KEEPER®

Keeper Securityインサイトレポート
ハイブリッド認証状況を乗り切る

はじめに

脅威を取り巻く環境が変化する中で、センシティブデータやアイデンティティを保護するためには高度な戦略が不可欠です。従来のパスワードに基づく認証方式は依然として広く使われていますが、フィッシングやクレデンシャルスタッフィングなどの高度化された脅威に対して脆弱であることが実証されるケースが増えています。パスキーは、ユーザーのデバイスにローカルに保存された秘密鍵、そしてサービスプロバイダーに保存された公開鍵で構成される、公開鍵暗号を活用した有望な代替手段です。これにより、たとえ漏洩が発生した場合でも、サイバー犯罪者が公開鍵にしかアクセスできないことが保証されます。公開鍵は秘密鍵がなければ無益です。

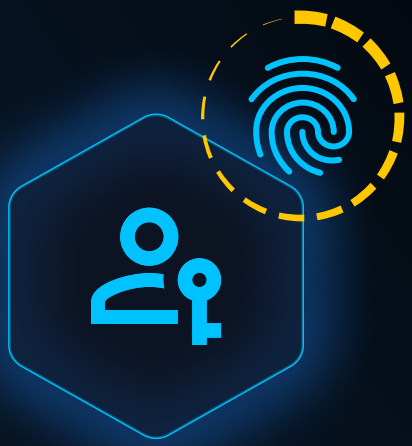
パスキーは非常に勢いを増しており、組織の80%がすでにこの技術を使用しているか、あるいは導入する計画を立てています。パスキーは、セキュリティ上のメリットに加えて、他に類のない使いやすさを備えています。ユーザーが複雑なパスワードを覚える必要がなく、シームレスな認証が可能になります。企業は、パスキーのメリット、特にフィッシングなどの一般的な攻撃ベクトルに対する耐性を認識するようになってきています。しかし、ウェブサイトやアプリケーションでのサポートが限られていることだけではなく、従来のシステムがもたらす課題や、パスキーが保存されたデバイスに物理的にアクセスする必要があることにより、パスキーの幅広い導入が依然として妨げられているのです。

パスキーの導入が進む一方で、パスワードは今もなお世界中の数百万ものシステムに深く根ざしています。これにより、パスキーとパスワードが共存するハイブリッドのアプローチが、個人や組織の両方にとって現実のものとなっています。

このレポートは、世界中のITリーダーやセキュリティリーダー800人以上からの洞察を引き合いにして、最新の認証ソリューションの進化について調査するものです。組織は、パスキーとパスワードのメリット、課題、そして相互運用性を検討することにより、より安全で使いやすいアプローチを開発してオンライン認証をすることが可能です。

ハイブリッド認証: 実践的なアプローチ

パスキーはもはや実験的なものではありません。最新の認証戦略に不可欠な要素なのです。Keeperの調査によると、パスキーの導入事例は急速に増加していますが、企業の40%は以前としてパスワードとパスキーを組み合わせたハイブリッドシステムを管理しています。これは、特に従来のシステムや特定のアプリケーションでは、依然としてパスワードに依存していることを明らかにするものです。



40%

は以前としてパスワードとパスキーを組み合わせたハイブリッドシステムを管理しています

ハイブリッドシステムのメリット

- **多層防御:** パスキーの使用によりフィッシングなどのリスクが軽減される一方、パスキーをサポートしていないシステムに対しては、パスワードの使用が解決策となる。
- **柔軟性の向上:** 企業は、依然としてパスワードに依存している環境でも、運用を維持しながら可能であればパスキーを導入することにより、少しずつ移行することができる。
- **ユーザーエクスペリエンスの簡素化:** パスキーを使用すると、ユーザーがパスワードを覚える必要がなくなり、素早く直感的な操作で認証されるため、ログインプロセスが合理化される。

ただし、ハイブリッドの認証アプローチを管理することには、複雑さが伴います。従業員は二つの異なる方法を操作しなければならず、ITチームは最新のソリューションを従来のシステムと統合するという課題に直面することになります。運用を合理化してセキュリティを維持するために、組織には明確なポリシーや確固たるトレーニング、安全なパスワード管理が必要です。

