MDMソリューション導入前に知っておきたい

モバイルデバイス管理(MDM)基礎講座

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

モバイルデバイス管理の登場背景

1.
Blackberryから見るMDMの登場背景

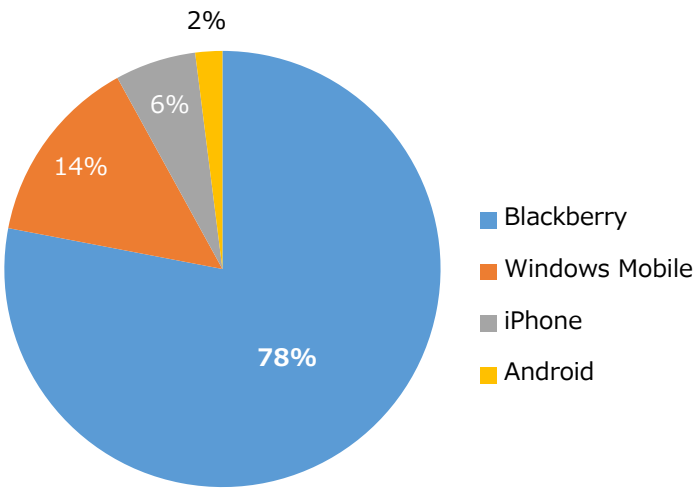
企業向けスマートデバイスの元祖Blackberry

企業ではかなり前から業務にモバイル端末を活用してきた。法人向け携帯電話が普及した時代にも携帯電話でメール確認をはじめ簡単な業務報告が行われ、電話帳の配布など簡単業務をしていた。

国内ではそれほど数多くのユーザ確保はできなかったが、最初の企業用スマート端末といえば、1999年カナダ企業RIMが製造したBlackberry 850 Pagerが挙げられる。Blackberry端末の代名詞であるキーボードとプッシュメール、そしてMS Exchange Serverと連動するBlackberry Enterprise Server (BES)を搭載したBlackberryは、iPhoneが普及されるまでアメリカとユーロッパで最大のユーザを獲得した企業用スマートフォンの象徴であった。

Blackberryは、2000年に最初のBlackberryのスマートフォンであるBlackberry957（Blackberry OS搭載）を発表、行政機関や金融企業などビジネスにおいて本格的業務用スマート端末に拡大され、アメリカのオバマ大統領やドイツのメルケル首相もBlackberryの愛用者で知られてる程、企業用スマートフォンとして成功し、iPhoneが登場した翌年の2008年９月までにBlackberryの使用者数は約2000万人に達した。

アメリカの企業で活用されるスマートフォンのシェア – 2010年



モバイルデバイス管理の登場背景

1.
Blackberryから見るMDMの登場背景

Blackberry導入効果

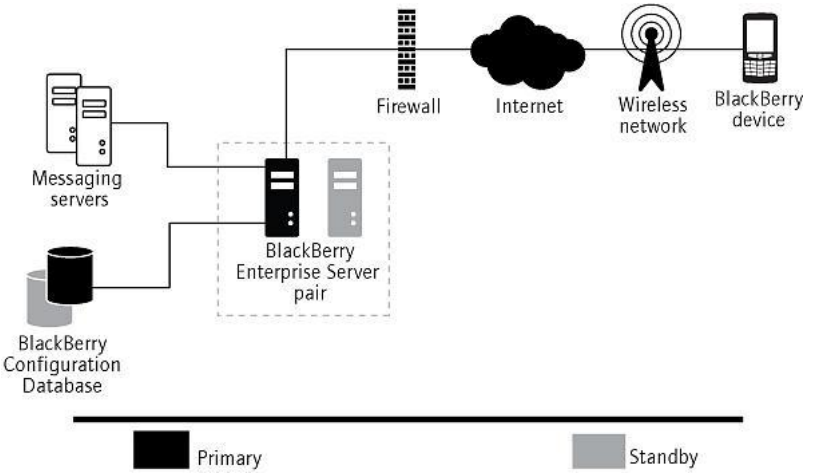
MDMの登場背景をBlackberryの説明からはじめたのは、企業がスマートフォンを活用することで業務効率や社員の満足度が上がる効果があったこと、またそれに伴うスマートフォンを管理する必然性を強調するがためである。
下記は「企業のBlackberry導入効果」を分析したものである。

