令和元年度
行政機関におけるパブリック・クラウドの
活用に関する調査研究　報告書

本編

令和 2 年 3 月 31 日
一般社団法人 行政情報システム研究所

目　次

はじめに

近年のクラウド技術の着実な発展を背景に、民間企業等ではかねてより基幹システムも含めたあらゆる領域でその導入を進め、情報システムのパフォーマンス向上とコスト削減を実現してきた。諸外国政府でも以前より積極的にクラウドサービスの導入を進めており、情報システムのモダイナイゼーション（現代化）を実現しつつある。こうした中、我が国政府・自治体の行政情報システムでは、プライベートクラウドは一定程度、利用されているものの、パブリック・クラウドの導入はほとんど進んでいないのが現状である。その結果、現在の技術水準であれば成し得たはずの行政サービスの高度化やコスト削減の機会を活かしきれていない。

政府が「世界最先端 IT 国家創造宣言・官民データ活用推進基本計画」に基づき、今後、我が国行政機関及び自治体が的確にクラウドサービスの導入を図っていくためには、現在、政府が制度化を進めている「政府情報システムのためのセキュリティ評価制度（ISMAP）」[1]と併せて、どのようなスキームで調達を行うべきかを中心とした、現場の実務レベルでのハウツーやノウハウが必要になると考えられる。しかしながら、これまで我が国では、クラウドサービスの調達の実績は乏しく、過去の実績から十分な知見を得ることは困難である。そのため、こうした知見を得るためには、諸外国の先行事例から得られるノウハウや教訓を参考としつつ、我が国行政機関の IT 調達特有の制約条件や、過去の検討成果や先行的取組の教訓等を踏まえて、想定される課題や解決策を検討することが必要となる。

また、諸外国政府では、クラウドサービスの調達をはじめとする調達・契約改革の一環として、近年、包括契約やマーケットプレイスの導入、技術的対話の活用等が進められている。クラウド活用の在り方を検討するにあたっては、こうした応用的・発展的な調達・契約手法も視野に入れ、これらの導入可能性や導入に当たっての課題も併せて検討を行うことが必要であると考えられる。

本調査研究は、行政機関におけるパブリック・クラウドの活用及び関連する調達・契約手法に関して、諸外国政府での先行事例を調査・分析するとともに、我が国政府及び当研究所会員企業の協力を得て、課題及び解決策の検討を行うことで、現場の実務で役立つハウツーやノウハウ及び中長期的に講ずべき施策を抽出・提示することを目的として行うものである。

なお、本調査研究は、株式会社 NTT データ経営研究所の協力を得つつ当研究所において実施した。また、内閣官房 IT 総合戦略室、総務省行政管理局、及び当研究所会員企業からは研究会への参画を、自治体、各国政府、専門家各位には、インタビューや資料提供の協力をいただいた。この場を借りて深く感謝申し上げたい。

一般社団法人行政情報システム研究所

主席研究員　狩野　英司
主任研究員　栗田　祐一
研究員　増田　睦子
研究員　松岡　清志
研究員　松本　智史
研究員　細井　悠貴

[1] https://www.ipa.go.jp/security/ismap/summary.html

1. 調査研究の全体像と調査方法

1.1. 調査研究の構成

本調査研究では、まず第 1 章でパブリック・クラウドの特徴、及び我が国のクラウドサービスの導入にかかる政策や制度を整理した上で、第 2 章でクラウドサービスに関係する諸外国の調達・契約スキームについて、公開情報調査を行う。第 3 章では諸外国政府におけるパブリック・クラウドの活用の実際について、各国政府に対しヒアリング調査を行う。その上で、調査を通じて得られた情報をインプットとしつつ、第 4 章において、行政機関がパブリック・クラウドを活用するにあたって直面すると想定される課題について、専門家へのインタビュー調査並びに政府及び IT 企業からなる研究会での検討を通じて整理し、解決策として提示する。

なお、第 2 章で収集した情報については、要点のみ本報告書本編に掲載し、詳細は資料編に整理している。

以上の構成を図 1-1 に示す。

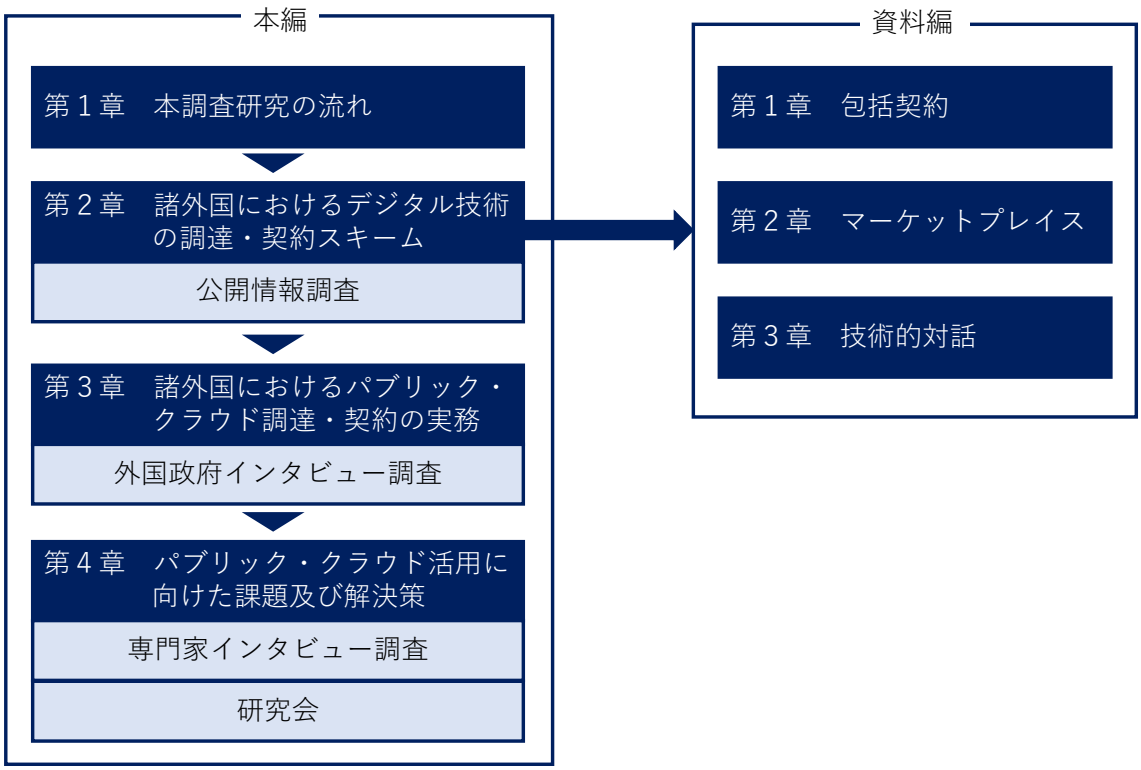


図 1-1　本書の構成

1.2. パブリック・クラウドの特徴

我が国の「政府情報システムにおけるクラウドサービスの利用に関する基本方針」（2018 年 6 月 7 日 CIO 連絡会議決定）、及び「パブリック・クラウドを利用した情報システムにおける計画・構築時の基本的な考え方」（2019 年 4 月政府 CIO 補佐官等ディスカッションペーパー）によれば、パブリック・クラウドは、任意の組織で利用可能なクラウドサービスであり、リソースは事業者（クラウドサービス提供者）によって制御される。パブリック・クラウドの特徴としては、以下の点が挙げられる。

- クラウドサービスの一時的な利用が容易に可能である
- 自ら構築・運用しなければ利用できなかった機能がクラウドサービス提供者によってサービスとして提供されるマネージドサービスが多数存在する
- 運用の効率化やセキュリティ対策の高度化等を目的として、新規サービスの提供や設定変更が継続的に行われる
- サーバの構築、負荷増大に伴うサーバの追加、障害時のサーバ再起動等、インフラ構築・運用の大半が自動化される
- 運用状況やクラウドサービスの利用料が逐次可視化される

また、このようなパブリック・クラウドの特長をさらに発展させ、利用したいときに各機関が利用できる状態を確保するとともに、多様なサービスの中から各機関が自らのニーズに合わせて適切なサービスを利用できるようにするための調達・契約のスキームとして、諸外国では、包括契約、マーケットプレイス、及び技術的対話が活用されている。

1.3. 用語

本報告書では、政府情報システムにおけるクラウドサービスの利用に係る基本方針に基づき、表 1-1 の用語定義を用いる。

表 1-1：本報告書で用いる用語

用語	意味
クラウドサービス	事業者等によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの
パブリック・クラウド	任意の組織で利用可能なクラウドサービスであり、リソースは事業者（クラウドサービス提供者）によって、制御される。
クラウド・バイ・デフォルト原則	クラウドサービスの利用を第一候補として、政府情報システムの検討を行うこと
クラウドサービスプロバイダー（CSP）	クラウドサービスの提供事業者。本報告書では、主にクラウドに特化したサービスの提供者を想定
（CSP との）直接契約方式	主として海外の大手クラウドサービスプロバイダー（CSP）が、顧客無差別に提供するクラウドサービスに対し、直接発注する方式

（CSP との）間接契約方式	CSP のサービスを顧客のニーズに合わせてカスタマイズして再販するリセラー又は SIer との間で締結する方式
リセラー	CSP のサービスを、システム開発は行わず（各種設定や小規模な開発を除く）再販する事業者
SIer	間接契約事業者のうち CSP のサービスを利用してシステム開発を行う事業者

1.4. 我が国のパブリック・クラウド調達に係る政府の政策及び制度

本調査研究は、表 1-2 に示す政府の政策及び制度を前提として行った。

表 1-2 パブリック・クラウド導入に係る政府の政策及び制度

名称	組織	概要
政府情報システムにおけるクラウドサービスの利用に係る基本方針[2]（2018 年 6 月 7 日）	CIO 連絡会議	本方針では、クラウド・バイ・デフォルト原則を具体化し、各府省が、効果的なクラウドサービスを採用し、かつ、クラウドサービスを効果的に利用するに当たり、クラウドサービス利用検討フェーズに係る基本的な考え方を示している。
パブリック・クラウドを利用した情報システムにおける計画・構築時の基本的な考え方[3]（2019 年 4 月）	政府 CIO 補佐官（ディスカッションペーパー）	オンプレミスのシステムを中心にシステムを計画・構築してきた情報システム関係者が、パブリック・クラウドを用いたシステムを計画・構築する際に必要となる基本的な考え方について、政府 CIO 補佐官等の有識者による検討内容を取りまとめている。
世界最先端デジタル国家創造宣言・官民データ活用推進基本計画[4]（2019 年 6 月 14 日）	内閣官房 IT 総合戦略本部	政府情報システムについて、取り扱う情報の特性、セキュリティ水準等を踏まえつつ、クラウドサービスの利用を第一候補として情報システムを導入する方針を示している。
デジタル・ガバメント実行計画[5]（2019 年 12 月 20 日）	内閣官房 IT 総合戦略本部	各府省が政府情報システムを整備する際に、対象となる行政サービス・業務、取り扱う情報等を明確化した上で、メリット、整備の規模、費用等を基に、各種クラウドサービスの利用を原則として検討する方針を示している。また、クラウドサービスを導入する際の安全性評価基準及び安全性評価の監査を活用した評価の仕組みを活用して安全性が評価されたクラウドサービスを利用できるように環境整備を行う方針を示している。
クラウドサービスの安全性評価に関する検討会 とりまとめ[6]（2020 年 1 月 30 日）	経産省・総務省	適切なセキュリティを満たすクラウドサービスを政府が導入するために必要な評価方法及び制度枠組みについて取りまとめている。

[2] https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf
[3] https://cio.go.jp/sites/default/files/uploads/documents/dp2019_01.pdf
[4] https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20190614/siryou1.pdf
[5] https://cio.go.jp/digi-gov-actionplan
[6] https://www.soumu.go.jp/main_content/000666496.pdf

政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて[7] （2020 年 1 月 30 日）	サイバーセキュリティ戦略本部	「サイバーセキュリティ戦略」及び「デジタル・ガバメント実行計画」を踏まえて、政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的な枠組みを定めたもの。情報セキュリティ監査の枠組みを活用した評価プロセスに基づいて、要求する基準に基づいたセキュリティ対策を実施していることが確認されたクラウドサービスを、本制度が公表するクラウドサービスリストに登録することを定めており、ISMAP（次項）の政策上の根拠となっている。
デジタル・ガバメント推進標準ガイドライン[8] （2020 年 3 月 31 日）	CIO 連絡会議	サービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理に関して、その手続き・手順に関する基本的な方針及び事項並びに政府内の各組織の役割等を定める体系的な政府の共通ルールである。
政府情報システムのためのセキュリティ評価制度（ISMAP）関連文書（基本規程、クラウドサービス登録規則、監査機関登録規則、情報セキュリティ監査基準、情報セキュリティ監査ガイドライン等）	ISMAP 運営委員会	「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」に基づき、「政府情報システムのためのセキュリティ評価制度」について定めるとともに、クラウドサービス事業者、監査機関、制度所管省庁、ISMAP 運営委員会、調達府省庁等が遵守しなければならない基本的事項を定めたものである。パブリックコメント後に正式にとりまとめられる予定。

[7] https://www.nisc.go.jp/active/general/pdf/wakugumi2020.pdf
[8] https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_20200331.pdf

2. 諸外国におけるデジタル技術の先進的な調達・契約スキーム

行政機関がクラウドサービスから得られるメリットを最大化するためには、クラウドサービスの導入に適した調達・契約スキームについて検討する必要がある。

このような観点から、本章では、クラウドサービスの調達において、調達コストの削減、期間の短縮、及び手続きの負荷の軽減を可能とするとともに、多様なサプライヤーへのアクセス機会の確保、革新的な技術の活用といったメリットをもたらす包括契約、マーケットプレイス及び技術的対話について、米国、英国、カナダ、豪州及びニュージーランドにおける調達・契約の枠組みを整理する。また、関連する参考事例として、単一省庁におけるクラウドサービスの大規模調達を行った米国国防総省の事例の概要を紹介する。

なお、各枠組みの導入の背景と目的、制度的根拠、調達・契約方式、基本的な契約・利用条件、関係組織、対象品目、現在の課題と今後の取組などの詳細は資料編で解説しているので、併せて参照されたい。

2.1. 調査手順

ウェブサイト等の公開情報を広く収集し、後述する第 3 章のヒアリング結果等を踏まえて解釈を加えつつ、情報の整理を行った。

2.2. 包括契約

包括契約という用語に一般的な定義は存在しない[9]。単一組織で、個々の品目ごとに、都度完結させる調達方式ではなく、複数組織、複数品目にまたがって包括的に契約を締結することで、調達／契約業務の効率化やボリュームディスカウント、新しいテクノロジーの取り込みなどを実現する契約方式が広く包括契約と称されている。

