yubico

耐フィッシングMFAでアカウント乗っ取りを阻止できる企業をつくる

企業のデバイス紐付け戦略においてパスキーを検討する際の重要な考慮事項

ユーザー中心の認証、企業での認証の新たな領域

パスワードは、従来のIAMアイデンティティライフサイクルの各段階で、あらゆる側面に組み込まれています。残念ながら、パスワードの盗難はオンラインのセキュリティを損なう最大の脅威ベクトルの1つです。しかし、最近では政府機関だけでなく民間企業においても、非常に脆弱なパスワードベースの多要素認証を耐フィッシング多要素認証（MFA）に置き換え、さらに理想的にはパスワードを完全に排除したパスワードレス認証に置き換えることで、フィッシング攻撃に対するサイバーセキュリティ防御を強化するという重要な義務が課されています。

ゼロトラストアーキテクチャ

耐フィッシングMFAの採用

パスワードレスや新しいオンデバイス認証ソリューションの最近の進化に伴い、組織がユーザーのアイデンティティ認証情報を確立し、そのライフサイクルを通して管理する方法が進化しています。

耐フィッシング認証から ……→ 耐フィッシングユーザーへ

従来、組織が考えていたのは、フィッシング耐性がある認証であり、フィッシング耐性があるユーザーではありません。これは、認証イベントを機密性の高いシステム、アプリ、サービスにログインする時点として考えるのか、ユーザーがどのように生活し、どのように働いているかについて考えるのかの違いです。多くの場合、ユーザーは、1日のうちにプラットフォーム（Apple、Google、Microsoft）やデバイス（スマートフォン、ラップトップ、タブレット）間を移動したり、個人用と企業用のアプリやサービスの間を移動したりします。企業は、ユーザーがどのようなビジネスシナリオ（リモートワーカー、モバイル機器の使用制限、共有ワークステーション、サプライチェーンのサードパーティなど）で従事しているかに関係なく、または使用しているプラットフォームやデバイスに関係なく、フィッシング耐性を提供する認証の種類をユーザーに提供することを考える必要があります。

パスキーの導入

FIDOアライアンスは、消費者と組織両方のパスワードレスを促進させる方法として、パスキーを導入しました。Google、Apple、Microsoft、Webブラウザなどの主要なプラットフォームでパスキーを使用できるようになりました。パスキーソリューションの開発により、企業ごとに新しいエンタープライズアイデンティティのセキュリティ・イベントが作成されました。

FIDO

パスワードベースのシステムからの移行に焦点を当てたグループ、FIDOアライアンスが支持するオープンなセキュリティ標準。

認証情報

システムにログオンしたときに「ゲートを通る」ことができるユーザーの一意のID。

多くの場合、組織とそのユーザーは、パスキーと、パスキーが常駐しているオーセンティケータを混同しがちです。パスキーは単なるFIDO2認証情報であり、スマートフォン、またはタブレットやラップトップなどの汎用デバイスに常駐させることができます。また、FIDOハードウェアセキュリティキーなど、セキュリティ専用のオーセンティケータであるポータブルデバイスにも常駐させることができます。

パスキーとは、認証情報そのものであり、デジタルファイルです。
オーセンティケータはパスキーが常駐している場所です。たとえば、スマートフォン、ラップトップ、ハードウェアキーなどのデバイスです。

パスキー

オーセンティケータ

企業ユーザーの保護

ユーザーには異なる認証ニーズがある

すべての企業ユーザーが毎日同じ仕事をするわけではありません。ビジネスのニーズに応じて、ユーザーはラップトップをリモートで作業したり、会議中にスマホで電子メールにアクセスしたり、製造現場の共有ワークステーションにアクセスしたりする必要があります。企業ユーザーは、さまざまなタイプの認証ニーズを持ち、それに応じて使用するオーセンティケータのタイプが異なります。企業ユーザーは、リモートワーカーまたはハイブリッドワーカーである場合もあれば、スマホが選択肢に入ることがない、モバイル利用が制限されたで作業する場合もあります。また、異なるユーザーがすべて同じコンピュータ端末上で安全にログインおよびログアウトする必要がある共有ワークステーションで作業している場合もあります。

したがって、ユーザーがパスキーを保持する必要があるオーセンティケータのタイプは、ユーザーの役割の機密性、またはアクセスする必要があるデータやシステムのタイプによって異なる場合があります。ハードウェアセキュリティキーは、セキュリティ専用のポータブルオーセンティケータであり、ユーザーが企業の広範なビジネスシナリオで安全かつシームレスに作業できるようにします。一方、プラットフォームオーセンティケータは、スマートフォンやラップトップなどの汎用デバイスに組み込まれています。さらに、オーセンティケータアプリなどのモバイルアプリケーションも、ユーザー認証ソリューションを提供します。これらのオーセンティケータにはすべて、セキュリティと使いやすさのトレードオフがあります。企業は、必要なセキュリティ保証のレベルと、許容できるリスクのレベルを決定する責任があります。

