okta

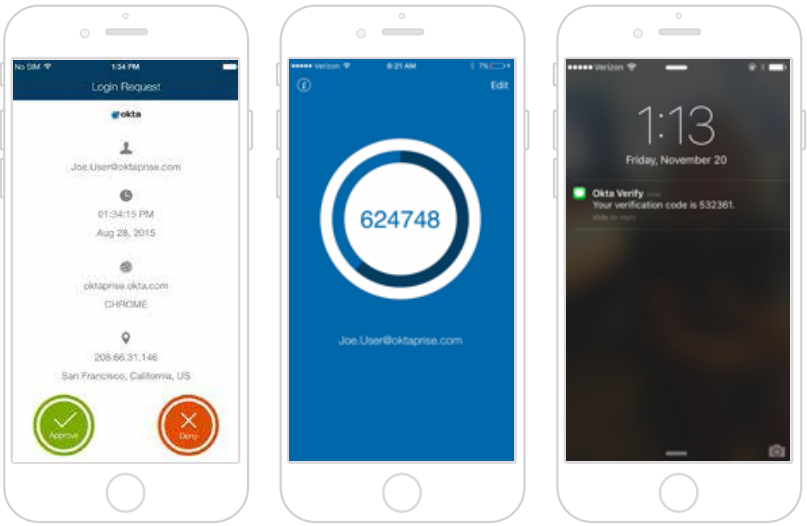
ADAPTIVE MULTI-FACTOR AUTHENTICATION
ホワイトペーパー

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

info@okta.com
1-888-722-7871

エグゼクティブサマリー

このホワイトペーパーでは、Oktaのアダプティブ多要素認証（MFA）の概要について説明します。Oktaのアダプティブ多要素認証は、アプリケーションとデータのセキュリティ強化に取り組む企業に最適な、包括的でありながらシンプルで強力な認証ソリューションです。ポリシーに基づきコンテキストに応じたアクセス管理を実現し、さまざまな最新の要素に対応します。さらに、何千社もの企業のビッグデータから得たインサイトを活用し、企業に必要なさまざまなアプリケーションやVPNと統合できます。Oktaのアダプティブ多要素認証を導入すれば、エンタープライズグレードのセキュリティを実現するとともに、優れたユーザーエクスペリエンスを提供できます。



セキュリティは経営幹部レベルの課題

セキュリティ侵害はもはや、IT部門だけの問題ではありません。機密データの流出による金銭的損失や風評被害から組織を守ることは、経営幹部にとって日々の最大の課題です。企業が侵害の発生に気付くまでには平均で205日かかります。[1] こうした侵害の影響は根深く、長く尾を引きます。さまざまな損害に対する責任が生じるだけでなく、機密データを守れない企業とみなした消費者が商品購入や情報提供を躊躇し、売上が落ち込む可能性もあります。

従来のユーザー認証では不十分

企業は従来、VPNやアプリケーションへのアクセスを保護するために、パスワードのみを使用する1要素認証に頼ってきました。しかし、パスワードは管理が面倒なうえ、数々の一般的な攻撃手法に対して脆弱です。攻撃者は、フィッシングやソーシャルエンジニアリングなどの手段を用いて、消費者、オンラインバンキング、エンタープライズアプリケーションのパスワードを盗み出します。こうした攻撃が蔓延する中で、ITやセキュリティの担当者は、攻撃を阻止するための新たなセキュリティ対策を導入することを求められています。

[1] http://www.itsecurityguru.org/tag/breach

23

データ漏えいコストの1年ごとの増加率[2]

23

フィッシングメールを開いた人の割合
（添付ファイルをクリックした人は11%）[3]

50.7

盗まれた資格情報を悪用したWebアプリケーション攻撃の割合[3]

