WebAuthnの仕組み

okta

WebAuthn

近年、サイバー攻撃によって個人情報が漏えいするWebサイトが急増しています。アカウント乗っ取りによる損害額は51億ドル以上に達し、Marriott社が運営するStarwoodホテルやGoogle社など、顧客と直接接する大手企業でも大規模なデータ漏えいが相次いでいます。消費者からの信用の失墜や数百万ドル単位の逸失利益を避けるため、企業はユーザー保護のアプローチの見直しを迫られています。

目次

パートI:

WebAuthnとビジネス上の効果

2019年3月、World Wide Web Consortium（W3C）は、WebAuthnがパスワードレスログインの正式なWeb標準として承認されたことを発表しました。WebAuthnは、すでに幅広いアプリケーションでサポートされているため、数年以内には広く普及すると見込まれています。

この新しい標準により、WebAuthnをサポートするブラウザで実行されるすべてのWebアプリケーションで、オーセンティケータを使用した安全なユーザー認証が可能になります。Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari、Opera、さらに各種のプラットフォーム（Windows Hello対応MS Edge、Google Androidなど）での早期サポートにより、ついにFIDO2/WebAuthnの実用の目途が立ちました。前身のU2Fは、サポートするブラウザやプラットフォームが少なかったためにあまり普及しませんでした。WebAuthnは、デバイス自体を認証に使用するため、YubiKeyなどの外部トークンを導入するか、サポートするプラットフォームを介して利用できます。

企業とユーザーのメリット

WebAuthnは、企業とユーザーの両方に多くのメリットをもたらします。ユーザーエクスペリエンスの向上（パスワードレスログインなど）だけでなく、セキュリティが強化され、対応すべき攻撃の種類が減るので、企業にとってもユーザーにとっても有益です。

企業側では、WebAuthnを使用することにより、パスワードスプレー攻撃やクレデンシャルスタッフィング攻撃のような、多数のサイトに対して自動で行われるパスワード攻撃を防ぐことができます。こうした攻撃では、一般的に、ユーザーのログイン資格情報が悪用されるため、この点はユーザーにとって、メリットになります。WebAuthnのメリットを受ける主な利害関係者については、パートIIで詳しく取り上げます。

顧客やエンドユーザーにとっては、フィッシングで盗まれた資格情報を悪用したアカウント乗っ取りを防げる点で大きなメリットがあります。WebAuthnでは、オーセンティケータをアプリケーションに登録し、秘密鍵と公開鍵のペアを生成して、ローカルの内部オーセンティケータ（Microsoft Edge、Androidなど）またはYubiKeyなどの外部オーセンティケータに資格情報を保存する仕組みになっているため、資格情報を盗み出すのは困難です。

WebAuthnなら、ユーザーは、資格情報の保管を外部の手にゆだねて、漏えいしないことをただ祈るのではなく、セキュリティを自身の手で管理できます。また、WebAuthnが標準として認められ、利用のハードルが下がったことで、今後、より多くの一般ユーザーがこの強力な認証方法を使用する機会が増えると期待されます。

パートII:

認証の歴史

現在の認証方式の欠点

WebAuthnが開発された理由とWebAuthnの仕組みをより深く理解するために、まずは、ユーザー認証の歴史と現在の方式の欠点について説明します。

パスワードクレデンシャル

ユーザー名とパスワードの組み合わせは、最も馴染み深い認証方式です。このフレームワークは一般ユーザーにもわかりやすく、広く普及していますが、アメリカ人の5人に1人が、パスワードクレデンシャルの漏えいによってアカウント乗っ取り（ATO）の被害にあっています。平均的なエンドユーザーが130以上のオンラインアカウントを持つようになる中、企業は、ビジネス上のメリットを考え、より成熟したユーザー認証フレームワークを求めるようになりました。

2要素認証

次に登場したクレデンシャル認証が、2要素認証（2FA）です。しかし、顧客アカウントの認証で第2要素としてよく使われるSMSのような確実性の低い方法は、フィッシング攻撃を受ける危険性があることが裏付けられています。このような2FAの欠点を克服するため、WebAuthnでは、高度なフィッシング攻撃を防ぐと同時にユーザーエクスペリエンスを向上させるための対策が盛り込まれました。