本調査研究で包括契約とは、調達手続きの一部又は全部の一元化を図ることにより、各機関が個別に調達することで重複して発生していたコストや手続きの負荷を軽減するとともに、政府全体として多様かつ革新的な IT 製品・サービスを活用することにより、政府の提供するサービスをより効率的かつ質の高いものとすることを目的とする仕組みのことをいう。包括契約を導入することにより、多様なサプライヤー及びサービスへのアクセス、サービスの効率的な調達によるコストと調達サイクルの短縮化、機関間での契約条件の標準化、革新的かつ最新の技術・製品・サービス・ソリューションの活用、そして政府、サプライヤー双方のサービス品質の向上といった便益も得られる。

こうした観点から、本調査研究では、クラウドサービスを切り口として、複数の公共機関（中央省庁や自治体、それらの関係機関等）に共通して適用される契約（政府機関の包括）や、複数種類の物品やサービスを対象とする契約（物品やサービスの包括）を調査対象とした。具体的には、米国の IT Schedule 70 及び基盤クラウドホスティングサービス、

[9] 例外的にニュージーランドには、中央集権的に物品・サービスを調達する契約の総称として collaborative contracts という用語がある。Government Procurement, “Types of contracts”,

英国の G-Cloud フレームワーク、カナダの SSC 非機密/機密クラウドサービス契約及び Microsoft Canada とのエンタープライズアグリーメント、豪州のクラウドサービスパネル・ヘッドアグリーメント及び大手 IT 企業との包括契約、並びにニュージーランドの政府一括調達契約、シンジケート契約及び共通機能契約である。

今回、調査対象とした各国の包括契約のスキームについて、適用組織、主管組織、目的及び対象製品・サービスを軸に、表 2-1 の通り整理した。

表 2-1　各国の包括契約の概要

国	名称	適用組織	主管組織	目的	対象となる製品・サービス
米国	IT Schedule 70	連邦政府、州政府等	一般調達庁（GSA）	調達サイクルの短縮、コンプライアンスの確保、革新的な技術・製品・サービス・ソリューションを利用することによるベストバリューの獲得	IT 製品・サービス全般
	基盤クラウドホスティングサービス（FCHS）	内務省及び内務省と合意を結んだ省庁	内務省（DoI）	長期の RoI を最大化する一方で、将来のミッションに関わるニーズを満たすためにクラウドのもつ拡張性や弾力性といった利点を最大限発揮	テクニカルサービス 7 分野 データセンター 商用クラウドホスティングサービス
英国	G-Cloud フレームワーク	中央省庁、自治体等	クラウン・コマーシャル・サービス（CCS）	多様なサプライヤー及びサービスへのアクセス、コストの削減、最新技術の活用、利用するサービスの拡張	クラウドサービス
カナダ	SSC 非機密/機密クラウドサービス契約	連邦政府等	シェアードサービス・カナダ（SSC）	信頼性が高く、費用対効果の高いデジタル通信サービスの提供	クラウドサービス
	Microsoft Canada とのエンタープライズアグリーメント	連邦政府	シェアードサービス・カナダ（SSC）	コスト削減、ユーザのタイプに応じた柔軟なサービス選択	Microsoft 製品、サービス
豪州	クラウドサービスパネル・ヘッドアグリーメント	連邦政府等	デジタル変革庁（DTA）	安価で良質のサービスを効率的に調達、透明性の確保、契約条件の標準化、政府及びサプライヤー双方にメリットをもたらすような契約管理の改善	クラウドサービス
	大手 IT 企業との包括契約	連邦政府	デジタル変革庁（DTA）		IBM、Microsoft、AWS、SAP 等の契約企業の製品・サービス
NZ	政府一括調達契約（AoG）	政府機関	内務省（DIA）（IT に関するもの）	各省庁の費用削減、サプライヤーとの関与の在り方の改善、調達方法の標準化、政府・サプライヤー双方のサービス品質の向上	複数政府機関が共通して利用するものが対象で、特定の物品やサービスに限定したものではない。（政府一括調達契約、シンジケート契約、共通機能契約は、契約のカテゴリーの名称）。本報告書ではクラウドの事例を紹介
	シンジケート契約	政府機関	契約に参加する機関の中から選定	契約及び購入製品・サービスの一貫性確保、スケールメリットを活かしたコスト削減	
	共通機能契約	政府機関	内務省（DIA）（IT に関するもの）	各省庁の費用削減、サプライヤーとの関与の在り方の改善、調達方法の標準化、政府・サプライヤー双方のサービス品質の向上	

表 2-1 のように、包括契約は取り扱う品目群（IT 製品・サービス、クラウドサービス、人材）及び適用対象となる機関（政府、自治体）によっていくつかのバリエーションが見られる。包括契約に関する各国の枠組みを、どのような品目を取り扱っているかという観点から分類すると、図 2-1 のようになる。

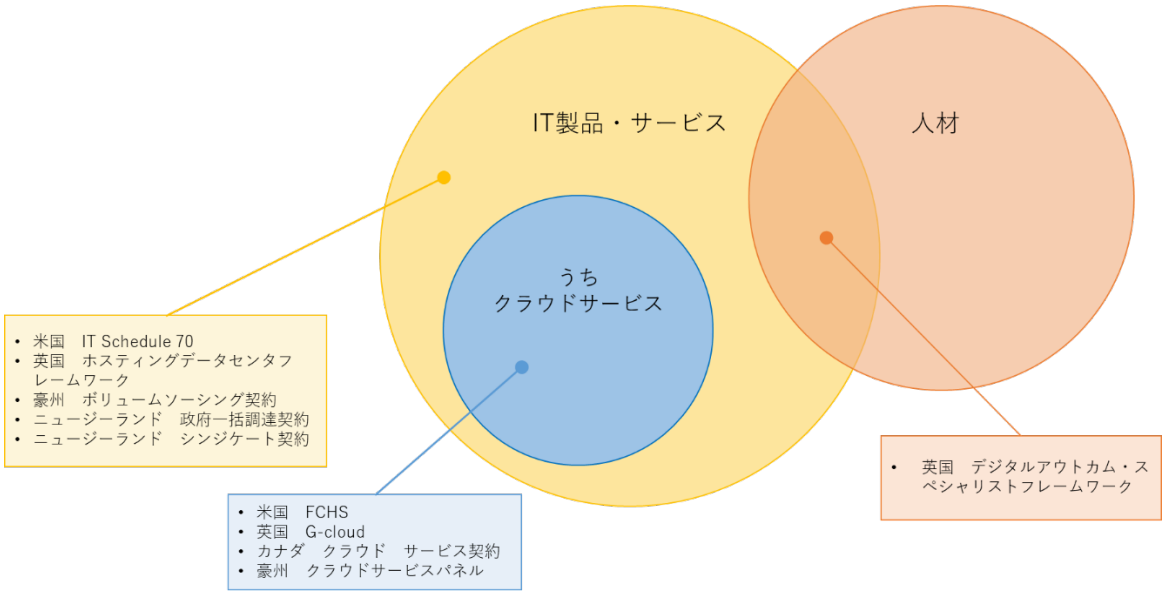


図 2-1　取り扱う品目群から見た包括契約の分類

また、適用対象となる機関が政府のみであるか、政府に加えて自治体も含む契約であるかという観点から分類すると、図 2-2 のようになる。

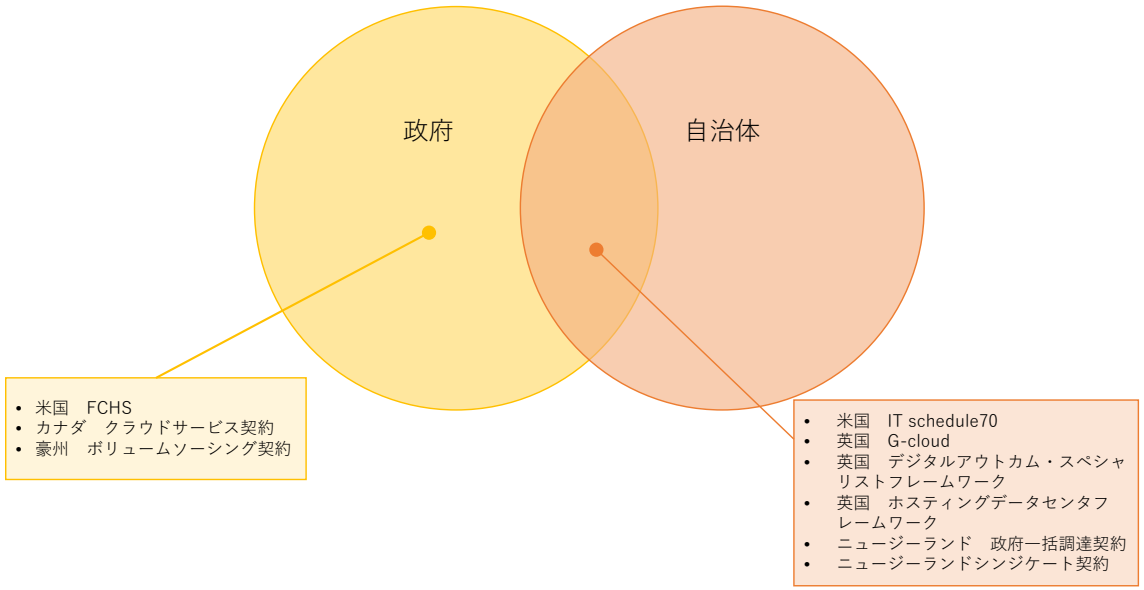


図 2-2　対象機関から見た包括契約の分類

表 2-1 で整理した包括契約の多くは各国の基本的な調達・契約制度の一つであり、必ずしもクラウドを含むIT製品・サービスに特化した枠組みではない。そうした中、米国のIT Schedule 70 や英国の G-Cloud フレームワークのように、IT に特化したものも存在する。また、カナダの SSC 機密／非機密クラウドサービス契約のように、クラウドサービスに特化した枠組みも存在している。

米国の GSA、英国の CCS、カナダの SSC のように、政府機関が利用する施設、物品、サービスの調達や管理を所掌する省庁が、契約条件の設定やサプライヤーとの交渉、契約を実施している例が多い。また、このカテゴリーの契約は、次節で紹介する、サプライヤーと政府機関との間の様々な IT 製品・サービス、及び関連するサービス等を扱う、デジタル上の取引市場であるマーケットプレイス等とセットになっていることが多い。包括契約を締結することによって、事業者はマーケットプレイス等に出品することが可能になり、実際に各政府機関が調達を行う際には、サプライヤーと個別契約（Call-Off）を締結するというプロセスが採られている。具体例として、英国における包括契約とマーケットプレイスの関係性を整理すると図 2-3 のとおりとなる。

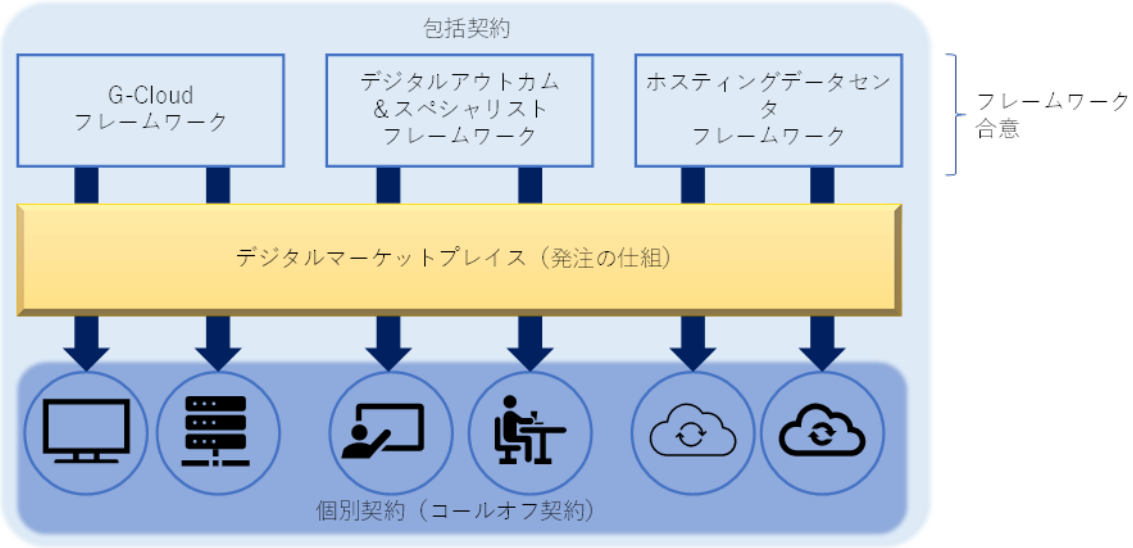


図 2-3　包括契約とマーケットプレイスを通じた個別契約との関係（英国の例）

2.3.　マーケットプレイス

マーケットプレイスとは、サプライヤーが製品やサービスに関する価格その他の提供条件をデジタル上の取引市場に提示し、発注者である行政機関がニーズに合う製品やサービスを検索して発注する仕組みである。本調査研究では、米国の GSA eLibrary、英国の Digital Marketplace、カナダの Cloud Brokering Service、豪州の ICT Procurement Portal 及び Digital Marketplace、並びにニュージーランドの The Marketplace を対象に調査を行った。

各国政府がマーケットプレイスを整備する目的としては、製品やサービスに関する多様なニーズへの対応、サプライヤーと行政機関との効果的、効率的な協働、及び行政機関が提供するサービスに係るコストの低減と質の向上といった点が掲げられている。また、マ

ーケットプレイスの活用によって、多様なサプライヤー／サービスへのアクセスによる選択肢の拡大、サービスの効率的な調達によるコストと調達サイクルの短縮、革新的かつ最新の技術へアクセスする機会の確保といった点も便益となり得る。

今回調査対象とした各国のマーケットプレイスについて、主管組織、目的、対象製品・サービス及び個別購買者の裁量の度合いを軸に整理したのが表 2-2 である。なお、同表の(D)個別購買者の裁量の度合いとは、基本的な契約／アグリーメントの縛りが弱く個別購買者の裁量が広く残されているか、又は基本的な契約／アグリーメントの縛りが強く個別購買者の裁量が狭いかを表すものである。

