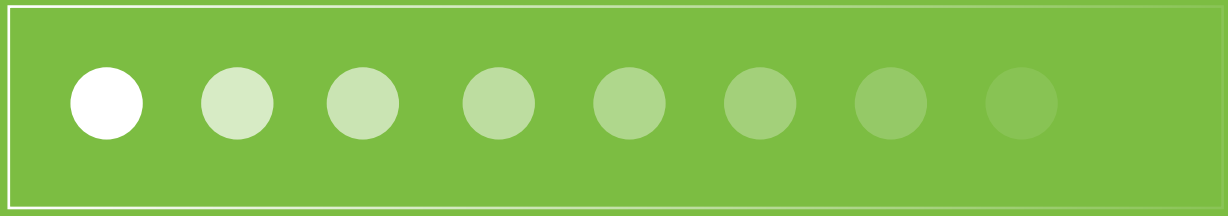
yubico

YUBICOのホワイトペーパー
2018年11月

FIDO2とWebAuthnで パスワードレス を実現



目次

はじめに

ユーザーが複数のパスワードを設定、リセットしたり、忘れて復元したりする必要がない世界を想像してみてください。パスワードは企業のセキュリティを弱体化させる主な原因であり、顧客体験や社内プロセスを合理化する際に主な障壁になるのもパスワードです。パスワードレス認証が登場したことで、世界は変わりつつあります。

組織がパスワードに起因するセキュリティの問題を解決する機会を提供してくれるのが、新しいFIDO2/WebAuthn認証規格です。FIDO2とは、Yubico、Microsoft社、その他のFIDOアライアンスのメンバーが共同で策定したオープンな規格であり、既存の2段階認証をサポートするだけでなく、パスワードレスの単一要素による認証やマルチファクターの強固な認証も柔軟にユーザーが利用できるようにすることで、ユーザーの選択肢を拡げるものです。

パスワードレス認証は、医療、製造、小売のようなあらゆる業界の企業、そして社員や協力業者、サプライヤーのセキュリティやユーザーエクスペリエンスを一変する機会をもたらします。これによりユーザー登録を簡略化できるだけでなく、パスワードのリセット作業がITサポートコストの大半を占めている現在において、パスワードレス・ログインを使用することで、ユーザーのパスワードを設定・リセットするためにITコールセンターのスタッフが費やしている多くの時間や労力を大幅に削減することができるでしょう。

パスワードレス・ログインで、顧客体験や業務プロセスをどのように合理化できるでしょうか？ パスワードが不要になったら、どのような新製品やサービスを実現できるでしょうか？ これらは、将来を見据えた企業やITの最前線にいる人たちが今考えるべきことです。

このホワイトペーパーでは、パスワードレス認証が生まれた背景、企業で導入する際の検討事項などをご紹介します。

データ流出の63%に脆弱なパスワードが関わっています[4]。

Verizon Data Breach
Investigations Breach

パスワードの時間とコスト

今日の企業は、クラウドやモバイルのテクノロジーを活用してより優れた製品やサービスを素早く効率よく提供する方法を模索しています。しかし、顧客体験や業務プロセスを合理化するという大きな計画に乗り出した企業は、すぐにセキュリティの課題に直面します。

セキュリティ技術・要件によって企業を保護することができますが、そのような要件があるとユーザー体験が悪化するおそれがあります。このようなもどかしいセキュリティ要件の一つとして、誰もが真っ先に思いつくのがパスワードです。

パスワードは1950年代以後、企業と消費者の両方に浸透していきました。そして、Facebookのようなソーシャルネットワーク、チェイスやMacy'sのような銀行・小売店からSalesforceやQuickBooks Onlineなどのビジネス・アプリケーションに至るまで、ほぼすべてのデジタル・サービスでパスワードが求められるようになっています。

平均的な米国な消費者は14個を超えるパスワードをなんとか管理しつつウェブサイトやサービス[1]でそれらを利用しており、企業のユーザーはさらに多く、191個ものパスワードを暗記しなければならないと推定[2]されています。また、IBM社の調査によると、労働力の割合を増やしているミレニアム世代は、このような認証情報を暗記する忍耐力が比較的乏しいということがわかっています。そのような世代は8つまでしかパスワードを記憶せず、パスワードを使い回し、セキュリティよりも利便性を優先する傾向があります[3]。

データ流出につながるパスワード疲れ

サービス毎に新しいパスワードを作成したり、セキュリティポリシーに従って数か月毎にパスワードを変更したりしなければならないため、ユーザーの負担がさらに大きくなってきています。多くのユーザーは暗記する分量を減らそうとして推定しやすい簡単なパスワードに頼るようになったり、複数のサイトで同じパスワードを使いまわし、いずれかのサービスでセキュリティ侵害が生じた場合に被害が他にも広がるような状態を作ってしまったりしています。

2017年度のVerizon Data Breach調査報告書(DBIR)によると、データ流出の約63%に脆弱なパスワードが関わっています[4]。驚くべきことに、大規模なデータ流出が何年も世間を賑わし続けているのにも関わらず、最も頻繁に使用されているパスワードは現在も変わらず「123456」と「password」です[5]。

