攻撃ベクトルを解き明かす：アイデンティティベースの脅威に対する組織の保護

攻撃ベクトルを解き明かす：アイデンティティベースの脅威に対する組織の保護

目次

脅威の状況

MFA を標的にする攻撃

組織が機密リソースの防御を強化するたびに、攻撃者は回避する新たな方法を見つけます。このような攻撃者は、映画で描かれるように地下室で孤立して活動している個人ではありません。攻撃者は組織化されたサイバー犯罪者であり、その活動はビジネスと同じように行われます。サイバー犯罪者が互いに協力する方法の 1 つに、セキュリティ管理の回避を容易にする攻撃キットがあります。攻撃キットの使用により、技術的な専門知識がほとんどない攻撃者でも、高度な攻撃を仕掛けることができます。

つまり、セキュリティソリューションは、攻撃者の戦術と同様に進化を続けなければなりません。過去には、特殊文字と数字を組み合わせた強力なパスワードがあれば、十分な防御になると考えられていました。その後もテキストメッセージ経由でのコード確認など、別の認証要素を追加すれば十分とされていました。しかし今では、攻撃者の侵入経路に障壁を設けつつ、信頼できるユーザーが容易にアクセスできるようにする包括的なソリューションを導入することが必要だと考えられています。

サイバー犯罪者は、アクセスを確保するためにどのようなことを行っているのでしょうか。幸いなことに、これらの攻撃ベクトルがどのように機能するかについて多くの情報があります。非営利組織の MITRE 社は、どのように攻撃者が不正にアクセスしているかを把握するのに役立つよう、攻撃の戦術と手法をまとめたナレッジベースを開発しています。MITRE ナレッジベースには数百件の攻撃が記録され、エンドユーザーを標的とする主要な攻撃の種類もいくつかあります。MFA 技術が適切に導入されていない場合、これらの手法によって、MFA 技術の弱点が悪用される場合があります。これには以下が含まれます。

MFA 傍受（MITRE ID T1111）：攻撃者は SMS（ショートメッセージサービス）や E メールで送信されるワンタイムコードを窃取し、ユーザーのログイン情報と MFA コードでログインします。

デバイス登録（MITRE ID T1098.005）：攻撃者は窃取したログイン情報を使用して不正なデバイスを MFA アカウントに新規登録し、永続的なアクセスを確保します。

MFA 要求の生成（MITRE ID T1621）：窃取したログイン情報を持つ攻撃者が、ユーザーが誤ってアクセスを許可したり、MFA 疲労攻撃による迷惑行為から逃れるために要求を承認したりすることを期待し、信頼できるユーザーに MFA 要求を繰り返し送信します。

中間者攻撃（AiTM）（MITRE ID T1539）：攻撃者は認証されたユーザーのセッション Cookie を窃取し、信頼できるユーザーを装って MFA の必要性を完全になくして無制限にアクセスできます。

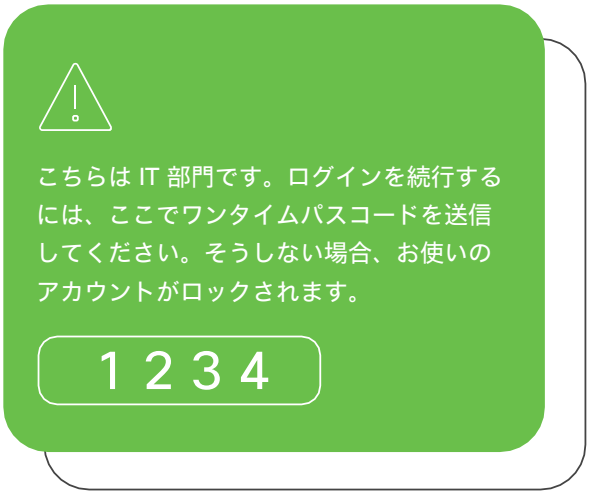
これらの戦術には、攻撃者が従業員や IT チームを装ってアクセスを騙し取るソーシャルエンジニアリングの手法も含まれる場合が多くあります。ソーシャルエンジニアリングは、一般的なフィッシング攻撃で行われる場合もあれば、ソーシャルメディアで得られる個人情報を使用して特定の個人や企業を標的にする、スピアフィッシングで行われる場合もあります。近年、企業のセキュリティプロトコルを回避しようと、従業員を装って IT ヘルプデスクに問い合わせをかけるといった音声スピアフィッシング攻撃が増えています。

