# 令和８年度

# 生成ＡＩサービス提供及び利用支援業務仕様書

和歌山県総務部総務管理局行政企画課

## １　調達案件の名称

生成ＡＩサービス提供及び利用支援業務（以下「本業務」という。）

## ２　調達の目的

行政事務の効率化、生産性の向上を図るため、十分なセキュリティ対策により安全性が確保された生成AIサービスを全庁的に導入するとともに、利用促進に係る施策の実施や行政実務に生成AIを効果的に活用するための環境整備を行い、庁内における生成AIの定着を図ることを目的とする。

## ３　サービスの納入場所

和歌山県総務部総務管理局行政企画課（以下「発注者」という。）

## ４　契約期間

令和８年４月１日から令和９年３月３１日まで

## ５　生成 AI サービスの要件

（1）サービス形態

以下の要件を満たすこと。

ア クラウドサービス（SaaS 型）であり、ブラウザ画面から当該サービスを利用できること。

イ 利用ブラウザは、Microsoft Edge 及び Google Chrome に対応していること。

ウ チャット形式で利用できること。

（2）利用アカウント

ア 最大約 4,500 名の職員に対し、アカウント発行が可能であること。

イ 100 名以上のユーザーが同時にアクセス可能であること。

（3）管理者機能

ア 管理者権限を持つアカウント（以下、管理者アカウント）は、ユーザーアカウントの登録、変更、削除が行えること。csv 形式などのデータを用いて一括で登録、変更、削除ができること。

イ 管理者アカウントにより、利用者の利用ログを確認できること。利用ログの内容は、当該サービスに入力されたメッセージ内容、利用文字数とする。また、利用ログをデータとして出力できること。

ウ 管理者アカウントにより、ユーザまたはグループ単位で、利用できる大規模言語モデルの種類を制限できること。

エ 管理者アカウントにより、一部のユーザーに対し、RAG 機能に用いるデータをアップロード、登録する権限を付与することができること。

（4）大規模言語モデル

当該サービスで取り扱う大規模言語モデルについては、以下の要件を満たすこと。

ア GPT-5.2、Gemini 3 Pro を利用できること。文字数制限を設ける場合は、１か月あたり 1,000 万文字（入力と出力の合計文字数）以上を利用可能とすること。
使用文字数が、月間の上限に達した場合は、文字数の制限がない大規模言語モデルに限って利用することができること。

イ GPT-5 mini、Gemini 3 Flash のいずれかと同じか、それ以上の性能を持つ大規模言語モデルを文字数無制限に利用できること。

ウ チャット内にドキュメント（Word/Excel/PowerPoint/テキスト/PDF）を添付し読み込ませることができること。

エ Deep Research 機能が利用でき、AI が自律的に多段階のリサーチを行い、詳細なレポートを生成することができること。

（５）RAG 機能

サービスにアップロードして登録したデータに基づいて文章生成することができる、検索拡張生成機能（RAG 機能）を利用できること。本機能については、以下の要件を満たすこと。

ア 複数のデータを当該サービスに登録できること。登録するデータは、用途別に整理、分類でき、回答生成時には、利用者が用途や分類に応じて、参照する領域を選択、切り替えが可能であること。

