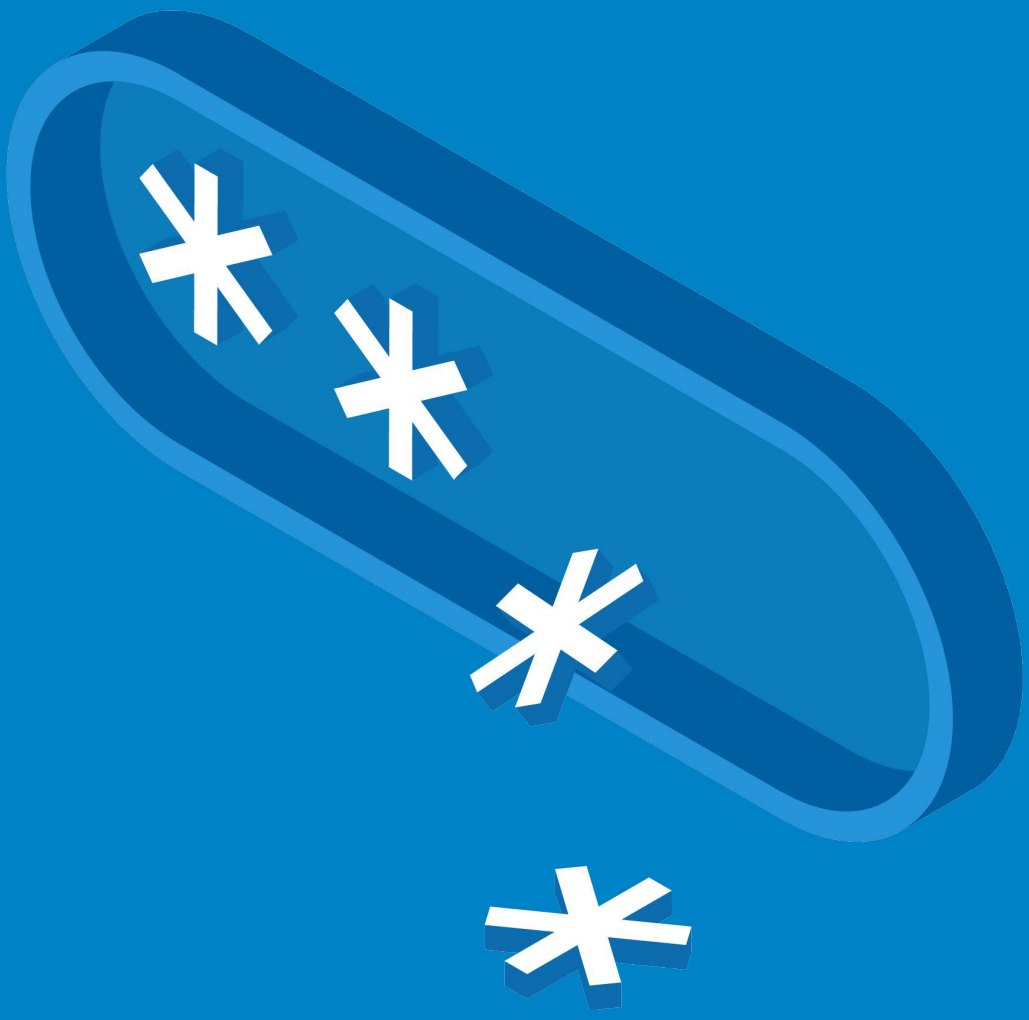
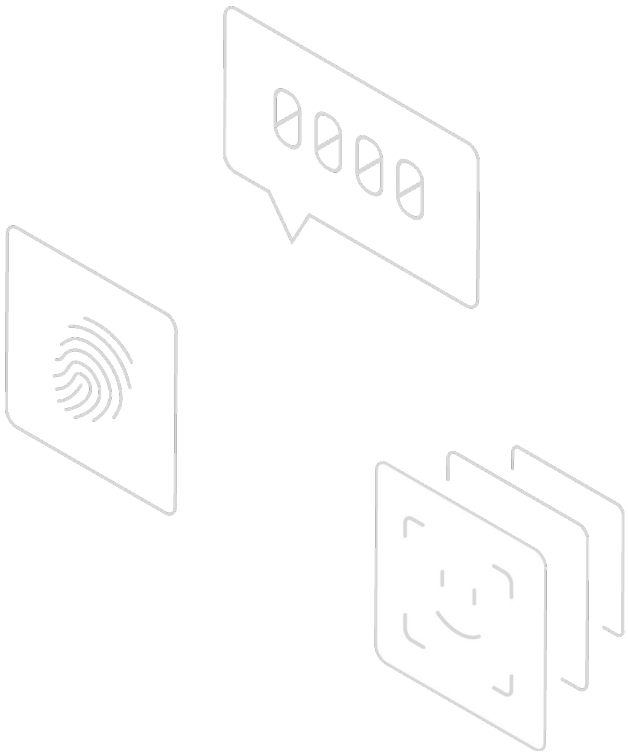
パスワードレスの実現



okta

目次

はじめに



ユーザー名とパスワードを使った従来の認証方法は、50年以上にわたりデジタルアイデンティティとセキュリティの基盤でした。ところが、ユーザーアカウントが増え続ける今日、新たな問題がいくつか生じています。エンドユーザーが複数のパスワードを覚えておかなければならない、サポートコストがかかるといった問題、そして最も重要なのは資格情報の侵害によって引き起こされるセキュリティリスクの問題です。こうした新たな課題は現在、パスワードの利便性よりも重視されています。認証エクスペリエンスからパスワードをなくそうという議論は、日々ますます高まっています。

