

DW184

エンドポイント管理に戦略を！ Workspace ONE UEM の 最新ユースケースと設計ポイント

グイエムウェア株式会社

プロフェッショナルサービス統括本部

コンサルタント 宮本 康男

コンサルタント 福田 和弘

#vforumjp

vmware

POSSIBLE
BEGINS
WITH YOU

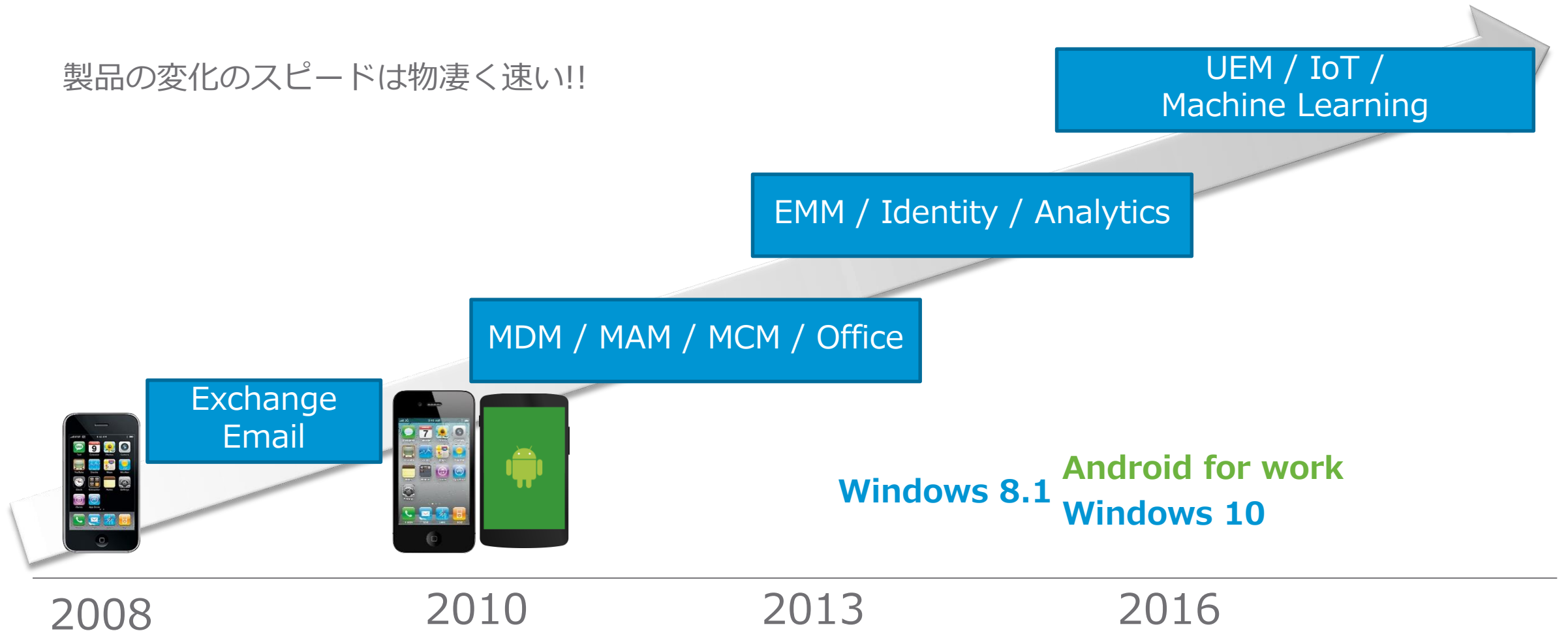
免責事項

- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

VMware の Endpoint Management の進化の歴史

MDM から EMM (エンタープライズモビリティ管理) そして UEM (統合エンドポイント管理) へ

製品の変化のスピードは物凄く速い!!



製品概要

UEM としての Workspace ONE



Workspace ONE UEM

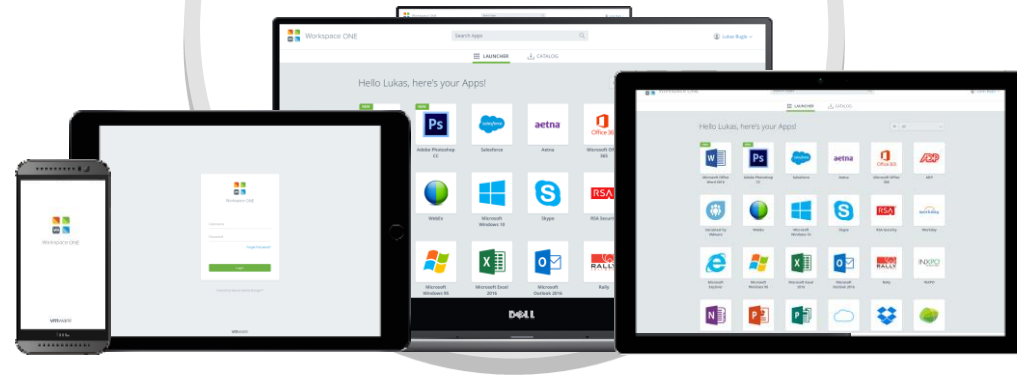


Identity Manager



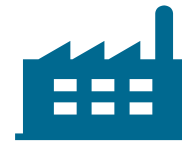
VMware Horizon

vmware®
Workspace™ ONE™



運用分析

デバイスの管理



お客様



従業員



IT 部門



OT
(運用技術)
部門

製品をフルで活用できた場合の価値

Workspace ONE とそれを取り巻くビジネス変化のイメージ図

利便性とセキュリティの両立を
図るセキュアなデジタルワーク
スペースの実現



モバイル端末 (PC,スマートフォン) ,VDI などをフル活用した働き
方改革を推進するツールとしての
統合エンドポイント管理

これだけのスケールのもをどのように導入するのか？



IT 導入に魔法はありません、優先順位を分けて考えよう

戦略を立てるために、必要な Step を考えるべし！

IT に魔法はありません。

戦略としてまずは、企画・計画段階から本番運用までを Step 分けしましょう。
Step 分けできれば、あとは各 Step で決められたことをやるだけです。



実際に Step 分けしていきましょう

実際に Step を分ける場合は、本番運用までの各フェーズを Step として考えていきます。

具体的な例としては、

- ・ Step1(フェーズ1)：方針の検討
- ・ Step2(フェーズ2)：要件定義
- ・ Step3(フェーズ3)：基本設計、構成設計
- ・ Step4(フェーズ4)：環境構築、展開方式策定

Agenda

方針の検討

要件定義

基本設計、構成設計

環境構築、展開方式

まとめ

Step1(フェーズ1)：方針の検討



まず、どこから始めるか

どう進めていくか

Step1(フェーズ1)：方針の検討(1/3)

