別添１

企業保有情報の新しい提出方法に係るシステム保守等

仕様書

令和６年１月

デジタル庁 国民向けサービスグループ

目　次

【附属資料】

別紙　個人情報取扱特記事項

1 調達案件の概要に関する事項

1.1 調達件名

企業保有情報の新しい提出方法に係るシステム保守等

1.2 調達の背景、目的及び期待する効果

「企業が行う従業員の社会保険・税手続のオンライン・ワンストップ化等の推進に係る課題の最終整理」（平成 31 年４月 18 日各府省情報化統括責任者（CIO）連絡会議決定）においては、企業が行政手続のために行っている負担を軽減するとともに、社会全体としての業務効率化を目指し、データの重複管理を削減し、共同利用の促進を図るため、企業保有情報の新しい提出方法に係るシステム構築計画の検討を行うこととされている。

また、デジタル・ガバメント実行計画（令和元年 12 月 20 日閣議決定）においては、社会保険・税手続の新たな方法として、金融機関に係る法定調書（注１）の提出（事業者提出の全ての法定調書について検討）に関して、クラウドサービス（注２）等を活用した企業保有情報の新しい提出方法に係る情報システムの利用を 2021 年度（令和３年度）以降開始し、事業者の事務作業の負担を軽減するほか、国民・事業者の負担軽減が見込まれるその他の手続についても、2022 年度（令和４年度）以降の対象拡大に向けて検討し、2020 年度（令和２年度）中に結論を得ることとされており、加えて、年金関係をはじめ、行政機関等から事業者への処分通知等について、デジタル化の課題や方策等を検討し、2021 年度（令和３年度）以降の順次対応を目指すとともに、活用拡大を検討することとされている。また、「デジタル社会の実現に向けた重点計画（令和４年６月９日閣議決定）」において、クラウド提出済みのデータを確定申告等において利活用することを検討し、令和５年（2023 年）１月以降の実現を目指すとともに、国民・事業者の負担軽減が見込まれるその他の手続についても、引き続き対象拡大に向けて検討を進めることとされている。

クラウドサービス等を活用した企業保有情報の新しい提出方法とは、①企業が、新しい提出方法による提出を行う旨を行政機関等に事前に申請し、承認された後、②企業が、その利用するクラウドサービスに提出情報を登録・記録すると、当該クラウドサービスは当該提出情報へのアクセス権を行政機関等に付与するとともに、当該提出情報の提出に係る通知（以下「提出通知」という。）を行政機関等に送付し、③その後、行政機関等が当該クラウドサービスに登録された提出情報を参照し、④一定期間の経過後（数年単位）に、行政機関等からクラウドサービスに対してアクセス権を解除する旨の通知を送付し、クラウドサービスが当該情報への行政機関等からのアクセス権を解除する仕組み（以下「参照型」という。）を想定している。

また、この新しい提出方法において構築する仕組みについては、上記の参照型を更に発展させ、①提出情報に記載されている者が、当該提出情報を自身の手続において参照すること（例：納税者が自分の情報が記載された法定調書に含まれる情報を参照）を想定している。

デジタル庁では、この企業保有情報の新しい提出方法の仕組みの構築に向けて、これまで、法定調書の提出など企業保有情報の新しい提出方法に係るユースケースの調査、新しい提出方法に係るシステムの構築に向けた関係行政機関等及びクラウドサービス事業者等への導入支援を行ってきた。

本調達は、当庁の委託を受けて、①データ提出領域のサンプル実装資材等に係る運用及び保守、②新しい提出方法に対応する関係行政機関等やクラウドサービス等におけるシステム構築等の導入支援等を行う請負業務等を調達するものである。

（注１） 法定調書とは、所得税法等の規定により税務署に対する提出が義務づけられて

いる資料をいう。なお本仕様書における「法定調書」には法定調書とあわせて提出される合計表を含めるものとする。また法定調書の内容については、本仕様書においては簡略化のため、「費目」「取引日」「支払人を特定する情報」「受取人を特定する情報」「金額」が記載されているものとする。国税庁は、当該情報と申告書に記載されている情報等を突合することにより、申告の適正性等を把握する。

（注２）クラウドサービスとは、民間事業者が提供するクラウド型のサービスをいう。新しい提出方法の仕組みにおいては、企業がクラウドサービスを提供する民間事業者と契約することを原則とするが、企業が独自で構築しているデータセンターを利用することも想定している。

なお、提案するクラウドサービスが「政府情報システムのためのセキュリティ評価制度」の対象になる場合、原則として、クラウドサービスリストに登録されていることを要件とすることとなる。

１.３ 業務フロー及び当該業務フローを実現するシステムの概要

クラウドサービス等を活用した企業保有情報の新しい提出方法について、想定される業務フロー及び当該業務フローを実現するためのシステムの実現方法の概要については、以下のとおりである。

なお、本項においては、業務やシステムの全体像の理解に資するよう、便宜上、各ステークホルダーの業務フロー等を記載しているが、本調達においては、「2.1 作業の実施内容」に記載されている事項が作業範囲である。

また、以下において、「1.3.3 非機能要件」を除いて経済的又は技術的に優れた代替方法がある場合には、これに限らず、提案書及び技術的対話等において積極的に提案すること。

