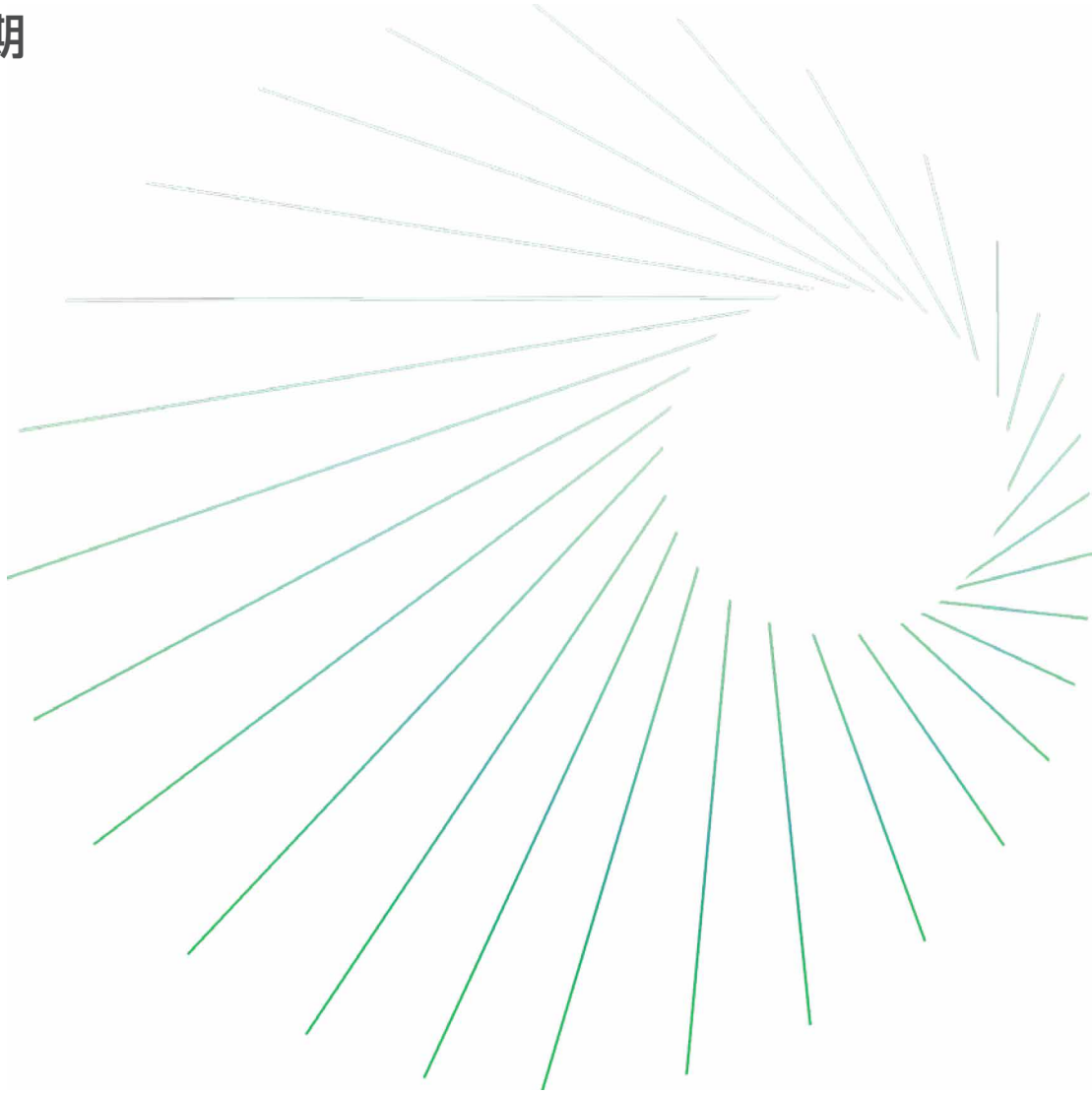
双方向のクラウドへの最適経路：

ハイブリッドクラウド環境とマルチクラウド環境の セキュリティ保護に関するユーザーの見解

White Paper

2019 年第 2 四半期



Jeff Wilson
サイバーセキュリティテクノロジー担当
上級リサーチディレクター

IHS Markit Technology | White Paper

目次

概要

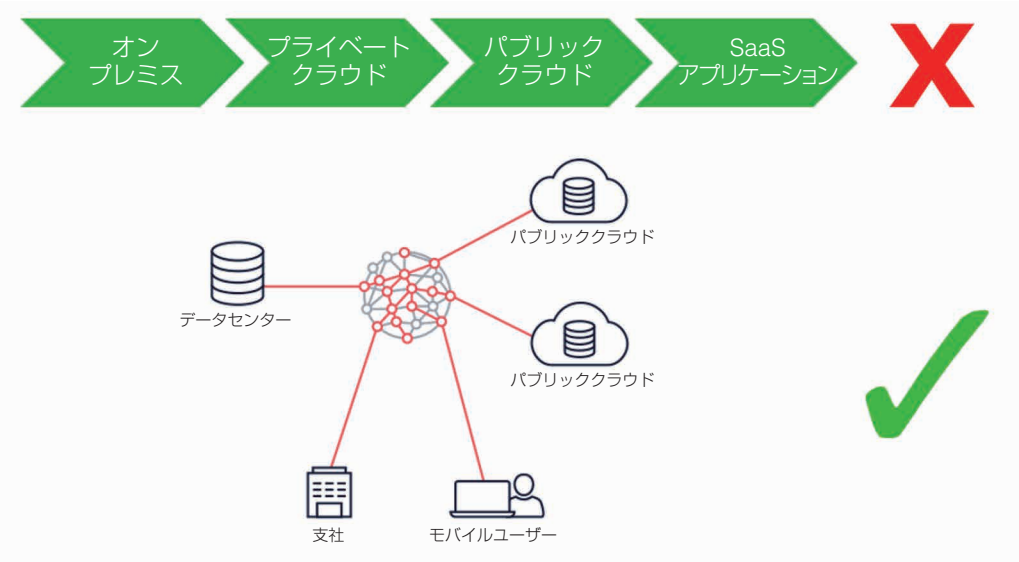
ビジネスコンピューティングの誕生以来、数多くの高度な新しいテクノロジーによって組織における日常業務のやり方が変化してきましたが、過去 15 年間におけるクラウドの進展は、コンピューティングと通信テクノロジーが最も大きく集約されたものとなっています。あらゆるタイプの組織が、ビジネスを改善するために、クラウドへのインフラストラクチャ、アプリケーション、データの移行をいかに利用できるかを真剣に検討しています。潜在的なメリットは極めて画期的であることから、クラウドへの移行は避けられないものとなっています。これらのメリットには、クラウド内で IT インフラストラクチャを管理し、セキュリティ保護するために必要となるプロセスやテクノロジーに影響する大きな課題が伴います。

クラウドとクラウドセキュリティに対する現在の考え方を把握するために、当社は 350 社の企業（米国内の従業員 1,000 名以上の企業、その他全ての地域の従業員 500 名以上の企業）を対象に調査を行い、その結果について重要な点を本書で紹介しています。対象となった企業には、過去のテクノロジー採用傾向に合致しない企業や、クラウドとクラウドセキュリティの採用がどのように展開するかという基本的な知識に沿っていない企業もあります。

