令和５年度箕面市情報セキュリティ監査業務委託

仕様書

令和５年８月

箕面市総務部システム管理室

１．業務名

令和５年度箕面市情報セキュリティ監査業務委託

２．目的

本業務は、本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セキュリティ対策について、独立かつ専門的な立場の第三者が基準等に照らし適切であるかを評価し、問題点の抽出及び改善方法等の検討、助言、指導を行うことにより、本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．業務の主管課室

箕面市総務部システム管理室

所 在 地 ：大阪府箕面市西小路三丁目１番８号

電話番号 ：072-724-6188

メ ー ル ：jyouhou@maple.city.minoh.lg.jp

４．監査対象

（１）監査対象システム

個別システム（3 システム）

（２）監査項目

別紙「監査項目一覧」に記載の 63 項目

（３）監査項目に関するヒアリング対象者

①情報システム管理者（各個別システムを所管する部署の所属長） 3 名

②職員等（各個別システムを利用する部署等の職員） 各システム 1~2 名程度

（３）監査項目に関するヒアリング実施時間（目安）

1 時間半~2 時間程度

監査項目や監査方法、ヒアリング実施方法等の詳細は、受託者が監査実施計画書を作成する際に、本市及び受託者の協議により決定するものとする。

５．業務内容

本市の情報セキュリティポリシーおよび各個別システムの実施手順書に基づき、情報システムに関連するすべての情報資産及び業務の管理状況について、本市が作成した監査項目を対象として監査を実施すること。監査の実施にあたっては、監査資料を調査した上で、現地における確認や実機等を用いた確認を行うこと。また、監査資料の調査や現地確認だけでは不十分な場合や妥当性の判断ができない場合等には、必要に応じて監査項目に関するヒアリングを実施し、監査結果に基づく問題点の抽出と改善案の提案・助言等を行うこと。

６．適用基準

情報セキュリティ監査の適用基準は、以下の規程によるものとする。なお、適用基準については、既に公開されているものを除き、別途受託者に提供する。ただし、業務完了時には、返却または破棄すること。

（１）必須とする基準

ア　箕面市情報システムの管理運営に関する条例施行規則

イ　箕面市情報セキュリティ対策基準

ウ　箕面市情報セキュリティ監査実施要綱

エ　各個別システムの実施手順書

（２）参考とする基準

ア　箕面市個人情報の保護に関する法律施行条例

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（総務省）

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（総務省）

エ　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、本市と協議して採用するもの

７．監査人の要件

（１）本業務の入札説明書に基づき、入札参加資格を有すること。

（２）ISO/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ができること。

（４）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ができること。

（５）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

ク　情報処理安全確保支援士

（６）監査チームには、監査の効率と品質の保持のため、地方公共団体における次のいずれかの実績（実務経験）を有する者が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）

（７）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。

（８）上記要件を満たしていることについて、別添「監査チーム編成表」を記載し、資格の免状等の写しを添付した上で、契約締結後すみやかに総務部システム管理室に提出すること。

８．契約期間

入札日の翌日から令和６年２月29日（木）まで

９．監査報告書の様式

（１）監査報告書の作成様式

ア　Ａ４版縦（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。）とし、様式は任意とする。

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。

（２）監査報告書の宛名

宛名は「箕面市長」とする。

10．監査報告書の提出先

総務部システム管理室とする。

11．監査報告会

監査対象となった課室の長及び情報セキュリティ責任者、情報システム管理者に対して、監査結果の報告会を実施すること。なお、開催回数は、全部署を対象に１回とする。

12．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版縦を基本とし、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。

（１）監査等成果物

ア　監査実施計画書　１部

イ　情報セキュリティ監査報告書（詳細版）　２部
ウ　情報セキュリティ監査報告書（公開版）　２部

（２）納品方法

ア　紙媒体 上記のとおり
イ　電子媒体　１部

13. 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。

14. 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、または破棄するものとする。

（３）現地またはリモートによる監査の実施等

本業務は原則として、本市内において実施するものとする。

ただし、やむを得ない事情により当初想定していた監査を実施することが困難である場合、本市及び受託者の協議に基づき、zoom 等リモートによる実施、監査項目の削減または変更等、監査実施方法を変更できるものとする。

（４）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庁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。

（５）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。

（６）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。

（７）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。

（８）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。

（９）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。

15. 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。