パスワードは忘れるため、サポートコストの増加につながる

パスワードを忘れたユーザーは結局、ヘルプデスクやサポートセンターに電話することが多いため、貴重な時間を消費してしまいます。コールセンターの業務のうち、パスワードのリセットに関する問い合わせが占める割合は最大6%であり、大企業の場合は年間500万ドルから2000万ドルのコストがかかります[6]。Gartner社は、このようなパスワードのリセットに関する問い合わせはさらに多く、よりコストがかかっており、ヘルプデスクの電話のうち20%～50%を占めていると推定しています[7]。

2017年のある月にMicrosoft社はユーザーのパスワードを686,000件リセットし、そのために1200万ドル以上のサポート費用をかけています。

Microsoft社は、単一のITサポート費用のうち、パスワードの管理コスト（パスワードの復元、締め出しやパスワードの変更を含む）が最大であると見積もっています。2017年のある月にMicrosoft社はユーザーのパスワードを686,000件リセットし、そのために1200万ドル以上のサポート費用をかけています[8]。

フィッシング攻撃の標的は認証情報の不正入手

攻撃技術は進化し続けており、今も変わらずフィッシングがセキュリティの大きな問題になっています。ユーザーに認証情報の再入力を求める偽りのメールメッセージを使用して、アカウントを乗っ取ることを目的として認証情報を集めることができます。受信者の約30%がフィッシングメールを開き、7%以上のメール受信者が内容を信頼して添付ファイルを開いたりリンク（ログイン用のリンクが多い）をクリックしたりします。大抵のフィッシング攻撃はその後、マルウェアをインストールして被害をさらに増やします[9]。ユーザーが複雑なパスワードを設定している場合でも、ハッカーはフィッシングとユーザーアカウントの不正利用を通じてアクセスを掌握できます。

売り買いされている、盗まれた認証情報のリスト

ハッカーが組織に侵入して認証情報を盗んだ場合、その組織のアカウントだけでなく、消費者が同じユーザー名とパスワードの組み合わせを使用している他の組織のアカウントにもアクセスできるようになります。例えば、2016年にYahoo!のログイン認証情報を10億件盗んだハッカーは、同じメールアドレスとパスワードの組み合わせでアクセスできる他のすべてのアカウントにもアクセスできるようになりました。何十億もの盗まれた認証情報がダークウェブで売り買いされており、サイバー犯罪者がこの盗まれたパスワードを使って機械的にログインを試みています。現在、大手の小売店や銀行のサイトで試行されるログインのうち、実際は10回中9回がボットによる攻撃です[10]。

企業のITが認証でパスワードを使用する限り、どうしてもサポートコストの増加、セキュリティの弱体化、顧客体験の低下は避けられません。パスワードを忘れたり盗まれたりすると顧客体験やブランドのロイヤルティが低下し、収益減につながります。

FIDO2でパスワードの問題を解決

パスワードを求めることなく、つまりパスワードを管理するための運営経費をかけずに、顧客や社員のようなあらゆるユーザーに任意のサービスを高速、快適、かつ安全に提供できるとしたらどうでしょう。パスワードをなんとかして思い出したり、サポートデスクに電話をかけて協力を求めたりすることなく、デスクトップパソコンやモバイルデバイスを使用している顧客、パートナー、社員が必要なコンテンツやサービスに即座にアクセスできるとしたらどうでしょう。即座に、簡単に認証を行えることでどのような新しいサービスを実現できるでしょうか。IT企業が日常的に行っているパスワードの管理やリセットにかかる経費がなくなるとしたらどうでしょう。

FIDO2は、パスワードレス認証の選択肢を提供する新しい認証規格です。

パスワードレス認証のメリット

利便性の向上
パスワードレス認証により、ユーザーはパスワードを記憶・入力する必要がなくなります。

セキュリティの向上
パスワードレス認証により、パスワードの盗難に伴うセキュリティ・リスクや、ログイン画面を標的にしたブルートフォース攻撃がなくなります。

効率改善
パスワードレス認証により、IT部門がパスワードを管理する必要がなくなります。

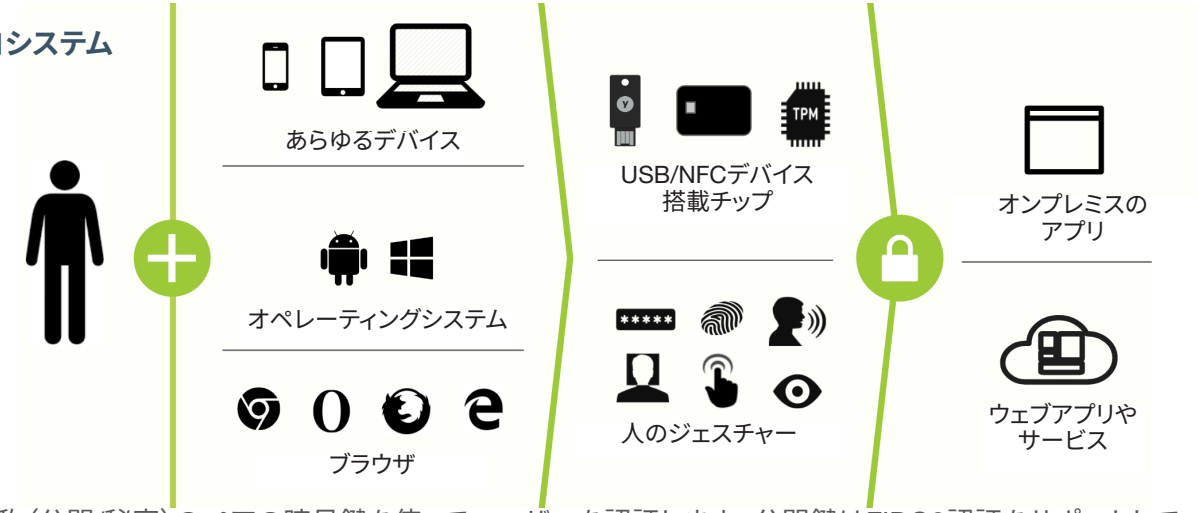
新しいFIDO2/WebAuthnのオープンな認証規格を使って、このようなパスワードレス認証のメリットを実現できる時代になりました。

