

情報セキュリティ対策等支援業務委託仕様書

1 業務名

情報セキュリティ対策等支援業務

2 目的

デジタル社会が進展する中、ＩＣＴやデジタル技術の活用に当たっては、その前提として、不正アクセスやウイルス感染、盗難や紛失など様々なリスクに対して、市民の個人情報をはじめとした情報資産の保護に万全を期することが不可欠である。

そのため、本市では、これまでから「京都市情報セキュリティ対策基準」をはじめとした情報セキュリティ関係規定を定め、技術的及び組織・人的な観点から多層的な対策を講じてきたところであるが、近年、サイバー攻撃がますます高度化し、増加する中においても、本市が保有する個人情報をはじめとした情報資産の漏えい事案を生じさせないことが極めて重要となっている。

また、令和４年１月の「京都市ＤＸ推進のための基本方針」の策定に伴う「ＩＴガバナンスの更なる強化」を具現化するため、高度な知見を有するＩＴ専門家の参画の下、各情報システム主管課が構築する情報システムの調達仕様や調達経費の適正化、費用対効果の向上を図ることが求められている。

これら本市の情報セキュリティ対策及びＩＴガバナンスの更なる強化の取組（以下「情報セキュリティ対策等」という）を的確に実施するためには、専門的な知見を有する事業者の伴走支援が必要である。

上記情報セキュリティ対策等支援事業の目的を達成するため、専門的な知見を有する事業者により「４ 委託内容」で定める業務を委託するものである。

3 委託期間

契約締結日から令和８年３月３１日まで

4 委託内容

(1) 情報セキュリティ対策支援業務

ア 情報セキュリティ対策の伴走支援等

- (i) 庁内からデジタル化戦略推進室に寄せられる様々な情報セキュリティに関する相談（所管課における実現の可能性など）について、最近の技術動向や本市のセキュリティ対策基準等を考慮し、専門家の知見からアドバイス等を行うこと。（上限１０件／月）
- (ii) 最新の「地方公共団体における情報セキュリティポリシーガイドライン」（総務省）並びに最新の技術動向等を参考に、令和６年度に改定した箇所を考慮して京都市情報セキュリティ対策基準をはじめとする関連規定等について見直しを行い、改定すべき対象規定名、項目及び案を提示すること。
- (iii) 所属独自で作成するウェブサイトに必要な情報セキュリティ対策等をまとめた「独自ウェブサイト作成の手引」の作成に必要な項目及び案を提示すること。
- (iv) 庁内の情報セキュリティ対策基準の遵守状況の点検結果を集計するとともに、その状

況等の分析を行うこと。また、その分析結果等をもとに改善に向けた提案等を行うこと。

- (d) 外部サービス（クラウドサービス）の利用について、必要な手続きや運用上の注意事項等をまとめた資料の作成に必要な項目及び案を提示すること。また、CASB のログの抽出条件の提案や、抽出したログの分析を行うこと。

イ 特定個人情報の適正な取扱いに関する外部監査（助言型）の実施

- (f) 特定個人情報を取り扱う事務で利用する情報システムについて、第三者による独立かつ専門的な立場から、特定個人情報保護評価書や京都市情報セキュリティ対策基準に基づき、適切な安全管理措置が実施されているかを監査し、特定個人情報の適正かつ厳格な取扱いの確保を図ること。
- (g) 監査対象は、2 事務で使用されている 2 システムとし、本市と協議のうえ決定する。
- (h) 監査基準は次のとおり。

No.	監査基準
1	監査対象の事務に関する特定個人情報保護評価書
2	京都市高度情報化推進のための情報システムの適正な利用等に関する規程
3	京都市情報セキュリティ対策基準
4	京都市情報セキュリティ共通運用手順
5	京都市特定個人情報等取扱要領
6	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	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 6 年 10 月版）
8	その他、監査人が必要とするもの

- (i) 監査対象の事務について、次のとおり助言型監査を実施すること。

a 監査項目の作成

監査基準に基づき、事務の執行における情報システムの利用、運用管理及び技術面における安全管理措置について、監査項目を作成すること。

なお、監査項目は 30 程度とし、項目ごとに根拠となる監査基準の該当箇所を明記すること。

b 事前説明会の実施

監査を円滑に進めるため、被監査部門に対し、監査の目的実施内容、流れ等について事前説明会を実施すること。事前説明会は 1 回実施するものとし、会場は本市が準備する。

