



## マイクロソフトのクラウド戦略からひも解くIoT活用ポイント

東京エレクトロン デバイス株式会社  
クラウドIoT カンパニー  
バイスプレジデント  
西脇 章彦

会社名	東京エレクトロン デバイス株式会社
設立年月日	1986年3月3日
代表者	代表取締役社長 徳重 敦之
上場証券取引所	東証一部（証券コード：2760）卸売業
資本金	24億9千5百万円（2019年3月31日現在）
売上高	1,410億円（2019年3月期）
従業員数	連結：1,210名（2019年3月31日現在）
本社所在地	神奈川県横浜市神奈川区金港町1-4 横浜イーストスクエア

## 主な事業内容

1. 半導体及び電子デバイス（EC）事業  
半導体、ボード、ソフトウェア、電子部品の販売、設計・開発
2. コンピュータシステム関連（CN）事業  
ネットワーク、ストレージ、ソフトウェアの販売、保守サービス

## 子会社

株式会社ファースト  
東京エレクトロンデバイス 長崎  
東京エレクトロンデバイス APAC  
東京エレクトロンデバイス 上海  
東京エレクトロンデバイス シンガポール  
東京エレクトロンデバイス タイ  
東京エレクトロンデバイス アメリカ

## 関連会社

Fidus Systems Inc.  
上海新致華桑電子有限公司  
無錫新致華桑電子有限公司



東京エレクトロン デバイス

## 約半世紀にわたる歴史と経験を有する専門商社

1965年 東京エレクトロンで電子部品ビジネスを開始  
1998年 東京エレクトロンから電子部品事業（現：半導体及び電子デバイス事業）を全て譲受け  
2003年 東京証券取引所 市場第2部上場  
2006年 東京エレクトロン からコンピュータネットワーク事業（現：コンピュータシステム関連事業）を承継  
2010年 東京証券取引所 市場第1部上場  
2017年 株式会社アバール長崎（現：東京エレクトロントライセイ長崎）を連結子会社化  
2018年 株式会社ファーストを連結子会社化

