

**2024 年度（令和 6 年度）**  
**情報提供等記録開示システムに関する**  
**設計・開発及び運用・保守業務一式**

**調達仕様書**

**デジタル庁**

1.	調達案件の概要	1
1.1.	調達件名	1
1.2.	調達の背景	1
1.3.	調達目的および期待する効果	1
1.4.	業務規模の想定	2
1.5.	用語の定義	2
1.6.	業務・情報システムの概要	3
1.7.	契約期間	4
1.8.	作業スケジュール	4
2.	調達案件及び関連調達案件の調達単位、調達の方式等	4
2.1.	調達範囲	4
2.2.	調達案件の一覧	4
2.3.	調達案件間の入札制限	5
3.	情報システムに求める要件	5
4.	作業の実施内容に関する事項	5
4.1.	設計・開発実施計画書等の作成	5
4.2.	要件定義	8
4.3.	設計	8
4.4.	開発・テスト	11
4.5.	受入テスト支援	12
4.6.	引継ぎ（受託者から他事業者へ）	12
4.7.	運用	12
4.8.	保守	13
4.9.	会議開催	13
4.10.	データ管理方法	13
4.11.	業務完了報告書の作成	13
4.12.	成果物の作成	13
4.13.	情報資産管理標準シートの提出	15
4.14.	その他	16
5.	作業の実施体制・方法に関する事項	17
5.1.	作業実施体制と役割	17
5.2.	作業要員に求める資格等の要件	19
5.3.	作業場所	20
5.4.	作業の管理に関する事項	21
6.	作業の実施に当たっての遵守事項	21
6.1.	機密保持、資料の取扱い	21
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	22

6.3.	個人情報等の取扱い.....	23
6.4.	法令等の遵守.....	24
6.5.	標準ガイドライン等.....	24
6.6.	情報システム監査.....	24
6.7.	情報セキュリティの管理体制について.....	24
6.8.	セキュリティ要件.....	25
7.	成果物に関する事項.....	26
7.1.	知的財産権の帰属.....	26
7.2.	契約不適合責任.....	26
7.3.	検収.....	26
8.	入札参加に関する事項.....	26
8.1.	公的な資格や認証等の取得.....	26
8.2.	受注実績.....	27
8.3.	複数事業者による共同入札.....	27
8.4.	入札制限.....	27
9.	再委託に関する事項.....	27
9.1.	再委託の制限及び再委託を認める場合の条件.....	27
9.2.	承認手続.....	28
9.3.	再委託先の契約違反等.....	28
10.	クラウドサービスの選定、利用に関するセキュリティ関連事項（要機密情報を取り扱う場合）.....	28
10.1.	クラウドサービスの選定、利用に関する共通セキュリティ要件.....	28
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.....	29
11.	その他特記事項.....	29
11.1.	機器等のセキュリティ確保、リストの提出.....	29
11.2.	入札公告期間中の資料閲覧等.....	30
11.3.	その他特記事項.....	31

# 1. 調達案件の概要

## 1.1. 調達件名

---

2024 年度（令和 6 年度）情報提供等記録開示システムに関する設計・開発及び運用・保守業務一式

## 1.2. 調達の背景

---

デジタル庁国民向けサービスグループマイナポータル担当（以下「主管課」という。）では、「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 条を根拠に、マイナンバーカードを本人認証のキーとした、マイナポータル（情報提供等記録開示システム）の設計・開発及び運用・保守業務を実施している。

2017 年（平成 29 年）7 月からの試行運用を経て、同年 11 月から本格運用を開始したマイナポータルは現在、デジタル庁が掲げるミッション（「誰一人取り残されない、人にやさしいデジタル化を。」）を実現するため、利用者からのフィードバックを得ながら、手続に当たって迷うことがなく、また利用したいという新たな体験も提供できるようにフロントエンドの刷新を行いつつ、継続して新たな利用シーンの拡大も推し進め、住民/国民向けのさまざまな行政手続のデジタル化に取り組んでいる。

また、マイナポータルが提供する各機能を、官民の Web サービス提供者が自らのサービスにおいても活用できるようにするため、電子申請等 API や自己情報取得 API、医療保険情報取得 API といった各種 API を開発し、審査をした上で、その仕様を公開している。

2024 年（令和 6 年）においても、引き続き、住民/国民向けに安定したサービスを提供しつつ、早急に新たな価値を提供するため、本プロジェクトを、迅速・柔軟・安全に遂行できる事業者の調達を実施するものである。

## 1.3. 調達目的および期待する効果

---

本業務は、マイナポータルを構成するシステムである情報提供等記録開示システムおよび API 基盤システムの機能改善や安定した運用保守を対象とするものである。

また利用シーンの拡大や利用者の増加に伴い、今後ますます重要な位置付けとなる本システムの利便性向上を図りつつ、令和 8 年 1 月に予定する次期システムへの更改を念頭に置きながら、各連携システムを担当する多くのステークホルダーとの調整を図り、プロダクト開発・運用を実施する必要がある。

今回の調達では、このような非常に重要かつ難易度が高い事業を完遂し、最終的には、いつでもどこでも誰でも自宅に居ながらスマートフォンで全ての行政手続が 60 秒以内に完結する世界を提供することができるように、主管課と相互に協力し合い、高い生産性を以て業務を遂行していくことを期待する。

## 1.4. 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。

表 1 マイナポータル利用状況

#	集計項目	件数	取得期間
1	有効アカウント数	約 6,976 万件	2023 年（令和 5 年）10 月 31 日時点
2	トップアクセス件数(Avg.) (過去 1 年間の月間平均)	約 2,870 万件/月	2022 年 11 月 1 日～2023 年 10 月 31 日
3	トップアクセス件数(peak) (過去 1 年間の月間ピーク)	約 6,063 万件/月	2022 年 11 月 1 日～2023 年 10 月 31 日
4	ログイン件数(Avg.) (過去 1 年間の月間平均)	約 1,168 万件/月	2022 年 11 月 1 日～2023 年 10 月 31 日
5	ログイン件数(peak) (過去 1 年間の月間ピーク)	約 2,319 万件/月	2022 年 11 月 1 日～2023 年 10 月 31 日

