Gartner

Publication Date: 5 September 2017 ID Number: INF-17-131 (G00311193)

エンタプライズ・モビリティ管理スイートのマジック・クアドラント

R. Smith, T. Cosgrove, B. Taylor, C. Silva, M. Bhat

エンタプライズ・モビリティ管理スイートは、増加し続けるモバイル・デバイスの数と種類に対応しながら、デバイスとエンタプライズ・ワークフローを結び付ける役割を果たしている。モバイルおよびエンドポイント戦略を担当するI&Oリーダーは、市場が急速に変化する中、短期的目標と長期的目標の両方への注力を続ける必要がある。

【日本語サマリ版】

日本語サマリ版は、お客様にレポートの概要を迅速に理解する一助としていただくことを目的として、オリジナル (英文) レポートの導入部の一部を翻訳したものです。レポート全体の内容につきましては、添付のオリジナル (英文) レポートの全文を閲読いただきますようお願いいたします。

■ 監訳アナリストの視点

スマートフォンやタブレット端末などのモバイル・デバイスを管理するツールには、モバイル・デバイス管理 (MDM)、モバイル・アプリケーション管理 (MAM)、モバイル・コンテンツ管理 (MCM)、アイディンティ管理という4つの中核となる機能があり、これらをエンタプライズ・モビリティ管理 (EMM) スイートと総称している。日本企業においても、ユーザーのモバイル利用が拡大するにつれ、プロビジョニング、監査、トレース、レポーティング、データ保護、サポートといった機能を含めて、管理上の視野を広げる必要が生じてきている。
企業は、まず最初に、ターゲットとなるモバイル・ワーカーの要件、利用目的、適用範囲を明確にし、これに見合う適切なリスク・レベルとサポート・レベルをプロファイリングする。その上で、設定したリスクやサポート・レベルに見合うEMM製品を選択する。そうしたEMM製品を選択する際にグローバル・ベンダーを対象とする場合、選択の一助として、本マジック・クアドラントを活用されたい。

(針生 恵理)

市場の定義と解説

エンタプライズ・モビリティ管理 (EMM) スイートは、モバイル・デバイスを社内のインフラストラクチャに結び付ける役割を果たす。企業は、社内のユーザーに向けて以下の機能を実行するために、EMMツールを利用している。

- **プロビジョニング**：企業内の展開と利用、アップデート管理、デバイスのアップグレード／廃止サポート向けにデバイスとアプリケーションを構成する。
- **監査、追跡、レポーティング**：社内ポリシーの遵守状況を確認して資産を管理するために、デバイスのインベントリ、設定、使用状況をトレースできる。
- **企業データの保護**：データ暗号化、データ・アクセス権、共有デバイス、アプリケーションのラッピングとコンテナ化、デバイスのロックダウンに関するコントロールを追加することで、データの漏洩、窃盗、従業員の退職、その他のインシデントによる影響を緩和できる。
- **サポート**：インベントリ、アナリティクス、リモート・アクションを通じて、IT部門によるモバイル・デバイス問題のトラブルシューティングをサポートする。

IT部門が上記のサービスを実施できるように、EMMには5つの中核的なテクニカル機能が存在し、その一部は重複している。企業は、社内要件に応じてこれらの機能をすべて利用することも、一部のみを利用することもできる。

