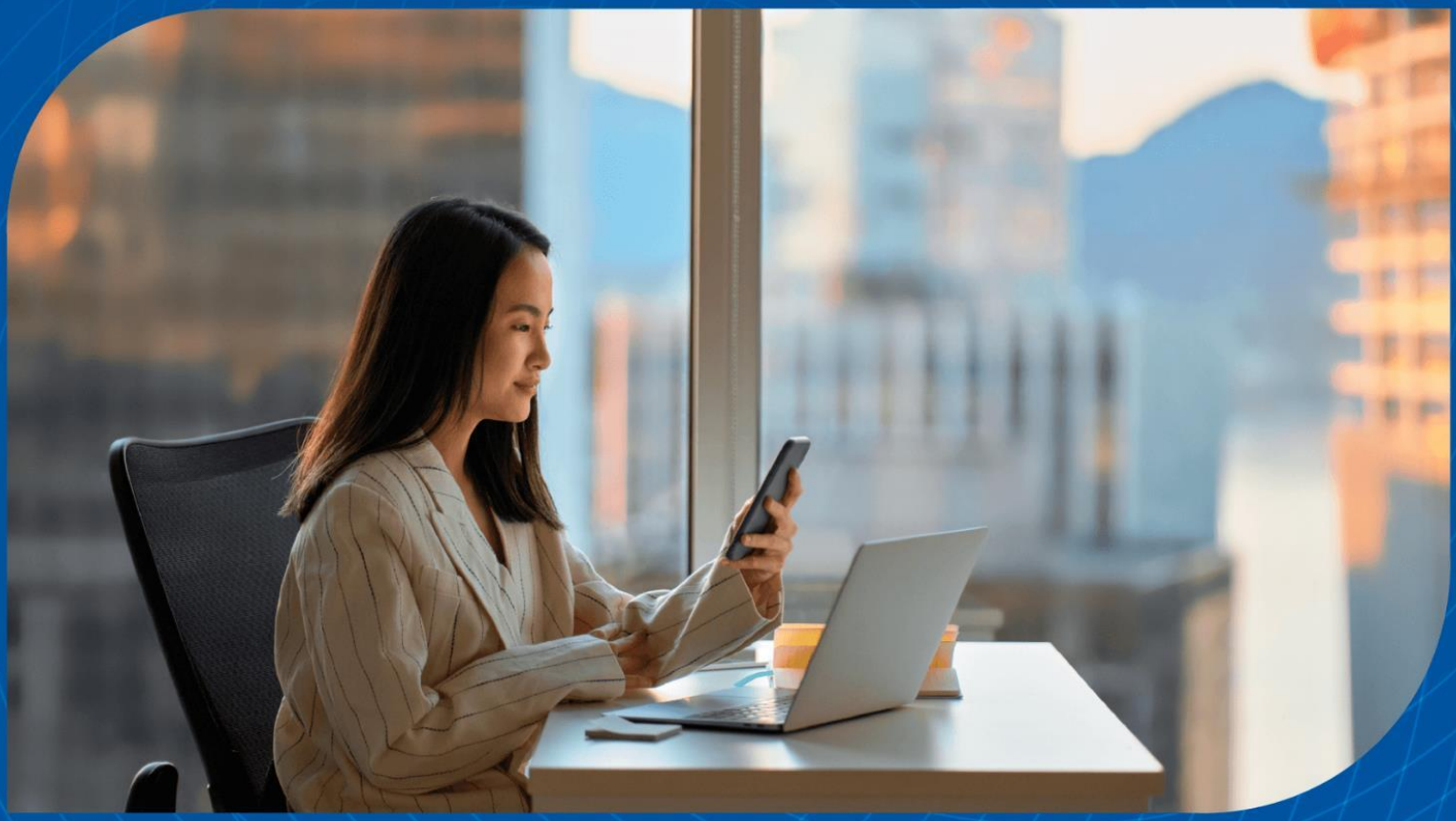
パスワードのその先へ

現在のWeb セキュリティにおける パスキー（Passkeys）の役割



cloud security alliance®

謝辞

Lead Author

Kurt Seifried

Contributors

Andrew Klaus
Mark Loveless
Guillaume Rossolini
Michael Roza

Special Thanks

Rolf Lindemann

CSA Staff

Josh Buker
Claire Lehnart
Stephen Lumpe
Kurt Seifried

日本語版提供に際しての告知及び注意事項

本書「パスワードのその先へ 現在の Web セキュリティにおけるパスキー(Passkeys)の役割」は、Cloud Security Alliance (CSA)が公開している「Beyond Passwords: The Role of Passkeys in Modern Web Security」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2024年2月28日	日本語版1.0	初版発行

CSA ジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSA ジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1. 責任の限定

CSA ジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2. 二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。

(2)　本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。

(3)　CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。

(4)　転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3.　本書の適切な管理

(1)　本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

(2)　本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。

(3)　本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4)　本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4.　原典がある場合の制限事項等

本書が Cloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5.　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSA ジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「SaaS セキュリティに関する年次調査報告書」は、CSA ジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

翻訳者
宮川　晃一

レビュアー
高橋　久緒
満田　淳
諸角　昌宏

目次

本書における主な注目点

- パスキー（Passkeys）はセキュリティを大幅に向上させ、セキュリティとユーザビリティのトレードオフはあるものの、新しい攻撃を発生させることはありません。 また、既存の多くの攻撃手法は通用しません（例：ブルートフォース攻撃やクレデンシャルスタッフィング攻撃）。
- パスキーは、人々にパスワードマネージャーを使用させるというハードルを回避させ、パスキーを保護するための生体認証を広く普及させる可能性があります。
- パスキー認証がサポートされればアカウント共有が難しくなる可能性があり、これには多くのサービスベンダーが賛成しています。パスキーは、デバイスの同期をサポートすることで、規模に応じた展開が容易でより信頼性が高いものです。パスキーは、パスワードと比較してアカウントリカバリーの必要性を減らし、サポートコストを削減するはずです。
- ソフトウェアトークンとセキュアなハードウェアトークンの両方でパスキークライアントをサポートしており、ほとんどのプラットフォーム、ブラウザ、多くのサードパーティ製のパスワードマネージャーで利用可能です。
- パスキーは主要ベンダーがサポートしています（例えば、2023 年 10 月 10 日現在、Gmail ユーザーと Google Workspace 管理者のための Passwordless by default: Make the switch to passkeys）
  https://blog.google/technology/safety-security/passkeys-default-google-accounts/

はじめに

Web 認証方式は、セキュリティとユーザーエクスペリエンスを向上させるために、長年にわたって大きく進化してきました。インターネットの黎明期には、ユーザー名とパスワードが主な認証手段でした。しかし、サイバー脅威がより巧妙になり、被害者に対して攻撃する効果的な手段となったため、より安全な方法の必要性が明らかになりました。このため、二要素認証（2FA）が開発されました。2FA は、ユーザーに 2 種類の本人確認を求めることで、セキュリティのレイヤーを追加するものです。セキュリティが強化されたとはいえ、2FA には、毎回 2 つの本人確認を提示しなければならない不便さなどの限界もありました。そのため、より安全でユーザーフレンドリーな認証方法として、パスキーの登場への道が開かれました。

パスキーは、Web 認証方式における大きな飛躍を意味します。従来のパスワードとは異なり、パスキーはユーザーのデバイス上で生成・保存される暗号鍵です。秘密鍵がユーザーのデバイスから公開されることがないため、攻撃者が不正にアクセスすることが非常に難しく、より安全な認証方式を提供します。さらに、パスキーは、複雑なパスワードを覚える必要がないため、ユーザーのエクスペリエンスを向上させます。

パスキー の台頭は、WebAuthn API 標準の開発によって促進されました。WebAuthn API 標準は、アプリケーションコードとパスキーのサポートを橋渡しするメカニズムを提供します。さまざまな API やサービスがこの標準を実装しており、開発者はフロントエンドで新しい パスキー を生成し、それをサーバーに送信して保存し、将来的に認証を行うことが可能になります。主要なブラウザが WebAuthn 標準を広く採用したことが、Web 認証におけるパスキー の重要性の高まりに重要な役割を果たしました。

パスキーについて

パスキーは、デジタルセキュリティにおける重要な進歩であり、従来のパスワードのみによる認証に代わる、より安全な代替手段を提供します。パスキーは、ユーザーの身元を確認するための認証プロセスで使用される暗号キーです。簡単に漏洩する可能性のある共有される共通キーであるパスワードとは異なり、パスキーは各ウェブサイトに固有であり、Relying Party ID（簡単に言うと、認証するサービスには一意の名前が必要です）は通常、サービスのホスト名にバインドされているため、ほとんど偽造することができません。最近のフィッシングは、ユーザーを騙して認証情報を入力させ、似たようなサイト（例えば、https://[yourdomain]-authentication.com）で認証情報を手にいれることが多いので、これはフィッシングを防ぐための重要な要素です。

