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-

注意

本書は、情報提供のみを目的として提供されています。特定国・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。クラウド利用者は、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、契約的コミットメント、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、または忠告と解釈されるものではありません。クラウド利用者は、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お勧めするものです。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、業界、一般生活、社会全般における役割について、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、全EU諸国で事業を行い、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、CISPEのデータ保護規範の1つ以上のサービス要件を満たす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
- 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
- 行動規範を使用し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に反対する

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、運用しています。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規範は、一般データ保護規則（GDPR）よりも以前に施行されました。本規範は、厳格なGDPRの要件に対応しており、クラウドサービス事業者が強力なフレームワークに準拠し、また提供することを促し、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旨としています。CISPEの行動規範では100以上のサービスが宣言されており、これらはEU加盟国の16か国に本社を置く30以上のクラウドサービス事業者によって提供され、数百万のエンドユーザーと消費者によって利用されています。https://cispe.cloud/code-of-conduct/

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、可能性の理解の向上に向けて取り組んでいます。

公共調達では、クラウドコンピューティングの選定および利用のプロセスについて要件定義する必要がありますが、クラウドサービスの購入は、公共部門で従来から知られている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、もって、欧州単一のクラウドインフラストラクチャ市場の成長と、デジタル単一市場（Digital Single Market: DSM）の成長を推進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://cispe.cloud/publicregister

目次

注意 2
CISPEについて 3
目次 4
本ハンドブックの概要および目的 5
1.0 クラウドフレームワーク契約の概要 8
2.0 クラウドサービスRFPの概要 11
2.1 クラウドサービスRFPの設定 11
2.1.1 序文および戦略目標 11
2.1.2 RFPの回答スケジュール 14
2.1.3 定義 14
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 15
2.1.5 入札者の最低限の要件 - 管理 19
2.2 技術 21
2.2.1 最低限の要件 22
2.2.2 ベンダー間の比較 24
2.2.3 契約 26
2.3 セキュリティ 28
2.3.1 最低限の要件 28
2.3.2 ベンダー間の比較 31
2.3.3 契約 32
2.4 料金表 32
2.4.1 最低限の要件 33
2.4.2 ベンダー間の比較 34
2.5 契約履行の設定／契約条件 38
2.5.1 契約条件 38
2.5.2 プロジェクトごとに契約締結先を選択する方法 41
2.5.3 オンボーディングとオフボーディング 41
3.0 ベストプラクティス／教訓 41
3.1 クラウドのガバナンス 41
3.2 クラウドの予算 42
3.3 パートナーのビジネスモデルを理解する 44
3.4 クラウドブローカー 45
3.5 RFP前のソーシング／市場調査 45
付録A—入札者相互間の比較に関する技術的要求事項 46
1. クラウドサービス事業者のプロファイル 46
2. グローバルインフラストラクチャ 46
3. インフラストラクチャ 47
3.1 コンピュート 47
3.2 ネットワーキング 50
3.3 ストレージ 54
4. 管理 59
5. セキュリティ 60
6. コンプライアンス 62
7. 移行 67
8. 請求 70
9. 管理 70
10. サポート 72
付録B — デモ 74

本ハンドブックの概要および目的

クラウドサービス購入ハンドブックの目的は、競争的な調達プロセス（**クラウドサービス提案依頼書 - RFP**）を通してクラウドサービスの購入を検討しているが、クラウドフレームワーク契約の専門知識が不足しているクラウド利用者に対してガイダンスを提供することです。

本書は、情報提供のみを目的として提供されています。特定国・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の下で**コールオフ**または**ミニ・コンペ**と言われるものを実施する際の追加的な選定要件の文言のサンプルともなります。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および要件定義の文言には、クラウドRFPと従来の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。

「**クラウドサービス**」とは、エンドユーザーがアクセスする必要のあるすべてのクラウドテクノロジーおよび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・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、既存の調達戦略を現代化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、料金表、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押さえておく(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**クラウドサービス事業者（*CSP*）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、クラウドサービス事業者から直接、またはクラウド

サービス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**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 2.3.2.ベンダー間の比較 2.3.3 契約
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プロジェクトごとに契約締結先を選択する方法 2.5.3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 3.5RFP前のソーシング／市場調査
付録A—入札者相互間の比較に関する技術的要件	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 - デモ	クラウドテクノロジー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を通してクラウドサービスを購入すると、関係する公共部門組織およびクラウドサービス事業者の双方にメリットがあります。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、クラウドサービス事業者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支援・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、クラウドサービス事業者から直接、または指定の再販事業者から購入することができます。
- **契約ガバナンス：**
    - 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。
    - これは、各公共部門組織ごとに異なることなく、標準の購入プロセス、契約条件、注文の仕組みを提供してナビゲートできるため、ベンダーにとってもメリットがあります。
    - 柔軟性が得られます。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が連携して、契約や仕組みを効率的に改善して締結できるようなフレームワーク契約を作成するほうが遥かに有益です。機能せず調整もできない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クラウドサービス事業者から選択し、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制御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、クラウドサービス事業者が提供する主要な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いるものが最適です。したがって、クラウドフレームワーク契約に係るクラウドサービス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クラウドサービス事業者から直接または指定の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、クラウドサービス事業者が提供する*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（クラウドサービス事業者から直接または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ことを鳥瞰するものです。

