「共通特実検索（検索部分）・商標検索・審判業務サーバ一式の更改に係るハードウェア等賃貸借及び保守等業務　一式」意見招請関係資料

特許庁総務部会計課

内訳

1. 意見招請に関する説明書
2. 調達仕様書（案）
3. 意見書

意見招請に関する説明書

特許庁総務部会計課

令和８年５月１５日付け官報に掲載のとおり、下記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。

記

１　調達内容

（１）購入物品等特定役務及び数量　「共通特実検索（検索部分）・商標検索・審判業務サーバ一式の更改に係るハードウェア等賃貸借及び保守等業務 一式」
詳細については、調達仕様書（案）を参照

２　意見の提出方法

（１）意見の提出期限　令和８年６月４日（木）　１２時００分（郵送の場合は必着のこと）

（２）提出先

〒100－8915　東京都千代田区霞が関三丁目４番３号
特許庁総務部総務課情報技術統括室
デジタル戦略調達班　加藤、吾妻 PA0G13@jpo.go.jp
電話番号 03-3581-1101 内線2506
特許庁総務部会計課契約第二班
契約第四係 河原、島貫 PAKEIYAKU04@jpo.go.jp
電話番号 03-3581-1101 内線2214
（人事異動等により担当者が変更となった場合は、新たに担当者となった者とする。）

３　仕様書案の交付

（１）交付期間　令和８年５月１５日（金）から令和８年６月４日（木）まで

（２）交付場所　特許庁ホームページによる
https://www.jpo.go.jp/news/chotatsu/iken/iken-shosei/index.html
※紙配布は行っておりません。

４　仕様書案の説明会

（１）開催日時　令和８年５月２１日（木）１０時３０分

（２）開催場所　オンライン開催　（「Microsoft Teams」を活用して実施）
参加希望の場合は、本説明書「２（２）」に記載の連絡先へ、オンライン参加者連絡先（企業又は団体名、担当者氏名、電話番号、メールアドレス）を令和８年５月２０日（水）１２時までに登録すること。連絡の際は、メールの件名（題名）は１．（１）の件名を記載すること（説明会の前にテスト連絡をする可能性があります。）。

５　資料閲覧の申込方法

調達仕様書（案）２２ページに記載。

共通特実検索（検索部分）・商標検索・審判業務サーバー式の更改に係る
ハードウェア等賃貸借及び保守等業務 一式
調達仕様書(案)

令和８年５月

特　許　庁

ー 目次 ー

1. 調達案件の概要に関する事項

1.1.調達件名

「共通特実検索（検索部分）・商標検索・審判業務サーバー式の更改に係るハードウェア等賃貸借及び保守等業務 一式」

1.2.調達の背景

現在稼動中の共通特実検索（検索部分）・商標検索・審判業務サーバー式の賃貸借期間は、令和 10 年 5 月に終了する予定である。共通特実検索（検索部分）・商標検索・審判業務サーバー式が提供するサービスの継続等の観点から、令和 10 年 5 月から稼動開始できるよう新たなハードウェア等の賃貸借及び保守等業務を調達し、サーバー式を更改する必要がある。

1.3.調達目的及び調達の期待する効果

本調達の目的及び期待する効果を以下に示す。本調達の共通特実検索（検索部分）・商標検索・審判業務サーバー式(以下、「本サーバー式」という。)を含む特許庁全体の方針として、安定稼動・低コストを最重要課題と位置付けている。

表 1.3-1 目的及び期待する効果

No.	目的及び期待する効果
1	【安定したサービスの提供】 ・システム特性を考慮した必要十分な性能、冗長性等を備える機器の調達や、速やかな障害復旧等が可能な保守業務等により、現行システムから継続して利用者に対して安定したサービスを提供する。
2	【コスト削減】 ・各種サーバの統合、仮想化によりコスト削減を図る。 ・作業の自動化・効率化やソフトウェアライセンスの最適化等により、コスト削減を図る。 ・仮想化基盤の運用管理機能を本調達の範囲外である共通仮想化基盤（JPO-PF）の仮想管理サーバへ集約することで、コスト削減を図る。 ・「ハードウェア導入ガイドライン」に記載された作業のうち一部の作業を不要とし、コスト削減を図る。

1.4.用語定義

本調達仕様書（以下、「本仕様書」という。）に記載される用語の定義について以下に示す。

表 1.4-1 用語定義

No.	用語	用語略称	説明
1	本システム	―	共通特実検索システム（検索部分）、商標検索システム及び審判業務システムを指す。
2	現行システム	―	本調達によって更改を予定する稼動中の本システムを指す。
3	次期システム	―	本調達によって更改された本システムを指す。
4	共通特実検索（検索部分）・商標検索・審判業務サーバー式	本サーバー式	本システムのうち、本調達のハードウェア、ソフトウェア及び作り込み機能を指す。
5	本調達の機器	―	本サーバー式のうち、ハードウェアを指す。なお、「等」を付記した場合は、OS、ソフトウェア製品を含む。
6	共通特実検索システム（検索部分）	―	本サーバー式上で稼動する共通特実検索システム（検索部分）（庁内）及び共通特実検索システム（検索部分）（庁外）の総称として用いる。
7	共通特実検索システム（検索部分）（庁	―	本サーバー式上で稼動するシステムである。特許庁職員向けに検索情報（未公開情報を含む）を提供する。

No.	用語	用語略称	説明
	内）		
8	共通特実検索システム（検索部分）（庁外）	―	本サーバー式上で稼動するシステムである。一般ユーザ向けに公開情報のみを提供する。
9	商標検索システム	―	本サーバー式上で稼動するシステムである。
10	審判業務システム	―	本サーバー式上で稼動するシステムである。
11	ソフトウェア	―	OS及びソフトウェア製品の総称として用いる。
12	ソフトウェア製品	―	既製のソフトウェア製品を指す。オープンソースソフトウェア（OSS）等を含む。
13	ユーザアプリケーションプログラム	UAP	以下APベンダにより開発された業務アプリケーションを指す。UAPは本調達の範囲外である。
14	作り込み機能	―	以下HWベンダによってスクリプト等で作成するソフトウェアの補完機能を指す。
15	ハードウェアベンダ	HWベンダ	特許庁システムに係るハードウェア等の設計・構築、保守を行う業者を指し、調達案件ごとに存在する。本仕様書においては受注者を指す。
16	アプリケーション開発ベンダ	APベンダ	UAP業者ともいう。特許庁システムに係る業務アプリケーションの設計・開発を行う業者を指し、調達案件ごとに存在する。本仕様書においては本システムの業務アプリケーションの設計・開発業者を指す。
17	システムインテグレーションベンダ	SIベンダ	特許庁システムに係るサービスレベル管理、アプリケーション開発・改造支援、インフラ導入支援、データベースコンテンツ管理等のシステムインテグレーションサービスを提供する業者を指す。
18	オペレーションベンダ	OPベンダ	特許庁システムに係るオペレーション、エンドユーザサポート等のオペレーションサービスを提供する業者を指す。

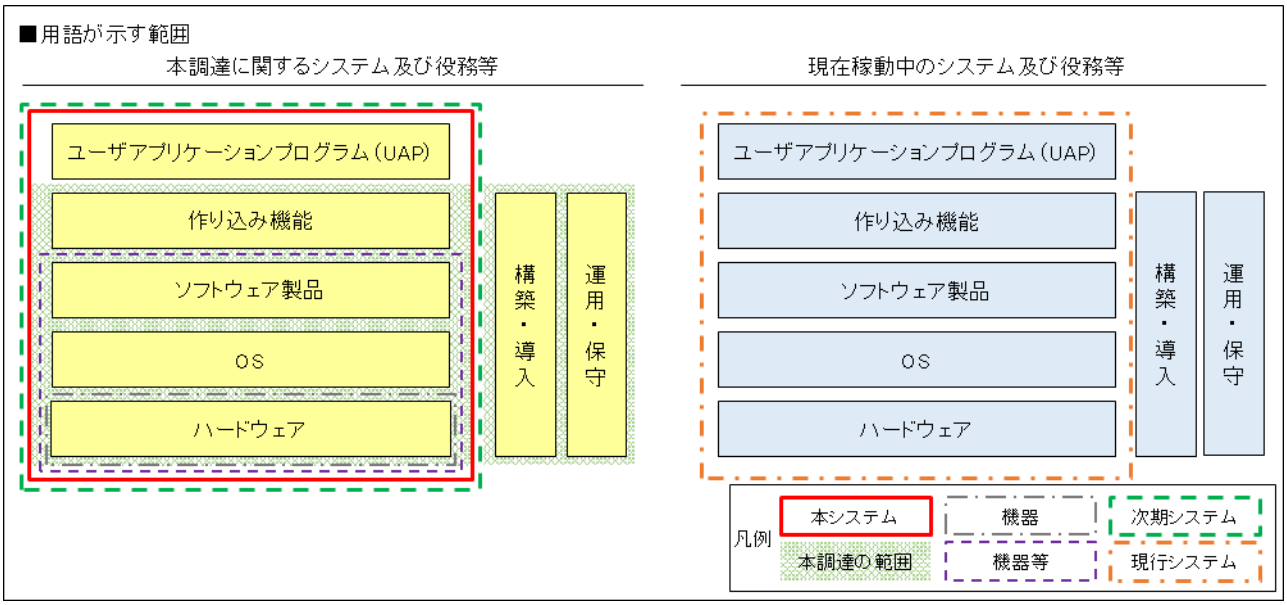


図 1.4-1 用語定義(図)

