ホワイトペーパー

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

目次

はじめに

テクノロジー史の専門家の視点で見ると、一般的なパスキー（特に同期パスキー）の登場は、フィッシング耐性のある Web 認証と大局的なパスワードレス化の流れにおける転換点として受け止めることができるかもしれません。

デバイスに紐づくパスキーは、ここ数年で利用できるようになっています。しかし、強力な認証セキュリティを促進する側面（特定のデバイスに縛られるという特性）が、主流の採用を阻む要因にもなっています。

これに対して、同期パスキーは以下の特長を持ちます。

- 複数のデバイス全体で同期する機能を持つ
- 多要素認証（MFA）をワンステップで実行可能にする

こうした特長によって利便性が高まり、同期パスキーの普及に大きく寄与すると期待されています。

大半のユーザーにとっても、パスキーはアカウントのセキュリティを大幅に向上させ、アカウント乗っ取り（ATO）攻撃を緩和するので、ユーザーとサービスプロバイダーに大きな損害が及ぶことを回避する上で役立ちます。

パスキーは、すべてのシナリオですべてのユーザーのニーズに対応できる完璧な認証ソリューションではありません。それでも、パスキーは実行可能で、フィッシング耐性があり、パスワードよりも優れた代替手段であると考える Okta は、開発者が認証フローにパスキーを簡単に導入できるよう取り組んでいます。

本書は、パスキーの採用を促進することを目的として、以下の内容を取り上げます。

- パスキーが提供するメリットを検証する
- パスキーの仕組みを解説する
- パスキーのさまざまな実装方法を紹介する

パスキーは、ブラウザが検出可能な 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格納されます。FIDO Alliance と World Wide Web Consortium（W3C）の標準に基づくパスキーは、暗号キーのペアを使用することでパスワードに置き換わるものとなります。

パスキーには 2 つの形式があります。

- 同期パスキー：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のように、クラウドサービスを介してユーザーのデバイス間で同期されます。
- デバイスに紐づくパスキー：単一のデバイスから離れることがありません。こうしたパスキーは、セキュリティレベル認証を達成したものを含め、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ます。

実際には、同期パスキーは、標準的なユーザーアカウントのパスワードと多要素認証（MFA）の組み合わせに取って代わるものであり、デバイスに紐づくパスキーは、さらに強力な保護と保証を提供できます。

FIDO Alliance と Okta

2012 年に設立され、2013 年に公に発足した FIDO Alliance は、「世界全体としてパスワードへの過度の依存を低減するために役立つ」認証標準の開発と促進を使命とするオープンな業界団体です。

こうした目的のため、同組織は以下の活動を行っています。

- ユーザー認証でのパスワードへの依存を軽減する、オープンで拡張性が高く相互運用可能な一連のメカニズムを定義する技術仕様を策定する
- この仕様を全世界に普及させるため、業界認証プログラムを運営する
- 正式な標準化のため、成熟した技術仕様を公認の標準化団体に提出する

Okta は、FIDO Alliance のスポンサーメンバーです（全メンバーの一覧はこちら）。

「パスキー」の歴史と関連用語
パスキーには聞きなれない用語が多く、またパスキーの進化についてもあまり知られていません。ここでは、歴史的な背景を説明します。

2018 年 4 月、W3C Web 認証標準が勧告候補となり、FIDO2 が正式に発足しました。FIDO Alliance によって開発された FIDO2 は、Web Authentication JavaScript API 標準（一般に「WebAuthn」と呼ばれます）と、これに対応する FIDO の Client To Authenticator Protocol（CTAP）を規定しています。

JavaScript API を使用することで、開発者はハードウェアキー（「ローミングオーセンティケーター」）またはデバイス上のセキュアハードウェア（「プラットフォームオーセンティケーター」）のいずれかを活用できます。後者は、パスワードレスでユーザーを認証するため、多くの場合にバイオメトリックセンサーによりゲート制御されます。

この一連の仕様は、公開鍵と秘密鍵が存在する場所の詳細を抽象化することで、最新のデバイスでフィッシング耐性のある認証機能の普及に貢献しました。

2022 年 5 月、テクノロジー大手の Apple、Google、Microsoft が、新しい同期ファブリックにプラットフォームオーセンティケーターをバックアップする機能を追加することによって、FIDO2 を拡張する計画を発表しました。この機能拡張セットは、Web サイトやアプリがパスワードの代わりに FIDO 資格情報を採用しやすくすることを目的とします。