例えば営業職など移動の多い職種に対しての「隙間時間の効率化」



「簡易な操作で事務処理を終わらせるものを如何に増やしていくか」が鍵

隙間時間を有効活用




承認業務

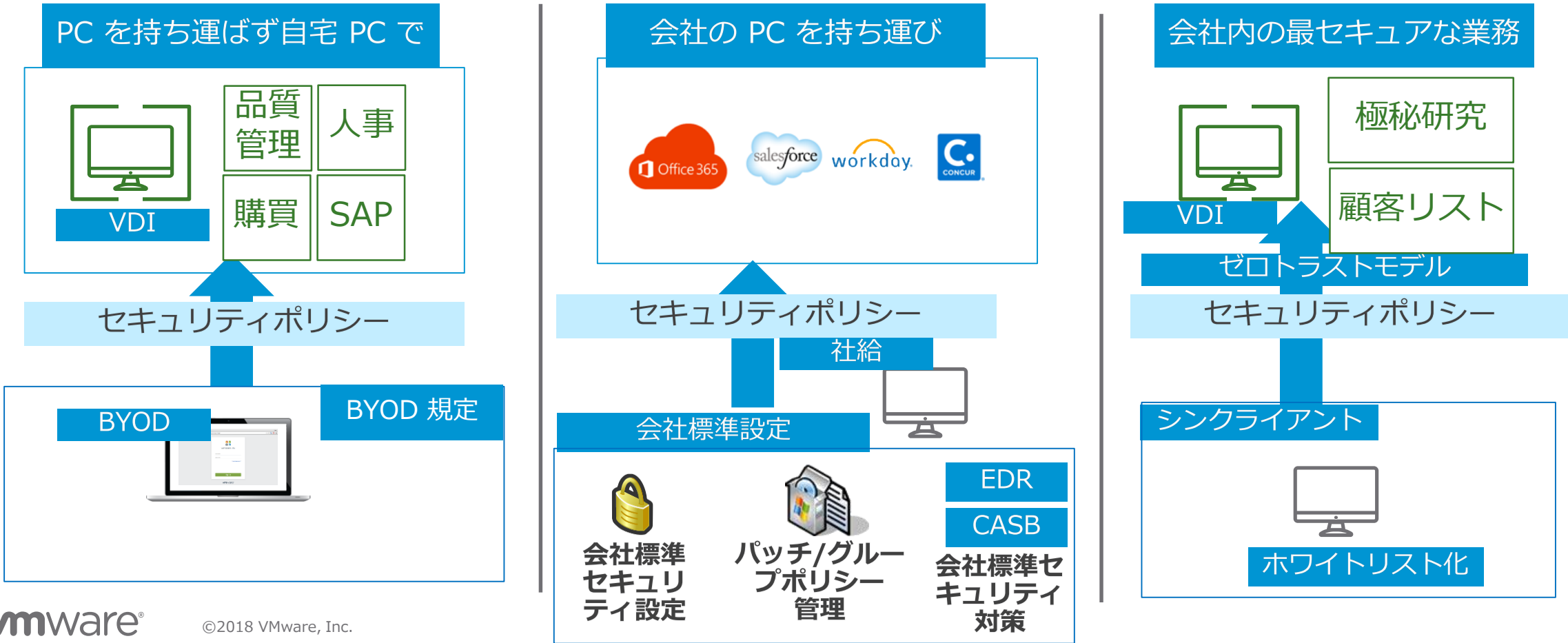
販促ツールと顧客情報

移動時間の予測
まで含めた
スケジュール設定

Step1(フェーズ1)：方針の検討(2/3)

モバイルでできない「がっつり時間を取る業務」に対しての「働く場所改善」

 ユーザーの特性に応じた働き方の選択

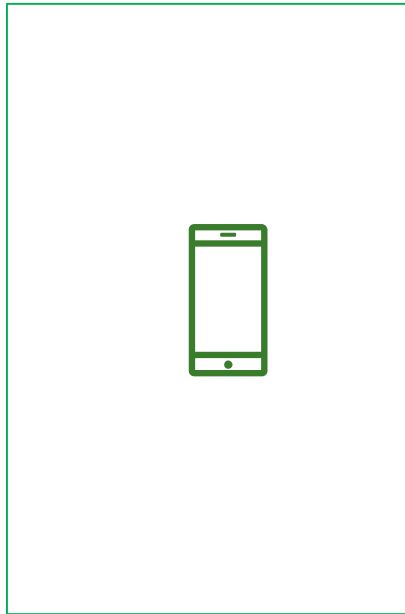


Step1(フェーズ1)：方針の検討(3/3)