## 1.5. 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）

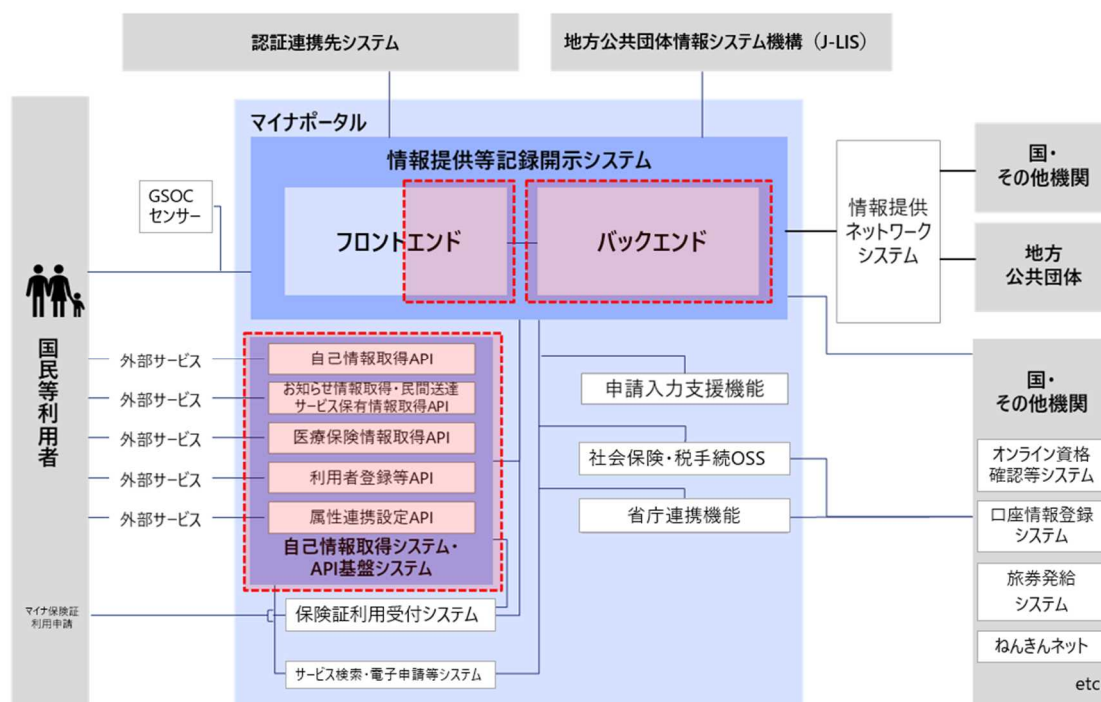
#	用語	説明
1	API 基盤システム	「情報提供等記録開示システムの再構築及び同システム等のサービス提供」に係る調達により構築・提供されており、マイナポータルの機能の一部及びマイナポータル API を提供するための機能又はシステムの総称。
2	GSOC センサー	内閣サイバーセキュリティセンターが運用する G S O C（Government Security Operation Coordination team）が政府情報システムに設置するセンサー。G S O C は当該センサーを通じ、24 時間 365 日体制の下、政府機関に対するサイバー攻撃等の不審な通信の横断的な監視、分析、情報収集を実施するとともに、各府省庁への通報、情報提供、助言などを行っている。
3	サービス検索・電子申請機能等システム	「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・提供されており、マイナポータルの行政手続のオンライン申請のために活用される機能又はシステムの総称。
4	自己情報取得システム	「情報提供等記録開示システムの再構築及び同システム等のサービス提供」に係る調達により構築・提供されており、行政機関等が保有する自身の公的な情報をマイナポータルで取得・閲覧するための機能又はシステムの総称。
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）を主な機能としている。
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、A P I 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。
10	バックエンド	データベースや Web サーバ、アプリケーションサーバ等サーバサイドシステムを指す。

11	フロントエンド	Web ブラウザなどのユーザーインターフェース (UI) を指す。
12	マイナポータル	情報提供等記録開示システム、サービス検索・電子申請等システム、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。
13	マイナポータル API	行政手続のオンライン申請や情報の取得といったマイナポータルが提供する機能を官民の Web サービス等においても活用できるようにデジタル庁が公開している各種 API の総称。
14	マイナポータルアプリ	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。
15	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。

## 1.6. 業務・情報システムの概要

本業務及び情報システムの概要は下図のとおりであり、赤枠で示した情報提供等記録開示システム、自己情報取得システム、API 基盤システムの設計・開発及び運用・保守が本プロジェクトの対象となる。なおフロントエンドの一部は、後述する「令和6年度マイナポータル新フロントの改善及び運用」に係る業務において実施するため、本事業には含まないことに留意すること。

