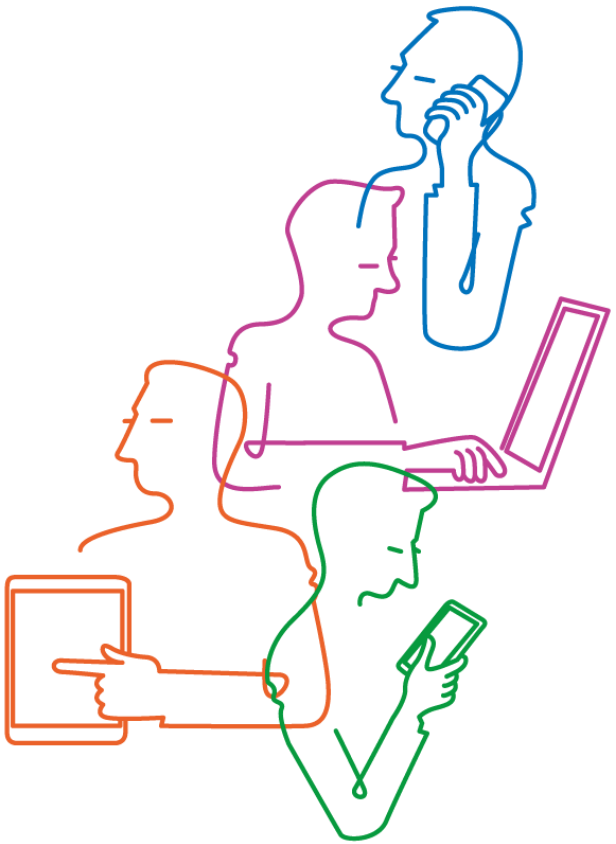
YOKOGAWA

# どうなる！？
# Win10でのアカウント認証

～AD以外もアリ！各社の解決手段を語ろう～

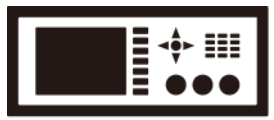


横河レンタ･リース株式会社

# 横河レンタ・リース株式会社

| | |
|---|---|
| 設立 | 1987年1月23日 |
| 資本金 | 5億2,800万円 |
| 代表者 | 代表取締役 社長　金川 裕一 |
| 従業員数 | 780人（男性492人、女性288人）※ 2019年4月現在 |
| 主な株主 | 横河電機㈱47.35% 芙蓉総合リース㈱47.35% 他5.3% |
| 主な事業 | |

パソコン・IT機器
レンタル



計測器
レンタル

システム
事業

Hewlett Packard Enterprise
Platinum Partner

# ソフトウェア開発の膨大な経験

PC-COEからDotCOE、Flex Work Placeへ

米国ヒューレットパッカードで
14万台のPCを標準化社内ツールを日本で商用化

**PC-COE**

**1993年頃～**
横河ヒューレット・パッカード
（現日本ヒューレット・パッカード）

クライアントPC管理ツール
**DotCOE**

**2003年～**
横河レンタ・リース

データレスPC™ソリューション
Flex Work Place

**2013年～**
横河レンタ・リース

北海道電力 様

JCB 様

約**25**年

Windowsクライアントソリューションの開発経験

# 当社は、Windows 10の運用では、
# オピニオンリーダー　各メディアに寄稿/連載

ITmedia エンタープライズ


ZDNet Japan
japan.zdnet.com

# 本日の内容

■Windows 10では、AD必須？

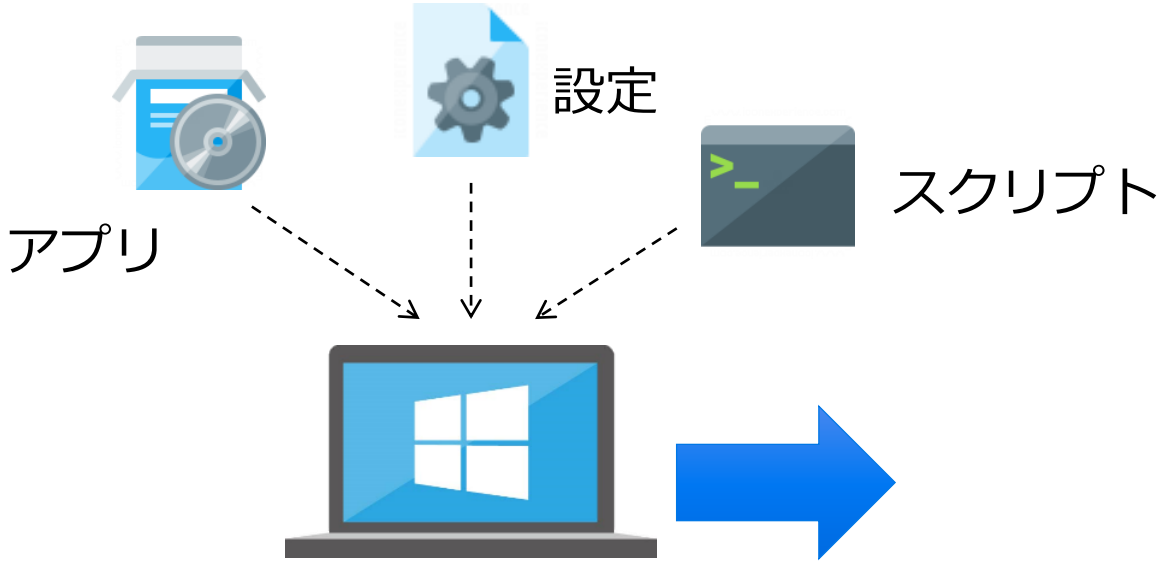
■これからのセキュリティと運用は、ID中心

■“as a Service” にとっても重要なID
　✓Device as a Serviceへ

# Widows 10では、AD必須？

# “プリインストール”は、無理

従来のプリインストール



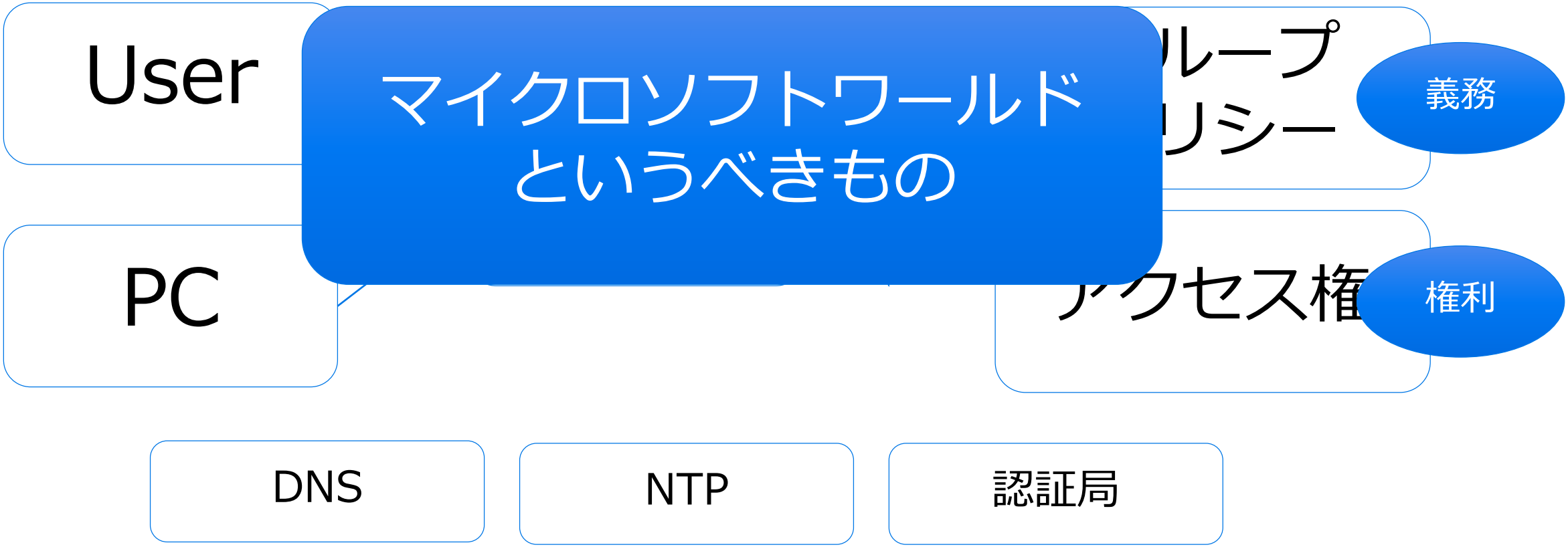

出荷前に詰め込んで、
ユーザーへ出荷
あとは塩漬け

Windows 10は、モバイルOS
基本はダウンロード

OSが
常にアップデート
されるため、
アプリも
アップデートが必要
設定も消えるため、
上書きが必要

# Active Directoryとは？

Active Directory とはマイクロソフトによって開発されたオンプレミスにおけるディレクトリ・サービス・システムであり、Windows 2000 Serverから導入された、ユーザとコンピュータリソースを管理するコンポーネント群の総称である。



