デジタル人材育成・DX 推進エコシステムにおける
プラットフォーム構築業務

調達仕様書

独立行政法人**情報処理推進機構**

1. 調達案件の概要

1.1. 調達件名

デジタル人材育成・DX 推進エコシステムにおけるプラットフォーム構築業務（以下、「本業務」という。）

1.2. 調達の背景

日本の国際競争力は長期低落傾向にあり、企業における DX 推進は進みつつも人材面の課題が浮き彫りになっている。人への投資、需給ギャップ、スキルと評価処遇のアンマッチなど課題は山積している。

日本においても、体系的なデジタル人材育成施策を実施しているが、生成 AI 時代において「技術進化のスピードにあわせて、変化をいとわず学び続けること」が一層重要となり、デジタル技術の継続的な学びを可能とするシステムが必要となっている。継続しているデジタル人材不足対応や労働市場の構造的な現状の課題を打破し、企業活動の基盤となる人材供給を達成するためには、（内部・外部問わず）労働市場でスキルベースでの継続的学びが可能となり、スキルに基づいて評価される環境づくりが必要不可欠である。

なお、「新しい資本主義のグランドデザイン及び実行計画 2024 年改訂版」においても、「個人のデジタルスキル情報の蓄積・可視化を通じてデジタル技術についての継続的な学びを実現する」と謳われている。

1.3. 調達目的および期待する効果

産業界、個社、政府等の取組を俯瞰的に運営しながら、様々なデータの収集と活用を通じてデジタル人材育成を効率的に支援するために DX 推進・デジタル人材育成の共通基盤を構築する。共通基盤のみならず、独立行政法人 情報処理推進機構（以下、「機構」という。）自身が、DX 推進・デジタル人材育成のサービサーとなって、DX 推進・デジタル人材育成のエコシステムを実現することを目指す。

無論、機構の既存サービスである情報処理技術者試験、マナビ DX などを包含しエコシステムと一体化することも念頭に置いている。

これら取組を通じて、「産業構造の変化に合わせた人材の適材化・適所化に貢献」し、機構が産学官の多様な人材をつなぎ、最先端の知が集まる組織となる、デジタル人材育成/DX の Center of Excellence（＝知が集う場）となることを目指す。

機構では、1.2.項に示す背景のもと、個人のスキル情報を蓄積・可視化する情報基盤を構築、デジタル技術の継続的な学びを実現し、スキルが共通言語として広く労働市場で活用され、自律的なキャリア形成が図られるエコシステムの基盤となる情報システムを「デジタル人材育成・DX 推進エコシステムにおけるプラットフォーム（以下、「本プラットフォーム」と記載）」として整備、構築することにより以下の効果を期待している。

- 外部の個人ユーザーには、スキル情報の蓄積・可視化を通じて、継続的な学びと目的をもったキャリア形成実現を支援する
- 外部の企業ユーザーには、他社や労働市場との対話を通じてスキル標準に基づくデジタル人材を戦略的に育成・確保する

- 学習サービス事業者には、ユーザーや業界との対話を通じてデジタルスキル標準に基づくリスキリング市場を拡大する
- アカデミアには、AI 時代の学びの最適化を支援する

1.4. 業務・情報システムの概要

当機構では、本プラットフォームの構築に向け、要件定義を 2025 年 2 月から 7 月に行ったところである。本業務では、当機構にて行った要件定義にもとづき、本プラットフォーム構築の設計・開発を行う。

業務の概要は、「別紙 1 要件定義書」の「1. 業務要件定義」に記載のとおりである。

1.5. 契約期間

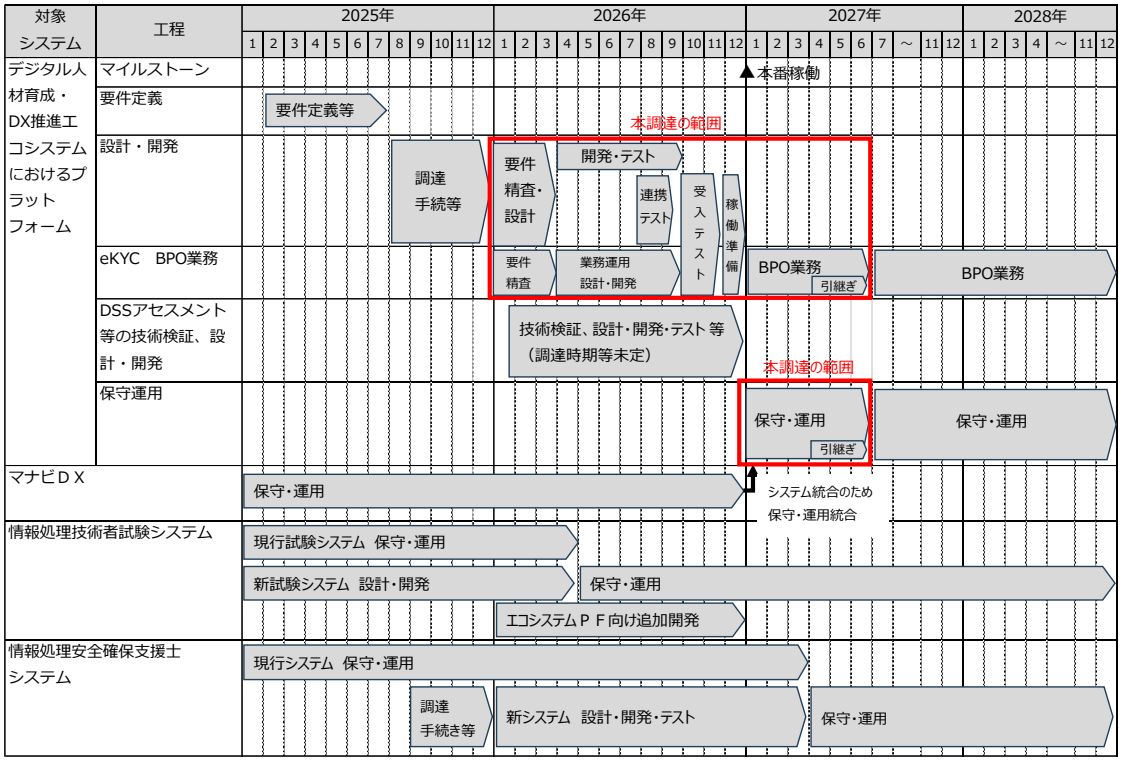
契約開始日から 2027 年 6 月 30 日まで

1.6. 作業スケジュール

作業スケジュールは、下図のとおりである。スケジュールの赤枠で囲った範囲が本調達を示す。本作業スケジュールは、現時点での想定を記載しているものであり、作業スケジュールの詳細については受託者の提案内容を踏まえ、当機構と受託者にて協議のうえ、決定する。

なお、本システムは、2026 年 12 月末に移行を行い、2027 年の 1 月 4 日の稼働を想定している。移行時期・稼働日の決定については、移行スケジュールを計画のうえ、当機構へ提案し協議のうえ決定すること。

図 1 作業スケジュール



2. 調達案件及び関連調達案件の調達単位、調達の方式等

2.1. 調達範囲

本調達は、本プラットフォームの設計開発業務および保守・運用業務であり、調達の対象業務範囲は、本プラットフォームのシステム設計開発、システム運用保守、eKYC による本人確認業務である。デジタルスキル標準のアセスメント開発業務については、本調達の範囲外とし、別調達にて行う。

なお、上記は調達範囲の基本方針である。調達範囲の調整が必要となった場合には、当機構と協議の上、決定すること。

2.2. 調達案件の一覧

調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期等は下表のとおりである。

表 1 関連する調達案件の一覧

項番	調達案件名	調達の方式	契約締結日	意見招請 入札公告 落札者決定時期 等	契約期間
1	デジタル人材育成・DX 推進エコシステムにおけるプラットフォーム構築の要件定義等に係る支援業務	一般競争入札 （総合評価）	2025 年 2 月 26 日	・公示 2024 年 11 月 29 日 ・事業者決定 2025 年 1 月 27 日	2025 年 2 月から 2025 年 7 月まで
2	デジタル人材育成・DX 推進エコシステムにおけるプラットフォーム構築業務 （本調達）	一般競争入札 （総合評価）	2025 年 12 月 26 日 （予定）	・公示 2025 年 10 月 3 日 （予定） ・事業者決定 2025 年 12 月 17 日 （予定）	2025 年 12 月から 2027 年 6 月まで
3	デジタル人材育成・DX 推進エコシステムにおけるデジタルスキル標準アセスメント等の技術検証、設計・開発業務	一般競争入札 （総合評価）	2026 年 1 月 （予定）	・公示 2025 年 11 月 （予定） ・事業者決定 2026 年 1 月 （予定）	2026 年 1 月から 2027 年 1 月まで

