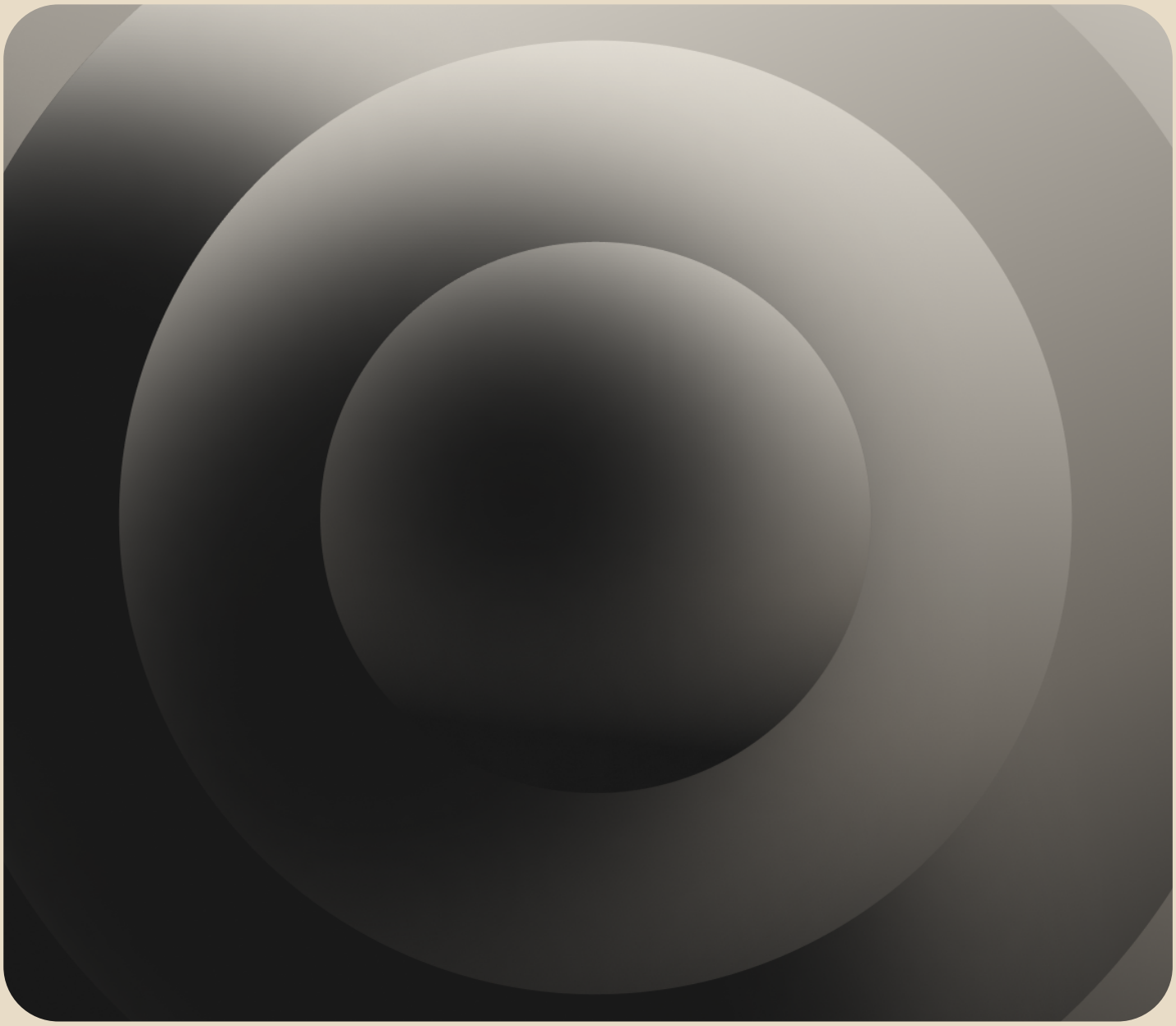
2024 年

MFA 導入状況と認証器の影響に関する洞察

セキュアサインインのトレンドレポート



okta

多要素認証（MFA）の利点が一般的に認識されるようになるまで、多少の時間がかかりました。

「パスワードを狙う多くの攻撃に対抗するには MFA が不可欠である」という考え方は、当初からセキュリティ分野では共通認識となっていました。しかし、多くの組織では、重要システムへのアクセスに限って MFA チャレンジを適用する状況が続いていました。

コロナ禍で MFA が主流となり、リモートワークに対応するために数か月間で利用率が 15%高まりました。現在では、多くの Okta 管理者と大半のユーザーが MFA チャレンジを経て業務アプリケーションにアクセスしており、規制当局や標準化団体もこうした強力なサインイン方法によるアクセス保護を組織に求めるようになっています。

今年のセキュアサインインのトレンドレポートでは、パスワードレスでフィッシング耐性のあるサインイン方法の導入が着実に増加していることが明らかになりました。Okta Workforce Identity Cloud ユーザーのうち、今年 1 月にサインインでパスワードを一度も使用しなかった割合は 5%です。わずか 5%という小さな数字ですが、これは大きな潜在力と可能性を示唆し、パスワードレスがすでに現実のものになっていることを物語っています。つまり、すでにパスワードレスを実現した Okta ユーザーが存在するのですから、他のユーザーも同様にパスワードを実現できるのです。

次の MFA 導入の波を牽引するのは、セキュリティに厳格な専門家でも、規制対象の組織に MFA 導入を求める政策立案者でもなく、ユーザーエクスペリエンスと保証レベルの向上を求めるユーザーになると予想されます。従業員であれ顧客であれ、一度でもパスワードレスを体験した人は、もはや後戻りすることはありません。

今年のレポートが皆様のお役に立つものになれば幸いです。

Todd McKinnon

Okta CEO

目次

MFA 導入率の定義

本レポートのデータと結論は、組織とその管理者 / 従業員がどのような認証を選択しているかを反映したものであり、この点を理解した上で読み進めることが重要です。ここでは頻繁に「ユーザー」という表現を使用しますが、通常は業務で認証を利用している従業員を指します。こうしたユーザーの認証オプションは、多くの場合に組織のポリシーによって制限されています。

多要素認証（MFA）の導入を測定する方法は複数あります（以下の表を参照）。この調査では、一定期間に MFA を使用してサインインしたユーザーの割合を、MFA の実際の導入率とみなして測定しました。

測定のオプション	定義
MFA アタッチ率	MFA を含む SKU を購入したお客様の割合
テナントレベルでの登録率	MFA の使用を構成したテナント（Okta org）の割合
ユーザーレベルでの登録率	MFA 認証器に登録したユーザーの割合
ユーザーレベルでの MFA 使用率	**一定期間に MFA を使用してサインインしたユーザーの割合**

また、ユーザー導入率を測定することが目的であることを踏まえ、ユーザーレベルで MFA の利用データを集計しました。

集計のオプション	定義
テナントレベルでの MFA 導入率	Okta を導入しているお客様のテナントのうち、MFA を使用して 1 か月に 1 回以上サインインしたユーザーがいる組織の割合
ユーザーレベルでの MFA 導入率	**1 か月間に MFA を使用してサインインしたユーザーの割合**
イベントレベルでの MFA 導入率	1 か月間に MFA チャレンジが関与したサインインイベントが成功した割合

この調査については、Okta Workforce Identity Cloud（WIC）の直接的な MFA 認証イベントのみを収集対象としている点にも留意する必要があります。たとえば、他のアイデンティティプロバイダーが提供する MFA のみを使用して認証し、エンタープライズフェデレーションやソーシャルログインを使用して Okta に接続するユーザーは、MFA 導入データには含まれません。したがって、報告された MFA 導入率では、Okta のお客様全体における MFA 使用率が若干低く見積られていると考えられます。さらに、テストアカウントも除外しました。すべての導入データと指標データは、収益に連動する本番環境のテナント（Okta org）から得られたものとなります。

認証器のユーザビリティとセキュリティのプロパティ

MFA 導入の障壁をよく理解するには、「フレームワークを開発し、認証器のプロパティを体系的かつ定量的に把握することは可能か」「顧客が組織の保護を強化して製品開発を導くことができるように、データドリブンな洞察を生かして教育することは可能か」といった基本的な問いを考える必要があります。

この点に関しては、認証器をユーザビリティとセキュリティの両方の観点から評価しました（表 2 参照）。各認証器のロジックやユーザーインターフェイス（UI）のフローは異なり、高いカスタマイズ性を持つため、これらの基準を測定するのは困難です。一貫性を保つため、より優れた設計と柔軟なアイデンティティエクスペリエンスやフローを提供する Okta Identity Engine（OIE）を活用しました。

調査では、パスワード、E メール、ハードウェアワンタイムパスワード（OTP）、プッシュ、ソフトウェア OTP、セキュリティ質問、SMS、音声 OTP、Okta FastPass、FIDO2 WebAuthn、スマートカードの各認証方法のプロパティを測定しました。特に断りのない限り、本レポートでは、Okta Workforce Identity Cloud で Okta Identity Engine を利用しているお客様から収集した、収益に連動する本番環境の 2024 年 1 月のデータを使用しています。

Okta は、認証器を同一条件で比較するためのデータ収集方法を開発するため、相当の注意を払いました。本レポートでは、こうした比較を複雑にしている状況を浮き彫りにし、それが調査結果に及ぼす影響を説明しています。また、全体的なトレンドが長期にわたって一貫していることを確認するため、月ごとのデータのばらつきもチェックしました。

調査結果の主な所見

MFA の導入は増加の一途をたどる

2024 年 1 月現在、Okta Workforce Identity Cloud ユーザーによる MFA 導入率は 66% に上昇し、管理者の 91% が MFA を使用しています。

業界や企業規模によって導入率は大きく異なる

行政機関と教育分野では、前年同期比で導入率が 5% 以上拡大しており、最近の米国大統領令（EO）や規制の変更によってさらに増加することが予想されます。

フィッシング耐性のある認証器が大きく進展

フィッシング耐性のあろ認証器の導入が大幅に増加しました。FIDO2 WebAuthn の導入率は 2023 年の 2% から 2024 年には 3% に増加し、さらに Okta FastPass の導入率は同じ期間で 2% から 6% へと急増しました。

パスワードレスの時代が到来

最新の認証方法の導入が広がり始め、Okta のお客様のパスワード使用がついに減少し始めました。2024 年 1 月時点で、ユーザーの 5% 弱がパスワードを使用せずにサインインしています。

「セキュリティか、UX か」という二者択一的な考え方は誤り

フィッシング耐性のある認証器は、優れたユーザーエクスペリエンスを提供します。認証器のパフォーマンスと使いやすさの評価において、FastPass と FIDO2 WebAuthn は、今回のレポートで改訂された実用的な基準の下でも、他のオプションよりも安全性とユーザーフレンドリーさで優れているという結果になりました。

はじめに

「多要素認証（MFA）は、今日利用可能な最も重要な予防的セキュリティ制御の 1 つとして広く認識されています。パスワードスプレー、漏洩したパスワードの再利用、場合によってはフィッシングなど、さまざまな攻撃手法に対する強力な防御を提供します。しかし、導入の難しさが主要課題となっており、規模の大小を問わず多くの組織がその価値を認識しつつも、依然として導入を実現できていません」[1]

多要素認証（MFA）がユーザーのサインイン時に提供する保証は、誰もが理解しています。

アイデンティティとアクセス管理において最も困難な課題の一つは、組織のアプリケーションやデータを保護するために、エンドユーザーにどの程度の負担をかけるべきかを見極めることです。負担が軽すぎると攻撃者に狙われるリスクが高まり、逆に負担が重すぎると従業員が許可されていないアプリケーションを利用するようになり、結果として新たなリスクを招く可能性があります。

深刻なセキュリティインシデントの増加とその対応コストの高騰を受けて、多くの組織や従業員は、特にリソースへのリモートアクセスを保護する上で、強力な認証が欠かせない要件であると受け入れつつあります。現在の課題は、保証レベルが高い認証を実現しながら、エンドユーザーにかかる負担を最小限に抑えることです。

本レポートでは、今日の企業がユーザーのアイデンティティを確認し、不正アクセスを防止するために取っている多種多様なアプローチを探っていきます。Okta のお客様の月間数十億件に上る認証の匿名化データに基づき、業界、地域、企業規模などのさまざまな角度から、認証のトレンドやアプローチを分析し、評価を更新しました。

今年のレポートには、状況が正しい方向に進んでいるものの、進捗のスピードが十分ではないことが示されています。コロナ禍では、リモートワークのセキュリティを強化するために MFA 導入率が 15% 増加しましたが、その後のペースは鈍化しています。2023 年以降、MFA 導入率の伸びは前年比 2 ポイントにとどまっており、すでに高水準に達している状態とはいえ、成長は限定的です。2024 年 1 月時点では、ユーザーの 66% が MFA を認証で使用しています。

今、私たちは転換点に差し掛かっています。米国の国家サイバーセキュリティ向上に関する大統領令の施行を受け、多くの組織やクラウドプロバイダーが認証の強化に取り組んでいます。同時に、Salesforce、GitHub、Okta、Microsoft といったテクノロジーリーダーが、特権ユーザーに MFA を必須化するプロジェクトを推進しており、高い保証レベルを維持しながらユーザーの負担を軽減する認証方法の開発と導入への関心が高まると予想されます。

