業務委託概要

1　委託の内容

(1) 情報セキュリティ内部監査

本区の情報セキュリティ内部監査を有効に行うため、以下を実施すること。

ア　内部監査項目の見直し

総務省が提示する「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」等を基に、本区の内部監査項目を見直すこと。また、内部監査項目は、有効かつ効果的に区セキュリティポリシー（情報セキュリティ対策基準、情報セキュリティ対策実施要領をいう。以下同じ。）の遵守状況等が把握できるように項目を整備すること。

イ　内部監査様式の見直し

上記アの内部監査項目に合わせて、本区が使用する内部監査チェックリスト及び内部監査関連様式を見直すこと。

ウ　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。

エ　情報セキュリティ内部監査の立会い

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、受託者は適切に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。

なお、監査対象は 12～13 所属程度とする。

- 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

- 内部監査人の権限を越えた質問対応
- 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
- 内部監査報告書のレビュー

オ 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。

- 書類調査
- レビュー

カ 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。

(2) 情報セキュリティ自己点検

本区の情報セキュリティ意識及び区セキュリティポリシーの理解の調査を有効に行うため、以下を実施すること。

ア 調査票の作成

情報セキュリティ意識及び区セキュリティポリシーの理解の調査の実施に必要な項目を設定し、調査票を作成すること。

また、調査項目は、職員の意識啓発に繋がる情報セキュリティリスクの理解度が測定できるようにすること。

なお、自己点検は、一般職員、システム担当者、保護担当者用の 3 つの区分により調査項目を作成すること。

イ 調査結果報告書の作成

自己点検等の結果を収集・分析し、その結果を報告書へ取りまとめること。

ウ 調査結果報告会

上記イで作成した調査結果報告書を基に、本区へ報告すること。

(3) 情報セキュリティ外部監査（情報資産及び特定個人情報）

情報セキュリティ外部監査を有効に行うため、以下を実施すること。

ア 監査対象

監査対象は特定個人情報を取扱う 1 事務（対象課が複数の所属となる場合もある）を対象とし、情報資産に対する監査と特定個人情報に対する監査を併せて、1 所属当たり概ね 1 時間半から 2 時間程度とする。

監査対象は、該当事務における本区で保有する情報資産全般を対象とし、特に特

定個人情報は厳格に監査すること。

イ　外部監査計画書の作成

情報資産及び特定個人情報の監査を効果的に実施するため、次に挙げる監査の手順及びその実施時期を記載した監査計画書を提出し、区及び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こと。

（ア）本調査実施方法の要領

（イ）調査実施場所ごとの監査従事者

（ウ）調査実施場所ごとの調査時期

（エ）収集する監査証拠の範囲

（オ）監査証拠の収集方法

（カ）特段の評価方法があるときはその旨

（キ）評価の日

（ク）監査の協議の日時・内容

（ケ）監査報告会の日時・内容

（コ）その他本件監査に必要な事項

なお、受託者は本件監査の目的を達するため、監査計画書を監査の進行に伴い、区と協議して変更することができる。

ウ　外部監査項目（チェックリスト）の作成

区セキュリティポリシー、国等が示す最新の基準に基づき、情報資産の保護及び特定個人情報の安全管理措置に関する外部監査項目を監査実施前に設定すること。

また、外部監査項目には激化するサイバー攻撃のトレンド、他自治体の傾向及び本区特有の課題を考慮すること。

エ　監査の事前準備

監査を円滑に行うため、受託者は情報資産及び特定個人情報に対する事前調査票を作成し、配付すること。

なお、事前調査の際には、被監査部門へ事前に提出を求める資料を一覧化するなどの工夫をすること。

その後被監査部門から事前調査結果及び事前提出資料を入手し、それを読み込み監査に備えること。

オ　監査説明会

本区の被監査部門に対し、外部監査の趣旨、実施方法、事前調査に係る事前準備等を説明すること。また、それに必要な資料を作成すること。

カ　監査の実施

外部監査計画書に基づき、担当者等へのヒアリング、文書・記録の閲覧、現場の視察等を組み合わせた監査を行うこと。

キ　外部監査報告書の作成

上記エの監査の事前準備及び上記カの監査の実施までの結果を報告書へ取りまとめること。また報告に当たっては、次の観点で可能な限り具体的かつ現実的な評価を行うこと。

(ア)サイバー攻撃に対し必要な情報セキュリティ対策

(イ)情報資産の保護について必要な情報セキュリティ対策

(ウ)特定個人情報の安全管理措置に必要な水準

ク　監査結果報告会

本区の被監査部門に対し、外部監査の結果並びに外部監査結果から見えた本区の課題点について、他自治体の事例等を踏まえた対応方法の説明を行うこと。また、それに必要な資料を作成すること。

