

ガバメントクラウドネットワーク運用管理補助業務委託仕様書

1 契約の目的

令和 3 年(2021 年) 5 月 12 日に「地方公共団体情報システムの標準化に関する法律」が成立し、地方公共団体の基幹業務システムについて、原則全ての地方公共団体が、目標時期である令和 7 年度(2025 年度)末までに、ガバメントクラウド等に構築された標準化基準に適合した基幹業務システム(以下「標準準拠システム」という。)へ移行することとなった。

標準準拠システムに移行する際は、国が用意するガバメントクラウドを利用することが努力義務とされている。県においても、原則としてガバメントクラウドを利用する予定である。

そのため、それぞれの環境にある標準準拠システムが効率的かつ円滑に業務を行うための仕組みづくりが必要となっている。

今回の契約は、庁内から、ガバメントクラウド上に運用管理補助業務を実施するための単独利用環境の構築、DNS 管理及びプライベート認証機関の構築を行うことで、それぞれの環境にある標準準拠システムが、効率的かつ円滑に業務を行えるようにすることを目的とする。

2 調達の範囲

2.1 調達の範囲

調達する機能は、ガバメントクラウドにおける①運用管理補助領域の構築、②DNS 管理(名前解決の中継機能)及び、プライベート認証機関の構築である。

①運用管理補助領域の構築

各事業者が円滑に業務を行えるように、AWS 上にネットワークのルーティング機能やその他の運用管理を行う領域の構築。

②DNS 管理

DNS 管理(Route53Resolver)を構成し、ドメイン管理機能と権威 DNS 機能を実現するために必要な環境の構築

本調達範囲を図1に例示する。

※ ASP との接続方法は、各自治体との協議の上、AWS TransitGateway、PrivateLink、ピアリングアタッチメント等に対応すること。

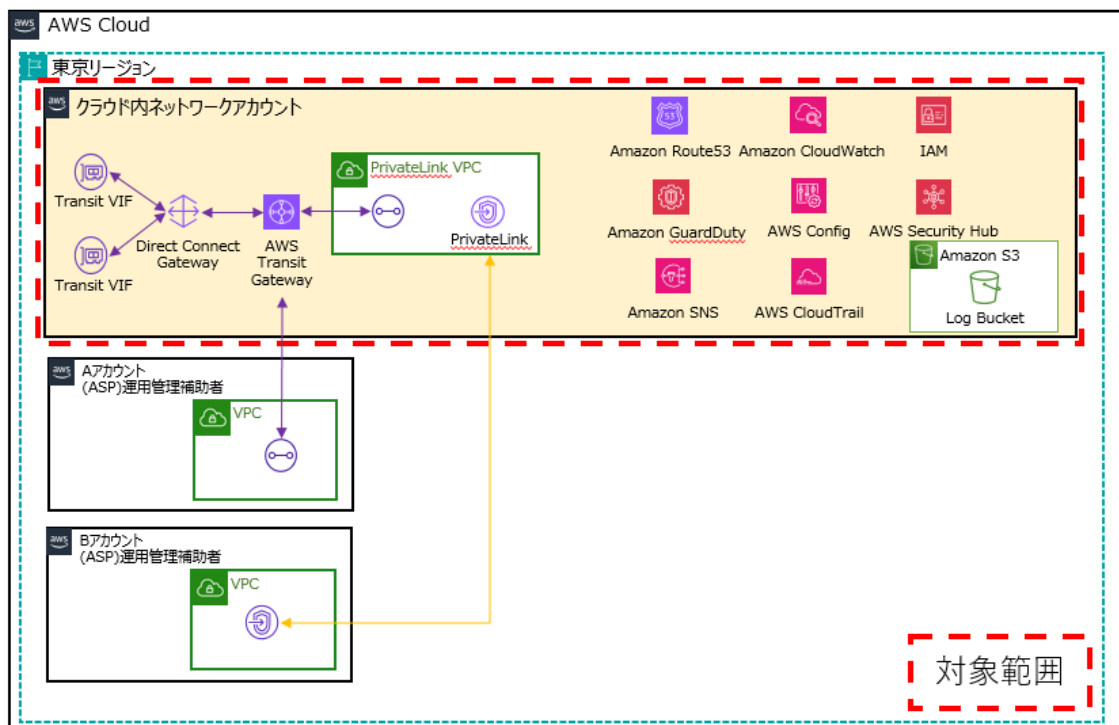


図 1:調達範囲(クラウド内ネットワークのみ)(例)

2.2 契約の範囲

本契約の範囲は、県の標準準拠システムをガバメントクラウドで整備・維持するための、ガバメントクラウドにおける AWS の運用管理補助領域の構築、テストにかかる一連の工程とする。なお、各工程に必要な機器(端末、認証機器等)は事業者が用意すること。

2.3 ガバメントクラウドへの接続方法

LGWAN ガバメントクラウド接続サービス(LGCS)により接続する

3 契約期間

契約締結日から令和 8 年3月31日まで

4 前提事項

本契約に関する前提事項を以下に記載する。

4.1 参考資料について

国が公表している「地方公共団体情報システムのガバメントクラウドの利用について【第 2.0 版】」に従い、ネットワーク運用管理補助業務を実施するための単独利用環境の構築を行うこと。
ドキュメント名:地方公共団体情報システムのガバメントクラウドの利用について【第 2.0 版】
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_res

ources/c58162cb-92e5-4a43-9ad5-
095b7c45100c/59fd75df/20240424_policies_local_governments_outline
_03.docx

