

2025

クラウドセキュリティ レポート

クラウド環境を保護するための重要な知見と戦略



FORTINET

はじめに

クラウドの採用は、比類のないスケーラビリティと柔軟性を提供することで、IT インフラとセキュリティ環境の継続的なトランスフォーメーションを可能にします。マルチクラウド戦略の採用によりこれらの優位性がさらに拡大しますが、固有の課題にも直面するため、組織は、革新的なソリューションを導入して重要な資産を効果的に保護する必要があります。

「2025 年クラウドセキュリティレポート」は、873 人のサイバーセキュリティ専門家から得られた知見に基づいて、進化するクラウドセキュリティ環境の詳細な分析を提供し、複雑化し続ける環境への対応にあたっての重要なトレンド、課題、優先事項を紹介します。本レポートが、ハイブリッド/マルチクラウドのセキュリティポスチャを強化しつつ、イノベーションを継続する方法を模索する IT やセキュリティのプロフェッショナルのガイドとなることを願っています。

主な調査結果

- **ハイブリッド / マルチクラウド戦略の拡大**：78% 以上が 2 社以上のクラウドプロバイダーを利用していると回答し、レジリエンスの強化と専門的な機能の活用にあたってのマルチクラウドアプローチの重要性が高くなっていることがわかりました。54% の組織がハイブリッドクラウドモデルを採用し、オンプレミスとパブリッククラウドの環境を統合して柔軟性と制御を最適化しています。
- **セキュリティとコンプライアンスの上位の懸念**：セキュリティとコンプライアンスの問題がクラウド導入の主な障害であり、61% の組織が、法規制の要件に対応して機密データを保護する努力を続けていると回答しました。
- **クラウドセキュリティの人材不足**：76% の組織がクラウドセキュリティの専門知識が不足していると回答したことは、自動化、特定の分野のスキルアップ、リソースの最適化の必要性を浮き彫りにしています。
- **リアルタイムの脅威検知についての自信の低さ**：今回の調査により、64% の回答者が自社のリアルタイムでの脅威検知能力に対して自信がないことが明らかになりました。
- **統合型クラウドセキュリティプラットフォーム**：本調査で、97% の回答者が、統合型クラウドセキュリティプラットフォームで一元化されたダッシュボードを利用することで、ポリシーの構成を簡素化し、一貫性を確保し、組織のクラウド環境の可視性を向上させたいと考えていることがわかりました。
- **クラウドセキュリティポスチャ管理 (CSPM) とクラウドネイティブアプリケーション保護プラットフォーム (CNAPP) の急速な採用**：構成ミスやコンプライアンスのギャップに対処するため、67% の回答者が CSPM を、62% の回答者が CNAPP ソリューションを導入してクラウド環境を保護しようとしていることがわかりました。



本レポートは、ポリシーの適用を合理化し、脅威検知を自動化し、ハイブリッドクラウドおよびマルチクラウド環境で一貫性のある保護を実現する統合型クラウドセキュリティソリューションの重要性を強調するものです。これらの知見とベストプラクティスを活用することで、組織は、進化する脅威とビジネスの需要に適応するレジリエントなクラウドセキュリティポスチャを構築できます。

この重要な調査プロジェクトをご支援いただいた [Fortinet](#) に心より感謝いたします。ハイブリッド/マルチクラウド環境の保護についての専門知識と知見を提供していただいたことで、調査結果や提案事項がさらに確かなものになりました。

クラウドが急速に拡大し続ける今、本レポートが組織の保護にあたる IT やサイバーセキュリティ専門家の皆様のための実用的ガイドとしてお役に立てることを願っております。

ありがとうございました。

Holger Schulze

Cybersecurity Insiders 創設者

クラウド導入戦略の変化

組織が選択するクラウド導入戦略は、その組織のセキュリティニーズ、オペレーションの成果、インフラストラクチャの要件に直接影響するため、今日の多面的な IT 環境において極めて重要な判断となります。

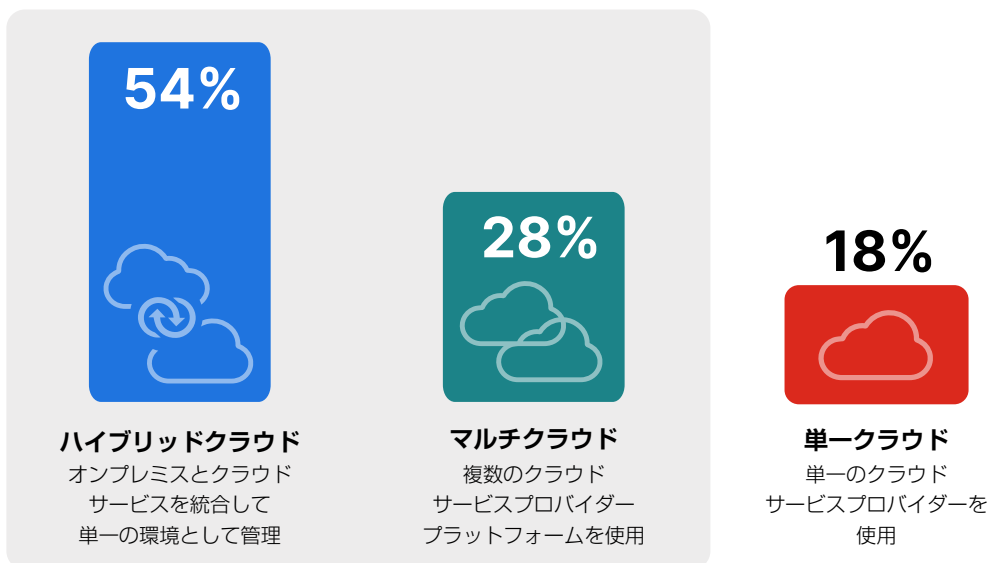
今回の調査で、54% の回答者がハイブリッドクラウド戦略を採用していることがわかり、昨年の 43% から増加しました。この増加は、単一クラウドからマルチクラウドへの移行が進み、マルチクラウドサービスとオンプレミスのシステムが統合された一貫性のある環境を構築する動きが強まっていることを反映しています。例えば、小売業の企業が顧客向けのアプリケーションのホスティングにはパブリッククラウドを利用し、機密度の高い決済データをプライベートのオンプレミスシステムに残すことで PCI DSS などのコンプライアンス要件に対応している場合もあるでしょう。このようなハイブリッドクラウド戦略により、組織は、パブリッククラウドのスケラビリティという利点を享受しつつ、重要なデータを制御できるようになります。

マルチクラウドの導入は、ワークロードを複数のプロバイダーに分散することで、ベンダーのロックインを回避したり、特定の機能を利用したりする組織が選択する方法であり、この回答が 28% で続きました。例えば、あるハイテク企業が処理負荷の高いアプリケーションのホスティングには Amazon Web Services (AWS) を利用し、データ分析には Google Cloud の高度な AI サービスを利用することで、単一のプロバイダーへの依存を軽減しつつパフォーマンスを最適化している場合もあるでしょう。

単一クラウドの採用は一般的ではなくなりつつあり、単一のプロバイダーを利用しているという回答は全体の 18% (2024 年の 22% から減少) にとどまりました。これは多くの場合、管理は簡素化されるものの、柔軟性の低下という潜在的なデメリットを伴う可能性があるためと考えられます。おそらくこれは、多様化よりも管理のしやすさを優先し、Microsoft の Azure のみを文書の保存やワークフロー管理に利用している法律事務所などの中小規模の企業が選択するモデルです。

