PERSOL

Microsoft Partner
Microsoft
Gold Cloud Platform
Gold Cloud Productivity
Gold Security
Gold Application Development
Gold Collaboration and Content

Windows Virtual Desktop In a Day workshop

パーソルプロセス＆テクノロジー株式会社
DXソリューション統括部
PFソリューション部
2020/12/10

会社情報

【社名】	パーソルプロセス＆テクノロジー株式会社
【株主】	パーソルホールディングス株式会社
【社員数】	4,251名（2020年3月1日時点）
【事業内容】	業務プロセスコンサルティング、クラウドサービス、 システム企画・開発・運用・保守、インフラ設計構築、 ICTアウトソーシング、エネルギーアウトソーシング、 カスタマーサポート支援、バックオフィス支援、 セールスアウトソーシング、WEBアナリティクスサービス、 パッケージソフト導入及び保守運用
【代表者名】	代表取締役社長　横道 浩一
【設立】	1977年9月（昭和52年9月24日）
【事業拠点】	豊洲本社、赤坂、大阪、名古屋、札幌、仙台、福岡、沖縄
【子会社】	パーソルプロセス＆テクノロジー ベトナム Bizer株式会社 パーソルメディアスイッチ株式会社
【本社所在地】	〒135-0061　東京都江東区豊洲3-2-20　豊洲フロント７階

Microsoft パートナーシップ＆クラウド普及活動

Microsoft Partner of the Year 2020 AWARD

マイクロソフト パートナー オブ ザ イヤー
2016・2018・2020

Microsoft Partner
Microsoft

- Gold Cloud Platform
- Gold Cloud Productivity
- Gold Security
- Gold Application Development
- Gold Collaboration and Content

ACE Azure Council Experts

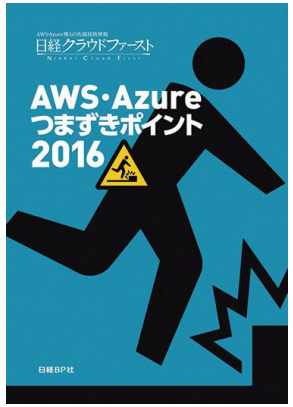
Microsoft Digital Trust Security Alliance

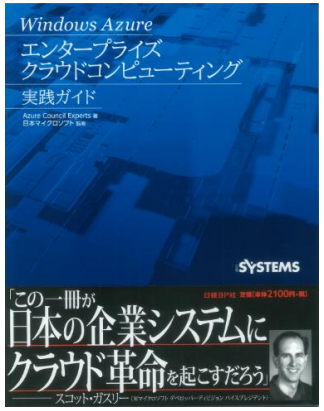
Deep Learning Lab

IoT ビジネス共創ラボ

各種コミュニティ活動

協力アーキテクト





執筆活動

■Microsoft Azure 自習書シリーズ　執筆
http://blogs.msdn.com/b/windowsazurej/archive/2014/06/02/blog-published-azure-self-learning-series.aspx

■Microsoft Azure SlideShare　　執筆
http://blogs.msdn.com/b/windowsazurej/archive/2014/07/18/blog-release-microsoft-azure-slide-series.aspx

■Microsoft Azure IaaSリファレンスアーキテクチャ　執筆
http://www.microsoft.com/ja-jp/server-cloud/local/documents/default.aspx?pdid=Azure&svid=Microsoft_Azure&dtid=all_DT

Windows Virtual Desktop の歴史

2019 11月 WVD 正式リリース @Ignite

2020年7月 Teams on WVD 正式サポート

2019 12月 管理プレーン 日本リージョン 対応

2020年5月 WVD ARM 管理UIのGUI化

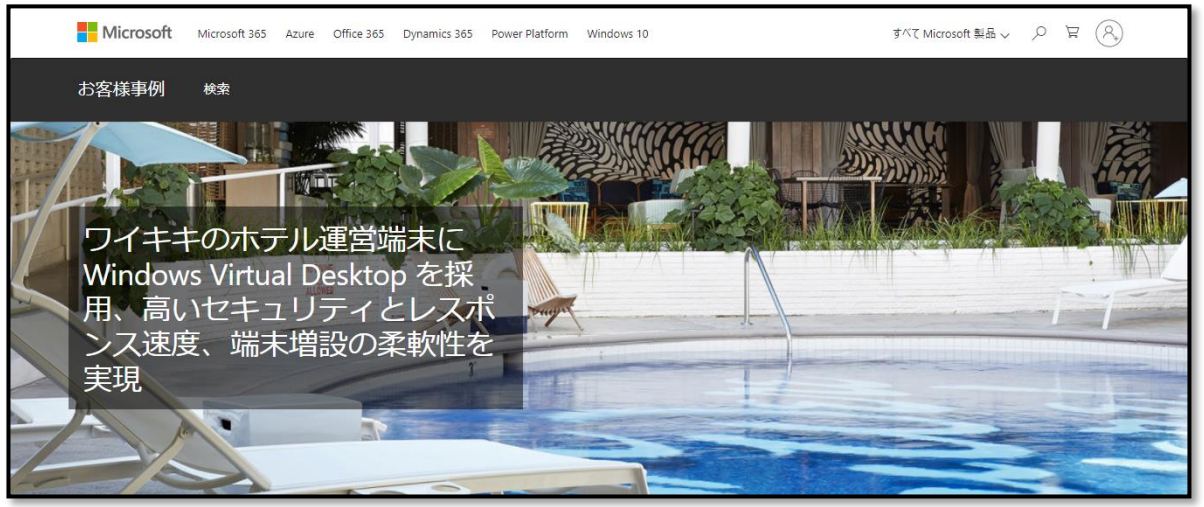
Native Windows Virtual Desktopの導入実績及び導入事例

- 導入実績（~2020年10月 時点）

40件以上

- 導入事例
  - お客様：株式会社星野リゾート
  - 利用者拠点：ハワイ州オアフ島
  - Azureリージョン：米国西部海岸
  - VDI台数：25台

詳細はMicrosoft
公開事例サイトにて



https://customers.microsoft.com/ja-jp/story/818862-hoshino-resort-holdings-inc-jp-japan

Agenda

午前の部：セミナー(10:00~12:00)

1. リモートワークの在り方
2. WVDの特徴と価値
3. 導入前に抑えておきたいポイント
4. 構成例のご紹介
5. 導入支援メニュー紹介
6. Appendix

午後の部：ハンズオン/デモ(13:00~16:00)

1. WVDの接続
    1. デスクトップアプリからの接続
    2. ブラウザアプリからの接続
2. 基本操作
    1. WVDの設定
    2. ユーザーの割当
3. 管理者操作
    1. 条件付きアクセス（多要素認証）
    2. 自動スケール
    3. 監視
    4. エラー対応
    5. マスター更新

本セミナーはMicrosoft Teamsのライブイベントにて配信いたします。
セミナー終了後12時間まではアーカイブが残りますので、後からご確認いただけます。

質問及びアンケートについて

Teamsライブイベントから質問を投稿いただけます。
お気軽にご質問ください。

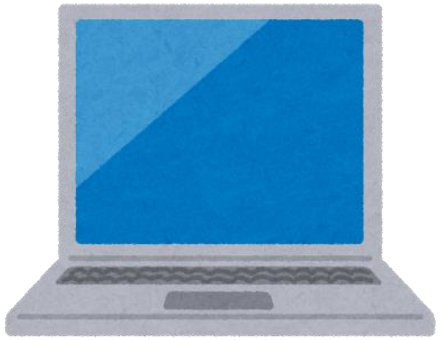
セミナー終了後は、お手数をおかけいたしますが下記のアンケートにご協力ください。
Microsoft Forms

https://forms.office.com/Pages/ResponsePage.aspx?id=qBOeDc_Oeke1zpJxi2t63RZHt4CqNtNKrtI3Uk2vAKNUMTBCVUdVTFZXRDRYSk84MzAyRkI1U0tBQi4u

1. リモートワークの在り方

加速するデジタル変革

場所やデバイスを選ばず、あらゆる従業員に最新のデスクトップ環境を提供。
→ デスクトップの仮想化が求められている。



デスクトップの仮想化が役立つとき

リモートワーク
・コールセンター
・ブランチ オフィスワーカー
・BYOD/モバイル

フレキシブルな労働環境
・合併/買収
・パートタイム

セキュリティと規制
・医療機関
・金融サービス
・政府機関

リモートワーク導入で気を付けるポイント

業務効率の低下
・プライベートのON/OFF
・長時間勤務
・ネットワークのレスポンス

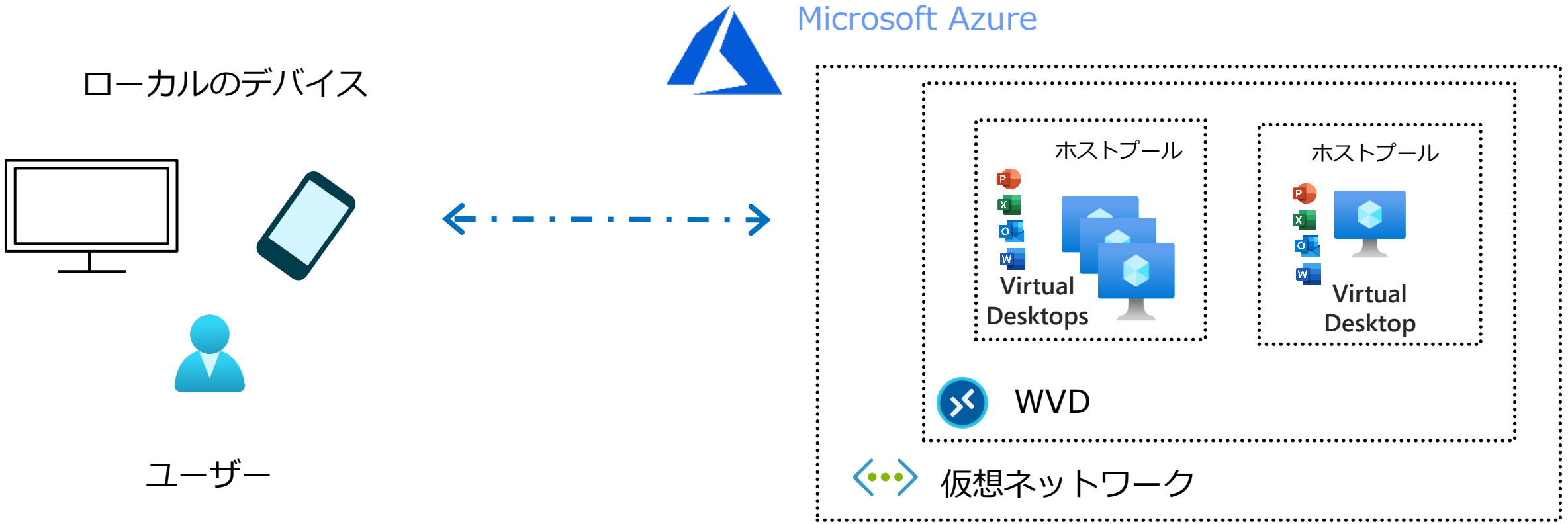
セキュリティリスク
・脆弱なネットワーク
・セキュリティ/OS更新

情報漏洩
・覗き見・書類置き忘れ
・PC等の紛失
・アクセスID・パスワード漏洩

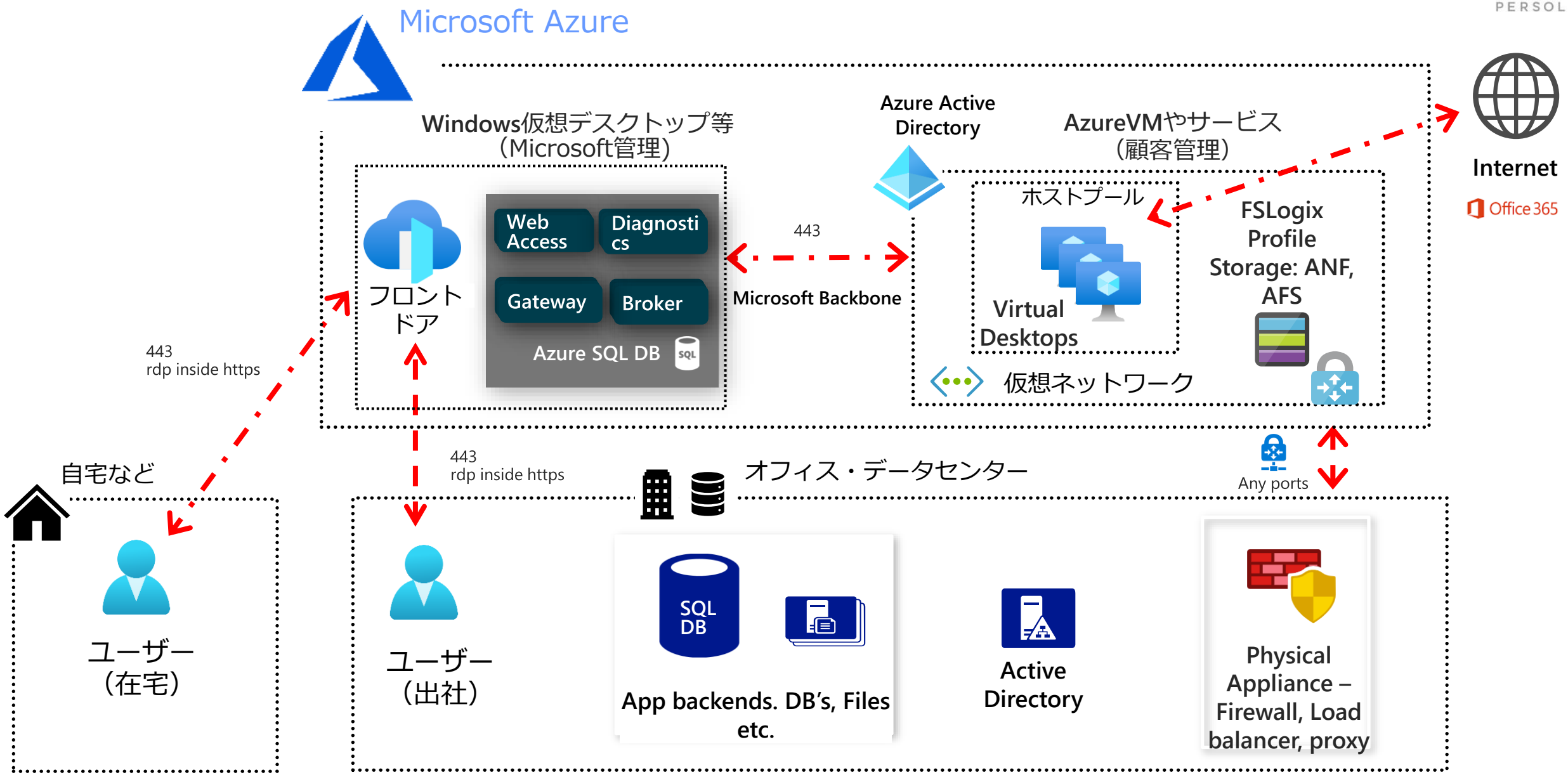
2. WVDの特徴と価値

WVDイメージ

WVD ： Virtual Desktops in Azure

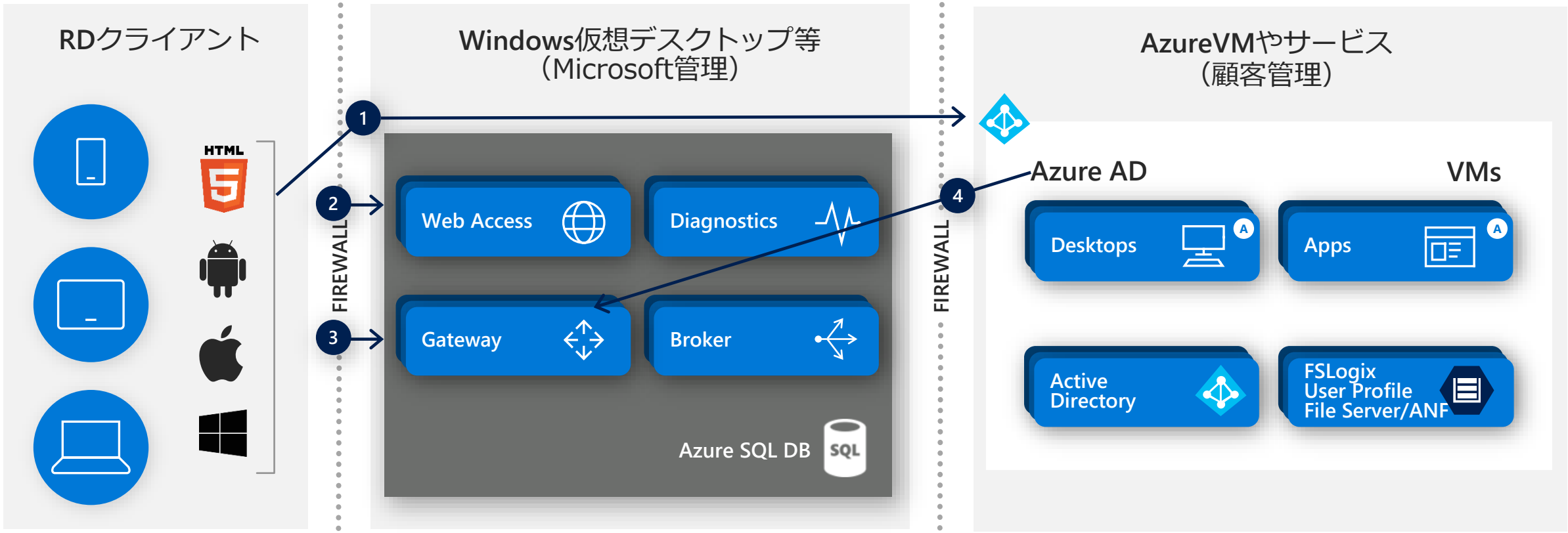


全体概要



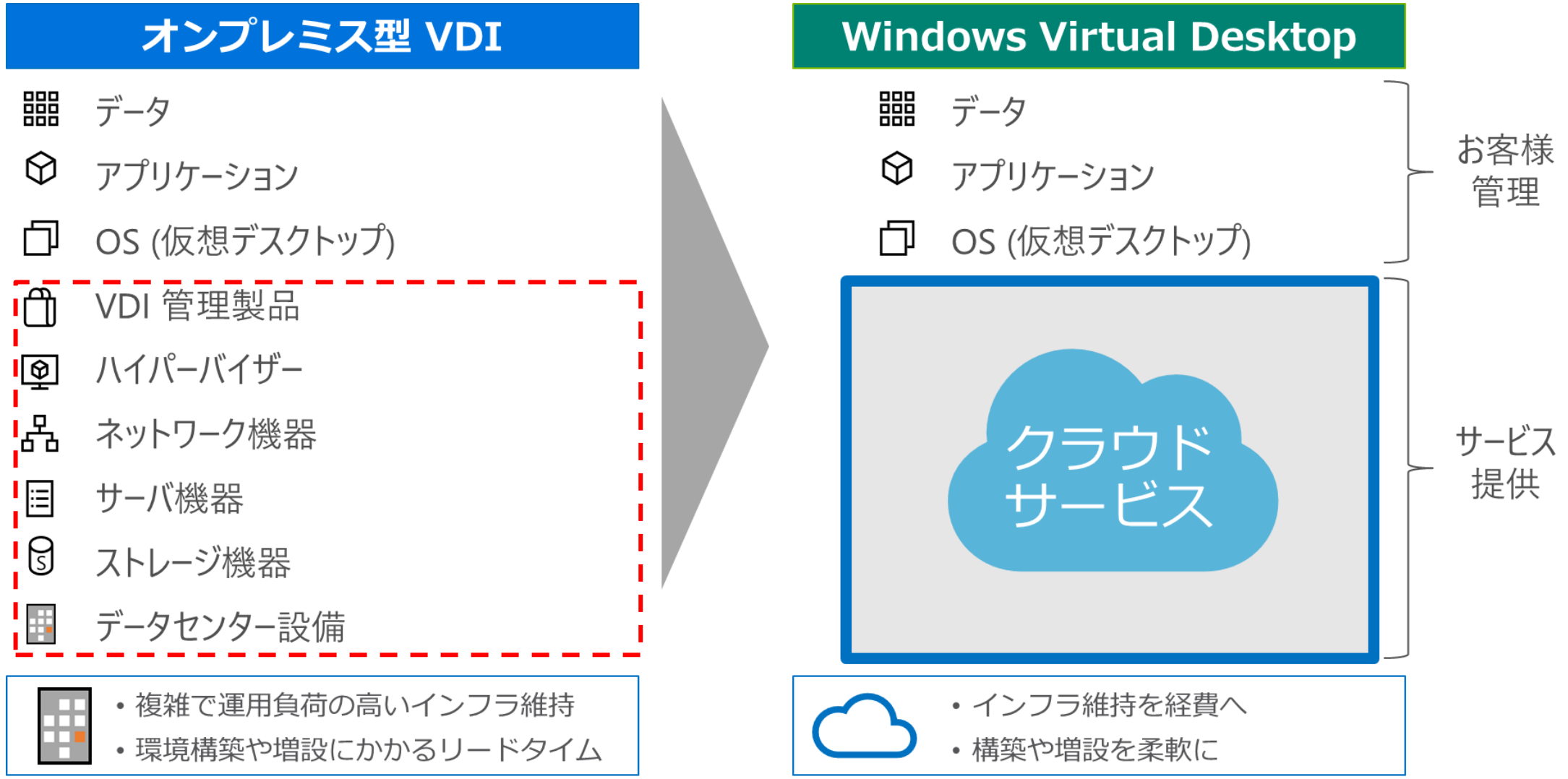
ユーザーの接続フロー

1. ユーザーがAzureADに接続するRDクライアントにサインインすると、AzureADがトークンを返します。
2. RDクライアントはwebアクセスにトークンを提示し、ブローカーがユーザーに承認されたリソースを確認するためSQLDBでクエリを実行します。
3. ユーザーがリソースを選択し、RDクライアントがゲートウェイに接続します。
4. ブローカーは接続を組み合わせ、ホストからゲートウェイへの接続を行います。



VDIのクラウド化の促進

管理層はマイクロソフトによるマネージドサービス



WVDの特徴と価値

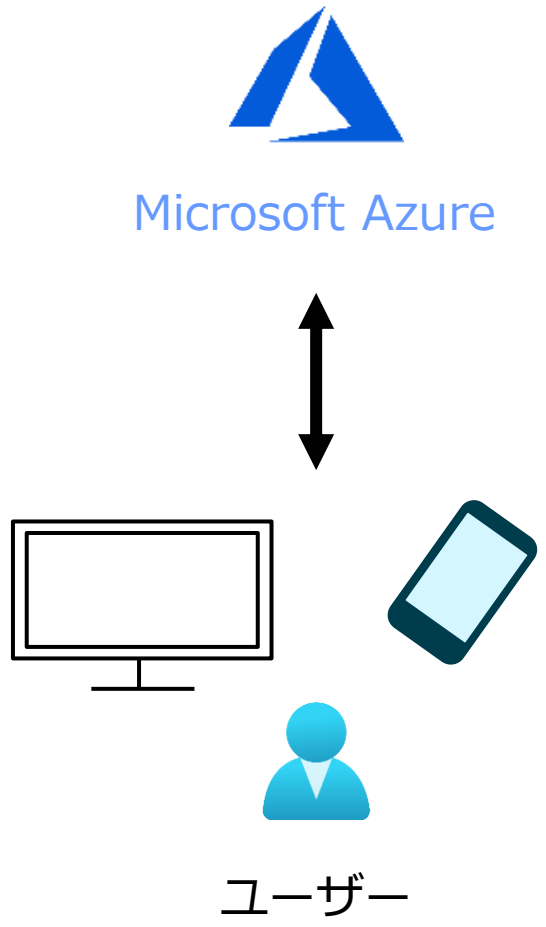
Point 1
Windows10 Multi Sessionの提供（WVDのみ）

Point 2
従量課金で低コストの実現

Point 3
拡張性/柔軟性/俊敏性

Point 4
FAT PCに近いUX

Point 5
マルチデバイスへの対応



WVDの特徴と価値

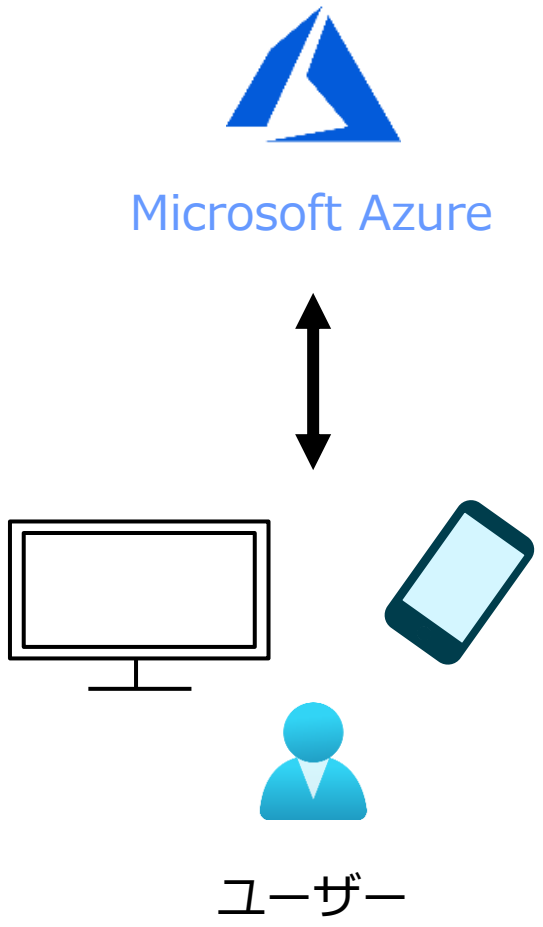
Point 1
Windows10 Multi Sessionの提供（WVDのみ）

Point 2
従量課金で低コストの実現

Point 3
拡張性/柔軟性/俊敏性

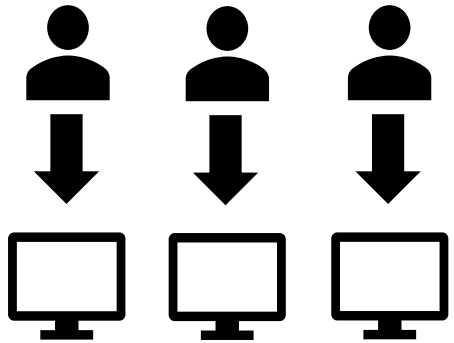
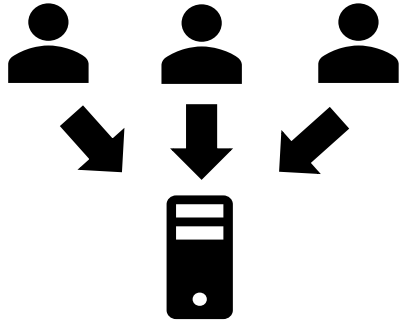
Point 4
FAT PCに近いUX

Point 5
マルチデバイスへの対応



Point 1 Windows 10 Multi Sessionの提供

従来提供されていた2種類のデスクトップ仮想化方式

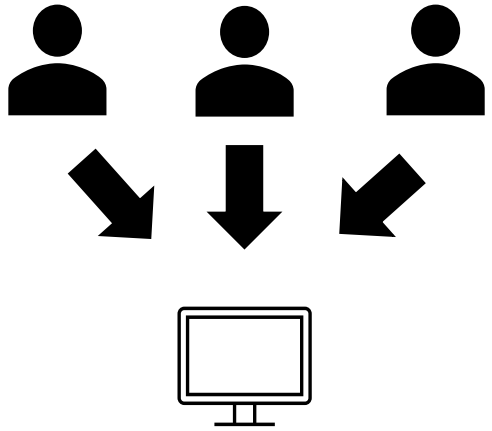
	集約率	コスト	OS	アプリ互換性
VDI(Virtual Desktop Infrastructure)  Windows 10 (Client OS)	低	高	Client OS	高
SBC(Server Based Computer)  Windows Server (Server OS)	高	低	Server OS	低

Point 1 Windows 10 Multi Sessionの提供

WVDのみに許されたWindows 10 Mulitisession

- VDI/SBC方式の良いとこ取り
  ※それぞれの方式を採用することも可能

WVD(Windows Virtual Desktop)



Windows 10 (Client OS)

	集約率	コスト	OS	アプリ互換性
WVD	高	低	Client OS	高
VDI	低	高	Client OS	高
SBC	高	低	Server OS	低

WVDの特徴と価値

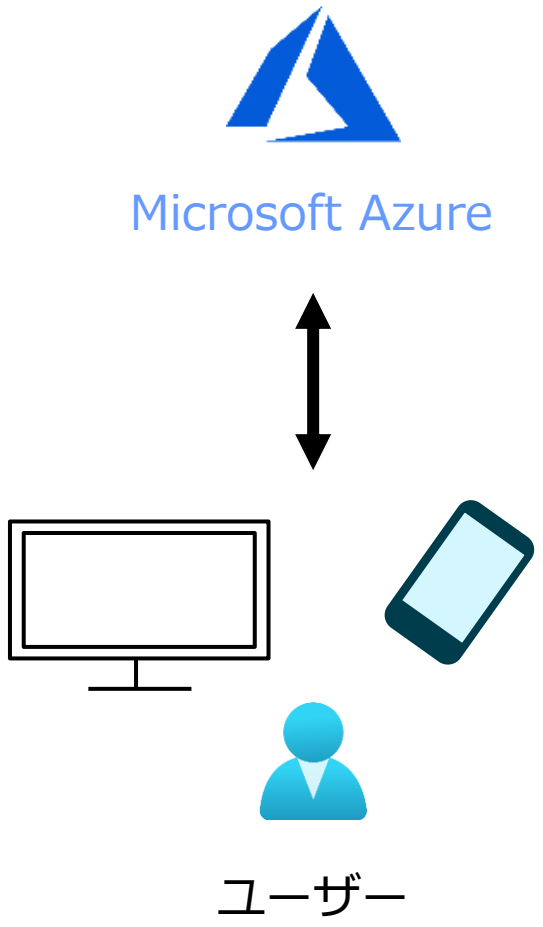
Point 1
Windows10 Multi Sessionの提供（WVDのみ）

Point 2
従量課金で低コストの実現

Point 3
拡張性/柔軟性/俊敏性

Point 4
FAT PCに近いUX

Point 5
マルチデバイスへの対応

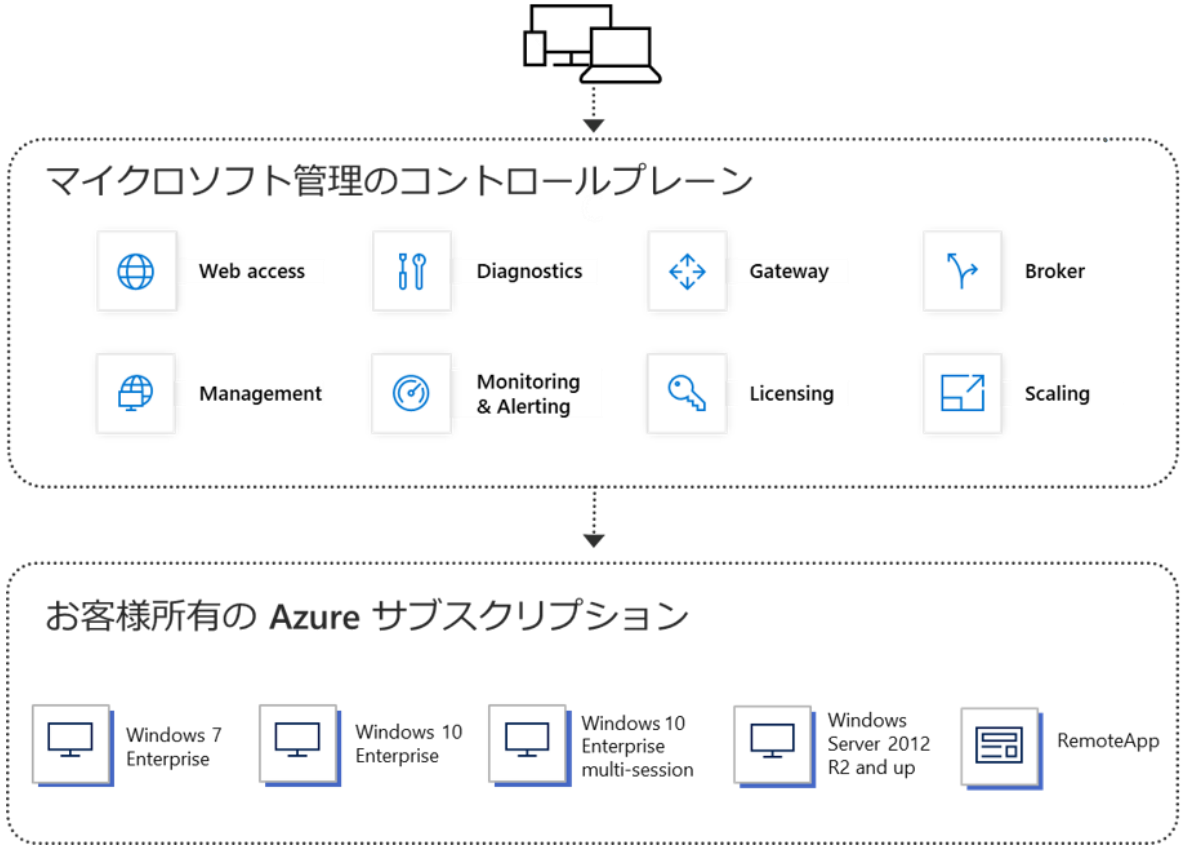


Point 2 使った分だけの従量課金で低コストを実現

従来のクラウドVDI利用料金：Windows 10 ライセンス + Azure 利用料＋**VDIライセンス**

WVDにおける利用料金：Windows 10 ライセンス + Azure 利用料

コントロールプレーンの使用料は
所定の Windows ライセンスに含まれており
追加コスト不要
（Microsoft 365 E3/E5 または Windows 10 E3/E5 等が必要）



