令和８年度情報セキュリティ監査業務委託

仕様書

－　目　次　－

内容

令和８年５月

千葉市総務局情報経営部業務改革推進課

１　業務名

令和８年度情報セキュリティ監査業務委託

２　目的

本市では、情報セキュリティ上の問題点及び脆弱性を明らかにし、情報セキュリティ対策の実効性を確保することを目的に、情報セキュリティ監査を実施している。

監査業務については、一部を監査法人等に委託し、最新の情報セキュリティ動向（最新の攻撃手法、運用事故例）や専門的知識、経験を活用した監査支援を受けることにより、監査機能の充実及び強化を図ることを目的とする。

また、千葉市情報セキュリティポリシー関連の資料作成に当たり、専門的な知見に基づく支援を受けることで、最新の情報セキュリティ動向や業界のベストプラクティスに準拠し、実効性のある情報セキュリティ対策を講じることを目的とする。

３　発注者

千葉市（総務局情報経営部業務改革推進課）
（住所）千葉市中央区千葉港１番１号　千葉市役所高層棟５階
（電話）043-245-5045
（ファックス）043-245-5692
（電子メール）gyomukaikaku.GEI@city.chiba.lg.jp

４　履行場所

千葉市総務局情報経営部業務改革推進課及び発注者が指定する場所

５　委託期間

契約締結日から令和９年３月３１日まで

６　監査における適用基準

本業務は、契約締結後に発注者から受注者へ提供する下記の規程を踏まえて実施するものとする。

なお、規程については、監査時点における最新版を適用すること。また、下記に掲げるもの以外にも、委託期間中において情報セキュリティに関し有用と認められる基準等であって、発注者と協議の上採用するものについては、必要に応じて適用するものとする。

（１）　千葉市情報セキュリティポリシー
　ア　千葉市情報セキュリティ対策基本方針
　　https://www.city.chiba.jp/somu/joho/kaikaku/security-kihon.html
　イ　千葉市情報セキュリティ対策基準
（２）　千葉市情報セキュリティポリシーに基づくガイドライン

（３） 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」
（４） 総務省「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」
※（１）イ、（２）は非公開資料であることから、発注者と契約締結後に受注者に提供する。
※（１）（２）と（３）（４）の内容が矛盾する場合には、（１）（２）を優先して適用する。

７ 監査人の要件

受注者は、次の（１）～（４）をすべて満たすものとする。
（１）独立行政法人情報処理推進機構がホームページにおいて公表している情報セキュリティサービス基準適合サービスリストの情報セキュリティ監査サービス分野に登録（記載）されていること。
（２）情報セキュリティマネジメントシステム（ISMS）認証を取得していること。なお、契約期間中に上記認証の有効期限が満了する場合は、当該認証を更新するものとする。
（３）監査チームには、次のア、イをすべて満たす者が１人以上含まれていること。なお、アについては、契約期間中に有効期限又は登録期間の定めがある資格については、当該資格を有効に維持すること。
ア 次の（ア）～（キ）いずれかの資格を有すること。
（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） ISMS 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
イ 令和３年度から令和７年度までの間に、地方公共団体等（※１）における情報セキュリティ監査の業務（※２）に従事した実績を有すること。ただし、当該期間内に当該監査業務が完了しているものに限る。
※１ 「地方公共団体等」は下表に記載する国及び団体とする。

区分		※１の対象
国		対象とする。
普通地方公共団体	都道府県	対象とする。
	指定都市	対象とする。
	指定都市を除く市町村	令和８年１月時点の住民基本台帳人口が５０万人以上の市のみ対象とする。
特別地方公共団体	特別区	令和８年１月時点の住民基本台帳人口が５０万人以上の特別区のみ対象とする。
	・地方公共団体の組合 ・財産区	対象外とする。

（地方公共団体の区分は総務省による。
https://www.soumu.go.jp/main_sosiki/jichi_gyousei/bunken/chihou-koukyoudantai_kubun.html）

※２　地方公共団体等における情報資産（情報システム、ネットワーク、情報セキュリティポリシーその他の規程を含む。）に対し、情報セキュリティ上のリスク及び対策の実施状況を評価し、課題の抽出、改善提言その他必要な助言を行うものを指す。