1.5.業務・情報システムの概要

共通特実検索（検索部分）・商標検索・審判業務サーバー式の業務概要を以下に示す。

表 1.5-1　共通特実検索（検索部分）の業務概要

No.	業務	内容
1	検索情報蓄積業務	文献データや登録論理式等の検索情報等を文献照会システム、F ターム検索システムを経由することにより、共通特実検索システム（検索部分）（庁内）および共通特実検索システム（検索部分）（庁外）への蓄積を可能とする。 ① 文献照会システムから F ターム検索システムへ検索情報の文献データを送信する ② F ターム検索システムから共通特実検索システム（検索部分）（庁内）へ検索情報等を送信する ③ F ターム検索システムから受領したデータを蓄積する。文献データから共通特実検索システム（検索部分）（庁内）用と共通特実検索システム（検索部分）（庁外）用の検索インデックスをそれぞれ作成する。共通特実検索システム（検索部分）（庁外）用のデータを共通特実検索システム（検索部分）（庁外）に送信する ④ J-PlatPat に検索結果の一覧に使用する表示用情報を送信し、蓄積結果の応答を受信する
2	検索業務（審査官等による検索）	審査官等が、特実検索クライアントから F ターム検索システムを経由し、共通特実検索システム（検索部分）（庁内）に論理式等を送る。共通特実検索システム（検索部分）（庁内）は受け取った論理式等に対応する検索結果を F ターム検索システム経由で特実検索クライアントに返信し、特実検索クライアントで検索結果の表示を行う。 ① 特実検索クライアントの画面上から論理式等の要求を F ターム検索システムに送信する ② F ターム検索システムから論理式等の要求を共通特実検索システム（検索部分）（庁内）に送信する ③ 共通特実検索システム（検索部分）（庁内）の検索情報等を検索し、検索結果を F ターム検索システムに応答する ④ F ターム検索システムで検索結果を編集し、特実検索クライアントに応答する
3	検索業務（一般ユーザーによる検索）	一般ユーザは、J-PlatPat から共通特実検索システム（検索部分）（庁外）に論理式等を送り、共通特実検索システム（検索部分）（庁外）は受け取った論理式等に対応する検索結果を J-PlatPat に返信し、J-PlatPat で検索結果の表示を行う。 ① ユーザからの検索要求を元に J-PlatPat より論理式の要求を共通特実検索システム（検索部分）（庁外）に送信する ② 共通特実検索システム（検索部分）（庁外）の検索情報等を検索し、検索結果を J-PlatPat へ応答する。

表 1.5-2　商標検索システムの業務概要

No.	業務	内容
1	6 条審査	商標の出願をする際、その商標をどのような商品や役務（サービス）に使用するか指定するにあたり、商品・役務の記述が明確か否かの審査を行う。商標検索システムでは、明確であると認められている商品・役務のデータを蓄積したデータベースを構築し、これを検索する機能を提供している。
2	4 条審査	出願された商標が、他人の登録商標と同一または類似するものか否か等の審査を行う。商標検索システムでは、登録商標等を蓄積したデータベース（商標基本マスタ）を構築し、これを検索する機能を提供している。

表 1.5-3 審判業務システムの業務概要

No.	業務	内容
1	方式調査	① 審判事件の担当部門を決定し、方式調査担当者を選任する。 ② 審判請求書等の受付書類を目視調査する前準備として、識別番号の調査や共同請求違背がないか等の機械チェックを行う。 ③ 前置移管の対象かを判断する。 ④ 受付書類に対する目視調査を行い、方式処分を設定する。 ⑤ 登録原簿に審判事件の予告登録をする。 ⑥ 審判事件の実体審理が開始できる状態にする。
2	起案・決裁（事務起案）	① 方式調査に係る発送書類を起案・決裁する。 ② 発送書類の照合確認、発送依頼、送達報告書の作成及び指定期間の経過の待ち合わせを行う。
3	起案・決裁（審理起案）	① 実体審理に係る発送書類を起案・決裁する。 ② 発送書類の照合確認、発送依頼、送達報告書の作成及び指定期間の経過の待ち合わせを行う。
4	訟務	① 訴え提起の通知を基に出訴事件情報を作成する。 ② 訟務結果を受け入れ、出訴事件情報に記録する。
5	確定	① 審判事件の確定予定日を設定する。 ② 審判事件を確定する。

上記業務を行うための本システムの概要（イメージ）は、以下のとおり。

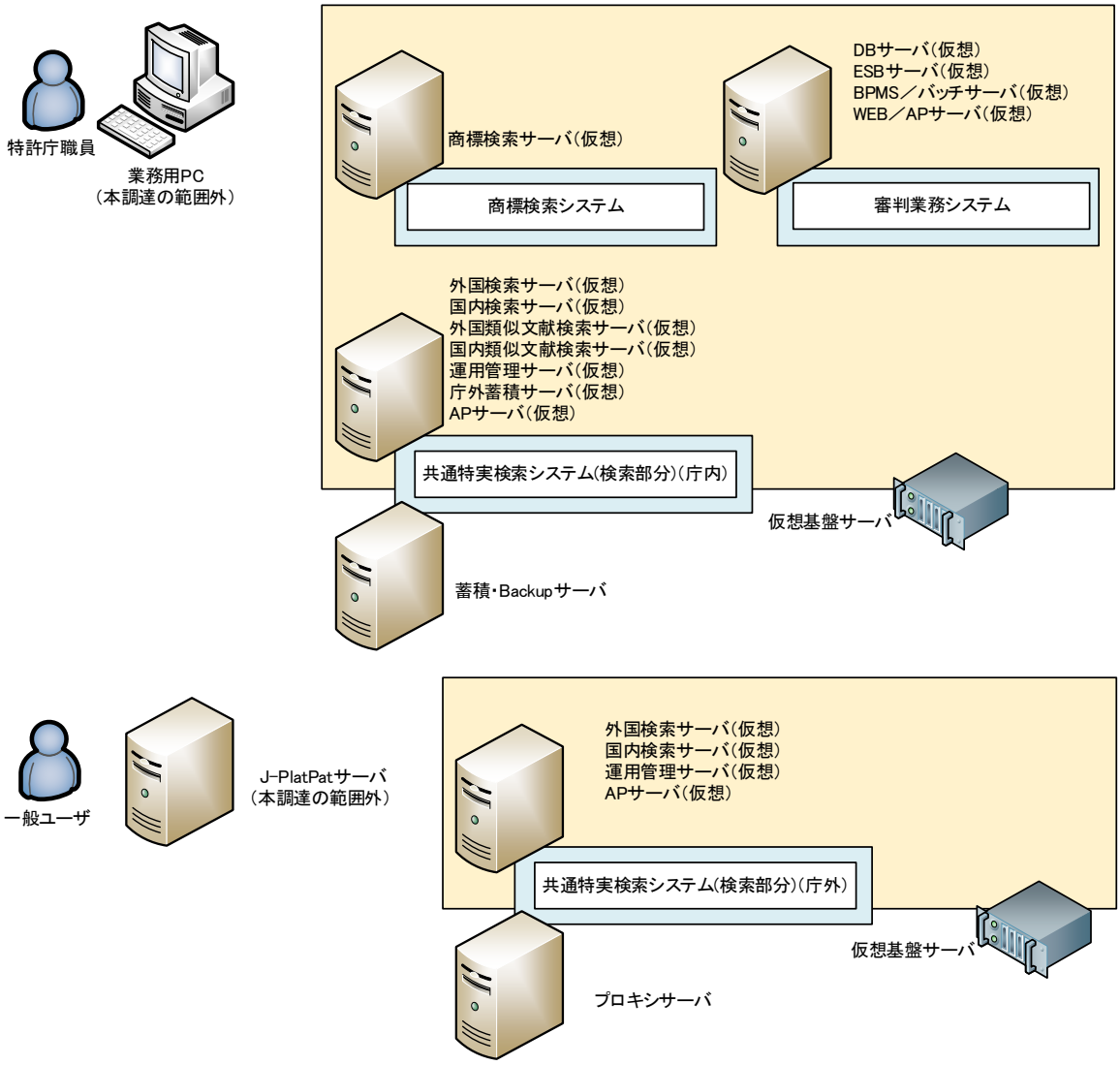


図 1.5-1　本システムの概要図

1.6.契約期間

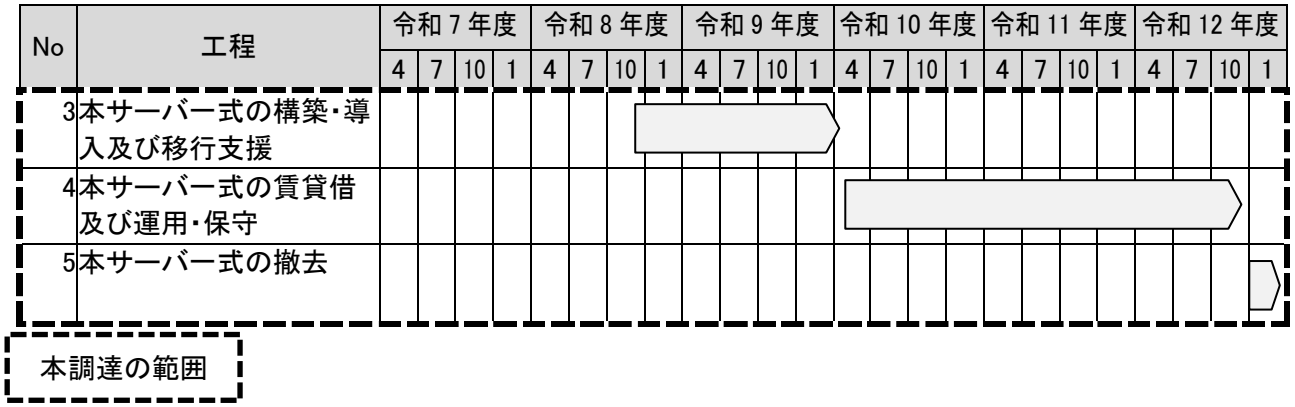
契約期間は、契約締結日から令和 12 年 12 月 31 日までとする。本サーバー式の賃貸借は、令和 10 年 5 月 8 日から令和 12 年 12 月 31 日までの月極によるものとし、本サーバー式の撤去作業は、令和 13 年 3 月 31 日までに行うこととする。なお、賃貸借は 2 年間延長することを想定しているが、法令及び予算に基づき、今後変更することがあり得る。延長に際しての特記事項については「10.2.導入・調達条件」(8)～(10)を参照すること。

