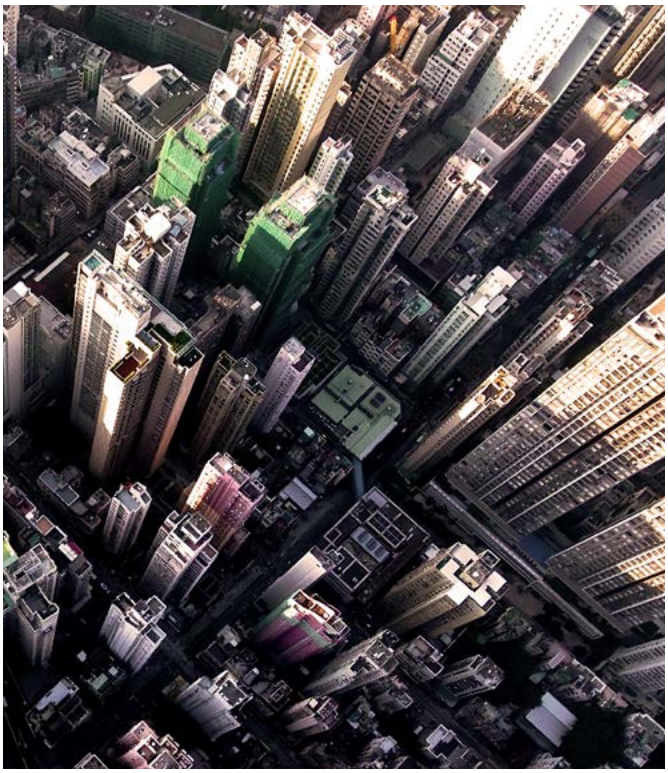

クラウドネイティブ
セキュリティ
ジャパンサーベイ 2021 年版
paloalto
NETWORKS

目次



はじめに

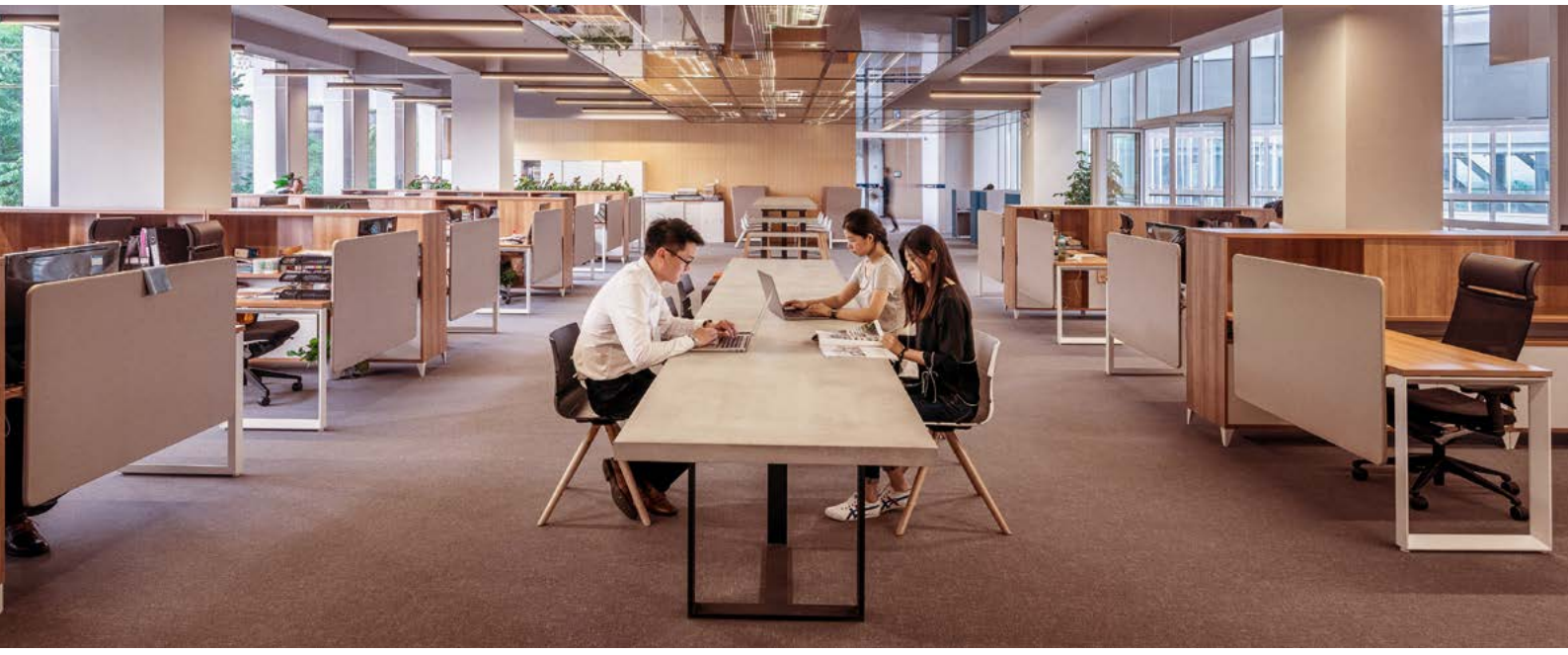
競争環境や顧客ニーズ、ビジネスにおける IT リソースの位置づけなど、企業を取り巻く様々な条件が変化する中で、国内でも企業や組織のクラウド移行が進行しています。

より妥当なコストで迅速かつ柔軟にコンピューティングリソースを活用できる手段として、クラウドは注目されています。近年では働き方改革に加え、新型コロナウイルス感染症の拡大に伴うテレワークの普及も重なり、どこからでもアクセスできるビジネスリソースの可用性が、これまで以上に重要視されています。

企業や組織の IT に対する考え方も、データセンターに構築した IT インフラとその環境で稼働するサーバーやアプリケーションを長期間所有し、継続的に利用・運用する形態から、必要な量だけ消費、稼働するという形態にシフトしています。また、アプリケーションライフサイクルマネージメントも、従来のウォーターフォール型からアジャイル型へと変化することで、機能拡張のスピードを上げる、市場のニーズに迅速に対応するといったスタイルに変化しています。

