公共部門におけるクラウドサービス購入

ハンドブック - クラウド フレームワーク契約に向けた RFP のサンプル 文言付き

バージョン 2: (2022 年 2 月)

通知

このドキュメントは情報提供のみを目的としています。特定地域の公共調達プロセスに係る法的要件に従って作成されたものではありません。クラウドの利用者は、本書の情報およびクラウドサービス事業者の製品またはサービスの活用に際し、独自に評価して責任を負うものです。本書は、いかなる保証、表明、契約上の約束、条件、または確約を意味するものではありません。

サンプル文書および文言は、法的な助言、ガイダンス、または忠告ではありません。本書は、クラウドの利用者に、事業を行うそれぞれの国の適用法における責任について、自身の法律顧問に相談することを推奨します。CISPE は、本書内に記載されている情報に関連する、または情報に起因するすべての保証、責任、または損害について一切の責任を負いません。

CISPE について

CISPE (Cloud Infrastructure Services Providers in Europe、https://cispe.cloud) は非営利の独立系業界団体です。私たちは欧州のクラウドインフラストラクチャサービス事業者を代表して、業界や政策決定者と協力しながら、クラウドサービスと、業界、一般生活、社会全般におけるそのサービスの役割について、ガイダンスおよび教育を提供しています。

私たちのメンバーは拡大しており、EU 全ての国で事業を行い、欧州の 16 か国にグローバル本部を置く企業などが加盟しています。私たちは、少なくとも 1 つのサービスが CISPE のデータ保護行動規範の要件を満たしていると宣言する企業に対して門戸を開いています。私たちの取り組みは以下の通りです:

- EU および EU 加盟国内における公共調達におけるクラウドファーストのメリットを提唱する
- 2030 年までに気候中立に達するようにクラウドインフラストラクチャ部門に関与する
- EU 全体の一貫的なセキュリティ要件および技術標準を推進する
- データ保護行動規範を用いて包括的なプライバシー要件を支援する
- 今後も EU のクラウドインフラストラクチャの市場が開かれ、競争力を持ち、閉鎖的にならないよう尽力する
- EU の法的フレームワークにおける不当なコンテンツ監視活動の義務を阻止する

私たちのメンバーは、政府、公的機関、企業が独自システムを構築し、数十億人の市民向けの重要なサービスの提供を実現するために不可欠な「IT のビルディングブロック」を提供し、維持しています。この役割において、私たちは人工知能 (AI)、コネクテッドオブジェクト、自動運転、5G、および次世代の移動通信技術を統合した最先端のテクノロジーとサービスの発展の実現をサポートしています。

クラウドインフラストラクチャサービスの行動規範

CISPE データ保護行動規範は、EU の一般データ保護規則 (GDPR) の施行以前の 2016 年 9 月に発表されました。本規範は、厳格な GDPR の要件に対応しており、クラウドインフラストラクチャサービス事業者がデータ保護コンプライアンスを運用し、強力なフレームワークを提供するのを支援し、また、これによってお客様がクラウドサービス事業者を選択しサービスを信頼

できるようにすることを企図しています。CISPE 行動規範は、2021 年 5 月に European Data Protection Board (EDPB) によって認証され、2021 年 6 月にフランスの監督当局である CNIL によって承認されています。https://www.codeofconduct.cloud/

Climate Neutral Data Centre Pact (気候中立的データセンター協定)

CISPE は 2019 年末に欧州委員会と連携して、2030 年までにデータセンターの気候中立を確保するための一連のメトリクスおよび自己規制イニシアチブを策定しました。このイニシアチブは、European Data Centre Association (EUDCA) と連携して、他の貿易団体やデータセンター市場参加者とともに策定され、2021 年 1 月に「Climate Neutral Data Centre Pact (気候中立的データセンター協定)」https://www.climateneutraldatacentre.net/として策定されました。

公正なソフトウェアのイニシアチブ

フランスの CIO 団体である CIGREF とともに、また欧州全体の CIO およびサービス事業者から成るその他の貿易団体の支援を受け、CISPE は「10 Principles of Fair Software Licensing for Cloud Customers」 (クラウド利用者のための公正なソフトウェアライセンシングの 10 原則) を発表しました。これは、成長イノベーションおよび柔軟性のために、クラウドに目を向けるビジネスに対する一連のベストプラクティスであり、ソフトウェアサービス事業者が公正なライセンシング契約を参照するように促すものです。
https://www.fairsoftware.cloud/

GAIA-X

CISPE は、オープンかつ透明で安全なデジタルエコシステムを提供するための欧州のイニシアチブである GAIA-X の 22 の創設メンバーの 1 つです。そのように CISPE は当初から、GAIA-X のビジョンとその信条にコミットしており、事務局長は 2021 年 6 月に理事に再選されています。このハンドブックで参照されているツールのいくつか (CISPE データ保護行動規範、SWIPO IaaS 行動規範) は、GAIA-X の原則を遵守していることを示すのに役立ちます。https://www.gaia-x.eu

CISPE と公共部門

CISPE は、欧州の公共政策に関する議論に貢献しており、欧州のクラウドインフラストラクチャ業界の役割、貢献、可能性の理解向上に向けて取り組んでいます。

公共購入モデルでは、クラウドコンピューティングの導入および利用のプロセスを条件付ける必要がありますが、クラウドサービスの購入は、公共部門で知られている最も伝統的なテクノロジーの購入とは異なるものです。このため、調達方法を再考する必要があります。: CISPE は、EU の政策決定者に対して、全欧州規模で「クラウドファースト」な政策イニシアチブをベースとしてより野心的で積極的なアプローチを展開するよう推奨しており、それによって、欧州単一のクラウドインフラストラクチャ市場の成長を推進できるようにし、デジタル単一市場 (Digital Single Market: DSM) の成長目標を支援しようとしています。

本ハンドブックは、公共機関がクラウドサービスを調達する際に役立つガイダンスおよびサポートを提供することを目的としています。

詳細情報

CISPE メンバー: https://cispe.cloud/members

理事会: https://cispe.cloud/board-of-directors

CISPE 行動規範で宣言されているクラウドコンピューティングサービス:
https://www.codeofconduct.cloud/public-register/

目次

本ハンドブックの概要および目的

この**クラウドサービス購入ハンドブック**の目的は、競争を伴う調達プロセス (**クラウドサービス提案依頼書** (RFP)) を通じてクラウドサービスの購入を希望しているものの、クラウドフレームワーク契約を作成する専門知識がないクラウドのお客様にガイダンスを提供することです。

このドキュメントは情報提供のみを目的としています。特定の国や地域の公共調達プロセスの法的要件に従って作成されたものではありません。

また、本ハンドブックは、クラウドフレームワーク契約に基づいて購入するときに**コールオフ**または**ミニコンペ**と言われる手順を実施する際の追加的な選定基準の文言にもなります。本ハンドブックの各セクションは、一般的な IT の RFP に似せた形で構成されています。サンプルの一般的な RFP および選択基準の文書には、クラウド RFP と従来の IT RFP とが異なる理由を理解するための解説を付しています。

欧州の公共施設および機関がクラウドファーストのアプローチを用いて IT インフラストラクチャをモダナイズする方法を示した欧州委員会のクラウド戦略の発表後に、CISPE は 2019 年 7 月にイベント「How to transform governments through a smart cloud policy」で欧州委員会に本ハンドブックを提出しました。

本ハンドブックの**バージョン 2** には、データ保護 (2.3.1.1 節)、クラウドサービス業者の切り替えとデータの移動 (2.3.1.2 節)、ソフトウェア契約および条件 (2.5.2 節)、クラウドの持続可能性 (3.6 節) に関する新しいガイダンスおよび更新された付録 B ライブ技術評価が含まれています。

「**クラウドサービス**」とは、要があるすべてのクラウドテクノロジーと関連サービスを指します。これには、クラウドインフラストラクチャ自体およびサービスとしてのソフトウェア (SaaS) 製品などクラウドマーケットプレース上のサービスに加え、クラウドへの移行の支援と実行、およびクラウド上のワークロードのサポートに必要なコンサルティングやプロフェッショナル サービスやマネージドサービスが含まれます。

公共部門の IT の第一の選択肢としてクラウドコンピューティングが登場したことは、既存の調達戦略をモダナイズする機会にもなります。公共部門の組織は、クラウド中心の購入プロセスによって、効率性とコスト削減を実現しながら、最先端のイノベーションの利用、スピードと俊敏性の向上、セキュリティ体制およびコンプライアンス管理の改善など、クラウドのメリットを最大限引き出すことができます。

従来のハードウェア、ソフトウェア、およびデータセンターを購入する IT 調達方式は、クラウドサービスの購入にそのまま適用できるものではありません。クラウドモデルでは、料金、契約ガバナンス、契約条件、セキュリティ、技術的要件、SLA などすべての方法が異なっており、既存の調達方法を利用すると、結果的にクラウドが提供するメリットが減少または消滅してしまいます。

公共部門がクラウドサービスを効果的に購入する最適な方法の 1 つが**クラウドフレームワーク契約**を利用することです。これは、複数の組織にまたがり、一連のクラウドのメニューを与える (award) もので、これにより、購買組織の関連機関がニーズに合致したクラウドテクノロジーや関連サービスを獲得できる (acquire) というものです。クラウド契約の手段として、このようなフレームワーク契約を利用すると、クラウドサービスを効率的かつ効果的に購入することが可能となります。結果として、購買組織およびエンドユーザーとなる各関連機関は幅広いクラウドサービスを利用できるほか、最終的にはクラウドのメリットである俊敏性、巨大な規模の経済の利点、低コストで優れた可用性を実現するスケーラビリティ、幅広い機能、イノベーションのスピード、新しい地域に展開する能力を最大限に享受することができます。

この文書はクラウドインフラストラクチャサービス事業者 (CISP) が提供するサービスとしてのインフラストラクチャ (IaaS) およびサービスとしてのプラットフォーム (PaaS) の購入に焦点を当

てている点にご注意ください。 これらのクラウドテクノロジーは、CISP から直接、または CISP の再販事業者から購入することができます。クラウドマーケットプレースサービス (PaaS および SaaS)、およびクラウドコンサルティングサービスのディストリビュータに対する RFP については、追加の考慮事項が必要になります。

また、本文書はエンドツーエンドなクラウド調達のフレームワークのすべての要素をカバーするものではないことにもご注意ください。クラウド調達のベストプラクティス、クラウドの予算策定方法、クラウドガバナンスなどの問題をカバーする業界団体およびアナリストによる文書は他にも多数あります。クラウド調達戦略全体を策定する際に、これらの助言や文書を考慮することを強く推奨します。以下の**表 1** には、クラウドサービス RFP ハンドブックの概要、およびクラウドサービス RFP の各構成要素の RFP のサンプル文書の場所が記載されています。

表 1 – クラウドサービス RFP ハンドブックの各節の概要

節	概要およびサンプル RFP の文書
1.0 **クラウドフレームワーク契約の概要**	クラウドフレームワーク契約モデルの大まかな概要 (ロット、作成方法、および契約)
2.0 クラウドサービス RFP の概要	以下の節をカバーする一般的な RFP の文書のサンプルと、クラウドサービス RFP の構成および使用する文言の背後にある根拠を説明する解説。
2.1 クラウドサービス RFP の設定	2.1.1 序文および戦略目標 2.1.2 RFP の回答スケジュール 2.1.3 定義 2.1.4 本フレームワーク契約の購入モデルおよび競争に関する詳細な説明 2.1.5 入札者の最低限の要件 - 管理
2.2 技術	2.2.1 最低限の要件 2.2.2 ベンダー間の比較 2.2.3 契約
2.3 セキュリティ	2.3.1 最低限の要件 2.3.1.1 データ保護 2.3.1.2.クラウドサービス事業者の切り替えおよびデータの移動 2.3.2.ベンダー間の比較 2.3.3 契約

節	概要およびサンプル RFP の文書
2.4 料金表	2.4.1 最低限の要件 2.4.2 ベンダー間の比較
2.5 契約履行の設定/契約条件	2.5.1 契約条件 2.5.2 ソフトウェア契約条件 2.5.3 契約締結先の選択方法 2.5.4. オンボーディングとオフボーディング
3.0 ベストプラクティス/教訓	3.1 クラウドガバナンス 3.2 クラウドの予算 3.3 パートナーのビジネスモデルを理解する 3.4 クラウドブローカー 3.5 RFP 前のソーシング/市場調査 3.6 持続可能性
付録 A – 入札者相互間の比較に関する技術的要求事項	コールオフまたはミニコンペにおける一般的なテクノロジー要件の一覧
付録 B – 実際の技術評価	クラウドテクノロジー製品のデモの評点のサンプル文書 (コールオフ契約またはミニコンペの一環のクラウドデモ)

1.0 クラウドフレームワーク契約の概要

適切に設計されたクラウドフレームワーク契約によるクラウドサービスの購入は、関係する公共部門組織およびクラウドベンダーの双方にメリットをもたらします。適切に設計されたクラウドフレームワーク契約には以下のメリットがあります:

- **自然な協力**:
    - 複数の組織が団結して同様の要件を求めることは、利便性、効率、コストの削減、および注文プロセスの簡素化を意味します。マーケットプレースソリューションおよびコンサルティングなど、公共部門の複数の組織に共通するクラウドテクノロジーおよび関連するクラウドサービスのニーズを効果的にまとめる方法を構築します。
- **幅広いクラウドサービス**:
    - 場合により、CISP が提供するクラウドテクノロジーとマーケットプレースサービスに加えて、クラウドへの移行の完全な支援とその実行、およびクラウド上のワークロードのサポートに必要なすべてのコンサルティング/プロフェッショナル/マネージドサービスが範囲に含まれます。
    - クラウドテクノロジーは、CISP から直接、または CISP の再販事業者から購入することができます。
- **契約のガバナンス**:
    - さまざまな組織/購入者の共通の契約条件を調整し、組織ごとに異なる契約ではなく、単一のマスター契約を締結します。
    - また、それぞれ異なるものではなく、標準の、購入プロセス、契約条件、注文の仕組みを、各公共部門組織に提供した上でナビゲートできるので、ベンダーにとってもメリットがあります。
    - 柔軟性を提供します。既存の政府の政策/法規の範囲内で効果的なクラウド契約を作成、承認、実施するには、試行錯誤と迅速な調整能力が必要です。公共部門とクラウドベンダーのすべてが協力し、契約として、機械的、効率的に改善で

きるようなフレームワーク契約を作成する方が遥かに有益です。機能せず、調整も不可能な複数年契約の場合には、公共部門のエンドユーザー、調達組織、およびクラウドベンダーの利便性が低下してしまいます。

- **選択**:
    - 購入者は複数の認定 CISP から選択し、クラウド PaaS/SaaS のマーケットプレイス、クラウドコンサルティングなど、すべてのクラウドサービスおよび関連サービスに対して高い評価基準を設定できます。
    - これにより、各契約締結先の水準が適切に精査されているかを確認することで、フレームワーク内のサプライヤーの数を管理することができます。

クラウドサービスを購入するためのフレームワーク契約は、公共部門のエンドユーザーが必要に応じてアクセスして、クラウド上で実行するワークロードを計画、移行、利用、および運用できるように、CISP が提供する主要な IaaS/PaaS テクノロジーとともに、PaaS/SaaS マーケットプレイス、およびコンサルティングサービスが含まれるものが最適です。したがって、クラウドフレームワーク契約を設定するためのクラウドサービス RFP は、以下の 3 つのロットに分割することをお勧めします。

- **ロット 1 - クラウドテクノロジー**
  クラウドテクノロジーを CISP から直接または指定の CISP 再販事業者経由で購入するもの
- **ロット 2 - マーケットプレイス**
  PaaS および SaaS サービスのマーケットプレイスへのアクセス
- **ロット 3 - クラウドコンサルティング**
  クラウド関連のコンサルティングサービス (トレーニング、プロフェッショナルサービス、マネージドサービス等) および技術サポート

前述の通り、本文書では、CISP が提供する IaaS および PaaS クラウドテクノロジー (**ロット 1**) の購入に焦点を当てています (CISP から直接、または CISP 再販事業者経由で購入)。クラウドサービス RFP のロット 2 およびロット 3 のベンダーについては資格要件を分けることが必要です。

以下の**図 1** は、3 つのロットに分割されて適切に構成されたクラウドサービス RFP が、公共部門の組織に俊敏性をもたらし (技術面および契約面)、費用やクラウド利用の可視性とコントロールを高めるほか、求められるソリューションの構築や運用に必要なすべてのクラウドサービスを利用できることを可能とし得るクラウドフレームワーク契約になりうるのか鳥瞰するものです。

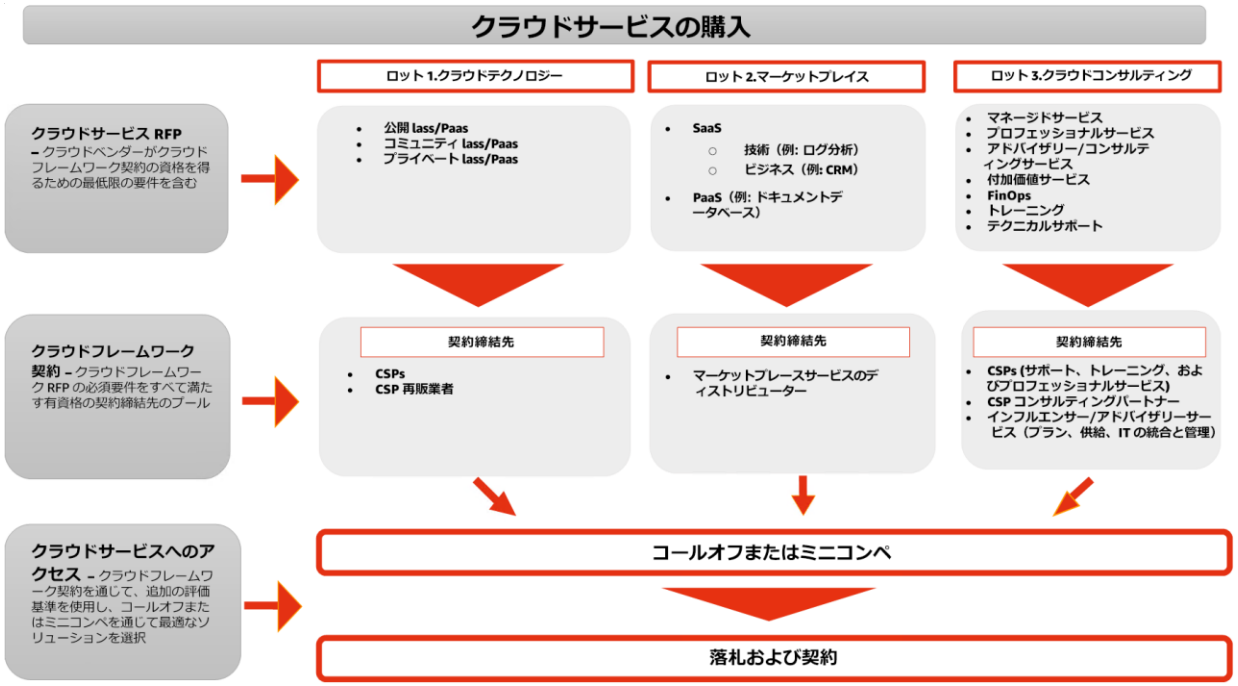

図 1 – 適切なクラウドサービス RFP は 3 つのロットに分割されます。クラウドフレームワーク契約の下で、技術面および契約面でエンドユーザーの要件が満たされるように、ロットごとにカテゴリや「提供の態様」を分類。

注意事項:

- 各ロットの契約締結者は複数です。
- ロット 3 は、別の RFP によって、またはコンサルティングサービスの既存の契約を介して締結される場合があります。

ロット 1 のカテゴリ

適切なクラウドフレームワーク契約では、CISP は提供するクラウドのモデルを、カテゴリに分けて各ロットにおいて説明することが求められます。**パブリック**クラウド、**コミュニティ**クラウド、および**プライベート**クラウドの定義については、クラウドコンピューティングの業界標準

(米国国立標準技術研究所 (NIST) クラウドの必須の特徴) を利用することをお勧めします。このようにしてクラウドフレームワーク契約を構築することで、購買組織およびこのフレームワークを利用する公的機関はさまざまなクラウドモデルから自身のニーズに適合したものを選択できます。

ロット 1 下の各クラウドモデルの NIST の定義 (パブリック IaaS/PaaS、コミュニティ IaaS/PaaS、およびプライベート IaaS/PaaS) については、節 「2.1.3 定義」 を参照してください。

競争方法 – コールオフ契約またはミニコンペ?

クラウドサービス RFP の適格基準は、必須要素および最低基準とすべきであり、「あると助かるもの」をそこに含めるべきではありません。フレームワークに適格となるためのベンダーのベースラインを超える追加的な基準を含めると、一部のベンダーが入札に参加できなくなり、最終的に調達者にとって選択肢が減ることになります。

RFP およびその後のクラウドフレームワーク契約の締結後、本フレームワークを締結した公共部門の組織は、必要な場合、自身が必要とするクラウドサービスを発注、すなわち「コールオフ」することができます。フレームワーク契約のもとでコールオフ契約を結ぶことにより、調達者は、フレームワーク契約下で提供されるメリットを維持しながら、コールオフのための機能仕様を追加し、要件を詳細化することができます。

必要と認められる場合には、特定のワークロードまたはプロジェクトに対して最良のサプライヤーを特定するためにミニコンペを開催することができます。ミニコンペとは、お客様がフレームワーク契約の下で更に競争をするもので、あるロット内のすべてのサプライヤーにある要件のセットに対応するように依頼するものです。お客様は、ロット内のすべての対応可能なサプライヤーに入札を依頼するため、クラウドサービス RFP の契約締結先には最低限の要件を設定して、各ロットのオプションに対して高い基準を確保することが重要です。

上記の図 1 の一覧の通り、ロットごとに一連の**異なる契約条件**があることは重要です。すべてのロットの契約について「万能なアプローチ」を求めることは、技術上の実現可能性と互換性に問題を生じさせることになります。

2.0 クラウドサービス RFP の概要

この節では、クラウドサービス RFP モデルと範囲について説明します。これには、戦略目標、参加者、定義、スケジュール、管理上の最低限の要件が含まれます。繰り返しますが、このハンドブックの焦点は**ロット 1 - クラウドテクノロジー**です。

2.1 クラウドサービス RFP の設定

クラウドサービス RFP を導入する際、公共部門の組織は大まかな目標および要件を明確にすることを強くお勧めします。

2.1.1 序文および戦略目標

戦略目標について明確化するためには、クラウドサービス RFP の序文で以下について明記することが推奨されます: (1) 組織がクラウドを使用して実現したいビジネス目標およびメリット、(2) 調達者、運用者、予算策定者など、フレームワーク契約の構成員、(3) クラウドの調達および利用の成功の核となる、公共部門とクラウドベンダー間の責任共有モデルの明確な理解、(4) クラウドサービス事業者 (CISP)、マーケットプレースサービスのディストリビュータ、コンサルティングパートナー、行政の調達/契約機関、および行政のエンドユーザー間で構築する関係のあり方。これらの 4 つのポイントを明確化することで、組織ごとの要件に適合した最適な RFP を作成できることに加え、お客様とベンダーの双方が RFP の成果物に関して明確に確認することができます。

クラウド RFP は、従来の IT RFP とは目的が異なります。クラウドテクノロジーは、単純に従来のコンピューティング手法に置き換わるものではなく、全く新しい方法でテクノロジーの利用を促進するものです。適切に設計されたクラウドサービス RFP は、公共部門組織が迅速にクラウドへ移行することでその利点を享受できるようにします。

クラウド調達を検討する際のベストプラクティスとして、責任共有モデルを明確に把握することが、最適なスタートポイントとなります。責任共有モデル[1] は多くの場合、クラウドのセキュリティおよびコンプライアンスの話をする際に使用されますが、ここでの責任の明確化はク

[1] クラウドインフラストラクチャサービスプロバイダー向けの CISPE 行動規範の 5 節を参照してください: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

ラウドテクノロジーのすべての側面に適用されます。クラウドサービス RFP では、クラウド環境における CISP の責任の範囲、およびお客様の責任の範囲を明確にする必要があります。たとえば、CISP はクラウド上で実行されるリソースやアプリケーションを監視する機能を提供します。**しかし**これらの機能を実際にどのように利用するかについてはお客様の責任となります。CISP は、大規模に運用するため、何百万ものお客様に個別に対応することは想定していません。

さらに、クラウド利用者は、お客様のクラウドの活用および責任の管理に CISP のパートナーネットワークがどのように役立つかを理解する必要があります。たとえば、クラウドマネージドサービスプロバイダー (MSP) は、お客様が CISP が提供する監視機能を設定および使用して、固有のコンプライアンスおよび監査要件を満たせるよう支援できます。

簡単に言うと、クラウドモデルの責任の所在は以下の通りです:

CISP はクラウドテクノロジーを提供

お客様はクラウドテクノロジーを活用

コンサルティング会社 (該当する場合) は、お客様のクラウドテクノロジーの入手および活用を支援

「コンサルティング会社」は、クラウド上のワークロードとアプリケーションの設計、建設、構築、移行、管理についてお客様を支援するコンサルティングおよびマネージド/プロフェッショナルサービス会社です。このような会社には、システムインテグレーター、戦略コンサルタント会社、代理店、マネージドサービスプロバイダー、付加価値再販業者が含まれます。

クラウドサービスの調達は、ホームセンターでの「買い物」に似ています。ホームセンターには、必要なものを作るために必要となる沢山の種類の材料やツールが揃っています。お客様は自分で選択して、キャビネット、スイミングプール、もしくは一軒家全てを作ることができます。材料やツールを購入する際、ホームセンターの従業員はガイダンスやノウハウは提供してくれますが、家に来てお客様のために何か作ってくれるわけではありません。そこで、いくつかの選択肢があります:

1. 材料やツールを自分自身で購入し、自分自身で何かを作る。
2. 材料やツールを自分自身で購入し、お客様のために、何かを作ると同時に/もしくは、作業をしてくれる 誰か と契約する。
3. お客様のために 何かを作る/作業をする 誰かと契約し、彼らの全体的な提供サービスの一部として、材料およびツールも含めて提供してもらう。

組織に、クラウド環境とソリューションを自ら構築し管理できる社内スキルがある場合、CISP の標準のクラウドテクノロジーとツールを利用するだけです (CISP を使って直接、または CISP の再販事業者を通して – **ロット 1** を参照)。必要な SaaS および PaaS ソフトウェアは、クラウドマーケットプレースで入手する必要があります (**ロット 2**)。 追加のコンサルティング、移行、実装、および/または管理の支援が必要な場合、CISP のパートナーネットワークを活用します (**ロット 3**)。

RFP のサンプル文書: 序文および戦略目標

クラウドコンピューティングを利用すると、公共部門の組織は、幅広い IT リソースを低コストな従量課金制で、柔軟にすばやく導入することができる。各組織は、最新の優れたアイデアを実現したり、IT 部門を運営したりする上で必要なタイプと規模のリソースをプロビジョニングすることができる。そのため、ハードウェアの大規模な投資や長期的なソフトウェアライセンス契約が不要になる。

<利用組織>は、幅広い関連組織全体の業務ニーズに対応するために、このような各種の商用利用可能なクラウドテクノロジーを利用する必要がある。

本 RFP の主な目的は、さまざまなクラウドテクノロジー、およびクラウド関連サービスを代表する最大**<x>**つのプロバイダーとの包括的な**<フレームワーク契約>**を並行して締結することである。

1. **ロット 1.** クラウドテクノロジーの購入先のクラウドサービス事業者 (CISP) または CISP の再販事業者
2. **ロット 2.** マーケットプレースサービスのプロバイダー
3. **ロット 3.** クラウドへの移行および CISP の提供サービスを活用するために必要となる追加のノウハウを提供するコンサルティングサービスのプロバイダー

ロット 1 について、入札する事業者 (CISP または CISP の再販事業者) は、提案する製品が以下の目的に合致していることを実証する必要がある:

- **俊敏性** – エンドユーザーは IT リソースを、従来の週および月単位のスケジュールではなく、分単位で利用できる。
- **イノベーション** – 市場で最新かつ最も革新的なテクノロジーにすばやくアクセスできる。
- **コスト** – 資本的支出から変動費に転換 (例; 資本的支出から運用経費へ)。消費した量のみの支払い。
- **予算編成** – 請求および使用状況の情報を詳細レベルと概要レベルの両方で表示し、将来の支出の予測に加えて、長期にわたる支出のパターンを視覚化できる。
- **弾力性** – クラウドによって提供される大きな規模の経済によって、変動費の削減を実現できる。
- **キャパシティー** – インフラストラクチャのキャパシティーのニーズを予測する必要がない。
- **データセンターへの依存は不要** - サーバーの重いラック作業、積み重ね作業、電源供給といった重労働がなくなり、市民のための業務に集中できる。
- **セキュリティ** – リソースの高い可視性と監査対応能力を備えたアカウント設計が定型化されており、施設および物理ハードウェアを保護するためのコストは不要。
- **責任共有** - ホストオペレーティングシステムや仮想化レイヤーから、サービスが稼働する施設の物理セキュリティにまで、CISP が運用、管理、制御するため、運用負荷が軽減される。
- **自動化** – クラウドアーキテクチャに自動化を組み込むことで、より安全かつ迅速に、高いコスト効率でスケールすることができる。
- **クラウドガバナンス** – (1) すべての IT の資産の棚卸しから始め、(2) これらの資産をすべて一元的に管理し、(3) 利用状況/請求/セキュリティなどに関するアラートを作成できる。また、すべてに資産のトラッキング、棚卸し管理、変更管理、ログ管理および分析、全体的な可視性およびクラウドガバナンスの機能が備わっている。
- **統制** – IT サービスの消費の状況、およびセキュリティ、信頼性、パフォーマンス、コストの調整が可能な部分を完全に可視化できる。
- **可逆性** – ポータビリティツールおよびサービスにより、CISP のインフラストラクチャへの移行および CISP のインフラストラクチャからの移行が可能なほか、ベンダーロックインを最小限に抑え、業界の行動規範を遵守できる。

