SYNNEX JAPAN

Microsoft Autopilot の機能と展開について

～展開時に抑えておくべき課題

Agenda

- Windows AutoPilot とは何か？
- Microsoft Intune の概要…Intune の概念、Intune が提供するサービスとその提供範囲
- Windows 10 の管理…Intune における Windows 10 の管理シナリオと構成について
- 従来のキッティングとの違い…クローニングとの違いについて
- Windows 10の更新管理について…更新管理のシナリオについて
- 機能紹介：条件付きアクセス…Intuneを活用した条件付きアクセスによるセキュリティの向上

Windows AutoPilot とは何か？

• Windows AutoPilot とは何か？

➢ カスタムイメージを企業内で展開して既存のクライアントをアップグレードしたり、ベアメタルPCに展開したりといった従来型のクライアント展開とは全く異なる、新しいアプローチが導入されています。(マイクロソフト公式説明より抜粋)

簡単に説明すると、以下のようになります。
Windows AutoPilot は、Windows セットアップの最終段階でエンドユーザーが自分の「資格情報」さえ入力すればあとは自動で設定が終了する。
一度導入してしまえば、端末が故障しても端末交換後にユーザー資格情報を入力すれば同じ環境を好感した端末上利用できる。

シナリオとしては以下のような条件で利用可能となります。
- Windows 10のプリインストールPCをボリューム単位で購入できる
- 初回起動時のセットアップの最終段階でユーザーに資格情報を入力してもらう
- 組織用のコンピュータとして基本的なセットアップを完了させるためにはインターネット回線さえあれば良い

費用感としては以下のような場合に推奨されます。
- クローニングではキッティング作業費は台数比例で高くなってしまうが、 AutoPilot では台数比例しないためコストは増えない
- クローニングと違い、マスターイメージ作成作業は発生しないため作業費が発生しない
- Intune 上のプロファイル設定を追加するのみで端末更新(バージョンアップ)が可能となる

• AutoPilot に必要な構成とは？

➢ AutoPilot を利用するために現状のPC管理・運用環境をクラウド側に寄せる必要があります。
  ◆ 具体的には以下のいずれかのクラウド環境を用意する。

必要なサービス	ライセンス(機能)	説明
	Azure ADのディレクトリ	組織のアカウントの管理に必須
	Azure AD Premium P1またはP2サブスクリプション	会社のブランドおよびモバイルデバイスを管理する場合に必要
	ビジネス向けMicrosoft Store（Microsoft Store for Business）Microsoft Intune、またはMicrosoft 365 Business	Windows AutoPilotを構成するためにいずれかのサービスが必須

クライアント環境	ライセンス(機能)	説明
	Windows 10 のPro、Enterprise、Educationのイメージ	OSとしてWindows10端末が起動すること
	インターネットアクセス	Windows10端末がMicrosoftクラウド環境へのアクセスに必須
	Azure ADの資格情報	デバイスとユーザーアカウントを紐づけるために必須

➢ Intuneと呼ばれるデバイス管理製品に、PCの情報登録をcsv形式でアップロードして利用する。
  ◆ CSVに含まれる情報とは以下のものとなります。
    -シリアル番号
    -Windows Prodcut ID
    -Hardware Hash ID
    -Model
    -OEM名

