別紙７

ガバメントクラウド運用管理補助者業務
仕様書（運用保守）

令和８年９月

奈良市

総合政策部 DX 推進課

内容

1. 目的

本市がガバメントクラウドを利用するにあたり、「地方公共団体標準準拠システムのガバメントクラウドの利用について」に基づいたガバメントクラウド環境の運用管理等を行い、別途契約の「申請管理システム構築業務委託契約」（以下、「構築契約」とする。）にて構築した申請管理システム（以下、「本システム」とする。）を安定稼働させ、継続的な改善を実施することを目的とする。

2. 全体概要

本市が採用するCloud Service Provider（以下「CSP」という。）は「AWS」とし、本業務におけるガバメントクラウド運用管理補助者（以下「補助者」という。）の管理範囲は、本システムの利用アカウント内とする。なお、別紙 6「申請管理システム運用保守業務仕様書」にも一部補助者業務を含んでいることに留意すること。

3. 利用権限付与

本市は、デジタル庁より付与されたクラウドサービス等の利用権限について、本業務に係る全部又は一部を、補助者に対し、本業務の遂行のために付与する。

4. 補助者の利用上の義務

・補助者は、奈良市個人情報取扱特記事項 第３条の作業責任者等の届出の通り、本業務の遂行を担当する作業責任者及び作業従事者を指定し、本業務開始前に本市に対し報告する。補助者は、事前に奈良市個人情報取扱特記事項添付の作業責任者等変更報告書（様式第２号）により本市に報告しなければならない。

・補助者は、前項の担当者以外の者にクラウドサービス等を利用、運用管理をさせてはならない。

・補助者は、担当者を含む補助者の作業責任者及び作業従事者の行為により本市に対して損害が生じた場合、損害を賠償する責任を負う。

5. ガバメントクラウド利用方針

・利用方式

構築契約にて決定した利用方式とする。

・利用アカウント

補助者は運用管理に必要となるガバメントクラウド環境の運用管理アカウント及び本番アカウント（ネットワーク管理）の利用権限が付与される。ガバメントクラウドの方針により各環境への接続時には多要素認証（以下「MFA」という。）が必須であり、本番環境及び本番相当環境のアカウントにアクセスする場合は、その MFA はハードウェアデバイスを用いたものでなければならない。また、CSP 環境の管理インターフェースへのシングルサインオン（SSO）に際して、アクセス元制御を実施するため、CEP ライセンスが必要となる。

・ロケーション

東京リージョンをメインサイトとし、大阪リージョンをバックアップサイトとする。

6. ガバメントクラウド運用管理補助業務

ガバメントクラウド運用管理補助業務を以下に記載する。なお、追加で対応が必要な業務が発生した場合（デジタル庁からガバメントクラウド運用管理補助者が実施すべき業務について通知があった場合等）についても対応を実施すること。

6.1 運用管理機能に係る運用・保守業務

6.1.1 ガバメントクラウド構成情報の提出

運用保守契約締結後、各年度の開示時までに補助者は以下の情報を本市に提示すること。

- 利用年度のクラウドサービス利用料（USD 建て）
- CSP 料金見積りツールによる計算結果を保存した URL
- 環境構成図

なお、デジタル庁がガバメントクラウドに関する情報提供や問い合わせ窓口として整備している GCAS（Government Cloud Assistant Service）を利用する場合、GCAS の利用に必要な作業を行うこと。

6.1.2　ユーザー管理

補助者は運用管理アカウントに関するユーザー及びその権限の管理を行うこと。なお、GCAS アカウントによる各 CSP 環境への SSO が可能になるため、CSP 環境内でユーザーアカウント作成は禁止されている。利用しているユーザー情報に変更（追加・更新・削除等）が生じた場合は GCAS ガイドを参照し適宜対応を行うこと。また、ユーザーに適用している権限設定についても定期的に見直し、適切な権限管理を行うこと。

6.1.3　CEP ライセンス管理

補助者は CSP 環境の管理インターフェースへの SSO に際して、アクセス元制御を実施するため、Google 社が提供する Chrome Enterprise Premium（CEP）に関して、補助者必要数分の把握、GCAS アカウント紐づけ作業及びライセンス管理を実施すること。詳細な作業内容については、GCAS ガイド「ガバメントクラウド手続き概要（全編）」を参照すること。

