

2026

グローバル 認証状況調査

認識と現実のギャップ：
認証セキュリティの落とし穴

yubico



okta

目次

エグゼクティブサマリー	1
導入のギャップ	3
最新の認証方式に対する高い理解	4
デフォルト設定に縛られる現実	5
家庭から職場への波及	6
楽観バイアスとNHI（非人間ID）の脅威	7
コストと道理：AIフィッシングの急増	8
「わかりやすい」フィッシングの終焉	9
ディープフェイクと高い成功率	10
ボットを見抜けるか？－ 専門家でも判別は困難な結果に	11
エージェントの未来：NHI（非人間ID）の保護	12
検証の必須要件	13
業務の権限委任がセキュリティ管理を追い越す	14
ヒューマン・イン・ザ・ループの必要性	15
地域別分析	16
新たなセキュリティアーキテクチャの構築	18
結論	20
企業ステートメントおよび調査方法	22

エグゼクティブサマリー

長年にわたり、企業のセキュリティ戦略は「人を教育すれば、セキュリティはおのずと向上する」という根本的な前提のもとで運用されてきました。サイバーセキュリティのリーダーたちは、組織と個人の双方を守るために何が必要かを明確に理解しています。すなわち、多要素認証（MFA）を採用し、既存のセキュリティギャップをさらに広げかねないAIを活用した攻撃の脅威に備えることです。

それでもなお、セキュリティに関する知識が実践に結びつかず、組織が脆弱なままであることが少なくありません。「知っていること」と「実行すること」の間には、根強いギャップが存在します。

本レポートの調査結果は、このギャップが教育の問題ではなく、むしろ構造的な問題であることを示唆しています。ログインの手間と認証疲れによって、どれほど知識のある専門家であっても、職場や家庭にて、最終的には「最も手間の少ない方法」を選んでしまう傾向が一貫して見られます。この傾向は、個人アカウントから締め出されることへの懸念によって強められている可能性があり、その結果、人々は単純なパスワードや使い慣れたSMSによるMFAへと逆戻りしてしまいかねません。ユーザー名とパスワードのような安全でないデフォルトを乗り越えるには、極めて高いスキルを持つ専門家であっても、無意識の思い込みや運用上の見落としがあることを認識する必要があります。重要なことは、個人の行動を変えることではなく、その背景にあるインフラを変えることです。組織は旧来のデフォルトを排除し、それらをあらゆるシステムにわたって、利便性が高くフィッシング耐性を備えた認証へと置き換えなければなりません。

ここ数年、Yubicoは世界中の働く人々を対象に、スマートなサイバーセキュリティの習慣をどれだけ生活に取り入れているかを調査してきました。そして今年、Yubicoは新たなアプローチとしてOktaと連携し、9カ国、2,000人近くのサイバーセキュリティおよびITの専門家を対象に調査を実施しました。回答者はセキュリティ業務に日々従事している人たちです。アクセス管理やセキュリティポリシーの策定を担い、従来型のパスワードがいかに容易に攻撃によって破られてしまうかを誰よりも深く理解しています。

2,000

人近くのIT・セキュリティ専門家

9

カ国

パスワードと意識向上からの脱却

調査結果からは、新たなセキュリティアーキテクチャを構築することで、組織がサイバーセキュリティ対策を刷新する大きな機会があることが明らかになりました。安全な認証方式に関する専門知識と認知度はかつてないほど高まっている一方で、セキュリティ専門家でさえ、入社時のオンボーディングで提供された旧来のパスワード認証の仕組みにいまだに依存しています。そして、企業がパスワードを前提とした運用を続ける限り、従業員もまたその利用を続けることになります。

フィッシング対策において、不正なWebページを示す微妙な異常を従業員の目視で見抜くことには限界があります。先進的なセキュリティチームは、フィッシング耐性のある認証こそが究極の防御策であり、真偽の判断を人間の目に頼る必要がなくなるものだと認識しています。その代わりに、最新の認証方式は、アクセスの瞬間に暗号学的に署名されたノンス（nonce）の交換とドメイン検証を行うことで本人確認を実施します。これにより、たとえ従業員がフィッシングのわなにかかっても、認証は自動的に失敗し、攻撃は完全に阻止されるのです。

結論から言えば、安全な企業環境の実現におけるボトルネックは、セキュリティ意識や知識不足ではありません。真の課題は、認証の前後を含めたアイデンティティ保護を十分に考慮していない、運用上の摩擦や時代遅れのデフォルト運用にあります。このギャップを埋めるには、教育にとどまらず、人間と機械の双方を含むあらゆるIDに対して、ハードウェアベースでフィッシング耐性のある認証の利用を徹底する必要があります。

