エンドポイント管理の評価ガイド：

従来のソリューションが現代の課題に対応できない理由

はじめに

今日の職場ではモバイルデバイスの普及に加えて勤務場所の分散も進み、これまでにない柔軟性が求められています。

貴社の業務形態がリモート・ハイブリッド・オフィス勤務のいずれであっても、モバイルデバイスなしでビジネスを進めることは考えられません。スマートフォンやタブレットなどのモバイルエンドポイントはさまざまな業界で不可欠な存在となっており、業務の効率を高め、リアルタイムにデータへアクセスし、ほぼあらゆる場所から働くために使われています。

モバイルデバイスの導入が加速している今、もはや「そのデバイスが企業のものかどうか」は問題ではありません。重要なのは、「当初の想定範囲を越えてデバイスを効果的に管理・保護できるかどうか」です。

医療、金融、建設、輸送など、さまざまな業界でモバイルデバイスはビジネスに必須のツールへと進化していますが、一方で、この進化によって複雑な問題も生じています。IT部門は、一貫性のないデバイス環境を管理し、所有モデルが混在する中でもコンプライアンスに準拠し、生産性向上とセキュリティおよびユーザのプライバシーを両立するよう求められています。しかも、こうした課題への対処と並行して、モバイルテクノロジーおよびITプロセスをビジネスの目標および成果へと結びつけなければなりません。

本書では、企業のモバイル管理とセキュリティで起きている重大な変化を明らかにし、現代のビジネス環境が抱えるニーズに従来のツールや「画一的な」アプローチでは対応できない理由を解説します。また、「モダンワークフローをサポート」、「エンドユーザの生産性を高める」、「IT部門がモバイルデバイスの活用を戦略的優先事項と連動させるために必要な制御と可視性を確保できる」という3点を網羅している、スケーラブルで統合されたソリューションの重要性をご紹介します。

もしも貴社でモバイルデバイス中心のハイブリッド環境に対応していないツールを利用しているのであれば、本ガイドは、それらのツールを今後も利用してよいのか、それとも体制を再考すべきなのか検討する一助となるでしょう。

勤務環境の境界の消失

業務がフルリモート体制であっても、オフィス復帰が求められていても、つまりはどこにいても、日常生活のあるゆるシーンでモバイルデバイスが使われているという事実は否定できないでしょう。実際、その普及度合いの高さからビジネスの現場でもモバイルデバイスの導入が進んでおり、機能性、性能、携帯性、効率性の高さも相まって多くの業界でメインのデバイスになった結果、個人利用と業務利用との線引きが薄れつつあります。

継続的なビジネス運営における モバイルデバイスの重要性

Verizon社の2024年版Mobile Security Indexの調査結果：

「調査参加者の80%は、自社の円滑な運営にはモバイルデバイスが欠かせないと回答しました」

このようにモバイルデバイスが継続的な事業運営や製品/サービスの提供に不可欠なツールとなる中、企業はこれらデバイスをただ管理し保護するだけでなく、ビジネス目標と密接に結びつけて、そのコンプライアンスを維持し、自社やユーザのニーズの変化に漏れなく対応し、日進月歩の脅威から保護することが求められています。

職務や業務体制の変化

近年では、多くの業界の企業がモバイルデバイスの導入を進め、このデバイスなしでは実現不可能な手段により事業を推進し、収益を拡大しています。
以下に、こうした業界および職務の具体例と、各業界でモバイルデバイスの導入により効率向上を実現する方法を紹介します。

航空業界

モバイルデバイスの導入により、搭乗ゲートからコックピットに至るまで**リアルタイムのデータアクセスとコミュニケーションを可能**にし、航空機のメンテナンス、フライト業務、乗客向けサービスのすべてを効率化できます。またパイロットの観点では、従来のフライトバッグの電子化により、地図やフライトマニュアル、ハンドブックなどの約18kgにも及ぶ資料類をわずか約2kgのiPad 1台に収め、業務効率とコンプライアンスの向上を実現することができます。

建設業界

タブレットやスマートフォンの導入は、デジタル文書化を促進します。また、現場内外で利用できるプロジェクト管理ツールへのアクセスを通じて共同作業の体制を向上させ、**プロジェクトの監督体制を強化により遅延を削減**します。特にiPadを活用すると、作業員は関係者やサプライヤーと絶えず意思疎通を図りながら、設計図にアクセスでき、監督者はその場で書類処理や文書への署名を行うことを可能にします。

金融業界

スマートフォンを導入し複数の暗号化通信プラットフォームを活用することで、顧客サービスを強化し、生産性を高め、コンプライアンス遵守を促進できます。アナリストなどの金融分野の専門家は、適切な権限のもとでクライアントデータに安全にアクセスできると同時に、いつでも市場の動向をモニタリングすることができます。同様に、ブローカーは、管理対象iPhoneを利用してどこからでも安全に取引を行い、**顧客一人ひとりに合わせてそのニーズに最適なサポートを提供**できます。

