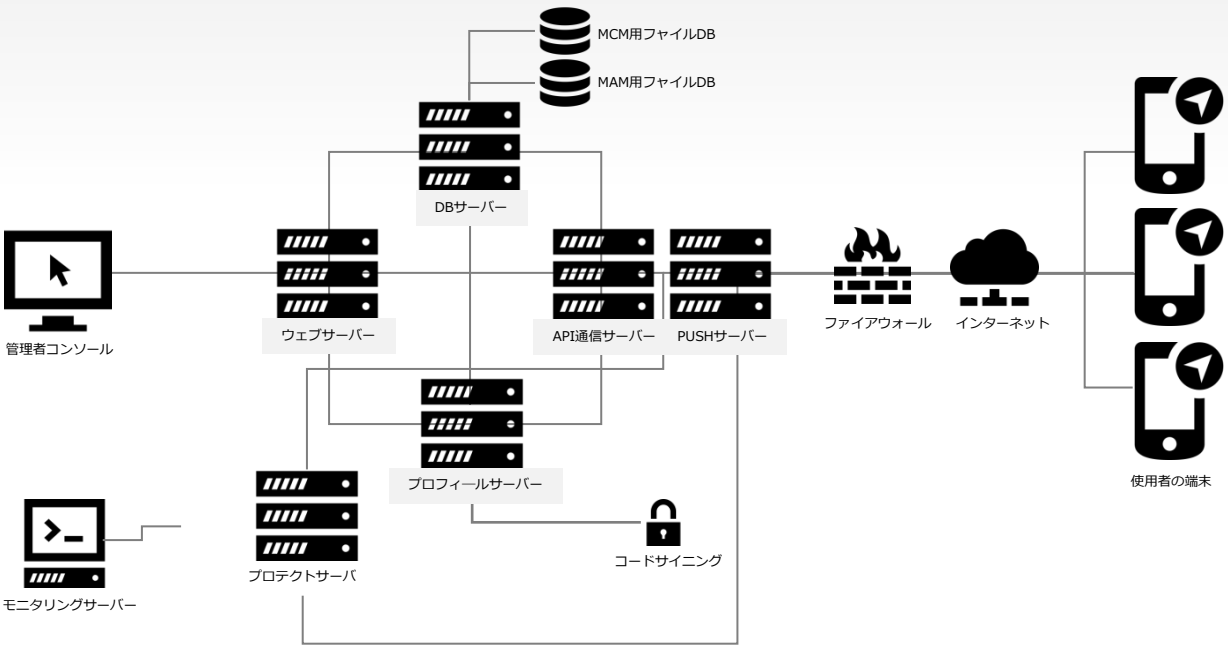
2014年 国内主要15の
モバイルデバイス管理(MDM) 製品比較表



Ascentnetworks
http://www.ascentnet.co.jp

MDMの選定基準

MDMで何をしたいですか？

MDMの選び方

近年、多くの企業においてスマートフォン・タブレットなどのビジネス利用が急増しています。しかし、業務効率向上のためにスマートデバイスを導入したものの、紛失や盗難時のデータ保護や情報漏えい、他の第三者による不正利用などといったセキュリティに対する懸念も増えています。

これを解決するのがモバイルデバイス管理のMDMです。

MDMの基本となるのが端末管理機能です。紛失や盗難時にリモートロックやリモートワイプでデバイスの情報漏洩を防ぎ、さらに、特定のアプリケーションの利用禁止、カメラやSDカードなど情報流出被害に繋がる可能性のある機能を禁止します。また、端末認証を使ってVPNによる社外からのアクセスや社内アプリケーションへのアクセスを制限することができます。

MDMシステムは提供形態としてSaaS型とオンプレミス型の二種類があります。オンプレミス型は運用コスト以外にも設備の構築で費用がかかります。このため小規模から始める企業にはSaaS型が適します。