パスキーは通常、ユーザーのデバイス上で生成・保存されます。モバイルデバイスの生体認証または PIN 照合で保護されている場合、デバイス上でホストされている他のデータと同様に安全です。最後に、パスキーは WebAuthn と FIDO（Fast IDentity Online）標準に依存して検証確認プロセスをネゴシエートするため、フィッシングやその他のソーシャルエンジニアリング攻撃に耐性があります。

パスキーと パスワードとの違い

パスキーとパスワードの基本的な目的は同じです。しかし、その方法は大きく異なります。パスワードは、セキュアなリソースにアクセスするために、ユーザーが記憶し正しく入力しなければならない文字列です。パスワードは、総当たり攻撃、辞書攻撃、フィッシングなど、さまざまな攻撃に対して脆弱です。

一方、パスキーの場合、ユーザーは複雑な文字列を覚える必要がありません。その代わり、生体認証スキャンやデバイスの暗証番号で認証します。各パスキーは一意であり、1 つのウェブサイトまたはアプリにのみ使用できるため、各アカウントの安全性は一意です。さらに、パスキーはフィッシングなどのソーシャルエンジニアリング攻撃にも耐性があります。

パスキーと **FIDO** ハードウェアトークンの違い

パスキーはハードウェアトークンと一緒に使用することができ、ハードウェアトークンのセキュリティ特性をすべて提供します。秘密鍵はハードウェアデバイス上で物理的に保護され、コピーすることはできません。また、ハードウェアトークンをアクティブにして認証要求をするには、ボタンを押すなどの物理的な操作が必要です。パスキーはソフトウェア実装でも使用できますが、通常ハードウェアベースのトークンと同レベルの保護は提供されません。(最近のモバイル・デバイス・セキュリティのおかげで、この境界線は曖昧になりつつあります。）ここでの 1 つの課題は、パスキーを使用したハードウェアトークンの監査とその適用です。この記事を書いている時点では、パスキーにその実装があるかどうかは不明です。バックエンドのトークンが何に保存されているか、どのように保護されているかなどをサーバーがクライアントに問い合わせることができます。

たとえば、認証が必要なアカウントごとに一意のパスキーを作成し、実質的にアカウントごとに新しい秘密鍵を作成することで、クレデンシャルスタッフィング攻撃を防ぐことができます。ほとんどの FIDO ハードウェアトークンでは、秘密鍵をエクスポートすることはできません。このため、鍵の安全性は高く、例えば PIN でアクセスを制御することができ、一定回数間違って入力された場合は秘密鍵を消去する

ように設定することもできます。デバイスが対応していれば、バイオメトリクスを使用することもできます。

セキュリティ要件が非常に高い場合、ハードウェアトークンは他のシステムよりも多くの利点があります。鍵のエクスポートができないことは、セキュリティ要件が低いアカウントにとっては大きな問題です。ハードウェアトークンをどのようにバックアップしますか？答えは「しない」です。2 つ以上のハードウェアトークンを購入し、認証したいサービスに登録します。これは高価で面倒です。パスキーは、一般的なケース（ソフトウェアベースのトークン）に対して明確なセキュリティのトレードオフを行い、ハードウェアに縛られた秘密鍵のセキュリティよりも、信頼性と使いやすさ（複数のデバイスで秘密鍵を同期するオプション）を選びました。ハードウェアにバインドされた秘密鍵のセキュリティとしてモバイルデバイスの安全性はますます高まっていることに注意する必要があります。モバイル・ハードウェアトークン（たとえば、デフォルトでセキュアエリアや暗号化されたストレージ、強力なバイオメトリック・センサーを備えているものが多い）、10 年前や 20 年前には利用できなかったこれらの共有の鍵に適した場所を作っています。これについては、「パスキーの脅威モデル」のセクションで詳しく説明します。

パスキーはサイトごとに異なる秘密鍵/公開鍵ペアを必要とすることに留意してください。いくつかの一般的なトークンは、例えば 25 のキーペアのみをサポートします。これは、パスキーをサポートするサイトをたくさん利用すると、ハードウェアトークンのストレージ容量が足りなくなる可能性があるため、パスキーを使用するサイトを選択する必要があることを意味します。

パスキーと **2FA/MFA** との違い

2FA/MFA（多要素認証）には、攻撃者がユーザーのアカウントにアクセスするのを防ぐために使われる 2 つの一般的な戦略があります：

1) SMS やアクセスコードを生成するアプリケーションなど、インターネット帯域外の通信方法を使用して、ユーザーのアクセスコードを取得します。
2) ユーザーが自分のアカウントにアクセスできるように、再利用できないワンタイムアクセスコードを使用します。たとえ攻撃者がそれをコピーしたとしても、再度使用することはできません。

これは、2FA/MFA システムの主な弱点であるフィッシングにつながる可能性があります。簡単に言えば、もしユーザーが電子メールや電話を通じて、攻撃者がコントロールするシステムにユーザー名/パスワードと 2FA/MFA を使ってログインする必要があると信じ込ませることができれば、攻撃者はその情報を採取し、それを使って実際にログインし、アカウントを乗っ取ることができます。

パスキーは、認証に使用される秘密鍵を特定の DNS ホスト名にバインドし（Relying Party ID は通常ホスト名にバインドされるため）、各トランザクション中にランダムで無意味な値を使用することで、攻撃者が認証をアクティブに傍受するためにサイトをハイジャックしなければならないようにする戦略を使用します。これを防ぐため、パスキーは TLS の存在に大きく依存しています。 しかし、Let's Encrypt（https://letsencrypt.org/）のようなプロバイダーから無料の証明書が提供されている現在では、TLS の存在に頼る方が安全です。

さらに、2FA/MFA をパスキーと併用することで、認証をさらに安全にすることができます。サイトが、通常のセキュリティ要件の低いログインには 2FA/MFA を使用せず、ユーザーがアカウント回復メールを使

って特権的なアクションを取ろうとする場合のステップアップ認証に 2FA/MFA を使用することを強く検討すべきであると思います。パスキーは、適切に使用されれば、2FA/MFA がパスワードベースの認証に追加しようとしてきた初回ログイン時のセキュリティ向上を提供します。

パスキーと SSO との違い

パスキーとシングルサインオン（SSO）は一般的には別なものです。つまり、それらは関連しているが、互いに独立しています。一般的に、安全な SSO プロバイダーで SSO を使えるなら、SSO を使うべきです。プロバイダーが SSO をサポートしていないか、SSO プロバイダーがあまり安全でない場合、ログインするために利用可能な最も安全な方法（すなわち、パスキー）を使い、次に他の選択肢（2FA/MFA システムを使ったパスワードなど）を使うべきです。言い換えれば、ユーザー名/パスワードだけでセキュアにしている SSO プロバイダーを経由してサービスにアクセスすることは、Passkey を使ってそのサービスにアクセスするよりも安全ではないでしょう。2023 年後半現在、さまざまなベンダーがパスキーのサポートを展開し始めており、Google のように Gmail アカウントのデフォルトオプションにしたり、エンタープライズユーザー向けに有効にできるオプションにしたりしているところもあります。

パスキーとパスワードマネージャーの違い

パスキーはパスワードマネージャーで使用することができるので、この部分は少し混乱するかもしれません。実際、現在多くのパスワードマネージャーがパスキーをサポートしています。一見したところ、パスキーはパスワードマネージャーで管理されているパスワードと非常によく似ています。コンピューターにサイトごとにユニークで安全なパスワードを生成させ、パスワードマネージャーは、手動で上書きしない限り、そのサイトでのみ、そのパスワードを使用できるようにします。ここでの大きな違いは、パスキーではこれを上書きできないので、フィッシングされる可能性を大幅に減らすことができます（FIDO ハードウェアトークンと同様）。パスワードマネージャーでは、保存したパスワードを同期することができます。簡単に言うと、組織でパスワードマネージャーをすでに導入している場合、そのマネージャーでパスキーのサポートを有効にすると、誰かがパスワードを間違えて侵入する可能性を減らすことができます。

パスキーの使いやすさ vs. セキュリティ

パスキー標準の設計者は、使いやすさを優先する代わりにセキュリティに関するトレードオフを行いました。（たとえば、鍵のバックアップや同期を可能にするなど）という一般的な認識があります。これは事実ではなく、先に述べたように、パスキー はほとんどのユーザーのセキュリティを向上させ、多くの既存の攻撃をかなり難しくしています。パスキーは“セキュリティとユーザビリティを引き換えにします”と言われる主な原因は、多くの人がパスキーを現在のモバイル・ファーストの世界ではなく、PC ベースの世界の文脈で考えていることです。ガートナーのデータを引用すると、"2022 年の PC 出荷台数は 2 億 8620 万台に達し、2021 年から 16.2%減少しました"。逆に、スマートフォンの出荷台数は 2022 年に約 13 億 9000 万台に達し、PC1 台の出荷に対して約 4.8 台のスマートフォンが出荷されたことになります。タブレットは 2022 年に 1 億 6,320 万台となり、2017 年以降ほぼ堅調に推移しています（一方、PC の出荷台数は鈍化しています）。今後どうなるかは分かりませんないが、スマートフォンの出荷台数は PC を凌駕し続

