＜一般委託＞

平成30年度情報セキュリティ監査業務委託（一般委託）仕様書

平成30年度情報セキュリティ監査業務委託に基づく内容は、本仕様書の定めるところによる。

1	目　　的	本市情報セキュリティポリシーに基づき、本市が実施している情報セキュリティ対策の向上に資すること。
2	履行期間	契約締結の日　から　平成31年3月31日 まで
3	施行場所	横須賀市役所本庁舎等、本市が指定する場所
4	業務内容	別紙特記仕様書のとおり
5	特記事項	「個人情報（特定個人情報を含む）の取扱いに関する特記事項」及び「作業従事者の横須賀市役所等への入退室に関わる事項」の記載内容を遵守すること。
6	関係法規	なし
7	資格要件	別紙特記仕様書のとおり
8	契約方法	総価による業務委託契約（一般委託）
9	支払方法	委託料の支払いは、業務完了後一括払いとする。
10	その他事項	この仕様書に定めのない事項及び疑義を生じた場合は、別途協議するものとする。
11	監　督　員 連　絡　先	横須賀市　政策推進部　情報政策課　ICT推進係　御園生 TEL:046-822-8179　FAX:046-822-9463

＜指示又は希望事項＞	
グリーン 物品購入 及び 環境配慮 関係	・この業務を施行するにあたって、仕様書でグリーン物品購入の指示がある場合は、横須賀市グリーン購入基本方針及び調達方針に基づく環境物品等を納入すること。また、仕様書で特に指示がない場合で委託代金に物品等の購入経費が含まれている場合は、できるだけこの方針に基づく環境物品等の調達をお願いします。 （上記方針については、本市のホームページ「よこすかのグリーン購入」参照） ・本市は、独自の環境マネジメントシステム（YES）により事務事業の環境負荷低減に努めているので、受託者においてもできる限り環境に配慮して業務を執行するようお願いします。

平成30年度情報セキュリティ監査業務委託特記仕様書

１　業務名

平成30年度情報セキュリティ監査業務

２　背景と目的

横須賀市（以下「本市」という。）は、マイナンバーによる情報連携の運用開始を前に、より一層の情報セキュリティ体制を確立するため、総務省の提示する「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」に準拠した情報セキュリティポリシーを策定し、平成29年４月からその運用を開始した。

本業務の受託事業者（以下　「受託者」という。）は、上記のポリシーに基づき本市が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、職員研修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、本市の情報セキュリティ対策の向上に資することを目的とする。

３　履行期間

契約締結の日から平成31年３月31日

４　履行場所

横須賀市役所本庁舎（横須賀市小川町11番地）等、本市が指定する場所

５　監査対象

本市情報政策課（以下「当課」という。）が所管する情報システム（別紙参照）

６　業務内容

総務省の「地方公共団体情報セキュリティ監査ガイドライン」を参考に、次の要領で本市の実情にあった助言型監査を実施すること。

（１）監査業務計画書の作成

契約締結後速やかに監査業務計画書を作成し、本市に提出すること。監査業務計画書には次の事項を含むこと。なお、提出にあたっては事前に本市と協議を行うこと。

ア　予備調査実施方法の要領
イ　監査実施方法の要領
ウ　監査従事者
エ　監査実施時期
オ　収集する監査証拠の範囲
カ　特段の評価方法がある場合はその旨
キ　監査に関する協議の予定日時及び内容
ク　監査結果の報告の予定日時及び内容

（２）監査チェックリストの作成

後述の「**７　適用基準**」で示す基準から、本市の実情に合わせた監査項目を設定し、具体的な確認内容を記載した監査チェックリストを作成すること。作成にあたっては事前に本市と打合せを行うこと。

