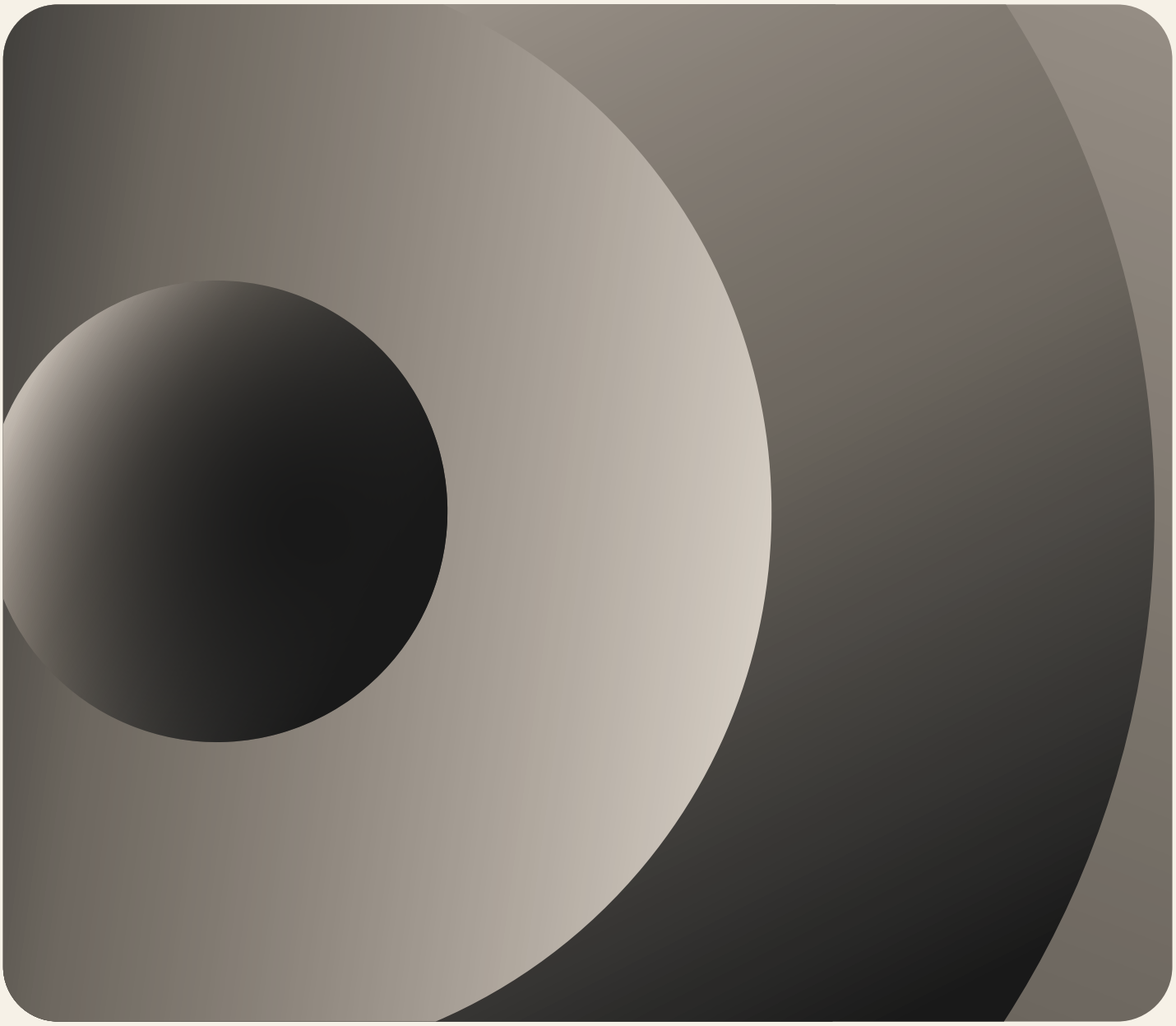
2023 年版

全世界におけるアイデンティティ / アクセス管理の取り組みを評価

ゼロトラストセキュリティの現状 2023



okta

目次

調査手法

本調査について

Okta は Qualtrics との提携により、2023 年 4 月に全世界のさまざまな業界で情報セキュリティの意思決定者を対象とした調査を実施しました。ここでの意思決定者は、「テクノロジー購入の意思決定に責任を負うディレクター以上の従業員」と定義されます。調査は、13 か国の Qualtrics パネルを通じて英語と日本語で行われました。以下、今回の調査を「本調査」「調査」と呼び、組織に代わって回答した人を「調査回答者」「回答者」と呼びます。

調査回答者

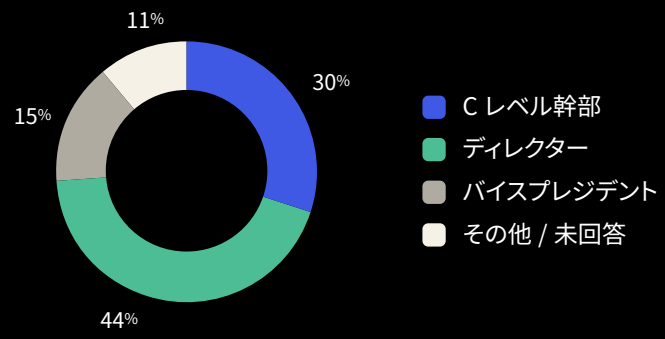
調査のサンプル総数は、北米（米国、カナダ）、EMEA（デンマーク、フィンランド、フランス、ドイツ、アイルランド、オランダ、ノルウェー、スウェーデン、英国）、APJ（日本、オーストラリア）の情報セキュリティ意思決定者 860 人です。本レポートは、医療、公共部門、金融サービス、ソフトウェアの各業界に焦点を当てていますが、その他の業界も含みます（地域と業種は回答者の自己申告に基づきます）。公共部門は、世界の 3 つの地域すべての組織を含みますが、州や地方組織は含みません。調査対象は、C レベル幹部、バイスプレジデント、ディレクターです。本調査は、Okta の従業員や顧客を対象としたものではありません。

調査手法の詳細

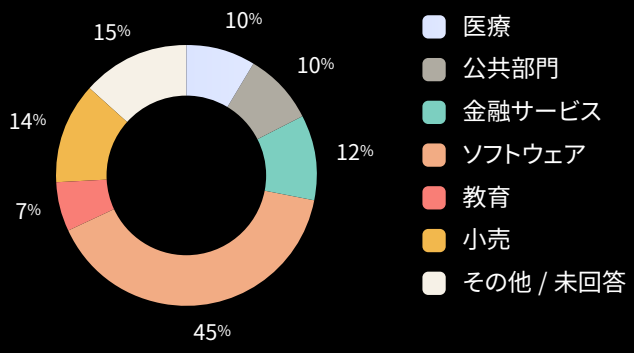
図表に示す「世界全体」または「全回答者」の回答には、全業種（重点 4 業種以外も含みます）および全地域（NAM、EMEA、APJ のいずれかの地域を特定したかどうかにかかわらず）の回答者が含まれます。便宜上、図表のデータはすべて、小数点以下を四捨五入し、0.5 未満の値は 0 に切り捨てています。そのため、図表の合計が 100% にならないことがあります。また、回答者が関連する複数の質問に「はい」と回答した場合（特定の取り組みを実施したことと、今後も実施する予定であることの両方を回答した場合など）、図表の合計が 100% を超えることがあります。

調査回答者の属性

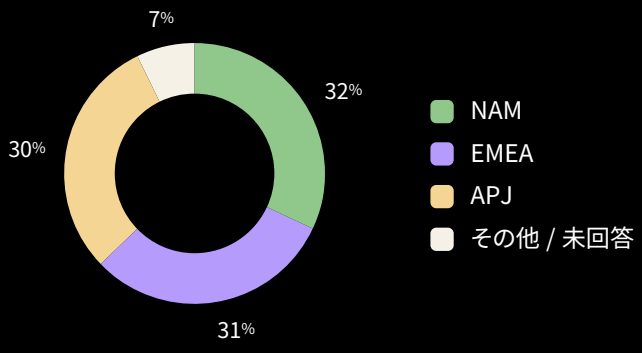
回答者の役割



企業の所属業界



企業の所在地域



ゼロトラストは目標から計画へ

組織が人、資産、インフラストラクチャの安全に維持する方法として、ゼロトラストの採用が拡大しています。

10 年前、ゼロトラストはセキュリティの理想であり、実現不可能なものと考えられていました。ゼロトラストという用語は、「決して信用せず、常に検証する」をセキュリティの理想として掲げる必要性が高まる中、この原則を端的に表現するものとして、Forrester のリサーチャー、John Kindervag 氏が 2010 年に編み出したと言われています。ゼロトラストは、理念から実現困難な目標へ、そして日々の運営上の現実へと、急速に進歩してきました。Okta が毎年実施しているゼロトラストの現状調査が示すように、この理想をビジネス戦略として全面的に採用している組織や、今後数か月でゼロトラストセキュリティを完全に導入するために具体的に取り組んでいる組織が、かつてないほど増えています。

実際、Okta が 2019 年にゼロトラストの現状レポートの発行を開始して以来初めて、ゼロトラスト戦略を策定し実施している組織の数は、依然として計画段階にある（あるいは、注力するほど重要であると考えていない）組織の数をはるかに上回っています。明らかに流れが変わったのです。

こうした状況は、侵害やデータ窃取が急増していることや、NIST や CISA が指針を示していることを踏まえると、それほど驚くべきことではありません。Identity Theft Resource Center の 2022 Annual Data Breach Report によると、昨年は米国で 1,802 件のデータ侵害が発生し、4 億 2,200 万人以上が影響を受けました。いつものことですが、こうした猛攻撃の中心にあるのがアイデンティティです。Javelin の 2022 Identity Fraud Study によると、2022 年には、米国で発生した個人情報詐欺の被害額だけで 430 億ドルに上りましたが、2021 年にアイデンティティ窃取により 520 億ドルの被害が出た中で苦戦を強いられたことが伺われます。米国司法省の 2023 年版報告書は、「個人情報詐欺が全世界のほぼすべての主要な犯罪に利用されており、世界中の国と市民の安全保障に対する脅威となっている」ことを示しています。

企業のセキュリティチームが現代の脅威と高度化している攻撃者に対抗するための最善の戦略は、ゼロトラストの中核となる「決して信用せず、常に検証する」という原則を守ることです。ゼロトラストセキュリティ戦略は、クラウドセキュリティの世界を想定していない従来のサイバーセキュリティのアプローチの枠を超えて進化し、アイデンティティをセキュリティ態勢の主要な推進力として位置づける上での基盤となります。多くの組織にとって、従来のアイデンティティは完全に IT チームの担当範囲でした。しかし、Okta のデータが示すように、今日ではセキュリティチームが大部分の（多くの場合、完全な）コントロールを担うようになっています。しかし、ゼロトラストの恩恵を受けるのは SecOps チームだけではありません。このベストプラクティスを導入する組織は、ネットワークインフラストラクチャ全体でアイデンティティ管理を活用して、新たな効率化やワークフォースエクスペリエンス / カスタマーエクスペリエンスの改善を実現できます。

マクロ経済のトレンドとクラウドのイノベーションにより、現代の組織は複雑なハイブリッド / マルチクラウドのエコシステムを採用するようになっています。その中で、パートナー、請負業者、外部ベンダーといった境界のない多様な業務ユーザー（ワークフォース）が、分散したリソースと IT 環境にアクセスしています。これらすべてを束ねる役割を果たしているのがアイデンティティです。強力なアイデンティティ管理は、複雑なグローバルワークフォースチームが安全かつ生産的なコラボレーションを行うための重要インフラストラクチャと考えられています。今年のデータが示すように、組織はモバイルデバイス管理を強化し、従業員だけでなく外部の協力者にもシングルサインオン（SSO）や多要素認証（MFA）を適用し、プロビジョニング / デプロビジョニングのワークフローを自動化し、企業資産（と人）の安全を守るために強力なゼロトラストの取り組みを実施することに注力しています。

ゼロトラストの実現は、一連のステップを経て推進していく必要があります。数十年続けてきたプラクティスやプロセスを改め、セキュリティスタックを再構築し、投資やソフトウェア廃止に関する厳しい意思決定を行うことは、最良の時であっても困難なことです。そして、金融関連ニュースにさっと目を通しただけでも明らかなように、今は最良の時ではありません。しかし、Okta の年次調査の対象となったグローバル組織は、適切なテクノロジーとベンダーを活用することで、問題を簡素化して迅速に歩みを進めています。本レポートの洞察を生かすことで、今日の先進的な成長組織がゼロトラストセキュリティの取り組みを「どこで」「どのように」実施しているかを理解できます。これにより、ゼロトラスト実現の道のりで目標設定から計画実施へと進んでいく上での適切なステップを特定できます。

ゼロトラストへの取り組みは飛躍的に拡大し続けている

ゼロトラストの取り組みを策定し実施している組織の数は、飛躍的に増え続けています。ゼロトラストに取り組んでいる組織の割合は、2021 年には調査対象の 4 分の 1 未満でした。しかし、2022 年には半数を超え、今年はさらに 61% へと増加しました。現在、多くの企業がゼロトラストの取り組み計画を急務として実施に移しています。その中で、依然として今後 18 か月以内に実施予定としている組織の割合は、前年比で減少しています。現在、調査対象となった組織の 6 割以上は、すでにゼロトラストの実現に向けて着実に前進しています。その他の組織についても、大部分が計画段階にあります。

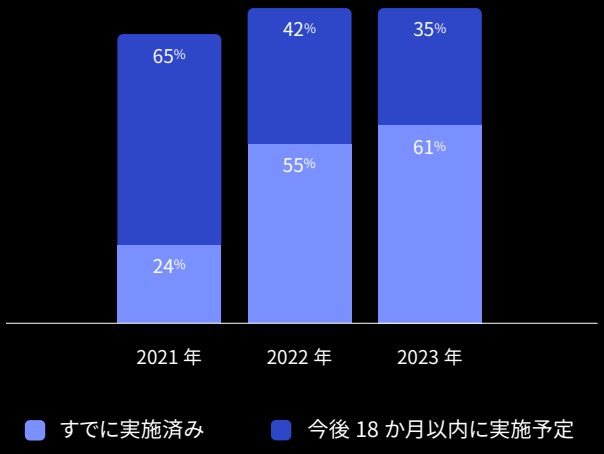
企業規模別のデータを詳しく見ると、小規模組織（従業員数 500 ～ 999 人の組織）では、大企業に比べてゼロトラストセキュリティの取り組みを策定し実施している割合が低くなっています。最も活発なのは従業員 5,000 ～ 9,999 人規模の企業で、4 社中 3 社がゼロトラストの取り組みを策定し実施していると回答しています。どの規模区分においても、現在ゼロトラストの取り組みを未策定であり、また今後 18 か月以内に策定する予定もない組織は、ごく少数（すべての区分で 10% 未満）にとどまっています。

全世界でゼロトラスト計画がビジネスの日常的な現実になりつつある

世界全体では、61% の組織がゼロトラストセキュリティの取り組みを策定し実施しています。28% は今後 6 ～ 12 か月以内に実施する予定であり、さらに 7% が今後 13 ～ 18 か月以内に実施する予定です。この全体的な傾向は、全地域に共通しています。北米地域は、他地域に先んじて取り組みを着実に進めています。一方、EMEA や APJ を拠点とする組織は急速に地歩を固めつつあり、両地域でゼロトラストの取り組みを実施していない組織も、大部分が今後 6 ～ 12 か月あるいは 13 ～ 18 か月以内に開始する予定です。

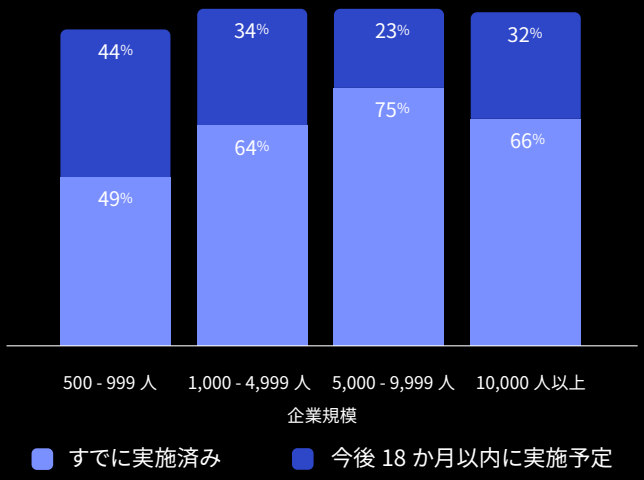
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか? または、今後 18 か月以内に実施する予定ですか?

全回答者



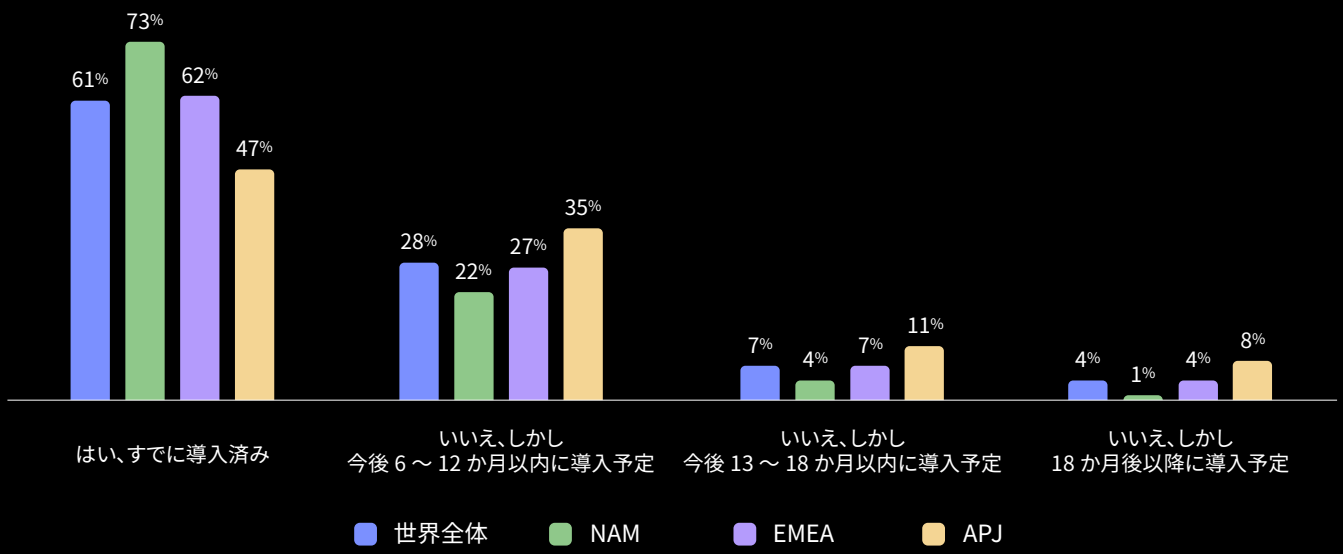
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施してしていますか? または、今後 18 か月以内に開始する予定ですか?

企業規模別の比較

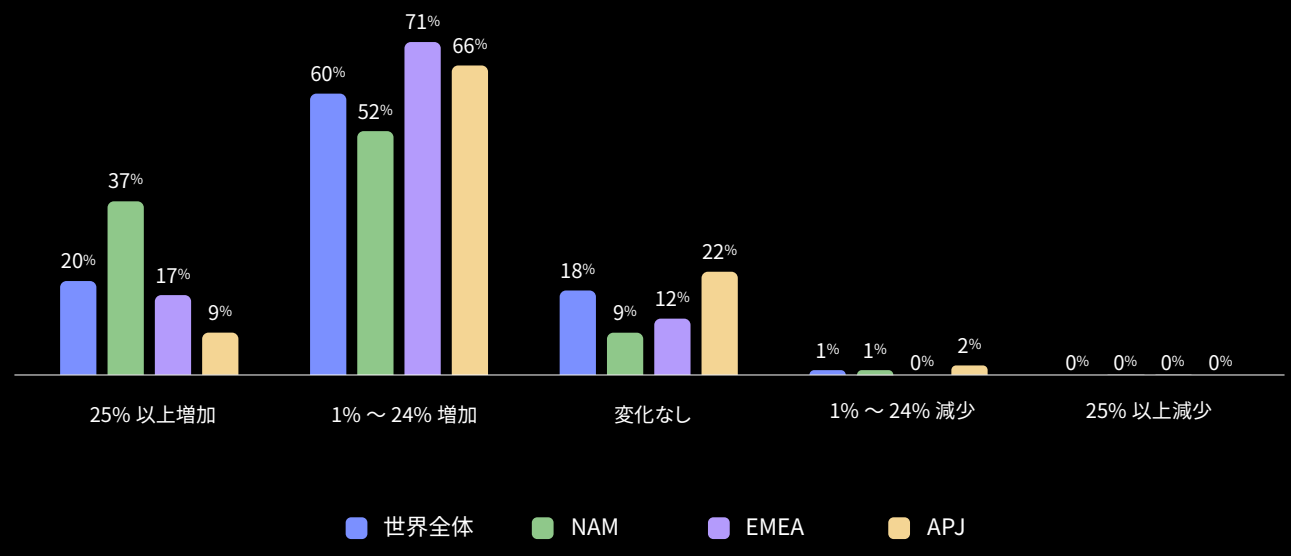


あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか? または、今後 18 か月以内に開始する予定ですか?