本レポートは、現在利用可能なソリューションに関するデータに基づいた洞察をセキュリティ/IT 専門家に提供するとともに、「強力な認証はユーザーに余分な摩擦を引き起こす」という誤解を払拭することを目的としています。実際には、フィッシング耐性のあるパスワードレス認証によって、安全性と使いやすさの両方が向上します。

特に断りのない限り、本レポートのデータおよび結論はすべて、匿名化された Okta データの分析に基づきます。

[1] https://media.defense.gov/2023/Oct/04/2003313510/-1/-1/0/ESF%20CTR%20IAM%20MFA%20SSO%20CHALLENGES.PDF

データの使用方法

本レポートは、多様な認証器を包括的に取り上げ、ユーザビリティとセキュリティのプロパティを測定するためのフレームワークを提供します。MFA 導入率にばらつきがある「理由」については、CIO、CSO、ポリシー策定者が理解しやすいように、以下のような問いへの回答として取り組みました。

- MFA の導入状況はどのように推移してきたか？
- 組織の業界、所在地、規模は MFA 導入率に影響するか？
- MFA の導入には、どのようなユーザビリティの特性が関係していると思われるか？
  - 特定の認証器を使用した認証には、通常どの程度の時間がかかるか？
  - 特定の認証器の設定 / 登録には、通常どの程度の時間がかかるか？
  - 特定の認証器を使用した認証イベントは、どの程度の頻度で失敗するか？
- MFA の導入には、どのようなセキュリティ機能が関連すると思われるか？
  - フィッシング耐性のある認証フローに、特定の認証器がどの程度の範囲で対応するか？
  - 総当たり攻撃で、攻撃者は特定の認証器を使用するアカウントをどの程度の頻度で標的にしているか？

これらの質問に対する回答は、IT/ セキュリティリーダーが、それぞれの組織やユーザーに最適なソリューションを見極めるために、さまざまな認証器のコストと利点を比較検討する上で役立ちます。

“Okta は、長年にわたりパスワードレスでフィッシング耐性のある認証のメリットを享受しています。前回の「セキュアサインインのトレンドレポート」以降の 12 か月間で、Okta はユーザーライフサイクル全体（ユーザー登録から、アクセス、アカウント復元まで）のフィッシング耐性強化に取り組んできました。朗報は、それが実現可能であるということです。”

David Bradbury

最高セキュリティ責任者

okta

MFA の導入状況

保証レベルが高いセキュリティ態勢には、MFA が欠かせません。MFA を使用してサインインする際、ユーザーは本人確認のために 2 つ以上の異なる認証要素を提供する必要があります。これらの認証要素には、知識要素（パスワードなどの「知っていること」）、所有要素（登録済みデバイスなどの「持っているもの」）、または生体要素（生体認証などの「自身の属性」）が含まれます。

MFA は一般的に、セキュアサインインのために最低限必要であると見なされていますが、その導入には複数の内的 / 外的要因が影響を与えます。このセクションでは、導入率のこれまでの推移に加えて、地域別、業界別、組織規模別、認証器タイプ別、ユーザータイプ別（ユーザーが管理者権限を持つかどうか）の導入率を検証します。結果は、組織と業界の進歩を測るベンチマークとして、また改善すべき領域を特定するための指標として役立ちます。

「認証要素」と「認証器」
本レポートでは、米国国立標準技術研究所（NIST）の定義に沿って、「認証器」と「認証要素」という用語を使用しています。

認証器（Authenticator）：認証を試みるユーザーが所有または管理し、本人であることを認証するために使用します。

認証要素（Factor）：認証のプロパティであり、知識要素（パスワードやセキュリティ質問など、ユーザーが知っているもの）、所有要素（登録済みデバイスなど、ユーザーが持っているもの）、または生体要素（指紋など、ユーザー自身の属性）を指します。

備考：すべての認証器は 1 つ以上の認証要素を含みます。しばしば用語が混同され、「認証器」の意味で「認証要素」が使用されることがあります。また、1 つの認証器が複数の認証要素に対応する場合もあります。たとえば、Okta FastPass は、所有要素（登録済みデバイス）と生体要素（生体認証を使用）の両方を提供できます。

MFA の導入状況

MFA 導入率の推移

図 1 は、Okta Workforce Identity Cloud のお客様（従業員、請負業者、パートナーに企業リソースへの安全なアクセスを提供するために Okta を使用している組織）における、2019 年 10 月から 2024 年 1 月までの MFA ユーザー導入率を示しています。各データポイントは、月ごとの MFA 導入率を表します。

2023 年のレポートでも述べたように、2020 年 2 月から 3 月にかけて、MFA の導入率は 35% から 50% へ急上昇しました。これは、企業が迅速にリモートワークへ移行し、企業ネットワークを超えた範囲を保護する必要があったためです。
それ以降、2020 年から 2023 年にかけて MFA の導入率は年平均 6% 増加しましたが、2024 年には 2% に減速しました。2024 年 1 月時点では、66% のユーザーが MFA を利用してサインインしています。

この成長率は、アイデンティティを標的とした攻撃の増加に追いついていません。2024 年には、MFA を有効にしていないユーザーアカウント（人間のアカウント）やマシンアカウントを狙った攻撃が確認されました。この状況を受けて、多くのクラウドベンダーが特権ユーザーアカウントあるいは全アカウントに MFA の導入を義務付けるようになっています。

重要ポイント

特権アカウントに対する MFA の適用が標準的な管理策となる中、MFA を特権アカウントに義務付けるサービスプロバイダーがさらに増加すると予想されます。この動きは、IT やセキュリティの専門家が組織全体での MFA 導入をさらに推進する上での弾みとなります。

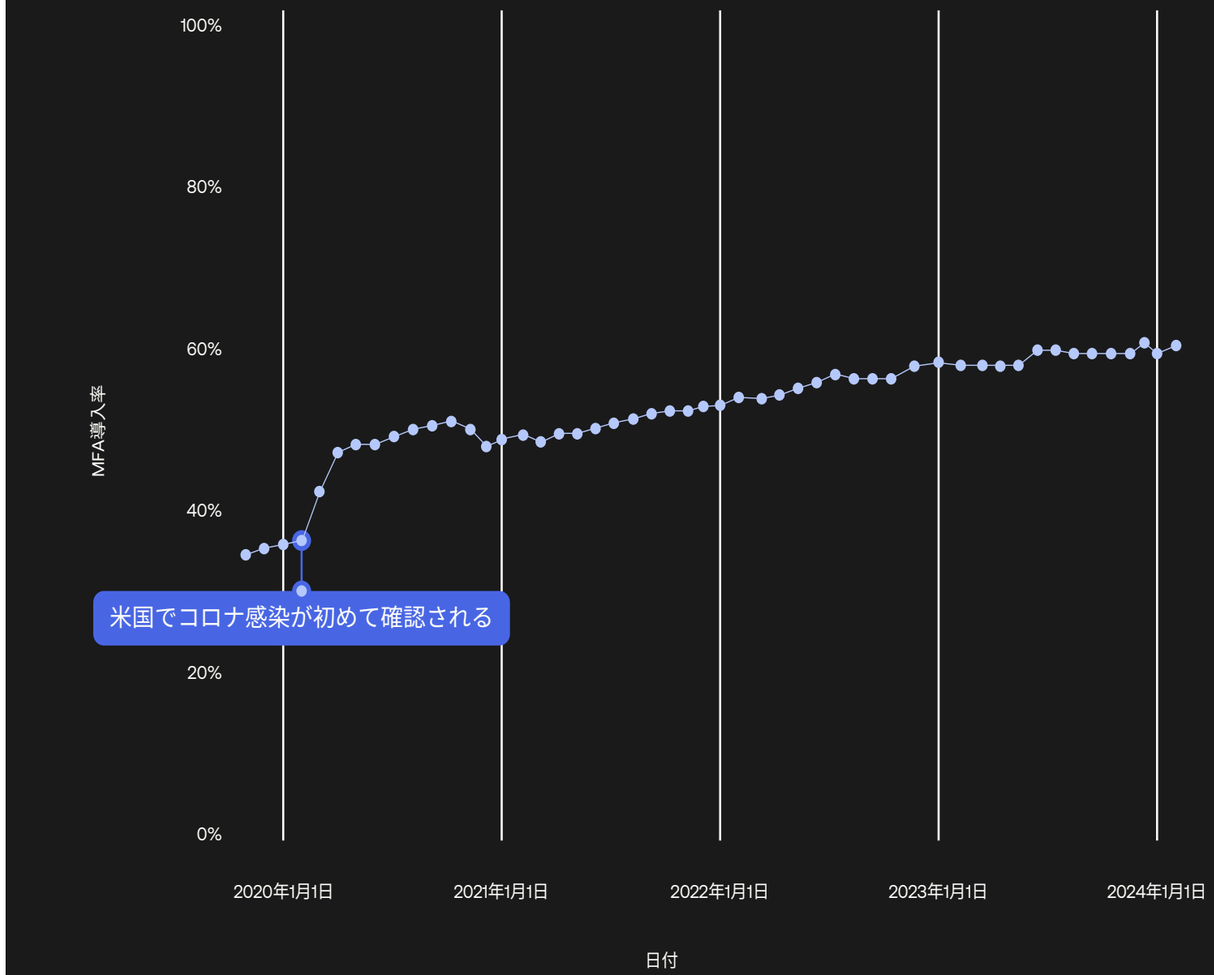


図1：2019年10月～2024年1月のMFAユーザー導入率の推移。このデータは、Okta Workforce Identity Cloudのワークフォースのユースケースを反映したものであり、Okta Customer Identity Cloud（旧Auth0）のデータやOktaプラットフォームの顧客向けユースケースは含みません。このデータには、Okta Federal Risk and Authorization Management Program(FedRAMP)HighおよびDoD Impact Level 4のお客様のデータも含まれません。

MFA の導入状況

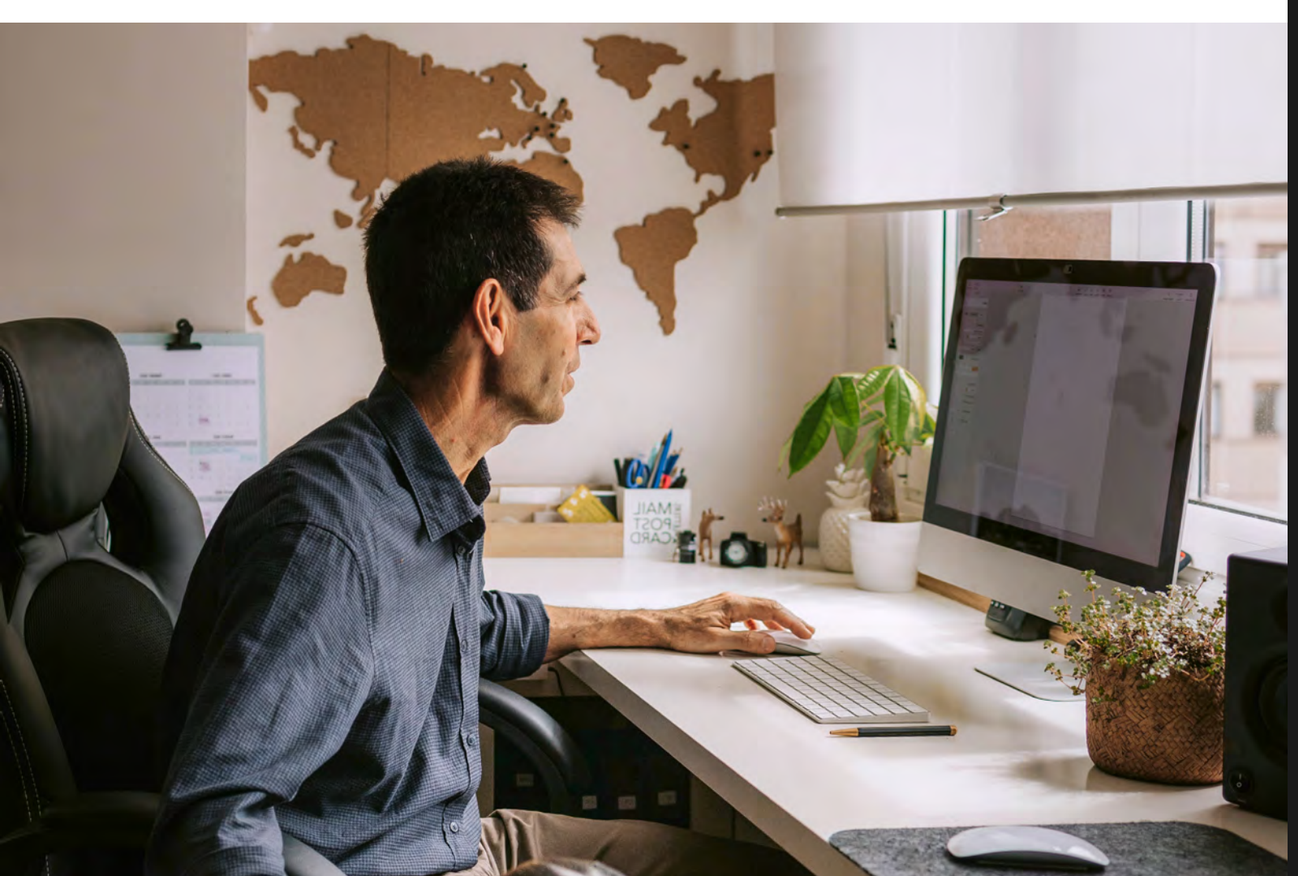
地域別の MFA 導入率

2023 年のレポートでは、地域ごとの MFA の導入率が比較的一様であることを確認し、この傾向が 2024 年も続くと予想しました。特に Okta のお客様は、他の競合サービスと比較して、地域に関係なくユーザーに MFA を適用する割合が高い傾向があります。

