

DW307

【株式会社リコー様】
リコーグループのデジタル革命と
モバイルデバイスマネージメント

株式会社リコー
デジタル推進本部 セキュリティ統括部
シニアスペシャリスト 和久利 智丈 様

#vforumjp

POSSIBLE
BEGINS
WITH YOU

リコーグループの デジタル革命と モバイルデバイス マネージメント

RICOH
imagine. change.

東京：2018年11月14日（水）

大阪：2018年12月14日（金）

（株）リコー
デジタル推進本部
セキュリティ統括部
和久利 智丈（わくり ともたけ）

vmware[®]

【免責事項】

本資料は、リコーグループのモバイルデバイスに関する担当者の意見であり、リコーおよびリコーグループの今後の方向性を約束するものではありません。

【本日の内容】

リコーグループではクラウド型グループウェアをグローバルで導入し、社内コミュニケーションをオープンにすると同時にワークスタイル変革の一環としてモバイルデバイスの活用を実践しています。その一方で情報セキュリティの一環としてモバイルデバイス管理の重要性も求められています。リコーではWorkspace ONEを導入することで、「改革」と「セキュリティ」の実現を目指しています。この講演では実際の担当者からの視点で「導入」「展開」「運用」時に発生した様々な課題と解決策を紹介していきます。

リコーグループの紹介

RICOH
imagine. change.

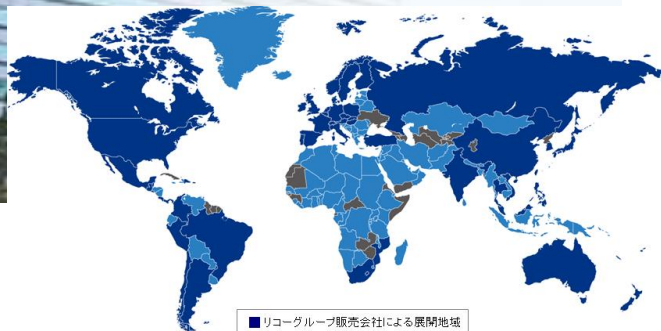
設立：1936

連結売上高：2兆633億円

売上高比率：国内/38.8%、海外/61.2%

約200の国と地域で販売・サービス展開

グループ従業員数：98,519名



*2015年9月現在

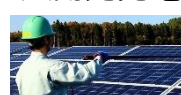
3Dプリンタ



脳磁計測



太陽光発電



サーマルメディア



時計



社員比率：国内/34,404名、海外/64,115名

国内主要子会社：リコー・ジャパン

迫リコー、リコー・インダストリー、山梨電子工業、リコー・エレメックス、リコー・テクノロジー、リコー・リース、リコー・クリエイティブサービス、リコー・ロジスティクス、リコー・ITソリューションズ、リコー・インダストリアルソリューションズ、リコー・電子デバイス、リコー・イメージング

360度全天球カメラ



車載用ステレオカメラ



インタラクティブ・ホワイトボード



TV会議システム



その他分野

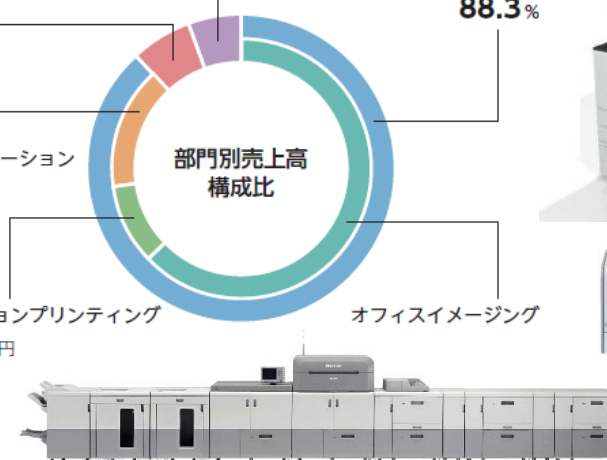
1,119億円
5.5%

産業分野
1,248億円
6.2%

ネットワーク
システムソリューション
3,109億円
15.3%

プロダクションプリンティング
2,062億円
10.2%

画像&ソリューション分野
17,920億円
88.3%



オフィスイメージング

「人々の“はたらく”をよりスマートに」に徹底的にこだわる

誰に対して

“はたらく”人々(個々人の個性を生かす)

