okta

Okta によるディレクトリ統合

アーキテクチャ概要

Okta Japan 株式会社
〒 150-0002 東京都渋谷区渋谷 2 丁目 24 － 12
渋谷スクランブルスクエア 38 階

Marketing-Japan@okta.com

目次

ユーザーディレクトリとクラウド：概要

ほとんどの企業では、Microsoft Active Directory（AD）や、SunOne、Oracle Internet Directoryといった Lightweight Directory Access Protocol（LDAP）ディレクトリが、アイデンティティとアクセス管理のポリシーを調整する中心的な役割を担っています。一般的に、ADやLDAPはユーザーアイデンティティの「信頼できる情報源」として機能し、ネットワーク、ファイルサーバー、ウェブアプリケーションなどのオンプレミスリソースへのアクセスを制御しています（図1を参照）。オンプレミスアプリケーションがActive DirectoryまたはLDAPに統合されている場合、ユーザーには最上のエクスペリエンスが提供されます。つまり、一度ドメインにログインするだけで、適切なリソースへのアクセスが付与されます。また、管理者にとっても、どのユーザーが何にアクセスできるかを明確に管理できるというメリットがあります。このモデルは、LANベースのアーキテクチャで、アプリケーションがファイアウォール内のハードウェアで稼働している限り、どの場所でも効果的に機能します。しかし、これから詳しく見ていくように、企業でクラウドベースのアプリケーションへの移行が進むのに伴い、このアプローチでは無理が生じます。そこで、新しいソリューションが必要になるのです。

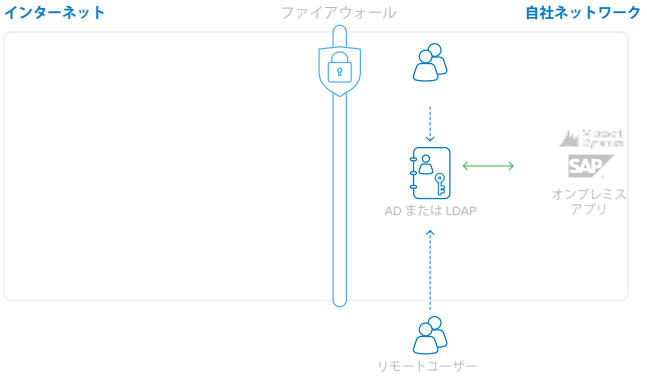

図1: オンプレミスアプリケーションのユーザーアイデンティティ用のADまたはLDAP

クラウドアプリケーションへの移行の副産物として、個々のユーザーストアも急増しています。各クラウドアプリケーションは個別に導入されるのが通常なので、ユーザー資格情報のデータベースがそれぞれ固有に存在することになります（図2を参照）。アプリケーションが1つや2つならば少しの手間で済みますが、企業が膨大な数のクラウドアプリケーションを導入すればするほど、管理者の手に余るユーザーディレクトリが増えていくのです。この問題は深刻化するばかりです。新しいアプリケーションが増えるたびにユーザーのパスワードも増えるため、管理者はどのユーザーが何にアクセスできるかを制御しきれなくなってしまいます。さらに困ったことに、従業員が退職した場合、多くの企業ではどのアカウントを非アクティブ化すべきかを正確かつ迅速に把握できません。また、適切なタイミングで必要なプロビジョニング解除が行われているかを監査する能力もありません。

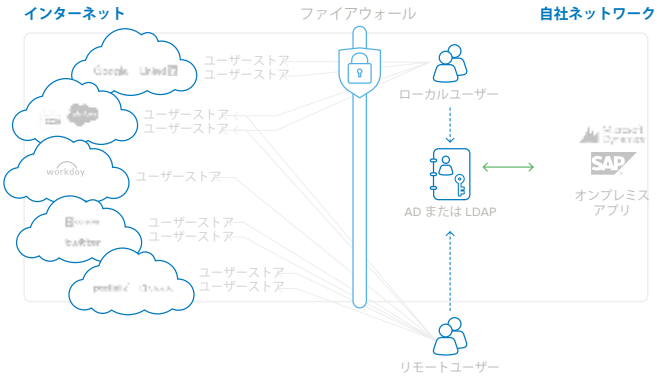

図2: クラウドアプリケーションの導入に伴い、ユーザーストアが急増

独立したユーザーストアが急増することに対処するソリューションの1つとして、すべてのクラウドアプリケーションを単一の共有アイデンティティストアに統合する試みがあります（図3を参照）。Active DirectoryまたはLDAPのユーザーストアは確かに、こうしたストアとしては最も有効な選択肢です。なぜなら、オンプレミス、クラウドベースの両方のアプリケーションにアイデンティティ管理を提供できるからです。一部のクラウドアプリケーションベンダーは、企業向けにアプリケーション単独のアイデンティティストアをADまたはLDAPに接続するためのAPIやツールキットを提供しています。しかし、API経由の統合にはカスタム開発が必要となり、ツールキットもそれぞれ異なるため、多くの場合はセットアップ、機器（コネクタソフトウェアを実行するためのハードウェア）、メンテナンス（アプリケーション変更が生じた場合）に膨大な投資が必要となります。クラウドアプリケーションの増加につれて、アプリごとのADやLDAP統合というモデルは、法外にコストのかかるものとなります。事業運営のために実行すべき新しいアプリケーションは常に発生しているからです。

