ポストコロナ時代における
Appleデバイス管理のあり方

2020年に始まったコロナパンデミックは、私たちの働き方を大きく変えました。テレワークやリモート会議などを活用する働き方の変化は、パンデミック収束後の世界にも少なからず影響を与えることでしょう。あらゆる場所からのネットワーク利用を安全かつ効率的に行うためには、新しい時代のネットワークアクセスや、セキュリティの考え方が必要になります。ここではポストコロナ時代を見据えた、ゼロトラストネットワークアクセスの実現へのステップと、その中で活用していただきたいJamf製品について解説します。

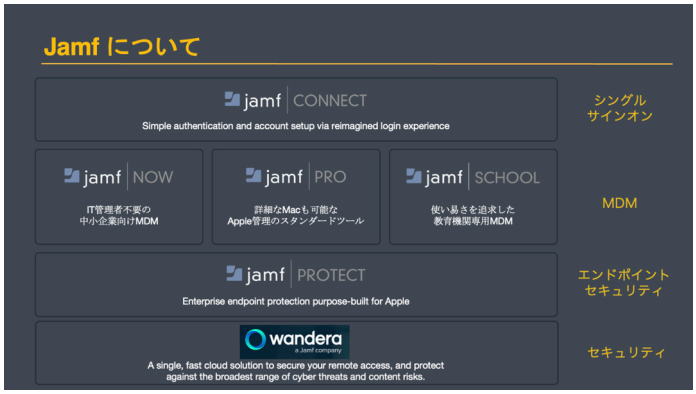
JamfとJamfのプロダクトについて

● Appleデバイス管理のスタンダードJamf

まずは弊社Jamfについて説明します。
右図の中でJamfのロゴの下にある「Helping organizations succees with Apple（Appleと共に成功するお客様を支援する）」。これはJamfのスローガン・社訓のようなもので、Appleデバイスを利用する法人の成功・成長をお手伝いする弊社のポリシーを表しています。
Jamfは2002年にアメリカのミネアポリスで創業し、昨年7月にはナスダックに上場しました。日本法人は2017年に設立しています。
全世界で50,000を超えるお客様に利用されており、Jamfで管理するデバイスは2,100万台を超えています。日本ではディー・エヌ・エー、SmartHR、シンプレクスなどの企業を始め、多くの学校や病院などでも利用されています。詳しくはWebで事例をご紹介しておりますのでご覧ください。

● Jamfのプロダクト展開

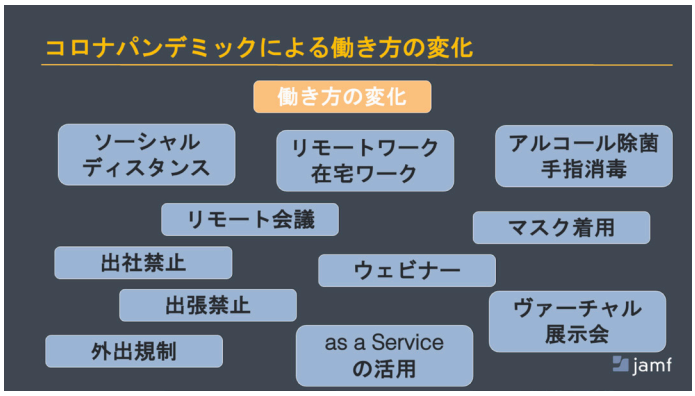
Jamfでは右下の図のようにプロダクトを展開しています。
まずはじめに、中央にあるJamf Pro。これは弊社のメインであるMDM（モバイルデバイスマネジメントツール）で、Mac、iPhone、iPad、Apple TVなどAppleデバイスを幅広くかつ、死角なく管理するものです。
Jamf Proの左にあるJamf Nowは、中小企業に特化したMDMで、3台まで無料で使えるソリューションです。右のJamf Schoolはその名の通り、学校向けのソリューションです。
上段のJamf Connectは、Macのシングルサインオンの機能を担うもので、学校や企業で使われるActive Directoryとの連携や、クラウドIdPをMac



とつなげるためのソリューションです。下段は、Mac専用のエンドポイントセキュリティソフトであるJamf Protectと、今年Jamfグループに加わったトータルセキュリティソリューションであるWanderaです。

