ソフトバンクロボティクス株式会社

Jamf ProとJamf Connect ZTNAで 安全かつ効率的にiPhoneのBYODを実現

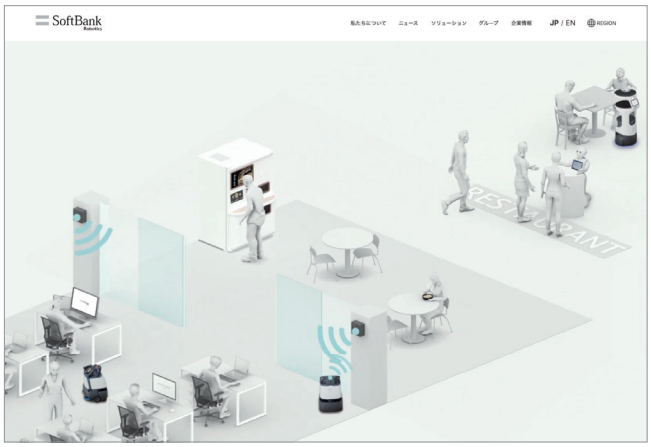
ロボットの開発・販売・メンテナンスサービスを提供するソフトバンクロボティクス株式会社では、Jamf Proを利用してMacやiPhoneのゼロタッチ導入を行い、効率的かつ安全なデバイス管理を実現しています。また、Jamf ProとJamf Connect ZTNAを組み合わせて、海外の従業員向けにiPhoneのBYODも実施しています。ゼロトラストセキュリティを前提としたグローバルレベルのIT統制に、"Jamfが欠かせなかった理由"を探ります。

"ゼロトラスト"の構築への第一歩 -Jamf Pro導入の理由と効果-

●グローバル志向のAppleデバイス管理

世界をリードする"ロボットインテグレーター"として知られるソフトバンクロボティクスでは、Jamf製品を用いて、業務端末として利用するAppleデバイスの管理運用を行っています。Jamf製品を初めて導入したのは、2021年9月。「Jamf Pro」を採用してMacのゼロタッチ導入を行い、その後2021年11月にはiPhoneのゼロタッチ導入、2022年1月には海外拠点へのMac展開、そして2023年4月には「Jamf Connect ZTNA（導入当時の製品名はJamf Private Access）」を採用し、2023年7月から海外の従業員向けにiPhoneのBYOD（Bring Your Own Device）を実現しています。

こうした一連の取り組みを行ったのは、新型コロナウイル



ソフトバンクロボティクスは、2014年にいち早く人型ロボット「Pepper」を発表し、2018年には清掃ロボット、2021年には配膳・運搬ロボット、そして2022年には物流自動化ソリューションの展開を開始しました。多様な製品の取り扱いを通じて得た知見や稼働データを活かし、ロボットを効果的に導入するためのソリューションを提供することで、ロボットインテグレーター（RI）として先駆的な役割を果たしています。
https://www.softbankrobotics.com/

ス感染症拡大やそれに伴う働き方の変化、そして海外拠点の増加などへ対応するために、企業のセキュリティモデルを"ゼロトラスト"へシフトする必要性があったため。特に、従来のオンプレミスを前提とした境界型防御モデルでは情報セキュリティの担保がもはや難しかったこと、また拠点ごとに利用するITシステムやツールが異なり、オンサイトかつ手動での管理運用に負担がかかっていたことから、今後のグローバル拡大も見据え、セキュリティ面でも、管理運用面でも統一した仕組みを導入し、グローバルレベルでITガバナンスを強化しようとしたのです。

●Jamf Proでゼロタッチ導入を実現

ゼロトラストセキュリティ構築のために同社がIDaaSやCASB／SWG／DLP、EDR／NGAVなどのソリューションと併せて導入したのが、Appleデバイス向け管理ソリューション（MDM）のJamf Proです。当時はスマートフォンよりもパソコンからアクセスできる情報資産のほうが多かったため、社内PCの半数以上を占めていたMacのデバイス管理から取り組みを開始しました。

