jamf

ホワイトペーパ

初心者向けのシングルサインオン(SSO)と認証

信頼できるアクセス

成功するために最も重要なのは、企業や組織の、全てのレベルのセキュリティを保護することです。ネットワーク、デバイスからユーザーまで、すべての面で常に保護されている必要があります。それを怠った場合、データ漏洩によって企業は活動を停止することを余儀なくされ、更には顧客の信頼を完全に失い、壊滅的な結果をもたらしかねません。

より多くの従業員がリモートで長時間働いているにも関わらず、オフィスと同様のリソースへのアクセスを必要としています。この状況で、悪意のあるソフトウェア（マルウェア）や脅威から、すべてのデバイスとユーザーを保護するのは、そう簡単にできるものではありません。達成するには、計画と正しいワークフロー、そしてリソースが必要です。

では、企業や組織がユーザーの生産性を妨げることなく脅威と戦うには、どうすればよいでしょうか？シングルサインオン（SSO）およびデバイス／ユーザーの認証セキュリティ対策を活用するこ

このホワイトペーパーでは、以下の点をご説明します。

- SSOと認証を定義
- SSOと認証工程における、クラウドアイデンティティプロバイダの役割を説明
- 最善のセキュリティを提供するための洞察力

シングルサインオン（SSO）とは？

SSOは、1つのログイン認証情報セットで、複数のアプリケーションにアクセスできる方法です。TechTargetによると、SSOはOAuthフレームワークを活用したフェデレーションID管理方式であるため、機密性の高いパスワード情報を公開することなく、すべてのユーザーのアカウント情報をサードパーティのサービスで使用できます。

OAuthはユーザーに代わる仲介役として、特定のアカウント情報の共有を許可するアクセストークンを提供します。ユーザーがサービスプロバイダからアプリケーションにアクセスしようとすると、サービスプロバイダはIDプロバイダに認証要求を送信します。サービスプロバイダは、認証を確認してユーザーのログインを許可、またはユーザーを確認できない場合は拒否します。

SSO構成には、次のような種類があります。

- セキュリティアサーションマークアップランゲージ（SAML）は、セキュリティで保護されたドメイン間でのユーザ認証と承認のやりとりをにします。このプロセスには、ユーザー、ユーザーディレクトリを管理するIDプロバイダ、およびサービスプロバイダ間の通信が含まれます。
- ケルベロスベースのSSOは、ユーザーの資格情報が提供されると、TGT (ticket-granting ticket) を発行します。毎回ユーザー情報を再入力しなくても、TGTによって、アクセスを希望するアプリケーションのサービスチケットが取得されます。

スマートカードSSOはユーザーにカードの使用を、サインイン資格情報と共に要求します。初回入力時以降は、スマートカードに資格情報が保持されるため、ユーザー名やパスワードを再度入力する必要はありません。

SSOでは、ユーザーが記憶しておかなければいけないユーザー名やパスワードの数を削減できるため、それらの情報紛失時に必要とされていたヘルプチケットの節減にも繋がります。また、アプリケーションにログインするプロセスを効率化します。

認証とは？

Next Webによると、認証とはセキュリティで保護された方法でシステムや人物のIDを特定し、確認するプロセスのことです。例えば、ユーザー名とパスワードを利用してデバイスにログインします。認証プロセスでは、アクセスを許可する前にユーザー本人であることを確認します。

Active Directory（AD）とライトウェイト ディレクトリ アクセス プロトコル（LDAP）は、オンプレミスIDとアカウント管理のための認証サービスの例です。ただし、多くのユーザーがクラウドでリソースにアクセスする現代の環境では、これらのサービスは急速に時代遅れになりつつあります。

ADとLDAPには、次のような制限があります。

- リモートユーザーが内部のリソースにアクセスするには、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ます。これではベストな使用感は提供できません。
- ADプラグインを使用している場合、ユーザーはADが到達可能な場合のみパスワードを変更できます。これは、ユーザーがパスワードを忘れた際に混乱を招くだけでなく、ヘルプデスクチケットのコスト増加の原因にもなります。
- ADやLDAPを使いながら、セキュリティプロトコルを増やすための多要素認証を導入するのは非常に困難です。
- Windows PCからMacに移行する組織が増えているため、プライマリIDプロバイダとしてADを使用すると、Mac向けの管理機能は低下します。これにはサードパーティのアドオン使用が必要となるため、ユーザー管理は複雑になり、コストは上昇します。
- IT管理者は、ポリシードキュメント形式のコマンドとスクリプトをデプロイして、管理するコンピューターやユーザーに設定を適用することはできません。