2.3. 調達案件間の入札制限

相互けん制の観点から、「表 1 関連する調達案件の一覧」項番 1 に挙げる業務の受託者は、項番 2 の本調達の業務への入札を制限する。

2.4. 当機構が調達する機器、ソフトウェア、サービスの一覧

本プラットフォームで利用するガバメントクラウドについては、本業務の契約中に当機構にて調達を行い、2026 年 4 月以降に利用開始できるようにする予定である。

3. 情報システムに求める要件

設計・開発の実施に当たっては、「別紙１　要件定義書」の各要件を満たすこと。「別紙１　要件定義書」は、あくまで、現状の想定を記載したものであることに留意し、受託者にて本システムにおいて最適な機能を設計すること。

4. 作業の実施内容に関する事項

本業務は、2025 年 2 月から 7 月に実施した「デジタル人材育成・DX 推進エコシステムにおけるプラットフォーム構築の要件定義等に係る支援業務」の検討結果を踏まえて実施すること。

本業務の結果、基本設計書・詳細設計書の記載内容に変更が生じる場合は、その都度基本設計書・詳細設計書を修正する。修正に関しては当機構のレビューを受けた上で、当機構の承認を得ること。

4.1. プロジェクト計画書等の作成

(1) プロジェクト計画書及び設計・開発実施要領

プロジェクト計画書及び設計・開発実施要領を作成し、当機構の承認を得ること。

プロジェクト計画書及び設計・開発実施要領は各工程での検討結果等を踏まえて必要に応じて詳細化・更新し、当機構の承認を得ること。

設計・開発・テスト等に際しては、関連する事業者やシステム側への依頼・連携が必要であるため、その内容や役割分担を記載すること。

(2) 標準ガイドライン遵守

作業実施に当たり、「デジタル・ガバメント推進標準ガイドライン」（令和 6 年 5 月 31 日デジタル社会推進会議幹事会決定。以下「標準ガイドライン」という。）の内容を遵守すること。契約期間中に標準ガイドラインが改定された場合は最新の版を参照し、当機構と協議の上、対応について決定すること。

受託者が作成する「プロジェクト計画書（案）」には、標準ガイドライン 第 3 編第 7 章 1.「1）設計・開発実施計画書の記載内容」に基づき、次に掲げる事項を含めること。

- 作業概要
- 作業体制
- スケジュール
- 成果物
- 開発形態、開発手法、開発環境、開発ツール等
- その他（前提条件・制約条件）

受託者が作成する「設計・開発実施要領（案）」には、標準ガイドライン 第 3 編第 7 章 1.「2）設計・開発実施要領の記載内容」に基づき、次に掲げる事項を含めること。

- コミュニケーション管理
- 体制管理
- 工程管理
- 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

本業務において作成する成果物、提出物は、成果物に係る納品期限によらず、作業進捗に応じた適切なタイミングで当機構に提出すること。

提出した内容に変更があった場合は、変更の事由が生じた都度、再度提出し、当機構の承認を得ること。

(3) プロジェクト管理の実施及び報告

ア　プロジェクト管理の実施

次のとおりプロジェクト管理を行うこと。

・　進捗管理

実施すべき全ての作業は具体的に進捗状況を把握できる単位まで詳細化し、階層構造で表したもの（WBS）及び定量的に状況が把握できる手法にて進捗管理を行うこと。進捗状況は進捗会議等で定期的に報告すること。

具体的な進捗管理方法は、プロジェクト計画書の策定時点で、プロジェクトの特性に合わせて当機構と協議の上決定すること。

受託者と当機構間でプロジェクト管理ツール等を共有する提案についても、妨げない。費用は原則として受託者の負担とするが、当該ツールのライセンス等を当機構が保有する場合はその限りではない。利用する各種管理ツールの詳細は契約後協議の上、決定する。なお、クラウドサービスの管理ツールを利用する場合は、要件定義書 3.2.(2)記載の要件を満たしたクラウドサービスとすること。

・　課題管理

解決するべき課題・問題は、再発防止に生かすことも含めて、項目ごとに進捗等を管理し、適切に解決していくこと。

・　リスク管理

リスクの洗い出しを行い、リスク内容を判別した上で、各リスクの発生頻度、影響度、対応策（低減、受容、転換、回避等）、責任等を、監視・管理すること。

・　情報セキュリティ対策

「6.作業の実施に当たっての遵守事項」の要件を満たすように実施すること。

・　品質管理

品質管理について、次の事項を明確にし、実施すること。

➢　品質管理方針

事前に各工程において品質目標及び工程完了基準を設定すること。

成果物に対して適切な検証活動を実施の上、結果について分析を行うこと。

分析結果から抽出した対策の立案と実施を行うこと。

➢　品質管理方法

各工程の完了に伴いレビューを実施し、品質基準との差を把握すること。

品質の自己評価を実施し、当機構の承認を得ること。

・　変更管理/構成管理

構成管理/変更管理について、管理手順を明確に記載すること。

当機構と合意した最新の状況を適時に各種ドキュメントへ反映すること。

設計書等のドキュメントとソースコード等の実装結果に差分が発生しないよう管理を行うこと。

・　問合せ管理

業務を遂行する中で、当機構から受託者に対する指摘や確認事項等について、適切に管理し、着実に対応すること。

イ　作業進捗の報告等

作業の推進方法、方針の確認、修正及び進捗状況確認等、作業進捗の報告で必要な書類を作成し、週 1 回程度の報告を行うこと。報告は原則としてオンライン会議での実施とするが、当機構から要請があった場合、又は、受託者が必要と判断した場合は、当機構と受託者で協議の上、対面で開催すること。また、別途当機構が報告を求める場合においては、当機構が指示する必要な書類を加えること。詳細は設計・開発実施要領の作成時に当機構と協議の上、決定すること。なお、報告にはプロジェクト全体管理者が出席すること。また、当機構が求める場合は、必要に応じて体制に参画しているメンバー（セキュリティ要員や UI/UX 要員など）を参加させること。

4.2. 作業管理

(1) 設計・開発工程の作業管理

受託者は、当機構が承認したプロジェクト計画書及び設計・開発実施要領に従い、各種管理を行うこと。

(2) コミュニケーション方法

コミュニケーションツールを活用し、継続性の高い開発体制を構築すること。当機構とのコミュニケーション、情報共有についてもコミュニケーションツールを活用すること。ただし、当機構が保有するライセンスで利用可能なコミュニケーションツールは Slack 又は Microsoft Teams である。これ以外のコミュニケーションツールを利用する場合には、当機構職員が利用するライセンスを受託者が提供すること。

4.3. 要件の精査

受託者は、設計・開発の実施に先立ち、「別紙 1　要件定義書」の内容の確認・精査を行うこと。要件の調整内容は、当機構及び関係するステークホルダーに提示し、合意形成を図りつつ進めること。また、要件の精査結果や業務フローをドキュメント化し、成果物として作成すること。

4.4. 設計

(1) 基本的な要件

ア　基本設計及び詳細設計

受託者は、要件定義書の要件を満たすための基本設計及び詳細設計（運用設計を含む。）を行い、成果物について当機構からの承認を得ること。

当機構やシステム関係事業者等の第三者が理解可能となるよう、特に用語の定義や表記ゆれに注意した上で、各種資料及び成果物を分かりやすく作成すること。

イ　外部インタフェース仕様書の作成

受託者は、他の情報システムとの連携を行うための外部インタフェース仕様書を作成すること。

また、連携先の情報システム関係者等が外部連携について正確に把握でき、連携機能の構築や連携テスト等の実施を円滑に行えるような外部インタフェース仕様書を作成すること。

ウ　本プラットフォームにて利用する環境

受託者は、設計・開発に用いる環境として、クラウドサービス上に構築する「本番環境」、「検証環境」及び「開発環境」の 3 種類を構築すること。

設計・開発に用いる環境は、原則として「検証環境」及び「開発環境」とし、システム稼働に当たってのアプリケーションプログラムリリースは本番環境で行うこと。

システム稼働後にインシデントが発生し、本番環境と同等の環境で動作確認が必要な場合は、検証環境で行うこと。システム稼働後にアプリケーションプログラム改修が必要な場合は主に開発環境で行うこと。