何を

さまざまなワークプレイスの変革

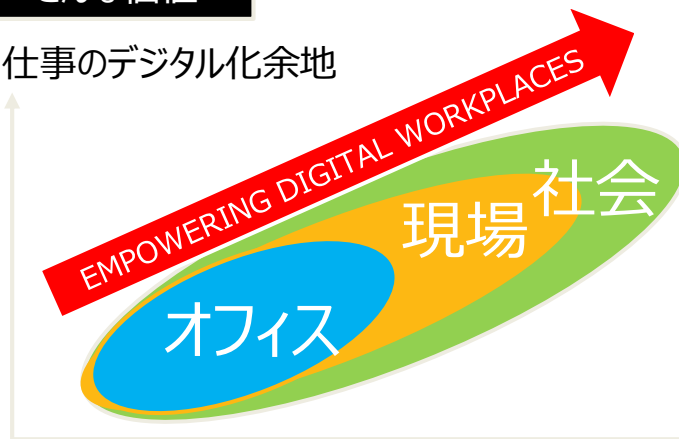
どういう手段で

テクノロジーとサービスのイノベーションでお客様とともに

どんな価値

“はたらく”をよりスマートに

B)仕事のデジタル化余地



A)価値提供領域の広がり

中期計画2017より抜粋

国内最大の利活用事例のベストプラクティスを元に他社に展開。日本の「働き方」を変革する



DIGITAL WORKPLACE

各従業員がいつでもどこでも働けるDIGITAL WORKPLACEを提供する

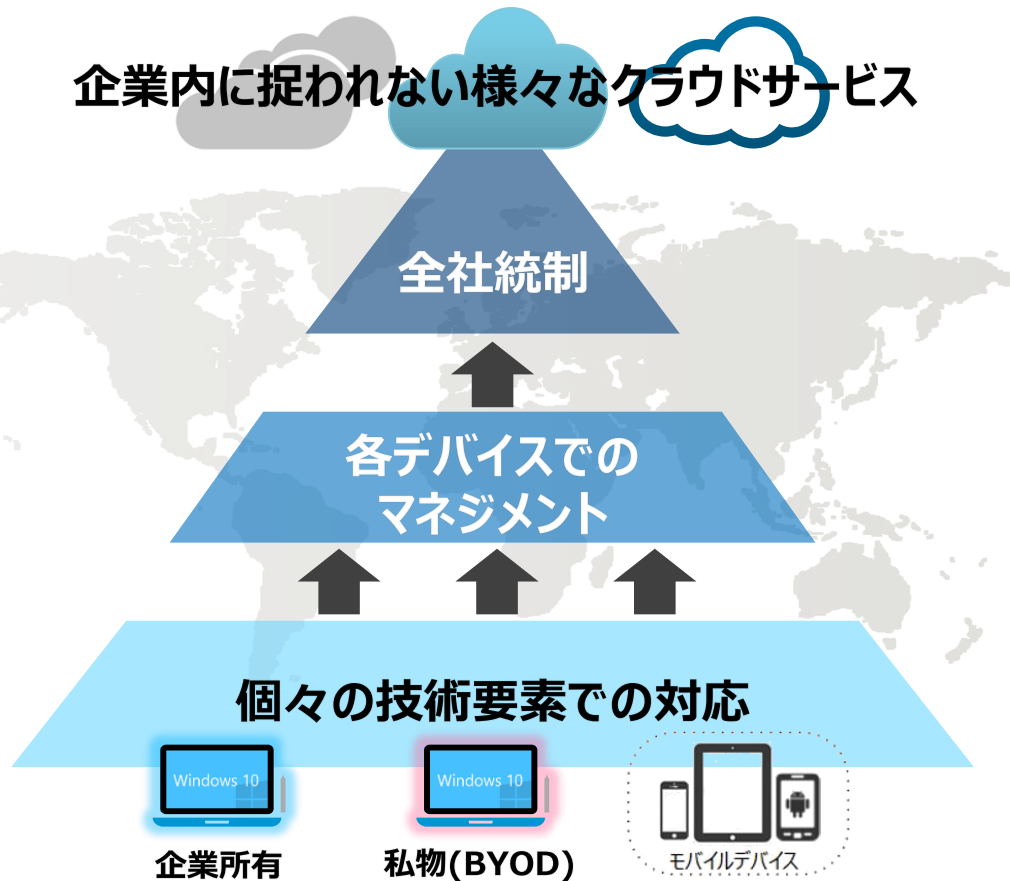
DIGITAL TRANSFORMATION

デジタルで働ける領域を増やし働き方そのものを変革する
「デジタル トランスフォーメーション」を推進する

「新しい働き方」の実現にも適切に統制されたセキュリティマネジメントが必要

グループ全体のセキュリティ強化

企業内に捉われない様々なクラウドサービス



デバイスマネジメントの方向性

目指す姿

全社統制

企業の情報を利用する全てのデバイスにおいて「誰が」「どのデバイスで」「何ができる」が適切に把握・管理された状態で必要な情報にアクセスでき働きやすいワークプレイスが提供できている状態

