RSA

RSA.com

2026 RSA ID IQ レポート

RSA IDセキュリティパルスチェック

このレポートの目次.

エクゼクティブ　サマリー.

2026年版「RSA ID IQレポート」では、世界中の2,000人以上の専門家に対し、アイデンティティセキュリティがどのくらいの頻度で問題が発生したか、その結果どれだけの損失を被ったか、そして最も懸念している脆弱性は何かを詳しく尋ねました。.

その結果は衝撃的なものでした。昨年よりも多くの組織でアイデンティティの問題が発生し、その財務的損害はさらに大きくなっていたのです。リーダーたちが今行動を起こさなければ、組織が直面するリスクはますます深刻化し、その結果としての損失はさらに増大するでしょう。

データから見えてくるのは、「アイデンティティセキュリティのギャップ」が拡大しているという現実です。多くの組織はいまだに古いソリューションを使い続けており、新たな課題に十分対応できていません。大多数のユーザはいまだにパスワード認証に依存しており、そうした組織では侵害の発生頻度も損失額も高いことが報告されています。

同時に、複雑な運用環境や難しいユースケースが障壁となり、パスワードレス化への移行も進んでいません。

さらに、組織はソーシャルエンジニアリングやITヘルプデスクを狙ったバイパス攻撃への防御能力を十分に持っていません。こうした攻撃手法がますます重大なリスクとなっているにもかかわらずです。

人、マシン、サービスといったアイデンティティを監視している組織もありますが、データ侵害の発生率を見る限り、その情報をリスク軽減に効果的かつ積極的に活用できていないことは明らかです。そのようなリスクの高まりを背景に、専門家たちはサイバーセキュリティ分野でのAI活用に全面的に賛同しています。

あらゆる業界で、AIはサイバー犯罪を助長するよりもむしろサイバーセキュリティを強化するものだと考える人が増えており、これまでになく多くの組織がAIをサイバーセキュリティ体制に統合する計画を報告しています。さらに、多くの組織が「エージェンティックAI（自律型AI）」をサイバーセキュリティ分野で最優先に導入したい機能として挙げています。

これらの調査結果が雄弁に物語っています。そして、この情報自体が有益であるだけでなく、リーダーたちは今こそ行動を起こすことが重要です。

具体的には、パスワードレス認証の優先導入、ヘルプデスク詐欺に対抗するための最新防御策の実装、侵害が発生する前にアイデンティティリスクを積極的に特定・解消すること、そしてAIを活用して意思決定を迅速化する力を高めることが求められます。

どんな問題にも、まず「問題が存在する」と認めることが解決への第一歩です。

2026年版「RSA ID IQレポート」は、ほとんどの組織におけるアイデンティティセキュリティに重大な懸念があることを明確に示しています。

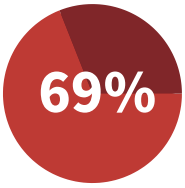
アイデンティティはあまりにも多くの組織で、あまりにも頻繁に失敗しています。

侵害が発生する可能性、そして何もしないことの代償はあまりにも大きく、「現状維持」はもはや許されません。

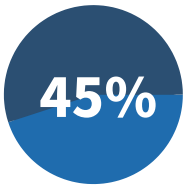
Greg Nelson, CEO, RSA

2026 RSA ID IQ レポートの主な調査結果

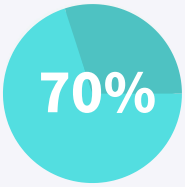
2026年版「RSA ID IQレポート」では、サイバーセキュリティ、アイデンティティとアクセス管理（IAM）、IT、その他の分野で働く2,120人の専門家から得られた情報を共有しています。主な調査結果は以下のとおりです。



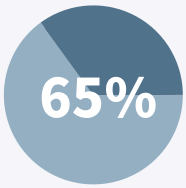
の組織が過去3年間にアイデンティティ関連の侵害を経験したと報告しており、これは2025年から27ポイントの増加となっています。



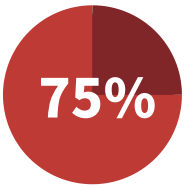
の組織が、アイデンティティ関連のデータ侵害は平均的なデータ侵害よりも高いコストがかかったと回答しています。



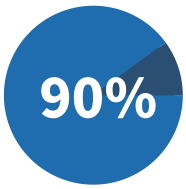
の組織が、アイデンティティ侵害によって深刻な被害を受けたと回答しています。



の組織は、自社のITヘルプデスクまたはサービスデスクがソーシャルエンジニアリング攻撃を阻止できないのではないかと深刻に懸念していると述べています。

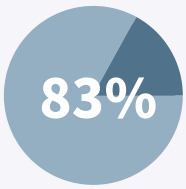


の組織がハイブリッド環境で運用しており、これは2025年から5ポイントの増加となっています。

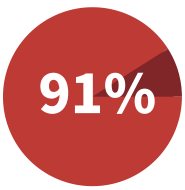


の組織は、パスワードレス認証への移行に課題があると報告しています。

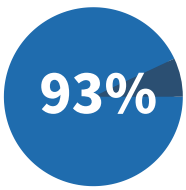
の組織は依然として、認証の主要な手段としてパスワードを使用し続けています。



の組織は、AIはサイバー犯罪を助長するよりもサイバーセキュリティを支援する効果が大きいと考えており、これは2025年から3%の増加です。



の組織が、今後1年以内に何らかの形でAIを自社の技術スタックに導入する計画を立てており、これは2025年から12ポイントの増加です。



の組織はまだ、最適なゼロトラスト成熟度には達していません。

より多くのアイデンティティ侵害が、さらに大きな被害をもたらす

調査回答の分析によると、今年はアイデンティティセキュリティの問題による侵害が、より多くの組織で発生していることが分かりました。過去3年間に侵害を報告した組織は69%に上り、これは2025年版「RSA ID IQレポート」から27ポイントの増加です。

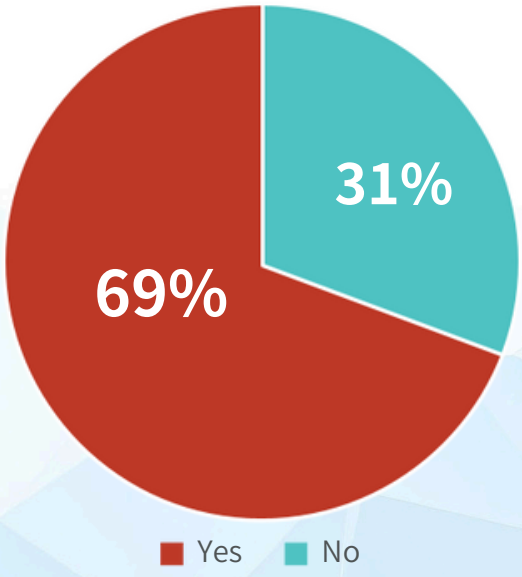
I侵害は頻度が増しただけでなく、被害規模も大きく、コストも高額になっています。回答者全体の5分の1以上（21%）が、アイデンティティ関連の侵害による損失額が500万～1,000万ドルであったと報告しており、ほぼ4分の1（24%）が侵害による損失額が1,000万ドルを超えたと回答しています。1,000万ドルを超える侵害の割合は、昨年のレポートと比べて3ポイント増加しました。

これらの数字は、どの観点から見ても非常に憂慮すべきものです。特に、あらゆる攻撃手法によるデータ侵害の世界平均コストと比較すると、その深刻さが際立ちます。**IBM Cost of a Data Breach Report 2025** によると、平均的なデータ侵害のコストは444万ドルです。アイデンティティの問題が発生すると、組織にかかる損失はそれを大きく上回ります。そのため、回答者の70%が侵害の深刻度を5段階中の4または5と評価しているのも当然と言えるでしょう。