千里の道も一歩から。例えば

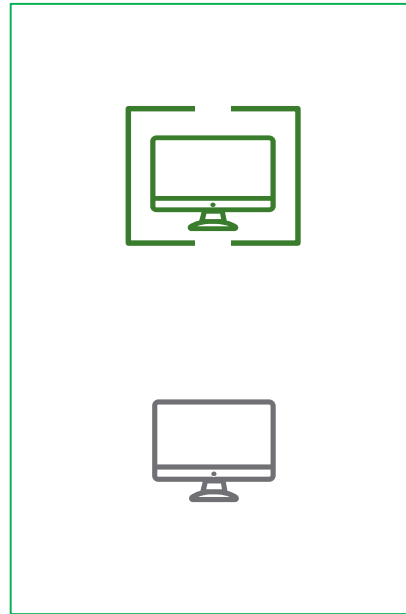
フェーズ1

スマートフォン一部業務
から始めて



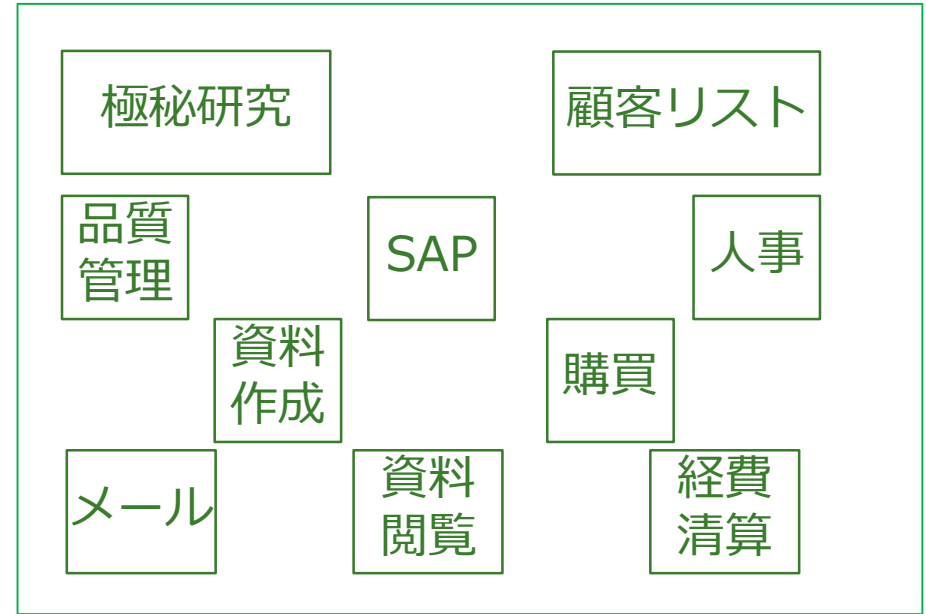
フェーズ2

PCとその業務も管理



フェーズ3

徐々に場所/時間を問わずできる業務を増やそう！！



Agenda

方針の検討

要件定義

基本設計、構成設計

環境構築、展開方式

まとめ

Step2(フェーズ2) 要件定義



鍵は初期導入時に連携するシステムの範囲を決める事です！

Step2(フェーズ2) 要件定義 スマートフォンの場合



一度に多くは望まず、連携はスモールスタートでの展開を計画

全体の8割以上の人を使うシステムとの連携のみがターゲット

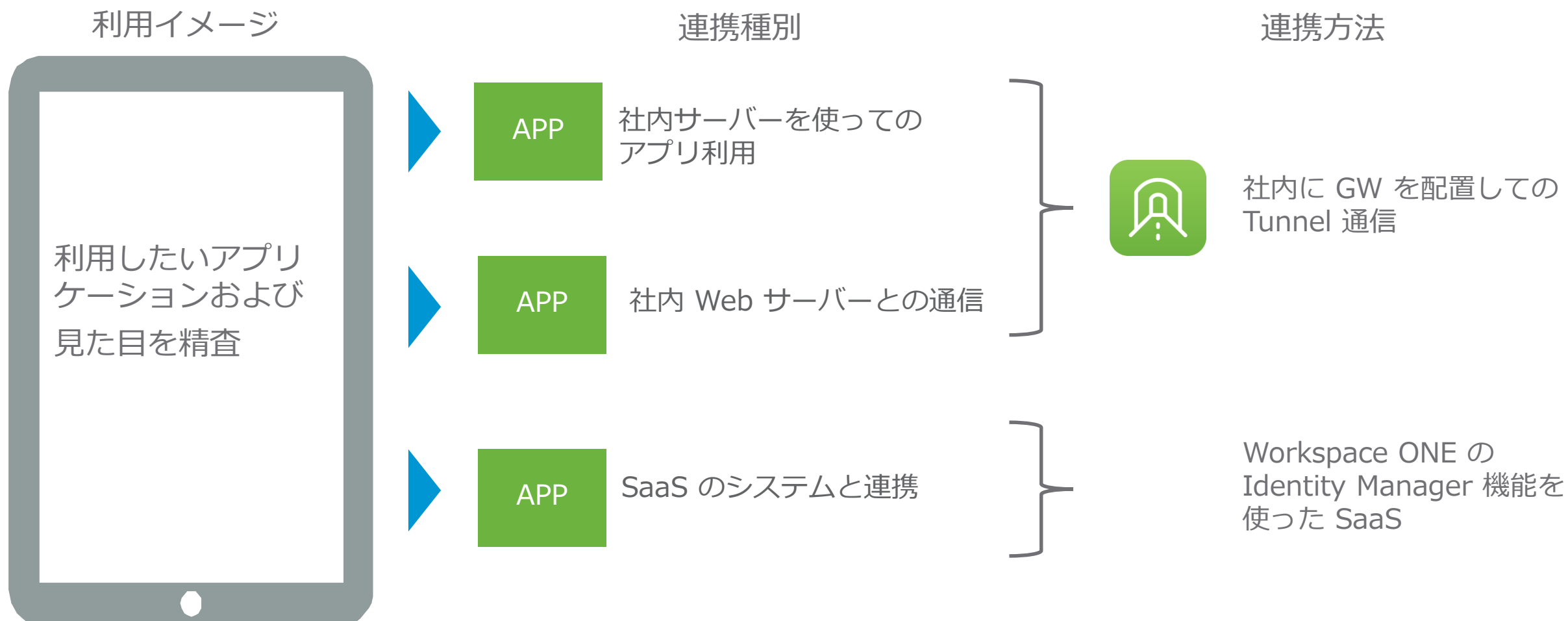
必要なのは利用者目線とセキュリティ

最初から連携するアプリが多いとユーザーが混乱しやすい為、スモールスタートで開始

Step2(フェーズ2) 要件定義 スマートフォン(1/4)

ユーザー目線のイメージで使い方定義(アプリ)

どのアプリケーションを使わせるか精査



Step2(フェーズ2) 要件定義 スマートフォン(2/4)

ユーザー目線のイメージで使い方定義(コンテンツ)

どのコンテンツを見せるかを精査

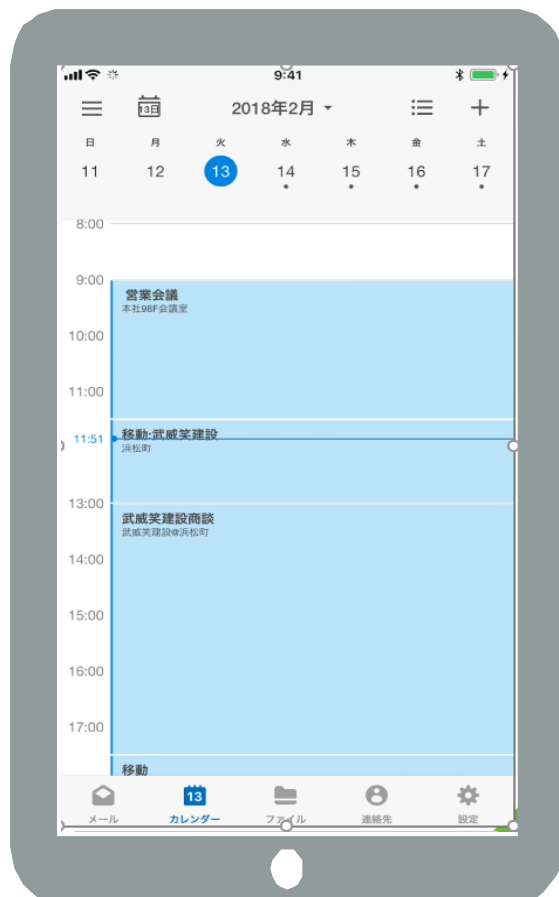


Step2(フェーズ2) 要件定義 スマートフォン(3/4)

ユーザー目線のイメージで使い方定義(メール)