パスワードレス認証のご紹介

Yubico、Microsoft社、FIDOアライアンスのメンバーがWorld Wide Web Consortium (W3C)と協力して共同策定した新しい認証規格であるFIDO2は、複数のユースケースや体験に対応できるようになっています。

FIDO2は、ウェブAPI (WebAuthn)とClient to Authenticator Protocol (CTAP)という2つの標準化されたコンポーネントで構成されています。連携して機能するこの2つは、パスワードレス・ログインを実現するのに不可欠です。WebAuthnは、ブラウザやウェブ・プラットフォームのインフラストラクチャに統合することで、ウェブ上で安全に認証を行える新しい手段をユーザーに提供する標準化されたウェブAPIを定義しています。CTAPにより、セキュリティキーのような外部のオーセンティケーターがローカルでUSB、NFC、Bluetoothを介してユーザーのPCや携帯電話と認証情報を安全にやり取りできるようになります。

FIDO2のエコシステム



FIDO2は非対称（公開/秘密）のペアの暗号鍵を使ってユーザーを認証します。公開鍵はFIDO2認証をサポートしている任意のサービスやコンピューティング・デバイス上に保存され、秘密鍵はユーザーが保管し、YubiKey 5シリーズやSecurity Key by Yubicoのような物理的なセキュリティキー上で保護されます。認証自体は素早く簡単に行えます。セキュリティキーを挿入あるいはタップするだけで認証チャレンジが完了し、即座にログインできます。

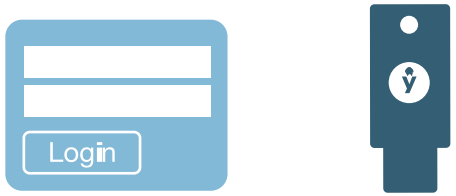
FIDO2を使用するセキュリティキーは独立して使用することも、PINやジェスチャーと組み合わせて使用して強固なパスワードレス認証を提供することもでき、さらに今後もパスワードを伴う2段階認証が認証モードとして継続的にサポートされます。

World Wide Web Consortium (W3C)がFIDO2をサポート

Web Authentication (WebAuthn) APIの仕様により、ブラウザのユーザーがFIDO2仕様に基づく新しい方式を使用してウェブ上で安全に認証を行えるようになります。Microsoft Edge、Google Chrome、MozillaブラウザはすべてWebAuthn　APIの仕様に対応しています。

FIDO2/WebAuthn認証の選択肢

単一認証（パスワードレス）
セキュリティキーを独立して強力な最初の認証要素として使用し、そのデバイスを所持すること以外は求めず、タップアンドゴーによるパスワードレス機能を有効化



2段階認証（パスワード＋）
2段階認証ソリューションでセキュリティキーを2つ目の認証要素として使用

複数認証（パスワードレス＋PINまたは生体認証）
デバイスおよび、PINまたは生体認証を求めるマルチファクター認証でセキュリティキーを使用し、厳格な要件に対応

Windows 10 Redstone 4にアップグレードした世界中の4億を超えるWindows 10のデバイスでFIDO2を利用できます。

パスワードレスにするメリット

利便性の向上

FIDO2パスワードレス・ログインにより、パスワードを求めることなく素早く簡単に認証を行えるようになります。

FIDO2パスワードレス・ログインによりパスワードを求めることなく素早く簡単に認証を行えるようになります。FIDO2を使用すれば、YubiKeyのような単一のハードウェア・オーセンティケーターを使用して、認証情報を共有することなく、職場で使用する業務用アプリケーションやサービス、自宅で使用するソーシャルメディア・ネットワークやその他の消費者向けアプリケーションなど、あらゆるサービスで認証を行うことができます。

その一方、FIDO2は単一のユーザーに対して複数のアイデンティティを提供することもできます。業務用か消費者向けかを問わず、ビルの中でも車内でも、FIDO2をサポートしているアプリケーション、ウェブサイト、サービス、サーバー、デバイスに、一つのYubiKeyを使用してアクセスできます。

