企画提案仕様書

1　件名

江東区情報セキュリティ監査及びPIA監査等並びに外部委託監査業務委託

2　履行期間

令和6年4月1日　から　令和7年3月31日　まで

3　履行場所

江東区役所(監査業務は出先機関(外部委託監査にあっては外部委託業者の作業場所)も含む)

4　業務概要

(1)　情報セキュリティ監査及び特定個人情報保護評価に関する監査(PIA 監査)並びに外部委託監査

江東区の情報セキュリティについて、江東区情報セキュリティポリシー等の基準に準拠して適切に実施されているか否かを、江東区情報セキュリティ監査等実施要綱(17江政広第1048号)に基づき、点検評価し、問題点の確認、改善方法についての検討、助言及び指導を行い、江東区の情報セキュリティの全体的なレベルアップを目指す。

また、江東区が個人情報を取り扱う業務を外部委託する際におけるセキュリティについて、契約書及び個人情報の取り扱いに関する特記条項等に準拠して適切に管理・監督(対応状況の確認等)されているか否かについて、監査対象組織及び外部委託事業者に対して調査点検し、年度内の契約に対する至急の改善を行うことで、委託事業者から発生するセキュリティ事故を防ぐ体制を強化することを目指す。

(2)　特定個人情報保護に関する説明会

特定個人情報をはじめとした個人情報の適正な取扱い及び個人情報等の保護に関して、本区職員の理解と意識を高め、個人情報に関わる事故の未然防止を図るため、PIA 監査の結果を踏まえ、特定個人情報を取り扱う実務担当者を対象とした、職員向け説明会業務を支援する。

5　業務内容

(1)　情報セキュリティ監査及びPIA監査並びに外部委託監査

本委託において、委託者は、主に監査対象課(出先機関も含む。以下「対象課」

という。)との調整、連絡、帳票類の配布と回収、監査作業各種事項に係る承認、監査作業進捗の確認、対象課での現地作業時の立会い及び確認等を行い、受託者は、以下の各項に記載する監査作業実務について主体となって従事すること。

ア　実施期間

令和6年4月1日から令和7年3月31日まで

イ　対象範囲

(ｱ)　監査対象とする情報資産

本業務の監査対象とする情報資産は以下のとおりとする。

① 対象課で利用する庁内LANシステム
② 対象課で利用する基幹系システム(住民記録系、税系、保険系、福祉系及び教育系等)
③ 対象課で利用するハードウェア及びインフラ全般(回線を含む)
④ 対象課で管理運用する独立系システム(スタンドアロンPCも含む)
⑤ その他委託者が指定する情報資産

(ｲ)　監査対象組織

情報セキュリティ監査及びPIA監査の監査対象組織は、年間13課とする。

うちPIA監査の対象課は、特定個人情報保護評価書に記す課を1課と数えることとし、運用面の監査として2から3の事務の主管課（最大3課)、システム面の監査としてシステム主管課（1課）を対象とする。

但し、詳細は委託契約締結後、協議に基づき当該年度の監査対象課を決定するものとする。なお、情報セキュリティ監査は本庁と出先機関等の複数の個所に拠点をもつ部署に対する監査は上限を2部署とする。

また、外部委託監査の監査対象組織は、年間5課とする。

(ｳ)　履行場所

本委託の履行場所は、情報セキュリティ監査及びPIA監査の対象課での現地閲覧、現地ヒアリング、現地視察等の作業時(以下、「実査作業」という。)及び外部委託監査での現地ヒアリング、現地視察(外部委託業者の作業場所を含む。)等の作業時(以下、「確認調査」という。)並びに定例会等各種会議の際に一時的に委託者が確保する会議室等の場所を除いて、受託者の自社内又は受託者が委託者との協議により定める任意の場所とし、その他必要に応じて委託者が指定する場所とする。

(ｴ)　作業時間帯

実査作業及び確認調査の作業時間帯は、原則として平日の8時30分から17時までとし、当該時間外での作業が必要である場合は、別途協議の上、調整す

るものとする。

ウ　支援項目

受託者は以下のとおり想定する時期に業務支援を行うこと。

(ｱ)　事前調査の支援(6 月)

