

デジタル庁におけるガバメントクラウド等の整備
のためのクラウドサービスの提供
- 令和8年度募集 -

調達仕様書

デジタル庁

1 調達件名

デジタル庁におけるガバメントクラウド等の整備のためのクラウドサービスの提供
- 令和8年度募集 - (以下「本調達」という。)

2 調達の背景

デジタル改革基本方針において、デジタル社会の目指すビジョンとして「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」を掲げ、このような社会を目指すことは「誰一人取り残されない、人に優しいデジタル化」を進めることに繋がるとしている。

また、デジタル社会の形成に向けた基本的な施策として、政府情報システムについて、共通的な基盤・機能を提供する複数のクラウドサービス (IaaS、PaaS、SaaS) の利用環境であるガバメントクラウドを整備することとされている。

上記の方針等を踏まえ、デジタル庁ではガバメントクラウド整備事業を進めており、令和3年度から利用を開始しているところである。

3 目的等

ガバメントクラウド整備事業については、Amazon Web Services (AWS)、Google Cloud (GC)、Microsoft Azure (Azure) 及びOracle Cloud Infrastructure (OCI) の利用が開始されており、令和5年度において、さくらのクラウド (さくらインターネット) が条件付きで採択され、令和8年度からの利用開始に向けて整備を進めているところである。

令和8年度以降、各府省庁、地方公共団体、独立行政法人等及び公共情報システムを運営する民間事業者において、ガバメントクラウドの利用がさらに進むことから、引き続きガバメントクラウドの要件を満たすクラウドサービスを募集する。

4 事業の内容

令和8年度以降も継続したガバメントクラウド利用を見込んでおり、安定したクラウド環境の提供のために最長で5年の長期契約を行う。その間、各府省庁、地方公共団体、独立行政法人等及び公共情報システムを運営する民間事業者が、ガバメントクラウドとして契約されたクラウドサービスを選択して利用できるクラウド環境を提供する。

また、生成AIを初めとするAI関連サービスも契約したクラウドサービスとしてそのガバナンスの範囲内で利用できるようにし、サービスとして提供していく。

ガバメントクラウドでは情報資産は日本国内に保管されることとしているが、最新の生成AIモデルが国外でのみ利用でき、利用者がその利用を希望するケースがあって、この対応が必要と判断する場合には、ガバメントクラウドとして契約されたクラウドサービスにおいて、国外での生成AI利用を可能にする環境として「国外AI推論環境」を用意し対応できるようにする。その際、ガバメントクラウド自体とは完全に管理範囲を分離して、AI推論とその関連機能のみを実行可能とする別のクラウド環境として提供する。

5 提案形態

1社による提案に加えて、複数社のクラウドサービスなどを組み合わせてガバメントクラウドとして提供する共同提案も可能である。

共同提案の場合には、以下を満たす必要がある点に留意する。

- ・ 共同提案するクラウドサービス毎の事業者名を記載した一覧の提出
- ・ 技術的ガバナンス、課金・決済及び不具合発生時の最終責任等は、統括する主幹事業者が対応する
- ・ 主幹事業者は、後述する項6(1)及び(2)の全てのサービスを提供する
- ・ 主幹事業者以外の事業者が提供可能なサービスは後述する項6(3)に限る
- ・ 共同提案の場合、全ての事業者は政府情報システムのためのセキュリティ評価制度である ISMAP[※]クラウドサービスリストに登録されていることを条件とする
- ・ 共同提案を行う場合は、共同提案全事業者による共同提案に関する協定書を作成し、提案時にその写しを提出すること
- ・ 共同提案に関する協定書には主幹事業者の指定、共同提案における責任の分担、経費の配分割合が必ず記載されていること
- ・ 共同提案の場合、デジタル庁と共同提案全事業者による連名契約とする

※ 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））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度

