別紙 1

業務概要

1　件名

世田谷区情報セキュリティ監査等業務委託

2　履行期限

契約締結日から令和９年３月３１日まで

※委託契約は単年度ごとに行い、前年度の履行内容が良好と認められること、予算が区議会で議決され、配当されることを条件として翌年度の契約を行う。

3　履行場所

（1） 世田谷区事務センター（世田谷区弦巻２丁目２３番１号）

（2） 受託者の事業所

（3） その他、世田谷区（以下。「区」という。）が指定する場所

4　監査目的

本業務は、区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資産の管理、各種情報システムの保守・運用等の情報セキュリティ対策について、第三者による独立かつ専門的な立場から、基準等に準拠して適切に実施されているか否かを点検・評価し、問題点の確認、改善方法等についての検討、助言、指導を行うことによって、区の情報セキュリティの向上に資することを目的とする。

5　履行内容

（1）外部監査・フォローアップ監査・基幹システム外部データセンター監査・基幹システムオペレーションセンター監査実施

区と協議のうえ、客観的な情報セキュリティ監査基準に基づき、区の実情にあった監査項目を抽出し、監査対象におけるシステム運用管理及びシステム利用、電算処理の外部委託契約内容等に関する世田谷区情報セキュリティポリシー等への準拠性について、助言型監査を実施すること。（詳細は、別紙１−１「委託業務内容」参照）

なお、基幹システム外部データセンター監査および基幹システムオペレーションセンター監査は1年ごとに交互に行うものとする。上記２種の監査の実施手順や提出物等は共通であるため、以下、基幹システム外部データセンター監査に関する記述は基幹システムオペレーションセンター監査にも適用されるものとする。

（2）内部監査・セルフチェック実施支援

区が実施する内部監査及びセルフチェック業務の実施を支援すること。（詳細は、別紙１−１「委託業務内容」参照）

（3）標的型攻撃メール訓練実施

区職員に対して標的型攻撃メールを装った模擬訓練メールを送信し、職員が不審な点に気付いて開封を回避できるかを訓練すること。（詳細は、別紙１−１「委託業務内容」参照）

（4）打ち合わせの実施

区と受託者は、実施計画書の進捗状況等について報告するために、必要に応じて打ち合わせを実施する。開催方式については原則対面とするが、Web 会議（リモート参加）も可能とする（実施する場合は、区が用意する Teams 会議を利用するものとする）。打ち合わせの記録（議事録）を作成し、原則３営業日以内に区側担当者あて送付し、確認すること。

（5）世田谷区情報セキュリティ監査等業務委託の全体報告書の作成

年度内の作業履行の実態を踏まえ、全体の監査結果等や評価、今後の提言等をとりまとめた「情報セキュリティ監査等業務委託全体報告書」を作成すること。また、必要に応じて、区の指示により CISO 等への報告の場に同席すること。

（6）「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」に関する問い合わせ対応

区が実施する、世田谷区情報セキュリティポリシーの改正を支援するため、区からの問い合わせをメール等で受付し、回答すること。回答や助言は、監査等の実施内容を踏まえて行うものとする。また、回答はメールや電話等を利用して行うこと。回答後は、問い合わせ内容及び回答内容を「問い合わせ管理台帳」に記録すること。

（7）共通基盤システム監査実施

本監査項目は、令和９年度に実施する。区と協議のうえ、「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（最新改訂版：総務省）」（以下、「監査ガイドライン」という。）や客観的な情報セキュリティ監査基準に基づき、監査ガイドラインに記載されている「β’モデルを採用する場合の追加監査項目」及び「β・β’モデルを採用する場合の組織的・人的対策に係る監査項目」への準拠性について、助言型監査を実施すること。

監査の実施にあたり、監査項目の内容に応じて、システムの画面上で実施状況を確認する等の手法にて証拠を収集すること。（詳細は、別紙１-１「委託業務内容」参照）

なお、本監査の報告書については、地方公共団体情報システム機構へ提出することを前提とする。

6　監査の適用基準

（1）世田谷区情報セキュリティポリシー

（2）区が提示する世田谷区情報セキュリティポリシー関連規程類（世田谷区情報セキュリティ共通実施手順／個別実施手順ネットワークシステム版／個別実施手順スタンドアロンシステム版、電算処理の業務委託契約の特記事項（兼電算処理の個人情報を取り扱う業務委託契約の特記事項）、その他の規程類）

（3）情報セキュリティ監査項目（「監査ガイドライン」）

（4）基幹システム外部データセンターシステム運用管理に関する要件（区と外部データセンターとの運用に関する契約仕様書に添付されている。本要件のうちセキュリティに関する項目数は 12 項目である。）