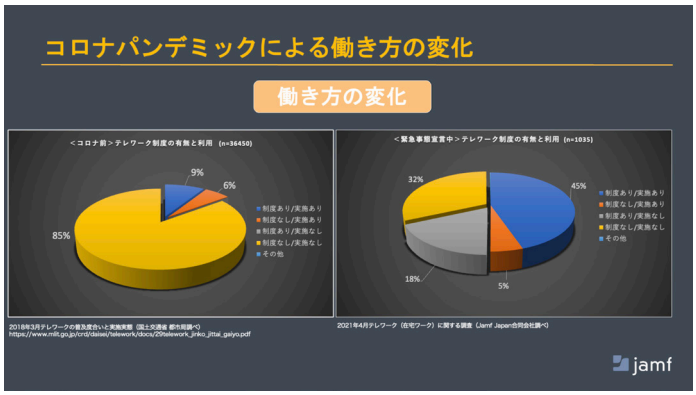
コロナパンデミックによる働き方の変化

● 日常生活も働き方も変化

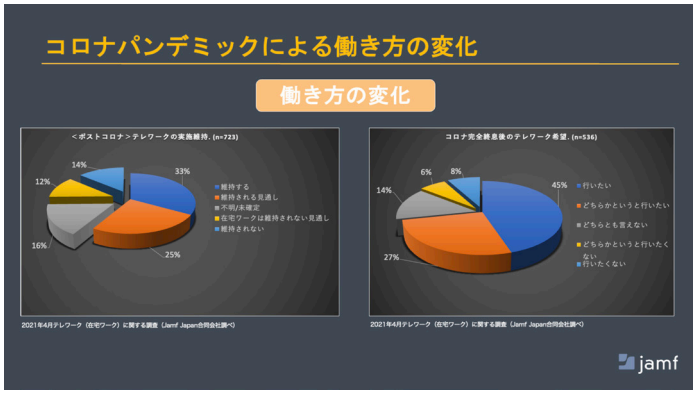


このコロナパンデミックにおいて、私たちの生活はどのような変化があったのでしょうか。
日常生活においては、ソーシャルディスタンス、マスクの着用、消毒、不要不急の外出自粛によって遊びに行くことができなくなりました。海外ではロックダウンや厳しい罰金制度も実施されました。全世界的に生活様式が大きく変化し、その影響が色濃く残っているのが現状です。
次に働き方の変化を見ていきましょう。こちらも日常生活と同様、大きな変化がありました。弊社でも在宅ワークを開始し、すでに1年半以上が経過しています。
働き方改革や、DXが叫ばれていた最中でのコロナパンデミックにより、従業員の働き方に関しても大きくメスが入っています。営業活動や、社内ミーティングもリモート会議に変化。遠方への訪問も、出張しないスタイルというのが定番化してきています。企業でも多くのアズ・ア・サービス（as a Service）が採用され、出社しなくても仕事ができる環境整備が行われてきたというのがよくわかります。

● ポストコロナ時代もテレワーク・在宅ワーク



では実際のテレワーク・在宅ワークの実施率はどうなっているのでしょうか。
右図は国交省が2018年に発表したデータ、並びに弊社Jamfににて調査をした結果です。4年前の2017年度では、まだテレワークを導入している会社は少なく、全体の15%程度でした。しかし2021年の緊急事態宣言下でのテレワークの実施率は、全体の50%に上り、約半数の企業においてテレワーク・在宅ワークが実施されています。これは物理的に作業を行わなければいけない製造業やサービス業、対人での対応が必要となる医療や介護などの業界を含んだ結果ですので、実際には相当数でテレワーク・在宅ワークについての整備が進んでいることがわかります。
次にコロナの収束後、ポストコロナの時代においてはどうなっているでしょうか。コロナが収束した後のテレワーク・在宅ワークの維持継続について、ヒアリングを行った結果が右の図です。
テレワークを維持・継続すると答えた企業は、全体の58%となっており、実に多くの企業が従業員の働き方の選択肢として、テレワーク・在宅ワークを推奨していることがわかります。また従業員においても、全体の7割以上の人たちがテレワーク・在宅ワークを希望しています。



ワークライフバランスの取り方、生産性の上げ方、社内社員間のコミュニケーションなど、課題は色々とありますが、

ポストコロナの時代においても、多くの企業でテレワークを行うでしょうし、従業員も制度を望んでいるという現状があるのです。今までの企業のしくみ、インフラ、システム管理の方向性についても新時代に合わせる時が来ていると言えるでしょう。

