平成３０年度
情報セキュリティ監査等一式
調達仕様書（案）

平成 30 年３月

厚生労働省政策統括官付

サイバーセキュリティ担当参事官室

目次

1. 作業の概要

1.1 調達件名

平成 30 年度情報セキュリティ監査等一式

1.2 調達の背景

厚生労働省では、平成 27 年 5 月に発生した日本年金機構への不正アクセスによる情報流出事案を踏まえ策定した「情報セキュリティ強化等に向けた組織・業務改革 －日本年金機構への不正アクセスによる情報流出事案を踏まえて－」（平成 27 年 9 月 18 日厚生労働省）及びサイバーセキュリティ戦略本部長の勧告に対する報告書（平成 28 年 4 月 28 日付）において、厚生労働省及び所管法人等の情報セキュリティ対策の強化を図るための取組を実施することとしている（次頁参照）。

平成 29 年度においては、平成 28 年度に引き続き、情報の重要性や業務運営で様々に生じ得る内在するリスクを正しく認識するため、厚生労働省及び所管法人等が保有する情報システムを対象として、構造化されたデータベースが保有する情報資産の棚卸しを行い、さらに個人情報等の重要情報を格納する情報システムについてはリスク評価を実施したところである。さらに、厚生労働省及び所管法人等が保有するファイルサーバ等に格納された非構造化データを対象として、情報資産棚卸し及びリスク評価を実施するための実施ガイドラインを策定したところである。加えて、厚生労働省（内部部局）、外局、地方厚生（支）局、都道府県労働局、施設等機関及び所管法人等を対象として、厚生労働省情報セキュリティポリシー及び情報セキュリティ関係規程等の準拠性や、平成 28 年度情報セキュリティ監査における検出事項に対する措置結果及び改善計画の実施状況について、情報セキュリティ監査を行い、問題点の確認、改善方法等について助言、報告を行う取組を実施したところである。

平成 30 年度においても、引き続き、情報セキュリティポリシー等に基づく情報セキュリティ対策や教育訓練等の継続的な取組が適切に実施されているか、PDCA の観点から確認し、実効性を担保していく必要があるため、情報セキュリティ監査を実施することにより、情報セキュリティ対策の更なる改善に取り組む方針である。

◎「情報セキュリティ強化等に向けた組織・業務改革　－日本年金機構への不正アクセスによる情報流出事案を踏まえて－」（平成 27 年 9 月 18 日厚生労働省）－抜粋－

第2　今回の事案を踏まえた再発防止策

1．厚生労働省における情報セキュリティ対策の強化

(3) 業務運営対策（ルールの見直し、徹底）

② 保有する情報を適切にリスク評価した上での情報管理の徹底

サイバーセキュリティ戦略において、被害を低減する取組として「個人情報や機微な情報を始め、外部に流出することや改ざんされることによって国民・社会等に多大な悪影響を及ぼす機密性・完全性の高い情報への不正なアクセスをより困難なものにするため、業務の内容や取り扱う情報の性質・量に応じた情報システムの分離や運用ルールを含む情報管理の更なる強化に取り組む。」とされています。

厚生労働省では、多種多様な個人情報や機微な情報を扱って業務を遂行していることから、インターネットのもたらす脅威を再認識し、個人情報等重要情報を取り扱う情報システムや業務の現状を把握し、それぞれの実態やリスクを組織的に共有するためリスク評価を実施します。

今後、リスク評価の結果に基づき、業務内容に応じた対策を講じることとしますが、緊急的な対応として、個人情報等の重要情報を取り扱う省内の情報システムについては、インターネットから物理的又は論理的に分離し、インターネットに接続された端末で利用しないこととする措置を講じたところです。

業務内容に応じた対策を講じるに当たっては、インシデント発生時に国民や社会へ与える被害や影響について定量的、定性的に分析を行い、その結果に基づき、事態の被害や影響を最小化するための対策を検討します。

また、対策の実施に当たっては、リスク評価の結果に基づいた機器の設定等はもとより、規程の見直しや職員への啓発等を行い、組織全体として情報を管理する能力を向上させます。

なお、リスク評価については、業務実態や社会の動向等を踏まえ、専門的な見地から実施します。

1.3 目的及び期待する効果

情報資産の棚卸し及びリスク評価や情報セキュリティ監査（以下「監査」という。）を継続して実施することにより、PDCA サイクルを通じて情報セキュリティ対策全般の改善・実効性の向上を図るとともに、厚生労働省（以下「当省」という。）の幹部・職員に対し、厚生労働省情報セキュリティポリシー（以下「厚労省ポリシー」という。）、情報セキュリティ関係規程及び情報セキュリティの脅威に関する理解を深め、厚生労働行政全体について、組織内・組織間連携の強化やリテラシー・スキルの向上を図る。

