okta

ゼロトラスト入門

「決して信頼せず、常に確認する」

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

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

ゼロトラスト入門

エグゼクティブサマリー

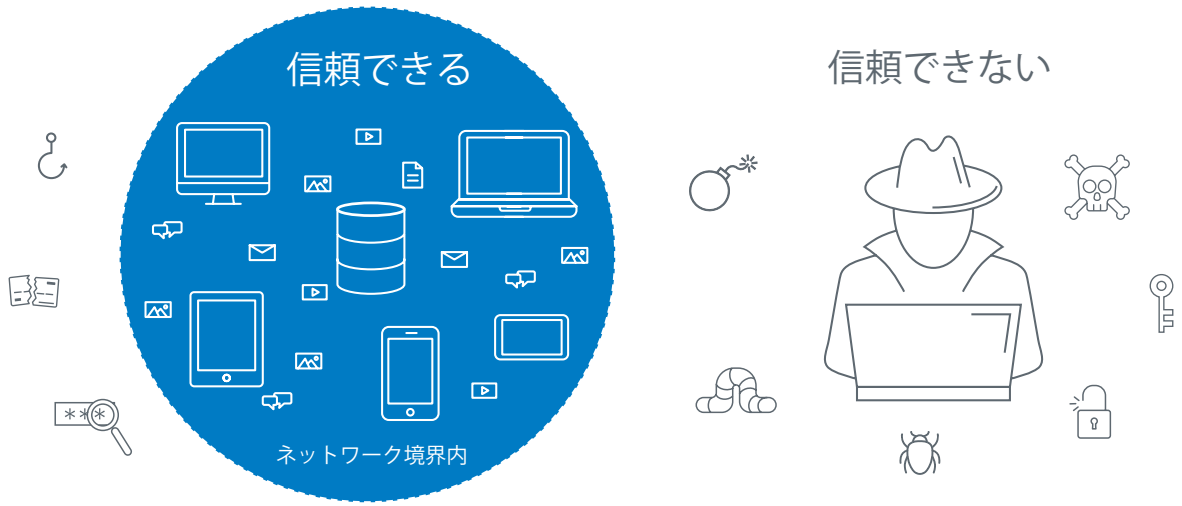
ゼロトラストセキュリティでは、「信頼できる内部ネットワーク」と「信頼できない外部ネットワーク」という考え方をとりません。モバイルやクラウドを導入するということは、ネットワーク境界中心のセキュリティという考え方が通用しなくなるということです。代わりに、従業員、パートナー、契約社員など多様なユーザーが、どのような場所やデバイスやネットワークからでもセキュアにアクセス可能にする必要があります。ゼロトラストセキュリティのアーキテクチャを構築するうえでの特効薬などはありません。ただし、導入に際しては最初に、アイデンティティとアクセスの管理を主要テクノロジーとして検討することが必要です。

この文書では、セキュリティを取り巻く状況の変化がゼロトラストの誕生につながったこと、Zero Trust Extended Ecosystem（ZTX）フレームワークの現状、組織が Okta をゼロトラストの基盤に活用して、現在から将来にわたり成功する方法についてご説明します。

課題 : データを守る壁の消失

従来のセキュリティアーキテクチャは 2 つのグループを念頭に作られていました。1 つは、組織内のすべてにアクセス可能な、信頼できる個人のグループ。もう 1 つは、外部にいる信頼できない個人のグループです。セキュリティ部門や IT 部門は、2 つのグループの間に防御壁を築くことで組織を守るシステムに投資してきました。ファイアウォールによってネットワーク境界を守ることを最重要視するという方法です。想定される脅威と企業エコシステムの安全性との間に壁を設けることには成功したものの、この「フルトラスト」モデルには問題が残りました。ネットワーク境界が侵害されると、攻撃者はかなり容易に企業のイントラネットにアクセス可能なのです。ましてや、悪意のある内部者ならば、境界を侵害すらしなくても被害をもたらすことができます。