ゼロトラストネットワークアクセスとは

● Zero Trust Network Access（ZTNA）

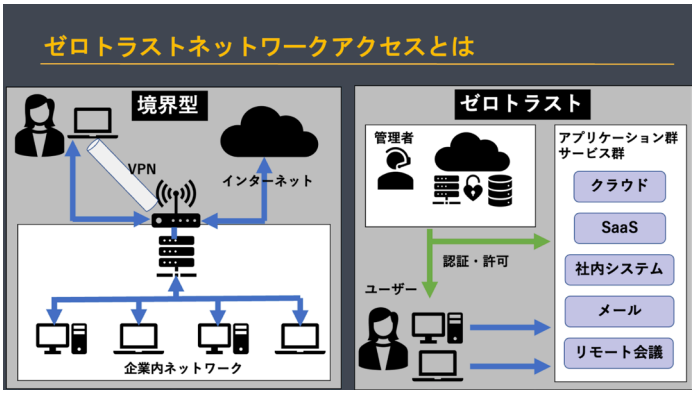
新時代の働き方に対応する新しいネットワークアクセスやセキュリティの考え方を、現在バズワードにもなっている「ゼロトラストネットワークアクセス」から説明します。
Wikipediaによれば、「ゼロトラストネットワークアクセスは境界のないセキュリティであり、企業のLANで繋がっていても、デフォルトは信頼されるべきではないという考え方。クラウドベースのサービスや、インフラ、リモート環境や、デバイス環境への接続が増えると、VPNを介してアクセスされたデバイスを信頼する（従来の）アプローチは意味をなさなくなる。ゼロトラストの考え方は、場所を問わずアイデンティティを確認する、またデバイスの健全性を信頼性に基づいてアクセス提供する（弊社抜粋・翻訳）」となっています。
ゼロトラストネットワークアクセスの大前提は、「基本的に信頼しないこと」です。誰がアクセスしたのか、どこから来たのか、どこへ行くのか、そしてデバイスは正常な状態か。これらの4つの項目を必ず毎回確認することで、信頼できるアクセスなのかどうかを確認します。当たり前のように感じられるかもしれませんが、この当たり前を都度確認し、都度認証していくということがゼロトラストの基本的な考え方なのです。

● 従来のネットワークアクセスとの違い

では、今までのネットワークアクセスと、ゼロトラストネットワークアクセスがどのように違うのか簡単におさらいしてみましょう。
従来のしくみは、社内と社外のネットワークを分離し、間に城壁のような強固な壁を作り防御する『境界型』と呼ばれるもので、壁をしっかりと守ることで壁の中は安全であるという考え方です。対してゼロトラストは、ネットワークの境界をなくし、来るものすべてに対して検疫をかけていくしくみです。
一見、境界型の方がセキュリティが高そうに見えるかもしれません。しかし、この境界型の欠点は、壁に穴が開いてしまった場合に壁の中の安全地帯が瞬く間に危険地帯になってしまうことです。社員が誤ってスパムメールを開いてしまったり、悪意のあるものの手によってセキュリティホールが開いたら、社内のネットワークは安全なものではなくなってしまいます。
その点ゼロトラストは、常に検疫をかけることで、状態の悪いものや怪しいものを排除することができるため、さまざまな場所・条件からのアクセスを行う新時代においては、非常に有用なものであることがわかります。

● ZTNAのしくみ

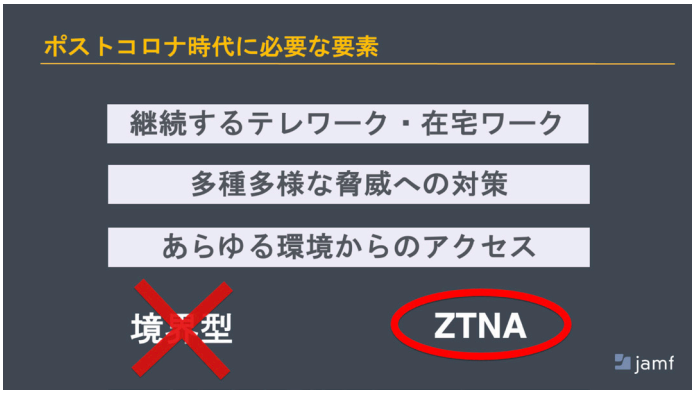
右の図は、企業内のシステムを簡略化したものです。境界型では社内のネットワークを安全に保ち、社内に対してアクセスを行う際は、VPNへトンネルを作りアクセスをするという形です。
しかし在宅ワーク・リモートワークが多くなった昨今では、VPNの帯域が不足したり、セキュリティの甘い自宅や、パブリックWi-Fiからのアクセスによって安全性が担保できなくなってきています。
ゼロトラストネットワークアクセスでは、企業内外の境界は存在せず、ユーザーは直接利用するサービスに対してアクセスを行います。社内のシステムにアクセスする場合においても、アイデンティティーの認証や、アクセス権限のチェック、許可を行います。
ではどのような要素がゼロトラストネットワークアクセスに必要なのでしょうか。



