社内にあるMac管理の必然性と セキュリティリスク

昨今のコロナ禍で、リモートワークを取り入れる企業が増えてきています。
このため企業のIT部門の方から、今までは管理していなかった『社内にあるMac』を管理する必要性について、「認識はしているものの、会社にその必然性を説明しきれない」といったご相談や、「既にWindowsと同じ環境でMacを管理しているが、管理しきれていないのではないか？」という懸念をお持ちの方が増えています。
またMac管理の必要性を感じていても、そのコストをかけることに対し、会社への説明に苦慮されている方も多いのではないでしょうか。
本資料では、社内にあるMacを管理することの必然性と、その中でのJamf Proの優位性について。また実際にMDMを導入される際に必要となるカウンタートークの3つのStepで解説いたします。

Step 1：Macを管理するとは？

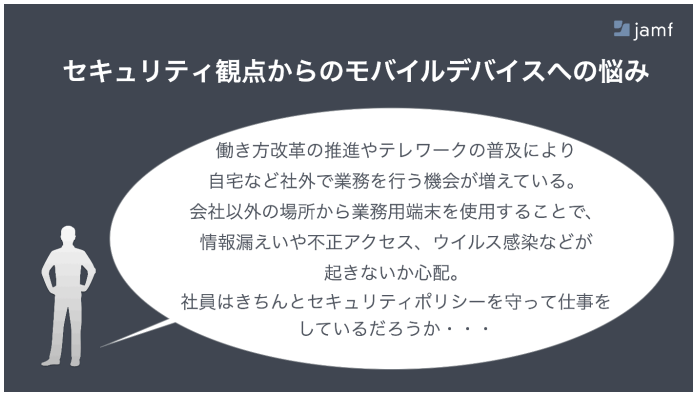
● デバイス管理の必要性

デバイス管理の必要性について尋ねられた場合、おそらく多くの方は「YES」と答えることでしょう。
では、なぜデバイス管理が必要なのでしょうか？
「デバイス管理」という言葉自体も曖昧で、『誰がどのデバイスを使っているかを管理すること』、『デバイスの状態を可視化すること』など、いくつかの解釈が考えられます。

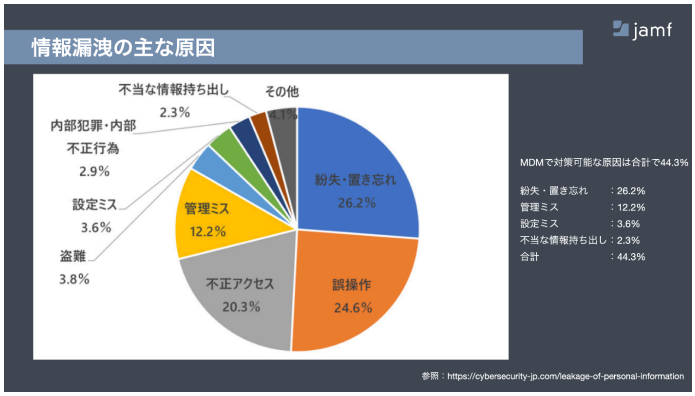
前者の『誰がどのデバイスを使っているかを管理すること』であれば、Excelで管理できなくもないでしょう。しかし今回ご紹介したいのは、『デバイスの状況を可視化し、さらに設定などの運用もできるソリューション』である、Mobile Device Management、通称『MDM』です。
次に、このMDMソリューションが必要とされる背景を考えてみます。
MDMを導入する目的は企業によっていろいろですが、ここでは2つに分けて考えます。
まず1つめはセキュリティ対策で、どの企業においても共通して挙げられる重要な要素です。