また、ソースコードの変更履歴およびバージョンを適切に管理するため、リポジトリ管理ツールを用いたリポジトリ環境を構築すること。リポジトリ管理ツールの選定・運用にあたっては、将来的なシステムの拡張及び更新や事業者間での引継ぎの妨げにならないようベンダーロックインとなる受託者の独自製品を避けたソフトウェアを選定し、当機構の承認を得ること。

エ　ライフサイクルコストの考慮

受託者は、本プラットフォームの設計・開発から運用終了に至るまでの保守性を考慮して、基本設計及び詳細設計を実施すること。

オ　クラウドネイティブなシステム構成

アプリケーションプログラムの設計・開発にあたっては、可能な限りクラウドネイティブなシステム構成を志向すること。また、Infrastructure as Code（IaC）を活用するなど、クラウドサービスの構成変更を効率的に実施できるよう配慮すること。

カ　モニタリングが容易に行える構成

システム運用に必要な情報等に対して、システムで適時に状況を取得できる構成とすること。また、統計処理等によって二次的に加工した情報だけでなく、その根拠となる一次情報（ローデータ）も確認できる構成とすること。

(2) 基本設計及び詳細設計の実施（アプリケーションプログラム）

ア　アプリケーションプログラムの基本設計

アプリケーションプログラムについて、システム全体図、データの流れと機能構成、機能・画面・帳票一覧、画面遷移、データ一覧等の基本設計を行うこと。

以上をもとに、基本設計書（アプリケーションプログラム）を取りまとめること。

イ　要件との網羅性

基本設計書（アプリケーションプログラム）には、要件と設計項目の対応表等、要件が網羅されていることを確認できる情報を含めること。

ウ　アプリケーションプログラムの詳細設計

アプリケーションプログラムについて、基本設計書（アプリケーションプログラム）に基づき、機能設計（機能定義、データチェック定義、アクセス制御方式等）、スキーマ定義、コード定義、ジョブネット定義等の詳細設計を行うこと。

以上をもとに、詳細設計書（アプリケーションプログラム）を取りまとめること。

エ　基本設計との網羅性

詳細設計書（アプリケーションプログラム）には、基本設計書（アプリケーションプログラム）の項目との対応表等、基本設計の内容が網羅されていることを確認できる情報を含めること。

オ　パラメータ設計

受託者は、アプリケーションの動作の前提となるソフトウェア（パッケージ製品）を選定し、パラメータ等の必要な設計を実施すること。

(3) 基本設計及び詳細設計の実施（運用・保守）

ア　運用・保守計画

受託者は、要件定義書の「3.16 運用に関する事項 (1) 運用・保守計画」に示す内容をもとに運用・保守計画書及び運用・保守実施要領の案を作成し、当機構の承認を受けること。

なお、運用・保守計画書の案には、以下の内容を含めること。

- 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内容
- 上記作業の発生が想定される時期等
- 作業実施に必要な資料
- モニタリングすべきデータ・リソース
- 使用する運用管理機能・ツール
- 各作業の完了条件
- 運用・保守実績を記録する成果物等

イ　運用・保守設計

受託者は、「ア 運用・保守計画」に記載された事項や、要件定義書の「3.16 運用に関する事項」、「3.17 保守に関する事項」に記載の運用・保守に関する要件を踏まえ、運用設計及び保守設計を行い、当機構の承認を受けること。

運用・保守設計に当たっては、当機構作業の軽減等、効率的なシステム運用・保守に資する内容を検討すること。また、システム稼働後にインシデント数が削減される等、効率的なシステム運用・保守に資する改善案があれば提案すること。

- 定常時における定型的な作業内容、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、暫定対応、恒久対応など）
- 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、対応手順
- 障害発生等により設計書、ソースコード等の修正が発生した場合の報告手順、対応手順

ウ　必要経費（ランニングコスト）の算出

運用・保守設計を行う際には以下の内容を取りまとめたランニングコスト試算表を作成し、当機構の承認を得ること。

- 運用・保守段階において発生する各種コストに係る予実管理のための管理様式
- 運用・保守設計実施時点で判明している所要見込額
- 必要となるソフトウェアライセンス所要額及びクラウドサービス利用額

エ　運用業務の効率化の方策

自動化、セルフサービス化等による効率的なシステム運用・保守に資するシステム改修案があれば提案すること。

オ　運用・保守手順書

受託者は運用・保守計画書を踏まえ、以下を取りまとめた運用・保守手順書（当該運用・保守手順書には運用・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、当機構の承認を得ること。

- 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

また、当機構が提示する運用規程の要件に基づき運用規程の案を作成し、当機構の承認を得ること。

(4) 基本設計及び詳細設計の実施（システム方式）

ア　基本設計

「4.3.要件の精査」を行った後の要件定義書の要件に基づき、システム方式に関する基本設計結果を記載したものとして基本設計書（システム方式）を作成し、当機構の承認を得ること。基本設計書（システム方式）には以下の内容を含むこと。

- 非機能要件（信頼性、性能、拡張性、運用・保守、セキュリティ等）を実現するための設計
- システム設計（システム環境、ネットワーク、設備・運用）
- 業務継続設計（システムバックアップ、データバックアップ、障害発生時の縮退運転や自動継続運転、大規模災害対策拠点・環境）等

イ　詳細設計

基本設計書（システム方式）を踏まえ、システム方式に関する詳細設計結果を記載したものとして詳細設計書（システム方式）を作成し、当機構の承認を得ること。詳細設計書（システム方式）には以下の内容を含むこと。

- 非機能要件（信頼性、性能、拡張性、運用・保守、セキュリティ等）を実現するための設計
- システム設計（システム環境、ネットワーク、設備・運用）
- 業務継続設計（システムバックアップ、データバックアップ、障害発生時の縮退運転や自動継続運転、大規模災害対策拠点・環境）等

ウ　環境定義

以下の環境定義に係る作業を行うこと。

- 構築作業全般のスケジュール、手順、要領等も必要に応じて記載すること。また、クラウドサービスプロバイダーが提供する稼動環境（本番環境・検証環境等）のセットアップ後に、稼働環境が想定どおりに構築できていることを確認するためのテスト・確認項目を記載したものとして、動作確認テスト項目表及び持込み機器疎通確認項目表を作成すること。
- 詳細設計書等をもとに、クラウドサービスプロバイダーが提供する資源（OS、ミドルウェア）や本プラットフォームが個別に配置し、独自に設計・実装して利用するソフトウェア（以下、「持込みソフトウェア」という。）の環境パラメータを取りまとめたものとして環境定義書を作成すること。
- 受託者は、基盤構築の結果、環境定義書の内容に修正が発生した場合は、環境定義書も修正すること。
- 持込みソフトウェアのセットアップを行うための手順を記載したものとして環境構築手順書を作成すること。
- 構築するシステム稼働環境について、クラウドサービス、機器、ソフトウェア等を一覧表で取りまとめたものとして機器、ソフトウェア等の一覧表を作成すること。

(5) 移行計画

受託者は、情報システムの環境、ツール、手順等を記載した移行計画書を作成し、当機構の承認を受けること。

4.5. **開発・テスト**

(1) ルールの規定

受託者は、開発に当たり、アプリケーションプログラムの開発又は保守を効率的に実施するため、プログラミング等のルールを定めた標準（標準コーディング規約、セキュアコーディング規約等）を定め、当機構の承認を得ること。

(2) ルール遵守や成果物の確認方法

受託者は、開発に当たり、情報セキュリティ確保のためのルール遵守や成果物の確認方法（例えば、標準コーディング規約遵守の確認、ソースコードの検査、現場での抜き打ち調査等についての実施主体、手順、方法等）を定め、当機構の承認を得ること。

(3) 開発手法

本プロジェクトでは、開発手法は当機構から指定しないものとする。従来のウォーターフォールに限定せず、スパイラル／アジャイル等柔軟な対応を可能とする手法をプロジェクトの特性を踏まえ検討し、機能により最適な開発手法を提案の上、当機構と協議、決定すること。アジャイル開発手法を採用する場合、当機構が実際の業務フローをイメージできる形でのレビューをあらかじめ計画し、フィードバックを反映できる期間を設けること。いずれの方式であっても、機能として実装した仕様は、ドキュメント（チケット管理システムの Activity のみでは不足）に整備すること。ドキュメント形式は問わないが、「デジタル・ガバメント推進標準ガイドライン解説書」（https://cio.go.jp/guides）の設計・開発の章にて謳われている内容を網羅するものとし、後の運用保守事業者などが俯瞰して仕様を把握できるようなものであること。ドキュメントは必ずしも実装と同時に整備されている必要はないが、マニュアル・周知資料に必要な内容やデータモデルなどは整備する時期をプロジェクト計画書に盛り込むこと。