図 1 業務・情報システムの概要



## 1.7. 契約期間

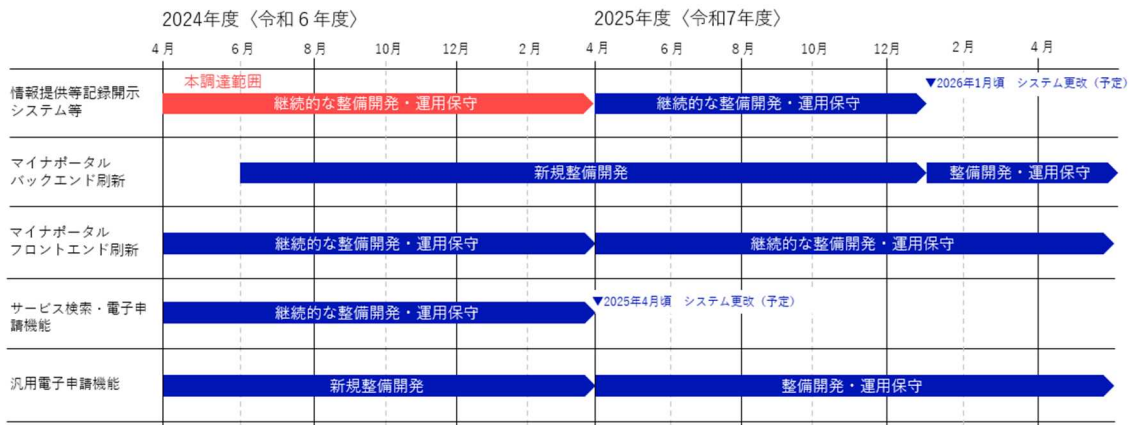
本プロジェクトの契約期間は、契約締結日から 2025 年（令和 7 年）3 月 31 日までとする。

## 1.8. 作業スケジュール

本プロジェクト及び関連システムに関する作業スケジュールは「図 2 作業スケジュール」のとおりである。なお本システムは 2026 年（令和 8 年）1 月を目途にシステム更改を予定しているため、システム更改を踏まえた効率的なシステム設計・開発、運用・保守を実施すること。

受託者は、本調達に関する詳細なスケジュールを提案するとともに、主管課と協議の上で、プロジェクト実施計画書を作成し、契約締結後 2 週間以内に提出すること。

図 2 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

本調達が対象とする業務範囲は、情報提供等記録開示システムに関する設計・開発、運用・保守業務及びそれに付帯する業務の内、デジタル庁マイナポータル担当が主管課として実施する業務全てとする。（ただし「令和 6 年度マイナポータル新フロントの改善及び運用」に係る業務は除く。）

なお、上記は調達範囲の基本方針であり、調達範囲の調整が必要となった場合には、主管課と協議の上、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。（一部予定を含む）

表 3 関連する調達案件の一覧

#	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	情報提供等記録開示システムの再構築及び同システムのサービス提	一般競争入札 (総合評価)	平成 31 年 4 月	平成 30 年 12 月 平成 31 年 1 月 平成 31 年 3 月	平成 31 年 4 月から 令和 6 年 3 月まで

	供				
2	令和5年度マイナポータル新フロントの改善及び運用	随意契約 (技術的対話)	令和5年5月	- 令和5年1月 令和5年4月	令和5年5月から 令和6年3月まで
3	情報提供等記録開示システムバックエンド機能の再構築に関する調査研究	随意契約 (企画競争)	令和5年7月	- 令和5年6月 令和5年7月	令和5年7月から 令和6年2月まで
4	令和5年度マイナポータル関係システムに係る工程管理等支援業務	随意契約 (企画競争)	令和5年12月	- 令和5年11月 令和5年12月	令和5年12月から 令和6年3月まで
5	令和6年度マイナポータル新フロントの改善及び運用	随意契約 (技術的対話)	令和6年4月	- 令和5年1月 令和5年3月	令和6年4月から 令和7年3月まで
6	情報提供等記録開示システムバックエンド機能の再構築	随意契約 (企画競争)	令和6年6月	- 令和6年5月 令和6年5月	令和6年6月から 令和8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本業務と「表 3 関連する調達案件の一覧」項番3及び4に挙げる業務は、相互に入札制限の対象とする。また「8.4 入札制限」も参照すること。

## 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、「要件定義書（開示システム\_業務編）」、「要件定義書（開示システム\_基盤編）」、「要件定義書（API 基盤\_業務編）」、「要件定義書（API 基盤\_基盤編）」の各要件を満たすこと。

## 4. 作業の実施内容に関する事項

本調達の受託者は、表3項番1「情報提供等記録開示システムの再構築及び同システムのサービス提供」に係る調達により構築された機能及び提供するサービス（以下「既存の開示システム等関連業務」という。）を継続し、安定して稼働させることを前提とする。そのため、受託者は設計・開発、運用・保守業務等の実施に先立ち、既存の開示システム等関連業務の受託者と連携し、遅滞なく業務の引継ぎを受けることを必須の要件とする。

また、本業務を実施する中で、基本設計書・詳細設計書などの各種設計書及びソースコードなどのシステム整備開発・運用保守に係るドキュメントについて内容に変更が生じる場合は、その都度、当該ファイルを修正すること。修正にあたっては主管課のレビューを受けた上で、主管課の承認を得ること。

### 4.1. 設計・開発実施計画書等の作成

#### (1) 設計・開発実施計画書及び設計・開発実施要領

設計・開発実施計画書及び設計・開発実施要領を作成し、主管課の承認を得ること。

設計・開発実施計画書及び設計・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、主管課の承認を得ること。



設計・開発・テスト等には、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」(2023年(令和5年)3月31日付け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、主管課と協議の上、対応について決定すること。

受託者が作成する「設計・開発実施計画書(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
- ・ 体制体制
- ・ 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主管課に提出すること。

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、主管課の承認を得ること。

## (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、設計・開発実施計画書の策定時点で、プロジェクトの特性に合わせて主管課と協議の上決定すること。

受託者と主管課間でプロジェクト管理ツール(JiraSoftwareなど)により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主管課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。