けるでしょう。最近も PC 販売台数の減少が発表されました。"Global PC Shipments Fall 9% in Quarter Seen as Bottom for Market."（世界 PC 出荷台数、市場の底と見られる四半期に 9%減少）などのタイトルが付けられています。

つまり、ほとんどのユーザーにとって、今やスマートフォン・ファーストのテクノロジー体験ということになり、PC は着実にその数を減らしています。簡単に言えば、ほとんどすべての人がスマートフォンを所有し、多くの人は PC や個人用ノート PC すら持たなくなっているのです。スマートフォンは（安価なものであっても）通常、指紋リーダーや顔認識機能付きカメラといった形で生体認証をサポートしています。このような機能は PC でも利用可能ですが、多くの場合は追加のハードウェア（サポート付きウェブカメラや USB 指紋リーダーなど）が必要になります。過去 10 年間の 2 つ目の大きな変化は、クラウドと顔認証の受け入れです。 クラウドで提供されるアカウントは、E メール以外のこともできます。Apple ID（関連する iCloud サービス付き）と Google アカウント（関連する Google サービス付き）は、2 つの選択肢に過ぎません。写真やゲームからパスワードや文書に至るまで、さまざまなアプリケーションの電子メールやデータの保存と同期を提供しています。

また、使うのが難しセキュリティはユーザーによって回避されるだけでなく、使うのが難しいなセキュリティは、それを使用または回避することができない一部のユーザーを締め出すことになることを覚えておくことも重要です。パスワードが良い例で、高齢者やその他の認知能力に問題がある人はともかく、精神的に認知能力のある人が何百もの強力でユニークなパスワードを覚えることは不可能です。私たちは、すべてのユーザーが安全にコンピューターやインターネットを利用できるように、すべての人が使えるセキュリティを確保する必要があります。よくある問題をいくつか挙げれば、視力や運動能力（画面上の物体を回転させる CAPTCHA など）、識字能力が低いという理由だけで、不必要に人々を締め出したくはありません。

パスキーとサポートされていないアカウントとサポートされているアカウント

認証技術は、攻撃者がアカウントにアクセスできないように設計されているため、パスキーによってユーザーがアカウントにアクセスできなくなる可能性もあります。誤ってパスキーを削除したり、デバイスを紛失したり、バッテリーが切れたり、などなど。このようなインシデントの影響は、大きく 1 つの単純な要因に依存しています：問題のアカウントがサポートされているか、サポートされていないか（管理対象または非管理対象とも呼ばれることもあります）。 実際ユーザーがログインできない場合、何らかのサポート窓口に連絡し、タイムリーな助言を得ることができるのでしょうか？

例えば、Gmail の無料アカウントには実質的なサポートがありません。例えば、銀行口座の場合、通常、サポート電話番号や銀行の支店を利用することができ、身分証明書を提示すれば、新しい銀行カードを発行したり、パスワードをリセットしたりすることができます。

パスキーの潜在的な懸念のひとつは、自動化と効率化が進み、その結果、サポートがなくなったり、縮小されたりする可能性があることです。効率とユーザーをサポートするコストのバランスを見つけること

は、各サービスによって異なるでしょうし、ユーザーによっても異なるでしょう。例えば、1 人のユーザーがアクセスできなくなった場合でも、サポートは必要になります。一方、大企業の顧客は、組織内のユーザーを直接サポートできる管理者アクセス権を持つ人が複数おり、すべての管理者が同時にアクセスできなくなる可能性は極めて低いため、通常、直接的なサポートはあまり必要ありません。

パスキーの脅威モデル

ここでは、文章で説明するのではなく、パスキーを使用しない場合と使用した場合の、ウェブベースのアカウントに対する一般的な攻撃と、それにまつわる問題を表にまとめました。

攻撃	パスキーなし	パスキーあり	結論
パスワード総当たり攻撃 (「a」から始まって「zzzzzzz」まで)	レート制限、アカウント・ロックアウト、2FA/MFA/ハードウェアトークンの使用	不可能	パスキーを使った攻撃は不可能（秘密鍵/公開鍵暗号は推測できない）
辞書パスワード攻撃 (ブルートフォース、ただし一般的なパスワードの既知のリストを使用)	レート制限、アカウント・ロックアウト、2FA/MFA/ハードウェアトークンの使用	不可能	パスキーでは攻撃は不可能（秘密鍵/公開鍵暗号は推測できない）
クレデンシャルスタッフィング攻撃 (様々なリークや攻撃から得たユーザー名とパスワードの組み合わせを使用)	パスワード漏洩サイトの監視、レート制限、アカウントロックアウト、2FA/MFA/パスワードマネージャー/ハードウェアトークンの使用	不可能	パスキーでは攻撃は不可能（秘密鍵/公開鍵暗号は推測できない）
中間者（WiFi/DNS スプーフィングなどで認証を傍受し、認証データを取得する）	TLS の使用、2FA/MFA/パスワードマネージャー/ハードウェアトークンの使用	TLS を使用すると、パスキーはホスト名でサイトにバインドされる	パスキーでは攻撃は不可能である（TLS が使われていると仮定しているが、これは安全な仮定である）
なりすましサイト（偽サイトを立ち上げる、フィッシングや SEO 対策でユーザーをそのサイトに誘導し、本当のサイトの前に表示させ、クレデンシャルを取得する)	TLS の使用、よく知られたドメインを使用、2FA/MFA/パスワードマネージャー/ハードウェアトークンの使用	TLS を使用すると、パスキーはホスト名でサイトにバインドされる	パスキーでは攻撃は不可能である（TLS が使われていると仮定しているが、これは安全な仮定である)。

サーバーをハッキングしてパスワードデータベースのコピーを入手する。	安全なパスワードの保管、何重もの暗号化、しかしこれさえも常に有効とは限らない	パスキーを使用すると、サーバーは公開暗号鍵しか持たないため、脅威はない	パスキーを使った攻撃は不可能（秘密鍵/公開鍵暗号は推測できない）
リプレイ攻撃（セッションを傍受する、例：WiFi/DNS スプーフィングを使い、認証データを取得し、後で再利用する)	2FA/MFA/パスワードマネージャー/ハードウェア・トークンの使用	ほぼ不可能。（次のような理由：擬似ランダム関数では、1 つのセッションの中でリプレイの順番が入れ替わるわずかな可能性がある)	パスキーでは攻撃は不可能である（TLS が使われていると仮定しているが、これは安全な仮定である）
フィッシング / スピアフィッシング (SMS/E メールを使ったメッセージの送信)	2FA/MFA/パスワードマネージャー/ハードウェア・トークンの使用	パスワードの取得はもはや機能しないため、攻撃者はユーザーに悪意のあるソフトウェアをインストールさせ、パスキーやセッショントークンをコピーさせることに集中する	パスキーでは攻撃は不可能（パスキーは特定のドメインにバインドされている）
ソーシャルエンジニアリング（通常、電話、ほぼリアルタイムの電子メール、テキストなどの双方向コミュニケーションにより、ターゲットに何かをさせること）	2FA/MFA/パスワードマネージャー/ハードウェア・トークンの使用	TLS を使用すると、パスキーはホスト名でサイトにバインドされる。	攻撃はパスキーでは非常に難しく、攻撃者とパスキーを共有するためには複数のステップが必要です。また、技術的なセキュリティコントロール（パスキーの共有を無効にする）で防ぐこともできます。
物理的キーロガー（USB インラインキーロガーの使用）	2FA/MFA/パスワードマネージャー/ハードウェア・トークンの使用	タイピングがない（ハードウェアトークンの PIN の可能性はあり）	パスキーでは攻撃は不可能（パスワードではなく、秘密鍵/公開鍵暗号が使用される）
ソフトウェアのキーロガー（キー入力を記録するマルウェア）	2FA/MFA/パスワードマネージャー/ハードウェア・トークンの使用	タイピングがない（ハードウェアトークン PIN の可能性はあり）	パスキーでは攻撃は不可能（パスワードではなく、秘密鍵/公開鍵暗号が使用される）