地域別の比較



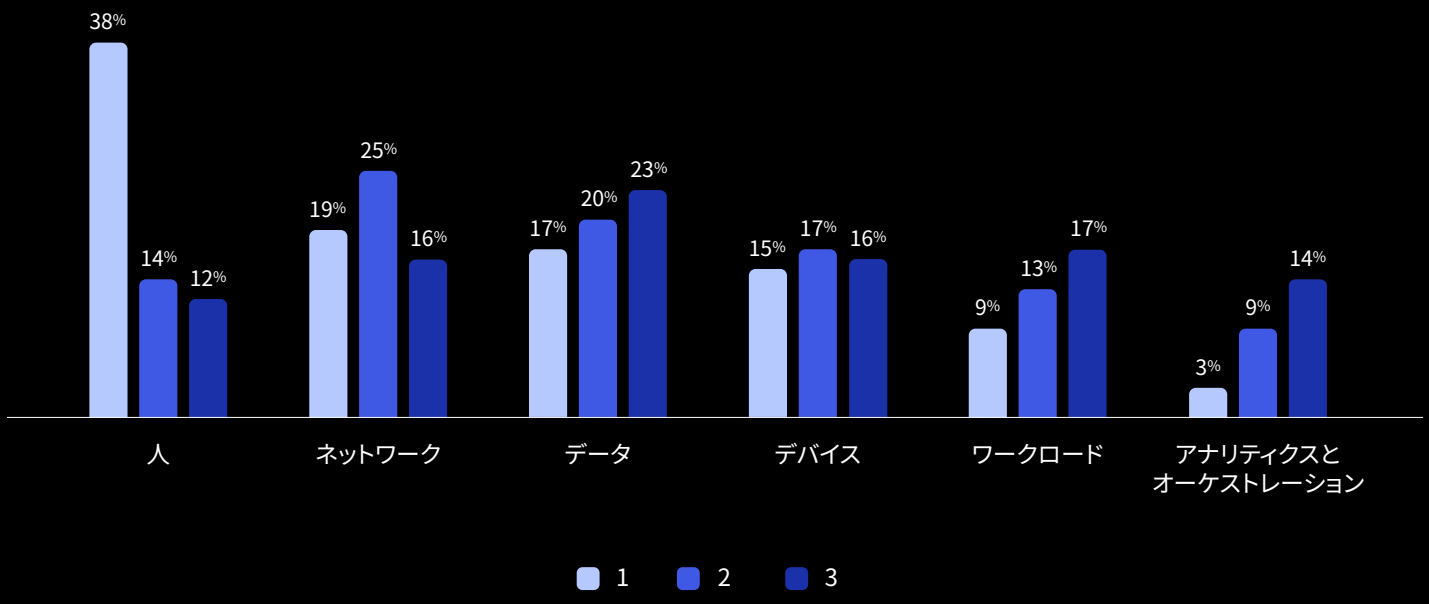
過去 12 ～ 18 か月で、ゼロトラスト予算はどのように変化しましたか（該当する場合）？
地域別の比較



あなたの組織のセキュリティプロジェクトで、以下の領域の優先度を評価してください。

（1 = 最高、3 = 最低）

全回答者



ゼロトラストの取り組みの予算は健全に推移

現在のマクロ経済的要因によって、あらゆる地域や業界で人材やコストの削減が進められています。このような時期においても、ゼロトラストセキュリティは予算を削ることができない重要な取り組みであると認識されているようです。実際に、調査対象となった企業の圧倒的大多数では、こうした予算は堅実に推移しているどころか、この 12 ～ 18 か月でむしろ増加しています。世界全体で見ると、60% の組織が昨年比で 1 ～ 24% 増加させ、さらに 5 社に 1 社はそれ以上増加させています。一方、調査対象組織のうち予算を減らした割合は、どの地域でも 3% 未満でした。

一方、日本だけに目を向けてみると、少し異なった状況が確認できます。41% の組織が予算を昨年比で 1 ～ 24% 増加させ、12% は 25% 以上増加させている一方、49% の組織は予算に変化なしと回答しています。

セキュリティプロジェクトでも依然として「人」が最優先

回答者に組織のセキュリティが懸念される領域の上位 3 つを尋ねたところ、今年は「人」が圧倒的に多く挙げられ、2 位の「ネットワーク」と 3 位の「データ」を大きく引き離しました。これまでも、「人」は最優先事項とされてきました。しかし、今年はかつてないほど多くなっており、ゼロトラストセキュリティの取り組みでアイデンティティが果たす重要な役割に対して理解が高まっている状況を反映しています。

ゼロトラストは目標から計画へ

重要ポイント

ゼロトラストは行動計画から通常業務へと急速にシフトした。

かつてゼロトラストを仮説的なフレームワークとみなしていた組織も、全体としては、そうした計画を実行に移しているか、その途上にあります。この動きは急激に進展しています。2021 年には、ゼロトラストの戦略的取り組みを実施していると回答した割合はわずか 24% でしたが、昨年は 55%、今年は 61% へと増加しました。これは、地域や組織規模を問わず、全体的に見られる傾向となっています。今回焦点を当てている 4 業種の中では、金融サービスが僅差でリードしており、71% の組織がすでにゼロトラストの取り組みを実施しています。これに、ソフトウェアが 69% で続いています。地域別では北米が最も進んでおり、73% の組織がゼロトラストの取り組みを策定し実施しています。APJ は、ゼロトラストの取り組みを実施している割合が最も低く（47%）なっていますが、今後 6 ～ 12 か月以内にゼロトラストの取り組みの実施を計画している割合は最も高く（35%）なっています。

今やアイデンティティは、ゼロトラスト戦略においてミッションクリティカルな要素であることが広く理解されている。

わずか 1 年で大きな変化が起こりました。昨年は、回答者の 71% がゼロトラストセキュリティ戦略にとってアイデンティティが重要であると考えていましたが、ビジネスにとって重要であると考える回答者は 27% にとどまっていました。今年は一転して、回答者の 51% がアイデンティティを「非常に重要」、40% が「ある程度重要」であると回答しました。強力なアイデンティティ / アクセス管理（IAM）が、ハイブリッド / マルチクラウドの世界で人と資産を安全に保つための基盤となる戦略であることを理解する組織が増えていることを踏まえると、このような認識の変化は驚くことではありません。

ゼロトラストの予算は、市場原理に逆らうかのごとく依然として増加し続けている。

さまざまなマクロ経済的圧力によって予算の引き締めが世界的に起こっている中、ゼロトラストの支出は増え続けています。今年、調査回答者の実に 80% が、ゼロトラストセキュリティの取り組みに対する予算が前年より増加したと報告しています。1 ～ 24% の増加を選択した回答者は 60%、大幅な増加（25% 超）を選択した回答者も 20% いました。この年次レポートでは、コストの懸念が主要な懸念事項として 3 年連続で挙げられています。しかし、際限なく続く詐欺や内部脅威、さらにハイブリッド業務や縛りのないクラウドアクセスに対する需要を受け、規模や業種を問わずあらゆる企業が、アイデンティティに裏打ちされたセキュリティ対策に注力（また、予算を投入）することを迫られています。

ゼロトラストの採用を目指す企業は、依然として困難な課題に直面している。

今年の調査では、ゼロトラストを確立する上での最大の課題として、コストの懸念とテクノロジーのギャップが挙げられ、次いでプライバシー規制 / データセキュリティ、人材 / スキル不足が挙げられました。ただし、状況は変化しました。これまでは、特定の懸念が単独で、その他の懸念をはるかに上回る傾向がありました。しかし、今年はこうした偏りが弱まり、統合しやすさ、ソリューションの認知度、監査コンプライアンス、ステークホルダーの賛同にも回答が分散しています。これに関連して、企業内での IAM のコントロールについても、これまではIT 部門の担当でしたが、主としてセキュリティチームが担う共有責任へと大きく移っています。

アイデンティティはゼロトラストの中核

最新のセキュリティにおけるアイデンティティの中心的役割が、世界的に受け入れられつつある。

従来のネットワーク境界がほとんど消滅した状況では、アイデンティティが新たな境界となり、防御の出発点としての役割を果たすようになっています。世界中のどこからでも、また多様な承認 / 未承認デバイスを使用して、自社のリソースにアクセスしようとするすべての人やマシンのアイデンティティを検証することは、現代の課題となっています。

しかし、その管理を実現することは、ビジネスの成功に他なりません。今年のデータが示すように、業界を問わずあらゆる規模の企業が、アイデンティティが単なるセキュリティ対策ではなく、ビジネスを安全に拡張し、収益の拡大、顧客ロイヤリティの強化、資産やブランド評価の保護など、多くのメリットを実現するための手段であることを理解しつつあります。

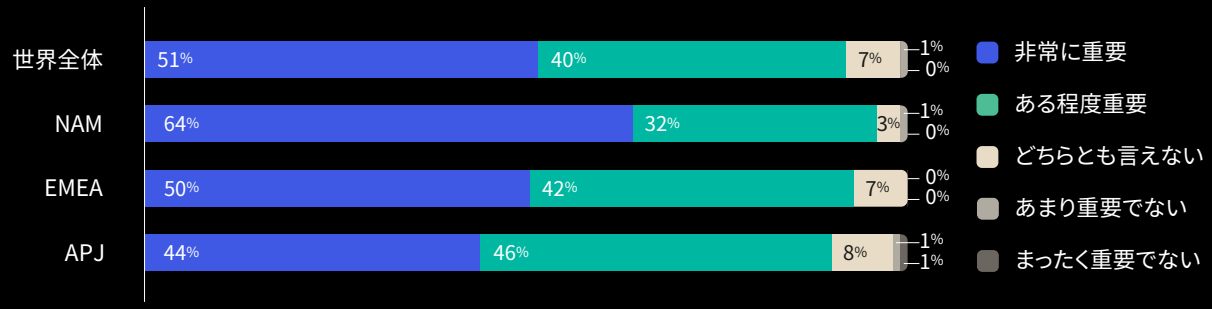
こうしたトレンドは 2023 年の調査結果にも反映されており、組織はゼロトラストの取り組みの一環として、これまで以上にアイデンティティを重視していることを明確に打ち出しています。過半数の回答者が、ゼロトラストセキュリティ戦略にとってアイデンティティが「非常に重要」であると回答しており、2022 年から大きく増加しています。後述するとおり、これはすべての地域で見られる傾向となっています。

「IT リーダーは、セキュリティとビジネスの両方の目標に沿う形で IAM に投資するようになっています。効果的な IAM は、認可、ポリシーの適用、プロビジョニング / デプロビジョニングのための安全なプロセスを実現します。これにより、摩擦を最小限に抑え、ビジネスのオペレーションを強化できるので、セキュリティと生産性の両面で改善が可能になります」

— Identity-Defined Security Alliance、2022 Trends in Securing Digital Identities Report

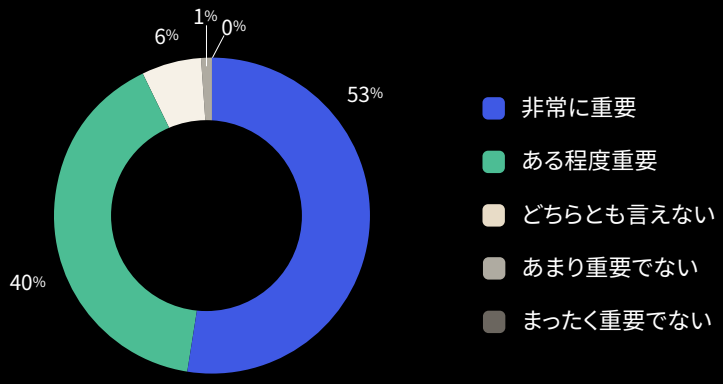
ゼロトラストセキュリティ戦略全体で、アイデンティティはどの程度重要ですか?

地域別の比較



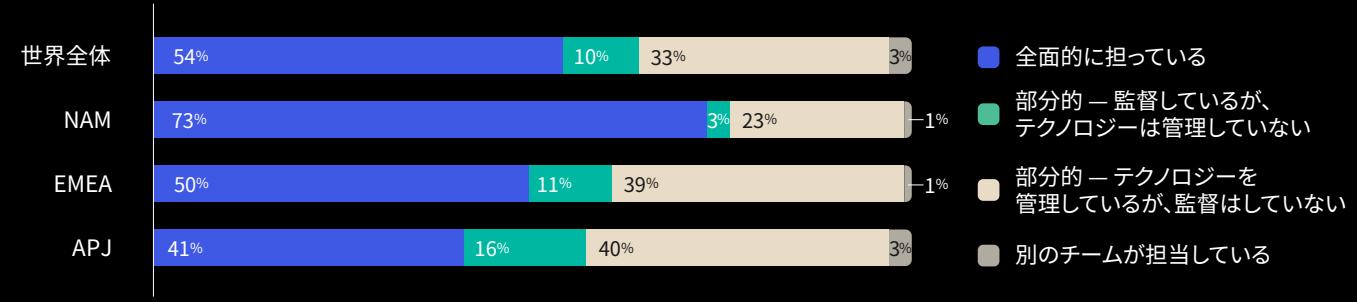
ゼロトラストセキュリティ戦略全体で、アイデンティティはどの程度重要ですか?

C レベル幹部の回答者



あなたの組織のセキュリティ部門は、IAM の制御をどの程度担っていますか?

地域別の比較



注：データラベルを四捨五入して整数にするため、棒グラフの合計が 100% にならないことがあります。

アイデンティティの重要性は明らか

ゼロトラストの取り組みを推進する上で、アイデンティティの重要な役割はますます明確になりつつあります。ゼロトラストセキュリティ戦略全体でアイデンティティが「非常に重要」であると回答した割合は、昨年は世界平均で 27% にとどまりましたが、今年は 51% へと増加しました。地域別に見ると、北米が最も進んでおり、回答者の 3 分の 2 近くがアイデンティティを「非常に重要」であると考え、3 分の 1 近くが「ある程度重要」であると考えています。EMEA と APJ の両地域では、アイデンティティの重要性について「どちらとも言えない」と答えている回答者がそれぞれ 7% と 8% となり、依然として認識の壁が立ちはだかっている可能性があります。とりわけ APJ 地域では、アイデンティティの重要性について「あまり重要でない」または「まったく重要でない」を選択した回答者が少数ながら（2%）存在します。

日本では 39% が「非常に重要」、35% が「ある程度重要」と回答している一方、19% が「どちらともいえない」、7% が重要でないと回答しており、世界全体と比較するとアイデンティティの重要性に関する認識が低い傾向が見受けられます。

C レベル幹部の見解

C レベル幹部の回答者の大多数は、昨年の調査時と同様、引き続きアイデンティティを優先させています。今年、C レベル幹部の回答者の過半数は、アイデンティティがゼロトラスト戦略にとって「非常に重要」であり、さらに 40% が「ある程度重要」であると回答しました（昨年、アイデンティティがミッションクリティカルであると回答した C レベル幹部は、わずか 26% でした）。このように、現代のセキュリティにおけるアイデンティティの重要な役割に対する一般的な理解が、かなり浸透してきた状況に注目すべきです。

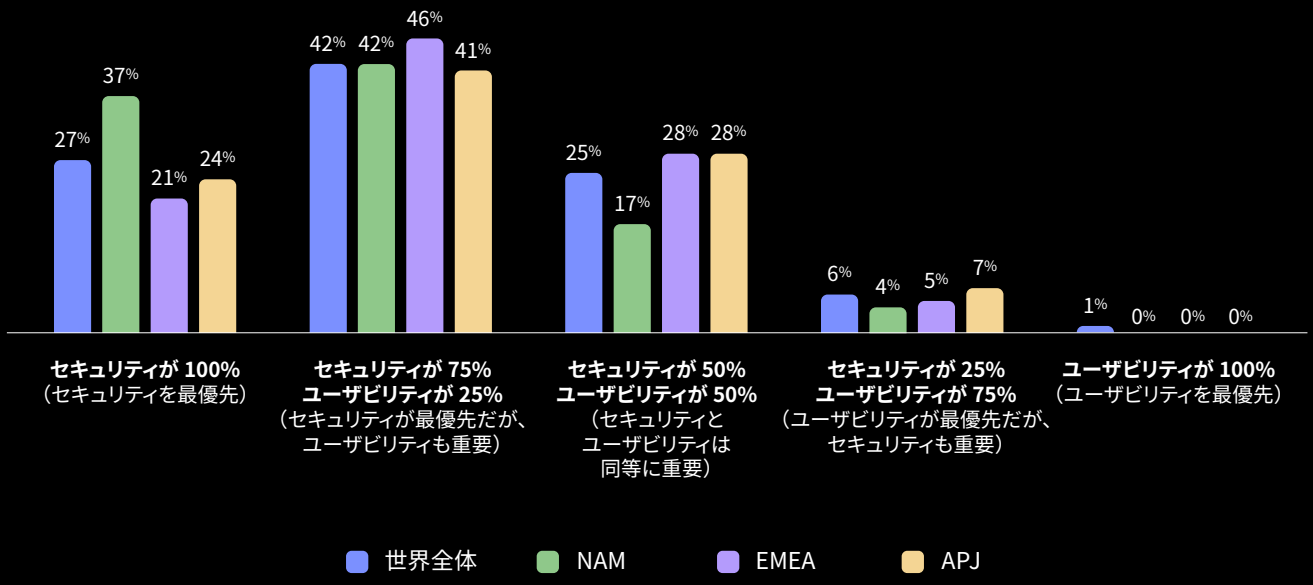
日本の C レベル幹部の認識も高くなっており、45% が「非常に重要」、40% が「ある程度重要」と回答しています。世界全体と比較して若干低い傾向ではあるもののゼロトラスト戦略におけるアイデンティティの重要性の認識が進みつつあります。

IAM の責任は変化している

セキュリティに対する企業のアプローチの急速な進化は、組織内で誰が IAM のコントロールを担っているのかを追跡することによっても理解できます。アイデンティティは、以前は主に IT 部門が担当していましたが、フィッシングのようなアイデンティティベースの脅威が攻撃の主流となる状況が続く中、近年はセキュリティチームへと責任が移行しつつあります（Verizon の 2023 Data Breach Investigations Report によると、昨年起きた侵害の 74% で人的要素が関与しています）。現在、EMEA では半数の組織でセキュリティ部門が IAM を担当しており、この割合は北米では 73% に上ります。APJ では、担当部門はより分散しており、セキュリティ部門に IAM の完全な管理を委ねている組織は 41% にとどまっています。56% の組織では、セキュリティ部門がアイデンティティを監督するか、テクノロジーを管理するかのどちらかであり、両方を担っていません。

日本では、45% の組織でセキュリティ部門が全面的な管理を担っている一方、38% の組織では部分的な管理、17% の組織では別の組織での管理となっており、他国と比較して、担当部門がさらに分散している傾向が見られます。

あなたの組織では、セキュリティの重要性とユーザビリティの重要性のバランスをどのように取っていますか?
地域別の比較



全体として、セキュリティはユーザビリティよりも優先されている

最新のハイブリッド / マルチクラウドの企業ネットワークでは、攻撃対象領域が急拡大しており、組織はアイデンティティベースの脅威に対してますます脆弱になっています。その結果として、企業は優先度のバランスを変更し、（場合によっては劇的に）ユーザビリティよりもセキュリティを優先するようになっています。世界全体では、3 社に 2 社以上が、セキュリティが文句なしに最優先事項であるか、または現在の優先度のバランスがセキュリティが 4 分の 3、ユーザビリティが 4 分の 1 であると回答しています。これは、2021 年（コロナ禍でリモートワークへの移行が急速に進んだ時期）にユーザビリティが最優先された状況からの大きな変化です。セキュリティが最優先事項であると答えた割合は、北米が 37% であったのに対し、EMEA は最も低くなりました（21%）。

日本では、他国と比較するとユーザービリティを重視すると回答した割合が高い傾向（合計で 13%）が見られ、セキュリティとユーザビリティの両方を考慮する必要があることを示唆しています。

ワークフォースアイデンティティの成熟

アイデンティティ管理の価値が組織に理解されるようになったが、問題は「理想」を「行動」に変えることである。

ゼロトラストは、一夜にして実現できるものではありません。また、複雑な取り組み、優先度の変更、ニーズの拡大は、いずれも時間とリソースを必要とするものとなります。このため、組織に明確な枠組みがなければ、脆弱性を理解し、進捗状況を評価する上で苦労することになりかねません。Okta のワークフォースアイデンティティ成熟モデルは、企業がゼロトラスト実現の道のりにおけるアイデンティティの側面を状況に当てはめて捉え、進捗を評価するために役立ちます。段階的に成熟度を高めていくための取り組みは、時間がかかるものとなります。しかし、アイデンティティ中心のセキュリティを活用し始めることで、組織は保護を強化し、攻撃対象領域を縮小させ、悪意ある攻撃への対応を迅速化させ、IT コストと管理負担を軽減し、安全性、効率性、俊敏性を向上できるようになります。ここでは、成熟の 4 ステージの概要を簡単に紹介します。

ワークフォースアイデンティティの成熟

4 つのステージ

ステージ 1：基本
集約と簡素化

- 手作業による管理の削減
- リスク領域の縮小
- ディレクトリの集約

ステージ 2：拡張
セキュリティコントロールの階層化

- オンボーディング / オフボーディングの自動化
- IT の生産性の向上
- 管理負担の軽減

ステージ 3：先進的
エクスペリエンスの自動化と向上

- すべてのアイデンティティシステムの接続
- すべての管理プロセスの自動化
- レガシーテクノロジーの廃止

ステージ4：戦略的
アイデンティティの最適化と拡張

- アクセスエクスペリエンスの近代化
- パスワードのリスクの排除
- デジタル成熟度のさらなる向上

ステージ 1：基本

集約と簡素化

ステージ 1 では一般的に、手作業による管理の削減とアイデンティティベースの攻撃に対する防御の強化が目標となります。この段階の組織は、防御を固めながら、ユーザーやアプリを手作業で管理することから脱却しようとします。取り組みがバラバラで場当たり的であるために四苦八苦し、意図せずリスク領域を拡大させ、ディレクトリを増大させるといった状況が少なからず起きます。

ステージ 1 で検討すべき価値の高いアイデンティティの取り組みとしては、アイデンティティシステムの集約、ロールベースのアクセスポリシーを使用した基本的な SSO や MFA の導入、高可用性アーキテクチャの構築、SLA 標準の追加、オンプレミス / クラウドアプリの包括的なインベントリ作成などが挙げられます。

ステージ 2：拡張

セキュリティコントロールの階層化

ステージ 2 では一般的に、IT の生産性の向上と管理に要する時間とコストの削減に取り組みます。この段階の組織は、パスワードへの依存が過度に高く、ユーザーのオンボーディング / オフボーディングのような手作業のプロセスに投資している可能性があります。目標は、生産性の向上、IT 管理者の負担軽減、セキュリティ態勢の強化、アプリケーションへのユーザーアクセスの簡素化などになります。

ステージ 2 で検討すべきプロジェクトには、アプリケーション、請負業者、ビジネスパートナーにまたがる MFA の拡張、クラウドとオンプレムのアプリケーションにまたがるセキュリティとアクセス制御の集約、ロールベースのアクセス制御と動的アクセスポリシーの導入、セキュリティとコンプライアンス向け監査 / 監視ツールの導入などが挙げられます。

ステージ 3：先進的

エクスペリエンスの自動化と向上

ステージ 3 では、残された手作業のプロセスを自動化し、すべてのアイデンティティシステムを単一の統合管理ソリューションの下に接続します。これにより、レガシーテクノロジーを集約 / 廃止するとともに、ダイナミックな働き方の効率化を実現し、すべてのシステムの接続とコミュニケーションを確保できます。

この段階で検討すべきアイデンティティプロジェクトには、属性ベース / ポリシーベースのアクセス制御の導入、API / 重要インフラストラクチャ / アプリケーションへの最小特権アクセスの適用などが含まれます。さらに、定期的なユーザーアクセス再認証の採用や、重要インフラストラクチャへの安全なパスワードレスアクセスの導入も検討すべきです。

ステージ 4：戦略的

アイデンティティの最適化と拡張

この段階の組織は、相互接続されたアイデンティティベースのシステムによって保護され、セキュリティと効率性を大規模に実現できます。最新のアクセスエクスペリエンスの実現やパスワード関連のリスクの排除など、次のレベルの目標に向け、安心できる態勢で注力できます。

ステージ 4 では、パスワードレス認証の全面的な導入、インシデントの予防 / 検知 / 対応プロセスの完全な自動化、リスクベース / ジャストインタイムのアクセスの導入、ゼロスタンディング特権の維持の徹底を目指します。

ワークフォースアイデンティティの成熟

ゼロトラストの取り組みを実行に移す

「決して信用せず、常に検証する」というゼロトラストの原則は、未来志向の組織がアイデンティティの取り組みを採用し、優先させるのに伴って、空論的な戦略から日常的なビジネスの現実へとまたたく間に変化しました。こうした組織は、MFA や SSO を従業員や外部ユーザーだけでなく、アプリや API、ネットワークインフラストラクチャのその他の重要要素へと拡張することを手始めとして、新しいセキュリティ基盤を構築しています。どの地域でも、ますます複雑化するアイデンティティベースのゼロトラストプロジェクトに取り組む組織が増えており、目覚ましい進展を遂げています。

従業員、請負業者、パートナー、ベンダーを含め、複雑化するワークフォースが常に確実なアクセスを必要しているために、世界中の組織は、アイデンティティに裏打ちされた強固なゼロトラストのセキュリティ態勢を確立すべく大きく前進しています。たとえば、多くの企業が優先的な取り組みとして、従業員向けの MFA（今年の調査でセキュリティ対策を実施していると回答した組織の 33%）とともに、外部ユーザー向けの MFA（同 34%）を挙げています。

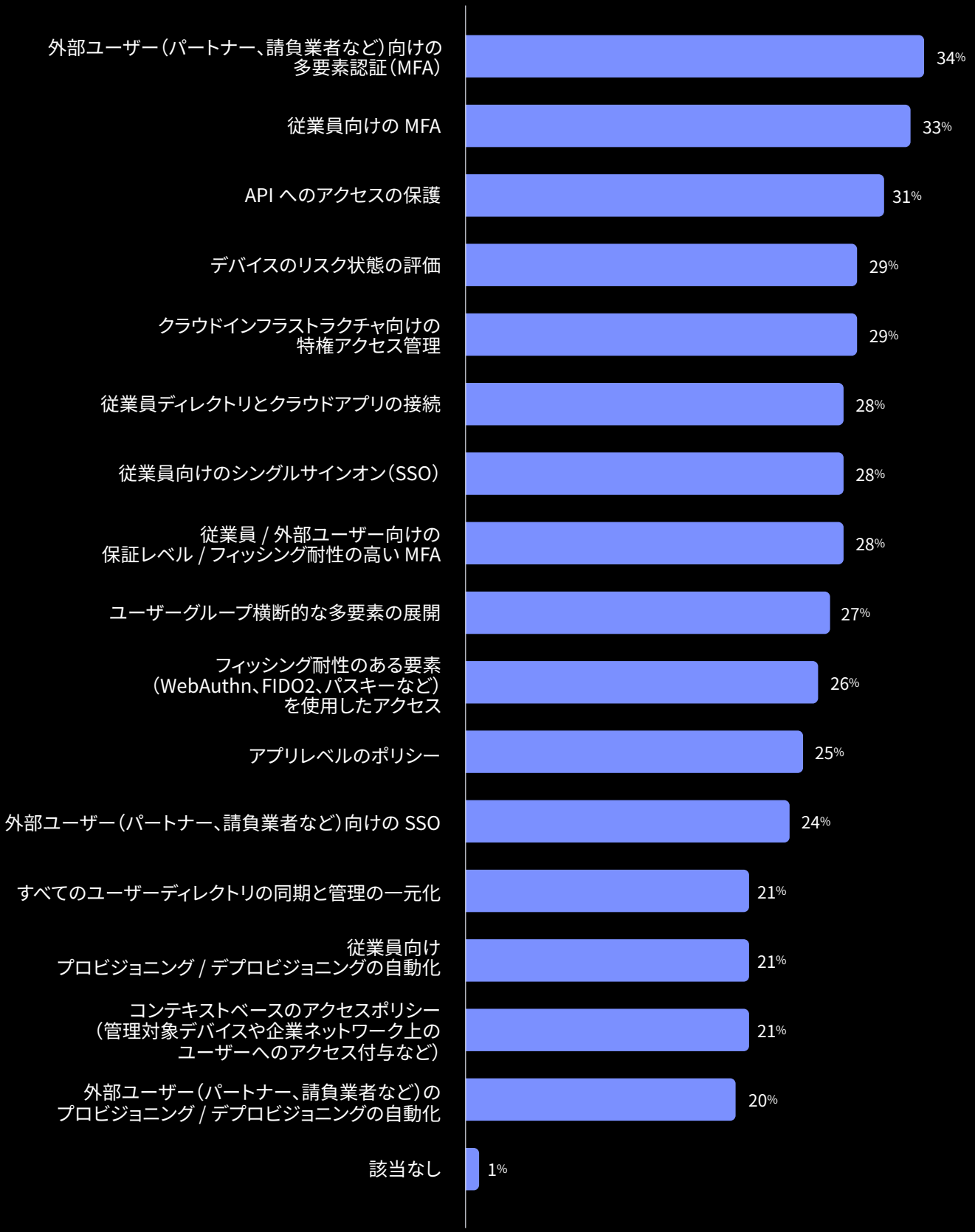
業種別に見ると、調査対象の組織が今年すでに実施している主要なセキュリティ対策は以下のとおりです。