- **データ保護** – クラウドインフラストラクチャサービス専用の業界行動規範である CISPE データ保護行動規範を通して、一般データ保護規則 (GDPR) に対するコンプライアンスを実証することができる。
- **透明性** – 顧客は、自身のデータの処理および保管に使用されるインフラストラクチャの場所 (地域) を知る権利を持つ。
- **気候中立** – 利用者は、2030 年までに気候中立目標を達成するために実証された具体的な手段を講じており、気候中立的データセンター協定に同意している CISP を利用する必要がある。これにより、利用者は自身の気候中立目標を達成できる。

2.1.2 RFP の回答スケジュール

クラウドフレームワーク契約および関連するクラウドサービス RFP を作成する際に、予想される入札アクティビティのスケジュールを入札者に提供することをお勧めします。業界との関わりが深いほど、RFP の要件についてすべての関係者が明確に理解し、実際にすべてのベンダーサービスがどのようにクラウドサービスモデルに適合しているかを把握するのに役立ちます。

RFP のスケジュールは現地の法律および法的義務に従うことに注意してください。以下に示すリストは、規範的な作業項目や時間軸ではなく、ベストプラクティスガイドとしての活用を意図したものです。

RFP のサンプル文書: 回答スケジュール

クラウドサービス RFP については、以下の RFP スケジュールを参照すること。:

クラウドサービス RFP のスケジュール
• **情報提供依頼書 (RFI) の発行:** • **RFI の回答:** • **提案依頼書 (RFP) のドラフトの発行:** • **ドラフト RFP の回答期限:** • **業界の相談フェーズ: <スケジュール>** • **事前資格 (pre-qualification) RFP の発行:** • **事前資格 RFP の回答:**

- **RFP の発行:**
- **第 1 回質問の期限:**
- **第 1 回回答:**
- **第 2 回質問の期限:**
- **第 2 回回答:**
- **RFP 回答期限:**
- **提案の明確化期間:**
- **交渉期間:**
- **締結予定日:**
- **契約締結:**
- **契約期間 (延長オプション) :**

RFP のスケジュールは現地の法律および法的義務に従うことに注意してください。以下に示すリストは、規範的な作業項目や時間軸ではなく、ベストプラクティスガイドとしての活用を意図したものです。

2.1.3 定義

クラウドサービス RFP には、定義の詳細リストを加える必要があります。このリストには、ベンダーの役割 (クラウドサービス事業者、クラウド再販事業者、ベンダーパートナーなど)、一般的な技術概念 (コンピューティング、ストレージ、IaaS/PaaS、SaaS)、および契約の他の主要な部分が記載されます。以下は定義リストのサンプルです:

RFP のサンプル文書: 定義

米国国立標準技術研究所 (NIST) によるクラウドコンピューティングの定義を以下に示す。[2]

- **サービスとしてのインフラストラクチャ (IaaS).**利用者に提供される機能は、処理、ストレージ、ネットワーク、およびその他の基本的なコンピューティングリソースをプロビジョニングする機能であり、利用者はオペレーティングシステムやアプリケーションを含む任意のソフトウェアをデプロイして実行できる。利用者は、基盤となるクラウドインフラストラクチャの管理または制御は行わないが、オペレーティングシステム、ストレージ、デプロイされたアプリケーション、

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

場合によっては、選択したネットワーキングコンポーネントの限定的な制御ができる (ホストファイアウォールなど)。

- **サービスとしてのプラットフォーム (PaaS)。** 利用者に提供される機能は、プロバイダーがサポートするプログラミング言語、ライブラリ、サービス、ツールを使用して利用者が作成した、または購入したアプリケーションをクラウドインフラストラクチャにデプロイすることである。3 利用者は、ネットワーク、サーバー、オペレーティングシステム、またはストレージを含む基盤となるクラウドインフラストラクチャの管理または制御は行わないが、展開されたアプリケーションと、場合によってはアプリケーションのホスティング環境の構成設定を制御できる。

- **サービスとしてのソフトウェア (SaaS):** 利用者に提供される機能は、クラウドインフラストラクチャ上で実行されているプロバイダーのアプリケーションを使用することである。さまざまなクライアントデバイスから Web ブラウザ (例: Web ベースの電子メール) などのシンクライアントインターフェイス、またはプログラムインターフェイスのいずれかを介してアプリケーションにアクセスできる。利用者は、ネットワーク、サーバー、オペレーティングシステム、ストレージ、さらには個々のアプリケーション機能など、基盤となるクラウドインフラストラクチャの管理または制御を行わないが、例外的に、ユーザー固有のアプリケーション構成設定は行う場合がある。

- **パブリッククラウド。** クラウドインフラストラクチャは、一般社会に開放された利用を目的にプロビジョニングされている。パブリッククラウドは企業、学術機関、行政機関、またはそれらの複合体によって所有、管理、運営されている場合がある。パブリッククラウドはクラウドサービス事業者の構内に存在する。

- **コミュニティクラウド。** クラウドインフラストラクチャは、課題 (ミッション、セキュリティ要件、ポリシー、コンプライアンスの考慮事項など) を共有している組織の利用者の特定のコミュニティが独占的に使用する目的でプロビジョニングされる。コミュニティ内の 1 つ以上の組織、サードパーティ、またはそれらの複合体によって所有、管理、および運用される場合があり、構内または構外に存在する。

- **ハイブリッドクラウド。** クラウドインフラストラクチャは、2 つ以上の異なるクラウドインフラストラクチャ (プライベート、コミュニティ、またはパブリック) で構成されるが、標準化された技術または独自技術によって結合されており、データおよびアプリケーションの移植が可能である (例: クラウド間の負荷分散のためのクラウドバースティングなど)。

- **プライベートクラウド。** クラウドインフラストラクチャは、複数の消費者で構成される単一の組織が独占的に使用する目的でプロビジョニングされる (事業部など)。プライベートクラウドはその組織、サードパーティ、またはそれらの複合体によって所有、管理、および運用される場合があり、構内または構外に存在する。

2.1.4 本フレームワーク契約の購入モデルおよび競争に関する詳細な説明

上記のように、公共部門の組織は、フレームワーク契約のモデルついて、クラウドテクノロジー、関連する実装・管理サービスの購入の仕組みがどのように運用されるかを示す必要があります。これは、クラウドテクノロジーのベンダー、関連するコンサルティングサービス企業、マーケットプレイスのディストリビュータ、および購買部門がそれぞれの役割を把握できるように、クラウドサービス RFP 上に明確化する必要があります。

フレームワーク契約の範囲、コールオフ契約、またはミニコンペに関して、各組織は次のことを考慮する必要があります:

- クラウドテクノロジーの利用に関するインテグレーションやマネージドサービスの契約上の責任者は誰か。
- CISP との契約関係の維持、一括請求サービスの提供、およびクラウドサービスの利用に関連する使用データや請求データにタイムリーかつ直接アクセスすること以外に、付加価値サービスを提供する CISP の再販事業者/パートナーの要件はあるか?
- フルサービスの付加価値再販業者、システムインテグレーター、マネージドサービスプロバイダー、または何らかの形態の IT に対する役務の要件はあるか?

CISP はシステムインテグレーター (SI) またはマネージドサービスプロバイダー (MSP) ではないことに注意することが重要です。多くの公共部門のお客様は、CISP に対して IaaS/PaaS を求めており、コンサルティングおよび「キーボードの操作を伴うような」計画、移行、および管理作業は、SI または MSP に外部委託しています。以下の **図 2** は、クラウドサービスモデルの役割と責任の概要を表しています。

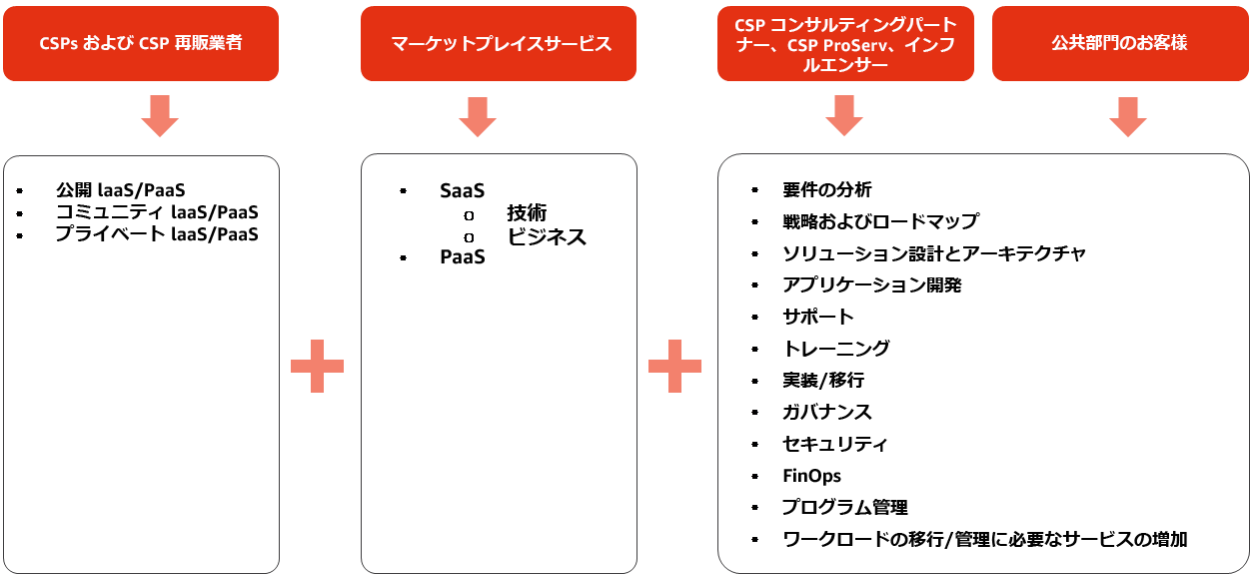

図 2 – クラウドサービス RFP では、必要となるすべてのクラウドサービスのメニューをエンドユーザーに提供する必要があります。公共部門のお客様は、CISP に対してクラウドテクノロジー、必要に応じて PaaS および SaaS 製品のマーケットプレイスを求めています。その後でお客様は、クラウドサービスの提供で引き受ける役割の大きさ、およびコンサルティング会社/システムインテグレーター/マネージドサービスなどへどれだけの規模を外部委託するかを判断できます。

以下のサンプル文書は、上記の 図 2 に示す役割と責任をもとに作成されています。クラウドフレームワーク契約および関連するクラウドサービス RFP では、調達者が各ベンダーの提供サービスを適切に評価できること、およびワークロード/プロジェクトに必要なサービスを選択できることを保証する必要があります。最適な対応は、既に説明したようにサービスをロットに分割し、フレームワーク契約においてコールオフ契約およびミニコンペがどのように実施されるかを明確化にすることです。

RFP のサンプル文書: 購入モデル

この契約は**フレームワーク**の購入手段の役割を担う。このクラウドフレームワーク契約は、<**利用組織**>によって定義されたクラウドテクノロジー、関連するマーケットプレースサービス/製品、コンサルティングサービス、プロフェッショナルサービス/システムインテグレーション/マネージドサービス/移行のプロフェッショナルサービス、トレーニングおよびサポートに関する<**利用組織**>によって定義された複数の**ロット**で構成され、<**利用組織**>と関連する資格を持つ複数の購入者によって使用される。これにより、調達プロセスが簡素化されると同時に、規模の経済も最適化される。

このフレームワーク契約が一旦締結されると、各組織は、個別の調達による購入とは異なり、必要なときに希望する特定のクラウドテクノロジーやクラウド関連サービスを購入することができる。このようなアプローチにより、管理的な要件が軽減され、調達の複雑さとサイクルタイムが大幅に削減される。

フレームワーク契約の期間は、あらゆる更新を含めて最大<X>年となる。フレームワークのコールオフ契約の最大期間は通常<x>か月である。これは契約の延長の必要に応じて、適切な内部承認を得ることで<x>か月、さらに<x>か月延長することができる。このことは、各個別の**コールオフ契約**に明記される。

フレームワークは 3 **つのロット**に分割される。

1. **ロット 1: クラウドテクノロジー** - クラウド提供者のテクノロジーの全範囲 (CISP から直接、CISP の再販事業者から、付加価値サービス/サポートを持つ再販事業者から):
    i. IaaS **および** PaaS **サービス** - クラウドテクノロジーのメニュー、たとえばコンピューティング、ストレージ、ネットワークキング、データベース、分析、アプリケーションサービス、デプロイ、管理、開発者、モノのインターネット (IoT) など。DR/COOP、アーカイブ、ビッグデータおよび分析、DevOps などのパッケージ化されたクラウドテクノロジーソリューションも含まれる。
2. **ロット 2: マーケットプレイス** – PaaS および SaaS サービス/製品の全範囲、たとえば経理、CRM、設計、HR、GIS とマッピング、HPC、BI、コンテンツ管理、ログ分析など。
3. **ロット 3: クラウドコンサルティング** – クラウドへの移行と利用に関するコンサルティングサービス (マネージドサービス、プロフェッショナルサービス、アドバイザリー/コンサルティングサービス、付加価値サービス、FinOps、技術サポート) の全範囲。これらのサービスには、計画、設計、移行、管理、サポート、QA、セキュリティ、トレーニングなどが含まれる。

ベンダーは提供サービスを複数のロットに提出することができる。

ベンダーは提供サービスおよび関連する料金表を任意のフォーマットで提出できる。

フレームワーク内の競争およびコールオフ契約の締結

コールオフ

フレームワーク契約の当事者である公共部門の組織は、必要なときに必要なサービスを発注 (「コールオフ発注」) できる。フレームワーク契約の下にコールオフ契約を結ぶことにより、調達者は、フレームワーク契約下で得られるメリットを保ちながら、コールオフ契約の追加の機能仕様を使って要件を詳細化できる。

フレームワーク契約を通じて締結された契約では、各ロット内のサプライヤーの選択で使用される要件について、明確な監査証跡を提示することができる。最終調達者は、早期の市場への関与、明確化のための質問、電子メールおよび対面での会話など、ベンダーとのコミュニケーションの記録を保持する。

1.コールオフの要件の作成、および調達の内部承認の要求

フレームワーク契約を利用する資格のあるすべての最終調達者は、ビジネスエンドユーザー、調達スペシャリスト、技術専門家の共同チームを作り、「必須」と「希望」のリストを作成する。これらの要件は、適用可能なロットおよび、要件を満たすのに最適なベンダーの決定に役立つ。要件を作成する際、調達者は以下について考慮すること:

- サービスを使用するために利用可能な資金
- プロジェクトの技術要件および調達要件
- 選択のベースとなる基準

2.サービスの検索

フレームワーク契約の下、調達者はオンラインフレームワークカタログ(資格を持つフレームワーク契約の締結者およびそのサービスが一覧になっているポータル)を使用して個別のニーズに合致する製品/サービスを見つける。適切なロットを選択し、サービスを検索する。

3.サービスのレビューおよび評価

フレームワーク契約に基づく調達者は、サービスの説明を確認して、要件と予算の両方に基づいてニーズに合致した最適なサービスを検索する。各サービスの説明には以下の内容が記載される:

- サービス定義文書またはサービス定義へのリンク
- 契約条件の文書

- 料金表の文書 (完全な料金の一覧/料金表の文書が要求に応じて入手可能であれば、公開されている料金表へのリンクでも)

料金は、最も一般的なサービス構成のコストになる。ただし、通常、価格設定は数量によって異なるため、調達者は常にサプライヤーの料金表、または公開されている料金表、および価格計算ツールを使用して、購入対象の実際の価格と購入者に提供される全体的な価値を算出する必要がある (たとえば、最適化のサービスによるコスト削減)。

フレームワーク契約に基づく調達者は、サービスの説明、契約条件、価格設定、またはサービス定義文書/モデルの説明をサプライヤーに求めることができる。サプライヤーとのすべてのやりとりの記録は保持される。

4.サービスの選択と契約の締結

単一ベンダー

要件を満たしているベンダーが 1 つのみの場合、その対象と契約を締結することになる。

複数ベンダー

候補リストに多数のサービスがある場合、調達者は最も経済的に有利な入札 (MEAT) のサービスを選択することになる。MEAT ベースの評価については、以下の表の基準を参照。調達者は、使用するにあたっての詳細な特徴、およびそれらにどう重きを置くか指定することができる。

調達者は場合により以下のことを行う必要がある点に注意が必要:

- さまざまなサプライヤーを組み合わせて確認する
- ボリューム割引または企業割引、およびベンダーによるコスト最適化サービスに関する具体的な情報を取得する

サプライヤーの評価は常に公正かつ透明でなければならない。選択は最適なものを基準として実施し、プロジェクトの要件を参照せずにベンダー/サービスを除外しないこと。

表 2 - MEAT ベースの評価

締結基準
生涯コスト: 費用対効果、価格、そしてランニングコスト
技術的なメリットおよび機能的な適合性: 該当するサービスレベルで指定されているカバー範囲、ネットワーク容量、パフォーマンス
アフターサービス管理: ヘルプデスク、ドキュメント、アカウント管理機能、さまざまなサービスの提供の保証
非機能の特徴

ミニコンペ

必要と認められる場合には、特定のワークロードまたはプロジェクトに対して最良のサプライヤーを特定するためにミニコンペを開催することができます。ミニコンペとは、お客様がフレームワーク契約の下で更に競争をするもので、あるロット内のすべてのサプライヤーにある要件のセットに対応するように依頼するものです。顧客は、定められたロット内の能力を持つすべてのサプライヤーを入札に招待する。詳細な比較情報は以降の、技術、セキュリティ、価格設定/価値に関する以下の節を参照すること。

契約

サービスを使用する前に、調達者とベンダーの両方が契約書のコピーに署名する。フレームワークの契約の最大期間は通常<x>か月である。これは契約の延長の必要に応じて、適切な内部承認を得ることで<x>か月、さらに<x>か月延長することができる。

サービスを使用する前に、すべての関係当事者 (調達者およびサプライヤー) が契約書の写しに署名する必要がある。

2.1.5 入札者の最低限の要件 - 管理

シンプルで明確な文言でフレームワーク契約の資格基準を設定することにより、従来のソリューションを「クラウド」と称してパッケージ化している、従来のデータセンターやハードウェアプロバイダーからの入札が行われないようにすることできます。 RFP の参加者は、以下の入札者の管理上の最低限の要件をどのように満たすかを示す必要があります。

繰り返しになりますが、この文書は**ロット 1- クラウドテクノロジー**に焦点を当てています。ただし、要件と RFP スコープの観点から全体的なコンテキストを補完できる場合、**ロット 2 - マーケットプレイス**および**ロット 3 - クラウドコンサルティング**に関する追加情報を記述しました。

たとえば、CISP の再販事業者/MSP/SI/コンサルティング会社などの最低限の資格基準を記載することは重要であり、これによって次のことを確認できます、(1) 再販事業者またはチャネルパートナーとして CISP と直接提携していること、(2) サードパーティの組織に対しての CISP の提供サービスへの直接アクセスの再販を CISP が認定していること、(3) 能力および専門知識を示す、CISP による認定資格があること。

RFP のサンプル文書: 入札者の最低要件 - 管理

このフレームワーク契約によって、次のカテゴリの複数のベンダーとの契約が締結される。ベンダーは、民間の CISP、CISP のサードパーティの再販事業者、マーケットプレースサービスのディストリビューター、および/または CISP 活用のためのサービス (例: コンサルティング、移行サービス、マネージドサービス、FinOps など) のプロバイダーでなければならない。入札する役割を明確化すること。

ロット 1

____ - パブリッククラウドサービス (IaaS および PaaS) の直接のプロバイダー (CISP)

____ - コミュニティクラウドサービス (IaaS および PaaS) の直接のプロバイダー (CISP)

____ - プライベートクラウドサービス (IaaS および PaaS) の直接のプロバイダー (CISP)

____ - CISP のサードパーティの再販事業者 (CISP のオンラインクラウド提供サービスへのアクセスを直接提供可能)

- そのサービスへの直接アクセスが再販可能な、CISP の提供サービスを明記すること: _____
- CISP の提供サービスの認定再販事業者であることを示す CISP からのレターを提示すること: _____

ロット 2

____ - CISP 上で実行するマーケットプレースサービスの直接のプロバイダー (PaaS および/または SaaS)

____ - CISP 上で実行するマーケットプレースサービスのディストリビュータ (PaaS および/または SaaS)

ロット 3

____ - プロフェッショナルサービスを提供する CISP

____ - CISP の技術サポートを提供するプロバイダー

____- CISP 上で利用または運用するサービスを提供する CISP のパートナー

____- CISP 上で利用または運用するサービスを提供する斡旋者/顧問

提供サービスの種類を明記すること:

- CISP 上のワークロードのマネージドサービス (Y/N): _____
  - 該当する場合、専門性を明記すること: _____
- プロフェッショナルサービス: (Y/N): _____
- コンサルティング – トレーニング (Y/N): _____
- コンサルティング – 戦略 (Y/N): _____
- コンサルティング – 移行 (Y/N): _____
- コンサルティング – クラウドガバナンス (Y/N): _____
- コンサルティング – FinOps (Y/N): _____
- コンサルティング – その他 (明記すること): _____

サービスを提供する対象の CISP を明記すること: _____

CISP モデルにおける CISP からのパートナー指定を裏付けるレターを提示すること: _____

ロット 1 の管理上の最低限の要件

クラウドサービス事業者 (CISP)

CISP の資格を得るには、以下の要件に適合する必要がある。

提案する CISP の資格基準	理由
組織の詳細、たとえば名前、法体系、登録/DUNS 番号、VAT など	

会社の規模、経済および財政状況[3]	顧客は、CISP が契約を遂行できることを判断できる。
除外基準として、犯罪/詐欺行為、など。	
ケーススタディ/顧客リファレンス (必要な数/種類を指定)	顧客は、必要なサービスを提供するための CISP の実績を判定できる。
企業の社会的責任	これらは、CISP が提供する公的にアクセス可能なバージョンである必要がある。
公的に入手可能な持続可能性に関するコミットメントおよび実践内容。	顧客は、CISP が可能な限り最も環境に優しい方法でビジネスの運営に取り組んでいることを確認できる。
CISP は、特に PaaS、機械学習と分析、ビッグデータ、マネージドサービス、クラウド利用の最適化機能の分野で、過去 5 年間にわたって新しく有用なサービスと機能を革新し、リリースした実績を提供する必要がある。本点を証明するには、公的にアクセス可能な変更ログ、または更新情報を使用できる。	CISP は新製品を迅速に顧客の手に届くよう取り組み、その後、製品を頻繁に繰り返し更新し、改善していることを実証する。これにより、顧客は資本を増やための投資を行うことなく、最先端の IT インフラストラクチャを維持できる。

CISPと再販事業者/パートナーとの関係

<利用組織>は、主契約者に対して、再販事業者またはチャネルパートナーとして CISP と直接提携していて、サードパーティの組織に対する CISP 提供サービスへの直接のアクセスの再販が CISP によって認定されていることや、能力や専門知識を保有することが CISP によって認定されていることを求める。これにより、**<利用組織>**は、**フレームワーク契約**の主契約者と CISP 間の下請け契約という追加的なレイヤーに関連する契約条件およびサービスを確認する必要がなくなる。また、この要件によって、(1) **<利用組織>**がデューデリジェンスを実施して、提供を受けるサービスに関する明確な責任の分担を確認する場合、および (2) **<利用組織>**がクラウドサービスの利用に伴う日々の管理業務を実施する場合に、追加的な再販事業者のレイヤーによって発生する複雑さが軽減される。

[3] クラウドサービス RFP では、企業の従業員数や社内の従業員チームの構成に注目するのではなく、全体的な会社情報に注目することに注意してください。クラウドテクノロジーでは、サービスパフォーマンスの保証と従業員数に相関関係はありません。代わりに、クラウド RFP においては、要件 (適切な規模)、実績/パフォーマンスを満たす会社全体の規模に注目します。

2.2 技術

クラウドサービス RFP では、お客様向けにカスタマイズされたソリューションを構築するために必要となる標準的なクラウドテクノロジーの提供を求めることで、CISP の評価基準を引き上げることが推奨されます。前述のように、標準化された技術とカスタマイズされた技術の違いは、クラウドサービス RFP にアプローチする際に非常に重要です。CISP は非常に多くのお客様に標準化されたサービスを提供しているため、クラウドサービス RFP のカスタマイズでは、さらに高い価値を創造するソリューションや成果が重視されます。これはソリューションの成果達成のために使用される基本的な手法、インフラストラクチャ、またはハードウェアとは異なります。

2.2.1 最低限の要件

従来の IT 調達はしばしば、組織が現在どのように業務を行なっているかを文書化する一連の作業セッションを通じて作成された、業務要件に基づくものでした。何も問題のない状況で、こうした要件を適切に抽出することは困難なプロセスです。仮にうまくいった場合でも、こうした要件セッションでは、それ自体が時代遅れで非効率な場合がある過去の業務プロセスを文書化しています。これらの要件が、CISP によって複製されるべき RFP に組み込まれた場合、唯一のソリューションはカスタムメイドなソリューションとなる可能性があります。このようなモデルは、クラウド調達とは相性がよくありません。

公共部門の組織は、業務目標と性能に関する要件を把握する必要がありますが、システムの設計と機能を縛るような RFP を策定してはいけません。反対に、各組織は業務に最適なものを求めるような調達にする必要があります。各組織は、サービスの成功につながらないかも知れない多数の項目が規定された要件をベースに、提案書を評価するのではなく、テクノロジーや関連するサービスが業務目標にどのように適合し改善するか、性能要件が達成できるかどうか、および構成によって業務ルールを微調整できるかどうかなどの要件をベースにした評価基準を設けることを推奨します。

クラウド RFP では、最適なソリューションを得るために適切に質問をすることが求められます。クラウドモデルでは物理的な資産を購入しないことを考えると、結果として従来のデータセンターの多くの調達要件は適用されません。**データセンターの質問をリサイクルして使用すると、必然的にデータセンターの回答につながるため、**CISP が入札できなくなるか、公共部門のお客様にとってクラウドの全ての機能とメリットを引き出せない不適切な設計の契約となります。

クラウドサービス RFP は、CISP とクラウドサービスに求められる鍵となる要件に焦点を当てており、ロット 1 の資格を持つベンダーが高い評価基準を達成できることを保証します。また、公共部門が資格を持つ幅広い範囲の CISP にアクセスすることを妨げないように、規範的な要件にし過ぎることは避けるべきです。

RFP のサンプル文書: クラウドサービス事業者の能力

ロット 1 については、上記の CISP の管理上の最低要件も参照すること。

提案する CISP の資格基準	理由
インフラストラクチャ	
CISP のインフラストラクチャは、2 つ以上のデータセンターのクラスタで提供されている必要がある。 各クラスタは低遅延のリンクで接続されており、可用性が高いアクティブ/アクティブ構成の展開および、DR-BC シナリオの実施が可能な 2 つ以上のデータセンターで構成されている必要がある。各クラスタを構成するデータセンターは、物理的に分離され、相互の障害とは独立している必要がある。	CISP は、単一障害点を回避可能であり、高可用性アプリケーションを構築することに適したインフラストラクチャを提供できること。
CISP は、論理的および地理的に分離されたリージョンを提供する必要がある。顧客データは、CISP によって指定されたリージョン外に複製されてはならない。	データの保管場所の要件においては、顧客が自身のデータの場所を完全に制御できることが義務付けられている。

CISP は、CISP データセンター間の直接接続できる専用線でのプライベート接続を提供できる必要がある。	プライベート接続は、ハイブリッドでセキュアなインフラストラクチャの構築を実現するための基本的な要件である。
CISP は、転送中のデータの暗号化を含む十分な仕組みを備えている必要がある。	顧客は、暗号化されていないデータは転送できない機能を要求することができる。
CISP の最低認定資格	
CISP は ISO 27001 規格の認証を受けている必要がある。	サードパーティによる監査、認証、認定を通して、顧客は品質、安全性、信頼性についてサービス (特にプラットフォーム) をベンチマークできる。最低限の認定資格を満たしていることが不可欠である。
iCISP は、顧客が iGDPRi 準拠のアプリケーションを構築できるように、iGDPRi に準拠して利用可能な機能やサービスを提供するために、iCISPEi データ保護行動規範に準拠している必要がある。	顧客が GDPR に準拠したアプリケーションを構築または実行できること。
CISP は、CISP の統制および手続きに関する透明性を確保するために、SOC 1 や SOC 2 レポート (EC が使用する拠点やサービスをカバー) などの第三者の独立監査人が監査したレポートを準備する必要がある。	CISP は、アプリケーションの動作および管理の方法に関して透明性を持つこと。SOC レポートは、信頼と透明性の確保に役立つ。
CISP は気候中立データセンター協定に準拠している必要がある。	気候中立データセンター協定は、CISP が 2030 年までに気候中立を実現し、それによりユーザーが独自の持続可能性目標に対応できるように促す。FTE (非 SME) が 250 人を超えているプロバイダーでは、第三者の監査人が必須である。
CISP は SWIPO IaaS ポータビリティ行動規範に準拠している必要がある。	SWIPO IaaS ポータビリティ行動規範により、サービスが非個人データの自由流通規則の第 6 条「Data Porting」に準拠できるようになる。
サービスの特徴	
CISP のインフラストラクチャは、プログラムインターフェイス (API) および Web ベースの管理コンソールからアクセスできる必要がある。	セルフサービスアクセスとプログラムインターフェイスは、CISP プロバイダーに求められる標準機能であり、ユーザーアクセスおよびプロバイダー自身の仲介をできる限り排除できる。

CISP は、オブジェクトストレージ、管理されたリレーショナルデータベース、管理された非リレーショナルデータベース、管理されたロードバランサー、監視、統合されたオートスケーリングなどの基礎となるサービスセットを提供する必要がある。	単に仮想マシンを提供するだけでは、プロバイダーをクラウドサービス事業者として認定するには不十分である。クラウドサービス事業者は、顧客のアプリケーションを加速および改善するために、PaaS および IAAS サービスのセットを提供する必要がある。
CISP は、顧客がサービスの使用と構成を自由に変更できるようにするか、CISP の内外でデータを移動できるようにする必要がある (セルフサービスの提供)。	サービスおよびデータへのセルフサービスアクセスは、顧客の完全な独立が可能になる厳しい要件である。
CISP は、サービスの「従量制」課金を許可する必要がある。	従量課金を採用することで、顧客は、短い期間のみ使用するアプリケーションや、PoC のワークロードのコストを最適化し、リスクを最小限に抑え、CISP を活用できる。
データおよびシステムセキュリティ	
CISP は、顧客自身のデータのフルコントロールを顧客に許可し、顧客がデータの保管場所 (都市圏) を自由に選択できるようにし、顧客自身によって移動が開始された場合のみ、そのデータが移動されることを保証する必要がある。	顧客は、データの保存場所、コンテンツへのアクセスの管理方法、およびサービスとリソースへのユーザーアクセスを制御できる必要がある。
CISP の特性上、顧客は自身のデータおよびシステムの機密性、完全性、可用性など、自身のセキュリティポリシーを完全に制御できる必要がある。	顧客は、ワークロード全体に対してセキュリティ基準を定義および実装できなければならない。プロバイダーが顧客のデータを使って「正しいことをする」と信頼するだけでは不十分である。
コスト管理	
CISP には、顧客が長期にわたって支出を監視できる仕組みとツールが必要である。ツールは、ワークロード、サービス、およびアカウントに基づいてコストの基本的な区分ができる必要がある。	
CISP は、コストのしきい値を超えた場合に顧客にアラートを出すツールを提供する必要がある。	