# AD ≠ Azure AD
# Azure ADは、スタンダードなIDaaS

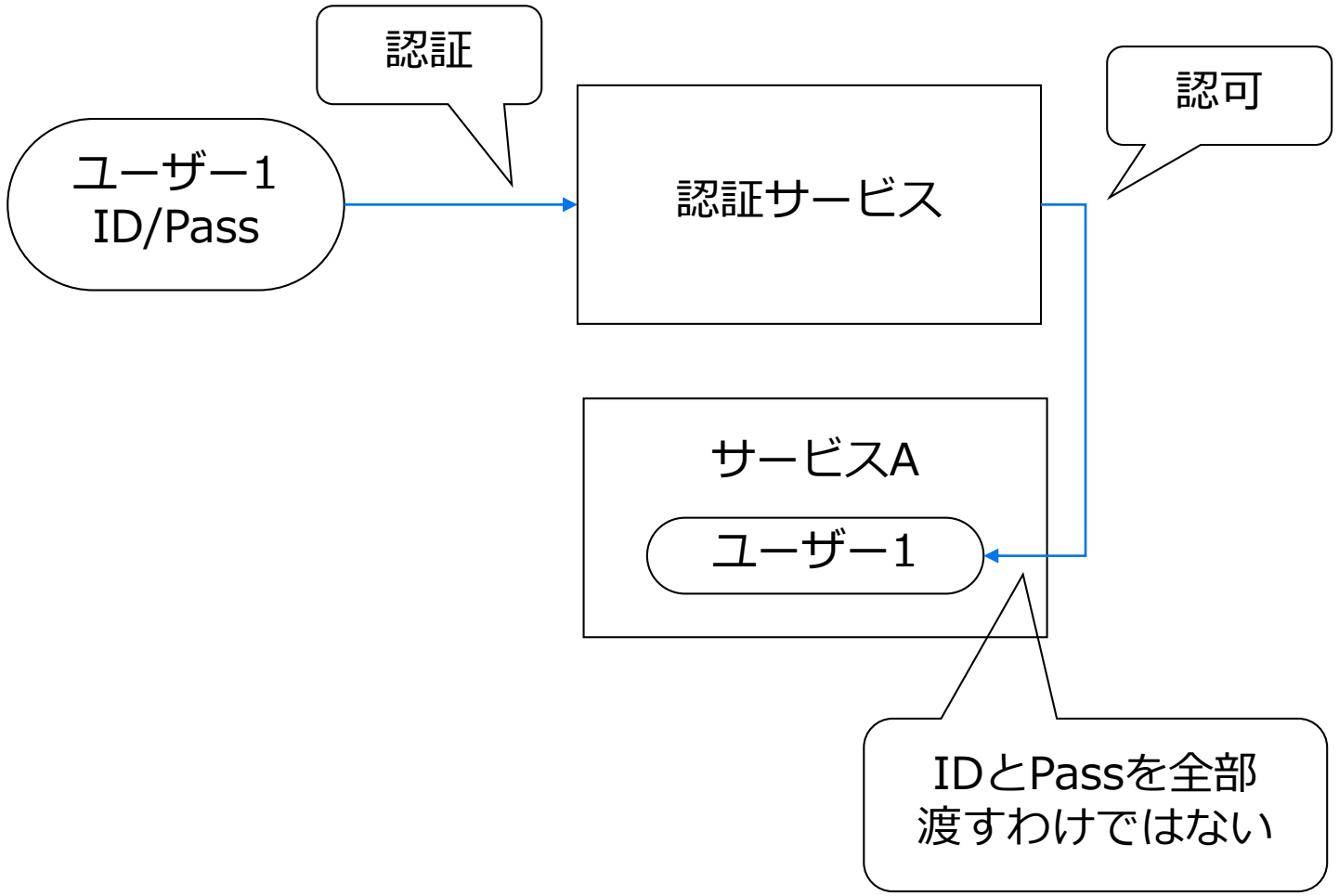
（ID as a Service）

| | | |
|---|---|---|
| AD | グループ<br>ポリシー | アクセス権 |
| Azure AD | | アクセス権 |

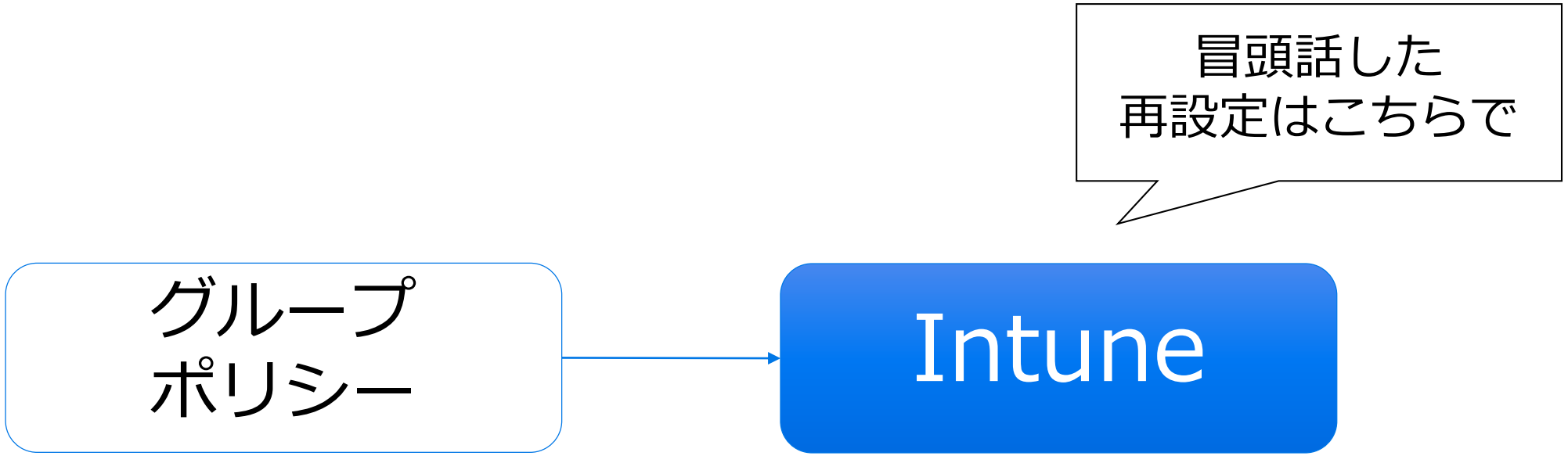
# 認証と認可

■認証（Authentication）
　✓誰か特定する。

■認可（Authorization）
　✓権限を与える。



# グループポリシー（義務）は？




MDM（Mobile Device Management）や
MAM（Mobile Application Management）で行う。

# Azure ADはややこしい?

■Azure AD Connect

■ADFS (Federation Service)

■Hybrid Azure AD Join

オンプレADが
あるから必要

# 移行は、ちょっとややこしい

■ユーザープロファイルの問題
- ✓ローカルユーザー
- ✓ドメインユーザー
- **✓Azure ADユーザー　←1種類増えている**

# Azure ADは、快適
# （Azure ADユーザーでログインする）

■Windowsにログイン　→そのまま資格情報をSSOに利用

■Office 365の各種アプリケーション

■Azure ADを認証プロバイダーに設定した各種クラウドサービス

# オンプレADがやめられない

■考えられるやめられない理由
- ✓ファイルサーバー
- ✓プリントサーバー
- ✓社内Webサーバー

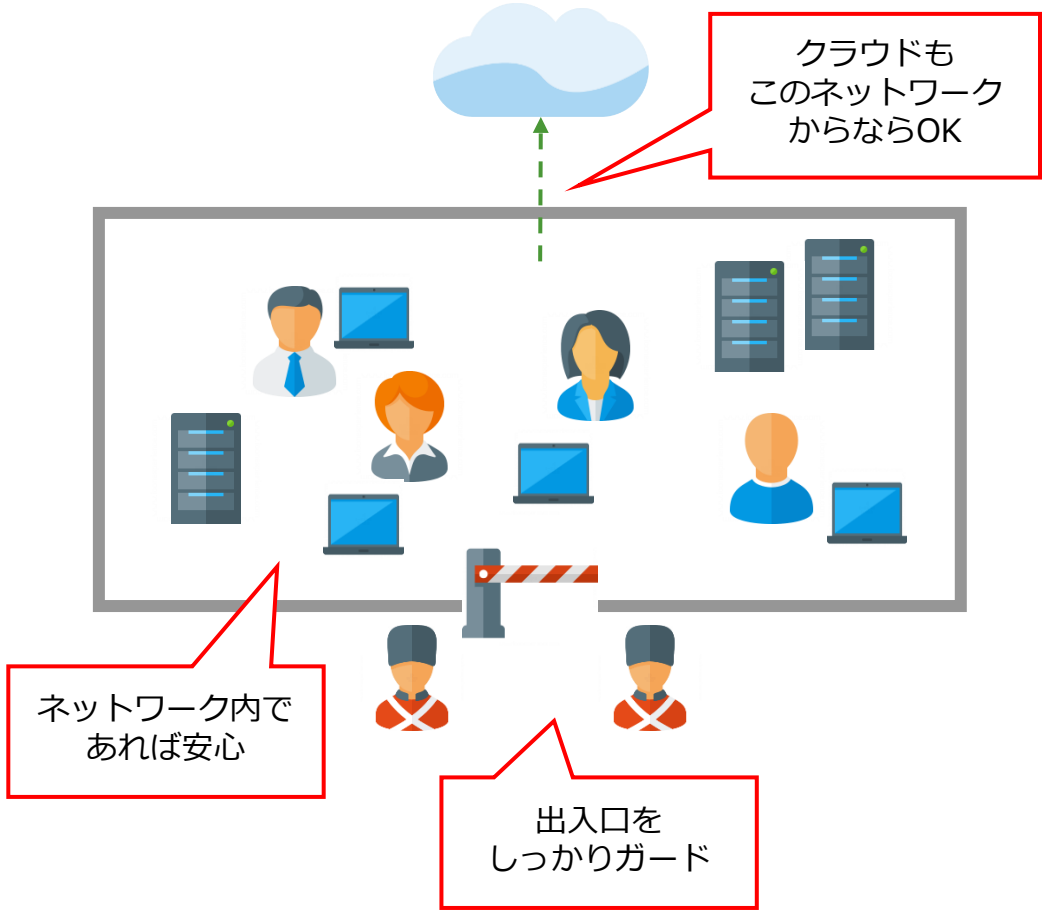
■最近、Kerberos認証はAAD Connectを経由できるようになった
- ✓Hybrid Azure AD Joinは、役割を終えつつある（早かった…）

