IDC MarketScape

IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Devices 2024 Vendor Assessment (Japanese)

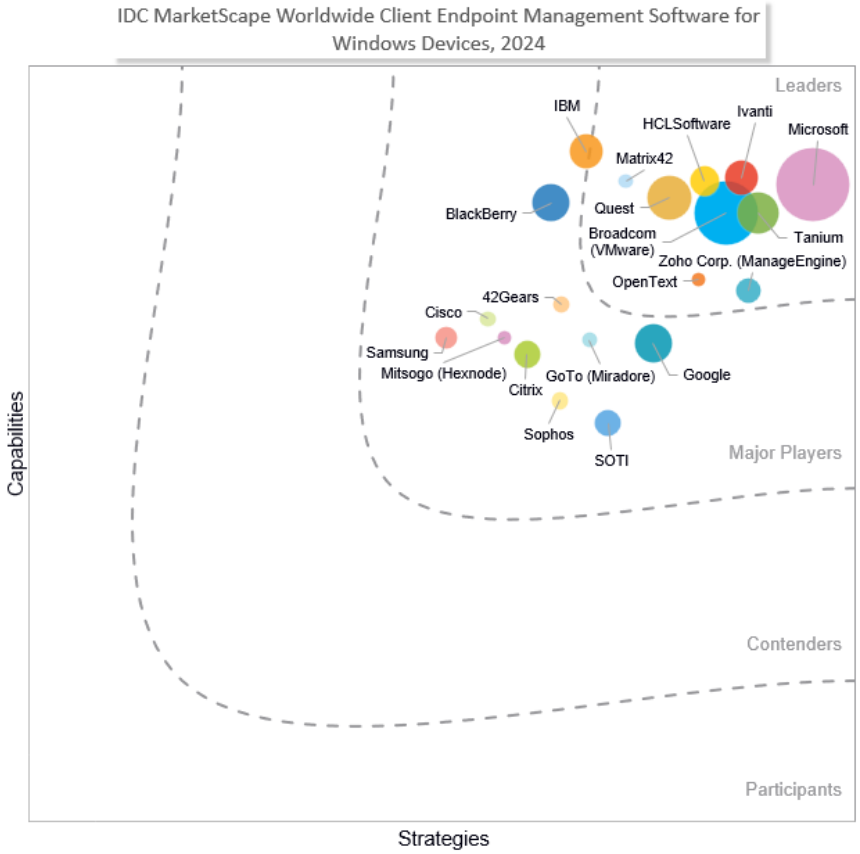
Phil Hochmuth

THIS IDC MARKETSCAPE EXCERPT FEATURES TANIUM

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Client Endpoint Management Software for Windows Devices Vendor Assessment



Source: IDC, 2024

調査方法、市場定義、ベンダーの評価基準については、「補遺」セクションを参照のこと。

April 2024, IDC #US51234324e_JP

調査概要

本 IDC MarketScape Excerpt は、『*IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Devices 2024 Vendor Assessment*（IDC #US51234324）』からの抜粋である。本調査レポートには、Figure 1 に加え、「IDC の見解」「IDC MarketScape 評価対象ベンダー選定基準」「IT バイヤーへの提言」「ベンダープロフィール（要約）」「補遺」「参考資料」のセクションの内容、またはその一部が含まれる。

IDC の見解

企業はエンドポイントデバイスの組み合せを多様化し、モバイル、IoT（Internet of Things）、および耐久性の高いタイプのデバイス導入を進めているが、エンドユーザーコンピューティング（EUC：End-User Computing）オペレーティングシステム（OS：Operating Systems）の主流は依然として Microsoft Windows である。IDC の調査データサービス「*Worldwide Personal Computing Device Tracker*」では、2024 年第 1 四半期に出荷された業務用 PC とラップトップ PC の 80%は Windows デバイスであった。

