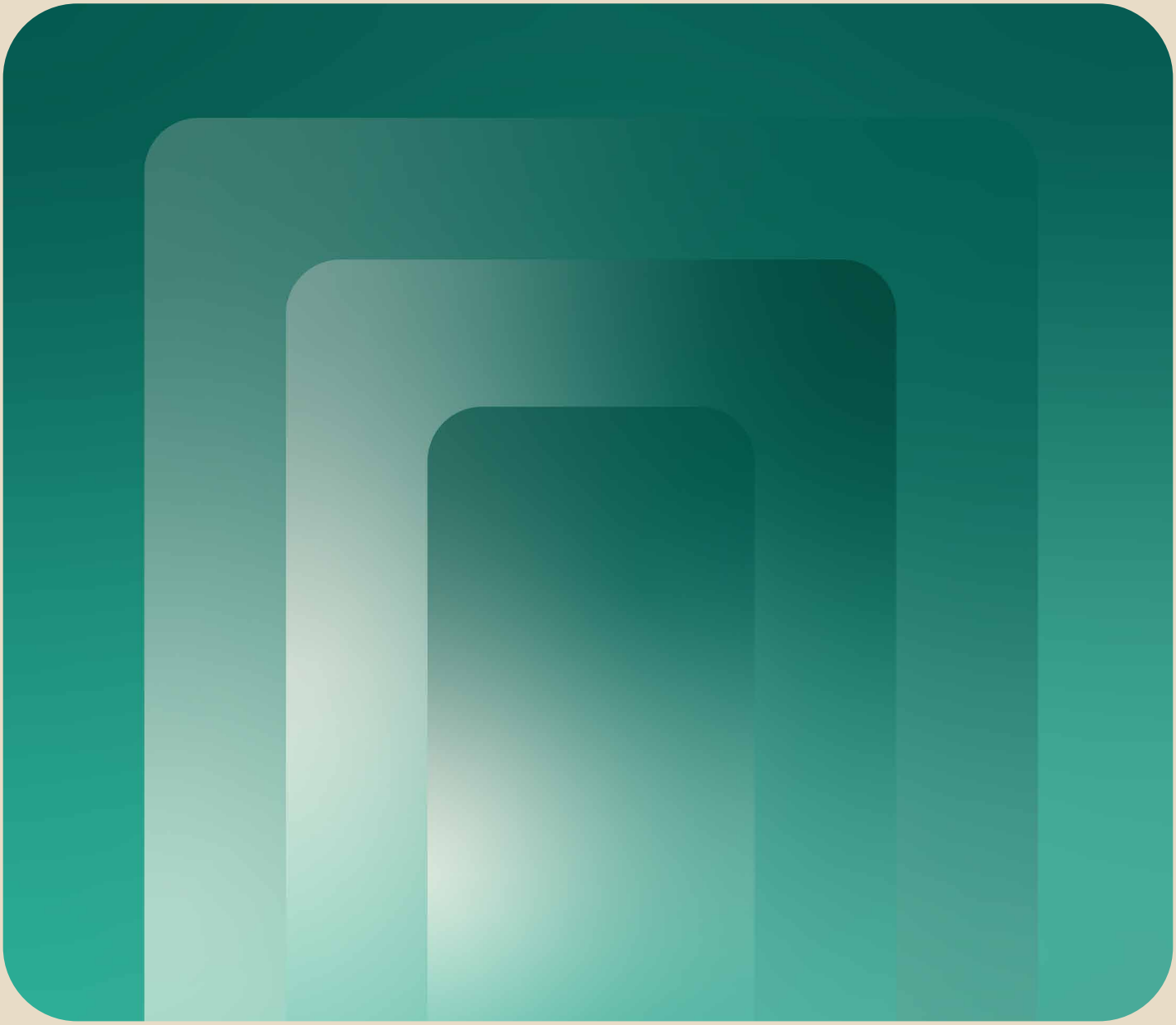
2023

ログイン認証と認証後の脅威とは？

The State of Secure Identity Report



okta

目次

序文

顧客認証の保護

この 10 年で、イノベーションが急速に進み、膨大な情報へアクセスできるようになり、アイデンティティソリューションに対する需要も大きく変化しました。現在、コンシューマーアプリケーションでも業務アプリケーションでも、アイデンティティが企業セキュリティの要となっています。その一方で、アイデンティティ攻撃が量と複雑さの両面で拡大しています。Okta は業界のリーダーとして、アイデンティティのセキュリティ標準を高めるための取り組みを支持する責任を担っています。 Okta Secure Identity Commitment（アイデンティティの保護に対する Okta の取り組み）は、業界のアイデンティティ攻撃との闘いを Okta が主導することを長期的に約束するものです。 そのために、市場をリードする安全な製品とサービスを提供し、当社の企業インフラストラクチャを強化し、お客様のベストプラクティスを支持し、アイデンティティ攻撃に対する業界の防御態勢を強化していきます。

こうした背景から、本レポートは、カスタマーアイデンティティのセキュリティに関する主要なトレンドについて業界の理解を高め、ベストプラクティスを共有することを目的としています。

ログイン画面のセキュリティを確保することは、アイデンティティ攻撃へ対策の最も重要なステップの 1 つとなります。**認証**は、**CIAM（Customer Identity and Access Management / カスタマーアイデンティティ & アクセス管理）**サービスの基本的な機能です。ログイン画面は認証を通して顧客のデジタルアイデンティティの確認を試みます。アプリケーションから見ると、ユーザーまたは人間以外のデバイスやシステムといったエンティティ（属性の変更とは無関係に存在する、単一で識別可能なオブジェクト。付録 A の用語集を参照）を定義する一連の属性がデジタルアイデンティティになります。

しかし、ログイン画面で認証を行うのは正規のユーザーだけではありません。サイバー犯罪者がこれらの認証画面から侵入に成功すれば、大きな対価を得ることができます。金銭的な利益を得ることを目的として、このようなログイン認証から**侵入**するためのテクノロジーやサービスなどを提供する広範なサイバー犯罪のエコシステムも形成されています。

業種や規模の大小を問わず、さまざまな企業が攻撃され、その勢いが加速し続けています。サイバー犯罪者は、ログイン画面を突破するため、多くの労力と専門知識を駆使しています。社会やビジネスを変革しつつある人工知能（AI）も、犯罪者に悪用されています。ログイン画面を保護するためには、これまで以上に高度な防御レイヤーが必要となっています。

消費者との取引（B2C）や企業間の取引（B2B）でも、インターネットから顧客ポータルにアクセスさせなければならず、問題が消えることはありません。さらに、ユーザーに認証を求めるときには、信頼してもらうための明瞭さと同時に、不要な負担を強いることのないシームレスなエクスペリエンスも求められます。

長年にわたり、顧客認証では、正規ユーザーとアプリケーションプロバイダーのみが把握しているとされる知識要素（通常はパスワード）が一般的に使用されてき

ました。しかし、この考えが誤りであることは何度も証明されてきました。知識要素は窃取や学習が可能であり（**オープンソースインテリジェンス［OSINT］**などを通じて）、特にパスワードは問題を引き起こします。アプリケーションプロバイダーも、CIAM サービスも、より安全な認証要素を顧客が利用するように取り組む必要があり、**多要素認証（MFA）**の活用が理想的だと言えるでしょう。

数年前まで、安全な認証と優れたユーザーエクスペリエンスを両立させることは不可能か、少なくとも非現実的であり、何らかの妥協が必要であると考えられてきました。特に MFA は扱いにくく、B2C では広域的な導入が困難だと考えられてきました。

しかし現在では、**パスキー**（具体的には**同期パスキー**）を簡単に利用できるようになっており、安全性と利便性の両立が可能となっています。**カスタマーアイデンティティ**の保護が同期パスキーによって重要なターニングポイントを迎えたことが、将来的に認識される日が来ることでしょう。パスキーのメリットはセキュリティの向上だけではなく、便利で親しみやすいユーザーエクスペリエンスを実現します。パスキーは多くの点で他の保護アプローチよりも簡単に利用できるのです。

また、パスキーが絶好のタイミングで登場したことも重要です。アプリケーションやサービスが増え続けている中で、アクセスを制御するデジタルアイデンティティによって、ユーザーの仕事や生活はさまざまな面で多大な影響を受けています。こうした影響は今後ますます大きくなり、信頼性、セキュリティ、プライバシーを確保するために、認証、認可、そして CIAM 全般が不可欠になっています。その結果、アクセシビリティでも CIAM が中心的な役割を果たすようになっています。CIAM によって情報格差（デジタルデバイド）が拡大するのか、それとも解消するのかは、アイデンティティ管理の実務者にかかっています。

本レポートは、Okta が年次で発行している「State of Secure Identity Report」の第 3 弾です。今回は、カスタマーアイデンティティへの脅威とその防御策について認識を深めていただくことに焦点を当てています。今年は少し趣向を変え、以下の 3 部構成になっています。

- 認証前の対策：ログイン画面は誰もがアクセスできる必要がありますが、実際には、無差別にすべてのユーザーに表示すべきではありません。
- 認証時の対策：ログイン画面は、アイデンティティをめぐる攻防が日々繰り広げられている場所となっています。
- 認証後の対策：ユーザーがログイン画面で認証した後も、継続的にアクセスを保護しなければなりません。

本レポートが皆様のお役に立てれば幸いです。

Shiven Ramji
Okta カスタマーアイデンティティ担当プレジデント

エグゼクティブサマリー

CIAM は、IAM（Identity and Access Management / アイデンティティ & アクセス管理）の分野において、カスタマーアイデンティティを対象とするセグメントです。顧客向けのアプリケーションは、ユーザーフレンドリーかつ安全であり、プライバシーを保護することが求められます。しかし、このようなアプリケーションは、絶えず変化・進化する脅威にさらされています。

サインアップ攻撃、クレデンシャルスタッフィング、MFA バイパス攻撃が毎日のように行われている中で、これらの脅威を防ぐ役割を顧客向けのログイン画面が担っています。本レポートでは、これらの状況について説明していきます。

エグゼクティブサマリー

犯罪者にとって ログイン画面は「宝の山」

本レポートでは、2023 年 1 月 1 日～ 6 月 30 日までの期間についての調査結果を報告します。

アカウント登録の試みのうち、13.9% が Okta Customer Identity Cloud, powered by Auth0 でサインアップ攻撃と判定された

- Customer Identity Cloud を最も利用している 10 業種を見ると、金融サービス（28.8%）、メディア（28.4%）、製造（25.1%）、ソフトウェア / SaaS / テクノロジー（24.0%）の 4 業種で不正な登録の割合が特に高くなっています。
- サインアップ攻撃が最も多く発生した日には、不正登録の試みが 1,000 万件近く検出されています。
- 4 月 15 日におけるアカウント登録の試みでは、64% 以上が不正と判定されました。

ログインの試み全体の 24.3% が、クレデンシャルスタッフィングと判定された

- Customer Identity Cloud を最も利用している 10 業種では、小売 / e コマース（51.3%）、メディア（42.3%）、ソフトウェア / SaaS / テクノロジー（32.1%）、金融サービス（30.3%）が、クレデンシャルスタッフィングの割合が平均を上回りました。
- クレデンシャルスタッフィングが最も多く発生した日には、2,700 万件以上の攻撃が検出されています。
- 1 月 1 日には、46% 以上がクレデンシャルスタッフィングと判定されました。

MFA の試みの 12.7% が、悪意ある活動（MFA バイパスなど）と判定された

- Customer Identity Cloud を最も利用している 10 業種では、メディア（12.8%）、金融サービス（10.9%）、製造（7.8%）、ソフトウェア / SaaS / テクノロジー（6.4%）で、MFA バイパスが試みられる割合が特に高くなりました。
- MFA バイパスの試みが最も多く発生した日には、75 万件以上のインシデントが検出されています。
- 6 月 11 日には、MFA バイパスがすべての MFA の試みの 30% 以上を占めていました。

組織が直面する脅威に影響を与える要因は、業種だけではありません。たとえば、不正な登録、クレデンシャルスタッフィング、MFA バイパスに関しては、中規模企業よりも小規模企業と大企業が狙われる割合が高くなっています。この背景として、サイバー犯罪者が大企業を価値の高い標的、小規模企業を攻撃が成功しやすい標的とみなしていることが考えられます。

本社所在地がある地域によっても、直面する脅威の傾向が異なります。アジア太平洋を拠点とする組織では不正登録が圧倒的に多く、北米 / 中南米を拠点とする組織ではクレデンシャルスタッフィングが非常に多くなっています。

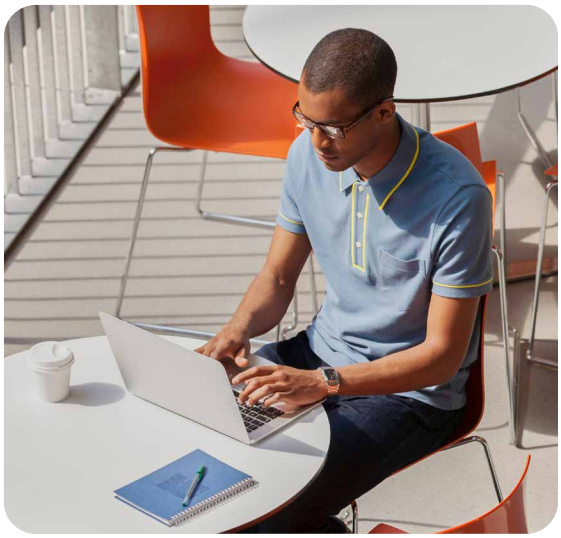
		不正登録の試み [1]		クレデンシャルスタッフィングの試み [2]		MFA バイパスの試み [3]	
		割合	順位	割合	順位	割合	順位
	全体（テクノロジー全般）	13.9%	—	24.3%	—	12.7%	—
Customer Identity Cloud を最も利用している 10 業種	広告 / マーケティング	1.0%	10	16.7%	6	3.4%	9
	金融サービス	28.8%	1	30.3%	4	10.9%	2
	飲食 / ホスピタリティ	9.0%	8	11.4%	8	5.5%	5
	医療	6.3%	9	16.1%	7	4.6%	7
	製造	25.1%	3	17.7%	5	7.8%	3
	メディア	28.4%	2	42.3%	2	12.8%	1
	プロフェッショナルサービス	13.4%	5	7.2%	10	4.5%	8
	小売 / e コマース	9.3%	7	51.3%	1	5.0%	6
	ソフトウェア / SaaS / テクノロジー	24.0%	4	32.1%	3	6.4%	4
	旅行 / 運輸	9.7%	6	7.2%	9	2.9%	10
組織規模	大企業	19.9%	1	39.4%	1	9.5%	2
	中規模企業	12.6%	3	20.1%	3	9.0%	3
	小規模企業	19.4%	2	30.9%	2	20.3%	1
本社所在地	北米 / 中南米	9.4%	2	28.0%	1	12.0%	1[4]
	アジア太平洋	27.9%	1	13.3%	3	11.0%	2
	欧州 / 中東 / アフリカ	8.1%	3	20.2%	2	7.6%	3

表 1：Customer Identity Cloud テクノロジーによるアイデンティティ攻撃率のまとめ（2023 年 1 月 1 日～ 2023 年 6 月 30 日の期間）

[1] 登録の試み全体に占める割合
[2] パスワード認証の試み全体に占める割合
[3] MFA の試み全体に占める割合
[4] 3 つの地域がいずれも世界平均を下回っている理由については、「調査手法」セクションを参照

エグゼクティブサマリー

顧客の保護と満足を CIAM で実現



ワークフォースアイデンティティ管理の対象となるユーザーは、主に企業や組織の従業員であり、セキュリティについても知識のある方が多く、また使いづらさや前提知識が求められるような「**摩擦**」を受け入れやすいと言えます。しかし、CIAM はコンシューマーをはじめとする十分なスキルや知識を持たない幅広いユーザーも対象としているため、利便性の高いユーザーエクスペリエンスを維持しながら、強固で優れたレジリエンスも確保できる、厳格なセキュリティ手法を採用しなければなりません。

顧客からの期待は高まり続け、脅威環境の進化が止まることもありません。そのため、ユーザーエクスペリエンス、セキュリティ、プライバシーの適切なバランスをとるため、これらの手法も調整し続ける必要があります。また、組織のリスクプロファイルや、リスクへの許容度によって、このバランス自体も異なってきます。

多層防御を実装する

レート制限、不審な IP アドレスのブロック、漏洩したパスワードの検知などは、いずれも欠かすことのできない防御手段ですが、これらの防御策だけでは不十分です。

同様に、基本的な要件として、効果的なパスワードポリシー（強力なパスワードを要求する、安全なリセットプロセスを導入するなど）や、適切なセッションハイジーン（URL からセッショントークンを除外する、ログイン後に予測不可能な新しいトークンを生成するなどの衛生管理）も挙げられますが、それだけでも現在の脅威を防ぐことはできません。

サイバー犯罪者がセキュリティ対策を迂回するための技術や手法に投資している中、CIAM サービスやアプリケーションのプロバイダーも次世代防御への投資を拡大しなければなりません。

Okta の AI を活用した Bot Detection は、こうした防御策の一例であり、認証システムを狙うボットの 80% 近くをフィルタリングして排除できることが実証されています。重要なのは、ユーザーに無用な「摩擦」をもたらすことなく、こうした防御を実現していることです。Bot Detection の中核となる AI を慎重に訓練し、継続的に調整することで、人間（ユーザー）には CAPTCHA がほとんど表示されなくなり、シームレスなエクスペリエンスを維持できます。

さらに、この機能が強力な抑止力となっていることを明らかに示すデータもあります。Okta を導入している大手企業の中には、Attack Protection に含まれるこの Bot Detection を有効にしたところ、ボットトラフィックの 90 日間平均の値が 90% 近く減少したケースも見られています。

認証を強化する

パスワードを使用したログインに比べて、パスキーは顧客認証を劇的に強化する可能性があります。パスキーがもたらすメリットは非常に大きなものです。パスワードはさまざまなアイデンティティ脅威の原因となっています。パスキーは、パスワードへの依存を低下させる重要な一歩となります。

- 特に同期パスキーは、使い慣れた便利な方法で強力な認証を実現することができ、優れた利便性を期待している一般的な多くのユーザー層に最適です。実際に、2023 年 10 月 10 日現在、Google は個人の Google アカウントでパスキーをデフォルトのサインインオプションとして提供しています。
- B2B 市場や、**FIDO** 認証オーセンティケーター / セキュリティキーによる認証の強化を必要とする顧客アプリケーションでは、**デバイスに紐づくパスキー**（device-bound passkey）が優れたオプションとなります。

全体として MFA も、顧客認証を強化する役割を引き続き果たします。これまで、一般ユーザーを顧客として抱えている組織は、認証時の摩擦の増大によってコンバージョンに悪影響が及ぶことを懸念して、MFA を強制的に適用することや導入を推奨することにさえ、二の足を踏んでいました。しかし最近では、アプリケーションプロバイダーが活用できる以下のようなテクノロジーが登場したことで、こうした懸念は不要になっています。

- **アダプティブ MFA：**リスクの高いログインに対してのみ MFA チャレンジを適用できます。リスクが高いかどうかは、多くの脅威シグナルを基準に判断されます。
- **ステップアップ認証：**低リスクのリソースにアクセスするときには、比較的強度が低い認証方法（パスワードなど）を使い、機密性の高いリソースにアクセスするときには強力な認証方法（MFA など）を適用できます。

しかし、これまで説明してきたように、比較的弱い MFA 要素をバイパスするために、攻撃者は多大なリソースを投資していることから、アプリケーションプロバイダーは、所有要素による認証や生体認証へと移行することが不可欠となっています。

CIAM ソリューションは、自社で構築すべきか、購入すべきか

このような階層型の CIAM ソリューションを自社で構築することは、潤沢なリソースがある大企業にしかできない大規模な取り組みです。しかし、プライバシーを保護しながら便利で安全なカスタマーエクスペリエンスを実現するには、このようなレイヤーやテクノロジーが必須です。

「セキュアバイデザイン」の思想を取り入れた俊敏な CIAM は、多くの組織にとって最も効果的で効率的なアプローチとなります。これらの CIAM ソリューションでは、自社のコアビジネスを前進させるためのリソースを割くことなく、CIAM をカスタマイズし、必要に応じて継続的に調整できます。

サードパーティ認証が大きな違いを生み出す

世界各国のアプリケーション開発チームメンバーを対象とした最近の調査によって、SaaS アプリケーションにサードパーティ認証を組み込むことの価値が明確になっています。

56 か国の専門家から寄せられた 675 件の回答をもとに、以下の状況が明らかになりました。

- 「認証の機能を自社で構築して維持すること」は、「データ管理 / ストレージ」「DevOps ツール / 自動化」に次いで **3 番目に多くの時間がかかる。**
- **サードパーティ認証は、他のどの SaaS コンポーネントよりも市場投入までの時間を短縮する。**認証にサードパーティ SaaS プラットフォームを使用している組織の 88% が、過去 1 年間で市場投入までの時間が短縮したと報告しています。

詳しくは、開発チームの SaaS 調達状況をご覧ください。

カスタマーアイデンティティのセキュリティについて

ログイン画面で認証して情報にアクセスしようとするのは、正規のユーザーだけではありません。攻撃者は、多大な労力をかけてでも、標的とする情報を手に入れようとします。あらゆるアプリケーションやサービスプロバイダーにとって、カスタマーアイデンティティの保護が最優先事項であるべきなのは、このためです。

Okta は、第 3 弾となるこの「State of Secure Identity Report」を通じて、以下についての認識を深めることに焦点を当てました。

- カスタマーアイデンティティを狙う脅威の状況
- 堅牢で信頼できる防御を構築するために導入すべき手法

こうした目標を達成するために、現在、一般的で危険な攻撃パターンと、将来の脅威環境を形成する全体的なトレンドを探っていきます。

本レポートでは、さまざまな規模の数千の組織に CIAM 機能を提供している Okta Customer Identity Cloud, powered by Auth0 から収集したデータを可能な範囲で使用し、アイデンティティの脅威の拡散と影響を紐解いていきます。

しかし、具体的な説明に入る前に、本書でのカスタマーアイデンティティの意味を深く理解するために、以下の点を確認しておく必要があります。

- 利便性と安全性を両立させることの必要性
- CIAM が果たす重要な役割
- 進化し続ける認証メカニズム
- 人工知能（AI）は「諸刃の剣」

カスタマーアイデンティティのセキュリティについて

顧客は安全で便利なエクスペリエンスを期待

デジタルチャネルでサービスを提供する組織にとっては、顧客とのあらゆるやりとりで摩擦を最小限に抑えることが非常に重要です。具体的には、クリック数を最小限に減らし、直感的な UI を設計し、遅延を短縮し、Web サイトやアプリなどのチャネル全体で一貫した便利なユーザーエクスペリエンスを提供する必要があります。

サービスと正規ユーザーを両方とも保護するためには、アイデンティティに関連する攻撃の多様化に対抗できるセキュリティ対策も導入しなければなりません。攻撃者にとっての摩擦を最大化しながら、正規ユーザーにとっての摩擦をゼロに近づけるアイデンティティを実装できれば理想です。ゼロに近いという表現を使っているのは、場所とタイミングが適切であれば、多少の摩擦は顧客からの信頼を得るために役立つためです。

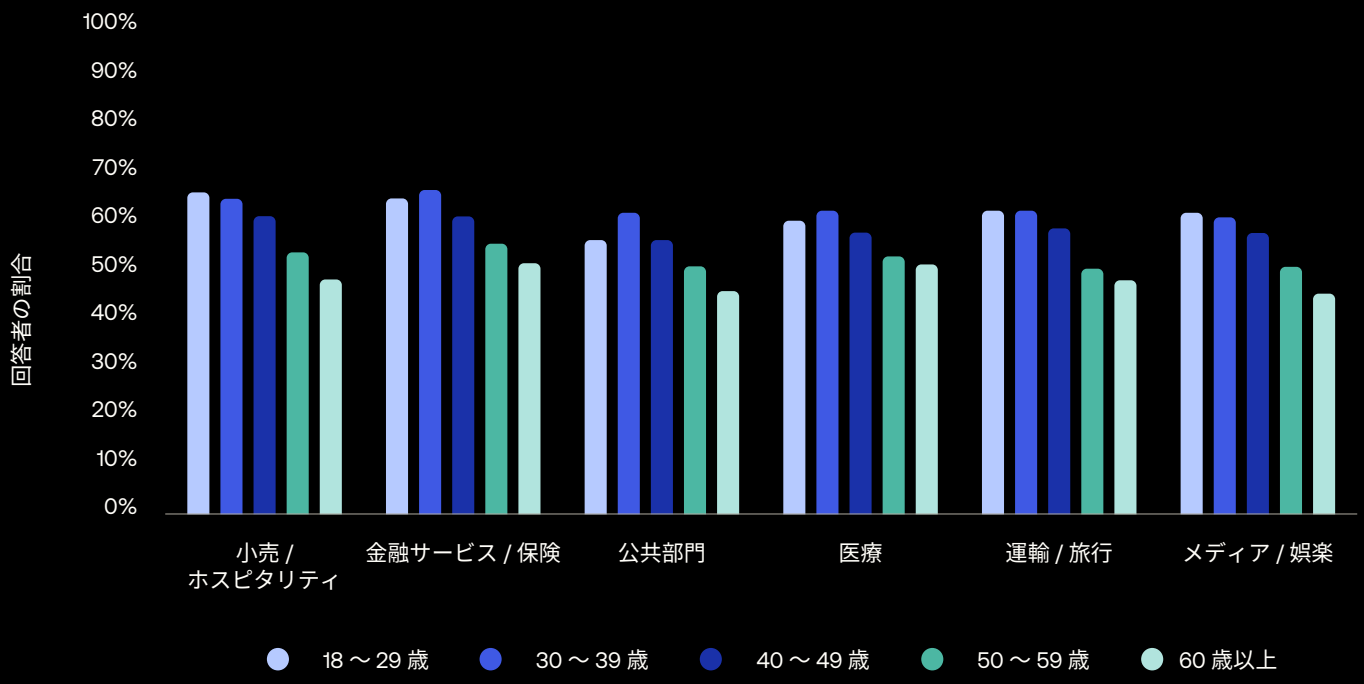
このような完璧なソリューションを目指すのは素晴らしいことですが、現実には「トレードオフ」が頻繁に起こります。たとえば、スクリプトによる大規模なボット攻撃を検知して阻止するメカニズムを導入すれば、アプリケーション全体のレジリエンスは高まる可能性があります。その一方で、一部のユーザーにセキュリティチャレンジが表示されるようになり、摩擦が増えるというマイナス面が生じます。

ソリューションを導入した後は、運用から得られる洞察に基づいてメカニズムを微調整し、セキュリティと利便性の適切なバランスを取ることができます。実際のところ、顧客基盤、脅威環境、セキュリティ設定の組み合わせは、アプリケーション、組織、業界によって異なり、何が適切なバランスなのかも異なってきます。また、攻撃者が TTP（戦術、手法、手順）を調整して新たな標的を選択し、顧客からの要望も変化しているため、このバランスも変わっていく可能性があることから、問題はさらに複雑化しています。

しかし、最適なバランスを取る努力を続けることで、大きなメリットが得られます。世界 14 か国のコンシューマー 21,512 人を対象に実施した調査に基づく Okta の Customer Identity Trends Report 2023 によると、回答者の 60% 近くが、使いやすくて安全、かつ摩擦のないログインである場合に、対価を支払ってサービスを利用する可能性が高くなると回答しています。重要な顧客層である若い世代が、このような利便性を特に重視しています。

図 1：コンシューマーは、シンプルで安全、かつ摩擦のないログインである場合に、対価を支払ってオンラインでブランドを利用する可能性が高くなる

（グラフは、「可能性が非常に高い」と「可能性がやや高い」の回答の合計）



カスタマーアイデンティティのセキュリティについて

アイデンティティとアプリケーションの保護でCIAMが果たす役割

前述したようなボット検知メカニズムは、アイデンティティセキュリティスタックの1つの要素に過ぎず、アイデンティティセキュリティも、CIAM の1つの側面でしかありません。

最新の CIAM ソリューションは、利便性、プライバシー、セキュリティのバランスを取るために役立ち、アプリケーションやサービスにアクセスするあらゆるタイプのユーザーに対応できます。また、CIAM ソリューションを導入すると、企業は継続的に UX を進化させることができ、エンジニアリングチームによるアイデンティティ関連の業務への負荷を軽減し、重要なコアビジネス業務に注力させることができます。さらに、規制、認証、契約上の要件に効率的かつ効果的に対応できるというメリットがもたらされます。

