

## 意見招請に関する公示

次のとおり調達物品の仕様書案の作成が完了したので、仕様書案に対する意見を招請します。

令和8年1月29日

日本司法支援センター 理事長 丸島 俊介

### 1 調達内容

調達等件名及び数量 第五世代インフラ共通基盤等システムの構築及び保守業務一式

### 2 意見の提出方法

- (1) 意見の提出期限 令和8年2月18日（水）17時00分
- (2) 提出先及び担当者 〒164-8721  
東京都中野区本町1-32-2 ハーモニータワー8階  
日本司法支援センター本部 総務部財務会計課第二係（担当 小室）  
電 話 050-3381-1573  
E-Mail keiyaku@houterasu.or.jp
- (3) 提 出 方 法 別紙様式を使用し、電子メールにより上記担当者宛て提出する。

### 3 仕様書案別紙の交付

- (1) 交 付 期 間 令和8年1月30日（金）から令和8年2月18日（水）まで  
（土日祝日を除き各日とも10時00分から17時00分までの間）
- (2) 交 付 場 所 上記2(2)に同じ。
- (3) 交 付 条 件 仕様書案別紙1から16については、「機密保持誓約書」を提出した者に交付する。交付を希望する者は、上記2(2)に示した電子メールアドレス宛てに、別添「機密保持誓約書」を使用の上、提出すること。

### 4 仕様書案の説明会

実施しない。

### 5 本件に関する問合せ先

日本司法支援センター本部 総務部財務会計課第二係（担当 小室）

電 話 050-3381-1573

E-Mail keiyaku@houterasu.or.jp

「第五世代インフラ共通基盤等システムの構築及び保守業務一式」  
仕様書案に対する意見書

令和8年 月 日

所在地

会社名

担当者

電 話

F A X

E-mail

項番	区分	箇所	意見内容
1	仕様書案	第5の3(1)	..... (内容は簡潔にまとめる)
2	その他	—	.....
3			

※意見書はエクセルファイルにて作成し、電子メール（keiyaku@houterasu.or.jp宛て）で送信すること。

※電子メールの表題は、「【意見提出】第五世代インフラ共通基盤等システムの構築及び保守業務一式（〇〇社）」とすること。

令和 8 年      月      日

日本司法支援センター 御中

所在地  
会社名  
担当者  
電 話  
F A X  
E-Mail

## 機密保持誓約書

当社は、貴センターの「第五世代インフラ共通基盤等システムの構築及び保守業務一式」に関して、貴センターから閲覧を許可された資料について、以下の事項を厳守します。

- 1 本件調達を受注するための検討以外の目的に利用しないこと。
- 2 社の内外を問わず、本件調達に関わらない第三者に対し、閲覧資料の内容を提供しないこと。
- 3 社の内外を問わず、本件調達に関わらない第三者に対し、閲覧資料の内容が漏えいすることのないように措置すること。
- 4 本件調達に関与した者が異動した後においても、機密が保持されるよう措置すること。
- 5 閲覧資料の内容の漏えい等によって機密が侵害され、貴センターに損害を与えた場合には、損害を賠償する責任があることを認めること。
- 6 その他、閲覧資料の機密保持に関して適切な措置を講じること。

以上

第五世代インフラ共通基盤等システムの構築  
及び保守業務一式  
調達仕様書（案）

---

令和8年1月

日本司法支援センター

1. 調達案件の概要	1
1.1. 調達件名	1
1.2. 調達の背景及び目的	1
1.3. 期待する効果	1
1.4. 本システムの概要	2
1.5. 契約期間	3
1.6. 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. 関連調達案件の一覧	4
2.3. センターが調達するソフトウェア、サービス等の一覧	5
2.4. 調達案件間の入札制限	6
3. 本システムに求める要件	7
4. 作業の実施内容に関する事項	7
4.1. 設計・構築実施計画書等の作成	7
4.2. 作業管理	9
4.3. 要件確認	9
4.4. 設計	9
4.5. 構築	12
4.6. テスト	12
4.7. 移行	12
4.8. 引継ぎ	12
4.9. 運用	13
4.10. 保守	13
4.11. 会議開催	13
4.12. データ管理方法	13
4.13. 業務完了報告書の作成	13
4.14. 成果物の作成	14
4.15. 情報資産管理標準シートの提出等	16
4.16. Azure サービス利用料等の算出	17
4.17. その他	18
5. 作業の実施体制・方法に関する事項	18
5.1. 作業実施体制と役割	18
5.2. 作業要員に求める資格等の要件	19
5.3. 作業場所	20
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 .....	23
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.	成果物の取扱いに関する事項 .....	25
7.1.	知的財産権の帰属 .....	25
7.2.	契約不適合責任 .....	26
7.3.	検査 .....	26
8.	入札参加に関する事項 .....	27
8.1.	競争参加資格 .....	27
8.2.	公的な資格や認証等の取得 .....	27
8.3.	受注実績 .....	27
8.4.	複数事業者による共同入札 .....	27
9.	再委託に関する事項 .....	28
9.1.	再委託の制限及び再委託を認める場合の条件 .....	28
9.2.	承認手続 .....	28
9.3.	再委託先の契約違反等 .....	29
10.	クラウドサービスの選定、利用に関する事項 .....	29
10.1.	クラウドサービスの選定、利用に関する要件 .....	29
10.2.	クラウドサービス利用に係る成果物の取扱い .....	29
10.3.	SaaS サービスの契約に当たっての留意事項 .....	29
11.	その他特記事項 .....	29
11.1.	前提条件等 .....	29
11.2.	機器等のセキュリティ確保 .....	30
11.3.	入札公告期間中の資料閲覧等 .....	30
11.4.	クラウドサービス利用料の概算見積り .....	31
12.	附属文書 .....	31

# 1. 調達案件の概要

## 1.1. 調達件名

---

第五世代インフラ共通基盤等システムの構築及び保守業務一式

## 1.2. 調達の背景及び目的

---

日本司法支援センター（以下「センター」という。）は、総合法律支援法（平成 16 年法律第 74 号）に基づき、国民等がどこでも法的なトラブルの解決に必要な情報やサービスの提供を受けられるようにすることを目的として設立された法人である。

センターの情報システムは、各種業務アプリケーション、これら業務アプリケーションにサーバ、ストレージ及びネットワーク等の基盤機能を提供するインフラ共通基盤、職員に業務環境を提供するクライアントシステム、各システムやデータを保全するための保全システム（以下インフラ共通基盤、クライアントシステム及び保全システムを総称して「インフラ共通基盤等システム」という。）などから成り立っている。

現行インフラ共通基盤等システム（以下「現行システム」という。）は令和 10 年 5 月をもって運用を終了するため、現行システムの運用終了以降も国民等に対してセンターのサービスを適切に提供できる環境を維持することを目的として、第五世代インフラ共通基盤等システム（以下「本システム」という。）への更改を行う。

## 1.3. 期待する効果

---

本システムは、原則として現行システムが有する機能を踏襲しつつ、クラウドベースのシステムとすることにより、センターの情報システム全体に係る将来的なライフサイクルコストの低減を目指す。