どこのメールサーバー情報を見せるかを精査

利用イメージ



連携種別

APP

社内 Emailサーバー
Exchange 等

APP

Office 365

APP

G-suite

連携方法



社内に GW を置いて
のメール連携

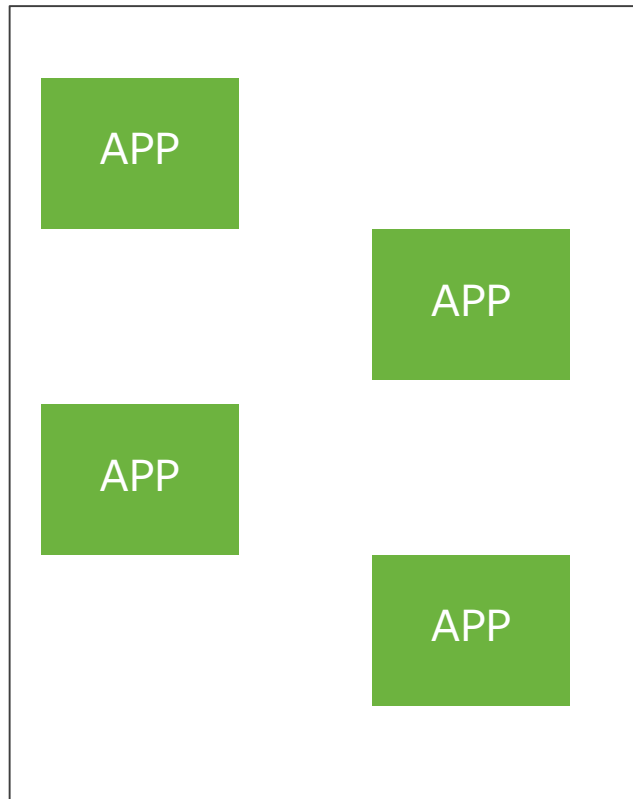


PowerShell/API 等で
接続

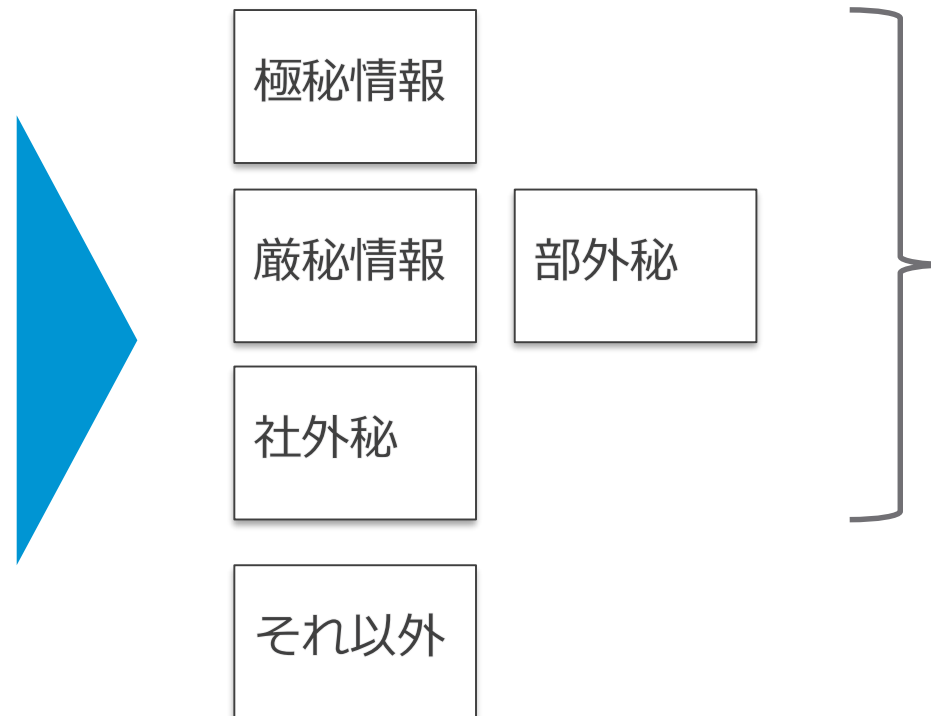
Step2(フェーズ2) 要件定義 スマートフォン(4/4)

利用に対してのセキュリティ

利用したいものの一覧



セキュリティカテゴリ精査



アクション

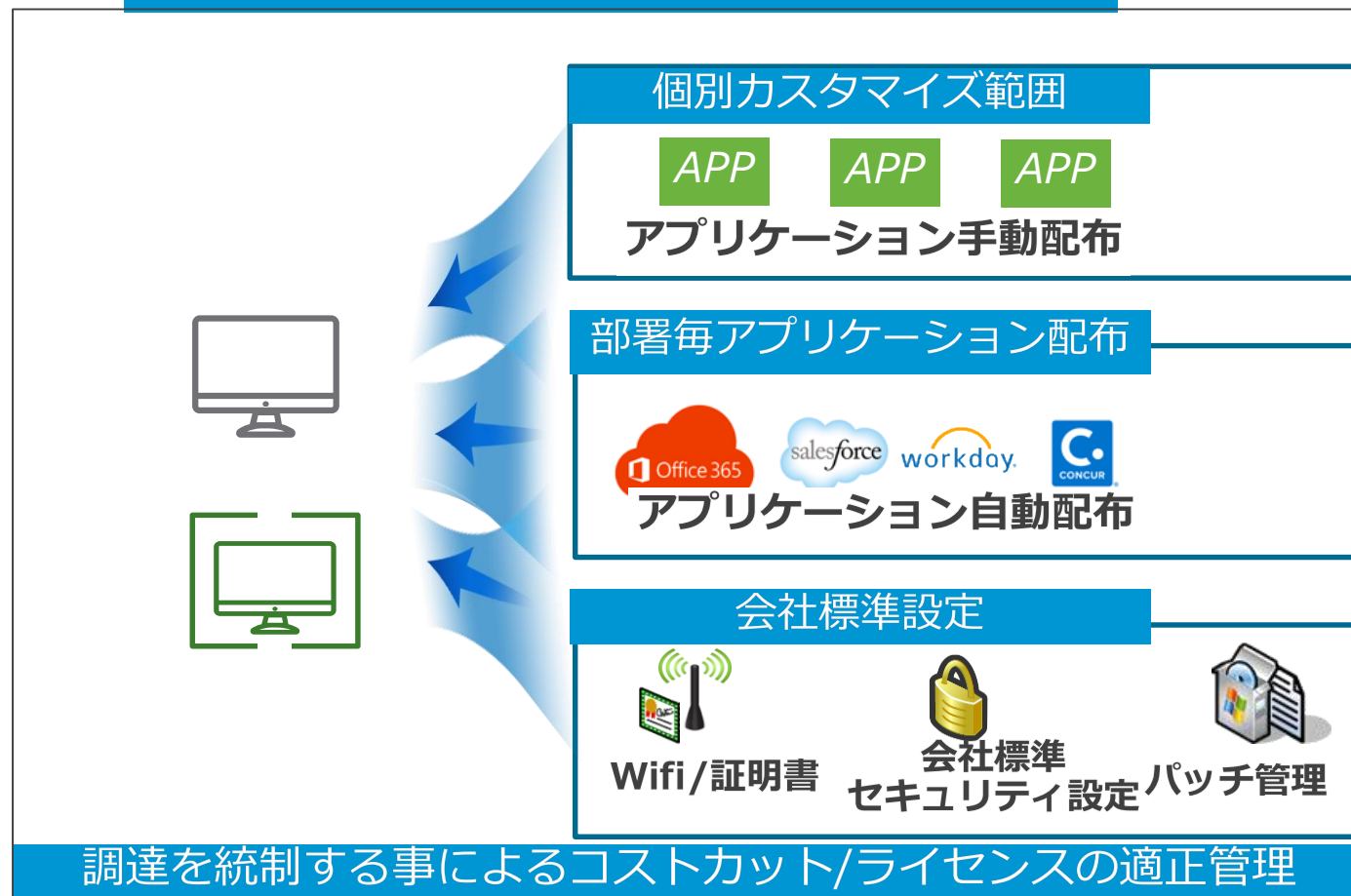


Step2(フェーズ2) 要件定義 PC の場合

現状の棚卸が重要



あるべき姿とのギャップを徐々に埋めていく



現状を整理し誰にどの設定を入れるかを棚卸。まずは最低限必要な設定に抑える。

Step2(フェーズ2) 要件定義 PC(1/3)

