（別紙）「生成AIの業務利用に関する技術検証、利用環境整備 要件定義書」

分類	項目	要件	対応区分	備考
1 基本要件				
	1.1 検証環境の提供形態	契約開始時点でデジタル庁、実証に参加する府省庁、自治体の保有する、機密性２情報を取り扱うことのできる安全な基盤上で、大規模言語モデル(以下「LLM」という。) を利用できるサービスを提供すること。	必須	
	1.2 必須要件（示唆）	政府に対する生成AI関係の示唆の提供を行うこと。具体的には次の２項目である。 （ア）政府のAI戦略に関する示唆：３件以上 （イ）官民のAIガイドライン、政府調達ルール等への示唆：２０件以上	必須	
	1.3 必須要件（利用促進）	検証環境の利用促進のために、次の３項目を実施すること。 （ア）AIの業務利用に関するセミナー開催：６回以上 （イ）AIの業務利用に関するユースケースの紹介：４０件以上 （ウ）ユースケースに応じた継続的な機能の改善	必須	
2 機能要件				
	2.1 大規模言語モデル	本件実証における評価検証対象のLLMは、一部検証のみを行う環境を除いて２種類以上として、商業的に広く利用されている最高水準のもの、モデルを広く公開しているオープンなもの、それぞれ一種類以上を含むこと。なお、LLMは同じだが、チューニング等が異なるサービスは同一とみなす。	必須	
	2.2 利用者登録	500人以上の利用者登録に対応すること。 アカウントに対して権限管理を行い、利用できるLLMや参照できるデータの範囲を指定できること。 利用者数やリクエスト数を日次で把握できるようにし、必要に応じて一時的に検証環境の利用やアクセスを制限できるようにすること。	必須	
	2.3 検証要件	検証を行う上で、LLMを密接に組み込んだ利用者向けSaaSアプリケーション（ソフトウェア開発支援ツールや生産性アプリケーション等）を使用する場合は、市場で広く利用されているものを利用することとし、評価に必要なライセンス量等を提案に含めること。	必須	
	2.4 アクセス制限	検証環境には、発注者が指定したデジタル庁職員、実験に参加する府省庁職員、自治体職員などの関係者がアクセスできるようにすること。環境の管理者権限も、発注者が指定したデジタル庁職員に払い出し、共同で作業にあたること。	必須	
	2.5 APIコール数等の制限	APIコール数等に制限がある場合は明示して、その制限を超えそうな場合は優先度の高い検証作業に必要なサービスレベルを確保しつつ、一般利用を制限できるようにすること。上限を引き上げることができる場合は、その条件等を提示すること。		
	2.6 構築情報	セキュリティ確保のため、本システムで用いるクラウドサービスは、原則としてISMAPクラウドサービスリストまたはISMAP-LIUクラウドサービスリストに登録されているクラウドサービスを選定すること。なお、例外的にISMAPクラウドサービスリスト、またはISMAP-LIUクラウドサービスリストに登録されていないクラウドサービスを選定する場合は、受託者の責任において、当該クラウドサービスが「ISMAP管理基準」の管理策基準における統制目標（3桁の番号で表現される項目）及び末尾にBが付された詳細管理策（4桁の番号で表現される項目）と同等以上のセキュリティ水準を確保していることものを選定すること。	必須	

分類	項目	要件	対応区分	備考
	2.7 構築情報	上記のセキュリティ要件に加えて、クラウドセキュリティ、データ保護に関する以下の要件を満たすようにクラウドサービスを選定し、利用すること。 〇「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」(以下、「クラウド方針」という。)を遵守すること。 〇情報資産を管理するデータセンタの設置場所に関しては、国内であることを基本とする。設置場所の考え方についてはクラウド方針を参照すること。 〇契約の解釈が日本法に基づくものであること。 〇クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。 〇主管課の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。情報資産を国外に設置されるクラウドサービスに保管する際の考え方についてはクラウド方針を参照すること。なお、利用者がアクセス可能な部分を除き、国外から情報資産へアクセスする場合も日本国外への持ち出しに該当する。 〇障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。 〇情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、主管課が要求する任意の時点で情報資産を他の環境に移管させることができること。	必須	
	2.8 構築情報	SaaSベースで構築することを前提に検討し、SaaSでは要件を満たさない場合は、PaaS、IaaSなどを選択すること。なお、本調達で構築するシステムでは、比較的短期間での機能の追加が求められることが想定されることから、簡易な操作で機能の追加が可能であること。 なお、今後、利用者の拡大が見込まれることから、今後の発行アカウント数の拡大時の安定稼働や運用費用の抑制等の観点から、本調達の趣旨に適したクラウドサービスを利用すること。	必須	
	2.9 データ管理	本件実証を通じて作成したデータは、実証終了後も必要に応じて実証参加者等が利用できるようにすること。	必須	
	2.10 利便性向上機能	学習済みの生成AIを単独で用いるだけでなく、利便性向上に寄与する機能や付加価値等はその提案が優れているとみなせる場合は公募審査の加点の対象になる。	任意	
3 委託先組織に求める情報セキュリティ対策遂行能力				
	3.1 情報セキュリティを確保するための体制の整備	受託者は、受託先において情報セキュリティ対策を確実かつ継続的に実施するための責任者を定め、個別の対策の実施・点検・改善等を行う体制（以下「情報セキュリティを確保するための体制」という。）を整備し、本調達に係る業務の着手に先立ち、その概要を示す資料を提示すること。 契約期間中、整備した情報セキュリティを確保するための体制 を維持すること。	必須	
	3.2 再委託における情報セキュリティの確保	受託者は、本調達に係る業務の一部を他の事業者への再委託により行わせる場合には、事前にデジタル庁の承認を得ること。受託者は、デジタル庁が受託者に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再委託先に行わせること。再委託先に行わせた情報セキュリティ対策及びこれを行わせた結果に関する報告を受託者に求める場合がある。	必須	
	3.3 対策の履行が不十分な場合の対処	受託者の責任者は、本調達に係る業務の遂行における情報セキュリティ対策の履行が不十分である可能性をデジタル庁が認める場合には、デジタル庁の求めに応じこれと協議を行い、合意した対応を取ること。	必須	
	3.4 情報の機密保持	受託者は、本調達に係る業務の実施のためにデジタル庁、実証に参加する府省庁、自治体から提供する情報及び当該業務の実施において知り得た情報について、以下の事項を遵守すること。ただし、既に公知である情報については、この限りではない。 (1) 本調達に係る業務にのみ使用し、他の目的には使用しないこと。 (2) 本調達に係る業務を行う者以外には機密とすること。	必須	
	3.5 情報セキュリティ対策の履行状況の確認等に関する事項の周知	受託者は、デジタル庁から、本調達に係る業務の遂行における情報セキュリティ対策の履行状況に関する以下の事項の報告を求められた場合は、速やかに回答すること。 (1) 本仕様において求める情報セキュリティ対策の実績 (2) 受託者に取り扱わせるデジタル庁の情報の機密保持等に係る管理状況	必須	