各デバイス マネジメント

各デバイスにおいてセキュリティ対策や利用できるアプリケーションが個々にマネジメントされ、バラつきなく利用者が必要な情報にアクセスできる状態

個別対応

個々の技術要素で個別にセキュリティ対策を実施しているが、実施できる内容にばらつきや差があり、使いにくい状態だが、最低限必要なセキュリティ対策が実施されている状態

日本一の活用事例(ベストプラクティス)を元に社会全体の問題の解決へ

中期経営計画

EMPOWERING DIGITAL
WORKPLACES

グループ全体のセキュリティ強化

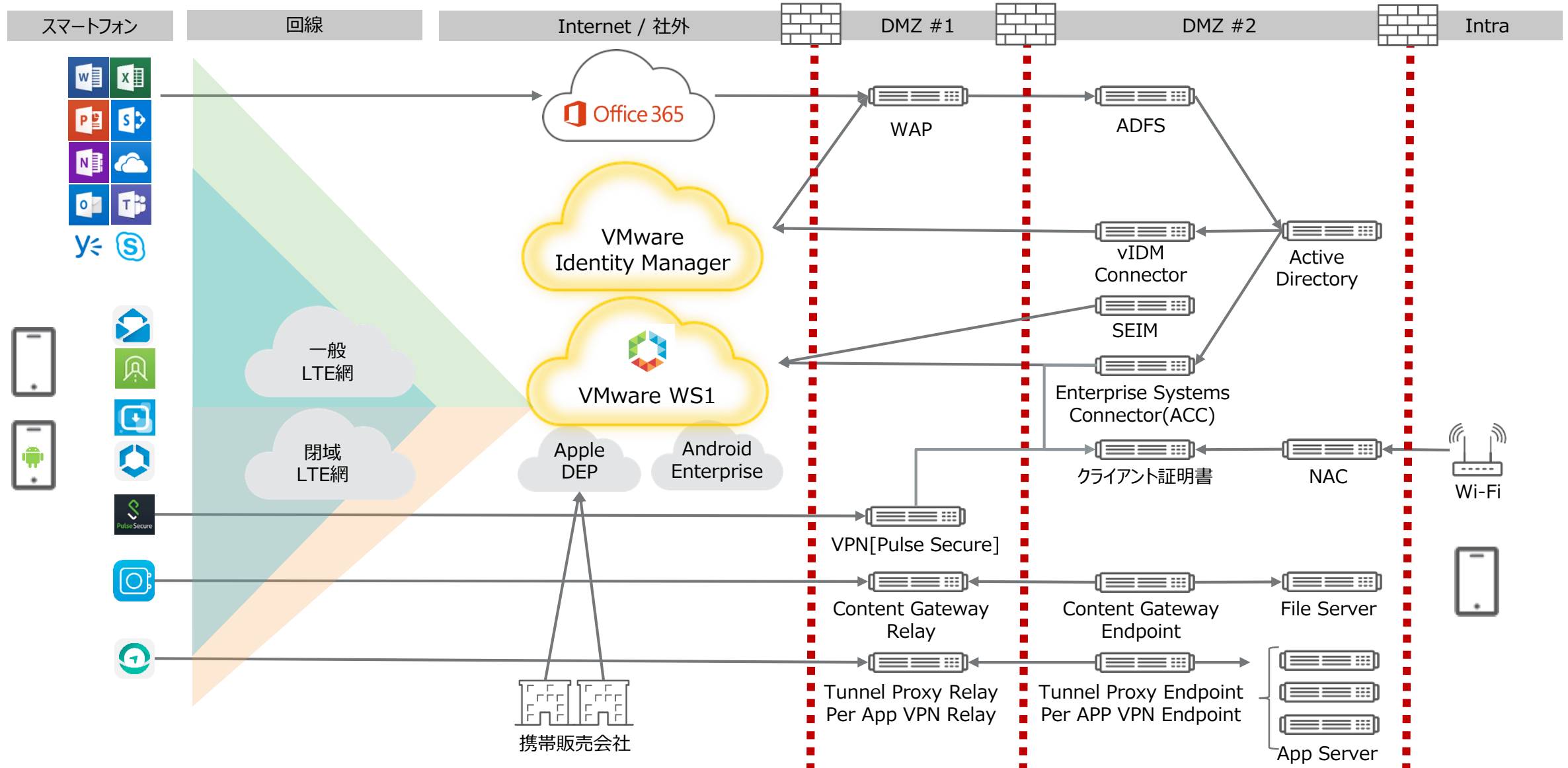
誰にでも使えて
利便性が高い

企業が求める
セキュリティを保てる

Workspace ONEのコンセプト



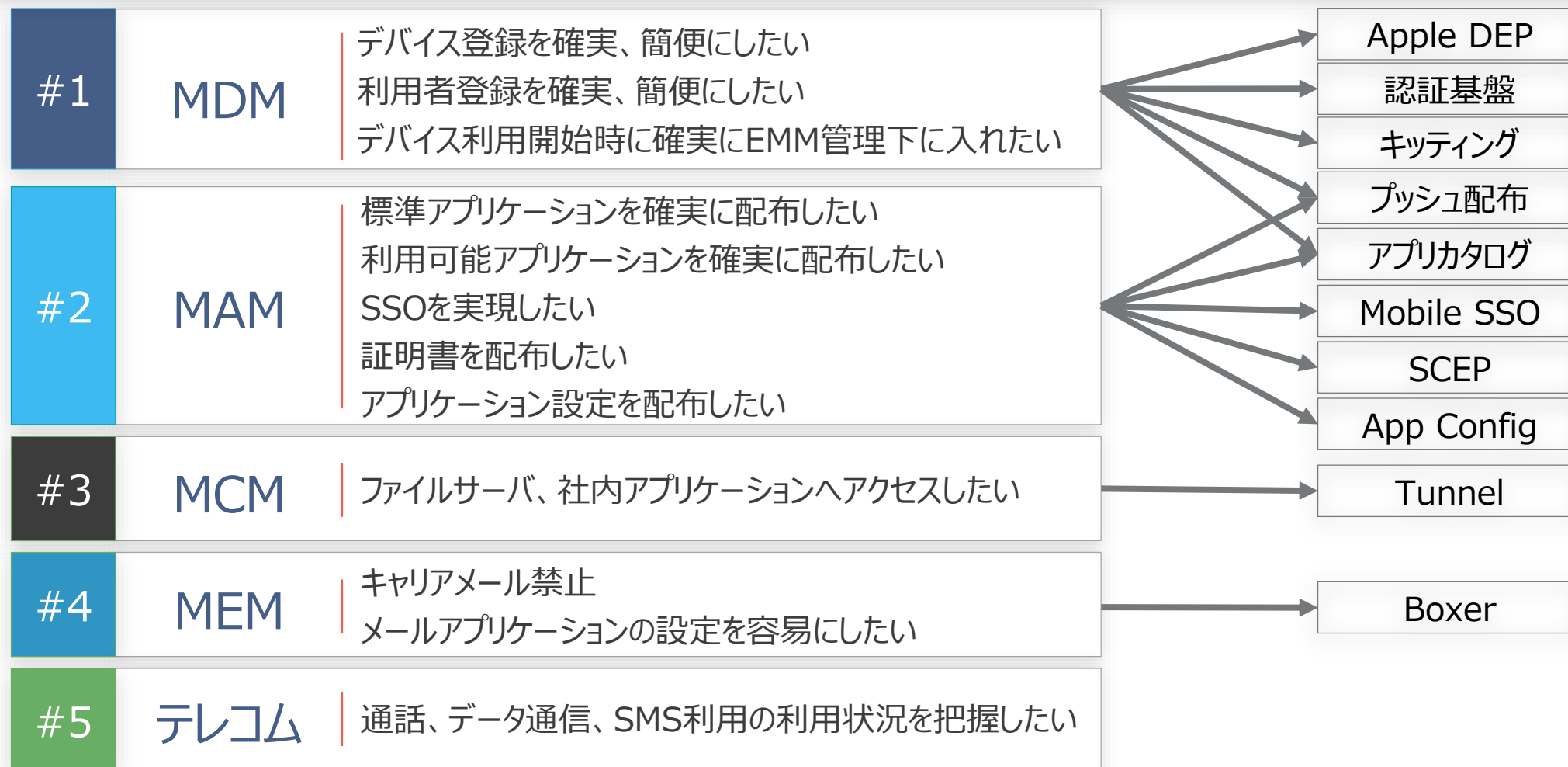
VMware Workspace ONEシステム全体像



MDM/MAM/MCM/MEMの要素から構成されるモバイル端末管理のしくみ

#1	MDM	デバイス管理
#2	MAM	アプリケーションの配布および設定
#3	MCM	コンテンツ管理
#4	MEM	メールの管理
#5	テレコム	通話、データ通信、SMS利用の管理

単なるセキュリティだけでなく、ユーザの利便性、提供側の設定、運用まで効率化できる



Device Enrollment を利用すれば、モバイルデバイス管理 (MDM) への登録を自動化し、デバイスの初期設定を簡単に済ませることができます。デバイスのアクティベーション中に本体に触れることなく監視し、継続管理のため MDM への登録を強制することができます。 引用:<https://support.apple.com/ja-jp/HT204142>

- | | | | |
|----|----|--|----------------|
| #1 | 登録 | | 登録情報と環境に課題 |