yubico



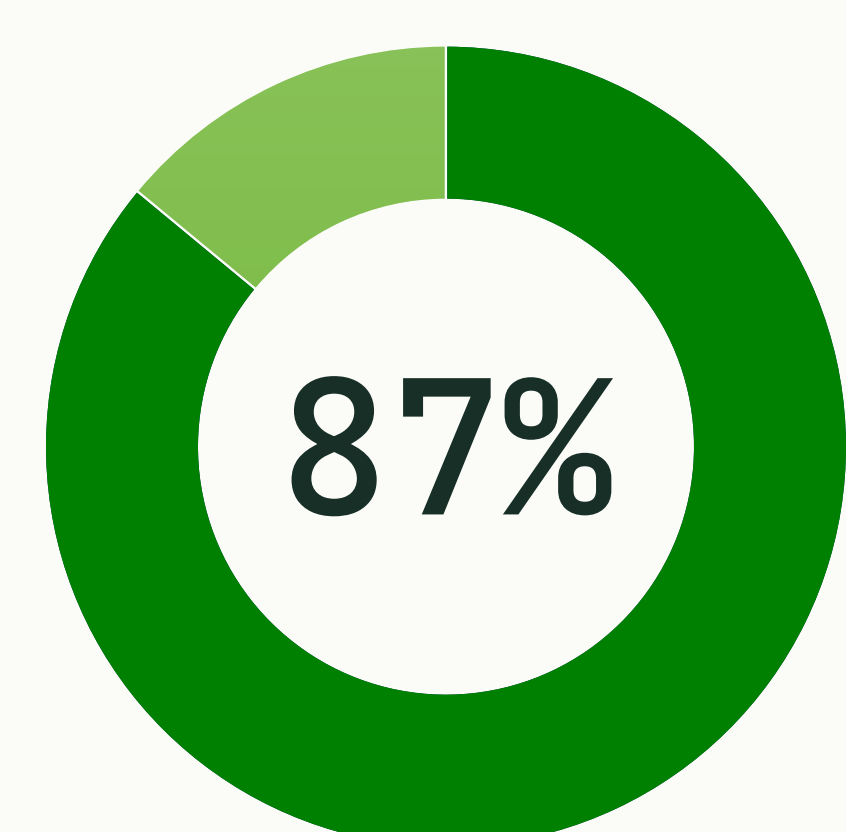
導入のギャップ



最新の認証方式に対する高い理解

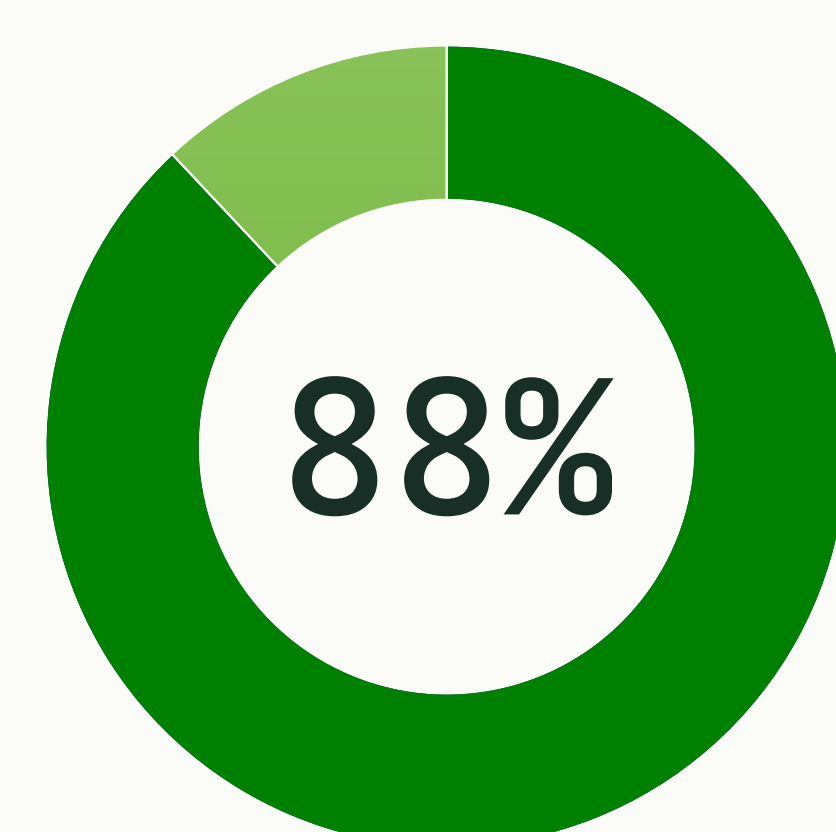
企業のセキュリティチームは深い専門知識を有しています。アクセス制御を評価するよう求められると、彼らはハードウェアベースのデバイスバインド型のパスキーを最も安全（31%）と評価し、モバイル認証アプリ（29%）や同期型パスキー（27%）を上回りました。

数字が示すとおり、その認知度の高さは疑いようがありません。87%がパスキーを認知し、82%が勤務先からセキュリティトレーニングを受けており、パスキーを一度も使ったことがない人はわずか3%です。理論上は、これらの専門家は、企業、従業員、そして顧客をサイバー脅威から守るうえで、どのツールが最も安全かを見極めるエキスパートと言えます。



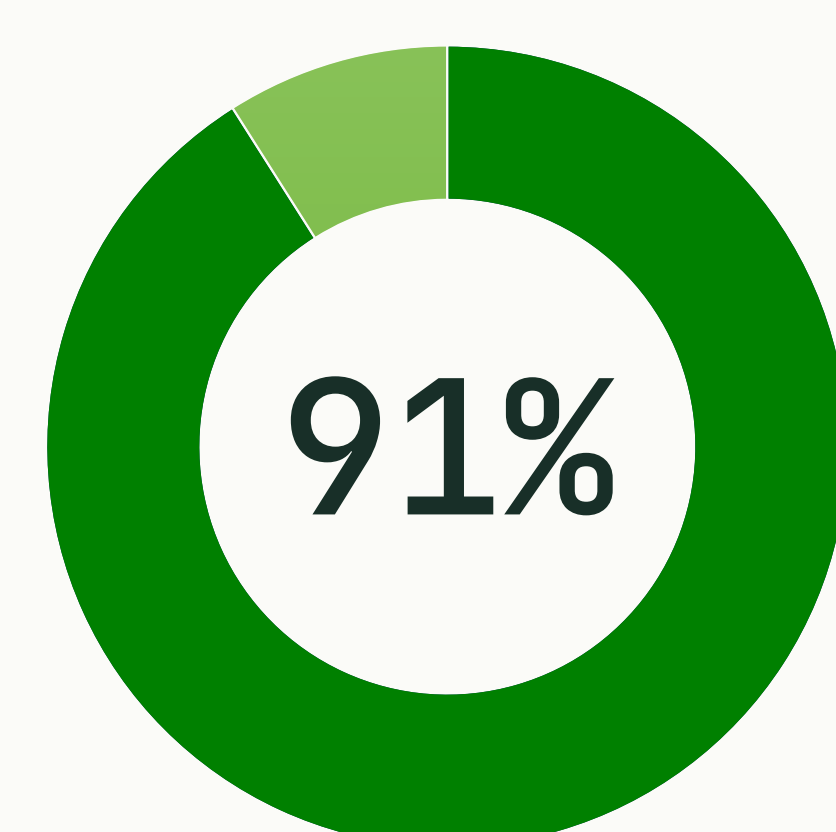
高い認知度

セキュリティ専門家の87%がパスキーを認知しており、31%はハードウェアベースのデバイスバインド型パスキーを、利用可能な認証情報の中で最も安全なものだと明確に認識しています。



積極的なセキュリティ文化

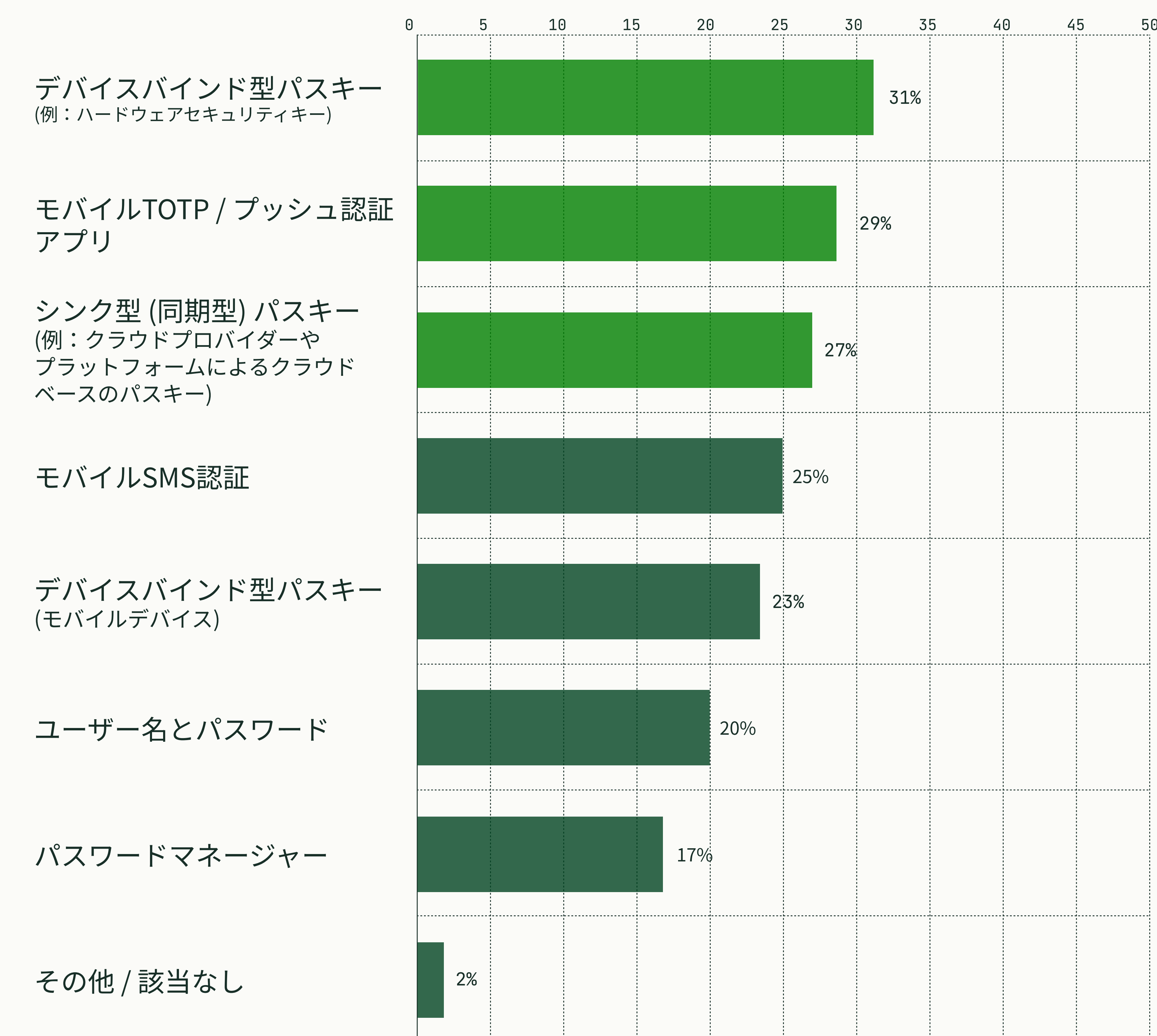
セキュリティリーダーの88%が自組織の現在のセキュリティ体制に自信を示しており、ツールやインフラ、人材育成への継続的な投資の成果が反映されています。