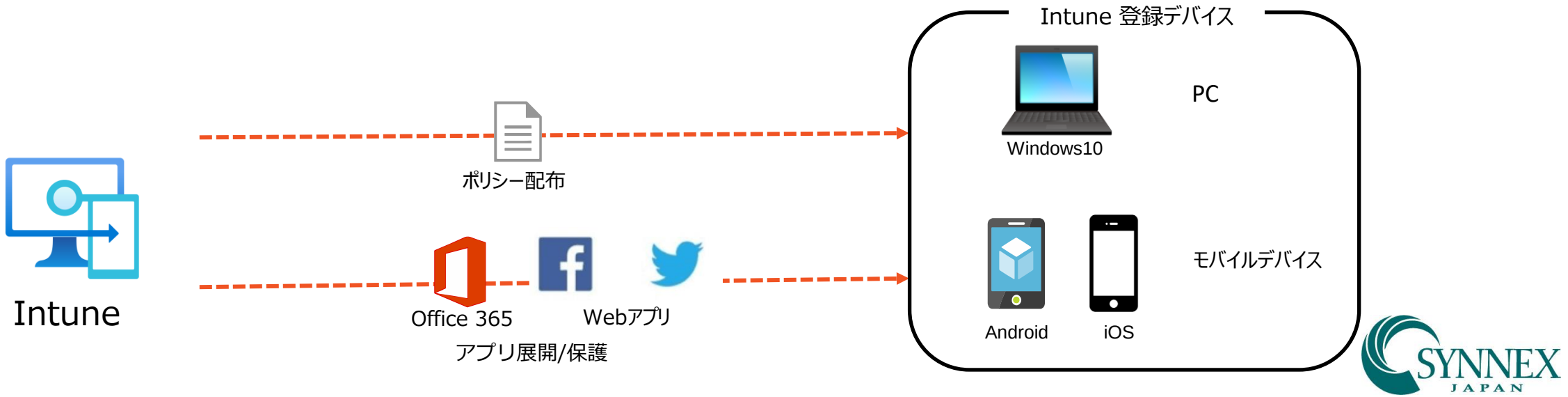
SYNNEX JAPAN

Microsoft Intune の概要

• Microsoft Intune とは？

➢ Microsoft が提供する、クラウド型のデバイス管理製品でアプリケーションとデバイスの制御します。またはマイクロソフトのデバイスとアプリケーションを統合管理する製品を指す。

A) いつでもどこからでも管理でき、デバイスの利用場所に制限がない。
B) クラウドサービスであるため、常に最新のサービスが利用可能である。
C) Windows10 PC だけでなく、Android や iPhone や Mac 端末を一元管理できる。
D) デバイス管理だけでなく、アプリケーション管理も可能である。



Windows 10 の管理

- PC管理の変化

➢急速に変化しつつある“働き方”の常識としてコロナ以前と以降で大きく取り巻く環境が変化した。

	Before COVID-19	With/After COVID-19
働き方を取り巻く環境	オフィスへの出勤が前提	在宅勤務(リモートワーク)が普通になる
	対面のコミュニケーションが必須	社内外を問わずオンライン会議が普及
	時間ベースの評価システム	成果ベースの評価システムに移行
PC環境	資料作成のためのツール • ドキュメント • メール • データ分析	コラボレーションツール • 共同編集 • オンライン会議 • ビデオプレゼンテーション