1.7.作業スケジュール

本調達に係る作業スケジュールを以下に示す。

表 1.7-1　作業スケジュール

No	工程	令和 7 年度				令和 8 年度				令和 9 年度				令和 10 年度				令和 11 年度				令和 12 年度			
		4	7	10	1	4	7	10	1	4	7	10	1	4	7	10	1	4	7	10	1	4	7	10	1
1	設備条件整理																								
2	調達仕様書等作成支援業務																								



2. 調達案件及び関連調達案件

2.1.調達案件の一覧

表 2.1-1 本調達案件及び関連調達案件の概要一覧

No.	調達案件名	調達の方式	実施時期 （契約期間）	備考
1	共通特実検索（検索部分）・商標検索・審判業務サーバー式の更改に係るハードウェア等賃貸借及び保守等業務 一式	一般競争入札 （総合評価落札方式）	令和 10 年 5 月～ 令和 13 年 3 月	本調達案件
2	特許庁ネットワーク一式の更改に係るハードウェア等賃貸借及び保守等業務 一式	一般競争入札 （総合評価落札方式）	令和 5 年 5 月～ 令和 10 年 3 月	2～4 年間の延長想定
3	運用管理サーバー式の更改に係るハードウェア等賃貸借及び保守等業務 一式	一般競争入札 （総合評価落札方式）	令和 4 年 4 月～ 令和 9 年 3 月	2 年間の延長想定

3. 情報システムに求める要件に関する事項

受注者は、「別紙 1 要件定義書」の要件を満たす本サーバー式を導入すること。

4. 作業の実施内容に関する事項

4.1.構築・導入に係る作業

受注者は、本サーバー式の構築・導入に係る作業を実施すること。各作業の詳細及び役割分担については、「ハードウェア導入ガイドライン」及び「別紙 1 要件定義書」によるものとする。ただし、下記作業については不要とする。

4.1.1.「ハードウェア導入ガイドライン」に記載された構築・導入に係る作業

「ハードウェア導入ガイドライン」に記載された構築・導入に係る作業を以下に示す。なお、本調達ではハードウェア導入ガイドラインにおける【UAP あり】の工程を参照すること。

表 4.1-1 ハードウェア導入ガイドラインに記載された構築・導入に係る作業内容一覧

No.	作業工程	作業内容
1	全体管理	契約締結からサービス開始までのプロジェクト管理
2	工事計画	機器搬入・据付の工事計画
3	機器発注／出荷前検査	出荷元への機器発注、出荷元での出荷前検査
4	現地調査 ／搬入・据付・調整等工事	現地調査／養生、機器の搬入、設置、ラッキング、信号ケーブル・電源ケーブル接続及びそれに関わる各種調整
5	環境定義設計※1	OS、ミドルウェアについての具体的な方針の検討／決定、ソフトウェア要件、信頼性要件、機能要件等を十分に考慮した上での設定値の設計、環境設定定義書の作成
6	OS 及びミドルウェア導入設定	環境設定定義書に基づく OS、ミドルウェアのインストール、設定
7	【UAP あり】 納品前検査・引渡し ／納品前チューニング	受注者が調達範囲内の機器を使用して行う納品前検査の試験・試験完了後の AP ベンダへの機器引渡し／試験の結果、不具合がある場合のチューニング、再試験
	【UAP なし】 結合試験	受注者が調達範囲内の機器を使用して行う結合試験 試験の結果、不具合がある場合のチューニング、再試験
8	初期バックアップ取得	インストールされた OS、ミドルウェアのバックアップ及びその設定値のバックアップ取得
9	インタフェース導通試験	【UAP あり】 対象のプロトコルに対して実施する、導入機器と既存システム間でのインタフェース導通試験、ミドルウェア導通試験。HW ベンダが導入機器側の業務通信以外で使用されるプロトコルのインタフェース導通試験対応を実施し、AP ベンダが導入機器側の業務通信で使用されるプロトコルのインタフェース導通試験対応を実施する。
		【UAP なし】 HW ベンダが全ての対象のプロトコルに対して実施する、導入機器と既存システム間でのインタフェース導通試験、ミドルウェア導通試験
10	【UAP あり】 総合試験 ／UAP 業者のチューニング	UAP を動作させて実施する総合試験（システム間連動試験、連続運転試験、性能・高負荷試験、信頼性試験 等） ／試験の結果、不具合がある場合の OS、ミドルウェアに対する設定変更、目標性能を達成するためのチューニング

No.	作業工程	作業内容
	【UAP なし】 総合試験	総合試験（システム間連動試験、連続運転試験、性能・高負荷試験、信頼性試験　等） 試験の結果、不具合がある場合の OS、ミドルウェアに対する設定変更、目標性能を達成するためのチューニング
11	セキュリティ検査	【UAP あり】 納品前検査完了後に行うセキュリティ検査
		【UAP なし】 結合試験完了後に行うセキュリティ検査
12	運用に関する教育・研修・引継ぎ※2	運用マニュアル作成、OP ベンダへの教育・研修、運用マニュアル（Ⅲ異常時運用）の SI ベンダへの引継ぎ
13	環境設定に関する引継ぎ等	環境構築手順、環境変更手順の作成、環境設定に関する引継ぎ等／構成資産情報等の提出・提供
14	データ移行及びシステム移行	データ移行及びシステム移行における移行リハーサル、本番移行

※1 ただし、本調達においては環境設定定義書について、①現行機−更改機差分、②現用系−待機系差分、③本番機−試験機差分、④実機（本番機）差分、⑤実機（試験機）差分のチェックを省略してもよい。

※2 上記に合わせて環境差分チェック結果の引継ぎを省略してもよい。

4.2.運用・保守に係る作業

受注者は、本サーバー式の運用・保守に係る作業を実施すること。各作業の詳細については、「ハードウェア導入ガイドライン」及び「別紙 1 要件定義書」によるものとする。

4.2.1.「ハードウェア導入ガイドライン」に記載された運用・保守に係る作業

「ハードウェア導入ガイドライン」に記載された運用・保守に係る作業を以下に示す。また、本作業は表 4.1−1 に示す作業工程時においても必要に応じて実施すること。

表 4.2−1　ハードウェア導入ガイドラインに記載された運用・保守に係る作業内容一覧

No.	作業工程	作業内容
1	システム運用・稼動	ソフトウェアパッチ情報収集、報告、パッチ適用、適用後の動作確認、設定変更実施等
2	故障保守※	ハードウェア、ソフトウェア故障時の原因調査、修復作業、報告
3	消耗品交換	消耗品の交換

※　ただし、本調達においてはハードウェア故障時の原因究明は省略してもよい。

4.3.撤去に係る作業

(1)　受注者は、本サーバー式の撤去に係るすべての費用を本契約に含めたうえで、撤去に係る作業を実施すること。各作業の詳細については、「ハードウェア導入ガイドライン」及び「別紙 1 要件定義書」によるものとする。「ハードウェア導入ガイドライン」に記載された撤去に係る作業を以下に示す。

表 4.3−1　ハードウェア導入ガイドラインに記載された撤去に係る作業内容一覧

No.	作業工程	作業内容
1	撤去	運用終了後の機器の撤去計画作成、撤去工事実施

(2)　受注者は、次期システムから次々期システムへの更改などにより特許庁が納入物の使用を終了する場合、受注者の責任において速やかに撤去するとともに、納入前と同等の状態に原状復帰すること。

(3)　納入物の使用を終了してから撤去までの間に、特許庁が本サーバー式への切り戻しによるサービスの再

開を必要と判断した場合、受注者はサービス再開に必要な対応を行うこと。その際、新たな費用負担が必要な場合は、特許庁と別途協議のうえ、対応を決定すること。

4.4.情報資産管理標準シートの提示に係る記載内容

(1) 受注者は、「デジタル・ガバメント推進標準ガイドライン（以下、「標準ガイドライン」という。） 別紙 2 情報システムの経費区分」に基づく区分等に応じて契約金額の内訳を記載した資料を契約締結後速やかに提示すること。

(2) 受注者は、次に掲げる事項等について記載した情報資産管理標準シートを提示すること。なお、提示時期及び提示が必要となる情報資産管理標準シートの詳細については、特許庁と協議のうえ、決定すること。

