

株式会社サイバーエージェント

約7,000台のMacをJamf Proで管理！ 「API活用による端末の可視化」が活用の鍵



1998年の創業以来、時代のニーズに合わせて事業領域を次々と拡大させてきた株式会社サイバーエージェントでは、社内に存在する約7,000台にもおよぶMacを管理するために、新たなMDMとして「Jamf Pro」を採用しました。選定の一番の決め手となったのは「Jamf Pro API」によってMacの稼働状況を可視化するワークフローを実現できること。従業員の自主性を重んじるサイバーエージェントならではの、利便性と安全性を見事に両立したMac管理に迫ります。

Macのセキュリティを徹底するために -Jamf Proが唯一の選択肢だった-

●旧MDMで抱えていた2つの課題

「21世紀を代表する会社を創る」をビジョンに掲げ、新しい未来のテレビ「ABEMA」をはじめとするメディア事業やインターネット広告事業、ゲーム事業を展開する株式会社サイバーエージェント（以下、サイバーエージェント）では、入社時に従業員自ら、業務端末をMacまたはWindows PCから選ぶことができます。このうちMacを選択する従業員の割合は年々増加傾向にあり、現在は約半数が利用。子会社や関連会社を含めると、その数は実に7,000台近くになります。

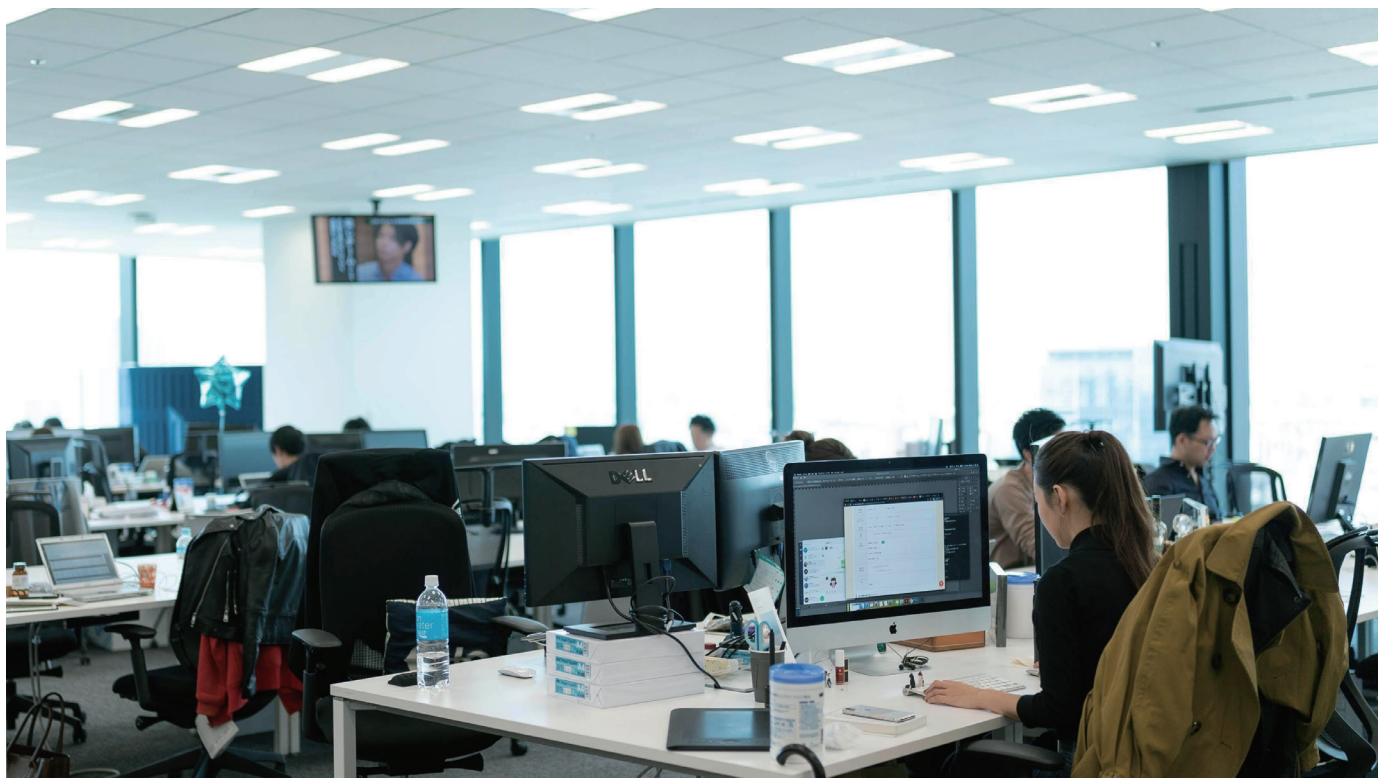
こうした大量のMacを一元管理するため、「グループIT推進本部（サイバーエージェントグループ全体のシステム・インフラ・セキュリティの課題解決や事業サポートを行う部署）」で



