Microsoft パートナー向けのシングル サインオンの実装

Microsoft Azure Active Directory B2B コラボレーションが Azure Active Directory (AD) にもたらす一連の新機能により、B2B パートナー間でセキュリティで保護されたコラボレーションが実現します。これら新機能を使用することで、マイクロソフトの運用チームでは簡単に Microsoft パートナーによるマイクロソフト エクストラネット アプリケーションへのシングル サインオンを実現できます。

膨大な数のパートナー ツール

マイクロソフトには、お客様にサービスを提供するための、信頼できる優れたパートナー コミュニティがあります。その広範なサプライ チェーンとパートナー ネットワークは、大小さまざまな規模のおよそ 31 万の企業から構成されており、顧客価値の提供に重要な役割を果たしています。マイクロソフトが長年にわたり進化するにつれ、Microsoft パートナー向けの B2B システムもまた、どんどんと数が増え、複雑さも増してきました。

一部のパートナーは、OEM、Azure、ボリューム ライセンスなど、各種事業部門にわたってマイクロソフトと連携するために、65 ものさまざまなツール、サイト、およびアプリケーションを使用していると報告しています。この複雑さに輪を掛けているのが、ツールやシステムへの一元化されたアクセスがないゆえに、サインインのために異なる認証プロトコルを使用しなくてはならないことです。ユーザーは、使用するツールへのリンクをブックマークし、ブラウザーのお気に入りに保存する必要があります。パートナーは、セキュリティで保護された各システムのパスワードを使用してサインインするために、自社のユーザー ID を管理する必要があります。種々雑多なユーザー ID の中には、Microsoft アカウント (すなわち、Windows Live アカウント)、企業 ID、Azure AD ID なども含まれており、パートナーはそれらの多数の ID を追跡しなくてはなりません。

ID とアクセス管理

ID とアクセス管理は、パートナー コラボレーションの中核となるものです。マイクロソフトでは、パートナーに重要なアプリケーションおよびデータへのアクセス権を付与する必要がありますが、それらの資産が権限のない人物に渡らないようにする必要もあります。従来のアプローチは、会社間のフェデレーション関係をセットアップすることですが、それには次のような課題があります。

- すべてのパートナー企業が、フェデレーションをセットアップして管理するためのサーバー インフラストラクチャに関する専門知識を持っているわけでも、その余裕があるわけでもありません。
- 各パートナーとのフェデレーション関係を管理する必要がある場合、複雑さは直線的に増大します。
- フェデレーションでは、ユーザー レベルの可視性に制限があり、そのためコンプライアンスと監査が困難です。

困難であるために、多くの企業では内部管理されるパートナー ID のディレクトリを作成するようになり、このプラクティスが独自のセキュリティや管理をもたらすことで懸念が高まっています。

- 内部管理されるディレクトリのアカウントがあまりに多くのアクセスを提供すれば、組織全体がリスクにさらされることになります。
- アカウントは、パートナーの ID システムに接続されていないため、パートナーの従業員が異動したり、退職したりした場合でも無効化されません。
- さらにパートナー用のユーザー名とパスワードのセットも覚えておく必要があり、また、マイクロソフト用の別の ID セットも管理する必要があります (プロビジョニング、プロビジョニング解除、パスワードのリセットなど)。

マイクロソフトの運用チームの役割

マイクロソフトの運用チームの役割は、パートナーが容易にマイクロソフトとビジネスを行えるようにすることです。マイクロソフトの運用チームは、パートナー エクスペリエンスについて責任を負います。"ブックマークされたパートナー ツールを使用するのも、必要なすべてのサインイン情報を管理するのも、ただもう複雑すぎる" というパートナーからのフィードバックを受け、運用チームは、サードパーティのテクノロジを検討し、マイクロソフトでは何が利用できるか考察を開始しました。以下を提供することでパートナー アクセスを効率化できる統合 ID ソリューションの作成に乗り出したのです。