実施に当たっては、予算の範囲内で最大限の効果を生み出すことができるよう効率的かつ効果的な監査手法を採用することが求められる。

1.4 用語の定義

No.	用語	説明
1	厚労省	厚生労働省（本省）、中労委、厚生局、労働局、労働基準監督署及び公共職業安定所、施設等機関をいう。
2	厚労省（本省）	厚生労働省（本省）をいう。 （中労委、厚生局、労働局、労働基準監督署及び公共職業安定所、施設等機関を含まない。）
3	中労委	外局である中央労働委員会をいう。
4	地方支分部局	地方厚生（支）局、都道府県労働局をいう。
5	厚生局	地方厚生（支）局　をいう。（8 カ所）
6	労働局	都道府県労働局をいう。（47 カ所）
7	労働基準監督署	各地域に設置される労働基準監督署をいう。（325 カ所）
8	公共職業安定所	各地域に設置される公共職業安定所（ハローワーク）をいう。（544 カ所）
9	施設等機関	国立医薬品食品衛生研究所、国立保健医療科学院、国立社会保障・人口問題研究所、国立感染症研究所、国立児童自立支援施設（2 カ所）、国立障害者リハビリテーションセンター（6 カ所）、検疫所（13 カ所）、国立ハンセン病療養所（13 カ所）をいう。
10	厚労省ポリシー	厚生労働省情報セキュリティポリシーをいう。
11	関係規程等	「情報取扱手順書」、「例外措置手順書」、「人事異動の際に行うべき情報セキュリティ対策実施規程」、「厚生労働省支給以外の情報システムによる情報処理の手順書」、「要管理対策区域外でのPCの利用における情報処理の手順書」、「アプリケーション・コンテンツの提供時に省外の情報セキュリティ水準の低下を招く行為の防止に関する規程」、「情報セキュリティインシデント対処手順書」、「外部委託及び機器等の購入における情報セキュリティ対策実施手順書」、「情報セキュリティ対策実施手順書作成のガイドライン」及び「スマートフォン・タブレット端末等の使用手順」等をいう。
12	政府機関統一基準群	「政府機関の情報セキュリティ対策のための統一規範」、「政府機関等の情報セキュリティ対策の運用等に関する指針」、「政府機関の情報セキュリティ対策のための統一基準(平成 28 年度版)」及び「府省庁対策基準策定のためのガイドライン」をいう。
13	担当職員	厚生労働省政策統括官付サイバーセキュリティ担当参事官室の本業務に関する職員をいう。
14	自己点検計画	厚生労働省情報セキュリティポリシーに基づき、毎年度策定する情報セキュリティ対策の実施状況に係る自己点検計画をいう。
15	自己点検結果	厚生労働省に対し、情報セキュリティ対策実施体制の構築及び対策の実施状況について、当省のサイバーセキュリティ担当参事官室の担当職員が実施する自己点検の結果（回答票）。

（注）厚生局、労働局、労働基準監督署及び公共職業安定所は、平成 29 年 4 月時点の箇所数であり、増減があり得る。

1.5 契約期間

契約開始日から平成 31 年 3 月 29 日(金)までの期間とする。

1.6 調達担当課室・連絡先

本仕様書に関する問合せ先は以下のとおりとする。

東京都千代田区霞が関1－2－2

厚生労働省政策統括官付サイバーセキュリティ担当参事官室

サイバーセキュリティ監査係

03(5253)1111(内 2236)

2. 調達案件、調達方式及び実施時期に関する事項

2.1 調達案件及び調達方式

2.1.1 調達案件

平成 30 年度情報セキュリティ監査等一式

2.1.2 調達の方式

一般競争入札(総合評価落札方式)

2.2 調達案件間の入札制限

監査の独立性及び客観性の確保の観点から、本業務は，本調達仕様書の「7.2 入札制限」にあげる業務とは相互に入札制限の対象とする。

3. 作業の実施内容に関する事項

3.1 作業の内容

受注者は、情報セキュリティ対策全般の改善・実効性の向上を目指す上で、再発防止策等に基づき、監査について、本仕様書や閲覧資料、政府が公表した方針等を参照し、各実施対象組織への職員負担を考慮した効率的かつ円滑な実施手法について、受注者の技術的な見地からの提案を踏まえ協議を行いつつ、実施又は実施支援を通じた一連の役務を行う。

なお、本仕様書に示す業務内容はあくまで現時点で想定されるものであるが、セキュリティ対策にかかる技術は日進月歩であり、新たな政府方針等の動向如何により早急な対応が求められることに留意する必要がある。

3.1.1 作業の概要

ア. 監査に係る実施計画書の策定

イ. 監査の実施

3.1.2 対象とする組織

対象とする組織を下表に示す。なお、本業務の実施に当たっては、「3.2.1 情報セキュリティ対策の強化等に係る実施計画書の策定」により定める計画書上において、実施対象となる組織及び情報システムを選定することとする。

項番	組織	対象組織
1	地方支分部局	東北厚生局、九州厚生局 茨城、埼玉、千葉、東京、神奈川を除く 42 労働局 （労働基準監督署、公共職業安定所を含む）
2	施設等機関	国立きぬ川学院、函館視力障害センター、神戸視力障害センター、福岡視力障害センター、別府重度障害者センター、秩父学園

3.2 具体的な作業の内容

平成 29 年度においては、厚労省（本省）、中労委、地方支分部局、施設等機関及び所管法人等を対象として、平成 28 年度監査の結果及びリスク評価の結果を踏まえ、PDCA サイクルを通じて情報セキュリティ対策全般の改善・実効性の向上を図るため、フォローアップを中心とした監査を行い、独立かつ専門的な立場から点検・評価し、問題点の確認、改善方法等について助言、報告を行う取組を実施した。平成 29 年度の実施内容については、別途閲覧に供する。

平成 30 年度に実施する本業務では、地方支分部局、施設等機関に対し、平成 28 年度、平成 29 年度監査において指摘が多かった事項を中心に、厚労省ポリシーに沿った情報セキュリティ対策が実施されているかについて点検・評価を行うことを予定している。

3.2.1 監査に係る実施計画書の策定

本業務の実施に当たって、担当職員の指示に基づき、監査を実施するため、以下の事項を含む実施計画書を作成し、当室との協議を経て、契約後 30 日以内に決定すること。

ア. 目的
イ. 対象及び範囲
ウ. 実施方法
エ. 実施スケジュール
オ. 実施及び実施支援における役割分担
カ. 実施及び実施支援体制
キ. 進捗管理及び報告方法
ク. その他、監査の実施に必要な事項

