企業のスマートデバイス活用を支えるMDM
―マルチキャリア・マルチOSに対応する「NRI-MDM」―

企業がスマートデバイスを業務で利用する場合、基盤管理や情報漏えい対策の観点からMDM（Mobile Device Management）システム（以下、MDM）の導入が必須である。本稿ではMDMの機能、製品やサービス検討時のポイントを解説するとともに、野村総合研究所（NRI）が提供するMDMサービス「NRI-MDM」の特徴を紹介する。

進むスマートデバイスの業務利用とMDM

スマートフォンやタブレット端末といったスマートデバイスの業務利用が進んでいる。スマートデバイスは携帯性、操作性に優れ、社内システムやクラウドサービスにも手軽に接続できる便利さがある。営業面でも、アプリケーションや動画を利用した効果的なプレゼンテーションが可能であり、契約書を電子化してデータ入力などのバックオフィスコストの削減を図ることもできる。

一方で、紛失・盗難のリスクが高く、情報漏えいや第三者の不正利用を誘発しやすい。ウイルス感染の危険性もある。このような理由から、スマートデバイスの業務利用を支える管理システムとしてMDMが普及してきた。個々の端末の状態を正確に把握し、必要な措置を素早く実施できるMDMは、スマートデバイスを活用したい企業にとって必須のツールと言える。

MDMの役割

MDMの主要機能は端末情報の収集、遠隔操作、設定配信の３つである。

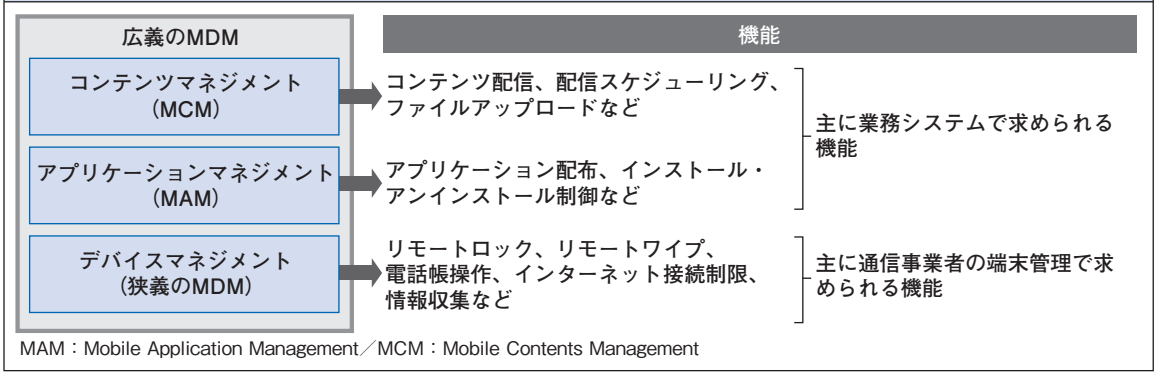
①端末情報の収集

端末名、シリアル番号、アプリケーションのインストール状況など端末の状態に関する情報（インベントリー）を収集して、業務上正しい使い方をしているかをチェックする。

②遠隔操作

紛失・盗難時に、端末の操作を不能にするリモートロックや、端末内のデータを消去す

図１　MDMの概念



MAM：Mobile Application Management／MCM：Mobile Contents Management

野村総合研究所
サービス・産業ソリューション第二事業本部
営業推進部
主任システムエンジニア
伊藤哲也（いとうてつや）
専門はWebサイト・Webシステムの設計・構築、スマートデバイスの導入支援・運用検討

るリモートワイプを行う。

③設定配信

セキュリティポリシーのような各種端末設定のほか、アプリケーションの配布やインストール・アンインストールの制御などのモバイルアプリケーション管理（MAM）、コンテンツの配信やそのスケジューリングなどのモバイルコンテンツ管理（MCM）が含まれる。

単にMDMと言う場合、端末情報の収集と遠隔操作の機能を備える製品やサービス（狭義のMDM）を指すことが多い。スマートデバイスを業務に本格活用する場合には、狭義のMDMにMAMとMCMを加えた製品やサービス（広義のMDM）が必要となる。（図１参照）

OSにより異なる端末管理の仕組み

MDMの端末管理機能は、スマートデバイスのOS（基本ソフト）が標準で備えている端末管理用API（Application Programming Interface：ソフトウェアが利用できる命令や関数、その利用のための手続きを定めたもの）によって実現する。現在、スマートデバイスのOSは米国Apple社のiOSと米国Google社のAndroid OSが大半を占めているが、iOSとAndroid OSでは端末管理機能の実現方法に違いがある。すなわち、iOSはAPIが豊富だがそれ以外の機能の作り込みには限度があり、Android OSはAPIは少ないものの柔軟な個別作り込みが可能である。