▶ クラウドの導入における御社の主要戦略は何ですか？

82% マルチクラウドまたはハイブリッド環境を使用している組織

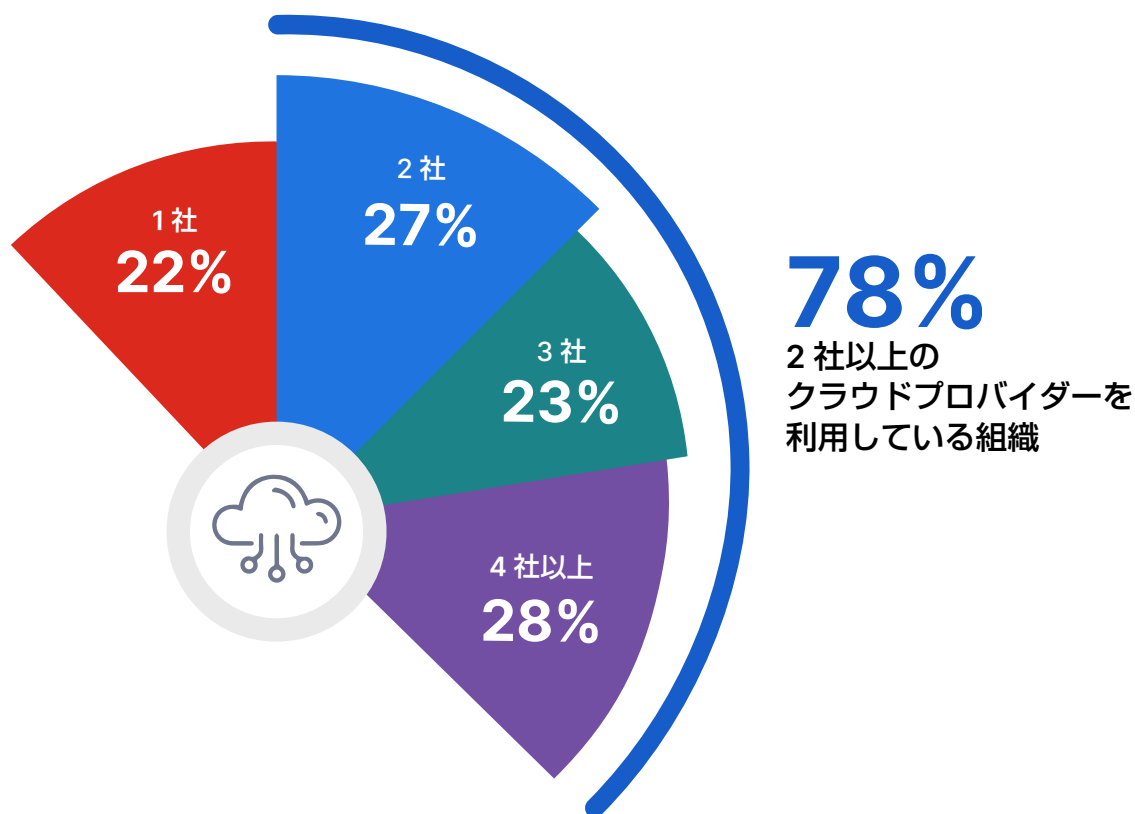


マルチクラウドの導入の拡大

組織が利用するクラウドプロバイダーの数の増加は、ハイブリッドクラウドやマルチクラウドの戦略が選択されるようになっていることを示すものですが、それに伴う運用の複雑さも反映しています。

今回の調査で、78%の組織が2社以上のクラウドプロバイダーを使用していることがわかり、昨年の71%から7%増加したことは、マルチクラウドの採用への移行が進んでいることを示しています。例えば、多国籍企業がグローバルのコンテンツデリバリーネットワークにはAWSを利用し、データの所在に関する厳格な法律が適用される地域ではMicrosoft Azureのコンプライアンスに対応する製品を利用する場合もあるでしょう。複数のプロバイダーを戦略的に利用することで、組織は、Google CloudのAIサービスやOracle Cloudのデータベースの専門知識など、分野に特化した機能を活用しつつ、冗長性により耐障害性を保証することができます。

▶ 現在、御社では何社のクラウドプロバイダーを利用していますか？



人気の高いクラウドプロバイダー

組織が現在利用している、あるいは導入を計画しているクラウドサービスプロバイダーを理解することで、市場のトレンドが明らかになり、進化するワークロードや分野に特化した機能に合わせてクラウド戦略をどのように調整しているかを知ることができます。

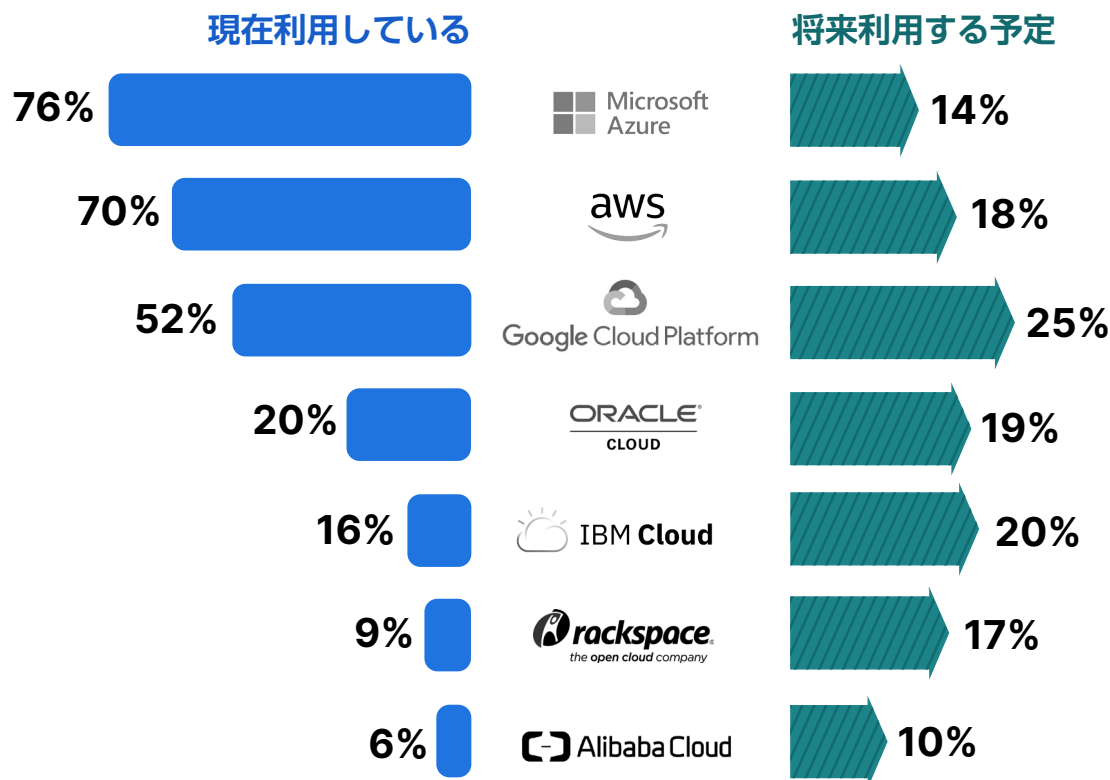
今回の調査結果によると、現在 Microsoft Azure と AWS を利用しているという回答がそれぞれ 76% と 70% で、この 2 つが人気のあるクラウドプロバイダーであることがわかりました。

現在利用しているという回答が 52% だった Google Cloud Platform は、将来利用する予定という回答が 25% となり、関心が高まっていることがわかりました。

その一方で、Oracle Cloud と IBM Cloud は、市場シェアは低いものの、おそらくはレガシーシステムとの統合についての専門知識という理由から、将来利用する予定であるという回答が多くなったと考えられます。

▶ 現在利用している、あるいは将来利用する予定のクラウド IaaS プロバイダーは？

(該当するものをすべて選択してください)



クラウド導入の障害への対処

今回の調査で、クラウドサービスを採用する組織が直面する主な障害が明らかになり、IT チームとセキュリティチームがクラウド環境の可能性を完全に実現するために取り組むべき課題が浮き彫りになりました。

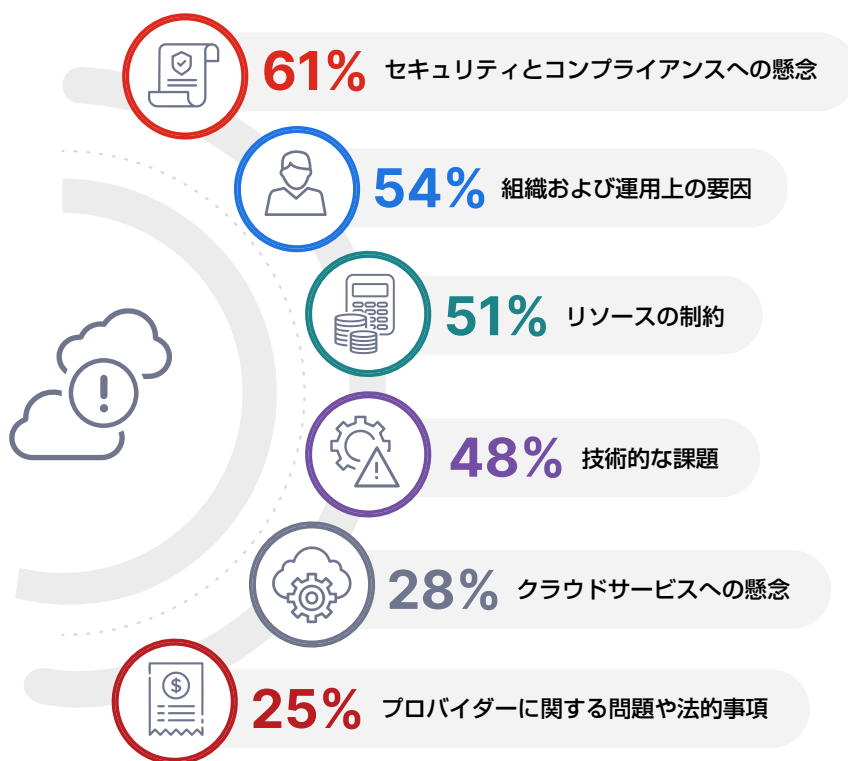
セキュリティとコンプライアンスに関する懸念を 61% の回答者（昨年の調査の 59% から増加）が挙げており、引き続き最大の課題であることがわかりました。これは、データ漏洩や法規制の要件への対応の複雑さといった問題に対する関心の高まりを反映しています。例えば、医療機関が HIPAA やその他の地域のデータ保護法のコンプライアンスが不透明であるという理由で、機密度の高い患者レコードのクラウドへの移行が遅れる場合もあるでしょう。