(4) 情報セキュリティ外部監査（情報システム）

ア　監査対象

発注者が指定する 2 事務で使用する情報システム（クラウドサービスも含む）を対象として、ポリシー等適用基準の遵守状況及び各情報システムの運用形態に応じた情報セキュリティ対策の妥当性に関する検証・評価及び改善に向けた助言型監査を実施する。

また、必要に応じて保守業者による区情報資産の取扱い状況やデータセンターへの視察及び技術的検証を行うこと。

イ　外部監査計画書の作成

情報システムの監査を効果的に実施するため、次に挙げる監査の手順及びその実施時期を記載した監査計画書を監査実施前に区へ提出し、区及び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こと。

（ア）本調査実施方法の要領

（イ）調査実施場所ごとの監査従事者

（ウ）調査実施場所ごとの調査時期

（エ）収集する監査証拠の範囲

（オ）監査証拠の収集方法

（カ）特段の評価方法があるときはその旨

（キ）評価の日

（ク）監査の協議の日時・内容

（ケ）監査報告会の日時・内容

（コ）その他本件監査に必要な事項

なお、受託者は本件監査の目的を達するため、監査計画書を監査の進行に伴い、区と協議して変更することができる。

ウ　外部監査項目（チェックリスト）の作成

区セキュリティポリシー、各課実施手順、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及びシステム管理基準等を適用基準とし、監査項目を設定すること。

エ　監査の事前準備

監査を円滑に行うため、受託者は対象システムに対する事前調査票を作成し、配付すること。

なお、事前調査の際には、被監査部門へ事前に提出を求める資料を一覧化するなどの工夫をすること。その後被監査部門から事前調査結果及び事前提出資料を入手し、それを読み込み監査に備えること。

オ　監査説明会

本区の被監査部門に対し、外部監査の趣旨、実施方法、事前調査に係る事前準備等を説明すること。

また、それに必要な資料を作成すること。

カ　監査の実施

外部監査計画書に基づき、担当者等へのヒアリング、文書・記録の閲覧、現場の視察等を組み合わせた監査を行うこと。また、必要に応じて、保守業者等も出席を承認し、情報システムの対策状況や保守業者等の区情報資産の管理方法の確認、データセンターの視察においても実施すること。

キ　技術的検証

技術的検証を実施する場合、ツールによって脆弱性の有無について検証すること。実施にあたっては、対象となる情報システム及び各種ネットワークの運用に対して、支障及び損害を与えないこと。

ク　外部監査報告書の作成

上記エの監査の事前準備及び上記オの監査の実施までの結果を報告書へ取りまとめること。また報告に当たっては、次の観点で可能な限り具体的かつ現実的な評価を行うこと。

(ア)サイバー攻撃に対し必要な情報セキュリティ対策

(イ)情報資産の保護について必要な情報セキュリティ対策

(ウ)特定個人情報の安全管理に必要な水準（監査対象が、特定個人情報の扱わないシステムの場合は不要とする）

ケ　監査結果報告会

本区に対し、外部監査の結果並びに外部監査結果から見えた本区の課題点について、他自治体の事例等を踏まえた対応方法の説明を行うこと。また、それに必要な資料を作成すること。

