ガバメントクラウド構築及び運用管理補助者業務委託仕様書

１　業務内容

受託者は、次に定める業務を行う。

なお、これまでの検討の過程から、藤沢市（以下、「委託者」という。）の主たるクラウドサービスプロバイダは Amazon Web Service（以下、「AWS」という。）を採用することを予定しており、本仕様書は AWS を前提として記載する。

また、委託者の利用する予定の標準準拠システムについては別紙「標準準拠システム一覧」のとおりとする。

（１）構築作業

構築範囲についてはネットワークアカウント（単独利用方式）及び共通基盤アカウント（単独利用）とする。

具体的な作業内容については以下のとおりとする。

ア　本業務に必要なアカウント申請支援

イ　デジタル庁指定のテンプレート適用作業

ウ　指定されたドメインを利用し、庁内やその他システムと接続できるよう DNS 設定を行うこと。

エ　主たる運用環境を行う東京リージョンに、災害対策環境としてバックアップデータおよび被災時に展開できる環境を大阪リージョンに、それぞれ配置すること。

オ　CIDR 設計

（ア）委託者の利用するシステム全体を考え、指定のあった CIDR の範囲内でシステムが構築できるよう設計すること。

（イ）Transit Gateway の接続先の単独利用・共同利用アカウントの VPC の CIDR 範囲が重複しないように設計すること。

カ　CIDR 設計に応じて VPC・サブネットの作成を行うこと。

キ　庁舎のネットワーク機器からガバメントクラウド接続サービス等にアクセスできるように設定すること。

ク　VPC 間の接続

（ア）ネットワークアカウントの VPC 同士、またネットワークアカウントの VPC と ASP の VPC 間の接続を行うこと。

（イ）IP アドレス設計との兼ね合いで CIDR が重複する場合は、AWS PrivateLink を用いるなどして回避することができるよう設計する。

ケ　インターネット接続の必要なコンポーネントの整理をすること。

コ　インターネットに接続可能な VPC を用意し、Proxy などを介して他の VPC からインターネットに接続する必要のあるコンポーネントがインターネット接続できるよう設定すること。

サ　インターネット接続およびOSのパッチ適用のためのWSUS サーバ、ウイルス対策ソフトのパターンファイル更新のための配信サーバをネットワークアカウント内に構築すること。

シ　庁内データ連携機能の構築

（ア）「地方公共団体情報システム共通機能標準仕様書【第2.1 版】」に定める庁内データ連携機能／ファイル連携を行うためのデータ保管領域について共通基盤アカウント上に設計・構築すること。

（イ）当該データ保管領域はオブジェクトストレージにて構成することとし、AWSのマネージドサービス（S3、Transfer Family 等）を積極的に活用すること。

（ウ）認証認可サーバー、通信経路の暗号化、保存データの暗号化ができる環境を整備すること。

（エ）詳細な要件については、「地方公共団体情報システム共通機能標準仕様書【第2.1 版】」の「機能要件」・「ファイル連携に関する詳細技術仕様書」等を参照すること。

ス　構築においてネットワーク回線事業者、各ASP事業者等、他の事業者との協力が必要な場合は随時対応すること。

セ　構築期間中の進捗会議の開催。また、開催頻度等の会議体の詳細は、委託者と協議の上決定すること。

ソ　（２）運用管理補助業務を開始するにあたり、運用が問題なく開始できる状態であることをテスト項目に沿って確認すること。なお、テスト項目の内容については、委託者と協議の上、決定すること。