- ・ 課題管理
    - 解決すべき課題・問題は、再発防止に活かすことも含めて、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、主管課の承認を得ること。
  - ・ 変更管理/構成管理
    - 変更管理/構成管理について、本プロジェクト開始時に、各機能や提供するサービスに必要な工数の積算や優先度付けを行い、優先度に従った作業計画（実施内容、工数、スケジュール等）を策定すること。また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、工数の積算や優先度について当庁と検討した上で、その都度、柔軟に計画の見直しを行うこと。また上述のような管理をするためのツールを含めて提案すること。
    - また管理手順を明確に記載した上で、主管課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。その際、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
    - 契約期間内における各月の業務に関する月別請求金額は、別途、月別請求金額内訳表において定めるものとする。月別請求金額に変更がある場合は、デジタル庁と受託者との協議により決定するものとし、別途、月別請求金額内訳表及び議事録等に定めるものとする。
    - 作業範囲や金額算出の前提条件について本契約締結時点のものから変更がある場合で、かつ、契約金額が変更となる場合には、契約金額を変更するものとし、書面による変更契約をもって行うものとする。
  - ・ 問合せ管理
    - 業務を遂行する中で、主管課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、原則週 1 回以上の報告を行うこと。報告は原則としてオンライン会議での実施とするが、主管課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、主管課と受託者で協議の上、対面で開催すること。また、別途主管課が報告を求める場合においては、主管課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主管課と協議の上、決定すること。また、主管課が求める場合は、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. 要件定義

---

受託者は、設計・開発の実施に先立ち、「要件定義書（開示システム\_業務編）」、「要件定義書（開示システム\_基盤編）」、「要件定義書（API\_基盤\_業務編）」、「要件定義書（API\_基盤\_基盤編）」の内容を確認すること。その際、内容について調整すべき事項があれば、主管課（および工程管理支援事業者）、関係省庁、関係機関、その他ステークホルダーと調整の上、合意形成を図りつつ、結果に基づき要件定義書の修正を行うこと。

## 4.3. 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、成果物について主管課からの承認を得ること。

主管課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は分かりやすく作成すること。

#### イ プロトタイプ作成

新規機能等については、設計内容が実現したい要件を満たしているか、利用者の利便性が向上するような UI/UX となっているか等を確認するために、必要に応じてプロトタイプにより主管課とともに検証を行い、結果を主管課に報告すること。

#### ウ 外部インター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ー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ーフェース仕様書を作成すること。

#### エ 設計・開発に用いる環境

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 種類を利用すること。ただし、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」とする。

本番環境及び検証環境では、アプリケーションプログラムのリリース、稼働後の動作確認等を行う。

開発環境では、アプリケーションプログラムの開発・テスト等を行うこと。

#### オ ライフサイクルコストの考慮

受託者は、本システムの設計・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。

#### カ 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。

#### キ モニタリングが容易に行える構成

システムの利用状況、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、取得した利用状況を週次で主管課に報告すること。（既存の開示

システム等関連業務において報告する全ての利用状況を報告の対象とする。) また、それらの情報について、プロジェクトの目標となる指標についても提案できることが望ましい。なお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 既存システムの運用・保守作業内容の棚卸し

受託者は、既存システムの運用・保守作業内容をベースラインとして、作業内容の棚卸しを行うこと。

本サービスを運用するに当たって不要となる作業、作業内容の変更を要する作業、新たに追加する作業を整理すること。

### イ 運用・保守計画

受託者は、運用設計及び保守設計を行った上で、以下の内容を取りまとめた運用・保守計画書の案を作成し、主管課の承認を受けること。

- 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

#### ウ 運用・保守設計

受託者は、「ア 既存システムの運用・保守作業内容の棚卸し」、「イ 運用・保守計画」に記載された事項や、要件定義書に記載の運用・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、主管課の承認を受けること。

運用・保守設計に当たっては、主管課作業の軽減等、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）
- 災害発生時における作業内容（IT 業務継続計画）
- 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

#### エ 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、主管課の承認を得ること。

- 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

#### オ 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。政府としても、デジタル社会の実現に向けた重点計画（2023年（令和5年）6月9日決定）において「2020年度（令和2年度）時点での政府情報システムの運用等経費及び整備経費のうちのシステム改修に係る経費計約5,400億円を、2025年度（令和7年度）までに3割削減することを目指す。」としているため、当該システムの運用・保守においても必要最小限のコストで、効果を最大化し、コスト構造の最適化を図ること。具体的には、コスト構造の確認・分析を踏まえたコスト削減方策について、効果を定量的に把握した上で策定し、主管課と協議の上で実行を図ること。

#### カ 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、主管課の承認を得ること。

- 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、主管課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、主管課の承認を得ること。

#### (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

要件定義書の内容を参照し、システム方式に関する基本設計結果を記載したものと基本設計書（システム方式）を作成し、主管課の承認を得ること。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詳細設計書（システム方式）を作成し、主管課の承認を得ること。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が提供する稼働環境（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、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が提供する資源（OS、ミドルウェア）や持込みソフトウェア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。
- ・ 本システムが個別に配置し、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」）のセットアップを行うための手順を記載したものと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。

#### 4.4. 開発・テスト

---

##### (1) 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）の実施主体、手順、方法を定め、主管課の承認を得ること。

##### (2) 開発手法

本プロジェクトでは、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すること。

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。

### (3) 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。

### (4) 開発の実施

受託者は、主管課の承認を得た基本設計書及び詳細設計書に基づき、本システムのプログラム設計、開発を実施すること。当該作業は、受託者の拠点に整備する開発環境にて行うこと。

開発に必要な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。

### (5) 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、主管課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。

- 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主管課に報告すること。

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。

## 4.5. 受入テスト支援

---

受託者は、主管課が受入テストのテスト計画書を作成するに当たり、情報提供等の支援を行うこと。

受託者は、主管課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。

## 4.6. 引継ぎ（受託者から他事業者へ）

---

受託者は、本事業の契約期間後も主管課もしくは他事業者にて円滑な整備・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ともに、回線の利用や機器の保守、提供するサービスの運用などの本事業で提供するサービスを円滑に継続して提供することができるように必要な引継ぎに係る作業を行うこと。なお実際の作業内容については主管課と協議の上、承認を得ること。

## 4.7. 運用

---

受託者は、要件定義書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。

## 4.8. 保守

---

受託者は、要件定義書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。

## 4.9. 会議開催

---

- (1) 受託者は、定例会を原則週 1 回以上開催するとともに、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) 主管課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。
- (3) 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。主管課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、主管課と受託者で協議の上、対面で開催すること。
- (4) 受託者は、会議終了後、5 営業日以内に議事録を作成、提示し、主管課の承認を受けること。

