

情報セキュリティ外部監査業務委託仕様書

1 業務名

情報セキュリティ外部監査業務

2 監査目的

本業務は、本町の「情報セキュリティポリシー」及び「愛南町特定個人情報等の安全管理に関する基本方針」、「愛南町特定個人情報の取扱いに関する管理規程」等に基づき実施している情報資産の管理、各種情報システムの保守・運用、職員研修等の情報セキュリティ対策について、第三者による独立かつ専門的な立場から、基準等に準拠して適切に実施されているか否かを点検・評価し、問題点の確認、改善方法等についての検討、助言及び指導を行うことによって、本町の情報セキュリティ対策の向上に資することを目的とする。

3 監査期間

契約締結日の翌日から令和9年3月10日まで

4 監査対象

本町の行政情報システム及び特定個人情報を取り扱う業務を対象とする（具体的な範囲は、別に受託者に指示する）。

5 監査内容

「地方公共団体情報セキュリティ監査ガイドライン」及び「地方公共団体等における監査のためのチェックリスト」等を基に本町の実情にあった監査項目を抽出して、助言型監査を実施すること。なお、技術検証及び標的型攻撃メール訓練の実施も含まれることに留意すること。

(1) 監査実施計画書の作成

監査の手順、実施スケジュール等を具体的に記載した監査実施計画書を作成すること。

(2) 監査チェックリストの作成

第6項で示す適用基準から、本町の実情に合わせた監査項目を設定し、具体的な確認内容を記載した監査チェックリストを作成すること。

(3) 現場視察の実施

ア 被監査者に対し、監査チェックリストに従いインタビューを行うこと。

イ 必要に応じて、記録類や情報保管場所等について情報セキュリティポリシーの遵守状況等をレビューすること。

ウ インタビュー及びレビューの結果、情報セキュリティポリシー等が十分に遵守されていない場合、現状の運用及び遵守できない理由について確認すること。

エ 監査対象所属は、本庁内の8所属程度とし、1所属当たり1時間程度で実施するこ

と。

(4) システム脆弱性等技術診断の実施

ア インターネット側に設置するホームページサーバ、メールサーバ等の脆弱性等の技術診断を実施すること。

イ 診断結果報告書を作成し、監査報告書にまとめること。

(5) 標的型攻撃メール訓練の実施

本町が保有する特定のメールアカウントに疑似標的型メールを送信し、標的型攻撃メールに対する免疫力や対応力を確認するための訓練を実施すること。

ア 訓練メールは、100～200 アカウントに対し送信（計2回）することとし、送信に当たっては、受信側のメールサーバの負荷を考慮し、本町と協議のうえ実施すること。

イ 訓練メールは、添付ファイル型若しくは URL 型いずれかとし、それぞれ添付ファイルを開封若しくは URL をクリックした際にウィルス感染することを前提とした訓練とすること。

ウ 本町が提供するデータを基に、開封したユーザーが特定でき、またそれを所属別に集計することが可能な形式で収集できること。

エ 訓練メールの標題、本文及び発信元については、カスタマイズが可能であること。

また、メール本文のテンプレートを提供すること。

オ 訓練メール開封者に対して、このメールが訓練用メールであること、また、教育用コンテンツを表示できること。

カ 訓練の実施に当たっては、実施計画書を作成し、本町と事前に協議及び動作確認を行ったうえで実施すること。

キ 訓練実施後、訓練結果報告書及び事後教育コンテンツを作成し、監査報告書にまとめること。

(6) 情報セキュリティポリシーの見直し提案

監査結果及び情報セキュリティと取り巻く状況の変化を踏まえ、本町の情報セキュリティポリシーやそれに係る運用について、改善すべき事項があれば提案し、監査報告書にまとめること。

(7) 監査報告書の作成

ア 監査で確認した内容及び標的型攻撃メール訓練結果を取りまとめた監査報告書を作成し、提出すること。

イ 監査報告書は、監査対象についての脆弱点を網羅した非公開の「監査報告書（詳細版）」と公開を前提とした「監査報告書（公開版）」の2種類を作成し、提出すること。

なお、様式は任意とするが、サイズについては、A4 版（縦）で作成すること。

(8) 監査報告会・情報セキュリティ研修会の実施

ア 最高情報セキュリティ責任者、統括情報セキュリティ責任者及び情報セキュリティ責任者（保護管理者）に対し、監査報告書を用いて監査報告会を実施すること（1 時間程度）。

- イ 各所属の情報システム運用担当者、保護担当者及び事務取扱担当者等に対し、監査結果（標的型攻撃メール訓練結果含む）及び最新の情報セキュリティの現状と動向を踏まえたセキュリティ研修を実施すること（1時間程度）。
- ウ 事前に研修資料を作成し、担当者の確認を得ること。
- エ 監査報告会・情報セキュリティ研修会は、同日の開催で可とする。

