ivanti　PULSE

アジア太平洋および日本地域におけるセキュアアクセスの動向

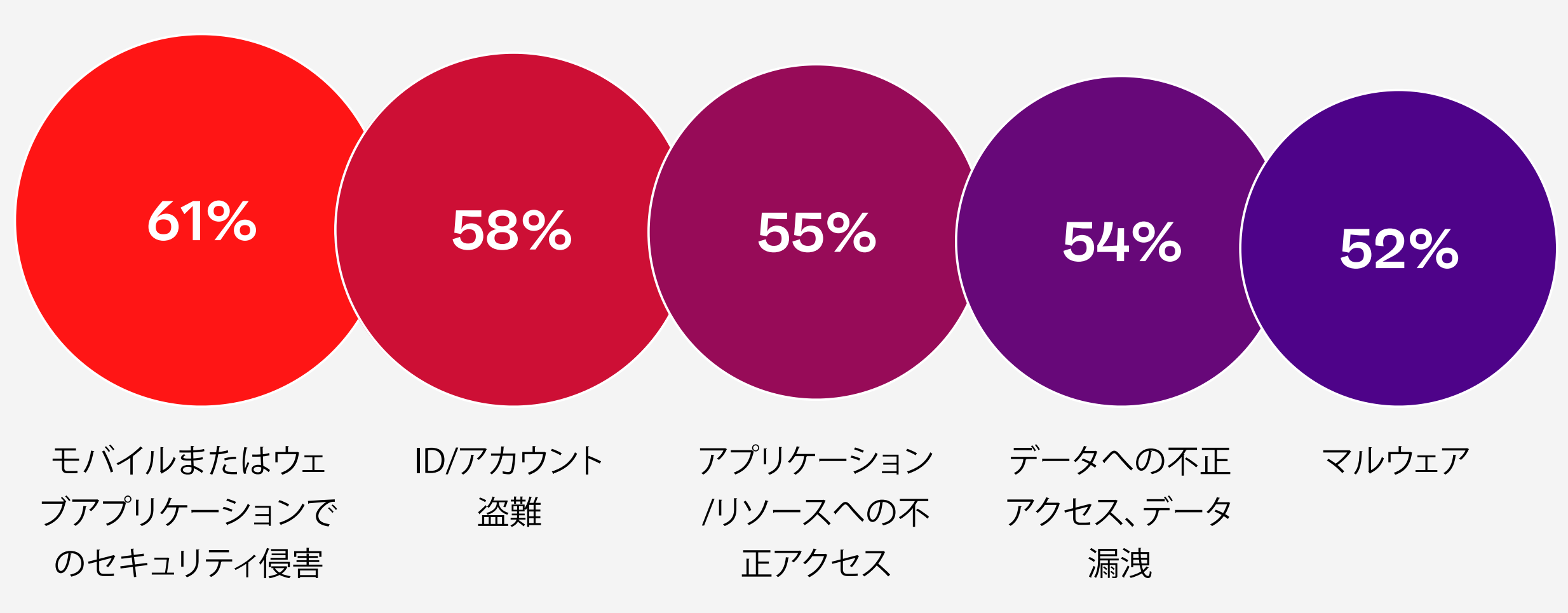
過去12か月、アジア太平洋および日本（APJ）地域のセキュリティ・IT部門のリーダーたちは多くのセキュリティの脅威を経験してきました。増加を続けるこうした課題に取り組むため、リーダーたちはアクセス保護対策を最優先事項とし、ゼロトラストプロトコルに則った予算を計画しています。しかし、様々な業種 — ソフトウェア、金融サービス、製造業 — においては、その優先度は異なります。

IvantiとPulseはAPJ地域のIT・セキュリティ部門長125人を対象に調査を行い、今後12か月におけるアクセス保護の優先度と、アクセス保護対策がセキュリティ問題の発生を低減させるためにどのように利用されるかを明らかにしました。

企業は、セキュリティの脅威に対抗するためにアクセスポリシーを定義する必要があります

過去1年間にわたって、APJ地域の企業の半数以上がセキュリティ攻撃を受けています。多くの場合、組織が影響を受けたのは、モバイルまたはウェブアプリケーションでのセキュリティ侵害（61%）、偽装アカウントおよびID盗難（58%）、アプリ/リソースへの不正アクセス（55%）でした。