また、継続的インテグレーション・継続的デリバリー（CI/CD）を可能とし、開発作業だけでなく運用・保守作業も含めて効率的な手法を取り入れること。

(4) 開発ツール

受託者は、プログラム設計・製造に当たり開発フレームワーク等のツールを用いる場合、ベンダーロックインを防ぐため、原則として特定の事業者しか使用できない技術、製品、サービス等に依存しないツールを用いること。なお、クラウドサービスの開発ツールを利用する場合は、要件定義書 3.2.(2)記載の要件を満たしたクラウドサービスとすること。

(5) 開発の実施

受託者は、当機構の承認を得た基本設計書及び詳細設計書に基づき、本プラットフォームのプログラム設計、開発を実施すること。当該作業は、受託者の拠点にて行うこと。

開発に必要となる環境設定やテストデータ、テストプログラム等の作成は、受託者が行うこと。

なお、設計・開発業務を推進する上で必要となる機器、ソフトウェア等がある場合は、受託者の負担にて用意すること。

(6) テスト計画と実施

受託者は、単体テスト、結合テスト及び総合テストについて、以下の内容を記載したテスト計画書を作成し、当機構の承認を受けること。なお、各テスト項目のうち、反復的にテストを実施するものについては、自動化することを原則とする。アジャイル開発手法を採用する場合には、テスト駆動開発、ビヘイビア駆動開発を前提とした開発手法を用いること。静的解析及びテスト自動化のための Continuous Integration（継続的インテグレーション）環境を構築すること。

- テスト体制
- テスト環境

- 作業内容
- 作業スケジュール
- テストシナリオの概要
- テスト結果に係る定性・定量評価の方法（テスト密度、バグ検出密度等）
- 合否判定基準等

受託者は、テスト計画書の内容を踏まえてテスト仕様書を作成の上、テストを実施すること。
受託者は、テスト計画書に基づき、各テストの実施状況を当機構に報告すること。
テストの実施に当たり必要な費用は全て契約金額に含めること。

(7) 脆弱性検査

使用するソフトウェア及び製造したプログラムに係る脆弱性について、第三者または当システム開発者とは異なるチームにより、サービスをリリースする前に確認を行うこと。また、発見された脆弱性はリリースまでに修正を行うこと。

本システムの稼働までに、当機構が指定する事業者の脆弱性診断（主な診断項目は以下 に示すとおり）を実施する（注：当該診断については 当機構の予算で実施するものとし、当機構 から第三者事業者へ依頼・発注するものとする。）。なお、診断で脆弱性が発見された場合には納期までに受託者にてその対策を行うこと。

＜Web アプリケーション診断＞

- クロスサイトスクリプティング
- クロスサイトリクエストフォージェリ
- SQL インジェクション
- バッファオーバーフロー
- セッション管理
- 認証機能の安全性
- ファイル拡張子
- OS コマンドインジェクション
- ディレクトリトラバーサル
- 権限昇格
- パラメータ書き換え
- その他 Web アプリケーション固有の問題

＜ネットワーク診断＞

- 管理者権限を持つアカウントによる OS・ミドルウェア等へのログイン
- 一般ユーザ権限を持つアカウントによる OS・ミドルウェア等へのログイン
- 権限昇格
- 認証を回避しての OS に対するコマンドの実行
- 認証を回避しての対象ホスト内の情報の窃取
- HTTP ヘッダ・インジェクション

4.6. **受入テスト支援**

受託者は、当機構が受入テストを行うためのテスト計画書を作成し、情報提供等の支援を行うこと。また、当機構が受入テストを実施するに当たり、環境整備、運用等の支援を行うこと。

4.7. **移行**

受託者は、要件定義書「3.13.移行に関する事項」に示す事項を踏まえ、移行に係る業務を適切に実施するとともに、成果物として以下のものを指定の期日までに納品すること。

- 移行計画書
- 移行設計書等一式（移行設計書、移行手順書、移行リハーサル設計書、移行リハーサル手順書等）
- 移行リハーサル結果報告書
- 移行結果報告書

4.8. **引継ぎ**

受託者は、要件定義書「3.14.引継ぎに関する事項」に示す事項を踏まえ、引継ぎに係る業務を適切に実施するとともに、成果物として以下のものを指定の期日までに納品すること。

- 引継ぎ資料（引継ぎ計画書、引継ぎに使用した資料、引継ぎ結果報告書等）

4.9. **教育**

受託者は、要件定義書「3.15.教育に関する事項」に示す事項を踏まえ、教育に係る業務を適切に実施するとともに、成果物として以下のものを指定の期日までに納品すること。

- 教育訓練実施計画書
- 操作マニュアル（利用者向け及び機構担当者向け）、教育資料一式
- 教育訓練実施結果報告書

4.10. **運用**

受託者は、要件定義書「3.16.運用に関する事項」に示す事項を踏まえ、運用に係る業務を適切に実施すること。

4.11. **保守**

受託者は、要件定義書「3.17.保守に関する事項」に示す事項を踏まえ、保守に係る業務を適切に実施すること。

4.12. **会議開催**

(1) 受託者は、定例会を週 1 回程度開催するとともに、業務の進捗状況を設計・開発実施要領に基づき報告すること。

(2) 受託者は各工程の完了に当たり、工程完了判定会議を開催し、当機構の承認を得ること。なお、開催要否は当機構と協議の上決定すること。

(3) 当機構から要請があった場合、又は、受託者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。

(4) 会議開催方法については、原則としてオンライン会議とすること。当機構から要請があった場合、又は、受託者が必要と判断した場合は、当機構と受託者で協議の上、対面で開催すること。

(5) 受託者は、会議終了後、3 日以内（行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第 1 条第 1 項各号に掲げる日をいう。）を除く。）に議事録を作成し、当機構の承認を受けること。

4.13. **データ管理方法**

(1) 本業務にて取り扱うデータについては、当機構の許可なく追加、変更、削除、公開しないこと。

(2) 本業務にて取り扱うデータについては、個人、国、地方公共団体、その他の法人等を問わず、当機構が管理する ID 等を付与された者が、その権限の範囲で利用可能とする。

(3) 受託者は、上記（1）（2）における条件を満たすシステム構成において設計・開発を行うこと。

4.14. **業務完了報告書の作成**

受託者は、以下の内容を含む業務完了報告書を作成し、当機構の承認を得ること。

- 本調達又は工程の概要
- スコープ目標、スコープの評価に利用される基準、完了基準が満たされていることの証拠
- 品質目標、本調達や成果物の品質評価に利用される基準、成果物の品質評価結果
- 実際のマイルストーン通過日、予実に乖離がある場合の理由
- サービス提供状況、成果物の評価を踏まえた本調達に対する事業者総評

4.15. **成果物と納品方法・納入期限**

(1) 成果物一覧

本調達の成果物を下表に示す。納品期限については想定を記載しており、詳細は契約後協議の上、プロジェクト計画書にて定める。成果物は現時点の案であるため、受託者が開発手法を提案の上で当機構が承認した場合は、成果物の種類、内容を変更することができる。

なお、下表の成果物のドキュメント類については、当機構と調整の上、レビューを必ず実施し、当機構の承認を得るようにすること。

また、アジャイル開発においては、ドキュメントよりもコミュニケーションを重視する事でドキュメントへの記載が不足する傾向があることから、後からプロジェクトを把握するのが難しくなる可能性がある。アジャイル開発手法を採用する場合は、設計書等の成果物の品質をどのように担保するか提案し、受託者にて適切なドキュメント管理を行うこと。

表 2 成果物一覧

項番	成果物名	提出期限	納入期限			
			2026年		2027年	
			3月末	9月末	3月末	6月末
1	プロジェクト計画書	契約締結後２週間以内	○	※	※	※

