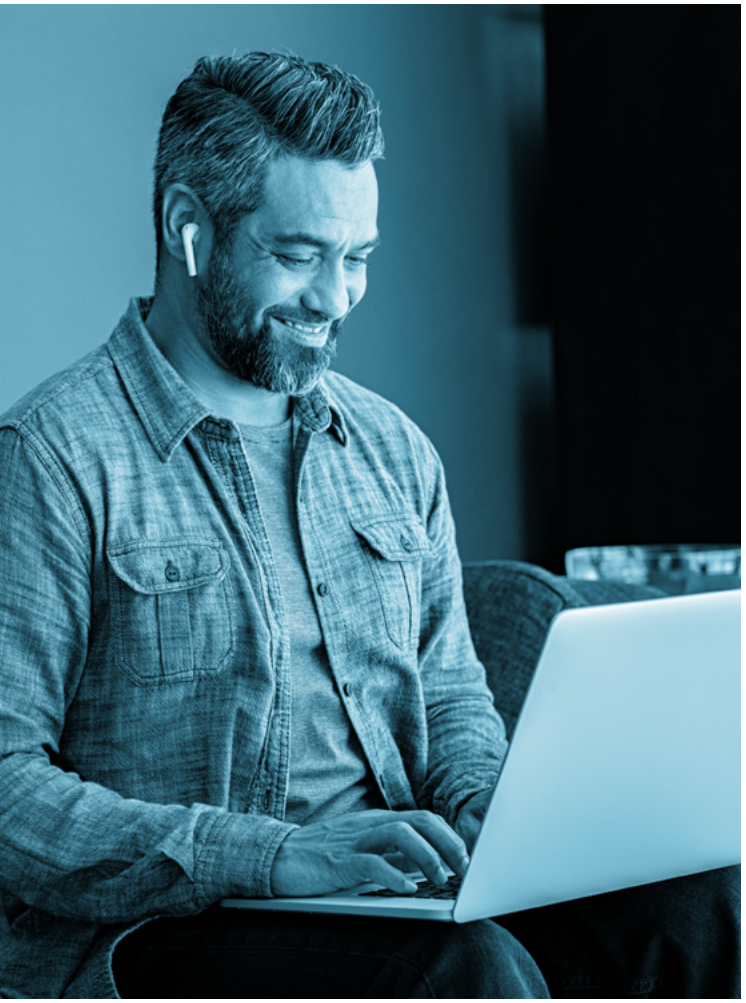
yubico

エンタープライズで同期型パスキーの導入を検討していますか

同期型パスキーのよくある落とし穴の回避



さまざまなパスキーの実装

パスキーは、スマートフォン、タブレット、ラップトップ、またはFIDOハードウェアセキュリティキーのようなセキュリティのために設計された認証機の中にある、パスワードレス対応のFIDOクレデンシャルです。

パスキーはパスワードよりも安全で、パスワードレス認証に移行できるため、セキュリティと効率を向上させることができます。パスキーの基礎について詳しくは、ここをクリックしてください。

パスキーには、同期型と専用ハードウェア型の2種類があります。同期型パスキーはコピー可能なクレデンシャルであり、スマートフォン、ラップトップ、タブレットなど、ユーザーアカウントに紐付けられた各種のデバイス間を移動できます。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。

職場で同期型パスキーが脆弱性になるような、よくあるシナリオをいくつかご紹介します。

1. **リモートワークのリスク：**従業員が在宅勤務の場合、同期型パスキーは簡単にコピーできるため、攻撃者のデバイスが従業員のクレデンシャルとして使用されるセキュリティリスクが発生します
2. **サプライチェーンの脆弱性：**従業員が複数のアカウントおよびデバイス間で同期型パスキーのクレデンシャルを共有すると、内部脅威が発生し、サプライチェーンの完全性が破綻します
3. **コンプライアンスとサポートの複雑さ：**パスキーエコシステムが無節操に拡大し、企業が複数のパスキープロバイダを利用するようになると、コンプライアンスに必要なクレデンシャルを追跡して信頼することが困難になり、ITヘルプデスクの負担とコストも増大します

