Macのセキュリティ向上にクラウドIDが不可欠な理由

進化するワークフォースが生み出す新たなチャンス

従業員たちは長年にわたってオフィスに通勤し、コンピュータを開いてユーザ名とパスワードで会社のネットワークにログインし、毎日の仕事をこなしていました。

しかし、物理的なオフィスで決まった時間働くスタイルは近年稀なものになりつつあります。Gallup 社のレポートによると、アメリカの従業員の43%がリモートワークを行っています。[1] そして、この増加するモバイルワークフォースは、会社のネットワークに接続せずにオフィスで働く同僚と同じリソースにアクセスしなければなりません。さらに、オンサイトかリモートかに関わらずすべての従業員が、増え続けるクラウド上のアプリケーションやリソースに安全にアクセスする方法を必要としています。それを実現するためには、エンタープライズのテクノロジーやIT部門の仕事の方法を変えていかなければなりません。

新しいワークスタイルに必要な最新のツールを従業員に提供するための最初のステップは、「従業員選択プログラム」と呼ばれるものです。これは、業務にPCとMacのどちらを使うのかを従業員本人が選べる制度のことです。これにより、多くの従業員がMacを選択するようになったため、IT部門は、ユーザのロケーションに関係なくデバイスとユーザを保護できる合理的なソリューションを必要としています。

このホワイトペーパーでは、Macとそのユーザやデータ、そしてユーザが所属する組織を保護するための、クラウドIDの新たな活用方法についてご紹介します。

今日のMac認証のあり方

Active Directory（AD）とLightweight Directory Access Protocol（LDAP）は、長年にわたってMacの認証に適したテクノロジーでしたが、今日の環境では急速に時代遅れになりつつあります。

ユーザは、会社のリソースにアクセスするためにローカルエリアネットワーク（LAN）上にいるか仮想プライベートネットワーク（VPN）を使用する必要があり、このような古いアプローチでは素晴らしいユーザエクスペリエンスは期待できません。Active Directoryプラグインを使用している場合、ユーザはADにアクセスできる時にしかパスワードを変更することができず、ヘルプデスクがその対応に追われることになります。

この時代遅れのプロセスには次のような問題があります。

1. ITチームの労力

リモートワーカーは自動的に会社のネットワークに接続できません。そのため、パスワードの問題が発生します。Gartner社のレポートによると、ITヘルプデスクの業務の最大40%がパスワードのリセットに関わるものであることが明らかになっています。[2]これらの多くは、パスワードを紛失したリモートワーカーからのリクエストです。

こうしたリクエストが増えれば、その分コストも増大します。Gartner社によると、ヘルプデスクへの1件の電話にかかるコストは17.88ドルです。[2]また、組織がヘルプデスクを外注している場合、単純なパスワードリセットであっても、問い合わせの1件1件に多額のコストがかかる可能性もあります。

こうしたコストはすぐに膨れ上がります。パスワードのリセットに莫大な金額を無駄にしている可能性があるのです。

2. セキュリティ脅威の増大

ADやLDAP、Kerberosなどを主要なユーザ認証手段として使用しながら、多要素認証を導入したり、デバイス信頼などを利用したセキュリティ強化を検討するのは非常に困難です。

iPassが実施した調査によると、企業のデータセキュリティに対する最大の脅威はモバイルワークフォースであることが明らかになっています。実際、世界中のCIO（最高情報責任者）およびIT部門の責任者の57%が、過去1年間にモバイルワーカーのセキュリティが侵害された、あるいはモバイルセキュリティの問題を引き起こした疑いがあると回答しています。[3]

不十分なオンプレミスのツール

Microsoft Active Directoryは、オンプレミスのアイデンティティ&アカウント管理ツールのスタンダードと呼ばれてきました。Active Directoryは、企業のデータやアプリケーションをディレクトリに含まれない社外のユーザから確実に保護します。

これまで多くの組織が認証にまつわる問題の解決策としてActive Directoryを利用してきましたが、残念ながらそれは今日私たちが直面する問題の解決策にはなりません。

これはなぜなのでしょうか？

エンタープライズの世界がWindowsからAppleに移行しつつある今、ITのプロはMacとActive Directoryを統合するためのベストプラクティスに疑問を持ち始めています。

実際、Active Directoryを使ってリモートユーザを安全かつ簡単に認証するというやり方にはいくつかの問題があります。

1. Active Directoryに照らし合わせて認証するにはユーザがドメイン上にいる必要があります。つまりリモートワーカーには適用できないということになります

2. Active Directoryはこれまで主要なIDプロバイダとして多くの組織で使われてきましたが、現在多くの企業が従業員にMacデバイスを支給するようになっています。そのため、リモートワーカーのAppleデバイスに対する管理能力が低下しています。さらに、サードパーティのアドオンが必要となるため、ユーザ管理がより複雑になり、コストも上昇しています

3. IT管理者は、管理対象のコンピュータやユーザに設定を適用するためのポリシーをコマンドやスクリプトを使って導入することができません

Active Directoryのドメインへの紐付けは、20年にわたって認証問題を解決する最適なソリューションでした。しかし、モバイルデバイスが普及した現代では、パスワードや時計が同期されなかったり、DNS（Domain Name System）の記録が外部からアクセスできないこともあり、Active Directoryはもはや実用的とは言えません。