● セキュリティ観点からのデバイスの悩み

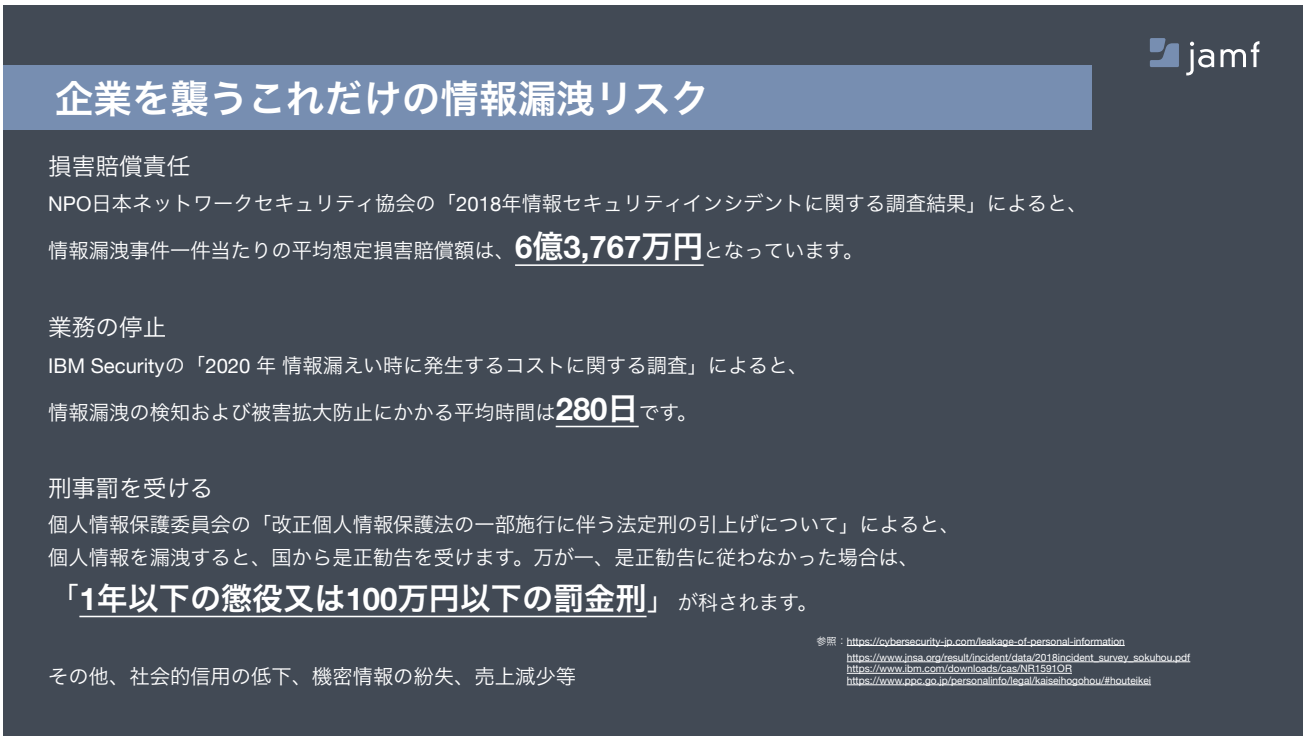
ではセキュリティの観点から、IT管理者や経営層が抱える悩みを見てみましょう。
働き方改革の推進や、テレワークの普及により自宅など社外で業務を行う機会が増えています。会社以外の場所から業務用端末を使用することで、情報漏洩や不正アクセス、ウイルス感染などが起きないか。あるいは社員がセキュリティポリシーを守って仕事をしているかどうかを心配する声は少なくありません。
また、業務用端末の盗難や紛失、パスワード設定やデータ暗号化といった対策が施されているか、といった点も懸念される部分です。



右の図はセキュアオンラインにて発表された、企業の情報漏えいの原因別グラフです。端末紛失、不正アクセス、管理ミス、設定ミスなど原因は様々ですが、この中の『紛失・置き忘れ』など、MDMで管理することで防げる項目を合計すると、44.3%にも達します。裏を返せば、現状もしMDMで端末管理していない状態であれば、4割はリスクのある状態だということです。