パスワードレス認証規格の出現、消費者向けエクスペリエンスや同様のエクスペリエンスへの期待の高まり、膨大なコスト上昇などが、1 つの理論でしかなかったパスワード排除を現実的な可能性に変えています。このホワイトペーパーでは、顧客と社員、双方の認証をパスワードレスに移行すべき根拠を紹介し、パスワードレス認証に移行するために組織や企業が実践できる手順を説明します。

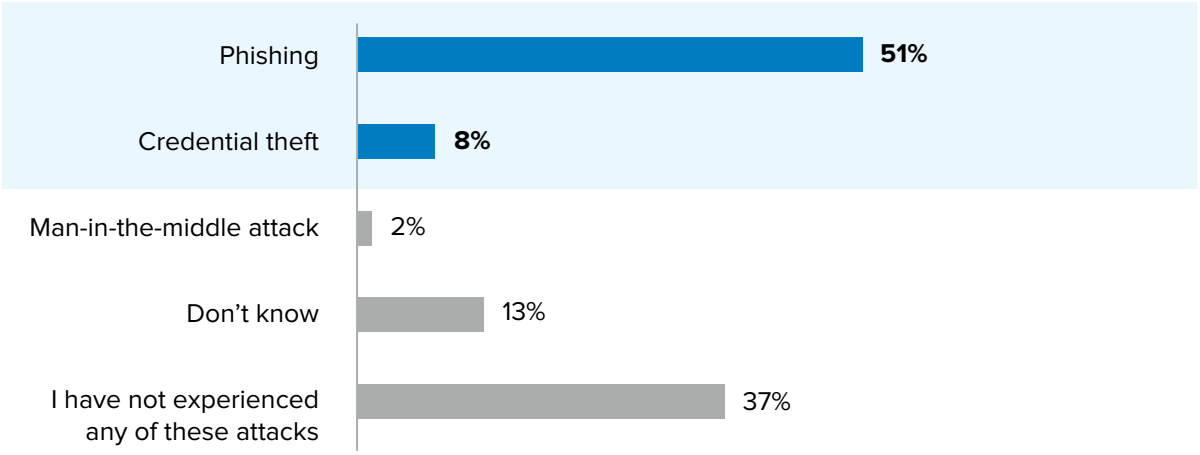
パスワードを使わない方法の探求

パスワードレス認証の必要性を理解するには、まずパスワードによって生じている課題を理解することが必要です。パスワードの主な課題は、次の領域に分類できます。

脆弱なアカウントセキュリティ

パスワードは、あらゆるカテゴリのセキュリティ /アイデンティティを利用した攻撃を引き起こしてきました。資格情報の漏えいによるパスワードの侵害、フィッシング、パスワードスプレー攻撃、パスワード管理の甘さなどによって、アカウント乗っ取り攻撃（ATO）が発生しています。こうした攻撃に対抗するには、まず、多要素認証（MFA）などの認証レイヤーを追加することから着手できます。

> 「ハッキング関連の侵害の 81% では脆弱なパスワードや盗み取ったパスワードが利用されています」
>
> — Verizon 社 2017 年度データ漏洩報告書



回答者の 59% が資格情報の盗難やフィッシングを経験
Ponemon 社 2019 年度認証レポート

しかし、MFA は完璧な解決策ではありません。このテクノロジの課題は、2 番目の要素として広く利用されている SMS などの確実性の低い要素に脆弱性があり、それがハッカーによって悪用されている点です。その例は多数報告されています。

お粗末なユーザーエクスペリエンス

パスワードは面倒なものです。 パスワード選びにはさまざまなベストプラクティスがありますが、少なくとも一意で推測されにくいと同時に、覚えやすいものである必要があります。 オックスフォード大学の調査では、 オンラインでの購入する人のおよそ 1/3 は、 パスワードを思い出せないために購入を途中で諦めてしまうことがわかっています。

コストの増加

パスワード関連のコストは、 パスワードを使うどのメリットよりも重要です。 コールセンターで最も多い問い合わせの 1 つはパスワード管理に関するものです。 パスワードに関連するサポート負荷を減らすことは、 組織にとってミッションクリティカルな課題の 1 つです。