- PC管理の変化

➢ 結果としてPC管理の在り方も従来のままでは対応できなくなってきているため変化を求められている。

これまで

Traditional IT

単一デバイス

社給デバイス

会社ネットワーク＆レガシーアプリ

オンプレミス環境・プライベートクラウド

これから

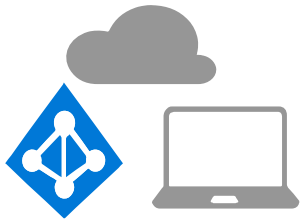
Modern IT

マルチデバイス

個人所有または社給デバイス

クラウド管理＆Saasアプリ

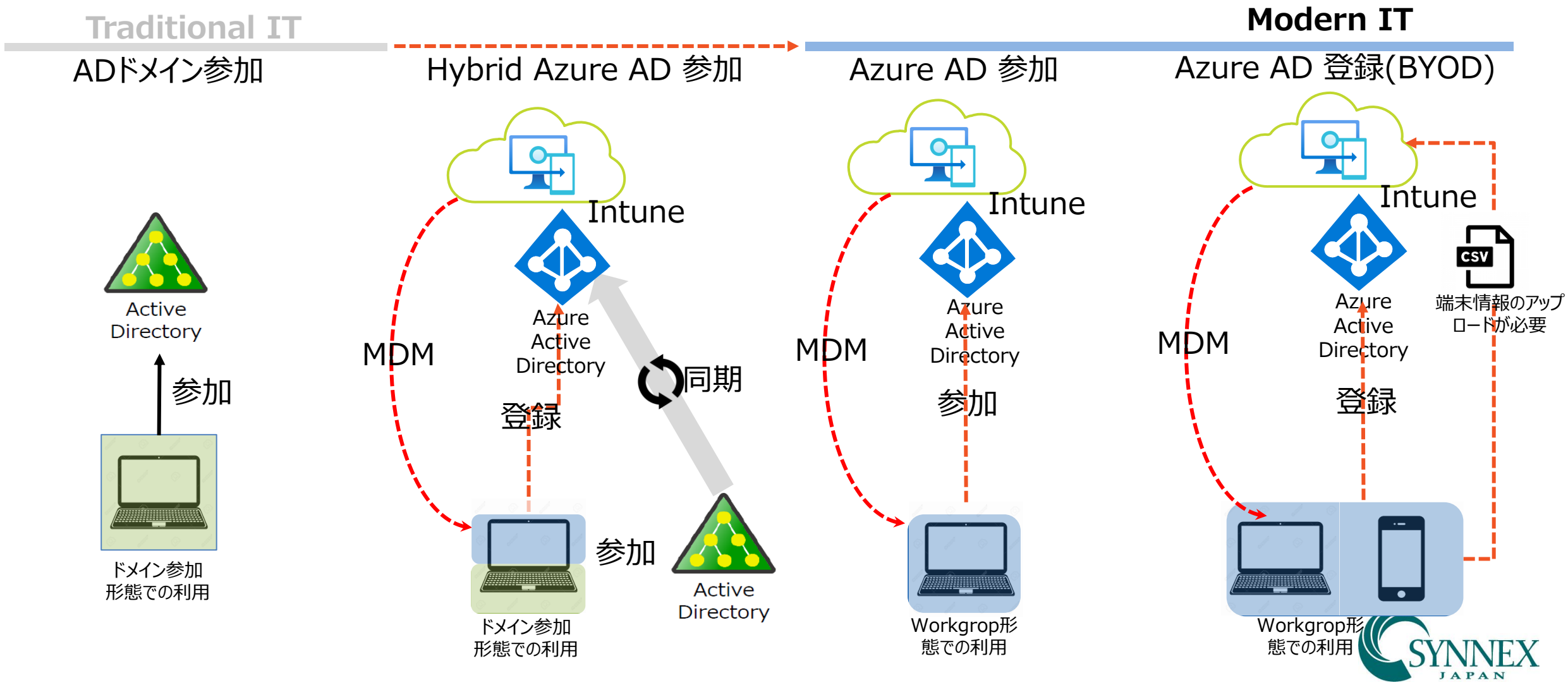
クラウド環境・マルチクラウド



Modern IT の基盤
Azure Active Directory ＋ Intune ＋ Microsoft 365

- Windows 10 管理シナリオ

➢ これまでは企業単位のドメインを管理し、クライアント端末はドメインに参加することでクローズドの環境でのみ使用してきた。
今後はクライアント端末はドメイン以外でのインターネット環境での利用が必須となっている。



従来のキッティングとの違い

クローニングについて(従来のキッティング)

- キッティング手法のクローニングとは？
  - ✓ マスターとなる端末に企業で使う設定やアプリケーションをインストールし、それをイメージ化して複数端末にコピーする手法。
  - ✓ バンドルされているライセンス(OEMライセンス)は使えず、別に Windows10 Pro 以上のライセンスの購入が必要。