東京都渋谷区に本社を構えるサイバーエージェントは、インターネット領域で時代の変化に合わせたさまざまな事業を展開しています。

<https://www.cyberagent.co.jp>

は、Appleデバイス専用のMDMである「Jamf Pro」を採用しています。約200名が所属するグループIT推進本部の中でクライアントPCの責任者を務める西永裕樹氏によると、以前は別のMDMを利用していましたが、Macのセキュリティを徹底



サイバーエージェントでは入社時に業端端末としてMacを選択可能。現在は7,000台近いMacが稼働しています。

できなかったことからJamf Proへの移行を決断したと言います。

「以前のMDMは、リモートワイプやリモートロックは行えるものの、Macを安全に管理するための機能が十分ではなかったのです。特に、MacのセキュリティポリシーやOSのアップグレードなどをコントロールできないことを問題に感じていました」

中でも大きな課題だったのが、macOSのバージョンアップに伴う仕様変更への対応です。2018年にリリースされたmacOS Mojave以降、セキュリティソフトを利用するためにはフルディスクアクセスの権限を設定しなければならず、これを行わないとセキュリティスキャンなどが正常に行えませんでした。

「従業員がmacOSをアップグレードすると、セキュリティソフトがMac内のフォルダにアクセスできるようにフルディスクアクセスの権限設定を求められます。この際に従業員側で管理者パスワードを入力して権限を許可する必要があるのですが、従業員依存になっていたことが問題でした。もし、この設定を行わないと脆弱な状態でMacを利用することになるため、セキュリティ的には大きなリスクを抱えます」

また、macOSのバージョンアップを制限できないことも課題でした。なぜなら、macOSのメジャーアップデートが行われたときは、時としてサードパーティ製ソフトウェアの対応に時間がかかる場合があるからです。

「たとえば、2020年にリリースされたmacOS Big Surのときは、当時利用していたセキュリティソフトが新OSに対応するまで半年ほどかかりました。もし従業員がその間にOSを

アップグレードしてしまうとセキュリティソフトが正常に動作しないため、OSのアップグレードを制限する必要があります。もちろん『OSをアップグレードしないでください』と通達はするのですが、全員にそれを徹底させるのが難しかったのです」

●Jamf Pro導入によるさまざまなメリット

こうした課題はJamf Proを導入したことで一気に解決しました。Jamf Proを利用すれば構成プロファイルを配付してセキュリティソフトのフルディスクアクセスを遠隔から許可することが可能。また、OSのアップグレードを禁止したり、ディスク暗号化機能である「FileVault」をオンにしたりなど、管理者にてさまざまなMacの設定および制御を行えます。

また、Jamf Proは最新のmacOSへの「同日サポート」を実現している点も重要なポイントでした。

「今秋にmacOS Sonomaがリリースされましたが、従業員のアップグレードを制御するために一定期間表示させないように設定していました。また、最近のmacOSはベータ版をインストールできるようになっているので、これもセキュリティ的な観点から表示しないようにしています。最新OSがリリースされた際にこのような対応がすばやく可能なのは、Jamf Proが最新OSに同日に対応してくれるからであり、そうでないとMDMを入れる意味が薄れてしまいます」

西永氏によると、旧MDMから移行する際はJamf Pro以外のMDMも一通りチェックしたそうですが、自分たちがしたいことを叶えるにはJamf Proしか選択肢がなかったと言います。