監査チェックリストの項目は40～50項目程度とし、次のとおり区分すること。

ア　管理体制

イ　情報資産の管理
ウ　物理的セキュリティ
エ　人的セキュリティ
オ　技術的セキュリティ
カ　運用、評価、見直し

（3）監査説明会の実施

監査説明会を次のように実施し、監査対象システムの主担当職員に対し監査の実施内容、手法について説明を行うこと。

ア　実施回数
　１回
イ　対象人数
　10名程度
ウ　実施場所
　本市が用意した場所を使用する。

（4）予備調査の実施

当課に対して、システムの概要等、本業務の実施にあたり必要な情報を把握するための予備調査を実施すること。

なお、予備調査にあたり、ヒアリング・現地調査を要する場合は、本市が指定する職員が立ち会うものとする。

（5）監査の実施

当課に対し、監査チェックリストに基づき、ヒアリング・資料確認、現地調査等を実施すること。

監査の実施にあたっては、本市が指定する職員が立ち会う。

また、業務をできるだけ阻害しないよう、１システム最大２時間程度で実施すること。

（6）監査調書の作成

監査で確認した内容を取りまとめた監査調書を作成し、本市に提出すること。監査調書には次の事項を含むこと。なお、提出にあたっては事前に本市と協議を行うこと。

ア　監査先とその日時
イ　本市及び受託者において監査に従事した者
ウ　監査結果
エ　監査チェックリストの点検及び確認結果
オ　監査結果に対する受託者の意見
カ　事実を証明する証拠資料名等

（7）監査報告書の作成

次の要領で監査報告書を作成し、本市に提出すること。

ア　Ａ４版縦（必要に応じてＡ３版三つ折も可。Ａ３版三つ折の場合、両面印刷は不可とする。）とし、様式は任意とする。
イ　監査報告書は、監査対象についての脆弱点を網羅した非公開の「監査報告書(詳細版)」及び公開を前提とした「監査報告書(概要版)」の２種類を作成すること。
ウ　監査報告書の宛名は、１部を「横須賀市長」宛てとし、他を「横須賀市CISO」宛てとすること。
エ　監査報告書には、実施した監査の対象システム、監査の内容、証拠に裏付けられた合理的な根拠に基づく意見、制約又は除外事項、その他当該監査の目的に照らして必要と判断した事項を明

瞭に記載すること。

オ　指摘事項を記載する場合は、併せて具体的な改善提案を記載すること。

（8）監査報告会の実施

監査対象となったシステムの情報システム管理者に対して、次のように監査結果の報告会を実施すること。

ア　実施回数

１回

イ　対象人数

10名程度

ウ　実施場所

本市が用意した場所を使用する。

エ　説明資料部数

10部程度

7　適用基準

（1）必須とする基準

ア　横須賀市情報セキュリティポリシー
（横須賀市情報セキュリティ規則及び横須賀市情報セキュリティ対策基準）

イ　各システムの情報セキュリティ実施手順書

（2）参考とする基準

ア　横須賀市個人情報保護条例

イ　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）

ウ　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）

エ　上記のほか委託期間において情報セキュリティに関し有用な基準等で、本市と協議して採用するもの

8　受託者及び監査人等の要件

（1）受託者は、経済産業省がとりまとめを行っている「情報セキュリティ監査企業台帳」に登録されており、当該台帳におけるセキュリティ監査対象の分類・業種として「公務（官公庁・自治体等）」を掲げていること。

（2）受託者はISO/IEC27001(JIS Q 27001)認証またはプライバシーマーク認証を取得していること。

（3）監査責任者、監査人、監査補助者、アドバイザー等で構成される監査チームを編成すること。

（4）監査の品質の保持のため監査品質管理責任者、監査品質管理者等の監査品質管理体制をつくること。

（5）監査チームは、受託者と直接雇用関係を有する者であること。

（6）監査チームには、情報セキュリティ監査に必要な知識及び経験（地方公共団体における情報セキュリティ監査の実績）を持ち、次に掲げるいずれかの資格を有する者が１人以上含まれていること。

ア　システム監査技術者

イ　情報処理安全確保支援士

ウ　公認情報システム監査人（CISA）

エ　公認システム監査人
オ　ISMS 主任審査員
カ　ISMS 審査員
キ　公認情報セキュリティ主任監査人
ク　公認情報セキュリティ監査人
受託者は、本業務の契約に先立ち、上記の事実を本市が確認できる書面等を提示または提出すること。