なお、実施計画書の作成に当たっては、以下に留意すること。

ア. 当室の体制を勘案した実施内容、実施体制であること。当室の体制は、別途閲覧に供する。
イ. 本業務の契約期間内に実施可能なスケジュールとすること。

3.2.2 監査の実施

受注者は、監査について実施及び実施支援を行う。監査の実施及び実施支援の役割分担については、当室の体制を勘案した分担であること。当室の体制は、別途閲覧に供する。

ア. 監査対象組織

監査対象組織は、地方支分部局、施設等機関とする。

なお、監査対象となる組織を対象の全てとしない場合は、選定基準など判断根拠を明確にした資料を提示し、担当職員と協議の上決定すること。

イ. 監査の実施方法

監査は、平成 28 年度、平成 29 年度監査において指摘が多かった事項及びインシデント事例の多い事項を中心に、厚労省ポリシーに沿った情報セキュリティ対策が講じられているかについて、ヒアリング及び実地調査（往査）または書面により実施する。

ヒアリング及び実地調査（往査）は、当室の実施体制も踏まえ、20 カ所程度を想定している。実施方法の決定においては、自己点検結果、前年度のリスク評価結果、監査結果、インシデント事例、内閣サイバーセキュリティセンター（NISC）のマネジメント監査結果等を分析し、監査事項の整理をした上で、判断根拠を明確にした資料を提示し、担当職員と協議の上決定すること。

なお、スケジュール及び当室の実施体制を考慮し、より効率的な実施方法とするときは、担当職員と協議の上決定すること。

事前調査資料は、別途当室が実施する平成 30 年度の監査に当たっての事前調査資料とするが、資料に不足がある場合には「オ. 監査実施通知書の作成」の中で提示し、当室の担当職員を通じて、監査対象組織へ依頼する。

平成 30 年度の監査に当たっての事前調査資料は、以下を予定している。

・情報セキュリティ管理体制
・情報セキュリティインシデント事案の発生及び対処状況
・外部電磁的記録媒体の利用の有無及び管理状況
・外部サービスの利用状況
・外部委託におけるセキュリティ対策の実施状況　等

別途当室が実施する平成 30 年度自己点検結果、NISCのマネジメント監査結果、インシデント事例については、契約締結後、受注者が担当職員に守秘義務の誓約書(別紙1-2)を提出した際に開示する。

平成 30 年度の監査に当たっての事前調査については、別途閲覧に供する。

ウ. 監査項目の選定と監査チェックリストの作成

受注者は、平成 28 年度、平成 29 年度監査における監査事項、指摘事項、インシデント事例及び NISC のマネジメント監査結果等を分析した上で、よく検出される事項を中心に監査項目の選定を行い、監査チェックリストの作成を行うこと。 監査項目は、分析結果等を示した上で、担当職員と調整の上決定すること。監査項目のうち、特に多く検出される事項については、厚労省ポリシーに沿った対策が講じられていない原因についても確認できるようなチェック内容とすること。

平成 28 年度、平成 29 年度監査の実施内容及び監査結果については別途閲覧に供する。

エ. ヒアリング及び実地調査（往査）の日程調整

ヒアリング及び実地調査（往査）は、当室の担当職員を通じて日程調整を行うこととし、受注者が往査を実施する場合には、担当職員が同行する。

オ. 監査実施通知書の作成

ヒアリング及び実地調査（往査）または書面による監査の実施に際して、各組織に対し、当室より監査実施通知書の送付を行う必要があるため、監査の実施内容、スケジュール、提出依頼資料、事前準備等の事項について、担当職員へ書面で提出すること。

カ. 監査の実施

監査は、「ウ. 監査項目の選定と監査チェックリストの作成」において作成した「監査チェックリスト」に沿って実施し、ヒアリング及び実地調査（往査）においては、監査終了時に簡易講評を行い、監査終了後に監査で検出された事項についての事実確認を監査対象組織あて書面にて行うこと。

キ. 例外措置の申請及び許可状況の評価

例外措置の適用審査の記録等から、地方支分部局、施設等機関における、例外措置の申請及び許可の状況を把握し、例外措置の審査手続に従った管理がなされているか調査・分析すること。

ク. 監査調書の作成

監査の実施に当たっては監査調書を作成すること。

各組織の監査実施の結果及び監査手続きの中で入手した資料等を監査証拠及び関連資料として綴り込み、それらを根拠づけながら、監査の結論に至った経緯がわかるよう監査調書を作成すること。

監査調書は、監査実施単位に作成し、実施単位ごとの監査結果報告書の一部（別添資料）として、監査結果報告書の納入期限にあわせて報告すること。

なお、監査結果報告書の納入期限前においても、担当職員から提出の指示があった場合は、協議し対処すること。

作成に当たっては、監査意見の根拠とするのみではなく、次年度以降の監査を合理的に実施することを前提にしつつ作成すること。

監査調書の作成に当たっては、当室の体制を勘案した作業分担であること。当室の体制は、別途閲覧に供する。

ケ. 監査結果報告書の作成

監査結果報告書は、監査実施単位に作成し、監査結果、問題点、指摘事項及びその根拠、発見された課題に応じて想定されるリスク、改善提案及びそれを実施した際の効果を記載し、当該業務を実施していく過程で作成した文書、資料、提案内容等の構成により作成すること。

