小金井市情報セキュリティ管理委託仕様書（案）

１　件名

小金井市情報セキュリティ管理委託

２　契約期間等

契約期間：契約確定日の翌日から令和６年３月３１日まで

履行場所：小金井市役所

３　目的

小金井市における情報セキュリティの適切な運用、セキュリティポリシーの実行性・有効性に関する評価、セキュリティポリシーの文書改訂等を行い、さらなる情報セキュリティの向上を図るために、小金井市が令和５年度に目指す情報セキュリティを改善及び改良することで、情報セキュリティの維持及び向上に必要な体制の整備を目的とし実施するものである。

４　委託内容

（１）　内部情報システムの技術的セキュリティ対策の妥当性評価確認

①　技術的診断（侵入検査）

ア　侵入検査

・　インターネット経由での侵入テスト　　４ＩＰ

・　内部セグメントからの侵入テスト　　８ＩＰ

・　検査実施日数　　１日

以上の要件で、本市と協議のうえ対象を定め、本市ネットワーク運用事業者立ち会いのもと実施する。実施に当たっては、受託者は検査用ツールを用意し、最新の脅威に対応できる方法を提案すること。

調査・解析を行うため、ログ等の資料を持ち出す場合は、あらかじめ申し出たうえ、小金井市の承諾を得ること。

検査実施後、本市の情報セキュリティ対策の水準を明らかにし、改善に向けた助言を行うこと。

イ　各機器の設定調査

アの侵入検査と併せて以下の項目についても調査し、必要があれば新たな調査項目を提案すること。

調査・解析に必要なログ等の資料を持ち出す場合は、あらかじめ申し出たうえ、小金井市の承諾を得ること。

・　攻撃者がシステムに仕掛けたと思われる不正なプログラム（マルウェア等）

・　容易に想定可能なアカウントやパスワード、初期設定のままのアカウントを検出すること。

・　ウェブで使用するＣＧＩファイルやプログラムの脆弱性を検出できること。
・　各種ＯＳに脆弱なバージョンがないか診断すること。
・　ＯＳ、モジュールおよびソフトウェアのバージョンおよびセキュリティパッチの適用等、適切な運用がなされているか確認すること。
・　プロトコルスタック、アプリケーション等に脆弱性がないか診断すること。
・　開いているポートの探索を実施すること。（この場合、開いているポート番号を通知するだけでなく、そのサービスが何であるか可能な限り特定すること。）
・　セキュリティ対策上、必要なログの取得および運用がなされているか確認すること。
・　不要なアクセス権の設定がなされていないか確認すること。
・　不要なアカウントが設定されていないか確認すること。
・　不要なサービスがインストールされていないか確認すること。
・　各サーバのウェブアクセス等に使用する匿名ユーザアカウントを含むアカウントのアクセス権限に対して必要な権限設定がなされているか、確認すること。

ウ　Ｗｅｂアプリケーション診断

主要な調査項目として以下を実施するとともに必要があれば新たな調査項目を提案すること。

・　小金井市が指定するＷｅｂアプリケーション２種、計１０ページ程度を検査対象とする。
・　ウェブで使用するＣＧＩファイルやプログラムの脆弱性を検出できること。
・　クロスサイトスクリプティング検査
・　ＳＱＬインジェクション診断
・　セッション管理診断
・　認証機能の安全診断

エ　パスワード検査

１０００ユーザアカウント程度の日常使用しているパスワードの強度を検査する。

実施に当たっては以下の手順を想定しているが、新たな方法がある場合は提案すること。なお、パスワードファイルの抽出作業は、本市ネットワーク運用事業者が行うこととする。

・　受託者が、パスワードファイル抽出ツール及び当該ツール運用手引書を準備する。
・ 本市ネットワーク運用事業者が、上記ツールを用いてパスワードファイルを抽出する。