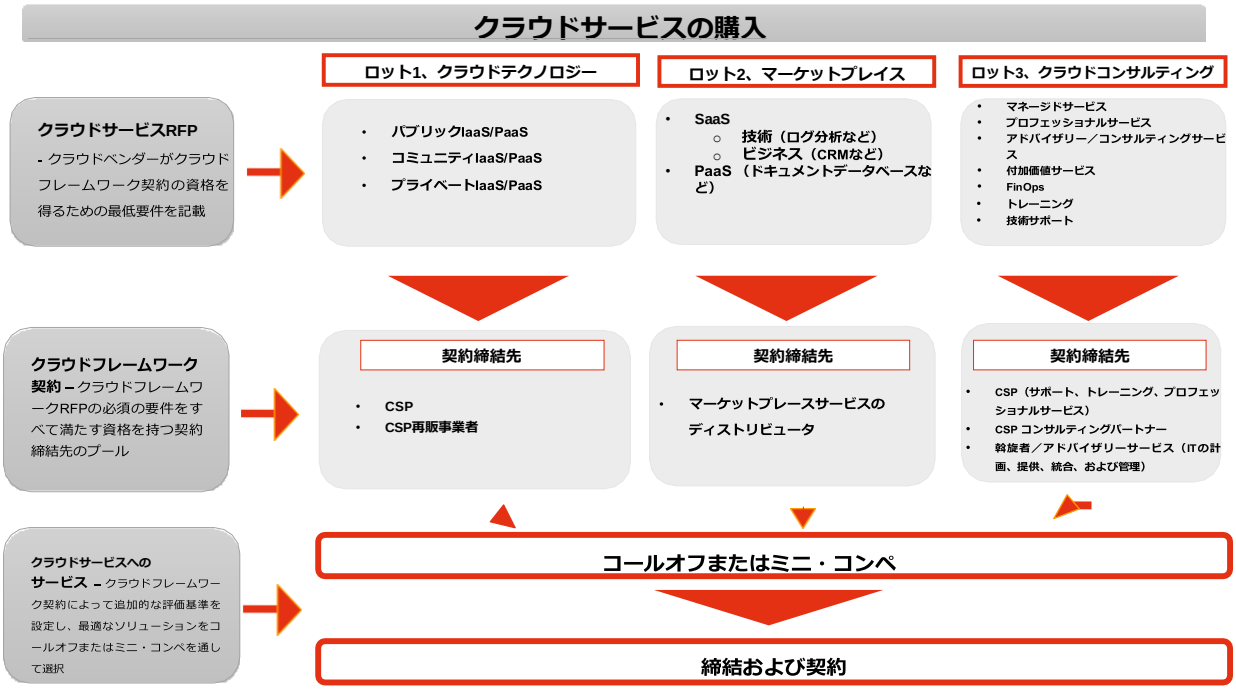

図1 – 適切なクラウドサービスRFPは3つのロットに分割されます。クラウドフレームワーク契約の下で、技術面および契約面でエンドユーザーの要件が確かに充足されるよう、ロットごとにカテゴリや提供の態様を分類。

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、クラウドサービス事業者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（アメリカ国立標準技術研究所（NIST）クラウドの必須の特徴）を参照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他の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の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、「*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（図 1 参照）の適格要件は必須項目および最低基準とすべきであり、いわゆる「nice to have (あるとうれしい)」な基準を含めるべきではありません。フレームワーク契約のため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、結果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で、調達者は、フレームワーク契約の下でもたらされるメリットを維持しつつ、コールオフのための機能仕様を追加して要件を詳細化することができます。

必要な場合、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させるもので、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としつつ、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になります。

上記の図*1*の一覧の通り、ロットごとに**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に関して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（CSP）、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し、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、この責任の明確化はク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クラウドサービス事業者の責任の範囲、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**、クラウドサービス事業者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が、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。クラウドサービス事業者は、大規模なクラウドインフラストラクチャ全体を運用するため、個々のお客様の環境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クラウドサービス事業者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、マネージドサービスプロバイダー（MSP）は、クラウドサービス事業者が提供する監視機能を設定および使用して、お客様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します。

[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

簡単に言うと、クラウドモデルの責任は以下の通りです：

クラウドサービス事業者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への導入および活用を支援

「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、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。ホームセンターでは、必要なものを作るために必要な幅広い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、家まるごと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ってくれる／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ってくれる／作業をしてくれる誰かと契約し、その人物に対して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運用できる社内スキルがある場合、クラウドサービス事業者の標準のクラウドテクノロジーとツールを導入するだけです（クラウドサービス事業者を使って直接、またはクラウドサービス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、クラウドサービス事業者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ために必要となる適切なタイプと規模のリソースを実装することができる。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ビジネス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（*CSP*）またはクラウドサービスの再販事業者
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***、移行およびクラウドサービス事業者の提供サービスを活用するための詳細な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（クラウドサービス事業者またはクラウドサービスの再販事業者）は、提案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なし。
- **データセンターへの依存は不要** - サーバーのラック作業、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** - 運用上の負担を軽減するため、サービスが運用される施設の物理的なセキュリティと、その上層のホストオペレーティングシステムおよび仮想化レイヤーまでのコンポーネントは、クラウドサービス事業者が運用、管理、統制を行う。
- **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、より安全に迅速に高い費用対効果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、クラウドサービス事業者のインフラストラクチャへの移行およびクラウドサービス事業者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）を知る権利が与えられる必要がある。

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、契約期間を含むRFP全体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*）の草稿の発行：** • **草稿*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、用語の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、クラウドサービスの再販事業者、ベンダーパートナーなど）、一般的な技術概念（コンピュート、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。以下は用語の定義リストのサンプルです。

RFPのサンプル文書：定義

アメリカ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、展開されたアプリケーション、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）。

- **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うが、例外的に、ユーザー固有のアプリケーション構成設定は制限される場合がある。

- **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、関連する構築・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。

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

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？
- クラウドサービス事業者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クラウドサービスの再販事業者／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？

クラウドサービス事業者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、クラウドサービス事業者に対してIaaS/PaaSを求めており、コンサルティングおよび「コンソール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線引きを表しています。

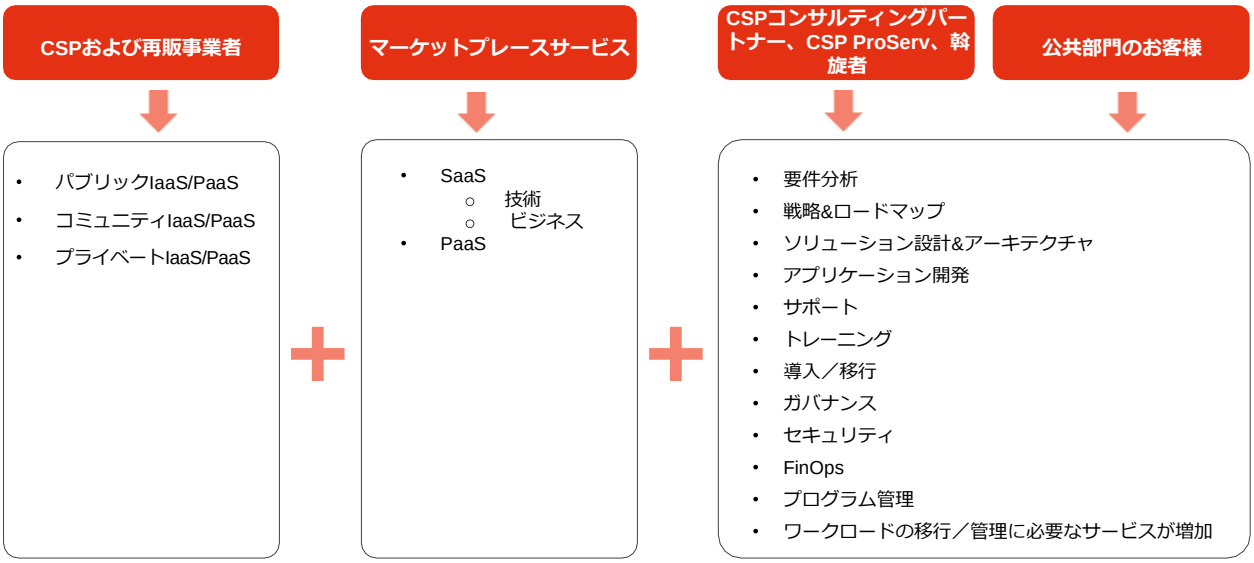

図2 – クラウドサービスRFPでは、必要となるすべてのクラウドサービスのメニューをエンドユーザーに提供する必要があります。公共部門のお客様は、クラウドサービス事業者に対してクラウドテクノロジー、必要に応じてPaaSおよびSaaS製品のマーケットプレイスを求めています。その後でお客様は、クラウドサービス事業者がクラウドサービスの提供で引き受ける役割の大きさ、およびクラウドサービス事業者が予定するコンサルティング会社／システムインテグレーター／マネージドサービスなどへの外部委託の規模を判断します。

