令和５年度　マイナポータル新フロントの改善及び運用に関する調達仕様書概要案

デジタル庁

目次

調達案件の概要

1. 調達の件名

令和5年度　マイナポータル新フロントの改善及び運用

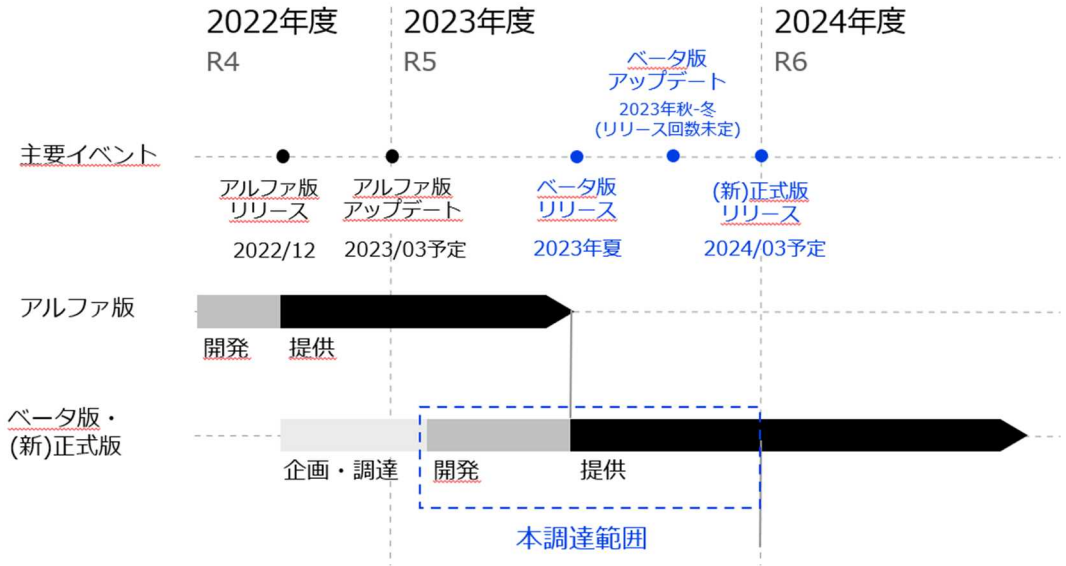
2. 調達の背景

「デジタル社会の実現に向けた重点計画」にて言及されるように、現在の日本において一人ひとりが多様な幸せを実現するため、自身のニーズに合ったサービスを選ぶことのできる、デジタルを活用したきめ細かなサービスの提供が重要である。

現在デジタル庁で管理運用するマイナポータルは、この実現の要となる生活者との接点であるが、今まで積み上げ的な機能開発により開発速度の低下、改修コスト増大が顕著化している状況となっている。また、画面の使い勝手として①情報量が多い、②どのような機能があるか分からない、③操作が複雑等の課題が顕著であった。

これを改善し飛躍的に住民の生活の質を向上させるため「見つからない・使いづらい・面倒」といった利用における問題を徹底的に解決し、サービスの網羅性とアクセスの容易性を向上、サービス利用時の労力・所要時間を削減し、先進国で顧客満足度が最も高いサービスをつくることを目指している。この布石となる取組として令和4年度に情報設計と表現を見直し、一部の機能に限定して速やかに実証環境を用意した実証アルファ版をリリースし現在実証を行っている。本事業では更なる利用者体験の向上を目指し、またこのサービスを正式にすべての利用者へ提供しうるものとするため、実証ベータ版及び新正式版の構築を行う。主要なマイルストーンは「図1. 主要マイルストーン」に示す。

図1. 主要マイルストーン



3. 調達目的及び調達の期待する効果

本調達範囲である新正式版では、オンラインサービスを利用したい国民・住民にとって「1.行政手続きをストレスなく忘れずに、2.損せず完了できる」こと、また UI/UX の見直しとオンライン化を推進することにより政府や自治体の窓口や事務処理コスト削減を目指す。

なお、実証ベータ版では以下をゴールとして想定している。

- 利用者が、あんしんして、ストレスなく当たりまえに使い続ける
- 利用者が、必要なタスクを忘れず、少ない手間で手続きを完了する
- 時事に応じたサービス・機能をすぐに受けられる

新正式版及び実証ベータ版の提供方針や対応予定内容についての詳細は、「別添4 新フロント提供方針」参照すること。

これらを実現するために、フロントデザイン変更の迅速化、運用ベンダーの柔軟化、開発コストの低減を目指す。既存のマイナポータルではフロントエンドとバックエンドが一体となったアーキテクチャを採用していたが、本事業ではフロントエンドとバックエンドの疎結合化を実現する。

また実証アルファ版では一部の機能について、暫定的なアーキテクチャでフロントエンド・バックエンドの分離を実現したが、本事業では実証アルファ版の実装範囲のアーキテクチャの見直しと再構築も含めて検討する。

4. 業務規模の想定

想定する業務規模は非機能要件の検討業務にて最新の利用状況を参考に検討する。参考情報として現在のマイナポータルの実績値を「表 1. マイナポータル利用状況」に示す。マイナンバー活用により今後も利用数増加が見込まれている。

表 1. マイナポータル利用状況

集計対象	件数	取得年月
有効アカウント数	3,417 万件	令和 4 年 11 月
サービストップアクセス件数（月間平均）	2,738 万件	過去半年間（令和 4 年 6 月～令和 4 年 11 月）の平均
サービストップアクセス件数（月間ピーク）	4,488 万件	令和 4 年 7 月 ※過去 1 年間（令和 3 年 12 月～令和 4 年 11 月）で最もアクセスが多かった年月
ログイン件数（月間平均）	1,184 万件	過去半年間（令和 4 年 6 月～令和 4 年 11 月）の平均
ログイン件数（月間ピーク）	2,034 万件	令和 4 年 7 月 ※過去 1 年間（令和 3 年 12 月～令和 4 年 11 月）で最もログインが多かった年月