攻撃ハンドブック

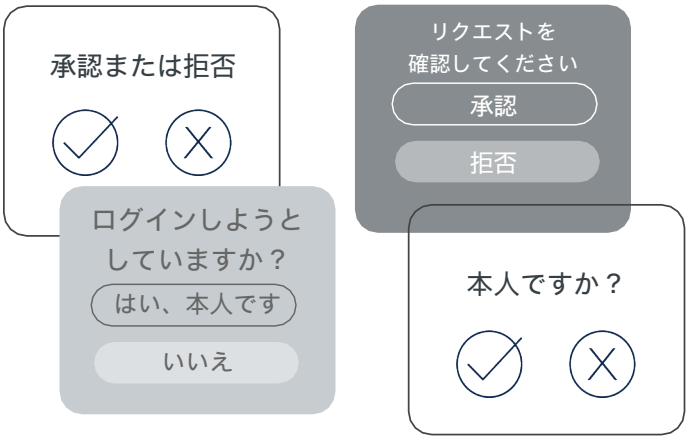
企業がサイバー攻撃を受けたというニュースは、誰もが見聞きしたことがあるのではないでしょうか。侵害された企業は大急ぎで自社のデータを保護および確保し、PR チームを通じて一般に情報発信し、財務面の影響が軽減されるよう努め、全体的な損害を最小限に抑える必要があります。攻撃によって少し違いはありますが、以下に典型的な攻撃について紹介します。

1. 攻撃者は企業の IT チームを装い、認証ユーザーのログイン情報を取得しようとスピアフィッシング E メールを送信します。

2. ソーシャルエンジニアリングを通じてユーザーを騙し、ワンタイムパスコード（OTP）を共有させ、MFA 要件を回避します。



3. OTP が認証手段としてブロックされている場合、攻撃者は MFA 疲労攻撃により承認させようと、MFA 要求を繰り返し送信する場合があります。



4. 攻撃者はアクセスを取得すると、デバイスを登録して権限を昇格させて、機密データを窃取するか身代金を要求します。

残念ながら、この話は特別なことではありません。サイバーセキュリティ インフラストラクチャ セキュリティ庁（CISA）は、**90% の攻撃がフィッシングから始まっている**ことを明らかにしました。AI の進化に伴い、フィッシングはより現実的で信用されやすいものになってきています。誤字脱字が目立っていたかつての E メールは、今では精巧に細工可能なほか、顔見知りである同僚のトーンやスタイルを真似ることもできます。従業員は騙しの手口に引っかからないよう強い警戒心を持つ必要がありますが、従業員にサイバーエキスパートのように求めるのは適切ではないでしょう。サイバー犯罪者による被害に遭ったユーザーを責めるのではなく、ユーザーを保護する方法を見つける必要があります。

セキュリティの有効性の向上

必要条件：環境の最新化

高度なアクセス管理のセキュリティ機能を利用するには、組織は自社環境で使用する認証プロトコルをアップグレードする必要があります。これは、クラウドを導入するプロセスで共通するステップです。多くの最新セキュリティ機能を利用するには、LDAP や RADIUS などの従来のプロトコルではなく、SAML または OIDC といったアップグレードされた認証プロトコルをアプリケーションに使用する必要があります。

LDAP は、ネットワーク上のディレクトリに接続してユーザーアイデンティティを検証し、オンプレミス アプリケーションへのアクセスを付与する認証プロトコルです。ユーザーがアプリケーションへのアクセスを要求すると、LDAP によりユーザーのログイン情報がディレクトリの情報に一致するかどうか、またはそのユーザーの対象リソースへのアクセスが承認されているかどうかが確認されます。RADIUS にも、ユーザーによるリモートネットワークへのアクセスを可能にするため、オンプレミスのコンポーネントがあります。

最新のプロトコルは動作が異なります。SAML と OIDC は、アイデンティティ プロバイダー（IdP）とアプリケーション間に信頼を確立することで機能します。これらは、シングルサインオン（SSO）と MFA を機能させるための重要なプロトコルであり、暗号化技術を採用しています。最新のプロトコルは、クラウドおよび Web ベースのアプリケーションに対する認証をサポートするよう構築されているため、従来のプロトコルよりも安全性に優れています。また従来のプロトコルは、パスワードなどの単一要素によるアクセスに依存しており、ユーザー体験が十分でない場合もあります。

定義：

- **SAML：**Security Assertion Markup Language（セキュリティ アサーション マークアップ言語）
- **OIDC：**OpenID Connect（OpenID 接続）
- **LDAP：**Lightweight Directory Access Protocol（ライトウェイト ディレクトリ アクセス プロトコル）
- **RADIUS：**Remote Authentication Dial-In User Service（リモート認証ダイヤルイン ユーザー サービス）

では、最新化するには何が必要でしょうか。

従来のプロトコルを使用する自社開発アプリケーションの場合、組織内でその機能を構築するために社内リソースを確保することが問題となります。外部アプリケーションの場合、対応する認証オプションを把握することが重要です。最新のオプションがまだサポートされていない場合は、サポートされるまでのロードマップを確認する必要があります。

アプリケーションが最新のインフラストラクチャを使用するようになると、攻撃者から防御するための新たな可能性も広がり、組織は現在および今後の脅威の状況に対処するのにより有利な立場に立てます。

組織の保護をさらに強化するために活用できる新しい機能とは、どのようなものでしょうか。ユーザーとアプリケーションを保護するためには、さまざまな方法があります。次のセクションでは、以下の利点をもたらす強化されたセキュリティ機能など、検討すべき主要なカテゴリについて概説します。