パスワードレス認証であれば、飛行機や地下鉄で移動中であり、Wi-Fiや携帯電波を利用できず、ネットワークにアクセスできないためにユーザー認証用のSMSやOTP認証情報を受信できないビジネスマンでもノートパソコンにログインでき、安全に生産的な作業を行うことができます。

FIDO2により、2つ目の認証要素を受信するのに必要なネットワーク・アクセス（携帯あるいはインターネット・ベース）が不要になります。FIDO2により、ITセキュリティが強化されるだけでなく、ユーザーが作業に必要なデバイスにいつでも、どこからでも簡単にアクセスできるようになります。

Windows 10 Redstone 4以降のバージョンを実行しているWindowsのデスクトップやモバイルシステムを含むWindows 10のデバイスがFIDO2をサポートしているため、数十億ものAzure ADアカウントに加え、世界中の4億台以上のデバイス[11]でFIDO2を利用できます。また、2018年11月の時点でMicrosoftアカウントがFIDO2認証に対応したため、次のようなMicrosoft社の多彩なサービスでパスワードレス・ログインを利用できるようになっています：Outlook、Office、Skype、OneDrive、Xbox Live、Bing、MSN、Windows。

オープンな業界標準として策定されたFIDO2は、Microsoft社とWorld Wide Web Consortium (W3C)に広く受け入れられており、Google社とMozilla社のサポートを得ているため、具体的な組織によって採用状況が左右されることはありません。FIDO2により、企業はパスワードの問題を解決するために独自のセキュリティモデルを構築・維持するコストをなくすことができます。どの業界の企業も、業界大手各社に支持されているオープンな認証規格を活用できるようになったのです。

NIST認証規格の条件を満たす

FIDO2は、単一認証要素の暗号トークンあるいはマルチファクターの暗号トークンです。NIST Special Publication 800-63に従うと、マルチファクターの暗号トークンは、その規格で定義されているもののうち最高の保証水準である認証保証水準3に分類されます。そのため、PINと共にFIDO2を使用すれば、NIST SP800-63を遵守しなければならない規制された業界の厳格な認証要件をクリアできます[12]

セキュリティの向上

FIDO2により、ユーザー認証のセキュリティとアクセス管理が大幅に改善されます。

FIDO2により、ユーザー認証のセキュリティとアクセス管理が大幅に改善されます。

パスワードレス・ログインを使用すればパスワードが不要になるため、ユーザーが騙されて意図せずパスワードを流出させてしまうことがなくなります。ユーザーはYubiKeyのようなハードウェア・オーセンティケーターを使用して認証します。大まかに言うと、これは次のようにして機能します。

- オリジンと呼ばれる特定のサービスと認証情報のバインディングを含めて、YubiKeyがFIDO2認証情報（公開/秘密鍵のペア）を作成・管理します。オリジン・バインディングは中間者攻撃を防止します。
- Azure ADのようなサービスが認証チャレンジを求めたら、秘密鍵を使用して署名したレスポンスをネットワーク経由で送信し、それをオンラインサービスが公開鍵を使って検証します。

FIDO2認証情報はYubiKey内のセキュアなチップに保存され、デバイス外に出ることがないため、サイトにログインしているユーザーをハッカーが盗聴できないようになっています。

FIDO2は一元的なストレージとセンシティブな認証情報の管理をなくすことで、アプリケーション、ウェブサイト、サービス、サーバー、デバイスのリスクを軽減します。FIDO2アカウントではパスワードが不要なため、盗難できるパスワードがそもそも存在しません。ウェブサイトや他のサービスは、ユーザーが登録した公開鍵だけを保存するため、秘密の情報（秘密鍵）のセキュリティがハードウェア・オーセンティケーター上で保たれます。従来のパスワードのようにネットワーク経由で送信されることはありません。この公開鍵は秘密鍵が生成した署名を検証できますが、それを独立して使用して他のリソースへのアクセスを開始することはできません。FIDO2の秘密鍵を持つエンドユーザーだけが、サービスへの認証を成功させることができます。より高速、簡単かつ信頼性に優れたエンドユーザーによるログイン・アクセスを実現しつつ、セキュリティを改善できます。

組織固有のセキュリティポリシー、GLBAやHIPAAのような業界の規制や、NIST SP800-63のような政府の規制に従う形で認証権限を付与できます。NIST SP800-63に準拠しているFIDO2は、NIST規格をもとにして作られた他の様々な規制にも対応できます。ユーザーが付箋やメールでパスワードを共有して認証に関する規則を破ることがなくなるため、IT管理者やコンプライアンス担当者は安心できます。各ユーザーには、登録済みのサービスやアプリケーションに認証するために使用する固有のキーが発行されます。

「FIDO2なら、証明書を管理するための複雑なPKI環境が不要になります」

効率改善

FIDO2により、IT部門（サービスデスクやコールセンターを含む）がパスワードを作成、保管、更新、リセットする作業から開放されます。

パスワードレス・ログインによって社員・契約者の採用時の手間がなくなるため、パスワードの発行・管理にかかるサポートコストを削減できます。FIDO2認証であれば、まずはすぐに変更し、その後は指定された間隔で定期的に変更しなければならない仮パスワードを新しい社員や契約者に発行する代わりに、エンドユーザーにFIDO2セキュリティキーを発行し、その際に任意でPINを指定させるだけで済みます。FIDO2認証権限は、社員や契約者の雇用終了時に簡単に無効化することができます。