宿泊・サービス業界

スマートフォンやタブレットの導入により、スタッフは常時インターネットに接続可能なモバイルデバイスシステムを使って、**お客様ひとり一人に合わせたサービス**を提供できます。そのことにより、お客様の満足度と業務効率を同時に向上させることができます。また、キオスクモードで運用されるiPadは、お客様セルフチェックインの選択肢を提供し、到着後すぐにくつろぎの体験を楽しむことができます。さらに、管理対象iPadを客室に配置すれば、客室のマネジメントを簡素化しながら、宿泊客に専用のアプリで詳細な情報やルームサービスをすぐに提供できます。

小売業界

モバイルデバイスの導入は、実店舗とオンラインストアの両方において、取引のスピードを高め、顧客エンゲージメントを向上させ、そして**より柔軟で迅速なオペレーションを実現**し、小売業者とお客様の双方にメリットをもたらします。従来のPOS（販売時点情報管理）システムをモバイルシステムに移行すれば、販売スタッフは売り場でお客様対応を行いながら、その場を離れることなく在庫管理を容易に行うことができます。さらにこの方式なら、iPhoneまたはiPadから必要なすべての情報を一目で確認し、顧客データの更新やモバイル決済による支払い処理も行えます。

企業が直面している課題

単一の管理ソリューションで均一なデバイス群を一括管理するという従来の手法は、モバイルファーストを推進する現代の企業環境にはもはや適していません。従業員の利用するモバイルデバイスが多様化し、所有モデルやオペレーティングシステム（OS）も複数にわたっている今、IT部門には社内の連携を図り、コンプライアンスを確保しながら、分断の進んだ環境でも生産性を支援することが強く求められています。しかも、エンドポイントの多様化と並行して脅威も進化しているので、現在運用しているソリューションでビジネスの成果を維持しながら、ますます複雑化する要件に対応できるのか（あるいは適応できるのか）を組織として見極める必要があります。

汎用型ソリューションの限界

これまで、IT部門の活動における考えは「社内全体でOSが同じデバイス1種を管理するなら、管理ソリューションは1つで足りる」というものでした。管理対象デバイスの台数が100台、1,000台、あるいは1万台を超えたとしても、この考えには確かな理屈があり、種類が均一のエンドポイントを管理および保護できていたわけです。

とは言え、今やモバイルデバイスというカテゴリだけを見ても、そこに含まれるデバイスの種類は以下のように多種多様です。

- スマートフォン
- タブレット
- ノートパソコン
- ウェアラブルデバイス
- IoTデバイス
- 電子書籍リーダー
- 携帯ゲーム機
- デジタルカメラ

モバイルデバイスの種類がこれほど多種多様であり、また世界の一人当たり**平均デバイス所有数**が3.6台に及んでいることを踏まえ、過去の企業環境と比較してみましょう。その違いは現代のコンピューティング環境とはほとんど共通点がないことがおわかりいただけるでしょう。そして、それは現代の脅威の状況も同様です。

「調査参加者の85%は、過去1年間にモバイルデバイスを狙った脅威のリスクが増加したと回答しています」

– Verizon社の2024年版Mobile Security Index

このように考えると、1つの疑問が生じます。貴社の管理・セキュリティソリューションは現在でもビジネス目標との整合性があり、コンプライアンス要件に準拠し、生産性向上のニーズに対応できているでしょうか？

所有モデルの多様化に伴うコンプライアンスの課題

前セクションで提示した質問についての答えを出す前に、所有モデルの多様化が企業におけるモバイルデバイスの活用法に与えた影響を考えないわけにはいかないでしょう。

このセクションでは特に、業務に使用するモバイルデバイスについて企業所有のものと個人所有のものが混在する状況下で**社内のセキュリティの同等性をどのように確保するか**という点を扱います。以下のようにサポート対象が拡大するため、事態は複雑化します。

- デバイスの種類の多様化（ノートパソコン、スマートフォン、タブレット、ウェアラブルデバイス）
- メーカーの多様化（Apple、Microsoft、Samsungなど）
- OSプラットフォームの多様化（Apple、Android、ChromeOS、Windows）
- ソフトウェアバージョンの混在（アプリとOS）
- 勤務場所の分散（オフィス回帰、リモートワーク、ハイブリッドワーク）

このように現代の企業はいわばデバイス、所有モデル、運用環境のるつぼと化しており、ニーズや要件について数え切れないほどの形で影響が生じていることは間違いありません。このような変化により、IT部門には次のような課題が生じています。まず、デバイスの所有状況にかかわらず、エンドユーザの生産性維持のためにエンドポイントから業務用リソースへアクセスできる環境を整える必要があります。次に、モバイルデバイスを活用する従業員の生産性が社内全体で包括的に保護されていなければなりません。重要なビジネスツールであるモバイルデバイスが、ビジネス目標に沿った方法で使用され、組織のニーズに合わせて成長やスケーラビリティを促進する形で業務を支援することが求められます。

