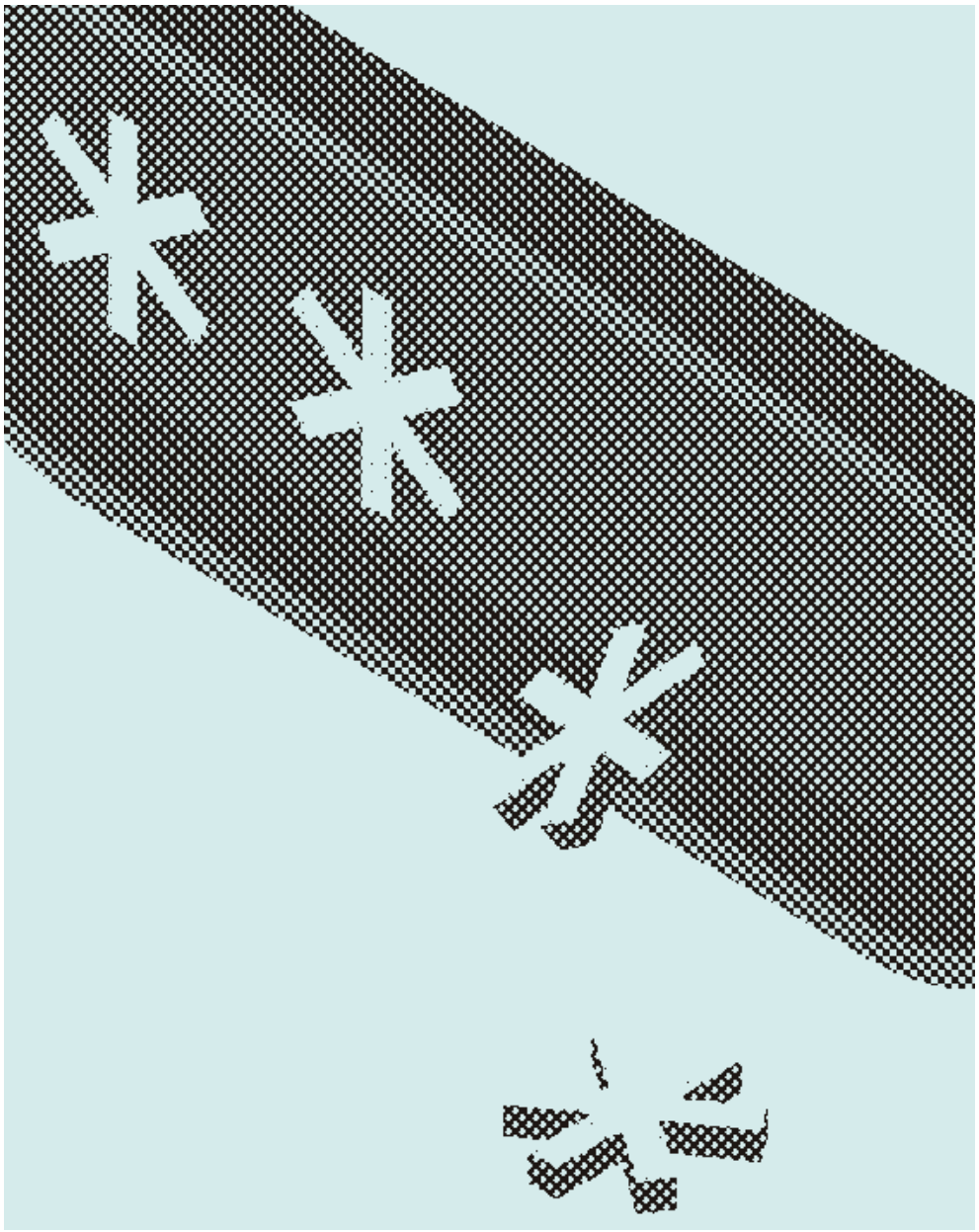
ホワイトペーパー
2022 年 3 月

# Oktaで パスワードレスを実現する方法

## Oktaパスワードレス認証オプション 摘要ガイド



〒150-0002
東京都渋谷区渋谷2丁目24-12
渋谷スクランブルスクエア38階
**Okta Japan株式会社**

Web: www.okta.com/jp/
Email: Marketing-Japan@okta.com

# はじめに

パスワードレス認証は、もはや遠い未来の夢物語ではありません。Apple の Touch ID や Face ID、Windows Hello など、消費者が日常的に利用するテクノロジーにより、パスワードを使用しないデバイスへのアクセスが可能になっています。また、仕事の場では、指紋やカードリーダー、モバイル認証アプリなどのテクノロジーがパスワードレスのエクスペリエンスを提供するのに役立っています。

パスワードからの脱却は、セキュリティとアイデンティティ / アクセス管理（IAM）の向上に向けた重要なステップです。また、毎回のログイン要求でコンテキストを考慮して認証を強化することも、同様に重要です。