新しいテクノロジーが出現する時には、通常、左から右への明確な進路が存在します。左側が古い方法（悪化）で、右側が新しい方法（改善）であり、どの企業も古い方法から新しい方法に移行します。クラウドが登場した当初には、導入はこのパターンに従って行われ、すべての IT インフラストラクチャにとってクラウドが最適な選択肢であると多くの人々が見なしていました。非常に長い期間この考え方が大勢を占めていましたが、今後しばらくの間は、インフラストラクチャ、アプリケーション、およびデータは、さまざまな環境や機会によってオンプレミスとプライベート / パブリッククラウドインフラストラクチャの間を行ったり来たりする移行が繰り返されることになるでしょう。

組織は、クラウドの使用が適している用途やクラウドの使用方法を把握し始めたところです。アプリケーションをクラウドに移行した企業が、タイム ドリブン型アプリケーションやイベント ドリブン型アプリケーション、合併や買収、セキュリティ上の新たな懸念、クラウドのパフォーマンス不足、規制の変化、導入コストや価格の変化、新規アプリケーションの開発、基盤テクノロジーの変更など、さまざまな理由のためにクラウドから手を引いたという事例が多数存在します。数多くの企業が動的にマルチクラウドを利用しているというのが現実です。この調査の目的は、これらの事例を掘り下げて明確な傾向を把握することです。

図 1：動的なマルチクラウド

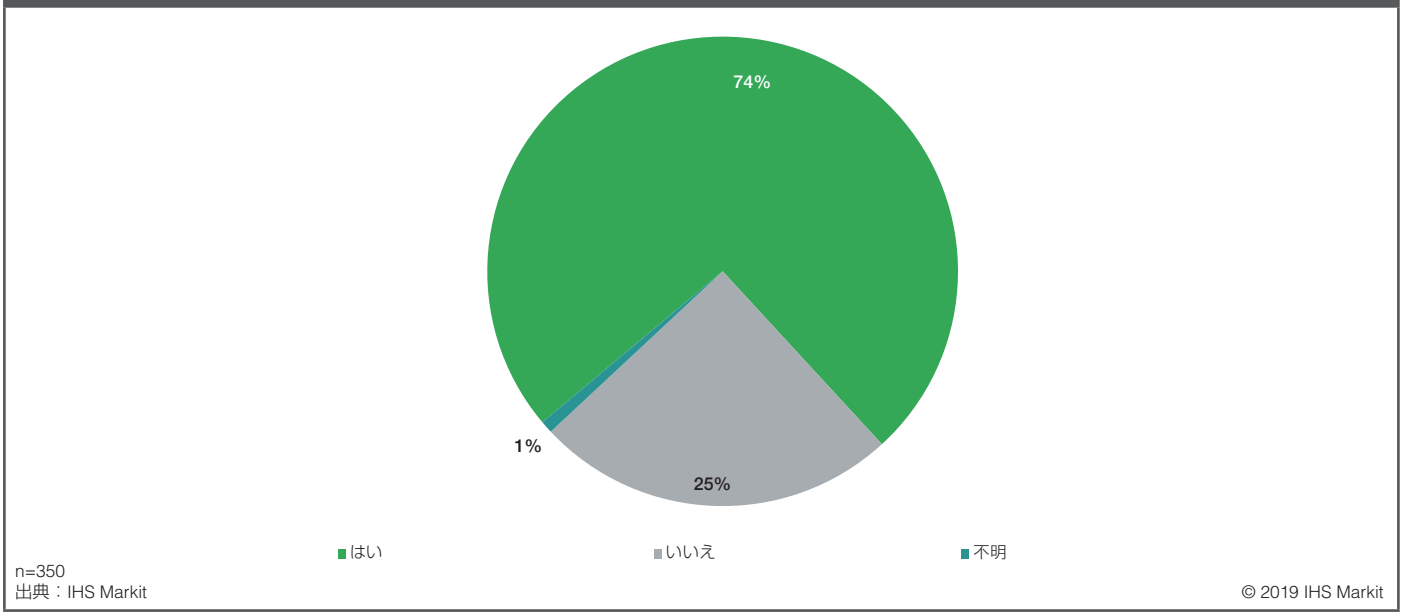


出典：IHS Markit

今では、ほとんどの組織が既にクラウドを検証しており、本番環境でクラウドテクノロジーを利用するために多額の投資も行っています。このような背景から、客観的な視点で、世界中の数多くの企業で IT インフラストラクチャおよび IT 戦略を担当しているアーキテクト（C レベルおよび VP レベルの IT プロフェッショナル、クラウドプロフェッショナル、および IT セキュリティプロフェッショナル）に対して、クラウドをどのように活用しており、実際にどのようなセキュリティ上の課題に直面しているのかを尋ねる最適な時期であるといえます。

調査で分かった興味深い結果として、まず、動的なマルチクラウド利用が現実的であるという認識が高まっていることが挙げられます。調査対象となった 350 社の企業の 74% が、アプリケーションをクラウドに移行した後で、自社インフラストラクチャに戻しています。これは、クラウド展開をすべて元に戻したということではなく、単に双方向の移行があったということです。クラウドを導入展開する企業と、これらの企業をインフラストラクチャ、管理、セキュリティで支援するテクノロジープロバイダーは、この傾向を基本条件であると見なし、双方向の移行を念頭において製品とサービスを構築する必要があります。

図 2：アプリケーションをクラウドからオンプレミスに再移行したか



n=350
出典：IHS Markit

主要なクラウドプロバイダーも、動的なマルチクラウドに関する現実を認識しています。2018 年 12 月、AWS は企業がオンプレミス環境に配備し使用できるクラウドハードウェアプラットフォームの提供を開始することを発表しました。この発表は、AWS プラットフォームを利用するメリットを引き続き享受しながら、アプリケーションをオンプレミスに配置する（またはオンプレミスに戻す）必要があるケースが存在することを裏付けています。Microsoft は Azure スタックで同様のサービスを提供していますが、顧客はパートナーからハードウェアを購入する必要があります。両方のケースの要点は同じです。ハイブリッド環境が普及しており、アプリケーションとインフラストラクチャは、オンプレミスからパブリッククラウドへの動的な移行が続くということです。

次に私たちは、アプリケーションを自社インフラストラクチャに戻すという状況を促進している要因について質問しました。最も回答数が多かったのはパフォーマンスとセキュリティの 2 つで、それぞれ回答者の 52% がこれを選択しています。パフォーマンスの問題は、クラウドインフラストラクチャの性能向上によって時間とともに改善されるでしょう。クラウドを利用する企業は、さらに日和見的にクラウドインフラストラクチャを使用するようになり、パフォーマンス向上やコスト削減のためにベンダーを切り替えることになるでしょう。多くの組織では、クラウドのセキュリティ確保について誰が責任を負っているかを把握さえしておらず（これについては後で詳しく説明します）、クラウド導入展開におけるセキュリティ確保に必要となるテクノロジーについて、確固としたエンドツーエンドのビジョンもないことから、セキュリティはさらに難しい問題となっています。

