jamf

もっとも脆弱なエンドポイント「モバイルデバイス」の管理とセキュアな運用

モバイルデバイスといえば、ノートパソコンやタブレット、スマートフォンを思い浮かべる人が多いのではないでしょうか。いずれもモバイルデバイスのカテゴリーに分類されますが、本資料は主にスマートフォンとタブレットに焦点を当てた内容となっています。これらのデバイスは、世界中の何百万人もの人々にとって、日々の仕事や学習、個人利用に欠かせないツールとなっています。しかし、これらのデバイスへの依存は、モバイルデバイスのセキュリティに対する重大な懸念も同時に引き起こしています。

モバイルエンドポイントのセキュリティおよびコンプライアンスの維持と、快適なユーザエクスペリエンスの両立は不可能ではありません。Mac や Windows PC と同じレベルでモバイルデバイスを効果的かつ効率的に守るには？本資料では、その具体的な方法をご紹介します。

モビリティセキュリティの現状

モバイルデバイスを活用することで、組織は多岐にわたる業務を合理化することができます。使いやすく、持ち運びやすく、どこからでもアプリやリソースにアクセスできるモバイルデバイスは、現場とオフィスをつなぎ、生産性の維持するのに役立ちます。

本資料のトピック：

現場スタッフ（看護師や店員など）向けの共有利用や一人一台利用モデルから、オフィススタッフ向けのCOPE（業務端末の私的利用）またはBYOD（プライベート端末の業務利用）に至るまで、企業はさまざまなモバイルデバイス用途をサポートする必要があります。導入と管理を担当するIT部門は、各モデル特有の要件に基づくカスタマイズされたセキュリティ構成を適用しなければなりません。加えて、デバイスが共有利用のため厳重に管理されているか、あるいは個人所有でプライバシーに配慮して管理されているかに関わらず、ユーザエクスペリエンス全体を向上させることも不可欠です。

一方で、モバイルデバイスの活用と依存度の高まりに伴い、セキュリティに関する懸念は増大しています。企業に影響を与える一般的な懸念には以下のようなものがあります：

- データ漏洩リスクの増大
- 個人情報への不正アクセス
- モバイルデバイスとユーザエクスペリエンス間における均衡の欠如
- コンプライアンスの実施と維持

コンピュータを保護するために設計されたセキュリティポリシーは、モバイルデバイスを十分に保護するようにはできておらず、これによってモバイルデバイスのセキュリティ体制に空いた穴が、組織全体のセキュリティ体制の弱体化につながる可能性があります。もうひとつ考慮すべき重要な点は、複数のプラットフォームをサポートする際に生じる運用の複雑さです。会社支給デバイスのプロビジョニングや、BYODデバイス上の企業データ保護といった対応は、多くの手間と調整を要し、結果としてモバイルデバイスの導入スピードを妨げる要因となり得ます。ユーザのプライバシーや使い勝手の良さに影響を与えることなく、これらの課題を解決する必要があります。

また、組織にBYODプログラムでカバーできないモバイルデバイスの使用を制限するポリシーがあるかどうかも重要です。「自分の組織にはモバイル脅威の影響はない」とお考えであれば、今一度見直す必要があるかもしれません。まずは、自社において、個人所有のモバイルデバイスの業務利用を許可しているかどうかを考えてみてください。

例えば取締役や副社長が通常の業務に使用するモバイルデバイスには、機密データが含まれ、重要なビジネスワークフローが実行されます。これらのデバイスは、組織内のコミュニケーションに活用される一方で、攻撃者のターゲットにもなりやすい傾向があります。一方で、売り場や製造現場のスタッフが携帯するiPadなど、特定の業務用途に対応したデバイスは「現場」での利用を前提としており、コンプライアンスやユーザビリティといった独自の要件を満たす必要があります。

企業におけるモバイル活用の加速

働き方の進化に深く関係する「モバイルを活用した業務スタイル」という従来の枠組みは近年大きな転換期を迎えており、企業には迅速なモデル変革が求められています。この変革が必要となった要因：