69%

の組織が、過去3年間にアイデンティティ関連の侵害を経験したと報告しており、**これは27ポイントの増加です。**

あなたの組織は、**過去3年間にアイデンティティ関連の侵害**を経験しましたか？

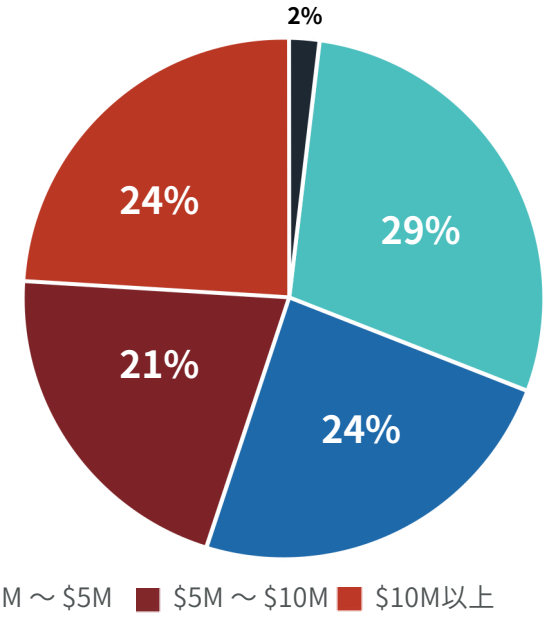


24%

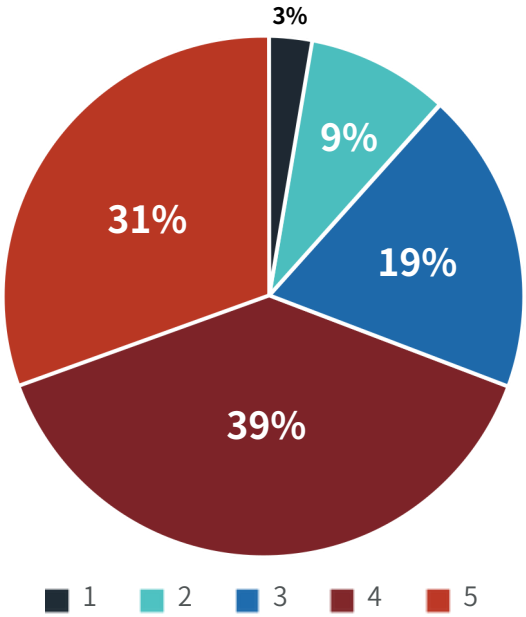
アイデンティティ関連の侵害を経験した組織のうち24%が回答しました。

その侵害による損失は1,000万ドル以上で、2025年から3ポイントの増加となっています。

過去3年間に発生したアイデンティティ関連のデータ侵害によって、**貴社はどのくらいの金額を損失したとお考えですか？**



過去3年間にアイデンティティ関連の侵害を経験した場合、その影響の深刻度を1から5で評価してください。



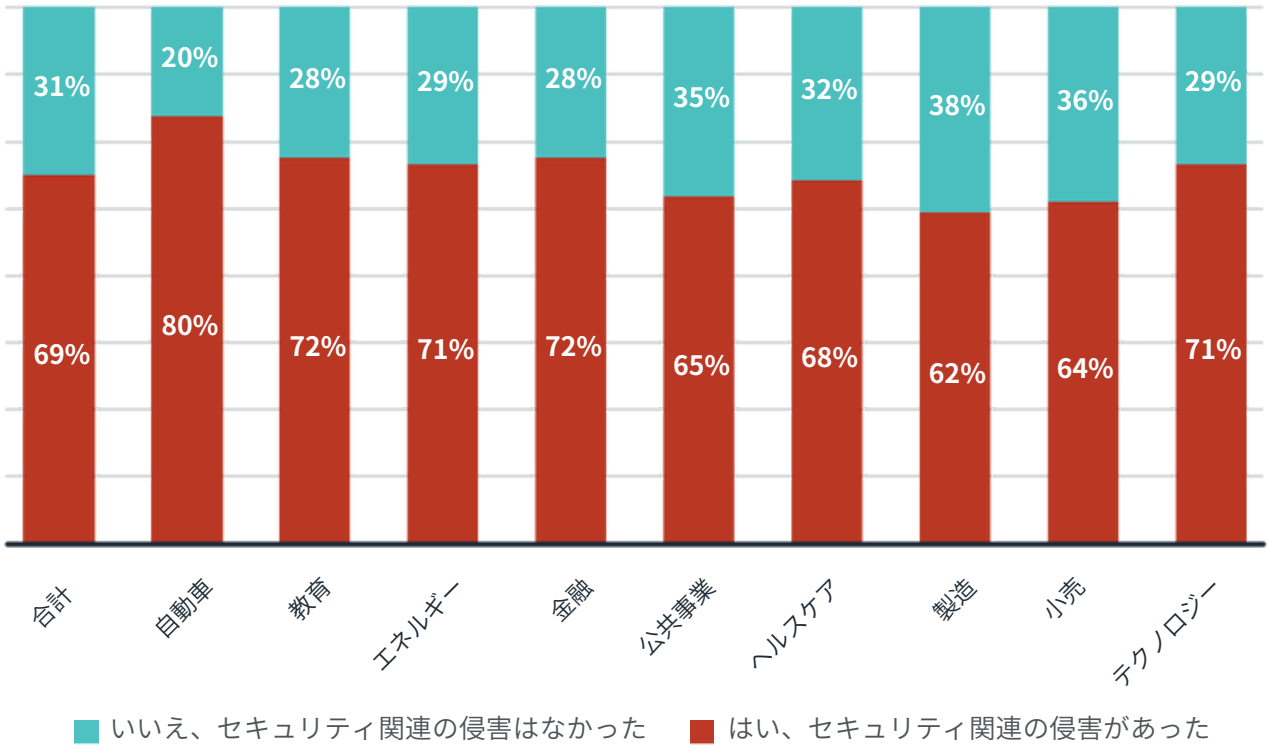
$4.44 Million

全データ侵害の平均コスト（世界平均）
IBM Cost of a Data Breach Report 2025

業種別のセキュリティ侵害

業種別のデータ侵害の発生率を調べたところ、自動車業界（80%）、金融（72%）、エネルギー・公益事業（71%）、テクノロジー（71%）が最も高い侵害発生率を報告しました。
一方、小売（64%）、製造（62%）は、業種別では最も攻撃を受けにくい分野となっています。

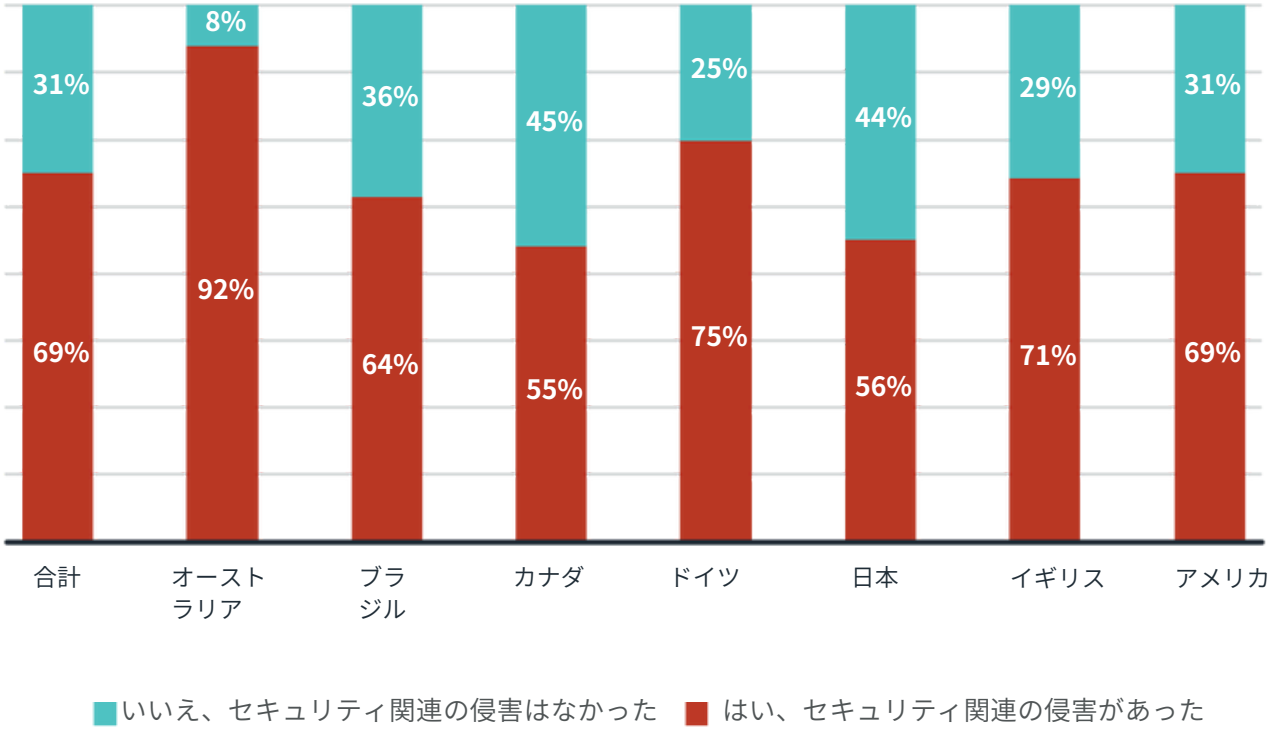
業種別：過去3年間に、貴社はアイデンティティ関連の侵害を経験しましたか？



国別のセキュリティ侵害

国別では、オーストラリア（92%）、ドイツ（75%）、イギリス（71%）、アメリカ（69%）が過去3年間で最も頻繁にアイデンティティ関連の侵害を報告しました。一方、日本（56%）とカナダ（55%）は最も少ない発生率となっています。
レポートの後半では、特定の対策や慣行が、侵害の発生頻度や影響とどのように関連しているかについて説明しています。

国別：過去3年間に、貴社はアイデンティティ関連の侵害を経験しましたか？



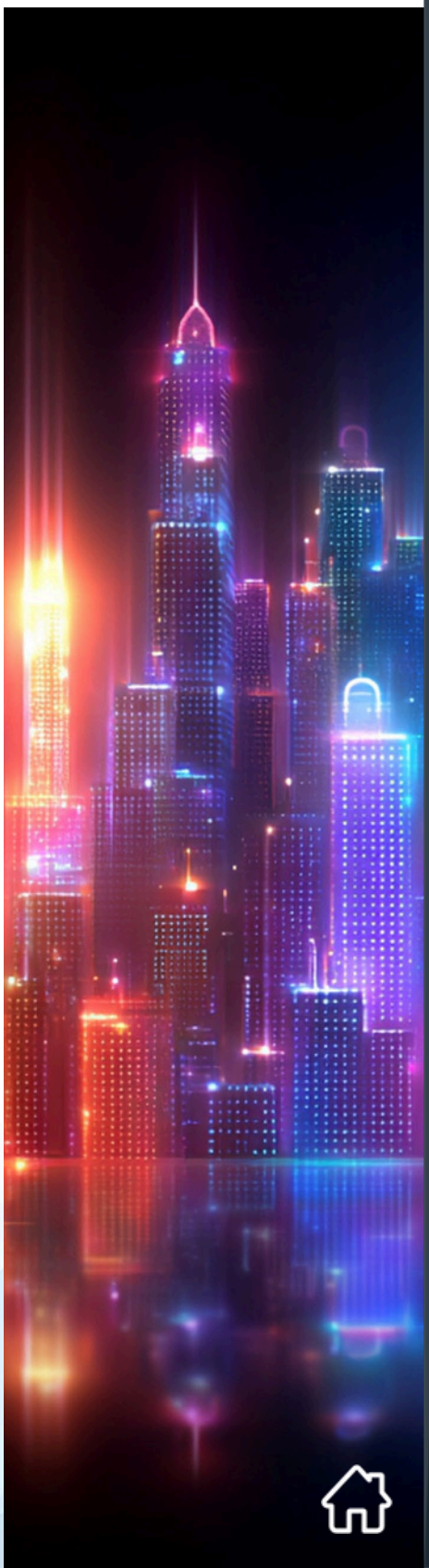
ゼロトラストの「進捗」

CISAが定義するアイデンティティに関する最適なゼロトラスト成熟度に到達したと報告している組織はわずか7%ですが、大多数の57%は「高度（Advanced）」なゼロトラスト段階に到達していると考えています。具体的には以下が含まれます：

- フィッシング耐性のある多要素認証（MFA）
- アイデンティティストアの統合と安全な連携
- 自動化されたアイデンティティリスク評価
- 必要性やセッションに基づくアクセス制御

しかし、これらの評価は事実と矛盾しています。
なぜなら**69%の組織が侵害を受け**、
70%がその侵害を「深刻」と報告しています。

これは、組織がゼロトラストの成熟度を高めることを思いとどまらせるためのものではありません。むしろその逆です。問題は、組織が自身のゼロトラストの進捗をどの程度だと考えているかと、実際の侵害発生頻度との間にギャップがある点にあります。このギャップは、セキュリティリーダーに対して、より一層の対策を講じる必要があることを警告しているのです。