セキュリティキー

アテステーションを使用してデバイスに紐付けた認証情報

プラットフォームオーセンティケータ

デバイスに組み込まれているオーセンティケータ

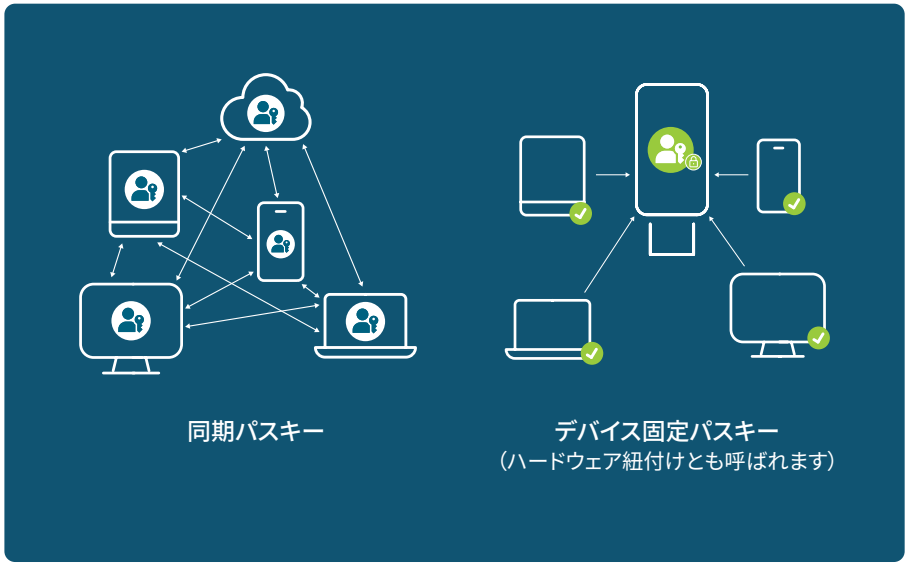
サードパーティオーセンティケータアプリ

ユーザー認証ソリューションを提供するアプリケーション

さまざまなパスキークラス

すべてのパスキーが同じように作られているわけではありません

パスキーはパスワードよりも安全であり、パスワードレス認証に迅速に移行できるため、セキュリティと効率を向上させることができます。さまざまなパスキーの実装があり、セキュリティと使いやすさのトレードオフがそれぞれにありますが、すべてのパスキーが同じように作られているわけではなく、すべてが企業に適しているわけでもありません。



同期パスキー

デバイス固定パスキー
（ハードウェア紐付けとも呼ばれます）

同期パスキー

企業向けではなく一般消費者向けに設計

同期パスキーはコピー可能な認証情報であり、スマートフォン、ラップトップ、タブレットなど、ユーザーのアカウントに接続されているすべてのデバイスにコピーされます。同期パスキーは、他のユーザーのアカウントと共有したり、別のユーザーのアカウントにコピーしたりすることもできます。これが企業にとって深刻な弱点の原因になることがあります。同期パスキーは、リモートワーク、サプライチェーンのセキュリティ、コンプライアンス、サポートの複雑さなど、主要な企業シナリオにおいて、重大なリスクとエクスポージャギャップをもたらします。

詳細については、企業の同期パスキーの落とし穴をご覧ください。

デバイス固定パスキー

企業ユーザー向けに設計

デバイス固定パスキーは、同期パスキーと比較して、企業がFIDO認証情報をより細かく制御できるようにします。

ただし、デバイス固定パスキーにはさまざまなタイプがあります。スマートフォンやラップトップなどの日常的な汎用デバイスに常駐する、デバイス固定パスキーがあります。ハードウェアセキュリティキーに存在するデバイス固定パスキーは、最高のセキュリティ保証を提供することが知られており、企業が認証情報の安全性を証明できるアテステーションが提供されます。ハードウェアセキュリティキーを使用すると、企業は信頼性の高い認証情報ライフサイクル管理プロセスを構築できます。セキュリティキーを使用すると、企業ユーザーは新しいデバイスを登録し、企業パスキープロバイダに対して認証することができます。また、各ユーザーは、認証プロセス中に自分自身を簡単かつ安全に認証するためのポータブルでフィッシング耐性を持つ認証情報を持っているため、別のデバイスに紐付けられた認証情報（Windows HelloやOkta FastPassなど）を登録できます。このソリューションは、ヘルプデスクからリスクを排除し、企業があらゆる業界の最も厳しい要件に準拠できるようにします。

同期パスキーとデバイス固定パスキー

同期パスキー

スマートフォン、タブレット、ラップトップ、その他のデバイス上に存在し、
多くのデバイス間でコピーや同期が可能です。

デバイス固定パスキー

日常的なデバイスとは別のUSBキーやその他の独立した
ハードウェア上に存在し、高いセキュリティ保証を実現できます。

パスキーツールボックスを使用してすべてを網羅

同期パスキーとデバイス固定パスキー間での異なるパスキー実装

ユーザーは基本的に、3種類のオーセンティケータを所有しており、これらのオーセンティケータ内に常駐しているパスキーを使用して認証を行うことができます。市場で最初に導入されたパスキーソリューションであり、認証の絶対基準はハードウェアセキュリティキーです。セキュリティキーを使用すると、ユーザーはデバイスに格納されているパスキーを使用して認証を受けることができます。ユーザーは、セキュリティキーをデバイスからデバイスに責任を持って移動させます。重要なことは、専用オーセンティケータは、多くの企業にとって重要であるモバイル利用制限環境や共有ワークステーション環境のセキュリティ保護など、モバイル上のオーセンティケータでは解決できない企業の特定のユースケースを解決するということです。

市場に新たに登場したその他のソリューションには、サードパーティパスキープロバイダがあり、これらのアプリケーションは、ユーザーがデバイス固定パスキーと同期パスキーの両方を管理できるように作成できます。2021年に導入が開始された同期パスキーは、これらの消費者向けパスキーに対するプラットフォームのサポートによって補完されていました。同期パスキーは、さまざまなプラットフォームでサポートされるようになりました。これらのプラットフォームの中には、同期パスキーの使用は、プラットフォームのオーセンティケータのみとしているものもあります。