WebAuthnの概要

WebAuthnは、Web認証の新しい世界標準です。ブラウザベースのAPIであり、登録したデバイス（スマートフォン、ノートパソコンなど）を要素として使用することで、Webアプリケーションでのユーザー認証の簡素化とセキュリティ向上を実現します。また、パブリックキーを使用することで、高度なフィッシング攻撃からユーザーを守ります。

WebAuthnのメリットと利害関係者

WebAuthnを使用するメリットは大きく3つに分けられます。各メリットを受ける利害関係者には、顧客、製品オーナー、セキュリティチーム、サポートチームが含まれます。

メリット	利害関係者
顧客エンゲージメントの向上	顧客、製品オーナー
セキュリティ体制の強化	**顧客、セキュリティチーム**
アプリケーションサポートの負担軽減 ● 主要ログイン方式としてのWebAuthnの使用 ● 下位互換性	サポート

顧客エンゲージメントの向上

顧客 — ログインの利便性向上

WebAuthnではデバイスベースの認証を使用するため、パスワードは不要です。つまり、顧客は、ログインのためにユーザー名とパスワードを覚えたり、ステップアップ認証の第2要素としてワンタイムパスワードを取得したりする必要がなくなります。認証用に登録したデバイスを使用すればよいだけなので、認証プロセスが簡単になります。

製品オーナー — 認証の時間短縮

前述のとおり、WebAuthnではパスワードが不要です。製品オーナーは、アプリケーションの使いやすさを重視し、通常、顧客の手間を軽減することは最優先事項です。WebAuthnを使用すれば、ログインの利便性を向上できます。

製品オーナー — リリースまでの期間短縮

WebAuthnでは、パスワードに関する面倒な設定も不要です。パスワードを管理および保管するための複雑なアーキテクチャを実装する必要がないため、製品をより迅速にリリースできます。

セキュリティ体制の強化

顧客 — 信頼の確保

データ漏えいが多発する今日、顧客からの信頼を維持することが特に重要になっています。顧客は、企業に個人情報を提供する際、情報が安全に守られるかどうか不安に感じます。WebAuthnなら、より安全性の高い認証方式を使用することで、パスワードが持つリスクを回避できます。

セキュリティチーム — パスワード固有の弱点の克服

WebAuthnを使用した認証では、ユーザー名とパスワードのような、記憶頼みの要素は使用しません。代わりに、エンドユーザーが所有する登録済みデバイスを使用します。物理的なデバイスはパスワードに比べて盗むのが難しいため、なりすまし認証のリスクが低く、セキュリティチームにとっても安心です。

アプリケーションサポートの負担軽減

サポートチーム — 多要素のサポートサイクルの軽減

WebAuthnの特徴は、主たるログイン方式として使用できることです。WebAuthnを実装することにより、登録が必要な要素が基本的にWebAuthnだけになり、多要素の管理が不要になるため、サポートサイクルの負担が軽減されます。

サポートチーム — 下位互換性

さらに、WebAuthnには下位互換性があるため、社内に配布済みのトークンを急いで更新する必要はありません。WebAuthnをサポートするWebブラウザでは、第2要素として、U2F対応YubiKeyなどのFIDO U2Fキーも従来どおり使用できます。そのため、移行計画を慎重に立て、時間をかけて実行することができます。

パートIII:

WebAuthnの仕組み（フローとOkta UI）

上記のとおり、WebAuthnはユーザーエクスペリエンスの向上やセキュリティ体制の強化に役立ちます。次に、WebAuthnの仕組みに目を向けて、認証フローとその各ステップでのベストプラクティスについて見ていきましょう。