現状を分析し、以下パターン分けを行う。
※主にキitting時に入れているもの等の分析を行う。
精査したものに今後取り組みたい内容を加える。

アプリケーション

プロファイル/設定

その他

会社共通

部署共通

個別

現状

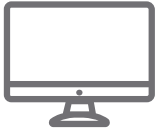

社内ポータル	Windows 10
セキュリティソフト	Chrome
BitLocker	Zip ソフト
パスワードポリシー	
今後	
パッチ管理	

BI システム	
マスター管理	
SAP	
品質管理	
在庫管理	
今後	
ホワイトリスト設定	

労務管理
連結決算システム
今後

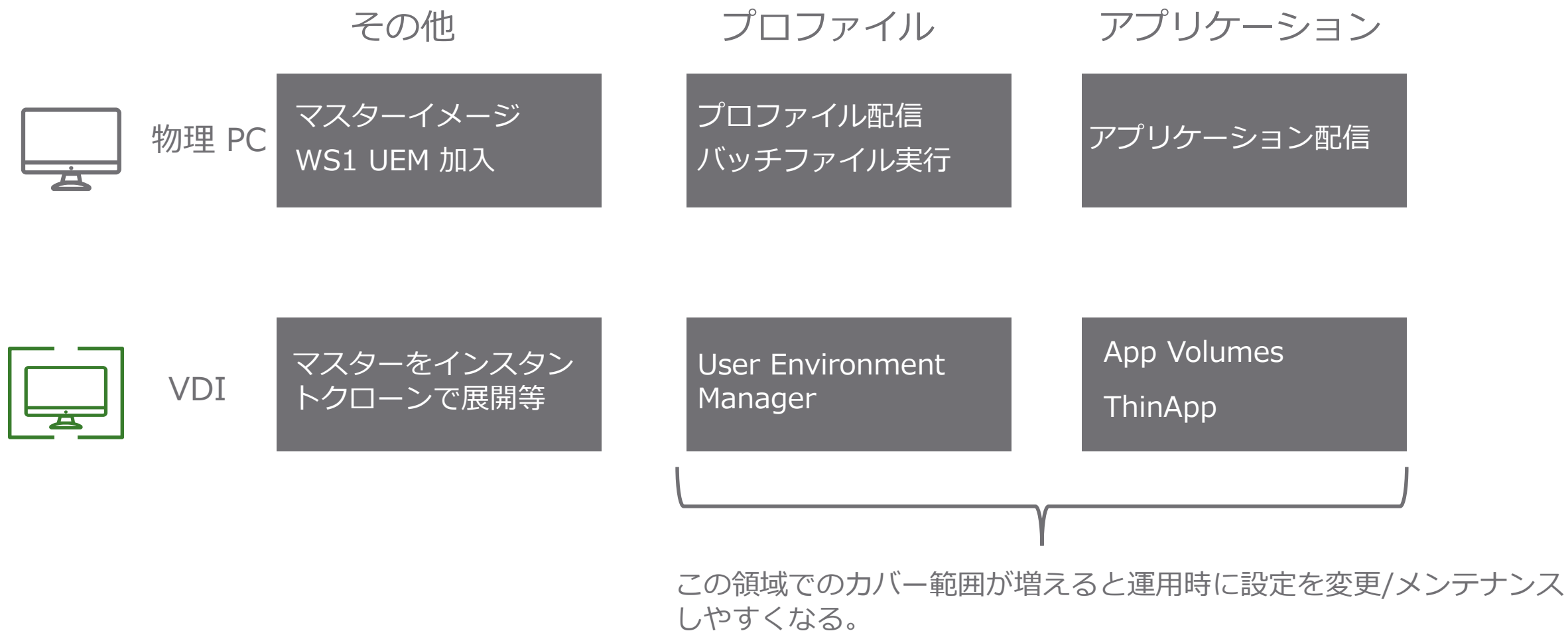
Step2(フェーズ2) 要件定義 PC(2/3)

洗い出したものをそれぞれどう実装するかを決める。プロファイルやアプリケーション側で実装できるものが増えるごとに管理するマスタイメージが減る。

		その他	プロファイル	アプリケーション	
	物理 PC	Windows 10	BitLocker	在庫管理	労務管理
			パッチ管理	Chrome	連結決算システム
			パスワードポリシー	セキュリティソフト	BI システム
	VDI	Windows 10	ホワイトリスト設定	社内ポータル	マスター管理
				Zip ソフト	SAP
				品質管理	

Step2(フェーズ2) 要件定義 PC(3/3)

洗い出したものをそれぞれどう実装するかを決める。プロファイルやアプリケーション側で実装できるものが増えるごとに管理するマスターイメージが減り、また運用時の変更も実施しやすくなる。



Agenda

方針の検討

要件定義

基本設計、構成設計

環境構築、展開方式

まとめ

Step3(フェーズ3) 基本設計、構成設計



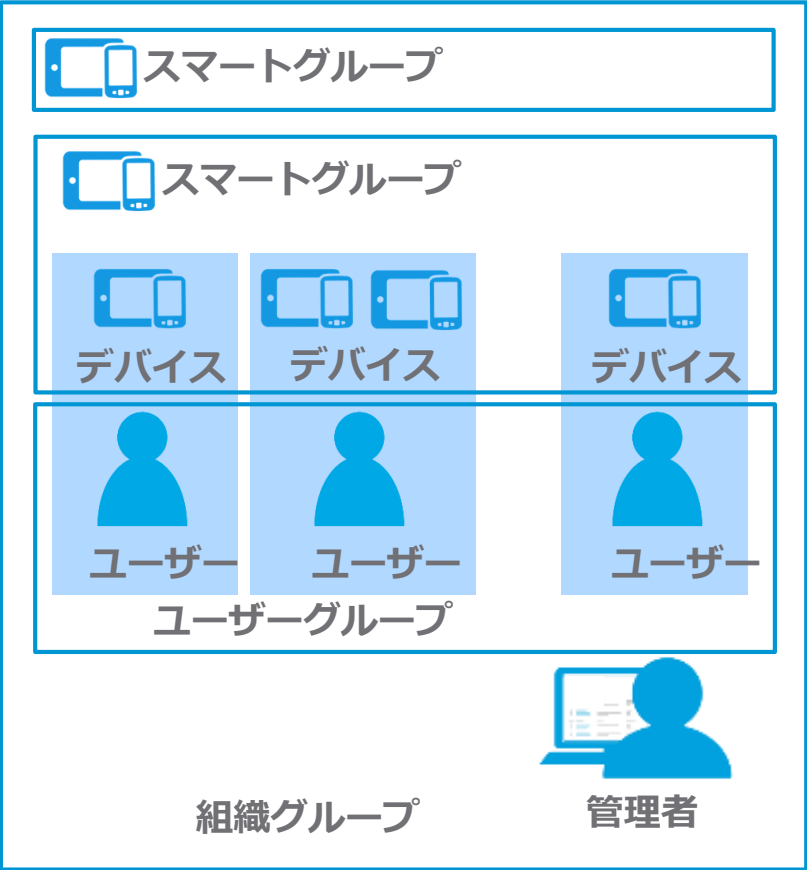
ユーザーのライフサイクルを意識する

デバイスのライフサイクルを意識する

連携システムとの連携性を確認する

Step3(フェーズ3) 基本設計、構成設計(1/6)

