Oktaを使用したレガシーWebアプリケーションのアクセス保護

okta

はじめに

古いWebアプリケーションは、SAMLやOpenID Connectなどの標準規格がまだなかった時代に開発されたため、多くの場合、エンドユーザーのアクセス許可にレガシー認証方式を使用しています。従来であれば、こうしたレガシーアプリケーションでエンドユーザーにシングルサインオンを提供したりアクセス管理を一元化したりするには、Webアクセス管理（WAM）製品が必要でした。これらのオンプレミスソフトウェアツールは導入に手間がかかり、維持費も高額になりがちです。Oktaなら、オンプレミスアプリケーションとクラウドアプリケーションの両方を単一のアイデンティティプロバイダで保護できます。このホワイトペーパーでは、最新の標準規格に対応していないWebアプリケーションをクラウドベースのIDaaS（IDentity-as-a-Service）アーキテクチャに統合する方法をご紹介します。

Oktaによるレガシー認証方式のサポート

Oktaのお客様は皆、それぞれのビジネス分野で新しいことに果敢に挑戦する革新的な企業です。こうした企業が、社員、パートナー、顧客とテクノロジを安全につなぐプラットフォームとしてOktaに信頼を寄せています。Oktaなら、何千ものアプリケーションやリソースの統合的なアクセス管理をすばやく実現できます。どんなに革新的であっても、ある程度成熟した企業であれば、前世代のテクノロジーに依存するレガシーリソースがあるはずです。また、認証に関しても古いモデルが残りがちです。基幹ビジネスアプリケーションでは、非公開のテクノロジーを利用した非効率的な古い認証アプローチが使用されていることがよくあります。そのため、すべてのアプリケーションやリソースにシームレスかつ安全にアクセスできるようにするには、レガシーテクノロジーと最新テクノロジーの両方に対応する必要があります。このホワイトペーパーでは、この課題に対処すると同時に統合アーキテクチャをシンプルに構築する方法をご紹介します。

アプリケーション認証の歴史

Webアプリケーションは、1990年代に企業の間で普及し始めました。しかし、エンドユーザーのアクセス管理が難しく、ユーザーエクスペリエンスが低いため、社内で浸透しないという問題に多くの企業が直面しました。Webアプリケーションに適した認証の標準規格として一般的なものがまだなかったため、多くの企業は、CA SiteMinder、Oracle Access Manager、IBM Tivoli Access Managerなどのwebアクセス管理（WAM）ソリューションを導入して、社内リソースへのアクセスの認証と認可を管理しました。WAMツールでは、Webアプリケーション向けに、シングルサインオン、ポリシーの一元管理、レポートと監査の各機能が提供されます。

2000年代後半に入ると2つの大きな動きがありました。1つは、SAML（Security Assertion Markup Language）やOIDC（OpenID Connect）など、フェデレーション認証の標準規格が人気を集めたこと、もう1つはSaaS、PaaS、IaaSの導入が企業の間で広まり始めたことです。このとき、認証の代替手段として、クラウドと軽量ディレクトリを統合するブリッジ機能をクラウドベースで提供するIDaaS（IDentity-as-a-Service）も誕生しました。フェデレーションの標準規格とクラウドサービスモデルのメリットを活かしたIDaaSでは、高価なインフラストラクチャを導入して保守しなくても、Webアプリケーションアクセスのユーザーエクスペリエンスを大幅に向上できます。

この代替手段への移行が進み、今日では多くの企業がIDaaSを中心に社内のアイデンティティとアクセス管理（IAM）プログラムを一元管理し、アクセス制御の軸足をクラウドに移しています。とはいえ、多くの企業では、まだレガシーアプリケーションを使用しています。最新のIAMアーキテクチャでもそれらを無視するわけにはいきません。そのため企業は、オンプレミスアプリケーションを最新化するか、より直接的にIDaaSと統合できるソリューションを導入するかの選択を迫られています。

Oktaは、オンプレミスのインフラストラクチャをできるだけ減らしながら、レガシーアプリケーションとクラウドアプリケーションを可視化し、アクセス制御を一元化して、ユーザーエクスペリエンスを向上させるためのアプローチを提供します。

