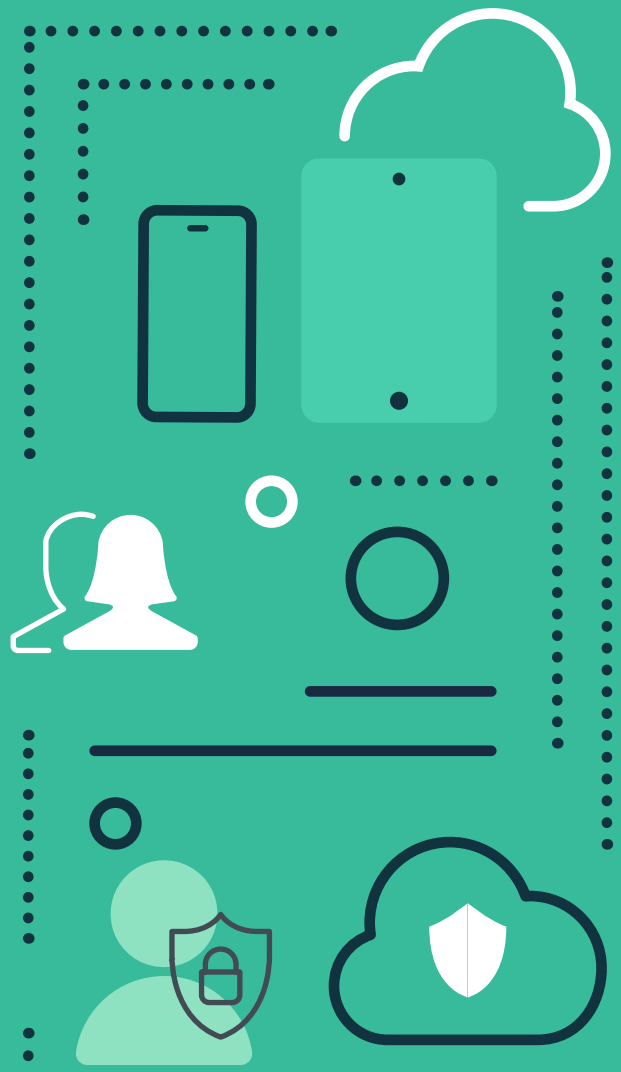

アイデンティティ管理

初心者ガイド

jamf

どのワーカーにも独自のアイデンティティがあります

従来の従業員は、物理的なオフィスに出向いてデスクに置かれたコンピュータで仕事をし、ハードウェアがオフィスを離れることはありませんでした。ひとつの組織にこのような従業員が数多くいることを考えれば、IT部門がデバイスやアクセスの管理に相当の労力を費やしていたことは容易に想像できます。ところが、今日の労働環境は大きく変わってきています。現代の従業員たちは、ノートパソコンからタブレット、そして携帯へとシームレスに移動しながら仕事をし、どこにいても自分の情報やデータにアクセスできなければなりません。

デバイスで作業する時間やアクセスするデータ量の両方において、現代のワーカーのデジタルフットプリントは拡大し、複雑さを極めています。組織がそのような情報を保護するために使う重要な方法のひとつが、特定のファイルやソフトウェア、データにアクセスできる人を制限するゲートです。これは、エンドユーザが必要なものを必要なときに提供し、それ以外のものは提供しないシンプルな手法で、エンドユーザエクスペリエンスの点においても優れています。

ITの世界では当たり前に行われていることですが、テクノロジーの世界が進歩し、従業員のニーズもそれに合わせて変化していく中で、企業は最新かつ将来を見据えた方法でワークフローを確立する必要性に迫られています。そのひとつであるアイデンティティ&アクセス管理は、組織にとって最優先事項とも言えるものです。

このガイドのトピック：

- アイデンティティ管理の基本
- 最新のアイデンティティ&アクセス管理のワークフロー
- クラウドが現代の成功に不可欠な理由
- Jamfでアイデンティティ管理を成功させる方法

アイデンティティ管理の基本

アイデンティティおよびアクセス管理（IAM）は、ユーザのアイデンティティと特定のシステムへのアクセスレベルを確認するための包括的な手法となっています。**そのために必要となるのが、ユーザを認証し、承認するプロセスです。**