「重要インフラ関わる調査回答者の87%は、モバイルデバイスやIoTデバイスの関わるセキュリティ侵害を受けると、自社のビジネスに大きな影響が生じると考えています」

– Verizon社の2024年版Mobile Security Index

課題の解決策

従来のツールはその設計上、今日のようなモバイルファースト型のハイブリッド環境には対応できません。そのため、IT部門では管理を安全かつ効率的に一括で行える統合型ソリューションを導入する必要があります。最新の統合型管理ソリューションなら、簡単な手順でゼロタッチ導入を展開し、パッチ適用を自動化し、複数プラットフォームにわたってコンプライアンスベースラインを適用して、目的のビジネス成果を達成できます。それと同時に、IDプロバイダとの緊密な連携を通じてゼロトラストアーキテクチャを展開し、あらゆるネットワーク接続からのアクセスを保護できます。また、脅威検出機能とリアルタイムのエンドポイント監視機能により、インシデント対応も強化されます。CISベンチマークへのサポートを組み合わせることで、IT部門はすべてのデバイスの種類や、所有モデル、作業環境において、生産性とパフォーマンスを維持しながら、継続的に監査を行い、コンプライアンスを証明することが可能になります。

専門的なプロセスとビジネス目標の調整

IT部門は、企業の成功に欠かせない存在です。その使命を達成するには、従来の実績あるデバイス管理戦略の枠を超え、モバイルデバイス、分散化した勤務環境、高度なセキュリティ上の脅威のすべてに対応することが求められます。

さらに、企業が競争力を維持するには、IT部門が主要なビジネス目標に方針を合わせて以下の面で直接的な貢献を行うことも必要です。

1. 戦略的成長
2. 業務効率
3. 長期的レジリエンス

これに加え、ユーザエクスペリエンスを損なわずにアジリティを強化し、生産性向上を促進し、リスク対策を講じて、企業活動を支援することも不可欠です。

基幹産業において、モバイルデバイスの多様化に対応した管理ソリューションをビジネス戦略に合わせた形で運用できれば、次の事例に示すような目覚ましい成果を期待できるでしょう。

製造業界

iPadを製造現場に導入すれば、サプライチェーンのデータへリアルタイムにアクセスし、業務工程をデジタル化できます。IDCの調査では、**DX（デジタルトランスフォーメーション）テクノロジーに投資**した組織の85%は、「従業員エクスペリエンスの向上」と「従業員エンゲージメントの向上」の相互作用が、より良い顧客体験、顧客満足度の向上、そして組織の収益増加につながる」という相関関係が示されています。

医療業界

医療従事者にiPadおよびiPhoneを支給すれば、電子個人健康情報（PHI）や遠隔医療ツールへ安全かつ即座にアクセスできるようになります。米国立衛生研究所（NIH）による論文「**Smartphone and Mobile App Use Among Physicians in Clinical Practice（臨床業務における医師のスマートフォンおよびモバイルアプリの活用状況）**」によると、調査対象の研究10件のうち70%がモバイルアプリを活用し、臨床判断の支援のために根拠に基づく医療（EBM）へのアクセス環境を整えて、患者転帰を改善するとともに医療サービスを効率化したとされています。

政府機関

iPhoneは、安全なリモートアクセスを機関のリソースに提供すると同時に、現場でのデータ収集をサポートします。Verizon社の**「2024 Data Breach Investigations Report（2024年版データ漏洩/侵害調査報告書）」**では、紛失や盗難に遭ったモバイルデバイスの90%以上に「データ漏えいが確認された」と報告されています。このため、拡張可能で包括的なセキュリティは、増加するデバイス群や高度化するポリシーに対応しつつ、一貫性のある総合的対策を維持することが求められます。

業務用モバイルデバイスのサポートの最適化

IT部門で個人所有から企業所有のデバイスまでを一括でサポートし、コンプライアンスを確保しユーザのプライバシーを守るには、最新のモバイルデバイス戦略が不可欠です。複数プラットフォームに対応したセキュリティ戦略なら、複数種のデバイスを同等に保護しコンプライアンスを確保すると同時に、共有デバイスの再構成を効率化してリスクを軽減し稼働時間を強化して、デスクレスワーカーの生産性を高められます。またこの方式では業務効率の向上とセキュリティ対策の一貫性が両立されるので、IT部門は変化する自社や従業員のニーズの変化に合わせてモバイルデバイス管理を調整できます。

所有モデルサポートの拡張性

現代の企業が個人所有デバイスと企業所有デバイスをまとめてサポートしようとすると、拡張性の面で課題が生じます。IT部門が以下の課題を解決するため、**さまざまな登録モデルのサポート機能**などを備えた専用ソリューションが欠かせません。