## 4.10. 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、主管課の許可なく追加、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、主管課が管理する 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、保守・運用を行うこと。

## 4.11. 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、主管課の承認を得ること。

- ・ 本調達又は工程の概要
- ・ スcope目標、スcope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

## 4.12. 成果物の作成

---

### (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、設計・開発実施計画書にて定める。

なお、成果物は現時点の案であるため、主管課が承認した場合は、成果物の種類及び内容を変更することができる。(下表に含まれない場合であっても、受託者と主管課が協議の上、必要に応じ納品物とする。)

表 4 成果物一覧

#	成果物名	納品期限 (想定)
1	プロジェクト実施計画書	契約締結後 2 週間以



		内
2	設計・開発実施計画書	契約締結後2週間以内
3	設計・開発実施要領	契約締結後2週間以内
4	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
5	情報セキュリティ管理計画書	契約締結後2週間以内
6	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、その他会議資料）	会議実施前まで 議事録については会議後3開庁日以内
7	要件確認書	設計・開発の状況に応じて順次
8	要件定義書（マスタとなる要件定義書を適時に更新し、契約期間終了時にはそれらを引継ぐことができるように整備すること）	ファイル更新時に随時
9	設計書等（画面フロー、画面構成、基本設計書、詳細設計書、実体関連図（ERD）、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、システム基盤制御機能設計書、シェル・スクリプト、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、機器構成図、ネットワーク構成図、施工図面、機器設置レイアウト図、ラック搭載図、配線図、データセンター設置対象機器一覧、消費電力一覧、排熱量一覧、ケーブル敷設経路図、ソフトウェア一覧、ライセンス一覧など）	設計・開発の状況に応じて、適時必要書類を順次
10	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
11	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
12	プロトタイプを作成する場合、当該プロトタイプの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	実行プログラム一式	設計・開発の状況に応じて順次
14	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
15	作業結果報告書	設計・開発の状況に応じて順次
16	テスト計画書、テスト仕様書	各テスト開始前まで
17	単体テスト手順書、単体テスト項目表（実績記入）	単体テスト開始前まで
18	受入テスト計画書（案）、受入テスト仕様書（案）	受入テスト開始前まで
19	テスト結果報告書	各テスト工程完了判定前まで
20	テストデータ	テストの状況に応じて順次
21	脆弱性検査結果報告書	総合テスト工程完了判定前まで
22	操作マニュアル（利用者向け及び行政職員向け）	運用・保守の状況に応じて順次
23	ランニングコスト試算表	契約締結後2週間以内
24	運用・保守計画書	総合テスト開始前まで
25	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）	運用・保守開始前まで
26	パッチ適用計画	運用・保守の状況に応じて順次
27	リリース管理台帳、リリース計画書（マスタとなる管理台帳及び計画書を適時に	ファイル更新時に随時

	更新し、契約期間終了時にはそれらを引継ぐことができるように整備すること)	
28	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
29	災害時復旧手順書	ファイル更新時に随時
30	IT業務継続計画	ファイル更新時に随時
31	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
32	運用・保守報告書（月次報告書、定期保守報告書、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
33	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
34	移行支援計画書、移行支援完了報告書	契約満了前
35	移行用データ	契約満了前
36	バックアップ切替訓練結果報告書	契約満了前
37	機器撤去計画書、機器撤去完了報告書	契約満了前
38	設備整備完了報告書	契約満了前
39	引継ぎ資料	契約満了前
40	業務完了報告書	契約満了前

## (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7日）」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、主管課が指定する保存場所に納品すること。
- ・ 納品後、主管課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、主管課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、主管課の承認を得ること。
- ・ 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、内容について主管課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主管課の承認を得ること。
- ・ 成果物については、必要に応じて更新を行い主管課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。

### 4.13. 情報資産管理標準シートの提出

受託者は、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、主管課と協議の上、対応を実施すること。

#### (1) 開発・運用に関する情報

- ・ 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
- ・ 運用
  - 個人利用者数、法人利用者数、サービス利用件数、ヘルプデスク問合せ件数
  - アクセス件数、利用省庁数、利用省庁
- ・ 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、クラウドファイアーウォール、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。再委託先がある場合は再委託先の法人番号と再委託金額を提示すること。

### 4.14. 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 に掲載される令和 6 年 2 月「グリーン購入の調達者の手引き」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/content/000197086.pdf>

(2) インターネット公開するシステムは原則として政府系ドメイン（go.jp）を用いること。

- (3) 受託者は、本システムの整備・管理に当たり、主管課が必要と認める関係者（デジタル庁内の関係部局等を想定）からの説明要請や質問等があった場合には、主管課が実施する資料作成、回答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「図 3 作業体制図」及び「表 5 本業務における組織等の体制と役割」を想定しているが、詳細は主管課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「設計・開発実施計画書 イ 作業体制に関する事項」に記載し、「4.14. 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。

また、作業開始後、作業要員の成果に疑義があると主管課が判断した場合、双方協議に諮る。その上で作業要員の交代が必要になった場合は、受託者は速やかに作業要員の交代に応じること。