では、パスワードレス認証の導入を目指して、どのように進んでいけばよいのでしょうか。多要素認証（MFA）の導入は、最終的にパスワードレスを導入するための重要な基盤となります。FIDO2.0/WebAuthn などの安全な要素や、生体認証をサポートするモバイル認証アプリは、最終的にパスワードレス認証を全社で導入するための道筋を提供します。これらの安全な要素とログインのコンテキストを併せることで、認証プロセスにおけるパスワードの必要性を廃除できます。

ここで大きな役割を担うのが Okta です。シングルサインオンと適応型多要素認証を統合する Okta のソリューションによって、パスワードレス認証を含めたアクセス判断でコンテキスト（ユーザー、場所、デバイス、ネットワークなど）に基づくリスク評価を導入できます。

たとえば、リスクの低いログインでのみパスワードレスログインを許可するように設定できます。一方、リスクの高いログインには、1 つまたは複数の強力な認証要素を要求できます。この入門ホワイトペーパーでは、従業員、顧客、消費者（B2E、B2B、B2C）にパスワードレス認証を提供する Okta のさまざまな機能を紹介します。

# パスワードレスの導入をどのように検討すべきか

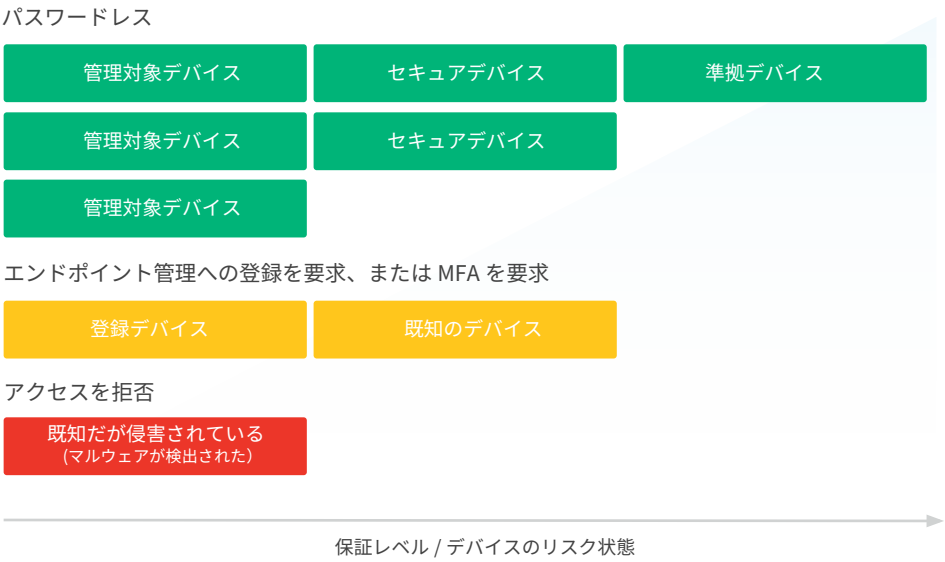
冒頭で、多要素認証の導入がパスワードレスに移行する上での基盤となることを述べました。