過去12か月間に貴社に最も影響を与えたセキュリティ上の脅威は次のうちどれですか？ 5つの中から選択してください。

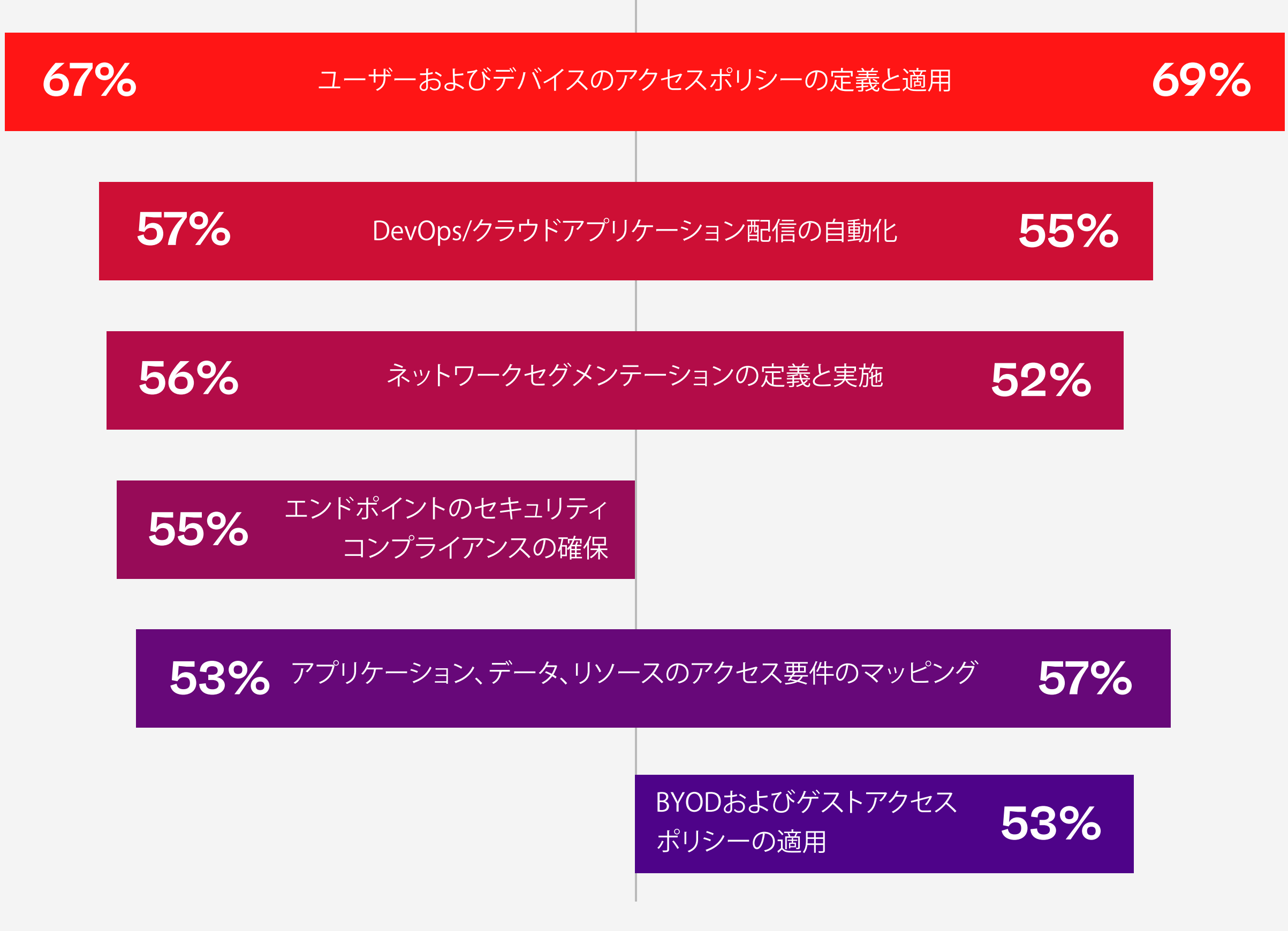


対照的に、北米では最も多く報告されたセキュリティの脅威はマルウェア（51%）、またヨーロッパではアプリケーション/リソースへの不正アクセス（70%）でした。

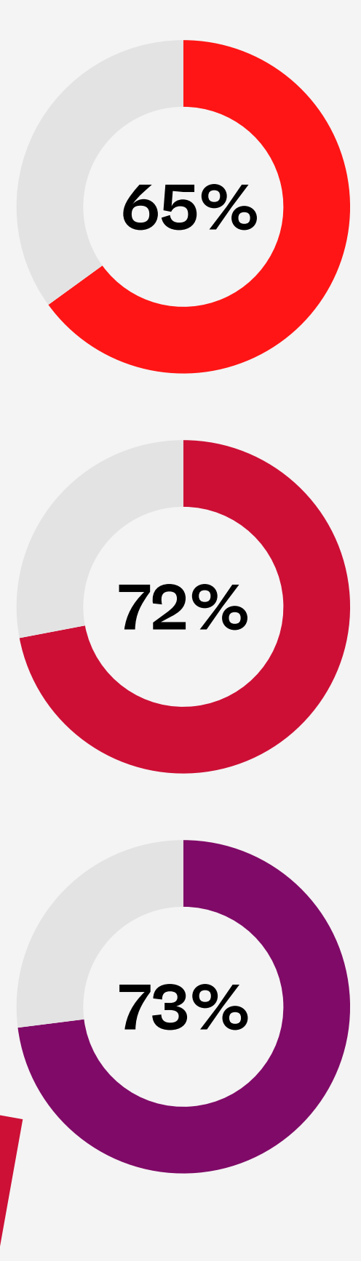
増大するこれらのセキュリティの脅威の影響を低減するため、ITおよびセキュリティ部門長の67%は自身の組織のユーザーとデバイスのアクセスポリシーを定義し実施することが最も重要だと答えています。しかし、最も重要だとされる施策上位5項目中の4項目は、最も実行が難しい施策の上位5項目中の4項目でもあります。