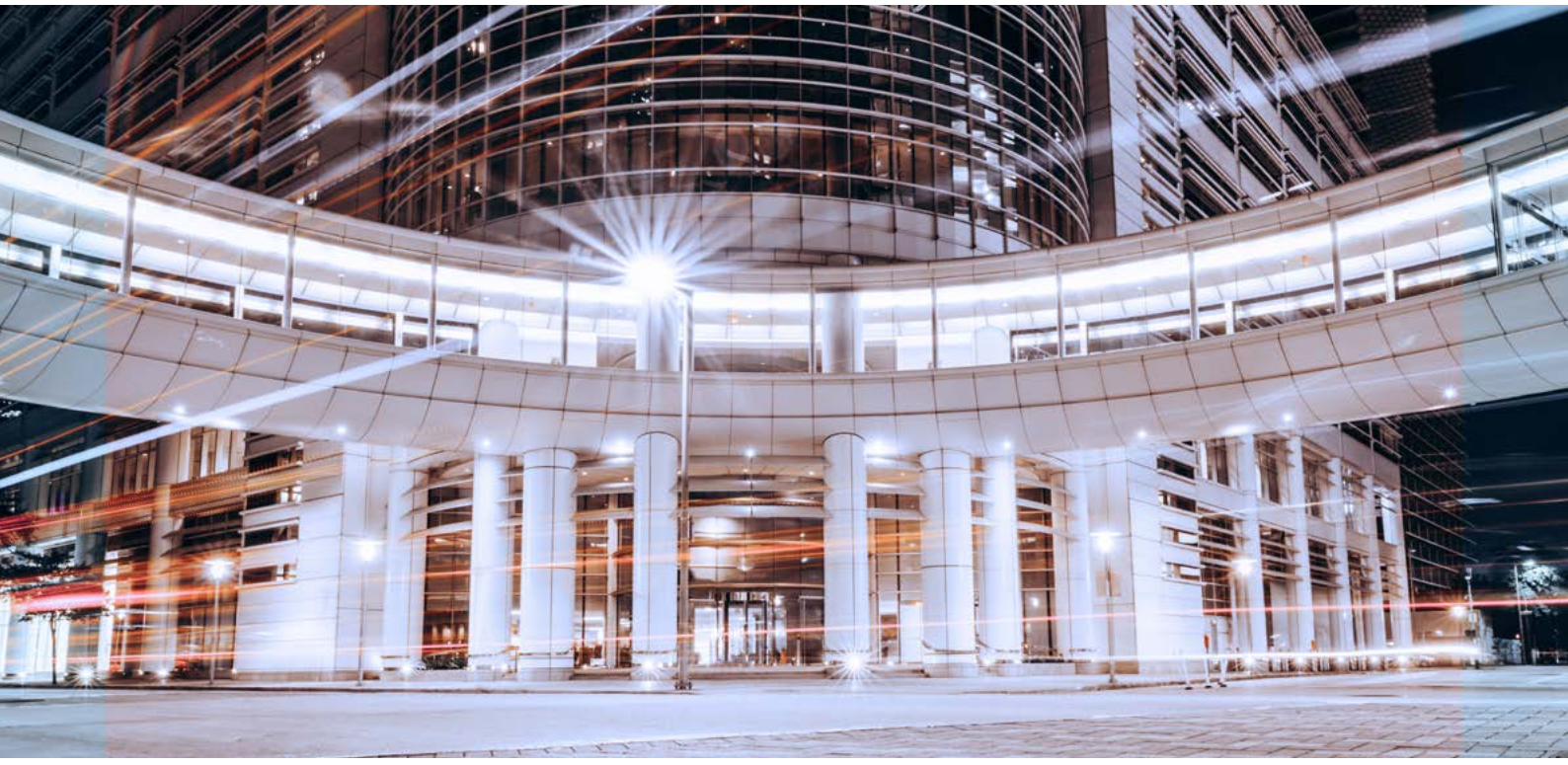
このように、クラウドには様々なメリットがありますが、移行にあたって企業や組織が直面する課題も少なくありません。特にセキュリティに関する問題は顕著で、すでにクラウド上で様々なセキュリティインシデントが発生しています。パロアルトネットワークスが調査した結果、国内外のクラウド上での情報漏えい事故の 65％は、クラウドインフラの設定ミスに起因している [1] ことが分かっており、多くの企業がクラウド特有のセキュリティ要件を課題としている様子が浮き彫りになっています。

サイバーセキュリティのリーディングカンパニーであるパロアルトネットワークスでは、国内民間企業のクラウド活用の現状や課題、セキュリティ対策の現状や課題について 2021 年 4 月に調査を実施しました。「クラウドネイティブセキュリティジャパンサーベイ 2021 年版」では、国内企業の取り組みや課題、今後の展望を明らかにすることができました。また、2020 年に実施した「クラウドネイティブセキュリティの状態 2020」[2] を基に、海外企業のクラウド利用やセキュリティ対策との比較をすることで、クラウドをすでに活用している組織、今後クラウドを計画している組織の一助になることを期待しています。



調査概要

調査名	**クラウド ネイティブ セキュリティ ジャパンサーベイ 2021 年版**	
目的	国内企業のクラウドの活用や投資の現状と、サイバーセキュリティの取り組みや課題を明らかにする。	
調査対象 (単位 : 名)	国内民間企業において、クラウド上でのアプリケーション開発やシステム運用、セキュリティ対策に従事する意思決定者ならびに現場担当者 400 名	
	売上高別	• 5,000 億円以上 : 172 • 1,000 ～ 4,999 億円 : 100 • 500 ～ 999 億円 : 66 • 100 ～ 499 億円 : 55 • 99 億円以下 : 7
	従業員規模別	• 10,000 名以上 : 156 • 5,000 ～ 9,999 名 : 50 • 1,000 ～ 4,999 名 : 142 • 500 ～ 999 名 : 40 • 499 名以下 : 12
	役職別	• 経営者・CxO: 4 • 執行役員・本部長 : 13 • 部長・課長 : 177 • 主任・チームリーダー : 146 • 現場担当者 : 60
手法	インターネット調査	
実施時期	2021 年 4 月 22 日～ 25 日	



エグゼクティブサマリー

The State of the Cloud and Cloud Native Adoption

クラウドとクラウド ネイティブ活用の現状

日本でも海外同様、今後 24 か月でクラウドがコンピューティング モデルの主流に

- 現在クラウド上で稼働するワークロードの割合は平均で 43%
- 今後 24 か月で平均 60% に到達すると予想される

クラウドワークロードのホスト環境では、主にパブリッククラウドを利用する企業が最多

- ワークロードの 60% 以上をパブリッククラウドで稼働させる企業が最多の 40%
- 海外はパブリックとプライベートを半々ずつ活用する企業が最多で 57% を占める
- 年間売上高や投資額が多いほどプライベートや混在へシフトする傾向がある

クラウドへの投資額は二極化

- クラウドを本格活用している企業とそうでない企業で投資額は二極化する傾向
- 国内ではクラウド投資額が 10 億円未満の企業が 47% と最多

国内企業もマルチクラウドにシフト

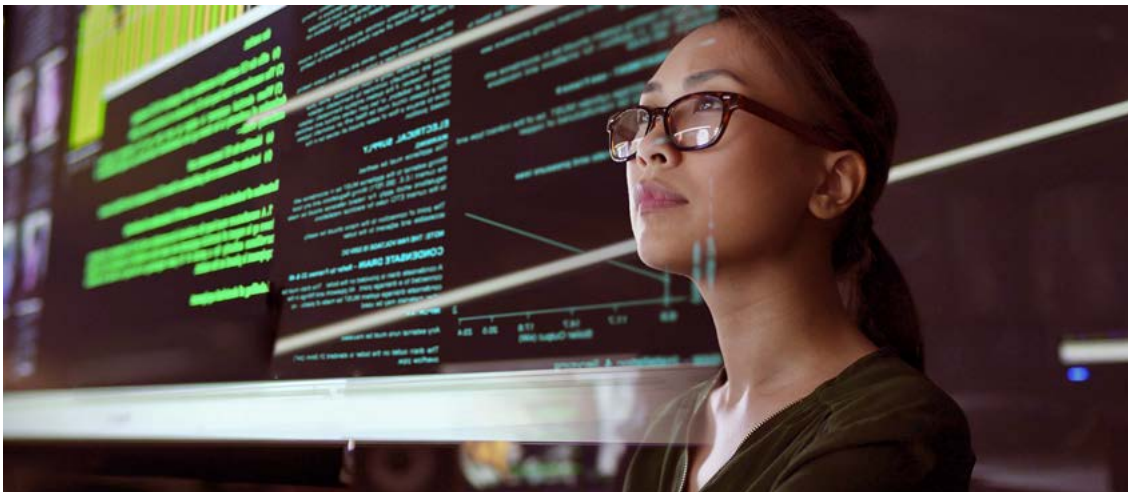
- 国内企業は平均で 2 つのサービスを活用
- 複数のクラウドサービス事業者 (CSP) を利用する企業が 59% でマルチクラウド化の傾向は明らか
- 最も活用されている CSP は Amazon Web Services (AWS)

仮想マシンは現在のコンピューティングオプションの主流

- 現時点のコンピューティングオプションは仮想マシンが 47% で圧倒的大多数を占める
- 今後 24 か月では 90% 以上の企業がコンピューティングオプションを現状維持か増加と予想

クラウド移行の最大の課題はセキュリティ確保

- 53% の企業が「包括的なセキュリティの確保」を最大の課題とみなしている
- 年間売上高・従業員の大きい企業ほどコンプライアンスや変更管理を懸念
- 年間売上高・従業員の小さい企業は人材不足を課題とする傾向