12.6
分/週

1 週間にパスワードの入力や
リセットにかかった平均時間

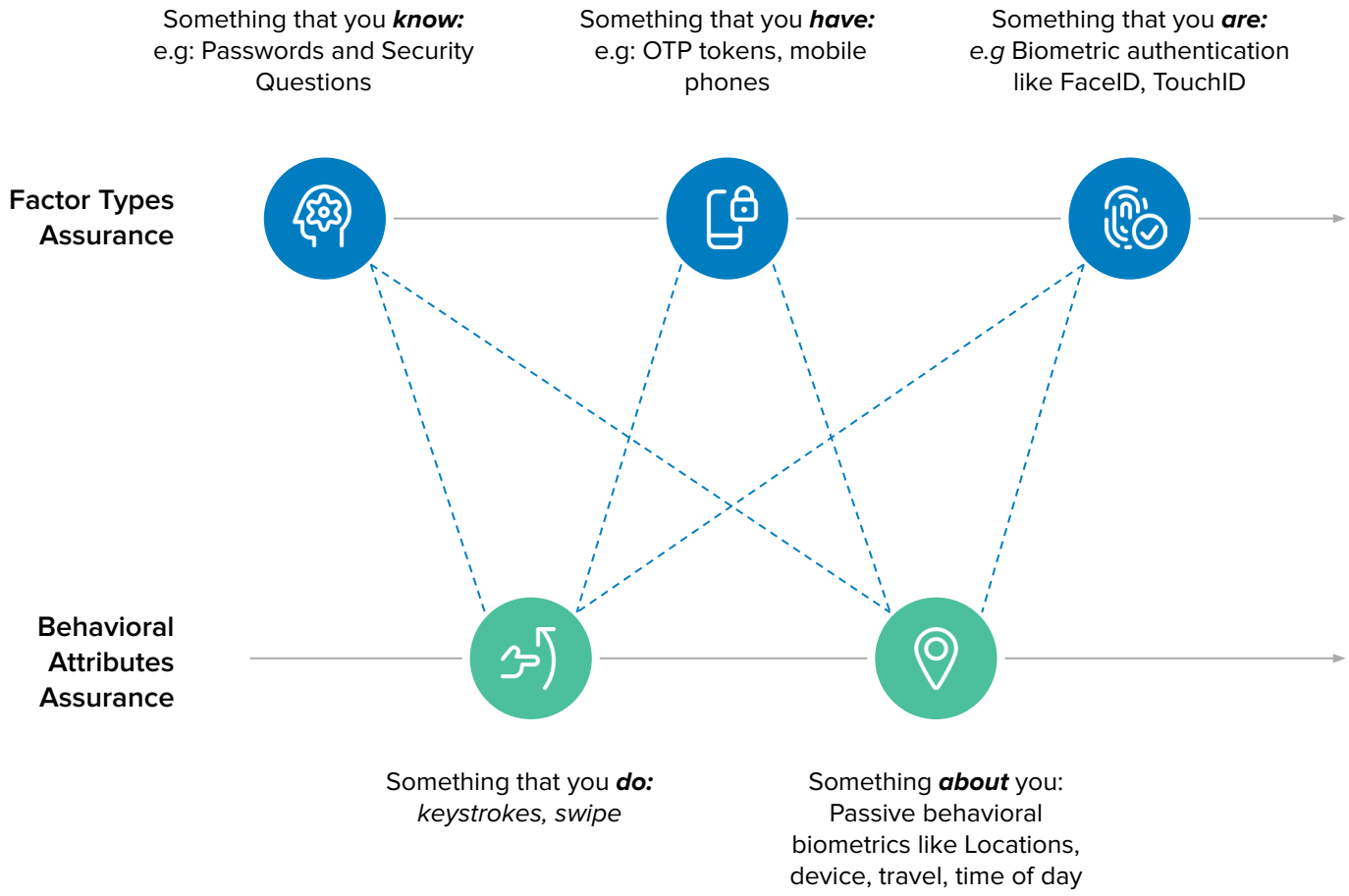
5,217,456
ドル

1 企業あたり失われた生産性や
労働力の年間コスト

出典: Ponemon 社 2019 年度認証レポート

現在の認証方法の評価

現在の認証方法では知識、 所有、 生体といった要素を利用しており、 多くの場合は 1 つ以上の要素と行動属性を組み合わせ、 アクセスの判断を行っています。 これは、 追加のセキュリティレイヤーを持つことにより、 攻撃者がユーザーアカウントにアクセスできる可能性は低くなるという考え方に基づいています。