Okta のデータはこの見解を裏付けており、北南米、アジア太平洋、ヨーロッパ / 中東 / アフリカでの MFA 導入率は61%から68%の範囲に収まっていました。2023 年と比較すると、北南米とヨーロッパ / 中東 / アフリカでは導入率が 3%上昇した一方、アジア太平洋では 1%低下しました。

重要ポイント

このデータから、Okta がサービスを提供している地域内では、少なくとも地域ごとの集計で見る限り、組織とそのユーザーの所在地は MFA 導入の決定要因ではないと結論付けることができます。



地域別のMFAユーザー導入率

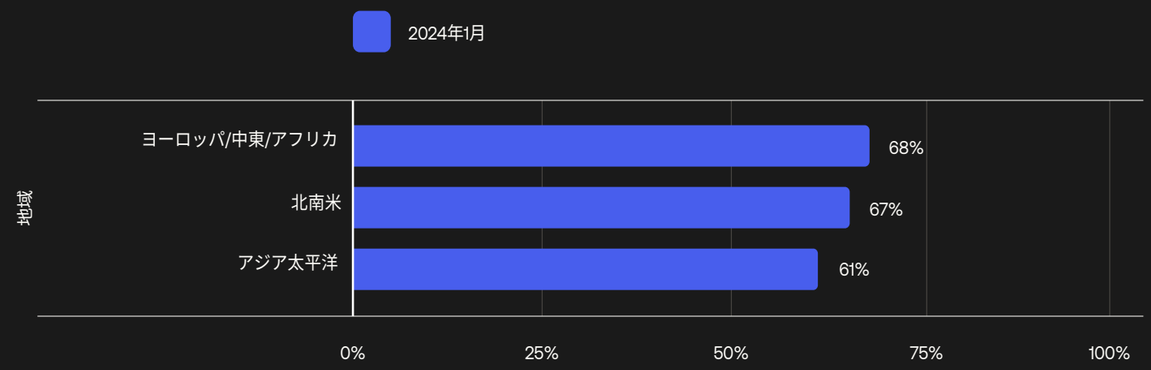


図2：北南米、アジア太平洋、ヨーロッパ/中東/アフリカの各地域における MFAユーザー導入率。

MFA の導入状況

業界別の MFA 導入率

2024 年には、業界ごとの MFA 導入率に依然として大きなばらつきが見られました。導入率が最も高い業界（テクノロジー）と最も低い業界（運輸 / 倉庫）の間の差は 50 ポイントに拡大しました。よくあることですが、「アーリーアダプター」の役割を果たしているテクノロジー部門は、Okta Workforce Identity Cloud を利用しているお客様の中で最も高い MFA 導入率（88%）を記録し続けています。

過去 1 年間で、ほぼすべての業界で MFA の導入率が向上しました。行政機関（48% から 55% へ）[2] と教育部門（64% から 69% へ）は、前年同期比で 5% 以上の増加を記録しました。これらの部門には厳格な規制があるため、比較的低い MFA 導入率からスタートしましたが、現在は追いつきつつあります。最近の米国大統領令や規制の変更が、この傾向をさらに加速させると予想されます。一方で、芸術 / 娯楽 / レジャー部門（57% から 53% へ）と保険部門（77% から 71% へ）では MFA の導入率が減少しました。これらの業界では、多くのビジネスパートナー(保険ブローカーなど) の認証時のユーザーエクスペリエンスが競争の鍵となっています。しかし、これらの中小企業が扱うデータを考慮すると、長期的に見て、パスワードのみやパスワードと SMS MFA の組み合わせが、規制当局から十分と見なされる可能性は低いと考えられます。本レポートでは、セキュリティを損なうことなく優れたユーザーエクスペリエンスを提供するための方法をいくつか紹介します。

重要ポイント

行政機関での進展に特に注目したいと思います。行政機関やその他の連邦規制対象部門にサービスを提供する組織は、最低でも特権アカウントに対して MFA を導入すべきです。2023 年のレポートでは、行政機関の MFA 導入率は民間部門に比べて 16 ポイント以上遅れていました。しかし、今年は行政機関の MFA 導入率が 7 ポイント増加して 55% に達し、今回のデータで最も大きな伸びの一つとなりました。米国大統領令の施行 [3] や、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）が MFA とフィッシング耐性のある認証を繰り返し推奨していることで、米国の公共サービス組織において実際に進展が見られています。

[2] 一部の行政機関職員は、個人識別証明(PIV) やスマートカードをサードパーティの認証方法として使用し、エンタープライズフェデレーションを通じて Okta に接続しています。このユースケースは行政機関の MFA 導入率 55% には含まれず、実際の行政機関の MFA 導入率が過小評価されている可能性があります。Okta は、2023 年にスマートカードをネイティブ認証器タイプとして導入しました。アプリレベルの認証ポリシーや Okta Device Access といった高度な機能を活用するため、X.509 フェデレーションからスマートカード認証器へ移行することを連邦機関に推奨しています。

[3] https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028

地域別のMFAユーザー導入率

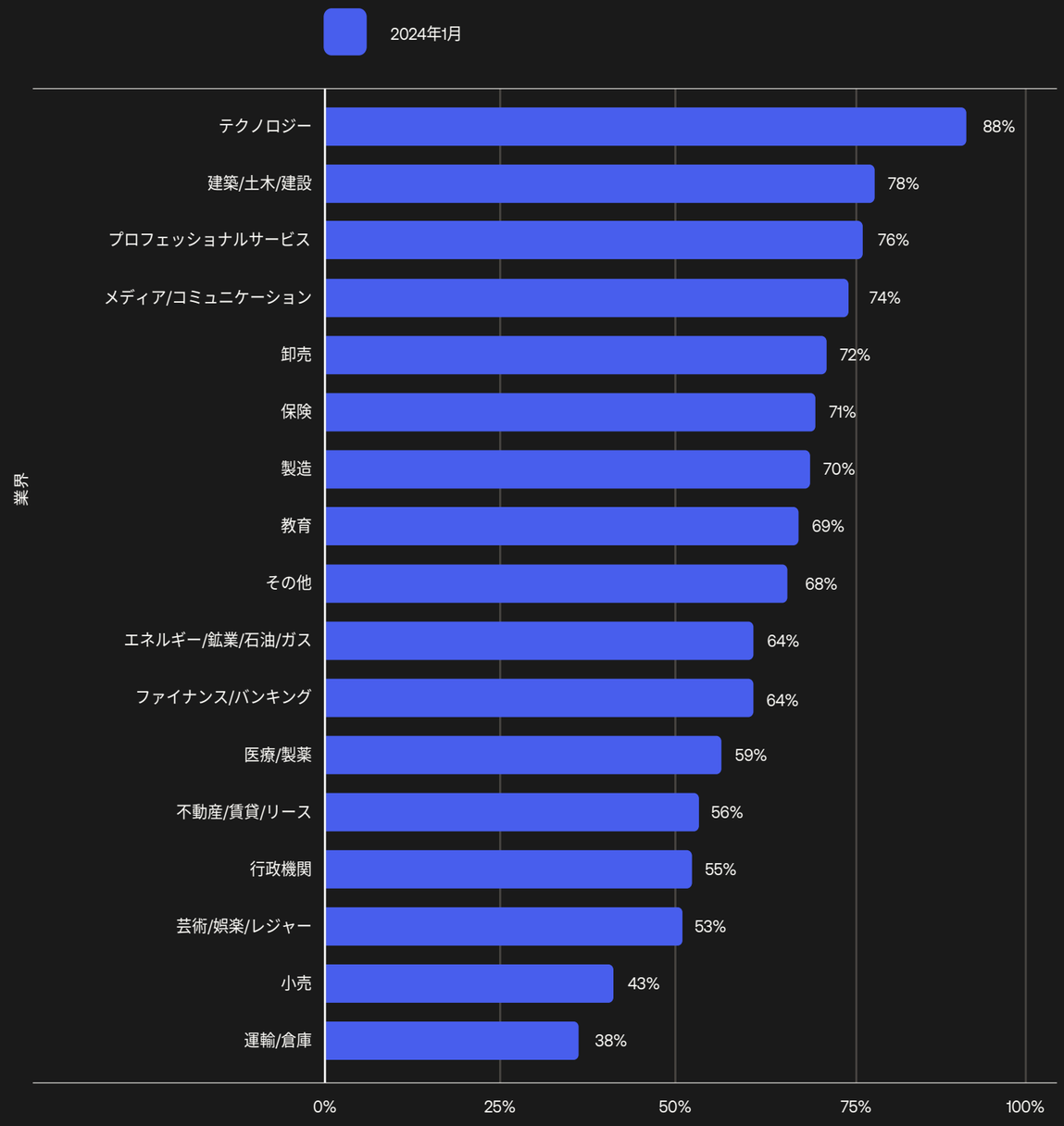


図3：業界別のMFAユーザー導入率（導入率の高い順に掲載）。

MFA の導入状況

組織規模別の MFA 導入率

MFA の導入率を組織規模別に見ると、従業員数が多いほど導入率が低くなる傾向が確認できます。従業員数 300 人未満の組織では導入率が最も高く（82%以上）、従業員数 2 万人以上の組織では導入率が最も低く（59%）なっています。ただし、後者のグループでも前年比 5%の上昇を達成しており、平均を上回る進展が見られます。

この導入率の差には、いくつかの要因が考えられます。行政機関や金融機関と同様に、大規模な企業ではレガシーインフラストラクチャの置き換えが複雑であるため、最新のアイデンティティフレームワークの導入が遅れる傾向があります。また、大規模企業は複数のアイデンティティプロバイダーを利用することが多く、Okta 以外の MFA ソリューションを使用しているケースも考えられます（本レポートは Okta プラットフォームを利用した MFA の導入状況に限定しています）。

重要ポイント

アイデンティティとアクセス管理（IAM）の集中管理が欠如していることは、大企業でも小規模企業でも問題となります。特に大企業は、信頼を損なうセキュリティインシデントがもたらす影響を重く受け止める傾向があり、MFA の適用範囲を拡大するための動機がより強いはずです。

組織規模別のMFAユーザー導入率

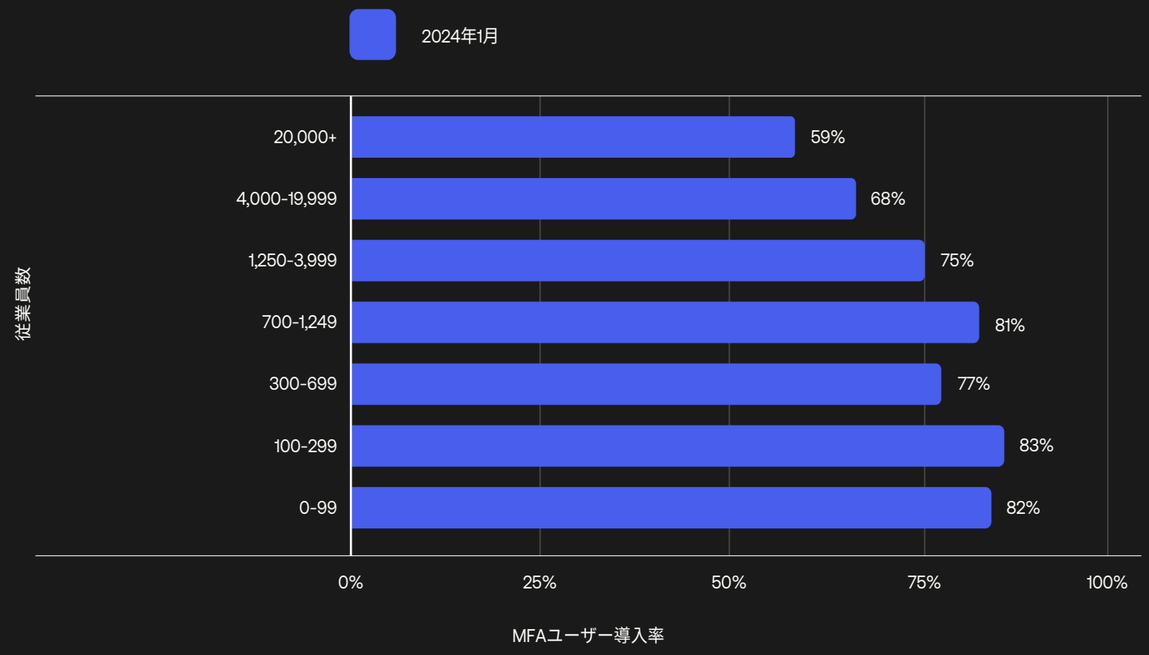


図4：組織規模別のMFAユーザー導入率（従業員数の少ない順に掲載）。

MFA の導入状況

ユーザータイプ別の MFA 導入率

Okta 管理者の MFA 導入率は 91%と非常に高く、昨年から 1%増加しています。ここでは、Okta 管理者のロールを 1 つ以上持つユーザーを管理者と定義し、IT ヘルプデスクから IAM/ セキュリティチームまでを対象に含めています。また、管理者はフィッシング耐性のある MFA を使用する上でロールモデルとなる傾向があります。管理者権限を持つユーザーの中で FIDO2 WebAuthn を導入している割合は、過去 1 年間で 8% から 9% に増加しました。また、管理者ユーザーの中で Okta FastPass を使用している割合は、5% から 13% に増加しました。