項番	成果物名	提出期限	納入期限			
			2026年		2027年	
			3月末	9月末	3月末	6月末
2	設計・開発実施要領	契約締結後２週間以内	○	※	※	※
3	設計・開発実施要領に基づく管理資料	契約締結後２週間以内	○	※	※	※
4	情報セキュリティ管理計画書	契約締結後２週間以内	○	※	※	※
5	要件精査結果資料、業務フロー	要件精査の状況に応じて順次	○	※	※	※
6	標準コーディング規約等プログラミング等のルールを定めた標準に関する資料	設計・開発開始前まで	○	※	※	※
7	設計・開発工程の各種会議資料（進捗状況報告、課題管理表、リスク管理表、会議の議事録等）	会議実施前まで 議事録は会議後３開庁日以内	○	○	○	○
8	設計書（基本設計書、詳細設計書、実体関連図（ERD）、画面デザインガイドライン、データ定義書、情報システム関連図、ネットワーク構成図、ソフトウェア構成図、ハードウェア構成図、プログラム一覧等、環境構築手順書、環境定義書、ハードウェア・ソフトウェア機器の一覧、外部インタフェース仕様書等）	設計・開発の状況に応じて順次	－	○	※	※
9	ソースコード（IaC設定ファイル類を含む）一式（ソースコードのコメントは原則として日本語または英語に限定すること。）	設計・開発の状況に応じて順次	－	－	○	※
10	ノンプログラミングによる自動生成等のツールを利用する場合、設計書やソースコード一式の生成等に利用される設定情報その他の必要な情報一式	設計・開発の状況に応じて順次	－	－	○	※
11	実行プログラム一式	設計・開発の状況に応じて順次	－	－	○	※
12	外部サービスを利用する場合、当該サービスに係る設定情報その他の必要な情報一式	設計・開発の状況に応じて順次	－	－	○	※
13	テスト計画書、テスト仕様書	各テスト開始前まで	－	－	○	※
14	受入テスト計画書（案）、受入テスト仕様書（案）	受入テスト開始二週間前まで	－	－	○	※
15	テスト結果報告書（テスト証跡も含むが、納品範囲は当機構と協議の上、決定すること）	各テスト工程完了判定前まで	－	－	○	※
16	テストデータ	テストの状況に応じて順次	－	－	○	※
17	脆弱性検査結果報告書	総合テスト工程完了判定前まで	－	－	○	※
18	移行計画書	総合テスト開始前まで	－	－	○	※
19	移行設計書等一式（移行設計書、移行手順書、移行リハーサル設計書、移行リハーサル手順書等）	移行リハーサル開始前まで	－	－	○	※
20	移行リハーサル結果報告書	移行判定前まで	－	－	○	※
21	移行結果報告書	契約満了前まで	－	－	○	※
22	教育訓練実施計画書	設計・開発の状況に応じて順次	－	－	○	※
23	操作マニュアル（利用者向け及び機構担当者向け）、教育資料一式	教育の実施一週間前まで	－	－	○	※
24	教育訓練実施結果報告書	受入テスト工程完了判定前まで	－	－	○	※
25	ランニングコスト試算表	運用・保守開始前まで	－	－	○	※

項番	成果物名	提出期限	納入期限			
			2026年		2027年	
			3月末	9月末	3月末	6月末
26	運用・保守計画書	案は総合テスト開始前まで 確定版は運用・保守開始前まで	－	－	○	※
27	運用・保守実施要領等一式（運用・保守実施要領、運用・保守手順書、ヘルプデスク運用マニュアル、FAQ等）	案は総合テスト開始前まで 確定版は運用・保守開始前まで	－	－	○	※
28	パッチ適用計画	運用・保守の状況に応じて順次	－	－	○	※
29	変更依頼書	運用・保守の状況に応じて順次	－	－	○	※
30	リリース管理台帳、リリース計画書	運用・保守の状況に応じて順次	－	－	○	※
31	大規模災害等対応訓練完了報告書	運用・保守の状況に応じて順次	－	－	－	○
32	情報漏洩等対応訓練完了報告書	運用・保守の状況に応じて順次	－	－	－	○
33	運用・保守報告書（運用状況報告、課題管理表、リスク管理表、会議の議事録等）	運用・保守の状況に応じて順次	－	－	－	○
34	情報セキュリティ対策実施報告書	運用・保守の状況に応じて順次	－	－	－	○
35	引継ぎ資料（引継ぎ計画書、引継ぎに使用した資料、引継ぎ結果報告書等）	契約満了前	－	－	－	○
36	業務完了報告書	契約満了前	－	－	－	○
37	情報資産管理標準シート	契約満了前	－	－	－	○

＜納入期限の凡例＞
○：納入対象とする。
※：成果物に更新があった場合、最新版を納入対象とする。
－：納入対象外とする。

(2) 成果物の納品方法

成果物の納品方法は以下のとおり。

- 成果物は、原則として日本語で作成すること。ただし、日本国においても英字で表記されることが一般的な文言や、ソースコード等の英字で作成することが一般的な成果物については、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11日内閣官房長官通知）」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での納品とすること。提出先は当機構と協議の上、決定すること。
- 納品後、当機構において改変が可能となるよう、Microsoft Office 形式や図表等の元データも併せて納品すること。なお、業務効率化のために、ツールから出力される結果を成果物にしている場合は、当機構と協議の上でそれを納品することも可能である。
- 成果物の作成に当たって、特別なツールを利用する場合は、当機構の承認を得ること。
- 成果物が外部に不正に利用されたり、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。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。
- 受託者が保有する特許などを用いる場合には、成果物にその旨を明記すること。

・ 受託者は、表 3「成果物一覧」に指定された期限に向けて成果物の草案を準備し、内容について当機構と適宜協議をした上で、成果物の初版を表 3「成果物一覧」に指定した期限に納品し当機構の承認を得ること。
・ 成果物については、必要に応じて更新を行い当機構の承認を得て最終版とした上で、契約満了日までに成果物一式を納品すること。

(3) 成果物の納入期限

成果物の納入期限は、以下のとおりとする。

・ 第 1 回目 2026 年 3 月 31 日（作業期間：契約開始日～2026 年 3 月 31 日）
・ 第 2 回目 2026 年 9 月 30 日（作業期間：2026 年 4 月 1 日～2026 年 9 月 30 日）
・ 第 3 回目 2027 年 3 月 31 日（作業期間：2026 年 10 月 1 日～2027 年 3 月 31 日）
・ 第 4 回目 2027 年 6 月 30 日（作業期間：2027 年 4 月 1 日～2027 年 6 月 30 日）

4.16. 情報資産管理標準シートの提出

受託者は、当機構から依頼があった場合は、以下の情報を含む情報資産管理標準シートを提出すること。提出時期は運用・保守実施要領にて定めること。

情報資産管理標準シートの様式や提出方法の変更が発生した場合は、当機構と協議の上、対応を実施すること。

(1) 開発に関する情報

・ 開発
  - スマホアプリ名、スマホアプリ対応 OS、開発環境（IDE）、開発言語、開発ライブラリ
  - コミュニケーションツール、バグ追跡ツール、バージョン管理ツール、プロジェクト管理ツール
  - プロジェクト管理情報
・ プラットフォーム
  - 利用プラットフォーム（ガバメントクラウド、パブリッククラウド等）
  - ネットワークアクセス、連携システム
  - 利用 IaaS、利用 PaaS、利用リージョン
・ ソフトウェア
  - 使用するソフトウェア一覧（以下のミドルウェア、ソフトウェアについては情報資産管理標準シートのカテゴリ分けを行うこと。）
    - Web サーバ
    - AP サーバ
    - DBMS
    - 統合運用管理
    - バックアップソフトウェア
    - CMS
    - クライアント PC 資産管理
・ ハードウェア
  - 使用するハードウェア一覧（以下の項目を一覧に含めること。）
    - ハードウェアベンダー名
    - ハードウェア型番
・ セキュリティ関連情報
  - 利用回線、プロトコル及びポート番号、個人情報取扱件数、内部 CSIRT

- SOC/ログ監視、クラウドファイヤーウォール、CASB、ネットワークセキュリティ
- WAF、IPS/IDS、アンチマルウェア、EDR、実施状況、法人番号、直近実施日
- 固定パブリック IP、公開ドメイン、公開 E メール

(2) 契約情報

人件費については人件費単価ごとに工数を提示すること。再請負先がある場合は再請負先の法人番号と再請負金額を提示すること。

最大何次請負、再請負総額、年度契約金額を提示すること。

4.17. **その他**

(1) グリーン購入法に定める特定調達品目については、以下 URL に掲載されている「グリーン購入の調達者の手引き」（令和 6 年 2 月）による各特定調達品目の「判断の基準」を満たすこと。
https://www.env.go.jp/policy/hozen/green/g-law/net/shiryou.html

(2) インターネット公開するシステムは、原則として IPA ドメイン（.ipa.go.jp）を用いること。利用するドメインは、当機構と協議のうえ、決定すること。