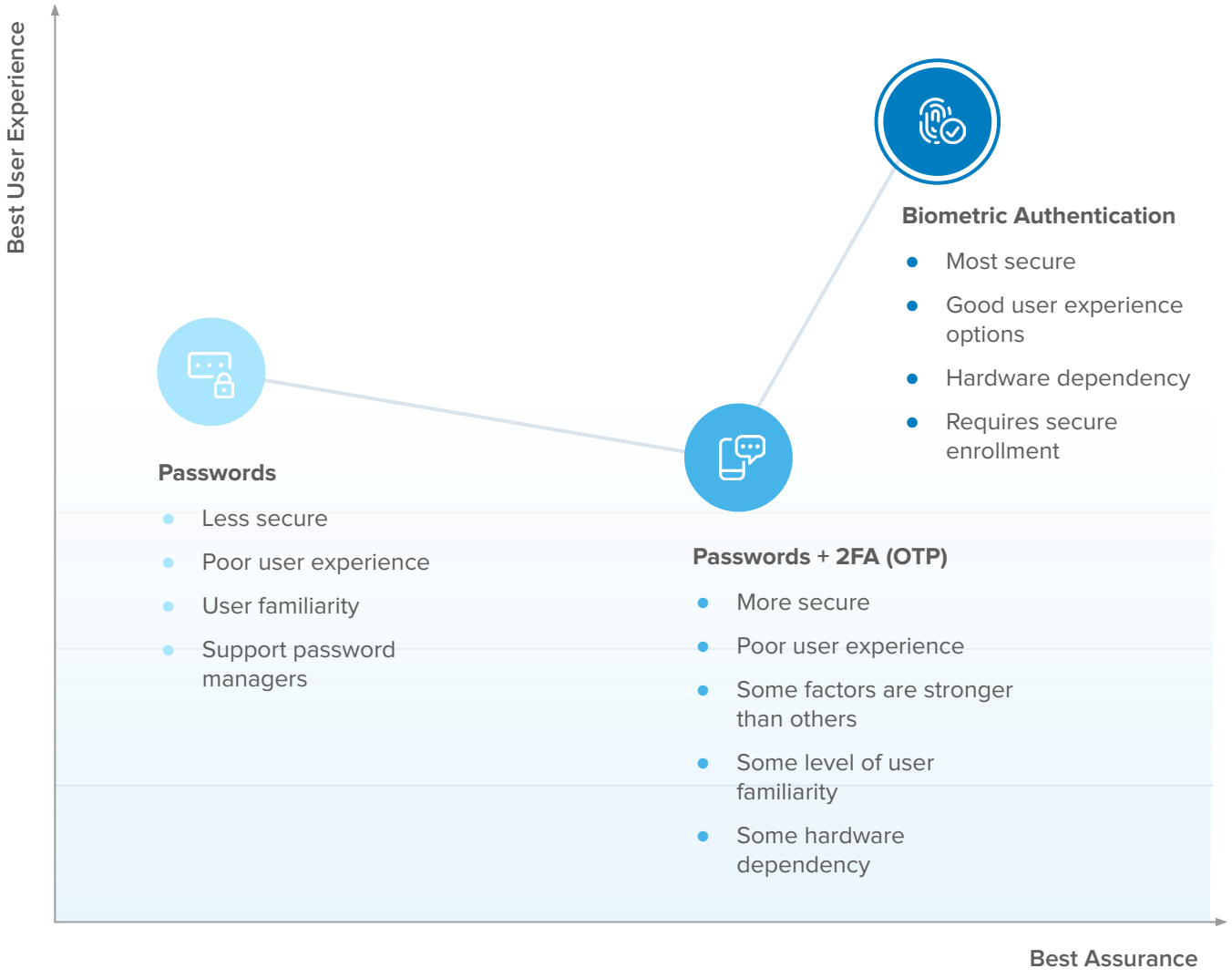
認証方法を評価する場合には、 次の 2 つの主要な特性について幅広く検討する必要があります。

保証/セキュリティ

認証メカニズムは、 承認されたユーザーしかアカウントにアクセスできないことを保証できるか？

ユーザーエクスペリエンス

- 認証メカニズムは、 登録から認証、 復旧までのシームレスなジャーニーを提供できるか？
- オーセンティケータは、 すべてのユーザーグループ、 デバイスタイプ、 ソフトウェアプラットフォームに対してあらゆる認証をサポートできるか？



パスワードレス認証の導入

パスワードを排除する場合は、詳細を慎重に検討する必要があります。パスワードの排除を決定する前に、脅威、テクノロジ、ユーザージャーニー、コスト、導入のしやすさ、実装の観点から検討して、段階的なアプローチをとることをお勧めします。