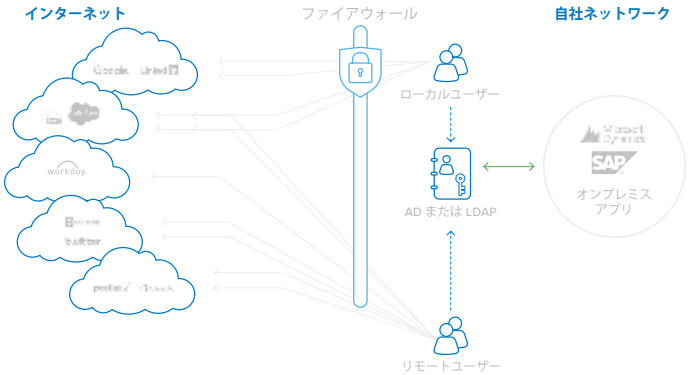

図3: 複数のクラウドアプリケーションの統合は、コストとメンテナンス負荷が高い

Oktaのクラウドベースのアイデンティティおよびアクセス管理サービスは、単一の統合ポイントであらゆるクラウドおよびウェブベースアプリケーションのAD/LDAP統合に対して高可用性ソリューションを提供することにより、こうした問題を解決します。

Oktaは、自社で複数のオンプレミスディレクトリを統合しようとすることで生じるさまざまな問題を解消します。

自社でAD/LDAP統合を試みる場合に注意すべきこと

こうした統合を開発するのに適切なスキルセットがあるか？
統合のアップグレードとメンテナンスの方法は？
統合の健全性を監視する方法は？
各クラウドアプリケーションへの接続に使用するプロトコルは？
ツールキットで自社開発した統合を実行しているサーバーで障害が発生した場合は、どうなるか？
複数ドメインで構成されたADまたはLDAPとクラウドアプリをどう統合するか？
クラウドアプリとAD/LDAPを統合するたびに、ファイアウォールでどのような変更が必要なのか？

Oktaのアプローチ

Oktaなら、統合にプログラミングや開発の経験は必要ありません。独自の使いやすいインターフェイスにより、数分で完了します。
Oktaは複数のISVと連携して変更を監視し、既存のAPIをアップグレードすることにより最新機能を利用できます。アップデートを毎週リリースして変更を反映します。
Oktaは継続的に既存の統合を監視およびテストすることで、アップグレードやリリースの後でも統合機能が想定どおり機能していることを確認します。
Oktaを使う場合は、SAML、OAuth、SCIM、その他多くの統合プロトコルの知識は必要ありません。Oktaが代わりに統合を管理するためです。
Oktaは冗長エージェントアーキテクチャにより自動的にフェイルオーバーリカバリを行います。
Oktaには、複数のAD/LDAPドメイン環境のサポートがあらかじめ組み込まれています。
OktaではADまたはLDAPの統合をサポートするのに、ファイアウォールの変更は不要です。

Oktaを配置すると、企業は従業員のユーザーアイデンティティに社内ディレクトリを引き続き活用しながら、新たなクラウドアプリケーションを自由に追加できるインフラストラクチャを得られます。これにより、ユーザーは既存のADやLDAPの資格情報を使ってあらゆるクラウドアプリにアクセスできます。また、IT管理者は単一のコントロールパネルからこれらのアプリケーションを制御できます。さらに、ADやLDAPのセキュリティグループと個々のユーザー割り当てが統合されます。

Oktaのディレクトリ統合により、すべてのクラウドアプリを統合

Oktaは、クラウドアプリケーションとオンプレミスウェブアプリケーションを全面的に統合できる、使いやすいディレクトリ統合ソリューションを提供します。Oktaによるオンデマンドのアイデンティティおよびアクセス管理サービスでは、ユーザー認証、ユーザープロビジョニング/プロビジョニング解除、アプリケーション利用状況に関する詳細な分析とレポートの機能を、クラウドアプリケーションとオンプレミスウェブアプリケーションの両方で実現します。このサービスの主要なコンポーネントは、簡単なセットアップで高可用性を実現する、Oktaのディレクトリ統合機能です。また、OktaのApplication Network（OAN）では何千ものアプリケーションをサポートしており、統合をメンテナンスします。

ADの統合については、次の3つの軽量かつセキュアなオンプレミスコンポーネントを提供します。

- Okta Active Directoryエージェント：すべてのWindows Serverにインストールできる軽量のエージェントで、ユーザーのプロビジョニング/プロビジョニング解除、認証リクエストを処理するオンプレミスのActive Directoryに接続されます。
- Oktaの統合Windows認証（IWA）ウェブアプリケーション：Internet Information Services（IIS）にインストールされる軽量のウェブアプリケーションで、統合Windows認証を介してドメインユーザーを認証します。
- Okta Active Directoryパスワード同期エージェント：ドメインコントローラにインストールされる軽量のエージェントで、ADパスワードの変更を自動で同期し、Oktaに送信することでユーザーのADパスワードとアプリのパスワードを同期します。