組織および運用上の要因が 54% と僅差で続き（昨年の 49% から 2 位に上昇）、変化への抵抗、ベンダーロックインの懸念、文化的なハードルなどの課題が浮き彫りになりました。例えば、製造業の企業が、レガシーシステムをクラウドに移行しようとする過程で、独自のプロセスをコントロールできなくなるという不安から、社内の反発に直面する場合もあるでしょう。

スタッフの専門知識の制限や予算の制約など、リソースの制約を 51%（2024 年の 49% から増加）の回答者が挙げたことは、多くの組織がクラウド機能の管理と保護で課題に直面していることを強調するものです。一方で、技術的な課題という回答は 48% と若干減少したものの、特に複雑なハイブリッドクラウド環境の統合では引き続き大きな障害であることがわかりました。

▶ 御社でのクラウド導入における主な課題は何ですか？

（該当するものをすべて選択してください）



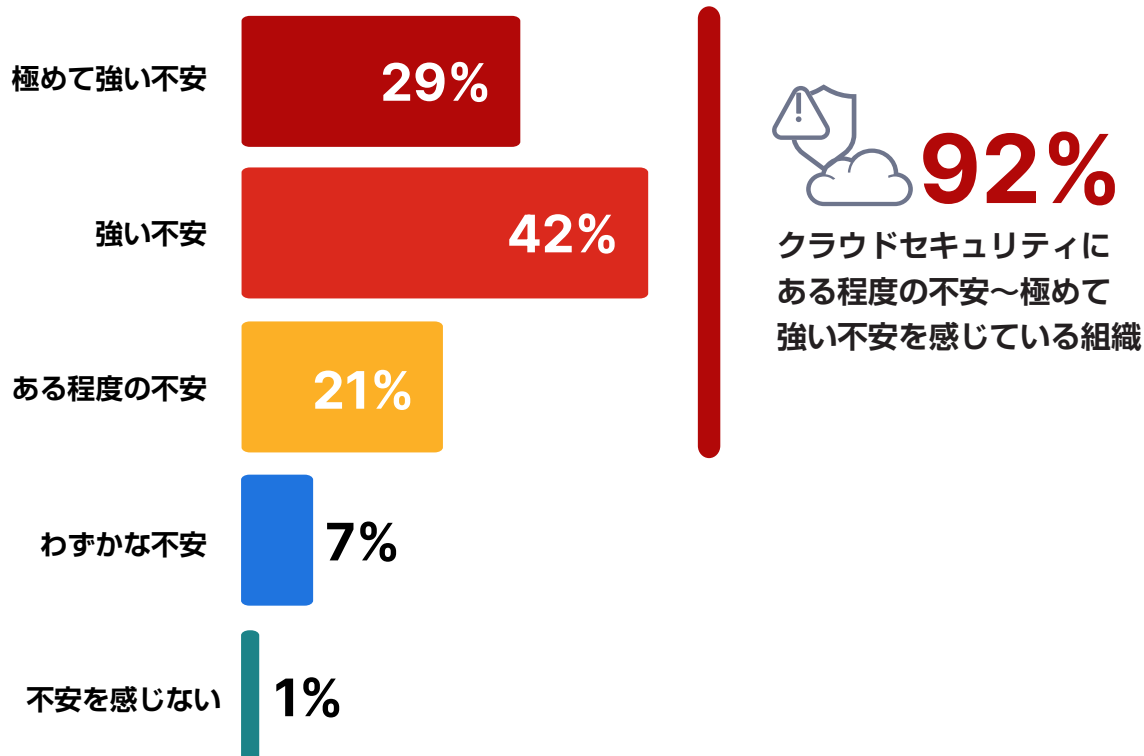
パブリッククラウドのセキュリティへの懸念

パブリッククラウドのセキュリティに関する変わらぬ懸念は、スケーラビリティと俊敏性という利点と堅牢な保護に対するニーズをうまく両立させるという課題を反映するものです。

92% もの回答者が、パブリッククラウドのセキュリティに懸念を示し、IT やサイバーセキュリティの専門家にとって重要な分野であることがわかりました。

この懸念は、61% がセキュリティとコンプライアンスがクラウド導入の最大の障害であると回答した今回の調査結果と一致するものでもあります。例えば、顧客取引データのクラウド移行を検討している金融サービス企業は、法規制へのコンプライアンス違反や構成ミスによる機密情報の漏洩の可能性を理由に移行に踏み切れない場合もあるでしょう。このような懸念は、データ漏洩、共同責任の不明瞭さ、クラウドプロバイダーの活動の限定的な可視性などの具体的なリスクにまで拡大し、採用の判断がさらに複雑化します。

▶ パブリッククラウドのセキュリティについてどの程度不安を感じていますか？



クラウドセキュリティオペレーションにおける課題

組織は日々のクラウドセキュリティオペレーションの過程で、自らの環境の保護で直面する、複雑で進化し続ける障害を知ることになります。

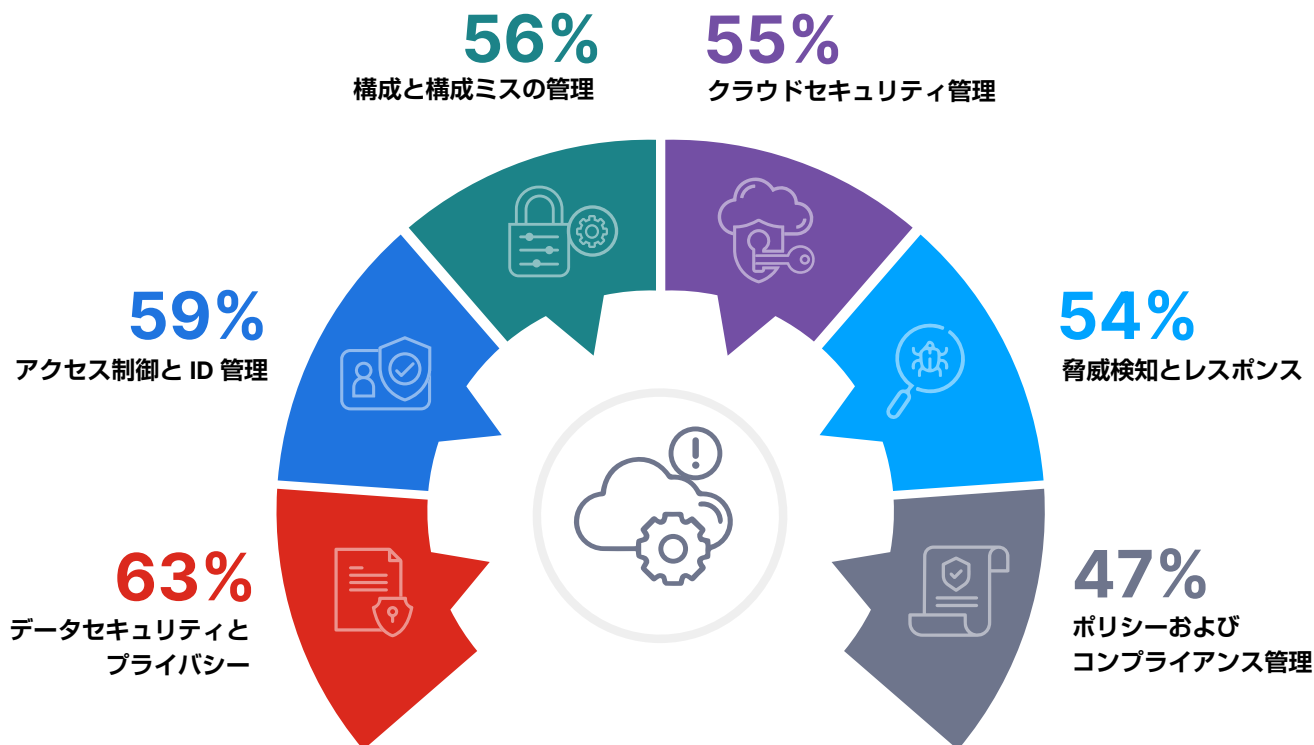
63% の回答者がデータセキュリティとプライバシーを最大の懸念事項として挙げたことは、機密情報の保護と漏洩の防止に対する継続的な懸念を反映するものです。アクセス制御と ID 管理が 59% でこれに続いたことは、堅牢な認証と特権の管理が分散クラウド環境に必要であることを強調しています。例えば、ハイブリッドクラウドの導入で、オンプレミスシステムとクラウドプラットフォーム間のユーザーアクセスポリシーの同期で課題に直面する可能性があります。