AI時代への備え

リーダーの91%がAIエージェントを認証することの重要性を認識しており、非人間ID（NHI：Non-Human Identity）についても先を見据えた準備ができていることを示しています。

あなたの考えでは、最も安全な認証方法は何だと思いますか？



デフォルト設定に縛られる現実

専門知識があるにもかかわらず、日々の認証行動は技術職ではない従業員とほとんど変わりません。ユーザー名とパスワードは、セキュリティ専門家が業務アカウントにログインする際の最も一般的な方法（43%）であり続けている一方、ハードウェアベースのパスキーは実際の日常的な利用率で最も使われていない方式の一つ（25%）にとどまっています。

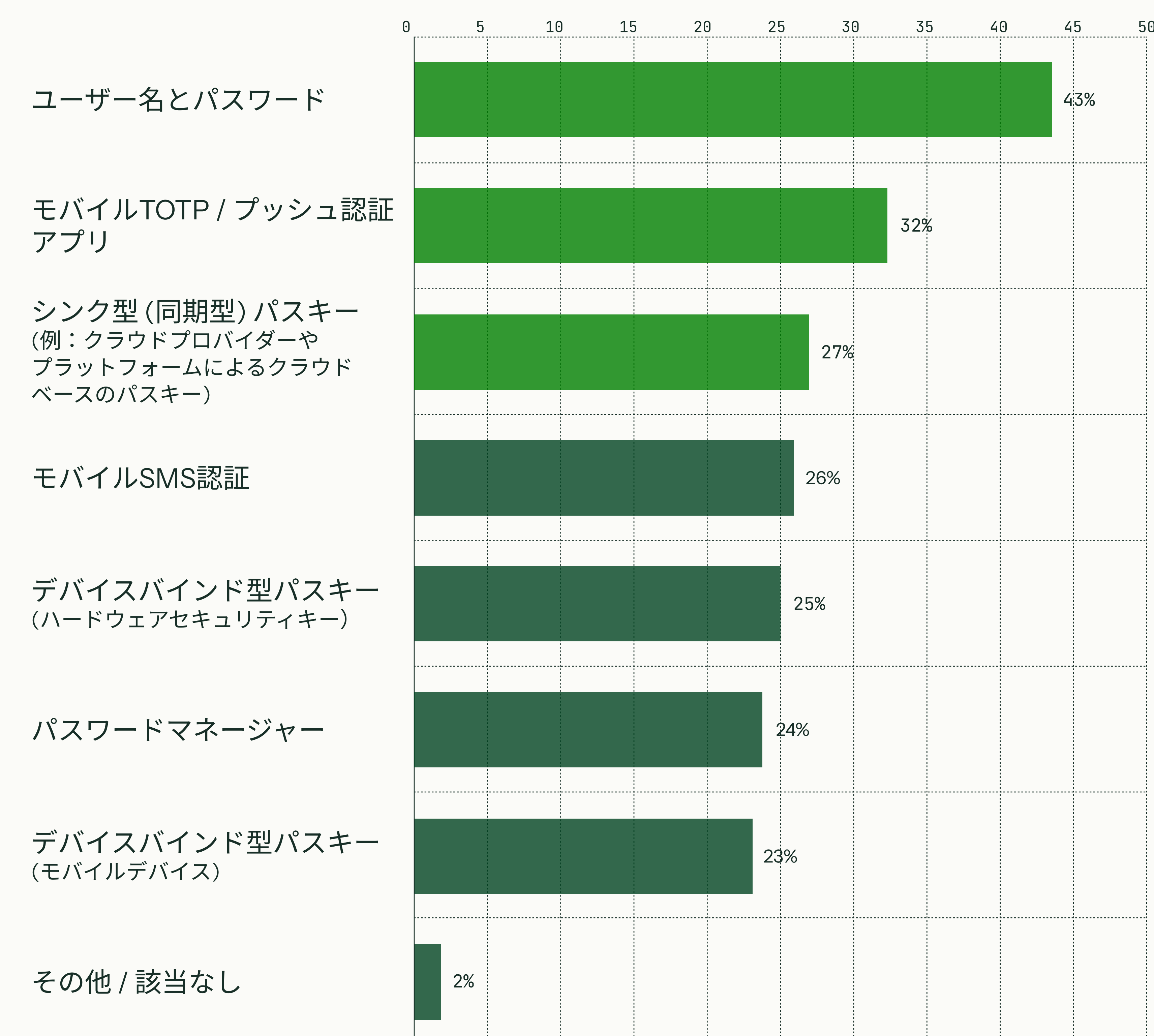
本調査からは、長年にわたる職場の習慣が、着任初日のデフォルト設定に起因している場合が多いことが明らかになりました。回答者の半数超（52%）が、着任時に従来型のユーザー名・パスワードによる認証情報を付与されており、それが、その後も続く旧来のログイン習慣の定着につながっています。

運用上の分断がリスクをさらに深めています。

- 76%の組織が、社内の異なるアプリケーション間で分断化した認証方式を使用しています。
- 45%が、分断化したシステム全体の主要な認証情報としてユーザー名とパスワードに依存しています。
- 23%の組織では、すべての業務アプリケーションおよびサービスで多要素認証（MFA）を義務付けていません。

これらのデフォルト設定が存在する状況は、職場と家庭とで異なります。職場では、オンボーディング時のデフォルト設定やアカウントから締め出される可能性があっても、アクセスを復旧するITヘルプデスクが後ろ盾となっています。一方、家庭では、個人が自分自身でセキュリティを管理するしかありません。