・ 本市より受託者にパスワードファイルを引き渡す。
・ 受託者がパスワード検査を行い、報告書を提出する。

② 実施に関する注意事項

ア 作業計画書の提出

作業にあたっては、詳細な作業内容、スケジュール、詳細な監査項目を記載した作業計画書を事前に示し、本市担当者と協議のうえ、実作業に入ること。

イ 技術的診断報告及び是正提案書の提出

技術的診断（侵入検査）の結果報告及び是正提案書（以下、「報告書」という。）を提出すること。報告書への記載事項としては、調査結果とあわせて、明らかになったシステムの脆弱性に対する提言事項を明記し、緊急性・重要性等に応じてレベル付けを行い、具体的な対策を提示すること。

対策については、システム構成や運用体制を考慮し、最も合理的なものとし、必ず受託者による分析を加えたものとする。パスワード検査の報告書には、以下の項目は必ず記載すること。

・ 解析ツール
・ 解析環境（ＯＳ、ＣＰＵ性能、メモリー容量）
・ 解析方法
・ 表頭に解析時間、解読数、解読割合、増分数、増分割合、表側解析時間欄に１０分、３０分、１時間、３時間、６時間、１２時間、２４時間、３日、７日、１０日等経過時間ごとの解析内容を記載し解析数を１表にまとめること。

なお、小金井市理事者向けの報告書の概要版を合わせて作成すること。

ウ 報告会の実施

本市担当者に対し、提出された報告書等に関する説明・報告会を実施すること。

なお、緊急を要する脆弱性等については、その都度本市担当者に報告すること。

エ 留意事項

検査や解析・調査用データの取得については、可能な限り１日で終わらせること。

稼働中のシステム等に対して検査を行う際は、ネットワークへの負荷が過大になったり、サーバが不安定になるような攻撃的パケットを流したりすることは避け、本市の業務遂行に支障をきたすことのないように十分配慮すること。

（２） 情報セキュリティ研修支援

研修実施に当たっては下記の条件を考慮して提案すること。

① 研修のレベル

・　初級研修…新規採用職員（初めて研修を受講する職員）及び会計年度任用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした研修。
・　中級研修…すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした研修。
・　運用管理者向け研修…各課の現場での情報資産の適正な管理運用を行うことを目的とした研修。
・　理事者向け研修…本業務に係る前年度の活動報告及び今年度の活動計画について説明し、市全体での統一した意思の下に本業務に取り組むことを目的とした研修（初年度については別途提供する前年度活動報告を読み取って行うこと)。

②　研修受講者数と回数

・　初級研修・・・・・・・年間目標受講者数　　３９０人程度　　計１回
・　中級研修・・・・・・・年間目標受講者数　　１２０人程度　　計４回
・　運用管理者向け研修・・年間目標受講者数　　８０人程度　　計３回
・　理事者向け研修・・・・情報セキュリティ推進本部向けの資料提出。

実施時期および内容は、契約締結後、本市担当者と協議のうえ決定する。

実施にあたり集合研修が難しい場合は動画等を提供し、原則として受託者が受講する人数や受講者の特性を配慮すること。また、事前にアンケートを行い、職員のレベルを把握してから研修を実施すること。研修終了後は、テストやセルフチェックリスト等の活用により、理解度等の分析も行うこと。