- クローニングのデメリット
  - ✓ マスターイメージを使用した従来の展開方法（Wipe & Load）を採用したことにより、マスターの作り替え作業が発生。
  - ✓ OSバージョンアップ時の配信コントロール設計が十分でなく、回線負荷が高まり業務影響が出てしまう。
  - ✓ OSが継続的にアップグレードされていくことや、標準機能としてクラウドとの連携が実装されているが利用できない。

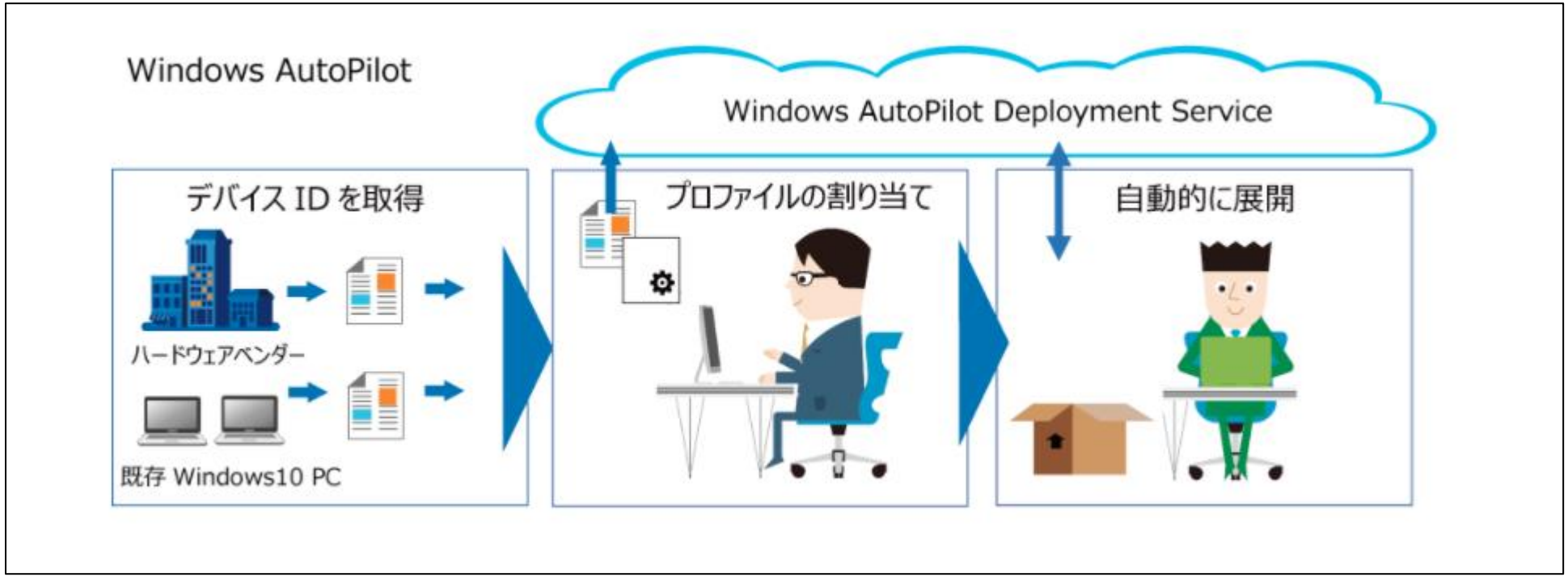
Windows AutoPilot について

➢ キッティング手法の AutoPilot とは？

- ✓ 自社環境に適した Windows 10 デバイスの初期セットアップをクラウドを介して自動的に行う手法。
- ✓ 新規デバイスを個別にセットアップする必要がなくなるため、端末を配布するだけで済む。
- ✓ 各エンドユーザーが企業の構成や設定、必要なアプリケーションをインストールされるため時間を節約可能。