WebAuthnの主な流れ

登録フロー

認証フロー

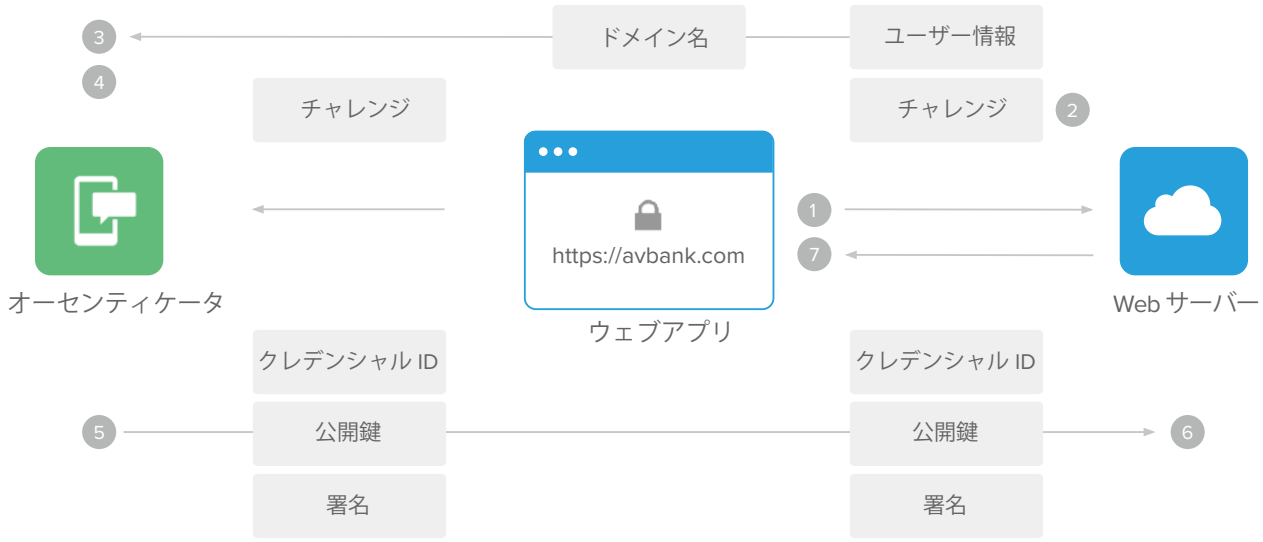
アカウント回復

登録フロー

登録では、ユーザーがオーセンティケータ（デバイス）をWebサーバーと結び付けます。ユーザーのデバイス登録で主に必要になるのは、オーセンティケータ、Webアプリケーション、Webサーバーの3つです。登録は以下のステップで行われます。

クレデンシャルID	q2we323d2rty123
シークレットキー	s12ds3d4s5da6
ドメイン名	avbank.com
ユーザー情報	Swaroop Sham

ユーザー	Jason Sham
チャレンジキー	a9ds9dw9eds9d
クレデンシャルID	q2we323d2rty123
パブリックキー	0x3idfkek309



1. ユーザーがデバイス上でデバイス設定を開始します。
2. Webサーバーが登録のためのチャレンジキー（1回限りの使用）を生成します。
3. WebサーバーがWebアプリケーションにチャレンジキーとユーザー情報を送信します。
4. Webアプリケーションが正規のドメイン名を追加して、その情報をオーセンティケータに送信します。
5. オーセンティケータがユーザーに承認を求めます。
6. ユーザーが承認すると、オーセンティケータがクレデンシャルID、パブリックキー/シークレットキー、ユーザー情報、ドメイン名を保存します。
7. WebアプリケーションがWebサーバーにクレデンシャルID、公開鍵、署名を送信します。
8. チャレンジキーが無効になり、デバイスが登録されます。

ユースケース1 — Oktaでの登録

Oktaでは、ユーザーが自社テナントにサインインする際に「プラットフォーム」オーセンティケータを登録できます。管理者は、サインオンオプションとMFA登録ポリシーを設定することにより、機能フラグを介してユーザーのWeb認証を有効にできます。エンドユーザー側では、ユーザー名とパスワードの入力後、Windowsのプラットフォーム認証であるWindows Helloの登録オプションが表示されます（図1）。これは、登録フローのステップ1に該当します。

