

調達仕様書

令和 8 年度 標準型電子カルテ導入版の設計・開発業務

2026 年 2 月

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・情報システムの概要	1
1.5.	契約期間	2
1.6.	作業スケジュール	2
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
2.1.	調達範囲	2
2.2.	関連調達案件	3
3.	情報システムに求める要件	3
4.	作業の実施内容に関する事項	3
4.1.	設計・開発実施計画書等の作成	4
4.2.	現行事業者からの引継ぎ	6
4.3.	設計	6
4.4.	開発・テスト	10
4.5.	JIS X 8341-3:2016 試験の実施	11
4.6.	モデル事業の稼働支援（運用・保守）	12
4.7.	引継ぎ	13
4.8.	外部連携システムとの連携に係る検討	13
4.9.	会議開催	13
4.10.	データ管理方法	14
4.11.	業務完了報告書の作成	14
4.12.	成果物の作成	14
4.13.	情報資産管理標準シートの提出	16
4.14.	その他	17
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	18
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	22
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.....	25
7.1.	知的財産権の帰属.....	25
7.2.	契約不適合責任.....	25
7.3.	検収.....	25
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.....	26
8.3.	複数事業者による共同入札.....	26
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.....	27
9.3.	再委託先の契約違反等.....	27
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.	その他特記事項.....	29
12.	附属文書.....	29

1. 調達案件の概要

1.1. 調達件名

令和 8 年度 標準型電子カルテ導入版の設計・開発業務

1.2. 調達の背景

デジタル庁国民向けサービスグループ（「主管課」という。）では、標準型電子カルテ導入版（以下「導入版」という。）を構築し、令和 8 年秋ごろよりモデル事業を開始することから、当該システムの稼働支援を実施する。

また、導入版においては、医療機関における所見の入力、電子カルテ共有サービスへのデータ連携・参照、電子処方箋管理サービスへの院外処方箋の連携・調剤情報の取得、検体検査の結果取得等、最小限の機能に限定して実装する。これらの実装にあたり、令和 7 年度の基本要件を前提に設計・開発を進めるとともに、令和 8 年度中でのリリースを行う。

併せて、標準型電子カルテの普及に向けて、医療機関における利便性向上に資するとともに、国民に質の高い医療を提供するための基盤の整備を目的として、外部システムを含めた他システムとの連携等を図る。

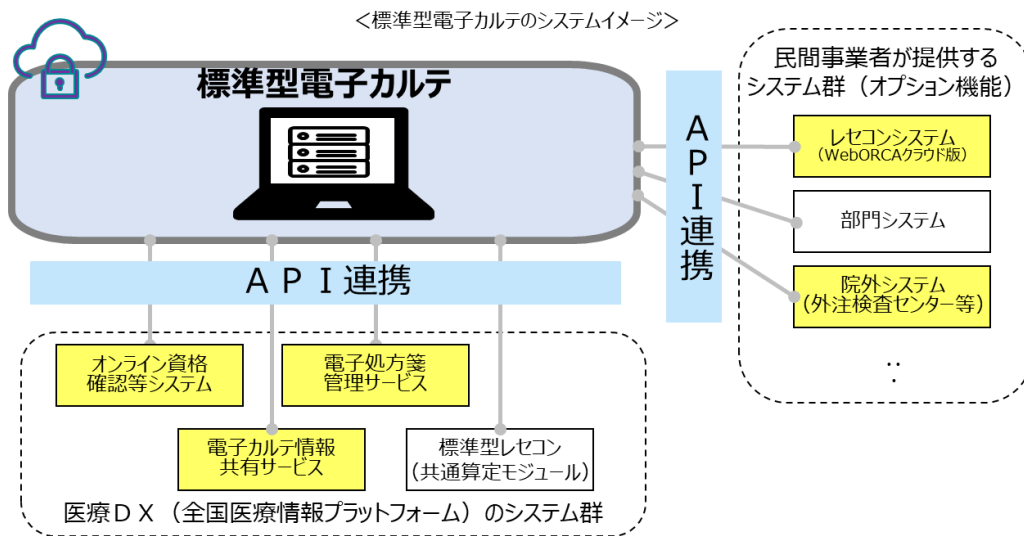
1.3. 調達目的および期待する効果

本業務は、令和 8 年度末頃の「標準型電子カルテ（導入版）」の本格リリースに向け、令和 7 年度設計・開発実績および過去半年間にわたる工数精査の結果を反映し、α版の機能拡充に係る設計・開発を完遂させることを主目的とする。具体的には、モデル事業で得られた知見を迅速に反映するとともに、令和 7 年度に策定した基本要件をベースとして、開発・テストまでを一貫して実施する。あわせて、モデル事業の稼働支援（運用・保守）を通じて実運用の品質・進捗管理を徹底し、次々年度以降の保守効率化（ランニングコスト抑制）を見据えたシステム基盤の高度化を図ることで、標準型電子カルテ導入版の社会実装を確実かつ迅速に推進する。