- **医療：**外部ユーザー向けの MFA、従業員向けの MFA、ディレクトリのクラウドアプリへの接続
- **公共部門：**外部ユーザー向けの MFA、API へのアクセスの保護、従業員向けの MFA
- **金融サービス：**従業員向けの MFA、外部ユーザー向けの MFA、クラウドインフラストラクチャ向けの特権アクセス管理
- **ソフトウェア：**従業員向けの MFA、API へのアクセスの保護、外部ユーザー向けの MFA

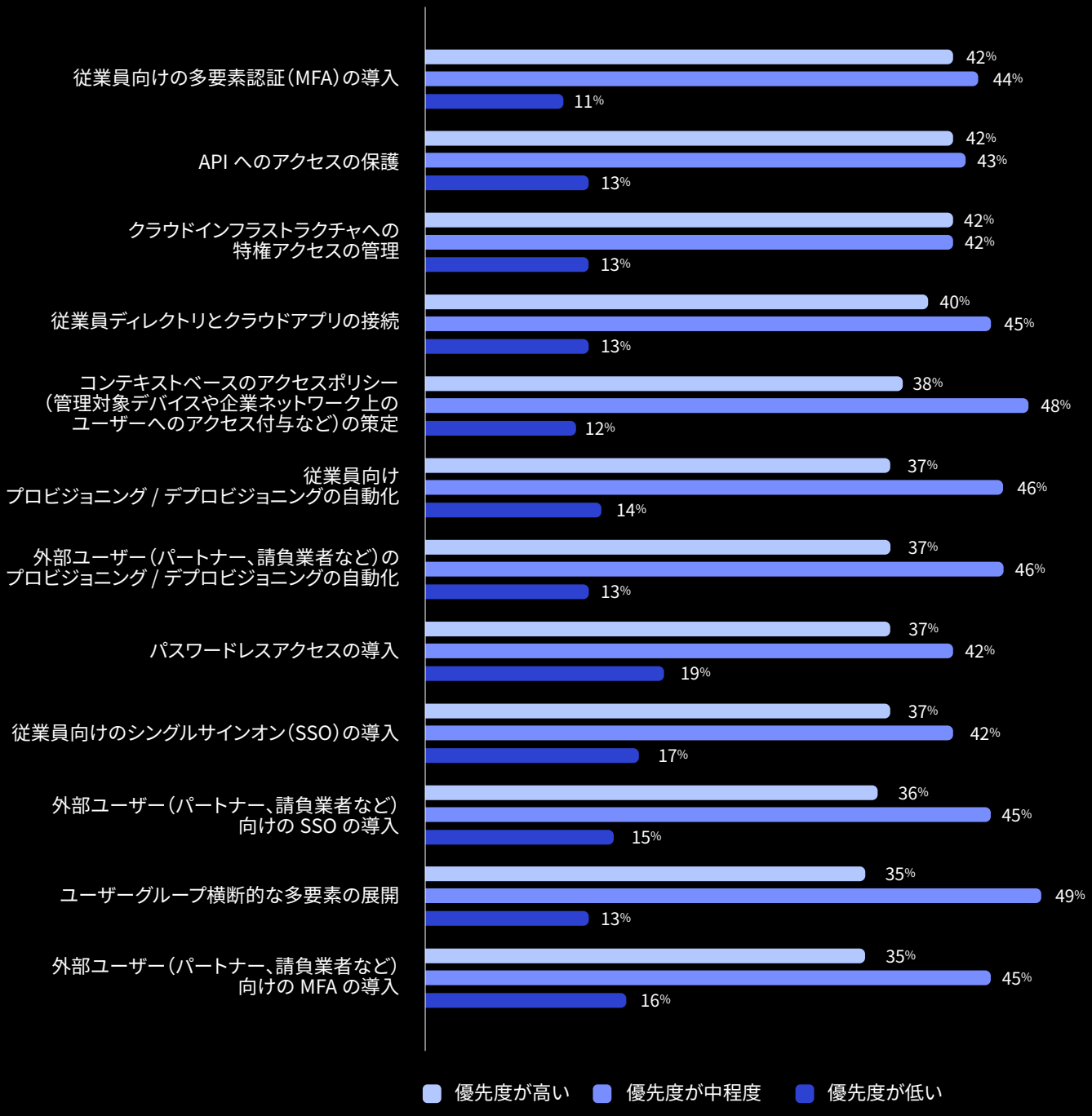
調査対象の企業が現在計画中のセキュリティ対策としては、今年は回答がかなり均等に分布していることがデータに表れており、上位 3 つはクラウドへの特権アクセスの管理、API へのアクセスの保護、従業員向けの MFA の導入が占めました。

2021 年と 2022 年には 2 年連続で、従業員向けの MFA と SSO が実施済みのセキュリティ対策として最も多く挙げられ、従業員ディレクトリのクラウドアプリへの接続が僅差で 3 位となりました。12 ～ 18 か月以内の優先課題としては、2021 年には外部ユーザー向け SSO、2022 年にはクラウドインフラストラクチャへの特権アクセスの管理が最も多く挙げられました。

次のセキュリティ対策のうち、あなたの組織がすでに実施している取り組みはどれですか？
全回答者



次のセキュリティ対策について、あなたの組織にとっての今後 12 ～ 18 か月の優先度をランク付けしてください。
全回答者



注：データラベルを四捨五入して整数にするため、棒グラフの合計が 100% にならないことがあります。

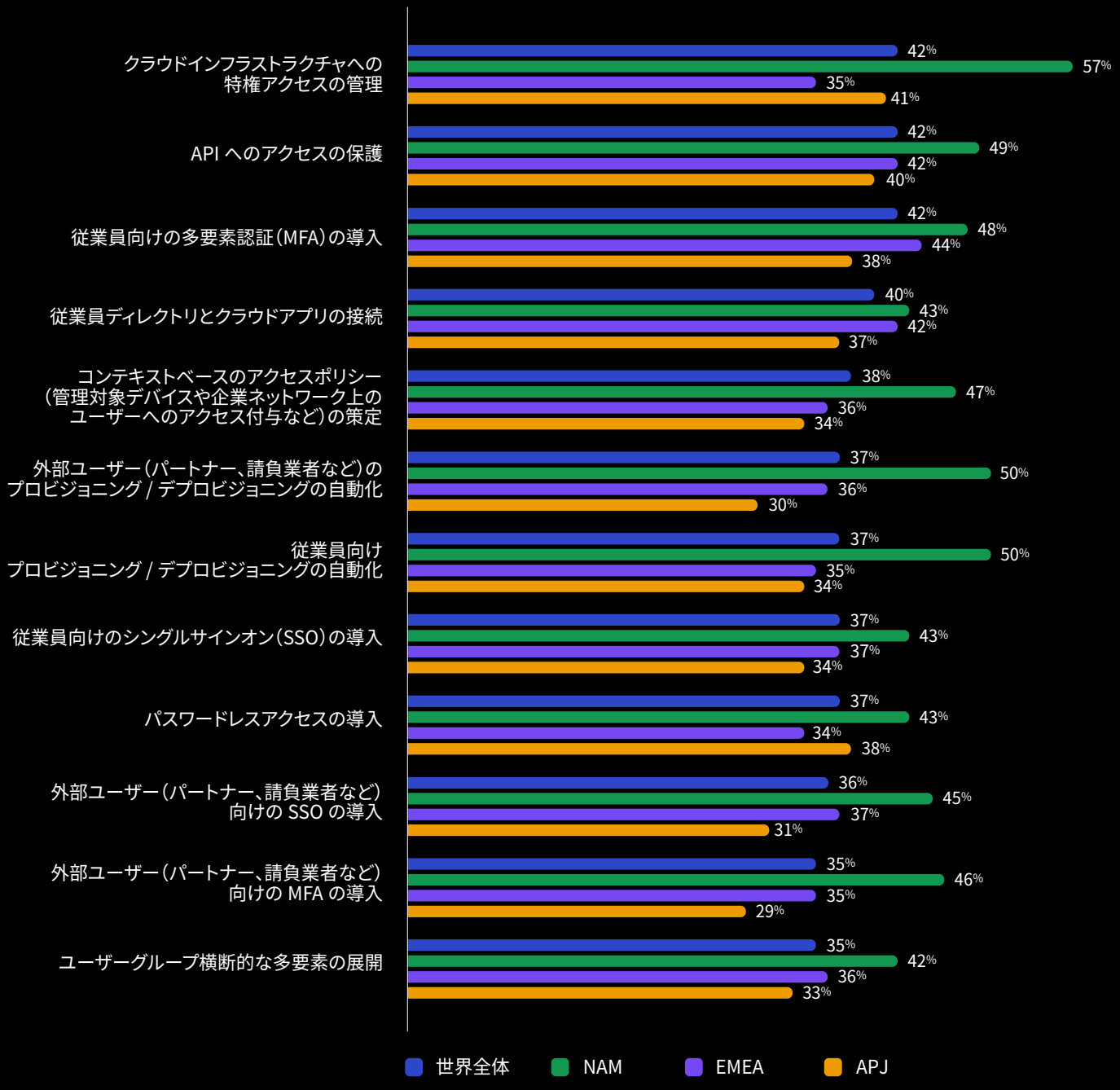
ワークフォースアイデンティティの成熟

実施の計画

2021	1 位　外部ユーザー向けのシングルサインオン（57%）
	2 位　コンテキストベースのアクセスポリシー（43%）
	3 位　外部ユーザー（パートナー、請負業者など）向けの多要素認証（MFA の導入（42%）
2022	1 位　クラウドインフラストラクチャへの特権アクセスの管理（45%）
	2 位　API へのアクセスの保護（41%）
	3 位　従業員のプロビジョニング / デプロビジョニングの自動化（38%）
2023	1 位　クラウドインフラストラクチャへの特権アクセスの管理（42%）
	2 位　API へのアクセスの保護（42%）
	3 位　従業員向けの多要素認証（MFA）の導入（42%）

Okta は毎年、今後 1 年～ 1 年半以内に実施する予定のゼロトラストソリューションについて尋ねています。世界全体での上位 3 つの回答を年ごとに見ていくと、興味深いトレンドの変化がわかります。2021 年に企業が最も関心を寄せていたのは、外部ユーザー向けの SSO と MFA とアクセスポリシーの強化でした。多くの組織でこれらの取り組みが軌道に乗るにつれて、クラウドへの特権アクセスと API へのアクセスの保護、そして従業員のプロビジョニング / デプロビジョニングの自動化（昨年）、従業員向けの MFA の導入（今年）へと焦点が移ってきました。

次のセキュリティ対策のうち、あなたの組織が今後 12 ～ 18 か月以内に優先的に取り組むセキュリティ対策はどれですか？
（グラフは「優先度の高い」回答のみを掲載）
地域別の比較



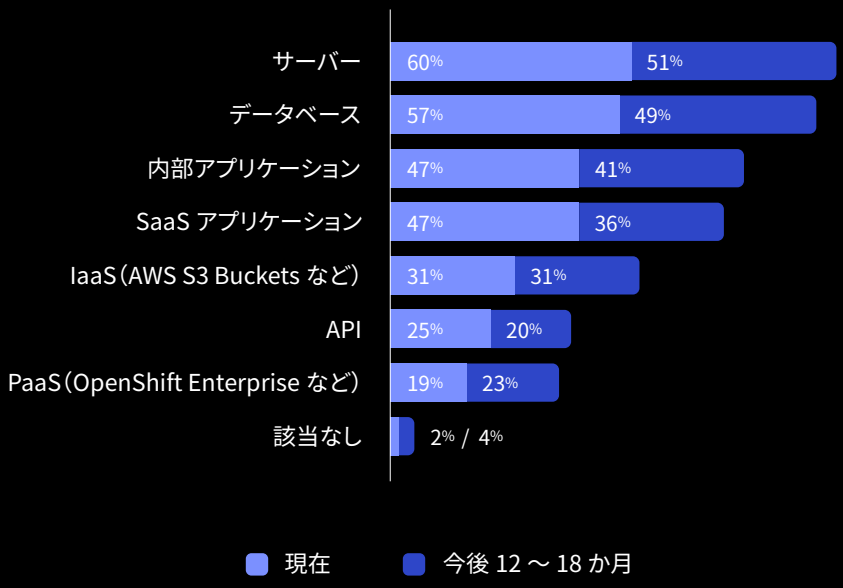
北米企業はセキュリティ対策を重視

今年のデータを掘り下げると、地域差が見えてきます。すべてのタイプのセキュリティ対策について、北米の組織は優先的に取り組む傾向があり、具体的な計画としてはクラウドへの特権アクセスの管理とプロビジョニング / デプロビジョニングの自動化が上位に挙げられました。EMEA では、従業員向けの MFA の導入、API へのアクセスの保護、従業員ディレクトリとクラウドアプリの接続が最優先の取り組みとして挙げられました。APJ 地域の企業は平均して、セキュリティに優先的に取り組むと回答する割合がやや低くなりましたが、全体として計画の対象が分散し、クラウドインフラストラクチャへの特権アクセスの管理と API へのアクセスの保護を筆頭に、従業員向けの MFA の導入、パスワードレスアクセスの導入、従業員ディレクトリとクラウドアプリの接続が挙げられました。

ワークフォースアイデンティティの成熟

認証の保護

次のうち、MFA / SSO をすでに導入したリソース、および今後 12 ～ 18 か月に導入する予定のリソースはどれですか?
全回答者



注：両方の回答を選択した回答者がいるため、棒グラフの合計が 100% を超えることがあります。

MFA / SSO により保護するリソースとしては、サーバーとデータベースが最も多く上げられました。

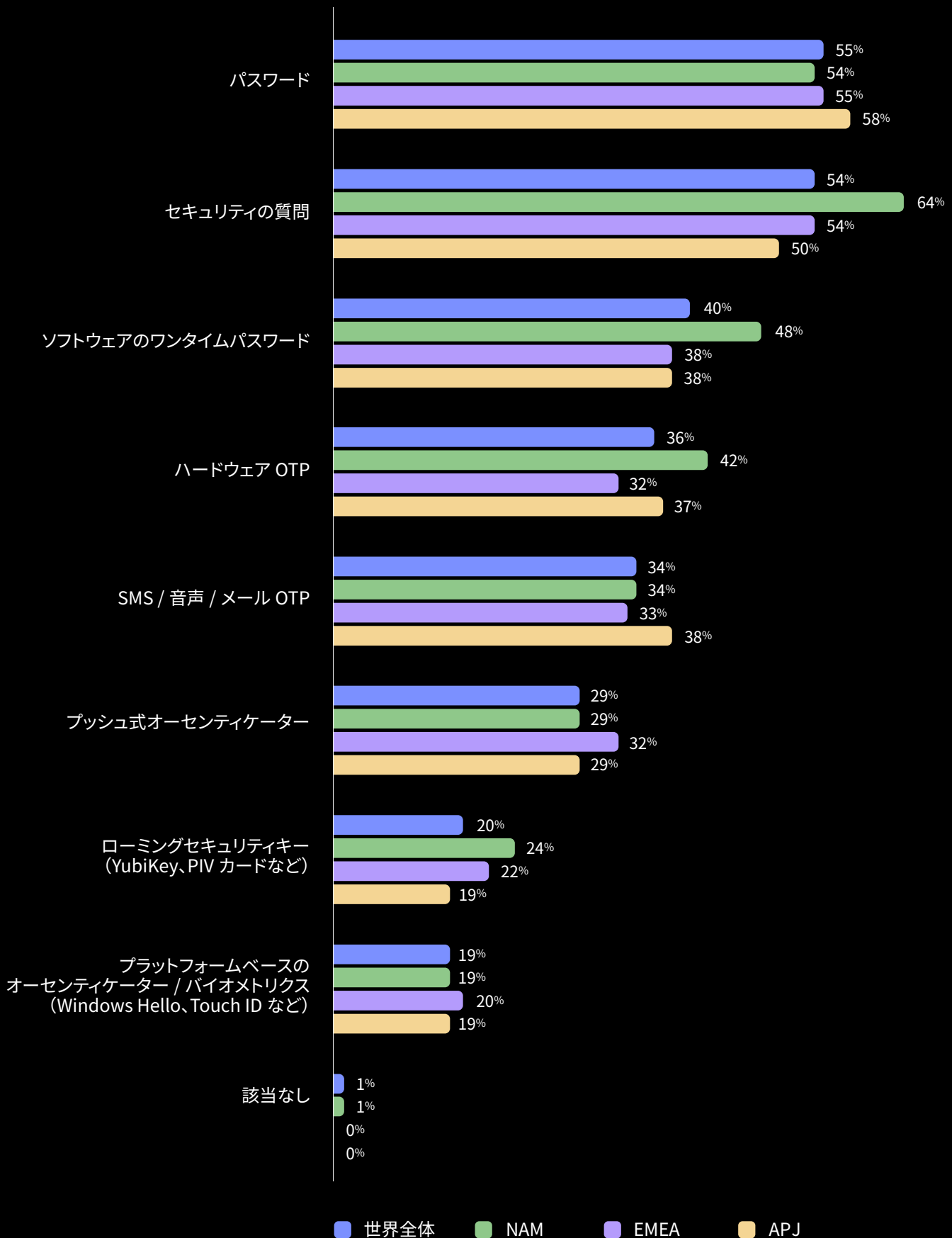
昨年の調査では、MFA と SSO を内部アプリケーションと SaaS（Software as a Service）アプリに拡張することに重点が置かれました。しかし今年は、中核的なネットワークコンポーネントに重点が移りました。回答者の 5 人中 3 人（60%）は、サーバーに MFA および / または SSO をすでに使用していると報告しています。また、データベースにもアイデンティティベースの新たな保護が適用されるようになり、57% がすでに MFA および / または SSO を拡張しています。また、各地域間に有意な差は見られず、北米、EMEA、APJ の各地域の企業は、すでに MFA / SSO を導入しているリソースと、今後導入予定のリソースの両方で、サーバー、データベース、アプリ（内部、SaaS）を上位に挙げました。

より強力なオーセンティケーターがパスワードとの差を縮める

パスワードは、保証レベルが低いにもかかわらず認証の標準としての位置づけを堅持しており、すべての地域で過半数の組織が使用しています。セキュリティの質問も、パスワードと同様に保証レベルの低い要素ですが、世界全体、そして EMEA と APJ で 2 番目に多く利用されています。また、北米ではトップの座を占めています。ハードウェア OTP や SMS / 音声 / メール OTP を含め、保証レベルの低い要素は、サイバー犯罪者によって比較的容易に侵害される可能性があります。それにもかかわらず、全体として多くの組織がこうした要素を現在も使用しています。

物理トークンの OTP やプッシュ認証のような保証レベルが中程度の要素を使用している組織は少なく（それぞれ 36% と 29%）、プラットフォームベースのオーセンティケーターやバイオメトリクスのような保証レベルの高い要素を使用している組織はわずか 19% です。Okta は、MFA が主流になっていく一方で、規制の強化を受けて、金融サービスや公共部門などの業界がパスワードレスのようなフィッシング耐性のある認証要素の採用へ向かうと予想しています。

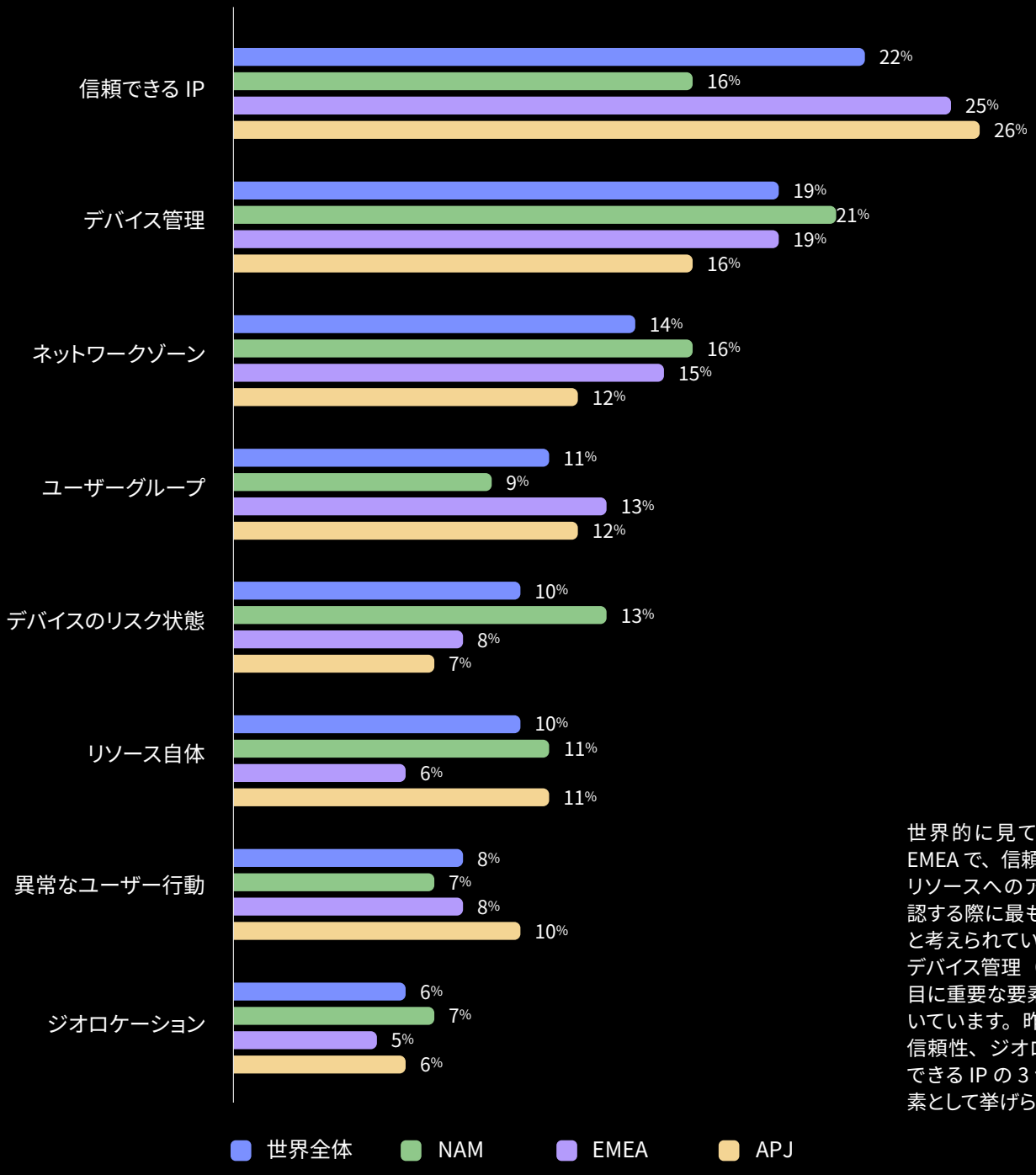
あなたの組織は、内部 / 外部ユーザーの検証にどの認証要素を使用していますか?
地域別の比較