図1

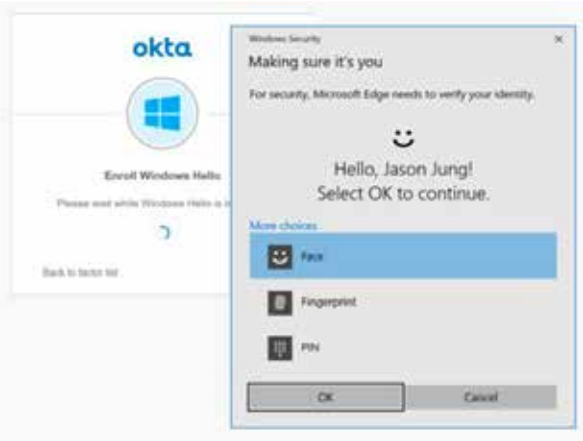
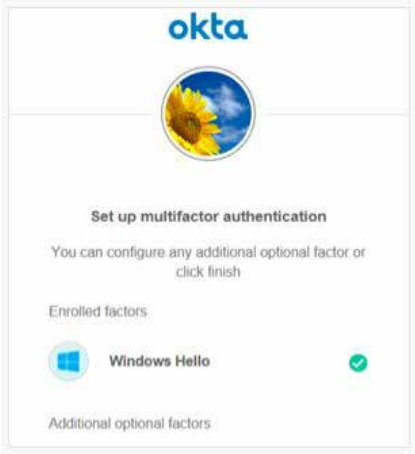


図2

Windows Helloの設定が完了すると、パブリックキー/シークレットキーを生成するための1回限りのセットアップ手順が実行されます（ステップ5）。上記の登録フローで示したように、ユーザーはローカルデバイスに保存されたデータによって顔認証、指紋認証、またはPIN認証を実行し、承認を行います。

生体要素またはPINによる承認が完了すると、クレデンシャルID、パブリックキー、署名がWebサーバーに送られて、登録が完了します。



Okta のベストプラクティス

登録については、ユーザーが社内ネットワークからアクセスしたときにのみ初回登録できるように制限し、登録の有効期間を設定すると（新規ユーザーは作成後３日以内に登録しなければならないなど）、登録段階でのリスクを軽減できます。

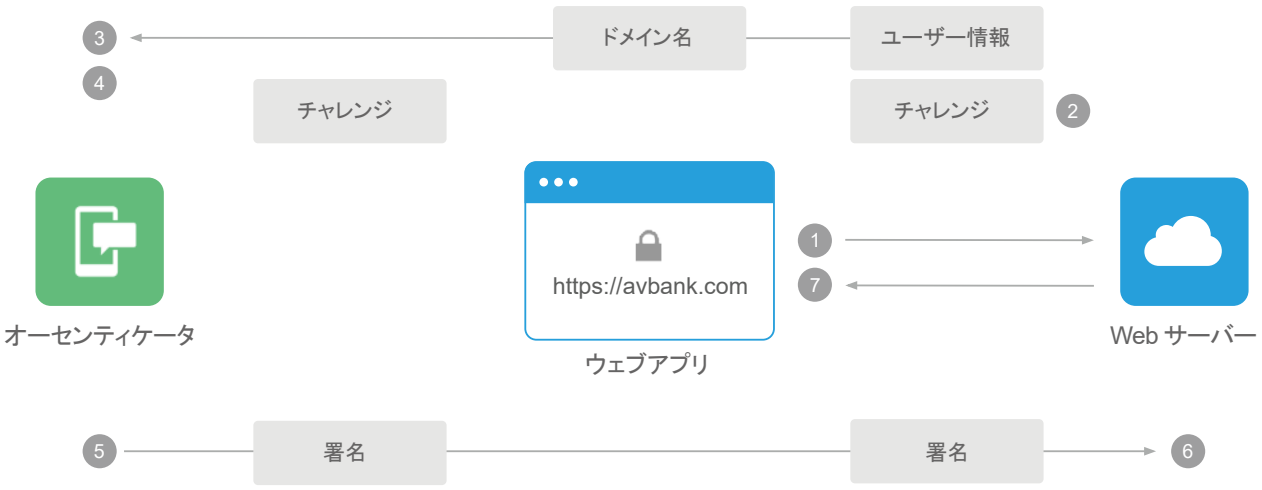
また、要素の登録と回復手順、アプリケーション固有の登録ポリシー（特定のアプリケーションにアクセスしたときの登録制限）、登録時の独自の本人確認プロセスをエンドユーザーにわかりやすく示すこともベストプラクティスとしてお勧めです。