## 東京エレクトロンの 電子部品事業・コンピュータネットワーク事業が分離・独立

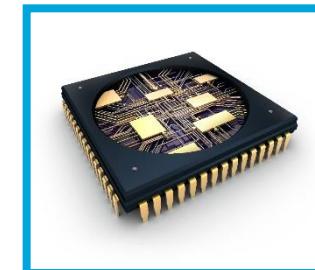
半導体製造装置メーカー  
**東京エレクトロン**

<2017年3月 出資比率33.82%>



1998年  
譲受け

半導体及び電子デバイス  
(EC) 事業



東京エレクトロン デバイス

2006年  
事業承継

コンピュータシステム関連  
(CN) 事業





半導体製品

ボード製品・  
一般電子部品



製品販売

システム  
構築

保守  
サポート



自社ブランド商品

設計・量産  
受託サービス

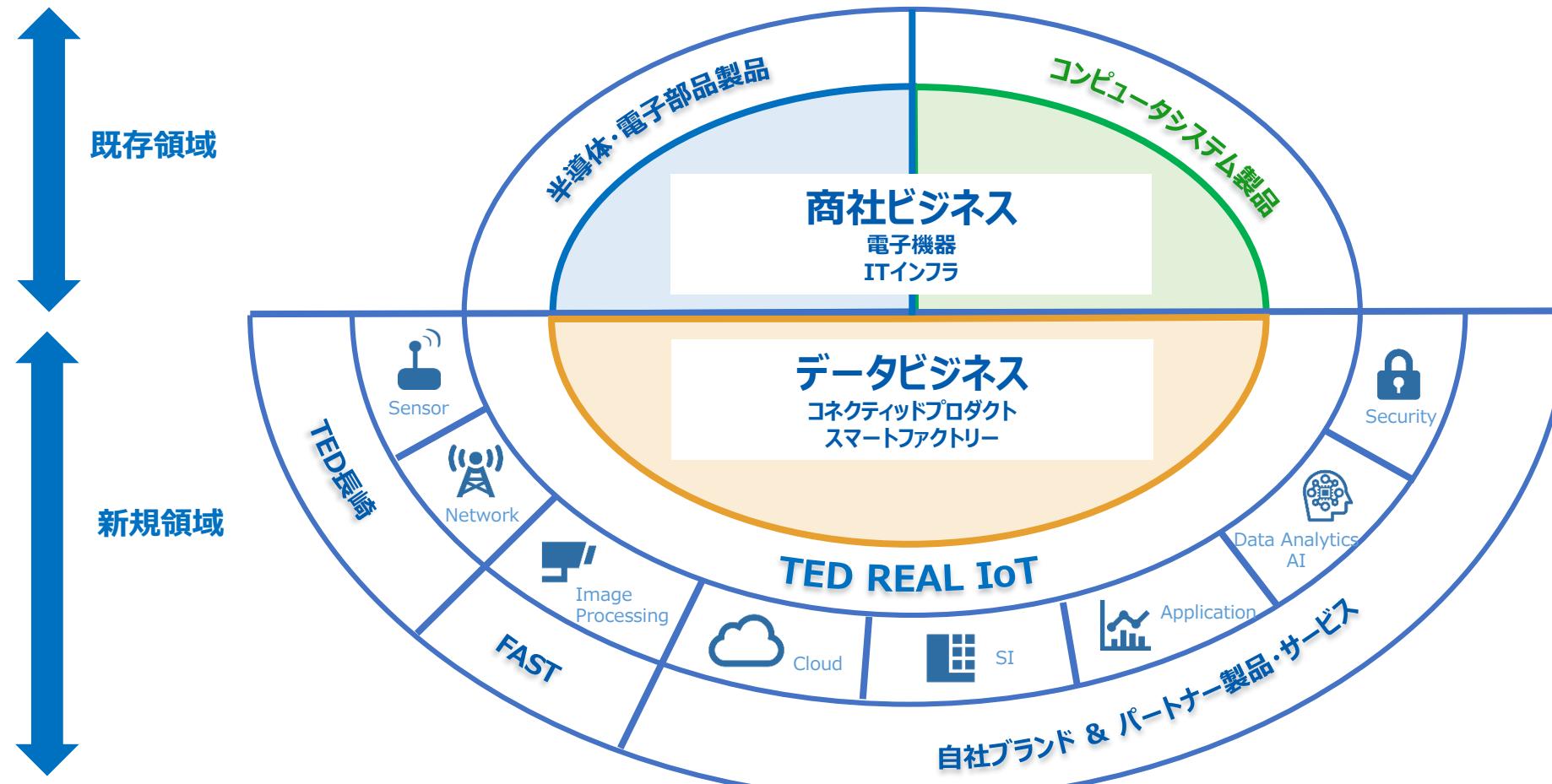


エッジデバイス  
組込ソフトウェア

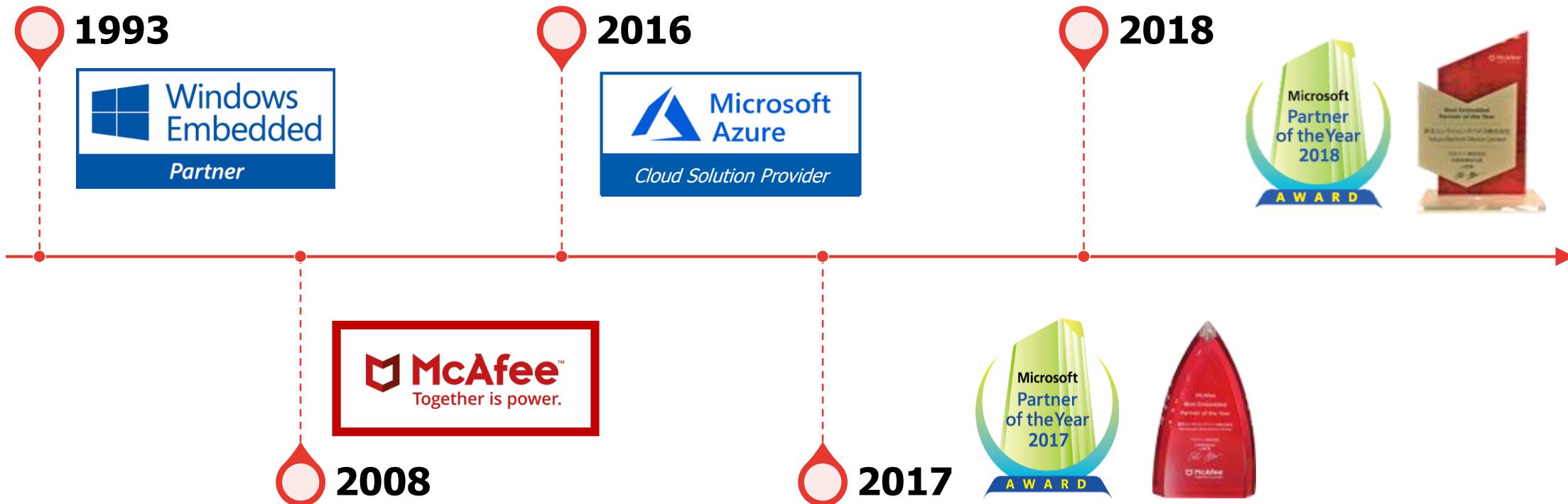
クラウドサービス



産業市場の「デジタルトランスフォーメーション」を推進すると共に  
TED自身のデジタルトランスフォーメーションを推進致します



# マイクロソフト&McAfeeビジネスの沿革



# TEDが提供するマイクロソフト CSPモデルについて



## 1. クラウドに最適な月額従量課金モデル

ライセンスプログラム	オープンライセンス プログラム	CSP	EA (Enterprise Agreement)
販売形態	販売店から卸売販売	販売店から卸売販売	国内の一部パートナーのみ
契約有効期間	12ヶ月有効	いつでも解約可能	長期(3年)
利用契約条件	100ドル単位 プリペイド	従量課金 月額請求	年間約160万円から締結 プリペイド
支払形態	請求書	請求書	請求書
サポート	Microsoft	東京エレクトロンデバイス	Microsoft

## 2. マイクロソフトCSPプログラムにより認定された クラウドディストリビューター



- 競争優位性を示すために、これまで以上にクラウドの導入／運用支援を強化する必要がある
  - ユーザー企業における従来型ITからパブリッククラウドへの移行は加速
  - 先駆的企業と比較すると「技術」「ITスキルの習得」に対する投資が限定的となる傾向

80%

ビジネスリーダーから  
IaaS 移行への  
プレッシャーを受けているCIO

52%

より多くのワークフローを  
クラウドに移行することに  
取り組み

40%

クラウドファースト  
戦略

※引用：Microsoft Digital Trust Summit 2019資料

## アクア『Cloud ITランドリーシステム』



IoT化により業界の枠組みを超えたコラボレーションを実現、オーナーと利用者それぞれのサービスレベルを向上

## 東京電力パワーグリッド『送配電網メンテナンス』



AIを活用することで、「点検作業の効率化」と「点検基準の平準化」を両立

## 加賀市『除雪車の運行管理システム』



除雪経路や稼働状況をリアルタイムに把握し、サービスレベルの向上を実現

## 大矢製作所『摩擦圧着機の生産管理システム』



職人の勘と経験に頼ったものづくりからの脱却を目指して、AI/IoTを活用した生産プロセスの可視化に成功

- デジタルトランスフォーメーションが加速する中、サイバーセキュリティ対策は急務しかし、セキュリティを取り巻く環境は大きく変化している

## 従来型のセキュリティ対策（ネットワーク境界型防御・多層防御）は限界…



世界は会社の外で動いている

### IT環境の変化

- ・アプリケーションのクラウド化
- ・インフラのクラウド化
- ・多様化するデバイス

### 働き方の変化

- ・働く場所、時間の多様化
- ・グローバル化
- ・B to B

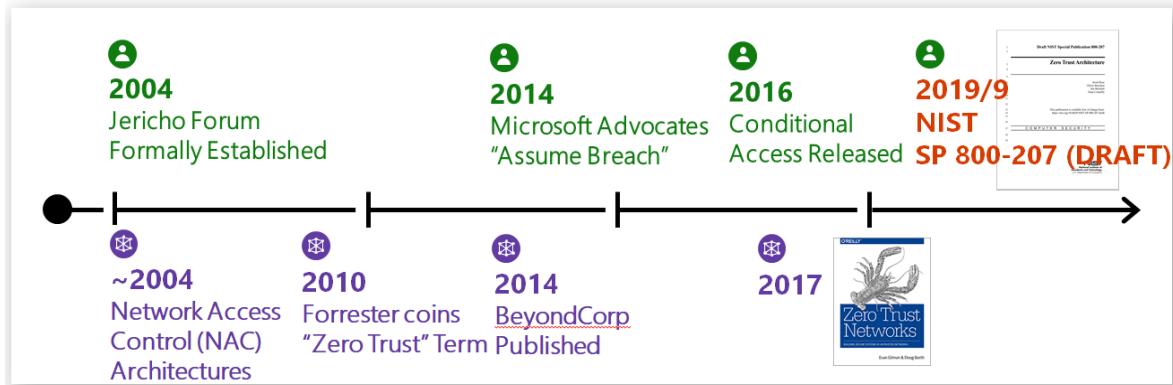
### 驚異の変化

- ・標的型攻撃
- ・内部犯行
- ・ビジネスとしてのサイバー攻撃

## Microsoftのクラウド戦略に セキュリティ を重要な要素と位置づけ

- ネットワーク・人・データ・モノ…全てを信頼せず、本物であることを1つ1つ確認していく  
ゼロトラストモデル の重要性を説いた
- NIST（アメリカ国立標準技術研究所）が標準化を考え始める

### "Zero Trust Model" というデザインの進化



### SP 800-207 (DRAFT)

NIST Zero Trust Architecture (ZTA) :  
<https://csrc.nist.gov/publications/detail/sp/800-207/draft>

ゼロトラストは、ネットワーク防御を広範なネットワーク境界から、個々または小規模のリソースグループに絞り込む、進化するネットワーク セキュリティパラダイムのセットの用語です。A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet). Access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established. ZTA is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary.

ZTA は、ネットワークの場所がセキュリティの主要なコンポーネントと見なされなくなったため、ネットワーク セグメントではなくリソースの保護に重点を置いています。This document contains an abstract definition of ZTA and gives general deployment models and use cases where ZTA could improve an enterprise's overall IT security posture.

## 保護対象：ネットワーク から リソース

## Microsoftのクラウド戦略に セキュリティ を重要な要素と位置づけ

- AIで強化された機械学習を取り入れ、オペレーションの自動化、管理の一元化によるワークフローの自動化をテクノロジとして実現していく

### セキュリティ人材の雇用や教育が困難

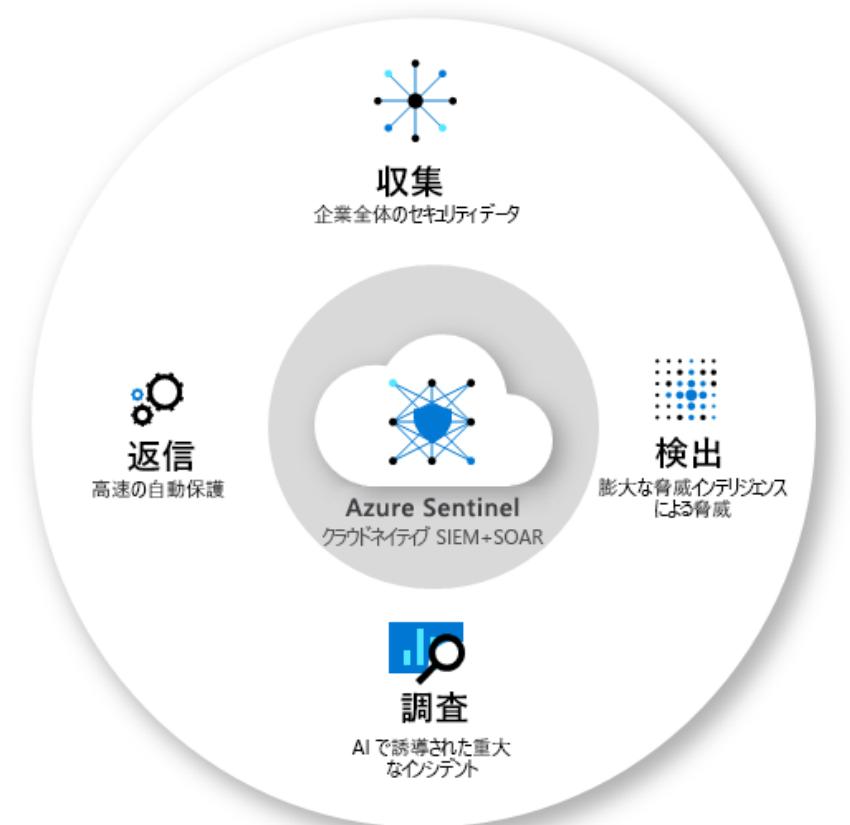
- ・2020年までにセキュリティ人材は1800万人不足すると予想
- ・社内のセキュリティ人材のトレーニングに投資することと、従業員間でセキュリティを意識した文化を構築することが重要