- 複雑さの軽減
- 組織全体へのセキュリティの展開
- 業務用データと個人データの分離
- コンプライアンスの遵守
- ユーザプライバシーへの配慮

セキュリティ対策とプライバシー保護を両立する鍵は、**業務用データを保護しながら社内リソースへのネットワーク接続は暗号化**し、かつ業務に関係ないトラフィックは個人所有デバイス上のインターネットへと直接ルーティングする機能です。このような機能があれば、所有モデルが混在する環境でも一貫性のあるデバイスセキュリティ体制を確立し、一括でポリシーを適用できます。

複数プラットフォームにわたって同等なエンドポイントセキュリティ

所有モデルの混在によりIT部門に生じる課題に加え、現代の企業の業務環境ではほとんどの場合、関係者が iOS/iPadOS もWindowsもAndroidも使うというように、異なる種類のOSが混在しているものです。このような複雑な環境にデバイスの多さも相まって、さまざまな変動要因が生じるため、リスク対策の難度上昇を止める術はほぼありません。

そのため、多層防御戦略と以下のような適切な対策を組み合わせることが推奨されます。

- 高度なテレメトリ
- 挙動に基づく脅威検出
- 統合アクセスポリシー

そのうえでクロスプラットフォームサポートも導入すれば、**プラットフォームに関係なく**、あらゆるモバイルエンドポイントをデバイス上およびネットワーク内で一貫して保護できます。また、このクロスプラットフォームサポートがあれば、IT部門は分断の解消と同時に、**業務用モバイルデバイス全体にわたり強固なセキュリティ基準を確保**できます。

共有デバイスとデスクレスワーカー

デバイスの共有やユーザの複数存在する環境が一般的な業界では、ユーザセッションの切り替えに伴うダウンタイムを短縮することが重要です。これは、ダウンタイムの理由が以下のいずれであっても関係ありません。

- 繁忙期に顧客対応用のiPhoneを素早く設定
- iPhoneをフライトクルーに支給し機内での飲食物の購入を効率化
- アプリを特定用途に制限したiPadの構成を迅速に変更して医療を支援

一刻一秒を争うような業務環境では、**ユーザがIT部門の介入なしで役割をすぐ切り替えられる**ようにしたり、**デバイスをワイプ・監視できるようにしてデバイスの再構成を簡素化する**ことで、人命を救う場合があります。専用のソリューションがあれば、共有デバイスのセキュリティを確保しながらユーザ切り替えの準備を行い、サポート要請を減らして全体的な業務効率を改善できます。

業務工程の刷新による生産性の向上

モバイルデバイス管理を効率化することで、企業全体のIT業務の最適化とユーザの生産性向上につながります。ID管理ツールやセキュリティツールとのシームレスな統合があれば、プロビジョニング、コンプライアンスレポート、アクセス制御を迅速化できます。展開の自動化機能には設定時間だけでなく手作業によるミスも減らす効果があり、Self Service を使うと重要なアプリやリソースにオンデマンドでアクセス可能な環境を整えられます。このようにして業務工程を刷新し効率を高めることで、ダウンタイムを最小化するだけでなく、IT部門がスキル強化にかける時間を増やし、ビジネス目標に役立つプロセスを開発できるようになります。

既存ツールとのシームレスな統合

「これ1つですべてを解決できる」というようなソリューションは存在しません。

したがって、**モバイルデバイスを管理しセキュアに運用するには、統合機能が重要です**。統合機能があれば、以下を実現できるからです。

- 総体的なサービスへの拡大
- 包括的なセキュリティ層の増設
- 既存のツールをベースとしてビジネスを拡張
- コンプライアンス要件に合わせたワークフローのカスタマイズ

例えば、**IDプロバイダ（Microsoft Entra IDやOkta）との統合機能**を使用すると、アクセス制御を一元化し、条件付きアクセスポリシーを展開して、認証ワークフローにフィッシング対策となる多要素認証（MFA）を追加することができます。このような保護すべきリソースへ不正にアクセスされるリスクの軽減は、セキュリティプラットフォームとの統合がIT部門にもたらすメリットの一例に過ぎず、他にも次のような活用例があります。

- デバイスのオンボーディングの効率化
- プロビジョニングの高速化
- コンプライアンスレポートの簡素化
- テクノロジースタック間の相互作用の促進
- 業務工程との連携

デバイスの導入とプロビジョニングを自動化

企業のニーズによっては、手作業によるモバイルデバイスのオンボーディングに1台あたり30分以上もかかる場合があり、結果として生産性の低下やIT部門の負担増加を招いています。

しかし、**ゼロタッチ導入によるモバイルデバイス導入の自動化**とApple Business Manager（ABM）を組み合わせれば、導入を効率化してプロビジョニングにかかる時間を大幅に削減し、実質的にダウンタイムも短縮できます。この方式では**IT部門の業務効率を高める**だけでなく、企業全体で以下のメリットも得られます。

- 手作業によるセットアップをなくし、ヒューマンエラーのリスクを減らす
- アプリのインストールや構成も含めたオンボーディングを高速化する
- 全デバイスを導入初日からセキュリティとコンプライアンス基準に準拠させる
- アクティベート後直ちにユーザに必要なリソースを提供しすぐに作業を開始できるようにする