（7）監査チームには、監査の効率と品質の保持のため次のいずれかの実績（実務経験）を有する専門家が１人以上含まれていること。
ア　情報セキュリティ監査
イ　情報セキュリティに関するコンサルティング
ウ　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）
受託者は、本業務の契約に先立ち、上記の事実を本市が確認できる書面等を提示または提出すること。

（8）監査チームの構成員が、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の企画、開発、運用、保守等に関わっていないこと。

9　成果物

納品成果物及び提出期限は次の通りとする。（書面の成果物については、Ａ４版縦を基本とし、必要に応じてＡ３版三つ折も可。Ａ３版三つ折の場合、両面印刷は不可とする）

成果物	部数等	提出期限
監査業務計画書	１部	平成 30 年７月末日
監査チェックリスト	１部	平成 30 年８月末日
監査調書	１部	平成 31 年１月末日
監査報告書（詳細版）	５部	平成 31 年１月末日
監査報告書（概要版）	５部	平成 31 年１月末日
会議議事録	電子ファイル	随時（会議終了後５営業日以内）
上記全ての電子ファイル	電子媒体１部	平成 31 年２月末日

10　成果物の帰属

成果物及びこれに付随する資料は、本市に帰属するものとし、書面による本市の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。

ただし、成果物及びこれに付随する資料に関し、受託者が従前から保有する著作権は受託者に留保されるものとし、本市は、本業務の目的の範囲内で自由に利用できるものとする。

11　委託業務の留意事項

業務の実施にあたっては、以下の事項に留意すること。

（1）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本市が妥当と判断する範囲内で提供する。

なお、受託者は、本市から提供された資料及びデータは適切に保管し、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、契約終了後又は契約解除後は本件監査にあたり収集した一切の資料を速やかに本市に返還するものとする。

（２）技術的検証

技術的検証については、対象情報システム及び行政LAN/WAN の運用に対し、支障及び損害を与えないように実施するものとする。

（３）再委託

受託者は、本業務の実施にあたり他の業者に再委託することを原則として禁止する。再委託が必要な場合は、本市と協議の上、事前に書面により本市の承認を得るものとする。

（４）秘密保持等

受託者は本業務の実施にあたり、知り得た情報及び成果物の内容を正当な理由なく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）個人情報の保護

受託者は、業務の実施に伴い、個人情報を取り扱うときは、別紙「個人情報（特定個人情報を含む）の取扱いに関する特記事項」を遵守しなければならない。

（６）議事録等の作成

受託者は、本業務の実施にあたり本市と行う会議、打ち合わせ等に関する議事録を作成し、５営業日以内に本市にその都度提出して内容の確認を得るものとする。

（７）関係法令の遵守

受託者は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。

（８）報告等

受託者は作業スケジュールに十分配慮し、本市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。

12　その他

本業務の実施にあたり、本仕様書に記載のない事項については本市と協議の上決定するものとする。

（別紙）

平成30年度情報セキュリティ監査対象システム

	監査対象とするシステム名	適用基準となるドキュメント	備考（システムの概要、内訳等）
1	行政情報基盤システム	行政情報基盤 情報セキュリティ 実施手順書	・行政情報基盤（インフラ） ・庁内LAN端末
2	庁内共有ファイルサーバ	庁内共有ファイルサーバ 情報セキュリティ 実施手順書	・庁内共有ファイルサーバ
3	基幹系システム	基幹系システム 情報セキュリティ 実施手順書	（基幹系システムの内訳） ・住民基本台帳システム（含む印鑑システム） ・戸籍システム ・国民年金システム ・税統合システム 税基盤(口座・納貯等) 税証明発行 収滞納管理 個人市民税 法人市民税 軽自動車税 事業所税 たばこ税 固定資産税 ・国民健康保険システム ・介護保険システム ・団体内統合利用番号連携システム ・生体認証装置（基幹系システム用に限る） ・情報持ち出し制御装置（基幹系システム用に限る）
4	情報システム課 コンピュータ室	情報システム課 コンピュータ室 情報セキュリティ 実施手順書	コンピュータ室の入退室管理（生体認証装置・監視カメラ等）
5	情報公開型GIS	情報公開型GIS 情報セキュリティ 実施手順書	市民向け地理情報提供システム
6	公共施設予約システム	公共施設予約システム 情報セキュリティ 実施手順書	市民向け公共施設予約システム
7	統合GIS	統合GIS 情報セキュリティ 実施手順書	庁内利用の統合型GIS
8	統合業務システム	統合業務システム 情報セキュリティ 実施手順書	財務会計・文書管理・文書決裁
9	グループウェア	グループウェア 情報セキュリティ 実施手順書	職員が利用するメール・掲示板・スケジュール管理等