プレスリリースには「パスキー」の一例が含まれていましたが、当時は以下のような状況にありました。

- 「パスキー」は、マルチデバイス対応 FIDO 資格情報のみを指す用語だった
- 名称としては、「マルチデバイス対応 FIDO 資格情報」が好まれて使用された

その後、「パスキー」は検出可能な FIDO 資格情報全般を指すようになりました。

しかし、広く採用され、主要プラットフォームがパスキーを受け入れるようになったことで、FIDO Alliance も「パスキー」という用語を使用するようになりました。この用語は現在、同期パスキーとデバイスに紐づくパスキーの両方を包含するようになっています。「マルチデバイス対応資格情報」という用語は、その後に非推奨となりました。

パスキーの重要性とは？

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の脅威との戦いにおいては、パスキーが一般ユーザーに普及することが大きな一歩となると考えられます。

これまでの常識では、より安全な認証はユーザーエクスペリエンスを犠牲にすると考えられてきました。しかし、パスキーは、認証フローを簡素化・高速化することで、ユーザーエクスペリエンスを向上させると同時にセキュリティを強化する可能性を秘めています。

パスキーはパスワード（そして従来の MFA 手法）よりも安全である

ユーザー認証の問題に対する解決策として、パスワードが不十分であることは周知の事実です。実際、パスワードやパスワード管理はもはや冗談として語られるようになったと言っても過言ではないでしょう。たとえば、Web コミックの「xkcd」は、この題材を 3 回以上取り上げています（Password Reuse、Password Strength、Encryptic）。

最初は人間が入力する単純なログインボックスだったものが、年月とともに劇的に変化しました。

- 攻撃者が脆弱なパスワードを推測する練度を高め、パスワードの使い回しが広く行われている状況に付け込むようになりました。これに伴い、複雑さに関する要件が進化し、特殊文字、大文字と小文字の組み合わせ、数字を含む、ますます長いパスワードが使われるようになりました。
- そのために、ユーザーはパスワードの増加や複雑化に取り組まざるを得なくなり、パスワードマネージャーの採用（ブラウザでの実装、個別のアプリケーションでの実装）が促進されました。
- フィッシングの脅威拡大や、膨大なパスワードがオンライン上に流出した状況を受け、ATO 攻撃に対する効果的な防御策として MFA が脚光を浴びるようになりました。
- 現在では、この重要な障壁を迂回するための、拡張性が高く経済的な方法を攻撃者が見出すようになっていることから、従来の多くの MFA 手法は有効性が脅かされています。
- こうした動きの舞台裏では、ワークフォースアイデンティティやカスタマーアイデンティティのシステムがセキュリティレイヤーを追加しています。自動化された多種多様なサイバー攻撃が企業のコストを増大させるとともに顧客のプライバシーを脅かしている中、アイデンティティが防御を提供しています。

こうした変更の多くによって、サービスへの登録やアカウントへのログインといった日常的な行動で摩擦が増大し、ユーザーエクスペリエンスが低下しました。

幸いなことに、パスキーは、パスワードに代わってフィッシング耐性のある手段を提供し、暗黙的に第二の認証要素も提供します。

パスワードをめぐる問題

Okta の「Customer Identity Trends レポート 2023」は、世界 14 か国のコンシューマー 21,512 人を対象として実施した調査に基づき、次の状況を明らかにしました。

- 回答者の 65% が、多数のユーザー名 / パスワードを管理しなければならないことに負担を感じている
- 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

パスキーにはフィッシング耐性がある

B2C ブランドがパスワードを FIDO 標準に置き換えることで、パスワードスプレーやパスワードスタッフィングのような自動化されたクロスサイトパスワード攻撃を Web サイトが受けても、攻撃が不成功に終わり、組織は影響を受けません。加えて、FIDO が公開鍵暗号方式を採用していることから、組織が保存するのは、攻撃者にとってほとんど価値のないユーザーの公開鍵だけになります。ユーザーの秘密鍵は、ローカルのデバイスに安全に保存されます。ユーザーが信頼するデバイス内に留まり、オペレーティングシステムのエコシステム内または信頼できるサードパーティサービスを通じてシームレスな同期を可能にします。パスキーの同期はエンドツーエンドで暗号化され、プロセス全体を通して機密情報を保護します。