1.4. 業務・情報システムの概要

本システムは、SaaS 型のクラウドサービスとして提供され、医療DX（全国医療情報プラットフォーム）のシステム群であるオンライン資格確認等システム、電子カルテ情報共有サービス、電子処方箋管理サービス及び各種院内システム並びに民間事業者が提供するシステム群と接続するものである。次に示す図は令和 6 年度時点のものであり、今後の機能追加に伴い、連携システムも増える想定である。

また、本システムは、ガバメントクラウド上での開発・実装を前提とした検討を行うものとする。具体的には、本調達に含まれる設計・開発工程において、ガバメントクラウドが提供する標準機能や共通部品の活用を考慮したアーキテクチャ設計を行うとともに、必要となるシステム構成の最適化や技術的検証を、主管課の指示に基づき、本業務の範囲内において実施する。



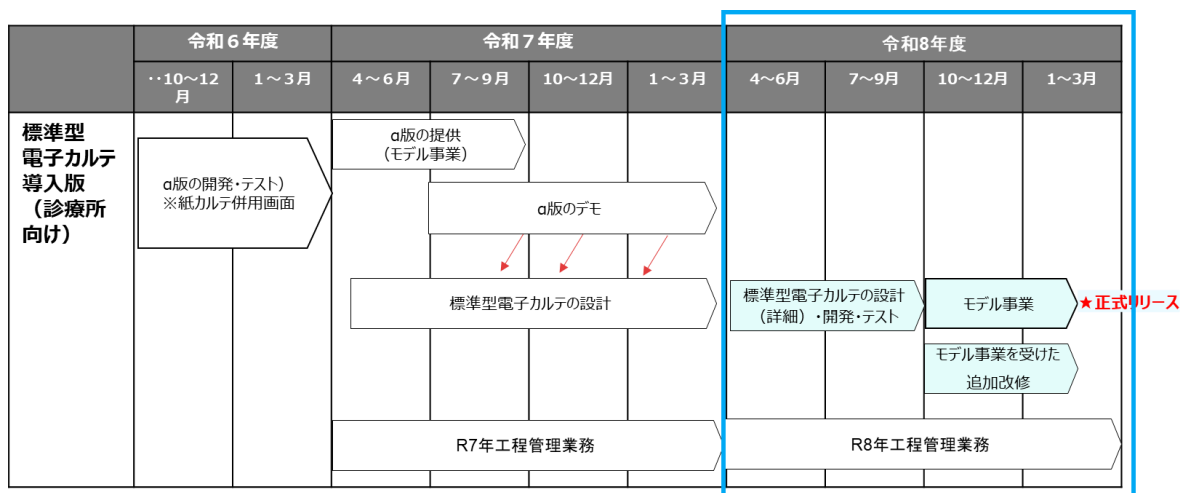
※黄色：令和6年度連携先システム

1.5. 契約期間

契約締結日から令和9年3月31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。以下はスケジュールの概要であり、実際の開発項目を踏まえて、詳細スケジュールは主管課と協議の上、決定すること。



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

以下の業務を実施するため、「プロジェクト計画書」を可能な限り具体的に策定するとともに、本調達に係る進捗管理、課題管理、品質管理等、設計・開発支援事業者として必要な管理を行うこと。

本調達の実行は、デジタル庁による対応の指示があった場合には、その指示に従って、必要な措置を講ずること。

なお、報告事項及び納品成果物等については受託者からデジタル庁に対して報告及び納品するものであるが、各工程の報告会議等においては厚生労働省及びデジタル庁の関係者も同席することから、直接、設計・開発を行っていない関係者に対して分かりやすい報告資料の作成について留意すること。

令和8年度以降も必要となる業務については、令和8年度以降の支援事業者に対しても適切な引継を行うこと。

2.2. 関連調達案件

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、実施時期等については、以下のとおり。

項番	調達案件	調達方式	実施時期	入札制限の該当有無
1	国内標準型電子カルテシステム等に係る導入支援等一式（厚生労働省）（予定）	一般競争入札（総合評価落札方式）（予定）	令和8年2月（予定）	なし
2	標準型電子カルテ（導入版）の設計・開発業務（本調達）	随意契約（公募）	令和8年2月	あり※
3	標準型電子カルテに係る支援業務	随意契約（企画競争方式）	令和8年2月	あり※