Windows の脆弱性と広範なアタックサーフェス（攻撃対象領域）に対処するため、PC エンドポイントセキュリティソフトウェアは 100 億ドル規模の市場となっている。Windows デバイスのクライアントエンドポイント管理（CEM：Client Endpoint Management）においては、セキュリティ、コンプライアンス、ポリシーの施行、およびソフトウェアパッチの適用が重要となる。マイクロソフト自身も、OS とアプリケーションのセキュリティを強化し、重要なソフトウェア更新を効率化するなど、Windows の安全性を確保するために多くの対策を講じている。しかし、依然として Windows エンドポイントは、個人情報窃盗、マルウェア投入、ランサムウェア、その他のサイバー犯罪行為の主な標的とされている。

コンプライアンス、異常なアクティビティの検知、悪意あるコードの検出、機密データの検出など、現行のエンドポイントテクノロジーの機能および運用は、エンドポイントのセキュリティ保護に不可欠である。そのため、組織の Windows エンドポイントフリート全体でこれらを実行するための、エコシステム全体と複数のテクノロジー市場が存在する。ただし、多くの場合セキュリティ対策は、エンドポイントデバイスの OS とアプリケーションのウイルス対策を徹底することが出発点となる。Windows デバイスを、デバイスのファームウェア、OS、およびアプリケーションの最新ソフトウェアバージョンに確実にアップデートすることは、セキュリティの課題に先んじて対策を講じる上で非常に重要である。CEM ツールは、セキュリティとコンプライアンスを確保するだけでなく、従業員のための生産的なエンドユーザーコンピューティング環境の構築と、効率的なプロビジョニングを可能にするものでなければならない。そのために不可欠な Windows CEM ツールの製品機能、および戦略的取り組みを以下にいくつか挙げる。

- **Windows のプロビジョニングと管理の多様なモデルのサポート**：エージェントベースの Windows 管理は、デバイスのセットアップ用の PC イメージングと同様に、依然として標準である。しかし、常時ハイブリッド／リモートで働くワーカーの増加、オフサイト／オフネットワーク接続、あらゆるもののクラウドベース化（アプリケーションやデータなど）といったことの進展を考えると、最新のデバイス管理と Windows の Over The Air（OTA）技術／クラウドプロビジョニングが、ワーカーにとってより重要になっている。
- **強力なセキュリティ機能**：ポリシーの適用、OS の状態と構成の制御、OS／アプリケーションのパッチと脆弱性アップデートの継続的な監視と適用は、あらゆる Windows CEM ツールに欠かせない機能である。
- **統合と有効化**：通常、業務用 Windows デバイスには、クライアント側のエージェント、プロセス、およびサービスが多数実行されている。Windows CEM ツールは、適切なソフトウェアがインストールされ正しく設定されていること、そして、このツール自体がデバイスのパフォーマンスやワーカーの生産性を妨げないようにするものでなければならない。

- **アナリティクス、従業員デジタルエクスペリエンス（DEX：Digital Employee Experience）および AI**：Windows CEM ツールは、高度なエンドポイントテレメトリーの収集や、エンドユーザーエクスペリエンスに照らしたエンドポイントテレメトリーの測定と分析など、新しい機能領域へと進化していかねばならない。脆弱性のクエリー、IT ワークフローの自動化とスクリプト作成、プロアクティブで予防的なエンドユーザーサポートといった特定のユースケースのために、どのベンダーもそのロードマップに AI を組み込むべきである。

IDC MarketScape のベンダー選定基準

IDC は、以下の重要な基準を満たすベンダーに、本評価に参加してもらった。

- Microsoft Windows 10/11 エンドポイントを実行するデバイスを管理できる CEM ソフトウェア製品を有するベンダー。
- 2023 年（暦年）の統合エンドポイント管理（UEM：Unified Endpoint Management）製品の推定売上高が 500 万ドル以上のベンダー。なお、収益は 2024 年 2 月に推定されたものであり、今後発表される市場シェアに関する調査レポートとは異なる場合がある。