「Mac向けのMDMを導入するうえで重視したのは運用面です。以前は別のMDMを利用していましたが、端末紛失時にワイプが行えなかったり、取得できるインベントリが限られていたりなど機能的な不十分さに課題を感じていました。Jamf ProはMacのゼロタッチ導入に対応していますし、macOSとの親和性が高く、機能が豊富なのも特徴です。また、さまざまなソリューションと連携するため拡張性にも優れます。特に、当社が導入するIDaaSとシームレスに連携できることも採用の決め手になりました」（プロダクト統括 技術本部 IT技術部 デジタル推進課 課長 渡邉邦尚氏）

Jamf Pro導入による大きな効果は、管理運用面での負荷が著しく低減したこと。特に拠点ごとに異なり、かつ手動で行っていたキッティング作業の時間を大きく改善できました。

「Jamf Proによるゼロタッチ導入を実現した今は、Macの箱を開けて本体に資産管理シールを貼って郵送するだけです。あとは従業員がMacの電源を入れて初期設定でネットワークに接続された瞬間にJamf Proで作成したポリシーが自動的に適用されます。これまでは1台キッティングするのに1～2時間かかっていましたが、10分～15分もあれば済むようになりました。また、端末の障害や故障、紛失時には代替機を送付するだけで従業員は素早く業務を再開できますし、退職後の再設定も簡単に行えます。オンボーディングから始まる端末のライフサイクル管理全体がとても楽になりました」

また、Jamf Proではリモートロックやワイプが可能なことから情報漏洩リスクを低減できたほか、アプリケーションの一括配付、豊富なインベントリ情報の取得も可能なため、業務効率化やセキュリティ強化にもつながっていると言います。そしてその結果、地理的に離れたグローバル拠点に対して、本社の東京にいながらIT環境を統一でき、オンサイト対応することなく、拠点ごとのリクエストやニーズに柔軟に対応できる環境を実現したのです。

ソフトバンクロボティクス株式会社
プロダクト統括 技術本部 IT技術部 デジタル推進課 課長
渡邉邦尚 氏

「Jamf ProでMacの端末情報を定期的に自動取得できるのも重要なポイントです。たとえば、特定の端末情報が欲しい場合は、インベントリ情報取得の処理をチェックイン時に実施するように設定すれば約15分おきに情報が取得できます」

さらにユーザ対応の際は、管理端末に対してリモートから画面共有を行い、遠隔操作やコマンドの実行が可能なJamf Proの「Jamf Remote Assist」も便利に活用しています。

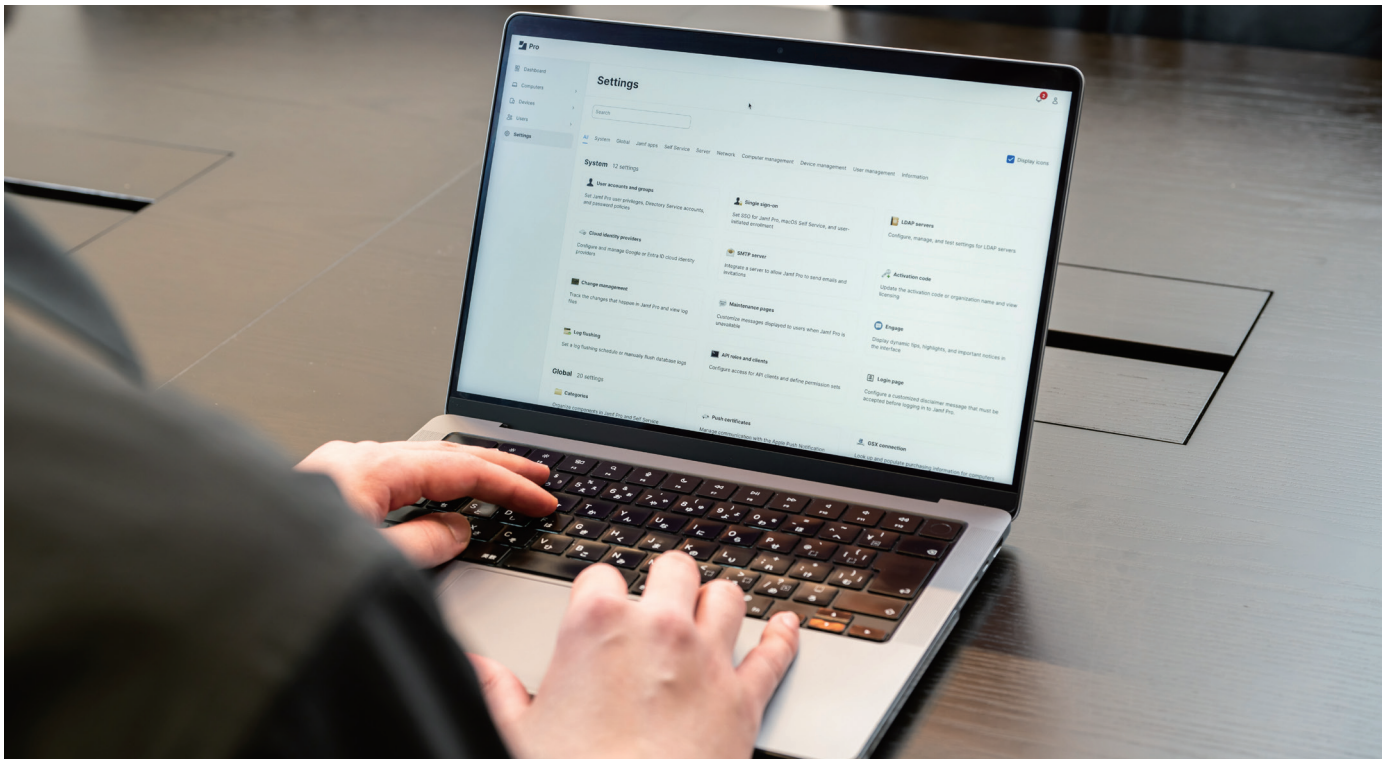
安全で効率的なBYOD運用 -必須だったJamf Connect ZTNAの選択-