業務アカウントへの認証・ログイン方法はどのようなものですか？

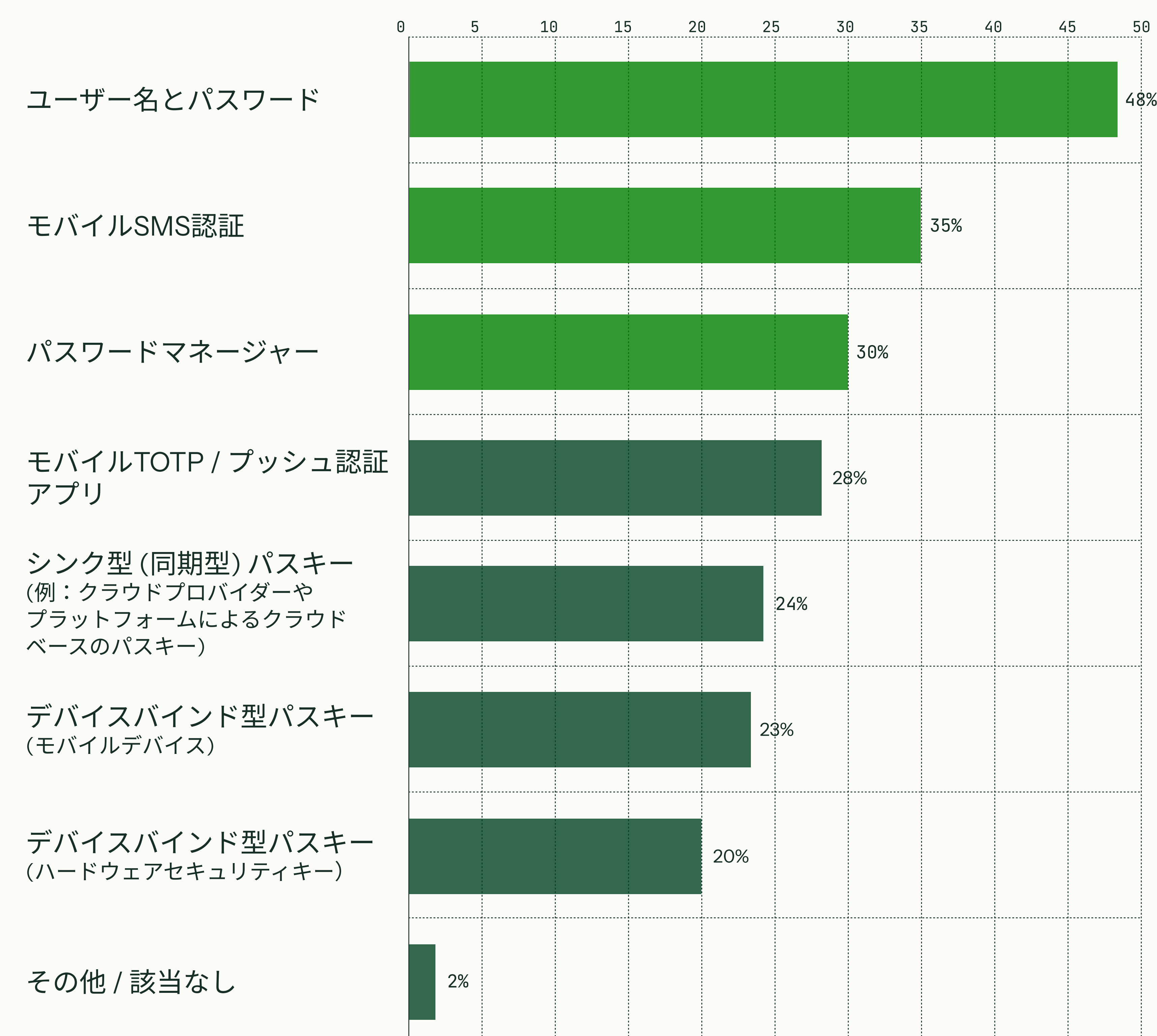


家庭から職場への波及

人には楽な道を選ぼうとする性質があります。そのため、認証のデフォルト設定から抜け出し、頻繁なセキュリティ確認から生じる認証疲れを克服するには、職場でも家庭でも意識的な努力が必要です。そう考えると、サイバーセキュリティ専門家であっても、個人利用においては**48%**が主にユーザー名とパスワードに依存し、次いでSMSベースの認証 (**35%**) が続くのも、意外ではないかもしれません。個人アカウントにハードウェアベースのパスキーを使っている人はわずか**20%**にとどまっています。

さらに、**28%**が個人のメールを多要素認証 (MFA) で保護していないため、攻撃者は容易な侵入口を得ています。加えて、**38%**が携帯電話番号と連携した個人メールアカウントを利用しており、これがSIMスワップ攻撃の起点となる可能性があります。そのデータが手に入ることで、攻撃者は電話ベースのリカバリーコードを乗っ取り、そこから連携する企業の認証情報へと直接侵入できます。その結果、個人のIDと企業の認証情報の双方が危険にさらされることになります。

個人用のアカウントには、どのような方法でログインしていますか？



楽観バイアスとNHI (非人間ID) の脅威

こうした脆弱性があるにもかかわらず、回答者の88%は自社のセキュリティ状態を「安全である」と評価しており、そのうち34%は「非常に安全である」と回答しています。

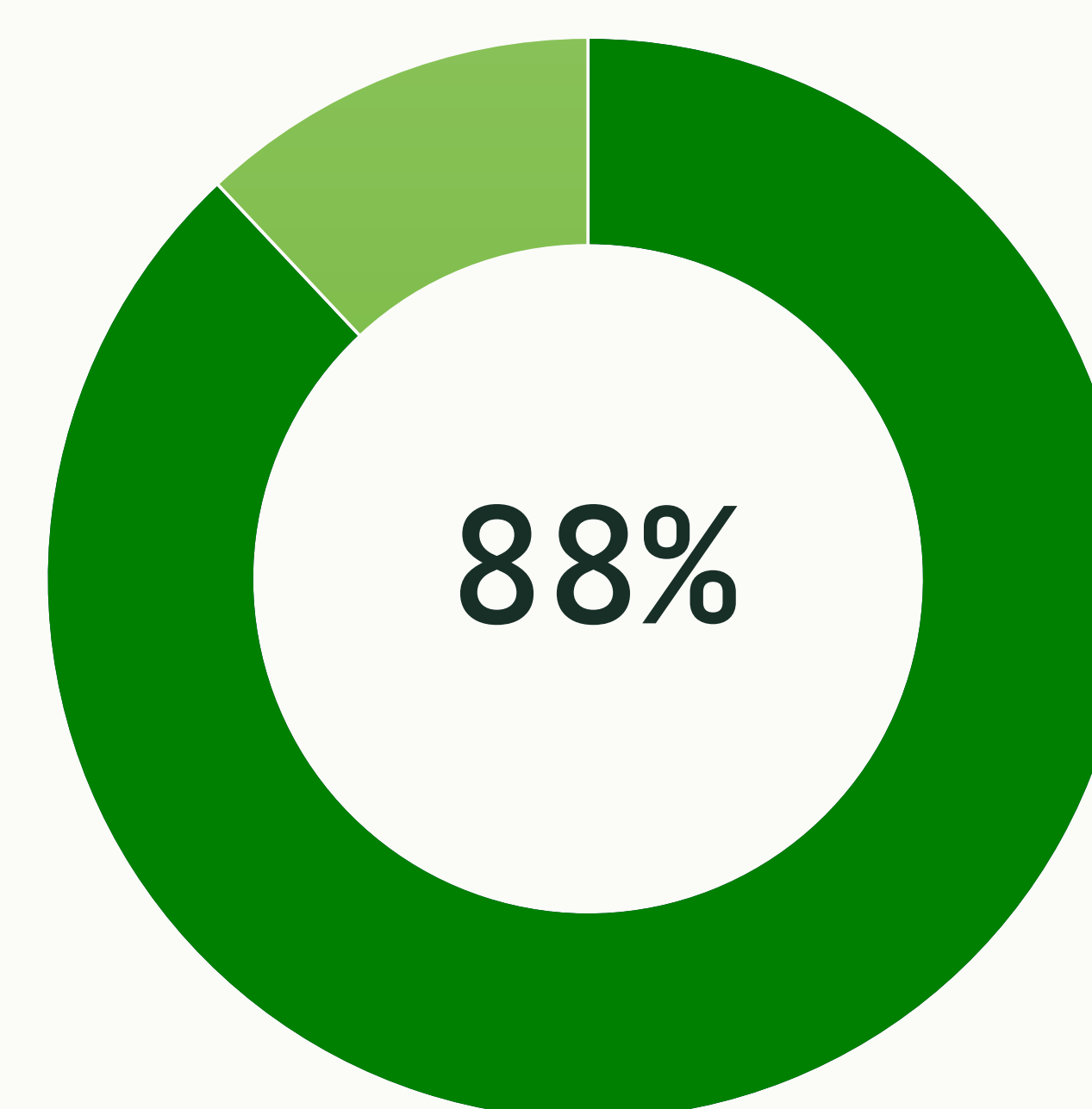
行動心理学では、これは**楽観バイアス**として知られています。専門知識があれば個人や組織が悪い結果を免れるはずだ、という思い込みです。セキュリティリーダーは自らの体制を甘めに評価する一方で、競合他社の方がリスクは大きいと想定しがちです。