ユーザが必要なリソースへ必要なときにアクセスできる環境を構築

IT関連のサポート要請への**適切な対応時間**は、一般的に24時間（1営業日）とされています。しかし、業務を遂行するうえで必要なアプリや構成のリクエストが関係者から上がった場合、対応が1分遅れるたびにその分だけ生産性が低下し、企業の業務、ひいては収益に影響を及ぼしかねません。

Self Serviceは、関係者に以下へのアクセス権を付与することで、ユーザの業務を支援します。

- 利用可能な承認済みアプリカタログ
- 業務用リソースとサービス
- セキュアな構成や設定

サポートチケットを提出する必要はありません！

ユーザは生産性向上に必要なリソースに安全にアクセスできる一方で、IT部門は可能な範囲を管理できるため、サポート業務のボリュームを減らしつつ、関係者が自信を持って行動できる環境を提供します。

包括的なセキュリティ戦略の導入

企業が多様化したモバイルデバイス環境全体にわたって現代の脅威へ効果的に対処するには、セキュリティ対策を進化させ、対象を拡大することが求められます。パッチ管理を自動化すると、IT部門の負担を減らしながらデバイスおよびアプリを常に最新の状態に保ち、脆弱性を最小化できます。高度な脅威検出でリスクを特定し軽減するには、リアルタイムの分析、緊密な統合、対策の多層化が必要です。
デバイスの健全性とユーザアイデンティティをベースにしたゼロトラスト戦略であれば、勤務場所やプラットフォーム、所有モデルを問わずリソースへのアクセスを保護できます。

パッチ管理の自動化

企業のサイバーセキュリティ計画において、ヒューマンエラーは唯一防ぐことが可能な脅威です。この領域に該当するものとしてソフトウェアのアップデート遅れがあり、モバイルデバイスに脆弱性をもたらし、組織のコンプライアンス目標を損なう原因となります。ただし、よい面もあります。この種の脅威は、**OSとアプリ両方のパッチ管理の自動化**を導入すれば以下を通じて軽減できるのです。

- リアルタイムのモニタリングとアラート
- 統合ログの能動的なレビュー
- **スマートグループ**の活用
- 動的ポリシーの適用
- **Appインストーラ**ワークフロー
- アプリの最小バージョンの指定

IT部門で自動化機能を利用すれば、手作業を減らしながらデバイスを常に最新の状態に保ち、社内および法規制の要件を遵守できます。しかも、ユーザへの影響やダウンタイムも最小限に抑えられます。

脅威の検出と防御

Kasperskyによれば、サイバー攻撃の件数は2020年をピークに減少傾向にあるものの、2023年の第1四半期から第4四半期にかけて**モバイルデバイス狙いの攻撃は147%増加**しています。モバイルデバイス狙いの脅威は巧妙化しており、従来のマルウェア対策ツールの機能を回避する動きも頻繁に認められています。そのため、効果的なモバイルセキュリティには、既知の脅威を防御するだけでなく、デバイス上およびネットワーク内の挙動分析でリアルタイムに高度な脅威を検出することも求められます。デバイス管理とID管理、セキュリティを緊密に統合することで、IT部門は以下のメリットを得られます。

- モバイルデバイスのアクティビティを詳細に可視化
- リスクポスチャをリアルタイムに評価
- 複数のプラットフォーム、所有モデル、業務環境にわたりインシデント対応の時間を短縮

所有形態と作業環境

- サードパーティのSIEMとシームレスに統合
- デバイスのパフォーマンスを下げることなく包括的な多層対策を展開

ゼロトラストネットワークアクセス（ZTNA）

業務環境もデバイスの活用法も進化している今、企業で現代のモバイルデバイスを管理および保護するにあたり、このような時代を想定していない従来ツールで十分でしょうか？

答えは「ノー」です。

クラウドコンピューティングへの移行や業務環境のハイブリッド化、モバイルデバイスの導入を受け、コンプライアンスを維持するにはユーザアイデンティティとデバイス健全性に基づいたアクセス制御が欠かせません。現代の業務環境の境界が消えつつある企業においてこれを実現するには、以下の対策が必要です。

- **従来のVPNを暗号化されたマイクロトンネルに置き換え、ネットワークトラフィックを分離する**
- **条件付きアクセスポリシーを適用し、アクセスの許可対象を認証済みユーザおよび検証済みデバイスに限定する**
- **管理およびセキュリティソリューションとID管理をシームレスに統合する**
- **ゼロトラスト戦略を策定し、従業員の勤務場所、使用デバイス、所有モデルにかかわらず社内全体にわたり業務用リソースを保護する**

企業全体にわたるコンプライアンスの標準化と準拠

有効なコンプライアンス体制を築く第一歩は、業界標準に基づいたセキュリティベースラインを導入し、すべてのモバイルデバイスについて運用開始初日から該当するポリシーに準拠させることです。エンドポイントの健全性をアクティブに監視することで、リアルタイムでの可視化とAIによるリスク検出が可能になり、IT部門はコンプライアンスの確保と脅威への迅速な対応を実現できます。最後に、CISなどのベンチマークに従ってコンプライアンス体制を検証することで、遵守状況を監査、是正、報告します。