レガシーITのシステムやプロセスは今の時代に合ったものではありません。今日の従業員は、どこにいても安全に仕事ができる環境を望んでいます。

では、MacをActive Directoryに紐付ける必要性をなくしつつ、アカウントのセキュリティを維持するにはどうすればよいのでしょうか？そこで登場するのがクラウドIDです。

クラウドIDの大手プロバイダ

適切なツールがなければ、リモートデバイスのセキュリティは脅かされることになります。時代と共に、アイデンティティとセキュリティに対するアプローチも進化しなければなりません。この進化を実現する道筋を示してくれるのが、クラウドIDプロバイダ（Microsoft、Google、Okta、IBM、OneLoginなど）、SAML（Security Assertion Markup Language）、そしてOAuth（Open Authorization）です。

クラウドIDとは？

クラウドIDを活用することにより、IT部門はユーザやグループ、パスワードに加え、企業アプリケーションやクラウドリソースへのアクセスをリモート管理できるようになります。

> **81%のエンタープライズがマルチクラウド環境を採用し、26%がクラウドのインフラストラクチャに年間600万ドル以上を費やすなか、アイデンティティとセキュリティの維持はかつてないほど困難になってきています。**[4]

Microsoftは、オンプレミスのActive Directoryから距離を置き、クラウドベースのMicrosoft Azure Active Directoryを活用するよう組織に呼びかけています。

Microsoft Azureは、特定のツールやフレームワークを利用することにより、大規模なグローバルネットワーク上でアプリケーションを構築、管理、導入できるクラウドサービスです。実際、このサービスはフォーチュン500社の95%によって利用されています。[4]

しかし、Microsoft Azureは唯一のクラウドIDプロバイダではありません。このようなサービスは他にも多数存在します。では、実際にどのプロバイダに注目すべきなのでしょうか？

クラウドIDとの統合を提供するJamf Connect

Jamf Connectでは、どのクラウドIDプロバイダを選ぶかは問題ではありません。Jamf Connectは、クラウドIDプロバイダが提供するシンプルなユーザのプロビジョニングに多要素認証（MFA）を追加したワークフローを提供します。

これにより、ディレクトリサービスやIDプロバイダが提供していたポリシーやコントロールをローカルユーザに適用することができるようになります。

ユーザはMacを開封し、電源を入れ、単一の認証情報でサインインするだけで、システムによって承認されたすべてのアプリケーションにアクセスできます。

Jamf Connectのメリット

1. セキュアな登録プロセス：最新の認証方法を利用することで、機密性の高いものをデプロイする前にデバイスを使っているのが正しいユーザであることを確認することができます

2. ジャストインタイムのアカウント作成：Okta、Azure、Google Cloud、IBM Cloud、OneLoginのアイデンティティをベースにローカルアカウントを作成します

3. 多要素認証：Okta、Azure、Google Cloud、IBM Cloud、またはOneLoginによってサポートされている多要素認識をログイン画面で使用します

オンプレミスの場合

NoMADをお勧めします。Active Directoryを活用したシームレスなアカウント同期を可能にするNoMADなら、組織のMacの力を最大限に引き出すことができます。

モバイルデバイス管理（MDM）と条件付きアクセス

オンプレミスのActive Directoryから移行する組織が増え、職場のMacデバイスが増えるなか、企業はデータセキュリティを維持しながらAppleが誇る最高のユーザエクスペリエンスを提供することを求められています。

Jamf ConnectとクラウドIDプロバイダの統合は、すべてがモバイル化している今日において、ユーザのパスワードや企業アプリケーションへのアクセスのリモート管理を可能にします。

このプロセスは、自動化されたMDM登録システムを利用することで簡単になります。

1. 自動MDM登録プロセスにユーザが招待されます
2. 登録プロセス開始後、MDMサーバーからJamf Connectがダウンロードされ、インストールされます
3. Jamf Connectのログインウィンドウが表示されます（ユーザ名とパスワードを作成する必要なし）

同じユーザー名とパスワードですべてにアクセスできるため、アカウントのセキュリティを維持しながら素晴らしいユーザエクスペリエンスを作り出すことができます。

Appleに特化したMDMを正しく使うことで、従業員がオフィスにいても、地球の裏側にいても、デバイスを開封するだけで自動化されたセットアップを体験することができます。

Jamfにお任せください

よりセキュアな環境でのAppleの運用を実現し、ITチームへのパスワード関連の問い合わせを減らすことをお考えなら、今すぐ弊社までご連絡ください。Appleデバイスセキュリティの次なるステップを踏み出すお手伝いをさせていただきます。

認証プロセスについてお悩みならJamfにお任せください。

詳細はJamfのスペシャリストまでお気軽にお問い合わせください。また、Jamf Connectの無料トライアルも実施中です。Jamfの誇るクラウドアイデンティティ統合をぜひお試しください。

お問い合わせ　　**トライアルに申し込む**

または、Apple認定販売代理店経由でJamf Connectのトライアルにお申し込みいただくこともできます。

出典：

1: *http://news.gallup.com/reports/199961/7.aspx#aspnetForm*

2: *Gartner Document #G00258742*

3: *https://www.ipass.com/mobile-security-report/*

4: *https://www.rightscale.com/lp/state-of-the-cloud*

jamf

www.jamf.com/ja/

Jamf Connectを使って最新のワークフローに乗り換える方法に興味がある方は、**こちら**をご覧ください。