なお、現行システムからの主な変更は以下のとおり。

- (1) クラウドサービスの積極的な活用
  - データセンターに集約していたシステムの大部分をパブリッククラウドに移行
  - センター拠点・パブリッククラウド・データセンター間を閉域接続するサービスの採用
  - 主要な認証基盤を Active Directory から Entra ID に変更
  - Active Directory と Entra ID における UPN 名の統一（代替ログイン ID 認証の廃止）
- (2) クライアント端末のセキュア FAT への更改
  - 職員が利用するクライアント端末をシンクライアントからセキュアな FAT 端末へ
  - FAT 端末の特性に合わせたセキュリティ対策の見直し
- (3) SharePoint のゲストアクセス許可を含む Microsoft365 サービスの積極的な活用
  - SharePoint へのゲストアクセス許可と適切なアクセスコントロールの実現
  - 職員の属性及び働き方に応じた適切な Microsoft365 ライセンスの使い分け

## 1.4. 本システムの概要

本システムは、センター職員が業務を実施するために必要な情報システム全体の基盤及びクライアント環境等を提供するものであり、構成概要は「表 1 本システムの構成概要」のとおり。詳細は別紙類を参照すること。

表 1 本システムの構成概要

項番	大分類	小分類	備考
1	クラウド（Microsoft Azure、M365）等－ 共通領域（プラットフォーム領域）		
1-1		ネットワーク基盤	ネットワークサービス、メインデータセンターに設置するネットワーク機器及び本部 L3・L2 スイッチ及び移行用専用線を含む。
1-2		ID・アクセス管理	
1-3		セキュリティサービス	
1-4		運用管理	
1-5		クライアント管理	
1-6		その他	
2	クラウド（Microsoft Azure）－ 利用サブシステム向け領域（アプリケーション領域）		
2-1	内部向けシステム	財務会計システム	業務アプリケーションはアプリ構築事業者が本システム上に構築する
2-2		情報共有システム	業務アプリケーションはアプリ構築事業者が本システム上に構築する
2-3		法人文書システム	業務アプリケーションはアプリ構築事業者が本システム上に構築する
2-4		権限管理システム（中継サーバ）	中継サーバをアプリ構築事業者が本システム上に構築する 中継サーバはアプリ構築事業者が提供する SaaS アプリケーションとインターネット経由で接続し、ファイル連携を行う
2-5		業務統合管理システム	業務アプリケーションはアプリ構築事業者が本システム上に構築する
2-6	外部向けシステム	利用者向けポータル	業務アプリケーションはアプリ構築事業者が本システム上に構築する
2-7		新弁護士等向けポータル	業務アプリケーションはアプリ構築事業者が本システム上に構築する
3	端末		
3-1	端末		
4	対象外		
4-1		情報提供業務システム	・データセンターに設置されている ・受注者からの情報提供に基づいて関連事業者が NW 設定等を変更する ・対象システムのサーバやストレージは、本調達の範囲に含まれない
4-2		コールセンター系 IP 電話シ	同上



項番	大分類	小分類	備考
		ステム	
4-3		事務所系 IP 電話システム	<ul style="list-style-type: none"> <li>・データセンターに設置されている</li> <li>・受注者からの情報提供に基づいて関連事業者が NW 設定等を変更する</li> <li>・対象システムのサーバやストレージは、本調達の範囲に含まれない</li> </ul>
4-4		支払先マイナンバー管理システム	<ul style="list-style-type: none"> <li>・関連事業者が本部に移設</li> <li>・受注者は、他の本部に設置される機器とは独立したネットワーク環境を提供</li> <li>・運用管理のための必要最小限の通信のほかは、同システムを構成する機器間のみで通信を許可（専用クライアント端末、サーバ及びストレージはいずれも本部に設置）。</li> <li>・受注者からの情報提供に基づいて関連事業者が NW 設定等を変更する</li> <li>・対象システムの専用クライアント端末、サーバ及びストレージは、本調達の範囲に含まれない</li> </ul>
4-5		人事システム	SaaS サービスを利用
4-6		(その他)	

### 1.5. 契約期間

契約締結日から令和 15 年 5 月 31 日まで

- ① 設計・構築期間：契約締結日から令和 10 年 5 月 7 日
- ② ハードウェア・ソフトウェア賃貸借及び保守期間：令和 10 年 5 月 8 日から令和 15 年 5 月 31 日
- ③ クラウドサービス（Microsoft Azure を除く）提供及び保守期間：令和 10 年 5 月 8 日から令和 15 年 5 月 31 日
- ④ クラウドサービス（Microsoft Azure）保守期間：令和 10 年 5 月 8 日から令和 15 年 5 月 31 日
- ⑤ システム保守期間：令和 10 年 5 月 8 日から令和 15 年 5 月 31 日
- ⑥ SIEM 保守期間：令和 10 年 5 月 8 日から令和 15 年 5 月 31 日
- ⑦ 初期運用期間：令和 10 年 5 月 8 日から同年 7 月 31 日

※1：②③④⑤⑥については、契約期間満了から最長 1 年間は延長可能なこと。ただし、延長期間中において対象製品のメーカーサポートが完全に終了する場合、受注者は当該製品を保守対象から除外することができる。延長する場合は、センターと受注者との延長に係る契約条件等についての協議を行うものとする。

※2：本調達の契約期間終了後も、SaaS サービスや月額/年額課金型パッケージ製品等について、契約期間終了前に契約の延長又はセンターへの引継ぎ等を行うことで、当該サービス/製品をそのまま継続利用することを想定している。そのため、契約の終了に際しては、継続利用に

支障のないよう手続きを行うこと。

## 1.6. 作業スケジュール

---

本システム及び関連するシステムの設計・構築・運用に関し想定する全体スケジュールを「別紙 1 作業スケジュール」に示す。受注者は業務の開始に当たって最適と考える具体的なスケジュールを計画・立案すること。

## 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

---

#### (1) 調達範囲

本調達の調達範囲は以下のとおり。

ただし、本システムの構築、正常稼働及び役務履行のために必要なものがある場合は、これを調達の範囲とする。調達範囲の調整が必要となった場合には、センターと協議の上、決定すること。

- ① 本システムの設計、構築及び導入並びにこれらに付随する必要な支援
- ② 本システムを構成するハードウェア・ソフトウェアの賃貸借及び保守
- ③ クラウドサービス提供（Microsoft Azure を除く）及び保守
- ④ クラウドサービス（Microsoft Azure）の保守
- ⑤ 本システムのシステム保守
- ⑥ 本システムの SIEM 保守
- ⑦ 本システムの初期運用
- ⑧ インフラ運用事業者（令和 10 年 6 月以降の本システム運用事業者）及びセンターへの引継ぎ

#### (2) 関連事業者との役務・コストの分担及び責任分界

本システムの構築においては、CSP からのクラウドサービス提供、NW ベンダーからのネットワークサービス提供、アプリ構築事業者への基盤引渡し等が発生し、センター以外にも複数の事業者との調整事項が発生する。受注者は、これらの調整事項について、調整のスケジュールを定める、必要に応じて調整会議を主催するなど、センターの管理のもとで主体的に調整を進めること。センター及びアプリ構築事業者との役務・コストの分担及び責任分界については、「別紙 4 構築役務に関する分担表」及び「別紙 5 調達対象に関する分担表」を参照すること。なお、受注者は、別紙 4 及び別紙 5 に記載が無い役務・コストであっても、本調達の目的を達成するために当然付随して必要なものについては、本調達の一部として適宜調整を図り、本調達の履行に支障が生じないよう留意すること。