今後も継続されるパスワードの役割

パスキーの登場は認証技術に大幅な飛躍がもたらされたことを意味しますが、パスワードがすぐに廃止されるわけではありません。多くの組織では、以前としてパスワードに依存しています。これは、特に従来のシステムが広く普及していることや、パスキーのみを使用する環境に移行するためにはリソースが必要であることが原因です。Keeperの調査によると、67%の企業が、パスワードとパスキーの両方を使用するハイブリッド環境でもフィッシングが継続的な脅威だと回答していることから、依然としてセキュリティリスクが強調されています。

この現実は、不十分なパスワード慣行によってさらに複雑なものとなります。従業員の40%が複数のアカウントでパスワードの使い回しをしているため、組織はクレデンシャルスタッフィング攻撃に対して無防備になります。パスワード管理を統合した包括的な特権アクセス管理 (PAM) プラットフォームを使用することは、重要なシステムへのアクセスを保護する一方で、強力かつ固有のクレデンシャルを強要することにより、このようなリスクを軽減するのに役立ちます。組織がパスキーを主な認証方法としたソリューションへの移行に備える中、PAMは、今日のハイブリッド認証環境を効果的に管理するツールを提供します。

パスワードが以前として存在する理由

パスワードは、以下のような理由で根強く残っています。

- **従来のシステム:** 企業のシステムの多くが依然としてパスワードによる認証に頼っており、まだパスキーをサポートしていない。
- **コスト上の考慮事項:** パスキーに完全に移行することは、特に小規模な組織の場合、リソースを多く消費することになる。
- **行動上の課題:** ユーザーはパスワードに慣れているため、その慣習から転換するには、継続的な教育やトレーニングに支えられた文化的な変化が必要となる。

67%

ハイブリッド環境でもフィッシングが永続的な脅威であると報告している企業の割合。

セキュリティと使いやすさのバランス

ITリーダーシップの視点

認証における最大の課題の1つは、ユーザーエクスペリエンスを損なうことなく、堅牢なセキュリティを維持することです。ハイブリッドの認証システムを導入する際は、このバランスを維持するために慎重に計画することが求められます。

57%

ITリーダーの57%が二重システムの管理について不安に感じており、特にユーザーの混乱や統合する際の課題、トレーニングの必要性を懸念事項として挙げている。

70%

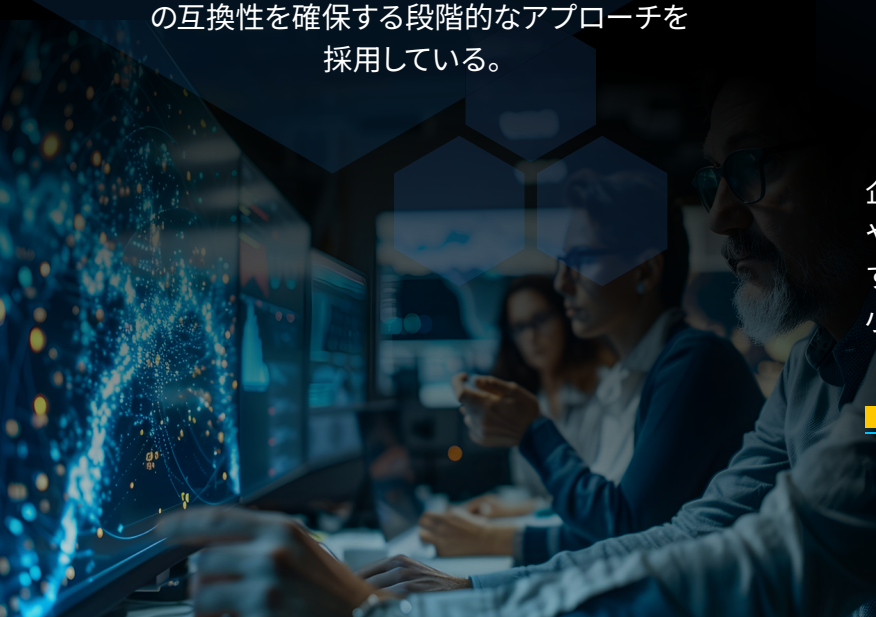
パスキーを導入する企業の70%は、徐々に取り入れることでユーザーからの賛同や運用上の互換性を確保する段階的なアプローチを採用している。