構成と構成ミスの管理が 56% で僅差の 3 位になったことは、クラウドを適切にセットアップすることの運用上の困難さを示すものであり、例えば、クラウドストレージバケットの意図しない公開の監視などがこれに含まれ、このような状況により、これまでに多くの注目された侵害が発生しました。

クラウドセキュリティ管理 (55%)、脅威検知とレスポンス (54%)、ポリシーおよびコンプライアンス管理 (47%) はいずれも、マルチクラウド環境を管理する、一貫性と拡張性のあるソリューションが必要であることを強調するものです。

▶ 日々のクラウドセキュリティオペレーションの管理における主な課題は何ですか？

(該当するものをすべて選択してください)



その他の回答：

シャドー IT と不正アプリ使用 46% | クラウド統合と自動化 43% | エンドポイントセキュリティ 40% | リソース配分 38% | DevSecOps の実践 31% | 運用の俊敏性と複雑さ 25%

マルチクラウド環境の保護

マルチクラウド環境の保護では、その環境に固有の複雑さ、標準化の欠如、急速に進化するテクノロジーに起因する明確な課題に直面します。これらの問題は、機密データを保護し、運用の効率性を維持し、多様なクラウドエコシステムを管理する組織の能力に直接影響します。

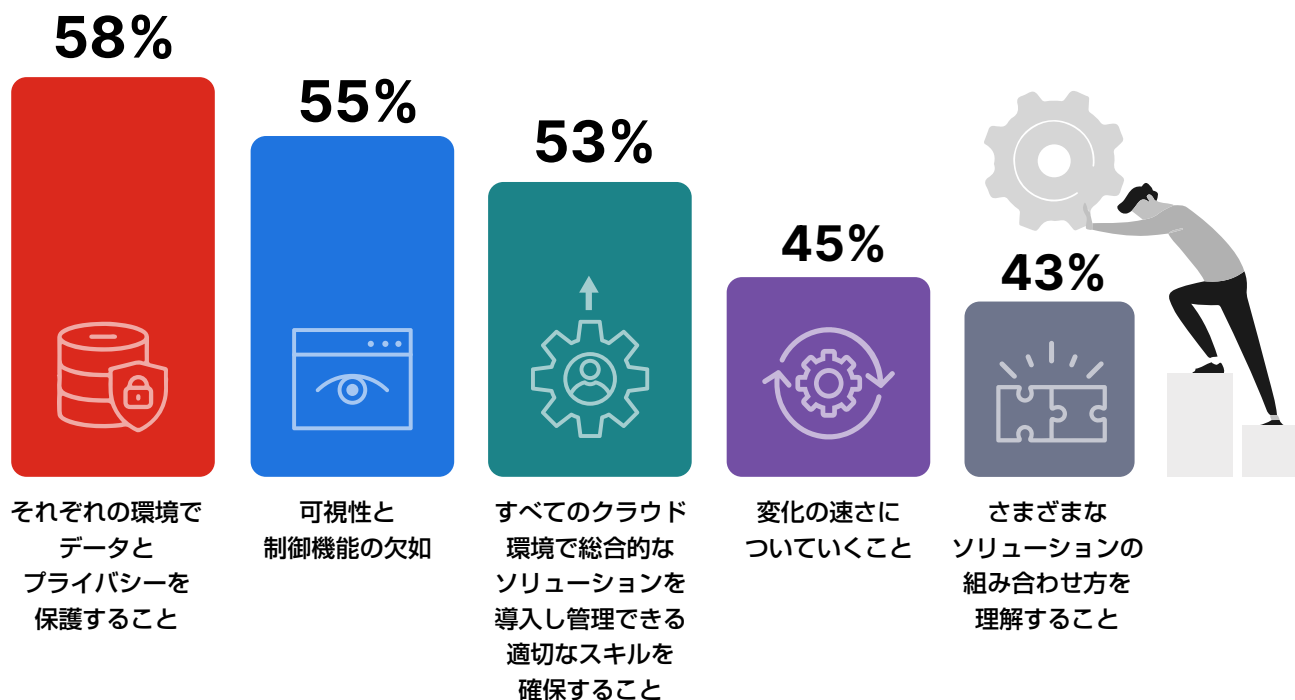
それぞれの環境のデータとプライバシーの保護は引き続き最大の課題であり、2024 年の 55% から増加して 58% の回答者がこれを課題として挙げました。これは、データセキュリティとプライバシーがオペレーションにおける最多の懸念（63%）になったことを反映するものであり、断片化されたクラウドインフラストラクチャにおける一貫した保護の必要性を強調するものです。

55% の回答者が可視性と制御の欠如を挙げたことは、マルチクラウド環境での監視を維持することの難しさを示すものであり、これは、55% の回答者が日々のクラウドセキュリティ管理を課題として挙げたことと一致するものです。

53% の回答者が包括的なマルチクラウドソリューションを展開して管理するスキルの不足を課題として挙げました。変化の速さについていくこと（45%）と、さまざまなソリューションの組み合わせ方を理解すること（43%）という課題は、クラウドテクノロジーの急速な進化に対応するための運用上や戦略上の障害を反映しています。

▶ マルチクラウド環境の保護における最大の課題は何ですか？

（該当するものをすべて選択してください）



その他の回答：

さまざまなソリューションのコストを管理すること 41% | サービス統合の選択肢を理解すること 40% | 認証情報に基づいてシームレスなアクセスをユーザーに提供すること 37% | サービスを正しく組み合わせる選択すること 30% | その他 1%

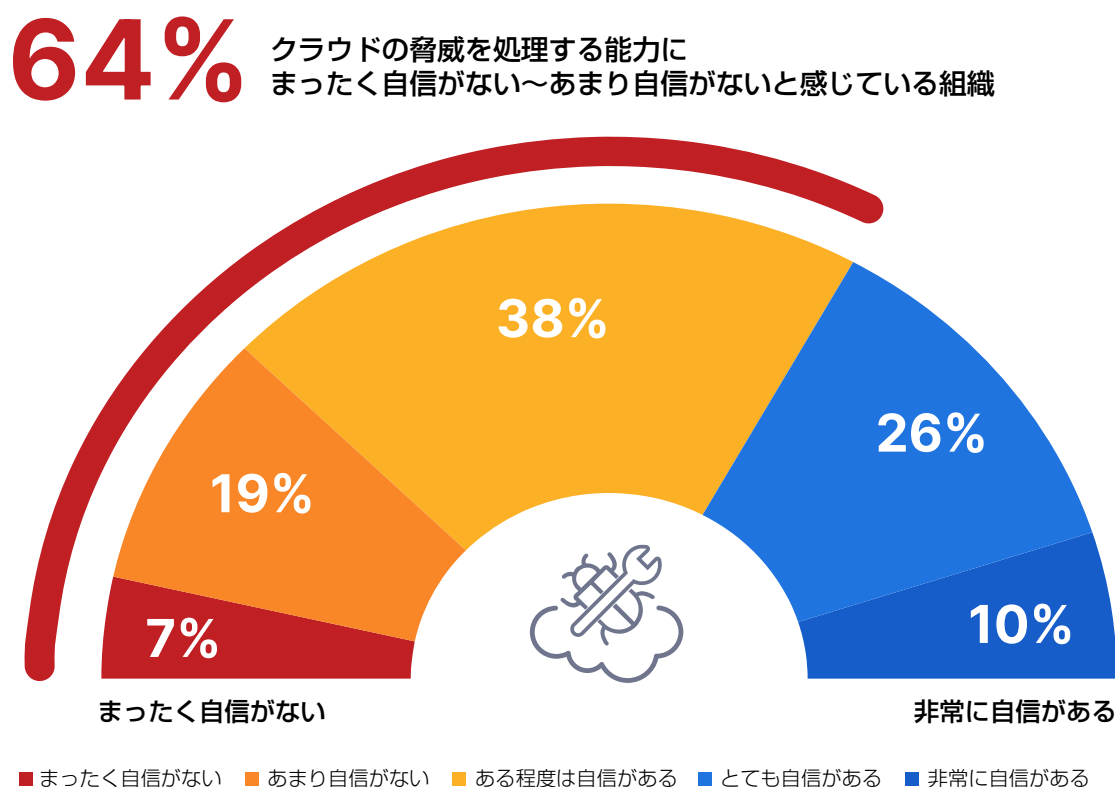
リアルタイムの脅威検知についての自信

複雑化するマルチクラウド/ハイブリッドクラウド戦略の採用にあたり、クラウド環境の脅威のリアルタイムでの検知とレスポンスの能力が極めて重要になります。これらのアーキテクチャにより、異種プラットフォームでのシームレスな可視性と迅速なレスポンスの実現で固有の課題に直面します。

