ivanti

Everywhere Workplace (場所にとらわれない働き方) のための統合エンドポイント管理

目次

はじめに

モバイルデバイスとITの普及は、企業の生活様式として既に定着しました。端的に言えば：今日のユーザーは、デスクトップやラップトップPCからタブレットやスマートフォンに至るまで様々なデバイスを使用して、いつでも、どこからでも、作業を行えることを期待しています。このことは、「Everywhere Workplace（場所にとらわれない働き方）」において、より一層重要になっています。かつて、最も「大事な」仕事はラップトップやデスクトップPCで行い、モバイルデバイスは外出先や自宅でメールやその他の限られた用途にのみ使用していました。今日のユーザーは、同じ情報にアクセスし、同じアプリケーションとサービスの多くを実行し、会社所有であるかBYODであるかにかかわらず、あらゆるデバイスで同じ仕事の多くを成し遂げることを期待しています。PCの開発動向は、PCとモバイルデバイスの境界線を曖昧にしつつあります。

このようなモバイルデバイスの普及は、企業にとって大きな課題となっていますが、同時に明確なチャンスでもあります。まず、課題ですが、IT部門は、ユーザーの生産性、好みのモバイルワークスタイル、デバイスの個人的な使用方法を損なうことなく、各デバイスからアクセスされ、保存される機密アプリケーションと情報を管理し、保護するポリシーを導入する必要があります。しかし、多くの企業において、エンドポイント管理とセキュリティは、デバイスの進化に追いついていないのが現状です。

行動を起こさないことによるリスク？ IT部門は、脅威やデータ侵害のリスクにさらされています。コンテキスト（従業員、デバイスと場所、ゼロトラストおよびパーソナライズされた従業員体験）がなければ、IT部門は、従業員の生産性に影響を与えるリスクを回避するために、ロックダウン状態にすることを余儀なくされます。

IT部門は、従業員ごとにセキュリティポリシーを自動的に調整し、プロアクティブにネットワークを監視して、IT担当者にアラートを通知できるソリューションを必要としています。

データ漏洩時代におけるデバイス管理

多くの企業では、デスクトップやラップトップ用の管理システムまたは管理システムのセットと、スマートフォンやタブレットなどのモバイルデバイス用の全く別の管理システム、ベンダー、戦略というアプローチになっています。多くのケースでは、異なる管理ツールを使用している場合、モバイルデバイスと従来のエンドポイントシステムに焦点を当てた2つの異なるITポジションが存在することになります。

この方法には重大な欠点があり、特にデータ漏洩がますます頻発し、被害が大きくなっている現代では、その欠点が顕著になっています。モバイル機器は紛失や盗難に遭いやすく、モバイル機器とそのアプリケーション、データが危険にさらされる可能性があります。モバイル端末のマルウェアは、企業ネットワークへの侵入口となる可能性が高まっています。紛失、盗難、マルウェアのほかにも、デバイスごとに2つの異なる管理システムを導入することには、重大な課題と影響があります。

一般的なエンドユーザー体験

管理用のアプリケーションや戦略が分かれているため、ユーザーが期待するような共通のユーザーエクスペリエンスをデバイス間で提供することが困難になっています。複数のデバイスのオンボーディング、プロビジョニング、サポートは、不必要に複雑になり、時間がかかる場合があります。

> クラウドからエッジまで、すべての従業員のデバイスを検出・管理し、コンテキストに基づく自動化で信頼性の高いアクセスを実現し、従業員が働く場所を問わずパーソナライズされた体験を提供するソリューションで、あらゆる場所での働ける環境を実現します。その結果、業務スピード、コスト、サービス品質が向上し、生産性が向上します

