横芝光町情報セキュリティ対策等支援業務仕様書

１．業務名

横芝光町情報セキュリティ対策等支援業務

２．目的

デジタル化の進展に伴い、本町においても情報システムやデジタル技術の活用が拡大する中、不正アクセスやサイバー攻撃、情報の漏えい等のリスクに対し、住民の個人情報をはじめとする情報資産を適切に保護することが、行政運営の前提として一層重要となっている。

本町では、これまで情報セキュリティポリシーをはじめとする関係規程を整備し、技術的対策に加え、組織的・人的対策を含めた多層的な情報セキュリティ対策を講じてきたところであるが、近年の脅威の高度化や制度・環境の変化を踏まえ、これらの取組を継続的に見直し、実効性を高めていくことが求められている。

また、情報セキュリティ対策を含むＩＴガバナンスの強化に当たっては、単なる規程整備にとどまらず、自己点検、監査、訓練、研修等を通じたＰＤＣＡサイクルの確立と、職員の理解・対応力の向上を図ることが重要である。

これらの取組を的確かつ計画的に推進し、将来的には本町が自律的に情報セキュリティ対策を運用できる体制を構築するためには、専門的な知見を有する事業者による継続的な伴走支援が不可欠である。

このため、本町の情報セキュリティ対策及びＩＴガバナンスの強化を目的として、専門的知見を有する事業者に対し、「４　業務内容」に定める業務を委託するものである。

３．業務期間

契約締結日の翌日から令和１１年３月２６日まで

４．業務内容

（１）令和８年度

（ア）情報セキュリティポリシーの見直し

本業務は、本町が定める現行の情報セキュリティポリシーについて、総務省が公表する最新の「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」に準拠した内容へと改定することを目的とし、専門的知見に基づき、実効性及び継続的な運用を確保した情報セキュリティポリシーの整備を支援するものである。受託者は、以下に定める内容に基づき、情報セキュリティポリシー改定支援業務を実施するものとする。

① 現行情報セキュリティポリシーの分析・把握
本町が現在運用している情報セキュリティポリシー（基本方針、対策基準等）について、その構成、記載内容及び運用実態を整理・分析し、現状を把握すること。

② ガイドラインとの対比・整理
総務省「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」に記載されている全項目について、現行の本町情報セキュリティポリシーとの対比を行い、記載の有無、記載内容の過不足、表現・考え方の相違等を体系的に整理すること。

③ 外部環境及び内部状況を踏まえた検討
近年の情報セキュリティを取り巻く外部環境の変化（クラウドサービスの利用拡大、サイバー攻撃の高度化・巧妙化等）及び、本町におけるＩＴの現状や運用上の課題等を踏まえ、専門家の立場から、現行ポリシーの課題整理及び改定について助言を行うこと。

④ 情報セキュリティポリシー改定案の作成

上記の検討結果を踏まえ、以下の文書について改定案を作成すること。
・情報セキュリティ基本方針
・情報セキュリティ対策基準
なお、改定案は、総務省ガイドラインとの整合性を確保するとともに、本町の業務実態に即した、実効性の高い内容とすること。

⑤ 改定経緯の記録作成
情報セキュリティポリシーの改定内容及びその検討経緯について、後年においても改定の背景や判断理由を確認できるよう、改定経緯を整理した記録（対比表、検討メモ等を含む）を作成すること。

（イ）情報資産重要性分類基準の改訂支援と情報資産台帳の整備支援

本業務は、前項に定める情報セキュリティポリシーの見直し業務で実施する、現行の情報資産の重要性分類の見直し、見直した重要性分類で情報資産台帳を整備する作業について、専門的知見と経験に基づき支援と助言を行うこと。

（ウ）情報セキュリティ対応マニュアルの改定

本業務は、前項に定める情報セキュリティポリシー改定支援業務の結果を踏まえ、本町における情報セキュリティ対策を実務レベルで確実に実行するため、各種情報セキュリティ対応マニュアル等の作成及び改定を行うことを目的とする。

改定及び作成にあたっては、情報セキュリティポリシー（基本方針及び対策基準）との整合性を確保するとともに、職員が理解しやすく、実際の業務において活用可能な内容とすること。