今回の調査で 64% の回答者が自社のリアルタイムでの脅威検知能力に対して、自信がまったくない～ある程度は自信があると回答したことは、この能力に対する自信に隔たりがあることを示しています。例えば、複数の関連性の不正活動を結び付ける能力が欠如しているために、潜在的な侵害の特定とレスポンスが大幅に遅れる可能性があります。この傾向は、多くの組織が基本的なセキュリティ対策を実施している一方で、クラウドの脅威が高度化し、多様な環境の管理が困難になっているために、高度な攻撃や構成ミスに対して脆弱であることを示しています。前述の調査結果もこれと一致しており、クラウドセキュリティオペレーションの最大の障害が可視性と制御の損失（55%）と脅威検知とレスポンスの課題（54%）であることがわかりました。

非常に自信があるという回答はわずか 10%、とても自信があるという回答は 26% であったため、最新のクラウド脅威管理の要求に対して十分な備えがあるという回答の割合は 40% 未満です。

▶ すべてのクラウド環境における脅威のリアルタイムでの検知とレスポンスの能力について、どの程度自信がありますか？



クラウドセキュリティの優先項目

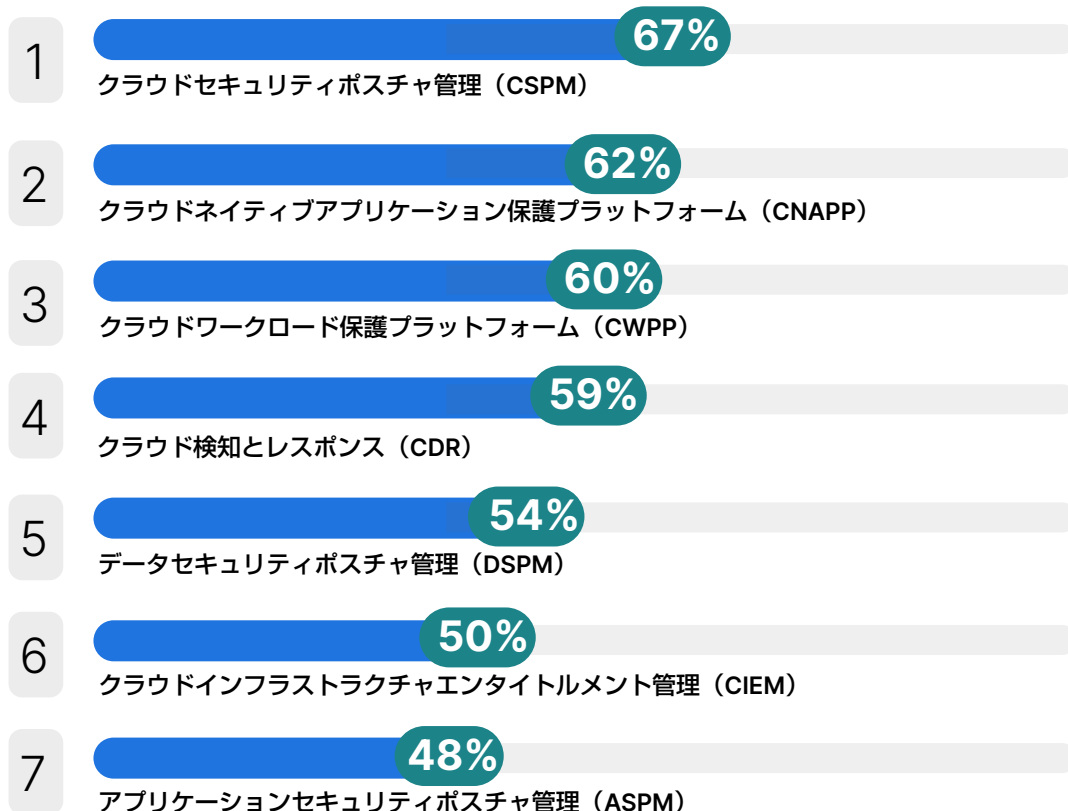
組織におけるクラウドの利用範囲が拡大し、脅威が増大する現状においても、レジリエンス、コンプライアンス、運用効率を確保するには、適切なセキュリティ機能を組み合わせて導入することが不可欠です。

今後 12 ヶ月間の重要なクラウドセキュリティツール導入の優先順位についての質問で、クラウドセキュリティポスチャ管理（CSPM）が 67% で最多となったことは、このツールがクラウド環境での構成ミスの特定と修復で重要な役割を果たすことを示すものです。例えば、小売業の企業が CSPM ツールを利用し、AWS のストレージバケットが一般公開されているというアラートを受け取ることで、多額の損害が発生するデータ侵害を防止できる場合もあるでしょう。

同様に、クラウドネイティブアプリケーション保護プラットフォーム（CNAPP）が 62% だったことは、エンドツーエンドのアプリケーションライフサイクルセキュリティの必要性が認識されるようになっていることを示しています。CNAPP は、Kubernetes で動作するコンテナ化されたワークロードの脆弱性をプロアクティブに認識し、悪意のあるランタイムアクティビティを特定し、侵害を示す一連のイベントを検知できる可能性があります。クラウドワークロード保護プラットフォーム（CWPP）が僅差で 60% になり、クラウド検知とレスポンス（CDR）が 59% になったことは、特にマルチクラウド環境においてワークロードのセキュリティと脅威の減災が注目されるようになっていることを強調するものです。クラウドインフラストラクチャエンタイトルメント管理（CIEM）の採用が 50% になったことは、多様なクラウドプラットフォームでの堅牢なアクセスと権限の制御に対する需要を証明するものであり、最小権限の実装や使用されていない認証情報の排除に向けた動きが加速していることを示しています。

▶ 利用している、あるいは今後 12 ヶ月間に利用する予定の機能は何ですか？

（該当するものすべてを選択してください）



サイバーセキュリティのスキルギャップの解消

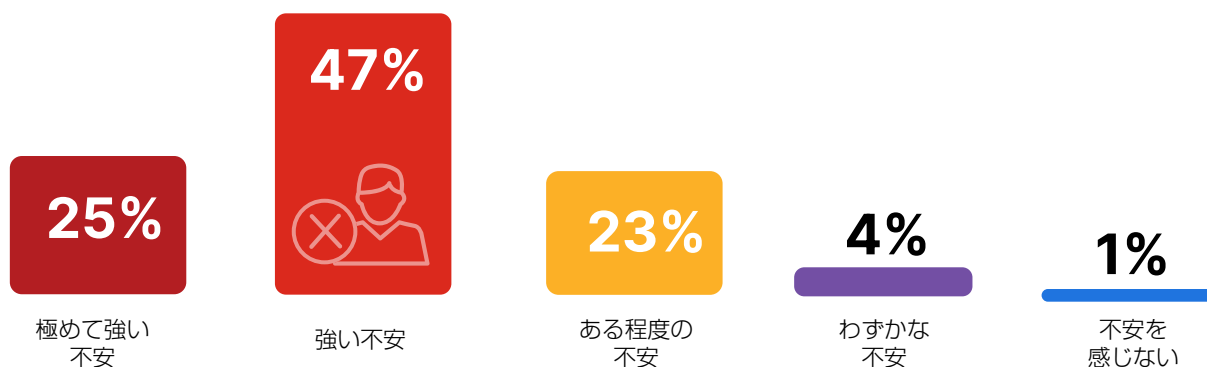
業界全体で適任のサイバーセキュリティ専門家が不足していることは、組織が資産を保護し、進化する脅威に効果的に対応する能力に直接影響する重大な問題であり続けています。