5. 用語の定義

本書において定義される用語を「表 2 用語定義（アルファベット、五十音順）」に示す。

表 2. 用語定義（アルファベット、五十音順）

項番	用語	説明
1	API基盤システム	今後、構築・提供を予定している、各種APIゲートウェイ等の機能又はシステムの総称（構築後の追加・改修を含む）。
2	フロントエンド	Web ブラウザ等の、ユーザーインターフェース（UI）を指す。
3	バックエンド	データベースや Web サーバー、アプリケーションサーバー等サーバーサイドシステムを指す
4	自己情報取得システム	「「マイナポータルを活用したサービス検索・電子申請機能等の提供」に係る追加開発等業務（電子申請に必要となる自己情報を取得する為のマイナポータル自己情報確認API機能の開発及び保守）」に係る調達により構築・提供されるデータ変換等の機能又はシステムの総称（構築後の追加・改修を含む）。
5	受託者	本調達仕様書に基づき業務を受託する者を指す。
6	情報提供等記録開示システム	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（平成 25 年法律第 27 号。以下「番号法」という。）附則第6条第3項に規定する情報提供等記録開示システムを指す。当該システムは、情報提供ネットワークシステムを介して自己の情報提供等記録を確認する機能等（「情報提供等記録表示」、「自己情報表示」、「お知らせ表示」及び「認証連携」の機能）を有する。
7	情報提供等記録開示システム等	情報提供等記録開示システム、自己情報取得システム、API基盤システムの3つのシステムの総称。
8	情報提供ネットワークシステム	番号法第2条第 14 項に規定する情報提供ネットワークシステムを指す。当該システムは、情報提供に用いられる個人を特定するための符号の付番・変換や情報提供の許可を行う機能、情報照会者及び情報提供者との接続のための機能等を有する。
9	情報保有機関	番号法第 19 条第7号に規定する情報照会者及び情報提供者並びに同法第 19 条第 14 号の規定により情報提供ネットワークシステムを使用して特定個人情報の提供を求める者、その求めにより情報提供ネットワークシステムを使用して特定個人情報を提供する者並びに同法附則第6条第6項の規定により、情報を開示又は提供する者を指す。

項番	用語	説明
10	ぴったりシステム	「マイナポータルを活用したサービス検索・電子申請機能等の提供」に係る調達により構築・提供されている機能又はシステムの総称（構築後の追加・改修を含む）。
11	マイナポータル	情報提供等記録開示システム、ぴったりシステム、自己情報取得システム、API基盤システムの4つのシステムの総称。
12	マイナポータルAP	マイナポータルのアカウント開設、ログイン認証等に当たり、マイナンバーカードによる電子署名や券面事項の読取等を行う専用のネイティブアプリケーション。
13	民間サービス	民間企業が提供するクラウドサービスであり、SaaS（Software as a Service）、IaaS（Infrastructure as a Service）等のサービス、付随する回線及び外部サービスを指す。
14	BFF	フロントUIとバックの中間に入り、固定のAPIから柔軟な情報に作り変え、フロントに渡す機能

6. 連携する関係者

本事業を実施する上で関係する者は以下「表 3. 本事業の関係者」のとおりである。

表 3. 本事業の関係者

関係者	役職	役割／関係性
担当職員	デジタル庁職員	本契約及び本システムの利用推進等を行うデジタル庁マイナポータル新フロントの改善　調達担当
マイナポータル班	デジタル庁職員	現行マイナポータルの維持運用を実施。必要に応じニーズ等のヒアリングを行う。
マイナポータル運用管理事業者	他事業者（2社）	マイナポータルの管理の維持運用 受託者とマイナポータル班と共に、必要なAPIを設計し構築を担当
他システム運用事業者	他事業者（複数）	マイナポータルと連携する他のシステム群の運用事業者
受託者		新正式版及び実証ベータ版の開発者

7. 契約期間

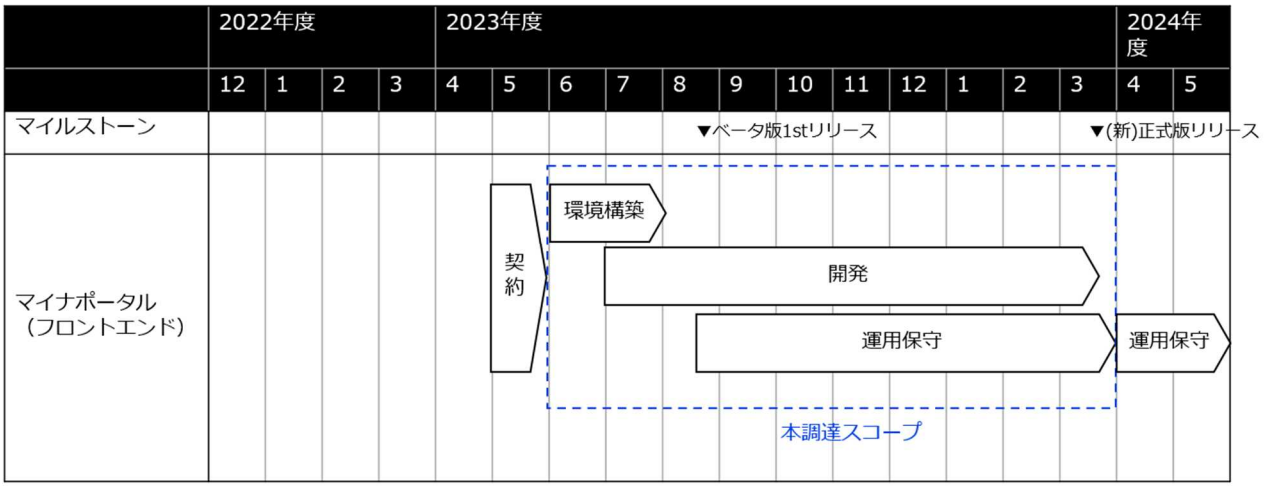
契約日～令和6年3月29日

※運用保守業務は令和6年3月31日まで

8. 作業スケジュール

作業スケジュールを「図 2. 作業スケジュール」に示す。ベータ版 1st リリースは 2023 年夏を想定し（具体的な時期は未定）、新正式版リリースは 2024 年 3 月を想定している。また、ベータ版 1st 後から新正式版リリースまでの期間は開発状況に応じて順次リリースを想定しているが、リリース回数・時期・対象機能は未定である。詳細は協議の上で決定するものとする。

図2. 作業スケジュール



9. 技術的対話の論点

技術的対話の論点は以下を想定している。

(1) アジャイル開発の進め方

本事業ではマイナポータルとして初めて仮説検証型のアジャイル開発を行うため、事業者の意見も取り入れながら最適な開発方法を検討したい。対話の論点は以下を想定している。

- 開発の進め方及び事業者と当庁の業務の棲み分けやコラボレーションの仕方
- 開発業務で作成すべき成果物
- 開発業務に求める要員規模、要員の要件や体制

(2) アプリケーションアーキテクチャ

本事業ではフロントエンドアプリケーションのアーキテクチャを、事業者の意見を取り入れながら検討することを想定している。本事業のシステム方針は、別添 13 情報システム稼働環境構築 に詳細を記載しているため、諸々の事前条件・前提条件を加味しつつ最適なアーキテクチャを対話の中で決定するものとする。