- 業務のクラウドサービスへの移行
- 分散型ワークフォースの採用
- 拡大するネイティブモバイルアプリの活用

モバイルビジネスアプリの開発と利用は、変化し続ける職場環境にシームレスに対応しています。また、利便性や柔軟性、業務へのモチベーションアップ効果、そしてコストパフォーマンスの高さにより、モバイルデバイスは欠かせない重要なツールとなっています。

ここでの焦点は、現代のグローバルな職場におけるモバイルデバイスとビジネスアプリケーションの重要性です。

モバイルデバイスによる仕事の効率化：

モバイルデバイスは、あらゆる場所からビジネスアプリやネットワークにアクセスし、よりスマートで効率的な業務を実現するために不可欠です。

モバイルアプリの普及：

モバイルデバイスは重要なワークフローをサポートし、機密データを保持しているため、攻撃の格好の標的となっています。エグゼクティブや現場チームが使用するデバイスは、使いやすさとコンプライアンスを両立させなければなりません。

多様な業務への対応:

モバイルデバイスを使用することで、ユーザは外出先からでもビデオ会議の参加、メッセージの送受信、在庫管理、顧客情報へのアクセス、ドキュメント編集、メール処理などを行うことができ、業務フローの効率化につながります。

モバイルパフォーマンスへの期待：

多くのユーザがデスクトップと並行して、あるいはデスクトップの代わりにモバイルデバイスを利活用しており、モバイルテクノロジーが業務を円滑化、効率化することへの期待が高まっています。

職場のイノベーション推進：

モバイルデバイスは、従業員の満足度や生産性、定着率を向上させるとともに、組織の業務効率化および変化への迅速な対応をサポートし、職場におけるイノベーションを促進します。

モバイルの継続的成長：

StatcounterのGlobalStatsによると、モバイルデバイスの2024年世界市場シェアは62.22%で、デスクトップやタブレットをはるかに上回り、インターネットや仕事関連の使用状況を支配しています。

リモートワークとハイブリッドワーク環境：

リモートワークやハイブリッドワークの実現にはモバイルの導入が不可欠であり、95%の従業員がリモートワークの選択肢を支持しています。モバイルデバイスは、物理的な場所にとらわれることなく、協業と柔軟性を促進します。

世界のモバイルデバイス普及率：

2024年時点で、世界で74億人が携帯電話を所有し、そのうちスマートフォンが71%（約67億契約）を占めており、モバイルの普及は世界的に広がっています。

高まる懸念

ここまで、組織におけるモバイルデバイス採用の急増に関連するセキュリティ上の懸念について触れましたが、ここからは、モバイルデバイスを標的とする脅威と、その使用に関連するリスクについて掘り下げていきます。また、職場におけるモバイルデバイスのセキュアな運用に関する一般的な誤解についても取り上げます。

最初の問題は、これらのデバイスが持ち運び可能であるという性質に起因するもので、以下の理由から攻撃者にとって魅力的な標的となっています。しろ障壁となりました。その背景には以下のような課題があります：

- 多様なモバイルOSの選択肢
- 各OSでサポートされているバージョンの断片化
- さまざまなタイプのOSにおける導入方法の進化
- 異なるサポートを必要とすることから生じるアップグレードの遅れ
- OSバージョンによって異なるビジネスアプリのサポート
- 開発者によって異なるアップデートスケジュールや機能サポート
- オーナーシップモデルによって異なる管理方法（例：BYOD、COPEなど）
- MDMソリューションによって異なる機能サポート（ネイティブおよび非ネイティブのフレームワーク）
- OSタイプによって異なるセキュリティレベル
- コンプライアンス条件を満たすためのポリシーベースの適用の不足

企業におけるモバイルデバイスの導入

従来、多くの組織はビジネスニーズに単一のプラットフォーム（多くの場合はMicrosoft Windows）で対応する傾向にあり、選択したオペレーティングシステム（OS）と互換性のあるコンピュータを導入する必要がありました。さらに、Microsoft社とのエンタープライズ契約により、組織は移行の準備が整うまでWindowsの最新バージョンの導入を遅らせることができ、古いOSバージョンには、組織のニーズに対応するため長期にわたってサポートが継続されるという利点がありました。