受託者は、以下に定める内容に基づき、情報セキュリティ対応マニュアルの作成及び改定支援を行うものとする。

① 既存マニュアル等の改定

A) 情報セキュリティ実施手順書
以下の区分ごとに、改定後の情報セキュリティポリシーに準拠した内容へ見直しを行うこと。
・管理職編
・一般職員編
なお、それぞれの立場・役割に応じて、求められる対応や判断事項が明確となる構成とすること。

B) 台帳集
情報資産管理、業務委託管理等に係る各種台帳について、改定後の対策基準及び運用内容を踏まえ、記載項目や様式の見直しを行うこと。

C) 様式集
申請書、報告書、点検記録等の各種様式について、実施手順及び運用フローと整合した内容となるよう改定を行うこと。

② 新規マニュアル等の作成

A) 情報セキュリティハンドブック
全庁職員を対象とした情報セキュリティハンドブックを新たに作成すること。
本ハンドブックは、情報セキュリティ対策基準のうち、全庁共通で特に重要な対策を抽出し、以下の点に留意して作成すること。
・分量は概ね 30 ページ程度とすること。
・文章中心の読み物ではなく、図表、イラスト、ピクトグラム等を効果的に用い、職員が「見れば理解できる」構成とすること。

・日常業務における留意点や、誤りやすいポイントが直感的に把握できる内容とすること

B) インシデント対応手順書
情報セキュリティインシデント発生時における対応を明確化するため、インシデント対応手順書を新たに作成すること。本手順書は、以下を基本方針として整備すること。
・インシデントの検知・初動対応から、被害拡大防止、原因分析、再発防止策の策定、収束に至るまでの一連の流れを整理すること
・CSIRT を中心とした対応体制及び役割分担を明確にすること
・管理職、関係部署、外部関係機関等との連携が分かる構成とすること

C) 業務委託・外部サービス利用手順書
業務委託及び外部サービス（クラウドサービスを含む）の利用に伴う情報セキュリティ対策を明確化するため、業務委託・外部サービス利用手順書を新たに作成すること。本手順書は、以下の観点を踏まえて整備すること。
・各種業務委託及び外部サービスの利用における共通的な考え方の整理
・利用前（企画・選定・契約段階）、利用中（運用・管理段階）、利用後（終了・廃止段階）における対応手順の体系化
・委託先及び外部サービス事業者に求める情報セキュリティ対策及び確認事項の明確化

（エ） 情報システムＢＣＰ（情報システム事業継続計画）の作成

本業務は、近年頻発するサイバー攻撃、自然災害その他の重大な事象により情報システムが被害を受けた場合においても、本町の重要な行政業務を継続又は早期に復旧させることを目的として、情報システムＢＣＰ（以下「ICT-BCP」という。）を策定するものである。

策定にあたっては、総務省が公表する「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」及び「ICT-BCP 初動版 導入ガイド」を踏まえ、特に発災直後から初動対応段階における実効性の確保に重点を置いた計画とする。

受託者は、以下に定める手順及び内容に基づき、ICT-BCP の作成支援を行うものとする。

① 業務影響度分析（BIA）の実施
重要業務及びそれを支える情報システムについて、業務影響度分析（BIA）を実施すること。

② 被害想定及びリスク分析
情報システム及び ICT 資源が受ける被害の内容及び程度について整理・分析を行うこと。

③ 初動対応体制及び手順の整備
発災又はインシデント発生直後から概ね初動対応期間における対応を明確化すること。

④ 復旧手順及び業務継続方法の策定
初動対応後を見据え、復旧手順や代替手段等を整理すること。

⑤ ICT-BCP（初動対応中心）の作成
ICT-BCP を文書として取りまとめること。

（オ） インシデント対応訓練の企画

本業務は、情報セキュリティインシデントが発生した場合を想定し、本町職員が実際の対応手順や判断プロセスに基づき、適切かつ円滑に対応できるかを検証することを目的として、情報セキュリティインシデント対応訓練を実施するものである。