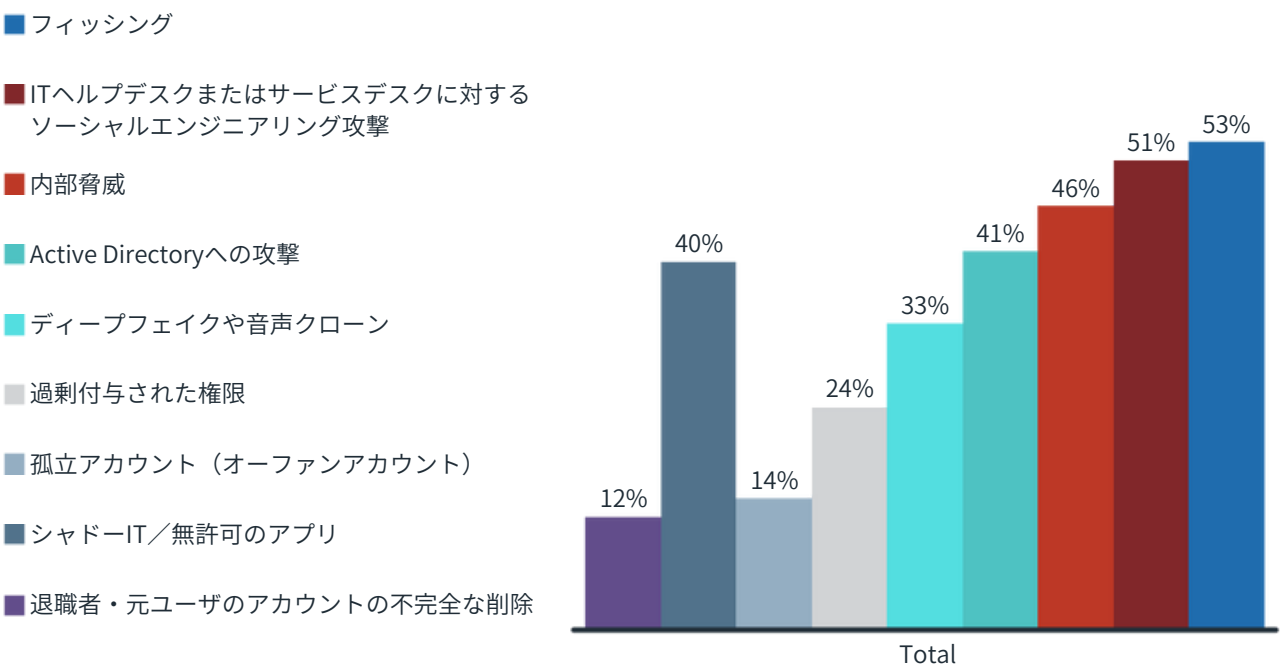
専門家を眠れなくさせる サイバーセキュリティリスク

回答者は、フィッシングを自社にとって最も重大なサイバーセキュリティリスクをもたらす脅威要素として選びました。フィッシングを優先すべき理由も明確です。年々、フィッシング（認証情報の盗難につながる）や盗まれた認証情報の使用は、最も頻繁かつ影響の大きい攻撃の一つとして残っています。
フィッシングを回避する最善の方法の一つは、フィッシング攻撃者が盗もうとする認証情報を排除することです。つまり、知識認証に依存するのではなく、組織はフィッシング耐性のあるパスワードレス認証の導入を目指すべきです。

192 日
フィッシングによる侵害を特定し封じ込めるまでに、組織が平均で費やす日数

$4.8 Million
フィッシングによるデータ侵害の平均コスト
IBM Cost of a Data Breach Report 2025

フィッシングは常に存在するサイバーセキュリティリスクですが、新たに浮上しているサイバーリスクも急速に重要なリスクとして認識されつつあります。回答者の51%は、ITヘルプデスクやサービスデスクに対するソーシャルエンジニアリング攻撃が、自社にとって最も重大なリスクであると回答しています。



ヘルプデスクも支援が必要です

MGMリゾート、シーザーズ・エンターテインメント・グループ、マークス＆スペンサー、コープ、ハウス・オブ・ディオールなどで大きく報道されたヘルプデスク攻撃を踏まえると、このリスクを優先すべき理由は明確です。Scattered Spiderをはじめとするサイバー犯罪グループが示す通り、サイバー犯罪者がITヘルプデスクやサービスデスクに正規ユーザを装って電話し、新しいアカウントを作成させたり、MFAを一時停止させたり、新しいユーザやデバイスを登録させたりしようとする場合には、大きなリスクが存在します。実際、サイバーセキュリティの専門家は、ITヘルプデスクに対するソーシャルエンジニアリング攻撃を、自社が直面する最大のリスクとしてランク付けしています。

このリスクをさらに悪化させているのは、組織がユーザの身元確認のために、新しいフィッシング耐性のある手法を十分に活用していないことです。ほとんどの組織は古い認証方法を使用しています。組織の58%がパスワード、50%がワンタイムパスワード（OTP）、46%が共有シークレットを使用しています。これに対し、両者が互いに認証できる双方向認証を使用していると報告した組織はわずか36%、ユーザやユースケースの優先順位付けを支援するリスクベースのソリューションを使用していると報告した組織は全体の4分の1（25%）に過ぎません。

ユーザの身元確認における旧来の方法

58%
の組織がパスワードを利用

50%
がOTPを利用

ユーザの身元確認における新しい方法

36%
の組織が双方向のアイデンティティ確認を利用

25%
がリスクベースのソリューションを利用

誰からの電話？

2023年以降、BlackCat、ALPHV、Scattered Spiderなどのサイバー犯罪グループは、組織のITヘルプデスク担当者に対してソーシャルエンジニアリングを行い、MFAバイパス攻撃を仕掛けて大きな被害と損失を引き起こしています。

MGM Resorts:
$145M

Caesars Entertainment:
$15M

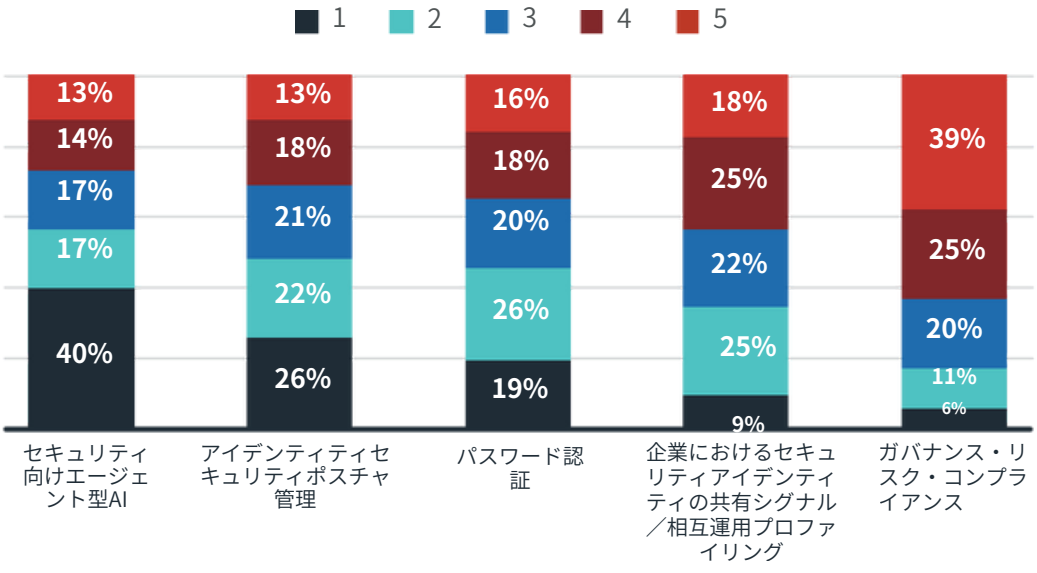
Marks & Spencer:
£300M

回答者の3分の1（33%）は、ディープフェイクや音声クローンなどの新しい手法が、自社にとって最も大きなリスクをもたらすと回答しました。これらの手法は、MFAバイパス攻撃を防ぐ最新の手段がない場合、より効果的に作用する可能性があります。
その他、専門家が特に懸念しているリスクの多くは、アイデンティティのライフサイクルや権限の過剰付与（entitlement creep）に関連しています。内部脅威（46%）、シャドーITや未プロビジョニングのアプリ（40%）、過剰付与された権限（24%）は、ユーザにとって優先度の高いリスクとして際立っています。これらの問題は、アイデンティティリスクの可視性不足、手動によるアイデンティティライフサイクル管理、事後的なリスク軽減といった要因によってさらに悪化する可能性があります。

ユーザが優先するサイバーセキュリティ能力

セキュリティ向けのエージェント型AI（Agentic AI）が、ユーザの間で大差をつけて最も重視されており、回答者の40%がこれを最優先事項として挙げています。
次に重要とされたのは、アイデンティティセキュリティポスチャ管理（ISPM）です。ISPMは、新しいサイバーセキュリティフレームワークであり、組織がリスクを管理し、ポリシーを適用し、複雑化する環境全体でコンプライアンスを強化することを可能にします。回答者の26%が、ISPMを最も重要な能力として挙げています。