### 複雑な攻撃・判断の難しさ

- ・信頼できるアラートを手にいれるために、大規模なクラウドプロバイダーが持つインテリジェンスや専門知識を活用
- ・自動化されたソフトウェアベースの処理で分析や対応をリアルタイムに行うことが重要

## ● Azure Sentinel=クラウドベースの SIEM+SOAR

- ゼロトラストモデル のセキュリティを推進
- 不足するセキュリティ人材に代わりAIを活用し巧妙化する攻撃からスマートに企業を保護



- ネットワーク境界防衛→ゼロトラストへの変革の時期
- 厳密なデバイス+IDの状態を常に確認することが重要

## <デバイスのモバイル利用でよくある要件・要望>

### 要件

クラウド移行に伴い、場所を問わず、ストレスフリーな会社データへのアクセスをセキュアなデバイスに許可

### 要望

デバイスの状態を継続して評価、状態に応じたアクセス制御、アクションおよび管理者へレポートが必要

安心・簡単なクラウドベースのデバイス管理ソリューション

【 Microsoft 365 + McAfee MVISION Cloud 】



## 安心・簡単なクラウドベースのデバイス管理ソリューション ～ Microsoft 365 + McAfee MVISION Cloud ～

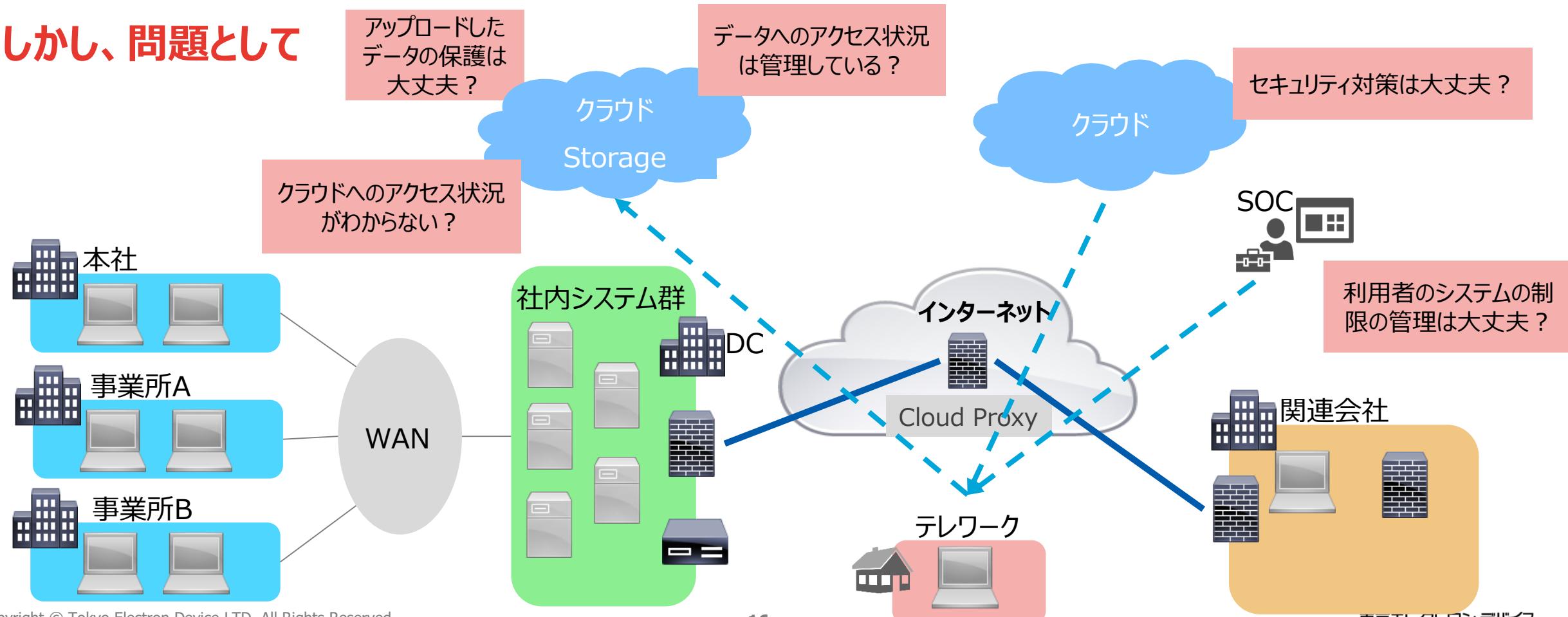
クラウドIoTカンパニー  
エンベデットソリューション部  
グループリーダー  
新谷 和之