仮想マシン、ストレージ、ネットワークなどの **Azure 利用料金を実費**でお支払い

台数やユーザー数に応じてスモールスタートも可能

料金のシミュレーションは後程説明いたします

WVDの特徴と価値

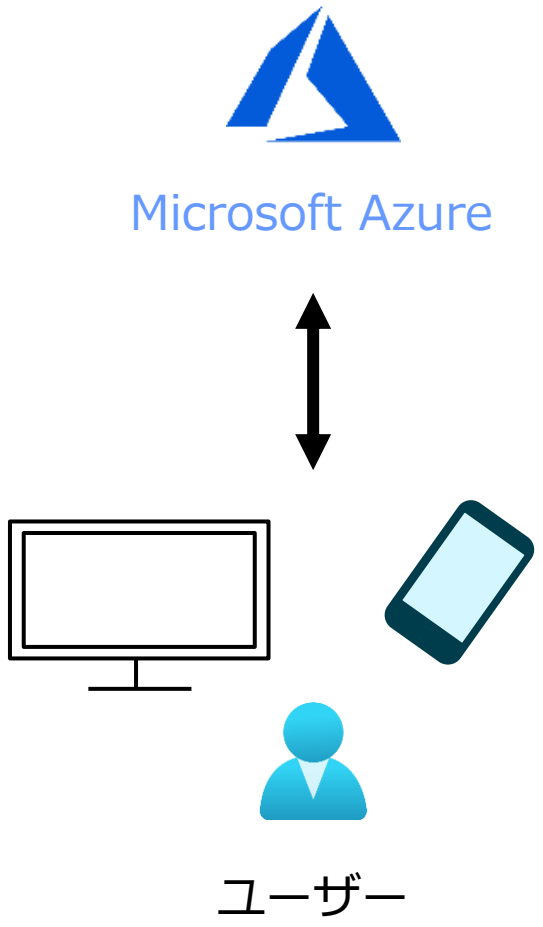
Point 1
Windows10 Multi Sessionの提供（WVDのみ）

Point 2
従量課金で低コストの実現

Point 3
拡張性/柔軟性/俊敏性

Point 4
FAT PCに近いUX

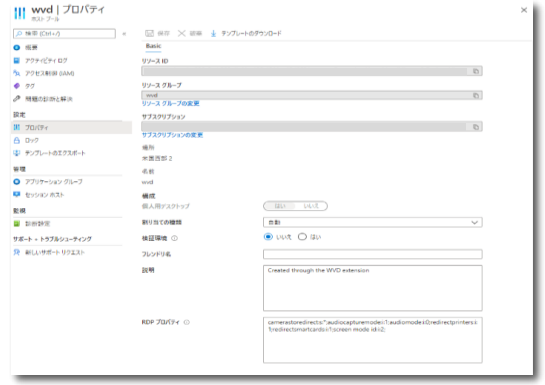
Point 5
マルチデバイスへの対応



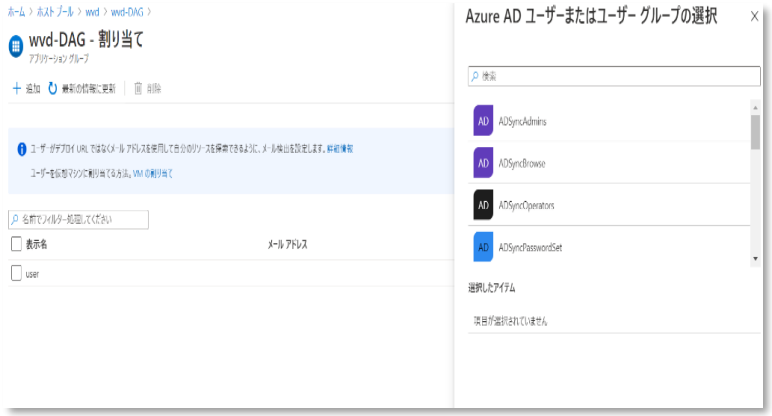
Point 3 Microsoft Azureが提供する 拡張性/柔軟性/俊敏性

オブジェクトをARMで視覚的に管理可能

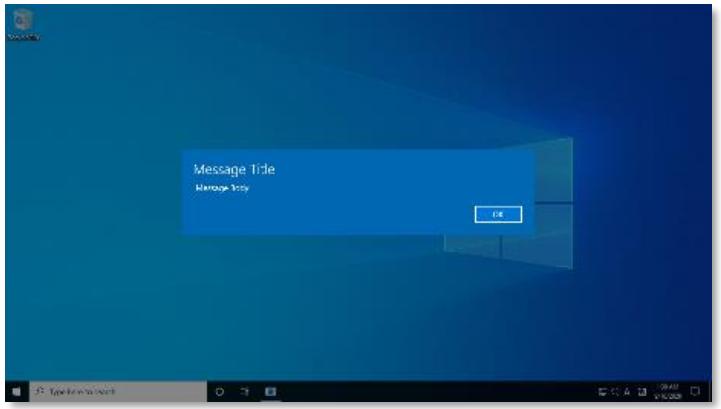
RDPコンフィグをポータル上で管理可能



ユーザー割り当てが容易



ユーザーへのメッセージを送ることも可能



Point 3 Microsoft Azureが提供する 拡張性/柔軟性/俊敏性

最近のアップデートでは、WVD上で快適なTeams利用を実現

更新情報 / Windows Virtual Desktop Azure portal and Microsoft Teams integrations are generally available

提供中

Windows Virtual Desktop Azure portal and Microsoft Teams integrations are generally available

公開日: 7月 28, 2020

In April 2020, we released the public preview of Azure portal integration (also called the Spring Update) which made it easier to deploy and manage Windows Virtual Desktop. We also announced a new audio/video redirection (A/V redirect) capability that provided seamless meeting and collaboration experience for Microsoft Teams. Both these capabilities are now generally available.

With the Azure portal integration, you get a simple interface to deploy and manage apps and virtual desktops. Host pool, workspace, and all other objects you create are Azure Resource Manager objects and are managed the same way as other Azure resources. You can provide fine-grained access to Windows Virtual Desktop resources using role-based access control, publish remote apps and desktops to AAD groups instead of individual users and troubleshoot issues faster with Azure Monitor.

https://azure.microsoft.com/ja-jp/updates/windows-virtual-desktop-azure-portal-and-microsoft-teams-integrations-are-generally-available/

WVDの特徴と価値

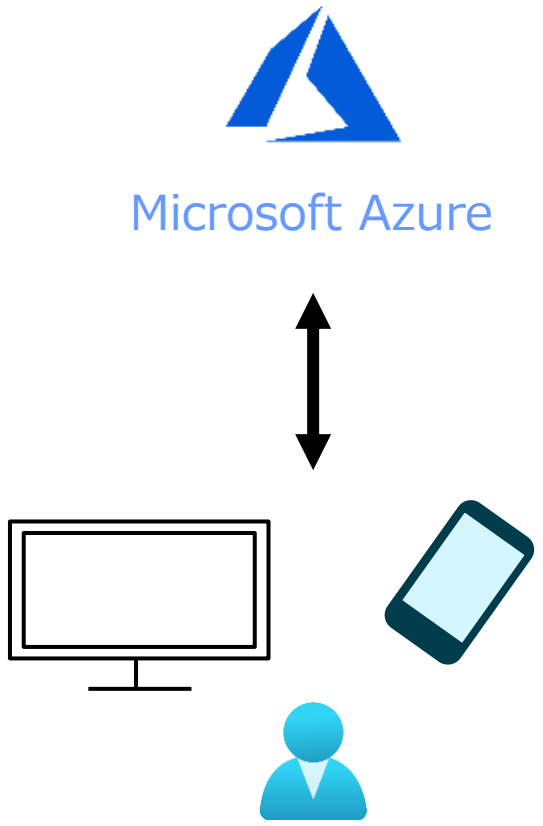
Point 1
Windows10 Multi Sessionの提供（WVDのみ）

Point 2
従量課金で低コストの実現

Point 3
拡張性/柔軟性/俊敏性

Point 4
FAT PCに近いUX

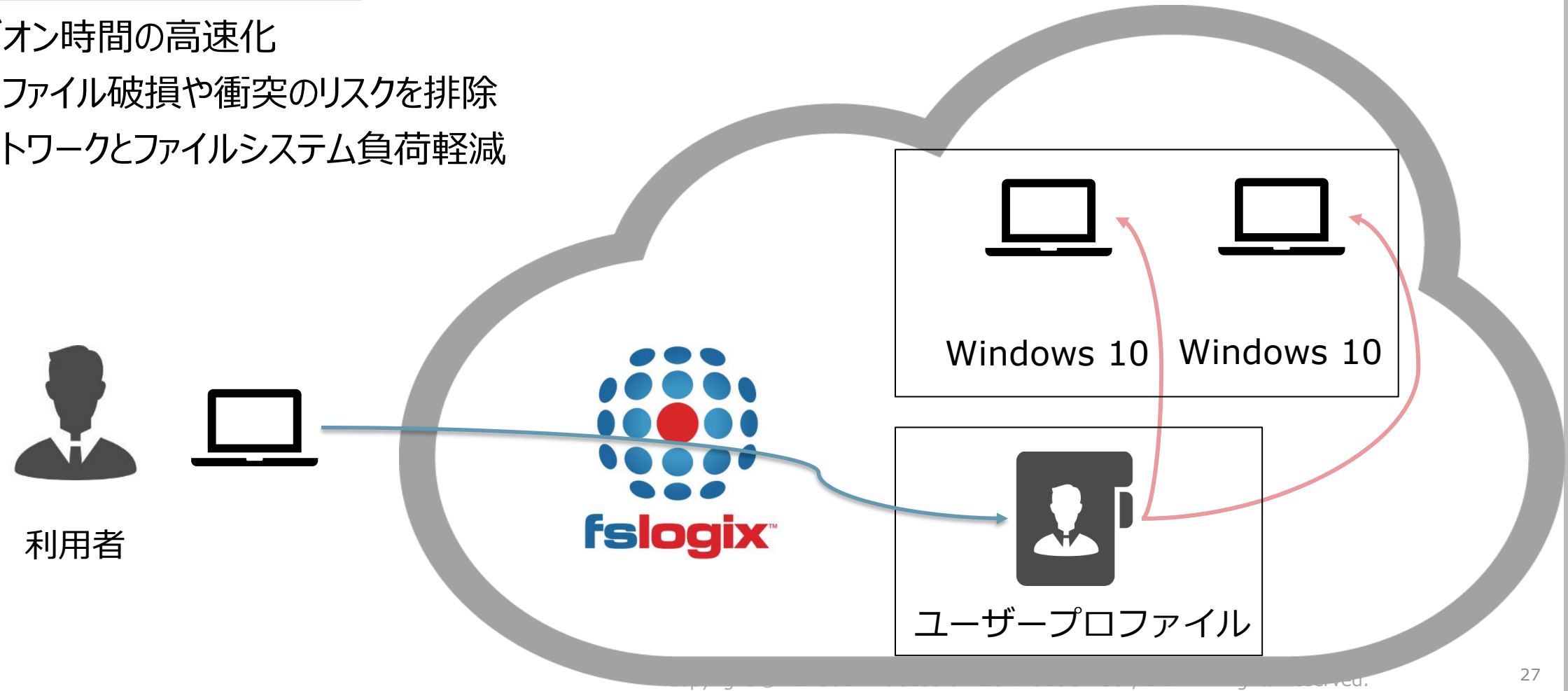
Point 5
マルチデバイスへの対応



Point 4 FAT PCに近いUX

FSLogix
- ユーザープロファイル管理を行う3rdパーティのローミング ソリューション

プロファイル管理の課題を解決
- ログオン時間の高速化
- プロファイル破損や衝突のリスクを排除
- ネットワークとファイルシステム負荷軽減



WVDの特徴と価値

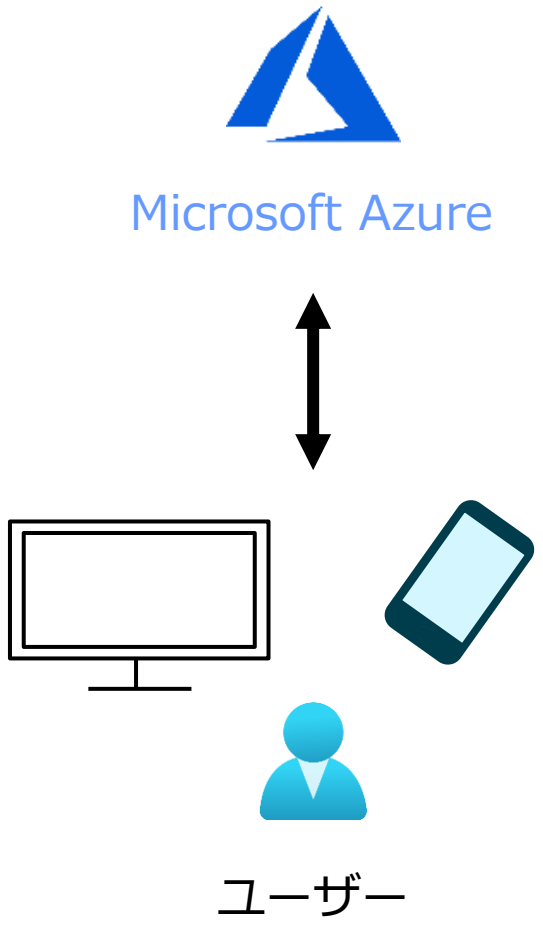
Point 1
Windows10 Multi Sessionの提供（WVDのみ）

Point 2
従量課金で低コストの実現

Point 3
拡張性/柔軟性/俊敏性

Point 4
FAT PCに近いUX

Point 5
マルチデバイスへの対応



Point 5 マルチデバイスへの対応

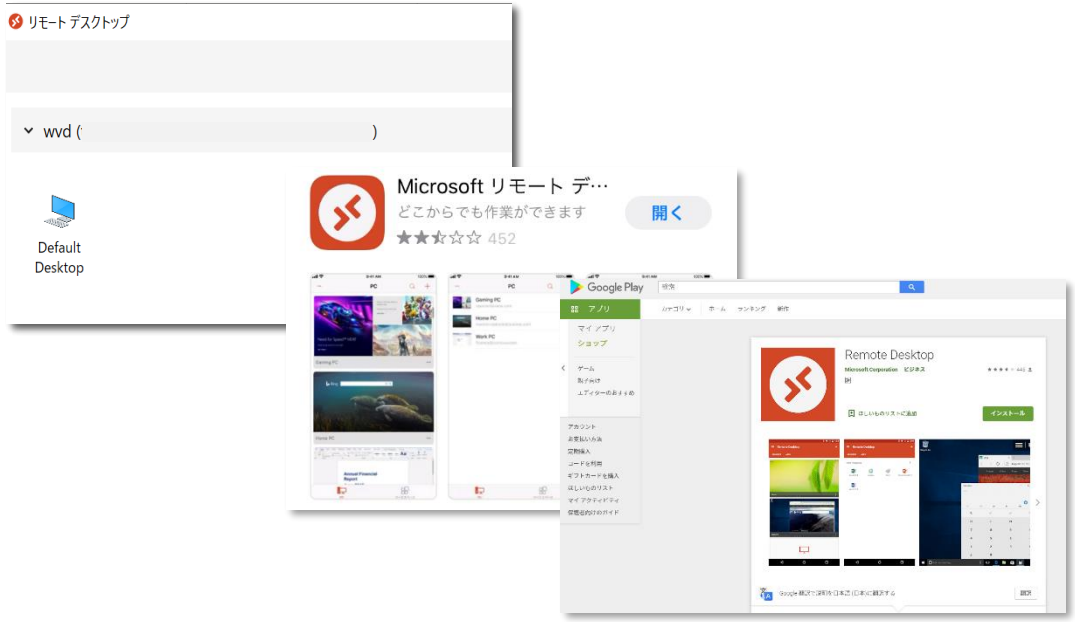
主要な端末、ブラウザに対応しているため、すぐに使える。

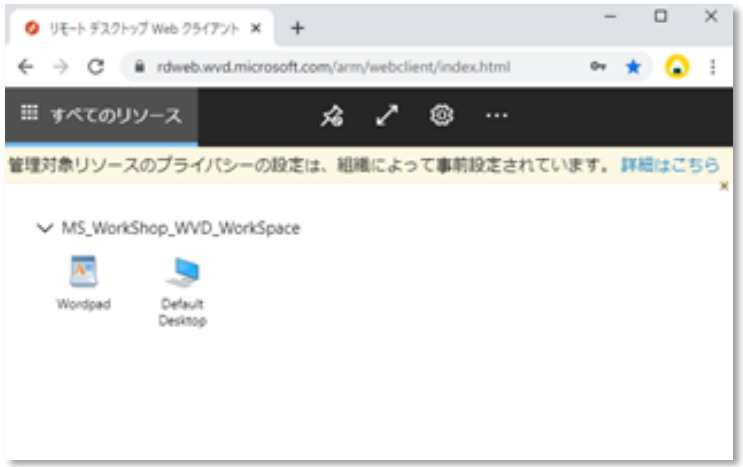
ClientApp

- Windows
- iOS
- Android
- macOS

Web

- Windows
- Chrome OS
- macOS
- Linux





WVDの特徴と価値

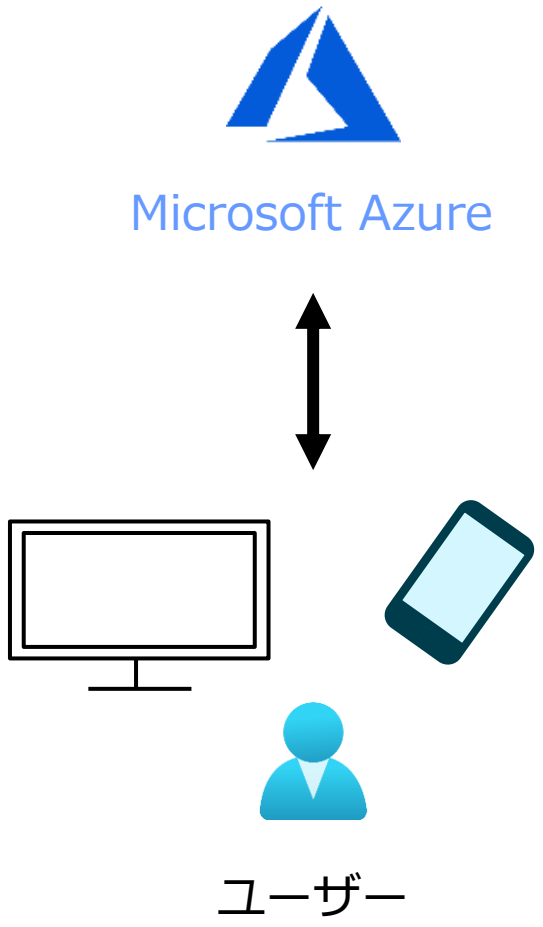
Point 1
Windows10 Multi Sessionの提供（WVDのみ）

Point 2
従量課金で低コストの実現

Point 3
拡張性/柔軟性/俊敏性

Point 4
FAT PCに近いUX

Point 5
マルチデバイスへの対応



3. 導入前に抑えておきたいポイント

導入前に抑えておきたいポイント

Point 1
VDIにインストールするアプリケーションの注意点

Point 2
Azure ADとActive Directoryの関係性

Point 3
ライセンスの種類

Point 4
既にAzureを利用している場合の注意点

Point 5
ネットワークの閉域化は一部のみ

Point 6
ネットワークセキュリティを強靭にするには

導入前に抑えておきたいポイント

Point 1
VDIにインストールするアプリケーションの注意点

Point 2
Azure ADとActive Directoryの関係性

Point 3
ライセンスの種類

Point 4
既にAzureを利用している場合の注意点

Point 5
ネットワークの閉域化は一部のみ

Point 6
ネットワークセキュリティを強靭にするには

アプリケーション セットアップ時の注意事項

- アプリケーションはマルチセッションOSで動作が保証されているか
  マルチセッションでは、CPU、メモリ、ディスクを他のユーザーと共用して利用します。
  アプリケーションが排他的な利用しかできない場合は、WVDをシングルセッションで構成する必要があります。
  ※アプリケーションの動作確認はお客様にて事前にご確認ください。

- アプリケーションはマシン単位にインストールする
  ユーザー単位にアプリケーションをインストールした場合、他のユーザーがそのアプリケーションを利用することはできません。

- アプリケーションはSysprep動作に影響を与えないか
  Azure環境では応答ファイルを利用することができないため、ウイルス対策ソフトなどは個別にインストールしなければならない場合があります。
  セッションホストの台数が多い場合は、サイレント インストールをご検討ください。

- 一部のユーザーには非表示にしたいアプリケーションがある
  利用ユーザーに合わせてマスターイメージを複数用意することもできますが、
  FSLogixのApplication Maskingソリューションを利用することで、
  マスターイメージの数を削減することを推奨します。

導入前に抑えておきたいポイント

Point 1
VDIにインストールするアプリケーションの注意点

Point 2
Azure ADとActive Directoryの関係性

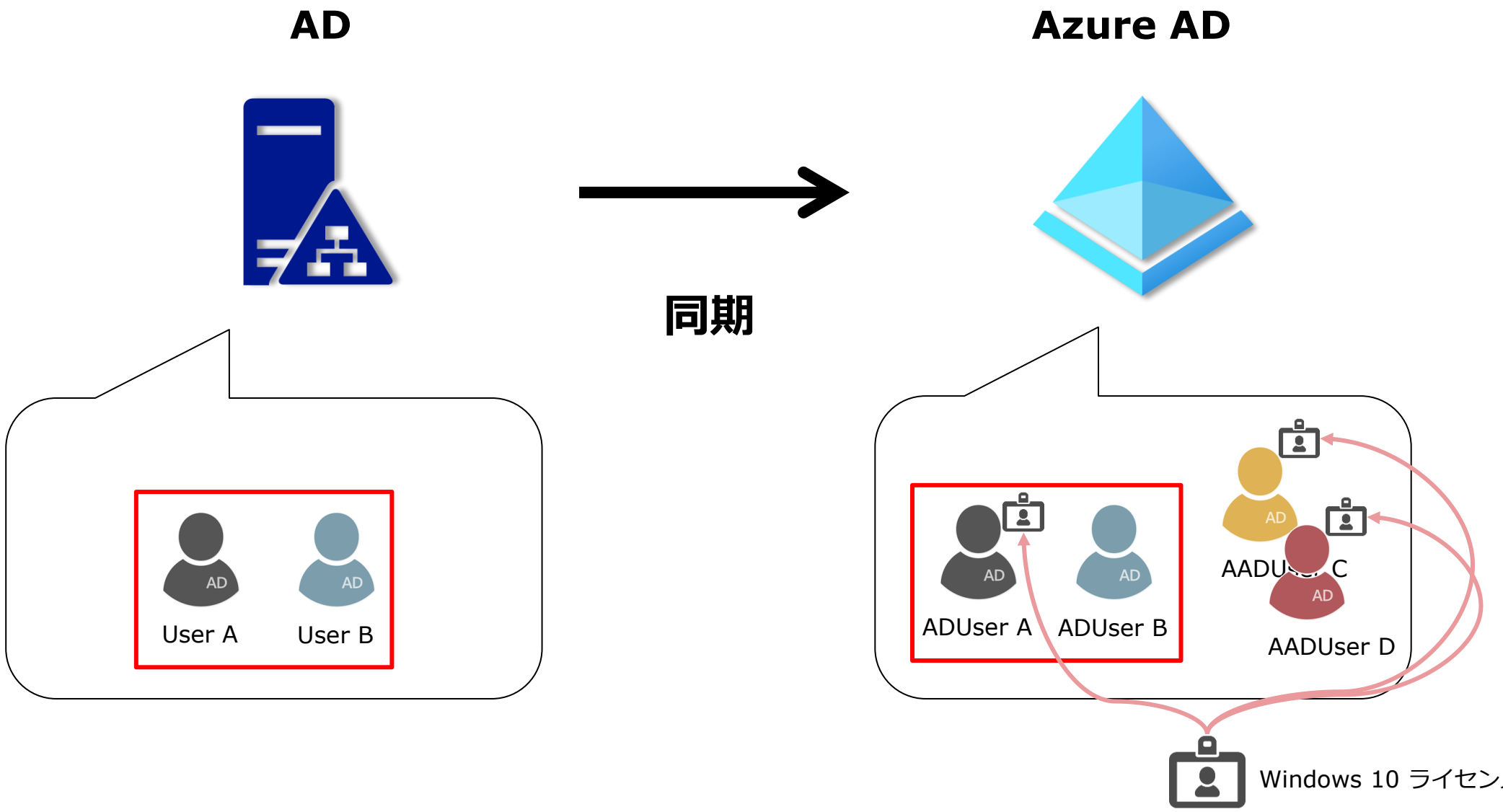
Point 3
ライセンスの種類

Point 4
既にAzureを利用している場合の注意点

Point 5
ネットワークの閉域化は一部のみ

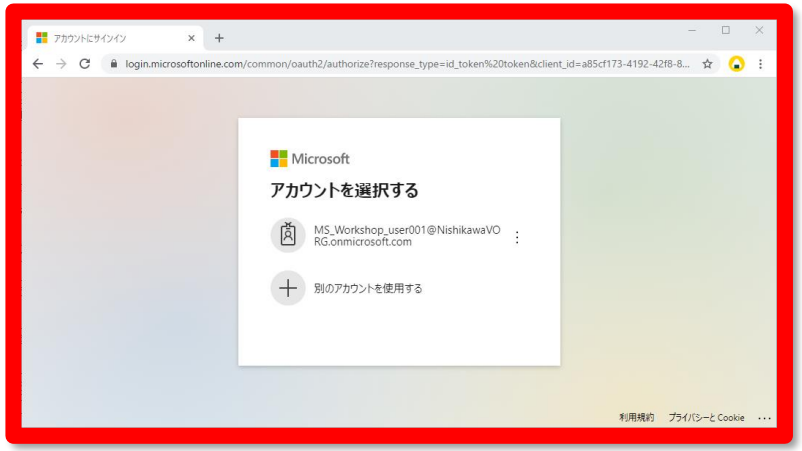
Point 6
ネットワークセキュリティを強靭にするには

Azure ADとActive Directoryは同期が必要

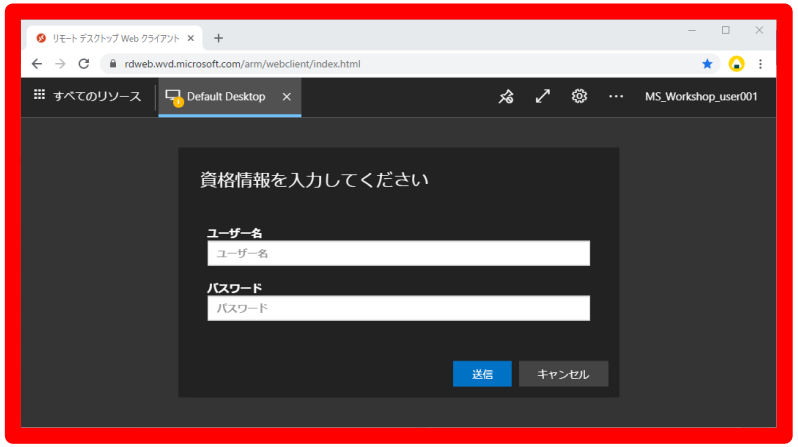


WVDではAzure ADとActive Directoryが必要

1. Azure AD 認証



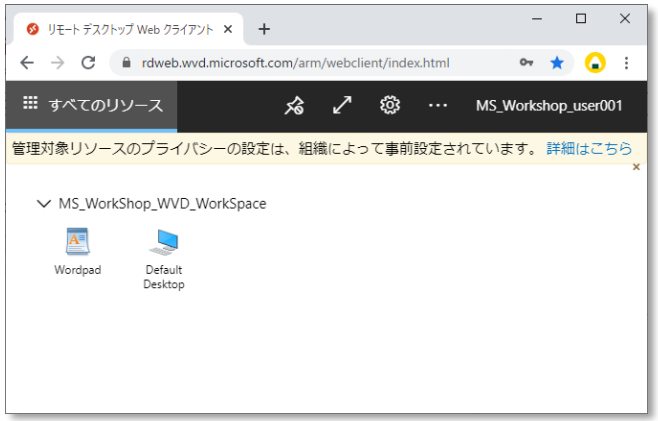
3. AD 認証



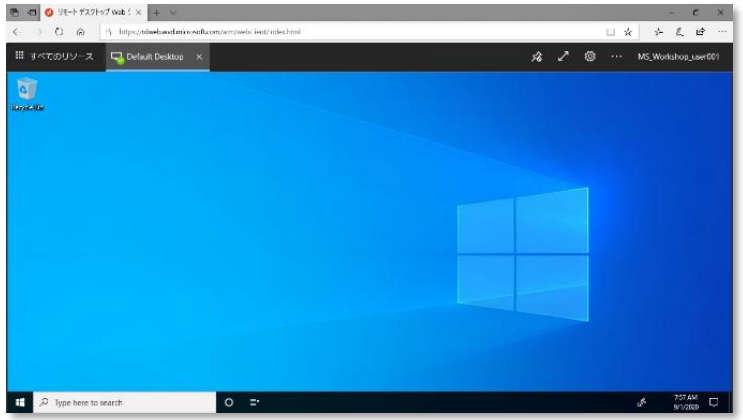
RD Web Client

接続フロー

2.フィード取得

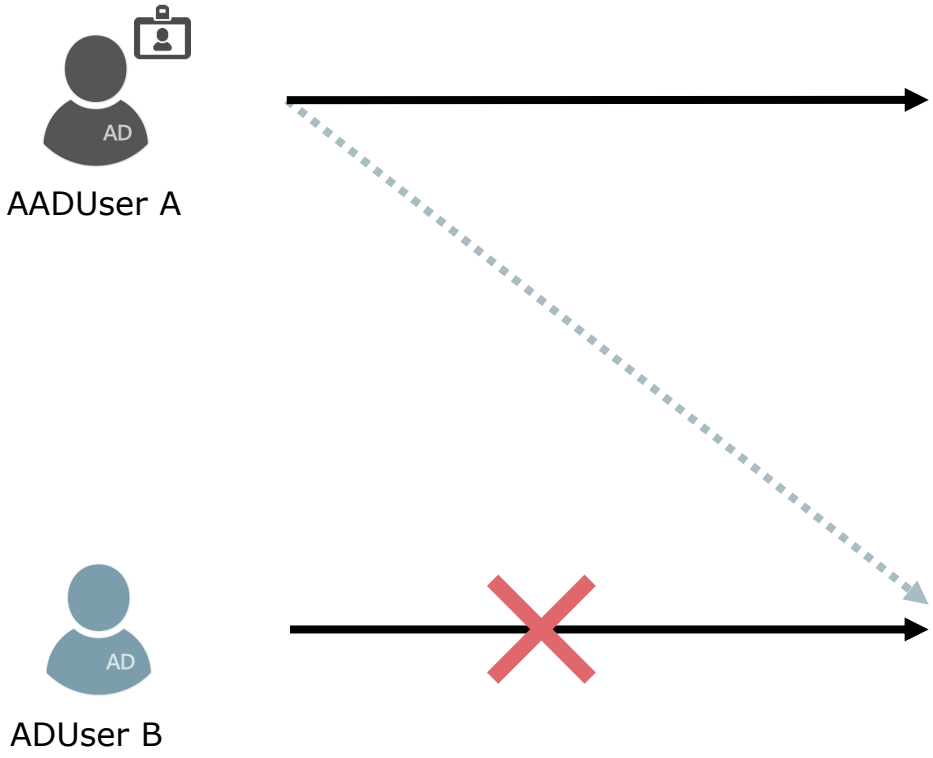


4.リモートデスクトップ接続

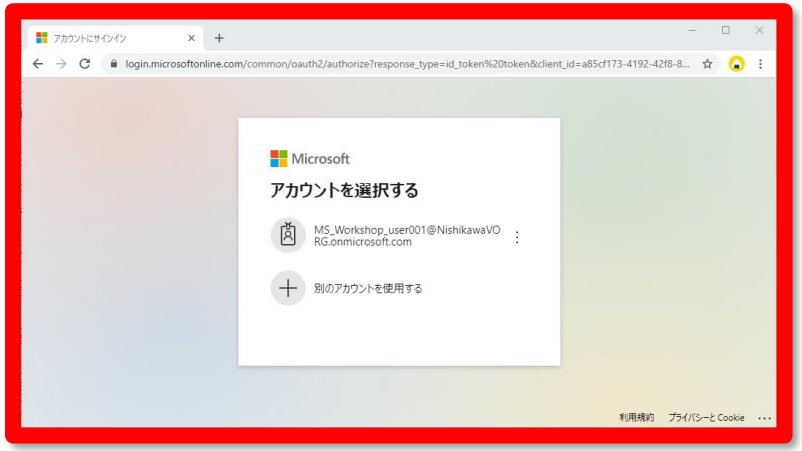


https://rdweb.wvd.microsoft.com/arm/webclient/index.html

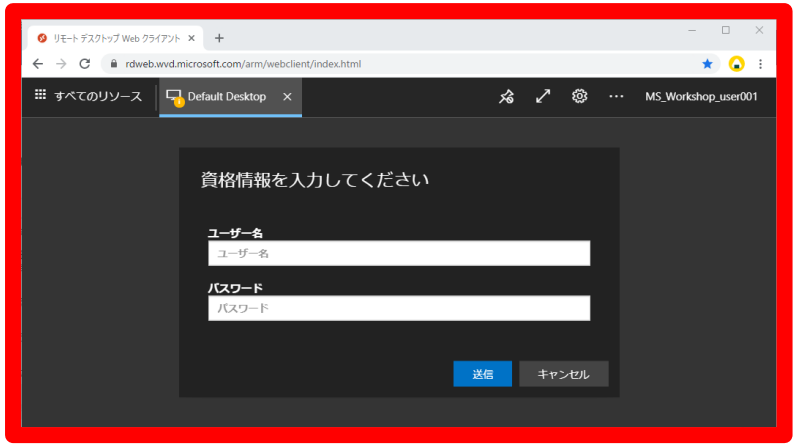
Azure ADとActive Directoryは同期が必要



1. Azure AD 認証



3. AD 認証



Azure ADとADの認証を別ユーザーで実施
→ システム上可能ですが、ライセンス違反 となる場合があります。

Windows 10 ライセンス

導入前に抑えておきたいポイント

Point 1
VDIにインストールするアプリケーションの注意点

Point 2
Azure ADとActive Directoryの関係性

Point 3
ライセンスの種類

Point 4
既にAzureを利用している場合の注意点

Point 5
ネットワークの閉域化は一部のみ

Point 6
ネットワークセキュリティを強靭にするには

ライセンス一覧

対応OS（2020年10月現在）

OS	必要なライセンス（ユーザー単位）
・Windows 10 Enterprise multi-session ・Windows 10 Enterprise ・Windows 7	・Microsoft 365 E3/E5 ・Microsoft 365 A3/A5/Student Use Benefits ・Microsoft 365 F3 ・Microsoft 365 Business Premium ・Windows 10 Enterprise E3/E5 ・Windows 10 Education A3/A5 ・Windows 10 VDA per user
・Windows Server 2012 R2 ・Windows Server 2016 ・Windows Server 2019	・RDS Client Access License (CAL) with Software Assurance

