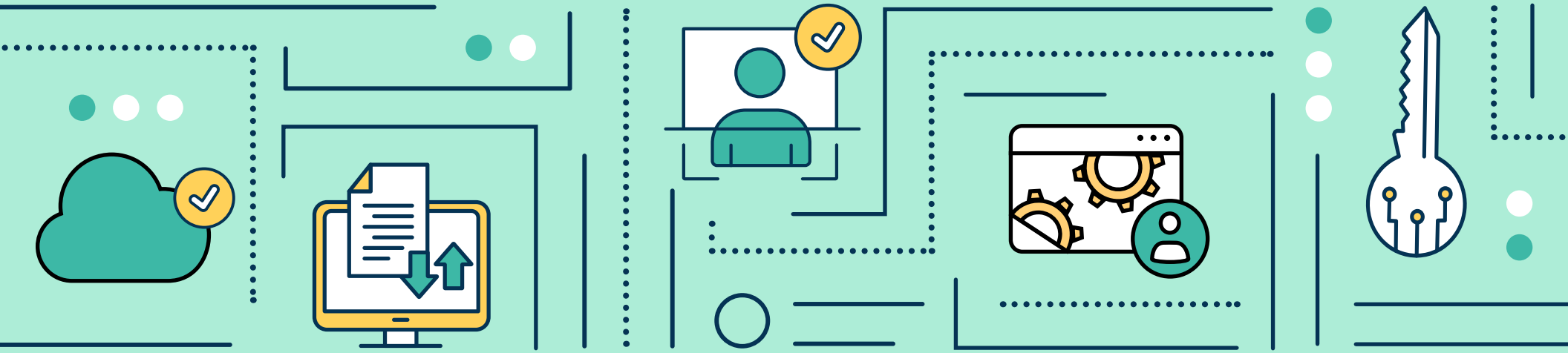
jamf

アイデンティティ管理

初心者ガイド



従業員一人ひとりに、それぞれ固有のID（アイデンティティ）があります。

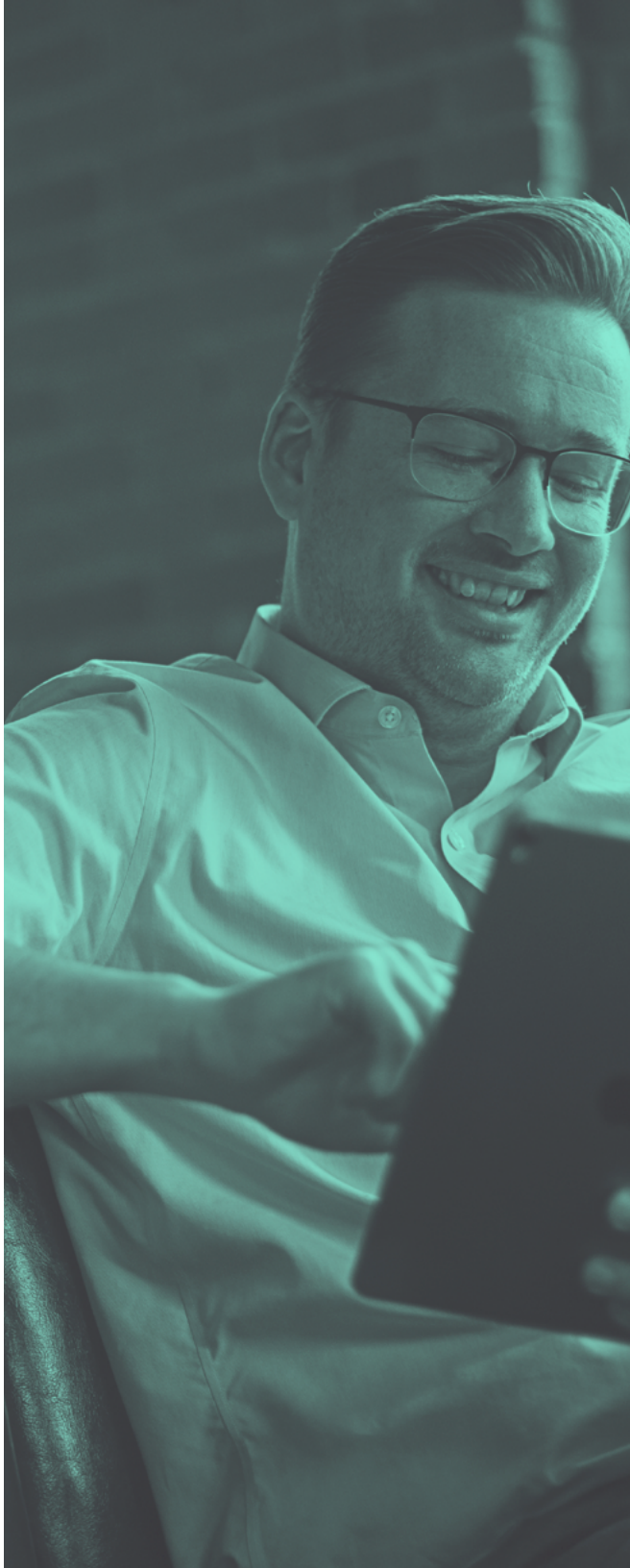
従来、従業員はオフィスに出社し、自分のデスクにはデスクトップPCが設置されており、そのハードウェアが社外に持ち出されることはありませんでした。これを組織全体の従業員数に掛け合わせれば、IT部門が管理しなければならないデバイスとアクセスの全体像が見えてきます。ところが、今日の労働環境は大きく変わってきています。現代の働き手はモバイルを前提とし、1日の中でノートパソコンからタブレット、スマートフォンへとシームレスにデバイスを切り替えながら業務を行い、どこにいても必要な情報やデータへのアクセスを求めています。

