高度なセキュリティが要求される金融業界向けシステム開発

Windowsと同等のセキュリティを Macでも実現させるには

シンプレクス 株式会社 様

Appleデバイス管理ソリューション Jamf Pro
Mac 認証・アカウント管理ソリューション Jamf Connect 導入事例

シンプレクス株式会社は1997年の創業以来、メガバンクや大手総合証券、大手FX会社を筆頭に、日本を代表する金融機関に向けて、収益業務に特化した金融フロントソリューションを提供しています。金融とITの両方に精通したプロフェッショナルが、コンサルティングからシステム開発、保守・運用に至るまで、一気通貫で手掛ける企業です。連結従業員数は846名（2020年4月1日現在）、東京に本店・事業所を構えるほか、グローバル拠点としてサンフランシスコ、ニューヨーク、香港にも展開しています。

シンプレクス様では、WindowsとMacを使用されており、MicrosoftのMDM製品IntuneとJamf Proを連携、双方を統合的に管理されています。また、MicrosoftのクラウドIdP製品 Azure ADとJamf Connectを統合、クラウドIdPのID/パスワードによって、Macのローカルアカウントの作成やログイン情報を一元管理されています。

WindowsとMacの混在環境でセキュリティやIDの管理をどのように実現されていったのか、セットアップを担当された一戸さんと、ネットワーク担当者の太田さんにお話を伺いました。

管理に手間のかかっていたMacをWindowsとともに一元管理

●金融業界ではより高度なセキュリティが要求される

全体的にWindows端末を使用している中で、iOS／Android用システム/アプリの受注も多く、iMac、Mac miniも使用しています。Macに関してはExcelで台帳を作成して端末情報をまとめており、問題が発生した場合には端末の特定に時間がかかっていました。

また、金融業界のお客様が多いので、セキュリティ要件としては高度なものが求められています。Mac端末に関しては、OSのバージョンやインストールアプリの管理のために、Mac向けのMDMの導入が急務となっていました。

もともと自分（一戸さん）はiOS/macOSの開発・端末管理を経験していたので、Macを管理するためのMDMを検討する中で、Casper Suite（Jamf Proの前身）が出始めたころから知っていた「Jamf Pro」はほぼ一択と言って良い選択肢でした。

●インベントリ管理がスムーズにできるように

Macのシステム管理が十分行き届いていないところに導入したので、最初からガチガチにポリシーを設定するのではなく、まずJamf配下に端末を置こうというところから始めました。まだまだ検討することは多い状況です。

インベントリ管理がスムーズにできるようになったというのが、まず快適に感じているところです。プロジェクトごとにどんなスペックのマシンを何台購入しているのかをユーザから求められることが多く、Jamfからレポートをエクスポート・管理コンソールから検索することで即座に把握するといった活用はよくしています。

新規端末購入にあたっては、かつては1台ずつキッティングしていました。Excelで手順書を作成して、それに従って設定を手動で行う形ですね。Jamf導入後は、端末購入時に適切なタイミングで証明書・設定を配布できるようになりました。これにより大幅なキッティング工数削減に成功しています。