※本調達は「デジタル庁における入札制限等に関する規程」（令和4年3月9日改訂）に従い、入札制限を行う。また、相互けん制の観点から本調達と「標準型電子カルテに係る支援業務」は、相互に入札制限の対象とする。

3. 情報システムに求める要件

モデル事業の稼働支援（運用・保守）の実施に当たっては、令和7年度事業者による「運用・保守計画書」、「運用・保守実施要領」等を引継ぎつつ、各要件を満たすこと。また、設計・開発の実施に当たっては、要件定義書の各要件を満たすこと。なお、本格展開を見据えた医療機関の増加等を想定し、医療機関の認証方式や性能担保及び運用保守効率化等について優先的に対応すること。

4. 作業の実施内容に関する事項

本業務は、令和7年度に実施した設計・開発業務の計画等を踏まえて実施すること。

本業務の結果、令和7年度事業者から引継ぎ予定の「運用・保守計画書」等の記載内容に変更が生じる場合は、その都度設計・開発実施計画書や運用・保守計画書等を修正すること。修正に関し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。

設計・開発については、要件定義書の要件を満たすため、定められた期間での設計・開発が可能となるよう計画を策定しつつ、本格展開を見据えた性能拡張や運用保守に関する設計もあわせて行うこと。

上記は調達範囲の基本方針である。業務範囲の調整が必要となった場合には、主管課と協議の上、令和8年度において実施する業務範囲を決定すること。

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。

(各工程完了にアクセシビリティ品質レビューが必要となることに留意すること。)

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 5 年 3 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、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」等に基づき、次に掲げる事項を含めること。

- ・各工程の目的
- ・各工程における作業概要及び成果物
- ・各工程における作業体制
- ・成果物の作成様式
- ・成果物単位の作業プロセス
- ・スケジュール・WBS
- ・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・PWG 構成員への依頼事項等)

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。なお、工程管理・品質管理・課題管理等においては、チームを跨るタスクの管理方法についても詳細を記載すること。

- ・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

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。

なお、品質目標にはアクセシビリティ品質を含むことに留意すること。

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

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。

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。

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、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、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、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。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、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 要員やアクセシビリティ要員など）を参加させること。

4.2. 現行事業者からの引継ぎ

受託者は、令和 7 年度事業にて作成し、検収した成果物一式（各種計画、要件定義書、ソースコード、実行プログラム、各種環境アカウント、テスト結果等）を引継ぎ、本業務にて実行する各種設計・テストの結果を踏まえて、必要に応じて最新化すること。

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（運用保守設計を含む。）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 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。

ウ 設計・開発システム改修に用いる環境

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」、「デモ環境」及び「開発環境」の 4 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。

エ アクセシビリティの確保

受託者は、アクセシビリティ方針について、デジタル庁と協議の上で策定し、本システムにおけるフロントエンドの全画面が、JIS X 8341-3:2016 適合レベル AA に準拠し、かつ必要に応じて適合レベル AAA の達成基準あるいは WCAG 2.1、WCAG 2.2 の達成基準にも準拠するように設計・開発を実施すること。

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（アクセシビリティ確保の維持を含む）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

要件定義書に記載したプロジェクトの目標となる指標、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。

ク 安全目標設計の実施

ヒューマンエラー（ユースエラー）により引き起こされる問題に対処するための安全目標を定め、安全目標を達成するための防護策・仕組みを設計すること。

なお、安全目標設計書には、原則として以下の要件を含めるものとする。

- * 適切な設計活動が行われなかった場合、誤操作等によって引き起こされる脅威の特定
- * 特に対策を取るべき脅威の検討
- * 脅威の発生に至るユースケースの特定（イベントツリー・フォールトツリー）
- * 損失を防止・抑制するために設定されるべきリスク回避施策
- * エラーが発生しても安全側に収束するように工夫するための仕組み（フェイルセーフ）
- * 異常な使い方や誤使用があっても、問題を引き起こす機能を働かせない仕組み（フォールブールフ）
- * 被害防止・低減のための仕組み
- * エラーレジスタンスを高めるための教育訓練
- * 操作手順書・規約

(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、データー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やアクセシビリティ方針との整合性の確認等、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（モデル事業の稼働支援（運用・保守））

ア 運用・保守計画

受託者は、令和7年の運用・保守計画等をベースとして、以下の内容を踏まえて、必要に応じて見直しを行うこと。なお、この際、次々年度以降の本格稼働を見据えた検討を実施すること。