アクセスセキュリティの脅威を軽減するために、組織が実行すべき最も重要なセキュリティ施策は次のうちどれですか？

アクセスセキュリティの脅威/リスクを軽減するために、組織にとって実行するのが最も困難なセキュリティ施策を5つあげるとすればどれですか？



各業種において、脅威を軽減する上で最も重要な施策は何ですか？



ソフトウェア
ユーザーおよびデバイスのアクセスポリシーの定義と適用

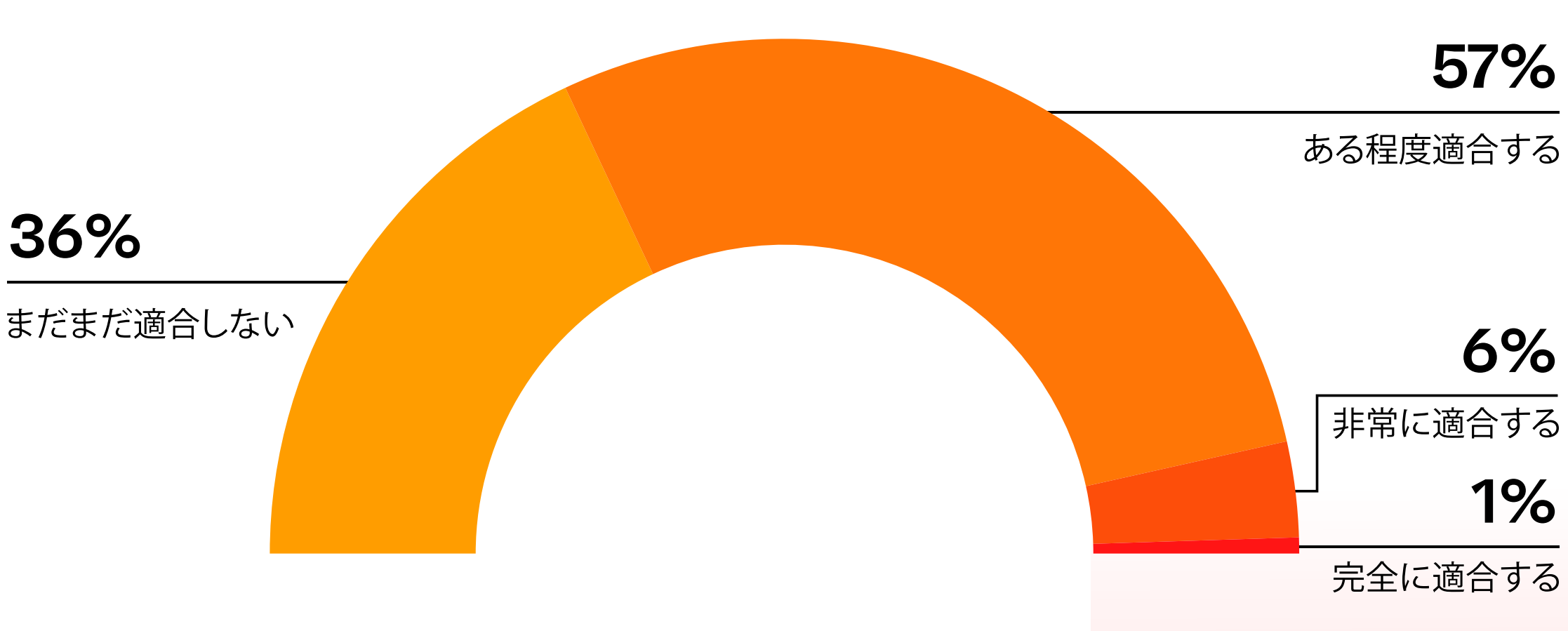
金融サービス
DevOps/クラウドアプリケーション配信

製造
ユーザーおよびデバイスのアクセスポリシーの定義と適用

セキュリティ上の脅威をさらに防ぐために、ITリーダーはゼロトラストとハイブリッドITのセキュリティを優先事項としています

APJ地域のITおよびセキュリティ部門の専門家の100%が、自社のセキュリティ対策は今後12か月でよりゼロトラスト戦略に沿ったものになると回答しました。

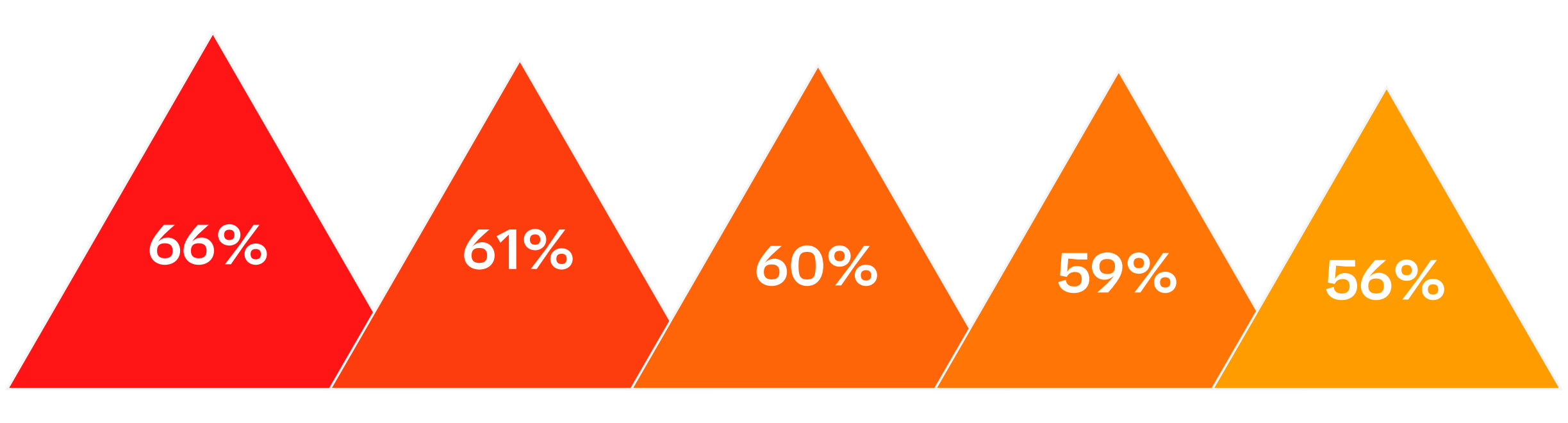
今後12か月で、組織の既存のセキュリティ制御はどの程度ゼロトラストに適合したものになると見込んでいますか？



北米ではAPJ地域に比べてゼロトラストへの調整の優先度が高くなっています。欧米では、ITおよびセキュリティ部門長の21%が来年内にゼロトラストの原則に非常に、もしくは完全に適合すると答えていますが、APJ地域では、その割合は7%に留まっています。