表 2-2　各国のマーケットプレイスの概要

国	名称	(A) 主管組織	(B) 目的	(C) 対象となる製品・サービス	(D) 個別購買者の裁量の度合い
米国	GSA eLibrary	一般調達庁（GSA）	コスト、質、サービスにおけるベストバリューの達成	Schedule（2 章）の対象全て	広い
英国	Digital Marketplace	クラウン・コマーシャル・サービス（CCS）	中小事業者の政府市場への参入機会の開放	クラウド、デジタルアウトカム、データセンター等	狭い
カナダ	Cloud Brokering Service	シェアードサービス・カナダ（SSC）	セルフサービスモデルの構築、新たな技術へのアクセス確保	クラウド	狭い
豪州	ICT Procurement Portal	デジタル変革庁（DTA）	政府とあらゆる規模の事業者、専門家との取引のハードルの低減による協働の促進	クラウド、IT 製品・サービス、データセンター等	狭い
	Digital Marketplace	デジタル変革庁（DTA）		IT 製品・サービス、SI、研修等	狭い
NZ	The Marketplace	ビジネス・イノベーション・雇用省（MBIE）及び内務省（DIA）	調達及びセキュリティアシュアランスの簡素化、省庁の選択肢の拡大、イノベーションへのアクセス、調達の時間及びコストの低減、省庁及びサプライヤーのセキュリティの確保	SaaS、マネージドサービス、コンサル等プロフェッショナルサービス	狭い

各国のマーケットプレイスは、米国 GSA や英国 CCS など、政府内で調達若しくはデジタル化を所掌する省庁が基本的な契約を締結してサプライヤーにマーケットプレイスに物品やサービスを出品させ、実際の購入にあたっては購買者がサプライヤーと個別契約を締結するという基本的な仕組みは共通している。しかし、マーケットプレイスに出品するための基本的な契約の効力の強さ、若しくは個別購買者の裁量の大きさには、以下のように違いが見られる。

- 米国は基本的な条件が定められている項目が少ないか、若しくは多かったとしても個別購買者の裁量により変更可能な部分がかなり残されている
- 英国、カナダ、豪州、及びニュージーランドは基本的な契約で価格などの基本的条件が大部分の項目について決められており、個別購買者がこれらの条件を変更する裁量の余地は小さい。

2.4. 技術的対話

本節では、契約に至る過程で行政と事業者が対話や交渉を行う調達プロセスである技術的対話に関して、各国の事例を紹介する。具体的には、米国の交渉による契約、英国の競争的対話及び交渉付き競争的手続き、カナダの競争的対話及び交渉付き競争的手続き、豪州の競争的対話及び評価過程における交渉、並びにニュージーランドの競争的対話を対象として取り上げる。

技術的対話の目的は、調達を行う際の課題の明確化、調達主体のニーズを満たす革新的なソリューションの発見、大規模かつ複雑な案件の調達に係る時間の短縮、アウトカムの質及びVfM（Value for Money）の向上、中小企業の参入促進などが挙げられる。

今回調査対象とした各国の技術的対話について、目的、適用条件、及び特徴を整理すると表2-3のとおりとなる。

表2-3　各国の技術的対話の概要

国	名称	目的	適用条件	特徴
米国	交渉による契約	中小企業の参入を促進しつつ、GSA及び各省庁のミッションを達成するための適切なソリューションを探索	• 簡易調達下限値（SAT）を超える場合 • 封印入札が適当でない場合 • FAR Subpart 13.5に規定される特定商用品のための簡易手続きが適用できない場合	• 仕様確定前の対話、提案のプレゼン、提案の改善のための対話等様々な対話が可能
英国	競争的対話	アウトカムの質の向上	• ニーズが既存のソリューションの改修なしには満たされない場合 • ニーズが新たな設計を要したり、イノベーティブなソリューションを促す場合 • ニーズの性格、複雑性、法的・財務的問題に関連する特別な事情やリスクによって事前の交渉なしに発注することができない場合 • 政府機関が技術的仕様を充分正確に策定できない場合	• 政府機関は、その要求を満たすことができる1つ以上のソリューションを確定できるまで対話を継続し、その後入札を実施する。入札では変更や交渉はなされない。（ただし、説明のための対話は可能）
	交渉付き競争的手続き	調達手続きにおける柔軟性の向上、契約する機関が自らのニーズを満たす方法を知らない場合の革新的なソリューションの発見、国際的な取引の拡大	• 調達する財やサービスの性格や複雑性により、事前の交渉を行わずに交渉契約を締結することが困難な場合	• 政府機関の招請を受けたサプライヤーが交渉のベースになる初期提案を提出することができ、その提案内容を改善するために、調達機関はサプライヤーと交渉を行う。 • 入札の最低要件と選定基準は交渉の対象ではない

国	名称	目的	適用条件	• 特徴
カナダ	競争的対話	革新的なアイディアの創出、ニーズを満たすようなソリューションの発見	不明	• 新しいソリューションに対する要求仕様を策定するために実施する個々のサプライヤーと個別協議
	交渉付き競争的手続き	複合的なニーズを満たすような革新的なソリューションの発見	• 市場にイノベーティブなソリューションが存在する場合 • 要求にある程度の柔軟性があり、販売者と購買者の間で交渉が可能な場合	• RFP に対する提案を、必須要件や本調達によってもたらされる付加価値に基づいた評価基準(value-based evaluation criteria) に照らして評価してサプライヤーを選定し、個々のサプライヤーと個別に交渉を行う
豪州	競争的対話	複雑・大規模な案件の調達にかかる時間の短縮	不明	• RFP の前に、政府機関のニーズや案件に関心のあるサプライヤーの技術、価格等に関して双方の理解を深めるための対話。正式な提案の前の仮提案の改善も実施
	評価過程における交渉	VfM の向上のための広範な機会の探索、調達を行う際の課題の明確化	• 政府機関が事前に交渉を行う意思を明示した場合 • 評価基準に照らして明らかに優れている提案がない場合（ビクトリア州政府）	• 提案が要求を満たしていない部分の改善等を求めるための対話
NZ	競争的対話	革新的なソリューションの発見	• 調達が複雑若しくは一般的でなく、調達対象としての特定のソリューションや、政府機関が調達した財若しくはサービスの確立した市場が存在しない場合 • 政府機関が、見込みサプライヤーとソリューションに関して協議することなしに要求仕様を記述することができない場合 • 政府機関が、財務的又は法的観点からどのように調達すべきなのか不明な場合 • インフラプロジェクトや、IT プロジェクト、PPP や PFI スキームのような複雑な調達の場合 （以上は条件ではなく、有効なケースとして示されているものである。）	• 要求仕様を固めるために政府機関が選択したサプライヤーと個別に行う対話（入札への参加招請を行うのは競争的対話に参加したサプライヤー）

表中の各国の事例のうち、特に適用条件に注目すると、競争的対話は、仕様を確定する前に対話を行うフェーズと、仕様確定後に提案をより仕様に適合させることを目的に提案

の改善のために対話を行うフェーズの 2 つに大別される。米国は両方を統合して 1 つの仕組みとしている一方、それ以外の国ではフェーズを分けて別の仕組みとして整備している（ただし、ニュージーランドにおいては、後半のフェーズに関する仕組みは確認できなかった）。我が国では「情報システムに係る新たな調達・契約方法に関する試行運用のための骨子」（2019（令和元）年 5 月 29 日 CIO 連絡会議決定）において、2 つの調達方法が想定されている。１つ目の方法は、発注者が技術提案要領を作成し、応札意思のある事業者からの技術提案を基に技術点による評価を行い、価格との総合点によって落札業者を決定する方式である、一般競争（総合評価落札方式）が想定されている。2 つ目の方法として、発注者が調達の概要となる書類を作成し、公募公告した上で、提案意思のある事業者からの技術提案書を基に提案内容と価格について、技術的対話等を行い、最も優れた技術提案書を提示した事業者を優先交渉権者として、最終の技術的対話等を行った上で事業者を決定する方式である、企画競争方式が想定されている。

これらの方式を上述した海外政府の調達枠組みとの関連で位置付けると、前者は米国以外の各国で実施されている「競争的対話（Competitive Negotiations）」に、後者は英国やカナダにおける交渉付き競争手続き（Competitive Procedure with Negotiations）」に相当する。したがって、我が国における競争的対話は両フェーズを合わせた米国の競争的対話と同じ範囲を指していると言える（図 2-4 参照）。

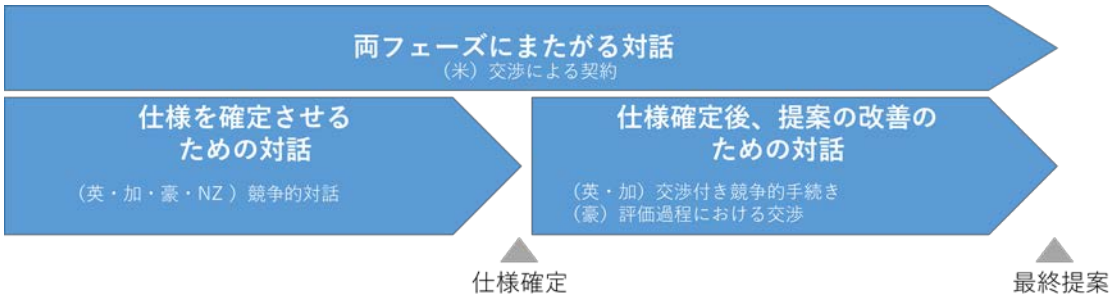


図 2-4　競争的対話のフェーズ

2.5.　単一省庁におけるパブリック・クラウド調達事例：米国国防総省

2.2.で示した包括契約には当たらないものの、パブリック・クラウドの大規模な一括調達事例として、米国国防総省（DOD）の取組の概要を解説する。

2009 年に連邦クラウド・コンピューティング・イニシアティブ（Federal Cloud Computing Initiative、FCCI）が開始されて以来、DOD を含む連邦政府は、物理的 IT インフラへの投資抑制を目的として、「クラウド・ファースト」などの戦略を通じて、IT ニーズのクラウドベース・サービスへの移行に積極的に取り組んできた。2017 年 9 月に、DOD 近代化の取組として、エンタープライズ・クラウドサービスソリューションの採用の加速を求める覚書を発行した。この取組の一環として、DOD はクラウドサービスソリューションを、Joint Enterprise Defense Infrastructure （JEDI）クラウドプログラムを通じて調達しようとした。この JEDI クラウド契約を通じて、DOD は「完全かつオープン（Full and Open）な競争」を実施し、アイテム（すなわち IaaS 及び PaaS）調達を、一社との不定納期／不定数量（Indefinite Delivery/Indefinite Quantity （ID/IQ））の企業固定価格契約（Firm-fixed price contract）として実現することを目指した。

その後、DOD は 2019 年 2 月にクラウド戦略を公開し、組織全体でクラウドコンピューティングサービスを採用する必要性を優先事項とし、「マルチクラウド、マルチベンダー …汎用クラウドと[複数の]目的に適合した」クラウドで構成されるエコシステム」を目指す方向性を示し、JEDI クラウド調達プログラムを推進している（図 2-5 参照）。

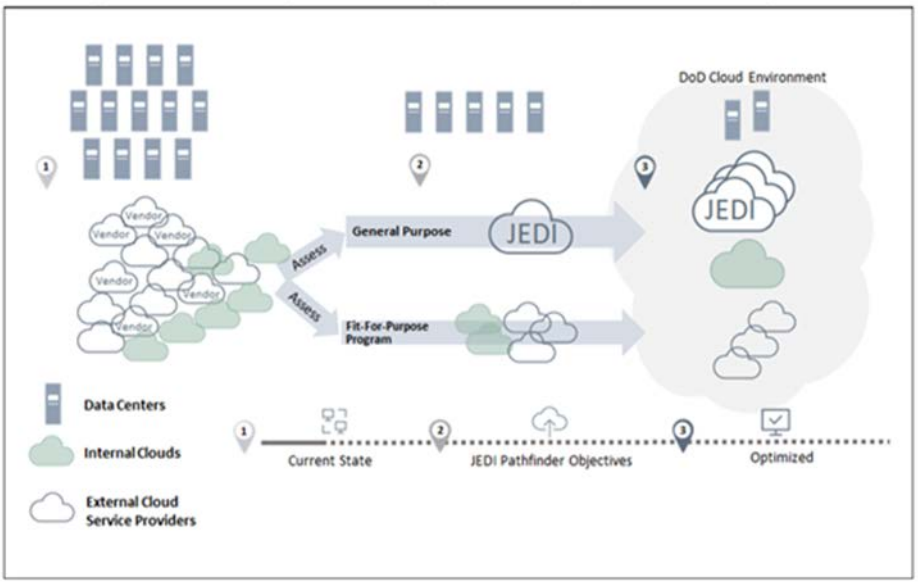


図 2-5　DOD クラウドエコシステム構築の道筋

出典：Congressional Research Service（CRS）

以上見てきたように、JEDI は大規模な一括調達であるものの、その仕組み自体は通常のパブリック・クラウドの調達と変わるものではなく、2.2.で解説した包括契約とは異なると考えられる。

3. 諸外国におけるパブリック・クラウド調達・契約の実際

3.1. 調査手順

パブリック・クラウドの先行国である米国、英国、カナダにおける表 3-1 に示す各国政府機関に対しヒアリングを行った。

表 3-1 海外ヒアリング実施先

国	ヒアリング先	実施形式	実施日時（日本時間）
米国	U.S. General Services Administration (GSA) Skip Jentch 氏 IT Specialist - Enterprise Architect IT Cloud products Manager Office of Information Technology Category (ITC) Federal Acquisition Service (FAS)	WEB 会議	2020 年 3 月 5 日（木） 8:00～9:00
英国	Crown Commercial Service (CCS) Patrick Nolan 氏 （Director - Digital Futures） Herman Nel 氏 （Commercial Agreements Manager - G-Cloud）	WEB 会議	2020 年 2 月 27 日（木） 18:30～19:45
カナダ	Enterprise Strategic Planning Office of the Chief Information Officer of Canada Dan Cooper 氏 (Senior Director - Enterprise Technology)	書面ヒアリング	2020 年 3 月 10 日（火） ※書面回答受領日

3.2. 調査項目

海外ヒアリング調査は、表 3-2 の質問項目を中心に行った。質問の観点として、契約方法、職員の専門性、責任範囲、利用規約・約款、PoC の実施、支払いサイクル、立入監査といった内容が含まれる。

表 3-2　調査項目一覧

項目	質問
契約方法	パブリック・クラウドの契約方法として、“CSP との直接契約”と“SIer 等を介在させた CSP との間接契約”をどのように使い分けているか。
職員の専門性	直接契約に際して、行政職員にキャッチアップさせている知識・スキルには何があるか。また、キャッチアップはどうやって行っているか。
責任範囲	間接契約の場合、CSP と SIer の責任分界点をどのように決めているのか。また、責任分界点の考慮漏れが生じた場合、どのような方法で対処しているのか。
利用規約、約款	政府と CSP はどのように利用条件に合意しているか。
PoC の実施	パブリック・クラウドの利用を検討するにあたって、PoC（Proof of Concept）や試用を行った上で、利用判断を行っているか。
支払いサイクル	パブリック・クラウドのサービス料は、月ごとに支払っているか。月ごとに支払いをするために支払代行業者を間に入れたりしているか。
立入監査	パブリック・クラウドに対する監査はどのように行っているか。