監査結果報告書は、監査対象組織の幹部を含む職員に対し、厚労省ポリシー、関係規

程及び情報セキュリティの脅威に関する理解を深めることができるよう工夫すること。

監査結果報告書の作成に当たっては、当室の体制を勘案した作業分担であること。当室の体制は、別途閲覧に供する。

3.3 納入成果物の範囲、納入期限等

受注者は、「3.3.1 納入成果物」に示す成果物を作成し、担当職員の了承を得た上で納入期限内に納入すること。

3.3.1 納入成果物

成果物	部数	納入期限
実施計画書	8部	契約後 30 日以内
情報セキュリティ監査結果報告書	3部	提案を勘案しつつ決定する
実施報告書	8部	平成 31 年 3 月 29 日(金)
実施報告書(概要版)	8部	平成 31 年 3 月 29 日(金)
会議等で使用する資料	必要数	当該会議の開催日前日
議事録	2部	会議等開催日含む 3 開庁日以内
月次活動報告書	2部	原則、当該月の翌月最初の開庁日 3 月分は平成 31年 3 月 29 日(金)
引継書	8部	平成 31 年 3 月 29 日(金)

(注)

・実施計画書、実施報告書、実施報告書(概要版)

本業務における全体坂野報告書を作成すること。

平成 29 年度に実施した、監査にかかる実施計画書、実施報告書については、別途閲覧に供する。

・情報セキュリティ監査結果報告書

監査を行う組織単位で作成する報告書。平成 29 年度に実施した監査にかかる情報セキュリティ監査結果報告書の例については、別途閲覧に供する。

・会議等で使用する資料

会議等で受注者が説明するための資料。

・議事録

受注業者が参加した会議等の議事録

・月次報告書

月単位に当該期間内において本調達に基づき実施した役務内容をまとめた報告書。

・引継書

次年度の情報セキュリティ対策関連事業に活用するため課題等をまとめた引継書。

3.3.2 納入方法

ア. 受注者は、成果物は紙媒体及び電磁的記録媒体(CD-R 又は DVD-R)により作成し、特に示すものを除き、紙媒体は2部、電磁的記録媒体は1部を納品すること。また、指定のドキュメントを表紙、目次及びページを付与した分かり易い構成で作成し、インデックスを添付の上、紙媒

体により指定の部数を納入すること。

イ. 紙媒体のサイズは、日本工業規格A列4番を原則とすること。図表については、必要に応じてA列3番を使用することができる。

ウ. 成果物は、すべて日本語で作成すること。ただし日本国内においても、英字で記載されることが一般的な文言については、そのまま記載しても構わないものとする。

エ. 用字・用語・記述符号の表記については、「公用文作成の要領（昭和 27 年 4 月 4 日内閣閣甲第 16 号内閣官房長官依命通知）」を参考にすること。情報処理に関する用語の表記については、日本工業規格（JIS）の規定を参考にすること。

オ. 電磁的記録媒体による納品について Microsoft Office2010（MicrosoftWord2010、同 Excel2010、同 PowerPoint2010）で読み込み可能な形式、または PDF 形式（Adobe Reader XI で読み込み可能）で作成し、納品すること。ただし、当省から他の形式による提出を求める場合は、協議の上、これに応じること。なお、受注者側で他の形式を用いて提出したいファイルがある場合は、協議に応じるものとする。当省において改変が可能となるよう、図表等の元データも併せて納品すること。