認証は一般的に「サインイン」という行為と結びついており、これはユーザの身分を確認するプロセスです。これはほとんどの場合、ユーザ名とパスワードを用いて行われます。

しかし、アイデンティティ管理の分野においては、「認証」とは実際にアクセスを手に入れることを意味するのではなく、単にその人が正当なユーザであることを証明するだけのものです。データやソフトウェア、ファイルへの実際のアクセスには「承認」が必要になります。**承認**は、認証に成功したユーザにどのリソースやソフトウェア、データへのアクセスを許すかということと関係しています。

認証 = 正当なユーザかどうか

承認 = 正当なユーザができること

アイデンティティ管理の基本

この「認証」と「承認」の概念を具体的なものにするために、企業はディレクトリ、つまり従業員のテクノロジーの記録を綴ったカタログのようなものを作成しました。ここには例えば、名前、デバイスの種類、役職、部署、ユーザ名、パスワード、アクセスが必要なソフトウェアやファイルなどが記載されています。これがアイデンティティ管理の基盤として使われていました。これは時に「レガシーIT」と呼ばれるものです。

15年ほど前は、アイデンティティ管理にはある種の一貫性がありました。ユーザのIDや詳細情報をカタログ化するLDAP（Lightweight Directory Access Protocol）、ユーザ認証のためのKerberos、そしてそれらを組み合わせたAD（Active Directory）があり、これらがアイデンティティ管理の中核をなしていました。ところが、この10年ほどでこのプロセスは進化しました。

レガシーITは「事実が集約された」ディレクトリサービスに依存していましたが、セキュリティと導入のニーズの進化に伴い、企業はエンタープライズ戦略の一環としてアイデンティティに対する新しいアプローチを採用する必要に迫られました。ハードウェアとソフトウェアにおけるアイデンティティ管理を統一することで、企業は機能性や高度なワークフロー、そして最終的にはビジネスの変革を実現しました。

アイデンティティ管理の基本

アイデンティティ管理では、ユーザの認証と承認にとどまらず、ユーザが組織のリソースにアクセスする方法も決めることができます。

オフィス以外のさまざまな場所で働く従業員は従来、仮想プライベートネットワーク（VPN）を通じてリソースにアクセスしていました。VPNの場合、アクセスは全体的に許可され、ネットワーク内のすべてのリソースへのアクセスをユーザに提供することになりますが、これは重大なセキュリティリスクとなります。攻撃者がVPN経由でネットワークへのフルアクセスを手にした場合、横方向に移動してそのネットワーク内のあらゆるコンテンツにアクセスすることができるからです。

また、VPNは歴史的に見ても、ユーザやモバイルにとって使いやすいものではありませんでした。現代の職場においては、ユーザがいつでもどこからでもリソースにアクセスできることが求められています。

最新のアイデンティティ&アクセス管理

レガシーITから最新のITへの移行は、テクノロジーそのものにおいてだけではなく、エンドユーザの生産性とビジネスの変革を実現に導いたテクノロジーの活用法にも見られます。

アイデンティティスタック

ディレクトリサービス

従業員の名前や部署などの情報が一元的に記録され、カスタマイズされたデバイスを導入する際に、Jamf Proのような管理ソリューションと統合して利用されます。

レガシー：オンプレミスのActive Directory

最新：クラウドディレクトリ

クラウドSSO

ディレクトリサービスからの情報に基づいて、企業のリソースにアクセスしようとするユーザに認証情報を安全に入力させる仕組みです。

レガシー：クラウドベースのアプリやリソースにアクセスするたびに認証情報を入力

最新：認証情報を何度も入力せずにMicrosoft OutlookやSlackなどのクラウドベースのアプリにアクセス可能

Jamf Connect

ディレクトリサービスとクラウドSSOに追加することで、信頼性を損なうことなく、すべての企業アプリとユーザのデバイス間でアイデンティティを統一させることができます。エンドユーザは単一のクラウドIDを活用して、生産性を維持するために必要なリソースに簡単かつ迅速にアクセスできます。

最新：

- プロビジョニングと認証を合理化し、デバイスを開封した瞬間からリモートワーカーを完全サポート
- ユーザのアイデンティティとデバイス認証情報を自動的に同期
- IT部門にアイデンティティ管理能力をフルに提供
- 次世代VPNによるビジネスリソースやアプリケーションへのセキュアなアクセス