(3) 受託者は、本プラットフォームの整備・管理に当たり、当機構が必要と認める関係者（当機構内の関係部署等を想定）からの説明要請や質問等があった場合には、当機構が実施する資料作成、回答案作成等の支援を行うこと。

5. 作業の実施体制・方法に関する事項

5.1. 作業実施体制と役割

本業務における組織等の体制と役割は下表を想定しているが、詳細は当機構と協議の上で決定する。なお、実施体制と役割、各役割に従事する実施者の氏名はプロジェクト計画書の「作業体制に関する事項」に記載し、「4.15. 成果物の作成」に記載された納品期限までに提出すること。

受託者は、本調達仕様書で示す作業を遂行可能な知識、スキル及び経験を有する体制を構築すること。また、開発に必要なスキルマップを定義し、要員がそれを満たすことを確認のうえ体制を提案すること。特に、アジャイル開発を採用する場合は、当機構と受託者との協力しコミュニケーションを密に図ることが不可欠であることから、表 3 に示す開発体制だけでなくアジャイル開発体制を提案の上、当機構との密なコミュニケーションをとるための方法および会議体を合わせて提案すること。

表 3 本業務における組織等の体制と役割

項番	組織又は要員		役割
1	当機構		・ 本プロジェクトの調達及び契約締結後の調整を主体となって実施する。 ・ プロジェクト管理状況の確認、承認及び成果物の承認を行う。 ・ プロジェクトの全体進捗管理を行う。 ・ 関係省庁との仕様調整及びテスト等内容確認において連携を行う。 ・ 業務機能の仕様を検討、確認する。
2	受託者	プロジェクト統括管理責任者	・ 本業務全体を統括し、必要な意思決定を行い、本プロジェクトの円滑な遂行の責任を担う。
3		プロジェクト全体管理者 (プロジェクトマネージャ)	・ スケジュール、リスク、課題及び品質等、本プロジェクトに係る包括的な管理を行うとともに、当機構との調整を行う。 ・ 本業務の請負期間中、専任でこれに当たるものとする。
4		システム 設計・開発班	・ 本プラットフォームの設計・開発を担う。 ・ リーダーはシステム設計・開発班の各業務の全体像を把握し、設計・開発に係る当機構との調整、対応方針の相談、事実確認等を円滑に実施できる者を設定すること。 ・ リーダーはシステム設計・開発作業期間中、専任でこれに当たるものとする。
5		品質管理責任者	・ 本プロジェクトの遂行に当たり、品質管理における受託者としての責任を持つ。
6		情報セキュリティ責任者	・ 本プロジェクトの遂行に当たり、情報セキュリティ管理における受託者としての責任を持つ。

5.2. 作業要員に求める資格等の要件

(1) プロジェクト全体管理者

受託者におけるプロジェクト全体管理者は、本プラットフォームと同等規模のシステム開発、及びクラウドサービスを活用したシステムの設計・開発の遂行責任者としての経験を 2 年以上有し、次のいずれかに該当すること。

- 情報処理の促進に関する法律（昭和 45 年 5 月 22 日法律第 90 号）に基づき実施される情報処理技術者試験のうちプロジェクトマネージャ試験の合格者
- プロジェクトマネジメント協会（PMI）が認定するプロジェクトマネジメントプロフェッショナル（PMP）の資格保有者又は技術士（情報工学部門又は総合技術監理部門（情報工

学を選択科目とする者））の資格を有すること
- 上記のいずれかの試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者

(2) システム設計・開発班リーダー

システム設計・開発班リーダーは、設計・開発の経験年数を 5 年以上有すること。また、その中でリーダークラスとしての経験を 2 年以上有し、次のいずれかに該当すること。

- システムアーキテクト試験の合格者
- データベーススペシャリスト試験の合格者
- ネットワークスペシャリスト試験の合格者
- 上記のいずれかの試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者

(3) システム設計・開発班（クラウドサービスの設計・開発担当者）

クラウドサービスの設計・開発担当者に次のいずれかに該当する者を含めるか、または、主として利用するクラウドサービスのクラウドサービスプロバイダーが提供するサポートサービス（AWS プロフェッショナルサービス、Azure 有償サポート等）を利用すること。

- 主として利用するクラウドサービスについて、当該クラウドサービスプロバイダーが認定している資格の中で、以下に例示する上級資格を保有している者
  - AWS 認定 ソリューションアーキテクト-プロフェッショナル
  - AWS 認定 DevOps エンジニア-プロフェッショナル
  - Google Cloud 認定 プロフェッショナルクラウドアーキテクト
  - Google Cloud 認定 プロフェッショナルクラウド DevOps エンジニア
  - Microsoft 認定 Azure ソリューションアーキテクトエキスパート
  - Microsoft 認定 DevOps エンジニアエキスパート
- 上記の試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者

(4) スクラムマスター（アジャイル型の開発を行う場合に限る。）

本システムと同等規模のシステム、短期間での大規模システム開発、及びクラウドサービスを活用したシステムの設計・開発の 3 年以上のスクラムマスターとしての経験を 3 年以上有すること。

(5) UI/UX デザイナー、HCD 専門家等

本プロジェクトの専任担当者として、UI/UX デザインに関する 5 年以上の実務経験を有する専門家（UI/UX デザイナー、HCD 専門家等）を 1 名以上配置すること。また、過去に手がけた公共分野または大規模 Web サイトにおける UI/UX 改善の実績を提示すること。

(6) 情報セキュリティ責任者

情報セキュリティ責任者は、次のいずれかに該当すること。

- 情報処理安全確保支援士試験の合格者または資格登録者
- 特定非営利活動法人日本システム監査人協会（SAAJ）が認定する公認情報システム監査人（CAS）の資格保有者
- 情報システムコントロール協会（ISACA）が認定する公認情報システム監査人（CISA）の資格保有者
- 情報システムコントロール協会（ISACA）が認定する公認情報セキュリティマネージャ（CISM）の資格保有者
- International Information Systems Security Certification Consortium が認

定するセキュリティプロフェッショナル認証資格（CISSP）の資格保有者
- 上記のいずれかの試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者

5.3. 作業場所

(1) 業務の実施場所
設計・開発、テスト等の作業場所は、受託者の責任において用意すること。その際は、「（2）諸設備、物品等資源」に示す要件をすべて満たすこと。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。

(2) 諸設備、物品等資源
当機構の情報セキュリティポリシーを遵守の上、当機構の了承を得ること。

6. 作業の実施に当たっての遵守事項

6.1. 機密保持、資料の取扱い

本業務に係る情報セキュリティ要件を遵守すること。本業務に係る機密保持及び資料の取扱いに係る要件は次の通りである。

(1) 請負した業務以外の目的で利用しないこと。

(2) 業務上知り得た情報について第三者への開示や漏えいをしないこと。

(3) 作業場所から持出しを禁止すること。

(4) 情報セキュリティインシデントが発生する等、万一の事故があった場合に直ちに当機構に報告すること。また、受託者の責に起因する事故であった場合は、損害に対する賠償等の責任を負うこと。

(5) 業務の履行中に受け取った情報の管理を実施し、業務終了後は返却又は抹消等を行い、復元不可能な状態にすること。

(6) 要件定義書の「1.5.業務実施手順 (5)管理対象情報一覧、2.4.データに関する事項 (2)データ一覧」で示されたデータ項目ごとの格付・取扱・アクセス制限を参照し、設計・開発時におけるデータ項目の追加・変更の際に機密性区分の格付を行うこと。また、格付ごとに適切な管理措置（例：アクセス制限、暗号化等）を講じること。

(7) 情報セキュリティ責任者は、情報取扱者を限定し情報セキュリティの管理体制を整備すること。

(8) 適切な措置が講じられていることを確認するため、履行状況の定期的な報告を行うこと。また、必要に応じて当機構による実地調査が実施できること。履行状況が不十分である場合は、当機構と協議の上、改善策を実施すること。

(9) 以上の要件における受託者の実施内容を情報セキュリティ管理計画書に取りまとめた上で当機構の承認を得ること。なお、プロジェクト計画書において情報セキュリティ管理計画書に相当する内容が記載されている場合は、当該資料を情報セキュリティ管理計画書に代えても差し支えない。

6.2. 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

「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」（令和 5 年 7 月 4 日サイバーセキュリティ戦略本部決定）に準拠して必要なセキュリティ対策を講じること（以下記載は、基本的な事項）。