多要素認証は、知識要素、所有要素、固有要素のうち 2 つの要素で構成されます。たとえば、パスワードと SMS ワンタイムパスワードは知識要素と所有要素の組み合わせであり、パスワードとバイオメトリクスの組み合わせは知識要素と固有要素の組み合わせです。

さらに、言及されないことも多い第 4 のカテゴリ、つまり暗黙の要素があります。これは、必ずしもエンドユーザーに提示されるものではなく、アクセス判断の前に検討される要素です。たとえば、新しいデバイスと新しい場所の両方を使用するログインでは、より強力な要素タイプを認証に使用する必要があります。その一方で、ログインが既知のデバイスと既知のネットワークから行われる場合は、強度の低い、または中程度の要素 1 つだけを使用することが許容される場合があります。

最終的には、さまざまなリスクレベルに適切な要素を紐付けることで、パスワードレスへの移行を開始することが目標です。

たとえば、次の画像に示すように、パスワードレス認証に紐付けられるデバイスの保証レベルは多様であり、保証レベルが中程度あるいは低い場合は強力な要素が必要になったり、ログインが完全に拒否されたりする可能性があります。



# Oktaで利用できるパスワードレス認証のオプション

Okta は、ワークフォースアイデンティティとカスタマーアイデンティティの両方で、ビジネス要件に対応する多様なパスワードレス認証方式を提供します。このセクションでは、パスワードレス認証の実現に役立つ、現在 Okta で利用可能な機能、および今後提供予定の機能について紹介します。また、各ユースケース（ワークフォースアイデンティティ、カスタマーアイデンティティ）に適した機能についても説明します。

## Okta FastPass

Okta FastPass は、作業に必要なあらゆるリソース（クラウドアプリ、オンプレミスアプリ、VPN）を、あらゆるデバイスで利用するためのパスワードレス認証を可能にします。Okta に接続し、SAML、WS-Fed、OIDC をサポートするリソースであれば、Okta FastPass でログインエクスペリエンスを強化できます。その仕組みは以下のとおりです。

1. ユーザーが Okta Verify を使用して、Universal Directory にデバイスを登録します。
   Okta は、この登録エクスペリエンスをサポートするため、iOS と Android の既存の Okta Verify アプリを強化し、Windows と MacOS の新しい Okta Verify アプリを提供します。

2. 管理者が、Okta FastPass を提供するタイミングについてポリシーを設定します。
   管理者は、どのような場合に Okta FastPass を利用するか（管理対象デバイスのみ、Okta に登録されたデバイスのみ、特定のネットワークからのみ、など）を指定できます。

3. ユーザーが Okta リソースにログインする際、ユーザー名やパスワードの入力は要求されません。Okta Verify は、管理者が設定したポリシーを確認し、ログインが正しいコンテキストを満たしていることを前提として、ユーザーのログインを許可します。
   このパスワードレスエクスペリエンスは、ブラウザ（サービスプロバイダー主導のフローと Okta ダッシュボードへの直接ログインの両方）、ネイティブのモバイルアプリ、およびデスクトップのシッククライアントで機能します。

Okta FastPass は現在利用可能になっています。詳しくは、**Okta FastPass の Web ページ**をご覧ください。

**ユースケース：**ワークフォースアイデンティティ

# 要素シーケンス

要素シーケンスにより、管理者はログインのリスクとコンテキストに基づいて、一連の要素を要求できます。Okta の適応型 MFA は、適切な要素と適切なリスクレベルを組み合わせることで、安全なパスワードレス認証を可能にします。

脅威レベルが低い場合には、ログインエクスペリエンスを合理化し、ユーザーがリソースにアクセスするためのパスを簡素化できます。しかし、ログインに関連するリスクレベルが高い場合、追加の認証要素が要求されます。要素シーケンスの仕組みは以下のとおりです。