- 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（この作業により、本システムのフロントエンド画面に更新が発生する場合は、その都度、アクセシビリティ品質レビューが必要となることに留意）
- 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、運用・保守計画書や、要件定義書を踏まえ、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、主管課作業の軽減およびアクセシビリティ確保の維持等、効率的かつアクセシビリティ品質に優れたシステム運用・保守に資する内容を検討すること。また、障害やインシデント等の発生状況やユーザからの問い合わせ対応の状況を踏まえ、インシデント数が削減される等、システム運用・保守の改善に資する施策があれば積極的に提案すること。

- 定常時における定型的な作業内容（この作業により、本システムのフロントエンド画面に更新が発生する場合は、その都度、アクセシビリティ品質レビューが必要となることに留意）、および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（この修正により、本システムのフロントエンド画面に更新が発生する場合は、JIS X 8341-3:2016 試験が必要となることに留意）

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、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

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

受託者は令和7年度の運用・保守計画書等をベースとして、必要に応じて以下の内容を見直すこと。その際、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

要件定義書の内容に基づき、令和7年の基本設計書等の設計書類をベースとして、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。内容の更新・見直しをおこなう場合は、基本設計書（システム方式）には以下の内容を含むこと。なお、この際、次々年度以降の本格稼働を見据えた検討を実施すること。

- 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

上記の基本設計書（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として詳細設計書（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、主管課の承認を得ること。

(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、主管課の承認を得ること。

(3) 開発手法

本プロジェクトでは、ウォーターフォール型を前提に進めることとする。一方、併行で実施されるモデル事業で得られた知見を適宜開発に活かすため、画面設計においては、パイロット手法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、令和7年のインテグレーション・継続的デリバリー（CI/CD）をベースとし、効率的な開発作業や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。

(5) 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。

(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全体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。

また、以下のテストについては必ず実施すること

- 単体テスト
- 内部結合テスト
- 外部結合テスト
- シナリオテスト
- ユーザビリティテスト
- アクセシビリティテスト
- リグレッションテスト
- 負荷テスト
- 脆弱性診断
- UAT

(7) 開発・テストにかかるデータの管理方法

開発中の以下のデータは、主管課の指定する方法にて、常に最新の情報が共有できるよう管理すること。

- 仕様書について適切に版をわけてデジタル庁 SharePoint にて管理すること
- 開発中のソースコードについて git リポジトリ全体をデジタル庁 GitHub のリポジトリにて管理すること
- テストフェーズにて発生した不具合等についてはデジタル庁 JIRA にて管理すること

4.5. JIS X 8341-3:2016 試験の実施

受託者は、令和6年度事業者から引継ぎを受けたα版をベースにした JIS X 8341-3:2016 試験を実施すること。また、本試験で得られた課題について、本年度実施する設計に適宜フィードバックし、改善を行うこと。必要に応じて修正・再試験等も実施すること。

試験方法・手順は、ウェブアクセシビリティ基盤委員会（WAIC）による「JIS X 8341-3:2016 試験実施ガイドライン」を参照のうえで決定して実施すること。試験を実施するときは、JIS X 8341-3:2016 の達成基準に加えて WCAG 2.1 と WCAG 2.2 で追加された次の達成基準も考慮の上、達成基準について主管課の承認をえること。

WCAG 2.1

- 1.3.4 表示の向き (AA)
- 1.3.5 入力目的の特定 (AA)
- 1.3.6 目的の特定 (AAA)
- 1.4.10 リフロー (AA)
- 1.4.11 非テキストのコンテンツ (AA)
- 1.4.12 テキストの間隔 (AA)
- 1.4.13 ホバー又はフォーカスで表示されるコンテンツ (AA)
- 2.1.4 文字キーのショートカット (A)
- 2.2.6 タイムアウト (AAA)

- 2.3.3 インタラクションによるアニメーション (AAA)
- 2.5.1 ポインタのジェスチャ (A)
- 2.5.2 ポインタのキャンセル (A)
- 2.5.3 ラベルを含む名前 (name) (A)
- 2.5.4 動きによる起動 (A)
- 2.5.5 ターゲットのサイズ (高度) (AAA)
- 2.5.6 入力メカニズムの共存 (AAA)
- 4.1.3 ステータスメッセージ (AA)

WCAG 2.2

- 2.4.11 隠されないフォーカス (最低限) (AA)
- 2.4.12 隠されないフォーカス (高度) (AAA)
- 2.4.13 フォーカスの外観 (AAA)
- 2.5.7 ドラッグ動作 (AA)
- 2.5.8 ターゲットのサイズ (最低限) (AA)
- 3.2.6 一貫したヘルプ (A)
- 3.3.7 冗長な入力項目 (A)
- 3.3.8 アクセシブルな認証 (AAA)
- 3.3.9 アクセシブルな認証 (高度) (AAA)