回答者の 40% が、自社インフラストラクチャに戻したクラウド導入展開の一部が、「計画に基づく一時的」なものであったと述べています。このような計画に基づく一時的クラウド導入展開の好例として、合併や買収に伴う避けられない IT 移行を実施している間に準備された一時的なインフラストラクチャが挙げられますが、その他にもさらに多くの事例があります。規制の問題については、回答者の 21% が選択しています。このことは、動的なマルチクラウドの「動的」部分を顧客企業が必ずしも制御できるとは限らないことを示しています。

すべてのアプリケーションがクラウドの新しい現実に

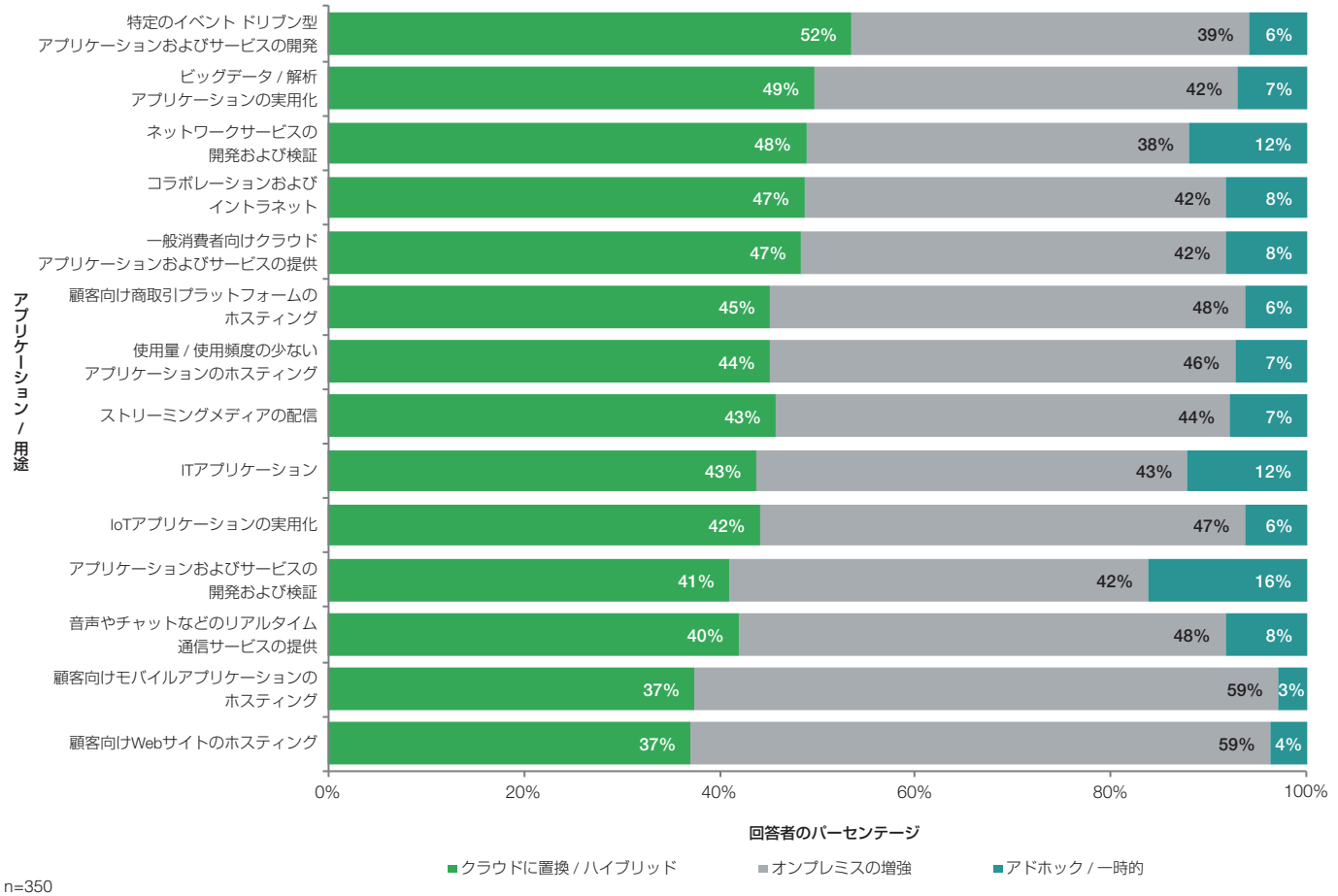
話をしている相手がクラウドプロバイダーなのか、クラウドインフラストラクチャを購入する企業なのか、クラウドの導入展開に必要となるテクノロジーを提供する企業なのかを問わず頻繁に話題になるのは、クラウドインフラストラクチャの最も一般的なアプリケーションや用途について、明確な答えは 1 つもないということです。クラウドに関する基本的な現実（大部分の企業は Office365 に移行している、または Salesforce が広く使用されている）を知ることで、企業はクラウドには無限の用途が存在すると考え、それらすべての可能性を模索しています。

この柔軟性は、長期に渡ってクラウドアーキテクチャの長所の 1 つとなっています。しかしながら、この柔軟性が原因で、導入の迅速化、クラウドアプリケーションとインフラストラクチャの管理性、そして最も重要な点としてクラウド環境の保護を実現するために誰もが理解しておくべき方向性を見出すことが難しくなっています。共有されるというクラウドインフラストラクチャの基本性質が理由で、クラウドインフラストラクチャで一体何が行われているのか、誰も実際に全体像を把握できません。

回答者がクラウドをどのように使用しているのかを詳しく把握するために、クラウドインフラストラクチャで使用している一般的なアプリケーションと用途のリストを提示し、使用状況を質問しました。使用しているアプリケーションと用途については、クラウドがどのような役割を果たしているかを質問しています。その際、クラウドの役割の選択肢として、完全な置換または常時使用のハイブリッド環境、プライマリのオンプレミス環境の増強（故障時またはディザスタリカバリ用）、およびアドホックまたは一時的な環境を提示しました。この質問の基本的な意図は、回答数の多いアプリケーションほど、「クラウド優先」または「クラウドネイティブ」の導入展開が一般的なものであることを把握することでした。

興味深いことに、それほど一般的でない用途（イベント ドリブン型のアプリケーションやサービス、サービス導入展開と検証など）が上位になるとともに、クラウドのパワーを実際に利用するアプリケーション（ビッグデータ / 解析アプリケーション向けなど）も上位に挙げられる結果となりました。長く使用され、十分に理解されているレガシーアプリケーション（顧客向け Web サイト、IT アプリケーション、通信アプリケーションなど）は、リストの下位になりました。企業がクラウドを優先するようになると、テクノロジーの新たな使用方法が検討されるケースが多くなります。より定着しているアプリケーションでは、企業は冗長性や追加の容量を提供して社内環境を強化するため、クラウドを日和見的に利用しています。