以下の各シナリオをお読みになり、なぜ同期型パスキーが企業のリスクとコストを高める原因となり得るのかをご確認ください。

同期型パスキーと専用ハードウェア型パスキー

同期型パスキー

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。

専用ハードウェア型パスキー

日常的なデバイスとは別の USB キーやその他のハードウェア上に存在し、安全性保証が高くなります。

シナリオ1

リモートワークのリスク

パスキーは、1つのiCloudアカウントに登録されているすべての所有デバイス間で同期されます。ここでは、テクノロジー企業のフルタイムのリモートワーカーであるJimにとって、この点がどのように危険であったかについて説明します。Jimは自宅で働いています。家族は全員で6台のデバイスを使って、同じiCloudアカウントを利用しています。攻撃者が同期型パスキーをどのように悪用できるか見てみましょう。

1. Jimは、携帯電話のパスキーを使用して仕事用アカウントにログオンしています。彼は自分の個人用iCloudアカウントに携帯電話を追加しました。このアカウントは、家族が使用している他のデバイスとも共有されています。

2. Jimの息子、Benは、よくプレイしているアプリベースのゲームに関する良さそうなリンクを含むメールを受信しました。Benはリンクをクリックしました。

3. Benは、騙されてiCloudのユーザー名とパスワードを入力してしまいました。これは攻撃者によって傍受されてしまいます。Benは、新しいデバイスを追加するリクエストを受け入れ、攻撃者が自分のデバイスを家族のiCloudアカウントに登録できるように許可しました。

4. Jimの仕事用の携帯電話はすでにクラウドに同期されているため、仕事用パスキーはiCloudアカウント上のすべてのデバイスと自動的に同期されます。これには攻撃者のデバイスも含まれてしまいます。

5. 攻撃者がJimの仕事用クレデンシャルを取得すれば、Jimとして仕事用サイトにログオンし、さらに権限の高い他のクレデンシャルを探すことができます。

ご存じでしたか？

89%の組織が、過去1年間にフィッシング攻撃を受けています。

HYPR, 2022 State of Passwordless Security Report

シナリオ2

サプライチェーンの脆弱性

同期型パスキーは、iPhoneのAirDrop機能を使用すれば、ユーザーの直接の制御下にない他のデバイスとも簡単に共有できます。また、パスキーの共有可能性が便利なこともありますが、従業員がクレデンシャルを不用意に共有すると、内部脅威などの重大なセキュリティギャップが生じる可能性があります。これにより、サプライチェーン全体のリスクが高まり、信頼が失われます。Kiraの体験談をご覧ください

1. 複雑なサプライチェーンを持つ大規模小売業者は、HVACシステム監視会社（外部ベンダー）が重要なシステムにログインして、リアルタイムの状態を確認することを許可しています。

2. Kiraはベンダーの新入社員です。彼女はまだ小売業者でのアカウントのセットアップを完了させていませんが、次のシフトで作業する必要があるため、BluetoothでAirDropを使用して、同僚にパスキーを共有させてもらいました。

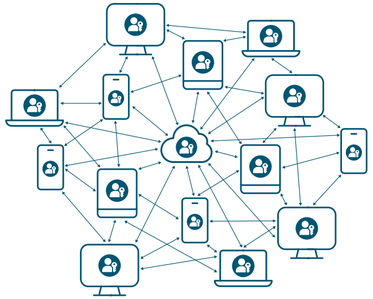
3. 数ヵ月後、Kiraは退職しましたが、同僚のパスキーがまだデバイスに残っています。Kiraのデバイスで共有されている同僚のパスキーを自動的に破棄する方法がないためです。

   組織はKiraのデバイスからパスキーを強制的に削除することはできません。

4. HVACシステムの設定調整に失敗すると、重大な停止が突然発生します。

   パスキーは少なくとも2つの場所に存在します。監査ログにはパスキーのクレデンシャルが使用された記録が残っていますが、ログインしたのがKiraなのか、同僚なのかは判別できません。

5. 監査ログの信頼性が低下し、パスキークレデンシャルがどこで保存および管理されているのかベンダーがコントロールできなくなると、法的リスクが高まります。



シナリオ3

コンプライアンスとサポートの複雑さ

パスキーは、さまざまなベンダーや製品に実装されています。ユーザーがその中からどれか1つだけを使用する必要はありません。つまり、企業が直面しているリスクは、ユーザーがさまざまなプラットフォームやパスワードマネージャーで数多くのパスワードを所有しているということです。どのパスキーがどこに保管されているのか、企業はどのように追跡するのでしょうか。また、企業が可視化できない場合、パスキー関連のサポート問題解決が必要なユーザーをどのように支援するのでしょうか?