	同期型 （使いやすさを重視; セキュリティは低い）	デバイス/ハードウェア固定（紐付け）型 （セキュリティ保証が高い;すべてが同じ ように構築されているわけではない）	
プラットフォーム	iOS OSX android	Windows Hello	セキュリティキー YubiKey
サードパーティ アプリケーションプ ロバイダ	DASHLANE 1Password	Microsoft Authenticator	

iOSおよびMacOSでは、プラットフォーム上での同期パスキーの作成のみがサポートされるようになりました。Google Androidでも、同期パスキーのみがサポートされるようになりました。Chromeでは、同期パスキーとデバイス固定パスキーの両方がサポートされており、リライングパーティやサービス（Dropboxなど）では作成できるものを選択できます。オプションに追加すると、Windows Helloでは、そのワークステーションデバイスに紐付けられたパスキーの作成のみが有効になります。また、1PasswordやDashlaneなどのサードパーティプロバイダは、同期パスキーの作成をサポートしています。市場には、ソフトウェアで支援するデバイス固定パスキーをサポートするソリューションもあり、新たに登場するパスキーにさらなる進展が見られます。

パスキーの用語で混乱していますか？ここで、覚えておくべき主なことは次のとおりです。秘密鍵を保護することが重要です。

秘密鍵が格納されている場所を特定することは、パスキーに関連するリスクを理解する上で不可欠です。リライングパーティまたはサービスは、認証情報の登録に含まれているデバイスアテステーションを利用して、パスキーが企業で使用が許可されているデバイスに保存されていることを判断できます。

すべてのパスキーは公開鍵暗号方式に基づいており、安全に格納されている秘密鍵と共有または公開されている公開鍵のペアが存在します。秘密鍵は秘密である必要があり、秘密を保持することはパスキーソリューションとパスキーが存在する基盤システムの義務です。同期型パスキーを使用すると、秘密鍵を複数のデバイスとクラウド管理システムにコピーできます。これにより、企業はパスキーを追跡し信頼することが困難になります。デバイス固定パスキーにより、企業が必要とする管理と制御が向上します。しかし、企業が必要とする秘密鍵の保護を提供できるのは、セキュリティのために特別に構築されたポータブルハードウェアオーセンティケータに常駐しているデバイスバインドパスキーだけです。

フィッシング耐性を持つユーザーになる

フィッシング耐性のある認証だけでは不十分

パスワードレス認証の採用を促進するためにパスキーが導入されたことで、企業における認証の新しい目標は、フィッシング耐性のある認証だけでなく、フィッシング耐性のあるユーザーを確立することとなります。パスキーは、真のユーザー中心の認証および組織内でのユーザーの業務状況という文脈で考慮する必要があります。この戦略では、すべてのユーザーが、すべての認証タスクにフィッシング耐性のある認証ソリューションを使用する必要があります。フィッシング耐性のある認証からフィッシング耐性のあるユーザーへと目的を移行すると、企業はユーザーがヘルプデスクに電話で問い合わせることなく新しいデバイスを登録できるようにすることができ、高いレベルの保証が維持されることで、ユーザーは安全にリモートで業務を遂行できるようになり、同時にヘルプデスクの運用上のリスクやセキュリティ上のリスクを排除できます。

このことを念頭に置いて、焦点は適切なオーセンティケータの選択（スマホかセキュリティキーなど）から、ユーザーが持つすべての認証オプション（およびパスキー）が安全に登録され、ユーザー体験の目標と企業のセキュリティニーズの両方を確実に満たすことに移ります。

パスワードや、SMS、ワンタイムパスワード、モバイル認証などの従来のフィッシング可能なMFAソリューションから移行することは、ユーザーが複数の認証情報、パスキー、パスキープロバイダを持つ世界へと移行することを意味します。この変化により、認証情報ライフサイクルは、ユーザーとの重要なやり取りを管理する必要がある企業にとって新しい転換点となります。

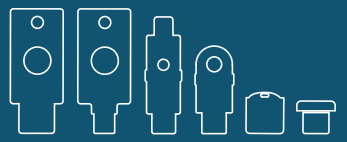
ユーザーごとに、企業には次のイベントに対するソリューションが必要です。

- **最初の認証：**新しいコンピューティングデバイス（スマホ、ラップトップ、またはデスクトップ）をデバイス管理システムに安全に登録するための、そのデバイスでの最初の認証
- **認証情報登録：**信頼できる/管理されたデバイス、または信頼できない/管理されていないデバイスでの、同期型またはデバイス固定型の認証情報のフィッシング耐性がある登録
- **パスキープロバイダへの最初の認証：**信頼できる/管理されたデバイスへのパスキーの同期を開始するために、新しいデバイスのパスキープロバイダへの最初の認証
- **パスキープロバイダへのWeb認証：**信頼できない/管理されていないデバイス上のパスキーにアクセスするための、パスキープロバイダへの認証
- **安全なセルフサービス認証情報管理：**従業員が以下のようになったときのためのセルフサービスツール
  - 管理されたデバイスを紛失または廃棄し、そのデバイスに保存されている認証情報を無効にする
  - パスキープロバイダへのアクセスを回復する必要がある
  - プラットフォームアカウントへのアクセスを回復する必要がある
  - 既存のYubiKeyを管理し、使用されなくなった認証情報をすべて無効にするか、紛失としてマークする必要がある
- **安全なセルフサービスオーセンティケータ管理：**ユーザーがアカウントロックアウトのリスクを回避するために新しいパスワードを必要とする場合に、追加のデバイス固定パスキー（たとえば、YubiKey上に存在している）をオーダーするためのセルフサービスプロセス
- **アカウントロックアウト：**すべてのオーセンティケータ/認証情報へのアクセスを失った後に、企業で管理されるアカウント用に発行された新しい認証情報をユーザーが取得するための安全なプロセス