受託者は、あらかじめ委託者とヒアリングを行うとともに、情報セキュリティ監査及び PIA 監査並びに外部委託監査の対象課の基本的な情報(職員数、外部委託の実施状況、保有する情報システムの内容、業務の内容及び業務の実態等)を把握するための事前調査項目を記載した予備調査事前アンケートを作成し、アンケート調査の支援を行うこと。

(ｲ)　計画策定支援(5 月～6 月)

令和 5 年度に実施する情報セキュリティ監査及び PIA 監査並びに外部委託監査の監査実施計画(年度計画及び主管課個別計画書)並びに中期的な監査基本計画の策定及び見直しを支援すること。なお、監査実施計画書には以下の項目を含めることとし、その他必要と判断される事項を記載するものとする。

①　監査目的
②　監査対象
③　監査項目
④　監査項目毎の手続
⑤　作業体制
⑥　作業スケジュール

(ｳ)　監査実施基準の策定支援(6 月)

江東区情報セキュリティポリシー(基本方針、対策基準、ガイドライン等)及び個人情報の取扱いに関する特記条項に基づき、監査での評価尺度となる監査実施基準を策定し、委託者の個々の業務の実施に係るセキュリティ対策が適切に整備及び運用されているかを評価及び検証することのできる監査項目ヒアリングシート(情報セキュリティ監査及び PIA 監査の 2 種)及び委託管理チェックシート(外部委託監査の 1 種)を作成すること。

監査項目ヒアリングシート及び委託管理チェックシートの作成に当たっては、次に掲げる項目を重点テーマに据える。

①　個人情報等の重要資産の適切な取扱いに関する項目
②　外部委託業者の管理に関する項目
③　システムの可用性、機密性及び完全性確保に関する項目

(ｴ)　監査説明会支援(7 月)

情報セキュリティ監査及び PIA 監査並びに外部委託監査の対象課に向けて

の監査説明会を実施する際の資料作成、説明実施等を支援すること。なお、説明会は監査作業開始前に対象課が集合の上1回の開催とする。

(オ) 情報セキュリティ対策状況調査(本監査)の支援(7月～8月)

(a) 情報セキュリティ監査及びPIA監査では、以下の各項目について、監査項目ヒアリングシートに基づき、情報資産の管理体制面を含め情報セキュリティ対策状況の調査、分析作業等を支援すること。

また、監査内容の証跡として監査調書を作成し、対象課に指摘及びアドバイスを行う。

① 技術的セキュリティ対策状況調査の支援

対象課における技術的セキュリティ対策状況の調査について、調査項目の策定や調査手法の検討、調査に用いる帳票類の作成及び調査作業等を支援すること。但し、ツール等を利用した擬似攻撃による脆弱性検査手法、及びその他の持込機器等をネットワークに接続する形態の調査手法は用いないこと。

② 人的(管理運用面)な情報セキュリティ対策状況調査の支援

対象課における人的(管理運用面)な情報セキュリティ対策状況調査について、調査項目の策定や調査手法の検討、調査に用いる帳票類の作成及び調査作業等を支援すること。

③ 物理的な情報セキュリティ対策状況調査の支援

対象課における物理的な情報セキュリティ対策状況調査について、調査項目の策定や調査手法の検討、調査に用いる帳票類の作成及び調査作業等を支援すること。

(b) 外部委託監査では、以下の各項目について、委託管理チェックシートに基づき、委託業務における管理体制面を含めた情報セキュリティ対策状況の調査、分析作業等を支援すること。なお、調査は、原則として監査対象組織だけでなく外部委託業者も含めて行う。

また、確認結果に基づき、対象課に指摘及びアドバイスを行う。

① 組織的セキュリティ対策状況

委託契約における組織的セキュリティ対策状況について、確認結果に基づく改善状況の確認を支援すること。

② 委託業務の運用における情報セキュリティ対策状況調査の支援

委託契約の運用状況における情報セキュリティ対策状況について、作業記録の確認や事前事後の情報共有(報告)等の実施状況を可視化し、委託事業者の管理手続きを支援すること。

(カ)　監査報告支援(9 月)