（４）監査チームの構成員が、監査対象となる情報資産の管理に関わっていないこと。

８　監査の実施体制、連絡体制

（１）監査の実施体制

監査チームにおける担当者の配置については、契約締結後に作成・提出する作業計画書に詳細を明記し、発注者の承認を受けること。

また、監査チームの中で主任担当者を定め、発注者からの指示や連絡事項、打ち合わせ内容等が当該主任担当者を通じて確実に関係者間で共有される体制とするとともに、担当者によって成果物等の品質に差が生じないよう、主任担当者が管理すること。

なお、委託期間中の業務担当者の変更は、原則として認めないものとする。やむを得ない事情により業務担当者を変更する場合は、変更の理由、新しい担当者の資格及び経歴等を発注者に示し、承認を得ること。このとき、発注者は新しい担当者の面接を行う場合がある。

（２）連絡体制

発注者との連絡手段は、電子メールを基本とすること。また、隔週を基本として平日（土日休日及び１２月２９日から１月３日を除く、月曜日から金曜日）の中から別途発注者と協議して定める日に、ＷＥＢ会議を基本とした打ち合わせを行い、業務状況等について報告すること。

ただし、ＷＥＢ会議開催のためのソフトウェアライセンスは受注者が用意し、端末は発注者、受注者それぞれが用意するものとする。なお、ＷＥＢ会議開催のためのソフトウェアについては、端末に特別なソフトウェアのインストールを必要とせず、ブラウザで利用可能なものを原則として用意すること。

９　業務内容

【概要】

（１）情報セキュリティ監査	発注者が監査対象局に対して実施する「自己点検」及び「予備調査」の結果を踏まえ、リスク値が高い部署や重点テーマに該当する部署（監査対象課）を対象に書類確認、ヒアリング及び現場確認を行うもの。
（２）情報セキュリティポリシー関連資料作成支援	下記に掲げる事情により情報セキュリティポリシー関連資料に改定が必要な場合に、必要な支援を行うもの。 ・情報セキュリティ監査の結果 ・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」等の改定

	・その他千葉市において情報セキュリティポリシー関連資料を見直す必要が生じた場合

【監査対象課】

千葉市の組織における特定の９局を対象とし、発注者が各局から概ね１課ずつ選定した課を「監査対象課」（監査対象課の数は４課）とする。監査対象局、監査対象課については、契約締結後に受注者に通知する。

【情報セキュリティポリシー】

千葉市情報セキュリティ対策基本方針、千葉市情報セキュリティ対策基準をいう。

なお、千葉市情報セキュリティ対策基準は非公開資料であることから、発注者との契約締結後に受注者に提供する。

【重点テーマ】

本監査における重点テーマは「外部サービス利用に係るガイドライン」とし、監査対象課における契約が当該ガイドラインに沿った対応となっているかを確認するものとする。

なお、本ガイドラインは、千葉市情報セキュリティ対策基準第３５を補足するものであり、非公開資料であることから、発注者との契約締結後に受注者へ提供する。

【自己点検、予備調査】

発注者が監査対象課に対し、情報セキュリティ対策の実施状況等を書面で調査するもの。

（１）情報セキュリティ監査

発注者が監査対象局に対して実施する「自己点検」及び「予備調査」の結果を踏まえ、リスク値が高い部署や重点テーマに該当する部署（監査対象課４課）を対象に書類確認、ヒアリング及び現場確認を行うもの。

ア　作業計画書及びスケジュールの作成並びにCISOへの説明

受注者は、本業務委託に係る作業計画書及びスケジュールの案を作成し、その内容について発注者のＣＩＳＯ（統括情報セキュリティ管理者）まで説明すること。

なお、スケジュールについては、本仕様書の「９　業務内容」に定める各項目をいつ実施するのかが分かるよう、ＷＢＳ（作業分解構成図）等を作成すること。

（ア）日程　　発注者と調整の上決定する（契約締結日から概ね１４日以内とする）

（イ）会場　　千葉市役所（千葉市中央区千葉港１番１号）

（ウ）開催方法　対面又はオンライン

イ　自己点検・予備調査に基づく確認

発注者が監査対象課に対して実施する情報セキュリティに関する自己点検及び予備調査により把握した課題等について、自己点検及び予備調査のみでは確認できない事項がある場合には、追加で提出を求める書類を特定した上で、監査対象課から提出された書類の確認、ヒアリング及び現場確認等の方法により、監査対象課におけるセキュリティ対策が適切に実施されているかを確認すること。