1. FrankはIT部門から、コーポレートログイン時のセキュリティを向上させる手段としてパスキーを登録するよう求められています。

2. Frankは、3つの異なるパスキーサービスプロバイダ（Apple、Google、パスワードマネージャー）を使用することにしました。同期型パスキーのいずれか1つを使用してコーポレートシステムにログインできるようにした方が便利だと思ったからです。

3. 数ヵ月後、データ漏えいインシデントが公表され、Frankが利用していたパスキーサービスプロバイダの1社にパスキー管理システムのセキュリティインシデントが発生していたことが明るみに出ました。

4. エコシステムによる過度な漏えいのため、FrankのIDは脆弱で、攻撃者が悪用しやすくなっています。Frankは、プロバイダ3社の同期型パスキーをすべて削除し、コーポレートログイン用のパスキーを再登録する必要があります。

5. コーポレートヘルプデスクは、さまざまなパスキーサービスプロバイダについて詳しくないため、Frankのような従業員のアクセス上の問題解決の支援に苦労しています。企業は、同期型パスキーを許可するサポートコストを考慮する必要があります。

組織に最適なパスキーはどれか?

重要な5つのポイント

パスキーがパスワードより優れているのは、最新のFIDOプロトコルに基づいており、フィッシングに対する防御力が高いためです。

ここでは、同期型パスキーについて覚えておくべき5つのポイントと、専用ハードウェア型パスキーの方が企業のニーズに適した安全でコンプライアンスに適合するオプションである理由について説明します。すべてのパスキーは同等に作成されていないため、企業は同期型パスキーの落とし穴を回避する必要があります。

- パスキーを使用すると、FIDO対応の環境を実現できますが、ユーザーIDの厳密なコントロールが必要な企業の場合、実際は同期型パスキーが組織のリスクを高める可能性があります。
- 同期型パスキーは移動できるため、実際の二要素というよりも、「サインイン手段」メカニズムと厳密には表現します。
- 同期型パスキーを使用すると、企業はセキュリティ専業ベンダーではないサードパーティーを信頼することになるかもしれません。
- 同期型パスキーは、ユーザーがクレデンシャルを簡単に共有できるようになり、共有設定有効になっている場合はそれをデフォルトにしてしまう可能性があります。
- 最新のポータブルなFIDOセキュリティキーに採用されている専用ハードウェア型パスキーは、高度な保護を提供し、企業のコンプライアンスニーズをより良く満たします。

お問い合わせ
yubi.co/contact-ja

詳細情報
yubi.co/ja

適切なパスキーソリューションの選び方

サービスプロバイダ

コンシューマー

ほとんどのコンシューマーは、パスワードよりも同期型パスキーを選択する方が適切なため、自分のデバイスで同期型パスキーを使用できます。

リスクの高いコンシューマー

高リスクのユーザー（ジャーナリストなど）は、ハードウェアセキュリティキーのパスキーなど、高い安全性保証を実現するパスキーの方が大きなメリットを得られる可能性があります。

企業

現場勤務の従業員

これらの従業員の多くは、職場で個人用の携帯電話やラップトップを使用できないため、それらのデバイスに依存しないパスキーソリューションが必要です

オフィス勤務の従業員

これらの従業員は、パスキーのクレデンシャルがコピーできないよう、ハードウェア認証を備えたセキュリティキーが必要です。

特権ユーザー

最もリスクの高いターゲットとなるユーザーは、パスキーのクレデンシャルがどこに保存されているかを把握するため、ハードウェア認証を備えたセキュリティキーが必要です。

yubico

Yubico（Nasdaq First North Growth Market Stockholm: YUBICO）は、YubiKeyを開発し、最高水準の耐フィッシング多要素認証（MFA）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。Yubicoの詳細については、yubi.co/jaをご覧ください。