しかし、これが問題でした。なぜなら歴史的にコンシューマー向けと考えられてきたモバイルデバイスの世界においては、OSアップデートは利用可能になったらすぐに導入すべきものとして扱われてきたからです。リリース後のアップデートをどの程度の期間内に行うかをユーザ自身が判断できるという点が、企業におけるモバイルデバイス導入においては、む

貴重なデータの宝庫：
モバイルデバイスには、個人やビジネスのデータに加え、PHI（個人健康情報）などに代表される規制対象のプライバシーデータや、さらにはPII（個人を特定できる情報）のような機密データが豊富に含まれています。脅威アクターは様々な目的でこの情報を悪用し、ユーザや組織への攻撃を開始します。そのため、このようなデータに正規のユーザ以外がアクセスできないように、何重もの保護レイヤーで保護することが極めて重要となります。

紛失や盗難の危険性：
モバイルデバイスは携帯性に優れていることから、様々な場所で仕事ができるという利点がある反面、盗難や置き忘れのリスクも高まります。これは脅威アクターにデバイスを盗む機会を与え、データセキュリティに直接的な危険がもたらされます。ほんの一瞬デバイスから目を離し無防備な状態にするだけで、そのデバイスが危険にさらされるほか、将来的な攻撃を受けやすくなる可能性があります。

セキュリティに関する誤解：
多様なセキュリティ対策以上のアクションが必要だと考える人もいます。しかし、急速に進化するモバイル脅威の状況を考えれば、エンドポイントフレームワークに対するネイティブサポートこそ不可欠です。このサポートが欠如しているソリューションを使用する場合、サポートされていない機能や特徴に対して攻撃ベクトルが向くことになりかねません。

過剰な保護 VS 管理不足：適度なバランスを見つけることの重要性

デバイス管理とセキュリティのバランスは、現場の従業員やスタッフをサポートするためにモバイルテクノロジーを最適化する上で非常に重要なコンセプトとなります。ITとセキュリティの優先順位は相容れないように見えますが、現実として、管理とセキュリティのどちらか一方だけに注力するだけでは不十分です。組織は、効率的かつ効果的なモバイルセキュリティソリューションを構築するために、両方の要素をシームレスに統合しなければなりません。

つまり適切なバランスを見つけることがカギなのです。厳格なセキュリティ対策によりデバイスの使用が過度に制限されると、操作性が損なわれ、結果として現場従業員の生産性が低下する懸念があります。一方で、セキュリティをおろそかにすれば、貴重なデータや業務がリスクに晒されます。重要なのは、セキュリティと生産性のいずれかを選択することではなく、両者のバランスを適切に取ることです。そのためには、モバイルデバイス管理とセキュリティ管理を連携させ、組織の資産を保護しながら、現場のチームを効果的にサポートする仕組みが求められます。

問題	過剰な保護	管理不足
パフォーマンスの低下		✓
使いやすさ		✓
シャドーIT（プライバシーへの懸念から従業員が個人所有のデバイスを使用するケース）		✓
企業のセキュリティ対策の回避		✓
モバイルワークスペースの可能性の損失		✓
業界規制要件へのコンプライアンス	✓	
進化するモバイル脅威への対策	✓	
ビジネスデータを個人データとは別の暗号化されたフォルダに分離	✓	
パッチ適用の定期的な実施	✓	
モバイルエンドポイント導入の効率化	✓	
非認可デバイスによる企業リソースへのアクセス阻止	✓	
ビジネスリソースを保護しながらプライバシーも適切に保護		✓

セキュリティ対策を強化しつつ、ユーザーのプライバシーにも配慮したアプローチを採用したいと考える組織は、以下のような戦略を検討することができます。

1. ユーザフレンドリーなセキュリティワークフローの優先的な採用：
使いやすさとシンプルさを考えたセキュリティプロセスの構築は、ユーザだけでなくモバイルデバイスの管理とセキュアな運用を任されている部門にもメリットを提供します。