１.３.１ 業務の概要（参照型）

参照型パターンとして、まずは、企業が税務署に提出する法定調書について、新しい提出方法として、企業がクラウドサービスに登録・保管し、クラウドサービスが国税庁に当該法定調書のアクセス権を与えることにより、法定調書を提出したとみなし、国税庁が当該法定調書を適宜のタイミングで参照する。

なお、当該パターンは、企業が国税庁に提出する法定調書以外にも、国民・事業者の負担軽減が見込まれる手続として、法人、事業所や個人が行政機関等（地方公共団体、日本年金機構、健康保険組合等）に対して提出する書類についても、将来的に応用できるようにすることも検討している。

１.３.１.１ ステークホルダー

ステークホルダーについて、法定調書のケースでは、以下を想定している。

・デジタル庁：クラウドサービスを活用した新しい提出方法を利用するためのサンプル実装資材等を提供するとともに、当該資材の開示を行政機関やクラウドサービス事業者に対して行う主体。

・クラウドサービス事業者：法定調書を提出するためのクラウドサービスを企業に対して提供する主体。デジタル庁が提供するサンプル実装資材等については、クラウドサービス事業者がクラウドサービスを提供するにあたって活用されることを想定している。クラウドサービス事業者向けのクラウドサービス等を利用した法定調書の提出に係る手続き等は以下を参照する。
https://www.nta.go.jp/taxes/tetsuzuki/shinsei/cloud/besshi.htm

・企業：新しい提出方法によりクラウドサービスを活用しつつ、国税庁に対して法定調書を提出する主体。
・国税庁：税法に基づく法定調書の提出制度を所管し、企業からクラウドサービスを活用した法定調書の提出を受け付けるほか、当該提出された法定調書を提出の際に取得したアクセス権をもとに参照するとともに、当該調書の行政文書としての保存期間が過ぎた際には、必要に応じてクラウドサービス事業者に、国税庁に対するアクセス権の解除を要請する主体。
・納税者：企業がクラウドサービス上で提出した法定調書に記載された受取人であって、当該法定調書データを自身の確定申告における提出の際に活用する主体。

１.３.１.２ 業務フロー

⑴ 企業がクラウドサービスを活用した新しい提出方法を利用するための申請等は以下を参照する。

国税庁ホームページ（クラウドサービス等を利用した法定調書の提出について）
https://www.nta.go.jp/taxes/tetsuzuki/shinsei/cloud/index.htm

⑵ 企業による提出通知の流れ

①提出者（企業等）の従業員により、業務処理を実施する。②クラウドサービスに業務データおよびアクセス権情報などの原本データが作成される。③原本データより、提出実データと、提出通知用情報を作成する。提出実データは、以後、行政機関よりデータ参照要求を受けて、その都度応答する必要があるため、アクセス権解除が通知されるまで、保持し続ける必要がある。④提出実データと提出通知用情報より、提出通知を作成して、行政機関に送信する。その際、提出実データの改変防止のため、提出実データよりハッシュ値を算出して添付する必要がある。また、提出通知用情報に含まれる、提出者特定キーと、行政機関が提出実データを特定するためのキー（アクセスキー）を付与する必要がある。さらに、クラウドサービス事業者の秘密鍵を用いて、提出通知に電子署名を付し、行政機関が送信者を正しく識別できるようにする。⑤行政機関は、リクエストを受け付け、クラウドサービス事業者の証明書を用いて署名検証を行い、リクエストの正当性を確認する。⑥行政機関は、提出通知をシステムに保存する。

⑶ 行政機関によるデータ参照の流れ

①行政機関は、提出実データの取得が必要になった際に、クラウドサービス事業者に対し、提出データの参照要求を行う。その際、提出実データのアクセスキーに、行政機関の秘密鍵を用いてに電子署名を付したリクエストを送信する。なお、データ参照要求のリクエスト先は、提出通知に記載されていたURLを用いる。②クラウドサービス事業者は、リクエストを受け付け、行政機関の証明書を用いて署名検証を行い、リクエストの正当性を確認する。③クラウドサービス事業者は、アクセス権の確認を行い、アクセス権を持つ行政機関からのリクエストの場合は、提出実データを応答する。（提出通知時とハッシュ値が同じデータを応答する必要がある。）④行政機関は、提出データを受信する。⑤行政機関は、提出データのハッシュ値を算出し、提出通知に付されていたハッシュ値と比較して、同一であることを確認する。

⑷　アクセス権解除の流れ

①行政機関は、提出実データへの参照を終了することになった際に、クラウドサービス事業者に対し、アクセス権解除要求を行う。その際、提出実データのアクセスキーに、行政機関の秘密鍵を用いてに電子署名を付したリクエストを送信する。なお、アクセス権解除要求のリクエスト先は、提出通知に記載されていた URL を用いる。②クラウドサービス事業者は、リクエストを受け付け、行政機関の証明書を用いて署名検証を行い、リクエストの正当性を確認する。③クラウドサービス事業者は、アクセス権の確認を行い、アクセス権を持つ行政機関からのリクエストの場合は、アクセス権の解除を行う。アクセス権解除により、該当の提出実データへのデータ参照が、以後行われなくなる。そのため、クラウドサービス事業者は提出実データを削除することが可能となる。(ただし、他の業務に利用するなどの理由があれば、実際に削除しなくても良い)

