

AI 基盤サーバー式の導入に係る
ハードウェア等賃貸借及び保守等業務 一式
調達仕様書(案)
(令和 8 年 2 月 13 日時点版)

令和8年2月
特許庁



－ 目次 －

1.調達案件の概要に関する事項	1
1.1.調達件名	1
1.2.調達の背景	1
1.3.調達目的及び調達の期待する効果	1
1.4.用語定義	1
1.5.業務・情報システムの概要	2
1.6.契約期間	3
1.7.作業スケジュール	3
2.調達案件及び関連調達案件	4
2.1.調達案件の一覧	4
3.情報システムに求める要件に関する事項	4
4.作業の実施内容に関する事項	4
4.1.構築・導入に係る作業	4
4.2.運用・保守に係る作業	4
4.3.撤去に係る作業	4
4.4.情報資産管理標準シートの提示に係る記載内容	5
4.5.納入物等の範囲、納入期日等	5
5.作業の実施体制・方法に関する事項	7
5.1.作業実施体制	7
5.2.作業場所	9
5.3.作業の管理に関する要領	10
6.作業の実施にあたっての遵守事項	11
6.1.遵守する法令等	11
6.2.秘密保持、資料の取扱い	11
7.成果物の取扱いに関する事項	12
7.1.知的財産権の帰属	12
7.2.契約不適合責任	12
8.入札参加資格に関する事項	12
8.1.入札参加要件	12
8.2.入札制限	13
9.再委託に関する事項	13
9.1.再委託の制限及び再委託を認める場合の条件	13
10.その他特記事項	13
10.1.撤去要件	13
10.2.稼動責任	13
10.3.導入・調達条件	13
10.4.調達仕様書の記載について	14
10.5.機能証明書等について	14
10.6.情報管理体制	14
10.7.業務従事者名簿	14
10.8.履行完了後の情報の取扱い	14
10.9.情報セキュリティについて	15

10.10.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	15
10.11.特許庁担当者	15
10.12.資料の閲覧について	15
11.附属文書	15
11.1.要件定義書	15
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	15
11.3.応札参考資料	16
11.4.事業者が閲覧できる資料一覧表	16
11.5.閲覧要領	16
11.6.提案書等の審査要領	17

別記 情報セキュリティに関する事項

別紙 1 要件定義書

別紙 2 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

1. 調達案件の概要に関する事項

1.1. 調達件名

「AI 基盤サーバー式の導入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

特許庁では、特許庁における人工知能(AI)技術の活用に向けたアクション・プランを公表し、業務への AI 技術の活用可能性について検討を行っている。当該アクション・プランにおける令和 8 年度までの成果を踏まえ、令和 9 年度からは開発・運用を本格的に実施予定である。

本格実施に当たり、これまでに技術実証やプロトタイプ開発を行った AI 活用システムにおいて機密性の高い申請書類等をセキュリティ上の懸念なく取り扱うとともに、技術実証時を大幅に上回る大量のデータを高速に処理し、実用的なレベルでの支援を提供するため、インターネットに接続されていない庁内の閉域ネットワークに設置される AI 基盤サーバー式を導入する必要がある。

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 AI 基盤サーバー式（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】 <ul style="list-style-type: none">・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、利用者に対して安定したサービスを提供する。
2	【コストパフォーマンスの高い実装】 <ul style="list-style-type: none">・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コストの低減等により、コスト削減を図る。
3	【更改も見据えた業務の実施】 <ul style="list-style-type: none">・更改を見据えたリソース情報の取得等により、継続的な本サーバー式の改善を実現する。

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	—	本調達によって導入を予定するAI(主に生成AI)モデルを活用した業務支援システム（以下、「AI基盤システム」という。）を指す。
2	AI基盤サーバー式	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。
3	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。
4	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。
5	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。
6	AIモデル	—	AIが特定のタスクを実行するために設計・学習された数学的な構造やプログラムのこと。AIモデルそのもの及びその構築・導入、運用・保守は本調達の範囲外である。
7	作り込み機能	—	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。

No.	用語	用語略称	説明
8	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。
9	アプリケーション開発ベンダ	APベンダ	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。
10	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・改変支援、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。
11	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。
12	特許庁の指定する支援ベンダ	支援ベンダ	本サーバー式に係る運用・保守の一部、及び、AIモデルの構築・導入、運用・保守の支援等のサービスを提供する業者を指す。