企業が自律型AIソフトウェアエージェントを日常の業務フローに組み込むにつれ、パスワードで保護されたアカウントは、まもなく非人間のヘルパーであるAIエージェントによってアクセスされるようになります。人間の従業員に対して強力な認証を徹底できない組織は、自律型エージェントを安全に統制することもできません。

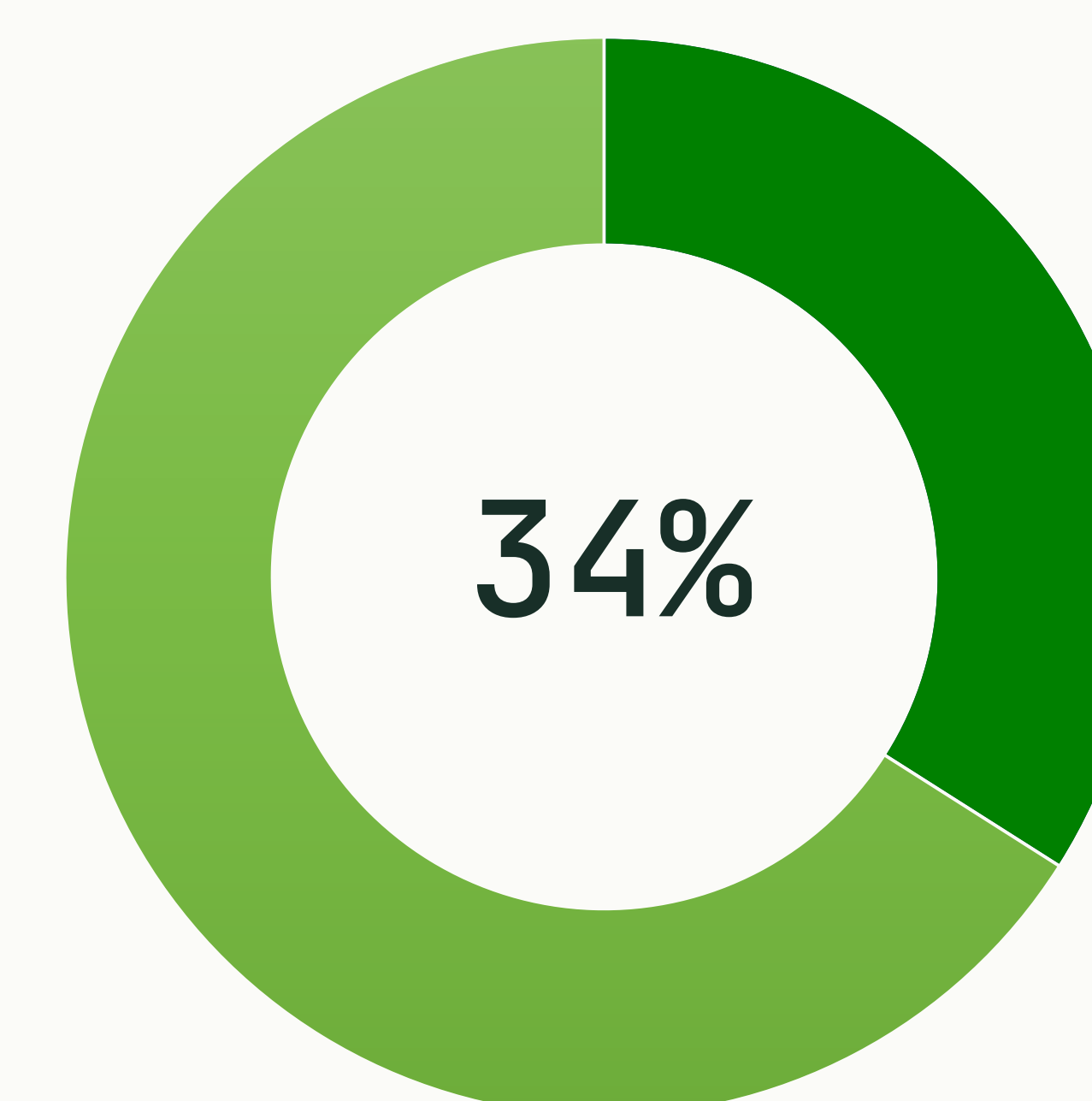
「**企業のサイバーセキュリティには、実行面で重大なギャップがあります。セキュリティリーダーは、パスワード、とりわけハードウェアセキュリティキーが最高レベルの保護を提供することを理解しています。それにもかかわらず、いまだに半数近くが日常的な認証手段としてユーザー名とパスワードに依存しているのです。ギャップがあるのは専門知識ではなく、時代遅れの企業ポリシーなのです。**

ブーパク・エンボム、
最高マーケティング・事業開発責任者

運用面のギャップがリスクをさらに深刻化



88%が、自社を「安全」であると回答しています。



34%が「非常に安全」と回答

AIフィッシングの 急増



「わかりやすい」フィッシングの終焉

生成AIがデジタルコミュニケーションを加速させ、よりカスタマイズされたものにするにつれ、業界全体でAIを活用したフィッシング攻撃も自然と増加しています。回答者の70%が過去1年間に組織へのフィッシングの増加を指摘し、55%はパーソナライズされた攻撃を直接受けたと回答しました。22%に至っては、直近1週間以内に標的型のメッセージを受け取っています。

以前はタイプミスや不自然な言い回しでフィッシングWebページを見分けられましたが、そうした従来のやり方はもはや通用しません。先を見据えたセキュリティチームは、人間による目視ではなく、フィッシング耐性のある認証こそが決定的な防御策だと認識しています。言い換えれば、AIベースの脅威を特定し阻止する責任を、人間が負うべきではないということです。その代わりに、最も革新的な認証手法では、ドメイン検証と暗号技術に基づくセキュリティを通じて、認証の瞬間に安全を確保できます。これにより、たとえユーザーが気づかないままフィッシングの被害に遭ったとしても、認証技術がログインを検知してブロックできるのです。



ディープフェイクと高い成功率

現代の攻撃は従来の認知フィルターをすり抜けるため、初期侵害の成功率は急増しています。回答者の44%が、過去12カ月間にAIを活用した攻撃が少なくとも1件成功し、自組織に被害が生じたと報告しています。