1. 管理者は、要素チェーンを定義するポリシーを作成します（組織レベルのサインオンルールを介して）。また、オプションで適応型ポリシーを組み合わせることが可能です。
   これには、パスワードの要求を廃除することも含まれます（希望する場合のみ）。

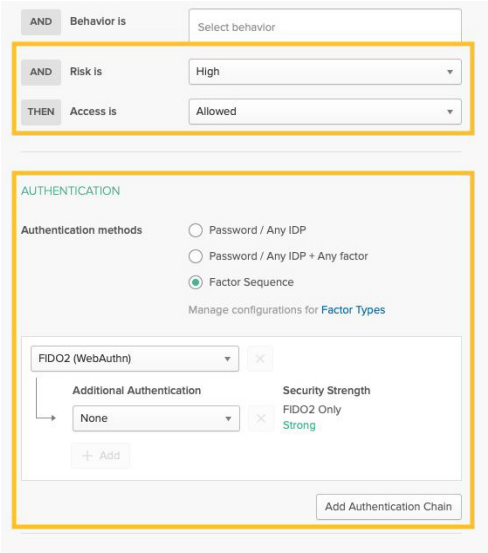
2. エンドユーザーは、管理者が定義したコンテキストと要素チェーンに基づいて、ログイン時に提示される要素を確認します。
   管理者がログインプロセスからパスワードのオプションを削除した場合、エンドユーザーは二次的要素であったものを一次的要素として使用できます。

要素シーケンスは、明確な MFA 戦略がパスワードレス認証の実現に役立つことを示す好例です。
要素シーケンスで作成できるポリシーの例をいくつか紹介します。

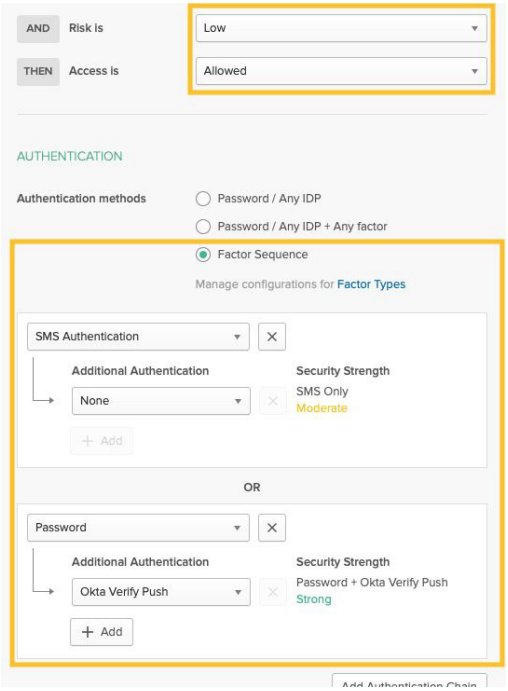
1. リスクが高い場合には、生体認証によるログイン（WebAuthn）を要求する。

2. Okta Verify の Push 認証または WebAuthn により、パスワード不要のログインを提供する。

3. パスワードの前に、パスワード以外の要素をユーザーに提示する（例：Okta Verify Push の後にパスワードを要求する）。
   これは、パスワードスプレー攻撃に対する保護に役立ちます。



4. リスクが高い場合は、WebAuthn のみを許可する。




5. リスクが低い場合は、SMS OTP またはパスワードに Okta Verify Push を追加して提供する。

**ユースケース：**ワークフォースアイデンティティとカスタマーアイデンティティ

# WebAuthn

WebAuthn はブラウザベースの API です。これによって、Web アプリケーションは登録デバイス（電話、ノート PC など）を要素として使用し、ユーザー認証を簡素化し保護します。高度なフィッシング攻撃からユーザーを保護するため、公開鍵暗号方式を使用します。現時点で、WebAuthn はフィッシングを防止する唯一の要素です。