「城と堀」のアプローチによる保護



モバイルやクラウドのテクノロジーの導入が進んだ今日、安全な企業ネットワークの外で行われる作業も多くなり、ネットワーク境界を厳密に線引きすることは難しくなっています。こうした状況では、企業の機密資産を守る壁はもはや存在しません。従業員、契約社員、パートナー、サプライヤーは皆、従来の境界を越えてデータにアクセスしています。

クラウドやモバイルの世界では、さらに多くのユーザーがさまざまなデバイスや場所からリソースにアクセスすることが増えます。その中にたった 1 人の悪意ある人間がいるだけで、エコシステム全体が被害を受けてしまうのです。その結果、組織の IT スタックにおいて、どのような場所も信頼できないという状況になりました。

新たなアプローチ : ゼロトラストの誕生と発展

セキュリティを取り巻く状況の変化を受けて、ゼロトラストのアプローチが誕生しました。ゼロトラストとは、Forrester Research 社のアナリストである Jon Kindervag 氏が 2009 年に開発したセキュリティフレームワークです。ゼロトラストは、信頼できる内部ネットワークと信頼できない外部ネットワークという考えを捨て去り、すべてのネットワークトラフィックは信頼できないと考えます。この最初のフレームワークで Kindervag 氏は、ネットワーク境界の見直しを強調するとともに、すべてのネットワークトラフィックをリアルタイムで検証することを推奨しました。これには、ネットワークセグメンテーションゲートウェイが必要となります。同氏が提唱したゼロトラストフレームワークは、次の 3 つの原則で構成されます。1) すべてのリソースは場所を問わずセキュアな方法でアクセスされる必要がある、2) アクセスは厳密に「必要のある人以外には付与しない」よう制御する、3) 組織はユーザーが適切なアクションを実施していることを確認できるようすべてのトラフィックを検査・記録する必要がある、というものです。

ADFS で SSO を実装する場合、その基本となるすべてのコンポーネントを理解することが重要です。ADFS 自体は、「ADFS サーバー」、ADFS サーバーファームと外部アプリケーション間にインストールする「フェデレーションサービスプロキシ」、「ADFS 構成データベース」の 3 つのコンポーネントで構成されます。

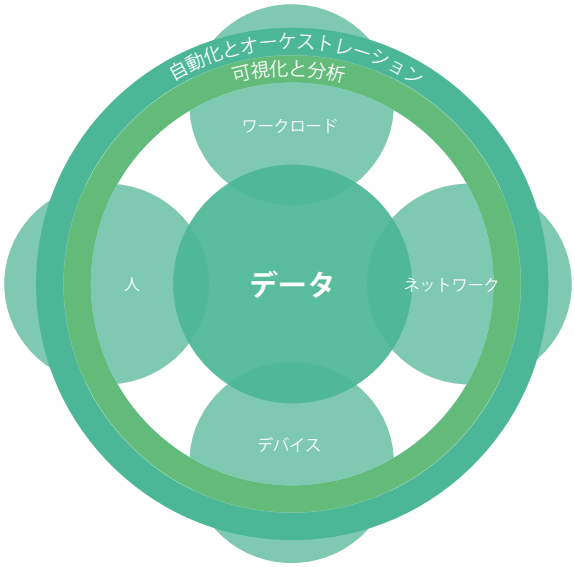
2009 年以降にクラウドとモバイルが台頭したことが契機となり、Kindervag 氏による最初のゼロトラストモデルはさらなる進化を遂げることになります。Gartner 社が 2017 年に発表した CARTA フレームワーク [1] は、Kindervag 氏のゼロトラストモデルを、最初の入り口でアクセスの認証と認可を行う点にのみ重点を置くのではなく、適応型のリスクベースの評価によって想定される脅威を特定することによって、ユーザーエクスペリエンス全体に広げたものです。Google 社が 2014 年に発表した BeyondCorp リサーチ [2] は、適切なゼロトラストを大規模に導入した例として広く知られています。

Forrester 社のアナリストである Chase Cunningham 氏を中心に発展したゼロトラストフレームワーク、Zero Trust Extended Ecosystem（ZTX）でも、ネットワークセグメンテーションを越えたこの移行について強調しています。Cunningham 氏は、ゼロトラストを「次世代のファイアウォール」から「次世代のアクセス」へと進化させました。つまり、人という観点を発展させ、このモデルを成功させるにはネットワークやデータに誰をアクセスさせるかのコマンドや制御が重要だという考え方です。Forrester 社は、シングルサインオン（SSO）などの機能を最重要だと位置付け、多要素認証（MFA）が「脅威を大幅に低減させる」と述べています。[3]