ハードウェアまたはソフトウェアによるヒューマン・インターフェース・デバイスのアクティビティ・インジェクション (悪意のある USB デバイスやソフトウェアの使用による)	攻撃者が生成できない追加アクションを要求する（例：2FA/MFA 値、ハードウェアトークンに触れるなど）	攻撃者が生成できない追加アクションを要求する（例：2FA/MFA 値、またはハードウェアトークンに触れる）。	攻撃はパスキーの有無にかかわらず同じであり、攻撃者は物理的またはマルウェアによってユーザーのシステムに侵入する。
強制的なブラウジング（ウェブページを開くなどのアクション をトリガーする JavaScript などによるブラウザの制御）	攻撃者が生成できない追加アクションを要求する（例：2FA/MFA 値、ハードウェアトークンに触れるなど）	攻撃者が生成できない追加アクションを要求する（例：2FA/MFA 値、ハードウェアトークンに触れるなど）	攻撃はパスキーの有無にかかわらず同じであり、攻撃者は物理的またはマルウェアによってユーザーのシステムに侵入する。
イービルメイドと呼ばれるデバイスによ る物理的攻撃、寿命の終わり (ユーザーが不在の間、デバイスに物理的にアクセスすること)	攻撃者が生成できない追加アクション （2FA/MFA 値やハードウェアトークンへのタッチなど）の要求、デバイスの安全なロック、使用終了時のワイプなど。	攻撃者が生成できない追加アクション （2FA/MFA 値やハードウェアトークンへのタッチなど）の要求、デバイスの安全なロック、使用終了時のワイプなど。	この攻撃はパスキーの有無にかかわらず同じであり、攻撃者がデバイスに物理的にアクセスする必要がある。
デバイスとユーザーが存在する状態での物理的な攻撃（脅迫、強制力の行使など）	時間と労力があれば、攻撃者はおそらく暴力などを使ってユーザーに特定の行動をとらせることができるだろう。	時間と労力があれば、攻撃者はおそらく暴力などを使ってユーザーに特定の行動をとらせることができるだろう。	この攻撃は、パスキーの有無にかかわらず同じで、攻撃者がデバイスとユーザーに物理的にアクセスする。通常、これは犯罪行為である
セッショントークンの盗難	ステップアップ認証の使用	ステップアップ認証の使用	攻撃があってもなくても同じである
(ユーザー認証後にシステムにアクセスし、データをコピーするマルウェア)。	攻撃者はより多くの管理操作を試みる。	攻撃者はより多くの管理操作を試みる。	パスキー、および攻撃者がユーザーのシステムを物理的またはマルウェアで侵害した場合
アカウントの回復（ロックアウトされた場合にアクセスを回復するために使用されるバックアップ電子メール/電話などのアカウント回復方法を攻撃する）	強力なアカウント回復メカニズム	強力なアカウント回復メカニズム	パスキーがあれば、ユーザーが不注意でロックアウトされる可能性は低くなり、より強力なアカウント回復プロセスを使用できる可能性がある

パスキーデータ、または過去に保存されたパスワードの盗難 (ユーザーデバイスのデータをコピーできるマルウェア)	パスワードを保持し、それらを同期するアカウント/システムで強力な保護を行い、2FA/MFA/ハードウェアトークンを使用する。	パスキーを保持し、同期するアカウント/ システムで強力な保護を行い、2FA/MFA/ ハードウェアトークンを使用する。	この攻撃は、パスキーの有無にかかわらず同じであり、攻撃者はバックエンドシステムへのアクセス、または高レベルの侵害を示すユーザーデバイスのコントロールを必要とする。 いずれの場合も、失効は容易ではない。

ほとんどの場合、パスキーは悪用の可能性を大幅に減らし、使い勝手も向上させます。いくつかのケースでは、それは無駄です。しかし、特にセッショントークンの盗難のようなことを考慮すると、良い技術的解決策がないことがよくあります。ある時点で、もし攻撃者がシステム上で任意のコードを実行できるのであれば、その安全性を確保することは難しいですが、不可能ではないということを認める必要があります。例えば、帯域外ステップアップ認証はオプションですが、そのような解決策は、技術的なログインの解決策をはるかに超えています。

パスキーのセキュリティに関する "新たな "懸念

これらの多くは目新しいものではありませんが、パスキーの仕組み上、脆弱性と攻撃の実際の性質に新たなひねりが加えられています。

パスキーは、 デバイスからコピーできる暗号鍵を使用する。

パスキーは、ソフトウェアキーまたはハードウェアトークンに格納されたキーを使用することができます。ここでの唯一の新しい問題は、すべてのパスキー実装が「パスキーはすべてハードウェアトークン上になければならない」とか「サイト X/Y/Z または example.org で終わるパスキーはハードウェアキー内になければならない」といったポリシーの実施をサポートしているわけではないということです。繰り返しますが、ソフトウェアキーが使用されていても、これはオプションであり、ほとんどの実装は強固なセキュリティを備えています。また、多くの実装では、パスワード共有や同期の仕組みがすでに構築されており、それらは現在広く使われており、何年にもわたる強固な攻撃に耐えています。これは、パスキーが同期され使用されるエンドユーザーデバイスについても同様です。パスキーが使用されているかどうかにかかわらず、エンドユーザーデバイスは、ウェブサイトへのログインに安全に使用されるためにセキュリティが確保されている必要があります。

パスキーは TLS に依存している。

パスキー、そしてほとんどのウェブベースの認証は、TLS に大きく依存しています。20 年前、TLS（当時は SSL）は珍しいもので、常に当たり前のものではありませんでした。しかし現在では、TLS は一般向けウェブサイトでも内部向けウェブサイトでも広くサポートされており、Let's Encrypt のような無料の TLS 証明書プロバイダーも数多く存在します。

パスキーは共有可能

パスキーは同期するデバイスからコピーすることができます。これはパスワードや一部の 2FA/MFA システムにも当てはまり、例えば TOTP（時間ベースのワンタイムパスワード）では、最初のシードを記録して異なるシステム間で共有することができます。ほとんどの パスキークライアントは現在、別のアカウントにパスキーを共有することを簡単にはしていません。パスキー をサポートするパスワードマネージャーのようなサードパーティのアプリケーションは、このあたりの動作を強制するポリシーを許可することが期待されています。また、ハードウェアトークンであっても、システムやユーザー間で共有できることに注意する必要があります。USB over Ethernet は、プリンタやサムドライブなどのリモート USB デバイスを可能にするもので、10 年以上前から利用可能です。

秘密鍵/公開鍵ペアや秘密鍵シードフレーズに依存する他の多くの 2FA/MFA システムと同様に、パスキーの実装の中には、他のデバイスへのパスキーの共有をサポートしているものもあります。共有を簡単にするために、特に異なるプラットフォーム間のモバイルデバイス（例えば iPhone から Android、またはその逆）のために、いくつかの実装ではパスキーデータの QR コードを生成し、それを別のデバイスでインポートすることができます。これにより、ユーザーが Apple デバイスでパスキーを設定し、それを Android 携帯で共有したい、または Windows デスクトップから Apple 携帯で共有したいという一般的なユースケースが可能になります。さらに、ユーザーが QR コードを生成するだけでなく、それを記録して攻撃者にコピーを送信する必要があるため、攻撃者が秘密鍵の共有をソーシャルエンジニアリングすることが非常に難しくなります。また、パスキーソフトウェアは、「パスキーの共有は無効」や「QR コードによるパスキーの共有には管理者の承認が必要」などのセキュリティポリシーに対応しているため、ソーシャルエンジニアリング攻撃をほぼ防ぐことができます。さらに、高セキュリティのシナリオでは、ハードウェアトークンは秘密鍵のエクスポートを防ぐよう特別に設計されているため、鍵の共有を防ぐことができます。

セッショントークンの窃盗はまだ可能である

ほとんどのアプリケーションでは、認証が行われ、セッショントークンが渡されます。このセッショントークンが盗まれると、攻撃者はセあなたができることは何でもできるようになります。攻撃者があなたのシステム上でローカルにマルウェアを実行することでトークンを盗むことができれば、あなたのシステムからリクエストを送信することもできます。パスキーベースのシステム、およびパスキーを使用していないシステムに関するここでの答えは、機密性の高いアクションや管理的なアクション、あるいはユーザーの IP アドレスが変更された場合などには、よりステップアップした帯域外の認証と承認を使用することです。

販売/廃棄の前にデバイスを拭かなければならない

現代のデバイスには、私たちの生活、パスワード、電子メール、写真、文書などが保存されています。そのため、売却や廃棄の前に安全にワイプする必要があります。パスキーがこれを大きく変えることはありません。また、デバイスやコンピューターが紛失したり盗まれたりする可能性があることにも注意する必要があります。最近では、デフォルトで暗号化されており、多くの場合、生体認証やパスワードなど、暗号化を解除するための強力なセキュリティコントロールが施されています。会社所有のハードウェアをリサイクル・プロセスの一環としてワイプすることを義務付けているポリシーを持つ多くの組織にとって、これは問題ではありません。しかし、"自分のデバイスを持ち込む "システムを許容するポリシーを持つ組織にとっては、これは問題となりえます。同様の懸念は、請負業者、ホームユーザー、テスト用デバイス、その他の関連シナリオにも当てはまります。