ワークフォースアイデンティティの成熟

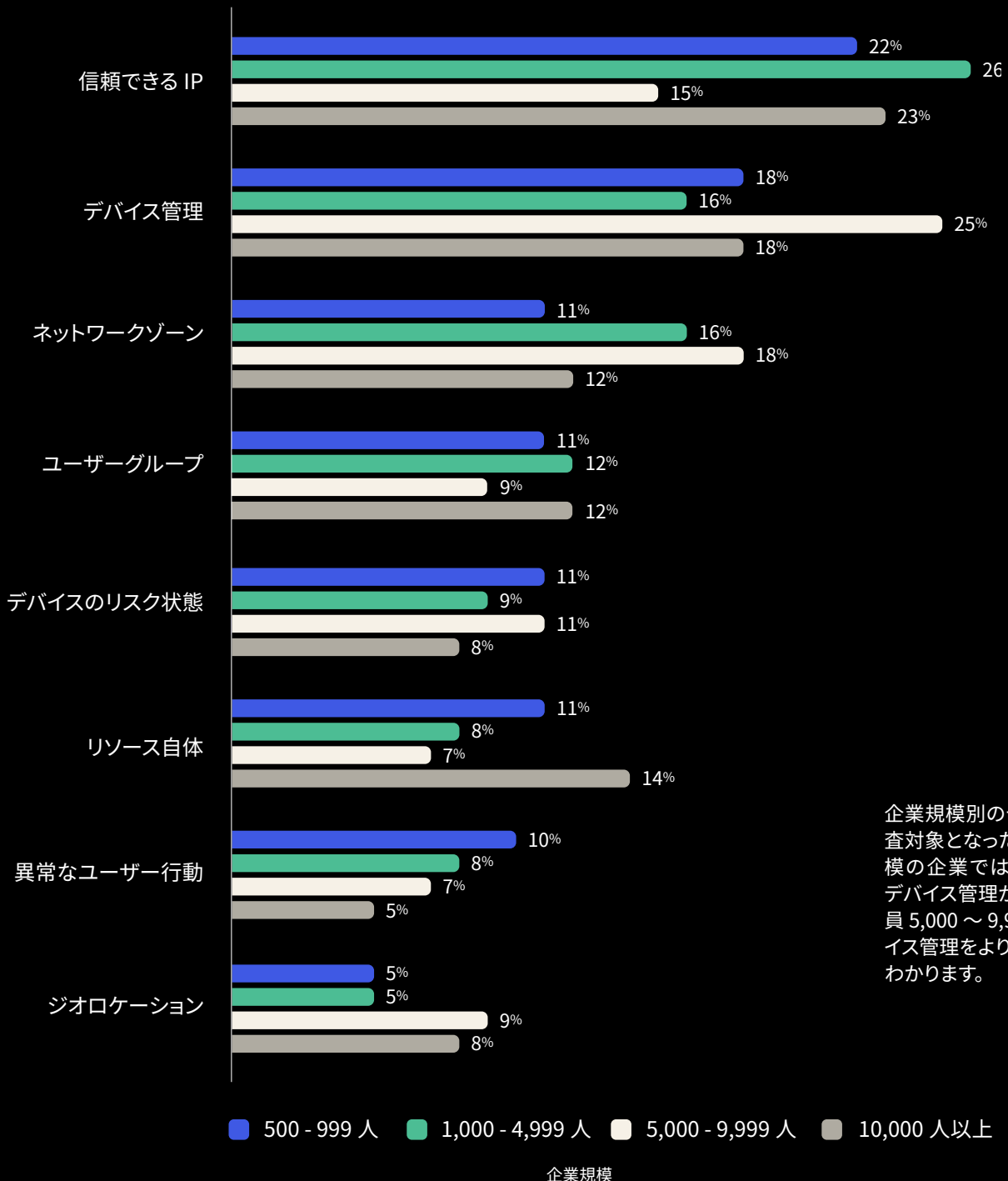
内部リソースへのアクセスの承認

内部リソースへのアクセスを制御 / 承認する際に最も重要な要素は何ですか?
地域別の比較



世界的に見て、また特に APJ と EMEA で、信頼できる IP は、内部リソースへのアクセスを制御 / 承認する際に最も重要な要素であると考えられています。北米でのみ、デバイス管理（世界全体では 2 番目に重要な要素）がこの要素を抜いています。昨年は、デバイスの信頼性、ジオロケーション、信頼できる IP の 3 つが最も重要な要素として挙げられました。

内部リソースへのアクセスを制御 / 承認する際に最も重要な要素は何ですか?
企業規模別



企業規模別のデータを見ると、調査対象となった最大規模と最小規模の企業では、信頼できる IP とデバイス管理が上位を占め、従業員 5,000 ～ 9,999 人の企業はデバイス管理をより重視していることがわかります。

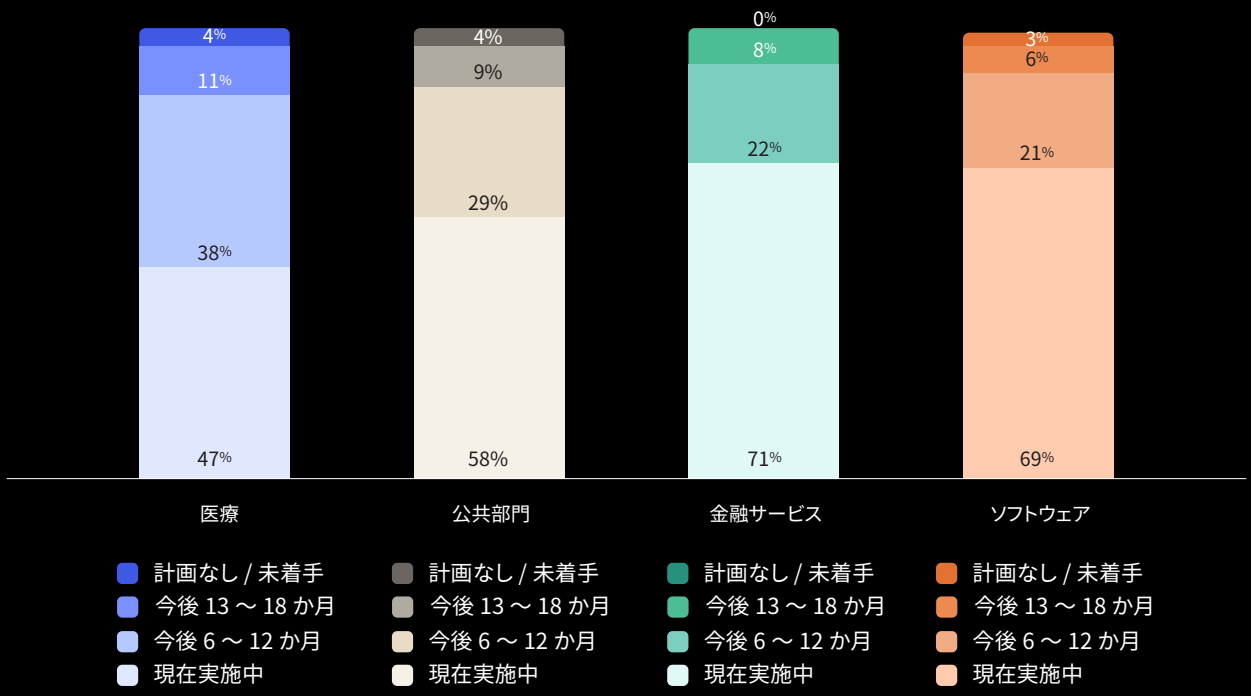
業種別のゼロトラスト進捗状況

主要業種の詳細な状況を掘り下げる

ゼロトラスト実現の道のりは、企業の優先課題やプラクティスと同様、業種によって大きく異なります。今年の調査でも、医療、公共部門、金融サービス、ソフトウェアの主要 4 業種のデータに焦点を当てました。ソフトウェア以外の 3 業種は規制が特に厳しく、エコシステムの安全性とコンプライアンスを維持するためにゼロトラストセキュリティの取り組みに投資する上での動機付けとなっています。全体として、4 つの業界はいずれも昨年よりも前進しているように見えますが、真のゼロトラストセキュリティの活用に向けた道筋は依然として明確になっていません。

あなた組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後 12 ～ 18 か月以内に開始する予定ですか？

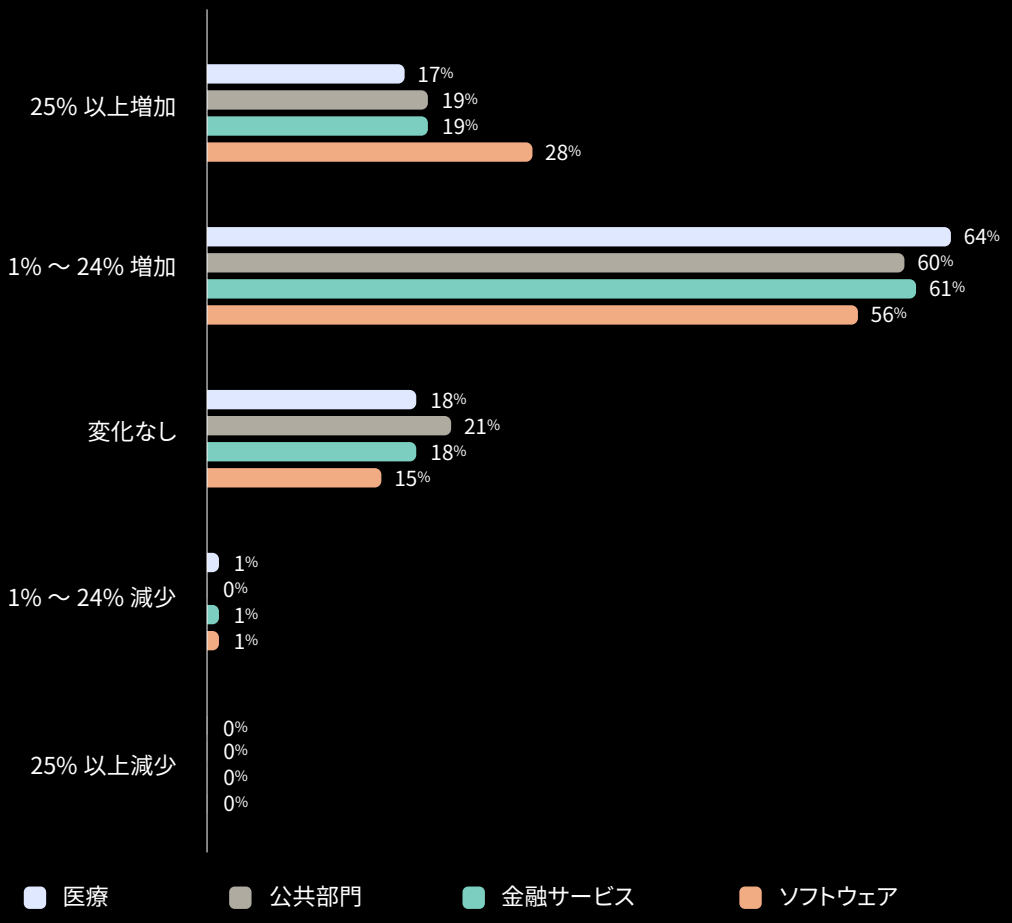
業種別の比較



金融サービスとソフトウェアがゼロトラスト導入で全業種を牽引

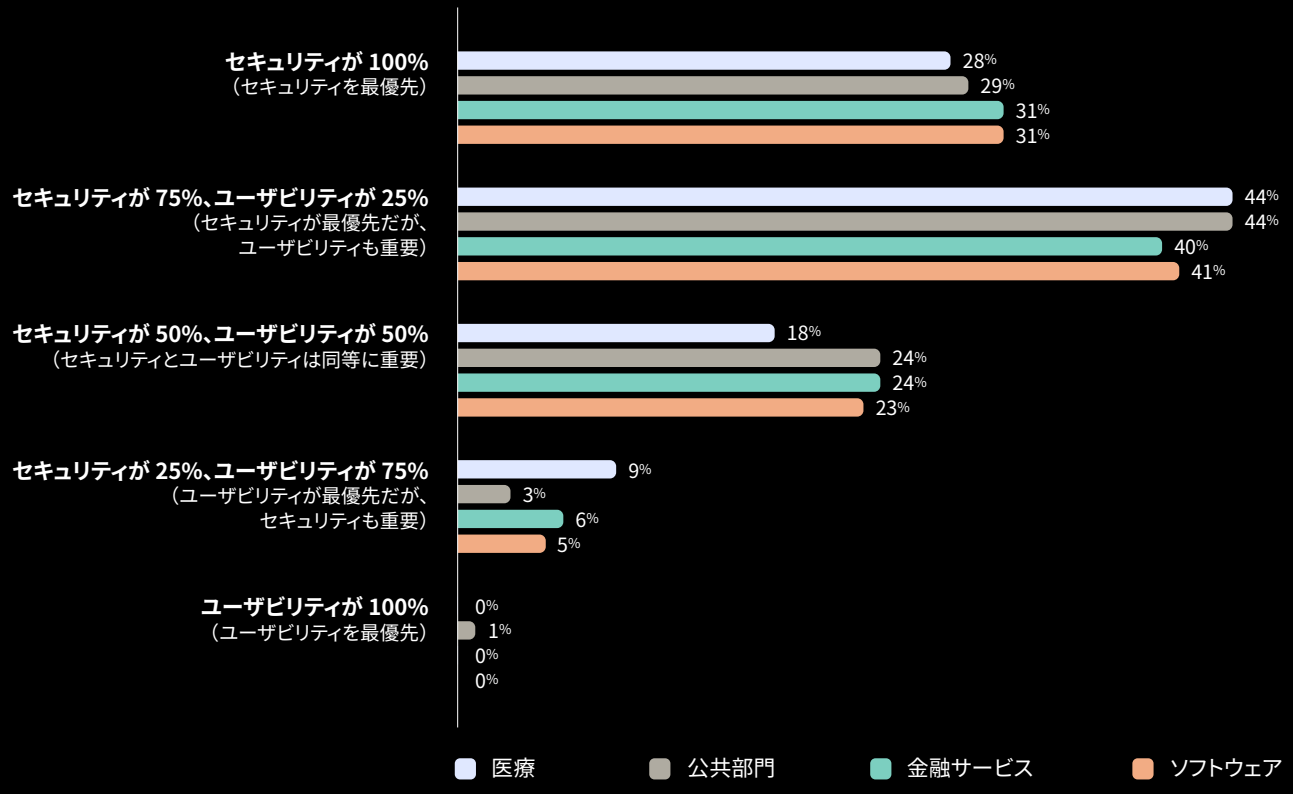
今年の調査では、ゼロトラストの実現へ向けて、どの業種でも明確な取り組みが進められていることが明らかになりました。Okta が注視する 4 業種のいずれにおいても、「ゼロトラストの取り組みを実施しておらず、今後 18 か月以内に実施する予定もない」と答えた回答者は 4% 以下でした。金融サービス業界とソフトウェア業界の企業は、現在取り組みを実施している割合が高く（それぞれ 71% と 68%）、医療業界と公共部門は取り組みが少し遅れています。この点については後述します。

あなたの組織では、過去 12 か月で、ゼロトラスト戦略の導入に関するセキュリティの取り組みの予算はどのように変化しましたか（該当する場合）？
業種別の比較



マクロ経済的な圧力により、その他の領域ではコスト削減を余儀なくされる状況にもかかわらず、Okta が注視する 4 業種すべてで、組織は引き続きゼロトラストセキュリティの取り組みに投資しています。調査対象の 4 業種すべてで、約 8 割の組織が過去 1 年間にセキュリティ対策予算が増やしました。その一方で、セキュリティ対策予算を減らした組織は、どの業種にもほとんど存在しません。

あなたの組織では、セキュリティの重要性とユーザビリティの重要性のバランスをどのように取っていますか？
業種別の比較



このグラフからは、セキュリティに軸足が移っていることを明確に見てとることができます。Identity Theft Resource Center の 2022 Data Breach Report によると、現在は 1 日あたり 5 回近くのデータ侵害が発生しており、こうした状況下でユーザビリティはセキュリティよりも後回しにされるようになっています。主要 4 業種すべてで、セキュリティに 75%、ユーザビリティに 25% の重点を置いている組織が最も多くなっています。続いて多いのが、セキュリティが紛れもなく最優先であると考える組織です。従業員や請負業者の摩擦を最小限に抑えることが重要である点は変わりありません。しかし、規制の厳しい業界では、適切とは言えないユーザーエクスペリエンスを提供するリスクは、セキュリティやコンプライアンス違反のリスクを上回るものではありません。

業種別のゼロトラスト進捗状況

医療

医療業界は、時として腰が重いこともありますが、今回調査対象となった回答者の組織については、ゼロトラストの計画と実行で持続的な前進が見られます。医療業界の回答者の大半は、ゼロトラストの取り組みを実施しているか、近い将来に実施する予定です。この業界では依然として、多くの組織が高リスクで保証レベルの低い認証要素からの脱却に苦戦を強いられています。しかし、こうした組織は概ね、アイデンティティの重要性を認識し、内部ユーザー / 外部ユーザー、そしてデータベースなどのリソース向けにMFAやSSOの導入を推進しています。

ゼロトラストの定義づけ / 計画段階にある組織が 100% に近づく

この 3 年間で、ゼロトラストの取り組みに対する医療業界の関心には盛衰が見られましたが、大きな変化ではありませんでした。今年調査した医療機関については、4% を除くすべての組織がゼロトラストの取り組みを現在実施しているか、今後 18 か月以内に実施を予定しています。そして、取り組みを実施している、あるいは近い将来に予定している医療機関の割合が、年々 100% に近づいています（The Wall Street Journal によると、2022 年の IT 支出が減少したためか、今年は昨年よりも取り組みをすでに実施していると報告する組織が減りましたが、この流れは今後変わる可能性があります）。全体として、より多くの医療機関がゼロトラストの取り組みを実行に移し、すでに実施済みの医療機関は取り組みをさらに推し進めていくと予想されます。

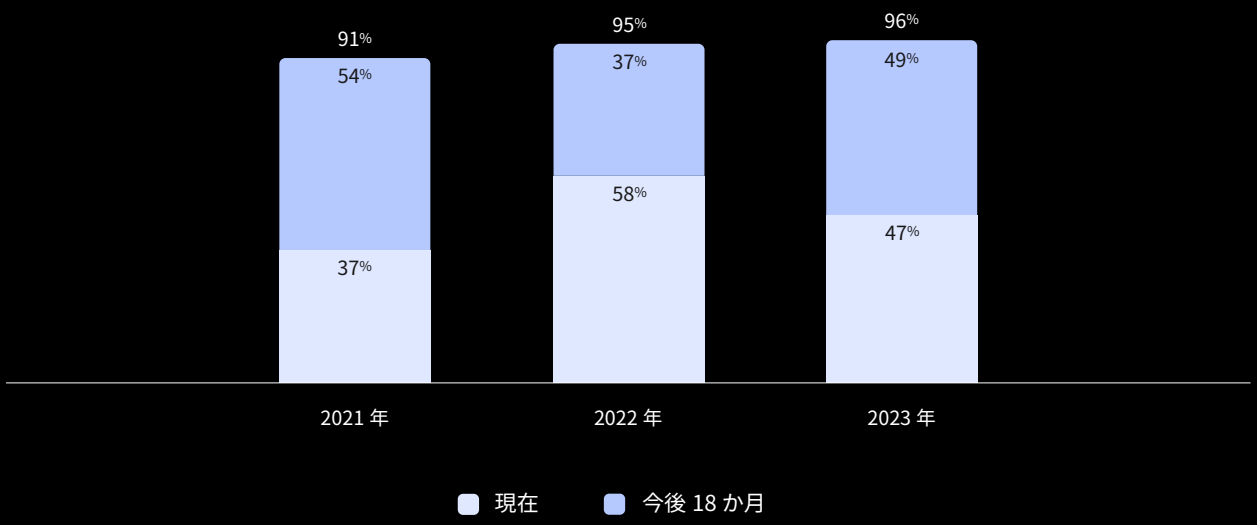
医療業界は平均よりやや遅れているが、追いつく計画がある

医療業界の取り組み状況を世界全体と比較すると、現在ゼロトラストの取り組みを実施している医療機関は世界平均に比べて少ないことがわかります。しかし、これらの組織はゼロトラストの潮流に追い付こうと一層努力しており、今後 6 〜 12 か月の計画に関しては世界平均を大きく上回っています。この期間内の実施を計画している割合は、世界平均がわずか 28% であるのに対して、医療業界では 38% です。

ゼロトラストセキュリティ戦略におけるアイデンティティの重要性については、医療業界の回答者の 9 割以上が、アイデンティティが「非常に重要」または「ある程度重要」であると回答しました。医療業界では、機密性が非常に高い個人識別情報（PII）を保護することが不可欠（規制当局もこの点を重視しています）であることから、この調査結果は特に驚くことではないでしょう。

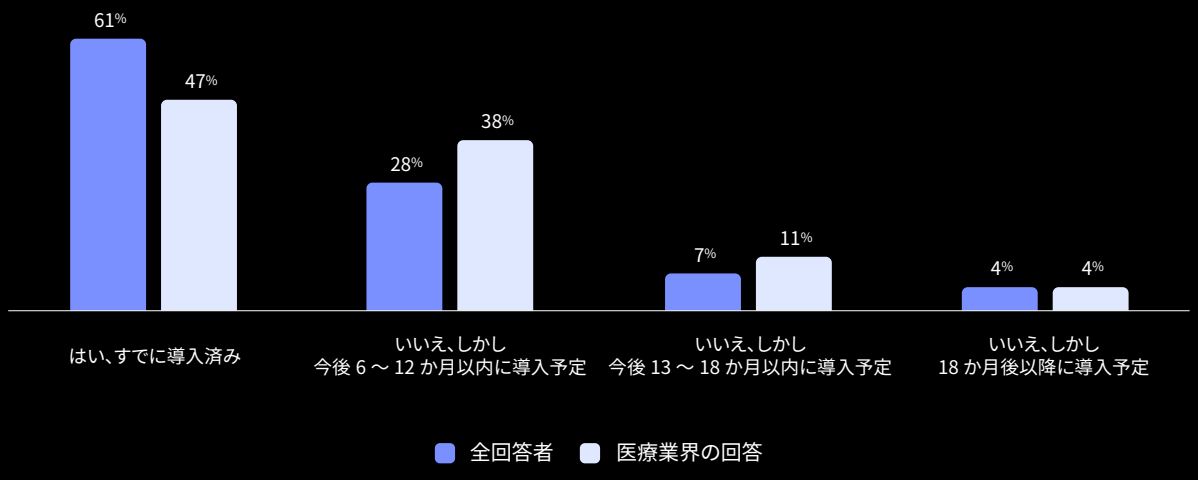
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後 18 か月以内に開始する予定ですか？

医療（前年比）



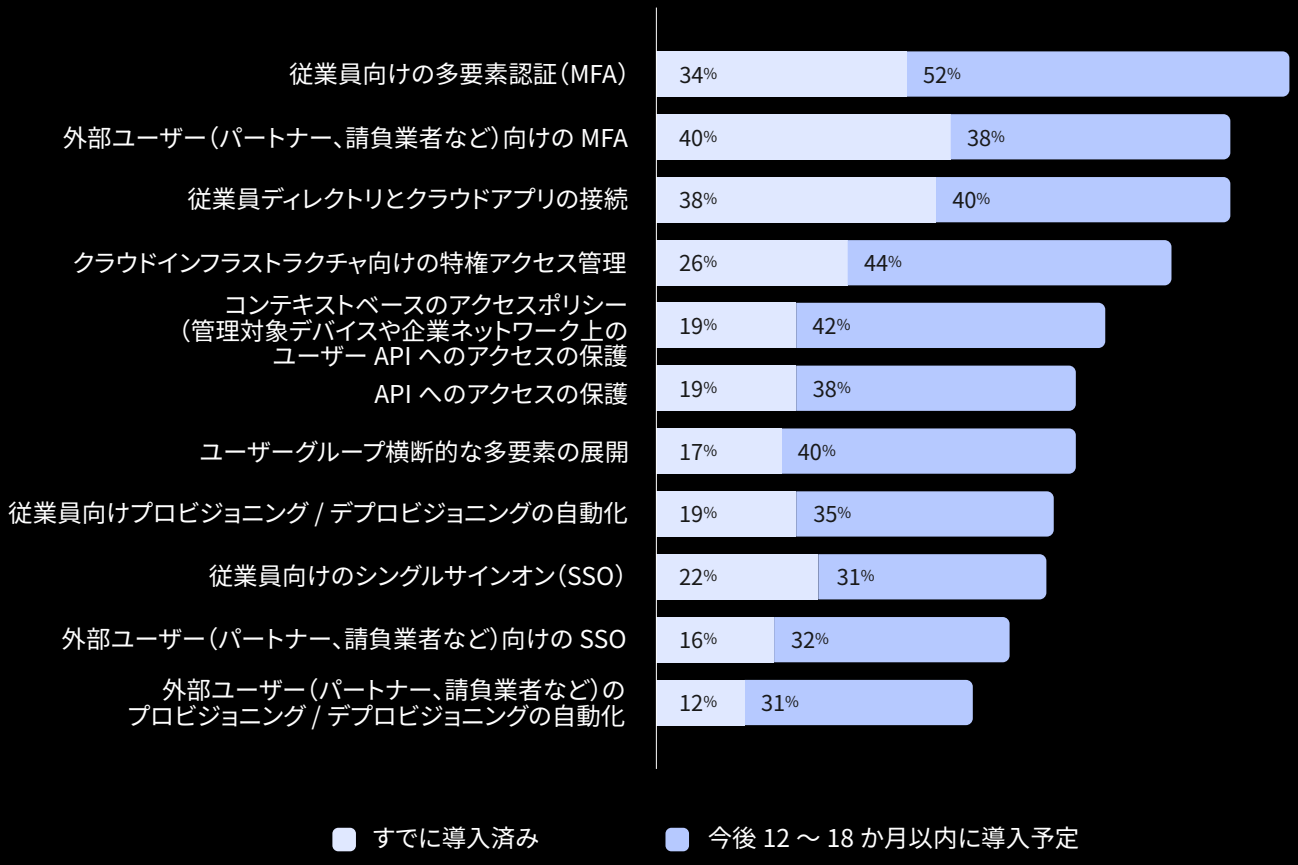
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後数か月で開始する予定ですか？