[1] 『Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats（高度な脅威の時代に CARTA の戦略的アプローチでデジタル機会を活用する）』、Gartner, Inc.、2017 年 5 月 22 日

[2] 『BeyondCorp: A New Approach to Enterprise Security（BeyondCorp: 企業セキュリティの新しいアプローチ）』、Google 社、2014 年

[3] 『The Zero Trust eXtended (ZTX) Ecosystem（ゼロトラスト拡張（ZTX）エコシステム）』、Forrester Research, Inc.、2018 年 1 月 19 日



ゼロトラストのモデルが進化しても、基本コンセプトは変わりません。ただし、今日のセキュリティ環境にあっては、その対象はネットワークにとどまらず、システムにアクセスするユーザー、それらのユーザーのアクセス制御という領域にまで拡大しています。アイデンティティ管理が求められ、したがって Okta が貢献できるのは、まさにその分野です。

2009 2011 2013 2015 2017 2019

2009 年: Forrester 社の「ゼロトラスト」が誕生

2018 年: ZTX フレームワークのリリース

2014 年: Google 社の BeyondCorp リサーチが公開

- 特定のネットワークからの接続かどうかでアクセス可能なサービスを決定してはいけない
- サービスへのアクセス許可はユーザーとデバイスの特定に基づいて付与される
- サービスへのすべてのアクセスは認証、認可、暗号化される必要がある

2017 年: Gartner 社の CARTA が公開

継続的で
適応型の
リスクおよび
トラスト
評価

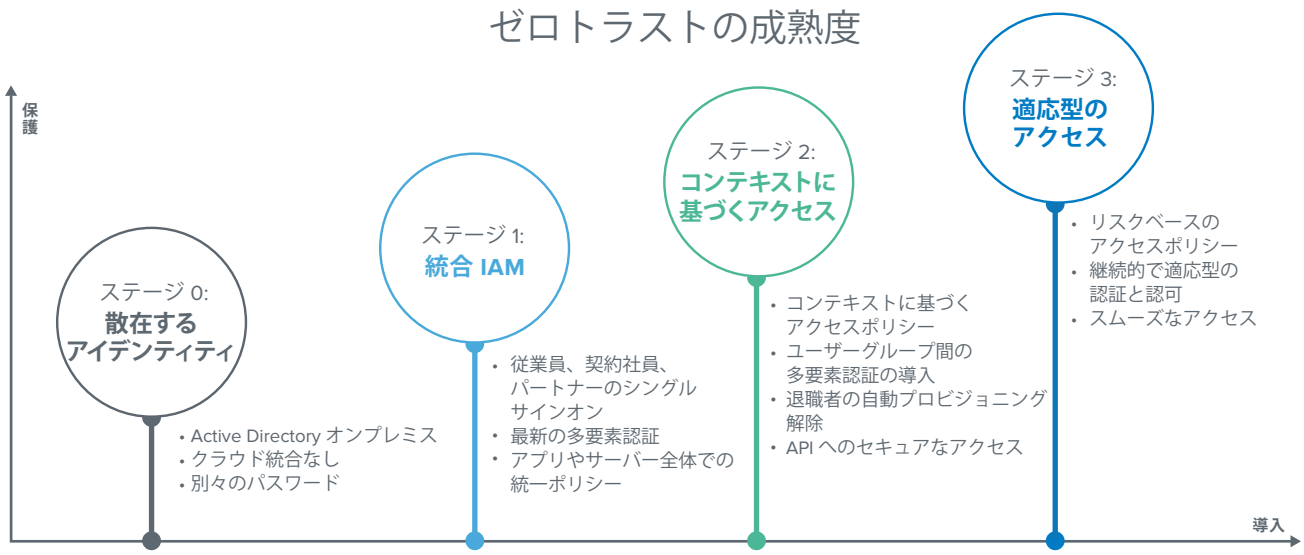
Forrester 社は先日、ゼロトラストに関する新しい調査結果を発表しました。[4] これは、アクセスの重要性をさらに強調しており、Okta をゼロトラストセキュリティ市場の「ストロングパフォーマー」に位置付けています。『The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers（The Forrester Wave™: ゼロトラスト拡張（ZTX）エコシステムのプロバイダ）』（2018 年第 4 四半期）のレポートには多数のベンダーが登場します。その中で Okta は、「人 / 従業員のセキュリティ」、「ZTX のビジョンと戦略」、および「市場アプローチ」の評価基準において最高のスコアを獲得しました。同社は、「従来の「システム」や「インフラ」の概念がなくなり、あらゆる形でアイデンティティの重要性がかつてなく高まっています」と述べています。Forrester 社は、その重要性から、アイデンティティを「ゼロトラストのコアとなる柱」と位置付けています。[5]