| #2 | 展開 | | 携帯販売会社との連携時に課題 |
| #3 | 運用 | | 登録内容の変更時に課題 |

Apple ID/SMS/番売店ID/D-U-N-Sが必要

- #1 AppleID | 自分のメールアドレスで登録 ⇒ 後に課題
- #2 SMS | DEPではApple IDは2ステップ認証が必須、携帯が必要
- #3 D-U-N-S | D-U-N-Sとは？ Safariのみ登録可能？

【D-U-N-S 番号の取得と管理】 引用:<https://developer.apple.com/jp/support/D-U-N-S/>
D-U-N-S 番号の申請後、D&B から番号を受け取るまで最大 5 営業日かかります。D-U-N-S 番号作成プロセスを優先的に行うよう依頼しても、この期間は短縮されません。申請処理に 2 週間以上かかっている場合は、D&B に E メールでお問い合わせください。

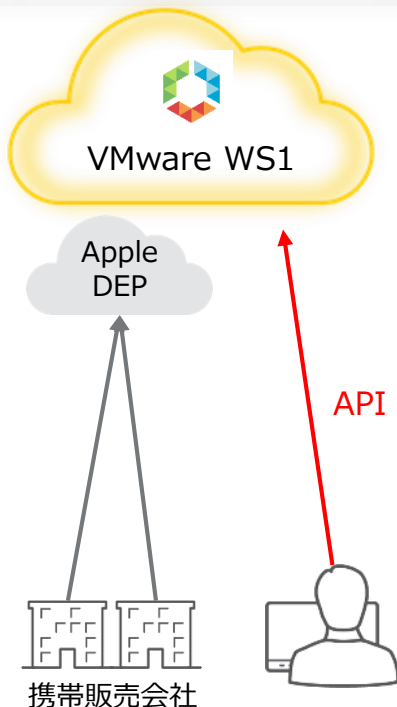
お客様が D-U-N-S 番号を受け取った後は、Apple が D&B からお客様の情報を受け取るまで最大 2 営業日かかります。この期間が経過した後は、Apple Developer Program で企業／組織として登録できます。

D&B プロファイルを更新するには、D&B に E メールでお問い合わせください。D&B が Apple に最新情報を提供するまで最大 2 営業日かかります。

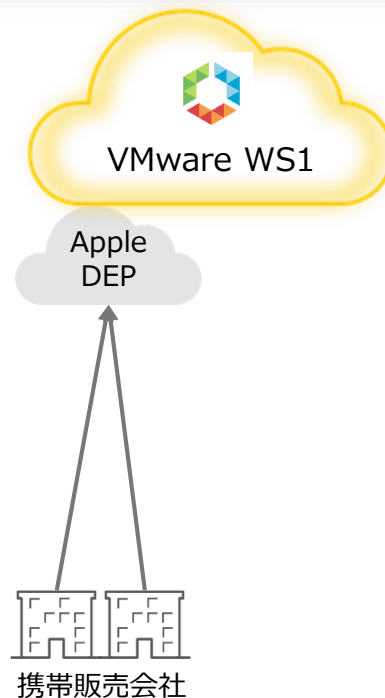
DEP(Apple Device Enrollment Program) #3

携帯販売会社との連携ミスにより、UAT環境に登録が発生（約800台）
WS1コンソールからは1台ずつしか削除できず、APIを使い、一括削除

UAT
(User Acceptance Test)