監査において資料調査又は現地調査が必要となる場合は、提出を求める資料及び調査内容等について説明するとともに、文書により提示すること。

c 調査の実施

監査対象の事務毎に、担当者へのヒアリング、執務室及び情報システムを構成する機器の設置場所に対する現地調査のほか、資料調査等により、監査項目について 2 名以上で調査を実施すること。

なお、調査に当たり、事前説明会で説明した資料のほか、新たに必要となる資料がある場合は、調査実施の 1 週間前までに本市に報告すること。

d 監査調書の作成

調査の実施結果に基づき、監査調書を作成すること。監査調書の作成に当たっては、事実誤認がないか等、被監査部門に十分な確認を行うこと。

e 監査報告書の作成

監査調書に基づき、以下の点に留意のうえ、監査報告書を作成すること。

- (a) 「監査報告書」には、評価できる事項、改善すべき事項、改善が望まれる事項という観点から監査結果を記載すること。また、改善すべき事項、改善が望まれる事項については、改善しないことによって発生しうる問題や、具体的な改善策についても記載すること。
- (b) 監査報告書は、本市職員が特段の専門的な知識を有することなく理解ができる内容とすること。
- (c) 提出された内容に不備があると判断した場合は、補足説明の実施や補足資料の提出等を求める場合がある。

f 監査報告会の実施

監査対象の事務ごとに、被監査部門向けの監査報告会を実施し、監査の結果について、「監査報告書」に基づき、改善すべき事項、改善が望まれる事項、評価できる事項を報告すること。改善すべき事項と改善が望まれる事項については、改善しないことによって発生しうる問題や具体的な改善策についても報告すること。

ウ ベンダのリモート保守拠点監査（想定件数：2件）

システムの標準化に伴い、ベンダの開発拠点から本市ガバメントクラウドへ接続するなど、本市の監理下でない拠点から基幹系システムへアクセスするにあたっての情報セキュリティに関する安全性を確保するために、現地で助言型監査を行うこと。

エ β' モデル採用自治体における外部監査（助言型）の実施

- (f) 最新の「 $\alpha'/\beta/\beta'$ モデル採用自治体における外部監査の実施及び監査報告書の提出について（総務省）」に沿って、市に対し外部監査を実施すること。
- (g) 監査の実施に先立ち、市の状況を確認したうえで、監査に向けて市が行う準備について必要な助言等を行うこと。
- (h) 監査終了後は、監査報告書に加え、最新の「 $\alpha'/\beta/\beta'$ モデル採用自治体における外部監査の実施及び監査報告書の提出について（総務省）」に添付の報告様式等提出資料案を作成し、市に提供すること。
- (i) 上記(h)の報告書様式等提出資料に記載した改善方針について、市に対し適切なフォローアップを実施すること。

オ ISMAP（政府情報システムのためのセキュリティ評価制度）を取得していない外部サービス（クラウドサービス）の利用に向けた評価等

基本的にISMAPを取得している外部サービスの利用を推奨する方針であるが、庁内からISMAPを取得していない外部サービス（クラウドサービス）の利用希望があった場合、当該サービスの利用可否について評価等を行うこと。

(2) ITガバナンス強化支援業務

本業務の遂行に当たっては、特定の情報システムベンダに有利にならないよう、独立性を

十分に確保すること。

ア 情報システムの企画・調達に係る支援業務

- (7) 情報システムの調達工程において、各情報システム主管課から提出される情報システムの企画又は契約に係る審査依頼資料等から、本市職員とともにその妥当性を審査すること。その際、業務に係る部分については、業務所管課において責任をもって検討を実施するが、技術的な要件に係る部分については、本市の情報セキュリティ対策基準や庁内のシステム基盤（ネットワーク、仮想化基盤など）の整備状況を踏まえて最適なシステム構成を提案するとともに、機能要件や非機能要件の記載が不足している項目については、具体的な記載案を提示するなど、本市の情報システムに係る調達仕様や調達経費の適正化、費用対効果の向上に資するための支援を行うこと。