ビジネス側面	社員の生産性向上	Blackberryを使用することでビジネス現場で費やす時間とコスト節減の効果が期待される。これにより業務全体の生産性が上がる。
	社員の満足度アップ	業務の自律性と遠隔コミュニケーションの増加で業務満足度が上がり、社員の離職率が減少する。
セキュリティ側面	コンプライアンス増進	SOX、PCI、HIPAA 等の企業が守るべきコンプライアンスに対する監視監督業務が増える。
	モバイルセキュリティ運営コストの節減	Blackberryで提供されるデータ暗号化などのセキュリティポリシーで使用者の端末を制御が可能、各使用者/端末の監視効率が上がる。

出所：Economic Impact Of A BlackBerry Solution In North American Enterprises, 2009

Blackberry Enterprise Server

Blackberryが企業で活用された圧倒的な理由の一つは、Blackberry Enterprise Server(NES)である。主要機能は、使用者管理、端末管理、ポリシー設定/配布、MS エクスチェンジサーバーとの連動、Data Encryption、リモートワイプなどの保安機能、そしてMAM(Mobile Application Management)機能など、今で言うMDMそのものだった。



モバイルデバイス管理の登場背景

2.
Blackberryから iPhone, Android時代へ

iOS、Androidの
Blackberry追掛け

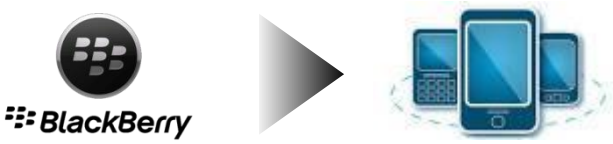
2009年半ば以降iPhone 3GSに対応するMDMソリューションがリリースされる。初期MDMベンダーたちはAppleのパートナーシップを組み、Blackberryで可能だったセキュリティをiPhoneでも実現できるように機能を増やした。
その結果、2011年から2012年に渡って企業でもセキュリティが強化されたiPhoneやiPad、Androidなどを活用する段階に入った。
つまり、ハードウェアの側面からみると、BlackberryがiOS、Android、Windowsに分散化されて、活用ソフトウェアの側面では、単一のBlackberryマーケットに比べ、多様で優秀なアプリケーションがApp StoreやGoogle Playに登場し、強力なセキュリティのBlackberryのBESサーバーはさまざまなMDMベンダーたちのソリューションに吸収されたと言える。