医療業界と世界平均の比較



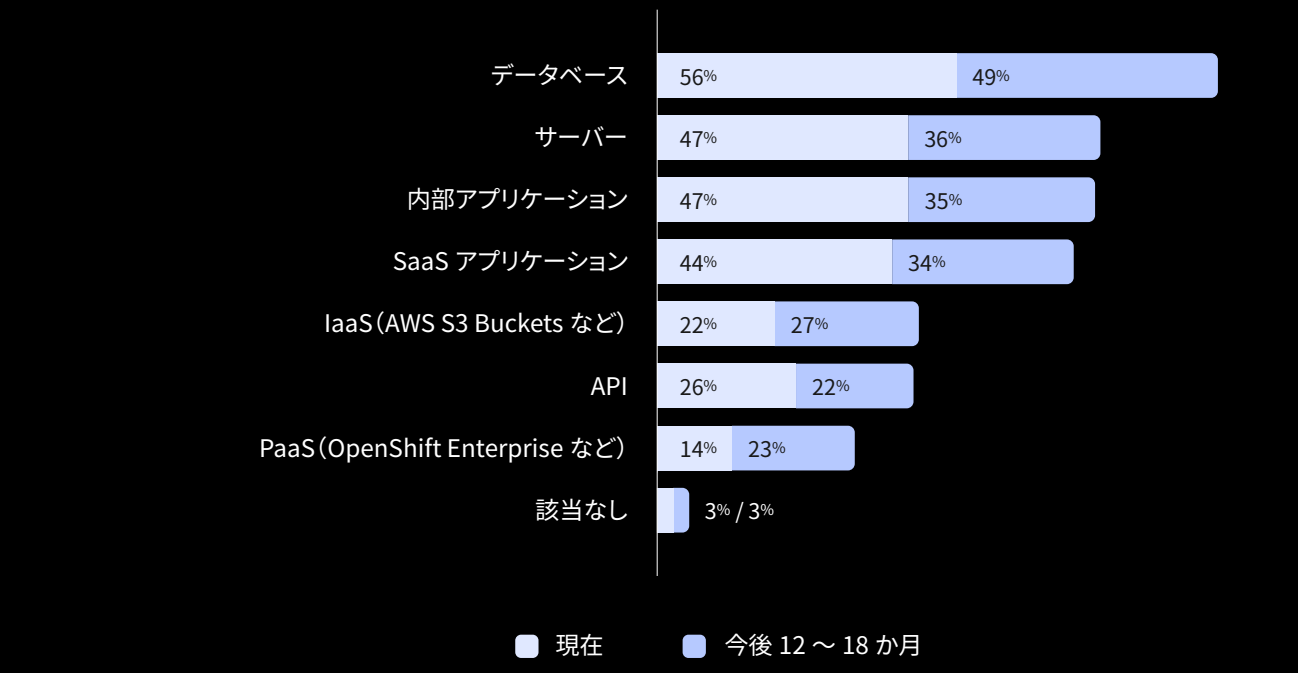
次のうち、あなたの組織がすでに実施している、または今後 12 ～ 18 か月以内に実施する予定の取り組みはどれですか?

医療



次のうち、SSO や MFA を導入済み、または今後 12 ～ 18 か月以内に導入する予定のリソースはどれですか?

医療



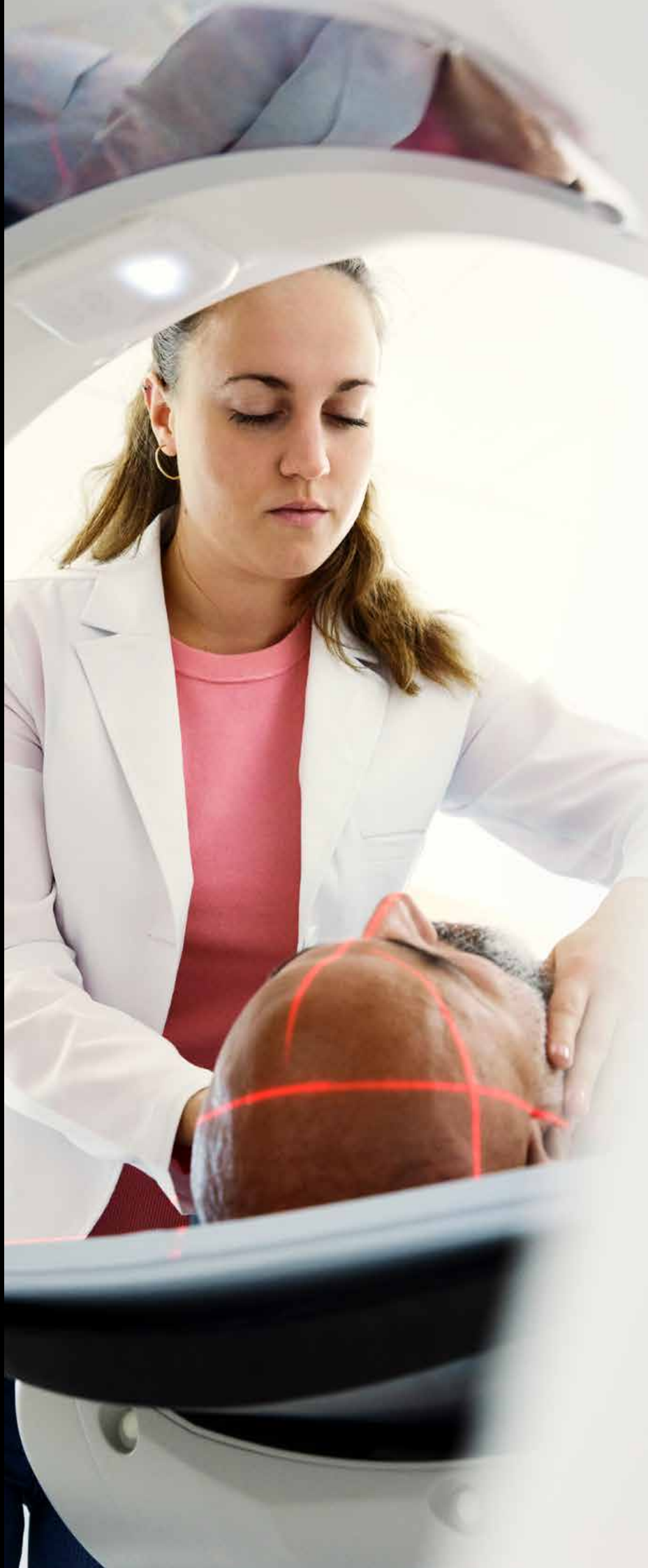
注：両方の回答を選択した回答者がいるため、棒グラフの合計が 100% を超えることがあります。

MFA とディレクトリ接続は医療業界の最重要課題

従業員向けの MFA と外部ユーザー向けの MFA は、常に多くの医療機関が取り組んでいる課題であり、その状況は今年も変わりません。これらに続いて、従業員ディレクトリとクラウドアプリの接続が、すでに実施しているセキュリティ対策の 3 位に入りました。従業員向けの MFA は、調査対象の医療機関のうち 3 分の 1 以上がすでに導入しており、さらに 52% が今後の導入を計画していることから、最も多い取り組みとなっています。SSO や自動プロビジョニングなどの取り組みは、今年の医療機関の計画では優先度が低くなりました。

SSO / MFA による保護対象として、データベース、サーバー、アプリが最多に

医療業界のデータベースは、機密度の高い患者の個人情報を含む可能性があり、サイバー犯罪者にとって価値の高い標的です。したがって、SSO および / または MFA による保護をデータベースへ拡張している医療機関の割合が最も高くなっています。しかし、この業界に属する組織の現在の採用状況や今後の計画という点では、サーバー / 内部アプリ / SaaS アプリへ SSO / MFA を拡張する取り組みもそれほど遅れていません。



信頼できる IP とデバイス管理がアクセス制御の最も重要な要素に

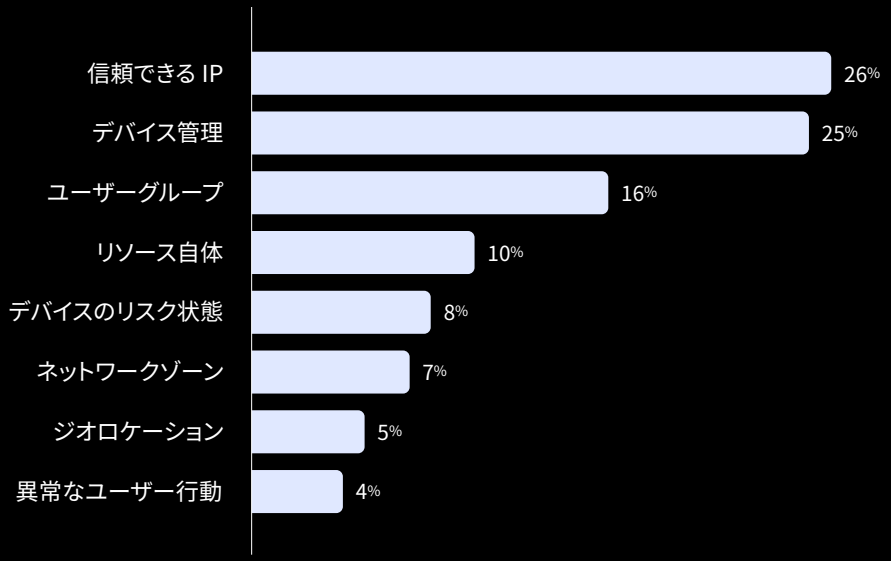
本調査に回答した医療機関の過半数が、内部リソースへのアクセスを制御 / 承認する際に、信頼できる IP かデバイス管理のいずれかを最も重要な要素と考えています。これは、世界全体の回答者が選んだ上位 2 つの要素と一致しています。続いて、ユーザーグループとリソース自体が、アクセスを制御 / 承認する要素の上位に入りました。

パスワードとセキュリティの質問が医療業界で最多の認証要素に

回答者の 61% がパスワードの使用を挙げており、医療機関にとってパスワードは依然として主要な認証要素です。このため、この業界でのパスワードレス導入はまだ遠い未来のものと考えられます。セキュリティの質問は、調査対象となった医療機関の過半数で使用されており、僅差で 2 位につけています。ハードウェア、ソフトウェア、SMS / 音声 / メールといった各種のワンタイムパスワード（OTP）は、ほぼ同率の 3 位となりました。また、プラットフォームベースのオーセンティケーターとバイオメトリクスは、この業界では最も導入率の低い認証要素となっています。

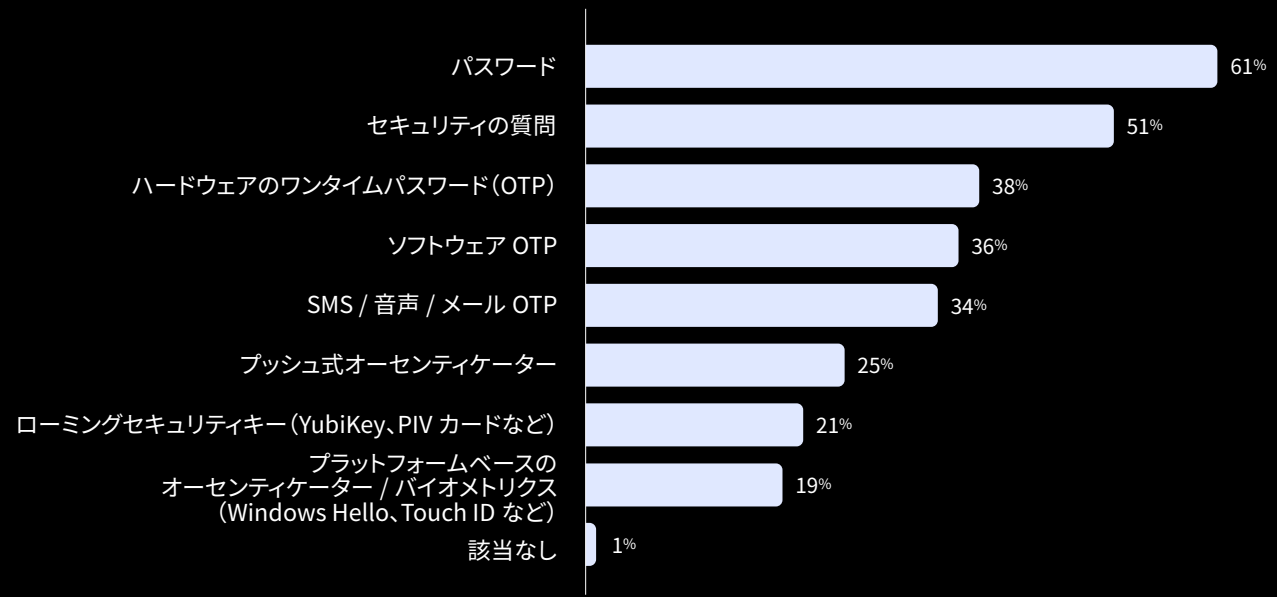
あなたの組織で内部リソースへのアクセスを制御 / 承認する際に、最も重要な要素はどれですか？

医療



あなたの組織は、内部 / 外部ユーザーの検証にどの認証要素を使用していますか？

医療



業種別のゼロトラスト進捗状況

公共部門

世界的に、公共部門ほどゼロトラストでセキュリティを強化する必要に迫られている業界はないでしょう。北米の例を挙げると、米国の連邦ゼロトラスト戦略では、高度化と持続化の度合いを高めている脅威に対する政府の防御を強化するために、すべての連邦政府機関が 2024 年 9 月までに特定のサイバーセキュリティ標準 / 目標を満たすことを明確に求められています。米国政府の指針としては、ほかにも国家サイバーセキュリティ戦略や国防総省のゼロトラスト戦略 / ロードマップなどがあります。

今年の調査では、北米、EMEA、APJ の公共部門も対象にしました（本レポートでは、州や地方の組織は公共部門に含めていません）。調査結果では、この業界では 58% の組織がすでにゼロトラストの取り組みを実施しており、さらに 38% が近い将来にゼロトラストの取り組みを開始する予定であることが明らかになりました。こうした組織は、最も重要なリソースを保護するために SSO や MFA を使用し、インフラストラクチャや資産を安全に保つために強固な境界を導入しています。

ほぼすべての公共組織がゼロトラストに取り組んでいる

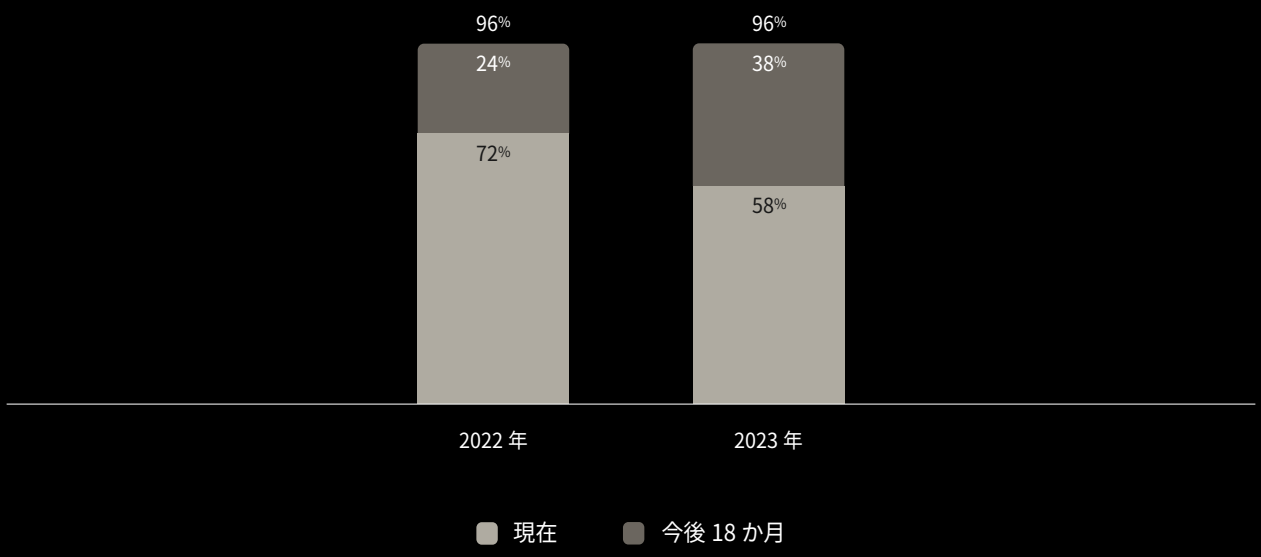
公共部門は、ゼロトラストの取り組みを着実に推進しています。2022 年から 2023 年にかけて、ゼロトラストの取り組みをすでに実施しているか、近く開始予定である公共組織の割合は、全体として 96% と変化していません。昨年は、公共組織の実に 72% がゼロトラストの取り組みを実施していました。しかし昨年の調査対象は、ほとんど（86%）が北米の公的部門の回答者でした。今年は調査範囲を拡大し、北米の組織の割合は 31% になりました。対象が拡大した今年の調査では、すでにゼロトラストの取り組みを実施していると報告した割合は 58% となり、さらに 38% が近い将来に取り組みを開始する明確な計画を持っています。

公共部門は取り組みの実施が遅れているが、計画では上回る

今回調査対象となった公共部門で、ゼロトラストセキュリティの取り組みをすでに実施している組織の割合は、世界平均とほぼ同じです。取り組みを実施している割合は、世界全体が 61% であるのに対して、公共部門は 58% です。しかし、公共部門では、（多くの場合に政府の指令により）3 分の 1 近くの組織が今後 6 ～ 12 か月以内に取り組みを開始する予定であり、世界平均をわずかに上回っています。

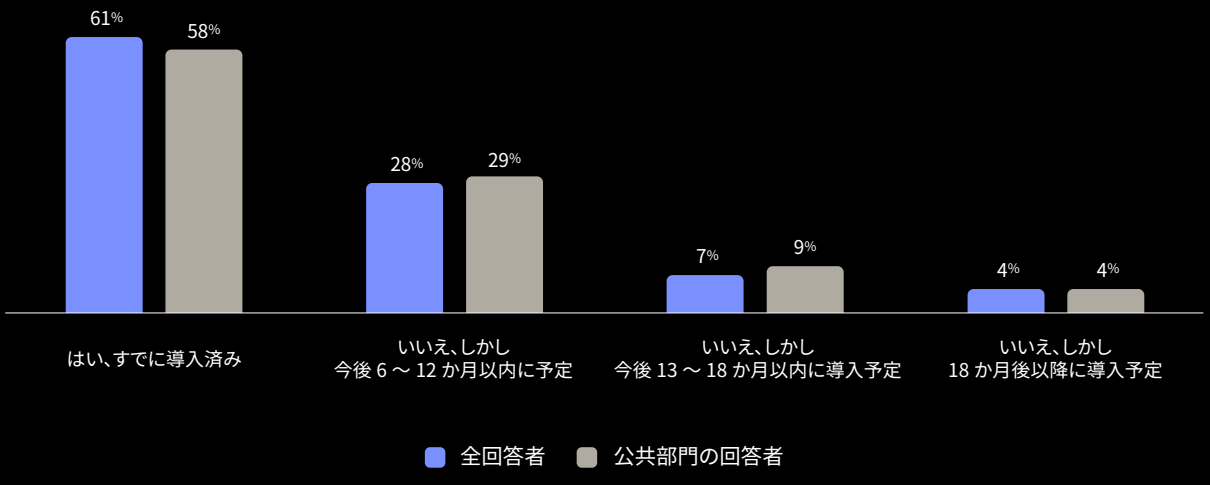
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後 18 か月以内に開始する予定ですか？

公共部門（前年比）



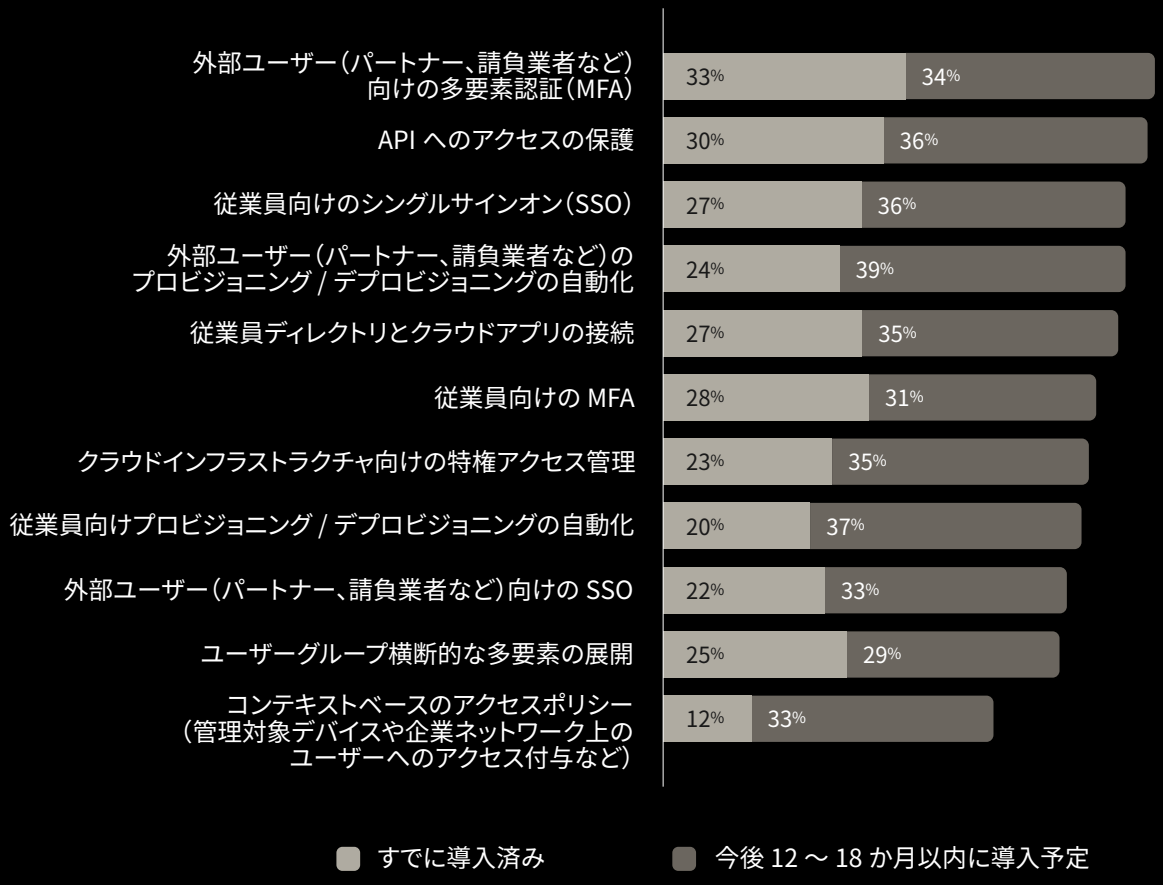
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後数か月で開始する予定ですか？

公共部門と世界平均の比較



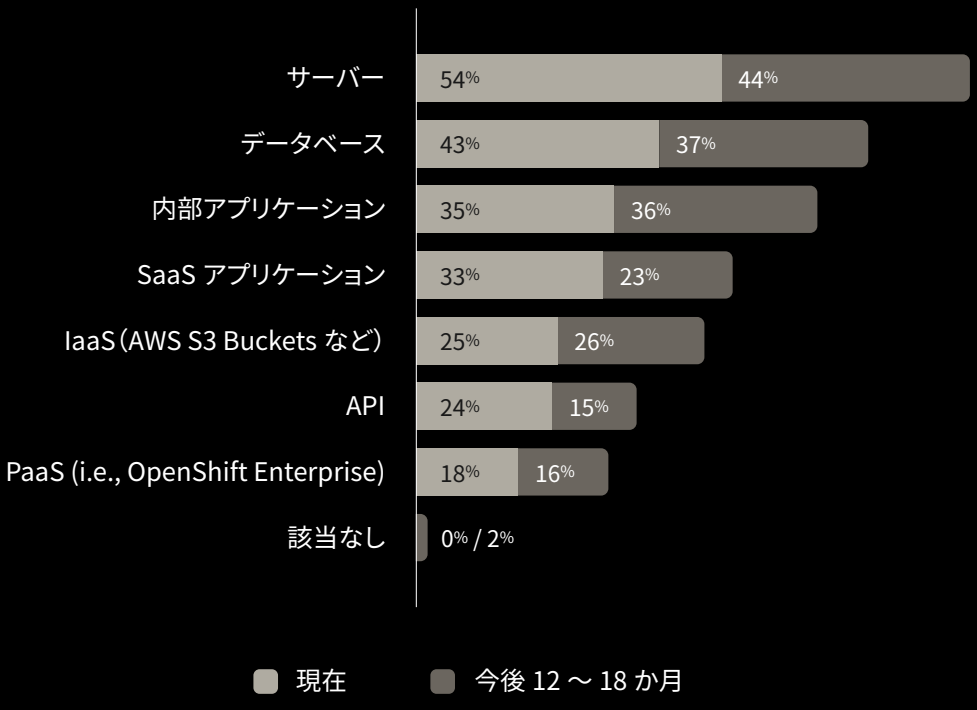
次のうち、あなたの組織がすでに実施している、または今後 12 ～ 18 か月以内に実施する予定の取り組みはどれですか?