Windows 10 Pro 未満デバイスからの接続可否

対象OS：Windows 10 Enterprise multi session, Windows 10 Enterprise, Windows 7

ライセンス名	Windows 10 Pro 未満デバイスからの接続可否
Microsoft 365 E3/E5	アクセス可能
Microsoft 365 A3/A5/Student Use Benefits	アクセス可能
Microsoft 365 F3	アクセス可能
Microsoft 365 Business Premium	アクセス可能
Windows 10 Enterprise E3/E5	特定の条件を満たせばアクセス可能
Windows 10 Education A3/A5	特定の条件を満たせばアクセス可能
Windows 10 VDA	アクセス可能

特定の条件

- Windows 10 Pro 以上の環境がWVDを利用するユーザーの手元にあり、且つ Windows 10 Pro の環境が主要な使用環境であること

  主要なユーザーであるかの判断基準（例）

  下記の2つの条件を満たした場合に主要なユーザーとして認められます。

  1. 対象のユーザーは、個人業務用として Windows 10 Pro 以上の OS が搭載されたデバイスを割り当てられている
  2. 主要な業務用デバイスとして Windows 10 Pro デバイスを使用していること
     (ex.日常業務を Windows 10 pro デバイス 40% iOS デバイス 30% / Android デバイス 30% の割合で業務を行っているため、主要な業務は Windows 10 Pro デバイスで行っていると判断できること)

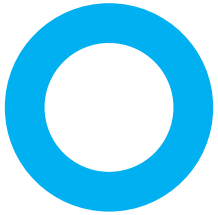
必要ユーザーライセンス数の考え方

同時接続ユーザー数：５人

必要ライセンス数は５個？

利用ユーザー数：１０人

利用ユーザー数分必要
最大同時接続数ユーザー5人で
もライセンスは10個必要



各ライセンスの比較 1/2

提供サービス名 ＼ ライセンス名		Microsoft 365 Enterprise		Windows 10 Enterprise	
		E3	E5	E3	E5
Windows 10 Enterprise	Windows 10 Enterprise	○	○	○	○
	Microsoft Defender Advances Threat Protection	-	○	-	○
Enterprise Mobility + Security	Azure AD Premium P1	○	○	-	-
	Azure AD Premium P2	-	○	-	-
	Azure Advances Threat Protection	-	○	-	-
	Cloud App Security Discovery	○	○	-	-
	Microsoft Azure Multi-Factor Authentication	○	○	-	-
	Microsoft Intune	○	○	-	-

各ライセンスの比較 2/2

提供サービス名 ＼ ライセンス名		Microsoft 365 Enterprise		Windows 10 Enterprise	
		E3	E5	E3	E5
Office 365	Applications	○	○	-	-
	Microsoft Defender for Office 365 P2	-	○	-	-
	Microsoft Cloud App Security	-	○	-	-

各ライセンスの料金比較

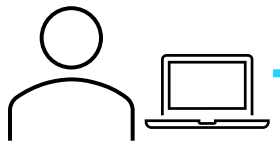
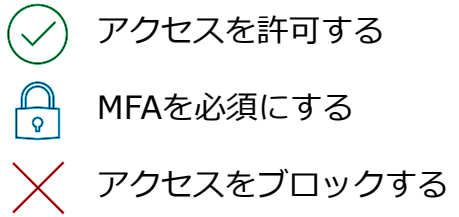
ライセンス名	月額料金(ユーザー単位)	備考
Microsoft 365 Enterprise E3	¥3,480/月	各E3 (Win10,EMS,Office) とVDAライセンスを包含
Microsoft 365 Enterprise E5	¥6,200/月	各E5(Win10,EMS,Office) とVDAライセンスを包含
Windows 10 Enterprise E3	¥760/月	VDAは含みません
Windows 10 Enterprise E5	¥1,200/月	VDAは含みません
Windows 10 VDA E3	¥1,430/月	VDAを含みます
Enterprise Mobility + Security E3	¥960/月	-
Enterprise Mobility + Security E5	¥1,610/月	-
Office 365 E3	¥2,170/月	-
Office 365 E5	¥3,180/月	-

M365 E3ライセンスに関するセキュリティ

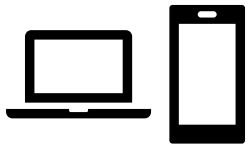
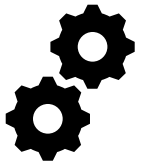
条件付きアクセス(Azure AD Premium P1)

- 条件に基づいたアクセス制御

■ 認証のプロセス

認証(第一段階)		認証 (第二段階)	
Azure ADへ接続	資格情報入力	シグナル検出	条件付きアクセス適用
			

■ シグナルの種類 

デバイス	ユーザー	場所	アプリ
			

M365 E5ライセンスに関するセキュリティ

Microsoft Defender（Advance Threat Protection）

- クラウドベースの電子メール フィルタリング サービス
- マルウェアやウイルスから組織を保護

脅威保護ポリシー

自動調査及び対応機能

レポート

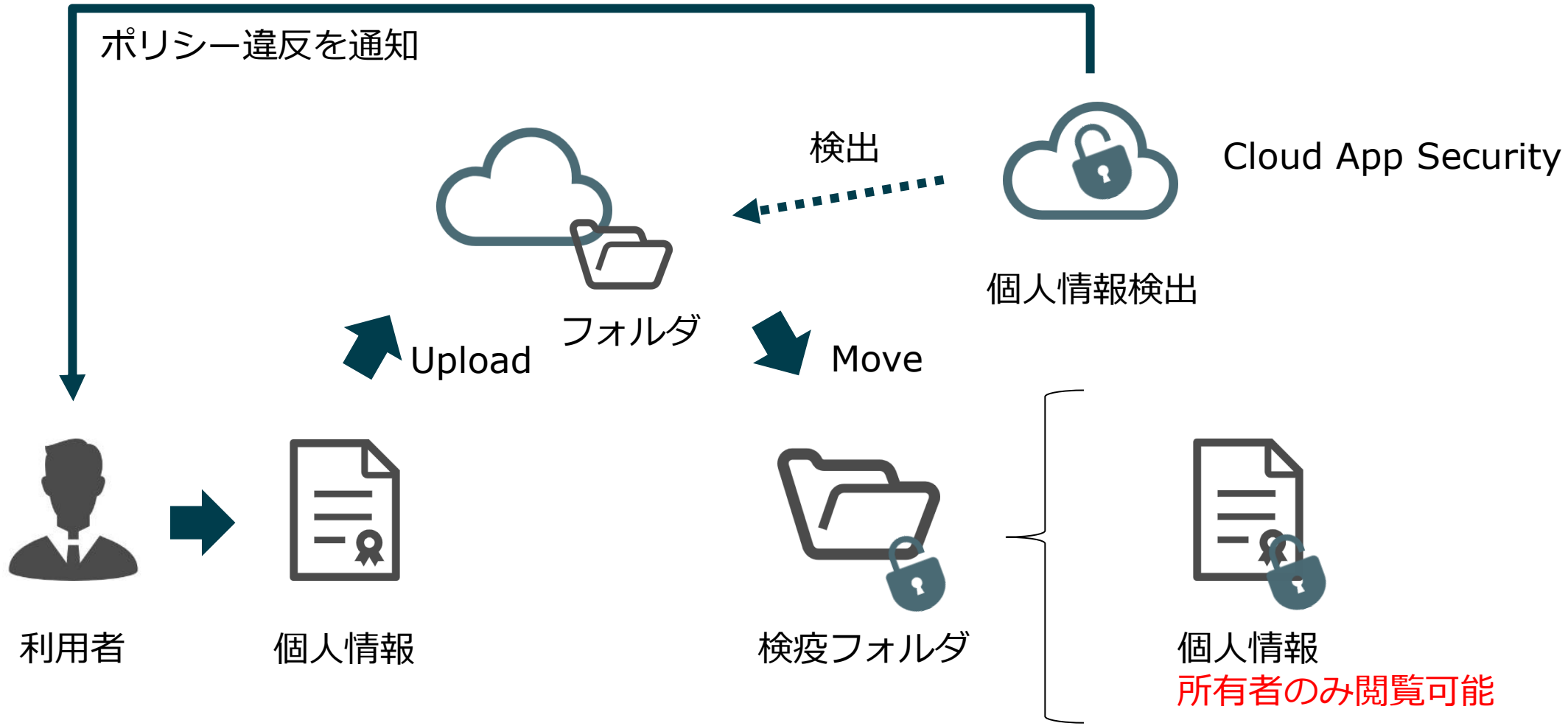
驚異の調査及び反応機能

※ただしWindows 10 Multisession OSではPublic Previewとなります

M365 E5ライセンスに関するセキュリティ

Cloud App Security

- 社内情報や個人情報等の機密情報を検知し、自動で保護



導入前に抑えておきたいポイント

Point 1
VDIにインストールするアプリケーションの注意点

Point 2
Azure ADとActive Directoryの関係性

Point 3
ライセンスの種類

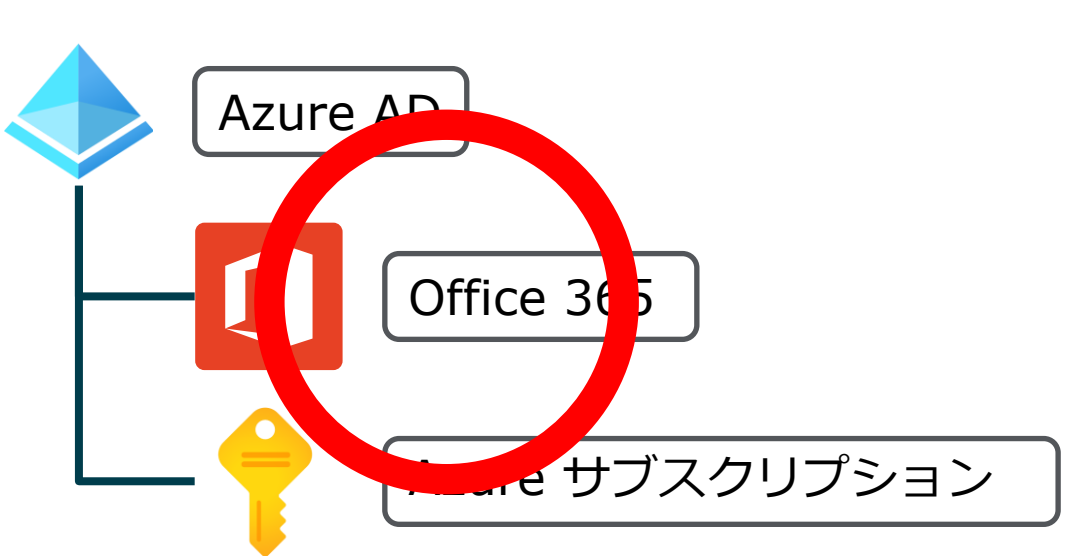
Point 4
既にAzureを利用している場合の注意点

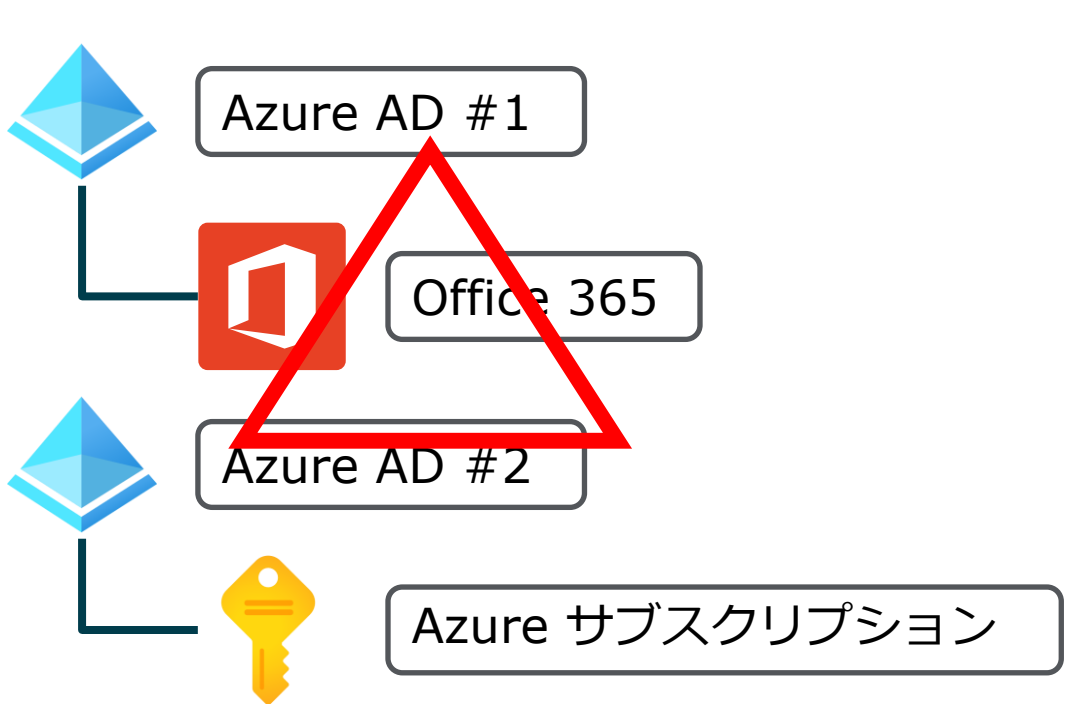
Point 5
ネットワークの閉域化は一部のみ

Point 6
ネットワークセキュリティを強靭にするには

Azure ADは複数存在しませんか？

検証利用などの用途を除いて、基本的にはAzure ADは1つであることが望ましいです。
Office 365を利用している場合は、同じAzure ADにサブスクリプションを紐づけましょう。
※Azure ADが複数存在する場合にはご相談ください。





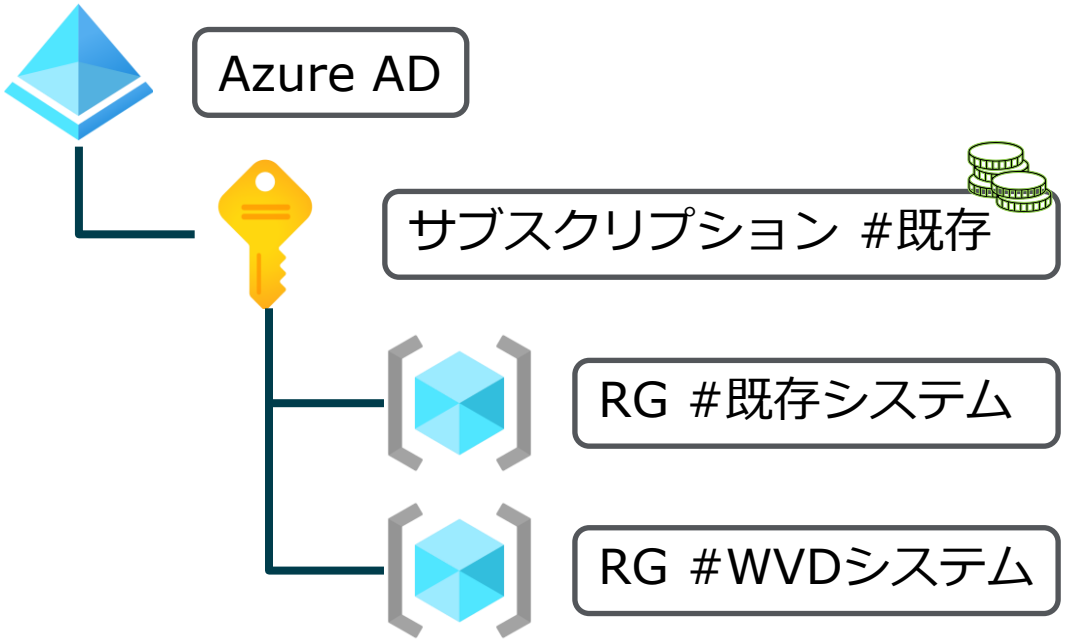
■複数のAzure ADを推奨しない理由

- Office 365とAzureサブスクリプションで別々にユーザー管理をしなければならないから
- ユーザーのライセンスはAzure ADに紐づいているから

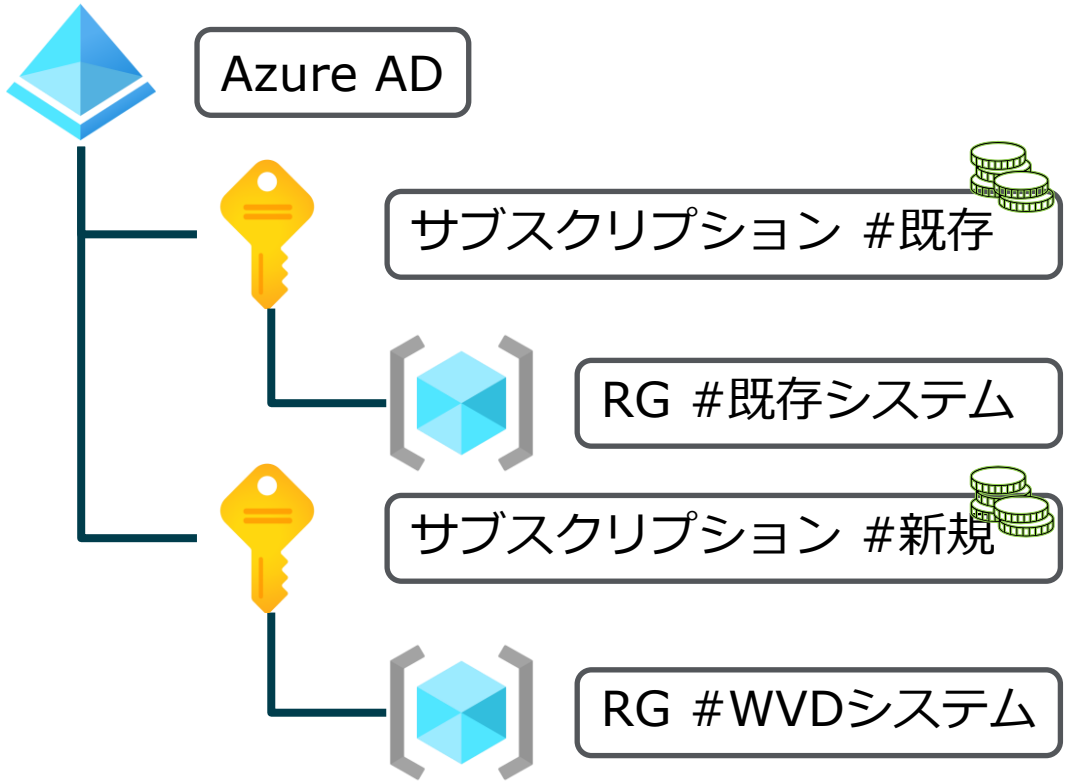
既存のサブスクリプションに対してWVDリソースを追加していいですか？

Azure サブスクリプションはリソースの論理グループであると同時に、課金の請求単位です。
既存のサブスクリプションにWVDを構築した場合、請求は既存のシステムと合算されます。

同一のサブスクリプションを利用した場合
・既存システムとWVDシステムの請求が合算



別々のサブスクリプションを利用した場合
・既存システムとWVDシステムの請求は別々

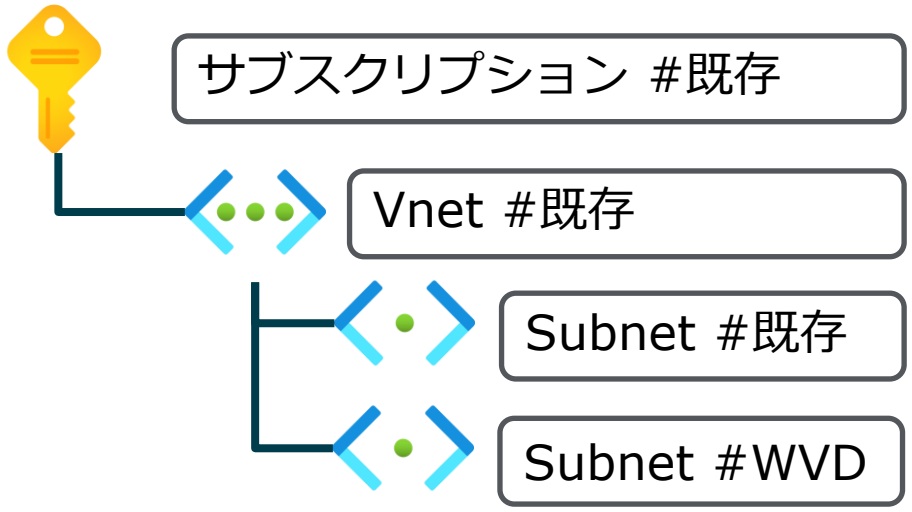


（補足）既存のサブスクリプションに対してWVDリソースを追加していいですか？

仮想ネットワーク(Vnet)はサブスクリプションのスコープであるため、異なるサブスクリプションのVnetと通信するにはピアリングを構成する必要があります。※ピアリングは有料です。

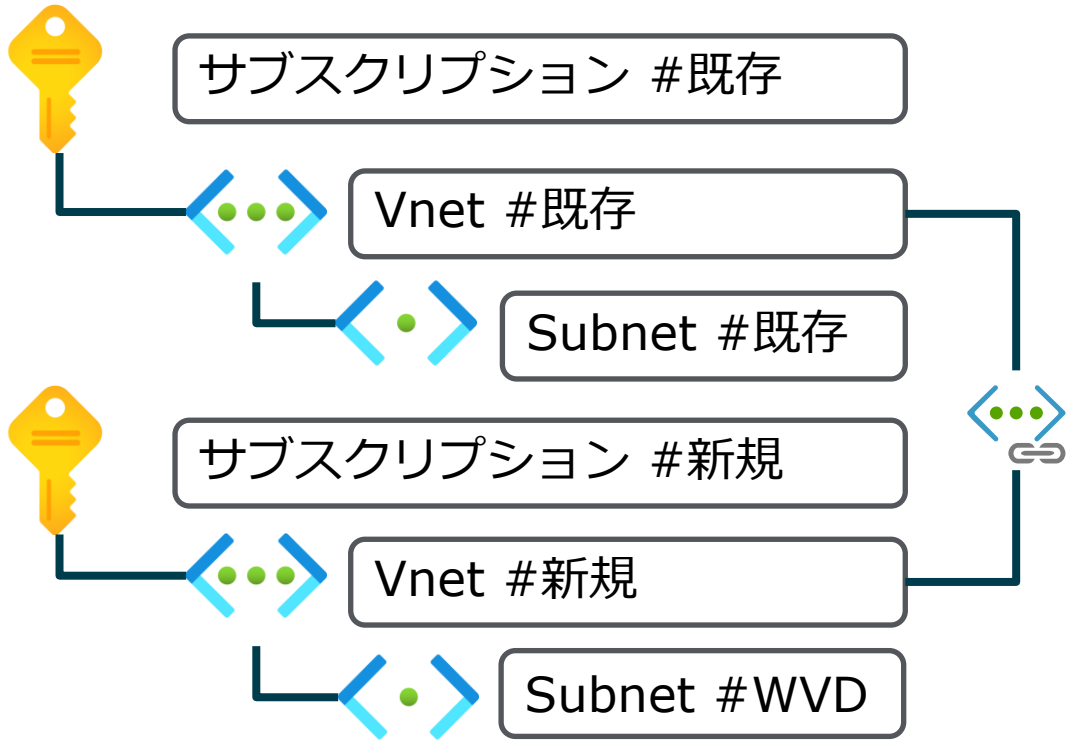
同一のサブスクリプションを利用した場合

・既存のVnetにWVDサブネットを追加



別々のサブスクリプションを利用した場合

・新規にVnetを作成しピアリングを構成



WVDのネットワーク要件を満たしていますか？

セッションホスト（Azure VM）を展開する仮想ネットワークから、以下に示すエンドポイントにアクセスできる必要があります。

必須/任意	Address	Outbound TCP port	Purpose	Service Tag
必須	*.wvd.microsoft.com	443	Service traffic	WindowsVirtualDesktop
必須	mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS stack updates	AzureCloud
必須	*.core.windows.net	443	Agent traffic	AzureCloud
必須	*.servicebus.windows.net	443	Agent traffic	AzureCloud
必須	gcs.prod.monitoring.core.windows.net	443	Agent traffic	AzureCloud
必須	catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
必須	kms.core.windows.net	1688	Windows activation	Internet
必須	wvdportalstorageblob.blob.core.windows.net	443	Azure portal support	AzureCloud
必須	169.254.169.254	80	Azure Instance Metadata service endpoint	N/A
必須	168.63.129.16	80	Session host health monitoring	N/A
任意	*.microsoftonline.com	443	Authentication to Microsoft Online Services	None
任意	*.events.data.microsoft.com	443	Telemetry Service	None
任意	www.msftconnecttest.com	443	Detects if the OS is connected to the internet	None
任意	*.prod.do.dsp.mp.microsoft.com	443	Windows Update	None
任意	login.windows.net	443	Sign in to Microsoft Online Services, Microsoft 365	None
任意	*.sfx.ms	443	Updates for OneDrive client software	None
任意	*.digicert.com	443	Certificate revocation check	None