FIDO2セキュリティキーを使用することで、ユーザーはAzure ADのような一元的なサービスに認証したり、スマートフォンのようなデバイスを新規登録するために本人確認を行ったりすることができます。コンピューティング・デバイスを共有している組織の場合、各ユーザーにパスワードを記憶・入力するよう求めることなく、素早く簡単に認証を行うことができます。NFCを利用できるYubiKeyを挿入あるいはタップするだけで、ユーザーはデバイスをロック解除してアカウントにアクセスできるようになります。

さらにFIDO2なら、証明書を管理するための複雑なPKI環境が不要になります。IT部門は空いた時間や労力を、より戦略的・生産的な作業に費やすことができます。

ユーザー認証に関する企業の要件を満たす

FIDO2は、ユーザー認証に関する次のような重要な要件をすべて満たしています。

- ハッキングや盗聴が不可能な認証情報を提供すること
- フィッシングを阻止できる認証方式を提供すること
- エンドユーザーにパスワードよりも優れた体験を提供すること
- マシンに紐付いた認証・本人確認を提供すること。認証情報をマシン間で転送できないこと
- 様々なセキュリティレベルの認証に対応すること
- 複数の認証情報に対応すること
- タップ、スワイプのようなユーザーによる単一のジェスチャーだけでアクセスを許可できること

簡単にログインできることで、デジタルサービスの利用が10〜20%増加

ソース：McKinsey ClickFox調査[14]

デビットカードのように便利

YubiKeyによるパスワードレス・ログインの利便性は、デビットカードの便利さに似ています。皆さんも常にデビットカードを持ち歩いているかもしれません。カードは保護しなければなりません。公共の場に放置することはできません。ATMでロックを解除する際は、短いPINを入力する必要があります。PINは変更しないか、変更するとしても非常に稀な頻度であり、パスワードを覚える必要はなく、ユーザー名もありませんが、ATMは非常に安全に利用できます。

パスワードレスのYubiKeyもこれと同様です。常に携帯します。デスクトップパソコンでも、スマートフォンでも、製造管理システムでも、医療ポータルでも、その他の任意のデバイスでも、YubiKeyをUSBポートに挿すかNFCセンサーにキーを近づけるだけでデバイスをロック解除できます。その後、指示に従ってキーをタップし、対象のアプリケーションやサービスによってはさらに任意でPINを入力するか生体認証機能を使用します。

デビットカードのPINと同じように、FIDO2の場合もセキュリティキーのメカニズにアクセスする際にPINを使用します。PINによってFIDO2セキュリティキーがロック解除された後、ローカル・デバイス、リモート・ディレクトリサービス、ウェブサイト、ソーシャルネットワーク、その他のITサービスなど、認証の対象が何であってもそのサービスとキーを交換できるようになります。

また、PINやジェスチャーを求めずにユーザーの認証を行うように設定されたサービスもあります。例えば、顧客にできるだけ迅速なサービスを提供するという目的で、NFCパッドにキーをセットするだけで認証を行い、即座にコンピューターシステムをロック解除することが許可されている販売担当者もいるかもしれません。ユーザーの存在を検知できる感圧パッドと共に構成されているコンピューターシステムであれば、認証済みの販売担当者がその場を離れた際に自動的にユーザーをログアウトさせることができます[13]。ユーザーの認証プロセスを大きく変えるFIDO2により、非常に簡単かつ高速なユーザーエクスペリエンスを実現してサポートコストを大幅に削減しつつ生産性を高められるため、企業は他の認証手段を追加する資金を十分確保できます。

これらすべてのケースで、FIDO2のパスワードレス・ログインはユーザー名とパスワードの組み合わせよりも迅速で安全なサービスを提供できます。パスワードレス・ログインは、ATMを利用する際の、皆が親しみなれている一瞬の便利さを、アプリケーション、ウェブサイト、サービス、サーバー、デバイスにログインする際のユーザーエクスペリエンスにもたらすものです。

FIDO2のパスワードレス・ログインでは、YubiKey 5シリーズのようなFIDO2認証を得たオーセンティケーターを使用する必要があります。

FIDO2、WebAuthn、FIDO U2F

FIDO2とWebAuthnはどのようにFIDO U2Fと連携するでしょうか？

U2Fは、ドライバーやクライアント・ソフトウェアを求めることなく、ハードウェア・オーセンティケーター、携帯電話、その他のデバイスがウェブベースのサービス（数は無制限）に安全かつ即座にアクセスできるようにするオープンな認証規格です。NXP社の協力を得てGoogle社とYubicoが共同策定したU2Fは現在、オープン認証の業界団体であるFIDOアライアンスによって管理されています。

U2Fは強固な認証ソリューションですが、最初の認証要素としてユーザー名とパスワードを使用する2段階認証のソリューションです。実際、名前にある2Fは第2要素(2nd factor)のことです。

FIDO2は第2世代のU2Fです。U2Fをもとにして、ユーザーがパスワードを使用せずに認証・本人確認を行えるよう、必要な項目を追加して作られたのがFIDO2です。FIDO2認証は強固な単一要素の認証、2段階認証、マルチファクター認証をサポートしています。