（３）　情報セキュリティ内部監査実施支援

全所属にセキュリティポリシーに基づいた管理及び運用ができているかを確認すること（２年程度かけて行うことを想定）。

情報セキュリティ内部監査の実施

①　情報セキュリティ内部監査基本計画書

内部監査を行うにあたり監査の目的、監査の範囲、対象所属及び実施期間等を定めること。

ア　対象所属数

全体の１／２所属を対象とする。

イ　実施時期

対象所属の繁忙期や議会対応等の業務負荷などを考慮し、最も効果的に実施できる時期を選択する。例えば上期・下期に分けるなど、対象所属に合わせた実施時期に行う。

ウ　実施時間

１所属あたり１時間程度とする。

エ　情報セキュリティ内部監査基本計画書の作成

実施すべき監査の内容、手順、手続などについて体系的に取りまとめ、作

成する。

② 情報セキュリティ内部監査実施計画書

情報セキュリティ内部監査基本計画書に基づき、監査の内容、手順及び手続等を体系的かつ対象所属を対象に作成する。また、対象所属へ事前に配布し、確認を受けること。

③ 情報セキュリティ内部監査チェックリストの作成及び修正

チェックリストの作成に当たっては下記の条件を考慮して提案すること。

- 全ての対象所属に対応できることを前提として設計し、有効且つ効果的にセキュリティポリシーの遵守状況等が把握できるよう項目を整備する。
- セキュリティポリシーを基に、「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）、「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）を考慮の上、本市と事前検討会を実施すること。

④ 情報セキュリティ内部監査人養成研修の実施

内部監査を円滑に実施する能力を育成するため、必要な研修資料を作成し、実技演習を踏まえた研修を開催すること。また、実技演習時に内部監査人が視察項目においても演習できるようにすること。

ア 研修形態

座学及び実技演習とする。

イ 実施回数

人数に応じて１～２回実施する。

ウ 実施時間

座学及び実技演習を合わせて３時間程度とする。

⑤ 情報セキュリティ内部監査の立会

対象所属全てに立会い、内部監査を円滑に実施するための支援を行うこと。立会いにあたり、受託者は次の事項が適切に行えているかを確認し、必要に応じて的確な補助をする。

- 進捗管理
- 監査の目的の達成
- 監査証拠の入手、適正性
- 監査技法の実施
- 検出事項の漏れの確認
- 計画段階で想定していなかった事項への対応
- 内部監査人の質問対応支援
- 監査の意見形成
- その他監査を円滑に実施するための事項

⑥ 情報セキュリティ内部監査報告書のレビュー

内部監査人が検出した事項の漏れ、検出した内容及び改善提言の適切性、有効性及び実現可能性を専門的見地から評価し、必要に応じて助言する。

⑦　情報セキュリティ内部監査のフォローアップ

監査の結果に基づき被監査所属が行っている情報セキュリティ管理の改善が、改善提言の主旨に沿って実施されているかを次の監査技法を用いて確認すること。

・　ヒアリング
・　レビュー
・　視察
・　再実施

⑧　情報セキュリティ内部監査のまとめ報告書の作成

内部監査人が作成した監査報告書を基に遵守状況、問題点及び対策案等を分析し、内容を総括的にとりまとめるとともに、来年度に向けた助言を記載した内部監査全体報告書を作成する。また、検出された課題は一覧にし、可視化した資料を作成すること。

（４）　マイナンバー運用管理支援

①　マイナンバー自己点検の実施

マイナンバーの利用事務及び関係事務に対し、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）（以下「番号法」という）及びそのガイドラインで求められている安全管理措置が行われているかを確認すること。

・　対象：マイナンバー利用事務及び関係事務の全ての事務。
・　実施方法：自己点検シートは、紙媒体、エクセルシート、受託者のＷｅｂ上を問わないが対象人数分を用意すること。