米国の保険会社Anthem社のデータ漏えい事件では、ハッカーは管理者の資格情報を悪用してデータベースから個人情報を盗み出しました。Anthem社が多要素認証（MFA）を導入していたら、ハッカーはデータにアクセスするために管理者パスワード以外の情報を入手する必要がありました。複数の認証あれば、Anthem社の顧客以外の880万～1,880万件の個人情報を含む合計約7,880万件の個人情報が流出する事態は防げたはずです。

モバイル普及の影響

モバイルワーカーの増加により、アプリケーションやデータへのアクセスを保護するために企業がとるべき対策も変化しています。ユーザーは、ホームオフィスやコーヒーショップ、ホテルやモバイルデバイスからアプリケーションにアクセスします。どこからでもアクセスできる柔軟性が求められるため、未知のネットワークやデバイスからも安全にアクセスできるようにする必要があります。

MFAのメリット

MFAは、盗まれた資格情報を悪用する幅広い攻撃から組織を守ります。MFAでは、ユーザーは認証時に、第1要素であるパスワード以外の要素（ユーザー自身の身体的特徴、ユーザーが持っている物、またはユーザーが知っていること）の提供を求められます。MFAを導入すれば、ユーザーのパスワードが盗まれても、攻撃者はほかの要素も盗むか偽装しなければならないため、ユーザーアカウントへの不正アクセスを防ぐのに効果的です。

[2] Ponemon Institute「2015 Global Cost of a Data Breach（2015 年版世界のデータ漏えいコスト）」レポート

[3] ベライゾン社「データ漏洩/侵害調査報告書」

従来のMFAソリューションの課題

ユーザーエクスペリエンスの低下

MFAはメリットが大きい一方で、さまざまな点でエンドユーザーに不便を強いることがあります。セキュリティトークンを使用するソリューションの場合は、管理に手間がかかり、維持費も高額です。トークンの管理コストと交換コストはかなりの負担になります。エンドユーザーにとっても、セキュリティトークンを持ち歩いてパスコードを入力するのは面倒です。MFAポリシーを厳しく設定した場合、エンドユーザーは1日に何度も認証を行わなければならず、生産性が低下し、不満がたまることもあります。

管理が複雑

従来のスタンドアローン型のMFA製品は、導入が容易ではありません。MFAとアプリケーションやシステムを個別に統合する必要があります。MFAによる保護対象を新しいアプリケーションに適用したり、ユーザーを追加するにも手間がかかるため、拡張も困難です。さらに、個別に統合を行う場合、新しいリソースの追加時に管理者がMFA保護を有効にし忘れたり、そもそもMFA保護が必要であることに気付かなかったりして、適用漏れが生じがちです。

拡張が困難

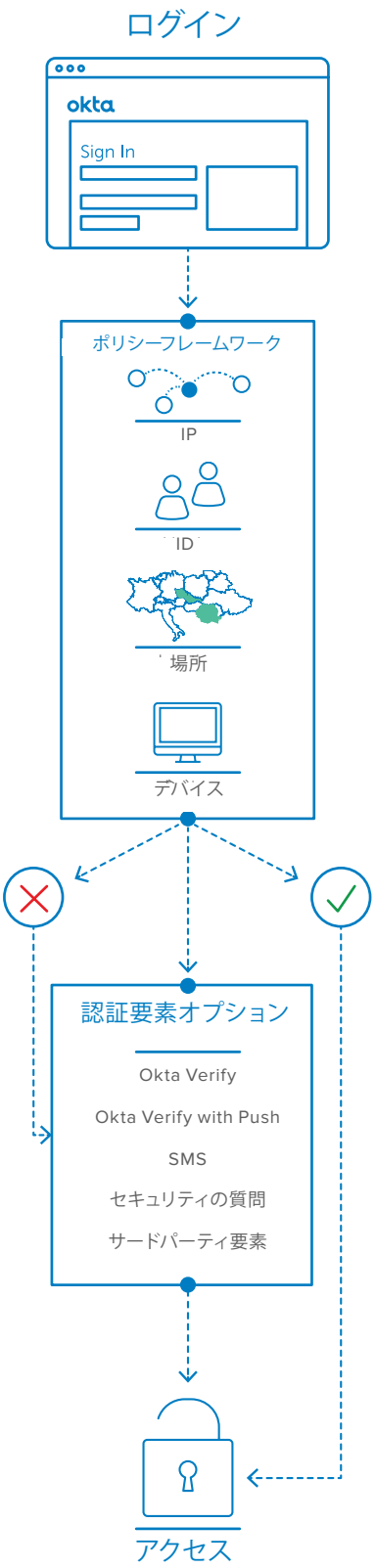
スタンドアローンのMFAでは、そのベンダーに固有の統合機能をサポートするアプリケーションやシステムしか使用できず、すべてのアプリケーションやリソースに幅広くMFA保護を適用するのが困難です。昨今、企業ではクラウドアプリケーションの導入が進んでいますが、多くのクラウドアプリケーションではMFAに内蔵の統合機能をサポートしていません。その場合、クラウドアプリケーションではMFAの使用を見送るか、SMSベースのパスコードやセキュリティ質問といった、クラウドアプリケーション固有の認証機能を使用することになります。その結果、エンドユーザーは、アクセスするアプリケーションやサービスによって複数の資格情報と複数のMFAを使い分けなければならなくなり、混乱が生じます。

