Active Directory と SaaS アプリケーションを統合する 3 つの方法

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

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

目次

SaaS（サービスとしてのソフトウェア）が抱える課題

ここ数年、 SaaS（サービスとしてのソフトウェア）の普及率が大きく伸びています。 試用した Salesforce. com、WebEx、NetSuite といったアプリケーションが全社に導入され、「SaaS 優先」のポリシーを採用する組織が増えています。 実際、 Goldman Sachs 社の調査によると、 58% の中小企業（SMB）が選択肢の 1 つとして SaaS を必ず検討し、 39% が SaaS を利用できるなら利用したいと回答しています。

しかし、 SaaS の導入には課題もあります。 SaaS アプリケーションはサイロ化する傾向があり、 ユーザーのアクセス権および認可の管理負荷という課題が大きくなっています。 ユーザーのオンボーディング作業は、 時間のかかる手動のプロセスであり、 複数の部門の管理者がかかわるため、 リスクが生じる可能性があります。 たとえば、 ユーザーディレクトリが一元化されていないことが多いため、 退職した社員のアクセス権をすぐに無効にできないということがよくあります。 また、「時間や場所を問わずに」アクセスできれば、 生産性向上というメリットを得ることができますが、 一方で、 導入とセキュリティに関する問題も生じることになります。 IT 部門は、 ビジネスリスクを最低限に抑えつつ、 SaaS のメリットを最大限活用できる方法を見つける必要があります。

Active Directory を統合することの重要性

ほとんどの企業では、 Microsoft Active Directory（AD）を信頼できるユーザーディレクトリとして使用して、 メールやファイルの共有といった基本的な IT サービスへのアクセスを管理しています。 また、 多くの場合、 幅広いビジネスアプリケーションや IT システムのアクセス管理にも AD が使用されます。

SaaS アプリケーションはそれぞれ、 個々のサービスへの直接的なアクセスを制御する独自のユーザーディレクトリを使用して開発されています。 また、 SaaS アプリケーションはファイアウォールの外部で動作するため、 元々 Active Directory の制御の範囲外に存在するものでした。

SaaS アプリケーションが普及するにつれ、 IT 部門およびユーザーの双方にとって、 ユーザーディレクトリの重複による複雑さと負担が大きくなっています。 ユーザーは、 Windows ネットワークだけでなく、 それぞれの SaaS アプリケーションのユーザー ID とパスワードも覚えなければなりません。 IT 部門は、 Active Directory と多数の SaaS アプリケーションの両方にユーザーアカウントを作成して管理し、 AD ユーザーを SaaS アプリケーションの対応するアカウントに手動で割り当てる必要があります。

Active Directory と統合されていない複数のユーザーディレクトリを別々に管理することにより、 セキュリティとアクセス管理に関する課題が数多く生じる可能性があります。 SaaS アプリケーションへのアクセスと認可の管理を行うあらゆるソリューションにとって、 AD とのシームレスな統合は欠かせません。

Active Directory との統合により、 上述のようなすべての課題に対処して、 以下を実現する必要があります。

- 双方向のユーザーおよびグループの同期: ユーザーやグループが AD に追加/削除されたときに、 これらの変更を SaaS アプリケーションに反映する必要があります。 具体的には、 SaaS アプリケーションを使用してユーザープロファイルやグループを AD にプッシュできる必要があります。
- アクセス権のプロビジョニングおよびプロビジョニング解除: ユーザーを AD に追加すると、 関連する SaaS アプリケーションを自動的にプロビジョニングし、 逆にユーザーを AD から削除すると、 SaaS のアクセス権を自動的に無効にする必要があります。
- シングルサインオン（SSO）: ユーザーが一度 Windows ネットワークにサインオンすると、 追加で資格情報を入力しなくても SaaS アプリケーションに簡単にアクセスできる必要があります。

上述の要件を満たして Active Directory を SaaS アプリケーションに統合する方法は 3 つありますが、 それぞれ成功の度合いが異なります。

オプション 1: AD との個別の統合

最も実績のある大手の SaaS アプリケーションの中には、独自の AD 統合ツールを提供しているものや、Active Directory とのカスタム統合を独自に開発できる API を公開しているものがあります。主な例が Google Apps、Microsoft Online Services、Salesforce.com などですが、いずれも大きな問題を抱えています。

