ガバメントクラウド環境構築業務仕様書

第１章　共同利用環境概要

第１条（業務概要）

本業務は、地方公共団体の標準化業務について、受託者のガバメントクラウド共同利用環境における運用管理補助サービスを提供するため、受託者が、Amazon Web Service（以下、AWS という。）にクラウド環境を構築する。

本業務は、受託者のサービス管理者が受託者標準構成に基づき本市の利用環境を構成する。

第２条（業務内容）

本業務の内容は以下の通りとする。

なお、本業務は AWS より提供される機能を使用し取得された情報を提供すること。

項番	業務内容
1	クラウドインフラの設計（権限管理含む）、構築
2	仮想サーバのウィルス対策及びセキュリティパッチの設定
3	セキュリティ対策
4	定期メンテナンス等のイベント管理設定
5	死活監視・エラー監視・リソース監視設定
6	インシデント管理設定
7	EC2 と RDS のバックアップとリストア設定 ※通常稼働リージョンとバックアップ格納リージョンを分ける
8	ネットワーク構成
9	クラウド環境の構築及びデジタル庁から提供されるテンプレートの適用
10	ガバメントクラウド個別領域利用権限の設定
11	デジタル庁又は AWS との間で、ガバメントクラウド構築のために必要な連絡
12	クラウドサービス等利用料の集計、複数の地方公共団体間での按分等の調整および設定
13	上記業務に付随・関連する業務

第３条（ガバメントクラウド環境構築業務仕様書の変更）

１．ガバメントクラウド環境構築業務仕様書（以下、本仕様書という。）について、変更が必要となった場合には、受託者から本市に対して書面で通知するものとする。

第２章　業務内容詳細

第４条（業務内容詳細）

1. クラウドインフラの設計（権限管理含む）、構築

   AWS の仮想サーバ（以下、EC2 という。）とデータベース（以下、RDS という。）等、アプリケーションが動作するインフラ環境のスケール設計・構築を行うこと。構築にあたっては、マルチ AZ を基本とした冗長構成を必要に応じてとることで、可用性を確保できるように設計すること。

   また、業務間連携にあたっては、既存の VPC にある S3 を介して行うため、これを前提に設計を講じること。

2. 仮想サーバのウィルス対策及びセキュリティパッチの設定

   EC2 に対し、Windows Update で公開されるセキュリティパッチの設定及び、ウィルス対策ソフトのパターンファイル適用のための設定を行うこと。インターネットゲートウェイ等の必要なサービスの利用にあたっては、十分なセキュリティ対策を講じること。

3. セキュリティ対策

   AWS のサービスで対応可能なファイアーウォールや暗号化等でセキュリティ対策を実施すること。

4. 定期メンテナンス等のイベント管理設定

   AWS より提供されるメンテナンス情報、各種マネジメントサービスのアップデート情報を基に、AWS のイベントを管理・設定すること。

5. 死活監視・エラー監視・リソース監視設定

   EC2、RDS 等、アプリケーションの実行に必要なマネジメントサービスの死活監視、エラー監視、リソース監視を２４時間３６５日行える設定を行うこと。監視結果の解決については以下の対応を行うこと。

   ａ．死活監視にて、EC2 及び RDS の停止が確認された場合は、前日のバックアップデータを使用して復旧を行うこと。

   ｂ．エラー監視にて、発見されたエラーについては、原因の特定、対処法の検討を行い、設定修正を行うこと。

   なお、AWS に起因する場合は、AWS に問い合わせを行い、対応を行うこと。

   ｃ．リソース監視にて、発見されたリソースの過不足については、メンテナンス時間を本市へ通知し、リソース調整を実施すること。

6. インシデント管理設定

   受託者の共同利用環境において、AWS のサービスに対処が必要なインシデント管

理設定を行うこと。

7. EC2 と RDS のバックアップとリストア設定

受託者の共同利用環境において、AWS から提供されるバックアップサービスを使用し、EC2 と RDS のバックアップを取得する設定をすること。

■バックアップの種類

月次バックアップ　　：フルバックアップ（1 世代）

日次バックアップ　　：フルバックアップ（7 世代）

データの遠隔地バックアップ：バックアップデータはクロスリージョンバックアップ機能でコピー

■データリストア

AWS の EC2 及び RDS の停止、破損等により復旧が必要になった場合は、取得したバックアップデータよりリストアを行うこと。

なお、リストアについては、アプリケーションの誤操作など本市の過失によるものや故意・重過失（ほぼ故意に近い操作）によるインスタンス破壊やデータ消失はリストア対象外とする。