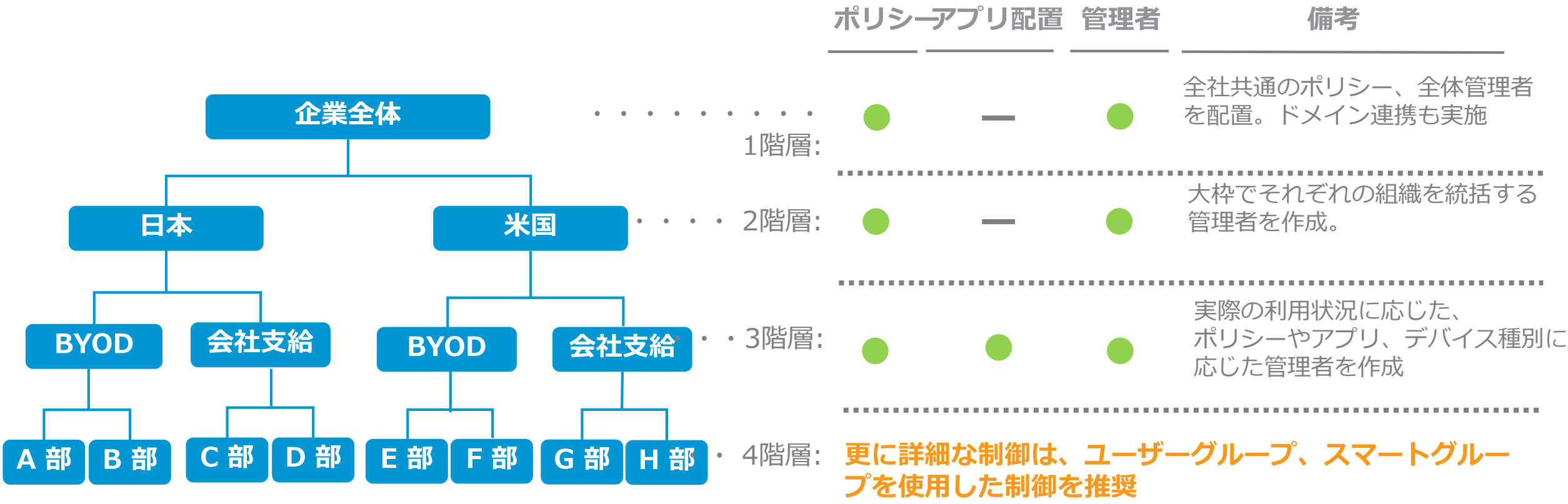
移り変わり行くデバイス・システムをユーザーに対して最適に割り当てるため、まずは構成要素および管理単位を把握しましょう。



名称	意味
組織グループ	管理およびオンプレミスとの接続などのモバイル/PC 管理を分けるグループ
管理者	組織グループ単位の管理者
ユーザーグループ	ユーザーをまとめるアカウントグループ
スマートグループ	ユーザーに設定を割り当てる権限グループ
ユーザー	Workspace ONE UEM の利用者
デバイス	管理するデバイス

Step3(フェーズ3) 基本設計、構成設計(2/6)

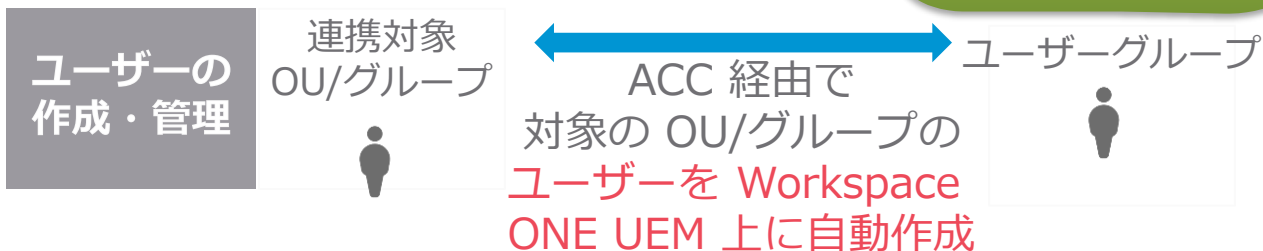
次に WorkspaceONE の最も基礎となる管理単位である、組織グループを定義しましょう。
組織グループを適切に定義することで、管理者・ユーザー・デバイス・連携システムの管理を適切に分割することが可能となります。



Step3(フェーズ3) 基本設計、構成設計(3/6)

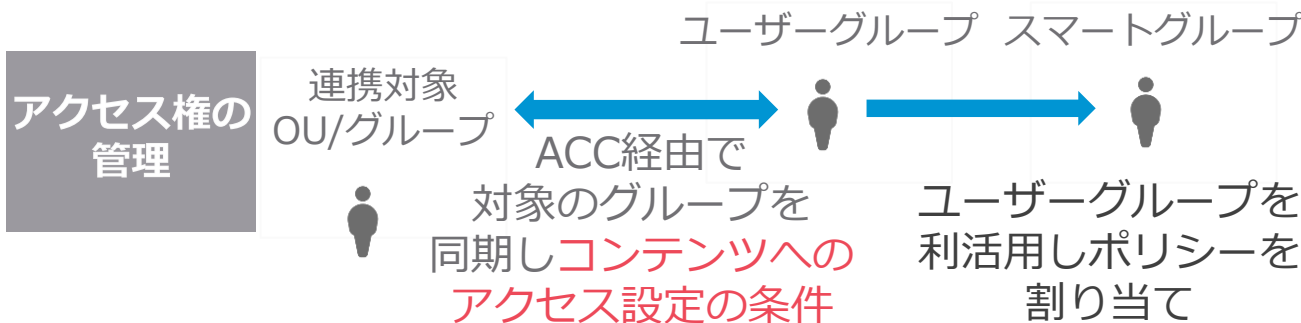
組織グループの設計後は、Active Directory へのユーザー作成や削除のタイミングを確認しつつ、Workspace ONE UEM 上のユーザーライフサイクルとその運用方法を考えていく。

ユーザーに変化が発生するイベントとその際の挙動



AD での挙動

- 1.作成：Active Directory にユーザーが作成されたタイミングで Workspace ONE UEM 上にも作成され、利用可能な状態になる。
- 2.編集：部署移動などでは属性値を同期する。
- 3.無効：Active Directory 上で無効化されると Workspace ONE UEM 上でもアカウントが非アクティブになる。
- 4.削除：Active Directory 上で削除されても、Workspace ONE UEM 上では削除されないため、定期的な削除運用が必要



- 1.追加：Active Directory 上でユーザーを対象のグループへ所属させると、Workspace ONE UEM 上でも同期したユーザーグループに所属
- 2.削除：Active Directory 上でユーザーを対象のグループから外すと、Workspace ONE UEM 上でも同期したユーザーグループから削除

Step3(フェーズ3) 基本設計、構成設計(4/6)