CISP は顧客に詳細な請求書を提供しなければならない。コストをワークロード、環境、アカウント別に分類できるよう請求書を構成できなければならない。	

また、CISP は、以下の技術要件の質問に対する回答も提供すること。

ソリューション

CISP は次のソリューションについて、CISP 上でホストされている、または CISP と統合されている事前作成のテンプレートやソフトウェアソリューションを提供する方法を示すこと:

- ストレージ
- DevOps
- セキュリティ/コンプライアンス
- ビッグデータ/分析
- 業務アプリケーション
- 通信 & ネットワーキング
- 地理空間
- IoT
- [その他]

次のワークロードについて、CISP の対応状況の概要を記入する:

- 災害対策
- 開発とテスト
- アーカイブ化
- バックアップと復元
- ビッグデータ
- 高性能コンピューティング (HPC)
- IoT
- Web サイト
- サーバーレスコンピューティング
- DevOps
- コンテンツ配信
- [その他]

2.2.2 ベンダー間の比較

クラウドサービス RFP では最低限の要件に加えて、競争評価時に CISP のテクノロジーを比較できる基準を提供することが重要です。

クラウドサービス RFP では、ソリューションの構築に向けて、利用者が使用する機能を理解した上で、組織に必要なクラウド機能を要求する必要があります。CISP が標準的に提供する機能を超える機能 (CISP の構築済みソリューションや自動化機能など) は、クラウドサービス RFP の「付加価値オプション」または「ベストバリュー」などとして、さらに有益な分析のために利用できます。

公共部門はしばしば、最高の価値、最も経済的に有利な入札 (MEAT)、または最低価格などの評価基準を使用し、入札者間の競争性を確保します。公共部門の組織は、クラウドサービス RFP のこの部分を計画する際に、クラウドに固有の機能を考慮したアプローチを構築することが重要になります。たとえば、クラウドサービス事業者の提供サービス間 (コンピューティングやストレージなど) のラインアイテムを単純に比較することは、提供サービスを比較する上で効率的な方法ではありません。代わりに、上記の節 2.2.1 に記載されているような大まかなソリューションに焦点を当てることが非常に重要となります。また、公共部門の組織は、付録 A – 入札者相互間の比較に関する技術的要求事項に記載されているような、クラウド固有の要件を参考にすることができます。

RFP には、クラウドソリューションを構築するために必須となるクラウドの特徴を記載する必要があります。これを行うには、公共部門の組織は、サードパーティの分析レポートの使用に加えて、アメリカ国立標準技術研究所 (NIST) の「クラウドの必須の特徴」を活用することで、その CISP が大規模な運用に最適な「真のクラウド」の提供サービスであることが確認できます。

RFP のサンプル文書 - ベンダー間の比較

クラウドサービス事業者は、**付録 A** 内のすべての技術的要件の質問に対して回答を記入する必要がある。

応札者は次の機能を備えていることに加え、クラウドサービスを提供することでクラウドコンピューティングの 5 つの必須の特徴をどのように満たすかを説明する必要がある[4]。

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

1) **オンデマンドセルフサービス**: 応札者は、各サービスプロバイダーとの人的なやりとりを行うことなく、必要に応じて自動的にサーバー時間やネットワークストレージなどのコンピューティング能力を利用者の操作により一方的にプロビジョニングする機能を提供する必要がある。応札者は、利用者の操作により (つまり、ベンダーの確認や承認が不要) サービスを一方的にプロビジョニングするための注文アクティビティ用の機能を提供する必要がある。提示する提供サービスまたはオファーにおいて、この部分の動作の仕組みを説明する必要がある。

2) **ユビキタスなネットワークアクセス**: 応札者は複数のネットワーク接続オプションを提供し、その 1 つはインターネットベースに存在する必要がある。提示する提供サービスまたはオファーにおいて、この部分の動作の仕組みを説明する必要がある。

3) **リソースプーリング**: 応札者の CISP は、利用者のニーズに応じて動的に割り当ておよび再割り当てされるさまざまな仮想リソースとともにマルチテナントモデルを採用して複数の顧客にサービスを提供する、プールされたコンピューティングリソースを提供する必要がある。利用者は、高い抽象化レベルで場所を指定できる (国、地域、データセンターの場所など)。応札者は、プロビジョニング要求から数分または数時間以内にこれらのリソースのスケーリングに対応する必要がある。提示する提供サービスまたはオファーにおいて、この部分の動作の仕組みを説明する必要がある。

4) **迅速な弾力性**: 応札者の CISP は、サービスのプロビジョニングおよびプロビジョニング解除機能 (スケールアップおよびスケールダウン) をサポートしており、プロビジョニング要求後、最小規定時間 (最大「x」時間) 以内にサービスが利用できる必要がある。i 応札者は、1 時間ごとまたは日次ベースで、これらのプロビジョニング要求に起因する請求調整をサポートする必要がある。

5) **測定サービス**: 応札者は、オンラインダッシュボードまたは同様の電子的手段を介してサービスの使用状況を可視化できる必要がある。

さらに、CISP は以下に対応する必要がある:

- IaaS に関するガートナーのマジッククアドラント[5]での評価において、クラウドサービスの提供におけるリーダーの位置付け
- CISP の実績ある機能および信頼性を証明するために、業界で認められているサードパーティのアナリストレポートの提供する。

最後に、CISP は付録 B に記載されているシナリオを用いて比較される。

[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

2.2.2.1 サービスレベルアグリーメント (SLA)

CISP は、多数のお客様向けに標準化された商用 SLA を規定しているため、オンプレミスのデータセンターモデルの場合のように、カスタマイズした SLA は提供できません。ただし、CISP のお客様 (多くの場合、CISP のパートナーの支援を受けて) は、CISP の商用 SLA を活用して、お客様固有の要件と独自の SLA を満たす、あるいは上回るように、自身のクラウド利用を設計することができます。

個々のエンドユーザーが性能や可用性の要件を満たせるように、クラウドサービス RFP では、各サービスや商用 SLA を活用するために必要となる機能とガイダンスが CISP から提供されることを確認する必要があります。

RFP のサンプル文書: サービスレベルアグリーメント

サービスレベルアグリーメント (SLA) に対する CISP のアプローチに関する情報およびリンクを提供すること。

<利用組織>は、CISP の SLA について継続的に注視し、SLA を満たさなくなった場合でも運用を継続できるように、重要なワークロードとアプリケーションをデプロイする必要がある。

<利用組織>は、**<利用組織>**が所有する装置または**<利用組織>**が CISP を使って運用するサービスについて、関連する SLA を適切に維持する責任がある。

高いパフォーマンス、耐久性、および信頼性を持つサービスを設計するために、CISP は**<利用組織>**に対して、運用中の SLA のパフォーマンスを継続的に可視化し報告する機能、および CISP のインフラストラクチャを活用するための文書化されたベストプラクティスを提供する必要がある。

2.2.3 契約

CISP の契約条件の設計は、クラウドサービスモデルの機能が反映されています (物理資産の購入はなく、CISP は標準化されたサービスを大規模に運用していること)。したがって、CISP の契約条件が、可能な限り最大限に組み込まれ、活用されることが重要です。契約条件および契約に関する詳細については、以下の節 2.5 を参照してください。

2.2.3.1 新規および変更サービス

CISP はサービスを通じて処理能力を提供しています。更新および有効期限があるサービス保守契約が必要な従来のオンプレミスソリューションとは異なり、クラウドサービス事業者は単に標準化されたサービスを提供するだけです。クラウドモデルでは、規模の経済を実現するために、基盤となるインフラストラクチャの更新と変更は個々のユーザーに対してではなく全員に対して展開されます。そして、お客様は自分が使用するサービスを選択します。サービスは過去のオンプレミスのシステムよりシームレスであり、クラウドサービス事業者は継続的に新規サービスや改善サービスを追加しており、お客様は希望に合わせて使用できます。

RFP の提出期限後に CISP の新規サービスまたは改善サービスを追加できない場合、公共部門の組織は、フレームワーク契約の次のバージョンが発行されるまで、新しいサービスと拡張機能は利用できません。したがって、フレームワーク契約においては、サービス提供を広義に記載し、提出期限後に新しい CISP サービスを追加できるようにすることを強く推奨します。EU の調達法では、実質的に異なる新しい CISP サービスはフレームワーク契約への追加が制限される場合がありますが、実質的な変更とはみなされないサービスの更新や新しいバージョンの追加については、調達上の問題もなく可能です。

サンプル RFP 文書: 新規サービスおよび変更サービス

CISP は、実績のある安定した仮想化テクノロジーと、継続的に更新される最先端テクノロジーの両方を活用した費用対効果の高いソリューションを提供する必要がある。**<利用組織>**は、当クラウドテクノロジーが**<利用組織>**、および共通コードベースおよび/または共通環境の CISP の他の顧客に対して共有サービスベースで提供されることを理解し同意する必要がある。また、**<利用組織>**は、CISP がときどきクラウドサービスの機能、特徴、パフォーマンスまたはその他の特性の変更、追加、または削除を行い、このような変更、追加、または削除を実施する場合、クラウドサービスの仕様がそれに応じて修正されることを理解し同意する必要がある。

このデリバリーオーダーの範囲には、**フレームワークの範囲内の**すべての既存のサービス、および新規または改善された CISP サービスが含まれる。CISP が提供するビジネス顧客向けのクラウドサービスを**<利用組織>**が利用できるようにする必要がある。

2.2.3.2 ベンダーロックイン/可逆性

クラウドテクノロジーは、物理的な資産を購入しないため、ベンダーロックインが軽減され、お客様はいつでもクラウドサービス事業者間でデータを移動できます。

ただし、クラウドサービスを購入する場合、ある程度のベンダーロックインは避けられません。すべてのクラウドが全く同じではないため、ある CISP では、別の CSIP が簡単に提供できないサービスや機能が提供されている場合があります。したがって、別のサービス事業者でそのようなサービスを使用できる可能性が低くなります。賢明なアプローチでは、合理的な「移行戦略」に役立つサービスの使用方法に関する文書とともに、CISP に対してそのクラウドから移行するために必要な機能やサービスの提供を求めます。これは、CISP にとって、お客様が標準化されたサービスを使用する際の独自の構成を知ることは不可能であり、個別の移行計画を提示することはできないためです。

EU の「非個人データの自由流通に関する規則」の第 6 条の要件に準拠し、「データの移動」および「クラウドサービス事業者の切り替え」に対応する業界の行動規範について、節 2.3.1.2 を参照してください。

RFP のサンプル文書: オンボーディングとオフボーディング

<利用組織>は、ベンダーロックインを防止するための合理的な移行戦略が記載された提案を求めている。**<利用組織>**は、物理的な資産を購入しないため、CISP は IT スタックをスケールアップ/ダウンするための機能を提供する。CISP は、CISP のプラットフォームへの移行、および CISP のプラットフォームからの移行をサポートするポータビリティツールとサービスを提供し、ベンダーロックインを最小限に抑える。CISP が提供するポータビリティツールやサービスの使用方法に関する詳細なドキュメントは、合理的な移行計画として役立つ。

CISP は、**必須の**最小コミットメントまたは**必須の**長期契約を締結してはならない。

サービス提供事業者にて格納されているデータは、いつでも顧客によってエクスポートできる。CISP は必要に応じて CISP ストレージの内外にデータを移動することを**<利用組織>**に許可すること。また、CISP は仮想マシンのイメージをダウンロードして、新しいクラウドサービス事業者に移動することを許可すること。**<利用組織>**は、自身のマシンのイメージをエクスポートして、それをオンプレミスまたは別のプロバイダーで使用することができる(ソフトウェアライセンスの制限を受ける場合がある)。

2.3 セキュリティ

セキュリティとコンプライアンスの責任は CISP とクラウド利用者間で共有されます。このモデルでは、クラウド利用者がインフラストラクチャに配置されている自身のアプリケーションやデータの設計およびセキュリティ保護の方法を管理します。一方で、CISP には、高いセキュリティと制御されたプラットフォーム上でサービスを提供する責任、および多岐にわたる追加のセキュリティ機能を提供する責任があります。このモデルでの CISP と利用者の責任レベルは、クラウド展開モデル (IaaS/PaaS /SaaS) によって異なり、利用者は各モデルでの責任について理解している必要があります。

成功するクラウドサービス RFP を策定するには、この責任共有モデルを理解することが重要です。公共部門の組織は、CISP の責任と自身の責任、およびコンサルティング/ISV パートナーとそのソリューションによって支援される部分を確実に把握する必要があります。

2.3.1 最低限の要件

クラウドのセキュリティのキーワードは**機能**です。公共部門の組織は、利用者が責任共有モデルにおける責任を確実に果たせるよう、CISP に対して必要となるセキュリティ機能の提供を求める必要があります。以下の典型的な要件リストからわかるように、CISP は、利用者が独自のクラウド環境の安全を確保できるような標準化されたセキュリティ機能を提供するように求められます。

- プライベートネットワークを作成し、インスタンスやアプリケーションのアクセス権を制御するために、ネットワークファイアウォールや Web アプリケーションファイアウォール**機能**を**提供**します。
- オフィスまたはオンプレミス環境からプライベート接続または専用接続が可能な接続**オプション**を**提供**します。
- 多層防御戦略を導入し、DDoS 攻撃を阻止する**機能**を**提供**します。
- ストレージおよびデータベースサービスで利用可能なデータ暗号化**機能**を**提供**します。
- CISP が暗号化キーを管理するか、お客様がキーを完全に維持管理することを選択できるように、柔軟なキー管理**オプション**を**提供**します。
- お客様が CISP 環境で開発、またはデプロイしたすべてのサービスに暗号化およびデータ保護を統合するための API を**提供**します。

- CISP のリソースの作成およびデコミッションを組織の基準に従って管理できるように、デプロイ**ツール**を**提供**します。
- CISP のリソースを識別し、対象のリソースに対する変更を経時的に追跡および管理するためのインベントリおよび構成管理**ツール**を**提供**します。
- お客様が CISP 環境で発生した内容を正確に確認できる**ツールと機能**を**提供**します。
- API 呼び出しについて、誰が、何を、誰を、そしてどこから呼び出したかなど、詳細な**可視化**を**実現**します。
- 調査やコンプライアンスレポートの作成を効率化するログ集約**オプション**を**提供**します。
- 特定のイベントが発生したとき、またはしきい値を超過したときのアラート通知を設定する**機能**を**提供**します。
- CISP サービス全体でユーザーアクセスポリシーを定義、実施、管理する**機能**を**提供**します。
- CISP のリソース全体への権限によって個々のユーザーアカウントを定義するための**機能**を**提供**します。
- 管理のオーバーヘッドを削減しエンドユーザーエクスペリエンスを向上させるために、企業ディレクトリとの統合や連携のための**機能**を**提供**します。

これらの要件の詳細については、「1」を参照してください。

RFP の「付加価値オプション」または「ベストバリュー」としてのより有益な分析には、セキュリティの最低標準以上の機能を使用できます。セキュリティについては、組み込まれたまたは自動化された機能が多いほど優れています。繰り返しますが、応札者間を比較するための要件について、「付録 A – 入札者相互間の比較に関する技術的要求事項」を参照してください。

公共部門の組織は、CISP に必要なセキュリティ統制が適切に実施されていることを保証するために、クラウドの認定、認証、および評価制度を活用する必要があります。たとえば、ISO 27001 認証規格への準拠を確認するために、独立監査人によって審査および認証された CISP を検討します。ISO 27001 規格の付録 A のドメイン 14 では、システムの購入、開発、保守に関する ISO の要件に基づいて CISP が準拠する具体的な統制を詳述しています。これらの統制は、すべてではないですが、IT 関連の RFP で組織から通常要求されるシステムの購入、開発、保守に関する統制の大部分をカバーしていると思われます。したがって、クラウドサービス RFP において、重複した取り組みやシステムの購入、開発、保守に関する一覧の統制を要求する代わりに、単に CISP が ISO 27001 の認定を受けていることを求めることは合理的です。

このサードパーティのコンプライアンスレポートを活用するアプローチは、ほとんどのセキュリティおよびコンプライアンスの統制に適用できます (たとえば、CISPE GDPR 行動規範、ISO、SOC など)。

RFP のサンプル文書: セキュリティ

CISP は、**<利用組織>**とサービスプロバイダー間で適切な保護と柔軟性が得られるように、公開されているセキュリティプロセスと技術的制限について、**<利用組織>**に開示する必要がある。

CISP は、セキュリティとコンプライアンスに関して、その役割と責任を明記する必要がある:

- 提案する提供サービスにおける、CISP および**<利用組織>**のセキュリティ関連の役割と責任を記述すること。クラウド環境のセキュリティ機能の構築および自動化について、責任の区分を明確にし、**<利用組織>**をサポートする CISP サービスの概要を記述すること。
- **<利用組織>**のセキュリティ要件に関連する**付録 A** 内の技術仕様に対する回答を記入すること。

<利用組織>のコンテンツの所有権および管理

CISP の機能によってどのように**<利用組織>**のデータプライバシーを保護できるかを記述すること。**<利用組織>**のコンテンツの保護に対応するために実施されている管理方法を記入すること。CISP は、あるリージョンに格納されたオブジェクトが、**<利用組織>**が明示的に他のリージョンに転送しない限り、そのリージョンから出ないようにする厳格なリージョンアイソレーション機能を提供している必要がある。

- **<利用組織>**はコンテンツ、サービス、リソースへのアクセスを管理する。CISP は、**<利用組織>**が効果的に管理できるように、高度な一連のアクセス、暗号化、ログ機能を提供する必要がある。CISP は、法的に要求される場合、CISP サービスを維持する場合、**<利用組織>**およびそのエンドユーザーに CISP サービスを提供する場合を除き、いかなる目的でも**<利用組織>**のコンテンツにアクセスおよび利用しないこと。
- **<利用組織>**は、コンテンツが格納されるリージョンを選択する。CISP は、法的に要求される場合、CISP サービスを維持する必要がある場合、および CISP サービスを**<利用組織>**およびそのエンドユーザーに提供する場合を除き、**<利用組織>**のコンテンツを選択したリージョンの外に移動したり複製したりしないこと。
- **<利用組織>**はコンテンツのセキュリティを保護する方法を選択する。CISP は、転送中または保存中の**<利用組織>**のコンテンツに対する強力な暗号化を提供する必要があり、かつ自身の暗号化キーを管理するためのオプションを**<利用組織>**に提供する必要がある。

- CISP は、**<利用組織>**が CISP のセキュリティ管理環境を設定、運用、活用するために、グローバルプライバシーおよびデータ保護のベストプラクティスを使用したセキュリティ保証プログラムを備えている必要がある。セキュリティ保護および統制プロセスは、複数の第三者による独立評価によってそれぞれ検証されなければならない。

クラウドの認定、認証、評価により、CISP が効果的な物理的および論理的なセキュリティ管理を実施していることが公共部門の組織に対して保証されます。RFP でこれらの認定が活用されると、調達プロセスが効率化され、クラウド環境では必要ではない可能性のある重複していたり過度に負担のかかるプロセスや承認ワークフローを回避できます。

クラウド RFP により、CISP はコンプライアンスの認定および評価に準拠していることを証明する機会を得ます。前述したように、これらの認定スキーム全体のリスクシナリオとリスク管理対応には多数の重複があります。認定制度による統制と要件をまとめ、CISP が認定に準拠することを求める方が、個々の統制の要件一覧を重複して確認するより、RFP のコンプライアンスに対応することを確認する簡単な方法です (**個々の統制の多くは、オンプレミスのデータセンターの過去の RFP から直接転記されている場合があり、これらはクラウドコンピューティングに適用できない可能性があります**)。

注意: 以下の一覧のレポートへのアクセス方法を把握することも非常に重要です。たとえば、SOC 1 および SOC 2 のレポートは通常は機密文書です。それらの文書へのアクセスに必要な契約 (例: 秘密保持契約 - NDA) を理解し、RFP の回答の一部として単純にそのような文書の提出を要求してはいけません (これらの文書は、記録公開法または類似の立法を通して公開され、クラウドセキュリティが危険にさらされる可能性があります)。

RFP のサンプル文書: コンプライアンス

データ処理、データセキュリティ、機密性、可用性など、クラウドサービス運用におけるベストプラクティスから得られた、広く認められているセキュリティ、コンプライアンス、運用基準を利用することで、クラウドテクノロジーの調達を効率化できる。

<利用組織>は、以下および**付録 A** の概要の通り、受け入れられているセキュリティ、コンプライアンス、運用基準に照らして独自の提案提供サービスを評価する。各基準に対するコンプライアンスに関するベ

ンダー認定を利用することで、**<利用組織>**は、基準に対する最低限のコンプライアンスを提案の評価のベースラインとして使用できる。

契約の全期間中、最低基準のコンプライアンスの維持を CISP に求めることで、サービスのコンプライアンスを最新の状態に保つメリットが得られる。

入札中の CISP は (直接または再販事業者を通じて)、以下の独立した第三者による証明、レポート、および認証を満たす能力を実証できる必要がある (注意 – これらの証明、レポート、および認証の一部について、セキュリティ問題のために開示が制限されている場合、**<利用組織>**は CISP と連携して、双方が同意してアクセスできるようにする):

認証/証明	**法律、規制、プライバシー**	**準拠 / フレームワーク**
☐C5 (ドイツ)		☐CDSA
☐CISPE データ保護行動規範 (GDPR)		
☐CNDCP (気候中立的データセンター協定)		
☐DIACAP	☐EU データ保護指令	☐CIS
☐DoD SRG レベル 2 および 4	☐EU モデル条項	☐刑事司法情報サービス (CJIS)
☐HDS (フランス、ヘルスケア)		
☐FedRAMP	☐FERPA	☐CSA
☐FIPS 140-2	☐GDPR	☐EU-US プライバシーシールド
☐ISO 9001	☐GLBA	☐EU セーフハーバー
☐ISO 27001	☐HIPAA	☐FISC
☐ISO 27017	☐HITECH	☐FISMA
☐ISO 27018	☐IRS 1075	☐G-Cloud (英国)
☐IRAP (オーストラリア)	☐ ITAR	☐GxP (FDA CFR 21 パート 11)
☐MTCS Tier 3 (シンガポール)	☐PDPA – 2010 (マレーシア)	☐ICREA
☐PCI DSS レベル 1	☐PDPA – 2012 (シンガポール)	☐ IT Grundschutz (ドイツ)

☐SEC 規則 17-a-4 (f)	☐PIPEDA (カナダ)	☐MARS – E
☐SecNumCloud (フランス)		
☐SOC1 / ISAE 3402	☐プライバシー法 (オーストラリア)	☐MITA 3.0
☐SOC2 / SOC3	☐プライバシー法 (ニュージーランド)	☐MPAA
☐SWIPO IaaS コード		
	☐スペイン DPA 認証	☐NIST
	☐英国 DPA - 1988	☐Uptime Institute Tiers
	☐VPAT/セクション 508	☐英国クラウドセキュリティ原則

以上のリストは説明を目的に提供されているものであり、クラウドサービスに適用できる認証および標準を網羅しているものではありません。

2.3.1.1 データ保護

クラウドサービスを利用する際の主要な考慮事項は、該当する EU データ保護法 (一般データ保護規則 (GDPR) など) に従って個人データの処理が実施されることです。GDPR は、原則に基づいた規制であるため、コンプライアンスの確保に役立つセクター固有のガイダンスは提供していません。ただし、GDPR は、そのようなガイダンスを提供するために行動規範などのコンプライアンスツールを導入することを促しています。CISPE は、フランスのデータ保護機関 (CNIL) と連携して、データ保護行動規範 (CISPE 規範[6]) を策定しました。これは、欧州データ保護委員会に承認されており、ヨーロッパで全般的に適用されます。この規範の目的は、CISP が GDPR に準拠できるようにすること、およびお客様が実行を望む個人データの処理に CISP が適しているかどうかをお客様が評価できるように導くことです。

- この規範は、IaaS セクターのみに焦点を合わせており、IaaS プロバイダーの特定の役割および責任に対応しています。
- クラウドインフラストラクチャサービスにおいて公正かつ透明な処理、および適切なセキュリティ手段の側面を明確化するのに役立ちます (GDPR の第 40 条[2])。

[6] https://cispe.cloud/code-of-conduct/

- データが EU 内にとどまるようにすることで、顧客がデータに対する主権を維持する方法を把握できるようにします。
- ヨーロッパのクラウドデータサービスを開発するために EU の GAIA-X イニシアチブをサポートするデータ保護のベストプラクティスを推進します。

CISP が CISPE 規範などのデータ保護の行動規範に準拠していれば、個人データが GDPR に厳密に準拠して処理されることが保証されます。

RFP のサンプル文書: データ保護

(直接、または再販業者を介して) 入札する CISP は、CISPE 規範などのデータ保護の行動規範に準拠する能力を示す必要がある。データ保護規範は、GDPR フレームワークで規定されている要件に準拠している必要がある。規範には、最低限 (1) CISP の役割と責任の明確な定義、(2) CISP がマーケティングや広告のために顧客のデータを使用しないという要件、(3) データを欧州経済領域内でのみ処理できる CISP サービスを顧客が選択できることが記載されている必要がある。規範に対する準拠は、欧州データ保護機関に認定された独立した外部監査人によって認定された外部の独立監査人 (監視機関) によって検証される必要がある。

2.3.1.2 クラウドサービス事業者の切り替えおよびデータの移動

お客様は、使用するクラウドサービスを自由に選択でき、CISP や PaaS/SaaS プロバイダーにロックインされるべきではありません。

CISP 提供のクラウドサービスは標準化されており、「1 対多」ベースで提供されます。サービスはお客様によって設定、プロビジョニング、そして管理されます。クラウドコンピューティングのメリットは、独自のアプリケーションおよびソリューションの開発に必要な標準化されたサービスをお客様が選択できる点にあります。このメリットにより、任意の特定の時点でお客様のニーズに最適な、新しいサービスや別のサービスに切り替えることもできます。

データ保護と同様に、オンプレミスインフラストラクチャからクラウドへの切り替えや CISP 間での切り替えの際、行動規範によってお客様へ保証や信頼を提供することができます。CISPE は EuroCIO (欧州 CIO 団体) とともに共同議長を務め、IaaS クラウドサービスのデータポータビリテ

ィとクラウドサービス切り替えの行動規範 (SWIPO IaaS 規範[7、8]) を策定しました。この規範の最初のバージョンは、EU のデータの自由流通に関する規則に従って策定され、2019 年 11 月に EU のフィンランド大統領によって欧州委員会に渡され、2020 年 5 月に団体である SWIPO AISBL によって公開されました。2021 年 4 月に最初のサービスが SWIPO AISBL によってこの規範に準拠していると宣言され、2021 年 5 月に最初の CISPE メンバーサービスがこの規範に準拠していると宣言されました。

RFP のサンプル文書: クラウドサービス事業者の切り替えおよびデータの移動

(直接、または再販業者を介して) 入札する CISP は、SWIPO IaaS 規範などの「スイッチングとデータ移植」の行動規範に準拠する能力を示すことができること。規範では、顧客が CISP から切り替えると決定したときに顧客による業務データの安全な転送を CISP が提供する方法が詳述されている必要がある。

2.3.2 ベンダー間の比較

上記の項の技術基準については、クラウドサービス RFP の最低セキュリティ要件に加えて、競争評価時に CISP のセキュリティ能力とサービスを比較できる基準を提供することが重要です。

サンプルの CISP セキュリティ要件については、付録 A – 入札者相互間の比較に関する技術的要求事項を参照してください。CISP を評価する公共部門の組織にとって、以下の機能を、セキュリティの主要な検討事項とすることを強く推奨します。:

RFP のサンプル文書: 主要なセキュリティ検討事項

- CISP の責任共有モデルに対する理解、および CISP の機能とサービス (たとえば、GDPR のコンテキストにおけるもの) のセキュリティ責任の詳細に関する顧客の理解に役立つ文書
- CISP のセキュリティ体制と物理的/論理的な統制に関する公開された非機密の文書がある、CISP インフラストラクチャのセキュリティの実績
- クラウドセキュリティに固有の CISP の対応
- 顧客がアカウント設計を作成し、セキュリティとクラウドガバナンス統制を自動化し、監査を効率化できるサービス

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security

[8] https://swipo.eu/

- テンプレート的な方法でリソースのコレクションを作成、プロビジョニング、および管理する機能 (CISP およびそのパートナーが作成した定型のセキュリティテンプレートを含む)
- 信頼性と再現性のある統制活動を構築する能力
- 継続的かつリアルタイムな監査に必要な機能
- クラウドガバナンスポリシーのための技術的なスクリプトの作成能力
- その機能の変更が許可されていないユーザーによる上書きが禁止された強制機能を作成する能力
- 強制的なセキュリティとコンプライアンスの構築と合わせて、過去のポリシー、標準、規定に記述されている内容を確実な実装を遂行できる能力。この結果、機能的で信頼性の高い IT 環境のクラウドガバナンスモデルが構築される
- 高度なアプリケーション層攻撃を緩和するためのカスタマイズされたルールを記述する能力とともに、一般的で最も頻繁に発生する一般的なネットワークおよびトランスポート層の分散型サービス拒否 (DDoS) 攻撃から防護するためのサービス
- マネージド型脅威検出サービス