こうしたレジリエンスは、企業のリスクとエクスポージャーを軽減するだけでなく、ユーザーにもメリットをもたらします。アカウントが乗っ取られると、ちょっとした不便が生じるだけの場合もあれば、プライバシー侵害、さらには個人情報の窃取が起こる場合もあります。パスキーの使用を選択することで、こうした事態に至る可能性が格段に低くなります。

パスキーは暗黙的に強力な MFA を提供できる

多要素認証（MFA）は、以下のような認証要素を 2 つ以上必要とします。

- 知識要素：パスワード、PIN、セキュリティの質問など、ユーザーが知っているもの
- 所有要素：登録されたデバイスなど、ユーザーが持っているもの
- 内在要素：指紋など、ユーザー自身の属性となるもの

パスキーはユーザーのデバイスに保管され（所有要素）、必要な検証は、バイオメトリクスやセキュリティコードなどの FIDO が承認した手法（内在要素または知識要素）を介してのみユーザーが行使できます。そのため、MFA の中核的な原則を暗黙的に満たします。

パスキーが提供する MFA は、とりわけ強度が高く、現在も一般的なマジックリンクやワンタイムパスコード（OTP）が提供する保護からの大きな進歩となります。

多くの顧客対応組織にとって、セキュリティ上のメリットだけでもパスキーのサポートを導入する正当性は十分にあります。しかし、話はここで終わりません。

中程度の保証のユースケース用パスキー

すべてのパスキーは、いくつかの共通のセキュリティ特性を持ち、高度なフィッシング耐性のある一意のキーペアを使用して強力な認証を可能にします。しかし、同期パスキーとデバイスに紐づくパスキーには重要な違いがあり、ユースケースの保証レベルの違いによって適性が異なります。

特に米国国立標準技術研究所（NIST）のオーセンティケーター保証レベル（AAL）との関連において、組織が十分な情報に基づいた意思決定を行えるよう、FIDO Alliance は 2023 年 6 月、中程度の保証のユースケースに向けた FIDO 認証を発表しました。

この文書は、中程度の保証環境（「AAL1、AAL2、AAL3 の保証レベルを組み合わせて対応可能な、複数の異なる認証ユースケースシナリオを持つ組織」と定義されます）において、両方の資格情報タイプをどのように利用できるかを判断するため、デバイスに紐づくパスキーと同期パスキーの両方の能力と特性を分析する際の指針を示しています。

備考：現在、NIST では同期パスキーの保証レベルを更新する作業が行われています。このため、最新情報については、NIST および FIDO Alliance の最新のリソースを参照してください。

パスキーはパスワード以上に便利である

煩雑な認証プロセスの代わりに、指のスワイプ、顔のスキャン、PIN の入力など、デバイスのロック解除で使い慣れたアクションを使用することで、同期パスキーは、ユーザーがオンラインサービスを利用する際に経験する摩擦を劇的に低減します。

Shopify、DocuSign、PayPal など、パスキーをいち早く採用した企業は、安全で便利なユーザーエクスペリエンスを提供しています。

実際、多くのサービスプロバイダーにとって、ユーザーの利便性の向上が、同期パスキーの最も魅力的な特性となっている可能性があります。デバイスに紐づくパスキーの場合、ユーザーは Web サイトやアプリごとに各デバイスを登録する必要があります。これに対して、同期パスキーを使用する場合、ユーザーには以下のメリットがあります。

- （新しいデバイスも含め）複数のデバイスで、サインインのための FIDO 資格情報に自動的にアクセスできる
- すべてのデバイスを紛失した場合でも、パスキーを復元できる

コンシューマー向けのビジネスにとって、摩擦（自社サービスとユーザーのインタラクションを遅らせるすべての要因）は、コンバージョン、ひいては収益の大きな障害となります。Okta の「Customer Identity Trends レポート 2023」によると、調査参加者の 60% 近くが、シンプルで安全、かつ摩擦のないログインエクスペリエンスを得られる場合に、サービスにお金を使う可能性が高くなると回答しています。このデータは、すべてのセクター / 業種で一貫しており、ユーザーがあらゆるインタラクションで利便性を望んでいることを示唆しています。