参考：https://docs.microsoft.com/en-us/azure/virtual-desktop/safe-url-list


只今、休憩時間です。
再開はHH:MMを予定しています。

導入前に抑えておきたいポイント

Point 1
VDIにインストールするアプリケーションの注意点

Point 2
Azure ADとActive Directoryの関係性

Point 3
ライセンスの種類

Point 4
既にAzureを利用している場合の注意点

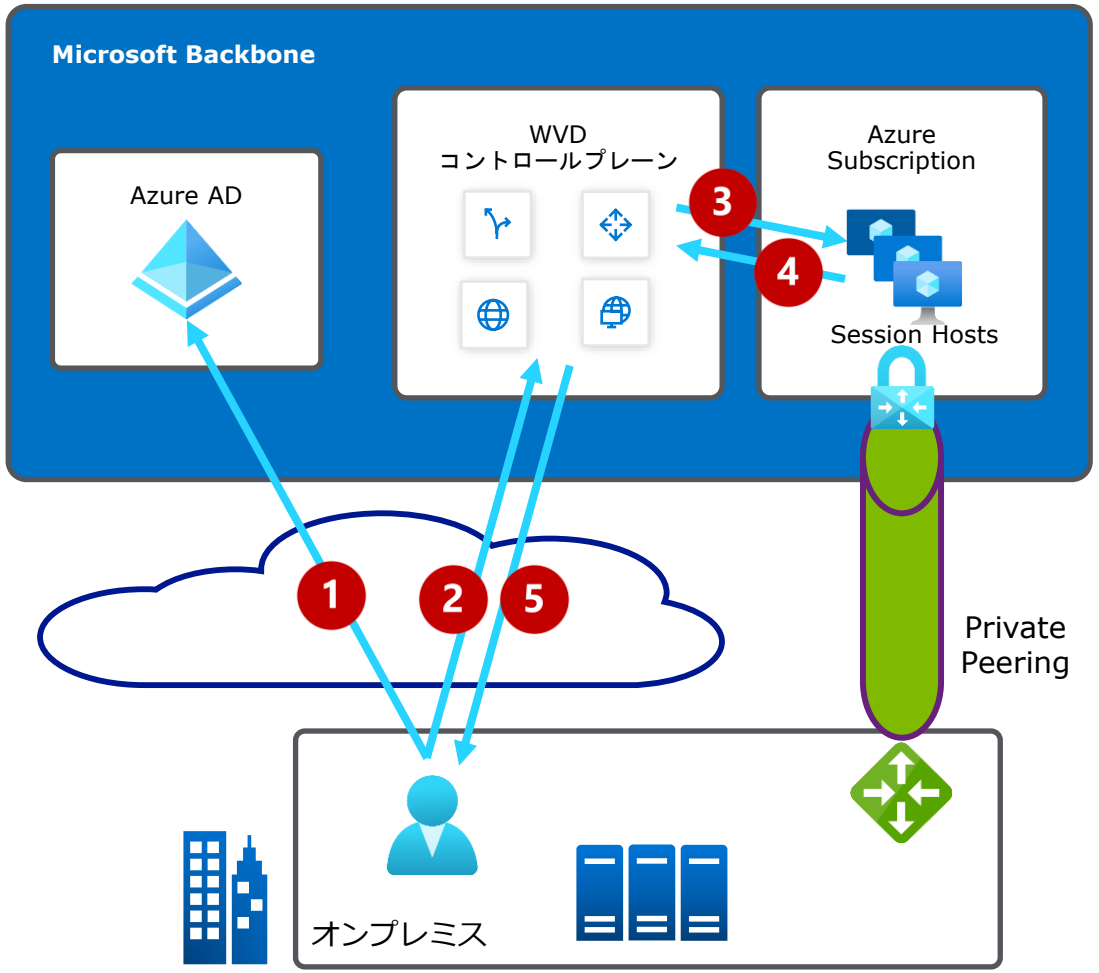
Point 5
ネットワークの閉域化は一部のみ

Point 6
ネットワークセキュリティを強靭にするには

オンプレミスとの接続経路 – ネットワークの閉域化

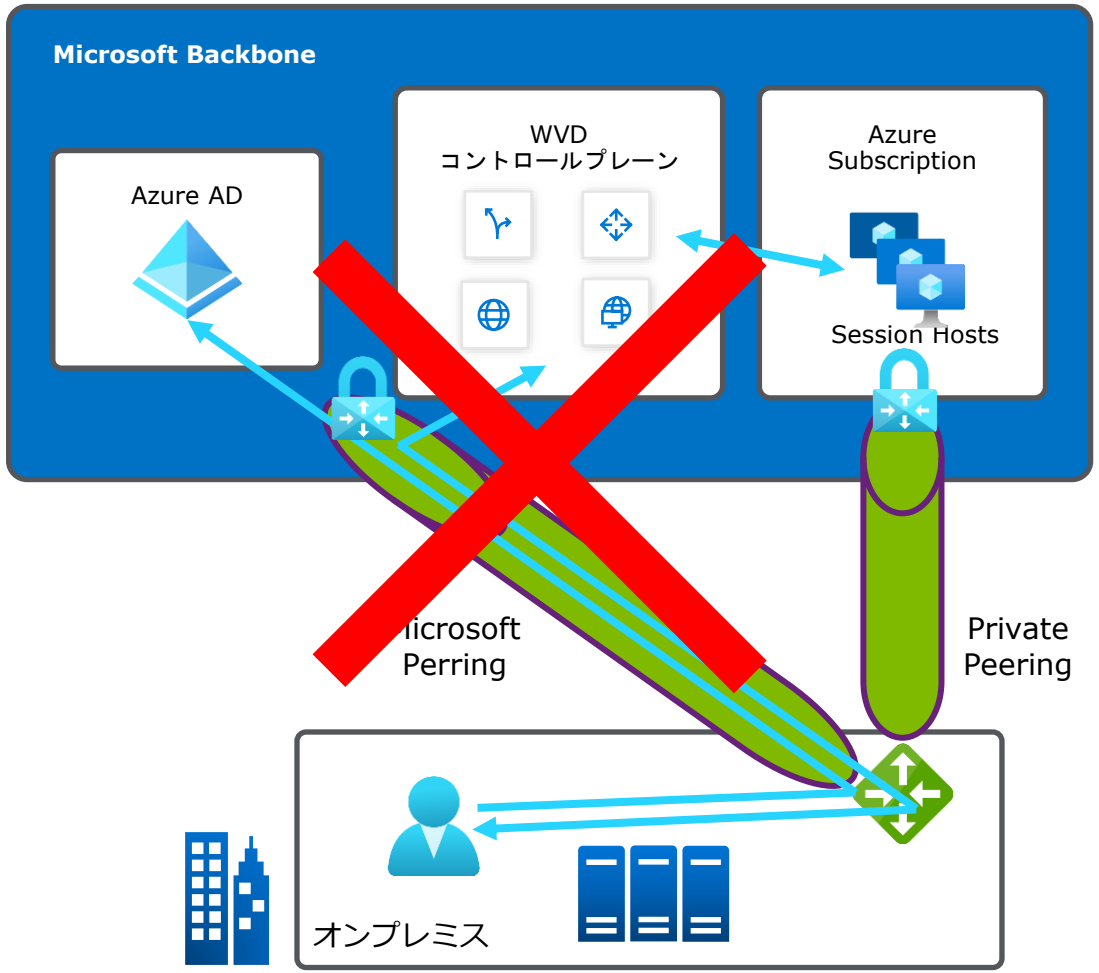
Native WVDではインターネットを経由した通信が前提となる

・Azure AD認証（インターネット）
・WVDコントロールプレーンを経由する画面転送（インターネット）



WVDではMicrosoft Peeringのサポート対象外

・Azure AD認証（Express Route）
・WVDコントロールプレーンを経由する画面転送(Express Route)

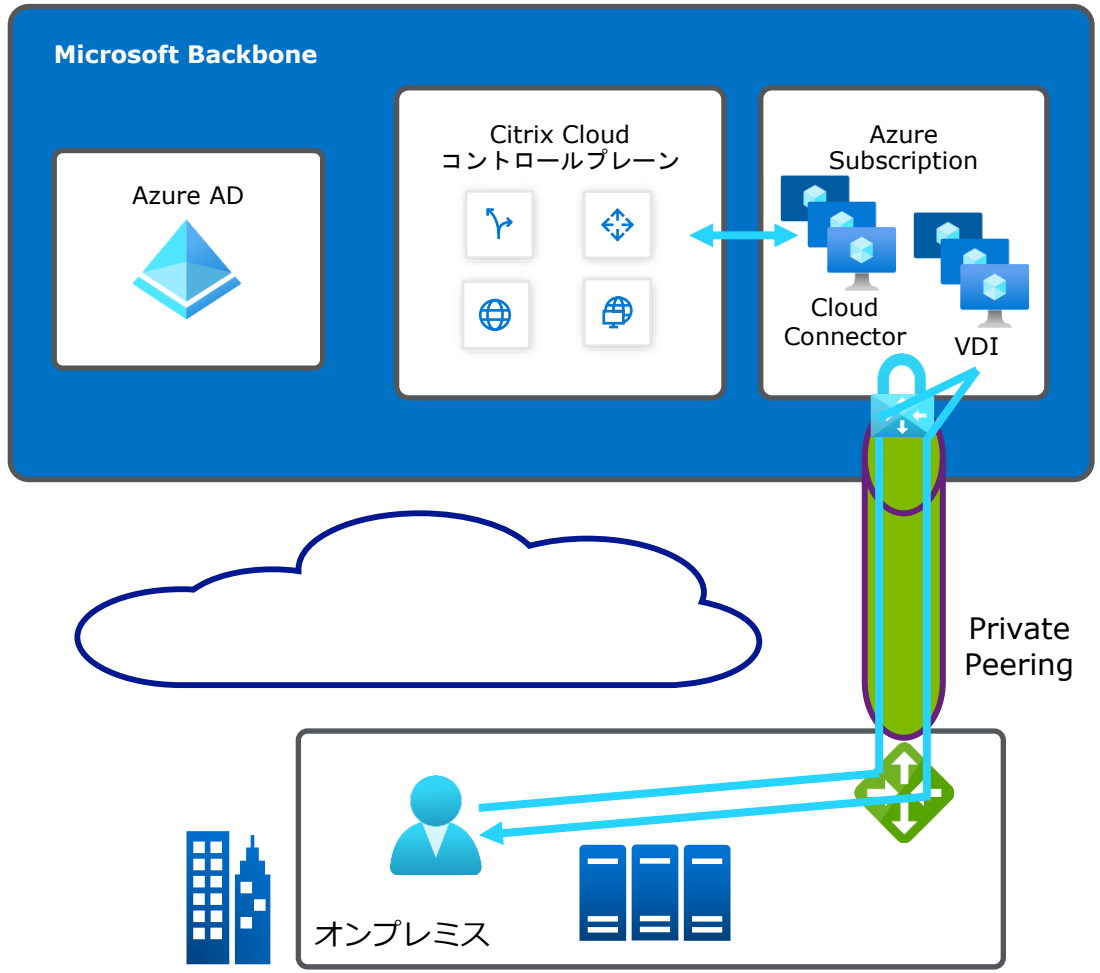


オンプレミスとの接続経路 – ネットワークの完全閉域化

画面転送情報なども含めて全て閉域化する場合はCitrix Cloudとの組み合わせが必要

・Azure AD認証 ⇒**オプション。必須ではない**

・画面転送情報は**コントロールプレーンを経由しない**



導入前に抑えておきたいポイント

Point 1
VDIにインストールするアプリケーションの注意点

Point 2
Azure ADとActive Directoryの関係性

Point 3
ライセンスの種類

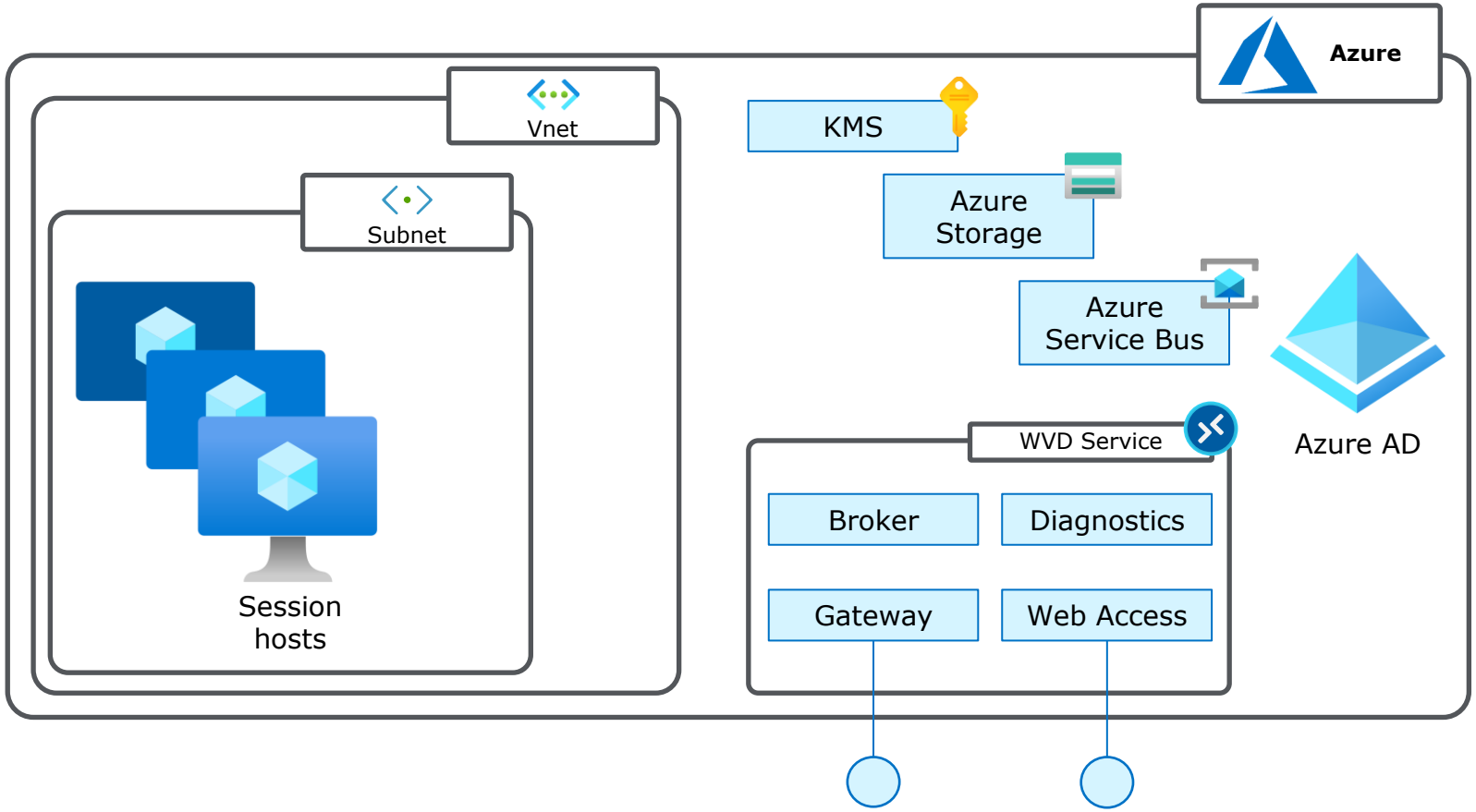
Point 4
既にAzureを利用している場合の注意点

Point 5
ネットワークの閉域化は一部のみ

Point 6
ネットワークセキュリティを強靭にするには

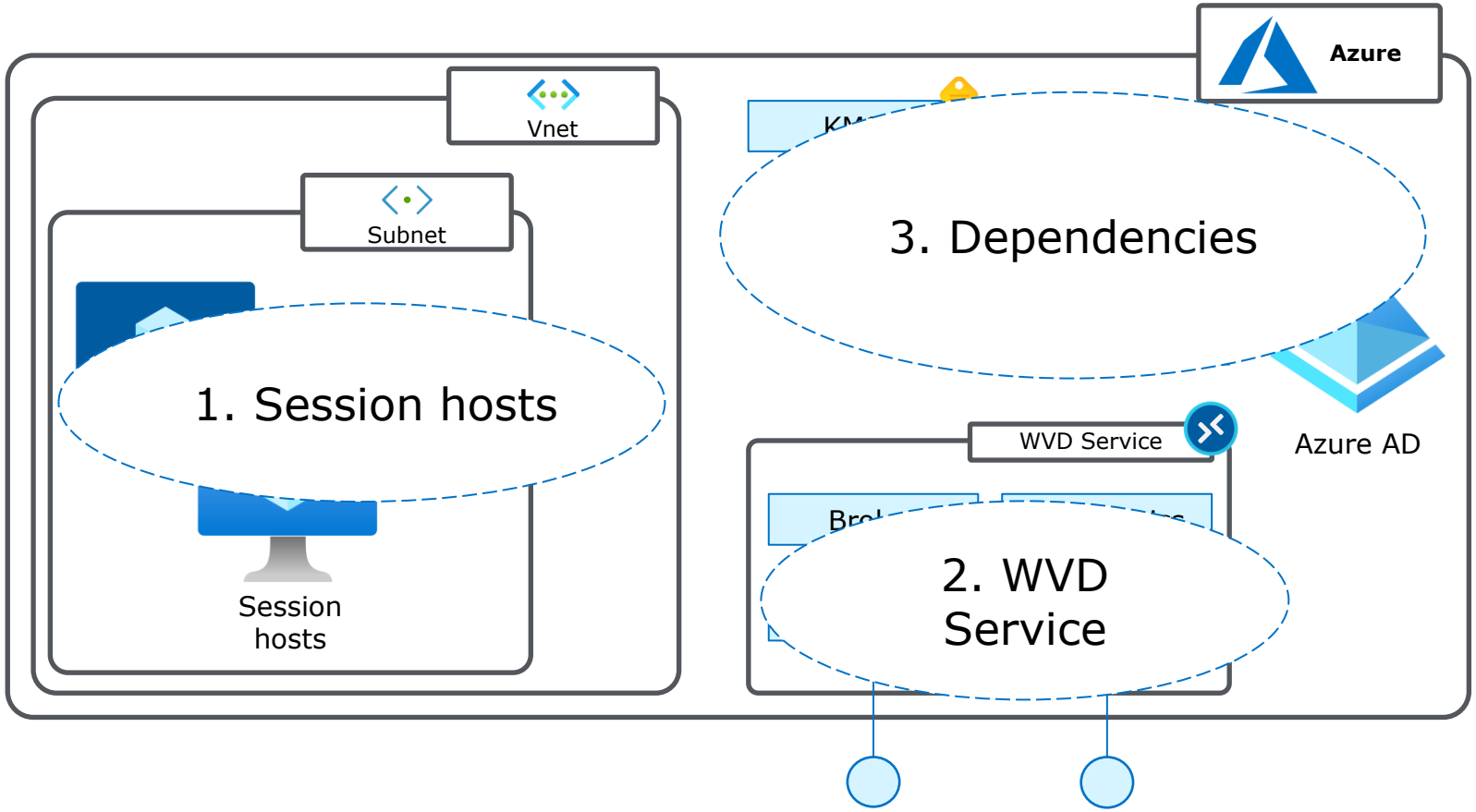
WVD ネットワーク アーキテクチャ – 概要

アーキテクチャ コンポーネント
1. Session hosts
2. WVD Service
3. Dependencies



WVD ネットワーク アーキテクチャ – 概要

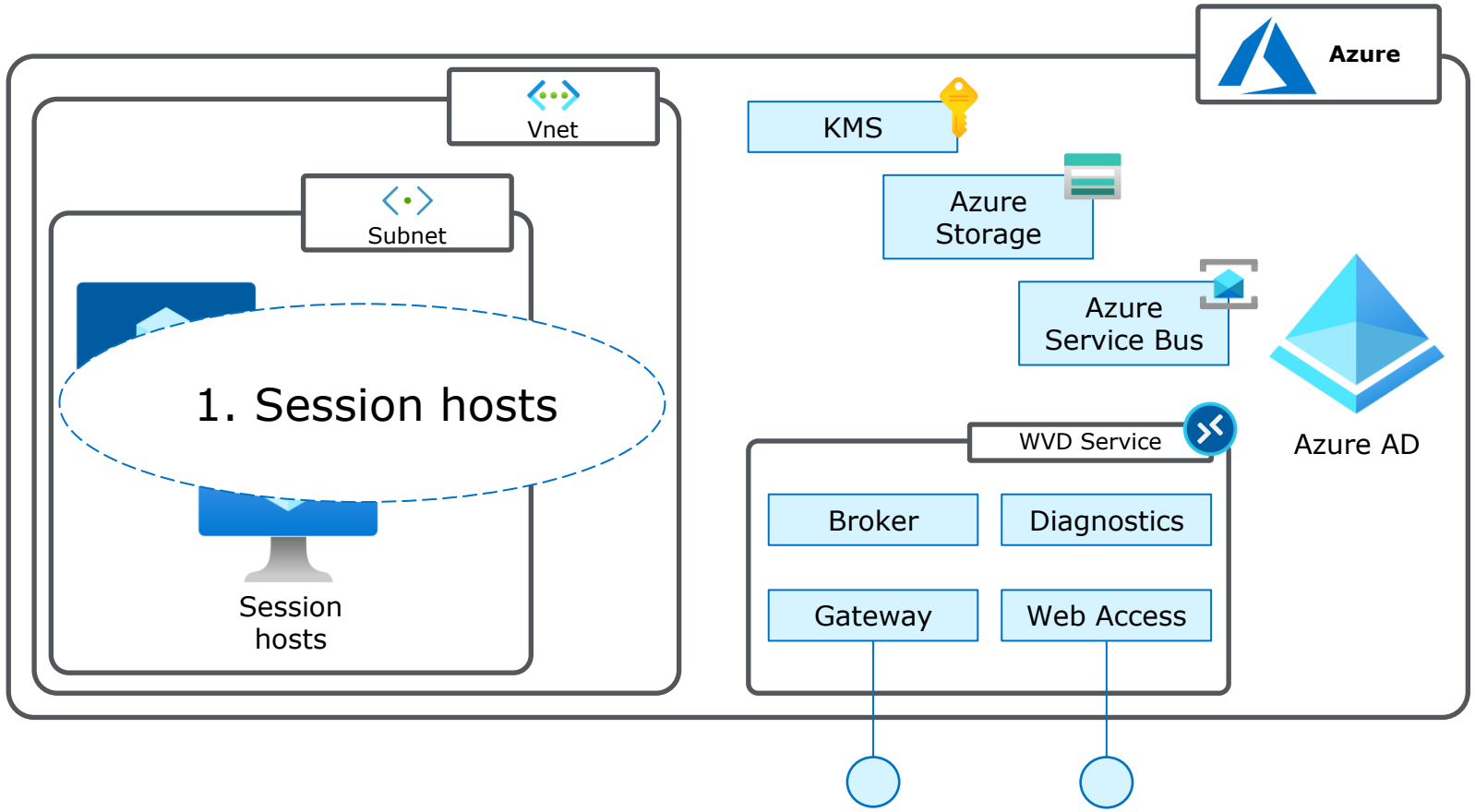
アーキテクチャ コンポーネント
1. Session hosts
2. WVD Service
3. Dependencies



WVD ネットワーク アーキテクチャ – セッションホスト

Session hosts

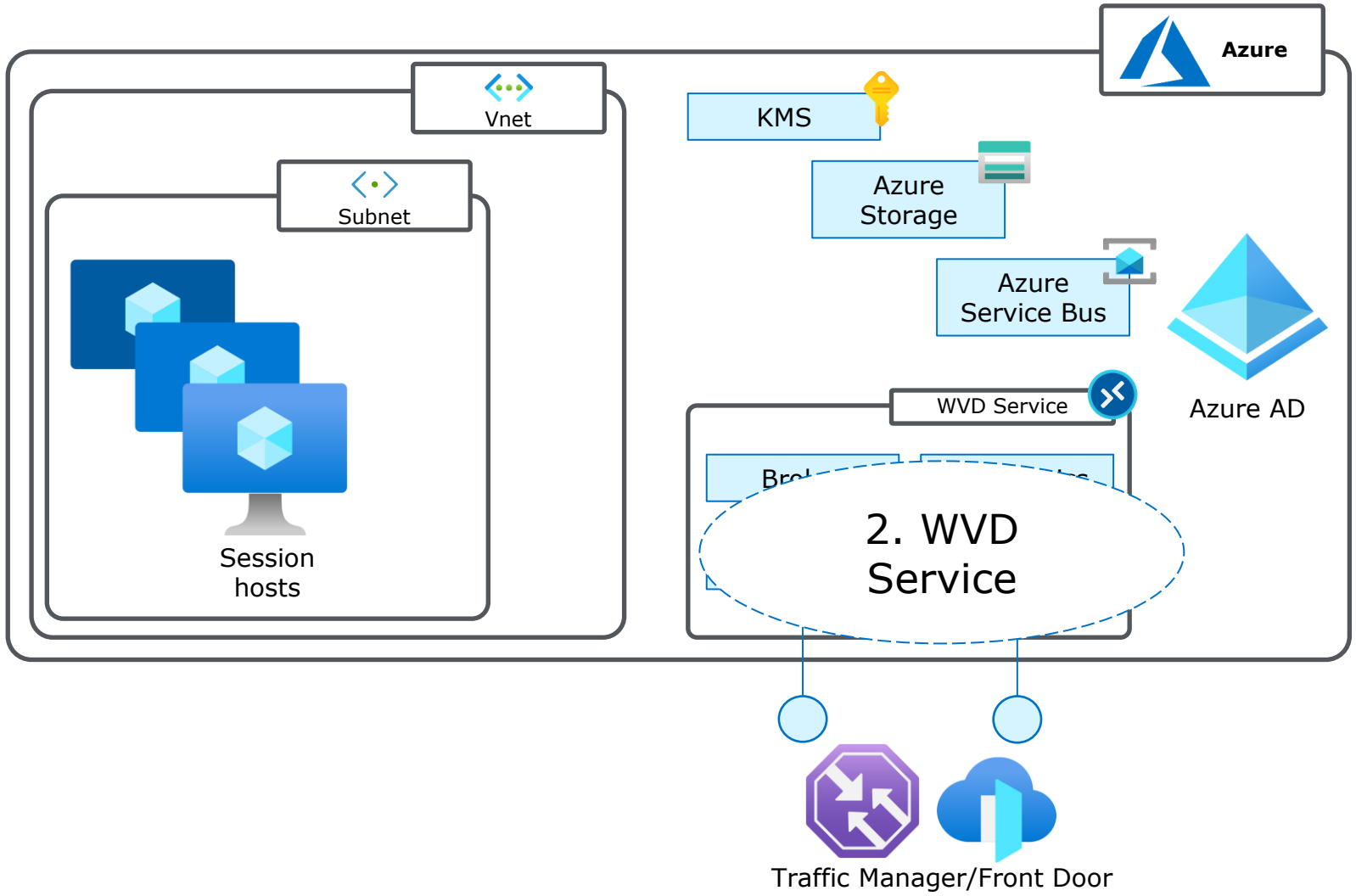
- セッションホストの仮想マシンはお客様が管理する仮想ネットワーク上に展開する。
- それぞれのセッションホストにはWVDのエージェントを構成する。
- 異なる複数のAzureリージョンでセッションホストを稼働させることは可能です。



WVD ネットワーク アーキテクチャ – WVDサービス

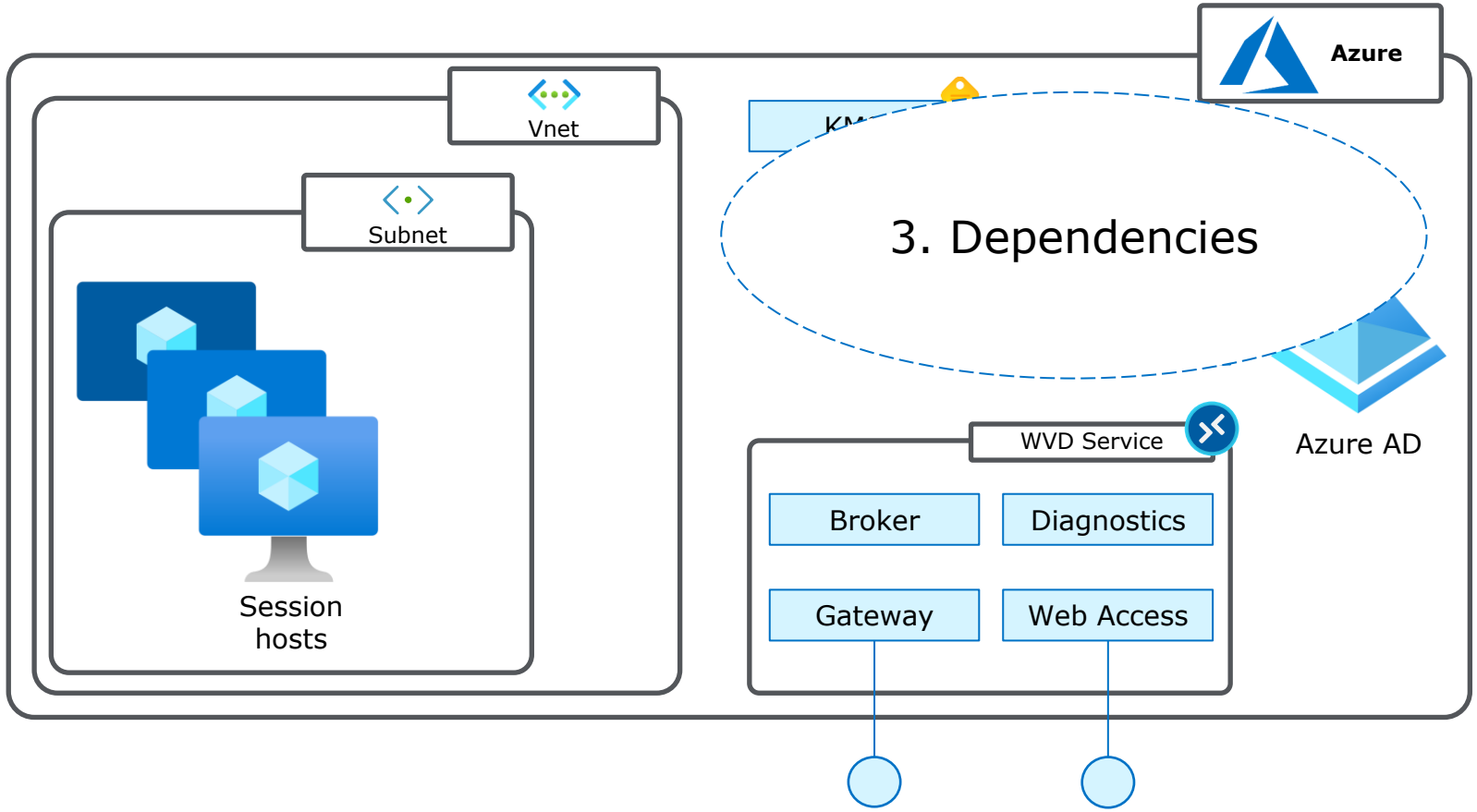
WVD Service

- WVDコントロール プレーンはマイクロソフトが管理する。
- WVD GatewayとBrokerは外部から到達可能なエンドポイントとして、インターネットに公開されます。
- WVD GatewayとBrokerの前にはTraffic Managerが存在します。（Front Doorへ移行中）



WVD ネットワーク アーキテクチャ – 依存コンポーネント

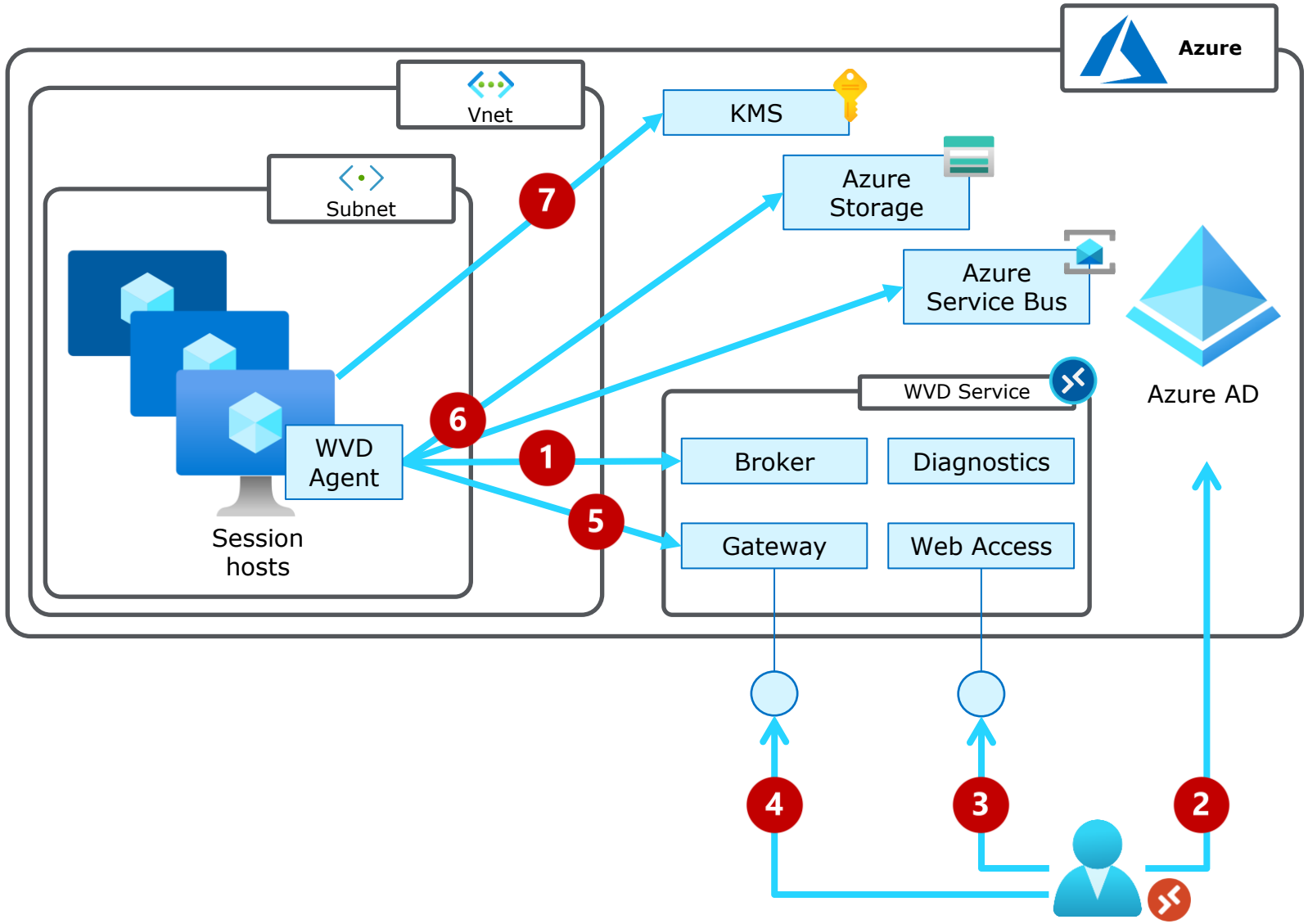
Dependencies
- KMS(Windows Activation)
- Azureサービス(Storage, Service Bus, Log Analytics, etc..)
- Azure Marketplace
- Windows Update
- WVD GatewayとBrokerはAzure AD認証によって保護されている。