# 昨今の企業インフラ

## ■ 取り組みイメージ

- 昨今、企業様ではテレワークなど外部から仕事をすることが多くなってきております。
- その上で、オンプレからクラウドへ移行してきております。

## しかし、問題として

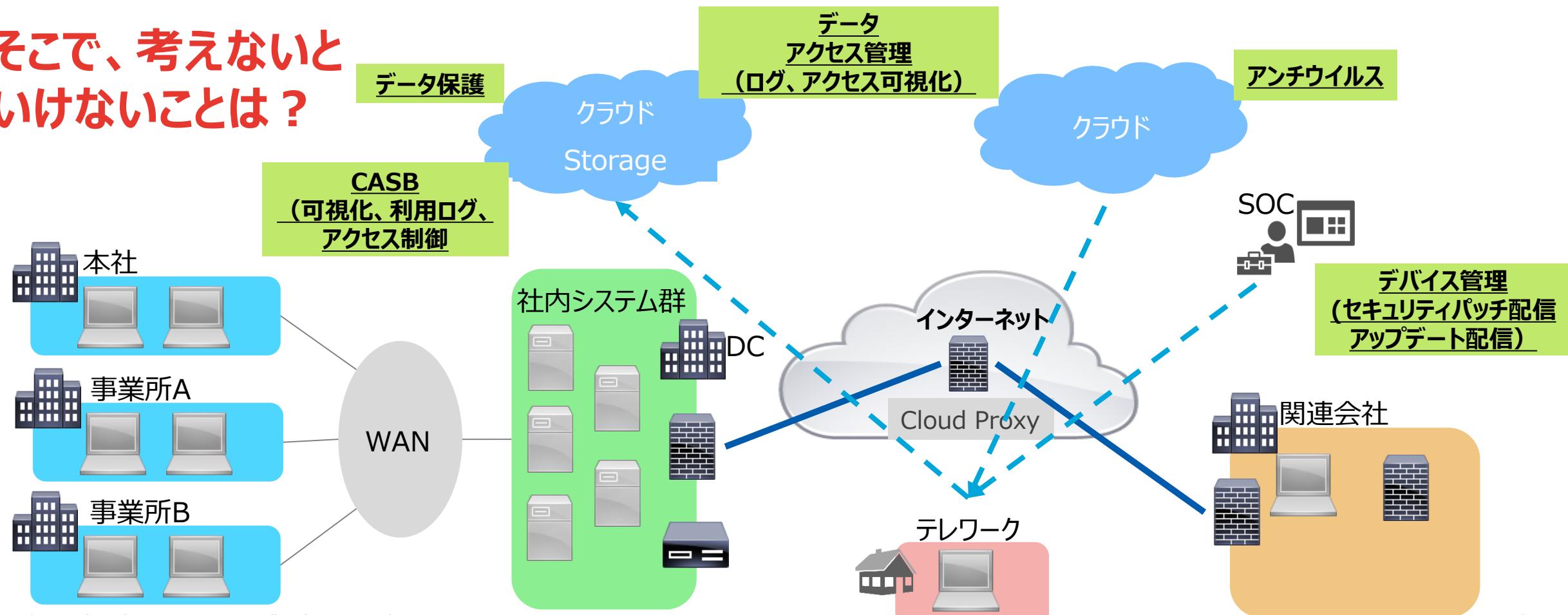


# 昨今の企業インフラ

## ■取り組みイメージ

- 昨今、企業様ではテレワークなど外部から仕事をすることが多くなってきております。
- その上で、オンプレからクラウドへ移行してきております。

そこで、考えないと  
いけないことは？



# パブリッククラウドを使用する上で考えるべきこと！

## ■ パブリッククラウドにおけるセキュリティの責任範囲

- 利用者の責任範囲

責任共有モデル			
オンプレミス	IaaS	PaaS	SaaS
ユーザー	ユーザー	ユーザー	ユーザー
データ	データ	データ	データ
アプリケーション	アプリケーション	アプリケーション	アプリケーション
オペレーションシステム	オペレーションシステム	オペレーションシステム	オペレーションシステム
ネットワーク	ネットワーク	ネットワーク	ネットワーク
ハイパーバイザー	ハイパーバイザー	ハイパーバイザー	ハイパーバイザー
インフラストラクチャー	インフラストラクチャー	インフラストラクチャー	インフラストラクチャー
物理	物理	物理	物理

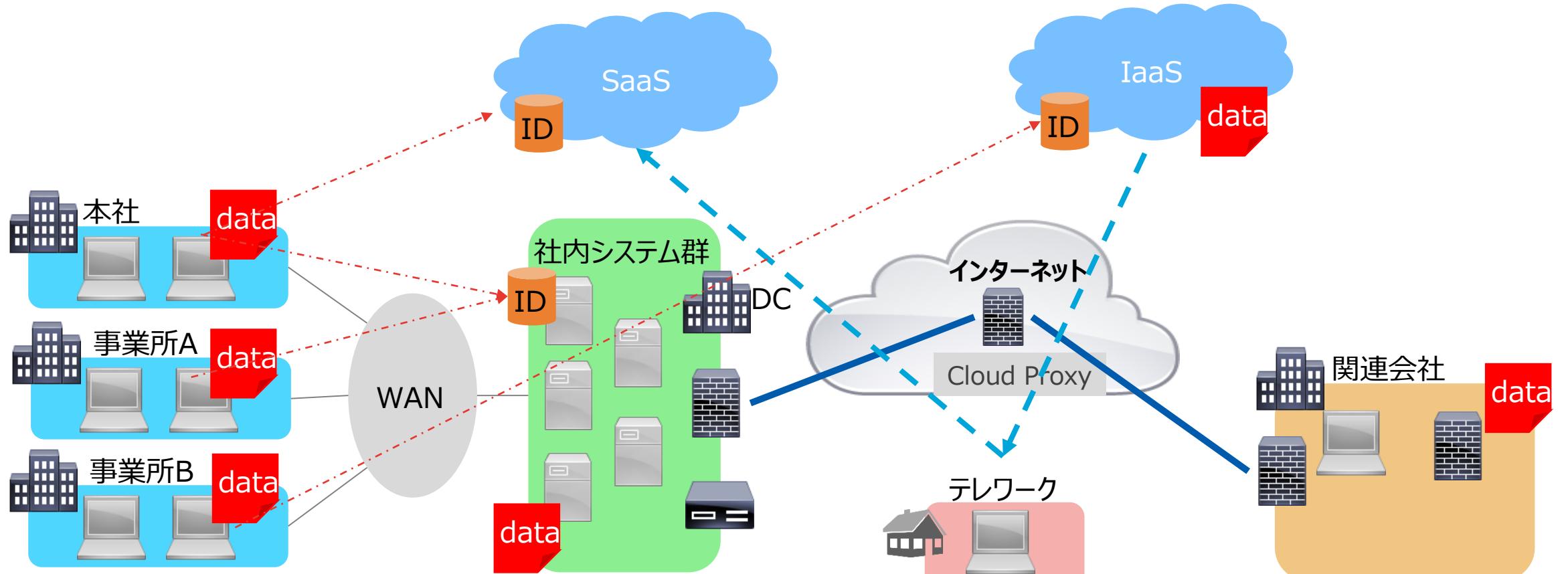
利用者責任

事業者責任

# 一般的なシステムの疑問点

## ■データセンターに通信を集約し、IaaSやSaaSを利用する一般的な構成イメージ

- 集約されていないデータ
- 管理の煩雑化したID
- クラウド上のデータ保護



# クラウドファーストを段階的に考える

## ■ 今どの段階？

- 企業インフラの大きな変化点はクラウドの活用です。



そこで、東京エレクトロンデバイスからのご提案内容  
安心・簡単なクラウドベースのデバイス管理ソリューション

- Microsoft 365とMcAfee MVISION Cloudを融合した4つの機能を実現

1. クラウドベースの新しいWindows10自動展開の活用 (Microsoft AutoPilot)
2. 外出先での業務を実現するデバイスセキュリティの実装 (Microsoft Intune)
3. クラウド基盤を利用したデバイス一元管理 (Microsoft Intune)
4. MVISION Cloudを使ったアクティビティ監査 (McAfee MVISION Cloud)



Microsoft

+



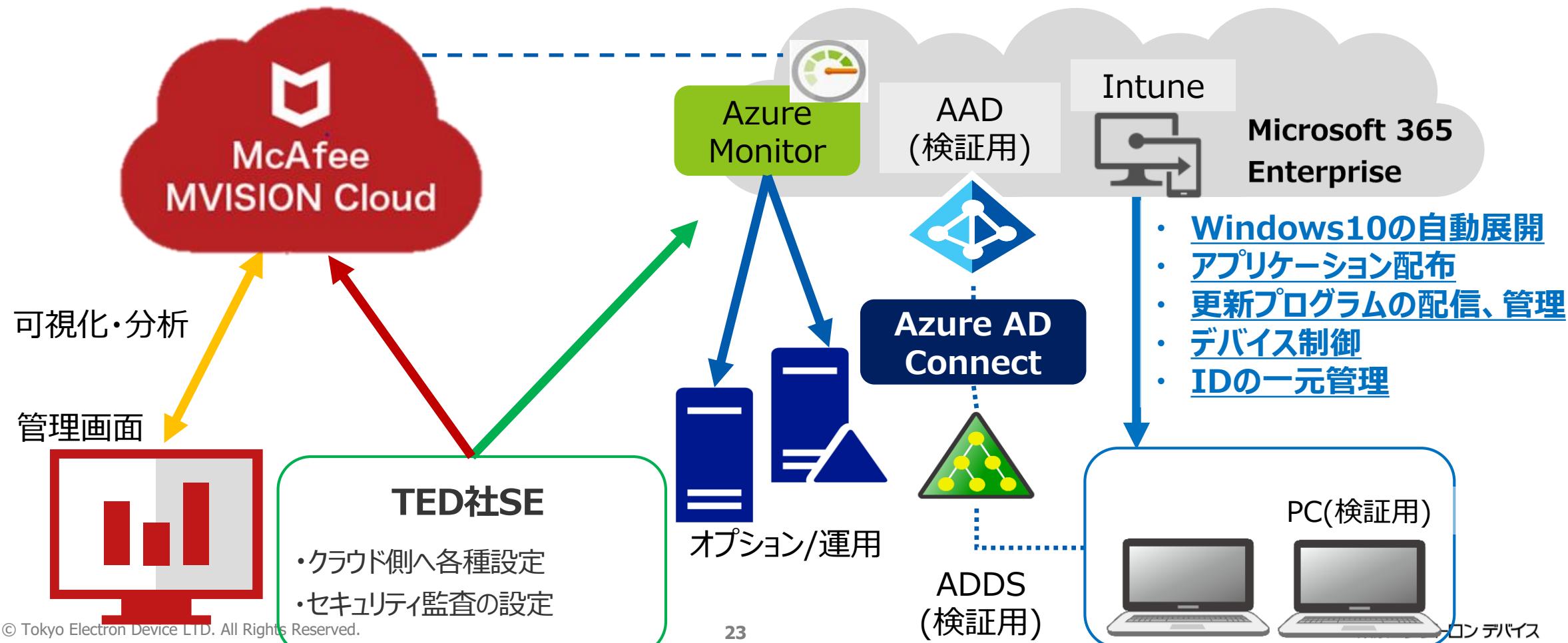
McAfee™  
Together is power.

