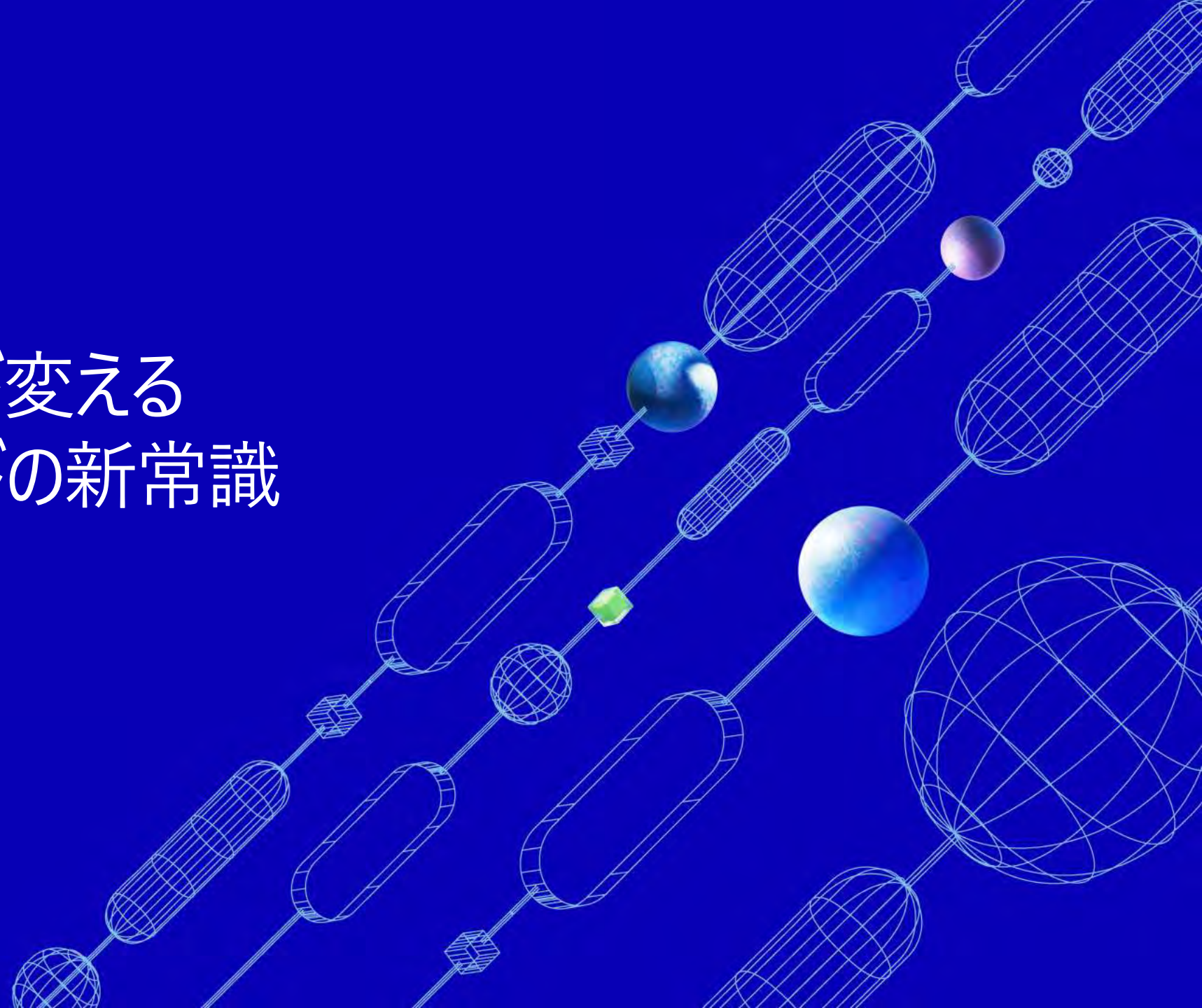




# 「Azure Local」が変える ハイブリッドクラウドの新常識

日本マイクロソフト株式会社  
コーポレートソリューション事業本部  
チャンネルパートナー技術統括本部  
シニア パートナーソリューションアーキテクト  
高添 修



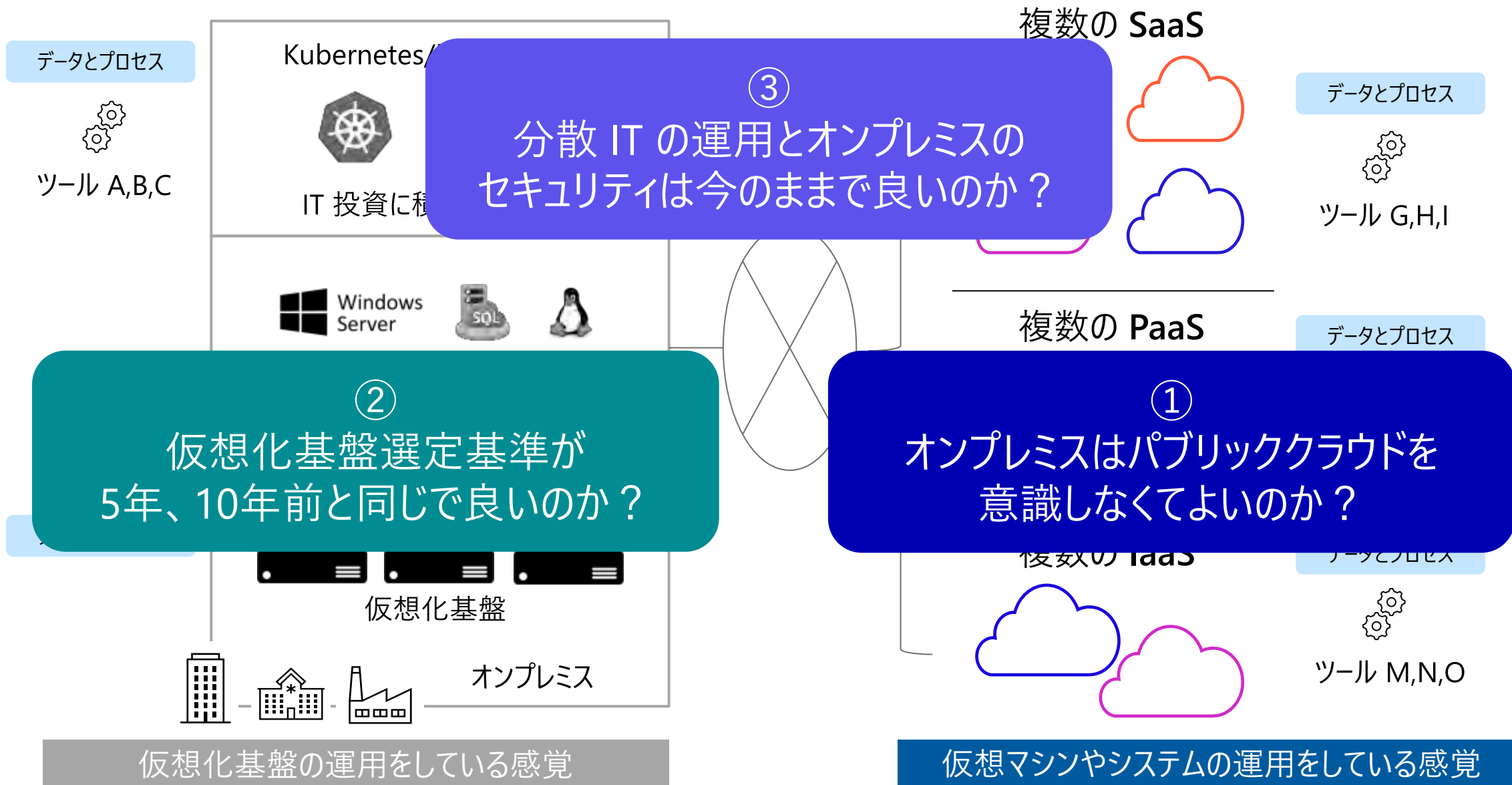


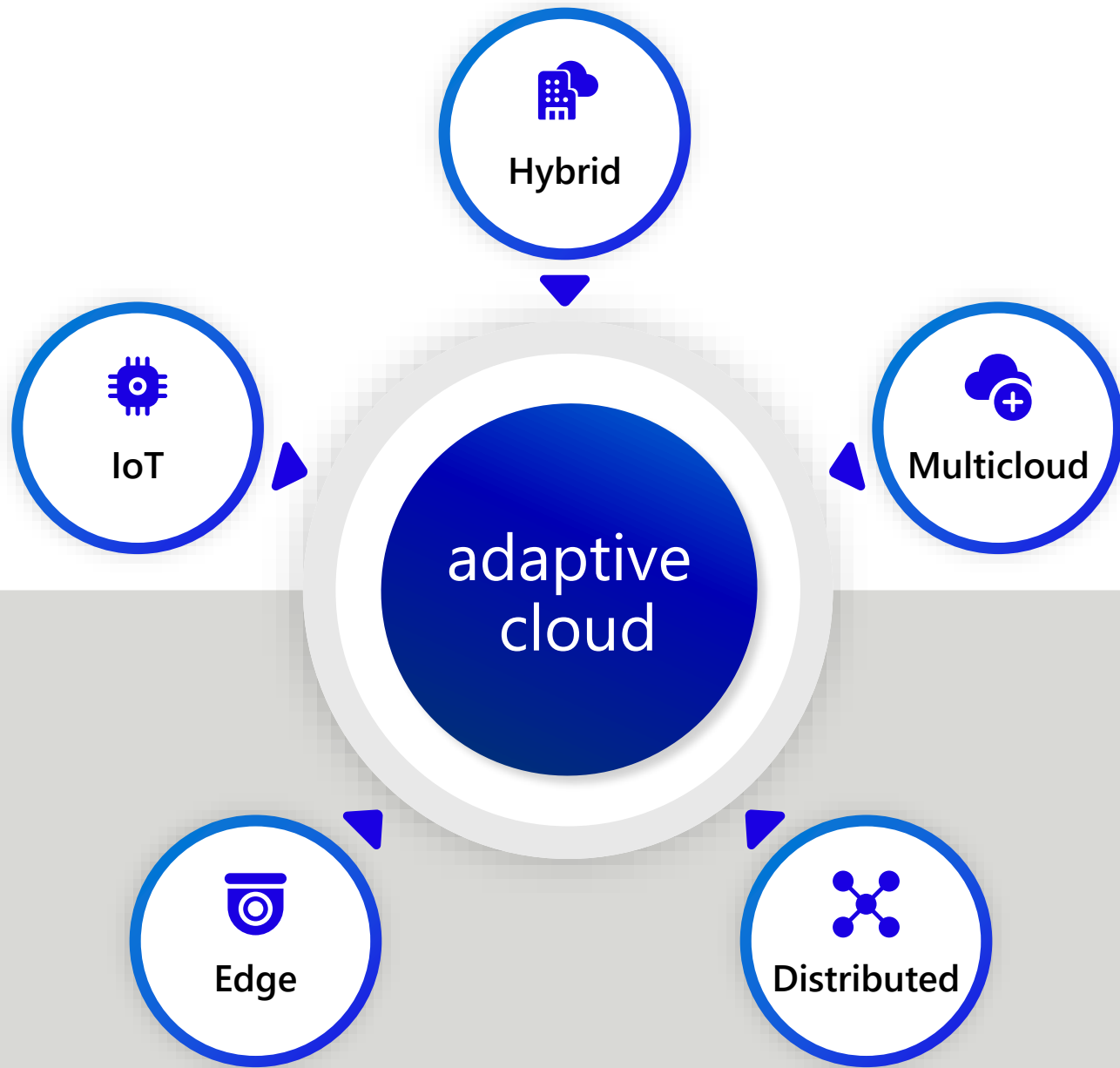
仮想化基盤 = 枯れた技術

運用を変える



# 企業 IT の現実





## ハイブリッドクラウドから アダプティブクラウドへ アプローチを進化

プラットフォーム、IT 選択の自由  
はそのままに、中心となる一点に  
接続することで複数拠点、  
分散システム、バラバラなチームの  
プロセスを統合し成功に導く