- より簡単なサインイン
- パスワード管理
- Microsoft パートナー ツールへの統合アクセス

完全統合されたツールの作成には数年を要すると思われましたが、運用チームは、Azure AD で使用できるモジュールである B2B コラボレーションを見つけました。

Azure AD B2B コラボレーションの導入

Azure AD は、エンタープライズ グレードのクラウド型 Identity as a Service (IDaaS) サービスで、数千ものクラウド (SaaS) アプリへのシングル サインオンおよびオンプレミスで実行されている Web アプリへのアクセスを可能にします。Azure Active Directory B2B コラボレーションは、マイクロソフトにおける企業間コラボレーションの基盤となるもので、ここで提供する企業間 ID モデルでは、各パートナーが自社の従業員 ID を管理します。

Azure AD B2B コラボレーションは、パートナー企業のポリシーに従って、企業間の可視性、コンプライアンス、および制御を実現しつつ、事業に役立つような方法で、パートナーの既存の IT システムに統合されます。Azure AD B2B コラボレーションは、パートナーが、自己管理 ID を使用して企業アプリケーションおよびデータに選択的にアクセスできるようにして、企業間の関係をサポートします。

Azure AD B2B コラボレーションの特長は次のとおりです。

- **シンプル**。各パートナー ユーザーは、既存の Azure AD アカウントを使用するか、アカウントを簡単に作成して使用します。このアカウントにより、ユーザーは、Azure AD アクセス パネルを通じて単一の企業アプリまたはアプリケーション セットに直接アクセスできるようになります。
- **安全**。管理者は、Azure AD ディレクトリを通じて企業アプリへのアクセスをすべて制御します。コラボレーションが終了した場合、パートナー ユーザーを Azure AD から削除し、アプリへのそのユーザーのアクセス許可を直ちに取り消すことができます。また、パートナー ユーザーがパートナー組織を退職した場合、アクセス許可は自動的に失効します。
- **無料**。B2B コラボレーションは、Azure AD に付属する無料の機能です。企業アプリにアクセスすることが必要なパートナー企業は、Azure AD を所有している必要はありません。Azure AD B2B コラボレーションは、よりシンプルなユーザー サインイン エクスペリエンスを実現して、パートナーがアプリに直ちにアクセスできるようにします。

シングル サインオン アクセス パネルの作成

運用チームはここ数年、マイクロソフトとの連携の複雑さについてパートナーにインタビューを行って、事例を収集しました。ポータル/ツールの増大や、各アプリに個別にサインインする必要性に関する問題に対処するため、運用チームは、シングル サインオン アクセス パネル (SOAP) を作成して、ツール群を 1 回のサインインで一元管理しようと考えました。

概念実証の開発

SOAP 作成のために Azure AD B2B コラボレーションの使用に関する概念実証を開発する際、運用チームはまず、どのアプリケーションを対象にし、どのような種類の ID を使用するのかを決める必要がありました。目標は、パートナーが、新しい SOAP ポータルを使用して、一般的に使用されているツールやサイトに確実にアクセスできるようにすることでした。

すべてのサイトはパートナーが外部アクセスできるように構築されており、サイトの背後にあるデータ (パートナー トランザクション データ、顧客情報、財務データなど) は高度なセキュリティで保護されています。簡素化されたエクスペリエンスのテストおよび検証では、最初のパートナーが重要でした。パートナー アプリケーションを使用するためのアカウントがすでにセットアップされているからです。

運用チームは、SOAP ポータルの最初のユーザーにパートナー企業を選択しました。そのパートナーは、運用チームと緊密に連携して、シングル サインオン ソリューションをテストし、残りのパートナーのオンボーディング前にすべての問題を特定するための支援をすることに同意しました。運用チームは、最初のパートナーとのテストに 10 時間を費やし、その後、10 社のパートナーのグループにテストを拡大しました。