ディレクトリサービス

ディレクトリサービス ＋ クラウドSSO

ディレクトリサービス ＋ クラウドSSO ＋ Jamf Connect

最新のアイデンティティ管理

最新のアイデンティティスタックには主に3つの構成要素があります

1. **AzureやOktaなどに代表されるクラウドアイデンティティプロバイダ（IdP）によって提供されるディレクトリサービスとクラウドベースのシングルサインオン（SSO）**
2. **モバイルデバイス管理（Jamf）**
3. **Jamf Connectを使ったクラウドIdP、ハードウェア、ソフトウェアの統合による、ビジネスアプリケーションへのセキュアなアクセス**

これら3つの構成要素が、リモートワーカーのユーザエクスペリエンスを向上させ、デバイス導入プロセスにおけるセキュリティレベルを全体的に底上げしてくれます。

アイデンティティプロバイダとは？
アイデンティティプロバイダ（IdP）は、デジタルアイデンティティを保存・管理するサービスです。従業員やユーザに必要なリソースへのアクセスを与えるために使われており、セキュリティを確保しながらアクセス管理や権限の追加・削除などを行う方法を提供します。

シングルサインオン（SSO）とは？
SSOは、単一の認証情報を使用して複数のアプリケーションやウェブサイトに安全にログインするための認証プロセスです。

最新のアイデンティティ&アクセス管理

従業員が同じ空間に集まりそこにあるテクノロジーのみを活用する状況においては、デジタルフットプリントは極めて小さく、基本的なアイデンティティ管理で十分に事足りていました。しかしながら、テクノロジーは進化し、業務に使用されるデバイスやアクセスが必要なデータやソフトウェアが大幅に増え、それと共にセキュリティリスクも増大し、ワークフォースは静的なものから動的なものへと変化しました。

テクノロジーやITインフラストラクチャの多くの側面がそうであるように、ワークフォースを取り巻く環境も変革を迫られました。アイデンティティ管理も同様です。Active Directory（AD）とLDAPを利用する場合、ユーザは自分のデバイスをオンプレミスのADに紐付けなければなりません。しかし前述の通り、多くの従業員はもはや常にオフィスにいるわけではありません。これによっていくつかの問題が生じました。

- オンプレミスでADにアクセスしなければパスワードの変更ができないため、ユーザがパスワードを忘れた際などに混乱が生じ、ヘルプデスクへの問い合わせが増加
- Windows用に構築されたADをプライマリIDプロバイダとして使用することでMacの管理能力が低下し、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複雑化しコストが上昇
- リモートユーザが組織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、ユーザエクスペリエンスが著しく低下

これらの理由を含むいくつかの理由から、現在のアイデンティティ&アクセス管理の中核を担っているクラウドIdPが採用されることになりました。

クラウドが現代の成功に不可欠な理由

クラウドアイデンティティ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、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できるようになります。Microsoft、Google、OktaなどのクラウドidPは、リモートとオンサイトで働くすべての従業員に、生産性を維持するために必要なリソースへの安全なアクセスを提供します。

アイデンティティ管理（レガシー）	アイデンティティ管理（最新）
• Active Directory	• Azure
• Open Directory	• Okta
• LDAP	• Google Suite

クラウドIdPと連携することで、組織はオフィスの壁を越え、データやデバイスのセキュリティを確保しながらシームレスなユーザエクスペリエンスを提供することができます。

クラウドが現代の成功に不可欠な理由

Okta、Azure、G Suiteなどのクラウド IdPは、ディレクトリサービスとしての機能を果たします。そこには、従業員の個人情報、所属する部署、役職、そしてもっとも重要な「どのアプリやリソースを必要としているか」が記録されています。クラウドIdPにログインしてそのアイデンティティが認証されると、ユーザは自分にスコープされたクラウドディレクトリ内のすべてのリソースにアクセスできるようになります。**これこそが、認証と承認のプロセスです。**