（5）その他、業務実施に関し有用な基準で、区と協議のうえ採用することとしたもの

7　監査人要件

（1）本件業務は、２名以上の監査人により行うこと。

（2）監査人のうち、チームリーダーを含めた複数名（主監査人及び主監査人補佐）に、以下のいずれかの資格を有する者をあてること。

①ＩＳＭＳ主任審査員又は審査員

②公認情報システム監査人（ＣＩＳＡ）

③システム監査技術者

④公認システム監査人（ＣＳＡ）

⑤ＪＡＳＡ公認情報セキュリティ主任監査人又は公認情報セキュリティ監査人

（3）本業務全体を管理し、区との窓口になるプロジェクト管理責任者を選任し、区へ通知すること。

（4）本業務の履行にあたっては、（2）に記載の資格を有する主監査人および主監査人補佐を割り当て、遅滞なく業務を推進できる体制を構築するものとし、監査の実施や計画書・報告書の作成等にあたるこ

と。また、区の業務担当者との会議・ミーティング等においても、（２）に記載の資格を有する主監査人又は主監査人補佐を必ず出席させること。

（５）主監査人および主監査人補佐は、自治体や省庁で稼動している基幹業務システム及び共通基盤システム（電子メールや職員ポータル等の庁内で共通するシステム）の情報セキュリティ監査を実施した実績を有していること。

（６）監査チームの構成員は、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企画、開発、運用、保守等に関わっていないこと。

８　納品物

（１）種別及び納期

No.	納品物	納期
1	外部監査計画書	外部監査実施初日の１週間前（※）
2	外部監査チェックシート	外部監査実施初日の１週間前（※）
3	外部監査結果一覧	別途、区との協議により定める
4	外部監査報告書	別途、区との協議により定める
5	フォローアップ監査計画書	フォローアップ監査実施初日の１週間前（※）
6	フォローアップ監査チェックシート	フォローアップ監査実施初日の１週間前（※）
7	フォローアップ監査結果一覧	別途、区との協議により定める
8	フォローアップ監査報告書	別途、区との協議により定める
9	基幹システム外部データセンター監査計画書	基幹システム外部データセンター監査実施初日の１週間前（※）
10	基幹システム外部データセンター監査チェックシート	基幹システム外部データセンター監査実施初日の１週間前（※）
11	基幹システム外部データセンター監査結果一覧	別途、区との協議により定める
12	基幹システム外部データセンター監査報告書	別途、区との協議により定める
13	内部監査事前調査票	別途、区との協議により定める
14	内部監査チェックシート	内部監査実施初日の１ヶ月前
15	内部監査結果集計表（概要版・詳細版）	別途、区との協議により定める
16	内部監査結果に対する提言書	別途、区との協議により定める
17	セルフチェック結果集計表（所属職層別版・概要版・詳細版）	別途、区との協議により定める
18	セルフチェック結果に対する提言書	別途、区との協議により定める
19	標的型攻撃メール訓練実施計画書	別途、区との協議により定める
20	標的型攻撃メール訓練実施報告書	別途、区との協議により定める
21	情報セキュリティ監査等業務委託全体報告書	別途、区との協議により定める
22	打合せ資料及び議事録	別途、区との協議により定める
23	共通基盤システム監査計画書	監査実施初日の１週間前（※[1]）
24	共通基盤システム監査チェックシート	監査実施初日の１週間前（※[1]）
25	共通基盤システム監査結果一覧	別途、区との協議により定める
26	共通基盤システム監査報告書	別途、区との協議により定める

※ 実施のスケジュールについては、区との調整のうえ決定する。

（２）納品媒体

MS-Office 製品がサポートするファイル形式等で納品すること。なお、契約期間末までには、すべての納品物を MS-Office 製品がサポートするファイル形式または PDF にして、最終納品物として１部納品

すること。納品物の提出は、区が指定するファイル転送サービスを利用して行うものとする。なお、納入する電子媒体は、最新のソフトウェアでウィルスチェックを行い、使用したソフトウェア名及びウィルスチェックを行った日付を電子媒体の表面もしくは別紙に明記し、納入すること。また、データ編集可能な形式とし、セキュリティロックなどは行わないこと。

９　納入場所

世田谷区ＤＸ推進担当部ＤＸ推進担当課（世田谷区弦巻２－２３－１　世田谷区事務センター内）

なお、令和８年度中に世田谷区役所本庁舎への移転を予定しているため、移転後は本庁舎の住所を納入場所とする。（世田谷区世田谷４－２１―２７）

１０　成果物の帰属

委託業務により生じた全ての物件、成果物の権利は区に帰属するものとする。

（１）納入物件に関する著作権は、契約金額の支払い完了を以って区に帰属する。但し、納入物件に含まれる、受託者が従前より有しているものに関する著作権は、受託者に留保される。また、事前に区の承認を受けることにより、受託者は納入物件を複製・改変して他の業務に利用することが出来る。