WebAuthn の仕組みは以下のとおりです。

**オフデバイスのローミングオーセンティケーター**
ハードウェア（コンピューター、携帯電話など）に内蔵されていない、WebAuthn がサポートする要素です。

- YubiKey 5Ci
- FEITIAN BioPass
- HID Crescendo スマートカード

**オンデバイスオーセンティケーターとプラットフォームオーセンティケーター**
ハードウェア（コンピューター、携帯電話など）に内蔵された、WebAuthn がサポートする要素です。

- Windows 10 1903 以降での Windows Hello
- MacBook での Touch ID
- Android 7.0 以降での指紋認証
- iOS での Touch ID と Face ID

WebAuthn のサポートは、Web アプリでの WebAuthn API をサポートする認証プロセス、ブラウザのサポート、OS のサポート、ハードウェアのサポートに依存します。
このように言われると気後れするかもしれませんが、幸い、すでに多くのオペレーティングシステム / デバイス / ブラウザが WebAuthn をサポートしています。また、Okta は AMFA（適応型多要素認証）製品を通じて WebAuthn をサポートしています。

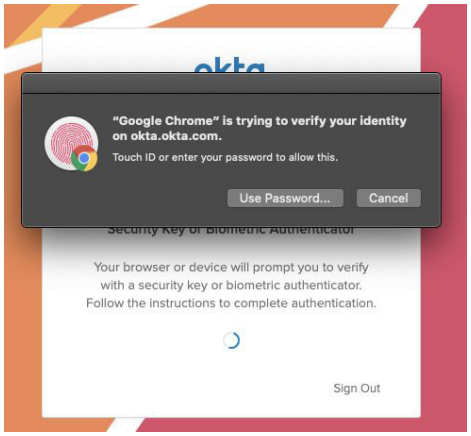
**WebAuthn のメリット（SMS OTP やモバイル認証アプリと比較した場合）**

- 標準ベースのアプローチにより、安全なパスワードレス認証を実現する
- ユーザーが登録する各 WebAuthn 要素の公開鍵 / 秘密鍵のペアにより、フィッシングを防止する
- エンドユーザーに最善のエクスペリエンス（生体認証による迅速でシームレスなログイン）を提供する
- デバイスのログインやロック解除に使用するのと同じ生体認証で、アプリにアクセスできる
- デバイスとセキュリティキーのオプションを複数提供する

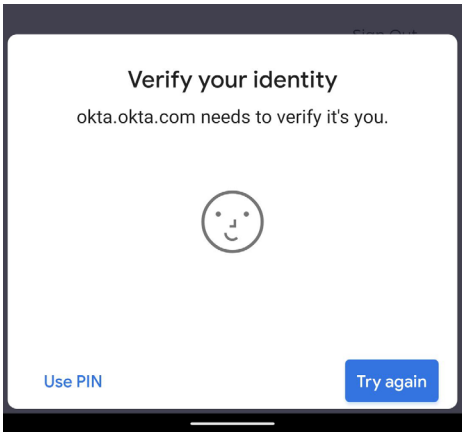
**WebAuthn をサポートするブラウザ、ハードウェア、OS の例**

- MacOS 上の Google Chrome で、Touch ID を使用する
- Windows 10 上の Google Chrome で、Windows Hello を使用する
- Windows 10 上の Microsoft Edge で、Windows Hello を使用する
- Windows 10 上の Firefox で、Windows Hello を使用する
- Android 7.0 以降を実行する指紋認証対応デバイス上の Google Chrome で、指紋認証を使用する
- Windows/MacOS で、WebAuthn 対応ブラウザを使用するデスクトップアプリにより、Windows Hello/Touch ID を使用してログインする
- Android 7.0 以降を実行する指紋認証対応デバイスで、WebAuthn 対応ブラウザ（Chrome など）を使用するネイティブのモバイルアプリによりログインする

