

(別紙1-3) ガバメントクラウド運用管理補助者\_構築要件一覧

ガバメントクラウド運用管理補助者_構築要件一覧						
項番	分類①	分類②	分類③	概要	運用管理補助者	ASP事業者
1	構築	運用 管理環境構築	ユーザ管理	ユーザ管理を行うこと。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
2			権限管理	権限管理を行うこと。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
3			ネットワーク設定	ガバメントクラウド領域全体のネットワーク設定を実施すること。 例えばAWSにおいては、VPC、Transit Gateway、ピアリング接続、PrivateLinkによるエンドポイント接続、Direct Connect Gatewayによるネットワーク接続サービスとの接続等。	○	—
4			セキュリティ設定	ガバメントクラウド領域全体のセキュリティ設定（アクセス制御）を行うこと。 ※アクセス制御の詳細は、発注者と協議の上で確定すること。	○	—
5			必須適用テンプレートの適用	必須適用テンプレートを用いて、セキュリティ/ガバナンス関連の設定を行うこと。	○	—
6			監視設定	領域全体のメトリクス監視設定、イベント監視設定、アラーム設定をすること。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
7			通知設定	ガバメントクラウド領域全体のアラートや稼働状況等について、必要に応じて通知を行うこと。 業務環境上に構築されるシステム毎の個別の通知は対象外とする。 通知先はガバメントクラウド運用管理補助者とASP事業者の両方に通知することを想定しているが、一次対応はASP事業者が担うものとし、ガバメントクラウド運用管理補助者は切り分けや対応の支援を実施すること。 ※通知先等の詳細は、発注者と協議の上で確定すること。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
8			ダッシュボード設定	ガバメントクラウド領域全体の稼働状況やアラート状況等をダッシュボードで管理すること。 ※ダッシュボードの詳細は、発注者と協議の上で確定すること。	—	○
9			証跡管理設定	ガバメントクラウド領域全体のクラウド上の操作について、証跡管理をすること。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
10			構成管理設定	ガバメントクラウド領域全体のリソースの変更履歴を管理すること。また、IaCと実際のリソース設定に乖離（ドリフト）があった場合の検知設定を行うこと。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
11			ベストプラクティスの確認と対応	ガバメントクラウド領域全体のコスト最適化/パフォーマンス/セキュリティ/耐障害性/サービス制限について、ベストプラクティスに準拠するための推奨事項を確認すること。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
12			セキュリティポリシー準拠状況の確認と対応	ガバメントクラウド領域全体のセキュリティポリシー準拠状況の確認をすること。 ・ダッシュボードでセキュリティコアの達成度を定期的にチェック ・検出された項目のステータス管理（抑制済み、解決済み等）	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
13			脆弱性管理設定	悪意のある操作や不正な動作を検知した場合、様々なログを調査し、潜在的なセキュリティ問題や不信なアクティビティを分析すること。	—	○
14			アクセス分析設定	リソースへのアクセスを分析し、適正をチェックすること。	—	○
15			ログ管理	証跡管理や構成管理等のログを集約して保管すること。	—	○
16			コスト管理	コスト管理すること。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
17			DNS管理	ガバメントクラウド領域全体のDNSを管理を行うこと。	○ (運用管理補助領域のみ)	○ (ASP領域のみ)
18			プライベートCA管理	ガバメントクラウド領域全体の証明書を管理を行うこと。 ※LGPKIの証明書利用も含めて、発注者と協議の上、方針を確定すること。	—	○
19			共通管理サーバ	共通管理サーバ（WSUSサーバ）を構築すること。（EC2で構築したサーバを管理するサーバ） Windows修正プログラム、Windows Defenderの定義ファイル等を管理し配信すること。 ※インターネットアクセスが必須となるため、総務省及びデジタル庁の各ガイドラインに準拠した環境を構築すること。	—	○