逆にオンプレADがないからと
Win10のためだけに入れちゃダメ

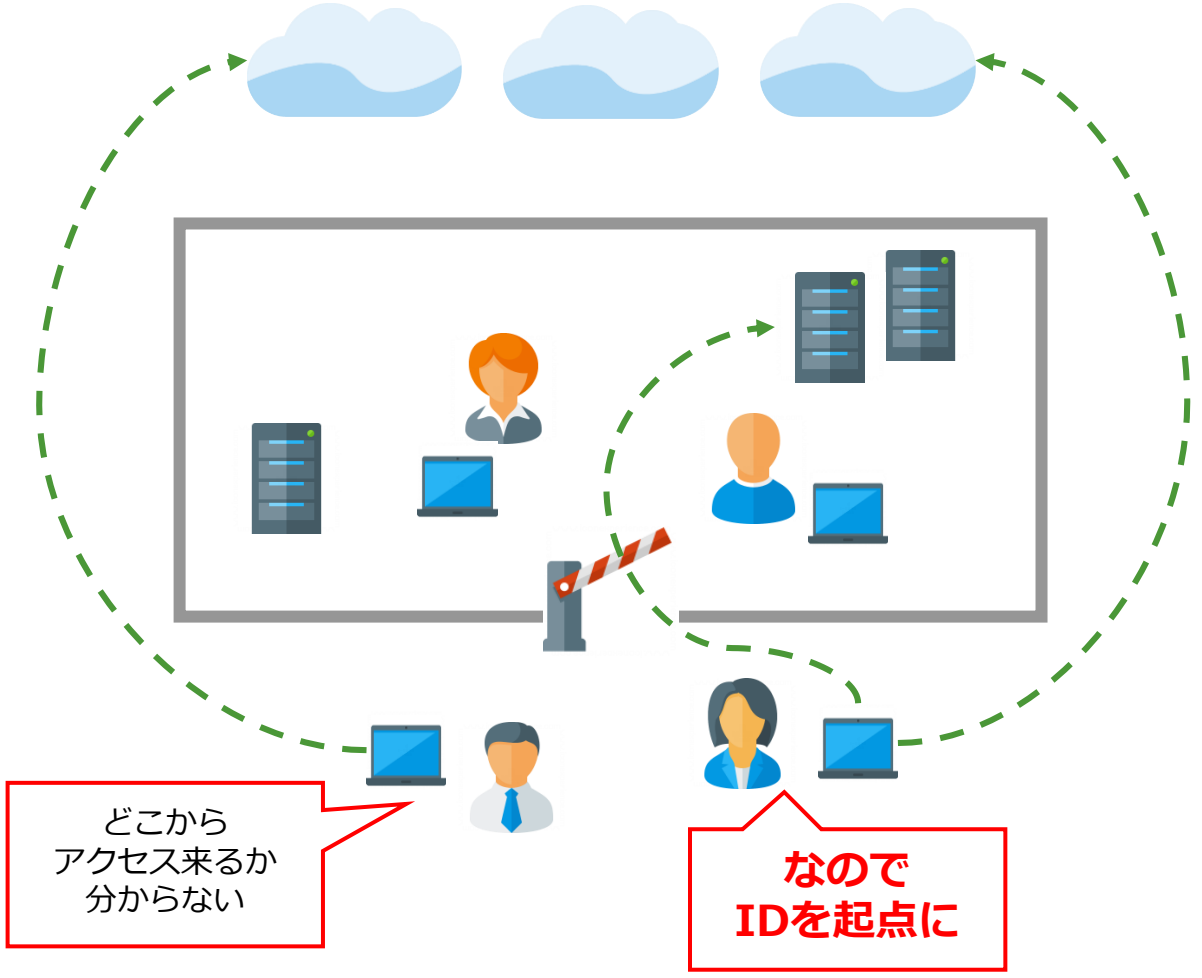

これからのセキュリティ
と運用は、ID中心

# 重要度が増す、ID

## 従来のセキュリティ




## これからのセキュリティ



# ゼロトラスト（信用ゼロ）とは？

# Azure ADの条件付きアクセス
# →IDaaS選定のもっとも重要な要素

■Azure AD Premium P1が必要

■認証プロバイダーをAzure ADにすることで、様々なクラウドサービスに同じポリシーを適用できる

Azure ADに参加しているデバイス以外からのアクセスを禁止できます

それ以外のデバイスからのアクセスは、Office Onlineのみ、ダウンロード禁止なども可能

# Windows ゆえの注意点

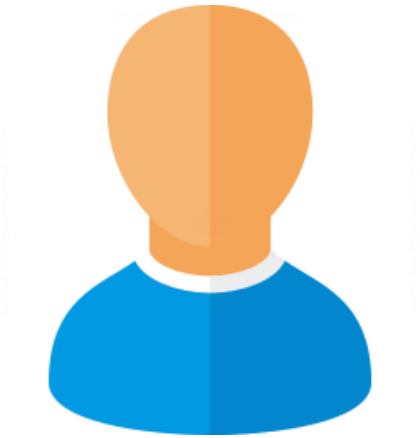
■このデバイスの管理者、という形のローカル管理者という設定ができない。（デバイス管理者を割り当てたユーザーは、すべてのデバイスが変更できる。）

■Azure ADは、「参加」と「登録」で意味合いが違う。

- ✓参加　→従来のドメインに参加の意味合い　＝Intune等のMDMから設定やアプリが強制的に入る。企業のデバイス。
- ✓登録　→許可されたデバイス　＝BYODの等のシナリオ