■用語が示す範囲

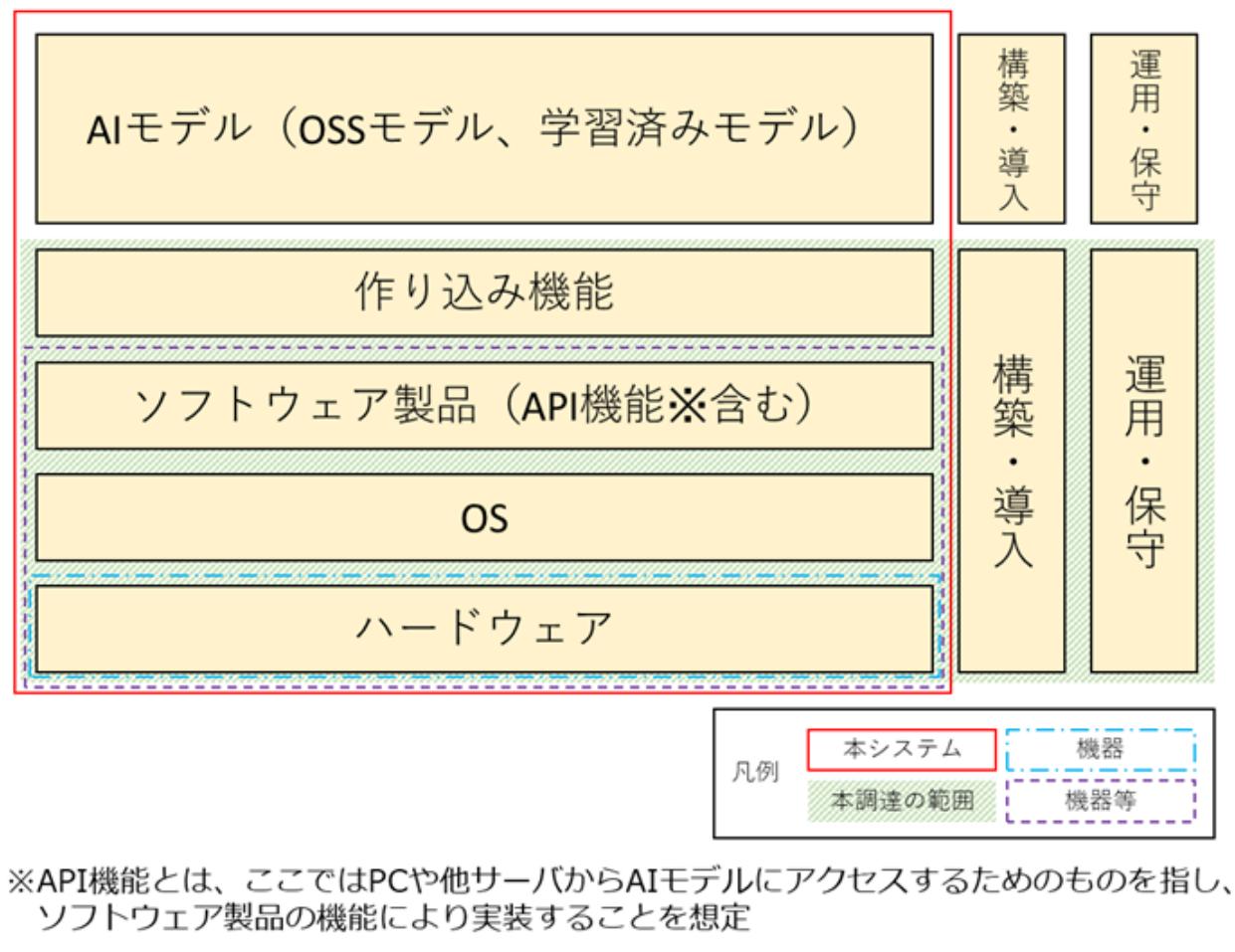


図 1.4-1 用語定義(補足)

1.5. 業務・情報システムの概要

AI 基盤サーバー式が提供する想定である主な機能(想定ユースケース)の概要を以下に示す。なお、これらの想定機能の詳細については必要に応じて情報技術統括室で閲覧(コピー不可)することが可能である。