●iPhoneを「会社領域」と「個人領域」に分離

MacやiPhoneのゼロタッチ導入実現後、同社では海外拠点におけるiPhoneのBYODにも着手しました。これまで各国で異なるポリシーで運用され、複数の経路で情報資産にアクセスするケースがあり、脆弱な認証や端末紛失、シャドーIT化、ウィルス感染などの情報漏洩のリスクがあったためです。

そこで、同社ではJamf Proの「アカウント駆動型ユーザ登録」を有効化して個人所有デバイスをJamf Proに登録し、iPhoneの中を「会社領域」と「個人領域」に分離。従業員がBYODの利用規約に同意したうえで「設定」アプリを起動して［一般］→［VPN とデバイス管理］と設定を辿り、会社管理のApple ID（管理対象Apple ID）およびIDaaSのアカウントでサインインして認証を行うと、会社領域を構成するプロファイルが適用され、必要な業務用アプリがインストールされます。

「会社として配布したアプリは会社の管理領域の中でしか



動かなくなります。また、会社の情報資産を個人領域に移動・コピー・ペーストができなくなるので、情報漏洩のリスクを圧倒的に下げられます。さらに、会社領域におけるインベントリ収集が行えますし、会社管理のApple IDでサインインしているので情報漏洩や不正が発覚したときは遠隔操作によって強制離脱させることも可能です」

●iPhone x Jamf Connectで安全な通信を実現

さらに同社ではiPhoneをBYOD運用するうえで、アプリの通信制御、すなわちゼロトラストネットワークアクセス（ZTNA）を実現するためにJamf Connect ZTNAの導入も行いました。その理由は、一般的なZTNAソリューションでは会社領域や個人領域にあるすべてのアプリの通信が同じネットワークサーバにVPN経由で接続されてしまい、個人領域にインストールしたアプリから企業リソースにアクセスできてしまうから。これではまったくセキュリティ的なアドバンテージがないことから、会社領域にあるアプリからは必ずJamf Connect ZTNAを経由して通信させることで業務リソースへのアクセスを制御しました。これにより、海外拠点の従業員の意思を尊重しながら、業務効率を落とすことなく、情報漏洩を防ぐことのできるセキュアな環境を構築したのです。

「Jamf Connect ZTNAでは専用ポータル（Jamf Security Cloud）からアプリ単位で通信の接続先などのきめ細やかなアクセスポリシーを作成できます。また、通信ログの可視化も可能で、情報漏洩につながる不正利用や不要な外部アクセスを確認できます。Jamf Connect ZTNAから直接インターネットに接続させるのではなく、当社サーバを一度経由してから接続させることで、Jamf Connect ZTNAとサーバによる2段階の通信ログを取得してセキュリティを高めています」