調達範囲

本事業における受託者の責任範囲は、以下の業務とする。

1. 総合調整業務

本事業が円滑に進行するよう、関係者間の調整を行う。具体的には本プロジェクトにおける計画策定、課題管理、進捗管理、その他事業全体の情報集約や方針策定等を行う。

2. アプリケーション開発業務

当庁とコラボレーションしながらアジャイル方式でアプリケーション開発業務を行う。

3. 情報システム稼働環境構築、調整業務

当庁と協議し非機能要件を定める。マイナポータル運用管理事業者と調整し情報ステム環境構築を行う。

4. 運用保守業務

開発した情報システムやフロント UI について、運用保守を行うとともに、将来、運用保守事業者が運用保守を円滑に実施するための各種ドキュメントを整える。またリリース直後の期間は重点的な監視業務を行う。なお、本事業の対象範囲外であるバックエンドやフロントエンドの一部機能については、運用保守業務の対象外とする。運用保守の範囲や作業内容は協議の上決定し、ドキュメントに記載すること。

作業の実施内容

1. 総合調整業務（事業全体に係る作業）

全般

(1) デジタル・ガバメント推進標準ガイドライン及び同解説書を踏まえた手順とすること。

(2) 契約締結後10営業日以内に作業体制とともにプロジェクト計画書（案）を作成し、当庁の承認を得ること。プロジェクト計画書にはマスタスケジュール、体制、開発方針の他、進捗管理、課題管理、変更管理、リスク管理、コミュニケーション管理、情報セキュリティ管理の各方法（以下①～⑤）に加え、受託者が有効なプロジェクト管理を行うために有効と思われるものについて、受託者

が提案し、当庁担当と検討し決定した項目について記すものとする。

① 情報セキュリティ対策の実施内容及び管理体制

② 本件特定役務の実施に当たり、生産物等に受託者又は受託者以外の他の者による意図しない変更が加えられないための管理体制

③ 情報セキュリティインシデントの対処方法

④ 情報セキュリティ対策その他の契約の履行状況の確認方法

⑤ 情報セキュリティ対策の履行が不十分な場合の対処方法

(3) 作業体制には、システム開発作業責任者、システム開発作業に係る個人情報取扱責任者及びシステム開発作業担当者の氏名及び所属、担当作業の内容、指揮命令系統、情報セキュリティ対策に係る管理・連絡体制並びに連絡先を明記すること。

(4) 開発期間中における変化への対応、運用開始後における継続的な改善にも対応可能な体制を確立すること。

全体工程・進捗管理

(1) プロジェクトの状況を正しく把握し、計画工数内で、所定の期日までに成果物を作成することを目的として、進捗管理手法を提示し、進捗管理を実施する方法を提案すること。なお、現行のマイナポータル運用管理事業者も、本事業において当庁の支援を担う者として、共同で実施することとなるため、他事業者とも協力し、プロジェクトの状況について情報共有やコミュニケーションを図ること。

(2) 進捗について週次進捗報告書及び月次進捗報告書を作成し、進捗会議を開催して当庁に報告すること。その際定性的・定量的に進捗状況を報告し、当庁及び支援事業者において進捗の妥当性が評価できるようにすること。遅れが発生した場合には当庁担当と協議の上必要に応じ計画の見直しを行うこと。

(3) 前項における報告等平時の報告は書面又はオンラインで行う等、効率的な事業運営に努めること。

課題管理

事業の進捗管理、成果物の品質確保及び納期遵守の観点から、顕在化している事象を課題として管理する。課題の管理に当たっては、その事象、解決策、解決期日、解決担当者等を記した課題管理台帳を作成し、適宜、更新して管理することを想定している。管理は当庁及び受託者の双方で共同管理できるようなツールを活用する等し、非効率な運用をできる限り避けること。

リスク管理

まだ発生していないが、顕在化すれば成果物の品質確保及び納期遵守に影響を及ぼす可能性のある事象をリスクとして管理すること。リスクの管理では、その事象、対応策を当庁と協議の上決定することとし、その実施については、状況を監視した上で、顕在化の恐れが高まった際に実施する等、監視方針や対応策実施の契機となる状態の定義等も合わせて管理すること。

変更管理

プロジェクト開始時に要求事項の優先度付けを行い、優先度に従った作業計画を策定すること。プロジェクト実施中に要求の追加や変更が発生した場合は、再度優先度について当庁と検討した上で、都度計画の見直しを行うこと。また上述のような優先度管理の方式を管理するためのツールを含めて提案すること。

定例会議の開催

当庁と各業務担当間の連絡調整のため、事業の進捗確認等を行う会議を定期に開催する。開催頻度及び開催方法については、当庁と協議して決定することとするが、週1回の開催を基本とし、その他については必要に応じて協議のうえ設定すること。また、その議事録については、営業日を基準として、会議実施の翌日から起算して5営業日以内に作成の上、当庁に提示し了承を得ること。

コラボレーション環境の整備

議論や連絡、資料作成は、できるだけスピーディに、無駄なく簡潔に行えるよう心がける。コラボレーションを前提とし、行政文書としての保存への考慮は当然ながら、チームでの取扱いやすさ及びセキュリティについて考慮した環境を整備する。

- メッセージング: Slack を基本とし、必要のある場合にのみメールを用いる。
- ミーティング: 効率的で安全なオンラインミーティングツール（Slack Huddle, Teams 等）を用意する。安全性を考慮して利用するツールを提案し、当庁の了承を得ること。またミーティングはオンライン開催を基本ルールとする。（オフライン開催も状況によって可能）
- ドキュメンテーション（企画書や議事録等）: 同期編集が可能な環境を用いる。ファイルを納品する場合も、編集可能形式で共有する等して、コラボレーションのしやすさに考慮する。安全な方式を提案し、当庁の了承を得ること。

情報セキュリティ管理

本事業では、受託者に提供、貸与若しくは閲覧を許可したすべての情報並びにそれらの情報を基に作成する成果物（中間成果物を含む。）及び関連資料、本システムの運用等により取得した事業者、事務局及び補助金に関するすべての情報を情報セキュリティ管理の対象とする。これらの情報は全てプロジェクト外秘とし、外部の人間への情報漏洩、改ざん、毀損が発生しないよう管理するとともに、そうした事象が発生していないことを確認できる方法及び体制を整備すること。

2. アプリケーション開発業務

必要な体制を構築しアプリケーション開発業務を行う。開発の進め方や当庁との業務の棲み分け等は対話で協議する。業務の想定及び要求事項は以下に示す。

(1) 要求関連資料

- 別添4 新フロント提供方針
- 別添5 要求事項一覧_エピック
- 別添6 要求事項一覧_ストーリー定義
- 別添7 要求事項一覧_ストーリー
- 別添8 要求事項一覧_既存機能
- 別添9 要求事項一覧_定義