各調査において分析した結果を基に、対象課における情報セキュリティ意識及び情報セキュリティ対策状況を評価し、情報セキュリティ監査及び PIA 監査並びに外部委託監査に応じた以下の項目を含む監査報告書(全体総括版、被監査対象課版及び特定個人情報保護評価書の準拠性監査報告書)の作成を支援し、その他必要と判断される事項について報告すること。

① 監査対象組織全体総評
② 対象課毎の評価
③ 特定個人情報保護評価書の準拠性
④ 監査実施基準毎の監査指摘
⑤ 各監査指摘に対する具体的な改善提案

(キ)　監査報告会の支援(9 月)

本監査終了後に情報セキュリティ監査及び PIA 監査の対象課に対して監査報告会を実施する際の資料作成、説明実施等を支援すること。なお、報告会は対象課が集合の上、1 回の開催とする。

報告会は、監査での指摘事項の共有をテーマとしたものと情報セキュリティに関する最新の動向等を研修形態で対象課にレクチャーするものの 2 部構成とする。

(ク)　改善支援(11 月～1 月)

監査報告後に監査での指摘事項に対して一定期間を設けて情報セキュリティ監査及び PIA 監査並びに外部委託監査の対象課にて改善作業を行う。改善作業に当たっては、対象課に対し改善するための方向性や実現可能な対策等をアドバイスし、改善計画書の作成を支援するとともに、改善結果の完了状況を確認すること。

(ケ)　情報セキュリティ自主点検の支援(1 月～2 月)

全課(約 70 部課所)に対する情報セキュリティ自主点検について、調査項目の策定や調査手法の検討、調査に用いる帳票類(全庁向け、独自システム向け及び職員向けの調査票等)の作成及び調査結果の集計・分析作業等を支援すること。

(コ)　特定個人情報の取扱いに関する自主点検の支援

特定個人情報の取扱い部署に対する特定個人情報の取扱いに関する自主点検について、調査項目の策定や調査手法の検討、調査に用いる帳票類の作成及び調査、集計及び分析作業等を支援すること。

(サ)　確認監査の実施

前年度(令和 5 年度)に実施した情報セキュリティ監査及び PIA 監査並びに委託管理対応状況確認調査における指摘事項について、改善状況の確認及び報告を支援すること。

(ｼ) その他

情報セキュリティ水準の維持向上に効果的と考える改善策の計画及び実施を支援すること。

エ 役割分担

委託者と受託者の役割分担は以下の表のとおり。

○：主体作業　△：支援・レビュー

業務	説明	役割分担	
		委託者	受託者
プロジェクト管理	監査業務の進捗管理、品質管理及びリスク管理	△	○
キックオフミーティング	監査業務全体の認識のすり合わせ、基本事項の確認	△	○
定例会	業務の進捗に応じた定例会の開催	△	○
会場の確保	説明会、報告会、実査作業、確認調査、定例会その他の実施に必要な場所の確保	○	△
実査作業対象課との各種調整	監査の実施に伴い必要な対象部署への情報発信、連絡調整	○	△
確認調査対象課との各種調整	調査の実施に伴い必要な対象部署への情報発信、連絡調整	○	△
資料の作成	説明会、報告会等に用いる資料の作成及びその説明	△	○

オ プロジェクト管理

受託者は、次によりプロジェクト管理を行うこと。

(ｱ) 進捗管理

受託者は、WBS(階層構造型進捗管理表)更新レビューによる進捗状況報告等を目的とする定例会を原則月 1 回の頻度で行うとともに、定例会開催後 2 週間以内に議事録を提出すること。定例会の場所は委託者が確保する。