また、Jamf Connect ZTNAに実装されている次世代VPN「WireGuard」は一般的なVPNプロトコルと比較して約4倍のスループットを実現し、ほぼ途切れることのない安定通信が可能なこと、またデバイス側のオーバーヘッドが少なくバッテリ消費を抑えられることもメリットだと言います。

「iPhoneのBYODを実現しようとしたとき、このようなZTNAによるアクセス制御やログ解析を行えるソリューションはほかには存在しません」

デバイストラストでセキュリティを向上 -Jamf Pro×Jamf Connectのメリット-

●管理者にも利用者にも優しい導入

同社でJamf Connect ZTNAを採用した理由には、Jamf Proとの親和性の高さもあります。たとえば、Jamf Proを利用すればiPhoneの環境分離を行ったうえで、Jamf Connect ZTNAの通信に必要なクライアントアプリ「Jamf Trust」を含めて業務に必要なアプリを一度に端末にインストールできます。ユーザ視点で見れば、iPhoneに管理対象Apple IDとIDaaSでログインすれば自動的に構成プロファイルが適用されて業務に必要なアプリを入手でき、Jamf Trustにログインするだけで、私物のiPhoneでも個人領域のアプリからの通信が阻害されることなく、会社領域にセキュアに接続できる環境が整うわけです。

「iPhoneのBYOD運用は従業員に一部設定を行ってもら

う必要がありますが、基本的にはいつも利用しているメールアドレスでログインし、Jamf Trustをオンにするだけなので非常に簡単です。従業員向けの説明用マニュアルも簡略化でき、とても楽になりました」

また、Jamf ProとJamf Connect ZTNAを組み合わせれば「デバイストラスト（MDMとの連携によるデバイス認証）」によって、MDMに登録されている安全なデバイスのみ、または特定のグループのみアクセスを許可してセキュリティを強化できるのも利点です。

「端末に証明書を配付してデバイス認証する方法もありますが、証明書サーバを運用するには年間数百万ほどのコストがかかりますし、その証明書を管理するのも非常に大変です。Jamf ProとJamf Connect ZTNAの連携であればJamf Proで適切に管理されたデバイスかつ、ユーザ認証に成功し、脅威にさらされていないことが確認されたデバイスにのみ、社内リソースへのアクセスを許可できます。他ソリューションを利用したデバイス認証よりも安価なので、Jamf ProとJamf Connect ZTNAを組み合わせるのがもっとも合理的なのです」

このように同社では「グローバルレベルでの端末管理にはJamf製品が不可欠」と捉え、海外従業員の私物iPhoneに加え、コストパフォーマンスや管理運用面から標準機として採用するようになったMac、および国内従業員向けに貸与するiPhoneをJamf製品によって効率的かつ安全に管理しています。

●社内セキュリティ意識の醸成にもつながる

今回のJamf Pro×Jamf Connect ZTNAによるiPhoneのBYODの実現は、単なるセキュリティ強化や管理運用の効率化のみならず、これまで各拠点で統一されていなかったレギュレーションやセキュリティ意識のばらつきを解消でき、「社内のセキュリティ意識をグローバルレベルで醸成し、共通化できたこと」にも大きな価値があったと言います。

「グローバルでITサービスを提供するうえで研修会や勉強会などは行っていますが、“どこまで安全か”の基準は個人や国ごとに異なりますので、グローバル全体で一定レベルまで引き上げるのは簡単ではありません。そうした中で当社では、ユーザができることを画一的に制限するのではなく、ユーザが気づかないうちに情報漏洩や不正利用してしまわないように“安全のレールを敷く”という考え方を大事にしています。また、制限を課すときでも、従業員に対してその理由を説明して、それによって業務を阻害することなく安全を担保していることをしっかりとコミュニケーションするようにしています」

“セキュリティは業務をブロックするものではなく、業務を安全に支援する最大のアクセラレーター”。Jamf ProとJamf Connect ZTNAは、そうした同社ならではのグローバルレベルのIT統制に大きな役割を果たしているのです。

jamf
www.jamf.com/ja

Jamf Japan合同会社
Tel. 050-1790-2200
本内容は2024年12月現在のものです。