(2) 開発に関する当庁の想定

- 別添 10 アプリケーション開発の進め方(想定)
- 別添 11 サービスデザイン業務
- 別添 12 デジタル庁の体制(想定)

3. 情報システム稼働環境構築、調整業務

必要な体制を構築し情報システム環境構築業務及び調整業務を行う。業務の想定は以下に示す。

- 別添 12 デジタル庁の体制(想定)
- 別添 13 情報システム稼働環境構築

4. 運用保守業務

システム監視

システムを構成するアプリケーション等を監視しインシデントを検知記録する。

監視要件運用・保守に求める要件を達成するため、24 時間 365 日のシステム監視業務、障害時復旧対応を実施する。本事業の開発範囲はフロンエンドアプリケーションが主となるため、利用者のブラウザ上で発生したエラーを収集する仕組みを構築し、アプリケーション起因・ブラウザ等の外部環境起因の障害を検知すること。障害の発生を検知した場合は、速やかに当庁の承認を得た上で一時対応・恒久対応を実施すること。本システムの設計書(ソースコード・基盤構成図等)に変更があった場合は、変更を反映した設計書を作成して作業終了後に提出すること。詳細は当庁と協議の上決定する。

障害対応

障害対応フロー・復旧手順を作成する。バックエンドの運用事業者等、他事業者との責任分界点や他事業者か関係する領域の対応フローは、他事業者や当庁と協議の上決定する。障害が発生した際は障害対応フロー・復旧手順に従い復旧作業を行う。

BCP 対応

災害対応フロー・BCP 出動手順を作成し、災害が発生した際には BCP を出動させる。

運用業務の実施・提供時間

運用業務に係る業務時間は、平日（土日及び祝日、毎年 12 月 29 日から 1 月 3 日を除く日）の 9 時から 18 時までとする。なお、対応時間帯外において緊急性の高い作業（システムトラブル、障害対応等）が発生した場合、当庁と協議の上対応すること。

運用設計及び保守設計（基本設計）

受託者は、本システムを対象とする運用・保守項目について、整理し、運用設計書及び保守設計書等を作成し、当庁の了承を得ること。

また、受託者は、運用設計及び保守設計を行った上、情報システムの次期更改までの間に計画的に発生する作業（例：セキュリティパッチ、定期メンテ等）の内容、その想定される時期等を取りまとめた運用計画書及び保守計画書の案を作成し、当庁の確認を受けること。

運用設計及び保守設計（詳細設計）

上述の基本設計を踏まえ詳細な運用設計及び保守設計を行い、定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容（初動対応、障害切り分け、暫定対処、等）、情報セキュリティインシデントを認知した際の報告手順や対処手順等を取りまとめた運用・保守作業計画を作成し、当庁の確認を受けること。

受託者は、運用・保守作業計画書を踏まえ、定常時及び障害時において想定される運用体制、保守体制、実施手順等を取りまとめた運用・保守作業手順書（当該運用・保守作業手順書には運用・保守作業員が実作業レベルで利用するマニュアル等も含めること。）を作成し、当庁の確認を受けること。また、運用・保守作業計画書との整合性を確保しつつ、運用業務及び保守業務の管理方法や手順、遵守事項等について定めた運用・保守実施要領を作成すること。

バックアップ

運用・保守計画書、運用・保守手順書に従い、システムバックアップ、データバックアップを取得すること。バックアップの対象・頻度については、当庁と協議の上、決定すること。
なお、協議の上で決定したアーキテクチャ上、本事業で開発する範囲でデータを保持しない場合においては、データバックアップは対象外とする。

重点監視業務

リリース後の一定期間を重点監視期間として必要な体制を構築して監視を行う。対象期間や体制については当庁と協議の上、決定すること。

利用者の利用状況のデータ収集

当庁の指示に基づき、利用者の利用状況のデータを集計し、当庁担当職員に定期的に報告すること。当庁が設定する KGI/KPI を十分理解した上で、受託者からも提案すること。

定期進捗報告と業務実施結果報告書の作成

当庁の指示による作業内容、脆弱性への対応等、事業の状況を把握するための定期的な報告を行うこと。なお、報告内容・頻度及び報告様式については、当庁と協議の上、決定すること。

5. その他業務

上記以外で必要な業務があった場合に、当庁担当及び他事業者と協議し、当庁担当承諾の上、実施すること。

6. 受託者から他事業者への引継ぎ（引継渡し）について

受託者は、当庁及び他事業者等に対して、それぞれ以下の引継ぎ作業を実施すること。

引継資料の作成

受託者は、本事業の契約期間後も当庁もしくは他事業者にて円滑な開発業務が速やかに実施可能となるよう、必要な情報を本事業の作業の実施状況に応じて文書として準備するともに、回線の利用や機器の保守等の本事業で提供するサービスを継続して提供するために必要な引継ぎに係る作業を行うこと。

引継ぎ作業の実施

当庁及び他事業者等に対し、少なくとも以下の情報を引き継ぐこと。
また、本事業の事業者は以下を現行事業者等から引き継ぎを受けること。

- 設計内容及び設定パラメータ
- 運用業務手順
- 作業経緯
- 残存課題
- 本システムの技術要素
- コンプライアンス及びセキュリティ教育等の教材
- 運用保守の業務を通じて使用もしくは新たに作成されたデータ及びドキュメント（データには、チケット管理等で使用したツール及びそのデータを含む）

7. 成果物

納入成果物

納入成果物は、以下のとおりとする。開発業務で作成する成果物は対話により決定する。納入成果物の詳細及び編集方法並びに納入期限等は、この仕様書の定めのある他、当庁担当職員と受託者が別途協議の上決定するものとする。また、以下に含まれていない場合であっても、当庁担当職員及び受託者が必要と認める場合はこの限りでない。

※以下、括弧内は納期を示す。記載の無いものは当庁と協議し納期を決定する。

- プロジェクト計画書（契約締結後10営業日以内）
- UX デザイン実施方針取りまとめ報告書
- ユーザーリサーチ実施計画書
- ユーザーリサーチ結果報告書
- インスペクション実施計画書
- インスペクション結果報告書
- ユーザー要求事項取りまとめ報告書
- ユーザー要求達成案
- 画面デザイン・UI コンポーネント資料
- 画面設計書（デザインガイドライン）
- ユーザビリティテスト実施計画書
- ユーザビリティテスト実施報告書
- アクセシビリティテスト実施計画書
- アクセシビリティ対応チェックリスト（実施報告書）
- コンテンツフィジビリティテスト実施計画書
- コンテンツフィジビリティテスト実施報告書
- プロダクト要求仕様書（PRD）