### 2.2. 関連調達案件の一覧

---

現時点で予定している主な関連調達案件（本システムのために別途調達を予定するものを除く）の調達単位、調達の方式、実施時期等は「表 2 主な関連調達案件の一覧」のとおり。

表 2 主な関連調達案件の一覧

No.	調達内容（概要）	調達の方式	契約締結日	入札公告 落札者決定
1	本システムの構築及び保守（本調達）	一般競争入札 （総合評価）	令和 8 年 6 月 （予定）	令和 8 年 3 月 令和 8 年 6 月 （予定）
2	令和 10 年 6 月以降の本システムに係る運用役 務	一般競争入札 （調達方式未定）	令和 10 年 5 月 （予定）	令和 10 年 2 月 令和 10 年 4 月 （予定）
3	人事・権限管理システムのクラウド移行及び保守	随意契約 （性質随契）	令和 7 年 10 月 （予定）	令和 7 年 10 月 （予定）
4	人事・権限管理システムのクラウド移行及び運用 に係る支援業務一式	一般競争入札 （最低価格）	令和 7 年 10 月 （予定）	令和 7 年 10 月 （予定）
5	財務会計システムの第五世代インフラ共通基盤 への移行	随意契約 （性質随契）	未定	－
6	情報共有システムの第五世代インフラ共通基盤 への移行	一般競争入札 （調達方式未定）	未定	未定
7	法人文書システムの第五世代インフラ共通基盤 への移行	随意契約 （性質随契）	未定	－
8	支払先マイナンバー管理システム移設	随意契約 （性質随契）	未定	－
9	第五世代システム更改に伴う工程管理及び技術 支援業務	一般競争入札 （総合評価）	契約締結済（令和 7 年 9 月）	
10	業務統合管理システムの更改に係る設計・開発 等業務一式	一般競争入札 （総合評価）	契約締結済（令和 7 年 9 月）	

### 2.3. センターが調達するソフトウェア、サービス等の一覧

本業務の契約中にセンターが本システムのために別途調達を予定するソフトウェア及びサービス等は「表 3 センターが調達するソフトウェア、サービス等の一覧」とおりである。一覧に記載されたソフトウェア・サービス等の調達主体はセンターとなるが、これらのソフトウェア、サービス等の設定等を含め、本システムを構築するのは受注者の役務となることに留意すること。

表 3 センターが調達するソフトウェア、サービス等の一覧

項番	ソフトウェア、サービスの種別	製品名等	調達予定時期	備考
1	ネットワークサービス	・Flexible InterConnect ・Flexible Secure	令和 8 年 10 月 （予定）	

		Gateway ・Flexible Remote Access ・上記に係る支援サービス		
2	パブリッククラウドサービス	・Azure Prepayment	令和 8 年 10 月 (予定)	センター負担分の Azure サービス利用料を支払うため定期的に購入する。
3	Microsoft OS・データベースソフトウェアライセンス	例 ・Windows Server ・Microsoft SQL Server	受注者と調整	AHUB 特典を利用することでコストの低減を実現できる製品のライセンスについては受注者と調整の上センターが別途調達する。
4	Microsoft365 ライセンス	・Microsoft 365 E5 ・Microsoft 365 F3 ・Microsoft Defender + Purview Suite FLW ・Microsoft Teams	受注者と調整 (令和 9 年 2 月以降を想定)	運用期間中の調達予定数量は以下のとおり。構築期間については受注者と別途調整する。 ・Microsoft 365 E5 (Teams あり) : 1,150 ・Microsoft 365 F3 : 500 ・Microsoft Defender + Purview Suite FLW : 500
5	Microsoft サポート	ユニファイドサポート	受注者と調整 (令和 9 年 2 月を想定)	契約期間は令和 9 年 2 月 1 日から令和 10 年 8 月末日までを想定している。 プロアクティブサービス (計 100 時間) を含むが、受けるサービスの内容は、センターが調達する範囲内で受注者と調整の上決定する。
6	データセンターラック賃貸借等		受注者と調整	
7	データ移行用等回線	未定	受注者と調整	
8	拠点インターネット回線	・フレッツ光ネクストファミリースーパーハイスピードタイプ 集 ・フレッツ光ネクストファミリーギガラインタイプ 等 ※サービス提供エリア等の都合で拠点ごとに異なる	令和 8 年 6 月までに順次開通	センターの全拠点 (本部、地方事務所・CC) に整備する。 本システムで直接利用するためのものではないが、これを活用する提案をすることは差支えない。

## 2.4. 調達案件間の入札制限

相互けん制の観点から、以下に示す事業者は入札に参加できない。

- ① 「第五世代システム要件定義書作成支援等コンサルタント業務 一式」の受注者 (再委託先等を含む。)
- ② ①の者に係る、「財務諸表等の用語、様式及び作成方法に関する規則」(昭和 38 年 11 月 27 日大蔵省令第 59 号) 第 8 条に規定する親会社及び子会社
- ③ ①の者と同一の親会社を持つ会社
- ④ ①の者の委託先事業者
- ⑤ その他①の者と緊密な利害関係を有する事業者

### 3. 本システムに求める要件

設計・構築の実施に当たっては、「別紙 2 要件定義書」の各要件を満たすこと。

### 4. 作業の実施内容に関する事項

作業は、調達仕様書、要件定義書及び受注者の作成する提案書を踏まえて実施すること。なお、提案書の記載事項のうち、実際に実施する事項はセンターと協議の上、決定する。

#### 4.1. 設計・構築実施計画書等の作成

##### (1) 設計・構築実施計画書及び設計・構築実施要領

設計・構築実施計画書及び設計・構築実施要領を作成し、センターの承認を得ること。

設計・構築実施計画書及び設計・構築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、センターの承認を得ること。

設計・構築・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 7 年 5 月 27 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、センターと協議の上、対応について決定すること。

受注者が作成する「設計・構築実施計画書（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・制約条件等）

受注者が作成する「設計・構築実施要領（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、成果物に係る納入期限によらず、作業進捗に応じた適切なタイミングでセンターに提出すること。

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、センターの承認を得ること。

##### (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・構築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センターと協議の上決定すること。

受注者とセンター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。費用は受注者の負担とする。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

課題管理表を用いて、課題分類、課題番号、期限、現時点の対応者を明記し、週次で棚卸しを実施し、残課題が明確になるように管理すること。また、課題解決の担当者が、受注者、センター、その他関係者のいずれかにかかわらず、受注者にて本プロジェクト全体の課題を管理すること。

- ・ リスク管理

リスク管理表を用いて、リスク事象、影響、影響度、リスク発生確率、予防策、リスク対応策（低減、受容、転嫁、回避等）、対応期限等を明記し、管理すること。定期的に新たなリスクの発生有無の確認及び棚卸しを実施し、リスクの状況が明確になるように管理すること。リスクが顕在化した場合は、速やかにセンターに報告するとともに、課題管理に移管し対策を行うこと。また、リスクの主体が受注者、センターのいずれかにかかわらず、受注者にてプロジェクト全体のリスクを管理すること。