「iPhoneやiPad向けのMDMは、製品によってできることに大きな違いはないかもしれませんが、Mac向けのMDMとしては、Jamf Proほど多機能な製品はほかにはないと思います」

このように語る理由として、西永氏は「Macの柔軟な管理ができること」「日本語によるサポートが存在すること」に加えてもう1つ、「APIが提供されていること」を挙げます。企業においてMDMを導入するのは、デバイスのキッティングを効率化したり、デバイスの設定や制限を実行したり、さまざまなインベントリ情報を参照したり、デバイス紛失時にリモート制御したりすることが一般的な目的とされます。もちろん、サイバーエージェントのグループIT推進本部でもJamf Proでこうしたことが行える点は評価していますが、それ以上に「Jamf Pro APIを用いて、独自のワークフローを実現すること」が重要であり、それがJamf Pro採用の一番の決め手になったのです。

Jamf Pro APIの活用で端末状況を可視化 -約7,000台のMacを安全に管理する-

●独自のワークフローでMac運用の効率化を実現

その独自のワークフローとは、Macだけでも7,000台に迫るグループ全体のクライアントPCの稼働状態を効率的にチェックするためのもの。具体的には、「AWS Lambda」でJamf Pro APIを叩いてMacの端末情報を取得し、そのデータをCSV形式で「Amazon S3」に保存、そしてデータクラウドの「Snowflake」へ取り込んだあと、Snowflakeへ接続したBIツール「Tableau」によって可視化しています。そして「セキュリティソフトが動いていない」「ディスク暗号化がかかっていない」「本人以外のアカウントでログインしている」などの端末を一覧で確認し、従業員にこまめに連絡を取って対応を促し、端末のセキュリティを会社全体でしっかりと担保できるようにしているのです。

「こうしたワークフローによる可視化を効率的に実現するためには、APIを用いて端末情報を取得する必要があります。以前のMDMではAPIが提供されていなかったため、CSVで都度エクスポートしなければならず、とても手間がかかっていました。Jamf Proを導入したのは、Macを細かに管理するためというよりは、当社のセキュリティーポリシーに準じて日々理想的な状態でMacを運用できているかをチェックするためなのです」

Jamf Proでは、Macのハードウェアやソフトウェアの情報、セキュリティ設定等のあらゆる情報を自動収集できますが、さらに「拡張属性」と呼ばれる機能を使うことでより細かなMacの情報を収集できます。グループIT推進本部では、セキュリティーソフトのオン/オフやユーザのログインID(独自のアカウ