- 基本設計書
- 詳細設計書
- テスト計画書
- 結合テスト結果報告書
- 総合テスト結果報告
- 脆弱性診断結果
- 欠陥報告書
- 利用者マニュアル・FAQ
- 本事業で改修したソースプログラム（事業期間終了時まで）
- 引継計画書（事業期間終了時まで）
- 運用保守計画書（事業期間終了時まで）
- 運用保守報告書（事業期間終了時まで）
- その他事業において作成した計画書、報告書等（事業期間終了時まで）
- 当事業で使用した各種ツールのライセンス（譲渡不可の場合は見読性のある export データ等）（事業期間終了時まで）

成果物の納品方法

納入成果物の納品方法は、以下のとおりとする。

- 成果物は、全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構わないものとする。
- 用字・用語・記述符号の表記については、「公用文作成の考え方（令和 4 年 1 月 7 日文化審議会建議）」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、日本産業規格（JIS）の規定を参考にすること。
- 成果物は電子データにより作成し、当庁が指定する保存場所に納品すること
- 電子データの納品については、Microsoft 社 Windows10 及び Apple 社 macOS で読込可能な形式で納品すること。また、ファイルは Office Open XML の docx 拡張子、xlsx 拡張子又は pptx 拡張子のファイル形式で作成すること。 ただし、左記ファイル形式で納品が困難な場合は、当庁と事前に協議の上、PDF のファイル形式で作成すること。
- 納品後、当庁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。
- 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、担当部署の承認を得ること。
- 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。
- 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等して、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。なお、対策ソフトウェアに関する情報（対策ソフトウェア名称、定義パターンバージョン、確認年月日）を記載したラベルを貼り付けること。

成果物の納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、当庁が納品場所を別途指示する場合はこの限りではない。

〒102-0094 東京都千代田区紀尾井町 1-3　東京ガーデンテラス紀尾井町 19 階、20 階 デジタル庁　国民向けサービスグループ　マイナポータル新フロントの改善 調達担当

作業の実施体制・方法

1. 作業実施体制

本事業の受託者は、本事業のプロジェクト体制を提示すること。当庁で想定している体制及び各メンバーに求める資格・要件については対話の中で協議するが、当庁に提案、協議の上、当該提案に基づき変更してもよい。なお、「3.1 総合調整業務」に係る責任者を本事業のプロジェクトマネージャとする。その他、作業要員の資格・要件については、次項「作業要員に求める資格等の要件」を参照するものとする。本要件についても対話の中で協議する。

作業開始後、作業要員の成果に疑義があると当庁担当職員が判断した場合、双方協議に諮る。その上で作業要員の交代が必要となった場合は、受託者は速やかに作業要員の交代に応じること。

2. 作業要員に求める資格等の要件案

(1) 下記一～三に該当しないこと

一　当該契約を締結する能力を有しない者

二　破産手続開始の決定を受けて復権を得ない者

三　暴力団員による不当な行為の防止等に関する法律（平成三年法律第七十七号）第三十二条第一項各号に掲げる者

(2) 本業務のプロジェクトマネージャは情報処理技術者試験制度の「プロジェクトマネージャ」試験の合格者、又はPMP（Project Management Professional）の有資格者、若しくはこれらと同等の技術水準を満たすことを業務経験等から証明できる者であること。

(3) デザイン業務に関する主担当者は、以下のア. イ. 及びウ. に示すいずれかの資格を有する、又はそれに相当する実務上の経験・実績・出版・講演等の実績有していること。また実務経験として、BtoC/BtoB のいずれにおけるシステム開発プロジェクトへの UX サービスの提供実績を有することと、既存の成果物の実例にて実績を証明すること。

ア. HCD-Net 認定　人間中心設計スペシャリスト

＊参照URL（https://www.hcdnet.org/certified/about/）

イ. HCD-Net 認定　人間中心設計専門家

＊参照URL（https://www.hcdnet.org/certified/about/）

ウ. 認定人間工学専門家

＊参照URL（https://www.ergonomics.jp/specialist.html）

(4) 本業務の UI デザイナーは、業務システムの UI デザイン経験、及び Material Design や Human Interface Guidelines 等の各 OS プラットフォームガイドラインを踏襲した UI デザインの経験 3 年以上、また迅速に良質な多くのワイヤーフレームや UI を作成するために Figma 等のプロトタイピングツールの十分な利用経験を業務経験等から証明できる者であること。

(5) 本業務の UX デザイナーは、ユーザビリティテストやインタビューの企画（目的設定、検証項目設定、プロトタイプ検討、評価指標の策定、被経験要件策定等）と実施の経験 10 回以上を業務経験等から証明できる者であること。

(6) 以下の OSS を用いたフロントエンド開発を主導した実務経験者を 1 名以上含めること。

（ア）TypeScript

（イ）Storybook

（ウ）React & Next.js / Vue.js & Nuxt.js

（エ）フロントエンド開発において以下の実務経験者を1名以上含めること。

（オ）フロントエンド刷新プロジェクトの経験

（カ）HTML と CSS を用いてデザイナーの意図した UI を構築した経験

（キ）ユーザの体験を意識した Web フロントエンドの設計・開発・運用経験

（ク）Web フロントエンドをゼロベースで設計・環境構築・実装・運用した経験

（ケ）パフォーマンス・セキュリティに配慮した設計経験

（コ）JIS や iOS/Android 各種プラットフォームのガイドラインを踏襲し実装した経験

（サ）読み上げ機能に配慮した HTML の設計経験

（シ）CI/CD ツールによるフロントエンドの自動テスト及び継続的デプロイ環境の構築経験

（ス）SEO に対する知識や、最新の技術的なリファレンスを適用できること

(6) 作業要員として常駐ではないが以下の知見を要する者に技術支援を求められる体制を構築すること

（ア）経済産業大臣認定「情報処理技術者（IT ストラテジスト）」の有資格者、若しくはこれらと同等の技術水準を満たすことを業務経験等から証明できる者を1名以上含めること。

（イ）経済産業大臣認定「情報処理技術者（システムアーキテクト）」の有資格者、若しくはこれらと同等の技術水準を満たすことを業務経験等から証明できる者を1名以上含めること。