① ハードウェアの管理
本サーバー式を構成するハードウェアの製品名、型番、ハードウェア分類、契約形態、保守期限等

② ソフトウェアの管理
本サーバー式を構成するソフトウェア製品の名称（エディションを含む。）、バージョン、ソフトウェア分類、契約形態、ライセンス形態、サポート期限等

③ 回線の管理
本サーバー式を構成する回線の回線種別、回線サービス名、事業者名、使用期間、ネットワーク帯域等

④ 外部サービスの管理
本サーバー式を構成するクラウドサービス等の外部サービスの外部サービス利用形態、使用期間等

⑤ 施設の管理
本サーバー式を構成するハードウェア等が設置され、又は情報システムの運用業務等に用いる区域を有する施設の施設形態、所在地、耐久性、ラック数、各区域に関する情報等

⑥ 公開ドメインの管理
本サーバー式が利用する公開ドメインの名称、DNS 名、有効期限等

⑦ 取扱情報の管理
本サーバー式が取り扱う情報について、データ・マスタ名、個人情報の有無、格付等

⑧ 情報セキュリティ要件の管理
本サーバー式の情報セキュリティ要件

⑨ 指標の管理
本サーバー式の運用及び保守の間、把握すべきKPI名、KPI分類、計画値等の案

⑩ 各データの変更管理
本サーバー式の運用及び保守において、上記の各項目についてその内容に変更が生じる作業をしたときは、当該変更を行った項目

⑪ 作業実績等の管理
本サーバー式の運用及び保守中に取りまとめた作業実績、リスク、課題及び障害事由

⑫ スケジュールや工数等の管理
役務を伴う調達案件については、PJMOの求めに応じ、スケジュールや工数等の計画値及び実績値

4.5.納入物等の範囲、納入期日等

4.5.1.納入物

受注者は、以下に示す納入物を納入期日までに納入すること。

表 4.5-1 納入物一覧

No.	納入物	納入数量	納入期日
1	本サーバー式	一式	令和 10 年 5 月 7 日

納入物のうち本調達の機器を以下に示す。詳細は「別紙 1 要件定義書」を参照すること。

表 4.5-2 調達機器の機器数（本番機）

No.	機器の区分	機器の名称	機器数
1	サーバ装置	仮想基盤サーバ	13 台
2		蓄積・バックアップサーバ	2 台
3		プロキシサーバ	2 台
4	ディスクアレイ装置	ディスクアレイ装置	2 台
5	バックアップ装置	LTO ライブラリ装置	2 台
6	ネットワーク装置	負荷分散装置	4 台
7		FC スイッチ	4 台
8		L2 スイッチ	2 台
9	コンソール装置	コンソール装置（KVM スイッチ含む。）	4 台
10	クライアント装置	特殊用途端末	5 台
11		商標検索ジョブ実行端末	1 台

表 4.5-3 調達機器の機器数（総合試験／開発機）

No.	機器の区分	機器の名称	機器数
1	サーバ装置	総合試験／開発用 仮想基盤サーバ	2 台
2		総合試験／開発用 蓄積・バックアップサーバ	1 台
3		総合試験／開発用 プロキシサーバ	1 台
4	ディスクアレイ装置	総合試験／開発用 ディスクアレイ装置	1 台
5	バックアップ装置	総合試験／開発用 LTO ライブラリ装置	1 台
6	ネットワーク装置	総合試験／開発用 負荷分散装置	4 台
7		総合試験／開発用 FC スイッチ	2 台
8		総合試験／開発用 L2 スイッチ	2 台
9	コンソール装置	総合試験／開発用 コンソール装置（KVM スイッチ含む。）	2 台
10	クライアント装置	総合試験／開発用 特殊用途端末	3 台
11		総合試験／開発用 商標検索ジョブ実行端末	1 台

4.5.2.提出物

(1) 提出物は、原則として日本語で作成すること。

(2) 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（建議）（令和 4 年 1 月 7 日文化審議会）を参考にすること。

(3) 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。

(4) 提出物は、特許庁から特別に示す場合を除き、原則以下に示す媒体・数量で提出すること。

表 4.5-4 提出物一覧

No.	提出物名	提出数量	提出期日
1	環境設定定義書（総合試験／開発環境）	電磁的記録媒体で 正 1 部・副 2 部	オンラインサービス開始前日 （令和 10 年 5 月 7 日）
2	環境設定定義書（本番環境）		
3	運用マニュアル	電磁的記録媒体で 正 1 部・副 2 部	オンラインサービス開始 2 週間前 （令和 10 年 4 月 24 日）

(5) 電磁的記録媒体による提出について、原則として Microsoft Word（Microsoft 365 E5）、Microsoft Excel（Microsoft 365 E5）により閲覧・編集可能なファイル形式で作成し、DVD-R の媒体に格納して提出すること。
(6) 提出後特許庁において改変可能な図表等の元データも併せて提出すること。
(7) 提出物の作成にあたって、特別なツールを使用する場合は、特許庁の了承を得ること。
(8) 提出物が外部に不正に使用されたり、提出過程において改ざんされたりすることのないよう、安全な提出方法を提案し、提出物の情報セキュリティの確保に留意すること。
(9) 電磁的記録媒体により提出する場合は、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、提出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。
(10) その他、「ハードウェア導入ガイドライン」に記載の提出物を作成し、提出すること。

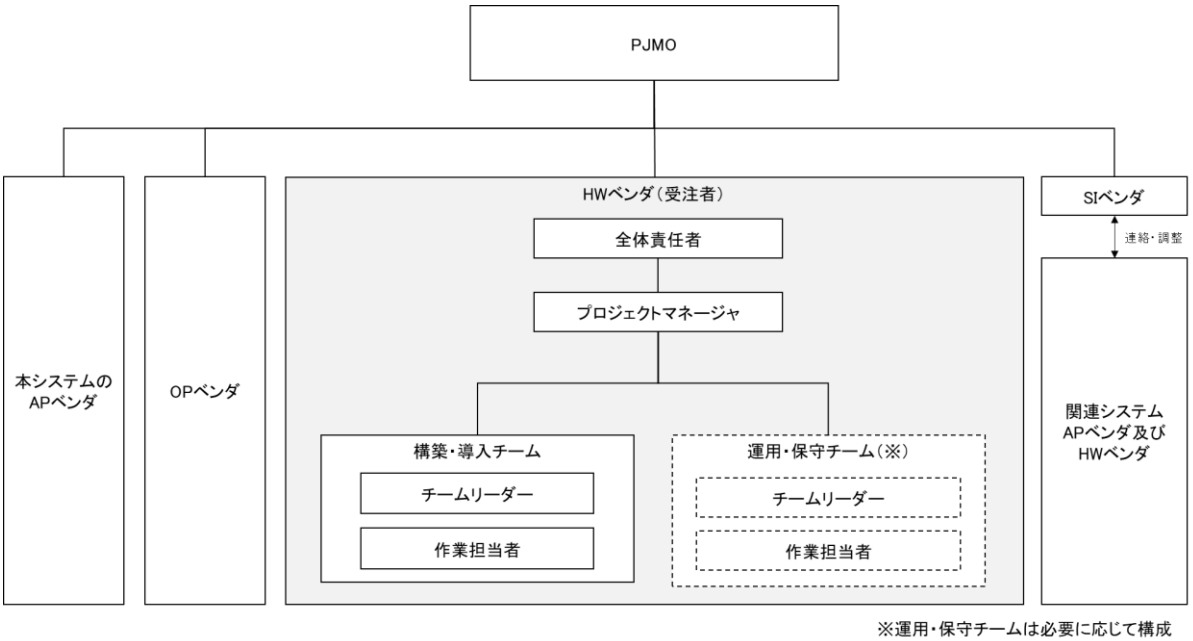
4.5.3.納入・提出場所

(1) 納入・提出場所は、特許庁庁舎（東京都千代田区霞が関三丁目 4 番 3 号）とする。
(2) 特許庁の指示により納入された機器の設置場所を変更する場合においても対応すること。ただし、この場合の追加費用については、特許庁と別途協議のうえで決定することとする。

5. 作業の実施体制・方法に関する事項

5.1.作業実施体制

(1) プロジェクトの実施に当たり、特許庁が想定する作業実施体制を図 5.1-1 に示す。構築・導入フェーズにおいてはプロジェクトマネージャ及びチームリーダーを定めたうえで構築・導入チームを構成し、各種作業を実施すること。運用・保守フェーズにおいては「表 5.1 1　要員に係る要件」No.4 の【運用・保守チームに係る要件】に基づき受注者で必要と考える体制を構成すること。また、受注者はプロジェクトの成功（「1.3 目的及び期待する効果」に記載された内容の実現）に責任を持つ者を全体責任者として 1 名定め、体制に含めること。なお、各フェーズにおける作業内容については、「4.1.構築・導入に係る作業」及び「4.2.運用・保守に係る作業」を参照すること。



※運用・保守チームは必要に応じて構成

図 5.1-1 作業実施体制図(想定)

(2) 作業実施体制について、特許庁が求める役割及び要件を以下に示す。なお、人材の効率的な配置の観点から、各役割・要件を満たす前提でプロジェクトマネージャと各チームリーダーの兼任は許容する。