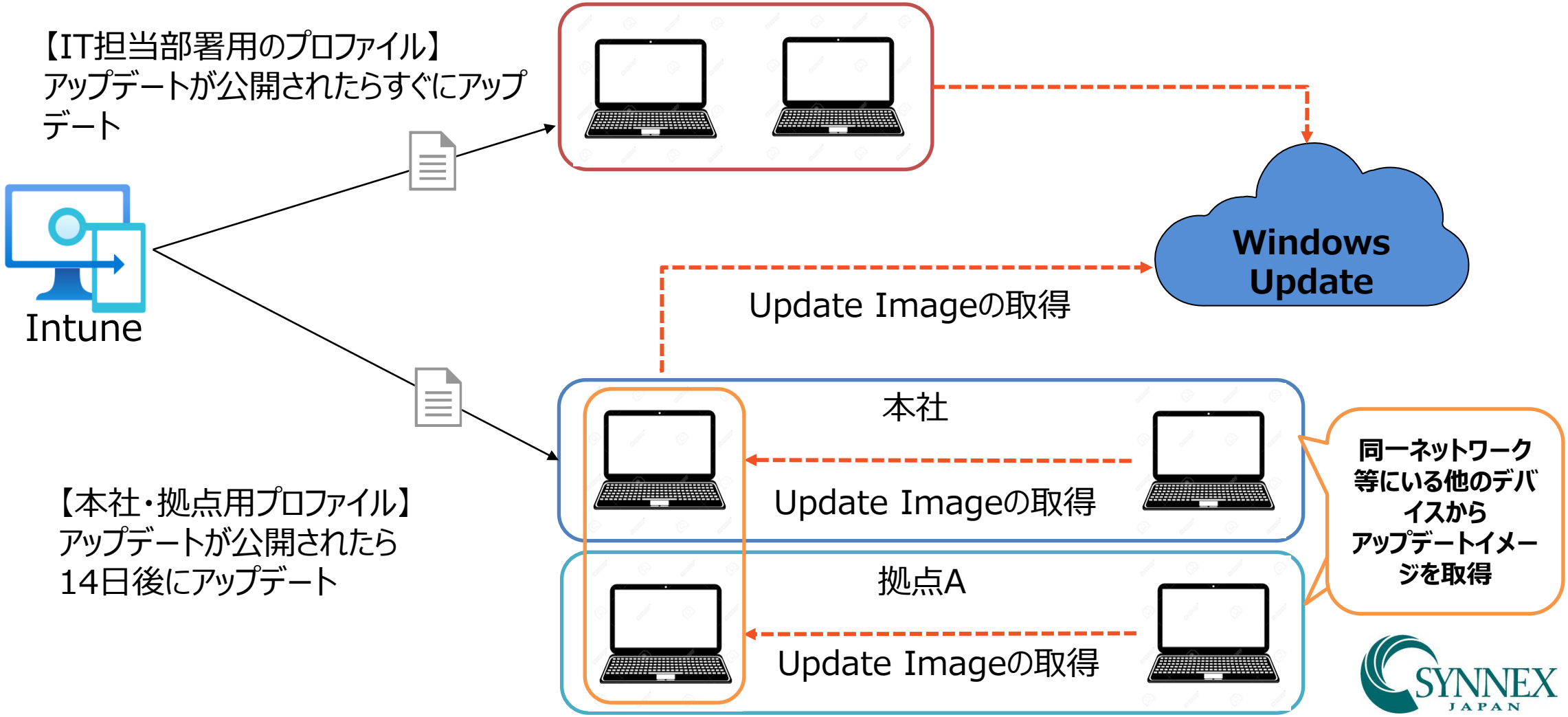
➢ AutoPilot のデメリット

- ✓ PCのセッティング処理を起動することはできるが、全てのPCのセットアップ処理を簡単に実装できるが個別の環境設定は不可。
- ✓ 全部の環境をクラウド環境に寄せる必要があるため、初期導入のハードルが高いと感じてしまう。
- ✓ デバイスの購入先が Windows Autopilot を使用して出荷しているメーカーに限られてしまう。



