マネーフォワード担当者に聞く
Jamf ProとIntune連係によるMacとWinの統合管理

マネーフォワードは、個人・法人向けの金融系Webサービスを扱う企業で、全国に拠点を展開しており、海外にも現地法人を構えています。「すべての人の、『お金のプラットフォーム』になる。」をミッションとし、主な事業内容としては個人向けに、複数の口座情報を一括管理し、家計簿を自動作成する、お金の見える化サービス「マネーフォワード ME」、事業者向けには、バックオフィスSaaS「マネーフォワード クラウド」などを開発、提供しています。Jamf ProとIntuneの連係により、MacとWindowsの統合管理を実践している、CIO室コーポレートインフラ部 ITサポートグループリーダーのムガール優人氏にお話を伺いました。

CYODですべての従業員に最適なデバイスを

● 企業規模の成長に伴い、デバイス環境を整備

「コーポレートインフラ部の業務の範囲は、MacとWindowsの全て、MDMとデバイスの調達・管理、エンドユーザへの提供と、幅広くITサポートを務めています」。ムガール氏が入社した際には120人程のスタートアップでしたが、現在は1000人程度の規模になっています。資金や体力が整い、環境整備を進めてきたのが現在の取り組みにつながっています。「2012年の創業時はBYOD※がメインで、個人所有の端末を会社に持ち込んで使用するのが基本でしたが、会社の成長に伴い、エンジニアの負担軽減のためにまず最新型のMacBook Proを導入しました。以降、従業員には最新のマシンを使ってもらう方針を貫いています。Macに関して言えば、型番によるデバイスドライバの違いが少ないため、管理が簡略化できる点も大きなメリットです」

株式会社マネーフォワード CIO室コーポレートインフラ部 ITサポートグループリーダーのムガール優人氏。MacおよびWindowsの調達やエンドユーザへの提供、MDMによる管理、およびITサポートを担当しています。

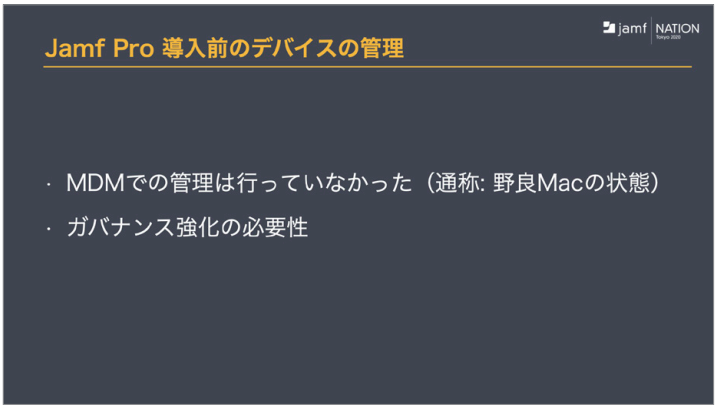
● MacとWindowsは半々ずつの混在環境

「Macはエンジニアやデザイナーが使うというイメージが強いですが、弊社ではビジネス職向けにもCYOD※の形でMacを提供しており、ユーザがスムーズに業務を進められるように、MacBook Air／Pro、iMac Pro、WindowsはThinkPad X1 Carbonといった端末を用意しています。そのほか業務要件に応じたカスタマイズにも対応し、使用状況はMacとWindowsが半々ずつぐらいという状況です。エンジニアとデザイナーに関しては、9割以上がMacを選んでいます」

※CYOD（Choose Your Own Device）：業務に使用してもいい端末を企業側が何種類か用意し、従業員が使いたい機種をチョイスする仕組み。一定の範囲内で私的利用を認める場合が多い。
※BYOD（Bring Your Own Device）：個人が所有する端末を職場に持ち込み、業務に使用すること。

会社が大きくなればMDMを導入することになる

●「DEP端末」の形で端末の購入を



現在は、CYODで、従業員に快適な業務環境を構築しているマネーフォワードですが、かつては社内で「野良Mac」と呼んでいた、MDMで管理されていないMacが多く使用されていたと言います。端末を1台1台、手作業でキッティングして管理することは大きな負担であり、セキュリティガバナンス上も大きな問題となります。キッティングの効率化とガバナンスの確保を目的として、Jamfの導入を検討し始めました。
「手作業によるキッティングが悪手というわけではありません。しかし、いずれ会社が大きくなればMDMを導入することになるはずです。手作業を続けるとしても、先にDEP※の契約だけはしておいたほうが良いでしょう。こちらを先に登録しておくだけで、MDM導入時の手間は大いに省けます。無料で登録できますので、ぜひ利用を検討してください。Macでは後からDEPに登録することができません※。「DEP端末」の形で購入しておくことを強くお勧めします」