表 5.1-1 要員に係る要件

No.	役職・チーム	役割	要件
1	全体責任者	・プロジェクトに対する成功責任 ・不測発生時の特許庁への説明(説明責任)	・プロジェクトの遂行に不測の事態が発生した場合において、特許庁に対して説明責任を持つこと。 ・必要に応じて各種リソース(追加要員やコスト等)をプロジェクトへ投入する等、プロジェクトを確実に推進させるために必要な事項を自らの判断で実行できること。
2	プロジェクトマネージャ	・プロジェクト推進・プロジェクト管理(品質管理、リスク管理等) ・作業チーム全体の統括 ・平常時における特許庁への進捗・課題・リスクの説明(説明責任) ・障害発生時におけるオンサイトでの迅速かつ的確な状況コントロール	【プロジェクトマネージャの業務面に係る要件】 ・プロジェクト全体のマネジメント(進捗管理、品質管理、課題・リスク管理等)を担い、プロジェクトの実行責任を持つこと。 ・作業チーム全体を統括し、チーム間の認識齟齬の防止・統一された品質担保等に責任を持つこと。 ・特許庁への説明責任を持つこと。 【プロジェクトマネージャが保有する経験及び資格に係る要件】 ・以下に示す条件を満たすプロジェクトにおいて、上記【プロジェクトマネージャの業務面に係る要件】に示す本業務のプロジェクトマネージャの役割と同等の役割としての業務経験を 1 件以上又はプロジェクトマネージャの補佐として本業務のプロジェクトマネージャに求める役割の一部を担った業務経験を 2 件以上有すること。 ➢ 本サーバー式と同等規模以上のサーバー式に対する類似業務の経験(ハードウェアの構築・導入及び運用・保守業務) ・以下のいずれかの資格または IT スキルを有する者であること。 [資格] ➢ プロジェクトマネージャ(IPA) ➢ PMP(Project Management Professional)(PMI) [IT スキル標準] ➢ プロジェクトマネジメント(レベル 4 以上)
3	構築・導入チーム	・構築・導入作業の	【構築・導入チームに係る要件】

No.	役職・チーム	役割	要件
	※チーム構成は応札者の提案に委ねる	円滑な実施	・構築・導入フェーズにおいて、本プロジェクトを円滑かつ確実に遂行するために必要なチームを組成すること。 ・チーム内のタスクを管理・推進する担当者（チームリーダー）を配置すること。複数チームを構成する場合は、原則各チームに最低 1 名のチームリーダーを配置すること。 【チームリーダーに係る要件】 ・特許庁の求めに応じて担当チームのタスクの状況等について説明ができる者であること。 ・以下に示す条件を満たすプロジェクトにおいて、上記【構築・導入チームに係る要件】を満たすチームにて構築・導入フェーズの業務を担当するチームリーダーと同等の役割としての業務経験を 1 件以上又はチームリーダーの補佐として本業務のチームリーダーに求める役割の一部を担った業務経験を 2 件以上有すること。 ➢ 本サーバー式と同等規模以上のサーバー式に対する類似業務の経験（ハードウェアの構築・導入業務） ・以下のいずれかの資格等を有する者であること。 [IT スキル標準] ➢ IT アーキテクト（レベル 4 以上） ➢ IT スペシャリスト（レベル 4 以上）
4	運用・保守チーム ※チーム構成は応札者の提案に委ねる	・運用・保守作業全体の管理 ・運用・保守作業の円滑な推進	【運用・保守チームに係る要件】 ・運用・保守フェーズにおいて、本プロジェクトを円滑かつ確実に遂行するために必要なチームを組成すること。 ・運用・保守フェーズにおいて、本システムの可用性を高く保ち、障害発生時には迅速な復旧が可能となるよう、機動的な対応ができること。

5.2.作業場所

(1) 本業務の作業場所、並びに作業に当たり必要とする設備・備品及び消耗品等については、受注者の責任において用意すること。なお、必要に応じて特許庁が現地確認を実施することができるものとする。

(2) 機器の設置や試験等、特許庁庁舎内での作業場所を確保する必要がある場合には、作業場所について特許庁の指示に従うこと。

5.3.作業の管理に関する要領

(1) 受注者は、「標準ガイドライン」に記載された事項を遵守し、「デジタル・ガバメント推進標準ガイドライン解説書」に記載された事項を参照すること。また、これらの文書が契約期間中において、改定された場合は、原

則として改定された文書に従うこととするが、より良い作業手法等の提案がある場合には、特許庁と協議のうえ、実施すること。

(2) 受注者は、契約締結後速やかに、ハードウェア導入計画を策定のうえ、「ハードウェア導入計画書」を作成すること。なお、「ハードウェア導入計画書」の作成にあたっては、「ハードウェア導入ガイドライン」及び以下の要件を踏まえること。

① プロジェクト管理における進捗管理方法、課題管理方法の他、作業体制、作業内容、作業スケジュール等を含めること。

② 作業体制には、受注者の作業実施体制における各要員の氏名、所属、担当する作業、指揮命令系統及び情報セキュリティ対策に係る管理体制（連絡体制及び連絡先を含む。）を記載すること。

③ 提案事項（作業の実施方法、実現方式等）について「ハードウェア導入計画書」にすべて反映し、特許庁から了承を得ること。

④ 作業スケジュールについては、「別紙 1 要件定義書」に示す、契約締結後に想定する作業項目、担当及び成果物の概要を踏まえること。また、作業スケジュールに記載するタスクについては、進捗遅延の兆候をより早期に検出し適宜適切なリカバリ策を講じることが可能な単位で管理することとし、作業スケジュールの粒度については、応札時に提出した「様式 3-2_概要スケジュール」より詳細なレベル 3 以上にタスク分解したものとすること。

⑤ 本業務にて発生し得るリスクを抽出し、各リスクについて発生確率及び影響度の分析を行ったうえで、リスクを顕在化させないための予防策及び顕在化した際の対策を記載した「リスク管理表」を作成し、特許庁の承認を得ること。また、受注者は、定期的に各リスクの発生確率及び影響度を再評価し、必要に応じてリスク顕在化の防止策及び顕在化した際の対策の見直しを行うこと。

(3) 受注者が作成した「ハードウェア導入計画書」については、必要に応じて SI ベンダの確認を受けたうえで、特許庁の承認を得ること。また、当該計画書を変更した場合も、必要に応じて SI ベンダの確認を受けたうえで、特許庁の承認を得ること。

(4) 受注者は、特許庁の承認を得た「ハードウェア導入計画書」に基づいて、本プロジェクトにおける各工程の管理を適正に実施し、本プロジェクトの実施状況について、特許庁に報告すること。なお、報告にあたっては、以下の要件を踏まえること。

① 進捗状況及び課題状況を取りまとめ、定期的（隔週程度）に報告会を開催し、特許庁へ報告すること。なお、報告会には SI ベンダも出席することに留意すること。

② 実施作業の進捗状況、作業予定及び課題状況を文書によって説明し、その都度 SI ベンダの確認を受けたうえで、特許庁の了承を得ること。なお、重点的に検討する事項がある場合は、検討用資料を作成のうえ、説明すること。

③ 打合せを効率的に実施できるよう、打合せの目的（情報共有、議論、意思決定等）及びゴールを打合せの際に特許庁に報告すること。また、特許庁が打合せ前に資料を確認できるよう、資料を事前送付すること。

④ 打合せについては Web 会議ツール等を用いたオンラインによる開催とする可能性があるため、特許庁の求めに応じて、いずれの場合においても実施できるよう対応すること。

⑤ 打合せの議事録(概要)は、打合せ後速やかに作成のうえ、SI ベンダの確認を受けたうえで特許庁の了承を得ること。また、特許庁又は SI ベンダとの確認事項のやり取りについても、受注者にて文書に記録し、特許庁及び SI ベンダの確認を得るものとする。

⑥ 作業の遅延を判断するポイントにおいて、作業遅延が明らかとなった場合には、別途、リカバリスケジュールを作成するとともに、リカバリ体制を含む具体的な対策について説明し、特許庁の承認を得たうえで、作業を行うこと。

(5) 受注者は、作業手順の事前確認、複数の担当者による作業連携等、効率的かつ円滑な作業体制を確保すること。

(6) 受注者は、特許庁が常時契約履行に関する調査を行える体制を確保すること。
(7) 受注者は、受注者の責に帰する理由により、リカバリスケジュールから、さらなる遅延が生じた場合、特許庁の判断により、契約履行の意思あるいは作業を遂行する能力がないものとみなされ、受注者側の責に帰する理由に基づく契約解除条項の適用がなされることもあることに留意すること。

6. 作業の実施にあたっての遵守事項

6.1.遵守する法令等

6.1.1.法令等の遵守

(1) 本調達に関する工事等においてディーゼル車を使用する場合は、「都民の健康と安全を確保する環境に関する条例」（平成 12 年東京都条例第 215 号）に規定する、ディーゼル車規制に適合する自動車を使用することが望ましい。
(2) 「国等による環境物品等の調達の推進等に関する法律（グリーン購入法）」（令和 3 年 5 月 19 日改正。令和 3 年法律第 36 号）第六条第 1 項の規定に基づき定められた「環境物品等の調達の推進に関する基本方針」（令和 8 年 2 月 3 日変更閣議決定）別記に記載された対象環境物品等については、各項目の【判断の基準】を満たすこと。なお、【配慮事項】については、対応していることが望ましい。
詳細は、環境省 HP に記載されている「環境物品等の調達の推進に関する基本方針」
（https://www.env.go.jp/policy/hozen/green/g-law/net/kihonhoushin.html）を参照のこと。
(3) 「国際エネルギースタープログラム制度要綱」の対象製品に記載された対象機器については、国際エネルギースタープログラム制度の登録製品であることが望ましい。