訓練を通じて、職員が自ら考え、気づきを得ることにより、インシデント対応力の向上及び既存のルール・手順の改善につなげることを目指す。

受託者は、以下に定める内容に基づき、情報セキュリティインシデント対応訓練の企画及び実施を支援するものとする。

① 想定インシデントの設定
訓練の実施に先立ち、本町と協議のうえ、訓練で取り上げる想定インシデントを設定すること。

② インシデントシナリオの作成
設定した想定インシデントに基づき、訓練用のインシデントシナリオを作成すること。

③ 訓練用テキストの作成
インシデントシナリオを基に、訓練当日に使用するテキストを作成すること。グループワーク用の議題は４議題以上作成すること。

（カ） 自己点検の実施

本業務は、次年度（令和９年度）以降に実施予定の情報セキュリティ内部監査に先立ち、本町における情報セキュリティ対策の実施状況及び課題を把握することを目的として、情報セキュリティに関する自己点検を実施するものである。

自己点検を通じて、現行の情報セキュリティポリシー及び関連手順の運用状況を可視化し、情報セキュリティ水準の向上及び次年度の情報セキュリティ監査計画の策定に資することを目的とする。

受託者は、以下に定める内容に基づき、情報セキュリティ自己点検の実施を支援するものとする。

① 自己点検項目の抽出
改定後の情報セキュリティポリシー及び総務省が公表する「地方公共団体における情報セキュリティ監査に関するガイドライン」を踏まえ、本町における自己点検項目を抽出すること。

② 自己点検シートの作成
抽出した自己点検項目に基づき、職員が回答しやすい形式の自己点検シートを作成すること。

③ 自己点検結果の分析
自己点検結果を集計・分析し、改善が必要と考えられる対策等を整理すること。また、次年度に実施予定の情報セキュリティ内部監査に向けて、重点的に確認すべき監査項目等を抽出すること。

（キ） 情報セキュリティ研修

本業務は、近年の情報セキュリティを取り巻く最新動向及び地方公共団体を取り巻く環境の変化を踏まえつつ、本町において改定した情報セキュリティポリシーの内容や自己点検結果を職員に周知し、情報セキュリティに対する理解及び意識の向上を図ることを目的として、情報セキュリティ研修を実施するものである。

受託者は、以下に定める内容に基づき、情報セキュリティ研修の企画及び実施を支援するものとする。

① 研修内容の企画

研修内容は、以下の事項を踏まえて構成すること。
・情報セキュリティに関する最新動向及び地方公共団体を取り巻く脅威・リスクの状況
・本町において改定した情報セキュリティポリシーの主な改定内容及び留意点
・実施した自己点検の結果の概要及び、情報セキュリティ上の課題や改善の方向性

なお、研修内容は、職員が自らの業務と結び付けて理解できるよう、具体的な事例等を交えて分かりやすい内容とすること。

② 研修テキストの作成

③ 研修の実施

作成した研修テキストを用い、情報セキュリティ研修を２回（午前・午後）実施すること。研修を欠席した職員に対しても受講機会を確保するため、研修の模様を後日オンデマンド配信することを前提とする。このため、研修の実施にあたっては、研修をビデオに録画することを事前に了承するものとする。

（ク） 情報セキュリティに関する相談・助言対応業務

本町が実施する情報セキュリティ対策を円滑かつ適切に推進するため、本町から寄せられる情報セキュリティに関する各種相談及び問合せに対し、専門的知見に基づく助言及び対応を行うことを目的とする。

受託者は、本町からの情報セキュリティに関する相談及び問合せに対し、以下の内容を含めて対応するものとする。

・情報セキュリティに関する一般的な相談への助言
・情報セキュリティポリシー、各種手順書及び運用に関する問合せへの対応
・新たな脅威や制度改正等を踏まえた対策検討に関する助言
・事故・トラブルの未然防止又は影響低減を目的とした対応方針に関する助言

なお、回答にあたっては、本町の業務内容及び運用実態を踏まえ、実務上有効かつ現実的な内容とすること。

（２）令和９年度

（ア） 情報セキュリティポリシーの見直し

令和８年度に改定した情報セキュリティポリシーについて、その後の制度改正、外部環境の変化及び運用状況等を踏まえ、必要に応じた見直しを行うこと。

（イ） 情報セキュリティ内部監査支援

本業務は、本町における情報セキュリティ対策の実効性を確保し、継続的な改善を図るため、情報セキュリティ内部監査の実施体制及び手続きを整備するとともに、内部監査の実施を支援することを目的とする。