また、地域差もありますが、最も大きな差が見られるのが世代間の違いです。若いコンシューマーは、年配のコンシューマーに比べて、シンプルで安全、かつ摩擦のないログインエクスペリエンスを得られる場合に、より多くのお金を使う可能性が 3 割程度高くなっています（図 1）。

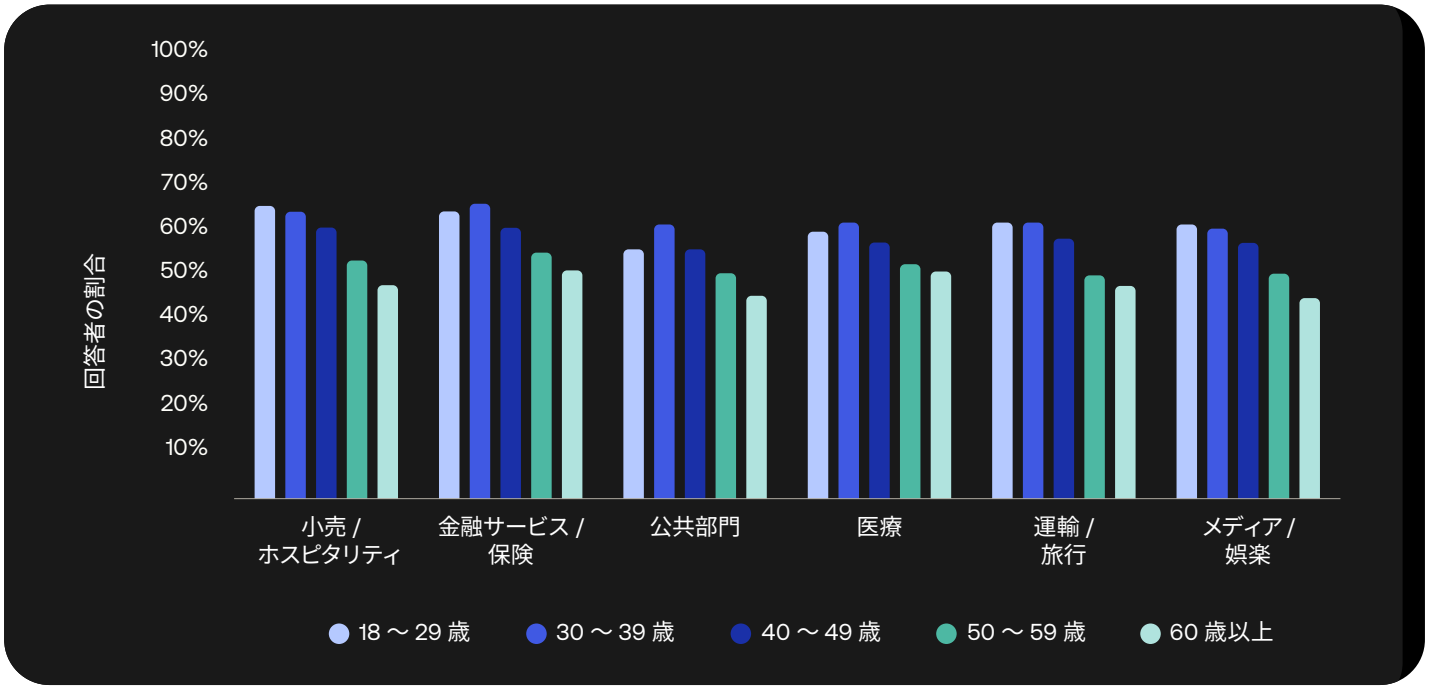


図 1：ブランドとのオンラインのインタラクションにおいて、シンプルで安全、かつ摩擦のないログインエクスペリエンスを得られる場合に、お金を使う可能性が高くなると思いますか？（グラフは、「可能性が非常に高い」と「可能性がやや高い」の回答の合計）