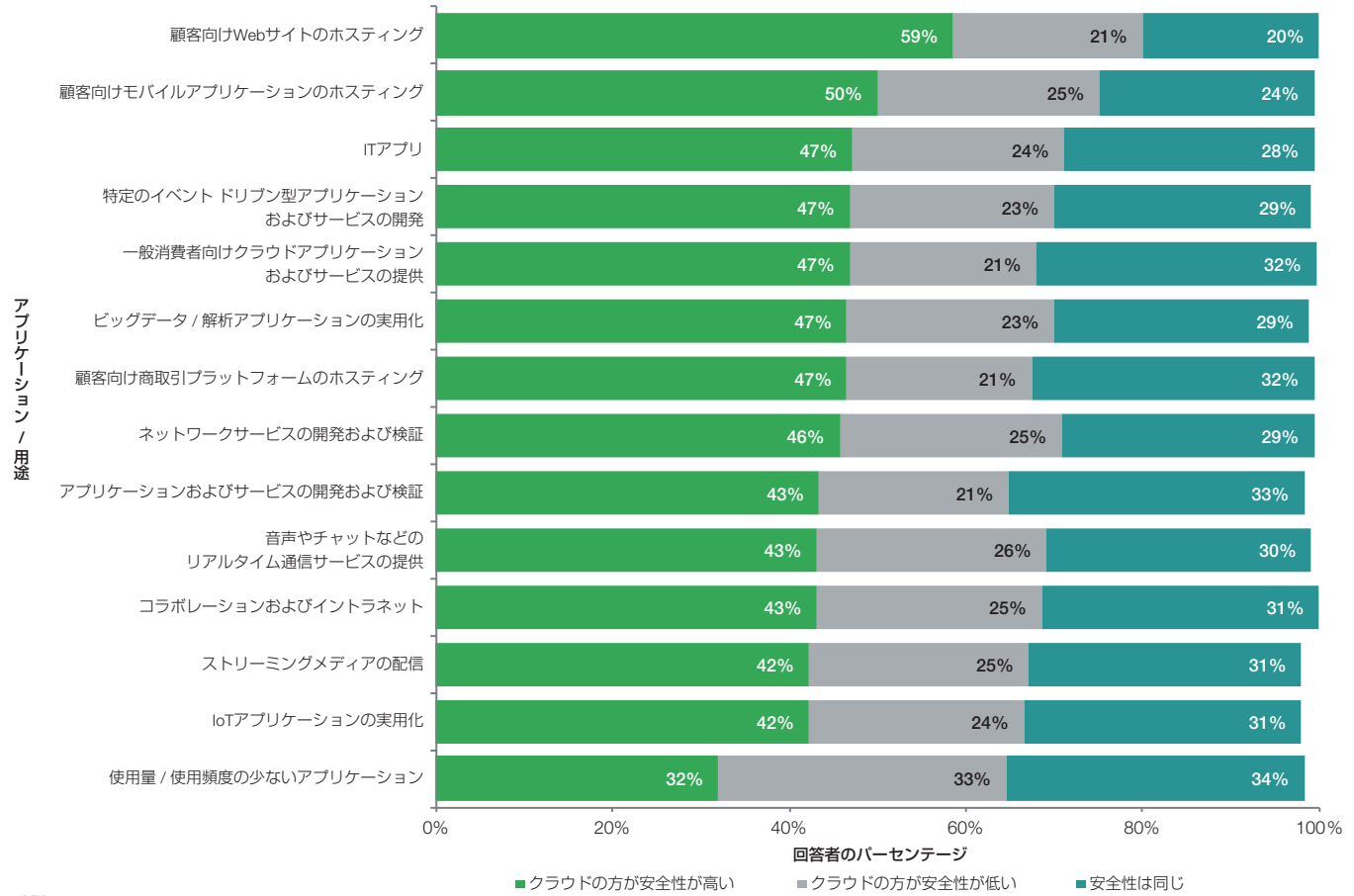
図 3：クラウドでの展開を最も優先するアプリケーション / 用途



n=350
出典：IHS Markit

ここまではクラウド環境に関連する質問と回答を示してきましたが、企業がクラウド環境への移行を躊躇している場合、一般的にセキュリティ上の懸念が主な問題となっています。回答者（IT プロフェッショナル、クラウドプロフェッショナル、およびセキュリティプロフェッショナル）に対して、アプリケーション / 用途別にクラウド内のセキュリティに関する認識を質問し、オンプレミス環境に比べてクラウドのセキュリティが高いのか、低いのか、あるいはほぼ同じなのかを尋ねました。

図 4：アプリケーション / 用途別のクラウドのセキュリティに関する認識



n=350
出典：IHS Markit

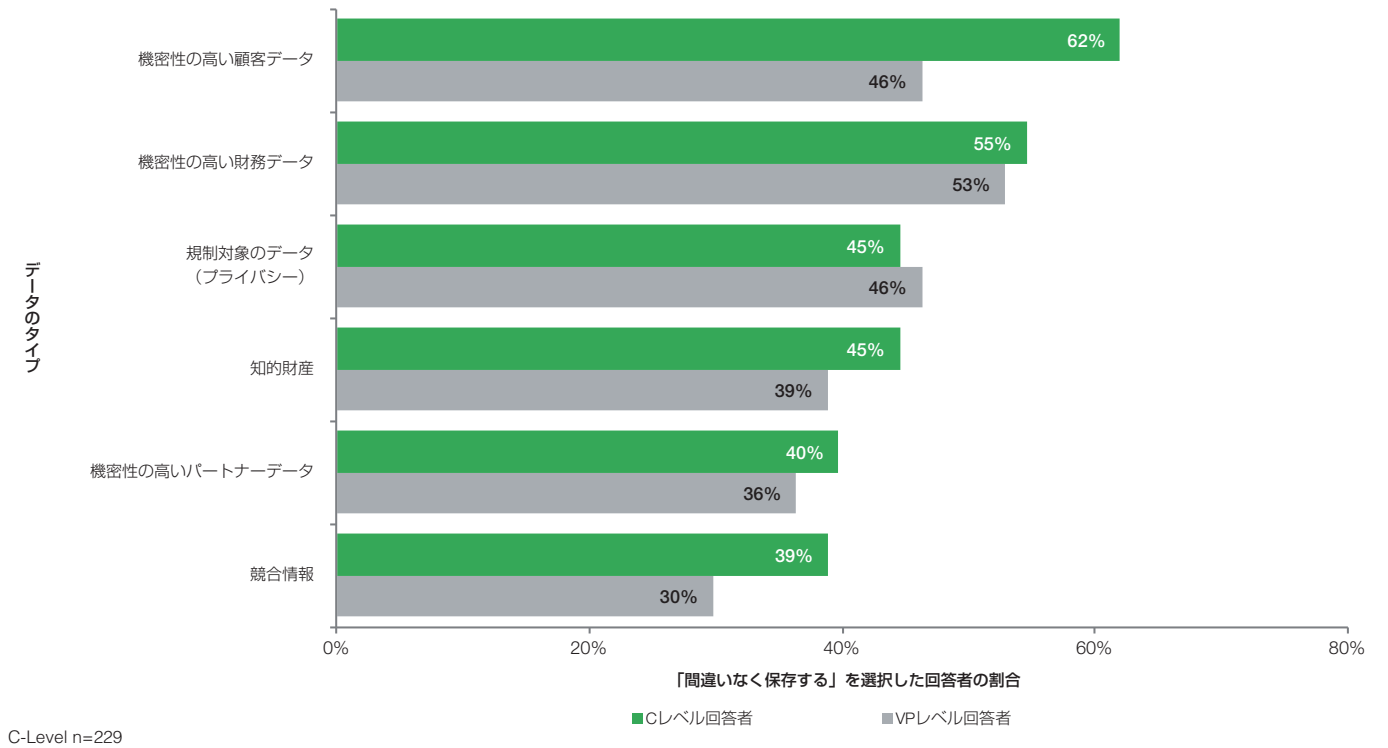
ここでは、グラフが前の質問とほぼ反対になっており、より定着し十分に理解されている用途では、全体的に「クラウドの方が安全性がが高い」と認識されており、新しい用途（「クラウド優先」のプロファイルに適合することが多いアプリケーション）では、クラウドの方が安全性が低いと認識されていることがわかりました。この理由として、十分に理解されているレガシーアプリケーションのセキュリティモデル（オンプレミスとクラウドの両方）はより適切に認識され、導入領域も広く、より成熟しているということもいえると考えられます。

