生成 AI の業務利用に関する技術検証、利用環境整備

調達仕様書

デジタル庁　戦略・組織グループ AI 班

１　調達件名

生成 AI の業務利用に関する技術検証、利用環境整備（以下「本調達」という。）

２　調達の背景

大規模で汎用性が高い基盤モデルを活用した「生成 AI」の性能が格段に向上し、その利用が急拡大するなど、AI の社会的な影響力が急速に増大している。

これによって、AI の活用を通じた新しい価値の創出への期待がこれまで以上に高まっている一方、社会に及ぼすリスクへの懸念も高まってきており、諸外国においては、AI 開発と並行して、社会受容の在り方に関する議論も加速している。

AI の適切かつ効果的な活用は、生産性向上や競争力強化を通じ、我が国における社会課題の解決や経済成長につながる可能性を秘めている。

こうした可能性を踏まえ、AI に係るリスクの懸念に適切に対処するとともに、「人による作業」の要否を整理し、AI 活用に向けた取組を進めていく必要がある。

目下、我が国としては、今後の AI の活用の基盤となるデータの整備等を含むインフラの整備・強化に向けた検討・取組と、AI の実態と動向を把握し、リスクと必要な対応策を特定した上で、官民における適切な活用に向けた検討・取組を進めることが重要である。

上記を踏まえ、急速な AI の進歩・普及を踏まえ、行政における生成 AI の利用について検討や環境整備を進めているところ。

引き続き、行政運営の効率化、行政サービスの質の向上等につなげるため、国・自治体における更なる積極的な技術検証が必要になると考えられる。

本調達は、そうした環境を整備すべく、技術検証を行うためにデジタル庁が調達するものである。

３　目的等

デジタル庁で安全な基盤上で、行政職員が生成 AI を扱うことのできる実証環境の調達を行う。併せて、各省庁・自治体において実施される技術検証への支援体制も整える。

４　事業の内容

(1) 前提条件

- 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。
- 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ものを選定し、上記対応が確認できる資料を提示すること。

- 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。
  - 「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」（以下、「クラウド方針」という。）を遵守すること。
  - 情報資産を管理するデータセンタの設置場所に関しては、国内であることを基本とする。設置場所の考え方についてはクラウド方針を参照すること。
  - 契約の解釈が日本法に基づくものであること。
  - クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。
  - 主管課の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。情報資産を国外に設置されるクラウドサービスに保管する際の考え方についてはクラウド方針を参照すること。なお、利用者がアクセス可能な部分を除き、国外から情報資産へアクセスする場合も日本国外への持ち出しに該当する。
  - 障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。
  - 情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、主管課が要求する任意の時点で情報資産を他の環境に移管させることができること。
  - SaaS サービスの利用や CSP の生成 AI　PaaS サービスの検証画面、自社開発等の提供形態には制限を設けない。
- SaaS サービスの選定に関する参考事項
  - SaaS ベースで構築することを前提に検討し、SaaS では要件を満たさない場合は、PaaS、IaaS などを選択すること。なお、本調達で構築するシステムでは、比較的短期間での機能の追加が求められることが想定されることから、簡易な操作で機能の追加が可能であること。
  - 今後、利用者の拡大が見込まれることから、今後の発行アカウント数の拡大時の安定稼働や運用費用の抑制等の観点から、本調達の趣旨に適したクラウドサービスを利用すること。

- 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を 1 種類以上、モデルを広く公開しているオープンなもの、または、提案者自身が開発または調整したもののいずれかを１種類以上含むこと。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。日本語に特化して品質向上可能なモデルがあれば望ましい。
- LLM のモデルそのものによる回答だけでなく、使途に応じた回答を返すことができるように、行政情報を読み込ませた個別のファインチューニング、エンベディング、外部検索 API との連携、外部サイトのクローリング等、ミドルウェア環境も合わせて提供すること。
- パブリッククラウド上で構築された検証環境については、その構築に必要な IaC テンプレート等を納品物に含めるとともに、成果の一部としてクラウドサービスのアカウントを引渡し、次年度以降にデジタル庁が必要な基盤費用やライセンス費用等を負担した場合には、同じ環境を使い続けられるようにすること。
- 検証環境には、発注者が指定したデジタル庁職員、実験に参加する行政職員等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。
- 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。次年度以降の事業や他システムに容易に移行できる形式でデータを引き渡すこと。