ア　マイナンバー自己点検シートの作成及び修正

市の状況と目的に合致した２０～３０項目程度を作成すること。また、専門的な観点からその都度項目を見直すこと。

イ　マイナンバー自己点検結果の分析

各事務担当者から提出された結果について集計し、当市の課題を可視化した上で丁寧且つ具体的な改善提案を含めた報告書を作成すること。

②　マイナンバー内部監査の代行

ア　マイナンバー内部監査基本計画書の作成

内部監査を行うにあたり監査の目的、監査の範囲、対象所属及び実施期間等を定めること。

・　対象所属数

４所属程度とする。

・　実施時期

対象所属の繁忙期や議会対応等の業務負荷などを考慮し、最も効果的に実施できる時期を選択する。

・　実施時間

１所属あたり３時間程度とする。

・　マイナンバー内部監査基本計画書の作成

実施すべき監査の内容、手順、手続などについて体系的に取りまとめ、作成する。

イ　マイナンバー内部監査実施計画書の作成

マイナンバー内部監査基本計画書に基づき、監査の内容、手順及び手続等を体系的に分けた部署毎に作成する。また、対象所属へ事前に配布し、確認を受けること。

ウ　マイナンバー内部監査チェックリストの作成及び修正

チェックリストの作成に当たっては下記の条件を考慮して提案すること。

・　全ての対象事務に対応できることを前提として設計し、有効且つ効果的に情報セキュリティポリシーの遵守状況等が把握できるよう項目を整備すること。

・　セキュリティポリシーを基に、「番号法」、「特定個人情報の適正な取り扱いに関するガイドライン」、総務省及び個人情報保護委員会が示す安全管理策を考慮の上、本市と事前検討会を実施すること。

エ　マイナンバー内部監査の実施

実施方法はヒアリング、レビュー、視察及び再実施による監査を実施し、検出された事項について、その対策を助言するとともに、業務内容・情報機器の利用状況・職場環境から専門的な視点による改善点を助言する。

オ　マイナンバー内部監査の個別報告書の作成

内部監査人が監査結果を所属ごとにとりまとめた報告書を基に作成する。作成にあたり次の事項に留意しながら作成すること。

・　法的根拠
・　検出事項の重要性
・　対応の容易さ
・　費用面での制約
・　物理的な制約
・　組織上の制約
・　その他事務特有の事項

カ　マイナンバー内部監査のフォローアップ

監査の結果に基づき被監査事務が行っている情報セキュリティ管理の改善が、改善提言の主旨に沿って実施されているか評価されていることを次の監査技法を用いて確認すること。

・　ヒアリング
・　レビュー
・　視察
・　再実施

キ　マイナンバー内部監査のまとめ報告書の作成

個別報告書を基に遵守状況、問題点及び対策案等を分析し、内容を総括的にとりまとめるとともに、来年度に向けた助言を記載した内部監査全体報告書を作成する。また、検出された課題は一覧にし、可視化した資料を作成すること。加えて全庁的な課題に対しては、課題解決に向けてひな型を作成するなどの支援を行い、市全体の対策水準の向上に寄与すること。

③　マイナンバー―研修（利用事務・関係事務）

ア　マイナンバー―研修教材の作成及び修正

マイナンバー―の取扱いがある所属の職員を対象に、特定個人情報の利用事務又は関係事務に係る安全管理措置に必要な研修を、国等が示す研修項目を満たす内容で行うこと。

イ　研修受講者と回数

・　利用事務・・・・・・・・年間目標受講者数　　４２人程度　計２回
・　関係事務・・・・・・・・年間目標受講者数　　３０人程度　計１回

実施時期および内容は、契約締結後、本市担当者と協議のうえ決定する。

実施にあたり集合研修が難しい場合は動画を提供し、原則として受託者が受講する人数や受講者の特性を配慮すること。また、事前にアンケートを行い、職員のレベルを把握してから研修を実施すること。研修終了後は、テストやセルフチェックリスト等の活用により、理解度等の分析も行うこと。

（５）　情報セキュリティ推進関連文書等の作成整備支援

実施可能で合理的な文書整備の方法を提案すること。

以下に示す情報セキュリティ対策基準で策定する文書等の作成支援を市と協議のうえ、改訂提案等の支援内容を提出すること。

・　セキュリティポリシー
・　危機管理対応策（情報セキュリティ事故対応手順）
・　情報セキュリティ法規制等登録簿
・　セキュリティ管理文書一覧表
・　管理記録一覧表
・　情報セキュリティ所掌事項一覧表
・　情報資産管理台帳
・　セキュリティ区画管理台帳
・　外部接続装置管理台帳
・　情報セキュリティリスク管理表
・　ウイルス対策管理台帳
・　情報セキュリティ対策実施手順書（個別実施手順）
・　その他情報セキュリティ推進において必要な文書類