- ・ 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、センターの承認を得ること。

- ・ 変更管理/構成管理

変更管理/構成管理について、管理手順を明確に記載すること。

センター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、センターから受注者に対する指摘や確認事項等について、一元的に対応可能な問合せ対応窓口の体制を作り、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、週次定例会を除き原則としてオンライン会議での実施とするが、センターから要請があった場合及び受注者が必要と判断した場合は、センターと受注者で協議の上、対面で開催すること。また、別途センターが報告を求める場合においては、センターが指示する必要な書類を作成すること。詳細は設計・構築実施要領の作成時にセンターと協議の上、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、センターが求める場合は、必要に応じて体制に参画しているメンバー（セキュリティ要員など）を参加させること。

## 4.2. 作業管理

---

### (1) 設計・構築工程及び運用・保守工程の作業管理

受注者は、センターが承認した設計・構築実施計画書及び設計・構築実施要領に従い、各種管理を行うこと。また、運用・保守開始後においては運用・保守作業計画書及び運用・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方法

コミュニケーションツールを活用し、継続性の高い構築・運用・保守体制を構築すること。センター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、センター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 Microsoft Teams（ただし WEB 会議のみ、資料共有不可）及び box である。これらのツールを用いる場合、受注者が必要とするライセンスは受注者が用意すること。センターがライセンスを保有しないコミュニケーションツールを利用する場合には、センター職員が利用するために必要なライセンスを受注者が提供すること。

なお、コミュニケーションにおいては、関係者間での適切な情報共有に留意し、電話、電子メール等の手段により、適時的確な情報共有に努めること。なお、連絡は原則として電子メール等の記録に残る方法で行い、特に軽微な内容を除き、電話・口頭のみ等の記録が残らない方法は行わないこと。

## 4.3. 要件確認

---

受注者は、設計・構築の実施に先立ち、「別紙 1 作業スケジュール」から「別紙 15 主な運用・保守作業一覧」の内容を確認すること。また、要件ごとに具体的な実現方法を記載した要件確認書を作成すること。その際、内容について確認・調整すべき事項があれば、センターまたは工程管理事業者と調整の上、結果に基づき要件確認書に反映させること。要件の調整内容は、センターに提示し、合意形成を図りつつ進めること。

## 4.4. 設計

---

### (1) 基本的な要件

#### ア 基本設計及び詳細設計

受注者は、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を行い、成果物についてセンターからの承認を得ること。

センター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。また、記載内容の粒度は、原則として現行システム図書と同等以上とすること。

- イ 要件充足確認資料の作成  
要件と基本設計及び詳細設計の対応表等、要件が網羅されていることを確認できる資料を作成し、センターに提示すること。
- ウ 外部インタフェース仕様書の作成  
受注者は、他の情報システム（例：権限管理システム）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。作成に当たっては、システム間の不整合が起きないように、連携先システムの設計や仕様を適切に把握すること。
- エ 本システムにて利用する環境  
本システムにて利用する環境は、要件定義書「2.3.情報システム稼働環境に関する事項」を参照すること。
- オ ライフサイクルコストの考慮  
受注者は、本システムの設計・構築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 ランディングゾーンアーキテクチャ  
設計に当たっては、Azure ランディングゾーンアーキテクチャをベースに、要件定義書に記載のある要件の実装を検討すること。
- キ クラウドネイティブなシステム構成  
設計・構築に当たっては、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。
- ク 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、本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（ロデータ）も確認できる構成とすること。

## (2) 設計に係る役務想定

以下に想定する設計に関する役務を示す。記載がなくとも必要な役務については提案し、センターの承認を受けた上で実施すること。また、センターが別途契約するインフラ運用事業者への引き継ぎ完了までの期間、追加・変更が発生した場合はこれを取り込むこと。

### ア 基本設計

- 本システム全体に係る設計方針、情報セキュリティ設計方針等の全体設計方針
- パブリッククラウドサービスに係る構成等の各種設計
- サーバ/ストレージに係る構成等の各種設計
- ネットワーク/セキュリティに係る構成等の各種設計
- 本システムが提供する各種機能に係る設計（クラウドサービス含む）

### イ 詳細設計



- 各種ハードウェア機器における個別の設定値や定義情報等の設計
- 各種ソフトウェアにおける個別の設定値や定義情報等の設計
- 各種クラウドサービス、セキュリティサービスにおける個別の設定値や定義情報等の設計
- 各種機器・サービスの設定値やコンフィグデータ等（別文書でも可とする）

### (3) 運用・保守設計

#### ア 現行システムの運用・保守作業内容の棚卸し

受注者は、現行システムの運用・保守作業内容をベースラインとして、作業内容の棚卸し（本システム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の整理）を行うこと。

本システム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

受注者は、要件定義書の「4.13 運用・保守に関する事項（1）運用・保守計画」に示す内容をもとに運用・保守作業計画書及び運用・保守実施要領の案を作成し、センターの承認を受けること。

なお、運用・保守作業計画書の案には、以下の内容を含めること。

- 本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

受注者は、「ア 現行システムの運用・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、要件定義書の「4.13 運用・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、本システムの機能要件及び非機能要件を実現・維持するために必要な運用設計及び保守設計を行い、センターの承認を受けること。

運用・保守設計に当たっては、センター作業の軽減等、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

#### エ 想定運用工数（ランニングコスト）の算出

運用・保守設計を行う際には、運用・保守設計に基づき想定される想定運用工数及びその内訳を取りまとめた想定運用工数試算表を作成し、センターの承認を得ること。

#### オ 運用・保守手順書

受注者は運用・保守作業計画書を踏まえ、以下を取りまとめた運用・保守手順書を作成し、センターの承認を得ること。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。

- 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

### 4.5. 構築

---

#### (1) ルールの規定

受注者は、本システムの構築や本システムを構成するサブシステムの開発に当たり、構築、開発又は保守を効率的に実施するため、ホスト名等の命名規則、プログラミング等のルールを定めた標準等を定め、センターの承認を得ること。

#### (2) ルール遵守や成果物の確認方法

受注者は、構築に当たり、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、標準規約遵守の確認、ソースコードの検査等）を定め、センターの承認を得ること。

#### (3) 構築手法

本プロジェクトではウォーターフォールを原則とするが、プロジェクトの特性を踏まえ他の手法を提案することは妨げない。

#### (4) 構築ツール

受注者は、構築に当たり IaC ツール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) 構築の実施

受注者は、センターの承認を得た基本設計書及び詳細設計書に基づき、本システムの構築を実施すること。

なお、設計・構築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、受注者の負担にて用意すること。

### 4.6. テスト

---

受注者は、要件定義書「4.9.テストに関する事項」に示す事項を踏まえ、テストに係る業務を適切に実施すること。

### 4.7. 移行

---

受注者は、要件定義書「4.10.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こと。

### 4.8. 引継ぎ

---

受注者は、要件定義書「4.11.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

切に実施すること。

#### 4.9. 運用

---

受注者は、要件定義書「4.13 運用・保守に関する事項」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。