（２）区は、納入物件を受託者の承認なく、区の業務のためにのみ改変できるものとし、区が受託者に当該改変作業に必要な納入物件の分析及び情報提供を委託する場合には、別途、区と受託者との間で協議する。

１１　支払方法

検査合格後、受託者の請求に基づき支払う。（１回）

１２　委託業務における留意事項

委託業務の実施にあたっては、以下の事項に留意すること。

（１）あらかじめ、以下の内容を含む従事者名簿を提出すること。

①主たる勤務場所の郵便番号、住所、電話番号

②所属組織名、部署名及び肩書

③電子メールアドレス

④緊急連絡先（業務用携帯電話番号等）

⑤情報セキュリティ監査業務の経験履歴

⑥情報セキュリティ監査に係る保有資格名及び当該資格取得年月

（２）受託者は、実施工程表等を明記した実施計画書を作成し、区との協議により委託業務の詳細内容及び実施時期を決定するものとする。スケジュール（予定）は以下のとおり。

５月～１２月　　共通基盤システム監査実施（令和９年度のみ）

７月～９月　　標的型攻撃メール訓練実施

７月～１２月　　外部監査・フォローアップ監査・基幹システム外部データセンター監査実施

８月～１０月　　セルフチェック実施

８月～１２月　　内部監査実施

２月～３月　　世田谷区情報セキュリティ監査等業務委託の全体報告書の作成

（３）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区が妥当と判断する範囲で提供する。なお、受託者は、区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区に返還し、又は破棄するものとする。

（４）秘密保持等

受託者は、本業務の実施にあたり、知りえた情報及び成果品の内容を他に開示し、又は自らの利益のために利用してはならない。これは、契約終了後又は契約解除後においても同様とする。

（５）議事録等の作成

受託者は、本業務の実施にあたり、区と行う会議、打合せ等に関する議事録を作成し、その都度、内容について区の確認を得るものとする。

（６）関係法令の遵守

受託者は、本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。

（７）報告等

受託者は、作業スケジュールに十分配慮し、区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　受託者の要件

（１）受託者は、令和３年度以降、自治体又は官公庁で情報セキュリティ監査業務を実施した実績があることを要件とする。

（２）受託者は、「情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度」の認証を取得していることを要件とする。

１４　その他

（１）別紙１-２「電算処理の業務委託契約の特記事項（兼電算処理の個人情報を取り扱う業務委託契約の特記事項）」を遵守すること。

（２）本仕様書に定めない事項については、区と協議のうえ定めること。

別紙 1-1

委託業務内容

1　プロジェクト管理

当業務を遂行するにあたり、管理者を選任し、スケジュール管理、品質管理など、プロジェクト全体のマネジメントを行わせること。

2　外部監査・フォローアップ監査・基幹システム外部データセンター監査実施

2－1　外部監査

（1）対象及び実施場所

①情報システム所管課３課

実施場所：監査対象の現地（世田谷区内）

監査対象となる情報システム数は、１システム以内とする。なお、必要に応じて情報システム利用課１課を加えること。

②情報システム所管課の業務委託先事業者３社以内

実施場所：業務委託先事業者の現地または上記監査対象の現地（世田谷区の近隣市または区内）

業務委託先事業者への監査は必要に応じて実施すること。

（2）実施内容

受託者は、区が提示する監査計画に基づき、以下の手順に準じて本件監査を実施すること。

①予備調査

監査対象に対して、以下の予備調査を行うこと。

ア．文書確認

区が提示する、情報セキュリティに関連する規程文書及び監査対象の業務、過去に実施した他所属における監査結果等に関連する資料等を確認し、区及び監査対象の概要を把握すること。

文書確認の結果、監査重点項目や指摘事項になると判断されるものについて、一覧にして整理すること。

イ．事前ヒアリング又は文書による調査

必要に応じて監査対象に、ヒアリング又は文書による調査を実施して業務実施状況やシステムの構成、管理、利用状況の概要等を聴取し、実効性に優れた最適な監査を実施できるよう十分に現場を把握すること。