なお、監査対象課への追加書類の提出依頼を含む連絡及びその他必要な連絡については、発注者が行うものとする。

（ア）方針の作成

監査対象課の自己点検・予備調査の結果は、令和８年９月末までに受注者に提供する。

受注者は、監査対象課における情報セキュリティ上の課題を整理した上で、次の事項を記載した方針を作成すること。なお、当該方針については、発注者と協議の上、決定するものとする。

【方針に記載する事項】

監査目的、実施方法（書類確認、ヒアリング、現場確認）、実施期間、監査対象課の作業スケジュール、監査対象課への依頼事項（書類提出等）、指摘・意見の基準、その他発注者が必要と認めた事項

【方針の作成期限】令和８年１０月まで

※発注者は、受注者が作成した方針に基づき、監査対象課に対して監査通知書を送付する。

（イ）書類確認、ヒアリング、現場確認

（ア）で作成した方針に基づき、自己点検及び予備調査のみでは確認できない事項がある場合には、追加で提出を求める書類を特定した上で、監査対象課から提出された書類の確認、ヒアリング及び現場確認等の方法により、監査対象課におけるセキュリティ対策が適切に実施されているかを確認すること。（監査対象課への追加書類の提出依頼を含む連絡及びその他必要な連絡については、発注者が行う。）

なお、ヒアリング、現場確認については、すべての監査対象課に対して一律に実施する必要はない。

ヒアリングの方法は、証跡を残すため原則としてメールで行うほか、対面・WEB 会議を想定している。対面等で行う場合は受注者にて議事録を作成し、５営業日以内に発注者に提出すること。

また、現場確認については、監査対象課４課のうち、情報資産の管理状況を確認する必要性が特に高い部署として、１～３課程度を想定している。ただし、受注者からの求めに応じて、さらに多くの監査対象課に対して現場確認を実施することを妨げるものではない。

現場確認において確認した発見事項の概要については、５営業日以内に発注者に提出すること。

ヒアリング及び現場確認は同日に実施することができるものとする。ただし、現場確認を行う場合は、当日のタイムスケジュールを作成の上、確認内容について事前に発注者の確認を受けること。

＜「自己点検及び予備調査のみでは確認できない事項」に対する確認の例＞

・ 監査対象課に対し、自己点検及び予備調査に基づく回答の根拠資料の提出を求め、情報セキュリティポリシーに基づき適切に運用されているかを確認する。

・ 市民等の来客が多い部署や、情報システムに係るサーバ室を所有するなど、情報資産の管理状況を特に確認する必要性が高い部署については、現場確認を行い、情報セキュリティに係るリスク管理が適切に行われているかを確認する。

【自己点検】

発注者が監査対象局に対し、所有する情報資産の管理状況を確認することを目的として、書面により調査を行うもの。なお、自己点検は毎年度実施している。

発注者は、監査対象局に対して実施する「自己点検」及び「予備調査」の結果を踏まえ、リスク値が高い部署又は重点テーマに該当する部署（監査対象課：４課）を選定する。

【自己点検のイメージ】

自己点検における確認事項は年度ごとに見直しを行っており、例年３０項目程度を設定している。

なお、下記のイメージは令和７年度に実施した自己点検シート（抜粋）であり、本業務で使用する自己点検シートとは内容が異なる可能性があるため注意すること。

No.	カテゴリ	①確認事項
1	1.情報資産の管理	会計年度任用職員に対して、情報セキュリティ対策を遵守する旨の誓約書を雇用の都度徴収していますか。
2		機密性３の情報資産は施錠管理等をし、鍵は無断で持出しができない等適切に管理されていますか。
3		機密性の高い情報資産を市民等の出入りの多いカウンターや通路の近くで保管していませんか。（開庁時間含みます。窓口で応対している申請者の資料は除きます。）
4		機密性３の情報資産や、業務用の端末（ＣＨＡＩＮＳパソコン等）を庁外に持ち出す際は情報セキュリティ責任者の許可を得た上で管理簿等に記載していますか。
5		機密性２以上の情報資産（紙）は、裏紙として使用せず、機密文書の廃棄サービス等を利用して廃棄していますか。

【予備調査】

発注者が、監査対象課が所有する情報資産の種類、量、使用頻度等を確認することを目的として、書面により調査を行うもの。

ウ　重点テーマ（外部サービス利用に係るガイドライン）に係る確認

発注者が指定する監査対象課における契約について、外部サービス利用に係るガイドラインに沿って、契約関係書類（募集要項、契約書、仕様書等、事業者募集から契約締結までの間に監査対象課が作成した一連の書類）が適切に作成されているかを確認すること。