WebAuthn は、組織全体でパスワードレスを安全に実現する手段となります。




MacOS の Touch ID




Android の Face Unlock

**ユースケース：**ワークフォースアイデンティティとカスタマーアイデンティティ

## PIV スマートカード

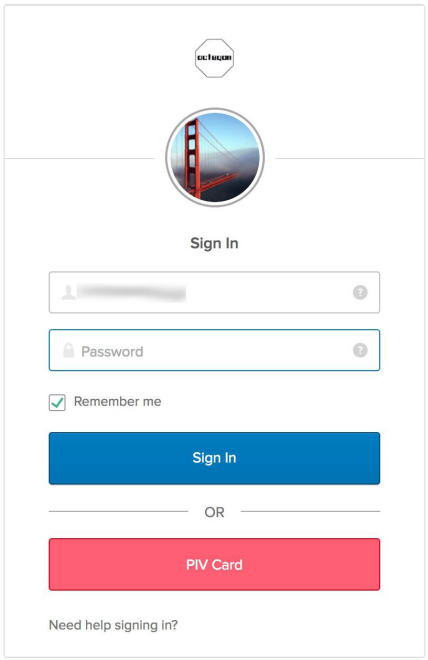
2004 年、当時のブッシュ大統領が発動した国土安全保障大統領令 12 号（HSPD12）により、米国のすべての連邦職員と請負業者に対する、どこでも使用可能な共通の身分証明書の交付が義務化されました。この大統領令を受けて、国立標準技術研究所（NIST）の情報テクノロジー研究所は、民間企業や他の連邦機関と協力して、政府機関に共通のアイデンティティシステムの標準を開発しました。

個人認証（PIV）システムの標準となる連邦情報処理標準（FIPS）は、X.509 に準拠した証明書と鍵のペアを使用するスマートカードの使用に基づきます。具体的には、物理的なカードに、所有者だけがアクセスできるデジタルファイルが格納されます。これを使用することで、PIV 資格情報が、認可されたエンティティにより発行され、有効期限が切れておらず、取り消されておらず、資格情報の保持者が発行先の個人と同じ人物であることを検証できます。

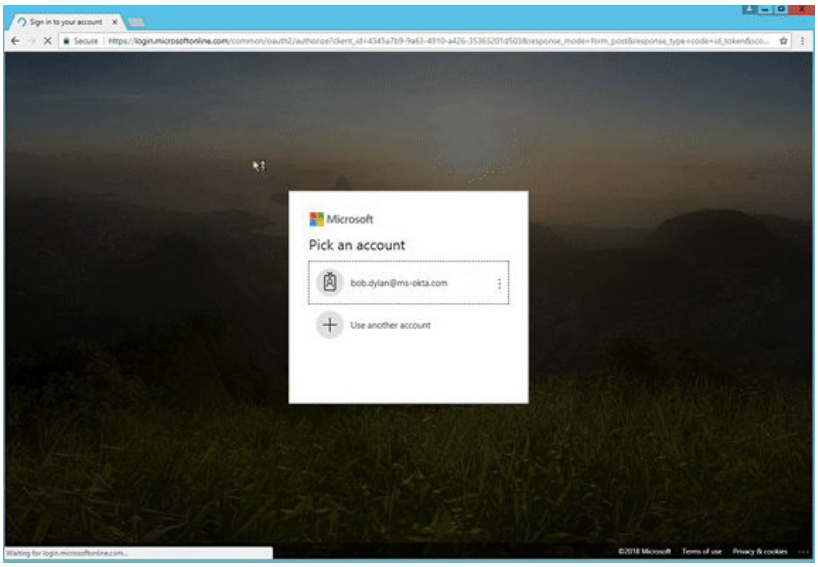
どの業種も PIV ベースの認証を適切に利用できるとは限りませんが、パスワードレス認証の一形態として Okta の PIV 認証を実装できます。その仕組みは以下のとおりです。