●Microsoft Intuneとの連携で高いセキュリティを確保

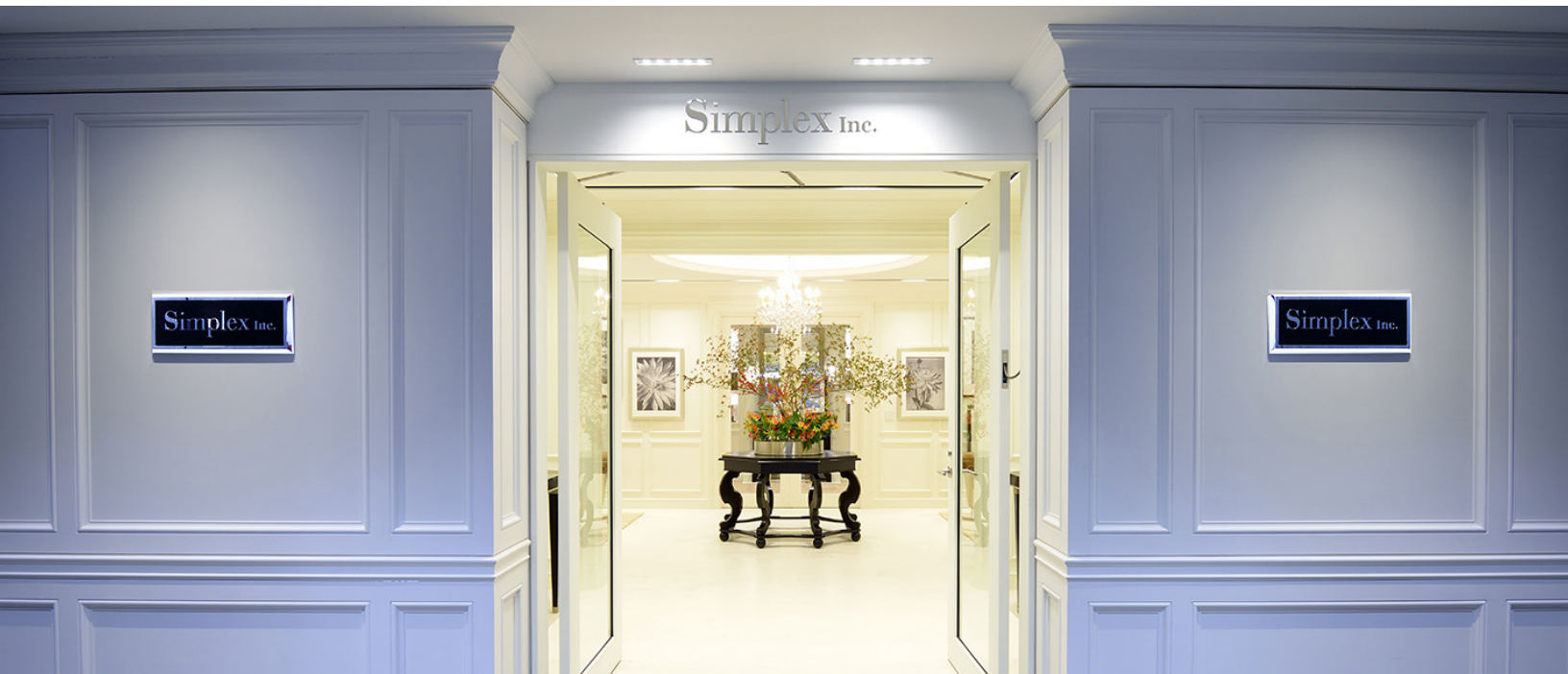
弊社では、Microsoft Azure ADの条件付きアクセスとIntuneのコンプライアンスポリシーを組み合わせセキュリティを担保し、Windows・モバイル端末を管理しています。Jamf Proを導入するにあたり、Macも同様の環境下で運用することが必須条件でした。

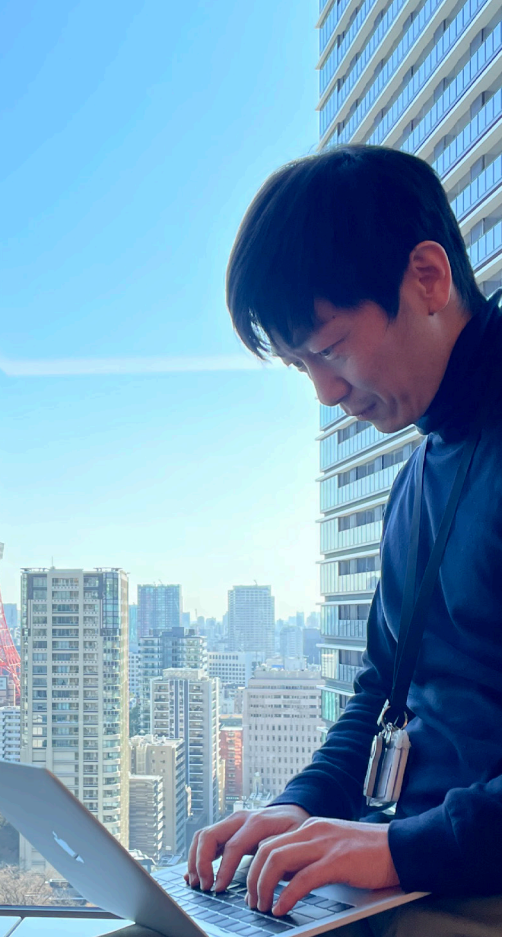
Jamfの設定というよりも、Appleの通信要件が障壁になってかなり苦労はしました。検証期間は半年程かかってしまいましたが、今は落ち着いて運用できています。MicrosoftのE5セキュリティとMacが、かなり密に連携できるようにJamfが仲立ちするというシステムになっています。

JamfとIntuneの統合連携に関しては実際に運用されている事例が少なく、またネットワークレベルでの細かい制御が必要だったのですが、試行錯誤しながら自分たちで導いていきました。