Okta は 2024 年 8 月から、Okta Secure Identity Commitment の一環として、管理 / マネジメントコンソールへのアクセスに MFA の構成を必須とするように取り組んでいます[4]。MFA の導入率は、WIC 管理コンソールへの適用開始前から高かったものの、全面的な導入には至っていませんでした[5]。現在の目標は、管理権限を持つ残りのユーザーを対象に、完全な導入を実現することです。

お客様への影響を最小限に抑えるため、この適用措置は既存のサインインフローの複雑さに応じて段階的に実施されています。一部の管理者は Okta WIC に直接ログインしますが、他の管理者はアイデンティティプロバイダーのフェデレーションや特権アクセス管理ソフトウェアとの統合を利用しているためです。Okta は現在、Okta 管理コンソールへの直接アクセスについて単一認証要素のポリシー作成を禁止し、既存の Okta Workforce Cloud テナントの 62%に対してコンソールへのアクセスに MFA を適用しています。

特権ユーザーがパスワードレスでフィッシング耐性のある認証器を使って簡単にサインインするようになることで、ユーザー全体の MFA 導入が加速することが期待されます。

重要ポイント

Okta が管理アプリで MFA を必須としたことは、IT/ セキュリティ担当者にとって組織全体の認証戦略を見直すきっかけとなります。この機会を活用し、すべての管理コンソールをはじめとして、高リスクまたは業務上重要なアプリケーションのサインインポリシーを徹底的に見直すことが推奨されます。

アプリケーション固有の認証ポリシーを活用し、高リスクまたは業務上重要なアプリケーションには強力な認証を適用する一方で、リスクの低いアプリケーションにはより簡易な認証を認めることで、導入を円滑に進めることができます。このアプローチにより、ビジネスのスピードを損なうことなく、組織のセキュリティを強化できます。

[4] https://support.okta.com/help/s/blog/a674z000000147HAAQ/mfa-enforcement-for-the-admin-console?language=en_US

[5] 管理者による MFA を使用した Okta 管理コンソールへのアクセス率は、管理者全体の MFA 導入率とは異なる測定基準です。前者は Okta 管理コンソールへのアクセスのみに焦点を当てており、後者はすべてのアプリケーションへのアクセスを対象としています。また、前者は管理コンソールにアクセスするたびに MFA が必要であるのに対し、後者では 1 か月に少なくとも 1 回 MFA を利用すれば測定基準を満たします。

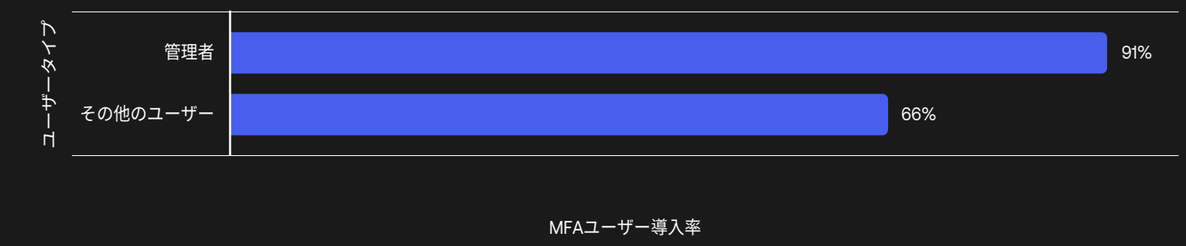


図5：ユーザータイプ別（管理者、その他のユーザー）のMFAユーザー導入率。

MFA の導入状況

認証器タイプ別の MFA 導入率

Okta Identity Cloud は、プラットフォームに依存せず、お客様が最適なテクノロジーを利用できるように設計されています。Okta は、あらゆるユースケースに対応できるよう、自社製および他社製の幅広い MFA 認証器を提供しています。これらの認証器は、基盤となる認証メカニズムに基づき、パスワード認証器、従来型 MFA 認証器、フィッシング耐性のある MFA 認証器の 3 つに分類されます。

従来型 MFA 認証器には、E メール、ハードウェアトークン、プッシュ通知、セキュリティ質問、SMS、ソフトトークンが含まれます。フィッシング耐性のある MFA 認証器には、Okta FastPass、FIDO2 WebAuthn、スマートカードが含まれます。表 1 に示すように、Okta は各認証器タイプにベンダーが提供するオプションを可能な限り含めています。ただし、認証データが認証器タイプごとに分離できない場合や、カスタムオプションを含む場合は、「その他」のカテゴリに分類し、さらなる分析からは除外しました。

表 1：認証器のタイプとプロパティ

この表には、MFA の導入、ユーザビリティ / セキュリティのプロパティ、認証器の主要な特徴の調査に使用した認証器タイプを一覧しています。

認証器タイプ	Okta でサポートされる認証器（認証器の導入に関する調査で使用）	認証器名:タイプ(ユーザビリティとセキュリティの調査で使用）	認証要素タイプ	保証レベル
パスワード	パスワード	パスワード	知識要素	低
E メール	E メールコードとリンク（別名マジックリンク）の組み合わせ	E メールコードとリンクの組み合わせ	所有要素	低
ハードウェアトークン	YubiKey OTP、RSA SecurID、カスタム TOTP	YubiKey OTP	所有要素	中
プッシュ	Okta Verify 認証器、プッシュ方式、Duo 認証器	Okta Verify のプッシュ通知	所有要素 所有要素＋生体要素	中
セキュリティ質問	セキュリティ質問	セキュリティ質問	知識要素	低
SMS	SMS、Duo 認証器	SMS	所有要素	低
ソフトトークン	Okta Verify OTP、Google Authenticator、RSA SecurID、カスタム TOTP、Duo 認証器	Okta Verify OTP、Google Authenticator	所有要素	低
音声	電話認証器の音声方式、Duo 認証器	電話認証器の音声方式	所有要素	低
FastPass	Okta Verify 認証器、FastPass 方式	Okta FastPass	所有要素 所有要素＋生体要素	高
WebAuthn	WebAuthn 認証器（Mac Touch ID、Android Fingerprint、Windows Hello、YubiKey、Google Titan、パスキーの組み合わせ）、Duo 認証器	WebAuthn 認証器（Mac Touch ID、Android Fingerprint、Windows Hello、YubiKey、Google Titan、パスキーの組み合わせ）	所有要素 所有要素＋生体要素	高
スマートカード	スマートカード	PIV、CAC の組み合わせ	所有要素＋知識要素	高

パスワードが職場環境で依然として広く使われているのは驚くことではありません。しかし、パスワードレス認証の導入も拡大しており、2023 年 1 月の 2%未満から 2024 年 1 月には約 5%にまで増加しています。最も利用されている MFA 認証器はプッシュ通知（29%）であり、これに SMS（17%）とソフトトークン（14%）が続いています。

従来型 MFA 認証器の導入率は昨年と比較して高まったものの、全体で 1.3%という微増にとどまりました。過去 3 年間で MFA 全体の導入率は 14%増加しましたが、同期間中に SMS MFA の導入率の増加はわずか 1.2%でした。これに対して、フィッシング耐性のある認証器の導入は大幅に拡大しています。たとえば、WebAuthn の導入率は 2023 年の 2%から 2024 年には 3%に増加し、Okta Verify FastPass の導入率は同じ期間で 2%から 6%に増加しました。

フィッシング耐性のある認証の導入を促進している重要な要因は 3 つあります。1 つ目の要因は、フィッシング攻撃の脅威が増え続けていることです。たとえば、Okta のセキュリティチームによると、フィッシングによるなりすまし被害を受けた組織の数は、2023 年 2 月から 2024 年 1 月にかけて前年同期比で 50%増加しました。同様に、Zscaler のネットワークセキュリティ製品のデータでは、昨年のフィッシング攻撃が 58%増加したことが報告されています[6]。

2 つ目の要因は、フィッシング耐性のあるオプションが利用可能になっていることです。Okta は、Okta FastPass や FIDO2 WebAuthn など、フィッシング耐性のある認証器を幅広くサポートしています。こうしたテクノロジーを簡単に利用可能にすることが、導入率に直接的な影響を与えています。FastPass は Okta Verify に組み込まれたパスワードレスでフィッシング耐性のあるサインイン方法です。Okta Identity Engine への無料アップグレードの一環として、Okta はすべてのお客様を対象に FastPass の提供を開始しました。2023 年 2 月から 2024 年 1 月の間に、OIE へ移行またはアップグレードした新しいテナントのうち、7%が最初の 90 日以内に FastPass を試用したことが確認されました。

3 つ目の要因として、規制コンプライアンスもフィッシング耐性のある認証要素の導入をさらに促進する役割を果たすと考えられます。たとえば、オーストラリアの行政機関は、Essential Eight（サイバーセキュリティ対策フレームワーク）の管理策の成熟度レベル 2 およびレベル 3 を満たすために、フィッシング耐性のある認証方法を導入する必要があります。

重要ポイント

OIE は、ログインフローの管理でより高い柔軟性を提供します。たとえば、アプリケーションのサインオンポリシーでは、管理者がアプリケーションごとに個別のルールを構成し、Okta FastPass によりパスワードレスでフィッシング耐性のある認証器をユーザーに提供できます。Okta は、管理者の利便性だけでなくユーザーの利益を最大限に高めるために、より強力な認証器を評価して導入することをお客様に推奨しています。たとえば、SMS 認証器は信頼レベルが低く、SIM スワッピング攻撃のリスクがあり、運用コストも高いことが知られています。最良の結果を得るには、IT チームとセキュリティチームの両方がアップグレードに関与して、迅速に最大の価値を引き出し、組織に最適な認証戦略を評価することが重要です。

[6] https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report

認証器別のMFAユーザー導入率

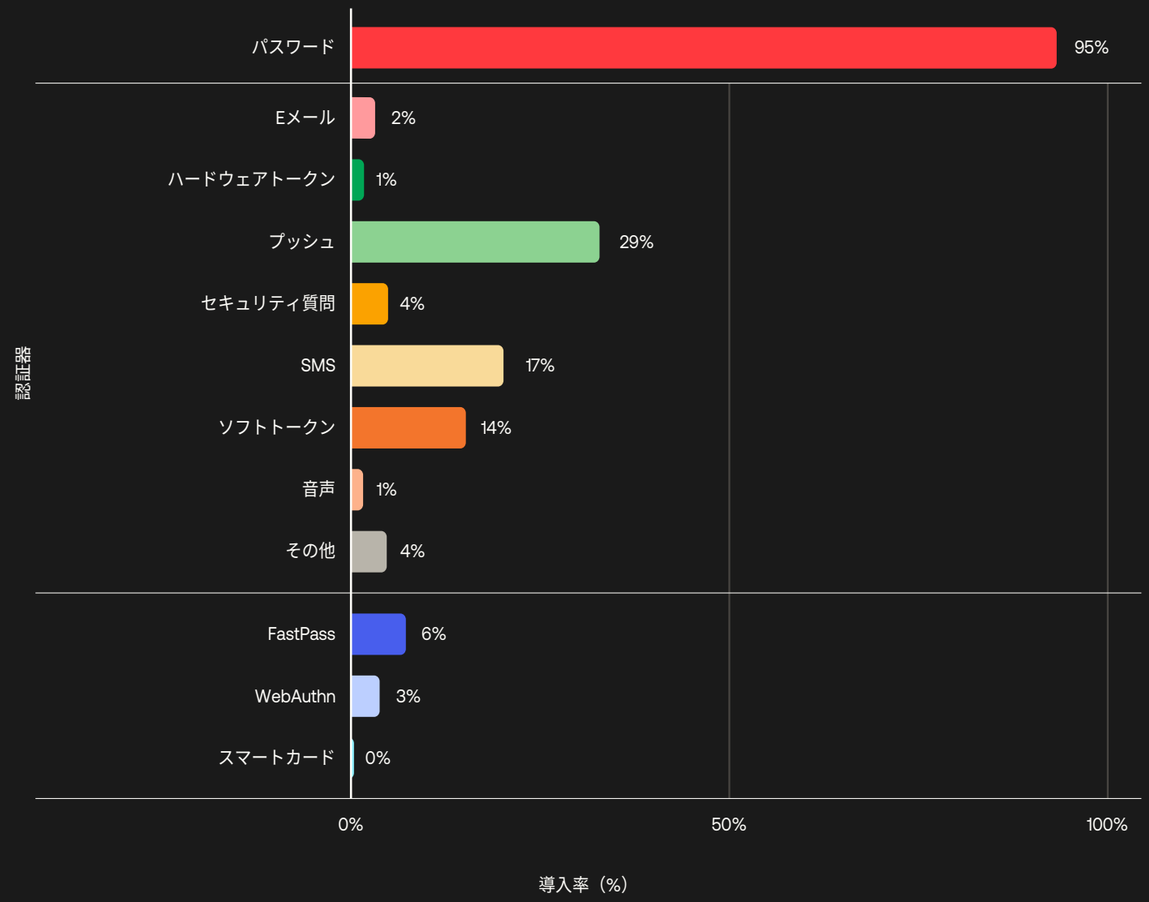


図6：Okta Workforce Identity Cloudで利用可能な認証器別のMFAユーザー導入率。ユーザーが認証に複数の認証器を使用している可能性があるため、各認証器の導入率の合計はMFA導入率よりも高くなります。