LDAPの統合については、単一の軽量かつセキュアなオンプレミスコンポーネントを提供します。

- Okta LDAPエージェント：すべてのWindows Serverにインストールできる軽量のエージェントで、ユーザーのプロビジョニング/プロビジョニング解除、認証リクエストを処理するオンプレミスのLDAPユーザーストアに接続されます。

OktaのAD/LDAPエージェント、Okta IWAウェブアプリ、Okta ADパスワード同期エージェントは、Oktaのクラウドサービスに組み込まれ、セットアップとメンテナンスが容易で可用性に優れたアーキテクチャを構成して、さまざまなユースケースをサポートします。本ホワイトペーパーでは、この柔軟なアーキテクチャについてさらに詳細をご紹介します。

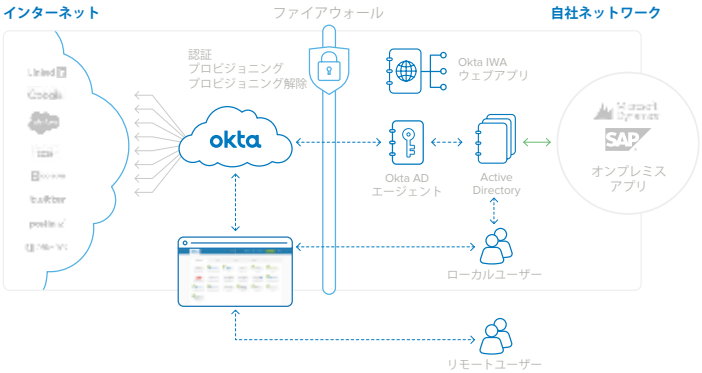

図4: Active Directoryの場合のOktaアーキテクチャ：1つの統合ですべてのウェブアプリケーションに対応

Oktaのディレクトリ統合には、次の特長があります。

- シンプルでセキュアなセットアップと設定
- リアルタイムのプロビジョニング
- インテリジェントなユーザー同期
- ジャストインタイムのユーザープロビジョニング
- 堅牢な認証の委任
- 統合デスクトップシングルサインオン（SSO）（ADのみ）
- セルフサービスによるパスワードリセットのサポート（ADのみ）
- セキュリティグループによるプロビジョニング
- ワンクリックの自動プロビジョニング解除
- ディレクトリ認証済みアプリのシングルサインオン

シンプルでセキュアなセットアップと設定

Oktaでは、ウィザードを使って簡単にディレクトリを統合できます。Okta管理コンソールからワンクリックで、Okta Active Directoryエージェントまたは LDAP エージェントをダウンロードし、ドメインコントローラにアクセス可能なあらゆるWindows Serverにインストールできます。Oktaエージェントは、ドメインコントローラとは別のサーバーで実行されます。