ベースラインを導入しセキュリティ体制を強化

コンプライアンス体制の構築には技術的な対策とポリシーが不可欠ですが、それぞれの業界固有のコンプライアンスと要件対応を始めるには何を手がかりとすればよいのでしょうか。答えは、業界で認められている基準やフレームワークに基づいたベースラインです。

構成のベースラインを確立すれば、企業所有か個人所有かを問わずあらゆるエンドポイントについて、**MDMへのモバイルデバイスの登録後すぐに該当のセキュリティ要件に準拠した状態**を確保できます。これは基礎的かつ重要なステップであり、多層防御型セキュリティ戦略を策定・実施するうえで不可欠です。これにより、IT部門では次のことが可能になります。

- **ターゲット指定のスマートグループに構成プロファイルを体系的に展開し、コンプライアンスを確保**
- **一貫性のあるプロビジョニングを自動で行い、社内全体の構成ドリフトを軽減**
- **データセキュリティに合わせてモバイルデバイスのプロセスを調整し、事業継続性を向上**
- **組織固有のニーズと業界規制に合わせてセキュリティ戦略をカスタマイズ**

エンドポイントの健全性を常に監視

ベースラインを実装した後の次の重要なステップは、モバイルデバイス全体を継続的に監視することです。非準拠のエンドポイントを検出した際に迅速なインシデント対応を行うためにも、各デバイスの健全性ステータスを常に可視化し、継続的なコンプライアンスを維持することが不可欠です。デバイス管理、ID管理、セキュリティの緊密な統合機能があれば、IT担当者間のサイロ化を解消し、**AIにより組織のセキュリティ体制を強化**できるほか、以下の対策も実現できます。

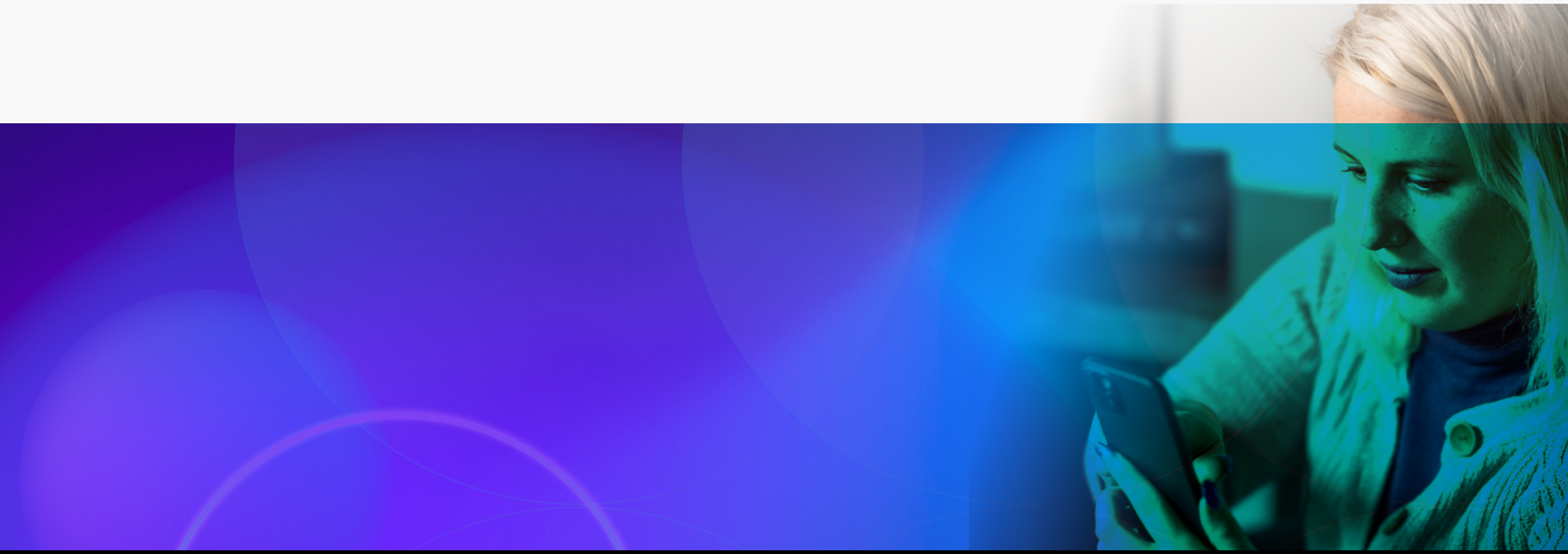
- **リアルタイムのテレメトリとインサイトでエンドポイントの挙動を把握**
- 機械学習（ML）でリスクを検出し、修復作業を高速化
- 巧妙化した**モバイルエンドポイントを狙った脅威を予防的に検出**し、分析して対応