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確認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複数の**ロット**で構成され、**<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／システム統合／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ついては、**<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時間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** - クラウドサービス事業者のテクノロジーの全範囲（クラウドサービス事業者から直接、クラウドサービスの再販事業者から、付加価値サービス／サポートを持つ再販事業者）：

    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ト、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、*Big Data & Analytics*、*DevOps*などのパッケージ化されたクラウドテクノロジーも含まれる。

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*、コンテンツ分析、ログ分析など。

3. **ロット*3*：クラウドコンサルティング** – 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）および関連するクラウド移行および利用の全範囲。これらのサービスには、計画、設計、移行、管理、サポート、*QA*、トレーニングなどが含まれる。

ベンダーは提出物を複数のロットで提出することができる。

ベンダーは提出物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

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または「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置くことにより、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、コールオフ契約の詳細な機能仕様を使って要件を細かく設定することができる。

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、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、要件を満足する資格を持つ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：

- サービスに使用する利用可能な資金
- 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／サービスを検索する。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（正規料金の一覧／料金表の文書であることを前提に、リクエスト時に有効な公開されている料金表へのリンクも許容される）

料金は、サービスを構成する最も一般的なコストになる。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の文書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ます。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、使用する詳細な特徴、およびそれらの重み付けを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にして実施し、プロジェクトの要件を参照せずにベンダー／サービスを除外してはいけない。

表2 - MEATベースの評価

締結基準
全ライフコスト：費用対効果、価格、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
機能以外の特徴

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る。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件に対応するように依頼することによって、顧客がフレームワーク契約の下でさらに競争を行うことである。顧客は、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、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、調達者とベンダーは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）が契約のコピー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要件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を想定していないことを明確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、要件事項と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**に関する詳細情報を記述しました。たとえば、クラウドサービスの再販事業者/MSP/SI/コンサルティング会社などの最低限の資格要件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がクラウドサービス事業者と直接提携していること、（2）サードパーティの組織に対するクラウドサービス事業者の提供サービスへの直接アクセスの再販をクラウドサービス事業者が認定していること、（3）能力および専門知識を示すクラウドサービス事業者による認定資格があること。

ロット*1*

- パブリッククラウドサービス（*IaaS*および*PaaS*）の直接プロバイダー（クラウドサービス事業者）

***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、民間のクラウドサービス事業者、クラウドサービスの再販事業者、マーケットプレースサービスのディストリビュータ、および／またはクラウドサービス活用のためのサービスのプロバイダー（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）でなければならない。入札する役割を明確化すること。

_____ - 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（*CSP*）

_____ - 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（*CSP*）

_____ - クラウドサービスの再販事業者（クラウドサービス事業者の提供サービスへのアクセスを直接提供が可能）。

- クラウドサービス事業者の提供サービスに対して直接アクセスできる再販可能なサービスを明記すること：_____
- クラウドサービス事業者の提供サービスの認定再販事業者であることを示すクラウドサービス事業者からのレターを提示すること：_____

ロット*2*

____- クラウド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*）

____ - クラウド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クラウドサービス事業者

____ - クラウドサービスの技術サービスを提供するプロバイダー

____- クラウド上で利用または運用するサービスを提供するクラウドサービス事業者のパートナー

____- クラウド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：

- クラウドサービス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 – 監視（*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（記載すること）：_____

サービスを提供する対象のすべてのクラウドサービスを明記すること：_____
クラウドサービスモデルにおけるクラウドサービス事業者からのパートナー指定を確認するための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（*CSP*）
クラウドサービス事業者の資格を得るには、以下の要件に適合する必要がある。

提案するクラウドサービス事業者の資格基準	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、クラウドサービス事業者が契約を遂行できることを判断できる。
除外基準、たとえば犯罪／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クラウドサービス事業者の実績を判定できる。
企業の社会的責任	これらは、クラウドサービス事業者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。
公的に入手可能なサステナビリティに関するコミットメントおよび実践内容	顧客は、クラウドサービス事業者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。
クラウドサービス事業者は、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。	クラウドサービス事業者は最新製品を迅速に顧客の手に届くよう取り組み、その後、製品を繰り返し頻繁に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。

クラウドサービス事業者と再販事業者／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クラウドサービス事業者と直接関係していることを求める。また、サードパーティの組織に対して提供サービスが再販できることに加え、クラウドサービスに関する能力や専門知識を保有することをクラウドサービス事業者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**の主契約者とクラウドサービス事業者間の下請け契約という追加的なレイヤーについて、関連する契約条件を確認する必要がなくなる。また、この要件によって、以下の場合に発生する追加的な再販事業者の複雑さが軽減される。

（*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

（*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

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、クラウドサービス事業者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。クラウドサービス事業者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価値提供を目的とするクラウドサービスの基本的な手法、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。

[3] クラウドサービスRFPでは、企業および社内の従業員チームの構成に注目するではなく、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では、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。

2.2.1 最低限の要件

従来のIT調達ではしばしば、組織が現在どのように業務を行なっているかを明文化することで作成されたビジネス要件に基づいていました。何も問題のない状況で、ビジネス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、文書化された要件は、それ自体が時代遅れで非効率な過去のビジネスプロセスである可能性があります。これらの要件が、クラウドサービス事業者によって置き換えられるべき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かも知れません。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、ビジネス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、各組織はビジネス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ビジネス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、および構成変更によってビジネスルールを最適化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てい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**、クラウドサービス事業者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、クラウドサービス事業者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クラウドサービス事業者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、上記のクラウドサービス事業者の管理上の最低要件も参照すること。

提案するクラウドサービス事業者の資格基準	理由
インフラストラクチャ	
クラウドサービス事業者のインフラストラクチャは、*2*つの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、可用性が高いアクティブ／アクティブで構成され、*DR*／*BC*シナリオの実施が可能な、低遅延のリンクで接続されている*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。	クラウドサービス事業者は、単一障害点を回避が可能な、可用性が比較的高い運用で構築されたインフラストラクチャを提供できる必要がある。
クラウドサービス事業者は、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、クラウドサービス事業者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では、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。
クラウドサービス事業者は、データセンターと直接接続できる専用線でのプライベート接続を提供する必要がある。	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。