（ウ）経済産業大臣認定「情報処理安全確保支援士」の有資格者、若しくはこれらと同等の技術

水準を満たすことを業務経験等から証明できる者を1名以上含めること。

（エ）International Information Systems Security Certification Consortium が認定を行っている情報セキュリティ・プロフェッショナル認定資格である「CISSP」の認定者、若しくはこれらと同等の技術水準を満たすことを業務経験等から証明できる者を 1 名以上含めること。

3. 作業場所

作業やデータの保管等は日本国内において行うものとし、本事業の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、受託者の責任において用意すること。また、必要に応じて担当職員が現地確認を実施することができるものとする。

4. 作業の管理に関する要領

受託者は、担当部署が承認した設計・開発計画書の作業体制、スケジュール、開発形態、開発手法、開発環境、開発ツール等に従い、記載された成果物を作成すること。その際、設計・開発実施要領に従い、コミュニケーション管理、体制管理、作業管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

作業の実施に当たっての遵守事項

1. 機密保持に関する事項

ア　当庁が開示した情報、契約履行過程で生じた納入成果物及び本作業の履行上知り得た一切の事項について、いかなる場合にもこれを当庁が開示することを認めていない第三者に開示又は漏えいしてはならないものとする。

イ　情報の開示を受けるにあたっては、開示する情報の内容、範囲、期限、開示を受けたものによる管理方法、使用後の措置を当庁と協議の上取り決めること。

ウ　情報の開示を受けるにあたっては、「機密保持体制表」を作成し、当庁の了承を得ること。

エ　本作業を実施する上で、開示を受けた情報、作成及び出力した一切の資料については、当庁の了承を得ずに本作業の作業場所以外に持ち出さないこと。

オ　上記の開示又は漏えい防止、当庁の了承を得ることについては、本作業の委託期間終了後も同様とする。

カ　当庁が提供する本作業に関連する文書等については、当庁と協議の上、決定した場所に保管し、原則として、契約期間終了時までに返却又は裁断・溶解等の処分を行うこと。

キ　本作業で作成したプログラム及びデータは事前に許可した機器やディレクトリのみに格納すること。

ク　本作業で作成したプログラム、データ及びその他本作業の履行上発生した納入成果物については、当庁の許可なしに、作業実施場所から外部に持ち出さないこと。

ケ　本作業で作成したプログラム、データ及びその他本作業の履行上発生した納入成果物については、当庁の許可なしに、外部からアクセスできる状態におかないこと。

コ　電子媒体によって運用するプログラム、データ及び文書等については、ウィルスチェックを実施すること。

サ　異なる業者間でのデータ等の授受は、原則として、当庁の了承を得ること。

2. 個人情報の取扱い

(1) 個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。以下同じ。）の取扱いに係る事項について当庁と協議の上決定し、書面にて提出すること。なお、以下の事項を記載すること。

(ア) 個人情報の取扱いに関する責任者が情報管理責任者と異なる場合には、個人情報の取扱いに関する責任者等の管理体制

(イ) 個人情報の管理状況の検査に関する事項（検査時期、検査項目、検査結果において問題があった場合の対応等）

(2) 本業務の作業を派遣労働者に行わせる場合は、労働者派遣契約書に秘密保持義務等個人情報の適正な取扱いに関する事項を明記し、作業実施前に教育を実施し、認識を徹底させること。なお、受託者はその旨を証明する書類を提出し、当庁の承認を得たうえで実施すること。

(3) 個人情報を複製する際には、事前に担当部署の承認を得ること。なお、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元できないように破棄・消去を実施すること。なお、受託者は廃棄作業が適切に行われた事を確認し、その保証をすること。

(4) 受託者は、本業務を履行する上で個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大を防止等のため必要な措置を講ずるとともに、担当部署に事案が発生した旨、被害状況、復旧等の措置及び本人への対応等について直ちに報告すること。

(5) 個人情報の取扱いにおいて適正な取扱いが行われなかった場合は、本業務の契約解除の措置を受けるものとする。

3. 遵守すべきガイドライン等

本作業の実施に当たっては、原則として以下の文書・ガイドラインに記載された事項を遵守すること。また、今後契約期間中に当該文書が改定された場合には、それに従うこととするが、より良い作業の進め方について提案がある場合には、担当職員に提案、協議の上、当該提案に基づき実施してもよい。

i. デジタル・ガバメント推進標準ガイドライン（2021 年（令和3年）9月 10 日デジタル社会推進会議幹事会決定）
https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_20210910.pdf

ii. 「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」(2019 年(令和元年)9 月 24 日内閣サイバーセキュリティセンター)
https://www.nisc.go.jp/active/general/pdf/SBD_manual.pdf

iii. 政府機関の情報セキュリティ対策のための統一基準群
イ 政府機関の情報セキュリティ対策のための統一規範(令和3年7月7日サイバーセキュリティ戦略本部決定)
https://www.nisc.go.jp/active/general/pdf/kihanr3.pdf
ロ 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(令和3年7月7日サイバーセキュリティ戦略本部決定)
https://www.nisc.go.jp/active/general/pdf/shishinr3.pdf
ハ 政府機関等の情報セキュリティ対策のための統一基準(令和3年度版)(令和3年7月7日サイバーセキュリティ戦略本部決定)
https://www.nisc.go.jp/active/general/pdf/kijyunr3.pdf
ニ 政府機関等の対策基準策定のためのガイドライン(令和3年度版)(令和3年7月7日サイバーセキュリティ戦略本部決定)
https://www.nisc.go.jp/active/general/pdf/guider3.pdf

iv. サイバーセキュリティ 2021(2021 年(令和3年)9月 27 日サイバーセキュリティ戦略本部)
https://www.nisc.go.jp/active/kihon/pdf/cs2021.pdf

v. デジタル庁情報セキュリティポリシー
デジタル庁情報セキュリティポリシーは非公表であるが、「(3) ロ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(令和3年7月7日サイバーセキュリティ戦略本部決定)」に準拠している。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。

vi. 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(2021 年(令和3年)3月 30 日各府省情報化統括責任者(CIO)連絡会議決定)
https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20210330kihon.pdf

vii. その他、開発等にあたっては以下文書・ガイドラインを参照・準拠すること。

viii. 独立行政法人 情報処理推進機構セキュリティセンターの定める安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

ix. OWASP (Open Web Application Security Project®)

https://owasp.org/

4. その他文書、標準への準拠

(1) 遵守すべき法令等

本調達における遵守すべき法令等の対応について以下に示す。

ⅰ 受託者は、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律（平成 11 年 8 月 13 日法律第 128 号）等の関係法規を遵守すること。

ⅱ 受託者は、個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）及び受託者が定めた個人情報保護に関するガイドライン等を遵守し、個人情報を適正に取り扱うこと。