一部のタイプのユーザーを保護できない

組織内のユーザーの種類や数が増え続ける中で、1つのタイプのMFAだけではモバイルユーザーや海外のユーザーに対応できないことがあります。職務によってはユーザーがスマートフォンを利用できない場合もあります。たとえば、コールセンターの多くは、従業員が個人所有のモバイルデバイスを持ち込むことを禁止しています。

セキュリティに対する新たなアプローチ：よりスマートに、使いやすく、包括的に

Oktaのアダプティブ多要素認証は、従来のスタンドアローン型のMFA製品で生じる課題を解消して、エンタープライズグレードのセキュリティを実現し、優れたユーザーエクスペリエンスを提供します。ポリシーに基づきコンテキストに応じたアクセス管理を実現するほか、最新のさまざまな要素や、ビッグデータ分析、企業が保護する必要のあるすべてのアプリケーションとVPNに対応する内蔵の統合機能を利用できます。



コンテキストに応じたアクセス管理でリスクを低減

Oktaのコンテキストに応じたアクセス管理では、ユーザーがアプリケーションやデータにアクセスした日時、場所、方法を確認して、リスクを低減できます。アクセスしようとしているユーザー、アクセス元のネットワークや国、およびユーザーが使用しているデバイスに基づいて、アクセスを許可するか、ステップアップ認証を要求するか、範囲を制限するか、アクセスを拒否するかを選択できます。管理者はさらに、ユーザーが検証のために選択した要素と、第1認証の実行状況に応じて、アクセスを調整することもできます。

Oktaのアダプティブ多要素認証では、コンテキストに応じてアクセスポリシーをきめ細かく設定できるので、正規のユーザーの手間を増やすことなく、第2要素を導入して簡単により多くのリソースのセキュリティを確保できます。ユーザーは、ログインのたびではなく、必要なときだけ検証を要求されます。

最新の第2要素で幅広いユーザーに対応

さまざまな第2要素に対応し、柔軟な登録ポリシーを設定できるため、ユーザーが最新のスマートフォンを持っていない場合や、海外でスマートフォンを使用できない場合でも認証が可能です。Oktaのアダプティブ多要素認証では、ユーザーの役割、権限、作業環境に応じて有効な要素を使用することで、すべてのユーザーのアクセスを保護できます。Okta Verify with Pushなど、スマートフォンを使用するオプションでは、エンドユーザーはすばやく簡単に自身のアイデンティティを検証できます。ユーザーがスマートフォンを使用できない場合は、SMSパスコードなどのアウトオブバンド要素を利用できます。さらに、Yubikeyを含む一部のサードパーティの要素とも統合できるため、RSAからOkta Verify with Pushなど、要素を簡単に移行できます。Oktaの登録ポリシーでは、管理者がユーザーやグループごとに、必須にする要素、オプションにする要素、無効にする要素を選択できます。また、ポリシーによって予備要素の設定を必須にすることにより、ITサポートコストを削減することもできます。