もちろん、信頼を確立し、セキュリティコントロールを提供するためには、ある程度の摩擦は避けられません。しかし、あらゆるコンシューマーとのインタラクションにおいて、実際に有効なあらゆる部分で摩擦を減らすことで、コンバージョン率を高め、それに応じて短期的にも長期的にも収益を伸ばすことができます。

次に、パスキーによってパスワードよりも摩擦を低減する方法をいくつか見ていきましょう。

同期パスキーの利用はパスワードよりも速い

調査によると、同期パスキーはパスワード以上に使いやすいだけでなく、圧倒的に速く使用できます。Google のセキュリティブログによると、パスキーを使ったログインにかかる時間は平均 14.9 秒で、パスワードを使った場合（30 秒）の 2 倍に高速化していることがわかります。

同ブログには、「ユーザー調査で収集された予備的な定性データも、ユーザーがすでにこの利便性をパスキーの重要な価値として認識していることを示唆している」とも述べられています。

パスキーのアクセシビリティはパスワード以上に優れている

摩擦は、多くのコンシューマーにとって不都合なものですが、一部のコンシューマーがサービスにまったくアクセスできなくなる可能性も生み出します。

視覚障害や認知障害、運動機能の制限などの障がいを持つ人が、長く複雑なパスワードを記憶し入力する（または、検索してコピーし、貼り付けるといった「些細」と思われるような動作を行う）ことをユーザーに求める煩雑な認証フローを実行することを想像してみましょう。あるいは、テクノロジーを気軽に使用できない人や不慣れな人が、オーセンティケーターアプリのダウンロードを求めるメッセージにどう反応するか考えてみましょう。

パスキーは、こうした従来のアプローチに代わる、アクセシビリティがより高い選択肢を提供します。

カスタマージャーニー全体でアクセシビリティを意図的に設計することは、金銭的なインセンティブも生みます。使う人を選ばないエクスペリエンスを創出するブランドは、市場へのリーチを最大化できます。

同期パスキーは強力な認証をより便利にする

同期パスキーは、強化したセキュリティをより便利にします。ユーザーから見ると、ユーザーのアイデンティティと秘密鍵の両方を1つのステップで検証するため、他の MFA 手法に比べて大幅な改善をもたらします。

こうした利便性の向上により、サービスプロバイダーは、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る、より高い頻度またはステップアップの再認証を検討できるようになります。たとえば、機密性の高いアプリへのアクセス、アカウント設定の変更、個人データへのアクセスなどで活用できます。Okta の **2023 年版「セキュアサインインのトレンドレポート」**でも述べているように、WebAuthn を使用したオーセンティケーターチャレンジは、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に比べて数倍速く、平均してわずか 3 秒で完了します。

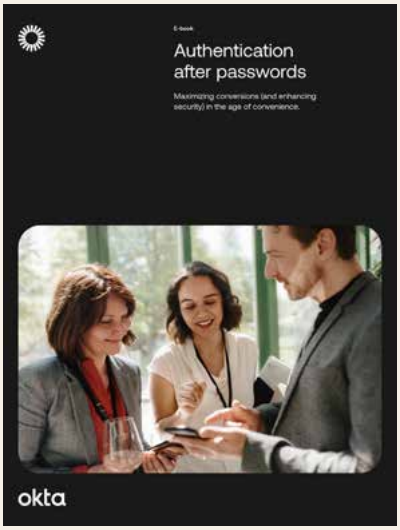
同期パスキーはパスワードよりも簡単に登録できる

もちろん、こういった便利な機能はすべて、ユーザーが同期パスキーを登録した後でなければ利用できません。したがって、登録が簡単であることが求められます。デバイスに紐づくパスキーの場合、登録を繰り返す必要がある点が、特にコンシューマー向けシナリオで WebAuthn がこれほど限定的な採用にとどまっている主な理由として一般的に挙げられています。

同期パスキーは、複数のデバイス全体でユーザーの FIDO 資格情報が簡単に（同時に安全に）移動できるので、登録自体が単純化され、1つのサービスで一度しか発生せず、こうした問題を克服しています。

実際、「セキュアサインインのトレンドレポート」によると、パスワードの登録にかかる時間の中央値は約 34 秒です（ユーザーが新しいパスワードを作成し、パスワードを再入力して確認する時間も含みます）。対照的に、WebAuthn ベースの登録に要する時間はわずか 19 秒であり、「高保証のオーセンティケーターは登録時のユーザーの負担が大きい」という見解の正当性を覆すデータとなっています。

