

令和 8 年度太宰府市情報セキュリティ監査(α'モデル)

業務委託仕様書

令和 8 年 8 月

太宰府市

1. 業務名

令和 8 年度太宰府市情報セキュリティ監査（α'モデル）業務

2. 目的

本業務は、本市のネットワーク及びシステムの運用管理等に対し、令和 7 年 3 月 28 日付けで公開された“別紙 2 「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」”において「第 2 章 3.情報システム全体の強靱性の向上 (2)LGWAN 接続系」で求められている「外部による確認」を第三者による独立かつ専門的な立場から適正に行うことを目的とする。

3. 履行期間

契約締結日の翌日から令和 9 年 3 月 31 日まで

4. 履行場所

受託者の作業場所を基本とし、必要に応じて太宰府市及び本市が指定する場所とする。

5. 監査対象及び監査項目

（1）監査対象

本市のα'モデル（行政 LAN/WAN）を対象とする。（個別ネットワークについては、監査対象に含まない。）

（2）監査項目

総務省ガイドラインに基づき設定する以下の監査項目

（ア）組織的・人的対策（α',β,β'共通）監査項目

（イ）α'監査項目

6. 適用基準

（1）必須とする基準

ア 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」（令和 7 年 3 月 28 日公開）

イ 総務省「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」（令和 7 年 3 月 28 日公開）

（2）参考とする基準

ア 太宰府市情報セキュリティポリシー

7. 業務内容

以下の手順をもとに監査を実施すること。

(1) 監査実施計画書の作成

受託者は監査実施計画書を作成し、市及び受託者の協議により委託業務の詳細内容及び各作業の実施時期を決定するものとする。

監査実施計画書には、監査の目的、監査項目、監査対象、監査手順、実施スケジュール、実施場所、実施体制及び担当者の氏名、本市との役割分担、成果物等を記載すること。

(2) 監査チェックリストの作成

別紙 1「d'モデル採用自治体における監査項目一覧」から、監査項目ごとに具体的な確認事項となる監査要点を列挙した上で、「監査資料の例」の記載をベースとした確認すべきエビデンス類を明記した監査チェックリストを作成すること。

(3) 監査の実施

本市の対策に不備がないかどうか、提供するエビデンス類を確認する「書面監査」を中心に実施することとし、書面監査では確認が不足する事項に対して、関係者へのヒアリング等を実施すること。また、発見された問題点について事実誤認がないか等確認を行うこと。

関係者へのヒアリング等は原則 Web 会議での開催とし、必要に応じて本市と調整して実施すること。

(4) 助言の実施

監査の過程において以下を実施し、本業務における目的の具体的な成果として、今後確認すべき事項の一覧と、それらの内容に対し、事業者の知見及び他自治体/団体の事例をまじえ、具体的なアドバイスを実施すること。

- ・ 情報セキュリティポリシーの内容を確認し、本市におけるポリシーの適用状況のレビューを行う上において確認すべきポイントを一覧化すること。また、改善が望ましい内容があればアドバイスを実施すること。
- ・ 監査の過程で以下の設計ドキュメントを確認し、リスクが懸念される事項を指摘し、改善ポイントについてアドバイスを実施すること。

【監査項目に含まれるもの】

- ・ ネットワーク設計（セグメント設計、アクセス制御等）
- ・ アカウント管理（AD 含む）
- ・ 資産管理
- ・ マルウェア対策
- ・ 脆弱性管理
- ・ ログ管理

- ・ 実際のログの内容や、各部署で行われている申請処理、起票された帳票等を閲覧し、ランサムウェア等のマルウェアへの感染時に侵入経路、情報の持ち出し等を追跡できるログが取得されているかを確認し、ログの取得方法や取得項目/内容、保管方法や全体としての情報処理の運用等についてアドバイスを実施すること。
- ・ 保守委託契約書、定例報告書、議事録の内容確認等からシステム運用の状況を確認し、より効率的かつリスクマネジメントを重視した運用となるようアドバイスを実施すること。
- ・ 教育の計画書、報告書、教育資料を確認し、見直すべき項目や追加すべき項目について指摘すること。また、具体的な内容についてアドバイスを実施すること。

(5) 監査調書の作成

監査結果を監査項目ごとに取りまとめた監査調書を作成すること。

(6) 監査成果物の作成

監査報告書及び、地方公共団体情報システム機構が提示した報告様式案（以下、外部監査の実施に係る報告様式と表記する）を作成すること。

監査成果物のうち、「監査報告書、監査調書（監査項目全てについて監査結果がわかるもの）、外部監査の実施に係る報告様式」は地方公共団体情報システム機構へ提出する必要があるため、その点を留意して作成すること。