最小限の労力

最も強力な認証

最大限のセキュリティ

優れた可視性

最小限の労力で優位に立つ：セキュリティ強化のために今すぐできること

攻撃ハンドブックから明らかなように、ユーザーはパスワードと二要素認証以外の追加の保護が必要です。ユーザーには、MFA を標的にした一般的な攻撃を認識して阻止できる認証要素が必要となります。

明日にでも組織が導入できる 1 つの解決策として、従来のプッシュ要求をアップグレードし、一意のコードを要求する方法があります。これは検証済みプッシュ要求としても知られています。この一意のコードは認証アプリケーションに入力されるもので、テキストメッセージや E メールで送信されるようなワンタイムパスコードとは異なります。エンドユーザーは、アクセスデバイス（ラップトップなど）で得られるコードを認証デバイス（通常は携帯電話）に入力する必要があります。ユーザーが実際にログインしようとしていない場合は、正しいコードを認証アプリケーションに入力することはできません。

しかし、業務を行うためにログインしている信頼できるユーザーにとっては、ログインするたびにコードを入力しなければならないことに不満を感じるかもしれません。そのため、組織はリスクベースのアプローチも検討できます。このアプローチでは、認証技術によりリスクシグナルと状況を考慮に入れて、ログイン時にユーザー要件を調整できます。たとえば、会社のラップトップや普段から使用している Wi-Fi ネットワークなど、信頼できるシナリオにいる場合、ユーザーは認証を行う回数を減らすことが可能です。

場所を移動するなど、ユーザーの状況が変わる場合は、再度認証を求められる可能性があります。さらに重要なことに、未知のデバイスから立て続けに複数のプッシュ要求が送信されるなど、攻撃パターンに類似した認証要求が発生する場合は、認証方法を検証済みプッシュに強化して攻撃を阻止できます。

最も強力な認証で優位に立つ：

パスワードレス化への道のり

多要素認証の基本的な考え方では、常に次の要素のうち少なくとも 2 つを使用してユーザーを保護します。

1. 知っているもの

2. 所有しているもの

3. 自身を表すもの

従来は、ユーザーがユーザー名とパスワード（知っているもの）を使用してログインし、モバイルデバイス（所有しているもの）上のアプリケーションを通じて認証を行ってきました。これは、ユーザーの記憶（あるいは付箋のメモ）とアプリケーションのデータベースにある、パスワードという共有の秘密に依存しています。ログインする際にアイデンティティを確認するため、プッシュ通知を承認するといった 2 番目のステップも必要です。

新しく革新的な技術によって、ログイン方法はより良いものに変わりつつあります。パスワードレス ソリューションは、自身を表すもの（指紋など）と所有しているもの（デバイスなど）を利用します。

これにより、記憶しておくのが困難で、盗まれやすく、あまり安全でないパスワードは除外されます。

「自身を表すもの」+「所有しているもの」の組み合わせによって、秘密キーと公開キーのペアが解除され、ワンステップでのアクセスができるようになります。秘密キーはユーザーのデバイスから外部に漏れることはないため、パスワードとは異なり強力に保護されます。

パスワードレス技術は、FIDO Alliance（Fast Identity Online）によりサポートされています。FIDO Alliance とは、認証の向上や、WebAuthn（Web Authentication API）などの FIDO2 標準規格の開発の監督を専門に行う企業のコンソーシアムです。ユーザーの初回ログイン時、WebAuthn プロトコルにより対象アプリケーションにユーザー名が送信されます。ユーザー名は、アプリケーションによってブラウザを介してユーザーのオーセンティケータに送信されます（デバイスまたはセキュリティキー）。ユーザーは、生体認証またはデバイス PIN を使用してアイデンティティを確認します。暗号化技術を使用して新たに作成されたユーザーの秘密キーはそのデバイスに保存されます。公開キーは、ユーザー名とともにアプリケーションに送信されます。公開キーはデバイス上で保護されている秘密キーなしでは価値がないため、公開されたままにしておくことが可能です。