IT バイヤーへの提言

Windows 用 CEM ツールのバイヤーは、以下のような属性、機能、および関連するユースケースシナリオのサポートに着目してベンダーを検討すべきである。

- エンドユーザーアナリティクスと従業員デジタルエクスペリエンスは、Windows クライアント管理プラットフォームの未来の姿であると言える。ワーカーのデバイスを包括的に把握できる UEM プラットフォームは、エンドユーザーのデジタルエクスペリエンスの状態に関して利用可能なデータを大量に収集して分析し、その結果に基づく対応を可能にする。場所、時間帯、ネットワークの種類などに基づく従業員の行動、デバイスとアプリケーションの健全性、使用パターンといった情報はすべて、従業員が業務用として与えられたデバイスやアプリケーションでどのように仕事をしているかをより深く理解する上で重要である。UEM ツールは、データの収集、分析、レポート作成に関する機能の提供において最前線に位置づけられ、UEM テクノロジーが先導する、より大きな DEX イニシアティブの一部である。
- モダンなマネジメントは、Windows デバイス管理の未来の姿であると言える。企業の PC 管理は、モバイルデバイス管理（MDM：Mobile Device Management）プロトコルという単一のプロトコルコンセプトに収斂しつつある。OS ベンダーとデバイス OEM は MDM プロトコルを実装しているが、中心となる前提と最終目標は同じである。つまり、エンドポイント全体における、ロケーションに依存しないエージェントレスなプロビジョニングとコンフィギュレーション、およびライフサイクル管理である。エージェントベースのデバイス管理は、多くの Windows 管理シナリオでは依然として必要であるが、Windows CEM ツールのバイヤーは、Microsoft Autopilot のような Windows の自動プロビジョニング技術と同様に、MDM プロトコルのサポートという原則を遵守し、そのサポートモデルの開発に重点を置いたベンダーに注目すべきである。
- 条件付きアクセス制御とポリシーの適用は最低限必要なものである。これは UEM プラットフォームに欠かせない機能になりつつある。条件付きアクセス制御（ユーザーがどのようなアプリケーションやデータに、またはその他のリソースに接続して利用できるか）は、ロケーション（GPS による位置情報やネットワークのコネクティビティのタイプ）、特定の日（週の特定の曜日など）、エンドユーザーの ID と役割、ならびに使用されているデバイスの状態または健全性（ジェイルブレイクされた、あるいは root 化されたデバイスであるか、または、サポートが終了した OS であるかという観点から、デバイスの状態または健全性が判断される）などの多数の要素に基づいている。

- フロントラインワーカー、マルチユーザーエンドポイント、フィールドワーカー、デスクレスワーカーなど、特殊用途の Windows デバイスのシナリオを考慮すべきである。Windows エンドポイントは、一般的なエンドユーザーコンピューティングや生産性アプリケーションに留まらず、幅広い役割を担っている。Windows 11 PC は、小売業向け POS（Point of Sale）端末、デジタルサイネージ、産業用制御監視ツール、セルフサービスキオスク、ATM（現金自動預払機）などのさまざまなユースケースで利用されている。CEM ツールは、従来とは異なる広範なユースケース（基本的なモバイルコンピューティングだけでなく、音声／ビデオ通話／会議、電子メール、カレンダー、メッセージング、生産性ツールなど）のデバイス管理をサポートする機能を備えたものでなければならない。
- 補完的な IT／システムインフラストラクチャソフトウェア製品の強力なポートフォリオへの近接性と関連性に着目すべきである。エンドポイントセキュリティ、セキュリティと脆弱性の管理、ID、クラウドアクセスセキュリティブローカー（CASB：Cloud Access Security Broker)、IT サービスマネジメント（ITSM：IT Service Management)、セキュリティ情報とイベント管理（SIEM：Security Information and Event Management)、ネットワークセキュリティ、Windows サーバー管理、LOB（Line of Business）／業界特化型（Vertical-Specific）アプリケーションプラットフォームなどのソリューションはどれも、Windows CEM ベンダーを検討する際の重要な着眼点である。Windows CEM ソフトウェアは単独で動作するわけではないため、ベンダーの市場参入において重要となるのは、補完的な IT ソフトウェア製品ポートフォリオを備えること、または、業界の主要プレイヤーとの強力な統合や協力関係を構築することである。