クラウドサービス事業者は、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。
クラウドサービス事業者の最低認定資格	
クラウドサービス事業者は*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。
クラウドサービス事業者は、顧客が*GDPR*準拠のアプリケーションを構築できるように、*GDPR*に準拠して利用可能な機能や*j*さービスを提供する必要がある。	顧客は*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必要があるため、*GDPR*準拠のサービスとツールの提供は、前提条件となる。
クラウドサービス事業者は、クラウドサービス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。	クラウドサービス事業者は、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がある必要がある。*SOC*レポートは、信頼と透明性の確認に役立つ。
サービスの特徴	
クラウドサービス事業者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、クラウドサービス事業者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。
クラウドサービス事業者は、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、統合された自動スケーリングなどの基本的な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。
クラウドサービス事業者は、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、クラウドサービス事業者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。
クラウドサービス事業者は、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、顧客は短命の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、クラウドサービス事業者を活用できる。
データおよびシステムセキュリティ	
クラウドサービス事業者は、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を自由に選択できるようにし、顧客からデータの移動を行わない限り、顧客のデータは移動しない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。
クラウドサービス事業者の特性上、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標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	
クラウドサービス事業者には、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。	
クラウドサービス事業者は、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。	
クラウドサービス事業者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、クラウドサービス事業者は、以下の技術要件の質問に対するの回答も提供する必要がある。

ソリューション
クラウドサービス事業者は次のソリューションについて、クラウドサービスに組み込まれている、またはクラウドサービスと統合されている事前組み込み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必要がある。

- 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
- ビジネスアプリケーション
- 通信&ネットワーキング
- *G*空間
- *IoT*
- *[その他]*

次のワークロードについて、クラウドサービス事業者の対応状況の概要を記入する：

- 災害復旧
- 開発とテスト
- アーカイブ化
- バックアップおよびリカバリ
- ビッグデータ
- 高性能コンピューティング（*HPC*）
- モノのインターネット（*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、競争評価時にクラウドサービス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。クラウドサービス事業者が標準的に提供する機能を超える機能（クラウドサービス事業者の構築済みの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、さらに有益な評価のために利用されるものです。

公共部門はしばしば、最高の価値、最も経済的な有利な入札（MEAT）、または最低価格などの評価基準を使用して、入札者間の競争性を確保します。公共部門の組織は、クラウドサービスRFPで競争性を確保するため、クラウドの固有機能を考慮したアプローチを導入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（コンピュートやストレージなど）の詳細な項目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高いレベルのソリューションに焦点を当てることが重要となります。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件」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、そのクラウドサービス事業者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]。

1) **オンデマンドセルフサービス：**応札者は、人的なやりとりを行わずに、必要に応じてサーバー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自動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、注文機能を提供し、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）サービスがプロビジョニングできる必要がある。提示する提供サービスにおいて、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のものを提供する必要がある。提示する提供サービスにおいて、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：**応札者のクラウドサービスは、マルチテナントモデルを採用してさまざまな仮想リソースを持つ複数の顧客にサービスを提供しており、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（データセンターがある国、地域など）。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：**応札者のクラウドサービスは、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。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ができる必要がある。
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、クラウドサービス事業者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、リーダーの位置付け
- クラウドサービス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

最後に、クラウドサービス事業者は付録*B*に記載されているシナリオを使用して比較される。

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

クラウドサービス事業者は、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、クラウドサービス事業者のお客様（多くの場合、クラウドサービス事業者のパートナーの支援を受けて）は、クラウドサービス事業者の商用SLAを活用して、お客様固有の要件や独自のSLAの満たす、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クラウドサービス事業者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*）に対するクラウドサービス事業者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、クラウドサービス事業者の*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>**がクラウドサービス事業者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、クラウドサービス事業者は**<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、およびクラウドサービス事業者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

クラウドサービス事業者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、クラウドサービス事業者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、クラウドサービス事業者の契約条件が、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

クラウドサービス事業者はサービスを通じて処理能力を提供しています。有効期限がありサービス保守契約の更新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すべてに対して展開され、その後、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の提出期限後にクラウドサービス事業者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記載されているサービス提供は、RFPの提出期限後に、新しいクラウドサービスの追加を広く許可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クラウド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、重要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は、調

達上の問題もなく可能です。

サンプル*RFP*言語：新規サービスおよび変更サービス

クラウドサービス事業者は、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／または共通環境のクラウドサービス事業者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、クラウドサービス事業者はしばしば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使用は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。

この調達仕様書の範囲には、**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クラウドサービスが含まれる。これにより、クラウドサービス事業者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>**は利用できる。

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、あるクラウドサービス事業者では、別のクラウドサービス事業者が簡単に提供できないサービスや機能が提供される場合があります。賢明なアプローチでは、クラウドサービス事業者に対してクラウドを終了するために必要な機能やサービスの提供や合理的な「移行戦略」に役立つサービスの使用方法に関する文書を求めることです。これは、クラウドサービス事業者にとって、標準化されたサービスを使用しているお客様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。

現在、EUの「非個人データの自由流通の法規」の第6条の要件に準拠し、「データの移植」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の策定が進められています。これらが公開された場合、このような可逆性を保証するためのツールとして利用することを推奨します。これらのリファレンスは、CISPEのWebサイトで入手できます。

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出口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ていないため、クラウドサービス事業者は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必要がある。クラウドサービス事業者は、ベンダーロックインを最小限に抑えて、クラウドサービス事業者のプラットフォーム間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する必要がある。クラウドサービス事業者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、合理的な出口戦略に役立つ。

クラウドサービス事業者は、規定の最小コミットメントまたは規定の長期契約を締結すべきではない。

クラウド上に格納されているデータは、顧客はいつでもエクスポートできる必要がある。クラウドサービス事業者は必要に応じてクラウド上のストレージの内外にデータを移動することを**<利用組織>**に許可するものとする。また、クラウドサービス事業者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植することを許可するものとする。**<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クラウドサービス事業者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の方法を管理します。一方で、クラウドサービス事業者は幅広く拡張されたセキュリティ機能を提供して、高いセキュリティと統制されたプラットフォーム上にサービスを提供する責任があります。このモデルでのクラウドサービス事業者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。

クラウドサービスRFPを成功させるには、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、クラウドサービス事業者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把握していることを確認することが重要となります。

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、クラウドサービス事業者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、クラウドサービス事業者は、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の提供が求められます。