表 1.5-1 AI 基盤サーバー式が提供する想定である主な機能

No.	機能名	内容
1	申請書類 AI-OCR	紙申請、特殊申請(PDF)の読み取り構造化を行う機能。手書き書類は含まない想定。
2	技術文献図表 AI-OCR	先行技術文献にある表を読み取り、読み取ったデータの単位自動変換まで行う機能。
3	起案文書自動作成	審決や拒絶理由通知等の起案文書を自動生成する機能。
4	起案品質監査	発送前に審査官が作成した起案の品質を監査する機能。
5	DWH-SQL 自動生成	定義テーブルを対象とした RAG などにより自然文から SQL を自動生成する機能。
6	先行技術文献要約	先行技術文献を要約する機能。
7	汎用生成 AI チャット	閉域 NW 内のオンプレミスサーバにおいて生成 AI チャットを実現する機能。
8	設計書 RAG・チャットボット	特許庁システムに関する仕様確認等のため、設計書を対象とした RAG を実現する機能。
9	設計情報のチェック	新規開発案件の要件定義資料等設計情報の品質チェック等を行う機能。
10	システムエラー解析	各システムのエラーログの集積、解析、原因調査、横展開調査を行う機能。
11	類似画像検索	先行技術文献検索、先行商標調査、先行意匠調査の一環として、図面の類似度に基づいた検索・ランキングを行う機能。

上記業務を行うための本サーバー式の概要(イメージ)は、以下のとおり。

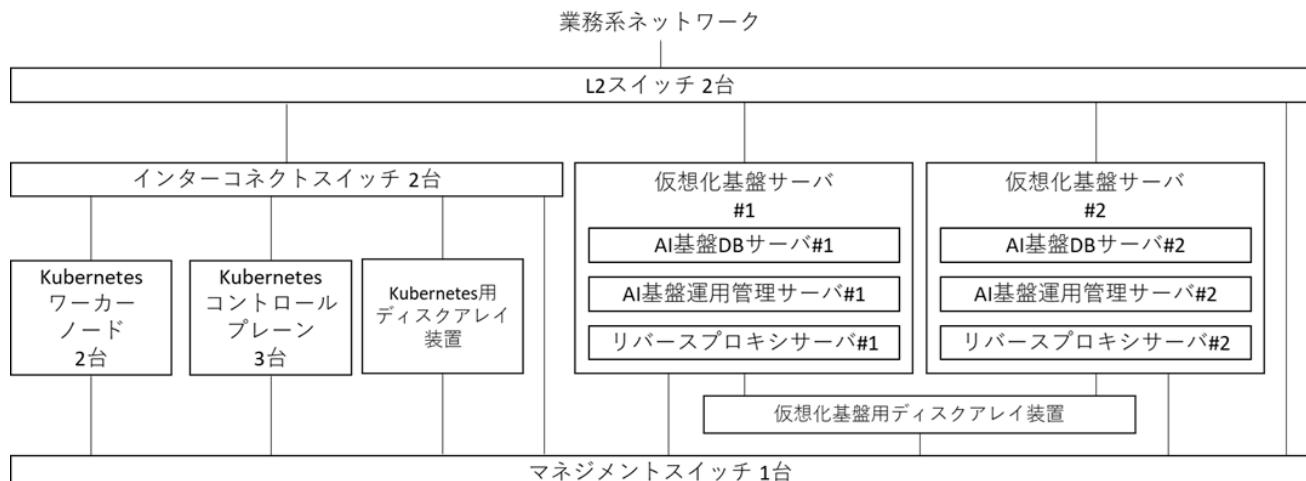


図 1.5-1 本サーバー式の概要図

1.6.契約期間

契約期間は、契約締結日から令和 13 年 3 月 31 日までとする。本サーバー式の賃貸借は、令和 9 年 7 月 1 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。

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 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
1	1本サーバー式の構築・導入																
2	2本サーバー式の賃貸借及び運用・保守																
3	3本サーバー式の撤去																

本調達の範囲

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	AI 基盤サーバー式の導入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 8 年 6 月～ 令和 13 年 3 月	本調達案件
2	特許庁ネットワーク式の更改に係る 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	

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、機器納入について「ハードウェア導入ガイドライン」を参考にしつつ「別紙 1 要件定義書」に準拠して作業を実施し、必要に応じて搬入経路を養生すること。

ただし、ハードウェア導入ガイドライン中の「SI ベンダ」、「OPベンダ」の記載は、適宜「特許庁または支援ベンダ」と読み替えること。(以下の「ハードウェア導入ガイドライン」を引用する記載についても同様。)