(2) 必須要件

業務効率化の有用性の検証にあたっては、生成 AI の利活用によって節約できると試算される時間の算出のほか、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

また、本調達の検証環境をより多くの利用者に活用いただくために、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

上記検証を行う上で、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。

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。

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。

また、アプリケーション開発として、以下の機能とそれに対応するコンポーネントから構成されるアプリケーションを構築すること。

- 主体認証機能
  （クラウドの認証サービスの利用を想定）
- フロントエンドアプリケーション
  （ブラウザで動く環境を想定。ユースケースによって既存チャットツールの拡張で十分な場合もある）
- セキュアな外部電磁的記録媒体
  （ログ取得用の暗号化されたクラウドストレージやVPCなどの外部から隔絶したネットワーク環境の構築を想定）
- 大規模言語モデルのPaaS
  （Web APIなどを介して大規模言語モデルを利用するサービス）

上記必須要件を満たすための本件技術検証の具体的な機能・取組については、各事業者によるニーズ把握及び創意工夫に委ねる。

(3) 加点となる任意要件

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。

（機能や付加価値の例）

- チャットインターフェース以外のインターフェース。大量のテキストが格納されたExcelをアップロードからの該当テキストがラベル付けされた状態でCSVダウンロード等
- ユーザが用語集等をアップロード・共有ができ、生成AIの出力のハルシネーションの自動検出や、文章に紐づく用語集の提案等
- 具体的なユースケースや性能測定に有用なデータセットの事前登録等
- ソースコードやＳＱＬの提案だけでなく、バックエンドにプログラム環境やデータベースが動き、そのコードやＳＱＬの実行結果の返却等
- 一問一答形式だけではなくユーザ定義のワークフローの作成等が実現可能な仕組み
- 一般的なLLMのcontext window(最大token超)を超えた数百ページ以上の長大な

ＰＤＦに準拠した回答生成・質問応答等

- テキストを使った学習・応答だけでなく、画像の解説・生成などに対応したマルチモーダル機能等
- 検証用のプロンプトやデータ、検証結果の会話履歴等の共有機能等
- その他、任意のツールと組み合わせることができる API エンドポイント等

(4) 法改正・バージョンアップ対応・リスク管理に係る要件

- 日々の運用で継続的な改善活動を行うこと。
- LLM やクラウドサービスにおける継続的なアップデートへの対応を行うこと。
- 各種認証情報の流出防止策、流出時の検知、インシデント対応をおこなうこと、加えてセキュリティ対策については、NISC 政府統一基準及びデジタル庁セキュリティポリシー（契約後に開示）に従って実施すること。
- AI 規制に係る国際的な動向、政府 AI 戦略チームの方針、AI 統合ガイドラインなどの外部環境を踏まえて必要な措置を講ずること。
- 当面は必要なリスク管理、リスク軽減策を講じつつ、将来へ向けた政府の生成 AI 調達ガイドラインの整備へ向けて盛り込むべき事項や、個々のユースケースに応じた機能要件、非機能要件について提案すること。
- LLM を活用したサービスについて、安全管理措置を講ずる上での制御可能な点や、品質管理のあり方を明らかにして、技術検証の中で実際に品質を担保できているか、応答内容が利用者の誤解やミスユースを誘発していないか、悪意あるプロンプト等に対する不適切な応答を防げているか、その他のリスク・インシデント等に適切に対応できたかについて検証を行うこと。