[4] 『Future-Proof Your Digital Business With Zero Trust Security（ゼロトラストセキュリティで将来のデジタルビジネスに備える）』、Forrester Research Inc. 社、2018 年 3 月 28 日

[5] 『The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers（The Forrester Wave™: ゼロトラスト拡張（ZTX）エコシステムのプロバイダ）』、2018 年第 4 四半期

アイデンティティはゼロトラストの基盤

ゼロトラストの大原則を簡単に言えば、「決して信頼せず、常に確認する」です。これにより、適切なユーザーが適切なアクセスレベルを持ち、適切なリソースに適切なコンテキストでアクセスし、そのアクセスが継続的に評価されます。ユーザーの手間はかかりません。ゼロトラスト環境は、一朝一夕に実現できるものではありません。組織がゼロトラストアーキテクチャを導入する際には、いくつかのステージを経て成熟度が高まることがわかっています。



ステージ 0: **散在するアイデンティティ**

多くの企業は、さまざまなオンプレミスアプリケーションやクラウドアプリケーションが統合されていない環境、またはそうしたアプリケーションが Active Directory などのオンプレミスディレクトリに統合されていない環境でゼロトラストの導入を始めます。その結果として IT 部門は、多数のシステムに加えて、IT 部門で把握していないアプリケーションやサービスで使われている、散在するアイデンティティの管理を強いられます。ユーザーにとっても、数多くのおそらく安全ではないパスワードを使うことになります。アイデンティティが散在していて全体像が把握できず責任の所在も明らかでないため、IT 部門やセキュリティ部門で管理しきれない領域が広く残り、攻撃者から不正アクセスされて個々のシステムを侵害される危険がある状況です。

ステージ 1: **統合 IAM（アイデンティティとアクセスの管理）**

散在するアイデンティティに起因するセキュリティギャップを埋める最初のステップは、オンプレミスとクラウド全体でアイデンティティを 1 つの IAM システムで統合することです。シングルサインオン（SSO）によるこのステージ 1 の統合は、アクセス管理に欠かせないものです。顧客だけでなく、従業員、契約社員、パートナーまでを広く含む、サービスへのアクセスが必要なすべてのユーザーに適用する必要があります。一元化されたアイデンティティアクセスポイントに 2 つ目の認証要素を加えると、資格情報を標的にした攻撃を減らすうえでさらに効果的です。さらに、IT インフラの重要な要素であるアプリケーションやサーバー間でアクセスポリシーを統合することも、IT 部門が 1 つのセキュアで管理可能な環境で IAM を実現するための鍵となります。