カ. 成果物の作成に当たって、特別なツールを使用する場合は、当省の承認を得ること。

キ. 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

ク. 電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。

ケ. 受注者は、成果物について、当省と十分協議を行い、当省の指示に従いながら作成すること。

3.3.3 納入場所

納入成果物の納入場所は以下のとおり。

東京都千代田区霞が関１－２－２

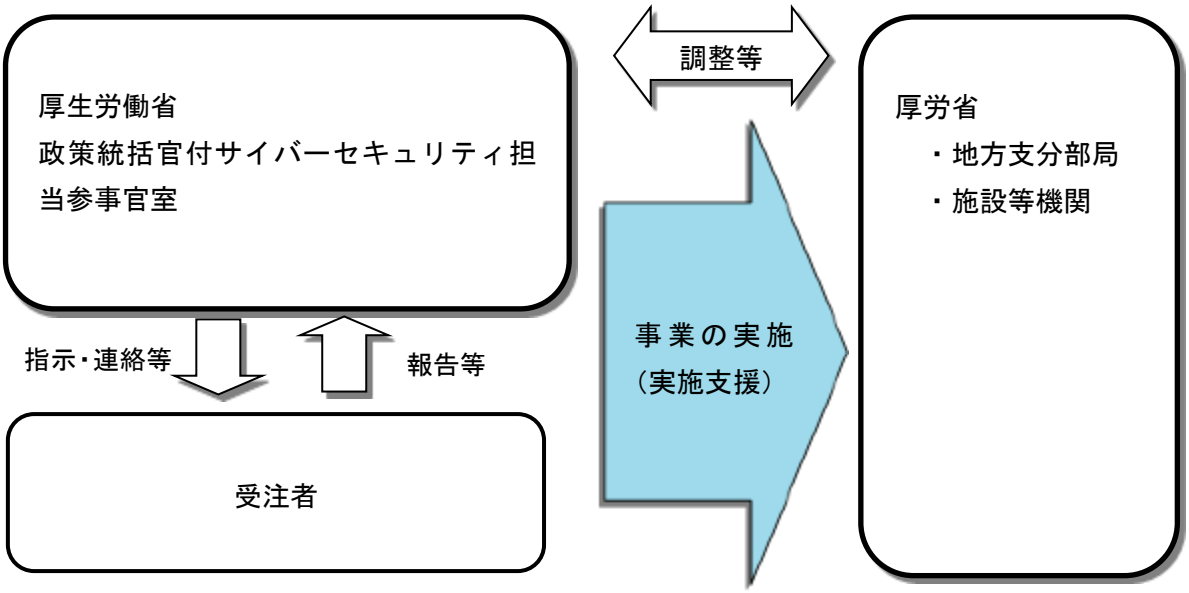
厚生労働省政策統括官付サイバーセキュリティ担当参事官室

4. 作業の実施体制及び方法に関する事項

4.1 作業実施体制

本業務の遂行に当たり、次の図の作業体制を想定している。

なお、受注者は、本仕様書に示す業務を履行できる専任の体制を設けるとともに、受注者側の業務体制図について、書面を提出し、当省の承認を得ること。



また、作業体制の構築、作業遂行に当たり、以下の要件を満たすこと。

ア. 実施業務の適切な単位でチームを編成し、それぞれ責任者を置くこと。

イ. 各業務の進捗状況を常に把握し、担当職員からの進捗の質問に対しては、すぐに対応できるようにすること。

ウ. 受注者は、報告書等の作成に関する詳細について、担当職員との密接な協議に基づき行うこととし、質疑あるいは協議の結果は、その都度、文書あるいは電子メールにて提出すること。

4.2 作業要員に求める資格等の要件

(1)公的資格等

当事業の実施に当たって、原則として契約期間を通して変更することなく本件業務の管理を行う者を統括責任者、チーム責任者として配置すること。

統括責任者は業務を総合的に把握し、円滑に実施するため、各チームの責任者に指揮命令・監督を行う立場にある者とする。

チーム責任者は業務の実施単位で配置し、統括責任者の指示の下、業務関係者に指揮命令・監督を行う立場にある者とする。

統括責任者及びチーム責任者は、政府統一基準群について理解し、情報セキュリティ監査業務の経験を有している者とし、次のいずれかの資格を有する者であること。

ア. 情報処理推進機構の実施する情報処理技術者試験のプロジェクトマネージャ試験の合格者

イ. プロジェクト・マネジメント協会が認定する PMP（Project Management Professional）の資格保有者

ウ. 情報処理推進機構の実施する情報処理技術者試験の情報セキュリティスペシャリスト試験の合格者

エ. 情報処理安全確保支援士の登録者

オ. システム監査技術者（SA：Systems Auditor）

カ. 公認情報システム監査人（CISA：Certified Information Systems Auditor）

キ. 公認システム監査人（CSA：Certified Systems Auditor）

また、「9.3 業務実績」に該当する業務に 1 つ以上参画したものであること。各チームの担当者は、担当する役割に応じた能力を保持することが、資格や経歴等において明らかであること。

(2)会議等に使用する言語

日本語

(3)後方支援体制

統括責任者、チーム責任者及び担当者を組織として支援する体制を整備すること。

5. 作業の実施に当たっての遵守事項

5.1 機密保持、資料の取扱い

本仕様書に基づき契約が成立した場合の業務実施中はもとより、契約終了後も当省が提供した業務上の情報で省外秘を要するものについては、第三者（第三者とは、一般的に言う第三者はもとより、受注者組織内で作業を行う場合の、本業務に係わる体制以外の受注者側（受注企業）社員等も含む。以下同様。）に開示、又は漏えいしないこと。また、そのために「受注者が機密保持を遵守するために講ずるべき措置」(別紙 1-1)にある措置を講ずること。なお、当省は措置状況について、随時、実地確認できるものとする。

受注者は、契約時に当省へ「機密保持に関する誓約書」(別紙 1-2)を提出すること。

当省が提供する資料は、原則として貸出しによるものとし、契約期間内に返却すること。また、当該資料の複写及び第三者への提供はしないこと。

当省が提供した情報を第三者に開示することが必要である場合は、事前に協議の上、承認を得ること。

5.2 遵守する法令等

ア. 「政府機関の情報セキュリティ対策のための統一基準」の最新版及び、「厚生労働省情報セキュリティポリシー」及び「厚生労働省情報セキュリティポリシー」に基づく実施手順書（以下「ポリシー等」という。）の最新版を遵守すること。なお、ポリシー等は非公表であるが、「政府機関の情報セキュリティ対策のための統一基準」に準拠しているので、必要に応じ参照すること。ポリシー等の開示については、契約締結後、受注者が担当課室に守秘義務の誓約書を提出した際に開示する。

イ. 受注者は、受注業務の実施において、「民法（明治 29 年法律第 89 号）」、「刑法（明治 40 年法律第 45 号）」、「著作権法（昭和 45 年法律第 48 号）」、「不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）」、「行政機関の保有する個人情報の保護に関する法律（平成 15 年

法律第 58 号）」等の関連する法令等を遵守すること。

5.3 情報セキュリティ管理

受注者は、以下を含む情報セキュリティ対策を実施すること。また、その実施内容及び管理体制についてまとめた情報セキュリティ管理計画書を作成し、「3.2.1 情報セキュリティ監査に係る実施計画書の策定」に示す実施計画書に含め、提出すること。

ア. 当省から提供する情報の目的外利用を禁止すること。

イ. 受注者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。

ウ. 情報セキュリティインシデントへの対処方法が確立されていること。

エ. 情報セキュリティ対策その他の契約の履行状況を定期的に確認し、当省へ報告すること。

オ. 本業務の実施場所及び環境（作業場所、情報機器、ソフトウェア、通信ネットワーク等の使用・管理方法）について、情報セキュリティ対策を講じること。

カ. 情報セキュリティ対策の履行が不十分である場合、速やかに改善策を提出し、当省の承認を受けた上で実施すること。

キ. 当省が求めた場合に、速やかに監査を受け入れること。

ク. 本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。

ケ. 当省から要保護情報を受領する場合は、情報セキュリティに配慮した受領方法にて行うこと。なお、当省から受領した要保護情報が不要になった場合は、これを確実に返却、又は抹消し、書面にて報告すること。