- **モバイル・デバイス管理 (MDM)**：インベントリ、OS構成管理、デバイスのプロビジョニングおよびプロビジョニング解除、リモート・ワイプ (消去)、トラブルシューティング用のリモート・ビューとコントロールの各機能を提供するプラットフォーム依存型ライフサイクル管理テクノロジである。MDMプロファイルをデバイスにインストールすると、これらの機能が利用可能になる。数社のEMMプレーヤーが、ワークステーション・クラスのPCやMacも管理可能な製品へと移行しつつある。
- **モバイル・アプリケーション管理 (MAM)**：アプリケーション単位で管理とポリシー・コントロールに関する機能を実行する。EMMコンソールを介して、アプリ・ストアからアプリケーションが配信され、デバイス上でローカルに管理される。また、MAMは、システム管理者とアプリケーション・オーナーが利用パターンを確認できるようにするアナリティクス機能を提供する。MAMの機能には、以下のものがある。
  - **企業向けアプリ・ストア**：社内で開発したアプリケーションと商用アプリケーションをビジネス領域で展開する際に利用する。
  - **アプリケーションの管理と配信のサポート**：OSネイティブ型API (Android for WorkやiOSのManaged App Configurationなど) や、Android、iOS、Windows用アプリの一括購入を利用する。
- **モバイル・アイデンティティ (MI)**：ユーザーとデバイスの証明書、認証、シングル・サインオン (SSO) といったアイデンティティ／アクセス管理 (IAM) 機能の管理をサポートすることで、信頼できるデバイスとユーザーのみが社内アプリケーションにアクセスできるようにする。アクセスに関する意思決定を評価する目的でコンテキスト情報 (ロケーションや時間など) を利用する傾向が高まっている。
- **モバイル・コンテンツ管理 (MCM)**：モバイル・デバイス上にコンテンツを配信するアクセス・ルールを管理するために利用する。高度なMCMツールは機能を完備したエンタプライズ・ファイル同期／共有 (EFSS) スイートでもあることが多く、コラボレーションやさらに高度なポリシー管理といった追加機能を提供しており、EMM製品スイートのコンポーネントとしてバンドルされている。MCMの機能が担う基本的な役割は、以下の3つである。

    - **ポリシー適用**：個々のファイルにまでポリシー (デバイスに依存しない暗号化キー、認証、ファイル共有ルール、コピー／ペーストの制限など) を適用できる。例としては、電子メール添付ファイルへの条件付きアクセス、バックエンド・リポジトリとファイルの同期化、クラウド内リポジトリとファイルの同期化が挙げられる。
    - **コンテンツのプッシュ配信**：プッシュ型のファイル配信／差し替え／削除に関するルールを適用できる。
    - **統合**：基本的なファイル・アクセス・ポリシーを超えて、エンタプライズ情報漏洩防止 (DLP)／エンタプライズ・デジタル著作権管理 (EDRM) インフラストラクチャのほか、サードパーティのアクセス権管理システム向けにモバイル互換性を追加している。
- **コンテナ化**：EMMツールは、業務利用を私的利用から隔離できるよう設計された検疫環境内でMDM、MAM、MI、MCMをカプセル化し、共有マルチユーザー・デバイス上でデータと機能の隔離を容易にする手段を提供する。この機能を、モバイルOS用APIを通じて実現する事例が増加している。ただし、ビルトインのAPIが利用できないか、利用することが望ましくない場合は、企業データを分離するためにEMMツールでコンテナ化する必要がある。コンテナ化は、個人情報管理 (PIM) クライアントなど、スタンドアロンの自己充足型アプリケーションの場合もある。この機能を利用すると、特定のAPIに対する依存性が解消され、その結果としてクロスプラットフォームの互換性を改善できる。また、管理対象外の (MDMプロファイルをインストールしていない) デバイス上で稼働するアプリに特に大きなメリットをもたらす、自己保護／強化機能を追加できる。コンテナ化テクノロジには、以下のものがある。
    - **設定済みアプリ**：EMMベンダーが、電子メールのカレンダー管理と連絡先管理、ブラウジング、ファイル共有といったよく要求される機能に対する管理性とセキュリティのレベルを高めるために、独自仕様のモバイル・アプリを提供するか、特定のサードパーティ・アプリと統合している。
    - **アプリケーション拡張機能**：ソフトウェア開発キット (SDK) を利用するか、個々のアプリをセキュリティ／管理レイヤでラッピングすることで、アプリケーションにポリシーを適用する。

モバイル・ライフサイクルを管理するアプローチは、ベンダーによってさまざまであり、多くのベンダーがアイデンティティとアクセス、コンテンツのセキュリティ、コンテナ化に注力している。ガートナーは、MDMとMAMに加え、MI、MCM、コンテナ化テクノロジのうち少なくとも1つが盛り込まれていることを、EMMスイートに分類されるための条件としている。最先端のスイートは、5つのテクノロジすべてが盛り込まれているものになる。