6 ガバメントクラウドの調達範囲

本調達の範囲は、クラウドサービス及びこれに関連するサービスであり、概要は以下のとおりである。

(1) 基本事項

提供するクラウドサービスにおいては、外部からの不正アクセスや意図しない情報漏洩を未然に防止できるよう、政府情報システムのためのセキュリティ評価制度である ISMAP クラウドサービスリストに登録されたクラウドサービスを条件とするなど別紙1 技術要件詳細「基本事項」を満たすこととする。

(2) サービス要件（基本）

提供するクラウドサービスにおいては、クラウドサービスに必要な基本的なサービスを自社で開発、運用してこれを提供することを求めており、これに必要な機能要件として、別紙2 技術要件詳細「サービス要件（基本）」を満たすこととする。

(3) サービス要件（データ連携や高度なセキュリティ等）

データ連携やデータ分析に関する機能群や、高度なセキュリティを実現する機能群については、サードパーティ製ソフトウェア、ハードウェア及びサービス（以下「サードパーティ製品」という。）を用いてその機能を提供することも許容する。その機能要件としては、別紙3 技術要件詳細「サービス要件（データ連携や高度なセキュリティ等）」を満たすこととする。

また、その場合には、クラウドサービスにおける情報セキュリティのサプライチェーンリスク防止の観点から、当該サードパーティ製品に対する第三者監査を実施し、当該監査の報告書を提出するとともに、サードパーティ製品に起因する不具合等も含め、自社のクラウドサービスが提供するものとして責任を負うこと。なお、この場合、当該サードパーティ製品に関する製品情報（製品名や製造企業等）の一覧を提出する。

サードパーティ製品を自社のクラウドサービスが提供するものとして責任を負うこととして必要な要件は次のとおりとする

- ・ ガバメントクラウド利用者が当該サードパーティ製品の利用にあたって、別途契約行為等が発生しないこと（デジタル庁と当該サードパーティ製品を用いて提供を行う事業者間の契約手続きのみで、ガバメントクラウド利用者の利用が可能であること）
- ・ ガバメントクラウド利用者からのサードパーティ製品利用に伴う利用料等の支払いは、当該サードパーティ製品を用いて提供を行う事業者のクラウドサービス利用料等の支払いの中で一括して行うこと
- ・ サードパーティ製品の利用などに関する問い合わせ等サポートは当該サードパーティ製品を用いて提供を行う事業者のサポートを通して提供できること
- ・ サードパーティ製品のユーザ認証（シングルサインオン）は当該サードパーティ製品を用いて提供を行う事業者のサービスと同じく、ガバメントクラウドが用意する認証と連携できること

(4) 猶予期間

ア 生成 AI 機能に係る 6 項目を除く技術要件 305 項目について

別紙 3 技術要件詳細「サービス要件（データ連携や高度なセキュリティ等）」に定める生成 AI 機能に係る 6 項目（項番 74～79）を除く技術要件 305 項目を満たしていない場合は、次のとおり取り扱うこととする。

- ・ 令和 8 年 9 月末までに全要件を満たす計画を提出し、デジタル庁がガバメントクラウド対象となるクラウドサービスに加わることが可能と判断した場合には、ガバメントクラウドとして契約する
- ・ ただし、令和 8 年 9 月末までに全要件を満たすことができないとデジタル庁が判断した時点で、直ちにガバメントクラウドとしての契約を解除する
- ・ 契約解除により生じる国及び地方公共団体等のシステムのガバメントクラウド移行に関する諸経費について、当該機関に経済的負担が生じることのないよう対応すること

イ 生成 AI 機能に係る 6 項目について

別紙 3 技術要件詳細「サービス要件（データ連携や高度なセキュリティ等）」に定める生成 AI 機能に係る 6 項目（項番 74～79）について、提案時点で ISMAP 対象の言明範囲外の場合は、次のとおり取り扱うこととする。