株式会社サイバーエージェント
西永裕樹氏

ントを作ってログインしているユーザがいるとパスワードが単純になってしまうという問題があるため)を拡張属性として取得しています。

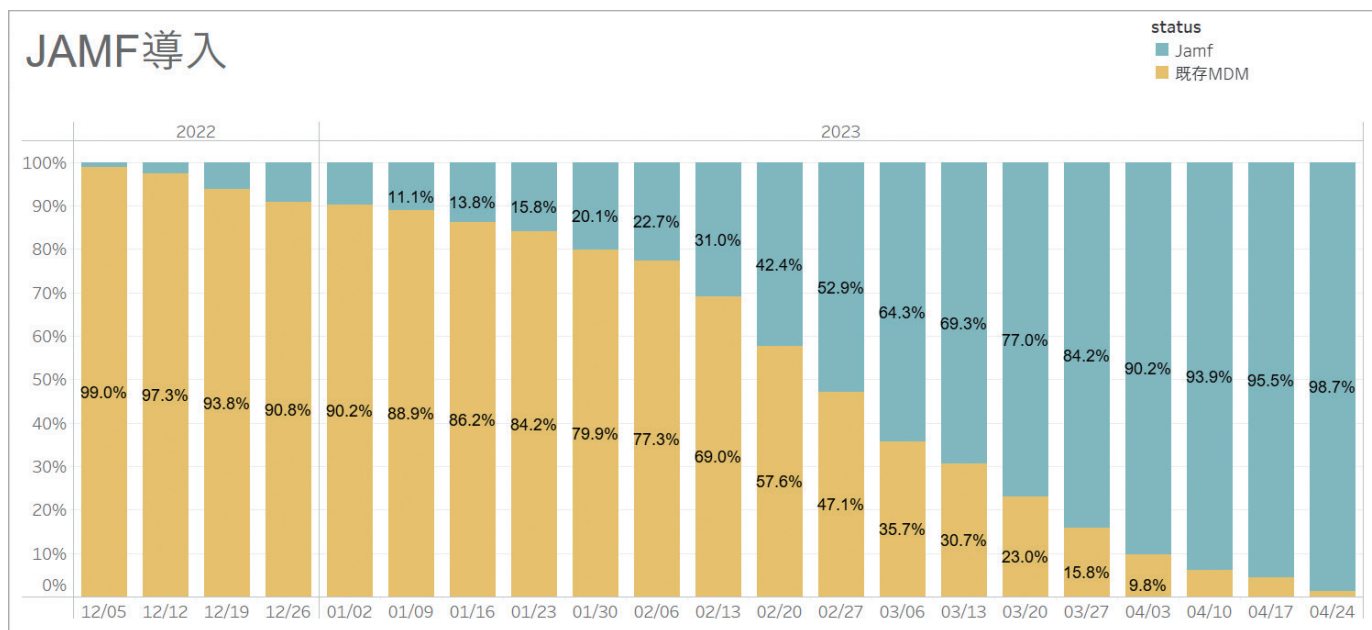
「Jamf Proの導入効果を一番感じたのは、やはり最新OSのリリース時でしょうか。これまでは我々の確認が完了する前にアップグレードしてしまう従業員がいたのですが、Jamf Pro導入後にリリースされたmacOS 14 Sonomaではアップグレードを制御することができたため、ユーザーを含めて対応工数を大きく圧縮することができました」

●大規模展開をスムーズに行えた理由

こうしたAPIの活用は日々の運用だけでなく、旧MDMからJamf Proへ移行する際にも役立ちました。グループIT推進本部でJamf Proの検証を開始したのは2022年9月。そして2022年12月頃からグループIT推進本部ならびに一部の新しい部署へパイロット導入を行い、翌年2023年1月～2月頃から事業部ごとに数段階に分けて全社展開を開始。そして同年4月末にはほぼすべての移行を完了しています。

MDMを移行するにあたり、従業員にはJamf Proへ登録するためのMDMプロファイルや証明書のインストールに加え、同時にセキュリティソフトの入れ替え作業を行ってもらったそうですが、グループIT推進本部ではできる限り従業員に負担をかけないように工夫したと言います。MDMの登録ポータルや作業手順書を用意したほか、自作スクリプトやAWS Lambdaを使ってインストール作業を自動化。さらに、Jamf Proの「スマートグループ」を用いて進捗フェーズごとにMacをグルーピングし、かつJamf ProのAPIを用いて端末情報を取得することでグループ全体のMDM移行状態をリアルタイムに可視化してチェックしたのです。

「グループ全体のインストール状況を一目で確認しながら、事業部別に分けてレポートを担当者と共有しました。これに



よって、なかなか移行が進まない従業員に催促してもらうことができたため、移行作業はとて進めやすかったです。APIとスマートグループの機能がなければここまでスムーズに実現できなかったと思いますので、それだけでもJamf Proを選んだ価値があったと思います」

驚くことに、こうした一連の移行作業 (Jamf Proの検証から導入、展開、管理までの設計や準備、そしてそれに伴う基本的な実作業) のほぼすべては西永氏だけで行ったといいます。

