SRA の技術情報誌
GS LetterNeo
Vol.174　2023 年 1 月

EMM を用いたデバイス管理

外山 由幸

アドバンスドクラウドエンジニアリング事業部

はじめに

EMM(Enterprise Mobility Management)は、業務で利用されるモバイルデバイス（スマートフォン、タブレット、PC）を管理する製品の総称です。昨今、テレワークの普及もありモバイルデバイスを業務で活用することは多くの企業で求められるようになっています。今回は、EMM を用いたモバイルデバイスの管理について紹介します。

目次

EMM とは

EMM は、MDM・MAM・MCM の 3 つの構成要素からなるモバイルデバイスの総合管理ツールです。

MDM(Mobile Device Management)は EMM の主たる機能の 1 つで、モバイルデバイスの管理を行う役割を担っています。具体的な機能はリモート制御、機能の制限、OS アップデート管理等です。MAM(Mobile Application Management)はアプリの管理を行う役割を担っています。デバイスにアプリのインストールを行ったり、特定のアプリを利用禁止にしたり等の制限を行うことができます。MCM(Mobile Contents Management)はコンテンツ（業務データ）を安全に利用する役割を担っています。

EMM はこれらの機能を兼ね備えているソリューションであり、これに加えて製品によってレポート機能やルール違反の検出・通知機能等、様々な付加機能を備えていることが一般的です。

EMM の構成要素

次に、EMM の構成要素である MDM、MAM、MCM の機能についてもう少し深く掘り下げていきます。

MDM(Mobile Device Management)

MDM はモバイルデバイスそのものの管理を行う役割を担います。この機能は一般的に OS（Apple iOS・iPadOS・macOS, Google Android, Microsoft Windows）が標準的に有している機能を用い、デバイスに対して様々な制御を行います。

- デバイスが有する機能を利用不可（禁止）にする
  カメラ、GPS、USB 外部デバイス、スクリーンショット　等
- デバイスが有する機能の利用を強制する
  パスコード設定、時刻同期、Wi-Fi を常にオン　等
- アップデートの制御
  iOS、Android、Windows の各 OS や更新プログラムの制御
- その他セキュリティ対策機能
  リモートワイプ、リモートロック、紛失モードの有効化等

スマートフォンに対する制御は、ＭＤＭを利用したことのない人にはあまり馴染みがないかもしれませんが、例えば飲食店の注文用タブレットで特定のアプリケーション以外を利用できなくすることも MDM の制御によるものです。また、Windows デバイスに対する制御は GPO とほぼ同じ制御ができます。例えば、パスワードの文字数や有効期限の設定、Microsoft Update の制御、Wi-Fi やアプリの設定情報の配布等を行うことができます。なお、これらの設定は BYOD(Bring Your Own Device)に対しても有効ですが、企業所有のデバイスとは異なり有効な制限等は一部に限られます。

MAM(Mobile Application Management)

MAM はモバイルデバイス内のアプリを管理する役割を担います。デバイスに対してアプリのインストールを行ったり、逆に特定のアプリを利用禁止したりすることができます。また、会社のデータを安全に利用するために専用のアプリケーション（ブラウザ、メーラ等）を提供している EMM 製品も存在しており、そういったアプリケーションでは特定アプリ以外へのコピー＆ペーストやファイルの受け渡し、スクリーンショットの取得等を禁止できるようになっています。

また、MAM は特に BYOD において効果的に利用されます。BYOD を効果的かつ安全に業務利用するには、個人領域のアプリ・データと業務領域のアプリ・データを分離する必要があります。MAM には先述のとおりアプリ配信の機能がありますが、配信されたアプリは業務用と個人用とで区別されます。先述のとおり、MAM はアプリ間のコピー＆ペーストやファイルの受け渡しを禁止する機能を有しており、業務領域のデータを個人領域のアプリから送信してしまう等の情報漏洩を防ぐことが出来ます。

MCM(Mobile Contents Management)

MCM は企業内にあるコンテンツを安全に利用する仕組みを提供します。企業内のファイルサーバには様々な業務用ファイルが存在しますが、これらのファイルをモバイルデバイスにコピーすることはセキュリティ上望ましくありません。しかし、モバイルデバイスでのファイルの利用を禁止してしまうと、利便性が損なわれることになります。そこで、MCM は、企業内のファイルへのアクセス権を管理したり、デバイス上にデータが残らないようにする専用のアプリケーションを利用したりして、安全に業務用ファイルを扱える仕組みを提供しています。