なお、以下を作成し、主管課の承認を受けること。

- JIS X 8341-3:2016 試験計画書
- 達成基準チェックリスト、および試験結果の内容記入済みのもの
- ページリスト
- 検証結果の公表ページ

なお、ページリストおよび公表ページは、本システムのフロントエンド画面のいずれ(注)からリンクし公表しなければならない。

(注) デジタル庁サービス紹介サイト等、本システムのフロントエンド画面以外でも妥当と見なされるウェブサイトがあるため、最終的な公表場所は主管課と協議のうえで決定する。

4.6. モデル事業の稼働支援（運用・保守）

受託者は、令和 7 年度の「運用・保守計画書」等の記載内容をもとにモデル事業における稼働支援のために本システムの運用・保守及びモデル事業実施医療機関の支援を実施すること。主管課と協議、承認を得た上で、適切に対策を講じること。

モデル事業を開始した後は、「運用・保守計画書」に基づき、問合せ対応・インシデント対応・運用・保守状況報告を含む本システムの運用・保守を実施すること。また、モデル事業の結果、「運用・保守計画書」に変更が生じる場合は、その都度運用・保守計画書等を修正すること。修正に関し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。

また、モデル事業にあたっては厚生労働省にてモデル事業計画書の作成、厚生労働省にて別途調達

する機器等の調達・モデル事業実施医療機関への設置・導入を予定しているため、モデル事業計画書の作成にあたって必要な情報の提供、機器の設置・導入にあたって必要となる導入手順書の作成・事前説明等の支援を実施すること。

また、モデル事業を実施する医療機関を対象とした「操作マニュアル（利用者向け）」を整備する他、利用者が導入版を操作するにあたり有用と考えられる教育・訓練を実施すること、モデル事業医療機関で受入テストをすることを想定した支援、具体的にはモデル事業開始条件チェックリストを含む受入テスト計画書案及び受入テスト仕様書案の作成、操作マニュアルを用いた教育・訓練の実施、受入テスト計画書及び受入テスト仕様書を用いた受入テスト方法の説明、受入テスト計画書に基づく各種準備作業の実施（環境構築・データ準備等）、受入テスト時の問合せ・インシデント対応、受入テスト結果報告書案の作成（インシデント分析結果・モデル事業開始条件チェックリストの記入）等を実施すること。

なお、モデル事業におけるフィードバックを踏まえた機能改善及び運用・守の効率化についての積極的な提案を求める。

当該モデル事業の稼働支援（運用・保守）を実施する中でより効率的な運用・保守の施策及び利用者のニーズに合った施策等を研究し、次々年度以降の運用・保守計画に反映することが妥当である場合等、当初の「運用・保守計画書」に変更が生じる場合は、その都度運用・保守計画書等を修正すること。修正に関し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。

4.7. 引継ぎ

受託者は、要件定義書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こと。

当該引継ぎに当たっては、3.4 設計において設計した設計及び 4.7 モデル事業の稼働支援において得られた知見を反映した「設計・開発実施計画書」及び「運用・保守計画書」に基づき行うこと。

4.8. 外部連携システムとの連携に係る検討

本システムを利用した情報共有及び電子処方箋の発行等を実現するためには、オンライン資格確認等システム、電子カルテ情報共有サービス、電子処方箋管理サービス、医療機関の顔認証端末、マイナポータル、外注検査システム等の関連する外部連携システムにかかわる開発部門や開発事業者と各開発工程の前後関係を調整して進める必要がある。

具体的に、本システムの要件定義・外部仕様は連携システムの開発のインプットとなるため協議の上確定し、適切なタイミングで検討を行うこと。また、各連携システムで次年度以降に実施予定の本システムとの結合テスト及び総合テストが滞りなく実施できるよう調整すること。

4.9. 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) 受託者は各開発工程の開始・終了に当たり、工程開始・終了判定会議を開催し、主管課の承認を得ること。（少なくとも工程完了ごとにアクセシビリティ品質レビューが必須であることに留意）

なお、開催要否は主管課と協議の上決定すること。

- (3) 定例会・工程開始・終了判定会議とは別に受託者が主催する諸会議等の開催計画をプロダクトオーナーと相談の上、スケジュールを策定すること。そのスケジュールに沿う形で構成メンバーとの日程

調整、会場確保や Web 会議等の設定、関係者への資料の共有、また当日以後の議事録の作成等、会議体の準備・運営に必要な作業を担うこと。なお、Web 会議は Microsoft Teams にて実施すること。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、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。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。
- (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、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) 本業務にて取り扱う一部データについては主管課以外の担当省庁へ提出する必要がある。提出方法等については「4.13.成果物の作成（2）成果物の納品方法」を踏まえて契約後協議の上決定するが、当該作業に係る費用は受託者にて負担すること。