BES > MDMへ

HW：Blackberryから iPhone、Android、windowsへ

SW：BlackberryマーケットからApp Store Google Playへ

管理：Blackberry Enterprise Server から MDMへ



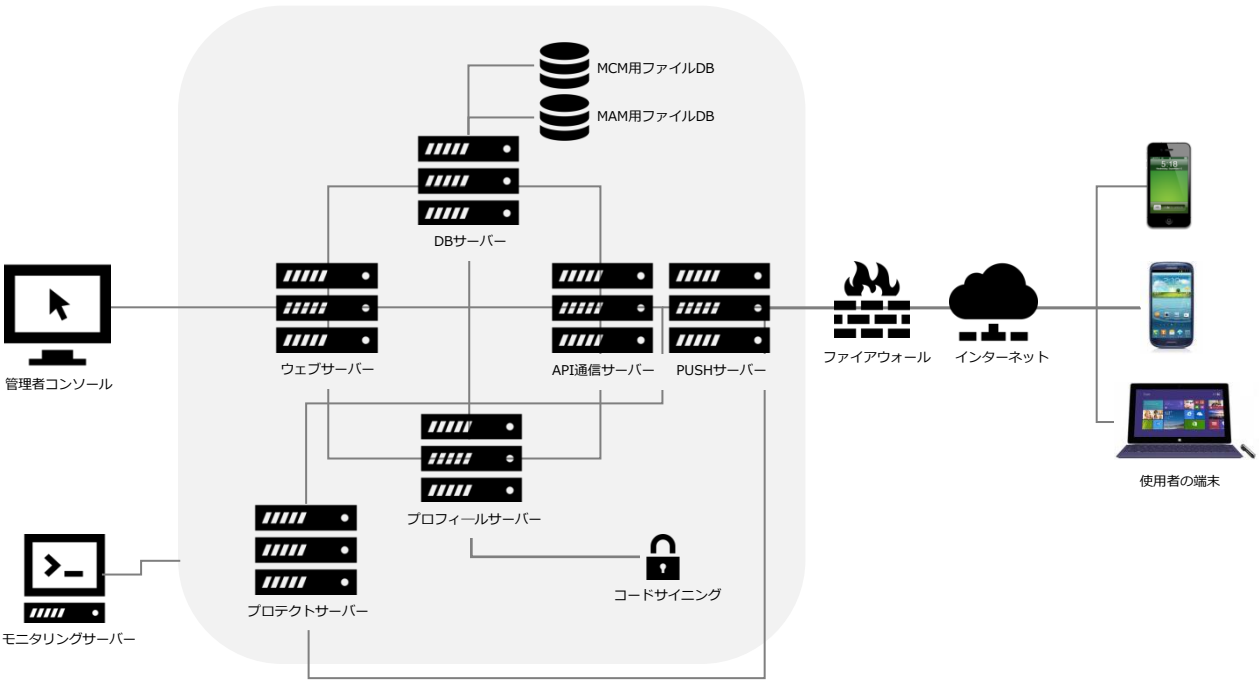
MDM

モバイルデバイス管理 (MDM) アーキテクチャ

MDM ソリューション構成図

MDM MoDeM Architecture

ここから MDMについて本格的に知っていこう。
まず構成を理解しよう。下図は MDM ソリューションの構成図だ。



管理者コンソール	ウェブインターフェースで管理者がデバイスを管理するコンソール。 デバイスロック、パスワード強制化、工場初期化、ポリシー設定および配布などを実施する。
ウェブサーバー	管理者コンソールから受けたリクエストをデータサーバー、API通信サーバー、プロファイルマネージャサーバーに転送する。
DBサーバー	デバイス情報、ユーザ情報、ポリシー情報などを保存する。 アプリケーションデータ、ドキュメントデータを保存する(1)
API通信サーバー	サーバーから受け取った管理者信号にしたがってユーザの端末にポリシーの配布、デバイスロック、工場初期化など実際にデバイスを管理する機能を果たす。 逆にユーザ端末から受け取った信号（位置情報、端末情報、アプリリスト等々）をDBサーバーに保存する。
プロフィールサーバー(2)	iOS 端末にデバイスロック、工場初期化、パスコード初期化などのMDM 機能を遂行する。
プロテクトサーバ	MDM プロファイル (MDM 機能を遂行させるプロファイルを端末にインストール) をユーザが削除した時に備えて実際削除されたらプロテクトサーバーより工場初期化を遂行する安全装置
PUSHサーバー	AndroidのGCM、iOSのAPNSのような方式でユーザの端末にプッシューメッセージを送信する。

(1) MAM(Mobile Application Management, MCM(Mobile Contents Management) 統合型 MoDeMに限る。
(2) プロテクトサーバーは二重安全装置で、国内 MDM ソリューション のなかではMoDeMとモビコネクトだけが提供している。

モバイルデバイス管理 (MDM) 機能

端末をMDMに登録 (Enrollment)