# PoC実装イメージ

## ■ Microsoft 365とMcAfee MVISION Cloudを融合したシステムイメージ

- より簡単にお客様環境でWindows10自動展開、アプリケーション配布およびデバイス制御等をお試しき、オプションでお客様のオンプレサーバーをAzure Monitorで監視・運用することも可能です。

**セキュリティ監査では、マカフィー社のMVISION Cloudをお試しいただくことが可能です。**



# 1. クラウドベースのWindows10自動展開の活用

～AutoPilotにより自動展開、個別アプリケーションや制御用ポリシーの配布～

## ● 自動セットアップ（Windows AutoPilot）

Windows AutoPilotとはパソコンを自動セットアップする仕組みです。

セットアップ実行時にはAzure ADやMicrosoft Intuneと連動することで

- デバイス制限設定やOfficeアプリのインストールを自動化することができます。

=>パソコン自動セットアップにより変わるPC運用

- パソコン利用者変更や故障時の対応でも利用可能です。

=>従来のPC運用と比較し大幅にコスト削減



### ICT運用担当者

- ①. クラウド側へ事前に以下設定
  - ・パソコン情報登録
  - ・パソコン制限設定
  - ・Officeアプリ選択

### パソコン利用者

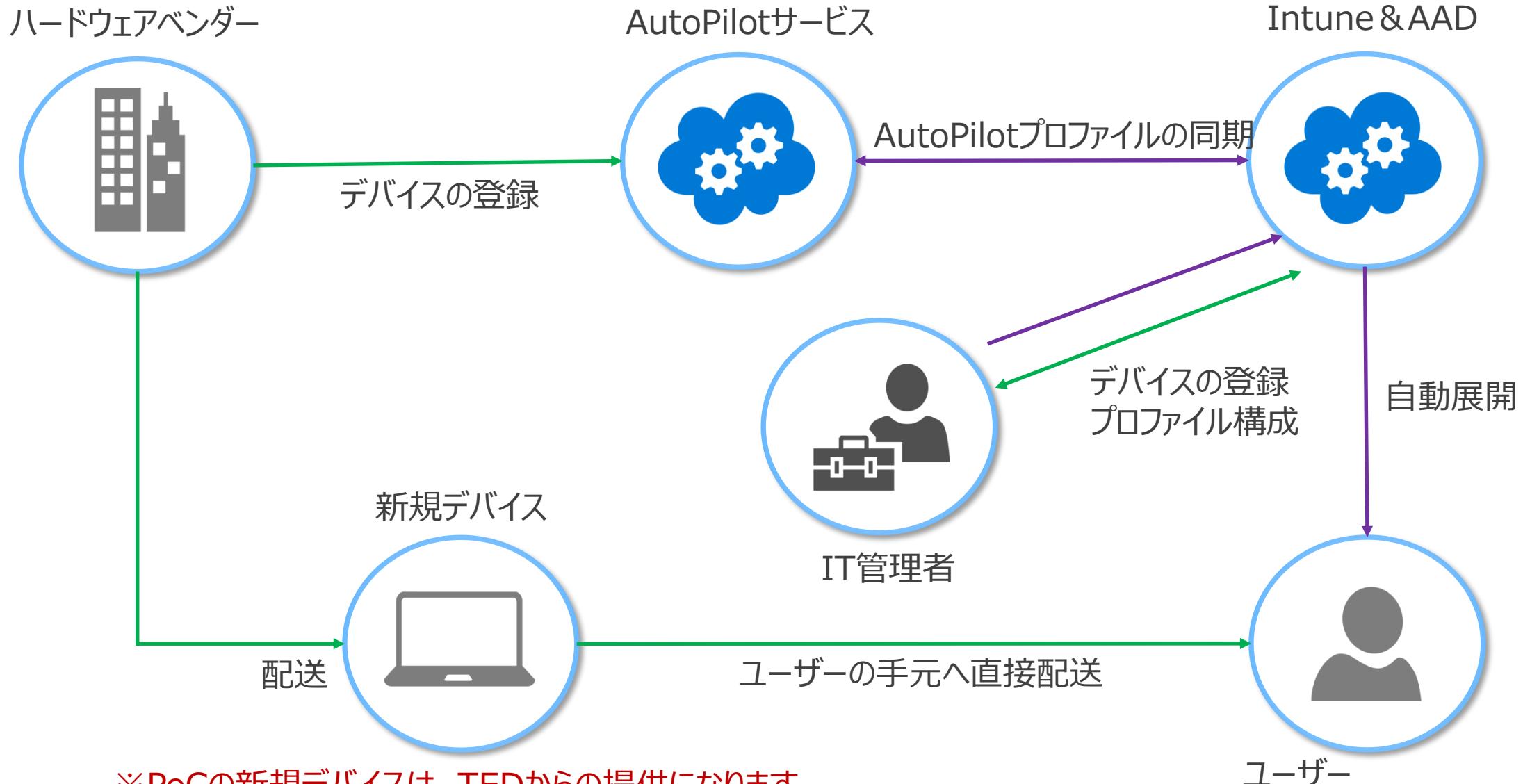
- ②. 開梱



- ③. パソコンを起動
- ④. NW設定後、  
数クリックと  
簡単な入力

# 1. クラウドベースのWindows10自動展開の活用

～AutoPilotにより自動展開、個別アプリケーションや制御用ポリシーの配布～



## 2. 外出先での業務を実現するデバイスセキュリティの実装

～外出先での業務を実現するためのセキュリティ～

### ● 利用者とパソコンを紐づけたデバイス制限（Microsoft Intune）

Microsoft IntuneはMicrosoft 365 Enterpriseに含まれるデバイス管理のクラウド製品です。

Microsoft Intuneで実装するデバイス制限とは、

- ・ パソコンを正しい利用者が、許可された権限、操作の中で利用する事が可能です  
=>人的ルール制限からシステム制限へ変更
- ・ 利用者は許可された範囲の権限、操作の中で利用する為、過失によるトラブルを未然に防止します。  
=>過失を未然に防止