認証器のユーザビリティとセキュリティに関するデータ主導の評価

MFA の導入が進んでいるとはいえ、依然として乗り越えなければならない障壁があります。どの認証器を導入すべきかについて、CIO、CSO、ポリシー策定担当者が十分な情報を得て判断するには、それぞれの認証器の長所と短所を理解することが役立ちます。

そのためにOktaは、ユーザビリティとセキュリティの両方のプロパティについて、認証器を評価するフレームワークを開発しました（評価カテゴリは表 2 を参照）。その結果から得られるデータ主導の洞察は、セキュリティ /IT リーダーが組織の保護を強化し、製品開発の指針を得る上で役立ちます。

2023 年版レポートをご覧いただいた方は、このセクションに見覚えがあるかもしれません。2024 年版では指標を更新しましたが、パスワードを入力する時間や E メールのコードを受け取る時間はほとんど変化していません。ただし、今年の調査では、OIE に移行した組織の増加に伴い、より多くのユーザーやイベントが対象になっています。さらに、Okta の IT/ セキュリティ実務者の調査結果を基に、測定基準の相対的な重み付けを決定する方法論を改良しました。このように改訂された実用的な基準を使用しましたが、フィッシング耐性のある認証器を使用する利点については前回同様の結論に至りました。加えて、スマートカード認証器の測定基準データも新たに追加しました。このセクションの洞察は、FastPass や WebAuthn などの最新の認証方法を評価する際に役立つと考えられます。

認証器のユーザビリティとセキュリティのプロパティ

認証器のチャレンジ時間

パスワードを使用した 2 つのシナリオ
パスワード認証器のチャレンジ時間については、2 つの UI 構成オプションによるデータを含めました。

- **ユーザー名とパスワードのフロー**では、サインイン時に同じページにユーザー名とパスワードのフィールドが表示されます。
- **パスワードのみのフロー**では、ユーザーは最初に表示されるページでユーザー名を入力し、次のページでパスワードの入力を促されます。

他のすべての MFA 認証方式では、チャレンジの前にユーザーがアカウントを特定する必要がありません。そのため、パスワード認証器のチャレンジ時間の中央値を他の認証器のチャレンジ時間と比較する上では、パスワードのみのシナリオが最も適した条件となります。この点を認識した上で、本レポートではあえて両方のフローをチャートに含めています。

認証器のチャレンジ時間は、ユーザーが認証器プロンプトを正常に完了するまでにかかる時間の中央値です。

認証器のチャレンジ時間の中央値は前年比で一貫しており、パスワード認証のチャレンジ時間の中央値は約 6 秒で推移しています。パスワードのチャレンジ時間が比較的短い傾向があるのは、パスワードマネージャーやブラウザの自動入力補助によるものと考えられます。パスワードから始まる認証フローでは、OTP の入力によって 12 秒以上長くなります。ユーザーが OTP を E メールや音声通話で取得する必要がある場合は、さらに時間がかかります。

Okta のデータには、所有要素と内在要素（生体認証など）を組み合わせた認証器が、最速のチャレンジ時間（4 秒）を実現することが示されています。他の認証器と比べて、FIDO2 WebAuthn、Okta FastPass（その名のとおり）、スマートカードは認証プロセスを劇的に効率化します。認証が高速化することで、機密性の高いアプリへのアクセス時に再認証の頻度を上げたり、ステップアップ認証として利用したりできるようになります。どちらもセッションハイジャック攻撃に対する重要な防御策となります。

重要ポイント

ワークフォースアプリケーションへのアクセスに 2 つの異なる認証要素が必要となる場合（NIST AAL2 の最低要件）、ユーザーエクスペリエンス（チャレンジ時間）の観点では、FIDO2 WebAuthn や Okta FastPass が最良の選択肢となります。さらに都合の良いことに、この 2 つは最善のセキュリティ成果（フィッシング耐性）も実現します。

これらの認証器は、通常は 4 秒以内に所有要素と内在要素を提供します。これは、パスワードと OTP ベースのチャレンジを組み合わせる場合と比べて数倍の速度です。

認証器のチャレンジ時間

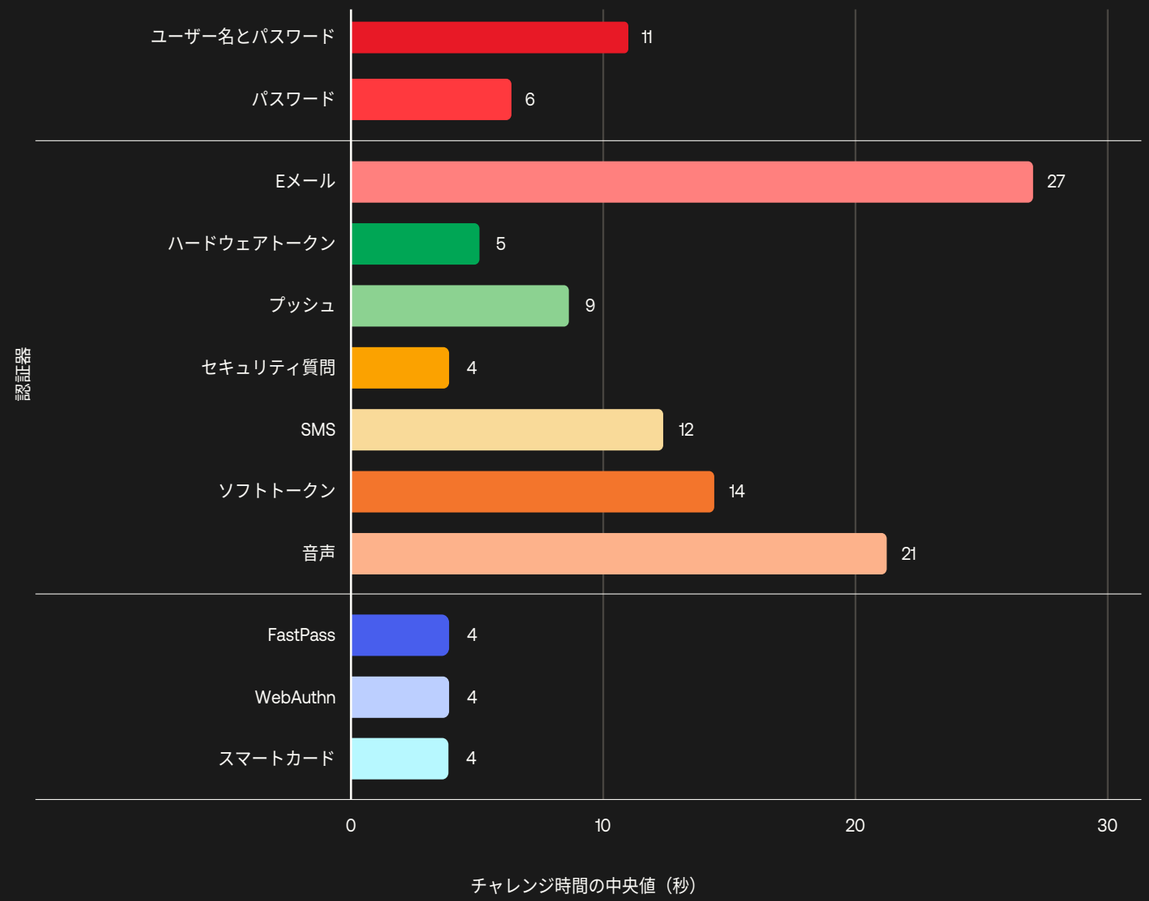


図7：パスワード（ユーザー名とパスワードのフロー、パスワードのみのフロー）、Eメール、ハードウェアトークン、プッシュ、セキュリティ質問、SMS、ソフトトークン、音声、FastPass、WebAuthn、スマートカード認証器のチャレンジ時間の中央値。

“

シンプルな MFA では、もはや十分に防御できません。Okta FastPass によって、容易に対策を強化し、フィッシング耐性のある MFA に加え、デバイスのコンテキストに応じた態勢認識を確立できます。フィッシング耐性を実現し、機密性の高いアプリケーションへのアクセスを管理デバイスに限定することで、攻撃の可能性を大幅に下げることができます。また、デバイス保証コントロールの活用によって、デバイスが適切にパッチ適用され、アクセス時に必要なコントロールが機能するよう確保できます。

しかし、セキュリティは単に厳格化すればよいのではありません。厳しい制御がユーザーエクスペリエンスを損なってしまえば本末転倒です。このため、当社はパスワードレスを推進しています。フィッシング耐性、管理デバイス、生体認証によるユーザー確認、デバイスのセキュリティ態勢を組み合わせることで、AAL2 を達成し、それ以上のセキュリティを確保しながら、エンドユーザーの日常的なエクスペリエンスを向上させることができます。”

Andrew Meinert 氏

システムオペレーション担当ディレクター

HubSpot

認証器のユーザビリティとセキュリティのプロパティ

認証器の登録時間

認証器の登録時間は、ユーザーが認証器を登録するのにかかる時間の中央値です。認証器登録ページが表示された時点から、ユーザーが提供された指示に従って登録に成功した時点までを指します。

認証器の登録、リセット、パスワードの回復によって、一時的にリスクが高まります。管理者は、登録やリセットの各イベントについて、「ユーザーのアイデンティティを開始し検証するために、どの認証器を要求するか」というルールを適用できます（また、適用すべきです）。この目的のために、フィッシング耐性のある認証器を構成することが推奨されます。

パスワードの登録にかかる時間の中央値は約 35 秒です。これには、ユーザーが新しいパスワードを作成し、パスワードを確認（再入力）し、他の認証済みデバイスからサインアウトするかどうかを選択する時間も含まれます。セキュリティ質問は、ユーザーがセキュリティ質問を選択または作成し、答えを入力する必要があるため、登録時間の中央値が最も長く（40 秒）なります。

Okta の認証器登録フローは、Okta Verify OTP、Okta Verify Push、Okta FastPass を Okta Verify アプリを使って一緒に登録できるように設計されています。1 回の動作で複数の認証器タイプを登録する場合、ユーザーが QR コードをスキャンし、Okta Verify の構成プロセスを完了するのに必要な時間を含め、登録にかかる時間の中央値は約 38 秒です。ハードウェア OTP、音声、SMS、FIDO2 WebAuthn は、25 秒未満という非常に短い登録時間を実現します。スマートカードの登録プロセスには、オフラインでのユーザー確認、スマートカードの製造、発送が含まれます。新しいスマートカードを取得するには数週間かかる場合があります。このようなプロセスは、Okta のアイデンティティプラットフォームでは可視化できません。

重要ポイント

興味深いことに、2023 年以降、全体的に登録の所要時間が若干長くなっています。登録は手動で行われるプロセスであるため、人的な要因や技術的な要因が関与している可能性があります。

このような負担を軽減するため、自動化された登録プロセスを導入する組織が増えています。たとえば、2024 年 4 月に Okta は YubiKey との提携を発表し、事前登録済みの YubiKey を従業員の自宅に直接配送できるようにしました。これによって、キーを挿入して初期 PIN を入力するだけでユーザー操作が完了し、従業員はほぼ即座に業務を開始できるようになりました。

認証器の登録時間

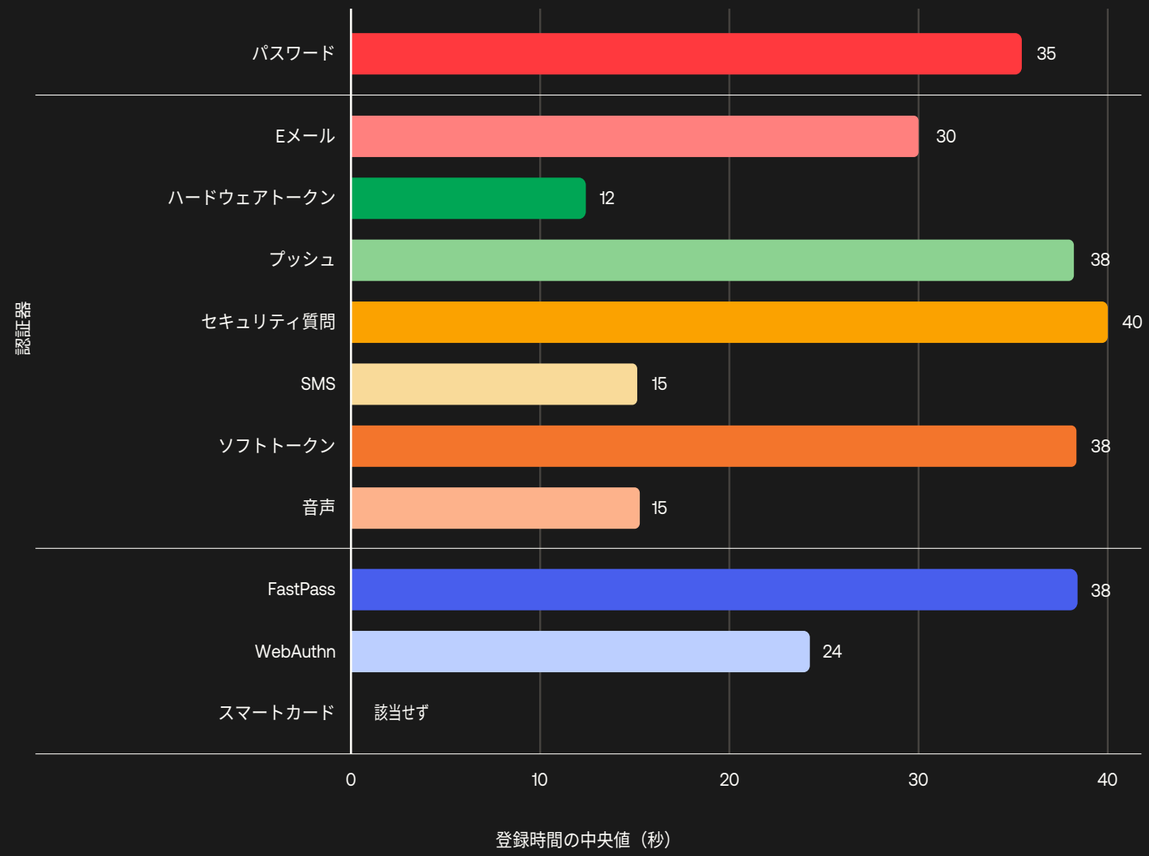


図8：パスワード、Eメール、ハードウェアトークン、プッシュ、セキュリティ質問、SMS、ソフトトークン、音声、FastPass、WebAuthn、スマートカード認証器の登録時間の中央値。ユーザー検証に費やされた時間は、認証器自体ではなく、登録ポリシーとリカバリポリシーによって決定されるため、この分析から除外されています。