MDMの選び方のポイント

まずMDMで何を管理したいのかを明確にしておく必要があります。企業の業種や特性によって管理目的も異なりますが、大体共通するのは概ね次の事項でしょう。

・紛失/盗難時にリモートロックやワイプで情報を守りたい
・勝手にアプリをインストールさせたくない
・操作ログをみたい（アプリやWebサイトのアクセスログ/利用時間など）
・GPSで移動経路を残したい
・特定アプリのインストールを強制または削除させたくない
・スマートフォンやタブレット以外PCも一元管理したい
・端末の利用状況を知りたい　等々

MDMは、AppleやGoogle側が提供するAPIを基に作られているので、上記のうち出来ることは限られおり、それはどのMDM製品でも同じです。

以上から見てMDM選び方のポイントは、

１）管理画面の充実度

２）メーカーの信頼性とサポート体制

３）PCとの一元管理

４）価格に絞られます。

MDMの選定基準

４つのポイント

１）管理画面の充実度

例えば、社員100人のスマートフォンを管理する場合、マルチOSを一元管理できるのはもちろん、業務に差し障るアプリはインストールを禁止し、逆に業務効率をあげるアプリケーションはインストールされているかを確認する必要があります。

インストールされているアプリケーションの内容や数の一覧表示、そして禁止アプリをインストールしたときの対応処置（警告通知）が充実していること。また、100台がMDMによってきちんと管理されているかなど管理状態が一目で把握できなければ、管理する意味がありません。

これらを含め、かつ管理者の予備知識がなくとも直感的で使用しやすい管理画面というのは、重要なポイントになります。

２）メーカーの信頼性とサポート体制

MDMシステム自体まだ歴史が浅く、この2年間で急成長してきたサービスです。数多くのMDM製品が登場しては淘汰されている状況です。

長期間利用するにあたってメーカー、および信頼のおけるサービス提供者を選ぶことは非常に重要です。OSのアップグレードや新機種への素早い対応、機能追加や改善など積極的にバージョンアップを行っている製品であるかどぷかもチェックのポイントとなります。

サポート体制を確かめるには体験版を試みるのも良いでしょう。ホームページに記載された説明とは違い、実際に使用してみるとOS別に対応機能が異なったり、課金されたりするケースも多々あります。また、問合せに対して丁寧かつ迅速な回答が受けられるかも重要なポイントになります。

MDMの選定基準

４つのポイント

３）PCとの一元管理

スマートフォンやタブレットを管理する一番の目的は情報漏洩を防ぐことです。モバイルに限らず社内のパソコンも除外ではありません。

既存のIT資産管理ツールもありますが、別製品として導入するとそれぞれの管理画面が存在してしまい、コストや管理で負担がかかります。

モバイルデバイスと一緒に社内のパソコンも一元管理ができると二度手間が省けます。

４）価格

SaaS型サービスの場合MDM価格は、大体の製品が月額１端末当たり300円(税抜)ですが、初期費用にはメーカそれぞれ偏差があります。

また、中にはjailbreak/rootingの危険検知やGPSを利用した位置確認など機能によってはオプション料金という製品も少なくありません。

コストパフォーマンスはMDM選びにおいては重要なポイントです。

導入実績やマーケットシェアだけで導入を決めるより、やりたい事とそのコストを勘案し、費用対効果の計算をすることが非常に大事です。

2014年 国内主要15のモバイルデバイス管理(MDM) 製品比較表(2014.02月版)