# 運用とセキュリティ対策はクラウドに移行中

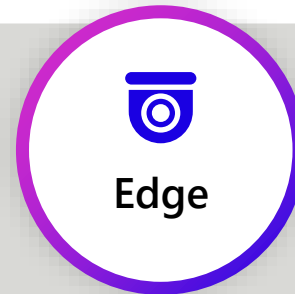
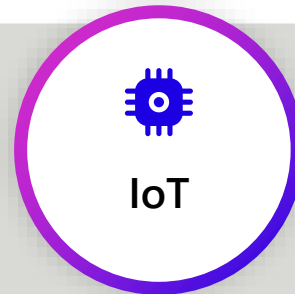
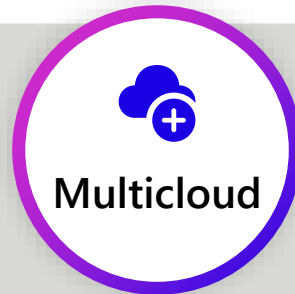
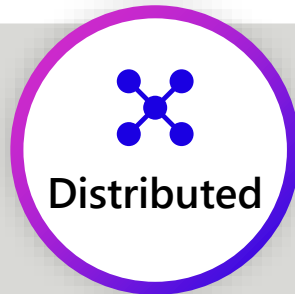
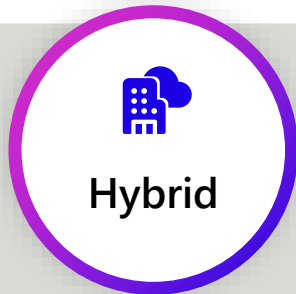
37,000社以上のお客様が Azure Arc を利用している



ポータル	Copilot	Graph	Entra 認証	Defender
監視	更新管理	ポリシー	サポート	課金管理

## Azure Arc

Windows Server				SQL	(連携) vCenter SCVMM
----------------	--	--	--	-----	--------------------------



# 部門/部署、配置場所や OS の違いを超えてシンプルかつセキュアに

お客様  
運用ベンダー

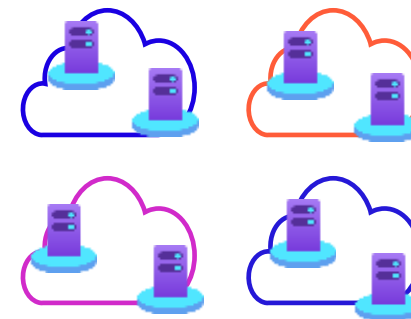


Microsoft Azure

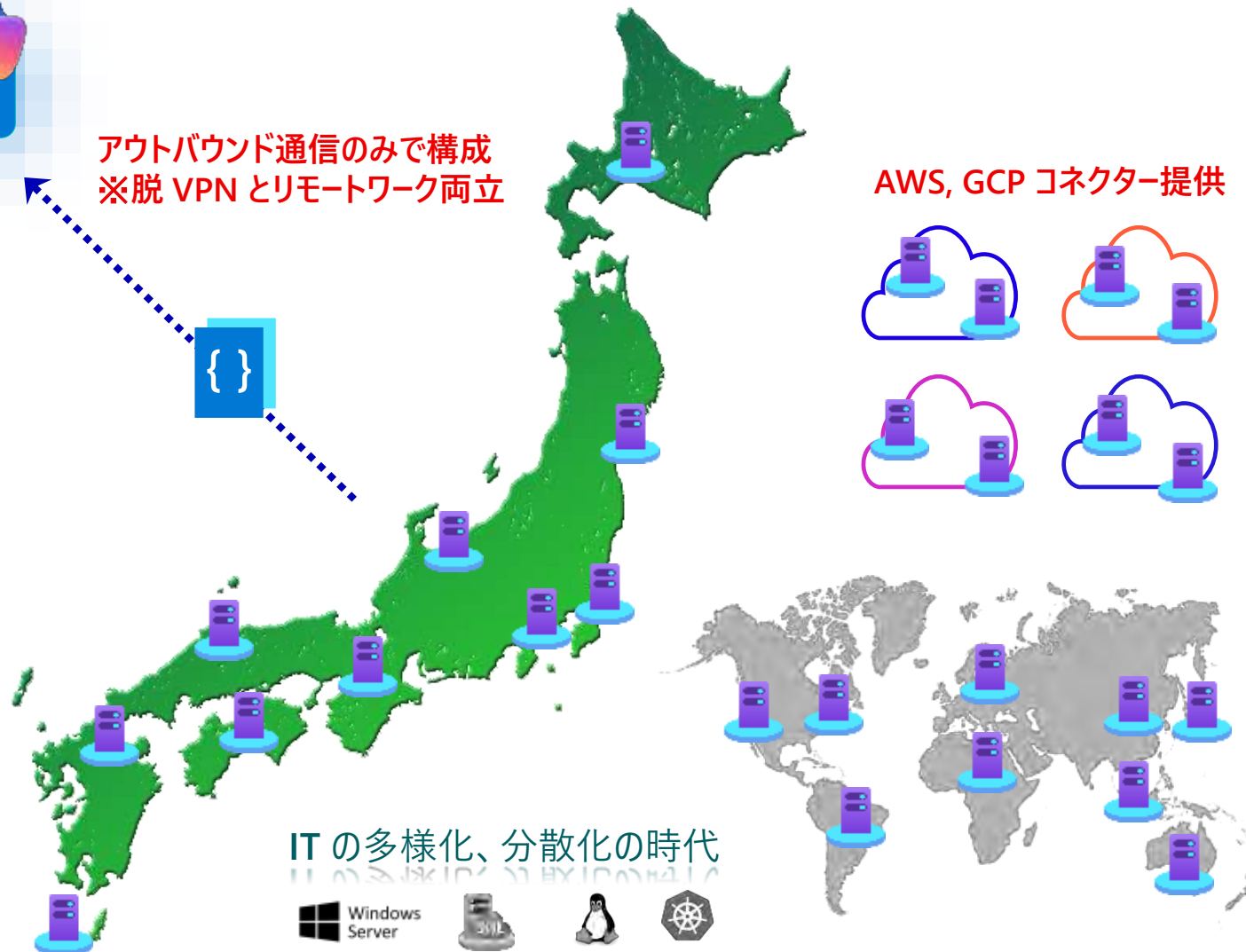


アウトバウンド通信のみで構成  
※脱 VPN とリモートワーク両立

AWS, GCP コネクター提供



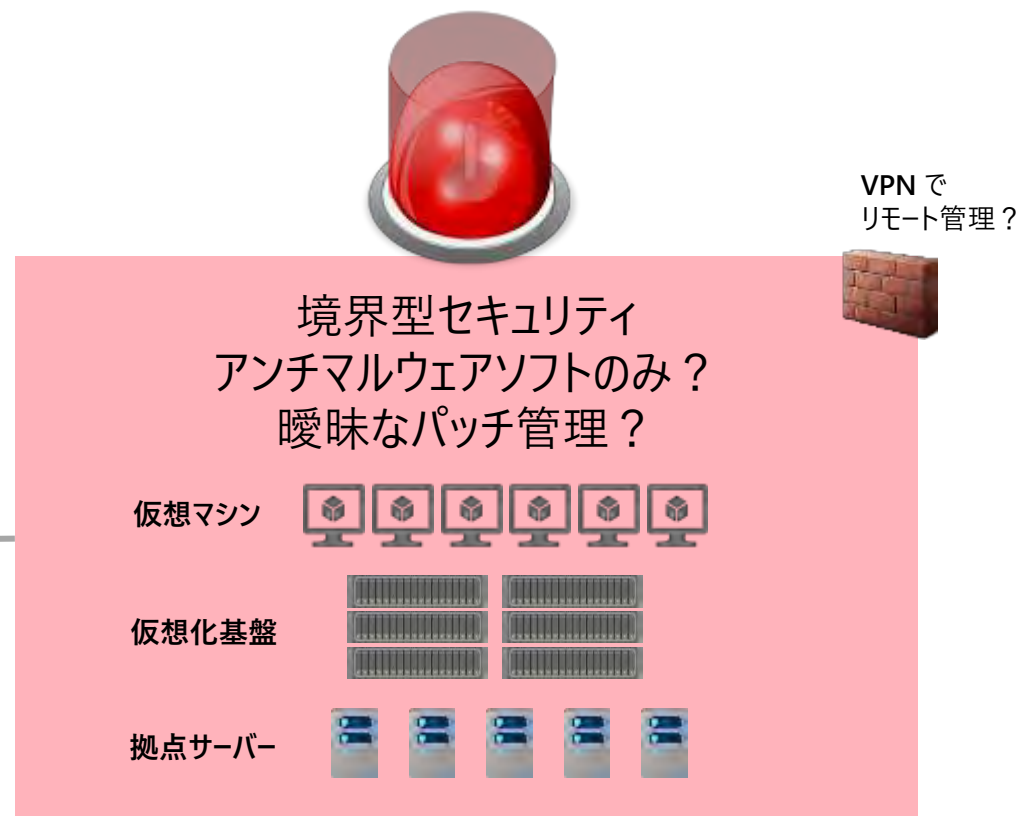
リモートコンソール SSH & RDP on SSH
IT 資産台帳のデジタル化 (IT 可視化とインベントリ管理、変更管理)
稼働監視と自動アラート発行 with AI (ログ分析、変更管理機能も提供)
ポリシーによる集中制御 (能動的構成管理と IT 基盤制御)
更新管理 = WSUS の代替案 + ホットパッチ (セキュリティ対策の一丁目一番地)
高度なセキュリティ対策 with AI (クラウドでは当たり前。最新セキュリティ監視)
AI SOC 連携 SIEM, SOAR, UEBA with AI
バックアップ(SQL SV)、災害対策(WinSV) 今後はクラウド移行のサポートも