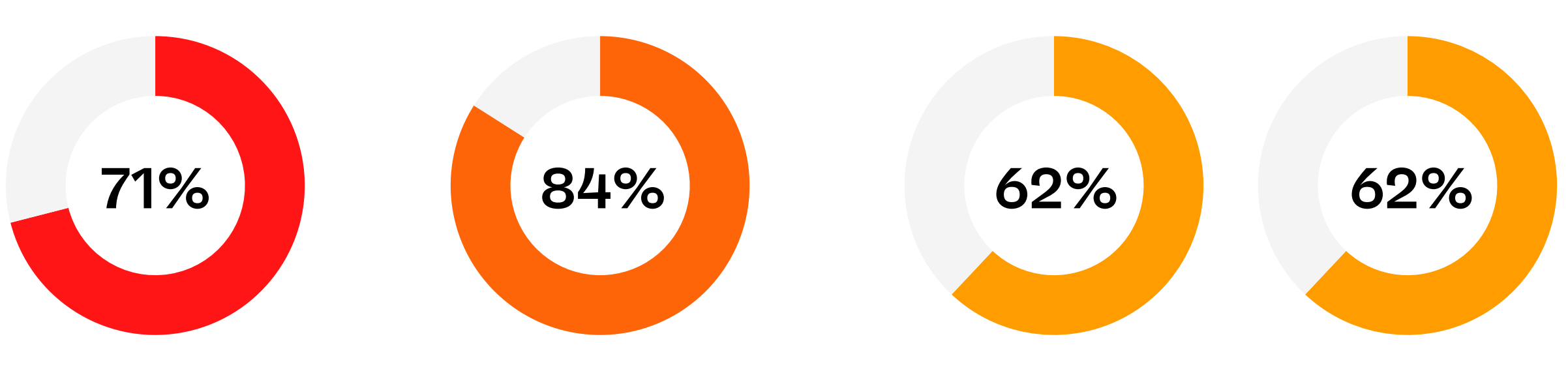
ITおよびセキュリティ部門長は、今後12か月における自身の組織での優先度の高いアクセスセキュリティ対策として、ハイブリッドIT環境全体でのアクセス制御の一貫性を実現する（66%）、アプリワークロードの配信と保護（61%）を挙げています。

今後12か月間で、貴社にとって最も優先度の高いアクセスセキュリティに関する施策はどれですか？



66%	61%	60%	59%	56%
ハイブリッドIT環境全体でのアクセス制御の一貫性の実現	アプリのワークロードの配信と保護を強化（マイクロサービスなど）	エンドポイントのセキュリティ向上とアクセス前の脅威の修復	IoTデバイスの検出、隔離、アクセス制御の強化	IDアクセス管理（IAM）のオーケストレーションの改善