監査対象課のうち、当該確認対象となる契約を保有していない課については、この確認を省略するものとする。

なお、確認対象とする契約は最大４つとする。

確認に当たっては、下記の（ア）、（イ）について、書類確認の他、書類だけで確認が不十分な事項については必要に応じてヒアリング、現場確認を行うものとする。

なお、下記の他に受注者が必要と認めた事項については、発注者と協議の上確認を行うことができる。

＜確認事項＞

（ア）本ガイドラインに基づく「外部サービス利用時チェックリスト」に示された２９のチェック項目が、契約関係書類に適切に反映されているかを確認する。

（イ）監査対象の外部サービスが本ガイドラインに基づく「外部サービス利用管理台帳」に適切に記載されているかを確認する。

上記確認事項（ア）の結果、チェック項目が契約関係書類に反映されている場合において、情報セキュリティ対策の観点から、より適切な記載が認められるときは、助言を行うこと。

また、上記確認事項（ア）の結果、契約関係書類において「外部サービス利用時チェックリスト」に対応する記載が確認できない場合には、発注者が不要と判断した場合を除き、情報セキュリティ対策の実効性が確保されるよう、必要な記載内容又は代替措置について助言（例：受注者において記載例を提示する、受注者において必要な代替措置を提示する）を行い、改善を支援すること。

【外部サービスとは】

外部サービスとは、民間事業者等の外部の組織が一般向けに情報システムの一部又は全部の機能を提供するものをいう。主な例として、クラウドサービスやLGWAN-ASP（エルジーワンエーエスピー）サービス、ホスティングサービス等が該当する。

【外部サービス利用に係るガイドラインの構成】

千葉市情報セキュリティ対策基準第３５を補足するものであり、次の資料で構成される。なお、非公開資料であることから、発注者との契約締結後に受注者へ提供する。

- 外部サービス利用判断基準（PDF、11 ページ）
- 外部サービス利用時チェックリスト（Excel ファイル、29 項目）
- 外部サービス利用時チェックリストの解説書（PDF、11 ページ）
- 外部サービス管理台帳（Excel ファイル）
- 外部サービス利用の管理について（PDF、1 ページ）

・ サンプル：外部サービス利用管理台帳（○○課）（（Excel ファイル））
・ 【参考資料】外部サービスとは（PDF、2 ページ）
・ 【参考資料】「外部サービス利用に係るガイドライン」活用フロー（PDF、5 ページ）
・ 【参考資料】「業務委託」及び「外部サービスの利用」における注意事項について（PDF、12 ページ）
・ 外部サービス利用に係るガイドラインについて（PDF、1 ページ）
・ 外部サービス利用に係るガイドライン Q&A（Excel ファイル、26 項目）

【外部サービス利用時チェックリストの項目】

1　外部サービスの選定基準
（1）外部サービスのセキュリティ要件（1 項目）
（2）外部サービス提供事業者の信頼性が十分であることの総合的・客観的な評価・判断（1 項目）
（3）流通経路全般にわたるセキュリティの適切な確保のためのセキュリティ要件（3 項目）
（4）情報資産が取り扱われる場所等（2 項目）
（5）再委託をする場合（1 項目）
（6）外部サービスの中断や終了時に円滑に業務を移行するための対策（2 項目）
（7）セキュリティ対策（7 項目）
（8）その他要件（4 項目）
2　外部サービスを利用した情報システムの導入・構築時の対策（4 項目）
3　外部サービスを利用した情報システムの運用・保守時の対策（1 項目）
4　外部サービスを利用した情報システムの更改・廃棄時の対策（3 項目）

