトウェア)。

（４）情報資産

①ネットワーク、情報システムで取り扱う全てのデータファイル並びに管理・運用する仕組み及びその構成機器(ハードウェア及びソフトウェア)。

（５）情報セキュリティ

①行政情報及び情報資産の機密性、完全性及び可用性を確保、維持すること。

（６）データファイル

①情報システムに電磁的に記録されたもの及び記録媒体に記録されたもの。

（７）記録媒体

①データファイルを記録するための媒体。例えば、磁気テープやフロッピーディスク、ハードディスク、ＵＳＢメモリ等。

（８）機密性

①行政情報の重要度等により、その行政情報及び情報資産へアクセスすることが認められた者だけが、アクセスできるようにすること。

（９）完全性

①不正アクセス・不正プログラム等により行政情報及び情報資産が破壊、改ざん又は消去されない状態とし、正しい行政情報を取得・利用できるようにすること。

（10）可用性

①行政情報及び情報資産への認められたアクセスが、中断されることなく、アクセスできる状態にすること。

（11）マイナンバー利用事務系（個人番号利用事務系）

①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。

(12) LGWAN 接続系

①LGWAN 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（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

①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。

(14) 通信経路の分割

①LGWAN 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。

(15) 無害化通信

①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。

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、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）行政機関の範囲

①本基本方針が適用される行政機関は、町長部局、各行政委員会（教育委員会、選挙管理委員会、監査委員、農業委員会及び固定資産評価審査委

員会）及び議会とする。

（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。

①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

②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。）

③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

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情報セキュリティポリシー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

①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

①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。

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。

②LGWAN 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、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

①サーバ、電算機械室、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

①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

①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

①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

①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。

②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。

③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

①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。

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。

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。