2. データを中心に据えたセキュリティへのシフト：
デバイスのセキュリティだけに注目するのではなく、データセキュリティの考えを持つことが重要です。デバイスは何かあれば交換できますが、機密データは、一度漏洩・喪失すると回復が困難であり、組織に甚大な影響を及ぼす可能性があります。そのため、確実な保護が求められます。

3. 多様なオーナーシップモデルの受容：
異なるオーナーシップモデルを受け入れ、それぞれのニーズに合ったセキュリティ対策を準備することで、様々なデバイスから企業リソースに安全なアクセスが行われるようになります。特定のオーナーシップモデルのデバイスを無視すると、全体的なセキュリティ戦略に脆弱性が生じます。

4. 包括的なデータ保護：
あらゆる形態のデータを確実に保護することが大切です。これには、ボリュームの暗号化、ビジネスデータと個人データの分離、あらゆるネットワーク接続を介して送信されるデータの保護が含まれます。

5. 最新のモバイル関連技術の導入：
最新のモバイルデバイスのニーズを満たすように設計されたテクノロジーを採用することが重要です。従来型のセキュリティツールでは、新たに出現するモバイル脅威への対応が困難であるケースが多く、結果としてセキュリティ対策が包括的ではなく、断片的なものにとどまりがちです。

6. スプリットトンネルの導入：
効率性はモバイル利用の要です。保護が必要な業務データを安全にルーティングする一方で、個人のデータや通信のようなビジネスに無関係なデータは会社のセキュリティプロトコルをバイパスさせます。このスプリットトンネルアプローチが、BYODデバイスにおけるユーザのプライバシーの尊重とデータセキュリティの維持を両立します。

モバイルデバイスをコンピュータと同様に扱うことの意味

macOSとiOSの統合が進むことは、モバイルとエンドポイントセキュリティの将来にとってどのような意味を持つのでしょうか？

デスクトップコンピュータであるMacとモバイルデバイスを比較することは、リンゴとオレンジを比較するようなものかもしれません。しかしmacOSとiOSがバージョンアップするたびにその距離を縮めているのは紛れもない事実です。新たなバージョンがリリースされるたびに、この2つのOSの統合はますますその重要性を高めていくはずです。

そして、もっとも重要なことは組織がいかにして、この深まる統合を活用できるかということです。この統合がさまざまなデバイスタイプに及ぼす影響には以下のようなものがあります。

- セキュリティギャップの迅速な解消
- 生産性のシームレスな回復
- ユーザエクスペリエンスの向上
- 従業員の信頼の獲得
- インフラ全体で一貫したコンプライアンス
- 組織のポリシーとの深い整合性
- 包括的で多層的なセキュリティプロセス
- 一貫したアプリ管理
- オーナーシップモデルを問わない多層防御戦略
- 柔軟かつ堅牢なセキュリティと管理ソリューションの連携による包括的サポート

モバイルデバイスのコンプライアンス

コンプライアンスは規制のある業界だけのものではありません。コンプライアンスは金融、ヘルスケア、教育といった業界の組織にとって不可欠なものですが、ルールやポリシーに準拠することは、ビジネスの継続に対するリスクを最小限に抑えながら特有のニーズを満たしたいと考えるその他の組織にとっても非常に重要です。このことから、Macの場合と同様に、組織全体を対象としたモバイルポリシーの適用は、デバイス全体に対する包括的なセキュリティ戦略を構築する上で重要な役割を果たします。

例えば、ハイブリッドワークやリモートワークの普及によりモバイルデバイスの盗難、紛失、悪用のリスクが高まり、機密データが危険に晒されている事実を例にとってみましょう。この場合IT部門は、MDMワークフローを活用してセキュリティ構成をすべてのデバイスに導入することで、暗号化ポリシーや安全な認証プロトコルを適用させることができます。さらに、リモートワイプ機能により、必要に応じて侵害を受けたデバイスからデータを安全に消去することもできます。

組織は、あらゆるユースケースにおいて、モバイルユーザのためのコンプライアンスプランを策定することが可能です。

このアプローチは、固有のリスクに対処すると同時に、基盤となる堅牢なベースラインを提供してくれます。これは、カリフォルニア州消費者プライバシー法（CCPA）のような規制にすでに準拠している**成熟したウェブサイトとはまったく異なる新しく設計されたモバイルアプリケーション**など、新たな枠組みに関連するリスクを軽減する上で特にメリットがあります。