The State of Securing the Cloud and Cloud Native Workloads

クラウドとクラウドネイティブワークロードのセキュリティの現状

企業のクラウド環境にとっての最大の脅威は「情報流出」

- 45% の企業が「情報流出」を最大の脅威と考えている
- 上位 3 つは「情報流出」「マルウェア」「アプリケーションの脆弱性」で海外企業と同じ
- 国内企業は特に情報流出にセンシティブな傾向

セキュリティ確保の最大の課題は「可視性の欠如」

- 27% の企業が「可視性の欠如」を最大の課題と考えている
- 上位 3 つは「可視性の欠如」「予算の確保」「自動化」

クラウドセキュリティ確保のための人材・セキュリティツールは海外と比較して不足傾向

- 海外は 77% 以上の企業が 21 名以上の担当者を確保している
- 自社のクラウド環境のセキュリティ確保にあたる人材が 21 名以上の国内企業は 48% のみ
- クラウドセキュリティに従事する人数を「10 名以下」とした企業は 32% を占める

クラウド投資に積極的な企業ほどクラウドセキュリティ投資にも積極的

- クラウド予算全体に占めるセキュリティ投資の割合が「0 ～ 10%」の企業が 42% と最多
- 「クラウド投資全体の 16% 以上をセキュリティに投資している企業」
  - 日本では 35%
  - 海外では 26%

クラウド・セキュリティの最重要課題は「データ保護」

- 最重要課題を「データ保護」「脆弱性管理」とした企業がそれぞれ 23% で最多
  - 「データ保護」「脆弱性管理」がセキュリティの優先投資対象となると予想される

クラウドセキュリティベンダーに求める絶対的要件は「マルチクラウド、ハイブリッドクラウド対応」

- 43% の企業が「マルチクラウド、ハイブリッドクラウドへの対応」を絶対要件と捉える
  - クラウド投資額や活用プラットフォームの多い企業ほどマルチクラウド・ハイブリッドクラウド対応の要件を絶対条件と考える傾向がある
- コンピューティングオプションの多様化とともに、一元的管理への要望は高くなる

The State of the Cloud and Cloud Native Adoption

クラウドとクラウド ネイティブ活用の現状

近年、国内においても民間企業のクラウド移行は進んでおり、より妥当なコストで迅速かつ柔軟にコンピューティングパワーを活用できる手段として注目されています。国内でのクラウド活用は、民間企業にとどまりません。システム利用においてはクラウドを第 1 候補とする「クラウド・バイ・デフォルト原則」が政府から発表[3]され、クラウドベースの政府共通プラットフォームの稼働が始まるなど、公共の分野でもクラウド利用が加速すると予測されています。クラウドは企業や組織にとって必要不可欠な IT リソースとなっています。

このセクションでは以下の調査結果を見ていきます。

- 国内企業によるクラウドの活用状況
- 国内企業が採用しているクラウドの種類と数
- 国内企業が使用しているコンピューティングオプション
- 国内企業のクラウド移行におけるセキュリティ上の課題

クラウド活用は国内でも加速

国内企業でのクラウド活用は加速しており、今後も一層進むものと考えられます。すでにクラウドを活用している国内企業は、企業のワークロード全体の 43%をパブリッククラウド上で稼働しており、海外企業の 46%と比較しても差はありません。また、パブリッククラウド上で稼働するワークロードの割合は、今後 2 年間で企業のワークロード全体の 60%に達すると予測しており、海外企業の 64%と比較しても大きな差はありません。

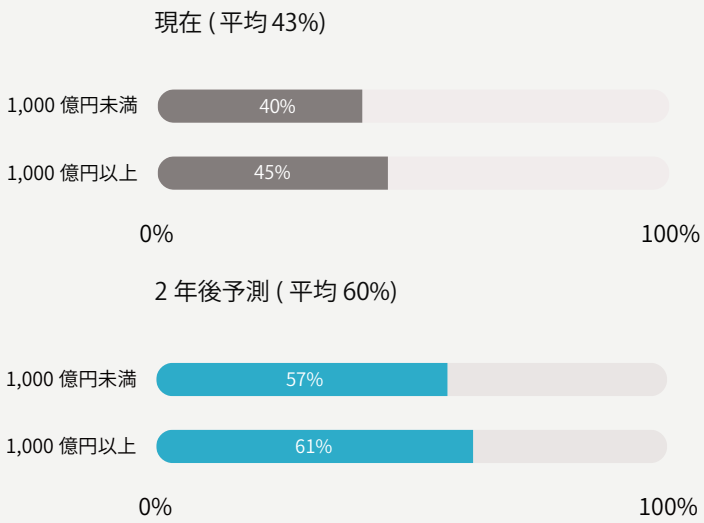
クラウド上のワークロードの割合

50%を超えるワークロードをクラウドで稼働している企業は、現時点では 46%になりますが、2 年後には 50%を超えると回答する企業は 72%にも上ります。クラウド上のワークロードの増加予測は、現時点で何らかのビジネスメリットを享受できていることを証明するものと言えます。ビジネス環境の変化に対応し、より迅速に顧客のニーズに応える、業務スピードを変革し競争優位性を確立する上で、クラウドが有益な手段であることを裏付けるものです。

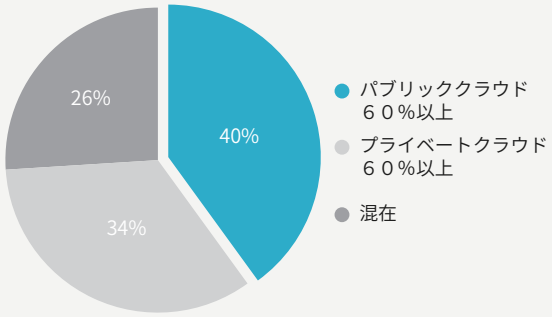
ワークロードのホスト環境内訳

ワークロードをホストしている環境の内訳を見てみると、60%以上のワークロードをパブリッククラウドにホストしている企業が 40%と最も多い結果となっています。これは、パブリッククラウドとプライベートクラウドを半々ずつ活用する企業が 57%を占める海外企業の結果とは大きく異なります。年間売上高やクラウド投資額が高くなるほど、60%以上をプライベートクラウド、あるいはパブリッククラウドとプライベートクラウドで半々という企業の割合が高くなる傾向があります。

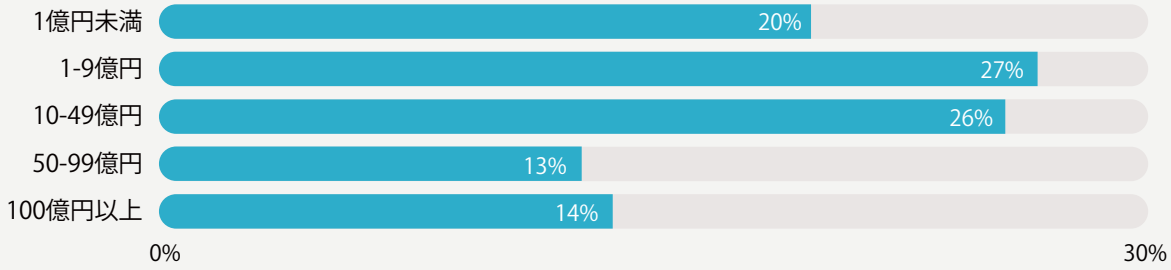
クラウド上で稼働するワークロードの割合 (企業売上別 n=400)