6.1.2.標準ガイドラインの遵守

本業務の遂行にあたっては、以下の文書に準拠した作業を行うこと。
(1) 「デジタル・ガバメント推進標準ガイドライン」
（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf）
(2) 「デジタル・ガバメント推進標準ガイドライン解説書」
（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/573c839f/20250619_resources_standard_guidelines_guideline_03.pdf）

6.1.3.その他文書、標準への準拠

本業務の遂行にあたっては、以下の文書に準拠した作業を行うこと。
(1) ハードウェア導入ガイドライン
(2) 経済産業省情報システム安全対策基準
（https://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf）
(3) 経済産業省情報セキュリティ管理規程
（https://www.meti.go.jp/information_2/downloadfiles/kanri_kitei.pdf）
(4) 経済産業省情報セキュリティ対策基準
（https://www.meti.go.jp/information_2/downloadfiles/taisaku_kijun.pdf）
(5) 特許庁個人情報保護管理規程
（https://www.jpo.go.jp/news/kokai/kojin-hogo/document/personal_block/tokkyo_003.pdf）
(6) 特許庁情報セキュリティ運用細則

6.2.秘密保持、資料の取扱い

(1) 受注者は、本契約に関して、賃貸借物品及び保守交換部品（ディスクやテープ媒体、不揮発メモリ等）に格納されたデータを本契約以外の目的に使用又は第三者に開示若しくは漏えい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。

(2) 受注者は、賃貸借物品及び保守交換部品に記録されているデータ、並びに移行作業で用いた媒体に記録されているデータ及び障害対策時に取得したログデータ等すべてのデータについて、特許庁と協議のうえ、物理的な破壊を前提とする廃棄等の措置を行い、特許庁へ報告するとともに、当該物品を廃棄したことを証明すること。なお、廃棄したことの証明については、受注者が指定する産業廃棄物処理業者が発行した証明書で代用しても良いこととするが、その場合は、「経済産業省情報セキュリティ管理規程」、「経済産業省情報セキュリティ対策基準」、「特許庁個人情報保護管理規程」及び「特許庁情報セキュリティ運用細則」に基づいた証明であることを事前に特許庁に通知し、承認を受けること。

(3) 特許庁は、読込／書込エラー多発等の故障範囲が制御部に及ばない軽微な故障の場合、データの復元や読取りを完全に不可能にすることの証明を条件に、データ消去ソフトウェアによるデータ消去又は磁気的破壊によるデータ消去を許容する。ただし、この場合には、データ消去が不十分であった等の原因により、特許庁における内部情報の漏えいが起こった際の損害賠償責任等を含めた全責任を受注者が負うものとする。

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) 受注者は、本業務にて作成した資料、プログラム（プログラムソースを含む。）及びツール等の著作物に係るすべての著作権（著作権法第 21 条から第 28 条に定める権利を含む。以下、同じ。）を特許庁に無償で譲渡しなければならない。

(2) 受注者は、当該著作物の著作者に著作者人格権を行使させない措置を講ずること。

(3) 受注者は、本業務の一部を第三者に委任し又は請負わせる場合、下請負人に対して委任又は請負わせた業務の履行により作成した資料、プログラム（プログラムソース含む。）及びツール等の著作物に係るすべての著作権を特許庁に無償で譲渡し、著作者に著作者人格権を行使させない措置を講ずること。

7.2.契約不適合責任

受注者は、貸借期間中の本サーバー式の契約不適合に関して、本調達の範囲で修正・対処を行い、関係するドキュメントを修正して提出すること。

8. 入札参加資格に関する事項

8.1.入札参加要件

8.1.1.競争参加資格

(1) 予算決算及び会計令第 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) 入札時において令和 7・8・9 年度全省庁統一資格の「役務の提供等」の「A」、「B」、「C」又は「D」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。

(4) 経済産業省からの補助金交付等停止措置又は指名停止措置が講じられている者ではないこと。

(5) 過去 3 年以内に情報管理の不備を理由に経済産業省から契約を解除されている者ではないこと。

8.1.2.公的な資格や認証等の取得

(1) 受注者のうち本調達を担当する部署又は事業所は、ISO9001 の認証又は CMMI レベル 3 相当以上の組織的な品質管理体制を持つこと。

(2) 受注者は、JIS Q 27001 又は ISO/IEC 27001 に基づく認証を取得していること。なお、事業部単位で認証を受けている場合は、当該事業部が本業務の実施体制に参画すること。

8.1.3.受注実績

応札者は、同等規模以上のシステムを設計（パラメータ設計）、構築、運用した実績を有すること。

8.2.入札制限

次の事業者（再委託先等を含む。）及びこの事業者の「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、子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者は、入札には参加できない。

(1) 本案件の調達仕様書の作成に直接関与した事業者

(2) 特許庁の情報システムに関わるプロジェクト管理支援事業者

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

本仕様書に基づく作業にあたっては、作業の全部又は大部分を一括して第三者に委任又は請負わせてはならない。ただし、書面により特許庁の了承を得た場合は、この限りではない。

10. その他特記事項

10.1.稼動責任

(1) 受注者は、本サーバー式における障害発生時に責任を持って原因究明（ただし、ハードウェア故障時の原因究明を除く）を行い、サービスを継続させること。

(2) 受注者は、受注者の責により次期システムの本番稼動の開始が遅延した場合、損害賠償責任を負う。

(3) 特許庁は、受注者の責により次期システムの本番稼動の開始が遅延した場合、賃貸借及び保守にかかる契約金額のうち、遅延した期間分の金額を支払わない。

(4) 特許庁は、受注者の納入物における障害により、提供されるサービスが表 10.1-1 に示す時間を超えて計画外で停止した場合、原則として、計画外で停止していた時間分の賃貸借料を支払わない。

表 10.1-1 次期システムの計画外サービス停止許容時間

No.	対象サービス	計画サービス時間※1	サービス停止許容時間※2
1	共通特実検索システム（検索部分）（庁内）	開庁日：8:00～20:00	月間 180 分以内
2	共通特実検索システム（検索部分）（庁外）	24 時間 365 日	月間 180 分以内
3	商標検索システム	開庁日：8:00～20:00	月間 180 分以内
4	審判業務システム	開庁日：8:00～20:00	月間 180 分以内

※1 システムのメンテナンス時間等、業務上必要なサービス停止時間は計画サービス時間から除く。

※2「月間」は各月の月初から月末までとする。

(5) 例として、サポート時間が平日 9:00 から 17:00 であるソフトウェア A において、計画外の停止時間の対象外とする時間帯について以下に示す。

表 10.1-2 ソフトウェア A における計画外の停止時間の対象外となる時間帯（例）

No.	対象時間	8:00	9:00	～	17:00	～	20:00
1	保守時間（開庁日 8:00 から 20:00）						
2	ソフトウェア A のサポート時間						
3	計画外の停止時間の対象外となる時間帯		障害発生		復旧		

10.2. 導入・調達条件

(1) 本調達の機器等は中古品であってはならない。

(2) 本調達に係る費用を一括して賃貸借契約に含めること。原則として搬入据付調整費用、運用支援・故障対策・保守費用、導入時の特許庁への技術支援費用及び教育サポート費用についても含めるが、前提条件の変更が生じた場合等、詳細は協議のうえ、決定するものとする。

(3) 機器の調整、OS・ソフトウェア製品等の設定及びバックアップ取得については、必要最低限の機器のみに電源を入れるようにして作業をするよう配慮すること。なお、製品出荷時までに予め行ったうえで特許庁に搬入・据付を行ってもよい。

(4) 本調達の機器等を構成するハードウェア及びソフトウェアは、入札時点において、同一機種で過去に出荷実績・稼動実績及び十分に高い信頼性を有する標準的な既製品で最新のものであること。「標準的な既製品」とはメーカが一般市場において販売するために、主要な製品系列の一環として製造する物品で、稼動実績を有するものをいう。なお、提案時においていまだ製品化されていない機器等を含める場合には、次の条件を厳守すること。

① いまだ製品化されていない部分の存在及びその範囲を明確にすること。

② 前項①に関して要件を満たす製品を納入時までに出荷する旨の意志表明を行うとともに、提供可能である根拠を十分に説明できる資料を提出すること。

③ 契約期間中に要件を満たせない等の不具合が発見された場合は、受注者の責任と負担において対処すること。

(5) 導入時点までに製造が中止され、提案機器等が調達できない場合は、当初提案した機器等と同等以上の機器等に交換すること。

(6) 本契約を変更し、本調達の機器等と同一（又は同等以上）の機器等を受注者から調達する場合は、原則として、該当機器等の価格を基に本調達の機器等全体の割引率（機器等それぞれの割引率表が提出された場合には、機器等それぞれの割引率）を適用した価格と市場の実勢価格とを比較して、いずれか低い方の価格を基準に契約を行うこととする。

(7) 将来、本システムを拡張する場合において必要な機器等を調達する際は、当該拡張機器等の価格が本調達の機器等の価格と比較して妥当なものであること。

(8) ハードウェアの保守部品は、2 年間の延長期間満了まで提供が可能であること。また、ハードウェア及びソフトウェアは、同期間の保守（原則としてメーカサポートを含む。）が可能であること。

(9) 本調達の機器等を令和 13 年 1 月 1 日以降も利用することとなった場合、ハードウェア借料及びソフトウェア借料の月額は当初契約における当該借料の総額を 48 で除した額の 10 分の 1 に相当する金額を超えな