これらの制限により、クラウドアイデンティティプロバイダの必要性が高まっています。

クラウドIDとは？

クラウドIDによりITは、ユーザー、グループ、パスワード、そして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、リモート管理出来るようになります。Microsoft、Google、Okta、IBM、OneLogin、Pingなどのクラウドアイデンティティプロバイダは、SAMLとOAuthを利用して、 リモートとオンサイト で働くすべての従業員に、業務で必要となるクラウドリソースへの安全なアクセスを提供します。

クラウドIDが利用可能となったことで、Microsoftは、企業や組織にオンプレミスのActive Directoryからクラウドベースの Microsoft Azure Active Directoryに移行するように奨励しています。

Microsoft Azureとは、大規模なグローバルネットワーク上で、ビジネスがアプリケーションを構築、管理、デプロイできるクラウドサービスです。Microsoft Azureは、Fortune 500 企業のうち95%で使用されていますが、やはり利用可能な唯一のプロバイダというわけではありません。

クラウドIDの統合

選択可能なクラウド アイデンティティプロバイダは多数存在しているため、企業や組織は、できればすべての、それが無理ならできるだけ多くのプロバイダと統合できるソリューションを利用したいと考えるでしょう。Jamf Connectは、Appleのプロビジョニングワークフロー中、クラウドIDサービスから、ユーザーのシンプルなプロビジョニングと多要素認証 (MFA) の完了を可能にします。

ユーザーはMacを箱から取り出して、電源を入れ、1組のクラウドID資格情報を使ってサインインするだけで、システム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。

メリットは次のようなものがあります。

- アカウント作成：Okta、Microsoft Azure、Google Cloud、IBM Cloud、PingFederateやOneLoginのIDに基づいてローカルのMacアカウントを作成することで、ユーザーはより簡単にログイン出来るようになり、ITはMacの組織化による管理が実現できます。
- 安全な登録：最新の認証を利用して、どのデバイスを使って、誰がどこからアクセスしているかを追跡、把握し、何らかの機密性がある物事をデプロイする前に、デバイス上にいるのが適切なユーザーであることを確認します。
- 共有の管理アカウントの廃止：共有サービスのアカウントを使用せずに、クラウドアイデンティティプロバイダの権限を活用して、複数のIT管理アカウントを作成できます。
- パスワードポリシーの適用：管理者が、IDプロバイダを通じてパスワードポリシーを適用し、すべてユーザーに対して良質なを維持できるようになります。
- パスワード同期：Macのユーザー名とパスワードを維持したままAzure、Okta、PingFederateの資格情報と同期することで、あらゆるタスクに対して、1つのIDを利用できます。

モバイルデバイス管理（MDM）の役割

組織がADから移行し、需要の拡大に伴ってより多くのMacデバイスが導入されるにつれて、組織は理想的なユーザーエクスペリエンスを提供しつつ、企業情報の安全性を確保するためのワークフローを組み立てる必要があります。

Jamf Connectと統合されたクラウドアイデンティティプロバイダを使えば、ITはユーザーパスワードと企業アプリケーションへのアクセスをリモート管理できます。自動MDM登録を使用しましょう。プロセスはシンプルで安全です。

1. ユーザーは、自動MDM登録に招待されます。
2. 登録時に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. ユーザーは、ユーザー名とパスワードを作成する必要はなく、Jamf Connectのログイン画面に直接移動します。

ユーザーは、すべてにおいて同じユーザー名とパスワードを使用できます。アカウントのセキュリティを確立するのと同時に、ユーザーエクスペリエンスは素晴らしいものになります。

より安全なセキュリティー環境を今日から作りましょう

SSO、認証、クラウドアイデンティティプロバイダは、新しい時代のIDとセキュリティ管理です。安全なセキュリティー環境を提供し、ヘルプチケットを削減します。双方にメリットがあります。

Jamf Connectを始めたい、またはJamf Connectを使ったワークフローをまずはお試しになりたい場合は、今すぐお問い合わせください。

今すぐ問い合わせる　トライアル版をリクエスト

または、Jamf Connect試用版を開始するには、Apple認定販売代理店までお問い合わせください。

jamf

www.jamf.com/ja/