ホワイトペーパー

アイデンティティベース攻撃の分析

ユーザーに関連する脅威からの防御方法

目次

セキュリティにおけるアイデンティティの役割

従来、組織のセキュリティ戦略におけるアイデンティティの役割は、認証時に正規のユーザーを確認し、適切なアクセスを付与することに限られていました。しかし、攻撃者がユーザーとその認証情報を標的にするケースが増える中、アイデンティティとアクセス管理（IAM、Identity and Access Management）システムは、こうした脅威に対抗するためのセキュリティ機能を拡張してきました。さらに、ゼロトラスト戦略を推進するセキュリティリーダーにとっても、アイデンティティは防御を強化する上で中心的な役割を果たすようになっています。

現在、アイデンティティは組織のサイバーセキュリティ戦略の重要な要素となりつつあります。リモートワークの普及、非管理デバイスの増加、クラウドや SaaS 環境の広がりにより、アイデンティティは、業務に必要なデバイス、アプリ、リソースと従業員をつなぐ唯一の要素となっています。アイデンティティプロバイダーは、このつながりを活用して多様な機能を提供しています。

IT 全体に統合された唯一のテクノロジーとして、アイデンティティは IT セキュリティで協調的なアプローチを促進する独自の立場にあります。Okta Workforce Identity Cloud は、独自のセキュリティ制御と他のシステムの制御を活用し、リスクの評価、脅威の排除、サイバーセキュリティ態勢の向上を支援します。セキュリティでアイデンティティを活用するアプローチには、以下のメリットがあります。

- IAM、アイデンティティガバナンス / 管理（IGA、Identity Governance and Administration）、特権アクセス管理（PAM、Privileged Access Management）を統合したプラットフォームにより、アイデンティティポリシーを統一し、可視性を高め、制御を強化する
- 単独で、またはお客様が現在お使いのセキュリティ製品と連携して、潜在的な脅威を検出する
- 認証前、認証時、認証後のリスクを継続的に評価する
- リアルタイムの情報に基づき、脅威にアダプティブに対応する

このホワイトペーパーでは、今日の組織に影響を及ぼしている以下の脅威の拡大を考察し、認証前、認証時、認証後の脅威に対する防御、検出、対応で Okta が果たす役割を解説します。

- フィッシング
- エンドユーザーデバイスの侵害
- 内部脅威
- 認証後の脅威
- 総当たり攻撃

アイデンティティとセキュリティに関する統計

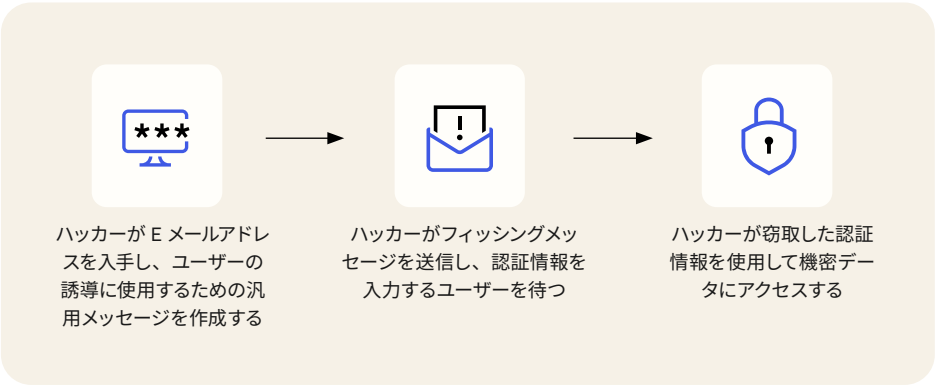
- **2022** 年には、データ侵害の **45%** で窃取された認証情報が使用されました（前年の **42%** から増加）[1]。
- 全データ侵害の**74%**は、人為的な要因によるものであり、誤操作、特権の不正使用、窃取された認証情報の使用、またはソーシャルエンジニアリングが関与しています [1]。
- Web アプリケーションの侵害の **86%** では、窃取された認証情報の使用が関与しています [1]。