(5) 想定スケジュール

項目	備考	実施主体	2023年度 1月	2月	3月	2024年度 4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
公募開始	参加要件や必要資格提示	デジタル庁			→	→											
必要書類を提出し応募	企画提案書	事業者					★										
プレゼンテーション	企画提案書に基づき、ニーズ把握及び創意工夫に関する取り組みを説明	事業者					★										
事業者選定	企画提案書及びプレゼンテーションの内容に基づき審査	デジタル庁					★										
契約		デジタル庁 事業者					★										
アカウント払い出し	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対象	事業者						→	→	→	→	→	→	→	→	→	→
実証実験								→	→	→	→	→	→	→	→	→	→
振り返り																→	→

５　調達の範囲

本調達の範囲は、行政における生成 AI の適切な利用に向けた技術検証の環境整備であり、概要は以下のとおり。

(1) 実験に参加する行政職員に対する検証環境の提供

別紙「要件定義書」の要件を満たす検証環境を構築し、実験に参加する行政職員等の関係者に提供できる環境を構築すること（利用申し込みを受けたら当該利用者が利用できる個別の検証環境を切り出し、提供をする作業を含む。）。

(2) LLM 検証環境の運用・保守

(ア)LLM 検証環境の運用・保守を実施し、技術検証に支障が生じないよう安定稼働させること。

(イ)LLM 検証環境の利用者数、所属組織、利用しているユースケース、問い合わせ対応（件数や主な内容）、安定稼働・バージョンアップのために実施した作業等の実績レポートを月次でデジタル庁に報告すること。

(ウ)サービスの稼働状況やサービスの主要 KPI（登録数やリクエスト数、ユニークユーザ数等サービスごとに事前に定義する）、セキュリティ遵守状況はダッシュボードとして常に確認できるようにすること。ダッシュボード掲載データ項目は、例として以下のような内容を想定しているが、詳細は協議の上決定する。また、これらデータ項目は複数ダッシュボード画面に分かれていてもよい。

No	項目	内容
1	サービスの主要 KPI	利用者数やリクエスト数、ユースケース別件数等
2	サービスレベルに関する項目	応答時間、エラー率、障害停止時間（率）等
3	セキュリティ設定遵守状況	クラウドの設定等が意図したとおりになっているかの自動チェック（クラウドの機能の利用）
4	アプリケーション／インフラのリリース状況	アプリケーションやインフラがリリースされた時刻、回数等（リリース承認プロセスと突合できるよう）
5	管理者の監査	管理者の一覧及び利用状況
6	管理者ロール監査	管理者のロールの一覧及び変更履歴
7	管理コンソール監査	管理コンソール等にログインした履歴
8	リソース監査	追加されたリソースの一覧
9	クラウドリソース利用状況	使用したクラウドリソースの利用状況等の情報（※地方公共団体単位での算出が望ましいが、按分できない部分については協議）

(3) 利用促進方策の実施

(ア)行政職員が技術検証を円滑に実施できるように、操作マニュアル等を作成すること。

(イ)技術検証を実施する工程で、職員と協働して検証作業を支援し、発生した課題への対応方法について助言すること。

(ウ)業務効率化の有用性検証にあたり、事業者独自のユースケースを提案すること。

(エ)技術検証環境の利用促進のため、AI の業務利用に関するセミナーを開催すること。

(オ)技術検証を職員が円滑に実施できるように、AI の業務利用に関するユースケースを紹介すること。

(カ)技術検証を実施する工程で、実用性を検証したユースケースを提案すること。技術検証完了後に、検証内容の評価、今後の課題等をまとめた技術検証報告書案を作成すること。

6 契約期間

本調達の契約期間は、契約締結日から令和７年３月 31 日（月）までとする。

7 成果物

(1) 成果物

本調達の成果物を下表に示す。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・開発実施計画書にて定める。なお、これらの成果物を作成するにあたり、参考とした中間成果物・プロジェクトの継続に必要な情報を引き渡すこと。