効果的な CIAM ソリューションには、認証、認可、アイデンティティ管理という 3 つの基本機能が備わっています。これらの各機能を見ていきましょう。

- **適切な認証**：アカウントにログインしようとしているユーザーが本人であることを確認します。
- **効果的な認可：**アプリケーションやリソースへの適切なアクセス権限をユーザーに提供するのに役立ちます。
- **包括的なアイデンティ管理：**管理者はユーザーのアクセス許可を更新し、セキュリティポリシーを実装できます。この機能により、特定のユースケースで認められ、規制で求められる範囲内で、顧客は自分のアイデンティティ、データ、設定を管理できます。

CIAM の従来の定義は、今も変わることなく一貫していますが、CIAM が対応できるユースケース、使用する機能コンポーネント、そして対応する組織について、CIAM が果たす役割は近年進化を遂げています。今日、CIAM は以下のようなユースケースで欠かすことができなくなっています。

- **コンシューマーへのサービスの提供：**効果的な CIAM を実装すれば、B2C（コンシューマーとの取引）でにおいて、個別の顧客に合わせてパーソナライズされたプロモーションやレコメンデーションを提供できるようになり、収益を向上して、顧客へのサービスの価値を高めることができます。同時に、デジタルチャネル全体でユーザーにとっての利便性を向上できます。
- **企業顧客の支援：**多くの組織にとって、B2B（企業間取引）の SaaS アプリケーションはビジネスに不可欠となっています。しかし組織のさまざまなユーザーは、多様なリソースに異なる権限レベルでアクセスする必要があります。アイデンティティとアクセス権限を厳格に管理しなければ、利便性と安全性を両立することはできません。CIAM は、B2B で SaaS の顧客が自らアイデンティティを管理できるように支援して、この課題に対応します。
- **サービスプロバイダーなどのパートナーやサードパーティの支援：**コンシューマー向けアプリケーションや SaaS アプリケーションでは、顧客自身がアイデンティティを管理しますが、サービスを提供する組織がアイデンティティを管理しなければならないシナリオも多くあります。CIAM は、サービスプロバイダーが顧客のアイデンティティを把握 / プロビジョニングできるように、顧客アカウントの作成、保守、登録解除を管理するツールを提供しています。

ワークフォースアイデンティティでは、管理者はユーザーエクスペリエンスについてそれほど考慮せずに、アイデンティティを管理できるでしょう。一方、カスタマーアイデンティティでは、特に認証について摩擦を最小限に抑えるか、少なくとも慎重に管理しなければなりません。

カスタマーアイデンティティのセキュリティについて

認証の安全性とシンプルさを両立

ゼロトラストの考え方により、従業員向けのアイデンティティ管理に大きな変化が生じていますが、CIAM は「何も信頼しない」ことをこれまでも前提として運用されてきました。CIAM のみを使用するほぼすべてのユースケースでは、アプリケーションプロバイダーもアイデンティティプロバイダーも、サービスへのアクセスが実行されるエンドポイントは制御できません。

より高度なアクセスによるやりとりやトランザクションを許可するには、十分な信頼を確立しなければなりません。そのような場合、ユーザーは 1 つ以上の要素を提示するよう求められます。

- **知識要素：**パスワード、セキュリティ質問の答えなどのユーザーが知っているもの
- **所有要素：**携帯電話、メールアカウントへのアクセス情報などのユーザーが持っているもの
- **生体要素：**指紋、顔、または声などの生体認証に用いることができるユーザー固有の身体的特徴。生体認証デバイスは、通常、認証を試みるユーザーが、同じタイプの生体認証を最初に設定したユーザーと同じであることを保証します

ログイン認証画面が登場した当初は、ユーザー名とパスワードを入力するだけの単純なものでしたが、時とともに以下のような大きな変化が起こりました。

- **パスワードの複雑化：**多くのユーザーが同じパスワードをいくつもの場所で使用するようになり、攻撃者が脆弱なパスワードを推測することで、この問題に付け込むようになりました。このため、ユーザーは複雑なパスワードを設定しなければならなくなり、特殊文字、大文字と小文字の組み合わせ、数字を含む、長いパスワードが使われるようになりました。
- **パスワード管理の発達：**ユーザーが管理するパスワードが増え、複雑化したため、ブラウザでパスワード管理機能が実装されたり、専用アプリケーションが導入されたりなど、パスワードマネージャーが広く利用されるようになりました。
- **MFA の重要性の高まり：フィッシング**の脅威が拡大しており、膨大なパスワードがオンライン上に流出するインシデントが発生していることから、**アカウントの乗っ取り**（ATO）に対する効果的な防御策として、MFA の利用が拡大しました。

残念ながら、従来の MFA ではユーザーにとっての摩擦が生じるため、コンシューマー向けのサービスではその採用は広がっていません。さらに、大規模かつ経済的な方法で MFA の防御をバイパスする方法を攻撃者が見つけ出しており、旧来の MFA 手法の安全性が脅かされつつあります。

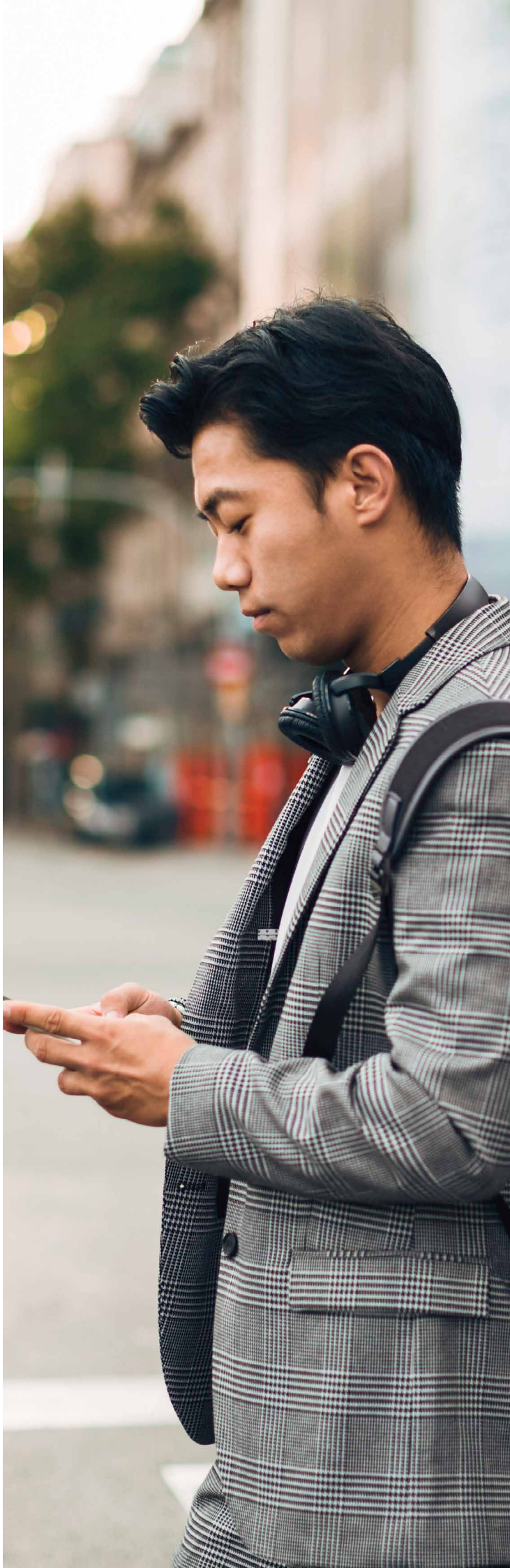
認証手法と攻撃者の TTP が進化する中で、多様なサイバー攻撃が自動的に行われるようになりました。このため、組織のセキュリティ対策への費用は増え続けて、

顧客のプライバシーも脅かされています。こうした攻撃を防御するため、CIAM ソリューションにはアイデンティティセキュリティの新しいレイヤーが追加されるようになりました。

アダプティブ MFA やステップアップ認証のような最新のセキュリティ対策は、理想的なソリューションに近づきつつあります。どちらも、相応のリスクがある場合にのみ、ユーザーに追加の認証を求めることを目的としています。セキュリティと利便性の最適なバランスを維持するには、セキュリティチャレンジが必要なタイミングを正確に判断しなければなりません。そのためには、リスクシグナルや、要求されているアクセスレベルなどの他のコンテキスト情報を踏まえてリスクを評価し、適切な認証チャレンジを選択するなどの処理を実行するインテリジェントなシステムが必要となります。

人工知能（AI）は以前からアイデンティティシステムに組み込まれていますが、AI は間違いなくさらに重要になっていきます。セキュリティに限らず、カスタマーエクスペリエンスを向上させる上でも AI は有用です。

AI の可能性は無限ですが、使い方次第では、悪用される恐れもあります。



カスタマーアイデンティティのセキュリティについて

大規模なアイデンティティ攻撃がAIで容易に

人工知能（AI）とは、基本的に、人による意思決定とは区別できないほど「インテリジェント」なコンピューターによる意思決定（意思決定の手法や過程は問わない）のを意味します。

AIの起源は、コンピューターが発明されるよりもはるか前の1943年に、論理学者のウォルター・ピッツと神経生理学者のウォーレン・マカロックが人間の脳の神経細胞の数学的表現を作成しようとしたときに遡ります。

1960年代以降、AIはさまざまなタスクを実行できるアルゴリズムの大規模な集合体へと進化してきました。パターンの検出と認識もこうしたタスクの1つであり、これが機械学習（ML）と呼ばれています。機械学習の分野は、ニューラルネットワークの構築と操作が進歩したことにより、過去15年間で急速に発展しました。コンピューターの処理能力がかつてないほど高まったことで、ニューラルネットワークを「深化」（大規模化）させることが可能になり、実用的で経済的なディープラーニングが実現しました。

しかし、AIは、驚異的そして衝撃的な生成AIへと発展し、世界を席巻しています。生成AIは、主として大規模言語モデル（LLM）の目覚ましい進歩によって急速な進化を遂げました。

突如として、小説や評論を書いたり、複雑で写実的な画像を作成したりすることが、人間ではなくコンピューターでも可能になったのです。さらに、LLMには、優れた記述能力があり、その能力はプログラミングなどにも活かされています。そのため、広範な領域でLLMが思いがけないブレークスルーや進歩をもたらすようになっています。

アイデンティティセキュリティに目を向けると、AIは脅威のリスクレベルを高めています。たとえば、AIによって以下のような攻撃が可能になっています。

- **既存の簡易なアイデンティティ攻撃が大規模化し、リスクが増大：**クレデンシャルスタッフィング、不正登録、SMSトラフィックポンピング詐欺などの攻撃の検知が難しくなり、攻撃が効果的で破壊的になる恐れがあります。
- **まったく新しいタイプのアイデンティティ攻撃の出現：**新しい攻撃であっても、防御側の組織や研究者が予期していたり、事前に特定したりする場合があります。一方、実環境で実行されていることが発見されて初めて明らかになる攻撃（「未知の未知」の問題）も登場する恐れがあります。
- **既存のセキュリティ対策の無効化：**すでに、AIを活用したツールは、CAPTCHAを突破したり、ディープフェイクを使って音声の生体認証システムを騙したりする能力を獲得していることが実証されています。

さらに、コーディングやスクリプト作成の能力を持つ生成AIによって、コーディングのスキルがなくても簡単に攻撃を実行できるようになり、サイバー犯罪に手を染める犯罪者が増え、攻撃の効率性も高まっています。

それぞれの標的組織に照準を合わせた、拡張性とコスト効果の高い攻撃の実現

しかし、新たなアイデンティティ脅威の中で最も危険なのは、大規模な**スピアフィッシング**を AI が可能にすることでしょう。攻撃者は以下のような流れで攻撃を実行できるようになることが想定されます。

1. 標的の組織を選ぶ。
2. **OSINT** の手法により、従業員のリストを作成する。
3. ソーシャルメディアを検索する API（その他にもさまざまな方法があります）に、このリストを送り、各従業員のソーシャルメディアアカウントのリストを取得する。
4. 情報を公開してソーシャルメディアを活発に利用している従業員を、フィルタリングによって絞り込み、フォローしている人物、よく見ている投稿、その従業員が投稿している内容、活動している時間などを調べる。さらに、トピックに基づくセンチメント分析を行って、その従業員向けにパーソナライズされた高度な心理プロファイルを作成し、これらのプロファイルを更新する可能性もあります。
5. 標的として絞り込まれた従業員との信頼関係を築くため、ソーシャルメディアでその従業員をフォローし、「いいね!」、投稿の再共有、コメントの追加などの一般的な方法でやりとりを始める。
6. 時事問題、ニュース、トレンドを監視して、従業員と個人的につながる機会を伺う。
7. 標的の従業員に、メールやダイレクトメッセージなどの方法で接触する。
8. 従業員から応答があれば、やりとりを続行し、高い確率でファイルを開かせたり、リンクをクリックさせたりする要求を成功させることができるまで、十分な信頼関係を確立していく。

このような攻撃チェーンでは、つい最近までは煩雑でコストのかかる手動の操作が必要でした。しかし今日では、ほぼ完全にこれらのプロセスを自動化でき、多くの組織の何千人もの従業員を個別に標的にする大規模な攻撃をわずかなコストで実行することができます。

防御の強化

AI は攻撃者によって悪用されることは確実ですが、防御側も AI を活用して対策を強化できます。たとえば、次のような用途に AI を利用できます。

- **「セキュアバイデザイン」に基づくアプリケーションの保護強化：**攻撃者は AI を利用して脆弱性やセキュリティ上の弱点を探ることができますが、同様にアプリケーションプロバイダーも、ソフトウェアやシステムをリリースする前に、これらの問題を特定して堅牢化でき、「先行者優位」の状況を得ることができます。
- **脅威を自動検知する能力の向上：**コンテキスト分析と行動分析は、インテリジェントなリスク評価と高度なアイデンティティ脅威の検知に役立ちます。また、AI の進歩によって、こうした機能を実行する能力が向上し、新たな機能の導入も促進されます。
- **リスクの軽減**：封じ込めのアクションや不正な操作のブロックなどの防御策を自動化する、あるいは、アラートと推奨される対策を記したプレイブックを組み合わせるなど、AI はプロアクティブにリスクを軽減し、攻撃に対応する上で非常に大きな力になります。

ここまでは、カスタマーアイデンティティに関する重要なポイントを見てきました。それでは、認証に関する現在の状況と今後の対策を見ていきましょう。

パート1:
認証前の対策

認証における最初の防御策は、人か機械 / システムを問わず、攻撃者によるログイン画面へのアクセスを防止することが目的です。

攻撃者を早期に排除できれば、後続の攻撃を検出および分析するコストを削減でき、攻撃者による偵察（エラーメッセージを受信して分析するなど）も制限できます。

そのためには、アイデンティティインフラストラクチャのさまざまなレイヤーで、以下などの多くの防御策を講じることができます。

- **ホスティングの防御：**ホスティングプロバイダー（Microsoft Azure、Amazon Web Services など）によって、あるいはホスティングレイヤー（Cloudflare など）で実行される防御
- **プラットフォームの防御：**CIAM プラットフォーム全体（Okta Customer Identity Cloud など）で実行される防御
- **アプリケーションの防御：**単一の CIAM アプリケーション（自社構築、ポイントソリューションなど）で実行される防御

パート1：認証前の対策

最前線に立つホストレイヤーの防御

ホスティングプロバイダーは、ホスティング対象のサービスが悪用されないように、以下のような多くのセキュリティ機能を提供しています。

- **分散型サービス拒否（DDoS）への対策：**特にTCP / UDP レイヤーで大規模な攻撃を受けても、正規ユーザーが CIAM アプリケーションを利用できる状態を維持できるように保護します。
- **ボット管理：**ボットフィルタリングの最初のレイヤーでは、通常、行動分析、脅威インテリジェンス、フィードバックループの組み合わせが使用されます。
- **レート制限：**特定のエンティティ（攻撃者や攻撃用のマシン）が CIAM プラットフォーム / アプリケーションにアクセスするレートを制限することは、DoS 攻撃、ブルートフォース攻撃、API の不正利用から組織を保護する上で役立ちます。

パート1：認証前の対策

プラットフォームレイヤーとアプリケーションレイヤーの防御に役立つ「ネットワーク効果」

これらのレイヤーにおける防御策は、戦術的なものから戦略的なものまで多岐にわたります。これらの防御策は、組み合わせて使用したり、特定のニーズに合わせてカスタマイズしたりすることで優れた効果を発揮します。

また、多くのユーザーが使用するほど、時間の経過とともに有用性が増す「ネットワーク効果」から大きなメリットを得ることもできます。個別に使用されているCIAM アプリケーションと比べて、何百、何千もの組織にカスタマーアイデンティティサービスを提供する CIAM プラットフォームは、はるかに多くの脅威インテリジェンスを直接収集でき、プラットフォームを利用するすべての組織がその利益を受けることができます。たとえば、特定のテナントへの攻撃が観測された場合には、関与した IP をすべてのテナントでブロックするといった対策が可能です。

レート制限

レート制限（スロットリング）は、特定のエンティティが CIAM プラットフォーム全体、または個別の組織の CIAM アプリケーションとやりとりできるレートを制限し、大規模なブルートフォース攻撃に対抗するための有用なツールとなります。

どちらのシナリオでも、所定のしきい値（1 時間以内の最大実行回数など）を超えた場合には、以下のコントロールが適用される対象となります。

- チャレンジ（CAPTCHA など）を完了することを要求される
- 「ペナルティ」の期間が経過し再認証できるようになるまで、ログインインターフェイスへのアクセスを制限される

レート制限は、アイデンティティサービスを標的にする DDoS 攻撃の影響を抑える上でも有効です。機能を利用する前にログインすることを顧客に求めているサイトやサービスの場合、攻撃によって認証サービスが妨害されると、正規の顧客がサービスを利用できなくなり、他のタイプの DoS 攻撃と同じような影響を受けることになります。

不審な IP のブロック

インターネットに接続するサービスでは、不審な IP からのアクセスをブロックする対策は、何十年も前から行われています。この方法には限界がありますが、限界があることを認識した上であれば、現在でも有用です。

このアプローチは、以下のとおり単純なものです。

- 何らかのソースを使用して、IP アドレスが信頼できるかどうかを判断する
- IP アドレスが定義されている信頼性のしきい値を満たさない場合、アプリケーションへのアクセスを拒否する

IP アドレスに限らず、電話番号、メールアドレス（有料メールサービスのユーザーのみが登録できるアプリケーションなど）などについても、同様の手法を広く利用できます。

このようなフィルタリングを効果的に行うために、多くの組織はサイバーセキュリティ脅威インテリジェンス（CTI）を利用しています。組織によっては、直接的な観測によって得られた独自データに基づくレピュテーションのリストを使用したり、複数のアプローチを組み合わせたりしている場合もあります。

ボット検知

ボットトラフィックは、ユーザージャーニーのあらゆるポイントでアイデンティティフローに悪影響を与えます。ボットトラフィックは、単に迷惑なだけでなく、隠れたコストも発生させます。Customer Identity Cloud では、ボットによるログイン要求を毎月何十億も検知しています。ボットによって発生するトラフィックを処理する計算能力にはコストがかかっており、アプリケーションプロバイダーの負担が何百万ドルにも上る恐れがあります。

さまざまなデータソースと観測結果を分析することで、ボットによる接続かどうかを高い信頼性で判断できます。

このようなシナリオでは、要求をブロックする、そのまま無視する、あるいは CAPTCHA などのチャレンジを表示するといった対応を適用できます。

機械をもって機械を制す

Bot Detection は、Customer Identity Cloud の Attack Protection アドオンの重要な機能の 1 つであり、ネイティブアプリケーション、**パスワードレス**のフロー、カスタムログインページに対するスクリプト攻撃（クレデンシャルスタッフィング、パスワード推測、パスワードスプレーなど）を軽減します。

Bot Detection は、IP アドレスに関連する過去のイベント、最近のログイン履歴、IP レピュテーションデータ、その他のさまざまなソースなど、60 以上のデータソースを分析することで、アイデンティティ要求がボットから発生している可能性を予測します。一定の予測値や信頼度のしきい値を超えると、認証フローにおいて CAPTCHA などの対策が提示されます。

Bot Detection は、AI が従来の防御手法を大きく改善できることを示す好例です。

- 2021 年 2 月に導入された初期バージョンは、ルールベースであり、18% のボットを検知していました。
- 2021 年 8 月に登場したバージョン 2 は、行動分析に機械学習を採用しました。この AI を活用したアプローチにより、45% のボットを検知するようになり、効果が倍増しました。
- 2022 年 6 月に提供が開始された最新バージョンは、79% のボットを検出します。攻撃者が絶えず手法を改良している中でも、これまでで最高のパフォーマンスを実現しています。

重要なのは、このような防御機能がユーザーに無用な摩擦をもたらさないという点です。Bot Detection の中核を成す AI を慎重に訓練し、継続的に調整することで、人間のユーザーに CAPTCHA が表示されることはほぼなくなっています。

さらに、Bot Detection の効果を社内で詳細に調査および検証したところ、以下のような強力な抑止効果が明らかになりました。

- Bot Detection を有効にした顧客では、悪意あるトラフィックが平均して 40% 以上も減少した
- 大規模組織の中には、ボットのトラフィックが 90% 近く減少したケースもあった

こうした調査結果は、最先端の防御を導入している組織を攻撃者が避けている傾向があることを示しています。

パート2：認証時の対策

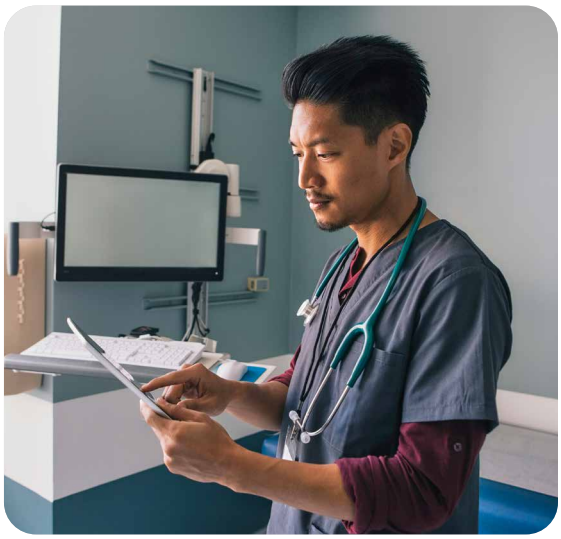
ログイン画面に到達したエンティティ（攻撃者や攻撃用のマシン）は、攻撃者を排除するために導入されている一連の対策をすでに乗り越えています。ログイン認証で、正規ユーザーが試みるアクションは、以下の２つです。

- アカウントのサインアップ
- 既存アカウントへのサインイン

後述するように、攻撃者は日常的に両方のサービスを標的にしています。

パート２：認証時の対策

サインアップのインセンティブが犯罪者を引き寄せる

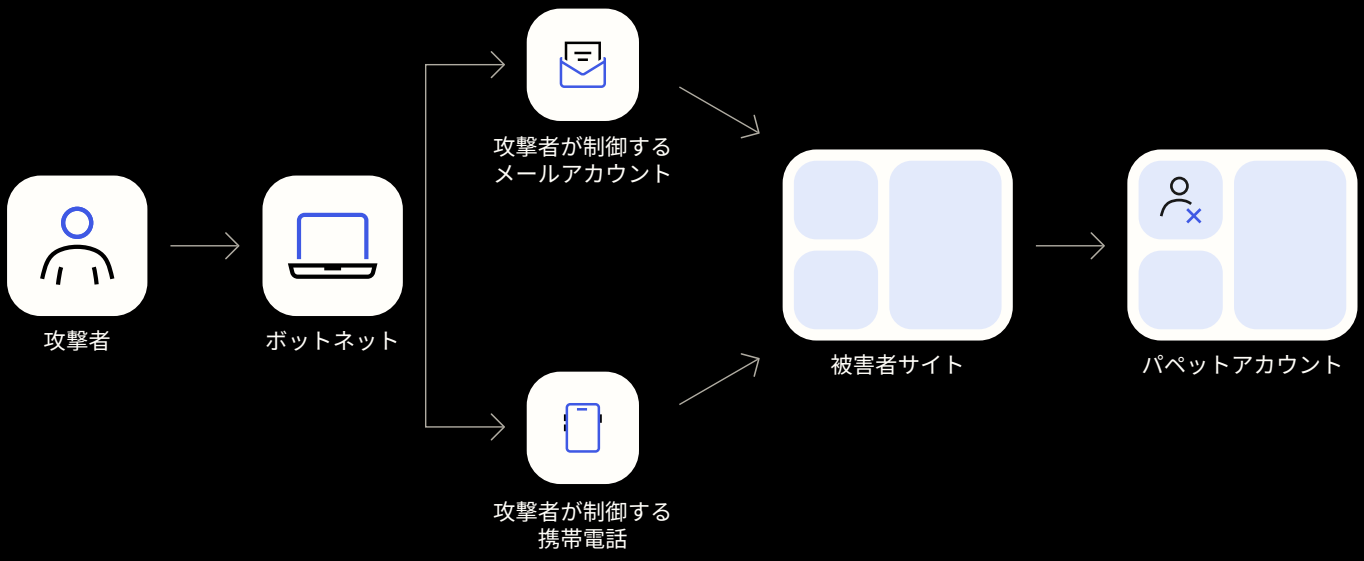


悪意あるユーザーがログイン画面を通過した後に、権限、サービス、情報にアクセスする最も簡単な方法は、認証後すぐに、自らが制御して操ることができるアカウントを作成することです。

こうした行為は、以下のような目的のために実行されます。

- 限定版スニーカーやコンサートチケット、品薄の新しいゲーム機など、**高価値のモノを不正に入手する**
- ギフトカード、暗号通貨トークンなど、**アカウントを作成することで獲得できる商品やインセンティブを受け取る**
- アカウントを利用してスレッドで発言したり、自分のメッセージを広く拡散したりする、**スパム、偽情報、ハクティビズムのキャンペーン**
- 金融サービスや公共料金のアカウントを悪用することが多い**合成アイデンティティ詐欺**
- 利害関係者への**アカウントの転売**
- 潜在的なユーザーの名前空間を使い果たして、正規ユーザーの登録を妨げて、**アプリケーションプロバイダーのサービス提供能力を低下させる**
- 自動的なセキュリティ対策を回避するために、偽造アカウントを使用してログインの成功率と失敗率を注意深く操作し、**アカウント乗っ取り（ATO）攻撃を最適化する**

図 2：不正登録の手口



不正登録の主な標的は B2C 企業です。ユーザーが無料で、購入証明などの何の条件もなくアカウントを作成できる場合には、特に狙われやすくなります。

偽のサインアップは、特に大規模に行われる場合に重大な問題を引き起こし、不要な出費を発生させることがあります。

第一の問題は、ユーザーエクスペリエンスに関連します。偽のユーザーによって、需要の大きい商品の買い占めなど、正規ユーザーのエクスペリエンスに悪影響を与えて、顧客満足度や企業の評判低下につながる可能性があります。組織のリソースも浪費されることになり、アクセスが悪用され組織が直接攻撃を受けたり、損害を被ったりする恐れもあります。

第二の問題は、コンバージョンに関連します。見込み客を新しい顧客にコンバージョンすることは、B2C 企業の大きな目標です。そのため、ユーザーがサービスをどのように利用しているかを示すアナリティクスデータに基づいて、コンバージョンのフロー全体が最適化されていることも多くあります。このデータが不正登録によって歪められるため、ビジネスアナリティクスが複雑になり、データをクリーンアップするコストが増大する可能性もあります。

特に B2C 企業は、コンバージョン率を最大化することを重視しています。そのため、登録プロセスでの摩擦を最小化しようとする動機が強く働きます。しかし、正規ユーザーの摩擦を低減すれば、攻撃者によって簡単に悪用されるようになります。

攻撃者は、いくつかの偽造アカウントだけを作成することもあれば、ボットネットを利用して、数千あるいは数百万の膨大なアカウントを自動的に作成することもあります。膨大なアカウントが作成されるケースでは、一般的なユーザー名のリストがその操作で利用される場合があります。

サインアップの失敗件数や失敗率が突然増えていることは、アプリケーションが攻撃を受けていることを示す強力な兆候になります。そのような状況では、登録のトラフィックを詳しく調べて、しきい値やルールを変更する必要があるかどうか見極める必要があります。