現実的には、当初は同期パスキーに不慣れなユーザーも、少なくとも他の認証メカニズムと同じ程度に直感的に登録でき、しかも各段に高速化できることをすぐに理解するでしょう。



同期パスキーは、パスワードレスへの移行における重要な一歩となる

同期パスキーは、パスワードを使用する場合に比べて、アカウントセキュリティを強化すると同時に、ユーザーエクスペリエンスの利便性を向上します。これにより、セキュリティを優先する IT 管理者や、さまざまな利点を認識するアーリーアダプターにとどまることなく、パスワードレス認証を普及させるチャンスとなると合理的に考えられます。

Okta の包括的なガイド、**Authentication After Passwords** をダウンロードして、パスワードレスの未来について詳しく学び、競争優位性を実現（そして維持）するため、今何ができるかをご確認ください。たとえば、パスワードレスのフローをまだ導入していないと勘違いしている組織が多いなど、よくある誤解を含めて理解できます。

Okta 独自のパスワードレスのジャーニーについては、**Okta が 100% パスワードレスを目指す理由**をご覧ください。

パスキーの仕組みとは？

FIDO Alliance の説明によると、基盤となる FIDO プロトコルは、強力な認証を提供するために標準的な公開鍵暗号手法を採用しています。ユーザーのデバイスは、オンラインサービスに登録するために、以下の要素で構成される新しい暗号鍵ペアを作成します。

- 公開鍵：オンラインサービスに登録される
- 秘密鍵：真のシークレットとしてデバイスに保持される

重要となるのは、鍵がアカウントごとに安全かつ一意に生成される点です。「ユーザーが強度の低い秘密鍵を選ぶのではないか」と懸念する必要がなくなり、秘密鍵が複数のサービスで使い回されることもありません。

特定のサービスで認証するために、クライアントデバイスは、サービスが提供するチャレンジに署名することで、アカウントが対応する秘密鍵を所有していることを証明します。サービス自体は秘密鍵を認識しないため、この情報を保管 / 保護する必要もありません。

特に重要な役割を果たすのが、秘密鍵はユーザーによってロック解除された後でなければ使用できないという仕組みです。通常、ローカルのロック解除は、第二要素デバイスの挿入、プライマリデバイスのロック解除メカニズム（多くの場合、Touch ID、Face ID、Windows Hello などの生体認証）、または PIN を介して行われます。

同期パスキーは、以下の点において以前の FIDO2 の実装と異なっています。

- ユーザーは、パスキーがデバイスとクラウドにバックアップされる特定のエコシステムで、どのデバイスでも同期パスキーを使用できる
- ユーザーは、クロスデバイス認証によりエコシステムの境界を容易に超えることができ、新しいデバイスに FIDO 資格情報を登録する摩擦が発生しない

パスキーの基本的な仕組みについての詳細は、FIDO Alliance の Web サイトをご覧ください。

パスキーを アプリに 実装するには？

大まかに言って、パスキーをサポートするために開発者が認証を拡張するアプローチは 2 つあります。

- 社内で API や SDK を使ってパスキーを実装する
- アイデンティティサービスプロバイダーを利用する

パスキーの導入に関する詳細情報

FIDO Alliance は、IT 管理者、企業セキュリティアーキテクト、組織全体で FIDO 認証の導入を検討している経営幹部向けに、一連のホワイトペーパーを発行しています。

DIY のアプローチ

実装の観点からは、同期パスキーは、認証ステートメントを提供しないプラットフォームオーセンティケーターと同じようなものとして認識されます。つまり、プロトコルの観点からは、Web アプリがすでに WebAuthn をサポートしており、認証応答を必要としない限り、技術的にはすでに同期パスキーをサポートしていることになります。しかし、ユーザーエクスペリエンスの観点からは、それが必ずしも真実ではない可能性があります。

- 現在の登録ページで表示されるプロンプトや文言は、デバイスに紐づく資格情報（「このデバイスからより速くサインインする」など）を参照している可能性が高く、同期パスキーについては完全に合致しなくなっています。
- 同期パスキーを使用する以前の組織は、アカウントの回復を直接担う必要がありました。このため、プラットフォームオーセンティケーターを使って第二認証要素のみを有効にしている可能性が高いと考えられます。