- ・ 令和 10 年 3 月末までに生成 AI 機能（項番 74～79）を ISMAP 対象言明範囲に含め更新されること

- ・ ISMAP 対象言明範囲に含め更新されるまでの間、生成 AI 機能（項番 74～79）に係るサービスの提供はできない
- ・ 令和 10 年 3 月末までに ISMAP 対象言明範囲に含め更新できなかった場合は契約を解除する

ウ 合意書の締結

アの全要件を令和 8 年 9 月末までに、イの全要件を令和 10 年 3 月末までに満たすこととして契約する場合は、デジタル庁と別添 5「合意書」を締結する。

(5) ガバメントクラウドとして利用する国内のデータセンターにおいて、以下の取組を実施していること及び当該取組の実績を証する書類を提出すること。

- ・ 電力利用料削減の取り組みを過去 3 年以上実施していること。
- ・ 再生可能エネルギーへの取り組みを過去 3 年以上実施していること。

(6) 付随作業

クラウドサービスを利用するに当たって、付随する関連サービスの提供を行う。

7 国外 AI 推論環境の調達範囲

国や地方公共団体において最新の生成 AI の利用を希望するケースがあることから、ガバメントクラウドと同等のセキュリティ対策などの統制を講じたうえで最新の生成 AI モデルを利用する環境の実現可能性について調査を行うこととしている。

具体的には、本調達においてガバメントクラウドに加えて当該調査環境の提供を希望する事業者については、今回の仕様書に記載する以下の要件を満たした上で別途契約を締結することを前提に、試験的に最新の生成 AI モデルの利用環境を提供することについて提案できることとする。

(1) 基本事項

提供するクラウドサービスにおいては、外部からの不正アクセスや意図しない情報漏洩を未然に防止できるよう、別紙 1 技術要件詳細「基本事項」を満たすこととする。

ただし、国内でのデータ保管を規定した、別紙 1 技術要件詳細「基本事項」項番 8、10～12、15 は除く。

(2) サービス要件（基本）

別紙 2 技術要件詳細「サービス要件（基本）」のうち、ネットワーク（項番 81～96）、モニタリング機能（項番 97～114）、リソース作成・管理機能（項番 115～117）、アクティビティ追跡機能（項番 118～122）、コスト・運用最適化支援（項番 123～127）、ユーザ管理（項番 130～138）を満たすこと。

(3) サービス要件（データ連携や高度なセキュリティ等）

別紙 3 技術要件詳細「サービス要件（データ連携や高度なセキュリティ等）」のうち、生成 AI 機能（項番 74～79）を満たすこと。

国外 AI 推論環境では、ガバメントクラウド自体とは完全に管理範囲を分離して、国外での最新の生成 AI モデルの利用を可能にする。

具体的には、基本契約とシングルサインオンによる認証（別紙1 技術要件詳細「基本事項」の項番 41～42）はガバメントクラウドと同じとし、環境自体、環境への設定（テンプレート）、管理権限とユーザ、管理画面、ログ管理、支払い等をガバメントクラウドと分離して管理できるようにする。また、国外で利用できるようにする生成 AI モデルとそのサービスでは、推論の実行はできるが情報資産の永続的な保管はできないこととする。

(4) 付随作業

クラウドサービスを利用するに当たって、付随する関連サービスの提供を行う。

8 契約期間

クラウドサービスを提供する事業者が、電気通信事業法第 9 条の登録又は同法第 16 条第 1 項の届出を行っている場合、本調達の契約期間は、契約締結日から最長で令和 13 年 3 月 31 日までとする。なお、これ以外の者における本調達の契約期間は、契約締結日から令和 9 年 3 月 31 日までとする。

9 個別契約の締結

クラウドサービスを提供するに当たっての詳細な条件は、デジタル庁と締結する「クラウドサービス基本契約書」に準拠して締結される「個別契約」において定めるものとする。

10 実績レポートの提出

(1) クラウドサービスを提供する事業者は、毎月の利用量及び利用料金の確定後、前月分の利用実績を提出するものとする。

(2) 実績レポートの内容及び提出時期は、個別契約において定めるものとする。

※ 本番環境での予定利用量を「別紙 4_クラウドサービスの整備に係るクラウド予定利用量」に示す。
なお、予定利用量は、調達仕様書作成時での想定量を示しており、確定した利用量ではない。