- **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。
- 多層防御方式を導入し、*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。
- クラウドサービス事業者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。
- お客様がクラウド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できるように、*API*を提供します。
- クラウドサービスのリソースの作成およびデコミッションを組織の標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。
- クラウドサービスのリソースを識別し、対象のリソースを経時的に追跡や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。
- お客様がクラウド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、誰が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
- クラウド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。
- クラウドサービスのリソース全体について、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するために、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、付録A – 入札者相互間の比較に関する技術的要件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評価については、セキュリティの最低標準以上の機能を使用することになります。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、入札者間を比較するための要件については、「付録*A* – 入札者相互間の比較に関する技術的要件」を参照してください。

公共部門の組織は、クラウドサービス事業者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ことを推奨します。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を受けたクラウドサービス事業者を検討します。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の要件に基づいてクラウドサービス事業者が準拠するための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、クラウドサービス事業者が単に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。

***RFP*のサンプル文書：セキュリティ**

クラウドサービス事業者は、**<利用組織>**とサービスプロバイダー間との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。
クラウドサービス事業者は、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。

- 提案する提供物に、クラウドサービス事業者および**<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>**をサポートするクラウド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

クラウドサービス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実施されている統制を記入すること。クラウドサービス事業者は、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分離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、リソースを管理する。クラウドサービス事業者は、**<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。クラウドサービス事業者は、法的に要求される場合、クラウド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クラウドサービスを提供する場合を除き、いかなる目的に対しても**<利用組織>**のコンテンツにアクセスや利用は行いこと。
- **<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。クラウドサービス事業者は、法的に要求される場合、クラウドサービスを維持する必要がある場合、およびクラウドサービスを**<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。クラウドサービス事業者は、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。
- クラウドサービス事業者は、**<利用組織>**がセキュリティ管理環境を構築、運用、活用するために、クラウドサービス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、複数の第三者の独立監査人によって独立して審査されなければならない。

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このアプローチは、GDPR、ISO、SOCなどの大部分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。

クラウドの認定、認定、評価により、クラウドサービス事業者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を公共部門の組織に対して保証できます。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し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、クラウドサービス事業者はコンプライアンス、認定、評価に準拠していることを証明する機会が得られます。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、クラウドサービス事業者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（**統制に関する記載の大半は、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を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、クラウドセキュリティ上の問題となり、記録公開法または類似の立法を通して公開されます）

RFPのサンプル文書：コンプライアンス

クラウドサービス運用におけるデータ処理、データセキュリティ、機密性、可用性などの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、運用基準の利用することで、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、運用基準に対する独自の提案を評価する。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クラウドサービス事業者に求めることで、サービスのコンプライアンスを最新の状態に保つことができる。

入札中のクラウドサービス事業者は（直接または再販事業者を通じて）、以下の第三者の独立監査人による証明、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 – これらの保証、レポート、および認証の一部がセキュリティ上の理由で開示が制限されている場合、**<利用組織>**は以下の項目へのアクセス時、クラウドサービス事業者と連携して双方が同意する必要がある）：

認証／証明	**規定、規制、プライバシー**	**準拠／フレームワーク**
□*C5*（ドイツ） □*CISPE*データ保護行動規範（*GDPR*）		□*CDSA*
□*DIACAP*	□*EC*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*
	☐スペイン*DPA*認証	☐*NIST*
	☐英国*DPA - 1988*	☐*Uptime Institute Tier*
	☐*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。

2.3.2　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、競争評価時にクラウドサービス事業者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。

サンプルのクラウド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件を参照してください。クラウドサービス事業者を評価する公共部門の組織にとって、以下の機能について、セキュリティの主要な考慮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

- クラウドサービス事業者の責任共有モデルに対する理解、およびクラウドサービスの機能とサービスのセキュリティ責任の区分に関する顧客の理解に役立つ文書
- クラウドサービス事業者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、クラウド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対する具体的なクラウドサービス事業者の対応
- 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

- 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（クラウドサービス事業者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能力
- クラウドガバナンスポリシーの技術的なスクリプトの作成能力
- 機能の変更が許可されていないユーザーが上書きすることを禁止する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に実装し遂行できる能力。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の構築につながります。
- 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、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
- マネージド脅威検知サービス

2.3.3 契約

上記の通り、クラウドサービス事業者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、クラウドサービス事業者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、クラウドサービス事業者の契約条件が、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、クラウドサービス事業者がRFPの元の項目を遵守していることに加えて、クラウドサービス事業者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RFPの提出期限後に製品の更新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いること、およびクラウドサービス事業者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、使用は無料です。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。各当事者はセキュリティ責任について明確にする必要があります。クラウドサービス事業者は、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、クラウドサービス事業者が提供するクラウドテクノロジーのクラウドサービス事業者と利用者の双方のセキュリティ責任を文書化する必要があります。

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、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を備え、利用状況と支出を可視化できることに加え、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では、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者や総合的な最低価格にはつながりません。

クラウドサービス事業者の料金表を評価するには、類似の能力を持つクラウドサービス事業者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**、クラウドサービス事業者の事前選考、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典型的なクラウドアーキテクチャおよび**価格シナリオ**の内容に注目し、クラウドサービス事業者に価格を提供してもらいます。また、クラウドサービス事業者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されます。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*を参照してください。

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は以下の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：**クラウドサービス事業者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：**クラウドの価格は市場価格に基づいて変動する柔軟性が備わっていること。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：**クラウドサービス事業者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）使用状況と支出を予測して将来のクラウド予算を計画できること。

RFPのサンプル文書：価格設定

<利用組織>は、応札するクラウドサービス事業者に対して、商用クラウドの機能としてエンドユーザーに提供される各サービスについて、提案方法および価格モデルを記載するよう要求する。

クラウドサービス事業者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（正規料金の一覧／料金表の文書であることを前提に、リクエスト時に有効な公開されている料金表へのリンクも許容される）

料金は、サービスを構成する最も一般的なコストになる。クラウドサービス事業者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。

詳細な価格要件

- 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動的な価格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む必要がある：
  - 料金は、オンデマンド式、公共料金スタイル、従量課金でサービスが提供されているか？価格モデルを説明すること。
  - 使用量の約束および／または一括購入の場合、さらに割引は可能か？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記載すること。
  - 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>**が支払うクラウド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絶対にあってはならない。

予算および請求アラート／レポート
クラウドサービス事業者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、クラウドサービス事業者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>**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、クラウド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、クラウドサービス事業者は**<利用組織>**に対してクラウドサービスの請求内容の**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必要がある。