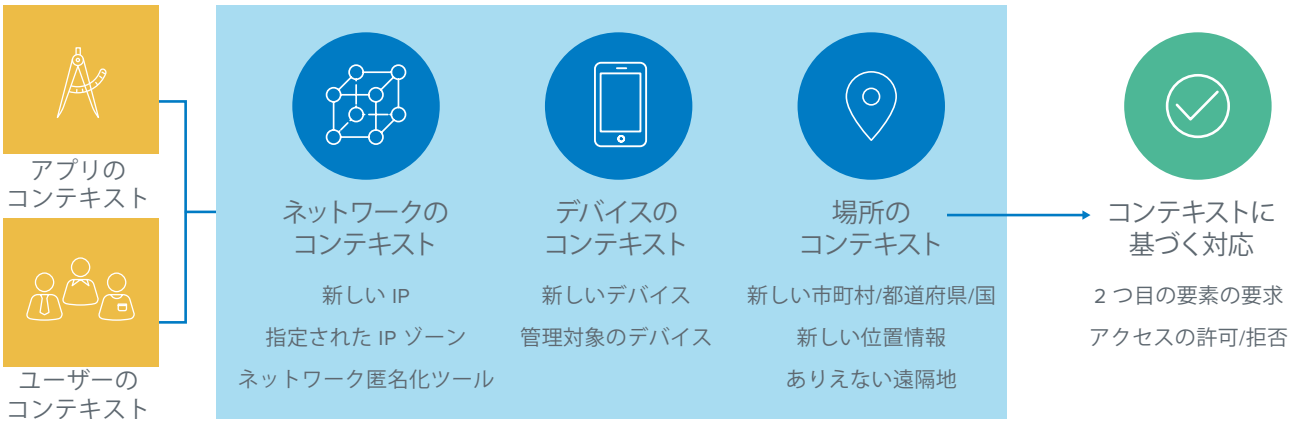
何千もの組織がユーザーアイデンティティの統合に Okta の SSO を利用しています。たいていは、Okta ユニバーサルディレクトリや Okta SSO と組み合わせて導入されています。Okta ユニバーサルディレクトリは、クラウドベースのディレクトリサービスであり、IT 組織にとって唯一の信頼できる情報源として、また複数の AD やオンプレミスのディレクトリサービスの統合ポイントとして機能します。Okta SSO は、広義の企業環境の管理と保護を簡素化し、ユーザーを困らせるパスワードの増加を解消します。Okta アドバンストサーバーアクセスを使えば、IT 部門は同じアクセス制御をサーバーレイヤーにまで拡張し、管理の必要なオンプレミスとクラウドのリソース全体のアクセスをセキュアに管理できます。

ステージ 2: **コンテキストに基づくアクセス**

IAM の統合に続いて、次のステージは、コンテキストに基づくアクセスポリシーを適用することです。つまり、ユーザーのコンテキスト（ユーザーは誰なのか、高リスクのユーザーグループに属しているかなど）、アプリケーションのコンテキスト（ユーザーがアクセスするアプリケーション）、デバイスのコンテキスト、場所とネットワークといった数多くのシグナルを収集し、それらの情報に基づいてアクセスポリシーを適用します。たとえば、企業ネットワークで管理されたデバイスに対してはシームレスなアクセスを許可し、管理対象外のデバイスが新たな場所からログインする場合は MFA を要求するというポリシーを設定できます。また、組織はユーザーグループにまたがって多要素認証を採用し、どのグループが認証を試行したかに基づいて段階的な認証を行うこともできます。たとえば、ワンタイムパスワードを使うスマートフォンを持たない低リスクのユーザーや、価値の高い情報資産へのアクセスには暗号ハンドシェイクを使ったハードトークンを要求することで、サービスに対するセキュアな認証を実現するなどです。さらに、ユーザーが役職を離れたり組織内での役割が変わったりした場合には、自動でプロビジョニングを行うことで、業務で必要なツールにのみアクセスを許可するよう徹底します。退職の場合は、すべてのアクセス許可を取り消すことで、退職後の孤立アカウントや潜在アクセスのリスクを低減します。最後に、こうしたきめ細かなアクセス制御は、職場で使用するすべてのテクノロジーに拡張できる必要があります。たとえば API は最新のアプリケーションの構成要素であると同時にウェブへの機密データ漏えいの原因にもなり得るので、API へのセキュアなアクセスも必要となります。