※DEP（Device Enrollment Program）：Apple が提供してきた、MDMにデバイスを自動的に登録する仕組み。現在は「Apple Business Manager」および「Apple School Manager」に統合され、「自動デバイス登録」として実装。ゼロタッチキッティングができる形での買い方として推奨される。

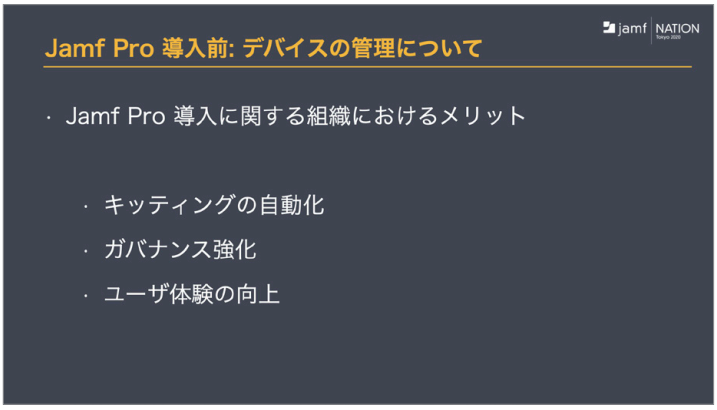
※2021年6月に開催された「WWDC2021」にて、購入後のADE対応予定がアナウンスされました。

● Jamf導入はトップが早急に理解

ガバナンス強化が喫緊の課題としてあったところ、トップがMDM導入を早急に理解してくれたことが幸運であったといいます。
「野良Macが非常に多く、DEP端末でなかったため、全社員にアナウンスしてMDMプロファイルを入れてもらう必要がありました。そこでトップがJamf導入を早急に理解してくれたのは幸運でした。導入当時は、日本でもJamfを使っているユーザは多くありませんでしたので、知見もそれほど共有されておらず、トラブルの解決も困難でしたが、現在は日本のEnterprise MacもJamfも利用者が増えて知見を得られるコミュニティが充実しており、大変助かっています」

Jamfでキッティングは確実に効率化

● Appleからのパッチ配布は解決の2日後



マネーフォワードでは、ゼロタッチデプロイメントを最終目標に、まずキッティングをゼロタッチで実現できるように取り組んでおり、新規ツールの全社配布、新たなゼロデイ脆弱性対策のためのバージョン確認などにJamfを活用していると言います。
「重大な脆弱性が発覚した際に、Appleからのパッチ配布を待っているのでは対応が遅くなり、被害の発生や拡大が懸念されます。そのような場合に、設定変更などで対策できるケースでは、Jamfからスクリプトを一斉配布することで対処できることがあり