さらに、クラウドIdPが提供するSSOを活用して組織のモバイルデバイスのセキュリティレベルを上げ、ユーザエクスペリエンスを一気に向上させることもできます。ユーザ自身が認証プロセスを踏んで各プラットフォーム、アプリケーション、サービスにログインする代わりに、SSOなら一度認証されるだけで必要なものすべてに安全にアクセスすることができます。

クラウドが現代の
成功に不可欠な理由

セキュリティをさらに強化したいと願う組織は、多要素認証（MFA）に注目すべきでしょう。MFAを追加することで、ユーザに必要なリソースへの安全なアクセスを提供する前に、脆弱なユーザ名とパスワード以外で本人確認をするための簡単なステップを追加することができます。

これを実現し、クラウドIdPとデバイスを結びつけるのがJamf Connectです。

多要素認証とは？

多要素認証（MFA）とは、リソースにアクセスするために、2つ以上の検証要素の提供をユーザに要求する認証プロセスです。これには、ユーザの携帯電話の暗証番号やFaceID、指紋認証、その他複数のオプションがあります。

すべてをシームレスにつなぐ
JAMF CONNECT

Active DirectoryはWindows用に設計されており、Appleユーザは紐付けしなければなりませんでした。それを変えたのがJamf Connectです。多くの組織がADから移行し、需要の拡大に伴ってより多くのMacデバイスを導入するにつれて、理想的なユーザエクスペリエンスを提供しつつ企業データの安全を確保するためのワークフローを構築する必要性に迫られています。

Jamf ConnectとクラウドIdPの統合により、IT部門は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をリモート管理できるようになります。さらに、自動MDM登録を利用することで、シンプルかつセキュアなプロセスが可能になります。

1. **自動MDM登録プロセスにユーザを招待**
2. **MDMサーバーからJamf Connectがダウンロードされ、インストール完了**
3. **Jamf Connectのログインウィンドウでユーザがクラウドidの認証情報を入力（ユーザ名とパスワードを自分で作成する必要なし）**

すべてをシームレスにつなぐ
JAMF CONNECT

Jamf Connectでは、同じユーザ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。

以下のようなメリットがあります

アカウント作成：Okta、Microsoft Azure、Google Cloudのアイデンティティに基づいてローカルのMacアカウントを作成することで、ユーザにとってはより簡単にログインが、そしてIT部門にとってはより徹底したMac管理が実現できます

安全な登録：最新の認証方法を利用することで、どのデバイスが誰によってどこからアクセスされているかを監視し、機密性の高いものを配布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します

共有の管理アカウントの排除：共有のサービスアカウントを使用せずに、クラウドIdPからの許可を使って複数の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：IdPを通じてパスワードポリシーを強制適用し、すべてのユーザに一貫したセキュリティ体制を提供することができます

パスワードの同期：Macのユーザ名とパスワードをIdPと同期させることで、生産性を維持するために必要なすべてのツールを単一のIDで利用できます

*現時点では、Google Cloudでパスワードの同期を行うことはできません

すべてをシームレスにつなぐ
JAMF CONNECT

Jamf Connectは、最新のアイデンティティ&アクセス管理とゼロトラストネットワークアクセス（ZTNA）ソリューションをオールインワンで提供します。

ZTNAは、ユーザの認証と承認を行い、ユーザがデータやリソースにアクセスするたびにデバイスが信頼できるものであることを確認してくれます。最小権限の強制適用とリアルタイムのデバイスポスチャ検証により、信頼できるデバイスを使う特定の認証されたユーザにのみに各アプリケーションへのアクセスが許可されます。

またZTNAでは、ご希望のクラウドベースのIdPを利用したSSOによるユーザ認証を行うことができます。すでにクラウドベースのIdPを使用している場合には、それと統合させることで、ポリシーの迅速な適用と管理が可能になります。特定のアプリケーションに対して適切な権限を持っているユーザ以外はリソースへのアクセスができないため安心です。

ZTNAについてもっと知りたい方はこちらをご覧ください。

アイデンティティ＆アクセス管理を今すぐ始めましょう

リモートワーカーやモバイルワークフォースの需要が高まり、場所を問わずいつでもリソースにアクセスできることが必然となっています。Jamfは、組織のインフラストラクチャをひとつにまとめ、ユーザとIT部門の双方にシームレスな体験を提供します。

トライアルに申し込む

または、販売代理店までお問い合わせください