観測結果の集計

図 3 は、30 か月の期間内に集計された不正登録の試み（テクノロジー全体）の推移を示しています。一見しただけで、以下の 2 点が際立っていることが分かります。

1. 不正登録は、顧客サインアップサービスに常に悪影響を与えている
2. 不正登録の件数（および、サインアップの試み全体に占める割合）は、日によって大きく異なる

上記の 2 点よりは目立ちませんが、次の 2 つの重要なトレンドも見受けられます。

1 点目は、この 30 か月間で、1 日当たりの登録の試みに対して不正登録が占める割合は低下していることです。

- 2021 年には、1 日の登録の試み全体の大半が不正登録であることが非常に多く（93 日）、全体の 70% 以上を不正登録が占めたのは 19 日間でした。
- 2022 年には、不正登録の試みが 60% 以上を占めたのは 5 日だけでした。
- 2023 年上半期には、過半数が不正と判定されたのは、1 日（4 月 15 日）だけでした。

2 点目は、この 30 か月間で、不正登録と判定される割合が低下していることです。

- 2021 年には、登録の試み全体の 31.8% が不正と判定されました。
- 2022 年には、この割合が 18.6% まで低下しました。
- 2023 年上半期には、この割合が 13.9% まで低下しています。

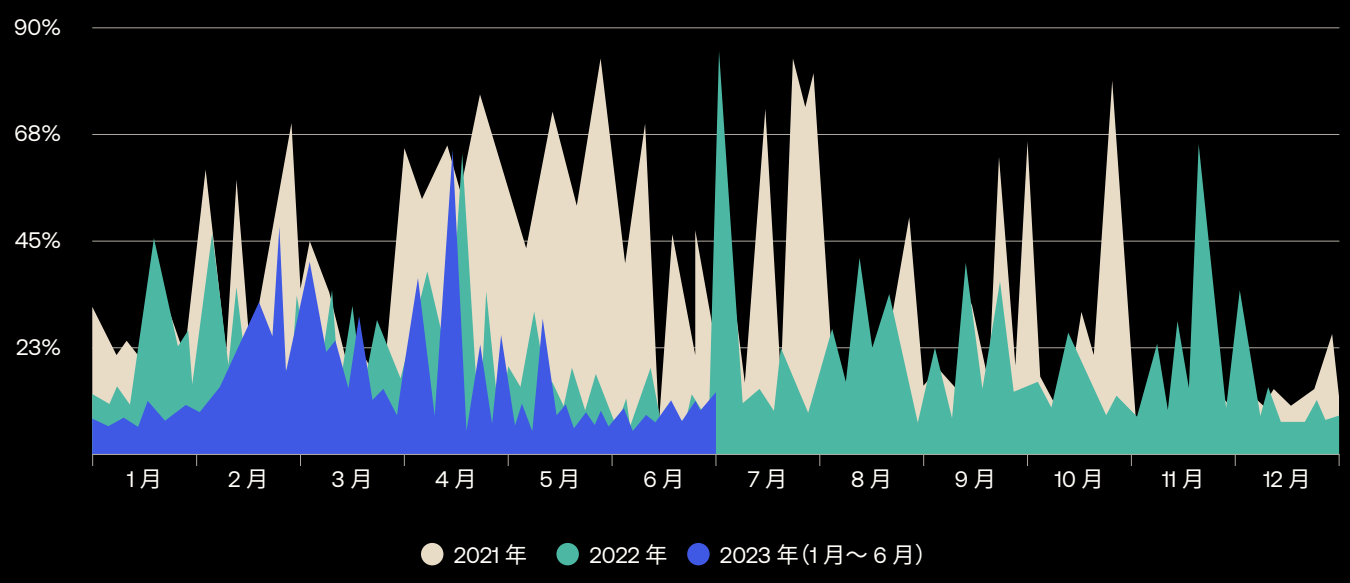
こうした改善傾向は、不正アカウントを開設する攻撃者の試みが大幅に減少したのではなく、多層防御テクノロジーが継続的に向上していることが主な理由となっていると考えられます（この仮説については後で説明します）。

また、詐欺と判定されるしきい値に達するのは、最も目立つ違反者だけであることに留意しなければなりません。しかも、サインアップ攻撃を行っているエンティティを特定のテナントが検知すると、他の多くのテナントに実装されている不正サインアップ防止機能によって、不正な試みが排除され、不正サインアップとしてカウントされず、ログに追加されることすらありません。

重要なので繰り返しの説明になりますが、攻撃者はログイン画面に到達するまでに、ホスト、プラットフォーム、アプリケーションの防御をくぐり抜けていることを忘れてはなりません。

こうした理由から、前後の図に示しているパーセンテージについては、最低ラインであると考えるべきです。現実的に、効果的な多層防御が十分に実装されていないサインアップサービスは、スクリプトによるアカウント登録によって大きな負荷を受けるか、場合によっては完全にサービスを利用できなくなる深刻なリスクも抱えています。

図 3：不正登録は常に存在する脅威だが、Customer Identity Cloud での登録の試み全体に占める割合は減少している



セグメント分析

基盤のデータを詳しく調べると、不正登録の試みに偏りがあることがわかります。

Customer Identity Cloud を最も利用している代表的な 10 業種のうち、金融サービス（28.8%）、メディア（28.4%）、製造（25.1%）、ソフトウェア / SaaS / テクノロジー（24.0%）では、不正サインアップの試みの割合が平均を上回っていました（図 4）。

攻撃者が、これらの業種のアカウントを特に標的としているのはなぜでしょうか。この理由を読み解くのは簡単ではなく、さまざまな答えがあるかもしれませんが、いくつかの説明が考えられます。

- 銀行や証券会社などの金融機関は、新規口座開設時にウェルカムボーナスなどの特典（旅費などに使用できるポイントや特別低金利ローンなど）を付与することが多く、金銭的価値のあるものはすべてサイバー犯罪者にとって魅力的な標的になります。口座は、マネーロンダリング（資金洗浄）の目的や合成アイデンティティ詐欺に悪用されることもあります。
- メディアは、フォーラムを開設してコメントを受け付けていることが多く、アカウントを取得して管理することで、偽情報、ヘイトメッセージ、プロパガンダ、スパムリンク、その他の悪意のあるコンテンツを幅広いオーディエンスに拡散することが可能になります。
- メーカーは、生産に支障をきたさないために身代金要求に応じようとする圧力が強く働き、サイバー犯罪者から特に狙われています。そのため、不正に作成されたアカウントの一部は、長期間に及ぶ攻撃チェーンで悪用するために作成される場合もあります。コンシューマーに直接商品を販売しているメーカーは、生産数や供給が限られた商品を特別に提供することがありますが、これは、転売目的でこれらの商品を買い占めるために、アカウントを大量に作成する動機にもなっています。
- 多くのソフトウェア、SaaS、テクノロジーサービスは、1 つまたはいくつかの要素（使用時間、ストレージ容量、利用可能なコンピューティングリソースなど）に制限を設けるフリーミアムモデルを採用していますが、詐欺アカウントは、これらの制限を回避するためにも作成されていると考えられます。

備考：業種別の分析に関する追加情報は、付録 C をご覧ください。

大企業と小規模企業は、中規模企業に比べて、不正サインアップの試みの割合が高くなっていることが統計的に有意に認められます（図 5）。

サイバー犯罪者は、正規の企業と同じ経済的利益に従い、利益を最大化しようとしています。そのため、大企業や小規模企業に対するサインアップ詐欺によって、中規模企業を標的にするよりも大きな利益を得られると、攻撃者が見込んでいることが考えられます。

サイバー犯罪者は、大企業の防御が周到であり、攻撃が成功する可能性が低いと評価している一方で、攻撃が成功した場合に得られる利益が十分にあり、投資対効果（ROI）が労力に見合うと考えているのでしょう。

小規模企業の場合は、状況が逆です。つまり、1 回の攻撃で得られる報酬は低いものの、高い成功率を期待できるため、攻撃する価値があるということになります。

備考：組織の規模別の分析に関する追加情報は、付録 D をご覧ください。

同様に、本社所在地の地域別に集計すると、さらに多くの違いが明らかになります（図 6）。北米 / 中南米（9.4%）と欧州 / 中東 / アフリカ（8.1%）を拠点とする組織は、アジア太平洋（27.9%）を拠点とする組織に比べて、不正登録の割合が低くなっています。

アジア太平洋と他の地域の間でこれほどの差異があるのは、アイデンティティセキュリティに対するアプローチの成熟度がアジア太平洋で低く、アカウント登録関連の不正を防止するためのセキュリティ製品 / 機能があまり導入されていない状況を反映しているためかもしれません。

備考：地域別の分析に関する追加情報は、付録 E をご覧ください。

図 4：いくつかの業界では、不正登録が試みられた割合が平均を上回っている

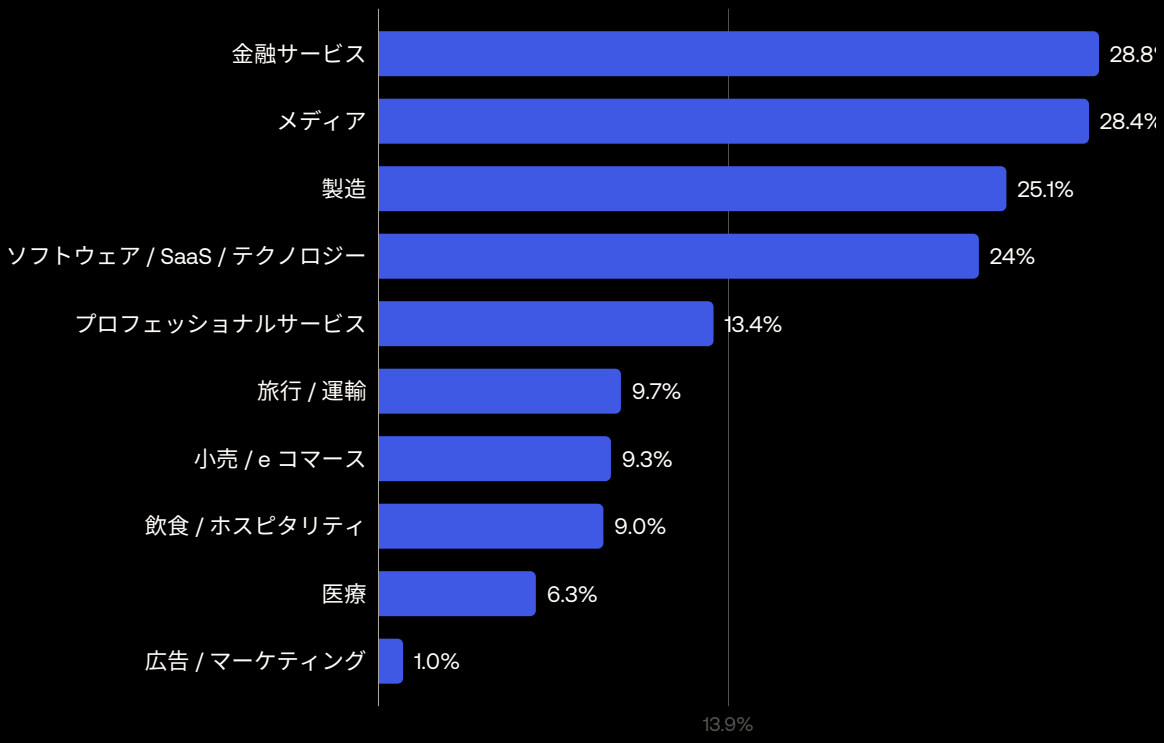


図 5：不正サインアップは、特に大企業や小規模企業で多くなっている

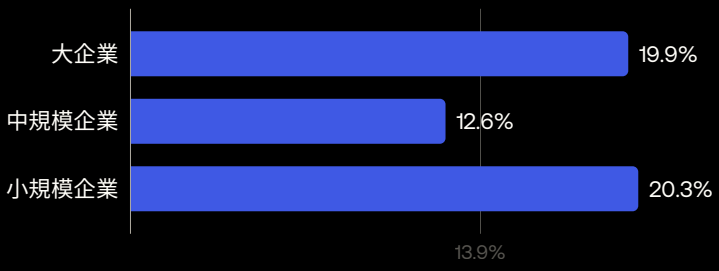
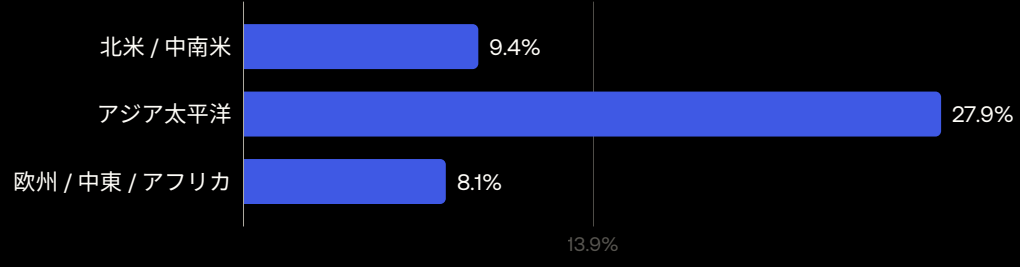


図 6：アジア太平洋を拠点とする組織は、北米 / 中南米や欧州 / 中東 / アフリカを拠点とする組織に比べて、不正登録が試みられた割合が特に高い



防御策

不正登録を削減するためには、ログイン画面に到達する前の防御レイヤーに加えて、以下のようなアプローチを利用できます。

- **サインアップ前のルールとアクション：**チャレンジの適用、追加情報の要求などにより、新規ユーザーが不正である可能性をさらに低減する
- **ソーシャルログイン：**SNS のアカウントを利用させてることで、不正サインアップの防止を「アウトソーシング」する
- **アイデンティティプルーフィング：**リスクが特に高いと考えられる場合に追加の認証方法を適用する
- **連絡先情報の検証：**ワンタイムパスコードや**マジックリンク**などにより、メールアドレス、電話番号などを確認する

サインアップが失敗する理由はさまざまですが、重要なのは、これらのインテリジェンスを収集して、総体的な脅威インテリジェンス評価を可能にすることです。たとえば、1 時間以内にアカウント 10 個のサインアップに失敗した IP を「高リスク」に指定できれば、その IP から試みられる接続は、認証前にプラットフォームまたはアプリケーションのレベルでフィルタリングされます。

しかし、ソーシャルログインは別として、上記の各アプローチは、サインアッププロセスで摩擦を増やすことになるため、適切なバランスを取るための配慮が必要になります。

また、攻撃者が SMS や通話ベースの検証方法を悪用するようになっていることにも注意が必要です（後述）。

脅威のスポットライト：SMS トラフィックポンピング詐欺と料金詐欺

どこでも利用できる SMS は、アイデンティティフローに組み込むことができる利便性の高いチャネルです。たとえば、SMS を使用した登録に対応するフローや、SMS ベースの登録のみを許可するフローを採用しているサイトも多く（Toast、Uber など）、SMS は登録や MFA チャレンジ（**OTP** やマジックリンクなど）で広く利用されています。

しかし、残念ながら、フォームフィールドを悪用してアプリケーションプロバイダーを騙し、有料通話番号に SMS メッセージを送信させたり、電話させたりすることで、攻撃者がその収益の一部を得ることも可能です。

いずれの場合も、大きなコストが発生する可能性があり、それを負担するのはアプリケーションを悪用された企業です。2023 年 2 月には、イーロン・マスク氏が、「偽の 2FA SMS メッセージ」によって Twitter が年間 6,000 万ドルの損失を被っていると ツイート しています。

本レポートで取り上げている他の攻撃と同様に、攻撃者は検知のリスクを減らすため、以下のような手口を見出しています。

- 電話番号ごとのしきい値を超えないように、電話番号をローテーションする
- 目立たないように時間をかけて、数日、数週間、あるいは数か月も検知されるまで、長期間にわたって攻撃を引き延ばす

多くの組織は、ユーザーのサインアップや認証で SMS を利用しているため、単純にこのチャネルの使用を停止することは現実的な選択肢ではありません。代わりに、テレフォニーベースの不正行為を防止 / 軽減するための高度にインテリジェントな方法を、アイデンティティインフラストラクチャに追加する必要があります。

ソーシャルログイン

ソーシャルログインによって、エンドユーザーは**シングルサインオン（SSO）**が可能になります。新しいアカウントを作成する代わりに、Facebook、Twitter、Google などのソーシャルネットワークプロバイダーで利用しているログイン情報を使って、サードパーティサービスに簡単に登録できます。

ソーシャルログインは、エンドユーザーに優れた利便性をもたらすだけではありません。ログインプロバイダーが強力なサインアップセキュリティ対策を実施している場合には、サインアップ詐欺対策にも役立ちます。

ただし、サービスによって対策にばらつきがあるため、どのサードパーティを信頼できるかをアプリケーションプロバイダーが判断しなければなりません。

注目すべき点として、ソーシャルログインはアプリケーションプロバイダーに以下のような潜在的メリットも提供します。

- **登録者数の増加：**多くのユーザーは、新しいアカウントを作成するよりも、既存のアカウントを再利用することを好みます。
- **確認済みのメールアドレス：**ソーシャルネットワークプロバイダーは、ユーザーのメールを確認する役割を担います。プロバイダーがこの情報を共有することで、Web アプリケーションに登録するためによく使われる偽のアドレスではなく、実際にユーザーが使用しているメールアドレスを入手できます。ソーシャルプロバイダーは、パスワードの回復プロセスにも対応します。
- **パーソナライゼーションとカスタマイズの可能性拡大：**ソーシャルネットワークプロバイダーは、位置情報、趣味、誕生日など、ユーザーが共有に同意した情報を追加で提供できます。こうした情報を使用して、サービスを強化できます。
- **ワンクリックで簡単にアプリケーションにログイン：**ユーザーがソーシャルログインでアプリケーションに登録すれば、簡単にアプリケーションにログインできます。ソーシャルネットワークにログインしていれば、ワンクリックでアプリケーションにログインできます。

アイデンティティプルーフィング

CIAM における認証とアイデンティティプルーフィングは、同じものであると誤解されることが多くあります。認証（ユーザー名とパスワードによるサインインなど）は、ユーザーが特定のアカウントに対応する資格情報を持っていることを示しますが、ユーザーが本人の主張している人物であることを証明するものではありません。この本人確認機能を果たすのがアイデンティティプルーフィングです。

アイデンティティプルーフィングは、追加的な検証により、登録希望者が本人であることを高い信頼性で保証します。

CIAM では一般的に、季節変動や販促プログラムに伴うトラフィック急増に対応するため、ワークフローをリアルタイムに調整することが要求されます。そのため、アイデンティティプルーフィングソリューションには拡張性が求められます。幸い、近年では、顧客登録のニーズを満たすために、以下のような自動化されたアイデンティティプルーフィングの手法が多数開発されています。

- **知識ベースの認証（KBA）：**ユーザー（理想的には、そのユーザーのみ）が知っていることを利用します。
- **文書スキャンと相互検証：**パスポートや運転免許証などの信頼できる写真付き身分証を使用して、ユーザーが主張するアイデンティティが実際のアイデンティティと一致するかどうかを検証します。
- **通信事業者による検証：**携帯電話サービスの契約時にユーザーのアイデンティティがすでに証明されていることを利用します。

パート2：認証時の対策

資格情報の使い回しがアカウント乗っ取りを助長

不正登録は、少なくともコストを増大させる迷惑行為です。一方、アカウント乗っ取りは、セキュリティとプライバシーにとって大きな脅威となります。

B2C の場合、攻撃者は、ロイヤリティポイントなどのリソースや限定商品を購入する機会を得たり、販売のターゲット層や個人識別情報（PII）にアクセスしたりできるようになります。

B2B では、攻撃者は侵害したユーザーアカウントを使用して、機密性の高いデータにアクセスする可能性があります。そのような場合には、標的となった組織は、コンプライアンス、法規制、契約に違反することとなり、厳しい罰則が科せられることになります。

ATO の試みの中には、個人を標的にしたものもありますが（パート 3 でいくつかのアプローチを説明します）、ほとんどは以下の手法によるブルートフォース攻撃（T1110）です。

- **クレデンシャルスタッフィング**（T1110.004）：他のサイトやサービスが侵害され流出した既知の資格情報を試す
- **パスワードスプレー**（T1110.003）：多くのアカウントで一般的に使用されている比較的小さなパスワードリストを試す
- **パスワード推測**（T1110.001）：やや粗雑なアプローチであり、多数のアカウントで多くのパスワードを試す

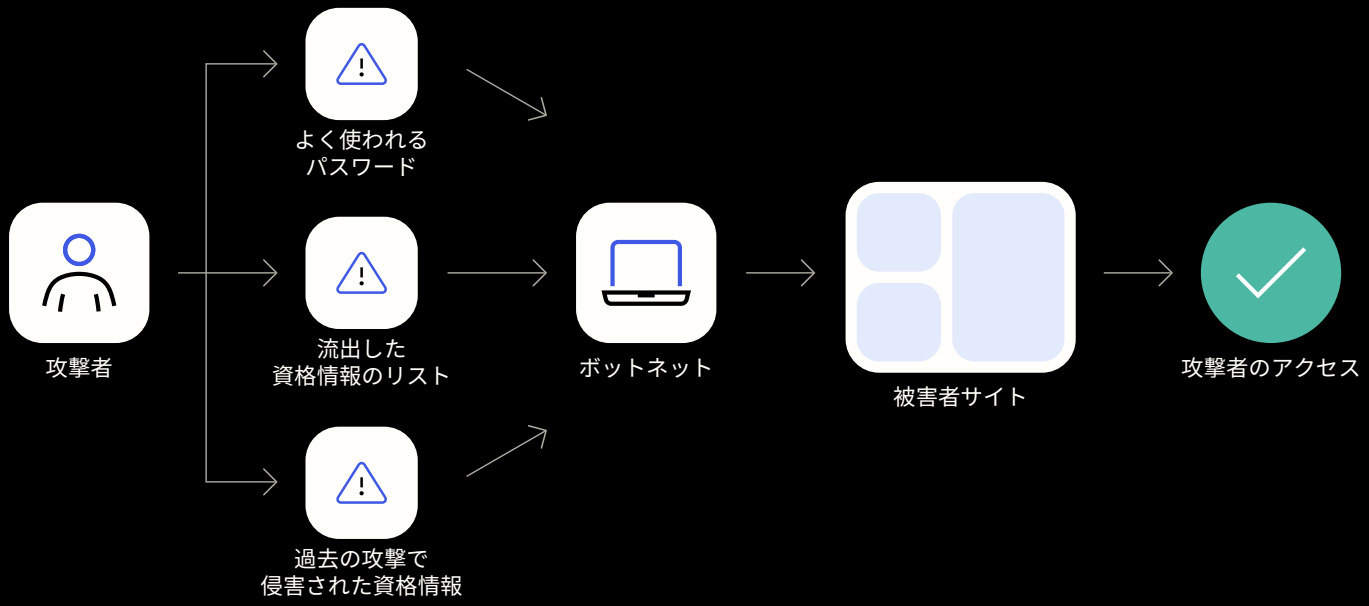
これらの攻撃が大規模に実行されると、意図的かどうかにかかわらず、正規ユーザーの認証に時間がかかったり、認証サービスが完全に利用できなくなったりするといった悪影響が生じる恐れがあります。

これら 3 つのアプローチはいずれも、強度の低いパスワード、パスワードの使い回しなど、ユーザーのパスワードの扱いに問題がある状況を悪用しています。攻撃者は、こうした問題に付け込むことで、攻撃を実行するためのコストや労力を大きく削減できます。たとえば、漏洩パスワードのリストや、その中で頻繁に使用されている単語の辞書を活用するといった最適化の手法によって、正しいパスワードを試す確率（正確に言うと、正しいパスワードと同じハッシュ値のパスワードを試す確率）を劇的に向上できます。

上記 3 つの攻撃のうち、攻撃者から見て最も効果が高く、アプリケーションプロバイダーとその顧客から見て最も危険なのは、クレデンシャルスタッフィングです。攻撃者が既知のユーザー名とパスワードの組み合わせを試すことで、自動検知メカニズムを作動させる可能性は若干低くなります。

残念ながら、このような攻撃は、実行するための障壁が非常に低く、攻撃者は多くの戦術を用いて防御を回避しようとします。たとえば、失敗率を慎重に管理するため、既知の有効な資格情報（恐らく、すでに取得している不正アカウントの資格情報）をログインストリームに紛れ込ませる可能性があります。

図 7：クレデンシャルスタッフィング攻撃の手口



クレデンシャルスタッフィングは、コストをかけずに、攻撃を大規模化できることから、高度な能力を有する攻撃者が好んで利用している手法です。図 7 から想定されるキルチェーンでは、攻撃者はサイバー犯罪向けのサービスを利用してフィッシングキャンペーンを開始し、資格情報を取得します。収集した資格情報は、盗み取られた時点で現在使用中であることがわかっており、攻撃者は高い成功率でクレデンシャルスタッフィング攻撃を仕掛けることができます。このシナリオでは、スクリプト内のパラメータを一部変更するだけの単純な操作で、複数の組織やサービスを標的にできます。

アカウント乗っ取りに加えて、クレデンシャルスタッフィングも、アカウント発見 / 検証の中間的なステップとして使用されることがあります。たとえば、流出した多数の資格情報を特定のサービスで検証します。その後、検証された価値の高いリストをプレミアム価格で販売することが考えられます。

観測結果の集計

図 8 は、30 か月の期間内に Customer Identity Cloud で観測されたクレデンシャルスタッフィングの試みの推移を示しています。不正登録の場合と同様、クレデンシャルスタッフィングに起因するログインが試みられる割合は、この期間では大幅に減少してきました。

- 2021 年には、ログインの試み全体の 42.8% がクレデンシャルスタッフィングに起因したものでした。不正登録と同様、この判定基準は非常に厳しく、一度不正と判定されると、その後の試みはログに記録されることすらありません。
- 2022 年には、この割合が 33.4% まで低下しました。
- 2023 年上半期には、この割合が 24.3% まで低下しました。

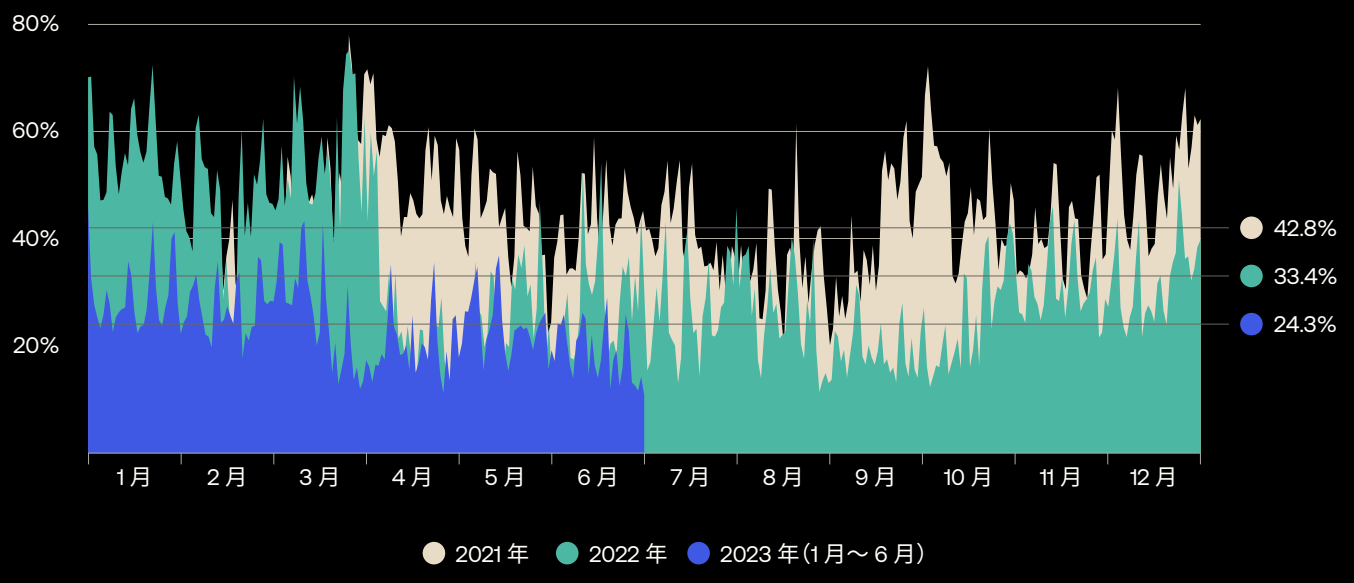
詳細に見ると、2022 年 4 月に大きな変化が起きたことがわかります。

- 2021 年 1 月 1 日から 2022 年 3 月 31 日まで、ログインの試み全体の 47.3% がクレデンシャルスタッフィングによるものでした。
- 2022 年 5 月 1 日から 2023 年 6 月 30 日まで、クレデンシャルスタッフィングと判定された割合は 24.6% にとどまりました。