フィッシング耐性のあるユーザーとポータブルパスキー

フィッシング耐性は、特定の隔離されたデバイスやプラットフォームに結び付けられるべきではありません。ユーザーがどのアプリ、サービス、システムにログインしているかに関係なく、企業生活や私生活全体にわたって、**ユーザーとともに移動できる**ようにすべきです。これにより、フィッシング耐性のある企業がエンドツーエンドで構築されます。YubiKeyに存在するようなデバイス固定パスキーは、ポータブルな独立したハードウェアにパスキーの安全な暗号化方式を組み合わせたものです。YubiKeyを使用すると、強力な認証がユーザーと一緒に移動し、特定のプラットフォームやモバイルデバイスに関連付けられていないフィッシング耐性のあるユーザーが作成されます。

YubiKeys



アテステーションを備えたデバイス固定型認証情報

適切なパスキーを選択する際の企業の考慮事項

すべてのパスキーは、フィッシング耐性があると考えられるが、すべてが企業のニーズに適合しているわけではない

多くのパスワード置き換えソリューションは、フィッシング耐性のある認証を市場に投入することに重点を置いており、企業はこれらのソリューションを活用してパスワードを置き換えようとしています。ただし、企業は、アカウントのライフサイクルの各段階および関連する企業の考慮事項に注目して、汎用デバイス上のデバイス固定パスキーが適切かどうか、またはセキュリティ専用に構築されたオーセンティケータ上のデバイス固定パスキーが適切に機能するかどうか、またはハイブリッドアプローチが適切かどうかを判断する必要があります。理想的な戦略は、重要な認証ポイントを耐フィッシングにするだけでなく、フィッシング耐性のあるユーザーの作成を可能にし、ユーザーは、生活や仕事の中で機密性の高いオンラインアカウントにログインする際に、お気に入りのあらゆるデバイス上でさまざまな認証手順を通じて保護されるようになります。

オンボーディング/登録

認証情報の復旧

コンプライアンスと監査

企業にとって安全なオンボーディングと復旧は必須

お客様が実装することを決定するMFAは、登録および復旧と同じ程度の安全性にしかなりません。OTPコードの送信などのフィッシング可能な方法を使用した登録またはオンボーディングプロセスは、脆弱なMFAの導入につながります。FIDO認証情報を登録またはリセットできる人がいると、耐フィッシングMFAを使用する目的が損なわれます。組織は、MFA方式の登録を可能にするための堅牢なオンボーディングおよび復旧ソリューションを備えている必要があります。

さまざまなデバイス固定パスキーのアプローチが、企業内のユーザーがオンボーディングや認証情報の復旧を行う際のユーザーのある日の行動に対してどのように機能するか、また、各パスキーアプローチのコンプライアンス、監査、リスクの影響についても見てみましょう。

1.オンボーディング/登録

1a.汎用デバイス上のデバイス固定パスキーを使用したオンボーディング

オンボーディング　サードパーティパスキープロバイダ；汎用デバイス上のデバイス固定パスキー

1.

従業員はPINまたは生体認証を使用してモバイルデバイスにサインインします

2.

従業員は、オーセンティケータアプリをパスキープロバイダとしてインストールし、設定します

3.

従業員は、フィッシング可能なシークレットコードでサインインします

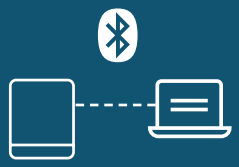
ここが欠陥ポイント！フィッシング耐性が破られる

4.

従業員は手順を完了し、アプリで管理されるパスキーを登録します。パスキーを使用して、同じモバイルデバイス上のアプリにサインインできます。

5.

他のワークステーション上でパスキーを使用するには、従業員はカメラでQRコードをスキャンし、Bluetoothでスマホを接続し、サインイン手順を完了する必要があります。オプションで電話機をワークステーションにリンクします。*



6.

従業員は、モバイルデバイス上のパスキーを使用して、他のデバイスにサインインできるようになりました。

7.

従業員は、デバイス固定型パスキーをワークステーションで直接登録して、サインインを効率化できます。*

*デバイスとユースケースでサポートされている場合

図1： スマートフォンなどの汎用デバイスに常駐するデバイス固定パスキーを使用してオンボーディングする新しい従業員のある日の行動

オンボーディング/登録

1a.汎用デバイス上のデバイス固定型パスキーを使用したオンボーディング

メリット

追加のハードウェアを購入または導入する必要がない

組織の利点は、ユーザーにハードウェアを導入する必要がないことです。組織は、個人のエンドユーザーデバイスに依存できます。または、すでにモバイルデバイスをユーザーに渡している場合は、そのデバイス1つで十分な場合もあります。

課題

低セキュリティなセットアップ

ユーザーがオーセンティケータアプリをインストールして設定した後、フィッシング可能なシークレットを使用してアプリにサインインします。これは、汎用デバイスのデバイス紐付け型パスキーを使用したパスキーの登録が、最初からセキュリティが低いことを意味します。悪意のある攻撃者は、ユーザーを騙してフィッシング可能なシークレットを共有させたり、ユーザーを騙して偽のまたは非準拠のパスキーアプリをインストールさせたりして、攻撃者にユーザーの認証情報へのアクセス権を与え、アカウントの乗っ取りを可能にすることもあります。