FIDO2のWebAuthnコンポーネントには、FIDO U2Fオーセンティケーターとの後方互換性があります。つまり、以前に認証を得ているFIDO U2F Security KeyとYubiKeyは、WebAuthnをサポートしているオンラインサービスとウェブブラウザを使用して行う2段階認証によるログインで引き続き使用できます。

新しいFIDO2のパスワードレス体験を導入する場合は、YubiKey 5シリーズやSecurity Key by Yubicoのような、新しいFIDO2の認証を得たセキュリティキーを使用する必要があります。

パスワードレス・ログインの新しいユースケース

社員

企業が社員を新規採用する際に仮パスワードを発行する必要がなくなります。その代わりに、YubiKeyのようなハードウェア・オーセンティケーターを発行するだけです。ユーザーはYubiKeyと、アプリケーションによっては短いPINも使用してAzure ADやその他のサービスに認証できます。またYubiKeyを使用すれば、スマートフォンやノートパソコンのような追加のデバイスをオーセンティケーターとして登録することもできます。

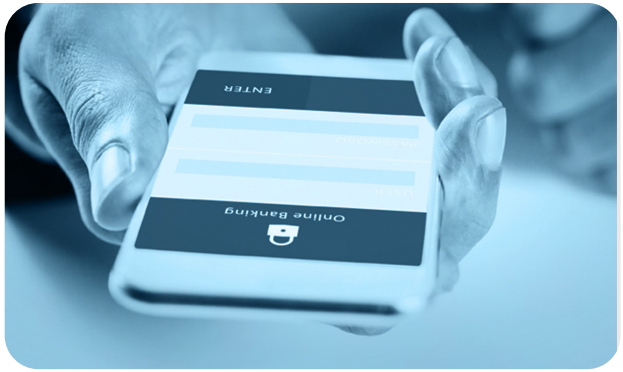
認証プロセスは非常に迅速かつ簡単です。例えば、社員は席についてユーザー名とパスワードを入力する代わりに、席についてYubiKeyをタップするだけで業務を開始できます。

小売

店員、フロアリーダー、チームリーダー、レジ係やその他の小売店の従業員は、ITシステムに素早く簡単にアクセスできなくてはなりません。パスワードレス・ログインにより、詐欺行為を防止するための強固な認証を提供しつつ、新規スタッフの訓練や情報へのアクセスを合理化できます。

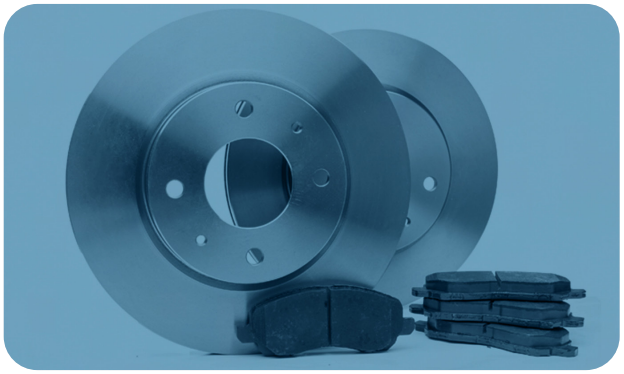
小売店はよく期間限定のスタッフを採用します。例えば、少なくとも北米のある大手小売店は通常、ホリデーシーズンに30,000名の一時スタッフを採用しています。これまで、このすべてのスタッフに対してユーザー名とパスワードを用意する必要がありました。FIDO2の場合は、セキュリティキーを発行するだけで済みます。期間限定の活動が終了したら、Azure ADのようなディレクトリサービスを使って認証済みのサービスを一元的に無効化することができます。

FIDO2により、IT部門がパスワードを作成、リセット、無効化する手間から開放されます。従業員を雇用したら、セキュリティキーを再び有効化して割り当て直すだけで、店舗のサービスにアクセスできるようになります。



金融

手間のかからない迅速なパスワードレス認証を利用できるようにすれば、ブランド体験を向上させ、Eコマースや顧客サポートのやり取りを合理化し、さらには新しい製品やサービスを生み出すことさえできます。銀行、信用組合、そしてセキュリティキーやパスワードレス認証を顧客に提供するその他の金融機関は、口座所有者の手間を減らしつつ口座の乗っ取りが発生するリスクを減らすことができます。



製造

小売店と同じように、製造業界にもシフトで働く作業員がいます。この立ち代わりの激しい作業員によるアクセスを、FIDO2で簡略化できます。FIDO2を使用すれば作業員がパスワードを入力することなく認証を行えるようになるため、社内のセキュリティやID管理の規則に従いつつ、ITシステムへのアクセスを合理化できます。また、パスワード管理ポリシー（定期的なパスワードの変更など）によって遅延やその他のオペレーションの問題が発生するというリスクもなくなります。

米国の国土安全保障省は、知的財産がハッカーの標的になりやすいことを一因として挙げ、これからも製造業界がハッカーの主な標的の一つであり続けると警告しています[15]。製造業界はフィッシング可能なパスワードをFIDO2セキュリティキーと入れ替えることで、フィッシングを防止できる強固な認証を提供し、この種の攻撃の入り口をなくすことができます。