#### 4.10. 保守

---

受注者は、要件定義書「4.13 運用・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。

#### 4.11. 会議開催

---

- (1) 設計・構築期間、受注者は、定例会を週 1 回程度開催して業務の進捗状況を設計・構築実施要領に基づきセンターに報告するとともに、仕様確認や協議等の必要な調整を行うこと。
- (2) 受注者は各構築工程の完了に当たり、工程完了判定会議を開催し、センターの承認を得ること。なお、構築工程ごとの開催要否はセンターと協議の上決定すること。
- (3) センターから要請があった場合、又は、受注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、週次定例会を除き原則としてオンライン会議とすること。ただし、センターから要請があった場合及び受注者が必要と判断した場合は、センターと受注者で協議の上、対面で開催すること。
- (5) 受注者は、議事録を作成の上、会議終了後、会議終了の翌日から起算して 3 日以内（センターの休日（土曜日、日曜日、国民の祝日に関する法律（昭和 23 年法律第 178 号）に定める休日及び 12 月 29 日から翌年 1 月 3 日）を除く。）にセンターに提出し、速やかにセンターの承認を受けること。

#### 4.12. 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、センターの許可なく追加、変更及び削除並びに公開をしないこと。
- (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、センターが管理する 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) 受注者は、上記（1）（2）における条件を満たすシステム構成において本調達に係る業務を行うこと。

#### 4.13. 業務完了報告書の作成

---

受注者は、以下の内容を含む業務完了報告書を作成し、センターの承認を得ること。

- ・ 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

#### 4.14. 成果物の作成

##### (1) 成果物一覧

本調達の成果物は「表 4 成果物一覧」のとおり。納入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・構築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、受注者が採用する構築手法に応じた適切な成果物の構成を提案の上でセンターが承認した場合は、成果物の種類、内容を変更することができる。

表 4 成果物一覧

項番	成果物名	納入期限（想定）
1	ハードウェア一式	令和 10 年 5 月 8 日
2	ソフトウェア一式	令和 10 年 5 月 8 日
3	クラウドサービス一式	令和 10 年 5 月 8 日
4	設計・構築実施計画書	契約締結後 2 週間以内
5	設計・構築実施要領	契約締結後 2 週間以内
6	情報セキュリティ管理計画書	契約締結後 2 週間以内
7	個人情報の取扱いにかかる事項について記載した書面	契約締結後 2 週間以内
8	払い出し環境に係る基盤設計情報一式	アプリ構築事業者への環境払い出し前まで
9	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 営業日以内
10	要件確認書	要件整理時に随時
11	設計書（基本設計書、詳細設計書、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、環境構築手順書、環境定義書、ハードウェア・ソフトウェア・クラウドサービスの一覧、外部インタフェース仕様書等）	設計・構築の状況に応じて順次
12	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・構築の状況に応じて順次
13	実行プログラム一式	設計・構築の状況に応じて順次
14	テスト計画書、テスト仕様書	各テスト開始前まで
15	テスト結果報告書（テスト証跡も含むが、納入範囲はセンターと協議の上、決定すること）	各テスト工程完了判定前まで
16	受入テスト計画書（案）、受入テストシナリオ（案）、受入テスト仕様書（案）	受入テスト開始前まで
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	稼働判定前まで
22	操作マニュアル（システム管理者用、センター職員用、外部ユーザー用）	受入テスト開始前まで
23	運用・保守作業計画書	案については総合テスト開始前まで 確定版については運用・保守開始前まで

24	想定運用工数試算表	案については総合テスト開始前まで 確定版については運用・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、脆弱性管理基準、脆弱性管理手順、ヘルプデスク運用マニュアル、FAQ等）	案については総合テスト開始前まで 確定版については運用・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（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
32	業務完了報告書	契約満了前
33	情報資産管理標準シート	契約満了前
34	標準ガイドライン別紙2「情報システムの経費区分」に基づく契約金額の内訳	センターの求めに応じて随時
35	Azureサービス利用料等の見積書（契約日～令和10年3月31日分）	令和8年11月30日までの間でセンターと協議して決めた日まで
36	Azureサービス利用料等の見積書（令和11年度～令和15年度分）	令和11年度以降 毎年1月31日まで

## (2) 成果物の納入方法

成果物の納入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、そのまま記載することを認める。
- ・ 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入とすること。提出方法はセンターと協議の上、決定すること。
- ・ 納入後、センター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入すること。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、センターと協議の上でそれを納入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、センターの承認を得ること。
- ・ 成果物が外部に不正に利用されたり、納入過程において改ざんされたりすることのないよう、安全な納入方法を提案し、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入する場合は、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。
- ・ 受注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。
- ・ 受注者は、「表 4 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、内容についてセンターと適宜協議をした上で、成果物の初版を「表 4 成果物一覧」に指定した期限に納入しセンターの承認を得ること。
- ・ 成果物については、必要に応じて更新を行いセンター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入すること。
- ・ 納入先は以下のとおり。
  - ① メインデータセンターに設置するハードウェア一式  
メインデータセンター（東京都区部に所在。詳細は受注者に開示する。）

- ② センター本部に設置するハードウェア一式  
〒164-8721 東京都中野区本町 1-32-2 ハーモニータワー 8 階  
日本司法支援センター本部 総務部 情報システム管理課
- ③ クライアント端末一式  
「別紙 11 センター拠点一覧（令和 8 年 1 月現在）」に示す拠点に各指定台数を  
納入すること。なお、本調達以降に拠点の統廃合や人事異動等により別紙 11 の情  
報は変更される場合がある点に留意すること。
- ④ その他ドキュメント等  
センター本部（②参照）

#### 4.15. 情報資産管理標準シートの提出等

受注者は標準ガイドライン「別紙 2 情報システムの経費区分」に基づき区分等した契約金額の内訳を提出すること。

また、受注者は、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。初期運用期間終了後の提出時期は運用・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、センターと協議の上、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、統合開発環境（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

- ・ 開発、運用
 

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。
- ・ 支援
 

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。

## 4.16. Azure サービス利用料等の算出

受注者は、「表 5 Azure サービス利用料等の見積対象及び期限」とおり Azure サービス利用料等について算出し、その結果をセンターに提出すること。なお、下表のほか、予算の確保その他理由によりセンターから求めがあった場合には、受注者はその求めに応じ Azure サービス利用料等の算出を行い、参考資料としてセンターに提出すること。

表 5 Azure サービス利用料等の見積対象及び期限

No.	提出期限	見積対象
1	令和 8 年 11 月 30 日までの間でセンターと協議して決めた日まで	契約日から令和 10 年 3 月 31 日までに要する Azure サービス利用料及び同利用料支払いのため必要となる Azure Prepayment のライセンス数（想定）（※）。
2	令和 11 年度以降 毎年 1 月 31 日まで	翌年度（12 か月間）の Azure サービス利用料及び同利用料支払いのため必要となる Azure Prepayment のライセンス数（想定）（※）

- ※ 表 5 において見積対象となる Azure サービス利用料は、本システムを構成する Azure サービスのうち、業務統合管理システム、新弁護士向けポータル及び利用者向けポータルで利用するサブスクリプションを除いた全てのサブスクリプションである。Azure ハイブリッド特典（Windows Server・SQL Server）の適用が可能なリソースがある場合には、適用の可否をセンターに確認の上算出すること。なお、センターは同特典を適用可能なライセンスを保有していないため、Azure ハイブリッド特典を適用した見積もりをする場合、同期間中に必要な Windows Server や SQL Server の

ライセンスの種類、金額及び数量を併せて提示すること。

#### 4.17. その他

- (1) 国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）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 7 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情報システムは原則としてセンタードメイン（houteras.or.jp）を用いること。