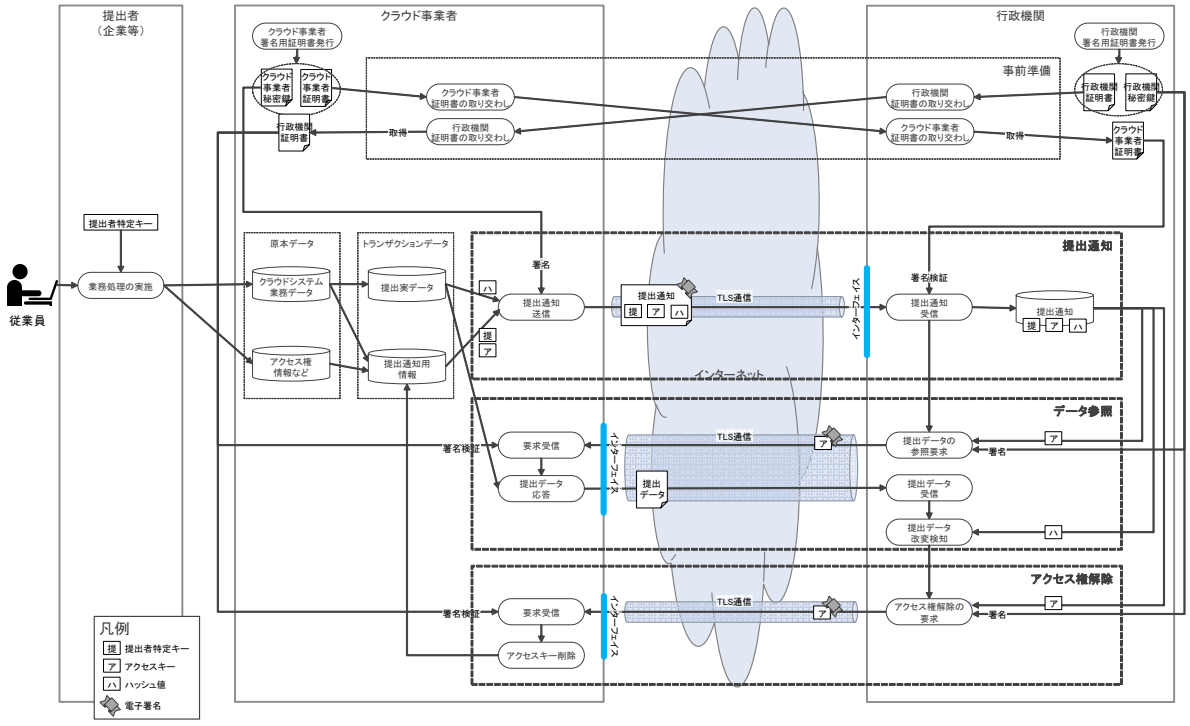

図２　システム連携の全体像

１.３.２ データ提出領域

⑴　提出通知機能

提出通知情報ファイルが配置されたことを検知し、行政機関へ提出通知を送付する機能。

⑵　データ参照機能

提出通知を受け取った行政機関よりデータ参照要求を受け付け、参照用の署名付き URL を払い出す機能。

⑶　アクセス権解除機能

データ参照が完了した行政機関より、アクセス権解除要求を受け付け、提出データに対するアクセス権限を解除する機能。

⑷　リカバリ機能

他機能での処理結果を非同期で監視し、問題があった場合に提出通知の再送をトリガーする機能。

１.３.３ 非機能要件

本事業を実施するにあたっては、以下の非機能要件に留意すること。

１.３.３.１ 拡張性要件

新しい提出方法は行政機関とクラウドサービスの情報のやり取りに特化しているが、組織の種別によらず、システムを特定の上、安全にデータを交換するための基盤であることに留意すること。また、社会環境の変化に対して柔軟に対応できるアーキテクチャを選択すること。さらに、必要に応じて機能や性能の拡張できる柔軟性を有したプログラム開発技法を採用する必要がある。

１.３.３.２ 情報セキュリティ対策

クラウドサービス事業者と行政機関の間の接続は、行政機関へ提出する個人情報を含むデータを一般のインターネット回線を利用して送受信するため、以下の 3 つのセキュリティ対策を行うこと必要がある。