運用チームは、小さく開始することがプラスになると判断しました。なぜなら、ユーザー一人一人の手順一つ一つを学習していく必要があったこと、また、ソリューションは構成であり、厳密には新規の開発ではなかったからです。Azure AD B2B コラボレーション チームはツールを提供し、運用チームはツールを構成して、パートナーへの展開を開始しました。

運用チームは、別のユーザーの ID を作成せずに、Azure サービスと互換性のある既存の ID を使用したいと考えました。ID の優先順位を決定し、どの ID を使用するかに焦点を絞るため、詳しいアンケートが作成されました。望ましい ID として第一に挙げられたのが Azure AD アカウントでした。

パイロットからサービスへの移行

運用チームは、パートナー エクスペリエンス指標を慎重に監視することによって、早期採用コミュニティにおける残りの 85 のパートナーに対する準備を非常にすばやく整え、オンボーディング プロセスを安定させることができました。SOAP の使用が増えるにつれて、運用チームは、B2B コラボレーション製品の向上に役立つ、次のような有益なフィードバックを Azure チームに提供しました。

- ユーザーがアプリを自分で選択できるようにプロセスを改善すること
- 使用に関する分析を向上させること
- 自動化された招待プロセスの向上とカスタマイズを確認すること
- 始めて使用するユーザーのユーザー エクスペリエンスを向上させること
- より長いセッション時間を提供すること
- 全般的なサイトのパフォーマンスを向上させること

100 社を超えるパートナーのオンボーディング後、SOAP はパイロットからサービスに移行しています。運用チームは現在、参加するパートナーを探し求めるのではなく、パートナー コミュニティ内での普及率を測定しています。マイクロソフトは、サービスが利用可能であること、およびサインアップをお勧めしていることをパートナーにお知らせしました。

オンボーディング プロセス

招待されたパートナーが運用チームによって提供されたサイトのリンクにアクセスすると、オンボーディング プロセスが開始されます。そのサイトから、パートナーは、電子メールによるテンプレート アンケートを開始します。このアンケートは、自社の位置付け、およびアクセスする必要があるアプリケーションを特定するのに役立ちます。運用チームの管理者は、各パートナー ユーザーのためのグループとアプリケーションを指定するコンマ区切り値 (CSV) ファイルを作成し、それを Azure 管理ポータルにアップロードします。

ポータルからユーザーに電子メールによる招待状が送信されます。この招待状には、アプリケーションが SOAP ポータルを通じてアクセス可能になったので、すぐにサインインしてくださいと記載されています。フェデレーションされていないアプリケーションの場合、ユーザーが、パスワードベースの SSO を使用してサインインするために、最初にタイルをクリックすると、ブラウザーにアクセス パネル拡張機能が自動的にダウンロードされます。必要なアクセス パネル拡張機能は、Internet Explorer、Chrome、および Firefox ブラウザーで使用可能です。

アクセス パネル拡張機能がインストールされたら、ユーザーは各自のアプリケーションにそれぞれ 1 回サインインすることが求められます。サインイン情報は、キャプチャされて保存され、ユーザーは、ポータルを通じてアプリケーションにアクセスする際に再度入力する必要はありません。

注: マイ アプリ (Android および iOS モバイル デバイス向けの Azure Active Directory モバイル アプリ) では、アクセス パネル拡張機能をインストールすることなく、同じエクスペリエンスが提供されます。