企業のセキュリティのために個人デバイスを使用することへのユーザーの抵抗

前述のように、スマートフォンなどの汎用デバイスでデバイス固定パスキーを使用する組織にとっての主な利点は、ユーザーに追加のハードウェアを導入する必要がなくなり、個人のモバイルデバイスでセキュリティギャップを解決できることですが、これにより、個人のデバイスにソフトウェアをインストールする必要がある従業員から反対意見が出たり、従業員に自分のデバイスの使用を要求するために、組織が経費を負担する要因になる可能性があります。また、Android14およびiOS17が一部のエンドユーザーデバイスでサポートされていない場合は、その従業員のために何をすべきかを組織が理解することが課題になります。

直感的ではないユーザー体験

ユーザーオンボーディングの体験が、すべてのプラットフォームとデバイスの間で標準化されていないため、ユーザーの混乱や生産性の低下につながります。これは、汎用デバイス上のデバイス固定パスキーを導入して成功させるために、企業が詳細なユーザートレーニングに投資する必要があることを意味します。特にBYODプログラムを使用している企業の場合、ユーザーはアプリのインストールと設定を行う必要が生じることが多く、そのために経費が増加し、劣悪なユーザー体験となります。

複数のデバイス/登録が必要

復旧と理想的なユーザー体験をサポートするには、システムへのアクセスが必要なすべてのデバイスで登録が必要です。また、アカウントの復旧のために別のパスキーを登録できる2台目のモバイルデバイスまたはデスクトップが必要になります。これは、企業やユーザーにとってストレスとなり、コストがかかる可能性があります。

企業ユースケースの範囲が限定される

これらのパスキーがモバイルフォンなどの日常的なデバイスに常駐するため、オーセンティケータを使用できる場所には制限があります。したがって、共有ワークステーションや共有デスクトップのシナリオ、BYOD、高セキュリティ、モバイル制限、および一部のオフラインのシナリオ、および古いデバイスやプラットフォームが関係している場合でも、これらのタイプのデバイス固定パスキーは、すべての企業のユースケースをカバーするほどには機能しない場合があります。

1.オンボーディング/登録

1b. セキュリティ専用のオーセンティケータ上のデバイス固定パスキーを使用したオンボーディング

ハードウェア紐付け型パスキーを使用してユーザーをオンボーディングするには、3つの方法があります。

- マネージャーまたは管理者が、エンドユーザーに代わってFIDO2セキュリティキーを登録します
- 従業員には、工場でプロビジョニングされた事前登録済みのセキュリティキーがメールボックスに直接送付されます
- エンドユーザーは、企業が指定したパスワードまたはフィッシング可能なコードを使用してサインインし、セルフサービスを実行します

ここでは、セキュリティキー（YubiKeyなど）に常駐しているデバイス固定パスキーを使用して、耐フィッシングMFAとパスワードレスに安全かつシームレスにユーザーをオンボーディングできる、最初の2つのオプションについて説明します。

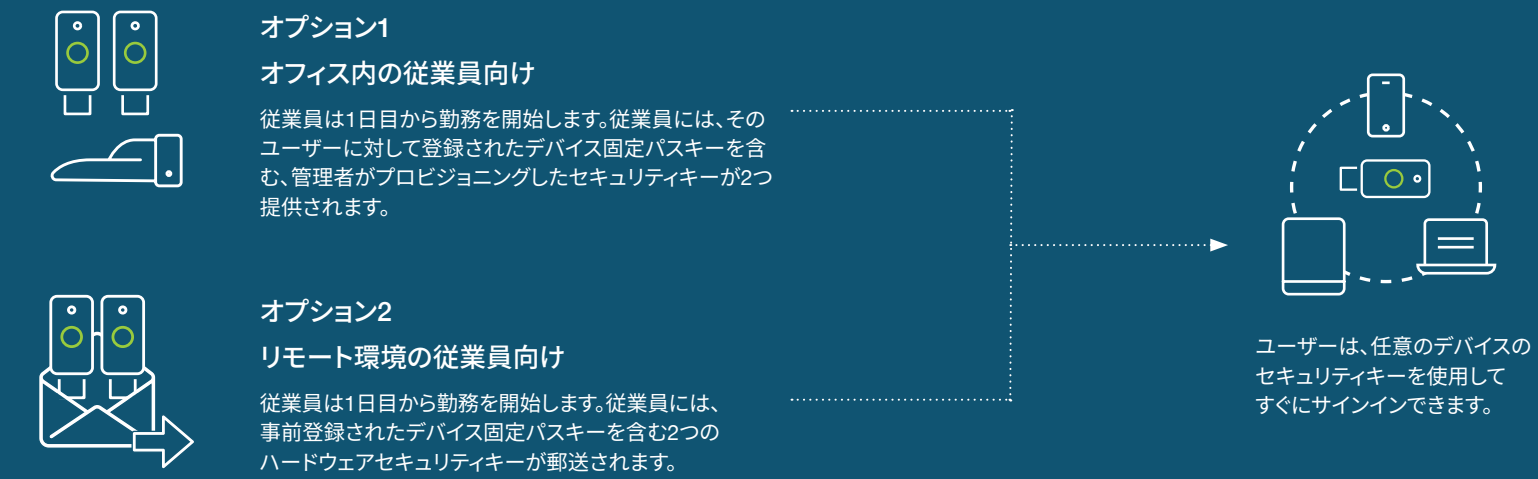


図2：YubiKeyを使用してオンボーディングする新しい従業員のある日の行動

オンボーディング/登録

1b.セキュリティ専用のオーセンティケータ上の
デバイス固定パスキーを使用したオンボーディング

メリット

耐フィッシングMFA

ユーザーまたはプロセスでは、パスキーを登録するためにフィッシング可能なシークレットを処理する必要はありません。

一貫したユーザー体験

YubiKeyにデバイス固定パスキーを常駐させている組織にとってのメリットは、デバイスやプラットフォーム間で一貫したユーザー体験を提供することであり、最高保証のセキュリティが、強力な認証セキュリティのポータブルな形態でユーザーと一緒に移動し、1日中でユーザーにフィッシング耐性を提供します。