脅威

- 資格情報の侵害
- 中間者攻撃
- MITB 攻撃
- パスワードスプレー攻撃
- 総当たり攻撃

テクノロジ

- ブラウザのサポート
- テクノロジに関するアプローチ
- プラットフォームオーセンティケータか外部のオーセンティケータか

ユーザージャーニー

- 登録フロー
- 認証フロー
- 復旧フロー

ビジネス上の検討項目

- サポート
- 統合
- デバイスへの適用
- コンプライアンス要件

導入のしやすさ

- 一般的なパスワード
- 一般的なパスワードマネージャ
- パスワードのプロビジョニングが容易

実装

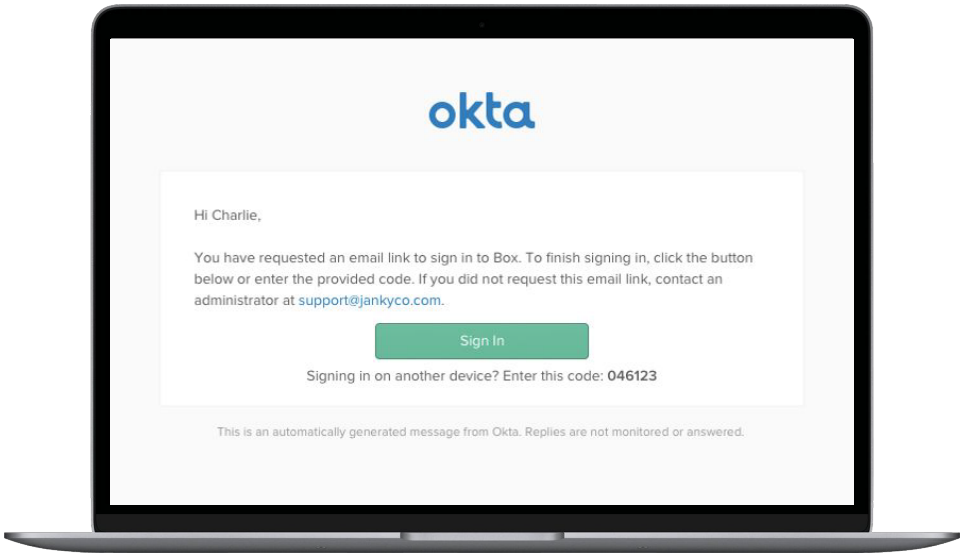
- セキュリティとコンプライアンスの要件
- Web サイトのサポート

パスワードレスへの一般的なアプローチ

パスワードを排除してパスワードレスにするには、さまざまなテクノロジの利用が可能です。メールのマジックリンクなどのアプローチでは、暗号化された OTP トークンまたはライブリンクを安全なメールの本文に記載します。一方 WebAuthn では、公開・秘密鍵ベースの暗号化を利用してセキュアな認証を実現します。

Okta ではさまざまなパスワードレスアプローチを提供しています。このセクションでは、パスワードレスへの主なアプローチをいくつか紹介します。

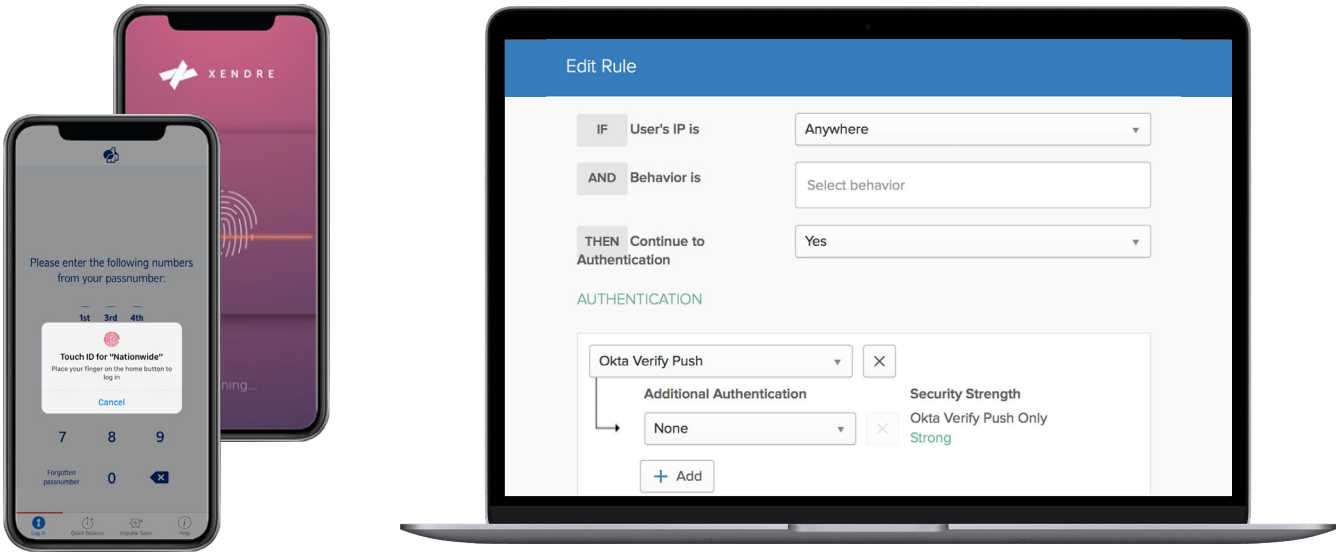
メールのマジックリンク



メールベースのパスワードレス認証は非常に一般的になりました。この方法はいわゆるパスワードリセットフローとして使用されます。ユーザーは送信されたシークレットリンクから、既存のパスワードを使わずに新しいパスワードを設定できます。ほとんどのユーザーが何十回、何百回と使ったことがあるでしょう。この認証方法は、Slack や Medium といったアプリケーションで一般的になりました。しかし真のパスワードレス認証を使用すれば、パスワードのリセット方法がもう一段階高度なものになります。アプリケーションの設計者がパスワード（および関連のリセット手順）を削除し、期間限定またはユーザーライフサイクル限定で 1 回のみ使用できるシークレットリンクをユーザーのメールアドレスに送信します。そのリンクをクリックすると、ユーザーが認証され、ログイン状態を維持するライフタイムの長い cookie が設定されます。ユーザーがパスワードを設定、保存、入力する必要は一切ありません。これは、特にモバイルデバイスを利用する場合に非常に便利です。この方法を使用したパスワードレス認証はハードウェアに依存しないため、消費者向けアプリケーションに非常に有効です。