漏洩したパスキーを取り消すことはできない

パスキーの漏洩が疑われる場合、パスキーを使用しているウェブサイトにサインインし、パスキーを削除してから新しいパスキーを作成しない限り、パスキーを取り消すことはできません。しかし、これはパスワードなど、事実上他のすべての認証方法にも当てはまり、SMS ベースのトークンや電子メールアドレスのような 2FA/MFA システムには特に当てはまります。一般的に失効をサポートしている認証方法は、クライアント TLS 証明書だけであり、その場合でも、TLS クライアント証明書を使用している多くのサイトは、失効した証明書のチェックを実装していません。OAuth のようないくつかの認証プロトコルは、トークン（たとえば、特定のサービスにアクセスするために発行された認証トークン）の失効をサポートしていますが、ベースとなる認証材料メソッドの失効（たとえば、「この ID に関連付けられているすべてのアカウントをリセットする必要がある」など）には簡単に対応していないことに注意する必要があります。

パスキーの監査とコンプライアンスは、 成熟していない

現在、ほとんどのパスキー実装には、強力なコンプライアンスポリシーと監査がありません。たとえば、「example.org という Web サイトのすべてのパスキーにはハードウェアトークンを使用しなければならない」というポリシーを簡単に設定することはできません。このようなコントロールは、特にパスワードマネージャーで利用できるようになることが期待されています。パスキーの多くは、強力なコンプライアンスポリシーと監査機能をすでに導入しています（実際、これらはパスキーのビジネスの基盤となっています）。

パスキーは、あなたが所持あるいは管理していないデバイスを安全に使用することはできない

ソフトウェアベースのパスキーを侵害されたデバイスに同期させると、攻撃者はシステムからパスキーをコピーできる可能性があります。これは、事実上、他のすべての認証システムにも当てはまり、また、ハードウェアトークンが存在する理由や、電話のようなデバイス外の方法が存在する理由でもあります。

パスキーはフィッシングされる可能性があるが、 より難しい

パスキーは、ユーザーを騙して攻撃者が管理するサイトにアクセスさせ、認証情報を入力させるという従来の意味でのフィッシングはできません。これは、パスキーで使用される依拠当事者識別子が、通常、問題のサービスのドメインとして設定されているためです。攻撃者がドメインをハイジャックしたり（DNS ハイジャックで可能）、ウェブサイトを侵害したりしても、認証情報を採取することはできません。これは、パスキーが秘密鍵/公開鍵暗号方式を使用しており、クライアントが認証フローの一部として秘密鍵を共有しないためです。

しかし理論的には、特定のサイトのパスキー秘密鍵をエクスポートして、デバイス間で同期することができます。しかし、ほとんどのソフトウェアクライアントでは、このデータは視覚的な QR コードとして共有されます。つまり、ユーザーは攻撃者にスクリーンショットを送るか、攻撃者と画面共有を行う必要があり、より複雑な攻撃を行うことになります。もしユーザーがハードウェアトークンを使って秘密鍵を保存しているのであれば、それをエクスポートして攻撃者に提供することは、たとえしたくてもできないでしょう。

パスキーの利点

パスワードの代わりにパスキーを導入するほぼすべての状況で、セキュリティが向上します。現在、パスワードマネージャーアプリケーションを使用してパスワードを管理している場合でも、パスキーに切り替えることで、誤ってパスワードを再利用したり、別のサイトに手動で入力したりすることがなくなります。現在パスワードマネージャーを使用しておらず、すべてのパスワードを安全に覚えて使用しようとしているとします。その場合、パスキーの方がより確実で良い仕事ができるでしょう。パスキーはまた、通知やアラートをサポートしていません。そのため、攻撃者は、ユーザーが最終的に我慢して「はい」や「OK」をクリックしてアラートを停止することを期待して、通知することでユーザーをスパムすることはできません。

パスキーのセットアップと 設定

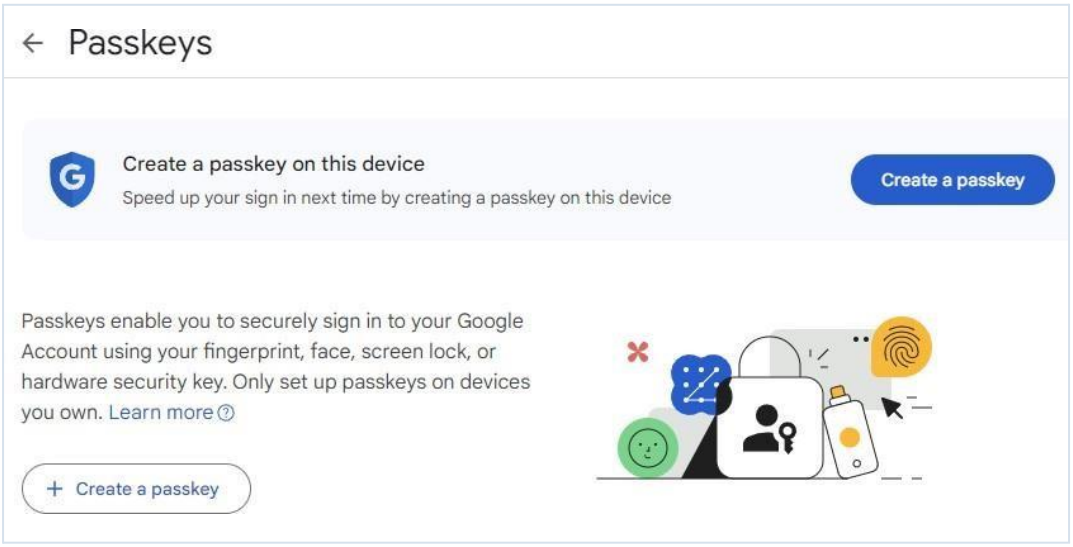
Google や Microsoft など、多くのベンダーが自社のサービスやクライアントソフトウェア、オペレーティングシステムでパスキーをサポートしているため、ここでも多くの混乱が生じています。パスキーはベンダーに縛られることはなく、パスキーをサポートするクライアント（Windows、Mac OS、Android や Apple などのモバイルデバイス、パスワードマネージャーなど）であれば、どのベンダーでも使用できます。

パスキー対応サービスとして３つあります。サーバー、ウェブブラウザ、パスキークライアントです。

Google ユーザーのパスキー

前述の通り、Google のような組織とは区別する必要があります。ウェブサイト側でのパスキーサポート（Google アカウントへのログインなど）と、クライアント側でのパスキーサポート（Android や Chrome OS の予定など）の両方があります。

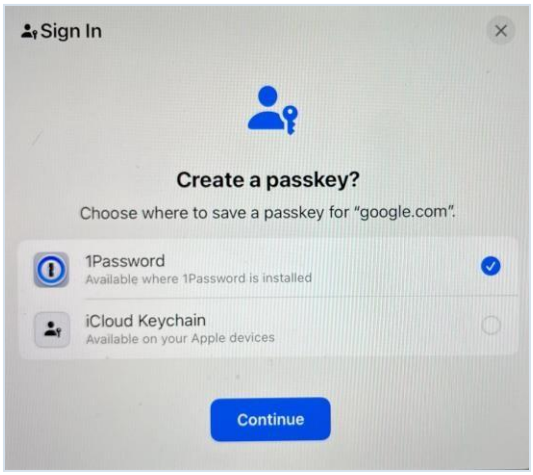
アカウントのパスキーサポートは、無料ユーザー（@gmail.com など）では現在利用可能で、Workspace ユーザー（ホストされたドメインなど）では有効にする必要があります。パスキーを設定するプロンプトが表示されない場合は、Google Account Security Configuration（https://myaccount.google.com/intro/security） から**"Passkeys"**を選択し、手動で設定することができます。パスキー を作成し、保存先（Chrome、パスワード マネージャー、Windows、Mac OS など）を選択します。