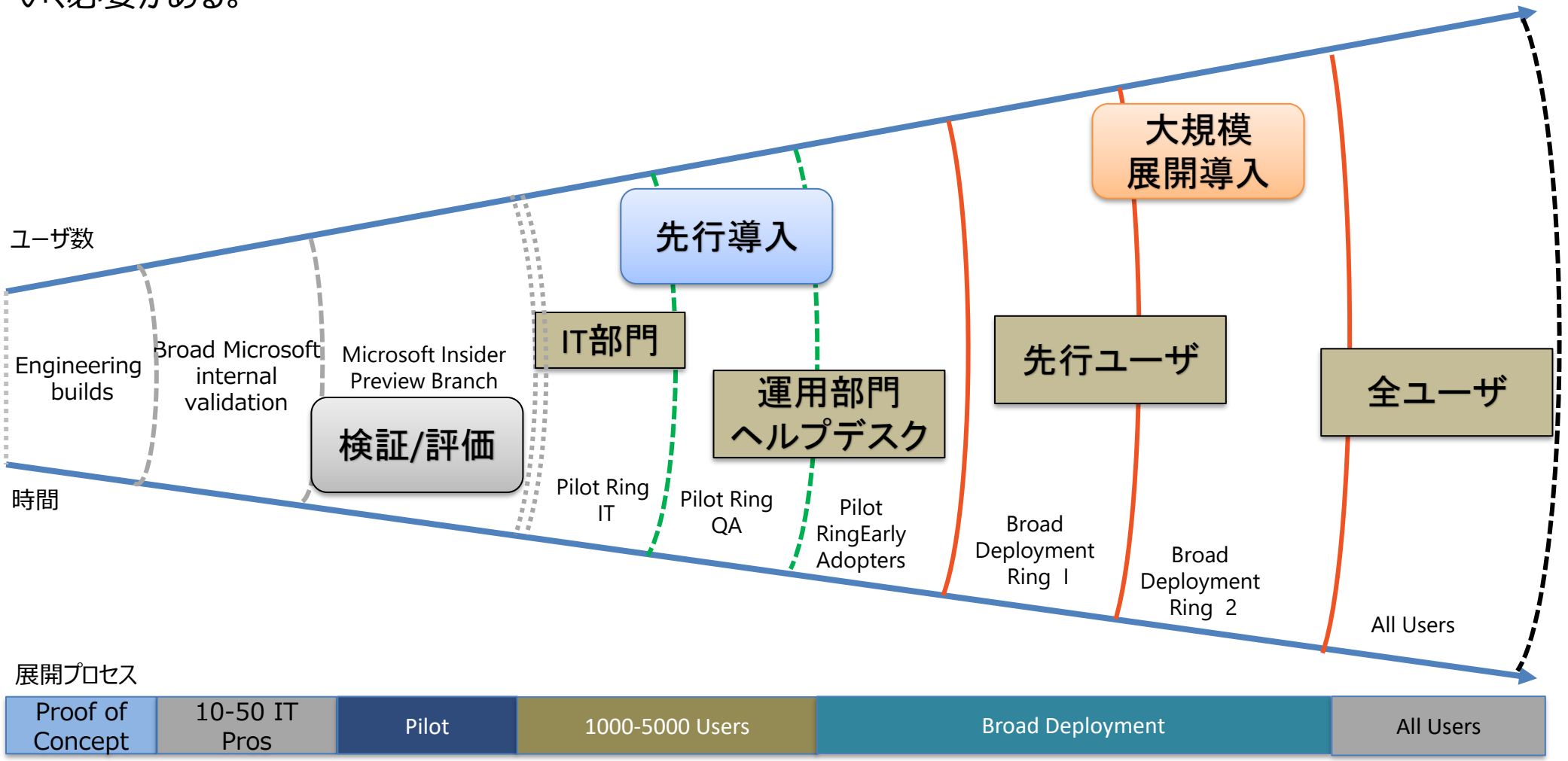
➢ Intune における Windows 10 更新管理の流れ

➢ Intune ではWindows 10の更新管理についてはプロファイルを構成して制御します。下記では2つのプロファイルを構成して管理している例を示す。



- Windows 10 の更新管理

➢ Windows 10の更新管理についてはアップデート実施時期と対象デバイスを適切に管理し、徐々に導入規模を拡大していく必要がある。



Hybrid AD Join について
(条件付きアクセス)