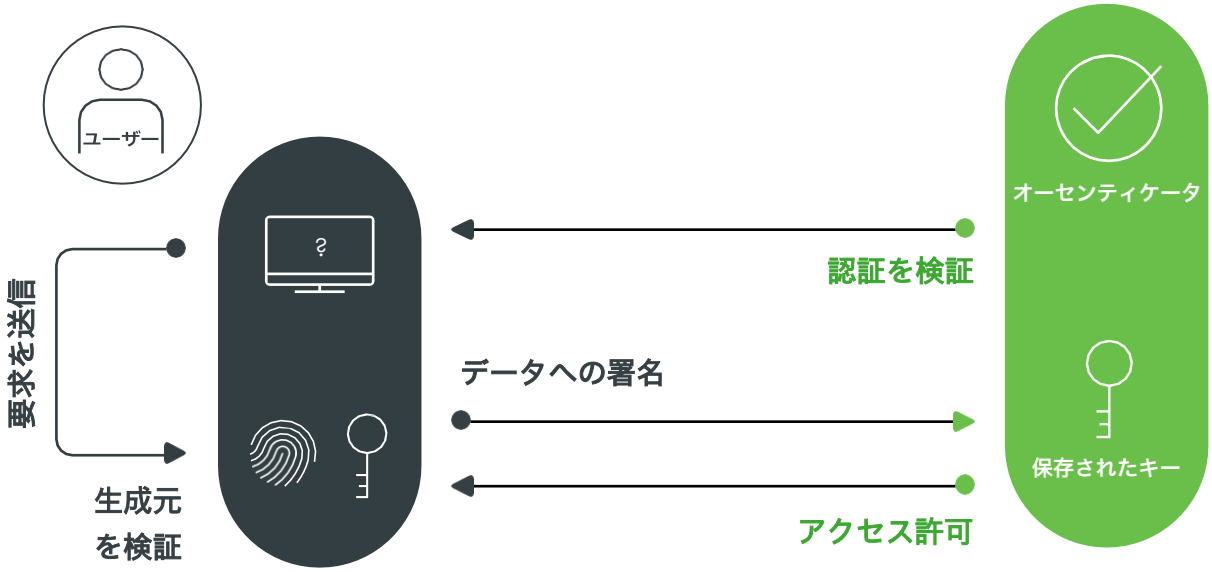
自身を表すもの：

生体認証（Face ID、指紋）

所有しているもの：

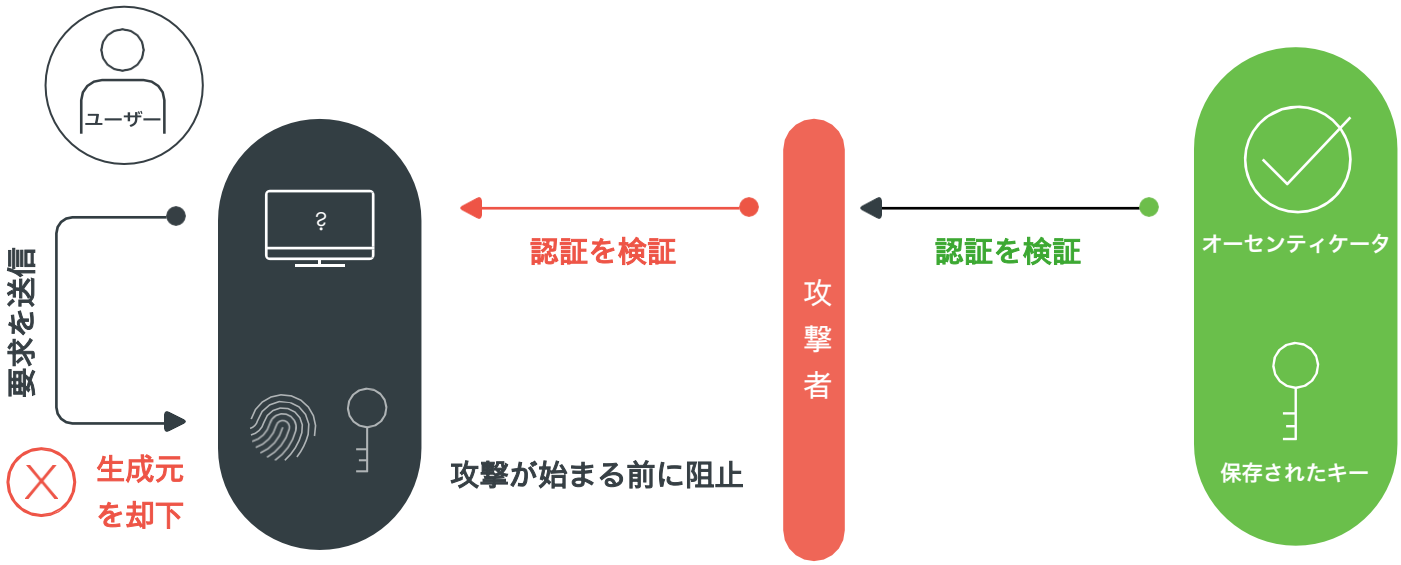
デバイス、セキュリティキー、モバイルアプリケーション

今後ユーザーがログインする際には、生体認証により公開キーとペアになっている秘密キーを利用できます。この秘密キーと公開キーのペアが、ユーザー名とパスワードに代わる必須のログイン情報になります。パスキーを使用すると、デバイス間で FIDO サインインのログイン情報にアクセスできるため、生体認証を再登録する必要がなく、パスワードレスをさらに容易にできます。



この認証方法は、攻撃者がユーザーのログイン情報を窃取するのが不可能なため、「フィッシング耐性」として知られています。たとえば、中間者攻撃のシナリオでは、攻撃者はプロキシを介してユーザーのセッション Cookie を盗み取ることが可能です。プロキシが、ユーザーと本物の Web サイトの間に置かれる悪意のある Web サイトとして機能し、その結果、見た目は全てが正常に見えます。