タ　その他、デジタル庁発行の「ガバメントクラウド利用における推奨構成 AWS編」になるべく準拠するよう、委託者と協議の上必要な作業等を行うこと。

（２）運用管理補助業務

具体的な作業内容については以下のとおりとする。

ア　構築時・運用管理時それぞれにおいてASP 事業者に適切な権限をIAMにより割り当てること。

イ　コスト管理

（ア）複数のASP事業者が1つのアカウントに混在する場合はタグを用いて事業者ごとにリソースを判別できるようにすること。

（イ）必要に応じてタグベースでの閲覧・操作などの権限を付与できること。

（ウ）システムごと・ASP事業者ごと・アカウントごとに月ごとの予算を設定し、設定値を超過した場合にメール等でアラートを発報すること。

（エ）コストをアカウントごと、ASP事業者ごとに確認できるようにすること。

ウ　セキュリティの設定

（ア）Security Hub、GuardDutyおよびその他セキュリティサービスからアラー

トが発報された場合は委託者に自動的に通知する仕組みをもち、それぞれのサービスの推奨に従った対応を実施すること。また、必要に応じて ASP 事業者と協力し、対応すること。

（イ）既存構成のベストプラクティスを提案するツールを活用し、定期的に推奨構成を確認・必要に応じて変更すること。

（ウ）委託者のセキュリティポリシーに合わせたアラートを設定すること。

（エ）デジタル庁から配布されているガバメントクラウド必須適用テンプレートを適用すること。

（オ）デジタル庁からテンプレートの変更があった場合やメンテナンス作業が必要になった場合は速やかに対応すること。

エ　CloudWatch や Config からアラートが発報された場合、アプリケーション側で対応が必要な事項について迅速に対応すること。また、必要に応じて ASP 事業者と協力し、対応すること。

オ　CloudWatch、CloudWatch Logs 等を利用して応答時間、エラー率、障害停止時間（率）等をモニタリングできるよう設定すること。

カ　AWS Personal Health Dashboard の通知へ対応すること。

キ　監視・障害については常時対応すること。

ク　障害発生時には、原因の切り分け、委託者、ASP 事業者等の関係者へのエスカレーションを速やかに行うこと。

ケ　各 ASP 領域との責任分界点、留意事項等に関する説明を委託者に実施し、必要に応じて ASP 事業者に対する説明資料を作成すること。

コ　ASP 事業者が疎通テスト等を実施する場合、協力すること。

サ　国からの通知、マニュアル等の資料を読み解き、必要な対応について支援すること。

シ　定例報告会の開催をし、発報されたセキュリティアラート・コスト・構成の見直し等に関して情報提供を行うこと。

ス　その他、運用管理補助業務上必要な作業等を行うこと。

2　成果品について

以下の成果品を納めること。なお、納品形態及び期限については、委託者と受託者で協議の上、決定する。また、委託者との協議により必要と判断された成果物が生じた際には、別途提出すること。

（1）基本設計書

（2）詳細設計書

（3）システム構成図

（4）各種会議資料・議事録

定例会その他の打合せ（臨時の打合せ、各業務主管課・ベンダへのヒアリング

を含む）の議事録を開催後２週間以内に受託者において作成・提出し、委託者に内容の承認を得ること。
（５）テスト結果報告書
（６）運用実績報告書（業務実績報告書）

３　業務の引継について

本業務の契約履行期間の満了、全部もしくは一部の解除、またはその他契約の終了事由の如何を問わず、本業務が終了となる場合には、業務システムへの運用負担を抑えるために（移行・再設定等の必要なく継続的に使用できるように）、受託者は委託者の指示のもと、受託者が構築した環境を次の受託者に引き継ぐことを基本とする。

このため、構築工程では以下の内容を詳細に記録した業務引継書を作成し、運用工程では、次の受託者への環境等に関するレクチャ、質問対応、設計書等を含むドキュメント提供等を行うこと。なお、次の受託者への引き継ぎは、本業務終了の最大半年前から実施することとする。

（１）業務引継書の内容
ア　業務の流れ
イ　業務の進捗状況
ウ　構成管理台帳（資産、資源の所在と明細）
エ　構成管理台帳（資産、資源の所在と明細）の提出
オ　その他円滑な業務引継ぎのために必要となる資料
（２）業務の引継に伴う作業について