では、2022 年 4 月に何が起こったのでしょうか。実は、この月の最初の 2 週間に、Consumer Identity Cloud の防御レイヤーが調整され、攻撃トラフィックをフィルタリングする順番が変更されました。Bot Detection の順番が昇格され、パイプラインの早い段階で適用されるようになったのです。

このたった 1 つの変更によって、ログイン画面でのクレデンシャルスタッフィングなどのブルートフォース攻撃が劇的かつ持続的に減少しました。それだけでなく、図 3 の不正登録の分析で明らかになった多くの改善にもつながったと考えられます。これは、防御の階層化に加えて、防御レイヤーの編成を最適化することがいかに重要かを明確に示しています。

図 8：クレデンシャルスタッフィングに起因するログインの試みの割合は、2023 年に大幅に減少した。Customer Identity Cloud の Bot Detection 機能の改善が減少につながっている可能性がある



セグメント分析

テクノロジー全体のデータを業種別のセグメントで見ると（図 9）、クレデンシャルスタッフィングが特定の業種で特に問題になっていることがわかります。

小売 / e コマース企業では、ログインの試み全体の過半数（51.3%）がクレデンシャルスタッフィングに起因しています。ロイヤリティポイントを窃取する、限定商品を不当に入手する、他人の金で商品を購入する、支払い情報を入手するなど、さまざまな理由が考えられますが、サイバー犯罪者がこれらの企業のアカウントを重視しているのは明らかです。

メディア企業でも、クレデンシャルスタッフィング（42.3%）の割合が非常に高く、これは先に説明した理由によるものと考えられます。

ソフトウェア / SaaS / テクノロジー企業は、この割合が 3 番目に高くなっています（32.1%）。この場合、アカウントを直接使用する、あるいはさらに大規模な攻撃で利用し、機密情報にアクセスして外部に送信している可能性があります。たとえば、フィッシング攻撃では、信頼できるサービスを利用していなければ入手できないプロジェクト情報に言及することで、標的を信頼させ攻撃の成功率を高めることができます。

最後に、金融サービス企業でも、クレデンシャルスタッフィング攻撃の割合が平均より高くなっています。この場合、個人情報を窃取して販売する、合成アイデンティティ詐欺に使用する、金融詐欺（取引や送金など）を実行するなど、多くの動機が考えられます。

不正登録と同様に、中規模企業よりも、小規模企業と大企業でクレデンシャルスタッフィングの割合が高くなっています（図 10）。

このデータは、前述の説明を裏付けています。大企業と小規模企業を標的にした攻撃の費用対効果が高い一方で、中規模企業への攻撃は労力に見合わないとサイバー犯罪者が考えている可能性があります。

図 11 に示すように、北米 / 中南米に本社を置く組織に対してクレデンシャルスタッフィングが試みられる割合（28.0%）は、アジア太平洋（13.3%）や欧州 / 中東 / アフリカ（20.2%）に本社を置く組織よりも高くなっています。

小売 / e コマース、メディア、ソフトウェア / SaaS / テクノロジー、金融サービスのグローバル企業の多くは、北米 / 中南米に拠点を置いています。大規模な企業が集中し、サイバー犯罪者が把握している企業が多いために、この地域でクレデンシャルスタッフィングの割合が高くなっている可能性があります。

図 9：小売 / e コマース企業は、非常に高い（平均の 2 倍近い）割合で発生しているクレデンシャルスタッフィングに対処しなければならない

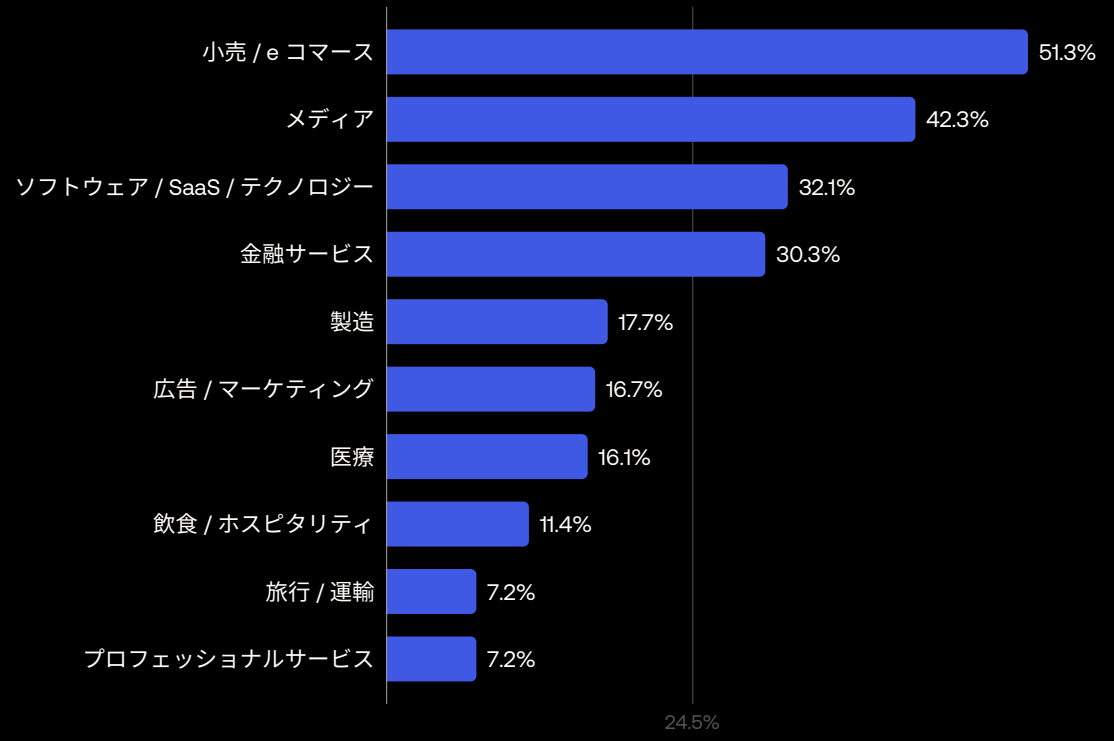


図 10：大企業と小規模企業は、中規模企業よりも魅力的な標的となっている。攻撃が成功した場合の投資対効果（ROI）が労力に見合うとサイバー犯罪者が考えている可能性がある

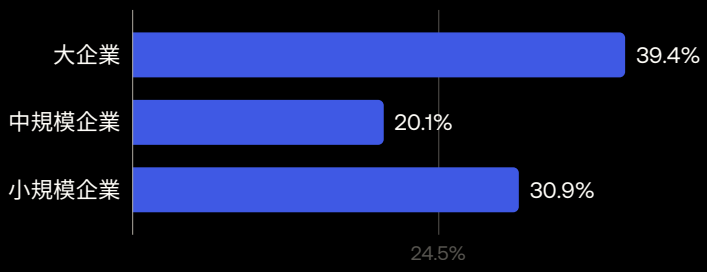
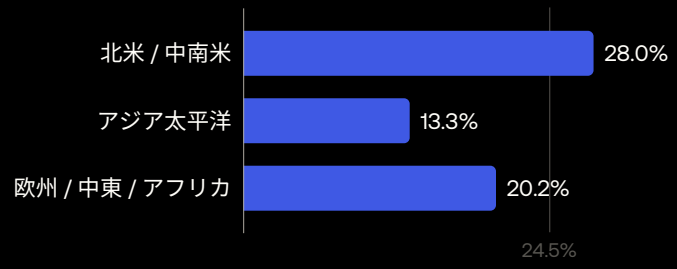


図 11：北米 / 中南米に本社を置く組織でクレデンシャルスタッフィングが試みられた割合は、アジア太平洋や欧州 / 中東 / アフリカに本社を置く組織よりも高くなっている



パスワードが問題を引き起こす

アカウント保有者がいくつものサイトで同じパスワードを使い回したり、類似したパスワードを使用したりすることで、「ドミノ効果」が生じ、一対の資格情報から複数のアプリケーションが侵害される場合があります。

現実的に、ユーザーが今後、自発的にパスワード利用の習慣を変えるとは考えられません。たとえば、Okta の Customer Identity Trends Report 2023 では、以下の状況が明らかになっています。

- 調査回答者の 33% は、特定の要件を満たすパスワードを作成しなければならない場合に不満を感じている
- 25% は、オンラインサービスごとに新しいパスワードを作成する必要があることに不満を感じている

さらに悪いことに、通常、ユーザーアカウント全体のうち、アクティブなアカウントはごく一部でしかなく、その他多くのアカウントは忘れられたか、または放置されています。このように見過ごされているサービスのいずれかを侵害することで、膨大なユーザー資格情報と関連する個人データを取得できます。

また、サイバー犯罪者はこのような情報を大規模に活用する手腕に長けており、ユーザーが他の企業で作成しているアカウントを侵害するために利用します。たとえば、Verizon の Data Breach Investigation Report (DBIR) 2023（2023 年データ漏洩 / 侵害調査報告書）によると、Web アプリケーション侵害の 86% で、窃取された資格情報が使用されています。さらに、資格情報と個人情報は販売されるだけでなく、パスワードの回復フローで悪用される可能性もあります。こうした情報は、窃取され外部に送信される最も多く、常に多くの攻撃を実施するための基盤となっています。

しかし、こうした状況は変えていく必要があり、実際に変わっていくと予想されます。

ユーザーから見た場合、これまでのログインエクスペリエンスは例外的なものとなり、パスワードは最終手段としての認証方法となるでしょう。パスワードへの依存度は低下し、アイデンティティ攻撃も全体として減少すると考えられます。

このような明るい未来については、Authentication after passwords: Maximizing conversions (and enhancing security) in the age of convenience（パスワードに代わる認証方法：利便性が重視される時代にコンバージョンとセキュリティを最大化するには）で詳しく解説しています。このレポートでは、今から実行できる対策も含めて紹介しています。

防御策

繰り返しますが、すでに導入している防御策を基盤として、さらに対策を追加していくことが、ATO の防止に役立ちます。

そのための簡単なアプローチとして、以下の 2 つを利用できます。

- **不可能な移動距離の検知：**「ユーザー」が、前回のログイン成功後に経過した時間内では移動できない場所からサインインを試みていることを検知します。
- **ソーシャルログイン：**ソーシャルログインは、サインアップを簡素化するだけはありません。ユーザーは重要なソーシャルアカウントについては十分な保護対策を行うことが見込まれるため、セキュリティを強化できます。

より高度な手法としては、漏洩パスワードの検知、効果的なパスワード管理（リセットを含む）ポリシーの導入、最高レベルの認証セキュリティのために強力な MFA を要求することが挙げられます。

しかし、パスワードを利用する ATO に対する最も効果的で「シンプル」な防御策は、パスワードからの脱却です。この対策は、共通のパスワードレスサインイン標準のサポートを Apple、Google、Microsoft が約束したことを受けて、より現実的になりました。

パスキー

パスキーは、ブラウザが検出できる FIDO 資格情報であり、ネイティブアプリケーションやパスワードレス認証用のセキュリティキー内に保存されます。FIDO Alliance と World Wide Web Consortium（W3C）の標準に基づくパスキーは、パスワードを暗号キーのペアに置き換えます。ユーザーは、モバイルデバイスのロック解除と同じように、通常は、生体認証を介して、あるいは、デバイスのアクセスコードを入力して、パスキーにアクセスして使用できます。

パスキーには、デバイスに紐づくパスキーと**同期パスキー**の 2 種類があります。

デバイスに紐づくパスキーは、それぞれ単一のデバイスに結びつけられ、所有要素として機能します。これらは、FIDO 認証オーセンティケーターやセキュリティキーで使用でき、セキュリティレベル認証を獲得しているものもあります。

デバイスに紐づくパスキーは、数年前から利用できるようになりました。しかし、特定のデバイスに紐づけられるという特性は、認証セキュリティを強化すると同時に、採用の広がりを阻む要因にもなっています。

対照的に、同期パスキーは、クラウドサービス（オペレーティングシステムのエコシステムやパスワードマネージャーなど）を介してユーザーのデバイス間で同期されます。これは、ユーザーにとって使いやすいものになっています。特にコンシューマー向けサービスで広く採用されるためには、このような利便性が必須条件になると考えられています。

ユーザーがサイトやサービスにログインしようとすると、パスキーを使用するかどうかを尋ねられます。このとき、ユーザーはデバイスで生体認証、PIN、パターンなどを使用して認証するだけでパスキーを利用できるようになります。

サイトやサービスから見ると、パスキーによって、所有要素（同期パスキーの使用が許可されたデバイス）を検証すると同時に、生体要素（生体認証が使用される場合）や知識要素（デバイスのアクセスコードが使用される場合）も検証できます。同期パスキーはこのように、多くのユーザーアカウントのセキュリティを大幅に向上し、パスワードベースの ATO を軽減するために役立ちます。

パスキー入門

どちらの形態のパスキーでも、一般ユーザーに普及すれば、フィッシングやアカウント乗っ取りなどのアイデンティティ脅威への対策は大きく前進します。

詳しくは、パスキー入門：ユーザーエクスペリエンス向上とアカウント乗っ取り防止のために、フィッシング耐性のある FIDO 認証を活用をご覧ください。

漏洩パスワードの検知

現実問題として、現在の脅威環境において、攻撃者の活動を支援するアンダーグラウンドマーケットが存在しています。攻撃者は、侵害された膨大な資格情報のリストを簡単に購入できます。

この資格情報のリストを活用することで、このリストに含まれる侵害されているパスワードをユーザーが使用していることを検知し、関連するリスクに対処できます。アプリケーションプロバイダーがこうした問題が検知されているユーザーに警告を発し、パスワードの変更、強力な MFA への登録などの緩和措置を取るように推奨あるいは要求できます。

専用のパスワードマネージャーや Web ブラウザ / オペレーティングシステムに連携する機能により、ユーザーは長く複雑なパスワードを簡単に作成して安全に保管し、容易に使用できるようになっています。これによって、脆弱なパスワードをユーザーが選択したり使い回したりする原因となる根本的な課題を解決できます。さらに、これらのソリューションの中には、資格情報が漏洩リスト内に見つかったユーザーにアラートを送り、リスクを認識させて対応を促すものもあります。

このような対策によって、漏洩パスワードの利用と脅威が減っていくことが期待されます。

Credential Guard でギャップを埋める

多くの場合、侵害された資格情報がサイバー犯罪のためのアンダーグラウンドマーケットで入手できるようになってから、脅威インテリジェンスフィードに取り込まれるまでには、長いタイムラグがあります。そのため、攻撃者はこれらの情報を長期間悪用しています。

Credential Guard は、このギャップを解決します。専門家チームが犯罪コミュニティに潜入し、セキュリティ侵害が発生した後に迅速に漏洩したデータにアクセスします。こうしたメリットを活かすことで、窃取されたパスワードをより早期にリセットして、ユーザーを保護し、アプリケーションの安全性を確保できます。

詳しくは、Detect Breached Passwords Faster with Auth0 Credential Guard（Auth0 Credential Guard によるパスワード侵害の検知）をご覧ください。

効果的なパスワードポリシー

漏洩パスワードの検知に加え、アイデンティティセキュリティを強化する簡単かつ効果的な方法として、以下が挙げられます。

- 強力なパスワードの作成をユーザーに義務付ける
- そのアプリケーション内でユーザーが過去に使用したパスワードを再利用できないようにする（パスワードのローテーションを防ぐ）
- 強力なパスワードリセットプロセスを導入する

パスワードリセットは、すべてのアプリで必須ですが、パスワードリセットのプロセスが煩雑であれば、顧客がサービスを利用しなくなる原因になりかねません。

Okta の Customer Identity Trends Report 2023 で は、この点に関する状況を以下のように明らかにしています。

- 調査回答者の 63% が、ユーザー名やパスワードを忘れてアカウントにログインできないことが月に 1 回以上あると回答している
- 24% は、週に一度の頻度でこの問題に遭遇している
- 6% は、毎日この問題に遭遇している

また、パスワードリセットは日常的に起こり得ることですが、特に B2C の顧客は、このプロセスを面倒と考える可能性があります。そのため、コンバージョンの低下だけでなく、ユーザー離れにもつながりかねません。実際に、すべてのアカウントへのアクセスを維持していると報告した回答者は 52% にとどまります。

優れたパスワードリセットプロセスは、以下の 2 つの条件を満たします。

1. **顧客が経験する摩擦を最小限に抑える：**パスワードリセットに 1 分以上かかることは避けなければなりません。また、顧客に要求する情報は、メールアドレスなど、ためらわずに入力できる情報にとどめるべきです。
2. **顧客の情報を保護する：**たとえば、何度もログインに失敗するようなケースに対しては安全策を講じたり、安全なチャネルでのみ情報を送信したりする必要があります。

メールがパスワードリセットに最もよく使われるのは、両方の条件を満たすためです。メールアドレスは、顧客がすばやく簡単に入力できる情報であるため、摩擦を最小限に抑えることができます。また、その顧客だけが受信トレイにアクセスできることを前提としていますが、顧客の情報を保護できます。

パスワードリセットのプロセスを少しでも間違えると、製品のカスタマーエクスペリエンス全体が大きく低下する恐れがあります。次のようなミスが多く見られています。

- **セキュリティの質問：**出身校、母親の旧姓、ペットの名前などの静的な情報は OSINT から簡単に入手できます。
- **プレーンテキストのパスワード：**パスワードをリセットする代わりに、元のパスワードを顧客に送り返すサイトがありますが、これは重大な脆弱性となります。プレーンテキストのパスワードを送信している場合、プレーンテキストでパスワードが保存されていることになり、攻撃を受ける可能性が高まります。
- **エラーメッセージ：**メールアドレスが登録されているかどうかをアプリケーションが表示する場合、顧客がアカウントを保有しているかどうかを攻撃者が把握できる可能性があり、顧客に関する情報を攻撃者に提供することになります。
- **不必要な情報の要求：**セキュリティと使いやすさのバランスを取ることが重要です。たとえば、写真付き身分証明書の提示を顧客に求めることは安全な対策ではありますが、カスタマーエクスペリエンス全体にマイナスの影響を及ぼします。

強力な多要素認証（MFA）

MFA を使用してアカウントを保護することで、アカウントを乗っ取るために攻撃者が費やす時間、労力、そして最終的にはコストは大幅に増加します。

しかし実際には、以下の 2 つの問題のために、ATO 対策としての MFA の効果が限定されています。

1. アプリケーションプロバイダーによる採用率や顧客の利用率が低い
2. 第 2 要素の使用を攻撃者が回避できる

本レポートでは、MFA の採用、登録、利用については深く掘り下げませんが、利用可能なデータをもとに、このテーマについて少し見てきましょう。

たとえば、すべてのデータセットを見ると、有効な MFA の試みに対するパスワード認証イベントの合計数の比率は、およそ 41 対 1 です。つまり、1 回の有効な MFA の試みに対して、約 41 回のパスワード認証が行われています。

この比率をもとに、業種別の MFA 利用率を割り出し、比較できます（図 12）。

その結果、MFA の利用率が平均より高い（有効な MFA の回数に対するパスワード認証の合計数の比率が低い）のは、代表的な 10 業種中 3 業種だけであることがわかります。

金融サービスでは、1 回の有効な MFA の試みに対して、12 回のパスワード認証が行われています。製造の場合、この比率は 24 対 1 となり、金融サービスの 2 倍ですが、プロフェッショナルサービスの 37 対 1 に比べると非常に低くなっています。

また、代表的な 10 業種中、飲食 / ホスピタリティ（137）、メディア（155）、広告 / マーケティング（400）の 3 業種では、パスワード認証の比率が極めて高く、MFA の利用が相対的に少ないことがわかります。

さらに、代表的な 10 業種以外についても調べたところ、パスワード認証の比率が平均より低い業種が 5 つありました（図 13）。法律サービス（4）、通信（6）、公共部門（6）の 3 業種では、MFA の利用率が極めて高くなっています。いずれも機密データや重要インフラストラクチャを対象とする業種であることから、MFA の利用率が高いことは歓迎すべきことです。

上記の比率は、あくまでも暫定的な指標ですが、特定の業界、特に機密データやシステムを扱う業種で、相対的に MFA の利用率が高いことを強く示しています。

しかし、アイデンティティの防御が全般的に強化され、MFA の採用が徐々に拡大する中で、攻撃者はこうしたセーフガードを突破することに注力するようになっています（図 14）。

図 12：規制の厳しい業界では MFA 利用率が比較的高い傾向がある。金融サービスと医療では、パスワード認証の利用率が（データセット内の代表的な 10 業種中）ほぼ平均、または平均より低い

（2023 年のデータセット内で最も代表的な 10 業種）

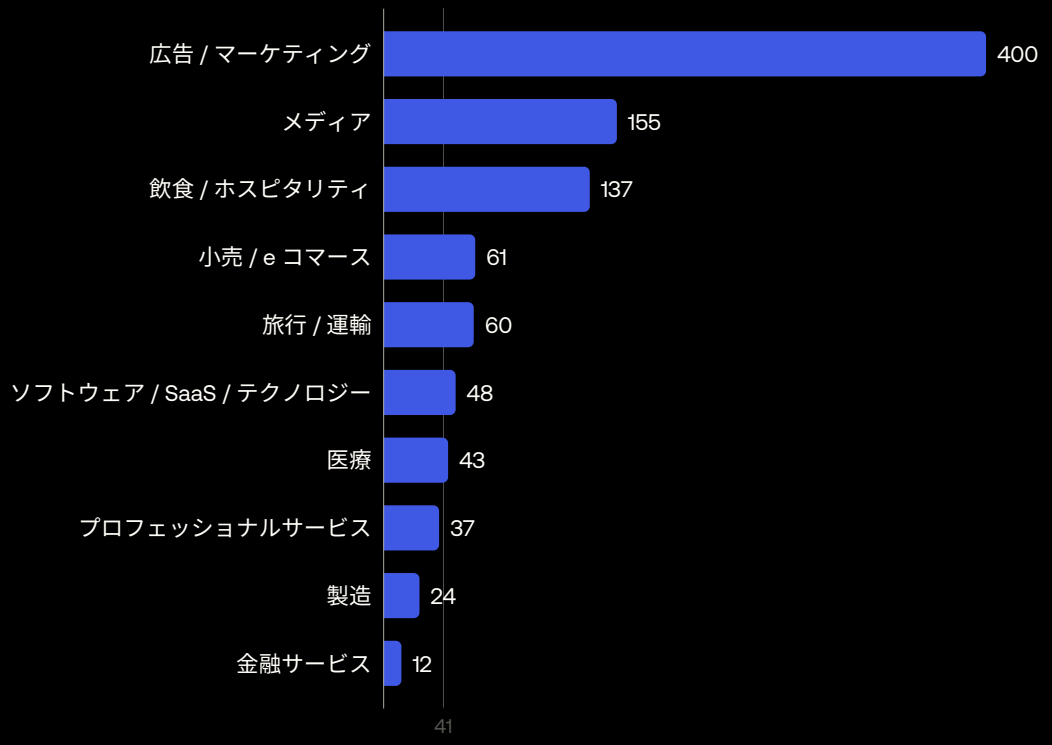
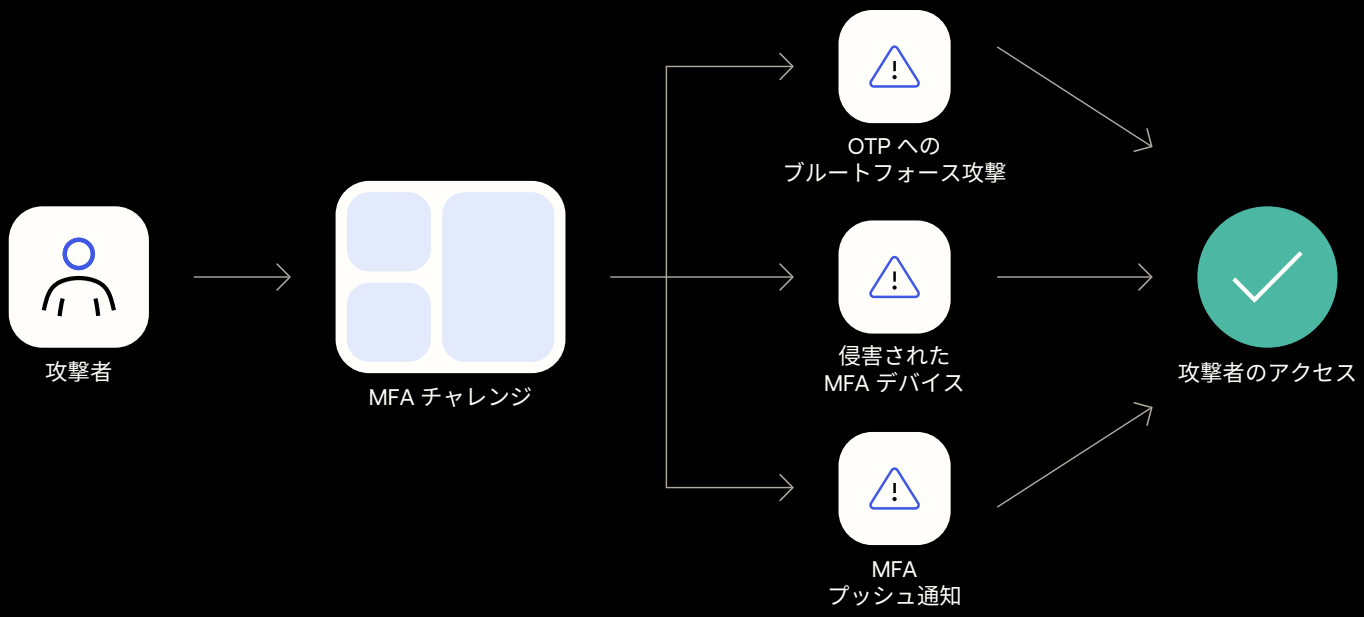


図 13：代表的な 10 業種以外では、5 業種で MFA 利用率が平均を上回っている有効な MFA の試みに対するパスワード認証の比率

（2023 年の代表的な 10 業種以外の注目すべき業種）

図 14：一般的な MFA バイパス手法の手口



たとえば、比較的弱い第 2 要素、中でも SMS で配信されるワンタイムパスワード（OTP）を簡単に攻撃できるツールがいくつか登場しています。最も一般的な攻撃ベクトルは、ブルートフォース攻撃によって **MFA 疲労**を引き起こし、ユーザー自身が要求していない MFA チャレンジをユーザーに完了させるように誘導 / 強要するものです。MFA チャレンジにユーザーが不用意に応答すると、攻撃者はログインできるようになります。

さらに、脅威者は MFA のセーフガードを回避するために、**SIM スワッピング**や**ソーシャルエンジニアリング**を利用しています。

SIM スワッピングでは、標的ユーザーが契約している携帯電話会社に、攻撃者が連絡し、ユーザーの携帯電話番号を攻撃者の所有する SIM カードに切り替えます。攻撃者は、ヘルプデスク担当者を騙すなどのソーシャルエンジニアリング、悪意ある内部関係者、または通信事業者の管理サービスへの不正アクセスによって、SIM を交換する場合があります。

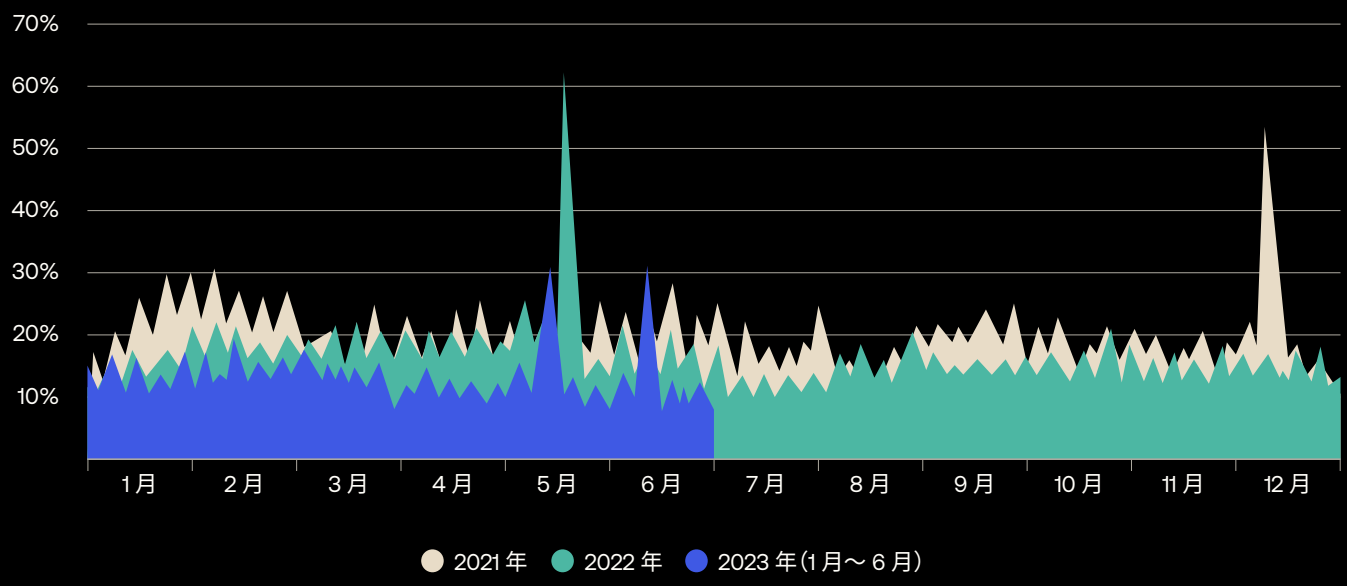
SIM の交換によって、電話番号を利用しているあらゆる MFA 要素（SMS OTP、SMS マジックリンク、音声 OTP など）を攻撃者が利用できるようになります。