ユーザーが認証を行う際、acme.com ではなく evil-acme.com からアクセスしている可能性があります。しかし、WebAuthn が導入されていると、ブラウザは何が認証を要求しているのかや、セッション要求がどこから来ているのかについて偽ることができません。それは、オーセンティケータが安全なドメインにのみ登録されているからです。そのため、攻撃が開始される前に認証要求は拒否されます。



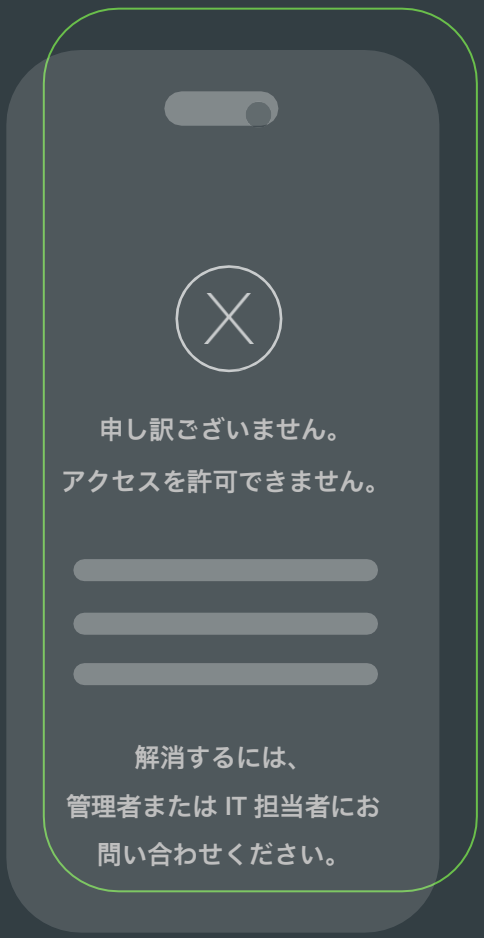
しかし、パスワードレスを導入することは、簡単なタスクではありません。特に、大規模ユーザーで多数のアプリケーションとハイブリッド インフラストラクチャがあり、複雑なログインフローを扱う場合はなおさらです。完全なパスワードレス環境を実現しようとすると、技術の進化とユーザー数の増加に対応できる段階的なアプローチを伴うプロセスが必要です。

最大限のセキュリティで優位に立つ：デバイスと認証のセキュリティを組み合わせる

パスワードレスはセキュリティが最大限確保された認証オプションですが、強力な認証とデバイス信頼ポリシーを組み合わせてその有効性を高める方法もあります。組織は、組織のリソースへのアクセスが認められるすべてのデバイス（管理対象および非管理対象を含む）を登録し、これを実践できます。デバイスが認識されない場合、そのデバイスは認証要求を開始できません。

その裏ではブラウザとデバイスが連携して、デバイス上のアプリケーションを通じてユーザーのアイデンティティを確認します。認証の際、ブラウザはデバイス アプリケーションと直接通信し、通常のユーザー要求やブラウザの通信経路を介さず、「このデバイスは安全です」や「このデバイスにアクセスを許可すべきです」と通信できます。

一方、デバイスが認識されなければ、攻撃されるリスクはありません。攻撃者がユーザーのログイン情報を持っているかどうかに関係なく、攻撃が開始される前に阻止できます。つまり、攻撃者がエンドユーザーとやり取りすることはありません。プッシュハラスメント攻撃を防止することで、プッシュ疲労を排除し、認証アプリケーションにコードを入力させるソーシャルエンジニアリングを防ぎます。



優れた可視性で優位に立つ：事後対策ツールの使用

組織のセキュリティ態勢を強化するには、予防的なツールは欠かせません。しかし、脅威の状況の現実を考えると、攻撃者が防御の壁を突破した場合に対応するためのツールも用意しておく必要があります。そこで、異常を明らかにするために、認証とログインデータを分析する事後対策の手段が必要になります。

ユーザー、デバイス、場所に関するデータ量が膨大なため、これを実践するのは簡単ではありません。自宅で業務リソースにアクセスする場合がほとんどである従業員が、長い週末休みを利用した旅行に業務用コンピュータを持ち込む場合、それは本質的なリスクにはなりません。リスクとして考慮に入れれば、セキュリティチームは多数の誤検出アラートを受け取ることになります。この場合、新たな状況ではあるものの、信頼できるユーザーであることに変わりありません。しかし、ユーザーがいつもと違う時間帯に、新しい場所で、新しいデバイスにログインするような場合は、注意に値するかもしれません。

組織には、エンドユーザーの動作を把握するソリューションが必要です。そうすれば、注意を向けアクションを起こすべきイベントを表面化できます。そして脅威が検出されると、セキュリティスペシャリストには環境からその脅威を分離および排除するためのツールが必要です。事後対策ツールには、基準となる動作を把握するためのユーザーデータ、脅威の信憑性をさらに確認するための調査、対策を講じる機能が必要です。これらの機能により、組織は従業員に関する可視性を向上させ、保護を確実にします。