⑴　通信路の暗号化と接続元の真正性確保を行うこと。

⑵　提出した提出実データの改変防止を行うこと。

⑶　エンドポイント（URL）の管理を行う。

１.４ 本調達の範囲

本調達の範囲は「2 作業の実施内容に関する事項」を、「1.5 契約期間」で定めた契約期間の中で実施することとし、本調達に係る一切の費用を契約金額に含めること。

１.５ 契約期間

本調達の契約期間は、契約締結日から令和７年３月 31 日（月）までとする。

2 作業の実施内容に関する事項

2.1 作業の実施内容

⑴　プロジェクト実施計画書の作成

本業務の実施方法及び成果物のテンプレート等を定めたプロジェクト実施計画書を作成し、デジタル庁の承認を得ること。

⑵　データ提出領域サンプル資材等の保守

クラウドサービスが企業保有情報を格納するためのデータ提出領域を構築するために必要な、サンプル資材、インターフェイス仕様書およびガイドの保守を行うこと。

また、AWS マネージドサービスの仕様変更に起因する変更が生じた場合にも、原因調査・修正・テスト・リリース等の保守対応を行う。

なお、保守作業等にあたって利用するテスト環境は受注者において用意すること。

⑶　導入支援

利用機関（クラウドサービス事業者および行政機関）がデータ提出領域を利用するにあたっての、技術支援および試験用資材の提供等を行う。

⑷　影響調査

社会保険や地方税手続きの対象拡大に伴う影響調査作業支援を行う。

⑸　次期受託事業者への引継ぎ

当該調達の受託者が変更となった場合は、次期受託者に引継ぎ・教育を行うこと。引継ぎには、以下を含めること。

イ　データ提出領域サンプル資材のソースコード等、データ提出領域サンプル資材の仕様が確認できる資料を引継ぎ対象とすること。

ロ　本調達に当たって取得又は開発した資産一切についても引継ぎ対象とすること。

2.2 納入成果物の範囲、納入期日等

2.2.1 納入成果物一覧

受託者は、「表 納入成果物一覧」に示すドキュメントについて納入成果物として納入すること。

なお、これらの納入成果物は一般的な納入成果物の体系を示すものであることから、本調達の履行に当たり、納入成果物に修正すべき内容がある場合には、契約締結後において、デジタル庁と協議の上、納入成果物を確定させること。

表　納入成果物一覧

項番	役務内容	納入成果物	納入時期
1	プロジェクト管理	プロジェクト実施計画書（スケジュール、履行体制図を含む）	契約締結後２週間以内
2	データ提出領域サンプル資材等の保守	インターフェイス仕様書	プロジェクト実施計画書にて定める日
3		ユーザガイド	
4		構築ガイド	
5		プログラムソース	
6	影響調査	調査計画書	プロジェクト実施計画書にて定める日
7		調査報告書	

項番	役務内容	納入成果物	納入時期
8	次期受託事業者への引継ぎ	引き継ぎ資料一式	プロジェクト実施計画書にて定める日

2.2.2 納入方法

納入成果物は、日本語により作成の上、日本産業規格 A 列 4 番（又は A 列 3 番）で日本語により作成の上、電子データにより納入すること。ただし、日本国において英字で表記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差し支えない。

納入成果物の様式、記載内容及び納入期限の詳細については、事前にデジタル庁と協議し、承認を受けた上で決定すること。また、各納入成果物は、それぞれ作成完了時にデジタル庁によって承認されたものとすること。

なお、電子データの納入については、以下のとおりとすること。

⑴ 納入のファイル形式は、「Microsoft Word」、「Microsoft Excel」「Microsoft Power Point」等で参照・編集可能な形式とする。また、納入成果物単位で一つの PDF にまとめたファイルを併せて納入すること。なお、他の形式による納入を求める場合には、デジタル庁と協議の上、これに応じること。

⑵ 電子データの納入に当たっては、事前に最新のウイルス定義パターンによる検疫を必ず実施すること。

⑶ 納入成果物は納入後、改変が可能となるよう、図表等の元データも併せて納入すること。

⑷ 特別なツールの使用を必要とする場合は、事前にデジタル庁の承認を得た上で、ツールとともに納入すること。

⑸ 用字・用語の表記については、「公用文作成の考え方」（令和４年１月７日文化審議会建議）に準拠すること。

⑹ 納入成果物を印刷して参照することも想定し、ページ設定（印刷範囲、印刷の向き、用紙、改ページ設定等）を適切に実施した上で納入すること。

2.2.3 納入場所、納入条件

納入場所は、デジタル庁が別途提示する場所（東京都 23 区内）とする。

また、受託者は、本調達の納入成果物の納入に際して以下の条件を満たすこと。

⑴ 上記「2.2.1 納入成果物一覧」に示す各納入時期までに納入すること。

⑵ 納入成果物の納入に係る受託者の作業及び関係書類等の作成等に関する費用は、一切を本調達の範囲に含めること。

⑶ 納入に当たっては、本仕様書に示された要件を十分に満足させるとともに、その品質が十分であることを説明できること。

⑷ 各納入成果物については、事前にデジタル庁のレビューを受け、受託者とデジタル庁の間に認識の齟齬が生じないようにすること。

⑸ 納入成果物の版管理を適切に行う方法を検討し、デジタル庁と合意の上、対応すること。

3 作業の実施体制・方法に関する事項

3.1 管理体制

受託者は、本調達を履行できる体制を整えること。受託者は、契約締結後に、履行体制図(受託者の資本関係・役員等の情報、本業務の実施場所、本業務に従事する要員の人数、連絡体制等を明らかにしたもの）を提出すること。また、体制の変更については、事前に当室の承認を得た上で行うこと。

3.2 作業要員に求める資格等の要件

3.2.1 要員に求める要件

本調達に従事する各要員は、以下に示す経験や資格を有していること。なお、要員のうち最低１名は経済産業省（旧通商産業省）情報処理技術者試験のシステムアーキテクト（SA）の資格を有するか、当該資格保有者と同等のスキルがあること。

また、各要員について、氏名、所属、役割、専門性（情報セキュリティに係る資格・研修実績等)、実績、国籍等を示すこと。

本調達仕様書において「統括責任者」とは、本調達に係るプロジェクト全体を統括して管理する者のことをいう。

⑴ 統括責任者の要件

統括責任者として必要なプロジェクト管理に関する知識・コミュニケーションスキルを有し、情報システムの構築・運用に関する業務の経験年数を 10 年以上有すること。また、以下のいずれかの資格を有するか、当該資格保有者と同等のスキルがあること。