WVD ネットワーク アーキテクチャ – 接続フロー

接続フロー

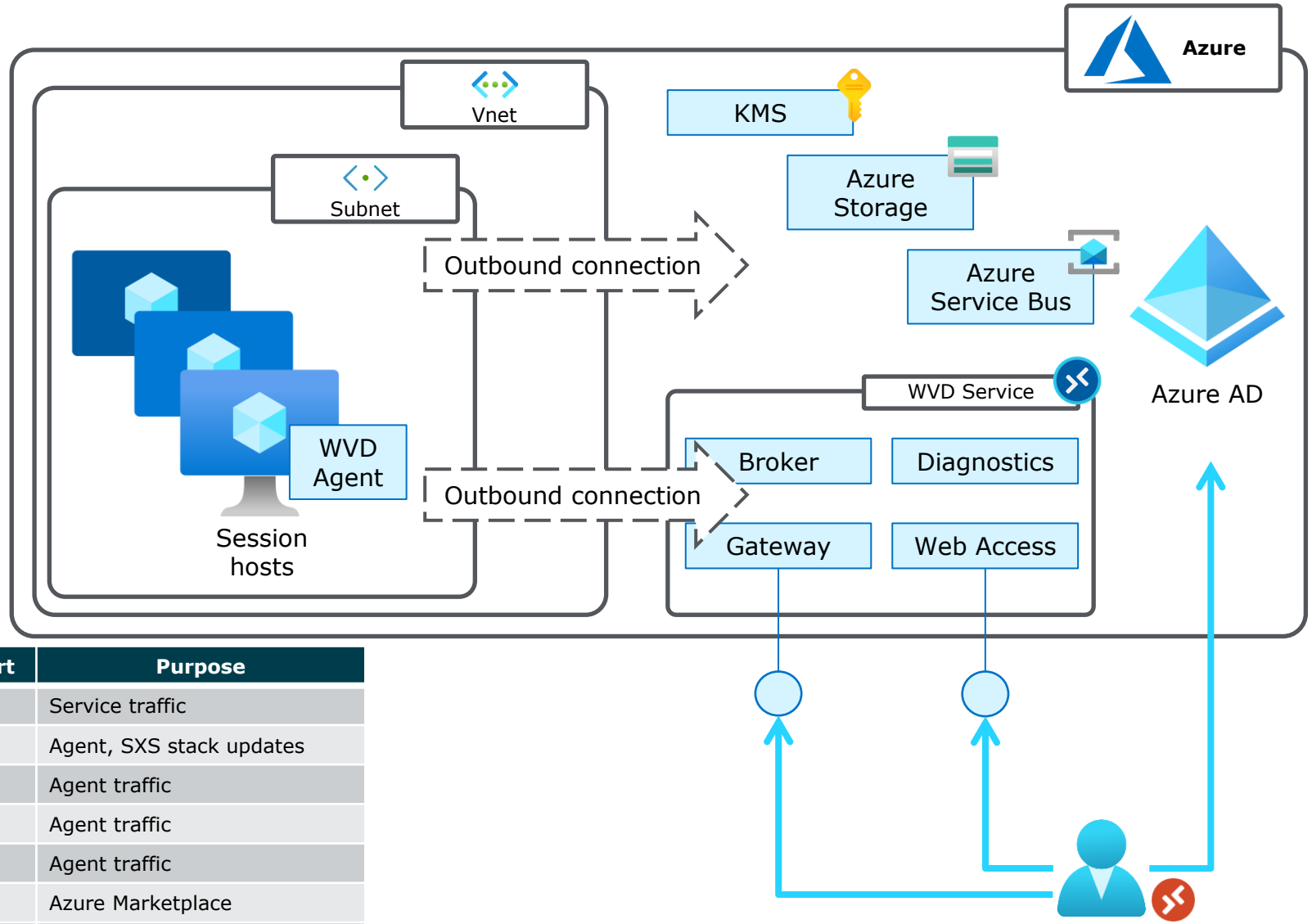
1. AgentをBrokerに登録（初回のみ）
2. Remote Desktop Clientを起動し、Azure AD認証
3. Web Accessからfeedを取得し、Application Groupを選択
4. Remote Desktop ClientがGatewayと通信する
5. BrokerがWVD AgentとGatewayを接続する
6. WVD Agentが外部サービスと通信する（Storage, Service Bus, …）
7. Session hostが外部サービスと通信する（例: KMS）



WVD ネットワーク アーキテクチャ – Session hostのネットワーク要件

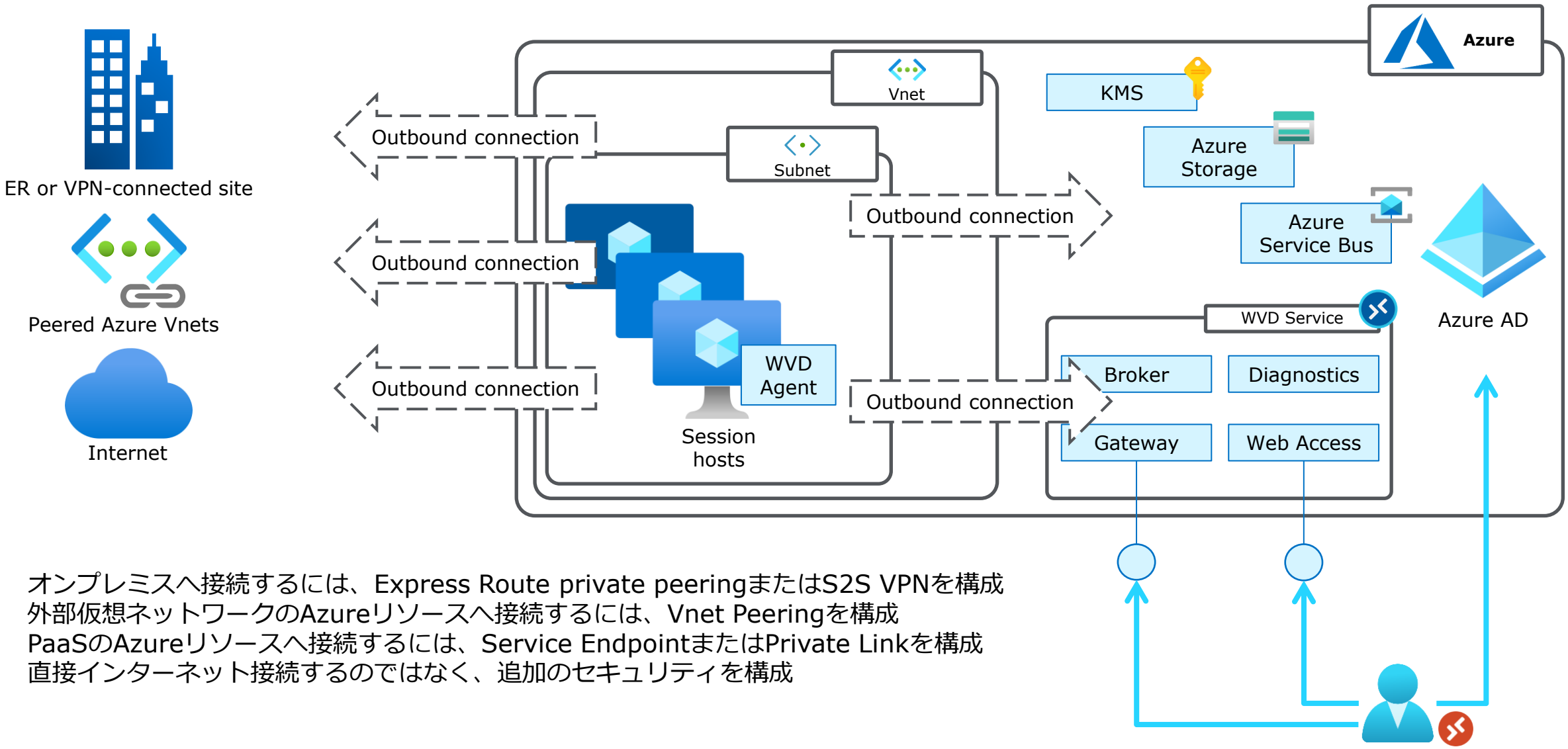
お客様が管理する仮想ネットワークから公開されるエンドポイントはありません

- Session hostにPublic IP不要
- WVD AgentはWVD Serviceと依存関係にあるその他サービスとの通信必須
  https://docs.microsoft.com/en-us/azure/virtual-desktop/safe-url-list
  ※以下に示す表は一部です。



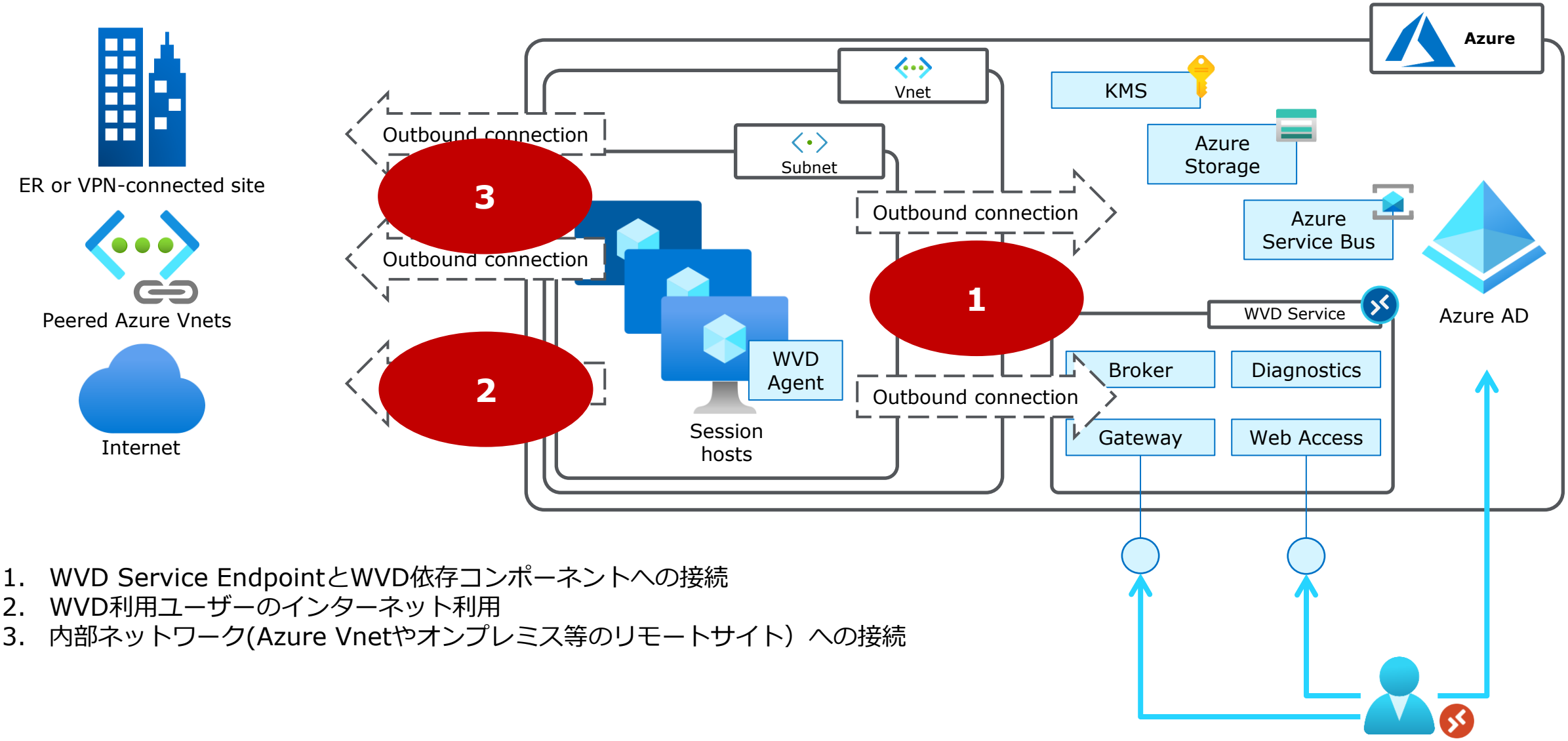
Required dependency	Protocol/port	Purpose
*.wvd.microsoft.com	TCP port 443	Service traffic
mrsglobalsteus2prod.blob.core.windows.net	TCP port 443	Agent, SXS stack updates
*.core.windows.net	TCP port 443	Agent traffic
*.servicebus.windows.net	TCP port 443	Agent traffic
prod.warmpath.msftcloudes.com	TCP port 443	Agent traffic
catalogartifact.azureedge.net	TCP port 443	Azure Marketplace
kms.core.windows.net	TCP port 1688	Windows 10 activation

WVD ネットワーク アーキテクチャ – 追加のネットワーク要件（オプション）



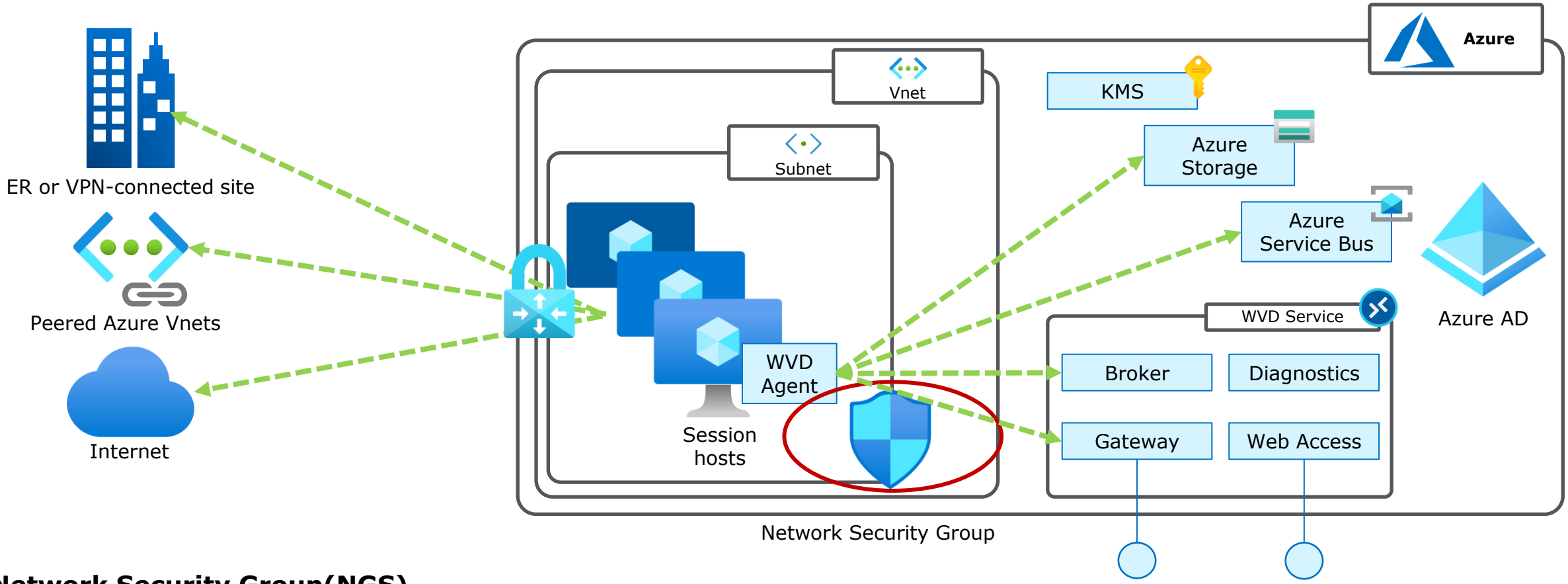
- オンプレミスへ接続するには、Express Route private peeringまたはS2S VPNを構成
- 外部仮想ネットワークのAzureリソースへ接続するには、Vnet Peeringを構成
- PaaSのAzureリソースへ接続するには、Service EndpointまたはPrivate Linkを構成
- 直接インターネット接続するのではなく、追加のセキュリティを構成

WVD ネットワーク セキュリティ– Overview



1. WVD Service EndpointとWVD依存コンポーネントへの接続
2. WVD利用ユーザーのインターネット利用
3. 内部ネットワーク(Azure Vnetやオンプレミス等のリモートサイト）への接続

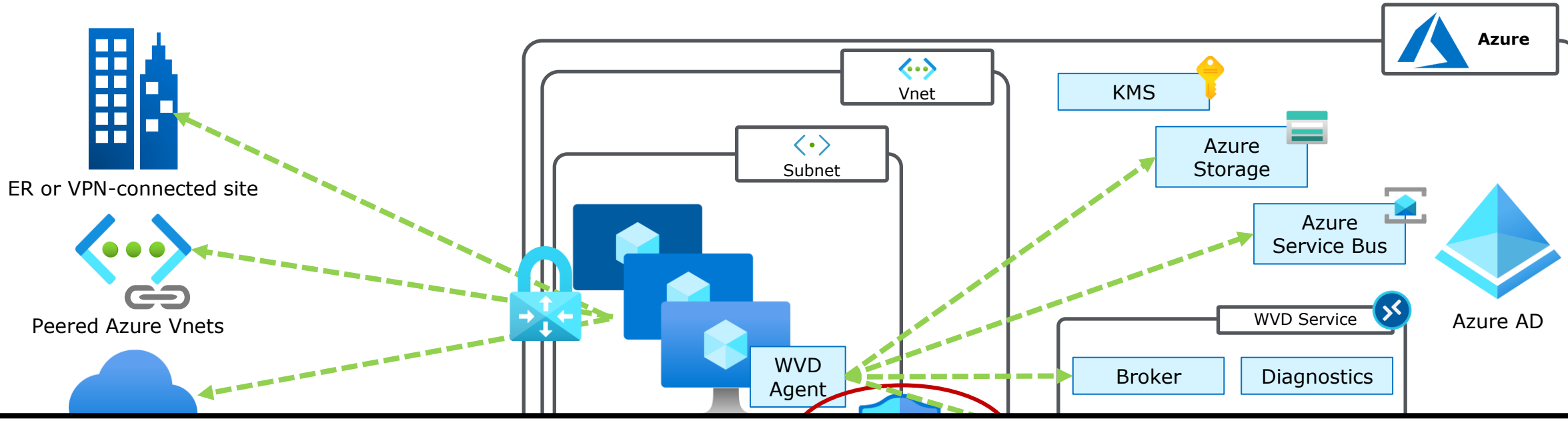
WVD ネットワーク セキュリティ– Network Security Group



Network Security Group(NGS)

- ネットワーク トラフィックは宛先に応じて、適切にルーティングされる
- NSGのセキュリティ ポリシーは IP-based アクセス制御リスト(FQDNの指定には対応していない)
- 大半のAzure PaaSサービス(WVD含む) はサービスタグが用意されており、サービス単位でアクセス制御することも可能
  ※PaaSサービスは定期的にIPアドレスが更新される可能性があるため、Azureサービスのアクセス制御はサービスタグで設定する

WVD ネットワーク セキュリティー– Network Security Group



追加　既定の規則　最新の情報に更新

優先度	名前	ポート	プロトコル	ソース	宛先	アクション
1000	AllowWVDServiceOutBound	443	TCP	VirtualNetwork	WindowsVirtualDesktop	許可
1100	AllowAzureServiceOutBound	443	TCP	VirtualNetwork	AzureCloud	許可
1200	AllowInternerWebApplicationOutBound	80,443	TCP	VirtualNetwork	192.168.15.0/24	許可
1300	AllowSpecificInternetSiteOutBound	443	TCP	VirtualNetwork	1.2.3.4	許可
65000	AllowVnetOutBound	任意	任意	VirtualNetwork	VirtualNetwork	許可
65001	AllowInternetOutBound	任意	任意	任意	Internet	許可
65500	DenyAllOutBound	任意	任意	任意	任意	拒否

WVD ネットワーク セキュリティ – Network Security Group

Virtual machines

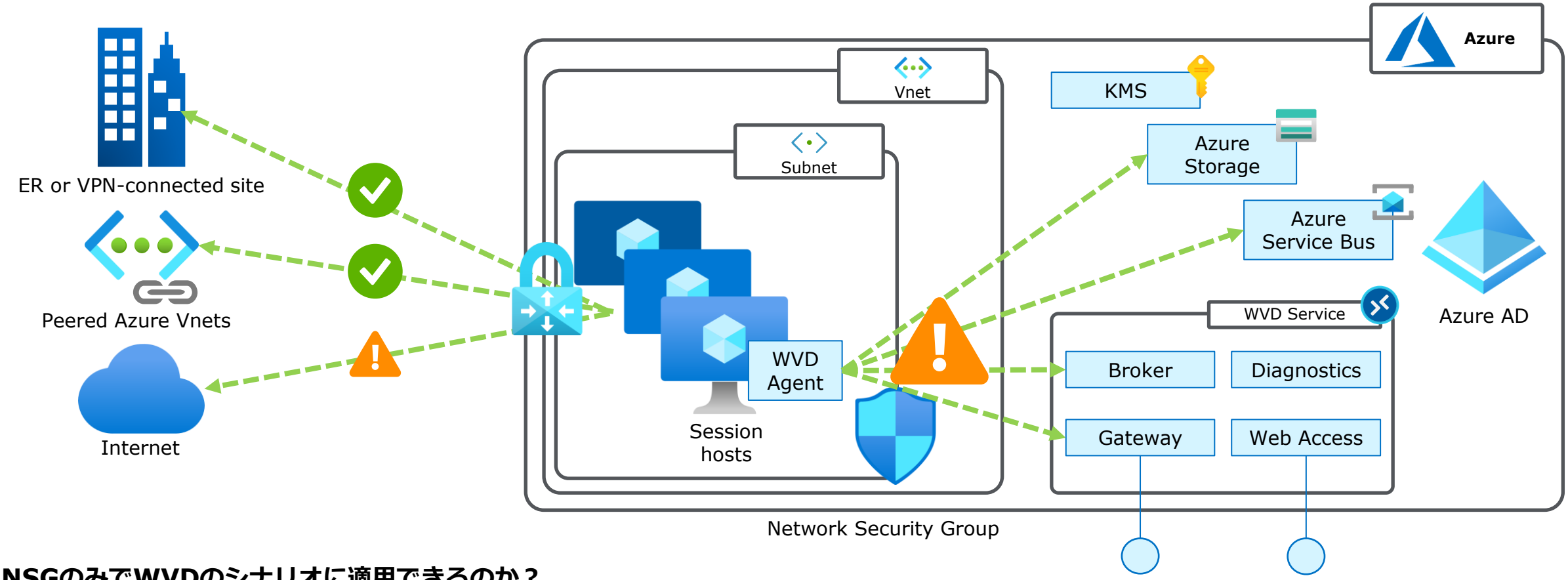
The Azure virtual machines you create for Windows Virtual Desktop must have access to the following URLs:

Address	Outbound TCP port	Purpose	Service Tag
*.wvd.microsoft.com	443	Service traffic	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS stack updates	AzureCloud
*.core.windows.net	443	Agent traffic	AzureCloud
*.servicebus.windows.net	443	Agent traffic	AzureCloud
gcs.prod.monitoring.core.windows.net	443	Agent traffic	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows activation	Internet
wvdportalstorageblob.blob.core.windows.net	443	Azure portal support	AzureCloud
169.254.169.254	80	Azure Instance Metadata service endpoint	N/A
168.63.129.16	80	Session host health monitoring	N/A

23.102.135.246

Azure CloudはAzure
全リージョンの
全てのサービス

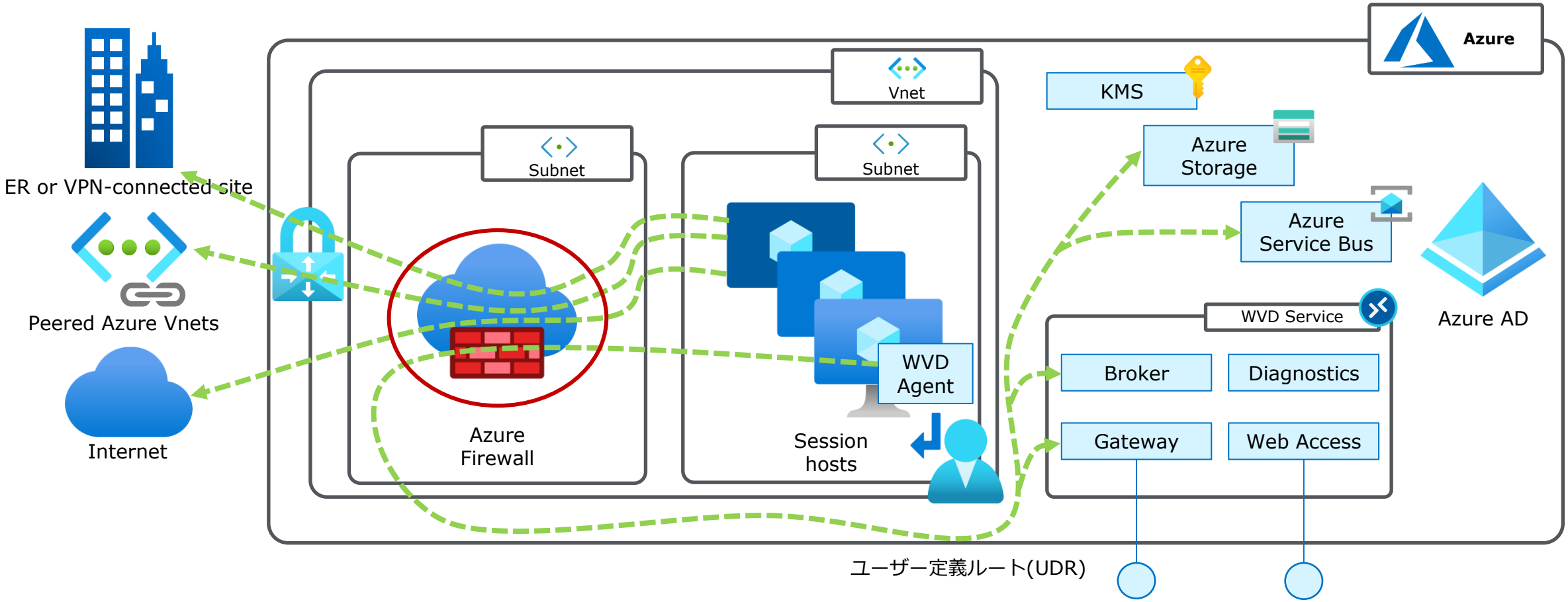
WVD ネットワーク セキュリティ– Network Security Group



NSGのみでWVDのシナリオに適用できるのか？

- 内部リソースに対する接続は、IP-based アクセス制御で制限できる ✅
- WVD依存コンポーネントはIPアドレスではなく、FQDNの指定となる。Azure Cloud サービスタグでは広範囲に許可してしまう ⚠
- 現時点においてはWVD Serviceのサービスタグは WVD利用において必要な通信すべてをカバーできていない ⚠
- インターネット閲覧は制限できない ⚠

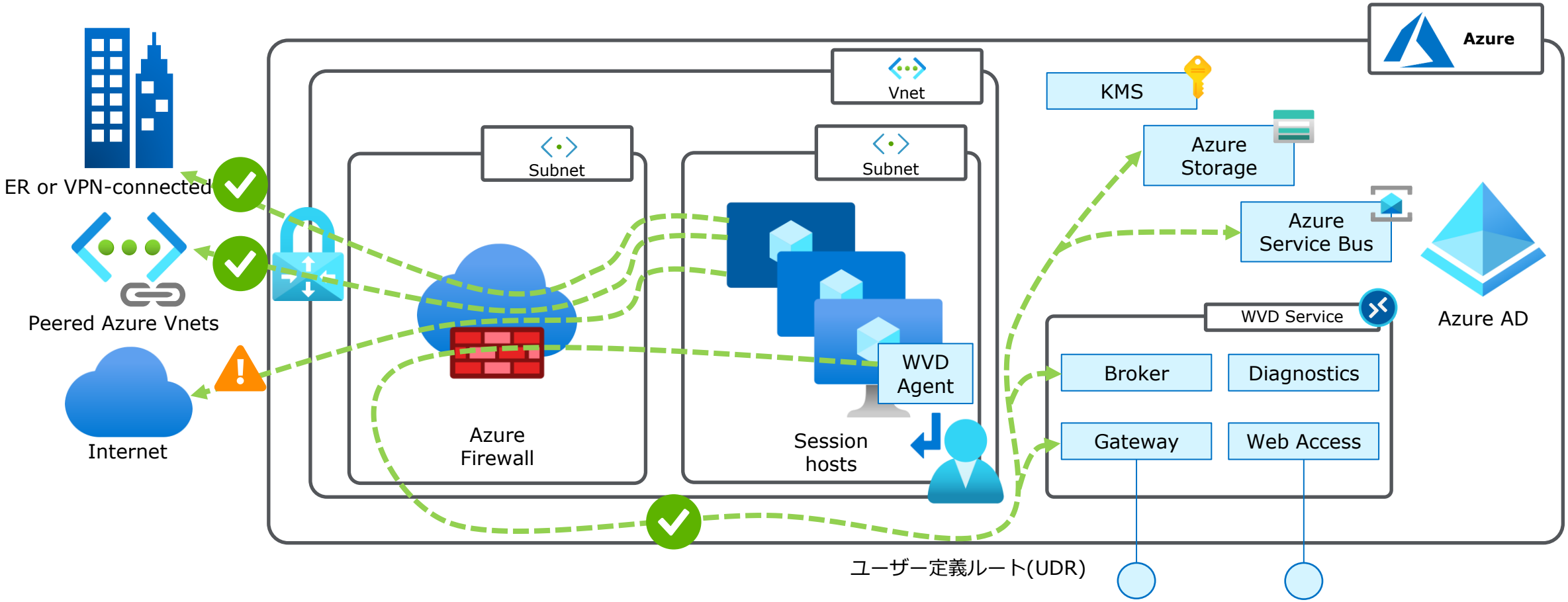
WVD ネットワーク セキュリティ– Azure Firewall



Azure Firewall(AFW)

- WVDサブネットの仮想マシン(Session hosts)は、UDRによってトラフィックがAzure Firewallに渡される
- AFWのセキュリティ ポリシーは FQDN-based アクセス制御リスト(FQDNの指定には対応していない)
- AFWの代わりにサードパーティ製のネットワーク仮想アプライアンス(NVA)に置き換えることも可能
  ※導入するNVAはFQDN-basedフィルタリング機能が実装されていることが望ましい

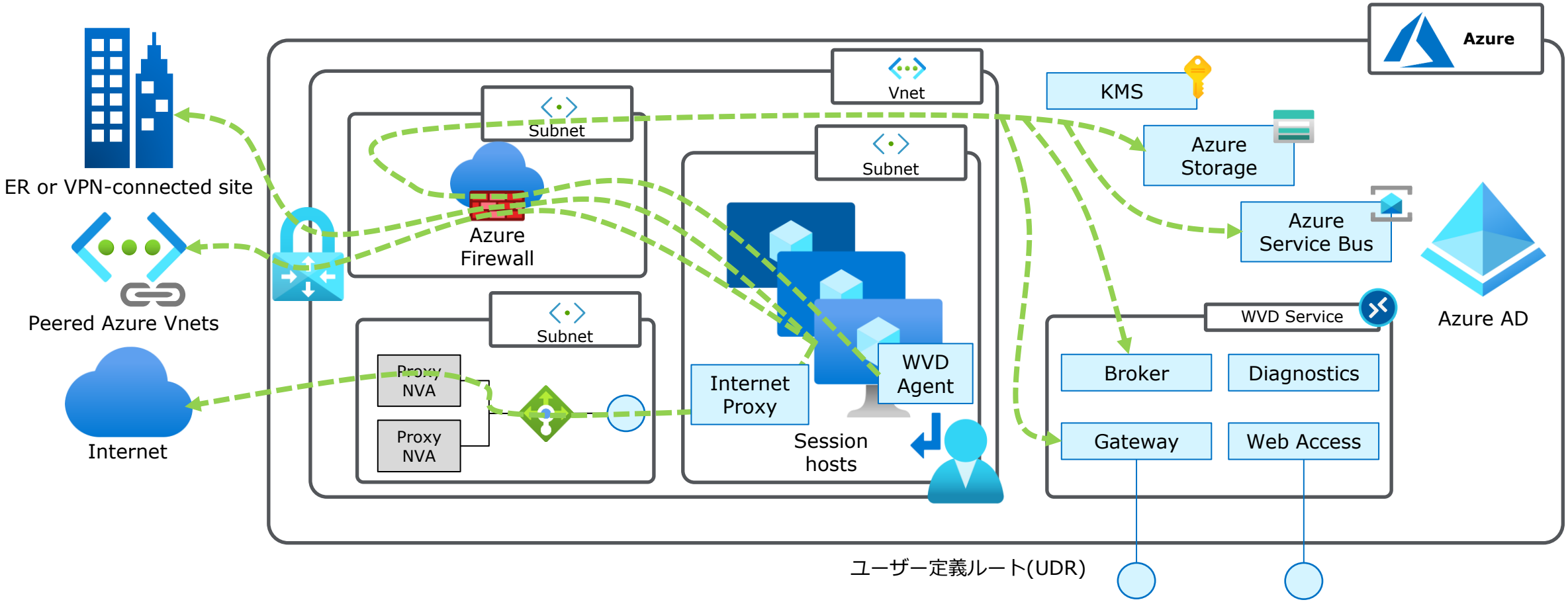
WVD ネットワーク セキュリティ– Azure Firewall



AFWを導入してWVDのシナリオに適用できるのか？

- 内部リソースに対する接続は、IP-based アクセス制御で制限できる ✅
- WVD ServiceとWVD依存コンポーネントに対する接続は、FQDN-basedアクセス制御で制限できる ✅
- インターネット閲覧は制限できない(カテゴリーフィルター機能などは存在しない) ⚠