組織には、エンドユーザーの動作を把握するソリューションが必要です。そうすれば、注意を向けアクションを起こすべきイベントを表面化できます。

Duo が できること：

組織がセキュリティ強化プロセスのどの段階にあっても、Duo はお客様の現状に合わせて、現在のセキュリティツールの有効性を高めることができます。

必要条件：

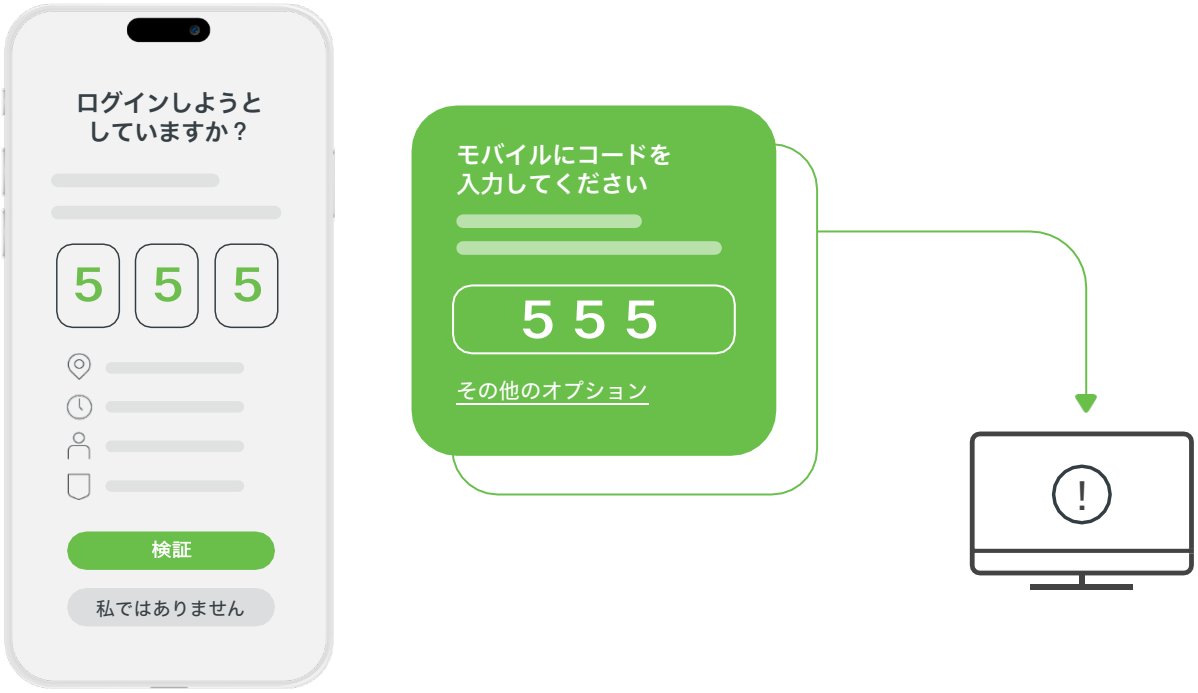
環境の最新化

Duo の Universal Prompt には、ユーザーを標的にする脅威への防御を目的に設計された数多くのセキュリティ強化機能が用意されています。**環境の最新化**に有用な最初のステップには、SAML または OIDC プロトコルをサポートするアプリケーションのインベントリとアセスメントの実施などがあります。これにより、アプリケーションへのアクセスにおいてエンドユーザー体験を向上させ、組織全体のセキュリティ態勢も強化できます。