攻撃者は、アプリケーションプロバイダーに対してソーシャルエンジニアリングを直接実行することもあります。たとえば、何らかの個人情報（多くの場合、OSINT を通じて容易に購入または入手できる情報）を入手した攻撃者が、ヘルプデスク担当者にアカウントの詳細を変更するよう仕掛ける可能性があります。また、攻撃者は、ユーザーを騙して特定のアカウント保護機能を無効にするため、ユーザーに直接接触する場合もあります。

残念ながら、ソーシャルエンジニアリングの実行コストは下がり続けています。AI や自動化などによる効率性の向上、大規模なデータ侵害や流出、そして多くのユーザーがオンライン（ソーシャルメディアなど）で積極的に情報を共有していることなどが、その理由となっています。

このため、今日の組織と顧客にとって、MFA バイパスは現実に起こり得る大きなリスクです。2023 年上半期（図 15）には、Customer Identity Cloud で MFA の試みの 12.7% が MFA バイパスと判定されました。この割合は、2022 年（15.5%）および 2021 年（18.1%）から低下していますが、脅威が縮小したというよりも、攻撃者による戦術が転換したことに起因するものと思われます。

図 15：MFA バイパスは 2021 年と 2022 年に比べて減少している。しかし、ソーシャルエンジニアリングの実行コストが低下し続けているため、攻撃者は引き続き MFA バイパスに注力している



興味深いことに、MFA バイパスが試みられる割合が平均を上回ったのは、代表的な 10 業種中メディア（12.8%）のみであり、しかも平均をわずかに上回る程度でした（図 16）。全体の平均を押し上げているのは、公共部門（29.9%）、娯楽（28.6%）、そして業種を特定しなかった回答者です。

この脅威は、特に小規模企業で広く見られ（図 17）、MFA の試み全体の 2 割以上（20.3%）が MFA バイパスと判定されました。

図 16：一部の業界では、MFA バイパスの試みが平均的、または平均を下回っており、旅行 / 運輸で特に低い（データセット内の代表的な 10 業種中）ことが朗報である

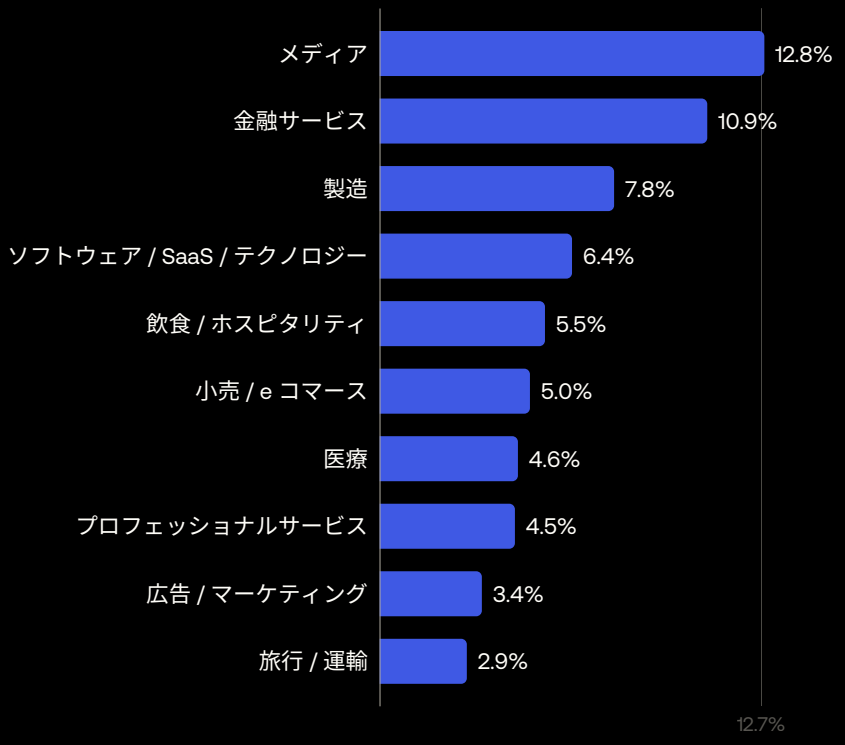
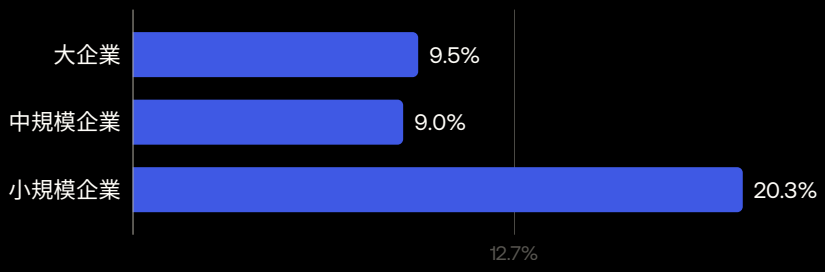


図 17：小規模企業では、MFA バイパスが試みられた割合が大企業や中規模企業よりも高い



脅威環境が急速に進化し危険性が増大していることから、MFA ソリューションの導入では以下の点を確保することが不可欠です。

- **適切な実装：**「レガシーの認証がサポートされる」「管理者が MFA を迂回できる」など、セキュリティ上の問題を起こしかねない実装である場合には、悪用される可能性があります。
- **強力な第 2 要素の使用：**MFA バイパスは、SMS に依存する要素などの一般的に古い要素を狙い、ブルートフォース攻撃は依然として知識要素に基づくオーセンティケーターを主な攻撃対象としています。このため、所有要素または生体認証要素に基づくオーセンティケーターを使用することで、ブルートフォース攻撃が成功する可能性を劇的に低減できます。

前述したように、コンシューマーアプリケーションでセキュリティ効果を高めるテクノロジーについては、セキュリティと使いやすさのバランスをとる必要があります。古い認証手法では、多くの場合、何らかのトレードオフが求められます。

しかし、このトレードオフは、間違った選択につながることが多くあります。

- **アダプティブ MFA：**柔軟で拡張可能な MFA ポリシーによって、正規ユーザーの摩擦を増やすことなく ATO を防止できます。ログイントランザクションで潜在的なリスクを評価し、必要な場合にのみユーザーに追加の確認を求めます。
- **安全かつ便利な新しい MFA 手法：WebAuthn** 対応デバイスの生体認証（Apple Face ID、Apple Touch ID、Windows Hello など）や、WebAuthn 対応のセキュリティキー（YubiKey、Feitian、Titan など）に基づく MFA は、強力なセキュリティ（攻撃者は WebAuthn を嫌う）と使いやすさを同時に実現し、本レポートの冒頭に示した理想的な認証ソリューションにさらに一歩近づく手法です。

コンシューマーの間で専用セキュリティキーの採用が拡大する可能性はまだ低いとはいえ、手頃な価格のデバイスでも生体認証が採用されることは一般的になりつつあります。生体要素を使ったユーザー認証をデバイスで可能にすることには、以下の 2 つの利点があります。

- 認証チャレンジ中の摩擦を大幅に軽減するため、ユーザーの定着と収益性が高まる
- 攻撃者は認証フローを「フィッシング」できないため、セキュリティが向上する

パート3:
認証後の対策

カスタマーアイデンティティと関連する権限 / 特権の保護は、認証時に完結するわけではありません。ユーザーのセッションが続く限り、保護を継続しなければなりません。


BICYCLES

パート３：認証後の対策

パスワードレス化で重要性が高まるセッショントークン

アプリケーションでユーザーを認証した後に、ブラウザは Web Cookie を保存します。Web Cookie に含まれるセッショントークン（アプリケーションによって生成される特定のデータブロック）によって、サインインしたユーザーを追跡でき、セッションが期限切れになるか、ユーザーがログアウトするまで、再度サインインする必要がなくなります。

攻撃者がセッションの Cookie を窃取してブラウザで悪用すると、多くの場合、セッションが有効である限り（有効期間はアプリケーションプロバイダーによって異なります）、正規ユーザーと同じセッションにアクセスできます。

以下のような多くの方法により、セッショントークンの侵害が可能になります。

- **クライアント側の攻撃**（T1539、T1185 など）：クライアントからセッショントークンを抽出する方法は、クロスサイトスクリプティング（XSS）、悪意ある JavaScript、マルウェアなど数多くあります。特に、現在蔓延しているマルウェアの多くは、Cookie を抽出する機能を持つ「情報窃取」モジュールを含んでいます。

- **中間者（AiTM）フィッシング攻撃**（T1557、T1566、T1539 など）：攻撃者は、ソーシャルエンジニアリングを利用して、ユーザーを悪意あるWeb サイトに誘導します。こうした Web サイトは、なりすました Web アプリケーションと標的ユーザーの間で要求を中継するリバース HTTP プロキシサーバーとして透過的に構成されています。騙されたユーザーがこれらの悪意のあるサイト経由で正規の Web アプリケーションにサインインすると、攻撃者はユーザーの資格情報とブラウザに返されたセッショントークンにアクセスできるようになります。攻撃者は、悪意あるアクセスポイントを利用してネットワークトラフィックを読み込み、セッショントークンを確認および窃取する場合があります。

セッションハイジャックが大規模に実行される場合もありますが、どちらかというと、高価値の企業の従業員に対する標的型攻撃で利用されることが多くなっています。

しかし、パスワードレス認証の採用が徐々に増加するにつれて、攻撃者はセッションハイジャックの TTP を高度化するため、さらに労力を投じるようになると予想されます。

セッショントークンも販売対象

窃取されたセッショントークンの多くは、その後にサイバー犯罪向けのマーケットで販売されます。特定の企業アカウントを侵害しようと狙っている攻撃者は、その企業のセッショントークンを購入できます。多くの場合、セッショントークンは数十ドル程度で入手できます。

後述するように、このリスクに対処する方法の1つは、セッションの最大時間を短くすることです。その場合でも、ユーザーが直接標的にされるケースには対処できません。しかし、トークン（および資格情報）が収集されてからアンダーグラウンドマーケットに売りに出されるまでにタイムラグがあることが多いため、市場で販売される情報窃取マルウェア対策としては非常に効果的です。

防御策

セッションハイジャックを防ぐためには、以下の 3 つの方法でセッションのセキュリティを向上できます。

- セッショントークンを URL に含めない
- サーバーサイドのセキュアなセッションマネージャーを使用して、予測不可能な新しいセッショントークンをログイン後に生成する
- セッショントークンを安全に保存し、ログアウト後に無効にする
- セッションの最大時間を短くする

大局的には、アプリケーションプロバイダーは、再認証が正当化される状況では、ユーザーを再認証することも検討すべきです（この問題については以下で説明します）。

アプリケーションセッション管理のベストプラクティス

アイデンティティプロバイダー（IdP）が関与する場合、アプリケーションセッションの管理は非常に困難になることがあります。また、最初に思いつく解決策が不十分であることも少なくありません。

詳しくは、Best Practices for Application Session Management（アプリケーションセッション管理のベストプラクティス）をご覧ください。

ステップアップ認証

繰り返し述べてきたように、セキュリティと使いやすさのバランスを取ることは、優れたユーザーエクスペリエンスを実現するために不可欠です。

アプリケーションプロバイダーによるステップアップ認証では、アイデンティティの要求を、リソースの重要性とリソースが侵害された場合のリスクレベルに合わせながら、このバランスを詳細に調整できます。

こうした階層型のアプローチでは、ユーザー（またはユーザーを装う可能性のある者）は、1つの資格情報で一部のリソースにアクセスできますが、機密性の高いリソースへのアクセスを要求する際には、MFA などの追加の資格情報を求められます。

ステップアップ認証に関するリスクは、その実装にあります。効果的な実装を実現するには、慎重に計画しなければなりません。

継続認証

ユーザーが最初に認証チャレンジを通過できた場合でも、長時間にわたってアクセスを提供してよいわけではありません。

認証システムは、必要に応じて、ユーザーの位置情報、デバイス、アプリ、利用パターン、時間帯、入力行動などのシグナルを継続的に監視し、引き続き十分に信頼できるかどうかをチェックし、これによって継続的なアクセスを許可する必要があります。

この「継続認証」は、セキュリティとユーザーエクスペリエンスの両方を高めるため、非常に強力であり、パスワードだけを使用する場合と比較して、信頼性が大幅に高まります。

しかし、カスタマーアイデンティティで継続認証を利用するには、詳細な同意をユーザーから継続的に得なければならず、何らかの形でデバイスを監視する必要が生じる可能性もあります。こうした要件のため、継続認証ソリューションの用途は、B2B のシナリオや、金融、医療など機密性の高い B2C のユースケースに限定されています。

顧客のセキュリティとエクスペリエンスをCIAMで向上

CIAM は、ユーザーエクスペリエンス、セキュリティ、プライバシーのニーズを同時に満たすために、拡張性に優れる方法で実装しなければならず、CIAM を適切に導入することは、あらゆる組織にとって大きな課題です。

- 顧客向けのシステムは、市場分析のためのインプットを提供し、顧客獲得、コンバージョン、顧客維持に大きな影響を与えます。CIAM はこれらのシステムの中核に配置されるため、マーケティングやカスタマーエクスペリエンスを担当する部署と連携して導入を進める必要があります。
- 同時に、CIAM はセキュリティとプライバシーでも大きな役割を果たすため、CISO、CIO、コンプライアンス責任者とも緊密に連携しなければなりません。
- また、CIAM は基本的に、テクノロジーソリューションの一つであるため、デジタルトランスフォーメーションを推進するイネーブラーとして認識される場合には、IT 組織や CTO とも連携することになります。

これらの部門のリーダーは、望まれるユースケース、顧客のタイプ、データのタイプ、業界固有のリスク、許容できるリスクレベルを検討し、カスタマーエクスペリエンスとシステムセキュリティのバランスをとりながら、CIAM の導入に向けて協力し合う必要があります。

カスタマーアイデンティティの保護

現在の高度なアイデンティティ攻撃を阻止し、サイバー犯罪のビジネスモデルを破壊し、優れたユーザーエクスペリエンスを維持するには、さまざまなレイヤーで機能するセキュリティツールを組み合わせて、包括的な防御策を構築する必要があります。

これらのツールを個別のソリューションとして調達、統合、構成し、継続的に監視、調整、オーケストレーションするには、極めて特殊なスキルが必要とされ、運用にも多大な注意を払わなければなりません。また、自社のコアビジネスを推進するための貴重なリソースを、これらの対策に割かなければならなくなります。

こうした点を含め、さまざまな理由から、アイデンティティスタックを社内で構築して維持することは最善のオプションではありません。それに代わるアプローチとして、「セキュアバイデザイン」に基づく多層防御の俊敏なアーキテクチャを備えた、ベストオブブリードのCIAMソリューションによって、効果的にアイデンティティセキュリティを達成できます。

カスタマーアイデンティティのベストプラクティス10選

ソリューションを自社開発する場合も、IDaaS（Identity-as-a-Service）プロバイダーを利用する場合も、以下の基本的な推奨事項に留意してください。

- **汎用的なエラーメッセージを使用する：**エラーメッセージに詳細情報を表示すると、システム内のユーザーに関する情報を提供し、攻撃者に悪用される恐れがあります。攻撃者にヒントを与えることがないように、汎用的なエラーメッセージだけを表示するようにします。
- **セキュアなセッション管理を実装する：**サーバーサイドのセキュアなセッションマネージャーを使用し、ログイン後に新しいセッションIDを生成します。URLにはセッションIDを含めず、セッションIDは安全に保存し、ログアウト後に必ず無効にします。
- **デフォルトの資格情報のまま提供しない：**多くの組織は、管理者のデフォルトの資格情報をそのまま利用しています。この情報は重大な攻撃ベクトルとなります。新しいデバイスや新しいユーザーをプロビジョニングするときには、デフォルトの資格情報を使用したくなるかもしれませんが、OpenID Connectのようなテクノロジーを使うか、パスワードレス認証を採用するか、初回ログイン時にパスワードを設定することをユーザーに強制することが推奨されます。
- **パスワードをプレーンテキストで保存しない：**パスワードデータベースが完全に判読できなければ、ハッカーにとって何の価値もありません。暗号化により、組織が標的となるリスクは低下しますが、暗号化を適切に実装しなければなりません。

次に、基礎的な防御策を導入します。

- **ログイン失敗回数を制限する：**クレデンシャルスタッフィングのようなブルートフォース攻撃は、失敗を繰り返しながらログインを成功させようとします。この動作を利用して攻撃を検知し、適切な対策を行います。
- **強力なパスワードを適用する：**多くのブルートフォース攻撃では、脆弱なパスワードやよく使われるパスワードが利用されます。NIST が推奨しているような根拠あるポリシーに基づいて、パスワードの長さ、複雑さ、ローテーションを適用します。
- **漏洩パスワードの使用を監視する：**多くのユーザーは、複数のサイトで同じパスワードや類似のパスワードを再利用しています。このため、いずれかのサイトが侵害されると、他の多くのサービスも侵害される恐れがあります。資格情報が侵害された場合、ユーザーに情報を変更させる必要があります。

最後に、より強力な認証メカニズムを採用しましょう。

- **パスキーを奨励する：**パスキーは強固な認証セキュリティを提供し、同期パスキーはコンシューマーユーザーの広い採用に役立つ便利なユーザーエクスペリエンスを提供します。
- **強力な MFA を提供する：**MFA を導入する場合は、優先的にオーセンティケーターアプリと WebAuthn ベースの手法を利用しましょう。すでに MFA をサポートしている場合は、これらの強力な二要素認証方法を使用するようにユーザーを促し、従来のアプローチから脱却するように取り組んでください。
- **アダプティブ MFA とステップアップ認証を採用する：**新たな摩擦の発生が特に心配される場合は、アダプティブ MFA とステップアップ認証を活用することで、セキュリティとユーザーエクスペリエンスのバランスをきめ細かく調整できます。

Auth0 by Oktaのアイデンティティ管理について、詳しくご確認ください。

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、どんなテクノロジーでも安全に利用できるように支援しています。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/jp をご覧ください。

Auth0 は、Okta および Okta の主力製品である Okta Customer Identity Cloud の基盤テクノロジーです。開発者は Auth0.com で詳細を確認し、無料でアカウントを作成できます。

免責事項

あとがき

今後注目される認可

今後数か月、数年、数十年で、デジタルアイデンティティの重要性は確実に高まるでしょう。その結果、カスタマーアイデンティティを管理し保護する能力が、あらゆるデジタル上でのやりとりにとって重要な基盤となります。

これまで見てきたように、カスタマーアイデンティティに対する脅威は拡大し、高度化し、そして進化しています。つまり、CIAM サービスには、常に予測し、反応し、適応する能力が求められています。

たとえば、パスキーの採用が拡大すると、サイバー犯罪者は認証後のセキュリティを侵害するための TTP に注力するようになり、セキュアなセッションの管理、ステップアップ認証、継続認証の重要性が高まると予想されます。

しかし、認証は CIAM の 1 つの側面にすぎません。認可は、ユーザーがアクセスできるリソースを決定するプロセスであり、あまり注目されていませんが、認証と同等に重要です。権利、情報、サービス、その他の特権は、ますますデジタルアイデンティティによって制限されるようになっています。これに伴い、パーソナライズされたサービスを実現するイネーブラーとして、また、侵入やそれに伴うデータ侵害に対する重要な防御策として、今後は認可への注目が高まると予想されます。

最終的に、カスタマーアイデンティティを保護することは、信頼を確立して維持し、実際の生活で実在の人物や組織と安心して関わり合うことができるようにすることなのです。

アイデンティティ保護の重要性は、Okta のコミットメントと同様、これ以上ないほど高くなっています。

Shiven Ramji
Okta、Customer Identity Cloud 担当プレジデント

付録

付録

付録 A：用語集

本レポートで使用している専門用語について、以下に解説します。

- **アカウント乗っ取り（ATO）：**IAM システムに対する多くの攻撃の目的。正規ユーザーが所有する既存のアカウントに攻撃者がアクセスして制御できるようになる
- **アダプティブ多要素認証（MFA）：**柔軟で拡張可能な MFA ポリシー。現実のユーザーの摩擦を増加させることなく、攻撃者からアプリケーションを保護する上で役立つ。このアプローチは、すべてのログイントランザクション中に潜在的なリスクを評価し、必要に応じてユーザーに追加の確認を求める
- **認証：**デジタルアイデンティティの確認（アプリがユーザーを識別する方法）
- **認可：**ユーザーがアクセスできるリソースを決定するプロセス（アプリがユーザーに許可する対象を決定する方法）
- **カスタマーアイデンティティ：**企業が顧客について継続的に学び、顧客がどのような人物であり、どのようなエンゲージメントを望んでいるかを理解することで、同意に基づく信頼を安全に構築する方法
- **カスタマーアイデンティティ & アクセス管理（CIAM）：**企業がエンドユーザーにデジタル資産へのアクセスを与える方法と、ユーザーのデータを統治 / 収集 / 分析し、安全に保存する方法
- **デバイスに紐づくパスキー（device-bound passkey）：**特定のデバイスに紐づけられたパスキー。これによって所有要素を証明する
- **デジタルアイデンティティ：**アプリケーションのコンテキストで、特定のユーザーを定義する属性のセット
- **エンティティ：**属性の変更とは無関係に存在する、単一で識別可能なオブジェクト。CIAM のコンテキストでは、エンティティは通常、ユーザー、デバイス、またはコンピューティングリソース（システムやアプリケーション）のいずれかを指す
- **FIDO：**「Fast Identity Online」の略。FIDO Alliance（パスワードへの世界的な過度の依存を低減するために、認証標準を開発・支持することを重点的な使命とするオープンな業界団体）の短縮形として使用される
- **摩擦：**デジタルの世界において、人とサービスのやりとりを遅らせる、あらゆる手間やストレスを指す。これらのやりとりには、ユーザーのサービスへのサインアップ、既存アカウントへのログイン、紛失したアカウント情報の回復、購入のチェックアウトなどが含まれる
- **侵入：**権限のないユーザーがシステムまたはシステムリソースにアクセスするセキュリティイベント（または複数のセキュリティイベントの組み合わせ）
- **マジックリンク：**認証 API によって生成されるリンク。ユーザーに送信され、リンクをクリックすると、ユーザーが直接ログインする（マジックリンクは、ユーザーが OTP を含むメールを受信し、アプリケーションに戻り、OTP を入力するのと同様の機能だが、実際にこれらの手順を実行する必要はない）
- **MFA 疲労：**攻撃者が大量の MFA 通知をユーザーに送りつけ、受け入れ / 承認させることで、アカウントやデバイスへの侵入を可能にする手法

- **多要素認証（MFA）：**複数の要素（顔、指紋、声などの生体要素、ワンタイムパスコード、オーセンティケーターアプリケーションなど）を必要とするユーザー認証方法
- **ワンタイムパスコード / パスワード（OTP）：**認証 API が生成する、1回のログインまたはトランザクションでユーザーを認証するための数字または英数字のシーケンス
- **OSINT（Open Source Intelligence）：**一般に公開され、法的にアクセス可能な情報（SANS による）の収集、分析、伝播
- **パスキー：**ブラウザが検出可能な FIDO 資格情報。ネイティブアプリケーションやパスワードレス認証用のセキュリティキー内に格納される
- **パスワードレス：**「パスワードレス認証」の短縮形。パスワードを入力することなくユーザーを認証する仕組み
- **フィッシング攻撃：**ソーシャルエンジニアリングの手法。通常、欺瞞、圧力、または操作を使ってユーザーを騙し、機密情報を共有させる
- **SIM スワッピング：**攻撃者が、標的ユーザーの携帯電話会社を説得して、ユーザーの携帯電話番号を攻撃者の所有する SIM カードに切り替えさせることで、ユーザーの携帯電話番号をコントロールできるようにする手法
- **シングルサインオン（SSO）：**単一のアイデンティティで一度ログインしたユーザーが、認証要素を再入力することなく、他の独立したシステムにアクセスできるように許可する認証ソリューション
- **ソーシャルエンジニアリング：**標的を騙して機密情報を開示させたり、攻撃者に代わって何らかのアクションを実行させたりすることを目的とした戦術や手法を包括的に指す用語
- **ソーシャルログイン：**多くの場合にソーシャルネットワークプロバイダーが提供する単一のアカウントを使って、複数のアプリケーションやサービスにログインできるシングルサインオンの実装
- **スピアフィッシング攻撃：**標的（個人または組織など）を絞ったフィッシングの形態。フィッシングでは標的の関連する情報や詳細が収集され使用されることが多い
- **ステップアップ認証：**ユーザーが1つの資格情報である程度の範囲のリソースにアクセスできるようにしながら、機密性の高いリソースへのアクセスには追加の資格情報を求めることで、セキュリティと摩擦の適切なバランスを取ることを目指した認証アプローチ
- **同期パスキー：**複数のデバイス間（オペレーティングシステムのエコシステム内、パスワードマネージャー経由など）で安全な共有が可能なパスキー
- **WebAuthn：**「Web Authentication JavaScript API」標準の短縮形。FIDO2 仕様の一部を成す

付録

付録 B：調査手法

本レポートでは、全世界のさまざまな規模の数千社の組織に CIAM 機能を提供している Okta Customer Identity Cloud, powered by Auth0 から得られたデータを使用しています。

具体的には、レポートは毎日のイベントログを分子（不正サインアップイベントなど）と分母（サインアップイベント総数など）に合計し、脅威のトレンドを有意に正規化し、Customer Identity Cloud の顧客構成の継続的な変化を管理しています。

イベントデータは、テナントの業種（回答者自身が特定）、規模（小規模企業、中規模企業、大企業の区分から選択）、本社所在地のデータがある場合に、こうした情報と結合された後、匿名で集計されています。

本レポートは、現実の本番環境に基づき、Customer Identity Cloud 上の実際の活動データを取得したものです。したがって、本レポートの形成には、各顧客が有効にした製品 / 機能（および構成）、並びにこうした製品 / 機能の能力の進化という 2 つの要因が大きく影響しています。

Customer Identity Cloud を最も多く利用している代表的な 10 業種を決定するため、Okta は以下の 4 つの要素に基づいて各業種をランク付けしました（2023 年 1 ～ 6 月の半年間が対象）。

- テナント数
- サインアップイベントの合計
- パスワード認証イベントの合計
- MFA の試みの合計

平均のランキングが最も高い 10 業種を、最も代表的な業種とみなしました。

サブセット分析で利用されている属性（業種、組織規模、本社所在地）は、すべての顧客 / テナントについて利用可能とは限りません。したがって、こうした属性に基づく全世界の集計を示すグラフは、すべてのテナントを含むわけではありません。たとえば、図 3 は全テナントのデータに基づいていますが、図 6 は以下に該当するテナントのみを含みます。

- 本社所在地のデータがある
- その本社所在地が、北米 / 中南米、アジア太平洋、欧州 / 中東 / アフリカのいずれかの地域である

つまり、図 6 には、本社所在地のデータがないテナントや、本社所在地が上記 3 地域以外のテナント（アフリカなど）のデータは含まれません。

こうしたサブセットの影響を受ける極端なケースとして、3 つの主要地域すべてで、MFA バイパスが試みられた割合が全世界平均を下回るという結果になりました。簡単に説明すると、3 つの主要地域以外に拠点を置く顧客や、本社所在地のデータがない顧客も全世界平均に寄与しており、特に MFA バイパスについては、北米 / 中南米、アジア太平洋、欧州 / 中東 / アフリカに拠点を置く顧客よりも割合が高くなりました。