4.2 ガバメントクラウド環境について

4.2.1 ガバメントクラウド利用方式

ガバメントクラウド利用方式に関して以下に重要な点を記載する。

- ・ システム標準化対象の業務システムはすべて共同利用方式を採用予定である。
- ・ AWS のコンソールにアクセスするために必要な MFA デバイスとライセンスを準備すること。MFA は、AAL3 のハードウェア MFA を原則とする。

4.2.2 作業場所及び利用環境

インターネット経由でマネジメントコンソールに接続する場合は、デジタル庁の示す「ガバメントクラウド利用における推奨構成」および「ガバメントクラウドリスクアセスメント」に記載されているものと同様の方式で行い、また同様のセキュリティ対策を行うこと。その際の端末や回線費用は受託者の負担とする。

なお個人情報を含む業務情報にアクセスする必要がある場合は、庁内ネットワーク経由で行うこと。

4.3 セキュリティ要件

以下の法規や規定等を遵守すること。

- ・ 個人情報保護に関する法規
- ・ デジタル庁が定める、ガバメントクラウドに設定するルール、ポリシー等
- ・ 総務省が定める、「地方公共団体における情報セキュリティポリシーに関するガイドライン」
- ・ 情報セキュリティポリシー
- ・ 別紙●「情報セキュリティに関する特記事項」
- ・ 別紙●「個人情報取扱特記事項」

5 クラウド内ネットワークの契約仕様について

5.1 クラウド内ネットワークの構成

クラウド内ネットワークについては、単独利用方式にて構築する。

5.2 工程別作業内容

工程	業務要件
(1) プロジェクト計画策定	クラウド内ネットワーク構築のプロジェクト計画を策定すること。 プロジェクト参加のメンバーの中に AWS のソリューションアーキテクトプロフェッショナルの資格を保有する者を1名以上配置すること。
(2) 構築	計画、設計した内容をもとにクラウド内ネットワークを構築すること。
(3) テスト	クラウド内ネットワークのテストを行うこと。なお、テストを実施するうえで、必要な庁内 NW とサーバの環境は別で準備する。テストの実施は庁内 LAN ベンダーと ASP ベンダー及び県と協力の上実施する
(4) プロジェクト管理	クラウド内ネットワーク構築プロジェクトに関する進捗報告、および各工程における課題管理等を実施すること。

5.3 構築要件

クラウド内ネットワークで必要な要件を以下に記載する。

要件	詳細
クラウド内ネットワーク	・CSP は AWS を使用すること。 ・構築の際は、CSPのリファレンスアーキテクチャに準拠すること。 ・クラウド内ネットワーク内に配置した Transit Gateway を用いて、各 VPC 等に接続すること。(※各 VPC との接続方法は、各自治体との協議の上、AWS TransitGateway、PrivateLink、ピアリングアタッチメント等に対応すること。)

6 DNS 管理及びプライベート認証機関について

6.1 DNS 管理(Route53 Resolver)

DNS 管理(名前解決の中継機能)を提供すること。

オンプレ環境から業務システム環境の名前解決を中継する Inbound Endpoint を2つ、業務システム環境からオンプレ環境へ名前解決を中継するアウトバウンドエンドポイント2つを構築すること。

Inbound Endpoint の構成にあたり、業務システム環境にて登録された Route53 Private Hosted Zone のルール共有すること。

Outbound Endpoint の構成にあたり、対象ドメインの Resolver ルールを当社にて設定し、Resolver ルールを共有こと。

6.2 プライベート認証機関(PrivateCA)

プライベート認証機関を構成し、ルート証明書を発行、管理する機能を有すること。

AWS 上の業務システム環境に対しプライベート認証機関のリソース共有、及びルート証明書を持ちて各種証明書の発行できること。

プライベート認証機関:AWS Private Certificate Authority ルート証明書の管理:
AWS Certificate Manager のリソースを構築すること。

7 成果物

7.1 成果物

- ・ 計画時に関する成果物
プロジェクト計画書(作業項目、スケジュール、体制図)
- ・ 設計時に関する成果物
設計ドキュメント一式(ヒアリングシート、詳細設計書(パラメータシート)、構成図)
- ・ テスト時に関する成果物
テストに係るドキュメント一式(結果報告書)
- ・ プロジェクト管理に関する成果物
議事録、課題管理表。履行期間の最後に作業の完了報告書を納品すること。
- ・ その他
県と協議の上、提出が必要となったもの。

7.1.1 成果物の納品方法

成果物の納品方法は Microsoft Word, Microsoft Excel, Microsoft PowerPoint 形式で提出を行うものとする。

7.1.2 成果物の提出期限

計画・設計・テストについては、各工程が完了次第資料を送付すること。その他の資料に関しては、履行期限までに提出すること。

8 その他

8.1 インシデント発生時の報告

インシデントが発生したときは、初報、最終報告のほか、必要に応じて随時進捗を報告すること。

報告方法はメール、WEB 等の電磁的記録とすること。

8.2 秘密を守る義務

受注者は、発注者の承諾なく、職務上知りえた秘密を漏らしてはならない。その職を引いた後もまた同様とする。

8.3 その他

令和8年度にガバメントクラウド運用管理補助業者が変更となった場合においても、円滑に業務の引き継ぎを行えること。