ポストコロナ時代に必要な要素

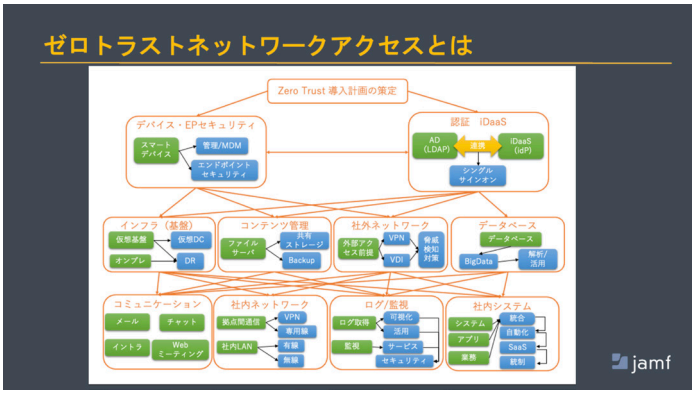
● ゼロトラストネットワークアクセスの構築

先に示した資料の通り、コロナが終息した後のポストコロナ時代においても、テレワーク・在宅ワークは多くの企業で継続される見込みです。
仮に社員の一部だけでテレワークを実施する場合であっても、社内外あらゆる所からのアクセスが発生することによって、ネットワークはさまざまな脅威にさらされることになるでしょう。
従来の境界型アクセスや、セキュリティのしくみは企業を守ることはできず、新時代のネットワークアクセス、ゼロトラストネットワークアクセスが必要になるのはおわかりいただけたと思います。
では、ゼロトラストネットワークに必要な要素はどのようなものでしょうか。
右図にあるのは、今年経産省が策定した『デジタルプラットフォーム構築事業の報告書』で、現時点で構築することのできるゼロトラストネットワークアクセスについてまとめた資料です。認証・認可に始まり、企業運営に必要な要素やモデルケースが記載されています。
https://github.com/meti-dx-team/METI-Digital-Tools/



● 必要なファクターと優先順位について

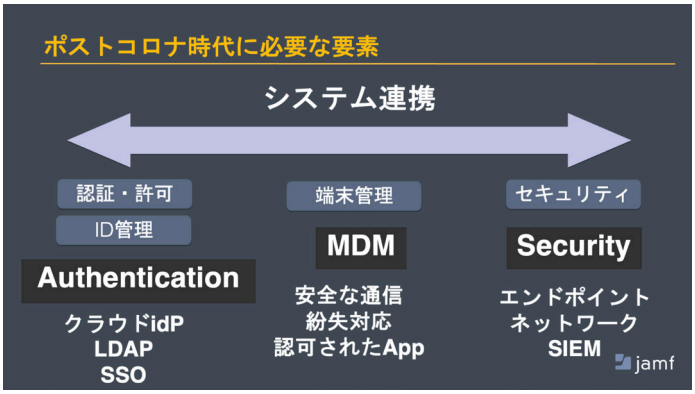
右図は、ゼロトラストネットワークアクセスを導入するにあたって必要なファクターと、順番の一例ををまとめたものです。
まず社員が使うデバイスの調達やその管理、そしてアクセスをつかさどる認証や、アイデンティティが最初に手をつけるべき要素でしょう。現在ある資産、しくみをうまく活用することもできますが、これからゼロトラストを検討する企業では、まずこれら