デバイスはまず加入方法を精査、その後レンタルか購入かに応じて故障時や返却時のフローも整える事が鍵

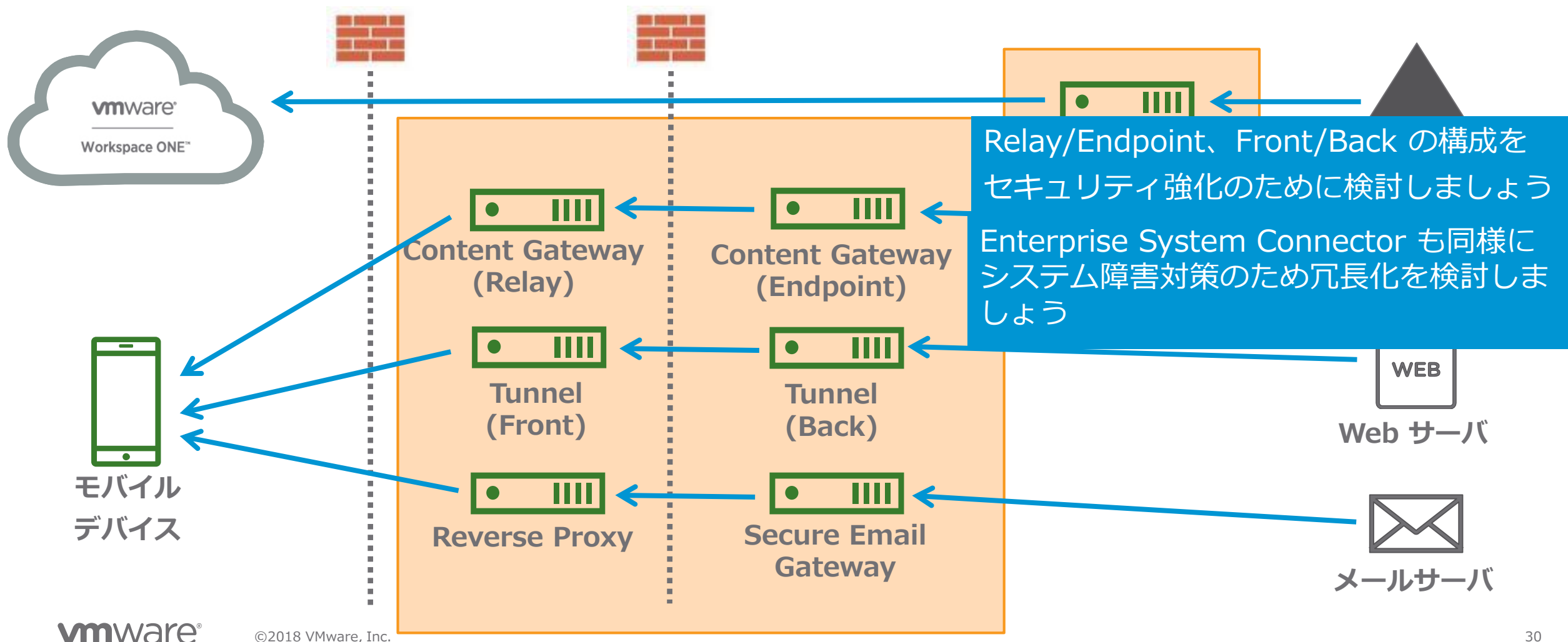
(加入方法一例)

OS	種別	加入方式	加入方法	加入先組織
 Apple iOS	会社支給 --- COPE	代理加入	DEP により自動で加入 キitting時に加入	DEP で指定/ユーザーグループで指定 キitting時に加入
	BYOD	直接加入	手動で加入	手動で加入/ユーザーグループで指定
 Windows	社給	代理加入	プロビジョニング パッケージで加入	キitting時に加入

Step3(フェーズ3) 構成設計、構成設計(5/6)

組織グループが決定すれば、構成を設計していきましょう。

構成設計には、採用する機能・ユーザー規模・耐障害性を考慮し設計を進めていきましょう。



Step3(フェーズ3)構成設計、構成設計(6/6)

ここまでで、組織グループと構成の設計ができました。 いよいよ、これからユーザーの操作にあたる部分の設計に入っていきます。 そこで、設計を進める上で、重要なとおきのポイントをお伝えします！

それこそ、 **User Acceptance Test (以降、UAT) 環境の作成**です。

WorkspaceONE 設計の最適な進め方

要件定義/構成設計

要件定義と構成設計を行い採用する機能と構成を設計します。

重要！

UAT 環境

ユーザー目線で動作を確認するために作成

機能設計検討時の
実動作の確認を行う

機能設計検討

採用した機能の基本設計を検討する

基本設計は常に UAT で
動作を確認しながら進める

Agenda

方針の検討

要件定義

基本設計、構成設計、UAT 構築

環境構築、展開方式

まとめ

Step4(フェーズ4) 環境構築、展開方式



UAT の環境をベースに本番を構成

利用開始もスモールスタートを意識する
※エンドユーザーにとって端末の変更は大きな業務変化となる為

Step4(フェーズ4) 環境構築、展開方式(1/3)

ここまでのフェーズで機能設計は無事終わることができました。 続いては、本番環境を構築し、端末を展開していくフェーズとなります。

が、すでに皆さまは、お気づきなのではないでしょうか？ 実は、環境構築はもう出来たも同然です。なぜならば、**UAT 環境**があるからです！ UAT 環境は都度検証をして、設計を固めるための環境です。言い換えれば設計が終わった今、本番と同じ設定が投入されているはずだからです。

設定項目	デフォルト設定	XXX-UAT-Console
	-	XXXUAT
現在の設定	継承	
パスワード保護処理		
管理者アカウント削除 (有効/無効)	無効	
管理者パスワード変更 (有効/無効)	有効	
VMware Enterprise System Connector証明書を再生成 (有効/無効)	有効	
APNs証明書変更 (有効/無効)	有効	
アプリケーションを削除する/非アクティブにする/回収する (有効/無効)	有効	
コンテンツを削除/非アクティブにする (有効/無効)	無効	
データ暗号化トグル (有効/無効)	有効	
デバイス削除 (有効/無効)	無効	
デバイスワイプ (有効/無効)	有効	
企業情報リセット (有効/無効)	有効	
企業情報ワイプ (有効/無効)	有効	
ユーザーグループメンバシップに基づく企業情報ワイプ (有効/無効)	有効	

パラメータシートの作成も楽々作成！

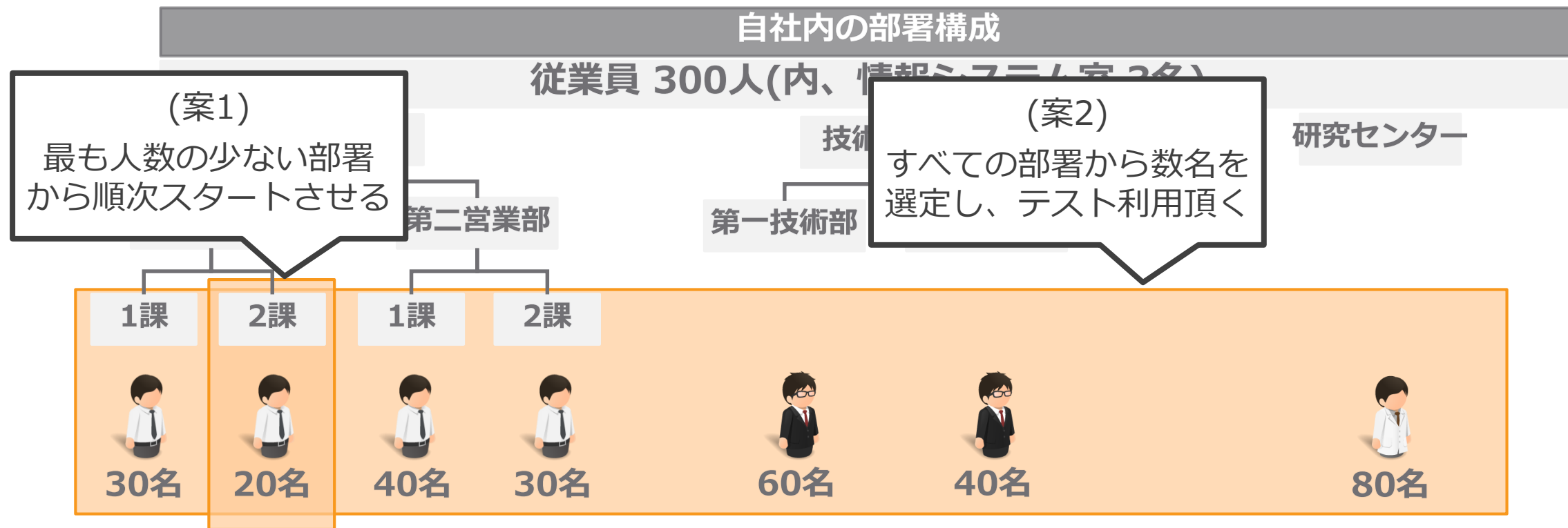


UAT 設定をそのまま入れれば設定完了！

Step4(フェーズ4) 環境構築、展開方式(2/3)