(7) 監査報告会の実施

監査報告会を実施すること。報告会は原則 Web 会議での開催とし、必要に応じて本市と調整して実施すること。

8. 受託者の要件

8.1 受託者に関する要件

(1) 受託者は以下の要件を全て満たしていること。

- ①情報セキュリティサービス基準適合サービスリスト（独立行政法人情報処理推進機構）の情報セキュリティ監査サービス分野に登録されていること。
- ②ISO/IEC27001（JIS Q 27001）認証またはプライバシーマーク認証を取得していること。
- ③監査対象となる庁内ネットワークの企画、開発、運用、保守等の契約を履行した実績（再委託を含み、現在履行中の契約も含む）を有しない者であること。
- ④過去 5 年以内に地方公共団体または団体において、 $\alpha'/\beta/\beta'$ モデル監査を履行した実績を有すること。

8.2 監査実施体制及び構成員に関する要件

(1) 受託者の監査体制は以下の要件を全て満たしていること。

- ①監査責任者、監査人、監査補助者、監査品質管理者等で構成される監査実施体制を作ること。
- ②監査責任者は本業務を円滑に進めるためプロジェクトマネジメントに必要な知識及び経験を持ち、以下資格のいずれかを有すること。
- ・プロジェクトマネージャ
 - ・PMP PMI
- ③監査の構成員には、情報セキュリティ監査に必要な知識及び経験を持ち、「ア ネットワーク技術分野」の資格を有するもの、「イ 情報セキュリティ監査分野」のいずれかの資格を有するものがそれぞれ 1 名以上含まれること。各分野の資格を保有する監査人は同一でも構わない。また監査責任者と兼務でも構わない。
- ア ネットワーク技術分野
- ・ネットワークスペシャリスト（テクニカルエンジニア(ネットワーク)も可）
- イ 情報セキュリティ監査分野
- ・公認情報セキュリティ主任監査人
 - ・公認情報セキュリティ監査人
 - ・ISMS 主任審査員
 - ・ISMS 審査員
 - ・システム監査技術者
 - ・公認情報システム監査人（CISA）
 - ・公認システム監査人
 - ・情報処理安全確保支援士
- ④監査の構成員には、監査の効率と品質の保持のため、次の実務経験を有する専門家が 1 人以上含まれていること。
- ア 過去 5 年以内に、日本国内の自治体または団体において情報セキュリティ監査の実務経験を有している者
- イ d'モデル採用自治体における外部監査の実務経験を有している者
- ⑤監査の構成員が、本市の庁内ネットワークの企画、開発、運用、保守等の契約を履行した実績（再委託を含み、現在履行中の契約も含む）を有しない者であること。

（２）上記要件を満たしていることについて、資格の免状等の写しを添付した上で、構成員の一覧表を契約締結後すみやかに本市に提出すること。

9. 監査成果物と納入方法

下記に掲げる監査成果物を書面（Ａ４版を基本とし、必要に応じてＡ３版三つ折も可。

Ａ３版三つ折の場合、両面印刷は不可とする。）及び電子媒体（ＣＤ－Ｒ）にて、必要数を提出すること。電子文書は Microsoft 社製の Office(WORD、EXCEL、PowerPoint 等)で読み込める形式とすること。

- (1) 監査等成果物
 - ア 監査実施計画書
 - イ 監査チェックリスト
 - ウ 監査調書
 - エ 監査報告書
 - オ 外部監査の実施に係る報告様式
 - カ アドバイス一覧
 - キ 議事録

- (2) 納品方法
 - ア 紙媒体 1 部
 - イ 電子媒体 1 部

10. 成果物の帰属

成果物及びこれに付随する資料は、全て本市に帰属するものとし、書面による本市の承諾を受けずに他に公表、譲渡、貸与また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、本市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。

11. 委託業務の留意事項

業務の実施にあたっては、以下の事項に留意する。

- (1) 監査実施計画書の提出

契約締結後、受託者は監査実施計画書を提出し、本市と受託者の協議により委託業務の詳細内容及び各作業の実施時期を決定するものとする。
- (2) 資料の提供等

本業務の実施にあたり、必要な資料及びデータの提供は本市が妥当と判断する範囲内で提供する。

なお、受託者は、本市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ものとする。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すみやかに本市に返還、または破棄するものとする。
- (3) 情報資産の操作

監査のため端末等の情報資産を使用（操作）する必要がある場合は、対象情報システム及び市内ネットワークの運用に対し、支障及び損害を与えないように実施するものとする。

(4) 再委託

本業務は原則として再委託を禁止とする。再委託が必要な場合は、本市と協議の上、事前に書面により本市の承認を得ること。

(5) 秘密保持等

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

(6) 議事録等の作成

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

(7) 関係法令の遵守

受託者は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。

(8) 報告等

受託者は作業スケジュールに十分配慮し、本市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。

12. その他

本業務の実施にあたり、本仕様書に記載のない事項については、本市及び受託者との協議の上、決定するものとする。