サービス名		Airwatch	XenMobile MDM Edition	MobiConnect	Optimal Biz for Mobile	Symantec Mobile Management Suite	FENCE-Mobile RemoteManager	MobiControl	McAfee Enterprise Mobility Management	CLOMO MDM	SPPM2.0	MoDeM	IIJ Smart Mobile Managerサービス	MobileIron AppConnecet App Tunnel	法人スマートフォン基本セット	DME
開発元		米エアウォッチ	米シトリックス・システムズ	インヴェンティット	オプティム	シマンテック	富士通ビー・エス・シー	カナダSOTI	マカフィー	アイキューブドシステムズ	AXSEED	アセントネットワークス	インターネットイニシアティブ	モバイルアイアン	KDDI	デンマークExcitor
提供形態		クラウド、オンプレミス	パッケージ、クラウド	クラウド	クラウド、オンプレミス	パッケージ、クラウド	パッケージ、クラウド	パッケージ、クラウド	パッケージ	クラウド	クラウド、オンプレミス	クラウド、オンプレミス	クラウド	クラウド、オンプレミス	クラウド	パッケージ、クラウド
対応OS		・iOS 4.0以降 ・Android 2.2以降 ・Windows Mobile ・Windows Phone 7 ・BlackBerry 4.5以降 ・Symbian S60	・iOS 5.0以降 ・Android 2.2以降 ・Windows ・Pocket PC 2003 ・Windows CE ・BlackBerry ・Symbian OS	・iOS ・Android ・Windows Mobile 6.5	・iOS 4.x以降 ・Android 2.x以降 ・Windows XP/Vista/7/8	・iOS 5.0以降 ・Android 2.3以降 ・Windows Phone 7.5	・iOS 4.3以降 ・Android 2.1以降 ・Windows XP/Vista/7/8	・iOS 4.0以降 ・Android 2.3以降 ・Windows XP/Vista/7/8 ・Windows Server 2003/2008/2012 ・Windows Mobile ・Windows CE	・iOS 4.3以降 ・Android 2.3以降 ・Windows Phone 7/8	・iOS 4.3以降 ・Android 2.3以降	・iOS 4.3～6.1 ・Android 2.2～4.2	・iOS 5.0以降 ・Android 2.2以降	・iOS 4.2以降 ・Android 2.2以降	iOS、Android、BlackBerry、 Windows、Symbian	・iOS 5.0.1以降 ・Android 2.2.1以降	・iOS 5.0以降推奨 ・Android 2.2以降
主なMDM機能	Jailbreak/root化検知	○	×	○	○	○	○	○	○	○	○	○	×	○	×	○
	リモートロック	○	×	○	○	○	○	○	○	○	○	○	○	○	○	○
	リモートワイプ	○	×	○	○	○	○	○	○	○	○	○	○	○	○	○
	パスワード初期化	○	×	○	○	○	○	○	○	○	○	○	○	○	○	○
	端末のパスコード強制	○	×	○	×	○	○	○	○	○	○	○	○	○	×	○
	デバイス証明書	○	×	○	×	×	○	○	○	×	○	○	△	○	×	○
	カメラ利用制限	○	×	○	○	○	○	○	○	○	○	○	△	○	×	○
	Bluetooth利用制限	○	×	×	△	×	△	×	○	△	○	○	×	○	×	×
	WiFi接続制限	○	×	×	△	×	△	×	○	×	△	×	×	○	×	×
	デザリング利用制限	○	×	×	×	×	△	×	×	×	×	×	×	×	×	×
	USBポート利用制限	○	×	×	×	×	×	×	×	×	×	○	×	×	×	×
	データ暗号化	○	×	×	○	○	×	×	○	○	×	○	×	×	×	×
	URLフィルタリング	○	×	×	×	×	△	×	×	×	△	○	×	×	×	○
	禁止アプリの検知/アラート	○	×	○	○	×	○	×	○	○	×	○	×	×	×	×
	アプリストアー無効化	○	×	○	○	×	○	×	○	○	○	○	×	○	×	×
	アプリインストール無効化	○	×	×	×	×	△	×	×	×	○	○	×	○	×	×
	スクリーンキャプチャ禁止	○	×	×	×	×	○	×	○	○	×	×	×	×	×	○
	位置情報取得	○	×	○	○	○	○	○	×	○	○	○	×	×	×	×
	AD/LDAP連携	○	○	○	×	○	○	×	○	対応予定	Androidのみ対応予定	対応予定	×	○	×	○
主なMAM機能	アプリのラッピング	○	×	×	×	○	×	×	×	×	×	×	×	○	×	○
	アプリ単位のVPN	○	×	×	×	○	×	×	×	×	×	×	×	○	×	○
	アプリ単位のワイプ	×	×	×	×	○	×	×	×	○	×	×	×	○	×	○
	自社アプリ配信	○	×	×	○	×	×	×	○	○	○	○	○	○	×	○
	推奨アプリリスト	○	×	○	○	○	×	×	○	○	○	○	×	○	×	○
主なMCM機能	データのコンテナ化	○	×	×	×	○	×	×	×	×	×	×	×	×	×	○
	データ編集	○	×	×	×	×	×	×	×	×	×	×	×	×	×	○