実際に情報漏洩が発生した場合、企業には下図のように、損害賠償責任、業務の停止刑事罰、信頼の低下売上減少などがデメリットがあり、損害賠償責任の平均賠償額は6億円を超え、業務停止期間は平均280日というデータもあります。MDMでデバイスを管理することで、このようなリスクを大幅に減らすことができるのです。



● MDMでデバイスをよりセキュアに

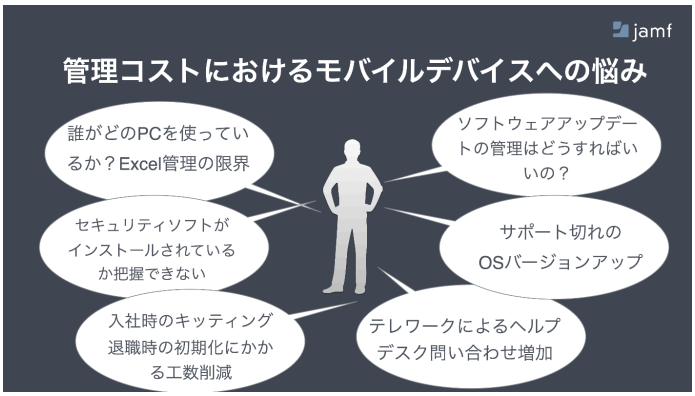
MDMによるデバイスの管理では、まずはじめにパスワードポリシーの設定や、ディスクの暗号化などセキュリティや機能に対しての制限を「構成プロファイル」と呼ばれる設定を作成し、遠隔で配布します。そしてこれらの設定が正しく配布できているかどうかを監視し、万が一会社のセキュリティポリシーから外れたデバイスがある場合は、ポリシーに準拠するように遠隔で設定を変更することが可能です。

また紛失や盗難時にも、対象のデバイスに対しロックをかけたり、最悪見つからない場合にはデータを消去することが行えます。

このように遠隔から社員のデバイスを設定して可視化し、制御できるのがMDMなのです 。

● 管理･運用コストにおける悩みを解決

MDMを導入する目的の2つめは、管理コストの削減です。
たとえ1台であっても、会社の機密情報や個人情報などが入っている業務端末の管理はしっかりと行う必要があります。もちろん管理端末が増えれば増えるほど、管理コストも上がります。
誰がどのPCを使っているか、Excel管理の限界、インストール済みのソフトウェアのバージョンアップの管理、セキュリティソフトやOSのバージョンアップ、入社や退職に伴うPCのセットアップなど。どれも対策に工数がかかるもの。さらにテレワークでヘルプデスクがパンク状態になってしまうといった悩みを抱えている企業も少なくないでしょう。
弊社のMDMであるJamf Proには、管理機能が大きく分けて5つあります。まず導入の部分では、ゼロタッチキッティングで自動セットアップが可能になります。またデバイス設定、アプリ配信、インベントリ情報でデバイス状態を可視化して管理します。インストール済みアプリケーションのバージョン管理も簡単に行えます。さらにはセルフヘルプにより、従業員の皆様ご自身で問題解決できる環境があります。これらを先ほどの悩みに当てはめると、管理コストにおける悩みの数々が解決できることがわかります。



● 業務用モバイルデバイスの管理は大丈夫？

『MDM』という言葉は、Appleが定義したものです。AppleがMDMプロトコルを開発し、iOS 4が登場した2010年に、MDMによる端末集中管理に対応させました。
今ではiOSに限らず、Android、Windows端末、macOSも対象となり、MDMという言葉が広く認知されるようになりました。企業においてiOSやAndroidを導入する際に、MDMの存在は欠かせないものとなっています。
では業務用PCの場合はどうでしょうか。企業は業務用PCの管理もしっかりMDMを利用して行なっているのでしょうか？多くの企業の答えはおそらく「Windows 端末だけ管理している」です。多くのMDMや資産管理ツールでは、Windowsは管理できても、Macに関してはほとんど管理できないからです。
下の表には、Apple、Microsoft、Googleの裏で動いているアーキテクチャが記載されています。プロビジョニングや暗号化など、それぞれのアーキテクチャはこのように異なっています。このためWindows向けに作られている管理ソリューションでMacの管理をすることは非常に難しいのです。Windows PCでは当たり前にできているデバイス状態の可視化が、Macの場合ほとんどできていないというのが実情です。