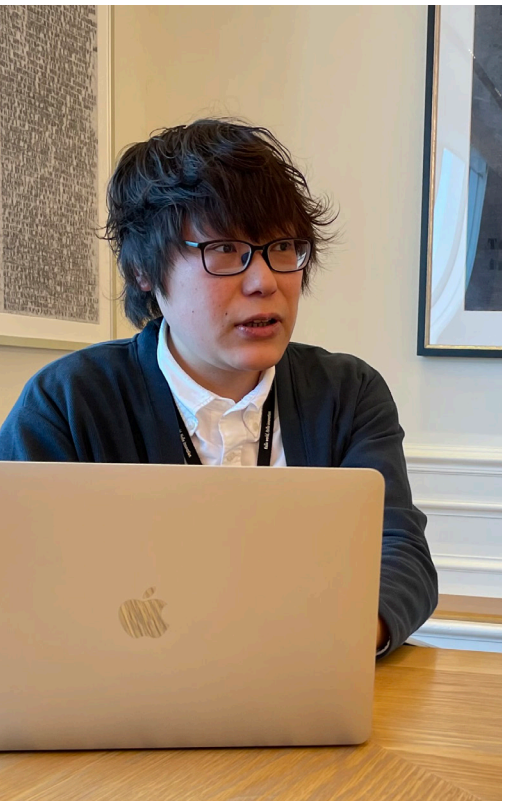
本当に地道な作業で、まず何も制御がかかっていないネットワーク上で正常に動作することを確認、そこから実環境で適用したいセキュリティポリシーを、1つかけてはテスト、もう1つかけてはテスト…といった具合に連携の構築を一歩一歩積み重ねていく作業でした。

MSとJamfの連携の実績が少ない中、主に社内のネットワーク部門と、組織として密に連携できたことが導入・運用に結びついた大きな要因ではなかったかと思います。





シンプレクス株式会社
オペレーションズディビジョン
太田貴之　氏



シンプレクス株式会社
オペレーションズディビジョン
一戸 慎也　氏

Jamf Connectの導入により残業規制を効率的に実践

●Windowsと同等のログイン管理をMacでも実現させた

高度なセキュリティが求められるなか、ログイン管理の煩雑さを解消することがJamf Connect導入のきっかけです。

当社ではAzure ADでID管理していますが、Macに限ってはローカルアカウントでの運用となっていました。アカウント管理をWindowsと統一できれば運用コストが大幅に削減できると期待し、追加でJamf Connectも検証・導入を行いました。

まだJamf Connectは導入したばかりで検証段階ではあるのですが、MacBookの導入とリモートアクセスも増えてきたので、早々に展開していこうと計画しています。

今後はセキュリティの向上とJamf Connectの展開を進めたい

●Microsoft Defender ATP for MacでWindowsと同等のセキュリティを

当社ではWindows端末はMicrosoft Defender ATPを導入して、アンチウイルスやセキュリティ関連を制御しています。先ごろ、macOS向けにもMicrosoft Defender ATPがリリースされたので、パターンファイル更新間隔、スキャンタイミングの設定更新等、Windows端末と同様のセキュリティポリシーにのっとって制御できるようになり、Jamf Proで配信・運用が開始できました。これによって、高度なセキュリティ・インシデント・レスポンス管理できる同一の基盤に、Mac端末とWindows端末を乗せることができました。

●Mac固有のセキュリティの問題をJamfでカバーしていく

Mac標準機能の多くはユーザにとってとても便利で扱いやすいものですが、管理者的には厄介なことが多いと感じています。例えばAirDropやBluetoothでのデータ転送が簡単にできてしまう点が挙げられます。これらをカバーしていくために、Jamfを通してセキュリティを強固にしていければと考えています。

今後のMDMをめぐる状況に関してですが、統合はどんどん進むと思います。どうしてもMicrosoftが中心で機能が追加されていく形にはなると思いますが、MacとIntuneの連携が早々に実現できたことは、私たちの今後の大きなアドバンテージになります。今回蓄積された構築のノウハウで、今後サービスが追加されていってもスムーズに対応していけると思います。そのいい例が今回、ATP for Macをスムーズに導入できたことですね。

今後もE5セキュリティの機能がMacにも拡充されていくと思いますが、蓄積してきたノウハウを武器に、Jamfを絡めながらそれらを展開していければと考えています。

Jamf Japan株式会社
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2020年12月現在のものです。