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、「別紙 1 要件定義書」によるものとする。

4.3.撤去に係る作業

- (1) 受注者は、本サーバー式の撤去について「ハードウェア導入ガイドライン」を参考にしつつ「別紙 1 要件定義書」に準拠して作業を実施し、必要に応じて搬入経路を養生すること。
- (2) 受注者は、次期サーバー式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。ただし、半導体不足等の影響により真にやむを得ず納入期限までに納入が間に合わない機器については、特許庁担当者に説明し承認を得て、令和9年6月30日までの納入とすることができる。

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9年3月31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	Kubernetes コントロールプレーン	3台
2		Kubernetes ワーカーノード	2台
3		仮想化基盤サーバ	2台
4	ディスクアレイ装置	Kubernetes 用ディスクアレイ装置	1台
5		仮想化基盤用ディスクアレイ装置	1台
6	ネットワーク装置	L2 スイッチ	2台
7		インターフェクトスイッチ	2台
8		マネジメントスイッチ	1台
9	コンソール装置	コンソール装置(KVMスイッチ含む。)	1台
10	サーバラック	サーバラック	2台
11	架設分電盤	架設分電盤 ※本番機および総合試験／開発機で共用	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	Kubernetes コントロールプレーン	3台
2		Kubernetes ワーカーノード	2台
3		仮想化基盤サーバ	1台
4	ディスクアレイ装置	Kubernetes 用ディスクアレイ装置	1台
5		仮想化基盤用ディスクアレイ装置	1台
6	ネットワーク装置	L2 スイッチ	2台
7		インターフェクトスイッチ	2台
8		マネジメントスイッチ	1台
9	コンソール装置	コンソール装置(KVMスイッチ含む。)	1台
10	サーバラック	サーバラック	2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9年3月31日)
2	環境設定定義書(本番環境)		

3	特許庁及び支援ベンダ向け運用マニュアル	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9年3月18日)
---	---------------------	---------------------	--------------------------------

※環境設定定義書および運用マニュアルの作成にあたってはハードウェア導入ガイドラインを参考にすること

- (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) 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。

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。プロジェクトの前半は構築・導入が主たる作業になり、運用・保守の作業の多くは後から発生することから、運用・保守チームはプロジェクト開始時点で必須とはせず、構築・導入チームと運用・保守チームが統合された体制も可能とする。受注者は図 5.1-1 を踏まえた体制にて主体的に構築・導入フェーズ及び運用・保守フェーズにおける各種作業を実施すること。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。

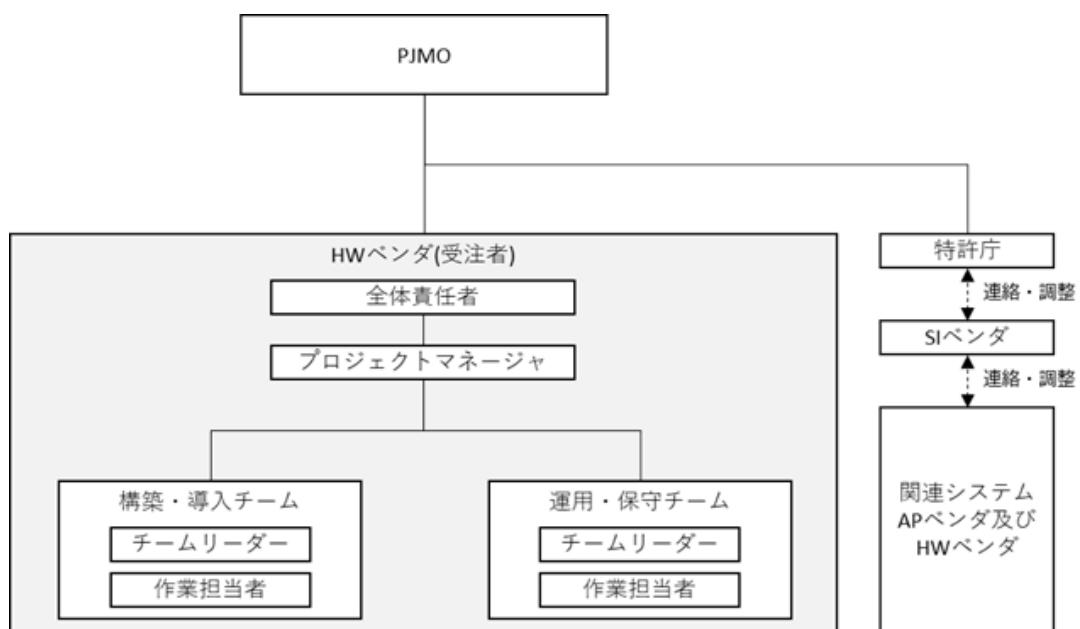


図 5.1-1 作業実施体制図(想定)