図 3 マイナポータル作業体制図（全体）

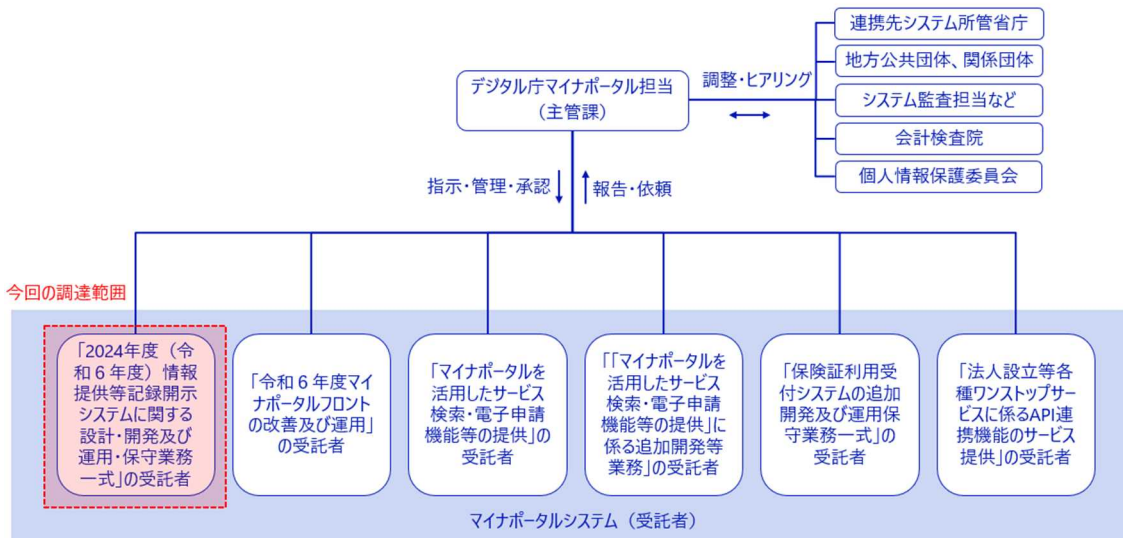


図 4 本プロジェクト作業体制図（詳細）

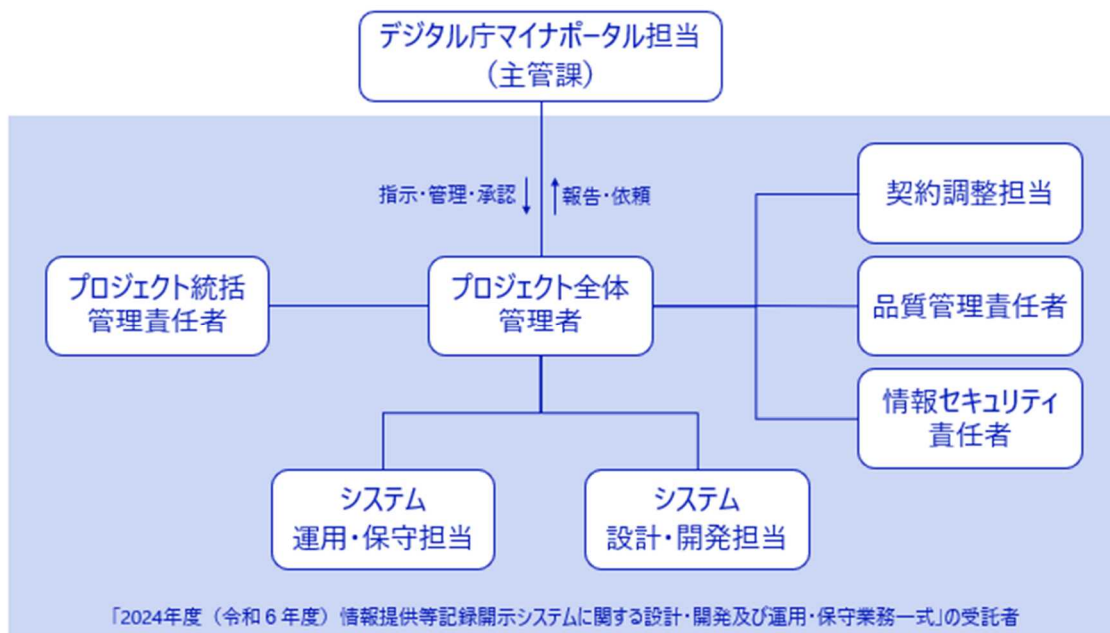


表 5 本業務における組織等の体制と役割

項番	組織又は要員	役割
1	主管課	<ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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。</li> <li>・ プロジェクトの全体進捗管理を行う。</li> <li>・ 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。</li> <li>・ 業務機能の仕様を検討、確認する。</li> </ul>
2	プロジェクト統括管理責任者	<ul style="list-style-type: none"> <li>・ 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。</li> </ul>
3	プロジェクト全体管理者	<ul style="list-style-type: none"> <li>・ 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、主管課との調整を行う。</li> <li>・ 本業務の委託期間中、専任でこれに当たるものとする。</li> </ul>
4	契約調整担当	<ul style="list-style-type: none"> <li>・ 本プロジェクトの遂行に当たり、主管課との契約調整を担う。</li> <li>・ リーダーは本プロジェクトの全体像を把握し、契約事務に係る主管課との調整、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。</li> </ul>
5	システム設計・開発担当	<ul style="list-style-type: none"> <li>・ 本システムの設計・開発を担う。またパッチ適用、障害対応等において他事業者の支援を行う。</li> <li>・ リーダーはシステム設計・開発担当の各業務の全体像を把握し、設計・開発に係る主管課との調整、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。</li> <li>・ 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。</li> </ul>
6	システム運用・保守担当	<ul style="list-style-type: none"> <li>・ 本システムの運用・保守を担う。</li> <li>・ 各機能・サブシステムの設計・開発担当と連携し、障害の一次切り分けやブラッシュアップ、機能改善の他、パッチ適用・障害対応・環境設定情報の設定変更等の保守業務に当たること。</li> <li>・ リーダーはシステム運用期間中、専任でこれに当たるものとする。</li> </ul>
7	品質管理責任者	<ul style="list-style-type: none"> <li>・ 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。</li> </ul>
8	情報セキュリティ責任者	<ul style="list-style-type: none"> <li>・ 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。</li> </ul>

## 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には、本システムと同等規模のシステム（本システムのスマートフォンアプリを含む。）、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、明らかなる者

### (2) システム設計・開発・保守班リーダー

システム設計・開発・保守班リーダーは、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・保守班（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・開発担当者は、次のいずれかに該当すること。