イ 情報処理技術者試験のプロジェクトマネージャ(PM)

ロ プロジェクトマネジメント協会（PMI）が認定する PMP（Project Management Professional)

ハ 情報処理技術者試験の IT サービスマネージャー

⑵ その他の作業従事者の要件

本調達において担当する作業について過去に同等の従事経験を有し、セキュリティ教育を施した者を要員とすること。

また、AWS や Azure 等のクラウド公式認定資格を有する者であること。

3.2.2 その他

⑴ 受託者は、作業従事者を限定して受託業務を行うものとし、当該作業従事者の氏名、保有資格、実績、国籍、現在の所属等を書面により提出し、当庁の承認を得ること。

⑵ 当庁が作業従事者（統括責任者を含む。）の中に委託業務の遂行について不適当な者がいると認める場合には、受託者に対してその理由を付して通知し、要員の交代も含めた必要な措置を要求することができるものとする。

3.2.3 実績

次に掲げる情報システムの開発及び保守の実績を有すること（該当する直近のシステムの開発実績を示す書類を提出すること。)。なお、⑴⑵の実績は必須とする。

⑴ 特定のコンピュータ機器（OS 含む。）に依存しないオープンシステム

⑵ システム間でデータ交換を行うシステム

⑶ インターネットを利用したセキュリティ要求が高いシステム
⑷ WebAPI を備えたシステム
⑸ クラウド技術（マイクロサービスアーキテクチャやサーバレスアーキテクチャ等）やコンテナ技術を用いたシステム

３.３ 社内教育に関する要件

受託者は、要員に対する教育体制及び情報セキュリティ教育の方針・計画をデジタル庁に提出すること。

３.４ 作業場所

受託業務の作業場所は、受託者の事業所内又は受託者の事業所と別に受託者の負担により受託者が用意する場所とし、事前に当室の承認を得ること。

３.５ 作業の管理に関する要領

３.５.１ プロジェクト管理

⑴ 受託者は、「7.6.6 遵守すべき文書等」の⑴に準拠したプロジェクト実施計画書を策定し、当室の承認を得ること。詳細については当室と協議の上、決定すること。
⑵ プロジェクト実施計画書を変更する必要が生じた場合は、速やかに改定する計画を策定し、当室の承認を得ること。

３.５.２ プロジェクト管理の実施及び報告

受託者は、プロジェクト実施計画書に基づき、適切にプロジェクトの進捗管理、課題・問題管理等を行うこと。また、会議等を通じ、プロジェクト運営上必要となる報告（進捗報告等）を行うこと。

３.５.３ 月次報告

導入支援開始後は、導入支援の状況について月次で報告すること。詳細については当室と協議の上、決定すること。

4 作業の実施に当たっての遵守事項

4.1 機密保持、資料の取扱い

4.1.1 機密保持

受託者は、本調達を実施するに当たり、入手した資料（電子媒体、文書、図面等の形態を問わない。）等については管理台帳等により適切に管理し、かつ、以下の事項に従うこと。

⑴ 秘匿性の高い書類の資料等については、施錠可能なキャビネット等に保管すること。

⑵ 業務に必要がなくなり次第、速やかに返納すること。

⑶ 受託者は、別紙「個人情報取扱特記事項」に基づき、本調達に関して入手した情報等（公知の事実等を除く。）及び業務遂行過程で生じた納入成果物に関する情報を本業務の目的以外に使用又は第三者に開示若しくは漏えいしてはならないものとし、本調達に係る作業に従事した者が異動又は退職等した場合も含め、必要な措置を講ずること。

関係者等に対しメールによる連絡をする場合にあっては、他の受信者のメールアドレスが閲覧できないよう BCC 機能により送信するなど、個人情報等（他の受信者の個人情報以外の情報を含む。）の流出防止に万全を期すこと。

⑷ 本調達に係る検収後、上記に記載される情報を裁断等の物理的破壊、消磁その他復元不可能な方法により削除又は返却すること。

⑸ 受託者の責任に起因する情報の漏えい等により損害が発生した場合は、それに伴う弁済等の措置はすべて受託者が負担すること。

⑹ 受託者は本調達に係る作業に従事する者の機密保持に関する誓約書等を取りまとめ、デジタル庁にその写しを提出すること。

⑺ この項目について受託者は、契約期間の終了後においても同様とする。

4.1.2 書類の貸与

当室は、受託者が本調達を履行する上で、必要な関連書類（各種実施要領等）を文書又はデータで随時貸与する。ただし、貸与された書類（貸与後に複製・複写したものを含む。）は、当室から請求があった場合及び本調達終了時に当室に返却又はデータの削除を行うこと。

なお、受託者は貸与された書類を本調達以外の目的に使用してはならない。

また、貸与に当たっては、当室へ申込みを行い、機密保持に関する誓約書等を併せて提出すること。

4.2 情報セキュリティに関する受託者の責任

4.2.1 情報セキュリティを確保するための体制の整備

⑴ 受託者は、受託者の組織全体の情報セキュリティを確保するとともに、本調達において取り扱う情報の漏えい、改ざん、滅失等が発生することを防止し、情報システムのセキュリティを確保する観点から、適正な保護、管理対策及びセキュリティ対策を実施すること。