ベンダープロフィール（要約）

本セクションでは、IDC MarketScape におけるベンダーのポジションを判断する上で決め手となった、ベンダーに対する IDC の主要な見解について簡潔に記述する。各ベンダーの評価基準は別表にまとめており、ここでは各ベンダーの長所と課題の概要を説明している。

Tanium

Tanium は、2024 年の IDC MarketScape で、Windows デバイス向けのクライアントエンドポイント管理ソフトウェアの世界的リーダー（Leader）企業として位置づけられている。

2007 年創業の Tanium は、米国ワシントン州カークランドを拠点とするエンドポイントセキュリティ管理ベンダーである。同社の「コンバージド・エンドポイント管理（XEM：Converged Endpoint Management）プラットフォーム」は、大中規模の企業環境におけるエンドポイントの管理とセキュリティに重点を置く。Tanium XEM プラットフォームは、多様なエンドポイント（Windows、Mac、Linux デバイスなど）のリアルタイムの可視化、制御、修復機能を提供する。Tanium のエンドポイント管理アプローチは、他の IT 運用ツールやセキュリティツールと統合することで、リスク管理とコンプライアンス管理の統一された戦略を推進する。Tanium のリニアチェーンクライアントアーキテクチャとリアルタイムデータ処理機能は、Windows デバイスの詳細な可視化と制御を可能にする。XEM プラットフォームの効率的なパッチ管理システムは、組織が高いパッチ効果を達成し、Windows デバイスフリート全体でエンドポイントの攻撃対象領域を削減することを支援する。デバイスのインベントリー作成、設定状態、インストール済みアプリケーションの監視、ユーザーアカウント管理、その他のテレメトリー収集機能を、単一のコンソールから実行できる。同製品はまた、Tanium のインシデント対応、リスクとコンプライアンス、および従業員デジタルエクスペリエンス製品とも密接に連動している（Tanium はこれらをまとめて「コンバージド・エンドポイント管理スイート（Converged Endpoint Management suite）」と呼ぶ）。

DEX の面では、Tanium 製品に備わった広範なテレメトリー収集機能と分析機能は、Windows デバイスのエンドユーザーエクスペリエンスの監視に役立つ（デバイスハードウェア、Windows OS、アプリケーションのパフォーマンス、応答性、ユーザーフィードバック、健全性などの監視）。これらの機能はまた、ユーザーの Windows PC の効率的な運用に影響を与え得る他の評価項目の監

視もサポートする。Tanium のエージェントベースの製品セットは、オンプレミスとクラウドの両方で利用できる。

強み

Tanium の XEM プラットフォームは、リアルタイムの脆弱性管理、機密データの監視、すべてのエンドポイントへのセキュリティポリシーの適用において優れている。この緊密に統合された管理／セキュリティアプローチは、リスク軽減と運用効率を重視しつつ、Windows の大規模デプロイメントをサポートしている現代の企業の方向性と一致している。同社製品の機能は、Windows サーバー、Mac、Linux、一部の UNIX クライアントおよびサーバーのエンドポイントにも拡張できる。

Tanium 製品の監視機能は、Windows エンドポイント全体の機密データの検出と保護（事前に機密データとして識別され構造化されたファイルデータ、および機密データタイプの識別）にまで拡張でき、コンプライアンスの強化とエンドポイントのセキュリティポスチャの改善につながる。

課題

XEM の包括的な機能は、IT リソースが限られている小規模企業や SMB（Small and Medium-sized Business：中堅中小企業）にとって、導入が困難となる可能性がある。XEM を既存の IT エコシステムに統合するには、IT 担当者のトレーニングに時間を費やす必要があるかもしれない。また、プラットフォームのメリットを最大限に引き出すには、Tanium の複数のモジュールが必要になる場合がある。

Tanium のデバイス展開モデルでは、最新のデバイス管理アプローチよりも、従来のイメージングとパッケージングに重点が置かれている。同社は、Microsoft Autopilot などのサービスとの将来的な連携を見据えており、これは最新デバイスのオンボーディング、および最新の管理方法への移行を支援することになるであろう。