1. 管理者は、Okta 組織でスマートカードを「アイデンティティプロバイダー」として有効にします。
   そのために、ルート証明書を Okta にアップロードし、PIV またはスマートカードによるログインが必要とされる条件を定義するルーティングルールを構成します。

2. スマートカードが構成されると、エンドユーザーが Okta にログインする際に PIV カードオプションが表示されます（以下のスクリーンショットを参照）。




3. エンドユーザーは、Okta 認証画面にリダイレクトされ、そこで PIV をログイン資格情報として使用できます。PIV カードに保存されている証明書を選択して PIN を入力すると、ログインできます。ユーザー名やパスワードを使用する必要はありません。




**ユースケース：**ワークフォースアイデンティティ

# デスクトップシングルサインオン

デスクトップシングルサインオン（DSSO）を使用する場合、ユーザーがデバイス（Windows、MacOS）上の Active Directory ネットワークにサインインすると、Okta によって自動的に認証されます。認証後、ユーザーは追加のユーザー名やパスワードを使用せずに、Okta を通じてアプリケーションにアクセスできます。DSSO を使用するとき、ユーザーは一度サインインするだけで済み、Okta を通じてアクセスするアプリケーションごとに個別の資格情報を使用する必要がありません。このため、ユーザーエクスペリエンスが向上します。DSSO の実装には 2 つの方法があります。

- エージェントレス（推奨）
- IWA Web エージェントをオンプレミスで実行

Okta のデスクトップシングルサインオンの仕組みは以下のとおりです。

1. ユーザーは、デスクトップのログインページで AD の資格情報を入力します。
2. ブラウザ経由、または最新の認証をサポートするデスクトップのシッククライアント経由で Okta にアクセスするとき、ユーザーは追加の資格情報を要求されません（MFA が必要となる場合を除きます）。

デスクトップシングルサインオンと前述の Okta FastPass 機能は何が違うのかと、疑問に思われるかもしれません。Okta FastPass のメリットは、パスワードレスのエクスペリエンスを実現するために、デバイスが Active Directory のドメインに参加している必要や、ネットワーク上に存在している必要がないことです。また、Okta FastPass は Windows、MacOS、iOS、Android にわたって利用できます。

**ユースケース：**ワークフォースアイデンティティ

## Device Trust の統合（SAML 経由）

Okta の Device Trust 機能を使用すると、管理者は管理対象デバイスと非管理対象デバイスにアクセスポリシーを設定できます。多くの場合に、管理対象デバイスから Okta へのアクセスは許可し、非管理対象デバイスからのアクセスには、最低限でも MFA を求めるか、または拒否します。「管理対象」とは、Jamf、VMware Workspace ONE、Microsoft Intune などのエンドポイント管理ソリューションによって管理されるデバイスを指します。

VMware Workspace ONE など、一部のソリューションにはパスワードレス機能が組み込まれています（「モバイルシングルサインオン」とも呼ばれることも多い機能です）。Okta は、これらのソリューションとの統合により、エンドユーザーに手間やストレスをかけないアクセスを提供します。Device Trust の SAML 統合の仕組みは以下のとおりです。

1. 管理者が Okta の IdP 検出機能を利用し、エンドポイント管理ソリューションへのログインをルーティングします。
   このために、エンドポイント管理ソリューションは独自の軽量なアイデンティティソリューション（VMware Workspace ONE、MobileIron Access など）を提供する必要があります。
2. エンドポイント管理ツールが、デバイスが管理対象かどうかをチェックします。
   管理者は、デバイスが管理対象かどうかに応じてポリシーを構成し、アクセスの拒否、登録の要求、アクセスの許可、MFA の要求のいずれかを指定できます。
3. 管理対象デバイスでは、ユーザーは追加の資格情報を要求されず、シームレスにアプリケーションにログインできます。