■デバイスに証明書をインストールするタイプの、ユーザーに紐づかないデバイス認証ソリューションは、これから難しくなる。

# IDを起点にする運用

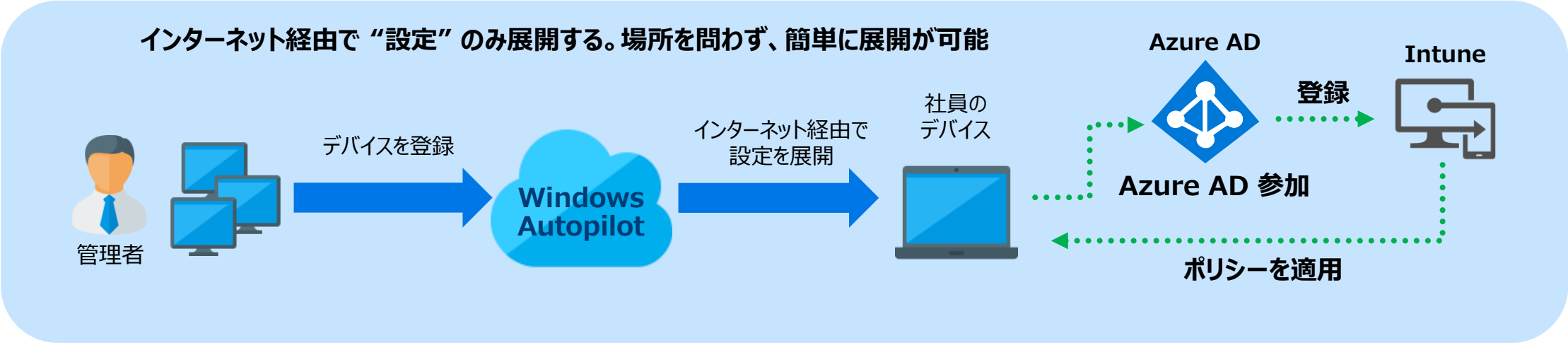


# Windows Autopilot

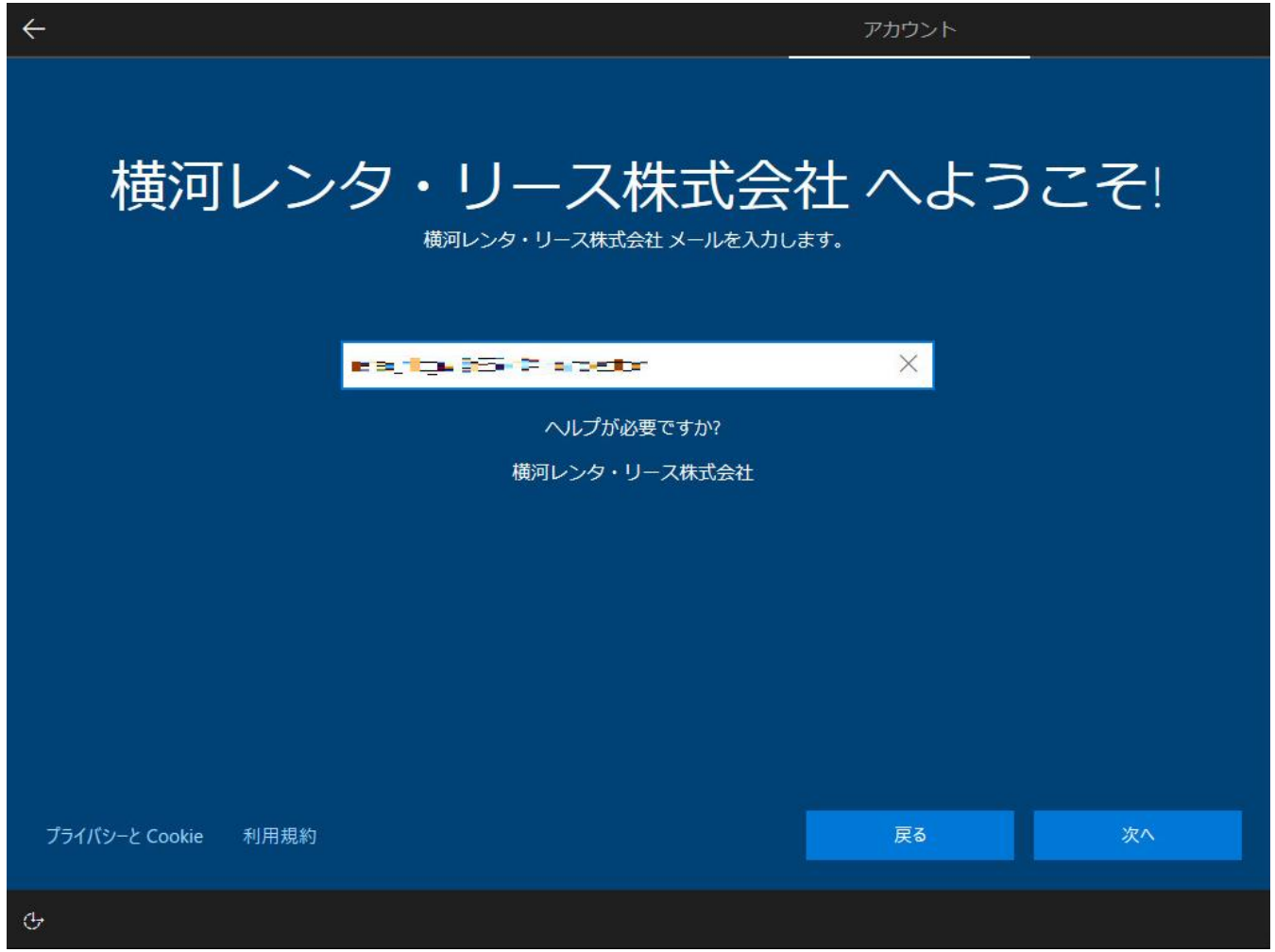
■マイクロソフトが提供する、クラウドからOS展開をサポートするサービスです。

- デバイスの情報とAzure AD のユーザー情報をベースに、Windows 10 初回起動時の OOBE（Out-Of-Box Experience）セットアップを簡易化