	データの暗号化	○	×	×	×	×	×	×	×	×	×	○	×	×	×	○
	個別データ/特定フォルダ削除	○	×	×	×	○	○	×	×	×	×	○	×	×	×	○
その他の特徴		・エージェントとの通信状況を常時監視	●iOS ・構成プロファイルの削除を防ぐ仕組みを搭載	●iOS ・ユーザーによるMDM関連の構成プロファイルの削除を防ぐ ・MDM関連の構成プロファイルが削除された際に、管理者に通知する ・MDM関連の構成プロファイルやエージェントがアンインストールされても、ワイプだけは確実に実行できる ●Android ・エージェントのアンインストールを防ぐ仕組みを搭載 ・エージェントを停止する危険性のあるタスクキラー系アプリを強制制御 ・一定期間サーバへのアクセスがない端末を通知	●Android、Windows ・エージェントにパスワード設定 ●Android ・タスクキラーアプリによるエージェント停止の防止 ・デバイス管理者機能のオフを禁止 ・独自の設定画面機能（USBデバッグモードの設定画面を非表示、Android標準の設定画面を禁止）	・エージェントやMDM証明書の削除を検知可能 ・エージェントやMDM証明書の削除検知時の自動アクションを作成可能	●Android、Windows ・クライアントエージェントのアンインストール抑止 ●iOS ・構成プロファイルの削除検知 ●Android ・通常のエージェントとは別に予備のエージェントを動作させ、一方がアンインストールや停止された際に、もう一方を復活させる	・通常のエージェントとは別に予備のエージェントを動作させ、一方がアンインストールや停止された際に、もう一方を復活させる ・構成プロファイルには最低限のセキュリティ設定のみ記載するよう推奨 ・ランチャー機能の利用により、端末をキオスク（特定用途端末）化することが可能	・MDM機能がアンインストールされると管理画面に表示	●Android ・エージェントのアンインストールを防ぐ仕組みを搭載 ●iOS ・エージェントをアンインストールすると管理者にアラートを送信	・設定時間ごとに端末の死活監視を実施 ・クラウドサービス用サーバ、回線を全て冗長構成 ●Android ・通常のエージェントとは別に予備のエージェントを動作させ、一方がアンインストールや停止された際に、もう一方を復活させる ・電話のダイヤル操作で端末ロックやワイプが可能	・対象端末の管理状態を管理コンソールで確認可能 ●iOS ・MDM関連の構成プロファイルが削除されても、リモートワイプは動作可能 ●Android ・エージェントをアンインストールしようとすると、端末を利用できなくなるように設定可能	・通常のエージェントとは別のエージェントを動作させ、一方が削除や停止された際にもう一方を復活させる ・ユーザーがMDM関連の構成プロファイルを削除した際、管理者用のWeb画面に通知 ・構成プロファイルには最低限のセキュリティ設定のみ記載するよう推奨	・MDMサーバの冗長構成が可能 ・MDM関連の構成プロファイルが削除された場合、端末に警告メッセージを表示。警告メッセージをクリックするとエージェントが起動し、プロファイルを再インストール ・エージェントを「必須アプリ」として設定し、エージェントがアンインストールされた場合、ユーザーと管理者に通知を送信	●Android ・「デバイス管理者権限」設定の解除防止 ・エージェントを端末にプリインストールしており、セーフモードでの起動時にも動作	・データの強制同期機能 ・エージェント削除時にセキュアコンテナ内のデータを削除 ●Android ・強制的に管理者モードでログインするように制御 ●iOS ・Apple標準のMDM関連の構成プロファイルを削除すると、再インストールを試行
価格（税別）		初期費用：2万円 端末1台当たり年額3600円	端末1台当たり年額3450円から。	初期費用：3万円、端末1台当たり年額1800～3000円	初期費用：4万5000円、端末1台当たり年額3600円	メンテナンス含め単価10500円	端末1台当たり月額300円	初期費用：5万円 端末1台当たり月額500円	端末1台当たり1万8606円～。次年度以後は1台当たり3717円	端末1台当たり年額3600円、初期費用：2万円、管理パネル利用料年額：2万4000円	端末1台当たり月額150～300円、初期費用:iOSの場合4万5000円	初期費用：2万円 端末1台当たり月額300円、 ベーシックプラン： 初期費用なし、年額19800円	・初期費用：5万円 ・iOS:端末1台当たり300円・Andoroid：端末1台当たり150円	問合せ	初期費用：1000円、月額基本料金：1000円端末1台当たり300円	1ユーザー当たり年額1万4400円。初期費用：1ユーザー当たり1200円、構築費：25万円
有償オプションのセキュリティ機能		–	–	–	・アンチウィルス ・Webフィルタリング	–	●iOS、Android ・Webフィルタリング ●Android ・ウイルス対策	–	–	・マルウェア対策） ・デバイス認証用電子証明書 ・24時間365日のリモートロック／リモートワイプ代行サービス	・アンチウイルス ・データ暗号化 ・日本ベリサイン製デバイス証明書 ・URLフィルタリング ・アプリフィルタリング	・Android用マルウェア対策「Mobile Security Pro（MOSE Pro）」 ・ファイル暗号化 ・キッティング	—	・Docs@Work ・Web@Work	–	