認証の仕組み

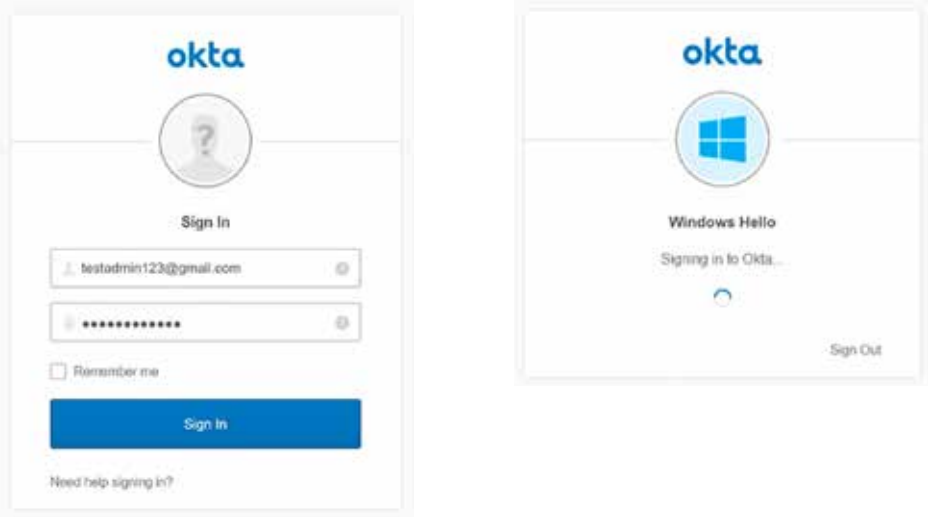
デバイスの登録後、WebAuthn でのユーザー認証はシームレスかつ安全に行われます。登録後の認証フローは、オーセンティケータに保存されたシークレットキーによる署名の生成が中心となります。これにより、チャレンジが毎回生成されるようになります。

クレデンシャル ID	q2we323d2rty123
シークレットキー	s12ds3d4s5da6
ドメイン名	avbank.com
ユーザー情報	Swaroop Sham

ユーザー	Jason Sham
チャレンジキー	a9ds9dw9eds9d
クレデンシャル ID	q2we323d2rty123
パブリックキー	0x3idfkek309

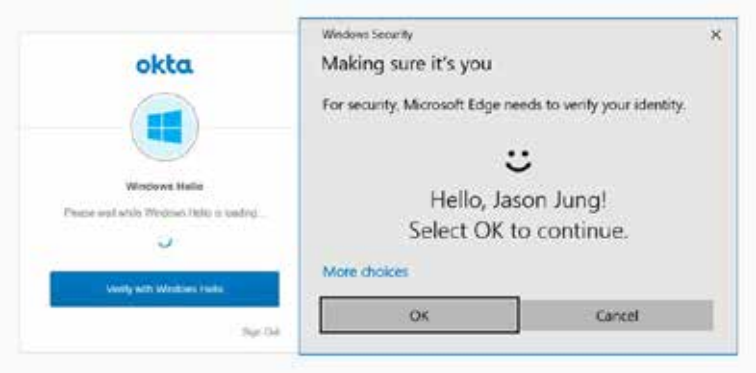


1. ユーザーがデバイス上でデバイス設定を開始します。
2. Web サーバーが一意のチャレンジを生成し、オーセンティケータに送信します。
3. オーセンティケータがチャレンジを受信し、チャレンジのドメイン名を保存します。
4. オーセンティケータがユーザーに生体認証を求め、承認を得ます。
5. オーセンティケータが暗号署名を生成し、Web サーバーに送信します。
6. Web サーバーが署名を一意のチャレンジと照合して検証し、ユーザーのログインを許可します。
7. ユーザーがログインします。