ベンチマークに基づいてコンプライアンスを検証・強制

3つ目の重要なステップは、強制・レビュー・改善の間のギャップを埋めることで、モバイルデバイスのコンプライアンスライフサイクルを完結させます。これにより、組織がコンプライアンスを継続的に監査できる手段が提供されます。このステップには、**規制の厳しい業界で義務づけられているコンプライアンスに関する証拠の提示**をスムーズにする効果もあります。

最新の管理ソリューションなら、CIS レベル1 / レベル2 など業界標準のベンチマークに照らしてコンプライアンスを検証するために必要なツールも標準で配備し、以下の形で社内のガバナンスと規制対応を強化できます。

- IT部門が、企業固有のニーズに応じてベンチマークを柔軟に調整
- ベースライン測定を自動化**して、ベンチマークからの逸脱を自動で修復**
- PDF、HTML、Adoc形式の監査レビュー用ガイダンスをワンクリックで作成



優先すべきは手頃さよりもセキュリティ：実際のデータ

ツールを手頃さやコストの安さで選ぶと、多くの場合セキュリティに穴が生じ、長期的なリスクが増加して業務停止に至ります。デバイスの種類ごとにセキュリティ対策の強度が異なっていると、全体的なセキュリティ体制が弱体化し、攻撃者の付け入る隙が生まれてしまいます。サイバーインシデントはセキュリティだけの問題ではなく、デバイスのパフォーマンスや生産性を低下させ、事業運営を阻害します。こうした落とし穴を避けるポイントは、IT部門は所有モデルやOSにかかわらず、あらゆるエンドポイントを保護するソリューションを優先的に導入し、有効性、レジリエンス、効率、組織の健全性を確保することです。

コスト優先で「手頃さ」を選ぶと、「安全性」にコストをかけた場合よりも高くつく

企業でモバイルデバイスの管理・保護ソリューションを検討する場合、コストが主な要因となります。既存のソリューションの維持や「オールマイティ」ソリューションの導入を選んだ場合、初期のセットアップに掛かる時間や初期費用は削減できるかもしれません。しかし、こうしたツールの多くは利便性や料金の面で優れているものの、それと引き換えに包括的なモバイルセキュリティを備えていません。

残念ながら、セキュリティ体制に穴があると、侵害を受けて多大な損害を被る可能性があります。IBMの「2025年データ侵害のコストに関する調査」レポートによれば、**データ侵害による平均被害額は世界全体で444万ドル**、米国では1,022万ドルにも上ります。

その一方で、IBMの同レポートにおけるコスト分析では、「セキュリティ部門にAIと自動化を導入する」と、デバイス管理、ID管理、セキュリティの基本的なサポートのみのソリューションを選んだ場合に比べて、190万ドルに及ぶコストを節約し、さらに侵害対応にかかる時間を80日も短縮し、侵害による平均被害額も抑えられると示されています。

ポイント：企業のサイバーセキュリティへの投資は本質的に業務、社会的評価、規制コンプライアンスとつながっており、これらがさまざまな形で自社の収益を高めてくれます。

セキュリティ対策のバラつきは組織全体のセキュリティ体制に悪影響

モバイルデバイス向けセキュリティの機能がプラットフォーム非依存型ではなくプラットフォーム依存型であると、企業のセキュリティ体制に不均衡が生じてしまいます。

端的に言うと、一部のモバイルデバイスは、他のデバイスが持つ保護機能を欠いています。

Infosecurity Magazineによる最近の調査に関する記事では、回答者の41%がデータ損失の主な原因として機密データが保存されたデバイスの盗難を挙げおり、脆弱な認証情報とその窃盗（36%）およびランサムウェア攻撃（32%）を上回っていました。このような盗難の発端は、サポート対象プラットフォームによって管理体制にズレがあったこと、ひいては全体的なレジリエンスの根底を揺るがすようなセキュリティギャップには対策できていると誤って認識されていたことでした。

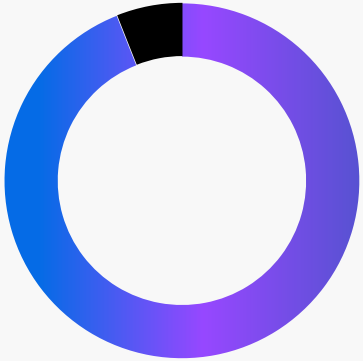
ポイント：社内インフラにアクセスするデバイスはすべて企業にとってのリスクになる（またリスクを招く可能性がある）ので、デバイスの種類やOS、所有者を問わずあらゆるエンドポイントに企業のセキュリティを適用する必要があります。リスクはリスク以外の何者でもありません。

デバイスのパフォーマンスと従業員の生産性に対する影響

サイバーインシデントがもたらす被害は、先述の財政面に留まりません。デバイスおよび組織のセキュリティ体制に害があるのはもちろんですが、パフォーマンスやユーザの生産性にも悪影響をもたらし、その結果、事業運営が繰り返し阻害されてしまいます。