最高保証のセキュリティ（AAL3）

YubiKeyは、高いセキュリティであるAuthenticator Assurance Level 3（AAL3）要件に準拠しており、最も厳しいコンプライアンス要件を満たしています。これにより、企業は強力なセキュリティを手に入れ、安心してビジネスを加速することができます。

課題

独立したデバイスの購入および導入

企業にとっての主な課題は、独立したデバイスを購入および導入し、ユーザーに届ける必要があることです。この送付作業は、企業が物流と流通を考慮する必要があるため、煩雑だと感じられます。Yubicoは、物流と流通のニーズをサポートするエンタープライズデリバリーサービスを提供しています。また、各地域の代理店パートナーと連携することもできます。

2.認証情報/アカウントの復旧

2a.汎用デバイス上のデバイス固定パスキーを使用した認証情報の復旧

認証情報の復旧 サードパーティパスキープロバイダ：汎用デバイス上のデバイス固定パスキー

1.

現場の従業員が、登録済みパスキーが含まれたモバイルデバイスを紛失した

2.

モバイルデバイスの紛失/盗難について、対面または電話でヘルプデスクに報告します

3.

対面またはリモートでの本人確認が開始されます。

ここが欠陥ポイント！ユーザーまたはユーザーの認証情報のスプーフィング

4.

本人確認が正常に完了しました。

5.

ヘルプデスクは、紛失/盗難にあったデバイスをユーザーのアカウントから削除します。

6.

新しいモバイルデバイスがユーザーに届けられている間に、ヘルプデスクが一時的なアクセス用にフィッシング可能なシークレットを発行します。

ここが欠陥ポイント！フィッシング耐性が破られる

7.

交換用のモバイルデバイスが利用できない間は、フィッシング可能なシークレットを使用してアクセスを維持し、ユーザーが生産性を維持できるようにします。

ここが欠陥ポイント！フィッシング耐性が破られる

8.

新しいデバイスが利用可能になると、ユーザーはフィッシング可能なシークレットを使用してサインインし、新しいモバイルデバイスに新しいパスキーを登録できます。

ここが欠陥ポイント！フィッシング耐性が破られる

9a.

ユーザーがパスキーが存在するモバイルデバイス上のアプリにのみログインする必要がある場合は、追加の手順は必要ありません。

9b.

ユーザーがモバイルデバイス上のパスキーを使用して別のワークステーションのアプリにログインする必要がある場合、ユーザーはQRコードをスキャンし、Bluetoothを接続してモバイルデバイスを接続してデバイスをリンクする必要があります。*

図3： モバイルデバイスが紛失した場合にアカウントを復旧しようとしている現場の従業員のある日の行動

認証情報/アカウントの復旧

2a.汎用デバイス上のデバイス固定パスキーを使用した認証情報の復旧

メリット

ユーザーのデバイス数が少なくなる：持ち運ぶものが1つ減る

すでにスマホを所有しているユーザーは、同じデバイスを生産性と認証に使用できます。

ハードウェアセキュリティキーの追加コストは不要

組織は、最高保証のハードウェアセキュリティキーを購入するための追加の支出を回避できる可能性があります。

課題

複数のデバイスが必要

ユーザーがパスキーをサポートするデバイスを1台しか持っていない場合、ユーザーのロックアウト/アカウントの復旧にはコストがかかり、リスクが高くなり、劣悪な体験になる可能性があります。このような落とし穴を回避するには、複数のデバイスにパスキーを登録する必要があります。

劣悪なユーザー体験

モバイルデバイスの紛失または盗難にあった場合、そのパスキーを使用してアクセスしていたすべてのワークステーションは、QRコードをスキャンし、モバイルデバイスをBluetoothでワークステーションに接続することで再リンクする必要があります。復旧後にクロスデバイスアクセスを再確立するには、複数のデバイスと手順が必要になる場合があります。

監視と管理のための追加コスト

汎用デバイスのデバイス固定パスキーには、通常、モバイルデバイスのセキュリティポスチャを管理および監視するための追加のソフトウェアと管理者が必要となり、コストが膨らむ可能性があります。