Prod
(Production)



Deployment Programs

デバイスが利用可能です

NTT DOCOMO,INC.が代行して提出したデバイスは、2018年10月29日 04:57 (GMT) にAppleが受理し、ご利用のApple Device Enrollment Programアカウントへ登録されました。

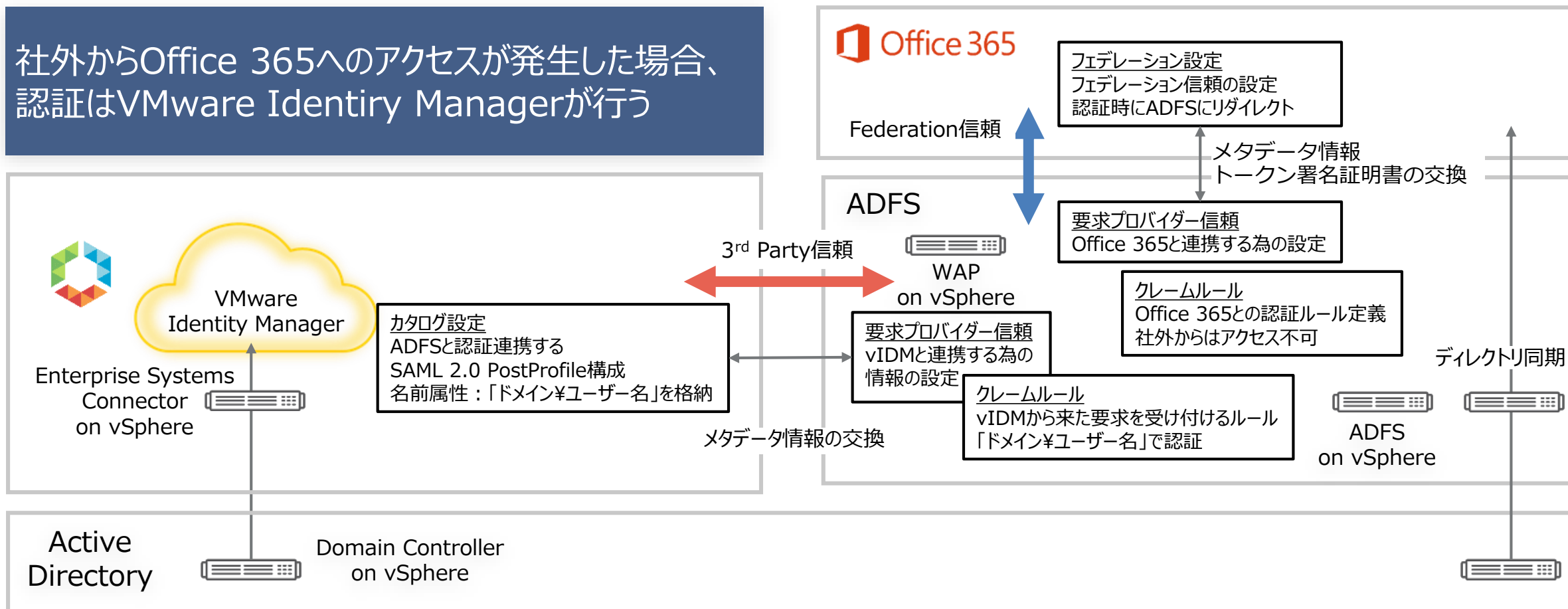
注文番号	注文日
201810291356OR64435	2018年10月28日
201810291357OR63369	2018年10月28日
201810291358OR63370	2018年10月28日
201810291359OR63371	2018年10月28日
201810291359OR64436	2018年10月28日

DEPは非常に便利、一方で導入時に管理体制をよく考えることが必要だった

- #1 AppleID | 管理者IDがシステムに組み込まれ変更が難しい
- #2 規約変更 | 規約変更が発生すると同意するまでDEP登録が停止する
- #3 登録通知 | 毎日大量の登録通知のメールが配送される