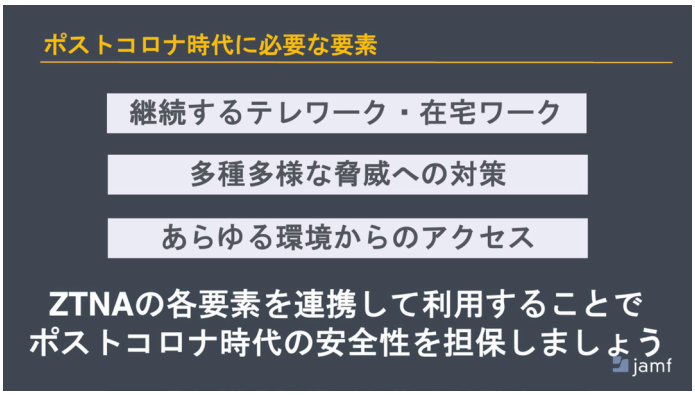


の2点を見直してみることをお勧めします。そして物理的なインフラをクラウド化するのか、社外からのアクセスをどう整備するのか、社外や社員間のコミュニケーションはどのようにするのか、社内のシステムに対してどう自動化させていくのかと順々に考えていくとよいでしょう。

● ID管理・端末管理・セキュリティ

ID管理、端末管理、セキュリティについてもう少し掘り下げていきます。
基本的に何も信頼しないことを前提としたゼロトラストネットワークアクセスにおいては、誰が、どこから、どこへアクセスをするのか、そしてそのデバイスは健全な状態なのか、を確認することが基本的な考え方です。この根本となる4つの要素については、認証・認可、ID管理、端末管理、そしてセキュリティで実現することができます。
具体的には、ID管理ではクラウドIdPやレガシーのAD。認証・認可においてはSAMLやLDAP、シングルサインオンの活用なども行われます。端末管理にはMDMを活用し、認可されたAppだけを使用した安全な通信をさせたり、物理的な紛失対応を行います。そしてセキュリティについては、エンドポイントやネットワークのセキュリティ、振る舞い検知、SIEMの統合なども重要なポイントです。
そしてさらにこれをシステム的に統合・連携させることも重要です。それぞれが単体で動作するだけではあまり意味がなく、常に検疫を必要とするゼロトラストではこの連携こそがキモであり、新時代に合ったゼロトラストネットワークアクセスの第一歩につながります。





ポストコロナの時代における多種多様なアクセス、そして多種多様な脅威から企業を守るためにはゼロトラストネットワークアクセスの要素をシステム的にも連携させ、安全性を担保していることが重要なのです。

Appleデバイス管理の必要性

● ZTNAとJamfのソリューション

ではゼロトラストネットワークアクセスの第一歩を踏み出すための、弊社Jamfのソリューションについて紹介しましょう。右図は冒頭にも紹介したJamfのポートフォリオですが、認証、デバイス管理、セキュリティの3つの要素を網羅していることがわかります。
またMDM（モバイルデバイスマネジメントツール）のJamf Proをベースとして、ID管理、シングルサインオン、セキュリティが総合的に接続し、互いに連携することによって、「Just Jamf」。つまりJamfによって、ゼロトラストネットワークアクセスが実現します。
MDMについて、以下でもう少し詳しく説明します。

● MDMの役割

企業においては、システムの導入が従業員の稼働を確保するという意味で、まずはじめの一歩となります。デバイスの導入を行う際にシステム担当者の方が懸念される点については、右のような図にしてみました。

まずはセキュリティです。あらゆる脅威への対策はもちろん、最新のセキュリティパッチを適用するためにOSのアップデートなども必要です。

次に利用する従業員のID管理やパスワード管理です。ここにはActive Directoryやシングルサインオンなども含まれます。またどのようなしくみを使い、どのような認証するのか、そしてどうやって安全なアクセスを実現するのか。その策定も必要でしょう。

そして何より時間を取られる部分は、大量のキッティング作業です。セキュリティポリシーやID管理のポリシーを策定しても、設定が行わなければ意味をなしません。情報システムの担当者は、従業員の増減などをトリガーに、大量のキッティング作業に追われることが多いと聞きます。特に新入社員が入る新年度・年度末は、寝る間も惜しんで作業を行った経験がある方も多いのではないでしょうか。

業務に必要なAppの配信や、盗難・紛失に対しての対応も必要です。このあたりもしっかり押さえておかなければ、いざという時の対処が難しいでしょう。このようにデバイスを導入するタイミングでは、さまざまな問題・課題が発生します。これらの課題を解決することができるもの、それがMDMです。

● 一般的なMDMでできること

右に一般的なMDMで行うことができる内容をまとめました。

前段で解説したセキュリティ、ID管理、大量のキッティング、Appの配布や、設定の配布、盗難・紛失対策といった情報システム担当者が懸念されるポイントを押さえていることがわかります。