- そのデバイスはAzure ADに自動的に参加され、Intuneを併用することにより、Windows 10 に必要な各種構成やアプリを展開

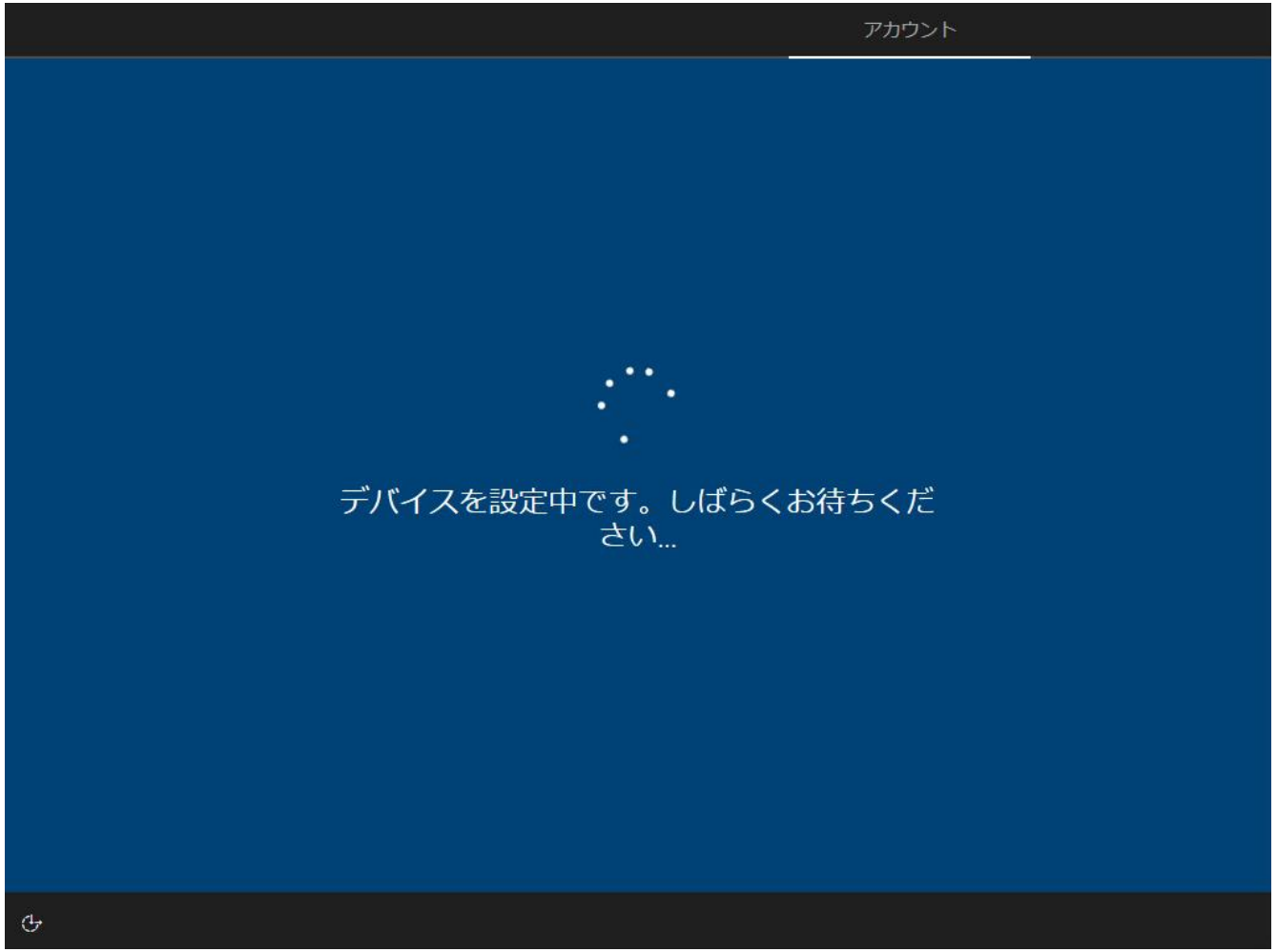


# AutoPilot 展開イメージ①




ユーザーは配布されたPCを起動し、Azure ADアカウントでサインインします。

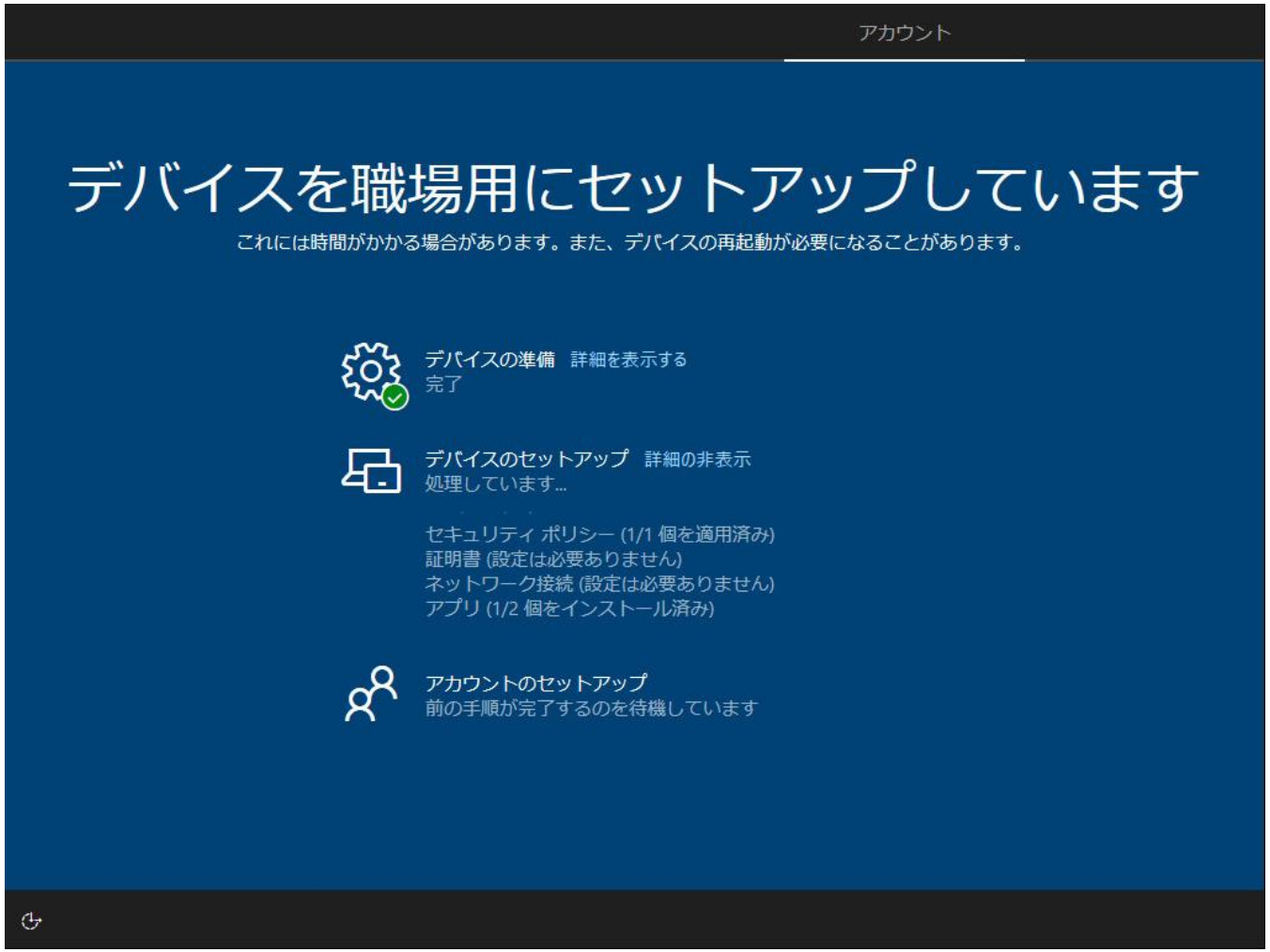
# AutoPilot 展開イメージ②




自動的にOOBEのデバイス設定が始まります。

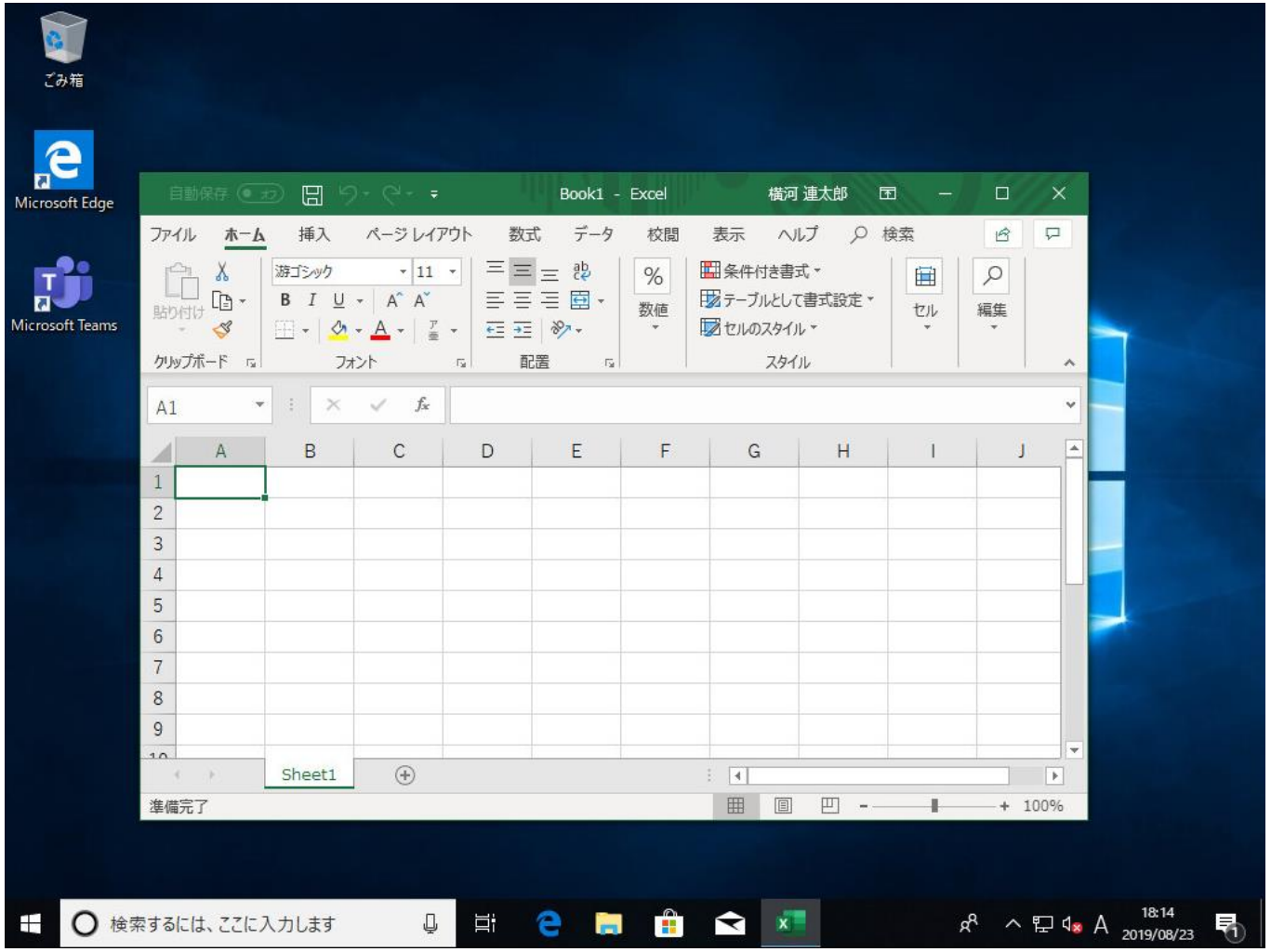
OOBEは自動で完了します。

# AutoPilot 展開イメージ④




Intuneから、ポリシーやアプリケーションが配備されます。

# AutoPilot 展開イメージ⑤




セットアップが自動で完了し、
企業用PCのセットアップが完成
します。

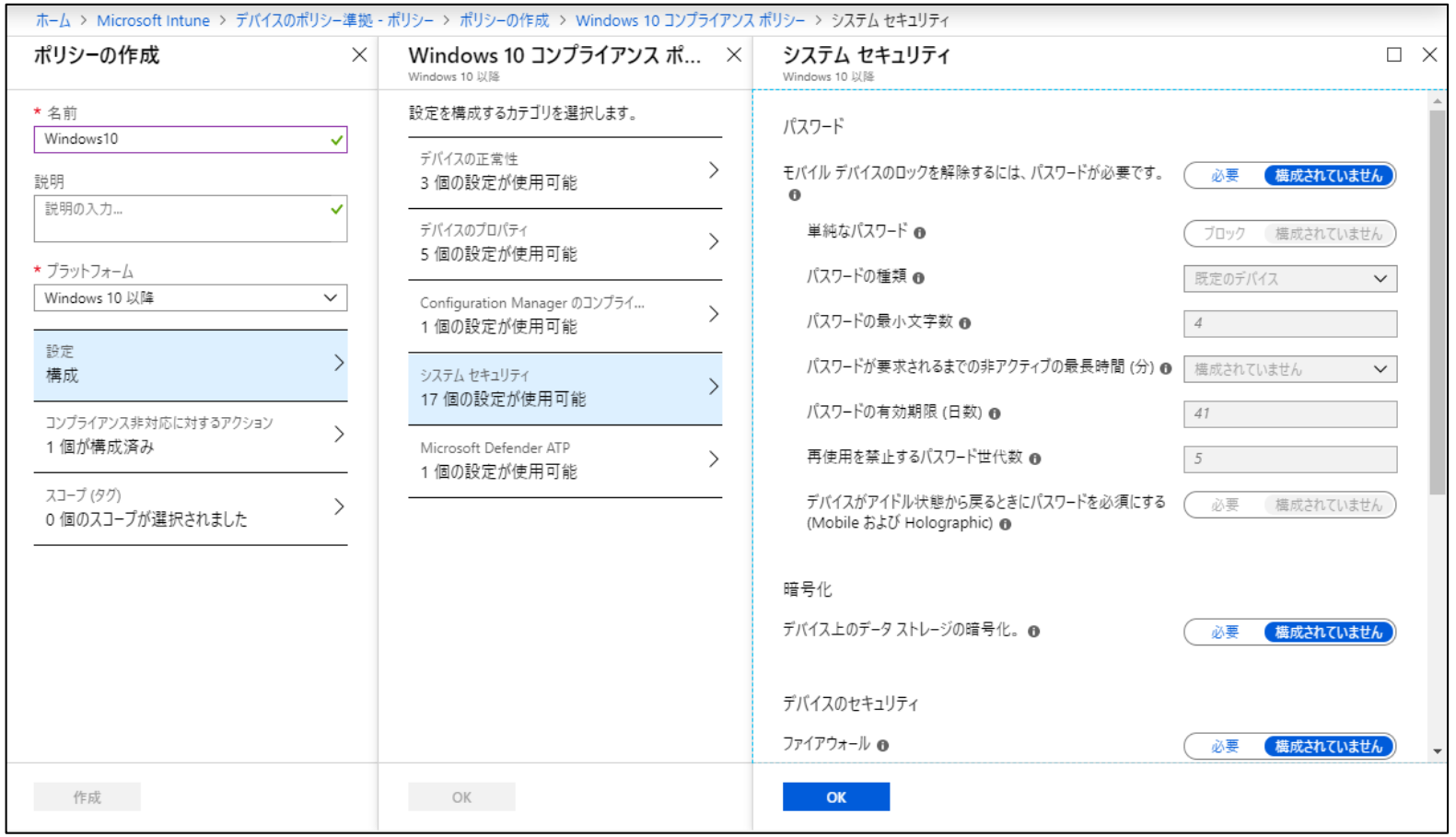
# Intune 管理画面イメージ①

デバイスのインベントリ情報の確認や、リモートワイプ、リモート再起動といった一般的なMDMツールの機能が備わっています。

# Intune 管理画面イメージ②

企業デバイスに対するセキュリティのポリシーを設定することができます。

企業デバイスは、PCの他にモバイルデバイスも管理できます。



# Intuneによる
# アプリケーションのインストール

■ストアアプリ　→ユーザー自身で

■C2R、MSI　→サイレントインストールオプションとともに
　✓Office 365 ProPlusは、C2R。White Gloveも利用可能。

■その他、スクリプトなど　→パッケージ化する

# クローニングは、やめよう

■アップデートについていくのが大変。

■Sysprepの癖がどんどん強くなっている。

■無駄に情シスが頑張るのはやめよう。

- ✓ファーストラインワーカーとナレッジワーカーを分けよう。
- ✓ナレッジワーカーは提携作業をしているわけではないので、様々なツールを使いながら生産的に仕事をしていく必要があるはず。（変に情シスが固定的な環境を提供していませんか？）