(ｲ) 品質管理

業務の品質を確保するため、受託者は以下の事項を遵守すること。

① 監査の実施に当たっては、情報セキュリティに対する脅威、情報セキュ

リティインシデントの発生状況等に関する最新の知見を身につけるとともに、これらの知見が委託者側の職員にフィードバックされるよう創意工夫すること。

② 監査において重大なリスクが発見されたときは、改善に向けた最善の対策、改善に費用を要する場合における概算費用を提示すること。

③ 各種打合せ、監査等の実施に当たっては、開始時間を厳守するとともに、想定する所要時間をあらかじめ関係者に伝えること。

(ｳ) リスク管理

業務の進捗に遅れが生じることが見込まれたときは、監査チームの構成の変更、体制の見直しを考慮した改善策を提示し、委託者の承認を得ること。

カ 情報セキュリティ監査及びPIA監査業務並びに外部委託監査実施上の留意事項

(ｱ) 翌年度以降の情報セキュリティ監査及び PIA 監査並びに外部委託監査実施に当たっての助言･指導等を、翌年度の予算要求時に実施するものとする。

(ｲ) 監査を実施したことにより、改善すべき事柄に対して経費が発生する場合は、全て委託者の負担とするものとし、経費の適正規模等について助言するものとする。

(ｳ) 本業務を受託しても、他のシステム構築等の契約相手方となることを妨げることは一切ない。

(ｴ) 本業務の実施において、適切に品質管理・情報管理をすることとし、議事録作成・作業進捗管理・授受情報管理等について実施すること。

キ 成果物

(ｱ) 本業務の成果物には以下を含めることとし、その他必要に応じて追加すること。

① 予備調査事前アンケート

② 監査計画書(年度計画、主管課個別計画書及び監査基本計画)

③ 監査実施基準(ヒアリングシートを含む)

④ 監査事前説明会説明資料

⑤ 監査調書及び付随する監査証拠

⑥ 監査報告説明会説明資料

⑦ 監査報告書(当日調書・対象課版・全体総括版・特定個人情報保護評価書の準拠性監査報告書)、確認調査結果(委託管理チェックシート結果)

⑧ 改善計画書及び改善措置状況記入票

⑨ 改善状況報告書

⑩ 情報セキュリティ自主点検における調査票(全庁向け、独自システム部署

向け、職員向け)

⑪　情報セキュリティ自主点検結果報告書

⑫　特定個人情報の取扱いに関する自己点検シート(特定個人情報取扱事務向け)

⑬　改善計画実施状況の確認書(前年度指摘事項対象)

⑭　業務管理・品質管理に関する各種ドキュメント類(メンバー表・作業進捗管理表・議事録等)(ｲ)　本業務の完了までに、(ｱ)に掲げる全ての書類の電子ファイルを格納したCD-R等の媒体を一部納品すること。

(ｲ)　成果物の取扱いは、以下のとおりとする。

①　著作権法(昭和45年法律第48号)第21条(複製権)、第26条の3(貸与権)、第27条(翻訳権、翻案権等)及び第28条(二次的著作物の利用に関する原著作者の権利)に規定する権利は、委託者に帰属する。

②　委託者は、著作権法第20条(同一性保持権)第2項第3号又は第4号に該当しない場合においても、その使用のために仕様書等で指定する物件を改変し、また、任意の著作者名で任意に公表できるものとする。

③　受託者は、成果物を公表しようとするときは、事前に委託者の承認を得なければならない。

ク　適用する基準

監査の実施に当たっては、以下の規程を監査基準とする。但し、規程に改訂が発生した場合は委託者と協議し方針を決定することとする。

(ｱ)　情報セキュリティ監査

①　江東区情報セキュリティ基本方針(平成16年12月22日制定、平成23年12月8日最終改正)

②　江東区情報セキュリティ対策基準(平成28年2月5日制定、令和5年4月1日改正予定)

③　対象課が作成する各課情報セキュリティ実施手順

④　地方自治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：令和5年3月28日最終改定)

(ｲ)　PIA監査

①　個人情報の保護に関する法律(平成15年法律第57号)

②　江東区個人情報の保護に関する法律施行条例施行規則(令和5年3月8日制定)

③　江東区個人情報等の取扱いに関する基準(平成28年4月1日制定、令和5年3月8日最終改正)

④　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・地方公共団体等編)(個人情報保護委員会：令和5年7月一部改正)

(ｳ)　外部委託監査

①　個人情報の保護に関する法律(平成15年法律第57号)

②　江東区個人情報の保護に関する法律施行条例施行規則(令和5年3月8日制定)

③　個人情報の取扱いに関する特記条項(令和4年12月最終改正)