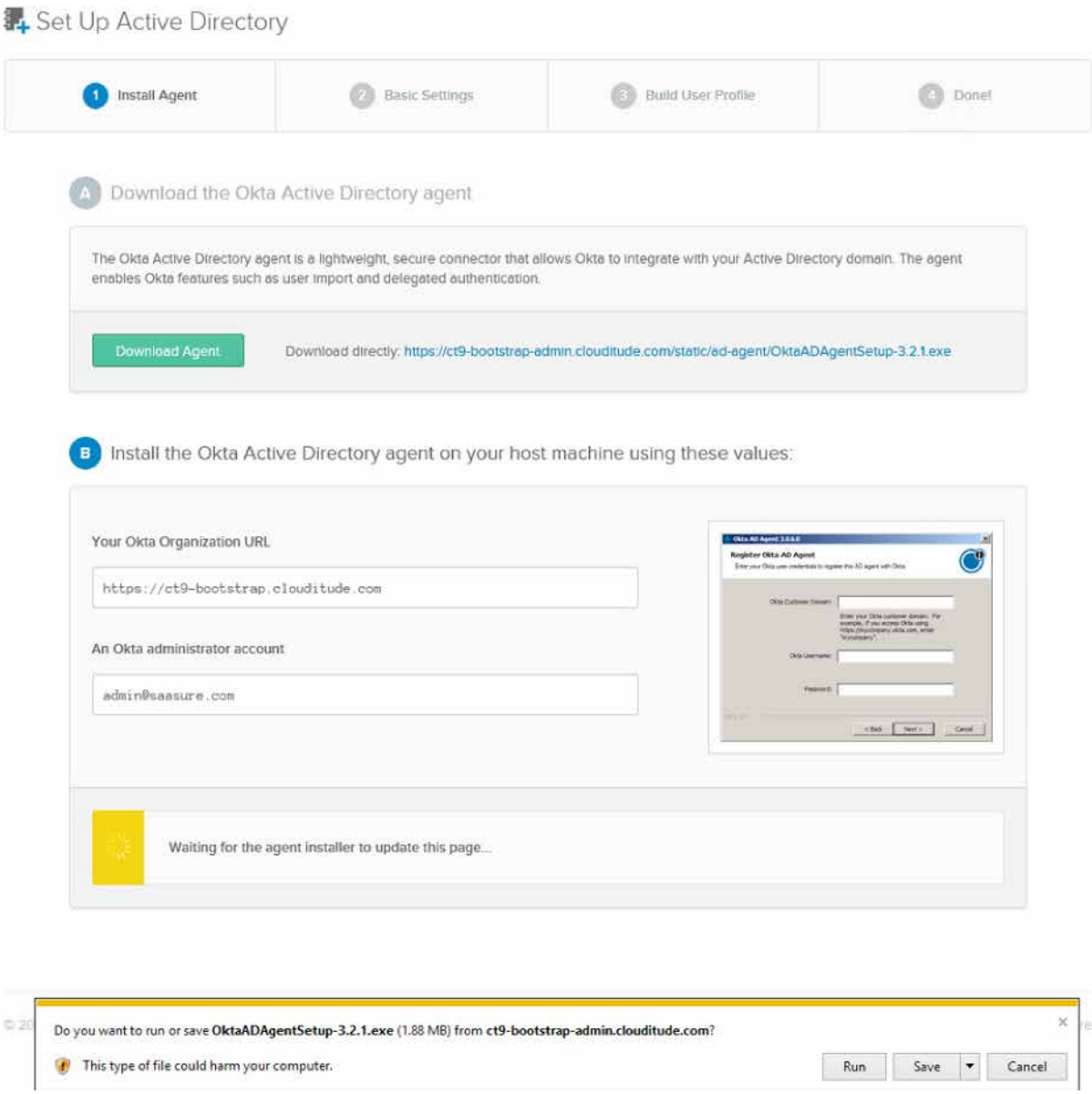

図5: Active Directoryのインストールプロセス

リアルタイムの同期

インストール中、OktaのURLとAD管理者の資格情報を入力するだけで、OktaのADエージェントが権限の低い読み取り専用の統合アカウントを作成し、Oktaインスタンスとのセキュアな接続を確立します。その際、ネットワークやファイアウォールの設定は不要です。

Okta ADエージェントは、443番ポートのアウトバウンドのSSL接続を使ってOktaクラウドサービスに接続します。この接続のサイクルは30秒間で、すべての既存ファイアウォールまたはセキュリティデバイスとの互換性が確保されます。大まかに言えば、ユーザーがAD資格情報を使ってホストマシンにログインでき、ブラウザからインターネットにアクセスできれば、Okta ADエージェントは正常に機能し、ファイアウォールを変更する必要はありません。

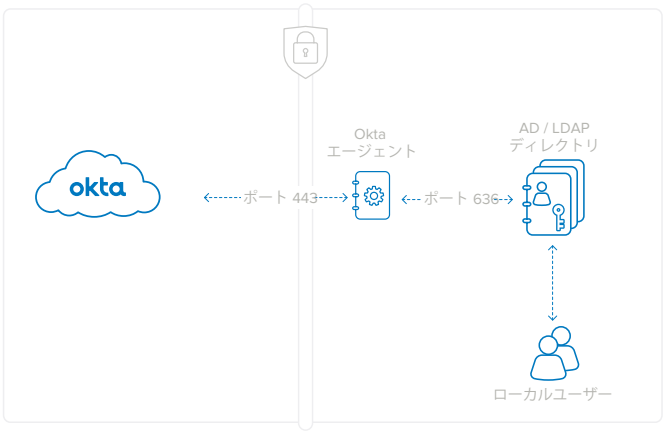

図6: OktaエージェントはADへの接続に443番ポート（SSL暗号化）を、LDAPへの接続に636番ポートを使用。ADエージェント、LDAPエージェントの双方ともファイアウォールの変更は不要

Okta AD/LDAPエージェントとの通信は、SSLと相互認証によりセキュリティ保護されています。具体的には次のとおりです。

- Okta AD/LDAPエージェントからOktaサービス：エージェントは、Oktaサーバーのmycompany.okta.comのSSL証明書を検証することでサービスの認証を行います。サービスは、登録時にエージェントに渡されるセキュリティトークンを使ってエージェントを認証します。登録プロセスでは、セキュリティトークンの生成前にOkta管理者の資格情報が必要となります。セキュリティトークンは各エージェントに固有のもので、いつでも取り消すことができます。
- Oktaエージェントからドメインコントローラまたは LDAPサーバー：エージェントは、インストールプロセスで作成された権限が低く読み取り専用の統合アカウントを使用してドメインコントローラの認証を行います。

企業は、ユーザーストアとOktaとの間の定期インポートでプロファイルの不整合が発生することを心配する必要はありません。リアルタイムの同期により、Oktaはログインのたびにプロファイルをシームレスにアップデートします。このため、変更したのが個々のプロファイル情報でも大規模なグループ情報でも、ユーザーについてはOkta全体で常に最新の状態を維持できます。