(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	<ul style="list-style-type: none"> ・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) 	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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 	<p>【プロジェクトマネージャの業務面に係る要件】</p> <ul style="list-style-type: none"> ・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。 <p>【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】</p> <ul style="list-style-type: none"> ・以下に示す条件をすべて満たすプロジェクトにおいて、本業務のプロジェクトマネージャと同等の役割としての業務経験、または、サブマネージャまたはチームリーダーと同等の役割としての2件以上の業務経験を有すること。 <ul style="list-style-type: none"> ➤ 本業務と類似するハードウェアの構築・導入及び運用・保守業務 ➤ 本サーバー式と同等規模のサーバー式の構築・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。 <p>[資格]</p> <ul style="list-style-type: none"> ➤ プロジェクトマネージャ(IPA) ➤ システムアーキテクト(IPA) ➤ ITストラテジスト(IPA) ➤ PMP(Project Management Professional)(PMI) <p>[ITスキル標準]</p> <ul style="list-style-type: none"> ➤ 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 ※チーム構成は応札者の提案に委ねる	<ul style="list-style-type: none"> ・構築・導入作業の円滑な実施 	<p>【構築・導入チームに係る要件】</p> <ul style="list-style-type: none"> ・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。 <p>【チームリーダーに係る要件】</p> <ul style="list-style-type: none"> ・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。 ・以下に示す条件をすべて満たすプロジェクトにおいて、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、または、サブチームリーダーと同等の役割としての2件以上の業務経験を有すること。

No.	役職・チーム	役割	要件
			<ul style="list-style-type: none"> ➤ 本業務と類似するハードウェアの構築・導入業務 ➤ 本サーバー式と同等規模のサーバー式の構築・導入業務 ・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] <ul style="list-style-type: none"> ➤ プロジェクトマネージャ(IPA) ➤ システムアーキテクト(IPA) ➤ ITストラテジスト(IPA) ➤ ITサービスマネージャ(IPA) ➤ ネットワークスペシャリスト(IPA) ➤ 情報処理安全確保支援士(IPA) ➤ PMP(Project Management Professional) (PMI) 【ITスキル標準】 <ul style="list-style-type: none"> ➤ 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	<ul style="list-style-type: none"> ・運用・保守作業全 体の管理 ・運用・保守作業の 円滑な推進 	<p>【運用・保守チームに係る要件】</p> <ul style="list-style-type: none"> ・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、本サーバー式の可用性を高く保ち、障害発生時にはプロジェクトマネージャと密に連携しながら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。 ・運用・保守作業全体を管理・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。 <p>【チームリーダーに係る要件】</p> <ul style="list-style-type: none"> ・以下に示す条件をすべて満たすプロジェクトにおいて、運用・保守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、または、サブチームリーダーと同等の役割としての2件以上の業務経験を有すること。 ➤ 本業務と類似するハードウェアの運用・保守業務 ➤ 本サーバー式と同等規模のサーバー式の運用・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] <ul style="list-style-type: none"> ➤ プロジェクトマネージャ(IPA) ➤ システムアーキテクト(IPA) ➤ ITストラテジスト(IPA) ➤ ITサービスマネージャ(IPA) ➤ ネットワークスペシャリスト(IPA) ➤ 情報処理安全確保支援士(IPA) ➤ PMP(Project Management Professional) (PMI) 【ITスキル標準】 <ul style="list-style-type: none"> ➤ カスタマサービス(レベル4以上) ➤ ITサービスマネジメント(レベル4以上)