3.3.　調査結果

ヒアリング先から入手した、パブリック・クラウドを導入する現場の実情、課題、及び制度の運用実態に関する情報を以下のとおり整理した。

3.3.1. 米国（GSA）

米国連邦政府は、各政府機関がそれぞれ調達を行っており、クラウドサービスもこの中に含まれる。GSA の役割は、こうした状況の中で契約の合理化を図るための各政府機関に対する支援を行うことである。

表 3-3　米国 GSA ヒアリング結果

項目	回答内容
契約方法	• 基本的にほとんどの政府機関は CSP と直接契約を結ばず、間に SIer やリセラーが入って契約する。クラウド導入後 5 年から 7 年たって、最初の段階で締結された契約を更新する時期になっており、各政府機関は、更新にあたって、旧来の契約でよかったのか、新たに契約しなおす必要があるのか検討している。 • CSP 一社ではなく、いくつかの CSP を利用できるリセラーが求められている。各 CSP がもっている技術メニューは異なるので、政府機関の IT 調達担当者は複数の選択肢が確保できることを求めている。 • 各政府機関は、管理的な部分、すなわち請求やインボイスに関してはリセラーや SIer に委ねる。そのような間接的な部分と、実際に各政府機関が CSP のネイティブでオーガニックなポータルにアクセスするところは分けている。クラウドの実際の利用量やマシンの提供（プロヴィジョン）については、クラウドのポータルに直接アクセスして確認している。

項目	回答内容
職員の専門性	• 今でも IT スキルのある優良な行政職員を見つけるのは困難である。クラウドのアーキテクチャーも扱えるレベルとなると、なおさら人材を見つけるのは難しくなる。政府機関はクラウドに移行しつつあるので、IT の専門職についている人の職務記述書（ジョブディスクリプション）の中身も変わってきている。したがってトレーニングは重要である。 • GSA として各政府機関に推奨しているのは、大学が若い IT ワーカーに提供するような研修ではなく、主要な CSP が提供しているカテゴリーごとの資格認定プログラムを受講することである。自社のサービスを使ってほしいという思いもあり、主要な CSP のプログラムは無償で受講できるというメリットもある。
利用規約・約款	• 各政府機関は単独で CSP と利用条件を交渉する立場にない。各 CSP は独自の利用条件を提示するが、市場環境により、CSP が提示する条件はそもそもフェアなものになっているので、どの政府機関が使っても大丈夫だという状況になっている。
PoC の実施	• クラウドの特徴は柔軟性に富みアジャイルであり、新しいものが次々に入ってくる。まずは実験をしてみるということを重視する。
支払い	• こういう内容でこのくらいの工数を要したという、ネイティブでオーガニックな、透明性のある明細が求められている • 会計担当者は好ましい FFP（Firm Fixed Price、確定固定金額）での契約を利用できる。私が今でも CIO だったら、この手段を選ぶ。コンピューティングのニーズを見て、それを確保したインスタンスを購入してしまう。コンピュータのニーズの大半を FFP で買ってしまい、わずかな部分を T&M（タイム＆マテリアル）方式にて市場価格でスポット買いをする。 • スターバックスのカードのように、例えば 1000 ドルという固定価格でクラウド側の提供するギフトカードを買い、クラウドコンピューティングを使う。固定価格でカードを買い、請求が発生する場面では使った分だけ支払う T&M のような形になっている。確かではないが、このギフトカードストラテジーは、CSP ではなく主にリセラーが提供しているものである。なお、こうしたスキームは必ずしも明示された会計ルールに則ったものであるとは限らない。
立入監査	• CSP はセキュリティを重視している意識が高いので、こちらから立入監査をしたいといっても許容しない。 • FedRAMP（米国政府が調達するクラウドサービスの基準が定められた認証プログラム）の認定、資格を持った人には CSP はそのファシリティへの立入を許可するという仕組みができている。CSP が立入監査を許容するのは、このセキュリティに関してのみ。 • 第三者評価機関（3PAO、Third Party Assessment Organization）が FedRAMP で使われている正しい用語であり、その機能は監査人と同じである。

なお、以下はヒアリング後に GSA から提供のあった補足情報である。

表 3-4　米国 GSA からの入手資料

項目	回答内容
GSA クラウドチームの役割	• 無料市場調査（M-RAS）の実施（省庁がアンケートに記入し、GSA が省庁に代わって RFI を発行する。） • 無料のクラウド調達戦略ガイダンス • Cloud に関する RFI、RFP 等の無料レビュー • GSA クラウドインフォメーションセンター（CIC）のコンテンツモデレーター
クラウドへの移行理由	• より少ない費用で、より多くのことを実施する • 過剰/過少購入のインセンティブとリスクを排除 • 大規模なデータ要件への対応 • セキュリティ対応（より安価でより高頻度の自動更新とパッチ） • 俊敏性/生産性（ボタンを押すだけでサーバの数やタイプを変更可能） • クラウドファーストイニシアチブ等の政府施策
クラウド移行に係る実現可能なアプローチ	• 小さいが俊敏性を求められる開発及びテスト環境 • 可能であれば、すべての新しいアプリをクラウドに構築。これらのアプリのライフサイクルは、すでにクラウド用に最適化されている • 反復実装 • 実装期間が短いアプリや利用期間が短いアプリでの適性の検査 • 古くなったサーバをクラウドアーキテクチャに置き換える。次の技術的な更新サイクルは、クラウド環境に移行する良い機会
セキュリティ対応	• 機密性、可用性、完全性については、FISMA、NIST 等のベースラインが引き続き適用される。FISMA High は現在 FedRAMP でカバー
データ所有権	• クラウドに格納した者がそのデータを所有する
ベンダー又はテクノロジーロックイン	• 契約は、通常、いつでも解約可能。省庁は、オンプレミスシステムの場合と同様、テクノロジーロックインに対して予防策を講じる必要がある
人材スキル	• クラウド環境でも、IT 組織が依然として必要。IT スタッフは、残存するオンプレミスインフラストラクチャコンポーネントの管理を継続しながら、クラウドアプリケーションの開発、展開、及び管理に集中
契約面	• 複数の CSP を扱うリセラーを相手にすることを検討すべきである
クラウドセキュリティ：FedRAMP	• 行政部門や省庁は、クラウドサービスのセキュリティ認可を作成するときに FedRAMP のセキュリティ要件を使用するよう OMB から義務付けられている • FedRAMP クラウドセキュリティコントロールは NIST ベースラインに追加されている • CSP の詳細なセキュリティドキュメントを確認したい省庁は、FedRAMP.gov からリクエストフォームをダウンロードして、記入済みのフォームを info@FedRAMP.gov に提出できる

3.3.2. 英国（CCS）

パブリックセクターのクラウド調達は、長期にわたって契約を行う可能性のある事業者との間で、契約条件や契約額の決定方法などの契約締結に関する枠組みに関して合意するフレームワーク・アグリーメントによって共通の調達条件を定め、サプライヤーを管理している。サプライヤーのタームズ・アンド・コンディション（条件）は、フレームワーク・アグリーメントによって管理されている点が特徴である。

表 3-5　英国 CCS ヒアリング結果

項目	回答内容
契約方法	• 顧客である政府機関とサプライヤーの間には3つの関係がある。1つ目は、政府機関が、CSP とサプライヤーとして直接契約するという形態である。これは、G-cloud フレームワークの対象になる。2つ目は、政府機関が SIer と契約する形である。これは、SIer 若しくは SIer のタームズ・アンド・コンディションということになる。3 つ目は、政府機関がリセラーと契約する形である • SIer は包括的な付加価値サービスを提供するということになっている。CSP にプラスして、例えばクラウドポータルコンソール等である。通常 CSP が提供するものだが、SIer の規模が十分に大きい場合は、クラウドポータルコンソールを提供し、CSP との間のゲートウェイという形で機能する • リセラーはどちらかというと、SIer に比べると責任も少なく、提供するものに機能的なものも少ない。仲介者、エージェントという形になる場合が多い。そこで CSP のタームズ・アンド・コンディションで直接的な関係を構築して、追加サービスをすることもある • SIer の方が多くのサービスを提供するので、中央政府が様々な CSP と契約している場合は、シングル・ビューでアクセスしたいという要望がある。その場合はリセラーではなく Sier との契約になることが多い。一方、リセラーは小さなプロジェクトを短期的に早く取引する場合に用いられる。さらに、リセラーは中小・中堅企業を対象にする場合が多い
職員の専門性	• 英国政府は契約管理をコンセプトにしているので、コントラクトマネジメントに集中しており、正当なコースを提供している。契約管理は、このコンセプトに基づきトレーニングを行っているが、クラウドサービスに関しても、例えば公共関連の政府職員や CCS の職員が集まり、実践的なトレーニング、ナレッジの共有、カンファレンス、セミナーが 70%くらいを占める • ほとんどの組織において、大半のトレーニングが現場指導力育成プログラム（OJT）で、同僚や経験のある先輩のレクチャーや実践から学ぶということになっている。残りの 15～20%くらいがオンラインでのフォーマルな教育、５%くらいがいわゆる座学のような形で行うのが通常のやり方になっている
責任範囲	• サプライヤーが直接契約か間接契約かに関係なく、どのような責任範囲か契約で定義することを期待することが前提となっている。つまり、関係性が重要であり、ビジネスニーズを理解していくことが重要になる。必ずしも契約上の関係ではない

項目	回答内容
PoC の実施	• PoC は、バイヤーに対してマーケットプレイスで無償トライアルをしているものを推奨している。PoC に関して２つのタイプがあると考えている。１つ目はセールス・マーケティング目的のものである。CSP が、お客様や潜在顧客に対して無償の容量を提供して使っていただくプロモーションのようなものである。２つ目は実証実験のテスト検証である
支払い	• クラウドサービスやクラウドホスティングなど、ほとんどのケースが月次払いになっている。将来的に、これらの利用が頻繁になると、もっと色々とコモディティ化されると思う • 現状は、クラウドプロジェクトによってケースバイケースで違う。SIer が戦略的に関わる場合は、決済の仕方等がボリュームによって違う
立入監査	• 我々の要件が満たされているか、という意味で確認の監査はしている。ただ、大半の監査において、現地に行くということはない。その組織の中のシニアオフィサーレベルの人に、エビデンスやサポートドキュメント、ステートメントを出してもらうようにしている

3.3.3. カナダ（政府 CIO 室）

カナダでは、政府クラウド（Government of Canada Cloud）において、データと情報の安全性を確保し、整然とした安全なクラウドへの移行を保証する一連のガイドラインを作成している。

表 3-6　カナダ政府 CIO 室へのヒアリング結果

項目	回答内容
契約方法	• クラウドサービスの調達を集中管理するクラウドブローカーを設立したうえで、適格な CSP を選択するための競争入札を導入している
職員の専門性	• 公務員の研修は各部署に一任で、部門は、従業員のニーズを満たすトレーニングを選択する • Canada School of Public Service は、デジタルアカデミーを通じてより近代的なオプションを提供するためにコンテンツを強化している
責任範囲	• カナダ政府セキュリティコントロールに基づいて様々な CSP セキュリティインフラを評価し、競争力のあるプロセスを通じてカナダ政府セキュリティコントロールに適合する CSP を選択している
PoC の実施	• 小規模から始めて、迅速に移行することが重要
支払い	• 政府部門は、標準又はクレジットカードを含む支払い方法の組み合わせ、さまざまな請求方法、又は請求書の金額に応じた両方の組み合わせを使用している
立入監査	• CSP のオンサイト監査を実施し、情報技術、データ、情報リソースを保護するために必要なカナダ政府セキュリティコントロールに準拠していることを確認。また、CSP が ISO 27001、27017、27018、SOC-2 の国際認証を維持していることにも注意を払った

3.3.4. まとめ

海外ヒアリングから得られた各項目の要点を整理すると表 3-7 のとおりである。

表 3-7　海外政府機関へのヒアリング結果（まとめ）

項目	ポイント
契約方式	• 大きく分けて、CSP との直接契約を結ぶ方式、及び SIer 又はリセラーとの契約を介して CSP のサービスを利用する方式（間接契約）があり、プロジェクトの性質、行政機関のスキル・能力等に応じて使い分けを行っている
職員の専門性	• 職員がクラウドサービスを利用する際のニーズを踏まえた形で、実践的なトレーニングや情報共有を行っている。その多くは、間接契約であっても必要とされる知識・スキルを提供するものである。トレーニングは政府機関が自ら行う場合に加えて、CSP が提供している研修コースを活用するという方法を採る場合もある
責任範囲	• CSP は、顧客無差別に適用される約款ないし利用規約の範囲でしか責任を負わず、行政機関側もそれを受容している
利用規約・約款	• CSP の利用規約や約款については、市場を通じて内容の公正さが一定程度担保されているとの判断に加え、フレームワーク合意を行うことで行政機関によって受容されている
PoC の実施	• 小規模に実証実験からスモールスタートすることが各国共通して重視されており、その一環として PoC が行われている
支払い	• CSP との契約では、従量課金やリザーブドインスタンス料金など、CSP が無差別にに提供する支払い方式が適用されるのが基本。その上で、間接契約を活用することで、FFP（Firm Fixed Price、確定固定金額）と T&M 方式の組み合わせなど、複数の支払い方式の組み合わせも含めた、多様な支払い方式が利用されている
立入監査	• 行政職員が現地のデータセンターに立入監査を実際に行うことは通常なく、第三者監査の枠組みを活用しつつ、エビデンスやサポートドキュメント、ステートメントの提出をもって代替することが多い。ただし、本社ビルなどへの監査は行われるし、立入検査の権限を放棄しているわけでもない

4. パブリック・クラウド活用に向けた課題及び解決策

4.1. 有識者ヒアリング

4.1.1. 実施手順

我が国の行政機関におけるパブリック・クラウド活用に向けた課題及び対応策についての示唆を得ることを目的として、クラウドサービス導入に関する制度と実務に精通した表 4-1 に示す専門家に対し、表 4-2 に示す調査項目を中心にヒアリングを実施した。

表 4-1　国内ヒアリング実施先

種別	ヒアリング先	実施形式	実施日時
政府	満塩尚史　経済産業省 CIO 補佐官	Web 会議	2020 年 4 月 7 日（火） 15:00～17:00
地方公共団体	市瀬 英夫　（前静岡県 CIO 補佐官、総務省地域情報化アドバイザー、J-LIS 自治体クラウド支援アドバイザー）	Web 会議	2020 年 4 月 13 日（月） 14:00～15:30