6 適用基準

(1) 必須とする基準

- ア 愛南町情報セキュリティポリシー（基本方針及び対策基準）
- イ 愛南町特定個人情報等の安全管理に関する基本方針
- ウ 愛南町特定個人情報の取扱いに関する管理規程
- エ 愛南町特定個人情報等取扱マニュアル
- オ 個人情報の保護に関する法律

(2) 参考とする基準

- ア 特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体編）
- イ 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
- ウ 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
- エ 情報セキュリティサービス基準
- オ 個人情報の保護に関する法律についてのガイドライン（行政機関等編）
- カ 個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）

7 監査人要件

- (1) 受託者は、監査対象となる情報資産の管理及び当該情報資産に関する情報システムに関わる業務（企画、設計、開発、構築、運用、保守又は支援のいずれかに関する業務）の受注者でないこと。
- (2) 監査責任者、監査人、監査補助者、アドバイザー等で構成される監査チームを編成すること。
- (3) 監査チームの監査責任者又は監査人のいずれか1名は、次に掲げるいずれかの資格を有すること。また、監査チームには、国又は地方公共団体における情報セキュリティ監査若しくはコンサルティングの実績など、必要な知識及び経験を持つ者が1名以上含まれていること。
 - ア システム監査技術者
 - イ 公認情報システム監査人（CISA）
 - ウ 公認システム監査人（CSA）
 - エ ISMS 主任審査員
 - オ ISMS 審査員
 - カ 情報セキュリティアドミニストレータ
 - キ 公認情報セキュリティ主任監査人

ク 公認情報セキュリティ監査人

8 監査成果物と納品方法

次の監査成果物を書面（A4 版縦）及び電子媒体（CD-R）にて提出すること。

(1) 監査成果物

ア 業務完了報告書

イ 監査実施計画書

ウ 監査チェックリスト

エ 情報セキュリティ監査報告書（詳細版）

※標的型攻撃メール訓練報告書及び情報セキュリティポリシーの見直し提案書含む。

オ 情報セキュリティ監査報告書（公開版）

カ 情報セキュリティ研修会資料

キ 議事録

ク その他必要な書類

(2) 納品方法

ア 紙媒体 各 2 部

イ 電子媒体（CD-R） 1 部

※電子ファイルは加工可能な形式のファイルとすること。

(3) 成果物の帰属

成果物及びこれに付随する資料は、全て本町に帰属するものとし、書面による本町の承諾を受けないでほかに公表、譲渡、貸与又は使用してはならない。

ただし、成果物及びこれに付随する資料に関し、受託者が従前から保有する著作権は、受託者に留保されるものとし、本町は、本業務の目的の範囲内で自由に利用できるものとする。

9 契約締結後、提出が必要な書類

次の書類を契約締結後速やかに提出すること（各 1 部）。

(1) 業務着手届

(2) 守秘義務誓約書

(3) 従事者の資格を証明する書類の写し

(4) 監査実施計画書

10 留意事項

業務の実施に当たっては、次の事項に留意すること。

(1) 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存し、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ものとする。また、契約終了後

は本件監査に当たり収集した一切の資料を速やかに本町に返還し、又は廃棄するものとする。

(2) 再委託

受託者は、本業務の全部を一括して他の業者に再委託することを原則禁止する。

本業務の一部をやむを得ず再委託する必要がある場合は、当該業務に係る業務遂行能力を持つ者を責任を持って選定することとし、再委託して処理する内容、再委託の理由、再委託先の事業者の名称、再委託先事業者において取り扱う情報、従事者の氏名及び経歴その他再委託先に対する安全性及び信頼性を確保する対策並びに管理及び監督の方法等を明記した書面を事前に提出し、承認を得なければならない。

(3) 秘密保持等

受託者は、本業務の実施に当たり、知り得た情報及び成果品の内容を正当な理由なくほかに開示し、又は自らの利益のために利用してはならない。これは、契約終了後又は契約解除後においても同様とする。

(4) 議事録等の作成

受託者は、本業務の実施にあたり、本町と行う会議、打ち合わせ等に関する議事録を作成し、本町にその都度提出して内容の確認を得るものとする。

(5) 関係法令の遵守

受託者は、本業務の実施にあたり、関係法令等を遵守し業務を円滑に進めなければならない。

(6) 報告等

受託者は作業スケジュールに十分配慮し、本町と密接に連絡を取り業務の進捗状況を報告するものとする。

(7) その他

今年度は町公式ホームページの更新事業が行われていることから、ホームページに対する脆弱性等の技術診断等の実施に当たっては、本町と事前に協議及び調整すること。

11 その他

本業務の実施に当たり、本仕様書に記載のない事項については本町と協議のうえ決定するものとする。