リアルタイムの同期化を有効にするプロセスは、次のとおりです。

1. 適切なエージェントをダウンロードし、インストールします。
2. OUとグループをインポートします（メンバーの属性を除く）。
3. OUの選択とユーザー名を設定します。注: 定期インポートのプルダウンメニューは［なし］に設定されます。
4. 認証の委任、ジャストインタイム（JIT）のプロビジョニングは、デフォルトで有効になっています。
5. ユーザーは事前のインポートやOktaユーザーへの登録がなくても、すぐにJITでプロビジョニングされます。
6. 認証の委任またはJITが行われるたびに、ユーザープロファイルに加えてグループメンバーもインポートされます。
7. ユーザーはログインのたびに非同期で完全に更新されます。

   管理者は、Active DirectoryでOU、ユーザープロファイル、およびグループ情報を変更でき、ユーザーは完全に更新されます。

ジャストインタイムのユーザープロビジョニング

Oktaのジャストインタイムプロビジョニングによるユーザーのプロビジョニングは、非常にシンプルで迅速です。これによってIT管理者は、Active DirectoryまたはLDAPのユーザーストアの既存ユーザーをOktaの新規ユーザーとして自動作成できます。

IT管理者は、ユーザーをアクティブ化する前に初回インポートを実行しなくて済むため、設定の時間を短縮できます。ユーザーは、ログインページからディレクトリ（ADまたはLDAP）の資格情報でサインインすることにより、すぐにOktaにサインインできます。管理者は、ユーザープロファイル、グループ、グループメンバーすべてを［メンバー］タブで確認できます。

ジャストインタイムプロビジョニングのプロセスは、次のとおりです。

1. Oktaサービスでプロビジョニングされていないユーザーが、mycompany.okta.comにログインしようとします。
2. OktaとOktaエージェントは、Active DirectoryまたはLDAPに対してユーザー資格情報をチェックします。
3. ADまたはLDAPでアクティブなユーザーの場合、Oktaに新規ユーザーが自動で作成されます。新規ユーザーアカウントは、既存のAD資格情報を元に作成されます。
4. ディレクトリのセキュリティグループ属性に応じて、ユーザーは自動プロビジョニングされ、Oktaサービス経由でクラウドおよびウェブアプリケーションにダウンストリーム配信されます。

ジャストインタイムのプロビジョニングにより、IT管理者はOktaサービスと割り当てられたすべてのクラウドアプリケーションにより多くのユーザーを導入でき、ユーザーは既に使っているADまたはLDAP資格情報を使い続けることができます。

使いやすい認証の委任

また、Oktaのディレクトリ統合サポートでは、ユーザーのOktaへの認証をオンプレミスのADまたはLDAPドメインに委任することもできます。つまり、ユーザーのmycompany.okta.comへのログイン試行は、認証時にActive DirectoryまたはLDAPに対してチェックされます。その結果、ユーザーはOktaのユーザー名とディレクトリのパスワードを使ってOktaに簡単にログインできます。

具体的なプロセスは次のとおりです。

1. ユーザーはOktaユーザーのホームページにユーザー名とパスワードを入力します。このログインページはSSLによって保護されており、フィッシング防止にセキュリティ画像が提供されます。多要素認証（追加のセキュリティ質問またはスマートフォンのソフトトークン）を有効にすることもできます。
2. ユーザー名とパスワードは、セットアップ中に事前に確立されたSSL接続によりファイアウォールの背後で実行されているOktaディレクトリエージェントに転送されます。
3. Oktaディレクトリエージェントは、認証のため、これらの資格情報をADまたはLDAPドメインコントローラに渡します。
4. ドメインコントローラはユーザー名とパスワードを検証し、はい/いいえで応答します。
5. はい/いいえの応答は、Oktaディレクトリエージェントによって Oktaサービスに返されます。応答が「はい」の場合、ユーザーは認証され、Oktaマイアプリケーションのユーザーホームページにリダイレクトされます。

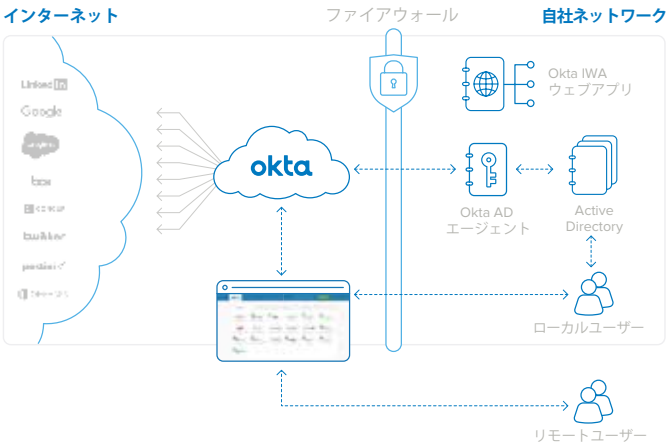

図7: Active Directoryへの認証の委任

デスクトップのシングルサインオン

ADまたはLDAPへの認証委任のユーザーエクスペリエンスはシンプルです。

1. Oktaホームページにログインします。アプリを起動します。
2. Oktaはディレクトリをチェックしてユーザーを認証します。
3. 有効であれば、Oktaはクラウドアプリにシングルサインオンします。

この機能はOktaへのユーザーアクセスを制御するため、アーキテクチャでは複数のOkta ADおよび/またはLDAPエージェントをサポートして冗長性を確保しています。いずれかのOkta ADまたはLDAPエージェントが動作を停止したりネットワーク接続が切断されたりした場合、認証リクエストは自動で、別のOkta ADまたはLDAPエージェントにルーティングされます。