20			バックアップ環境の整備	庁内または別リージョンへのバックアップ環境を検討し整備をすること。 ※バックアップ要件については、発注者と協議の上で確定すること。	—	○
21			リモート保守環境の構築	コンソール接続、及び運用管理環境への接続環境を構築すること。 ※具体的な構成については発注者の承認をもって確定すること。	—	○
22	ASP 業務環境構築	ユーザ管理	業務アカウント内のユーザ管理を行うこと。	—	○	
23		権限管理	業務アカウント内の権限管理を行うこと。 また、制限付き権限移譲については、発注者と協議し、方針を確定した上でASP事業者と調整すること。	—	○	
24		必須適用テンプレートの適用	必須適用テンプレートを用いて、セキュリティ/ガバナンス関連の設定を行うこと。	—	○	
25		業務システム検証環境の構築	VPC、VNETの初期設定はガバメントクラウド運用管理補助者が実施する。 VPC初期設定以降の業務システム検証環境の構築は、ASP事業者が主体的に行い、ガバメントクラウド運用管理補助者はその支援を行う。	—	○	
26		業務システム本番環境の構築	VPC、VNETの初期設定はガバメントクラウド運用管理補助者が実施する。 VPC、VNET初期設定以降の業務システム本番環境の構築は、ASP事業者が主体的に行い、ガバメントクラウド運用管理補助者はその支援を行う。	—	○	
27		業務システムテンプレートの適用	ASP事業者が業務システム用のテンプレートを適用する。 ガバメントクラウド運用管理補助者は必要に応じて支援する。（テンプレート適用時のエラー対応支援等）	—	○	
28		インフラ設定監査	ASP事業者が実施したインフラに関する設定について、セキュリティ及びガバナンス上問題がないかチェックすること。	—	○	
29		共通管理サーバの利用	ガバメントクラウド運用管理補助者が作成する「ガバメントクラウド利用ガイドライン」を参照し、ASP事業者が共通管理サーバを利用する設定を実施する。 ガバメントクラウド運用管理補助者は、共通管理サーバ利用に関する支援をすること。	—	○	
30		バックアップ環境の整備	庁内または別リージョンへのバックアップについてASP事業者を支援すること。 ※バックアップ要件については、発注者と協議の上で確定すること。	—	○	
31		リモート保守環境の構築	コンソール接続、業務システムVPCへの接続環境を構築する。 構成については、庁内ネットワーク担当、ガバメントクラウド運用管理補助者、ASP事業者が協議し、発注者の承認をもって確定すること。	—	○	
32	ASP業務 環境構築 リハーサル	業務システム環境構築手順の確立	構築手順を確立しガバメントクラウド利用ガイドラインに反映すること。また、監視等の運用管理に必要な機能が正常に動作することを確認すること。	—	○	
33	ネットワーク接続	CSP-NSP間のネットワーク接続	CSP-NSP間のネットワーク接続環境について、NSP事業者と調整して構築すること。	○	○	
34		共同利用方式システムとの接続	共同利用方式で提供されるシステムとのネットワーク接続について対応すること。	○	○	
35	共通機能アカウント構築	AWS S3上のファイル連携用バケット等の作成	1 AWSのオブジェクトストレージ上に業務の組み合わせごとのバケットを作成すること。 2 オブジェクトストレージ上に作成されたバケットにおいて、ファイル連携を行うシステムの格納先（以下、「フォルダ」という。）を作成すること。 3 作成したフォルダの配下に、退避・移動ファイル履歴管理フォルダを作成すること。 4 申請管理機能からファイルを受け取る利用側業務システムのフォルダの配下に、手続き別フォルダを作成すること。手続き別フォルダの配下には、退避・移動ファイル履歴管理フォルダと申請ZIP別フォルダを作成すること。 5 バケット単位でアクセス権限付与を行うこと。（AWS上のIAMポリシー、バケットポリシー等で設定できる範囲で実施すること） 6 利用側業務システムが、退避・移動した連携ファイルと格納完了通知ファイルを日次処理30日分・月次処理3か月分・年次処理13か月間経過したファイルを自動的に削除すること。また、経過期間の変更が可能なこと。 7 オブジェクトストレージ自身の障害をAWS側で検知した場合は、メール発報等で検知できるように設定をすること。 8 オブジェクトストレージの使用状況を確認できるようにすること。 9 上記1-8の作業について、地方公共団体情報システムデータ要件・連携要件標準仕様書の構築時点の最新版に則ること。	—	—	