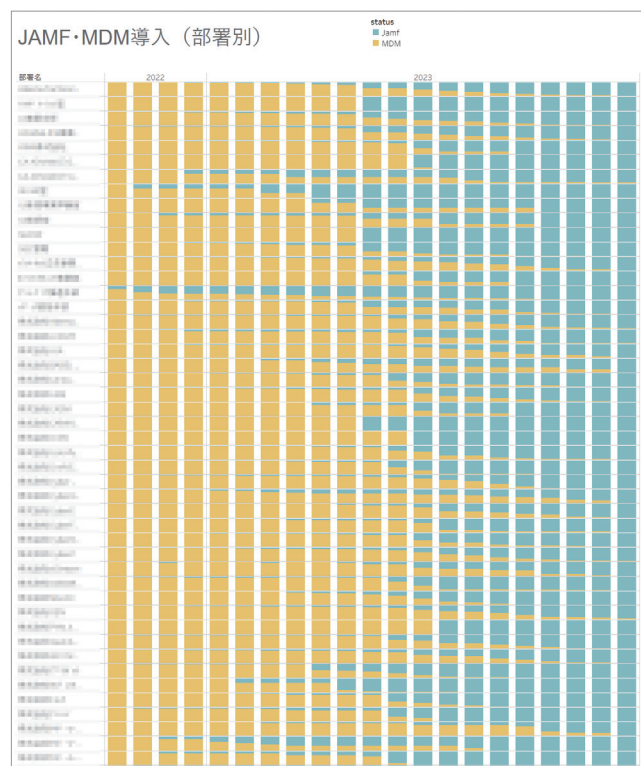
「端末のキッティングや従業員への直接の連絡、また従業員からの問い合わせ対応はそれぞれの担当者に行ってもらいましたが、それ以外は基本的に私ひとりで担当しました。7,000台というと大変な規模に思われるかもしれませんが、Jamf Proであれば同じような導入・展開は一人でも十分に可能です」

なお、グループIT推進本部ではクライアントPCの管理台帳をKintoneで作成していますが、ここから廃棄・レンタル返却されたMacの情報を取得して、Jamf Proの管理下から自動的に削除する自作スクリプトを活用しているとのこと。さらに今後は従業員がMacの箱を開封してすぐにJamf Proの管理下のもと使い始めることのできるゼロタッチ導入や、SCEPプロトコルを使用して端末への証明書の配付を検討するなど、さらなるJamf Proの活用を図っていきたいといいます。

従業員の利便性を損なわない管理 -利便性と安全性の見事なバランス-

●「従業員ファースト」が基本

このように7,000台にも及ぶ大量のMacのMDMをJamf Proへとスムーズに移行し、Macのセキュリティを徹底させ



Jamf Proへの切り替え時にはグループ全体そして部署ごとのインストール状況を可視化することで進捗状況を管理し、スムーズな移行につなげました。

ることに成功したグループIT推進本部。年々高度化するサイバー攻撃のリスクや、新型コロナウイルス感染症の影響によって広がったリモートワークをはじめとする新しい働き方に対応するためにセキュリティ強化が求められたことも、Jamf Proの導入背景にあったと西永氏は振り返ります。

しかし、ここで特筆すべきなのは、サイバーエージェントのグループIT推進本部ではあくまで「従業員ファースト」の考え方を基本にしていることです。業務端末としてMacを選択できること、またアプリを自由にインストールできるように業務端

末の管理者権限を従業員に与えていることがその表れと言えるでしょう。また、たとえ高機能なJamf Proを導入したとしても、同社では厳しくMacの利用を制限をしているわけではありません。

「Jamf Proを使って制限しているのは、セキュリティソフトの権限設定、OSのアップデート禁止、FileVaultの強制、拡張属性を用いたログインIDの取得、そして怪しい振る舞いを検知するセキュリティソフトのインストールの徹底くらいでしょうか。グループIT推進本部はグループ全体の情報システム部門としての役割を担いますが、子会社や関連会社とうまく連携を図りながら『事業のスピードを止めない』ことを重要なミッションとしています」

Windows PCのみを支給したり、システムの設定を行えないように管理者権限を剥奪したりする企業も多くありますが、

そうした運用では管理者がセキュリティを管理しやすい反面、従業員への締め付けが厳しくなり、業務の生産性や効率化に大きな影響を及ぼすことがあります。

サイバーエージェントでは従業員に自由度高く、希望するデバイスを使ってもらえることを前提としたうえで、必要十分なセキュリティを担保し、かつ独自のワークフローによる可視化によって管理を効率化するためにJamf Proを活用しているのです。これは「従業員の能力を活かすこと」を事業拡大の大きな原動力として、自主性と責任感を持ったイノベーションを推進するサイバーエージェントならではのアプローチであり、同社のグループIT推進本部のJamf Pro導入は「利便性と安全性を見事に両立したセキュリティ対策のベストプラクティス」の好例として、同様の課題に悩む多くの企業にとって非常に参考になるでしょう。