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

4.12. 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。成果物については各プロセスにて作成後順次共有するものとし、納品物としては契約満了前までにまとめて納入する想定である。

なお、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主管課が承認した場合は、成果物の種類、内容を変更することができる。

表 1 成果物一覧

項番	成果物名	納品期限（想定）
1	設計・開発実施計画書	契約締結後 2 週間以内

項番	成果物名	納品期限（想定）
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	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
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、会議の議事録等）	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	要件定義書の改定案	要件整理時に随時
8	設計書（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、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	UI/UX設計資料（想定する業務を総覧できるフローチャート、情報設計ドキュメント、UIデザインファイル（Figma、画面設計、スタイルガイド、コンポーネントインベントリ）、詳細な画面遷移図（業務フローと突合できるもの）等）	設計・開発の状況に応じて順次
10	安全目標設計書	設計・開発の状況に応じて順次
11	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
12	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
13	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
14	実行プログラム一式（標準型電子カルテ導入版本体）	設計・開発の状況に応じて順次
15	実行プログラム一式（α版デモ用）	設計・開発の状況に応じて順次
16	実行プログラム一式（医療情報共有アプリ版デモ用）	設計・開発の状況に応じて順次
17	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
18	全体テスト計画書、テスト仕様書	設計・開発の状況に応じて順次
19	テスト結果報告書（デモンストラリオテストに係る実施結果及びテストケース）	各テスト工程完了判定前まで
20	JIS X 8341-3:2016試験で作成される各ドキュメント	テストの状況に応じて順次
21	テストデータ	テストの状況に応じて順次
22	操作マニュアル（利用者向け）	教育の実施一週間前まで
23	ランニングコスト試算表	運用・保守開始前まで
24	運用・保守計画書	運用・保守開始前まで
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	変更依頼書	運用・保守の状況に応じて順次
28	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
29	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
30	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
31	引継ぎ資料	契約満了前
32	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。提出先は主管課と協議の上、決定すること。
- 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1「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1「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

(2) 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

(3) 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。

最大何次請負、再委託総額、累計契約額（前年度まで）、年度契約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 8 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/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下表を想定しているが、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、「4.13. 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。

表 2 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"> 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	プロジェクト統括管理責任者	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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。 本業務の委託期間中、専任でこれに当たるものとする。
4	システム設計・開発・保守班	<ul style="list-style-type: none"> 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。 リーダーはシステム設計・開発・保守班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。 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	システム運用班	<ul style="list-style-type: none"> 本システムの運用を担う。 各機能・サブシステムの設計・開発・保守班と連携し、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。 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。
6	品質管理責任者	<ul style="list-style-type: none"> 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。
7	情報セキュリティ責任者	<ul style="list-style-type: none"> 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) 品質管理責任者

品質管理責任者は、ウェブアクセシビリティに関する知見を有するとともに、実務の経験年数を5年以上有すること。

ウェブアクセシビリティに関する知見とは、少なくとも JIS X 8341-3:2016、WCAG 2.0～2.2、WAI-ARIA 1.2の内容に精通していることをいう。ウェブアクセシビリティに関する実務とは、JIS X 8341-3:2016 試験の計画・達成基準・実施・レポート作成の各業務や、フロントエンド画面の設計・デザイン・実装結果に対するアクセシビリティ品質レビューの実績をいう。

なお、次のいずれかに該当すること。

- デジタルアクセシビリティアドバイザー Basic レベルの認定者かつデジタルアクセシビリティアドバイザー Standard レベルの認定者
- 上記の試験合格者・資格保有者等と同等の知見・実務経験を有することが、経歴等において、明らかな者

品質管理責任者自身に、ウェブアクセシビリティに関する知見・実務実績が伴わない場合は、知見・実務経験を有するアクセシビリティ要員を追加し、アクセシビリティ要員がアクセシビリティに関する作業を担当してもよい。