	Apple		Microsoft		Google	
	macOS	iOS	Windows	Windows10 Mobile	Chrome	Android
プロビジョニング	Device Enrollment Program		Azure AD によるダイナミックプロビジョニング		ゼロタッチ登録	ゼロタッチ登録
暗号化	FileVault	パスワードで有効化	BitLocker		クラウドストレージによる暗号化	最新デバイスではビルトイン暗号化
管理フレームワーク	Apple Push Notification ServiceによるMDM		Windows Push Notification ServiceによるSCCM＋ MDM	Windows Push Notification Service による MDM	Chrome Management	Google プッシュ通知による MDM
設定管理	構成プロファイル		グループポリシーオブジェクト	構成ポリシー	Chromeポリシー	Android (旧Android for Work)
ソフトウェアライセンシング	Volume Purchase Program		Winsows Store for Business		Chrome Web Store	Google Play Volume Purchse

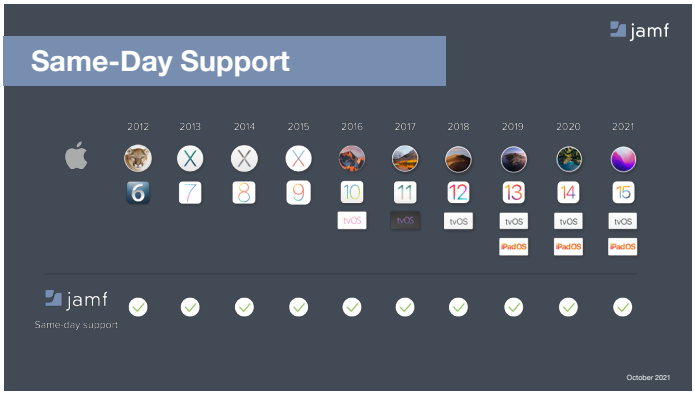
Step 2：Appleデバイス特化MDM、Jamf Proの優位性

● Appleデバイスに特化したMDM『Jamf Pro』

このStepのポイントは2点あります。
まず1つめは、Jamf ProがAppleデバイスに特化したMDMであるということ。管理対象のAppleデバイスはMac、iPad、iPhoneの他にApple TVも含まれます。
一般的なMDMの場合、AndroidやWindowsも管理できるマルチプラットフォーム対応となっています。しかしStep 1の最後でも解説したように、Windows PCとMacでは裏で動いてるアーキテクチャがそれぞれ異なるため、Windows向けに作られている管理ソリューションでMacの管理をすることは非常に難しいのです。
では、JamfがMacを管理する人において最も優れているという理由はどこにあるのでしょうか。
実はAppleのMDMフレームワークが作られるよりずっと前から、JamfはJamf独自のフレームワークJamf Agentを開発し、Macの管理サービスを提供していました。
そのためMacにおいては、AppleのMDMフレームワークと、Jamf独自のフレームワークJamf Agentによってより高度なMacの管理が可能になっています。
右の図はJamf Agentによって可能になる項目です。遠隔でFileVaultというディスク暗号化の強制や、復旧キーの一元管理、ディレクトリへのバインドや各Macのユーザーアカウントを遠隔で作成・管理することも可能です。また特定のAppのプロセスを強制化することもできます。