2.3.3 契約

上記の通り、CISP の契約条件の設計にはクラウドサービスモデルの機能が反映されています (物理資産の購入はなく、CISP は標準化されたサービスを大規模に運用・提供していること)。したがって、CISP の契約条件が、可能な限り最大限に組み込まれ、活用されることが重要です。契約条件および契約に関する詳細については、以下の節 2.5 を参照してください。

セキュリティに関しては、CISP が RFP の元の項目を遵守している限り、CISP が継続的に提供サービスを更新すること、またはサプライヤーが提出期限後に製品を追加することを許可することを強く推奨します。これは、セキュリティ機能とサービスが急速に進化しており、CISP がセキュリティ重視のサービスを頻繁にリリースしているという事実を反映しており、多くの場合、これらは無料で提供されています。セキュリティ提供サービスの変更によって悪影響が出ないことを保証するために、基準となるセキュリティレベル (上記の最小要件を参照) を設けることが重要だという点にも注意が必要です。

もちろん、責任共有モデルは、クラウドサービス RFP のセキュリティの中核です。各当事者は彼らのセキュリティ責任について明確にする必要があります。利用者がセキュリティのベストプラクティスを統合し自動化するための文書に加えて、CISP が提供するクラウドテクノロジーの CISP と利用者の双方のセキュリティ責任を文書化するように CISP に求める必要があります。

クラウドフレームワーク契約では、ベンダーがクラウドサービス RFP に規定された最低限のセキュリティ要件およびコンプライアンス要件に準拠できない場合、そのベンダーを排除できる柔軟性が必要です。

2.4 料金表

変動するニーズに基づいてクラウドテクノロジーを契約するには、公共部門の組織は、求められるクラウドガバナンスと、利用状況と支出の可視化に加え、サービスを従量課金で支払うことができる契約を結ぶ必要があります。

重要な点として、クラウドサービス RFP では、単価を単純に比較するのではなく、価値と総保有コスト (TCO) に注目する必要があります。最も低い単価に注目する従来の対応は、クラウドモデルに適用できないため、最も経済的に有利な入札や総合的な最低価格にはつながりません。

CISP の料金表を評価するには、類似の能力を持つ CISP がフレームワーク契約の資格が得られるよう、最初に、**最低価格関連の要件**と合わせて、CISP の事前選考、または候補者リストを使用すると便利です。次に、コールオフ契約およびミニコンペの評価プロセスでは、公共部門の一般的なワークロードに適合する、厳選した典型的なクラウドアーキテクチャ例、および**価格シナリオ**に注目し、CISP に価格を提供してもらいます。また、CISP が提供するクラウドテクノロジーサービスのパフォーマンスと柔軟性を比較できるように、実演でのテストデモの実施も推奨します。クラウドテクノロジーのデモテストのサンプル文書については、付録 B をご参照ください。

2.4.1 最低限の要件

クラウドサービス RFP の料金表のセクションには 4 つの主要な要素があります:

1. **公共料金的な価格設定**: クラウド利用者は、毎月月末に単純に使用量に対して支払う従量課金の公共料金モデルを組み込めること。これは活用やリソースの指標の最適化につながります。
2. **透明な価格設定**: CISP の価格設定は公開され透明性があること。

3. **動的な価格設定**: クラウドの価格を市場価格に基づいて変動させることができる柔軟性を備えていること。このアプローチは、クラウド価格の動的で競争原理的な性質を生かすことで、イノベーションや価格の削減を実現します。

4. **支出管理**: CISP がお客様に提供する報告、監視、予測ツールは、(1) 概要レベルと詳細レベルで使用状況と支出を監視し、(2) 使用状況や支出がカスタムのしきい値を超過した場合にアラートを受信し、(3) 将来のクラウド予算計画のために、使用状況と支出を予測する。

RFP のサンプル文書: 価格設定

<利用組織>は、応札する CISP に対して、商用クラウドの機能としてエンドユーザーに各サービスを提供するための提案方法および価格モデルを記載するよう要求する。

CISP は以下の項目を提供する必要がある:

- サービス定義文書またはサービス定義へのリンク
- 契約条件の文書
- 料金表の文書 (完全な料金の一覧/料金表の文書を要求に基づいて入手できることを前提に、公開されている料金表へのリンクも容認される)

料金は、最も一般的なサービス構成のコストになる。CISP は数量ベースの割引オプションと、調達内容の実際の価格や調達者に提供される全体的な価値 (たとえば、最適化のサービスによるコスト削減) を算出するための価格計算ツールを提供する必要がある。

フレームワーク契約に基づく調達者は、サービスの説明、契約条件、価格設定、またはサービス定義文書/モデルの説明をサプライヤーに求めることができる。サプライヤーとのすべてのやりとりの記録は保持される。

追加の価格要件

- ビジネスの柔軟性を最大限引き出し、スケーラビリティと成長を実現するダイナミックプライシングモデルを持つクラウドテクノロジーを提供する。
- 価格の項目には以下の内容を含める必要がある:
    - 料金は、オンデマンド式、公共料金スタイル、従量課金制で提供されているか? 価格モデルを説明すること。

- 利用が確定している/または一括購入の場合、さらに割引が可能か? 方法に関する詳細を記入すること。
- 料金表は公開されており透明性があるか? 公開されている料金表へのリンクを掲載すること。
- 価格設定は動的であり、市場競争に基づいて迅速かつ効率的に対応しているか?
- 支出を追跡するためのベストプラクティスとリソースの提供はあるか?
- コスト最適化のためのベストプラクティスとリソースを提供しているか?

料金の透明性

商用クラウドテクノロジーの価格は、イノベーションと競争によって常に下降傾向にあるため、フレームワーク契約の下、**<利用組織>**が支払う CISP サービスの計測による単価は、顧客がサービスの項目を使用する時点でクラウドサービス事業者の Web サイトに公開されている単価を超過することは決してあってはならない。

予算および請求アラート/レポート

CISP はクラウドテクノロジーの提供内容と使用状況を証明するために、**<利用組織>**に対して、組織のアカウント別、製品や製品リソース別、または顧客が定義したタグによって、1 時間、日次、月次単位でコストを分類した詳細な請求レポートを作成するツールを提供する必要がある。**<利用組織>**は、クラウドの責任共有モデルの一環として、CISP が提供する予算や請求機能、ツールを使用して、独自の予測やレポート要件に対応することに関しては**<利用組織>**自身に責任があることを理解する。

- **<利用組織>**が、将来の支出の予測に加えて、CISP リソースの経時的な支出パターンを視覚化して、詳細レベルと概要レベルの両方で請求情報を閲覧する方法に関する情報を提供すること。
- **<利用組織>**が使用状況/請求をサービス別、関連アカウント別、またはリソースに適用されているカスタムタグによってフィルターする方法、および**<利用組織>**が定義したしきい値/予算にサービスの使用状況が近づいた、または、超過した場合に通知を送信する請求アラートを作成する方法に関する情報を提供すること。
- **<利用組織>**が、定義した予測期間におけるクラウドサービスの使用量を、過去の使用状況に基づいて予測する方法に関する情報を提供すること。コストと支出に関するガバナンスを強化するために、CISP は**<利用組織>**に対して CISP の請求内容の**予測**を提供する必要がある。また、**<利用組織>**は使用予測量に関するアラームおよび予算を使用できること。

2.4.2 ベンダー間の比較

公共部門の組織は、ベストバリュー、最も経済的に有利な入札 (MEAT)、または最低価格などの評価基準を使用して、入札者間の競争を要求することがしばしばあります。フレームワーク契約のコールオフ契約またはミニコンペの価格設定を計画する場合、クラウドの固有の機能を考慮したアプローチを策定することが重要です。たとえば、単純にクラウドサービス事業者の提供サービス (コンピューティングやストレージなど) のラインアイテム同士を比較することは、有効な方法でないことを理解する必要があります。なぜなら、クラウドネイティブなサービスを使用したパフォーマンスやコストの最適化や CISP の監視ツール、または CISP が無料で提供する差異化サービスが考慮されていないためです。また、CISP の定価には多数の項目がある場合があり、価格モデルもサービスごと、またはプロバイダーごとに異なります。

TCO の分析

クラウドソリューションのすべての要素 (パートナーサービス、CISP の標準割引、パフォーマンスを改善しコストを削減/最適化するための技術的な機能などを含む) が考慮されている定義済みのユースケースに対する総所有コスト (TCO) に注目することを推奨します。

シナリオ別の比較

また、評価プロセスでは、一般的なシステムやアプリケーションに対応した代表的なシナリオを考慮することもできます。これらのシナリオ (Web ホスティング、ユーザーが x 人の HR システムの導入など) では変数を追加することが可能で、これらにはリソースのスピードや規模、アプリケーションやソリューションのパフォーマンス、ストレージのアクセス回数、少量の複雑なデータと大量の単純な計算タスクとの比較などがあります。また、アプリケーションやシステムには、納税申告や洪水等の緊急通知といった大量の処理が発生する際の代表的なシナリオなどが含まれることもあります。このシナリオは、お客様がプロジェクト中に使用する可能性のあるテクノロジーやサービスの範囲が含まれる包括的なものでなければなりません。これによって、お客様はプロジェクトの全体的な予測コストを比較できます。

シナリオをコスト面および技術面で比較する

また、CISP の提供サービス同士の価格を比較する場合、技術的な利点を考慮することも重要です。たとえば、ある CISP の場合、1 つの地理的なリージョン内のクラスターに複数のデータセンターを持つモデルを採用しているため、アクティブ/アクティブな災害復旧 (DR) トポロジを構

築できる点などが挙げられます。このタイプの冗長化やデータセンター構成を持たない CISP の場合、災害復旧の必要性を考慮に入れたコストは x%高くなる可能性があります。CISP を評価する場合、付加的な技術機能を含めた包括的な価格設定のアプローチが重要になる理由の例として、以下では、直接的で「単純」な比較の別のシナリオを検討します。

例: お客様は、フレームワーク契約内の認定を受けた CISP が提供するオブジェクトストレージの価格を比較したいと考えています。CISP 1 のストレージ「ユニット」の項目の価格は € 0.023/GB です。CISP 2 の同じ「ユニット」の価格は € 0.01 GB です。ユニット同士の単純な比較では、お客様は以下のような重要な質問はしないと思われます:

1. 障害の場合、冗長化されたオブジェクトのコピーはいくつありますか? 上記の例では、CSP 1 は 2 箇所の異なる施設でデータの同時喪失に耐えるよう設計されており、複数のデータのコピーを保管しています。CSP 2 では、冗長コピーを作成していません。
2. 保管されたオブジェクトの持続可能性のレベルはどうでしょうか? CSP 1 の 99.999999999%に対して、CSP 2 は 99% です。
3. データの保管方法と使用方法については、プロジェクトやワークロード全体の総所有期間のコスト、およびコスト最適化機能によって削減可能なコストを考慮します (たとえば、CISP のサーバーレス機能の利用を増やすと、コストを x%削減できるなど)。

これらは、特にセキュリティとコンプライアンスに関連して、価格設定を考慮する上でのその他多くの技術面での考慮事項の一部にすぎません。

価格シナリオの考慮事項には以下のものが含まれます。

基本料金 – 基本的には公開されている CISP の価格です。CISP はこれらの料金を公開している必要があります。ただし、上記の CISP の適切な比較で説明した通り、お客様はすべてのベンダーから 3～5 件 (またはお客様が納得する数) の具体的なシナリオについての価格の提供を求めることができます。各シナリオは、お客様がプロジェクトにて使用する可能性のあるサービスやテクノロジーの範囲が含まれる包括的なものでなければなりません。これによって、お客様はプロジェクトの全体的な予測コストを比較することができます。項目/SKU レベルでの比較は、お客様やベンダーにとって役立つどころか問題となる傾向があります (お客様はすべての

CISP の何万もの項目を比較する必要があります。一方でベンダーは実際の価格がサービスの使用量によってのみ決定する場合、このレベルの詳細内容を提供し、対応する必要があります)。

CISP の包括的な機能セットを評価することは、ベストバリューを得ることを考えるクラウド利用者にとっては必須です。たとえば、CISP に無料または基本的に無料のサービスが数多くある場合、価格評価では他の CISP が同様の機能に対して料金を請求するようなそれらのサー

評価基準は、CISP に「デフォルトで含まれる」機能、そして、そういったサービスがコスト全体にどのような影響をもたらすかによって記載されます。また、評価基準では CISP のボリュームベース/階層型の価格設定、およびリザーブドインスタンス/スポットインスタンスなど商用向けの割引も注目されます。例:

- お客様がリザーブされたコンピューティング能力 (1 年、3 年など) を購入する場合、x%節約
- 階層型/ボリューム価格設定における x%の割引
- 最適なコンピューティングオプションに切り替えるなどインフラストラクチャのアーキテクチャレビューや最適化に基づいて、x%節約
- 前述の通り、全ライフコストおよびコスト最適化機能によるコスト削減の考慮

価格設定シナリオ

入札者は、評価のみを目的として、次のシナリオの価格設定を提供する必要がある。実際の価格は、オンデマンド式の従量課金モデルで、サービスの利用量に基づく。

以下は、均衡価格を見つける目的で使用される代表的な要件で、契約期間中にこれらの形式的な要件に変更が発生することを明確に理解していることを条件に提供される。12 か月と 36 か月間のオンデマンド形式、および 12 か月と 36 か月間のリザーブドキャパシティーの両方の価格を記載すること。

記載内容:

- 提案ソリューションの名前:
- 入札者のベスト価格:
- サービス時間: 24 時間 365 日
- サービスの可用性: 99.95%

価格設定シナリオには、過去 1/2/3 年にわたり、CISP の監視ツールや最適化ツール、最適なクラウドネイティブソリューションの採用、および CISP の価格割引を通して支出を最適化した類似のワークロードを使用する既存の顧客の例も記載できる。

2.5 契約履行の設定/契約条件

CISP が提供するクラウドテクノロジーと運用は意図的に標準化されているため、契約条件も標準化されています。ただし、現地の法律や規制の状況に対応するために、これらの契約をわずかながら調整することができます。

従来の IT 調達方式では、応札者が多くの調達要件またはすべての調達要件に準拠しなければ、除外される厳格なルールが含まれている場合が多くあります。もしくは、非常に厳しい必須の要件のサブセットが含まれていることも考えられます。実際には、カスタムソリューションの設計に役立つ標準化された一連のコンポーネントやツールであるクラウドテクノロジーでこのタイプの調達方式を利用すると、調達が失敗に終わる傾向があります。

2.5.1 契約条件

クラウドサービス RFP で契約する際の最初のステップは、多くの場合、CISP の Web サイトで公開されている CISP の既存の取引条件を確認した上で理解することです。公共部門の組織が CISP の取引条件を快く受け入れるケースが増えています。CISP やそのパートナーとの会合をもうけて、彼らのアプローチについて深く掘り下げることも、条件を理解する取り組みのひとつです。質問の鍵は、CISP が特定の条件を付けて運用する「理由」を尋ねることです。一部の利用規約は、従来の IT の規約とは異なるように思われるかも知れませんが、「何故」それがクラウド契約の一部であるか、という特別な理由があります。一般に公表されている規約が受け入れられない場合、CISP には多くの場合、法人客向けに若干変更可能で、修正協議に応じることのできる契約が用意されています。

CISP の利用規約を見直すとともに、既存の方針や規則と/または法規 (例えば、テクノロジー、データ分類、プライバシー、要員等に関連するもの) を理解することが重要です。多くの場合、既存の方針や規則、法規は従来の IT 製品の購入や利用を目的として設計されており、CISP のモデルとは相容れません。例えば、当初のフレームワーク契約の入札に含まれていたクラウド技術の利用のみをクラウドサービス RFP を通じて許可することがそれに該当します。CISP は、絶

えず、新規サービスや新機能を追加しています。従来の IT 製品の更新アプローチに従っているという理由だけで、新しいサービスへのアクセスを制限することは、エンドユーザーにとって意味がありません。その場合には、これらの方針/規則および/あるいは法規の検討も含め、CISP と綿密に協議することが重要です。

事前 RFP 協議の活用

前述のように、RFP の草案を作成する前に、CISP および関連ベンダーとの会合をもうけて、各社の利用規約を理解し、組織の取り組みや方針、規則、法規について理解してもらう時間をとってください。 このような協議では、関連する規約がそのように作られている「理由」について両当事者が理解することが最も重要です。例えば、クラウドの利用規約は、従来のデータセンター、マネージドサービス、ハードウェア、パッケージソフトウェア、およびシステムインテグレーションに関する規約とは異なります。これらは単一のモデルであり、継続的なイノベーションを伴うため、CISP のビジネスモデルでは、理解が得られるように交渉や協議に RFP プロセスが十分柔軟に対応できることが求められます。

協議や交渉を通して利用規約を明確化できるようにすることで、公共部門の組織はクラウドモデルをより深く理解し、各組織のニーズに実際には対応できる潜在的なプロバイダーを拒否することのないようにしています。代表的なプロセスの 1 つとして、組織では、落札前に協議と交渉を行う意思があることを条件として事前に示します。各組織は、事前に入札者と受け入れ可能な条件を交渉することによって、その落札に最も適した条件を満たしていることを保証し、効果的な提案の拒否につながる差異を解消します。公共部門の事業体もまた、それぞれの方針、規則および法規を見直すことができます。両当事者はクラウドの利用がこれらのモデルにどのように適合するかについて理解を得ることができます。多くの場合、既存の条項に基づいて事業を行う方法があります。ただし、ある領域に問題が生じた場合は、両方のチームが協力して解決策を見出すことができます (できれば、RFP やその後の契約交渉よりも前に十分に協議することをお勧めします)。

交渉上の柔軟性

CISP による標準化された契約条件に依存しつつ、現地の法規に準拠した契約を締結できるようにするためには、(1) 申請者に標準契約を要求すること、(2) クラウドサービス RFP のフレーム

ワーク契約を設定する際に不適切な契約条件を制定しないこと、(3) フレームワーク契約につながる協議と提案のすべての条項について交渉オプションをもうけること (法律で義務付けられている義務条項を除くことは当然です) が推奨されます。

注: 責任共有の範囲はクラウドモデルに固有のものであり、契約の条件に反映される必要があります。例えば、CISP はお客様がデータを所有していること、および、そのデータの保存場所を確認し、データの保存場所の選択の制限を保証するツールを提供します。**ただし**、これらのツールは、お客様またはパートナーの責任のもとに使用します。

ロットごとに異なる契約の契約条件がクラウドフレームワーク契約に設定されていることが重要です。すべてのロットの契約について「万能なアプローチ」を求めることは、技術上の実現可能性と互換性に問題を生じることになります。

前述したように、交渉不可能な必須条件を含む RFP は、本質的には、プロバイダーにとって「無条件で受け取るか、やめるか」という提案であり、場合によっては受け入れ可能な提案を拒否することになりかねません。公共部門の組織は、**法的要件でない限り**、必須条件を適用した場合の結果を慎重に検討する必要があります。必須要件に分類することによって将来の交渉が回避されるため、各組織は必須の要件または条件の必要性に確信をもっている必要があります。各組織が最高のテクノロジーとソリューションの獲得に必要な柔軟性を得られるように、必須の要件または条件の使用は必ず最小限に抑える必要があります。

CISP のクラウドテクノロジーは完全に標準化され、完全に自動化された方式で提供されることに留意する必要があります。したがって、CISP では、基本サービスのカスタマイズを必要とするような契約条件の変更は、いかなるものもできません。さらに、サービスの価格は一般的に公開されており、すべてのユーザーに対して標準化されています。つまり、CISP は特定のお客様に代わって多くのリスクをとるために価格を調整することはできません。

間接的な購入

CISP から直接クラウドテクノロジーを購入する代わりに、CISP の再販業者から購入するという選択肢もあります。CISP の再販業者の詳細については、上記の節 2.1.3 を参照してください。

RFP 言語のサンプル: 利用規約

CISP または代表ベンダーは、公開されている利用規約を提供し、**<利用組織>**によって用意された主要利用規約に関するフィードバックを提供する必要がある。

<利用組織>は、落札者の契約条件に基づき、落札者と書面による契約を締結する意図を有する。入札者は、入札者の商業上・法律上最良の提案として一連の契約条件案を**<利用組織>**に提示して審査に付す必要がある。提案者と**<利用組織>**は、<協議/交渉>段階で両方の利用規約セットについて協議を行うことができる。

- ハイレベルのフレームワーク見出し条件は、最大限、以下の要素で構成されるものとする。
  - フレームワーク期間
  - フレームワークのガバナンス
  - フレームワークのパフォーマンス
  - フレームワークの終了
  - フレームワークの範囲
  - オーダー・プロセス
  - 秘密保持規定
  - カテゴリ固有の IP および情報
  - 品質基準、認定、セキュリティ、データ保護など、CISP が満たすべき最低限の技術的要求事項
- **フレームワーク契約のロットごとに異なる条件が存在する。**
- CISP サービスの詳細は検討可能であり、コールオフ時に対処される。
- 契約変更が許容される — 顧客とサプライヤーの契約変更への同意を制約したり、新しいサービスや機能拡張に縛られるという制約を設けるべきではない。クラウドサービスは進化していくものであるため、サービスの拡張が継続的に利用できるようになり、顧客は効率性を高めることができる。
- サービスレベルアグリーメント (SLA) は、顧客が指定するものではない。CISP の標準的なサービス提供モデルとは異なる委託業務固有のカスタム SLA を顧客の条件で定義しない。CISP の標準 SLA を許可することで、CIAP はコストを低く抑え、これらの SLA が顧客に提供される。それによって、顧客は CISP が SLA を満たすことを確信できる。
- 責任の上限は比例分配すること。責任は、調達されるサービスにつり合ったものとし、不相応に高い責任上限を設けてはならない。上限が不相応に高くなると、CISP が低価格プロジェクトを受

け入れる意欲がそがれてしまう。低価格プロジェクトは、特定のクラウドソリューションが顧客の組織にとって有効であるかどうかを判断する上で顧客にとって有益な導入事例となり、「テストケース」となる場合が多い。

- 顧客が自身のデータを所有する必要がある。顧客はデータの管理と所有を行い、データの保存先となる地理的な場所を決定することができる。したがって、顧客はベンダーによる囲い込みを受けることなく、データを新しいプロバイダーに自由に移動することができる。

2.5.2 ソフトウェア利用規約

このハンドブックでは、CISP によって提供される IaaS および PaaS クラウドテクノロジーの購入に焦点を合わせていますが、公共部門の組織がソフトウェアをベンダーから購入する際に考慮できるソフトウェア利用規約に注目することも重要です。図 1 (5 ページ) を参照して、十分に構造化されたクラウドサービス RFP の一環としてソフトウェアを購入する方法を確認してください。

ソフトウェアは、公共部門も含め、ほぼすべての業種で重要な役割を果たします。クラウドサービス RFP にソフトウェア利用規約などの義務を含めると、公共部門の組織がソフトウェアの購入時にベストバリューを実現し、ベンダーを自由に選択できるようになります。

詳細については、「Ten Principles of Fair Software Licensing for Cloud Customers」[9]を参照してください。この原則は、CISPE と連携して、その他のヨーロッパの CIIO やプロバイダーから成る貿易団体の支援を受け、デジタルテクノロジーのユーザーであるフランスの大手企業および行政で構成された団体である Cigref [10]によって策定されました。その目的は、クラウドに移行する際にあらゆる規模の組織のデジタルトランスフォーメーションにとって害になると両団体が見なしている慣習に対処することです。

RFP のサンプル文書: ソフトウェア

<利用組織>は、落札者の契約条件に基づき、落札者と書面による契約を締結する意図を有する。入札者は、入札者の商業上・法律上最良の提案として一連の契約条件案を**<利用組織>**に提示して審査に付す必要がある。ソフトウェアベンダーと**<利用組織>**は、<協議/交渉>段階で両方の利用規約セットについて協議を行うことができる。

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

要件 1.0. ソフトウェアベンダーは、概要レベルと詳細レベルのコストの明細を含め、明確なライセンス条件を提供する必要がある。

要件 1.1. ライセンス条件に対する非準拠に関連するすべての料金を概要レベルおよび詳細レベルで示す必要がある。

要件 2.0. ソフトウェアライセンスでは、**<利用組織>**が、同じソフトウェアの別個の重複したライセンスを購入することなく、ライセンスソフトウェアをオンプレミスから任意のクラウドに移行できるようにすること。

要件 2.1: ソフトウェアライセンスには、**<利用組織>**が任意のクラウドでライセンスソフトウェアを実行できる能力を制限するようなライセンスの制限やコストの増加が含まれていない必要がある。

要件 3.0. ソフトウェアライセンスでは、<利用組織>が任意のクラウド上および独自のハードウェア上で (通常、「オンプレミス」ソフトウェアと呼ばれる)、ライセンスソフトウェアを実行することを許可する必要がある。

要件 4.0. ソフトウェアライセンスでは、ライセンスソフトウェアを**<利用組織>**専用のハードウェアでのみ実行することを要求してはならない。

要件 5.0. ソフトウェアベンダーは、ベンダーのライセンスソフトウェアが別のサプライヤーのクラウド提供サービスで使用された場合に、立ち入ったソフトウェア監査を実施したり監査の回数を増やしたりする権利やソフトウェアライセンス料金を引き上げる権利を含めるなど、**<利用組織>**にペナルティを与えてはならない。

要件 6.0. 他のアイデンティティサービスとの間で差別的でない方法で、ユーザーアイデンティティの同期と認証に対してディレクトリソフトウェアがオープンスタンダードをサポートしている必要がある。

要件 7.0. ソフトウェアベンダーは、インストール先のハードウェアの所有者だけに基づいて、同じソフトウェアに対して異なる料金を請求してはならない。

要件 7.1.ソフトウェアの料金は、<利用組織>独自のデータセンター、サードパーティが管理するデータセンター、サードパーティがリースするコンピュータ、または<利用組織>が選択したクラウドサービス事業者のそれぞれにインストールされるソフトウェアの間で、差別してはならない。

要件 8.0. 契約期間中、法律で定められている場合やセキュリティ上の懸念がある場合を除き、ソフトウェアベンダーはライセンス条項に対して、<利用組織>に以前に許可された使用を制限するような変更を行ってはならない。
要件 9.0. <利用組織の要求事項>に示された<利用組織>の意図するソフトウェア使用において、そのような使用には追加ライセンスの購入が必要になる可能性がある場合、ソフトウェアベンダーは、ソフトウェアライセンスがそのような使用に対応することを示して<利用組織>を誤解させてはならない。
要件 10.0. <利用組織>がソフトウェアライセンスの再販および譲渡の権利を有する場合、ソフトウェアベンダーは、再販のライセンスを合法的に取得した<利用組織>にとって公正な条件でサポートおよびパッチを引き続き提供する必要がある。

2.5.3 プロジェクトごとに契約締結先を選択する方法

フレームワークの当事者である公共部門機関は、必要に応じて必要なサービスを発注したり「コールオフ」(中止) したりできます。フレームワーク契約のもとでコールオフ契約を結ぶことにより、調達者は、フレームワーク契約下で提供されるメリットを維持しながら、コールオフのための機能仕様を追加し、要件を詳細化することができます。

必要と認められる場合には、特定のワークロードまたはプロジェクトに対して最良のサプライヤーを特定するためにミニコンペを開催することができます。ミニコンペとは、あるロット内のすべてのサプライヤーに一連の要求事項に対応するように依頼することによって、お客様がフレームワークの下でさらにコンペを行うことです。お客様は、ロット内のすべての対応可能なサプライヤーに入札を依頼するため、クラウドサービス RFP の契約締結先には最低限の要件を設定して、各ロットのオプションに対して高い基準を確保することが重要です。

この場合も、あらゆるロットの契約に対して「どのような場合でも対応できるアプローチ」は、技術的な実現可能性と互換性に問題が生じるため、提案の種類 (公共部門の IaaS/PaaS、コミュニティの IaaS/PaaS、民間部門の IaaS/PaaS) のロットカテゴリー別に契約の契約条件 (Terms & Conditions) が明確に設定されていることが重要になります。

契約締結先の選考に関する RFP 言語のサンプルについては、セクション 2.1.4 を参照してください。

2.5.4 オンボーディングとオフボーディング

クラウドフレームワーク契約を設定する際の留意点のひとつは、動的購買システム (Dynamic Purchasing System: DPS) というオプションです。DPS モデルを使用すると、フレームワーク契約の最低要求事項を満たすすべてのベンダーがフレームワークに参加することが認められます。フレームワークに参加できるベンダーの数に厳しい制限はありません。また、従来のフレームワークモデルとは異なり、ベンダーは「DPS フレームワーク」の存続期間中にいつでも参加を申請することも可能です。

公共部門の事業体に対しては、適格なベンダーのサービスの品質と保証が確保されるように高い基準を設けることを強く推奨しますが、公正な競争が保証できない方法でクラウドサービス事業者を不適格にするほど固有のものであってはいけません。最終目標は、利用可能なクラウドテクノロジーの標準を高く維持しながら、エンドユーザーに膨大な数のオプションを示して供給過剰にしないようにすることです。

3.0 ベストプラクティス/教訓

以下に、適切に作成されたクラウドサービス RFP を用いてクラウドフレームワーク契約の実現を成功させる方法について得られた教訓を紹介します。

3.1 クラウドガバナンス

クラウドにおけるガバナンスは責任の共有です。クラウドサービス事業者は、クラウド環境のあらゆる側面にクラウドガバナンスを組み込むための機能とサービスを提供します。一方、お客様は既存のクラウドガバナンスの基準を持ち込み、クラウドがいかにクラウドガバナンスのイネーブラーになるかを学びます。

クラウドでは、お客様は所有している IT 環境を管理するだけでなく、必要な IT 環境を構築することができます。クラウドによって、お客様は次のことを行えます。(1) すべての IT 資産のインベントリを完備した状態でスタートできます。(2) これらの資産をすべて一元管理します。(3) 使用法・課金・セキュリティなどに関するアラートを作成できます。このようなクラウドの重要なメリットを通して、お客様は、最適化され、最大限に自動化されたアーキテクチャを実現することができます。新しいハードウェアを継続的に調達してインストールする必

要はありません。これはクラウドサービス事業者によって実現されるため、お客様は、付加価値を生み出さないインフラストラクチャ管理から解放され、よりミッションクリティカルな運用レベルに重点を移すことができます。