⑵ 上記⑴の実施状況について、定期又は不定期の把握及び評価を行う場合があるが、これに応じることとし、万が一、受託者における情報の漏えい、改ざん、消去等の事象、情報システムに対する侵害等が発生した場合に実施すべき事項及び手順等を明確にすること。

⑶　各工程において、当庁の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。第三者機関による品質保証体制を証明する書類等（国際規格（ISO9001やISO/IEC27001）の公的資格等）が提出可能な場合は、提出すること。

４.２.２ 情報セキュリティが侵害された場合の対処

⑴　受託者は、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、直ちにデジタル庁に報告した後、再発防止策を立案し、デジタル庁の承認を得た上で実施すること。

なお、受託者は、被害の程度を把握するため、必要な記録書類を契約終了時まで保存し、デジタル庁の求めに応じて納入成果物とともに、デジタル庁に引き渡すこと。

また、上述の「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、以下の事象を含むことに留意すること。

イ　デジタル庁が受託者に提供し受託者によるアクセスを認めるデジタル庁の情報の外部への漏えい及び目的外利用をしたこと。

ロ　受託者がデジタル庁の内部情報へアクセスしたこと。

⑵　受託者は、情報セキュリティが侵害され又はそのおそれがある事象が本業務中及び契約に定める瑕疵担保責任の期間中に発生し、かつ、その事象が受託者における情報セキュリティ上の問題に起因する場合は、受託者の責任及び負担において次の各事項を速やかに実施すること。

イ　情報セキュリティ侵害の内容及び影響範囲を調査の上、当該情報セキュリティ侵害への対応策を立案し、デジタル庁の承認を得た上で実施すること。

ロ　発生した事態の具体的内容、原因及び実施した対応策等について報告書を作成し、デジタル庁へ提出して承認を得ること。

ハ　再発防止策を立案し、デジタル庁の承認を得た上で実施すること。

ニ　上記のほか、発生した情報セキュリティ侵害について、デジタル庁の指示に基づく措置を実施すること。

４.２.３ 情報セキュリティ監査等への対応

⑴　受託者は、デジタル庁が本契約期間中において情報セキュリティ監査等を実施する場合（再委託先においても同様とし、セキュリティ診断業者へ委託した場合を含む。）、あらかじめ情報セキュリティ監査等を受け入れる部門、場所、時期、条件等をデジタル庁へ提示し、各種情報等をデジタル庁へ提供するとともに、デジタル庁から以下に示す指示等があった場合は、それに従って支援すること。

イ　監査人への資料の提示

ロ　監査人によるヒアリングへの対応

ハ　監査人による視察における立ち合い

ニ　監査人が監査に使用するアカウントの割り当て及び監査実施後のその無効化

ホ　監査人が実施する監査作業に必要なシステムの設定変更及び監査実施後のその復旧

⑵　情報セキュリティ監査等に係るデジタル庁からの指摘事項について、情報セキュリティ監査等に係る対応策の検討、提示及び実施を行うこと。

なお、対応策については、デジタル庁と調整の上、受託者の責任と負担により実施すること。

⑶　受託者自ら情報セキュリティ監査等を実施することを妨げるものではないことから、受託者は、当該実施結果についてもデジタル庁へ報告すること。
⑷　情報セキュリティ監査等の実施については、上述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。

４.２.４ 情報セキュリティ対策の改善

受託者は、前各項に記載するもののほか、本業務遂行における情報セキュリティ対策の履行状況についてデジタル庁が改善を求めた場合には、デジタル庁と協議の上、必要な改善策を立案して速やかに実施するものとする。

４.２.５ セキュリティ教育

本業務に係る情報の漏えい事故等の発生は、番号制度全体への信頼を揺るがし、また、社会に重大な影響を及ぼすことから、受託者においては、当該漏えい事故等を予防するため「3.3 社内教育に関する要件」に掲げる教育について、具体的なセキュリティ事故を想定し、確実かつ定期的に実施すること。

４.３ 遵守する法令等

本業務の遂行に当たっては、以下の法令等を遵守し履行すること。
ア　民法（明治 29 年法律第 89 号）
イ　刑法（明治 40 年法律第 45 号）
ウ　私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号）
エ　著作権法（昭和 45 年法律第 48 号）
オ　不正アクセス行為の禁止等に関する法律（平成 11 年法律 128 号）
カ　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）

５ 成果物の取扱いに関する事項

５.１ 知的財産権の譲渡

本調達における知的財産権等の扱いを以下に示す。

⑴　本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、受注者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全て当庁に帰属するものとする。

⑵　当庁は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。また、受注者は、成果物について、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（以下「複製等」という。）ができるものとする。ただし、成果物に第三者の権利が帰属するときや、複製等により当庁がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

⑶　納品される成果物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。）が含まれる場合には、受注者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の受注者は、当該既存著作物の内容について事前に当庁の承認を得ることとし、当庁は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専ら当庁の責めに帰す場合を除き、受注者の責任及び負担において一切を処理すること。この場合、当庁は係る紛争等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じるものとする。