ヒアリングの結果に基づき、上記ア.の文書確認結果一覧に必要な加除訂正をすること。

②監査

監査計画書等の作成及び監査対象に対する監査を行うこと。

ア．監査計画書及び監査チェックシートの作成

上記①の結果を踏まえて、それぞれ以下の事項を含む監査計画書及び監査チェックシートを作成、提出すること。

【監査計画書に記載する事項】

・監査基準

・監査対象部門（部門名、責任者等）及び監査対象システム

・監査従事者及び体制

・監査実施方法の要領

・収集する監査証拠の範囲
・監査証拠の収集方法
・実施スケジュール
・評価基準
・その他本件監査に必要な事項

【監査チェックシートに記載する事項】
・監査項目
・監査項目ごとの該当する適用基準
・確認の要点
・監査証拠の例示
・その他本件監査に必要な事項

イ．監査の実施

監査対象に対し、実施場所において、文書確認、ヒアリング調査、現地視察調査及びシステムの設定状況の調査を実施すること。

ウ．監査実施結果の作成

上記イの監査実施結果を踏まえ、監査実施内容、監査証拠を記載した監査結果一覧を作成、提出すること。

③実施報告

実施した監査で得られた結果について、監査報告書を作成、提出すること。
報告書には､本件監査の目的に照らして必要だと判断した事項を明瞭に記載すること。
報告書は、Ａ４判で作成し、１つの指摘事項に対する具体的な改善提案は、概ね１ページ以上とすること。

④改善計画の確認

監査対象所属が作成した改善計画案をレビューし､必要に応じて助言を提案すること。

２－２　フォローアップ監査

（１）対象及び実施場所

令和７年度の外部監査対象（３課）
実施場所：監査対象の現地（世田谷区内）

（２）実施内容

令和７年度に実施した外部監査の指摘事項及び特記事項に対する改善状況について、監査対象が作成した改善計画書兼進捗状況一覧表を基に、点検、評価すること。

参考として、令和６年度に実施した外部監査の指摘事項及び特記事項は、２課合わせて２３項目程度である。

監査の実施にあたっては上記２－１（外部監査）同様（ただし、事前ヒアリング又は文書による調査については、必要に応じて実施すること）に行い、以下の４点を作成、提出すること。

①監査計画書
②監査チェックシート
③監査結果一覧
④監査報告書

２－３　基幹システム外部データセンター監査

（１）対象及び実施場所

①基幹システム外部データセンターまたは基幹システムオペレーションセンター

実施場所：１年ごとに、下記２か所を交互に監査対象とする。

基幹システム外部データセンターの現地（世田谷区の近隣市）
基幹システムオペレーションセンターの現地（世田谷区の近隣市）

（２）実施内容

上記２－１　外部監査（２）と同等の内容とする。

ただし、監査基準となる文書は以下の２点とする。

・基幹システム外部データセンターシステム運用管理に関する要件

（基幹システムオペレーションセンター監査の場合は、同センターのシステム運用管理に関する要件）

・区の電算処理の業務委託契約の特記事項

また、監査チェックシートに記載する事項は以下のとおりとする。

【監査チェックシートに記載する事項】

・監査項目
・監査項目ごとの該当する適用基準
・確認の要点
・監査証拠の例示
・その他本件監査に必要な事項

監査の実施にあたっては上記２－１（外部監査）同様に行い、以下の４点を作成、提出すること。

①監査計画書
②監査チェックシート
③監査結果一覧
④監査報告書

３　内部監査・セルフチェック実施支援

３－１　内部監査

（１）対象

書類監査：５０～６０所属程度
現場監査：１０所属程度　※書類監査の結果を基に選定

（２）実施支援内容

①内部監査チェックシートの作成

現場監査の前に、５０～６０所属程度を対象として書類監査を行うこととする。世田谷区情報セキュリティポリシー及びその関連規程類の遵守状況をチェックできるよう、書類監査、現場監査の共通で使える「内部監査チェックシート」（２０項目程度）を新たに作成すること。【内部監査チェックシートに記載する事項】

・監査項目
・ヒアリング目的
・監査内容／確認ポイント
・監査証拠の例示
・監査項目ごとの該当する適用基準
・その他本件監査に必要な事項

②現場監査対象選定の支援

書類監査の結果を基に、現場監査対象の所管（１０所属程度）を選定するため、どの所属を監査対象にするべきか等の助言を行うこと。

③結果集計表及びセキュリティ向上のための提言書作成

区が提示する内部監査の実施結果を一覧化し、区の指定する様式に沿って集計表（詳

細版及び概要版）に整理すること。
上記集計結果及び過去の内部監査結果を踏まえて、被監査部門だけでなく、全組織に存在する課題あるいは効果的な改善策であるもの等を明記し、組織全体のセキュリティを向上させるための施策を提言書としてとりまとめること。

３－２　セルフチェック

（１）対象

区の職員（７，０００名程度）、情報化担当者（２９０名程度）

（２）実施支援内容

①セルフチェックシートの作成支援

区が、セルフチェックの実施にあたり作成する「セルフチェックシート」（選択式、全職員用２０項目程度、情報化担当者用３５項目程度）について、区が提示する過去のセルフチェック資料等に基づき、必要なアドバイスを実施するなど、その作成を支援すること。