- ・ 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が認定している資格の中で、上級資格を保有していること。
- ・ 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) システム運用班リーダー

システム運用班リーダーは、運用の経験年数を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。

- ・ ITサービスマネージャ試験の合格者
- ・ ITIL4 マネージングプロフェッショナル
- ・ 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) 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

ア 設計・開発業務

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。

イ 運用・保守業務

運用・保守業務の作業場所は、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。

#### ウ 非常時の業務

非常時の参集場所は、以下のとおりとする。

- 優先順位 1 位：デジタル庁 19 階 19S- 2
- 優先順位 2 位：デジタル庁 19 階 19S- 1
- 優先順位 3 位：デジタル庁 19 階 RED ゾーン ハイテーブル
- オンライン(Web 会議等)の場合：teams/slack による Web 会議

### (2) 諸設備、物品等資源

#### 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を遵守の上、主管課の了承を得ること。

## 5.4. 作業の管理に関する事項

---

- (3) 受託者は、主管課が承認した設計・開発実施計画書の作業体制、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。また、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、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を行うこと。また、運用・保守開始後においては運用・保守計画書及び運用・保守実施要領に基づき各種管理を行うこと。
- (4) 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、以下を基本としつつ、コミュニケーションツールを活用し、感染症流行状況などにおいても継続性の高い開発・保守・運用体制を構築すること。

#### メッセージング

Slack を基本とし、必要のある場合にのみ Teams 及びメールを用いる。

#### 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。

## 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) 委託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主管課に報告すること。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、必要に応じて主管課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、主管課と協議の上、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主管課の承認を得ること。なお、設計・開発実施計画書や運用・保守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拠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、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主管課と協議の上決定し、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、主管課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、主管課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、主管課と協議のうえ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、事前に主管課の許可を得ること。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、速やかに主管課に通知してその指示を受けること。また、主管課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、本業務の一部を再委託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、主管課の承認を得た上で実施すること。
- (9) 主管課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、主管課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、主管課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、以下の適用される法令などを遵守し履行すること。

- ・ 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）
- ・ 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）
- ・ 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）
- ・ 電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号）
- ・ 住民基本台帳法（昭和 42 年法律第 81 号）等

#### 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

---

- (1) 本調達において整備・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、主管課が情報システム監査の実施を必要と判断した場合は、主管課が定めた実施内容（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。（契約後の委託事業開始前より実施される主管課が別途選定した事業者による監査を含む。）
- (2) 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、対応案を主管課と協議し、指示された期間までには是正を図ること。

#### 6.7. 情報セキュリティの管理体制について

---

- (1) 情報システムの設計・開発、運用・保守工程において、主管課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。
- (2) 主管課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）を主管課との協議の上、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。
- (3) 情報システムに主管課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、主管課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主管課との協議の上、必要と判断された場合は提出すること。

- (4) 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。
- (5) セキュリティ関連のテストの実施結果が確認できること。脆弱性検査については、「デジタル庁 政府情報システムにおける脆弱性診断ガイドライン」の実施基準を満たすように、脆弱性診断の実施、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実施内容及び結果を脆弱性検査結果報告書に取りまとめること。
- (6) 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
- (7) 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表 6 に示す。各項目に対して漏れなく対応すること。

表 6 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	<ul style="list-style-type: none"> <li>・ 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</li> <li>・ 推測されやすい脆弱なパスワードが使用されている</li> <li>・ 認証情報がファイル等に平文で書かれている</li> </ul>
2	アクセス制御不備	<ul style="list-style-type: none"> <li>・ 必要な強度の認証が行われていない</li> <li>・ 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</li> <li>・ 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</li> </ul>
3	暗号化不備	<ul style="list-style-type: none"> <li>・ 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</li> </ul>
4	資産管理、脆弱性管理不備	<ul style="list-style-type: none"> <li>・ 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）</li> <li>・ 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</li> </ul>
5	Web アプリケーションの脆弱性	<ul style="list-style-type: none"> <li>・ 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</li> <li>・ 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</li> </ul>
6	ログ管理不備	<ul style="list-style-type: none"> <li>・ 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）</li> <li>・ 定期的なログの点検又は分析が実施されていない</li> </ul>
7	外部委託の管理不備	<ul style="list-style-type: none"> <li>・ 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</li> <li>・ 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</li> </ul>

## 6.8. セキュリティ要件

セキュリティ要件については、「要件定義書（開示システム\_基盤編）」及び「要件定義書（API 基盤\_基盤編）」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) 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。
- ・ 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。
  - ・ 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。
  - ・ 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。
  - ・ 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。
- (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、変更点について主管課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。なお、受託者から提出された納入成果物については、デジタル庁が承認したことをもって検収合格とする。

## 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。

- ・ 財団法人日本情報処理開発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

---

- (3) 応札者は、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。
- (4) 応札者は、1000 万人以上の利用者が利用するデータベース機能を有する情報システムの設計・開発を行った実績を過去 3 年以内に有すること。
- (5) 応札者は、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。

## 8.3. 複数事業者による共同入札

---

- (1) 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こと。また、本代表者が本調達に対する入札を行うこと。
- (2) 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。
- (3) 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の参加を行っていないこと。
- (4) 代表者以外の共同入札を構成する全ての事業者も、公的な資格や認証、受注実績を除いて全ての応札条件を満たすこと。また、入札参加資格及び誓約書の提出に際しては全ての事業者分を提出すること。

## 8.4. 入札制限

---

本調達は、「デジタル庁における入札制限等に関する規程」に従い、入札の制限を行う。

# 9. 再委託に関する事項

## 9.1. 再委託の制限及び再委託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委託してはならない。
- (2) 受託者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。
- (3) 受託者は再委託先の行為について一切の責任を負うものとする。
- (4) 再委託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、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委託先に担保させること。また、再委託先のセキュリティの対策実施状況を確認できるよう、再委託先との契約内容に含めること。（再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる（以下「再々委託」という。）場合の取扱いも同様）