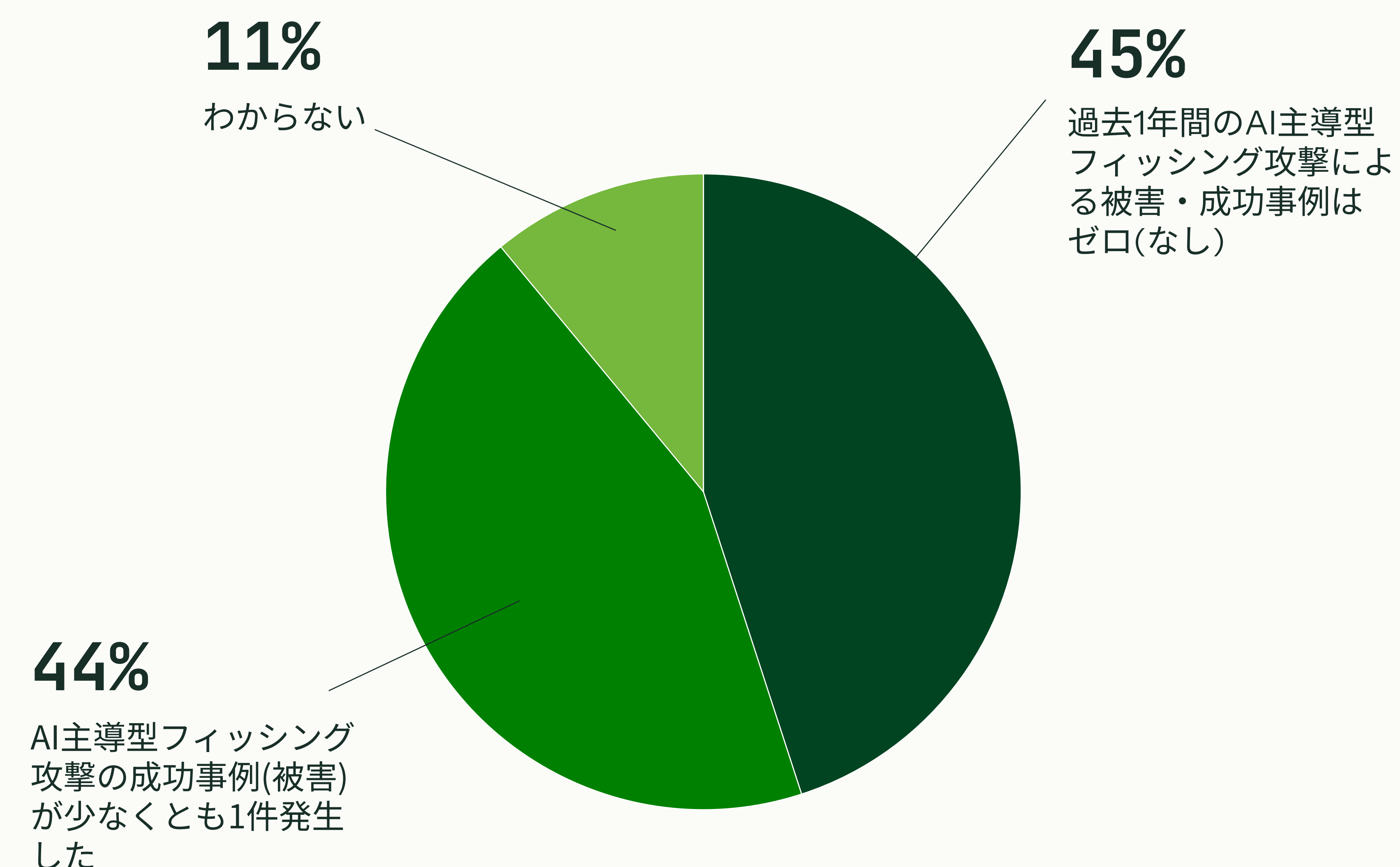
音声クローンや合成メディアにより、悪意ある攻撃者はごくわずかな素材から信頼された同僚になりすませるようになっています。

- 43%が、経営幹部や顧客を標的とした不審な動画・ボイスメモ・電話でのなりすましを報告しています。
- 29%が、ディープフェイクによるコミュニケーションで直接標的にされました。

Oktaの調査レポート「2026 AI Agents at Work」は、同じ組織へのもう一つの侵入経路について説明しています。調査対象となったナレッジワーカー(知識労働者)の半数超(52%)が、職場で認可されていないAIツールを使用していると回答し、4分の1近くが日常的に使用していました。未承認のツールを使う人々の間で最も多く共有されていた情報は、社内メッセージやメール(54%)、人事関連情報(45%)、そして財務や契約を含む機密の社内文書(39%)でした。



過去1年間における、貴社(貴組織)でのAI主導型フィッシング攻撃の成功状況について、次の記述のうち当てはまるものはどれですか？



ボットを見抜けるか？（専門家でも判別は困難な結果に）

組織は長年、異常を見抜く「人間のファイアウォール」として従業員に頼ってきました。この防御力を検証するため、私たちはセキュリティリーダーに2つのメッセージ（1つは人間が書いたもの、もう1つはAIが生成したもの）を提示し、その作成者を識別できるかをテストしました。

その結果、**人間による識別はもはや有効なセキュリティ対策ではないこと**が明らかになりました。

- ・人間が書いたメッセージを正しく見分けられたセキュリティ専門家はわずか36%で、54%はAIがそのメッセージを書いたと考え、10%は判断がつきませんでした。
- ・また、回答者の39%は、AIが生成したメッセージを見抜くこともできませんでした。

人間が書いたメール

[名前] 様

2027年に向けた改定に伴い、従業員ハンドブック（就業規則）が更新されました。複数の項目が新たに追加されています。更新された文書の全文をご確認のうえ、2026年11月1日までに受領確認（同意手続き）を行ってください。

【対応要請 - 期限: 2026年11月1日】
社内イントラネットにログインし、「To Do (対応事項)」欄の案内をご確認ください。本ハンドブックを含むすべての規約・ポリシーは、社内ポータルトップページから閲覧いただけます。

コンプライアンス維持へのご協力に心より感謝申し上げます。

敬具
人事チームより

AIが生成したメール

[氏名] 様

今後の会社の成長と展望を見据え、2027年に向けた従業員ハンドブック（就業規則）の改定を行いました。皆様と成長するチームを引き続き最適な形でサポートできるよう、いくつか重要な新セクションを追加しております。

今回の改定に伴い、全従業員の皆様に更新文書をご確認いただき、承認手続きを行っていただく必要がございます。

【2026年11月1日までの対応事項】
1. 社内イントラネットにログインする
2. トップページの「To Do (対応事項)」欄を確認する
3. 更新されたハンドブックの内容を確認し、受領確認ボタンをクリックする

＊本ハンドブックをはじめとする社内規約・ポリシー類は、いつでも確認できるようイントラネットのトップページに固定されています。

業務をスムーズに進行し、法令遵守を推進するためにご協力いただき、誠にありがとうございます。

敬具
人事チームより

エージェントの 未来：NHI (非人間 ID) の保護



検証の必須要件

自律型AIエージェントが受動的なアシスタントから能動的な業務ツールへと移行するにつれ、マシンIDの検証は最優先事項となっています。回答者の91%がAIエージェントの本人性 (Identity) と真正性 (Authenticity) を検証することが不可欠だと述べ、57%はそれを極めて重要だと評価しています。

Oktaの調査レポート「2026 Businesses at Work」によると、74%の組織が非人間IDを広範または中程度に利用していると報告する一方、90%がそれらを統制する包括的な戦略を欠いており、AIエージェントを人間のIDと同等の厳格さで統制している組織はわずか32%にとどまります。