ただし、回答者がクラウドへ「全て」を移行することを期待しているアプリケーションおよび用途については、セキュリティの目標を達成するためには、さらに時間とコストを投資することが必要な可能性が高くなっています。そのため、根本的な課題（これらのアプリケーションと用途では、クラウドの方が安全性が低い前提）によって実装面の問題が生じています。これらの新しい用途がビジネスに不可欠と見なされない場合、セキュリティへの投資を正当化することはできるのでしょうか。それとも、これらのクラウドプロジェクトは取り残されてしまうのでしょうか。ユースケースはそれぞれ異なるため答えは 1 つではありませんが、検討対象となるさまざまなアプリケーションのクラウドセキュリティに対する理解は、このような興味深いやり方で形成されています。

力関係のジレンマ：ビジネス上の優先順位とテクノロジーの現実

このジレンマはさまざまな形で現れますが、最も成功し（そして失速した）クラウド導入展開の中核をなす概念である、「ビジネス上の優先順位」対「テクノロジーの現実」という不変の攻防において、最も顕著に表面化していると考えられます。このジレンマを把握する 1 つの方法として、優先するデータのタイプを役職別におおまかに分けることができます。ここでは、調査に回答した C レベルのエグゼクティブ（CEO、CIO、CISO、CTO）と VP レベルのエグゼクティブ（IT 部門の VP、IT セキュリティの VP、クラウドの VP）に分けています。回答者は全て上級のエグゼクティブですが、VP レベルのエグゼクティブは、一般に C レベルのエグゼクティブよりも実装や運用の難しさを深く理解しています。これを念頭に置いて、ひとつの重要項目について C レベルと VP レベルの回答が大きく異なっている質問を紹介します。クラウドに特定のタイプの機密情報を保存することについて、回答者の意見を尋ねました。VP レベルの回答者も C レベルの回答者も、ほとんどの項目については同じ意見でしたが、C レベルはより高い割合で顧客データをクラウドに「間違いなく」保存すると回答しています。

図 5：クラウドでのデータの保存：VP レベルと C レベルの比較

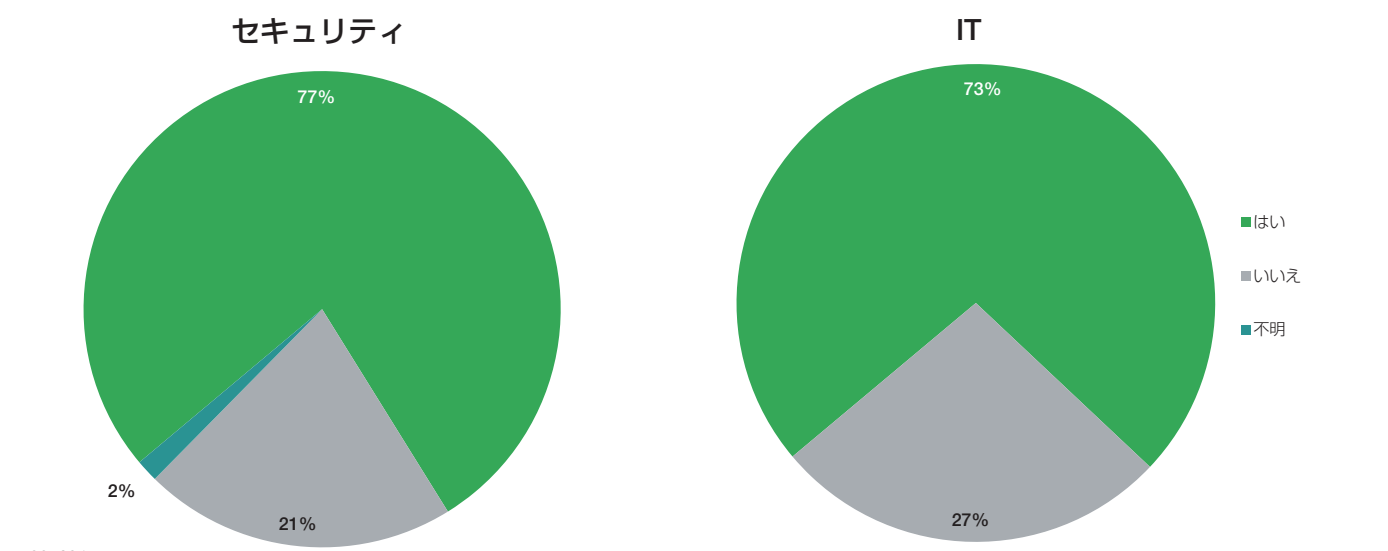


C-Level n=229
VP n=121
出典：IHS Markit

この回答にはさまざまな要因（業種や規制など）が影響していますが、クラウドにデータを保存することが規制に違反しないケースにおいて、2 つのグループで回答に差があるのは何故でしょうか。ほとんどの場合、セキュリティ以外の理由で（選択したテクノロジーパートナー、ERP または CRM 用に選択したアプリケーション、顧客情報を第三者に提供する必要性など）、該当するデータをクラウドに保存するというビジネス上の指示が行われています。これらの指示は、通常 C レベルの判断に基づいて実装担当者に伝えられ、対応が行われます。VP レベルの回答者にとっての問題は、顧客データをクラウドに保存したくない場合でも、保存場所に関しては選択肢がないことです。このため、クラウドパートナーやセキュリティテクノロジーパートナーに不安を解消できるテクノロジーの提供を依存しているのです。

回答者のグループを分ける別の方法として、レベルを問わずセキュリティ関連の役職（CISO、セキュリティの VP）を持つ回答者すべてを 1 つのグループ（以下のグラフ内の「セキュリティ」）にまとめて、他の回答者はすべて 2 番目のグループ（「IT」）に集約しています。セキュリティ上の懸念に関連する一連の質問に続いて、導入展開におけるセキュリティ上の特定の懸念にもかかわらず、アプリケーションまたはインフラストラクチャをクラウドに移行したことがあるかどうかを質問しました。「IT」グループの回答者の 73% が「移行したことがある」と回答したのに対して、「セキュリティ」グループの回答者の 77% が「移行したことがある」と回答しています。両方のグループで高い結果となりましたが、懸念があるにもかかわらず導入展開するセキュリティチームは、導入に際して細心の注意を払うと考えられます。