イ 登録できるデータの種類は、Excel、PowerPoint、Word、PDF、CSV、txt 形式に対応していること。

ウ 登録したデータについて、利用可能となるユーザーまたはグループの範囲を設定できること。

エ 登録するデータの総容量は、100GB 以上を蓄積可能とすること。なお、個別データ当たりの容量制限を設けることは問題ないものとする。

オ 文字数制限のない大規模言語モデルにおいて、本機能を利用できること。

カ RAG 機能で生成された回答には、根拠資料を確認できるように、参照文書名などを回答と合わせて表示できる機能があること。

（６）セキュリティ対策

ア 当該サービスに入力した情報が生成 AI の学習データとして利用されないこと。

イ 和歌山県庁の庁内 LAN 以外の環境からサービスにログインできないよう、グローバル IP アドレスによるアクセス制限がかけられること。

ウ 当該サービス内で処理されたデータは、暗号化された状態で通信しサーバで処理されること。

エ 当該サービスにセキュリティホール等の脆弱性が発見された場合は、協議の上、最新のセキュリティパッチを適用すること。

オ 情報漏えい事故発生時の対応についての手順が整備されていること。

カ 別紙１「外部サービス要件確認表（機密性２以上)」に定めるセキュリティ要件を満たすものであること。

キ 禁止ワードや機密情報の入力制限の機能を有すること。

（7）プロンプトテンプレート

ア プロンプトテンプレートを登録し、ユーザ間で共有して利用することができること。

イ 行政実務に適したプロンプトテンプレートを提供すること。

## ６　RAG 環境の構築支援

（１）委託者（本県）が提供する電子データにもとづき、RAG の精度向上のためのデータの整理・構造化（クレンジング）を行い、的確な指示を与えることで信頼性の高い文章生成が行えるように努めること。

データの整理・構造化の対象とするデータは、平成２３年度から令和７年度までの１５年分の和歌山県議会の定例会・臨時会の質疑及び一般質問に係る公開データ（和歌山県議会ホームページに掲載されている会議録データ）とする。（本会議のみとし、委員会は含まない。）

（２）議会答弁作成業務を支援するプロンプトを登録すること。

プロンプトは、本県の要望に応じたカスタマイズが可能であること。

（３）上記の議会答弁以外の RAG 環境構築や将来的な RAG 運用の自走化に向け、本県からの以下の相談に随時、オンラインミーティング等で対応すること。（６回程度を想定）

・RAG に登録するドキュメントの選定に係る技術的助言
・RAG の登録ドキュメントのデータの整理、構造化に係る技術的助言
・RAG による情報の検索精度を向上させるためのプロンプト作成支援
・RAG による情報の検索精度を維持・向上させるための継続運用方法に係る助言

## ７　利用支援

（１）利用マニュアル等の提供

最新版の詳細な利用マニュアルをブラウザ上で常に参照することができること。
サービスの利用方法やよくある質問をまとめた FAQ サイトを提供すること。

（２）問い合わせ対応

管理者のみならず一般職員からの使用方法に関する問い合わせに対し、電子メール等により対応すること。全ての職員へ以下の項目を満たす問い合わせサポートを提供すること。

・技術的な問題や操作方法の相談
・プロンプトの相談
・RAG の精度向上に関する相談

対応時間は、原則として、午前１０時から午後５時（土・日・祝日、年末年始（12 月 29 日から翌年１月３日）を除く。）とするが、その他対応できない日時等がある場合は、発注者に報告し承認を得ること。

（３）アカウント管理

アカウントの初期登録および職員の異動等に伴う変更管理を行うこと。

（４）利用推進に関する伴走支援

ア　サービスの月間利用者数や利用文字数などの利用状況や傾向が把握できる情報をレポート形式等で月次提供すること。

イ　他自治体などでの利用事例やプロンプト例、新たに追加された機能の活用方法などの情報提供を定期的に行うこと。

ウ　契約締結後、１か月以内を目安に、生成 AI の利用促進に係る定量的な評価指標（例：アクティブユーザ数、部局別利用文字数など）を県と協議の上、決定することとし、合意された評価指標は、以降の定例打ち合わせにおいて、推移を報告すること。

エ　以上の内容の提供等のため、オンライン形式での打ち合わせを原則月１回以上実施すること。

オ　自治体業務で使えるプロンプトを随時テンプレートとしてサービスに登録すること。

## 8　研修

（1）生成 AI の基礎、プロンプトエンジニアリング、RAG 活用などの内容を含む、オンデマンドの研修動画を３種類以上提供すること。

## 9 料金体系

（1）生成 AI サービスの利用量（質問回数、回答回数、入出力された文字数、登録データ量など）に応じた従量料金ではなく、定額の料金体系とし、原則として、毎月定額の精算払いとする。