# オンプレミスのセキュリティ対策、足りてますか？

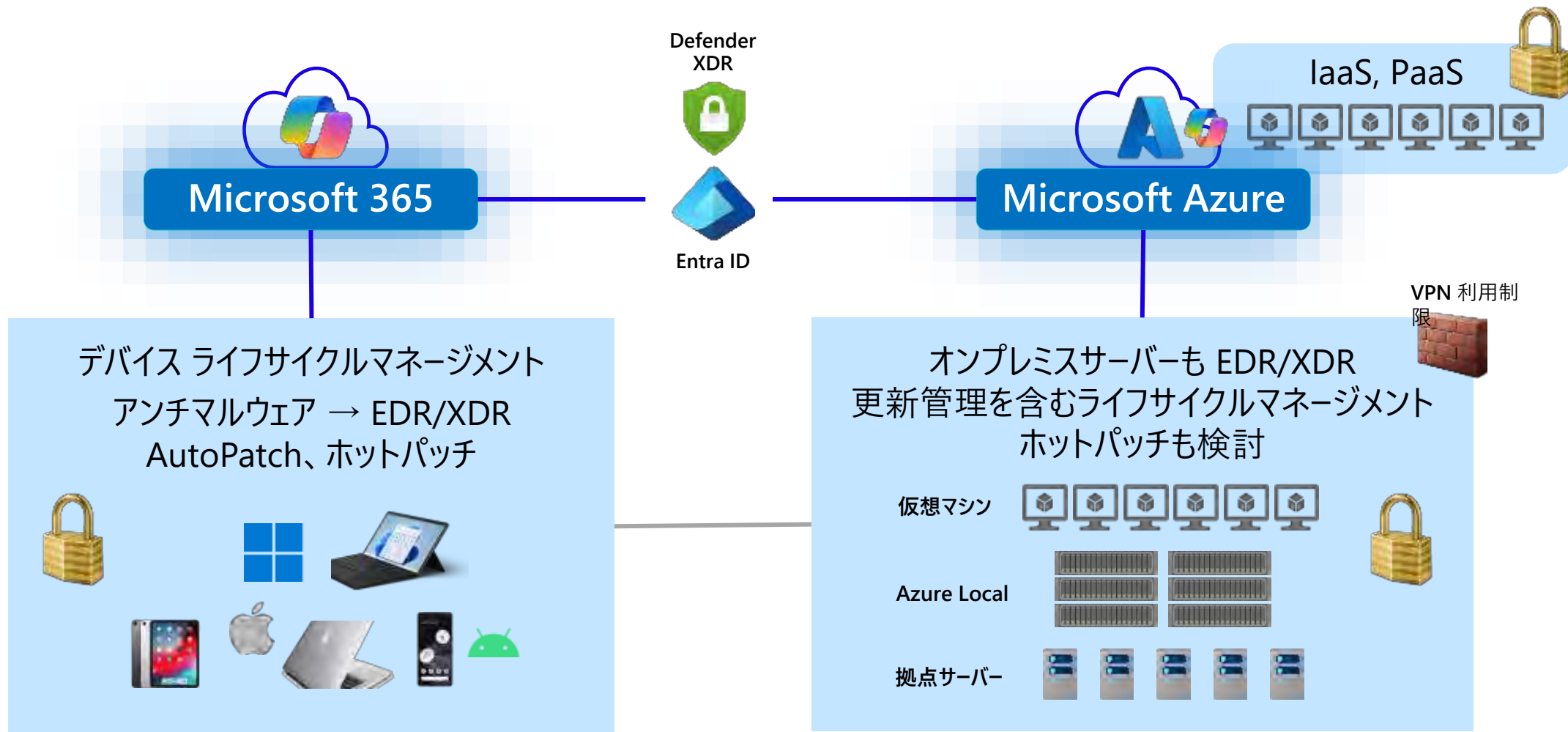


【質問】攻撃者が最終的に狙いたいのはどこ？



※ ハードウェアレベルの脆弱性対策やセキュアコアサーバー化も進んでいる  
※ ゼロトラスト、多層防御の観点からすると足りない

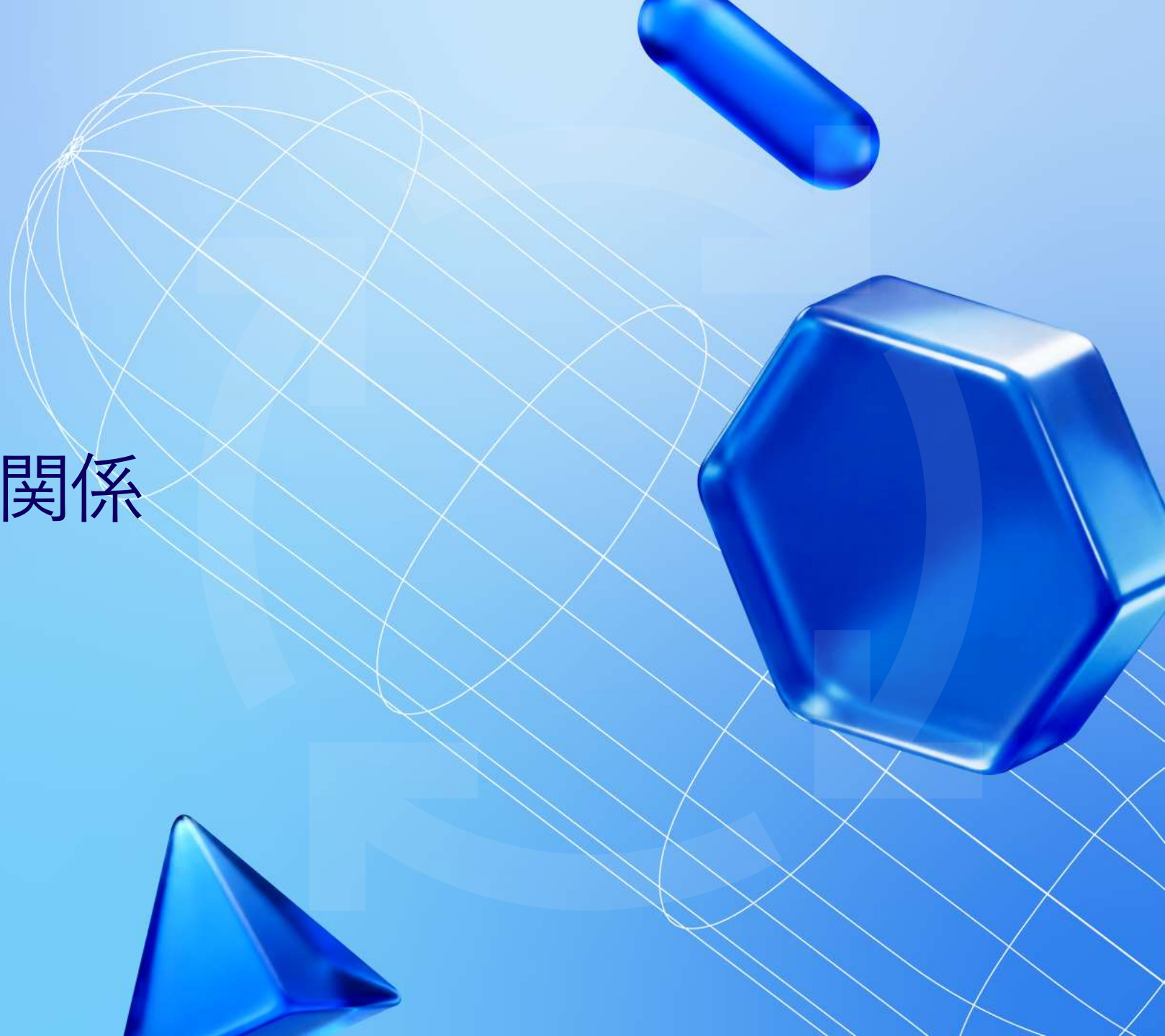
# オンプレミス仮想化基盤とサーバーも EDR/XDR で常に監視を





仮想化基盤も管理対象に

# Azure Arc と Azure Local の密な関係



同じコンセプトで  
仮想化基盤  
Kubernetes  
も管理対象へ

adaptive  
cloud



ポータル



Copilot



Graph



Entra 認証



Defender



監視



更新管理



ポリシー



サポート



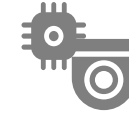
課金管理



Azure Local



Windows  
Server



(連携)  
vCenter  
SCVMM



Hybrid



Distributed



Multicloud

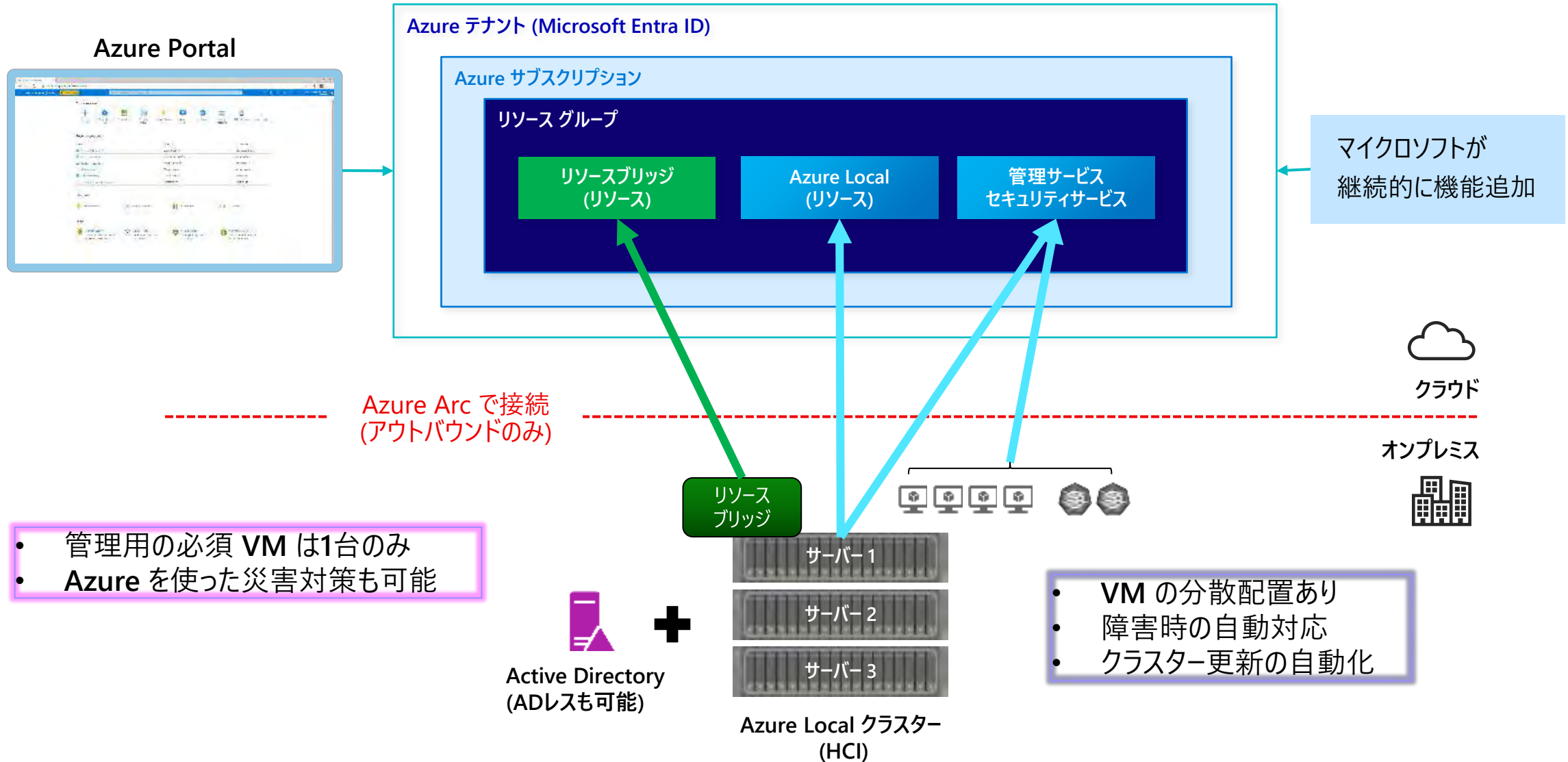


IoT

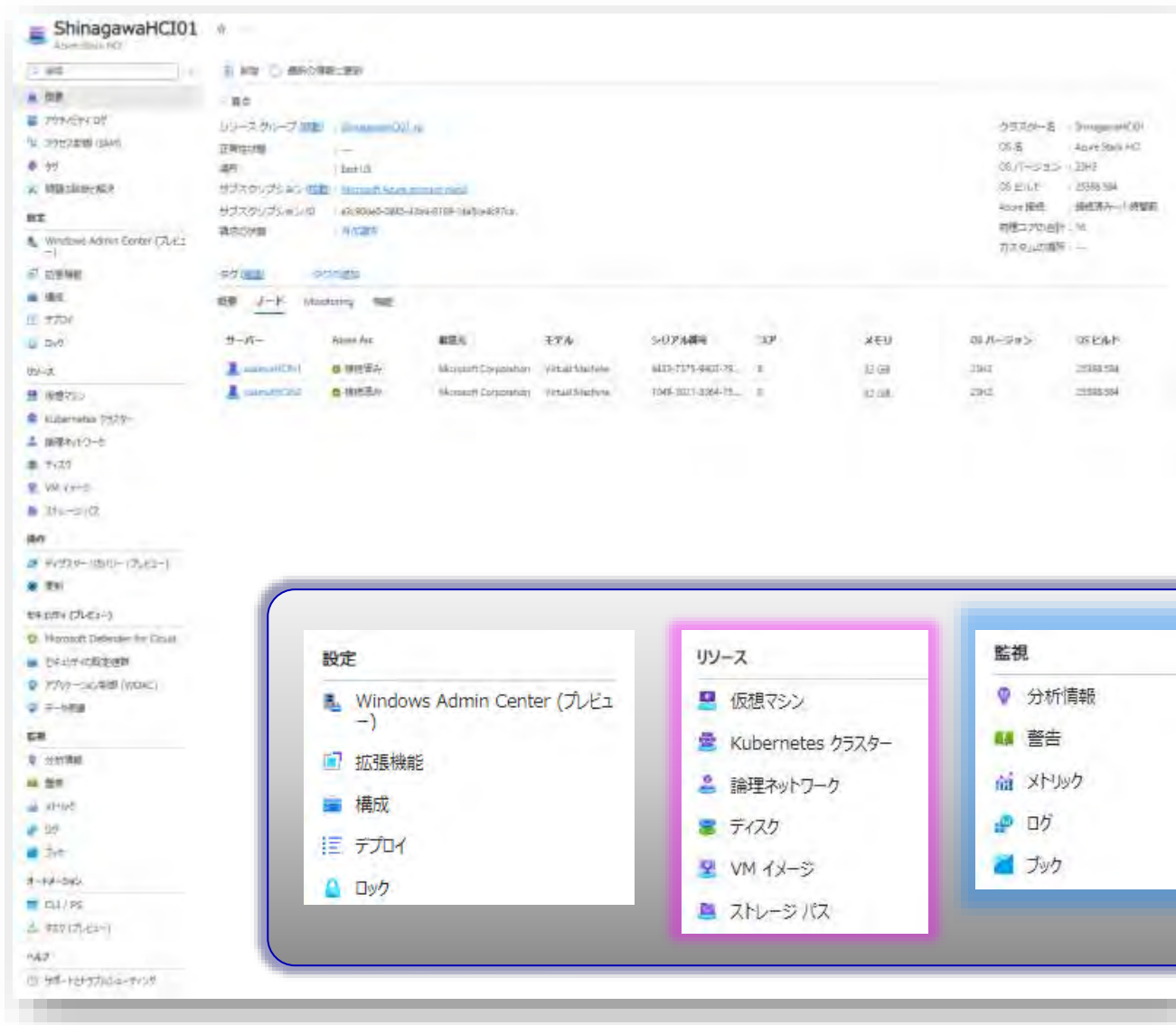


Edge

# Azure Local の全体像～



# 仮想化基盤の運用は Azure ポータル(API) から実施



- 稼働監視 (ログ分析)
- 更新管理 (HW 含む)
- セキュリティ態勢管理
- ディザスターリカバリー (プレビュー)
- ネットワークセキュリティグループ (NSG)
- ワークロードの展開と管理
  - 仮想マシン
  - Kubernetes

仮想化基盤もサーバー EDR 対象へ

# 徹底した多層防御型セキュリティ

管理およびセキュリティ  
ツール

Centralized security  
management

Azure Policy, OS Config



Simplified compliance

Azure Policy, Azure Security Benchmarks

Security posture mgmt.

Azure Policy, Monitor, Defender for Cloud



運用強化の簡素化

VM isolation

Hardware enforced VM isolation

Privileged access

JIT, JEA, PIM, PAM, CG



Network security

Datacenter Firewall, Secure DNS

機密性の高い  
ワークロードの保護

OS + firmware protection

TVM, Guest attestation



Confidential Compute\*

CVM, Guest & workload attestation

保存データの保護と  
整合性の確保

Encryption + data protection

SMB, BitLocker

System security + zero trust

Hardened defaults, Trusted Boot, Certificates, Cryptography, Code Signing and Integrity, Device Attestation, Zero trust

セキュア コア認定

Hardware root-of-trust

TPM 2.0, DRTM, Secure Boot