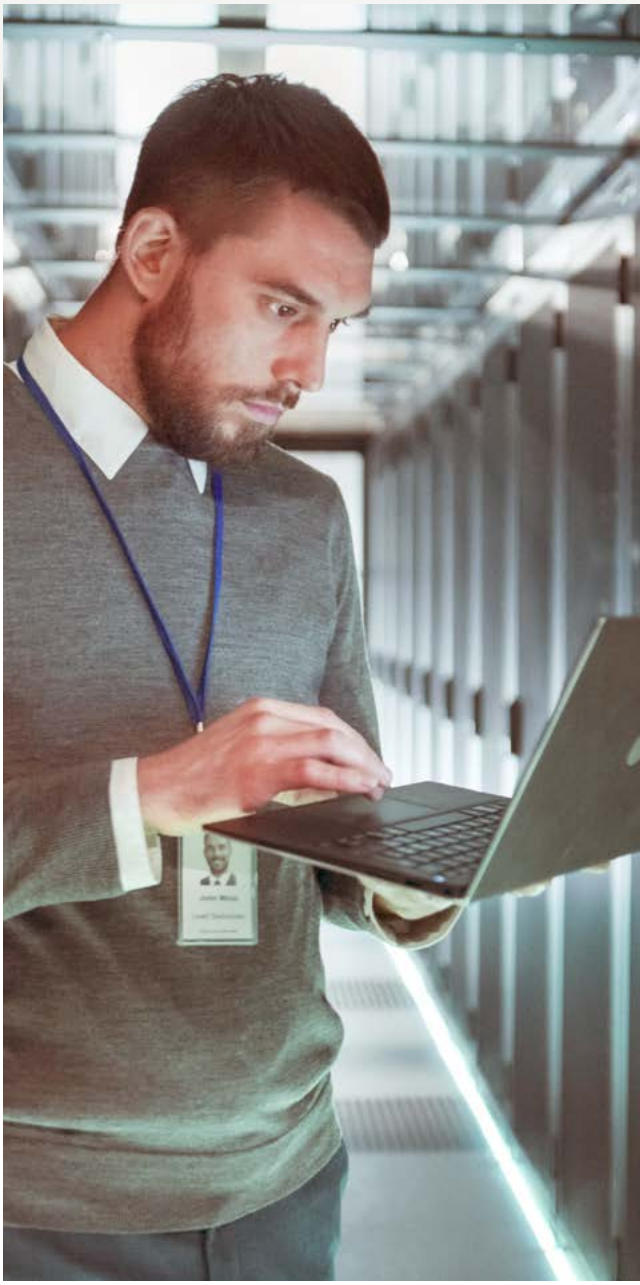
ワークロードのホスト環境内訳 (n=400)



クラウド投資額（n=229）



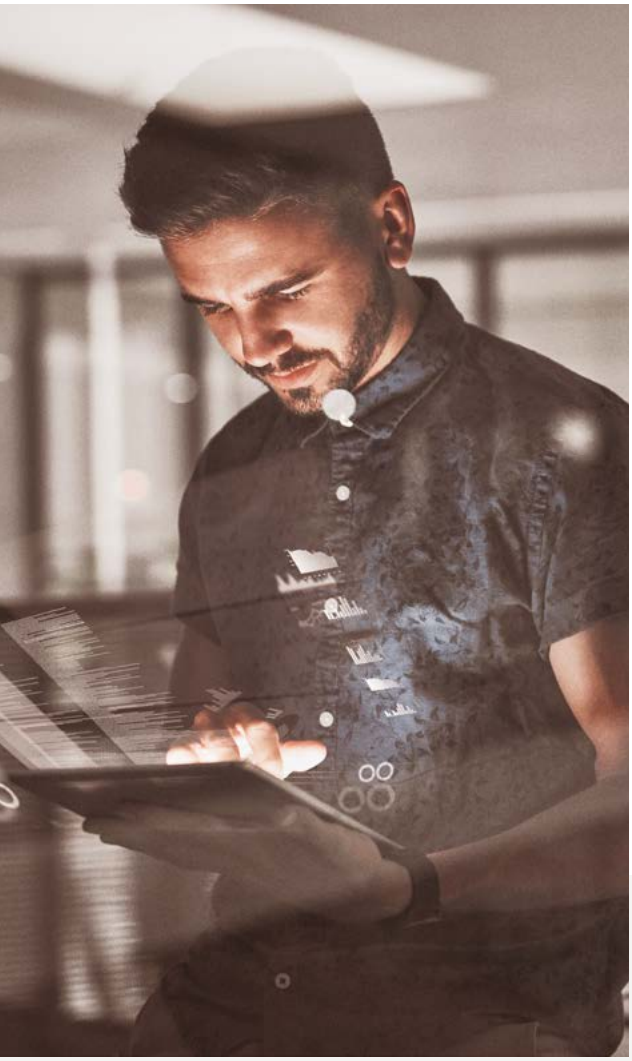
クラウドを本格活用している企業とそうでない企業で二極化している可能性がある



クラウドへの投資額

クラウド移行が加速していることは間違いない一方で、国内企業のクラウドへの絶対的な投資額は、海外と比較すると決して多くはありません。クラウド投資額が 50 億円未満の海外企業は 56%の一方で、国内企業は 73%にも上ります。全体的には 10 億円未満が 47%と最も多く、年間売上高 1,000 億円未満の企業では 74%と特に顕著です。

絶対的な投資額は事業規模などとも大きく関係するため一概には言えませんが、クラウドを本格的に活用している企業とそうでない企業で二極化している可能性が考えられます。IT 投資全般、セキュリティ投資にも言える傾向かもしれませんが、クラウドを「戦略的投資」ではなく「コスト」として考えている企業も依然として相当数あるものと考えられます。クラウドをどのようにビジネスの戦略的 IT リソースとして位置づけるかが、これからの国内企業のテーマといえるかもしれません。



国内企業もマルチクラウドにシフト

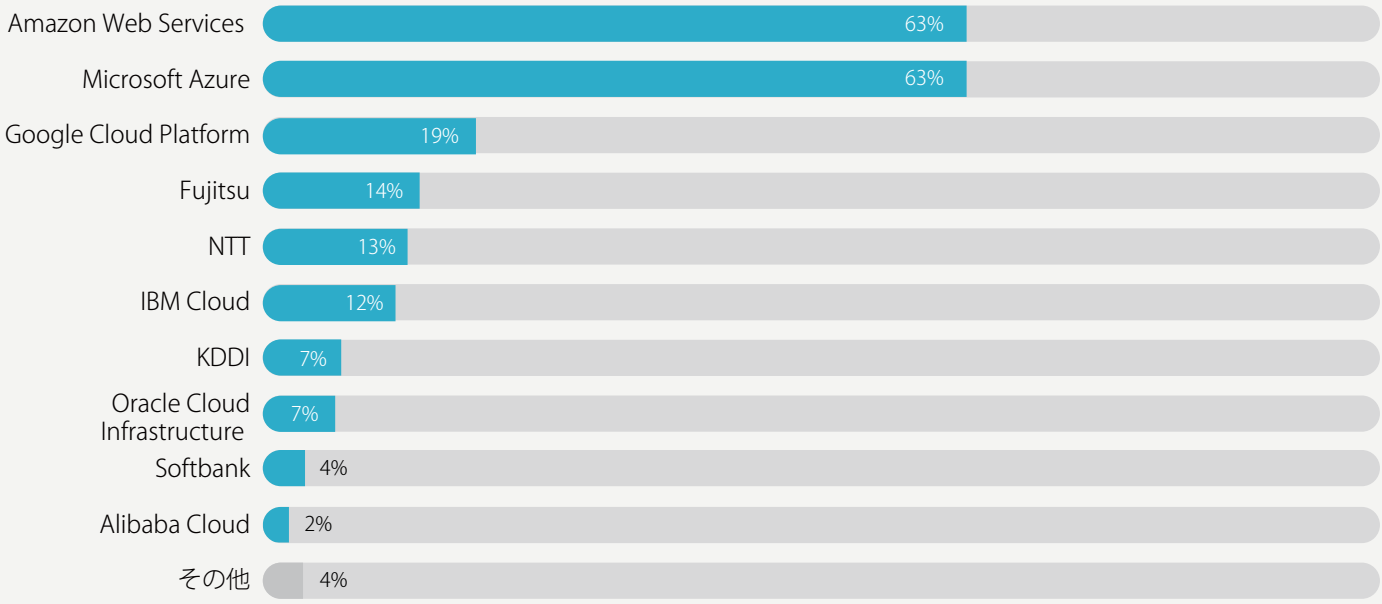
企業が IaaS プラットフォームとして活用しているクラウドサービス事業者（CSP）を見てみると、平均で 2 つのサービスを活用しています。複数の CSP を活用している企業は 59％にも上り、国内でも単一の CSP を活用するシングルクラウドから、複数の CSP を活用するマルチクラウドにシフトし始めていることが分かります。