EMM で出来ること

ここまで、 MDM, MAM, MCM と EMM を構成する 3 つの要素について説明しました。これらの 3 つの要素は互いに関係しあっており、協調してデバイスの管理を行うことで、より安全に、より使いやすく、より効率的に、モバイルデバイスを管理することができるようになります。EMM はこれら 3 つの機能を併せ持つ総合管理ツールで、複数のデバイスを効率的かつ安全に管理することができます。

ここでは、EMM で出来ることの例として、デバイスのキッティングとアップデート管理について取り上げます。

デバイスのキッティング

社給のスマートフォンやパソコンを社員に配布する場合、利用の際に適切な制限をかけることも大事ですが、配布前に様々なアプリケーション・ソフトウエアのインストールや設定を行う、いわゆるキッティングも重要です。しかし、キッティング作業には大きな時間と労力がかかります。EMM を用いることにより、これらの初期設定をサーバで一括管理することができます。

例として、具体的に iPhone のキッティング時の流れで説明してみましょう。iPhone の電源を初めて投入すると、初期セットアップが行われます。この際にはパスコード設定、GPS の設定、利用規約への同意、ディスプレイ調整などの様々な設定が対話的に行われますが、手作業でこれらの設定を一つ一つ選択すると多くの時間を要します。EMM（MDM）を使うとこれらの設定を任意に非表示（スキップ）にすることができ、多くの時間を短縮することができます。

初期設定が完了した後は、業務で利用するアプリのインストールを行います。通常のiPhone の場合は App Store にアクセスして必要なアプリを一つずつインストールしますが、EMM(MAM)の機能を用いることによりアプリの自動配信を行うことができます。また、アプリケーション構成の配布に対応しているアプリに対しては、MDMからその設定情報である構成プロファイルを配布することもできます。例えば、メールアプリにおいて自身のアカウントのセットアップ情報（メールアドレス、サーバの設定情報等）を配布することで、利用者が設定する手間を省くことができます。

このような初期設定の管理はiPhone(iPad)の他、Android・macOS・Windows等でも同様に行うことができ、様々なデバイスでキッティングの所要時間・工数を削減することが可能です。

デバイスのアップデート管理

モバイルデバイスのセキュリティ対策として重要なものの一つに、iOS や Microsoft Update 等のアップデート管理があります。MDM には、アップデートの適用を一定期間遅延させたり、強制的に適用したりする機能があり、これらの機能を用いることでデバイスのアップデートを管理することができます。

例えば、iOS/iPadOS では制限プロファイルを配布することで iOS/iPadOS のリリースから最大 90 日の間、デバイスへの適用を遅延させることができます。また、Windows では機能更新プログラムのアップデート制限（ターゲットリリースバージョンの設定）を行うことで、機能更新プログラム（21H2 等）の意図しない適用を制限することができます。

また、EMM 製品の多くは、インベントリ情報の収集を通じてデバイスのアップデート状況を容易に確認できる機能を有しています。レポート機能を有している製品であれば、フィルタ条件を設定することによりアップデートが行われていないデバイスを一覧化し、そのデバイスの管理者が誰なのかを確認することができます。さらに、これらの諸条件を基に管理者やデバイスに対して警告の通知を出したり、デバイスの利用制限や一部機能の制限を施したりすることができる製品あり、IT 管理者の手間を減らすことができます。

おわりに

今回は EMM の入門的内容として、構成要素と具体的な活用例をご紹介しました。冒頭でも記載したように、テレワークの普及や働き方改革の一環でモバイルデバイスを業務で活用することは多くの企業で求められるようになっています。EMM 製品によっては、ここに記載した以外にも様々な機能を有しているものがあり、利用者の使い勝手の向上、セキュリティリスクの低減、管理コストの低減等、数多くのメリットがあります。

GSLetterNeo Vol.174

2023 年 1 月 20 日発行
発行者　株式会社 SRA 技術本部 先端技術研究室

編集者　熊澤努　方 学芬
バックナンバー https://www.sra.co.jp/public/sra/gsletter/
お問い合わせ　gsneo@sra.co.jp

株式会社SRA
〒171-8513 東京都豊島区南池袋 2-32-8

夢を。Yawaraka Innovation
やわらかいのべーしょん