特に WebAuthn をすでに導入している場合、上記の変更はどれも特に難しいものではありません。しかし、エクスペリエンスを向上するためには、依然として多少の作業を行う必要があります s。

2022 年 10 月 に W3C WebAuthn Community Adoption Group と FIDO Alliance が開発者支援のために立ち上げた passkeys.dev は、ドキュメントの提供やデバイスサポートの追跡などのオンラインリソースです。

Identity Unlocked

Andrew Shikiar 氏と Tim Cappalli 氏がパスキーについて語る

Identity Unlocked は、Auth0 のプリンシパルアーキテクト、Vittorio Bertocci がホストするポッドキャストです。同期パスキーが（マルチデバイス対応資格情報として）発表された直後、FIDO Alliance のエグゼクティブディレクター兼 CMO の Andrew Shikiar 氏と、Microsoft のデジタルアイデンティティ標準アーキテクトの Tim Cappalli 氏が同ポッドキャストに出演しました。

FIDO 資格情報の進化について知り、マルチデバイス対応資格情報の仕組みについて、開発に焦点を充てた知見を得るため、ぜひ**ご視聴ください**。

アイデンティティサービスプロバイダーを利用する

アイデンティティの構築は難しく、経験豊富なプロフェッショナルにとっても、効果的かつ効率的な実装は課題の多い作業です。加えて、顧客の期待は高まり続け、誰もが自身が経験した最善のエクスペリエンスと比較して、それぞれのエクスペリエンスを評価するようになっています。このため、企業は提供する UX を常に進化させなければならないという大きなプレッシャーにさらされています。

その一方で、コアコンピテンシーの拡張に必要な貴重なエンジニアリングリソースを大量に消費せずに、アイデンティティのニーズに対応する必要があります。これらの目標はいずれも、規制要件を見過ごしたり、セキュリティで妥協したりすることなく満たさなければなりません。

これらの理由から、多くの組織は、アイデンティティサービスをアプリケーションとテクノロジースタックに統合する方が効率的であり、費用対効果も高いと判断しています。さらに、アイデンティティサービスプロバイダーと提携することで、企業は以下のような CIAM（カスタマーアイデンティティおよびアクセス管理）の幅広い要件に対応できるようになります。

- 認証
- 認可
- ユーザー管理

確立されたアイデンティティプロバイダーが今後パスキーをサポートすることは確かであり、アプリケーション開発者が認証オプションを拡張し、急速に進化する認証環境に対応するための便利なオプションを提供します。

たとえば、認証に Okta Customer Identity Cloud を使用するようにアプリがすでに構成されている場合は、コードを一切変更せずに、スイッチのオン / オフのようにパスキー認証を有効にすることができます。

ただし、提供される機能はアイデンティティプロバイダーによって異なるため、十分な注意を払う必要があります。ソリューション候補を選ぶ際には、注目すべきポイントがいくつかあります。

- 独立性と中立性：組織を制約するのではなく、支援する CIAM ソリューションを選ばなければなりません。つまり、既存のソリューションと統合し、オープン標準を活用してベンダーロックインを回避し、どのクラウドプロバイダーとも連携できる必要があります。
- 包括的かつカスタマイズ可能：顧客はそれぞれに独自であり、複雑なニーズを持ちます。CIAM ソリューションは、シームレスで一貫性と信頼性の高いエクスペリエンスを、あらゆるタイプのユーザーのために構築する支援を提供しなければなりません。
- 構築、保守、使用が容易：エンジニアリングチームは、どのようなテクノロジーについても、展開、構成、運用にかかる労力と時間を削減することを目指しており、CIAM ソリューションもこの使命をサポートする必要があります。
- 信頼性：深刻なセキュリティ侵害、コンプライアンス要件の不履行、サービスの可用性低下、サービスの劣化によって、ブランド / 法律 / 財務の側面に重大な影響が及ぶ可能性があります。CIAM ソリューションは、このようなリスクを軽減するものでなければなりません。