今回の調査で 95% が継続的なサイバーセキュリティのスキル不足にある程度の不安～強い不安を感じていると回答したことは、複雑化するサイバーセキュリティの課題の対処に必要な人材の雇用や引き止めが組織にとって大きな負担であることが示しています。例えば、マルチクラウドのセキュリティ管理を導入しようとする医療機関は、構成管理や CIEM などのクラウドに特化した人材の不足により、導入が遅れる可能性があります。

▶ 適任のサイバーセキュリティ専門家が業界全体で不足していることに、どの程度不安を感じていますか？

95%

適任のサイバーセキュリティ専門家が業界全体で不足していることにある程度の不安～極めて強い不安を感じている組織



この不安は、76% の組織がサイバーセキュリティの人材不足に直面しているという調査データでも実証されています。

▶ 御社ではサイバーセキュリティ人材が不足していますか？



今日の脅威への対抗で重要なセキュリティスキル

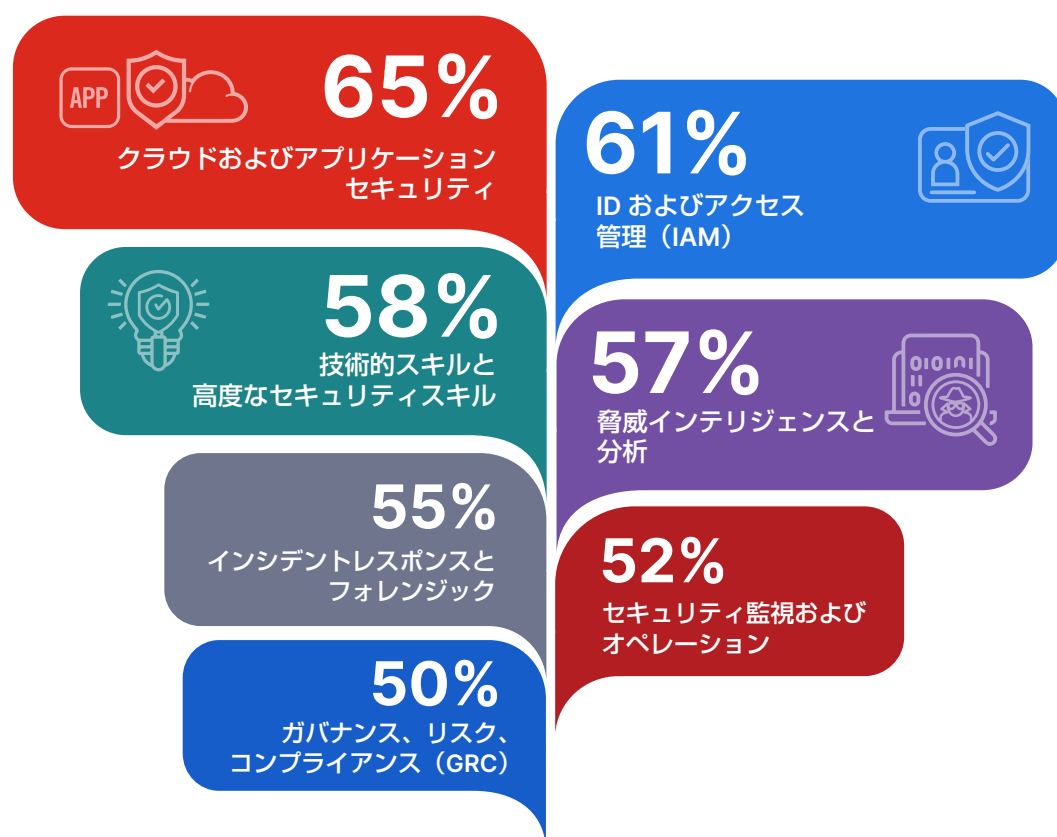
最も重要なセキュリティスキルについての回答は、複雑化するクラウドセキュリティの課題への対応で組織に必要とする専門知識が多様化し、進化していることを示しています。

クラウドとアプリケーションのセキュリティスキルが 65% で最多であったことから、クラウドプラットフォームとアプリケーションの保護が組織の優先事項であることがわかります。例えば、クラウドプラットフォームに特化したセキュリティの専門知識としては、自動化されたガードレールやスケーラブルでセキュアなランディングゾーンの作成などがあり、いずれもコードとして利用して導入を自動化することができます。

ID およびアクセス管理が 61% と僅差で続いたことは、特にハイブリッド / マルチクラウド環境では統合型のユーザー権限管理が不可欠であることを示しており、堅牢なアクセス管理の必要性を強調するものです。技術的スキルと高度なセキュリティスキル (58%) と脅威インテリジェンスと分析 (57%) は、特に侵害されたクラウド管理者アカウントに対する悪意のある活動を迅速に特定して減災する目的で AI を利用し、攻撃者の高度な戦術を理解することができる専門家に対する需要が高まっていることを示しています。インシデントレスポンスとフォレンジック (55%) は、依然として侵害の減災に不可欠なスキルであり、セキュリティ監視およびオペレーション (52%) は、異常の検知と迅速な減災の専門知識に対する必要性を強調するものです。

▶ 御社で必要とされている最も重要なセキュリティスキルは何ですか？

(該当するものをすべて選択してください)



その他の回答：

トレーニングと意識向上 45% | コミュニケーションと戦略 39% | わからない 3%

クラウドセキュリティ投資の動向

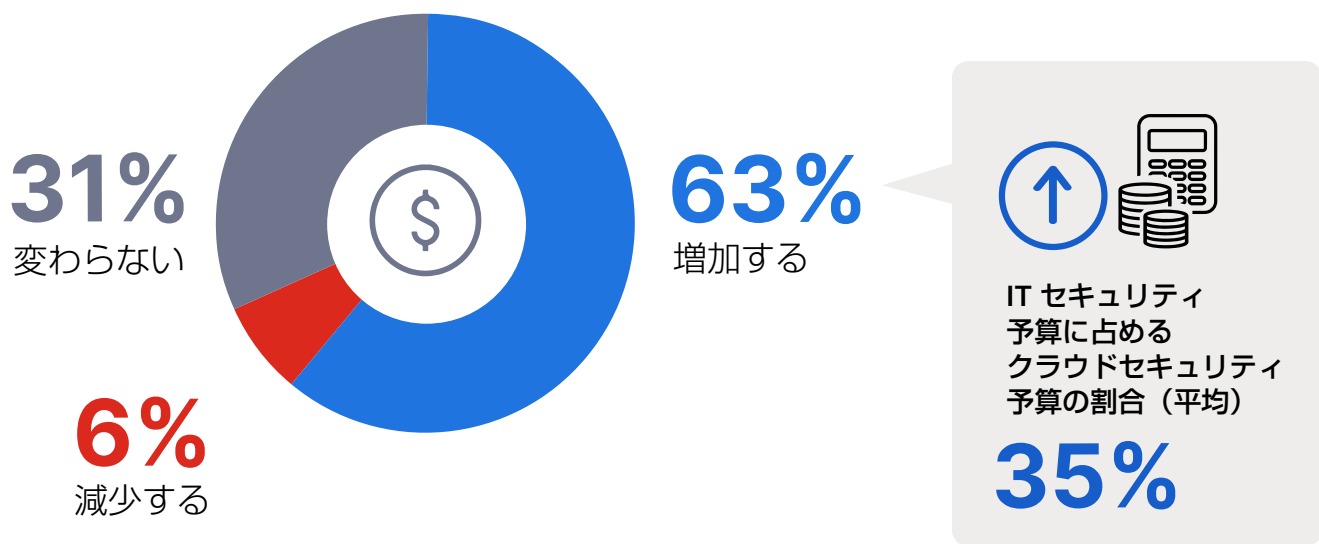
今回の調査で、組織が自らの財務リソースをどのように優先させ、クラウドセキュリティの課題を解決しようとしているかについての新たな知見が明らかになりました。半数を超える 63% の回答者が、今後 12 ヶ月間にクラウドセキュリティ予算を増額する予定と回答したことは（昨年の 61% から増加）、ハイブリッド / マルチクラウドの環境の防御を強化する必要性を強く認識していることを示しています。

一方で、31% が予算は変わらないと回答したことは（2024 年の 32% から減少）、すでに多額を投資している組織や運用のニーズが変動しない組織をおそらく反映するものです。減少するという回答はわずか 6% でしたが、クラウドの脅威や法規制の要件が拡大している今、これは珍しい傾向と言えるでしょう。