今や多くの組織がすでに Okta アダプティブ多要素認証を導入して、コンテキストに基づくアクセス管理機能を利用しています。Okta のポリシーフレームワークは、リソースへのアクセス元であるユーザー、デバイス、場所、ネットワーク、アプリケーション、ブラウザを対象としてコンテキストに関するさまざまなインサイトを処理することで、コンテキストに基づいた対応を実現します。この対応の基準となるのが組織のリスク許容度で、これが組織をセキュアに保つ最前線として機能します。たとえば、ユーザーが通常の企業のノートパソコンから認証を試みた場合、正しいパスワードを入力させるというポリシーを設定するだけで十分です。しかし、ユーザーが企業のノートパソコンを使い、外国のパブリック Wi-Fi ネットワークから認証しようとした場合、ポリシーはパスワードに加えて 2 つ目の要素を要求する必要があります。このようなコンテキストに基づくアクセスは、常時ではなく、リスクの高い認証が試行されたときにだけ 2 つ目の要素を要求すればよいため、ユーザーにとっても IT/ セキュリティ部門にとっても好都合です。

コンテキストに基づくアクセス管理



ステージ 3: **適応型のアクセス**

ゼロトラスト導入の最後のステージは、組織がアクセスの認証や認可にまでゼロトラストを拡張している状態です。つまり、認証は最初の入り口だけにとどまるのではなく、ユーザーエクスペリエンス全体が継続的に対象となり、適応型のリスクベース評価によって想定される脅威を特定するしくみです。これは、見たところステージ 2 で設定したコンテキストに基づく対応に、インテリジェントかつリスクベースのエンジンを追加するようなかたちで、前のステージで設定した個別ポリシーの先を行くものです。IT 部門はリスク許容度を設定でき、コンテキスト関連の各種シグナルに基づいてリスク判定を行えるようになりました。これにより、特定の認証イベントのリスク度を判断し、そのインサイトに基づいて 2 つ目の要素を要求することができます。ただし、その信頼も不変のものではありません。適応型の認証では、こうしたシグナルのいずれかに変更がないかを継続的にモニタリングします。ユーザーのコンテキストに何らかの変更が生じた場合は、認証と認可の確認を再度要求します。最後に、こうしたインテリジェントかつリスクベースのアクセス制御によってセキュリティが強化されても、エンドユーザーのエクスペリエンスはシンプルなままで、必要なアクセスはスムーズに得られます。つまり、IT 部門が設定したポリシーに基づいてパスワードなしの認証が可能な場合には、認証の手間はかかりません。

Okta を使えば、管理者はポリシーの設定によって認証にかかわるエンドユーザーエクスペリエンスを変えることができます。認証フローからパスワードを完全に排除することも可能です。1 つ目の認証要素としてパスワードの代わりに Okta Verify や YubiKey など別の要素を使うことで、IT 管理者にとっては選択肢が増えます。さまざまなシグナルに基づくリスク許容度に基づいて段階的な認証を要求する、リスクベースの認証ポリシーを設定することができます。ユーザーの資格情報の信頼度が高い場合、そのユーザーに要求されるのは、パスワード以外の 1 つ目の要素だけです。

Okta は効果的なポリシー中心のアプローチでコンテキストに基づくシグナルデータを取り込む一方、ポリシーエンジンのインテリジェンスもより行動に基づいたものにするよう、継続的に進化させています。

現時点ではほとんどの組織が、ゼロトラスト成熟度ではステージゼロに位置しています。しかし、これらの組織が IT セキュリティについて「決して信頼せず、常に確認する」アプローチを導入していく中で、Okta はより強力でシンプルなアクセス管理を可能にする追加機能を引き続きサポートしていきます。

ゼロトラストアプローチを、より広いセキュリティエコシステムに拡張する

Okta はアイデンティティをゼロトラストの基盤として提供するだけでなく、セキュリティソリューション全体をゼロトラストのアプローチへと緊密に統合します。Okta のインテグレーションネットワークを通して、拡張ゼロトラストエコシステムのあらゆるコンポーネントの緊密な統合への投資を続けていきます。

netskope	McAfee Together is power.	データセキュリティ
paloalto	CISCO	ネットワークセキュリティ
vmware	Carbon Black.	デバイスセキュリティ
CYBERARK	BOMGAR	ワークロードセキュリティ
splunk>	IBM QRadar	分析
servicenow	splunk>	オーケストレーション