いこと。また、ハードウェア保守費用及びソフトウェア保守費用の月額は当初契約における金額を原則超えないこと。ただし、保守条件の変更など、やむを得ない事情がある場合は、保守条件及び費用について特許庁と別途協議のうえ、決定するものとする。

(10) 本調達の機器等を令和 15 年 1 月 1 日以降も利用する場合のハードウェア借料及びソフトウェア借料並びに保守条件及び費用については、特許庁と別途協議のうえ、決定するものとする。

(11) 受注者は、標準ガイドラインの「別紙 2 情報システムの経費区分」に基づく区分等ごとに割引率を記載した資料を契約締結後速やかに提出すること。

10.3. 調達仕様書の記載について

(1) 本仕様書内の「～できること」や「～可能なこと」、「～すること」や「～行うこと」等の記載に関して、費用について特許庁と協議することが明示的に記載されている場合を除き、本調達の範囲内とし、新たな費用負担なく各機能及び要件を実現すること。

(2) 本仕様書内に記載の製品名及び会社名などの固有名詞は、各社の商標又は登録商標である。

(3) 本仕様書に記載のない事項であっても、本システムの構築・稼動・運用に必要と認められる事項については、特許庁と協議のうえ、実施すること。

(4) 本仕様書に記載した要件と「準拠すること」や「従うこと」等としている各種資料において齟齬が生じた場合、特許庁に報告し、協議のうえで優先すべき要件を決定すること。

10.4. 情報管理体制

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

（確保すべき履行体制）

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

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

(3) (1)の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め特許庁へ届出を行い、同意を得なければならない。

10.5. 業務従事者名簿

業務従事者の氏名、所属、役職及び業務経験がわかる資料を提出すること。

10.6. 中小企業者に関する国等の措置について

「中小企業者に関する国等の契約の基本方針について」において、最低賃金額の改定に伴う契約金額の見直し及び労務費、材料費、エネルギーコスト等の上昇への対応について定められていることを踏まえ、以下の措置を実施する。

(1) 受注者においては、契約金額に労務費、原材料費、エネルギーコスト等（以下「労務費等」という。）の改定、増加をあらかじめ反映する。

(2) 特許庁においては、複数年度にわたる契約について、労務費等の上昇に よる契約金額の見直しが必要か

どうか、契約期間中に定期的（年１回程度）に確認する。

(3) 単年度の契約については、契約締結後の状況変更により契約金額の見直しが必要となった場合には、協議を行い、見直しを行うこととする。

中小企業者に関する国等の契約の基本方針について
https://www.chusho.meti.go.jp/keiei/torihiki/kankoju.html#K01

10.7. 情報セキュリティについて

「別記 情報セキュリティに関する事項」を遵守し、情報セキュリティ対策を実施すること。

10.8. 課室情報セキュリティ責任者及び情報システムセキュリティ責任者

特許庁総務部総務課情報技術統括室
情報技術統括室長　上尾 敬彦

10.9. 特許庁担当者

特許庁総務部総務課情報技術統括室
システム計画班長　北原　昂
システム計画班　　佐藤　賢斗
デジタル戦略調達班長　加藤　優一
デジタル戦略調達係長　吾妻　駿一
（人事異動等により担当者が変更となった場合は、新たに担当者となった者とする。）

10.10. 資料の閲覧について

本調達においては、「11.4.事業者が閲覧できる資料一覧表」のとおり、閲覧資料を用意している。応札者は、「11.5.閲覧要領」に従い、応札前に必ず資料内容を確認すること。

11. 附属文書

11.1. 要件定義書

本調達の機器等の具体的な要件が記載されている「別紙 1 要件定義書」は、機密保持誓約書の提出後に応札者に提示する。機密保持誓約書の提出については「11.5.閲覧要領」を参照すること。

11.2. 本調達仕様書を作成するに当たり参考とした資料一覧

本調達仕様書を作成するに当たり参考とした資料を以下に示す。

表 11.2-1 本調達仕様書を作成するに当たり参考とした資料一覧

No.	資料名	資料の概要及び位置付け
1	デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf
2	経済産業省情報システム安全対策基準	https://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf
3	経済産業省情報セキュリティ管理規程	https://www.meti.go.jp/information_2/downloadfiles/kanri_kitei.pdf
4	経済産業省情報セキュリティ対策基準	https://www.meti.go.jp/information_2/downloadfiles/taisaku_kijun.

No.	資料名	資料の概要及び位置付け
		pdf
5	特許庁個人情報保護管理規程	https://www.jpo.go.jp/news/kokai/kojin-hogo/document/personal_block/tokkyo_003.pdf
6	特許庁行政文書管理規則	https://www.jpo.go.jp/news/kokai/jpo-jouhou/document/index/gyousei_kanri_kisoku.pdf
7	行政機関の保有する個人情報の保護に関する法律	https://elaws.e-gov.go.jp/document?lawid=415AC0000000058_20220401_503AC0000000037
8	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	https://www.cyber.go.jp/pdf/policy/general/kijyunr7.pdf
9	過去の調達仕様書等	特許庁が過去に作成した以下の案件に係る調達仕様書及び応札資料作成要領等である。本業務の調達仕様書の作成に当たり参考とした。 「共通特実検索(検索部分)サーバー式の新規導入に係るハードウェア等賃貸借及び保守等業務 一式調達仕様書」 「商標検索サーバー式の更改に係るソフトウェア等賃貸借及び保守等業務 一式調達仕様書」 「審判システムに係る構築及び賃貸借・保守等 一式 調達仕様書」
10	設備条件整理結果報告書	本サーバー式の更改に向けて、UAP の稼動を保証するための設備条件が整理されている報告書である。本業務の調達仕様書の作成に当たり参考とした。 「共通特実検索（検索部分）・商標検索・審判業務サーバ更改対応設備条件整理結果報告書」

11.3.応札参考資料

応札に当たり参考となる資料（以下、「応札参考資料」という。）を以下に示す。応札参考資料については、「11.1.要件定義書」と同様に、機密保持誓約書の提出後に応札者に提示する。

表 11.3-1 応札参考資料一覧

No.	資料名
1	ハードウェア導入ガイドライン
2	特許庁情報セキュリティ運用細則
3	情報の格付及び取扱制限の基準並びに格付及び取扱制限を明示する手順
4	改造・運用ガイドライン
5	特許庁システムインテグレーションサービス サービス仕様書
6	特許庁オペレーションサービス サービス仕様書
7	設備条件整理結果報告書

11.4.事業者が閲覧できる資料一覧表

事業者が特許庁庁舎にて閲覧できる資料（以下、「庁内資料」という。）を以下に示す。庁内資料の閲覧については、「11.5.閲覧要領」を参照すること。

表 11.4-1 庁内資料一覧

No.	資料名
1	バックアップ設計指針
2	パッチ適用方針

No.	資料名
3	ポリシー実施手順（運用編）
4	ポリシー実施手順（開発編）
5	ポリシー実施手順（開発編別紙「設計基準」）
6	特許庁ネットワーク設計基準
7	運用マニュアル引継ガイドライン
8	障害報告ガイドライン
9	環境設定定義書
10	運用マニュアル

11.5. 閲覧要領

庁内資料の閲覧、要件定義書及び応札参考資料の送付を希望する者は、以下の手続に沿うこと。

(1) 機密保持誓約書の様式を入手する

① 意見招請時は、特許庁ウェブサイトから入手する。

② 入札公告時は、調達ポータル・政府電子調達システム（GEPS）から入手する。

(2) 記名済みの機密保持誓約書（PDF ファイル）をメールにて次のとおり送付するか、特許庁担当者まで手渡し又は郵送する。

【件名】

共通特実検索（検索部分）・商標検索・審判業務サーバー式の更改に係る要件定義書等の送付希望（/庁内資料閲覧の希望）

【メール宛先】

総務部　総務課　情報技術統括室　デジタル戦略調達班 PA0G13@jpo.go.jp

【本文記載事項】

① 企業又は団体名

② 担当者名

③ 連絡先（日中連絡可能な電話番号及びメールアドレス）

④ 庁内資料の閲覧希望日時（希望する場合のみ。できる限り複数候補を提示すること）

【手渡先、郵送先】

〒100-8915　東京都千代田区霞が関 3 丁目 4 番 3 号

特許庁総務部総務課　情報技術統括室　デジタル戦略調達班　宛て

(3) 特許庁担当者より、メール又は大容量ファイル交換サービスにて要件定義書及び応札参考資料の送付を受ける。

(4) 庁内資料の閲覧日時については、特許庁担当者から、具体的な来庁日時等について連絡を受ける（庁内資料閲覧に関しては、原則、閲覧希望日の 2 開庁日前までに連絡すること。）。

(5) 連絡を受けた来庁日時に来庁し、庁内資料を閲覧する。

R8-U-1
（別記）

情報セキュリティに関する事項

以下の事項について遵守すること。

【情報セキュリティ関連事項の確保体制及び遵守状況の報告】

1）受注者（委託契約の場合には、受託者。以下同じ。）は、契約締結後速やかに、情報セキュリティを確保するための体制並びに以下 2)～17)に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、特許庁（以下「当庁」という。）の担当職員（以下「担当職員」という。）に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について担当職員に提示し了承を得た上で提出したときは、この限りでない。また、定期的に、情報セキュリティを確保するための体制等及び対策に係る実施状況（「情報セキュリティに関する事項の遵守の方法の実施状況報告書」（別紙 2））を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に担当職員へ案を提出し、同意を得ること。