付録

付録 C：業種別の要約

以下のサブセクションは、2023 年のデータセットで代表的な 10 業種についての補足説明です。

広告 / マーケティング

製品やサービスをサポートするため、オーディエンスに情報を提供し関与するキャンペーンの作成、宣伝、配信を行う

金融サービス

銀行、保険、ウェルスマネジメント、その他の資本を管理分配するためのサービスを提供する

飲食 / ホスピタリティ

食品飲料の生産流通および関連サービス、ホテルやレストランなどのレジャー活動や宿泊施設を含む

医療

医療提供者、支払者（医療保険など）、製薬会社、ヘルスケアテクノロジーを含む

製造

家電製品から自動車まで、物理的な財の生産を含む

メディア

ニュース、娯楽、広告などのコンテンツを制作、配信、放送する組織を含む

プロフェッショナルサービス

法律、コンサルティング、会計、マーケティングなど、ビジネスニーズをサポートする幅広いサービスを含む

小売 / e コマース

実店舗またはデジタルプラットフォームを通じて、コンシューマー向けの商品やサービスの販売流通に従事する組織を含む

ソフトウェア / SaaS / テクノロジー

Software-as-a-Service（SaaS）やテクノロジーを含むソフトウェアの開発、流通、サポートを中心とする

旅行 / 運輸

航空会社、鉄道会社、ホテル、旅行代理店、および人やモノの移動を専門とする関連サービスを含む

表 2：広告 / マーケティング

広告 / マーケティング組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	1.4%	1.5%	1.0%
クレデンシャルスタッフィングの試み	2.7%	4.9%	16.9%
MFA バイパスの試み	17.6%	4.1%	3.4%

表 3：金融サービス

金融サービス組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	23.4%	50.8%	28.8%
クレデンシャルスタッフィングの試み	46.6%	41.8%	30.3%
MFA バイパスの試み	3.7%	4.8%	10.9%

図 18：広告 / マーケティング組織に対するアイデンティティ脅威の 30 か月日次ビュー

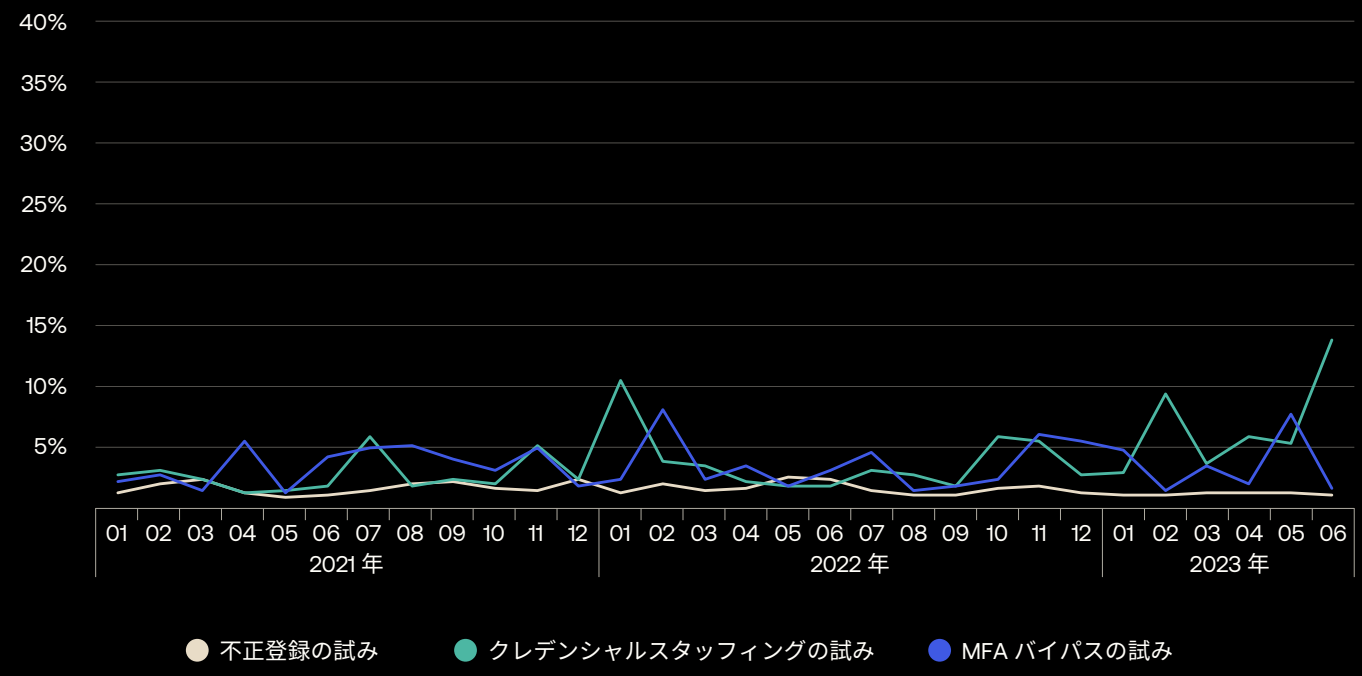


図 19：金融サービス組織に対するアイデンティティ脅威の 30 か月日次ビュー

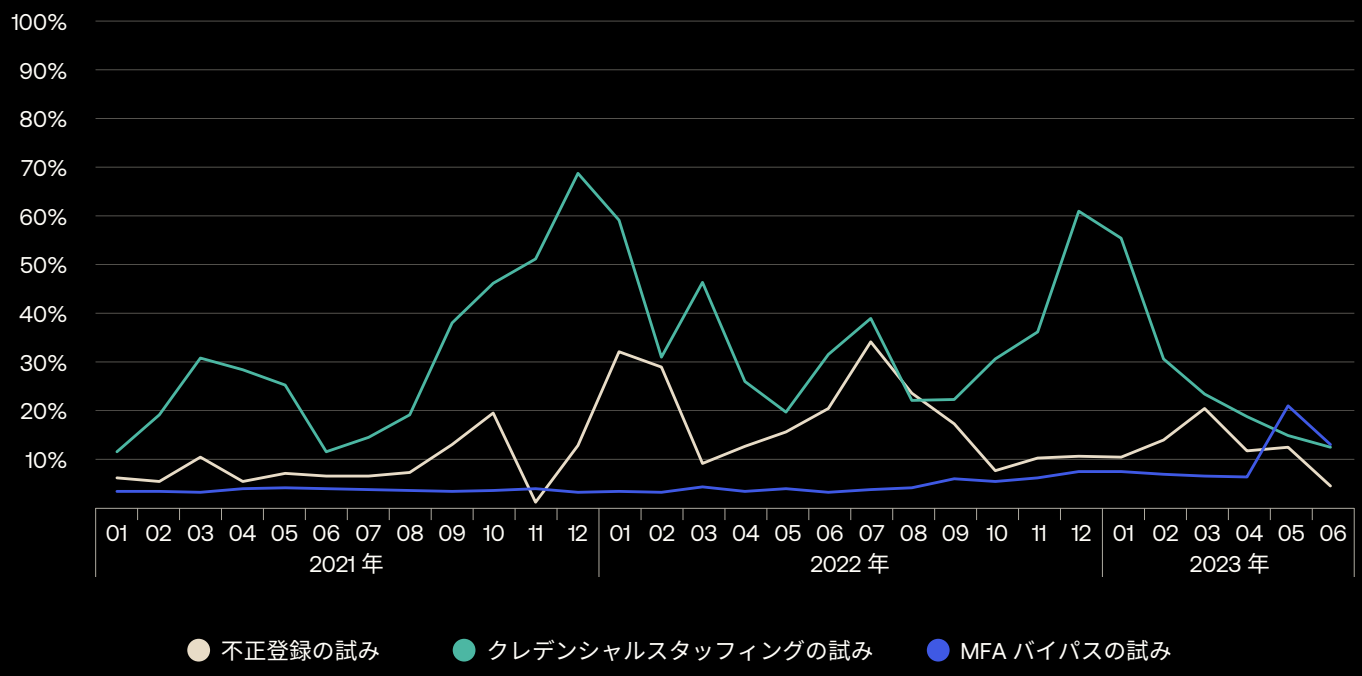


表 4：飲食 / ホスピタリティ

飲食 / ホスピタリティ組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	3.3%	17.8%	9.0%
クレデンシャルスタッフィングの試み	23.6%	21.5%	11.4%
MFA バイパスの試み	8.3%	9.2%	5.5%

表 5：医療

医療組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	1.9%	2.8%	6.3%
クレデンシャルスタッフィングの試み	4.5%	3.3%	16.1%
MFA バイパスの試み	6.0%	9.0%	4.6%

図 20：飲食 / ホスピタリティ組織に対するアイデンティティ脅威の 30 か月日次ビュー

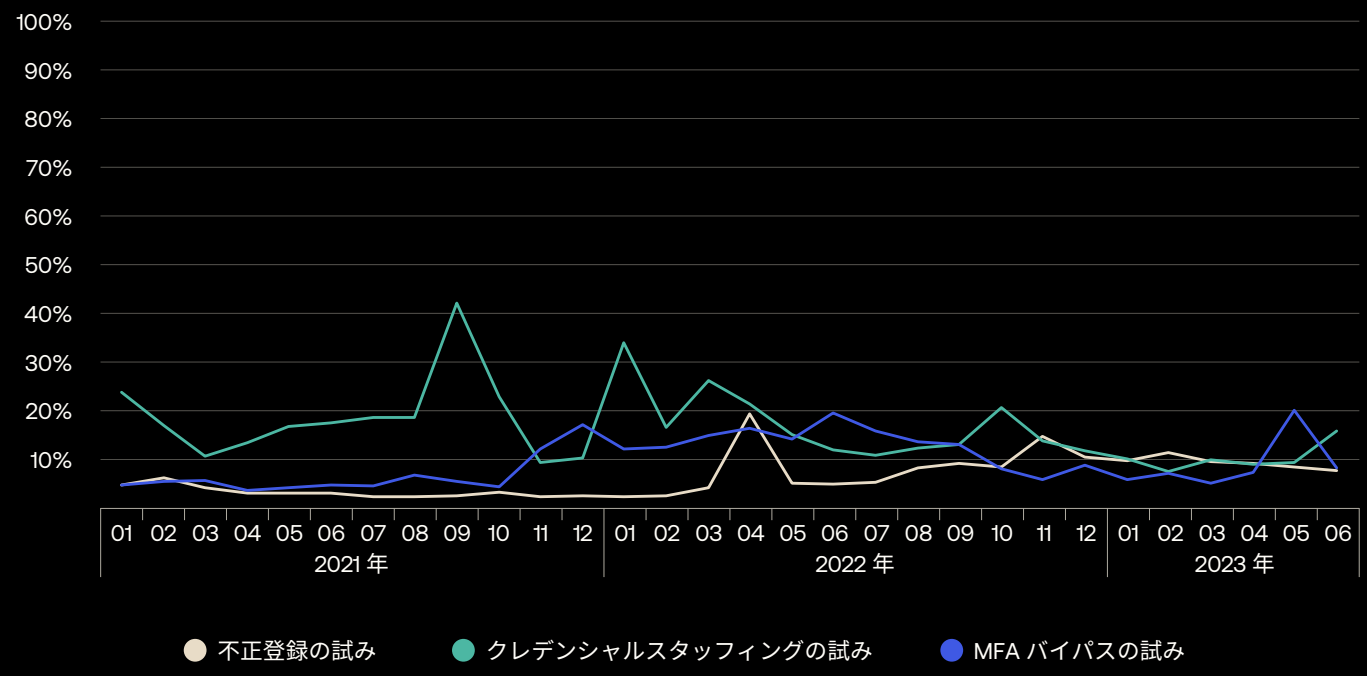


図 21：医療組織に対するアイデンティティ脅威の 30 か月日次ビュー

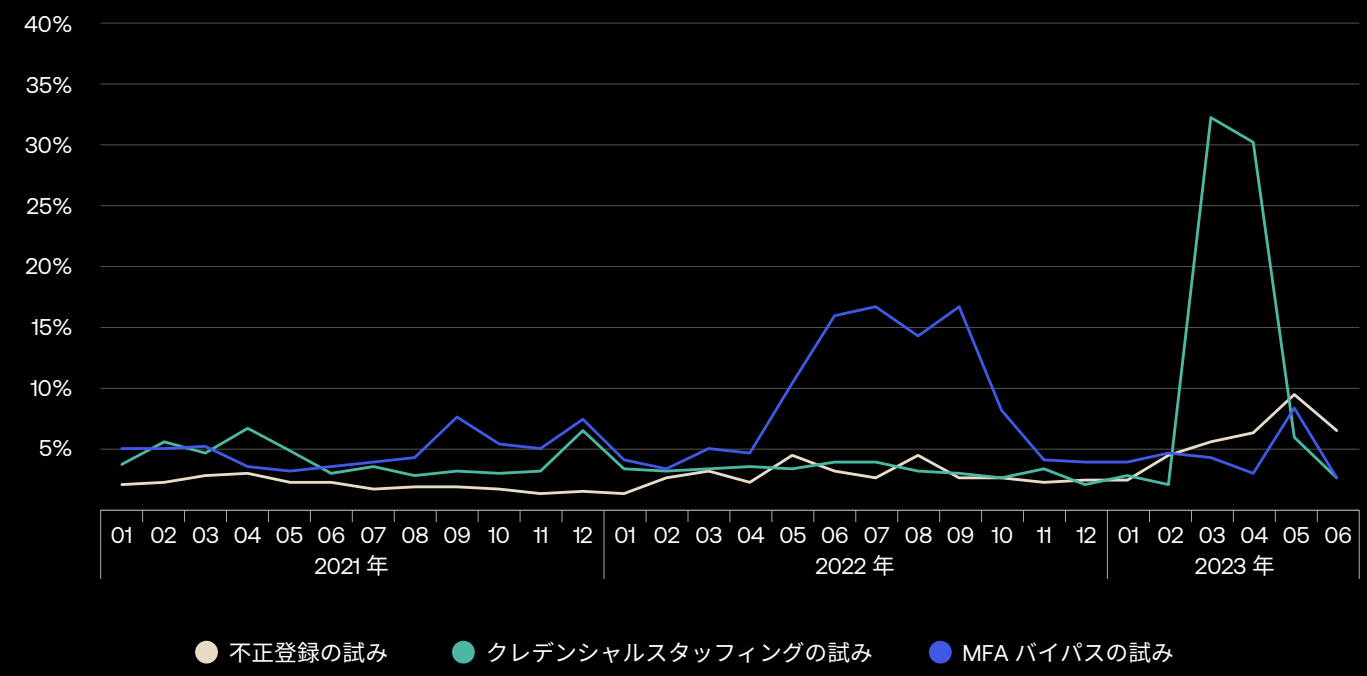


表 6：製造

メーカーに対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	14.3%	17.8%	25.1%
クレデンシャルスタッフィングの試み	45.9%	18.4%	17.7%
MFA バイパスの試み	6.5%	10.0%	7.8%

表 7：メディア

メディア組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	9.0%	15.7%	28.4%
クレデンシャルスタッフィングの試み	22.7%	17.9%	42.3%
MFA バイパスの試み	27.4%	25.1%	12.8%

図 22：メーカーに対するアイデンティティ脅威の 30 か月日次ビュー

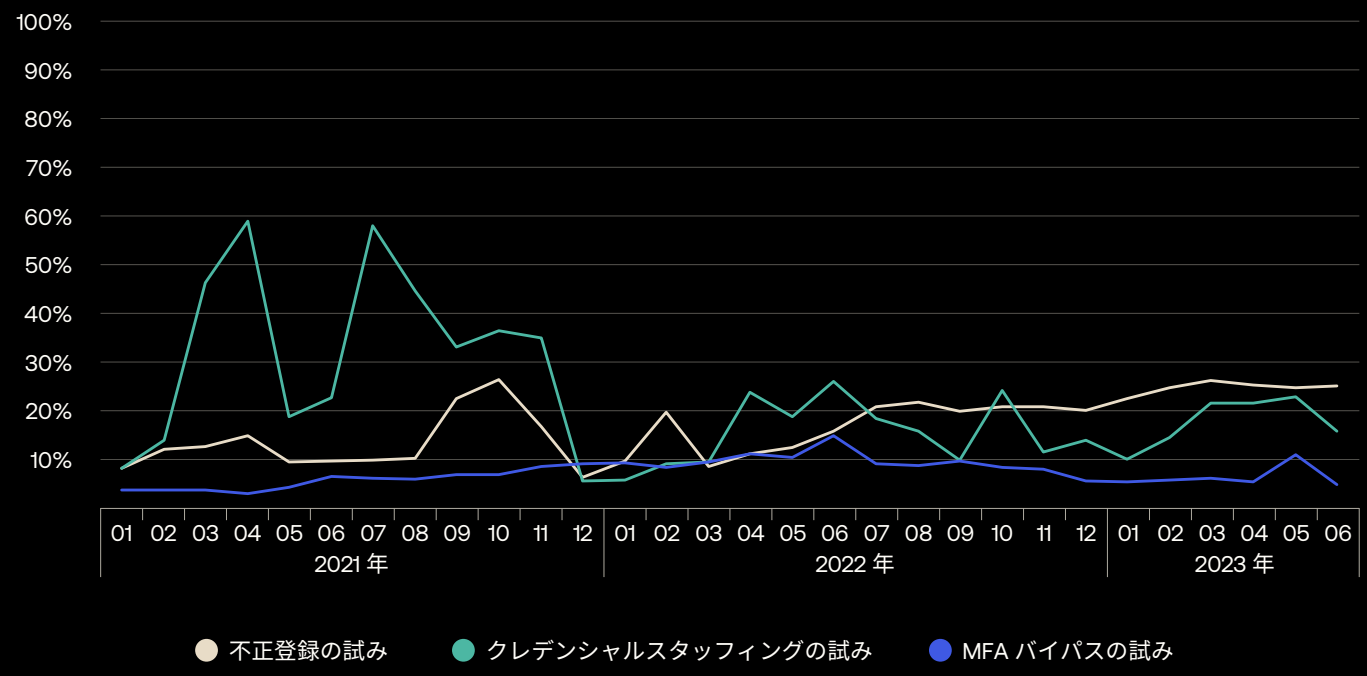


図 23：メディア組織に対するアイデンティティ脅威の 30 か月日次ビュー

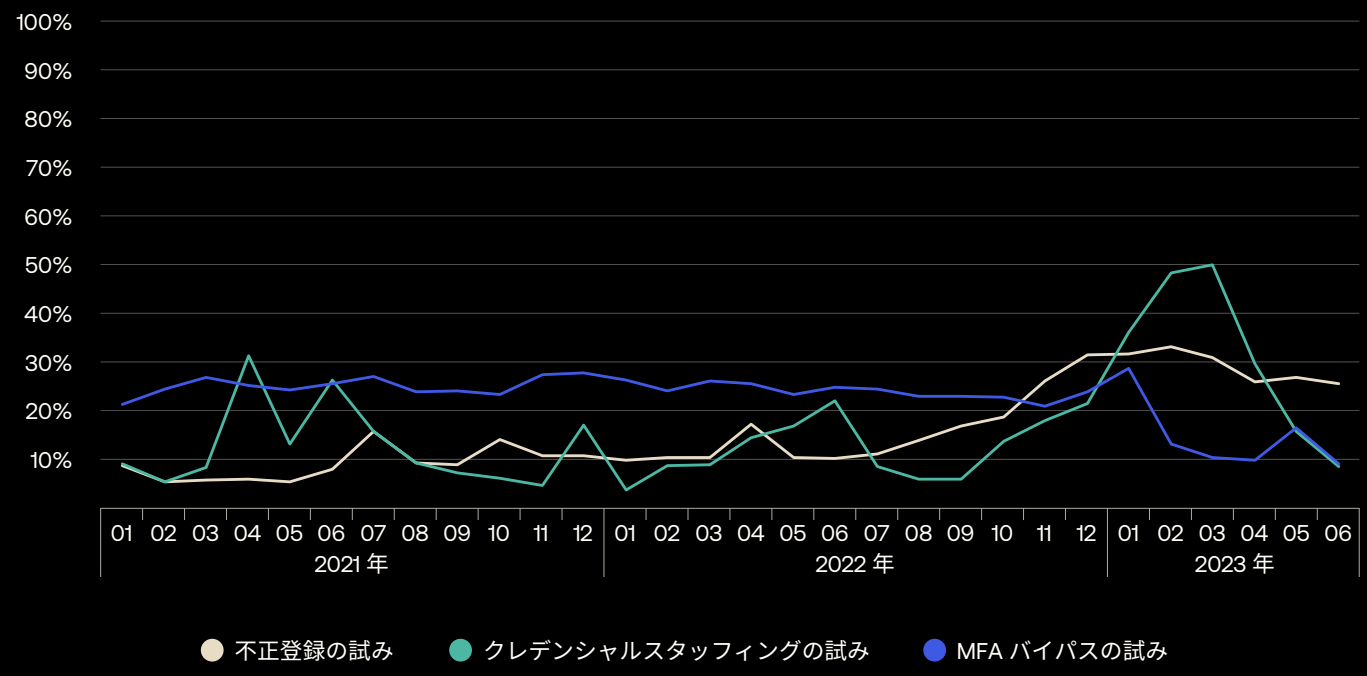


表 8：プロフェッショナルサービス

プロフェッショナルサービス組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	5.9%	6.1%	13.4%
クレデンシャルスタッフィングの試み	7.3%	4.8%	7.2%
MFA バイパスの試み	13.1%	6.7%	4.5%

表 9：小売 / e コマース

小売 / e コマース組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	2.0%	3.6%	9.3%
クレデンシャルスタッフィングの試み	55.6%	56.8%	51.3%
MFA バイパスの試み	5.7%	5.3%	5.0%

図 24：プロフェッショナルサービス組織に対するアイデンティティ脅威の 30 か月日次ビュー

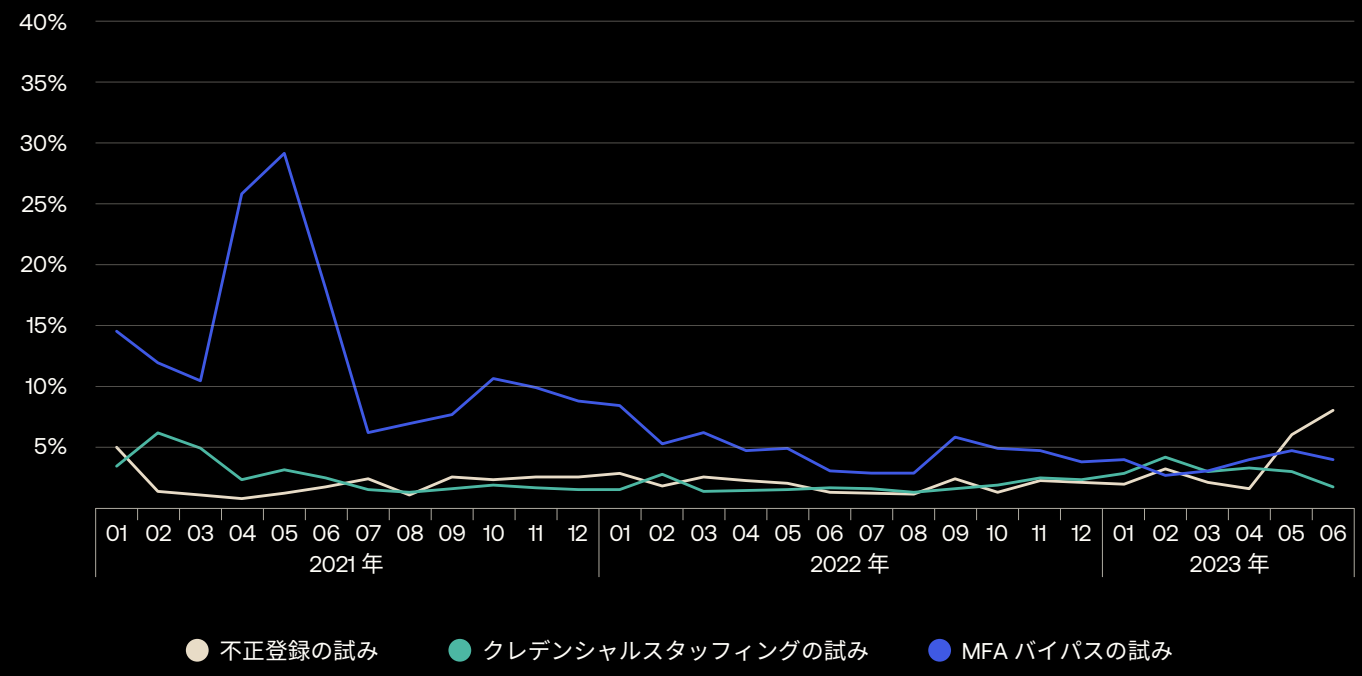


図 25：小売 / e コマース組織に対するアイデンティティ脅威の 30 か月日次ビュー

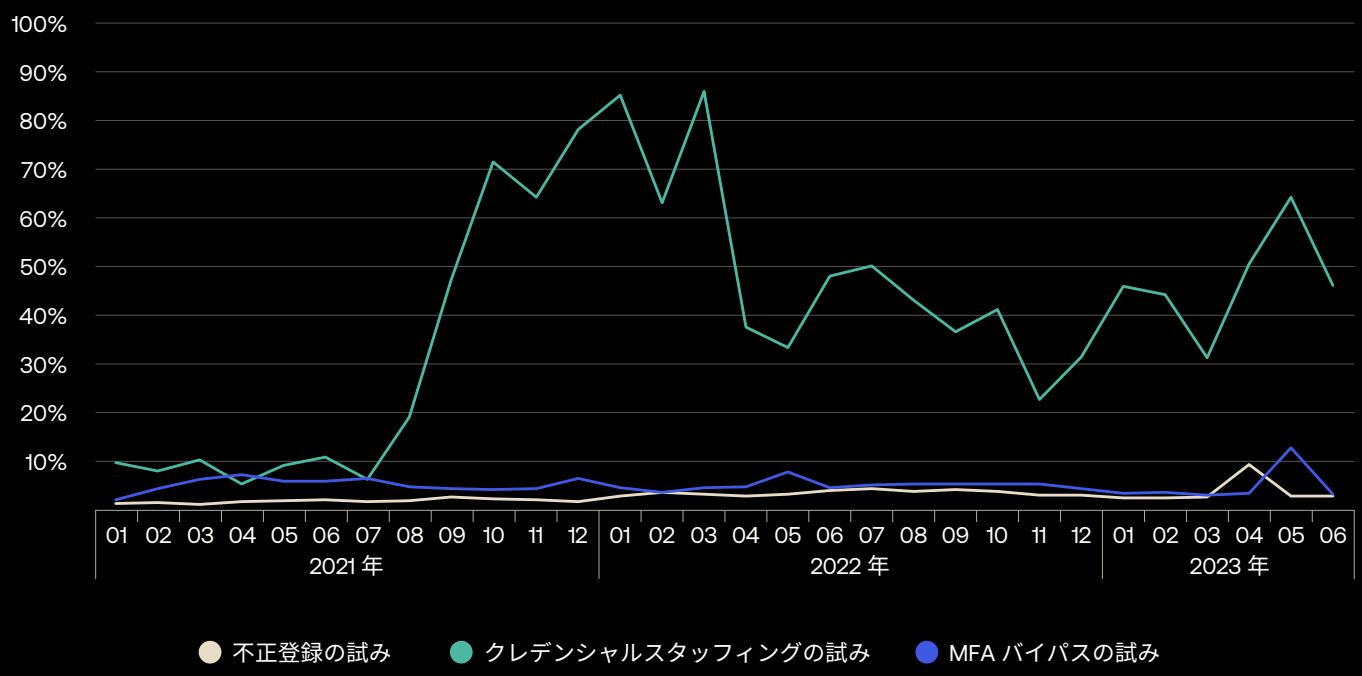


表 10：ソフトウェア / SaaS / テクノロジー

ソフトウェア / SaaS / テクノロジー組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	54.9%	26.1%	24.0%
クレデンシャルスタッフィングの試み	53.6%	34.5%	32.1%
MFA バイパスの試み	37.5%	21.6%	6.4%

表 11：旅行 / 運輸

旅行 / 運輸組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	5.1%	13.7%	9.7%
クレデンシャルスタッフィングの試み	27.4%	19.0%	7.2%
MFA バイパスの試み	6.9%	3.0%	2.9%

