MobileIron®

MDMからEMMへ、進化するモバイルファーストプラットフォーム

MOBILE FIRST

MDMからEMMへの進化
企業モバイルのプラットフォーム

第一世代のMDMの役割はロック、ワイプといったデバイスの基本的な管理機能のみでした。その後、モバイルの本格的な業務利用に伴い、アプリやその中に含まれるコンテンツをいかにセキュアに管理するか？すなわちMAMやMCMといった機能がMDMに追加されてきました。これらを全て含んだ次世代MDMは、EMM: Enterprise Mobile Managementという新しいカテゴリーに進化しました。

MDM: Device

- マルチOS対応
  - iOS7/Android/Windows 8.1/BlackBerry
- セキュリティポリシー強制
  - パスワード、暗号化、JB/Root化検知
- 資産情報管理
  - 機種、OS ver、電話番号、シリアル番号等
  - 企業全体のアプリ一式
- 定義情報配布と削除（セレクティブワイプ）
  - Provisioning Profile/WiFi/VPN/Active Sync
  - アプリ毎の証明書配布と削除

MAM: App

- App@Work（企業版AppStore）
  - アプリの更新、VPPに対応
- App Configuration（アプリ設定情報配布）
  - AD/LDAP連携も可能
- App Connect（アプリのコンテナ化）
  - Open-in、Copy&Paste、印刷の制御
- App Tunnel（アプリ毎のトンネリング）
  - 証明書認証でユーザー負担なし
- App Control（アプリのホワイト・ブラックリスト）
  - サイレント（アン）インストール対応

MCM: Contents

- メール添付ファイル保護
  - 添付ファイルのコンテナ化と暗号化
  - 専用ビューアと編集機能
- 社内ファイルサーバーセキュアアクセス
  - SharePoint, WebDav, CIFS対応
  - 端末へのセキュアなコンテンツ保存
- 社内Webサーバーセキュアアクセス
  - URL配布機能
  - Open-in, Copy&Paste、印刷の制御による情報漏洩防止

Atlas

- 運用管理：レポーティングツール
  - OS毎の一覧表示等、各種テンプレート
  - あぶり出し機能：ポリシー違反一覧等
- グローバル対応
  - 複数管理者と権限委譲機能
  - 日本語含むマルチ言語対応
- さらなる拡張性
  - 複数VSPの一元管理機能
  - csv形式によるデータ外部抽出

VSP

- インベントリーとセキュリティポスチャ管理
  - ハードウェア（モデル、シリアル等）
  - ソフトウェア（アプリ一覧）
- 各種コマンドとポリシー・コンフィグ配布
  - セキュリティポリシー強制
  - 定義情報強制（WiFi/VPN等）
- Web APIによる外部システムとの連携機能
  - ダイナミックポリシー(Assemble)
  - Cisco/Aruba等インテグレーション

Sentry

- 認証機能
  - アプリ、ActiveSyncアクセス認証
  - 証明書をもちいた認証
- トンネリング機能
  - アプリ単位でのトンネリング
  - https/SSL管理
- プロキシ機能
  - ActiveSync情報の外部露出の防止
  - Webトラフィックプロキシ

Mobile First: 4つのユースケース

メール、グループウェアのモバイル展開
ホワイトカラーの生産性向上

ユースケース

- Microsoft ExchangeやIBM Lotus Notes等のActiveSyncメールをモバイルで閲覧、かつメールのコンテナ化による添付ファイルの情報漏洩防止、ほか
- 社内Webシステムへのセキュアなアクセスのためのセキュアブラウザ機能
- 証明書をベースにした多要素認証の導入（特許取得）

事例

- 総合電気A：2万台以上のiOS管理
- 総合電気B：1万台以上のAndroid+iOS混在環境の管理

BYOD: 公私分離機能による
セキュリティとプライバシーの両立

ユースケース

- 公私分離による企業領域（メール、PIM、企業アプリ、社内コンテンツアクセス）と個人領域の分離による情報漏洩の防止
- 端末紛失時や退職時などのセレクティブワイプ（特許取得）によるプライバシーを考慮したセキュリティ確保
- BYODポータル機能による登録作業の負荷軽減と、同時に持ち込み台数制限、機種制限、利用規約遵守等ポリシー適用