企業で活用されている個々の CSP で見てみると、国内のクラウド移行を牽引してきた Amazon Web Services（AWS）が最も広く活用されています。しかしながら、Microsoft Azure も同率で活用され、Google Cloud Platform（GCP）が続き、これらの CSP がマルチクラウド化を結果的に牽引していることがうかがい知れます。今後は、国内においてもさらなるマルチクラウド化が進んでいくものと予測されます。

国内で活用されている CSP トップ 5

1. Amazon Web Services
2. Microsoft Azure
3. Google Cloud Platform
4. Fujitsu
5. NTT

クラウドサービスの内訳 (n=400)



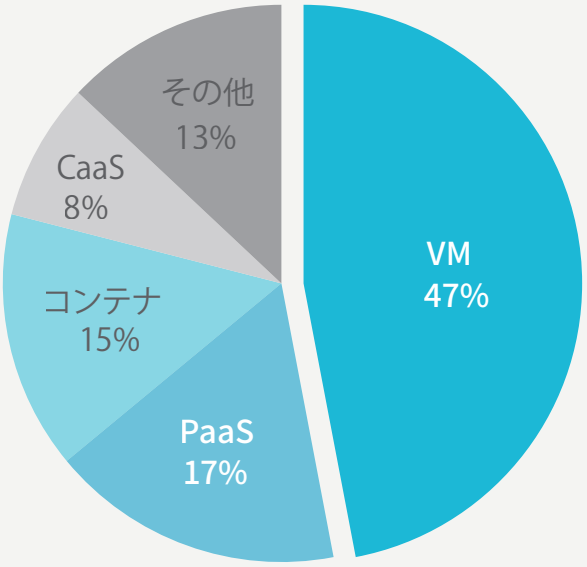
コンピューティングオプションは仮想マシンが主流

クラウドを活用するにあたっては、従来の仮想マシンに加えて、コンテナ、CaaS（Container as a Service）、サーバーレス、PaaS（Platform as a Service）など様々なコンピューティングオプションがあり、それぞれ異なる特徴を持っており、特に運用面において異なるメリットをもたらしてくれます。

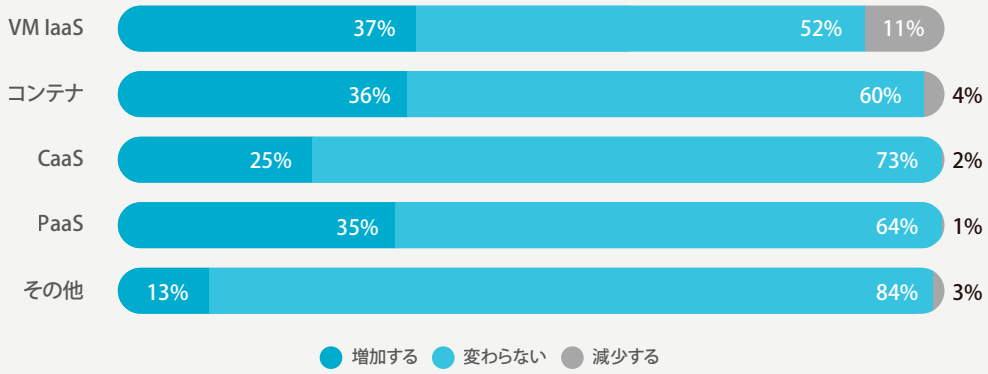
国内企業が活用するクラウドのコンピューティングオプション比率を平均的に見てみると、コンテナ、CaaS、サーバーレス、PaaS などの選択肢と比較して、仮想マシンの比率が 47％と圧倒的に高いことが分かります。この結果は、様々なコンピューティングオプションが同比率となっている海外企業の分散型の結果とは大きく異なっています。新しい選択肢を積極的に活用する海外企業と、そうではなく従来データセンターで稼働していたものの場所変え的な位置づけや、新しい選択肢の採用に慎重な国内企業の考え方や取り組みの違いと見ることもできます。

一方で、仮想マシン、コンテナ、CaaS、PaaS それぞれの活用度合は、概ね約 30 ～ 40％が今後 2 年間で増加、変わらないを含めると 90％以上が増加か変動なしと回答していることからも、利用するコンピューティングオプションに違いはあれど、クラウド活用は一層加速することが予測されます。逆に、今後クラウド活用が一層進むと同時に、コンテナや CaaS、サーバーレス、PaaS の利用も海外同様に増加するものと予測されます。

活用しているコンピューティングオプション内訳 (n=400)



コンピューティングオプションの使用状況が今後 24 か月でどのように変化すると予想しますか？

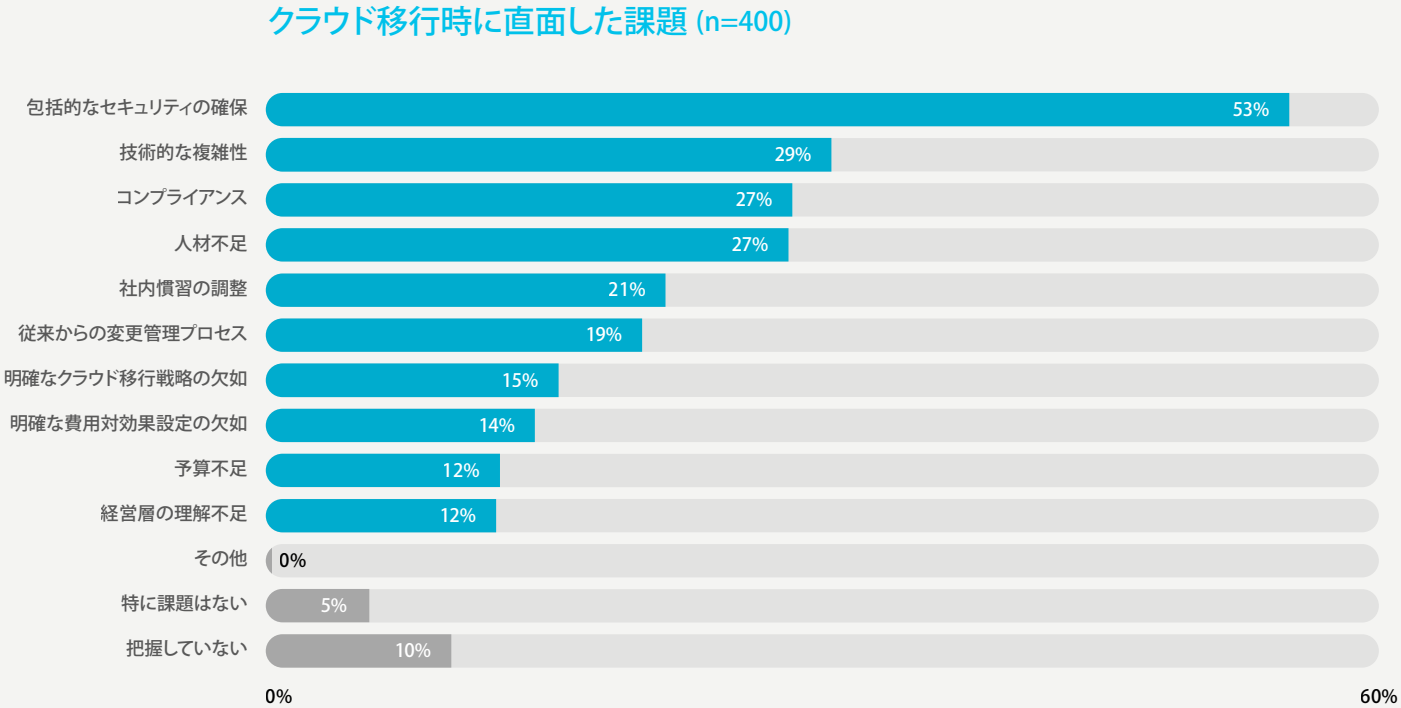


クラウド移行にあたっての最大の課題はセキュリティの確保

クラウドを活用する企業は、コンピューティングリソース活用の柔軟性、コスト削減、ビジネス俊敏性、そしてリモート環境からのビジネスリソースの可用性など、様々なメリットを享受するためにクラウドを活用しています。しかしながら、従来オンプレミスのデータセンターにあったワークロードをクラウドに移行するにあたっては、多くの企業が困難に直面しています。

