



パスキー：パスワードレスの未来に一步前進

国家が支援するサイバー攻撃や悪意のある攻撃者がオンラインで激増する中、Google は、個人、企業、政府機関に対する保護をこれまで以上に重視しております。すべての人にとってより安全な世界を築くために、Google の専門知識を共有し、社会での連携を強化、サイバーセキュリティの最先端技術を前進させる取り組みを継続的に行っています。

現在、パスワードはオンラインの安全性確保における根幹をなす一方で、フィッシング攻撃をはじめとする脅威の増加はとどまるところを知りません。Google は以前からこうした問題を認識しており、2 段階認証プロセス (2SV)、Google パスワード マネージャー、セキュリティ キー、そして最新のパスキーに至るまで、認証ツールの利用を推進してきました。

課題

過去 60 年以上にわたって、パスワードはコンピュータで利用されてきました。しかし、現在のパスワード技術は、ユーザーや組織のデータの安全な保護という点からは、もはや十分な役割を果たしていません。フィッシング攻撃はパスワードにおけるセキュリティの脆弱性を突き、その規模は増大し続け、手口も巧妙さを増すばかりとなっています。以下、3 つの統計データを示します。

- ✓ 2021 年に発生したデータ侵害の 60% 以上は、認証情報の漏洩、もしくはフィッシング攻撃によるものでした¹。
- ✓ フィッシング攻撃によるデータ侵害は、2022 年に平均 491 万ドルの損害を企業や組織に与えました²。
- ✓ フィッシング攻撃は 2022 年に 61% 増加し、半年間で 2 億 5500 万回に達しました³。

2 段階認証プロセス / 2 要素認証 (2SV/2FA) は効果的ですが、余計な手間ユーザーを疲弊させてしまう場合も出てくるほか、フィッシング攻撃や、「SIM スワップ」による SMS 認証を突破してくる手口から完全に防ぐことはできません。

Google のソリューション

Google は FIDO アライアンスと連携して、パスワードに代わる、より簡単で安全なパスキーの実現を支援しました。そして、世界中の何十億人もの人々にフィッシング耐性のあるテクノロジーの提供を可能にしました。パスキーならパスワード入力は不要です。指紋認証、顔認証、または画面ロックを使用して、より簡単かつ安全なログイン体験を実現できます。

パスキーは 2023 年初頭に提供を開始しました。その導入の皮切りは、個人用 Google アカウント、900 万以上の Google Workspace ユーザー、Chrome や Android で利用可能なサードパーティ製のサイトやアプリでした。

最も簡単かつ迅速なログイン方法

パスキーは覚える必要も入力する必要もないので、**使いやすさが 4 倍**にアップします。指紋認証、顔認証、または画面ロックのみで、ご利用のすべてのデバイスとプラットフォームにログインできます⁴。

次世代のアカウントセキュリティ

パスキーは、フィッシングなどの脅威からアカウントを保護する非常に強力な手段です。また、パスキーの情報はローカルデバイスに保存されるので、推測や再利用が不可能であり、攻撃者から情報を安全に保護できます。

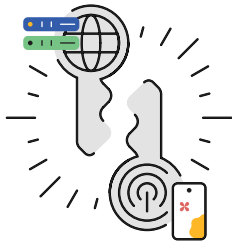
あなただけのプライバシー

パスキーは個人のデバイス上に非公開のまま保持されます。Google またはその他のパートナー事業者と共有されることは決してありません。本人だけが秘密鍵にアクセスできるよう、指紋認証、顔認証、または画面ロックを使用して認証します。





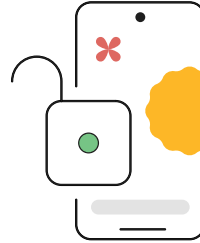
パスキーの仕組み



パスキーは2つの鍵で構成されています。1つは公開鍵で、ログインするウェブサイトのサーバーに保存されます。もう1つは秘密鍵で、個人のデバイスに保存されます。



ログインすると、ウェブサイトは公開鍵が秘密鍵と照合するかどうかを確認します。



照合を確認する際にユーザーに求められるのは、デバイスのロックを解除することだけです。



アカウントにログイン後、秘密鍵と生体情報は個人のデバイスに安全に保存され、外部で共有されることはありません。

より安全なエコシステムの実現

企業や政府機関にパスキーを提供

パスキーの使用により、ユーザーはセキュリティとユーザビリティの両面で大きなメリットを得られます。Google は、このテクノロジーをお客様（あらゆる規模の企業、学校、政府機関）に提供する初の主要なパブリッククラウドプロバイダであることを誇りに思います。

インターネット全体でパスワードレスのより安全なログインを実現するために提携

Google はパートナー各社と提携して、Chrome および Android プラットフォーム全体でパスキーを有効化し、ユーザーのためのより簡単で安全なログインを提供しています。1Password、Adobe、Dashlane、DocuSign、Kayak、メルカリ、ペイパル、Yahoo! Japan など、e コマース業界、金融テクノロジー業界、旅行業界のパートナーが、他のソフトウェアプロバイダとともに、Google のパスワードレス化への取り組みに参加しています。

Google におけるパスワードレス化への取り組み

パスキーは、Google が 10 年以上にわたって構想を描いてきた、パスワードレスの未来に大きく近づけてくれます。

2008	2011	2012	2013	2014	2017	2019	2023
簡単かつ安全なログインを実現する、Google パスワードマネージャーの提供開始。	Google アカウントで 2 段階認証プロセス (2SV) 導入。	Google 社員向けにフィッシング耐性のあるセキュリティキーを採用。	FIDO アライアンスに加盟し、パスワードレスの世界に向けた認証技術の標準化を推進。	フィッシング耐性のあるセキュリティキーの採用を外部人材へと拡大。	高いリスクにさらされるユーザー向け機能として、高度な保護機能プログラム (APP) を導入。	ウェブサイトをパスワードレスで再認証できるように、Android における FIDO のサポートを拡張。	Google アカウント、Workspace ユーザー、Chrome および Android におけるサードパーティパートナーへ、パスキーの提供を開始。

パスキーへの移行が進んでいくとはいえ、パスワードはこれからも私たちの生活の一部であり続けるでしょう。こうした状況の中、Google でログインをより簡単かつ安全にするために、Google は業界を含め、人々が次のステップに進むのを支援することに全力で取り組んでいきます。

出典: 1 - Verizon Data Breach Investigation report 2022 | 2 - IBM Cost of Data Breach report 2023
3 - CNBC's Cyber Report | 4 - Google Security Blog, May 2023



あらゆる人のオンラインでの安全を守るための、Google の取り組みを g.co/safety でご覧ください。