表 4-2　調査項目一覧

- 財政当局（主に予算要求）、情報システム部門、原課、ユーザ部門におけるパブリック・クラウド調達への理解の現状、理解の壁を破るための方策
- パブリック・クラウド導入の先進事例や参考となる取組
- CSP に対する立入監査の扱い
- 人材の継続的確保、育成の課題や取組のあり方

4.1.2. 有識者

① 満塩　尚史氏（経済産業省 CIO 補佐官）

満塩氏からは、クラウドで取り扱う情報への正しい理解、契約形態、職員がクラウドを理解し習熟するための取組、セキュリティ対策に関して、表 4-3 に示す指摘を得た。

表 4-3　ヒアリング結果概要（満塩氏）

項目	回答内容
理解の壁を打ち破る方策	• クラウド導入に関しては、職員の導入に対する心理的抵抗よりもむしろクラウドを正しく理解できるかが重要である。情報格付けに関する正しい認識によって、クラウドの理解を進めていく必要がある。政府のクラウドの利活用方針では、クラウド化の対象外である特定秘密と極秘文書は既にリストになっているが、それらに該当していないにもかかわらず、クラウドを使えないと懸念する場合がある • 従来はデータセンターが止まってもレポートはすぐには上がってこなかったが、クラウドの場合 CSP によるレポート、ログ機能がむしろ充実し、かつ対応もリアルタイムに把握できる
参考となる事例、取組	• セキュリティ対策については、安全性評価で問題ないとしてもそのまま使用するのではなく、必要な場合は、セキュリティ機能を追加で入れることを推奨している • 最近はクラウド導入を推進する組織として COE（Center of Excellence）を設け、COE が中心となってプロジェクトを評価し進めることでプロジェクトが成功するケースが目立つ
契約形態	• 契約期間は月単位、年単位など、多様な期間が存在する • 契約は必ずしも CSP との直接契約とは限らない。米国など諸外国ではリセラーが間に入っての間接契約も行われており、これらの契約形態について理解を深める必要がある
立入監査	• 一般的に、立ち入りしたからと言ってデータそのものを視覚的に認識できるわけではない。データセンターでモノを確認できてもそれ以上わかるわけではない。物理的な立入監査に重きを置くのは賛成できない。データを監査する手法の研究が必要だ • 物理的な立入監査の重要性からは、拠点が国外か国内かは関係ない
人材確保	• 座学ありきでなく、実際に触ることを重視している。クラウド環境をある程度触れる sandbox（試行環境）も必要。豪州ではそのようなプロジェクトを行っているようである。日本でも、現在、職員にノンコーディングツールに触ってもらう取組を進めているところである
その他	• ベンダーロックイン解決方法として、docker コンテナでのシステム構築までいければポータビリティが高い。今も Docker Hub にコンポーネントを公開することを試行している。したがって、システム構築環境として、docker コンテナを想定することが重要である

② 市瀬 英夫氏（前静岡県 CIO 補佐官、現総務省地域情報化アドバイザー及び J-LIS 自治体クラウド支援アドバイザー）

市瀬氏からは、地方公共団体においては、ネットワーク・セキュリティに求められる要求水準の高さがクラウドの利活用拡大に向けたボトルネックとなっているとの基本認識の下、表 4-4 に示す指摘を得た。

表 4-4　ヒアリング結果概要（市瀬氏）

項目	回答内容
三層分離について	• 自治体のシステムは、基幹系（マイナンバー利用事務系）、LGWAN 接続系、インターネット接続系の三層分離になっている。基幹系においては、原則として、他の領域との通信をできないようにすることとされている。また、LGWAN接続系とインターネット接続系は分割し、両システム間で通信する場合には、ウイルスの感染のない無害化通信を図ることとされている • パブリック・クラウドの適応度はインターネット接続系の方が高い。東京都の新型コロナウィルス対策サイトのシステムはオープン系で作り、他でも使われている。これはパブリック・クラウドの成功事例と言えるだろう
課題認識	• 基幹系と LGWAN 接続系の間でネットワークが切れている。プライベートクラウドであっても、個人情報を外に出すことには今でも抵抗感は強い • 一方、基幹系は、レガシー度合いやベンダーロックインも強く、クラウドネイティブ化が難しい。また SIer からすると、運用部分がなくなることで収益が得られなくなるため積極的ではない。さらに、データ保護、データ移行、システム移行のリスクもある • パブリック・クラウドとの親和性が高いインターネット接続系は新規事業になることが多く、財政難の昨今では予算化は相当難しい。一方の基幹系ではインターネットセグメントを活用した新規事業につながることがそもそも少ない
理解の壁を打ち破る方策	• 自治体に横の連携は少なく、「一人情シス」で孤独な状態だ。共同化することによって連携が生まれるのが良いと考えている。周辺がやり始めると自分たちでもやろうという動きになるが、皆で同一社にするとは限らない。兄貴分的な自治体が音頭を取ると周りがついていくことはある。またベンダーが自治体を集めて共同化の勉強会を行っている例もある
参考となる事例、取組	• 新しいもの、いろいろ試しながら作っていくものが、パブリックやアジャイルに向いている
人材確保	• 県や中核都市は、きちんとした仕様書が書けるが、「一人情シス」のところは、積極的にイニシアティブをとることがない。信頼できるベンダーに丸投げだ。むしろ、ローテーションが滞っていると知見が高まる。10 万人以下の自治体では、パブリック・クラウドについては、「そんなものがあるらしい」、「自分たちには関係ない」、といった認識だ。中核都市以上では災害系システムに使ったりするが、お金のある大きな自治体が主である • 県や中核都市では IT 管理と IT 政策の 2 つの担当を持っている。後者は動向をウォッチする任務があるので、パブリック・クラウドのことも理解している • 行政職員は研修には熱心で、J-LIS の研修はよく受けている。ただ、トレーニングだけ受けてもダメで、実際に使ってみる、触ってみることが重要で、課題を持ってワークショップを行ったりする必要がある

4.2. 研究会の開催

行政機関におけるクラウドサービス調達に当事者として取り組む政府及びIT企業からなる研究会を2回にわたり開催した。第1回会合で、パブリック・クラウドサービス活用に当たっての課題の整理を、第2回会合でそれに対する解決策の検討を実施した。

参加者として、政府からはクラウドサービスの政策立案を行う内閣官房情報通信技術（IT）総合戦略室及びクラウドサービスの調達実務を企画する総務省の協力を得た。また、事業者からは当研究所の会員企業のうちクラウドベンダーの売上上位2社及び国内SIerのうち政府の支出額上位4社の計6社の参画を得た。なお、研究会は別途実施した「行政におけるアジャイル型のサービス開発に関する調査研究」の研究会を兼ねる形で開催した。

表4-5　第1回研究会開催概要

開催日時	令和2年1月24日（金）16：30～18：00
開催場所	一般社団法人行政情報システム研究所会議室
主な議題	1.　研究会の趣旨・全体の進め方について 2.　行政におけるクラウドサービス調達に係る課題及び論点について 3.　アジャイル型開発に係る課題及び論点について 4.　先進事例調査の進め方について
参加者 （順不同）	内閣官房IT総合戦略室　参事官補佐　安藤　功一
	総務省行政管理局　企画官　千葉　英之
	日本電気株式会社　第一官公ソリューション事業部　部長　江上　俊夫 同　政策渉外部　部長代理　新井　隆 同　政策渉外部　課長　多田　晴紀
	アマゾンウェブサービスジャパン株式会社　パブリックセクター統括本部長補佐　小木　郁夫 同　パブリックセクター法務部統括　笹沼　穣 同　パブリックセクター技術本部　根本　裕規
	日本マイクロソフト株式会社　パブリックセクター事業本部　デジタル・ガバメント統括本部　荒井　俊貴 同　パブリックセクター事業本部　デジタル・ガバメント統括本部　久保田　朋秀 同　パブリックセクター事業本部　デジタル・ガバメント統括本部　石田　真彩
	株式会社エヌ・ティ・ティ・データ　社会基盤ソリューション事業本部　部長　渡邉靖隆 同　技術革新統括本部　部長　本橋　賢二 同　技術革新統括本部　部長　市川　耕司 同　公共・社会基盤事業推進部　課長　東谷　展誉
	株式会社日立製作所　公共システム事業部　部長　安藤　靖 同　公共システム事業部　センター長　並木　靖 同　公共システム営業統括本部　主任　柳元　真介
	富士通株式会社　政策渉外室　シニアマネージャー　押鐘　快之 同　政策渉外室　曾根　芳康
事務局	一般社団法人行政情報システム研究所
	株式会社NTTデータ経営研究所

表 4-6　第 2 回研究会開催概要

開催日時	令和 2 年 3 月 6 日（金）13：00～15：00
開催場所	霞ケ関ナレッジスクエア（Web 会議拠点）
主な議題	1.　アジャイル型開発に係る解決策の検討 2.　質疑・まとめ 3.　行政におけるクラウドサービス調達に係る解決策の検討 4.　質疑・まとめ
参加者 （順不同）	総務省行政管理局　企画官　千葉　英之
	日本電気株式会社　　第一官公ソリューション事業部　部長　江上　俊夫 同　政策渉外部　部長代理　新井　隆 同　政策渉外部　課長　多田　晴紀
	アマゾンウェブサービスジャパン株式会社　パブリックセクター統括本部長補佐　小木　郁夫 同　パブリックセクター法務部統括　笹沼　穣 同　パブリックセクター技術本部　根本　裕規
	日本マイクロソフト株式会社　パブリックセクター事業本部　デジタル・ガバメント統括本部　荒井　俊貴 同　パブリックセクター事業本部　デジタル・ガバメント統括本部　久保田　朋秀 同　パブリックセクター事業本部　デジタル・ガバメント統括本部　石田　真彩
	株式会社エヌ・ティ・ティ・データ　社会基盤ソリューション事業本部　部長　渡邉　靖隆 同　技術革新統括本部　部長　市川　耕司 同　技術革新統括本部　課長　高津　健 同　公共・社会基盤事業推進部　課長　東谷　展誉
	株式会社日立製作所　公共システム事業部　部長　安藤　靖 同　公共システム事業部　センター長　並木　靖 同　公共システム営業統括本部　主任　柳元　真介
	富士通株式会社　　政策渉外室　シニアマネージャー　押鐘　快之 同　政策渉外室　曾根　芳康 同　クラウドサービス事業本部　部長　出口　雄一
事務局	一般社団法人行政情報システム研究所
	株式会社 NTT データ経営研究所

4.3.　課題の全体像

有識者ヒアリング及び研究会での検討を踏まえ、パブリック・クラウドの活用に向けて、現場職員が認識している課題を表 4-7 の通り整理した。

課題の分類にあたっては、「デジタル・ガバメント推進標準ガイドライン」（各府省情報化統括責任者（ＣＩＯ）連絡会議決定）　第３編　IT マネジメントの章立てを参考としつつ、IT 調達プロセスのうち①サービス・業務企画、②要件定義、③予算要求、④調達、⑤システム監査・立入検査の工程を取り上げた。

なお、課題の整理及び解決策の検討にあたっては、主要な論点に焦点を絞っている。こ

のため、導入形態として、ハイブリッド、マルチクラウドといった応用的な活用方式に係る検討は、実務的には重要になるものの、本調査研究では割愛している。同様に、導入方式として、リフト&シフトといった段階的な移行方式に係る検討も同様に割愛している。また、契約方式に関して、本調査研究では、直接契約／間接契約を次のように位置づけている。

- 直接契約方式：主として海外の大手クラウドサービスプロバイダー（CSP）が、顧客無差別に提供するクラウドサービスに対し、直接発注する方式
- 間接契約方式：CSP のサービスを顧客のニーズに合わせてカスタマイズして再販するリセラーとの間で締結する方式

ただし、国内勢を中心に、パブリック・クラウドサービスでありながら、個別事情に応じてカスタマイズして直接、顧客にサービス提供する事業者も見られる。この場合は、直接契約・間接契約に関する問題は先鋭化されないことから、本調査研究では特に論点としては取り上げないこととする。

表 4-7　課題の全体像

No.	工程	課題	課題の内容
1.1	サービス・業務企画	クラウド導入に対する心理的抵抗	—
1.1.1		クラウド移行に伴うリスクへの懸念・不安・負担感	• データ移行に伴うリスクへの懸念 • 行政職員の漠然とした不安（例：今までできていたことができなくなる） • 新たな知識や業務の習熟への負担感
1.1.2		障害リスク、セキュリティリスクへの懸念	以下のリスクへの懸念 • 障害状況の把握の遅れ • 他企業が障害を起こした際の影響の波及 • 設定ミスによる、機密データへの不正アクセスリスク • 障害発生時の復旧タイミングが不明確
1.1.3		未知の技術への抵抗感・クラウドに対する理解不足	• 未知の技術を受け入れることへの漠然とした（明確な根拠のない）抵抗感 • クラウド自体をイメージアップできない • 「パブリック・クラウド＝SaaS（あるいは IaaS）」といった固定観念、誤解
2.1	要件定義	クラウド導入に対する心理的抵抗	—
2.1.1		イントラネット外でデータを管理することへの不安	• （機密性観点で）中央省庁や地方公共団体がデータを庁外に出すことに伴うリスクへの懸念 • ネットワーク分離のポリシーに抵触することへの不安、ポリシー変更の必要が生じた際の関係部門・機関との調整に係る負担への懸念
2.2		移行形態の判断が困難	• リホスト/リライト/リビルドの判断の難しさ
3.1	予算要求	予算要求のための見積の困難	• 極度額の妥当な見積が（特に導入初年度は）難しく、見積額と実際の支払額の間に大きな乖離が生じるリスクがある • 既存事業者からの見積がクラウドを前提としたものとなっておらず、妥当な見積が困難な場合が多い
4.1	調達	パブリック・クラウドに合った適切な調達区分、契約方法（直接、間接）が分からない	• パブリック・クラウドの利用目的、利用形態を踏まえた調達区分、契約方法の明確な判断基準や検討材料がないため、①調達側がパブリック・クラウドを敬遠する、②適切な調達区分・契約方法を選択できない、③適切な調達仕様・契約内容を規定できない等のリスクがある • 上記のリスクがあるため、慎重な検討や分析が必要となり、作業負荷がかかる
4.1.1		CSP と SIer の責任範囲をどう設定すればよいか分からない	以下の考え方の整理が必要 • パブリック・クラウドとその上位層（アプリケーション等）との責任分界点の明確化 • 問題発生の防止策及び問題発生時の解決方法の整理
4.2		行政機関と CSP 間での支払サイクル/スキームのギャップ	年度ごとの一括精算払いが基本の行政機関の現状と、毎月利用した分だけ請求するという CSP の支払サイクルや取引スキームとのギャップ
4.3		調達におけるベンダーロックインの可能性に対する一般的な懸念	いったん特定の CSP が受注すると、以後の調達でも当該 CSP を使わざるを得なくなるのではないか、という一般的な懸念が（事実かどうかは別として）存在する。 例えば、日本の政府機関でのパブリック・クラウドの導入実績を参加要件とする、市場に１つしかない機能要件を課す、といったことが行われると、先行 CSP には有利に、後発 CSP には不利に働く、等）
5	システム監査・立入検査	CSP に対し、どのようなシステム監査・立入検査を規定すべきかが明確でない	データセンターへの立入検査を原則受け入れない CSP と、契約書上、立入検査の権利を留保してきた公的機関の立場の不一致
6	IT ガバナンス	行政職員側のクラウド利用に係る知識の不足	パブリック・クラウドを選択肢として検討するにあたり、行政職員がパブリック・クラウドに関して身につけるべき知識・スキルが不足している