クラウドサービス事業者のクラウドは事実上、非常に大きな API であると考えると分かりやすくなります。新しいサーバーを起動する場合でも、セキュリティ設定を変更する場合でも、API を呼び出すだけで構いません。環境を変更するたびに、その変更のログが取られて記録されます (各変更の実行者、内容、場所、および日時が記録されます)。これにより、クラウド環境でのみ実現可能なクラウドガバナンス、クラウドコントロール、および可視性が与えられます。お客様は、現在使用中の IT ガバナンスモデルを見直し、クラウドがもたらすメリットを活用することで、これらのモデルをいかにして合理化し、改善できるのかを判断できます。

クラウドガバナンスは、クラウドによってもたらされる積極的なプロセス変更や新しいスキルセットを伝達し、取り入れることでもあります。例えば、プロジェクトマネージャは、IT 環境が構築されるのを何ヶ月も待つことに慣れているため、クラウドに開発環境またはテスト環境を構築するためのスケジュールを大幅に過剰に見積もる可能性があります (クラウドを使えば、ほんの数分で行えます)。この新たな俊敏性への適応は徐々に進むプロセスであり、それはプログラムごとに起こります。このような教訓を共有することで、要求事項が新しいプロセスや俊敏性に適切に適合できるようにクラウドフレームワーク契約を進化させ続けることができます。

3.2 クラウドの予算

公共部門の調達と予算編成の要求事項に合わせて従量課金方式のクラウド料金設定を構築する場合は、クラウドサービス事業者のサービスを単一のラインアイテム (コンピューティング、ストレージ、ネットワーキング、データベース、IoT など) にバンドルし、すべてを**クラウドテクノロジー**というラインアイテムのもとで扱うことがよいことがわかりました。この手法では、クラウドサービス事業者の現在と新規のすべてのテクノロジーをリアルタイムでユーザーに提供するという柔軟性が得られ、ユーザーが必要なときに必要なリソースにすばやくアクセスできるようになります。また、変動する需要にも対応でき、利用率の最適化とコストの削減を実現します。

公共部門の組織は、コンサルティングやプロフェッショナルサービスまたはマネージドサービス、あるマーケットプレイスのソフトウェア、クラウドサポートサービス、およびクラウドサービス事業者が提供するサービスのトレーニングが必要になった場合に、クラウドフレームワーク上で他のロットからのオーダーにさらにラインアイテムを追加することができます。

適切なリソースカテゴリでオプション契約のライン品目を採用することで、契約の柔軟性を高めて将来の成長に対応することができます。また、クラウドテクノロジーとコンサルティング・プロフェッショナルサービス・マネージドサービスを 1 つのライン品目にバンドルする場合は、「クラウドテクノロジーとそれに付随する役務」などのライン品目が利用できます。

以下に、この手法の代表例を示します。以下の例では、ライン品目「#1001 - クラウドテクノロジー」の各ユニットは、使用した「クラウドテクノロジー」の €1.00 に相当します。毎月、現在および予測される使用量予測に基づいて、発注増分を資金として積み立てることができます。

表 3 - 単一ライン品目の価格設定体系の例

アイテム番号	供給/サービス	数量	単位	単価	金額
1001	クラウドテクノロジー	1,000	件別	€1	€1,000
1002	コンサルティングサービス	1	週別	€ 3,000	€ 3,000
1003	クラウドサポート	1	月別	€ 1,000	€ 1,000
1004	クラウドトレーニング	1	日別	€ 3,00	€ 3,000
1005	クラウドマーケットプレイス	10	件別	€ 10	€ 100

この体系が機能する仕組みを示す例として、公共部門の組織がクラウドサービス事業者と連携し、クラウドテクノロジーサービスの利用率を推定します。この組織は 5 年間で 1000 万ユーロ、つまり、1 年ごとに 200 万ユーロという条件でベンダーと合意しています。同組織は最初に年額 200 万ユーロを拠出します。毎月請求が発生し、その代金は資金から引き落とされます。その口座の残高は減少していきます。残りの資金は、クラウドサービス事業者の監視・予測ツールを使用して回転率が監視されます。資金の残高が少なくなると、組織はサービスの維持にコミットできる追加資金を CFO に要求します。

RFP 言語のサンプル: 価格設定 - 契約

支払条件

支払条件は、以下に示すように、**<利用組織>**が使用したリソースに対してのみ支払うように適切に設定する必要がある。

1. 月別支払いは、サービスの実際の利用量/消費量に基づくものとし、クラウドサービス事業者が公表している価格設定に従うものとする。

最低限の保証と最大限の支出

ある期間に特定のクラウドサービスプロバイダーのリソースがどの程度消費されるかを**<利用組織>**が正確に判断することは不可能であるため、オーダーは「クラウドテクノロジー」に対する単一の発注ライン品目の固定価格のユニット数量として指定される。

発注されたライン品目の各ユニットは、発注されたクラウドテクノロジーの**< € 1.00>**に相当する。このオーダーをさまざまな数量に変更して追加オーダーを定期的に行うことによって、**<利用組織>**は、変動する期間のニーズに対して推定される使用量に基づいてクラウドサービス事業者のクラウドテクノロジーのさまざまな「ユーロ金額」の数量を事前に発注できるという柔軟性が得られる。多様な要求事項を満たすために使用されるクラウドテクノロジーの推定コストをカバーするのに十分な金額で、**<利用組織>**は数量を定期的に事前発注する。

アイテム番号	説明	数量	単位	価格
01	クラウドサービス事業者のクラウドテクノロジー	1,000	EA	€ 1,000.00

最小オーダー/追加オーダー

オーダーは<10.000>というライン品目ユニットのさまざまな数量に対して定期的に行われるが、これは**<利用組織>**のクラウドテクノロジーの推定使用量に基づいて行われる。この仕組みにより、**<利用組織>**は、クラウドコンピューティングの運用サポートと「賦課方式」という商慣行との整合性を保つために必要な**< 10,000 >**ユニットの「クラウドテクノロジー」を事前に発注できる柔軟性が得られる。

コールオフが実行されると、初期追加分の**< 100,000 >**ユニットが**<€ 100.000 >**の対価として発注される。1つまたは複数のライン品目を使用して単一の追加オーダーに対して発行できる合計ライン品目ユニッ

トの最小数は<x>である。 納入指示で発注できる最大ユニット数が<x>を超えることはできないが、以前に発注したすべてのユニットと組み合せると、コールオフ値を超えることはない。**<利用組織>**は、すべてのオーダーがこのセクションで指定した限度内になるようにする責任を有する。

最大オーダー

最大オーダー合計値は<x>までとする。これは、ユニットあたり<x>で価格設定された単一ライン品目の<x> ユニットを最大として構成されたものである。この値は、実行期間での**<利用組織>**の要求事項の推定に基づいているが、保証されていない。

3.3 パートナーのビジネスモデルを理解する

公共部門の事業体は、クラウドサービス事業者のサービス提供モデルについて理解を深めるとともに、コンサルティング、マネージドサービス、再販などを提供するパートナーがこのプロセスにおいてより重要であることを認識する必要があります。多くのお客様は、自社のインフラストラクチャ向けにクラウドサービス事業者を必要としており、「実践的な」プランニング、移行、および管理作業をシステムインテグレーター (SI) またはマネージドサービスプロバイダーにアウトソーシングしています。このように「サービス」が混在している状況では、下請業者に対するフローダウン条項など、クラウドサービス事業者には適用されない要求事項が存在するかもしれません。

このようなフローダウン条項を用いて、パートナーと再販業者がクラウドサービス事業者とどのように関連しているかを理解することがなぜ重要であるかを説明すると、一部の調達形態では、主契約者に対し、特定の必須条項をすべてのパートナーおよび下請業者にフローダウンすることを求める条項が存在します。通常、クラウドサービス事業者が大規模に提供する標準化されたサービスは、特定のエンドユーザー固有の要求事項 (公共部門の契約に基づく公共部門のお客様のニーズを含む) に適合するように調整されたものではないため、正式な下請けパートナーとして対応したり、入札に応じたりすることはありません。間接調達モデル (クラウドサービス事業者の再販事業者によるクラウドサービスの調達) では、クラウドサービス事業者は、商業サービスの「第 2 階層」供給者には適用されないとして、再販業者に対してこれらの条項を拒否することができます。この場合、クラウドサービス事業者自身が契約上の業務範囲の遂行者ではなく、クラウドサービス事業者のパートナーがクラウドサービス事業者のインフラストラクチャを使用して業務を遂行しています。したがって、クラウドサービス事業者は、

パートナーの業務に対する商業上のサプライヤーになります (下請業者ではありません)。直接調達モデル (クラウドサービス事業者からクラウドサービスを直接購入する) では、クラウドサービス事業者は、典型的な商品下請業者に適したこれらの「必須」条項を通常は拒否します。それは、契約対象サービスの商業的な性質と、多くのクラウドサービス事業者が自社の商業的サービスを供給するのに下請業者を必要としないためです。

3.4 クラウドブローカー

ベンダーロックインの可能性を低減する手段であるクラウドブローカーの概念には、問題がある可能性があります。クラウドブローカーは理論上、健全な考え方かもしれませんが、実際には実現される価値よりも複雑さと混乱をもたらす可能性が高いと思われます。

複数のクラウドにまたがり、同時に、あるいは交互に機能するようアプリケーションを設計すると、実現能力のトレードオフが避けられません。つまり、**クラウドにとってのロゼッタストーン (問題解決につながる重大な鍵) は存在しないのです。**この手法では最終的に、公共部門のお客様とクラウドサービスとの間に複雑性という不必要な層が追加され、達成しようとしている効率性とセキュリティの向上が損なわれる可能性があります。その結果、拡張性と俊敏性が低下し、コストの増加につながり、イノベーションが減速します。

3.5 RFP 前のソーシング/市場調査

公共部門の事業体がクラウドサービスの RFP を計画する場合は、プロセスの最初から、すべての関連組織 (上級リーダー、業務上のステークホルダー、技術、財務、調達、法務、契約) のステークホルダーを含める必要があります。この手法により、すべてのステークホルダーがクラウドモデルを確実に理解できるようになります。その結果、学習を経て、従来の IT 調達方法を再評価することに取り組めるようになります。

産業界との対話に関しては、公共部門の事業体は時間をかけて徹底的な対話を行い、産業界 (クラウドサービス事業者やそのパートナー、PaaS/SaaS マーケットプレイスのベンダー、産業界の専門家) からフィードバックを集めることを強く推奨します。例えば、このような対話は、特定の産業ごとにセキュリティと調達のワークショップといった形式で実施することができます。クラウド調達に関して理解を深めるもう一つの効果的な方法は、RFI のリリース、理想的には

RFP 文書の草案をリリースすることです。多くの場合、最終的なクラウドサービスの RFP がリリースされる前に、潜在的な問題が指摘され、議論や調整が可能になります。

3.6 持続可能性

持続可能性はクラウドコンピューティングに固有のものであり、クラウドに移行することで、オンプレミスのサーバーやエンタープライズデータセンターに比べてエネルギー効率が向上します。持続可能性を優先しており、持続可能性の目標を達成することを公約しているクラウドサービス事業者を特定すると、クラウドが持続可能なものになるという保証が高まります。欧州のクラウドサービス事業者とデータセンター事業者 (欧州委員会の支援のもと)は、気候中立的データセンター協定 (Climate Neutral Data Centre Pact) [11]を設立しました。これは、データセンター産業の持続可能性に関して明確かつシンプルな将来にわたる基準を確立し、データセンター事業者とクラウドサービス事業者が 2030 年までに気候中立的となるための自主規制イニシアチブです。この自主規制イニシアチブには、データセンターのエネルギー効率、水の保全、サーバーの再利用と修理、カーボンフリーのエネルギーを利用したデータセンターの稼働に関する明確な目標が盛り込まれています。自主規制イニシアチブに調印するクラウドサービス事業者は、これらの目標を達成することに合意し、気候中立的な事業者であるとみなすための基準に照らし合わせて認定が行われます。

クラウドサービスの RFP では、クラウドサービス事業者に対して、このような基準にコミットしているかどうか、特に自主規制に参加しているかどうかと、このようなコミットメントを行った時期について確認する必要があります。

RFP 言語のサンプル: 持続可能性

気候中立的データセンターの、自主規制イニシアチブに調印することで、気候中立的データセンターの運営にコミットしているか。 コミットしている場合、調印者となったかどうか。

気候中立的データセンター協定の印を利用のために与えられているかどうか。

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

付録 A – 入札者相互間の比較に関する技術的要求事項

以下に、クラウドフレームワーク契約のコールオフ時またはミニコンペの際に、クラウドサービス事業者の比較検討に使用できる一般的なクラウドテクノロジー要求事項を示します。

1.クラウドサービス事業者のプロファイル

	要求事項
1.	**市場実績:** このクラウドサービス事業者は、クラウド市場で何年事業を展開しているか?
2.	**開放性とデータ保護:** このクラウドサービス事業者は、データ保護または復元可能性に関する業界の行動規範を遵守しているか? このクラウドサービス事業者は、オープンソースとオープン API の開発原則を遵守しているか?

2.グローバルインフラストラクチャ

	要求事項
1.	**グローバルな展開** このクラウドサービス事業者は、ユーザーが低レイテンシーと高スループットを達成できるグローバルなインフラストラクチャを提供しているか?
2.	**地域:** このクラウドサービス事業者は、必要とされる地域に拠点を擁しているか?
3.	**ドメイン/ゾーン:** このクラウドサービス事業者は、複数のデータセンターが低レイテンシーのネットワークを介してグループ化し、より高いレベルの高可用性とフォルトトレランスを提供するドメインまたはゾーンの概念を実装しているか? • 「はい」の場合は、必要とされる地域内のドメインまたはゾーンの数とデータセンターの数を記載すること。

4.	**ドメイン/ゾーンの距離:** このクラウドサービス事業者は、冗長性、高可用性、および低レイテンシーをサポートするために、物理的に離れた場所にあるデータセンターを使ってドメインまたはゾーンを構築しているか?
5.	**データセンターの構築:** このクラウドサービス事業者は、他のデータセンターの障害から分離されるように設計されたデータセンターに、冗長電源、冷却機能、およびネットワーキングを備えているか?
6.	**データセンターのレプリケーション:** このクラウドサービス事業者は、自動フェイルオーバー機能を備えたドメインまたはゾーン内のデータセンター間でのデータレプリケーションを提供しているか?
7.	**ドメイン/ゾーンのレプリケーション:** このクラウドサービス事業者は、ある地域内のドメインまたはゾーン間でのデータレプリケーションを提供しているか?

3.インフラストラクチャ

3.1 コンピューティング

	要求事項
1.	**コンピューティング - 通常のインスタンス - 汎用:** このクラウドサービス事業者は、以下のインスタンスタイプを提供しているか? • 汎用 - 汎用アプリケーション向けに最適化され、コンピューティング、メモリ、およびネットワークリソースの間でバランスをとったインスタンスタイプ。 ○ 「はい」の場合、最大のインスタンスは何か?
2.	**コンピューティング - 通常のインスタンス - メモリ最適化:** このクラウドサービス事業者は、以下のインスタンスタイプを提供しているか? • メモリ最適化 - メモリ負荷の高いアプリケーション向けに最適化されたインスタンスタイプ ○ 「はい」の場合、最大のインスタンスは何か?

3.	**コンピューティング - 通常のインスタンス - コンピューティング最適化:** このクラウドサービス事業者は、以下のインスタンスタイプを提供しているか? • コンピューティング最適化 - コンピューティング集約型のアプリケーション向けに最適化されたインスタンスタイプ o 「はい」の場合、最大のインスタンスは何か?
4.	**コンピューティング - 通常のインスタンス - ストレージ最適化:** このクラウドサービス事業者は、以下のインスタンスタイプを提供しているか? • ストレージ最適化- 大量のローカルストレージ容量を提供するインスタンスタイプ o 「はい」の場合、最大ストレージ容量 (5、10、20、50 TB) とインスタンスに提供可能かつ接続可能な最大ディスク数 (HDD/SSD) はいくつか?
5.	**コンピューティング - 通常のインスタンス - グラフィック最適化:** このクラウドサービス事業者は、以下のインスタンスタイプを提供しているか? • 低コストのグラフィック - 低コストのグラフィックアクセラレーションをコンピューティングインスタンスに提供 o 「はい」の場合、最大のインスタンスは何か?
6.	**コンピューティング - 通常のインスタンス - GPU 最適化:** このクラウドサービス事業者は、以下のインスタンスタイプを提供しているか? • GPU - グラフィック集約型アプリケーション用のハードウェアのグラフィック処理装置 (GPU) を提供 o 「はい」の場合、このクラウドサービス事業者はインスタンスごとに何台の GPU と、どの GPU モデルを提供できるか?
7.	**コンピューティング - 通常のインスタンス - FPGA 最適化:** このクラウドサービス事業者は、以下のインスタンスタイプを提供しているか? • FPGA - アプリケーション用にカスタムハードウェアアクセラレーションを開発および展開するためのフィールドプログラマブルゲートアレイ (FPGA) を提供 o 「はい」の場合、このクラウドサービス事業者はインスタンスごとに何個の FPGA を提供できるか?

8.	**コンピューティング - バースト可能インスタンス**: このクラウドサービス事業者は、中央演算処理装置 (CPU) のベースラインレベルのパフォーマンスを提供し、ベースラインを超えるバーストを可能にする能力を備えたバースト可能なインスタンスを提供しているか? • 「はい」の場合、最大のバースト可能なインスタンスは何か?
9.	**コンピューティング - IO 集約型インスタンス**: このクラウドサービス事業者は、低レイテンシー、超高ランダム I/O パフォーマンス、および高シーケンシャル読み取りスループットに最適化された不揮発性メモリ express (NVMe) ソリッドステートドライブ (SSD) を使用するインスタンスを提供しているか? • 「はい」の場合、最大インスタンスの毎秒最大 I/O 処理 (IOPS) の容量はいくつか？
10.	**コンピューティング - 一時ローカルストレージ**: このクラウドサービス事業者は、頻繁に変更される情報の一時ストレージに使用されるコンピューティングインスタンスのローカルストレージをサポートしているか?
11.	**コンピューティング - 複数の NIC サポート**: このクラウドサービス事業者は、特定のインスタンスに割り当てられる複数の (プライマリおよび追加の) ネットワークインターフェイスカード (NIC) をサポートしているか? • 「はい」の場合、インスタンスあたりの NIC 最大数はいくつか?
12.	**コンピューティング - インスタンスのアフィニティー**: このクラウドサービス事業者は、同じデータセンター内でインスタンスを論理的にグループ化する機能をユーザーに提供しているか?
13.	**コンピューティング - インスタンスの反アフィニティー**: このクラウドサービス事業者は、インスタンスを論理的にグループ化し、それを地域内の異なるデータセンターに配置する機能をユーザーに提供しているか?
14.	**コンピューティング - セルフサービスのプロビジョニング**: このクラウドサービス事業者は、プログラマチックなインターフェイス、管理コンソール、または Web ポータルを通じて、複数インスタンスに対して同時実行されるセルフサービスのプロビジョニングを提供しているか?
15.	**コンピューティング - カスタマイズ**: このクラウドサービス事業者は、カスタマイズ可能なインスタンス、すなわち、仮想中央処理装置 (vCPU) やランダムアクセスメモリ (RAM) などの構成設定を変更する機能を提供しているか?

16.	**コンピューティング - テナント属性**: このクラウドサービス事業者は、1 人のユーザー専用のハードウェア上で動作するシングルテナントインスタンスを提供しているか? • 「はい」の場合、使用可能なシングルテナントインスタンスで最大のものはどれか?
17.	**コンピューティング - ホストのアフィニティー**: このクラウドサービス事業者は、インスタンスを起動し、このインスタンスが常に同じ物理ホスト上で再起動するように指定する機能を提供しているか?
18.	**コンピューティング – ホストの反アフィニティー**: このクラウドサービス事業者は、異なる物理ホスト間で特定のインスタンスを分割してホストする機能を提供しているか?
19.	**コンピューティング - オートスケーリング**: このクラウドサービス事業者は、パフォーマンスを維持するために、需要の急増時にインスタンス数を自動的に増加させる機能 (つまり「スケールアウト」) を提供しているか?
20.	**コンピューティング - イメージのインポートの仕組み**: このクラウドサービス事業者は、ユーザーが既存のイメージをインポートし、将来においてインスタンスのプロビジョニングに使用できる新しい非公開のイメージとして保存できる機能を提供しているか? • 「はい」の場合、どのフォーマットがサポートされているか?
21.	**コンピューティング - イメージのエクスポートの仕組み**: このクラウドサービス事業者は、既存の実行中のインスタンスまたはインスタンスのコピーを取得して、そのインスタンスを仮想マシンのフォーマットにエクスポートする機能をサポートしているか? • 「はい」の場合、どのフォーマットがサポートされているか?
22.	**コンピューティング - サービス中断**: このクラウドサービス事業者は、ホストレベルでハードウェアやサービスのメンテナンスを行っている際、インスタンスの停止やダウンタイムを回避する仕組みを提供しているか?
23.	**コンピューティング - インスタンスの再起動**: このクラウドサービス事業者は、元の物理ホストに障害が発生した場合に、正常なホスト上でインスタンスを自動的に再起動する仕組みを提供しているか?

24.	**コンピューティング - 通知**: 回復力のあるコンピューティングイベントの場合、このクラウドサービス事業者は、そのようなイベントが発生したことをユーザーに通知する機能を有しているか? また、ユーザーは、セルフサービスでこの通知を有効化または無効化することができるか?
25.	**コンピューティング - イベントスケジューリング**: このクラウドサービス事業者は、インスタンスの再起動、停止、起動、廃棄など、ユーザーのインスタンスのイベントをスケジュールする機能を提供しているか?
26.	**コンピューティング - バックアップとリストアの仕組み**: このクラウドサービス事業者は、バックアップとリカバリを統合した仕組みを提供しているか?
27.	**コンピューティング - スナップショットの仕組み**: このクラウドサービス事業者は、手動のオンデマンドスナップショットの仕組みを提供しているか?
28.	**コンピューティング - メタデータ**: このクラウドサービス事業者は、ユーザーが任意のキーと値のペアをインスタンスに設定できるようなインスタンスメタデータサービスを提供しているか?
29.	**コンピューティング - メタデータコール**: このクラウドサービス事業者は、インスタンスが自身に関する情報を見つけるために呼び出すことができるアプリケーションプログラミングインターフェイス (API) を提供するインスタンスメタデータサービスを提供しているか?
30.	**コンピューティング – 入札の仕組み**: このクラウドサービス事業者は、非ミッションクリティカルなワークロードをホストするために、即時のインスタンス化が可能な、より低いコストのインスタンスに入札する仕組みを提供しているか?
31.	**コンピューティング - スケジュール設定の仕組み**: このクラウドサービス事業者は、追加のコンピューティング能力を定期的にスケジュールして予約する方法を提供しているか (日単位、週単位、月単位など)?
32.	**コンピューティング - 予約の仕組み**: このクラウドサービス事業者は、将来のために追加のコンピューティング能力を予約する方法を提供しているか (1 年、2 年、3 年など)?

33.	**コンピューティング - Linux オペレーティングシステム:** このクラウドサービス事業者は、少なくとも 1 つのエンタープライズ Linux ディストリビューション (Red Hat、SUSE など) と、 1 つの一般的に使われているフリー Linux ディストリビューション (Ubuntu、CentOS、Debian など) の、最新の 2 つの長期サポートバージョンをサポートしているか?
34.	**コンピューティング - Windows オペレーティングシステム:** このクラウドサービス事業者は、Windows Server の最新の 2 つの主要バージョン (Windows Server 2017 および Windows Server 2016) をサポートしているか?
35.	**コンピューティング - ライセンスのポータビリティ:** このクラウドサービス事業者はライセンスのポータビリティとサポートを提供しているか? • 「はい」の場合は、ソフトウェアベンダー、ソフトウェア名、エディション、およびそのバージョンを記載すること。
36.	**コンピューティング – サービスの制限:** このクラウドサービス事業者は、上記のコンピューティングセクションに関して、何らかの制限 (つまり、サービスの制限) を設けているか? 例: アカウントごとのインスタンスの最大数 アカウントごとの専用ホストの最大数 予約済みインターネットプロトコル (IP) アドレスの最大数

3.2 ネットワーキング

	要求事項
1.	**ネットワーキング – 仮想ネットワーク:** このクラウドサービス事業者は、クラウド内の企業独自のネットワークを表す分離された仮想ネットワークというロジックを作成する機能をサポートしているか?
2.	**ネットワーキング - 同一地域の接続性:** このクラウドサービス事業者は、プライベートインターネットプロトコル (IP) アドレスを使用して、同一地域内の 2 つの仮想ネットワークを接続し、この 2 つの仮想ネットワーク間でトラフィックをルーティングする機能をサポートしているか?

3.	**ネットワーキング - 異なる地域の接続性:** このクラウドサービス事業者は、異なる地域にまたがる 2 つの仮想ネットワークを接続し、プライベートインターネットプロトコル (IP) アドレスを使用してこの 2 つの仮想ネットワーク間でトラフィックをルーティングする機能をサポートしているか?
4.	**ネットワーキング – プライベートサブネット:** このクラウドサービス事業者は、パブリックなインターネットプロトコル (IP) アドレスまたはインターネットルーティングを使用せずにインスタンスのプロビジョニングを行える完全に分離された (プライベート) 仮想ネットワークおよびサブネットを作成する機能を提供しているか?
5.	**ネットワーキング - 仮想ネットワークのアドレス範囲:** このクラウドサービス事業者は、パブリックにルーティング可能なクラスレスドメイン間ルーティング (CIDR) ブロックと同様に、 Request for Comments (RFC) 1918 で指定されたインターネットプロトコル (IP) アドレス範囲をサポートしているか?
6.	**ネットワーキング - 複数のプロトコル:** このクラウドサービス事業者は、伝送制御プロトコル (TCP)、ユーザーデータグラムプロトコル (UDP)、およびインターネット制御メッセージプロトコル (ICMP) を含む複数のプロトコルをサポートしているか?
7.	**ネットワーキング - IP アドレスの自動割当:** このクラウドサービス事業者は、パブリックなインターネットプロトコル (IP) アドレスをインスタンスに自動的に割り当てる機能をサポートしているか?
8.	**ネットワーキング - 予約済みの固定 IP アドレス:** このクラウドサービス事業者は、特定のインスタンスではなく、ユーザーアカウントに関連付けられたインターネットプロトコル (IP) アドレスをサポートしているか? その IP アドレスは、明示的に解放されるまでアカウントに関連付けられたままにすること。
9.	**ネットワーキング - IPv6 サポート:** このクラウドサービス事業者は、ゲートウェイまたはインスタンスのレベルでインターネットプロトコルバージョン 6 (IPv6) をサポートし、この機能をユーザーに公開しているか?
10.	**ネットワーキング - NIC ごとの複数の IP アドレス:** このクラウドサービス事業者は、所定のインスタンスに接続されているネットワークインターフェイスカード (NIC) にプライマリおよびセカンダリインターネットプロトコル (IP) アドレスを割り当てる機能をサポートしているか?

11.	**ネットワーキング - 複数の NIC:** このクラウドサービス事業者は、複数のネットワークインターフェイスカード (NIC) を所定のインスタンスに割り当てる機能をサポートしているか?
12.	**ネットワーキング - NIC と IP の移動性:** このクラウドサービス事業者は、ネットワークインターフェイスカード (NIC) とインターネットプロトコル (IP) アドレスをインスタンス間で移動する機能をサポートしているか?
13.	**ネットワーキング - SR-IOV サポート:** このクラウドサービス事業者は、パフォーマンスの向上 (毎秒パケット数 - PPS)、レイテンシーの短縮、ジッタの低減を実現するために、シングルルート入出力仮想化 (SR-IOV) などの機能をサポートしているか?
14.	**ネットワーキング - 受信のフィルタリング:** このクラウドサービス事業者は、インスタンスへのインバウンドトラフィック (受信) に適用可能なルールの追加や削除をサポートしているか?
15.	**ネットワーキング- 送信のフィルタリング:** このクラウドサービス事業者は、インスタンスから発信されるアウトバウンドトラフィック (送信) に適用可能なルールの追加または削除をサポートしているか?
16.	**ネットワーキング – ACL:** このクラウドサービス事業者は、サブネットへのインバウンドおよびアウトバウンドトラフィックを制御するためのアクセス制御リスト (ACL) を提供しているか?
17.	**ネットワーキング - フローログサポート:** このクラウドサービス事業者は、ネットワークトラフィックフローログをキャプチャする機能を提供しているか?
18.	**ネットワーキング – NAT:** このクラウドサービス事業者は、プライベートネットワーク内のインスタンスがインターネットやその他のクラウドサービスに接続できても、インターネットがそれらのインスタンスへの接続を開始できないようにするネットワークアドレス変換 (NAT) ゲートウェイのマネージドサービスを提供しているか?
19.	**ネットワーキング - 送信元/送信先チェック:** このクラウドサービス事業者は、ネットワークインターフェイスカード (NIC) の送信元/送信先チェックを無効にする機能を提供しているか?

20.	**ネットワーキング – VPN サポート**: このクラウドサービス事業者は、クラウドサービス事業者とユーザーのデータセンター間の仮想プライベートネットワーク (VPN) 接続をサポートしているか?
21.	**ネットワーキング – VPN トンネル**: このクラウドサービス事業者は、仮想ネットワークごとに複数の仮想プライベートネットワーク (VPN) 接続をサポートしているか?
22.	**ネットワーキング - IPSEC VPN サポート**: このクラウドサービス事業者は、ユーザーがパブリックインターネット上でインターネットプロトコルセキュリティ (IPsec) の仮想プライベートネットワーク (VPN) トンネルまたはセキュアソケットレイヤー (SSL) の仮想プライベートネットワーク (VPN) トンネルのいずれかを経由してクラウドサービスにアクセスすることを許可しているか?
23.	**ネットワーキング – BGP サポート**: このクラウドサービス事業者は、インターネットプロトコルセキュリティ (IPsec) の複数の仮想プライベートネットワーク (VPN) トンネルにまたがっているフェイルオーバーを改善するために、ボーダーゲートウェイプロトコル (BGP) を採用しているか?
24.	**ネットワーキング - プライベート専用接続**: このクラウドサービス事業者は、大規模で高速なデータ移転を可能にする、クラウドサービス事業者の所在地とユーザーのデータセンター、オフィス、またはコロケーション環境との間で直接的なプライベート接続サービスを提供しているか?
25.	**ネットワーキング - フロントエンドロードバランサー**: このクラウドサービス事業者は、インターネット経由でクライアントからの要求を受け取り、ロードバランサーに登録されているインスタンス間でその要求を配信するフロントエンド (インターネット接続) のロードバランシングサービスを提供しているか?
26.	**ネットワーキング - バックエンドロードバランサー**: このクラウドサービス事業者は、プライベートサブネットでホストされているインスタンスにトラフィックをルーティングするバックエンド (プライベート) のロードバランシングサービスを提供しているか?
27.	**ネットワーキング - レイヤー 7 のロードバランサー**: このクラウドサービス事業者は、複数のインスタンス間でネットワークトラフィックの負荷分散が可能なレイヤー7 (ハイパーテキスト転送プロトコル - HTTP) のロードバランサーサービスを提供しているか?