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」を参考にしつつ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、作業に遅延が生じた場合の可視化対策として、遅延と判断するポイントを設定すること。
 - 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。
 - ② 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。
 - ③ 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。
 - ④ 打合せの議事録(概要)は、打合せ後速やかに作成のうえ、特許庁の了承を得ること。また、特許庁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、特許庁の確認を得るものとする。
 - ⑤ 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(平成 12 年法律第 100 号)第 6 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/hozan/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/1fc6722a/20240605_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/9462b2d8/20240605_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) 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>)
- (2) 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)
- (3) 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)
- (4) 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)
- (5) 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、そのためには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、読み込み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、データの復元や読み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き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。
- (4) 特許庁は、受注者が本仕様書に基づく契約(以下、「本契約」という。)を履行するうえで、必要な関連書類(紙媒体、電子媒体を含む。以下、同じ。)を隨時、受注者へ貸与する。ただし、特許庁から請求があった場合は、貸与された関連書類を速やかに特許庁へ返還しなければならない。なお、受注者は、貸与された書類を本契約の目的以外に使用してはならない。
- (5) 受注者は、本調達に係る作業を完了又は契約解除する場合、特許庁から貸与された関連書類を速やかに特許庁に返却し、必ず特許庁の確認を受けること。

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。

8.2. 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. 撤去要件

受注者は、撤去に係るすべての費用を本契約に含めること。

10.2. 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を行い、可及的速やかなサービスの復旧に努めること。
- (2) 受注者は、受注者の責により本サーバー式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、受注者の責により本サーバー式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。

10.3. 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) 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。
- (5) 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。

- (6) 将来、本サーバー式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。
- (7) 本調達の機器等を令和13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。
- (8) 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。

10.4. 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、本サーバー式の構築・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。

10.5. 機能証明書等について

受注者は、応札時に提出した機能証明書等の内容を遵守すること。

10.6. 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。

10.7. 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。

10.8. 履行完了後の情報の取扱い

特許庁から提供した資料又は特許庁が指定した資料の取扱い(返却・削除等)については、特許庁の指示に

従うこと。

10.9. 情報セキュリティについて

業務情報を取り扱う場合又は業務情報を取り扱う情報システムやウェブサイトの構築・運用等を行う場合、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。

10.10. 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

10.11. 特許庁担当者

特許庁 総務部 総務課

情報技術革新室 村田 泰利

情報技術革新室 鍬 利孝

情報技術革新室 櫻井 亮太

(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。)

10.12. 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-9c31-0f06fc67afc/1fc6722a/20240605_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.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_503AC00000000037

No.	資料名	資料の概要及び位置付け
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.nisc.go.jp/pdf/policy/general/kijyunr5.pdf

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	想定ユースケース詳細

11.4. 事業者が閲覧できる資料一覧表

事業者が特許庁舎内の会議室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
3	ポリシー実施手順(設計基準)
4	ポリシー実施手順(運用編)
5	ポリシー実施手順(開発編)
6	特許庁ネットワーク設計基準
7	サービスネットワーク利用基本方針
8	運用マニュアル引継ガイドライン
9	障害報告ガイドライン
10	特許庁が使用しているソフトウェア一覧
11	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を PDF 化したうえで、メールにて当該 PDF ファイルを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】

「AI 基盤サーバー式の導入に係るハードウェア等賃貸借及び保守等業務 一式」に係る要件定義書等の送付希望

【メール宛先】

特許庁 総務部 総務課 情報技術革新室 bzl-kakushin@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(複数提示すること)

【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革新室 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。
- (5) 連絡を受けた来庁日時に来庁し、庁内資料を閲覧する。

11.6. 提案書等の審査要領

審査要領は入札説明書による。

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および遵守状況の報告】

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。）に提示した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た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5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、当庁又は内閣官房内閣サイバーセキュリティセンター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、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、リスクが許容でき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、O S、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。

- ・サービス開始前および、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) 等の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、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、必要があつ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。

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5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内閣サイバーセキュリティセンター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、リスクが許容でき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)	<p>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。</p> <p>(1) 各工程において、特許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。</p> <p>(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、特許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。</p> <p>(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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>(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。</p> <p>(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</p>	

	<p>こと。</p> <p>(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、O S、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。</p> <p>(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特許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「. g o . j p」を使用すること。</p> <p>(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。</p> <ul style="list-style-type: none"> ・サービス開始前および、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。 <p>(9) 電子メール送受信機能を含む場合には、SPF (Sender Policy Framework) 等の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。</p> <p>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、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。</p>	
情報セキュリティに関する事項 16)	<p>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。</p> <p>(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。</p> <ul style="list-style-type: none"> 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、特許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、H T M Lソースを表示させるなどして確認すること。 <p>(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。</p> <p>(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。</p> <p>(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（G P K I）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。</p> <p>(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O S、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O S、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。</p> <p>(6) 特許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、必要があつ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、特許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</p>	

	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

- 「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。
- 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))。)