プロアクティブなセキュリティとリスクベースの適応型認証

Oktaのビッグデータ分析では、豊富なユーザープロファイルに基づいてリスクスコアを計算することで、誤検知を減らすと同時に、アプリケーションやデータをプロアクティブに保護できます。セキュリティチームは、攻撃の兆候を特定し、不正アクセスを防ぐために、数百万のユーザー、デバイス、認証要求に関するOktaのインサイトを活用できます。全体像を把握するのが難しいスタンドアローン型のMFA製品とは異なり、Oktaのアダプティブ多要素認証では、Oktaのシングルサインオンデータやエンタープライズモビリティ管理データにアクセスできます。各ユーザーの認証時の全操作に関するこれらのコンテキストデータを組み合わせて、攻撃者がユーザーになりすますために偽装する必要のある特徴の数を増やすことにより、セキュリティを強化できます。

さらに重要な点として、Oktaアダプティブ多要素認証はアラートを生成するだけではありません。Oktaがすべてのアプリケーションへのアクセスを一元管理するため、Oktaアダプティブ多要素認証が異常な認証要求を検出すると、攻撃の可能性があると判断して自動的にアクセスを停止し、完全に阻止するか特定のリソースにのみアクセスを許可するかのオプションを管理者に提示します。この方法で、リスクを効果的に低減します。

アプリケーションとVPNの統合機能が内蔵されているため導入が簡単

Oktaアダプティブ多要素認証は、すべてのアプリケーションと重要インフラストラクチャに強力な認証セキュリティを導入できる、100%クラウドベースのソリューションです。Oktaアプリケーションネットワーク（OAN）に用意された500以上のSAMLおよびRADIUS統合機能によって新しいアプリケーションやVPNをすばやく追加できます。ユーザー、デバイス、MFAセキュリティポリシーを一元管理することで、ユーザーやリソースの追加、変更、削除に的確に対応して、適用漏れを防ぐことができます。

開発者にとって実装が容易

従来、独自のアプリケーションやポータルを開発する開発者にとって、MFA の実装は容易ではありませんでした。Oktaアダプティブ多要素認証はAPIやOktaシングルサインオンウィジェットを介して利用できるので、登録、無効化、認証機能を簡単に実装できます。これにより、あらゆるタイプの強力な認証をカスタムアプリケーションにすばやく追加できます。Oktaアダプティブ多要素認証APIでは、MFAエクスペリエンスのブランディングも可能なので、ユーザーはセキュリティ上のメリットと簡素化を実現できるだけでなく、なじみのある外観と操作性でOktaアダプティブ多要素認証を利用できます。

まとめ

Oktaアダプティブ多要素認証なら、IT管理者やセキュリティ管理者は、効果的なセキュリティ対策を導入して、エンドユーザーのエクスペリエンスを低下させることなくアプリケーションとインフラストラクチャを保護できます。Oktaは、ユーザー、デバイス、振る舞いに関するコンテキストに応じたデータと、あらゆるユーザーをサポートするさまざまな最新の要素に基づく、よりスマートなMFAソリューションを提供します。既存のオンプレミスMFA製品からコスト効率に優れたOktaのクラウドベースソリューションへの移行は簡単に実行できます。新しいアプリケーションやユーザーの追加も容易で、短期間で価値を実現できます。統合されたシングルサインオンとエンタープライズモビリティ管理により、ユーザー、デバイス、アプリケーションを効率的に保護できます。

okta

さらに詳しい情報については、
OktaのWebサイトをご覧ください:
okta.com/learn/Adaptive-MFA