ユースケース	メリット	課題
• ログインパターンが不定期 • WebAuthn の代替のパスワードレス認証 • パスワードベースの攻撃の阻止	• 導入と利用が簡単 • シームレスなオンボーディング • ハードウェアに依存しない • 容認可能で使い慣れたユーザーエクスペリエンス • デスクトップとモバイルで一貫したエクスペリエンス	• セキュリティ管理がメールアカウントのセキュリティにアウトソースされる • リンク（メール）共有の制御や可視化ができない • メールが暗号化されていなければ中間者攻撃の影響を受けやすい

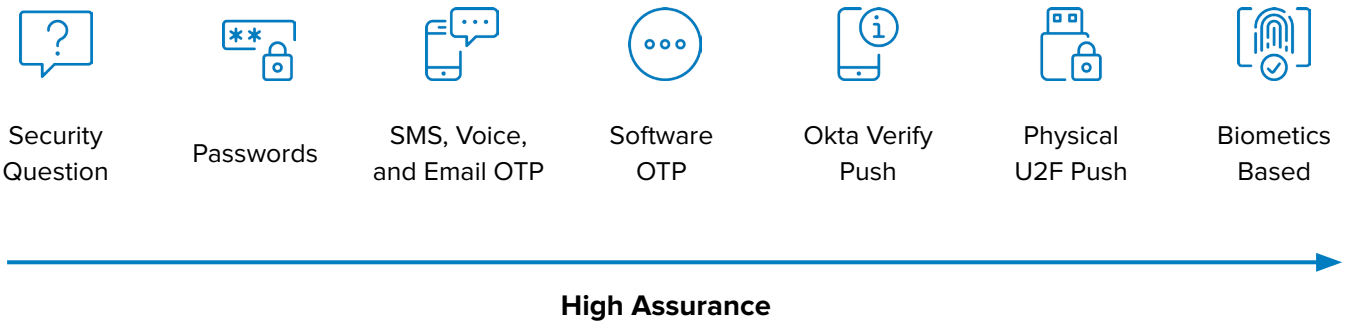
Factor Sequencing



Okta Adaptive MFAのコンテキスト認識とThreatInsightのインテリジェンスを組み合わせることで、組織は、さまざまな認証要素を利用してパスワードレスソリューションを安全に設定することができます。 脅威レベルが低い場合はログインエクスペリエンスを合理化できるため、 ユーザーは必要なデータやアプリケーションにより簡単にアクセスできます。 ただし、 ログインに関連するリスクレベルが高い場合は、 追加の認証要素が必要となります。 たとえば管理者には、 第 1 認証要素として Okta Verify モバイルアプリケーションを設定します。 ユーザーが既知の場所やデバイスからログインした場合、 Okta はアクセスを取得するためにユーザーが承認したアプリケーションを介して認証要求を送信します。

一方で Adaptive MFA がログイン要求のリスクレベルが高まる異常を検出すると、 Okta はユーザーに WebAuthn などの 2 番目の認証要素を使用するよう要求できます。