[1] Verizon：2023 年度データ漏洩 / 侵害調査報告書

フィッシング

フィッシング詐欺は、米国で最も多く報告されているインターネット犯罪であり、被害者に最も大きな経済的損失をもたらしています[2]。攻撃者は、AI と自動化を活用して大規模にフィッシング攻撃を仕掛けており、その結果、検出や追跡がますます困難になっています。フィッシング攻撃の多くは、ユーザーを偽の Web サイトに誘導し、認証情報を入力させるよう仕向ける E メールから始まります。こうした E メールや Web サイトは、本物らしく見えるように作られており、信憑性のあるブランドロゴや表現を使用し、ターゲットの E メールアドレスに似た送信元アドレスを用いることが一般的です。攻撃者は、窃取した認証情報を使ってログインし、これを足がかりにして、以下のような大規模な攻撃を実行します。

- 組織のシステムにランサムウェアをインストールして支払いを要求する
- ビジネス E メール詐欺（BEC）を実行し、自身が管理する銀行口座へ資金を送金させようとする（給与振込や請求書の口座番号を変更するなど）
- アプリケーションから機密データを抽出し、ダークウェブで販売する



毎日世界中で送信される 1 億 5,600 万通以上のフィッシング E メールに対抗するため、多くの組織がスパムフィルター、E メールセキュリティソフトウェア、アンチウイルス、Web フィルター、ユーザー教育プログラムに投資しています。しかし、攻撃が高度化するにつれ、これらの従来の防御策が回避されるケースが増えています。同様に、多要素認証（MFA）はフィッシングを含む認証情報の窃取を防ぐための最も信頼できる手法とされてきましたが、最近の大規模な攻撃により、MFA だけではすべてのデータ侵害を防ぐには不十分であることが明らかになっています。MFA は、中間者攻撃（AiTM）、SIM スワッピング攻撃、Pass-the-Cookie 攻撃、MFA 疲労攻撃（MFA 爆撃攻撃とも呼ばれ、攻撃者が MFA プッシュ通知を繰り返し送信する手法）などに対して脆弱になる可能性があります。MFA が有効であるためには、回避やハッキングに対して強靭であることが求められます。

[2] 米連邦捜査局（FBI）：2022 年版インターネット犯罪レポート

緩和策

1. **ユーザー向けのツールとトレーニング：**フィッシング攻撃はユーザーを標的とするため、予防策として適切なツールをユーザーに提供する必要があります。
    a. MFA 疲労に関するユーザー教育のために、Okta Workflows を活用して偽の MFA プロンプトを送信するフィッシングシミュレーションキャンペーンを実施できます。
    b. Okta HealthInsight を活用して、アカウントの認証の変更を簡単にエンドユーザーに通知できます。また、ユーザーはこの機能を利用して、不審な認証イベントを手軽に報告できます。
2. **最小権限アクセス：**Okta Identity Governance（OIG）は、ユーザーが自身の役割やプロジェクトに必要なリソースにのみ、一定の期間に限りアクセスできるよう制限するアクセス制御を提供し、フィッシングやその他のソーシャルエンジニアリング攻撃が成功した場合のラテラルムーブメントのリスクを低減します。また、OIG はクラウドおよびオンプレミスのリソース全体で、入社 / 異動 / 離職プロセスを自動化して管理し、定期的なアクセス認証を実施します。この自動化により、攻撃者が休眠アカウントを悪用してフィッシング攻撃を仕掛けたり、不正アクセスを試みたりするリスクを低減します。
3. **ステップアップ認証：**Okta Adaptive MFA の動作の検出機能は、ユーザーの行動パターンを分析し、過去のアクティビティに基づいて典型的なプロファイルを作成します。これにより、ユーザーの行動に変化があった際に自動的に対応するポリシールールを構成でき、たとえば、異なる国や IP アドレスからのサインイン試行時に追加の要素を要求することが可能です。
4. **フィッシング耐性のある認証：**フィッシング耐性のある認証は、セキュリティ質問などの共有シークレットを排除することで、攻撃者による MFA の回避を防ぐよう設計されています。また、攻撃者が用意した偽のドメインにユーザーが認証情報を入力するのを防ぐ機能も備えています。Okta は以下の手法をサポートしています。
    a. フィッシング耐性のあるすべての主要な認証方法：FIDO2 WebAuthn オプション、PIV/CAC スマートカードを含む
    b. Okta FastPass：フィッシング耐性のあるパスワードレスの認証器であり、ゼロトラストに基づき、管理対象デバイスと非管理デバイスの両方に対応