一般的なユーザーポリシー

企業の機密情報やネットワークへのアクセスを保護するためには、ユーザーアクセスやセキュリティに関するポリシーを厳格に策定する必要があります。モバイルデバイスの普及と高度化に伴い、IT部門は、各従業員が使用するすべてのエンドポイントシステムに共通のアイデンティティとアクセスポリシー、およびポリシーの枠組みを作成し、展開することが課題となっています。2つの完全に分離した管理システムを使用する場合、共通のポリシーセットを導入することはより複雑になります。よりシンプルなアプローチとして、単一の統合エンドポイント管理（UEM）ソリューションを使用することが挙げられます。これは、複数のチームが関与することによる「複雑さ」を軽減することにもつながります。

かつて多くの企業では、デスクトップやラップトップはIT部門が担当し、スマートフォンは総務部門が担当することが一般的でした。そのため、両者のスキルや優先順位、役割は異なっていました。

このような仕組みには、ポリシーの作成と展開において目に見えないギャップがあり、ハッカーに侵入されたり、データが侵害されたりする可能性がありました。さらに、一見同じように見えるポリシーを2つの異なる管理プラットフォームに依存することは、時にそれらが異なる形で展開され、隠れたギャップにつながる可能性があることを意味します。

統一されたUEMシステムは、単一のユーザーアクセスおよびセキュリティポリシーセットを作成し、すべてのユーザーデバイスに一貫性と流動性をもって展開することができます。

管理コストとリソース

ベンダー、サポート契約、インターフェースが異なる2つの別々の管理プラットフォームで作業する場合、単一のプラットフォームを使用するよりも多くの時間、トレーニング、およびリソースが必要になります。これは、オンボーディング、サポートコスト、およびリソース要件が大きくなるだけでなく、ユーザーのステータスやアクセス権を変更する場合には2つの別々のシステムで規定を変更しなければいけなくなるのでリソースを大量に消費し、単一の管理システムを使用する場合よりもエラーが発生しやすくなります。

デバイス管理に費やす時間とリソースが増えるということは、ビジネスを強化するテクノロジー戦略に割く時間とリソースが減るということでもあります。テクノロジーの変化のスピードが速く、この変化がビジネス競争力に果たす役割がますます重要になっている現在、IT部門は日々の管理業務にできるだけ時間をかけないようにすることができれば、それに越したことはないのです。

統合管理

エンタープライズモビリティ管理（EMM）プラットフォームが企業内で目立つようになるにつれ、ベンダーは既存のデスクトップやラップトップのエンドポイント管理プラットフォームとの統合を謳うようにになりました。これは良い傾向ですが、まったく異なるシステム間の統合を想定しても、単一の UEM システム、インターフェース、ベンダーとの関係と同等のコスト削減や使いやすさを実現することはできません。UEM の焦点は、モバイルと従来のシステムやデバイスを人為的に分離するのではなく、各ユーザーのすべてのデバイスに対して一貫したポリシーとサポートリソースを展開することにあります。このようなシステムは、すべてのデバイスで次のような機能を提供する必要があります。

デバイスの検出とインベントリ、デバイスのプロビジョニング（OSの展開/デバイスの登録）、ソフトウェア/モバイルアプリの配布、サポート、リモート制御など、すべてのユーザーデバイスのエンドポイント管理

パッチ管理、エンドポイントセキュリティ、ソフトウェアの配布、アップデート、アイデンティティとアクセスポリシーの実施により、より強固な運用セキュリティを実現するセキュリティ・エンフォースメントを提供します。モバイルデバイスの場合、紛失や盗難の疑いがある場合のリモートロックやワイプは重要な機能です。

ソフトウェアのライセンス、契約、保証、リース契約の追跡を支援する資産管理

プロビジョニング（新しいデバイスやデバイスイメージのユーザーオンボーディングとオフボーディングを含む）。ユーザーのセルフ・プロビジョニングは、多くの MDM ソリューションで提供されている機能であり、包括的なエンドポイント管理ソリューションでも同様に提供されるべきものです。

理想的には、これらのアプリケーションとデータのセキュリティ機能をすべて同じUEMシステムに緊密に統合して、ユーザーのラップトップ、PC、モバイルデバイス、アプリケーション、および情報の管理をすべて単一の画面と一貫したエンタープライズポリシーセットで実現し、1人の担当者がすべてを管理できるようにすることです。