たとえば、「技術・組織・プロセスの面でなんらかの課題に直面した」と回答した企業は 85% にのぼっています。中でも最大の懸念は「包括的なセキュリティの確保」で、全体の 53%と過半数を超える企業がセキュリティを最大の課題として挙げています。「技術的な複雑性」（29%）、「コンプライアンス」（27%）といった課題をはるかに超える結果となりました。

全体的な傾向としては、年間売上高別、従業員別、クラウド稼働率別などの様々な観点で見ても、課題の順位には大きな差異はありません。しかし、割合で見てみると、年間売上高や従業員数が多い企業は、コンプライアンスや従来からある変更管理プロセスの存在を課題として挙げる割合が高く、逆に少ない企業ほど人材不足を課題として挙げる傾向がやや強いことが分かっています。事業規模や組織の特徴が、クラウド利用に影響を及ぼしていることがわかります。従来のデータセンターとクラウド環境での開発プロセスの違い、セキュリティに対する考え方や実装方法の違いも、大きな要因として考えられます。



The State of Securing the Cloud and Cloud Native Workloads

クラウドとクラウドネイティブワークロードのセキュリティの現状

企業は俊敏性や柔軟性を求めてクラウドを採用していますが、特に多くの企業が「包括的なセキュリティの確保」を課題と考えています。この課題を解決するには、従来のデータセンターや開発プロセスのセキュリティとは異なるクラウドネイティブなアプローチが求められます。

クラウドネイティブなアプローチとは、クラウドの特性や利点を活かす形で最適化されていることを意味しています。クラウドサービス事業者はハードウェアなどのセキュリティを提供する一方で、その上で稼働する仮想マシン、コンテナ、ストレージなどのセキュリティ確保は、利用する企業の責任となります。またネットワーク、リソースの設定、アクセス権限など、利用する企業が自ら対策を講じる必要がある領域は多岐にわたります。

このセクションでは以下の調査結果を見ていきます。

- 企業のクラウド環境にとって最大の脅威
- セキュリティ確保における最大の課題
- クラウドのセキュリティ確保に当たる人材数、セキュリティツール数
- クラウド投資で見られた傾向
- クラウドセキュリティの最重要課題
- クラウドセキュリティベンダーに求める絶対的要件

企業のクラウド環境にとって最大の脅威は情報流出

驚くべき結果ではありませんが、クラウドを利用する企業の多くは、自社のクラウド環境が直面する最大の脅威は「情報流出」であると回答しています。全体の 45％が情報流出を懸念しているという突出した結果になりました。次いで「マルウェア」「アプリケーションの脆弱性」となっており、上位 3 位は海外企業と同様の結果になりました。海外企業と比較して国内企業は情報流出に特にセンシティブな傾向があり、報道による影響が特に大きいものと考えられます。

情報流出には大きく分けてサイバー攻撃や内部犯行によるものが存在しますが、クラウドにおいては設定ミスや不備といったものが情報流出につながる危険性があります。ストレージが公開設定になっている、アカウント管理やアクセス権限の不備といった問題が、情報流出のリスクにつながってしまいます。サイバーリスクの結果として発生する情報流出などの事象は、もちろん懸念すべき点ではありますが、事故につながる原因となるクラウド特有の課題に目を向けることが重要と言えます。

45%

**の調査回答者は、
最大の脅威は
情報流出であると答えています**

セキュリティ確保における最大の課題は可視性の欠如

自社のクラウド環境のセキュリティを確保する上での最大の課題は、「クラウドアプリケーションに存在する脆弱性の可視性の欠如」（27％）が最も多く、「セキュリティ予算の確保」（13％）、「反復的なセキュリティ対応の自動化」（13％）と続いています。自社のクラウド環境にとっての最大の脅威としても、アプリケーションの脆弱性は 3 番目に上げられています。

クラウド全体で稼働しているアプリケーションの状態をどのように可視化して対処に結び付けるのかが、クラウド利用する企業、マルチクラウド化するインフラにおいての喫緊の課題と言えます。

27%

**の調査回答者は、
最大の課題は
可視性の欠如であると答えています**

クラウド環境における セキュリティの脅威・懸念（n=400）

1	情報流出	45%
2	マルウェア	12%
3	アプリケーションの脆弱性	10%
4	インフラ環境の誤設定	7%
5	アカウント情報流出	6%
6	内部脅威	6%
7	アクセス設定の不備	5%
8	アプリケーションの誤設定	4%
9	安全性に問題のある API	3%
10	認証の不備	3%
11	その他	0%

クラウド環境のセキュリティ確保に あたっての課題（n=400）

1	可視化の欠如	27%
2	予算の確保	13%
3	セキュリティ対応の自動化	13%
4	セキュリティツールのインテグレーション	11%
5	セキュリティの現状評価	10%
6	安全な運用に関するトレーニング	8%
7	セキュリティ レポーティングツール	8%
8	ツールに関するトレーニング	5%
9	経営層の理解	5%
10	その他	1%

48%

自社クラウド環境のセキュリティ確保に
関わる人材が 21 人以上の企業

32%

クラウドセキュリティに従事する
人数が 10 人以下の企業

60%

1-5 社のセキュリティベンダーを
活用する企業

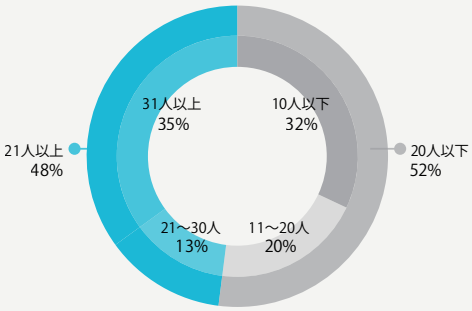
クラウドのセキュリティ確保に当たる人材とセキュリティツールは海外と比較して不足傾向

サイバーセキュリティの分野においては、セキュリティ人材の慢性的な不足が国内外で問題視されています。自社のクラウド環境のセキュリティ確保に関わる人材が 21 人以上いる企業は 48%と、海外の 77%と比較して決定的に少ないことが分かりました。従業員規模や事業規模と直接的に関係するため一概には言えませんが、クラウドセキュリティに従事する人数として最も多いのが 10 人以下で全体の 32%を占めています。今後クラウド投資が一層進むことで、国内全体的にはクラウドセキュリティに従事するエンジニアの絶対数が増加することが期待される一方で、ユーザー企業で従事するエンジニアが不足する懸念も考えられます。