5. **脅威の検出：**セキュリティチームは、主要な E メールプロバイダーとの Okta の統合を活用し、リスクに基づいたアダプティブな認証ポリシーを構成できます。たとえば、E メールレイヤーで脅威が検出された場合、Okta のポリシーに沿ってステップアップ認証を要求したり、ユーザーアカウントをロックしたりすることが可能です。Identity Threat Protection with Okta AI は、E メールセキュリティベンダーを含むさまざまなセキュリティソリューションからのセキュリティシグナルを活用します。これらのベンダーがフィッシング E メールや悪意のあるリンクを検出すると、Okta に通知され、ユーザーのリスクレベルが引き上げられ、適切な対応がインラインで実行されます。
6. **脅威への対応：**検出にとどまらず、Identity Threat Protection はポリシーの構成と評価されたユーザーのリスクレベルに基づき、適切な対応を調整します。たとえば、リスクが中程度の場合は、SIEM やインシデント対応チームへの通知が送信されることがあります。一方、リスクが高い場合は、ユーザーの再認証の要求、ユーザーセッションの終了、またはサポートされるアプリケーションからの強制ログアウト（機能が有効になっている場合）が実行されることがあります。

エンドユーザーデバイスの侵害

リモートワークと BYOD の普及により、ユーザーのスマートフォン、ノートパソコン、その他のデバイスに対する脅威が増大しています。フィッシング耐性のある認証の導入が進むにつれ、攻撃者は組織への侵入手段としてデバイスの侵害を狙う可能性もあります。

サイバー攻撃は、エンドユーザーのデバイスを侵害することから始まることが多く、ユーザーをだましてマルウェアをインストールさせるといった手口が使用されます。このマルウェアは認証情報を窃取し、フィッシングと同様に、攻撃者が組織内でラテラルムーブメントを行い、ランサムウェアの拡散、機密データの窃取、BEC の実行を可能にします。アイデンティティは、デバイスのセキュリティを増強し、認証時および認証後にデバイスを検証することで、エンドポイント攻撃の防止や検出に貢献できます。

緩和策

1. **デバイス信頼：**デバイス信頼は、信頼された管理対象デバイスを使用するユーザーのみが環境にアクセスできるようにする仕組みです。Okta は、各管理対象デバイスが適切なセキュリティ態勢を備えていることを確認した上で、ユーザーのログインを許可することでデバイス信頼を強化します。Okta Verify アプリは、モバイルデバイス管理（MDM）およびエンドポイント検出 / 対応（EDR）ツールと統合し、サインイン時にデバイスのシグナルを取得します。Okta は、これらのシグナルと設定されたポリシーに基づき、アクセスを判断します。
2. **デバイス保証：**非管理デバイスや、MDM や EDR に対応していない管理対象デバイスに対して、Okta Verify はデバイスのヘルスチェックを実施し、設定されたポリシーに基づいてアクセスを判断できます。たとえば、ディスク暗号化や最新の OS バージョンを必須とし、ジェイルブレイクされたデバイスの使用を禁止することが可能です。認証後、FastPass はユーザーが新しいアプリを開くたびにバックグラウンドでデバイスチェックを継続します。デバイスが返す情報によっては、FastPass が再認証を要求したり、アプリへのアクセスを拒否したりすることがあります。
3. **デバイスアクセス保護：**Okta Device Access は、ユーザーのデスクトップへのサインインにも同じ安全な MFA エクスペリエンスを適用し、デバイスに対する追加の保護を提供します。Device Access は、インターネット接続がなくてもユーザーのアイデンティティを確認し、アクセスを許可できます。

4. **許可アプリケーションフィルター：**管理者は許可リストを作成し、ユーザーデバイス上の悪意のあるアプリケーションや未確認のアプリケーションがFastPass を悪用して不正アクセスするのを防ぐことができます。
5. **脅威の検出と対応：** Identity Threat Protection は、主要 EDR ベンダーと統合し、デバイスのマルウェアスキャンと対応を実施します。自動対応には、リアルタイムのリスク評価に基づいて、再認証の要求や、侵害されたデバイスからのユーザーの強制ログアウトなどのアクションが含まれます。