● 10年連続同日サポートの実績

Jamfの優位性の2つめは同日サポートで、他社に真似のできないJamf Proの大きな特徴です。
Appleは、毎年秋に新OSをリリースしていますが、Appleがリリースする新しいソフトウェアに Jamf Proは10年連続で同日サポートを行いました（2021年現在）。新しいバージョンがリリースされたその日から、新OSのバージョンアップを行っても問題なくJamf Proをご利用いただけます。
「他の業務用アプリから兼ね合いもあり、すぐにバージョンアップをしません」といったご意見もあるかもしれません。しかし、デバイス管理のソリューションが新OSに対応しているかどうかはとても重要なことです。バージョンアップしたいときに「新OSに対応していないから」と、バージョンアップができないといったことはあってはなりません。Jamf Proであれば、切れ目のないデバイス管理を実現できます。



Step 3: 稟議時のカウンタートーク

●「現状維持で良いのでは？」と言われたら

このStepでは、Jamf Proの導入を検討する際に、上長や決済者との間で想定される会話について具体例を挙げて考えてみます。1つめの例題は、「これまで問題なかったし、Macの管理は現状維持で良いのでは？」と、上長から質問された場合です。

「Macにも、会社の機密文書やお客様への提案書など重要なデータが入っていますよね？情報漏洩や紛失時の対策などは強化すべきではないですか？」と、危機管理を仰ぐような質問を投げかけてみてください。あるいは、「MacもWindowsと同じように管理できるMDMがJamf Proです」と答えることもできます。

● 二重管理になると言われたら？

2つ目の例題は、「Windowsの管理もする必要があり、Appleと分けると二重管理になる」と言われた場合です。

「WindowsとMacを1つのMDMで管理できれば理想ですが、一般的にWindows向けに作られている管理ソリューションでは、Macの管理をすることは非常に難しいです」と付け加えた上で、「導入したいJamf Proは、Microsoftともパートナーシップを結んでおり、MicrosoftのMDMと統合管理できるようになっています。OSごとに特化して細かく管理しつつ工数も削減できるようになります」と、返すことができます。

● カウンタートークの裏付けとなる材料

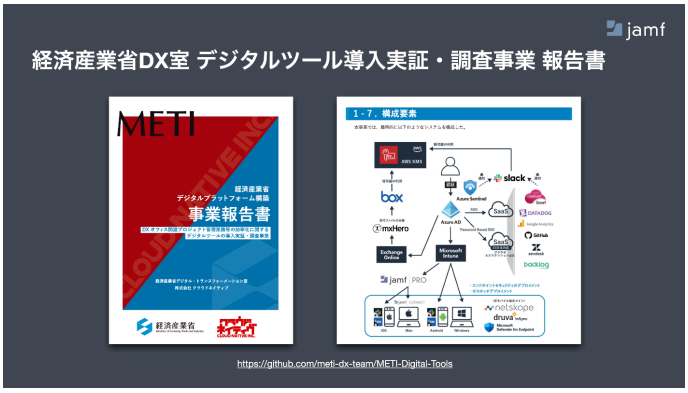
実はMicrosoftでもMacは使われており、その管理にはJamf Proが利用されています。

右図の写真は2018年の弊社ユーザーカンファレンスJamf Nationのものです。登壇いただいたMicrosoftのコーポレートVPのお話は、「『JamfかMicrosoftか？』ではなく、『JamfとMicrosoft』だ。それぞれの強みを合わせて生まれる価値は本物」ということでした。

また2020年のMicrosoft社による開発者向け会議Microsoft Igniteでもライトなの管理にはIntune、複雑な管理にはJamfと提言されました。

さらに、経済産業省がデジタルツールに関する実証実験を行い、その結果をまとめた報告書でも、MacとiOSはJamfで管理しながら、Microsoft Intuneで統合管理することを推奨しています。

MDMはプラットフォームごとに管理することが重要でであることが改めてよくわかります。



● まとめ

本資料では社内のMacを管理する必然性と、そのソリューションとしてのJamf Proをご紹介しました。よりセキュアでリモートワークにも適した、新時代にふさわしいネットワークアクセスの形をご検討いただくとともに、その環境を実現するための資料やカウンタートークをお役立てください。

Webinar Information

本記事は、2021年11月11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11月現在のものです。