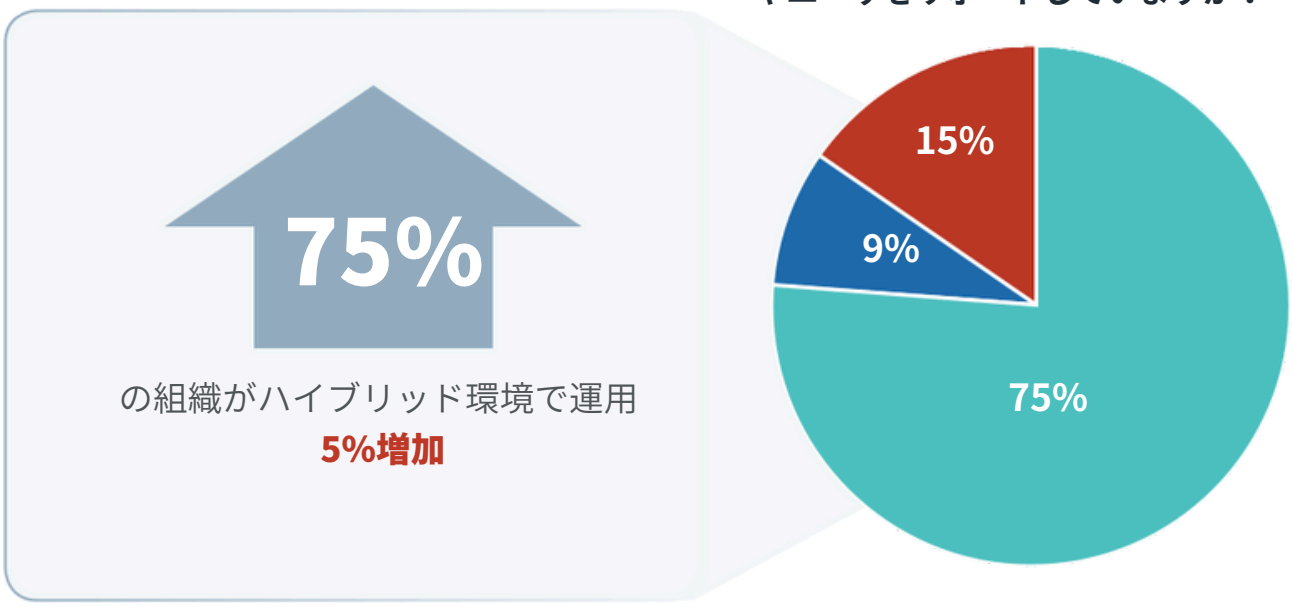
次のサイバーセキュリティ能力を、1から5のスケールで順位付けしてください。



運用環境

ほとんどの組織はハイブリッド環境で運用しており、クラウドとオンプレミスの両方のリソースを組み合わせて使用しています。企業は、すべてのユーザ、デバイス、権限、環境が十分に保護されていることを確実にする必要があります。

以下のどの環境で、アプリケーションやユーザをサポートしていますか？



パスワードとパスワードに関わるリスクは依然として存在

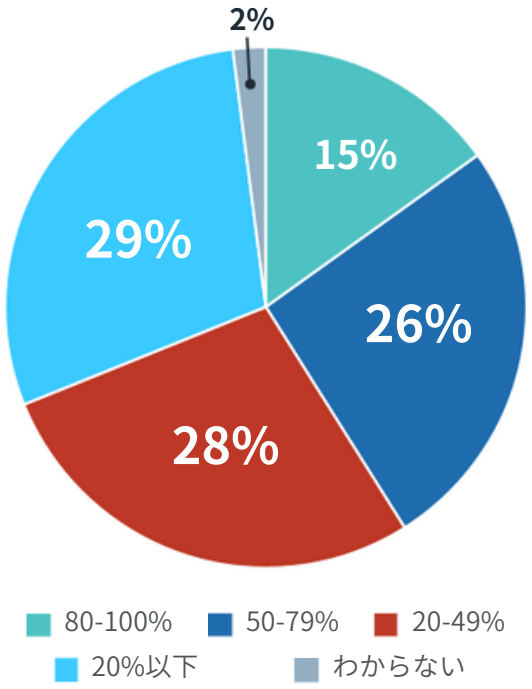
ほとんどの組織は、パスワードレスを主要な認証方法として使用していません。これはサイバー犯罪者にとって好都合です。年々、盗まれた認証情報の使用がデータ侵害の主な原因となっています。

複雑な環境や、混在するユースケースやユーザグループにより、組織が包括的なパスワードレス認証を導入することは困難です。パスワード認証の継続的な使用は、より頻繁で高コストなデータ侵害と相関しています。

オーストラリアの組織は、国別で最も低いパスワードレス導入率の一つを報告しており、50%の組織がまだ導入の最初の段階にあります。また、オーストラリアの組織は、国別で最も高いアイデンティティ関連データ侵害率（過去3年間で92%の組織が侵害を報告）、最も深刻な影響（47%が侵害による重大な被害を報告）、および最も大きな金銭的損失（44%が侵害による損失が1,000万ドル以上）を経験しています。

これに対し、日本はパスワードレスを主要な認証方法として使用している割合が最も高く、37%の組織が少なくとも80%の認証にパスワードレスを使用していると報告しています。日本はまた、アイデンティティ関連データ侵害の発生率が低く（56%の組織が侵害を報告）、影響も比較的軽微です。

主にパスワードレス方式で認証を行っている割合はどのくらいですか？



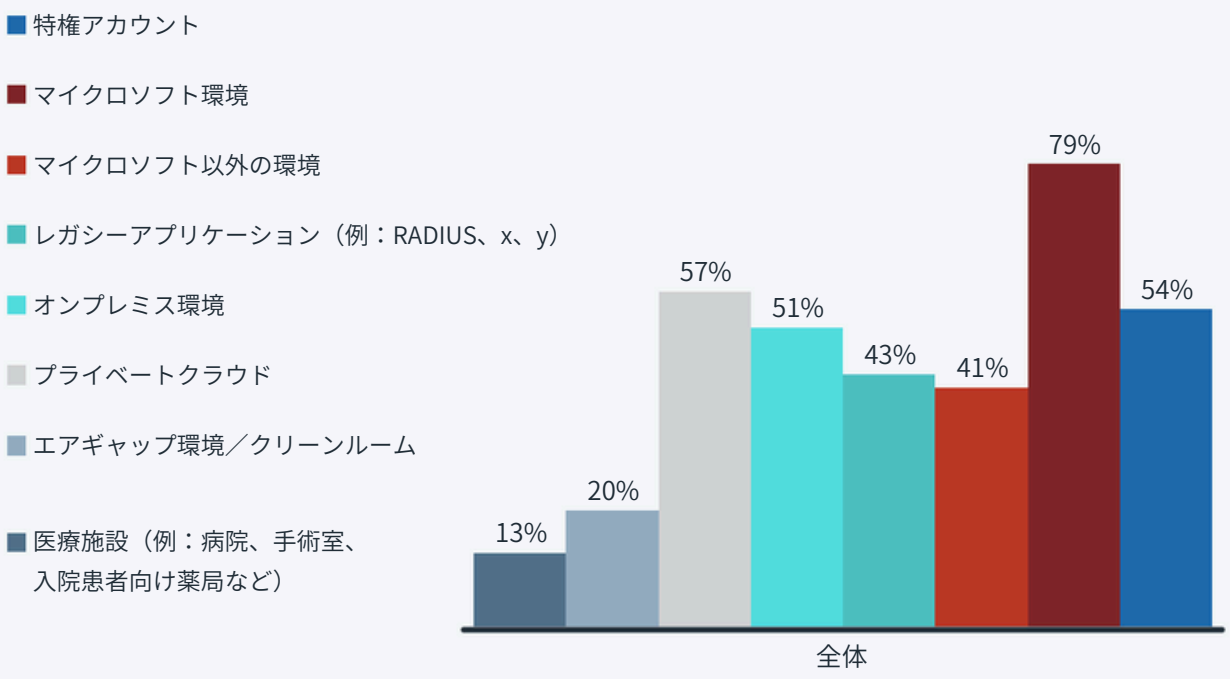
	オーストラリアの組織	日本の組織
国別のパスワードレス利用状況ランキング	#5	#1
パスワードレスを主要な認証方法として使用しているユーザの割合	10%	37%
報告された侵害件数	92%	56%
侵害が重大な被害（5段階中5）をもたらしたと報告した割合	47%	44%
1,000万ドル以上の損失が発生した侵害の割合	24%	28%

> “複雑な環境や多様な利用ケース、さまざまなユーザグループがあるため、組織が包括的なパスワードレス認証を導入することは難しい状況です。”

パスワードレスの普及を遅らせている要因は何ですか？

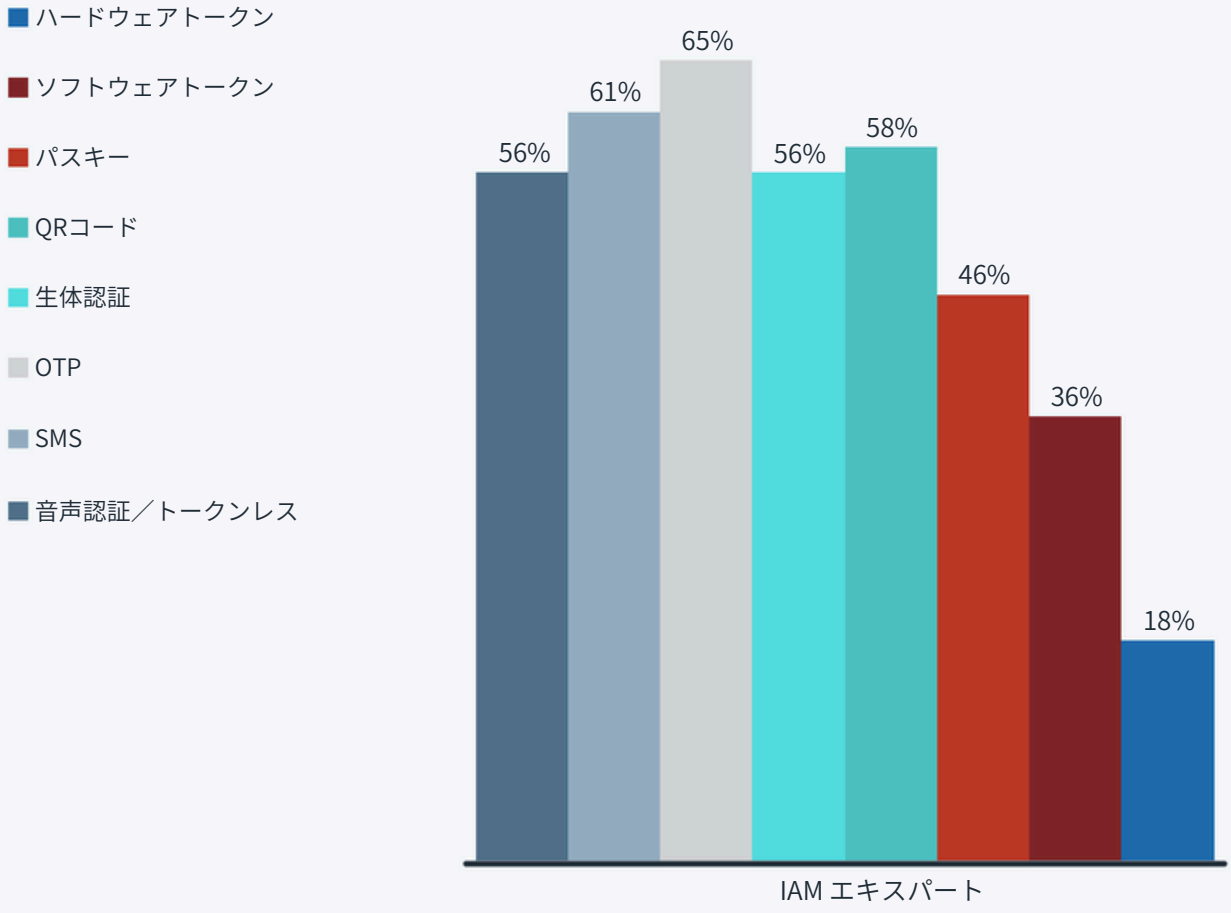
パスワードレスの導入にあたっては、多くの組織が幅広いユーザ層や利用ケースに対応する必要があります。私たちは、このことがパスワードレスの普及が進まない大きな課題となっていると考えています。