このように広いカテゴリをカバーする統合が、Okta Identity Cloud の特長である、ベンダーに依存しないベストオブブリード型のアプローチを支えています。

企業リソースへのアクセスをインテリジェントに制御することは行動モニタリングの前提となりますが、セキュリティ侵害の根本原因を正確に突き止めるのは、特にそれがモノではなく人の問題だと困難です。Okta のセキュリティ分析と SIEM 統合を利用すれば、組織は Okta の充実したアイデンティティコンテキストとユーザーアクティビティを活用して、侵害を受けたアカウントへの修復アクションを実行できます。また、Okta は Netskope や McAfee といった CASB も統合しており、組織は、認証されたセッション中も継続的にリスクの高いイベントをチェックして詳細を確認したり、アラートを受信したりできます。Okta の SIEM パートナー同様、Okta が提供する価値ある認証データにより CASB サービスは異常を正確に検知して Okta に応答を返し、Okta はアイデンティティレイヤーでアクセスを取り消すことができます。これらは、Okta インテグレーションネットワークが企業にゼロトラストを提供する例の、ほんの一部にすぎません。

導入事例 : 21st Century Fox 社

世界最大手のケーブルテレビ、放送、映画、有料テレビ、衛星放送企業である 21st Century Fox 社にとって、セキュリティは常に重大な問題でした。同社は毎日約 50 言語で 18 億の契約者に配信しており、映画やテレビの制作スタジオを含め、ケーブルテレビや放送のネットワークと番組を世界各地に所有しています。数年前、別の大手スタジオが攻撃を受けたことにより、同社のセキュリティ強化は急務となりました。

ステージ 1: ゼロトラストの導入に着手

21st Century Fox 社は、ファイアウォールやウイルス対策ソフトといった従来の境界ベースのセキュリティ対策はすべて配備していました。同社の CISO である Melody Hildebrandt 氏が最初に IT 部門に課したのは、すべての社内ユーザーを同じ環境に集約することでした。この取り組みには認証の強化、つまり、どのユーザーがどのアプリケーションにアクセスを要求しているかを確認しやすくし、アイデンティティ管理プロセスを合理化することも含まれていました。Hildebrandt 氏はコアのアイデンティティとアクセスのインフラを統合すると、新たなゼロトラストアーキテクチャの設計に着手しました。これは、今や大きなニュースとして取り上げられるデータ漏えいの原因となる資格情報の盗難やフィッシング攻撃の対策として役立ちました。こうした変更は、従業員、契約社員、パートナーといった Fox ネットワークを支えるユーザーのエクスペリエンスを損なうことなく行われました。

ステージ 2: 21st Century Fox 社のエコシステム全体を対象に、コンテキストに基づいた動的なアクセス制御を導入

21st Century Fox 社は全社にゼロトラストアプローチを適用するのに Okta Identity Cloud を採用し、従業員向けには Okta のワークフォースアイデンティティ製品を、パートナーや契約社員のエコシステム向けには Okta API 製品を利用しました。同社はすでに Okta SSO、ユニバーサルディレクトリ、およびライフサイクル管理を利用していたため、これら一連の製品にアダプティブ多要素認証と API アクセス管理も追加することにしました。

「Okta を基盤にして、ゼロトラストモデルの成熟度を高めることができました。アイデンティティ管理の基準として、ユーザーが誰なのかを判断するために必要となるさまざまな制御を導入できたのです。Okta によって、ゼロトラストの理解が深まるとともに、導入を早期に実現できました」

–Melody Hildebrandt 氏、CISO、21st Century Fox 社

主要インフラを配備した後は、動的アクセスモデルへの移行が Hildebrandt 氏のチームにとって不可欠でした。これこそが、Okta ライフサイクル管理とユニバーサルディレクトリを導入した理由だったからです。同社の人事管理システム Workday でユーザーのステータスが変更されたらすぐに、ユニバーサルディレクトリはそのユーザーの属性を確認し、適切なグループに振り分けます。続いてライフサイクル管理が、ユーザーの業務に必要なツールやアクセスレベルをプロビジョニングします。