最小限の労力で優位に立つ：

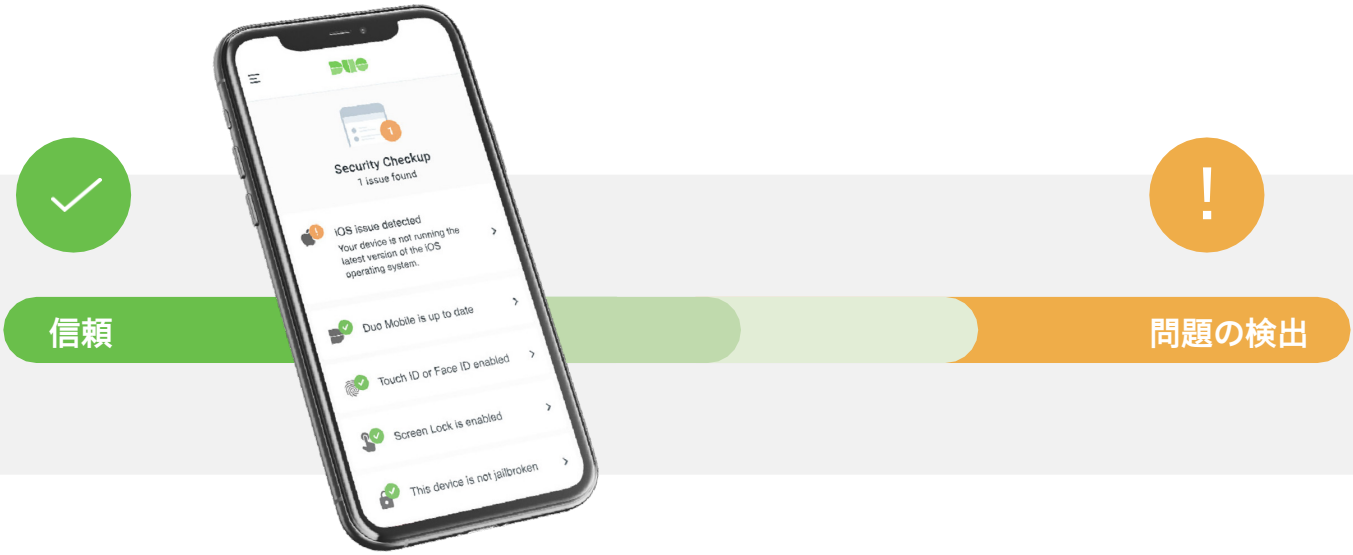
明日からできるセキュリティ強化の方法

Verified Duo Push は従来の Duo Push 要求の強化版です。認証要求を承認するにはアクセスデバイスで指定される 3 桁から 6 桁のコードが必要になります。Duo のすべてのエディション（Essentials、Advantage、Premier）を対象に、お客様は Duo Push を特定のユーザー向けに Verified Duo Push にアップグレードできます。



MFA 疲労や余分な手間に対する従業員の反発を懸念するお客様には、Advantage および Premier パッケージで利用可能な Duo のリスクベース認証ソリューションが優れた選択肢となります。Duo は高度なアルゴリズムを活用し、ユーザーの場所、デバイスのレピュテーション、ネットワークのコンテキストなどの要素を考慮に入れつつ、それぞれのログイン試行に関連付いたリスクをリアルタイムで評価します。

ユーザーが信頼される状況にある場合、必要なリソースに簡単にアクセスできます。状況に変化があれば、Duo はユーザーに対し再認証を要求します。また MFA プッシュハラスメントなど、サイバー犯罪者からの攻撃が発生した場合、Duo は認証要件を Verified Duo Push に強化します。Duo のリスクベース認証ソリューションの目的は、シームレスなユーザー体験を維持しながらセキュリティを優先することです。



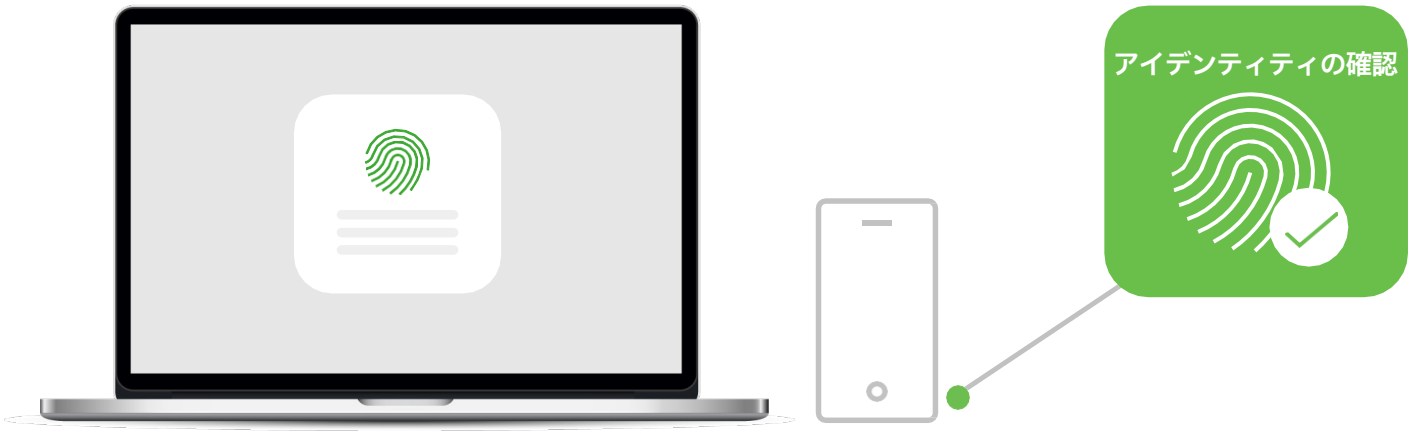
最も強力な認証で優位に立つ：

パスワードレス化への道のり

すべての Duo エディションで利用可能な Duo のパスワードレス ソリューションでは、パスワードの必要性をなくし、WebAuthn プロトコルを採用しています。パスワードレス認証では、パスキーの活用などの Flexible Authentication オプションをサポートしています。パスキーは、ユーザーごとに生成される一意の暗号化キーで、デバイスまたは信頼できるプラットフォーム内に安全に保存されます。ユーザーがログインする際、パスキーを使用してアイデンティティを検証し、パスワードを必要としないセキュアな認証体験を実現します。