なお、その際、本市において情報システムを導入・調達する際の指針である「京都市情報システム利用指針」に掲げる以下の基本方針等に基づき、審査依頼資料等を精査すること。

- a 業務プロセスの最適化を図ったうえで、機能の最適なシステムを構築しているか
 - b 全庁のスケールメリットを発揮して、安価なシステムを構築しているか
 - c 重複を省き、コストの最適なシステムを構築しているか
 - d 有効な競争下で調達し、価格の最適なシステムを構築しているか
 - e 運用や改修などを考慮し、後年度負担の少ないシステムを構築しているか
 - f 特定の個人及び企業への依存を避け、オープンなシステムを構築しているか
 - g 扱う情報の機密性等に応じた万全の情報セキュリティ対策を実施しているか
 - h その他、令和6年度の事業者が案件に対して指摘した観点について検討しているか
- (4) 支援業務の対象は、以下のとおりとする。支援対象の上限は a、b、c 合わせて30件とする。
- a 令和6年度の受託業者が令和7年度予算の企画審査支援を行った案件の調達審査
 - b 重要性の高い、令和7年度予算案件の調達審査
 - c 審査依頼額が36,000千円以上のものや、36,000千円未満であっても重要性の高い案件の企画審査

イ 全体最適化の視点に係る業務に関する支援

外部講師として、職員に情報セキュリティの重要性を理解してもらえよう、身近なインシデント事例等を含めた研修を実施すること。講義時間は約30分を想定している。

5 スケジュール

- (1) 本委託業務のスケジュールの詳細については、本市と調整し、決定することとする。
 なお、現時点で想定している概ねのスケジュールは以下のとおり。

委託業務	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	備考
(1) 情報セキュリティ対策支援業務													
情報セキュリティ対策の伴走支援等													随時
特定個人情報の適正な取扱いに関する外部監査(助言型)の実施													監査の実施は9月頃を想定
ベンダのリモート保守拠点監査													
βモデル採用自治体における外部監査(助言型)の実施													
ISMAPを取得していない外部サービスの利用に向けた評価等													随時
(2) ITガバナンス強化支援業務													
情報システムの企画・調達に係る支援業務													随時
全体最適化の視点に係る業務に関する支援													随時
(3) プロジェクト管理													
定例会(月1回程度)	キックオフ												
作業計画書作成	作成												
(4) マイルストーン	契約											最終納品	

(2) 定例会の開催等

ア キックオフ会議

業務の実施に当たり、実施計画書を作成しキックオフ会議において説明を行うこと。

イ 定例報告会

- (i) 月1回を目途に開催すること。
 (ii) 進捗状況及び次回定例報告会までに実施する予定の作業について報告し、進捗状況報告書、課題管理表、概要スケジュール、その他必要な資料を受託者において作成し開催すること。

なお、会議の次第、必要な資料の電子データについては、事前確認用として原則2開庁日前に提出すること。

- (iii) 業務を実施するに当たって、有益となる国や自治体における事例や技術動向等、情報セキュリティ関連の情報提供を行うこと。

ウ 作業会議

業務を進める上で、本市又は受託者が必要と定めた場合は、定例会以外の作業会議を別途開催することができる。

なお、開催場所については、本市と受託者により別途協議し決定する。

エ 開催手法（Web会議）について

ア～ウの開催手法について、本市と受託者の協議の上、Web会議等に代えても差し支えない。その場合、Web会議の実施に当たって必要となる設備等は、原則として受託者が用意すること。

6 実施体制

- (1) 本業務を確実に履行できる体制を設けること。
- (2) 本業務に従事する者の中から、本プロジェクトをマネジメントする担当者（プロジェクトマネージャ）と、本市との情報共有、連絡を行う担当者（プロジェクトリーダ）をそれぞれ1名選任すること。
- (3) なお、本市への常駐は不要であるが、1週間に1度は、本市に赴いての対面又はWeb会議による打合せ等を実施するものとする。その他、業務の実施にあたって必要な場合はWeb会議による打合せ等を実施する。
- (4) 本業務に従事する者については、以下の要件を満たす者が従事すること。