内部脅威

内部脅威が増加しており、その中には情報を窃取したり損害を与えたりする意図的な攻撃も含まれます。しかし、内部インシデントの 55%は、デバイスの保護を怠る、セキュリティアップデートを適用しない、企業のセキュリティポリシーに従わないといった従業員の過失によるものです。その他の内部脅威には、意図しないミスや、新たな攻撃手法に騙されるケースも含まれます。昨年、内部インシデントの封じ込めには平均 86 日を要し、1 組織あたりの内部リスクの平均コストは 1,620 万ドルに増加しました [3]。

アイデンティティは、組織の内部リスク管理プログラムにおいて重要な役割を果たします。たとえば、組織の 56% [3] が、特権認証情報や特権アカウントへの誤った、または悪意のあるアクセスを防ぐために、特権アクセス管理（PAM）ソリューションを導入していると報告しています。同様に、IGA システムも内部脅威が組織に与える影響を最小限に抑えるのに役立ちます。

[3] Ponemon Institute：内部脅威による損失グローバルレポート、2023 年

緩和策

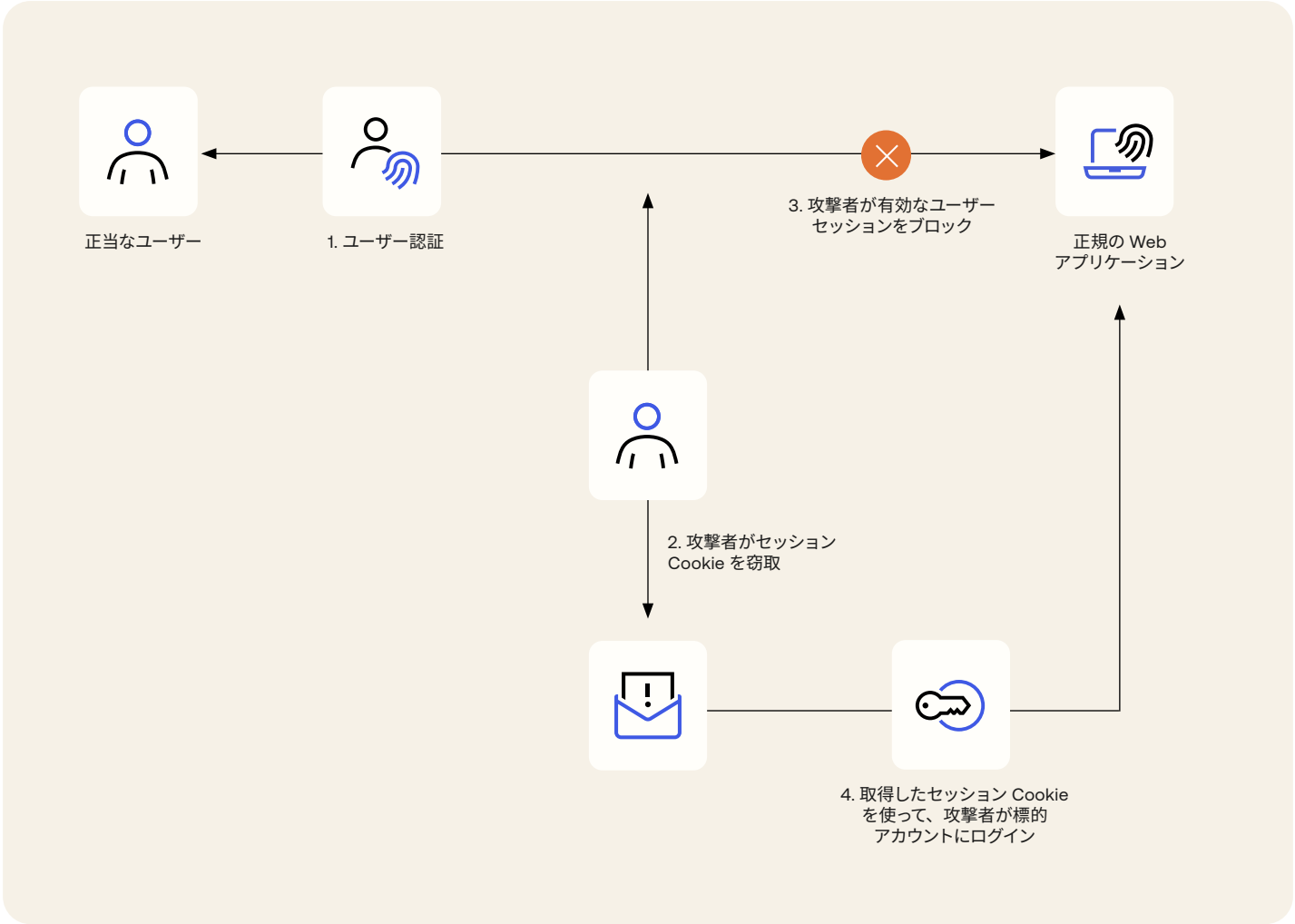
1. **デバイスアクセス保護：**内部関係者がノートパソコンを紛失したり、安全でない場所に放置したりした場合、Device Access が提供する追加のセキュリティ対策により、インターネットに接続されていなくても未確認のユーザーがデバイス内のデータにアクセスするのを防止できます。
2. **最小権限アクセス：**Okta Identity Governance を利用することで、内部ユーザーが自身の役割やプロジェクトに必要なアプリやリソースのみにアクセスできるよう制限するプロセスを構築できます。これにより、貴重な情報への不適切なアクセスリスクを最小限に抑制できます。管理者は、アクセス権が一定期間後に自動的に失効する設定や、適切なアクセスかを確認するための Access Certification キャンペーンを利用できます。