図1. エンタプライズ・モビリティ管理スイートのマジック・クアドラント

出典：ガートナー (2017年6月)

結論

企業は、社内のビジネス・ワークフローにモビリティを組み込むためにEMMツールを利用している。自社に適したベンダーや製品を判断する要因は多数存在する。ベンダーは、モバイル・デバイス特有の急速な変化に追随する能力を実証する必要がある。企業は、社内の重要なモバイル・アプリと自社のITインフラストラクチャ (公開鍵インフラストラクチャ [PKI]、VPN、ワイヤレス・ネットワーキング、IAMプラットフォームなど) との統合をサポートするEMMベンダーの能力を見極める必要がある。

EMM製品の要件は、モバイル・プラットフォームに応じて変化する。したがって、モバイル・プラットフォームの変化に追随し、モバイル・デバイス市場の変化とそのモビリティ管理への影響を理解するために、ガートナーのアナリストと定期的に協議することを推奨する。ベスト・プラクティスは、まず自社の要件を確立し、BYOD (個人所有デバイスの業務利用) や自社固有のユースケースなど、社内で考え得るモバイル・シナリオをすべて考慮した上で、ベンダーの最終候補を選定することである。本マジック・クアドラントの位置付けのみを根拠にベンダーを選択してはならない。

市場の概況

EMMは、極めて幅広く、かつ多様なツールのセットであり、複数のツールが連携することで、デバイス、アプリ、データの総合的なライフサイクル管理を行うフル装備のスイートを形作っている。顧客のニーズはセクタによって大きく異なるが、大半の顧客がMDMとMAMの機能を利用している。MI、MCM、コンテナ化といった高度な機能を利用している顧客は比較的少数であり、EMMの5つの機能すべてを利用している顧客は、ほとんど存在しない。その結果、組織全体で使用されるEMMの機能は、平均で全EMM機能のわずか10%にとどまっている (もっとも、使用される機能は組織のタイプによってかなり差がある)。最も先進的なEMM導入事例では、全EMM機能の30～40%が使用されることが多いが、大半の組織にとってこの数字は当たり前のものではない。

EMMが「接着剤」として機能

モバイル・プラットフォーム上で何かを管理する計画を立てている場合は、EMMが出発点となる。EMMは、推定の足掛かりとなるエージェントであるため、プラットフォーム上のほかのサービスとツールにポリシーを展開させる上で理にかなった選択肢である。EMMは、以下のようなデバイスに関するポリシーを設定、保持、検証、適用、更新するためのプラットフォーム共通のベースラインを提供する。

- ゲートウェイ
- プロキシ
- VPN
- ネットワーク・アクセス・コントロール／証明書
- アプリケーション証明書
- コンテンツ／権限管理システム
- IAM
- バージョン・コントロール／バックアップ
- システム更新
- デバイス初期化／消去

EMMは、ポリシーと説明責任の一元管理ポイントとして、エージェントの肥大化 (PC上で頻発しているように、アドオン・ユーティリティが際限なく追加されるためにローカル・リソースが浪費され、システム管理者によるポリシー調整作業の煩雑化を招く) を回避する機会を提供する。PCにはこうした状況に対処するリソースがあるが、小型モバイル・デバイスの場合、必要以上に複雑性が高まるとユーザー (特にBYOD対象者) は適切に対処できない。

MDM

MDMは、EMMの「接着剤」としての効果を実現する鍵である。パスコードの強制やデバイス・ワイプといった基本的なポリシー管理を行うスタンドアロンの製品カテゴリから、EMMスイート内で必須の重要な機能に変化している。MDMコントロールは、すべてのOSをカバーする形で進化しており、Windows 10とMac OSに対応する従来型のデスクトップ管理にまで拡張されている。さらにガートナーは、管理の対象が拡大し、モノのインターネット (IoT) デバイスとLinuxを含むようになったことを確認している。各OSが同様の基本的コントロールを提供しているが、高度なコントロール (Windows 10搭載デバイス向けのOSバージョン・コントロール、Device Enrollment Program [DEP] を利用したiOS向けの自動デバイス・ステージング、Android for WorkとSamsung Knoxの業務／個人向け環境に各種ポリシーを適用する機能など) は大きく異なっている。