御社は、次のどの環境、ユーザグループ、またはユースケースをサポートしていますか？



ほとんどの組織がハイブリッド環境で運用され、さまざまなユーザやユースケースをサポートする必要があるため、アイデンティティの専門家たちは、すべてのユーザにパスワードレス認証を提供するために、多様なフォームファクター（認証手段）の活用を準備しています。

パスワードレスソリューションを導入するにあたり、次のうちどのフォームファクター（認証手段）を使用する予定ですか？



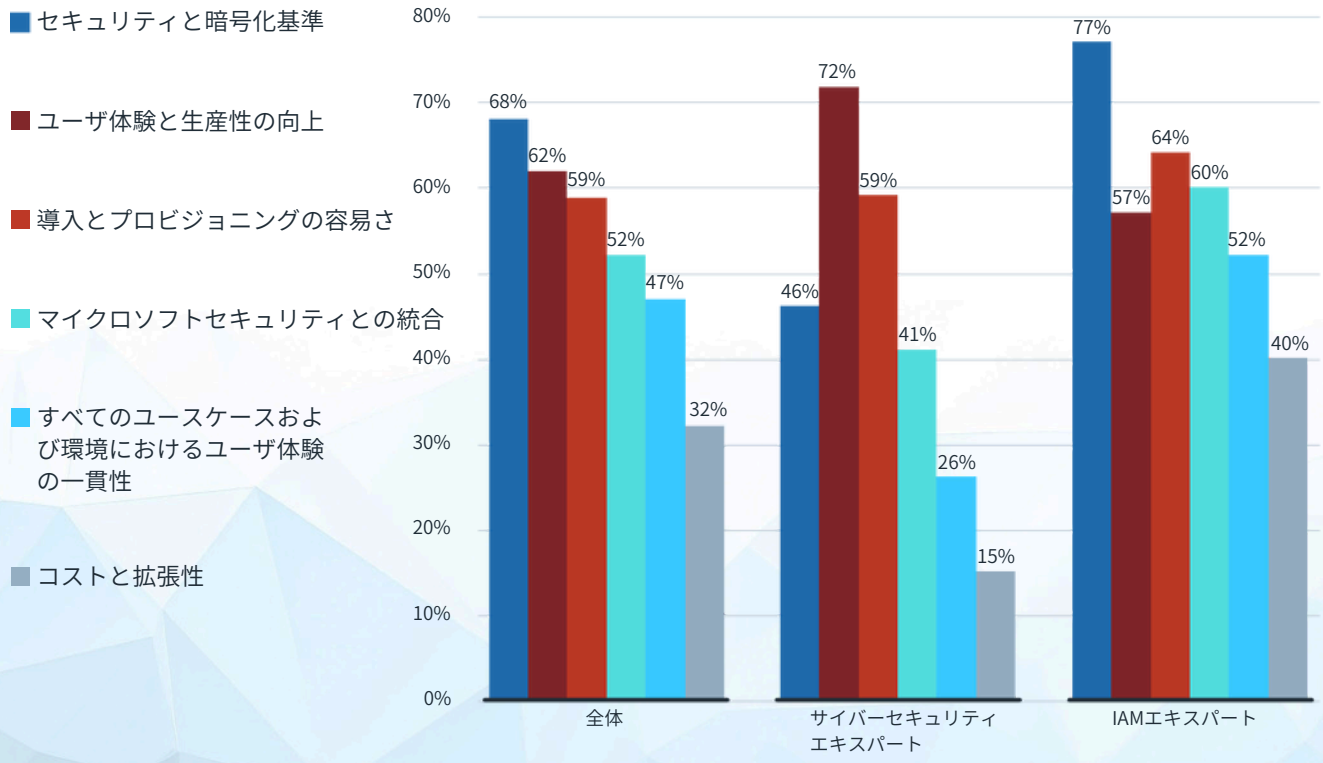
パスワードレスへの挑戦

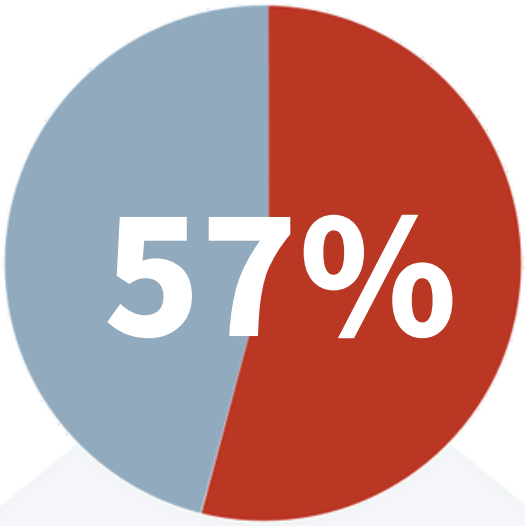
ほぼ全員（90%）の回答者が、パスワードレスソリューションの導入を遅らせる何らかの課題があると答えています。しかし、これらのユーザにとって、取り組むべき特定の課題は一つではありません。むしろ、三つの課題があります。57%の回答者はセキュリティ上の懸念がパスワードレスの導入を遅らせていると答え、56%はユーザ体験への懸念を挙げ、52%は完全なプラットフォームサポート（レガシーアプリやサードパーティシステムを含む）の不足がパスワードレスの展開を妨げる主な課題だと答えました。

これらはいずれも、組織がパスワードレスを効果的に導入するために克服すべき重要な課題です。興味深いことに、より実務的な制約はそれほど大きな問題ではなく、導入資金が不足していると答えたユーザはわずか47%でした。

組織が取り組むべき明確な課題は一つではありません。専門家ごとのパスワードレスの優先事項に対応し（そして導入を妨げる課題を克服するために）、企業はセキュリティと暗号化基準、UXの改善、使いやすさのバランスを取る必要があります。

パスワードレスソリューションを選定する際に、最も重要な要素は何ですか？





の組織は、パスワードレスを主要な認証手段として使用していません

新しい年でも、問題は変わらず

年々、パスワードはデータ侵害の主要な原因となっています：

2025 Verizon Data Breach Investigations Report: 資格情報の不正使用は「依然として最も一般的な攻撃経路」です。

2024 Verizon Data Breach Data Breach Investigations Report: 過去10年間で、盗まれた資格情報は侵害のほぼ3分の1（31%）に関与しています。

2023 Verizon Data Breach Investigations Report: 過去5年間で、盗まれた資格情報の使用が侵害の最も一般的な侵入経路となったため、資格情報の影響力は大きくなっています。

2022 Verizon Data Breach Investigations Report によると、過去15年間、毎年パスワードの不適切な管理は『データ侵害の主要な原因の一つ』となっています。

アイデンティティリスクの監視と管理

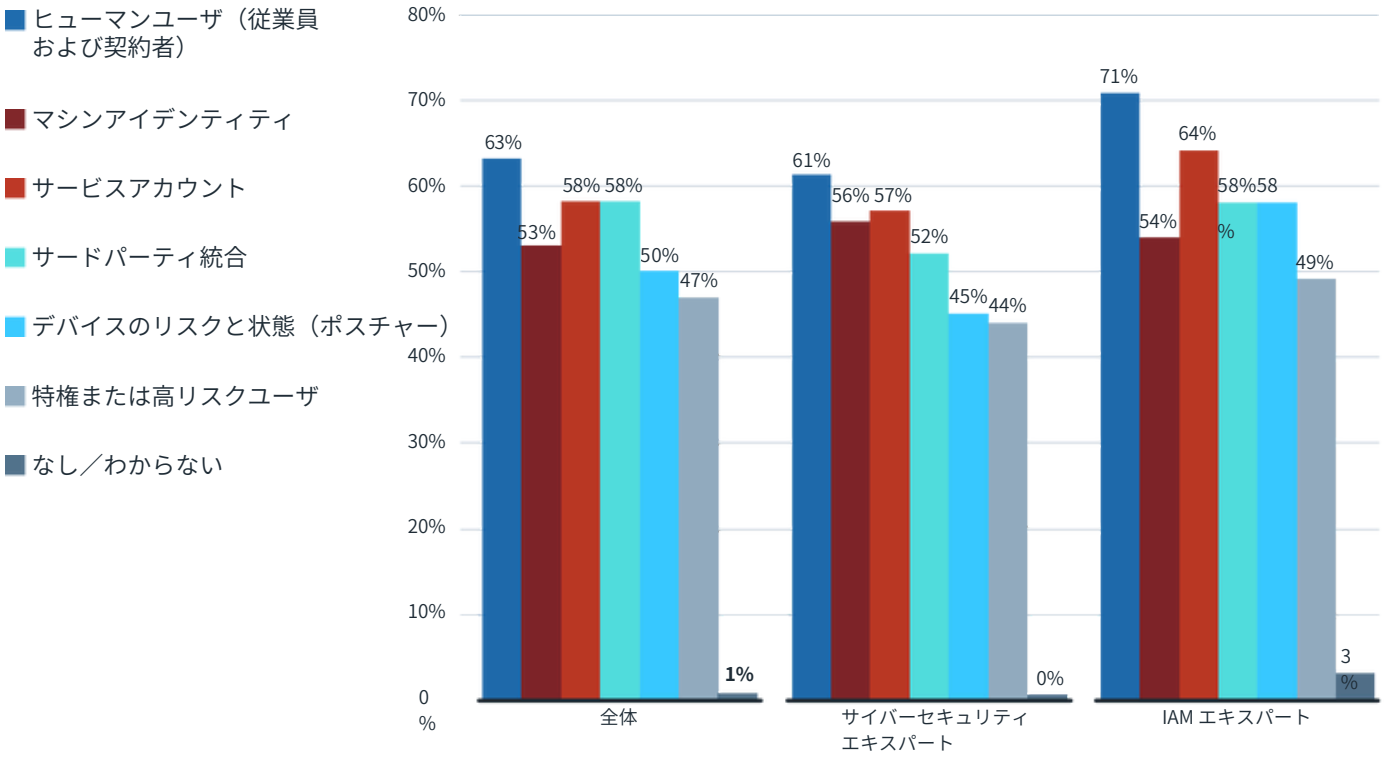
組織は、ユーザや種類ごとのアイデンティティリスクの監視率が高く、ほとんどの回答者がユーザ、マシンアカウント、サービスアカウント、サードパーティ統合を監視していると答え、半数はデバイスのリスクや状態（ポスチャー）も監視しているとしています。IAMの専門家は、サイバーセキュリティ担当者よりもこれらのアカウントのアイデンティティリスクを監視する傾向があります。