Webアクセス管理（WAM）

従来のWAMモデルには、一般的に、プロキシベースとエージェントまたはプラグインベースの2種類があります。プロキシベースのアプローチでは、すべてのWebトラフィックがまずネットワークトラフィックマネージャに集約され、そこでポリシーに基づいてHTTPリクエストの可否が判断されます。このモデルではネットワークコンポーネントを追加する必要がありますが、ソフトウェアをインストールせずにプロトコルレベルの詳細なアクセス制御ができます。一方、エージェントベースのアプローチでは、アプリケーションサーバーまたはWebサーバーにそれぞれエージェントをインストールします。これらのプラグインを使用して HTTPリクエストを処理し、中央のポリシーサーバーに問い合わせを行い、適切なアクセスルールに基づいてレスポンスを返します。このアプローチでは、すべてのトラフィックをプロキシ経由で送受信する必要はありません。しかし、環境内の個々のアプリケーションサーバーにベンダー独自のエージェントをインストールし、管理および更新する手間がかかります。

これに対して、SAMLやOIDCなどの最新の標準規格では、トークンベースのアプローチが使用されます。このモデルでは、アイデンティティプロバイダがアプリケーション（サービスプロバイダ）に、JSON Web Token（JWT）やSOAPペイロードなど、ユーザーに関する情報を含むトークンを渡します。たとえばSAMLでは、SOAPベースのWebサービスメッセージであるSAMLアサーションがトークンとして使用されます。このトークンにはアイデンティティプロバイダの署名が付けられ、ユーザーに関するクレームが含まれます。アプリケーションコードでは、この情報に基づいてアクセスの可否を判断できます。トークンモデルでは、アイデンティティプロバイダ（IdP）とサービスプロバイダ（SP）、つまりアプリケーション間で情報をやり取りするために、エンドユーザーのブラウザコンテキストを暗号化したデータが使用されます。このモデルの利点は、IdPとSPが直接通信する必要がないことです。これにより、ネットワークの変更も、エージェントのインストールも、プロキシ経由でのトラフィックの送受信も不要になります。この利点を実現するためにSAMLとOIDCが誕生しました。これらは今日、人気を集め、従来のWAMモデルに取って代わりつつあります。

ただし、SAMLまたはOIDCにネイティブで対応するにはアプリケーションの修正が必要です。レガシーアプリケーションの最新化は企業にとって最優先の課題とは言えないため、後回しにされたり十分に行われなかったりします。そうなると、アーキテクチャが分断されてしまいます。最近のアプリケーションでは最新の標準規格がサポートされますが、古いアプリケーションではサポートされていません。IAMのメリットを引き出すには、単一のアイデンティティアーキテクチャでこの2つのタイプのアプリケーションに対応する必要があります。

認証方式

アプリケーションの高度なアイデンティティとアクセス管理を目指すには、現在社内で使用している認証方式を把握することから始めます。一般的に、Webアプリケーションのエンドユーザー認証には、以下のいずれかの方式が使用されます。

最新の方式には以下のものがあります。

最新の方式

- **フォームベース認証** — この方式では、カスタムページを使ってエンドユーザーのユーザー名とパスワードを取得し、ユーザーを認証します。Oktaでは、Secure Web Authenticationプラグインを使用することでフォームベース認証がネイティブでサポートされます。

- **SAMLまたはWS-Federationベースのフェデレーション** — この方式では、エンドユーザーはまずアイデンティティプロバイダに対して認証を行い、アイデンティティプロバイダが発行したセキュアトークンを使って他のサービスやアプリケーションにアクセスします。Oktaでは、SAMLとWS-Federationがいずれもネイティブでサポートされます。OktaとSAMLについて詳しくは、Oktaの開発者サイトを参照してください。

- **OIDCベースのフェデレーション** — この方式は、SAMLのいわば最新版です。エンドユーザーが特定のサービスに対して認証を行うと、他のサービスにアイデンティティ情報が安全な方法で渡されます。OktaはOIDCもネイティブでサポートします。OktaとOIDCについて詳しくは、Oktaの開発者サイトを参照してください。