複数環境（パブリッククラウドとプライベートクラウドの混在環境やオンプレミス環境）にまたがるデータ侵害の封じ込めについて、前ページで紹介したIBMのレポートによれば、データ侵害の平均特定時間（MTTI）は207日に及んでいます。侵害の平均封じ込め時間（MTTC）でさらに70日を要しているため、複数環境におけるデータ侵害の特定から封じ込めにかかる平均期間は276日となります。このデータから、財政面の費用と、デバイスおよび社内システムの侵害によるパフォーマンス低下の機会費用とのギャップが見えてきます。

前者は従業員に直接的および間接的な影響をもたらしますが、特定の脅威や攻撃による影響の方がユーザの生産性により大きな影響を及ぼす可能性があるのです。たとえば、ランサムウェア攻撃を例にとってみましょう。**Help Net Security**が長期的なネットワークおよびビジネスの中断がもたらす影響をまとめた記事では、次のように述べられています。



「ランサムウェア攻撃の被害者の94%は、長期にわたり業務が中断され、生産性が低下しました。このうち40%は、一定期間にわたり業務が完全に停止し、生産性も失われたと回答しています」

ポイント：サイバー攻撃は財政面の直接的な被害だけでなく、事業機会の喪失や生産性、社会的な信頼、市場価値の低下をはじめとしてさまざまな影響をもたらし、多くの場合、侵害を封じ込めた後も影響が残ります。

本ガイドのポイント

1.

モバイルデバイスは業務に不可欠：

モバイルデバイスはさまざまな業界で必須のツールとなっており、リモート・ハイブリッド・オンサイトの全環境でリアルタイムのコミュニケーションを実現し、業務工程の柔軟性や事業継続性を高めるために使われています。

2.

従来のツールでは不十分：

現代では企業のモバイルデバイス運用は複雑化し、所有モデルやOSも多様化しているため、従来のオールマイティ型管理ソリューションでは均一なセキュリティ体制を確保できません。

3.

セキュリティには包括性が求められる：

現代の企業では、リアルタイムの脅威検出や条件付きアクセスポリシー、自動パッチ管理などが揃った複数プラットフォーム対応のID統合型セキュリティ戦略を導入する必要があります。

4.

コンプライアンスは絶対条件：

効果的なモバイル管理を実行することで、セキュアなベースラインを展開し、エンドポイントの健全性を監視し、業界ベンチマークの準拠状況を検証して、監査に対応可能なコンプライアンス体制を整えられます。

5.

鍵は拡張性と自動化：

専用のソリューションなら、導入を効率化し、プロビジョニングを簡素化し、手作業を削減して、業務環境が分散した環境でもIT部門が社内全体を支援できます。

6.

ユーザエクスペリエンスの重要性：

従業員にセルフサービスツールを提供し、業務用リソースに一貫してアクセス可能な環境を整えることで、生産性向上、プライバシーとセキュリティの確保、IT部門の負担軽減をすべて実現できます。

7.

社内の連携で事業価値を推進：

モバイルデバイス管理を戦略目標に連携させると、業務効率を高めながら成長を促進し、IT部門にイノベーションの推進役を任せられます。

まとめ

現在では生産性向上を目的としてモバイルデバイスの導入が進み、オフィス内・オフィス外を問わず業務を行うことが可能です。ビジネス成果の創出はもはや一過性のものではなく、現代の企業を特徴づける要素となっています。

デバイスの種類や所有モデルの多様化、複数OSのサポートにより複雑さが高まる中、従来の管理ツールでは、現代の企業が抱えているセキュリティ、コンプライアンス、ユーザエクスペリエンスに関する最も基本的な要件にさえ対応が難しくなっています。

IT部門がデバイスの管理だけを任される時代は終わりました。

今やIT部門には、ビジネス目標を支援するため、テクノロジーや管理プロセスの足並みをビジネス戦略と揃えることが求められています。また、重要な資産を保護すると同時に、従業員が最も仕事のしやすい好みのデバイスとOSを使用し、どこからでもシームレスにアクセスできる環境を構築することも重要です。

1. **危険の度合いは高まっています**
2. **リスクは高まっています**
3. **そして、ミスの許容度は狭まっています**

最新のエンドポイント管理ソリューションは、本書で述べたようなニーズの高度化に対応できるよう設計され、ゼロタッチ導入や高度な脅威検出からクロスプラットフォームサポート、ゼロトラストセキュリティまで備えています。IT部門は専用のツールを活用し、セキュリティ、効率、生産性を損なうことなくモバイルデバイスを利用した業務を一括で保護、最適化できます。

これらを踏まえ、本書で提示した疑問の答えを考えてみてください。貴社が現在利用している管理ソリューションで、社内やIT部門、従業員のニーズの高度化に対応できているでしょうか？

このようなニーズへの対応は、ビジネスの成否を左右します。自信を持って「イエス」と言えない場合は、今こそアプローチを考え直す時です。

トライアルに申し込む