28.	**ネットワーキング - レイヤー 4 のロードバランサー:** このクラウドサービス事業者は、複数のインスタンス間でネットワークトラフィックの負荷分散が可能なレイヤー 4 (伝送制御プロトコル - TCP) のロードバランサーサービスを提供しているか?
29.	**ネットワーキング - ロードバランサーのセッションアフィニティー:** このクラウドサービス事業者は、セッションアフィニティーをサポートするロードバランシングサービスを提供しているか?
30.	**ネットワーキング - DNS ベースのロードバランシング:** このクラウドサービス事業者は、単一のドメインに属する複数のホストでホストされているインスタンスにトラフィックを負荷分散できるロードバランシングサービスを提供しているか?
31.	**ネットワーキング - ロードバランサーのログ:** このクラウドサービス事業者は、ロードバランサーに送信されたすべての要求に関する詳細情報をキャプチャするログを提供しているか?
32.	**ネットワーキング – DNS:** このクラウドサービス事業者は、可用性と拡張性に優れたドメインネームシステム (DNS) サービスを提供しているか?
33.	**ネットワーキング – レイテンシーベースの DNS ルーティング:** このクラウドサービス事業者は、レイテンシーベースのルーティングをサポートするドメインネームシステム (DNS) サービス (つまり、DNS サービスは DNS クエリーに対して、最適なレイテンシーを提供するリソースで応答する) を提供しているか?
34.	**ネットワーキング – 地理情報ベースの DNS ルーティング:** このクラウドサービス事業者は、地理情報ベースのルーティングをサポートするドメインネームシステム (DNS) サービス (つまり、DNS サービスは、ユーザーの地理的位置に基づいて DNS クエリーに応答する) を提供しているか?
35.	**ネットワーキング - フェイルオーバーベースの DNS ルーティング:** このクラウドサービス事業者は、フェイルオーバーベースのルーティングをサポートするドメインネームシステム (DNS) サービス (つまり、DNS サービスは DNS クエリーを現在アクティブなリソースにルーティングする。一方、2 番目のリソースは待機し、プライマリリソースで障害が発生した場合にのみアクティブになる) を提供しているか?

36.	**ネットワーキング - ドメイン登録サービス:** このクラウドサービス事業者は、ドメインネーム登録サービス (ユーザーは利用可能なドメイン名を検索して登録できる) を提供しているか?
37.	**ネットワーキング - DNS の健全性チェック:** このクラウドサービス事業者は、健全性チェックを使用してリソースの健全性とパフォーマンスを監視するドメインネームシステム (DNS) サービスを提供しているか?
38.	**ネットワーキング - DNS とロードバランサーの統合:** このクラウドサービス事業者は、クラウドサービス事業者のロードバランサーと統合されたドメインネームシステム (DNS) サービスを提供しているか?
39.	**ネットワーキング – ビジュアルエディター:** このクラウドサービス事業者は、ユーザーがトラフィック管理のポリシーを構築できるツールを提供しているか?
40.	**コンテンツ配信ネットワーク (CDN):** このクラウドサービス事業者は、低レイテンシーかつ高速なデータ転送速度でコンテンツを配信するためのコンテンツ配信ネットワーク (CDN) サービスを提供しているか?
41.	**ネットワーキング - CDN キャッシュの期限切れ:** このクラウドサービス事業者は、オブジェクトの無効化やオブジェクトのバージョン管理などの機能を含め、期限切れになる前にエッジキャッシュからオブジェクトを削除できるコンテンツ配信ネットワーク (CDN) サービスを提供しているか?
42.	**ネットワーキング - CDN の外部配信元:** このクラウドサービス事業者は、カスタム配信元、すなわちハイパーテキスト転送プロトコル (HTTP) サーバーをサポートするコンテンツ配信ネットワーク (CDN) サービスを提供しているか?
43.	**ネットワーキング - CDN の最適化:** このクラウドサービス事業者は、複数の配信元サーバーを構成し、異なるユニフォームリソースロケータ (URL) のプロパティをキャッシュするために詳細な制御が可能なコンテンツ配信ネットワーク (CDN) サービスを提供しているか?

44.	**ネットワーキング - CDN 地理的制限:** このクラウドサービス事業者は、特定の地域のユーザーがコンテンツにアクセスできないようにする地理的制限をサポートするコンテンツ配信ネットワーク (CDN) サービスを提供しているか?
45.	**ネットワーキング – CDN トークン:** このクラウドサービス事業者は、コンテンツへのアクセスをユーザーがより細かく制御できるように、通常は有効期限の日付/時刻などの追加情報を含む署名済み URL をサポートするコンテンツ配信ネットワーク (CDN) サービスを提供しているか?
46.	**ネットワーキング - CDN 証明書:** このクラウドサービス事業者は、エッジロケーションからセキュアなハイパーテキスト転送プロトコル (HTTPS) を介してセキュアにコンテンツを配信するために、カスタムセキュアソケットレイヤー (SSL) 証明書をサポートするコンテンツ配信ネットワーク (CDN) サービスを提供しているか?
47.	**ネットワーキング - CDN 多層キャッシュ:** このクラウドサービス事業者は、レイテンシーを短縮するために、地域エッジキャッシュを使用した多層キャッシュアプローチを採用しているコンテンツ配信ネットワーク (CDN) サービスを提供しているか?
48.	**ネットワーキング - CDN 圧縮:** このクラウドサービス事業者は、ファイル圧縮をサポートするコンテンツ配信ネットワーク (CDN) サービスを提供しているか?
49.	**ネットワーキング - CDN 暗号化アップロード:** このクラウドサービス事業者は、ユーザーの配信元インフラストラクチャ内の特定のコンポーネントおよびサービスによってのみ閲覧可能な方法で、ユーザーが機密データをセキュアにアップロードできるコンテンツ配信ネットワーク (CDN) を提供しているか?
50.	**ネットワーキング – エンドポイント:** このクラウドサービス事業者のネットワーキングサービスは、通信コストを削減し、トラフィックセキュリティを向上させるために、プロバイダーの内部ネットワーク接続 (プライベート接続) を通じてトラフィックをルーティングすることができるエンドポイントをユーザーに提供しているか?
51.	**ネットワーキング - サービスの制限:** 上記のネットワーキングセクションに関して、このクラウドサービス事業者は何らかの制限 (つまり、サービスの制限) を設けているか? 例: アカウントあたりの仮想ネットワークの最大数

	仮想ネットワークの最大サイズ アカウントあたりのサブネットの最大数 アカウントあたりのロードバランサーの最大数 アクセス制御リスト (ACL) エントリの最大数 仮想プライベートネットワーク (VPN) トンネルの最大数 配信ごとの配信元の最大数 ロードバランサーあたりの証明書の最大数

3.3 ストレージ

	要求事項
1.	**ブロックストレージサービス**: このクラウドサービス事業者は、コンピューティングインスタンスで使用するブロックレベルのストレージボリュームを提供しているか?
2.	**ブロックストレージ - IOPS:** このクラウドサービス事業者は、一定数の毎秒の入出力操作 (IOPS) やスループットの毎秒のメガバイト数 (MB/S) など、ブロックストレージボリュームに関する明示的なパフォーマンス目標またはパフォーマンス階層の購入オプションを提供しうるか?
3.	**ブロックストレージ - ソリッドステートドライブ**: このクラウドサービス事業者は、1 桁のミリ秒単位のレイテンシーを提供するソリッドステートドライブ (SSD) を搭載したストレージメディアをサポートしているか? • 「はい」の場合、インスタンスごとに接続可能な SSD の最大数はいくつか?
4.	**ブロックストレージ - 拡張:** このクラウドサービス事業者は、新たにボリュームをプロビジョニングしたり、データをコピー/移動したりすることなく、既存のブロックストレージボリュームのサイズを増加させる機能をユーザーに提供しているか?
5.	**ブロックストレージ - スナップショット**: このクラウドサービス事業者は、そのブロックストレージサービスに対してスナップショット機能を有しているか?

6.	**ブロックストレージ - データ消去:** このクラウドサービス事業者は、許可されていないユーザーや第三者によるデータの読み取りやアクセスができなくなるようなデータの完全消去をサポートしているか?
7.	**ブロックストレージ - 保存時の暗号化:** このクラウドサービス事業者は、ボリュームおよびそのスナップショットに保存されているデータに対して、保存時のデータのサーバー側での暗号化を提供しているか? • 提供している場合、採用している暗号化アルゴリズムは何ですか?
8.	**オブジェクトストレージサービス:** このクラウドサービス事業者は、Web 上のあらゆる量のデータを保存および取得するための、セキュアで耐久性があり、拡張性に優れたオブジェクトストレージを提供しているか?
9.	**オブジェクトストレージ - 頻繁ではないアクセス:** このクラウドサービス事業者は、アクセス頻度の低いオブジェクトやファイルの保存を目的とした低コストのストレージサービス階層を提供しているか?
10.	**オブジェクトストレージ - 低冗長化:** このクラウドサービス事業者は、ユーザーが重要ではない、再現しやすいオブジェクトを低価格で保存できるような、低冗長性の階層を提供しているか?
11.	**オブジェクトストレージ - 低頻度アクセス:** このクラウドサービス事業者は、アクセス頻度は低いが、高速アクセスを必要とするデータ向けに階層を提供しているか?
12.	**オブジェクトストレージ - オブジェクトの階層化:** このクラウドサービス事業者は、オブジェクトストレージの階層化機能、すなわち、アクセス頻度に基づいたオブジェクトストレージのクラスまたは階層間でのオブジェクトの移行を推奨する機能を提供しているか?
13.	**オブジェクトストレージ - ライフサイクル管理:** このクラウドサービス事業者は、オブジェクトの作成から削除までの存続期間中の管理方法を定義するライフサイクル設定を使用した、オブジェクトのライフサイクルの管理をサポートしているか?
14.	**オブジェクトストレージ - ポリシーベースの管理:** このクラウドサービス事業者は、保存されたデータとそのライフサイクルおよび階層化設定を管理するためのポリシーを作成、および適用する機能を提供しているか?

15.	**オブジェクトストレージ- 場所および時間ベースのポリシー:** このクラウドサービス事業者は、ユーザーの場所と要求時間に基づいてデータへのアクセスを制限できるポリシーを作成する機能をユーザーに提供しているか?
16.	**オブジェクトストレージ - Web サイトのホスティング:** このクラウドサービス事業者は、オブジェクトストレージサービスからの静的 Web サイトのホスティングをサポートしているか?
17.	**オブジェクトストレージ - 保存時の暗号化:** このクラウドサービス事業者は、クラウドサービス事業者が暗号化キーを管理することで、保存時のデータのサーバー側での暗号化 (SSE) をサポートしているか? • 提供している場合、採用している暗号化アルゴリズムは何ですか?
18.	**オブジェクトストレージ - ユーザーキーによる暗号化:** このクラウドサービス事業者は、顧客が提供する暗号化キーを使用したサーバー側での暗号化 (SSE) 機能を提供しているか?
19.	**オブジェクトストレージ - キー管理サービス:** このクラウドサービス事業者は、暗号化キーを作成し、キーの使用方法を制御するポリシーを定義し、キーが正しく使用されていることを証明するためにキーの使用状況を監査するキー管理サービスを使用した、サーバー側での暗号化 (SSE) をサポートしているか?
20.	**オブジェクトストレージ - クライアント側のマスターキー:** このクラウドサービス事業者は、暗号化キーの制御を維持し、クライアント側でオブジェクトの暗号化/復号化を完了するオプションをユーザーに提供しているか?
21.	**オブジェクトストレージ - 厳格な一貫性:** このクラウドサービス事業者は、新しいオブジェクトに対する PUT 操作のリードアフターライトの一貫性をサポートしているか?
22.	**オブジェクトストレージ - データの局所性:** このクラウドサービス事業者は、あるリージョンに保存されたオブジェクトが、ユーザーが明示的に他のリージョンに転送しない限り、そのリージョンから出ないようにする厳格なリージョン分離機能を提供しているか?
23.	**オブジェクトストレージ - 複製:** このクラウドサービス事業者は、ユーザーが選択したリージョン間でオブジェクトを自動的に複製する、リージョン間複製機能を提供しているか?

24.	**オブジェクトストレージ – バージョン管理**: このクラウドサービス事業者は、バージョン管理、すなわち、あるオブジェクトの複数のバージョンを保存・維持する機能をサポートしているか?
25.	**オブジェクトストレージ - 削除不可マーカー**: このクラウドサービス事業者は、ユーザーが項目を削除不可とマークできる機能を提供しているか?
26.	**オブジェクトストレージ - MFA 削除**: このクラウドサービス事業者は、追加のセキュリティオプションとして、削除操作に対して多要素認証 (Multi-Factor Authentication: MFA) をサポートしているか?
27.	**オブジェクトストレージ - マルチパートアップロード**: このクラウドサービス事業者は、各パートがオブジェクトのデータの連続した部分であり、これらのオブジェクトのパートを任意の順序で個別にアップロードできるように、オブジェクトを 1 セットのパートとしてアップロードできる機能を提供しているか?
28.	**オブジェクトストレージ - タグ**: このクラウドサービス事業者は、変更可能な動的タグをオブジェクトレベルで作成して関連付ける機能を提供しているか?
29.	**オブジェクトストレージ - 通知**: このクラウドサービス事業者は、特定のイベントがオブジェクトレベルで発生した場合 (すなわち、追加/削除操作) に通知を送信する機能を提供しているか?
30.	**オブジェクトストレージ - ログ**: このクラウドサービス事業者は、要求者、要求時間、要求アクション、応答ステータス、エラーコードなど、ひとつのアクセス要求に関する詳細を含めた監査ログを生成する機能を提供しているか?
31.	**オブジェクトストレージ - オブジェクトのインベントリ**: このクラウドサービス事業者は、ユーザーがパブリックアクセスでオブジェクトを迅速に特定できるように、オブジェクトとその状態を迅速に視覚化できるようなオブジェクトインベントリ機能を提供しているか?
32.	**オブジェクトストレージ - メタデータのインベントリ**: このクラウドサービス事業者は、ユーザーがオブジェクトのメタデータを迅速に視覚化できるようなオブジェクトインベントリ機能を提供しているか?

33.	**オブジェクトストレージ - アップロードの最適化**: このクラウドサービス事業者は、最適化されたネットワークパスを使用して、エッジロケーションからストレージサービスにデータをルーティングする機能を有しているか?
34.	**オブジェクトストレージ - 照会機能**: このクラウドサービス事業者は、構造化照会言語 (SQL) ステートメントを使用して、オブジェクトストレージサービスに照会する機能をユーザーに提供しているか?
35.	**オブジェクトストレージ - サブセットの取得**: このクラウドサービス事業者は、簡単な構造化照会言語 (SQL) 式を使用して、オブジェクトからデータのサブセットのみを取得する機能をユーザーに提供しているか?
36.	**ファイルストレージサービス**: このクラウドサービス事業者は、クラウド内のコンピューティングインスタンスで使用するための簡易かつスケーラブルなファイルストレージサービスを提供しているか?
37.	**ファイルストレージ - 冗長性**: このクラウドサービス事業者は、より高いレベルの可用性と耐久性を達成するために、複数のデータセンターまたは施設にまたがってファイルシステムオブジェクト (ディレクトリ、ファイル、リンクなど) を冗長的に保存しているか?
38.	**ファイルストレージ - データ消去**: このクラウドサービス事業者は、許可されていないユーザーや第三者によるデータの読み取りやアクセスができなくなるようなファイルストレージデータの完全消去をサポートしているか?
39.	**ファイルストレージ - 高可用性**: このクラウドサービス事業者のマネージド型ファイルシステムは、優れた高可用性を備えているか?
40.	**ファイルストレージ - NFS**: このクラウドサービス事業者は、ネットワークファイルシステム (NFS) プロトコルをサポートしているか?
41.	**ファイルストレージ - SMB**: このクラウドサービス事業者は、サーバーメッセージブロック (SMB) プロトコルをサポートしているか?
42.	**ファイルストレージ - 保存時の暗号化**: このクラウドサービス事業者のファイルストレージサービスは、保存時の暗号化をサポートしているか?

43.	**ファイルストレージ - 転送時の暗号化:** このクラウドサービス事業者のファイルストレージサービスは、転送時のデータの暗号化をサポートしているか?
44.	**ファイルストレージ - データ移行ツール:** このクラウドサービス事業者は、ユーザーがオンプレミスシステムからクラウドベースのファイルシステムにデータを移動できるようにするデータ移行ツールを提供しているか?
45.	**アーカイブストレージサービス:** このクラウドサービス事業者は、アクセス頻度が低く、ほとんど変更のないオブジェクトやファイルのアーカイブを目的とした非常に低コストのストレージサービスを提供しているか?
46.	**アーカイブストレージ - 耐障害性:** このクラウドサービス事業者のアーキテクチャは、そのアーカイブストレージサービスに耐障害性を提供しているか?
47.	**アーカイブストレージ - 不変性:** このクラウドサービス事業者は、アーカイブされたオブジェクトやファイルの不変性をサポートしているか?
48.	**アーカイブストレージ - WORM:** このクラウドサービス事業者は、Write Once Read Many (WORM) 機能を提供しているか?
49.	**アーカイブストレージ - サブセットの取得:** このクラウドサービス事業者は、簡単な構造化照会言語 (SQL) 式を使用して、アーカイブされたオブジェクトからデータのサブセットのみを取得する機能をユーザーに提供しているか?
50.	**アーカイブストレージ - スピード検索:** このクラウドサービス事業者は、異なるコストと検索時間でデータ検索の複数の選択肢をユーザーに提供しているか?
51.	**アーカイブストレージ - 保存時の暗号化:** このクラウドサービス事業者のアーカイブストレージサービスは、保存時の暗号化をサポートしているか?
52.	**ストレージ - サービスの制限:** このクラウドサービス事業者は、上記のストレージセクションに関して、何らかの制限 (つまり、サービスの制限) を設けているか?

	例: 最大ボリュームサイズ 1 つのインスタンスに接続されるドライブ最大数 毎秒の最大入出力操作 (IOP) 最大オブジェクトサイズ ストレージアカウントあたりのオブジェクトの最大数 スナップショットの最大数

4.管理

	要求事項
1.	**管理 - ユーザーおよびグループ**: このクラウドサービス事業者は、自社のインフラストラクチャとリソースのユーザーおよびユーザーグループを作成・管理するためのサービスを提供しているか?
2.	**管理者 - パスワードのリセット**: このクラウドサービス事業者は、ユーザーが自分のパスワードをセルフサービスでリセットすることを許可しているか?
3.	**管理 - アクセス許可**: このクラウドサービス事業者は、リソースレベルでユーザーやグループにアクセス許可を追加する機能を提供しているか?
4.	**管理 - 一時的なアクセス許可**: このクラウドサービス事業者は、一定期間有効なアクセス許可を作成する機能を提供しているか?
5.	**管理 – 一時的な認証情報**: このクラウドサービス事業者は、数分から数時間の範囲で存続するように設定された一時的なセキュリティ認証情報を作成し、それを信頼できるユーザーに提供する機能をユーザーに提供しているか?

6.	**管理 – アクセス制御:** このクラウドサービス事業者は、自社のインフラストラクチャリソースに対するきめ細かいアクセス制御を提供しているか? • 「はい」の場合、これらの制御によってどのような条件を適用できるか (時刻、発信元 IP アドレスなど)?
7.	**管理 – 組み込みのポリシー:** このクラウドサービス事業者のインフラストラクチャには、ユーザーやグループに適用できるアクセス制御ポリシーが組み込まれているか?
8.	**管理 – カスタムポリシー:** このクラウドサービス事業者のインフラストラクチャでは、ユーザーやグループに適用できるアクセス制御ポリシーの作成とカスタマイズが許可されているか?
9.	**管理 – ポリシーシミュレーター:** このクラウドサービス事業者は、アクセス制御ポリシーを本番環境に適用する前に、その効果をテストするための仕組みを提供しているか?
10.	**管理 – クラウド MFA:** このクラウドサービス事業者は、インフラストラクチャへのアクセス制御および認証の追加レイヤーとして、多要素認証 (Multi-Factor Authentication: MFA) の使用をサポートしているか?
11.	**管理 – サービスの制限:** このクラウドサービス事業者は、上記の管理セクションに関して、何らかの制限 (つまり、サービスの制限) を設けているか? 例: ユーザーの最大数 グループの最大数 管理ポリシーの最大数

5.セキュリティ

	要求事項
1.	**セキュリティ – 身元調査**: このクラウドサービス事業者のサービスインフラストラクチャ (物理的か非物理的かを問わず) へのアクセス権を持つ要員は全員、身元調査の対象となっているか?
2.	**セキュリティ – 物理的アクセス**: このクラウドサービス事業者は、特定のトラブルチケット、変更要求、または同様の正式な承認がない限り、要員がサービスインフラストラクチャにアクセスするのを制限しているか?
3.	**セキュリティ – アクセスログ**: このクラウドサービス事業者は、自社のインフラストラクチャに対する要員のアクセスをログに取っているか?その場合、そのようなアクセスは常にログに記録され、最低 90 日間保存されているか?
4.	**セキュリティ – ホストログイン**: このクラウドサービス事業者は、自社の要員がコンピューティングホストにログインすることを制限し、その代わりに、コンピューティングホストで実行されるすべてのタスクを自動化しているか? その場合、自動化ジョブの内容はログに記録され、最低 90 日間保存されているか?
5.	**セキュリティ – 暗号化キー**: このクラウドサービス事業者は、ユーザーデータの暗号化に使用される暗号化キーを作成および管理するサービスを提供しているか?
6.	**セキュリティ – アクセスキー管理**: このクラウドサービス事業者は、アクセスキーが最後に使用された日時を特定し、古いキーを交替し、非アクティブなユーザーを削除する機能を提供しているか?
7.	**セキュリティ – お客様提供のキー**: このクラウドサービス事業者は、ユーザーが自身のキー管理インフラストラクチャからクラウドサービスプロバイダーのキー管理サービスにキーをインポートすることを許可しているか?
8.	**セキュリティ - 暗号化キーサービスの統合**: このクラウドサービス事業者のキー管理サービスは、他のクラウドサービスと統合されて、保存時のデータの暗号化機能を提供しているか?

9.	**セキュリティ - HSM:** このクラウドサービス事業者は、専用のハードウェアセキュリティモジュール (HSM)、すなわち、セキュアキーストレージと暗号化操作を、耐タンパー性を備えたハードウェアモジュール内で提供するハードウェアアプライアンスを提供しているか?
10.	**セキュリティ – 暗号化キーの耐久性:** このクラウドサービス事業者は、キーが必要なときに利用できるように複数のコピーを保存するなど、キーの耐久性をサポートしているか?
11.	**セキュリティ - SSO:** このクラウドサービス事業者は、ユーザーが複数のアカウントやビジネスアプリケーションへのアクセスを一元管理できるマネージド型シングルサインオン (SSO) サービスを提供しているか?
12.	**セキュリティ – 証明書:** このクラウドサービス事業者は、Secure Sockets Layer (SSL) /Transport Layer Security (TLS) の証明書をプロビジョニング、管理、およびデプロイするための管理サービスを提供しているか?
13.	**セキュリティ – 証明書更新:** このクラウドサービス事業者の証明書管理サービスは、証明書の更新を容易にしているか?
14.	**セキュリティ – ワイルドカード証明書:** このクラウドサービス事業者の証明書管理サービスは、ワイルドカード証明書の使用をサポートしているか?
15.	**セキュリティ – 認証局:** このクラウドサービス事業者の証明書管理サービスは、認証局 (CA) としても機能するか?
16.	**セキュリティ - Active Directory:** このクラウドサービス事業者は、クラウド内でマネージド型の Microsoft Active Directory (AD) サービスを提供しているか?
17.	**セキュリティ - オンプレミス Active Directory:** このクラウドサービス事業者のマネージド型の Microsoft Active Directory (AD) サービスはオンプレミスの Microsoft Active Directory (AD) との統合をサポートしているか?
18.	**セキュリティ - LDAP:** このクラウドサービス事業者のマネージド型の Microsoft Active Directory (AD) サービスは、Lightweight Directory Access Protocol (LDAP) をサポートしているか?

19.	**セキュリティ - Active Directory:** このクラウドサービス事業者のマネージド型の Microsoft Active Directory (AD) サービスは、Security Assertion Markup Language (SAML) をサポートしているか?
20.	**セキュリティ – 認証情報管理:** このクラウドサービス事業者は、ユーザーがアプリケーションプログラミングインターフェイス (API) キー、データベース認証情報、その他のシークレットなどの認証情報を簡単にローテーション、管理、取得できるようにするマネージド型サービスを提供しているか?
21.	**セキュリティ - WAF:** このクラウドサービス事業者は、アプリケーションの可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする可能性のある一般的な Web 攻撃から Web アプリケーションを保護するための Web アプリケーションファイアウォール (WAF) を提供しているか?
22.	**セキュリティ - DDOS:** このクラウドサービス事業者は、最も頻繁に発生する一般的なネットワークおよびトランスポート層の分散型サービス拒否 (DDoS) 攻撃から保護するためのサービスを、高度なアプリケーション層攻撃を緩和するためのカスタマイズされたルールを記述する機能とともに提供しているか?
23.	**セキュリティ – セキュリティに関する推奨事項:** このクラウドサービス事業者は、アプリケーションやリソースの潜在的な脆弱性を自動的に評価するサービスを提供しているか?
24.	**セキュリティ – 脅威の検出:** このクラウドサービス事業者は、マネージド型の脅威検出サービスを提供しているか?
25.	**セキュリティ – サービスの制限:** このクラウドサービス事業者は、上記のセキュリティセクションに関して、何らかの制限 (つまり、サービスの制限) を設けているか? 例: 顧客マスターキーの最大数 ハードウェアセキュリティモジュール (HSM) の最大数

6.コンプライアンス

以下のリストは説明のために提供されているものに過ぎず、クラウドサービスに適用できる認証および標準を網羅しているものではない。

このクラウドサービス事業者が満たしている国際的なコンプライアンス基準と業界固有のコンプライアンス基準を示すこと。

認証/証明	法律、規制、プライバシー	準拠 / フレームワーク
☐C5 (ドイツ)	☐EU データ保護指令	☐CDSA
☐CISPE データ保護行動規範	☐EU モデル条項	
☐CNDCP (気候中立的データセンター協定)		
☐DIACAP	☐FERPA	☐CIS
☐DoD SRG レベル 2 および 4	☐GDPR	☐刑事司法情報サービス (CJIS)
☐FedRAMP	☐GLBA	☐CSA
☐FIPS 140-2	☐HIPAA	☐EU-US プライバシーシールド
☐HDS (フランス、ヘルスケア)	☐HITECH	☐EU セーフハーバー
☐ISO 9001	☐IRS 1075	☐FISC
☐ISO 27001	☐ ITAR	☐FISMA
☐ISO 27017	☐PDPA – 2010 (マレーシア)	☐G-Cloud (英国)
☐ISO 27018	☐PDPA – 2012 (シンガポール)	☐GxP (FDA CFR 21 パート 11)
☐IRAP (オーストラリア)	☐PIPEDA (カナダ)	☐ICREA
☐MTCS Tier 3 (シンガポール)	☐プライバシー法 (オーストラリア)	☐ IT Grundschutz (ドイツ)
☐PCI DSS レベル 1	☐プライバシー法 (ニュージーランド)	☐MARS – E

☐SEC 規則 17-a-4 (f)	☐スペイン DPA 認証	☐ MITA 3.0
☐SOC1 / ISAE 3402	☐英国 DPA - 1988	☐MPAA
☐SOC2 / SOC3	☐VPAT/セクション 508	☐NIST
☐SWIPO IaaS コード		
		☐Uptime Institute Tiers
		☐英国クラウドセキュリティ原則

上記のコンプライアンス報告書を活用することで、公共部門の組織は一般に認められているセキュリティ、コンプライアンス、運用上の標準に照らして、独自のサービスを評価できる。CISP は、報告書を遵守することによって、パブリッククラウドサービスプロバイダーに要求される以下のデータセンター運用管理を満たしていることを示すことができる。そのような報告書の遵守を要求することにより、公共部門の事業体では以下の管理が行われていることが保証される。

- **アクセスの精査**: CISP には、業務上の正当な理由で立ち入る必要がある人々に限定して、物理的なアクセスを許可することが求められる。アクセスが承諾されている場合、必要な作業が完了し次第、無効にする必要がある。
- **立ち入りの制御と監視**: 境界防御レイヤーへの立ち入りは、制御対象のプロセスである。クラウドサービス事業者は、入り口ゲートに警備員を配置し、監視カメラを介して警備員と訪問者を監視する監督官を配置する。立ち入りが許可された人にはバッジが渡され、そのバッジにより多要素認証が実行され、アクセスは事前承認されたエリアに制限される。
- **CISP のデータセンター従業員**: 定期的にデータセンターへ出入りする CISP の従業員は、職務に基づいて施設の該当するエリアへのアクセスを許可され、そのアクセスは毎回綿密に精査される。職員リストは、従業員ごとに許可がまだ必要かどうかを確認するために、エリアアクセスマネージャーが定期的に見直す必要がある。データセンターに立ち入る継続的な業務を与えられていない従業員には、一般の訪問者と同様のプロセスが必要とされる。
- **不正侵入の監視**: CISP は、ビデオ監視、侵入検知、およびアクセスログ監視システムを使用して、データセンターの敷地内への不正侵入を継続的に監視する必要がある。ドアを無理に開けたり、開いたままにされた際に、警報音が鳴る装置によって、出入り口のセキュリティを確保すること。
- **CISP のセキュリティオペレーションセンターによるグローバルセキュリティの監視**: CISP はセキュリティオペレーションセンターを世界中に配置して、CISP データセンターのセキュリティプログラムの監視、トリアージ、実行に責任を有する。ここでは物理的なアクセス管理と侵入検知対応を監視し、現場のデータセンタ