②結果集計表及びセキュリティ向上のための提言書作成

区が提示するセルフチェック（全職員用及び情報化担当者用）の結果（ＭＳ－Ｅｘｃｅｌ形式のデータを予定）を集計するとともに、概要を一覧化し、区の指定する様式に沿って集計表（所属職層別版・概要版・詳細版）に整理すること。

上記集計結果及び過去のセルフチェック結果をもとに、全組織に存在する課題あるいは効果的な改善策であるもの等を明記し、組織全体のセキュリティを向上させるための施策を提言書としてとりまとめること。

４　標的型攻撃メール訓練実施

（１）要件

メール送信数：区職員のメール数約 7,000 名のうち、訓練の効果が期待される送信数。
送信回数：１回以上
訓練形式：添付ファイル付きメールまたは URL リンク付きメール、若しくはその両方

（２）区の環境

職員が利用するメール環境は下記のとおり。

環境（予定）	メール数
職員が利用するパソコンがインターネット環境に接続された環境。（β’モデル）インターネットメールについては、区サーバの Microsoft Defender for Office 365 により添付ファイルの解析及び悪意のある URL の検査を実施したうえで、メール本文及び添付ファイルが受信される。 メール本文の URL リンク先をクリックしてウェブサイトを参照することができる。	約 7,000

パソコンの仕様は以下のとおり。

OS	Windows11
メールソフト	Microsoft Outlook for Microsoft 365
Word、Excel 等ソフト	Microsoft Office 365
ブラウザ	Microsoft Edge、Google Chrome

（３）事前準備

区の環境をもとに、訓練の効果が期待される送信数、送信回数、実施時期及び訓練形式等について区と協議のうえ、実施計画書を作成する。

（４）テスト送信

事前にテストメールを送信して、受信確認を行う。テストメールにおいて、メールが正常に受信できない事象（受信拒否等）が発生した場合、メール内容の変更やホワイトリスト設定を行う等の回避策について区と協議すること。

（５）訓練メール送信

訓練対象の職員に対して模擬訓練メールを送信する。区のメールサーバに負荷がかからないよう送信間隔を調整すること。

（６）実施報告

開封状況を所属職層別に集計し、評価結果について実施報告書を作成、提出すること。

５　共通基盤システム監査実施（令和９年度に実施予定のため、令和８年度は実施しない）

（１）対象及び実施場所

対象所属：共通基盤システムの所管課（ＤＸ推進担当課）

必要に応じて、上記以外にも区が全庁の部署から選定する１課について実施状況の確認をすること

対象システム：共通基盤システム※

※共通基盤システムには以下のものを含む。

・庁内ネットワーク及びネットワーク分離(β´モデル)（LGWAN 及びインターネットへの接続を含む）に関すること

・職員のＩＣカードやユーザ ID の管理に関すること

・事務用パソコンやプリンタの管理に関すること

・庁内で共通するシステム（ActiveDirectory、電子メール（MS-Exchange)、ファイルサーバ、職員ポータル（MS-Sharepoint）等）に関すること

実施場所：区が選定する世田谷区内の現地（監査を実施する場合）

（２）実施内容

①予備調査

監査対象に対して、以下の予備調査を行うこと。

ア．文書確認

区が提示する、情報セキュリティに関連する規程文書、監査対象の業務並びにネットワークや基盤システムの構成及び運用方法等に関連する資料等を確認し、区及び監査対象の概要を把握すること。

文書確認の結果、監査重点項目や指摘事項になると判断されるものについて、一覧にして整理すること。

イ．事前ヒアリング又は文書による調査

必要に応じて監査対象に、ヒアリング又は文書による調査を実施して業務実施状況やシステムの構成、管理、利用状況の概要等を聴取し、実効性に優れた最適な監査を実施できるよう十分に現場を把握すること。

ヒアリングの結果に基づき、上記ア.の文書確認結果一覧に必要な加除訂正をすること。

②監査

監査計画書等の作成及び監査対象に対する監査を行うこと。

ア．監査計画書及び監査チェックシートの作成

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」（１３項目）及び「β・β’モデルを採用する場合の組織的・人的対策に係る監査項目」（２３項目）についてチェックシートを作成、提出すること。

ただし、監査ガイドラインの改定があった場合は、監査項目を追加・変更する場合がある。

【監査計画書に記載する事項】

・監査基準
・監査対象部門（部門名、責任者等）及び監査対象システム
・監査従事者及び体制
・監査実施方法の要領
・収集する監査証拠の範囲
・監査証拠の収集方法
・実施スケジュール
・評価基準
・その他本件監査に必要な事項