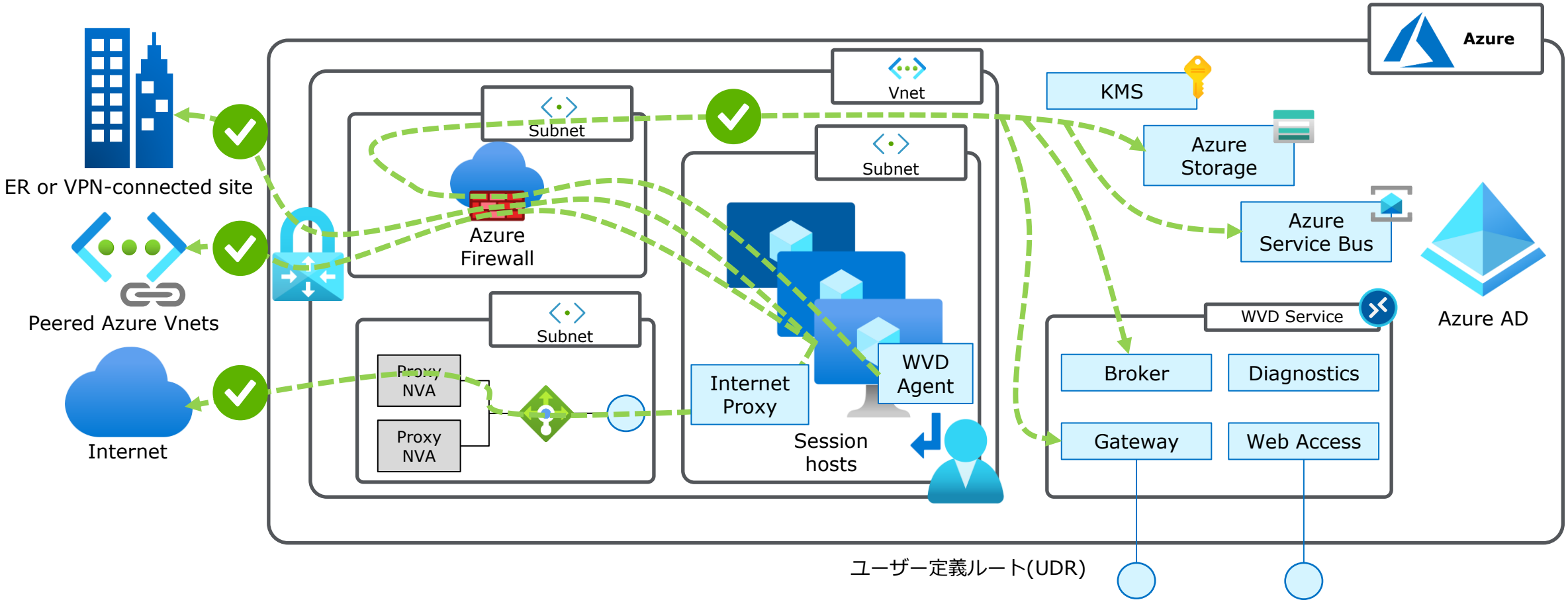
WVD ネットワーク セキュリティ– Azure Firewall + internet proxy



Internet proxies

- 明示型プロキシを使用する必要があります（ブラウザでのプロキシ設定）
  - WinHTTPとしてのプロキシ構成はできません（サポータ対象外のシナリオです）
- セッションホストからのプロキシ宛てでない全ての通信はUDRの設定によりAzure Firewallを経由します
- ユーザーがプロキシをバイパスした場合、トラフィックはAzure Firewallへ送られます

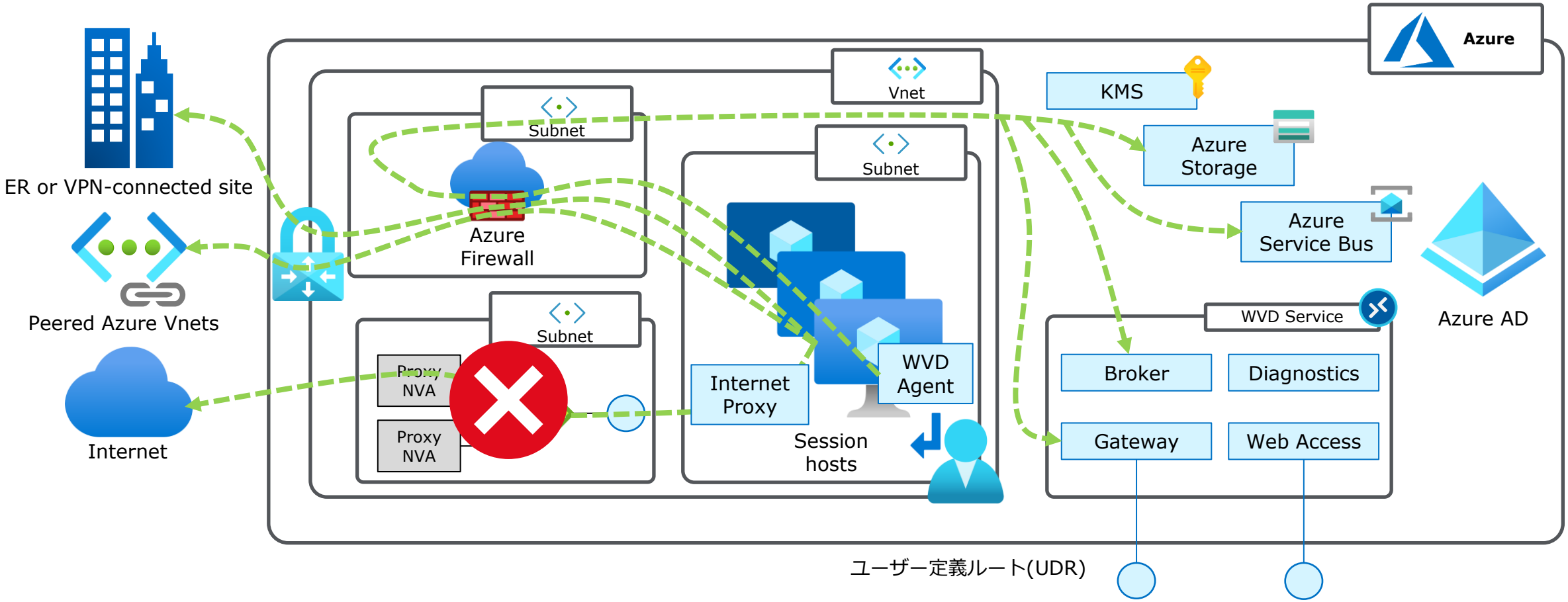
WVD ネットワーク セキュリティ– Azure Firewall + internet proxy



AFW + Internet proxiesを導入してWVDのシナリオに適用できるのか？

- 内部リソースに対する接続は、IP-based アクセス制御で制限できる ✅
- WVD ServiceとWVD依存コンポーネントに対する接続は、FQDN-basedアクセス制御で制限できる ✅
- インターネット閲覧はプロキシで制限する ✅

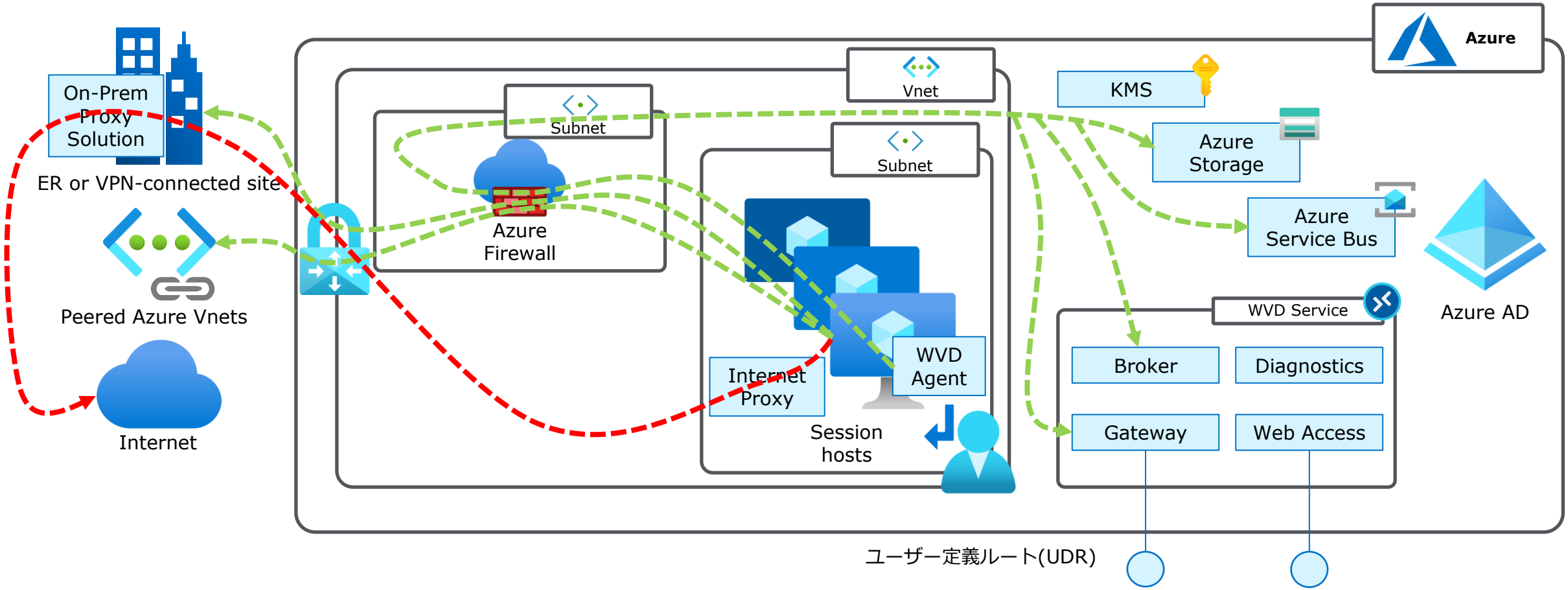
WVD ネットワーク セキュリティ– “Azureにプロキシを構成したくない！”



Why?

- ユーザーが利用するデバイスがインターネット接続するときは、オンプレミスで構成しているソリューションを経由する要件があります
- 使いたいプロキシのソリューションがAzure Marketplaceに公開されていません
- AzureにIaaSで構築するのではなく、クラウドサービスとしての proxy-as-a-serviceを利用したいです(Zscaler等)
- 信頼できるインターネット接続を使用する必要があります（政府機関のお客様）

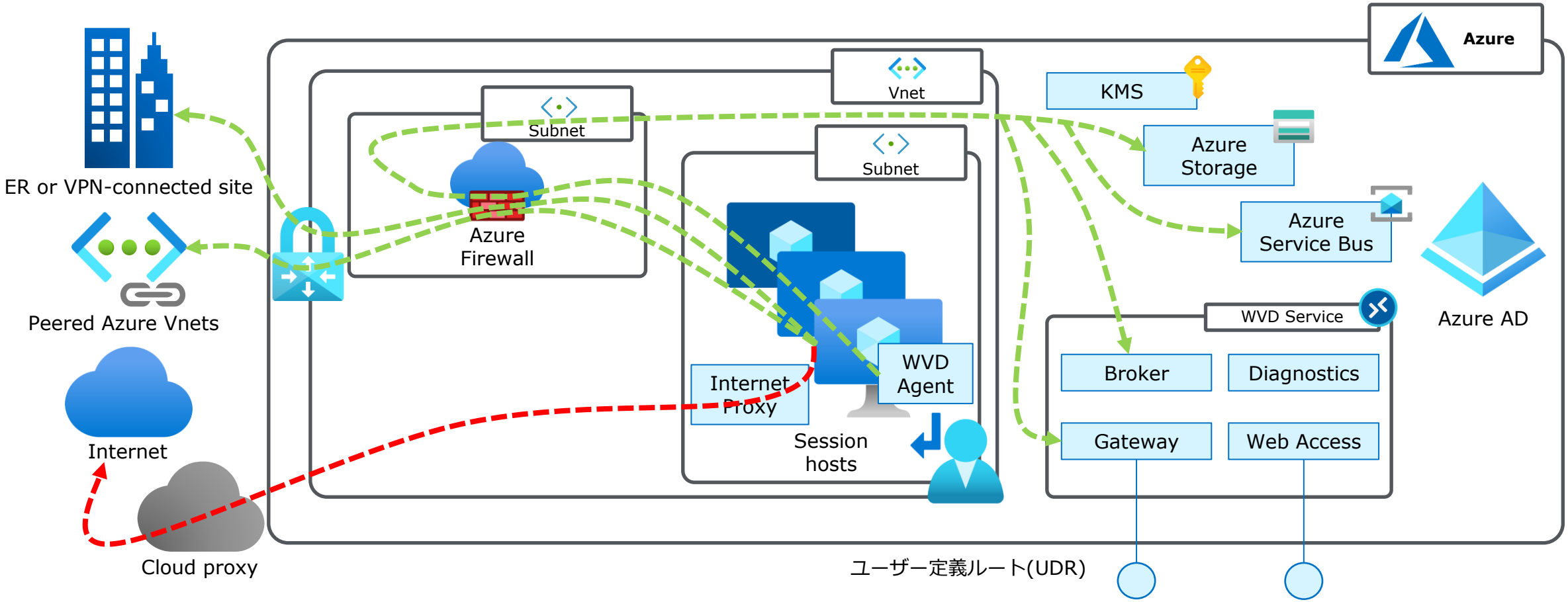
WVD ネットワーク セキュリティ– “Azureにプロキシを構成したくない！”



On-Prem internet proxy

- 重要なトラフィックはAzure Firewallを介して直接インターネットに送信されます
- 明示型プロキシを使用する必要があります（ブラウザでのプロキシ設定）
- パフォーマンスが低下する恐れがあります

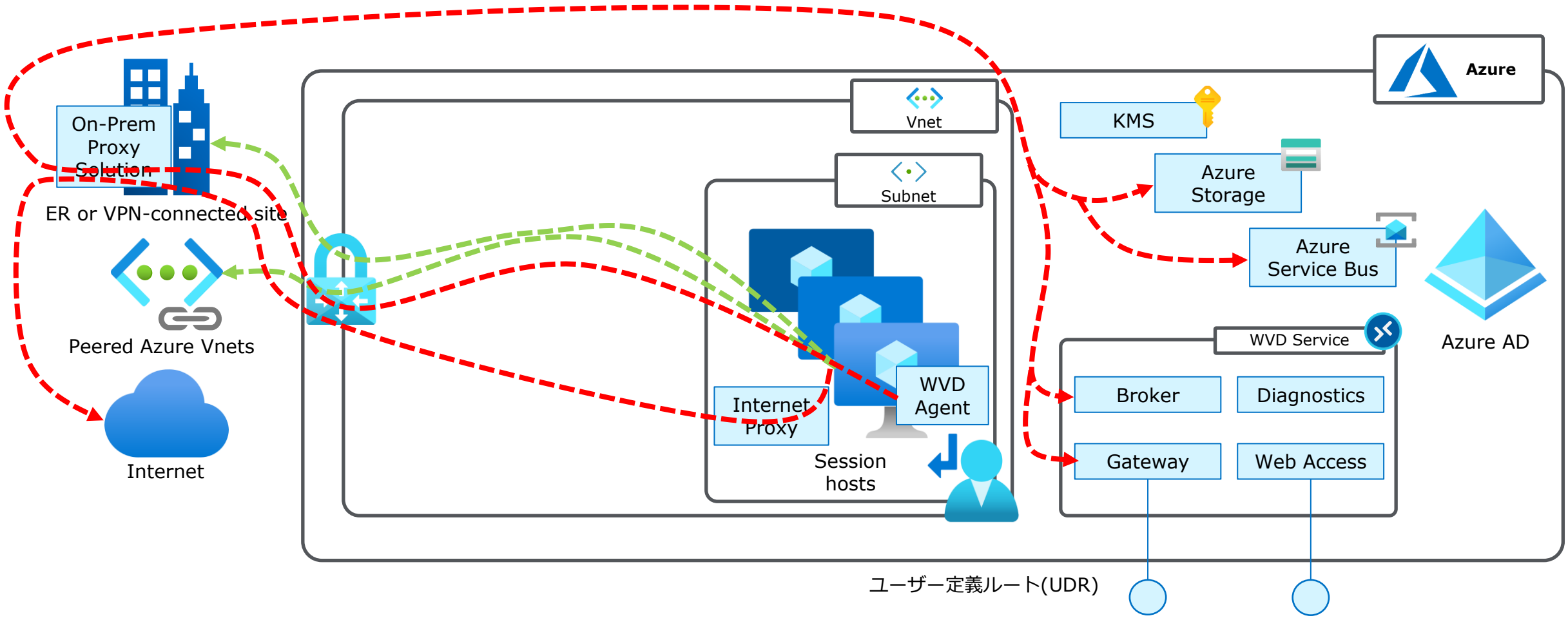
WVD ネットワーク セキュリティ– “Azureにプロキシを構成したくない！”



Internet proxy as-a-service

- 重要なトラフィックはAzure Firewallを介して直接インターネットに送信されます
- 明示型プロキシを使用する必要があります（ブラウザでのプロキシ設定）
- インターネット トラフィックは IPSec tunnel で クラウドのプロキシへ送られます（要ベンダーへの確認）

WVD ネットワーク セキュリティ– “全ての通信をオンプレミス経由にしたい”



強制トンネリング

- 強制トンネリングは技術的には可能 – インターネット トラフィックをERまたはS2S VPNを経由してオンプレミスへ送る
- WVDにおいて強制トンネリング構成はサポート対象外
- 全ての通信がオンプレミス経由となるため、パフォーマンスが極端に低下する可能性があります
- Azureサービスが正常に利用できるように、オンプレミス側で設定変更が必要です

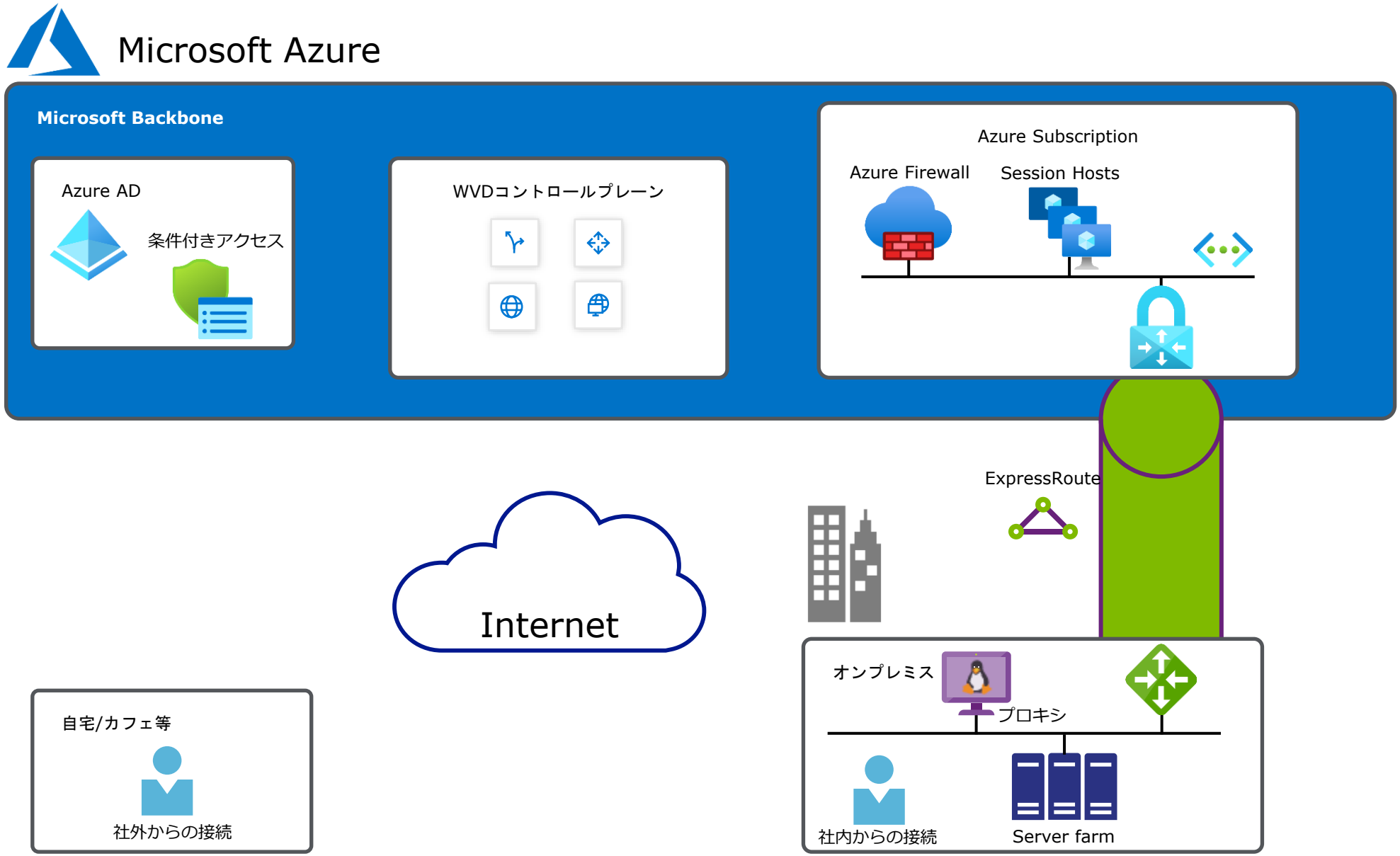
WVDネットワーク構成 – どの構成案を選択するか

No	構成案	AzureCloudサービスタグ	ユーザーのインターネット利用	備考
1	NSG	許容できる	以下のいずれかを満たす ・インターネット利用させない ・利用を制限しない	
2	NSG + AFW	許容できない	以下のいずれかを満たす ・インターネットを利用させない ・利用を制限しない	
3	NSG + AFW + Proxy on Azure	許容できない	利用を制限する	
4	NSG + AFW + Proxy on On-Prem	許容できない	利用を制限する	インターネット利用時にはオンプレミスのソリューションを利用する
5	NSG + AFW + Proxy-as-a-service	許容できない	利用を制限する	インターネット利用時にはクラウドサービスを利用する
6	NSG + Proxy on Azure	許容できる	利用を制限する	
7	NSG + Proxy on On-Prem	許容できる	利用を制限する	インターネット利用時にはオンプレミスのソリューションを利用する
8	NSG + Proxy-as-a-service	許容できる	利用を制限する	インターネット利用時にはクラウドサービスを利用する
9	Traffic force-tunneled to On-Prem	許容できない	利用を制限する	全ての通信をオンプレミスに送る