用語解説

上記の比較表で使用されたキーワード

クラウド型	企業や組織外で提供されるインターネットを介したシステム形態
オンプレミス型	企業や組織内にネットワーク機器やサーバ等を構築して提供されるシステム形態
BYOD	Bring Your Own Deviceの略称。私
リモートロック	遠隔で端末の操作を制限する仕組み
リモートワイプ	遠隔で端末上のデータを消去する仕組み
セキュリティポリシー	企業や組織全体の情報セキュリティに関する基本方針
暗号化	内部メモリやSDカード等の外部メモリにおける保存領域の暗号化/復号化
MAM	Mobile Application Managementの略称。業務に関わるアプリケーションやデータを適切に管理する手法
MCM	Mobile Contents Managementの略称。業務に必要なコンテンツを適切に管理する手法
構成プロファイル	iPhone構成ユーティリティを使ってPhone/iPad/iPodの様々な設定を保存し、PCから一括適用できるソフトウェアツール
AD	Active Directoryの略称。ネットワーク上に存在するハードウェア資源やそれを使用するユーザの属性、アクセス権などの情報を一元管理するディレクトリサービス
LDAP	Lightweight Directory Access Protocolの略称。ネットワーク機器やユーザーなどの情報を管理するディレクトリサービスへ接続するためのプロトコル
エージェントアプリ	デバイスを管理するにあたり、MDMサーバと通信を行うために必要なMDM専用のアプリ
マルウェア	悪意のこもったソフトウェアのこと。遠隔でコンピュータに侵入して攻撃したり、情報を漏洩する有害なソフトウェア
Webフィルタリング	インターネット上で閲覧にふさわしくないtと判断したサイトをブラックリストに基づいて遮断すること

All in One MDM MoDeM

http://ascentnet.co.jp/mdm-modem/

株式会社アセントネットワークス

東京都千代田区九段南３－５－５グレース和平ビル3階
本資料に関するお問合せは下記までお願いします。
info@ascentnet.co.jp

Ascentnetworks
http://www.ascentnet.co.jp