従業員のデジタル環境は拡大・複雑化しており、デバイスの利用時間だけでなく、アクセスが求められるデータ量そのものも増加しています。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、必要なものを必要なタイミングで過不足なく提供することで、エンドユーザの体験を向上させるシンプルな手法にもなります。

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eBook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



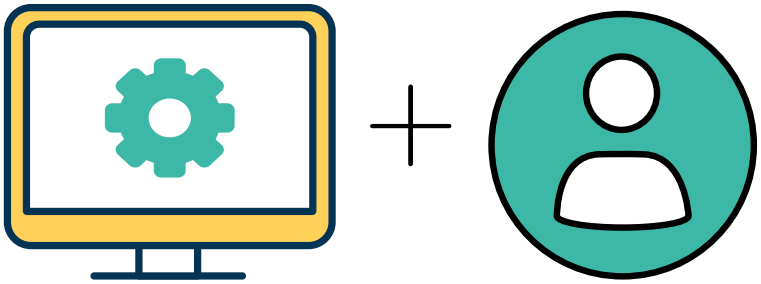
アイデンティティ管理の基本

アイデンティティ管理は、「アイデンティティおよびアクセス管理」（IAM）とも呼ばれ、ユーザのID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。かつては、ユーザ情報の管理に LDAP（Lightweight Directory Access Protocol）、認証には Kerberos を使用し、それらを組み合わせたものが Active Directory（AD） として提供されていました。そして、それこそが当時の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年ほど前にこのプロセスは進化を始め、ここ5年でさらに飛躍しています。

従来型のIT環境では、ディレクトリサービスが「信頼できる唯一の情報源（source of truth）」とされてきました。しかし、セキュリティや導入ニーズの変化に伴い、企業はアイデンティティ管理に対して、新たなアプローチを戦略の一部として取り入れる必要があります。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。

最新のアイデンティティ管理

レガシー IT からモダン 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した。

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Mac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

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. ディレクトリサービスや、AzureやOktaなどのクラウドIDプロバイダー（クラウドIdP）による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 を使えば、クラウドIDプロバイダー（IdP）、ハードウェア、ソフトウェアを統合することができます。

これらのコンポーネントが連携することで、モバイルワーカーのエンドユーザ体験を向上させ、導入環境全体を取り巻くセキュリティレベルの強化にもつながります。

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。多くの企業では、従業員やユーザに必要なリソースへのアクセスを許可するためにこのサービスを利用しており、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。

最新のアイデンティティ管理

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。問題は、テクノロジーが進化したことで、従業員が日々使用するデバイスの数は増え、アクセスするデータやソフトウェアの量も膨大になっていることです。それに伴い、セキュリティリスクは高まり、従業員の働き方も静的なものから動的なものへと変化しています。

テクノロジーやITインフラの多くの側面と同様に、従業員がモバイル化したことで、対応の在り方も大きく変わらざるを得ませんでした。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Active Directory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、これではユーザ体験が損なわれ、不満が一気に高まってしまいます。

これらを含むいくつかの理由から、現在のアイデンティティ管理の核となっているクラウドIDプロバイダ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、IBM、OneLogin、Ping などのクラウドIDプロバイダーは、リモート勤務と出社勤務の両方の従業員に対して、生産性向上に必要なクラウドリソースへの安全なアクセスを提供しています。

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

世界的なパンデミックによってそれまで当たり前だった働き方が崩れ、グローバル経済へのリモート参加を強いられるワーカーが増える中、従業員は場所を問わず仕事のリソースにアクセスしなければならなくなりました。自宅、空港、ホテル、一時的なワークスペース、取引先のオフィスなど、もはや「仕事をする場所」に境界は存在しません。クラウドIDプロバイダと連携することで、組織はオフィスの壁を越えてユーザに必要なものを届け、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すことができます。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を利用することで、シングルサインオン（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ができます。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。

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。

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企業は、多要素認証（MFA）に注目すべきでしょう。MFA（多要素認証）を導入することで、脆弱なユーザ名とパスワードだけに頼らず、ユーザに対して本人確認のためのシンプルな追加ステップを求めることができ、必要なリソースへのアクセスも引き続き確保できます。

これを実現し、クラウドIDプロバイダとデバイスを統合するのが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。企業がActive Directory（AD）からの移行を進め、増え続けるニーズに応えるかたちでMacデバイスの導入を拡大するなか、企業は業務効率を損なうことなく理想的なユーザ体験を提供しながら、企業情報のセキュリティを確保するためのワークフローを整備する必要があります。

Jamf Connect とクラウド ID プロバイダの統合により、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

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。

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、IBM Cloud、PingFederate、OneLogin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なログインが、そしてIT部門にとってはより徹底したMacの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IDプロバイダ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：IDプロバイダを通じてパスワードポリシーを強制適用し、すべて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のユーザー名とパスワードをAzureやOkta、PingFederate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ものを単一の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

アイデンティティ管理はすでに重要な要素となっており、さらに進化を続けています。

リモートワーカーやモバイルワークの需要が高まり、あらゆるタイミングで業務資料へアクセスする必要がある現在、それはもはや欠かせない存在となっています。Jamf Connect は、すべて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。

無料トライアルに申し込む またはApple製品販売代理店までお問い合わせください。