（別紙）「生成AIの業務利用に関する技術検証、利用環境整備 要件定義書」

分類	項目	要件	対応区分	備考
4 アクセスコントロール及びログ				
	4.1 ユーザー認証	職員個人単位でユーザ登録し、ログイン処理時にユーザー認証できること。（一般的なシステムのログイン認証）	任意	検証環境と同一のネットワーク上に国・地方公共団体の保有する既存の認証基盤がある場合は、連携（シングルサインオン）できるよう努めること。（オプション機能としての提供可）
	4.2 アクセス制御	ユーザー単位でアクセスできるデータの範囲や権限をコントロールできること。	必須	
	4.3 一時的なアクセス制限	利用者数やリクエスト数を日次で把握できるようにし、必要に応じて一時的に検証環境の利用やアクセスを制限できるようにすること。	必須	
	4.4 ログ取得	ユーザー単位で、システム利用監査証跡（データ参照、更新、削除等）や印刷・データ出力時のログを取得できること。 取得したログの漏えい、改ざん、消去、破壊等を防止し、契約期間中は保存し、いつでもデジタル庁に提供可能とすること。 ログの提供にかかる経費は、利用料の範囲内に含まれるものとする。	必須	
	4.5 年度切替処理	職員異動に伴うユーザーの削除や登録、変更等の作業負荷を軽減する機能（CSVによる職員情報の一括取込等）を実装すること。	必須	
5 SLA				
	5.1 サービス稼働時間	24時間365日とする。（計画停止等を除く）	任意	
	5.2 サービス稼働率	99.5%以上とする。	任意	
	5.3 平均応答時間	通常の業務アプリケーションの応答時間として、リクエストの99.9%以上を3秒以内とする。（複雑な検索／分析処理機能を除く）	任意	
	5.5 障害通知時間	1時間以内	任意	
	5.5 平均障害復旧時間	一般的な障害（プロセス停止等）は5分以内に自動復旧すること。 自動復旧できない重度の障害（多重障害等）は3時間以内に復旧すること。 大規模障害（クラウドサービスプロバイダー自体の停止）は可及的速やかに復旧を目指すが障害復旧目標を設けない。	任意	
	5.7 RPO（目標復旧地点）	平常時、業務停止を伴う障害が発生した際には、直近のバックアップまたはシステム変更時までのデータ復旧を目的とする。	任意	
	5.8 システムバックアップ頻度	コンテナとマネージドサービスで構成すればシステムバックアップ不要とする。 やむを得ずサーバインスタンスやファイルサーバを使う場合は日次でのシステムバックアップを取得する。	任意	
	5.9 データバックアップ頻度	日次、システム変更時	任意	
	5.10 計画停止予定通知	30日前にメール/Webで通知	任意	
	5.11 ヘルプデスク	検証環境の管理運用に関し、国・地方公共団体のシステム管理者からの問い合わせ受付から障害対応まで、一元的な運用保守窓口（ヘルプデスク）を設置すること。なお、受付方法（メール・ビジネスチャット等）については事業者側で判断すること。	任意	
	5.12 ヘルプデスク	受付時間は、メール・ビジネスチャット等により24時間365日とする。 対応時間は緊急時を除き、平日のデジタル庁の開庁時間に合わせることを基本とする。	任意	
	5.13 サービス終了通知	サービス終了する日を含む月を除いた12月前にメール/Webで通知すること。	任意	

分類	項目	要件	対応区分	備考
6 その他			任意	
	6.1　脆弱性対策	検証環境のアプリケーション領域の脆弱性対策は検証環境提供事業者の責任において実施すること。	任意	
	6.2　データ消去	検証で用いる顧客側のデータについては、派生データも含めて顧客側で管理できるようにすること	任意	