さらに、コンプライアンスには、深刻な脆弱性や規則違反に発展する前に問題を特定し、それに対処することも含まれます。この場合、セキュリティ（監視）と管理（徹底）の組み合わせが連携して脅威を検出・対処し、モバイルデバイスがコンプライアンスを維持できるようにします。

モバイルデバイスの汎用性により、ユーザが誤って業務用の承認済みアプリをプライベートで使用したり、反対に承認されていないアプリを業務関連のタスクに使用したりしてしまう可能性があります。どちらのケースも、データの混在、プライバシーの侵害、データ漏洩、もしくは規制違反など、組織にリスクを及ぼす可能性を含んでいます。

モバイルコンプライアンスを他のエンドポイントと同等に扱うことで、組織は、企業リソースにアクセスするすべてのエンドポイントが最新の脅威に対して同レベルの保護を受けていることを確認し、デバイスのインベントリ、使用状況、発行デバイス、企業データへの従業員アクセス、導入されたセキュリティ対策の正確な記録を維持することができます。

モバイルデバイスのコンプライアンスについて考えるべき最後の事項は、ユーザの継続的なセキュリティトレーニングです。これは、しばしば見落とされがちな点ですが、**セキュリティのベストプラクティス**や、セキュリティを脅かす脅威に遭遇した際に従うべき手順やワークフローに関する知識をユーザに授けるという意味で、包括的なモバイルセキュリティ計画において非常に重要です。このようなトレーニングは重要なセーフガードとして機能し、管理およびセキュリティ対策を補完する重要な役割を果たします。

要するに、サイバーセキュリティはIT部門や企業だけの責任ではなく、すべての社員一人ひとりの責任でもあります。

モバイルデバイスの管理とセキュリティを一体化させるためのポイント

ここまでの内容を一言でまとめると、「セキュリティの要は、デバイス群全体に対する管理とセキュリティの統合にある」ということになります。

1. コンバージェンス：
モバイル中心の現代の職場において、デバイス管理とセキュリティが堅牢なセキュリティプロトコールとシームレスに一体化することを指します。

2. 課題の克服：
モバイルセキュリティの問題を解決するには、従来のように複数のツールを積み重ねる断片的なアプローチではなく、一つの包括的なソリューションが必要です。複数のツールを組み合わせても、単独のいずれのツールも十分に効果を発揮できていないのが現状です。

3. 一貫性：
一貫性を確保するためには、異なるデバイスのセキュリティベースラインを確認し、エンドポイントに問題があることを示す変化がないか、またはセキュリティ脅威、脆弱性、異常の有無について調査が必要かどうかを、積極的に監視する必要があります。

4. 使いやすさ：
ユーザエクスペリエンスを優先しつつ、保護とのバランスを取ることは、包括的な戦略にとって不可欠であり、IT部門、セキュリティ部門、エンドユーザにとっての有効性とシンプルさの微妙なバランスを達成するために非常に重要になります。

5. 対応：
すべてのデバイスタイプ、異なるプラットフォーム、そしてインフラ全体において、適切な優先順位付けや調査、解決に重点をおいてセキュリティ脅威に迅速に対応することが重要です。

6. バランス：
適切なバランスを実現するためには、ユーザーエクスペリエンスを損なわずにセキュリティを確保すること、そして安全性とユーザ満足度をシームレスに両立させる可能性を常に意識することが重要です。

Jamfでは、すべてのデバイスが妥協のない保護を得られる未来を目指しています。バランスの取れた包括的なデータおよびプライバシー保護を、インフラ内のすべてのデバイスに拡大することこそがJamfの目指す最終的なゴールです。

組織のセキュリティニーズやエンドポイントの管理・保護方法について見直しをご検討の際は、ぜひJamfまでご相談ください

jamf

www.jamf.com/ja/

トライアルに申し込む
または、販売代理店までお問い合わせください。