4.4. 課題分析及び解決の方向性

前節で示した各課題について、研究会での検討を通じて根本原因や制約条件等を分析し、以下のとおり解決の方向性を導出した。

4.4.1. サービス・業務企画

表 4-8　課題分析及び解決の方向性（サービス・業務企画）

No.	工程	課題	分析結果	解決の方向性
1.1	サービス・業務企画	クラウド導入に対する心理的抵抗		—
1.1.1		クラウド移行に伴うリスクへの懸念・不安・負担感	• オープン化の場合にも同様のリスクは存在するものであり、パブリック・クラウド特有のリスクは確認できない • 組織に未知の技術を導入する際に一般的に起きる抵抗感を軽減するための知識付与、実務的負担軽減への手当が必要	• ICT 研修やセキュリティ教育によるリスク、メリット、留意点への理解の向上 • 移行により不利益が生じないことを立証する研究、事業等の実施、事例の蓄積 • 移行の手順のガイド、参考事例の共有による事務的負担の軽減
1.1.2		障害リスク、セキュリティリスクへの懸念	• 障害発生時のメディアの大々的な扱いが影響 • 実態は、オンプレミスやプライベートクラウドよりも障害頻度が高かったり、セキュリティレベルが低かったりするわけではない	• 同上
1.1.3		未知の技術への抵抗感・クラウドに対する理解不足	• 例えば「パブリック・クラウド＝IaaS のみ」といった誤った認識、障害発生時のメディアなどのネガティブな報道が正確な理解を阻害（※上段と同じ）	• 同上 • 実際にクラウドに触れたり、実証したりする機会を作る • クラウドの先進事例や、誤解を解消するための情報発信を積極的に行う

4.4.2. 要件定義

表 4-9　課題分析及び解決の方向性（要件定義）

No.	工程	課題	分析結果	解決の方向性
2.1	要件定義	クラウド導入に対する心理的抵抗		—
2.1.1		イントラネット外でデータを管理することへの不安	• ユーザのパブリック・クラウドに対する知識の不足 • 情報漏洩が起きた場合、調達機関が責任を問われるので踏み切れない、踏み切るだけの強い動機や関係者への説得材料がない • 情報漏洩のリスクを分析・整理しておくことが必要 • ポリシー変更等が必要な場合、関係機関との調整負荷は避けられない	• データの峻別（セキュリティレベル付け）等の諸外国の事例を紹介 • 前例として、判断の参考に供するための事例の蓄積・共有

4.4.3. 予算要求

表 4-10　課題分析及び解決の方向性（予算要求）

No.	工程	課題	分析結果	解決の方向性
3.1	予算要求	予算要求のための見積の困難	• 極度額で見積もるにあたり、導入初年度は妥当な見積が難しいが、パブリック・クラウド特有の問題ではない • 海外政府でもこの課題はきれいに解決できているわけではない • 既存事業者からの見積がクラウドを前提としたものとなっておらず、妥当な見積が困難な場合が多い	• 複数年の運用を通じて見積の精度を高めていく諸外国の事例を紹介する • 初年度の見積のブレの影響を補正するための手段（年度途中での契約変更や上限価格付従量契約等）を検討する • 既存事業者からの見積がクラウドに適した方法で行われるよう、参考となる事例を蓄積・共有する • 技術的対話の実施、複数の事業者からリスク低減策の提案や情報提供を求めること等により、調達仕様書の記載を適正化し、トラブルの原因となるリスクを低減させる

4.4.4. 調達

表 4-11　課題分析及び解決の方向性（調達）

No.	工程	課題	分析結果	解決の方向性
4.1	調達	パブリック・クラウドに合った適切な調達区分、契約方法（直接、間接）が分からない ※本報告書で間接契約とは、CSP のサービスを利用するために CSP 以外の事業者と結ぶ契約をいう	• 以下の理由から、諸外国でも間接契約が大勢を占める。 ① CSP は基本的に個別対応を行っておらず、政府調達手続きにマッチした受注対応は困難 ② 政府職員が IT のプロでない場合、直接パブリック・クラウドを運用するのは知識・スキルの面で困難 ③ 政府が直接パブリック・クラウドを運用するためには、間接契約以上に大きなリソースが必要な場合が多い • （従来は SIer に一括で請負責任を負わせていたが）間接契約とした場合に、CSP と SIer 又はリセラーと発注者の 3 者間の責任分界点をどう設定するか、調達形態に応じて整理しなければならない	• 当面は、間接契約を中心にパブリック・クラウドの利用を推進する • パブリック・クラウドに適した調達区分、契約方法、問題発生の防止策及び問題発生時の解決方法に関するベストプラクティスを蓄積・共有し、前例として参照できるようにする
4.1.1		CSP と SIer の責任範囲をどう設定すればよいか分からない	※上と同じ	※上と同じ
4.2		行政機関と CSP 間での支払サイクル/スキームのギャップ	• 諸外国でも共通の課題があり、試行錯誤を通じて制度整備を進めている • 今のところ間接契約によって、行政機関と CSP の間のギャップを埋める対応が大勢を占める	当面は、間接契約を前提に（将来的には直接契約も視野に入れて）、参考にしながら、よりクラウドの長所を引き出せるような支払方式を模索する
4.3		調達におけるベンダーロックインの可能性に対する一般的な懸念	• クラウド固有のベンダーロックインについては実例を確認できなかった（あくまで今後の可能性） • 海外の事例でも、CSP 特有の要件が問題視されることはなかった • ただし、一般的な懸念が存在する以上、それを払しょくしておくことが望まれる	調達時にデータポータビリティの確保、移行手段の明示を提案として求める。ただし、具体的な記載方法については、事例の蓄積を待つ必要がある

4.4.5. システム監査・立入検査

表 4-12　課題分析及び解決の方向性（システム監査・立入検査）

No.	工程	課題	分析結果	解決の方向性
5	システム監査・立入検査	CSP に対し、どのようなシステム監査・立入検査を規定すべきかが明確でない	• 政府情報システムにおけるクラウドサービスの利用に係る基本方針により、「第三者による認証や各クラウドサービスの提供している監査報告書を利用することが重要」となっている • 諸外国でも CSP のデータセンターに行政職員が監査に入る事例は確認できない • 実務的には、立入検査は本社ビル等に対するものだが、契約上、立入検査の範囲を限定しているわけではない • したがって、データセンターへの立入検査は通常、想定すべきでない一方、パブリック・クラウドのみ契約上の立入検査の範囲を局限する理由もない	• CSP のデータセンターへの行政職員による立入検査は通常意味がないことの理解を拡げる • 調達担当者に対し、ICT 研修やセキュリティ教育を通じて以下を周知する ① システム運用の適正性は、政府の方針に則り、ISMAP や「基本方針」に基づく第三者の認証、監査報告書を利用して担保する ② 契約書に定める立入検査は通常、本社ビル等での支払額の検証など主にビジネス面に関して行う

4.4.6. IT ガバナンス

表 4-13　課題分析及び解決の方向性（IT ガバナンス）

No.	工程	課題	分析結果	解決の方向性
6	IT ガバナンス	行政職員側のクラウド利用に係る知識の不足	• 定期人事異動によりプロが育たない、維持できないという話はクラウドに限った話ではない • 「パブリック・クラウドを利用するにあたって、行政職員が身につけるべき知識・スキル（≒専門性）を組織的に習得する方法」が不明確である点が課題である • 諸外国でも、基本的には、間接契約による運用を的確に遂行できるようにすることを念頭に教育が行われている	間接契約による運用を前提に以下に重点を置いて職員の教育を行う a. クラウドについての基本的理解 b. 調達/契約方式における留意事項 c. 使用量の見積精度向上の方法 d. ハンズオンでのコンソール操作体験 e. セキュリティ担保のための諸制度

4.5. 具体的な解決策

前節で示した解決の方向性に沿って、前章で収集・整理した諸外国の取組事例、及び 4.1 で得られた専門家の示唆を踏まえ、具体的な解決策を整理した。

4.5.1. サービス・業務企画

① クラウド導入に対する心理的抵抗への対応

表 4-14 課題の解決策（サービス・業務企画）

No.	工程	課題（再掲）		課題の内容（再掲）
1.1	サービス・業務企画	クラウド導入に対する心理的抵抗		—
1.1.1			クラウド移行に伴うリスクへの懸念・不安・負担感	• データ移行に伴うリスクへの懸念 • 行政職員の漠然とした不安（例：今までできていたことができなくなる） • 新たな知識や業務の習熟への負担感
1.1.2			障害リスク、セキュリティリスクへの懸念	以下のリスクへの懸念 • 障害状況の把握の遅れ • 他企業が障害を起こした際の影響の波及 • 設定ミスによる、機密データへの不正アクセスリスク • 障害発生時の復旧タイミングが不明確
え			未知の技術への抵抗感・クラウドに対する理解不足	• 未知の技術を受け入れることへの漠然とした（明確な根拠のない）抵抗感 • クラウド自体をイメージアップできない • 「パブリック・クラウド＝SaaS（あるいは IaaS）」といった固定観念、誤解

海外ヒアリング、研究会を踏まえての考察

解決策

① 移行により不利益が生じないことを立証する研究、事業等の実施、事例の蓄積
- 各行政機関内で関係者との間で検討を行う際に役立つエビデンスとなる研究の実施、PoC 的な事業の実施、事例の蓄積・共有を行う

② 移行の手順のガイド、参考事例の共有による事務的負担の軽減
- クラウドに移行する際の実務的な手引きとなるガイドや事例集を共有し、前例として参照できるようにすることで事務負担を軽減する

③ ICT 研修やセキュリティ教育によるリスク、メリット・留意点への理解の向上
- 行政機関における IT 関連研修や情報セキュリティ研修にパブリック・クラウドの基礎知識やメリット・リスク・留意点（クラウドの理解不足による責任分界を巡るトラブルの可能性等）の説明を取り入れる

④ 実際にクラウドに触れたり、実証したりする機会を作る
- クラウドサービスに接したことがない職員に、実際にハンズオンでクラウドサービスを体験することを通じてイメージアップしてもらう
- 実際のシステム導入に着手する前に、少額又はフリートライアルで実証実験環境を構築し、PoC(概念実証)を行う

⑤ クラウドの先進事例や、誤解を解消するための情報発信を積極的に行う
- 政府や自治体の職員向けに、専門誌やウェブサイト等を通じて基本的な知識（責任分界の整理等）や事例紹介等の情報発信を継続的に行う

4.5.2. 要件定義

①　データ移行、システム移行に伴う不安への対応

表 4-15　課題の解決策（要件定義）

No.	工程	課題（再掲）	課題の内容（再掲）
2.1	要件定義	クラウド導入に対する心理的抵抗	
2.1.1		イントラネット外でデータを管理することへの不安	• （機密性観点で）中央省庁や地方公共団体がデータを庁外に出すことに伴うリスクへの懸念 • ネットワーク分離のポリシーに抵触することへの不安、ポリシー変更の必要が生じた際の関係部門・機関との調整に係る負担への懸念

海外ヒアリング、研究会を踏まえての考察

解決策検討の根拠

① 日本ではデータの機密性がレベル１～３に分類されているが、パブリック・クラウドでのデータ管理の是非の判断との紐づけは部分的であり、イントラネット外でデータを管理することへの不安の材料になっているものと思われる。欧米でも同様にレベル１～３の分類があるが、パブリック・クラウドの利用に際して、利用可否を容易に判断できるようになっている。

② 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」において、パブリック・クラウド上で扱わないデータの分類としては、「特定秘密（特定秘密の保護に関する法律（平成 25 年法律第 108 号）第 3 条第 1 項に規定する特定秘密をいう。）」及び「行政文書の管理に関するガイドライン（内閣総理大臣決定。初版平成 23 年 4 月 1 日。）に掲げる秘密文書中極秘文書」に該当する情報が指定されている（＝データの機密性レベルはパブリック・クラウドの利用判断基準ではなく、公的機関での認識齟齬が生じている可能性がある）。これら以外の情報については、機密性レベルにかかわらずクラウドでの取り扱いの是非に係る判断は示されていない。

解決策

① データの峻別（セキュリティレベル付け）等の諸外国の事例を紹介

② 前例として、判断の参考に供するための事例の蓄積・共有
- クラウドサービスで扱っても問題のない情報の事例の蓄積・共有
- 情報システムのパブリック・クラウドへの移行方式について（2019 年 4 月）を参照

4.5.3. 予算要求

① 予算要求の見積精度の向上

表 4-16 課題の解決策（予算要求）

No.	工程	課題（再掲）	課題の内容（再掲）
3.1	予算要求	予算要求のための見積の困難	• 極度額の妥当な見積が（特に導入初年度は）難しく、見積額と実際の支払額の間に大きな乖離が生じるリスクがある • 既存事業者からの見積がクラウドを前提としたものとなっておらず、妥当な見積が困難な場合が多い

海外ヒアリング、研究会を踏まえての考察

解決策検討の根拠

① 欧米諸国においても日本と同様、極度額で見積もっており、パブリック・クラウド導入初年度は妥当な見積は容易ではないと認識しており、見積を精緻化するために専門家の支援を仰ぐなどの対応を行っている機関もある。ただし、基本的には、見積の精度向上にはこだわり過ぎず、まずは極度額で見積もっている。いかにして、2 年目以降に前年度の実績値を踏まえて精緻にしていくかというところに重点が置かれており、日本もこれに倣うことが現状採りうる方法であると考えられる。

解決策

① 複数年の運用を通じて見積の精度を高めていく諸外国の事例を紹介する
- 導入初年度は期中に予算不足とならないよう見積はリスク分を考慮した額とし、2 年目以降は前年度の利用量の実績を踏まえ、見積の適正化を図っていく

② 技術的対話の実施、複数の事業者からリスク低減策の提案や情報提供を求めること等により、調達仕様書の記載を適正化し、予算超過の原因となるリスクを低減させる（例：事業者（SIer、リセラー）との技術的対話、CSP のコンサルティングサービス等を利用した見積の精度向上）