コ. 本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに当省に報告すること。

6. 納入成果物の取扱いに関する事項

6.1 知的財産権の帰属

ア. 調達に係り作成・変更・更新される書面（電子媒体を含む。）、その他類似の派生物（提案等の構想等も含む。）の著作権は、受注者より予め提案書にて権利譲渡不可能と示されたもの以外、全て当省に帰属するものとすること。

イ. 受注者の著作又は一般に公開されている著作を引用する場合には、出典を明示するとともに、受注者の責任において著作者等の了解を得るものとし、当省宛に提出する際は、その旨、合わせて報告するものとする。（当省は、必要に応じ随時書面による報告提出を求めることができる。）

なお、受注者は、当省に対し、一切の著作者人格権を行使しないこととし、また、第三者をして行使させないこと。

ウ. 調達に係り発生した権利については、今後、二次的著作物が作成された場合等であっても、受注者は原著作物の著作権者としての権利を行使しないものとすること。

エ. 調達に係り作成・変更・修正されるドキュメント等に第三者が権利を有する著作物（以下、「既存著作物等」という。）が含まれる場合、受注者は当該既存著作物等の使用に必要な費用負

担や使用許諾契約等に係る一切の手続を行うこと。この場合、受注者は、事前に当該既存著作物の内容について当省の承認を得ることとし、当省は、既存著作物の内容について当該許諾条件の範囲で使用するものとする。

オ. 調達に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら当省の責めに帰す場合を除き、受注者の責任・負担において一切を処理すること。この場合、当省は係る紛争の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講ずる。

6.2 損害賠償

受注者は、受注者の責めに帰すべき事由により、当省及び第三者に損害を与えたときは、受注者はその損害を賠償しなければならない。

6.3 瑕疵担保責任

受注者は、本調達について検収を行った日を起算日として 1 年間、成果物に対する瑕疵担保責任を負うものとする。その期間内において瑕疵があることが判明した場合には、その瑕疵が当省の指示によって生じた場合を除き（ただし、受注者がその指示が不適当であることを知りながら、または過失により知らずに告げなかったときはこの限りではない。）、受注者の責任及び負担において速やかに修正等を行い、指定された日時までに当省の承認を得た上で再度納品するものとする。なお、修正方法等については事前に当省の承認を得てから着手するとともに、修正結果等についても当省の承認を受けること。

6.4 検収

本仕様書の定めに則って、納入成果物を提出すること。その際、当省の指示により、別途品質保証が確認できる資料を作成し、納入成果物とあわせて提出すること。当省が指定する場所において納入成果物の確認をもって検収合格とする。

検査の結果、納入成果物の全部又は一部に不合格品を生じた場合には、担当職員からの改善指示に従い、受注者は直ちに引き取り、必要な修正を行った後、納入期限までに修正が反映されたすべての納入成果物を納入すること。

ただし、検査後、瑕疵等が認められた場合には、受注者の責任及び負担において対処するものとする。

本仕様書に定める納入成果物以外にも、必要に応じて納入成果物の提出を求める場合があるので、作成資料は常に管理し、最新状態に保っておくこと。

7. 受注者の条件

7.1 入札参加資格

受注者は、以下の条件を満たす必要がある。なお、本業務の作業を行うに当たっては、業務開始までに、受注者の責任及び負担において、事前準備を行うこと。

7.1.1 非該当要件

受注者は、以下に記載するいずれかの規定に該当してはならない。

ア. 予算決算及び会計令第 70 条の規定(未成年者、被保佐人又は被補助人であっても、契

約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。）

イ. 予算決算及び会計令第 71 条の規定

ウ. 当省から業務等に関する指名停止期間中

7.1.2 競争参加資格

平成 28・29・30 年度当省競争参加資格(全省庁統一資格)において、当省大臣官房会計課長から「役務の提供等」で「A」、「B」又は「C」等級に格付けされ、関東・甲信越地域の競争参加資格を有する者であること。

7.1.3 公的な資格や認証等の取得

本調達を担当する組織（会社全体または所属部門）において、「プライバシーマーク付与認定」、「ISO/IEC27001 認証（国際標準規格）」または、「JIS Q 27001 認証（日本工業標準規格）」のうち、いずれかを取得していること。

7.1.4 受注者組織内における教育制度の完備

以下の内容を含む教育を実施する受注者組織内における社内教育制度を有し、要員に対し教育を実施していること。

ア. プライバシーや個人情報保護に関する教育

イ. 守秘義務に関する教育

ウ. 情報セキュリティに関する教育

7.2 入札制限

情報システムの調達の公平性を確保するため、参加者は、以下に挙げる事業者並びにこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者でないこと。

・平成 29 年度及び 30 年度の当省全体管理組織（PMO）の支援業務の受注事業者。

なお、本業務の受注者であることをもって、当省の情報システムの設計・開発の作業に関する調達案件への入札を制限するものではない。

7.3 その他

入札に参加しようとする者は、支出負担行為担当官が別に指定する暴力団等に該当しない旨の誓約書を提出すること。入札に参加した者が、誓約書を提出せず、又は虚偽の誓約をし、若しくは誓約書に反することとなったときは、当該者の入札を無効とする。

その他予算決算及び会計令第 73 条の規定に基づき、支出負担行為担当官が定める資格を有する者であること。

この入札の入札書提出期限の直近１年間において、当省が所管する法令に違反したことにより送検され、行政処分を受け、又は行政指導（行政機関から公表されたものに限る。）を受けた者にあっては、本件業務の公正な実施又は本件業務に対する国民の信頼の確保に支障を及ぼすおそ