- (5) 入札金額の 20%を超える再委託を予定する事業者がいる場合、当該再委託先事業者についても同様に「2.3 調達案件間の入札制限」及び「8.4 入札制限」に示す要件を満たすこと。

## 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委託する場合には、以下①～③の内容を記載した「再委託承認申請書」を主管課に提出するとともに、④～⑨に記載した文書についても併せて提出し、あらかじめ承認を受けること。
- ①再委託の相手方の商号又は名称、住所
  - ②再委託を行う業務の範囲
  - ③再委託の必要性及び契約金額等
  - ④再委託に係る履行体制図
  - ⑤再委託先の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を証明するもの
    - ・ 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
    - ・ 財団法人日本情報処理開発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
  - ⑥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
  - ⑦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
  - ⑧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
  - ⑨その他デジタル庁が求める情報
- (2) 前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を主管課に提出し、承認を受けること。
- (3) 再々委託には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。

## 9.3. 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。また、主管課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。

# 10. クラウドサービスの選定、利用に関するセキュリティ関連事項（要機密情報を取り扱う場合）

## 10.1. クラウドサービスの選定、利用に関する共通セキュリティ要件

---

- (1) 要機密情報を取り扱うクラウドサービスの選定、利用に関しては、「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（令和 5 年度版）」の「4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）」「4.2.2 クラウドサービスの利用（要機密情報を取り扱う場合）」の内容を遵守すること。
- (2) セキュリティ確保のため、本システムで用いるクラウドサービスは、原則として ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録されているクラウドサービスを選定すること。な

お、例外的に ISMAP クラウドサービスリスト、または ISMAP-LIU クラウドサービスリストに登録されていないクラウドサービスを選定する場合は、受託者の責任において、当該クラウドサービスが「ISMAP 管理基準」の管理策基準における統制目標（3 桁の番号で表現される項目）及び末尾に B が付された詳細管理策（4 桁の番号で表現される項目）と同等以上のセキュリティ水準を確保していることを選定すること。

(3) (2) のセキュリティ要件に加えて、クラウドセキュリティ、データ保護に関する以下の要件を満たすようにクラウドサービスを選定し、利用すること。

- ・ 「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」（以下、「クラウド方針」という。）を遵守すること。
- ・ 情報資産を管理するデータセンタの設置場所に関しては、国内であることを基本とする。設置場所の考え方についてはクラウド方針を参照すること。
- ・ 契約の解釈が日本法に基づくものであること。
- ・ クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。
- ・ 主管課の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。情報資産を国外に設置されるクラウドサービスに保管する際の考え方についてはクラウド方針を参照すること。なお、利用者がアクセス可能な部分を除き、国外から情報資産へアクセスする場合も日本国外への持ち出しに該当する。
- ・ 障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。
- ・ 情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、主管課が要求する任意の時点で情報資産を他の環境に移管させることができること。

(4) SaaS サービスの選定に関する参考事項

- ・ SaaS ベースで構築することを前提に検討し、SaaS では要件を満たさない場合は、PaaS、IaaS などを選択すること。なお、本調達で構築するシステムでは、比較的短期間での機能の追加が求められることが想定されることから、簡易な操作で機能の追加が可能であること。
- ・ 今後、利用者の拡大が見込まれることから、今後の発行アカウント数の拡大時の安定稼働や運用費用の抑制等の観点から、本調達の趣旨に適したクラウドサービスを利用すること。

## 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・リスクの観点から内閣サイバーセキュリティセンターに対して、講ずべき必要な措置について助言を求めため、技術等提案書提出時において「機器等リスト」に想定の機器等を記載の上、提出すること。



と。主管課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、主管課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、内閣サイバーセキュリティセンター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. 入札公告期間中の資料閲覧等

---

本業務の実施に参考となる過去の類似業務の報告書等に関する資料については、デジタル庁内にて閲覧可能とする。なお、資料の閲覧に当たっては、必ず事前に主管課まで連絡の上、閲覧日時を調整すること。

### (1) 資料閲覧場所

東京都千代田区紀尾井町 1-3 ガーデンテラス紀尾井町 19F,20F

### (2) 閲覧期間及び時間

公募期間を予定

行政機関の休日を除く日の 10 時から 17 時まで（12 時から 13 時を除く。）

### (3) 閲覧手続

閲覧者は最大 3 名までとする。応札希望者の商号、連絡先、閲覧希望者氏名を「閲覧申請書（守秘義務に関する誓約書）」に記載の上、閲覧希望日の 3 日前（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。）までに提出すること。（「守秘義務に関する誓約書」については、閲覧日当日までに記載の上、提出すること。）

### (4) 閲覧時の注意

閲覧にて知り得た内容については、提案書の作成以外には利用しないこと。また、本調達に関与しない者等に情報が漏えいしないように留意すること。（3）閲覧手続にて提出した資料閲覧申請書に準拠すること。

### (5) 連絡先

東京都千代田区紀尾井町 1-3 ガーデンテラス紀尾井町 19F

電話 03-6771-8482（山口）、03-6872-6327（金築）

Mail mynaportal\_procurement@digital.go.jp

### (6) 事業者が閲覧できる資料一覧

閲覧に供する資料の例を次に示す。ただし、先行する案件は閲覧期間中も契約期間内であり、閲覧可能とする資料についても受注時点では変更されている可能性がある。

現行システムの以下の資料

1. 要件定義書（開示システム\_業務編）
2. 要件定義書（開示システム\_基盤編）
3. 要件定義書（API 基盤\_業務編）
4. 要件定義書（API 基盤\_基盤編）
5. 職員向け研修資料

### 11.3. 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「デジタル庁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 3 年 9 月 1 日内閣総理大臣決定）第 3 条に規定する合理的配慮について留意すること。