レガシー方式

- **認証なし** — これは匿名アクセスとも呼ばれます。この方式では、誰もが認証なしでサイトにアクセスできます。一般に公開するWebアプリケーションであれば問題ありません。ただし、場合によってはWebページのセキュリティを確保する必要があります。Oktaでは、セキュリティ向上のために認証を必須にして、認証したユーザーのみがアプリケーションにアクセスできるようにすることを推奨しています。

- **ヘッダーベース認証** — Webアクセス管理システムでエンドユーザーに認証を求め、ユーザーが使用するブラウザのHTTPヘッダーにアイデンティティデータを挿入します。保護されたアプリケーションでは、そのデータを確認します。よく使用されるWAMシステムには、CA Siteminder、Oracle Access Manager、Tivoli Access Managerがあります。Oktaでは、この方式を採用する場合、プロキシベースの最新のアーキテクチャに移行することを推奨しています。

- **クライアント証明書ベース認証** — この方式では、PKI証明書を使って、アプリケーションに対するエンドユーザーの認証を行います。この仕組みは、多くのWebサーバーがネイティブで対応していますが、WAMシステムで実装することもできます。Oktaでは、アプリケーションを最新化できない場合、プロキシベースの最新のアーキテクチャを利用してこの方式を採用することを推奨しています。

- **Windows認証** — この方式は、使用するプロトコルによってはKerberos認証とも呼ばれます。この方式では、アクティブなWindowsドメインセッションを使ってユーザーが自動的に認識されます。この仕組みにはドメイン権限が必要になり、デフォルトでは内部ユーザーにのみ使用できます。Oktaでは、この仕組みを使用するアプリケーションへのリモートアクセスを提供する場合、プロキシベースのアーキテクチャと統合することを推奨しています。

- **URLベースの認可** — この方式は、上述の方式の補完として使用されます。URL認可では、Webアクセス管理システムによって、エンドユーザーが要求したURL（レルムまたはURIとも呼ばれます）が認可ポリシーと照合され、リソースへのアクセスの可否が判断されます。認可ポリシーには、ユーザーがリソースへのアクセス権を持っているかどうかを検証するためのルール（通常はグループ単位）が含まれます。

レガシーアプリケーションへの対応

各種の認証方式を理解したところで、既存のWebアプリケーションをすべてIAMプラットフォームに統合するためのアプローチを説明します。次の決定木は、Oktaがお客様に提供しているもので、非常に効果的です。全体像は次のとおりです。各項目の詳細は以降に示します。