れがないこと。これに該当すると思われる事実がある者は、あらかじめ入札書の提出場所、契約条項を示す場所及び問い合わせ先に照会すること。

8. 再委託に関する事項

8.1 再委託の制限及び再委託を認める場合の条件

受注者は、受注業務の全部又は受注業務における総合的な企画及び判断並びに業務遂行管理部分を第三者に再委託することはできない。

受注者は、知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関して本調達仕様書が定める受注者の責務を再委託先業者も負うよう、必要な処置を実施し、当省に報告し、承認を受けること。

受注業務の一部を再委託する場合は、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額（契約金額に占める再委託契約金額の割合は、原則2分の1未満とする。）について記載した「再委託に係る承認申請書」を当省に提出し、承認を受けること。

なお、第三者に再委託する場合は、その最終的な責任を受注者が負うこと。

8.2 承認手続

受注者は、受注業務の一部を再委託する場合は、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額（契約金額に占める再委託契約金額の割合は、原則2分の1未満とする。）について記載した「再委託に係る承認申請書」を当省に提出し、承認を受けること。また、再委託の相手方から更に第三者に委託を行うことは禁止とする。なお、受注者が再委託する事業者は、「7.2 入札制限」に挙げる事業者及びこの関連会社でないこと。

当初申請内容に変更が生じた場合は、「再委託に係る変更承認申請書」を当省に提出すること。

9. その他特記事項

9.1 前提条件及び制約条件

ア. 本調達仕様書は、受注者に業務遂行を求める最低限の基準を示したものである。したがって、受注業務の目標を達成するため、本調達仕様書に記載していない事項であっても、本調達に必要と認められる事項は、当省と協議の上、これを行うこと。

イ. 本業務受注後に本調達仕様書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって当省に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、納期の影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。

ウ. 本調達の作業を行う際には、当省に報告する全ての内容について、信憑性が確認できることに努めること。

エ. 本業務の遂行に当たっては、省内規程等に従うこと。

オ. 業務を遂行する者は外部専門家としての「独立性・中立性」を保つことが要求されるとともに、省内外において、当省としての活動を行う場合があることから、担当職員と同様の立場での業務遂行に努めなければならない。

カ. 本業務の勤務及び倫理に関する取扱いについては、国家公務員法及び国家公務員倫理法に

準じた取扱いとする。

9.2 環境への配慮

納入成果物について、環境保護の観点から可能な限り、「国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）」（グリーン購入法）に基づいた製品を導入すること。

9.3 業務実績

本調達を担当する組織（会社全体または所属部門）において、以下の業務実績を有することが望ましい。

ア. 多数の情報システムを保有する組織に対して、情報セキュリティ監査業務を履行した実績。

イ. 中央省庁又は独立行政法人に対して、情報セキュリティ監査業務を履行した実績。

ウ. 多種多様な業務を所管する組織に対するBPR（Business Process Re-engineering）業務を履行した実績。

9.4 その他

ア. 当省全体管理組織 (PMO)が担当職員に対して指導、助言等を行った場合には、受注者もその方針に従うこと。

イ. 受注者は、電子行政推進に関する基本方針等の各種方針（今後決定されるものを含む。）に従うこと。

ウ. 納入成果物について、担当職員から別途様式が提示された場合は、その指示に従うこと。

エ. 当省に報告するものは、全て信憑性が確認できるよう努めること。

オ. 本業務を実施する際、システムの運用及び当省職員の通常業務に支障や悪影響を及ぼさないこと。支障や悪影響を及ぼすことが予想される場合は、事前に担当職員に危険度等を説明の上、了承を得ること。なお、事前に当省に危険度等を説明しない事項において発生した障害等については、受注者の責任において復旧等を実施すること。また、情報セキュリティが侵害され又はそのおそれがある場合には、速やかに当省に報告すること。

10. 附属文書

10.1 事業者が閲覧できる資料一覧表

入札参加予定者は、以下の資料の閲覧を希望する場合は、守秘義務に関する誓約書（別紙 1-2）を提出の上、当省が定める期間、場所、方法において閲覧を許可する。

ア. サイバーセキュリティ担当参事官室の体制

イ. 厚労省ポリシー及び関係規程

ウ. 平成 29 年度情報資産棚卸し及びリスク評価実施ガイドライン

エ. 平成 29 年度情報資産棚卸し及びリスク評価の実施結果

オ. 平成 28 年度情報セキュリティ監査実施計画書

カ. 平成 28 年度情報セキュリティ監査実施報告書

キ. 平成 29 年度情報セキュリティ対策にかかる自己点検計画の策定について

ク. 平成 29 年度情報セキュリティ対策にかかる自己点検の実施ついて

ケ. 平成 29 年度情報セキュリティ対策にかかる自己点検の実施結果

コ. 平成 29 年度情報セキュリティ監査計画書の策定について

サ. 平成 29 年度情報セキュリティ対策強化等一式にかかる実施計画書
シ. 平成 29 年度情報セキュリティ対策等強化一式にかかる実施報告書
ス. 平成 29 年度情報セキュリティ監査結果報告書
セ. 平成 29 年度情報セキュリティ監査の実施対象組織、日程
ソ. 平成 29 年度情報セキュリティ監査報告書の送付及び改善指示(依頼)
タ. 平成 30 年度情報セキュリティ対策にかかる自己点検計画の策定について
チ. 平成 30 年度情報セキュリティ対策にかかる自己点検の実施ついて
ツ. 平成 30 年度情報セキュリティ監査計画書の策定について
テ. 平成 30 年度情報セキュリティ対策に関する監査の事前調査について
ト. 当室以外の組織が実施する情報セキュリティ関係施策の実施状況
ナ. 情報セキュリティ対策に関連する各種施策にかかる各種指示等