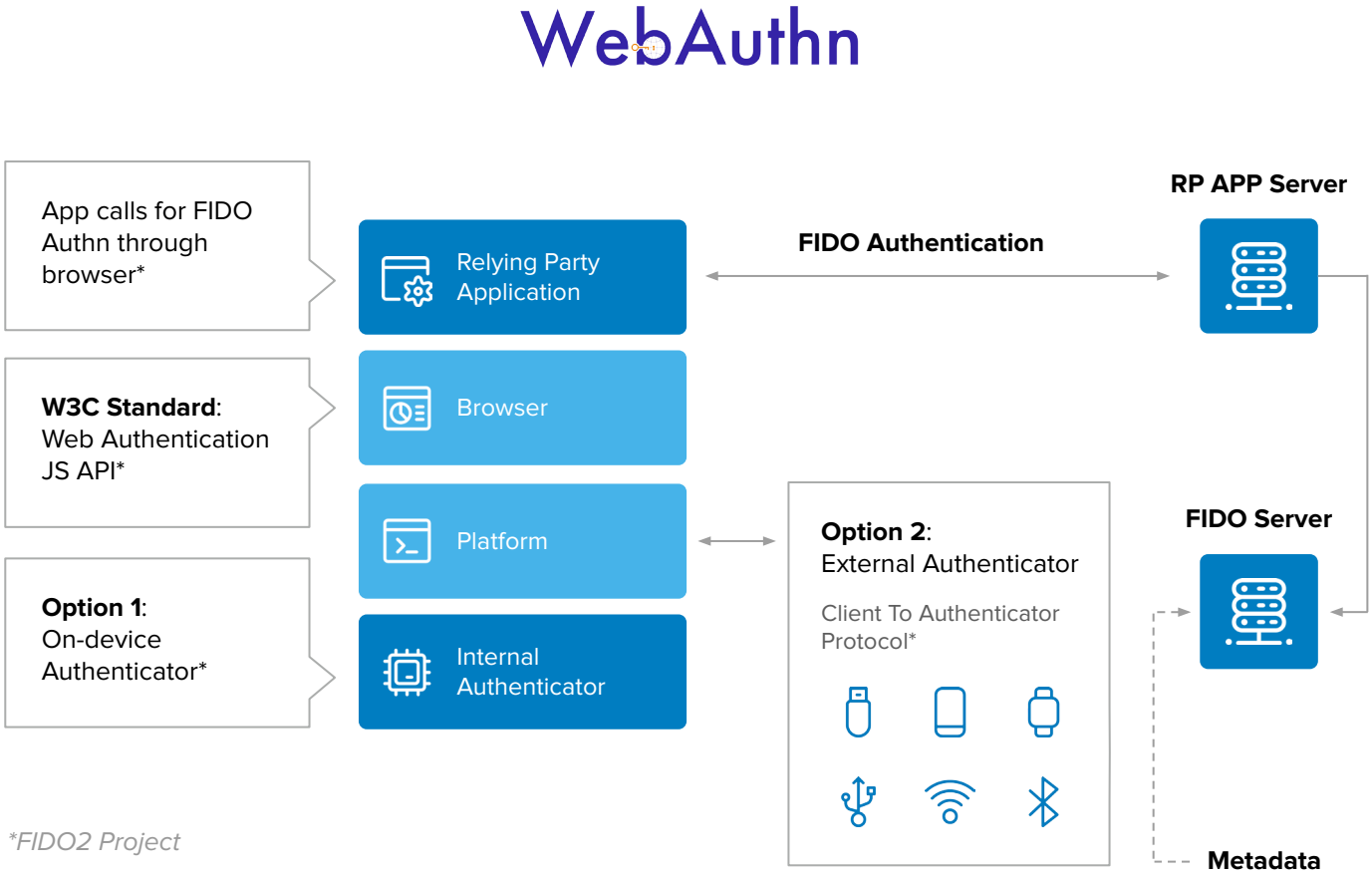
認証方法と要素を選択する際に、 管理者は保証レベルの変更を考慮する必要があります。 ユーザーのコンテキストを参照して、 状況が許せば、 より簡単なログインを許可して使いやすさを向上させることができます。 秘密の質問などの知識要素は使いやすいですが、 U2F などの所有要素に比べて安全性は低くなります。 これを念頭に置いて、 ユーザーが普段利用している本社のネットワークと場所からサインインした場合はシンプルな所有要素を選択し、デバイス、ネットワーク、場所のリスクレベルが高い場合にはよりセキュアな要素を利用することができます。



当然ながら、 管理者は企業で利用できるテクノロジに合わせて要素を選択する必要があります。 たとえば Okta Verify は、 組織の全ユーザーがスマートフォンにアクセスできなければ使用できません。 そのため、 場合によっては SMS OTP といった別の要素を使用できるようにするとよいでしょう。

ユースケース	メリット	課題
• セッションのリスクに応じてログインエクスペリエンスを変更する • 認証エクスペリエンスに保証レベルの高い要素を紐づける	• ログインの保証レベルを強化 • デスクトップとモバイルで一貫したエクスペリエンス	• ハードウェア依存の可能性

WebAuthn



WebAuthn は標準規格に基づいたパスワードレス認証フレームワークです。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強化を実現します。この新しい標準規格により、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、これらの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）での早期採用により、FIDO2/WebAuthn の導入が実現されています。WebAuthn はデバイス自体を認証に使用するため、YubiKey などのローミングオーセンティケータを利用することも、WebAuthn をサポートするプラットフォームを介して利用することもできます。