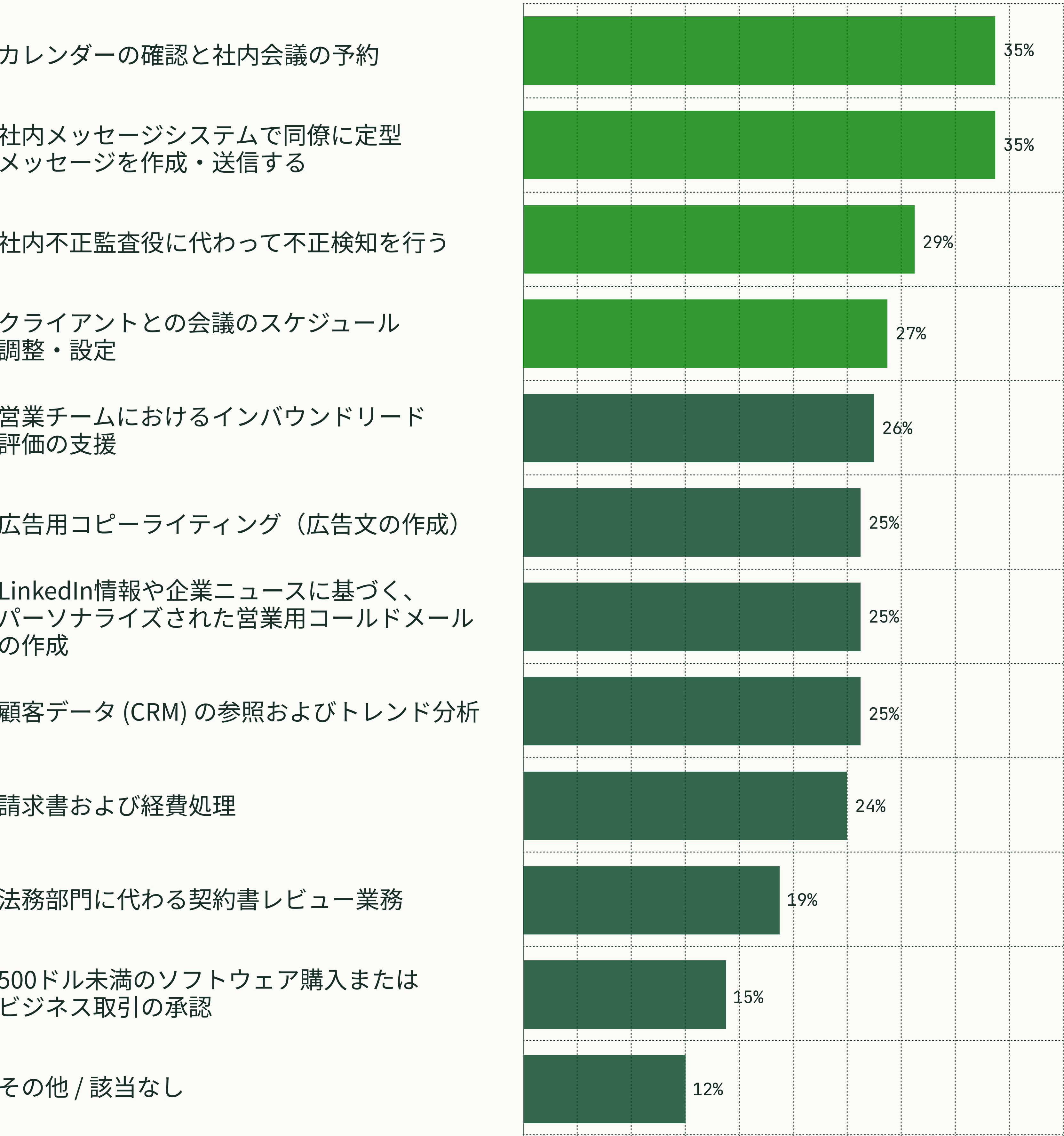
業務の権限委任がセキュリティ管理を追い越す

AIエージェントへの業務の委任は加速しており、セキュリティリーダーは運用タスクをAIに委ねることにますます抵抗を感じなくなっています。

- 1. スケジュール・カレンダー管理（35%）
- 2. 社内向けコミュニケーションの下書き作成（35%）
- 3. 不正の自動検知（29%）
- 4. 顧客との会議（27%）

AIにコミュニケーションを任せることへの意識は、世代によって大きく異なります。**Z世代の専門家の68%**が、自分の代わりにAIエージェントに顧客や同僚とのやり取りを任せることに抵抗を感じないのに対し、**ベビーブーマー世代ではわずか27%**にとどまります。

自身の代わりにAIエージェントへ委任・自動化してもよいと思えるタスクはどれですか？



ヒューマン・イン・ザ・ループの必要性

AIに業務を任せることへの安心感の度合いはさまざまであるものの、「ヒューマン・イン・ザ・ループ」が依然として不可欠だという点は共通しています。実際、91%が、エージェントが回答者に代わって処理を実行する前にヒューマン・イン・ザ・ループによる承認ステップを維持すべきだと強く主張しています。

エージェント間のワークフローは、規模を拡大するために自律的な実行を必要とします。その一方で、人間による検証は、重要なワークフロー、たとえばエージェントが権限を昇格させたり金融取引を実行したりする前の、安全確認として機能し得ます。

「セキュリティリーダーや若い世代は、日常的なスケジュール管理 (35%) から顧客とのやり取り (Z世代では最大68%) に至るまで、運用タスクを積極的にAIへと委ねています。それでも、圧倒的多数である91%は、実行の段階には依然として明確な一線を引いており、最終承認については人間を関与させ続ける『ヒューマン・イン・ザ・ループ』を強く求めています。」