組織がアイデンティティ攻撃の範囲に対応していることは励みになります。しかし、この情報を統合し、効果的に活用することは課題となります。1アカウントあたり何千もの権限があるため、セキュリティチームはリスクを特定し、優先的に対応するために、多くのノイズを解析する必要があります。

この膨大なデータセットが、回答者のサイバーセキュリティ投資の優先順位に影響している可能性があります。回答者の4分の1以上（26%）が、ISPM（アイデンティティセキュリティポスチャ管理）を最優先事項として挙げています。ISPMは、組織がアクセスの露出状況を評価し、リスクを制限するための優先的な対応を決定するのに役立ちます。

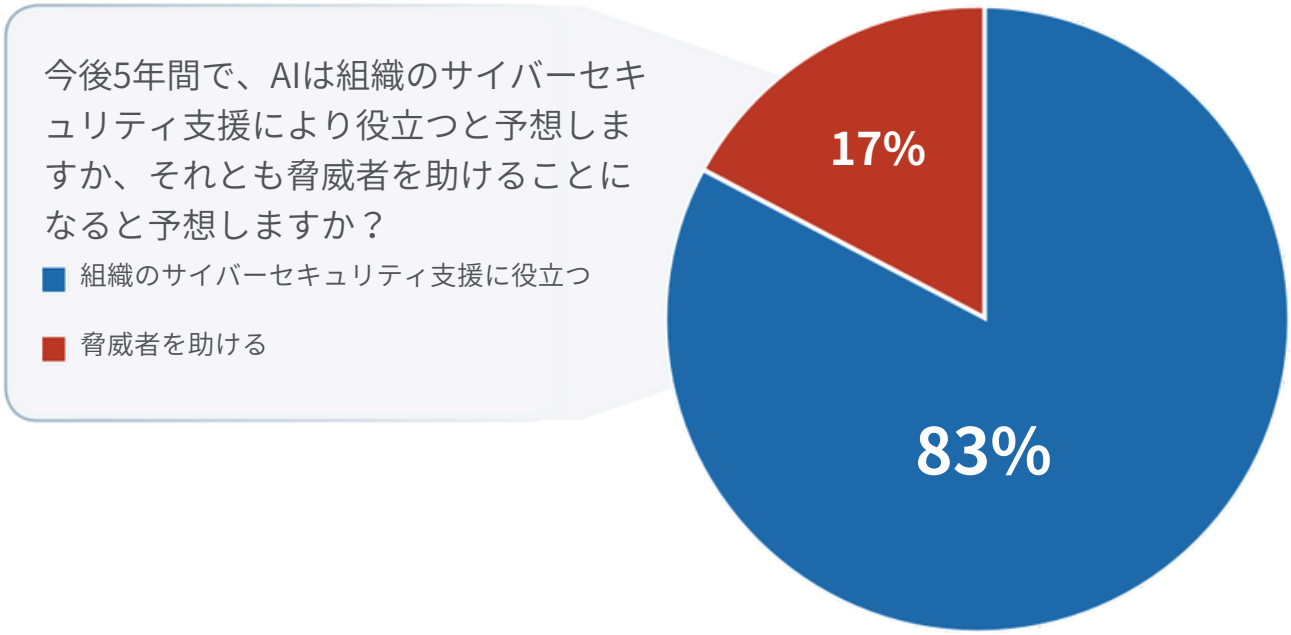
組織がノイズの中から重要な信号を見つけ、リスクを低減するためにISPMが必要な理由の一例が、マシンアイデンティティです。マシンアイデンティティを監視している組織は、最も頻繁に侵害を受け、影響や損失も最大でした。マシンアイデンティティを監視している組織のほぼ4分の3（72%）が、過去1年間にアイデンティティ関連の侵害を報告しています。これらの組織は、侵害による被害も最も大きく、34%が「重大な被害」を受けたと回答し、また最も壊滅的な損失では、27%が1,000万ドル以上の損失を報告しています。

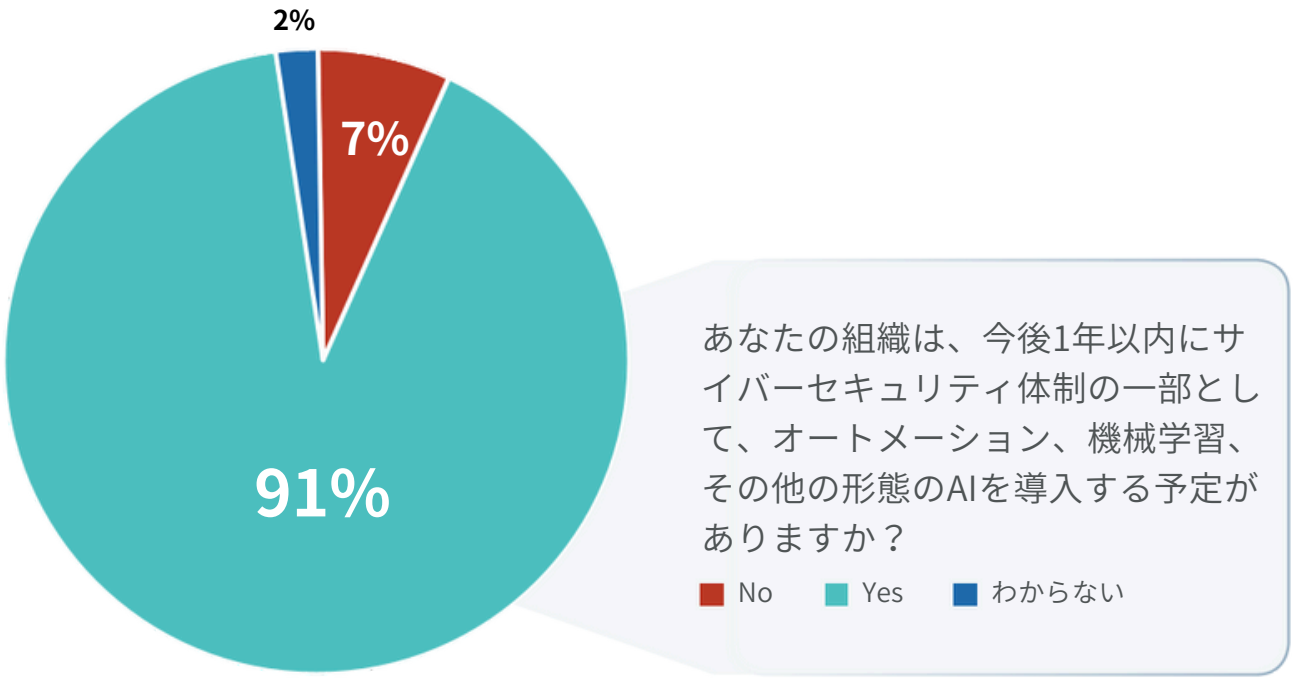
どの分野のアイデンティティリスクを積極的に監視またはスコアリングしていますか？



サイバーセキュリティ向けAI

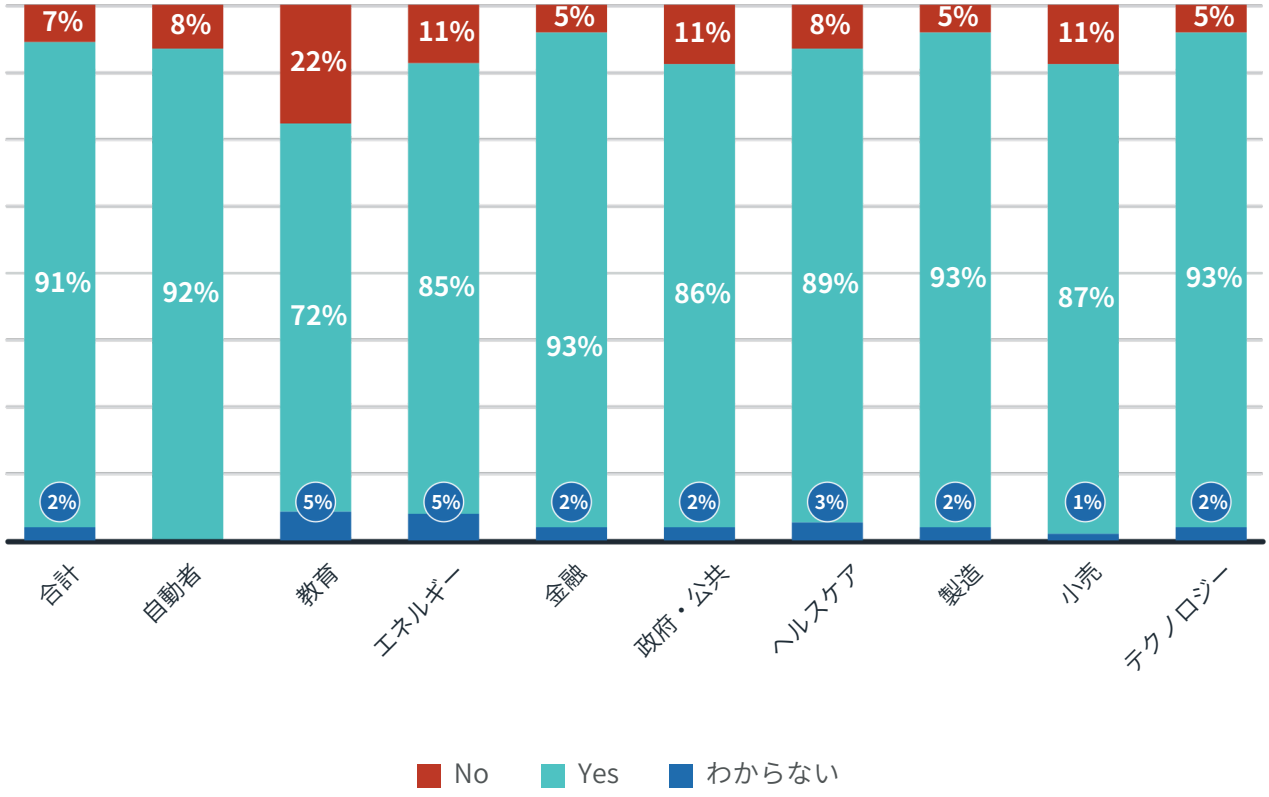
AIはサイバー犯罪を助長するよりも、セキュリティ支援に役立つという認識が高まっており、83%のユーザがこの技術は組織防御において敵対者よりも資産となると答えています。同様に、回答者の91%が今後1年以内に自社の技術スタックにAIを導入する予定であると答えており、これは昨年の調査から12ポイント増加しています。
これらの回答は、ユーザがサイバーセキュリティ機能の中で何を優先するかという点とも一致しています。回答者の40%が「セキュリティ向けの主体的AI（エージェント型AI）」を最優先の機能として挙げており、すべての機能の中で最多となっています。