(2) プロジェクト計画書等

本業務の遂行に当たっては、担当部署が定めるプロジェクト計画書及びプロジェクト管理要領との整合を確保して行うこと。

(3) アプリケーション・コンテンツの作成規程

(ア) 提供するアプリケーション・コンテンツに不正プログラムを含めないこと。

(イ) 提供するアプリケーションにぜい弱性を含めないこと。

(ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

(エ) 電子証明書を利用する等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

(オ) 提供するアプリケーション・コンテンツの利用時に、ぜい弱性が存在するバージョンのOSやソフトウェア等の利用を強制する等の情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

(カ) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供される等の機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

(キ)「.go.jp」で終わるドメインを使用してアプリケーション・コンテンツを提供すること。

5. 情報システム監査

本事業において整備又は管理を行う情報システムに伴うリスクとその対応状況を客観的に評価するために、当庁が情報システム監査の実施を必要と判断した場合は、当庁が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報システム監査を受託者は受け入れること（当庁が別途選定した事業者による監査を含む）。

情報システム監査で問題点の指摘又は改善案の提示を受けた場合には、対応案を担当部署と協議し、指示された期間までに是正を図ること。

6. セキュリティ要件

本プロジェクトでは、受託者に提供、貸与若しくは閲覧を許可したすべての情報並びにそれらの情報を基に作成する成果物（中間成果物を含む。）及び関連資料を情報セキュリティ管理の対象とする。これらの情報は全てプロジェクト外秘とし、外部の人間への情報漏洩、改ざん、毀損が発生しないよう管理するとともに、そうした事象が発生していないことを確認できることが肝要である。これらを踏まえて情報セキュリティ管理について提案すること。

記載にあたっては、前述した「機密保持に関する事項」及び「個人情報の保護に関する事項」を参照の上、必要な体制、プロセス、ツール等を提案すること。また、本事業の実施に当たっては、別添 14「情報セキュリティに関する事項」を遵守すること。

成果物の取扱いに関する事項

1. 知的財産権の帰属

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、受託者が本事業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、全てデジタル庁に帰属するものとする。

(1) デジタル庁は、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、受託者は、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、複製等によりデジタル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。

(2) 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、受託者は、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、本業務の受託者は、当該既存著作物の内容について事前にデジタル庁の承認を得ることとし、デジタル庁は、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デジタル庁の責めに帰す場合を除き、受託者の責任及び負担において一切を処理すること。この場合デジタル庁は係る紛争等の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力措置を講じるものとする。

(3) 本件プログラムに関する権利（著作権法第 21 条から第 28 条に定める全ての権利を含む。）及び成果物の所有権は、デジタル庁から受託者に対価が完済されたとき受託者からデジタル庁に移転するものとする。
(4) 受託者はデジタル庁に対し、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。
(5) 受託者は使用する画像、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。

2. 契約不適合責任に関する事項

(1) 委託業務が完了した後でも、その成果物もしくは役務行為の成果が種類、品質又は数量に関して本契約の内容に適合しない（以下、「契約不適合」という。）ときは、受託者に対して相当の期間を定めて催告し、その契約不適合の履行の追完をさせることができる。ただしフロント UI 開発において実現する機能の数量に関してはこの限りではなく、「3. 善管注意義務に関する事項」を遵守するものとする。
(2) 前項の規定により種類又は品質に関する契約不適合に関し履行の追完を請求するにはその契約不適合の事実を知った時から１年以内に受託者に通知することを要する。ただし、受託者が、本委託業務の成果物もしくは役務行為の成果を委託者に引き渡した時において、その契約不適合を知り、又は重大な過失によって知らなかったときは、この限りでない。
(3) 受託者は、本委託業務の成果物もしくは役務の成果について、契約不適合のある場合、速やかに、履行を追完すること。
(4) 前項の規定により、追完を行うときには、不適合の原因と追完の方法、追完を行った場合の影響について当庁に提示し、了承を得ること。
(5) 受託者は、当庁が了承した計画にもとづいて、調査及び必要な修補又は履行の追完を実施するとともに設計書、マニュアル等の関連する納入成果物も併せて修正の上、提出すること。
(6) 受託者が第１項の期間内に履行の追完をしないときは、委託者は、受託者の負担にて第三者に履行の追完をさせ、又は契約不適合の程度に応じて受託者に対する対価の減額を請求することができる。ただし、履行の追完が不能であるとき、受託者が履行の追完を拒絶する意思を明確に表示したとき、本契約の履行期限内に履行の追完がなされず本契約の目的を達することができないとき、そのほか委託者が第１項の催告をしても履行の追完を受ける見込みがないことが明らかであるときは、委託者は、受託者に対し、第１項の催告をすることなく、委託者の負担において直ちに第三者に履行の追完をさせ、又は対価の減額を請求することができる。

3. 善管注意義務に関する事項

(1) 受託者は、契約の履行に関して、本契約の目的に従い、善良な管理者の注意をもって本業務を行う義務を負うものとする。

(2) 受託者は、業務の進捗が適切に管理できるよう、必要なマネジメントを行う義務を負うものとする。

(3) 検収

(ア) 本業務の受託者は、成果物等について、納品期日までにデジタル庁に内容の説明を実施して検収を受けること。

(イ) 検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点についてデジタル庁に説明を行った上で、指定された日時までに再度納品すること。

(4) 複数事業者による共同入札

(ア) 複数の事業者が共同入札する場合、その中から全体の意思決定、運営管理等に責任を持つ共同入札の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。

(イ) 共同入札を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の契約不適合責任に関しても協定の内容に含めること。

(ウ) 共同入札を構成する全ての事業者は、本入札への単独提案又は他の共同入札への参加を行っていないこと。

(エ) 共同入札を構成する全ての事業者は、公的な資格や認証等の取得を除く全ての応札条件を満たすこと。

(5) 履行可能性審査に関する要件

本業務及び情報セキュリティ管理の履行可能性を証明するため、業務計画書作成時に以下の 2 点に留意すること。なお、提出された業務計画書において履行可能性を認めることができないとデジタル庁が判断した場合は、入札に参加することができない。

- スケジュール、作業内容及び工数の実行実現性を記載すること
- 別添 14「情報セキュリティに関する事項」を遵守すること。

再委託に関する事項

受託者は、事業全体の企画及び立案並びに根幹に関わる執行管理について、再委託（委託業務の一部を第三者に委託することをいい、請負その他委託の形式を問わない。以下同じ。）を行わないこと。

また、再委託を行う場合には、その合理的理由と再委託先の業務履行能力について記載した再委託承認申請書を作成し、当庁に提出しなければならない。

再委託先の契約違反等

再委託先において、本調達仕様書の遵守事項に定める事項に関する義務違反又は義務を怠った場合には、受託者が一切の責任を負うとともに、デジタル庁は、当該再委託先への再委託の中止を請求することができる。