Tanium を検討すべき場合

Windows デバイスを大規模に導入している組織や、大規模に分散した拠点に従業員を抱える企業は、Windows エンドポイントデバイス管理とエンドポイントセキュリティ全体を強力に統合している Tanium の採用を検討すべきである。エンドポイントデバイス管理とセキュリティ運用の統合による、サイバーハイジーン（衛生管理）の改善、リスク低減、コスト削減に取り組むチームを有する現代の企業にとって、Tanium は特に魅力あるパートナーとなるであろう。

注目すべきベンダー

IDC MarketScape のサイクルでは、毎回調査の対象からは除外されるベンダーが出てくる。多くの場合、それらのベンダーはライフサイクルの初期段階にあるか、製品の移行中であるか、もしくは、単に規模が小さすぎるかのいずれかである。本 IDC MarketScape では、注目すべきベンダーとして、以下のベンダーを紹介する。

- **1E**：ロンドンを拠点とするソフトウェアプロバイダーである 1E は、既存の Windows エンドポイントデバイス管理ツールのサポートと拡張、またはそれらのツールの置き換えに重点を置いた IT インフラストラクチャと CEM 製品を開発している。このベンダーはまた、DEX ソリューションやその他の従業員エクスペリエンスツールも有している。
- **baramundi software**：ドイツを拠点とする UEM ベンダー。エンドポイントデバイス管理の自動化と、そのポートフォリオ（ネットワーク管理、IoT 管理、サーバー管理、セキュリティ製品など）との統合に重点を置いている。
- **CrowdStrike**：大手企業向けエンドポイントセキュリティソフトウェアベンダー。2024 年 3 月に初の UEM 製品を発売。この製品は Windows、macOS、Linux デバイスの登録、構成管理、ソフトウェアパッチの適用といった機能を備え、大手企業で広く採用されている同社

の大規模な Falcon エンドポイント検出／対応（EDR：Endpoint Detection and Response）プラットフォームと緊密に連動している。

- **Fleet**：Windows、macOS、Linux をサポートするオープンソースのエンドポイント管理プラットフォーム。2024 年にはモバイルデバイス OS も対象とする予定。このデータ中心のプラットフォームは、大規模なデバイスフリートを有する企業を対象としており、エンドポイントへのソフトウェアのプッシュ配布や、管理対象のデバイスからのデータ取得（SIEM またはその他の分析ツールへの取り込み）を自動化するための API（Application Programming Interface）を提供している。
- **Kaseya**：マイアミを拠点とする IT システムソフトウェアベンダー。CEM、RMM（Remote Monitoring and Management）、ITSM、セキュリティ管理ツールなど、幅広い IT 製品群を有する。このベンダーは主に SMB や大企業を顧客とするマネージドサービスプロバイダーをターゲットにしている。
- **Scalefusion**：インドのプネに本社を置く Scalefusion は、Windows、macOS、Android、iOS、Linux のエンドポイントを管理するクラウドベースの UEM プラットフォームのベンダー。多様な OS が混在する大規模なデバイス群を保有する SMB や中堅企業の IT 部門向けに、レポート機能や分析機能、セキュリティとコンプライアンスのテンプレート、ツールなどを提供している。

補遺

IDC MarketScape Graph の読み方

本調査レポートにおいて、IDC は、企業の成功の可能性を示す主要な指標として、ケイパビリティ（能力）とストラテジー（戦略）の 2 つのカテゴリーに分けて分析している。

Y 軸上の位置付けは、ベンダーの現在のケイパビリティとサービスメニュー、そしてベンダーが顧客のニーズにどの程度沿ったものであるかを示す。ケイパビリティのカテゴリーは、現時点のベンダーおよび製品の能力に焦点を当てている。このカテゴリーでは、IDC アナリストは、企業が選択した市場戦略を遂行する上で、こうした能力をどのように組み立て発揮しているかを分析する。