今後の展望は？

WebAuthn が登場したとき、Auth0（現在の Okta Customer Identity Cloud）はすぐにその価値を見出し、管理者が管理ダッシュボードにアクセスする際の第二要素の 1 つとして、また開発者が Web アプリを保護する際にユーザーを認証する手法の 1 つとして採用しました。

しかし、セキュリティ上のメリットが明確であるにもかかわらず、コンシューマー向けアプリでの FIDO2 認証の採用は、今のところ低い水準にとどまっています。Okta の観察では、専門家が管理対象リソースへのアクセスで、高いレベルの保証を必要とするために利用しているケースが大半を占めることが示されています。

多くの説明が考えられますが、一致した見解として以下の点が挙げられます。

- ハードウェアキーは、一般コンシューマー向けというよりは、おおむね管理者や主要ナレッジワーカー向けとなっている
- プラットフォームオーセンティケーターの方が受け入れやすいが、単一のデバイスに縛られるという特性（ビジネスシナリオでは潜在的に要望される）が、ユーザーが多数のデバイスを使用し、新しいデバイスを頻繁に追加しているコンシューマー領域では、ユーザビリティの課題を引き起こす

しかし、同期パスキーの登場、そして Apple、Google、Microsoft などが及ぼす大きな影響は、重要な転機を生み出す可能性があります。パスキーを歓迎するユーザーもいれば、躊躇するユーザーもいるでしょう。しかし、パスキーは今後、どこにでもある身近な存在になっていきます。

より広い観点では、パスワードレス認証は全体として、肯定的なユーザーエクスペリエンスとセキュリティ上のメリットによって採用が増え、普及していくと予想されます。パスキーや他のパスワードレス認証メカニズムを顧客や他のユーザーに提供する組織は、その報酬を得るようになります。

ただし、以下のような未解決の問題が残っていることも確かです。

- パスキーにはフィッシング耐性がありますが、新規ユーザーのオンボーディングで、パスキーとその回復方法（オペレーティングシステムのエコシステムに関連するメールアカウントなど）の両方を使用することには、潜在的な脆弱性があります。
- これまでのところ、ユーザーエクスペリエンスは、プラットフォームのエコシステムやパスワードマネージャーによって異なります。FIDO Alliance は一貫性の創出に取り組んでいますが、（少なくとも短期的には）一貫性のないエクスペリエンスが解消されず、一部のユーザーの不満を生じさせる要因になる可能性があります。
- 前述したように、NIST AAL フレームワーク内での同期パスキーの位置づけは未解決の問題です。これは、多くの業務ユーザーが個人所有のデバイスを使って組織の保護されたリソースにアクセスしている時代に、さまざまな影響を及ぼす可能性があります。
- 最後に、新しいテクノロジーが常に直面する課題として、特にセキュリティ、プライバシー、利便性の側面に関して、パスキーに関するコンシューマー教育が挙げられます。

そして、パスキーは非常に新しいものであり、さまざまな実装が登場しては改良されるという流れの中で、この領域が全体として進化していくという点に改めて留意すべきでしょう。

「優秀」なソリューションがあれば、「完璧」を待つ必要はない

パスワードの使用が引き起こしている問題に比べると、パスキーをめぐる問題は些細なものであると言ってもよいでしょう。パスワードは、消滅するか、少なくとも利用が大きく縮小する必要があります。アイデンティティ業界の誰もが、パスキーのデメリットを最小限に抑えながら、メリットを生かす道を見出す取り組みに焦点を充てるべきです。

Okta も、業界の一員としての役割を果たすことを約束します。そのために、パスキーを可能にするタイムリーで最先端、かつ「開発者フレンドリー」な機能を提供し、このテクノロジーの未来を形作る業界の議論に積極的に参加しています。

プラットフォームベンダーとデバイスメーカーが、回復、発行、拡散防止のための標準化されたフローで足並みをそろえることができれば、パスワードレスの導入はより容易になるでしょう。パスワードレス認証の導入や拡張を検討している組織には、以下の機能を提供するオーセンティケーターを探すことをお勧めします。

- 摩擦のない認証を実現する
- サインイン時のエラーを減らす
- ユーザー登録を簡単にする
- フィッシング耐性がある

何はともあれ、これらの条件をすべて満たすのがパスキーです。

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、どのようなテクノロジーでも安全に利用できるよう支援しています。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。