個人情報（特定個人情報を含む）の取扱いに関する特記事項

（個人情報を取り扱う際の基本的事項）

第１条　受託者（以下「乙」という。）は、個人情報（特定個人情報（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第２条第８項に規定する特定個人情報をいう。以下同じ。）を含む。）の保護の重要性を認識し、業務に関して個人情報を取り扱うときは、個人の権利利益を侵害することのないよう、個人情報を適正に取り扱わなければならない。

（適正な管理）

第２条　乙は、個人情報の漏えい、滅失、改ざん、き損及びその他の事故を未然に防止するため必要な措置を講じなければならない。

２　乙は、個人情報の取扱いに関する責任体制を整備し、管理責任者を定めなければならない。

３　乙は、個人情報を取り扱う従事者の範囲を具体的に定め、当該者以外の者が個人情報を取り扱うことがないよう必要な措置を講じなければならない。

４　乙は、個人情報の保管にあたっては、この契約による業務により取得した個人情報とそれ以外の個人情報を明確に区分し、管理しなければならない。

５　乙は、委託者（以下「甲」という。）の指示又は承諾があるときを除き、個人情報を乙の事業所内から持ち出してはならない。

（管理責任者等の教育及び研修）

第３条　乙は、個人情報の保護及び情報セキュリティに対する意識の向上を図るため、管理責任者及び従事者に対し、横須賀市個人情報保護条例第14条（受託者等の責務）、第32条及び第33条（罰則）並びに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第48条、第49条、第50条及び第51条（罰則）の内容並びに本特記事項において従事者が遵守すべき事項その他この契約による業務の適切な履行に関し必要な事項について、教育及び研修を実施しなければならない。

（秘密の保持）

第４条　乙は、個人情報の内容を第三者に漏らしてはならない。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。

２　乙は、この契約による業務の処理の従事者が個人情報を管理責任者の承諾を得ることなく事務所以外の場所に持ち出し、又は不適切な取扱いにより第三者に漏らすことのないように、必要かつ適切な監督を行わなければならない。

（収集の制限）

第５条　乙は、この契約による業務を処理するため個人情報を収集するときは、その目的を明確にし、当該目的の達成に必要な範囲内で、適法かつ公正な手段により収集しなければならない。

（目的外利用等の禁止）

第６条　乙は、甲の指示又は承諾があるときを除き、この契約による業務の目的以外の目的に個人情報を利用し、又は第三者に提供してはならない。

（複写等の禁止）

第７条　乙は、あらかじめ甲の指示又は承諾があった場合を除き、業務を実施するために

甲から提供された個人情報を複写し、又は複製してはならない。

（資料等の返還）

第８条　乙は、この契約による事務を処理するために甲から貸与され、又は乙が収集し、複製し、若しくは作成した個人情報が記録された資料等を、この契約が終了し、又は解除された後直ちに甲に返還し、又は引き渡し、若しくは消去しなければならない。ただし、甲が別に指示したときは、当該方法によるものとする。

２　乙は、前項の規定により電子記録媒体に記録された個人情報を消去する場合は、当該個人情報が復元できないように確実に消去しなければならない。

３　乙は、前項の規定により個人情報を消去した場合は、当該個人情報を消去した旨の報告書を甲に提出しなければならない。

（再委託の禁止等）

第９条　乙は、個人情報の処理を自ら行うものとし、第三者にその処理を委託（以下「再委託」という。）してはならない。ただし、書面により甲の承諾を得た場合は、この限りでない。