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（コンピュートやストレージなど）の項目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クラウドサービス事業者の監視ツール、またはクラウドサービス事業者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、クラウドサービスのカタログ価格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
私たちは、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、クラウドサービス事業者の標準割引、パフォーマンスを改善しコスト削減／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も含まれます。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、クラウドサービス事業者の提供サービス同士の価格を比較する場合、技術的な利点も考慮することが重要です。たとえば、あるクラウドサービス事業者の場合、地理的なリージョン内で複数のデータセンターによるクラスタ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を持たないクラウドサービス事業者の場合、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。クラウドサービスを評価する場合、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クラウドサービス事業者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。CSP 1のストレージ「ユニット」の項目の価格は€ 0.023/GBです。CSP 2の同じの「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の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は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、クラウドサービスのサーバーレス機能の利用を増やすと、コストを%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ものものが含まれます。

基本料金 – 基本的にはクラウドサービス事業者の公開されている価格です。クラウドサービス事業者はこれらの料金を公開している必要があります。ただし、上記のクラウドサービス事業者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だけ）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（お客様はすべてのクラウドサービス事業者の多数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）。

クラウドサービス事業者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必須です。たとえば、クラウドサービス事業者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、価格評価では他のクラウドサービス事業者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ビスを顧慮する必要があります。

評価基準は、クラウドサービス事業者が提供する「xの機能がデフォルトに含まれる」コールオフ契約、および対象のサービスがコスト全体に与える影響度を考慮して記載することができます。また、評価基準ではクラウドサービス事業者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利用可能な割引にも注目することができます。例：

- お客様がリザーブされたコンピュート能力（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ではx%の割引
- 最適なコンピュート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、全ライフコストの考慮、およびコスト最適化機能によるコスト削減

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、サービスの利用量がベースになる。

以下は、価格発見の目的に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、クラウドサービス事業者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、およびクラウドサービス事業者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すること。

2.5 契約履行の設定／契約条件

クラウドサービス事業者が提供するクラウドテクノロジーと運用は設計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、応札者は多くの調達要件またはすべての調達要件に準拠することを求める厳格なルールが含まれている場合が多く、さもなければ拒否されます。もしくは、非常に厳しい必須の要件が含まれていることが考えられます。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場合、現実は標準化された一連のコンポーネントやツールの調達となり、特化したソリューションや調達の設計は失敗する傾向があります。

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、クラウドサービス事業者のWebサイトで公開されているクラウドサービス事業者の既存の取引条件を確認して理解することです。公共部門の組織はクラウドサービス事業者の取引条件を問題なく受け入れるケースが増えています。クラウドサービス事業者やそのパートナーとの会合をもうけて、考え方について深く掘り下げることは、条件を理解する取り組みの一環となります。質問の鍵は、クラウドサービス事業者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、それがクラウド契約の一部である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、クラウドサービス事業者は、法人客向けに若干変更可能な、修正協議に応じることのできる協定を用意して対応しています。

クラウドサービス事業者の利用規約を見直すとともに、既存の方針や規則、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、クラウドサービス事業者のモデルとは相容れない場合があります。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などです。クラウドサービス事業者は新規サービスの追加と新機能の追加を常に行っています。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、これらの方針や規則、法規の検討も含め、クラウドサービス事業者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、クラウドサービス事業者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、御社の取り組みや方針、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、関連する規約の仕組み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、管理対象サービス、ハードウェア、パッケージソフトウェア、およびシステム統合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、RFPプロセスは、理解が得られるように交渉や協議に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、公共部門の組織では、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、効果的な提案を拒否していたことも考えられる場合の差異を解消します。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で、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です）。

交渉上の柔軟性

クラウドサービス事業者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) 申請者から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、クラウドサービス事業者はお客様がデータを所有していることと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を確実に制限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（Terms & Conditions）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向けの「万能なアプローチ」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免除されるため、各組織はそのような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、必須要件または条件の適用は必ず最小限に抑える必要があります。

クラウドサービス事業者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納入されることに留意する必要があります。したがって、クラウドサービス事業者では、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、クラウドサービス事業者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
クラウドサービス事業者から直接クラウドテクノロジーを購入する代わりに、クラウドサービスの再販業者から購入するという選択肢もあります。クラウドサービスの再販業者の詳細については、上記のセクション*2.1.3*を参照してください。

***RFP*言語のサンプル：利用規約**

クラウドサービス事業者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、クラウドサービス事業者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。**
- クラウド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。クラウドサービス事業者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。クラウドサービス事業者に標準的な*SLA*を許可することで、クラウドサービス事業者はコストを低く抑え、これらの*SLA*が顧客に提供される。それと同時に、顧客はクラウドサービス事業者が*SLA*を満たすことを確信できるようになる。
- 責任の上限は比例分配するようにすること。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、クラウドサービス事業者は低価値プロジェクトを受け入れる意欲がそがれることになる。低価値プロジェクトは、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。
- 顧客は独自のデータを所有している必要がある。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　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て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。

2.5.3　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できます。

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状況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　クラウドのガバナンス

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を呼び出すだけでよいのです。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考え直し、クラウドがもたらすメリットを活用することで、合理化し、改善することができます。

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漸進的なプロセスであり、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、クラウドサービスを単一のライン品目（コンピュート、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**というライン品目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、現在と新規のすべてのクラウド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品目を追加することができます。

適切なリソースカテゴリの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つのライン品目にまとめる場合は、「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	ユニット	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ース	10	件別	€10	€100

この体系の仕組みを示す例として、クラウドサービス事業者を使用する公共部門の組織の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協定を結んでいます。同組織は最初に年額200万ユーロを拠出します。毎月請求書が発生し、その代金は基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。残りの基金については、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。基金の残高が減少してくると、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	内容	数量	単位	価格
01	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
<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発注されるが、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、請負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、入札に応じることはありません。間接調達モデル（クラウドサービス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って同時にあるいは交互に機能するようにアプリケーションを設計しようとすると、どうしても実現能力のトレードオフが生じてしまいます（**クラウドにとってのロゼッタストーンは存在しません**）。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議論や調整の余地のある潜在的な問題が指摘されます。

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の要求事項を説明します。

1. クラウドサービス事業者のプロファイル

	要求事項
1.	**市場経験：** 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地域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入すること。
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 コンピュート