Enrollment

MDM 機能を使用するには、まず端末を MDM ソリューションに登録する必要がある。これをEnrollという。下図で登録するフローを説明しよう。

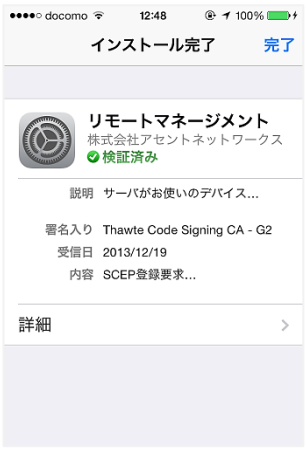
MDM ソリューションの管理コンソール(web)で端末追加機能でユーザに MDM プロファイルをインストールするように信号 (メール)を送る。

* 大量の端末で行うときは CSV ファイルを使って一括で登録することができる

管理コンソールから受けた MDMプロファイルを端末にインストールする。このMDMプロファイルこそが管理コンソールから端末を制御する役割をする。

注意）iOS、Android、Windowsの管理は端末利用者のその権限がまかされるので、インストールされた MDM プロファイルはユーザによって設定を解除したり、削除したりすることができる。MDMプロファイルが削除された端末は管理者が制御することができなくなる。

* MDM製品の中 MoDeMとモビコネクトが独自の仕組みでMDM無効化防止機能を提供している。



端末の登録は案内された順番通り進めれば誰でも簡単にできる。
端末登録が完了したら、左図のように「インストール完了」が記される。
この端末はこれから管理者の管理下で制御できる準備ができた。

モバイルデバイス管理 (MDM) 機能

MDMに登録された端末

管理コンソール（web）

端末登録が完了したら、管理コンソールに端末情報が次の①ように表示される。

端末に関する基本情報 はもちろん、本端末のjailbreak/rooting の検知もできる。

また、適用されているポリシーやインストールされているアプリを確認することができる。

②は、端末を制御する機能を表示している。次は端末管理/制御機能について紹介しよう。

モバイルデバイス管理 (MDM) 機能

1.
MDM 基本機能

MDMは OS 従属的

ここでまず理解しておくものがある。MDMはOSに従属するということである。つまり、OS側で提供する部分に対してのみ管理ができる。AppleのConfiguration Payload、GoogleのDevice Administration APIs、Windowsの Device Management Protocolが公開しているパートとの連携を通じて端末を制御することができるようになる。

MDMの基本機能

MDMの基本中の基本に該当するリモートロック、リモートワイプ、パスコード強制化など紛失や盗難時の対策がある。MDMに登録された端末の詳細情報、位置情報、端末所有者の情報および管理機能である。

MDM 基本機能 (iOS, Android, Windows 共通)		
ハードウェアの制御	リモートロック	紛失や盗難時に携帯電話を遠隔地からロックをかける
	リモートワイプ	リモートワイプ：全データを削除し、端末を工場出荷時の状態にする
	パスコード設定	単純なパスコードを許可：同じ文字の繰り返し、あるいは単純上昇/下降形（123、CBAなど）の文字列が含まれるパスコードを許可するか否かを指定 英数字の値が必要：英字（「abcd」など）を入力しなければならないか、または数字だけでよいかを指定 パスコードの文字数：パスコードの長さの最小値を指定 入力を失敗できる回数：設定回数を超えてしまうデバイスを工場初期化
端末管理	端末の位置情報	端末の位置情報を確認
	端末の詳細情報	UDID、ICCID、端末名、バージョン、モデル名、電話番号、シリアル番号、IMEI、使用可能な空き領域、バッテリー情報、ローミング状態、ネットワーク情報、MACアドレス、キャリア、セキュリティ情報（Jailbrake/Rooting）
	端末使用者の情報	端末所有者に関する情報登録・変更
	プッシュ通知	端末にプッシュ通知

次のページでひとつの機能を例に、図で説明する。

モバイルデバイス管理 (MDM) 機能

1.
MDM 基本機能

MDMの基本機能中、

パスコード設定

基本機能のなかでパスコードを設定してみよう。パスコード設定は、パスコードに 1つ以上の英数字を含める、英数字以外の文字の最小数指定など難しいパスコードを設定するようにできる。また、パスコード変更を要求するまでの日数を指定することで毎度新しいパスコードを維持するよう強制することができる。設定しようとする端末に信号を送ると、