項番	成果物名	納入期限（想定）
1	設計・開発実施計画書	契約締結後２週間以内
2	設計・開発実施要領	契約締結後２週間以内
3	設計書	設計・開発の状況に応じて順次
4	検証環境一式	設計・開発の状況に応じて順次
5	操作手順書	設計・開発の状況に応じて順次
6	運用・保守計画書	設計・開発の状況に応じて順次
7	運用・保守実施要領	運用・保守開始前まで
8	情報セキュリティ管理計画書	運用・保守開始前まで
9	定例ミーティングの議事録	定例ミーティング実施後３開庁日以内
10	機密性２情報を取り扱い可能である根拠資料	事業開始後４か月以内
11	報告書	契約満了前

(2) 納品方法

- 成果物は、全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については、そのまま記載しても構わないものとする。
- 用字・用語・記述符号の表記については、「公用文作成の考え方（令和４年１月 11

日内閣官房長官通知)」を参考にすること。
- 情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。
- 成果物は電子データでの納品とすること。提出先はデジタル庁の担当と協議の上、決定すること。
- 納品後、デジタル庁において改変が可能となるよう、Microsoft Office 形式や図表等の元データも併せて納品すること。
- 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、デジタル庁の担当の承認を得ること。
- 成果物が外部に不正に利用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
- 電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。なお、対策ソフトウェアに関する情報（対策ソフトウェア名称、定義パターンバージョン、確認年月日）を記載したラベルを貼り付けること。
- 受託者が保有する特許などを用いる場合には、成果物にその旨を明記すること。

(3) 納品場所

- 原則として、成果物はメール・郵送等にて引渡しを行うこと。ただし、発注者が納品場所を下記をはじめ、別途指示する場合はこの限りではない。

連絡先　東京都千代田区紀尾井町１－３　東京ガーデンテラス紀尾井町
デジタル庁　戦略・組織グループ AI 班

(4) 契約不適合責任

(ア)発注者は、受注者に対し、成果物が本契約の内容に適合しないものであるとき（ただし、発注者が本契約の内容に適合しないことを本契約締結前に認識している場合を除く。）は、成果物の補修による履行の追完を請求することができる。ただし、受注者は、発注者に不相当な負担を課するものでないときは、発注者が請求した方法と異なる方法による履行の追完をすることができる。

(イ)アの場合において、発注者が、相当の期間を定めて履行の追完を催告し、その期限内に履行の追完がないときは、発注者はその不適合の程度に応じて代金の減額を請求することができる。

(ウ)アの場合において、本契約の不適合により損害を被ったときは、発注者は、損害賠償の請求又は本契約の解除をすることができる。

(エ)アからウの請求に当たっては、受注者が本契約に不適合な成果物を引渡した場合

において、発注者がその不適合を知ったときから１年以内に、受注者に対して不適合の内容を通知するものとする。

８　その他

(1) 本調達は、原則として日本語により対応すること。

(2) 本仕様書に記載がない事項でも、以下のドキュメントを参照し、対応すること。

(ア)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）

(イ)デジタル庁セキュリティポリシー

(ウ)ChatGPT 等の生成 AI の業務利用に関する申合せ

(エ)地方公共団体における情報セキュリティポリシーに関するガイドライン

(オ)その他、関係府省が定めた AI に関するガイドライン等

(3) 発注者が指定した行政職員が、安全に LLM を利用できる環境を提供すること。例えば既存の政府職員・自治体職員しかアクセスできないサイト上に利用ページを開設すること、共創プラットフォーム上に bot を設置するなど、既存のサービスを活用して提供することも別途協議の上で考えられる。

(4) 技術検証の開始以降、利用状況をダッシュボード等を通じて月次で報告すること。

(5) 本仕様書に記載なき事項にあっても本調達の業務遂行において必要と認められる事項に関しては、別途協議の上、実施すること。

９　附属文書

・要件定義書

10　担当・連絡先

担　当　デジタル庁　戦略・組織グループ AI 班

連絡先　東京都千代田区紀尾井町１－３　東京ガーデンテラス紀尾井町

メール：digital-ai@digital.go.jp