Why not Mac?

vol.7

Macのユーザ管理はどう行うか

“ MacへのログインもIDaaSで行う時代がやって来る ”

Macの企業導入時の問題点と解決策

Macを使う際に必ず行う作業がある。それは、ユーザアカウントとパスワードを使ったMacへのログインだ。ユーザアカウントとは、コンピュータやネットワークなどを許可された人のみが利用できるようにするために登録される利用者の識別情報や資格情報のセットで構成されたものだ。ユーザーアカウントを持つ利用者がコンピュータを使用するには、まず「ログイン」と呼ばれる認証手続きを行い、パスワードの入力で本人確認を行う。ログインするとアカウントに設定された識別情報や権限に基づいてシステムを操作することができ、アプリケーションを使って業務が行えるようになる。

Macのユーザアカウントにはいくつかの種類があり、そのアカウントの種類によってできることも変わってくる。Macを最初にセットアップする時にできるローカルアカウントは「管理者」の権限を持っており、アプリケーションの追加や一部のシステム環境の設定変更が可能である。その他にもMacには「一般」アカウントや「ゲスト」アカウントというものが存在する。

現在多くの企業で採用されているMacのユーザアカウントは大きく二つのパターンに分けられる。一つは管理者権限がそのまま付与されたユーザアカウントを利用しているパターン。もう一つは、IT管理者が最初のMacのセットアップを行い、一般権限のユーザアカウントを設定して、利用しているというパターンだ。管理者権限を持ったユーザアカウントを利用している背景の多くは、Macに関して情報システム部門が関与しておらず、業務上の理由から現場主導でMacがそのまま導入されているため、特にユーザアカウントの権限を意識することなく、そのままセットアップされたものが使われていることが多い。一般権限を付与しているパターンは、情報システム部門のセキュリティポリシーをしっかり適用することから、Macの初期セットアップをIT管理者が行なっているからである。

それぞれのパターンにはメリット・デメリットがあり、Macの企業利用の利便性について大きく影響するところである。Macの企業導入で課題となるのが、このユーザアカウントの管理である。従業員がどんなユーザアカウントを使って、Macにログインしているのか、持っているユーザアカウントの資格情報や権限によって、Macにログイン後にできることが大きく変わってくるからだ。

セキュリティの観点で見れば、会社が許可していないアプリケーションを勝手に追加されることで、予期せぬ情報漏洩や事故につながる可能性が高まる。ユーザの利便性の点で言えば、使いたいアプリケーションをApp Storeやインターネット上からダウンロードしてきて、自由にインストールすることができないため、都度IT管理者に相談する必要が発生したり、場合によっては使いたいアプリケーションが使えないようなことにもなっている。

実際の現場では、アプリケーションの追加を行う必要性が発生すると、IT管理者がMac利用者のところまで行き、管理者権限のユーザアカウントでログインし直し、インストール作業を行なっているようなこともある。IT管理者がネットワーク上のMacに対し、リモートアクセスできるApple Remote Desktopを使ってアプリケーションのインストールをサポートしているような運用管理の例もある。

ただし、このApple Remote Desktopも社内ネットワークの中にあるMacに対してリモートアクセスするので、現代のモバイルが中心のMacの利用環境においては、あまり効果的なツールとはならない。iOSデバイスと同じようにMDM（モバイルデバイス管理）でMacを管理することが今の主流であるが、Macのユーザアカウントの部分までMDMが管理できないため、企業でのMac管理もデバイスやアプリケーション、ネットワークの統制までで、肝心の利用者が誰かを管理する部分が弱いと言える。

また、Windows PCが標準PCとして配付されている企業においては、このユーザアカウントについても、Windows Serverの機能であるActive Directoryによって管理されている。通称ADと呼ばれるこのシステムにより、ユーザアカウントは社内ネットワークの中で管理され、Macへのログインの認証にも使われている場合もある。過去を振り返れば、macOS ServerにもOpen Directoryというサービスがあり、同様にユーザアカウントを管理するシステムがある。日本国内の企業で使われているケースは減ってきているが、Macのユーザアカウントを管理するということは、長年企業のMac管理の課題として挙げられている。

ビジネスの現場では、データはクラウドに保存されており、アプリケーションもWebベースで利用可能になっている。そして、利用者個人のIDについてもクラウドで管理できるようになっており、一つのIDで様々なアプリケーションやサービスが利用できるようになっている。IDaaS（ID as a Service）と呼ばれるサービスが増えている。将来的にはMacのユーザアカウントも、このIDaaSと連携し、Macへのログインも、アプリケーションやサービスへのログインも全て一つのIDとパスワードで実現できるようになることが、管理者視点でも負担を軽減できるし、利用者にとっても、複数のIDを意識することなく、Macを使い業務に集中することができるはずだ。