エグゼクティブサマリー

The State of Secure Identity Report 2023

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の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。

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 日から 2023 年 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
	専門サービス	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 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の割合
[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

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。

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。このため、システムが辞書攻撃に対して脆弱な状態であり続け、主要な攻撃ベクトルとなっています。
- **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。