２　乙は、個人情報の処理を再委託する場合及び再委託の内容を変更する場合は、あらかじめ次の各号に規定する事項を記載した書面を甲に提出し、前項ただし書きの承諾を得なければならない。

（１）再委託の相手方

（２）再委託を行う業務の内容

（３）再委託で取り扱う個人情報

（４）再委託の期間

（５）再委託が必要な理由

（６）再委託の相手方における責任体制及び管理責任者

（７）その他甲が必要と認める事項

３　乙は、前項の規定により個人情報を取り扱う事務を再委託の相手方（以下「再受託者」という。）に取り扱わせる場合には、乙と再受託者との契約内容に関わらず、再受託者の当該事務に関する行為について責任を負うものとする。

４　乙は、再委託契約において、再受託者に対する監督及び個人情報の安全管理の方法について具体的に指示しなければならない。

５　乙は、この契約による業務を再委託した場合は、その履行を監督するとともに、甲の求めに応じて、再受託者の状況等を報告しなければならない。

（立入調査等）

第10条　甲は、個人情報を保護するために必要な限度において、乙に対し、個人情報を取り扱う事務について管理状況の説明若しくは資料の提出を求め、又は乙の事務所に立ち入ることができる。

２　乙は、甲から個人情報の取扱いに関して改善を指示されたときは、その指示に従わなければならない。

（事故発生時等における報告）

第11条　乙は、個人情報の漏えい、滅失、き損及び改ざん等の事故（以下「漏えい事故」という。）が生じ、又は生ずるおそれがあることを知ったときは、速やかに甲に報告し、甲の指示に従わなければならない。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。

２　乙は、漏えい事故が生じた場合、当該事故の被害を最小限にするため、甲と協力して必要な措置を講じ、かつ、甲の指示に従わなければならない。

（補則）

第12条　乙は、この契約における個人情報の取扱いについて疑義が生じたときは、甲と協議し、その指示に従わなければならない。

平成 30 年 4 月 1 日改訂

作業従事者の横須賀市役所等への入退室に関わる事項

【必要な届け出】

1. 委託契約に関わる作業従事者（予定を含む）について、「作業従事者名簿一覧」を作成し、事前に横須賀市に提出し、その承認を受けることとする。
2. 1 の作業従事者のうち、本市事務室（コンピュータ室等を含む）及び本市職員が指定する施設（以下「関連施設」という）への入退室が必要な者については、「誓約書」に署名の上、横須賀市に提出することとする。
3. 2 を提出した者のうち、本市情報政策課が所管するコンピュータ室への入室が必要な者で、作業の期間・入室の頻度を勘案し生体認証による入室が必要な者については、「コンピュータ室 入室許可申請書」に署名し、顔写真付き身分証明書の写しを添付のうえ、情報政策課に提出し、生体情報等の登録を行うこととする。
4. 3 以外の者のうち、一時的に本市情報政策課が所管するコンピュータ室への入室が必要な者については、「コンピュータ室 一時入室 許可申請書」に署名し、顔写真付き身分証明書の写しを添付のうえ、情報政策課に提出し、入室の許可を受けることとする。
5. 作業従事者名簿一覧に記載されていない者が緊急時等諸事情により、本市事務室及び関連施設への入室が必要となった場合も、事前に本市へ該当作業者の誓約書を提出し承認を受けること。
   また、コンピュータ室への入室が必要な場合は、上記 3 または 4 の記載に従い入室の許可を受けることとする。

【入室時の注意事項】

1. 作業従事者は、「誓約書」、「コンピュータ室 入室 許可申請書兼同意書」、「コンピュータ室 一時入室 許可申請書」に示された事項を遵守すること。
2. 作業従事者は、本市事務室及び関連施設の入退室にあたり、顔写真付き身分証明書の携行を必須とする。入退室時には、本市職員等による荷物チェックを受け、その指示に従うものとする。

【その他】

上記の記載に定めのない事項及び不明な事項については本市職員等の指示に従うものとする。