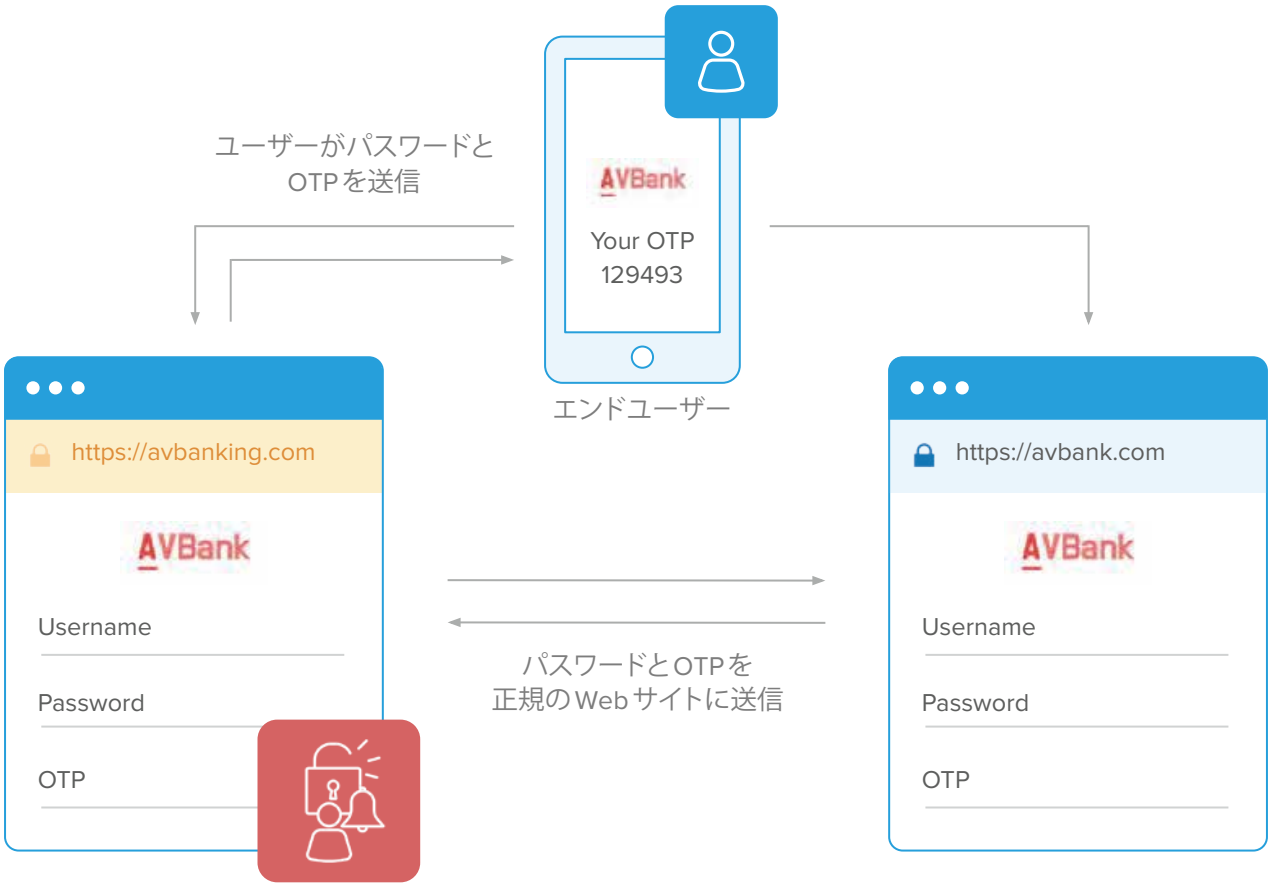
ユースケース 2 — Okta での認証

Okta では、ユーザーは、ステップアップ認証の代わりにプラットフォーム認証を使用できます。ユーザー名とパスワードの入力後、WebAuthn を追加要素として使用してセキュリティを確保できます。Okta では、ネットワークゾーン、時刻、およびデバイスのタイプに基づいてチャレンジを行うように設定することもできます。エンドユーザーは、Okta への認証時に、Windows Hello での検証を求められます。