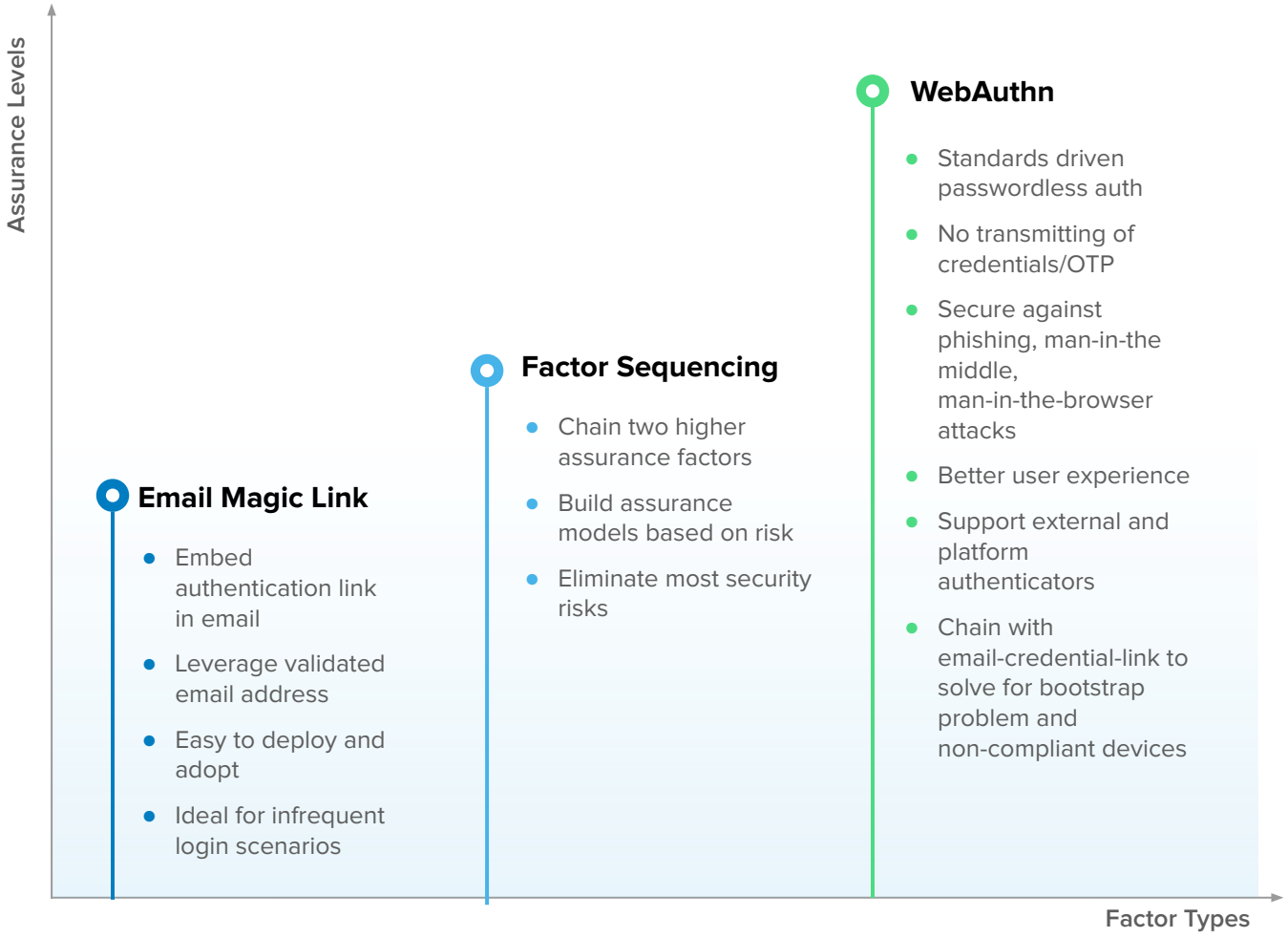
ユースケース	メリット	課題
• 標準規格に基づいたパスワードレス認証 • 拡張性のある認証エクスペリエンス	• アカウント乗っ取り: フィッシング、クレデンシャルスタッフィング、パスワードスプレー攻撃などのアイデンティティを利用した攻撃を阻止 • 資格情報の管理が不要 • ユーザー認証エクスペリエンスが向上 • パスワード管理の企業側のサポートを削減	• ハードウェアおよびブラウザでのサポートが必要 • ユーザーが自力で復旧する安全なフローが必要 • 代替認証方法として資格情報のリンクをメールで送信するなど、他のパスワード認証方法との組み合わせが必要

詳細については、 WebAuthn のホワイトペーパーをご覧ください。

パスワードのない将来に向けたプランニング

パスワードレス認証の導入は、 組織やサービスが幅広いセキュリティリスクを管理してシームレスなカスタマーエクスペリエンスを提供するための、 最も強力なインパクトのある手段の 1 つです。 現在、 パスワードレス認証を導入しようとしている企業や組織は数々ありますが、 パスワードレスは何かを大きく変えるプロセスというよりは、 今あるものを発展させるプロセスと言えます。 そのため、 真のパスワードレス認証に移行する前に、 シンプルなオプションをいくつか記載した以下のロードマップをぜひご利用ください。 パスワードレスには、 慎重な検討と計画が必要です。 セキュアな登録、 パスワードからの移行、 導入のしやすさ、復旧、オフボーディングなど、認証ライフサイクル全体について考える必要があります。すべての側面とニーズを理解した組織だけが、 パスワードレスを効果的に実現してアイデンティティ攻撃を排除し、 満足度の高いエクスペリエンスを提供して、 ビジネスを成長させることができます。

Okta を利用したパスワードレスジャーニーの実現



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 Identity Cloud 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。 20th Century Fox、 JetBlue、 Nordstrom、 Slack、 Teach for America、 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アイデンティティを保護しています。

www.okta.com/jp/