前回も言ったけど・・・

# “as a Service” にとっても重要なID

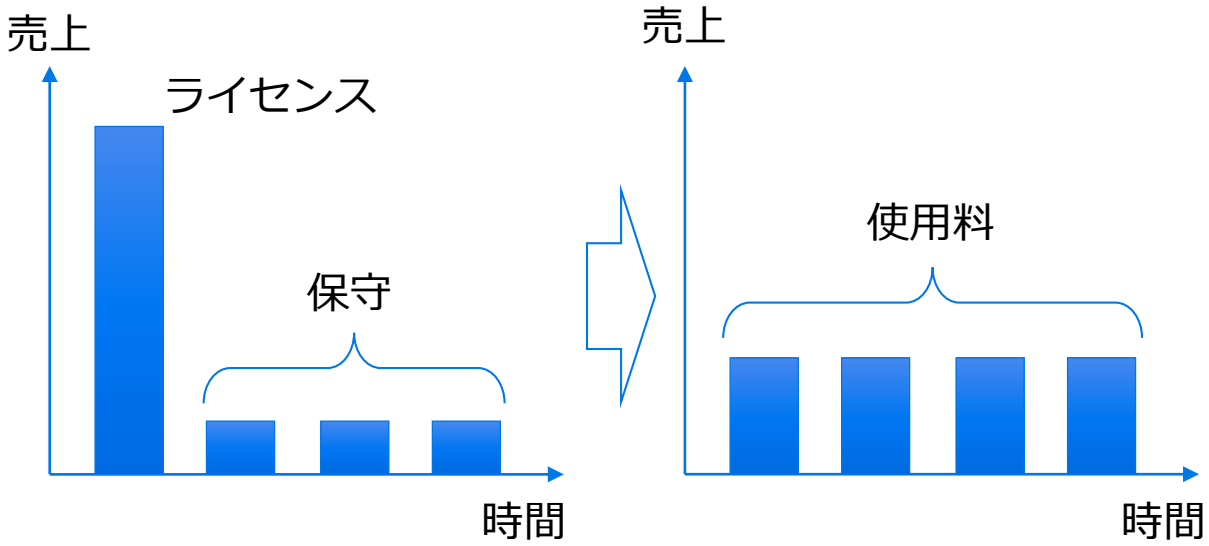
# “As a Service” とは？

■「モノ」を買う　＝買ったモノを運用していくのは管理者
■「サービス」を受ける　＝運用された状態の「モノ」を提供

管理者を介さない ＝ ユーザーダイレクト

**ユーザーを特定するIDが必要**

# サブスクリプションは、“as a Service” が必須になる




**従来の販売**

最初にドンっと
ライセンスの売上が入る

**“as a Service”**

最初に売上が入らない
徐々に売り上がっていく

継続的に利用してもらう必要がある


解約リスクがもっとも高まるのは、サポート終了。
そこを作らないために、自動でアップデートされる必要がある。

サポート終了で解約

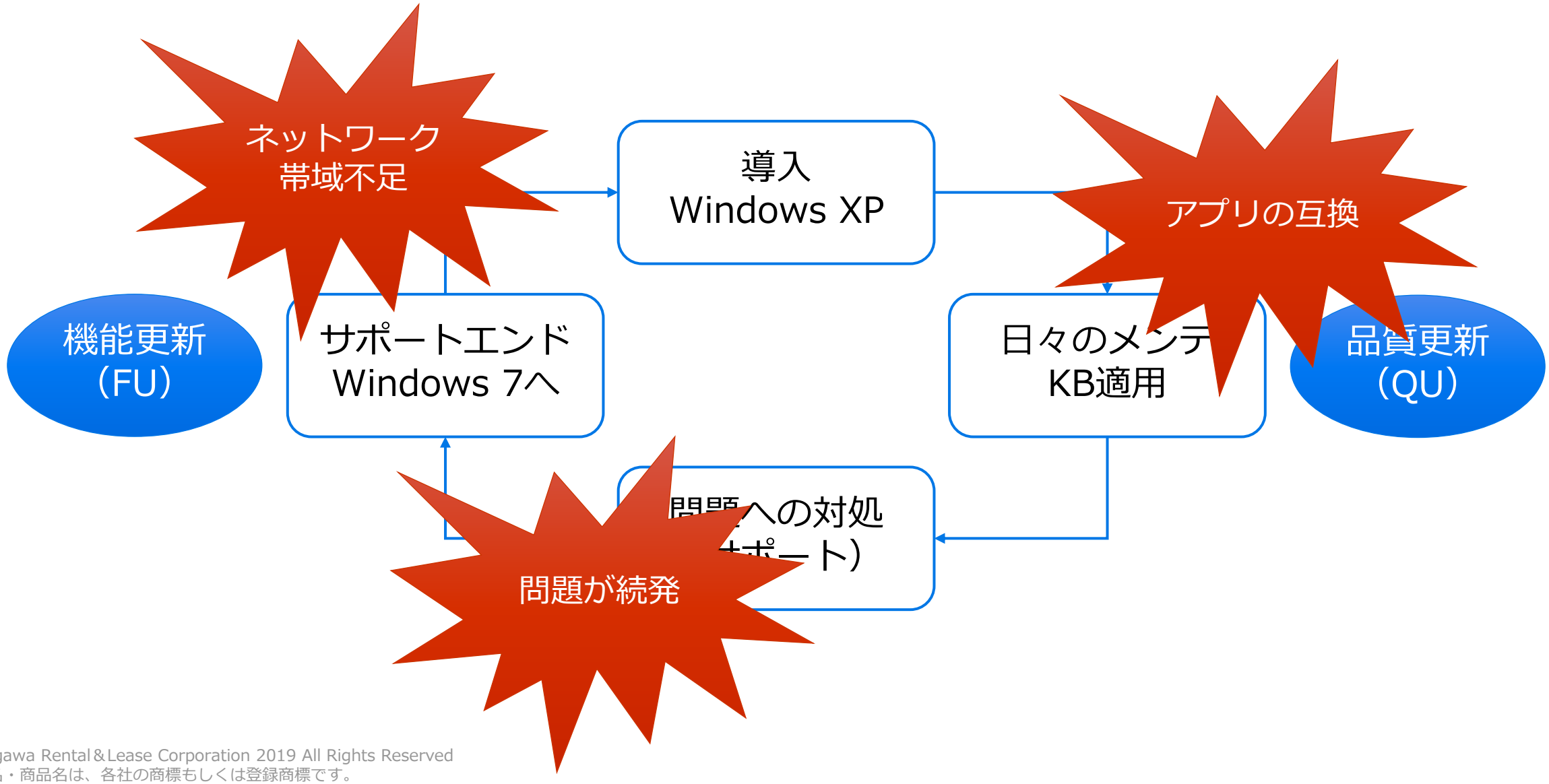
人の出入りに際して、足りないから買う、あれば買わないという調整をするために管理が必要。
サブスクリプションなら、その調整は必要ない。

資産管理が不要に

# Windows as a Service


こんな絵で
よく語られますが

# Windows as a Serviceの本質



# Windows as a Serviceを阻む壁

アプリケーション

全てのアプリが
“As a Service” に
なれば解決

ネットワーク

ゼロトラストで
クラウドダイレクトに
なれば解決


デバイス（PC）

? ? ?