（2）初期設定費が発生する場合は、最初の月額料金の支払時に、月額料金に加算して支払うものとする。

（3）発注者と受託者が協議し、５に規定する大規模言語モデルの文字数制限等の要件を変更する場合においては、必要に応じて月額料金を変更するものとする。

## 10　機密保護

（1）個人情報、秘密と指定した事項および本業務の履行に際し知り得た秘密（以下「秘密情報」という。）を第三者に漏らし、または不当な目的で利用してはならない。契約終了後も同様とする。

（2）秘密情報を取り扱う責任者および従事者は、秘密保持を誓約しなければならない。再委託先についても同様とする。

## 11　保守

（1）当該サービスの提供時間については、24 時間を保証すること。ただし、契約に基づく範囲外の障害要因及び計画停止に基づく時間は除くものとする。

（2）障害や故障、不具合等に対する受付窓口を設置し、緊急連絡先を示すこと。

（3）障害発生時においても、サービス停止が極力生じないようにすることとし、確実かつ速やかにシステムの復旧を行えるようにすること。

（4）当該サービスに起因する障害が発生した際は、障害内容、対応方法、復旧見込等を発注者に迅速に連絡すること。

## 12　法令等の遵守

本業務の遂行に当たっては、和歌山県情報セキュリティ基本方針及びその他の関連法令を遵守しなければならない。

また、別添「安全確保の措置」に係る遵守事項を遵守すること。

## 13　インシデント発生時の対応

サイバーテロ、ウイルス感染及び情報漏洩等のセキュリティインシデント発生時には、発注者に報告のうえ、速やかに対応を行うこと。

## 14　再委託等の禁止

（1）受託者は、委託業務の全部又は一部を第三者に委託し、又は請け負わせてはならない。ただし、受託者は、あらかじめ発注者に対して書面により申請を行い、承認を受けた場合は、委託業務の一部を第三者に委託し、又は請け負わせることができる。

（2）受託者は、前項の規定により、委託業務の一部を再委託した場合においても、この契約

の当事者としての責めを免れない。

## 15　協議

本仕様書に定める事項に疑義が生じた場合、または本仕様書に定めのない事項で協議の必要がある場合は、受託者は発注者と協議を行うこと。

# 「安全確保の措置」に係る遵守事項

（基本的事項）

第１　乙は、この契約による事務の実施に当たっては、甲の情報を閲覧する者の個人情報を侵害することのないよう、甲から委託を受けて情報を公開するために利用する機器等の管理を適正に行わなければならない。

２　乙は、この契約による事務の実施に当たり、ホスティングサービス、レンタルサーバー、ハウジングサービス又はこれらに類するサービスを利用する場合は、第 1 項に沿って本遵守事項に定める各事項を満たすよう、この契約による事務を処理するに当たり、事前にサービス提供者との間で取り決め又は確認をすること。