ガートナーは、MDMを企業所有デバイスの重要な要件と見なしている。個人情報保護と法務面の懸念から反発が強まっているが、こうした反発の原因の多くはユーザーがMDMの機能を誤解していることにある。

MAM

MAMは、モバイル・アプリの展開／運用ライフサイクル管理をサポートする。機能としては、システム管理者によるプッシュ配信、ユーザーによるカスタム／公開 (アプリ・ストア) アプリの展開と更新、関連アプリ・ライセンスの管理などがある。ユーザーによる展開は、エンタプライズ・アプリ・ストアを通じてサポートするが、こうしたストアはWebベースのポータルかモバイル・アプリの形態を取ることが多い。ライセンス管理は、AppleのVPPなど、主要なエンタプライズまたはボリュームライセンス機構をサポートする必要があります。MAMには、アプリを (BYOD対象の個人所有アプリやCOPE [企業所有デバイスの個人利用] のユースケースではなく)「管理対象」エンタプライズ・アプリと認識してタグを付ける機能や、これらのアプリに管理／セキュリティ・ポリシーを適用する機能、デバイス内のアプリと関連データを選択的に消去する機能もある。

エンタプライズ・アプリに適用されることが多いポリシーには、以下に例示するセキュリティ・ポリシーとDLPポリシーがある。

- アプリの起動時に、アプリ単位で VPN 接続を開始するよう要求する。
- 特定のアプリの証明書を登録できる。
- アプリをリモートから選択的に消去できる。
- アプリをブラックリストに登録できる。
- エンタプライズ・アプリ内に含まれるデータ (場合によってはファイル・レベルのデータ) を暗号化する (基盤であるOSが採用しているものよりも強力な暗号化手法を採用している場合もある)。
- 「Open In」や類似のアプリ・データ交換を管理対象 (自社所有) アプリのみに制限する。
- カット／コピー／ペーストを制限する。
- 条件付きの起動やアクセスを必須とする (デバイスが承認済み状態にあることや、ジェイルブレイクやルート化を行っていないなど)。

MAMの差別化機能は、複数の分野に表れている。例えば、企業向けアプリ・ストアは基本的なものから高機能なものにまで至り、一部は使い勝手と機能がApple App StoreやGoogle Playといった主要な商用アプリ・ストアに近づいている。一方、ローエンドの製品は、入手可能なすべてのアプリを全ユー

ザーに提示するごく基本的なWebポータルや単純なアプリと大差なく、フィードバックやアプリ評価の仕組みを備えていないため、ユーザーにとってはアプリを見つけるのが困難である。

また、差別化がOSのサポートやMAMに対応する各種の仕組みのサポートに表れることもある。アプリにポリシーを適用する際は、以下の3つの汎用的な仕組みから1つを利用する。

- OS がネイティブに備えている MAM 用 API
- 独自仕様の SDK を開発中にコンパイルしてアプリに仕上げたもの
- アプリ・ラッパー (バイナリに対するコード・インジェクション [開発後])

EMMベンダーの中には、主要モバイルOSのすべてを対象として3つの仕組みをすべてサポートするものと、一部のみをサポートするものがある。例えば、ベンダーがAppleの内蔵MAM APIのサポートは盛り込むが、GoogleのAndroid for Work内蔵MAM APIはサポートしないこともあり得る。

コンテナ化

「コンテナ化」は業界内でさまざまな意味に用いられているが、ここでは業務データと個人データを分離する機能の拡張セットを表す。例えば、PIMクライアント、公開モバイル・アプリや独立系ソフトウェア・ベンダー (ISV) が提供するモバイル・アプリ (いずれも設定済みのもの)、アプリケーション拡張機能 (SDKやアプリ・ラッパーなど) である。