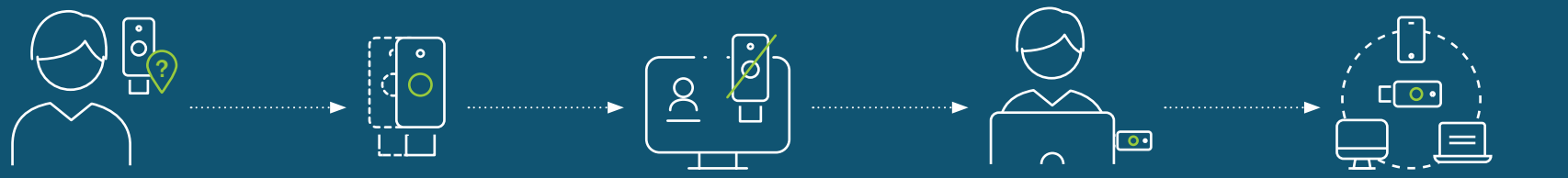
高い復旧頻度

混雑した公共の場所でデバイスを使用すると、スマホが盗まれたり、置き忘れたり、故障したり、壊れたりする可能性が高くなります。YubiKeyに常駐するパスキーなどのデバイス固定パスキーでは、この可能性は、はるかに低くなります。また、スマートフォンなどの汎用デバイスにあるデバイス固定パスキーが誤って削除される可能性があることに注意してください。一方、YubiKey上のパスキーを誤って削除することはありません。最後に、デバイスのアップグレードサイクルを考慮することが重要です。アップグレード中に、オーセンティケータアプリとパスキーが、ユーザーのアップグレードされたデバイスに正しく移行されない可能性があります。さらに、OSのアップデート、ファームウェアのアップデート、およびアプリのアップデートによってパスキーのフローが中断され、計画どおりに動作しなくなる可能性があり、潜在的な脆弱性が定期的に発生するため、組織はデバイスの管理とパッチ適用に絶えず取り組む必要があります。

2.認証情報/アカウントの復旧

2b.セキュリティ専用のオーセンティケータ上のデバイス固定パスキーを使用した認証情報の復旧

認証情報の復旧**セキュリティキー**：セキュリティのために構築されたオーセンティケータ上のデバイス固定パスキー



1. セキュリティキーの紛失または盗難。ユーザーはセルフサービスでこれを解決できます。
2. ユーザーはバックアップセキュリティキーを取得します。
3. ユーザーはセキュリティ登録ポータルにサインインし、紛失したセキュリティキーをアカウントから削除します。
4. ユーザーは、交換用キーを待つ間、バックアップキーを使用したフィッシング耐性のある認証によりアクセスを維持し、生産性を維持します。
5. 交換用キーをアカウントに追加したら、ユーザーがログインする必要があるすべてのデバイスに特別なプロセスは必要ありません。

図4：YubiKeyを使用してアカウントへのアクセスを復旧しようとしている従業員のある日の行動

認証情報/アカウントの復旧

2b.セキュリティ専用のオーセンティケータ上の
デバイス固定パスキーを使用した認証情報の復旧

メリット

法外なコストはかからない

2台のモバイルデバイスを所有する場合と比較して、YubiKeyなどのバックアップセキュリティキーを所有する方が、コストが大幅に削減されます。また、バックアップのYubiKeyを持つことで、より迅速でシンプルなセルフサービス復旧が可能になります。

フィッシング耐性が常時有効

1つのセキュリティキー（デバイス固定パスキーを含む）が紛失しても、通常のワークフローが中断されることはなく、認証強度が低下することもありません。

課題

バックアップキーが必要

ユーザーがセキュリティキーを紛失した場合、アカウントへのアクセスを復旧するためのいくつかの手順が必要になります。したがって、各ユーザーは、アカウントへのアクセスを維持するための2番目のセキュリティーキーを保持し、新しいバックアップ方法を追加するためのフィッシング耐性のある方法を提供することが推奨されます。

YubiKeyは、他のデバイス固定パスキーの安全性を高める

次のように、二者択一ではありません。サードパーティパスキープロバイダをリスクの低いアプリ/ユーザーに使用したり、復旧シナリオで一時的に使用したりするなどの主なシナリオでは、ハイブリッドアプローチが企業に最適な方法となる場合があります。また、プロビジョニングされ、エンドユーザーに配布される、事前に登録されたYubiKeyを使用すると、サードパーティパスキープロバイダ内で別のタイプのデバイス固定パスキーのセットアップを開始するために必要な強力な紐付けが作成されることも考慮してください。これにより、セキュリティと使いやすさの水準が大幅に向上し、組織が基盤とすることができる堅牢な認証情報ライフサイクル戦略が作成されます。

その他の企業の考慮事項

コンプライアンス、監査、リスク

汎用デバイス上のデバイス固定パスキーを使用したコンプライアンスと監査

課題

限定されたアテステーション機能。パスキーを保護しているデバイスやハードウェアを特定するのが困難です

スマートフォン、ラップトップ、タブレットなどの汎用デバイス中のデバイス固定パスキーは、AAL2までしか満たしていません

最も厳格なコンプライアンス要件および認定要件を満たしていません

セキュリティ専用のオーセンティケータ上のデバイス固定パスキーを使用したコンプライアンスと監査

メリット

ハードウェアオーセンティケータのアテステーションは、既知の特性を持つ既知の信頼できるハードウェアに、パスキーが安全に保存されるという最も高い信頼を提供します

YubiKey中のデバイス固定パスキーは、AAL3を満たす唯一のキーです

最も厳格なコンプライアンス要件および認定要件を満たしています

YubiKeyは、最高のセキュリティ保証を求める米国連邦政府の要件を満たしています

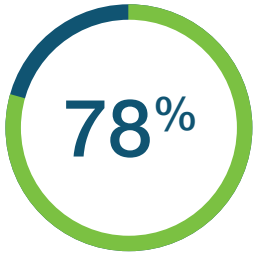
- YubiKeyは、モバイルデバイスが禁止されている保安区域で使用できます
- YubiKeyは、政府機関が、汎用デバイス上のデバイス固定パスキーと互換性のないレガシーシステムまたは特注システムを使用している場合に役立ちます。