認証器のユーザビリティとセキュリティのプロパティ

認証器のチャレンジ失敗率

認証器のチャレンジ失敗率は、認証に失敗した回数を、認証器を使用して Okta のバックエンドサーバーが受信した認証試行回数の合計で割ったものです。

認証の失敗は、予想以上の頻繁で起こっています。たとえば、ユーザーがパスワードやセキュリティ質問の入力を誤った場合、OTP の入力を誤った場合、プッシュ要求を拒否した場合、Okta FastPass や FIDO2 WebAuthn などの生体認証器を使用した認証の応答署名が無効な場合などのイベントが含まれます。

認証失敗イベントは悪意の有無に関連することから、認証器のチャレンジ失敗率はユーザビリティとセキュリティの両方の指標となります。悪意のない試行の失敗率が高いということは、ユーザーが認証中に所定の認証器を使用してミスを犯す可能性が高く、生産性が低下することを意味します。不審な試行の失敗率が高いということは、一般的に、こうした方法を攻撃者が「ソフトターゲット」と考えていることを示しています。残念ながら、本レポートで Okta が使用している匿名化データには、通常のイベントと悪意のあるイベントを区別するために必要な利用パターンの詳細が含まれていません。ただし、それぞれの環境に特化したレポートについては、お客様の社内セキュリティチームが作成できる可能性があります。

Okta のデータからは、最も大きな負担をユーザーに課すのが知識ベースの認証器であり、これに各種ワンタイムパスワードが続いていることが明らかになっています。シンプルなパスワードは失敗率が最も高く（約 10%）、次いでソフトトークン、E メールで送信される認証チャレンジ、セキュリティ質問の順となっています。

FIDO2 WebAuthn とスマートカードの認証には、ユーザーによる意図しない操作ミスや不審な試行を減らし、失敗率を低くする効果が期待できます。ただし、これには注意点があります。WebAuthn とスマートカードの実装は、他の認証方法と完全に一致しているわけではなく、設計上、認証アクションはユーザーのシステム上で行われます。そのため、アイデンティティプロバイダー（Okta）がこれらの認証器に関連する失敗イベントをすべての把握することはできません。たとえば、ユーザーが FIDO2 WebAuthn を使用してフィッシングプロキシにサインインしようとし、認証器がドメインの不一致を検知した場合、この情報をアイデンティティプロバイダーのバックエンドサーバーに送信するメカニズムはありません。そのため、管理者は悪意のある認証の試みの件数を正確に報告できません。

重要ポイント

WebAuthn の失敗率に関する注意点を考慮に入れても、フィッシング耐性のある認証形態が最善のユーザーエクスペリエンスを提供することを改めて理解できます。

認証器のチャレンジ失敗率

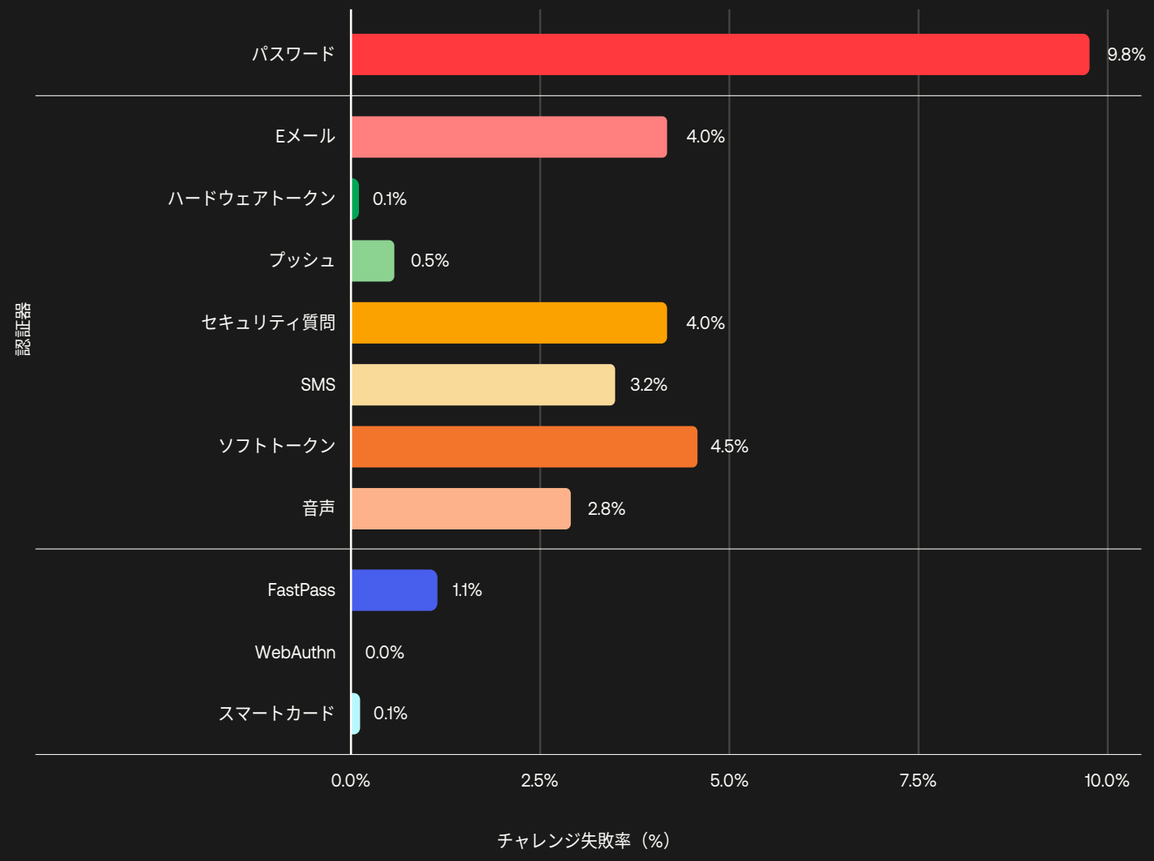


図9：パスワード、Eメール、ハードウェアトークン、プッシュ、セキュリティ質問、SMS、ソフトトークン、音声、FastPass、WebAuthn、スマートカード認証器のチャレンジ失敗率。

認証器のユーザビリティとセキュリティのプロパティ

フィッシング耐性範囲

フィッシング耐性範囲は、NIST によるフィッシング耐性の定義を満たす認証器によって保護できるユーザーの割合を指します。

認証器にフィッシング耐性がない場合、そのフィッシング耐性範囲はゼロになります。フィッシング耐性のある認証器の場合、そのフィッシング耐性範囲は、この機能をサポートするブラウザやオペレーティングシステムを使用するユーザーの割合に等しくなります。この基準によると、フィッシング耐性範囲がゼロを超える認証器は、Okta FastPass、FIDO WebAuthn、スマートカードの 3 つだけです。

FIDO 2 WebAuthn に対応するブラウザやプラットフォームでは、FIDO ベースのフィッシング耐性認証をログインページに追加できます。caniuse.com によると、ブラウザやプラットフォームで WebAuthn を利用可能なデバイスは 96% に上ります。しかし、どの WebAuthn 認証器についても、WebAuthn のフィッシング耐性範囲は理論的な上限値になります。たとえば、WebAuthn プラットフォーム認証器は一部のプラットフォームでしかサポートされない場合があるため、実際のフィッシング耐性範囲はグラフに示す理想的な範囲よりもはるかに小さくなる可能性があります。

Okta FastPass は、認証情報のフィッシング攻撃を防ぐ上でも効果的であり、認証の試みが行われるたびに発信元の URL を検証することで、これを実現しています。FastPass は、Windows、macOS、Android、iOS といったプラットフォーム全体でフィッシング耐性を提供します。caniuse.com が示すブラウザおよびプラットフォームの利用比率を基にすると、従業員向け環境では約 95% のユーザーが FastPass のフィッシング耐性機能を利用できます。

重要ポイント

WebAuthn と FastPass はどちらもフィッシング耐性を提供します。従来、WebAuthn の実装は、物理的なセキュリティキーのようなローミング認証器や、Face ID や Windows Hello のようなプラットフォーム認証器として、単一デバイスで使用する認証情報が一般的でした。しかし昨年、FIDO と主要な OS プラットフォームベンダーは、ユーザーが複数のデバイス間で同期できる WebAuthn 認証情報として、マルチデバイス対応のパスキーを導入しました。

すべての WebAuthn の実装にはフィッシング耐性があります。しかし、すべての実装が同じというわけではありません。たとえば、Windows、MacOS、iOS、Android 間の実装の違いは、混乱を招き、ユーザーエクスペリエンスを損なう可能性があります。マルチデバイス対応パスキーの導入は、消費者向け認証では大きな進歩ですが、従業員向け環境では、デバイス間でのパスキーの移動が企業ポリシー違反の問題となる可能性があります。また、一部のオペレーティングシステムプロバイダーがデバイスに紐付けられた WebAuthn のサポートを終了し、マルチデバイス対応パスキーを優先したことで、ユーザーエクスペリエンスが直感的でなくなるケースもあります [7]。

FastPass は、Workforce 向けのユースケースやセキュリティモデルに合わせて設計されており、強力なデバイスバインディングやデバイス保証態勢のチェックを提供します。また、デスクトップやモバイルを含むすべてのプラットフォームで一貫した外観と操作性を維持し、利用可能な最も強力な認証方法を使用するようユーザーに促します。

スマートカードは専用のハードウェアを必要とするため、一般的に、均質な IT インフラストラクチャを整える余裕がある高度に規制された業界での実装に限定されます。

[7] https://passkeys.dev/device-support/

認証器別のフィッシング耐性範囲

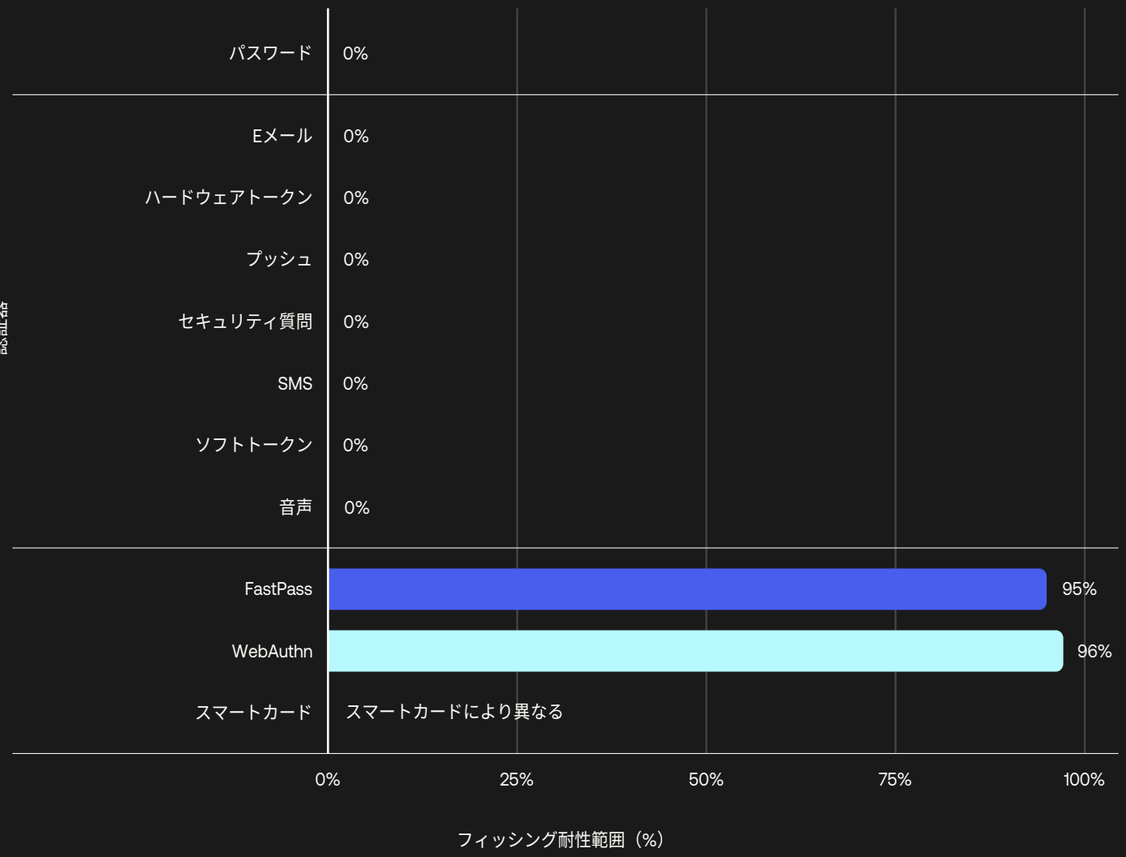


図10：パスワード、Eメール、ハードウェアトークン、プッシュ、セキュリティ質問、SMS、ソフトトークン、音声、FastPass、WebAuthn、スマートカード認証器のフィッシング耐性範囲。