- **PIM**：業務用の電子メール、カレンダー管理、連絡先管理を実現するモバイル・アプリであり、通常はネイティブの電子メール・クライアントにないセキュリティ／管理機能を備えている。利用は減少しているが、現在でも金融、医療、公共セクタといった規制対象業種や高セキュリティ業種では要件となっていることが多い。
- **設定済みアプリケーション**：EMMベンダーは、管理性レベルを高めるべく、独自仕様のモバイル・アプリを提供するか、特定のサードパーティ・アプリと統合している。ほとんどの場合、これらのアプリにはEMMプロバイダーかサードパーティが提供するセキュア・ブラウザのほか、オフィス／コラボレーション・アプリケーションが含まれる。
- **アプリケーション拡張機能**：これらの独自仕様のツールは、EMMを介してモバイル・アプリを管理できるようにする機能を備えている。企業やISVがSDK内のライブラリとモバイル・アプリをコンパイルすると、特定EMMベンダーのポリシーを適用できる。ラッパーは通常、モバイル・アプリの実行可能バイナリに対し、ある種の形態のコード・インジェクションを実行することで、特定のEMMベンダーのポリシーを適用する。SDKやラッパーは、(ISVが当該EMMベンダーのSDKを利用している場合を除き) EMMに登録していない (または登録できない) デバイスに管理対象アプリを配信する必要のある「MAM限定」ユースケースに必須である。ベンダーの中には、SDKとアプリ・ラッピングのアプローチを両方サポートしているものと、一方のみをサポートしているものがある。

ガートナーは、基本的なMAM用語との混乱を避けるために、本機能をコンテナ化として定義している。こうしたコンテナ化のユースケースは、アプリケーションにビルトインするか、SDKを使うか、ラッパーを適用して活用する。なぜなら、ネイティブのOS APIではEMMに登録することにより作られた「信頼された関係」なしにはアクセスできないからである (「モバイル・アプリケーション管理のマーケット・ガイド」APP-16-55、2016年6月20日付参照)。

MI／アクセス

現在、ユーザーが所有するデバイスは1台だけではない。スマートフォン、タブレット端末、ノートPCを1台ずつ所有しているユーザーも多く、BYODプログラムの一環として複数のデバイスを利用したいと考えているユーザーも多い。そのため、組織は、ネットワークに接続しているユーザーを特定す

るだけではなく、自社が許可したデバイスで接続しているか否かを確認できなければならない。ガートナーがモバイル・アイデンティティ管理をEMMの重要な能力と位置付けているのは、このためである。多くの場合、モバイル・アイデンティティ管理にはデジタル証明書が用いられるが、生体認証やトークンによる認証をはじめ、さまざまなテクノロジを通じて管理することもできる。

ガートナーは、IAMツールを備えたEMMが登場し始めていることを確認している。そのため、数社のEMMベンダーがSSOなどのIAM機能を実現し、アイデンティティ・プロバイダーとして活動している。一方、サービスとしてのアイデンティティ (IDaaS) を提供しているベンダー数社が基本的なEMM機能の提供を開始するという、逆方向の動きもある。

認証機能によって、ユーザーとデバイスばかりか、ユーザーがネットワークに接続している場所と手段 (オフィス内／自宅／国外にいるか、公衆Wi-Fiを使用しているか) も特定できる。また、これらのコンテキストに応じて、ユーザーに提供するアクセスのレベルを調整できる。ガートナーはまた、アクセスに関する重要な決定を下すために、人工知能 (AI) が使用されるようになると予測している。ガートナーは、今後2年間にコンテキスト・ベースのモバイル・アイデンティティ管理がEMM製品の標準機能になるとみている。

EMMがエッジ部でファイル・レベルの保護を実行

モバイル・デバイスに保存されている社内データの保護は、これまで多岐にわたるアプローチに基づいていた。すなわち、静止中、利用中、移動中の各データの暗号化や、デバイス・レベルとアプリケーション・レベルのポリシー (タイムアウトによるスクリーン・ロック、個人識別番号 [PIN] の強制、「Open In」機能の制限など) である。しかし、ひとたびデータが保護対象のデバイスやネットワークを離れると、こうした間接的な保護アプローチは有用ではないと見なされる。ユーザーは、社内データを社外の関係者や個人用の電子メール・アカウントに電子メールで送信したり、データを自分のPCにコピーしたりすることで、間接的なコントロールを迂回でき、実際、頻繁にそういった操作を行っている。そのため、データを本質的に保護するか、または権限管理ベースのアプローチをモバイル・データ保護に採用するニーズが高まっている。