ブーパク・エンボム、
最高マーケティング・事業開発責任者



地域別分析： 米国における導入 のギャップ

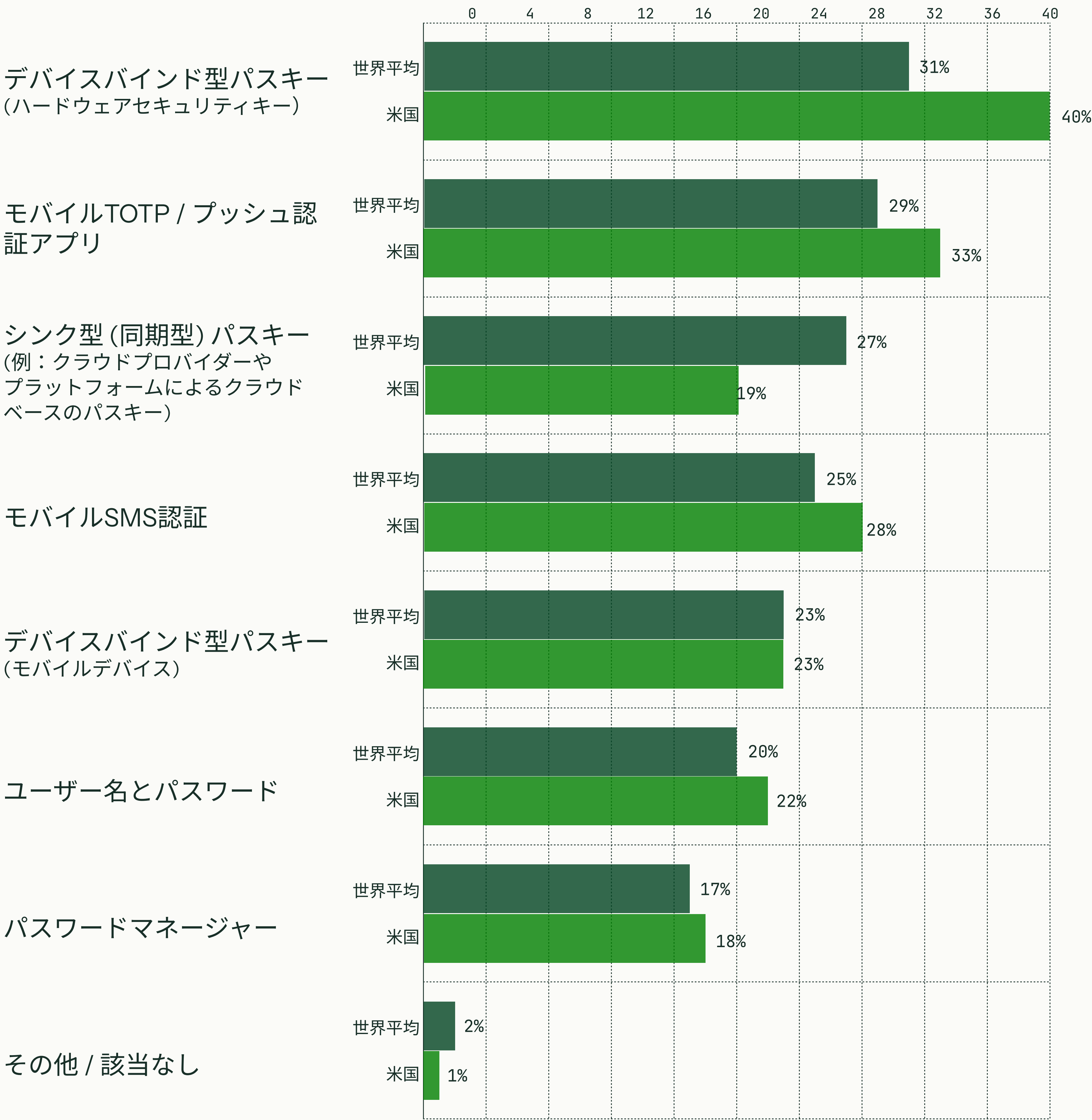


地域別分析：米国における導入のギャップ

認識と実践のギャップを、米国ほど明確に示す市場はありません。米国は技術への認知度が最も高い一方で、システムに対する信頼は最も低く、運用面の変化のペースは最も遅いという特徴があります。

- **高い認知度**：米国のセキュリティリーダーの**40%**がハードウェアベースのパスキーを最も安全な認証情報と評価しており（英国では**23%**）、パスキー利用者の**48%**がハードウェアベースのキーを実際に使用した経験があります（シンガポールでは**28%**）。
- **旧来型の認証情報への高い依存**：同時に、米国はパスワード依存度が全市場で最も高くなっています。職場では**50%**が、家庭では**56%**がユーザー名とパスワードを使用しています。
- **より低い信頼**：米国の回答者のうち、自分の個人データを扱う企業がその保護に十分取り組んでいると考えているのは、わずか**58%**です（インドでは**82%**）。

最も安全な認証方法は何ですか？



新たな セキュリティ アーキテクチャの 構築



認証リスクゼロへ：3段階のハードウェア防御

より安全な企業にするには、セキュリティ意識向上トレーニングだけでは構造上の問題を解決できないと認識することが必要です。高いセキュリティリテラシーを備えているにもかかわらず、組織は依然として、運用上の手間や負担、導入コストに対する認識、そして高い信頼性をもつMFAを基盤的な要件ではなく、任意の追加機能として扱う旧来のオンボーディングデフォルトによって、足かせをはめられています。

AI時代に認証情報に起因するリスクを排除するには、フィッシング耐性のあるハードウェアベースのパスキーやその他のデバイスバインド型の暗号認証器を、セキュリティアーキテクチャ全体で強制適用する必要があります。その実現には、3つのフェーズにわたる対策が求められます。

- **認証の前：**アクセスセッションを確立する前に、デバイスの健全性と状態（ポスチャ）のチェックを義務付け、エンドポイントのコンプライアンスを検証します。ワークフォースのオンボーディングプロセスの一環として、新しく入社した社員にフィッシング耐性のある認証器を発行し、最初のログインから高い保証レベルのMFAを実現します。
- **認証の最中：**アプリケーションのサインオンポリシーにフィッシング耐性のある認証の利用を義務付け、サインイン時にAIを活用したフィッシング攻撃の試みを一貫して自動的に軽減します。
- **認証の後：**継続的にコンテキストとリスクを評価し、セッションの侵害を検知します。自律型AIワークフローをヒューマン・イン・ザ・ループで認可する際には、キーへのタッチのような物理的なハードウェア操作、または生体認証を通じて、人間が存在している証明を要求します。



結論



意識から実施の徹底へ

「グローバル認証状況調査2026」の結果は、セキュリティ意識だけでは企業を守るのに不十分であることを示しています。改善の糸口は、構造的なパターンを断ち切ることにあります。知識を持つ専門家であっても、運用上のデフォルト設定や日々の煩わしさから、職場の内外でつい楽な方を選んでしまいます。人間の警戒心だけに頼っていても本当の安全は守れません。必要なのは賢明な選択が自然と選ばれるように、企業のアーキテクチャそのものを変えていくことです。

何が効果的かは、セキュリティリーダーならすでに分かっています。あとは、企業のポリシーとインフラがその知見に追いつくだけです。



企業ステートメントおよび調査方法

Yubicoについて

Yubico（Nasdaq Stockholm: YUBICO）は、グローバルなサイバーセキュリティのパイオニアであり、フィッシング耐性のあるハードウェアベースの認証のゴールドスタンダードであるYubiKeyの開発元です。2007年にグローバルなパスキー標準の共同策定に携わって以来、Yubicoは160カ国以上の企業・政府・個人にわたってアカウント乗っ取りを根絶してきました。当社のグローバル拠点には、スウェーデン・ストックホルムの本社、米国カリフォルニア州シリコンバレー、そしてシンガポールが含まれます。

詳しくは www.yubico.com をご覧ください。

Oktaについて

Oktaは、The World's Identity Company™です。アイデンティティを保護することで、すべての人があらゆるテクノロジーを安全に利用できるようになります。当社のカスタマーソリューションとワークフォースソリューションは、企業と開発者がアイデンティティの力を活用してセキュリティ、効率性、成功を推進できるようにし、同時にユーザー、従業員、パートナーを保護します。世界のトップブランドが認証、認可、その他の機能でOktaを信頼する理由については、以下をご覧ください。

<https://www.okta.com/jp/>

調査方法

Talker Researchは、米国、英国、オーストラリア、インド、日本、シンガポール、フランス、ドイツ、スウェーデンの9つの市場で、1,890人のテクノロジーおよびセキュリティの専門家を対象に定量的なオンライン調査を実施しました。

回答者は、企業組織 (従業員500人以上規模) 内でサイバーセキュリティ、IT、プロダクトマネジメント、ソフトウェアエンジニアリング、ハードウェアエンジニアリングの役割を担う人々です。本調査はYubicoとOktaの委託により、2026年7月2日から7月16日にかけて実施されました。

結果は場合により異なります：ケーススタディ、顧客の声、およびパフォーマンス指標は、取り上げた組織がそれぞれ固有の構成、ネットワーク環境、実装パラメータのもとで得た具体的な運用成果を示すものです。これらの資料は一般的な情報提供のみを目的としており、法務・プライバシー・セキュリティ・コンプライアンス・ビジネスに関する助言を意図したものではありません。

©2026 Okta, Inc. および/またはその関連会社