公共部門



次のうち、SSO や MFA を導入済み、または今後 12 ～ 18 か月以内に導入する予定のリソースはどれですか?

公共部門



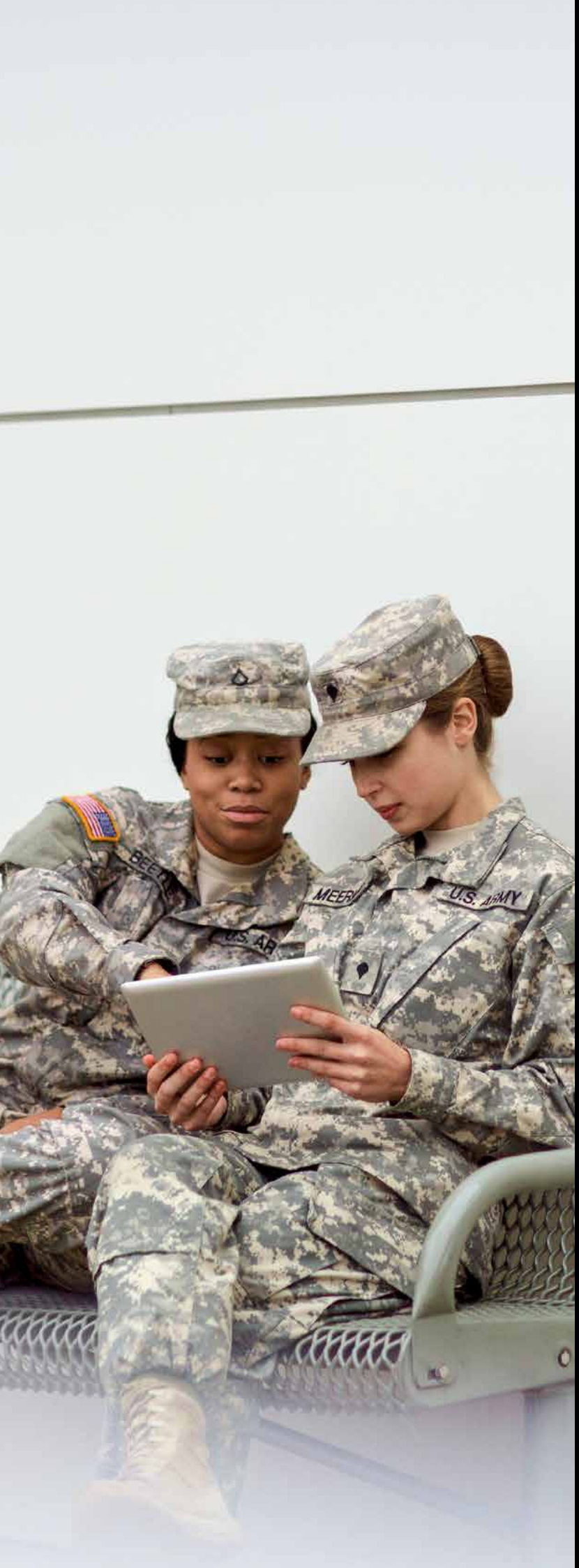
注：両方の回答を選択した回答者がいるため、棒グラフの合計が 100% を超えることがあります。

外部ユーザー向けの MFA と API へのアクセスの保護が公共部門で最多に

世界中の政府機関は、国際的に活動する多様な請負業者や外部パートナーを利用しています。そのため、外部ユーザー（パートナーやサードパーティベンダーを含む）に MFA を適用するのは当然です。また、API へのアクセスの保護も公共部門にとって主要な取り組みであり、それぞれ 33% と 30% の組織が実施しています。さらに、公共組織の 34% が、今後 12 ～ 18 か月以内に MFA の適用範囲を外部ユーザーへ拡大する予定です。続いて、従業員向けの SSO の導入と、外部ユーザー向けの自動プロビジョニング / デプロビジョニングが、今日の公共組織の取り組みとして多く挙げられています。

SSO / MFA による保護の拡張は、まずはサーバーとデータベースから

公共部門では、SSO や MFA による保護の対象は、サーバーとデータベースが最も多くなっています。この業界では、過半数の組織が、すでに SSO および / または MFA による保護をサーバーに適用しており、43% は SSO または MFA のいずれか、または両方をデータベースに適用しています。内部アプリと SaaS アプリがこれらに続き（それぞれ約 3 分の 1 の組織ですでに実施）、さらに IaaS、API、PaaS が続いています。



リソースへのアクセスに最も重要な要素は「ユーザーグループ」と「リソース自体」

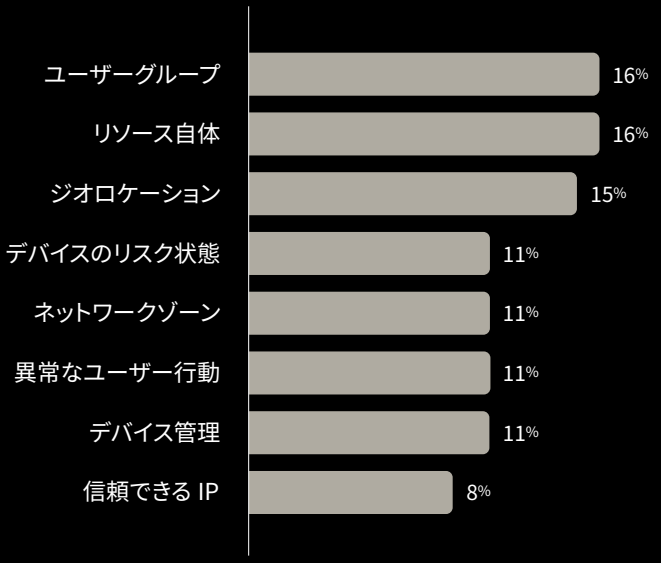
公共組織は、デジタル資産の不正アクセスからの保護に特別の注意を払っています。内部リソースへのアクセスの制御 / 承認で重視される要素としては、ユーザーグループ、リソース自体、ジオロケーションの順に多く上げられ、その他の要素はほとんどがほぼ同率となりました。

「パスワード」と「セキュリティの質問」は依然としてユーザー認証で最も使用されている

公共組織でも、本レポートの他の業界のデータに見られるのと同様、保証レベルの低い認可要素が最も使用され、パスワードとセキュリティの質問が他のどの要素よりも多く挙げられています。しかし、ソフトウェアやハードウェアの OTP、SMS / 音声 / メールの OTP のように、保証レベルのより高い要素の利用が拡大しており、変化が見られます（OTP の要素は、短期間のみ有効であるという特性を持つことから、保存可能でハッキング可能なパスワードやセキュリティの質問に比べて本質的に安全です）。

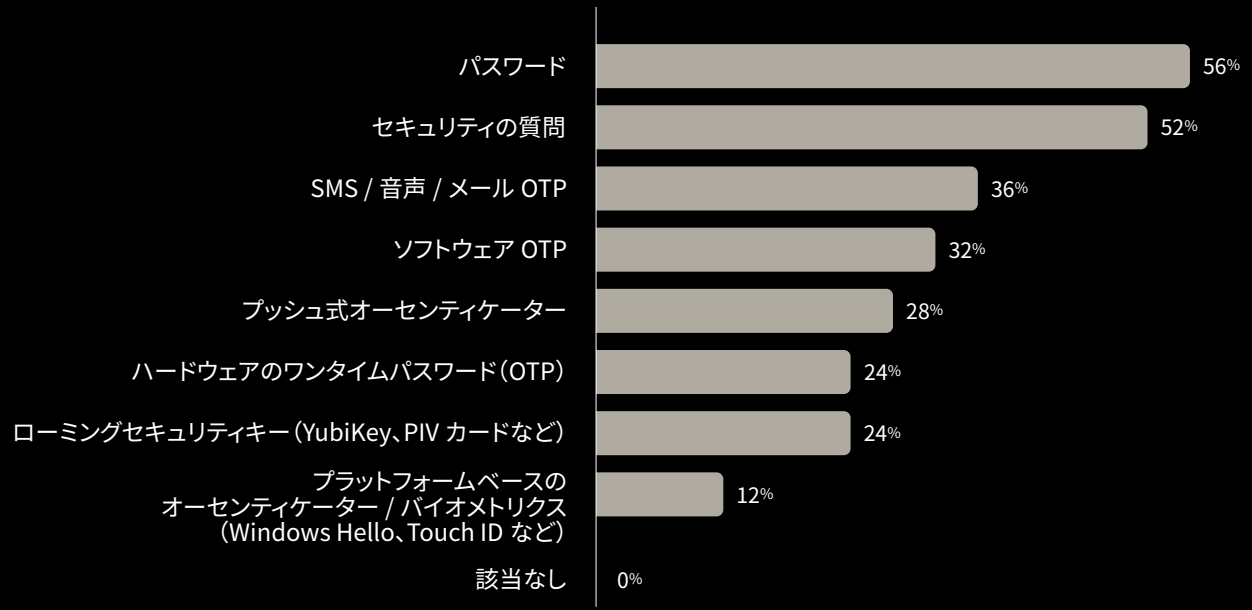
あなたの組織で内部リソースへのアクセスを制御 / 承認する際に、最も重要な要素はどれですか？

公共部門



あなたの組織は、内部 / 外部ユーザーの検証にどの認証要素を使用していますか？

公共部門



業種別のゼロトラスト進捗状況

金融サービス

金融サービス業界の組織はサイバー攻撃の格好の標的であり、ここ数年はセキュリティ侵害によって特に著しい被害を受けています。米国では 2022 年に、少なくとも 79 の金融サービス組織が、1,000 人以上のコンシューマーに影響を与えるデータ侵害を報告しました。最大規模の侵害では、それぞれ数百万人のコンシューマーが影響を受けました。これらの組織にとって、ゼロトラストは、重要なシステムと顧客データを保護するための明確な道筋を示すものとなります。現在、3 分の 2 を超える金融サービス組織がゼロトラストの取り組みを実施しており、残る 3 分の 1 の組織も大部分が取り組みを準備しています。

7 割の金融サービス組織がゼロトラストの取り組みを実施している

IBM の Cost of a Data Breach 2023 レポートによると、セキュリティ侵害は 1 件あたり平均 445 万ドルと、驚くほど高額のコストを発生させる可能性があります。したがって、ゼロトラストの取り組みを実施する金融サービス組織が年々増えているのも偶然ではありません。2021 年には、この業界でゼロトラストの取り組みを策定し実施していると回答した割合は、わずか 3 分の 1 でした。今年は、調査対象となった金融サービス組織のうち、実に 71% がゼロトラストの取り組みを現在実施していると報告しています。この 3 年間の増加には目を見張るものがあります。

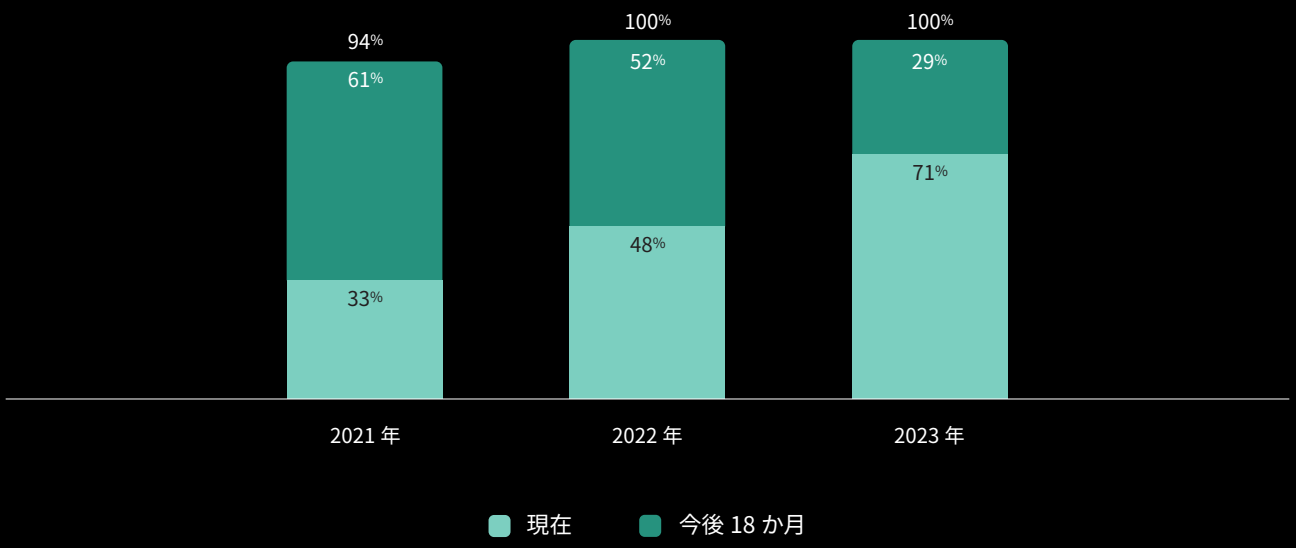
金融サービスがゼロトラストの取り組みを牽引

金融サービス業界では、3 分の 2 以上の組織がゼロトラストの取り組みを策定し実施しています。また、22% は今後 12 か月以内にゼロトラストの取り組みを予定し、さらに 8% は今後 18 か月以内に予定しています。この業界では、すでに実施されている取り組みが世界平均を上回っており、調査対象となったすべての金融サービス組織が、すでにゼロトラストの取り組みを実施しているか、18 か月以内に実施する予定であると回答しています。

金融サービス業界は、ゼロトラストにおけるアイデンティティの価値を全面的に認識しています。この業界の回答者の 9 割以上が、ゼロトラスト戦略でアイデンティティが「非常に重要」または「ある程度重要」であると回答しており、特に半数近くが「非常に重要」であると回答しています。「あまり重要でない」または「まったく重要でない」と回答した割合は、わずか 2% 程度でした。

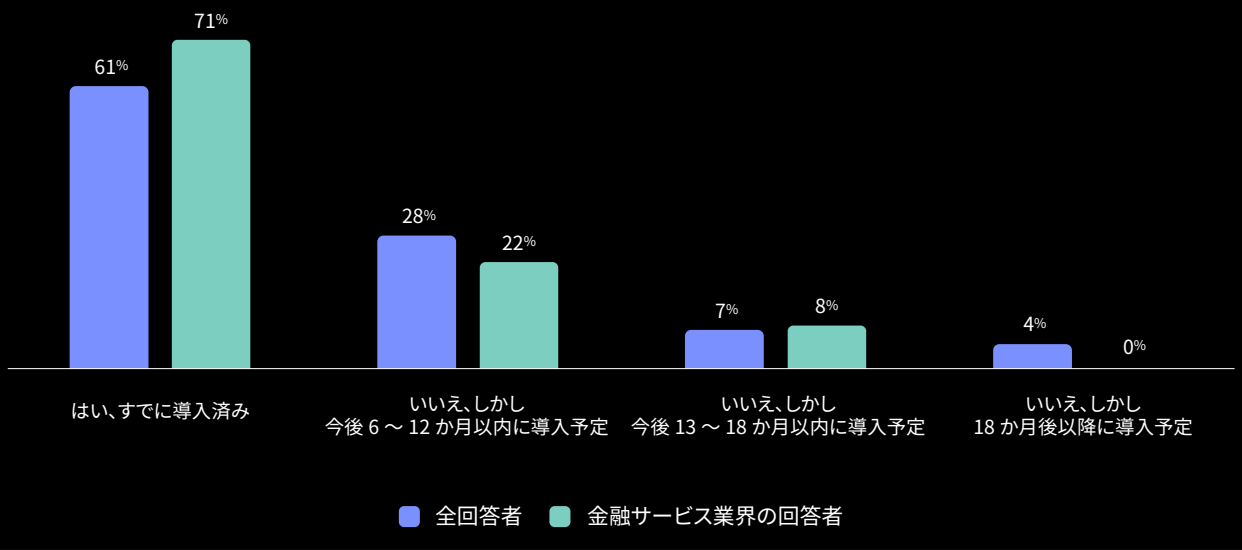
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後 18 か月以内に開始する予定ですか？

金融サービス（前年比）



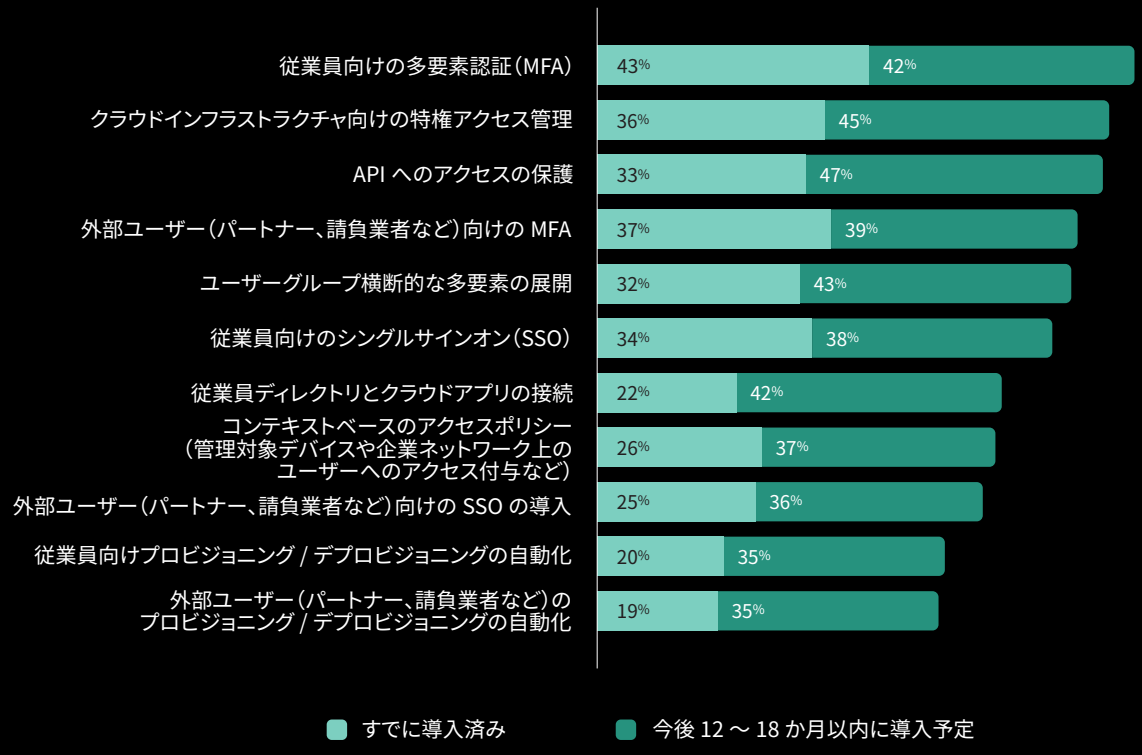
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後数か月で開始する予定ですか？

金融サービス業界と世界平均の比較



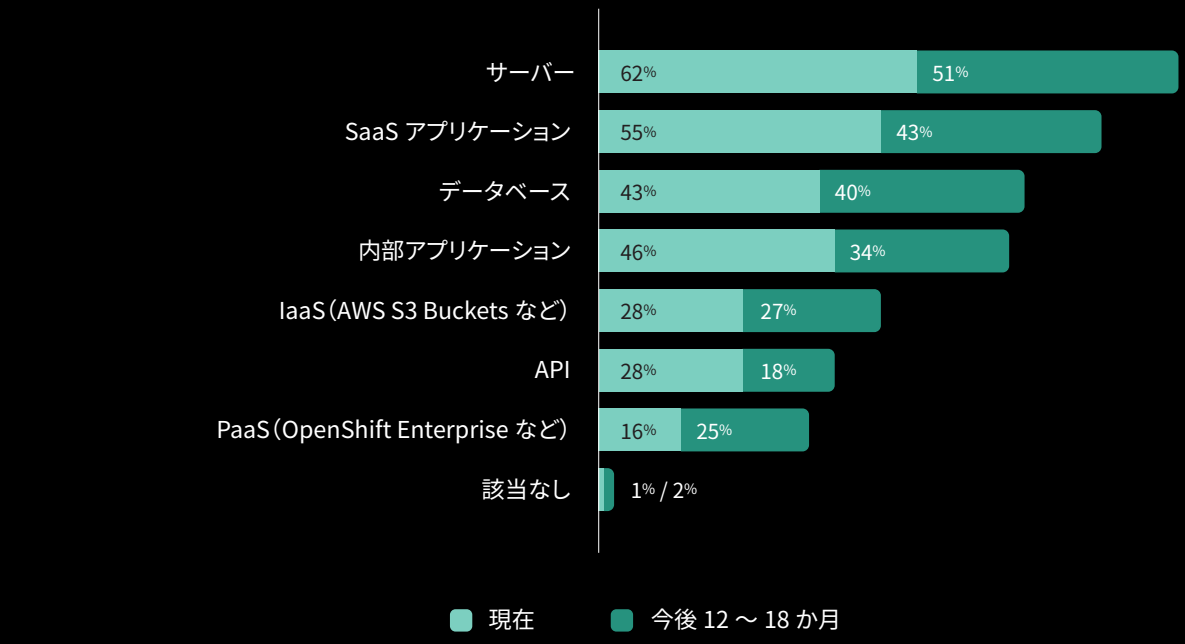
次のうち、あなたの組織がすでに実施している、または今後 12 ～ 18 か月以内に実施する予定の取り組みはどれですか?

金融サービス



次のうち、SSO や MFA を導入済み、または今後 12 ～ 18 か月以内に導入する予定のリソースはどれですか?