(5)情報セキュリティ教育・研修

情報セキュリティ教育を有効に行うため、以下を実施すること。

研修の実施方法は、e ラーニングとし、それぞれ演習問題も含め 1 回あたり 1 時間程度の所要時間とする。

また、動画の視聴が困難な職場のために同様の内容のテキストも用意すること。

なお、教育・研修の内容は、区のインシデント発生状況を踏まえた内容とすること。

ア　個人情報保護研修

職員に対し、情報セキュリティ対策を維持・向上していく上で必要な教育を行うこと。

なお、個人情報保護委員会ガイドラインに従い、教育・研修の内容は、一般職員・システム担当者・管理職の区分に応じて研修資料及び演習問題に差異を設けること。

イ　特定個人情報保護研修

個人番号事務取扱担当者に対し、特定個人情報の安全管理措置に必要な教育を行うこと。

なお、個人情報保護委員会ガイドラインに従い、一般職員（事務取扱担当者）・システム担当者・管理職の区分に応じて研修資料及び演習問題に差異を設けること。

また、サイバーセキュリティの確保に関する内容も含めること。

(6) 情報セキュリティ事故対応訓練

情報セキュリティ事故対応訓練を実施するために、以下の項目を実施する。

なお、訓練は、区が指定する 23 所属程度を対象に実施する。

また、区職員同士の伝達のみならず区民サービス等への影響が生じる想定の訓練とすること。

ア　各種資料及び書式の見直し及び修正

情報セキュリティ事故対応訓練の実施に必要な資料及び書式を作成する。作成にあたっては、区の状況を踏まえた資料及び書式とする。

また、作成する資料及び書式は以下のものを含むものとする。

(ア) 情報セキュリティ事故対応訓練業務計画書

情報セキュリティ事故対応訓練を実施するための計画を記載した資料。計画書は、年度単位の計画書と訓練当日の計画書を作成する。

(イ) 訓練資料

情報セキュリティ事故対応訓練で使用する資料。

(ウ) 訓練評価報告書

情報セキュリティ事故対応訓練の実施内容について、専門的な視点から講評及び改善事項を記載した資料。

(エ) 情報セキュリティ事故対応訓練業務報告書

情報セキュリティ事故対応訓練業務の実施内容とその結果を報告する資料。

(オ)その他区が必要とする資料

イ　訓練の実施

(ア)打合せ

情報セキュリティ事故対応訓練を実施するために必要な打合せを行う。

(イ)事前準備

訓練シナリオを作成する。

(ウ)訓練の立会い

区が実施する情報セキュリティ事故対応訓練に立会い、訓練実施のアドバイスを行う。

(エ)訓練への助言及び講評

訓練についてアドバイス及び講評を行う。

(オ)訓練結果の報告

後日、報告書を作成し提出する。

(7) インシデント対応

本区のインシデントの発生を予防するために必要な支援及び発生した場合に効果的な再発防止ができるよう、以下を実施すること。

ア　インシデント発生時の臨場による助言

本区でインシデントが発生した場合は、臨場にて発生内容を確認し、原因を追跡するとともに再発防止へ向けた助言を行うこと。なお、臨場による助言の対象数は、年間で５件程度を想定しているが、１件当たり複数の所属が関与してインシデントが発生することもあり得る点に留意すること。