■ 認証の仕組み ~Office 365連携~

認可されたスマホからのみOffice 365へアクセスを許可



■ 認証の仕組み ～証明書配布～

証明書管理はWS1と連携し管理上の課題を解消

#1

利用シーン

- 無線LAN接続時の認証(802.1x)
- VPN接続時の認証（多要素認証）

#2

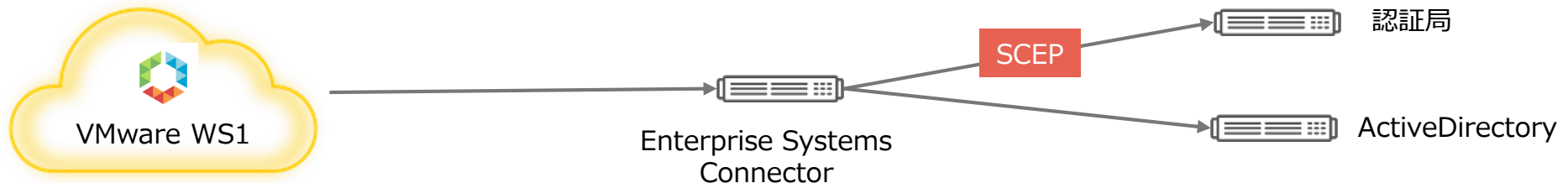
課題

- 発行の手間
- インストールの手間
- 失効管理の手間

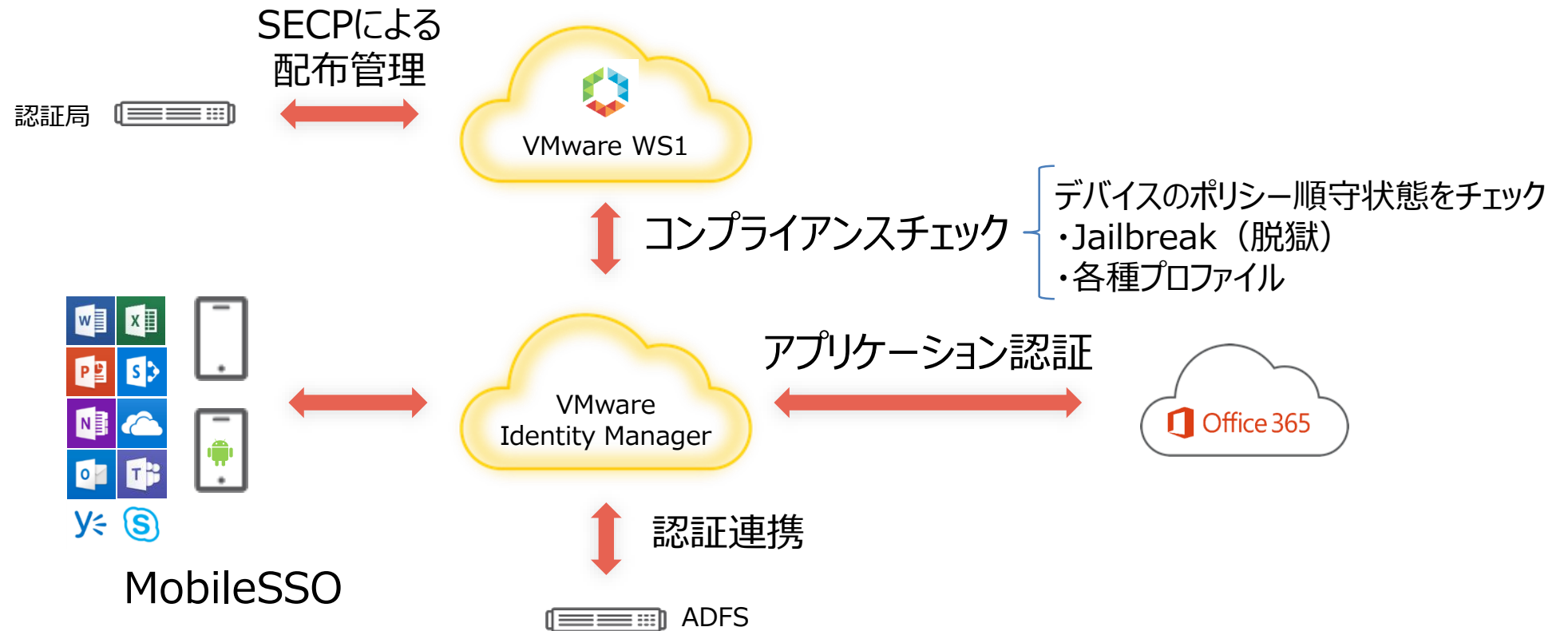
#3

解決

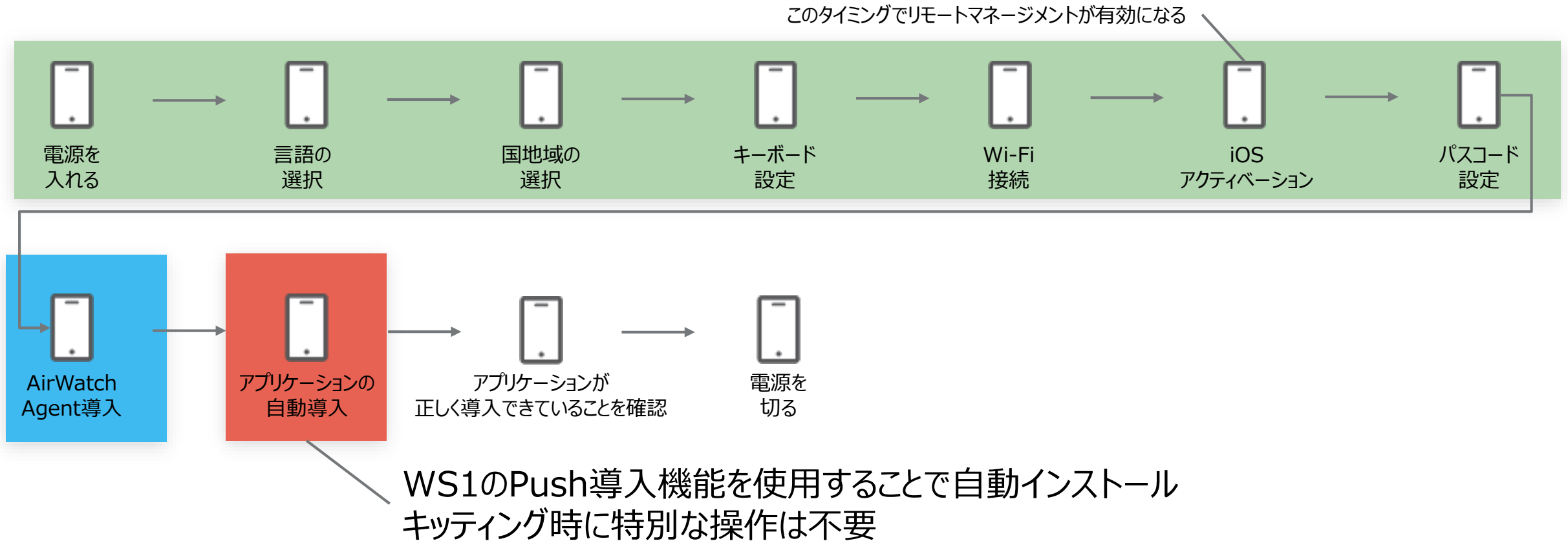
WS1のSimple Certificate Enrollment Protocol (SCEP) 連携機能を利用し自動配布