Silicon assisted security

Firmware, DMA, Memory, Secured Kernel

規制の厳しい業界

Security assurance



Certification



Secure supply chain

Host component governance

Provenance, patching and continuous vulnerability management of OS components

[Azure Local security book overview - Azure Local | Microsoft Learn](#)

# Azure からのシンプルな管理と監視

クラスター対応更新  
(自動ライブマイグレーション & ローリングアップデート)

※ HW ドライバー & ファームウェア更新も統合

クラスター > ボリューム	最終更新	ボリューム正	サイズ	使用状況	IOPS	傾向
ShinagawaHCI01	2022/6/13 17:56:07	2 Healthy	10.02 TB	2.28%	74.56 / 秒	
ClusterPerformanceHistory	2022/6/13 17:56:07	Healthy	20 GiB	6.16%	0 / 秒	
VMVDI01	2022/6/13 17:56:07	Healthy	10 TiB	2.28%	74.56 / 秒	
ShinagawaHCI02	2022/6/8 21:54:50	2 Healthy	10.02 TB	2.36%	156.21 / 秒	

マルチクラスターおよび Software Defined Storage の  
監視とアラート

更新の準備状況	現在のバージョン	前回の正常更新
正常	12.2509.1001.22	2023/10/20 午後 1:12

# Azure Local 管理画面からみたセキュリティ

強固なセキュリティベースライン + Defender for Cloud (オプション)

**ストレージとネットワーク暗号化**

**各種セキュリティはポリシーで強制**

ポリシー	状態
AzCL_Supplemental_Policy	2台のうち2台のマシンに適用
AD_Base_Policy_Miq2	2台のうち2台のマシンに適用
Microsoft Windows Virtualization Based Security Policy	2台のうち2台のマシンに適用
MSI_TWI_6X_14G_622509_1411_Supplemental_Policy	2台のうち2台のマシンに適用

ボリューム	マシン	暗号化の状態
OS ボリューム		
C:	TOKHCIN03	構成済み
D:	TOKHCIN04	構成済み
データ ボリューム (CSV)		
C:\ClusterStorage\SCSI-Images		未構成 管理
C:\ClusterStorage\UserStorage_2		構成済み
C:\ClusterStorage\UserStorage_1		構成済み
C:\ClusterStorage\Infrastructure_1		構成済み

※ 今後は 機密コンピューティングなども展開予定

# ネットワーク制御

## 【論理ネットワーク】

- ネットワーク環境を事前に定義
- 仮想マシンを論理ネットワークに配置

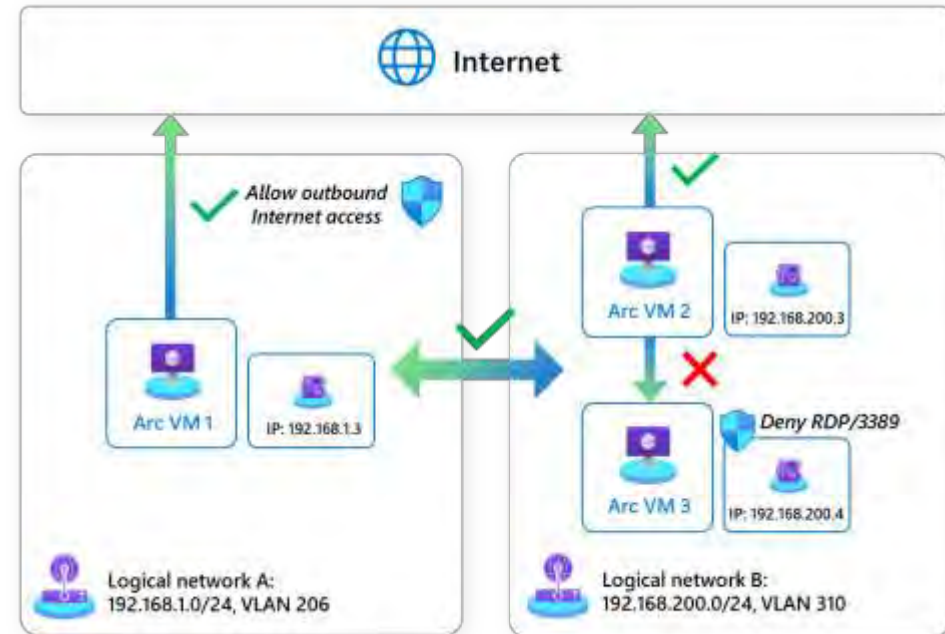
The screenshot shows the 'Create logical network' configuration page in the Azure portal. The 'Network configuration' tab is active. The configuration includes:

- Static IP address:** Selected. IPv4 address range: 172.16.10.0/24 (256 addresses).
- Subnets:** One subnet is defined with address range 172.16.10.1/24.
- Default gateway:** 172.16.10.1
- DNS servers:** 172.16.1.5
- VLAN ID:** 149

- マシン名変更、ドメイン参加、Arc 接続を VM 作成時に自動化

## 【ネットワークセキュリティグループ】

- (NSG)
- 5 タプルでの通信制御ルールを定義
- 論理ネットワークや仮想マシンの NIC に割り当て、通信を自動制御



# 1,380万IOPS ?

## ストレージの高速さと構成の柔軟さ



- 記憶域スペースダイレクト (S2D: Storage Spaces Direct)
  - Windows Server 2016 からの豊富な実績
  - Windows Server フェールオーバークラスターベース
  - Azure Local OS として独自の進化を開始
  - ディスクをプール化し、論理ボリュームを切り出して利用
  - シンプロビジョニング、暗号化、重複除去 などにも対応



## 仮想マシンの災害対策 (Preview)

～ Azure Site Recovery 連携が Azure Local 管理画面に登場 ～

ShinagawaHCH | ディザスタリーカバリー (プレビュー)

Azure にレプリケートすることで、システムがダウンしたときに VM を複製させ続ける

- 仮想マシンを5分(or 30秒)に1回、Azure に複製
- 災害時は Azure 上で仮想マシンを起動
- テストフェールオーバー、フェールバックも可能

## インフラとアプリに対する強力なデフォルト セキュリティ (ロードマップ込み)

管理およびセキュリティ ツール	Centralized security management Make things self-secure	Simplified compliance Apply Microsoft Security Baselines	Security posture mgmt. How things matter. Governance Cloud
運用強化の簡素化	VM isolation Prevent an affected resource	Privileged access Use just what you need	Network security Control access. Monitor risk
機密性の高いワークロードの保護	OS + firmware protection VM Guard enabled	Confidential Compute <sup>1</sup> CPU (and GPU) without external I/O	
保存データの保護と整合性の確保	Encryption + data protection With BitLocker	System security + zero trust Hardware health, Trusted Boot, Firmware, Cryptography, Code Signing and Patching, Device Attestation, ZeroTrust	
セキュア コア認定	Hardware root-of-trust TPM 2.0, Secure Boot, Memory Guard	Secure assisted security Hardware-Enabled Platform Security	
規制の厳しい業界	Security assurance	Certification	Secure supply chain
	Host component governance		

## Network ATC : ネットワークのインテント管理と自動修復

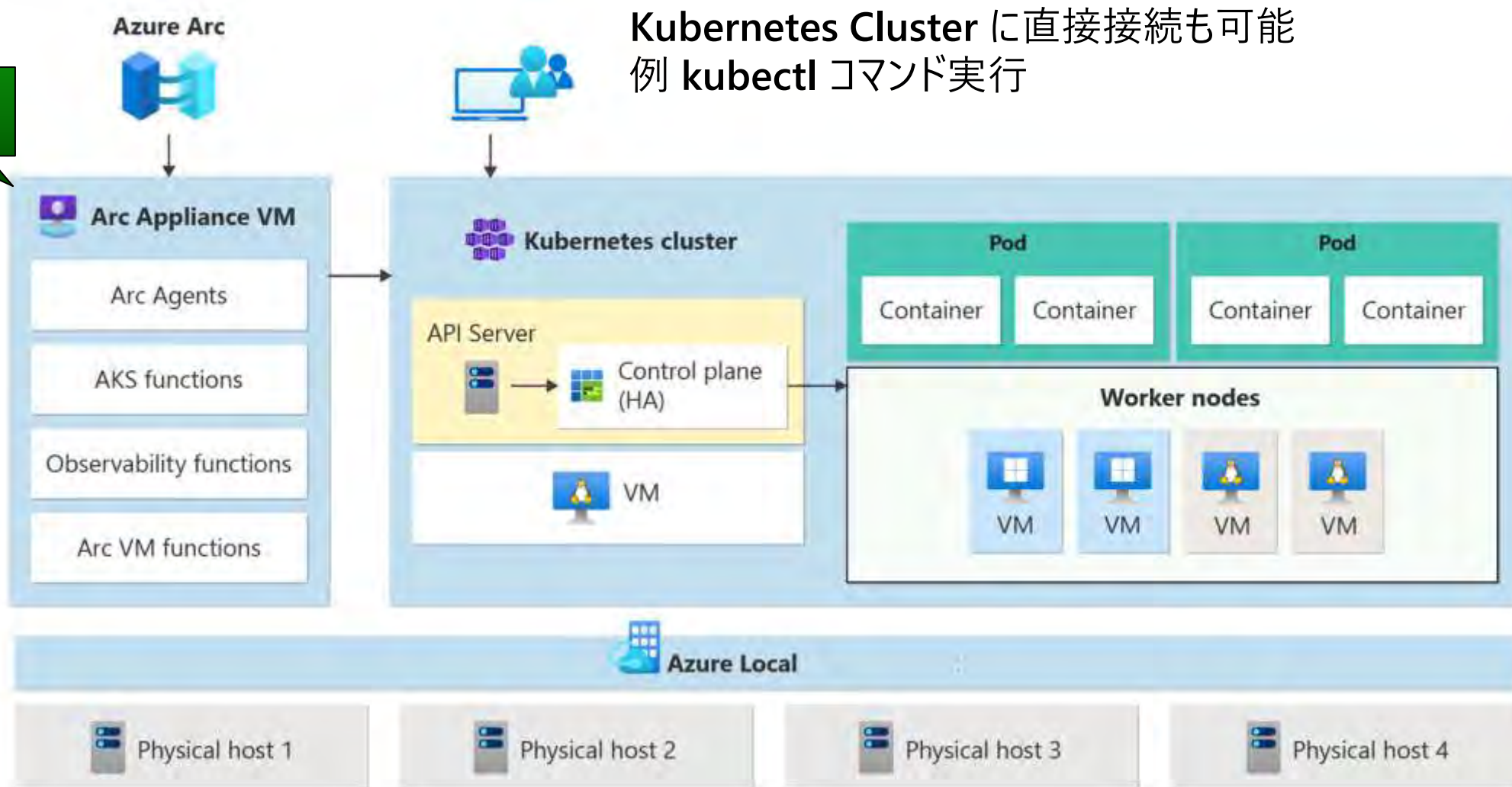
- 各種ネットワークをインテントにて意味づけし、本来あるべき設定を定義
- Network ATC サービスにより、本来あるべき設定で稼働していることをクラスターレベルで保証



- Network ATC = インテントに対して新しい設定をオーバーライドすることで、全体の挙動を変えられる
  - 各 NIC に定義をするのではなく、常にインテントで制御
  - クラスターワイドで設定が可能
- ただし、IPアドレスは VLAN ID など既定値があり、実環境に合わせるには正しく設定をする必要がある

# もし Kubernetes が必要と言われたら・・・ AKS を簡単導入

リソース  
ブリッジ



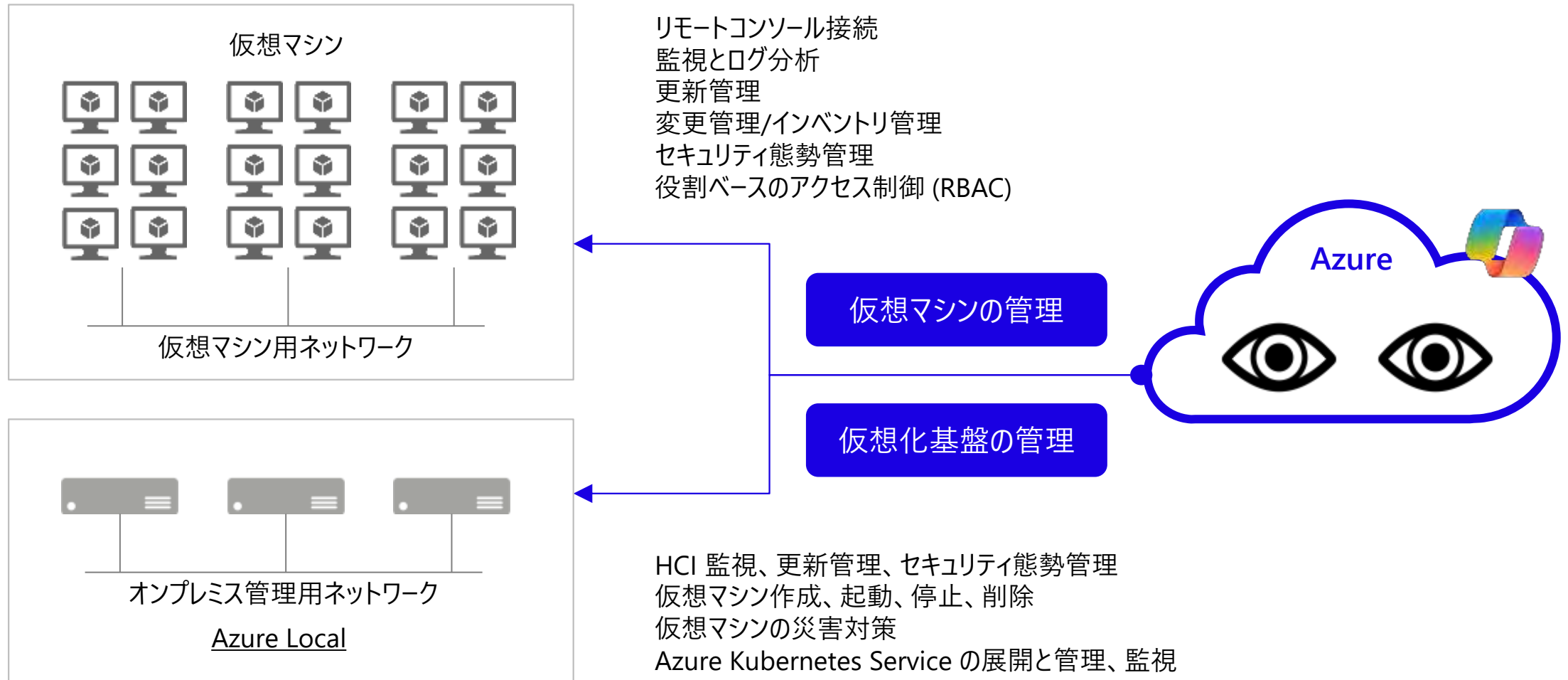
Kubernetes Cluster に直接接続も可能  
例 kubectl コマンド実行