金融サービス



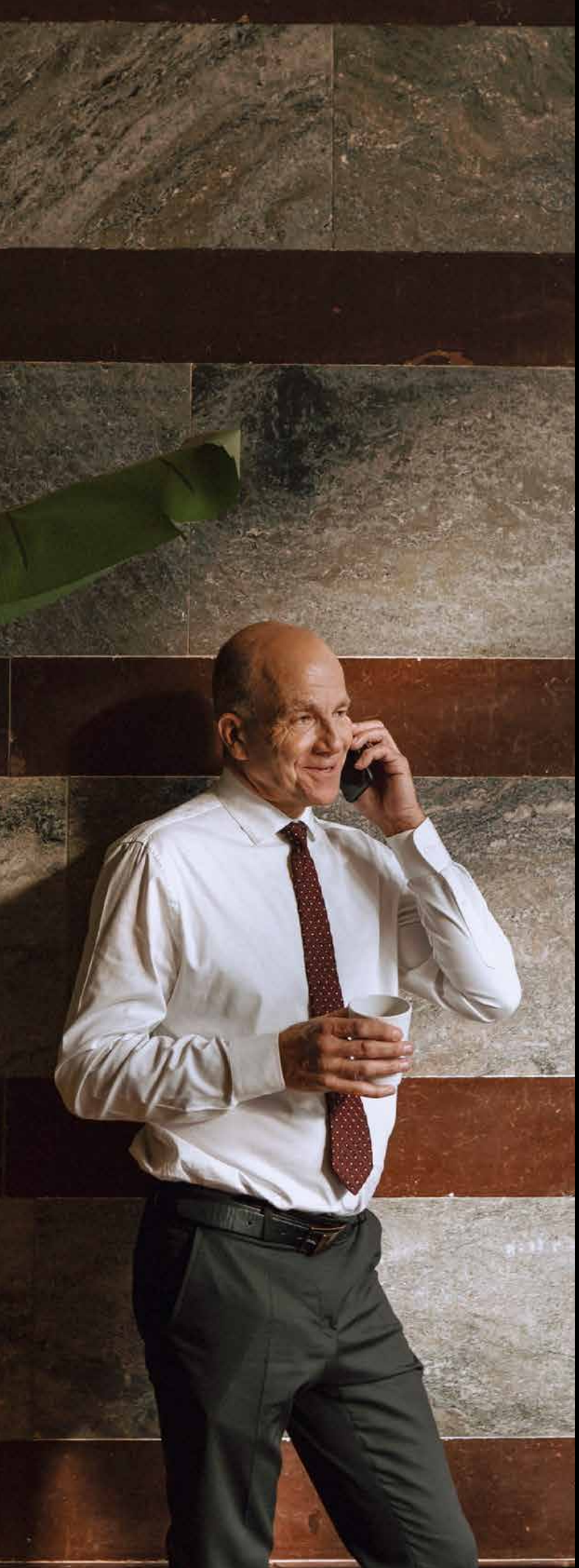
注：両方の回答を選択した回答者がいるため、棒グラフの合計が 100% を超えることがあります。

金融サービス組織は MFA と特権アクセス管理を優先させている

従業員向けの MFA は、金融サービス組織が今年ゼロトラストで最も注力している取り組みです。回答者の 43% がこのセキュリティ機能をすでに導入しており、さらに 42% が今後 12 ～ 18 か月以内に導入を予定しています。2 番目に多い取り組みとして、36% の組織がクラウドの特権アクセス管理を挙げ、また 33% が API へのアクセスの保護を挙げています。この業界で優先度が低い取り組みには、外部ユーザー向けの SSO やプロビジョニング / デプロビジョニングの自動化が含まれます。

SSO または MFA はサーバーと SaaS アプリケーションに最も適用されている

金融サービス組織はサーバーの保護を重視しており、62% がすでに SSO および / または MFA でサーバーへのアクセスを保護しており、51% が近い将来にそのような適用範囲を拡大する予定です（回答者は両方の選択肢を選択できました）。金融サービス組織がこれらのアイデンティティ対策を適用している（または適用を計画している）リソースの上位には、さらに SaaS アプリ、データベース、内部アプリが含まれます。



信頼できる IP とデバイス管理がアクセス承認の最も重要な要素に

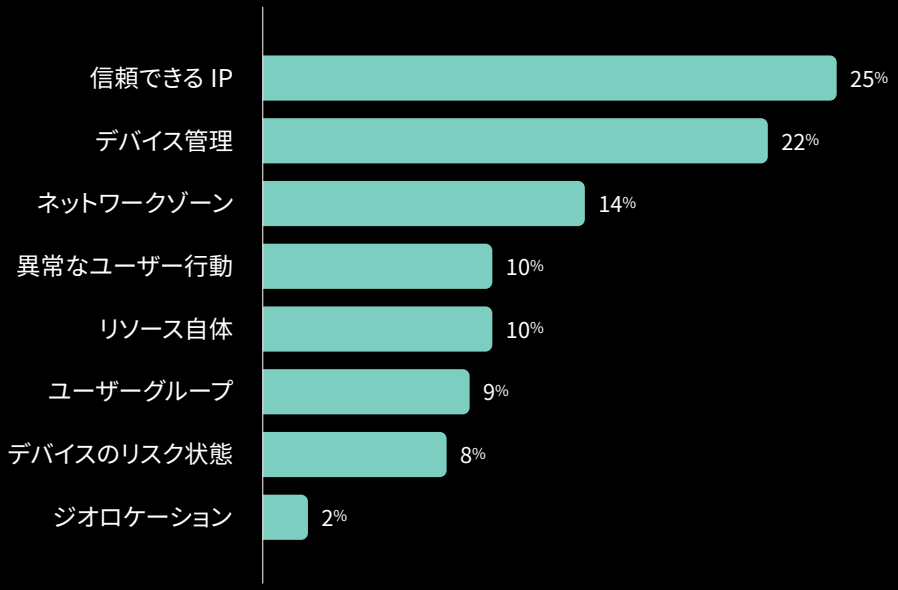
内部リソースへのアクセスの制御 / 承認に関して、金融サービス組織はユーザーの場所と使用デバイスの確認を重視しています。アクセス承認での最重要要素として、調査対象の 4 人に 1 人は信頼できる IP を挙げ、22% はデバイス管理を挙げています。さらに、ネットワークゾーン、異常なユーザー行動、リソース自体が続きます。またジオロケーションについては、選択した回答者が最も少ない点が目立っています。

金融サービス組織はパスワードとセキュリティの質問を認証要素として最も使用している

パスワードは、金融サービス組織の認証要素として引き続き最も使用されています。現在使用している認証要素としてパスワードを挙げている割合は、回答者の 3 分の 2 に上ります。知識ベースのセキュリティの質問が続いて多く（48%）、OTP オプションはそれぞれ金融サービス組織の回答者の約 3 分の 1 が挙げています。

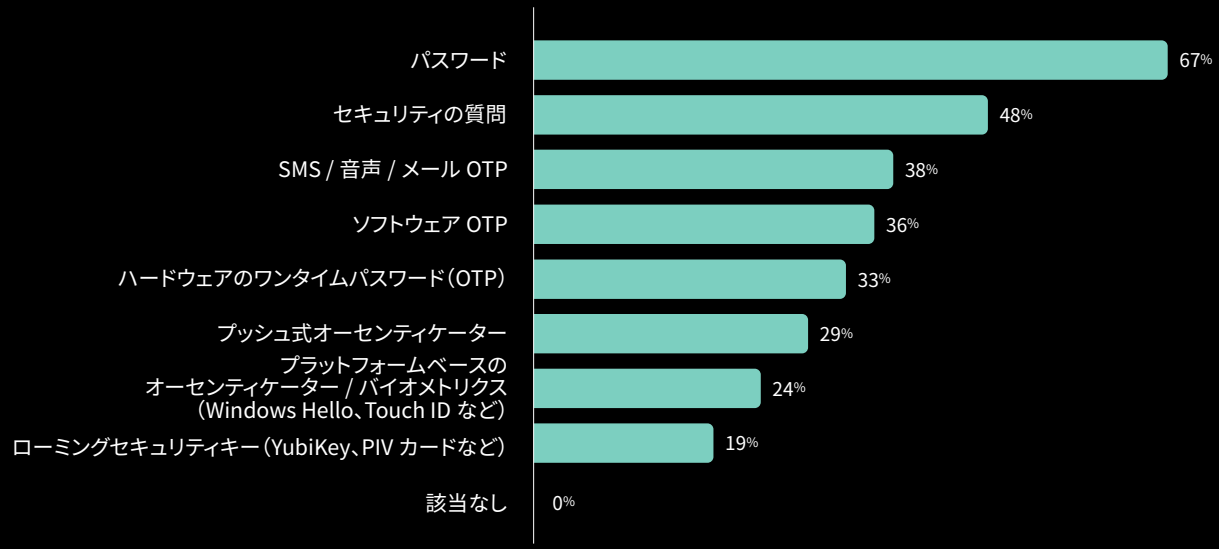
あなたの組織で内部リソースへのアクセスを制御 / 承認する際に、最も重要な要素はどれですか？

金融サービス



あなたの組織は、内部 / 外部ユーザーの検証にどの認証要素を使用していますか？

金融サービス



業種別のゼロトラスト進捗状況

ソフトウェア

昨年までの調査で、他のターゲット業種に後れをとることもあったソフトウェア業界は、着実に地歩を固めつつあり、ゼロトラストセキュリティへの取り組みを前進させています。本レポートの他のセクションで述べた、規制の厳しい他の主要業種のような追加のインセンティブがないにもかかわらず、平均を上回るようになっています。特に、保証レベルの高い認証要素の利用を拡大させ、他の重点業種に比べて認証手法をさらに進化させている点に注目すべきです。

この業界では 3 分の 2 の組織がゼロトラストの取り組みを実施している

ゼロトラスト実現の道のりにおいて、ソフトウェア組織は他の重点業種に急速に追いつきつつあります。2021 年のレポートでは、ゼロトラストへの取り組みを実施しているソフトウェア組織は 1 割未満でした。しかし、現在は 70% 近くに達しており、その他の組織も大部分が近い将来にゼロトラストへの取り組みを開始する予定です。調査対象となったソフトウェア企業のうち、ゼロトラストの取り組みを実施しておらず、今後 18 か月以内に実施する予定もない企業はわずか 4% でした。

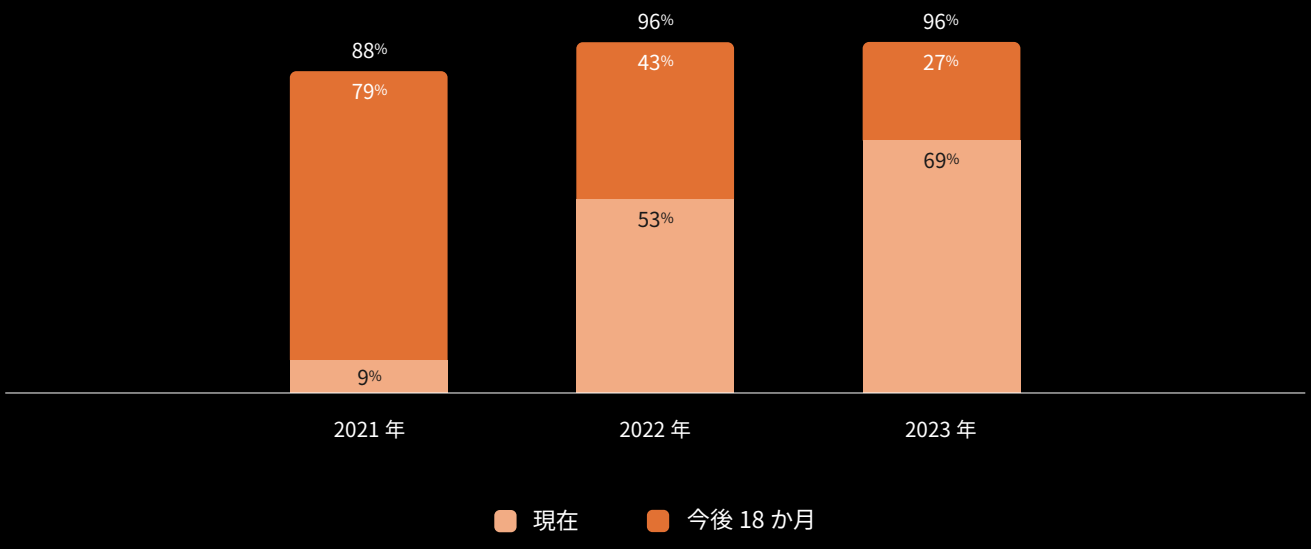
ソフトウェア業界はゼロトラストの取り組みの実施で他業種を上回る

ゼロトラストセキュリティの取り組みを策定し実施している割合については、ソフトウェア組織（69%）は世界平均（61%）を上回っています。未実施の組織も、今後 6 ～ 12 か月以内（21%）、13 ～ 18 か月以内（6%）、または 18 か月以上先（3%）に取り組みを開始する予定です。

今回の調査で、ゼロトラストに対するアイデンティティの価値をソフトウェア業界以上に理解している業界はありません。ゼロトラストセキュリティ戦略におけるアイデンティティの重要性については、ソフトウェア業界の回答者の 9 割以上が、アイデンティティが「非常に重要」（54%）または「ある程度重要」（37%）であると回答し、「あまり重要でない」と答えた回答者は 1% 未満でした。

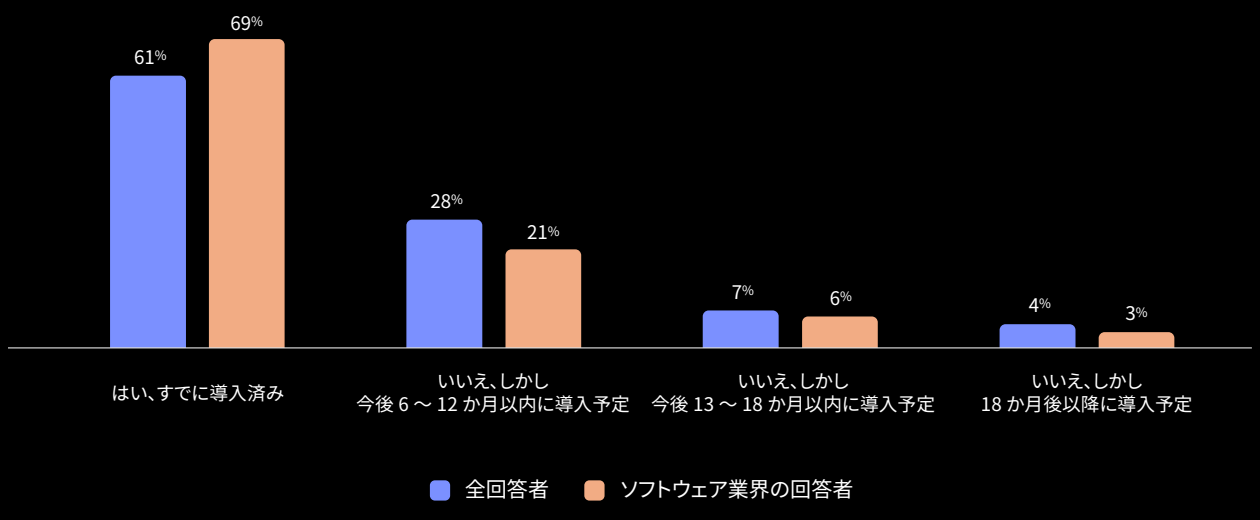
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後 18 か月以内に開始する予定ですか？

ソフトウェア（前年比）



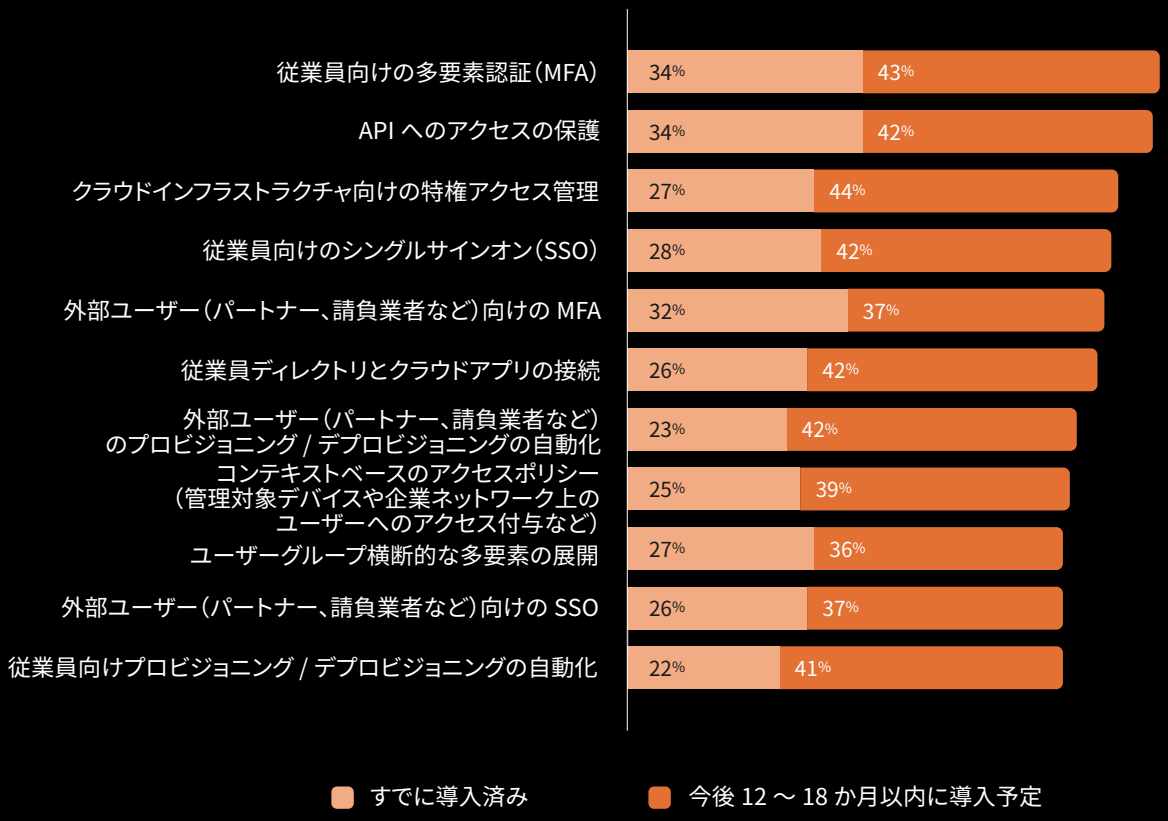
あなたの組織では、現在、ゼロトラストセキュリティの取り組みを策定し実施していますか？または、今後数か月で開始する予定ですか？

ソフトウェア業界と世界平均の比較



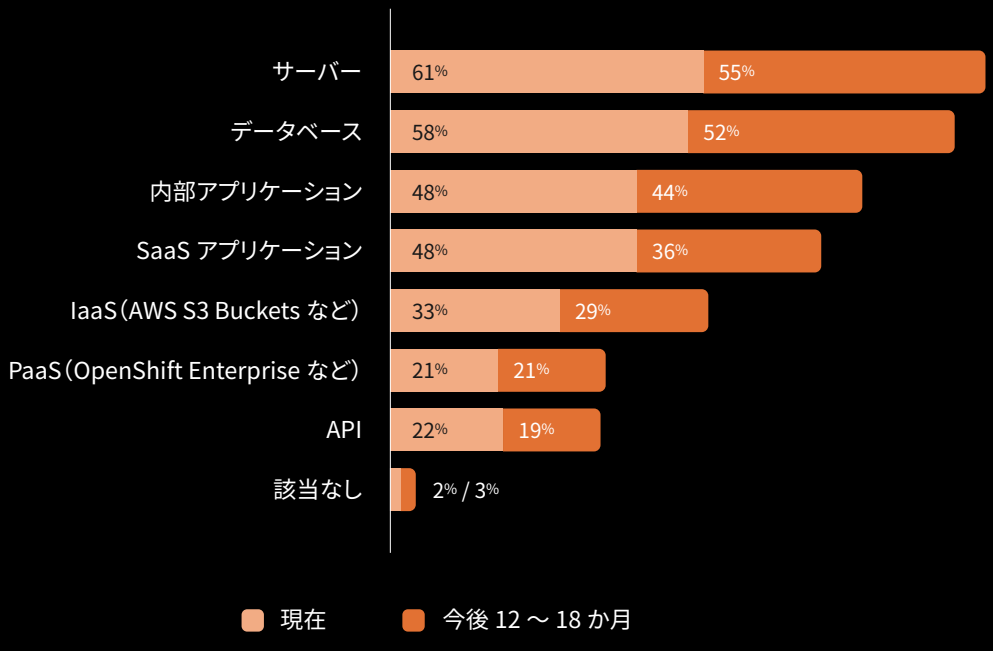
次のうち、あなたの組織がすでに実施している、または今後 12 ～ 18 か月以内に実施する予定の取り組みはどれですか？

ソフトウェア



次のうち、SSO や MFA を導入済み、または今後 12 ～ 18 か月以内に導入する予定のリソースはどれですか？

ソフトウェア



注：両方の回答を選択した回答者がいるため、棒グラフの合計が 100% を超えることがあります。

ソフトウェア業界は従業員向けの MFA と API のセキュリティを最優先させている

従業員向けの MFA と API へのアクセスの保護は、今回調査したソフトウェア組織にとって同等に重要な取り組みとなっています。それぞれのカテゴリについて、回答者の 34% がすでに取り組みを実施していると答えました。また、4 割以上が今後 12 ～ 18 か月以内にいずれか、または両方を実施する予定です。この業界の企業がすでに導入しているセキュリティの取り組みでは、外部ユーザー向けの MFA が 32% で続きました。

SSO / MFA を拡張するリソースとしてサーバーとデータベースを重視している

今年、ソフトウェア組織は、シングルサインオン（SSO）や多要素認証（MFA）を拡張することで、サーバー（61%）やデータベース（58%）へのアクセスを保護することに全力を注ぎました。さらに、調査対象の 48% が、現在 SSO または MFA により内部アプリが保護されていると回答しました。また、同じく 48% が、SaaS リソースを SSO または MFA で保護していると回答しています。

リソースへのアクセスでは信頼できる IP とデバイス管理が重視される

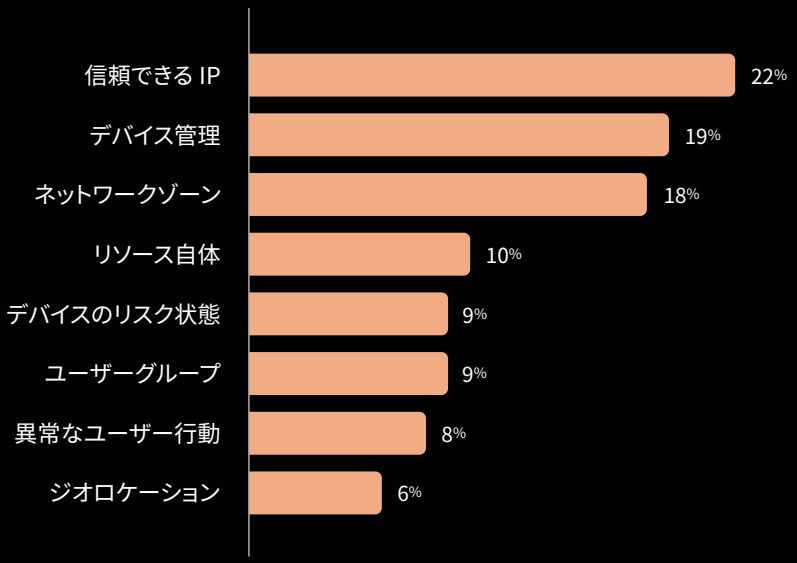
内部リソースへのアクセスを制御する場合、ソフトウェア企業の 22% が信頼できる IP を、さらに 19% がデバイス管理を最重要視し、続いてネットワークゾーン（18%）が 3 位に入っています。約 10 人に 1 人が、個々のリソース（機密システムなど）を最重要要素として挙げ、9% がデバイスのリスク状態またはユーザーグループを選びました。ジオロケーションは、調査対象のソフトウェア企業が選んだ割合が最も低い要素となりました。

ソフトウェア組織の認証要素として、セキュリティの質問がパスワードを抜いて 1 位に

ソフトウェア業界は、本レポートの中で、リスクが高く安全性が低いパスワードが最も広く使用される認証要素となっていない唯一の重点業種です。パスワードは依然として 2 位につけており、回答企業の 56% で使用されています。しかし、セキュリティの質問が 1 位（調査対象のソフトウェア組織の 61% が挙げています）に浮上したことは、少なくともこの業界ではパスワードの地位が揺らぎ始めたことを示しています。はっきり言って、セキュリティの質問とパスワードはどちらも保証レベルの低い要素であり、OTP のような保証度の高い要素に置き換えるのが最善です。

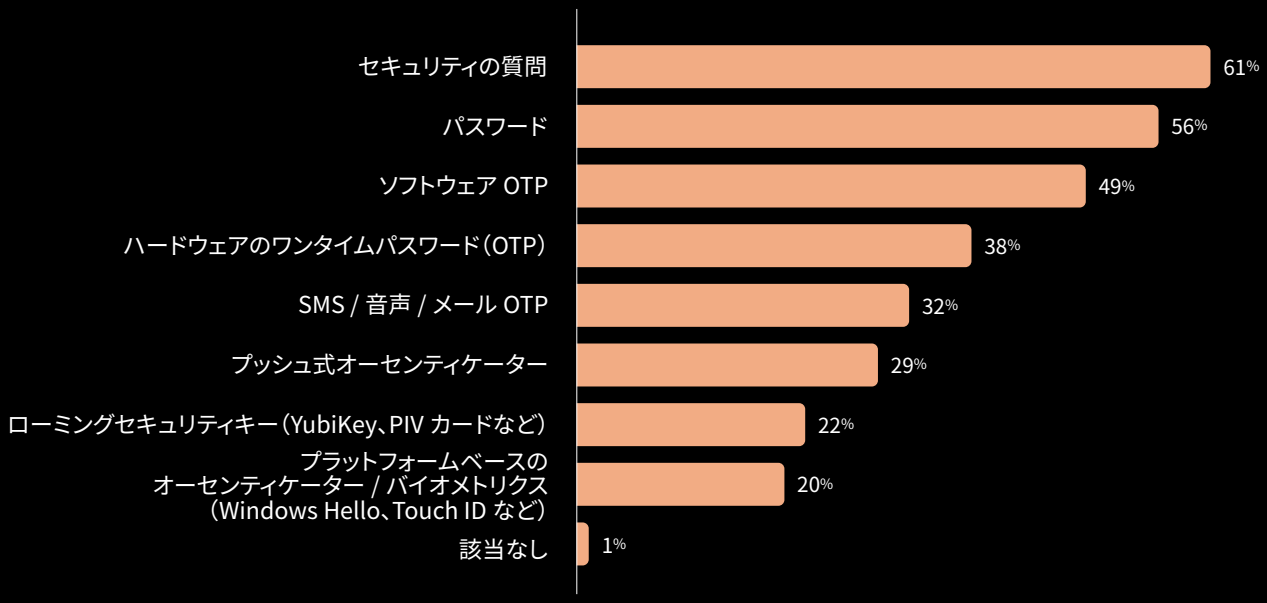
あなたの組織で内部リソースへのアクセスを制御 / 承認する際に、最も重要な要素はどれですか？