業界別のセキュリティに関する優先度の高い取り組み：

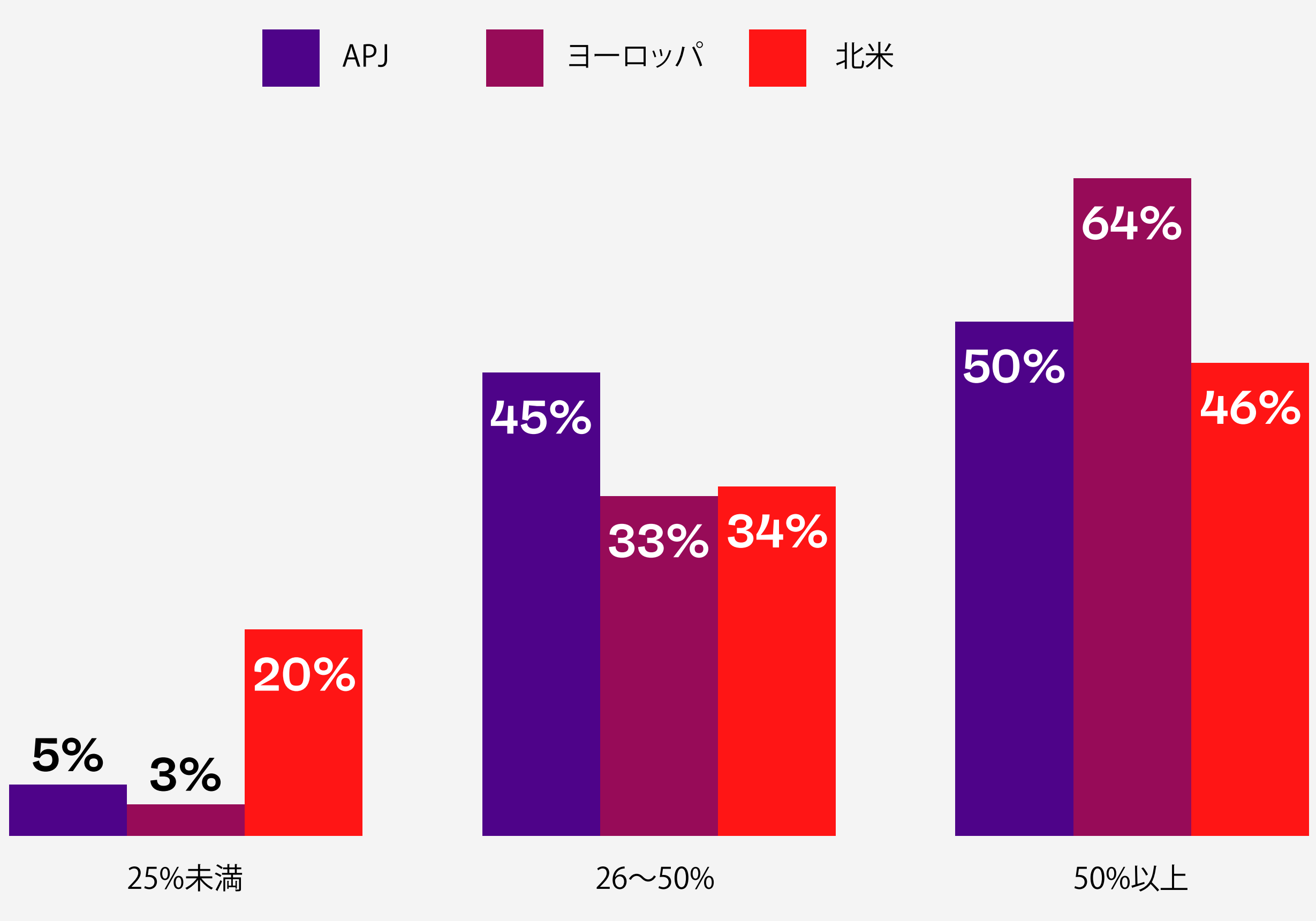


ソフトウェア	金融サービス	製造	製造
71%	84%	62%	62%
エンドポイントのセキュリティ向上とアクセス前の脅威の修復	ハイブリッドIT環境全体でのアクセス制御の一貫性の実現	アプリのワークロードの配信と保護の強化（マイクロサービスなど）	IDアクセス管理（IAM）のオーケストレーションの改善