管理者からパスコード設定信号を受けた端末はユーザにパスコード入力を要する。ユーザはこの要請を避けることはできない。「後で」を押して一時的にダイアログを非表示することはできる。

しかし、ダイアログは何分後に繰り返して表示されるので、管理者の設定要請に従わずに使用することは難しい。

モバイルデバイス管理 (MDM) 機能

2.
MDM 機能：iOS ポリシー

iOS Policy

iOSはバージョンがアップグレードされるほどより細かく管理できる機能を公開している。下記は iOS7.0に合わせられた iOS ポリシー機能だ。設定した後に端末に信号を送ると適用される。

MDM 機能 > iOS ポリシー設定	
機能制限	• iCloudのフォトストリームオプションを制御 • カメラの使用を制御 • スクリーンショット保存禁止 • AppStoreやiTunesを使用したアプリケーションのインストールやアップデートを禁止 • アプリケーション内の課金を禁止 • iTunesStoreパスワードの入力を強制 • ゲームセンターのマルチプレイヤーゲームのプレイを禁止 • ゲームセンターの友人追加禁止 • iCloudのバックアップオプションを制御 • iCloudの書類の同期オプションを制御 • ローミング中の自動同期を許可 • 音声コマンドを使用しての電話ダイヤルを制御 • 強制的に暗号化バックアップ • 信頼できないTLS証明書の受け入れを許可 • ユーザが信頼できないTLS証明書を受け入れることを許可 • Siriの制御 • スクリーンロック中にSiriを許可
コンテンツ制限	• YouTubeの使用を制御 • iTunesMusicStoreの使用を制御 • Safariの制御 • Cookieの受け入れ
プロファイル	• VPN構成 • Wi-Fi設定 • APN設定 • Exchangeアカウント設定 • メール設定 • Webクリップ設定
カレンダー/連絡先の設定	• CardDAVアカウントの設定 • CalDAVアカウントの設定
監視モード* (Supervised Mode)	• Airdropを許可：アプリでAirDropの使用を制御 • iMessageを許可：iMessageを使用したメッセージの送受信ができなくなる • iBook Storeを許可：iBooks Storeが無効になり、ユーザが「iBooks」アプリからiBooks Storeにアクセスできなくなる • Appの削除を許可：ユーザはアプリを削除できるようになる。App Storeや「iTunes」など、iOSに付属しているアプリをユーザが削除することはできない • Game Centerの使用を許可：「Game Center」が無効になり、ホーム画面からアイコンが削除される • 友達を探す設定の変更を許可：「友達を探す」アプリの設定を変更できなくなる • Apple Configurator以外のホストとペアリングを許可：デバイスを任意のMacと同期することができる
禁止アプリ	• 禁止アプリを設定
Webサイト制限 (監視モード)	• デバイスが表示できるWebサイトを選択 • アダルトコンテンツを自動的に除外 • 特定のサイトへのアクセスを許可または拒否

* 監視モードとは?
http://ascentnet.co.jp/mdm-modem/ios%E7%9B%A3%E8%A6%96%E3%83%A2%E3%83%BC%E3%83%89supervised-mode%E3%81%A8%E3%81%AF/

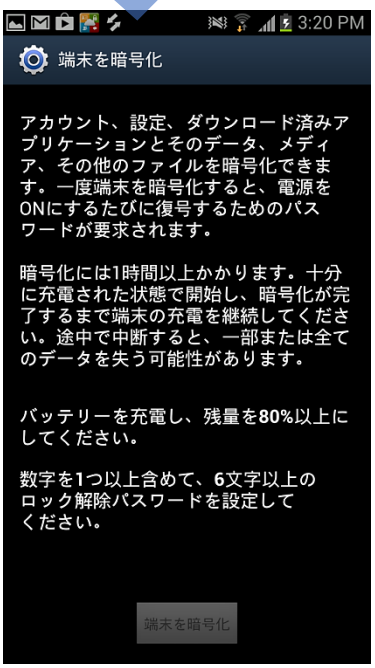
モバイルデバイス管理 (MDM) 機能

3.
MDM 機能：Android ポリシー

Android Policy

Androidは iOSに比べて制御する機能が少ない。しかし、4.X バージョンから発展し、今後はSELinuxの採用などでより強力なセキュリティ管理ができるようになると予想される。