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

【情報セキュリティ関連規程等の遵守】

2） 受注者は、「経済産業省情報セキュリティ管理規程（平成 18･03･22 シ第 1 号)」、「経済産業省情報セキュリティ対策基準（平成 18･03･24 シ第 1 号)」及び「政府機関等のサイバーセキュリティ対策のための統一基準群（令和７年度版)」（以下「規程等」と総称する。）を遵守すること。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

3）受注者は、当庁又は内閣官房国家サイバー統括室が必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行うこと。

【情報セキュリティを確保するための体制】

4）受注者は、本業務に従事する者を限定すること。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等)、実績及び国籍に関する情報を担当職員に提示すること。なお､本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示すること。

5）受注者は、本業務を再委託（業務の一部を第三者に委託することをいい、外注及び請負を含む。以下同じ。）する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記 1)から 17)までの措置の実施を契約等により再委託先に担保させること。また、1)の確認書類には再委託先に係るものも含むこと。

【情報の取扱い】

6） 受注者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、当庁内に複製が可能な電子計算機等の機器を持ち込んで作業を行う

必要がある場合には、事前に担当職員の許可を得ること。なお、この場合であっても、担当職員の許可なく複製してはならない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明すること。

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

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

9）受注者は、契約期間中及び契約終了後においても、本業務に関して知り得た当庁の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。

なお、当庁の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供すること。

【情報セキュリティに係る対策、教育、侵害時の対処】

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

11） 受注者は、本業務の遂行において、情報セキュリティが侵害され、又はそのおそれがある場合の対処方法について担当職員に提示すること。また、情報セキュリティが侵害され、又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。

【クラウドサービス】

12） 受注者は、本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、2)に掲げる規程等で定める不正アクセス対策を実施するなど規程等を遵守すること。

13）受注者は、本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストから調達することを原則とすること。

14）受注者は、前２項におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容出来ることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。

【セキュアな情報システム（外部公開ウェブサイトを含む）の構築・運用・閉鎖】

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

①各工程において、当庁の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。

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

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

(a) 不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。

(b) 不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。

(c) 不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

(d) 不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

(e) EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。

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

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

⑥受注者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。

⑦ウェブサイト又は電子メール送受信機能を含むシステム等の当庁外向けシステムを構築又は運用する

場合には、政府機関のドメインであることが保証されるドメイン名「.go.jp」を使用すること。

⑧外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。

・サービス開始前及び、運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。

・インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。

なお、必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。

⑨電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）によるなりすましの防止策を講ずるとともにSMTPによるサーバ間通信のTLS（SSL）化やS/MIME等の電子メールにおける暗号化及び電子署名等により保護すること。

⑩ウェブサイト又は電子メール送受信機能を含むシステム等の当庁外向けシステムを構築又は運用する場合は、ドメインに関する情報が正確であることの定期的な確認、当庁が指定する期日にドメインの抹消、DNSやCDN情報の削除、運用環境の削除を行える事業者を選定すること。

また、運用を閉鎖する場合は、終了告知を一定期間行うこと。一定期間の終了告知を終えた後は、ドメインの抹消、DNSやCDN情報の削除、ドメインへのリンクの削除、SNSを利用していた場合はアカウント削除等、なりすましの防止策を漏れなく講ずること。

なお、本事項は、「実施」の場合はその実施内容、「未実施」又は「該当なし」の場合はその理由等を必ず報告すること。

【アプリケーション・コンテンツの情報セキュリティ対策】

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

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

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

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

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

②提供するアプリケーション・コンテンツが脆弱性を含まないこと。

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

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

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

⑥当庁外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をアプリケーション・コンテンツに組み込む場合は、当庁外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該アプリケーション・コンテンツに掲載すること。

17）受注者は、外部に公開するウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に基づくこと。また、ウェブアプリケーションの構築又は更改時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施すること。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出すること。なお、チェックリストの結果に基づき、担当職員から指示があった場合は、それに従うこと。

R8-U-1
別紙２

令和　　年　　月　　日

特許庁総務部総務課情報技術統括室長　殿

住　　所
名　　称
代 表 者 氏 名

情報セキュリティに関する事項の遵守の方法の実施状況報告書

情報セキュリティに関する事項１）の規定に基づき、下記のとおり報告します。

記

１．契約件名等

契約締結日	
契約件名	

２．報告事項

項目	確認事項	実施状況
情報セキュリティに関する事項２）	本業務全体における情報セキュリティの確保のため、「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年度版）、「経済産業省情報セキュリティ管理規程」（平成１８・０３・２２シ第１号）及び「経済産業省情報セキュリティ対策基準」（平成１８･０３･２４シ第１号）（以下「規程等」と総称する。）に基づく、情報セキュリティ対策を講じる。	
情報セキュリティに関する事項３）	特許庁又は内閣官房国家サイバー統括室が必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行う。	
情報セキュリティに関する事項４）	本業務に従事する者を限定する。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報を担当職員に提示する。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示する。	
情報セキュリティに関する事項５）	本業務の一部を再委託する場合には、再委託することにより生ずる脅威に対して情報セキュリティに関する事項１）から１７）までの規定に基づく情報セキュリティ対策が十分に確保される措置を講じる。	
情報セキュリティに関する事項６）	本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、特許庁内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に特許庁の担当職員（以下「担当職員」という。）の許可を得る。 なお、この場合であっても、担当職員の許可なく複製しない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明する。	
情報セキュリティに関する事項７）	本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく特許庁外で複製しない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明する。	
情報セキュリティに関する事項	本業務を終了又は契約解除する場合には、受注者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当	

8）	職員に返却し、又は廃棄し、若しくは消去する。その際、担当職員の確認を必ず受ける。	
情報セキュリティに関する事項9）	契約期間中及び契約終了後においても、本業務に関して知り得た特許庁の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。 なお、特許庁の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供する。	
情報セキュリティに関する事項１０）	本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施する。	
情報セキュリティに関する事項１１）	本業務の遂行において、情報セキュリティが侵害され又はそのおそれがある場合の対処方法について担当職員に提示する。また、情報セキュリティが侵害され又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従う。	
情報セキュリティに関する事項１２）	本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、「情報セキュリティに関する事項2)」に定める不正アクセス対策を実施するなど規程等を遵守する。	
情報セキュリティに関する事項１３）	本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ISMAP)」の ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストから調達することを原則とすること。	
情報セキュリティに関する事項１４）	情報セキュリティに関する事項１２）及び１３）におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容出来ることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。	
情報セキュリティに関する事項１５）	情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施する。 （1）各工程において、当庁の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。 （2）情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当庁と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。 （3）不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。また、以下を含む対策を行うこと。 ①不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。 ②不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。 ③不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。 ④不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。 ⑤EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。 （4）情報セキュリティ対策による情報システムの変更内容について、担当職員に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。 （5）サポート期限が切れた又は本業務の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わないこと、及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。	

	（６）受注者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。 （７）ウェブサイト又は電子メール送受信機能を含むシステム等の当庁外向けシステムを構築又は運用する場合には、政府機関のドメインであることが保証されるドメイン名「.go.jp」を使用すること。 （８）外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。 ・サービス開始前及び運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。 ・インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。 ・必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。 （９）電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）によるなりすましの防止策を講ずるとともに SMTP によるサーバ間通信の TLS（SSL）化や S/MIME 等の電子メールにおける暗号化及び電子署名等により保護すること。 （１０）ウェブサイト又は電子メール送受信機能を含むシステム等の当庁外向けシステムを構築又は運用する場合は、ドメインに関する情報が正確であることの定期的な確認、当庁が指定する期日にドメインの抹消、DNS や CDN 情報の削除、運用環境の削除を行える事業者を選定すること。 また、運用を閉鎖する場合は、終了告知を一定期間行うこと。一定期間の終了告知を終えた後は、ドメインの抹消、DNS や CDN 情報の削除、ドメインへのリンクの削除、SNS を利用していた場合はアカウント削除等、なりすましの防止策を漏れなく講ずること。 なお、本事項は、「実施」の場合はその実施内容、「未実施」又は「該当なし」の場合はその理由等を必ず報告すること。	
情報セキュリティに関する事項１６）	アプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行う。 （１）提供するアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。 ①アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。 ②アプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。 ③提供するアプリケーション・コンテンツにおいて、当庁外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させるなどして確認すること。 （２）提供するアプリケーション・コンテンツが脆弱性を含まないこと。 （３）実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。 （４）電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。 （５）提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳ、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。 （６）当庁外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をアプリケーション・コンテンツに組み込む場合は、当庁外へのアクセスが情報セキュリティ上安全なものであることを確認した上	

	で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該アプリケーション・コンテンツに掲載すること。	
情報セキュリティに関する事項１７）	外部公開ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」(以下「作り方」という。）に従う。また、ウェブアプリケーションの構築又は改修時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施する。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出する。 なお、チェックリストの結果に基づき、担当職員から指示があった場合には、その指示に従う。	

記載要領

１.「実施状況」は、情報セキュリティに関する事項２）から１７）までに規定した事項について、情報セキュリティに関する事項１）に基づき提出した確認書類で示された遵守の方法の実施状況をチェックするものであり、「実施」、「未実施」又は「該当なし」のいずれか一つを記載すること。「未実施」又は「該当なし」と記載した項目については、別葉にて理由も報告すること。

２．上記に記載のない項目を追加することは妨げないが、事前に特許庁と相談すること。

（この報告書の提出時期：定期的（契約期間における半期を目処（複数年の契約においては年１回以上））。）