WebAuthnとフィッシング

WebAuthnがフィッシング攻撃に強い理由は、ドメイン名がオーセンティケータに保存されるためです。多くのフィッシング攻撃では偽のWebサイトが使用されますが、オーセンティケータでは、ステップ3で保存したドメイン名とWebサイトのドメイン名が照合されます。



フィッシング攻撃の例

オーセンティケータは、チャレンジを受信すると、チャレンジの送信元のドメイン名を確認します。上の図に示すように、一般的なフィッシング攻撃では、通常、エンドユーザーが偽のWebサイトにリダイレクトされ、そこで資格情報を入力してしまい、その情報がアカウントの乗っ取りに悪用されます。WebAuthnを使用する場合は、オーセンティケータ（この例ではスマートフォン）によってユーザー側でドメイン名が検証されるため、そのリスクはありません。これにより、ユーザーが誤って悪質なWebサイトで資格情報を入力してしまうのを防ぐことができます。

アカウント回復の仕組み

デバイスを紛失して、そのデバイスからWebAuthn認証でログインできなくなった場合に備えて、回復用に安全性の高い他の要素を登録および設定しておくことが重要です。Oktaでサポートされる回復用の要素には以下のものが含まれます。

Okta Verify	SMS Auth	Google Auth	Windows Hello
U2F (FIDO 1.0)	YubiKey	Duo Security	Symantec VIP
On-Prem MFA	RSA SecurID	Security Question	Voice Call Auth

Oktaのベストプラクティス

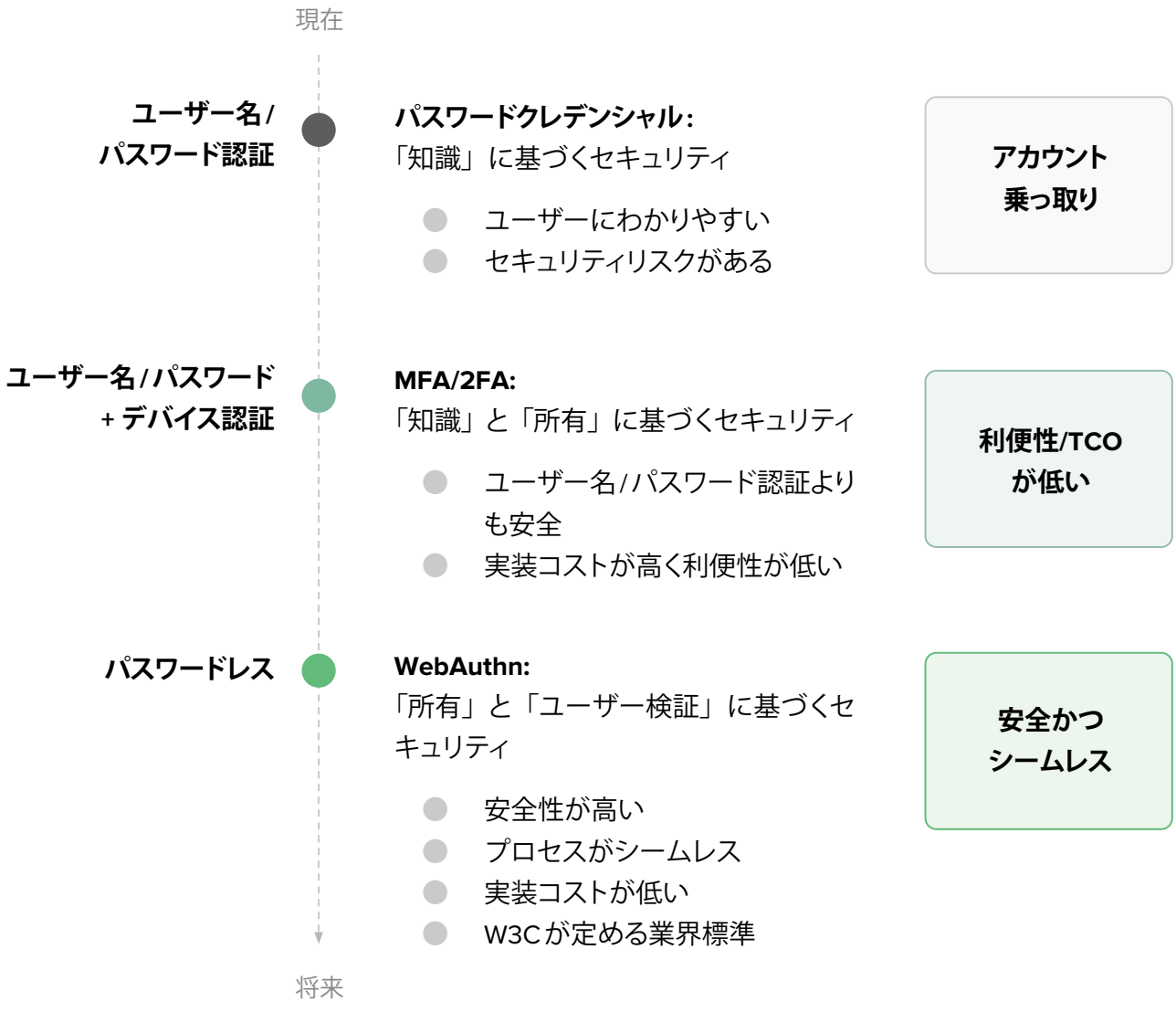
企業のセキュリティ体制の強さは、セキュリティが最も脆弱な部分によって決まります。何らかの理由で回復用の要素を設定できない場合は、可視性を高めることで（要素やパスワードの回復が必要なときにユーザーに自動でメール通知を送るなど）、不審なインシデントをただちに検出し、対処できるようにすることが大切です。