## 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「表 6 本業務における組織等の体制と役割」のとおり想定しているが、詳細はセンター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・構築実施計画書の「作業体制に関する事項」に記載し、「4.14 成果物の作成」に記載された納入期限までに提出すること。また、作業要員が病気等により長期にわたり不在となる場合は、迅速に代替となる要員を加えること。

表 6 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	【センター】 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>
2	【センター】 担当部署 (情報システム管理 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>関係システム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>
3	【受注者】 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、センターとの調整を行う。</li> <li>本業務の設計・構築期間及び初期運用期間を通じて、専任でこれに当たるものとする。</li> </ul>
4	【受注者】 設計・構築チーム	<ul style="list-style-type: none"> <li>本システムの設計・構築を担う。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・構築チームの各業務の全体像を把握し、設計・構築に係るセンターとの調整、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・構築作業期間中、専任でこれに当たるものとする。</li> </ul>
5	【受注者】 保守チーム	<ul style="list-style-type: none"> <li>本システムの保守を担う。またパッチ適用、障害対応等において他関係事業者の支援を行う。</li> <li>リーダーは保守チームの各業務の全体像を把握し、保守に係るセンターとの調整、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>本番稼働開始から令和 10 年 7 月 31 日までの間は、設計・開発体制の各チームリーダー等の、本システムの設計・開発において主要な役割を</li> </ul>



		担い、開発内容を十分に理解しており、不具合等が発生した際に迅速に対応できる者から構成される特別体制を確保すること。 ・ 令和 10 年 8 月 1 日以降のシステム保守においても、設計・開発体制の各チームリーダー等の、本システムの設計・開発において主要な役割を担い、開発内容を十分に理解しており、不具合等が発生した際に迅速に対応できる者に助言を求めることが可能な体制を確保することが望ましい。
6	【受注者】 運用チーム	・ 本番稼働開始から令和 10 年 7 月 31 日までの間、本システムの運用を担う。 ・ 設計・開発体制の各チームリーダー等の、本システムの設計・開発において主要な役割を担い、開発内容を十分に理解しており、不具合等が発生した際に迅速に対応できる者から構成される特別体制を確保すること。 ・ 各機能・サブシステムの設計・構築チームや運用チーム（令和 10 年 8 月以降はインフラ運用事業者）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業務に当たること。
7	【受注者】 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注者としての責任を持つ。
8	【受注者】 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注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

受注者におけるプロジェクト全体管理者には、本システムと同種・同等規模のシステム構築及びクラウドサービスを活用したシステムの設計・構築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

### (2) 設計・構築チームリーダー

設計・構築チームリーダーは、本システムと同種・同等規模のシステム構築及びクラウドサービスを活用したシステムの設計・構築の経験年数を 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  
（アプリケーションエンジニア試験の合格者を含む）
- ・ ネットワークスペシャリスト試験の合格者  
（テクニカルエンジニア（ネットワーク）試験の合格者を含む）
- ・ 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) 設計・構築チーム

以下に記載する Microsoft 認定資格全てについて、クラウドサービスの設計・構築担当者のうちそれぞれ少なくとも 1 名は保有していること。

- ・ Azure Solutions Architect Expert (AZ-305)  
（AZ-303 及び AZ-304 の両方を保有する場合を含む）
- ・ Microsoft Cybersecurity Architect (SC-100)
- ・ Microsoft 365 Administrator (MS-102)

(MS-100 及び MS-101 の両方を保有する場合を含む)

(4) 運用チームリーダー

運用チームリーダーは、本システムと同種・同等規模のシステム及びクラウドサービスを活用したシステムの運用の経験年数を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の認定資格者  
(ITIL v3 エキスパート又は ITIL v2 マネージャーでも可)
- ・ 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) 保守チームリーダー

保守チームリーダーは、本システムと同種・同等規模のシステムの保守の経験年数を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年以上有すること。

(6) 保守チーム

保守チーム担当者のうち少なくとも1名は Microsoft 認定資格「Microsoft Azure Administrator Associate」(AZ-104) 又は「Microsoft Azure Administrator」(AZ-103) を保有していること。

(7) 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又は資格登録者
- ・ 特定非営利活動法人日本システム監査人協会 (SAAJ) が認定する公認システム監査人 (CSA) 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

### 5.3. 作業場所

---

(1) 原則

本件調達に係る作業については、原則として、受注者の社内で行い、本調達の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、受注者の責任及び負担において用意すること。なお、本システムの構築拠点と本システムとの間を接続するネットワークや、構築拠点到設置するネットワーク機器、及び構築業務に必要な機器（端末、プリンタ等）についても受注者にて準備を行うこと。また、必要に応じてセンターが現地確認を実施することができるものとする。

(2) 移行作業

情報システムの移行作業についてはセンターが指定する場所（受注者の社内又はセンターが指定するデータセンター等）で行うこと。詳細については、センターと協議し、決定するものとする。

(3) 移行期間等に係る補足

移行期間及び稼働開始直後（最長 2 週間程度）は、迅速かつ効率的な対応を行うことを目的としてセンター本部に設置する 4 席程度の作業場所を利用することができる。詳細は「別紙 2 要件定義書 4.10 移行に関する事項（12）問合せ対応」を参照すること。

## 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とおりである。

- (1) 本調達に係る業務以外の目的で利用しないこと（本契約終了後も同様とする。）。
- (2) 本調達に関してセンターが開示した情報、契約履行過程で生じた成果物（印刷した帳票を含む。）及び本調達を履行する上で知り得た一切の情報（公知のものを除く）を、いかなる場合にも第三者（センターが事前に書面により開示することを承諾した者を除く）に開示又は漏らしてはならないものとし、そのために必要な措置を講じること。
- (3) センターと合意した作業場所からの情報の持出しを禁止すること。
- (4) 受注者は、本調達に係る業務を実施するに当たり、上記(1)以外での利用を含む情報セキュリティインシデントの発生、又は、発生する可能性を認知した場合は、受注者の責任及び負担において、速やかにセンターへ報告し、機密情報を回収するために必要な措置を講じ、被害を最小限に抑えるよう最大限の努力を払うこと。また、受注者の責に起因する情報セキュリティインシデントにより生じた損害に対する賠償等の責任を負うこと。受注者は、上記の措置に加え、受注者の責任及び負担において、速やかに、次に掲げる措置を講じること。
  - ・ 情報セキュリティインシデントの内容及び影響範囲の調査・報告
  - ・ 情報セキュリティインシデントに対応するための手順等の作成・報告
  - ・ 情報セキュリティインシデントに対応するための対応手順等に基づく報告及び措置の実施
  - ・ 情報セキュリティインシデントによって被害を受けたセンター情報システムの復旧措置
  - ・ センターの指示に基づく措置の実施
  - ・ 情報セキュリティインシデントの具体内容及び原因並びに実施した対応措置等を内容とする報告書の作成及び提出
  - ・ 再発防止対策の迅速な立案及び提出並びにセンターが承認した後における同対策の実施
- (5) 受注者は、本調達の履行に際し、本システムにセンターの意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、センターと連携して原因を調査し、排除するための手順及び体制（例えば、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、センターから要求された場合には提出する等）を整備すること。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提出すること。
- (6) 受注者は、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って復元不可能な状態にし、センターに報告すること。
- (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、必要に応じてセンター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、センターと協議の上、改善策を実施すること。