複雑さを乗り切る

パスキーを実装するにあたり、組織は以下のことが求められます。

- **ユーザーの教育:** パスキーをパスワードに代わって使用するタイミングと使い方に関する明確で一貫した指針を提示して、ユーザーの混乱やワークフローの中断を最小限に抑える。
- **システムの更新:** パスキーを既存のアプリケーションに統合するためには、ITインフラストラクチャへの投資が不可欠である。
- **プロセスの合理化:** シングルサインオン (SSO) や一元化された認証管理などのツールを使用すると、ハイブリッド環境での摩擦を軽減するのに役立つ。

企業は、セキュリティ目標に取り組むのと並行して使いやすさに対する懸念にも対処することで、システムに対する信頼を高め、生産性を向上させ、運用への混乱を最小限に抑えることができます。



パスキーの戦略的な導入

パスキーは、銀行や医療、重要インフラなど、不正アクセスが最も危惧される高度なセキュリティが求められる業界において、特に効果的です。一方、パスワードは依然としてリスクの低いアプリケーションに対して有効な選択肢であり、従来のシステムやそれほど重要ではない資産に対してコスト効率の高い解決策を提供します。十分なセキュリティを確保するためには、パスワードは少なくとも16文字の長さで、大文字、小文字、数字、記号が含まれたものであり、多要素認証が利用できる場合はいつでもそれを有効にして保護されることが推奨されます。

認証方法を多層化するこの戦略により、セキュリティと効率のバランスが確保されるため、企業は脅威による影響が最大となる箇所にリソースを割り当てることができます。

リスクに合わせて認証を調整する

認証戦略を最適化する組織は、次のことを考慮する必要があります。

- **厳重なセキュリティが求められる環境:** 可能な場合はパスキーを使用して、センシティブデータ、特権アカウント、顧客記録を保護する。
- **低リスクのアプリケーション:** 漏洩のリスクが低い重要ではないシステムに対しては、パスワードの使用を維持す
- **従来のアプリケーション:** パスキーを使用できない場合は、パスワードのベストプラクティスを適用し、MFAを実装してセキュリティを強化する。

将来に備える

80%

組織の80%が、今後パスキーとパスワードの両方を統合する計画を立てている。

70%

現在パスキーをサポートしていない企業の70%が、重要なシステムを優先する段階的な導入を検討している。

デジタル脅威の環境が変化するにつれて、認証戦略も進化しなければなりません。パスキーへの移行は大きな前進を意味しますが、企業は長期的な視点でこれにアプローチする必要があります。Keeperの調査で得られた重要な結果は以下のとおりです。

企業向けの推奨事項

企業は、チームがパスキーを効果的に使用し、潜在的なセキュリティ脅威を認識する知識を確実に身につけるために、従業員トレーニングに優先的に投資すべきです。パスキーを使用できるシステムにアップグレードすることは、シームレスな相互運用性を確保するのに役立つため、インフラストラクチャを最新にすることが不可欠です。また、認証方式への多層化されたアプローチも推奨されます。これにより、企業はパスキーと従来の方法の両方の長所を活用できるため、さまざまなシステムで発生するリスクを軽減できるためです。結局のところ、認証の未来は適応性に依存します。情報を入手し積極的に行動することで、企業は現在の課題に対処できるだけでなく、セキュリティを強化する新しい技術を受け入れることも可能になるのです。

調査方法

この調査は、Keeper Securityが独立系の調査機関であるTrendCandyと協力して実施しました。調査は、米国やカナダ、英国、フランス、日本、オーストラリア、ニュージーランド、ドイツなど、世界の主要地域のITリーダーおよびセキュリティリーダー合計801人を対象に実施されました。