図 6：セキュリティ上の懸念にかかわらず、クラウドに移行したことがある：「セキュリティ」グループの回答者と「IT」グループの回答者の比較

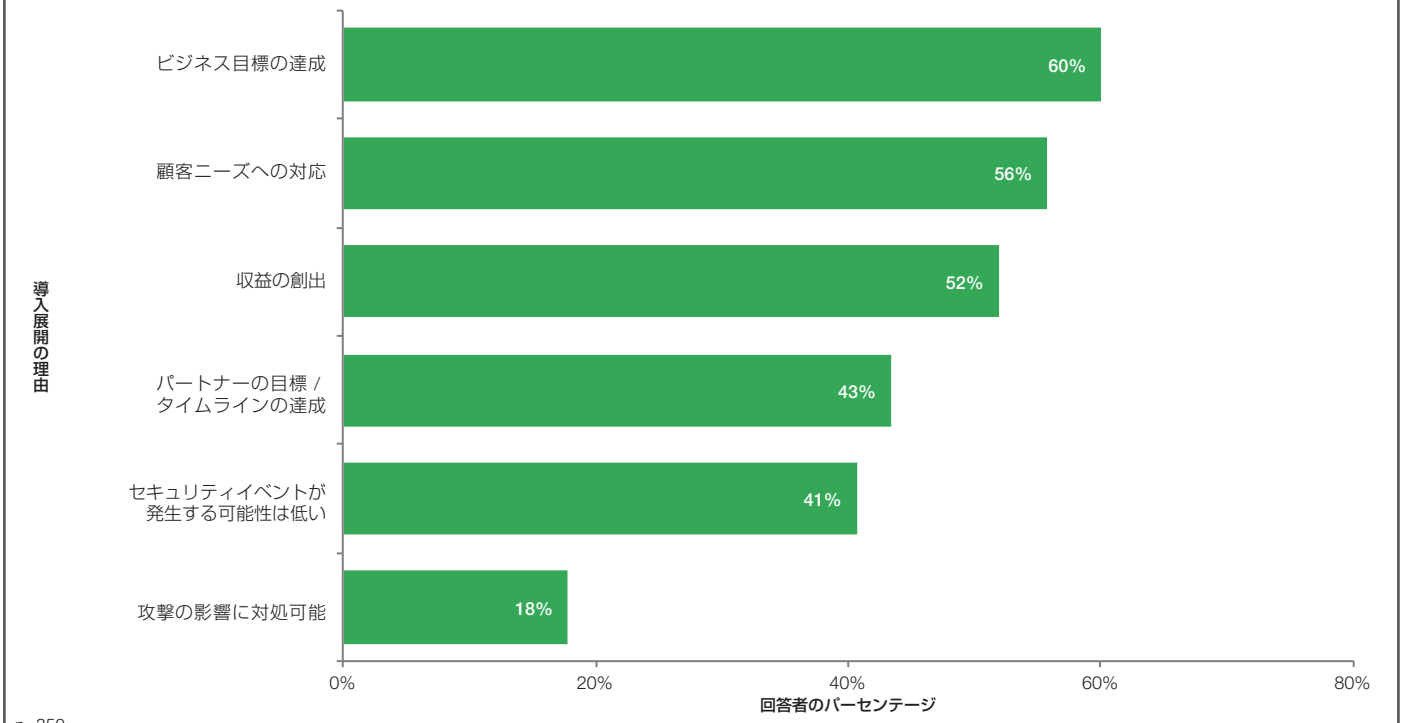


n=66, 284
出典：IHS Markit

プライベートインフラストラクチャではアクセスは常にセキュリティに勝るという考え方が当てはまるといえますが、クラウドへの移行においても変わっていないようです。懸念があるにもかかわらず導入を促進している要因は何なのかを把握するため、さらなる質問を行いました。上位 3 つの回答から、このようなリスクを伴うクラウド導入は、*主要なビジネス目標の達成に役立つ*、*顧客ニーズを満たすために有効である*、そして*収益を直接生み出す*ものであることが分かりました。大部分の IT インフラストラクチャはこれらの目標を支援するために存在しており、急速なクラウド採用は、クラウドがこれらの目標に全体として適切に対応できていることを示しています。

回答者は侵害が発生しないとは考えておらず（41% が、セキュリティイベントが発生する可能性は低いため、導入を推進すると回答）、クラウドで侵害が発生した場合は甚大な被害が生じることを理解しています（セキュリティイベントの影響に対処可能と考えているため、クラウド導入を推進すると回答したのは 18% に留まっています）。回答者は、単純にビジネス目標を達成するためにクラウドを導入展開する必要があり、甚大な被害が生じる前にセキュリティの問題に対処できることを願っているのです。

図 7：懸念がある場合でもクラウドへの移行を推進している要因



n=350
出典：IHS Markit

両方の場合で（C レベルと VP レベル、および「セキュリティ」グループとそれ以外）、現実としてクラウド実装担当者とセキュリティチームがクラウド用のアプリケーションに共同で取り組む必要があります。その際、どの既存テクノロジーを使用して導入展開を管理するのか、何を構築する必要があるのか（DevOps において）、テクノロジーパートナーから何を購入する必要があるのか、クラウドサービスプロバイダーに対して何を依頼するのかを、これまでよりも短期間で見極めることが必要になります。