3. **特権アカウントアクセス：**内部ユーザーが機密リソースに不適切にアクセスするリスクを低減します。Okta Privileged Access は、スタンディングアクセスを排除し、共有アカウントを保護し、使用履歴の個別追跡を可能にすることで、重要なリソースを保護します。Okta は、重要な PAM 機能を IAM および Identity Governance と統合し、単一プラットフォームで特権アカウントおよびリソースの可視性を向上させ、ポリシー適用を簡素化します。この統合により、IAM、IGA、PAM を個別のツールで管理する必要がなくなり、セキュリティが強化されます。また、IAM でユーザーのリスクレベルを引き上げる行動やシグナルは、自動的に Privileged Access へ伝達され、適切な対処が行われるため、悪意のある内部関係者や過失による特権付き認証情報の不正利用リスクを低減します。
4. **脅威の検出：**正規のユーザーであっても、組織のリソースを不適切に使用することがあります。Identity Threat Protection with Okta AI は、EDR ソリューション、クラウドアクセスセキュリティブローカー（CASB）、SIEM などのセキュリティツールと連携します。これらのツールは、ユーザーがディレクトリから大量のファイルをダウンロードするなどの不審な行動を検出し、ユーザーのリスクレベルの上昇を Okta に通知します。
5. **脅威への対応：**他の攻撃と同様に、Okta はユーザーのリスクプロファイルが上昇した場合に、自動的かつ適切に対応し、再認証を要求したり、アクセスを制限したり、対応機能が有効なアプリケーションからユーザーを強制ログアウトさせたりできます。