その他特記事項

1. 前提条件等

本業務受注後に調達仕様書（別添資料を含む。）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デジタル庁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、納期に影響を及ぼさない）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。

2. 公告期間中等の資料閲覧等

入札予定者は、本業務内容を適切に把握するため、提案書・入札書提出前に、別添 14「情報セキュリティに関する事項」に記載の「デジタル庁情報セキュリティポリシー（2021 年（令和３年）９月１日デジタル監決定）」及び情報提供等記録開示システム設計書、非機能要件定義書、外部システムインターフェース仕様書等のドキュメント類の閲覧を希望する場合には、front-service-lg@digital.go.jp にその旨を連絡の上、後日、担当職員から返信される電子メールの指示に従い閲覧すること。

別添 14

情報セキュリティに関する事項

以下の事項について遵守すること。

1)　受託者は、契約締結後速やかに、情報セキュリティを確保するための体制を定めたものを含み、以下に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、デジタル庁（以下「当庁」という。）の担当職員（以下「担当職員」という。）に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について担当職員に提示し了承を得た上で提出したときは、この限りでない。また、契約期間中に、担当職員の要請により、情報セキュリティを確保するための体制等及び対策に係る実施状況を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に担当職員へ案を提出し、同意を得ること。

　なお、報告の内容について、担当職員と受託者が協議し不十分であると認めた場合、受託者は、速やかに担当職員と協議し対策を講ずること。

2）受託者は、本事業に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本事業にかかわる従事者に対し実施すること。

3）受託者は、本事業遂行中に得た本事業に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、当庁内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得ること。なお、この場合であっても、担当職員の許可なく複製してはならない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明すること。

4）受託者は、本事業遂行中に得た本事業に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく当庁外で複製してはならない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。

5）受託者は、本事業を終了又は契約解除する場合には、受託者において本事業遂行中に得た本事業に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却又は廃棄若しくは消去すること。その際、担当職員の確認を必ず受けること。

6）受託者は、契約期間中及び契約終了後においても、本事業に関して知り得た当庁の業務上の内容に

ついて、他に漏らし又は他の目的に利用してはならない。ただし、担当職員の承認を得た場合は、この限りではない。

7）受託者は、本作業の遂行において、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の対処方法について担当職員に提示すること。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ことを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。

8）受託者は、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（「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」、「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」、「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」及び「政府機関等の対策基準策定のためのガイドライン」の総称）（以下、これらを総称して「統一基準群」という。）及び「デジタル庁情報セキュリティポリシー（2021 年（令和３年）９月１日デジタル監決定）」を踏まえた情報セキュリティ対策を実施する。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

9）受託者は、当庁又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行うこと 。

10）受託者は、外部公開ウェブサイト（以下「ウェブサイト」という。）を構築又は運用するプラットフォームとして、受託者自身（再委託（事業の一部を第三者に委託することをいい、外注及び請負を含む。以下同じ。）先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。また、ウェブサイト構築時においてはサービス開始前に、運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。

11）受託者は、ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に基づくこと。また、構築又は改修したウェブアプリケーションのサービス開始前に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施すること。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出すること。なお、チェックリストの結果に基づき、担当職員から指示があった場合は、それに従うこと。

12）受託者は、ウェブサイトを構築又は運用する場合には、インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、

TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。
なお、必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。

13）受託者は、ウェブサイト又は電子メール送受信機能を含むシステムを構築又は運用する場合には、原則、政府機関のドメインであることが保証されるドメイン名「.go.jp」（以下「政府ドメイン名」という。）を使用すること。なお、政府ドメイン名を使用しない場合には、第三者による悪用等を防止するため、事業完了後、一定期間ドメイン名の使用権を保持すること。

14）受託者は、情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施すること。

①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管理が、一貫した品質保証体制の下でなされていること。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。

②情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当庁と連携して原因を調査し、排除するための手順及び体制を整備していること。それらが妥当であることを証明するため書類を提出すること。

③不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。

④情報セキュリティ対策による情報システムの変更内容について、担当職員に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容を含めること。

⑤サポート期限が切れた又は本事業の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わない及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。

⑥電子メール送受信機能を含む場合には、ＳＰＦ（Sender Policy Framework）等のなりすましの防止策を講ずるとともにSMTPによるサーバ間通信のTLS（SSL）化やS/MIME等の電子メールにおける暗号化及び電子署名等により保護すること。

⑦製品選定の際には、別紙5「クラウドサービス_ISMAP管理策基準」を全て遵守すること（ISMAP登録製品の選定等）。ただし実施業務や取扱う情報等の特性を踏まえて、適用困難なISMAP管理策基

準がある場合は、適用除外根拠を合理的に説明し当庁と協議を行い、承認を得ること。

15) 受託者は、本事業に従事する者を限定すること。また、受託者の資本関係・役員の情報、本事業の実施場所、本事業の全ての従事者の所属、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を担当職員に提示すること。なお、本事業の実施期間中に従事者を変更等する場合は、事前にこれらの情報を担当職員に再提示すること。

16) 受託者は、本事業を実施するに当たり、約款による外部サービスやソーシャルメディアサービスを利用する場合には、それらサービスで要機密情報を扱わないことや不正アクセス対策を実施する等規程等を遵守すること。

17) 受託者は、ウェブサイトの構築又はアプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行うこと。

①提供するウェブサイト又はアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。

（a）ウェブサイト又はアプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

（b）アプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。

（c）提供するウェブサイト又はアプリケーション・コンテンツにおいて、デジタル庁外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させる等して確認すること。

②提供するウェブサイト又はアプリケーションが脆弱性を含まないこと。

③実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。

④電子証明書を用いた署名等、提供するウェブサイト又はアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをウェブサイト又はアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

⑤提供するウェブサイト又はアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳやソフトウェア等の利用を強制する等の情報セキュリティ水準を低下させる設定変更を、ＯＳやソフトウェア等の利用者に要求することがないよう、ウェブサイト又はアプリケーション・コンテンツの提供方式を定めて開発すること。

⑥デジタル庁外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供される等の機能がウェブサイト又はアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をウェブサイト又

はアプリケーション・コンテンツに組み込む場合は、デジタル庁外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該ウェブサイト又はアプリケーション・コンテンツに掲載すること。

18) 受託者は、本事業を再委託する場合は、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、上記 1)～17)の措置の実施を契約等により再委託先に担保させること。また、1)の確認書類には再委託先に係るものも含むこと。