あわせて、将来的に本町が自律的に情報セキュリティ内部監査を実施できる体制を構築することを目的とする。受託者は、以下に定める内容に基づき、情報セキュリティ内部監査支援業務を実施するものとする。

① 情報セキュリティ監査実施要綱の策定

情報セキュリティ内部監査を円滑に実施するため、監査の目的、位置付け、体制、手順等を定めた監査実施要綱を策定し、情報セキュリティ監査に関する全庁共通の認識を統一すること。

② 情報セキュリティ中期監査計画の策定

情報セキュリティ内部監査を計画的に実施するため、３年間で本町の全課を一巡する中期監査計画を策定すること。
なお、特定個人情報等の重要情報を取り扱う課については、毎年度監査対象とするものとする。

③ 年度計画及び実施計画の策定

中期監査計画に基づき、当該年度に実施する監査対象、監査範囲、スケジュール等を整理した年度計画及び個別の実施計画を策定すること。

④　監査項目及び監査チェックリストの作成

前年度に実施した自己点検結果等を踏まえ、当該年度において確認すべき監査項目を抽出すること。
抽出した監査項目に基づき、情報セキュリティ内部監査で使用する監査チェックリストを作成すること。

⑤　内部監査人向け研修の実施

選出された内部監査人に対し、情報セキュリティ内部監査の目的、手法及び留意点等について理解を深めるための監査研修を実施すること。

⑥　内部監査実施支援

内部監査の実施にあたり、受託者はアドバイザーとして往査に同行し、監査の進め方、ヒアリング方法等について内部監査人を支援すること。

⑦　監査報告書のレビュー

内部監査人が作成した監査報告書について、内容の妥当性及び表現等の観点からレビューを行い、必要に応じて助言を行うこと。

⑧　改善計画及びフォローアップ監査支援

監査により指摘された事項に対して原課が作成する改善計画についてレビューを行うこと。
あわせて、改善状況を確認するためのフォローアップ監査の計画策定を支援すること。

⑨　情報セキュリティ内部監査マニュアルの作成

上記①から⑧までの一連の手続き、様式及び留意事項等を整理し、将来的に本町が自律的に情報セキュリティ内部監査を実施できるよう、情報セキュリティ内部監査マニュアルを作成し、納品すること。

（ウ）　インシデント対応訓練の実施

令和８年度に作成したシナリオ及びテキストを用い、職員がグループワーク形式で参加するインシデント対応訓練を１回実施すること。仮想の情報セキュリティインシデントを想定し、職員参加型のインシデント対応訓練を実施する。

（エ）　自己点検の実施

次年度以降の情報セキュリティ監査を見据え、令和８年度と同様の自己点検項目及び手法により、情報セキュリティ自己点検を実施する。

（オ）　情報セキュリティ研修

情報セキュリティを取り巻く最新動向、本町の情報セキュリティポリシー及び自己点検結果等を踏まえ、令和８年度と同様の内容で情報セキュリティ研修を実施する。

（カ）　情報セキュリティに関する相談・助言対応業務

本町からの情報セキュリティに関する各種相談及び問合せに対し、令和８年度と同様に、専門的知見に基づく助言及び対応を行う。

（3）令和１０年度

（ア） 情報セキュリティポリシーの見直し

令和９年度に改定した情報セキュリティポリシーについて、その後の制度改正、外部環境の変化及び運用状況等を踏まえ、必要に応じた見直しを行うこと。

（イ） 情報セキュリティ内部監査支援

令和９年度に整備した情報セキュリティ内部監査の仕組みを基盤として、本町における情報セキュリティ内部監査を継続的かつ実効的に実施すること。あわせて、内部監査マニュアルに基づく運用の定着を図るとともに、監査内容の継続的改善を支援すること。