民間企業等において、情報システム分野で概ね5年以上（プロジェクトマネージャについては10年以上）の実務経験を有し、情報システムの調達、管理運用、情報セキュリティ対策や情報セキュリティポリシーの策定や改定、情報セキュリティ監査にかかる専門的な知見を有していること（いずれかを専門的に有する場合も可）。

プロジェクトマネージャについては、プロジェクトマネジメントを確実に実施するため、以下いずれかの資格等を保有すること。

プロジェクトマネージャ（独立行政法人情報処理推進機構（IPA）実施）

PMP（一般社団法人PMI日本支部実施）

プロジェクトリーダについては、下記のいずれかの資格等を有していること。

独立行政法人情報処理推進機構（IPA）が実施する下記高度試験のいずれか

情報処理安全確保支援士

ITストラテジスト

システムアーキテクト

プロジェクトマネージャ

ITサービスマネージャ

システム監査技術者

ネットワークスペシャリスト

データベーススペシャリスト

エンベデッドシステムスペシャリスト

一般社団法人PMI日本支部が実施するPMP

EXIN等が実施する「ITILエキスパート」「ITILマスター」

監査チームは監査責任者、監査担当者、監査補助者、アドバイザー等で構成すること。令和7年度はネットワークの知識が必要な「ベンダのリモート保守拠点監査」も含まれるため、次に掲げる「監査分野」のいずれかの資格を有している者を1名以上、「ネットワーク技術分野」の資格を有している者を1名以上選任すること。なお「監査分野」保有者と「ネットワーク技術分野」保有者は同一でも構わない。

監査分野

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 I S M S 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
- ネットワーク技術分野
- ア 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）も含む）

7 成果物

本業務で想定している成果物は以下のとおりである。

成果物	内容	納入時期
業務完了報告書	各業務の実施結果をまとめたもの。	業務終了後
その他	本業務の遂行過程で取得し、又は作成した資料	随時

※ 成果物は指定のない限り電子データとし、日本語表記とすること。また、電子データの作成は、特に指定がない限り、本市職員が、Word、Excel、PowerPointで編集できるソフトを使用すること。それ以外のソフトを使用する際には本市に相談すること。

8 守秘義務等

- (1) 受託者は、本業務において知り得た情報を第三者に漏らしてはならない。この項については、契約期間の終了後又は解除後も同様とする。また、機密や個人情報を含む成果物（業務の過程で得られた記録等を含む。）を本市の許可なく第三者に閲覧、複写、貸与又は譲渡してはならない。
- (2) 資料・データの紛失、滅失、毀損、盗難等を防止するための必要な措置を講ずること。

9 著作権

- (1) 本業務の範囲内で、第三者が権利を有する著作物又は知的所有権等を利用する場合は、受託者の責任において、その権利の使用に必要な費用を負担し、使用許諾契約に係わる一切の手続を行う。
- (2) 本業務の範囲内で、本市に帰属しない著作物がある場合にあっては、受託者は、本市に当該著作物の関連文書を成果物として納入するものとし、この関連文書についても上記(1)に準じる。

10 再委託

受託者は、本市の文書による承認を得なければ、契約に係る義務の履行を第三者に委託し（以下「再委託」という。）、契約に係る権利を第三者に譲渡し、又は契約に係る義務を第三者に継承させてはならない。また、再委託の内容が一括再委託に該当すると判断される場合には、本市は再委託について承認しない。

11 資料の提供等

本業務の実施に当たり、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受託者に提供する。

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こと。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速やかに返還し、又は廃棄するものとする。

12 その他

- (1) 本業務を開始するに当たっては、本市と事前に十分な調整を行うこと。
- (2) 本仕様書に記載のない事項又は仕様書に疑義が生じた場合は、本市と協議し、その決定に従うこと。
- (3) 本市は、必要があると認める場合は、契約内容の遵守状況及び委託業務の履行状況について、いつでも受託者に対して報告を求め、検査又は必要な指示等を行うことができるものとする。受託者は、再委託の事業者も含め、本市から上記の申し出を受けた場合には受け入れること。