平均すると、IT セキュリティ予算の 35% がセキュリティ予算に配分されており、特にクラウドの導入の加速に伴い、セキュリティ支出がクラウド保護に重点的に配分されるようになりつつあることを示しています。

このようにクラウドセキュリティへの投資が重視されるようになったことは、本レポート全体で課題として指摘している、可視性、アクセス制御、脅威検知のギャップに対処するプロアクティブなアプローチを反映するものです。予算の増額を予定している組織は、CNAPP などの重要な機能を効率的に統合するソリューションに重点的に予算を配分することで、投資の効果を最大化する必要があるでしょう。

▶ 今後12ヵ月間で御社のクラウドセキュリティ予算はどのように変化しますか？




統合型クラウドセキュリティプラットフォームの価値

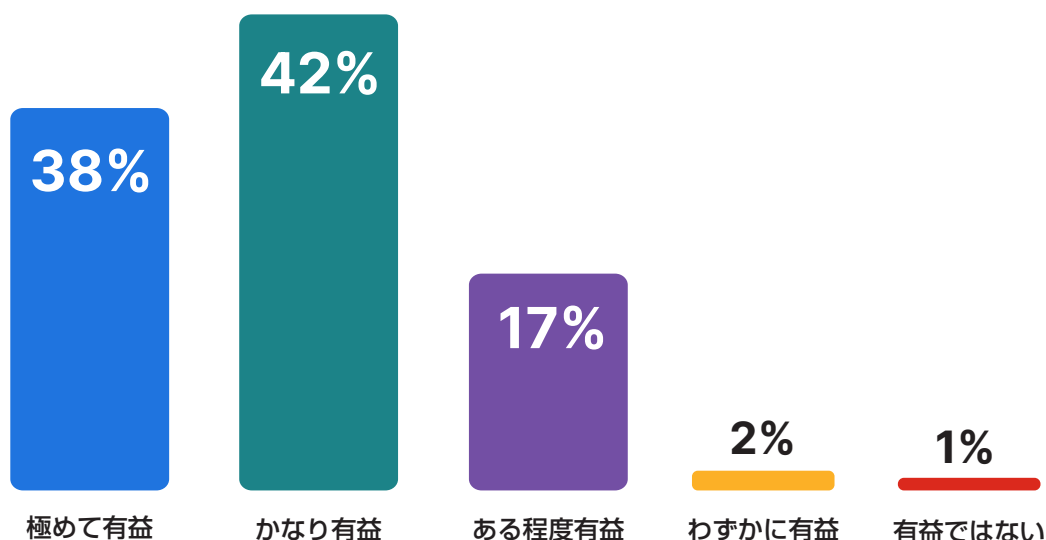
単一の統合型クラウドセキュリティプラットフォームで一元化されたダッシュボードを利用することには、ポリシーの構成を簡素化し、一貫性を確保し、組織のクラウド環境の可視性を向上する可能性があるという価値があります。

今回の調査で、この概念に対する関心が極めて高く、97%の回答者が、このようなプラットフォームがある程度有益～極めて有益と考えていることがわかりました。例えば、金融サービスの組織は、単一のダッシュボードを利用して、AWS、Azure、Google Cloud に同じアクセス制御を適用することで、構成ミスの可能性を減らすことができるでしょう。これは、55%の回答者が可視性と制御の損失をマルチクラウドやハイブリッド環境の主な課題として挙げた、これらのギャップを解消する一元ツールの必要性を強調する前述の結果と一致しています。

- ▶ 単一のダッシュボードを備えたクラウドセキュリティプラットフォームを使用して、必要なすべてのポリシーを設定し、クラウドフットプリント全域でデータを一貫して包括的に保護できるとしたら、それは御社にとってどれくらい有益ですか？

97% 

単一のダッシュボードを備えたクラウド
セキュリティプラットフォームの使用が
ある程度有益～極めて有益と考える専門家



ハイブリッド / マルチクラウドセキュリティ強化の ベストプラクティス

ハイブリッド / マルチクラウド環境の導入の進行に伴い、多様なプロバイダーの管理や堅牢なセキュリティの維持がさらに複雑化します。このような課題に効果的に対応するには、業界の知見に沿った戦略的ベストプラクティスを採用し、高度なセキュリティソリューションを利用することが不可欠です。

マルチクラウドのセキュリティポスチャを強化する、推奨される実用的なステップを以下に紹介します。

1 クラウドのリスクの検知と修復を自動化する

構成ミスは一般的な脆弱性であり、67% の回答者が、この問題に対処する自動化ツールを使用しているか使用する予定であると回答しました。継続的な監視とリアルタイムの修復を可能にするソリューションにより、ストレージの構成ミスや過剰な権限などのリスクをプロアクティブに特定し、効率的に修正できます。これらのツールにより、業界の規制のコンプライアンスも簡素化されます。

2 クラウド環境のデータフローを保護する

データが複数のクラウド環境で移動する場合、そのセキュリティと整合性の確保が極めて重要です。58% の回答者がデータ保護とプライバシーを最大の懸念として挙げましたが、データフローを包括的に可視化するツールを利用することで、移動中の情報を保護できます。これらのツールにより、潜在的なリスクの監視、不正アクセスの防止、GDPR や CCPA などの法規制のフレームワークの遵守が可能になり、データ保護の取り組み全体が強化されます。

3 統合型の脅威検知メカニズムを実装する

回答者の半数以上（54%）が、マルチクラウド環境における脅威検知とレスポンスの困難さを指摘しました。統合型の脅威検知ソリューションは、可視性を一元化することで、チームによる迅速な異常の特定とレスポンスを可能にします。これらのツールは、異なるクラウド環境のデータを相関付けることで、検知時間を短縮し、レスポンスの精度を向上させることができます。

4 クラウドに特化したセキュリティチーム向けトレーニングに投資する

76% の組織がスキル不足の影響を受けており、結果として、クラウドネイティブのソリューションを効果的に展開して管理する能力が制限されます。DevSecOps やコンテナセキュリティなどの分野での従業員のスキルアップにより、チームが新たなセキュリティの課題に対処できるようになります。

5 PaC（Policy as Code）を利用して一貫したセキュリティの適用を実現する

43% の回答者が、異なるソリューションがどのように統合されているかを理解することを課題として挙げましたが、PoC（Policy as Code）アプローチを利用することで、複数のプラットフォームで一貫したポリシーの適用が可能になります。PoC により、監査が簡素化され、構成管理を自動化できるため、セキュリティ制御を組織の要件に常に一致させることができます。

6

セキュリティ投資とアプリケーションワークロード要件を一致させる

アプリケーションレベルのセキュリティの優先度が高くなっており、62%の回答者が、包括的な保護プラットフォームの導入を計画していると回答しました。開発からランタイムまでのエンドツーエンドのアプリケーションのセキュリティにより、ワークロードの保護をカスタマイズしつつ、複数の環境で一貫したポリシーをサポートできます。コンテナ環境やランタイム保護を統合するソリューションにより、このニーズに効果的に対応できます。

7

クラウドプラットフォームのアクセス制御を標準化する

アクセス制御とID管理は、59%の組織で最大の課題であり続けており、特に分散クラウド環境においては深刻な問題です。一元的なアクセス制御ソリューションにより、ユーザー権限の管理を合理化し、ハイブリッド/マルチクラウド環境で一貫したセキュリティポリシーを適用できます。統合型のアイデンティティプラットフォームを実装することで、シームレスなポリシーの適用を可能にしつつ、不正アクセスのリスクを最小化できます。

8

クラウドベースのセキュリティのツールを採用してスケーラビリティを実現する

54%の回答者がハイブリッドクラウドを主要な導入モデルとして挙げたことは、スケーラブルなクラウドベースのセキュリティツールが不可欠であることを示しています。これらのソリューションは、オンプレミスのシステムとパブリッククラウドで一貫した保護を可能にするため、組織は、運用効率を低下させることなくクラウド環境を拡大できます。

終わりに

本レポートでは、統合型のツールやトレーニングに加えて、ハイブリッド/マルチクラウドのセキュリティの進化する要求に合わせカスタマイズしたプロセスに戦略的に投資することの重要性を説明しました。構成ミス、スキル不足、可視性の欠如などの課題に対処することで、組織は、レジリエントなセキュリティ態勢を構築できます。

本レポートで紹介したベストプラクティスを実装することで、企業は、複雑なクラウド環境を適切に管理し、重要な資産を保護しつつ、デジタルトランスフォーメーションが急速に進む時代にあっても俊敏性とコンプライアンスを維持できます。