ソフトウェア



あなたの組織は、内部 / 外部ユーザーの検証にどの認証要素を使用していますか？

ソフトウェア



アイデンティティ主導のセキュリティ

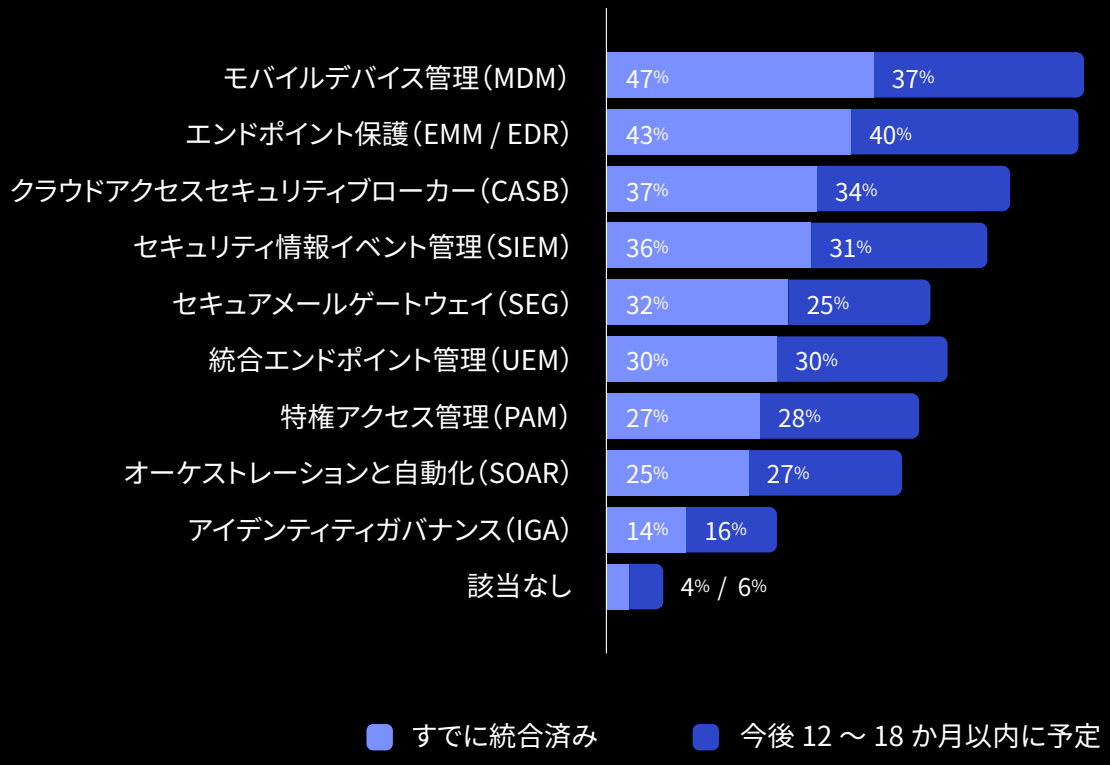
進化する企業エコシステム

アイデンティティが新たなセキュリティ境界であるとすれば、アイデンティティ管理がセキュリティ戦略の中心に位置づけられることになります。今日のハイブリッド / マルチクラウド組織は、IAM ソリューションがセキュリティシステムと確実に連携し、認証されたワークフォースの効率を妨げることなく、セキュリティチームが外部 / 内部の脅威を寄せ付けないようにしなければなりません。言い換えると、真のゼロトラストエコシステムを構築することは、アイデンティティ管理ツールとセキュリティスタックを統合することを意味します。

Okta は今回の調査で、セキュリティと IT のリーダーに、すでに IAM システムと統合しているツールと、近い将来に統合する予定のツールを尋ねました。結果は、セキュリティ情報イベント管理（SIEM）が主導していた昨年から若干変化したものとなりました。調査回答者によると、現在最も広く統合されているシステムはモバイルデバイス管理（MDM）であり、IAM ソリューションとの直接統合を優先すべき「最重要」システムは SIEM、MDM、エンドポイント保護の 3 つです。

次のうち、アイデンティティ / アクセス管理ソリューションと統合済みのツール、また今後 12 ～ 18 か月以内に統合を予定しているツールはどれですか？

全回答者



2023 年に IAM との統合が最も優先されたソリューションはモバイルデバイス管理

モバイルデバイス管理は、これまで時間をかけて着実に重要性を高めてきましたが（2021 年は 7 位、昨年は 4 位）、今年は IAM との統合が最も広く行われたソリューションとなりました。MDM を IAM ソリューションと統合した回答者は、2021 年には 11% でしたが、現在では 47% に増加し、さらに 37% が今後 12 ～ 18 か月以内に統合を計画しています。業界は、価値の高いセキュリティ監視 / 保護ツールや信頼性の高いエンドポイント管理を提供する統合を引き続き重視しています。

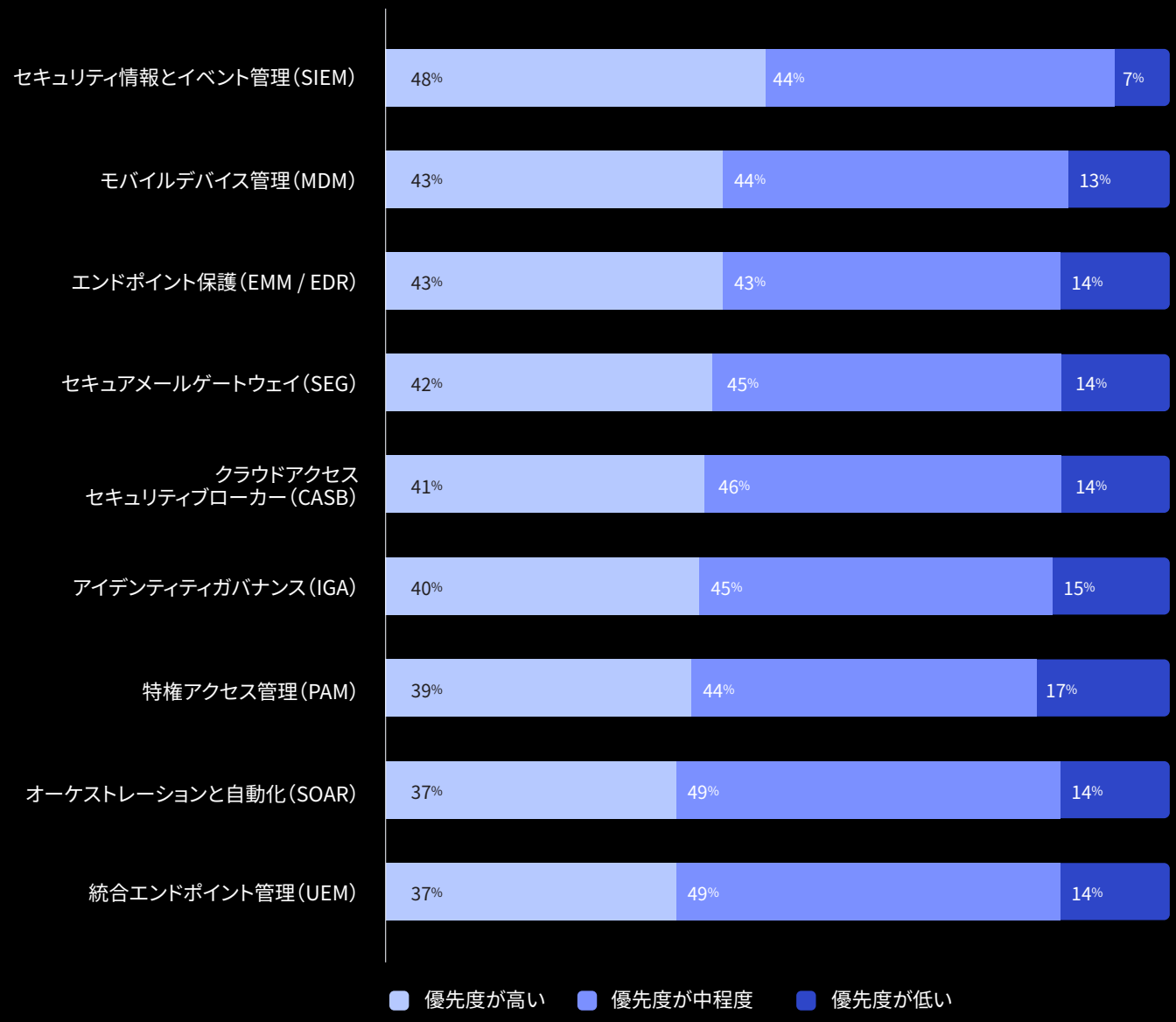
地域別の優先事項

- NAM：モバイルデバイス管理、CASB、エンドポイント保護
- EMEA：SIEM、セキュアメールゲートウェイ、統合エンドポイント管理
- APJ：モバイルデバイス管理、SIEM、SOAR、エンドポイント保護

これらの IAM 統合は、ガバナンスを簡素化し、ポリシーベースのアクセス制御、きめ細かな認可など、先進的な組織が直感的な自動化を安全に実現するための連携を可能にします。

次のうち、ゼロトラストセキュリティをサポートするために、IAM ソリューションと統合することが最も重要だと思われるツールはどれですか？

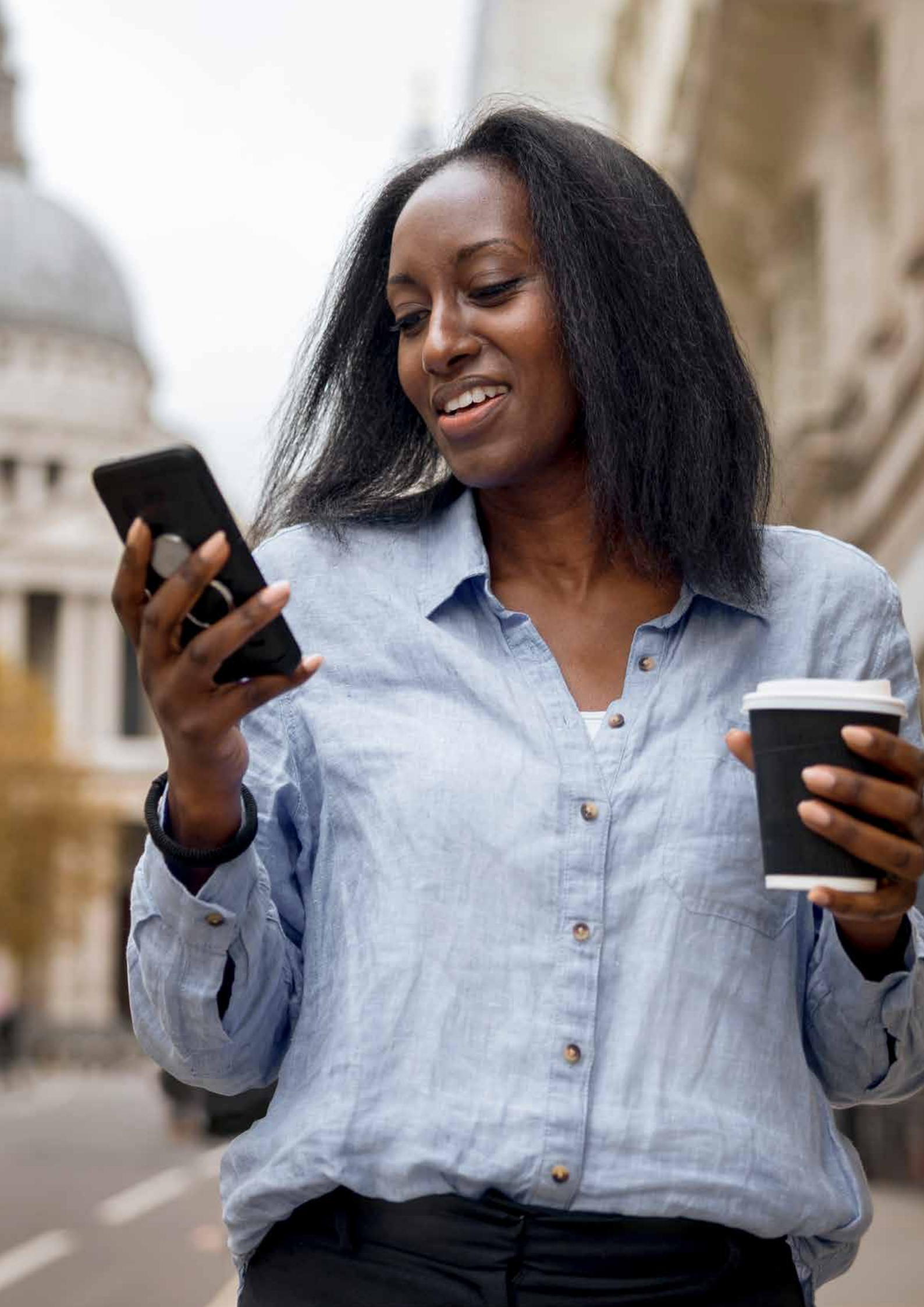
世界全体の優先事項



IAM 統合の優先付けでは、SIEM、MDM、エンドポイントが上位を占める

上記の IAM 統合の可能性について優先度（高、中、低）を尋ねたところ、世界全体としては SIEM の優先度を「高」とする回答が最も多く（48%）、MDM とエンドポイント保護がそれぞれ 43% で続きました。SOAR と UEM については、統合の優先度が「中」となる傾向が強く、また優先度が「低」とされた割合が 17% 以上のカテゴリはありませんでした。

注：データラベルを四捨五入して整数にするため、棒グラフの合計が 100% にならないことがあります。

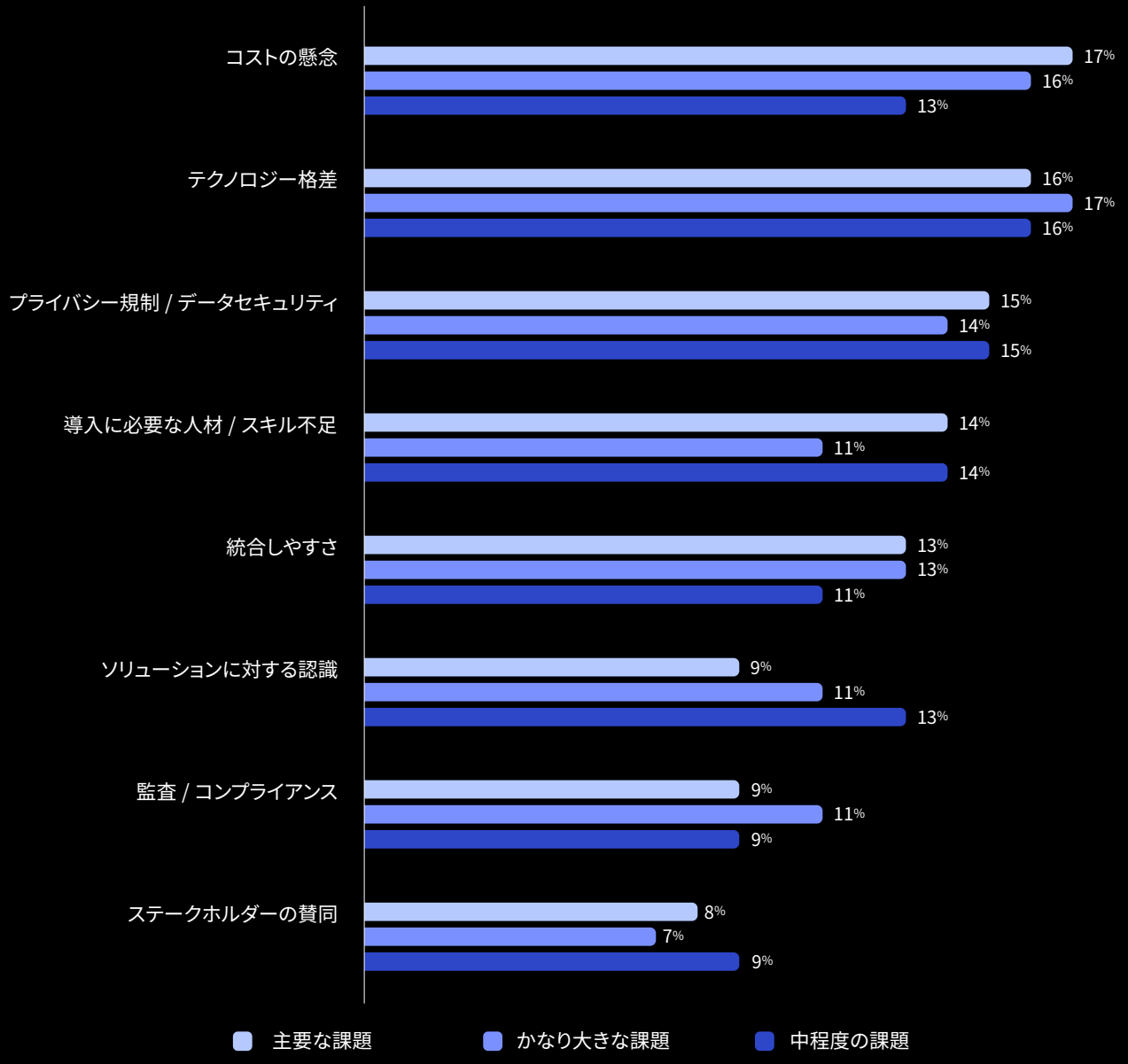


ゼロトラストへの長い道のり

企業は構造的な課題を克服し、ミッションクリティカルなゼロトラストの取り組みを開始している。

ゼロトラストは、ハイブリッド / マルチクラウド環境を運用する現代の企業を適切に保護する唯一の方法です。これによって、組織は自信を持ってグローバルチームのアクセスとプロビジョニングを自動化しながら、内部 / 外部の脅威を緩和できます。ゼロトラストの理念は今や十分に理解され、規模、業界、地域を問わず、大多数の組織が計画を策定済み、または実施中です。しかし、原則を実行に移し、ゼロトラストの「約束」を十分に生かすには、適切なソフトウェア、パートナー、プロセスが必要です。今年のデータが示すように、世界中の組織は、コストの懸念、テクノロジー格差、スキル不足など、セキュリティに関連するさまざまな問題を抱えて困難な戦いを続けています。

ゼロトラストソリューション導入における主要な課題



ゼロトラスト導入に向けた今年の最重要課題は、コストの懸念とテクノロジー

今年、ゼロトラストセキュリティの取り組みを実行に移す上での最大の課題として、回答者が最も多く挙げたのは、コストの懸念、テクノロジー格差、プライバシー規制 / データセキュリティでした。プライバシー規制は今年初めて上位に入りましたが、コストの懸念は以前から繰り返し主要な課題となっていました。2021 年には、コストの懸念が 2 番目に多く挙げられました（1 位は人材 / スキル不足、3 位はテクノロジー格差）。また、2022 年には、人材 / スキル不足、ステークホルダーの賛同の問題に次いで、コストの懸念が 3 位となりました。今年は、人材 / スキル不足に関する問題は比較的高いままですが、ステークホルダーの賛同に関する課題は減少しています。これは、ゼロトラストの原則が信頼できる専門家による検証を経たことが影響していると見られます。

今年のデータを職種別に見ると、全体的なトレンドが若干変化していることがわかります。主な懸念として、C レベル幹部はプライバシー規制と人材不足を、バイスプレジデントは統合しやすさとプライバシー規制を、ディレクターは監査コンプライアンスと統合しやすさを、それぞれ挙げました。

ゼロトラストへの長い道のり

ゼロトラストの今後

ゼロトラスト実現の道のりは、組織それぞれで異なります。近代化を進め、急速に進化するセキュリティの脅威を先取りしようと努めている組織にとって、このような複雑な戦略的取り組みの展開は、何年もかかる大きな課題となる可能性があります。とはいえ、不透明な経済状況にもかかわらず、ゼロトラストの取り組みの予算を増やし、クラウドセキュリティの強化に向けて着実に前進している組織も見られます。

真のゼロトラストを達成するには、データセキュリティとプライバシーの懸念（規制ガイドラインを含む）に対応しながら、ワークフォースの生産性を維持する必要があります。組織が投資から最大限の価値を引き出すには、既存のテクノロジースタックやエコシステムに簡単かつ迅速に統合できるソリューションが必要です。また、スキルや人材の格差のような継続的な課題にも取り組まねばなりません。

幸い、ステークホルダーの賛同を得やすくなりつつあると見られ、強力なアイデンティティ管理のメリットはより明確になってきています。今や多くのビジネスリーダーが、ゼロトラストの価値はセキュリティにとどまらないことを認識しています。ゼロトラストは、ワークフォースエクスペリエンスやカスタマーエクスペリエンスを向上させ、ハイブリッドチームの有意義なコラボレーションを促進し、顧客の信頼と収益を高める円滑で安全なエクスペリエンスを支える戦略的なビジネス推進要素でもあります。

新しいアイデンティティの境界を保護することは、おそらく今日の企業が直面する最も重要な課題です。しかし、アイデンティティに裏打ちされた真のゼロトラストを実現することで、組織はクラウドの力を全面的に活用し、俊敏性、イノベーション、ビジネス成長の新たな機会を切り開くことができます。

ゼロトラストへの長い道のり

重要ポイントのまとめ

- **ゼロトラストは行動計画から通常業務へと急速にシフトした。**

  以前は実現の難しい目標であると考えられたゼロトラストが、現在では日々の運営上の現実となっています。大半の組織はすでにゼロトラストの取り組みを展開し、安全性と競争力を維持するために活用しています。その他の組織も概ね、計画を策定し、準備しています。

- **今やアイデンティティは、ゼロトラスト戦略においてミッションクリティカルな要素であることが広く理解されている。**

  ハイブリッド / マルチクラウド環境で機敏に活動する今日の企業にとって、アイデンティティは新たな境界です。強力なアイデンティティ管理は、成功の基盤となる戦略であり、自信を持って拡張する上での安全な道筋を提供するものとなります。

- **ゼロトラストの予算は、市場原理に逆らうかのごとく依然として増加し続けている。**

  外部からの攻撃や内部の脅威は、不景気だからと手を緩めることはりません。セキュリティ予算も同様であり、企業はアイデンティティベースのセキュリティの取り組みを通じて防御を強化することに注力しています。

- **ゼロトラストの採用を目指す企業は、依然として困難な課題に直面している。**

  ゼロトラストセキュリティ戦略の設計、スケジューリング、実施は、多くのステークホルダーが関与する複雑な取り組みです。また、成功への道筋は組織それぞれに異なり、プライバシー規制、テクノロジー格差、コストの懸念などの要素によって、課題がさらに複雑化しています。

Okta のワークフォースアイデンティティ成熟モデルで自社の現状を評価する方法など、詳細はこちらをご覧ください。

Okta について

Okta は、世界を代表するアイデンティティ企業です。独立系の主要アイデンティティパートナーとして、すべての人が、場所やデバイス / アプリを問わず、どのようなテクノロジーでも安全に利用できるよう支援しています。世界で最も信頼されるブランドが Okta を信頼し、安全なアクセス、認証、自動化を実現しています。Okta が提供する Workforce Identity Cloud と Customer Identity Cloud は、柔軟性と中立性を中核に据え、カスタマイズ可能なソリューションと 7,000 以上の事前構築済みの統合を提供しています。これにより、ビジネスリーダーや開発者はイノベーションに集中し、デジタルトランスフォーメーションを加速させることができます。Okta は、アイデンティティを積極的に管理できる世界を作っています。詳しくは okta.com をご覧ください。

免責事項

okta

Okta Japan 株式会社
〒 150-8510 東京都渋谷区渋谷
2-21-1 渋谷ヒカリエ 30 階
お問い合わせ先：
okta.com/jp/contact-sales/