認証後の脅威

初回ログインのセキュリティ対策だけではもはや不十分です。多要素認証やフィッシング耐性のある認証の導入が進むにつれ、攻撃者にとってログイン時の認証情報の窃取は困難になります。その結果、認証後のユーザーやデバイスを標的とする攻撃が増加すると考えられます。すでにいくつかの大規模なデータ侵害により、認証後の攻撃のリスクが明らかになっています。

セッションハイジャック

ユーザーが特定のアプリケーションサーバーへの認証に成功すると、そのサーバーはセッショントークンや Cookie を生成し、ユーザーのブラウザに保存します。セッションハイジャックでは、クロスサイトスクリプティング（XSS）攻撃、マルウェアのインストール、セッションスニッフィングなど、さまざまな手法によりセッショントークンが窃取される可能性があります。攻撃者が有効なセッショントークンを取得すると、そのアプリケーション内で正規ユーザーと同じ権限で操作を実行できます。



緩和策

1. **リスク軽減の構成：**Okta は、セッション窃取のリスクを軽減するために、さまざまな構成オプションを提供しています。

    a. ユーザーセッションの有効期限を特定の時間またはアイドル時間で設定することで、攻撃者がセッショントークンを窃取 / 悪用できる時間を短縮できます。

    b. 同様に、Okta Identity Governance は、ユーザーの役割やプロジェクトに基づいてアプリケーションのきめ細かなタイトルメントをプロビジョニングし、特定のアプリケーション内で攻撃者が実行できる操作を制限することで、セッション Cookie の窃取に伴うリスクを軽減します。

    c. 新しいアプリにアクセスするたびにユーザーに再認証を要求するよう、認証ポリシールールを設定できます。FastPass を使用したパスワードレス認証により、ユーザーの負担を最小限に抑えることができます。

2. **追加の VPN セキュリティ：**仮想プライベートネットワーク（VPN）は、セッションスニッフィングを防ぐ有効な手段です。しかし、多くの VPN はユーザー名とパスワードのみで認証を行うため、攻撃のリスクが伴います。Okta は多くの VPN ベンダーと統合し、MFA やフィッシング耐性のある MFA を追加することで、公共 WiFi ネットワーク利用時のスニッフィング攻撃の成功率を低減します。

3. **セッションリスク分析：**ユーザーが認証された後も、Identity Threat Protection は継続的にユーザーセッションを監視し、不審な行動や通常とは異なる行動を検出します。行動分析はアナリティクスによって強化されます。さらに、Identity Threat Protection は Okta Verify やサードパーティのセキュリティツールからのシグナルを受信し、セッションリスクをリアルタイムに可視化します。

4. **コンテキストの再評価：**さまざまな種類のデバイスを導入している組織向けに、FastPass は認証済みユーザーが新しいアプリケーションを開くたびにデバイスのヘルスチェックを自動で実行します。これにより、アクセスを許可する前にデバイスやそのセキュリティ態勢に変更がないことを確認し、セッションハイジャックのリスクを低減します。

5. **特権アカウント：**Okta Privileged Access は、セッション攻撃のリスクを最小限に抑えるため、正当な必要性を持つ認可された担当者のみに特権アカウントへのアクセスを許可し、セッション中の権限範囲を制限します。

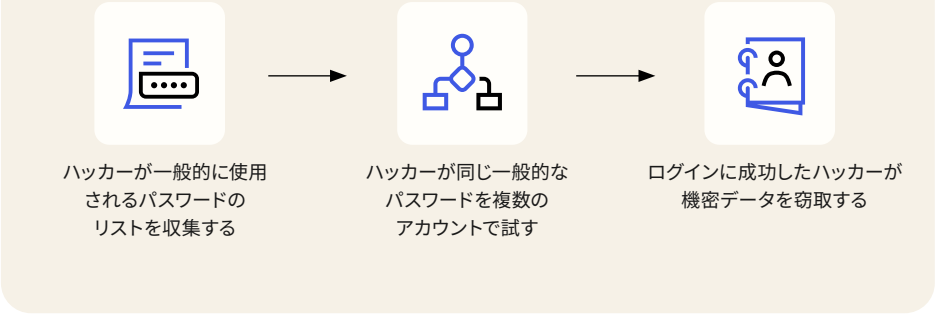
6. **脅威への対応：**Okta は、ユーザーセッションで特定されたリスクに適応的に対応し、再認証を要求したり、セッションを完全に終了させたりできます。一方で、Identity Threat Protection は、リスクの低いユーザーに対してセッションの有効時間を延長し、ユーザーエクスペリエンスを向上させます。