Google Apps Directory Sync では、Active Directory から Google Apps アカウントへの単一方向でユーザーをプッシュします。これにより、柔軟にインポート対象のユーザー（およびその属性）を定義できます。ただし、セットアップと管理が Google Apps の管理コンソールから完全に切り離されているため、管理者はローカルにインストールした別のユーティリティを使用して管理しなければなりません。継続的な同期という概念がない（同期は手動で実装する必要がある）だけでなく、このツールではシングルサインオンをサポートしていない点に大きな問題があります。このため、SSO を提供するには、さらに別のサードパーティソリューションを利用する必要があります。結果的に SSO とユーザー管理のために 2 つの管理モデルとユーザーストアが個別に存在することになります。

Microsoft Office 365 のディレクトリ同期も、Active Directory から Office 365 への単一方向でユーザーをプッシュします。管理者はこのツールを使って、Active Directory でユーザーの追加/削除を行うときに、Office 365 でのユーザーのプロビジョニングとプロビジョニング解除の両方を実施できます。Google Apps のツールと同様に、メインの管理エクスペリエンスとは切り離されているため、管理はオンプレミスのユーティリティで行います。また、SSO も提供しておらず、こちらも管理モデルとユーザーストアが 2 つ個別に存在することになります。

Salesforce.com は API を公開しているため、AD からユーザーをプッシュしたり、Salesforce.com にアクセスするユーザーを AD で認証したりする独自のソリューションを構築できます。ただし、これらの処理を実現するための使いやすいツールが用意されていません。このため、統合の要件を満たすために開発やメンテナンスに膨大な投資を行う必要があります。

これらのベンダー固有のオプションによる AD 統合の欠点は明らかです。組織は、最低でも各ベンダーのツールをインストールし、メンテナンスする必要があります。一方、そういったツールが用意されていない場合、組織はベンダーに合わせて独自のソリューションを開発しなければなりません。このようなソリューションを開発してインストールした後も、SaaS アプリケーション全体でメンテナンスが必要な一連のテクノロジが存在するため、IT のコストが増加します。

オプション 2: Microsoft AD FS の利用

Microsoft 社は、Windows Server 2008 R2 の発売と同時に、Active Directory Federation Services（AD FS）2.0 をリリースしました。AD FS は、ファイアウォールの外部にあるアプリケーションに対してシングルサインオンを実現できる拡張性の高いプラットフォームです。このため、AD FS を利用すれば、AD 統合の SSO 要件を満たすことができます。ただし、ユーザーの同期やユーザーのプロビジョニング/プロビジョニング解除には対応していません。

SSO のニーズを満たすために AD FS の利用を検討する場合には、プラットフォームを必ず考慮することが重要です。Windows Server の一機能であり、プラットフォームとして開発された AD FS は、元々、シングルサインオンのニーズを満たすエンドツーエンドのソリューションではありませんでした。プラットフォームとは一般的に、効果的で優れた柔軟性を備えていますが、包括的なソリューションを開発するには膨大な追加作業が求められます。

しかし、AD FS は無料のソリューションであるにもかかわらず、なぜ利用する組織が少ないのでしょうか。AD FS ベースのソリューションには、ハードウェアとソフトウェアが必要になります（AD FS 自体を構成するサーバーロールには、Federation Service、Federation Service Proxy、Web サーバーエージェントの 3 つがあります）。さらに、AD FS ではカスタム開発とメンテナンスも必要となるため、管理者が対象の SaaS アプリケーションとの SSO の接続を理解して設定し、メンテナンスするまでに時間がかかります。このような要件をすべて考慮すると、AD FS ベースのソリューションが無料にはならないことは明らかです。

AD FS を構成するには、有効な SSL 証明書を取得する必要があります（テストの場合は自己署名証明書で十分ですが、本番環境では第三者機関の署名が必要です）。セットアップ作業では、SSL 証明書のインポート、証明書のエクスポート、共有証明書の作成などを行い、AD FS サーバーと対象のフェデレーションサービスとの間の信頼関係を確立します。信頼関係が確立されたら、対象の SaaS アプリケーションとの認証を行うための適切なクレームルールを生成する必要があります。