業種別に見ると、ほぼすべての業界が今後1年以内に何らかの形でAIを自社のテクノロジースタックに導入する可能性が高いと報告しています。金融（93%）、製造（93%）、テクノロジー（93%）、自動車業界（92%）はいずれもAI統合の水準が高いと報告しました。一方で、教育業界（72%）はAI導入の水準が最も低い結果となりました。

業種別：あなたの組織は、今後1年以内にサイバーセキュリティ体制の一部として、オートメーション、機械学習、その他の形態のAIを導入する予定がありますか？



方法論とサンプル

RSAは、2025年7月20日から2025年8月15日にかけて「2026 RSA ID IQ調査」を実施しました。調査では、回答者に対し、サイバーセキュリティの優先事項、組織が直面しているリスク、ID関連のデータ侵害の発生頻度と影響、その他アイデンティティ分野に関する要因など、26の質問に回答するよう依頼しました。

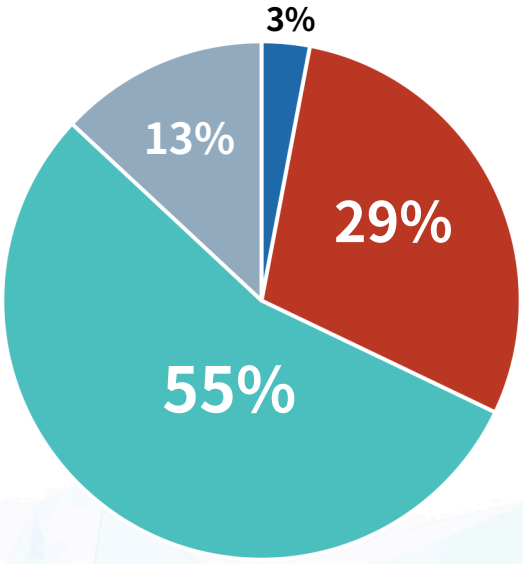
この期間中に、オーストラリア、ブラジル、カナダ、ドイツ、日本、イギリス、アメリカの合計2,120件の回答が寄せられました。

回答者には、自身の組織における役職、所属する業界分野、組織の規模を特定するよう求めました。

RSAはすべての回答を精査し、いくつかの回答間に相関関係があるかどうかを確認するため、回答同士の関連性を分析しました。

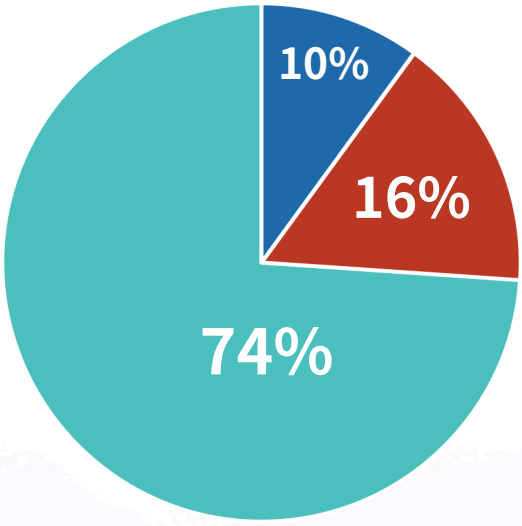
2026年 RSA ID IQ 調査の回答者属性

組織内での役職

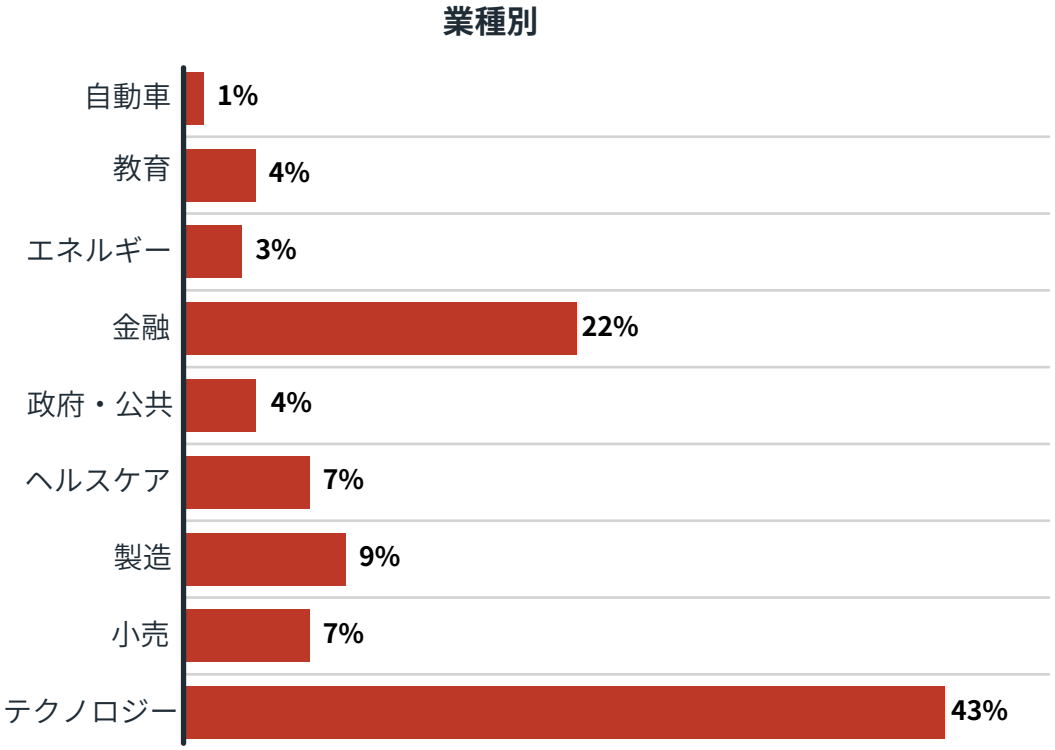


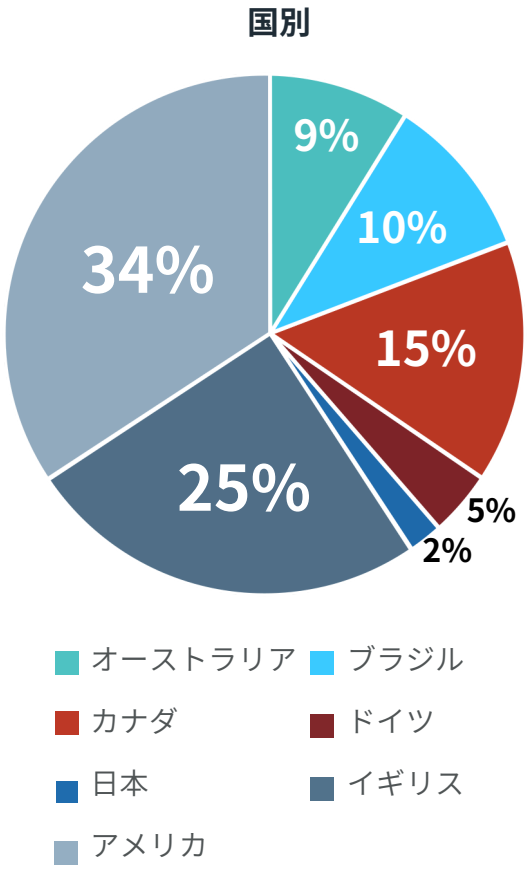
- コンプライアンス／リスク担当責任者
- サイバーセキュリティ専門家
- IT意思決定者／アーキテクト
- IAM／アイデンティティ専門家

組織の規模



- 2,500 - 4,999
- 5K - 9,999
- 10K+


業種別
自動車
1%
教育
4%
エネルギー
3%
金融
22%
政府・公共
4%
ヘルスケア
7%
製造
9%
小売
7%
テクノロジー
43%


国別
9%
10%
15%
5%
2%
25%
34%
オーストラリア
ブラジル
カナダ
ドイツ
日本
イギリス
アメリカ

2026年 RSA ID IQ レポート：
日本のハイライト

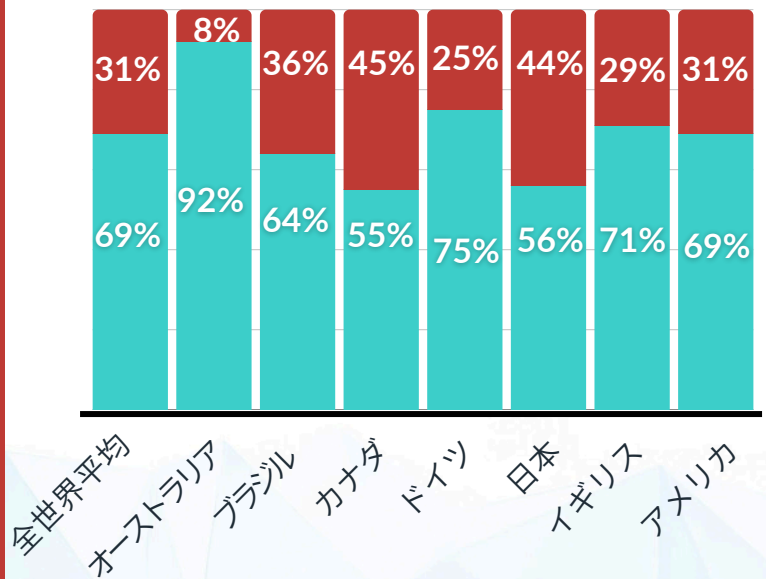
世界の他の地域と比べて、日本の回答者は最も複雑な技術環境に直面しており、フィッシングをグローバルの人たちよりもはるかに大きなリスクと捉えています。