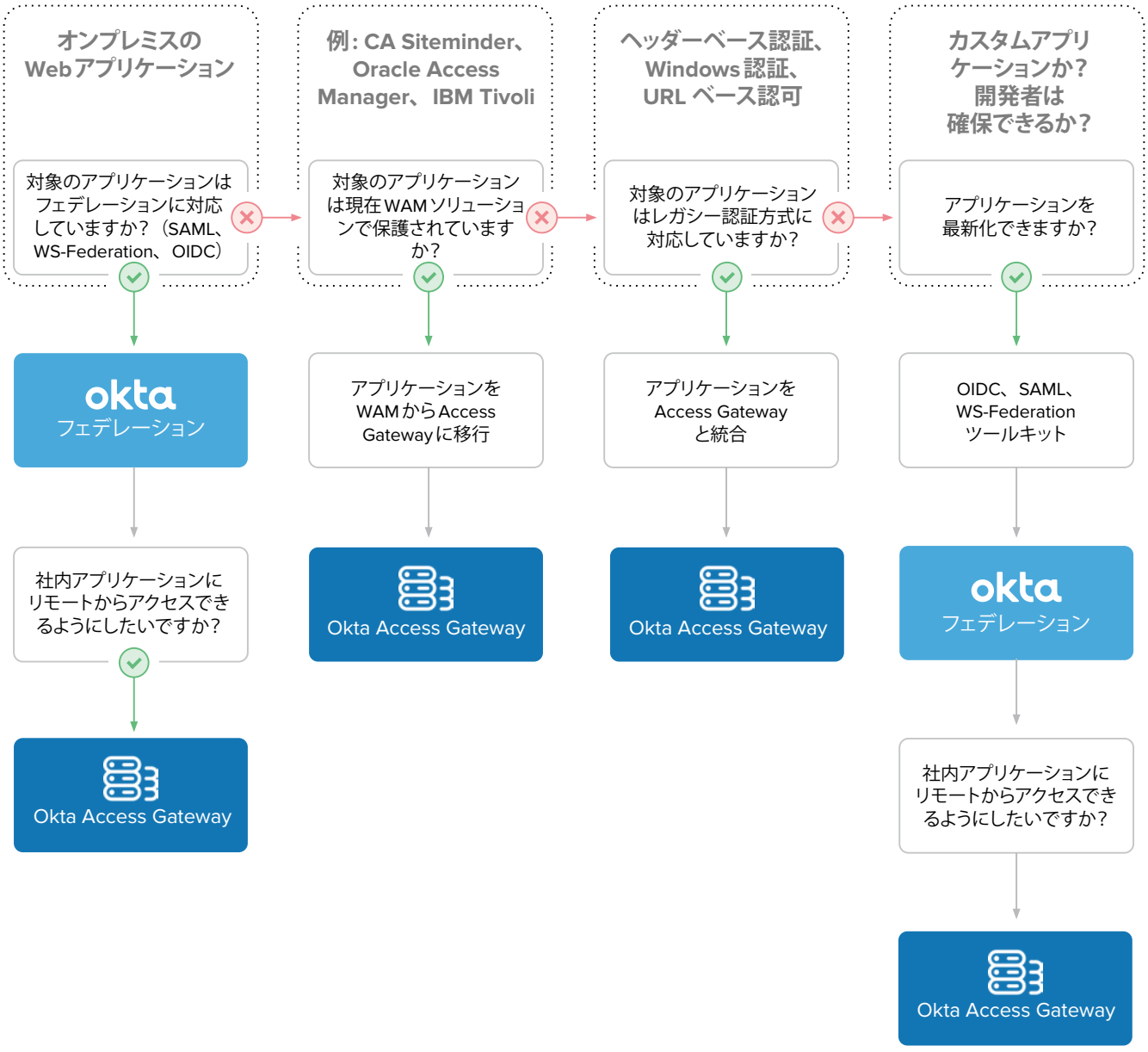

図1: 最新のアイデンティティプラットフォームへの
レガシーアプリケーション統合に関する意思決定プロセス

意思決定プロセス — 詳細

1

対象のアプリケーションは最新の認証方式に対応していますか？

対象のアプリケーションが、SAMLやOpenID Connectなどの最新の標準規格に対応しているかどうかを確認します。最近の企業向けWebアプリケーションにはSAML機能が搭載されていますが、機能を有効にする必要がある場合や、アドオンの追加購入が必要である場合もあります。アプリケーションでこの機能を有効にすれば、Okta Integration Network（OIN）の構築済みのSAML、WS-Federation、またはOpenID Connect統合機能を使ってアプリケーションにすばやく接続できます。Oktaは1000種類以上の構築済みSAMLアプリケーション統合機能を提供しています。しかし、何らかの理由でこの統合機能を利用できない場合は、WS-Federationテンプレートを使用するか、OINのSAMLおよびOpenID Connectアプリケーション統合ウィザードを使用して、独自の統合機能を作成することもできます。（その場合はOktaにお知らせください。該当するアプリケーションをOktaのカタログに追加します）

2

対象のアプリケーションは現在WAMソリューションで保護されていますか？

最新の標準規格に対応していないアプリケーションを保護するために、CA SiteminderやOracle Access ManagerなどのWAMソリューションをすでに使用している場合もあります。その際は、Okta Access Gatewayを使って、オンプレミスのアプリケーションをWAMからOktaに移行できます。このゲートウェイは、Oktaとオンプレミスリソース間でブローカとして機能します。オンプレミス側では、アプリケーションのネイティブでサポートされるレガシー認証方式を使ってアプリケーションに接続します。クラウド側では、SaaSプラットフォームで一般的なセキュリティ標準規格を使って各アプリケーションとOktaを接続します。ゲートウェイを使用する場合、次の3段階で移行を行うのが一般的です。