総当たり攻撃

総当たり攻撃は、ユーザーが弱いパスワードを使用したり、既存のパスワードを使い回したりする限り、なくなりません。

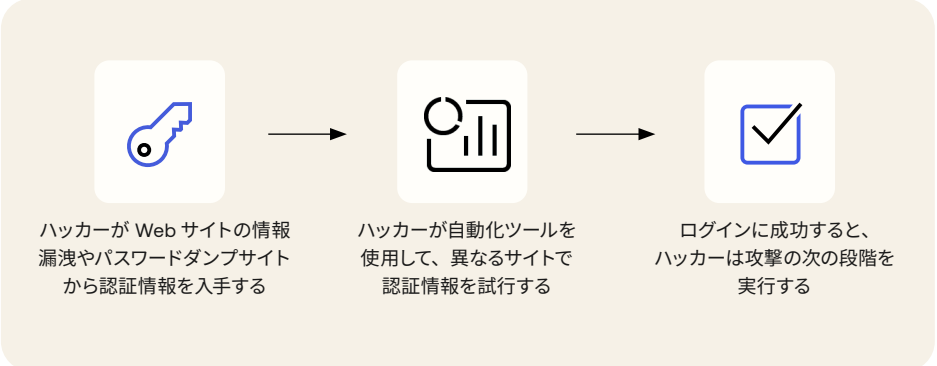
パスワードスプレー

パスワードスプレー攻撃は、特定のユーザーやアカウントを狙うのではなく、大量の試行を行うことで成功を狙う手法です。攻撃者は、一般的に知られているパスワードを複数のアカウントに対して試し、いずれかのユーザーがそのパスワードを使用していることを期待します。多くの場合、アカウントロックのしきい値を超えないように、少数のパスワードを多数のアカウントに試すことで検知を回避しようとします。また、攻撃の成功率を高めるため、攻撃者は標的の組織を調査し、システムが特定の長さや特殊文字を含むパスワードを要求しているかを確認することがあります。



クレデンシャルスタッフィング

クレデンシャルスタッフィング攻撃では、攻撃者がオンライン上のデータダンプから収集した有効な認証情報を多数の異なるサイトで試し、どれかでログインできることを狙います。この攻撃は、ユーザーが複数のサイトで同じパスワードを使い回す傾向を悪用するものです。攻撃者は自動化ツールを使用し、短時間で膨大な数のシステムに対して試行を行います。この攻撃が成功しやすいのは、有効な認証情報を使用しているため、パスワードロックの仕組みが作動しないためです。



緩和策

1. **ユーザー向けのツールとトレーニング：**パスワードを使用している場合に、以下が有効です。

    a. パスワードの使い回しを減らすことで、クレデンシャルスタッフィング攻撃の成功率を下げることができます。そのための一つの方法として、ユーザーが強力なパスワードを作成する負担を軽減することが挙げられます。Okta のブラウザプラグインは、一意のパスワードを提案し、新しいアカウント作成時に自動保存できます。

    b. Okta は、アカウント作成時にパスワード要件を適用することで、一般的に使用されるパスワードを避けるよう支援し、パスワードスプレー攻撃のリスクを低減できます。詳しくはこちらをご覧ください。

2. **悪意のある IP の検出：**ThreatInsight は、Okta のお客様基盤全体でデータを集約し、認証情報を狙った攻撃を試みる悪意のある IP アドレスを検出します。Okta は、このような IP アドレスが認証段階に到達するのを防ぎ、正規のユーザーがアカウントから締め出されるリスクを低減します。

3. **安全な認証方法：**Okta は、総当たり攻撃を防ぐために複数の認証オプションを提供しています。

    a. FastPass は、パスワードを不要にするゼロトラスト認証器であり、主要な攻撃ベクトルを排除します。また、デバイスとブラウザのヘルスチェックを実施し、信頼されたユーザーとデバイスのみが環境にアクセスできるようにします。

    b. Okta は、この他にもフィッシング耐性のある多様な認証方法をサポートしています。

    c. Adaptive MFA は、攻撃者が認証情報を窃取した場合でも認証フローを完了できないように確保します。Okta は、ユーザーの位置情報、IP アドレス、その他のデータポイントを収集し、基準となるプロファイルを構築してログイン試行のリスクレベルを判断します。すべてのユーザーやログインに対して MFA を適用できない場合でも、デバイスフィンガープリントなどのチェックと組み合わせることで、セキュリティを強化できます。
    さらに、セキュリティ管理者は、ログインフロー内で CAPTCHA を設定し、認証要求のセキュリティを強化できます。

まとめ

Workforce Identity Cloud は、認証前、認証時、認証後の各段階でユーザー、デバイス、セッションを脅威から保護する多様な機能を提供します。行動分析、デバイスのヘルスチェック、他のセキュリティツールとの即時統合によりリスクを継続的に評価する Okta をご活用いただくことで、お客様はアイデンティティに関連するリスクが影響を及ぼす前に自動的に対応できます。

Workforce Identity Cloud の詳細をご確認ください。