- (9) 以上の要件における受注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センターの承認を得ること。なお、設計・構築実施計画書や運用・保守作業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

調達公示時点で最新の「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。なお、公示後に同基準の改定があった場合は、改定の都度、最新版への対応についてセンターと協議のうえに対応を決定すること（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・構築し、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、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、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当たり、「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 27 年 5 月 21 日内閣サイバーセキュリティセンター（現：内閣官房国家サイバー統括室））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センターと協議の上決定し、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、センター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、センター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、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、センター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、必要な管理監督及び教育を行うこと。
- (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、事前にセンターの許可を得ること。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、受注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（情報システム上のログによるもの等）を残すこと。
- (7) 受注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の保護に関する法律（平成 15 年法律第 57 号）その他適用ある法令に基づく請求が行われた場合には、速やかにセンターに通知してその指示を受けること。また、センターによる同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を行い、これを可能とする体制及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續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、受注者はその旨を証明する書類を提出し、センターの承認を得た上で実施すること。
- (9) センターが必要と認めた場合であってその態様が受注者の業務その他の営業を著しく妨げるものでないとき、センター又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) 受注者は、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、センター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、センターは本業務の契約を解除することができる。

#### 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 年法律第 128 号）、個人情報の保護に関する法律、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）等、適用される法令等を遵守し履行すること。

なお、受注者が個人情報取扱事業者に該当する場合には、個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）における個人情報取扱事業者等の義務等に係る規定（第 4

章) もあわせて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、センターが情報システム監査の実施を必要と判断した場合は、センターが定めた実施内容（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注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センター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、対応案をセンターと協議し、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) 本システムの設計・構築、運用・保守工程において、センター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) センター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）をセンターとの協議の上、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) 本システムにセンター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、センター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センターとの協議の上、必要と判断された場合は提出すること。
- (4) 本システムの設計・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導入ガイドライン」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) 本システムの開発環境、本番環境、検証環境を分離し、各環境で取り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) 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 7 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」に示す。各項目に対して漏れなく対応すること。

表 7 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、情報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、「別紙 2 要件定義書」に記載の要件を満たすこと。

## 7. 成果物の取扱いに関する事項

### 7.1. 知的財産権の帰属

- (1) 受注者が作成した成果物（提出書類、設定等）について、著作権法（昭和 45 年法律第 48 号）第 21 条から第 28 条までに定める著作権は、「7.3. 検査」に定める検査完了により、センターへ帰属するものとする。なお、受注者が本調達より前に留保している著作物に関しては、事前にセンターに提示するとともに、改修や再利用に関する条件を明示し、センターによる将来にわたる利用が行えるように調整すること。
- (2) 受注者が作成した成果物について、センター及びセンターが指定する第三者に対し、同法第 18 条から第 20 条までに定める著作権人格権を行使しないこと。
- (3) 受注者は、全ての成果物が第三者の著作権、特許権その他の知的財産権を侵害していないことを保証すること。また、本調達において第三者の知的財産権又はノウハウを使用・実施する場合、受注者は、その使用・実施に対して一切の責任を負うこと。

- (4) 受注者が納入した成果物に関わる知的財産権及び製造者責任について、第三者からの請求を受け、又は訴訟を提起された場合には、受注者が自らの責任と費用負担において対応すること。
- (5) 納入される成果物に第三者が権利を有する著作物が含まれる場合、受注者は、当該著作物の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、受注者は当該著作物の内容について事前にセンターの承認を得ることとし、センターは当該著作物を許諾条件の範囲で使用するものとする。

## 7.2. 契約不適合責任

---

- (1) センターは、成果物の納入を受けた後、その内容が本契約の内容又は本システムの性質上仕様として当然に要求されるものに適合しないものであること（バグを含む。）を発見したときは、受注者に対して、受注者の費用でこれを修補等の追完を請求することができる。ただし、その不適合がセンターの責めに帰すべきものであるときは、追完を請求することができない。
- (2) センターは、相当と認める期間を定め、受注者に対し上記(1)の催告を行ったにもかかわらず、その追完がないときは、センターは、受注者に対してその不適合の程度に応じて代金の減額請求をすることができる。  
ただし、以下に掲げる場合には、センターは追完の催告をすることなく、受注者に対して直ちに代金の減額請求をすることができる。
  - ・ 履行の追完が不能であるとき。
  - ・ 受注者が履行の追完を拒絶する意思を明確に表示したとき。
  - ・ 契約の性質により、履行期限前に履行しなければ本契約の目的を達することができない場合において、受注者が履行期限までに履行の追完をしないでその期限を経過したとき。
  - ・ 上記のほか、センターが追完の催告をしても受注者が追完する見込みがないことが明らかであるとき。
- (3) センターは、上記(2)の規定にかかわらず、本契約の不適合により損害を被ったときは、受注者に対して、損害の賠償を請求することができる。
- (4) 受注者は、本契約についてセンターが検査を行った日を起算日として1年間、成果物に対する契約不適合に係る責任を負うものとする。ただし、検査完了時において、受注者が当該不適合を知り若しくは重過失により知らなかった場合又は当該不適合が受注者の故意若しくは重過失に起因する場合にはこの限りでない。

## 7.3. 検査

---

- (1) 本業務の受注者は、成果物について、納入期限までにセンターに対し内容の説明を実施して検査を受けること。
- (2) 受注者は、本システムの稼働後対応については、契約期間中の毎月末日（当該末日がセンターの休日に該当する場合は、その翌営業日）に、履行に係る検査を受けること。
- (3) 検査の結果、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、変更点についてセンターに説明を行った上で、指定された日時までに再度納入し検査を受けること。



## 8. 入札参加に関する事項

### 8.1. 競争参加資格

---

応札者は以下の要件を全て満たすこと。

- (1) 予算決算及び会計令（昭和 22 年勅令第 165 号）第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。
- (2) 予算決算及び会計令第 71 条の規定に該当しない者であること。
- (3) 公告日において令和 7・8・9 年度全省庁統一資格の「役務の提供等」の「A」の等級に格付けされ、競争参加資格を有する者であること。

### 8.2. 公的な資格や認証等の取得

---

応札者は以下の要件を全て満たすこと。

- (1) 業務を遂行する組織が、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。）の認定を有していること。
- (2) 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。

### 8.3. 受注実績

---

応札者は、最終需要者から直接受注したか否かにかかわらず、以下の設計・構築業務を実質的に遂行した実績を全て有すること。ただし、受注者自らのシステム及び親会社及び子会社、同一の親会社を持つ会社のシステムに関する実績を除く。

- (1) 応札者は、Microsoft Azure を活用したシステム基盤（複数の情報システムが同一基盤上で稼働するもの）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、1,000 名以上の利用者が利用するクライアントシステム（管理機能を含む）の設計・構築を行った実績を過去 3 年以内に有すること。
- (3) 応札者は、官公庁及び独立行政法人等公的機関に係る情報システムの設計・構築の実績を過去 3 年以内に有すること。

### 8.4. 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、当該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認めない。