その結果として、ユーザーは初日に必要なすべての情報にアクセスできるようになります。許可されない情報に誤ってアクセスしてしまうリスクも生じません。さらに、ユーザーの資格情報が漏えいするという万一の事態が発生しても、誰かが機密データやコンテンツにアクセスできるリスクは低くなります。また、21st Century Fox 社の従業員が退職したり、パートナーの契約が終了したりした場合、ほぼリアルタイムで必要な処理が行われます。ユニバーサルディレクトリでアカウントがプロビジョニング解除されると直ちにアクセスが取り消されるため、「ゾンビ状態のアカウント」が残ることはありません。アダプティブ多要素認証により、ユーザーが誰で、使用するデバイスの種類は何で、どの場所からどのアプリケーションにアクセスしようとしているかといった要素に基づいてスマートに認証の判断を行うこともできます。つまり、従業員が認証プロセスで不要な手順を強いられることなく、高いセキュリティレベルを維持できます。21st Century Fox 社はアダプティブ多要素認証を導入するに際して、従業員やパートナーの意見に注意深く耳を傾け、Okta Verify、YubiKey、プッシュ送信、音声、SMS、U2F USB トークンを使った Okta Verify など、できる限り多くの要素オプションを用意しました。

21st Century Fox 社におけるゼロトラスト環境 : セキュリティと使いやすさの両立

21st Century Fox 社が Okta を導入したことで簡単かつセキュアに消費者にコンテンツを提供できるようになったことは、結果が成功であることを示しています。その一例が Hot Star です。これはインドで提供しているモバイルアプリケーションで、最近では同時ライブ視聴者が 700 万人を超えています。「リリースから 2 年にもならないアプリとしては、大変すばらしい結果です。このアプリは、インドで初めて、クリケットの試合をモバイルユーザーに配信すると同時に、DDoS 攻撃や流出アカウントを悪用した攻撃といった重大な脅威からユーザーを保護するものでした」と、Hildebrandt 氏は述べています。

Okta を導入したことで、21st Century Fox 社の従業員とパートナーは社外の脅威を心配する必要なく、お客様に楽しんでもらえるコンテンツを提供するという本来の業務に集中することができました。基本的に、ユーザーと IT 部門にとっての複雑さを解消しつつ、大きなセキュリティギャップを埋めることができています。それによってコンテンツはさらに充実し、視聴者のさらなる満足につながるのです。

Okta とゼロトラストの将来

ゼロトラストを実現するうえでの特効薬などはありません。一部のテクノロジーベンダーは別な主張をするかもしれませんが、組織はより高い柔軟性と生産性を求めて、各社の優れた製品を組み合わせた最高のテクノロジーを導入したいと考えています。だからこそ、現在のそのような組織は、ゼロトラストの実現に向けた出発点として、アイデンティティと Okta を頼みに、次世代のアクセス戦略の中核に Okta Identity Cloud を使用して、適切なユーザーのみが適切な情報に適切なタイミングでアクセスできるしくみを目指しています。合言葉は「決して信頼せず、常に確認する」です。

Okta はゼロトラストの実現を目指す組織をすべてのステージで支援するべく、継続的な投資を行っています。当社のブログとセキュリティブログ（okta.com/blog および www.okta.com/security-blog/）をご覧になり、プラットフォームに関する最新情報をご確認ください。

Okta について

Okta は、エンタープライズのための ID 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、世界最大手の数多くの企業で従業員をつなぎ、保護しています。また、企業とパートナー、サプライヤ、顧客とのセキュアな接続も実現しています。5,000 を超えるアプリケーションを緊密に統合することにより、Okta Identity Cloud はあらゆるデバイスを使うあらゆるユーザーに、シンプルでセキュアなアクセスを提供できます。

20th Century Fox 社を始め、Adobe 社、Dish Networks 社、Experian 社、Flex 社、LinkedIn 社、News Corp 社といった何千もの顧客企業が、Okta を信頼し、業務の効率化、収益の向上、セキュリティの維持に役立てています。Okta は顧客が最も重要な業務に必要なテクノロジーを安全かつ簡単に利用できるようにすることで、ミッションを達成できるお手伝いをしています。

詳しくは www.okta.com/jp をご覧ください。


okta