令和8年度東大阪市情報セキュリティ外部監査業務委託仕様書

1. 業務名

令和8年度東大阪市情報セキュリティ外部監査業務

2. 目的

本業務は、東大阪市の情報セキュリティポリシー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、指導を行うことによって、東大阪市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. 契約期間

契約締結の日から令和9年3月31日まで

4. 履行場所

東大阪市本庁舎及び本市が指定する場所

5. 業務内容

「7. 適用基準」に基づき監査項目を抽出し、助言型監査を実施すること。

業務詳細は「別紙1　情報セキュリティ外部監査詳細仕様」で定める。

6. 監査対象

特定個人情報を扱うシステムのうち、本市が指定する4システム（6所属）

（1）共通基盤システム（ICT推進課）

（2）住民総合システム（市民課）

（3）障害者福祉システム（障害施策推進課、障害福祉認定給付課、障害児サービス課、健康づくり課）

（4）成人保健システム（健康づくり課）

※契約締結後、情報セキュリティインシデントの発生等、監査対象を変更すべき事由が生じた場合は、本市と受託者双方協議のうえ、監査対象を変更することがある。ただし、上記所属数を超えることはない。

7. 適用基準

（1）東大阪市情報セキュリティポリシー（基本方針及び対策基準）

（2）実施手順（共通実施手順／システムごとの実施手順）

（3）特定個人情報保護評価書

（4）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」

（5）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」

（6）特定個人情報保護委員会「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」
（7）その他監査人が有用と評価する基準等で、本市と協議して採用するもの

8. 監査人の要件

（1）受託者は IPA（独立行政法人情報処理推進機構）が公開する情報セキュリティサービス基準適合サービスリスト（うちセキュリティ監査サービスに係る部分）に登録されていること。
（2）受託者は IS0/IEC27001（JIS Q 27001）認証又はプライバシーマーク認証を取得していること。
（3）監査責任者、監査人、監査補助者等で構成される監査チームを編成すること。
（4）監査チームには、情報セキュリティ監査に必要な知識及び経験（地方公共団体における情報セキュリティ監査の実績）を持ち、次に掲げるいずれかの資格を有する者が1人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
（エ）ISMS 主任審査員
（オ）ISMS 審査員
（カ）公認情報セキュリティ主任監査人
（キ）公認情報セキュリティ監査人
（5）監査チームには、監査の効率と品質の保持のため次のいずれかの実績（実務経験）を有する専門家が、上記（4）とは別に1人以上含まれていること。
（ア）情報セキュリティ監査
（イ）情報セキュリティに関するコンサルティング
（ウ）情報セキュリティポリシーの作成に関するコンサルティング（支援を含む）
（6）監査チームの構成員が、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の企画、開発、運用、保守等に関わっていないこと。

9. 想定スケジュール

想定スケジュールは下記のとおりとする。ただし、詳細は本市と調整の上進めること。

項目	7月	8月	9月	10月	11月	12月	1月	2月	3月
契約・打合せ									
監査実施計画書の作成									
監査説明会									
予備調査の実施									
本監査の実施									
監査報告書の作成									
措置方針の確認・フォローアップ									

10. 監査成果物と納入方法

(1)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)措置状況報告書

(カ)会議・打ち合わせ等に関する議事録

(2)納品方法

(ア)A4(必要に応じて A3)の用紙に印刷ができるものとし、様式は任意とする。

(イ)Microsoft Office で編集可能な形式で作成し、電子データを納品すること。

(3)提出期限

各業務のスケジュールに沿って提出すること。

11. 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ないで他に公表、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。

12. 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)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、契約終了後は本件監査にあたり収集した一切の資料を速やかに本市に返還し、又は破棄するものとする。

(2)技術的検証

技術的検証については、対象情報システムの運用に対し、支障及び損害を与えないように実施するものとする。

(3)再委託

受託者は、本業務の実施にあたり他の業者に再委託することを原則、禁止する。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。

(4)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。

(5)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。

（6）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。

（7）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。

13. 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と協議の上決定するものとする。

別紙1

令和8年度東大阪市情報セキュリティ外部監査詳細仕様

受託者は、次に記載する業務を実施すること。

1. 監査実施計画書の作成

本市に次の事項を含む「監査実施計画書」を提出し、承認を得ること。

（1）監査対象
（2）実施体制
（3）監査手順
（4）実施スケジュール
（5）本市との役割分担
（6）進捗管理及び報告方法
（7）その他、監査実施時に必要な事項

2. 監査説明会

対象所属に対して、監査実施内容や手法等について事前に説明会を開催すること。説明会は、オンライン形式での開催も可能とする。

3. 予備調査の実施

（1）監査チェックリストの作成

（ア）適用基準から、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チェックリストを作成すること。

（イ）監査対象システムの運用管理要綱、仕様書や完成図書等の資料収集が必要な場合は、チェックリストに必要となる資料を明記し、対象所属に提出を求めること。

（2）予備調査の実施

本監査を効率的に実施するため、チェックリストの回答内容やその他資料の確認による予備調査を行うこと。

4. 本監査の実施

（1）本監査の実施

（ア）対象所属へのヒアリング、当該システムの運用管理に係る各種帳簿等の追加チェックや現地調査等を行う、本監査を実施すること。

（イ）ヒアリング項目の作成や監査対象となる帳票等の指定については受託者で対応すること。

（ウ）本監査に際し、直接システムの設置場所を確認する必要がある場合は、これに対応すること。なお、対象所属へのヒアリングについては原則対面で実施すること。

（2）監査調書の作成

ヒアリング内容を取りまとめた監査調書を作成すること。

5. 監査報告書の作成

（1）監査報告書には、監査により検出された問題点や脆弱性等を指摘事項として示すとともに、指摘事項に対し、具体的な改善策を記載すること。

（2）監査報告書に記載した指摘事項及び改善提言について、一元的に措置方針や措置状況を確認できるよう、措置状況報告書を作成すること。様式は本市と協議のうえ作成すること。

6. 措置方針の確認・フォローアップ

（1）措置方針の確認

（ア）監査実施後、対象所属から提出される措置方針について、改善提言の主旨に沿っているか確認すること。

（イ）措置方針が不十分な場合は、改善指導を行うこと。

（2）フォローアップ

（ア）対象所属の措置内容について、資料閲覧や現地視察等により確認すること。なお、現地視察を行う場合は、定例議会開会中を避けること。

（イ）措置内容が不十分な場合は、改善指導を行うこと。

（ウ）措置内容の確認結果について、措置状況報告書に記載のうえ提出すること。契約期間内に改善が確認できなかった事項については、翌年度以降職員が進捗を確認することを前提として、確認事項・確認方法等の助言を記載すること。

（エ）前回の情報セキュリティ監査について、職員がフォローアップを実施するにあたり、確認事項・確認方法等の助言を行うこと。