ーセキュリティチームにグローバルな 24 時間 365 日のサポートを提供する必要がある。これにより、アクセス活動の追跡、アクセス許可の取り消し、および潜在的なセキュリティインシデントへの対応と分析などの継続的な監視活動を実施することができる。

- **レイヤーごとのアクセスレビュー**: インフラストラクチャーレイヤーへのアクセスは、業務上のニーズに基づいて制限する必要がある。レイヤーごとのアクセスレビューを実施することにより、デフォルトではすべてのレイヤーにアクセスする権限が付与されない。特定のレイヤーへのアクセスは、その特定のレイヤーにアクセスする必要がある場合にのみ許可するものとする。

- **設備のメンテナンスは日常業務の一環**: CISP のチームは、マシン、ネットワーク、およびバックアップ機器の診断を実行し、常時、緊急時いずれにおいても正常に動作することを確認する必要がある。データセンターの機器およびユーティリティの定期的なメンテナンスチェックは、通常の CISP データセンター運用の一環として行う必要がある。

- **緊急時に対応可能なバックアップ装置**: 水道、電力、通信、インターネット接続は冗長性を備えて設計する必要がある。これにより、CISP は緊急時において継続的な運用を維持することができる。電力系統は、完全な冗長性を備えて設計する必要がある。これにより、停電時に無停電電源装置が特定の機能に対応し、発電機から設備全体にバックアップ電力を供給することができる。人とシステムは、温度と湿度を監視および制御して過熱を防止し、起こりえるサービス停止をさらに低減する必要がある。

- **テクノロジーと人との協力でセキュリティを強化**: データレイヤーにアクセスするための認可を得るために必須の手続きがあること。これには、認証を受けている個人によるアクセス申請のレビューと承認も含まれる。一方、脅威および電子侵入検知システムは、特定された脅威や疑わしい活動を監視して、自動的にアラートを発動す必要がある。例えば、ドアを開いたままにしたり、無理に開けたりすると、アラームが発動されること。CISP は、監視カメラを配備し、法的要件およびコンプライアンス要件に従って映像を保存する必要がある。

- **物理的および技術的な侵入の防止**: サーバー室へのアクセスポイントは、多要素認証を必要とする電子制御デバイスで強化する必要がある。CISP はまた、技術的侵入の防止についても対策を講じる必要がある。CISP のサーバーは、データを削除しようとすると従業員に警告できる必要がある。万一違反が発生した場合、サーバーは自動的に無効になるものとする。

- **サーバーとメディアに対する万全の注意**: カスタマーデータを保存するためのメディアストレージデバイスは、CISP によって「クリティカル」に分類され、そのライフサイクル全体を通じて影響が大きいものとして扱われる必要がある。CISP は、デバイスのインストールと保守方法、そして無用になった場合の最終的な廃棄方法について厳格な基準を設けておく必要がある。ストレージデバイスの有効寿命が終わった場合、CISP は、NIST 800-88 に詳述される技法を用いてメディアを廃棄する。カスタマーデータを保存していたメディアは、セキュアに廃棄されるまで CISP の管理対象から除去されないこと。

- **第三者監査人による CISP の手順とシステムの検証**: CISP は、外部監査人による監査を受けてデータセンターを検査し、CISP がセキュリティの認証を取得するために必要なルールに従っていることを確認するための詳細な調査を実行する必要がある。外部監査人は、コンプライアンスプログラムとその要求事項に応じて、CISP の従業員にメディアの取り扱いと廃棄についてインタビューすることができる。監査人は、監視カメラのフィードを監視したり、データセンター全体の入口や廊下を監視したりすることもできる。また、CISP の電子アクセス制御装置や監視カメラなどの機器を検査することもある。

- **不測の事態の備え**: CISP は、自然災害や火災などの潜在的な環境上の脅威に事前に備える必要がある。CISP がデータセンターを保護する方法には、自動センサーと応答装置の設置という 2 通りの方法がある。自動ポンプで漏水を除去し、損害を防ぎ、従業員に問題を警告するために漏水検知デバイスを設置する必要がある。同様に、自動火災検知・鎮火装置はリスクを低減し、CISP の職員と消防士に問題を通知することができること。

- **複数のアベイラビリティーゾーンによる高可用性**: CISP は、耐障害性を高めるために複数のアベイラビリティーゾーンを提供する必要がある。各アベイラビリティーゾーンは、最低 1 つのデータセンターで構成され、互いに物理的に分離され、冗長電源、冗長化されたネットワークを擁している必要がある。アベイラビリティーゾーンは、中断することなくアベイラビリティーゾーン間で自動的にフェイルオーバーするアプリケーションを設計するために、高速なプライベート光ファイバーネットワークで相互に接続する必要がある。

- **障害のシミュレーションと対応の測定**: CISP は、事業継続計画を策定しておく必要がある。それは、自然災害による障害を回避および軽減する方法を示したものであり、イベントの発生前、発生期間中、および発生後に実行すべき詳細な手順を含む業務プロセスガイドとなるものである。予期しない事態を軽減し、それに備えるために、CISP は、さまざまなシナリオをシミュレートする訓練を行って事業継続計画を定期的にテストする必要がある。CISP は、職員とプロセスがどのように機能しているかを文書化し、得られた教訓と、応答率改善のために必要と思われる是正措置について結果をまとめる必要がある。CISP の職員は、エラーによるダウンタイムを最小限に抑えるための体系的なリカバリプロセスを通して、障害から迅速に立ち直るためのトレーニングを受け、備えておく必要がある。

- **効率目標の達成を支援**: CISP は、環境リスクへの取り組みに加え、持続可能性に対する配慮をデータセンターの設計に組み込む必要がある。CISP は、自社のデータセンターに再生可能エネルギーを利用するというコミットメントの詳細を提供し、顧客が自社のデータセンターに比べてどのように炭素排出量を削減できるかについての情報を提供する必要がある。

- **立地地点の選定**: 立地地点を選定する前に、CISP は初期の環境および地理的評価を実施する必要がある。データセンターの立地地点は、洪水、異常気象、地震活動などの環境リスクが軽減されるように慎重に選択する必要がある。CISP のアベイラビリティーゾーンは、互いに独立し、物理的に分離しているように構築する必要がある。

- **冗長性**: データセンターは、サービスレベルを維持しながら、障害を予測し耐えるように設計する必要がある。障害が発生した場合は、自動プロセスによってトラフィックを影響のあるエリアから移動するようにす

る必要がある。重要なアプリケーションは N+1 の基準に従って展開される。これにより、データセンターで障害が発生した場合でも、トラフィックをその他のサイトへ負荷分散できるような十分なキャパシティーが確保される。

- **可用性**: CISP は、システムの可用性を維持し、停止時にサービスを復旧するために必要となる重要なシステムコンポーネントを特定する必要がある。重要なシステムコンポーネントは、複数の離れた場所にバックアップしておく必要がある。各立地地点またはアベイラビリティーゾーンは、高い信頼性を備えて独立して稼働できるように設計する必要がある。アプリケーションが中断することなく、アベイラビリティーゾーン間で自動的にフェイルオーバーできるようにアベイラビリティーゾーンを接続する必要がある。復旧力の高いシステム、つまり、サービスの可用性は、システム設計の機能のひとつと考えるべきである。データセンターの設計にアベイラビリティーゾーンとデータレプリケーションを考慮することにより、CISP の顧客は、非常に短い目標復旧時間と目標復旧時点を実現し、最高レベルのサービス可用性を達成することができる。

- **キャパシティー計画**: CISP は、サービスの使用状況を継続的に監視して、可用性に対するコミットメントと要求事項に対応可能なインフラストラクチャを展開する必要がある。CISP は、CISP インフラストラクチャの使用状況と需要を少なくとも毎月評価するキャパシティー計画モデルを維持管理する必要がある。このモデルは将来の需要の計画をサポートするものであり、情報処理、通信、監査ログの保存などの考慮事項が含まれているものである。

事業継続性および災害復旧

- **事業継続計画**: CISP の事業継続計画では、環境破壊を回避し減少させるための措置の概要を示す必要がある。それにはイベントの発生前、発生期間中、発生後に取るべき措置に関する運用上の詳細が含まれる。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストを実施して裏付けをとる必要がある。CISP はテストの実施中と実施後に、継続的改善を目指して、人員とプロセスのパフォーマンス、是正措置、および得られた教訓を文書にまとめる必要がある。

- **パンデミックへの対応**: CISP は、感染症発生の脅威に迅速に対応するために、パンデミックへの対応方針と手順を災害復旧計画に組み込む必要がある。緩和戦略には、重要なプロセスを地域外のリソースに移転する代替要員配置モデルや、重要な事業運営を支援するための危機管理計画の発動を含める必要がある。パンデミック対策計画では、国際機関の連絡窓口を含め、国際的な保健機関や規制を参照する必要がある。

監視活動およびロギング

- **データセンターのアクセスレビュー**: データセンターへのアクセスを定期的にレビューする必要がある。CISP の人事システムで従業員の記録が削除された場合、その従業員のアクセス権は自動的に取り消されること。さらに、従業員または請負業者のアクセス権が承認済み要求期間に従って期限切れになった場合は、その従業員または請負業者が引き続き CISP の従業員であっても、そのアクセス権を取り消す必要がある。

- **データセンターアクセスログ**: CISP データセンターへの物理的なアクセスを、ログに記録し、監視し、保持する必要がある。CISP は、必要に応じてセキュリティを強化するために、論理的および物理的な監視システムから得られた情報を相互に関連付ける必要がある。

- **データセンターのアクセス監視**: CISP は、セキュリティプログラムの監視、優先順位付け、および実行を担当するグローバルなセキュリティオペレーションセンターを使用して、データセンターを監視する必要がある。データセンターのアクセス活動を管理および監視し、地域チームやその他のサポートチームに、優先順位付け、コンサルティング、分析、および対応のディスパッチによってセキュリティインシデントに対応できるようにして、24 時間 365 日体制のグローバルサポートを提供する必要がある。

監視と検出

- CCTV: サーバー室への物理的アクセスポイントは、閉回路テレビカメラ (CCTV) で記録する必要がある。画像は、法律およびコンプライアンスの要求事項に従って保存する必要がある。

- **データセンター入口点**: 物理的アクセスは、サーベイランスシステム、侵入検出システムやその他の電子的手段を利用する専門のセキュリティ担当者によって、建物の入口で制御する必要がある。許可された職員は、多要素認証メカニズムを利用してデータセンターにアクセスする必要がある。サーバー室の入口は、ドアが無理に開けられたり、開いたままである場合にアラームを鳴らして、インシデント対応を始動する装置によってセキュリティを確保する必要がある。

- **侵入検知**: セキュリティインシデントを監視し、検知して、適切な要員に自動的に警告する電子侵入検知システムをデータレイヤー内に設置する必要がある。サーバー室への入退室ポイントでは、入退室を許可する前に各個人に多要素認証の提示を要求する装置によってセキュリティが確保されている必要がある。このような装置は、認証なしでドアを無理に開けたり、開いたままにしておくと、アラームを鳴らす。また、ドア警報装置は、個人が多要素認証を提示せずにデータレイヤーに出入りする事例を検出するように構成されなければならない。アラームを 24 時間 365 日体制の CISP のセキュリティオペレーションセンターに直ちに発信して、即時ロギング、分析、および対応にあてる必要がある。

デバイス管理

- **アセットマネジメント**: CISP が所有するアセットの所有者、所在地、ステータス、保守、および記述情報を格納・追跡するインベントリ管理システムを介して CISP のアセットを一元管理する必要がある。調達後に、アセットをスキャンおよび追跡し、保守中のアセットの所有権、ステータス、および決定内容をチェックして監視する必要がある。

- **メディアの破壊**: カスタマーデータを保存するためのメディアストレージ・デバイスは、CISP によって「クリティカル」に分類され、そのライフサイクル全体を通じて影響が大きいものとして扱われる必要がある。CISP は、デバイスのインストールと保守、そして無用になった場合の最終的な廃棄方法について厳格な基準を設けておく必要がある。ストレージデバイスの有効寿命が終わった場合、CISP は、NIST 800-88 に詳述さ

れる技法を用いてメディアを廃棄する必要がある。カスタマーデータを保存していたメディアは、セキュアに廃棄されるまで CISP の管理対象から除去しない必要がある。

運用支援システム

- **電力**: CISP データセンターの電力システムは完全な冗長性を備えたものであり、毎日 24 時間運用に影響を与えずに保守できるように設計する必要がある。CISP は、データセンターに必ずバックアップ電源を装備することとし、施設内のクリティカルかつ不可欠な負荷に対して電気的障害が発生した場合に、運用を維持するための電源を確保しておく必要がある。
- **気候と温度**: CISP のデータセンターでは、気候を制御してサーバーやその他のハードウェアの動作温度を適切に維持するメカニズムを使用して、過熱防止とサービス停止の可能性の低減を図る必要がある。職員および各システムは、温度と湿度を適切なレベルで監視し、制御する必要がある。
- **火災検出と消火**: CISP のデータセンターは、自動火災検出・消火設備を備えておく必要がある。火災検知システムは、ネットワーク、機械、およびインフラストラクチャのスペース内に煙検知センサーを活用するものとする。これらのエリアもまた、消火システムで防護しておく必要がある。
- **漏水検出**: CISP は、漏水を検出するために、データセンターに水検出機能を装備する必要がある。水が検出された場合には、さらなる水害を防ぐために、水を取り除く仕組みを設ける必要がある。

インフラストラクチャの保守

- **設備保守**: CISP は、CISP データセンター内のシステムの継続的な操作性を維持するために、電気機器と機械設備を監視して、予防保守を実施する必要がある。設備保守手順は、有資格者によって実施するものとし、文書化された保守スケジュールに従って完了する必要がある。
- **環境管理**: CISP は、電気・機械システムと設備を監視して、迅速な課題の特定を図る必要がある。これは、CISP のビル管理システムと電気的監視システムを通じて提供される継続的な監査ツールと監査情報を利用することによって行うものとする。設備の継続的な操作性を維持するために、予防保全を実施する必要がある。

ガバナンスとリスク

- **データセンターの継続的リスク管理**: CISP のセキュリティオペレーションセンターは、データセンターの脅威と脆弱性に関する定期レビューを実施する必要がある。潜在的な脆弱性に対する継続的な評価と軽減作業は、データセンターのリスク評価活動を通じて実施されるものとする。この評価は、事業全体に存在するリスクを特定し管理するための企業レベルのリスク評価プロセスに加えて実施される必要がある。このプロセスでは、地域別の規制上および環境上のリスクも考慮に入れる必要がある。
- **第三者によるセキュリティ認証**: 第三者のレポートに記載されているように、第三者による CISP データセンターのテストでは、セキュリティ認証を取得するために必要な定則に沿ったセキュリティ対策を CISP が適

切に実施していることを保証する必要がある。外部監査人は、コンプライアンスプログラムとその要求事項に応じて、メディア廃棄のテスト、監視カメラ映像のレビュー、データセンター全体の入口と廊下の観察、電子アクセス制御デバイスのテスト、データセンターの設備検査を行うことができる。

7.移行

	要求事項
1.	**移行サービス**: クラウドサービス事業者が、何種類のデータ移行サービスを提供しているか?
2.	**移行 — 集中監視活動**: このクラウドサービス事業者は、組織が自社のサーバーおよびアプリケーションの移行状況を追跡・監視できる、集中管理された (統一されたインタフェースを通じて) サービスを提供しているか?
3.	**移行 — ダッシュボード**: このクラウドサービス事業者の移行ツールは、移行状況、関連指標、および移行履歴をすばやく視覚化するダッシュボードを提供しているか?
4.	**移行 — クラウドサービス事業者のツール**: このクラウドサービス事業者の移行ツールは、サーバーとアプリケーションの移行を実行できるクラウドサービス事業者の他の移行ツールと統合することができるか?
5.	**移行 — 第三者のツール**: このクラウドサービス事業者の移行ツールに第三者の移行ツールを組み込むことはできるか? • 「はい」の場合、サポートされている第三者の移行ツールは何か?
6.	**移行 — 複数地域にまたがる移行**: このクラウドサービス事業者の移行ツールは、異なる地域で発生するサーバーとアプリケーションの移行を追跡・監視する機能を提供しているか?
7.	**移行 — サーバーの移行**: このクラウドサービス事業者の移行ツールは、オンプレミスの仮想サーバーをクラウドに移行する方法を提供しているか? • 「はい」の場合、現在サポートされている仮想化環境を提示すること。
8.	**移行 — サーバーの検出**: このクラウドサービス事業者の移行ツールには、クラウドに移行するオンプレミスの仮想サーバーを自動的に検出する機能があるか?

9.	**移行 – サーバーのパフォーマンスデータ**: このクラウドサービス事業者の移行ツールには、中央処理装置 (CPU) やランダムアクセスメモリー (RAM) の利用のように、サーバーや仮想マシンのパフォーマンスを収集して表示する機能があるか?
10.	**移行 – 検出データベース**: このクラウドサービス事業者の移行ツールには、収集した全データを集中管理されるデータベースに保存する機能があるか? • 「はい」の場合、組織はこれらのデータをエクスポートできるか? どのフォーマットにエクスポートできるか?
11.	**移行 – 保存中の暗号化**: このクラウドサービス事業者は、収集されて検出データベースに保存されている保存中のすべての情報を暗号化しているか?
12.	**移行 – インクレメンタルサーバーレプリケーション**: このクラウドサービス事業者の移行ツールは、サーバーまたは仮想マシンに対して行われたすべての変更が最終移行イメージに含まれることをサポートする方法として、サーバーまたは仮想マシンの移行時に、自動化されたライブのインクリメンタルサーバーレプリケーションを提供するか? • 「はい」の場合、このサービスはどのくらいの期間稼働するか?
13.	**移行 – VMWare:** このクラウドサービス事業者の移行ツールは、オンプレミスからクラウドへの VMWare 仮想マシンの移行をサポートしているか?
14.	**移行 – Hyper-V:** このクラウドサービス事業者の移行ツールは、オンプレミスからクラウドへの Hyper-V 仮想マシンの移行をサポートしているか?
15.	**移行 – アプリケーションの検出**: このクラウドサービス事業者の移行ツールには、アプリケーションを移行する前に検出してグループ化する機能があるか?
16.	**移行 – 依存関係のマッピング**: このクラウドサービス事業者の移行ツールには、アプリケーションを移行する前にサーバーとアプリケーションの依存関係を検出する機能があるか?

17.	**移行 – データベースの移行**: このクラウドサービス事業者の移行ツールには、オンプレミスのデータベースをクラウドに移行する機能があるか?
18.	**移行 – データベース移行のダウンタイム**: このクラウドサービス事業者の移行ツールには、ダウンタイムを最小限に抑えてクラウドへのデータベース移行を実行する機能があるか (つまり、移行プロセスの間、ソースデータベースは完全に動作可能な状態を維持する必要がある)?
19.	**移行 – ソースデータベース**: このクラウドサービス事業者の移行ツールは、Oracle、SQL Server 等、異なるデータベースソースの移行をサポートしているか? • 「はい」の場合は、クラウドに移行可能なサポート対象のソースデータベースをすべて記載すること。
20.	**移行 – 異種移行**: このクラウドサービス事業者の移行ツールには、異種データベースの移行、つまり、Oracle から SQL Server への移行のように、1 つのソースデータベースから異なるターゲットデータベースへの移行を実行する機能があるか? • 「はい」の場合は、可能な異種データベース間の移行の組合せをすべて記載すること。
21.	**移行 – ペタバイト規模のデータ移行**: このクラウドサービス事業者は、大量のデータをクラウドとの間でやり取りするためにセキュアな装置を使用するペタバイト規模のデータ移送ソリューションを提供しているか?
22.	**移行 – エクサバイト規模のデータ移行**: このクラウドサービス事業者は、非常に大量のデータをクラウドに移送するためのエクサバイト規模のデータ移送ソリューションを提供しているか?
23.	**移行 – エンタープライズバックアップ**: このクラウドサービス事業者は、顧客のデータセンターをクラウドストレージサービスとシームレスに統合し、データをクラウドサービス事業者のストレージサービスに転送して保存できるようなサービスを提供しているか?
24.	**移行 – エンタープライズバックアップ – オブジェクトストレージ**: このクラウドサービス事業者のエンタープライズバックアップサービスは、サービス事業者のクラウドオブジェクトストレージサービスとの統合を提供しているか?

25.	**移行 – エンタープライズバックアップ – ファイルアクセス**: このクラウドサービス事業者のエンタープライズバックアップサービスでは、ユーザーはネットワークファイルシステム (NFS) プロトコル等のファイルプロトコルを使用してオブジェクトを保存したり検索したりすることができるか?
26.	**移行 – エンタープライズバックアップ – ブロックアクセス**: このクラウドサービス事業者のエンタープライズバックアップサービスでは、ユーザーは Internet Small Computer System Interface (iSCSI) プロトコル等のブロックプロトコルを使用してオブジェクトを保存したり検索したりすることができるか?
27.	**移行 – エンタープライズバックアップ – テープアクセス**: このクラウドサービス事業者のエンタープライズバックアップサービスでは、ユーザーは仮想テープライブラリを使用してデータをバックアップし、そのテープバックアップをサービス事業者のクラウド上に保存することができるか?
28.	**移行 – エンタープライズバックアップ – 暗号化**: このクラウドサービス事業者のエンタープライズバックアップサービスは、保存中および転送中のデータの暗号化を提供しているか?
29.	**移行 – エンタープライズバックアップ – サードパーティソフトウェアの統合**: このクラウドサービス事業者のエンタープライズバックアップサービスは、一般に使用されているサードパーティのバックアップソフトウェアと統合されているか?
30.	**移行 – サービスの制限**: このクラウドサービス事業者は、上記の移行セクションに関して、何らかの制限 (つまり、サービスの制限) を設けているか? 例: 仮想マシンの同時移行の最大数 オーダー可能なデータ移送ソリューションの最大数

8.請求

	要求事項
1.	**請求 — 追跡および報告:** このクラウドサービス事業者は、ユーザーがクラウドサービスの利用状況を管理したり監視したりするのに役立つ請求の追跡・報告サービスを提供しているか?
2.	**請求 — アラームと通知:** このクラウドサービス事業者は、ユーザーの支出が特定のしきい値を超えたときに、ユーザーに警告するための通知付きアラームを設定する仕組みを提供しているか?
3.	**請求 — コスト管理:** このクラウドサービス事業者は、コストと支出を要約したグラフを作成して表示する仕組みを提供しているか?
4.	**請求 — 予算:** このクラウドサービス事業者は、予算を表示して管理し、推定コストを予測するための仕組みを提供しているか?
5.	**請求 — 統合表示:** このクラウドサービス事業者は、複数のアカウントからの請求を 1 つの主要な支払アカウントに統合する仕組みを提供しているか?
6.	**請求 — サービスの制限:** このクラウドサービス事業者は、上記の請求セクションに関して、何らかの制限 (つまり、サービスの制限) を設けているか? 例: グループ化可能なアカウントの最大数 作成可能なアラームの最大数 管理可能な予算の最大数

9.管理

	要求事項
1.	**管理 — 監視サービス:** このクラウドサービス事業者は、事前に定義された指標を使用して収集、監視、報告するクラウドリソースおよびアプリケーションを管理するための監視サービスを提供しているか?
2.	**管理—アラーム:** このクラウドサービス事業者の監視サービスでは、ユーザーがアラームを設定することはできるか?
3.	**管理 — カスタムメトリック:** このクラウドサービス事業者の監視サービスでは、ユーザーがカスタムメトリックを作成して監視することができるか?
4.	**管理 — 監視精度:** このクラウドサービス事業者の監視サービスは、1 分のレベルまで細分化されたさまざまなレベルの監視精度を提供しているか?
5.	**管理 — API 追跡サービス:** このクラウドサービス事業者は、クラウドリソースに対するアクティビティをログに記録し、監視し、保存するサービスを、コンソールとアプリケーションプログラミングインタフェース (API) レベルの両方で提供して、視覚性を高めているか? • 「はい」の場合、この追跡サービスに統合されているクラウドサービス事業者のサービスは何か?
6.	**管理 — 通知:** このクラウドサービス事業者は、アプリケーションプログラミングインターフェイス (API) のアクティビティレベルに基づいて通知を送信する機能を有効にすることができるか?
7.	**管理 — 圧縮:** このクラウドサービス事業者は、ユーザーがこのサービスに関連するストレージコストを削減できるようにするために、アプリケーションプログラミングインターフェイス (API) 追跡システムによって生成されたログを圧縮する仕組みを提供しているか?
8.	**管理 — 地域の集約:** このクラウドサービス事業者は、すべての地域でアカウントアプリケーションプログラミングインターフェイス (API) のアクティビティを記録し、その情報を使いやすいように集約させて配信する機能を提供しているか?

9.	**管理 – リソースのインベントリ**: このクラウドサービス事業者は、ユーザーが展開したリソースの構成を査定、監査、および評価するサービスを提供しているか?
10.	**管理–構成の変更**: このクラウドサービス事業者は、リソース構成の変更が発生したときに自動的に記録しているか?
11.	**管理 – 構成履歴**: このクラウドサービス事業者は、過去の任意の時点のリソース構成を調査する機能を提供しているか?
12.	**管理–構成ルール**: このクラウドサービス事業者は、プロビジョニング、設定、およびコンプライアンスの継続的な監視に関するガイドラインと推奨事項を提供しているか?
13.	**管理 – リソーステンプレート**: このクラウドサービス事業者は、テンプレートのような方法でリソースのコレクションを作成、プロビジョニング、および管理する機能をユーザーに提供しているか?
14.	**管理 – リソーステンプレートのレプリケーション**: このクラウドサービス事業者は、災害復旧の状況で使用できるようにするために、これらのリソーステンプレートを異なる地域間で迅速にレプリケートする機能を提供しているか?
15.	**管理 – テンプレートデザイナー**: このクラウドサービス事業者は、このようなリソーステンプレートの作成プロセスを高速化するドラッグ & ドロップ機能を備えた使いやすいグラフィカルツールを提供しているか?
16.	**管理 – サービスカタログ**: このクラウドサービス事業者は、サーバー、仮想マシン、ソフトウェア、データベースなどの各種サービスのカタログを作成し、管理するためのサービスを提供しているか?
17.	**管理 – コンソールアクセス**: このクラウドサービス事業者は、クラウドサービスの管理と監視を容易にするウェブベースのユーザーインターフェイスを提供しているか?
18.	**管理 – CLI アクセス**: このクラウドサービス事業者は、コマンドラインインターフェイス (CLI)から複数のクラウドサービスを管理および設定し、スクリプトを使用して管理タスクを自動化するための統合ツールを提供しているか?

19.	**管理 – モバイルアクセス**: このクラウドサービス事業者は、ユーザーがクラウドサービスに接続してリソースを管理するためのスマートフォンアプリケーションを提供しているか? • 「はい」の場合、そのアプリケーションは iOS と Android の両方で使えるか?
20.	**管理 – ベストプラクティス**: このクラウドサービス事業者は、ユーザーがクラウドの利用状況をベストプラクティスと比較するのに便利なサービスを提供しているか?
21.	**管理 – サービスの制限**: このクラウドサービス事業者は、上記の管理セクションに関して、何らかの制限 (つまり、サービスの制限) を設けているか? 例: アカウントごとの構成ルールの最大数 作成可能なアラームの最大数 保存可能なログの最大数

10.サポート

	要求事項
1.	**サポート – サービス**: このクラウドサービス事業者は、電話、チャット、および E メールを介して 24 時間 365 日いつでもサポートを提供しているか?
2.	**サポート – サポート層**: このクラウドサービス事業者は、さまざまなレベルのサポート層を提供しているか?
3.	**サポート – レベル割り当て**: このクラウドサービス事業者には、ユーザーが利用したリソース/サービスを詳細なクラス分けに基づいて異なるレベルのサポートに自ら割り当てる機能が用意されているか? また、異なるレベルのサポートを得たり受けたりするために別のクラウドアカウントを維持するようユーザーに強制することはないか?

4.	**サポート – フォーラム**: このクラウドサービス事業者は、顧客の問題について話し合うための公開サポートフォーラムを提供しているか?
5.	**サポート – サービス健全性ダッシュボード**: このクラウドサービス事業者は、複数の地域にわたるサービスの可用性について最新情報を表示するサービス健全性ダッシュボードを提供しているか?
6.	**サポート – パーソナライズドダッシュボード**: このクラウドサービス事業者は、ユーザーの特定のリソースを支えるサービスのパフォーマンスと可用性をパーソナライズしたビューで表示できるダッシュボードを提供しているか?
7.	**サポート – ダッシュボードの履歴**: このクラウドサービス事業者は、365 日分のサービス健全性ダッシュボードの履歴を提供しているか?
8.	**サポート – クラウドアドバイザー**: このクラウド事業者は、カスタマイズされたクラウドエキスパートのように機能し、リソースの使用状況をベストプラクティスと比較できるサービスを提供しているか?
9.	**サポート – TAM**: このクラウドサービス事業者は、クラウドサービスの全範囲について技術的な専門知識を提供するテクニカルアカウントマネージャ (TAM) を提供しているか?
10.	**サポート – サードパーティ製アプリケーションのサポート**: このクラウドサービス事業者は、一般的なオペレーティングシステムおよび一般的なアプリケーションスタックコンポーネントのサポートを提供しているか?
11.	**サポート – パブリック API**: このクラウドサービス事業者は、サポートケースを作成、編集、および終了するために、プログラマチックにサポートケースと対話するパブリックアプリケーションプログラミングインタフェイス (API) を提供しているか?
12.	**サポート – サービスのドキュメンテーション**: このクラウドサービス事業者は、ユーザーガイド、チュートリアル、よくある質問 (FAQ)、リリースノートなど、すべてのサービスに関する高品質で一般に公開されていて表示可能な技術文書を提供しているか?