【監査チェックシートに記載する事項】

・監査項目
・監査項目ごとの該当する監査ガイドラインの例文の番号
・確認の要点
・監査証拠の例示
・その他本件監査に必要な事項

イ．監査の実施

監査対象に対し、現地において、文書確認、ヒアリング調査、現地視察調査及びシステムの設定状況の調査を実施すること（１日程度）。

なお、監査項目の内容に応じて、システムの画面上で実施状況を確認する等の手法にて証拠を収集すること。

③実施報告

実施した監査で得られた結果について、監査報告書を作成、提出すること。

報告書には、本件監査の目的に照らして必要だと判断した事項を明瞭に記載すること。

報告書は、Ａ４判で作成し、１つの指摘事項に対する具体的な改善提案は、概ね１ページ以上とすること。

また、必要に応じて区確認用と地方公共団体情報システム機構への提出用の２種類の監査報告書を作成すること。

６　その他

本紙に定めのない実施の詳細は、事前に区と協議のうえ定めること。

別紙 1-2

電算処理の外部委託基準　別紙

電算処理の業務委託契約の特記事項
（兼電算処理の個人情報を取り扱う業務委託契約の特記事項）

（秘密保持義務）

1　受託者は、当該委託契約（業務内容に保守委託を伴う賃貸借契約等を含む。以下同じ。）に係る電算処理業務（以下「委託業務」という。）により知り得た個人情報その他の情報（以下「情報」という。）を、いかなる理由があっても第三者に漏らしてはならず、この旨を委託業務に従事する者（以下「従事者」という。）へ周知徹底しなければならない。また、契約期間満了後も、同様とする。

（書面主義の原則）

2　受託者は、本特記事項により通知、報告、提出等が求められている事項については、特段の定めがない限り、書面により行うものとする。

（管理体制等の通知）

3　受託者は、当該委託契約の締結後直ちに、以下の文書を区に提出しなければならない。提出後に内容の変更があった場合も、同様とする。

(1) 情報セキュリティ及び個人情報保護に関する社内規程又は基準

(2) 以下の内容を含む従事者名簿

① 電算処理の責任者及び電算処理を行う者の氏名、責任、役割及び業務執行場所

② 委託業務において個人情報を取り扱う者の氏名、責任、役割及び個人情報の授受に携わる者の氏名並びに業務執行場所

③ 委託業務に関する緊急時連絡先一覧

(3) 委託業務に係る実施スケジュールを明記した文書

(4) 委託業務において使用する情報システムのネットワーク構成図（特定個人情報ファイル（コンピュータ等で検索することができるよう体系的に構成した情報の集合物であって、個人番号をその内容に含むもの。以下同じ。）を取り扱う場合のみ。第 23 項の事項を証するもの。）

(5) 委託業務において使用する情報システムのセキュリティ仕様書（特定個人情報ファイルを取り扱う場合のみ。第 24 項の事項を証するもの。）

(6) クラウドサービス（有料、無料に関わらず、民間事業者等がインターネット上で提供する情報処理サービスで、約款への同意及び簡易なアカウントの登録等により当該機能が利用可能となるサービスのこと。以下同じ。）利用に係るリスク対策文書（委託業務においてクラウドサービスを利用する場合のみ。第 25 項の事項を証するもの。）

（再委託の禁止）

4　受託者は、委託業務の全部又は一部を、他の者に再委託してはならない。ただし、附属業務でやむを得ず再委託する必要があるときは、受託者は、再受託者（委託先の子会社（会社法（平成 17 年法律第 86 号）第 2 条第 1 項第 3 号に規定する子会社をいう。）である場合も含む。以下同じ。）に当該委託契約及び本特記事項を遵守させ、かつ、再受託者にかかる再委託の内容及び第３項に規定する事項を、区に事前に書面をもって通知し、その承認を得なければならない。

再受託者も、委託業務の全部又は一部を、他の者に更に再委託してはならない。附属業務でやむを得ず更に再委託する必要があるときは、再委託と同様の条件と手続きにより、区の承認を得なければならない。更に再委託が繰り返される場合も同様とする。

（目的外使用等及び複写等の禁止）

5　受託者は、委託業務で取り扱う情報を委託業務の目的以外に使用してはならない。また、第三者に提供してはならない。

6　受託者は、区が委託業務での使用を目的として受託者に提供し、又は貸与する情報及び情報資産（世田谷区電子計算組織の運営に関する規則（平成１６年世田谷区規則第４７号）第２条第９号に規定する情報資産をいう。以下同じ。）を、委託業務以外の目的に使用してはならない。