	要求事項
1.	**コンピュート—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、コンピュート、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.	**コンピュート—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.	**コンピュート—通常のインスタンス—コンピュート最適化：** 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? ● コンピュート最適化—コンピュート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 ○ 「はい」 の場合、最大のインスタンスは何か?
4.	**コンピュート—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 ○ 「はい」の場合、最大ストレージ容量（*5*、*10*、*20*、*50TB*）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.	**コンピュート—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 ○ 「はい」 の場合、最大のインスタンスは何か?
6.	**コンピュート—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向け、ハードウェアのグラフィック処理装置（*GPU*） ○ 「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.	**コンピュート—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*） ○ 「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.	**コンピュート—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.	**コンピュート—*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.	**コンピュート—テンポラリ・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テンポラリストレージに使用されるコンピュート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.	**コンピュート—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フェースカード*(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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—自動拡張：** 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（すなわち「スケールアウト」）を提供しているか?
20.	**コンピュート—画像インポートの仕組み：** このクラウドサービス事業者は、ユーザーが既存の画像をインポートし、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画像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.	**コンピュート—画像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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—通知：** 回復力のあるコンピュートイベントの場合、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能力を有しているか? 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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—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.	**コンピュート—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ース（*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.	**コンピュート—低価格での購入の仕組み：** 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を購入する仕組みを提供しているか?
31.	**コンピュート—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、追加の処理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.	**コンピュート—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処理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.	**コンピュート—*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、少なくとも一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、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.	**コンピュート—*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.	**コンピュート—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.	**コンピュート—サービスの制限：** このクラウドサービス事業者は、上記のコンピュート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代表する論理的かつ隔離された仮想ネットワー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、相互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相互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隔離された（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*ごとに複数の*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フェースカード（*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、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、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しているか?
14.	**ネットワーキング—侵入のフィルタリング：** 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（侵入）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.	**ネットワーキング退出のフィルタリング：** 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*(*退出*)*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）のロードバランサー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、コンピュート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、毎秒の一定数の入出力操作（*IOPS*）または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ているか?
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保存時データのサーバー側での暗号化を提供しているか? • 「はい」 の場合、採用される暗号アルゴリズムは何か?
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場合のあ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て、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? • 「はい」 の場合、採用される暗号アルゴリズムは何か?
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て、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、暗号化キーの管理を保持し、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（*RAW*）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—データ居所性：** このクラウドサービス事業者は、あるリージョンに格納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*Multi-Factor Authentication*（*MFA*）（多要素認証）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独立して任意の順序で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・トレージ—通知：** このクラウドサービス事業者は、ある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—クエリー機能：** 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—件名検索：** このクラウドサービス事業者は、構造化照会言語（*SQL*）の簡易表現を使用して、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ト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、可用性と耐久性を高度化するために、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）を重複して格納しているか?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ト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?
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の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管理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、保存中の暗号化をサポートしているか?
43.	**ファイルストレージ—移行中の暗号化：** 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、移行中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、ほとんど変動し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—フォルトトレランス：** 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フォルトトレランスを提供しているか?
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 0nce Read Many*（*WORM*）機能を提供しているか?
49.	**アーカイブストレージ—サブセット検索：** このクラウドサービス事業者は、構造化照会言語（*SQL*）の簡易表現を使用して、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は、保存中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 インスタンスに接続するドライブ最大数 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—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—一時信用証明書：** 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、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—組込みポリシー：** 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、*Multi-Factor Authentication*（*MFA*）（多要素認証）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こと。
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トホストにログインすることを制限し、その代わりに、コンピュート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こと。
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、保存中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管理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、および展開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—アクティブディレクトリ：** このクラウドサービス事業者は、クラウド内で管理されたマイクロソフトのアクティブディレクトリ（*AD*）サービスを提供しているか?
17.	**セキュリティ—オンプレミスアクティブディレクトリ：** このクラウドサービス事業者の管理されたマイクロソフトアクティブディレクトリサービス（*AD*）は、オンプレミスのマイクロソフトアクティブディレクトリとの統合をサポートしているか?
18.	**セキュリティ—*LADP*：** このクラウドサービス事業者の管理されたマイクロソフトアクティブディレクトリ（*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—アクティブディレクトリ：** このクラウドサービス事業者の管理されたマイクロソフトアクティブディレクトリ（*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—信用証明書の管理：** 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、およびその他の機密情報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管理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、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、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を提供しているか?
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、脅威検出マネージド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	規定、規制、プライバシー	準拠／フレームワーク
□*C5*（ドイツ） □*CISPE*データ保護行動規範（*GDPR*）		□*CDSA*
□*DIACAP*	□*EC*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*
	□スペイン*DPA*認証	□*NIST*
	□英国*DPA - 1988*	□*Uptime Institute Tier*
	□*VPAT* / セクション *508*	□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、独自のソリューションを評価できる。クラウドサービス事業者は、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の運用管理を満たしていることを、報告書を通して示すことができる。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：**クラウドサービス事業者は、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は、必要な作業が完了し次第、アクセスを無効にする必要がある。
- **立ち入りの制御と監視：**周辺データセンター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、事前承認されたエリアへのアクセスを制限される。
- **クラウドサービス事業者のデータセンターの作業員：**日常的にデータセンターへ出入りするクラウドサービス事業者の従業員は、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る。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。従業員が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場合は、一般の訪問者と同様のプロセスが実行される必要がある。
- **不正侵入の監視：**クラウドサービス事業者は、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、データセンター資産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、開いたままにしておくと警報音が鳴る装置で、出入り口のセキュリティを確保する必要がある。
- **クラウド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：クラウドの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、クラウド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ものとする。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りる。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に利用可能であること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：**クラウドサービス事業者のチームは、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て、常時も緊急時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、通常のクラウド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、クラウドサービス事業者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必須の手続きがある。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。クラウドサービス事業者は、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。クラウドサービス事業者はまた、技術的侵入の防止についても対策を講じる必要がある。クラウドサービス事業者のサーバーは、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、クラウドサービス事業者によって 「クリティカル」 に分類し、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う必要がある。クラウドサービス事業者は、デバイスのインストールと使用方法、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、クラウドサービス事業者は、*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クラウドサービス事業者の管理対象から除去されない。

- **第三者監査による手順とシステムの検証：**クラウドサービス事業者は、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、クラウドサービス事業者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、クラウドサービス事業者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、クラウドサービス事業者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：**クラウドサービス事業者は、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。クラウドサービス事業者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、クラウドサービス事業者の職員と消防士に問題を通知することができる。
- **複数のアベイラビリティーゾーンによる高可用性：**クラウドサービス事業者は、可用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、*1*つ以上のデータセンターで構成され、互いに物理的に分離され、冗長電源と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構築するために、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：**クラウドサービス事業者は、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、*C*クラウドサービス事業者は、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。クラウドサービス事業者は、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。クラウドサービス事業者の職員は、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：**クラウドサービス事業者は、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。クラウドサービス事業者は、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、クラウドサービス事業者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。クラウドサービス事業者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。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：**クラウドサービス事業者は、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、クラウドサービス事業者の顧客は、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：**クラウドサービス事業者は、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。クラウドサービス事業者は、クラウド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：**クラウドサービス事業者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。クラウドサービス事業者は試験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：**クラウドサービス事業者は、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の発動計画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。クラウドサービス事業者の人事システムで従業員の記録が終了した場合は、その従業員のアクセス権が自動的に取り消されるようにする。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クラウドサービス事業者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：**クラウドデータセンターへの物理的なアクセスは、ログに記録し、監視し、保持する必要がある。クラウドサービス事業者は、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：**クラウドサービス事業者は、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、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*日体制のクラウドサービス事業者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：**クラウドサービス事業者ののアセットは、所有者、所在地、ステータス、保守、およびクラウドサービス事業者が所有するアセットの記述情報を格納・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、クラウドサービス事業者によって 「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。クラウドサービス事業者は、デバイスのインストールと使用方法、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、クラウドサービス事業者は、*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クラウドサービス事業者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：**クラウド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、*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。クラウドサービス事業者は、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：**クラウドサービス事業者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：**クラウドサービス事業者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：**クラウドサービス事業者は、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：**クラウドサービス事業者は、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：**クラウドサービス事業者は、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、クラウドサービス事業者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は、予防保全が必要である。

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：**クラウドサービス事業者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、第三者によるクラウド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クラウドサービス事業者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：** このクラウドサービス事業者は、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.	**マイグレーション—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か?
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ト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、クラウド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統合されているか?
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クラウド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.	**課金—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*つの主要な支払口座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は何か?