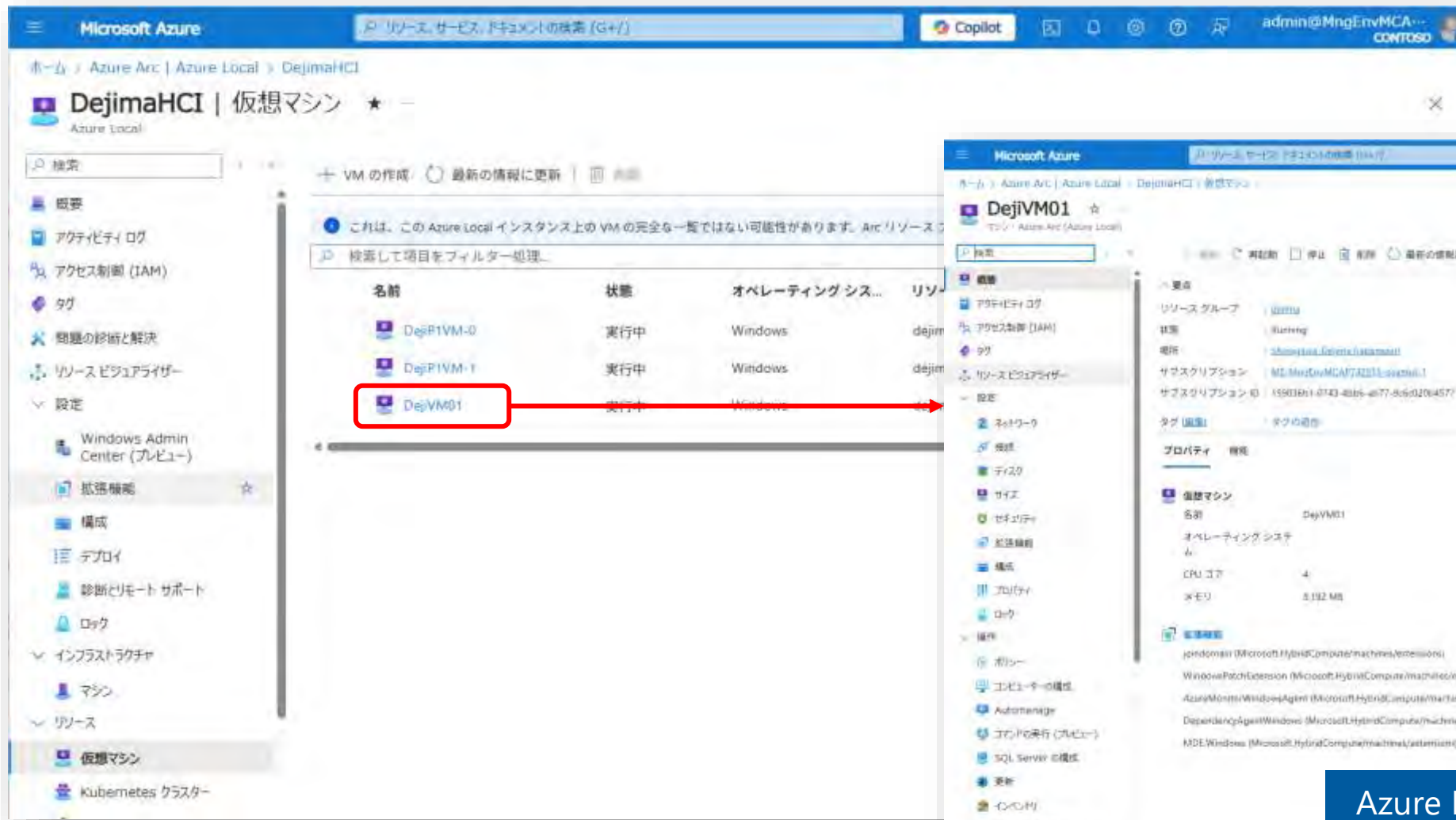
Azure Arc x Azure Local のメリット

ゲスト管理も Arc でカバー

# 仮想化基盤と仮想マシンを一元管理へ



# Azure Local の仮想マシンの管理



- リモートコンソール SSH & RDP on SSH
- IT 資産台帳のデジタル化 (IT 可視化とインベントリ管理、変更管理)
- 稼働監視と自動アラート発行 with AI (ログ分析、変更管理機能も提供)
- ポリシーによる集中制御 (能動的構成管理と IT 基盤制御)
- 更新管理 = WSUS の代替案 + ホットパッチ (セキュリティ対策の一丁目一番地)
- 高度なセキュリティ対策 with AI (クラウドでは当たり前。最新セキュリティ監視)
- AI SOC 連携 SIEM, SOAR, UEBA with AI
- バックアップ(SQL SV)、災害対策(WinSV) 今後はクラウド移行のサポートも

Azure Local 上の仮想マシンの管理画面

# SSH / RDP on SSH による Azure 経由のリモートコンソール



- 脱VPN
  - パブリックIP、インバウンド接続不要
  - Entra ID にて多要素認証、条件付きアクセス制御可能
- Arc 拡張機能で OpenSSH を簡単展開 (Windows Server)
- ※ Azure RBAC との組み合わせによる VM 管理のセルフサービス化も実現

RDP オプションにより SSH 上で RDP 接続を実施し、Azure 経由で仮想マシンコンソールを表示  
SSH を使用して Azure ローカル仮想マシン (VM) に接続する - Azure Local | Microsoft Learn

RDP on SSH 接続コマンド

```
az ssh arc --resource-group <resourcegroupname> --vm-name <servername> --local-user <localuser> --rdp
```



利用者目線のソリューションで語る

# Azure Local x Arc の価値

1. オンプレミス VDI
2. オンプレミス AI
3. ソブリンクラウド

# オンプレミス VDI

# Gartner Magic Quadrant for DaaS

Microsoft has been named a Leader in the 2025 Gartner® Magic Quadrant™ for Desktop as a Service (DaaS) for the third consecutive year: Highest in execution and furthest in vision

Windows 365 and Virtual Desktop provide a full range of scalable, flexible, and secured virtual, Azurehybrid and on prem solutions to help businesses of any size.

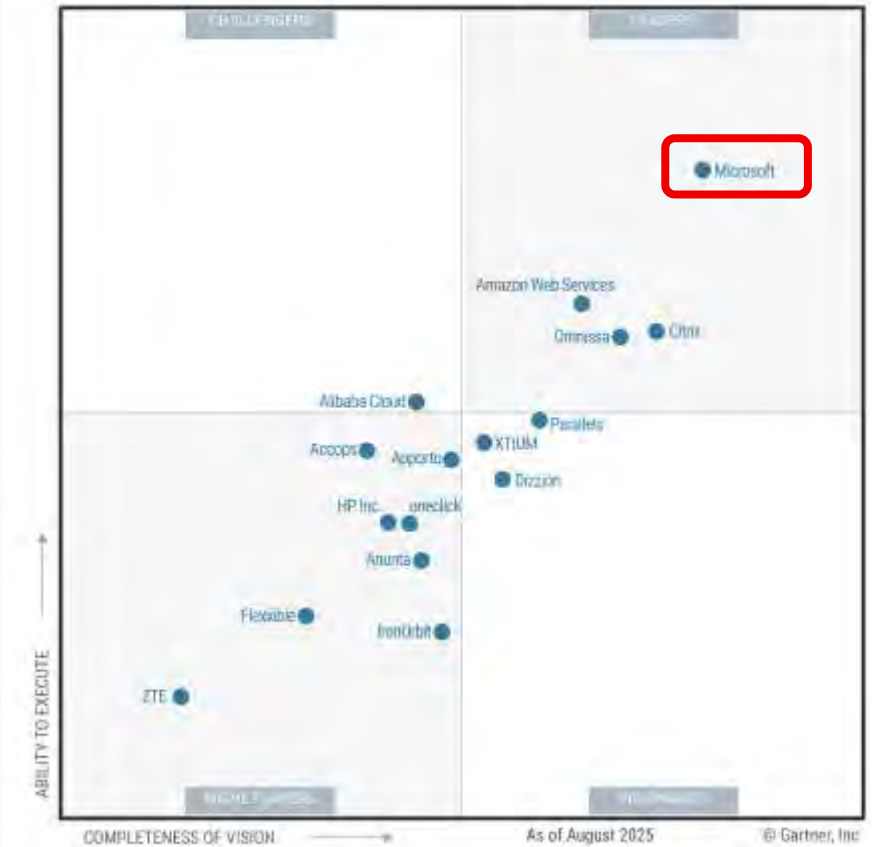
- Broad capabilities across digital workplace technologies, hyperscale cloud and AI.
- Robust global infrastructure provides support for clients in all regions and of all sizes.
- By 2027, virtual desktops will be cost-effective for 95% of workers compared to 40% in 2019. By 2027, virtual desktops will be used as the primary workspace for 20% of workers, up from 10% in 2019.



Read full report: [aka.ms/DaaS2025](https://aka.ms/DaaS2025)

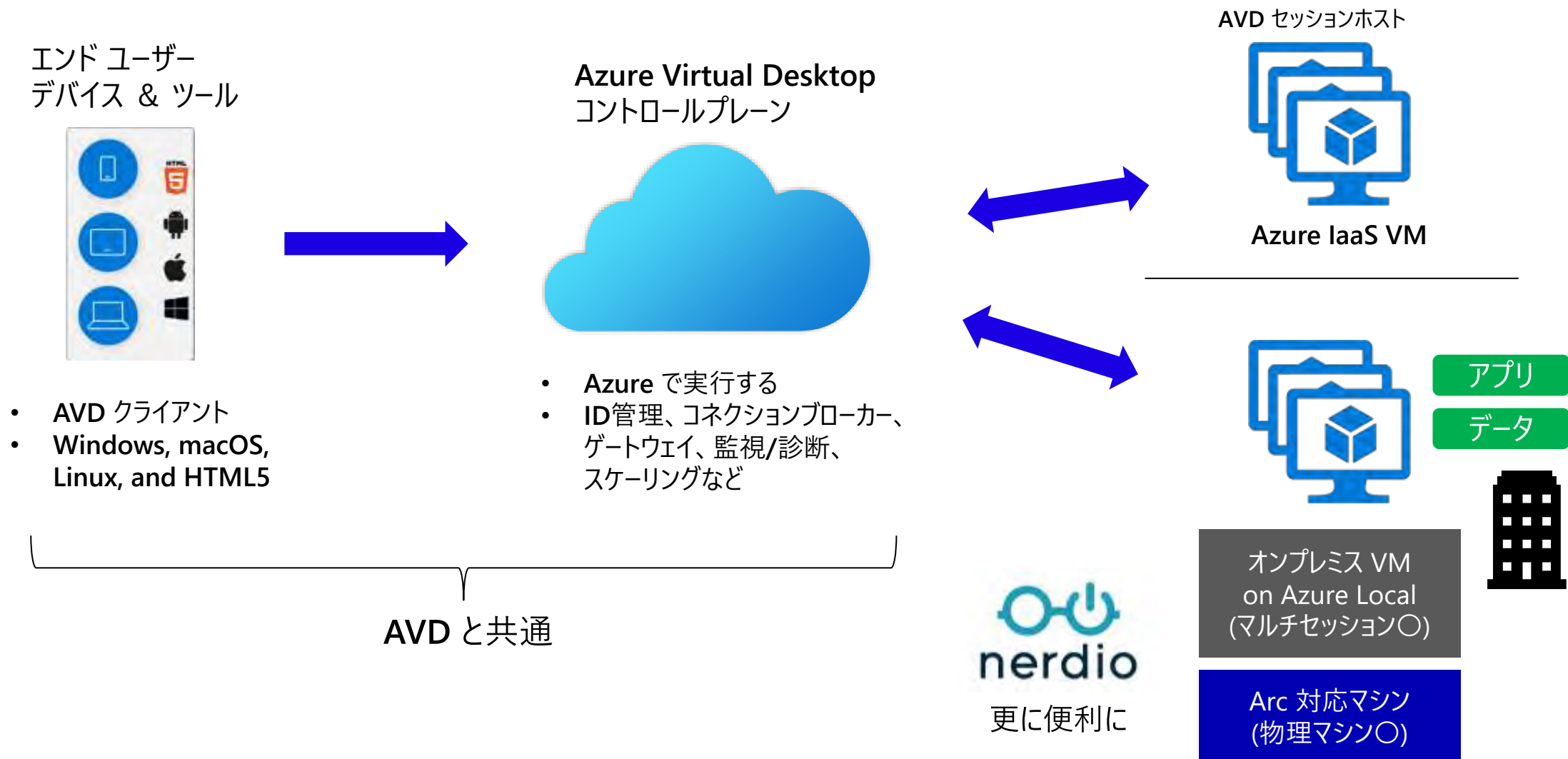
Gartner, Magic Quadrant for Desktop as a Service, Stuart Downes, Craig Fisler, Sunil Kumar, Eri Hariu, Mark Margevicius, Tony Harvey, 11th August 2025. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Microsoft.

