隠岐の島町
サイバーセキュリティを確保するための方針

策定日: 令和 8 年 3 月 16 日

隠岐の島町 総務課

目次

1　方針策定の目的と背景

本町は日本海上に位置する離島であり、本土との通信インフラの制約や、台風・津波等の自然災害による孤立リスクを抱えている。本方針は、これらの地理的特性を踏まえ、住民の個人情報（マイナンバー等)、観光・水産業等の地域重要情報、および防災情報を守り、安全で安定した行政サービスを継続することを目的とする。

なお、本方針は地方自治法第 244 条の 6 に基づき策定するものであり、総務大臣指針に則り、住民に対して公表するものとする。

2　推進体制の確立

町のセキュリティ対策を全庁的に推進するため、以下の体制を確立し運用する。

- **最高情報セキュリティ責任者（CISO）**

  副町長を充て、対策の統括と重要事項の意思決定を行う。

- **情報セキュリティ統括責任者**

  総務課長を充て、実務的な推進を指揮し、CISO を補佐する。

- **情報セキュリティ委員会**

  原則として四半期に 1 回開催し、全課長が参画して組織的な意思統一を図る。

  - **外部専門家との連携**

    離島における専門人材確保の課題を補うため、島根県や外部専門機関との連携体制を構築する。

- **CSIRT（情報セキュリティ対応チーム）**

  平時の情報収集および有事の連絡窓口として CSIRT を設置し、島根県、警察、J-LIS 等の外部機関との連携を強化する。

3　重要施策（重点対策事項）

3.1　離島特性を踏まえた強靭なインフラ構築

- **通信回線の冗長化**

  本土との通信において、有線回線（光ファイバー）に加え、無線回線（LTE、衛星通信）を確保し、単一障害点（SPOF）を解消する。

  また、庁内無線 LAN においては、クライアント証明書認証による厳格な接続制御を実施するとともに、ネットワーク機器の調達にあたってはセキュリティ適合性（JC-STAR 等）を確認する。

- **災害対策（BCP）の強化**

  津波等の災害を想定し、サーバ室の設置場所を検討するとともに、停電に備えた非常用電源の確保を行う。

- **データの遠隔地バックアップ**

  島内でのバックアップに加え、大規模災害に備えて重要データを本土（島外）またはクラウドへ定期的にバックアップする。

  また、ランサムウェア等のサイバー攻撃に備え、国ガイドラインに基づき、バックアップ

データの一部はネットワークから切り離した状態（オフライン）での管理を実施する。

3.2 「三層の対策」による技術的防御

情報システムを以下の 3 つに分離し、それぞれの重要度に応じた対策を講じる。

- **マイナンバー利用事務系**

  他のネットワークから原則分離し、端末からの情報持ち出し不可設定や多要素認証を徹底する。

- **LGWAN 接続系**

  インターネット接続系との通信経路を分割し、無害化通信（メール本文のテキスト化等）を導入する。

  （なお、業務効率化のため、特定クラウドサービスへの直接接続（α'モデル）の導入を検討する）

- **インターネット接続系**

  不正通信の監視やマルウェア対策、Web フィルタリング等の高度な対策を実施する。

3.3 情報資産の適正な管理

- **資産分類の徹底**

  全ての情報を機密性（3A, 3B, 3C, 2, 1）に基づいて分類し、特に機密性 3A（特定個人情報）は最高レベルの管理を行う。

- **持ち出し制御**

  情報の持ち出しは原則禁止とし、やむを得ない場合は「情報持出し申請書」による事前承認と、暗号化等のセキュリティ対策を義務付ける。

- **パスワード管理**

  パスワードは最低 12 文字以上とし、総務省ガイドラインおよび NISC 基準に基づき安全性を確保するため、流出時を除き定期的な変更は求めないものとする。

  また、多要素認証の導入を推奨する。

3.4 人的セキュリティと緊急時対応

- **職員研修の実施**

  全職員に対し年 1 回以上の定期研修を実施するほか、新任職員着任後 1 ヶ月以内の基礎研修受講を義務付ける。

  特に、台風時の通信途絶対応など、離島特有のシナリオを含めた教育を行う。

- **インシデント対応**

  インシデント発生時は、速やかに CISO（副町長）を中心とした対策本部を設置する。

  また、平時からの情報収集および緊急時の連絡窓口として CSIRT（Computer Security Incident Response Team）を整備し、島根県、警察、J-LIS 等の関係機関との連携体制を構築する。通信断絶時を想定し、衛星電話を用いた緊急連絡網を整備する。

4 運用と外部委託管理

- **クラウドサービスの利用**

政府情報システムのためのセキュリティ評価制度（ISMAP）登録サービス等の利用を検討し、利用申請書によるリスク評価を経て承認する。 機密情報の保存先国や外国法制リスクも評価対象とする。 機密情報の保存先国や外国法制リスクも評価対象とする。

- **生成 AI サービスの利用**

  業務における生成 AI サービスの利用については、別途「生成 AI 利用に関するガイドライン」を策定し、これに基づき運用する。

- **委託事業者管理**

  委託先には ISO27001 等の認証取得を要件とし、島嶼部での作業実績や緊急時の対応能力を選定基準に含める。契約時には秘密保持や監査受入義務、および個人情報保護法に基づく安全管理措置義務を明記する。また、再委託は原則禁止とし、やむを得ない場合は事前の書面承認を必須とする。

5　評価と見直し（PDCA サイクル）

- **監査と点検**

  毎日のシステム点検に加え、年 1 回の内部監査および 3 年に 1 回以上の外部監査を実施する。
  監査にあたっては、離島の制約を考慮しリモート監査の手法も活用する。
  内部監査は、監査対象から独立した立場の者が実施する。

- **継続的改善**

  監査結果や技術動向、新たな脅威（サイバー攻撃の手口の変化等）を踏まえ、本方針およびポリシーを適宜見直す。