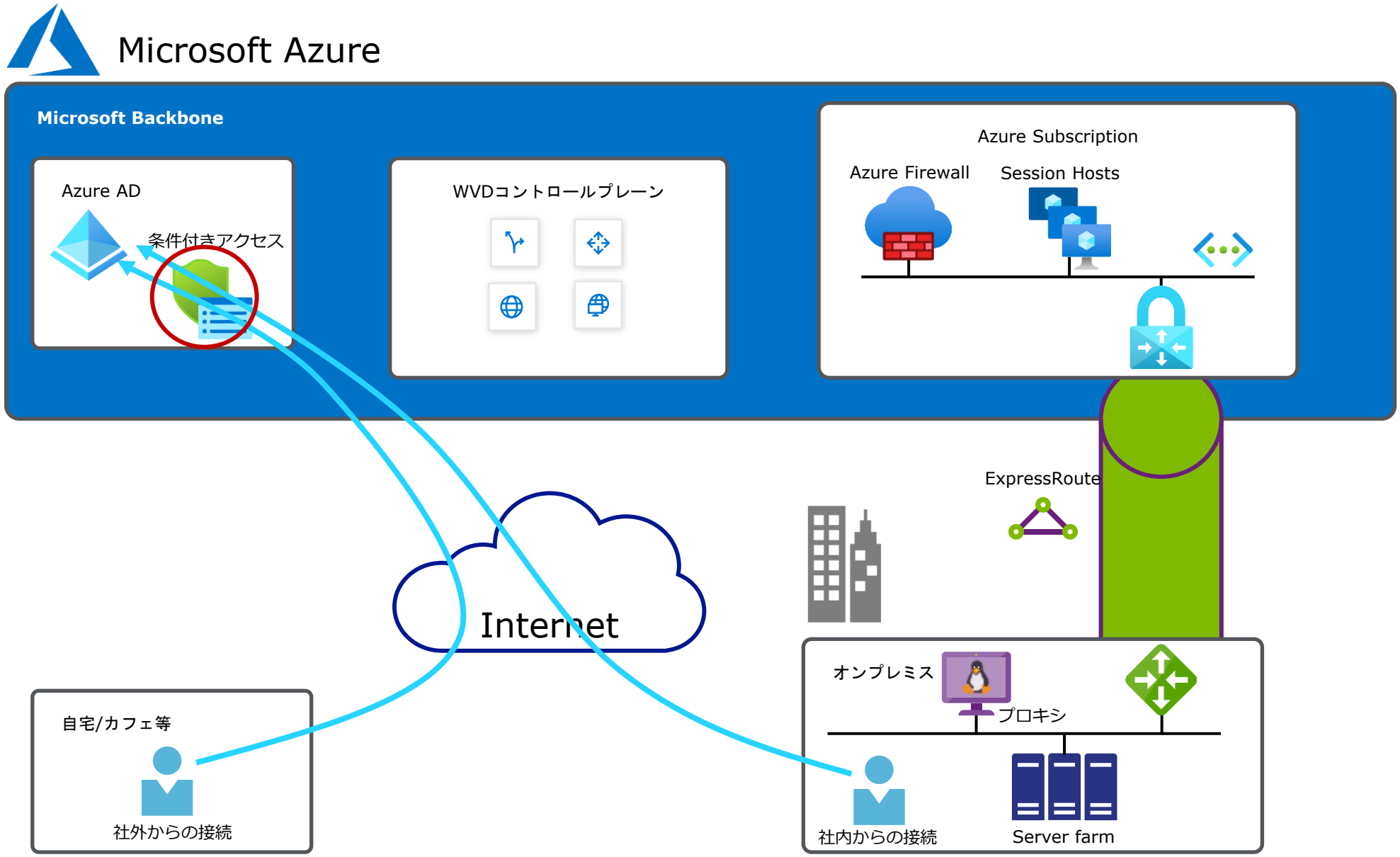
※上記はあくまで例であり、その他の要件も踏まえて構成を検討する必要があります

4. 構成例のご紹介

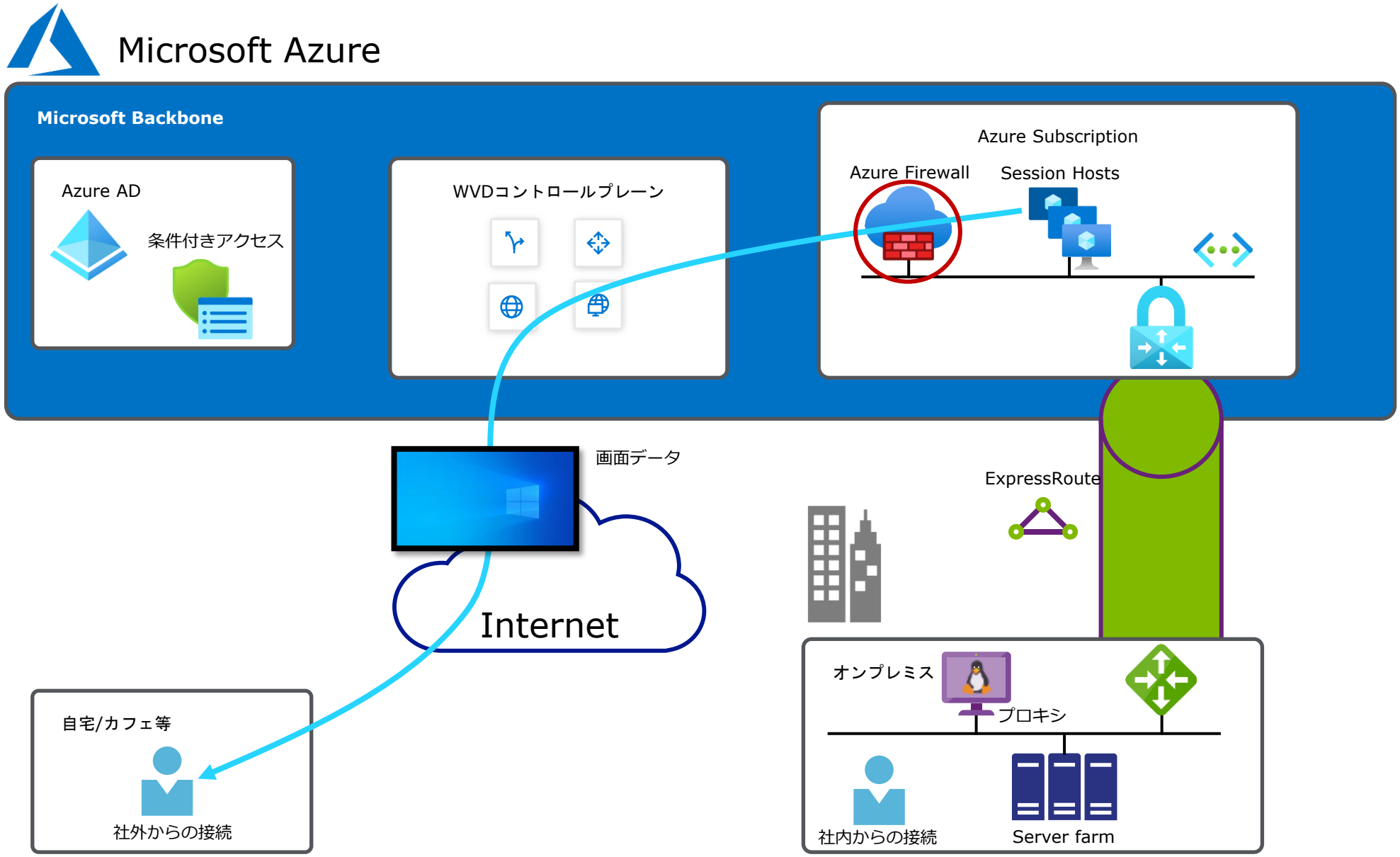
全体像



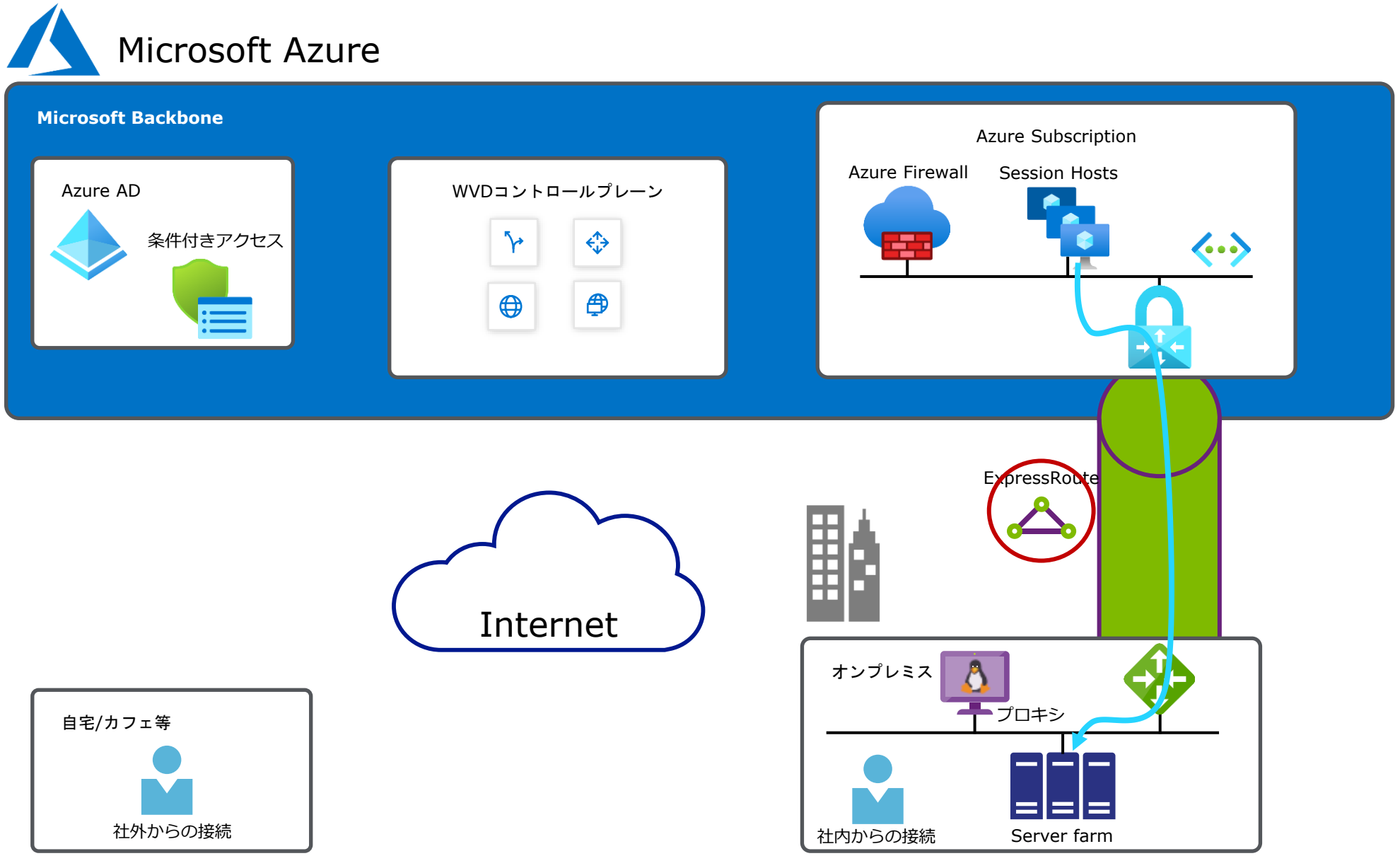
WVD接続時にはAzure AD条件付きアクセスを構成



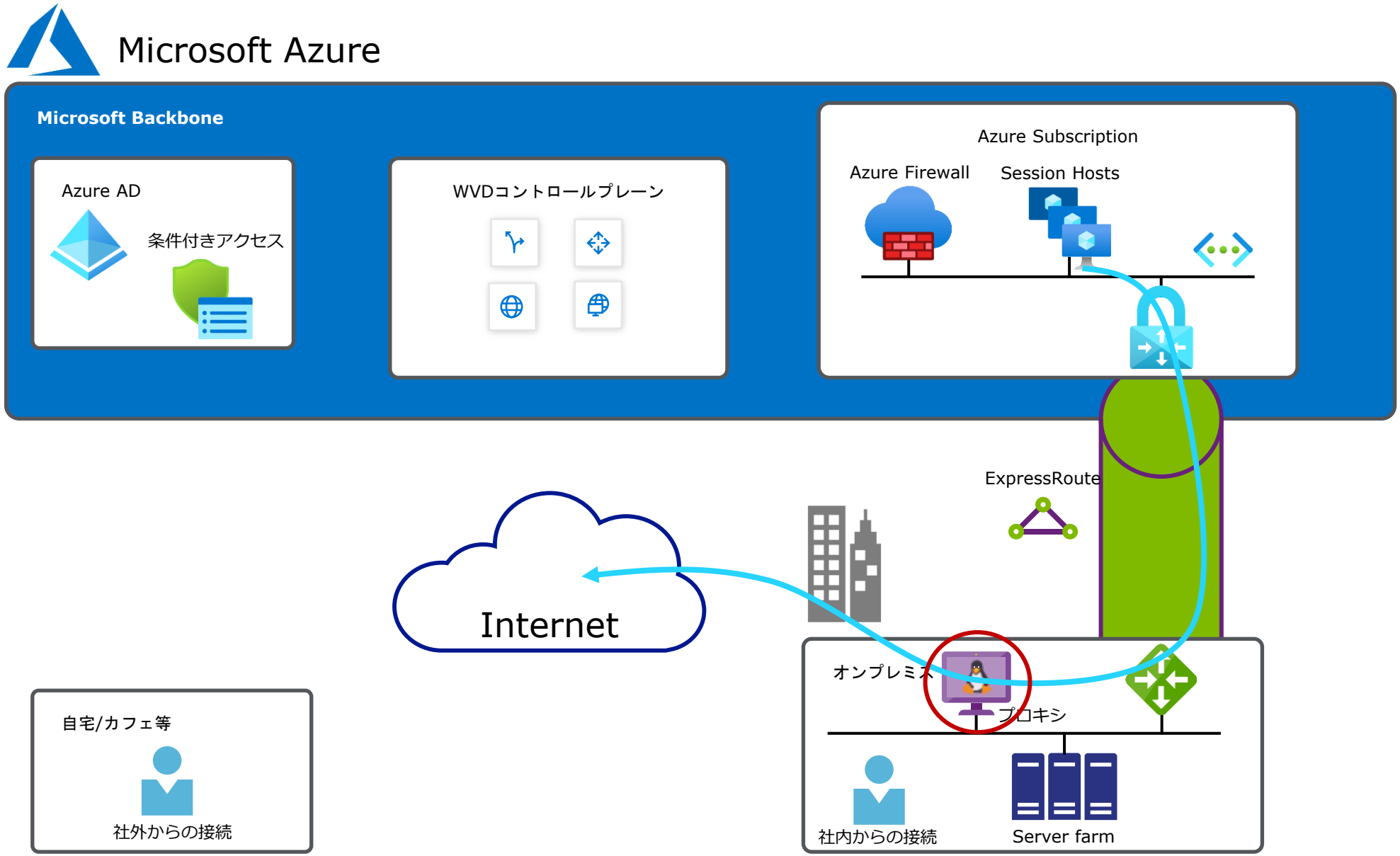
WVDコントロール プレーンとはAzure Firewall経由で接続



社内システムには専用線経由でアクセス



インターネット閲覧にはオンプレミスのプロキシを利用



5. 導入支援メニュー紹介

導入支援メニュー一覧

		トライアル プラン（プラン1）	新規環境 簡易 PoC プラン（プラン2）	既存環境 簡易 PoC プラン（プラン3）	カスタム プラン
サービス提供価格		無償	50 万円	30 万円	個別見積り
Azure 環境		弊社環境	お客様環境	お客様環境	お客様環境
基本環境構築	新規 AD 構築	○	○	-	○
	新規 Azure AD 連携	○	○	-	○
	既存 AD 連携	×	×	-	○
	既存 Azure AD 連携	×	×	-	○
	VNet 構築	○	○	-	○
	VPN 接続	×	×	-	○
設計方法		-	ヒアリングシートへの入力	ヒアリングシートへの入力	個別設計
カスタムイメージ、カスタムアプリ		× ※弊社指定イメージ	× ※弊社指定イメージ	× ※弊社指定イメージ	○
構成、イメージのパターン数		1	1	1	応相談
グループポリシー設定		× ※弊社指定の設定は対応可	× ※弊社指定の設定は対応可	×	○
FSLogix ユーザープロファイル設定		×	○ ※Blob のみ対応可	○ ※Blob のみ対応可	○
利用ユーザー設定		10 名まで	50 名まで	50 名まで	無制限
お問い合わせ / QA 対応		サービス提供期間内	構築後2週間まで	構築後2週間まで	応相談

トライアル プラン（プラン１）

弊社にてご用意した WVD 環境をご提供し、
お客様にて WVD の使用感を検証いただくためのサービス

サービス提供価格

無償

含まれる作業

- 弊社提供の WVD トライアル環境の提供
- マルチセッションまたはシングルセッションのいずれか一方
- 弊社指定のカスタムイメージまたは標準イメージ
- VM 台数は最大 2 台まで
- 10 名までユーザー作成可能

免責事項

- 月間約 1.7 万円のクラウド利用料または最大 2 週間の期間、いずれかの制限に達するまでの利用となります。

新規環境 簡易 PoC プラン（プラン２）

クラウド独立型の WVD 環境の PoC 環境構築支援サービス

サービス提供価格

50万円

※　別途 Azure 利用料が必要となります

含まれる作業

- 基本環境構築
  - WVD 用新規 Azure AD の用意
  - WVD 用新規 AD の構築および Azure AD との同期
  - WVD 用の Vnet 構築
    など
- WVD の展開
- マルチセッションまたはシングルセッションのいずれか一方
- 弊社指定のカスタムイメージまたは標準イメージ
- FSLogix ユーザープロファイル設定
- ユーザーの追加（50 名まで）
- お問い合わせによる QA 対応（環境提供後 2 週間）

お客様対応作業

- PoC 確認内容の決定
- 設計時のヒアリングシートへの入力
- PoC の実施（構築後の確認）
- PoC 後のフィードバック

納品物

- パラメータシート

既存環境 簡易 PoC プラン（プラン3）

WVD のシステム要件が整っているお客様向けの PoC 環境構築支援サービス

サービス提供価格
30万円
※　別途 Azure 利用料が必要となります

本メニューの対象者
- チェックリストの条件を満たしていること

含まれる作業
- WVD の展開
- マルチセッションまたはシングルセッションのいずれか一方
- 弊社指定のカスタムイメージまたは標準イメージ
- FSLogix ユーザープロファイル設定
- ユーザーの追加（50 名まで）
  ※Azure AD 上にユーザーが存在することが前提
- お問い合わせによる QA 対応（環境提供後 2 週間）

現在、本サービスの提供はオフサイトによるリモート構築となります。
ヒアリングシート受領後、最短で 2、3 日での提供が可能です。

お客様対応作業
- チェックリストの条件確認および問題解消
- PoC 確認内容の決定
- 設計時のヒアリングシートへの入力
- PoC の実施（構築後の確認）
- PoC 後のフィードバック

納品物
- パラメータシート

免責事項
- オンプレミスのネットワークの問題など、既存構成に起因するトラブルはお客様に解決いただくことを前提といたします。

WVD に必要な環境・ライセンスのチェックリスト

- ☐Azure サブスクリプションおよび共同作成者権限
- ☐Azure AD（Office 365 や Azure のテナントに付属）

※Azure に付属の Azure AD を利用することになる
※既存 Office 365 ユーザーが利用する場合は、同一テナントに Azure を用意する必要がある

- ☐以下のいずれかのドメインコントローラー
  - ☐ 上記Azure AD と同期している Active Directory（AD）
  - ☐ 上記Azure AD で Azure AD Domain Service を有効化
- ☐Microsoft 365 または Windows 10 ライセンス

※検証利用においては不要

- ☐[Azure] 仮想ネットワーク（VNet）
- ☐[Azure] VNet の DNS サーバーに AD が指定されていること
- ☐[Azure AD] 全体管理者アカウント

※MFA などの条件付きアクセス設定時のみ全体管理者またはセキュリティ管理者のアカウントが必須

- ☐[AD] コンピュータをドメイン参加させる権限をもつアカウント

参考：必要条件
https://docs.microsoft.com/ja-jp/azure/virtual-desktop/overview#requirements

カスタム プラン

お客様要件に応じたカスタムプラン

サービス提供価格

個別見積もり

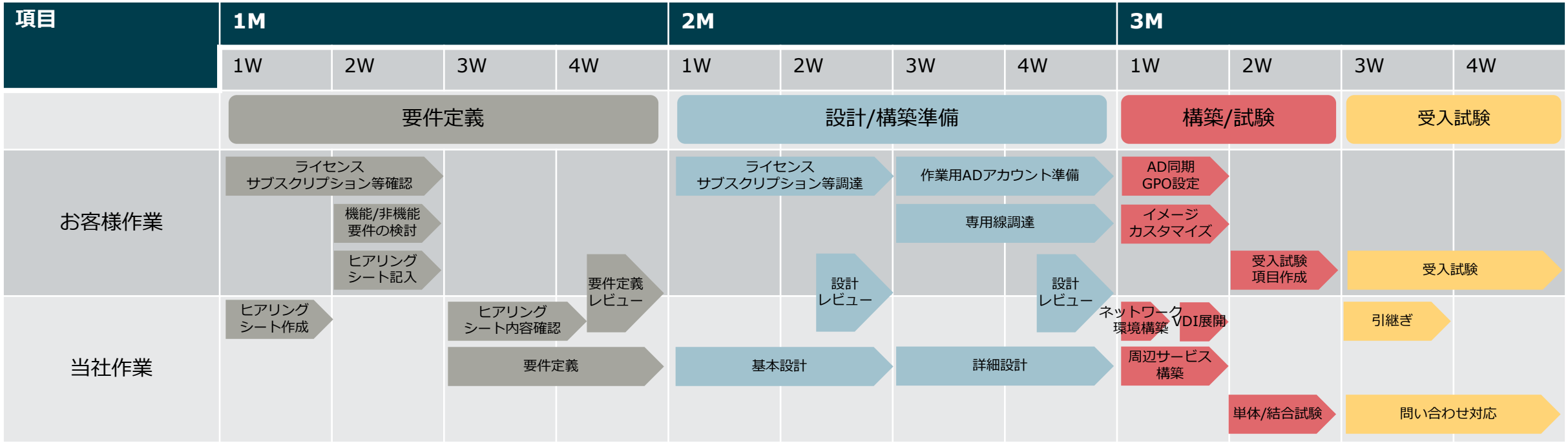
※　別途 Azure 利用料が必要となります

以下のそれぞれのフェーズにおける要件・作業内容に応じて個別見積もりを行います。

設計 → 基本環境構築 → WVD 構築 → 運用支援

カスタムプラン（参考）

- 期間：3ヵ月
- ドキュメント：基本設計書、詳細設計書、テスト仕様書兼結果報告書



Azure 費用シミュレーション

Windows Virtual Desktop 料金計算ツール
https://cloudsteady.jp/solution/wvd_cost/index.html

※精緻な金額を算出する場合にはMicrosoftの料金計算ツールをご利用ください

Appendix

PERSOL

Windows Virtual Desktop
導入支援・提供サービス

2020 年 10 月

パーソルプロセス＆テクノロジー株式会社

弊社関連サービス紹介

WVD に必要な環境・ライセンスのチェックリスト

- ☐Azure サブスクリプションおよび共同作成者権限
- ☐Azure AD（Office 365 や Azure のテナントに付属）

※Azure に付属の Azure AD を利用することになる
※既存 Office 365 ユーザーが利用する場合は、同一テナントに Azure を用意する必要がある

- ☐以下のいずれかのドメインコントローラー
  - ☐ 上記Azure AD と同期している Active Directory（AD）
  - ☐ 上記Azure AD で Azure AD Domain Service を有効化
- ☐Microsoft 365 または Windows 10 ライセンス

※検証利用においては不要

- ☐[Azure] 仮想ネットワーク（VNet）
- ☐[Azure] VNet の DNS サーバーに AD が指定されていること
- ☐[Azure AD] 全体管理者アカウント

※MFA などの条件付きアクセス設定時のみ全体管理者またはセキュリティ管理者のアカウントが必須

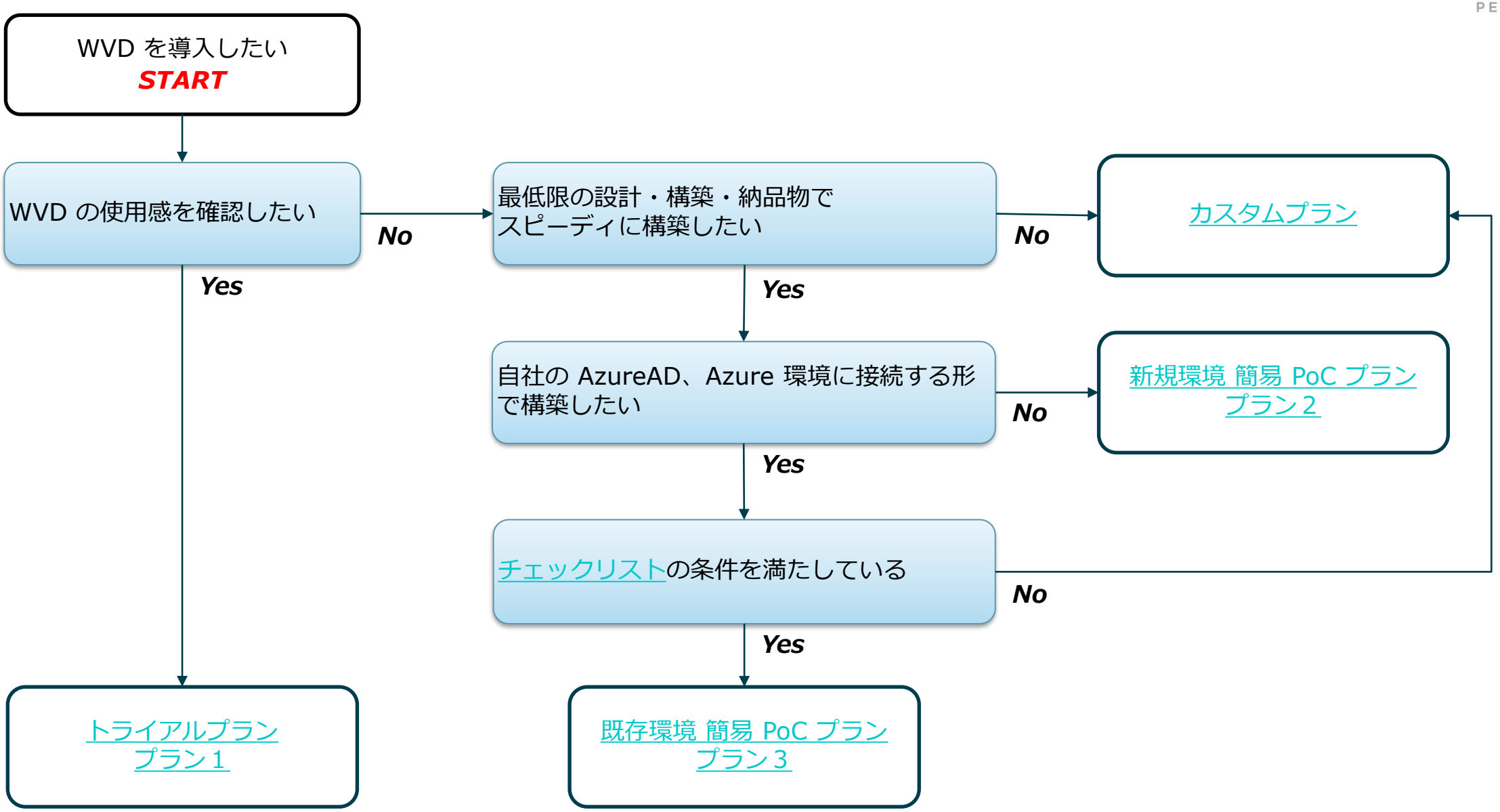
- ☐[AD] コンピュータをドメイン参加させる権限をもつアカウント

参考：必要条件
https://docs.microsoft.com/ja-jp/azure/virtual-desktop/overview#requirements

導入支援メニュー一覧

		トライアル プラン（プラン1）	新規環境 簡易 PoC プラン（プラン2）	既存環境 簡易 PoC プラン（プラン3）	カスタム プラン
サービス提供価格		無償	50 万円	30 万円	個別見積り
Azure 環境		弊社環境	お客様環境	お客様環境	お客様環境
基本環境構築	新規 AD 構築	○	○	-	○
	新規 Azure AD 連携	○	○	-	○
	既存 AD 連携	×	×	-	○
	既存 Azure AD 連携	×	×	-	○
	VNet 構築	○	○	-	○
	VPN 接続	×	×	-	○
設計方法		-	ヒアリングシートへの入力	ヒアリングシートへの入力	個別設計
カスタムイメージ、カスタムアプリ		× ※弊社指定イメージ	× ※弊社指定イメージ	× ※弊社指定イメージ	○
構成、イメージのパターン数		1	1	1	応相談
グループポリシー設定		× ※弊社指定の設定は対応可	× ※弊社指定の設定は対応可	×	○
FSLogix ユーザープロファイル設定		×	○ ※Blob のみ対応可	○ ※Blob のみ対応可	○
利用ユーザー設定		10 名まで	50 名まで	50 名まで	無制限
お問い合わせ / QA 対応		サービス提供期間内	構築後2週間まで	構築後2週間まで	応相談

メニュー選択におけるフローチャート



Windows Virtual Desktop

導入支援メニュー詳細

トライアル プラン（プラン１）

弊社にてご用意した WVD 環境をご提供し、
お客様にて WVD の使用感を検証いただくためのサービス

サービス提供価格

無償

含まれる作業

- 弊社提供の WVD トライアル環境の提供
- マルチセッションまたはシングルセッションのいずれか一方
- 弊社指定のカスタムイメージまたは標準イメージ
- VM 台数は最大 2 台まで
- 10 名までユーザー作成可能

免責事項

- 月間約 1.7 万円のクラウド利用料または最大 2 週間の期間、いずれかの制限に達するまでの利用となります。

新規環境 簡易 PoC プラン（プラン２）

クラウド独立型の WVD 環境の PoC 環境構築支援サービス

サービス提供価格

50万円

※　別途 Azure 利用料が必要となります

含まれる作業

- 基本環境構築
  - WVD 用新規 Azure AD の用意
  - WVD 用新規 AD の構築および Azure AD との同期
  - WVD 用の Vnet 構築

  など
- WVD の展開
- マルチセッションまたはシングルセッションのいずれか一方
- 弊社指定のカスタムイメージまたは標準イメージ
- FSLogix ユーザープロファイル設定
- ユーザーの追加（50 名まで）
- お問い合わせによる QA 対応（環境提供後 2 週間）

お客様対応作業

- PoC 確認内容の決定
- 設計時のヒアリングシートへの入力
- PoC の実施（構築後の確認）
- PoC 後のフィードバック

納品物

- パラメータシート

既存環境 簡易 PoC プラン（プラン3）

WVD のシステム要件が整っているお客様向けの
PoC 環境構築支援サービス

サービス提供価格
30万円
※　別途 Azure 利用料が必要となります

本メニューの対象者
- チェックリストの条件を満たしていること

含まれる作業
- WVD の展開
- マルチセッションまたはシングルセッションのいずれか一方
- 弊社指定のカスタムイメージまたは標準イメージ
- FSLogix ユーザープロファイル設定
- ユーザーの追加（50 名まで）
  ※Azure AD 上にユーザーが存在することが前提
- お問い合わせによる QA 対応（環境提供後 2 週間）

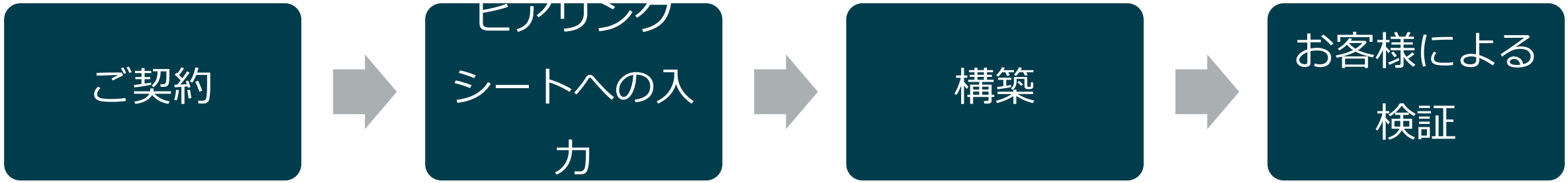
現在、本サービスの提供はオフサイトによるリモート構築となります。
ヒアリングシート受領後、最短で 2、3 日での提供が可能です。

お客様対応作業
- チェックリストの条件確認および問題解消
- PoC 確認内容の決定
- 設計時のヒアリングシートへの入力
- PoC の実施（構築後の確認）
- PoC 後のフィードバック

納品物
- パラメータシート

免責事項
- オンプレミスのネットワークの問題など、既存構成に起因するトラブルはお客様に解決いただくことを前提といたします。

PoC プラン 2 / プラン 3 の進め方



※ ヒアリングシート受領後、構築は数日で完了します。
※ 原則として、構築完了後の引き渡し確認をもって検収いただくものとします。

カスタム プラン

お客様要件に応じたカスタムプラン

サービス提供価格

個別見積もり

※　別途 Azure 利用料が必要となります

以下のそれぞれのフェーズにおける要件・作業内容に応じて個別見積もりを行います。

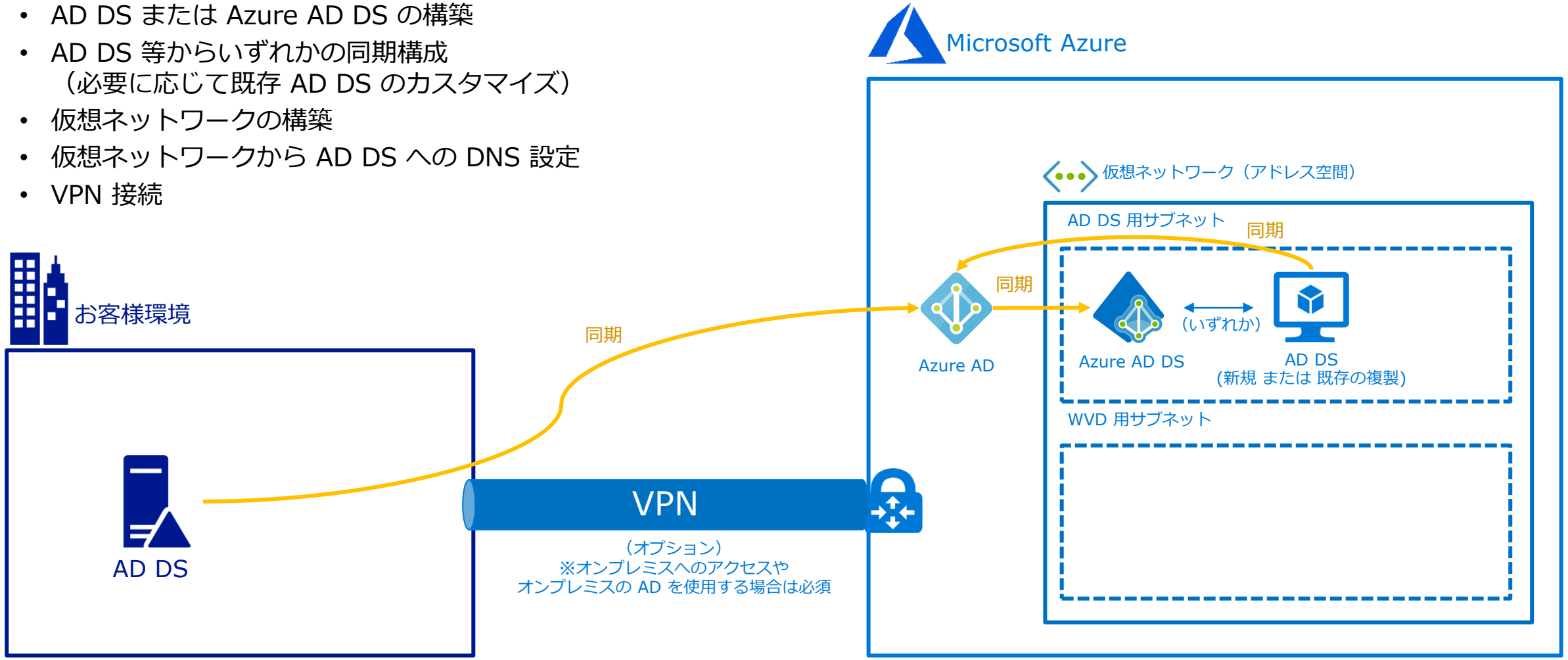
設計 → 基本環境構築 → WVD 構築 → 運用支援

基本環境構築とは

WVD 構成要件となっているネットワークや AD DS 等の環境構築を指します。

主な作業（要件により異なります）

- AD DS または Azure AD DS の構築
- AD DS 等からいずれかの同期構成
  （必要に応じて既存 AD DS のカスタマイズ）
- 仮想ネットワークの構築
- 仮想ネットワークから AD DS への DNS 設定
- VPN 接続



設計フェーズ メニュー

No	サービスメニュー	概要説明	構築 / 対応 フェーズ
1-1	新規 AD 構築設計	WVD 用に新規で Windows Server Active Directory を作成するための OS および AD DS の役割に関する設計を行います。	基本環境構築
1-2	新規 Azure AD DS 構築設計	WVD 用に新規で Azure Active Directory Domain Services を作成するための設計を行います。	
1-3	既存 AD 同期設計	既存の AD DS を Azure AD に同期するための Azure AD Connect に関する設計を行います。AD DS の設定や属性の変更の有無を確認します。	
1-4	新規 Azure AD 同期設計	AD DS を新規の Azure AD に同期するための設計を行います。	
1-5	既存 Azure AD 同期設計	AD DS を既存の Azure AD に同期するための設計を行います。すでに同一の UPN が存在する場合、ソフトマッチ等による ID の名寄せを行うことになります。	
1-6	VPN 接続等のネットワーク設計	ネットワーク関連の設計を行います。Azure 内のネットワーク設計の他、要件に応じてオンプレミスとの接続や通信制御に関する設計を行います。	
1-7	WVD 全体構成設計	WVD の構成に関する設計を行います。	WVD 構築
1-8	カスタムイメージ設計	カスタムイメージを作成する場合、OS やアプリケーションに関する設計を行います。	
1-9	グループポリシー設計	WVD の各種動作やセキュリティ関連のポリシーを制御するための設計を行います。	
1-10	プロファイル用ストレージ設計	利用ユーザー数や同時接続数の要件に応じて最適なストレージの設計を行います。	
1-11	FSLogix 設計	ユーザープロファイル管理およびアプリケーション管理に使用する FSLogix の設定に関する設計を行います。	
1-12	Azure AD 条件付きアクセス設計	WVD に接続する際に MFA 等のセキュリティ対策を行う場合に必要な設計を行います。	
1-13	運用・監視設計	運用および監視のための構成に必要な設計を行います。	運用支援
1-14	各種設計ドキュメント	上記設計に関する成果物として必要なドキュメントをご要望に応じて作成します。	-

基本環境構築フェーズ メニュー

No	サービスメニュー	概要説明
2-1	AD 構築 / 属性設定	WVD に必要な AD DS の構築または属性設定を行います。
2-2	AD と Azure AD の同期	AD DS と Azure AD を Azure AD Connect を使用してパスワードハッシュ同期を行います。
2-3	Azure AD DS 構築	Azure AD に対して Azure AD DS の機能を有効化を行います。
2-4	VNet 構築	Azure 上に WVD に必要なネットワークを構築し、Azure からルーティング設定やポート開閉の設定を行います。
2-5	VPN 接続	オンプレミスと Azure を VPN 接続します。必要に応じてオンプレミスの VPN 機器の設定を変更します。
2-6	Azure Firewall 構築	Azure と外部の通信を FQDN 等をベースに詳細なコントロールを行います。
2-7	WSUS / MECM（SCCM） 構築	Windows Update 管理や構成管理のためのサーバーを構築します。

※　作業内容に関連した設計が必要となります。

WVD 構築フェーズ メニュー

No	サービスメニュー	説明
3-1	WVD 基本構成構築	WVD の基本構成を構築します。
3-2	カスタムイメージ作成	お客様の要件に応じたカスタムイメージを作成します。
3-3	お任せカスタムイメージの利用	弊社で作成した日本語言語パックインストール済み、Microsoft 365 Apps for enterprise (Office 365 ProPlus) インストール済みの既成のイメージを利用します。
3-4	プロファイル用ストレージ構築	要件に応じて選定したプロファイル用のストレージを構築します。
3-5	FSLogix プロファイル設定	FSLogix のユーザープロファイルや Office プロファイルの設定を行います。
3-6	FSLogix アプリケーション管理設定	FSLogix によるアプリケーション管理・制御の設定を行います。
3-7	グループポリシー設定	グループポリシーの設定を行います。
3-8	アプリケーション配信設定	WVD によるアプリケーション配信設定を行います。
3-9	時間による自動起動・シャットダウン	時間管理型のスケールイン/アウトの設定を行います。
3-10	セッションホストの追加	既存の WVD に対して VM を追加します。
3-11	バックアップ設定	VM やプロファイル用ストレージのバックアップ設定を行います。
3-12	地理冗長設定	WVD の災対サイトを構築します。
3-13	Log Analytics 監視設定	WVD の状態を Log Analytics で確認できるように設定します。
3-14	Azure AD 条件付きアクセス設定	WVD に接続する際の Azure AD の設定を変更します。