⑷　本件成果物の所有権は、当庁から受注者に対価が完済されたとき受注者から当庁に移転するものとする。

⑸　受注者は当庁に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。また、受注者が本受託業務の実施の過程で生じた納入成果物に係る著作権を自ら使用し又は第三者をして使用させる場合は、当庁と別途協議するものとする。

⑹　受注者は使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

５.２ 契約不適合に関する責任

本調達における契約不適合に関する責任を以下に示す。

⑴　受託者は、デジタル庁に納入した納入成果物について、本業務の検収日から起算して１年間、契約不適合に関する責を負わなければならない。

⑵　受託者は、納入成果物の契約不適合が受託者の故意又は重大な過失に基づく場合には、上記⑴の定めにかかわらず、本業務の検収日から起算して 1 年を経過した後も契約不適合に関する責を負わなければならない。

⑶　デジタル庁は、前各項の期間において、契約不適合のある本調達の納入成果物について、受託者に相当の期限を定めて修補を請求又は修補に代え若しくは修補とともに当該契約不適合により通常生ずべき損害に対する賠償の請求をすることができる。

⑷　本調達の契約期間及び上記⑴⑵の期間におけるサービスの障害対応に当たり、他の

関係者との協議が必要な場合には速やかに実行できる体制を確保し、他の関係者と協力して対応すること。

５.３ 検収

５.３.１ 検査

デジタル庁は、納入成果物の作成や役務の提供が本調達に示す要件を満たしているか検査を実施する。受託者は、検査に際し以下を遵守すること。

⑴ 受託者は、納入成果物の納入が完了した時は、デジタル庁の検査職員に対し、その旨を報告するとともに、検査を受けなければならない。また、当該検査は納入成果物の修正・改善の場合も同様とする。

⑵ 検査の結果、納入成果物の全部又は一部が不合格となった場合には、受託者は直ちに対象の納入成果物を引き取り、必要な修正・改善を行った後に、指定した日時までに再度納入すること。

⑶ 受託者は、デジタル庁職員からの質問、検査への対応を行うとともに資料の提示等の指示に従うこと。また、納入成果物に対し、デジタル庁から修正及び改善要求があった場合には、適切に対応を行うこと。

⑷ 検査に係る受託者の作業及び関係書類の作成等に要する費用は、一切を本調達の範囲に含めること。また、必要に応じ作成資料の再提示を求める場合があることから、作成資料は常に履歴を管理し、最新状態を保つこと。

５.３.２ 検収期限

受託者から納入された成果物については、デジタル庁が承認したことをもって検収合格とする。

本調達の検収期限は令和７年３月 31 日（月）とする。

６ 参加資格に関する事項

６.１ 参加要件

⑴　品質管理体制について、ISO9001:2008、ISO9001:2015 若しくは組織としての能力成熟度について CMMI レベル３以上の認証のうちいずれか、又はこれらと同等以上の認証等を取得していること。

⑵　プライバシーマーク付与認定、ISO/IEC27001 認証（国際規格）若しくは JIS Q 27001 認証（日本産業規格）のうちいずれか、又はこれらと同等以上の認証を取得していること。

⑶　次に掲げる情報システムの開発の実績を有すること（該当する直近のシステムの開発実績を示す書類を提出すること。）。また、官公庁との契約実績があること(当該情報システムの開発に係る契約について示すこと。)。

イ　特定のコンピュータ機器（OS 含む。）に依存しないオープンシステム

ロ　複数システム間でデータ交換を行うシステム

ハ　インターネットを利用したセキュリティ要求が高いシステム

ニ　WebAPI を備えたシステム

ホ　クラウド技術(マイクロサービスアーキテクチャやサーバレスアーキテクチャ等)やコンテナ技術を用いたシステム

６.２ 参加制限

デジタル庁における入札制限等に関する規程に基づき入札制限対象企業の指定を受けていない者（入札制限の適用を除外された者を含む。）であること。

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c5d7192e-22e0-4810-8afd-ce83c50af6a4/20220309_policies_procurement_doc_01_1.pdf

7 再委託に関する事項

7.1 再委託の制限

受託者は、受託業務の全部又は一部を第三者に委託することはできない。ただし、受託者があらかじめ書面により再委託の申請を行い、当庁が承認した場合にはこの限りではない。

なお、受託者は、この契約により生じる権利又は義務を第三者に譲渡又は継承させてはならない。

7.2 再委託の承認手続

⑴ 受託者は、本業務の一部について再委託の承認を求める場合は、次のイからニを記載した再委託承認申請書を提出するとともに、ホ及びヘを記載した文書、再委託に係る履行体制図についても併せて提出すること。

イ 再委託先名称（商号）、住所

ロ 再委託する業務の範囲、再委託の必要性及び再委託予定金額

ハ 再委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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

ニ その他当庁が求める情報

ホ 受託者と同等のセキュリティ水準を再委託先も具備すべきことを受託者との間に定めている内容

ヘ 再委託先の情報セキュリティに関する対策方針及び管理方法

⑵ 再委託先の追加若しくは変更又は再委託先から更なる委託など複数の段階で再委託等を行う必要が生じた場合は、上記⑴に準じてあらかじめ文書により提出し、デジタル庁の承認を受けること。