（ウイルス対策の実践）

第２　乙は、この契約による事務の実施に当たっては、利用するサーバ等の機器について、ウイルス検知用データは常に最新のものに更新すること。

２　Ｗｅｂサーバの管理用又は更新用等にパソコン等の機器を利用する場合は、乙はこれら機器に対しても第１項で規定する措置を講じること。

（ソフトウェアの更新）

第３　乙は、本遵守事項の第２の対象となる機器で利用するソフトウェアに対しては、定期的に修正プログラムを適用し、できる限りソフトウェアを最新の状態にしておくこと。

（ファイアウォールの導入）

第４　乙は、この契約による事務の実施に当たっては、ファイアウォールを設定し通過させるパケットや遮断するパケットに対するルールを設定しておくこと。

２　乙は、侵入防止システム（IPS）を導入すること。ただし、甲の承諾があるときは、この限りでない。

（セキュリティ診断）

第５　乙は、外部の者によるセキュリティ診断を受けること。ただし、甲の承諾があるときは、この限りでない。

（ログのチェック）

第６　乙は、この契約による委託期間中、定期的にログ（Web サーバー、OS、ルータ、DB 等）をチェックすること。

（コンテンツ内容の確認等）

第７　乙は、著作権を侵害するような写真やイラスト、ファイル等は使用しないこと。

２　乙は、この契約による事務を処理するに当たっては、コンテンツの取込持出時の検疫方法と取扱手順を事前に定めておくこと。

（パスワードの管理）

第８　乙は、この契約による事務を処理するに当たっては、本遵守事項の第２の対象となる機器等には安全なパスワードを設定することとし、定期的に変更すること。また、不要なアカウントを登録しないこと。

（コンテンツ等の管理）

第９　乙は、Web サーバやデータベースサーバ等、コンテンツや情報等を格納するディレクトリやファイルに対しては適正なアクセス権限を設定すること。

２　乙は、この契約による事務を処理するに当たり、下記の対策を講じること

① 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脆弱性への対策を講じること。

② 不要なページやウェブサイトを公開しないこと。

③ 不要なエラーメッセージを返さないこと。

④ 不要なサービスやアプリケーションを起動させないこと。

（セキュリティポリシー）

第１０　乙は、この契約による事務を処理するに当たり、セキュリティポリシーを策定すること。ただし、既にセキュリティポリシーを定めている場合はこの限りではない。

２　乙は、この契約による事務を処理するに当たり、不正侵入やウイルス感染が発生した場合の対応方法を策定しておくこと。ただし、既にこれらの対応方法を定めている場合はこの限りでない。