APJ地域の企業は、他のどの地域よりもクラウド型セキュリティサービスを活用し、ベンダーの統合を計画しています

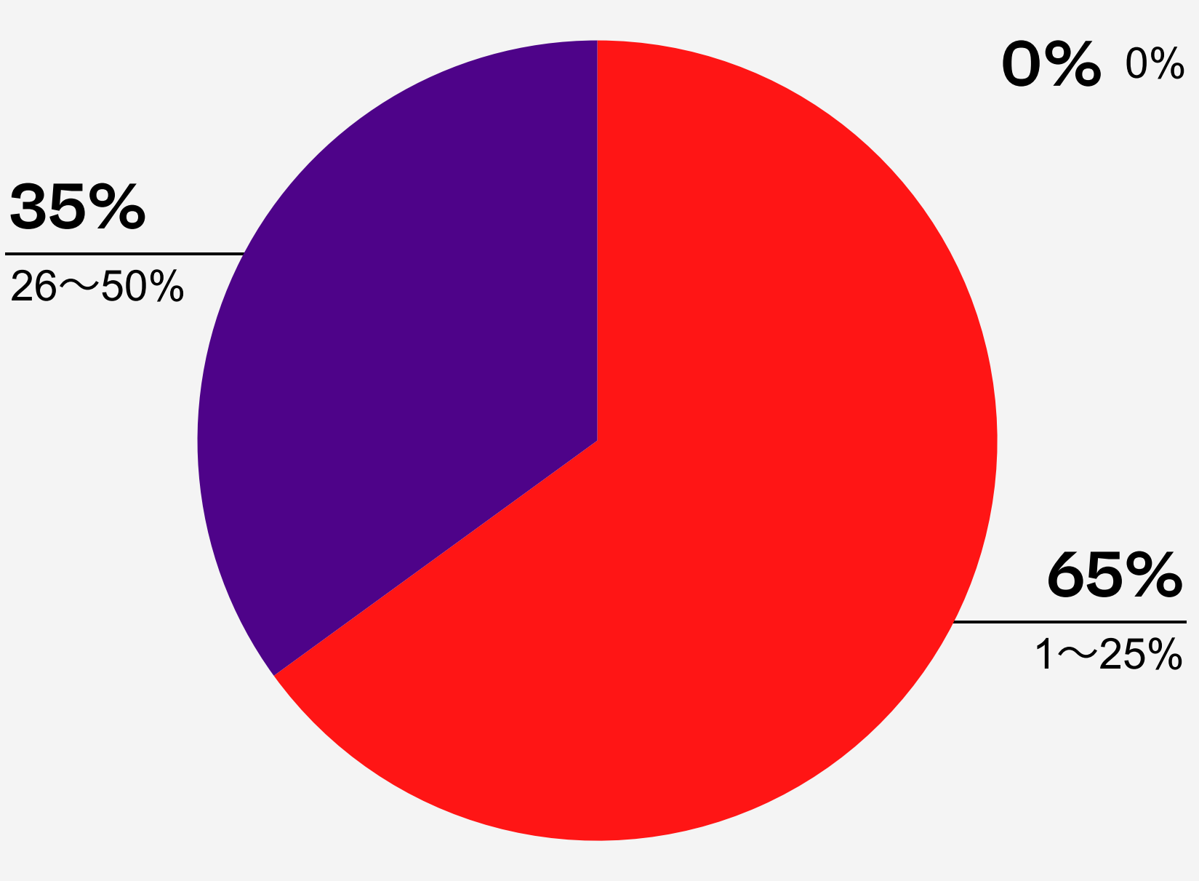
APJ地域を拠点とするITおよびセキュリティ部門長の95%は自身の会社のセキュリティサービスの4分の1以上をクラウドに移行したと述べています