6.	**管理—通知：** このクラウドサービス事業者は、*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、*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*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、過去のどの時点でも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—テンプレート設計者：** 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分で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、共通的なオペレーティングシステムおよびアプリケーションのスタックコンポーネントをサポートしているか?
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ース*(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共通ソリューション（*DevOps*、*Big Data*、*Data Warehouse*、*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別手順書（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 — デモ

デモンストレーションは、エンドユーザーがクラウドサービスをテストしたり、自社組織のビジネスニーズに最適な内容を反映させるために認証決定を行ったりする場合に効果的な方法と思われます。以下に、クラウドテクノロジーのデモンストレーションテストのスクリプト例を示します。

1. クラウドサービスのコンソールと一般に公開されているサービス／リソースのハイレベルなデモンストレーションを行う。
    - ストレージ機能
    - コンピュート機能
    - データベースの機能と種類
    - ネットワーキング
    - 管理および分析ツール
    - セキュリティ
    - その他の機能
2. デモで使用するクラウドテクノロジーの操作方法を記述する。
3. クラウドサービスを使用して、このデモをリアルタイムで実行する方法を実演する。
4. アカウント：
    - デモで使用するアカウントキーシステム（ルートとユーザー）について記述する。
    - アカウントキーの管理方法と保護方法のデモを行う。
5. ワークロード／データが保存されている物理的な場所を選択する方法のデモを行う。
6. 大規模なコンピュートおよびストレージソリューションをセットアップして、提供するサービスの規模のデモを行う。
7. エンドユーザーがクラウドサービスにさまざまなサービスを要求する方法を示す。以下のデモを行うこと。
    - アカウントの設定方法
    - セキュリティのプロビジョニングを有効化する方法
    - 主アカウントをサブアカウントに分割する方法
    - *Identity and Access Management*（*IAM*）で各種リソースにアクセスを分離する方法：
        - アカウントをセキュアにする方法
        - ユーザーとグループの作成
        - ポリシーの付加
        - パスワード設定
8. セキュリティとネットワーキングの観点から仮想環境を分離する方法のデモを行う。
    - サブネットの作成
    - インターネットルーティング
9. *2*か所以上の離れた場所に環境を構築する方法のデモを行う。
    - 複数の環境間でのロードバランシングのデモを行う。
10. 複数の方法を使用してクラウドコンピューティングサービス（例：*API*、*Web*コンソール、コマンドライン）と対話する機能を実演する。
11. ストレージ：
    - ストレージオプションの説明
    - 使用可能なストレージの種類（ブロック、オブジェクト等）とデータライフサイクルのプロセスのデモ
    - ストレージボリュームを設定して、データの読み込みと取得のデモ
    - コンピュートオプションを使用する場合と使用しない場合のそれぞれで*XGB*ストレージボリュームの作成
    - これらのボリュームにアクセスする許可のデモを行い、有効性を確認
12. コンピュート：
    - コンピュートオプションの説明—コンピュートリソースのサイズと機能
    - コンピュートリソースのアクティブ化と非アクティブ化のデモ
    - 特性（*X*個のインスタンスを同時に起動する機能、ネットワークの選択、偶発的終了に対する防護、テナント属性等）についてのデモ

- *RAM*のコア数および*GB*数に相当するコンピュートオプションのデモ
- ワークロードの実行による負荷ベースのリソース拡張のデモ
- 自動拡張機能のデモ
- コンピュートを停止して、あとで再起動する方法のデモ
- コンピュートオプションを使用して、構成のサイズ拡大・縮小や構成を維持する方法のデモ
- コンピュートオプションを使用してコピーする方法のデモ
- セキュリティグループの構成方法のデモ
- クラウドサービス事業者が提供のサービスで利用可能なオペレーティングシステムの記述
- *Linux*オペレーティングシステムのインストール例のデモ
- コンピュートサービスにイメージを提供する機能について記述
- サポートしているイメージフォーマットについて記述
- イメージをロードして操作する方法のデモ
- サーバーレスコンピューティングのデモ
- スポット市場に基づいて料金が変動するコンピュートインスタンスのクラスタを起動する機能のデモ

13. データベース：
    - データベース機能についての記述
    - *MySQL*、*MS SQL Server*、*Oracle*、および*Postgres*の各機能のデモ
    - データ・ウェアハウジング機能のデモ
    - これらのリソースをバックアップする機能のデモ
14. ネットワーキング：ソフトウェア定義のネットワークオプションとネットワーク管理機能のデモを行う。
15. 管理および分析
    - クラウド管理・分析機能についての記述
    - 監視オプションのデモ
    - *Hadoop*フレームワークを使用して各種機能のデモ
16. セキュリティ：ネットワークセキュリティのデモを行う。
    - セキュリティに対する取り組みについての記述
    - ファイアウォール
    - セキュリティグループ
    - ゲートウェイ
    - *NACL*
    - システムログ
    - 暗号化
    - 利用可能なコンプライアンス認定
    - 主要なストレージ
    - その他の機能
17. プロビジョニング：関連するクラウドリソースのコレクションを作成し、再利用可能なテンプレートを使用してそれらを整然と、予測可能な方法でプロビジョニングする方法のデモを行う。
18. ソフトウェア：一般に使用されるソフトウェアへのアクセスと利用を可能にする機能のデモを行う。
19. 大規模なデータ移転を実行する方法のデモを行う。
20. 以下に示す請求オプションのデモを行う。
    - 概要ビュー、詳細ビュー、タグ付きリソース別ビュー
    - 現在の支出/使用率に基づいて予測される支出/使用率
21. 利用可能なサポートおよびコンサルティング機能のデモを行う。
    - 使用可能なサポートオプション
    - サービスの利用状況に関するチェックやアドバイスを行う機能の有無

提供するサービスの差別化要因になると思われるその他の機能についてデモを行う。