6.1.4　費用按分情報の登録

共同利用方式を採用しているアカウントに関する費用按分情報の登録を補助者にて実施すること。

6.1.5　必須適用テンプレートの適用

必須適用テンプレートにより、予防的統制や発見的統制、セキュリティ監視情報収集の設定等、ガバナンスに関する設定が適用される。補助者は環境構築後においても、定期的にテンプレート適用更新が必要になるため、GCAS ガイド等で案内された手順に従い対応すること。

6.1.6　補助者環境からの接続

補助者が管理する拠点からガバメントクラウドへの接続は、本市の定める情報セキュリティポリシーに従うこと。また、運用開始後リモートでの保守を実施する場合は、補助者にて以下の「表 1 リモート保守におけるセキュリティ要件」を満たす環境を整備すること。ただし、以下に挙げる要件と補助者における実装に差異がある場合には、代替案を提示のうえ、協議により対応方法を決定すること。なお、運用保守契約締結後、表 1 に関連するチェックリストを本市より提示するため、その要件についても満たすこと。

表１リモート保守におけるセキュリティ要件

項番	区分	要件内容
1	不正アクセス対策 ※項番５～８は、構築するシステムの環境に合わせて記載すること	保守拠点から保守環境へは専用回線（閉域網）で接続すること。
2		保守端末のネットワークと保守拠点内のその他のネットワークを分離すること。
3		保守端末とインターネットの通信は必要最小限に限定すること。
4		保守環境へアクセス可能な端末を限定し、専用の保守端末（以下、保守端末）とすること。
5		保守拠点から奈良市庁内 NW への通信制御を実施する。
6		保守拠点から管理基盤環境へ直接接続することを禁止する。
7		保守拠点から奈良市庁内 NW に構築されているシステム・データ環境へ直接接続することを禁止する。
8		保守拠点からガバメントクラウドに構築されているシステム・データ環境へ直接接続することを禁止する。
9	不正操作対策	操作履歴などのログを取得すること。
10		取得した操作履歴などのログから、不正ログがないか定期的に点検すること。
11		保守端末へのログインは必要なユーザーに限定し、必要最小限の操作権限を付与すること。
12		離席の際など一定時間端末を操作しないときには、端末のロックを行うこと。
13		保守端末へログインする際は、多要素認証を行うこと。
14		保守拠点での作業時には、専用スペースで実施すること。
15		保守端末および保守環境へログインするための ID/パスワードの使いまわしは禁止する。
16		保守環境への接続は必要な場合のみ行うこと。
17		保守人員（再委託、再々委託含む）に対し、定期的な教育を実施すること。
18	高負荷攻撃対策	DDoS 攻撃等の対策を実施すること。
19	通信データ改ざん対策	通信の暗号化を実施すること。
20	物理的侵入対策	保守端末は保守拠点に設置し、持ち出しは禁止すること。
21		保守拠点へは、許可されていない機器の持込みを禁止すること。
22		保守拠点への不正侵入（関係者以外の入室、共連れ入室など）を防止すること。
23		取得した監視カメラや入退室の記録から、不正侵入がないか定期的に点検すること。
24	その他	保守端末からインターネットへの接続先は必要最小限に限定すること。
25		保守端末へ USB メモリ等の電磁記録媒体の接続は禁止する。
26		保守業務に関係のないソフトウェアの使用を制限すること。

27		保守端末の OS、ウイルス対策のバージョンは常に最新とすること。
28		保守端末に対する脅威の発生または事前の兆候を自動で検知し通知できるようにすること。
29		保守端末に対する脅威の発生または事前の兆候を自動で検知した場合、速やかに状況調査を実施すること。

6.1.7　長期継続割引の検討・実施

補助者は長期継続割引の購入検討に係る助言及び作業等を実施すること。

6.1.8　性能・キャパシティ管理・コスト管理

・補助者が運用保守する領域のリソースの利用料金及び稼働実績（vCPU 利用率・ストレージ使用量・通信量、ログ等）を収集、分析を行うこと。情報の収集、分析は、CSP の管理コンソールやデジタル庁から提供されるガバメントクラウドテンプレートを基に、補助者にてツール（ダッシュボード等）を活用して、人的対応を最小化した効率的な運用を実施すること。

・補助者はアカウントごとに月ごとの予算額を閾値として設定し、超過した場合等にメール等でアラートを発報できるようにしコスト管理を行うこと。

・補助者は継続的に性能やキャパシティ等の見直しを実施すること。