

(別紙6) ガバメントクラウド運用保守要件

1 アカウント管理

ガバメントクラウドを継続して利用するために必要となる資料（C S P 料金見積りツールにより試算した次年度のクラウドサービス利用料及び試算結果を保存したURL等）を提供すること。また、本市がデジタル庁から利用情報等の報告を求められた場合には、報告事項に係る情報を提供する等、本市の資料作成を支援すること。

2 ネットワーク接続管理

必要に応じて、共同利用領域内におけるネットワーク通信／ゲートウェイ等のパラメータ変更及びDNSの設定変更を行うこと。

なお、設定の変更前に本市の承認を受けるとともに、変更後には疎通テスト等を実施し、その結果を本市に報告すること。

3 システム監視

次期システム構築事業者が提供するサービスを対象にガバメントクラウド領域の監視を常時行うこと。なお、死活監視に加え、リソースの利用状況やスループット等のパフォーマンスの状況も監視すること。

また、障害発生を検知した際には、自動で障害状況等を通知できる仕組みを設けること。

4 イベント・ジョブ管理

次期システム構築事業者は、ガバメントクラウド領域のバックアップ等のイベント・ジョブのスケジュールを管理すること。なお、ジョブ実行・終了に係る異常発生時には、一時切り分け、本市へのエスカレーションを速やかに実施すること。

5 障害対応

ガバメントクラウド領域に障害（セキュリティに関するアラートやインシデントへの措置を含む）が発生している場合は、速やかに復旧に取り組むとともに、本市に障害発生状況や復旧の状況等を通知すること。障害対応に伴い、必要に応じて広島市ガバメントクラウド運用管理補助者に連絡を行うこと。

本市からの障害連絡またはシステム監視の自動発報等により障害を検知した場合は、速やかに障害対応を実施すること。

ただし、人的な障害対応が発生することを前提としつつも、次期システム構築事業者が構築する範囲は、マネージドサービスを活用し自動で切り替え・縮退等を行うことにより、可能な限り人的対応を必要としない設計・構築を基本とする。

なお、クラウド全体の停止など大規模障害の発生時には、例外的な対応が必要となることもあるため、対応に関して本市との協議に応じること。

6 セキュリティ管理

次期システム構築事業者は、本業務の実施にあたり、セキュリティリスクを低減させるための指針の策定及び予防対策等を実施すること。

7 性能・キャパシティ管理・コスト管理

次期システム構築事業者が運用保守する領域のリソースの使用料金及び稼働実績（vCPU利用率・ストレージ使用料・通信量等）を収集、整理し、運用・保守定期報告会において本市へ報告すること。広島市ガバメントクラウド運用管理補助者においても、共同利用方式システム領域の使用料金及び稼働実績を管理し、本市へ報告することになっているため、整理した情報は広島市ガバメントクラウド運用管理補助者へも提供すること。なお、情報の収集、整理は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、次期システム構築事業者にてツール（ダッシュボード等）を整備、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。

報告の中では、システム（ネットワーク、サーバ、サービス）ごとの内訳を明確にするとともに、CSPが提供するアドバイザーツールやデジタル庁から提供されるGCAS（Government Cloud Assistant Service）から得られる情報等を参考に、その利用状況について第三者視点から評価を行うこと。

また、半年または1年に1回程度を目安に、数ヶ月単位での利用状況結果を分析して、システムの構成やコストが最適化されるよう改善提案を行うこと。

8 バックアップ・リストア管理

障害が発生した場合も、ガバメントクラウドがIaC等により迅速に復旧できることを前提として、バックアップ／リストアができる状態を確保すること。具体的な方法については、本市と次期システム構築事業者との協議の上決定する。なお、リージョン単位での長期の障害が発生している場合は、国内の別リージョンに同環境を構築することとする。同環境の迅速復旧を目的とするため、ネットワーク通信／ゲートウェイ等の都度、バックアップを取得すること。

9 ログ管理

次期システム構築事業者は、適切にログの収集・分析を行うこと。

10 保守・メンテナンス

ガバメントクラウドの維持の観点において、必要なメンテナンスを行うこと。メンテナンスはシステムが稼働していない時間帯またはシステム稼働に影響しないように実施すること。なお、次期システム構築事業者が維持する機能（ゲートウェイ等）のメンテナンスに加え、C S P等のメンテナンスにおいて、システム・業務に影響を及ぼす可能性がある場合は、事前に本市に報告すること。

保守・メンテナンスにおいては、システム構成のベストプラクティスを提案するツール（AWS Trusted Advisor等）を活用し、当該ツールが提案する推奨構成の内容を定期的に確認するとともに、その内容を十分に考慮して、設定変更等の必要なメンテナンスを実施すること。また、セキュリティに関するマネージドサービス（AWS Security Hub／Amazon GuardDuty等）を活用し、C S Pのベストプラクティスに従ったセキュリティ対策が実施されていることを確認するとともに、当該サービスからアラートが発砲された場合は、そのアラートの内容に従い、設定変更等の必要なメンテナンスを実施すること。

1 1 ドキュメント管理

サービスの設定変更等に伴い、必要なドキュメント（設計書等）の最新化を行うこと。

1 2 その他

C S Pのコンソール画面にAdminユーザとしてアクセスする場合は、ハードウェア方式の多要素認証（MFA）によるサインインをすること。多要素認証（MFA）をする場合に必要となるMFA認証デバイスは次期システム構築事業者にて必要数用意すること。