（６）　定例会議の開催及び相談事の解決支援

① 定例会議の開催

事業の進捗状況等を確認するため月１回程度又は、必要に応じてそれ以上の回数の会議を開催する。

② 相談事の解決

本市において情報セキュリティインシデントの発生時、情報セキュリティ事業運営に係る相談、マイナンバーに係る相談、調査等に係る相談がある場合、それを受け付け、迅速かつ適切な対応を実施すること。一方で訪問までに至らない相談事はメール及び電話にて対応すること。

（7） β’モデル採用に係る情報セキュリティ外部監査の実施

① 監査対象

ア 小金井市内部情報ネットワーク基盤

イ インターネット接続系のネットワークに設置する３つの個別業務システム

② 監査実施計画の作成

監査に係る具体的な実施内容、実施体制、実施工程等を明記した監査実施計画書を本市と協議・調整のうえ策定すること。

③ 外部監査の実施

監査項目には、次の内容を含むこととし、監査資料のレビュー及び監査対象部署へのヒアリング等により実施する。

ア βモデル・β’モデル 共通の監査項目

β/β’モデルの採用にあたり必須となる、「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４年３月版）」（以下、「監査ガイドライン」という。）における組織的・人的対策に係る監査項目（23 項目）

イ β’モデル 固有の監査項目

監査ガイドライン「3.12.β’モデルを採用する場合の追加監査項目」（13 項目）

④ 監査報告書の作成

報告書の構成には以下の項目を含め、報告書の様式は任意のものとする。なお、監査結果は本市と事実確認を行った上で決定するものとする。

ア ③で示す監査項目すべてについての監査結果

イ 指摘事項がある場合は、その具体的な内容

ウ 指摘事項に対する改善方針案

⑤ 報告会の実施

本市担当者に対し、提出された報告書等に関する説明・報告会を実施すること。なお、緊急を要する検出事項については、その都度本市担当者に報告すること。

5 成果物

（1） 成果物の形式

電子媒体（ＣＤ－ＲＯＭ）２部（ＰＤＦフォルダ及びMicrosoft Officeフォルダを作成し、それぞれの形式で格納すること）

（２）　成果物

①　内部情報システムの技術的セキュリティ対策の妥当性評価確認の作業で作成した資料一式（年１回）

- 情報セキュリティ技術的診断報告及び是正提案書
- 情報セキュリティ技術的診断報告及び是正提案書（概要版）
- Ｗｅｂアプリケーション診断報告及び是正提案書
- その他業務で作成した資料

②　情報セキュリティ研修の作業で作成した資料一式

- 情報セキュリティ初級研修資料及び理解度の分析結果
- 情報セキュリティ中級研修資料及び理解度の分析結果
- 情報セキュリティ運用管理者研修資料及び理解度の分析結果
- 情報セキュリティ推進本部に提出するために作成した資料
- 情報セキュリティ推進方針および計画案（骨子）是正提案書（案）
- その他業務で作成した資料

③　情報セキュリティ内部監査実施支援の作業で作成した資料一式

- 情報セキュリティ内部監査基本計画書
- 情報セキュリティ内部監査実施計画書
- 情報セキュリティ内部監査チェックリスト
- 情報セキュリティ内部監査委人養成研修資料
- 情報セキュリティ内部監査報告書（レビュー後）
- 情報セキュリティ内部監査改善報告書
- 情報セキュリティ内部監査フォローアップ結果報告書
- 情報セキュリティ内部監査のまとめ報告書
- 情報セキュリティ内部監査検出事項一覧表
- その他業務で作成した資料