(2)　特定個人情報保護に関する説明会

ア　説明会の概要

当該年度に実施したPIA監査結果の紹介及び特定個人情報を取り扱う職員が事務を遂行するに当たり留意すべき内容について、個人情報保護委員会が定める「特定個人情報の適正な取扱いに関するガイドライン」の運用における指摘事例・事故事例を元に講義形式で説明する。

(ｱ)　実施回数　年1回(90分程度)

(ｲ)　実施時期　情報セキュリティ監査及びPIA監査終了後

※具体的な日時等は、担当者と協議の上決定する。

イ　業務支援内容

本業務において、委託者は、主に説明会の会場確保、受講者の募集・出席調整及び説明会実施に必要な什器類(プロジェクター、スクリーン及び音響設備)の手配等を行うことを予定している。受託者は、以下の各項に記載する説明会作業実務について、主体となって従事すること。

(ｱ)　説明会開催方法・内容に関する助言・提案、打合せ

(ｲ)　説明会で使用するテキスト及び資料の作成(区指定媒体で納品)

(ｳ)　説明会当日の講師派遣及び使用テキストの印刷

(ｴ)　説明会会場の設営及び原状回復

ウ　成果物

(ｱ)　説明会で使用するテキスト及び資料

※CD-R（又はDVD-R)1枚

(ｲ)　成果物の取扱いは、以下のとおりとする。

①　著作権法(昭和45年法律第48号)第21条(複製権)、第26条の3(貸与権)、第27条(翻訳権、翻案権等)及び第28条(二次的著作物の利用に関する原著作者の権利)に規定する権利は、委託者に帰属する。

②　委託者は、著作権法第20条(同一性保持権)第2項第3号又は第4号に該

当しない場合においても、その使用のために仕様書等で指定する物件を改変し、また、任意の著作者名で任意に公表できるものとする。

③　受託者は、成果物を公表しようとするときは、事前に委託者の承認を得なければならない。

6　支払方法

履行完了後に提出される完了届に基づき検査員による検査を行い、合格と認定した後、受託者の適法な支払請求に基づき一括で支払う。

7　受託要件

受託者は、以下の要件を全て満たすこと。

(1)　監査を行うプロジェクトマネージャー、監査責任者及び監査担当者からなる監査チームを編成すること。

(2)　監査チームの構成員のうち半数以上が、以下のいずれかの資格を有すること。

ア　公認情報セキュリティ主任監査人

イ　公認情報セキュリティ監査人

(3)　監査チームの構成員のうち１名以上が、以下のいずれかの資格等を有すること。

ア　情報処理安全確保支援士又は情報処理安全確保支援士試験合格者

イ　システム監査技術者

(4)　受託者は、委託事業の実施部門において「ISMS 認証」(JIS Q 27001:2014(ISO/IEC 27001:2013)の基準に適合することにより与えられるものをいう。)を取得していること。

(5)　受託者は、経済産業省の公告に基づき作成される「システム監査企業台帳」及び独立行政法人情報処理推進機構が公表する「情報セキュリティサービス基準適合サービスリスト（情報セキュリティ監査サービス)」の最新版に登録されていること。

8　留意事項

(1)　契約は単年度毎とし、令和 7 年度は令和 6 年度委託事業者の翌年度の継続意向及び江東区による履行状況判断により、契約締結するものとする。但し、予算が認められなかった場合はこの限りではない。

(2)　受託者は、本委託の履行を通じて知り得た事項について、その一切を第三者に漏らし又は委託者に無断で利用しないこと。

(3)　本委託の履行に当たり事故が生じた場合は、受託者は速やかにその原因、影響範囲及びその時点での対応内容を委託者に報告すること。

(4)　本委託の履行に当たり、受託者は江東区情報セキュリティポリシー及びその他関係法令を遵守すること。

(5)　本仕様書に定めの無い判断事項及び疑義が生じた場合は、その都度委託者と協議して決定すること。

9　担当及び連絡先

(1)　情報セキュリティ監査

江東区政策経営部情報システム課情報基盤係　安岡

電　話：03－3647－9367

メール：itsuishin-k@city.koto.lg.jp

(2)　PIA 監査、外部委託監査及び特定個人情報保護に関する説明会

江東区政策経営部広報広聴課情報公開個人情報保護担当　本間

電　話：03－3647－4022

メール：joko-tan@city.koto.lg.jp