X 軸、あるいは戦略軸上の位置は、ベンダーの将来に関する戦略が 3〜5 年後の顧客の要求に合致するかを示す。この戦略カテゴリーは、オファリング、顧客セグメント、ビジネスに関するハイレベルの判断や仮説、そして今後 3〜5 年間の市場開拓計画に焦点を合わせている。

IDC MarketScape において、各ベンダーを表すマーカーの大きさは、分析対象である市場セグメントにおけるそれぞれのベンダーの市場シェアを表す。

IDC MarketScape の調査方法

IDC MarketScape における評価基準の選択、重み付け、ベンダースコアは、市場やベンダーに関する十分な調査に基づいた IDC の判断によって設定されている。IDC アナリストは、標準的な特性の範囲を定め、その基準に基づき、市場のリーダーや関係筋、エンドユーザーとの整理された議論、サーベイ、インタビューを通して、ベンダーの評価を行っている。市場の重み付けは、市場ごとに、ユーザーの取材、IT バイヤー調査、それぞれのテクノロジー市場を担当する IDC の専門家からの情報に基づいて行われる。IDC のアナリストは、詳細な調査やベンダー取材、公開されている情報、エンドユーザーの体験に基づいて個々のベンダースコアのベースとし、最終的に IDC MarketScape におけるベンダーの基本的な位置を設定して、各ベンダーの特性、行動、能力に関する正確で一貫性のある評価を行う。

市場定義

クライアントエンドポイント管理ソフトウェアおよび SaaS（Software as a Service）ソリューションは、クライアント、デスクトップ、モバイルデバイス、一部の IoT デバイス、および周辺ハード

ウェアとソフトウェア資産の変更、構成、コンプライアンス、資産追跡、およびソフトウェア配布を提供するが、ネットワークデバイス、ストレージ、またはサーバーシステムは提供しない。

参考資料

関連調査

- *Five Trends to Watch in Endpoint Device Management in 2024*（IDC #US51763224、2024 年 1 月発行）
- *The Role of Client Endpoint Management Tools in Digital Employee Experience Monitoring*（IDC #US46460821、2023 年 12 月発行）
- *Worldwide Unified Endpoint Management Software Forecast, 2023-2027*（IDC #US47945922、2023 年 7 月発行）
- *IDC MaturityScape: Apple Device Management in the Enterprise 1.0*（IDC #US50671623、2023 年 5 月発行）
- *What's Behind the Windows/Mac Device Management Gap in the Enterprise?*（IDC #US50688223、2023 年 5 月発行）

Synopsis

本調査レポートは、IDC MarketScape モデルに基づいて、Windows エンドポイント向けのクライアントエンドポイント管理ソフトウェアを提供しているベンダーを評価している。

IDC の Endpoint Device Management and Enterprise Mobility のリサーチバイスプレジデントである Phil Hochmuth は、「ほとんどの企業で使用されている主要なエンドポイントコンピューティングツールは依然、Windows である。企業の大規模な Windows デバイスフリートを管理するのは容易なことではない。Windows エンドポイントの展開、構成、セキュリティ、ライフサイクル管理は、IT 運用チームとセキュリティチームの双方にとって大きな試練となる。Windows に特化したクライアントエンドポイント管理ツールは、IT チームとセキュリティチームが、従業員の Windows 環境が安全で、コンプライアンスに準拠し、使用可能で、生産的であることを保証することを支援するものでなければならない」と述べている。

IDC 社 概要

International Data Corporation（IDC）は、IT、通信、コンシューマー向け IT 分野に関する調査／分析、アドバイザリーサービス、イベントを提供するグローバル企業です。1964 年の設立以来、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。現在、110 か国以上を対象として、1,300 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査／分析および市場予測を行っています。IDC は、IDG（インターナショナル・データ・グループ）の系列会社です。

IDC Japan

IDC Japan（株）〒 102-0073 東京都千代田区九段北 1-13-5
81.3.6897.3812
Twitter: @IDC
blogs.idc.com
www.idc.com