Figure 1: Magic Quadrant for Desktop as a Service



Gartner

# AVD for Azure Local (GA) / AVD Hybrid (プレビュー)



# オンプレミス AI

# Azure Local 上で動作する Local AI Chat 画面

The screenshot displays the Local AI Chat interface. The main chat area shows a query: "Grid failure, Sector 7 Ironcrest. Pull the emergency protocol and any past transformer failures in this district." The AI agent, GridOps Agent, has responded with a "Grid Failure Alert — Searching local SharePoint..." and a table of search results.

Document	Date	Type
ironcrest-Emergency-Protocol-v3.2.docx	Mar 2026	Active SOP
PIR-2023-112-ironcrest-S7-Transformer-Failure.docx	Sep 2023	Post-incident review
T4-Inspection-Report-Q1-2026.docx	Feb 2026	Engineering inspection

Below the table, a "Critical finding" is noted: "This exact failure pattern hit Sector 7 in September 2023 — same transformer class, same thermal failure mode. Restoration took 8.1 hours because spares had to be sourced from Forgefield. The Q1 2026 inspection report flagged this unit for..." A recommendation is given: "Recommend activating Emergency Protocol v3.2. Want me to pull the..."

At the bottom of the chat area, there is a "Sources" section with a search bar and a list of sources with toggle switches:

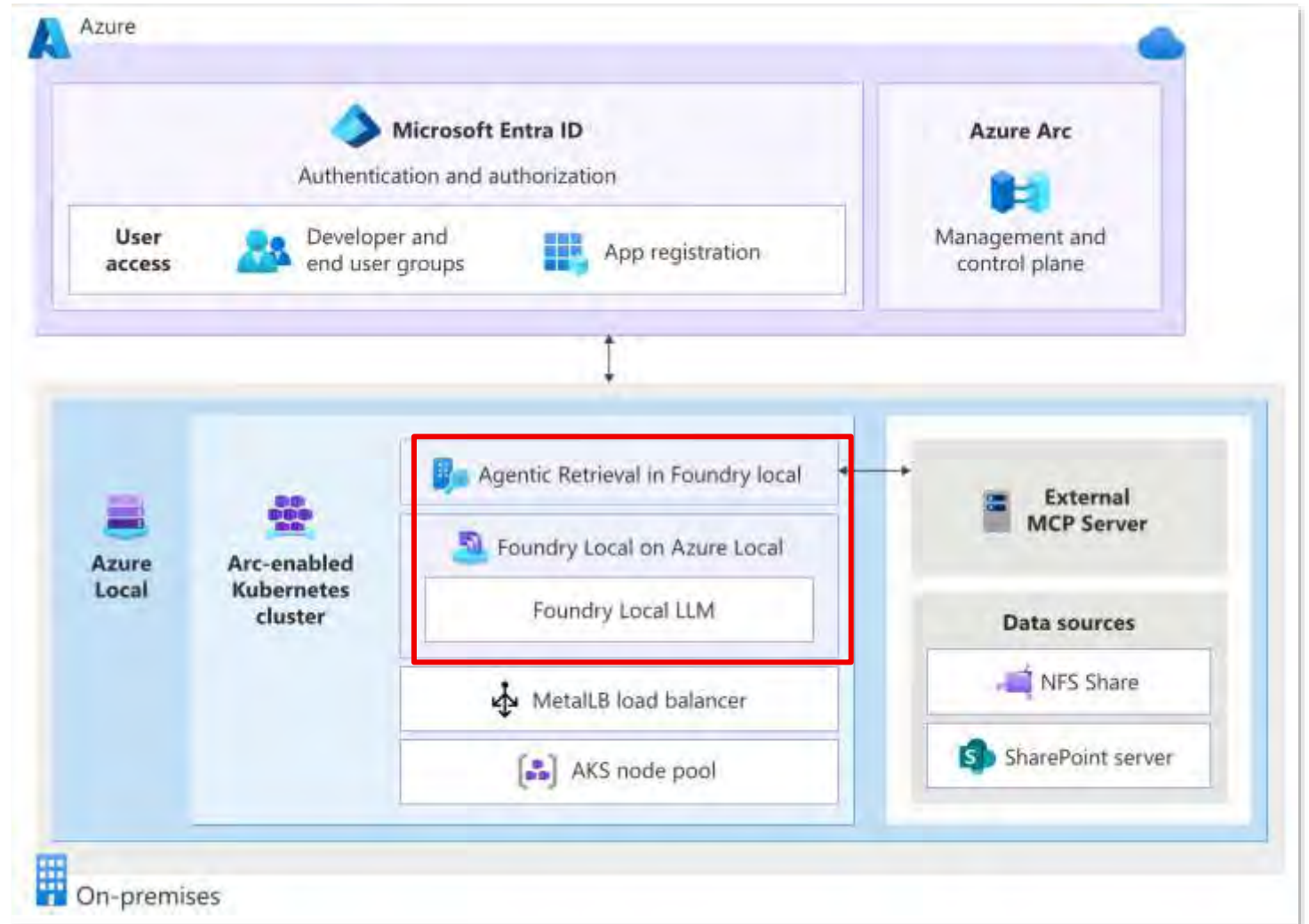
- SharePoint (checked)
- Exchange (checked)
- Navara Emergency Desk MCP (checked)

A callout box highlights the "Sources" section, containing the text: "NFS および SharePoint データの Vector Index 化と SharePoint/Exchange の情報ソースとしての活用".

At the bottom of the interface, there is a "Message Local AI chat" input field with a "Sources" button highlighted by a red box.

# Foundry Local x Agentic Retrieval on Azure Local (プレビュー)

- ユーザーインターフェイス
  - ユーザー向け UI
  - 開発者向け Playground UI
- ナレッジレイヤー
- エージェントレイヤー
- MCP サーバー
- OpenAI 互換エンドポイント
- モデルキャッシュ
- ライフサイクル管理
- APIキー/Entra ID認証
- Azure Monitor、Grafana による可視化



# Vision AI: Azure AI Video Indexer

プレビュー

リアルタイムビデオインテリジェンスを有効化



最大16台のカメラと接続し、小売、サービス、セキュリティ、営業のビデオエージェントが、安全性、行動パフォーマンスを監視



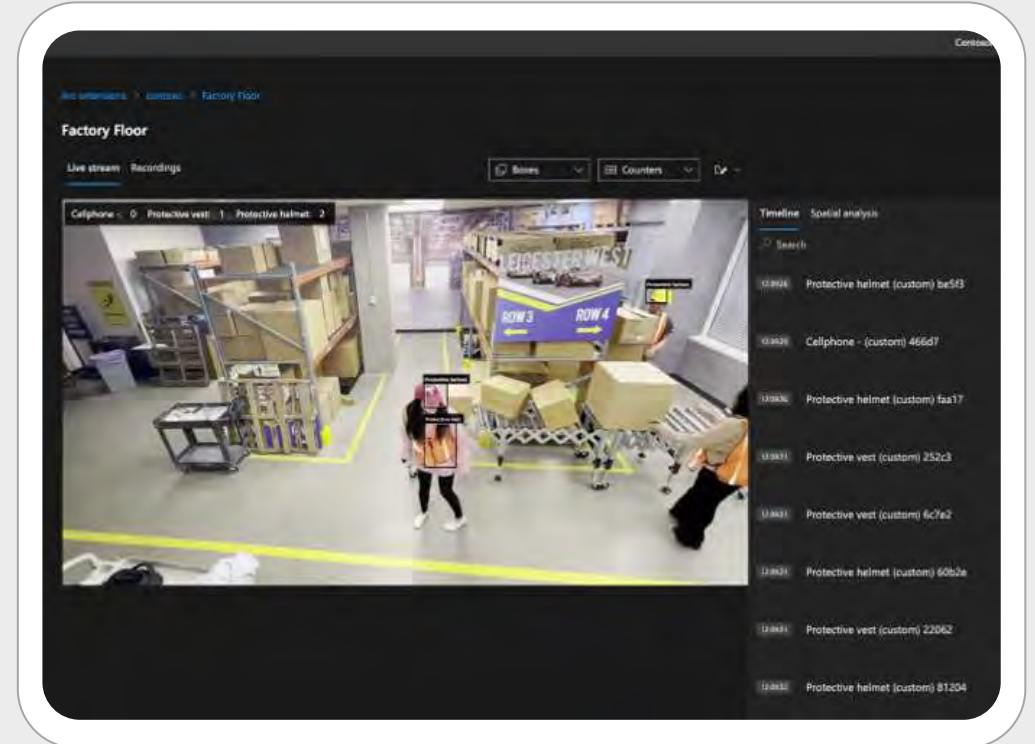
自然言語を用いたカスタムAIモデルを作成し、制限区域でのオブジェクト検出を適用



AIビデオアシスタントチャット:自然言語で質問をし、リアルタイムで答えを入手可能



自然言語を用いて重要な出来事や洞察を捉え、要約を生成



# 小型フォームファクターの導入 (プレビュー)



- 小売店、工場、支社、遠隔地などでのエッジサーバー展開を自動化
- 現地作業：ラッキング、電源オン、準備済みのUSBを挿入するだけ
  - FIDOデバイスオンボーディング(FDO)仕様に基づいている
- Azure からクラスターを展開
- 展開後はAzureから管理

## ダウンロードとインストール

Use the downloaded softwares to install the maintenance image and extract the ownership voucher. [詳細を確認します](#)

### Steps to follow for on-site setup



1. Provide the software to on-site staff to set up the machine.
2. Share the [instructions](#) to guide machine setup.

### 法的条件

By clicking "Download", I agree to the legal terms associated with the following terms.