MDM 機能 > Android ポリシー設定	
機能制限	• カメラの使用の制御 • SDカードの使用の制御 • Bluetoothの使用の制御 • デバイス「設定」へのアクセスを許可 • メール同期の使用を許可 • 端末設定機能へのアクセス禁止
コンテンツ制限	• YouTubeの使用の制御 • ブラウザの使用の制御 • Google Playの使用の制御：アプリのダウンロードを禁止
Data 暗号化の強制	• 端末内部の全データに暗号化を強制
APP管理	• 禁止アプリを設定
VPN	• PPTP • IPSEC • L2TP



このなかでも強力なセキュリティ機能はデータ暗号化強制機能だ。データを暗号化すると、紛失や盗難時に第三者による複製が不可能なた、データを守ることだできる。

管理者がデータ暗号化強制信号を端末に送信すると、ユーザに左図のような画面が表示される。

ユーザが暗号化設定をするまで左図の画面は繰り返して表示される。

モバイルデバイス管理 (MDM) 機能

4.
MAM機能

Mobile Application Management (MAM)

MAMは、Mobile Application Managementの略称で、厳密に言えばMDMに該当する機能ではない。しかし、多くの企業が MDMとアプリ（ソフトウェア）を一緒に使用することが一般化されている。

* MDM MoDeMは唯一 MDM-MAMが統合されたソリューションである。

MAM 機能	
アプリ管理及び端末への配布	• 自社開発アプリケーションの配布 • iTunes App Store 推奨アプリケーションの配布 • Google Play 推奨アプリケーションの配布
インストールアプリの管理	• 端末にインストールされているアプリのリストを管理画面に表示
Black List	• 禁止アプリをインストールしたとき、管理者に通知メールを自動送信 • 禁止アプリをインストールしたとき、強制リセット
VPP (iOS)	• Appleの Volume Purchase Programとの連動により、アプリを購入して配布する
OTA 配布	• Over the Air (アプリの強制インストール) でアプリ配布

MAM 機能のなかで強力な機能が OTAである。OTA（Over The Air）つまり、遠隔配布という意味で、管理者はユーザが手動でインストールしなくても遠隔でアプリをインストールさせることができる。

管理者がアプリを OTAで配布すると、下記のように自動でアプリをインストールすることができる。Apple IDとパスワードの入力が不要なのでユーザが気づかないうちにインストールされる。

有料アプリの場合、誰が料金を支払うのか問題が出てくるかもしれない。この問題を解決するために、AppleのVPPとの連携機能を提供する。VPPで管理者が有料アプリを購入しOTAで配布すればユーザは料金を払わずそのまま利用することができる。

モバイルデバイス管理 (MDM) 機能

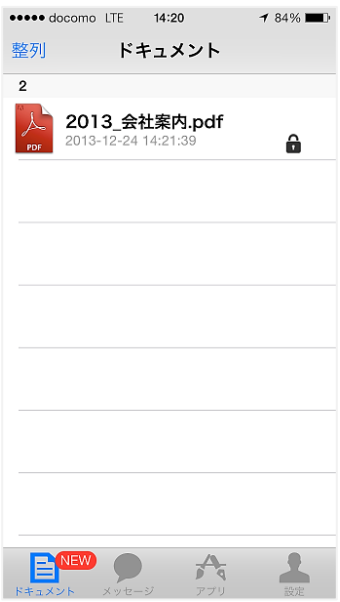
5.
MCM機能

Mobile Contents Management (MCM)

MCMは、Mobile Contents Managementの略称で、これもMDM の基本機能ではない。しかし、企業でDropboxなど管理されないアプリを介せずにファイルを転送するにはどうしてもMCM機能が必要となってくる。