③ 初年度の見積のブレの影響を補正するための手段（年度途中での契約変更や上限価格付従量契約等）を検討する
- 仮に当初見積額よりも支払額が少なくて済んだ場合にコスト削減効果が何らかの形で還元される方策については、上限価格付従量契約を導入する可能性も含めて検討する

④ 既存事業者からの見積がクラウドに適した方法で行われるよう、参考となる事例を蓄積・共有する

4.5.4. 調達

① 調達区分、契約方法（直接・間接）の整理

表 4-17 課題の解決策（調達：調達区分及び契約方法）

No.	工程	課題（再掲）	課題の内容（再掲）
4.1	調達	パブリック・クラウドに合った適切な調達区分、契約方法（直接、間接）が分からない	• パブリック・クラウドの利用目的、利用形態を踏まえた調達区分、契約方法の明確な判断基準や検討材料がないため、①調達側がパブリック・クラウドを敬遠する、②適切な調達区分・契約方法を選択できない、③適切な調達仕様・契約内容を規定できない等のリスクがある • 上記のリスクがあるため、慎重な検討や分析が必要となり、作業負荷がかかる

海外ヒアリング、研究会を踏まえての考察

解決策検討の前提事項

① 欧米諸国においても、前述の理由から CSP との直接契約を行っている例は多くないことから、現時点では CSP との直接契約は積極的には推奨しない。ただし、直接契約も現実的な選択肢に加えられるよう、引き続き、課題解決に向けた検討が望まれる。

② 欧米諸国でも、以下の理由から直接契約することは殆どない。
- CSP の多くは個別対応を行っておらず、政府調達手続きにマッチした受注対応は困難
- IT のプロでない政府職員が直接パブリック・クラウドを運用するのは知識・スキルの面で困難
- 政府が直接パブリック・クラウドを運用するためには、間接契約以上に大きなリソースが必要な場合が多い

③ 日本の行政機関では、直接契約を行うための知識やスキル、さらには直接契約と間接契約を合理的に比較検討するための知見も欠くことから、現状では、リセラーや SIer を介した間接契約とするのが現実的である。

解決策

① 当面は、間接契約を中心にパブリック・クラウドの利用を推進する

② パブリック・クラウドに適した調達区分、契約方法、問題発生の防止策及び問題発生時の解決方法に関するベストプラクティスを蓄積・共有し、前例として参照できるようにする

【コラム】リセラーを経由した間接契約

クラウドサービスを利用する方法としては、CSP と直接契約する方法、SIer を介して契約する方法のほか、リセラーを経由して契約する方法がある。CSP は原則として、顧客無差別自動化された支払スキームを採っており、政府の調達制度や支払いスキームには対応できないことが多い。そこで、リセラーが間に介在することで、両者を橋渡しすることが可能となる。例えば、自社規程によりクレジットカード払いが認められていない法人利用者であっても、リセラーの請求書払いサービスによって、支払方法がクレジットカードに限られるクラウドサービスを利用できる。また、従量制の課金に対応が難しい利用者に対し、定額でクラウドサービスを利用できるプランを提供しているリセラーもある。

リセラーは多数の最終ユーザの利用をとりまとめることで、ボリュームディスカウントの適用対象となり、結果的に直接 CSP と契約を結ぶ場合に比べてより安価に利用できる場合がある。加えて、リセラー独自のサービスも付加されるため、利用者にとっては、直接契約以上のコストメリットとサービス向上を得られる可能性がある。

以下の表は、リセラー企業のウェブサイト情報をもとに、リセラーが提供するサービスを整理したものである。これらのサービスは、請求書払いのように多くのリセラーが共通して提供しているサービスと、定額利用のように一部のリセラーのみが提供するサービスとに大別される。リセラー各社のサービスの組合せは様々であることから、利用者は必要とするサービスや自組織が置かれた条件に応じてリセラーを選択することが重要となる。

表：リセラーの提供するサービス

No.	区分	サービス	サービスの詳細	リセラー企業別のサービス提供状況								リセラーの特徴
				A社	B社	C社	D社	E社	F社	G社	H社	
1	多くのリセラーが提供する基本的なサービス	日本円での請求書払い	支払方法がクレジットカード払いに限定されたクラウドサービスを利用する場合であっても、リセラーへの支払いを請求書払いとする	○	○	○	○	○	○			多くのリセラーが提供
2		リセラー独自のサポート窓口	CSP が提供する有償サポートなどと同等のサポート窓口をリセラーが無償で提供する	○	○	○	○		○	○		
3		各種申請代行	クラウドサービスを利用するために必要な手続きをリセラーが代行する	○	○		○	○				
4	一部のリセラーが提供する特徴的なサービス	ボリュームディスカウントを考慮した料金設定	クラウドサービスの利用量が多いリセラーはボリュームディスカウントが適用されるため、直接クラウドサービスを利用する場合よりも、利用料を抑えられる。このほか、長期利用により利用料がディスカウントされるリザーブドインスタンスをリセラーが確保した上で、利用量分析により効率的にインスタンスを運用することで、利用料を抑える方法もある	○	○		○					顧客数やクラウドサービスの利用量の多いリセラーが提供
5		インシデント発生時の保険	CSP が補償しないセキュリティインシデントなどによる損害をリセラーが補償する		○	○						特定の業界の顧客に対応するリセラーが提供

6		定額でのクラウド利用	従量制のクラウドサービスを定額利用できるように、リセラーが調整するしくみを提供する。例えば、リセラーが特定の金額までクラウドサービスを利用できるチケットを販売する方法（※）などがある ※費用が固定されることで組織内における予算申請や稟議がスムーズなるという利用者のためのサービスであり、調査時点においては、特定の業界向けのサービスプランとして紹介されている	○					○			（特定の商慣習や特定のニーズに対応するためのサービス）
7		複数のクラウドサービスへの対応	単独のリセラーが複数のクラウドサービス（AWS、Azure 及び GCP など）に対応するため、利用者はそれぞれのサービスの長所を活用することができる	○							○	複数のクラウドサービスをリセールできる技術的な対応範囲の広いリセラーが提供
8		幅広い技術的な提案	複数の IT 企業と提携し、クラウドサービスを含めた多くの IT ソリューションの中から利用者のニーズ合う最適なサービスを提案する								○	

②　責任範囲の整理

表 4-18　課題の解決策（調達：責任範囲）

No.	工程	課題（再掲）	課題の内容（再掲）
4.1.1	調達	CSP と SIer の責任範囲をどう設定すればよいか分からない	以下の考え方の整理が必要 • パブリック・クラウドとその上位層（アプリケーション等）との責任分界点の明確化 • 問題発生の防止策及び問題発生時の解決方法の整理

海外ヒアリング、研究会を踏まえての考察

解決策検討の前提事項

① 本課題は、そもそも CSP とそれ以外のプレーヤーの責任範囲をどのようにして決めるかという点がポイント
- まず前提として、パブリック・クラウドサービスは、本来的に個別機関・個別調達ごとの独自要件への対応とは、相容れないビジネスモデルとなっている（個別対応が逐一行われるのであれば、それはパブリック・クラウドとは呼べない）。したがって、CSP 及びリセラーは、顧客無差別に適用される約款（利用規約）の範囲でしか責任を負い得ない。
- その上で、いかに上位層（アプリ）の要件と CSP の要件のミスマッチのリスクに実際に対応するかについては、特定の CSP を上位層の調達の前提として想定する／しない場合の 2 つのシナリオへの分岐が考えられる。前者の場合、CSP を前提にアプリを構築する蓋然性が高まるため、両者の間にミスマッチは生じない。後者の場合、CSP と上位層の調達先はパラレルに決まるので、両者の間にはミスマッチが生じ得る。上位層の設計には、CSP のサービス内容を反映する必要がある。

② パブリック・クラウドについては、新しい取組であり、試行錯誤が避けがたいため、トラブル発生の可能性は予め想定しておく必要がある。問題が生じた場合、又は問題発生が予見される場合、欧米諸国では、CSP、リセラー/SIer、発注者間でのコミュニケーションの場を設け、共通認識を得て解決していくことを重視している。その上で、必要な契約変更を行って解決を図っている。

解決策

① 総務省「ICT スキル総合習得教材」（後掲）でも紹介されている「責任共有」モデルの考え方を基本とする
- その上で、いかに上位層（アプリ）の要件と CSP の要件のミスマッチのリスクに実際に対応するかについては、後掲の＜パブリック・クラウドと上位層（アプリ）間の要件ミスマッチへの対応の考え方（試案）＞を推奨する

② 問題が生じた場合、又は問題発生が予見される場合はステークホルダーとのコミュニケーションを図る
- 問題が生じた際の責任主体がグレーの場合は、関係者（発注者、CSP、SIer/リセラー）が一同に会し、CSP がもともと規定している責任範囲について確認を行い共通認識を持ったうえで、残りの部分の責任の所在や取扱いを発注者、SIer/リセラー間で明確化し、必要に応じ契約変更を行う（CSP に利用規約以上の対応を求めることは想定しない）

（参考）「責任共有」モデルの考え方

クラウドにおける責任共有モデル

◆「責任共有モデル」は、クラウド事業者と利用者の管理権限に応じた責任分担の考え方です。

- AWSなどのIaaSに関するクラウド事業者は、情報セキュリティに関して一般に**責任共有モデル**を採用しています。
  - IaaSをはじめとするクラウドのサービスモデルに関しては、講座2-2にて紹介しました。
  - 英語の「shared responsibility model」の日本語訳として「責任共有モデル」が定着していますが、「shared」は「共有」よりも「分担」と訳す方が意味が明瞭になります。

AWSにおける責任共有モデルの表記

【出所】責任共有モデル［Amazon Web Services, Inc.］
https://aws.amazon.com/jp/compliance/shared-responsibility-model/

- AWSのウェブサイトにおいて、責任共有モデルの説明として「AWS の責任は"クラウド**の**セキュリティ"」としている一方で、「お客様の責任は"クラウドに**おける**セキュリティ"」としています。
  - クラウドの基礎部分のセキュリティはAWSの責任である一方で、クラウドの内部のセキュリティは顧客（利用者）の責任であることを指しています。
- IaaSでは、利用者がインストールしたOSやソフトウェアに起因するセキュリティのトラブルは、管理権限のある利用者（顧客）の責任となります。
  - IaaSにおいては、利用者は自由に仮想サーバにインストールするOSやソフトウェアを選択できるため、クラウド事業者は仮想サーバの中を管理できません。
  - 情報セキュリティの国際規格で認証されたクラウド事業者であっても、管理権限がない領域に関する情報セキュリティには責任を持つことはできません。

クラウドプラットフォームにおける責任分担に関する表記

◆国際的なクラウド事業者は、責任共有モデルに対応する責任分担を表明しています。

- AWSに限らず、国際的なクラウド事業者は責任共有モデルに対応する責任分担を表明しています。
- GoogleのGCPにおいては、「アプリケーション レベルでのデータ制御」は利用者（顧客）の責任」であることを示しています。
- MicrosoftのAzureでは、クラウドのサービスモデル別・サービス運営の内容別にクラウド事業者と利用者（顧客）の責任分担を示しています。

GCPにおける責任共有モデルに対応する説明（抜粋）

Google Cloud Platform プロジェクトの安全性確保

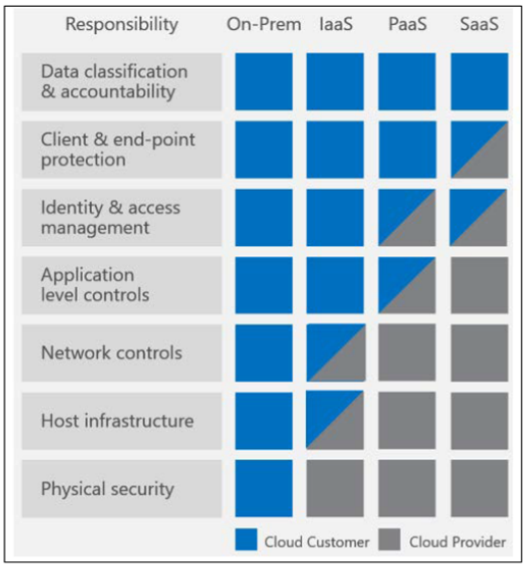
Google はお客様のプロジェクトの安全性を一部担いますが、セキュリティに対する責任は Google 単体ですべてを担えるものではなく、お客様の協力が不可欠です。

機密データの管理

データの重要性はその性質により異なります。Google Cloud Platform では、安全なアプリケーションの構築に必要な基本機能を提供していますが、これらのデータの適切な移動やアクセスをアプリケーションレベルで制御するのはお客様の責任です。これには、エンドユーザーが企業ネットワークやパブリック クラウド インフラストラクチャの外で重要な情報を共有しないよう防ぐ対策（データ損失防止）も含まれます。

【出所】GOOGLE CLOUD PLATFORM のセキュリティ［Google］
https://cloud.google.com/security/?hl=ja

Microsoftによるサービスモデル別の責任分担のイメージ



【出所】Shared Responsibilities for Cloud Computing［Microsoft］https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

- クラウドに関するセキュリティの責任分担は、サービスモデルのIaaS、PaaS、SaaSの分類にも依存しています。

各サービスモデルにおける情報セキュリティの分担

◆クラウド事業者と利用者の情報セキュリティの責任分担は、サービスモデルによって異なります。

- 2011年にNIST（米国国立標準技術研究所）の研究者は、クラウドサービスに関する情報セキュリティのガイドラインを示した「Guidelines on Security and Privacy in Public Cloud Computing」を公表しました。
- この資料において、クラウドの3種のサービスモデルの情報セキュリティ分担に関して、下表のように記載しています。

各サービスモデルに関する情報セキュリティの記述

サービスモデル	管理権限と情報セキュリティに関連する説明（抜粋）
IaaS	クラウドの利用者は、一般に搭載するOSや開発環境の選択に関して、高い自由度を持っている。**クラウドの基礎部分を越えるセキュリティ対策は、主としてクラウド利用者が実施する。**
PaaS	クラウドの利用者は、プラットフォーム上のアプリケーションやアプリケーションの環境を管理・設定できる。**セキュリティ対策は、クラウド事業者とクラウド利用者で分割される。**
SaaS	**セキュリティ対策は、主としてクラウド事業者が実施する。**一部を除いて、クラウド利用者はクラウドの基礎部分や個別のアプリケーションの設定を管理、操作できない。

【出所】Guidelines on Security and Privacy in Public Cloud Computing［NIST］から翻訳
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