Ivantiのソリューション

Ivanti のユーザーデバイス管理ソリューションは、従来のデスクトップやラップトップシステムとモバイルデバイスとの間の人為的な分離を排除します。Ivantiは、統合エンドポイント管理に焦点を当てており、各企業のユーザーが使用するすべてのデバイスをライフサイクル全体を管理するための単一のエンタープライズ IT 管理ソリューションとポリシーセットを提供します。UEMでは、デバイスではなく、ユーザーに焦点が当てられています。このユーザー中心のアプローチにより、Ivantiは、すべてのデバイスでユーザーが期待するシームレスな体験を提供する唯一の包括的な管理ソリューションを提供します。Ivanti の業界をリードする Endpoint Manager の機能は以下のとおりです。

検出およびインベントリ情報
Ivantiは、OSに関係なく、ネットワークに接続されているすべての管理対象および管理対象外のPC、ラップトップ、スマートフォン、タブレット、およびその他のモバイルデバイスを自動的に検出し、インベントリを作成します。Ivanti Cloud Services Applianceを使用すれば、IT部門は、遠隔地にあるデバイスを検出してインベントリを作成し、VPNを必要とせずに低帯域幅の接続でデバイスを管理することもできます。

OSの導入と配布
Ivanti は、関連するすべてのユーザー システムにおける Windows および macOS オペレーティング システムのインストールと移行を簡素化および自動化し、ユーザー、アプリケーション、設定、ファイルを保持して、新規または既存のマシンに復元できるようにします。

ソフトウェアの配布
Ivantiは、WindowsからMac、iOSおよびAndroid対応のモバイルデバイスに至るまで、すべてのデバイスへのソフトウェア配布を自動化します。特許取得済みのエンタープライズ配布技術は、帯域幅の消費を最小限に抑えながら、大規模なソフトウェアパッケージを、僅か数分間のうちに何千個ものデバイスへの配布を可能にします。

シンプルなユーザーベースの管理
ユーザーが携帯するすべてのデバイスに対して、単一のユーザー構成とセキュリティポリシーを実装できます。この機能を使用すると、1つのポリシー展開で、新しい従業員のデバイスを数分で接続してプロビジョニングできます。

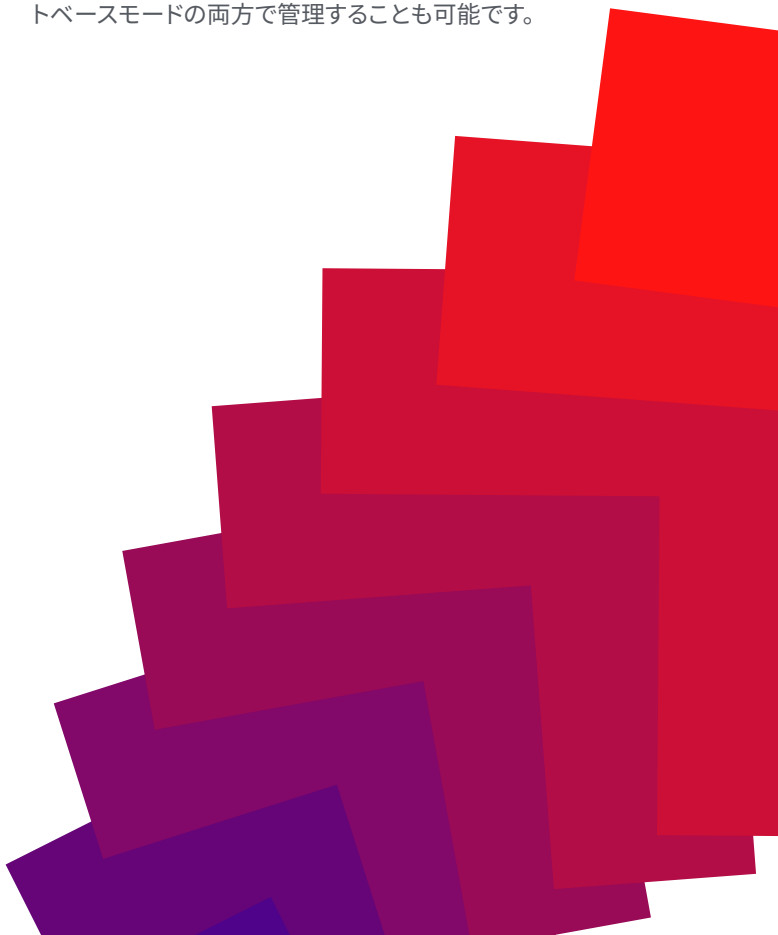
ソフトウェアライセンス管理
これらのツールは、自動化されたソフトウェアライセンスの監査と監視を行い、組織が実際に必要なものだけを購入できるようにし、ベンダーライセンス契約の再交渉に役立つ詳細情報を提供して、コストをコントロールします。ソフトウェアライセンス管理を賢く利用することで、企業は数千ドルから数十万ドルのコスト削減を実現することができます。