事例

- 製造業（機械）C：全社規模のBYOD顧客、LotusNotes連携。
- 製造業（自動車）D：全社規模のBYOD顧客、Lotus Notes連携、さらにセキュアブラウザやアプリコンテナ利用。

Office365/Google App等
クラウド利用と認証によるアクセス制御

ユースケース

- Office365やGoogle Apps（Gmail, Drive）のモバイル利用
- 端末証明書と連携する形で、SAML/SSOサイトでの認証行為と、クラウドアカウント（IDとパスワード）をユーザーに秘匿することによる個人端末からのアクセス制限
- MDMサービスのクラウド提供（Connected Cloud: SOC2 Type2準拠のデータセンターまたは販売代理店による国内データセンター））

事例

- 製造業（建機）E、製造業（化学）F：Google Appを認証基盤との連携によるクラウドサービスに対するアクセス制御、セキュアブラウザによるデータを端末に残さない利用、AppConnect/Tunnelによるデータを残すがコンテナによって情報漏洩を防ぐ仕組み。

モバイルのキオスク利用
汎用的なモバイルを業務専用端末に

ユースケース

- Apple Single App ModeによりiOS端末を業務専用端末化
- サムスンKIOSKモードによるシングル、マルチアプリ対応
- アプリ配信、企業版AppStore（特許取得）と大規模アプリ配信のためのApp Delivery Network（Akamai相当）
- マルチユーザーによる端末の共有利用への対応

事例

- 鉄道G：車両運行乗務員業務
- 航空H：キャプテン、キャビンアテンダント、グランドスタッフの各種業務
- 小売りI：店頭販売員の接客業務
- 放送J：記者による取材業務