業務の引継に伴いデータ移行等の作業が発生する場合、以下の対応事項について、委託者及び次の受託者に対して誠意を持って協力すること。
ア　構築・運用を行っている全ての環境について、移行のために必要となるデータを汎用的なデータ形式に加工し提供すること。
イ　サービス構成・設定情報等の資料を提供すること。

４　作業環境

（１）リモート開発・保守環境の整備

受託者の拠点からリモート開発・保守ができる環境を整備し、受託者の拠点からの接続経路についても、受託者にて整備すること。

（２）接続方法

リモート開発・保守ができる環境への接続方法は、閉域ネットワークでの接続を前提とする（本閉域ネットワークの冗長化までは要件としない）。なお、総務省「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」に定義される、インターネット経由での管理コンソールへの接続は、委託者と協議

の上、セキュリティ面等に問題がない業務範囲において、例外的に認めることとする。また、接続に必要なMFAデバイス等、本環境を利用する際の機器、端末、環境等は受託者側で用意すること。

（３）セキュリティ

委託者のマイナンバー利用事務系ネットワークに接続することとなるため､「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」等に記載されるセキュリティ要件を満たすよう留意すること。

５　作業条件について

（１）資料等の貸与

委託者が業務委託の履行上必要と認めた資料・データについては、受託者に貸与する。受託者は、貸与した資料・データについては細心の注意をもって取り扱うとともに、作業終了後は速やかに委託者に返還もしくは廃棄すること。

（２）服務条件

受託者が委託者の施設・設備等で作業を行う場合は、身分証を携帯するなど、作業者の身分等が判別できるようにすること。

（３）施設設備等の利用範囲・条件及び入退管理について

藤沢市役所での作業場所入退室の際は、入退室管理簿に日付、氏名、入退室時間等を記入し、指定の入室許可証を携帯しなければならない。

６　費用負担について

本業務に係る費用負担は次のとおりとする。

（１）人件費、諸手当等

本業務の遂行にあたり、必要となる受託者の人件費、出張旅費、諸手当等の費用は全て契約金額に含むこと。

（２）消耗品費

委託者との打合せをはじめとする各種会議等で使用する印刷物の作成、納品に係る消耗品の費用は全て契約金額に含むこと。

（３）通信運搬費

委託者との連絡調整に必要となる電話・郵便等の通信運搬費については、受託者から委託者へ向け発信、発送するものについては全て契約金額に含むこと。

（４）その他

上記以外で本業務の実施に当たって必要な費用（ライセンス費用等）に関しても全て契約金額に含むこととし、別途委託者に請求は行わないこと。なお、ガバメントクラウド内のクラウドサービスを利用するために発生するクラウド利用料は、デジタル庁「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関する基準」に従い委託者にて負担するため費用に含めないこと。

７　契約不適合責任

本契約の成果物の検査終了後、１年以内の期間において、本業務の成果物に係る安定稼働に関して契約不適合の疑いが生じ、委託者が必要と認めた場合は、受託者は速やかに契約不適合の疑いについて調査し、回答しなければならない。

調査の結果、本業務の成果物に関しての契約不適合が認められた場合は、受託者の責任と負担において、速やかに改修を行わなければならない。なお、改修については、委託者の承認を得てから作業に着手し、改修結果については委託者の承認を得なければならない。

８　機密の保持

別紙「データの保護及び秘密の保持等に関する仕様書」に準ずること。また、藤沢市情報セキュリティポリシー＜基本方針＞の趣旨を理解し、情報資産の適切な管理に努めること。

９　環境保全

受託者は、「藤沢市地球温暖化対策実行計画」の趣旨を理解し、第５章の各取組項目を実施するよう努めること。

１０　疑義等の決定

本仕様に定めのない事項及びこの契約に際し疑義が生じたときは、双方協議のうえ、定めるものとする。