この認証メカニズムでは、ユーザーのパスワードがOktaサービスに保存されることはなく、ディレクトリは資格情報を検証する迅速かつ最終の情報源として管理されます。ユーザー認証に際してはADまたはLDAPが常に使用されるため、ユーザーのステータス変更（パスワード変更や非アクティブ化）はすぐにOktaサービスに反映されます。

Oktaはデスクトップのシングルサインオンをサポートすることで、ローカルユーザーのWindowsドメインでの処理を、Oktaやクラウドアプリケーションへのアクセスの付与にまで拡張できます。OktaのAD統合では、Microsoft社の統合Windows認証を使ってWindowsドメインログインを介して既に認証済みのユーザーをOktaにシームレスに認証します。貴社はOktaのIWAウェブアプリケーションをダウンロードしてインストールし、関連のIP範囲を設定するだけでセットアップを完了できます。

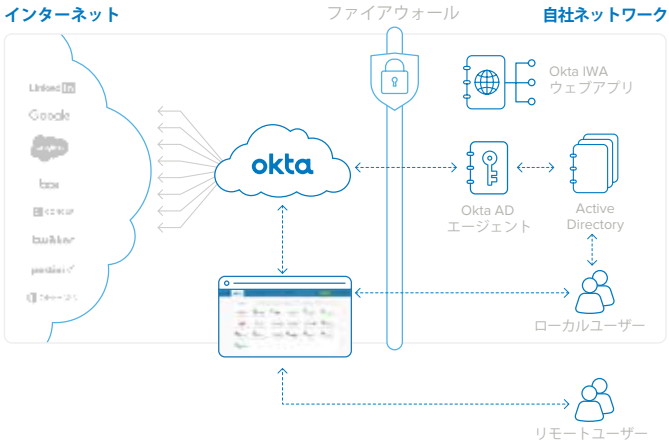

図8: Okta IWAウェブアプリケーションを使ったデスクトップSSO

デスクトップシングルサインオンを介したOktaサービスへのシームレスなログイン（図9を参照）は、次のようなしくみで実現します。

1. ユーザーがhttps://mycompany.okta.comにアクセスします。
2. ユーザーはローカルにインストールしたIWAウェブアプリケーションにリダイレクトされます。
3. IWAウェブアプリケーションは、統合Windows認証（Kerberos）を使ってユーザーを透過的に認証します。
4. ユーザーは、ADユーザーアイデンティティに含まれる暗号署名済みのアサーションとともにOktaログインページに戻されます。
5. Oktaサービスは署名済みのアサーションを検証し、ユーザーを直接Oktaホームページに送ります。

上記すべてのステップは、ユーザーが意識することはありません。ユーザーエクスペリエンスはシンプルです。https://mycompany.okta.com にアクセスしたら、すぐに自身に割り当てられたすべてのアプリケーションのリンクを含むホームページにリダイレクトされます。または、ユーザーは特定のアプリケーションに対応するリンクをクリックするだけで、自動的にそのアプリケーションにサインインできます。システム内でのADへの認証をユーザーが意識することはありません。

最後に、リモートユーザー、つまりオフィス外にいるユーザーは、Okta ユーザーホームページにアクセスするだけで、割り当てられたすべてのクラウドアプリケーションを探してシングルサインオンできます。

セルフサービスによるパスワードリセットのサポート

ユーザーは Okta から Active Directory のパスワードを変更することもできます。ユーザーの AD パスワードの期限が切れるか、リセットされると、ユーザーは次回の Okta へのログイン時にパスワードを変更するよう自動で要求されます。ユーザーは、Okta ホームページの［アカウント］タブで、自ら直接 AD パスワードを変更することもできます。Okta はこれらの資格情報をすべて AD と同期させます。

セキュリティグループによるプロビジョニング

Okta のサービスには、所属するグループに基づいた Okta ユーザーへのアプリケーションの一括プロビジョニングや一括割り当てに使用できるグループ機能があります。Okta では、Active Directory または LDAP のセキュリティグループを Okta のネイティブグループにマッピングし、その結果、AD または LDAP セキュリティグループのメンバーシップに基づいてアプリケーションをユーザーに自動プロビジョニングします。

ユーザーをディレクトリに追加する際、そのユーザーをセキュリティグループに配置することができます。またそのユーザーが追加される Okta との自動同期中に、そのセキュリティグループにマッピングされたアプリケーションのアカウントが自動でプロビジョニングされます。ロール、プロファイル、ユーザー情報などアプリケーション固有のパラメータも、Okta サービスで定義されたルールに基づいて自動的に設定されます。たとえば、「Sales」という AD/LDAP セキュリティグループのすべてのメンバーには Salesforce.com のアカウントがプロビジョニングされ、Salesforce.com へのアクセスが付与されるというルールを、Okta に定義できます。