MDMサーバーと端末間の通信方式も異なる。iOSではApple社の「APNSサーバー」を利用する通信方式が一般的であり、この方式に沿った環境の準備や運用が必要となる。これに対してAndroid OSでは次のようなバリエーションがある。

①通信事業者のSMS（ショートメッセージサービス）サーバーを利用する方式

②端末が定期的にMDMサーバーにアクセスするポーリング方式

③Google社のプッシュ通知サーバーであるC2DM（Cloud to Device Messaging）サーバーを利用する方式

④ベンダー独自のプッシュ通知サーバーを利用する方式

一般に、iOSはカスタマイズ性は限定的だが標準の範囲内で実現可能な機能が多く、Android OSはカスタマイズ性は高いが不足機能の個別の作り込みが必要となる。

MDM選定のポイント

スマートデバイスの業務利用の拡大に伴って多数のMDMが登場してきた。MDMの選定に当たって検討すべきなのは主に以下の点である。

①自社運用かSaaSか

大規模導入の場合は自社運用（オンプレミス）方式の方がコストメリットが出る場合があり、時間をかけずに始めたい場合にはSaaS（Software as a Service：ソフトウェアをインターネットを通じてサービスとして利

用する）方式が適している。

②付加機能

端末管理用APIを利用するリモートロックやリモートワイプ、端末情報の収集などの基本機能に関しては製品・サービス間の違いは小さい。違いがあるのは管理機能の柔軟性（設定の自由度）や通信方式の種類、関連セキュリティサービスの有無などの付加機能であり、これらを確認する必要がある。

③ヘルプデスクは社内か社外か

紛失や盗難などの緊急事態に備えるためには、休日や深夜を問わず24時間365日の即時対応が求められる。社内のヘルプデスクが平日の日中しか受け付けない場合、サービス時間を変更するか、社外のヘルプデスクを利用するかを検討すべきである。

NRIが提供するMDMサービス

NRIが提供しているMDMサービス「NRI-MDM」は次のような特徴を持っている。

①SaaS方式のサービスであり、企業が自社で調達・構築する場合と比べて初期費用が低く短期間で導入が可能である。

②マルチキャリアおよびマルチOSに対応しており、キャリアやOSが異なる端末が混在する場合でもそれらを一元的に管理することが可能である。

③MDMの機能の提供だけでなく、NRIのサポートデスクがMDMの運用や24時間365日の盗難・紛失対応を実施する。企業側は特別に操作を習得する必要がなく、盗難・紛失に備えた休日夜間を含む対応体制を整備する必要もない。

OSごとに最適なエンジンを採用

「NRI-MDM」では、企業が導入している端末に合わせて最適な機能を提供できるように、iOS向けにはカナダAbsolute Software社の「Absolute Manage MDM」を、Android OS向けには自社開発のエンジンを採用している。どちらのエンジンも、端末情報の収集、遠隔操作、設定配信などMDMの基本的な機能のほか、アプリケーションの配布、不正端末（OSを改変した端末）の検知および通知、メッセージ送信、コンテンツ配信の機能など、端末の基盤管理だけでなくスマートデバイスの活用を促進するための機能を提供している。