7　受託者は、委託業務で取り扱う情報及び情報資産について、業務上必要なバックアップを取得する場合を除き、区の承認を得ずに複写してはならない。委託業務を実施する上でやむを得ず複写するときは、あらかじめ区に通知し、その承認を得なければならない。この場合において、委託業務の終了後、受託者は、直ちに複写した電磁的記録の消去及び印刷物の廃棄を行い、使用できない状態にするとともに、消去又は廃棄した日時、担当者及び処理内容を区に報告しなければならない。

8　受託者は、区の事前の承諾なく、委託業務で取り扱う情報及び情報資産を区の事業所または受託者の事業所から持ち出してはならない。

（物的セキュリティ対策）

9　受託者は、委託業務に使用する情報システムに係る装置の取付けを行う場合は、できる限り、火災、水害、埃、振動、温度、湿度等の影響を受けない場所に設置するものとし、施錠等容易に取り外すことができないよう必要な措置を講じなければならない。

10　受託者は、委託業務に係る区が運用する情報システムのサーバ等を区庁舎外に設置する場

合は、区の承認を得なければならない。また、定期的に当該サーバ等への情報セキュリティ対策状況について確認するとともに、区から要請があった場合は、その結果を区に報告しなければならない。
11　受託者は、その従事者に名札等の着用及び身分証明書等の携帯を義務付け、区の情報システム室その他の区の管理区域に立ち入る場合において区から求められたときは、身分証明書等を提示するよう指導しなければならない。
12　受託者は、委託業務で使用するパソコン等の盗難を防止するため、当該パソコン等をセキュリティワイヤーで固定し、又は従事者が業務執行場所を離れる間において施錠可能なロッカー等に収納させるなどの措置を講じなければならない。

（人的セキュリティ対策）
13　受託者は、委託業務において、区に提出した情報セキュリティ及び個人情報保護に関する社内規程又は基準を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに区に報告し、代替策について協議しなければならない。
14　受託者は、情報及び情報資産を適切に保管するものとし、パソコン等により情報及び情報資産を使用する場合は、第三者に使用され、又は閲覧されることがないように、離席時にパスワードロック又はログオフ等を行わなければならない。
15　受託者は、従事者に情報システムの保守又は運用業務に関し、次の事項を遵守させなければならない。
(1) 自己が利用している ID は、他人に利用させないこと（ID の共用を指定されている場合は除く。）。
(2) 共用 ID を利用する場合は、共用 ID の利用者以外の者に利用させないこと。
(3) パスワードを秘密にし、パスワードの照会等には一切応じないこと（パスワード発行業務を除く。）。
(4) パスワードのメモの不用意な作成等により、パスワード流出の機会を作らないこと。
(5) パスワードは、十分な長さとし、想像し難い文字列とすること。
(6) 複数の情報システムを取り扱う場合は、パスワードを情報システム間で共有しないこと。
(7) パソコン等のパスワードの記憶機能を利用しないこと。
(8) 社員間でパスワードを共有しないこと（ID の共用を指定されている場合を除く。）。
16　受託者は、従事者に対して、情報セキュリティに関する教育及び緊急時対応のための訓練を計画的に実施しなければならない。

（技術的及び運用におけるセキュリティ対策）
17　受託者は、情報システムの保守又は運用業務を遂行するに当たり、情報システムの変更記録、作業日時及び実施者を記録するとともに、各種アクセス記録及び情報セキュリティの確保に必要な記録を全て取得し、一定期間保存しなければならない。
18　受託者は、アクセスログ等を取得するサーバについて、正確な時刻設定を行わなければならない。自動的にサーバ間の時刻同期が可能な場合は、その措置を講じなければならない。
19　受託者は、情報システム等に記録された重要性の高い情報について、定期的にバックアップを取得しなければならない。また、バックアップの取得前にその手法を区に通知し、承認を得なければならない。
20　受託者は、情報システムの開発及び導入に当たり、開発及び導入前に区と協議の上、情報セキュリティに係る検証事項を定め、検証を実施しなければならない。
21　受託者は、委託業務に使用する情報システムがネットワークに接続されている場合は、不正アクセスを防ぐため、常にセキュリティホールの発見に努め、メーカー等からのセキュリティ修正プログラムの提供があり次第、情報システムへの影響を確認し、区と協議の上、修正プログラムを適用しなければならない。また、ウィルスチェックを行い、ウィルスの情報システムへの侵入及び拡散を防止しなければならない。
22　受託者は、情報システムを開発する場合は、システム開発及びテスト環境と、本番運用環境を分離しなければならない。
23　受託者は、委託業務において特定個人情報ファイルを取り扱う場合は、当該特定個人情報ファイルをインターネットから物理的又は論理的に分離された環境にて取り扱わなければならない。
24　受託者は、委託業務に使用する情報システムにおいて特定個人情報ファイルを取り扱う場合は、定期に及び必要に応じ随時に当該情報システムのログ等の分析を行うなど不正アクセス等を検知する仕組みを講じるとともに、当該情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講じなければならない。
25　受託者は、委託業務においてクラウドサービスを利用する場合は、当該クラウドサービスの利用に伴い想定される情報セキュリティ上のリスクを回避するために必要な措置を講じなければならない。（例：当該クラウドサービス提供事業者が公表している情報セキュリティ対策内容の確認、受託者が従業員に付与するクラウドサービス用 ID の適切な付与管理、クラウドサービス上に記録した情報が第三者に提供される場合についての確認、サービス利用終了時のデータの取扱い条件の確認、等）