- **ステップ1**: SAMLを使ってOktaとWAMを統合する。このステップでは、ユーザーがオンプレミスとクラウドの両方のアプリケーションにSSOでグローバルにアクセスできるようにします。また、新しいアプリケーションはOktaに直接統合して、WAMの利用範囲を拡大しないようにします。

- **ステップ2**: オンプレミスのアプリケーションを調査してWAMからOktaに移行する。このステップでは、通常、最初にヘッダーベースのアプリケーションとIWAアプリケーションを移行し、次にエージェントベースのアプリケーションを移行します。エージェントはゲートウェイまたはその他の方式に置き換えます。たとえば、WebLogic Serverの場合はSAML、E-Business SuiteやPeopleSoftなどのシステムの場合はOktaとのネイティブ統合を利用できます。このプロセスで、すべてのアプリケーションをOktaに移行します。

- **ステップ3**: 既存のWAMをバックアップして廃止する。

3

対象のアプリケーションはレガシー認証方式に対応していますか？

企業によっては、レガシー認証方式に対応したオンプレミスのアプリケーションがあっても、WAMソリューションには統合されていない場合があります。これらのアプリケーションは、Access Gatewayを使い、WAMソリューションからの移行時とほぼ同じ方法でOktaに統合できます。唯一の違いは、既存のSSOプラットフォームから移行するのではなく、アプリケーションとAccess Gatewayのドキュメントに従って統合機能を最初から構成することです。

4

アプリケーションを最新化できますか？

この質問は、ほとんどのカスタムWebアプリケーションに当てはまります。アプリケーションを最新化する場合、最も単純な方法は、既存のWebアプリケーションにSAMLまたはOIDCのサポートを追加することです。実装方法はプラットフォームと開発言語によって異なるため、Oktaでは、一般的なプラットフォームでの各種ガイダンスを開発者サイトで提供しています。アプリケーションの最新化にはある程度の時間と労力が必要です。しかし、アプリケーションをモバイルプラットフォームに対応させるなど、ビジネス上の必要性からすでに最新化を行っている場合は、それだけの投資をする価値があると考えられます。

認証（Authentication）と認可（Authorization）の違い

認証とは、何らかのセキュリティ資格情報（パスワードなど）を使ってユーザーとアカウントを結び付けることを指します。一方、認可とは、アプリケーション内でアクセス制御を適用することを指します。認可には3つのレベルがあります。まず、アプリケーションレベルでは、アプリケーションを起動する権限がユーザーに与えられます。次に、URLレベルでは、アプリケーション内でURLにアクセスする権限がユーザーに与えられます。最後に、詳細レベルでは、ボタンをクリックする、フォームに入力するなど、アプリケーションページ内の特定のコンポーネントを表示および操作する権限がユーザーに与えられます。

従来のWAMツールでは、非常に詳細な認可を行うことができます。通常は、独自のSDKやプロトコルを使ってそれらを実行します。こうした詳細な認可が必要な場合、WAMソリューションの置き換えは高コストになります。ただし、アプリケーションを最新化すればそれを回避できます。そのためOktaでは、このような状況でWAMを完全に置き換えるかどうかを判断する際、コスト分析において複雑さを高めに想定することを推奨しています。

完成図

では、Oktaで実現するシンプルな統合アーキテクチャはどのようになるのでしょうか。図2に、Okta Access Gatewayを使ってすべてを統合した場合の構成を示します。