システムダッシュボードとレポーティング
システムダッシュボードとレポートは、PC、Mac、スマートフォン、タブレットを含むすべてのシステムがどのように動作しているかを把握を支援します。Xtractionは、CIO、部門長、ITディレクターに、ITの価値と意思決定を示すビジネスプレゼンテーション用のビジュアルグラフやチャートをタイムリーに提供することができます。さらに、ROIベネフィットレポートのためのツールも提供します。また、Ivanti には包括的な閾値監視とアラートツールが含まれているため、IT 部門は問題がビジネスに影響を与える前に対処することができます。

Ivantiのリモートコントロールと問題解決
IT部門は、サポートに関する問題を解決するためにデバイスをコントロールし、可能な限りシステム間でファイルを転送することができます。

権限管理
ネットワーク全体に権限管理ポリシーを作成して展開します。

包括的なエンタープライズモビリティ管理
これには、モバイルアプリケーション管理、モバイルデバイス管理、およびリモートデバイスの検索、ロック、ワイプなどのモバイルセキュリティ管理機能が含まれます。この機能は、デスクトップ、ラップトップ、ハイブリッドデバイスを、MDMモードまたはすべての管理アクションを可能にする完全なエージェントベースモードの両方で管理することも可能です。



ivanti

役割に応じた業務

ユーザーは、サービスデスクやセキュリティアップデートを含むすべてのITサービスに、すべてのデバイスでアクセスすることができます。

オプションのモジュールは、Endpoint Managerと緊密に連携し、資産管理、ソフトウェアとハードウェアのライフサイクル管理、サービス管理、ユーザーの生産性と組織の効率性を維持するためのプロセスを提供します。

Ivanti UEMは、ユーザーが使用する全てのデバイスをサポートし、ユーザーとIT部門の両方の生産性を向上させます。企業のIT部門は、デバイスとアプリの管理に対する統一されたIvantiアプローチを採用することによって、エンドポイント管理のコストとリソース要件を削減し、エンドポイントセキュリティのギャップを埋め、シームレスなユーザー体験を提供するソリューションを手に入れることができます。

ユーザー中心のIT活用

かつて、PCとラップトップは、モバイルデバイスとは異なる世界に存在し、その機能も異なっていました。当時は、それぞれに別の管理システムを開発し、展開することに一定の論理がありました。今日のEverywhere Workplace（場所にとらわれない働き方）では、ユーザーは仕事を遂行するためにすべてのデバイスに依存しています。このような環境では、2つの別々の管理システムを持つことは、ユーザーとIT部門の双方に不必要な負担を生じさせることになります。

Ivanti の統合エンドポイント管理は、セキュリティと管理をユーザに集中させることで、この負担を解消し、統合管理だけでなく、いつでも、どこでも、あらゆるデバイスで一貫したユーザ体験を提供します。

ivanti.co.jp
+81 (0)3-6432-4180
contact@ivanti.co.jp