

デジタル庁におけるガバメントクラウド整備  
のためのクラウドサービスの提供  
-令和5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整備のためのクラウドサービスの提供-令和5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、令和3年度から契約している Amazon Web Services（AWS）及びGoogle Cloud（GC）が地方公共団体の先行事業等として利用されており、令和5年度も事業が継続されている。

また、令和4年度に新たに加わった Oracle Cloud Infrastructure（OCI）及びMicrosoft Azure（Azure）については、ガバメントクラウドとして利用するためのアカウント管理や利用者向けマニュアルの作成等、検証作業を実施しており、令和5年度中に利用が開始されることとなっている。

令和5年度以降、各府省庁等及び地方公共団体においてガバメントクラウドへの移行が本格化することから、令和5年度も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5年度におけるガバメントクラウド利用者は以下を見込んでおり、これら利用者がガバメントクラウドとして利用できるようクラウドサービス及びこれに関連するサービスを提供する。

- ① 地方公共団体の情報システム
- ② 各府省庁等が所管する情報システム
- ③ デジタル庁が調達又は認めた国や地方公共団体等の利用に供する SaaS

## 5 調達の範囲

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) 基本事項及びマネージドサービス

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 Information system Security Management and Assessment Program (以下、「ISMAP」という。)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\_基本事項及びマネージドサービスの技術要件詳細」を満たすこととする。

なお、以下の条件に該当する場合は、「別紙1\_基本事項及びマネージドサービスの技術要件詳細」を満たすことを証明する書類等に具体的に記載すること。

- ① 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の場合には、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を提出する。また、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、統括する主幹事事業者が対応すること。なお、この場合、全ての事業者は ISMAP 取得を条件とする。
- ② 自社のクラウドサービスに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、「サードパーティ製ソフトウェア等」という。)を用いてガバメントクラウドとして提供する場合には、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ソフトウェア等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、サードパーティ製ソフトウェア等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ソフトウェア等に関する製品情報 (製品名や製造企業等) の一覧を提出する。
- ③ 現状、「別紙1\_基本事項及びマネージドサービスの技術要件詳細」に記載する要件を満たすことが出来ないが、2025年度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整備事業に係る検証作業等に参加することができるものとする。なお、2025年度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に関する検証作業等の参加資格の対象から除外する。これ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。

本項により、ガバメントクラウド整備事業に係る検証作業等に参加が認められた事業者は、デジタル庁と別紙2「覚書」を締結するものとする。

- ④ 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。

## (2) 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。

## 6 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、本調達の実行期間は、契約締結日から令和8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6年3月31日までとする。

## 7 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。

## 8 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3\_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。

## 9 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働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、機密性及び完全性を確保するため

- 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。

## 10 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。

## 11 連絡先

本調達の仕様書、「別紙 1\_基本事項及びマネージドサービスの技術要件詳細」及び「別紙 2\_クラウドサービスの整備に係るクラウド予定利用量」に関する問い合わせについては、次の連絡先までメールにてお問合せ下さい。

なお、問合せ期間については、公告期間終了までとし、解釈や考え方などの問合せについては、公平性を期すため、デジタル庁のホームページで公表する。

mail : [government-cloud@digital.go.jp](mailto:government-cloud@digital.go.jp)

デジタル庁省庁業務サービスグループガバメントクラウド担当宛