⑶ 本業務は、受託者又はデジタル庁より承認を得た再委託先において完結できること。ただし、デジタル庁が承認した場合でも、受託者はデジタル庁に対し、承認を得た第三者の行為について全責任を負うものとする。

⑷ 提出先の詳細及び承認申請書等の様式については、別途指示する。

7.3 再委託に係る責任

受託者は、デジタル庁が再委託を承認した場合であっても、デジタル庁に対し「7.2 再委託の承認手続」の規定により受託者から業務の再委託を受けた事業者が行った作業について、全責任を負うものとする。

なお、受託者は、再委託先に対して本仕様書の「4.1 機密保持、資料の取扱い」、「4.2 情報セキュリティに関する受託者の責任」及び「5.1 知的財産権の譲渡」を含めて受託者と同等の義務を負わせるものとし、再委託先との契約においてその旨を定めるものとする。

また、再委託先が義務に違反した又は義務を怠った場合には、デジタル庁は、当該再委託先への再委託の中止を求めることができるものとする。

7.4 再委託先の管理・監督

受託者は、再委託先に対して、定期的又は必要に応じて、作業の進捗状況及び情報セキュリティ対策の履行状況等について報告を行わせる等、再委託業務の適正な履行の確保に努めるものとする。

また、受託者は、デジタル庁が再受託業務の適正な履行の確保のために必要があると認める時は、その履行状況についてデジタル庁に対し報告するものとする。

7.5 環境への配慮

本調達に係る納入成果物については、「国等による環境物品等の調達の推進等に関する法律（グリーン購入法）」に基づいたものを可能な限り導入すること。

7.6 その他

7.6.1 提案の形態

単独の事業者による提案とし、複数の事業者による共同提案は認めないものとする。

7.6.2 業務改善に係る提案

受託者は、作業及び納入成果物の内容について、技術的又は経済的に優れた代替方法及びその他改良事項を発見・発案した場合は、当該発見・発案に基づき作業及び納入成果物の内容変更を提案するものとする。この場合、デジタル庁は、受託者との協議の上、必要があると認めた場合は、作業又は納入成果物の内容変更を指示するものとする。

7.6.3 指示等の証跡主義

本調達における具体的な指示、報告、申出、質問、回答、協議等は、原則としてすべて電子メール等の証跡が残る手段で行うものとする。ただし、緊急又はやむを得ない場合は口頭で行うことができることとするが、事後において必ず書面に記載し、交付するものとする。また、コミュニケーションツールについては、電話・電子メール以外にも有効な手段があれば積極的に提案を行うこと。

なお、本項については、技術的対話の際には特に指示がある場合を除き適用されない。

7.6.4 代替提案

⑴　提案書の作成に当たり、本調達に示す仕様によることなく、経済的又は技術的に優れた代替方法による提案を行うことを妨げない。なお、代替提案を行う場合は、本仕様書に記載された仕様との差分を明らかにした上で、優れている点を具体的に示すとともに、その代替提案を採用することによる影響範囲を明確にすること。また、代替提案を採用することにより生じる追加作業及び費用については、一切を本調達に含めること。

⑵　契約締結後において、作業及び納入成果物の内容に、技術的又は経済的に優れた代替方法、その他改良事項を発見・発案した場合には、その発見・発案された内容に基づいた作業及び納入成果物の内容変更をデジタル庁に提案するとともに指示を求めるものとする。なお、代替提案を採用することにより生じる追加作業及び費用については、一切を受託者の負担とすること。

7.6.5 技術等提案の遵守

本仕様書及び企画提案書に記載した内容については、確実に履行すること。

7.6.6 遵守すべき文書等

本調達の実施に当たっては、次の文書に記載された事項を遵守すること。また、次の文書以外でも、業務・システムの最適化に際して遵守すべき文書等が決定された場合には、それらに記載された事項も遵守すること。なお、遵守すべき文書が変更された場合は、変

更後の文書を遵守すること。

⑴ デジタル・ガバメント推進標準ガイドライン
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/8a3b6203/20230331_resources_standard_guidelines_guideline_01.pdf
⑵ 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル
https://www.nisc.go.jp/pdf/policy/general/SBD_manual.pdf
⑶ 政府機関等のサイバーセキュリティ対策のための統一基準群
イ　政府機関等の対策基準策定のためのガイドライン
https://www.nisc.go.jp/pdf/policy/general/guider5.pdf
ロ　政府機関等のサイバーセキュリティ対策のための統一基準
https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf
ハ　政府機関等のサイバーセキュリティ対策のための統一規範
https://www.nisc.go.jp/pdf/policy/general/kihanr5.pdf
ニ　政府機関等のサイバーセキュリティ対策の運用等に関する指針
https://www.nisc.go.jp/pdf/policy/general/shishinr3.pdf
⑷ サイバーセキュリティ 2023
https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023.pdf
⑸ デジタル庁情報セキュリティポリシー
当該セキュリティポリシーの開示は、契約締結後、受託者がデジタル庁に守秘義務の誓約書を提出した際に開示を行う。
⑹ 政府情報システムにおけるクラウドサービスの利用に係る基本方針
https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210910.pdf

７.６.７ その他

⑴　本調達は、原則として日本語により対応すること。
⑵　本調達仕様書に記載なき事項にあっても本調達の業務遂行において必要と認められる事項に関しては、別途デジタル庁と協議の上、実施すること。