クラウドセキュリティ用語集

この用語集では、本レポートで紹介した重要なクラウドセキュリティテクノロジーの概要、機能、解決すべきセキュリティの課題に加えて、今日の複雑なクラウド環境の保護でそのテクノロジーが重要である理由を説明します。

アプリケーションセキュリティポスチャ管理 (ASPM : Application Security Posture Management) : ASPM は、ソフトウェア開発ライフサイクルにおけるアプリケーションの脆弱性や構成の問題を可視化します。安全なコーディングプラクティスをサポートし、DevSecOps ワークフローにセキュリティを統合します。ASPM は、アプリケーションの安全性を開発から導入、ランタイムまでで確保するために極めて重要です。

クラウド検知とレスポンス (CDR : Cloud Detection and Response) : CDR は、クラウド環境での脅威の特定と減災に特化したテクノロジーです。クラウドのアクティビティをリアルタイムで可視化することで、迅速な異常の検知とインシデントレスポンスを可能にします。CDR は、分散クラウド環境で強力な防御を確立し、高度な脅威に対抗するために極めて重要です。

クラウドインフラストラクチャエンタイトルメント管理 (CIEM : Cloud Infrastructure Entitlement Management) : CIEM は、クラウド環境の権限とアクセス制御の管理に重点を置いています。過剰な権限を特定し、最小権限の原則を適用し、権限が悪用されるリスクを軽減します。CIEM は、安全でコンプライアンスに準拠したアクセスポリシーをマルチクラウドアーキテクチャで維持するために重要です。

クラウドネイティブアプリケーション保護プラットフォーム (CNAPP : Cloud Native Application Protection Platform) : CNAPP は、複数のセキュリティ機能を統合することで、クラウドネイティブのアプリケーションをライフサイクル全体で保護します。ワークロード保護、構成管理、ランタイム防御を組み合わせることで、コンテナ、サーバーレス関数、その他のクラウドネイティブのワークロードを保護します。CNAPP は、DevOps やマイクロサービスなどの最新の開発プラクティスを採用する組織に不可欠です。

クラウドセキュリティポスチャ管理 (CSPM : Cloud Security Posture Management) : CSPM は、クラウド環境における構成ミスの検知を自動化するソリューションです。クラウドインフラストラクチャを継続的に監視し、外部に公開されているストレージバケットや過度に許容範囲が広いアクセス制御などのセキュリティリスクを監視し、法規制のフレームワークのコンプライアンスを保証します。CSPM は、マルチクラウドやハイブリッド環境の可視化と脆弱性への対処に不可欠です。

クラウドワークロード保護プラットフォーム (CWPP : Cloud Workload Protection Platform) : CWPP は、仮想マシン、コンテナ、サーバーレスアーキテクチャなどのクラウド環境のワークロードを保護します。脆弱性を可視化し、一貫したセキュリティポリシーを保証し、高度な脅威からワークロードを保護します。CWPP は、多様で動的なクラウドワークロードを管理する組織にとって重要なソリューションです。

データセキュリティポスチャ管理 (DSPM : Data Security Posture Management) : DSPM は、クラウド環境の機密情報を特定、分類、保護を支援する、データ中心のソリューションです。これにより、データが適切に保護され、GDPR や CCPA などのプライバシー規制に適合できるようになります。DSPM は、複雑なクラウドエコシステムでの機密情報の保護で直面する課題への対応に不可欠です。

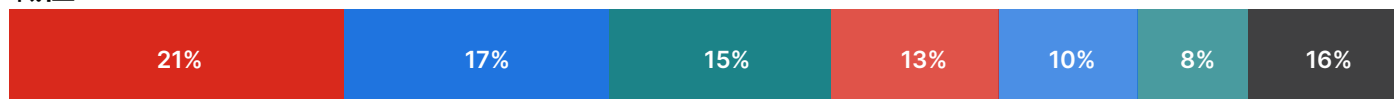
調査の方法と回答者

「2025 年クラウドセキュリティレポート」は、さまざまな国のテクノロジー、金融サービス、医療、政府機関を始めとする業種の 873 人のサイバーセキュリティ専門家を対象に 2024 年後半に実施された総合的な調査に基づくものです。回答者は、中小企業から大企業までさまざまな規模の組織を代表しており、専門職から C レベルの経営幹部までの幅広い職務に就くプロフェッショナルからバランスよく選出されています。

オンラインで実施された調査により、クラウドセキュリティの主要なトレンド、課題、優先事項が明らかになりました。調査の結果は、組織がクラウド環境の複雑さにどのように対応し、新たな脅威に対処するセキュリティテクノロジーをどのように導入しているかについての包括的な見解を示しています。

複数回答が可能な質問で回答者が複数の選択肢を選択する可能性があるため、パーセンテージの合計が 100% を超える場合があります。

職位



■ マネージャー / スーパーバイザー ■ スペシャリスト ■ CTO、CIO、CISO、CMO、CFO、COO ■ コンサルタント ■ ディレクター ■ 統括本部長 / 事業部長等 (VP レベル) ■ その他

部署



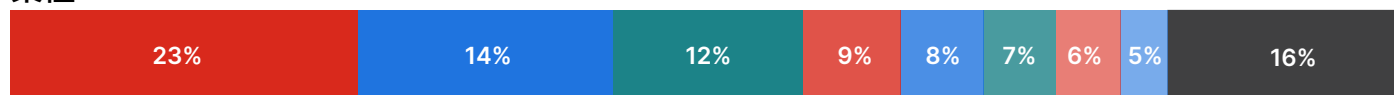
■ IT セキュリティ ■ IT オペレーション ■ コンプライアンス ■ SecOps ■ オペレーション ■ DevOps ■ その他

企業規模



■ 10 人未満 ■ 10 ～ 99 人 ■ 100 ～ 499 人 ■ 500 ～ 999 人 ■ 1,000 ～ 4,999 人 ■ 5,000 ～ 9,999 人 ■ 10,000 人以上

業種



■ テクノロジー、ソフトウェア、インターネット ■ 金融サービス ■ 政府機関 ■ 専門サービス ■ 医療、医薬品、バイオテック ■ コンピューター、電子機器 ■ 通信 ■ 教育および研究機関 ■ その他

コンテンツの再利用について

本レポートに掲載されているデータ、図表、テキストの再利用については、[クリエイティブ・コモンズの表示 4.0 国際ライセンス](#)の条件に従うことを推奨いたします。同ライセンスが規定する条件に従って本レポートの属性を明示する限りにおいて、本レポートの内容を自由に共有および商用利用することができます。例：「2025 Cloud Security Report by Cybersecurity Insiders and Fortinet」（2025 年クラウドセキュリティレポート、Cybersecurity Insiders およびフォーティネット著）



フォーティネット（NASDAQ：FTNT）は世界中の大企業、
サービスプロバイダー、政府機関をセキュリティで保護しています。

当社は拡大する攻撃対象領域を
全面的に可視化および制御し、現在だけでなく将来にわたり、
増大の一途をたどるパフォーマンス要件に対応した機能をお客様に提供します。

フォーティネット セキュリティ ファブリックは、
ネットワーク、アプリケーション、マルチクラウド、エッジなど
いかなる環境においても最も重大なセキュリティ課題に対処し、
デジタルインフラストラクチャ全体でデータを保護できる
唯一のプラットフォームです。

フォーティネットは世界におけるセキュリティアプライアンスの
出荷台数で首位を獲得しており、
80 万社を超えるお客様がビジネスの保護にフォーティネットを利用しています。

www.fortinet.com/jp

Cybersecurity

I N S I D E R S

Cybersecurity Insiders は、今日の最も重大なサイバーセキュリティの課題に取り組む中で、60 万人以上の IT セキュリティ専門家と世界的テクノロジーベンダーを統括し、スマートな問題解決と協力体制を推進しています。

弊社のアプローチは、サイバーセキュリティの最新動向、ソリューション、ベストプラクティスなどをサイバーセキュリティの専門家に周知、伝達する独自のコンテンツを作成し、提供することに主眼を置いています。総合的な研究調査、公平な製品レビュー、実用的な E ガイド、魅力的なウェビナー、教育関連の記事など、今日の複雑なサイバーセキュリティ課題に対し、証拠に基づいた解決策を示すリソースを提供できるよう努めています。

競争の激しい市場で突出した実績を上げ、需要、ブランドの知名度、ソートリーダーとしての存在感を高める上で、Cybersecurity Insiders がいかに有益かを今すぐお確かめください。

E メール（info@cybersecurity-insiders.com）でお問い合わせいただくか、cybersecurity-insiders.com をご覧ください。