- (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。

## 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) 本業務の受注者は、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。ただし、主たる部分を除く一部について、受注者があらかじめ再委託の申請を行い、センターが承認した場合はこの限りでない。
- (2) 再委託先事業者の社員は、プロジェクト全体管理者、設計・構築チームリーダー、運用チームリーダー及び保守チームリーダーとすることはできない。
- (3) 受注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注者の責任とする。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、本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等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とする。）
- (5) 再委託において、入札金額の2割を超える再委託を予定する事業者がいる場合、当該再委託先が「2.4 調達案件間の入札制限」に示す要件を満たすこと。
- (6) 契約金額に対する再委託予定金額の割合は、原則2分の1未満とすること。

### 9.2. 承認手続

---

- (1) 本調達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」をセンターに提出し、あらかじめ承認を得ること。
- ・ 再委託の相手方の商号又は名称、住所、資本関係や役員等の情報を含めた基本情報及び作業場所
  - ・ 再委託を行う業務の範囲、再委託に従事する従業員の所属・国籍
  - ・ 再委託を行う理由、再委託に係る業務の履行能力（実績・情報セキュリティに係る資格・研修実績を含む。）、履行体制図、インシデント対応手順、再委託予定金額
  - ・ その他センターが求める事項
- (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一式をセンターに提出し、承認を得ること。
- (3) 再々委託の場合には、当該再々委託を行う業務の範囲及び理由等必要事項を上記(1)と同様に書面一式でセンターに提出し、あらかじめ承認を得ること。

- (4) 受注者は、本契約上受注者に求められる水準と同等の情報セキュリティ水準を、再委託の相手方又は再々委託の相手方においても確保すること。また、受注者は、再委託の相手方又は再々委託の相手方が実施する情報セキュリティ対策及びその実施状況並びに「6 作業の実施に当たっての遵守事項」の遵守についてセンターに報告すること。

### 9.3. 再委託先の契約違反等

再委託先又は再々委託先において、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、受注者が一切の責任を負うとともに、センターは、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「2.2.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」及び「2.3.情報システム稼動環境に関する事項 (2)クラウドサービス構成」を参照すること。

### 10.2. クラウドサービス利用に係る成果物の取扱い

クラウド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。

### 10.3. SaaS サービスの契約に当たっての留意事項

本システムで受注者が提案する SaaS サービスは、本調達の契約期間終了後も、SaaS サービスの契約期間終了前に契約の延長又は他の引継ぎ先（センター又は運用事業者を想定）への引継ぎ等を行うことで、SaaS サービスをそのまま継続利用することを想定している。引継ぎに際しては、必要に応じて引継ぎ先及びクラウドサービスプロバイダとの間で書面による契約等を行い、しかるべく管理者権限の引渡し等を行うこと。

## 11. その他特記事項

### 11.1. 前提条件等

- (1) 本調達受注後に調達仕様書本紙の内容の一部について変更を希望する場合は、その変更の内容、理由等を明記した書面をもってセンターに申入れを行うこと。同申入れがあり、双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名押印することによって変更を確定する。
- (2) 受注者は、本調達の円滑な運営を図るため、センターと連絡を密にするとともに、本調達を実施する上で不明な事項が生じた場合は、必ずセンターと調整を行うものとする。
- (3) 受注者は、センターが本契約に基づき、情報の開示又は作業の改善を求めた場合には、速やかに対応するものとする。

- (4) 受注者は、施設設備等の管理及び運用に関し、センターやその他関係組織が定める諸規程及びセンターの指示を遵守するものとする。
- (5) 本仕様書に明示されていない事項で必要な作業が生じたとき、又は本調達の内容を変更する必要があるときは、センターと受注者で協議の上、決定するものとする。
- (6) 本仕様書の内容又は解釈等に疑義が生じた場合は、センターと受注者で協議の上、決定、解決するものとする。

### 11.2. 機器等のセキュリティ確保

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、調達時点において、当該製品に Critical または High レベルの既知の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。

### 11.3. 入札公告期間中の資料閲覧等

本調達に係る資料等の閲覧については、以下のとおりとする。なお、資料の閲覧に当たっては、必ず事前に(5)に定めるメールアドレス宛て連絡の上、閲覧日時を調整すること。また、資料を閲覧した者は、(6)に掲げる資料（特に機密度の高い情報を除いた版）及び「12. 附属文書」に掲げる別紙様式の交付を受けることができる。交付を希望する者は、その旨上記連絡の際に併せて申し出ること。閲覧後、センターが管理するオンラインストレージを利用してデータを交付する。

#### (1) 資料閲覧場所

日本司法支援センター本部

#### (2) 閲覧期間及び時間

入札公告期間中、一定期間での実施を予定

センターの休日を除く日の 10 時から 17 時まで（12 時から 13 時を除く。）のうち、最大 2 時間とする。

#### (3) 閲覧手続

1 事業者について最大 3 回までとし、閲覧人数は最大 6 名まで。閲覧希望日の前日までに財務会計課担当者宛てに閲覧予約依頼をし、閲覧日当日までに別記様式「機密保持誓約書」を作成の上、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、本調達の応札に係る検討及び提案書等作成以外には使用しないこと。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。閲覧資料の複写等による閲覧内容の記録は行わないこと。

#### (5) 連絡先

日本司法支援センター本部財務会計課

電話 050-3381-1573

Email : keiyaku@houterasu.or.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。

- ・ 現行システムの設計書類（PDF 形式/Microsoft Office 形式）
- ・ 情報セキュリティ関係規程（PDF 形式）
- ・ 現行システム運用事業者作成の運用報告書（PDF 形式）

- ・ 業務統合管理システムの基本設計書の一部（PDF 形式/Microsoft Office 形式）
- ・ 環境払い出し依頼票のサンプル（Microsoft Office 形式）

#### 11.4. クラウドサービス利用料の概算見積り

本調達では、本システムで利用するパブリッククラウドサービス（Microsoft Azure 本番環境・検証環境）の費用はセンターが別途負担することから、そのコストも含めた総合的な観点での評価を実施する。

受注者は、「別紙 16 クラウドサービス利用料概算見積りテンプレート」を利用して、令和 15 年 5 月 31 日までの間に本システム（ラック渡しのサブシステム分を除く）で利用する具体的な仮想サーバやデータベース等のクラウドサービス（Microsoft Azure 本番環境・検証環境）とその数量を提示すること。なお、本概算見積りに当たっては、Azure ハイブリッド特典（Windows Server・SQL Server）の適用が可能なリソースであっても、Azure ハイブリッド特典を適用せず、ライセンス費込みの見積もりとすること。

## 12. 附属文書

- 別紙 1 作業スケジュール
- 別紙 2 要件定義書
- 別紙 3 システム構成一覧
- 別紙 4 構築役務に関する分担表
- 別紙 5 調達対象に関する分担表
- 別紙 6 ラック渡しにおける構築役割分担
- 別紙 7 機能要求一覧
- 別紙 8 PowerBI 導入方針
- 別紙 9 システム構成概要図
- 別紙 10 NW ベンダーによる構築支援及び運用支援の想定について
- 別紙 11 センター拠点一覧（令和 8 年 1 月現在）
- 別紙 12 権限管理システムより取得可能な CSV ファイル概要
- 別紙 13 非機能要求マトリクス
- 別紙 14 セキュリティ対応要件一覧
- 別紙 15 主な運用・保守作業一覧
- 別紙 16 クラウドサービス利用料概算見積りテンプレート