13.	**サポート – CLI のドキュメンテーション**: このクラウドサービス事業者は、コマンドラインインターフェイス (CLI) について、品質が高く、一般に公開されている表示可能な技術文書を提供しているか?
14.	**サポート – リファレンスアーキテクチャ**: このクラウドサービス事業者は、顧客がクラウドサービス事業者のクラウドサービスを組み合わせて特定のソリューションを構築できるように、リファレンスアーキテクチャ文書の無料のオンラインコレクションを提供しているか?
15.	**サポート – リファレンス導入**: このクラウドサービス事業者は、自社のクラウドサービスに一般的なソリューション (DevOps、ビッグデータ、データウェアハウス、Microsoft ワークロード、SAP ワークロード等) を実装するための、詳細でテスト済み、かつ検証済みのステップバイステップの手順書 (ベストプラクティスも含む) の無料のオンラインコレクションを提供しているか?

付録 B — ライブ技術評価

CISP を選択する際には、CISP の公開されているサービスおよびインフラストラクチャを使用して、「ライブ」でクラウドプラットフォーム機能を評価することが重要です。候補の CISP ごとに丸一日以上かけて技術評価を実施することをお勧めします。評価中には、1) 詳細な評価を実施して、デモの機能が RFP 要求事項および CISP の文書による回答に合致しているかどうかを評価したり、2) エキスパートが CISP を調べて特定の技術のニーズおよび組織のニーズに適合および準拠していることを確認するためのプラットフォームを提供したり、3) CISP のサービスおよび CISP のスケーリング、セキュアな運用、耐久性に優れた運用、将来のニーズを満たすための継続的なイノベーションの能力の信頼性を確認したりすることができます。

CISP は、クラウドサービス RFP の要求事項に回答する際に、要求事項の大まかな解釈に基づいてコンプライアンスを記述することがあるため、組織の運用環境/アプリケーションのニーズの十分なコンテキストが欠落していることがあります。ライブ技術評価パネルには、技術、運用、セキュリティ、およびアプリケーションの上級エキスパートを動員することをお勧めします。評価者は評価を通して CISP の問題点を探す必要があり、ベストプラクティスとして、独立して CISP のスコアを付け、0 から 4 (0＝許容できない、1＝最低限度、2＝許容できる、3＝良好、4＝傑出) といった規定尺度で各シナリオを評価する必要があります。その後、デモのスコアを統合し、各評価シナリオの平均スコアを集計して、全体的な CISP 評価を出すことができます。標準偏差が大きいシナリオは、最終決定前に評価チームで話し合う必要があります。スコアの統合後、シナリオの重要度に基づいた重み付けを適用できます。

デモの範囲の観点からは、CISP のプラットフォームの全体像をつかんでから、詳細に移ってプラットフォームで実行される特定のワークロードを評価することをお勧めします。以下に、プラットフォームとワークロードの評価のサンプル概要を示します。組織は、選択した CISP が特定の機能および非機能の要求事項を満たしているかを確認するために、このベースラインに基づいて構築することも、これをカスタマイズすることもできます。ベストプラクティスとして、シナリオおよび要求事項のリストが提示されたサプライヤーには、カバレッジを最大化し、20 % の Q&A 時間を含めたライブ評価のスケジュールを提案することを許可できます。

プラットフォーム評価: 複数の CISP が、最適な価値を提供してリスクを最小化するクラウドのアプローチを指す用語として「Well Architected (適切に設計された)」を採用しています。ライブ技術デモにおける Well Architected シナリオには、以下を含めることができます。

1. **セキュリティ**: アイデンティティ、一元化ガバナンス、自動脅威検出、データ保護、イベント対応
2. **パフォーマンス効率**: 適切なサイズ設定、スケーラビリティ/伸縮性、サーバーレス
3. **信頼性**: 高可用性 (障害耐性)、変更のリスクの低減、災害復旧、バックアップ
4. **コスト管理**: 財務オペレーション、商用最適化、予算、コスト割り当て
5. **運用上の優秀性**: 自動化、監視、サポート、管理、クラウドへの移行およびクラウド内での運用に必要な機能

ワークロード評価: デモを行うことができる一般的な一連のアプリケーションタイプは、以下の通りです。

- **ウェブアプリケーション**: バックエンドデータベースおよび静的オブジェクトストレージを含む、動的ウェブサイトのパブリックなホスティング。
- **データ分析**: 異種のデータプロバイダーからのデータを統合でき、ハイボリューム (TB/PB 単位のデータ) を処理する能力、多様性 (構造化、非構造化、各種フォーマットなど) 、および速度 (データ生成、および変更クエリパターンの速度) を実現するデータレイクまたはレイクハウスアーキテクチャ。
- **データサイエンスプラットフォーム**: 組織全体で AI/ML をベースとする機能の開発、デプロイ、使用を可能にするプラットフォーム。
- **IoT アプリケーション**: クラウド、ネットワーク能力、デバイスにまたがる IoT プラットフォーム/能力。

組織にとって重要な代表的なワークロードごとに、CISP がデモを行うシナリオを定義できます。シナリオでは、Well Architected の方法でワークロードのデプロイを実現する全体的な機能のデモを行う必要があります。以降のページでは、1) CISP のプラットフォームおよび 2) サンプルウェブアプリケーションワークロードのサンプルライブ技術評価基準を示します。

プラットフォーム – サンプルライブ技術評価

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Sec.1	ID フェデレーション	4	既存の ID ストアからクラウドサービスにフェデレーションする機能のデモを行う。	• SAML などの標準プロトコルのサポート。 • SCIM ベースの ID レプリケーションのサポート。 • 企業 ID ストア内で各種アクセスレベルを定義し、クラウドサービス事業者内で適用する機能。 • 特定のチーム/個人を特定のアカウント/プロジェクト/ワークロードに制限する機能。 • 属性ベースのアクセスコントロール (ABAC) をサポートし、クラウドサービス事業者の ID およびアクセス管理 (IAM) システム内でそれらの属性を使用してクラウドリソースへのアクセスを制御する機能。
Plat.Sec.2	ガバナンスの一元化	4	組織レベル (グローバルポリシー) とビジネス単位、およびプロジェクトレベルで、ポリシーおよび要求事項を一元的に定義する機能を持つことを示す。	• ポリシーは、サービスの有効化/無効化、地理的制限の適用 (リージョンの制限) を含むこと。 • ポリシーは、管理者を含むユーザーが監査/ガバナンスの統制を無効にできないことも必要である。
Plat.Sec.3	ユーザー許可の制限	3	ユーザー許可の制限の自動推奨事項を示す。	• 現在の許可を必要な許可と比較する機能。 • 最小特権を推進するポリシーの自動生成。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Sec.4	監査ログ記録	4	許可されたアクションと許可されなかったアクションの両方を含む、クラウドアクティビティの監査ログ記録のデモを行う。	• 組織全体の一元化されたログ。 • 低レベルの追跡および説明責任をサポートする、アカウント/プロジェクト固有のログ。 • ログのクエリを可能にするツール。 • 特定のイベント/ログエントリに基づいたアクションのトリガーを可能にするツール。 • サプライヤーサポートアクティビティを表示する機能。 • 管理者であってもログを削除できないようにする機能。
Plat.Sec.5	ネットワークの分離	4	可能な限り、クラウド内の各種テナントの分離のデモを行い、証明する。分離された (接続のない) サブネット、プライベート (インターネットがない) サブネット、およびパブリック (インターネットアクセスがある) サブネットの設定のデモを行う。	• テナント (VPN およびクロス接続サービス上のものを含む) の分離。 • クラウドインフラストラクチャ外 (オンプレミス) からのトラフィックフロー、クラウドインフラストラクチャ内のトラフィックフロー、およびインターネットへのトラフィックフローを制御する機能。 • コンテナホスティングやサービスとしての機能などの共有サービスを使用する際に分離を適用する方法。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Sec.6	保管時の暗号化	4	BYOK およびクライアントサイド暗号化のオプションを含め、保管時のデータを暗号化する機能のデモを行う。	• 機密データの暗号化を要求する機能。 • プロバイダー管理キーまたはカスタマー管理キーを使用する機能。 • FIPS 140-2 の準拠。 • 暗号化要件の非準拠に対してアラートを出し、ログに記録する機能。 • 追加のコストの影響。 • パフォーマンスの影響。 • 耐量子アルゴリズムとキーサイズのサポート。
Plat.Sec.7	転送時の暗号化	4	転送時のデータを暗号化する機能のデモを行う。	• サービス API のデフォルトでの暗号化。 • ロードバランサーおよびマネージド API にて転送時の暗号化 (TLS) を有効にする機能。 • 相互 (クライアントとサーバー) 認証のサポート。
Plat.Sec.8	キーの管理	4	キーの管理機能のデモを行う。完全なキーのライフサイクルを含める。クラウドサービスとの統合を含める。	• ログの作成、キー使用のローテーション、および破棄。
Plat.Sec.9	設定管理	3	クラウドプラットフォームの設定管理機能のデモを行う。	• 正確な CMBD の維持。 • コンプライアンスの確認。 • コンプライアンス違反に基づいたアクションの自動トリガー。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
				• ベストプラクティスまたはカスタムルールに照らして設定変更を評価する機能。
Plat.Sec.10	ネットワークセキュリティ	3	サードパーティのルールセット/ファイアウォールとの統合や Volumetric 攻撃からの保護など、ウェブアプリケーションファイアウォールおよびファイアウォールの機能のデモを行う。	• WAF (Web Application Firewall) 機能: スケーラビリティ。 • プライベートおよびパブリックのネットワークのサポート。 • ルールセットの業界/ベンダーフィードをサブスクライブする機能。 • WAF からのイベントに基づいた、インフラストラクチャ内でのアクションの自動トリガー。 • ファイアウォール機能、スケーラビリティ。 • ホストベースおよびネットワークベースのファイアウォール。 • CIDR IP ブロックを指定する機能に加え、論理グループまたはオブジェクトを参照する機能。 • 各レベル/コンポーネントでサポートされるルールの数。 • ポリシーおよびネットワークの設定を介して分散運用モデル (ネットワークチーム + 開発チーム) をサポートする機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Sec.11	ネットワーク接続	3	オンプレミスネットワークに接続する機能、およびエンドポイント/クライアントをクラウド内のプライベートネットワークに接続する機能のデモを行う。	• プライベート接続 (10GBs を超える高帯域幅)。 • 組織全体でルーティングおよびファイアウォールポリシーを制御する機能。 • VPN 接続 (サイト間およびクライアントベース)。 • IPV6 サポート。
Plat.Sec.12	インスタンス管理	3	インスタンス管理機能のデモを行う。	• 大量のインスタンスのパッチ状態を監視および管理する機能。 • Linux および Windows オペレーティングシステムのパッチ管理のサポート。 • SSH を必要とせずにサーバーフリート全体でコマンドを実行する機能。 • 仮想マシンへのリモートアクセスを一元的に制御および監査する機能。 • コンソール、CLI、および API を使用して、インスタンスサイズの変更、追加ボリュームのアタッチ、ネットワーク設定などの変更などを行う機能。
Plat.Sec.13	ポリシー適用	3	パブリックインターネットからのアクセスを防止するようにサービスを設定する機能のデモを行う。	• 重要な/機密のデータを含む可能性が高いサービスのプライベートネットワークへのトラフィックを分離する機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
				• ソースネットワークに基づいてデータへのアクセスを制御するポリシーを定義する機能。 • ハイレベルの認証情報を備えたユーザーも含め、すべてのユーザーに対するこれらのアクセス制限の適用。
Plat.Sec.14	脆弱性スキャン	2	イメージ (コンテナおよび VM) で脆弱性をスキャンする機能のデモを行う。	• レジストリー内のコンテナを自動的にスキャンする機能。 • 仮想マシンで既知の脆弱性をスキャンする機能。 • ネットワークスキャンを実行する機能。
Plat.Sec.15	ネットワーク検査	2	カスタマー環境内からのネットワークトラフィック (NetFlow および完全なパケット) をキャプチャ/ミラーリングする機能のデモを行う。	• 完全なパケットのキャプチャも含め、(カスタマーテナントの観点における) クラウドサービス事業者のインフラストラクチャ内のトラフィックの一部/すべてをミラーリングする機能。 • キャプチャするトラフィックを簡単に選択する機能。 • 50 GBps を超える非常に大きなトラフィックボリュームにスケールする能力。
Plat.Sec.16	脅威検出	3	ネットワークからの脅威、認証情報の使用、使用パターン分析など、プラットフォームの侵入検出機能のデモを行う。	• 「マイニング」などの疑わしいアクティビティを検出する機能。 • SSH ログインなどの認証総当たり攻撃を検出する機能。 • 認証情報の漏えいや悪用を検出する機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
				• ML を適用し、大量のイベントを分析して優先順位付けされたイベントを表示する機能。 • 有効化/構成に必要な作業 (シンプルな方が良い)。 • 外部サービスと統合して通知をトリガーする機能。 • すべてのプロジェクト/アカウントに対してグローバルレベルで IDS を設定する機能。
Plat.Perf.1	コンピューティングの最適化	2	サービスとしての仮想マシンおよび機能のコストを最適化するための自動推奨事項のデモを行う。	• 実際の使用およびワークロードのパターンに基づいた推奨事項。 • 推奨事項には、推定削減額および予期される負荷レベル/技術的影響に対するインサイトが含まれていること。 • 最適化には、削減額と、たとえば仮想マシンのサイズが不足する可能性があるといった「パフォーマンスのリスク」の両方が含まれていること。
Plat.Perf.2	環境の最適化	2	ロードバランサー、ネットワークデータベース、ストレージなどのその他のクラウドコンポーネントの自動推奨事項のデモを行う。	• 推奨事項では、コアコンピューティング以外のコンポーネントにおける削減額と潜在的なパフォーマンス効率の機会を特定すること。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Perf.3	コンピューティングのオートスケーリング	4	仮想コンピューティング環境でロードバランサーの背後にデプロイされたアプリケーションのオートスケーリング機能のデモを行う。使用可能な各種オプション/アプローチや、スケーリングイベントの前後に他の (オプションの) アクションをトリガーする、通知などの機能のデモを行う。	• スケーリングの各種オプション (トリガーベース、時間ベース、手動、機械学習を適用して必要なキャパシティを予測するさらにインテリジェントなアプローチ)。 • ロードバランサーおよびヘルスチェックへの登録も含めた、完全に自動化されたスケーリング。 • スケーリングライフサイクルの特定の時点で任意のコードを実行する機能。
Plat.Perf.4	ストレージのオンラインスケーリング	3	ワークロードを中断することなく、ブロックストレージのキャパシティとスループットの両方をスケールする機能のデモを行う。	• サービスを完全に再構築することなく、異なるストレージタイプ間でブロックストレージを移行する機能。 • VM に提供されるボリュームのサイズを増やす機能。
Plat.Perf.5	マネージドサービスのオートスケーリング	3	オブジェクトストア、API ゲートウェイ、FaaS プラットフォーム、および NoSQL データベースで同時ユーザー数を少数 (十単位) から多数 (千単位) にスケールする機能のデモを行う。	• シームレスなオートスケーリング (できれば、管理者による介入なし)。 • 本番スケーリング要求事項に合致した、段階的スケールアップ期間における一貫したパフォーマンス。 • FaaS などの一部のコンポーネントでは、同時実行制限を事前ウォーミングおよび管理するためのオプションも必要に応じて示すこと。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Perf.6	コンテナベースのワークロード	3	コンテナベースのワークロードをホストする機能のデモを行う。	• コンテナホスティングプラットフォームのオプション。 • ロードバランサーなど、他の IaaS コンポーネントとの統合。 • サービスメッシュソリューションが利用可能かどうか。 • Kubernetes などのコンテナホスティングの非専有オプション。 • コンテナコントロールプレーン内の高可用性のネイティブサポート。 • オンプレミスでのコンテナのホストを管理する機能。
Plat.Rel.1	リージョンレジリエンス	4	局地的な障害 (停電など) をシミュレートした場合におけるリージョン内のリレーショナルデータベースインスタンスの自動フェイルオーバーのデモを行う。	• 自動フェイルオーバー。 • クラウドリージョン内の障害ゾーンの分離。 • 明確に境界を分け、シンプルに設計することによる高可用性の実現。
Plat.Rel.2	インスタンスの自動リカバリ	2	ヘルスチェックの失敗後における単一のインスタンス/インスタンスセットの自動リカバリのデモを行う。	• 構成可能なヘルスチェック。 • 完全に自動化されたインスタンスのリカバリ/再プロビジョニング。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Rel.3	ロードバランサーのヘルス認識	3	ロードバランサーが障害の発生しているインスタンスを自動的に検出して、トラフィックを他の正常なホストに再ルーティングする方法のデモを行う。	• 構成可能なヘルスチェック。 • 正常なホストへの自動トラフィックルーティング。
Plat.Rel.4	リージョンフェイルオーバー	3	セカンダリリージョンへの自動トラフィック移動など、マルチリージョンアーキテクチャのデモを行う。	• グローバル対応ヘルスチェック。 • 自動ルーティングオプション: レイテンシー、重み付け、そしてフェイルオーバー。 • 仮想マシンワークロードだけでなく、オブジェクトストア/NoSQL データベースサービスのようなマネージドサービスのサポート。
Plat.Rel.5	バックアップと復元	4	仮想マシン、データベース、マネージドサービスのバックアップとリカバリのオプションのデモを行う。	• 自動化のレベル。 • 同じ/別のクラウドリージョンに復元する機能。 • バックアップを別のクラウドリージョンにコピーする機能。
Plat.Cost.1	予算	3	予算管理機能 (サブアカウントおよびプロジェクト用に構造化する方法など) のデモを行う。	• 組織の各種レベルで予算の管理および監視を適用する機能を考慮すること。 • 例えば (タグ付けによって) コンポーネントをグループ化する機能、特定のクラウドサービスの予算を設定する機能、アラート/監視のしきい値を設定する機能など、柔軟性を確認すること。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Cost.2	予算の割り当て	1	プロジェクトの予算割り当てプロセスなど、新しいプロジェクト環境 (アカウント) のプロビジョニングのデモを行う。プロビジョニングには、手動による承認ステップとして 1) 技術レビュー/IT、2) 商用レビュー/財務が含まれていること。	• 適切な承認を受けて、セルフプロビジョニングする機能。 • 組織に合った、適切な予算設定、通知、または予算ポリシーの設定の自動化。
Plat.Cost.3	予算のレポート作成	2	組織全体で予算に関するレポートを作成する機能のデモを行う。特定の部門と組織全体のレポート作成 (必要最低限ベース)。レポートには、実績値に加え、予測/推定される支出値が含まれること。	• 組織の各種レベルで可視性を提供し、認識と透明性を確保する機能 (ただし、必要最低限ベース)。 • 予測は、現在と過去の利用トレンドに基づき、潜在的な予算超過を早期に警告すること。
Plat.Cost.4	予算管理	1	予算しきい値に達したときにアクションを実行する機能のデモを行う。アクションには、通知、制約の適用、予算の支出超過を防止するためのアクティブな介入を含めることができる。	• 異なるプロジェクトに対するアクションを定義する機能。 • プロジェクトごとに異なるアクションを実行する機能 (たとえば、開発環境への影響や本番環境への影響を考慮)。 • 同じ予算/プロジェクトで複数のアクションおよびしきい値を定義する機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
				• 標準機能に加え、カスタムアクションを定義する機能。
Plat.Cost.5	予算の周期性	1	異なる期間 (日次/月次/年次など) の予算を適用する機能のデモを行う。年次予算では、1 年に予期される支出の変化する配分を適用する機能のデモを行う。	• 各種期間の予算を定義する機能。 • 納税申告などの季節的/弾力性の高いワークロードで特に重要な、年次予算で 1 年にわたる支出の配分を設定する機能。
Plat.Cost.6	サードパーティのマーケットプレイス	3	サードパーティの製品を購入してデプロイする機能のデモを行う。マーケットプレイスで入手可能な一連のサードパーティ製品の予算を設定する方法、および利用可能な製品を制限する機能のデモを行う。	• グローバル予算、一連のプロジェクト/アカウントの予算などの、特定の製品の予算を設定する機能。 • 幅広いマーケットプレイスのサブセットのみをクラウドユーザーに表示する機能。
Plat.Cost.7	コンピューティング料金モデル	3	仮想マシンに適用できる各種料金/商用モデルのデモを行う。	• 能力として、長期契約が不要な、オンデマンドの詳細な (分/時間あたりの) 料金が含まれていること。 • 割引が適用されたオプションの長期契約。 • 割引が適用された、中断のあるインスタンスを購入する機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
				• 重要事項として、同じプロジェクト/アカウントでこれらのモデルを混用できること、また複数のアカウントでメリットを共有できること。
Plat.Cost.8	商用最適化の推奨事項	3	(技術的な変更を行うことなく) 支出を最適化するための商用最適化の推奨事項を受け取る機能のデモを行う。	• 仮想マシンやマネージドデータベースなどの複数のサービスの全体的な推奨事項。 • 容易に推奨事項を実行し、予期される節約/メリットを把握する機能。
Plat.Cost.9	専用ホスト	4	専用ホストをプロビジョニングして、特定のホストに関連付けられたオンプレミスライセンスを使用できるようにする機能のデモを行う。	• プロビジョニングの簡単さ。 • ホストの利用を管理する機能。 • 複数のプロジェクト/テナントでホストを共有する機能。
Plat.Ops.1	仮想マシンの移行	3	オンプレミスからクラウドベースの VM サービスへの仮想マシンのインポートのデモを行う。	• Windows と Linux ベースの両方のオペレーティングシステムをインポートする機能。 • 複数のマシンを同時にインポートする機能。 • レプリケーションセッションを維持して、クラウドへの迅速な「フェイルオーバー」を可能にする機能。
Plat.Ops.2	DevOps および自動化の機能	4	コードとしての環境の定義方法、完全に自動化されたデプロイ環境からのサポート、自動化されたテストおよび	• ネットワーク、仮想マシン、ストレージ、データベースなど、すべてのシステムコンポーネントをコードとして定義する機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
			ロールバックを含む、DevOps/自動化の機能のデモを行う。	• パイプラインを作成する機能。 • コードリポジトリを作成する機能。 • ビルドを自動化する機能。 • Blue/Green デプロイを実行する機能。 • 複数の環境を作成し、デプロイに複数のステージを用意する機能。 • デプロイ失敗時のロールバックの自動化。
Plat.Ops.3	アプリケーションのホスティング	2	ローコード/プラットフォームサービスでシンプルな 2 層アプリケーションのホスティングのデモを行う。リレーショナルデータベースと、アプリケーション/ウェブ層のオートスケーリングを含む。	• UI を使用したシンプルな設定。 • ヘルスチェック、スケーリング、高可用性の組み込み。Windows および Linux のプラットフォームサポート。
Plat.Ops.4	セキュリティ統合	2	セキュリティインシデントおよびイベント管理の観点からプラットフォームの統合機能のデモを行う。	• 統合のためにクラウドサービス事業者および API からセキュリティ関連のログを簡単に統合して取り込む機能。
Plat.Ops.5	ITSM 統合	3	ITSM (IT サービス管理) の観点からプラットフォームの統合機能のデモを行う。	• API を使用してサポートケースを作成、監視、更新する機能。 • API を使用して「製品」としてサービスまたはサービスセットをプロビジョニングする機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Plat.Ops.6	サポート	4	サポートサービスのデモを行う。	• ワークロードのタイプごとに異なるレベルのサポート。 • 特定のサービスに合わせて、オペレーティングシステム/データベースエンジンなどをサポートする能力。 • 重要なワークロードに対して指定されたサポートリーダーによって高度なサービスを提供する能力。 • 構造化されたイベント対応およびアーキテクチャーレビュープロセスを提供する能力。 • プロバイダーのロードマップに対するインサイト。
Plat.Ops.7	監査可能性	4	コンプライアンス監査をサポートするために用意されているツールのデモを行う。	• コンソールでコンプライアンス監査の詳細を取得する機能。 • 環境監査を管理および自動化する機能。
Plat.Ops.8	VM からコンテナへ	1	仮想マシン上のアプリケーションをコンテナに変換し、クラウドサービス事業者のコンテナプラットフォームを使用してサービスを提供する方法のデモを行う。	• 変換の使いやすさ。 • 変換にかかる時間。 • プラットフォームサポート (.Net および Java)。

ワークロード: ウェブアプリケーション – サンプルライブ技術評価

以下のセクションでは、特定の「ウェブアプリケーション」ワークロードのサンプルワークロード評価シートを示します。特定のアプリケーションの評価シートを作成する際には、アプリケーションユーザー、開発者、および管理者を参加させることを強くお勧めします。要求事項、現在の課題、制約について最も理解している可能性が高いためです。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Web.Sec.1	セキュリティ – アプリケーションの保護	3	SQL インジェクション、XSS スクリプティング攻撃などの攻撃でアプリケーションを悪用しようとする悪意のある試行をブロックする機能のデモを行う。	• 初期状態から、標準ルール/機能によって一般的な攻撃から保護する機能を持つこと。 • カスタムのチェック/ルール/関数を作成する機能。
Web.Sec.2	セキュリティ – レートベースの保護	3	大きなリクエストレートやデータボリュームをアプリケーションに送信することによる攻撃からブロック/保護する機能のデモを行う。	• 限度を設定し、特定の IP アドレスまたはアドレスのリストからのリクエストレートを制限する機能。
Web.Sec.3	セキュリティ – ソースベースの保護	3	ネットワーク/地理的なソースに基づいてアクセスを制限する機能のデモを行う。	• ネットワークブロックまたはネットワークブロックのリストによって制限する機能。 • (IP リストを管理することなく) 発信国で制限する機能。
Web.Sec.4	セキュリティ – ネットワー	4	コンポーネント (ウェブサーバー、アプリケーションサーバー/DB サーバ	• 複数のサブネットにコンポーネントを配置し、異なるサブネット間のトラフィックフローを制御する機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
	クセグメンテーション		ー) を分離/保護し、インフラストラクチャを介した南北および東西の伝搬から、保護する機能のデモを行う。	• ネットワークインターフェイスレベルでトラフィックフローを制御する機能。 • 論理グループおよび CIDR ブロックを参照する機能。
Web.Sec.5	セキュリティ — TLS のサポートおよび証明書管理	4	TLS で保護されたエンドポイントを提供し、それを提供するサポートコンポーネントを自動的に管理する機能のデモを行う (証明書の自動ローテーションなど)。	• 最新の TLS プロトコルのサポート、および必要に応じてレガシーバージョンを無効にする機能。 • シンプルな証明書の生成、管理、およびローテーション (完全に自動化されていることが好ましい)。
Web.Perf.1	パフォーマンス — スケーラビリティ	4	動的なオートスケーリングによって、ウェブアプリケーションの同時ユーザー数を 10 人から 100,000 人にスケールできる能力のデモを行う。	• 時間ベースおよびトリガーベースのスケーリングルールを定義する機能。 • エンドユーザーおよび管理者にとってシームレスなスケーリング。負荷の増加時の自動スケールアウト、負荷の減少時の自動スケールイン。 • ウェブアプリケーションの各レイヤー (ロードバランサー、ウェブレイヤー、データレイヤーなど) でスケーラビリティが確保されていること。 • 必要に応じてアプリケーションのレイヤーごとにキャッシングサービスが用意されていること。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Web.Perf.2	パフォーマンス - グローバル配信	3	オーストラリア、アジア、アフリカ、中東、北米、南米、ヨーロッパなど、世界中のさまざまな地点からのレイテンシーのデモを行うなど、CDN の能力のデモを行う。	• CISP コンソール/API を使用して CDN を作成および設定する機能。 • 各地域の構成可能な配信ルール。 • 各ユースケース/アプリケーションの構成可能なキャッシング。
Web.Rel.1	信頼性 - シングルリージョンレジリエンス	4	CISP データセンターへのネットワーク接続が失われるなど、局地的なイベントに耐える能力のデモを行う。	• クラウドリージョン (都市) 内の自動フェイルオーバーおよび高可用性。
Web.Rel.2	信頼性 – マルチリージョンデプロイ	3	グローバルにレプリケートされたデータベースなど、ウェブアプリケーションのマルチリージョンデプロイのデモを行う。	• マルチリージョンアプリケーションをプログラムでデプロイする機能。 • データストアのリージョン間のレプリケーション。 • 最適なリージョンへのユーザーの自動ルーティング。
Web.Rel.3	信頼性 - マルチリージョンフェイルオーバー	3	特定のリージョンに影響するサービスの問題が発生した場合における、ウェブアプリケーションの自動フェイルオーバーのデモを行う。	• 複数のクラウドリージョンにおける、自動フェイルオーバー、および高可用性。
Web.Cost.1	コスト - 可視性	2	アプリケーションごとにコストを追跡する機能のデモを行う。	• スケールアップ/ダウン時を含む、特定のアプリケーションのコストの履歴を表示する機能。

シナリオ ID	シナリオ名	重要度 (1＝低、4＝重要)	デモの要求事項	スコアリングに関する考慮事項
Web.Cost.2	コスト - 予算	2	アプリケーションごとに予算および関連アラートを設定する機能のデモを行う。	• アプリケーションごとに設定される予算、および設定されたしきい値に基づいてアクション/アラートをトリガーする機能。
Web.Ops.1	Ops - メンテナンスウィンドウ	3	(特にメンテナンスがアプリケーションの可用性に影響を与える可能性がある場合に) ビジネス要件に合わせてメンテナンスウィンドウを設定する機能のデモを行う。	• リレーショナルデータベースサービスなどのコンポーネントの構成可能なメンテナンスウィンドウ。
Web.Ops.2	Ops - ログ記録	3	仮想マシンの終了/障害発生時にログを永続化するなど、複数のコンポーネントを使用するアプリケーションのログ記録を一元化する機能のデモを行う。	• アプリケーション要件に合わせてスケールできる一元化されたログ記録サービスを設定する機能。 • 特定のログイベントに基づいてアラートまたはアクションをトリガーするルール/フィルターを定義する機能。
Web.Ops.3	Ops - 監視	3	パフォーマンス、可用性、応答時間、エラー数などのアプリケーションの監視、および各種指標しきい値に基づきアクションの実行/通知のトリガーを行う機能のデモを行う。	• ディスク入出力、CPU、データベース指標、ネットワーク、ロードバランサーなど、使用可能な一連の標準指標。 • カスタム指標、しきい値を定義する機能。 • カスタムダッシュボードを作成して、最も重要な指標を表示する機能、およびそのダッシュボードを関連ユーザーに共有する機能。