【外部サービス利用時チェックリストのイメージ】

設問	確認項目	回 答
1 外部サービスの選定基準		
（1）外部サービスのセキュリティ要件		
1-1-1	外部サービスを提供する事業者が外部サービスのセキュリティ要件として、セキュリティに係る国際規格（ISO/IEC 27001）又はそれと同等以上の認証を取得していることを調達仕様書又は入札参加資格要件にて定められているか。	□ はい　□ いいえ
	「いいえ」の場合、その理由や代替措置をご回答ください。	
（2）外部サービス提供事業者の信頼性が十分であることの総合的・客観的な評価・判断		
1-2-1	以下のいずれかの要件を満たしていることを調達仕様書又は入札参加資格要件にて定められているか。 ①外部サービスを提供する事業者がISO/IEC 27017によるクラウドサービス分野におけるISMS認証の国際規格又はそれと同等以上の認証を取得していること。 ②外部サービスが政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program（ISMAP,イスマップ））への登録が行われていること。 ③外部サービスを提供する事業者が日本セキュリティ監査協会のクラウド情報セキュリティ監査の受入れが可能であることやセキュリティに係る内部統制の保証報告書であるSOC報告書（SOC2・SOC3）を取得していること。	□ はい　□ いいえ
	「いいえ」の場合、その理由や代替措置をご回答ください。	

エ　発見事項の作成及び監査結果通知案の作成支援

上記「イ（自己点検・予備調査に基づく確認）」及び「ウ（重点テーマ（外部サービス利用に係るガイドライン）に係る確認）」において、情報セキュリティポリシー、外部サービス利用に係るガイドライン、その他の情報セキュリティ関連資料に照らし、不適切な運用が認められた場合は、当該事項を「発見事項」として整理し、発注者の確認を受けること。なお、監査対象課に対し、「発見事項」について認識の齟齬が生じていないかの確認は、発注者が行うものとする。

発見事項の確認完了後、監査結果通知案の作成支援として、監査対象課ごとに「発見事項」、「指摘・意見の評価」、「想定されるリスク」、「改善提言」を整理すること。

※発注者は、受注者が整理した内容に基づき、監査対象課に対して監査結果通知書を送付する。

【発見事項の確認完了時期】令和９年２月まで

【監査結果通知案の整理の時期】令和９年２月まで

オ　監査結果に係る CISO への説明、監査対象課への説明

受注者は、上記「エ　発見事項の作成及び監査結果通知案の作成支援」にて整理した監査結果通知案の内容について、発注者の CISO（統括情報セキュリティ管理者）まで説明すること。

（ア）日程　　令和９年２月まで　※詳細は発注者と調整の上決定する

（イ）会場　　千葉市役所（千葉市中央区千葉港１番１号）

（ウ）開催方法　対面又はオンライン

受注者は、発注者が監査対象課に対して通知した監査結果について、監査対象課に対して説明を行うこと。ただし、発注者が説明を要しないと判断した場合は、この限りではない。

（ア）日程　　令和９年３月上旬まで　※詳細は発注者と調整の上決定する

（イ）会場　　千葉市役所（千葉市中央区千葉港１番１号）

（ウ）開催方法　対面又はオンライン

カ　事業報告会への出席

受注者は、本業務委託に係る事業報告書の案を作成し、その内容について発注者のＣＩＳＯ（統括情報セキュリティ管理者）まで説明すること。

（ア）日程　　令和９年３月下旬　※詳細は、発注者と調整の上決定する

（イ）会場　　千葉市役所（千葉市中央区千葉港１番１号）

（ウ）開催方法　対面又はオンライン

（２）情報セキュリティポリシー関連資料作成支援

次に掲げる事情により情報セキュリティポリシー関連資料に改定が必要な場合に、必要な支援を行うもの。

・情報セキュリティ監査の結果

・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」等の改定

・その他千葉市において情報セキュリティポリシー関連資料を見直す必要が生じた場合

※支援方法は、発注者が作成した資料等に対する助言を３回程度実施することを想定している。

１０　情報セキュリティに関する事項

本業務では、発注者における機密性３の情報資産（※）を取り扱うことから、下記のとおり情報セキュリティに関する事項を定める。

※「機密性３の情報資産」は、千葉市情報セキュリティポリシー（「千葉市情報セキュリティ対策基本方針」、「千葉市情報セキュリティ対策基準」）に基づく、千葉市における個人情報等の不開示情報を指す。千葉市情報セキュリティ対策基準は、それ自体が機密性３の情報資産であるため、発注者との契約締結後に必要に応じて発注者から受注者に提供する。

（１）情報セキュリティに関する規程の遵守

受注者は、業務の遂行に当たり、「千葉市情報セキュリティ対策基本方針」並びにこれに基づく千葉市の情報セキュリティ関連規程、ガイドライン等を遵守し、発注者が提供する情報の漏えい、改ざん、滅失その他の事故の防止に必要な措置を講じるものとする。