WS1/IDMを使用し認証連携・モバイルSSO・コンプライアンスチェック機能を実現



WS1の配布機能を利用し約8,000台を4か月でキitting



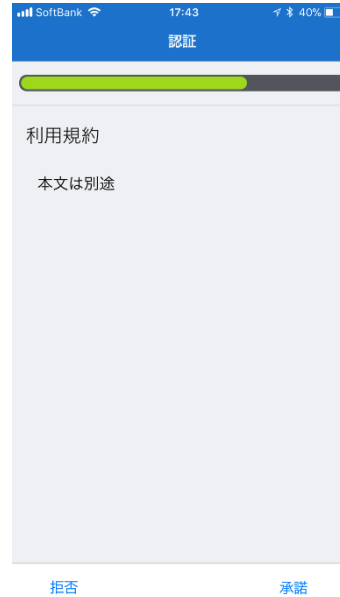
AirWatch Agentを起動しADのID/PW入力、パスコードの設定のみ



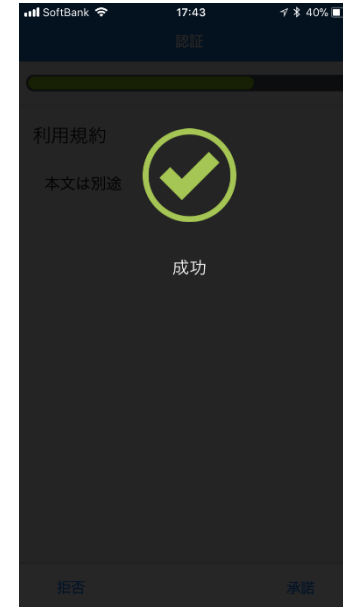
AirWatch Agentを
起動



ADのID/PWを入力



利用規約を承諾



加入成功



パスコードを設定

■ 運用フェーズでの課題 ~全体~

ポリシー設計、認証連携、証明書連携、アプリケーション連携、キッティングは行ったが実際は。。

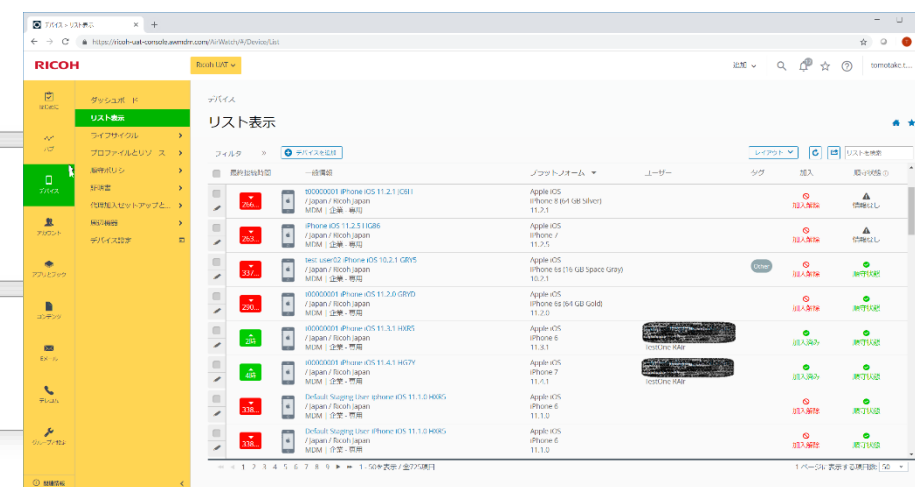
#1 加入操作をしないユーザーが存在 ⇒ コンソールで確認、指導

#2 加入操作をしたが、その後、利用している形跡がない ⇒ コンソールで確認、指導

#3 データ通信が多いユーザーを発見 ⇒ 理由を確認

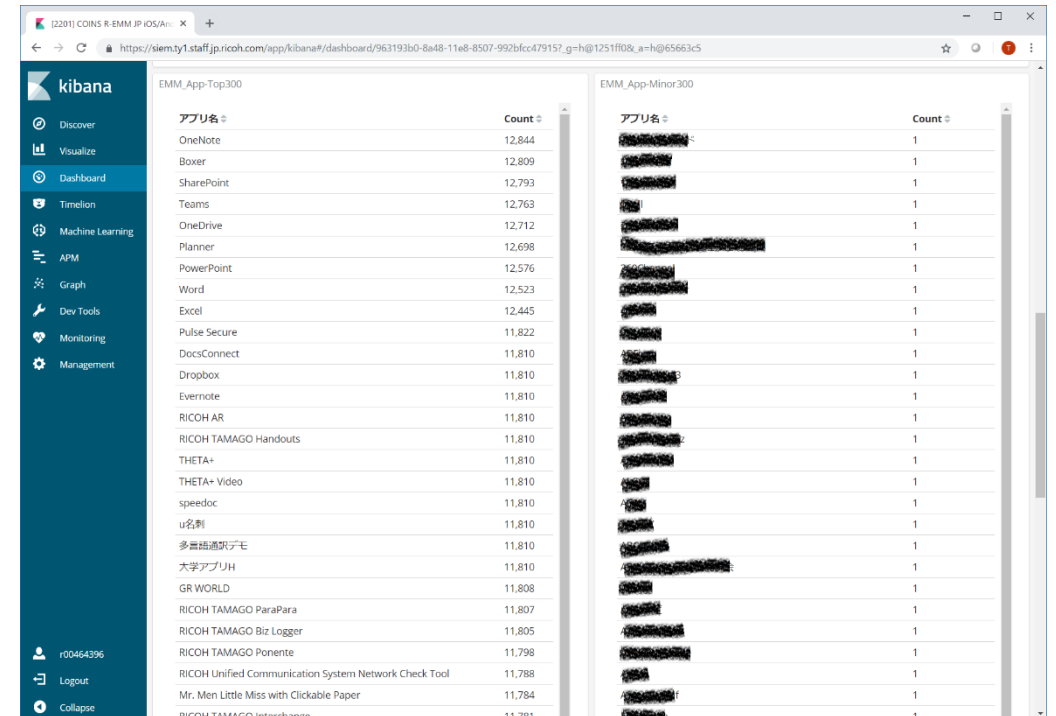