認証器のユーザビリティとセキュリティのプロパティ

フィッシング耐性アラート範囲

フィッシング耐性アラート範囲とは、オリジンチェックに失敗した要求をログに記録できる認証器によって潜在的に保護されるユーザーの割合を指し、中間者攻撃（AiTM）の一般的な指標となります。

現在、Okta FastPass は、フィッシングの試みがオリジンチェックに失敗した場合でも、サーバーサイドのイベントを作成できる唯一の認証器です。フィッシングサイトのドメイン名や Cookie の不一致が検出されると、FastPass は要求を拒否し、エンドユーザーと管理者に警告を送ります。また、脅威に対するユーザーや組織の認識も高まり、悪意のあるアクティビティを検出して対応する能力が向上します。

FastPass が真価を発揮

2023 年初頭に OIE にアップグレードし、FastPass を展開した Okta のお客様で実際に起こった事件をご紹介します。

2024 年 7 月の夕刻、数百の組織を標的とする広範なソーシャルエンジニアリングキャンペーンが発生している中、このお客様の社内でも従業員の 1 人が攻撃の電話を受けました。同社の実際の電話番号を偽装し、アメリカ英語のアクセントで IT チームを名乗る発信者は、企業ドメインによく似た Web サイトにログインするよう従業員に求めました。従業員は Okta FastPass を利用していましたが、ドメインと認証情報が自社の Okta org と一致しなかったため、FastPass がログインを拒否しました。その後の 5 分間で、攻撃者はフィッシングサイトへのログインを何度も従業員に試みさせましたが、FastPass がすべて拒否しました。一方、セキュリティチームは、他のユーザーに対するソーシャルエンジニアリングの失敗を検知して警戒を強めていたため、この従業員のログイン失敗をシステムログで迅速に把握し、標的となった従業員のアクセスを一時的に削除しました。こうした一連の対応により、翌朝にはこの従業員も必要なアクセスを復旧し、通常どおり業務に戻ることができました。

その後の調査で、FastPass とそのアラート適用範囲によって、ソーシャルエンジニアリング攻撃によるアカウント乗っ取りが阻止され、同時に従業員の生産性への影響も最小限に抑えられたことが明らかになりました。

注目すべきは、FastPass が従来の定義による単なる認証器ではない点です。デバイス管理状態、OS バージョン、デバイスロック、ディスク暗号化、脱獄やルート化の検出といったデバイスコンテキストのシグナルを収集することも可能です。また、FastPass は Jamf、Microsoft Intune、Workspace One、CrowdStrike、Windows Security Center、Chrome Device Trust などの UEM（統合エンドポイント管理）および EDR（エンドポイント検出 / 対応）ベンダーと統合し[8]、認証に使用されるデバイスが管理されていること、適切なセキュリティ状態を示していることを保証します。このコンテキスト情報により、脅威検知の精度をさらに高め、認証ポリシーの適用を強化できます。

重要ポイント

サイバー攻撃対策で、検出 / 対応スピードが主要な差別化要因となっています。こうした状況では、ソーシャルエンジニアリングや AiTM フィッシングキャンペーンを事前に検出してアラートを発する機能の重要性が、今後さらに高まっていくと予想されます。Okta FastPass のアラート機能を活用することで、フィッシングに対するほぼリアルタイムの防御と検出を実現できます。

[8] https://support.okta.com/resource/device_context_deployment_guide

認証器別のフィッシング耐性アラート範囲

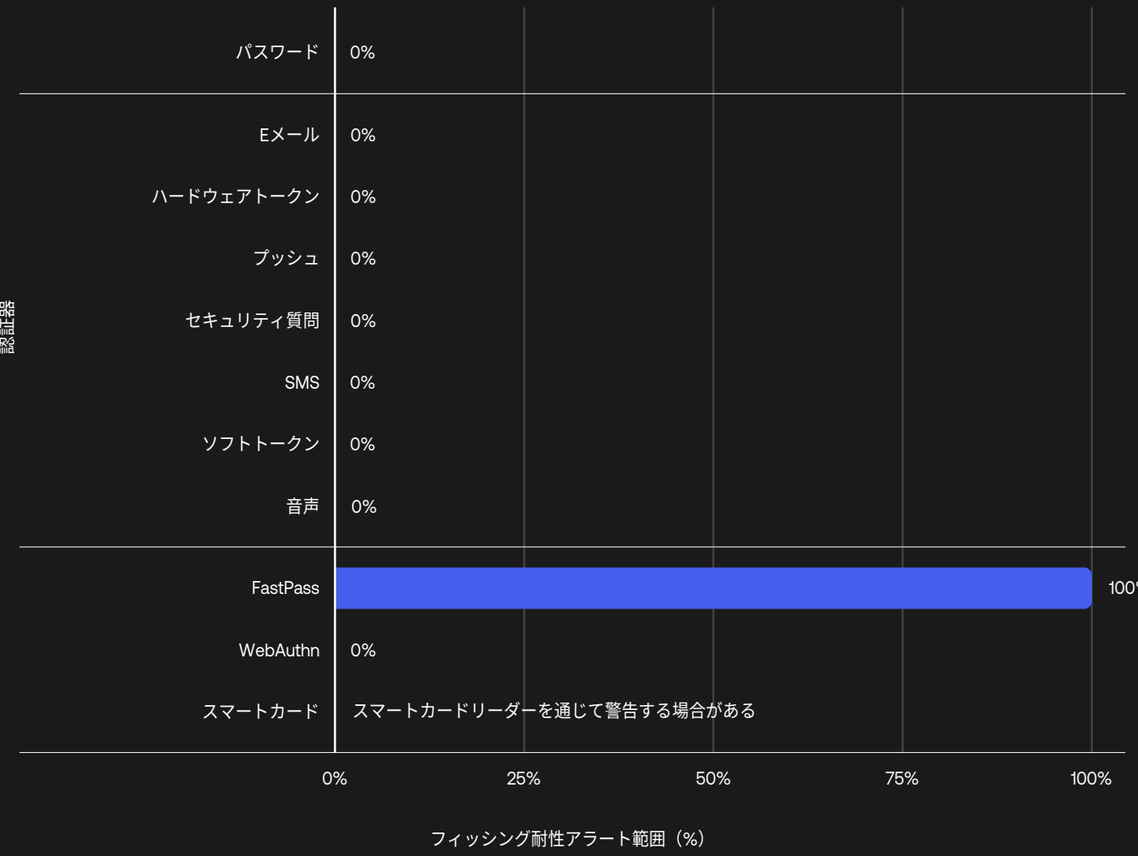


図11：パスワード、Eメール、ハードウェアトークン、プッシュ、セキュリティ質問、SMS、ソフトトークン、音声、FastPass、WebAuthn認証器のフィッシング耐性アラート範囲。

認証器のユーザビリティとセキュリティのプロパティ

認証器の総当たり攻撃チャレンジ失敗率

総当たり攻撃失敗率は、1 日で N 回を上回って認証に失敗したユーザー数を、同じ認証器を使ってサインインしたユーザー数に対する割合として表したものです。

総当たり攻撃の失敗は、悪意のあるユーザーまたは善意のユーザーが認証に N を超える回数失敗した場合に発生します（N は、総当たり攻撃の失敗を定義するためのしきい値）。正当なユーザーが 10 回を超えて試行を行う可能性は極めて低いと考えられるため、本レポートでは N=10 として分析を行っています。攻撃者は、パスワードや OTP の推測の自動化や認証チャレンジの繰り返し生成により、ユーザーを騙したり疲労させたりしてアクセスを承認させようと試みることがあります。そのため、総当たり攻撃失敗率は、特定の認証器に対して総当たり攻撃を実行する上での攻撃者の好みを反映しているとも言えます。

2023 年のレポートで確認されたように、知識ベースのシークレットは、引き続き自動攻撃ツールの主要な標的となっており、繰り返し失敗してもログインを試みる正当なユーザーにとっても大きな負担となっています。FIDO2 WebAuthn は、総当たり攻撃失敗率が最も低くなっていますが、上記で指摘したとおり、標準の実装により失敗がすべて Okta に報告されるわけではないため、失敗率が実態よりも低く見える可能性があります。

FastPass の動作は他の認証器とは異なり、2 つのプロービング方式があります。サイレントプロービング（サイレント認証）は、Okta サインインウィジェットがデバイスに FastPass が構成されているかを自動的に確認し、ユーザーの操作なしで認証を実行することが可能です。一方、インタラクティブプロービング（標準的な認証）は、FastPass 認証器を使用してユーザーがログインする際にトリガーされ、従来の方法で動作します。サイレント認証はバックグラウンドで動作し、ユーザーに負担をかけることなく頻繁にデバイスやユーザーの状態を確認します。そのため、他の認証器より頻繁に FastPass チャレンジが発生し、FastPass の総当たり攻撃チャレンジ失敗率が比較的高い理由の 1 つになっていると考えられます。

重要ポイント

MFA バイパスイベントが増加している一方で、従来の総当たり攻撃は主として知識ベースの認証器に焦点を当てています。所有要素や生体要素に基づく認証器を使用することで、総当たり攻撃によるアカウント乗っ取りの確率を劇的に減らすことができます。

認証器別の総当たり攻撃失敗率

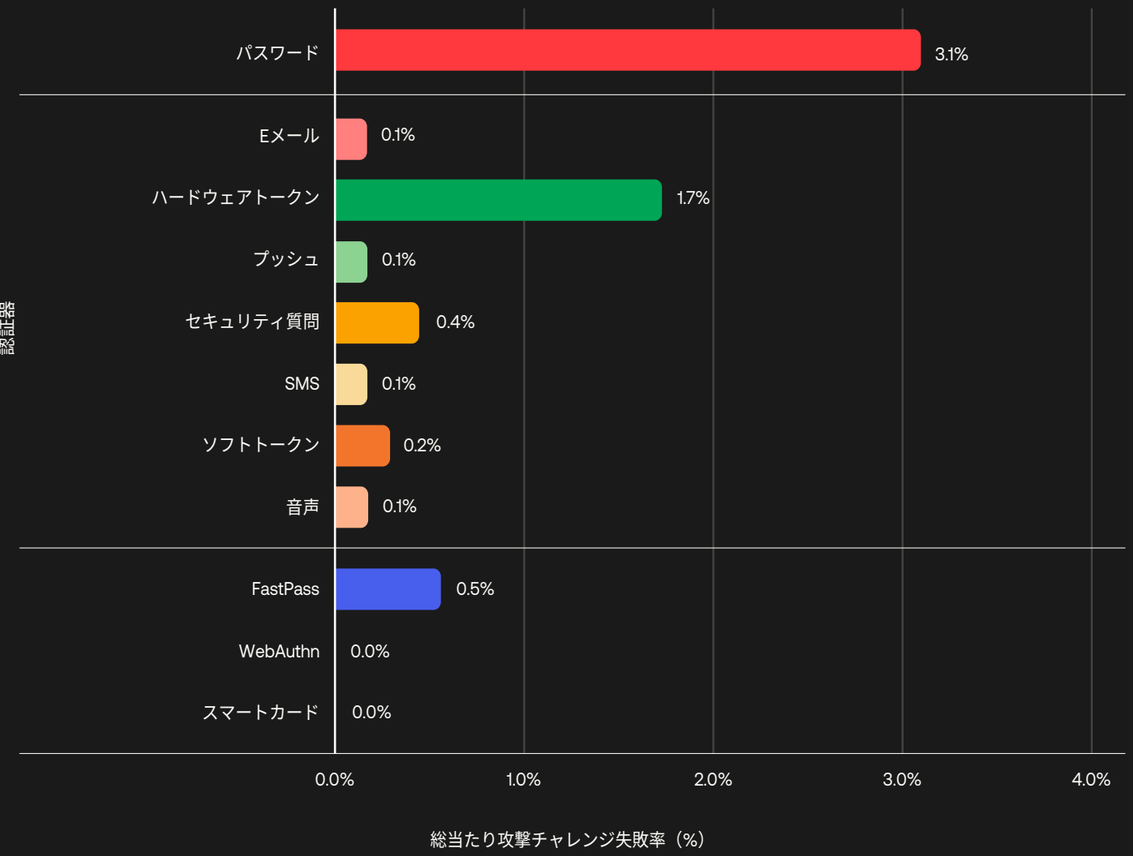


図12：パスワード、Eメール、ハードウェアトークン、プッシュ、セキュリティ質問、SMS、ソフトトークン、音声、FastPass、WebAuthn認証器の総当たり攻撃失敗率。2023年11月から2024年1月までの期間に収集されたデータを使用しています。