なお、「千葉市情報セキュリティ対策基本方針」を除く資料は非公開情報であることから、発注者との契約締結後、必要に応じて発注者から受注者へ提供する。

また、情報セキュリティに係る各種書類の提出期限は、発注者が別に指定する。

（２）外部サービスの利用に関する制限事項の遵守

受注者が業務の遂行に当たり外部サービス（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について、十分な情報セキュリティ対策が講じられていることを確認できるものとして、次のいずれかを満たすこと。

- ISMAP クラウドサービスリストに登録されていること
- ISO/IEC27017 に基づく ISMS クラウドセキュリティ認証を取得している事業者により提供されるクラウドサービスであること
- SOC2 報告書（Type2）等の第三者保証報告書により、当該サービスの統制状況が確認できること
- その他、これらと同等以上の情報セキュリティ水準を有すると発注者が認めること

（３）受注者の責任者、作業者の所属、作業場所の特定

受注者は、本業務に係る機密性３の情報資産を適正に管理させるための責任者（情報管理責任者）を設置しなければならない。

また、受注者は、本業務に従事する者を明確にし、その者の氏名及び所属を、情報管理責任者、情報取扱従事者（役割の例：情報作業責任者、情報作業従事者、情報授受担当者　等）の役割並びに特定個人情報の取扱いの有無等を明らかにして、その内容を市に通知しなければならない。

受注者は、本業務に係る事務の処理（機密性３の情報資産に限る）については、発注者の庁舎内において行わない場合、当該事務を処理しようとする場所における機密性３の情報資産の適正管理の実施その他の措置について、あらかじめ発注者に届け出て、発注者の承諾を得た場合には、当該作業場所において事務を処理することができる。

（４）従業員に対する教育の実施

受注者は、この業務に係る機密性３の情報資産を取り扱う場合に遵守すべき事項（安全管理措置に係る事項を含む。）、関係法令等に基づく罰則の内容及び民事上の責任その他事務の適切な履行のために必要な事項に関する研修等を行わせることとするとともに、発注者に研修等の実施計画を報告し、また、当該研修等の実施後、速やかにその旨を報告しなければならない。

（５）提供された情報の目的外利用及び受注者以外の者への提供の禁止

受注者は、この業務に係る機密性３の情報資産を目的外に利用し、又は第三者に提供してはならない。

（６）業務上知り得た情報の守秘義務

受注者は、この業務で知り得た機密性３の情報資産をみだりに他人に知らせ、又は不当な目的に利用してはならない。この契約が終了し、又は解除された後においても同様とする。

受注者は、従事者に対し、在職中及び退職後においてもこの契約による事務に関して知り得た機密性３の情報資産をみだりに他人に知らせ、又は不当な目的に利用してはならないことなど、機密性３の情報資産の保護に関して必要な事項を了知させるとともに、了知後速やかにその了知させたことが分かる書面等を提出しなければならない。

（７）再委託に関する制限事項の遵守

受注者は、この業務に係る機密性３の情報資産を自ら取り扱うものとし、第三者に取り扱わせてはならない。ただし、この契約による事務の一部かつ重要な部分に該当しない業務については、次に掲げる事項市に対して報告の上、あらかじめ再委託先において講じられる安全管理措置が発注者と同等程度であると認められるものとして発注者の書面による承諾を得ることで、再委託することができる。

ア　再委託が必要な理由

イ　再委託先

ウ　再委託の内容

エ　再委託先が取り扱う情報

オ　受注者の再委託先に対する監督方法

受注者は、機密性３の情報資産を再委託先に取り扱わせる場合には、この契約により受注者が負う義務を、あらかじめ契約書等で市が指定する事務を除き、「発注者」を「受注者」に、「受注者」を「再委託先」に読み替えて、再委託先に対しても遵守・履行させるとともに、受注者と再委託先との間で締結する契約書等においてその旨を明記しなければならない。この場合において、受注者は、発注者の提供した機密性３の情報資産並びに受注者及び再委託先がこの業務のために取得した機密性３の情報資産をさらに委託するなど、第三者に取り扱わせることを禁止しなければならない。