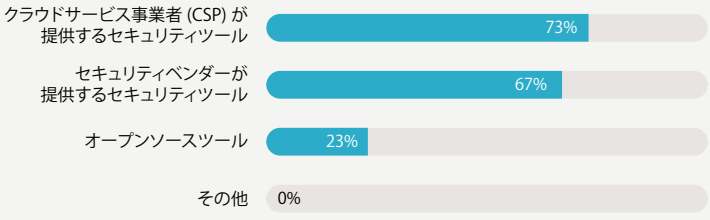
クラウド環境のセキュリティ対策を実施するにあたり、60%の企業が 1 ～ 5 社のセキュリティベンダーを活用しており、海外平均の 42%を大幅に上回っています。活用するクラウドセキュリティツールの数も 1 ～ 5 個が 52%と最も多く、海外企業の 43%と比較しても高い傾向にあります。CSP が提供するプラットフォームネイティブなツールを活用している企業は 73%、次いでセキュリティベンダーが提供するツールを活用する企業が 67%と、ここは海外平均と比較しても大きい違いは見られませんでした。一方、オープンソースツールを活用する企業は僅かに 23%と、海外企業の 62%と比較しても圧倒的に低いことが分かります。また、2 つ以上の種類のツールを使っているのは全体の 50%と、海外企業の 75%と比較しても大きく異なります。

マルチクラウド化が進み始める中で、CSP が提供するネイティブなセキュリティツールのみを活用する、あるいは CSP 提供ツールを補完する位置づけてセキュリティベンダーのツールを活用している企業が圧倒的に多いと考えられます。一方で、オープンソースツールなども駆使してクラウドネイティブな開発環境を最大限に活用できている企業は、現時点では少数派とみることができます。

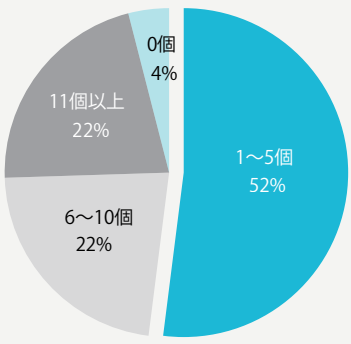
クラウドセキュリティ チームの人材数 (n=400)



活用しているクラウドセキュリティ ツールの種類 (n=384)

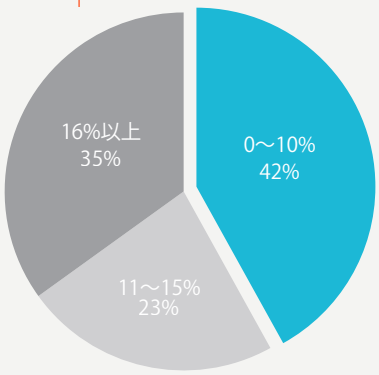


活用しているセキュリティ ツールの数 (n=400)

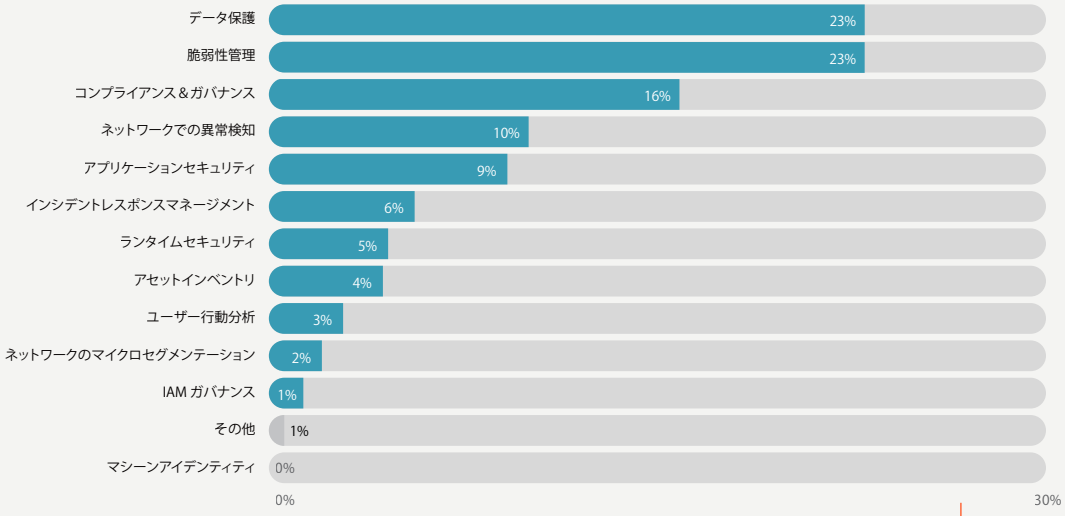


クラウド予算全体に占めるセキュリティ投資の割合は、0 ～ 10% の企業が 42%と最も多い

クラウド投資に占める セキュリティ投資の割合 (n=229)



クラウドネイティブなアプリケーションの セキュリティ確保における最優先事項 (n=400)



「データ保護」と「脆弱性管理」をそれぞれ 23% の企業が最優先課題と考えている

クラウド投資に積極的な企業ほどクラウドセキュリティ投資も積極的

クラウドへの絶対的な投資額が多い企業は決して多くはない中で、クラウド上のワークロードのセキュリティに対しては、どれだけの投資をしているのでしょうか。クラウド予算全体に占めるセキュリティ投資の割合は、0 ～ 10%の企業が 42%と最も多い結果になっています。

一方で、全体の 35%がクラウド投資全体の 16%以上をセキュリティに投資しており、この数値は海外企業の 26%と比較して突出していると言えます。特に、クラウド投資額が 50 億円を超える企業の場合は、60%以上がクラウド投資額の 16%以上をクラウドセキュリティに対して投資していることが分かります。

クラウドセキュリティの最重要課題はデータ保護

クラウドネイティブなアプリケーションのセキュリティ確保における最優先課題は、「データ保護」と「脆弱性管理」が最も多く、それぞれ 23%が課題として上げています。情報流出を最大の脅威、アプリケーションの脆弱性の可視性の欠如を最大の課題として上げていることからも当然の結果と言えますが、クラウド環境のセキュリティ強化の中では、国内企業はこれらの領域への投資を優先的に行うと考えられます。マルチクラウド上に散在する様々なデータ、そして稼働する様々なアプリケーションを一元的に可視化して保護、対処することの重要性を浮き彫りにしているといえます。

クラウドセキュリティベンダーに求める絶対的要件は「マルチクラウド、ハイブリッドクラウド対応」

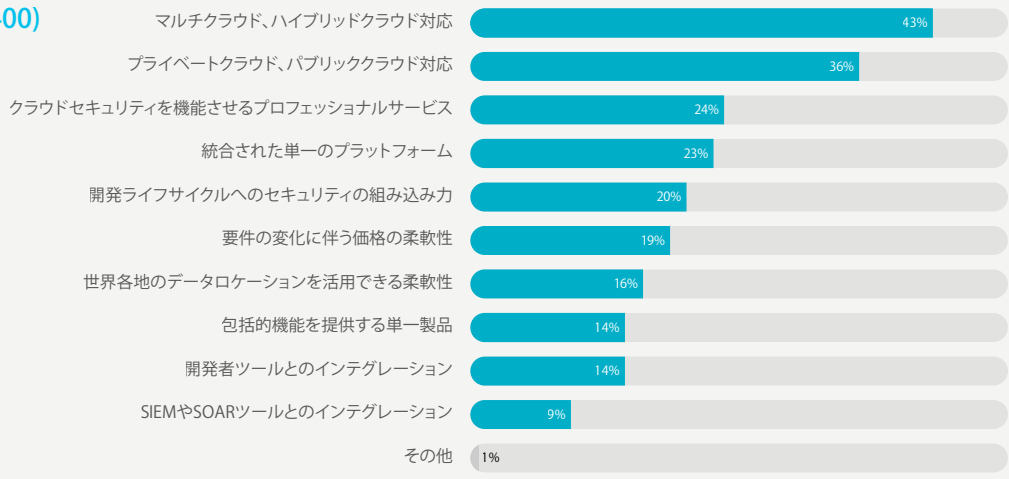
クラウドによって開発サイクルへの考え方や設定管理や可視性の重要度が変わり、マルチクラウドによってその管理、運用は一層複雑なものになります。単にセキュリティファンクションを活用できるだけでなく、それがどのような形で提供されるか、どれだけクラウドネイティブな形で提供されるかは、クラウドを運用・管理するエンジニアにとって重要です。