# 今は過渡期だから必要 Unifier Cast

※ これは、CMです。

Windows Update

MicrosoftのWindows Updateから
FU/QU/SSUなどのアップデータを
自動取得、配布可能形式に変換

自動で
ダウンロード

**Feature 1**
ネットワークの
負荷を上げない
分散配布

Unifier Cast

拠点A

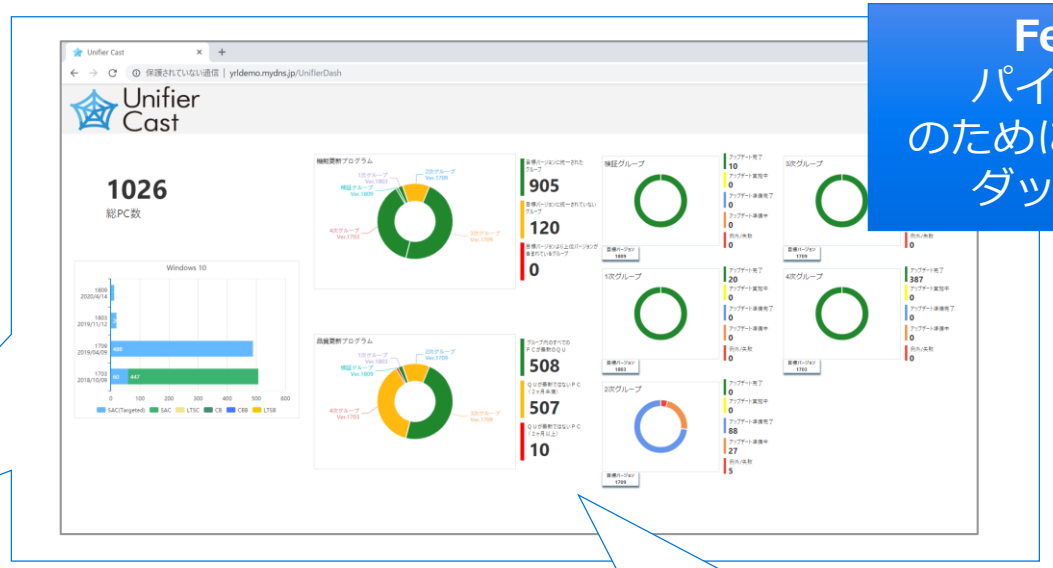
拠点B

拠点でサーバーに
アップデータを取りに行く
PC台数を予め設定可能

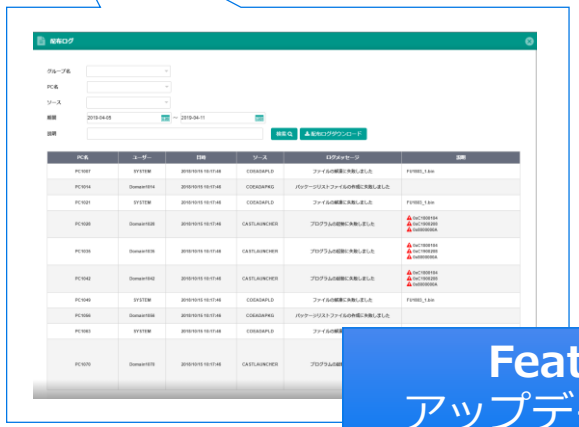
拠点内でデータブロックを
共有する

細かいデータブロックに
分割して配布

従量課金のモバイルNWの場合、
ダウンロードを停止することも可能




**Feature 2**
パイロット運用
のために状況を可視化
ダッシュボード



**Feature 3**
アップデート失敗の
情報を収取し、分析
強力なトラブル
シューティング機能

データブロック取得中に
拠点を移動しても、
異動先で不足のデータブロックを
持つPCを探して受信を継続

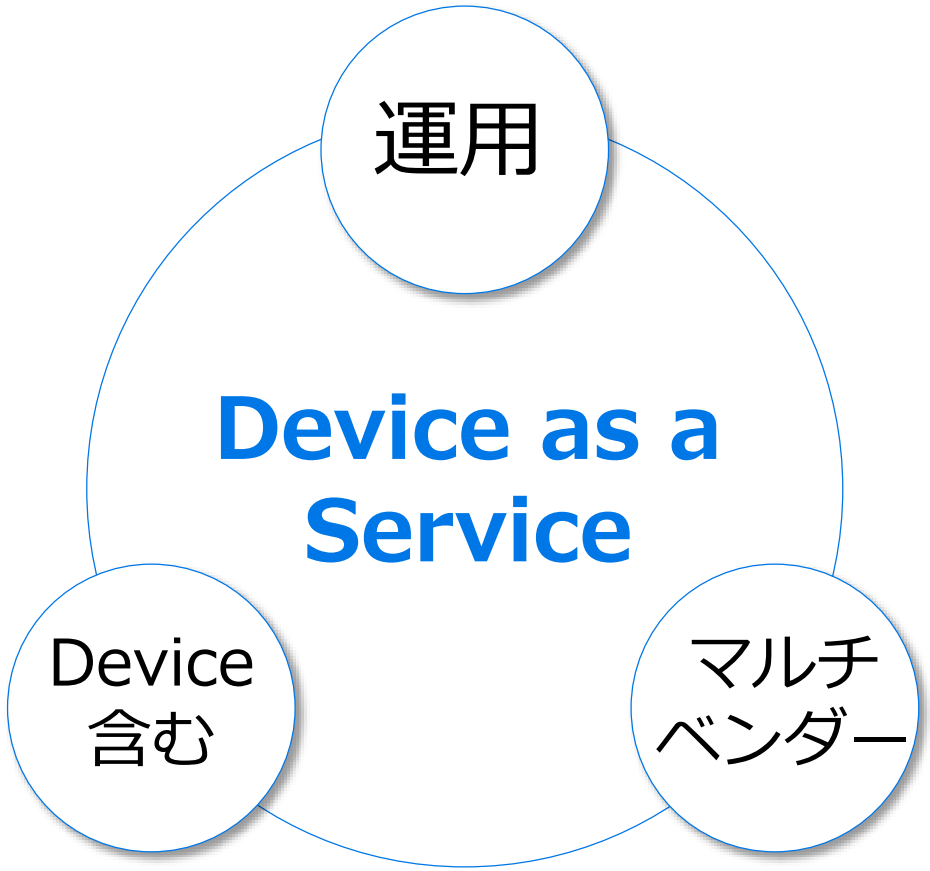
設定変更などは不要

# 残るデバイスをどうしよう

デバイス（PC）

**？ ？ ？**

# より進化した
# “ Device as a Service “ へ




マイクロソフト 曰く、

**2020**年までに

約**30**%のPCが

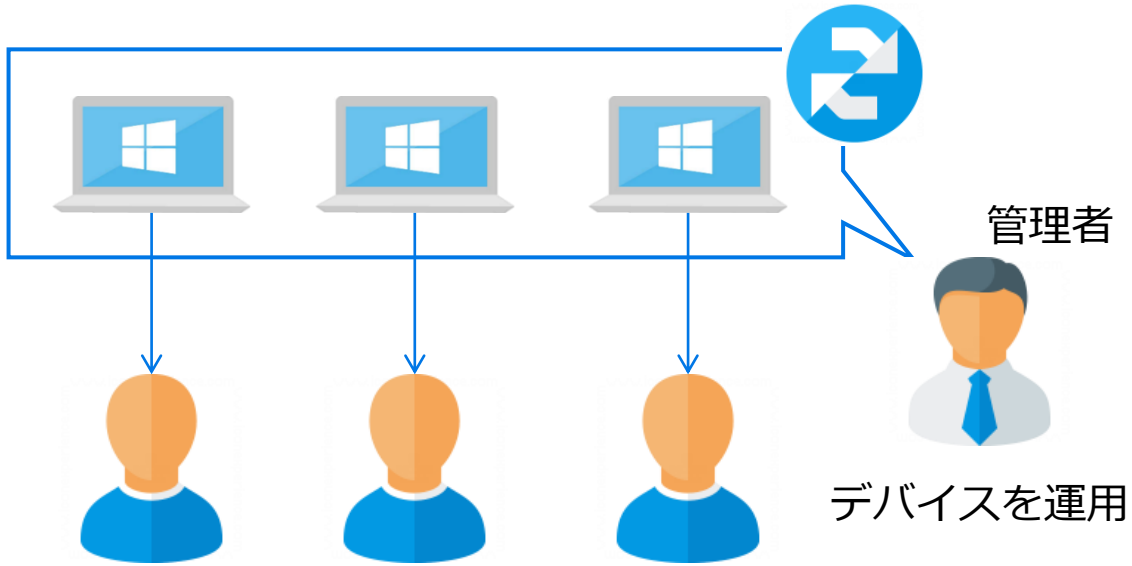
このDaaSで調達される

# Device as a Serviceとは？

※ 諸説あります。

## モノのPC＝管理者が運用

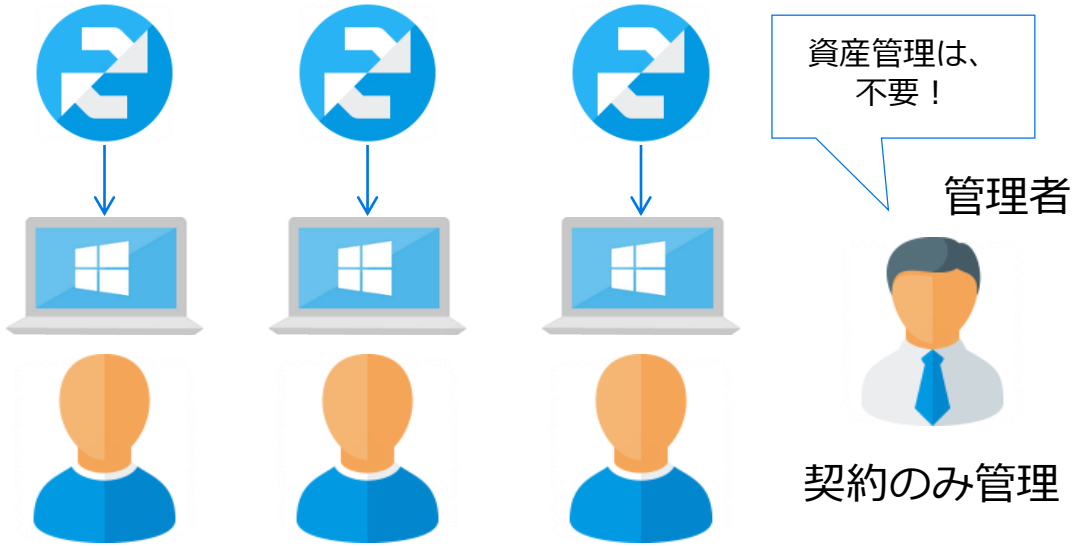
管理者がデバイスをモノとして調達し、
モノを中心に管理、ユーザーへ提供する。




機器の選定・調達からリプレースまで
管理者の責任

## Device as a Service

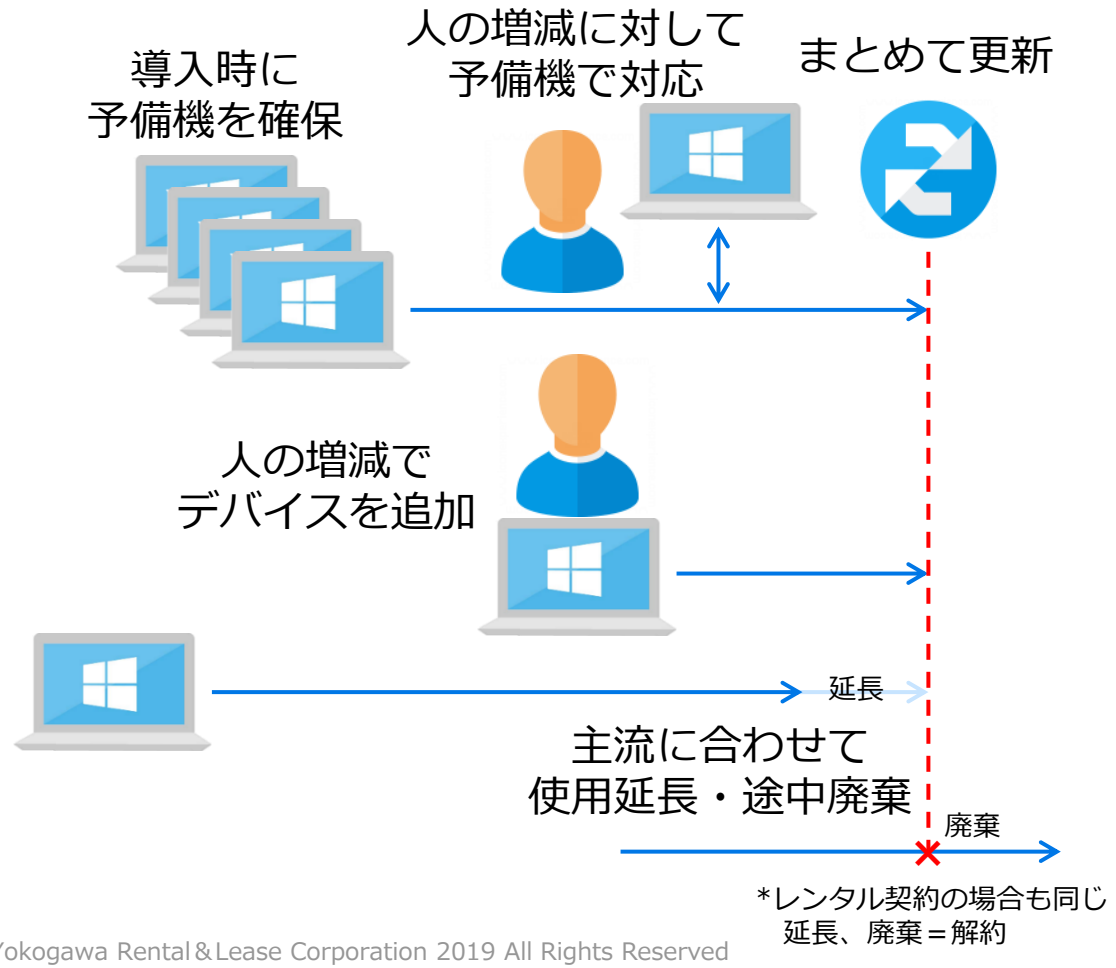
ユーザーは個々にデバイスをサービスとして受ける。
デバイスは、定期的にアップデートされる。



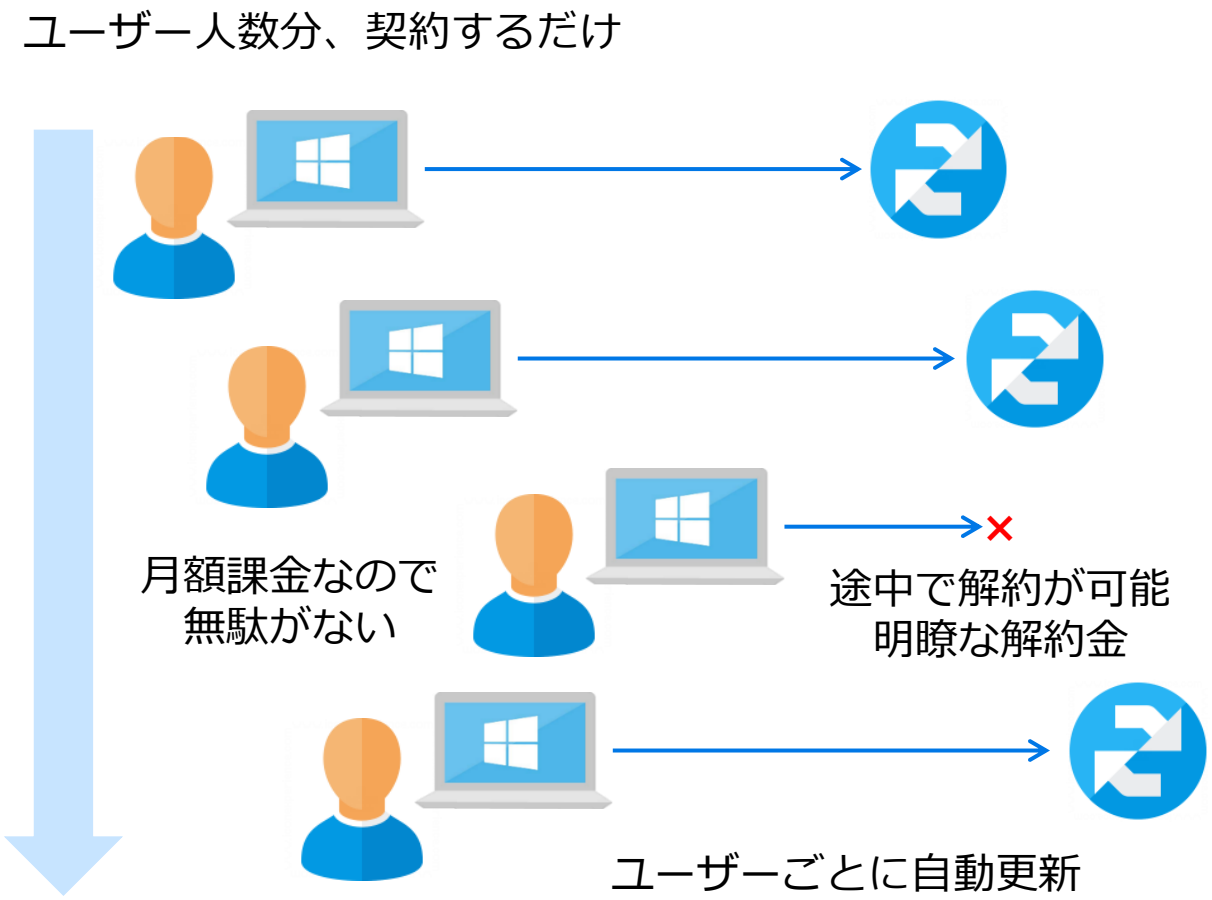

機器選定は、ユーザー
調達とリプレースは、ベンダーの責任

# ユーザーダイレクトに価値を届ける

## モノのPC＝管理者が運用




## Device as a Service



# Device as a Serviceの便益

## ユーザーが最適なデバイスを選択

Microsoft Surface
Lenovo
dynabook
VAIO
hp
DELL
Mac Pro