ICT運用担当者

- ①. クラウド側へ以下設定  
・パソコン制限設定

パソコン利用者



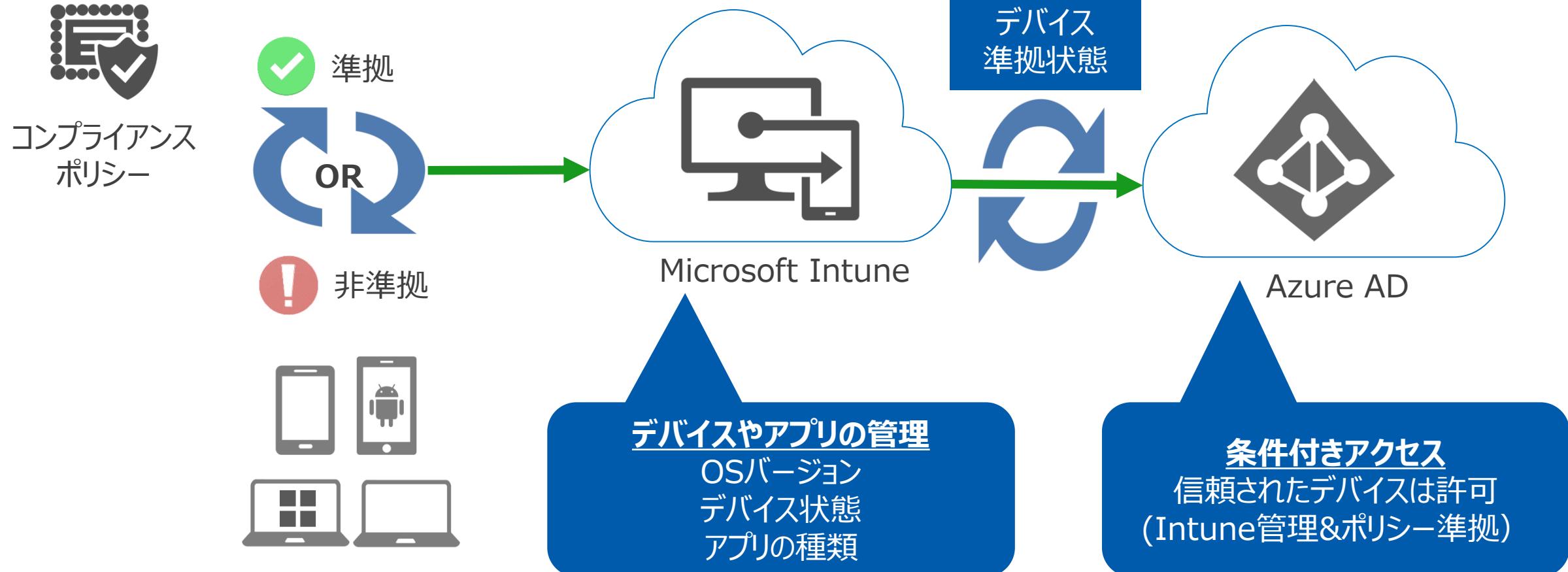
<外部記憶域制限例>

- ②. 制限設定自動適用
- ③. リムーバブル記憶域ブロック

USBを接続しても利用出来ない！

## 2. 外出先での業務を実現するデバイスセキュリティの実装

～外出先での業務を実現するためのセキュリティ～



### 3. クラウド基盤を利用したデバイス一元管理

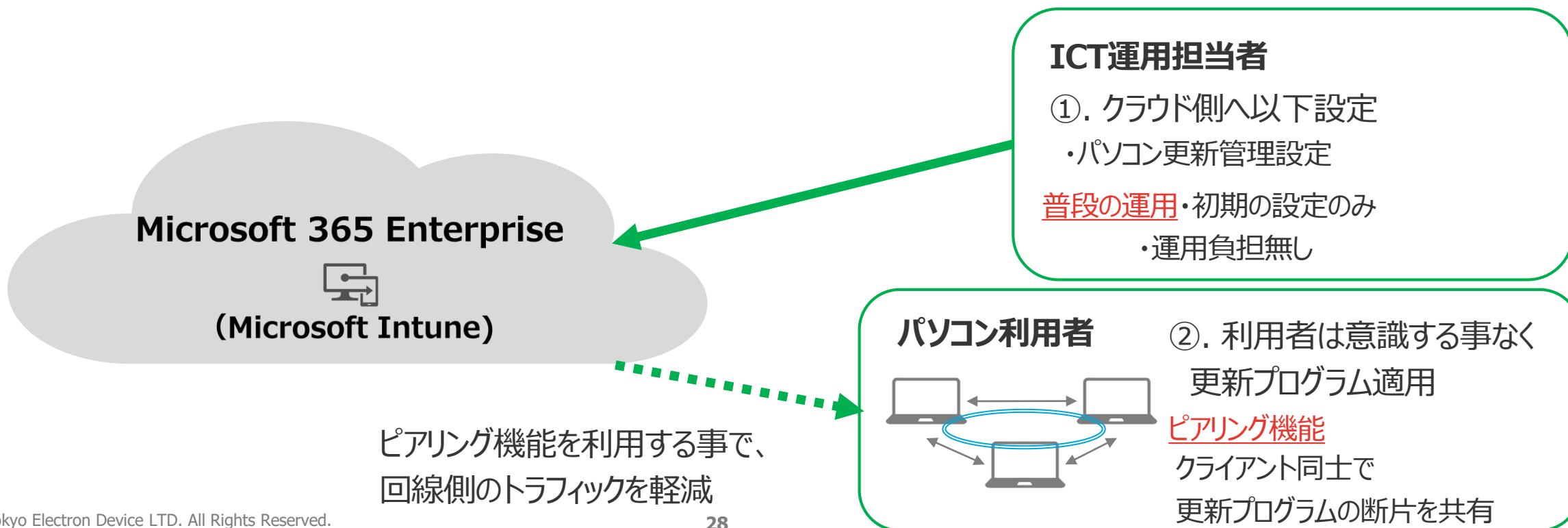
#### ● Windows Updateの自動化 (Microsoft Intune)

Windows 10の更新プログラムは機能更新プログラム (FU)と品質更新プログラム (QU)の2種類がございます。  
機能更新プログラムは半年に1回、品質更新プログラムは月に1回リリースされています。

- このアップデートを自動化する事は運用負荷の軽減につながります。

=>デバイス状況をリアルタイムで把握

=>必要な情報を必要なタイミングで活用

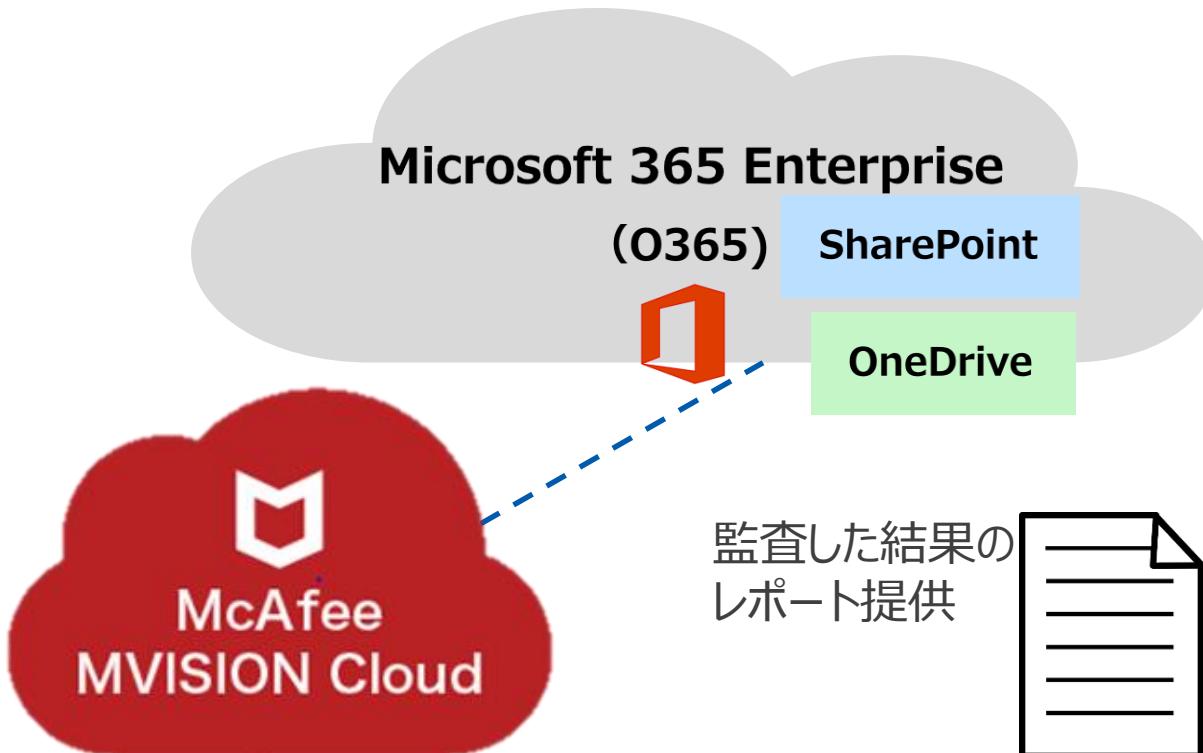


## 4. MVISION Cloudを使ったセキュリティ監査

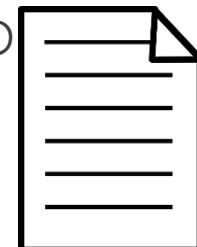
### ● Office 365のアクティビティ監査 (Exchange, OneDrive, SharePoint)

Microsoft 365には、Office 365も含まれており、クラウドサービスを利用する上でセキュリティを考える必要があります。

- Office 365を使用する上で、SharePointやOneDriveへのファイルアップロード  
=>SharePoint/OneDriveへのアクセスを確認



監査した結果の  
レポート提供



#### ICT運用担当者

- ①. クラウド側へ以下設定
  - ・テスト用OneDrive
  - SharePoint
- ②. MVISION側の設定

#### パソコン利用者

- ③. 利用者は意識する事なくOneDriveなどへファイルをアップロード

# 安心・簡単クラウドPC管理PoCメニュー

**TED REAL IoT**  
IoTの加速とAIへの挑戦

Microsoft Intune と McAfee MVISION Cloudで実現する  
**安心・簡単な  
クラウド時代のPC管理**

PoCシリーズ  
今だけキャンペーン  
Surface Goを最大5台プレゼント!!  
コミュニケーションツール(Teams)体験!!