図 26：ソフトウェア / SaaS / テクノロジー組織に対するアイデンティティ脅威の 30 か月日次ビュー

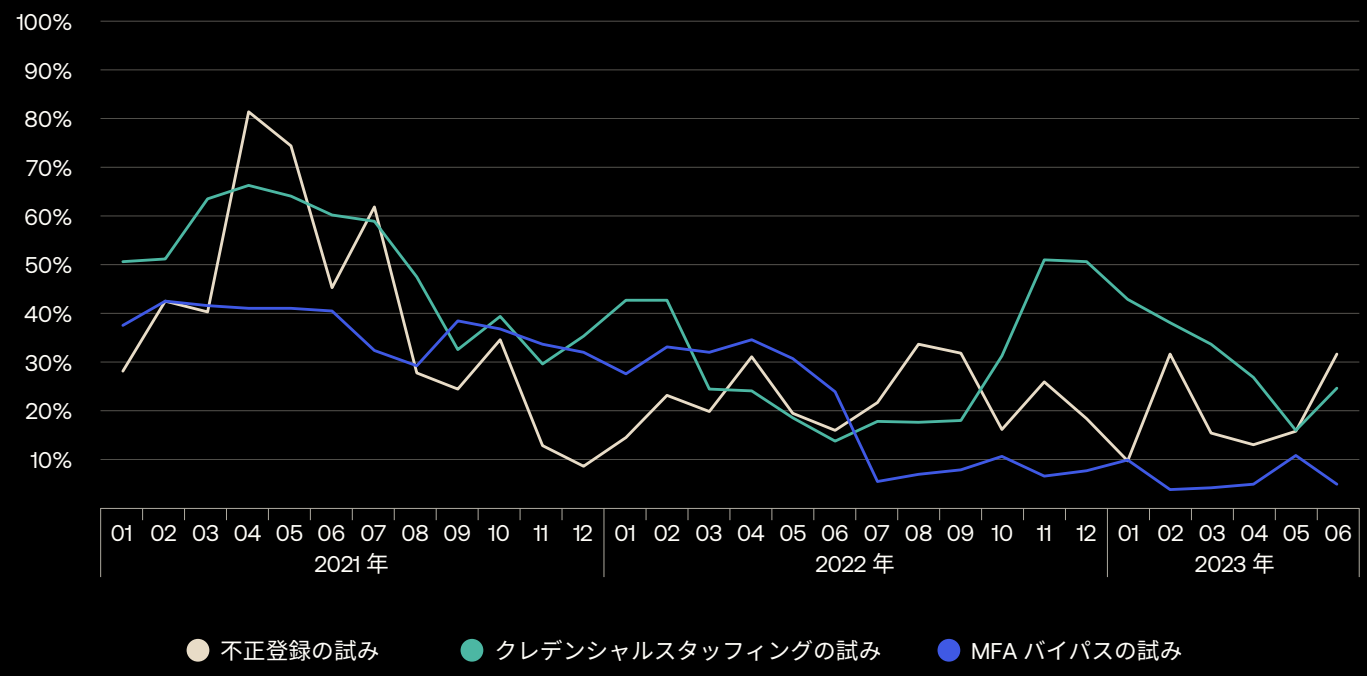
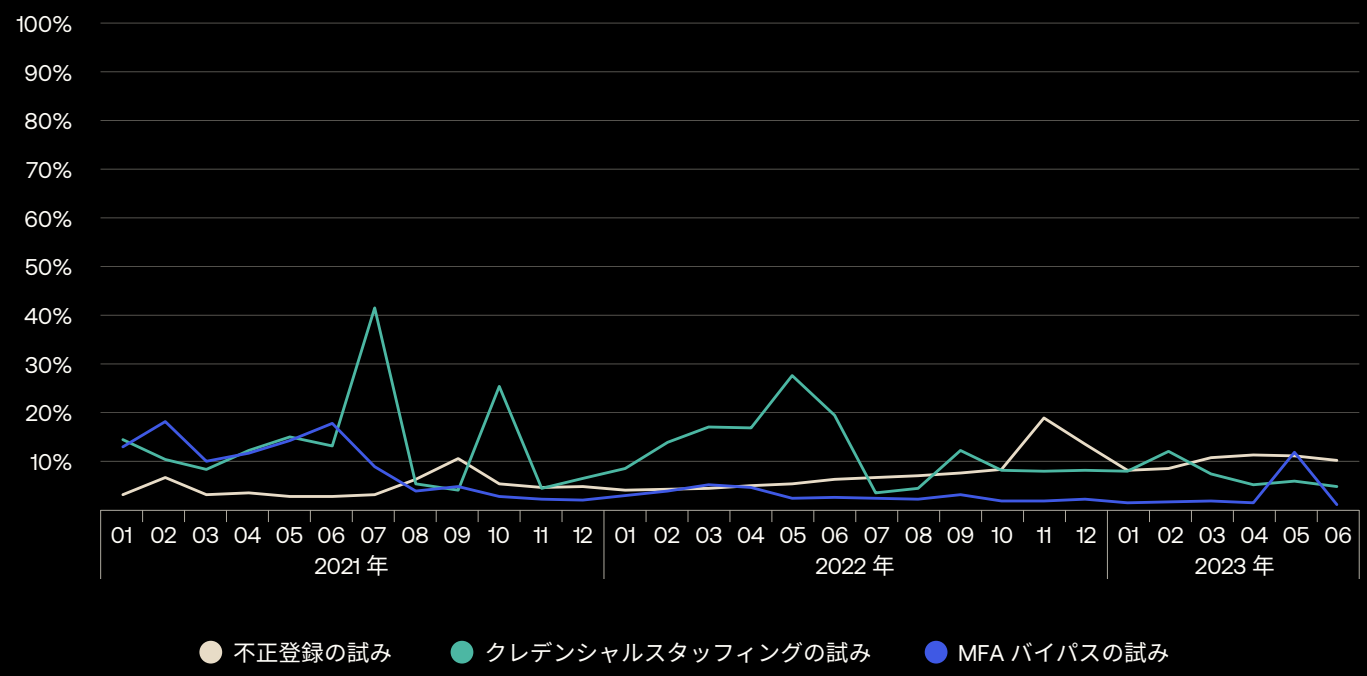


図 27：旅行 / 運輸組織に対するアイデンティティ脅威の 30 か月日次ビュー



付録

付録 D：組織規模別の要約

以下のサブセクションは、小規模企業、中規模企業、
および大企業についての補足説明です。

表 12：小規模企業

小規模企業に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	65.1%	44.6%	19.4%
クレデンシャルスタッフィングの試み	54.0%	35.7%	30.9%
MFA バイパスの試み	9.1%	25.0%	20.3%

図 28：小規模企業に対するアイデンティティ脅威の 30 か月日次ビュー

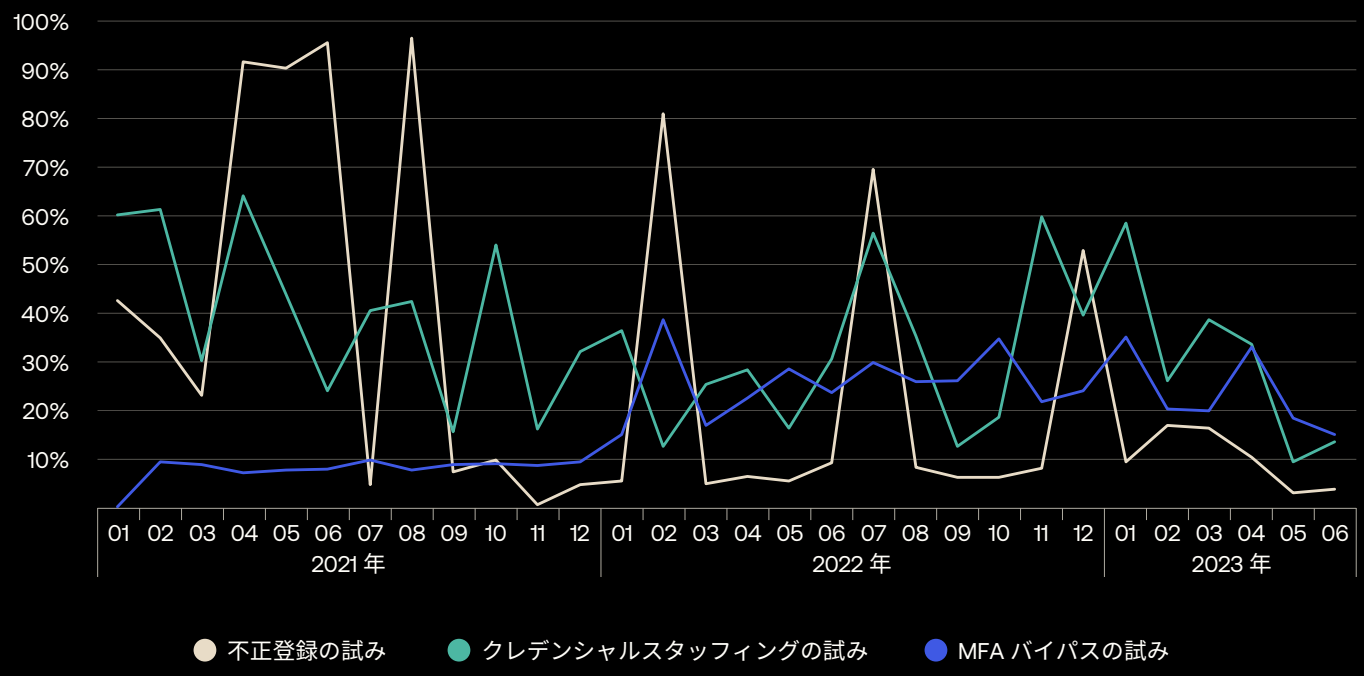


表 13：中規模企業

中規模企業に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	39.9%	6.0%	12.6%
クレデンシャルスタッフィングの試み	32.1%	30.5%	20.1%
MFA バイパスの試み	4.4%	6.2%	9.0%

表 14：大企業

大企業に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	16.2%	20.7%	19.9%
クレデンシャルスタッフィングの試み	50.6%	44.0%	39.4%
MFA バイパスの試み	32.3%	16.4%	9.5%

図 29：中規模企業に対するアイデンティティ脅威の 30 か月日次ビュー

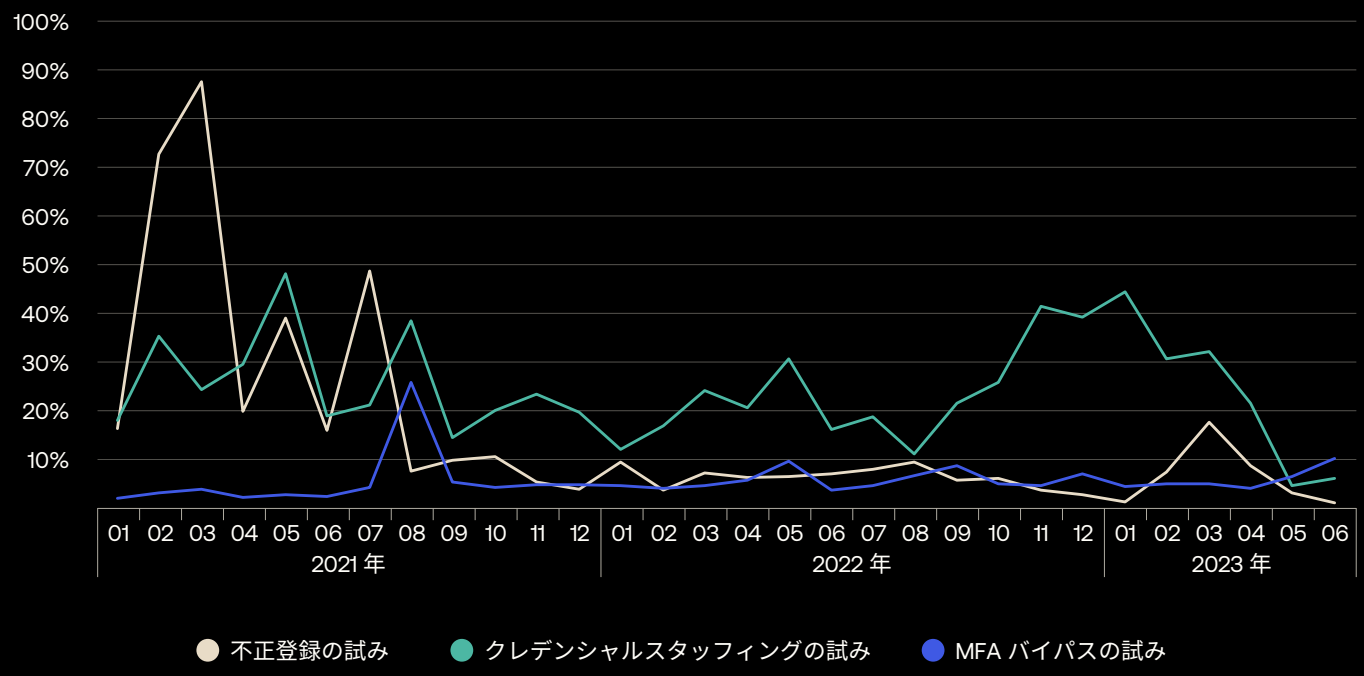
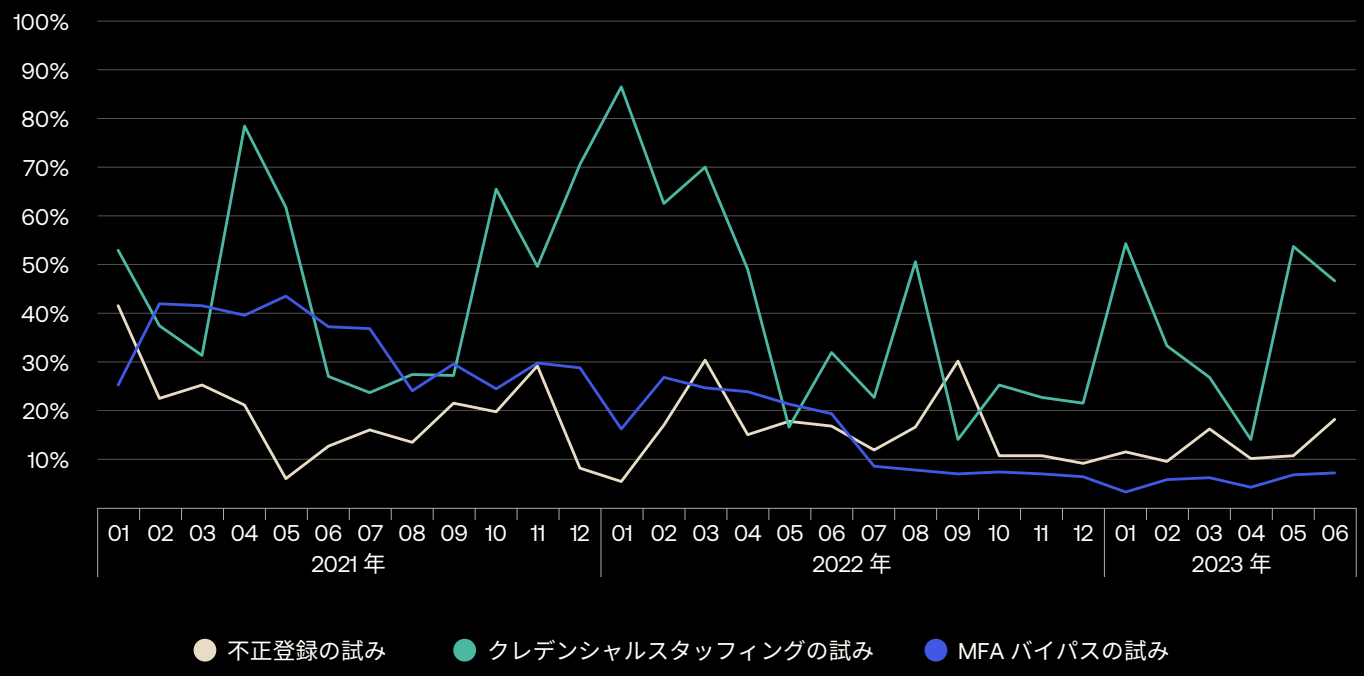


図 30：大企業に対するアイデンティティ脅威の 30 か月日次ビュー



付録

付録 E：地域別の要約

以下のサブセクションは、地域別の分析についての補足説明です。

備考：焦点を充てる地域が絞られるにつれて、関連するデータセットのサンプルサイズも縮小するため、短期的な変動がより頻繁になり、振幅がより大きくなることがあります。

表 15：北米 / 中南米

米国連邦航空局の西半球諸国一覧に記載された国が含まれる可能性があります。

北米 / 中南米に本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	35.8%	14.7%	9.4%
クレデンシャルスタッフィングの試み	48.1%	43.8%	28.0%
MFA バイパスの試み	6.9%	11.0%	12.0%

表 16：ラテンアメリカ

含まれる可能性のある国：アルゼンチン、ベリーズ、ボリビア、ブラジル、チリ、コロンビア、コスタリカ、エクアドル、エルサルバドル、フランス領ギアナ、グアテマラ、ガイアナ、ホンジュラス、メキシコ、ニカラグア、パナマ、パラグアイ、ペルー、スリナム、ウルグアイ、ベネズエラ。

ラテンアメリカに本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	15.8%	13.7%	5.7%
クレデンシャルスタッフィングの試み	59.0%	31.3%	17.6%
MFA バイパスの試み	5.0%	4.8%	10.7%

図 31：北米 / 中南米に本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

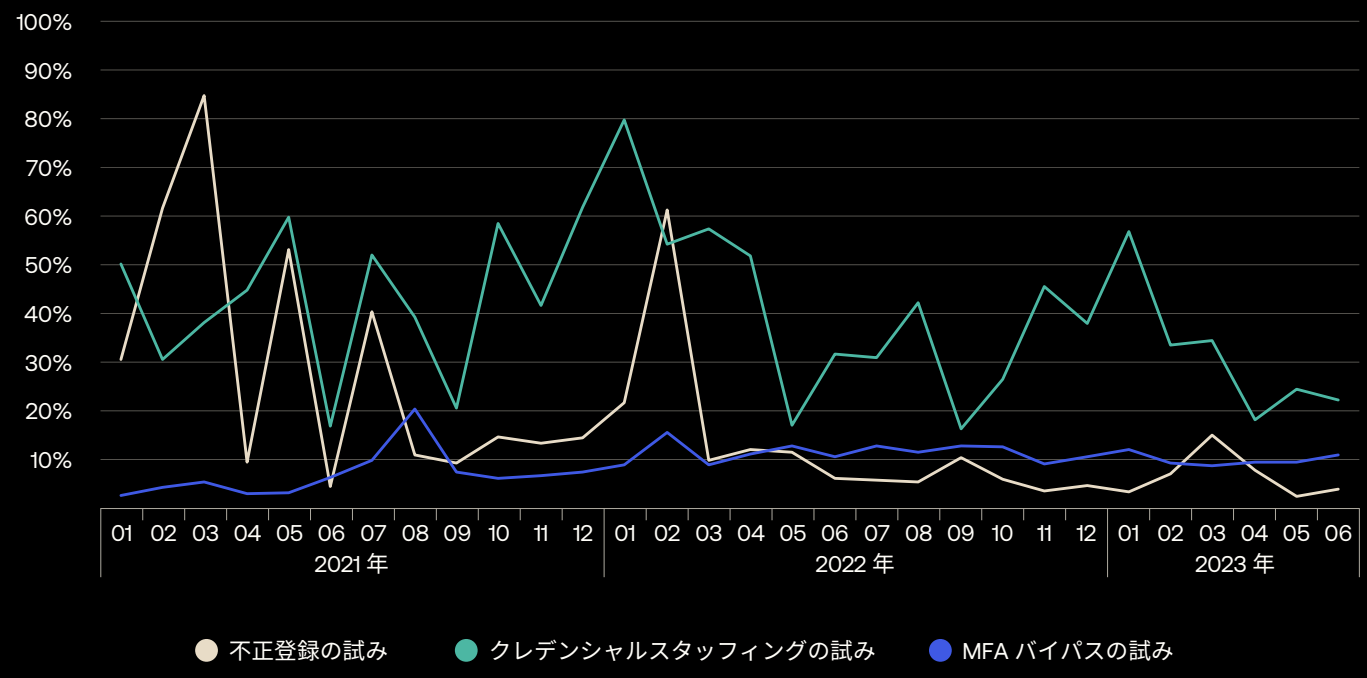


図 32：ラテンアメリカに本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

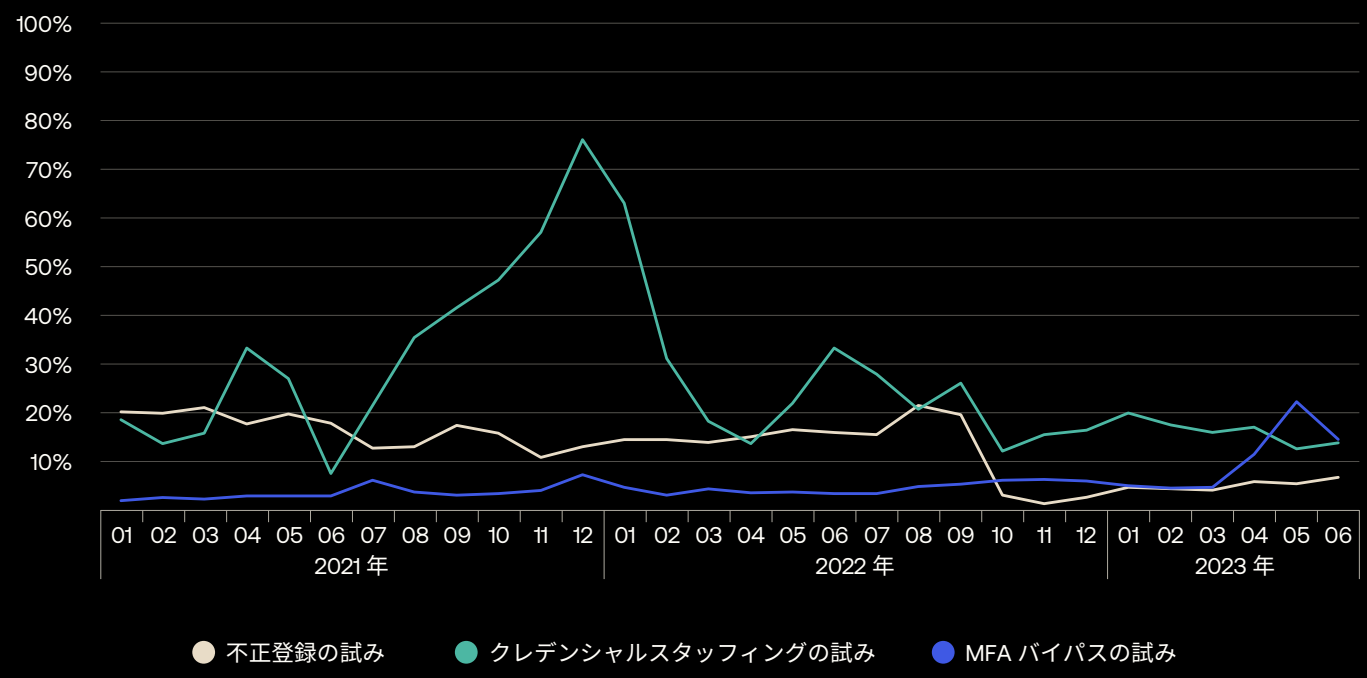


表 17：米国 / カナダ

米国 / カナダに本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	37.1%	14.8%	9.5%
クレデンシャルスタッフィングの試み	46.1%	45.1%	28.5%
MFA バイパスの試み	7.5%	14.1%	12.4%

表 18：欧州 / 中東 / アフリカ地域

米国連邦航空局のアフリカ / ヨーロッパ / 中東諸国一覧に記載された国が含まれる可能性があります。

欧州 / 中東 / アフリカ地域に本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	18.1%	20.5%	8.1%
クレデンシャルスタッフィングの試み	26.4%	14.1%	20.2%
MFA バイパスの試み	34.8%	20.3%	7.6%

図 33：米国 / カナダに本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

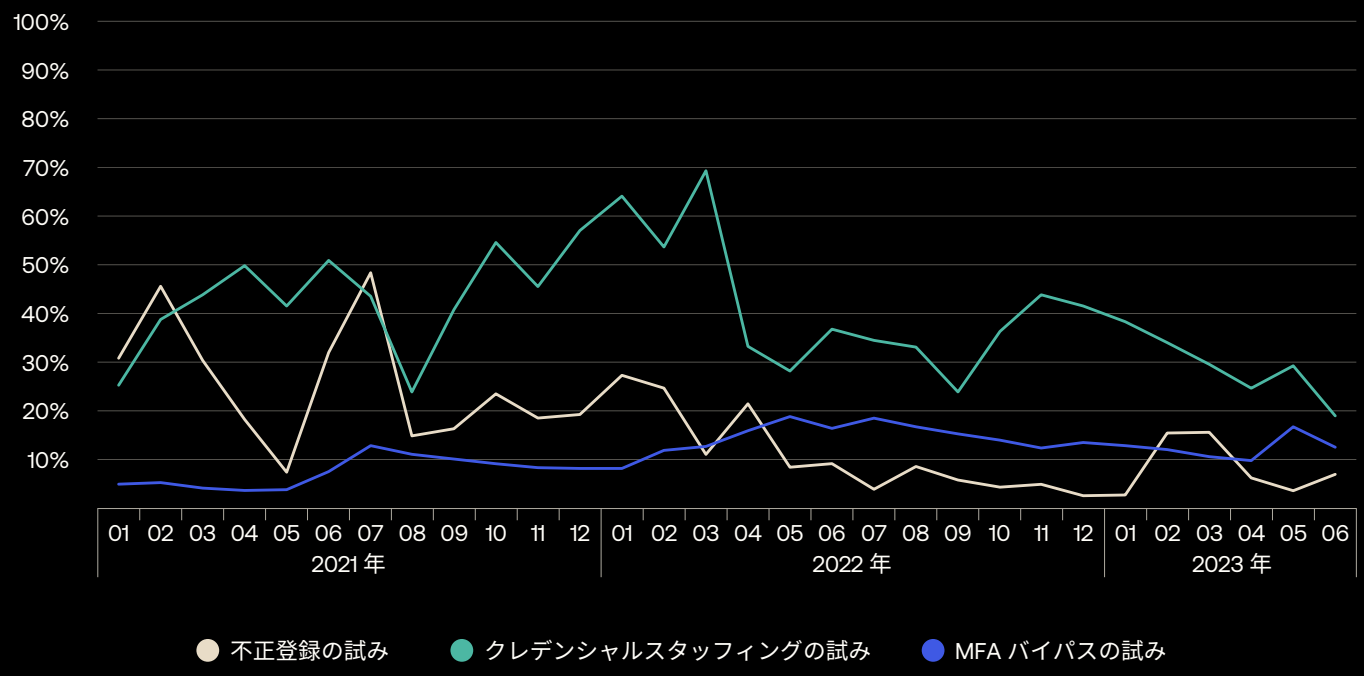


図 34：欧州 / 中東 / アフリカ地域に本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

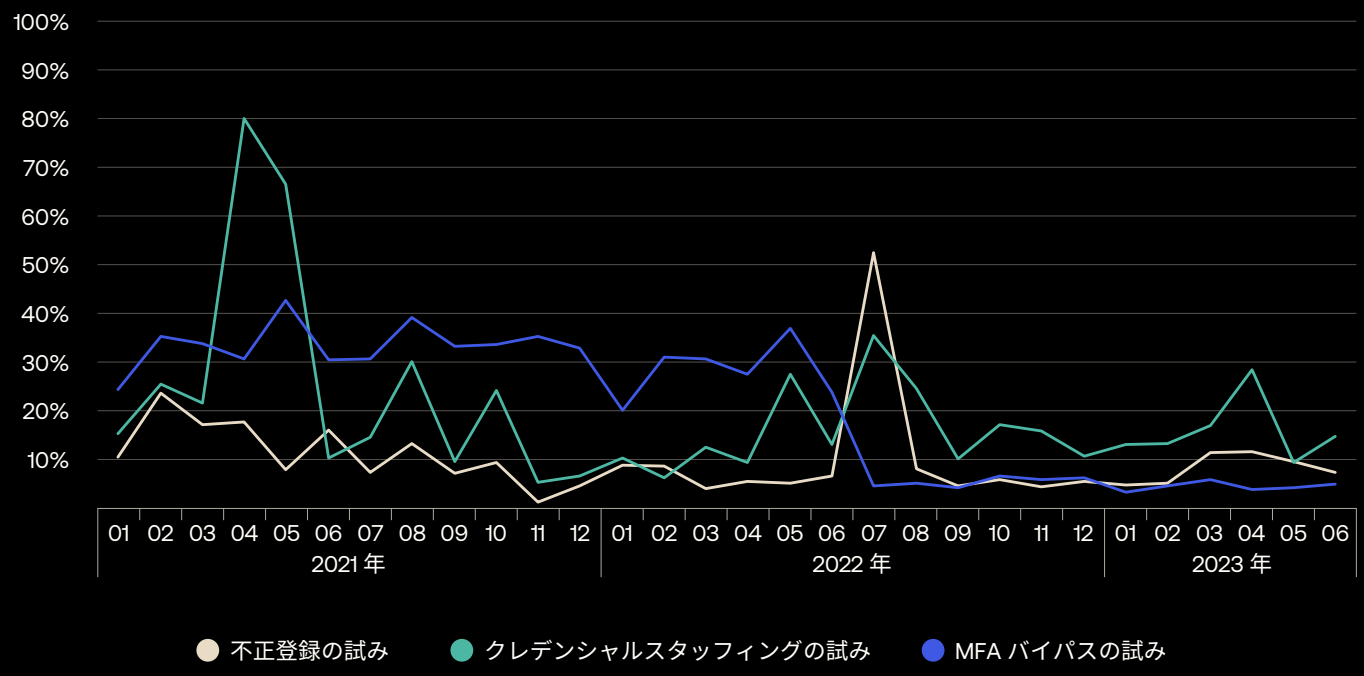


表 19：北ヨーロッパ

含まれる可能性のある国：デンマーク、フィンランド、アイスランド、ノルウェー、スウェーデン、グリーンランド。

北ヨーロッパに本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	45.4%	14.9%	5.2%
クレデンシャルスタッフィングの試み	15.0%	5.2%	12.5%
MFA バイパスの試み	6.0%	2.9%	4.1%