Duo では、Windows Hello、Touch ID、YubiKey などの FIDO2 セキュリティキーを含む多様なエンドユーザー認証とパスキーをサポートしているため、組織はパスワードレス技術を容易に展開できます。

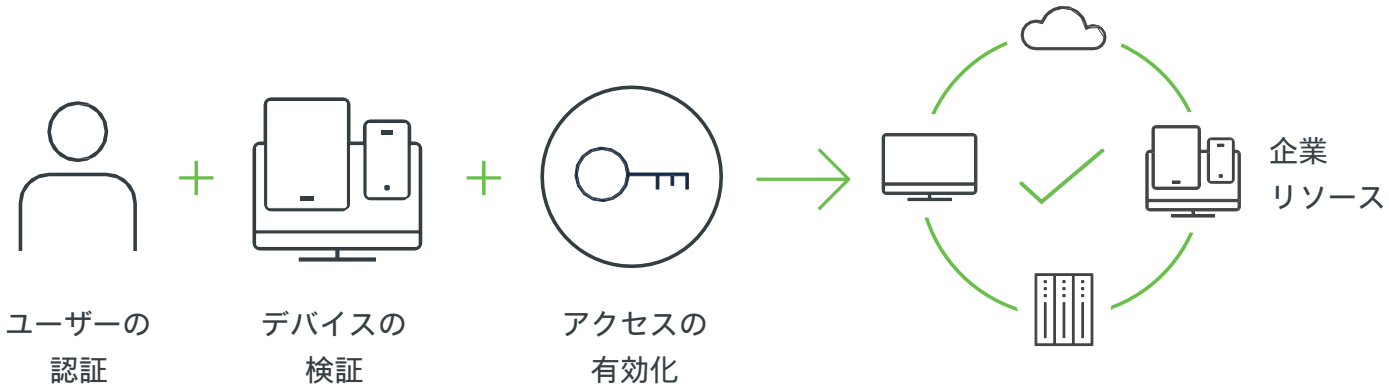
組織での導入方法に関しては、『パスワードレス化に向けた Duo 管理者ガイド：パスワードレスの運用開始』で、パスワードレス化を実現するための段階的アプローチについて詳細を説明しています。



最大限のセキュリティで優位に立つ：

デバイスと認証のセキュリティを組み合わせる

強力なユーザー保護の絶対的基準は、強力な認証要素とデバイスポリシーを組み合わせることです。RSAC 2023 で、Duo はパッケージに関する重要な変更を発表し、すべてのお客様が Trusted Endpoints 機能を利用できるようにしました。Duo Desktop により提供される Trusted Endpoints を使用すると、管理対象かどうか、会社支給、請負業者所有、個人所有のいずれにかかわらず、すべてのエンドポイントに対して信頼を定義できます。また、Duo Mobile App により、モバイルデバイス管理（MDM）ソリューションを確認し、モバイルユーザーがアクセスできるかどうかを検証できるようになります。



管理者は、Duo のポリシーを通じてアクセスを付与するユーザー、アプリケーション、デバイスを決定したり、組織全体を対象にグローバルレベルでポリシーを有効化したりできます。

強力な認証要素とデバイス信頼ポリシーの強力な組み合わせがバリアとなり、最も一般的な攻撃ベクトルを使用したサイバー犯罪者をブロックできます。また、信頼できるデバイスでリソースにアクセスする際、ほとんどのユーザーはバックグラウンドでその技術が動作していることを認識しないため、信頼できるユーザーはシームレスな体験を維持できます。

優れた可視性で優位に立つ：

事後対策ツールの使用

Duo Trust Monitor は、価値のある実用的なセキュリティイベントを管理コンソールで Duo 管理者に提示することに重点を置いた Duo の脅威検出機能です。Duo の認証データを分析およびモデル化して、通常のユーザーとデバイスのアクセス動作の基準を設定します。この機能は、ユーザーがアプリケーションにアクセスする対象者、内容、理由、場所、時期といった要素を考察します。

Trust Monitor では、ユーザーの動作をそのユーザーの過去の状況と比較するため、本当に不審な動作に注目しやすくなります。誤検出によってチームの集中を妨げるようなことはありません。実際に攻撃が発生した場合は、Trust Monitor により Duo 管理者はユーザーをロックアウトすると同時に、潜在的な脅威を調査できます。

Cisco Duo は、最先端のアクセス管理スイートによって侵害から保護します。強力な多層防御と革新的な機能で、正当なユーザーのアクセスを許可し、攻撃者の侵入を防ぎます。世界中の 40,000 社を超えるお客様の信頼できるパートナーである Duo は、強力なセキュリティを迅速に実現するとともに、ユーザーの生産性も向上させます。

Duo Security についてもっと詳しく知りたい場合は、無料トライアルをお試しください。

1265386799 01/2024