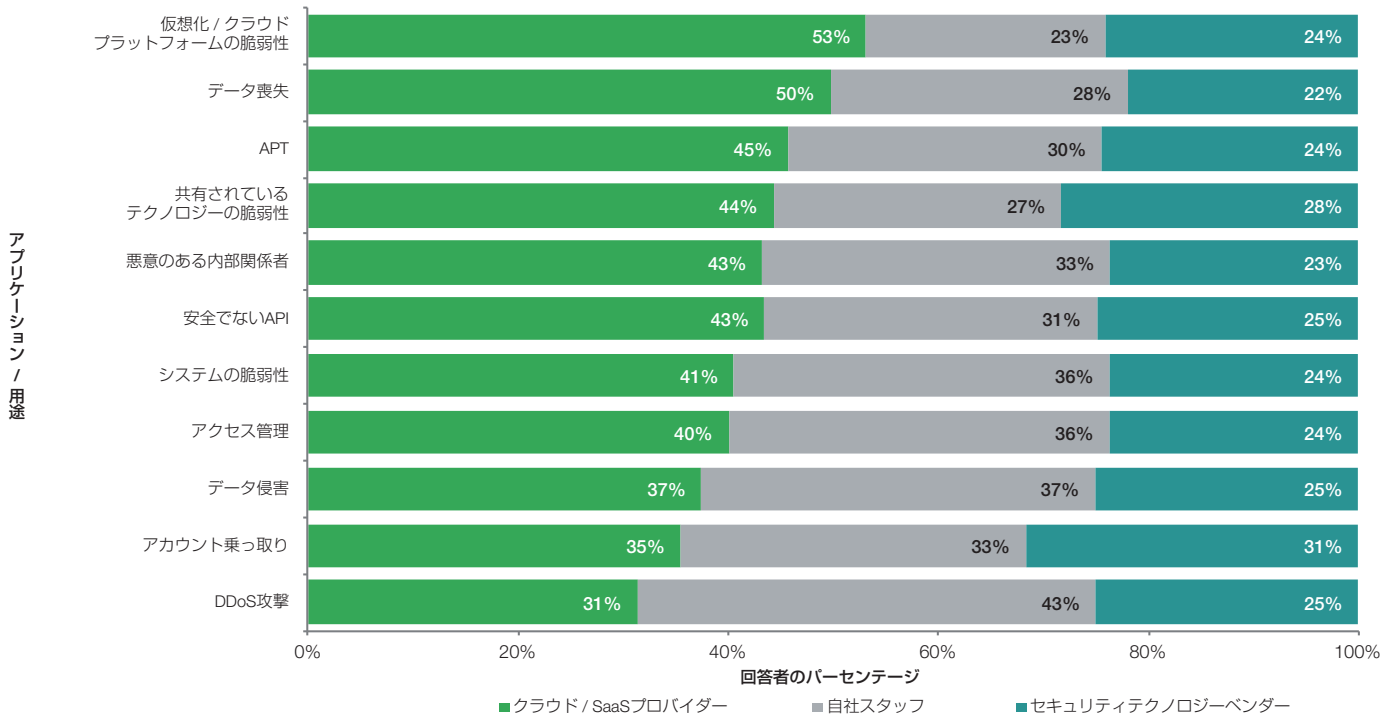
責任という難問：自社と外部の役割のバランス

すべてのタイプのクラウド導入展開に対して、さまざまなセキュリティソリューションが提供されています。サイバーセキュリティを主なテーマとした展示会では、「クラウドのセキュリティ」がすべてのセキュリティテクノロジー企業の最優先事項となっていることが分かります。例えば、回答者の誰かが明日にでも AWS か Azure を採用し、一時的なアプリケーション用にわずかなスペースを取得したり新しいアプリケーションやサービスを検証したりする場合、クラウドの市場ではアドオンの選択肢が膨大なセキュリティベンダーのリストに辟易することになります。クラウドプロバイダー自体が幅広いセキュリティソリューション（自社のプラットフォームに組み込み、またはアドオンされた）を提供しており、多くのクラウド管理プラットフォーム、ハイパーバイザー、オーケストレーションツール、その他のクラウドインフラストラクチャの構成要素では、さまざまなレベルのセキュリティが提供されています。

クラウドの導入を成功させるためには、ベンダー、パートナー、およびインフラストラクチャプロバイダーとの連携が重要ですが、クラウドの導入展開において脆弱性やセキュリティイベントが発生した場合、実際に責任を負うと回答者が考えているのは誰でしょうか。誰にも責任はなく、また誰もが責任者であるというのが答えです。誰が責任を負うか明確になっている最良のシナリオの場合（仮想化 / クラウドプラットフォームの脆弱性など）、真に責任を持っている組織、つまり脆弱なプラットフォームを構築した企業（VMware や AWS など）に責任を負わせているのは、回答者のほぼ半数のみでした。これは、多数の脆弱性が存在する欠陥のあるテクノロジーを利用してきた長い経験に基づいた、皮肉な回答です。大抵の場合は、脆弱なプラットフォームで実行されているデータとアプリケーションを所有しているのは顧客企業であり、顧客企業の IT チームとセキュリティチームが責任を負ってきました。

クラウドプロバイダーがインフラストラクチャの保護（DDoS 攻撃からの保護など）に秀でている場合、高い割合の回答者が上位レイヤーの脅威（APT など）にクラウドプロバイダーが責任を持つことを期待していることから、多少の学習が必要となりますが、クラウド内で発生したセキュリティイベントへの対応に関しては、各組織の能力、究極的にはその強みに関する理解は、時間とともに構築されます。

図 8：さまざまな攻撃シナリオにおいて最終責任を負うのはだれか

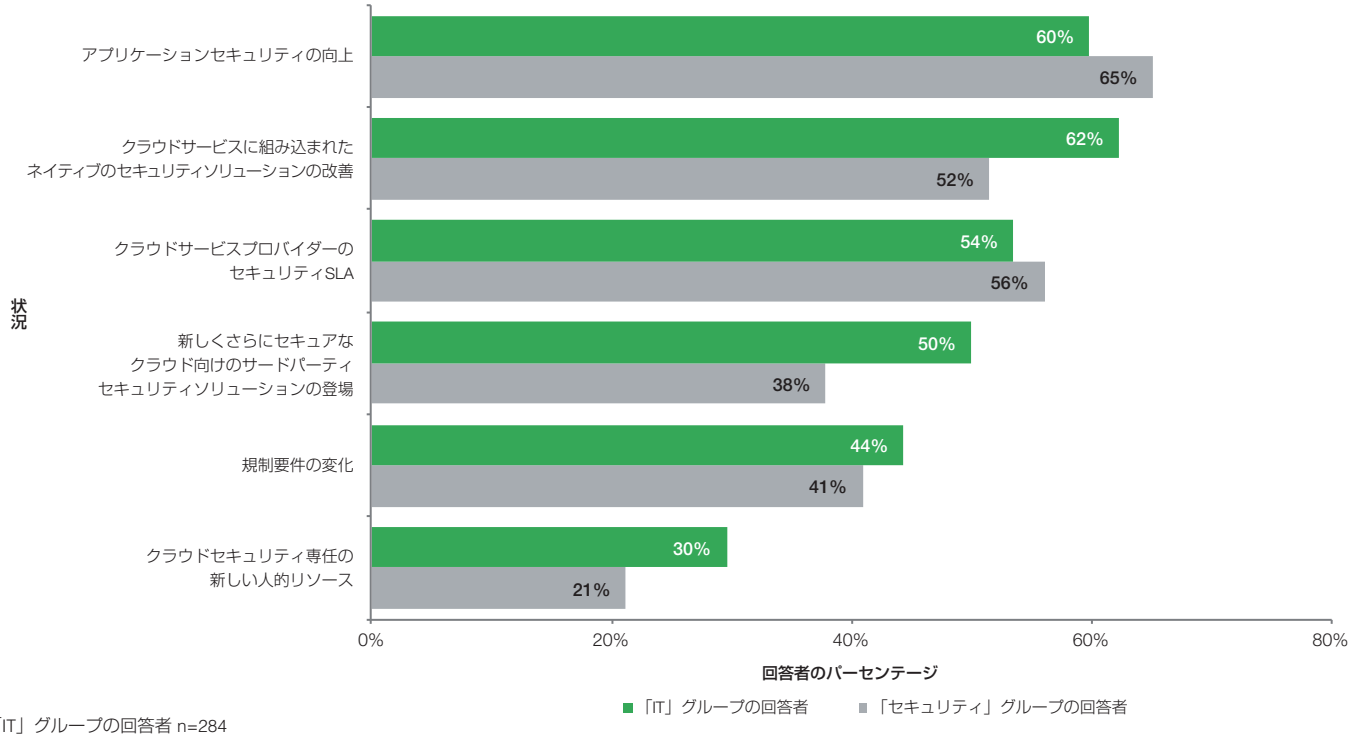


n=350
出典：IHS Markit

私たちが考える最善策とは、関連するすべての組織に対してアクションと責任を策定するという、クラウドでのセキュリティイベントに対する戦略を構築し、最終的にその戦略をデジタル化し、テクノロジーを利用してすべての組織間の対応を統合することであると確信しています。一部の対応を自動化できるとしても、クラウドは共有インフラストラクチャであることから、セキュリティイベントが発生した場合の責任も常に共有されるということが真実です。