その結果、ユーザーがディレクトリに追加されると、そのユーザーにクラウドやウェブベースのアプリケーションへのアクセスを付与する必要のあるすべてのタスクが自動的に処理されます。これにより、新しい従業員のプロビジョニング時間を大幅に削減でき、IT 管理者は AD または LDAP をユーザーアクセスの基盤として引き続き使用できます。

ユーザーのセキュリティグループへのメンバーシップが変更されると、Okta ディレクトリエージェントによって変更が検出され、Okta サービスに伝達されます。変更が伝わると、割り当てルールは再計算されます。これらのルールによって、アプリケーションを新規に割り当てたり、既存の割り当てを解除したり、ダウンストリームのアプリケーションのユーザープロパティを更新したりします。

新規および更新されたアプリケーションの割り当ての動作は、まったく同じです。アカウントのプロビジョニング、SSO のセットアップ、ユーザーのマイアプリケーションホームページの更新について、すべてのステップは自動で処理されます。削除も同様に処理されます。ユーザーのアプリへのアクセスが取り消されると、ユーザーはそのアプリケーションにアクセスするシングルサインオンから直ちに排除されます。その後、アプリケーションアカウントが Okta サービスによって非アクティブ化されるか、それが自動ではできない場合は、アカウントが手動で非アクティブ化されたら消去されるべき管理タスクが作成されます。これらのアクションはすべて自動実行、または Okta 管理者の確認後に実行されます。

ワンクリックのプロビジョニング解除

ユーザーの非アクティブ化は通常、Active Directory または LDAP など標準の企業アイデンティティストアからトリガーされます。Okta の一元化されたプロビジョニング解除では、ユーザーストアのユーザーの非アクティブ化がすぐにプロビジョニング解除ワークフローを開始し、Okta やその他のクラウドアプリケーションに対する無許可のアクセスをできる限り効果的に防ぎます。ワークフローは管理者への通知を生成し、特定のユーザーやアプリケーションに関連する、手動のプロビジョニング解除タスクをすべて完了するよう IT 担当者に指示します。さらに、このワークフローは監査証跡としても機能します。Okta 内では、監査証跡全体がレポートと監査の目的でキャプチャされるため、ユーザーやアプリケーションごとのプロビジョニング解除の履歴レポートを簡単に生成できます。

認証済みアプリの シングルサインオン

ほとんどの企業で使用しているオンプレミスのウェブアプリケーションは、Oktaのソリューションに簡単に統合できます。また、多くの企業には、認証にディレクトリの資格情報を使っているウェブアプリケーションもあります。これらのアプリケーションは、統合Windows認証を使用しない代わりに、ユーザーがサインイン時にADまたはLDAP資格情報を入力する必要があります。Oktaを Active Directoryに認証を委任するよう設定すると、これらの社内アプリケーションへのサインインも自動化できます。

ディレクトリ認証の社内ウェブアプリケーションをSSOに対応させるシステム内の手順（図10を参照）は、次のとおりです。

1. OktaをAD/LDAPに認証を委任するよう設定します。
2. 顧客がAD/LDAP認証のオンプレミスアプリを使用しています。
3. ユーザーがAD/LDAP資格情報を使ってOktaにログインします。
4. ユーザーがAD/LDAP資格情報を使い、Web認証（SWA）でアプリ1とアプリ2にアクセスします。
5. アプリ1とアプリ2は、AD/LDAPに対してユーザーを認証します。

Oktaは独自のセキュアWeb認証（SWA）プロトコルを利用して、ユーザーをこれらの社内ウェブアプリケーションに自動ログインさせます。社内ウェブアプリケーションが適切なディレクトリ（Oktaの認証の委任先と同じ）に認証を委任するよう設定された場合、Oktaはログイン時にユーザーのAD/LDAPパスワードを取得し、AD/LDAPに委任しているすべてのアプリケーションでそのパスワードを自動でユーザーに設定します。これにより、ユーザーはリンクをクリックするだけでこれらのアプリケーションにアクセスし、自動ログインできます。

OktaはADパスワードをセキュアに同期します。パスワードが変更されると、変更イベントがOktaへのログイン時にキャプチャされてそのアプリケーションのセキュアなパスワードストアが更新されるため、次回以降も正常にログインできます。