クラウドを活用する企業がクラウドセキュリティベンダーに求める絶対的な要件を聞いてみると、「マルチクラウド、ハイブリッドクラウド対応」が43%と半数近くを占めています。マルチクラウド、ハイブリッドクラウド対応への需要は、他の要件と比較して全体的に高い傾向にありますが、特にクラウド投資額や活用プラットフォーム数が多い企業ほどその傾向は強くなります。

クラウド環境の保護を実現するセキュリティファンクションには、ワークロードを脅威から保護するCWPP（Cloud Workload Protection Platform）、ワークロードの態勢管理やコンプライアンスを実現するCSPM（Cloud Security Posture Management）、ワークロード横断でアクセス権限の最適化をするCIEM（Cloud Infrastructure Entitlement Management）、ワークロード間の通信の保護やマイクロセグメンテーションを実現するCNS（Cloud Network Security）など様々なものがあります。CSPが提供するセキュリティツールやオープンソースツールには、個別のセキュリティファンクションを提供するものが多数ある中で、マルチクラウド化する企業がセキュリティベンダーに求める要件は明確です。

ワークロードがマルチクラウドでの稼働にシフトし、各クラウドサービス上で稼働する仮想マシン、コンテナ、サーバーレスとコンピューティングオプションも多様化し、それぞれの設定管理や脆弱性の可視化が課題になる中で、一元的なセキュリティ管理の必要性に気付き、その実現を求める企業が多いと言えます。

クラウドセキュリティベンダーが提供すべき絶対的要件 (n=400)



クラウドネイティブセキュリティプラットフォームの必要性

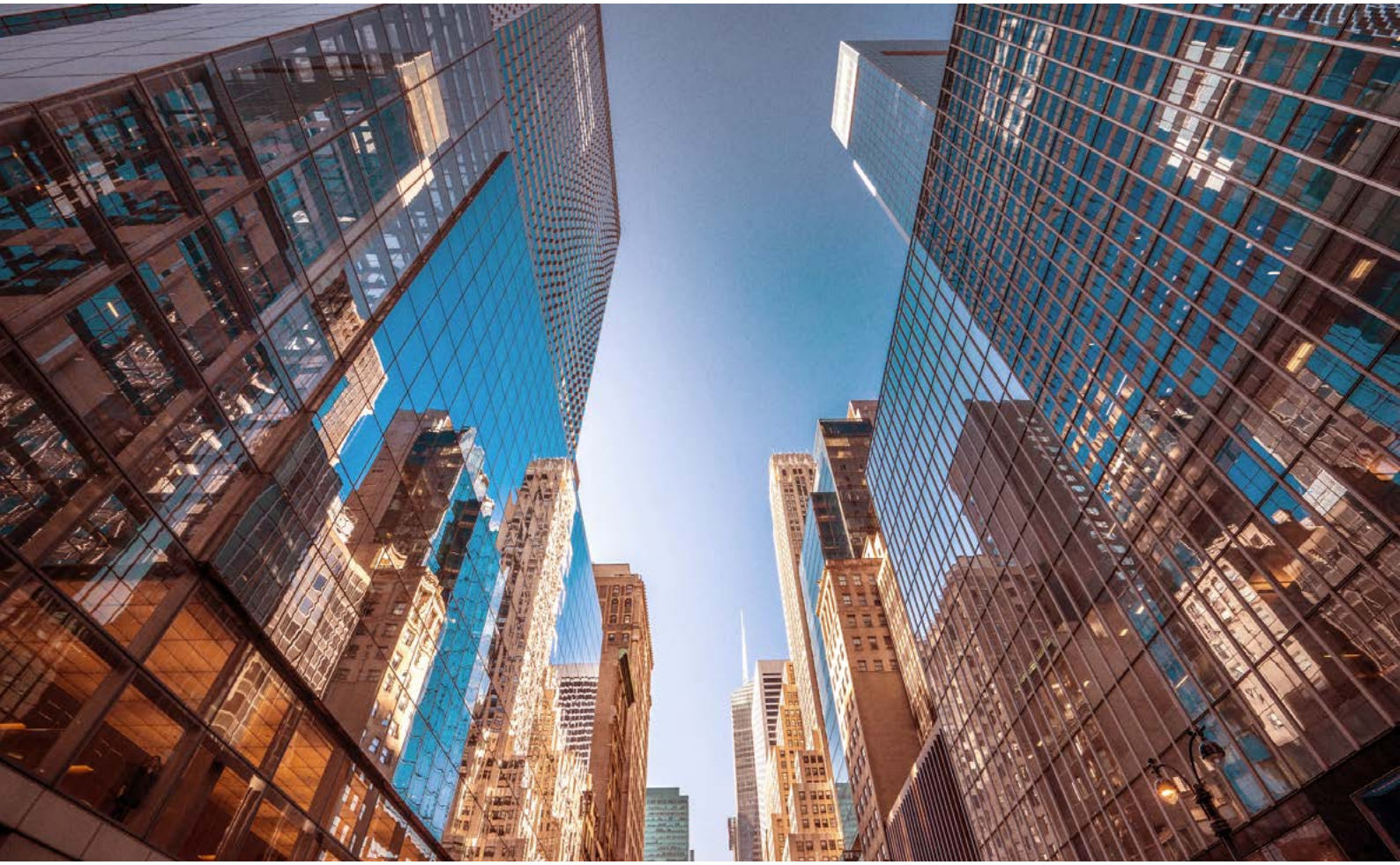
海外と比較して国内ではクラウド利用が数年遅れている点は、これまでに幾度となく指摘されてきました。今回の調査でも、その傾向は依然として継続しています。

ただし、国内企業のクラウド移行、マルチクラウド化は確実に進み始めており、企業のワークロード全体に占めるクラウドの割合も確実に増加すると予測されます。

その一方で、クラウド上のワークロードが単に増加するだけでなく、マルチクラウド環境に分散し、技術的な複雑性が増加することで、企業は活用している CSP やコンピューティングリソースの種類に関係なく一貫したセキュリティ確保の実現を求めています。

そうした企業の要望を満たすには、個別に対策を提供するタイプのセキュリティファンクションでは不十分です。

マルチクラウド上のワークロードを統合された 1 つのプラットフォームでサポートするクラウドネイティブセキュリティプラットフォーム（CNSP、Cloud Native Security Platform）が不可欠になるでしょう。



提供：

パロアルトネットワークスが提供するクラウドネイティブセキュリティプラットフォーム Prisma Cloud は、CWPP、CSPM、CIEM、CNS などのマルチクラウド環境で求められるセキュリティファンクションを 1 つのプラットフォームで提供するソリューションです。このようなセキュリティプラットフォームを活用することで、マルチクラウド上の広範なコンピューティングリソースの監視や保護、オートスケールや CI/CD ライフサイクルに対応したセキュリティ確保、アクセス権限の効率的な管理、ネットワーク通信の保護をクラウドネイティブな形で実現することができます。

Twitter で @Prisma_Cloud をフォローするか、
https://www.paloaltonetworks.jp/prisma/cloud で詳細をご確認ください。

参考文献：

1 パロアルトネットワークス株式会社 .「脅威予測 : クラウドでのエントロピー増大のリスク」. https://unit42.paloaltonetworks.jp/cloudy-with-a-chance-of-entropy/ (参照 2021-07-16)

2 パロアルトネットワークス株式会社 .「クラウドネイティブセキュリティの状態 2020」. https://www.paloaltonetworks.jp/resources/research/cloud-native-security-report (参照 2021-07-16)

3 内閣官房 情報通信技術（IT）総合戦略室 .「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」. https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf (参照 2021-07-16)