イ　レポートの提出

臨場点検した結果はレポートに取りまとめ、都度、本区へ提出すること。また、年度末には年間の総括を取りまとめた報告資料を提出すること。

(8) 新規の外部事業委託開始及びクラウドサービス導入支援

各所属が新規に行う外部事業委託開始及びクラウドサービス導入に当たり、セキュリティ上の安全性を確保するために以下を実施すること。

ア　チェックリストの作成

外部委託を予定する事業者及び新規に導入するクラウドサービスの検討に必要なチェックリストの作成について助言を行うこと。

(9) 区セキュリティポリシー改訂等の見直し及び作成支援

受注者は、最新の総務省ガイドラインの改訂及び外部監査の結果を加味し、本区が行う区セキュリティポリシー及びインシデント対応ハンドブックの見直しについて専門

的な視点から支援するため、次の業務を行うこと。

ア　区セキュリティポリシー改訂支援

（ア）総務省ガイドラインと区セキュリティポリシーを比較し、相違点（改訂漏れや追加必要事項等）を洗い出し、整合表を作成すること。

（イ）前項アにおける各相違点を区セキュリティポリシーへ反映する上での課題を洗い出し、課題解決及び反映可否判断のために発注者と協議すること。

（ウ）区セキュリティポリシーについて、改訂案、見え消し版及び新旧対照表を作成すること。

イ　実施手順等の見直し及び作成支援

（ア）区セキュリティポリシー及び総務省ガイドラインで求められる実施手順の作成及び見直しの支援を行うこと。

（イ）その他、情報セキュリティに係る専門的知識や他区の作成状況などを考慮した助言を行うこと。

ウ　区セキュリティポリシー改訂等の周知支援

区セキュリティポリシー改訂案の変更点や見直し・作成した実施手順等について、理解を深めるための職員向け教材動画作成又は研修会等を実施すること。

エ　インシデント対応ハンドブックの見直し及び作成支援

区セキュリティポリシー改訂や本区インシデントの発生状況等を踏まえ、インシデント対応ハンドブックの見直し及び作成支援を行うこと。

（10）本業務の進捗管理

本業務を効果的かつ有効に行うため、以下を実施すること。

ア　進捗管理

本業務を遅滞なく遂行するために、進捗管理を行うこと。また、進捗が滞った場合は、スケジュールの見直しや本業務を遂行するための方法を模索し、提案すること。

イ　定例会の開催

定例会は月に1回・各1時間程度開催し、本業務が効率的かつ有効に行えるようにすること。

また、(1)から(9)までの業務の状況及び区のインシデントの発生状況等から、必要に応じて、全庁的な情報セキュリティ向上及びインシデントの未然の防止を目的として専門的見地から区のセキュリティ施策に対して提言を行うこと。

なお、会議は対面又はオンラインでの開催とし、定例会の内容は議事録として記録すること。

ウ　相談事の解決

本区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、他自治体の動向調査等の必要があり相談事が発生した場合は、受注者はこれまでの他自治体等における対応実績を活かした提案を行うこと。

エ　支援計画書の作成

国や他自治体等の動向に鑑みて、本区に適した次期支援計画書（案）を作成すること。

2　個人情報の保護

別紙１－１「機密情報の取扱いに関する標準特記仕様書」のとおり。

3　成果物の提出

本業務で作成した成果物は、本区と調整の上で必要な時期に提出し、それらを取りまとめた納品物として、次の項目を期限内に製本して紙で１部、電子データにて１部を納品すること。

(1)　情報セキュリティ内部監査

ア　内部監査チェックリスト

イ　内部監査様式

ウ　内部監査研修資料

エ　内部監査報告書

(2)　情報セキュリティ自己点検

ア　調査票

イ　調査結果報告書

(3)　情報セキュリティ外部監査（情報資産及び特定個人情報、情報システム）

ア　外部監査計画書

イ　外部監査チェックリスト

ウ　外部監査事前調査票

エ　外部監査報告書

(4)　情報セキュリティ教育

ア　個人情報保護研修資料

イ　特定個人情報保護研修資料

(5)　情報セキュリティ事故対応訓練

ア　情報セキュリティ事故対応訓練業務計画書

イ　訓練資料

ウ　訓練評価報告書

エ　セキュリティ事故対応訓練結果報告書

(6)　インシデント対応

ア　インシデント再発防止レポート

イ　年間の総括を取りまとめた報告資料

(7)　新規の外部事業委託開始及びクラウドサービス導入支援

ア　チェックリスト

(8)　区セキュリティポリシー改訂等の見直し及び作成支援

ア　総務省ガイドライン及び区セキュリティポリシーの相違点整合表

イ　区セキュリティポリシー改訂案（見え消し版含む）

ウ　区セキュリティポリシー新旧対照表

エ　区セキュリティポリシー改訂案の職員向け教材又は研修会資料等

(9)　本業務の進捗管理

ア　議事録

イ　次期支援計画書（案）

(10) その他、本業務において作成した資料等

4　その他

(1) 本業務はすべて受託者で行い、業務の一部であっても本区の同意なく再委託は行わないこと。また、不測の事態発生時に業務が滞ることのないように人員を配置すること。

(2) 本業務の実施時において知り得た情報は、漏らしてはならない。

(3) 本業務を担当する主たる者は、原則として委託期間中変更しないこととする。

(4) 受託者は、貸与を受けた資料等の取り扱いに十分注意し、本業務終了後、速やかに本区に返却するものとする。なお、業務処理上作成した資料等の文書一切を抹消、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。

(5) 労働基準法をはじめ関係法令を遵守し、業務を履行しなければならない。

(6) 本仕様書に記載されていない事項、又は仕様について疑義が生じた場合は、その都度協議のうえ誠意をもって実施すること。

以　上