しかし、こちらはあくまでも一般的なMDMの例です。では、弊社が提供しているJamf Proにはこれらに加え、どのような特徴があるのでしょうか。

● Jamf Proの特徴

Jamf Proは、Appleデバイス専用のMDMです。Appleのデバイスは他のデバイスと比較し、もともとセキュリティが高いため、企業で使うデバイスとして適していると言えます。

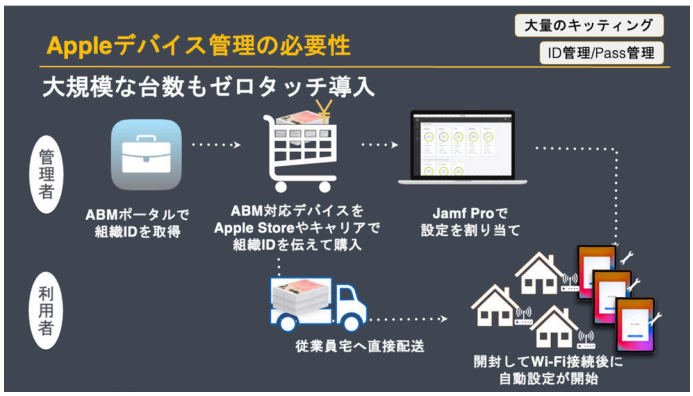
このセキュリティの高いMac OS、iPad OS、iOS、tvOS を管理することができるソフトウェアがJamf Proです。Appleデバイス専用なので、管理機能もマルチOS対応のMDMに比べ、AppleのMDMフレームワークに詳細まで対応しています。

● Apple Business Managerとの連携

Jamf Proは、Appleが企業向けに展開しているサービスポータルであるApple Business Manager（ABM）への対応はもちろん、連携もしています。ABMと連携することで、Jamf ProはAppleデバイスをゼロタッチでキッティングすることもできます。またVolume Purchasing（従来のVPP）を使用し、企業で使うAppの一括購入も可能となるため、大規模な導入であってもしっかりと力を発揮することができるのが特徴です。

● ゼロタッチ導入

Automated Device Enrollmentを活用したゼロタッチ導入について簡単な図で表してみました。まず管理者がABMで組織IDを取得します。次にABM対応のAppleデバイスを、Apple Storeや通信キャリアで購入します。そのあと、シリアルなどの情報をもとにJamf Proで設定を割り当てておきます。購入したストアからは、各従業員が在宅ワークを行っている自宅へ直接デバイスを配送します。従業員は手元に端末が届き、開封、初期セットアップの大タイミングでWi-Fiに接続をすると、その端末に割り当てられている設定が自動的に適用され、すぐに業務を開始することができます。管理者は実際にデバイスを触ることなく、ゼロタッチで従業員にデバイスを割り当てることができるのです。

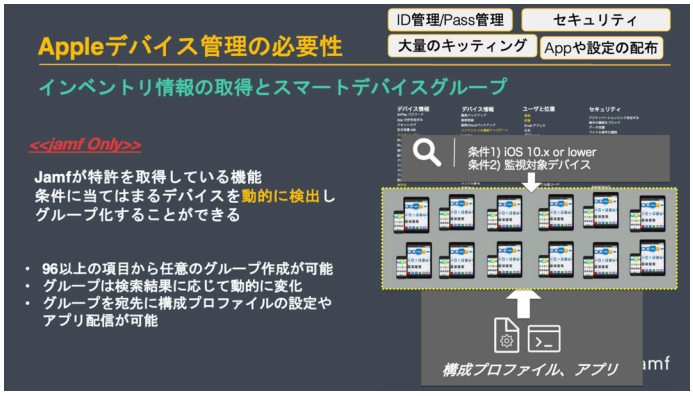


● Self Serviceの機能

Appleのしくみと、MDMを組み合わせることにより、時間・工数の大幅な削減を実現することができます。Appや設定を配布するのに便利な機能が、Self Service（セルフサービス）の機能です。
Self Serviceは企業向けの専用アプリカタログで、組織が推奨するAppやドキュメントを配布することができます。従業員に使わせてもよいAppをSelf Serviceに掲載することで、認可されたAppのみの利用に制限することができます。スクリプトセットを掲載することもできますので、SMCリセットや、NVRAMのリセットコマンドを掲載しておけば情報システム担当者の方への問い合わせを軽減することができます。企業で独自開発されたAppについても掲載することが可能で、マニュアル類に関してもブック形式で配布することができるのが、Jamfならではの特徴です。