パスキーの作成を選択すると、パスワードマネージャーやオペレーティングシステムなど、パスキーの管理を有効にしているものに保存するよう促されます。

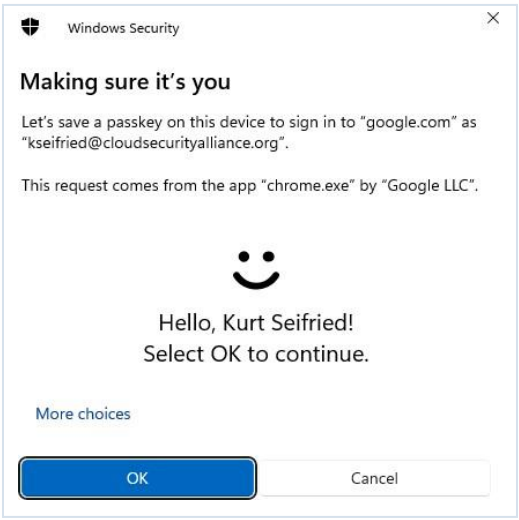
Apple ユーザーのパスキー

パスキーを設定すると、もちろんそれをローカルに保存することができ、キーチェーンに保存するオプションが提供されます：

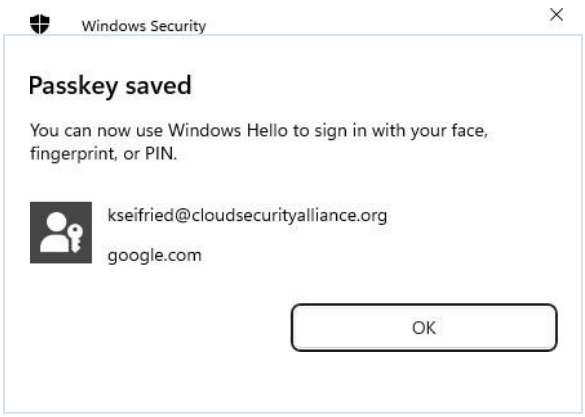


Windows ユーザーのパスキー

パスキーを設定する際、Windows に保存するよう促されます。



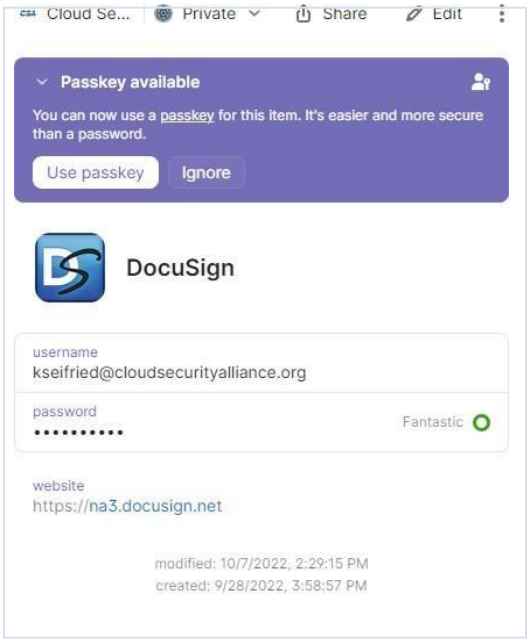
私自身は、バイオメトリクスを使ってセキュリティを確保しており、保存されると次のような画面が表示されます。



もちろん、Windows に保存されているパスキーを保護するために、他のセキュリティ方法（ハードウェアトークン、パスワードなど）を使うこともできます。

パスワードマネージャーユーザーのパスキー

他のシステムと同様に、パスワードマネージャーでパスキーを使用するのは非常に簡単です。パスワードマネージャーがウェブサイトと簡単にやり取りできるように、ブラウザの拡張機能をインストールする必要があります。限られたテストでは、パスワードマネージャーのウェブブラウザ拡張機能が、通常パスキー のセットアップを傍受し、それを処理することがわかりました。(実際、多くのパスワードマネージャーは、可能であればパスキーにアップグレードすることを勧めています。)

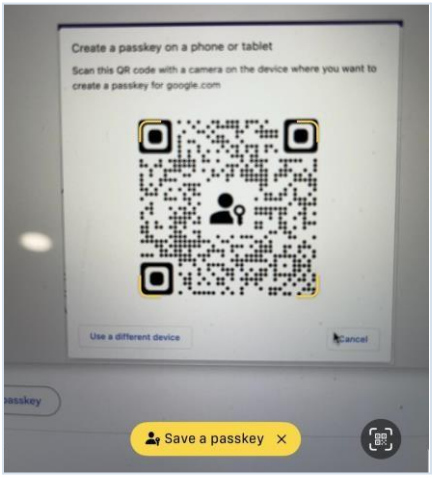


パスワードマネージャーを見ると、他のクレデンシャルと同じように保存されているのがわかります。

ユーザーエクスペリエンスとインターフェースに関しては、「パスワードマネージャーを使い続ける。アップグレードの選択肢がある場合は、パスキーを選択してください。」

他の デバイスにパスキーを設定する

また、メインデバイスを使って他のデバイスにパスキーをセットアップすることもできます（例えば、デスクトップ PC を使って携帯電話をセットアップする）。これにより、Android 携帯を使って Mac OS ラップトップ PC をセットアップしたり、Apple デバイスを使って Windows マシンをセットアップしたり、パスワードマネージャーを使ってセットアップしたりといった、エコシステムの「橋渡し」が可能になります。パスキーをセットアップする際、"別のデバイスを使う "というオプションを選ぶだけで、モバイルデバイスでパスキーをセットアップするための QR コードが表示されます。



パスキーの紛失に対処するシナリオ

パスキーの紛失に対処するシナリオは、パスワードマネージャー（使用している場合）やその他の方法で保存されたパスワードの紛失に対処するシナリオと事実上同じです。

パスキーを使用するすべてのデバイスの紛失に対処する

パスキーを使用して認証するために使用しているすべてのデバイスへのアクセスを失った場合（例えば、家の火事など）、主に 2 つのケースがあります。すべてのパスキーのバックアップがない場合、パスキーは失われ、影響を受ける各アカウントのアカウント復旧にフォールバックする必要があります。パスキーのバックアップがある場合は、新しいデバイスでそのデバイスへのアクセスを回復し、パスキーをそのデバイスに同期して通常通り使用する必要があります。

パスキーを同期・保存しているアカウントの紛失への対応

アカウントに接続された同期サービスを使用している場合、アカウントが削除されたり、アカウントへのアクセスが失われたりする可能性があります。このような場合、ほとんどの場合、デバイスにパスキーの作業コピーが残っているはずです。パスキーをエクスポートできるかどうか、または新しいアカウントで同期を再設定できるかどうかに応じて、パスキーを新しいアカウントに追加し、パスキーを保存および同期するための新しいアカウントを効果的に作成することができます。

パスキー紛失への対応

すべてのパスキーの同期と保存に使用されているアカウントが削除されただけでなく、すべてのデバイスにパスキーの削除を指示した場合、またはすべてのデバイスを失い、使用されなかったためにアカウントが削除された場合。基本的には、すべてのデバイスを失い、バックアップがないのと同じ状況です。影響を受けたアカウントごとにアカウントリカバリーにフォールバックする必要があります。

必要条件としてのパスキー vs. オプションとしてのパスキー

プロバイダーとしてパスキーを実装しても、すべての認証がパスキーを介して行われなければならないというわけではありません。例えば、Cloud Security Alliance は一般的に Apple、Google、Linkedin、Microsoft 経由の SSO をサポートしており、"クラシックな "ユーザー名とパスワードスタイルのログインをサポートしています。その理由は単純で、すべての人がリストにある SSO プロバイダーのアカウントを持っているわけでも、アカウントを取得できるわけでもないからです。これは、私たちが 2FA/MFA を要求しない理由でもあります。SSO プロバイダーで 2FA/MFA を使用することを選択できますが、Cloud Security Alliance は、2FA/MFA をサポートするデバイスにアクセスできない人も私たちのシステムにアクセスして使用できることを保証するために、2FA/MFA を要求しません。

しかし、多くのプロバイダーにとって、規模が大きくなれば、パスワードを完全に廃止し、人々をパスキーに移行させる方が良い選択肢だと考えられています。また、多くのプロバイダーは、ユーザーに パスキーへの移行を求めたり、選択肢を与えたりすることはできないと感じています。パスワードの代わりにパ

スキーを要求することは、もちろん、アカウントに対するフィッシングやクレデンシャルスタッフィングに終止符を打つことになります。フィッシングやクレデンシャルスタッフィング攻撃は、アカウント回復プロセスに対してはまだ可能でしょうが、前に議論したように、これは新しい脆弱性でも、著しく増加した脆弱性でもありません。パスキーを要求することは、パスキーを使用できるデバイスにアクセスできない人々（例えば、スマートフォンやコンピューターを所有せず、パブリックアクセスのコンピューターに依存している人々がまだいる）を事実上締め出すという可能性もあります。

パスキーを導入するベンダーは、特に多くの人が利用する「無料」サービス（電子メールなど）において、不利なグループに悪影響を及ぼすか、大人数のユーザーの全体的なセキュリティの健全性のバランスを考慮する必要があります。

パスキー 保証

必要条件としてのパスキーとオプションとしてのパスキーと同じように、保証に関する長期的な疑問もあります。保証は、クライアントが何かのセキュリティ特性を安全に保証することを可能にします。パスキーの場合、これは例えば「このパスキーはハードウェアトークンに格納されているのか、それともソフトウェアに格納されているのか」というプロパティかもしれません。保証の核となる部分は、いくつかのプラットフォーム（Apple など）でサポートされていますが、保証の利用はまだあまり始まっていません。ベンダーの中には、パスキーの保証に関して、セキュリティよりもユーザビリティを重視することを推奨しているところもあります：