(1) 不正アクセスの防止や万が一侵入された場合のログ等の証跡を蓄積するとともに、検知・通知を行えるようにすること。

(2) セキュリティパッチ等の適用を適宜正確かつ迅速に行うこと。

(3) 脆弱性が生じないよう留意して設計・開発し、稼働前及び定期的な検査を通じた確認により修正を適用できるようにすること。

(4) 不正行為の検知、発生原因の特定に用いるために、システムの利用記録、例外的事象の発生に関するログを蓄積し、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。

(5) ログの改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざん等の脅威の軽減）のための措置を含む設計とすること。

(6) 想定されるサプライチェーン・リスクを分析・評価し、それに対する軽減策を講じるにあたり、「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」（平成 28 年 10 月 25 日 内閣サイバーセキュリティセンター）を参照すること。

6.3. 個人情報等の取扱い

(1) 生存する個人に関する情報であり、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。）は個人情報として取り扱うこと。

(2) 個人情報、個人関連情報、特定個人情報等、仮名加工情報及び行政機関等匿名加工情報（以下、「個人情報等」という。）の取扱いに係る事項について当機構と協議の上決定し、書面にて提出すること。なお、以下の事項を記載すること。
- 管理体制
- 個人情報等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）

(3) 本業務の遂行において、安全性や確実性を考慮し、仕様外の個人情報等を取得し、取り扱う必要性や有用性がある場合は、当機構と協議してその妥当性を検討し、承認を得た上でこれを行うこと。また、当機構と協議の上で当該個人情報等の利用目的と性質を考慮し、保持期間を定めること。当該保持期間が経過した後は、業務仕様にしたがって遅滞なく消去し又は匿名化すること。

(4) 本業務の遂行に際して個人情報等を取得し取り扱う場合、本業務のために定められた利用目的外の利用を厳に慎み、本業務のために供する個人情報等は他の個人情報等と分別して保管し、当機構と協議のうえで書面により定めた環境下で所定の仕様に依拠して遂行すること。また、本業務を遂行する業務従事者にあってもこれを実効あらしめるものとするため、必要な管理監督および教育を行うこと。

(5) 個人情報等を本業務のために定められた利用目的外で複製する際には、事前に当機構の許可を得ること。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。

(6) 個人情報等の取扱いに際して、その本人によるデータの入力、本人による情報システムの利用に伴うデータの生成、その他本人による関与を通じてデータ処理が行われる場合には、その処理の記録（システム上のログによるもの等）を残すこと。

(7) 受託者が本業務のために取り扱う個人情報等に関して、利用者等から個人情報等の保護に関する法律その他適用ある法令上の請求が行われた場合には、速やかに当機構に通知してその指示を受けること。また、当機構による法令上の請求への対応のために必要な個人情報等の抽出、変更、削除その他合理的な協力を行い、これを可能とする体制および仕様を維持すること。

(8) 作業を派遣労働者に行わせる場合を含め直接雇用していない第三者の使用人等に業務従事させる場合には、本業務の一部を再請負する場合の手続きに準じて労働者派遣契約書に秘密保持義務など個人情報等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、当機構の承認を得た上で実施すること。

(9) 当機構が必要と認めた場合であってその態様が受託者の業務その他の営業を著しく妨げるものでないとき、当機構またはこれが指定した者による個人情報等の取扱いの状況および管理体制の監査を受け入れ、合理的に必要と認められる資料の提出を行うこと。

(10) 受託者は、本業務を履行する上で個人情報等の漏えい等安全確保の上で問題となる事案又はそのおそれのあ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、当機構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方針等について直ちに報告すること。

(11) 個人情報等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。

6.4. 法令等の遵守

本業務の遂行に当たっては、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）、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）、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に関する法律（平成 25 年 5 月 31 日法律第 27 号）等、適用される法令等を遵守し履行すること。

6.5. 標準ガイドライン等

本業務の遂行に当たっては、「標準ガイドライン」に基づき、作業を行うこと。具体的な作業内容及び手順等については、「デジタル・ガバメント推進標準ガイドライン解説書（デジタル庁）」（以下、「解説書」という。）を参考とすること。なお、「標準ガイドライン」及び「解説書」が改定された場合は、最新のものを参照し、その内容に従うこと。

6.6. 情報システム監査

(12) 本業務おいて整備・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、当機構が情報システム監査の実施を必要と判断した場合は、当機構が定めた実施内容（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。（契約後の請負事業開始前より実施される当機構が別途選定した事業者による監査を含む。）

(13) 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、対応案を当機構と協議し、指示された期間までに是正を図ること。

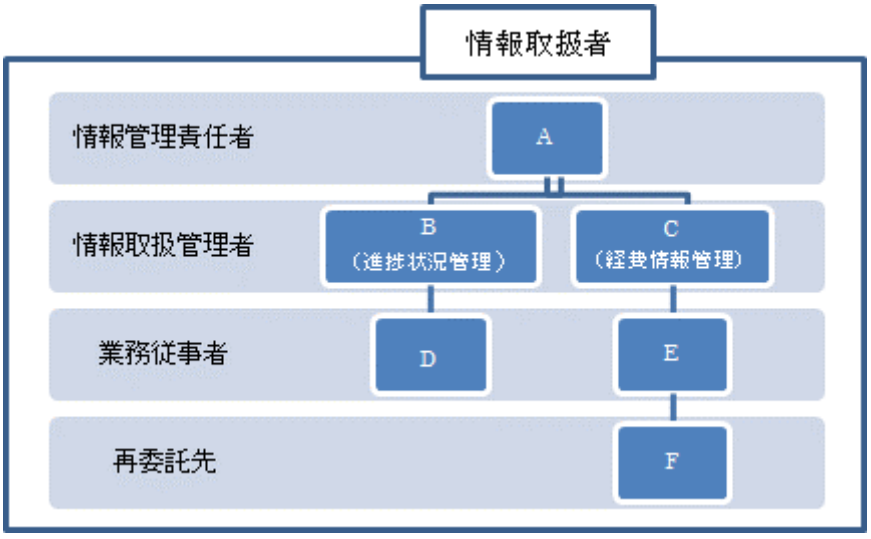
6.7. 情報セキュリティの管理体制について

(1) 受託者は本業務で知り得た情報を適切に管理するため、次の履行体制を確保し、当機構に対し「情報セキュリティを確保するための体制を定めた書面（情報管理体制図）」及び「情報取扱者名簿」（氏名、個人住所、生年月日、所属部署、役職等が記載されたもの）を契約前に提出し、当機構の承認を得ること。（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当部門から求められた場合は速やかに提出すること。）なお、情報取扱者名簿は、業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

（確保すべき履行体制）

契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、当機構が保護を要さないと確認するまでは、情報取扱者名簿に記載のある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。

＜情報管理体制図（例）＞



【情報管理体制図に記載すべき事項】

- 本業務の遂行にあたって保護すべき情報を取り扱う全ての者。（再請負先も含む。）
- 本業務の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。

＜情報取扱者名簿（例）＞

		(しめい) 氏名	個人 住所	生年 月日	所属 部署	役職	パスポート 番号及び 国籍(※4)
情報管理責任者（※1）	A						
情報取扱管理者（※2）	B						
	C						
業務従事者(※3)	D						
	E						
再委託先	F						

（※１）受託者としての情報取扱の全ての責任を有する者。必ず明記すること。

（※２）本業務の遂行にあたって主に保護すべき情報を取り扱う者ではないが、本業務の進捗状況などの管理を行うもので、保護すべき情報を取り扱う可能性のある者。

（※３）本業務の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※４）日本国籍を有する者及び法務大臣から永住の許可を受けた者（入管特例法の「特別永住者」を除く。)以外の者は、パスポート番号等及び国籍を記載。

（※５）個人住所、生年月日については、必ずしも契約を前に提出することを要しないが、その場合であっても担当部門から求められた場合は速やかに提出すること。

(2) 本業務で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならないものとする。ただし、当機構の承認を得た場合は、この限りではない。

(3) 情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め当機構へ届出を行い、承認を得ること。

(4) 情報システムの設計・開発、運用・保守工程において、当機構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。

(5) 当機構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）を当機構との協議の上、必要と判断された場合は提出すること。また、第三者機関による品質保証体制を証明する書類等が提出可能な場合は、提出すること。

(6) 情報システムに当機構の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、当機構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。（例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、発注元から要求された場合には提出させるようにする等）また、当該手順及び体制が妥当であることを証明するための書類を当機構との協議の上、必要と判断された場合は提出すること。

(7) 情報システムの開発・構築等の各工程において、情報セキュリティに係るサプライチェーン・リスクを低減する対策が行われていること。

(8) 「4.5.開発・テスト (7)脆弱性検査」に示す事項について、脆弱性検査にて検出された脆弱性への対応を行うこと。また、脆弱性検査の終了時には、対応内容及び結果を脆弱性検査対応結果報告書に取りまとめること。