● スマートグループの活用

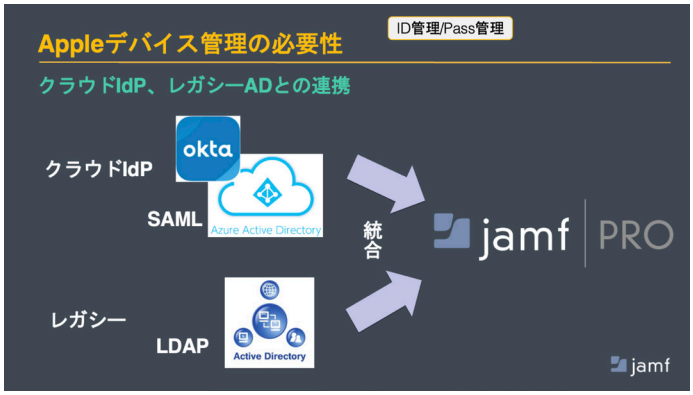
Jamf Proの一番の特徴が、動的なグルーピングである、スマートグループです。
一般的なMDMでは、静的にデバイス1台1台を選択しグルーピングを行うことがほとんどです。
Jamf Proでも手動のグルーピング作成はもちろん可能ですが、さらにインベントリ情報でリアルタイムに収集した情報を元に、事前に設定したルールに基づく端末を動的に抽出しグルーピングを行うことができます。取得できるインベントリ情報は右の一覧の通り93項目あり、これらの項目から条件を設定することができます。
具体的には、例えば『 iOSのバージョンが10.x以下で、かつ監視対象のデバイス』というグループを作った場合、自動で該当する端末がこのグループに入ります。
自動生成されたグループに対しては、プロファイルの設定やAppの配信、あるいはOSのアップデートをかけることができます。OSアップデートが終了し



たものは、条件から外れるため自動的にこのデバイスグループから削除されます。
この動的なスマートデバイスグループの作成を行うことで、各種設定の漏れや、脅威が付け入る隙を極限まで少なくすることができ、管理者の負担軽減に大いに役立ちます。ちなみに、このスマートデバイスグループの機能はJamfがパテントを取っているため、他社にはないJamf独自の機能です。
またOSのアップデートに関しては、Jamfは9年連続でAppleがローンチしたその日にJamf Proのアップデートを行い、対応しています。OSのバージョンアップには、クリティカルイシューの回収や、セキュリティの強化、便利な拡張機能が含まれています。常に最新版のOSを使うことにより便利に、そしてなにより安心安全にデバイスを利用することができます。

● アイデンティティの連携

アイデンティティの連携もJamf Proの大きな特徴のひとつです。カスタムMDMは単体で利用されることが多く、このようなレガシーのADやIdPとの連携機能を持たないものもあります。
ゼロトラストネットワークアクセスでは、IDの連携、シングルサインオンが非常に重要なファクターです。Jamf ProではレガシーのAD、LDAPの統合はもちろん、クラウドIdPであるOktaやAzure ADとの統合を行うことができます。SaaSを多く利用される企業では、SAMLの認証が必要となるため、統合させることにより、より多くのシステムと連携を行うことが可能になってきます。



● Wandera

そして最後に紹介するのが、2021年の7月1日にJamfが買収したWanderaです。Wanderaは、Jamfのポートフォリオの中で唯一、マルチモバイルOSに対応したソリューションです。
特徴は、Threat Defense、Data Policy、Private Accessの3点で、モバイルのエンドポイントセキュリティや、データ使用量の可視化、そしてIdPとの統合が実現可能です。またJamf Proと連携することが可能で、Appの配布やステータスからスマートグループを作成するなどの機能を実装しています。

● まとめ

以上のように、Jamfが連携するソリューション、Jamf ProやWanderaを活用することによって、ゼロトラストネットワークアクセスの第一歩目を踏み出すことが可能になります。
セキュリティに強く、企業での導入が増えているiPhone、MacなどのAppleデバイスと、Jamf ProやWanderaを組み合わせて利用することで、新時代に即したゼロトラストネットワークアクセスの形が見えてくるのではないでしょうか。

Webinar Information

本記事は、2021年7月16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
www.jamf.com/ja

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。