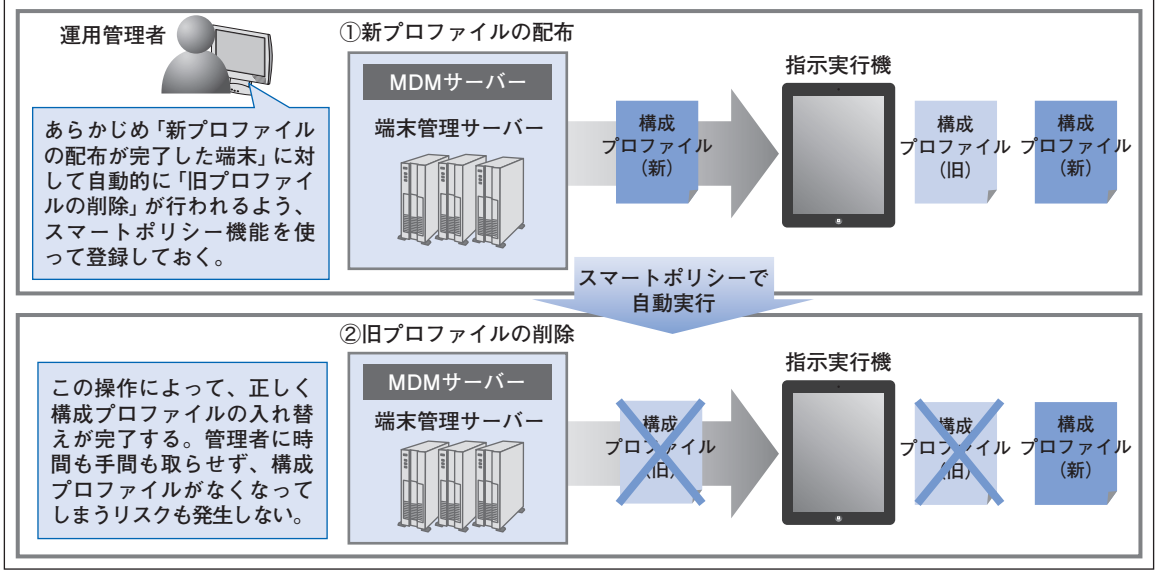
(1) iOS向け「NRI-MDM」の特徴

「Absolute Manage MDM」の大きな特徴は、設定の自由度が高く柔軟性の高い端末管理が可能だという点である。そのため、企業の管理ニーズに合わせた柔軟な運用が可能である。以下に代表的な機能を紹介する。

①柔軟な端末抽出・グルーピング

管理する端末の情報として、機器情報だけでなく端末が持たない情報、すなわち利用者の名前、社員番号、メールアドレス、部署名などをカスタムフィールドとして自由に追加することができる。これらを組み合わせて、

図２　構成プロファイルの入れ替えイメージ



端末の抽出やグルーピングをきめ細かく行うことができる。例えば「営業部管理で最終接続日時が３日以上前の端末」「マーケティング部管理かつ管理職以外の端末で、禁止アプリケーションをインストールしている端末」などである。

②スマートポリシー機能

「端末の抽出条件設定」と「抽出した端末に対するアクション実行」を１つのポリシーとして設定する「スマートポリシー」機能を備えている。

「端末の抽出条件設定」は上述のとおりきめ細かく行うことができる。抽出した端末に対するアクションは、メッセージ送信、管理者へのメール送信、リモートロック、構成プロファイルやアプリケーションの配布・削除などを登録することができる。抽出条件とアクションを組み合わせると、「OSやアプリケーションのバージョンが最新でない端末に注意喚起のメッセージを送信する」「不正端末を検知し、構成プロファイルを削除して社内システムへのVPN（Virtual Private Network：仮想専用ネットワーク）接続を不可にする」といったことが可能である。

スマートポリシー機能は、端末のパスワードポリシーやネットワーク接続の変更に伴う構成プロファイルの入れ替えに特に有効である（図２参照）。

iOSの仕様上、画面ロックがかかっている端末に対して旧プロファイルの削除指示と新プロファイルのインストール指示を同時に実行すると、削除だけが行われてインストールが行われない。そのため、セキュリティポリシーが何も適用されない端末が発生してしま

う。スマートポリシー機能を利用すると、全端末に対して新プロファイルのインストール指示を実行した後に、「新プロファイルが入った端末」という抽出条件と「旧プロファイルの削除」というアクションをスマートポリシーとして設定すれば、構成プロファイルの入れ替えが自動的に確実に行われ、セキュリティポリシーが外れた端末を発生させることがない。

③管理者IDの自由な割り当て

複数の管理者IDを発行し、利用できる機能をIDごとにコマンドレベルで指定することができる。例えば、本社の統括管理者だけでなく、地域管理者や現場管理者にも適切な管理者機能を利用させることが可能となる。

(2) Android OS向け「NRI-MDM」の特徴

Android OS向けにはNRIが独自に開発したエンジンを採用している。独自通信方式のメリットがあるほか、企業が持つアプリケーションやシステムとの連携が可能という特徴を持っている。

①独自通信方式の採用でGoogleアカウントが不要

Android OSのMDMは、提供するキャリアやベンダーによって通信方式が異なっている。Google社が定める通信方式を用いた製品・サービスを利用する場合、MDMサーバーと端末の間にGoogle社のプッシュ通知サーバーであるC2DMサーバーを介する必要があり、端末ごとにGoogleアカウントの取得が必要となる。これに対し「NRI-MDM」では独自のプッシュ通知サーバーを利用するためGoogleアカウントが不要で、煩雑な運用業務を省略できる。

