舟形町情報セキュリティポリシー

基本方針

令和８年３月

舟形町

【目次】

1. 目的

本基本方針は、地方自治法（昭和 22 年法律第 67 号）第 244 条の６第１項の規定に基づき、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。

また、個人情報の保護に関する法律（平成 15 年法律第 57 号）、サイバーセキュリティ基本法（平成 26 年法律第 104 号）及びデジタル社会の形成を図るための関係法律の整備に関する法律（令和３年法律第 37 号）の趣旨を踏まえ、町民の個人情報及び行政運営上重要な情報を適切に保護し、もって町民の信頼の維持向上に資することを目指す。

2. 定義

本基本方針において、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）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、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） 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。

（9）LGWAN 接続系

LGWAN（総合行政ネットワーク）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及びインターネット接続系の業務用システムを除く。）。

（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、及び財務会計、人事給与、文書管理等の業務用システム（クラウドサービスとして提供されるものを含む。）並びに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。なお、インターネット接続系に配置された業務用システムについては、高度なセキュリティ対策を講じた上で、LGWAN 経由の通信を可能とする。
（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。
（13）クラウドサービス
　事業者等が保有する情報システム（サーバ、ストレージ、アプリケーション等）をネットワーク経由で利用するサービスをいう。

3. 対象とする脅威
　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。
（1）不正アクセス、ウイルス攻撃、サービス不能攻撃、標的型攻撃、ランサムウェア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、重要情報の詐取及び不正等
（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及び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、水害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、通信の途絶及び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
　本基本方針が適用される行政機関は、町長部局、教育委員会事務局、議会事務局、農業委員会事務局、選挙管理委員会事務局、監査委員事務局及び地方公営企業とする。
（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

町長、副町長、教育長、職員及び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。

また、職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合には、速やかに所属長及び情報システム管理者に報告し、必要な措置を講じなければならない。

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。具体的には、最高情報セキュリティ責任者（CISO）、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者等を配置し、役割と責任を明確にする。

（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。情報資産は、その重要度に応じて適切なアクセス制御、暗号化、バックアップ等の措置を講じる。

（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 を経由した国・他自治体との情報連携を行う情報システムを配置する。

③インターネット接続系においては、次の対策を講じる。

ア インターネットメール、ホームページ管理システム等の外部公開系システムについては、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。

イ 財務会計、人事給与、文書管理等の業務用システムについては、クラウドサービスとして提供されるものを含め、インターネット接続系に配置することができる。この場合、次の対策を講じる。

（ア）情報資産単位でのアクセス制御

（イ）通信の暗号化（TLS1.2 以上）

（ウ）エンドポイント保護（EDR 等の導入）

（エ）ログの取得・監視・分析

（オ）定期的な脆弱性診断

（カ）データのバックアップ

（キ）インシデント対応体制の整備

ウ LGWAN 接続系との通信が必要な場合は、通信経路の分割を行った上で、必要最小限の通信のみを許可する。

（4）物理的セキュリティ

サーバ、電算室、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。具体的には、入退室管理、機器の固定、施錠管理等を実施する。

（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。定期的な研修、標的型メール訓練、情報セキュリティに関する意識向上のための取組を実施する。

（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、脆弱性対策、ログ管理、暗号化、多要素認証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、緊急時対応計画（インシデント対応計画）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、委託事業者を適切に選定し、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。クラウドサービスの利用に当たっては、クラウドバイデフォルト原則を踏まえ、セキュリティ、可用性、事業者の信頼性等を総合的に評価した上で選定する。

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

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。

情報セキュリティ監査は、年１回以上実施するものとし、監査結果については最高情報セキュリティ責任者に報告し、必要な改善措置を講じる。

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。

また、地方自治法第 244 条の６第２項の規定に基づき、本基本方針を変更したときは、遅滞なく、これを公表する。

9. 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。

情報セキュリティ対策基準は、総務省が策定する「地方公共団体における情報セキュリティポリシーに関するガイドライン」に準拠して策定する。

10. 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、情報セキュリティポリシー及び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。ただし、本基本方針については、地方自治法第 244 条の６第２項の規定に基づき公表する。

【附則】

この基本方針は、令和８年３月２日から施行する。