貴社で、従来のオンプレミスのセキュリティツールからクラウドに移行したセキュリティサービスはどのくらいありますか？



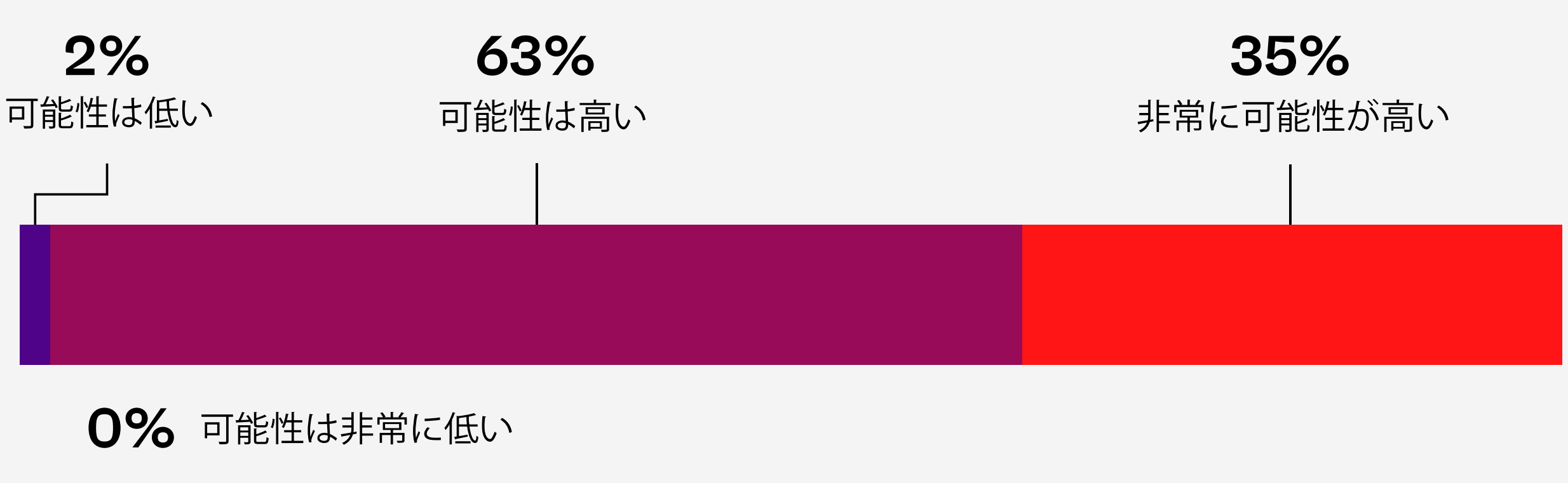
また3分の1以上（35%）の回答者が、来年、クラウド型セキュリティサービスの予算を25%以上増額するだろうとしています。APJ地域では予算を現状維持するとした回答者はいませんでした。