(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、明らかなる者。

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。

(2) 諸設備、物品等資源

ア 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、主管課の承認を得ること。

イ 立地等の条件

作業場所は日本国内とし、事前に主管課の承認を得ること。

ウ 設備等の要件

主管課の求めに応じて作業場所を確保できる状態とすること。

本業務で使用する機器に対し必要なセキュリティ対策等が講じられていること。

会議等は原則オンラインで開催することを想定しているが、状況に応じて当該作業場所での開催も可能となるよう、準備を行うこと。

リモート作業をセキュアに行える設備を用意すること。

デジタル庁及び厚生労働省等との情報資産授受用のファイルサーバを用意すること。

本システムの業務を実施するために必要となる机、椅子等の什器、通信回線、プリンタ、電話等について、受託者の負担と責任において導入すること。

資料を保管する鍵付きの棚を用意すること。

エ 物理的アクセス制御及び監視要件

作業場所は以下の物理的なアクセス制御及び監視要件を満たすこと。

作業を行う施設は、電子錠による入退室管理が行われており、許可された利用者のみが入退室できるようにすること。

監視カメラによる入退室及び室内映像の収集ができること。

入退室の記録を取得できること。

通信回線を安全に敷設できる対策がとられていること。

(3) その他の要件

本業務の履行状況を監督するため、主管課職員が随時、受託者の作業場所やデータ保管場所の立入調査を行うこととする。ただし、データの保管にクラウドサービスを利用している等の理由により、データの保管場所への立入調査が困難な場合については、クラウドサービス事業者との契約内容にセキュリティ上の問題がないことの説明の聴取をもって立入調査に代えることができることとする。

受託者の作業場所では実施できない作業に限り、デジタル庁内で作業を行うことができる。その場合は、あらかじめ必要な手続きを実施し、主管課の承認を得ること。

5.4. 作業の管理に関する事項

- (1) 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。
- (2) コミュニケーションツールを活用し、感染症流行状況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。主管課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、主管課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、主管課職員が利用するライセンスを受託者が提供すること。

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) 要件定義書に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7年6月27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）。
<https://www.cyber.go.jp/policy/group/general/kijun.html>

- (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、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、合理的に必要な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、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）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

- (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下表に示す。各項目に対して漏れなく対応すること。

表3 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"> ・ 共有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	<ul style="list-style-type: none"> ・ 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	<ul style="list-style-type: none"> ・ 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	<ul style="list-style-type: none"> ・ 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	<ul style="list-style-type: none"> ・ 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	<ul style="list-style-type: none"> ・ 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	<ul style="list-style-type: none"> ・ 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、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、納品期日までに主管課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。

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、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。
- (2) 応札者は、1000 名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。
- (3) 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「8.1 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、以下の内容を記載した「再委託承認申請書」及び「再委託先事業者一覧」を主管課に提出し、あらかじめ承認を受けること。
 - 再委託の相手方の商号又は名称、住所
 - 再委託を行う業務の範囲
 - 再委託の必要性及び契約金額等
- (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「別紙 2 機器等リスト」に想定 of 機器等を記載の上、提出すること。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. 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。

12. 附属文書

別紙 1-1 再委託承認申請書

別紙 1-2 再委託先事業者一覧

別紙 2 機器等リスト

別紙 3 情報セキュリティに関する事項

支出負担行為担当官
デジタル庁会計担当参事官 殿

住 所
名 称
代 表 者 氏 名

再委託承認申請書

令和●年●月●日付け、貴庁と契約を締結した下記契約件名に関して、契約書の再委託条項に基づき、下記のとおり申請します。

記

1. 契約件名等

契約締結日	令和●年●月●日
契約件名	
契約金額(税込)	●円

※単価契約等の契約書に契約金額（総額）が明記されていない場合は、予定金額（総額）を記載。

2. 再委託内容

再委託先の氏名又は名称	〇〇株式会社 (再々委託先：△△株式会社) (再々々委託先：□□株式会社)
再委託先の法人番号(13桁)	0000000000000 (再々委託先：0000000000000) (再々々委託先：0000000000000)
再委託先の企業規模 (中小企業者等の定義：下記※参照)	〇〇 ※以下より選択 大企業者 中小企業者 小規模企業者 その他(社団法人等) (再々委託先：△△) (再々委託先：□□)
再委託先の住所	東京都千代田区～ (再々委託先：東京都千代田区～) (再々々委託先：東京都千代田区～)
再委託先が業務を行う期間	令和○年○月○日（又は再委託承認後）～令和○年○月○日 (再々委託：令和△年△月△日（又は再委託承認後）～令和△年△月△日) (再々々委託先：令和□年□月□日（又は再委託承認後）～令和□年□月□日)
再委託する金額	〇円 (再々委託：△円) (再々々委託先：□円)
再委託費率 ・契約金額に占める再委託費の割合 ・再々委託の場合、全体の契約金額に対する費率として記載（再委託先に含まれる）	〇% (再々委託：△%) (再々々委託先：□%)
再委託する（又は再委託先を変更する）合理的理由	