Device Trust の統合については、**ブログ**で詳しくご紹介しています。

**ユースケース：**ワークフォースアイデンティティ

## メールマジックリンク

近く提供予定

メールベースのパスワードレス認証は、消費者のユースケースで一般的になっています。この方法では、パスワードリセットのフローが中心になります。秘密のリンクを受信したユーザーは、パスワードを使用せずに新しいパスワードを設定できます。多くのユーザーにとっては、何十回、何百回と使っている馴染みのある方法です。

この認証方式は、Slack や Medium などのアプリによって普及しました。真の意味でのパスワードレス認証は、パスワードリセットのフローをさらに一歩進めたものとなります。メールマジックリンク機能の仕組みは以下のとおりです。

1. ユーザーは、メールアドレスを入力するだけで、アプリに登録 / ログインできます。
2. アプリは、メールで送ったリンクをクリックして認証プロセスを完了するように求めます。
3. ユーザーがメールのリンクをクリックすると、アプリにリダイレクトされ、ログインが完了します。

アプリの設計者は、パスワード（および関連するリセットの手続き）を廃除し、時間またはユーザーライフサイクルの制限があり、一回だけ使用可能な秘密のリンクをユーザーのメールアドレスに送信するように簡素化します。このリンクをクリックすると、ユーザーが認証され、ログイン状態を持続するための長い有効期間を持つ Cookie が設定されます。ユーザーがパスワードを設定 / 保存 / 入力する必要が一切なく、特にモバイルデバイスでは魅力的な機能です。
この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とってはメリットが大きい方式です。

**ユースケース：**カスタマーアイデンティティ

| 機能 | ユースケース |
| --- | --- |
| **Okta FastPass**<br>Windows、iOS、Android、MacOS に対応するデバイスベースのパスワードレス認証。オンプレミスのディレクトリや特定のエンドポイント管理ツールに依存しない | ワークフォース アイデンティティ |
| **要素シーケンス**<br>ユーザー、デバイス、場所のコンテキストとの組み合わせを使用して、要素の連鎖を定義する | ワークフォース アイデンティティ、カスタマー アイデンティティ |
| **WebAuthn**<br>FIDO2.0 標準に基づく生体認証。フィッシングを防止する | ワークフォース アイデンティティ |
| **PIV スマートカード**<br>x509 証明書による認証。主に米国連邦政府機関で使用される | ワークフォース アイデンティティ |
| **デスクトップシングルサインオン**<br>AD ドメインに参加したマシン向けに、パスワードレスのログインを提供する | ワークフォース アイデンティティ |
| **Device Trust の統合**<br>エンドポイント管理ソリューションのモバイルシングルサインオン機能を活用して、パスワードレスを実現する | ワークフォース アイデンティティ |
| **メールマジックリンク（近く提供予定）**<br>メールベースのパスワードレス認証。消費者向けアプリでの使用に最適である | カスタマー アイデンティティ |

## さらに詳しく知る

このホワイトペーパーでは、Okta が提供する多様なパスワードレス機能の概要を説明しました。パスワードレスの導入における考慮事項、機能のメリットや課題についての詳細は、**パスワードレスの実現**をご覧ください。多要素認証の活用を通じたパスワードレスの実現についての詳細は、**Okta の適応型 MFA の Web ページ**をご覧ください。

## Oktaについて

Okta は、企業向けのアイデンティティ管理ソリューションを提供する最先端の独立企業です。Okta Identity Cloud は、適切なタイミングで適切なユーザーを適切なテクノロジーへと安全に接続します。6,500 以上のアプリケーションやインフラストラクチャとの統合機能が事前に用意されているため、Okta のお客様はビジネスにおいて最善のテクノロジーを簡単かつ安全に活用できます。20th Century Fox、JetBlue、Nordstrom、Slack、Teach for America、Twilio など、8,400 以上の組織が Okta を信頼し、従業員や顧客のアイデンティティ保護に役立てています。詳しくは、**okta.com** をご覧ください。