（データのセキュリティ対策）
26　受託者は、委託業務に関し、区より情報及び情報資産を受領した場合は、預かり証を区に対して交付しなければならない。また、当該情報及び情報資産を適切に管理するため、情報

及び情報資産の受領日時、受領者名、受領した情報及び情報資産の種類等の記録簿を作成するとともに、区から要請があった場合は、速やかに当該記録簿を区に提示しなければならない。

27　受託者は、委託業務に係る重要度の高い情報及び情報資産を運搬する場合は、可能な限り暗号化、パスワード設定等の保護対策を行い、鍵付きのケース等に格納する等、情報及び情報資産の滅失や不正利用を防止するための処置を講じなければならない。また、重要度の高い情報を電子メール等で送受信する場合は、暗号化、パスワード設定等の保護対策を行わなければならない。

28　受託者は、委託業務で取り扱う情報及び情報資産を施錠可能な金庫、ロッカー等に適切に保管する等善良な管理者の注意をもって当たり、情報及び情報資産の取扱いには十分注意し、情報及び情報資産の滅失、毀損及び漏えいの防止に努めなければならない。

29　受託者は、委託業務が終了したときは、区より受領した情報及び情報資産を速やかに区に返却しなければならない。また、返却が不可能な場合は、区の了承のもと、バックアップデータを含む電磁的記録の消去及び印刷物の廃棄を行い、使用できない状態にする（電算処理機器を廃棄する場合は復元できない状態にする）とともに、消去又は廃棄した日時、担当者及び処理内容を区に報告しなければならない。

30　受託者は、情報資産の作成業務を終了したときは、直ちに当該情報資産を区があらかじめ指定した職員に引き渡さなければならない。

（電算処理機器の廃棄）

31　受託者は、委託業務で使用しているサーバ、パソコン等の機器（以下これらを「電算処理機器」という。）を廃棄する場合は、事前に当該電算処理機器に保存されている情報及び情報資産を消去、復元できない状態にした上で廃棄しなければならない。

（委託業務の報告）

32　受託者は、区に対し、委託業務の状況を定期的に報告するものとする。ただし、必要があるときは、その都度報告するものとする。

（監査、施設への立入検査の受入れ）

33　受託者は、情報及び情報資産の情報セキュリティ管理状況について、区の求めに応じて報告するものとする。また、区が必要に応じて監査又は検査を実施する場合は受け入れなければならない。なお、再受託者及び更に再委託が繰り返される場合も同様とする。

34　受託者は、区が必要とする場合は、業務執行場所へ区の職員の立入りを認めるものとする。

（緊急時の対応）

35　受託者は、委託業務において、業務上のトラブル、災害、事故、電算処理機器の不良、故障及び破損等が発生した場合は、直ちに区にその状況について報告し、区の指示に従わなければならない。

36　受託者は、委託業務について次に掲げる事象が発生した又は発生したおそれがある場合は、直ちに、区にその状況を具体的に報告しなければならない。

（1）情報及び情報資産の滅失
（2）情報及び情報資産の毀損
（3）情報の漏えい
（4）不正アクセス
（5）情報セキュリティポリシーの違反
（6）前各号に掲げるもののほか、情報セキュリティに悪影響を及ぼす事象

（サービスレベルの保証）

37　受託者は、委託業務のサービスレベルについて、事前に区と合意している場合は、そのサービスレベルを保証するものとする。

（契約解除及び損害賠償）

38　受託者が、法令及び本特記事項に違反した場合、区は、この契約を解除することができる。ただし、債務の不履行がこの契約及び取引上の社会通念に照らして軽微であるときは、この限りでない。また、受託者は、本特記事項に違反し、又は本特記事項を履行しなかったことにより、区に損害が生じた場合には、区に対しこれを賠償するものとする。