（調査）

第１１　甲は、乙がこの契約による事務を処理するに当たり、本遵守事項に定める各事項の状況について、随時調査することができるものとする。

注　甲は委託者である和歌山県を、乙は受託者を指す。

# 外部サービス要件確認表（機密性2以上）

（別紙1）

| 外部サービス名称 | | | 記入日 | | | |
|---|---|---|---|---|---|---|
| 外部サービス提供者名称 | | | 記入者 | | | |
| 区分 | | 要件 | 取扱情報が機密性2以上の場合 | | | |
| | | | 要否 | 適用状況 | 備考 | |
| 1.外部サービス要件（機密性2以上） | | | | | | |
| 1.1. | セキュリティ評価制度 | 利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））への登録が行われていること。 | 任意 | | | |
| | | 1.1でISMAPへの登録が行われていない場合 | | | | |
| 1.2. | | 利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度「ISMAP-LIU」（ISMAP for Low-Impact Use）への登録が行われていること。 | 任意 | | | |
| 1.3. | SLA | サービスレベルの保証が定められていること。<br>SLAには以下の内容が定められていること。<br>・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順及び情報セキュリティインシデントの対応等の取り決め<br>・外部サービス利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得、保持し、定期的にレビューできること。<br>・利用する外部サービス又はシステムの技術的脆弱性に関する情報は、公表された後に速やかにクラウドサービス利用者が入手できるようになっていること。 | 任意 | | | |
| 1.4. | 生成AIを利用したサービスにおける入力情報の取扱 | 外部サービスが生成AIを利用したサービスに該当する場合においては、同サービスへの入力情報が、県の許可なく生成AIの学習に用いられたり、サービスを提供する事業者による監査の対象にならないことが確認できること。 | 必須 | | | |
| 1.1.でISMAPへの登録が行われている場合、1.2.でISMAP-LIUへの登録が行われている場合、以下の要件は不要 | | | | | | |
| 1.5. | 資格・認証<br>※アプリケーション提供事業者のみ | サービス提供を行う組織が、ISO/IEC 27001認証を取得していること。 | 任意 | | | |
| 1.6. | 資格・認証<br>※クラウドサービスプロバイダー<br>（外部サービスを構成する基盤部分について記入すること） | サービス提供を行う組織が、ISO/IEC 27001認証を取得していること。 | 必須 | | | |
| 1.7. | | サービス提供を行う組織が、ISO/IEC 27017認証もしくはPCI DSSを取得していること。 | 必須 | | | |
| 1.8. | | サービス提供を行う組織が、ISO/IEC 27018認証を取得していること。 | 任意 | | | |
| 1.9. | データの所在・適用法と裁判管轄 | サービス上のユーザ所有データ（バックアップデータを含む。）の所在地が日本国内に限定できること。 | 必須 | | | |
| 1.10. | | サービス提供事業の実施場所（事務所、運用場所）（地域（リージョン）が特定できるようにすること）を情報提供すること。提供にあたっては文書にて内容を確約すること。 | 必須 | | | |
| 1.11. | | 準拠法、裁判管轄を国内に指定できること。 | 必須 | | | |
| 1.12. | | 県が登録したデータは、県に確実に提供でき、提供後のデータの所有権・管理権は、県が保有すること。また、県が登録したデータは、本契約に明示的に定められているところを除き、県の承諾なく、利用できないものとすること。 | 必須 | | | |
| 1.13. | データセンター要件 | データセンターは、日本データセンター協会が制定するデータセンターファシリティスタンダードのティア3相当の基準を満たした設備とすること。 | 必須 | | | |
| 1.5 及び 1.7の認証を取得している場合、以下の要件は不要　※以上の要件を満たせない場合は、以下の各要件について根拠資料等を提出させる等、入念な審査を行う。 | | | | | | |
| 1.14. | セキュリティ対策・体制 | サービス提供業務の遂行のために提供する情報（契約等の手続に付随して外部サービス事業者が知りうる利用者情報等）を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守（義務）の表明をすること。 | 必須 | | | |
| 1.15. | | サービス提供を行う組織若しくはその従業員、再委託先又はその他の者によって、県の意図しない変更が加えられないための管理体制について提示すること。 | 必須 | | | |
| 1.16. | | 情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について提示すること。 | 必須 | | | |
| 1.17. | | 障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示すること。 | 必須 | | | |
| 1.18. | データ暗号化 | 機密性の高いデータ等については、暗号化等によって蓄積・伝送データを保護できること。 | 必須 | | | |
| 1.19. | ログ取得 | 外部サービス上におけるアクセスログ等の証跡に係る保存期間について、1年間以上の保存が可能であること。その手法について提示すること。 | 必須 | | | |
| 1.20. | 脆弱性対策 | 外部サービス上の脆弱性を発見する方法があり、実施可能であること。その手法について提示すること。 | 必須 | | | |
| 1.21. | 不正アクセス対策 | 通信内容を監視する等により、不正アクセスや不正侵入を検知及び通知できること。 | 必須 | | | |
| 1.22. | 機器停止 | 機器に異常があった場合、検知できること。<br>また、機器を死活監視し、停止した場合、検知できること。 | 必須 | | | |
| 1.23. | データ取扱い時の権限管理 | データの取り扱いについて、権限管理及びアクセス制御ができること。 | 必須 | | | |
| 1.24. | 保守端末 | 保守端末は、認証管理、持出管理、施錠管理、ログ管理等によりセキュリティを確保していること。 | 必須 | | | |
| 1.25. | データ消去 | データを消去する際は、ISO27001に準拠してデータを復元できないように電子的に完全に消去又は廃棄すること。また、データを消去又は廃棄した証明書を提示すること。<br>なお、ISO27001にデータ消去が未規定の場合、サービス終了までに規定し、認証を受けること。 | 必須 | | | |
| 1.26. | セキュリティ監査 | 情報セキュリティ監査の受入れが行われていること。 | 任意 | | | |
| 1.27. | セキュリティ教育 | 情報セキュリティ意識の向上を図るための教育を実施する計画が策定され、その実施体制が整備されていること。 | 必須 | | | |