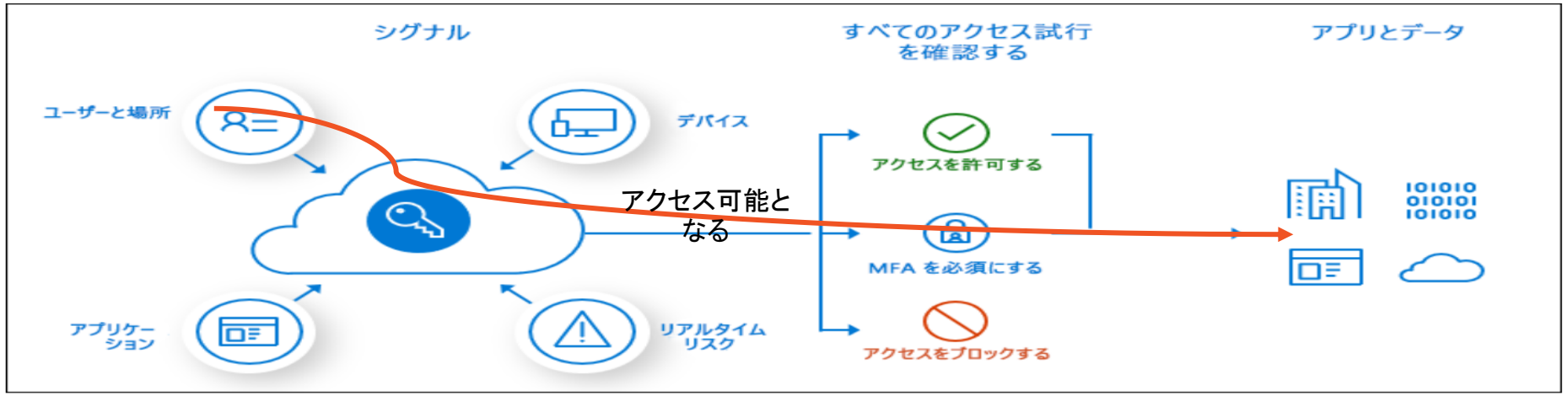
- 条件付きアクセスとは？

➢ 条件付きアクセスは、Azure Active Directory で使用されるツールを指す。

➢ “アクセス制御”に“条件(ポリシー)”の要素を組み合わせるアクセスコントロール機能を指す。
  - ✓ 条件付きアクセスポリシーを作成し、割り当てる。

➢ “条件” では、条件付きアクセスポリシーを発動するアクセス元の要素を指定
  - ✓ アクセスするユーザを特定する
  - ✓ アクセスする場所を指定する
  - ✓ 利用するデバイスを特定する
  - ✓ アクセスするクラウドアプリを指定する

➢ 要件を満たした場合のみアクセス許可を与える。
  - ✓ 多要素認証を利用することが前提条件となりクリアする必要がある。
  - ✓ デバイスに依存したデバイスベースのアクセス条件を指定できる。
  - ✓ アプリケーションに依存したアプリケーションベースのアクセス条件を指定できる。
  - ✓ ユーザもしくはセキュリティグループをベースとしたアクセス条件を指定できる。
  - ✓ ネットワークに依存したネットワークベースのアクセス条件を指定できる。



条件付きアクセスポリシーの例

➢ 以下にアクセスポリシーの例を示す。

例えば“営業は、支給したWindows 10で社外から企業データへのアクセスが可能、但しコントロール要件を満たしたもののみ“というポリシーの動作例