＊ MDM MoDeMは唯一 MDM-MAMが統合されたソリューションである。

MCM 機能	
ドキュメント管理	• OpenInを使ったドキュメント閲覧（iOS） • ファイル表示時に縦横支援（iOS） • 配布ファイルの閲覧状況筧確認遠隔削除 • 配布ファイルの遠隔削除
ドキュメント配布	• doc/docx/pdf/xls/xlsx/mp3/mp4/pages/ppt/pptx/rtf/txt/png/jpg/gif/psd/numbers/keynoteなどのファイルを各端末に配布 • ドキュメントをフォルダ単位で配布
暗号化	• ファイルを暗号化して端末に配布 • USB接続してPCからのファイル抽出防止 • ネットワーク送信中のハッキング阻止



管理者が暗号化されたファイルを端末に配布すると、ユーザ端末に転送され、ユーザはファイルダウンロードして閲覧および編集することができる。

MDM ソリューションの導入

MDMソリューションの導入ポイント

ソリューション導入時のチェックポイント

2014年現在、国内にも多くのMDMソリューションがある。ソリューション導入にあたっての選択ポイントを参照し、自社に適合したMDMを選択することを推奨する。

MDM ソリューションの導入ポイント	
マルチOS 対応	大体はがiOSとAndroidに対応しているが、一部は片方OSだけ対応する製品もある。
アップデート	Apple 、Google両方も頻繁にアップデートするが、MDMもこれに素早く対応しなければならない。 よって、メーカーの公式ホームページで定期的に製品アップデータが行われているかを確認する必要がある。 中にはOSのアップデートに追いつかない製品もある。
トライアル版で事前確認	メーカーのホームページに記述された機能だけでなく、トライアル版で十分試した後に導入しなければならない。 メーカーごとにUIが違うので操作の利便性もそれぞれである。またホームページでは対応しているように記述されていても実際にはOS別対応だったりすることも多々ある。
価格	大体が端末1台あたり300円前後になっている。 基本機能に限定し、手頃な価格のソリューションを求めるなら、MoDeMの Basic Plan、または CLOMOZeroをお勧めする。

国内 MDMソリューション比較

国内主要15社のソリューションの比較 (2014年 3月基準)をダウンロードし、比較検討の後、トライアル版の試用後に導入を決めることをお勧めする

2014年 国内主要15の
モバイルデバイス管理(MDM)製品比較表

内容：MDMを導入時の選ぶポイントとMDM製品の比較
対象：MDMの導入を検討される方
ページ数：5ページ(A4)+1ページ(A3) 比較表
ファイル：PDF

http://ascentnet.co.jp/mdm-modem/mdm%E8%B3%87%E6%96%99/

MDMの未来

企業内の主要インフラとして、ウェアラブルへの対応

多様な役割で拡大予想

スマートフォンは電子機器に留まらず、
個人の身分証明書や物を買える電子財布としても活用されている。
企業で認証されたスマートフォンは入退室時のIDカードに代わったり、または会議室予約などに活用される。

そして、備品の購入申請など手間がかかる業務にもスマートフォンを使用できる。また社員証のIDと連携処理されるなど企業内の多様な業務処理に応用される可能性を秘めている。

ウェアラブル機器対応予想

Google glassは企業や組織でも応用される可能性が増えてきた。アメリカの場合、一部の病院や物流センターでGoogle glassを活用した業務を試験的に実施している。病院で使用されるGoogle glassは患者を識別するなど重要なデータを保有することになる。したがって、スマートフォンやタブレットのようにGoogle glassをはじめ、引き続き出てくる多様なウェアラブル機器たちのMDMによって管理されるだろう。

上の写真はGoogle glassが病院で患者診療に活用できる可能性を示している。
参考動画は以下で参照可能。
https://www.youtube.com/watch?v=8uoBahl4zQ8

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いたします。
info@ascentnet.co.jp

Ascent networks
http://www.ascentnet.co.jp