パートIV:

パスワードレスの将来への移行

WebAuthnの新しいフローを導入すれば、より安全なパスワードレス環境に近付くことができます。Oktaは、お客様が認証の課題を解決するために役立つソリューションの開発に注力しています。また、パスワードレス戦略の採用拡大に役立つ、WebAuthnなどの認証標準のサポートにも取り組んでいます。

WebAuthnが普及すれば、アカウントの乗っ取りやユーザーエクスペリエンスの低下といった問題が解消され、快適な認証プロセスを実現できるはずです。



Oktaは、企業のセキュリティ体制強化に貢献するさまざまな製品を提供しています。認証プロセスの脆弱性によって、数多くのアイデンティティ攻撃が生まれています。Oktaのアダプティブ多要素認証は、これらのリスクを緩和すると同時にユーザーへの影響を最小限に抑えることを目的としたソリューションです。

WebAuthnの技術仕様について詳しくは、W3Cが公開しているWebAuthnドキュメントを参照してください。

Oktaが提供するその他の参考情報

WebAuthnの概要

開発者ガイド: WebAuthn

パスワードレスへの道

FIDO2とWebAuthnによるシームレスで安全なログインの実現

Oktaについて

Oktaは、エンタープライズのためのアイデンティティ管理ソリューションを提供する、業界トップの独立系プロバイダです。Oktaアイデンティティクラウドは、組織が適切な人を適切なテクノロジに適切なタイミングで安全に結びつけられるようにします。6,000を超えるアプリケーションやインフラストラクチャのプロバイダとの統合機能があらかじめ用意されているOktaなら、ビジネスに最適なテクノロジを簡単かつ安全に使用できます。20世紀フォックス映画、ジェットブルー航空、ノードストローム、Slack、ティーチ・フォー・アメリカ、Twilioをはじめとする6,100を超える組織が、Oktaを使用して職場や顧客のIDを保護しています。

www.okta.com/jp/