医療

様々なデータ流出の被害に遭いやすいのが医療機関(HCO)です。病歴や支払情報などを含む医療情報は、ブラックマーケットにおける販売額がクレジットカード情報の10倍になっています[16]。どうしてでしょうか？ それは、偽の保険請求のような医療詐欺で得られる金額が大きいからです。

また、HCOはランサムウェア攻撃の被害にも遭いやすく、この攻撃の多くがフィッシングを通じて実行されています。パスワードの代わりにセキュリティキーを使用することで、HCOやその関連企業はこの種の攻撃に対する脆弱性を大幅に改善することができます。

また、FIDO2を使用すれば、HIPAAの規制に基づいて権限を持つユーザー以外が個人の医療情報(PHI)にアクセスできないようにすることもできます。最近の医療業界の調査では、米国の医師の76%が同僚のパスワードを使ってPHIにアクセスしたことがあると答えています[17]。ログイン作業を簡略化することで、医師がPHIやその他の保護されたデータやサービスにアクセスする際に自分の認証情報を使用する頻度が増え、認証情報の共有を阻止できます。少なくとも、その場にいる人物にしかアクセスを許可できなくなります。対照的に、パスワードを共有するとどこからでもアクセスできるようになってしまいます。

またFIDO2により、迅速かつ簡単に認証を行えるという、医療業界にとって重要なもう一つのメリットも得られます。患者、部屋、デバイスが入れ替わる度に、医師や看護師は一日に何十回もログインし直さなければなりません。パスワードレス・ログインを使用すれば、即座に、安全に情報にアクセスできるようになります。介護士は面倒なログイン作業に手間を掛けることなく、介護にフォーカスすることができます。

ベンダーおよびサプライヤーのネットワーク

2013年のTarget社のデータ流出は、ベンダーやサプライヤーのネットワークにあるセキュリティ・リスクの重要性を今も示し続けています。このデータ流出は、ハッカーがHVACサプライヤーのネットワークに侵入して始まりました。Target社のパートナーポータルに接続したサプライヤーは、その小売業者の店舗販売システムにアクセスできるようになります。

FIDO2セキュリティキーでパートナーポータルの認証を強化することで、盗まれたパスワードを使ってパートナーポータル経由で企業に侵入されるリスクをなくしつつ、パートナーによるアクセスを合理化できます。

さらにFIDO2を使用する企業は、サプライヤーのアイデンティティをすべて管理する必要はありません。その代わりに、企業は「パスワードなし」のポリシーを採用し、ベンダーにセキュリティキーを使用して認証を行うよう求めるだけで済みます。ベンダーは自身で簡単にFIDO2セキュリティキーを取得できます。他の認証技術を利用していた以前はこのような管理構成が不可能であり、コストが掛かりすぎてベンダーネットワークを保護するのが難しい状態でした。

まとめ

うんざりするほど長い間、エンドユーザー、セキュリティチーム、ITチームはパスワードに悩まされてきました。FIDO2によってパスワードレスのセキュリティが実現したことで、企業IT、顧客サービス、人と機械のインタラクションが次の時代へと進みます。

企業はFIDO2のパスワードレス・ログインを使用することで、ネットワークのセキュリティを強化し、ITコストを削減し、生産性を高め、高速かつ便利で信頼性に優れたテクノロジーによって実現できる新しい種類のサービスを開発して利益につなげることができます。パスワードレス・ログインがもたらすもの：

- **利便性の向上**パスワードレス・ログインを使用すれば、ユーザーが時間をかけてパスワードを入力したり、なんとかパスワードを思い出そうとしたりする必要がなくなります。情報へのアクセスがより迅速かつ簡単になります。
- **セキュリティの向上**パスワードをなくすことで、パスワードの盗難、フィッシングによるパスワードの不正入手、単純なパスワードを標的にしたブルートフォース攻撃に関連する脆弱性がなくなります。
- **効率改善**パスワードレスに移行すれば、IT管理者が何十、何百、あるいは何千ものパスワードを準備する作業から開放されます。ITサポートの利用が減り、それでいてセキュリティや利便性が向上します。

Windows 10 RS4にアップグレードすれば、何億ものWindows 10のデバイスのユーザーが今すぐFIDO2のソリューションを利用開始できます。これは、ITベンダーや企業のIT部門が協力し始めることで、社内のITセキュリティのニーズだけでなく、顧客のセキュリティのニーズにも応えられるソリューションです。

パスワードレス・ログインで、顧客体験をどのように合理化できるでしょうか？ パスワードが不要になったら、ユーザーエクスペリエンスがどのように変わるでしょうか？ どこからでもより高速、簡単かつ安全にアプリケーションやサービスにアクセスできるようになったらどうなるでしょうか？

パスワードが不要になり、遠隔地にあるデスクトップパソコンやモバイルデバイスを簡単に準備・信頼できるようになり、データ流出や詐欺行為のリスクが（ついに）大幅に減ったら、どのような新製品やサービスを実現できるでしょうか？