以下は、2026年 RSA ID IQ レポートにおいて、日本が先行している分野、遅れをとっている分野、そして世界の他地域と比べてどのように異なるかを示したものです。これらのハイライトは、日本の回答者55名を対象としています。

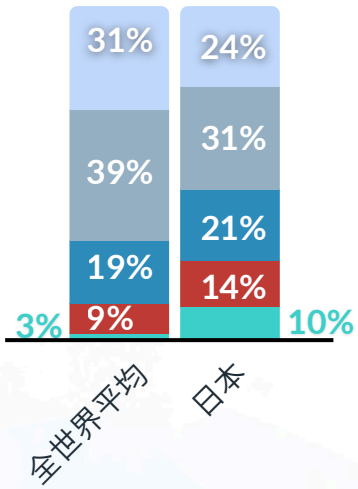
侵害件数が少なく、影響も小さい

過去3年間にアイデンティティ関連の侵害を経験したと回答した日本の回答者はわずか56%で、世界でも最も低い水準の一つです。同様に、日本の組織は、これらの侵害の深刻度が世界の他地域の組織ほど大きくなかったと報告しています。

過去3年間に、御社はアイデンティティ関連の侵害を経験しましたか？



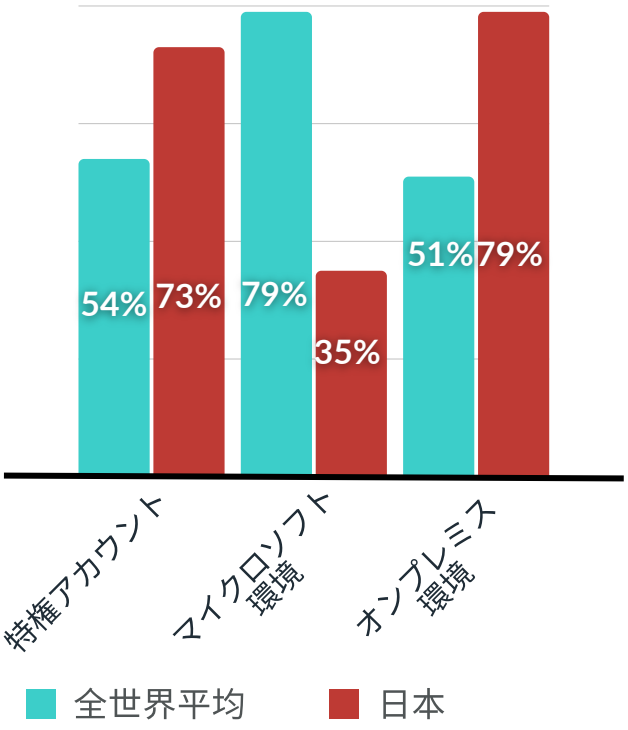
過去3年間にアイデンティティ関連の侵害を経験した場合、その影響の深刻度を1から5のスケールで順位付けしてください



世界で最も複雑な技術環境

日本では、複合環境の利用頻度が最も高いと報告されており、81%の組織がハイブリッド環境とオンプレミス環境の両方で運用していると回答しており、世界平均より6ポイント高くなっています。同様に、日本は最も独自性の高い技術環境を持つと報告されており、Microsoftのみの環境への依存が最も低く、オンプレミスシステムや特権アカウントの割合が最も高くなっています。

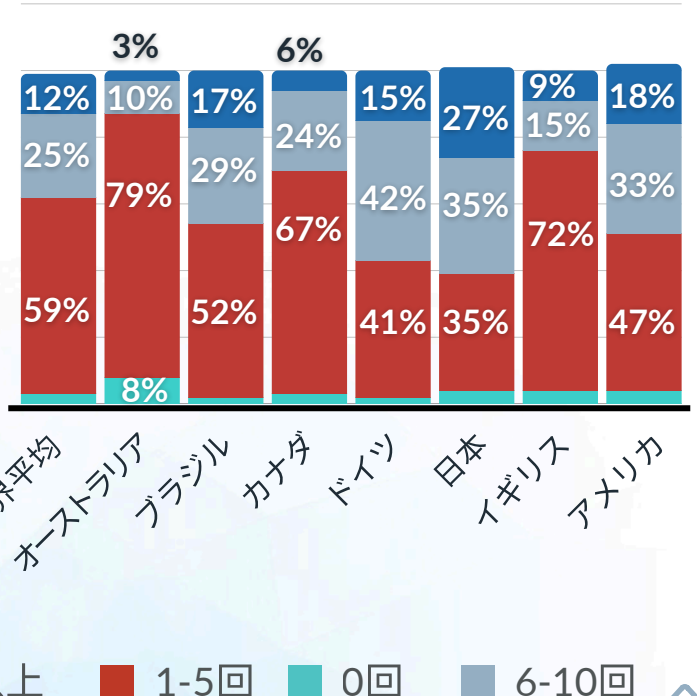
御社は次のどの環境、ユーザグループ、またはユースケースをサポートしていますか?



パスワードの負担

日本の組織では、ユーザが仕事でパスワードを入力する必要がある頻度が他国よりも高く、回答者の62%が1日に6回以上資格情報を入力する必要があると答えています。

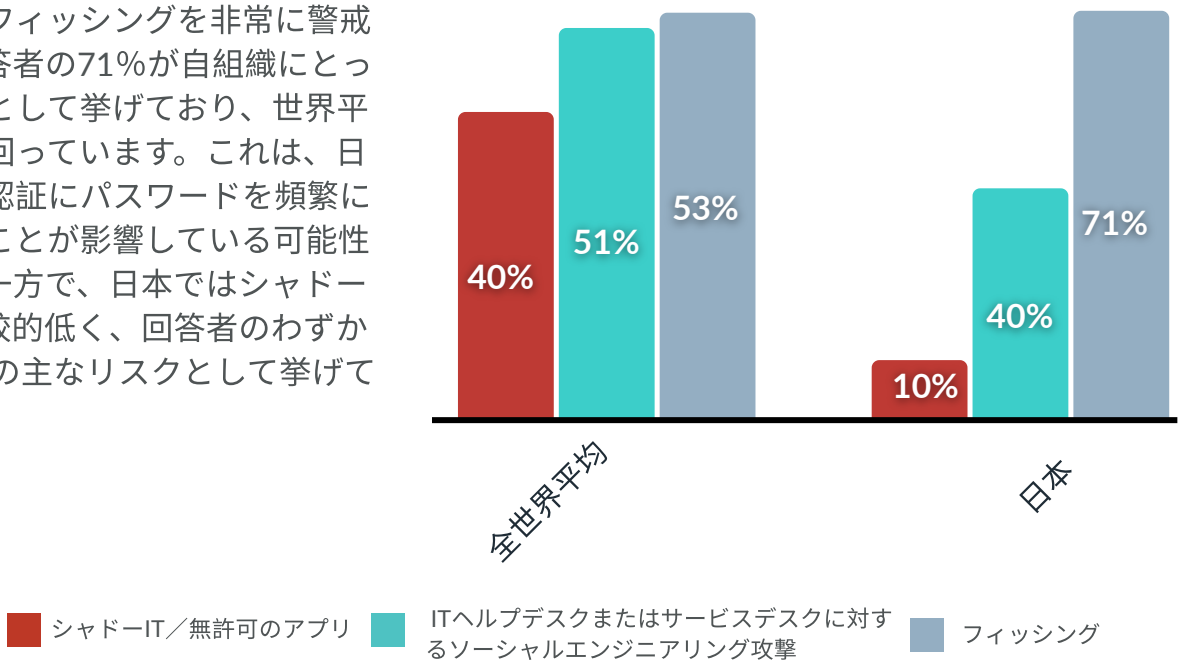
平均して、仕事で1日に何回パスワードを入力する必要がありますか?



フィッシングへの恐怖が大きい

日本の組織はフィッシングを非常に警戒しており、回答者の71%が自組織にとって最大の脅威として挙げており、世界平均を大きく上回っています。これは、日本のユーザが認証にパスワードを頻繁に使用していることが影響している可能性があります。一方で、日本ではシャドーITの懸念は比較的低く、回答者のわずか10%が自組織の主なリスクとして挙げています。

次のうち、御社にとって最も重大なサイバーセキュリティリスクとなるものはどれだと思いますか?



情報から行動へ

あらゆる問題を解決するための第一歩は、その問題が存在することを認めることです。「2026年 RSA ID IQレポート」は、多くの組織にとってアイデンティティが重大な課題であり、高コストかつ深刻な影響を及ぼすデータ侵害を引き起こしていることを示しています。

組織は、自身のセキュリティを維持するために以下の機能を優先的に導入すべきです：

- すべてのユーザ、すべての環境、すべての状況で機能するパスワードレス認証
- リスクを発見し、対応策を推奨するISPM（アイデンティティセキュリティポスチャーマネジメント）
- クラウド、ハイブリッド、オンプレミスのユーザを保護できるクロス環境対応
- ITヘルプデスクおよびユーザをMFAバイパス攻撃やソーシャルエンジニアリングから守る双方向のアイデンティティ検証
- リスクを動的に評価し、対応を自動化する自動化アイデンティティインテリジェンス

RSAへのお問い合わせからこれらの機能のデモのリクエストが可能です。 あるいは、世界で最も安全な組織がなぜRSAによって守られているのかをご覧ください：今すぐ **「RSA ID Plus」の45日間無料トライアル** を開始できます。

RSAについて

RSAは、世界で最もセキュリティに敏感な組織を保護する、ミッションクリティカルなサイバーセキュリティソリューションを提供しています。

RSA Unified Identity Platformは、真のパスワードレス・アイデンティティセキュリティ、リスクベースのアクセス制御、自動化されたアイデンティティインテリジェンス、クラウド・ハイブリッド・オンプレミス環境における包括的なアイデンティティガバナンスを提供します。

9,000以上の高いセキュリティが求められる組織が、6,000万以上のアイデンティティの管理、脅威の検出、アクセスの保護、コンプライアンスの実現のためにRSAを信頼しています。

詳細については、当社のウェブサイトをご覧いただき、**営業担当へのお問い合わせ**、**パートナーの検索**、または **RSAに関する詳しい情報** をご確認ください。