NEC
Panasonic
Let's note

**YRL's Choice**

膨大な年間調達量を
誇る当社だから
最適な価格で提供可能

## サブスクリプションに一本化して管理

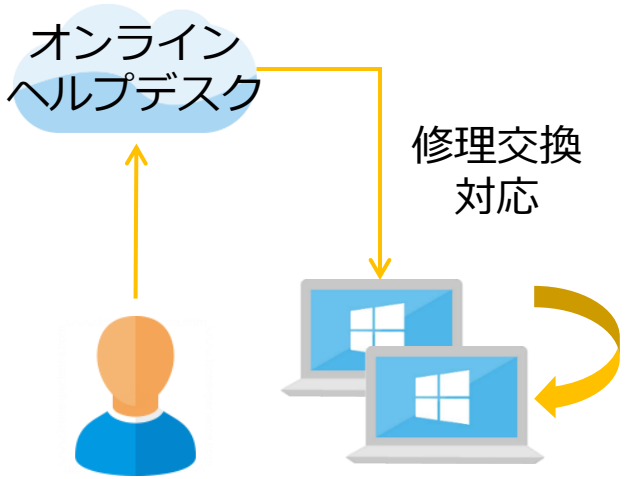
OpenID®

グローバル標準の
Open ID Connectに準拠

Microsoft
box
salesforce
G Suite
zoom
slack

デバイスと一緒に
サブスクリプションで管理
追加購入も可能

## サポートは、ユーザーダイレクト




Free

管理者を介さず
オンラインで直接
ユーザーをサポート

*リリース当初は、Microsoft・Google・Boxの追加購入に対応予定。

# 本日のまとめ

■Win10でADは、必須ではない。
　✓アプリや設定をネットワークで配れる必要はある
　　＝IntuneなどのMDMが重要

■ゼロトラストネットワーク前提の世界へ
　✓セキュリティも、運用もIDをベースに提供される
　✓IDaaSを持とう！

■Device as a Serviceへ

YOKOGAWA

横河レンタ・リース株式会社
Yokogawa Rental & Lease Corporation

本資料に記載されている横河レンタ・リース株式会社の製品情報は、本書の各項目に関する発行日現在の横河レンタ・リース株式会社の見解を表明するものです。ここに記載した情報に対していかなる責務を負うものではなく、提示された情報の信憑性について保証できません

本資料は、横河レンタ・リース株式会社の内部情報および一般情報他、信頼できると判断した情報をもとに作成されておりますが、横河レンタ・リース株式会社は、その内容について、真実性、正確性および完全性を保証するものではありません。また、本資料には、横河レンタ・リース株式会社の主観的意見が含まれることがあります。

横河レンタ・リース株式会社は、本資料の内容について、事前の予告なく将来にわたって変更することがあります。

# Office 365から学ぶ
# IDを中心としたサブスクリプション

| | Office 365 ProPlus | 従来のソフトウェア |
|---|---|---|
| ライセンス | Azure AD<br>ユーザー紐づき | 所有<br>＝資産管理が必要 |
| 利用開始手続き | Office 365 Portal | 営業、メール |
| インストール | Office展開ツール<br>Office CDN | メディアダウンロード |
| アップデート | Office CDN | メディアダウンロード |
| 稼働把握<br>フィードバック | 各アプリから<br>ユーザーダイレクト | 営業、メール |
| セキュリティ | ユーザーID起点の多要素<br>ゼロトラスト | 社内ネットワークは安全 |