②アプリケーションレベルでの制御が可能

Android OSでは、iOSと比較して端末利用の制御範囲が広い。そのため、端末にインストールされているアプリケーションレベルでの制御も可能である。「NRI-MDM」ではホワイトリスト方式（利用可能なアプリケーションを指定し、それ以外のアプリケーションは使用させない方式）により、端末にインストールされているアプリケーションの実行をバックグラウンドで監視し制御している。

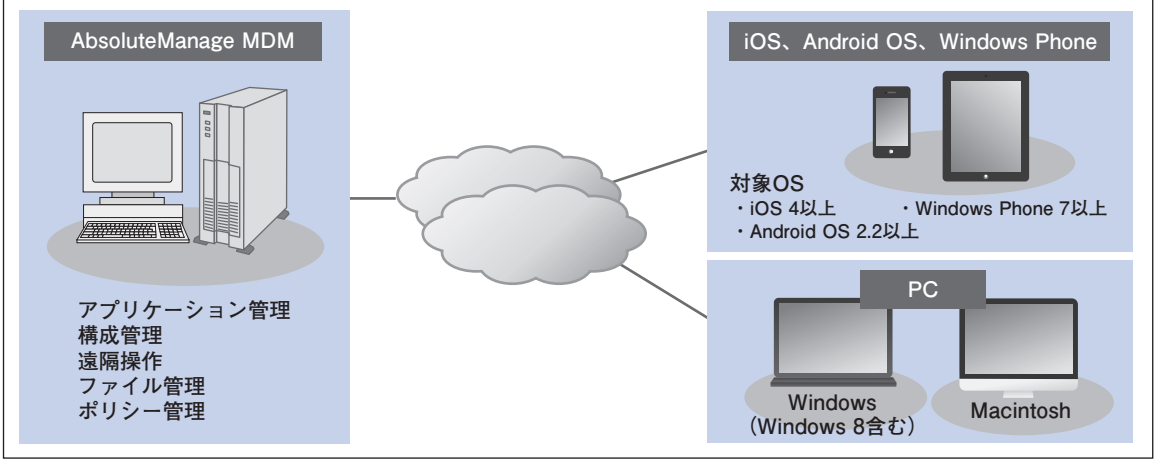
③業務システム・業務アプリケーションとの連携が可能

独自開発のエンジンであることから、企業が持つ業務システムや端末アプリケーションと連携させるためのカスタマイズも可能である。例えば、企業が作成した端末アプリケーションに対し「NRI-MDM」からコンテンツデータを配信することができる。また、業務システムの端末アプリケーションを「NRI-MDM」から実行タイミングをコントロールして遠隔起動することも可能である。

PCやWindowsタブレットの管理も可能

iOS向けのエンジンとして採用している「Absolute Manage MDM」はもともとマルチOS対応であり、機能が一部限定されるもののAndroid OSの管理も可能である。さら

図３「NRI-MDM」のマルチプラットフォーム



にはWindows、Macintoshの両OSのPCまで管理することができる。（図３参照）

PC管理の機能としては、端末情報の収集、遠隔操作、設定配信（ソフトウェア管理）といったMDMの基本機能以外に、パッチ管理、イメージング、パワーマネジメント（電源管理）といったIT資産管理ツールとしての機能も有している。

「NRI-MDM」のサービス拡充に向けて

MDMの分野には多くのベンダーが参入してきており競争も激しくなっている。「NRI-MDM」はさらなる差別化を図るため、今後、以下のような機能強化を予定している。

①管理者機能の強化

「Absolute Manage MDM」は、管理者機能のWebアプリケーション化（現在はWindowsアプリケーションでの提供）や、Absolute Software社の他の製品との統合が予定されている。NRIはそれらの機能拡充を積極的に取り入れ、サービスとして顧客企業に提供していく予定である。またAndroid OS向けのエンジンも継続的に機能改善を行うことにしている。

②MDMサポートデスクの海外対応強化

NRIのMDMサポートデスクは現在でも規定フォーマットによる依頼であれば英語での対応が可能だが、さらに海外対応を強化していく方針である。

③金融機関向けガイドラインへの対応

より高いセキュリティレベルが求められる金融機関向けに、公益財団法人金融情報システムセンター（FISC）が定める「金融機関等コンピュータシステムの安全対策基準」への対応を進めていく。

NRIでは、お客さまの多様なニーズに応えるため、このように「NRI-MDM」の継続的なサービス拡充を図っていく。 ■