デバイスの加入方法が決まれば、次は展開方法の計画を立てましょう。お勧めは、スモールスタート方式で徐々に展開をする方法です。

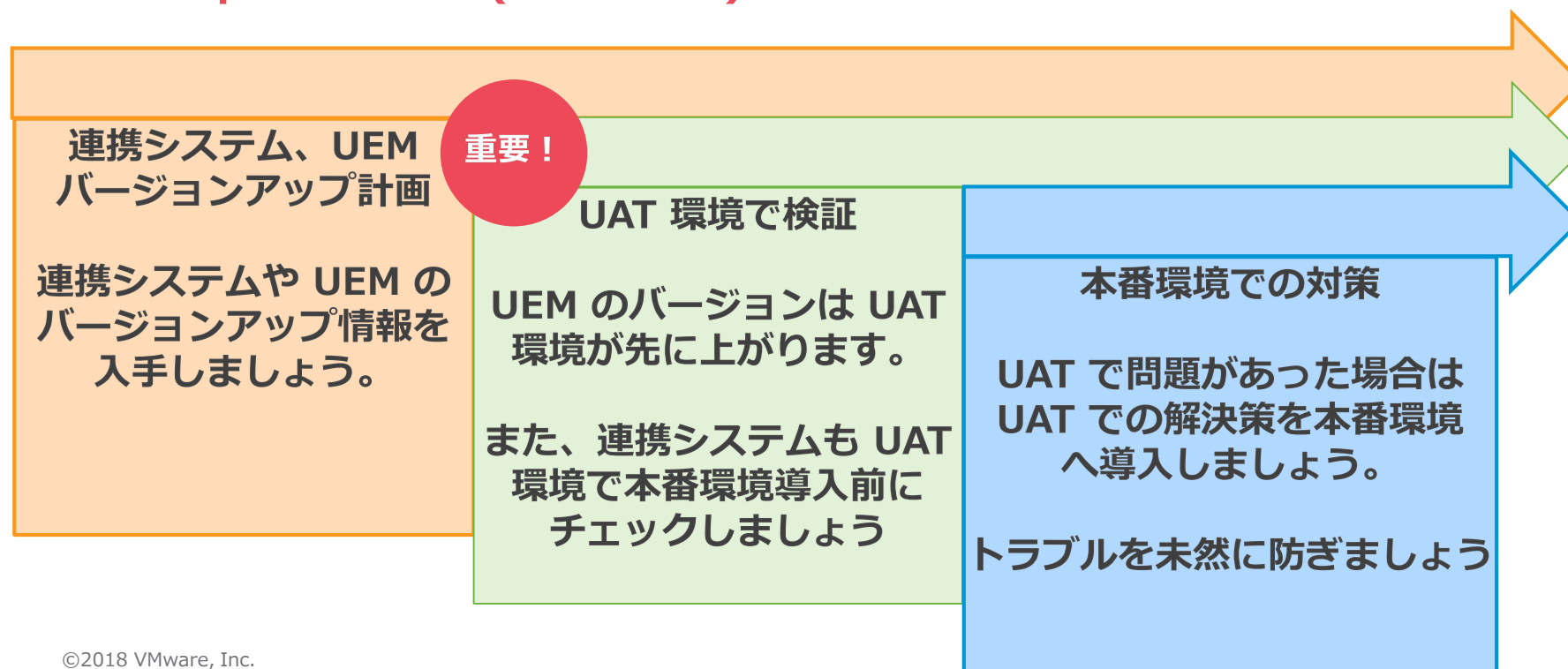
こうすることで、問合せの集中を防ぐことができ、質問/回答のナレッジをためる事ができます。



Step4(フェーズ4) 環境構築、展開方式(3/3)

Workspace ONE は、デバイス管理やシステム連携をメインとした製品となっています。但し、デバイスはOS バージョンアップされますし、連携するシステムもバージョンアップや新規採用が考えられます。それらを都度、本番環境で実施することは困難です。そもそも WorkspaceONE UEM SaaS のバージョンも上がっていきます。

そのため、**User Acceptance Test (以降、UAT) 環境**を活用しましょう！



まとめ

Workspace ONE を導入する上で、特に重要なポイントを3点まとめましたので、本日はこの3点をぜひ覚えて頂ければ幸いです。

その1. アプローチや要件で「戦略」を考える！

Step 分けを行い一つずつ確実に進めていきましょう。
考えるにあたりユーザー目線は忘れるなかれ。

その2. 設計から運用まで「UAT」を使いこなせ！

机上の空論では連携要素が多い為、失敗しやすいです。
動作確認は確実に！

その3. 展開の段階で「現実的な」を計画しましょう！

エンドユーザーからすると利用するデバイスが変わるので大きな変化です。問い合わせは来る前提で徐々に展開しましょう。

最後に



全てのデバイスで、エンドポイントの統合管理ができるまで
長く険しい道だと感じる方もいらっしゃるでしょう。



ただし、本気で取り組みれば1年後にはエンドポイント管理が大きく変わり、同時に働く人の環境も大きく変わります。



働き方が変わり会社や社会が変わる姿を作りあげていく。今社会で様々な働き方の問題が起きている中、改善をする事が IT に関わるものの使命かもしれません。



本気で取り組み、新しい未来を一緒に作り上げていきましょう！！

ライセンス



コンサル

\セットで検討お願いします /

vmware®
Workspace ONE™



そして、製品と一緒に我々コンサルタントのご検討もお願い致します(笑)

本セッション受講の方へのお勧め

DW177	09:00~ Room I	VMware によるマルチクラウド環境に対応した 各種仮想デスクトップサービスのご紹介
DW180	13:00~ Room A	VDI・アプリケーション仮想化のシームレスな ハイブリッド展開の選択肢
DW307	14:40~ Room I	【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

本セッションに関連する展示・ハンズオンラボのご紹介

お客様のペースで
利用いただける
セルフペースラボです。

以下の製品については
日本語マニュアルも
提供されています。

- VMware Horizon 7 Enterprise
- VMware Workspace ONE
- What's new in vSphere 6.7
- vSphere 6.7 Challenge Lab
- VMware vSAN 6.7 Getting Started
- VMware Cloud on AWS

VMware
ハンズオン
ラボ

VMware
ソリューション展示

いつでも・どこでも・どのデバイスからもセキュアに
アプリケーションやデータへアクセスし、業務を実施
できる環境、それがデジタルワークスペースです。
ユーザーにとっての利便性と管理者に必要なセキュリ
ティをいかに実現しているかをご紹介します。

ご清聴、ありがとうございました。