クレームルールは、システムと統合する SaaS アプリケーションによって大きく異なります。管理者は、SaaS アプリケーションの URI（Uniform Resource Identifier）、アプリケーションに必要なクレーム、アプリケーションでユーザーに公開する URL、そしてトークンを暗号化するかどうかを把握する必要があります。AD FS では、ほとんどの環境に対応できる柔軟なルールエンジンを提供していますが、すべての統合でこれらのルールだけを定義すればよいわけではありません。この他にも、対象の SaaS アプリケーションの変更に伴い、継続的にルールをメンテナンスする必要もあります。

各 SaaS アプリケーションに最適なクレームルールを見つけるために、ブログ記事、Web サイト、技術文書などを調査する作業は時間がかかり、そうして見つけた情報の信頼性も保証されません。時間の経過とともに各アプリケーションのルールが変わることで、SSO 統合が無効になる可能性もあります。このため、このような変更を追跡する必要があります。

AD FS インフラストラクチャを構築し、対象の各 SaaS アプリケーションに適したクレームルールを作成しても、実際にユーザーがどのように SSO を利用してこれらのアプリケーションにアクセスするかを判断しなければなりません。おそらくは、ユーザーがこれらのアプリケーションにアクセスできるポータルを作成するか、既存の自社ポータルにアクセスを統合する必要が生じるでしょう。

AD FS 2.0 は、AD と SaaS アプリケーションの統合に利用できる強力なプラットフォームであることには間違いありません。しかし、最終的に、組織はかなりの時間とコストをかけなければ、エンドツーエンドのソリューションを開発してメンテナンスすることができず、Active Directory 統合に関する課題の 3 分の 1 にしか対応できません。

オプション 3: サードパーティベンダーのソリューションの利用

SaaS アプリケーション導入のスピードが加速する中、企業のシングルサインオンとユーザー管理のニーズに対応できるベンダーがいくつか登場しました。これらのベンダーを完全に評価するには、Active Directory との統合機能を理解する必要があります。アプリケーション固有の統合戦略とは異なり、これらのソリューションを使用して 1 カ所でオンプレミスの Active Directory を統合し、SaaS アプリケーション全体をフェデレーションできる必要があります。また、AD FS のオプションと違い、一部のベンダーではメンテナンスを請け負い、既存の AD インフラストラクチャとも連携できる完全なソリューションも提供します。

こういったベンダーが提供する AD の統合機能を評価する際は、考慮すべき以下のような要素がいくつかあります。

- ソリューションまたはツールキットによる提供: 製品を追加購入したり、インストールサービスを購入したりする必要がないオプションを選択します。また、カスタム開発をしなければユーザーがメリットを実感できないオプションも選ぶべきではありません。代わりに、以下を実現できる必要があります
  - サービスを利用しなくても、シームレスに AD と統合できる
  - 事前統合されたビジネス用および個人用アプリケーションが豊富に用意されている
  - AD との統合により、前述した、双方向のユーザーおよびグループの同期、シングルサインオン、プロビジョニング/プロビジョニング解除の 3 つの主要要件に対応できる
  - すべてのユーザーがあらゆる SaaS アプリケーションにシングルサインオンでアクセスできるポータルが提供されている
  - 1 つのコンソールで、時間と場所を問わずにユーザー、アプリケーション、AD 統合を管理できる管理ツールがある
- ハードウェアの購入とメンテナンスが必要: SaaS アプリケーション自体と同じように、100% オンデマンドで、可用性が高く、ハードウェアを必要としないソリューションを選ぶ必要があります
- 長期にわたる統合環境の維持: 完全なソリューションを使用して、基盤となる SaaS アプリケーションに変更が生じてもその影響を業務に与えることなく、長期的にユーザーと SSO を管理できる必要があります

- 安全で設定が不要の統合: AD との統合はすべてアウトバウンド通信で実現します。通信には標準の HTTPS を使用して安全を確保し、既存のファイアウォールの設定を変更しないように構成します
- アーキテクチャによるユーザーエクスペリエンスの低下: パフォーマンスとユーザーエクスペリエンスを最大化するには、SSO ソリューションでの認証を実現し、ユーザーに負担をかけないようにする必要があります。すべてのトラフィックをプロキシ経由でルーティングするとボトルネックが生じ、パフォーマンスが低下します。また、一般的に使用率が上がっても拡張できません