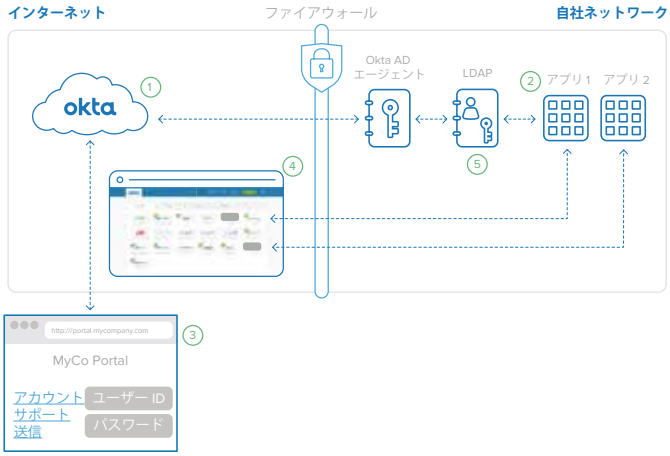

図9: OktaがLDAP認証の社内ウェブアプリケーションをSSOに対応させるしくみ

結論：Oktaを活用して、ディレクトリをクラウドへと拡張する

従来のオンプレミスアプリケーションから最新のクラウドベースサービスに重点を置く企業が増え続けています。最新のクラウドサービスには、機能拡張の点でも全体的なコスト削減の点でも大きなメリットがあります。今ここで問題となるのは、こうした移行が可能かどうかではなく、どれだけ迅速に移行できるかという点です。移行するうえで最大の障壁の1つは、ユーザーと管理者のエクスペリエンスや期待値を満たせる方法でユーザーアイデンティティを管理することです。Active DirectoryまたはLDAPをクラウドサービスにリンクすることで、この問題は解決します。それはOktaのクラウドベースのアイデンティティ管理ソリューションで実現が可能です。Oktaは柔軟で冗長性が高く拡張性に優れたソリューションでクラウドのアイデンティティを管理します。そのサービスは簡単にセットアップが可能で、事実上メンテナンスが不要です。ぜひ、Oktaを導入してディレクトリをすべてのクラウドアプリケーションにも活用してください。Oktaなら、現在利用しているアプリケーションだけでなく、将来必要となるアプリケーションまでもカバーできます。

Okta Active Directoryエージェントの詳細

Okta ADエージェントは簡単かつ透過的に拡張できるよう設計されています。冗長性を確保するため、複数のWindows ServerにOkta ADエージェントをインストールすることでクラスタを作成できます。Oktaサービスは各OktaAD エージェントを登録し、認証とユーザー管理コマンドをこれらのサーバー全体に自動配信します。エージェントで接続の切断やコマンドへの不応答があった場合は、そのエージェントがローテーションから削除され、管理者にメールで通知されます。並行して、Okta ADエージェントは最大1分まで加速度的に試行間隔を延ばしながら、接続を再試行します。

Okta ADエージェントのシステム要件

以下は、Okta ADエージェントをサポートする最小システム要件です。

- Windows Server 2003 R2以降
- 20 MBのメモリ（サービス用）
- Okta ADエージェントインストール時に作成したADサービスアカウント

以下は、推奨システム要件です。

- 256 MBのメモリ（サービス用）
- ドメインユーザー権限を持つAD専用サービスアカウント
- ドメインコントローラとは別のサーバー（共有可能）

Okta IWAウェブアプリケーションの詳細

Okta IWAは軽量なIISウェブアプリケーションで、Oktaサービスでのデスクトップ SSOを可能にします。Okta IWAウェブアプリケーションは、Windows Server 2008にWebサーバーロールでインストールされます。インストーラでは、IISとすべてのWindowsコンポーネントが設定されます。

Okta IWAウェブアプリケーションのシステム要件

以下は、Okta IWAウェブアプリケーションをサポートするのに必要なシステム要件です。

- Webサーバーロールの Windows Server 2008
- 50 MBのメモリ

Okta LDAP エージェントの詳細

Okta LDAP エージェントは簡単かつ透過的に拡張できるよう設計されています。冗長性を確保するため、複数の Windows Server に Okta LDAP エージェントをインストールすることでクラスタを作成できます。Okta サービスは各 Okta LDAP エージェントを登録し、認証とユーザー管理コマンドをこれらのサーバー全体に自動配信します。エージェントで接続の切断やコマンドへの不応答があった場合は、そのエージェントがローテーションから削除され、管理者にメールで通知されます。並行して、Okta LDAP エージェントは最大1分まで加速度的に試行間隔を延ばしながら、接続を再試行します。

Okta LDAP エージェントのシステム要件

以下は、Okta LDAP エージェントをサポートする最小システム要件です。

- Windows Server 2003 R2 以降
- 20 MB のメモリ（サービス用）
- Okta LDAP エージェントインストール時に作成した LDAP サービスアカウント

以下は、推奨システム要件です。

- 256 MB のメモリ（サービス用）
- ドメインユーザー権限を持つ専用サービスアカウント
- ドメインコントローラとは別のサーバー（共有可能）

Okta LDAP エージェントは、以下を含む一般的な LDAP ベンダーを多数サポートしています。

- SunOne LDAP 5.2 以上、6.*、7.*
- Oracle Internet Directory
- OpenLDAP
- OpenDJ

Okta について

Okta は、人とテクノロジーを安全に結びつけるための基盤です。クラウドの力を利用することで、ユーザーがあらゆるデバイスからいつでもアプリケーションにアクセスできるようにすると同時に、強固なセキュリティポリシーも適用します。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で稼働するため、企業は大規模かつ低いコストで迅速にサービスを実装できます。Adobe 社、Allergan 社、Chiquita 社、LinkedIn 社、MGM リゾーツインターナショナル社、Western Union 社をはじめとする 2,500 以上のお客様が、Okta を利用して作業を効率化し、収益を上げ、セキュリティを確保しています。

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ください。