今後18か月以内に、貴社ではクラウド型のセキュリティサービスへの投資をどの程度増やす予定ですか？



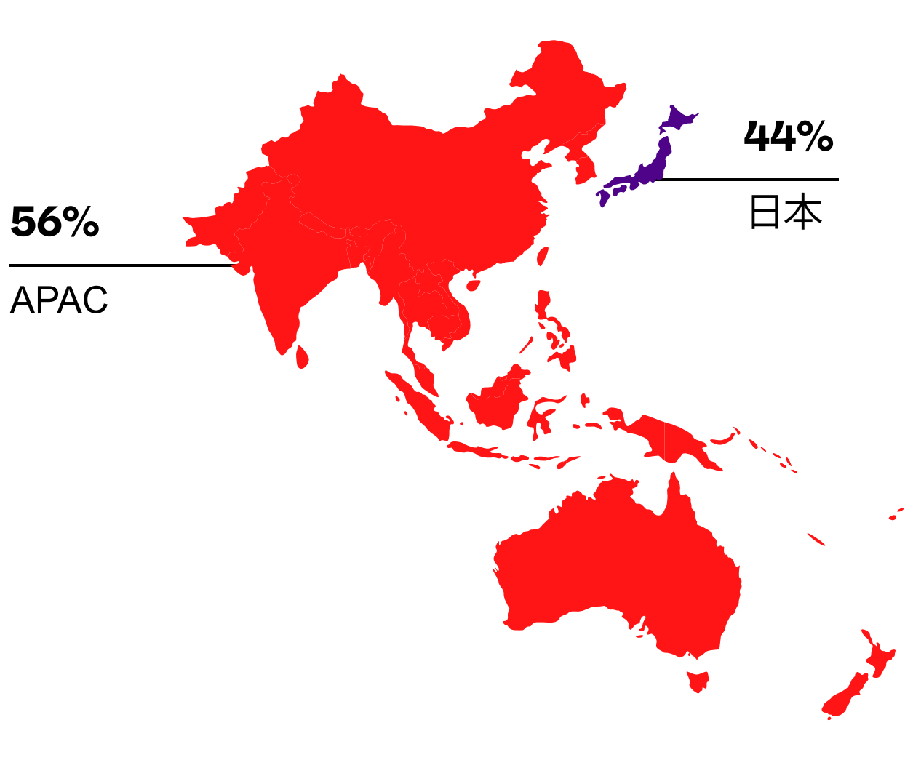
最後に、圧倒的多数の回答者（98%）が、現在セキュリティベンダーを統一プラットフォームに統合している、または数か月以内にその予定があるとしています

今後12か月以内に、それぞれのセキュアアクセスツールをより少ないベンダーに選別し、統合されたプラットフォームに統合する可能性はどの程度ありますか？

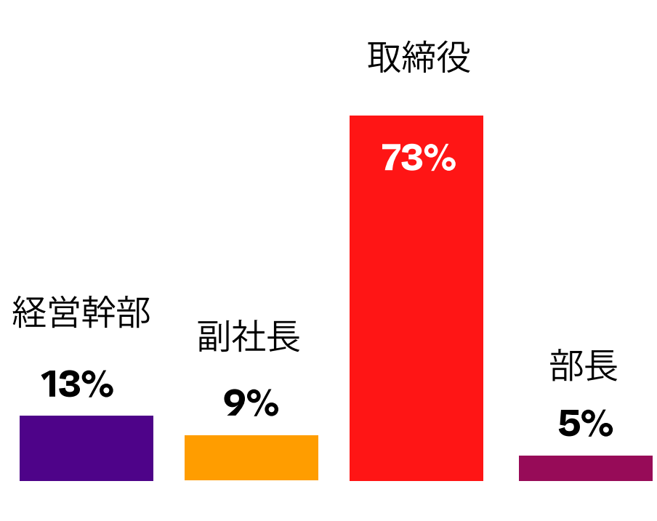


回答者の内訳

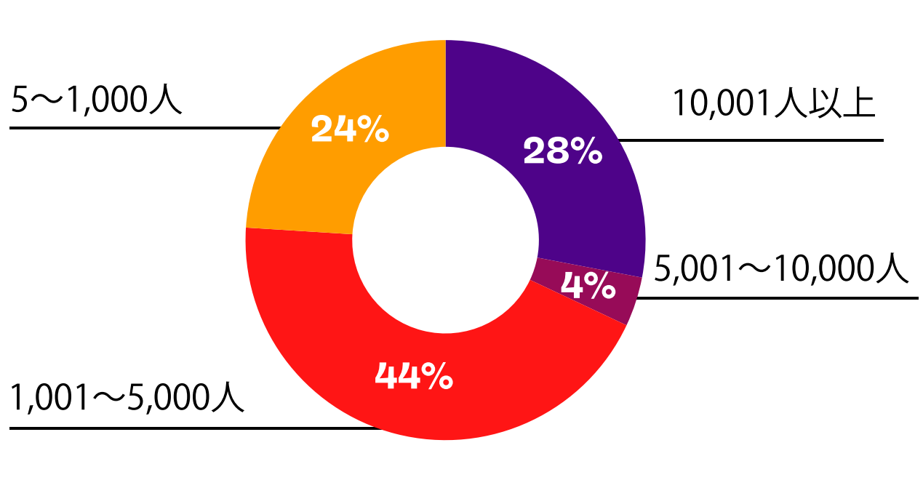
地域



役職



企業規模（従業員数）



データ収集期間：2020年10月1日〜11月23日

回答者：ITおよびセキュリティ部門長125人

インサイト提供：PULSE