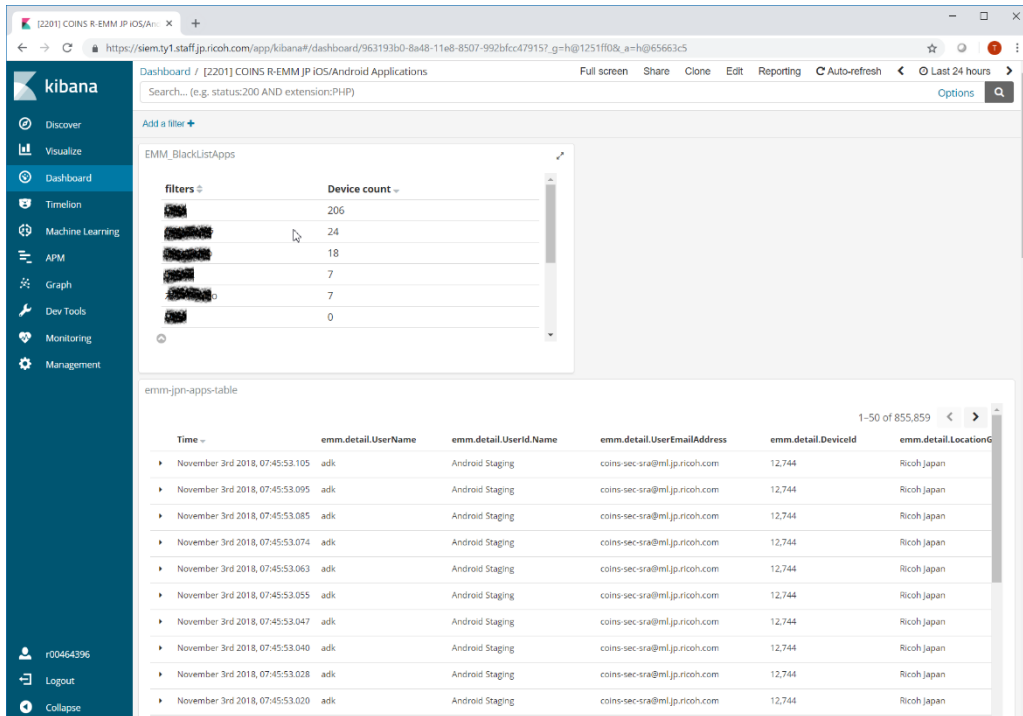
#4 同僚にデバイスを譲渡するユーザー

#5 自由にアプリケーション導入できないことへの不満



運用フェーズでの課題 ~アプリの管理~

アプリ導入を自由化した端末に対して導入アプリケーションを可視化
APIを使用しログをSEIM（Elastic）に取り込みダッシュボードを作成



モバイルデバイスマネージメントは始まったばかり、これからが本番
WS1をいかに使いこなしていくかがモバイルデバイス管理の成否を決める

- | | |
|----|--------------------------------|
| #1 | 国内リコーグループ全社員約4万へWS1を導入したスマホを配布 |
| #2 | 職種、業務に適したセキュリティポリシー（プロファイル）の配布 |
| #3 | BYODの実現 |
| #4 | リコーグループが作成するモバイルアプリケーションの標準化 |
| #5 | SIEMと連携した異常検知と検知の自動化 |

RICOH
imagine. change.