④　マイナンバー運用管理支援

- マイナンバー自己点検シート
- マイナンバー自己点検分析結果書
- マイナンバー内部監査基本計画書
- マイナンバー内部監査実施計画書
- マイナンバー内部監査チェックリスト
- マイナンバー内部監査の個別報告書
- マイナンバー内部監査のフォローアップ結果報告書
- マイナンバー内部監査のまとめ報告書
- マイナンバー内部監査検出事項一覧表
- 利用事務向け研修資料及び理解度の分析結果
- 関係事務向け研修資料及び理解度の分析結果

・　その他業務で作成した資料

⑤　情報セキュリティ推進関連文書等の作成整備支援の作業で作成した資料一式

・　４-（５）で実施した改訂提案等

・　その他業務で作成した資料

⑥　定例会議の開催及び相談事の解決支援の作業で作成した資料一式

・　議事録

・　全体計画書

・　４-（６）②で実施した相談事対応資料

⑦　β’モデル採用に係る情報セキュリティ外部監査の実施で作成した資料一式

・　監査実施計画書

・　監査チェックリスト

・　監査報告書

6　従事者要件

本業務を履行するに当たり、受託者は業務責任者、業務担当者等で構成される業務体制を編成する。また、支援の品質保持のため品質管理者を体制に加え、以下に示す要件を満たすこと。

（１）　次のいずれかの業務について３年以上の実績を有する専門家を含むこととする。

①　地方公共団体に対する情報セキュリティ監査人としての経験

②　地方公共団体に対する情報セキュリティに関するコンサルティングの経験

③　地方公共団体に対する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）

（２）　次のいずれかの資格を有する専門家を含むこととする。資格を有する者は、（１）で示す実績を有するものと同一人物でもよい。

①　システム監査技術者

②　情報処理安全確保支援士

③　公認情報セキュリティ主任監査人

④　公認情報セキュリティ監査人

⑤　公認情報システム監査人（CISA）

⑥　公認システム監査人(CSA)

⑦　ISMS 主任審査員

⑧　ISMS 審査員

（３）　従事者が所属する事業所（部署）が次の認証を取得していること。

①　ＩＳＯ９００１の認証

②　ＩＳＯ２７００１の認証

③　プライバシーマークの認証

（４）　情報セキュリティサービス基準審査登録制度（旧情報セキュリティ監査企業台長制度）において、情報セキュリティ監査サービスの公務（官公庁・自治体等）及びセキュリティ診断サービスの公務（官公庁・自治体等）に登録されていること。
（５）　本業務を遂行するうえで必要な情報セキュリティの最新動向を常に把握するため、自社にＣＳＩＲＴが構築され、かつサイバーセキュリティ協会及び日本シーサート協会へ加入していること。

7　再委託

本業務の実施にあたっては、個人情報取扱特記事項第１４条に則り対応すること。

8　守秘義務

本業務の内容の機密を保持するとともに、本業務の実施により知り得た情報を契約履行中か否かに関わらず、第三者に提供・開示または漏えいしてはならない。

また、受託者（再委託含む）にあっては、守秘義務遵守の旨を示す誓約書に署名のうえ、本市に対し都度提出すること。

9　その他

その他の留意事項については、以下のとおりとする。

（１）　納品物についての著作権等一切の権利は、本市に帰属するものとする。
（２）　支払は納品・検査後に一括で行う。
（３）　本業務完了後、受託者は本市に返還、納品、特に保管を要する物を除き、業務処理上作成した文書一切を抹消、焼却、切断など復元不可能な状態にして処分するものとする。
（４）　受託者は、必要に応じて、業務過程の各段階の責任者を定め、処理状況を記録する等の措置を講じるものとする。
（５）　本業務を行うに当たっては、本市担当者と協議のうえ、定期的な打ち合わせを持つこととする。
（６）　本仕様書に記載されていない事項、または仕様について疑義が生じた場合は、本市、受託者双方が協議して決定するものとする。
（７）　納品物及び本業務を実施するにあたって使用する物品は、可能な限り環境に配慮した物を使用するものとする。