**実施メリット**

- 既存PC運用からWindows10運用への切替
- 外出先での業務を実現するデバイスセキュリティの実装
- クラウド基盤を利用したデバイス一元管理
- クラウド環境と既存オンプレ環境の一元監視
- McAfee MVISION Cloudでパブリッククラウドの設定監査およびアクティビティの可視化

**実施イメージ**

McAfee MVISION Cloud  
Azure Monitor, Azure AD, Intune, Microsoft 365 Enterprise  
Azure AD Connect  
AD DS (検証用)  
お客様  
Windows 10の自動展開 (AutoPilot)  
Officeアプリケーション配布  
更新プログラムの配信、管理  
デバイス制御  
IDの一元管理  
お客様  
AD DS (検証用)  
お客様  
Surface Go LTE Advanced + カバー  
PoC期間中のPCBOX利用権  
Microsoft 365 Enterprise E5ライセンス  
PoC期間中のAzure利用料金  
Azure AD構築内容およびIntune構築内容など  
PoC実施内容をレポートとしてお渡しします  
お客様をご訪問し、レポート内容をご説明

■ お客様にてご用意頂くもの  
- インターネット接続環境  
- 貸出PC Box用設置場所と電源(100V x1)  
- 機器接続に伴うLANケーブル (Cat5e以上)

■ PoCに必要なクラウド環境、仮想サーバ、動作確認用PCは費用に含まれております。オプションで、お客様のオンプレサーバーをAzure Monitorで監視・運用と、セキュリティ監査としてMcAfee MVISION Cloudで可視化・監視を体験いただけます。

**東京エレクトロンデバイス**

**McAfee**  
Together is power.

**東京エレクトロン デバイス**

**Microsoft**

**安心・簡単クラウドPC管理PoC**

**PoCの特長**

- お客様の環境でMicrosoft Intuneの自動展開（事前インストール不要）
- Microsoft Windows10 PCの遠隔監視・管理支援（Microsoft Azure上での監視体験）
- クラウド活用のためセキュリティ導入支援（McAfee MVISION Cloud）

**実施項目**

【初期導入】  
 - 自動展開の実施  
 - Officeアプリケーションの配布  
 - 個別アプリケーションの配布  
 - 更新プログラムの配布  
 - 制御用ポリシーの配布  
 【運用】  
 - クラウド側の故障対応用作業  
 - クラウド側変更後の自動実行  
 - オンプレ環境の運用監視  
 - MVISION Cloud上の可視化/分析

**PoCの流れ**

1ヵ月間 → ①ヒアリングとサービスのご説明  
ご訪問し、サービスのご説明、ライセンス状況環境ヒヤリングをします。

2ヵ月間 → ②評価の検討  
構成や評価内容を検討いたします。

③PoC実施  
クラウド環境の準備とPoCを実施いたします。

④報告会  
結果のレポートを作成し、本番運用後もサポートいたします。

⑤本番運用  
本番運用後もサポートいたします。

※PoC期間は2ヵ月の想定となります。

**提供物**

項目	内容	数量
Surface Go	Surface Go LTE Advanced + カバー	5台
AD/AD Connector PC Box	PoC期間中のPCBOX利用権	1 ※1
Microsoft 365 Enterprise	Microsoft 365 Enterprise E5ライセンス	5 ※2
Azure 利用料金	PoC期間中のAzure利用料金	2ヶ月 ※3
マニュアル	Azure AD構築内容およびIntune構築内容など	1式
結果レポート	PoC実施内容をレポートとしてお渡しします	1式
報告会実施	お客様をご訪問し、レポート内容をご説明	1回

※1 PCBOXには、Active DirectoryとAzure Active Directory Connectorがインストールされています。  
 ※2 Windows10、Intune、Teams等PoCに必要なすべてのライセンスが含まれます。  
 PoC終了後もライセンスをご利用になられる場合は、ライセンス費が必要となります。  
 ※3 PoC終了後に本番環境としてAzureをご利用の際は、サービスにより重量課金または月額固定となります。

■ お客様にてご用意頂くもの  
- インターネット接続環境  
- 貸出PC Box用設置場所と電源(100V x1)  
- 機器接続に伴うLANケーブル (Cat5e以上)

**お問い合わせ**

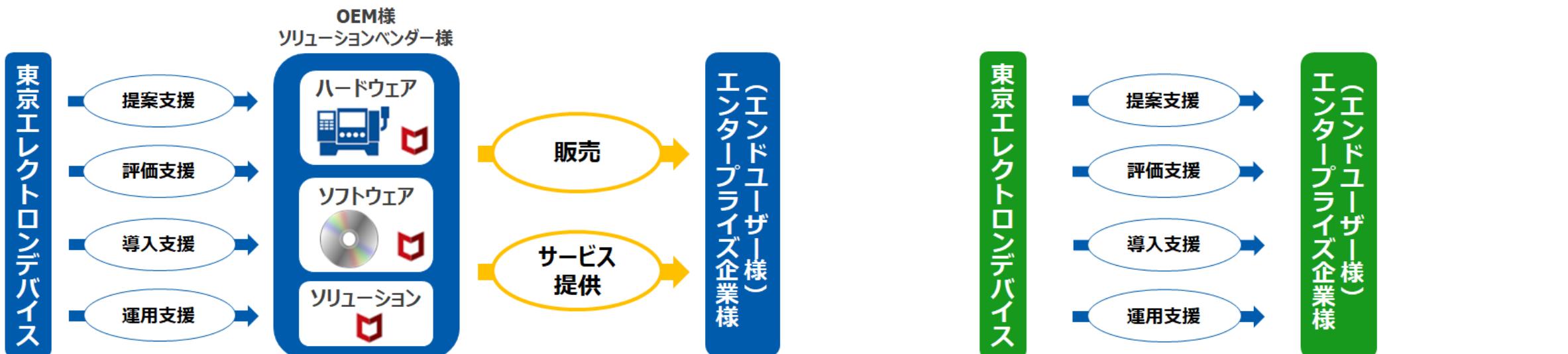
**東京エレクトロン デバイス株式会社**  
クラウドIoTカンパニー

エンベデッドソリューション部  
esg@teldevice.co.jp  
<https://esg.teldevice.co.jp/iot/mcafee/>





# McAfeeビジネスにおける弊社の強み



# デバイスからクラウドまで課題やお悩みを解決します

Windows / Linux / Android / iOS / Azure / AWS / Google

東京エレクトロンデバイスは、製造業における **デジタルトランスフォーメンション** を実現する革新的な製品、サービス、ソリューションの提供を行い、日本の製造業をより強くします！

