

奈良市自治体情報システム β' モデル採用に係る外部監査業務委託 仕様書

1. 業務名

奈良市自治体情報システム β' モデル採用に係る外部監査業務委託

2. 履行場所

奈良市総合政策部 DX 推進課（奈良市二条大路南一丁目 1 番 1 号）

その他奈良市が指定する場所

3. 監査目的

本業務は、奈良市の情報システムにおいて β' モデル採用に関する監査を行うものであり、国が示す「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6年10月版：総務省）」（以下「監査ガイドライン」という。）に則り、組織内の情報セキュリティ対策体制や業務システムのセキュリティ確保等について外部監査を実施し、発注者における適正な情報セキュリティ管理・運用に資することを目的とする。

4. 監査対象

奈良市行政 LAN/WAN 上の情報システムを対象とする（具体的な範囲は、別に受託者に指示する。）

5. 業務委託期間

（1）契約期間

契約締結日から令和 7 年 12 月 31 日まで

（2）監査実施期間

前項契約期間のうち、監査の実施日は協議の上決定する。ただし、 β' モデルの「監査報告書」「外部監査の実施に係る報告様式」の提出期限は令和7年8月29日とする。

6. 受託者の要件

（1）資格要件

監査責任者、監査人等で構成される監査チームを編成すること。また、入札公告日を基準に、過去 2 年間に奈良市又は他の官公庁（公社、公団を含む。）と本件に係る業務に類似する業務の契約を 2 回以上にわたって締結し実績があること。また、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 名以上含まれていること。

- ① システム監査技術者
- ② 公認情報システム監査人 (CISA)
- ③ 公認システム監査人
- ④ ISMS 主任審査員
- ⑤ ISMS 審査員
- ⑥ 公認情報セキュリティ主任監査人
- ⑦ 公認情報セキュリティ監査人

(2) 実績要件

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（1）とは別に1名以上含まれていること。

- ① 情報セキュリティ監査
- ② 情報セキュリティに関するコンサルティング
- ③ 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）

(3) 実施体制

監査の品質の保持のため監査品質管理責任者、監査品質管理者等の監査品質管理体制をつくること。

7. 業務内容

(1) 監査実施計画書の策定

- ① 受託者は、契約締結後速やかに、方針決定のための打ち合わせ会議を行うこと。原則 Web 会議等による実施とするが、必要に応じて対面での実施を行うものとする。
- ② 打ち合わせ会議後2週間以内に、奈良市に次の事項を含む監査手順及びその実施時期を記載した「監査実施計画書」を提出し、承認を得ること。
 - ア 監査対象及び範囲
 - イ 実施方法
 - ウ 実施スケジュール
 - エ 監査の実施体制
 - オ 進捗管理及び報告の日時
 - カ 監査結果の報告の日時・内容
 - キ その他、監査実施時に必要な事

(2) 監査の実施

- ① 監査項目は、「β' モデル採用自治体における監査項目一覧」で指定する以下の項目とし、関係部署へのヒアリング等により実施すること。
 - ア βモデル・β'モデル共通の監査項目
監査ガイドラインにおける組織的・人的対策に係る監査項目
 - イ β'モデル固有の監査項目
監査ガイドラインの「β'モデルを採用する場合の追加監査項目」

※監査ガイドラインの改定があった場合は、監査項目の追加・変更の可能性あり。

- ② 監査の進捗状況について、進捗状況説明会を実施し、委託者に説明すること。
原則 Web 会議による実施とするが、必要に応じて対面での実施を行うものとする

る。

ただし、業務主管課との応対で疑問等が生じた場合は、業務主管課への連絡前に DX 推進課へ相談することとする。

- ③ 実地監査において、対象課数は 5 課以内とする。

(3) 監査報告書の作成

① 奈良市への報告

書面監査、実地監査及び技術監査の結果を「監査報告書」としてまとめ、奈良市に書面で報告すること。

同報告書は、各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、具体的な改善指導内容を記載すること。

改善指導内容については以下に例示するが、その他必要な内容があれば記載すること。

ア 運用管理要綱等の作成・修正の指導

監査の結果、監査対象システムの運用管理要綱等に作成・修正の必要がある場合は、その内容を具体的に示すこと。

イ 物理的・人的な脆弱性改善の指導

監査の結果、監査対象システムの物理的・人的な脆弱性が判明し、改善する必要がある場合は、改善案を具体的に示すこと。

ウ システム上の脆弱性改善の指導

監査の結果、監査対象システム上の脆弱性が判明し、改善する必要がある場合は、改善案を具体的に示すこと。

② 報告書の宛名

宛名は「奈良市長」とする。

③ 報告書の提出先

総合政策部 DX 推進課とする。

また、同報告書は庁内で公開するため、全庁公開にそぐわない内容（セキュリティホールの詳細情報等）を省略した、庁内公開版の報告書を別途用意すること。

(4) 本監査実施にあたり、必要な資料等の作成

(5) 監査報告会

監査結果の監査報告会を実施すること。

- ① 監査結果の概要、分析等の全体説明を行うとともに、改善指摘事項等の内容、問題点の説明及び改善提案を行うこと。

- ② 指摘事項が多数確認された、又は重要な指摘事項があるシステム等について、本項(3)①から③の内容を業務主管課に説明すること。原則 Web 会議等による実施とするが、必要に応じて対面での実施とする。

8. 適用基準

(1) 必須とする基準

- ① 奈良市情報セキュリティポリシー（基本方針及び対策基準）
- 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（総

務省) (令和 6 年 10 月改定)

③ 監査ガイドライン

(2) 参考とする基準

① 奈良市情報セキュリティ監査実施基準

② 個人情報の保護に関する法律 (平成 15 年法律第 57 号)

③ 上記のほか委託期間において情報セキュリティに関し有用な基準等で、市と協議して採用するもの。

9. 監査人の権限

受託者は、必要に応じて次の行為を行うことができる。

- (1) 奈良市の所有・管理する場所に存する各種の文書類及び資料類の閲覧、収集
- (2) 奈良市職員等に対する質問及び意見聴取
- (3) 奈良市施設の現地調査
- (4) 監査技法を適用するためのコンピュータ機器の利用
- (5) 本件監査の監査報告書を決定する前における奈良市との意見交換

10. 成果物

各成果物に対し紙媒体 1 部及び電子データ 1 部提出すること (電子データは、まとめてメディア 1 部に格納可能)。

- (1) 監査実施計画書
- (2) 監査報告書
- (3) 外部監査の実施に係る報告様式
- (4) 本監査実施にあたり作成したもの

11. 成果物の帰属

成果物及びこれに付随する資料は、すべて奈良市に帰属するものとし、書面による奈良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、奈良市は、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奈良市が妥当と判断する範囲内で提供する。

なお、受託者は、奈良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奈良市に返還し、又は破棄するものとする。

(2) 技術的検証

(別添 1_別紙 1)

技術的検証を行う場合は、対象情報システム及び行政 LAN/WAN 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) 議事録等の作成

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

(4) 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。

(5) 報告等

受託者は作業スケジュールに十分配慮し、奈良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奈良市と協議の上決定するものとする。