なお、これらの資料については、契約締結後、受注者が担当職員に守秘義務の誓約書(別紙 1-2)を提出した際に開示する。

10.2 閲覧要領

入札参加予定者が、資料の閲覧を希望する場合は、守秘義務に関する誓約書(別紙 1-2)を提出の上、当省が定める期間、場所、方法において閲覧を許可する。

10.3 その他事業者の提案に資する資料

本件業務は以下の資料を参考として実施すること。

ア.「情報セキュリティ強化等に向けた組織・業務改革　―日本年金機構への不正アクセスによる情報流出事案を踏まえて―」
(http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150918-02.pdf)

イ.「サイバーセキュリティ戦略本部長の勧告に対する報告書について(報告書)」
(http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_160428-01.pdf)

ウ.「政府情報システムの整備及び管理に関する標準ガイドライン」
(http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html)

エ.「政府機関の情報セキュリティ対策のための統一基準群(平成 28 年度版)」
(http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf)

オ.「高度サイバー攻撃対処のためのリスク評価等のガイドライン」
(http://www.nisc.go.jp/active/general/risk.html)

（別紙 1-1）

受注者が機密保持を遵守するために講ずるべき措置

１．情報セキュリティを確保するための体制の整備

（1） 受注者は、受注者組織全体のセキュリティを確保するとともに、当省から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。

（2） 本体制には、経営者が関与し、経営者の責任の明確化を図ること。

（3） 本体制における要員には、「情報処理の促進に関する法律」（昭和 45 年法律第 90 号）に基づき行われる情報処理技術者試験のうち、情報セキュリティに関する資格を有する者若しくは同等の知識及び技能を有することを自ら証明出来る者を含むこととし、当該者を以下で記載する管理責任者又は管理担当者とし、継続して新たな知識の補充を行うこと。

（4） 当省が提供した業務上の情報（以下「情報」という。）を適正に管理するために、管理責任者をおくこと。

（5） 管理責任者は、その事務の一部を担当させるため、管理担当者を指定すること。

（6） 管理責任者及び管理担当者の役職及び氏名をあらかじめ当省に提出すること。また、その内容に変更が生じた場合には、その都度報告すること。

（7） 管理責任者は、受注者側組織内で作業を行う場合の情報の取扱いに関して、情報セキュリティが侵害され又はそのおそれがある場合等の非常時における対策を定めると共に、その内容を要員に徹底すること。

２．取り扱う国の安全に関する重要な情報の秘密保持等

（1） 本調達に係る業務の実施のために当省から提供する国の安全に関する重要な情報その他当該業務の実施において知り得た国の安全に関する重要な情報については、情報のライフサイクルの観点から管理方法を定め、その秘密を保持し、また当該業務の目的以外に利用しないこと。

※「国の安全」とは、国家の構成要素である国土、国民及び統治体制が害されることなく平和で平穏な状態に保たれていること、すなわち、国としての基本的な秩序が平穏に維持されている状態をいう。

３．情報の管理

（1） 当該業務の日々の活動場所は、当省の指定する場所（当省の庁舎内等）であることに鑑み、情報は原則として省内で利用すること。ただし、庁舎間の移動、他府省との会議等における持ち出しはその限りではない。

（2） 個人情報が記載された情報に関しては、原則として省外に持ち出さないこと。

（3） 受注者側組織内で作業を行う場合には、作業を行う施設は、IC カード等電磁的管理による入退館管理がなされていること。

（4） 同様に、上記作業施設内の作業実施場所は、IC カード等電磁的管理による入退室管理がなされていること。

（5） 電磁的に情報を保管する場合には、当該業務に係わる体制以外の受注者側がアクセスできない

ようアクセス制限を行うこと。

4. 情報セキュリティが侵害された場合の対処

(1) 本調達に係る業務の遂行において、定期的に情報セキュリティ対策の履行状況を報告するとともに情報セキュリティが侵害され又はそのおそれがある場合には、直ちに当省に報告すること。これに該当する場合には、以下の事象を含む。

- 受注者に提供し、又は受注者によるアクセスを認める当省の情報の外部への漏えい及び目的外利用
- 受注者による当省のその他の情報へのアクセス

(2) 被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、当省の求めに応じて成果物と共に当省に引き渡すこと。

5. 情報セキュリティ監査の実施

(1) 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、当省が情報セキュリティ監査の実施を必要と判断した場合は、当省がその実施内容(監査内容、対象範囲、実施者等)を定めて、情報セキュリティ監査を行う(当省が選定した事業者による監査を含む。)。

(2) 受注者は、あらかじめ情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「情報セキュリティ監査対応計画書」等により提示すること。

(3) 受注者は自ら実施した外部監査についても当省へ報告すること。

(4) 情報セキュリティ監査の実施については、これらに記載した内容を上回る措置を講ずることを妨げるものではない。

6. 報告の義務

(1) 当省から求めがあった場合には、以上の状況について書面等での報告を行うこと。

（別紙 1-2）

平成　　年　　月　　日

機密保持に関する誓約書

厚生労働省大臣官房参事官(サイバーセキュリティ・情報システム管理担当)　殿

所在地

会社名

代表者

契約開始日から平成 31 年 3 月 29 日までの「平成 30 年度情報セキュリティ監査等一式」の契約に伴い、本件業務に関与する自己の従業員に「受注者が機密保持を遵守するために講ずるべき措置」（別紙 1-1）を遵守させることを誓約いたします。

平成　　年　月　日

支出負担行為担当官

厚生労働省大臣官房会計課長　殿

申込者　住所

氏名　　印

（連絡先）