## 組込装置/企業システムのエンドポイント対策 (ホワイトリスト / ブラックリスト)

### 豊富な導入実績

#### 医療機器

- ・検体検査装置
- ・画像診断装置
- ・生体情報モニタ
- ・心臓カテーテル用ポリグラフ

#### シスメックス株式会社



#### 流通・小売

- ・POS
- ・CAT端末
- ・KIOSK
- ・販売機、券売機

#### 金融

- ・ATM
- ・行員端末
- ・両替機

#### 株式会社ソディック



#### 産業機器

- ・半導体製造装置
- ・マウンター
- ・工作機械
- ・検査装置

## クラウドサービスの脅威対策(CASB)

PoCから実運用まで支援



状況の可視化



アクセス制御



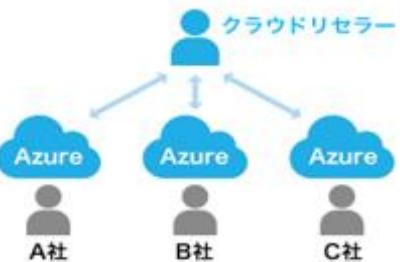
分析



暗号化

## クラウド活用 (Azure CSP)

展示会、セミナー等の豊富なクラウドリセラー支援



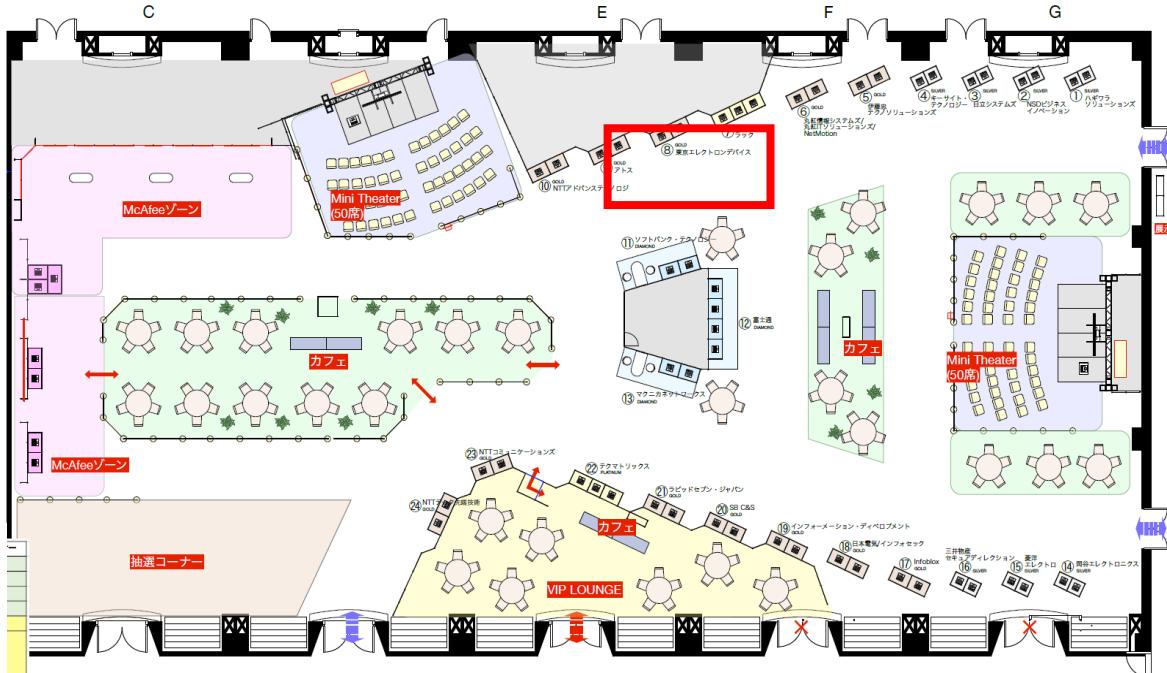
Microsoft Japan Partner of the Year  
Internet of Things (IoT) Award  
2年連続受賞

# 東京エレクトロンデバイスブースへお立ちよりください

ノベルティ引換券をブースへお持ちください。  
※アンケートと引き換えにお渡しします

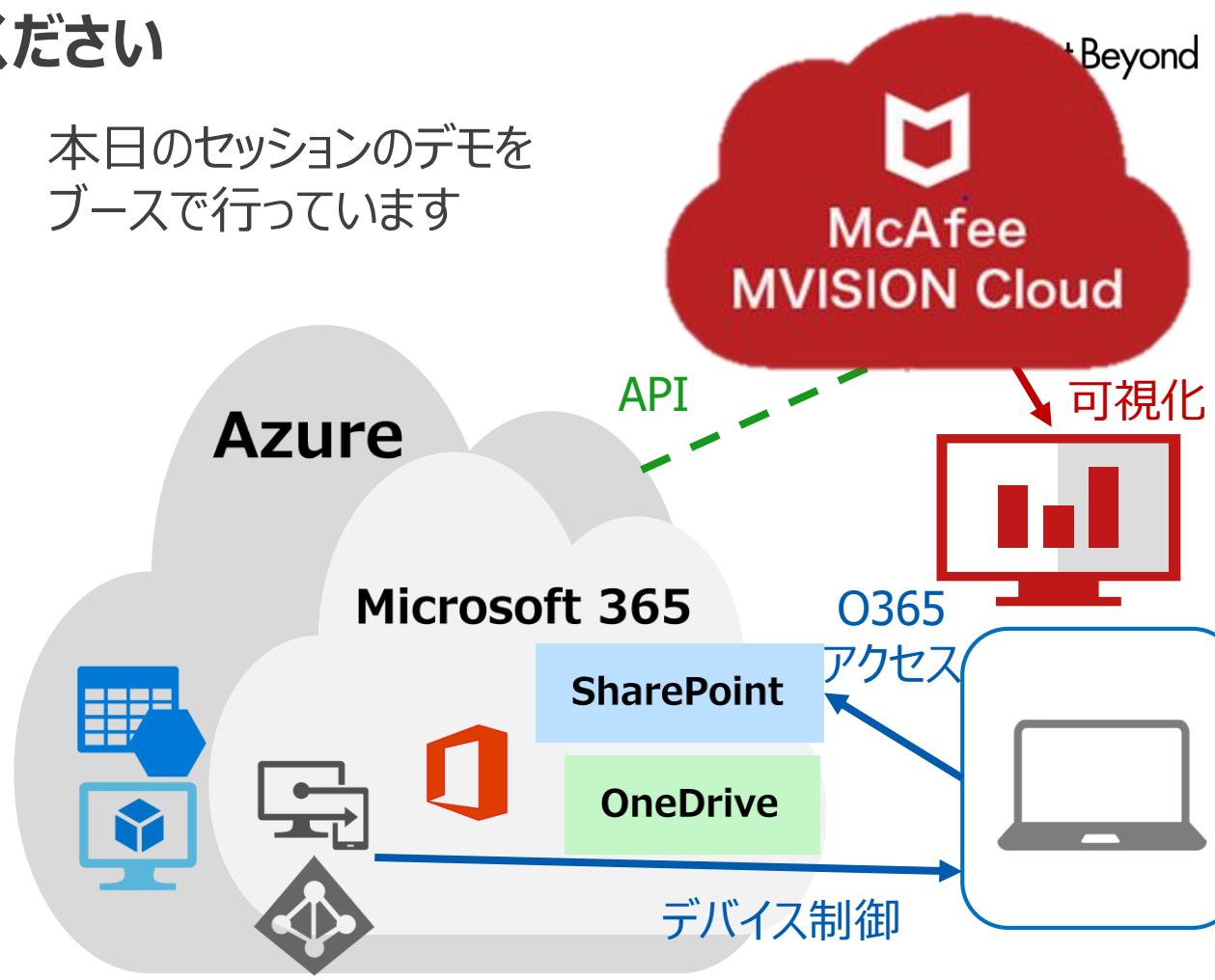


展示会場はこちら↓



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

本日のセッションのデモを  
ブースで行っています



## パソコン側のデモ

- ・Windows10の自動展開/アプリケーション配布
- セキュリティソリューション (**MVISION Cloud**)
- ・IaaS監視/O365監視  
=> SharePoint, OneDrive

# 皆さんと共に 新たな価値の創造に挑戦してまいります。



東京エレクトロン デバイス



Azure



東京エレクトロンデバイス株式会社  
クラウドIoTカンパニー  
エンベデッドソリューション部

Email : esg@teldevice.co.jp  
URL : <https://esg.teldevice.co.jp/iot/azure/>  
: <https://esg.teldevice.co.jp/iot/mcafee/>

McAfee