8. ネットワーク構成

受託者のデータセンター内部のネットワーク及び受託者の共同利用環境のネットワークの構成を行うこと。

また、本市のガバメントクラウドネットワークアカウントからの接続ができるように対応すること。

9. クラウド環境の構築及びデジタル庁から提供されるテンプレートの適用

受託者の共同利用環境にデジタル庁から提供されるテンプレートを適用し、受託者標準構成に基づき本市の利用環境の構築を行うこと。

10. ガバメントクラウド個別領域利用権限の設定

受託者の共同利用環境のアカウントを管理し、CSP のコンソールから不正操作されることを防止する設定をすること。

11. デジタル庁又は AWS との間で、ガバメントクラウド構築のために必要な連絡

ガバメントクラウドの構築を行うため、デジタル庁又は AWS と必要な情報提供や調整支援を行うこと。

12. クラウドサービス等利用料の集計、複数の利用者での按分等の調整および設定

受託者の共同利用環境における団体ごとのクラウド利用料の集計及び費用按分の調整および設定を行うこと。

第５条（共同利用環境内容）

受託者の共同利用環境は以下の対策を講じた環境を構築すること。

１．運用・保守性

ａ．実行環境の復旧については、定時バックアップで取得した情報のみを使用して復旧を行う。

ｂ．定時バックアップは日次バックアップとする。

ｃ．OS 等パッチ情報の展開及び適用について、緊急性の高いパッチは、仮想サーバで稼働するシステムがパッチを適用してもシステムの動作に問題が無いことが確認でき次第、速やかに適用する。

それ以外については、アプリケーションの定期メンテナンス時に適用を行う。

ｄ．データの損失については、障害発生時のデータ損失防止対策として、定時バックアップで取得したデータから復旧を行う。

ｅ．受託者の共同利用環境については、死活監視、トレース情報を含むエラー監視、リソース監視を行う。

２．セキュリティ

ａ．ウィルス定義ファイルについては、定義ファイルリリースされ次第、自動適用を実施する。

ｂ．伝送データについては、CSP が提供するマネージドサービスから発行される証明書が必要な通信のみ許可する。

ｃ．蓄積データについては、CSP が提供するマネージドサービスを利用して、記憶装置全体を暗号化する。

ｄ．共同利用環境は重要度の高い情報資産が格納される範囲と定め、不正アクセスの調査に必要なログを取得する。

ｅ．受託者提供のアプリケーションにおける脅威、脆弱性に関する対策度合いに応じて、不足部分を補填するための対策を講じる。

３．可用性

ａ．業務停止を伴う障害が発生した際は、1 営業日前の時点を目標復旧地点と定め、復旧を行う。

ｂ．業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、窓口対応等、システム停止が及ぼす影響が大きい機能を優先し１２時間以内に全システムの復旧を行う。

ｃ．大規模災害が発生した際、電源及びネットワークが利用できることを前提に遠隔地に設置されたバックアップデータを利用して１か月以内に業務の再開が行えるよう全システムの復旧を行う。

ｄ．受託者作業において、リモート保守ができることを前提に、安定的な稼働ができるように運用を行うこと。また、運用ができない場合の補償の定義がされていること。ただし、本市に了承を得た計画メンテナンスによる停止時間、CSP の定期メンテナンスにかかる時間、受託者の責任範囲以外の故障による停止時間、アプリケーションの責による停止時間は除く。

ｅ．地震、水害、テロ、火災などの大規模災害時では、同一の構成で情報システムを再構築する。

ｆ．地震、水害、テロ、火災などの大規模災害時に備え、バックアップデータは通常稼働リージョンとは別リージョンに保管する。

第 6 条（責任分界点）

本業務は以下に示す範囲の構築を行うこと。

<table>
<tr><td rowspan="2">本サービス
提供範囲外</td><td colspan="4">アプリケーションに格納されるデータ
（業務で使用している蓄積データ）</td></tr>
<tr><td colspan="4">アプリケーション、ＩＤとアクセス管理</td></tr>
<tr><td rowspan="2">本サービス
提供範囲</td><td colspan="4">EC2のオペレーティングシステム、CSP内のネットワーク、
ファイアーウォール構成</td></tr>
<tr><td>クライアント側のデータ
暗号化とデータ整合性認証</td><td>サーバー側の
データ暗号化</td><td colspan="2">ネットワークトラフィック保護
（暗号化、整合性、アイデンティティ）</td></tr>
<tr><td rowspan="5">AWS
提供範囲</td><td colspan="4">AWSから提供されるソフトウェア</td></tr>
<tr><td>コンピュート</td><td>ストレージ</td><td>データベース</td><td>ネットワーキング</td></tr>
<tr><td colspan="4">ハードウェア/AWSグローバルインフラストラクチャー</td></tr>
<tr><td>リージョン</td><td colspan="2">アベイラビリティゾーン</td><td>エッジロケーション</td></tr>
</table>

第 7 条（納品物）

本業務における納品物は以下の通りとする。

・本番環境情報

・テスト項目

第 8 条（その他）

本仕様書に記載のない内容については、提供範囲外とする。