(a) Public Preview Terms. "プロビジョニング" ("プレビュー") は、次の対象となります: [Supplemental Terms of Use for Microsoft Azure Public Preview](#). 特に明記されていない限り、お客様は、プレビューを使用して法的または規制上のコンプライアンス要件の対象となる個人データまたはその他のデータを処理しないでください。

(b) 制限. プレビューは、テスト、評価、フィードバックにのみ使用できます。運用環境のワークロードは許可されていません。

(c) 機密性. プレビューおよび関連する資料またはドキュメントは機密情報であり、Microsoft との秘密保持契約書における義務の対象となります。

# ソブリンクラウド

# Microsoft ソブリン クラウド

AI、生産性向上、セキュリティ、クラウドプラットフォームを網羅した  
最も総合的なソブリンソリューション群

## ソブリン パブリック クラウド

クラウド規模の主権管理と  
コンプライアンスの機能を内蔵  
生産性向上サービスの地域ごとの  
データ境界を定義  
選択可能な AI モデル、  
国内での AI 処理

## ソブリン プライベート クラウド

**Azure Local** をベースに  
ハイブリッド環境や外部から遮断された  
環境でも運用を継続可能  
Microsoft 365 Local による統合型の  
クラウドと生産性向上ソリューション  
Azure Local による AI 機能と  
高度な GPU のサポート

## ソブリン パートナー エコシステム

グローバルなパートナーと当該国の  
組織による大規模なエコシステム  
主権に関する確かな専門知識を  
身に付けるためのパートナー専用プログラム  
国内でクラウドのホスティングと調達を行う  
ことも可能なパートナー エコシステム

← 一貫性のあるインフラストラクチャ管理と開発プラットフォーム →

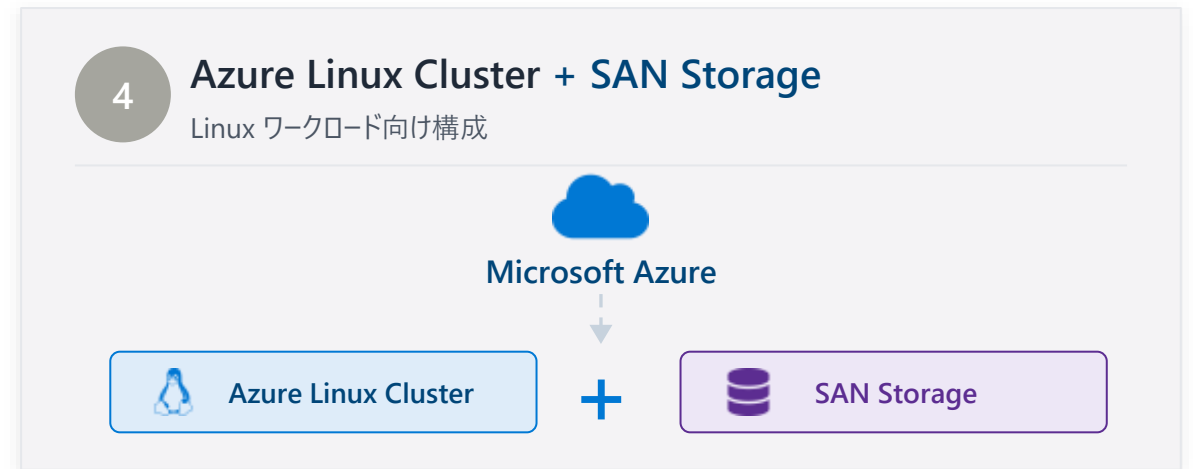
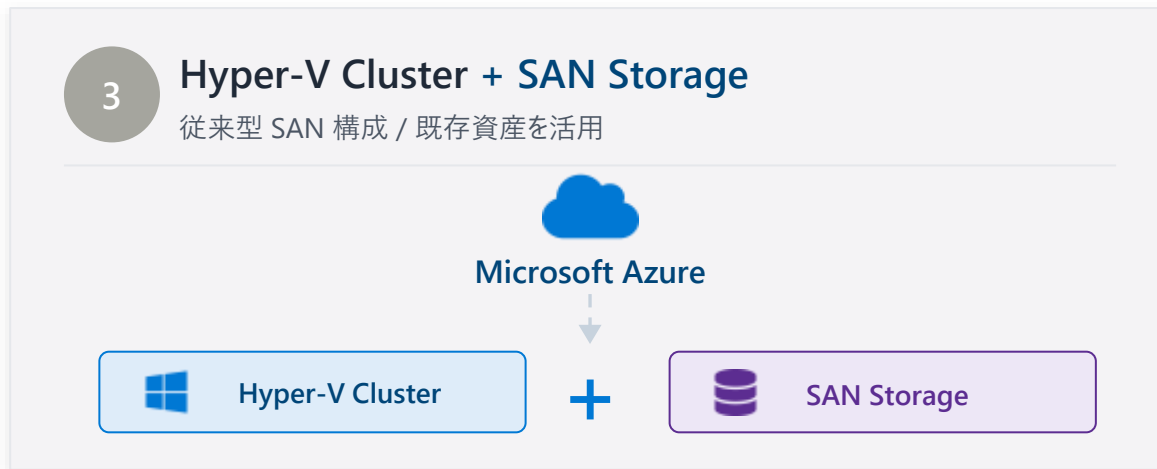
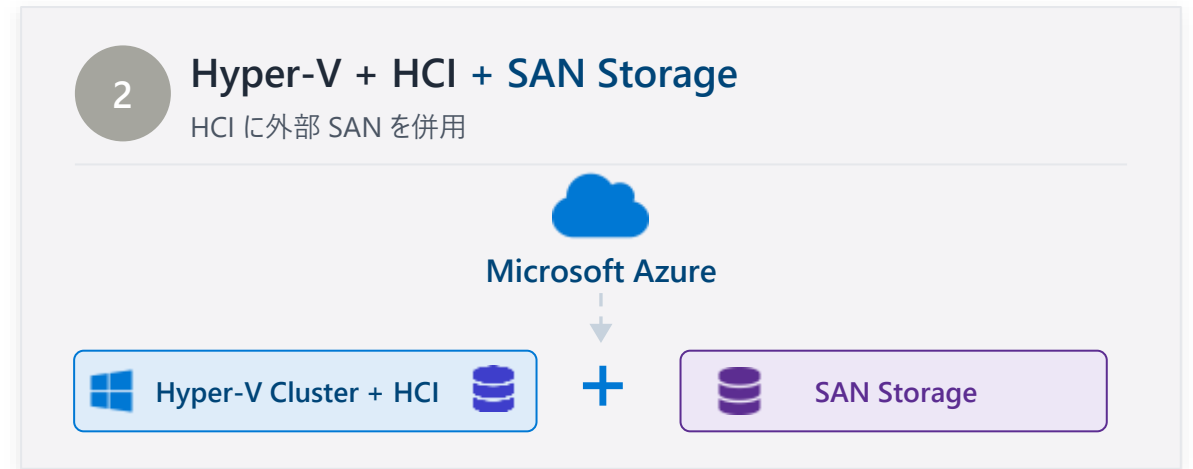
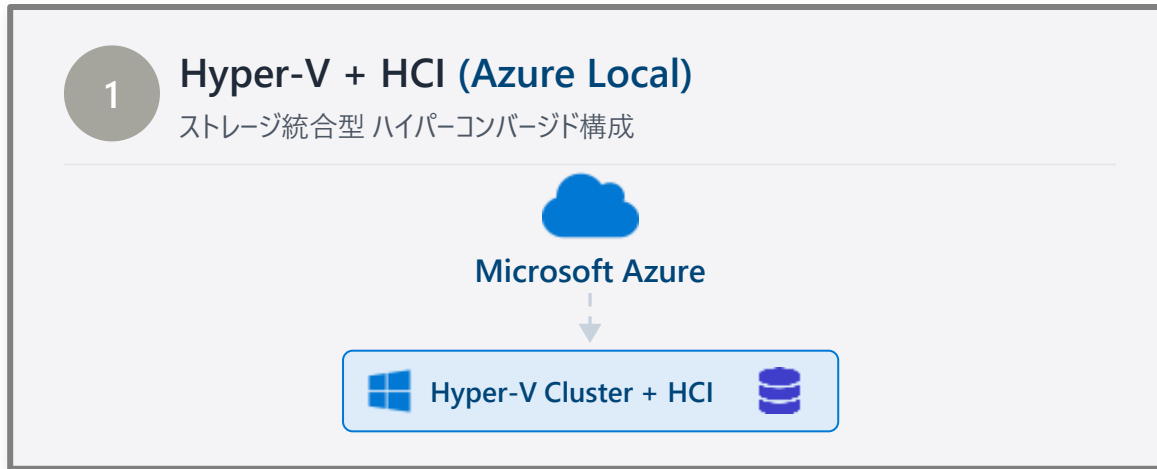


弱点も克服中

まとめ



# Azure Local 展開方式



● + Disconnected operations クラウド非接続環境

# Azure Local

 企業の仮想化基盤から分散拠点プラットフォームまで、幅広く対応するクラウド時代のインフラストラクチャソリューション

 Connected to Azure region (標準)

 Enabled by Azure Arc

 Disconnected to Azure region

 Enabled by Azure Arc

データ主権  
主権的制御

 マネージド Kubernetes/AKS

汎用 VMs/IaaS

コアインフラストラクチャサービス: コンピュート | ストレージ | ネットワーク | 高可用性

ホスト OS: Windows Server | Azure Linux

Azure ベースの  
インフラストラクチャ  
管理

プロビジョニング/展開、  
ライフサイクル管理、  
セキュリティ、アップデート

← お客様資産: ソブリンAIのためのコンポーザブルスケールポイント  
(単一ノードから複数のラッククラスターまで) →



小型デバイス



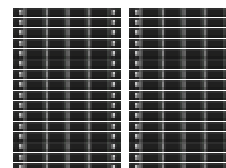
タワー型



シングルノード  
(ラックマウント)



マルチノード  
(ラックマウント)



マルチラック  
(現在 2 ゾーン)



Preview

100 ノード越えの  
クラスター

# クラウド & AI 時代の新しい仮想化基盤 誕生！



1 仮想化基盤も仮想マシンも Azure で運用

2 ソリューションを追加して投資対効果を数倍に

3 まずは簡単に Azure Arc の検証を

4 Azure Local と本格ハイブリッドクラウド化へ着手



ありがとうございました。