ファイル・レベルの暗号化製品は、(単に保存されているデータとネットワーク・トンネルを暗号化するのではなく) 個々のファイル自体を暗号化し、PKIを通じてマネージド・ファイル・アクセスを促進するため、保存場所やアクセスされる場所を問わず、データを保護できる。暗号化キーを持たないユーザーは、こうした方式で保護されたファイルにアクセスできない。

権限管理製品は、IAMのフレームワークを拡張することによって、ファイルへの「アクセス」に対するコントロールに加えて、ファイルの「操作」に対するコントロールを実現する。権限管理製品を導入した企業は、ユーザーに対して、例えばファイルの閲覧権、編集権、削除権のほか、電子メールで転送する権利を制限できる。こうした製品の多くは、モバイル・データ保護スキームの一環としてファイル・レベルの暗号化もサポートしている。したがって、権限管理アプローチを環境内で有効利用するには、効果的なデータ分類が必要不可欠である。

ファイル・レベルの保護機能や権限管理機能を中核製品のアドオンとして開発しているEMMベンダーもあれば、自社のEMMシステムと汎用IAM製品を緊密に統合することによってこの機能を相乗的に実現しているベンダーもある。デバイス、アプリ、コンテンツの各レベルに対応するポリシーと同様、EMMを導入すると、暗号化とアクセス／権限ポリシーの両機能が併存する場で一元的なシステム管理を実現できる。

統合エンドポイント管理 (UEM)

EMMのマジック・クアドラントを発行するのは2017年で4年目となるが、ガートナーには今でも頻繁に、EMMという用語を認識していない顧客からMDMに関する問い合わせが寄せられている。EMMは、以前の基本的なMDMに代わり顧客のニーズを満たすよう設計されたものだが、現在ではEMMでさえ、

もはや企業の要求を満たせなくなりつつある。これは、クライアント・コンピューティングとモバイル・コンピューティングが融合し、エンドユーザー・コンピューティングという領域を生み出していることによる。結果として、従来のクライアント・デバイスとモバイル・デバイスの両方を管理する単一のソリューションが必要になってきた。AppleおよびMicrosoftは、こうした融合に容易に対応できるよう、自社のプラットフォームにMDM APIを追加している。今日、UEMを実装する上で最大の課題となっているのは、企業には昔ながらの要件が存在するということである。すなわち複雑なWin32アプリケーションとグループ・ポリシー・オブジェクト (GPO) を多くの企業が有しており、EMMツールではこれらに対応できない。しかしながら、EMMツールによってPCの管理を可能にするような変化も起こっている。第1に、MicrosoftがWindows 10のMDM APIを継続的に強化し、GPOとのギャップを埋めている。第2に、EMMベンダーが独自の機能を提供し、セキュリティ・ポリシーの運用やスクリプトの管理、Win32アプリケーションの展開といった分野におけるギャップに対処している。こうした進展により、企業がEMMツールを使用してPCを管理できるシナリオが拡大しつつある。

本市場におけるその他の進展としては、同じエンドユーザー・コンピューティング・グループの下で管理されるIoTデバイスへの需要の増加が挙げられる。ガートナーは、従来のデバイス、モバイル・デバイス、EMMによる管理が可能なIoTデバイスを管理する単一のソリューションを、UEMとして定義している。今後数年にわたってデバイスが変化し続け、新しい管理要件が生じる中で、この定義も進化すると考えられる。ただし、すべてのIoTオブジェクトがEMMツールの管理対象になるわけではない。デバイスによってはメーカーが直接管理するか、独自の管理ツールを備えるものも登場するであろう。また、管理をまったく必要としないデバイスも多数現れる。ただし、デバイスの台数が右肩上がりとなり、多様化もますます進むため、IT部門がそうした事態に備える必要があることは明白である。

(監訳：針生 恵理)

【オリジナル・レポート】

「Magic Quadrant for Enterprise Mobility Management Suites」(G00311193、2017年6月6日付)