> *パスキーを使用する方が、パスキーを使用しないよりも安全だからです。将来参照するために、保証情報を要求し、保存することは有用かもしれません。例えば、認証にセキュリティ上の問題が発見された場合、ユーザーに警告するためです。しかし、特別な理由がない限り、信頼された保証を要求しないことを推奨します。*
>
> *https://developers.yubico.com/Passkeys/Passkey_relying_party_implementation_guidance/Attesta tion/*

パスキーの未来

パスキーの採用は、クライアントデバイスとサーバーの両方のサポートにかかっています。良いニュースとしては、パスキーのサポートはクライアントデバイスではすでに広まっており、Microsoft や Apple、Google Chrome、そして評判の良いサードパーティのパスワードマネージャーアプリケーションのほとんどがパスキーをサポートしています。さらに、Google や Auth0 などの多くの認証プロバイダーは、ワンクリックで有効化できる パスキー 認証をすでにサポートしています。

パスキーの導入には、電話番号、ハードウェアトークン、その他の特別なハードウェアやサービスが必要ないため、ほとんどのユーザーやサイトにとって参入障壁が低くなります。そのため、パスワードやトークン/2FA/MFA の紛失によるアカウントのロックアウトに関連するサポートコストの削減（パスキーはバックアップと同期が可能）や、エンドユーザーにとっての使いやすさから、パスキー認証のサポートは急速に普及すると予測しています。また、ハードウェアトークンを持っているユーザーは、高セキュリティアプリケーション用のパスキーの保存にハードウェアトークンを選択できるという利点もあります。

ほとんどのユーザーは、デバイスへのアクセスを制御する生体認証などの強力な保護を備えた暗号化されたデバイスをすでに持っています。また、ほとんどの管理環境では、サードパーティのパスワードマネージャーが引き続き使用されると予測しています。サードパーティのパスワードマネージャーは、クロスプラットフォームに対応しており（Apple の iPhone と Windows の PC を使用しているのは一般的な状況です)、一般的に管理ツールや監査ツールが優れており、TOTP（時間ベースのワンタイムパスワード）のような他の認証方法もサポートしているからです。

パスキーはまた、バイオメトリクスがモバイルデバイスのセキュリティのデフォルトになり続けることを意味し、強力な認証と、ローカル・デバイスがバイオメトリクス・データを保持し、第三者と直接共有することなく処理することによる、プライバシー保護の両方の長所を提供すます。

対処すべき主なギャップは、ステップアップ認証の導入の増加です。ユーザーが、アカウントの制御を他人に委譲するなど、損害を与える可能性のある管理操作を行った場合、そのユーザーが攻撃者ではなく、本当にその操作を行っていることを確認する必要があります。
同様に、アカウント回復システムの改善も必要です。現在、大半のプロバイダーは、ユーザーの電子メールアドレスや電話番号の入手に頼っており、それを管理できなくなると、アカウントの回復やパスワードのリセットができなくなります。これはまれなことですが、起きないことではありません（ドメイン名の登録が失効したり、アカウントが非アクティブになったり、支払いがされなかったり、引っ越しをして新しい電話番号を取得したりなど)。その結果、その電子メールアドレスや電話番号に関連するすべてのアカウントにアクセスできなくなるようなことはあってはなりません。

電話番号／SIM スワッピング攻撃はまだ簡単すぎるし、エンドユーザーが利用できる防御メカニズムはほとんどありません。

結論

脅威モデルの観点からは、新たな重大なリスクや攻撃は見当たりません。ユーザビリティと信頼性の観点からは、パスキーはパスワードよりもはるかに優れています。最後に、サポートの観点からは、現在パスワードを管理するシステムを使用している場合、すでにパスキーがサポートされている可能性があります。セキュリティの高いアプリケーションでは、ハードウェアトークンを使用することもできます。

ウェブアプリケーションやウェブサイトは、日常生活（バンキング、ヘルスケア、教育、ショッピングなど）にとってますます重要になってきています。セキュリティを全面的に向上させ、ユーザー名やパスワードのような古くて安全でないものを排除しなければなりません。世界はまた変化し、スマートフォンはほとんどの文化圏で広く利用され受け入れられており、誰かが自分のコンピューターをポケットに入れていることに依存することは、もはや SF ではなくなりました。

簡単に言えば、パスワードを使っているすべての状況において、可能であればパスキーにアップグレードし、パスキーをバックアップして使用するデバイス間で同期させるのが理想的です。

次のステップ

パスキーの恩恵を受けるには、いくつかの具体的なステップがあります。

クライアントのためのパスキー実装の選択

前述したように、パスキーの実装を選ぶことは、パスワードマネージャーの実装を選ぶこととほとんど同じです。すでにパスキーをサポートしているものがあれば、それを有効にして使い続けるべきです。パスキーのサポートは、一般的に言って、パスワードマネージャーと同じ方法で提供されています：

- オペレーティングシステムのサポート（例：Windows と Apple）
- サードパーティのパスワードマネージャー

パスキーのサポートがある場合は有効にし、パスワード管理に使用しているシステムを使い続けることをお勧めします。現在パスワード管理を使用していないとすると、ウェブブラウザなどで保存パスワードを無効にしない限り、ユーザーはパスワードを保存していることになります。その場合、すぐにパスキー をサポートするパスワード管理戦略を選択する必要があります。

パスキーのサービスおよびソフトウェアのサポートについて

ユーザー名/パスワードのサポートを提供しているベンダーがある場合は、そのベンダーにいつパスキーをサポートする予定かを尋ねる必要があります。ソフトウェアベンダーも同様です。パスキーディレクトリで（https://passkeys.directory/）ベンダーのパスキーサポートを確認することもできます。

パスキー のサポート

このリストは包括的なものではなく、これらのベンダーを推薦するものでもないことにご留意ください。

オペレーティングシステム ベンダー

Android／Chrome

https://developers.google.com/identity/Passkeys/supported-environments

Apple

https://support.apple.com/en-ca/guide/iphone/iphf538ea8d0/ios

https://support.apple.com/en-ca/guide/iphone/iphf538ea8d0/ios

マイクロソフト

https://learn.microsoft.com/en-us/windows/security/identity-protection/Passkeys/

Web ブラウザ

Android／Chrome

https://developers.google.com/identity/Passkeys/supported-environments

Firefox (2023 年現在、USB トークンのみ)

https://www.mozilla.org/en-US/firefox/114.0/releasenotes/

Safari

https://support.apple.com/en-ca/guide/iphone/iph37306ae67/ios

サードパーティのパスワードマネージャー

1Password

https://1password.com/product/Passkeys

BitWarden

https://bitwarden.com/passwordless-passkeys/

Dashlane

https://www.dashlane.com/blog/tag/passkey

Nordpass

https://nordpass.com/passwordless/

ハードウェアトークン

Google Titan Key
https://blog.google/technology/safety-security/titan-security-key-google-store/Yubico
Yubikey
https://www.yubico.com/blog/a-yubico-faq-about-passkeys/

SSO プロバイダー

Google Gmail
https://blog.google/technology/safety-security/passkeys-default-google-accounts/
Google
https://support.google.com/a/answer/13529161

passkeys.dev（https://passkeys.dev/）によるデバイスおよびソフトウェアでのパスキーのサポート概要

passkeys.dev のウェブサイトには、デバイスのサポートリストを含め、パスキーに関する多くの優れたリソースがあります。

以下のデータは 2023-10-02 に https://passkeys.dev/device-support/ におけるものです。
iOS または iPadOS で作成したパスキーは、以下の環境で使用できます：

※FIDO クロスデバイス認証：(https://passkeys.dev/docs/reference/terms/#cross-device-authentication-cda)

- 同じ iPhone または iPad
- 同じ Apple ID を使用している iPhone と iPad（自動的に同期されます）
- 同じ Apple ID を使用している Mac（自動的に同期されます）
- FIDO クロスデバイス認証を使用する Mac
- FIDO クロスデバイス認証を使用する Edge と Chrome の Windows デバイス
- FIDO クロスデバイス認証を使用する Chromebook およびその他の ChromeOS デバイス
- FIDO クロスデバイス認証を使用した Edge と Chrome の Ubuntu デバイス