受注者は、再委託先の当該業務に関する行為及びその結果について、再委託先との契約の内容にかかわらず、発注者に対して責任を負うものとする。

上記の規定は、再委託先が受注者の子会社である場合も同様とする。

（８）委託業務終了時の情報資産の返還、廃棄等

受注者は、この業務のために発注者から貸与され、又は受注者が取得し、若しくは作成した情報資産が記録された資料等を、この契約の終了後直ちに発注者に返還し、又は引き渡すものとする。また、その他発注者の承諾を得て行なった複写又は複製物を含むこの業務のために用いた情報資産については、解読不能な状態で廃棄又は消去しなければならない。なお、当該情報資産が機密性３に該当する場合

は、上記すべての措置について、発注者にその旨の報告をしなければならない。

なお、この業務のために用いた機密性３の情報資産を保存していた電子媒体等を廃棄等する場合は、復元できないよう措置を講ずるものとする。ただし、発注者が別に指示したときは、当該方法によるものとする。

（９）緊急時の報告義務

受注者は、契約書等（契約書、仕様書）に違反する事態及び受託した事務に係る機密性３の情報資産の漏えい、毀損、滅失等が生じ、又は生ずるおそれがあることを知ったときは、速やかに発注者に報告し、発注者の指示に従うものとする。この契約が終了し、又は解除された後においても同様とする。

（１０）発注者による情報セキュリティインシデント発生時の公表

前述の報告があった場合において、発注者は、受注者の意図に関わらず、市民に対して適切な説明責任を果たすため、必要な範囲においてその内容を公表することができる。

（１１）発注者による監査、検査

発注者は、受注者がこの業務に当たっての作業の管理体制及び実施体制や機密性３の情報資産の管理状況について、安全確保の措置の実施状況を確認するため、年１回以上、実地（同一内容の委託事務において委託先や委託先が機密性３の情報資産を取り扱う場所が複数ある場合は、そのうちの一か所以上）に検査するものとする。ただし、次のいずれかに該当する場合は、受注者からの書面の提出をもって替えることができる。

ア　書面による確認で足りる場合

イ　委託先又は委託先が個人情報を取り扱う場所が遠方である場合

ウ　その他実地検査ができないことについてやむを得ない理由があるとき

受注者は、発注者から前述の求めがあったときは、速やかにこれに従わなければならない。

（１２）発注者又は第三者に損害を与えた場合の規定

発注者は、次のいずれかに該当するときには、契約の解除及び損害賠償の請求をすることができるものとする。

ア　この契約による事務を処理するために受注者が取り扱う機密性３の情報資産について、受注者又は再委託先の責めに帰すべき事由により発注者又は第三者に損害を与えたとき。

イ　前号に掲げる場合のほか、受注者がこの契約書等（契約書、仕様書）に違反していると認めたとき。

１１　納品物

下記の納品物を書面（Ａ４版又はＡ３版）又は電子媒体（Microsoft Word形式、Excel形式又はPower Point形式、電子メール提出可）で提出すること。

なお、受注者が納品物作成のために作業する環境は受注者の負担で用意することとし、発注者が別に指定する場合を除いて、発注者からは一切提供しないこととする。

また、納品物に契約不適合が見つかった場合には、本契約終了後においても、速やかに発注者の指示に基づき、関係図書等の改正を行わなければならない。なお、同改正作業に要する費用は、すべて受注者の負担とする。

受注者は、本業務委託終了後であっても、本業務委託の範囲内における発注者の問い合わせ等に応じること。

（１）納品物

ア　作業計画書（書面で提出する場合は２部）

契約締結後、１４日以内に作業計画書を作成の上、発注者の承認を得ること。

〈留意事項〉

(ア) 作業計画書の作成に当たっては、業務項目別に、作業の内容を明確にするとともに、作業間の相互関係を明示すること。また、運営体制（業務担当者の配置を含む）を明示すること。

(イ) 発注者の承認を得た後に作業計画書を変更する場合は、発注者の承認を再度得た上で変更を行い、変更後の作業計画書を再提出すること。

イ　事業報告書（書面で提出する場合は２部）

本業務により実施した成果について、「１０　業務内容」の項目に対応するよう報告書として取りまとめること。

（２）納品物の帰属

納品物及びこれに付随する資料は、すべて発注者に帰属するものとし、書面による発注者の承諾を受けずに他に公表、譲渡、貸与又は使用してはならない。ただし、納品物及びこれに付随する資料に関し、受注者が従前から保有する著作権は受注者に留保されるものとし、発注者は、本業務の目的の範囲内で自由に利用できるものとする。

１２　その他

本業務の実施に当たり、本仕様書に記載のない事項については発注者と協議の上決定するものとする。