11 クラウドサービスの利用におけるセキュリティ対策

(1) 原則、準拠法については日本法とし、国際裁判管轄は東京地方裁判所とすること。

(2) クラウドサービスの廃止、サービス内容の変更等に伴い契約を終了する場合は、他のクラウドサービス等に円滑に移行できるよう、原則、1 年以上の期間をもって事前にデジタル庁へ通知すること。なお、1 年に満たない場合には、クラウドサービス上で稼動する情報システムの移行期間を考慮した対策方法を提示し、デジタル庁と協議すること。

(3) クラウドサービスの契約を終了する場合、クラウドサービス上に保存されたデータについて、汎用性のあるデータ形式に変換して提供するとともに、クラウドサービス上において復元できないよう抹消し、その結果をデジタル庁に書面で報告すること。なお、実施方法等の詳細については、デジタル庁と協議するものとする。

(4) クラウドサービスに係るアクセスログ等の証跡を保存し、デジタル庁からの要求

- があった場合は提供すること。なお、証跡は1年間以上保存することが望ましい。
- (5) インターネット回線とクラウド基盤との接続点の通信を監視すること。
 - (6) クラウドサービスにおける脆弱性対策の実施内容をデジタル庁が確認できること。
 - (7) クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切り替え等の対策が講じられていること。また、クラウドサービスに障害が発生した場合の復旧時点目標（RPO）等の指標を提示すること。なお、データセンターは地理的に離れた日本国内の複数の地域（例えば、関東と関西、北海道と関東、関西と九州など）に設置するなどの大規模地震や電力供給障害を想定した災害対策が講じられていること。
 - (8) クラウドサービス上で取り扱う情報について、機密性、完全性及び可用性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。
 - (9) クラウドサービスの利用者が、自らの意思によりクラウドサービス上で取り扱う情報を確実に抹消できること。
 - (10) 本業務において、クラウドサービスに係る情報について、業務開始時に開示項目や範囲を明記した資料を提出すること。
 - (11) 主管元に対して、クラウドサービスに係る機密性の高い情報を開示する場合は、主管元において、当該情報を審査又は本業務以外の目的で利用しないよう適切に取り扱うため、必要に応じて当該情報に取扱制限を明記するなどの措置を講じること。
 - (12) ISO/IEC27001 又はそれに基づく認証を取得していること。また、当該認証の証明書等の写しを提出すること。
 - (13) ISO/IEC27018 もしくはそれに基づく認証を取得していること。又は、同等の取扱いを行うこと。
 - (14) クラウドサービスの情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。もしくは、同等の実績を有することを示すこと。
 - ・ ISO/IEC27017 又は ISMS クラウドセキュリティ認証制度に基づく認証
 - ・ セキュリティに係る内部統制の保証報告書（SOC 報告書（Service Organization Control Report））
 - ・ 第三者監査人による情報セキュリティ監査により対策の有効性が適切であることを証明する報告書（クラウド情報セキュリティ監査制度に基づく CS マークが付された CS 証明書等）
 - (15) クラウドサービスのサプライチェーンリスクへの対応として、NIST SP800-53 rev4 又は相当以上の規格に対応する監査フレームワークに対応し、第三者監査人により適切であると説明された報告書等を示すこと。

12 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。
- (3) 基本契約書第2条及び第3条に基づき、本調達に伴い契約を行う際に必要となる

契約書等の構造を示す資料を提示すること。

資料はデジタル庁との間で締結する基本契約書を起点に、本調達により必要となる個別契約書、約款等が構造的に整理されていること。

ただし、具体的な契約名称などの記載は不要であるため、資料上個別契約書などが分かる記載とすること。