Okta が提供するすべての SaaS アプリケーション向けの AD 統合

Okta は、顧客の成功を第一に考えてクラウドでゼロから構築された、企業向けのアイデンティティ管理サービスを提供します。Okta のサービスでは、ディレクトリサービス、シングルサインオン、強力な認証、プロビジョニングのワークフロー、そして組み込みのレポート機能を活用できます。世界中の企業が Okta を利用して、あらゆるアプリケーション、ユーザーまたはデバイスでのアクセスを管理してセキュリティと生産性を向上し、コンプライアンスを確保しています。

Okta のサービスには、業界で最も実績のある包括的で使いやすい Active Directory 統合ソリューションが用意されています。Okta のサービスと Active Directory 向けの統合コンポーネントのメリットは以下のとおりです。

- サービスのインストールが不要で、次の機能を備えた完全にエンドツーエンドのソリューション:
  - 自動設定が可能で、安全性が高く、既存の AD インフラストラクチャと自動で包括的な統合が可能。手動によるグループの割り当てが不要
  - 事前統合されたビジネス用および個人用アプリケーションを豊富に提供。Okta が統合の管理と更新を行うため、基盤となるアプリケーションが変更されても、安心してシームレスな統合環境を維持できる
  - あらゆるユーザーがホームページとモバイルアプリケーションにシングルサインオンでき、1 クリックですべての Web アプリケーションにアクセス
  - 統合された管理エクスペリエンスにより、ユーザー、アプリケーション、AD 統合を 1 つのコンソールで、場所や時間を問わずに複数のデバイスで管理可能
- リアルタイムの同期: 環境を保護するには、退職した社員のアクセス権を速やかに無効にする必要があります
- 双方向の同期: Okta では、オンプレミスとクラウドサービスのハイブリッド環境向けに、SaaS アプリケーションから AD に対してグループとユーザープロファイルをプッシュできます
- 100% オンデマンドのサービス: Okta の主要サービスでは、フットプリントがきわめて小さいマルチテナント型のソリューションを提供します。AD エージェントをローカルでインストールするため、ハードウェアの購入やメンテナンスは一切不要です
- シームレスで優れた可用性: 並列実行する Okta エージェント間のフェイルオーバーは瞬時に行われるため、ユーザーへのサービスの中断がありません。また、専用のハードウェアも不要です。

- 単一の AD 統合: 一度設定すれば、 SaaS アプリケーション全体に対して Active Directory のフェデレーションを行えます
- HTTPS を使用したアウトバウンド通信による AD 接続: Okta の軽量エージェントを使用すれば、 HTTPS によるアウトバウンド通信だけを使用して安全に接続を確立できるため、 ファイアウォールの設定を変更する必要がありません。
- 帯域外認証: Okta は、 SaaS アプリケーションのユーザー認証を行うことで、 スムーズな認証プロセスを実現します。 その後のトラフィックはすべてユーザーとアプリケーション間でやり取りされます。
- Active Directory の信頼できるドメインと信頼できないドメインを同時に統合可能

無料トライアルの利用

Active Directory と SaaS アプリケーションの包括的で簡単な統合方法や、クラウドベースのアプリケーションの安全な拡張方法を確認するには、www.okta.com/freetrial にアクセスして Okta をお試しください。

Okta について

Okta は、 人とテクノロジを安全に結びつけるための基盤です。 Okta はクラウドの力を活用することで、強力なセキュリティポリシーを適用しながら、ユーザーがいつでもどのデバイスからでもアプリケーションにアクセスできるようにします。 また、企業の既存ディレクトリやアイデンティティシステム、4,000 個を超えるアプリケーションを直接統合します。 Okta は統合プラットフォーム上で稼働するため、 サービスを迅速に拡張し、 全体的なコストを削減することができます。 Adobe 社、 Allergan 社、 Chiquita 社、 LinkedIn 社、 MGM Resorts International 社、 Western Union 社を始めとする 2,500 を超える企業が、 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を実現しています。

詳細については www.okta.com/jp/ をご覧いただくか、 www.okta.com/blog より弊社のブログをフォローしてください。