Android で作成したパスキーは、Android 上で使用することができます：

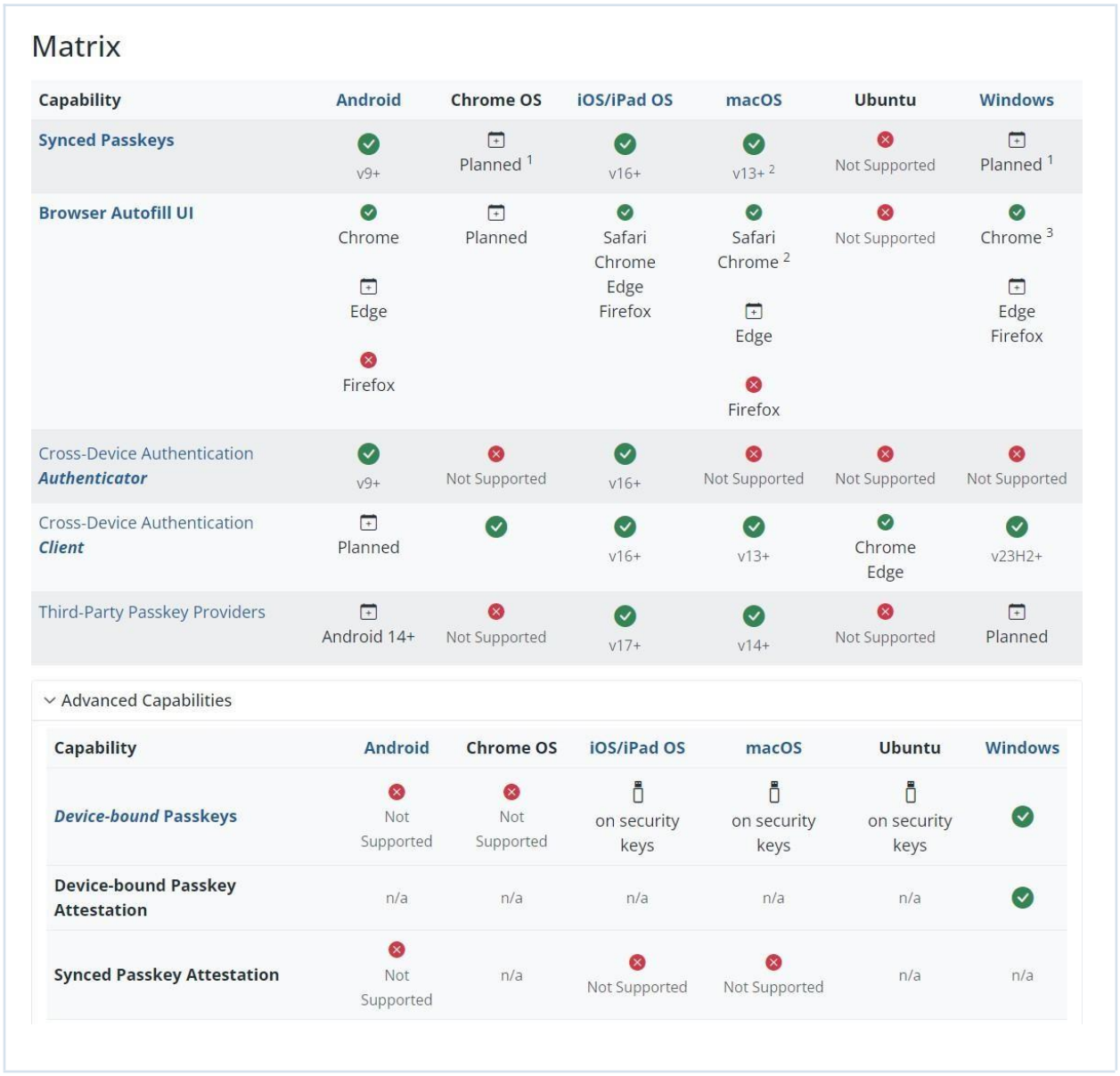
- 同じ Android 端末
- 同じ Google アカウントを使用している Android 端末（自動的に同期されます）
- FIDO クロスデバイス認証を使用する Mac
- FIDO クロスデバイス認証を使用する Edge と Chrome の Windows デバイス
- FIDO クロスデバイス認証を使用する iPhone と iPad
- FIDO クロスデバイス認証を使用する Chromebook およびその他の ChromeOS デバイス
- FIDO クロスデバイス認証を使用した Edge と Chrome の Ubuntu デバイス

MacOS で作成したパスキーは、以下の環境で使用できます：

- 同じ Apple ID を使用している Mac（自動的に同期されます）
- 同じ Apple ID を使用している iPhone と iPad（自動的に同期されます）
    - Mac で作成され、iCloud キーチェーン経由で iPhone や iPad に同期されたパスキーは、上記の "iOS または iPadOS "のすべての場所で使用することができます。

Windows で作成されたデバイス・バインド・パスキーは、Windows 上で使用することができます：

- それらを作ったのと同じ Windows デバイス



Matrix

Capability	Android	Chrome OS	iOS/iPad OS	macOS	Ubuntu	Windows
Synced Passkeys	v9+	Planned [1]	v16+	v13+ [2]	Not Supported	Planned [1]
Browser Autofill UI	Chrome Edge Firefox	Planned	Safari Chrome Edge Firefox	Safari Chrome [2] Edge Firefox	Not Supported	Chrome [3] Edge Firefox
Cross-Device Authentication ***Authenticator***	v9+	Not Supported	v16+	Not Supported	Not Supported	Not Supported
Cross-Device Authentication ***Client***	Planned		v16+	v13+	Chrome Edge	v23H2+
Third-Party Passkey Providers	Android 14+	Not Supported	v17+	v14+	Not Supported	Planned

Advanced Capabilities

Capability	Android	Chrome OS	iOS/iPad OS	macOS	Ubuntu	Windows
Device-bound **Passkeys**	Not Supported	Not Supported	on security keys	on security keys	on security keys	
Device-bound Passkey Attestation	n/a	n/a	n/a	n/a	n/a	
Synced Passkey Attestation	Not Supported	n/a	Not Supported	Not Supported	n/a	n/a

ご覧の通り、サポートは急速に向上しており、クロスプラットフォームへの対応もすでに完了しています。

パスキー の教育

ベンダーの中には、ユーザーがログインするときに パスキーのダイアログを表示するところもありますが、ユーザーにとっては、このダイアログが何のためにあるのか、なぜこのダイアログを使いたいのかが明確でない場合があります。また、多くのベンダーの場合、ユーザーはサービスのアカウント設定に入り、パスキーを手動で追加する必要があります。この場合のセールスポイントの 1 つは、パスワードの有効期限切れや、誤ってパスワードを公開してしまう心配がないことです。

続きを読む

パスキーに関する優れた資料は数多くあります：

Passkeys.dev
https://passkeys.dev/
Passkeys.directory
https://passkeys.directory/
Passkeys.io
https://www.passkeys.io/
Google Identity – パスキーによるパスワードレスログイン
https://developers.google.com/identity/passkeys
Windows におけるパスキーのサポート
https://learn.microsoft.com/en-us/windows/security/identity-protection/passkeys/
Passkeys の互換性：パスキーをサポートするプラットフォーム Apple-Passkeys のセキュリティについて
https://www.authgear.com/post/passkeys-compatibility
EFF - パスキーとプライバシー
https://www.eff.org/deeplinks/2023/10/passkeys-and-privacy

基礎となる規格と関連技術：

WebAuthn.io - WebAuthn 仕様のデモ
https://webauthn.io/
ウェブ認証：公開鍵認証情報にアクセスするための API FIDO アライアンス
https://w3c.github.io/webauthn/

参考文献

パスキーに関する誤解を解く
https://www.stavros.io/posts/clearing-up-some-passkeys-misconceptions/
ガートナー、2022 年第 4 四半期の世界 PC 出荷台数は 28.5%減、通年では 16.2%減
https://www.gartner.com/en/newsroom/press-releases/2023-01-11-gartner-says-worldwide-pc-shipments-declined-28-percent-in-fourth-quarter-of-2022-and-16-percent-for-the-year
世界 PC 出荷台数は 9%減、市場の底と見られる四半期に
https://www.bnnbloomberg.ca/global-pc-shipments-fall-9-in-quarter-seen-as-bottom-for-market-1.1982281
Hackernews - パスキー認証スレッド
https://news.ycombinator.com/item?id=35861260
PRF（疑似ランダム関数）
https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html#prfValues

Google Passkey の導入に関する議論

Google - デフォルトでパスワードレス：パスキーに切り替えよう
https://blog.google/technology/safety-security/passkeys-default-google-accounts/

Hackernews - Google ユーザーのデフォルトでパスキーが有効に
https://news.ycombinator.com/item?id=37832585

Slashdot - Google、全ユーザーのデフォルトサインイン方式をパスキーに
https://tech.slashdot.org/story/23/10/10/1235254/google-makes-passkeys-the-default-sign-in-method-for-all-users

TechCrunch - Google、全ユーザーのデフォルトサインイン方式をパスキーに
https://techcrunch.com/2023/10/10/google-makes-passkeys-the-default-sign-in-method-for-all-users/

Wired - Google、パスワード撲滅への取り組みを強化
https://www.wired.com/story/google-passkey-default/