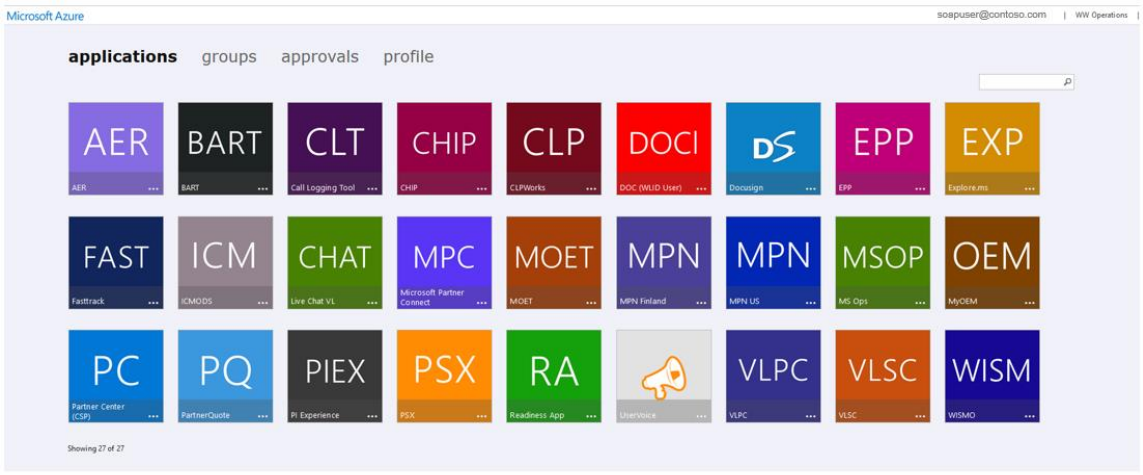

図 1. SOAP ポータル

シングル サインオンのベスト プラクティスの実装

- ID サービスの欠如は、不適切なセキュリティの習慣を招きかねません。最も安全なパスワードは、未承認のユーザーが推測することが難しい、複雑でわかりにくいものです。Azure AD B2B コラボレーションを使用することで、さらにセキュリティで保護された行動を促進するのに役立ちます。
- プロセスの自動化によるパートナーのオンボーディングを簡素化します。運用チームは、パートナーが適切な ID、電子メール アドレス、およびアカウントを選択できるようにするためにアンケートを使用しました。選択肢の絞り込みに役立つ基準を提供することによって、オンボーディングは、より効率的なプロセスになり、運用チームが好む ID の種類を使用するようパートナーを導くようになっています。
- Azure AD を導入していないビジネス パートナーに対しても、B2B コラボレーションでは、マイクロソフトのビジネス パートナーに無料の Azure AD アカウントを提供できる、効率的なサインアップ エクスペリエンスが実現します。

SOAP の利点

- パートナー ツールのダッシュボードによるポータル エクスペリエンスの提供は、ユーザーにとって著しい改善でした。ユーザーは、ブラウザーのお気に入りにリンクを保存および整理する必要はなく、アクセスする必要のある個々のシステムのサインイン情報をすべて個別に保守管理する必要もありません。
- 検査およびテストの後、SOAP ポータルをサービスとしてセットアップすることは、Microsoft IT の関与はほとんどなく、数週間のうちに完了しました。
- エクストラネット アプリへのセキュリティで保護されたアクセスは今もなお、パートナーの ID および情報を保護する Azure プラットフォームのセキュリティにとって最優先事項です。

まとめ

Azure AD チームと連携することで、運用チームは数か月のうちに SOAP ソリューションを作成することができ、最もトランザクションの多い 300 社のパートナーのうち、半数を超えるパートナーのオンボーディングが実現しました。運用チームは、今年度の終わりには導入の目標を達成できる見込みです。将来的により多くのパートナー、より多くのパートナーの種類、および他の業種にサービスを拡大する計画によって、SOAP は、長年のビジネス上の問題を具体的に改善します。

運用チームは、Azure AD チームに重要なフィードバックを提供し、ID とセキュリティに関する複雑なユーザー シナリオを明らかにしてきました。このことから得られた知見は共有されて、今後、他のマイクロソフトのチームがポータルを構築するために役立てられます。

SOAP を使用している Microsoft パートナーからのフィードバックでは、非常に好評をいただいています。Microsoft パートナーは、ソリューションがこれほど早くロールアウトされたのは感激だ、シングル サインオン エクスペリエンスでマイクロソフトとのビジネスは本当にやりやすくなると述べています。

詳細情報

Microsoft IT

microsoft.com/ITShowcase