購入等件名 (調達案件名)	
登録番号	
法人名	

担当者名	
連絡先メールアドレス	
連絡先電話番号	

○ 提案機器等一覧

法人名	通番	区分	製造業者名	製造業者の 法人番号 (半角数字)	製品名	型番
(記載例)		サーバ	×××		××サーバ	AAA 0123
◎◎電機		ストレージ	×××		××ストレージ	BBB-bb
		端末装置	△△△		△△端末	CCC-1111
		ウイルス対策ソフト	●●●		ウイルス対策	VVV123
		スキャナ	〇〇〇		〇〇スキャナ	DD dddd
		プリンタ	△△△		△△E1234e	E1234e
	1					
	2					
	3					
	4					
	5					
	6					
	7					
	8					
	9					
	10					
	11					
	12					
	13					
	14					
	15					
	16					
	17					
	18					
	19					
	20					

※ 記載欄が足りない場合は、行を追加してください。なお、行の追加以外の変更は行わないようお願いいたします。

項番	要件区分	方針	名称	セキュリティ仕様の要件	補足
1	侵害対策	通信回線対策	通信経路の分離	不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。	
2	侵害対策	通信回線対策	不正通信の遮断	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。	
3	侵害対策	通信回線対策	通信のなりすまし防止	情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。	
4	侵害対策	通信回線対策	サービス不能化の防止	サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。	セキュリティ対応方針に従い、L3～L7層で対策可能な仕組みを導入すること
5	侵害対策	不正プログラム対策	不正プログラムの感染防止	不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。	
6	侵害対策	不正プログラム対策	不正プログラム対策の管理	システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること	
7	侵害対策	脆弱性対策	構築時の脆弱性対策	情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること	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（政府情報システムにおける脆弱性診断導入ガイドライン（digital.go.jp）」で求める方針、基準に
8	侵害対策	脆弱性対策	運用時の脆弱性対策	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること	「 digital.go.jp 」で定める方針、基準に
9	不正監視・追跡	ログ管理	ログの蓄積・管理	情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報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、一定期間（要件定義時に検討）保管するとともに、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	「 digital.go.jp 」で定める方針、基準に
10	不正監視・追跡	ログ管理	ログの保護	ログの不正な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及び消去や改ざんの事実を検出する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の脅威の軽減）のための措置を含む設計とすること	「 digital.go.jp 」で定める方針、基準に
11	不正監視・追跡	ログ管理	時刻の正確性確保	情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること	
12	不正監視・追跡	不正監視	侵入検知	不正行為に迅速に対処するため、府省庁内外で送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること	不正アクセス等のインシデントの兆候を即時に検知可能な仕組みを導入すること
13	不正監視・追跡	不正監視	サービス不能化の検知	サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。	セキュリティ対応方針に従い、L3～L7層で対策可能な仕組みを導入すること
14	アクセス・利用制限	主体認証	主体認証	情報システムによるサービスを許可された者のみに提供するため、不正ログインを防止、早期検知するための策を講じること	
15	アクセス・利用制限	アカウント管理	ライフサイクル管理	主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること	
16	アクセス・利用制限	アカウント管理	アクセス権管理	情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。 ・利用時間や利用時間帯によるアクセス制御 ・同一IDによる複数アクセスの禁止 ・IPアドレスによる端末の制限 ・ネットワークセグメントの分割によるアクセス制	
17	アクセス・利用制限	アカウント管理	管理者権限の保護	特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。	
18	データ保護	機密性・完全性の保護	通信経路上の盗聴防止	通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。	
19	データ保護	機密性・完全性の保護	保存情報の機密性保護	情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存しないことに加えて、保存された情報を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。	

20	データ保護	機密性・完全性の保護	保存情報の完全性保護	情報が改ざんされた場合にその事実を検知し、早期に対処することができる。	
21	物理対策	情報窃取・侵入対策	情報の物理的保護	情報の漏えいを防止するため、物理的な手段による情報窃取行為を防止・検知する機能を備えること。	
22	物理対策	情報窃取・侵入対策	侵入の物理的対策	物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。	
23	障害対策	構成管理	システムの構成管理	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。	
24	障害対策	可用性確保	システムの可用性確保	サービスの継続性を確保するため、情報システムの各業務の異常停止時間が目標復旧時間として2時間を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。	
25	サプライチェーン対策	情報システムの構築等の外部委託における対策	委託先において不正プログラム等が組み込まれることへの対策	情報システムの構築において、府省庁が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。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、府省庁が情報セキュリティ監査の実施を必要と判断した場合は、受託者は情報セキュリティ監査を受け入れること。また、役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して、情報セキュリティを確保すること。	
26	サプライチェーン対策	機器等の調達における対策	調達する機器等に不正プログラム等が組み込まれることへの対策	機器等の製造工程において、府省庁が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。	
27	利用者保護	情報セキュリティ水準低下の防止	情報セキュリティ水準低下の防止	情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。	
28	利用者保護	プライバシー保護	プライバシー保護	情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。	