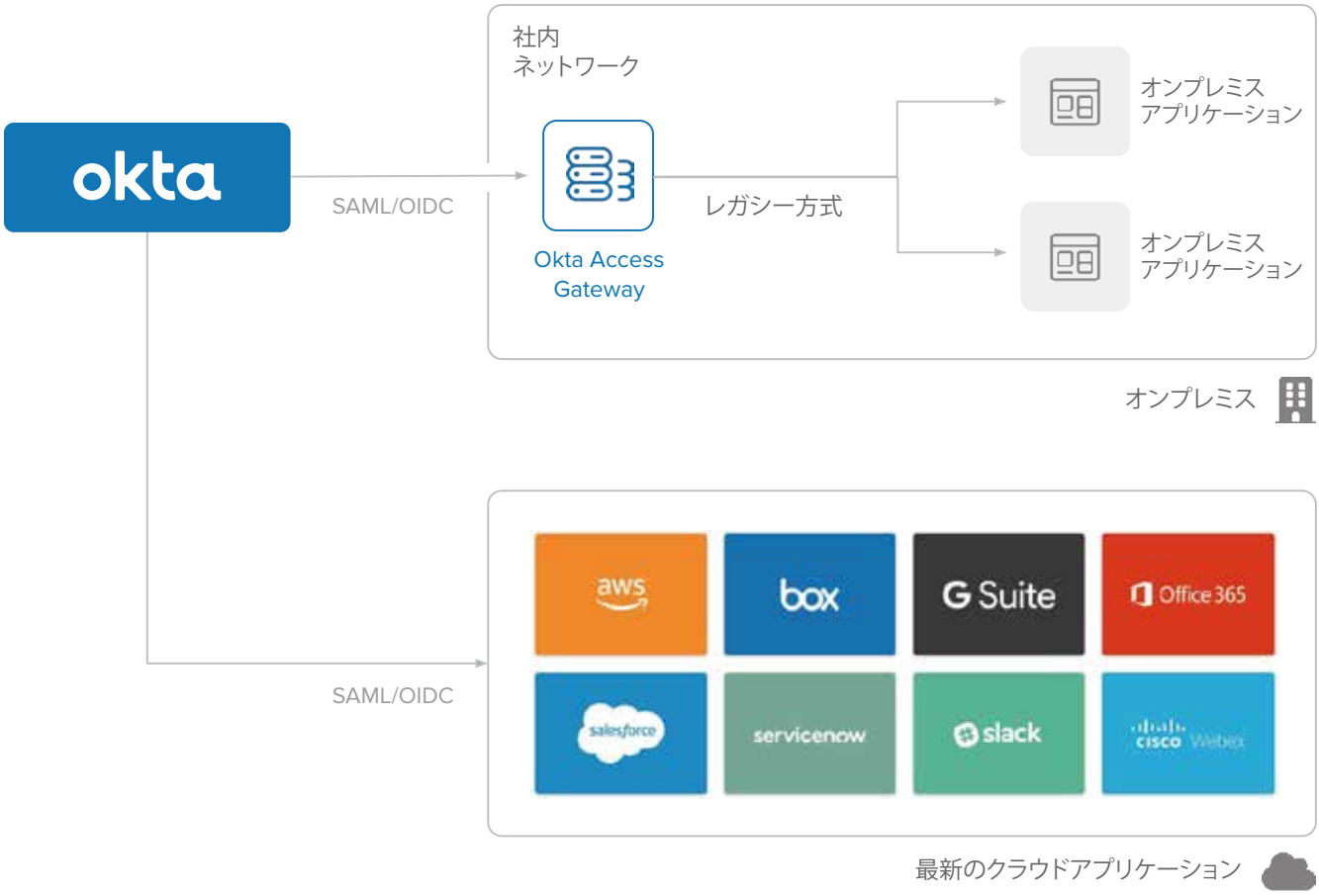

図2: クラウドアプリケーションとレガシーアプリケーションへのアクセスを提供するOktaのリファレンスアーキテクチャ

このアーキテクチャは非常にシンプルです。そしてこの一番のメリットは、すべてのアクセスを単一のアイデンティティプロバイダに集約できることです。

アイデンティティプロバイダを一本化することで、ユーザーがオンプレミスアプリケーションとSaaSソリューションのどちらにアクセスするときも、シングルサインオンのエクスペリエンスを統一できます。また、インフラストラクチャを縮小したり既存のシングルサインオンソリューションを廃止したりすることによってコストを削減できます。さらに、ポリシー管理を一元化し、クラウドで最新の多要素認証を取り入れることによって、セキュリティを向上させることもできます。

その他の一般的なユースケース

オンプレミスのアプリケーションにファイアウォールの外側からアクセスする際の保護

Oktaのお客様は通常、Okta Integration Networkで構築済みの6,000以上の統合機能を利用しています。Oktaでは、フェデレーションの標準規格に対応したアプリケーションを追加するためのフェデレーションプロトコルも完全にサポートしています。さらに、各種のログインフォームを備えたクラウドアプリケーションも簡単にOktaに追加できます。アプリケーションがファイアウォールで保護されている場合、認証だけでは不十分です。アプリケーションが配備されているネットワークにユーザーがアクセスできるようにする必要があります。この場合、VPNを利用するのが一般的ですが、エンドユーザー側にもいくつかの手順が必要になり、面倒になりがちです。