これらは、将来を見据えた企業やITの最前線にいる人たちが今考えるべきことです。

FIDO2パスワードレス・ログインの登場により、これらの考えがもはや机上の空論ではなくなり、CISO、プロダクト・マネージャー、UXデザイナー、マーケティング担当者や、できるだけ優れた製品、サービス、体験を提供することに努めているその他のスタッフにとって、現実的な疑問（あるいは速やかに解決しなければならない課題）になっています。

当社の提案

ビジネスリーダー、CIO、CTOやその他のIT業務の総括者は、パスワードレスの時代に向けてどのような準備をすれば良いでしょうか？ こちらがYubicoからの提案です。

情報収集

www.yubico.com/go-passwordlessにアクセスしてYubicoが提供する最新情報を定期購読

Yubicoの開発者プログラムに参加

開発者の皆様はYubicoの開発者プログラムに参加し、ウェークショップ、オープンソース・ソフトウェア、開発サポートをご利用ください。

2段階認証のオプションを今すぐアップグレード

FIDO2セキュリティキーをサポートし、パスワードレス・ログインの準備を行うためです。

パスワードレスへの移行戦略を立てる

組織の運営およびIT部門の代表者を集め、パスワードレス認証を活用する方法を検討しましょう。まずはチームで次のことを始めると良いでしょう。

- パスワードのコスト・モデルを作成します。ヘルプデスクやコールセンターに、パスワード関連のリクエストは何件来ますか？ 通常、各リクエストでどれだけ時間がかかっていますか？ 管理者が新規ユーザーにパスワードを発行するのにどれだけ時間がかかっていますか？ アカウントの締め出しが原因で、生産性がどの程度低下していますか？ 現在の認証プロセスにかかる時間と費用のベンチマークを取り、コスト削減に関する知見を得ます。
- チームが一部のユーザー集団にパスワードレス・ログインを段階的に導入していけるよう、試験プログラムを作成します。ユーザーエクスペリエンスの最適化が大きなメリットにつながるような、強固な認証を要する領域にフォーカスします。段階的導入の進捗状況を監視し、そこで得た知識を次の導入で活かします。

参考資料

1. 「Is Cybersecurity Incompatible With Digital Convenience?」McKinsey & Company社https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience
2. 「Average Business User Has 191 Passwords」Security Magazine. https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
3. Kessem, Limor「Millennial Habits May Bring An End To The Password Era | SC Media」SC Media社https://www.scmagazine.com/millennial-habits-may-bring-an-end-to-the-password-era/article/746144/
4. 「Data Breach Investigation Report」Verizon Enterprise社https://enterprise.verizon.com/resources/reports/2017_dbir.pdf
5. Ehrenkranz, Melanie「The 25 Most Popular Passwords of 2017: You Sweet, Misguided Fools」Gizmodo.com. https://gizmodo.com/the-25-most-popular-passwords-of-2017-you-sweet-misgu-1821425092
6. McKinsey, ibid
7. 「Password Management: Getting Down To Business」https://www.infosecurity-magazine.com/webinars/password-management-getting/
8. 「Windows Hello For Business: What's New In 2017」Channel 9. https://channel9.msdn.com/events/Ignite/Microsoft-Ignite-Orlando-2017/BRK2076?ocid=cx-blog-mmpc
9. Verizon, ibid
10. Ward, Kelsey「Credential stuffing rules the day as 90% of login attempts no longer made by humans」Secureidnews.com. https://www.secureidnews.com/news-item/credential-stuffing-rules-the-day-as-90-of-login-attempts-no-longer-made-by-humans/
11. 「Windows 10 Hits 500 Million Active Devices」Engadget. https://www.engadget.com/2017/05/10/windows-10-500-million-users/
12. 「NIST SP 800-63 Digital Identity Guidelines」Nist.Gov. https://www.nist.gov/itl/tig/projects/special-publication-800-63
13. 「Pcprox® Mat | RF Ideas」Rfideas.Com. https://www.rfideas.com/products/presence-detectors/pcprox-mat
14. McKinsey, ibid
15. 「Energy Sector Tops List Of US Industries Under Cyber Attack, Says Homeland Security Report - Iot Now - How To Run An Iot Enabled Business」Iot Now - How To Run An Iot Enabled Business. https://www.iot-now.com/2015/03/12/30962-energy-sector-stays-top-of-the-list-of-us-industries-under-cyber-attack-says-homeland-security-report
16. 「Your Medical Record Is Worth More To Hackers Than Your Credit Card」ロイター社https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
17. 「Do Doctors Share Electronic Health Record Passwords?」The Millennium Alliancehttps://mill-all.com/blog/2017/10/04/do-doctors-share-electronic-health-record-passwords/

yubico

Yubicoについて コンピューター、サーバー、インターネット・アカウントを安全かつ簡単に利用できるようにする新しい標準を世界的に打ち立てているのがYubicoです。2007年創立のYubicoは、オーストラリア、ドイツ、シンガポール、スウェーデン、英国、米国にオフィスを置く非上場会社です。10社中9社の大手インターネット・ブランドや160か国以上の数百万のユーザーが当社のテクノロジーを使用している理由を**www.yubico.com**でご紹介します。

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Swedenスウェーデン

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301米国
844-205-6787（フリーダイヤル）
650-285-0088