（ウ） インシデント対応訓練の実施

仮想の情報セキュリティインシデントを想定し、職員参加型のインシデント対応訓練を、令和９年度と同様の方法により実施する。

（エ） 自己点検の実施

令和９年度と同様の自己点検項目及び手法により、情報セキュリティ自己点検を実施する。

（オ） 情報セキュリティ研修

情報セキュリティを取り巻く最新動向、本町の情報セキュリティポリシー及び自己点検結果等を踏まえ、令和９年度と同様の内容で情報セキュリティ研修を実施する。

（カ） 情報セキュリティに関する相談・助言対応業務

本町からの情報セキュリティに関する各種相談及び問合せに対し、令和９年度と同様に、専門的知見に基づく助言及び対応を行う。

５．成果物

本業務で想定している成果物は以下のとおりである。

成果物	納入時期
情報セキュリティ基本方針（改定案）	年度毎の業務終了時
情報セキュリティ対策基準（改定案）	年度毎の業務終了時
ガイドライン対比表、改定経緯を整理した記録一式	年度毎の業務終了時
改定後の情報セキュリティ実施手順書（管理職編・一般職員編）	年度毎の業務終了時
改定後の台帳集、様式集	年度毎の業務終了時
情報セキュリティハンドブック	年度毎の業務終了時
インシデント対応手順書	年度毎の業務終了時
業務委託・外部サービス利用手順書	年度毎の業務終了時
情報システム BCP（ICT-BCP）一式	年度毎の業務終了時
インシデント訓練用テキスト	年度毎の業務終了時
自己点検シート	年度毎の業務終了時

自己点検結果集計・分析報告資料	年度毎の業務終了時
情報セキュリティ研修テキスト	年度毎の業務終了時
情報セキュリティ監査実施要綱	年度毎の業務終了時
情報セキュリティ中期監査計画	年度毎の業務終了時
情報セキュリティ監査年度計画	年度毎の業務終了時
情報セキュリティ監査実施計画	年度毎の業務終了時
監査チェックリスト	年度毎の業務終了時
内部監査人向け研修資料	年度毎の業務終了時
情報セキュリティ内部監査マニュアル	年度毎の業務終了時
課題管理表	随時
議事録	随時

※ 成果物は指定のない限り電子データとし、日本語表記とすること。また、電子データの作成は、特に指定がない限り、本町職員が、Ｗｏｒｄ、Ｅｘｃｅｌ、ＰｏｗｅｒＰｏｉｎｔで編集できるソフトを使用すること。それ以外のソフトを使用する際には本町に相談すること。

６．守秘義務等

⑴ 受託者は、本業務において知り得た情報を第三者に漏らしてはならない。この項については、契約期間の終了後又は解除後も同様とする。また、機密や個人情報を含む成果物（業務の過程で得られた記録等を含む。）を本町の許可なく第三者に閲覧、複写、貸与又は譲渡してはならない。

⑵ 資料・データの紛失、滅失、毀損、盗難等を防止するための必要な措置を講ずること。

７．著作権

⑴ 本業務の範囲内で、第三者が権利を有する著作物又は知的所有権等を利用する場合は、受託者の責任において、その権利の使用に必要な費用を負担し、使用許諾契約に係わる一切の手続を行う。

⑵ 本業務の範囲内で、本町に帰属しない著作物がある場合にあっては、受託者は、本町に当該著作物の関連文書を成果物として納入するものとし、この関連文書についても上記⑴に準じる。

８．再委託

受託者は、本町の文書による承認を得なければ、契約に係る義務の履行を第三者に委託し（以下「再委託」という。）、契約に係る権利を第三者に譲渡し、又は契約に係る義務を第三者に継承させてはならない。また、再委託の内容が一括再委託に該当すると判断される場合には、本町は再委託について承認しない。

９．資料の提供等

本業務の実施に当たり、必要な資料及びデータの提供は本町が妥当と判断する範囲内で受託者に提供する。

なお、受託者は、本町から提供された資料は適切に保管し、特に個人情報に係るもの及び情報システムのセキュリティに係るものの保管は厳格に行うこと。また、契約終了後は本業務に当たり収集した一切の資料を速やかに返還し、又は廃棄するものとする。

１０．その他

⑴ 本業務を開始するに当たっては、本町と事前に十分な調整を行うこと。

⑵ 本仕様書に記載のない事項又は仕様書に疑義が生じた場合は、本町と協議し、その決定に従うこと。

⑶ 本町は、必要があると認める場合は、契約内容の遵守状況及び委託業務の履行状況について、いつでも受託者に対して報告を求め、検査又は必要な指示等を行うことができるものとする。受託者は、再委託の事業者も含め、本町から上記の申し出を受けた場合には受け入れること。

以上