リスクエクスポージャとコストエクスポージャ

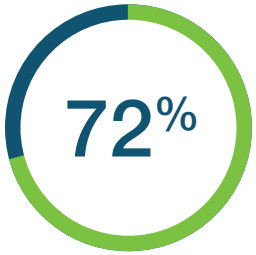
一般的に、ユーザーはモバイルデバイスをさまざまなアクティビティに使用するため、これらのデバイスの紛失、盗難、または侵害のリスクが高くなります。汎用モバイルデバイスに常駐するパスキーは、ハードウェアセキュリティキーなどのセキュリティ専用のオーセンティケータに常駐するパスキーと比較して、侵害されるリスクが高くなります。スマートフォンの交換は、セキュリティキーを交換するよりもはるかにコストがかかります。

セキュリティ用の汎用デバイス

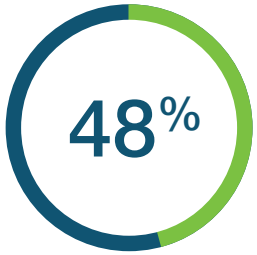
危険なユーザー



個人的なアクティビティに仕事用デバイスを使用しているユーザー。



個人用デバイスを仕事に使用しているユーザー。



友人や家族にデバイスの使用を許可しているユーザー。

出典：Proofpoint 2023-State-of-Phish-Report

YubiKey：他のすべてのパスキープロバイダのセキュリティの水準を上げる

企業がユーザーの日常生活からパスワードを排除しようとしている中で、YubiKeyはセキュリティを強化するためのシンプルで安全、ポータブルな方法を提供できます。ユーザーはYubiKeyを使用してワークステーションを認証し、パスキープロバイダ（プラットフォームとサードパーティの両方）をロック解除して、パスキーアプリケーションのセキュリティの水準を上げることができます。

YubiKeyに常駐するデバイス固定パスキーは、組み込みのFIDOアテステーションの基準に基づいて秘密鍵がどのように管理されるかについて、最高レベルの保証を提供します。YubiKeyは、専用のセキュリティハードウェアモジュール内に秘密鍵を格納して保護されていることを保証します。他の形態のデバイス固定パスキーは、秘密鍵のセキュリティと制御に関する情報を提供するために、信頼性のより低いアプローチに頼る必要があります。可視化された制御がないと、コンプライアンス規制や必要なセキュリティ基準を満たすという企業のニーズを満たせない可能性があります。

まとめ

企業におけるパスキーの考慮事項

パスキーによりFIDOに対応した世界が実現されますが、ユーザーアイデンティティの厳密な管理を必要とする企業では、スマートフォン、ラップトップ、タブレットなどの汎用デバイスに常駐しているデバイス固定パスキーでは、組織のリスクを軽減することはできないかも知れません。セキュリティキーに常駐するデバイス固定パスキーは、最高のセキュリティ保証を提供し、最も強力なセキュリティ、最もシンプルなユーザーオンボーディング、認証情報/アカウントの復旧をデバイスやプラットフォーム全体で実現し、業界全体の最も厳格な要件に準拠するために必要な、信頼できる認証情報ライフサイクル管理とアテステーション機能を企業に提供します。

- フィッシング耐性のあるユーザーを作るために、認証および認証情報管理のすべての領域をサポートできる、フィッシング耐性のある認証方式を探しましょう。オンボーディングと復旧のフローは、フィッシング耐性が破られる一般的な領域です。このフローは魅力的な攻撃ベクトルの対象となります。
- 多種多様なデバイスでは、アテステーションが不十分であったり存在しない場合があります。サービス/リライングパーティまたは企業は、どのタイプのデバイスが使用されたか、オーセンティケータに信頼をおくことができるか、パスキーがどのように格納されているかを知ることもできません。企業は、ユーザーが使用するパスキーを信頼できることが重要です。
- 最新のFIDOセキュリティキーに存在するようなパスキー認証情報は、スマートフォンのパスキーよりも高い保証レベルを提供します。スマートフォンのパスキーは低いセキュリティパスキーであり、AAL2までしか保証が提供されません。一方、セキュリティキーに存在するパスキーでは、コンプライアンスを確保するために重要なAAL3保証（最高のオーセンティケータ保証であるレベル3）が提供されます。

お問い合わせ
yubi.co/contact-ja

詳細情報
yubi.co/passkey

yubico

Yubicoについて Yubico（Nasdaq First North Growth Market Stockholm：YUBICO）は、YubiKeyを開発し、耐フィッシング多要素認証（MFA）の絶対的な基準を提供しています。YubiKeyは、アカウントの乗っ取りを未然に防ぎ、誰でも安全なログインを簡単に利用できるようにします。2007年の設立以来、コンピュータ、モバイルデバイス、サーバー、ブラウザ、インターネットアカウントへのセキュアなアクセスに関するグローバル・スタンダードの確立をリードしてきました。Yubicoは、FIDO2、WebAuthn、FIDO Universal 2nd Factor（U2F）オープン認証標準の作成者かつ中核的な担い手であり、160ヵ国を超えるお客様に最新のハードウェアベースのパスキー認証セキュリティを大規模に提供するパイオニアでもあります。

Yubicoのソリューションは、最も安全な形のパスキー技術を使用したパスワードレスログインを可能にします。YubiKeyは、数百の消費者向け/企業向けアプリケーションやサービスですぐに使用することができ、強固なセキュリティを迅速かつ簡単に提供します。

Yubicoでは、インターネットをすべての人にとってより安全なものにするというミッションの一環として、社会貢献活動であるSecure it Forwardを通じて、危険にさらされる人々を支援する団体にYubiKeyを寄贈しています。本社は、ストックホルムとカリフォルニア州サンタクララにあります。詳細については、www.yubico.comをご覧ください。