最後の質問については、回答データを「セキュリティ」グループと「IT」グループに分けて確認しました。質問はシンプルで、現在クラウド内での保存を拒否している資産 / データに関して、再検討を行う際の要因は何かということでした。2 つのグループの違いは著しく、多くの場合、「セキュリティ」グループの回答者は、どのような資産 / データをクラウドに保存すべきか、および保存すべきでないかを理解していると考えており、改善や変更があった場合にも、比較的判断を変えません。「セキュリティ」グループ以外の回答者は再検討に肯定的ですが、これは「ビジネス目標を達成する」必要性に対して重圧を感じているためと考えられます。この必要性は、セキュリティプロフェッショナルが別のデータブロックをクラウド（保存場所にすべきでないと考えている）に移行せざるを得ない場合に用いられる「くさび」となっています。

図 9：クラウド導入を再検討する要因：「セキュリティ」グループと「IT」グループの比較



「IT」グループの回答者 n=284
「セキュリティ」グループの回答者 n=66
出典：IHS Markit

結論：セキュアなクラウドを実現する方法の策定

クラウドは、避けることのできない事項であると思われ始めています。世界中の大部分の企業のテクノロジースタッフが、複数のクラウドアプリケーションの使用、評価、または開発に携わっています。クラウドが避けられないのと同じように、クラウドを理解することは簡単ではありません。クラウドは、半パブリックの共有インフラストラクチャで実行される、無限のアプリケーションと無限の導入モデルをサポートしています。セキュアなクラウド環境への移行を成功させるためには、適切な計画、スタッフ、パートナー、および組織内のサポートが不可欠です。しかしながら、本調査の結果やクラウドセキュリティソリューションの分析における私たちの経験に基づいて、動的なマルチクラウドへのスムーズな移行に役立つ助言を以下に提示します。

- 変化に対応できるように計画を立案します。クラウドの強みを真に活用するには、インフラストラクチャで使用しているツールおよびテクノロジーが機動性を備えている必要があり、複数のパブリッククラウド環境、プライベートクラウド、およびオンプレミスで機能することが重要です。
- 完了したプロジェクトと進行中のクラウドプロジェクトすべてを確認し、それらのプロジェクトが「クラウド優先」と「クラウドに対応」のどちらの領域に該当するか検証します。このプロセスは、該当するアプリケーションのセキュリティモデルに対する考えを整理するのに役立つほか、モデルの拡張や再活用も可能になります。
- ユースケース毎に、セキュリティに関する責任を組織内の DevOps スタッフ、IT セキュリティスタッフ、クラウドプロバイダー、セキュリティテクノロジーパートナーなど、すべての関係者でどのように共有するかを明示した、明確な計画を策定します。
- クラウドのテクノロジーチェーン（クラウドプロバイダーのプラットフォーム、オーケストレーションツール、既存のセキュリティ製品）において、どのような機能（特にセキュリティ）が組み込まれているかを常に監視します。セキュリティ機能は、顧客ロイヤルティを差別化し維持する方法として使用されることが多く、クラウド導入展開におけるセキュリティの継続的な強化の推進理由として活用することができます。
- 組織内のさまざまなグループ間の緊張を和らげるように努めます。クラウドの導入には、エグゼクティブ、事業部門、すべてのレベルの IT スタッフ、セキュリティスタッフの間で最大限の調整が必要となり、関係するこれらの人々すべてが、「ビジネス目標の達成」の意味することが人々の役割に応じて異なることを、適切に理解することが重要です。
- スタッフが抱えているセキュリティ上の懸念を深刻に受け止めながら、クラウドおよびクラウド導入展開に関する関心を企業のカルチャーとして育てるように努めます。サポートされているすべてのクラウドテクノロジー（そして特にセキュリティ）は急速に変化し、進化するため、「セキュリティ上の懸念が理由の No」を「Yes」に変更可能かどうか、絶えず見直す必要があります。

回答者および調査の概要

2019 年 3 月、当社が適格と判断した IT 意思決定者を回答者として、世界中の 350 社の企業を対象に Web 上で調査を実施しました。適格と判断されるためには、回答者は組織でクラウドおよびクラウドセキュリティ製品 / サービスの管理または計画を担当する、C レベルまたは VP レベルの意思決定者である必要があります。回答者の 65% が C レベル（CIO、CSO、CTO、CISO）であり、35% が VP レベル（IT 部門の VP、クラウドアーキテクチャの VP、IT セキュリティの VP）で構成されています。また、回答者は組織のクラウドおよびクラウドセキュリティ製品 / サービスについて詳しい知識を持っており、これらの購入決定に影響力を持っていることを必須条件としました。以下の表は、その詳細を示しています。

図 10：回答者に関する情報

国	回答者数	企業規模
米国	105	1,000 名以上
英国	35	500 名以上
フランス	35	500 名以上
ドイツ	35	500 名以上
オーストラリア	35	500 名以上
香港	35	500 名以上
ニュージーランド	35	500 名以上
シンガポール	35	500 名以上

出典：IHS Markit

この調査では、以下の 4 つの主なクラウドサービスモデルを使用して、ユーザー、顧客、またはパートナー向けにアプリケーション、データ、およびインフラストラクチャを提供する、企業のクラウド用途に重点を置いています。

- IaaS：Infrastructure as a Service では、データセンター（DC）施設、サーバー、ネットワーク、ストレージ、データベース、ネットワークアプリケーション（レイヤー 4 ～ 7）、管理機能が提供されます。
- CaaS：Cloud as a Service では、バンドルされたアプリケーション実行環境が提供され、それにはサーバー、ネットワーク、ストレージ、管理、オーケストレーションが含まれます。このサービスはバンドルとして購入され、価格は使用量に基づきます。
- PaaS：Platform as a Service では、アプリケーションの開発 / 実行環境が提供され、これにはアプリケーションミドルウェア（Web サーバー、データベース管理システム）、サーバー、ネットワーク、ストレージ、管理、オーケストレーションプラットフォームが含まれます。このサービスはバンドルとして購入され、価格は使用量に基づきます。
- SaaS：Software as a Service では、完全なアプリケーションが従量課金制の料金体系で提供されます。

クラウドおよびクラウドセキュリティの導入に関するエンドユーザーの見解を考察した本レポートは、フォーティネットの依頼によって実施した独自の調査レポートとして作成されました。IHS Markit は、本レポートおよび本レポートに記載されているすべての分析と内容について、全面的に責任を負います。本調査の実施時に使用された分析および測定の基準は、IHS Markit およびサイバーセキュリティテクノロジー担当上級リサーチディレクター Jeff Wilson の独自の視点によるものです。

お問い合わせ

Jeff Wilson
サイバーセキュリティテクノロジー担当上級リサーチディレクター
+1 408.583.3337
Jeff.Wilson@ihsmarkit.com

IHS Markit カスタマーケア：

CustomerCare@ihsmarkit.com
米国：+1 800 IHS CARE（+1 800 447 2273）
欧州、中東、アフリカ地域：+44 (0) 1344 328 300
アジアおよび環太平洋地域：+604 291 3600

WP-IHS-Cloud-201911-R1

IHS Markit™