Mobile@Work

MDMサーバーと連携するためのエージェントアプリ。
最初にAppStoreからダウンロードする必要があります。

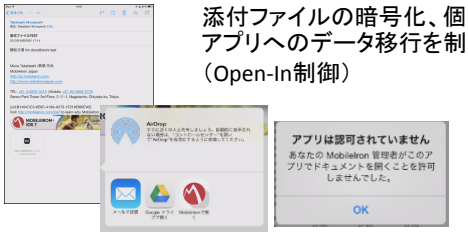
Web@Work

独自のセキュアブラウザー。Sentryサーバーと組み合わせる事でイントラネットWEBサイトへのセキュアなアクセスを保証します。

Apps@Work

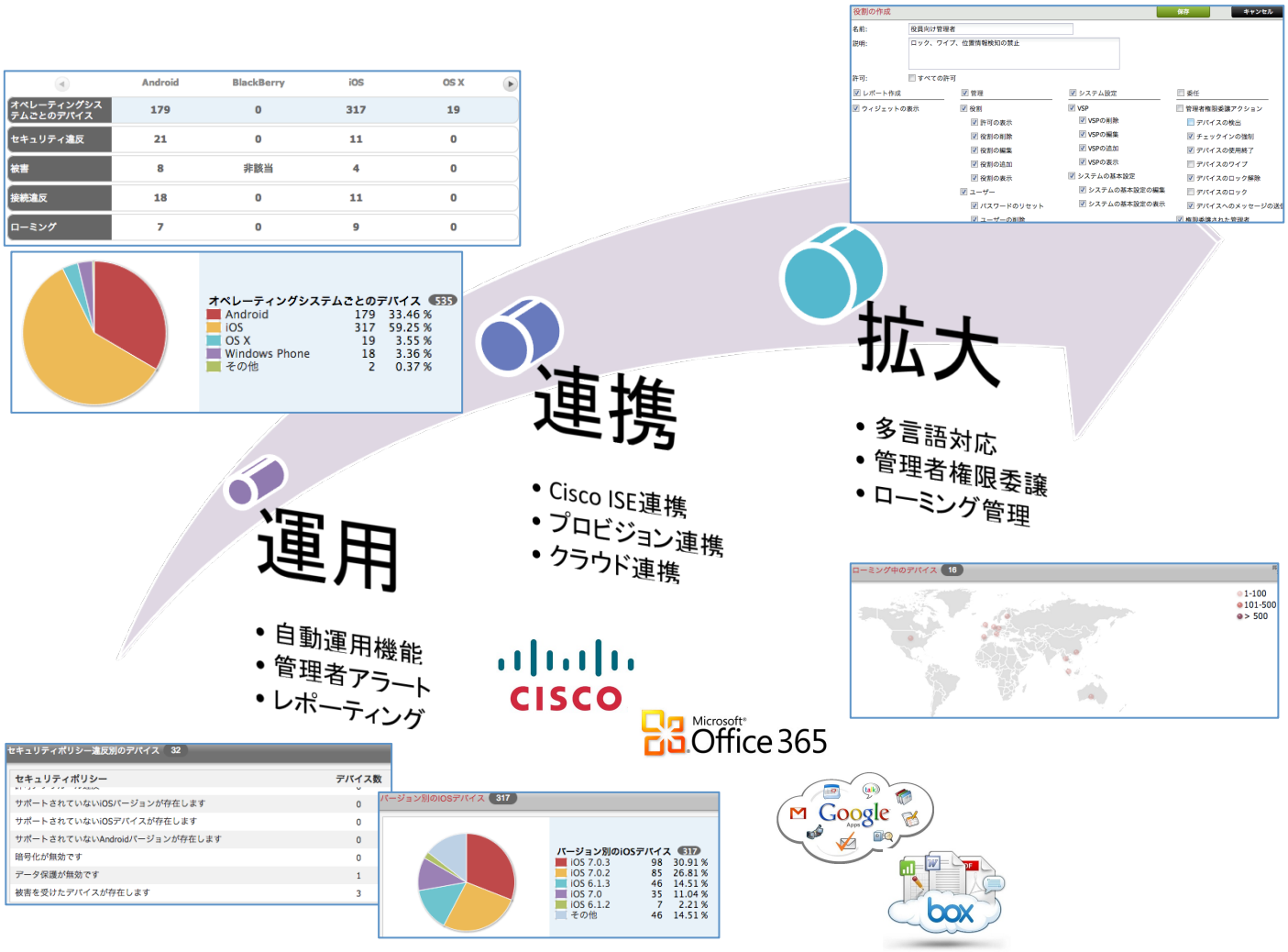
企業が許可したアプリを効率的に配信。（AppStore/Google Play アプリ、セキュアアプリ、自社開発アプリ、VPPなど）

iOSメール+Sentry



添付ファイルの暗号化、個人アプリへのデータ移行を制限（Open-In制御）

運用開始後のさまざまなサービス



メーカー参考価格

	バンドル製品				単品
	プレミアム バンドル	ウェブ バンドル	ドック バンドル	アップ バンドル	アドバンス マネジメント
MDM	√	√	√	√	√
MAM（AppConnect/Tunnel)	√			√	
MCM(Docs@Work)	√		√		
MCM(Web@Work)	√	√			
Perpetual 永続ライセンス	16,000円 保守別途20%／年	11,900円 保守別途20%／年	11,900円 保守別途20%／年	14,000円 保守別途20%／年	9,000円 保守別途20%／年
Subscription 毎年支払い	9,600円／年 800円／月 保守込み	7,200円／年 600円／月 保守込み	7,200円／年 600円／月 保守込み	8,400円／年 700円／月 保守込み	5,400円／年 450円／月 保守込み
含まれる主な機能（共通） 管理サーバライセンス （VSP, Atlas, Sentry、他） アップグレードライセンス 最新OS対応 （iOS7, Windows 8.1、他）	右記すべての機能	セキュアブラウザ	メール添付ファイルコンテナ セキュアファイルビューア MS Sharepoint WebDav	企業ペルソナ アプリコンテナ SDK/ラッピング アプリVPN App Sentry	App@Work Mail Sentry Atlas CA連携 AD/LDAP連携 定義情報配布管理 ポリシー管理

MobileIron
モバイルアイアン・ジャパン
〒100-6162 東京都千代田区永田町2-11-1 山王パークタワー3階
TEL : 03-6205-3414
Email : japan@mobileiron.com　日本語資料 : www.mobileironjapan.com
Homepage : www.mobileiron.com/ja　Twitter : @mobileironjapan

2013年10月版