- IaaSやPaaSは利用者も情報セキュリティに関する責任や保守作業の一部を分担する一方で、SaaSにおける情報セキュリティ対策は、原則としてクラウド事業者が実施します。
  - IaaSやPaaSでは、仮想サーバ内のOS/ソフトウェアのアップデートといった保守作業は利用者の責任で行う必要があります。
  - SaaSでは、利用者に情報セキュリティに関する専門知識や保守作業を要求しませんが、ログインIDやパスワードの管理は利用者の責任となります。
- 一般にクラウドサービスにおける情報セキュリティは、サービスモデルに応じて利用者にも責任や保守作業の一部分担が求められます。

出典：総務省 ICT スキル総合習得教材（http://www.soumu.go.jp/ict_skill/pdf/ict_skill_2_3.pdf ）

パブリック・クラウドと上位層（アプリ）間の要件ミスマッチへの対応の方向性（試案）

まず前提として、パブリック・クラウドサービスは、本来的に個別機関・個別調達ごとの独自要件への対応とは、相容れないビジネスモデルとなっている（個別対応が逐一行われるのであれば、それはパブリック・クラウドとは呼べない）。したがって、CSP は、顧客無差別に適用される約款（利用規約）の範囲でしか責任を負い得ない。

その上で、いかに上位層（アプリ）の要件と CSP の要件のミスマッチのリスクに対応するかについては、調達側の責任において慎重に設計を行うことが前提となるが、実務的には、特定の CSP を上位層の調達の前提として想定する場合／しない場合の２つのシナリオに分けて検討することが必要である。前者の場合、CSP を前提にアプリを構築する蓋然性が高まるため、両者の間にミスマッチは生じない。後者の場合、CSP と上位層の調達先はパラレルに決まるので、両者の間にはミスマッチが生じ得る。よって上位層の設計には、CSP のサービス内容を反映する必要がある。なお、ここでは、CSP と上位層は分離調達とすることを前提とする（一括調達であれば、そもそも CSP との契約や調達を検討する意味は乏しいため。）

① 順次調達型：特定の CSP を想定して上位層を調達する場合（推奨）

CSP の約款は顧客無差別のため、基本的には、CSP の責任範囲は、調達者・利用者が合意する約款に記載された範囲に限られる。したがって、発注者は、CSP の責任範囲を所与のものとして、パブリック・クラウドの上位層の要件・スコープを設定することが適当。発注者は、約款にない要求を CSP に期待することはできない。こうした要件は、そもそも CSP に求められるべきではない他のカテゴリーの要件であることがほとんどであり、どうしても必要な要件は、上位層・若しくは他の調達単位や工程に求めるべき要件として明記することが必要。

なお、特定の CSP を想定する場合には、前工程で、ライフサイクルコストを含めた評価・検証を行い、CSP の選定を行うことが必要。この場合、後工程での公平性を担保するため、CSP の調達に係る設計に関わった事業者が有利にならないことを担保する必要がある。

② 並行調達型：特定の CSP を想定せずに上位層を調達する場合（非推奨）

調達仕様におけるクラウドサービスの要件と CSP の約款の要件は一致しない。CSP はいずれにせよ顧客無差別なので、不一致に伴うリスクを取ることはできない。SIer は、どの CSP の約款が適用されることになるのか予測できないので、リスク分を費用に上乗せせざるを得なくなる上、トラブルの可能性も残ってしまう。発注側は、調達工程マネジメントを通じ、スケジュールの長期化やプロジェクトの遅延などの行政コスト増や経費の上振れのリスクとなり得る要素をハンドリングすることが必要となる。

③　支払サイクル・スキームのギャップへの対応

表 4-19　課題の解決策（調達：支払サイクル・スキーム）

No.	工程	課題（再掲）	課題の内容（再掲）
4.2	調達	行政機関と CSP 間での支払サイクル/スキームのギャップ	年度ごとの一括精算払いが基本の行政機関の現状と、毎月利用した分だけ請求するという CSP の支払サイクルや取引スキームとのギャップ

海外ヒアリング、研究会を踏まえての考察

解決策検討の根拠

① クラウドサービスを単価契約/月払とすることは制度上可能。ただし毎月の支払い手続きに係る行政職員の事務負荷がかかる。
② 間接契約では、CSP への毎月の支払いは、リセラー、SIer に委ねることが可能。
③ 利用した分だけ支払うというクラウドサービスのメリットを少しでも多く享受する方法としては、欧米諸国では期中の契約変更を行っており、日本もこれに倣うことは可能。ただし、この場合も契約変更の手続きに係る事務負荷及び財源を手当てする方法が課題となる。

解決策

① 当面は、間接契約を前提に（将来的には直接契約も視野に入れて）、よりクラウドの長所を引き出せるような支払方式を模索する
- リセラーや SIer を介した CSP との間接契約を利用する
- 将来的には、費用対効果等の観点で有利と判断される場合には直接契約も可能となるよう、課題の整理と解決策の検討が望まれる

② パブリック・クラウドに適した調達区分、契約方法、問題発生の防止策及び問題発生時の解決方法に関するベストプラクティスを蓄積・共有し、前例として参照できるようにする

④　ベンダーロックインの回避

表 4-20　課題の解決策（調達：ベンダーロックイン）

No.	工程	課題（再掲）	課題の内容（再掲）
4.3	調達	調達におけるベンダーロックインの可能性に対する一般的な懸念	いったん特定の CSP が受注すると、以後の調達でも当該 CSP を使わざるを得なくなるのではないか、という一般的な懸念が（事実かどうかは別として）存在する。 例えば、日本の政府機関でのパブリック・クラウドの導入実績を参加要件とする、市場に１つしかない機能要件を課す、といったことが行われると、先行 CSP には有利に、後発 CSP には不利に働く、等

海外ヒアリング、研究会を踏まえての考察

解決策検討の根拠

① 欧米では、同様の基準を満たした CSP であれば、サービス要件について事業者による差はあまりなく、それがベンダーロックインの要因になるようなことはない。

② そのうえで、パブリック・クラウドの導入において担保されるべきものとして、データポータビリティにフォーカスすることが重要と考えられるが、どのようにして実効性を持たせるかについては、今後の事例の蓄積が必要。なお、データ移行については、大手各社とも移行サービスを充実させている。こうした移行サービスがベンダーロックインへの懸念の解消に寄与する可能性もある。

解決策

① 調達時にデータポータビリティの確保、移行手段の明示を提案として求める。ただし、具体的な記載方法については、事例の蓄積を待つ必要がある

- パブリック・クラウドの調達仕様書に、データポータビリティが担保できる要件を盛り込むとともに、その根拠や具体的な実施方法を提案書やプレゼンテーションにおいて説明してもらうのも一案
- データポータビリティをどうすれば担保できるかについて調達事例を蓄積・共有するとともに、調達担当者へのトレーニングメニュー化することも有効と考えられる

4.5.5. システム監査・立入検査

① システム監査・立入検査の位置づけの整理

表 4-21 課題の解決策（システム監査・立入検査）

No.	工程	課題（再掲）	課題の内容（再掲）
5	システム監査・立入検査	CSP に対し、どのようなシステム監査・立入検査を規定すべきかが明確でない	データセンターへの立入検査を原則受け入れない CSP と、契約書上、立入検査の権利を留保してきた公的機関の立場の不一致

海外ヒアリング、研究会を踏まえての考察

解決策の前提事項

① 「政府情報システムのためのセキュリティ評価制度(ISMAP)」で認定を受けた CSP は、「クラウドサービスに対して要求するべき基本的な情報セキュリティ管理・運用の基準」を満たすこととなるが、「情報システムの性質を踏まえ、各政府機関等が実際に調達又は運用を行うに当たり、本制度において設定された各種基準に加えて、必要に応じて追加的な要求事項を設定することは妨げられるものではない。」とされている。

② システム管理基準のうち、ISMAP に含まれない事項（手順の文書化や遵守等の品質面の監査項目）については、従来通りの取扱いとなる可能性がある。

③ 官庁の契約書に標準的に記載されている立入検査は、契約、支払、報告等といった主としてビジネス面での問題が生じた場合に実地に確認を行うものであり、通常想定される検査先は本社ビルなどである。他方で、セキュリティ面については、ISMAP の枠組みに準拠すべきであり、通常の立入検査で行政職員自らが確認を行うべきものではない。ただし、立入先等について予め制限をかけるべきものでもなく、これは諸外国も同様である。すなわち、実行はしないが、権利は留保している。もっとも、この場合の検査も無制限に許されるべきではなく、あくまで契約履行に必要な範囲で抑制的に行われるべきである。

解決策

① CSP のデータセンターへの行政職員による立入検査は通常意味がないことの理解を拡げる

② 調達担当者に対し、ICT 研修やセキュリティ教育を通じて以下を周知する

- システム運用の適正性は、政府の方針に則り、ISMAP や「基本方針」に基づく第三者の認証、監査報告書を利用して担保する

A) 情報セキュリティに係る監査については、ISMAP 情報セキュリティ監査ガイドライン（案）に基づき、ISMAP 運営委員会によって公開された「ISMAP 監査機関リスト」に登録された監査機関が、本ガイドラインに基づき実施した監査報告書を利用して実施する

B) 一方、ISMAP クラウドサービスリストに掲載されていないクラウドサービスを利用する場合には、別途、監査業務を調達し、以下のいずれかの認証（*1）に必要な項目を満たしている、又は以下の監査フレームワーク（*2）に対応していることを確認することが考えられる

*1. 「ISO/IEC 27017 による認証取得」、「JASA クラウドセキュリティ推進協議会 CS ゴールドマーク」、「米国 FedRAMP」

*2. 「AICPA SOC2（日本公認会計士協会 IT7 号）」及び「AICPA SOC3（SysTrust/WebTrusts）（日本公認会計士協会 IT2 号）」

なお、手順の文書化や遵守等の品質面の監査項目については、欧米においては（データセンターのロケーションの秘匿性の点から）第三者認証や監査報告書で確認をとっている

③ 契約書に定める立入検査は通常、本社ビル等での支払額の検証など主にビジネス面に関して行う

4.5.6. IT ガバナンス

① 行政職員側に求められる知識の整理

表 4-22 課題の解決策（IT ガバナンス）

No.	工程	課題（再掲）	課題の内容（再掲）
6	IT ガバナンス	行政職員側のクラウド利用に係る知識の不足	パブリック・クラウドを選択肢として検討するにあたり、行政職員がパブリック・クラウドに関して身につけるべき知識・スキルが不足している

海外ヒアリング、研究会を踏まえての考察

解決策の前提事項

① 欧米諸国の例を見ても、行政職員に求められる専門性は、基本的には間接契約による運用を的確に行うために必要な知識である。この観点から以下がパブリック・クラウドについて行政職員が身につけるべき専門性になると考えられる[10]。

A) クラウドサービスの基礎的知識、本質的な理解 （メリット、従来との違い、注意点等）
B) 契約に関する知識（調達手続き、利用量の監視・着地見込の試算）
C) サービスコンソールの操作に関する知識（利用状況の監視、リソースの増減設定、アクセス制限の設定、アカウント・権限管理、各種マスタ設定等）

解決策

① 間接契約による運用を前提として、以下に重点を置いて職員の教育を行う
a. クラウドについての基本的理解
b. 調達/契約方式における留意事項
c. 使用量の見積精度向上の方法
d. ハンズオンでのコンソール操作体験
e. セキュリティ担保のための諸制度

② 研修方法：外部講師による座学（基礎知識）、CSP が提供するトレーニング（本質的理解と体験）、情報システム導入時トレーニング（実務知識）

例）AWS はカナダ政府に対し、クラウドサービスの導入支援のための AWS DigiGov プログラムを提供している。2 日間の教室内教育プログラムで講義、クラウドベースのカリキュラム、ハンズオンラボを通じて、参加者はクラウドを使用し、クラウドテクノロジーに対する障壁を取り除く方法を学習する
https://aws.amazon.com/jp/blogs/publicsector/learning-create-citizen-specific-cloud-aws-digigov/

[10] 外国政府では、政府職員がクラウドを利活用する際の手がかりとなる情報をまとめたウェブサイトを公開している国もある。具体例として、
・米国：GSA のクラウドチームがクラウド利活用に関するガイド、ベストプラクティス、テンプレートなど、クラウド利活用に関する職員向けの情報を集約したウェブサイトである、「クラウドインフォメーションセンター（CIC）」を 2019 年 5 月に開設している（https://cic.gsa.gov/）
・英国：GDS が 2019 年 12 月にクラウド利活用の際のベンダーロックインを回避するためのガイドを公表し（https://www.gov.uk/guidance/managing-technical-lock-in-in-the-cloud）、その後 2020 年 3 月にはクラウドを利活用する際に留意すべき点、関連するルールや戦略へのリンク集、及び実際のクラウド活用事例集をまとめた公共部門向けガイドを公表している（https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector）
・カナダ：クラウドサービスを導入する際のセキュリティ、リスク、データの取扱いなどに関する留意点をとりまとめ、ウェブサイト上に掲載している（https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services.html）
・ニュージーランド：カナダと同様のガイド・ツール集が整備されている（https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/）。

5. まとめ

本調査研究は、政府のクラウド・バイ・デフォルト原則を踏まえ、今後、行政機関がパブリック・クラウドの活用を推進するに当たっての実務的な課題を棚卸しして整理・分析し、解決策を提示したものである。

調査研究では、諸外国の調達・契約制度等の公開文書調査、諸外国におけるパブリック・クラウドの調達及び契約に関する実務運用のヒアリング、専門家ヒアリング、並びに政府及び会員企業による研究会での課題及び解決策の検討を行った。その結果、諸外国におけるパブリック・クラウドの利活用の実際、諸外国の調達・契約スキームの発展状況、及び今後の我が国での活用推進に当たっての以下の課題及び解決策を提示することができた。

特に、「課題及び解決の方向性」では、政府・自治体においてクラウドサービスの調達に携わる実務担当者や、クラウドサービスの活用の推進に複数組織をまたいで取り組む機関の施策立案の担当者にとって、実務的に役立つ知識を導出できたと考えている。

本調査研究を通じて、パブリック・クラウドは既に行政機関において実用的な選択肢たり得ることが明らかになった。他方で、今後パブリック・クラウドのメリットを引き出すとともに、パブリック・クラウドの活用によって生じるリスクを低減するためには、①間接契約を想定した調達・支払方式の活用、②クラウドの活用事例及びノウハウの蓄積と共有、③クラウド活用を組織横断的に支援する仕組みづくり、④クラウドの理解不足を解消し実務スキルを習得するための教育訓練が重要になると考えられる。

もとよりパブリック・クラウドは調達手段の一つに過ぎない。しかしながら、今後の行政情報システムの見直しを検討するにあたり、選択肢として欠かせないものとなってくることは間違いないと考えられる。政府・自治体においては、本調査研究の結果を踏まえ、組織間で連携して、パブリック・クラウド活用の検討に取り組むことが期待される。

初版：2020 年 3 月 31 日
一般社団法人　行政情報システム研究所