(9) 情報システムの開発環境、本番環境、検証環境を分離し、各環境で取扱う情報の機微性等に応じてアクセス制御等必要なセキュリティ対策を実施すること

(10) 政府情報システムにおいて含有されやすいセキュリティ上の問題点を下表に示す。各項目に対して漏れなく対応すること。

表 4 政府情報システムにおいて含有されやすいセキュリティ上の問題点

項番	要因	セキュリティ上の問題点
1	認証管理不備	・ 共用アカウントが使用される際に、利用者特定の仕組みや取扱いに関するルールが整備されていない ・ 推測されやすい脆弱なパスワードが使用されている ・ 認証情報がファイル等に平文で書かれている
2	アクセス制御不備	・ 必要な強度の認証が行われていない ・ ネットワーク、システムへのアクセス制限が実施されていない ・ アクセス権が必要最小限のアクセス権付与が守られておらず、過剰である
3	暗号化不備	・ 重要情報が流れる各機器間の通信経路において、必要な暗号化が実施されていない
4	資産管理、脆弱性管理不備	・ 利用しているソフトウェアや機器の状態を把握していない（最新状態を維持できていない） ・ OS やミドルウェア、ファームウェア等の脆弱性対策が適切に実施されていない
5	Web アプリケーションの脆弱性	・ SQL インジェクション、クロスサイトスクリプティング等の初歩的な Web アプリケーションの脆弱性が存在している ・ パラメータ改ざんにより、本来アクセスできないデータを操作できるなどの脆弱性が存在している
6	ログ管理不備	・ ログ取得の範囲が目的に応じて定められていない（必要なログが取得されていない） ・ 定期的なログの点検又は分析が実施されていない
7	外部委託の管理不備	・ 外部委託に係る契約に、遵守事項で定める委託先の情報セキュリティ対策が含まれていない ・ 外部委託に係る契約に基づき、委託先における情報セキュリティ対策の履行状況を確認していない

6.8. セキュリティ要件

セキュリティ要件については、「別紙１　要件定義書」に記載の要件を満たすこと。

7. 成果物に関する事項

7.1. 知的財産権の帰属

知的財産権の帰属については、契約書に記載の通りとする。

7.2. 契約不適合責任

契約不適合責任については、契約書に記載の通りとする。

7.3. 検収

(1) 本業務の受託者は、成果物等について、納入期限までに当機構に内容の説明を実施し、検収を受けること。

(2) 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、交換等を行うこと。また、変更点について当機構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。

8. 入札参加に関する事項

8.1. 公的な資格や認証等の取得

(1) 応札者は、品質マネジメントシステムに係る以下のいずれかの条件を満たすこと。
- 品質マネジメントシステムの規格である「JIS Q 9001」又は「ISO9001」（登録活動範囲が情報処理に関するものであること。）の認定を、業務を遂行する組織が有していること。
- 上記と同等の品質管理手順及び体制が明確化された品質マネジメントシステムを有している事業者であること（管理体制、品質マネジメントシステム運営規程、品質管理手順規定等を提示すること。）

(2) 応札者は、情報セキュリティに係る以下のいずれかの条件を満たすこと。
- 情報セキュリティ実施基準である「JIS Q 27001」、「ISO/IEC27001」又は「ISMS」の認証を有していること。
- 一般財団法人日本情報経済社会推進協会のプライバシーマーク制度の認定を受けているか、又は同等の個人情報保護のマネジメントシステムを確立していること。
- 個人情報を扱うシステムのセキュリティ体制が適切であることを第三者機関に認定された事業者であること。

8.2. 受注実績

(1) 応札者は、以下の必須要件を満たすこと。

- Web アプリケーションを構築した実績を過去 3 年以内に有すること。
- AWS、Azure、Google Cloud 等のクラウド上のシステムの設計・開発を受注した実績を過去 3 年以内に有すること。
- 官公庁等公的機関に係るシステムの設計・開発の実績を過去 3 年以内に有すること。
- データ分析基盤の設計・開発を受注した実績を過去 3 年以内に有すること。

(2) 応札者の実績として望ましい推奨要件を以下に示す。

- 本プラットフォームと類似する統合 ID 基盤の設計・開発の実績を過去 3 年以内に有すること。
- AWS、Azure、Google Cloud 等のガバメントクラウド上のシステムの設計・開発を受注した実績を過去 3 年以内に有すること。

・　データ分析基盤の設計・開発を受注した実績を 5 件以上有すること。

9. 再請負に関する事項

9.1. 再請負の制限及び再請負を認める場合の条件

(1) 本業務の受託者は、業務を一括して又は主たる部分を再請負してはならない。

(2) 受託者における遂行責任者を再請負先事業者の社員や契約社員とすることはできない。

(3) 受託者は再請負先の行為について一切の責任を負うものとする。

(4) 再請負先における情報セキュリティの確保については受託者の責任とする。再請負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、当該調達仕様書のセキュリティ対策にかかる措置の実施を再請負先に担保させること。また、再請負先のセキュリティの対策実施状況を確認できるよう、再請負先との契約内容に含めること。（再請負の相手方が更に請負を行うなど複数の段階で再請負が行われる（以下「再々請負」という。）場合の取扱いも同様）

9.2. 承認手続

(1) 本業務の実施の一部を合理的な理由及び必要性により再請負する場合には、以下の内容を記載した書面を当機構に提出し、あらかじめ承認を受けること。
- 再請負の相手方の商号又は名称、住所
- 再請負を行う業務の範囲
- 再請負の必要性及び契約金額等

(2) 前項による再請負の相手方の変更等を行う必要が生じた場合も、前項と同様に再請負に関する書面を当機構に提出し、承認を受けること。

(3) 再々請負には、当該再々請負の相手方の商号又は名称及び住所並びに再々請負を行う業務の範囲を書面で報告すること。

9.3. 再請負先の契約違反等

再請負先において、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。また、当機構は当該再請負先への再請負の中止を請求することができる。

10. クラウドサービスの選定、利用に関する事項

10.1. クラウドサービスの選定、利用に関する要件

クラウドサービスの選定、利用に関する要件については、要件定義書「3.2.システム方式に関する事項 (1)システム方式についての全体方針、 (2)クラウドサービスの選定、利用に関する要件」を参照すること。

10.2. クラウドサービスを利用する場合の成果物の取扱い

クラウドサービスを利用する場合は、当該サービスに係る設定情報やその他必要な情報一式を取りまとめること。

11. その他特記事項

11.1. 機器等のセキュリティ確保、リストの提出

システムで使用する機器やソフトウェア（ミドルウェア、ライブラリ）等を調達する際は、不正侵入の経路となるバックドアや脆弱性が含まれていないことを確認し、システム稼働中にメーカーサポートを受けられる安全なプロダクトを選定すること。

「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」に基づき、サプライチェーン・リスクの観点から国家サイバー統括室に対して、講ずべき必要な措置について助言を求めるため、「別紙 16 機器・役務リスト」に再委託先、クラウドサービス、機器等を記載の上、入札説明書記載の期限までに提出すること。当機構がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、当機構と迅速かつ密接に連携し提案の見直しを図ること。調達機器に変更が生じる場合、国家サイバー統括室に対して助言を設ける必要があるため、再度機器等リストを提出すること。

11.2. その他特記事項

本業務の履行に当たっては、障害を理由とする差別の解消の推進に関する法律（平成 25 年法律第 65 号）第９条第１項に基づく「独立行政法人情報処理推進機構における障害を理由とする差別の解消の推進に関する対応要領」（令和６年３月 28 日 2023 情総企第 806 号）第３条に規定する合理的配慮について留意すること。

12. 附属文書

別紙１ 要件定義書
別紙２ 業務フロー
別紙３ 機能一覧
別紙４ 機能概要補足資料
別紙５ 画面一覧
別紙６ 画面イメージ
別紙７ サイトマップ
別紙８ 帳票一覧
別紙９ データモデル
別紙 10 データ一覧
別紙 11 データ定義
別紙 12 CRUD マトリクス
別紙 13 外部インターフェース一覧
別紙 14 情報セキュリティに関する事項
別紙 15 独立行政法人情報処理推進機構における障害を理由とする差別の解消の推進に関する対応要領

別紙 16　機器・役務リスト

別紙 16 については添付無し。入札説明書「6．入札参加前に提出する資料」記載の方法で問い合わせること。