ます。実際にこの方法で脆弱性を回避できたことがあり、チームの大きな実績の一つとなっています。ちなみにAppleからのパッチ配布は解決の2日後でした」

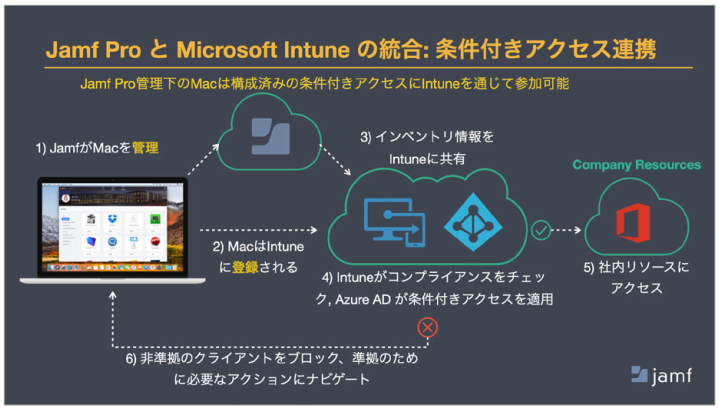
● 操作がわかりやすく手軽なJamf

ムガール氏はJamfを導入すればキッティングは確実に効率化できるといいます。
「私自身、手作業によるキッティングを担当していましたので、これは間違いないと断言できます。社内の端末管理でできることの幅も格段に広がりますし、さまざまなアプリとのインテグレーションができるのも大きな利点です。操作がわかりやすく、手軽である点も魅力です。GUI上で操作できるツールなので、いわゆるコマンドラインによる操作等に抵抗がある方にもおすすめです。
また、Jamfは共有されている情報の量が圧倒的に違います。Jamfを使って何かしたいと考えた際、多くのケースでそのノウハウやヒントをGitHubやSlackのワークスペースなどで見つけることができます。この点において、Jamfは他のMDMと比べて非常に優位に立っているのではないでしょうか」

ツールを組み合わせて活用し網羅性のある管理を

● Windowsとの共存をどう実現するか

「IdPとしてはAzure AD、Windowsの管理にはIntuneを使用しています。Azure ADでMacも管理する方法はありますが、弊社ではすでにJamf Proを導入していたので、Azure ADと統合していく方向としました。
統合の実例としては条件付きアクセスがあります。まず、Jamfから抽出したMac端末の情報をAzure ADのIntuneに送ります。その情報をAzure ADが評価し、例えば特定のアプリや特定の機密情報に、条件が合致していなければアクセスできないようにできます。そのMacがJamfで管理されていないMac（前述のいわゆる「野良Mac」）であればアクセスを拒否するという仕組みを実現できます。また、そのMacのバージョンが極端に古くないかといった条件を組み合わせて、特定のアプリケーションに対するAzure ADのアクセス権限を動的に指定することもできます」



● 安全性の担保されていない PC をシャットアウト

まだVPNを使用している企業も多いと思います。自宅で作業することが増えていますが、個人の安全性の担保されていないデバイスから社内のセキュアな閉域網にVPNアクセスされることは、管理者としては防ぎたいところです。
条件付きアクセスの仕組みを用いれば、会社から配布されたもので、かつ一定のガバナンスが担保されているデバイスからでなければアクセスできないような仕組みも構築できます。これは元々Azure AD／Intuneが持っている機能で、それらとJamf Proを連係することにより、実現できる仕組みです。

● 1つのツールで管理しなくてもいい

1つのツールで、MacもWindowsもすべてを管理したいという考えもありますが、マネーフォワードではOSに最適な

ツールをそれぞれ活用することを決めました。
「もともとMacはJamfで管理していたので、その部分の変更は検討しませんでした。1つの画面ですべてを管理するのも一つの考えですが、JamfはOpenAPIですので、例えばSlackに情報を渡し、Slack上で端末ステータスを確認することもできます。一方で、APIから参照不能な情報もありますので、追加で必要な情報があればその時はJamfにアクセスすればよい、という考えです。Azure ADで統合管理していくのが一番の理想ではありますが、Slackなどさまざまなツールを組み合わせて活用することで、効果的な管理ができるのではないでしょうか」

OpenAPIという強みを活かし統合・拡張を進める

● さらなるキッティングの効率化とユーザ体験の向上を

「今後はJamfのOpenAPIという強みを活かし、他のプラットフォーム、例えばSlackでパッチ管理の最新情報などを通知して可視化するような取り組みを強化する予定です。また、Jamfの機能を追加・拡張できるMarketPlaceを使って、例えばパッチ自動アップデートツールといったものを追加して、Jamfの拡張を進めていこうと考えています。AppleがEnterprise機能拡充をアナウンスしていますので、次期OSも含め、注視し対応していく予定です」
マネーフォワードでは、さらにJamf Connectの検証も進めています。
「Jamf Connectを導入することで、Mac管理とAzure ADの真の統合ができると考えています。完了すればユーザは一つのIDとパスワードですべてのアクセスが可能となります。結果として、さらなるキッティングの効率化と、ユーザ体験の向上が実現できると大いに期待しています」

Webinar Information

本記事は、2020年11月17日に「BrightTALK」（https://www.brighttalk.com/）で開催されたウェビナーの内容を編集したものです。フルバージョンの動画は右のQRコードからBrightTALKのサイトで視聴いただけます。

Jamf Japan合同会社
東京都港区虎ノ門4-3-20神谷町MTビル16階
Tel. 03-4578-2000
本内容は2021年8月現在のものです。