Okta Access Gatewayを使用すれば、エンドユーザーはOktaで一度認証を行うだけで、オンプレミスのアプリケーションにシームレスにアクセスできます。このアーキテクチャでは、ネイティブの認証機構を備えていないアプリケーションや、ヘッダーベース認証に対応していないアプリケーションでもOktaの認証機能を利用できます。

外注先やパートナーによるオンプレミスのSharePointポータルへのアクセス

通常、外注先やパートナーなどの外部ユーザーがオンプレミスのSharePoint Serverを利用できるようにするのは容易ではありません。Oktaなら、フェデレーションを使用してSharePointを統合し、SSOを実現できます。ただし、SharePointのビジネスインテリジェンス機能など、特定のSharePointモジュールを使用する場合は、ユーザーにKerberosトークンが必要になります。Okta Access Gatewayを使用すれば、OktaからKerberosトークンにSAMLアサーションを渡して、SharePointのすべての機能を利用することができます。OktaとAccess Gatewayを組み合わせることで、外注先やパートナーのアイデンティティを管理し、多要素認証を適用することが可能です。

IaaS上でのレガシーアプリケーションの多要素認証

オンプレミスのサーバーをIaaSに移行する場合、これらのリソースへのアクセスを保護する戦略を考える必要があります。IaaSに移行するメリットの1つは、どのネットワークからでも簡単にサービスにアクセスできるようになることです。Access Gatewayを使用すれば、オンプレミスのサーバーにインターネットからアクセスできます。その際は、セキュリティを考慮して、これらのサービスへのアクセスに対して多要素認証を要求することが推奨されます。Oktaでは、ソフトトークン（iOS、Android、Windows Phone）、SMS、または音声通話を要素として使用する多要素認証を簡単に追加できます。

オンプレミスとクラウドのすべてのアプリケーションにアクセスするための単一のエンドユーザーポータル

Oktaのエンドユーザーポータルを使用すれば、エンドユーザーは1カ所からすべてのアプリケーションに簡単にアクセスできます。ポータルはエンドユーザー自身がカスタマイズできるため、利用率の向上も期待できます。Oktaのポータルを使用する場合、エンドユーザーが利用するすべてのアプリケーションをポータルからアクセスできるようにするのが一般的です。Okta Access Gatewayを使用することで、ユーザーはOktaに一度ログインするだけで、クラウドとオンプレミスの両方のアプリケーションに1カ所からアクセスができるようになります。

このアプローチのメリット

このアプローチは、オンプレミスアプリケーションの動作を変更することなく以下のメリットが得られるため、オンプレミスアプリケーションをOktaに統合するのに最適な方法です。

- アプリケーションの展開先に関係なく、すべてのアプリケーションに単一のアイデンティティプロバイダを使用できる
- アイデンティティ用のインフラストラクチャを縮小したり、既存のSSOサーバーを廃止したりすることでコストを削減できる
- セキュリティポリシーを一元管理し、適応型多要素認証を導入することで、セキュリティを強化できる
- ベンダーによるソリューションのサポート終了や提供終了のリスクを移行によって回避できる

まとめ

クラウドの活用は、ビジネスの俊敏性を向上させて、大きな競争優位を確立に役立ちます。もちろん、すべてを一度に移行できるわけではないので、当面はレガシーシステムをサポートする必要があります。最新のアイデンティティ管理プラットフォームを導入して堅実なアクセス管理戦略を立てれば、信頼性の高いオンプレミスアプリケーションと、これから導入する新しいテクノロジーの間のギャップを埋めながら、社内のITを進化させることができます。

詳細情報

Okta Access Gateway、およびオンプレミスのWebアプリケーションの動作を変更せずにアクセスを保護する方法について詳しくは、OktaのWebサイト、www.okta.com/products/access-gatewayを参照してください。