認証器のユーザビリティとセキュリティのプロパティ

認証器の測定基準に関する調査

昨年のレポートでは、認証器の測定基準の相対的な重要性を明らかにするため、測定基準を重み付けして評価しました。この重みは、認証器のプロパティに関して Okta が有する知識と、お客様にとっての重要度に基づいて算出しました。

2023 年のレポート公開後、さらに実用的な重みを使用して測定基準を評価する方法を検討し、Okta の IT/ セキュリティ実務者を対象に調査を実施して、認証器のユーザビリティとセキュリティのプロパティに関する測定基準の相対的な重要性を確認しました。この結果を基に、ログから収集したデータを、管理者から見た測定基準の重要性と連携させ、前回使用した推定値に代わって表 2 に示すデータを利用できるようになりました。

こうしたデータを組み合わせ、調査結果を基に認証器のユーザビリティとセキュリティのスコアを計算し、チャートに示すことができました。まず、各カテゴリの最大値と最小値を用いて、各認証器の測定基準を 0 から 1 の範囲に正規化しました。たとえば、Webauthn はチャレンジ失敗率のスコアは 1 になり、パスワードのスコアは 0 になります。次に、調査結果を基に、認証器のユーザビリティとセキュリティへの影響度に応じた重みを適用しました。この方法で、現実の状況や優先度を反映した認証器のユーザビリティとセキュリティのスコアのチャートを作成しました。次のページで、それぞれの認証器の評価をご確認ください。

重要ポイント

セキュリティインフラストラクチャを強化する上での重要な成功要因の一つは、セキュリティ /IT ステークホルダー間の全面的な連携とコミットメントを実現することです。測定基準の重み付けに関する調査は、認証方法を選択する際の重要なポイントやリスクについて、ステークホルダー間で合意を形成する効果的な手段となります

表 2：認証器のユーザビリティとセキュリティの評価カテゴリ

導入		ユーザビリティ		セキュリティ	
測定基準	重み	測定基準	重み	測定基準	重み
ユーザーレベルでの導入率	該当せず	チャレンジ時間	7.33/10	チャレンジ失敗率	5.71/10
		登録時間	5.14/10	総当たり攻撃チャレンジ失敗率	7.14/10
		チャレンジ失敗率	6.25/10	フィッシング耐性範囲	8.65/10
				フィッシング耐性アラート範囲	7.47/10
認証器の導入スコア		認証器のユーザビリティスコア		認証器のセキュリティスコア	

“強力な一意のパスワードを多数記憶することをユーザーに要求するのは、時代遅れなアプローチであり、成功することはありません。パスワードレス MFA の優れている点は、利便性とセキュリティ強化の両方を実現する非常に稀なオプションであることです。

セキュリティのメリットは、ビジネスを加速させ、成長の機会を広げる場合にのみ意味を持ちます。パスワードレスはこの条件を完全に満たします。パスワードを必要としない MFA 要素は、より迅速でシンプルなだけでなく、コストを削減し、統合パートナーシップの可能性を広げます。”

Shana Uhlmann 氏

IT ディレクター兼 CISO

Tattarang

認証器のユーザビリティとセキュリティのプロパティ

認証器のパフォーマンスと導入の評価

フィッシング耐性のある認証器は、優れたユーザーエクスペリエンスを提供する

ここまで見てきた観察結果を踏まえると、組織はどのように認証器を選択すべきでしょうか。また、セキュリティ /IT リーダーは、ユーザーフレンドリーで安全な認証器の導入を推進するために、どうすべきでしょうか。

情報セキュリティの分野では、テクノロジーの意思決定者にはセキュリティとユーザーエクスペリエンスの「トレードオフ」が必要となると思われがちです。

Okta の分析は、これが誤った選択であることを明らかにしています。この調査では、ユーザーの嗜好に関する測定は試みていないものの、認証の未処理データには、フィッシング耐性のある認証が卓越したユーザーエクスペリエンスを提供することが示唆されています。FastPass や FIDO2 WebAuthn を使うことで、ユーザーはエクスペリエンスの質を下げずにアカウントのセキュリティを向上させることができます。

重要ポイント

MFA やパスワードレスを大規模に導入することは、技術的な課題というよりも文化的な課題です。組織は選択肢と柔軟性を必要とします。Okta アイデンティティプラットフォームは、各組織固有のニーズに対応する幅広いオプションを提供するので、最適な方法論やフレームワークを選択して適用することが可能です。認証器のプロパティに基づく重み付けの定義や、これらの測定基準を主要ステークホルダーと調整するアプローチを生かして、強力な認証を促進する新しい方法をお客様が考えるきっかけとなれば幸いです。

認証器のパフォーマンスと導入率

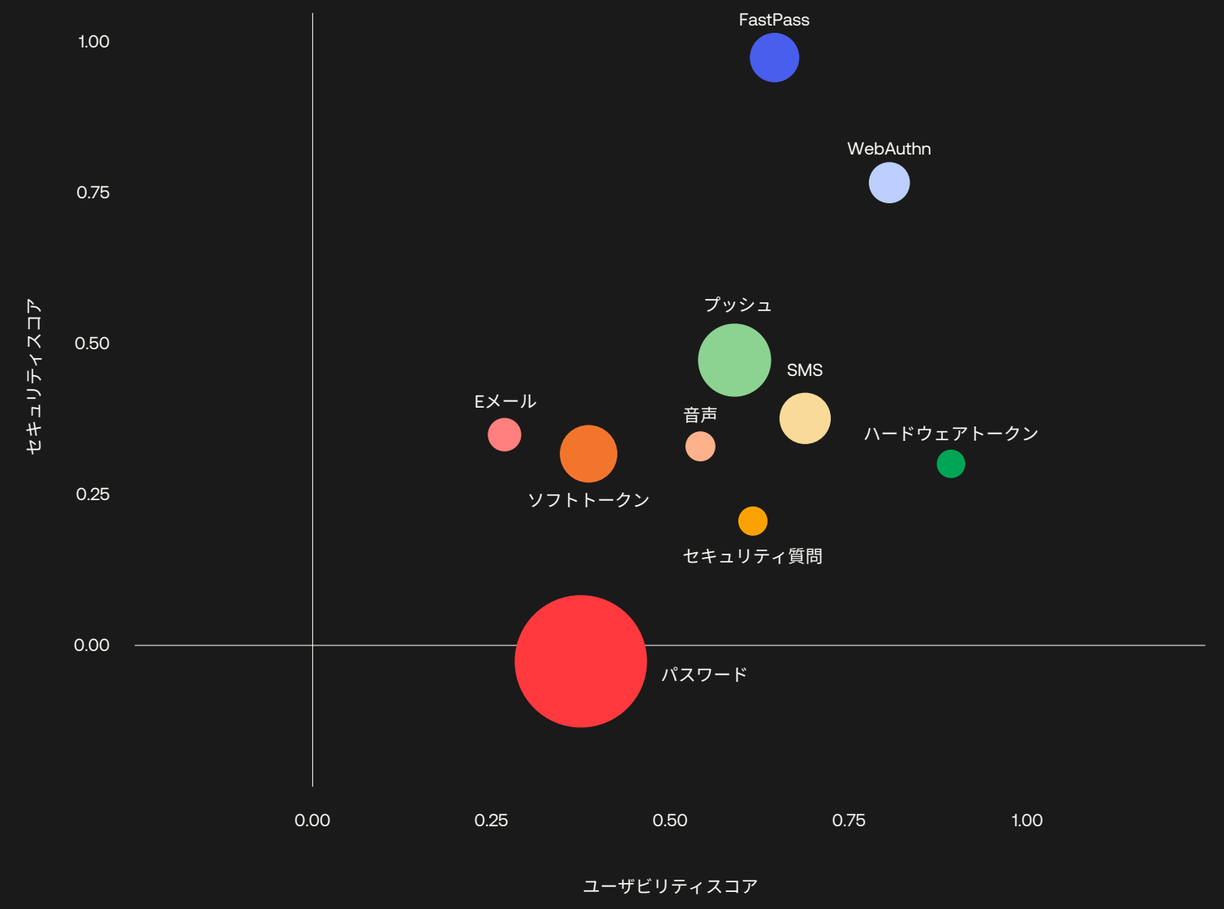


図13：パスワード、Eメール、ハードウェアトークン、プッシュ、セキュリティ質問、SMS、ソフトトークン、音声、FastPass、WebAuthn認証器のパフォーマンスと導入。各認証器のパフォーマンスは、2×2のマトリクスに示すように、ユーザビリティとセキュリティのスコアで表されます。円の大きさは、認証器の導入率（0%〜100%の尺度）を反映しています。

今後進むべき道

過去 12 か月間における攻撃者のフィッシングやソーシャルエンジニアリングの成功度を考えると、フィッシング耐性のある認証方法の導入がさらに進むことが予想されます。このデータが収集されて以降、数々の大規模なセキュリティ事件がこの問題を浮き彫りにしました。Salesforce、GitHub、Okta、Microsoft はそれぞれのユーザーベースの一部に対して、MFA のロールアウトを進めています。Okta のお客様の間でも FastPass の導入が加速しており、AI の進化によって生じた新たなフィッシングの脅威に対する懸念が広がっています。これらの動きがニュースや経営層の議論にも反映される中、Okta は前向きな展望を持っています。

フィッシング耐性のある MFA は、高い安全性と使いやすさを兼ね備えた実現可能な認証方法です。管理者にもユーザーにもメリットをもたらし、脅威の拡大に対抗するための最先端のテクノロジーであり、組織での導入を支援することが重要です。皆さまが強力で簡単な認証を目指す上で、他社との比較で自社の現状を把握し、経営陣やユーザーと議論を進めるために、本レポートが助けとなることを願っています。

皆様の組織の安全を確保し、優れたユーザーエクスペリエンスを実現するための個別のアドバイスについて、Okta にご連絡ください。

認証戦略を強化するための 5 つのヒント

より堅牢な認証戦略への移行は、気の遠くなるような取り組みに思えるかもしれません。しかし、比較的簡単なステップで開始できます。

1. サインオンポリシーに MFA を必須とし、機密性の高いアプリケーションやデータへの管理者のアクセスにはフィッシング耐性を適用します。特に、パスワードレス認証器の Okta FastPass が提供するフィッシング耐性機能やデバイス保証機能を活用することをお勧めします。
2. MFA の導入を C レベル幹部や取締役会レベルの優先課題とします。MFA は、組織の最も重要な資産や情報を保護するために不可欠であり、経営層が MFA の導入率を把握し、積極的に推進する必要があります。
3. アクセスに対して、ゼロトラストのアプローチを取ります。これにより、セッション単位かつ最小特権ベースで、アイデンティティのプロパティに従ってアクセスが付与され、要求されたアプリケーションやデータの保証要件に沿って判断されます。
4. 動的アクセスポリシーを策定します。これによって、ユーザーの属性、デバイスのコンテキスト（デバイスが既知であるか、管理されているか、態勢が強固か）、ネットワークの属性（ネットワークを信頼できるか）、要求に過去のユーザー行動との一貫性があるかを評価します。
5. パスワードの使用を最小限に抑えるか、または排除するための長期的な計画を策定します。

調査手法

本レポートの作成にあたっては、Okta Workforce Identity Cloud のデータを利用しました。世界各国からの毎月数十億件に上る認証 / 検証データを匿名化して集約しました。Okta のお客様とその従業員、請負業者、パートナー、顧客は、デバイス、Web サイト、アプリ、サービスのログインやデータの安全性確保のために Okta を使用しています。あらゆる主要業界で、小規模な組織から世界有数の組織まで、多様なお客様が Okta を活用しています。

組織規模の区分はフルタイム従業員数に基づき、業界分類は北米産業分類システム（NAICS）に準拠しています。組織規模、業界、地域情報の検証には、サードパーティのリソースを使用しています。

特に断りのない限り、本レポートは Okta Workforce Identity Cloud のデータとワークフォースのユースケースのみに焦点を当てています。Okta Customer Identity Cloud データは含まれません。

Okta について

Okta は世界のアイデンティティ企業です。独立系アイデンティティ管理の主要企業として、だれもが、どこでも、どんなデバイスやアプリでも、あらゆるテクノロジーを安全に使えるようにいたします。最も信頼されているブランドが Okta を信頼し、安全なアクセス、認証、及び自動化を実現しています。柔軟性と中立性を中核に備えた Okta Workforce Identity Cloud と Customer Identity Cloud により、ビジネスリーダーと開発者は、カスタマイズ可能なソリューションと 7,000 を超える事前構築済みの統合を活かすことができるため、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することができます。当社は、自分のアイデンティティが自分自身のものである世界を構築しています。詳しくは okta.com/jp/ をご覧ください。

免責事項

本書およびセキュリティ対策に関する推奨事項は、法律、セキュリティ、ビジネスに関する助言ではありません。本書は、一般的な情報提供のみを目的としており、最新のセキュリティや法律の動向、また関連するセキュリティや法律上の問題をすべて反映していないことがあります。本書の利用者は、自身の責任において、自身の弁護士またはその他の専門アドバイザーから法律、セキュリティ、またはビジネスに関する助言を得るものとし、本書に記載された推奨事項に依存すべきではありません。本書に記載された推奨事項を実施した結果生じるいかなる損失または損害に対しても、Okta は責任を負いません。

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871