表 20：南ヨーロッパ

含まれる可能性のある国：アルバニア、アンドラ、ボスニアヘルツェゴビナ、ブルガリア、クロアチア、キプロス、トルコ、ジブラルタル、ギリシャ、イタリア、コソボ、マルタ、モンテネグロ、北マケドニア、ポルトガル、サンマリノ、セルビア、スロベニア、スペイン、バチカン市国。

南ヨーロッパに本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	11.7%	15.2%	24.8%
クレデンシャルスタッフィングの試み	18.1%	14.9%	10.9%
MFA バイパスの試み	5.2%	4.7%	5.5%

図 35：北ヨーロッパに本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

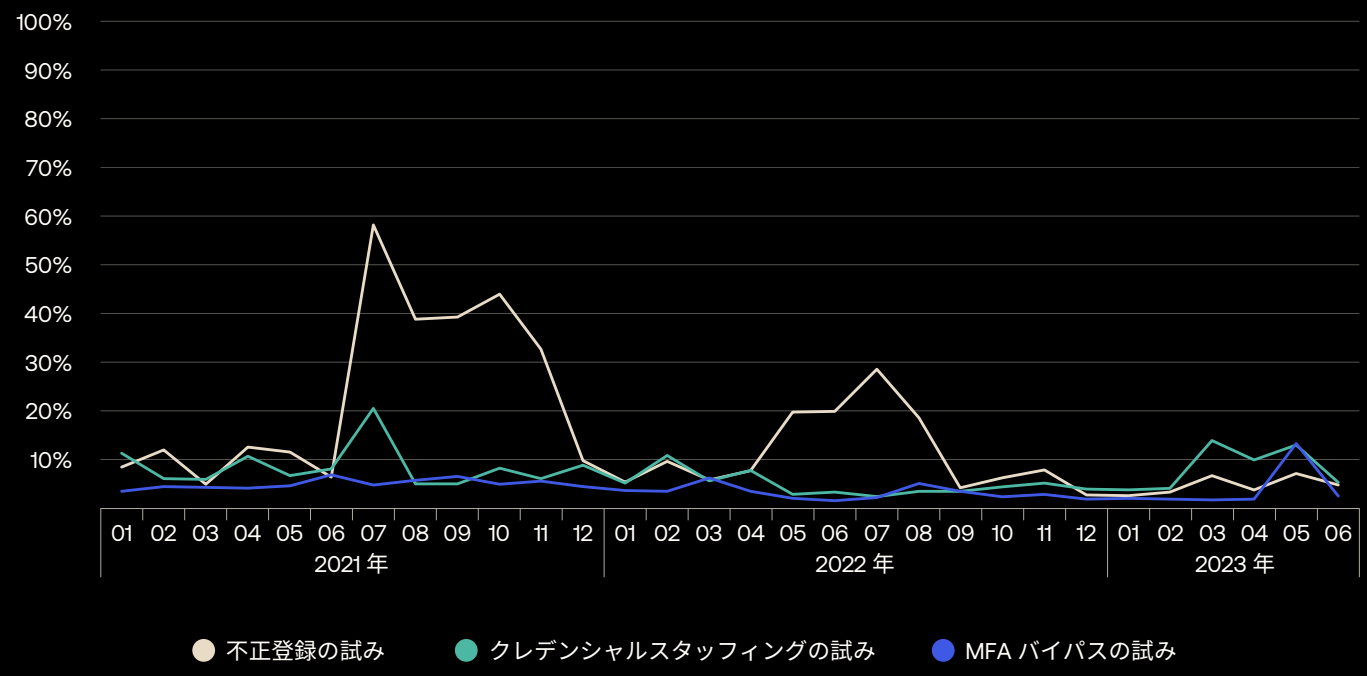


図 36：南ヨーロッパに本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

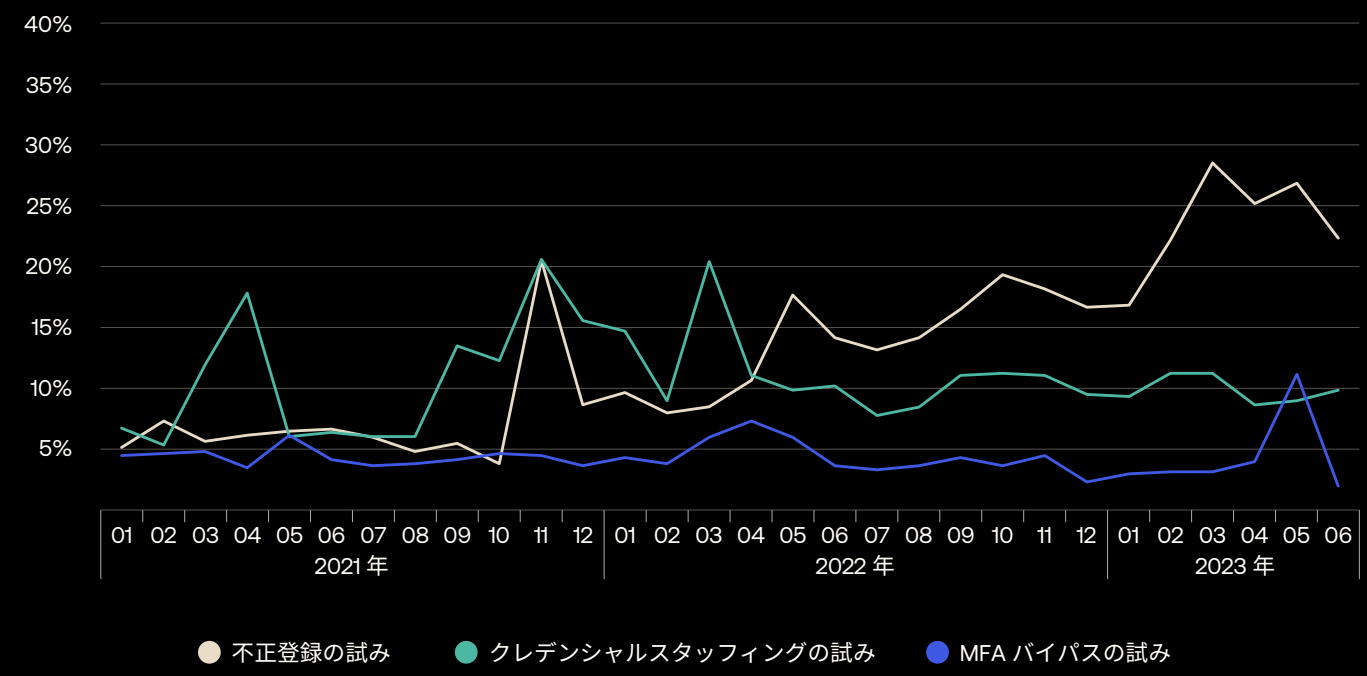


表 21：英国

含まれる可能性のある国：イングランド、北アイルランド、スコットランド、ウェールズ。

英国に本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	5.1%	11.1%	13.6%
クレデンシャルスタッフィングの試み	14.5%	12.9%	13.3%
MFA バイパスの試み	1.6%	2.7%	4.6%

表 22：西ヨーロッパ

含まれる可能性のある国：オーストリア、ベルギー、フランス、ドイツ、リヒテンシュタイン、ルクセンブルク、モナコ、オランダ、スイス。

西ヨーロッパに本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	14.6%	28.7%	5.1%
クレデンシャルスタッフィングの試み	22.7%	11.2%	6.3%
MFA バイパスの試み	10.8%	11.1%	14.5%

図 37：英国に本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

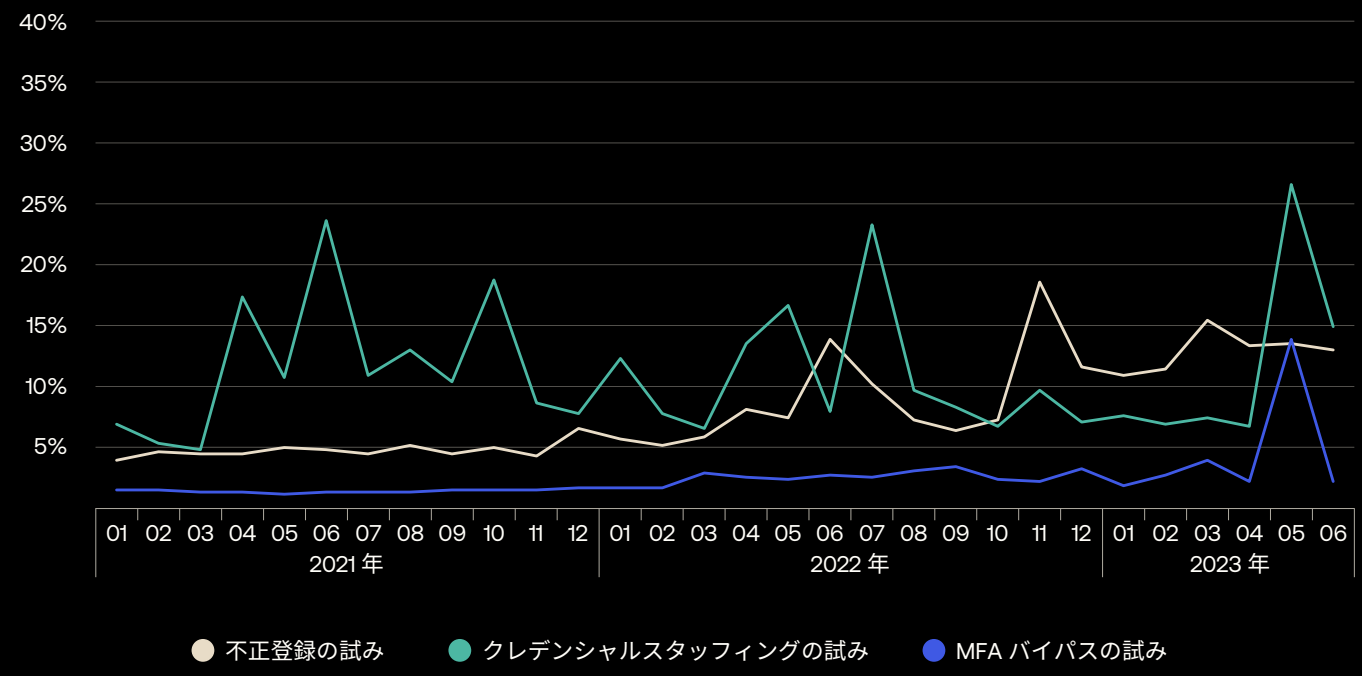


図 38：西ヨーロッパに本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

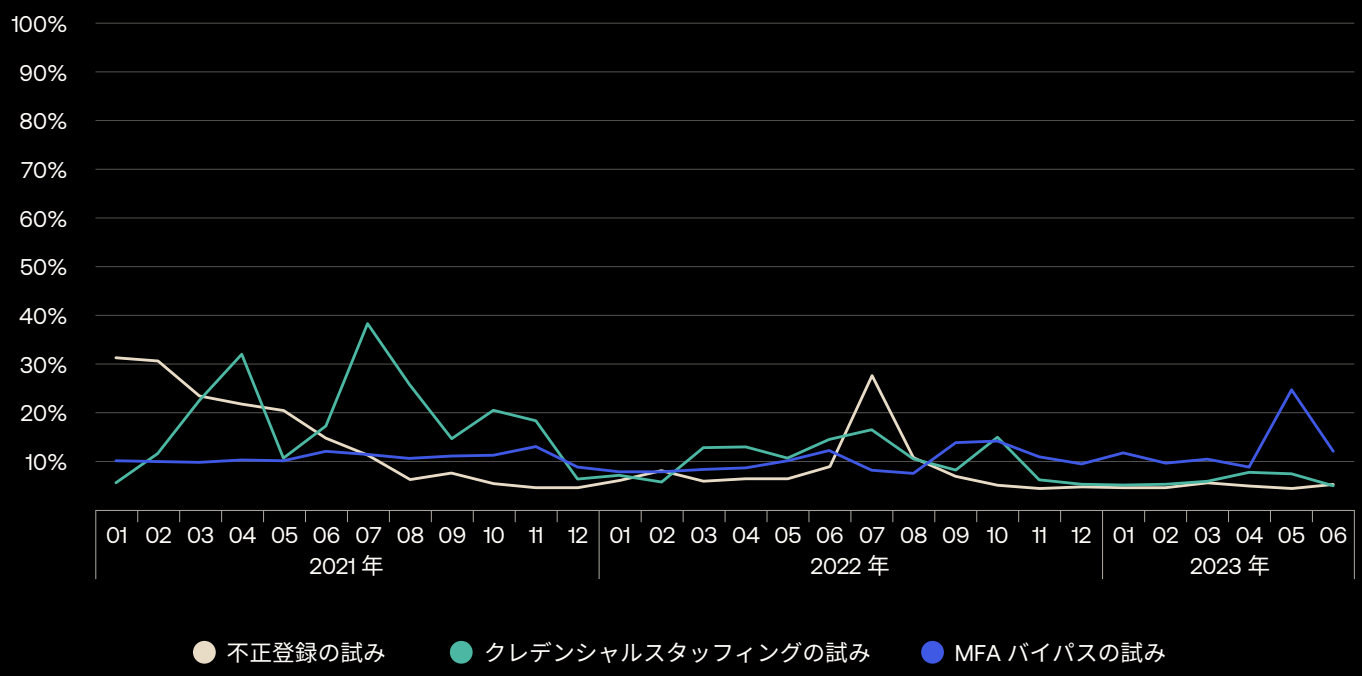


表 23：アジア太平洋地域

米国連邦航空局のアジア太平洋地域諸国一覧に記載された国が含まれる可能性があります。

アジア太平洋地域に本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	52.4%	28.9%	27.9%
クレデンシャルスタッフィングの試み	55.0%	24.3%	13.3%
MFA バイパスの試み	6.9%	10.3%	11.0%

表 24：日本

日本に本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	16.5%	33.9%	43.6%
クレデンシャルスタッフィングの試み	4.1%	2.7%	2.4%
MFAバイパスの試み	25.3%	16.6%	21.2%

図 39：アジア太平洋地域に本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

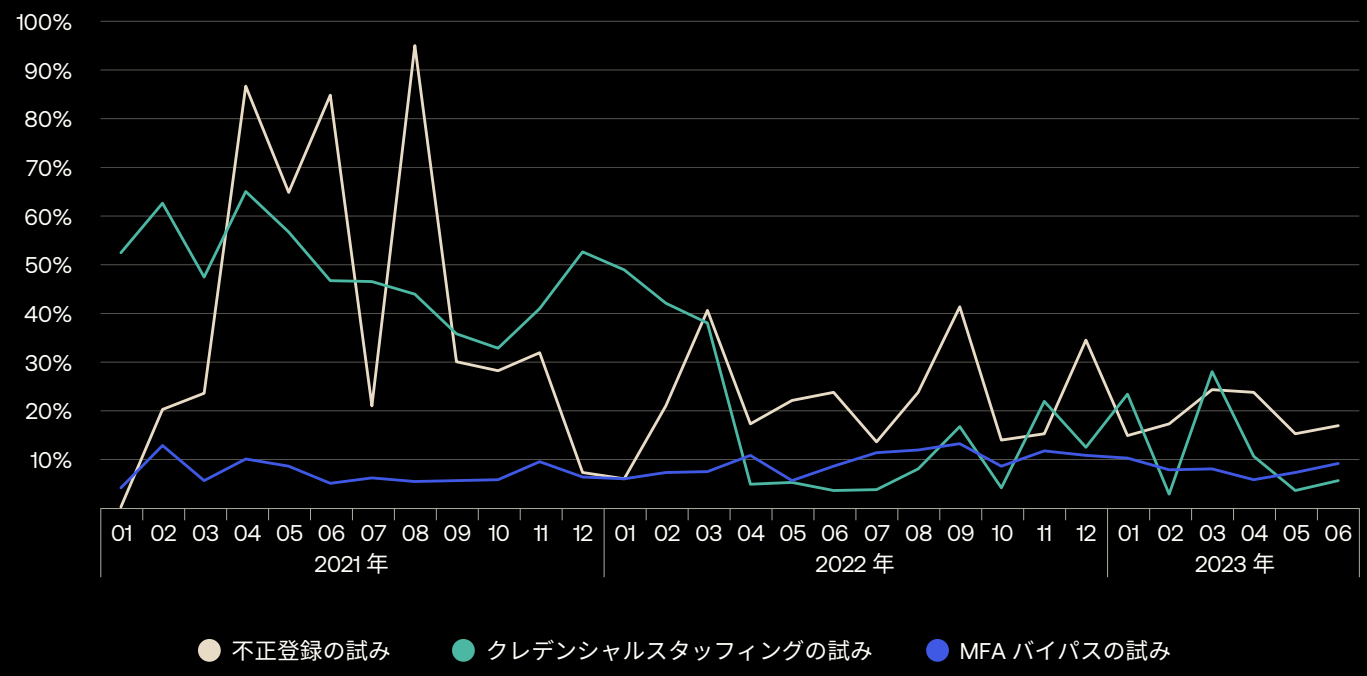


図 40：日本に本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

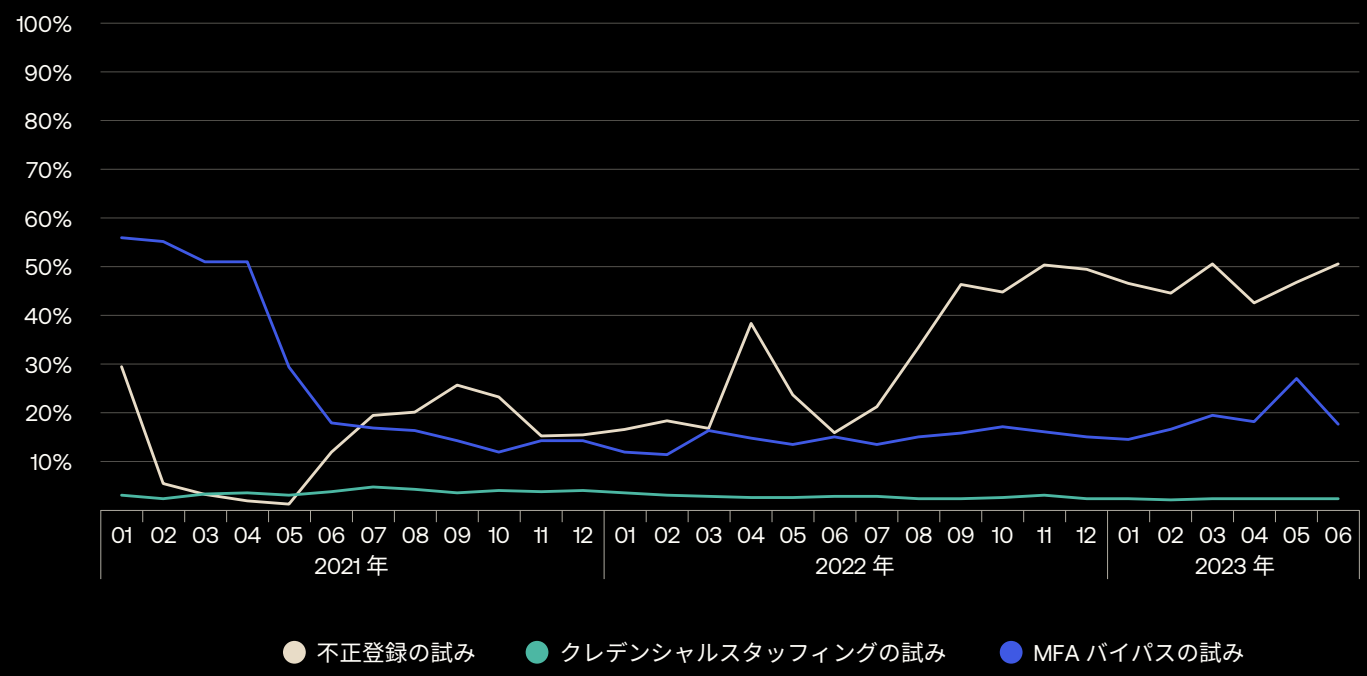


表 25：オーストラリアおよびニュージーランド

オーストラリアまたはニュージーランドに本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	53.0%	29.1%	26.7%
クレデンシャルスタッフィングの試み	57.1%	26.6%	14.8%
MFA バイパスの試み	4.3%	8.7%	9.1%

表 26：東南アジア

含まれる可能性のある国：ブルネイ、カンボジア、東ティモール、インドネシア、ラオス、マレーシア、ミャンマー、フィリピン、シンガポール、タイ、ベトナム。

東南アジアに本社を置く組織に対するアイデンティティ脅威のトレンドの要約

	2021	2022	2023上半期
不正登録の試み	47.3%	15.2%	16.2%
クレデンシャルスタッフィングの試み	73.4%	55.8%	24.3%
MFA バイパスの試み	16.2%	34.7%	3.5%

図 41：オーストラリア / ニュージーランドに本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー

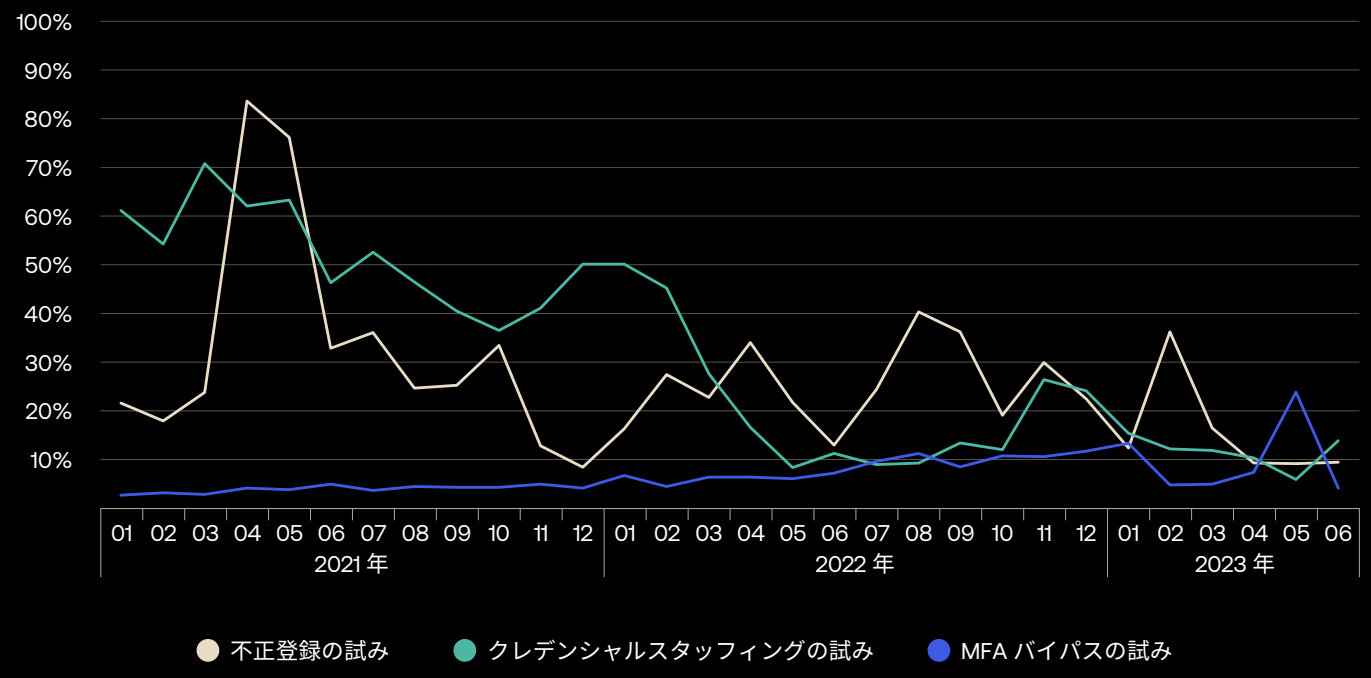
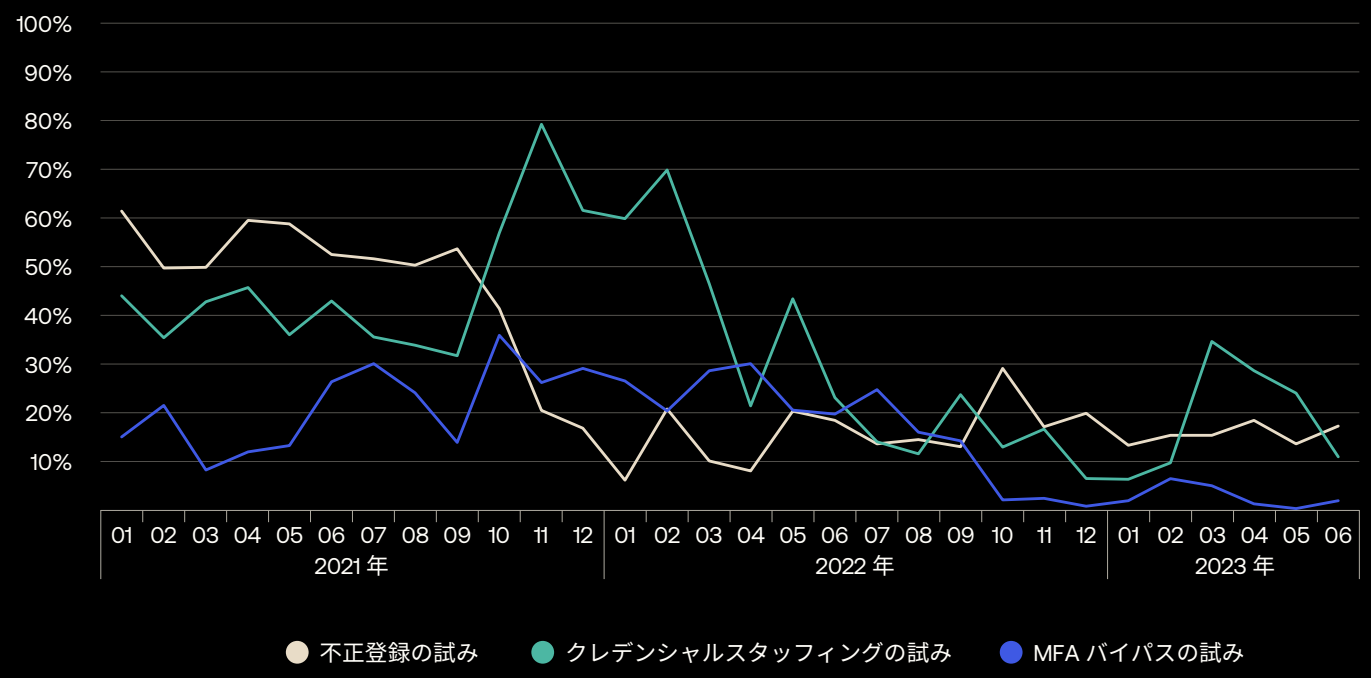


図 42：東南アジアに本社を置く組織に対するアイデンティティ脅威の 30 か月日次ビュー



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/