※　作業内容に関連した設計が必要となります。

運用支援フェーズ メニュー

No	サービスメニュー	説明
4-1	クライアント環境導入サポート	WVD 用クライアントアプリケーションの配布およびインストールに関する支援を行います。
4-2	管理者向け QA 対応	構築後の管理者を窓口とした QA 対応を行います。対応期間と月ごとの想定対応件数（目安）を定めさせていただきます。
4-3	利用者マニュアル作成	WVD の利用者向けのマニュアルを作成します。
4-4	管理者マニュアル作成	WVD の管理に関するマニュアルを作成します。管理対象に応じて内容をカスタマイズします。
4-5	オンサイト トレーニング	WVD の使い方に関するオンサイト トレーニングを行います。
4-6	監視サポート	Azure や WVD のメトリックや死活の監視を行います。本メニューでは閾値または状態によるアラートのみを対象としています。
4-7	運用サポート	Azure や WVD の管理業務やメンテナンス対応などの定型の運用オペレーションを行います。
4-8	障害復旧サポート	Azure や WVD の障害時の原因切り分けや復旧、再発防止策の検討を行います。
4-9	PoC 検証サポート	WVD の PoC におけるお客様による検証作業を支援します。

※　作業内容に関連した設計および構築が必要となる場合があります。

その他オプション メニュー

No	サービスメニュー	説明
5-1	VM 稼動管理ツール	弊社で作成した VM 稼動管理ツールを導入します。
5-2	SysTrack 導入サポート	Lakeside Software 社の SysTrack を導入します。
5-3	SysTrack 運用サポート	Lakeside Software 社の SysTrack の運用を行います。
5-4	内製向け WVD 構築サポート	お客様による WVD 構築作業を支援します。設計レビューやアドバイザリーサポートなど要望に応じて対応内容をカスタマイズします。
5-5	WVD Spring Update 対応	2020 年 5 月以前に構築された WVD を Azure ポータルに対応した WVD にアップデート対応します。
5-6	プロファイル用ストレージ改善サポート	サインイン ストームなどプロファイル用ストレージに関する問題を解決します。WVD でご利用中のプロファイル用ストレージを最適な構成に見直します。必要に応じて WVD の利用状況を調査し、必要な IOPS やスループットを試算し、それに応じた構成に変更いたします。

オプションメニュー

個別説明

プロファイル用ストレージ改善サポート

WVD のサインイン ストームなどプロファイル用ストレージに関する問題を解決します
多くのケースでは Azure NetApp Files により解決することになります

サービス提供価格（参考）
60 万円～
※　WVD の規模により異なります
※　Azure 料金はお客様のご負担となります

含まれる作業
- 既存構成の簡易調査（ヒアリングなど）
- 新しいプロファイル用ストレージの構築
- FSLogix 設定支援
- 導入後の 2 週間程度の最適化支援

オプション
- 必要なパフォーマンスの詳細分析（構成を踏まえて IOPS やスループットの分析）
- 仮想マシン構成コンサルティング
- プロファイル用ストレージ移行
- Azure NetApp Files のボリュームのオートスケール
- その他構成変更（バックアップや冗長化等）

お客様対応作業
- 既存構成に関する情報提示
- FSLogix の GPO 等への設定

納品物
- 作業報告書

免責事項
- 本サービスはストレージのパフォーマンスを対象に改善を支援する準委任作業となります。仮想マシンなどストレージ以外が原因がある場合には必ずしもパフォーマンスが改善されない場合があります。


只今、休憩時間です。
再開は13:00を予定しています。

PERSOL

Microsoft Partner
Microsoft
Gold Cloud Platform
Gold Cloud Productivity
Gold Security
Gold Application Development
Gold Collaboration and Content

Windows Virtual Desktop In a Day workshop

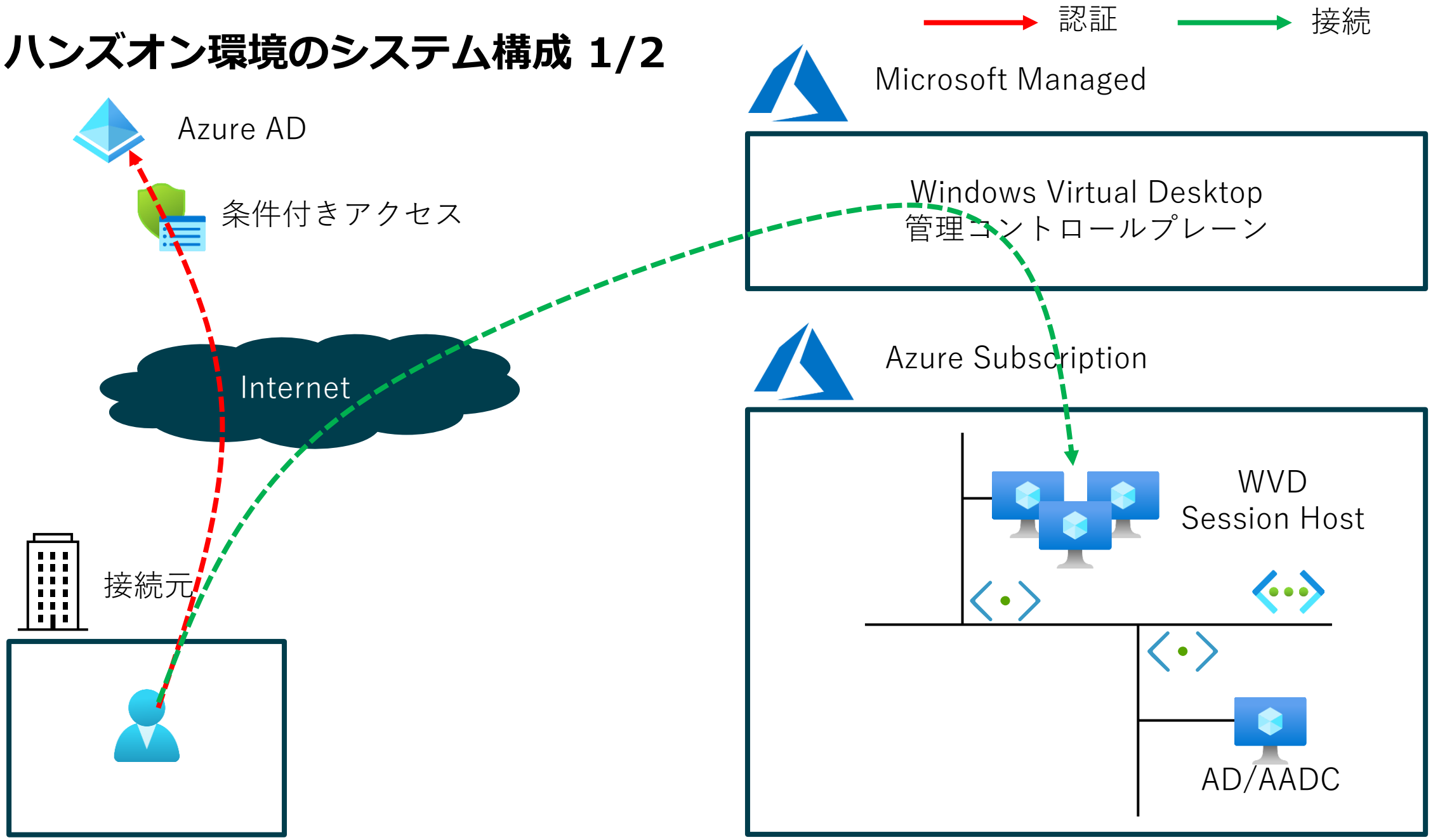
パーソルプロセス＆テクノロジー株式会社
DXソリューション統括部
PFソリューション部

ユーザーIDとパスワード

- ユーザーID：皆様のメールアドレスの@より前をご利用ください。
  @以降は、「poc.hogeda.com」としてください。
  例：メールアドレスが「kyohei.uchida@persol.co.jp」の場合は、
  「kyohei.uchida@poc.hogeda.com 」となります。

- パスワード：Ppt#20201210

ハンズオン環境のシステム構成 1/2



ハンズオン環境のシステム構成 2/2

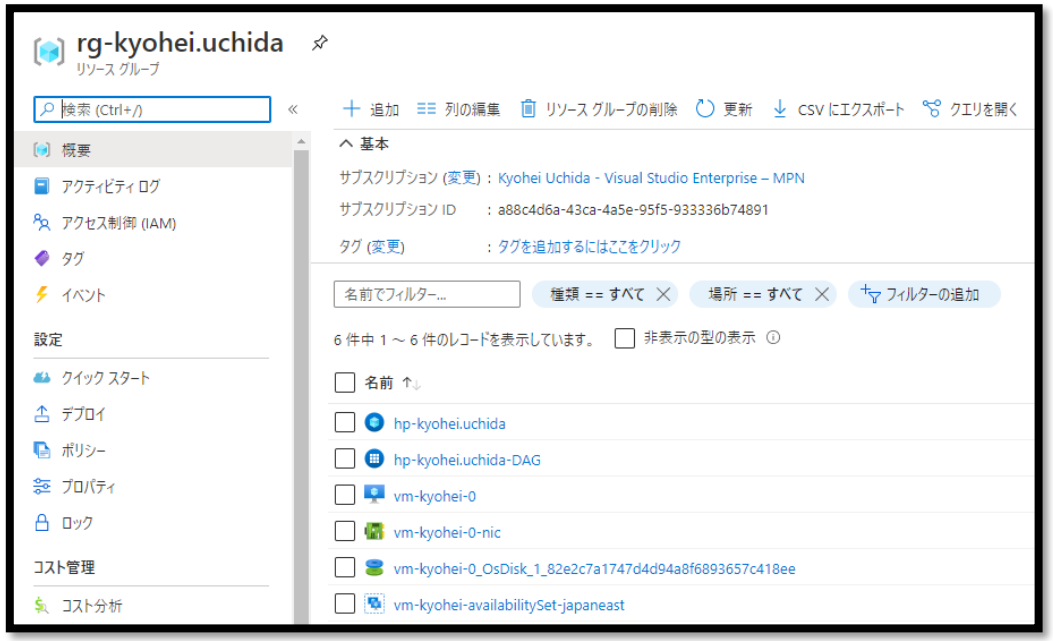
- パーソルが用意した環境と、皆様がご自由に触れる環境があります。

rg-workshop

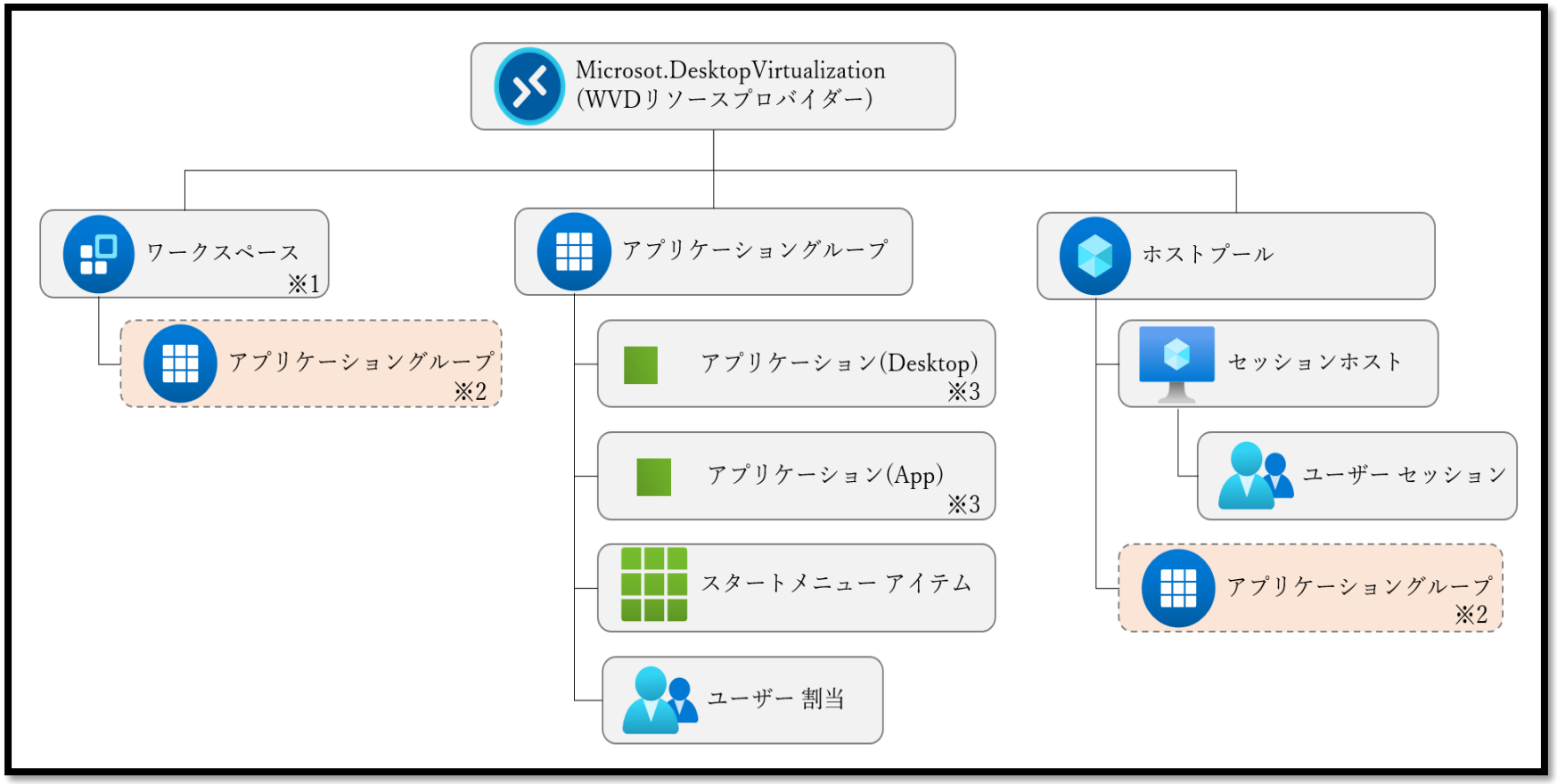
パーソル環境：デモに使用

rg-<名前>

ハンズオン環境：ご自由に触れます



Windows Virtual Desktop 管理領域のアーキテクチャ



※1:ユーザーはワークスペースにアクセスし、自分に割り当てられたアプリケーショングループをフィードする。
※2:ワークスペースとホストプールには、アプリケーショングループを関連付ける。
※3:スタートメニュー アイテムの中からアプリケーションを選択する。

1. WVDへの接続

WVDへの接続（ハンズオン内容）

実際にWVDにアクセスいただき、ユーザーがどのように利用するのかご確認ください。

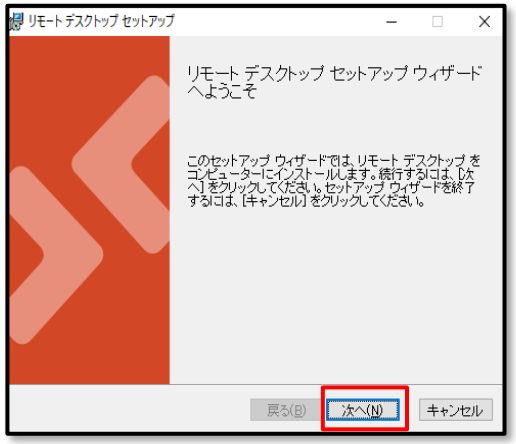
- 専用アプリケーション(Windows)のインストール
- 専用アプリケーションからの接続
- Webブラウザからの接続

デスクトップアプリからの接続

WVDの接続（デスクトップアプリ）

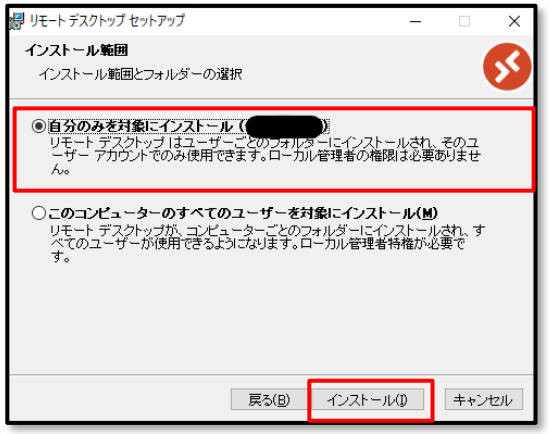
1. 以下URLからWVDクライアントアプリケーションをインストール。
   https://go.microsoft.com/fwlink/?linkid=2068602

①

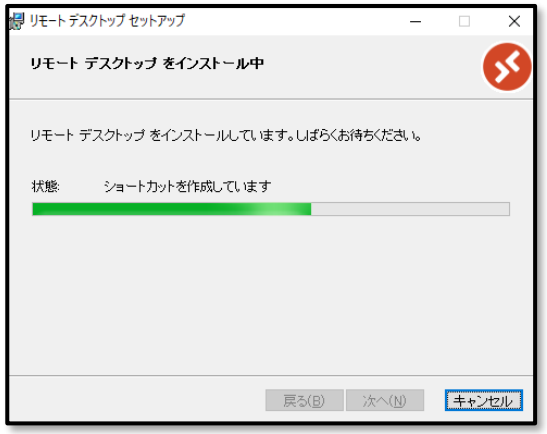


②

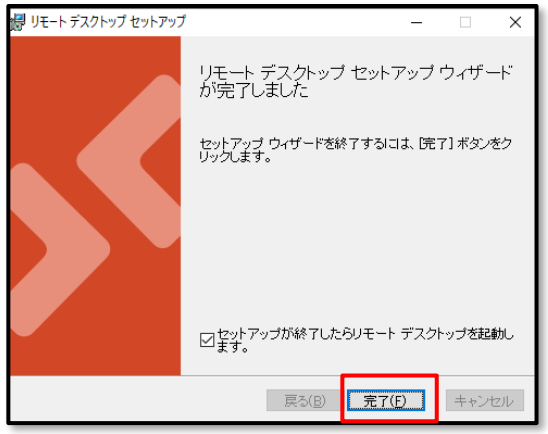
③



④

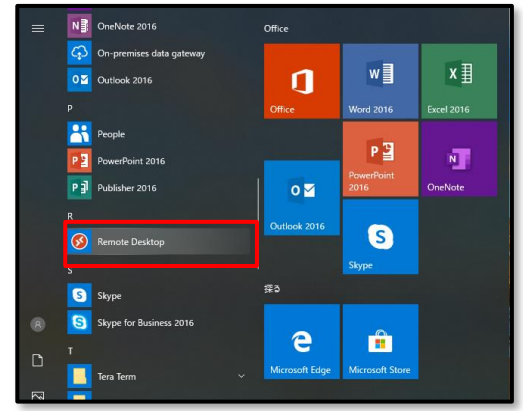


⑤



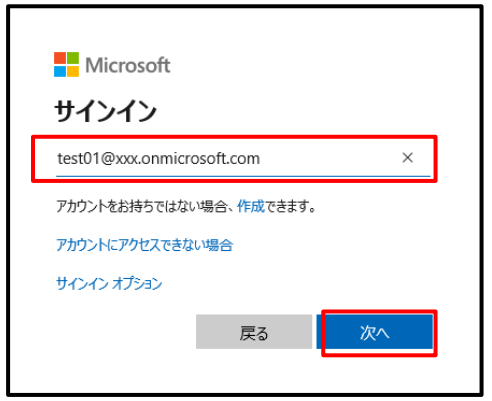
WVDの接続（デスクトップアプリ）

2. インストール完了後、ホーム画面から
「Remote Desktop」をクリック。



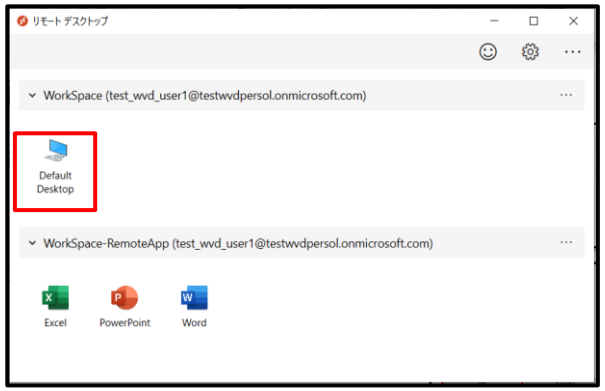
3. WVDのクライアントアプリ起動後、
右記画面が表示されるので、
「登録」をクリック。

4. 右記サインイン画面が表示されるので、
次のページに紹介するユーザーでログイン。
次回からこの認証はスキップされる。

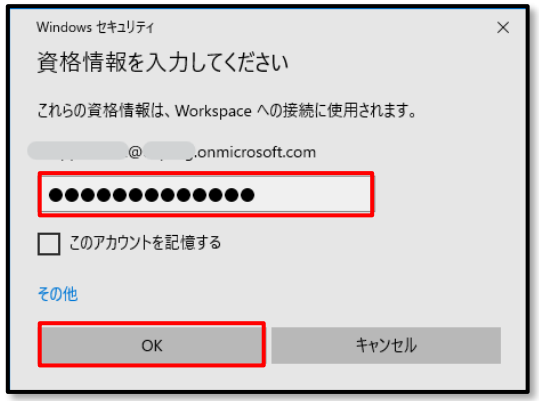


WVDの接続（デスクトップアプリ）

5. サインイン完了後、右記画面が表示されるので、
対象のリモートデスクトップをクリック。



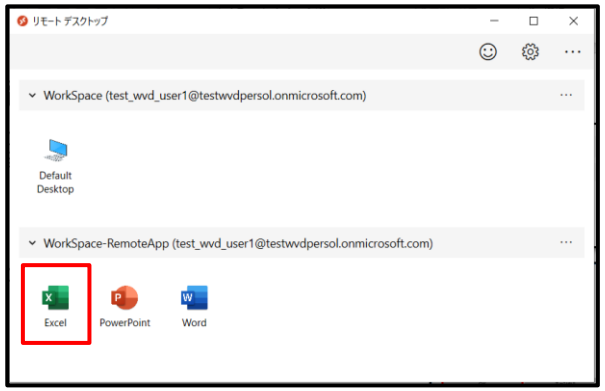
6. 右記サインイン画面が表示されるので、
4. で入力したパスワードと同じものを入力。



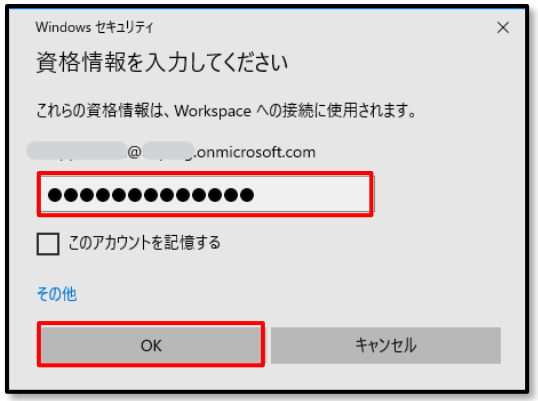
7. 右記のようにデスクトップ画面が
表示されたら、成功。

WVDの接続（デスクトップアプリ）

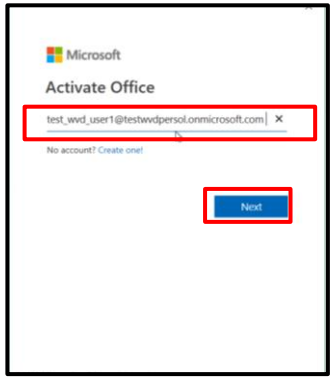
8. 続いて、右記画面から、
リモートアプリ(今回はExcel)をクリック。

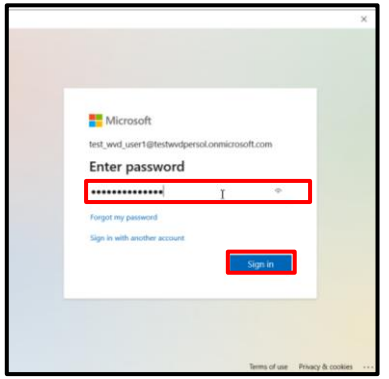


9. 右記サインイン画面が表示されるので、
4. で入力したパスワードと同じものを入力。



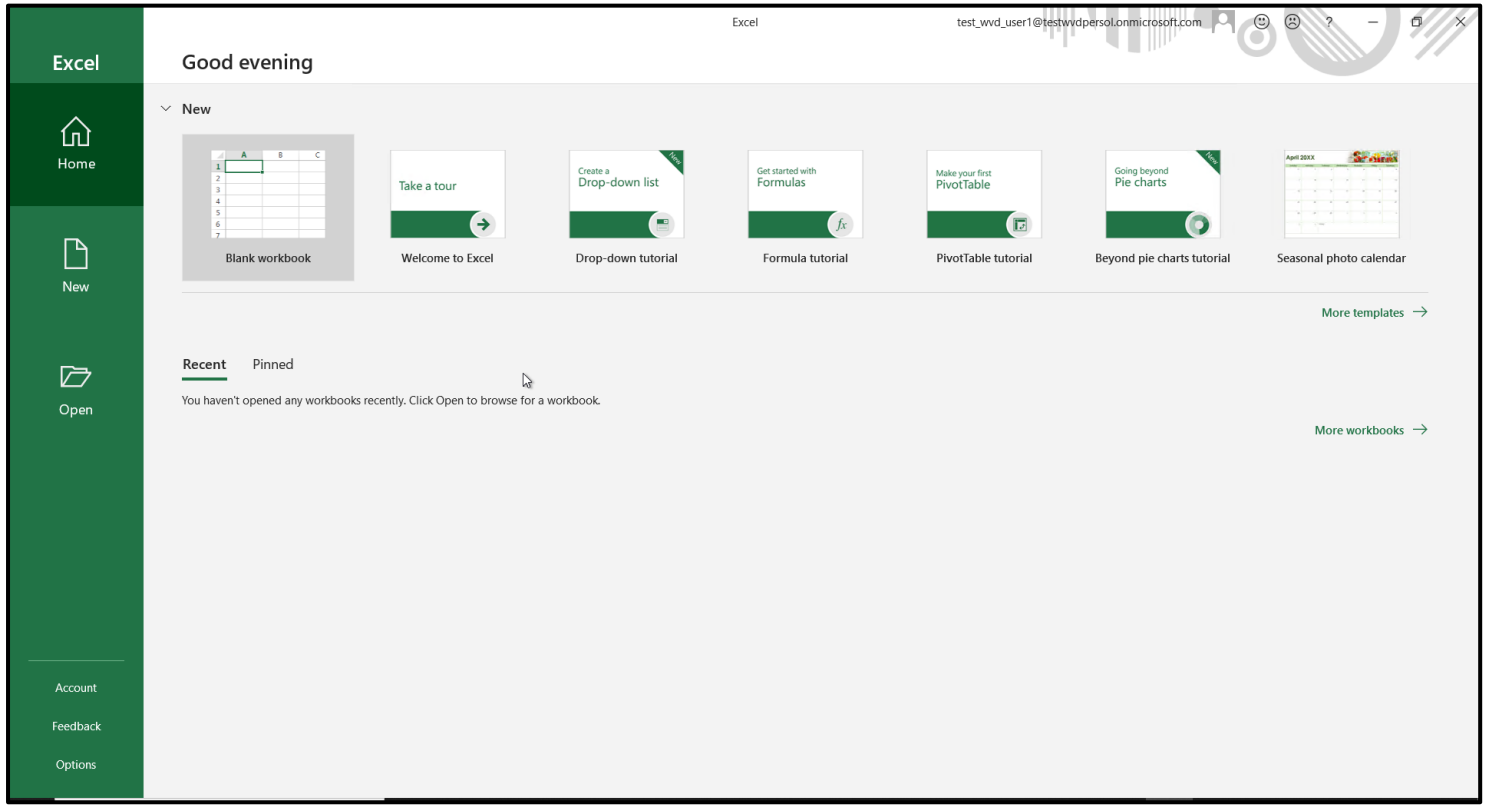
10. 右記サインイン画面が表示されるので、
4. で入力した認証情報と同じものを入力。





WVDの接続（デスクトップアプリ）

11．右記のようにExcelの画面が表示されたら、成功。

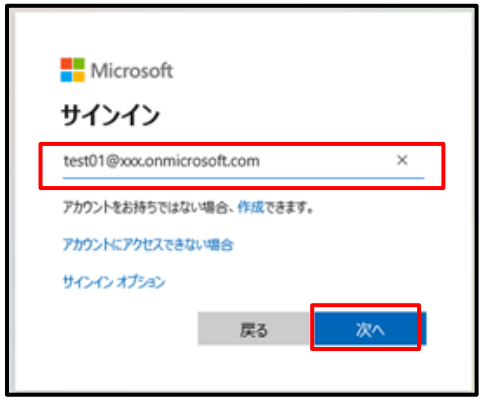


ブラウザアプリからの接続

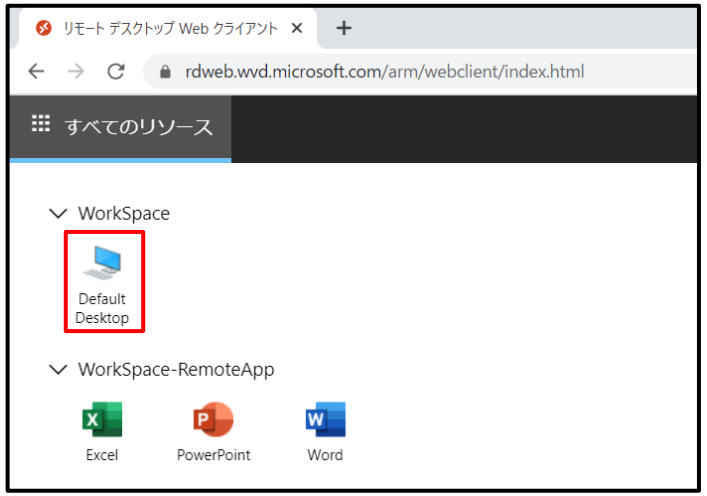
WVDの接続（ブラウザアプリ）

1. 端末のブラウザを起動し、以下URLにアクセス。
   https://rdweb.wvd.microsoft.com/arm/webclient

2. 右記サインイン画面が表示されるので、
   前のページと同様の認証情報を入力。



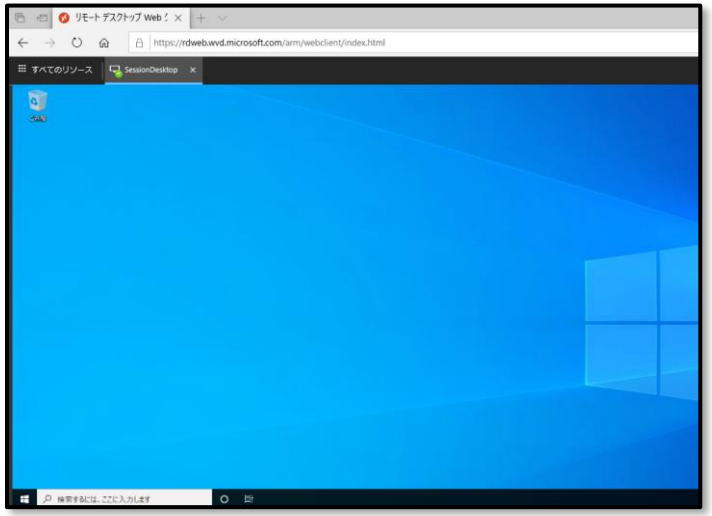
3. サインイン完了後、右記画面が表示されるので、
   対象のリモートデスクトップをクリック。



WVDの接続（ブラウザアプリ）

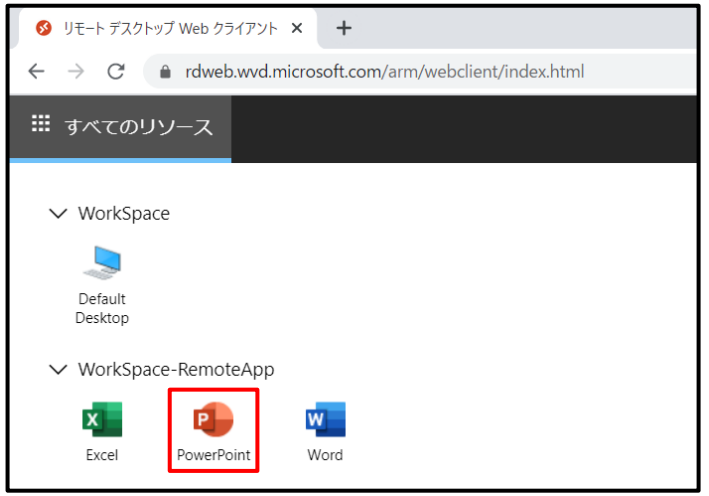
4. 右記サインイン画面が表示されるので、
2. で入力した認証情報と同じ情報を入力。
※但し、ユーザ名については、ドメイン名を
Azure ADのものではなく、
オンプレADのドメインを指定すること。

5. 右記のようにデスクトップ画面が
表示されたら、成功。



WVDの接続（ブラウザアプリ）

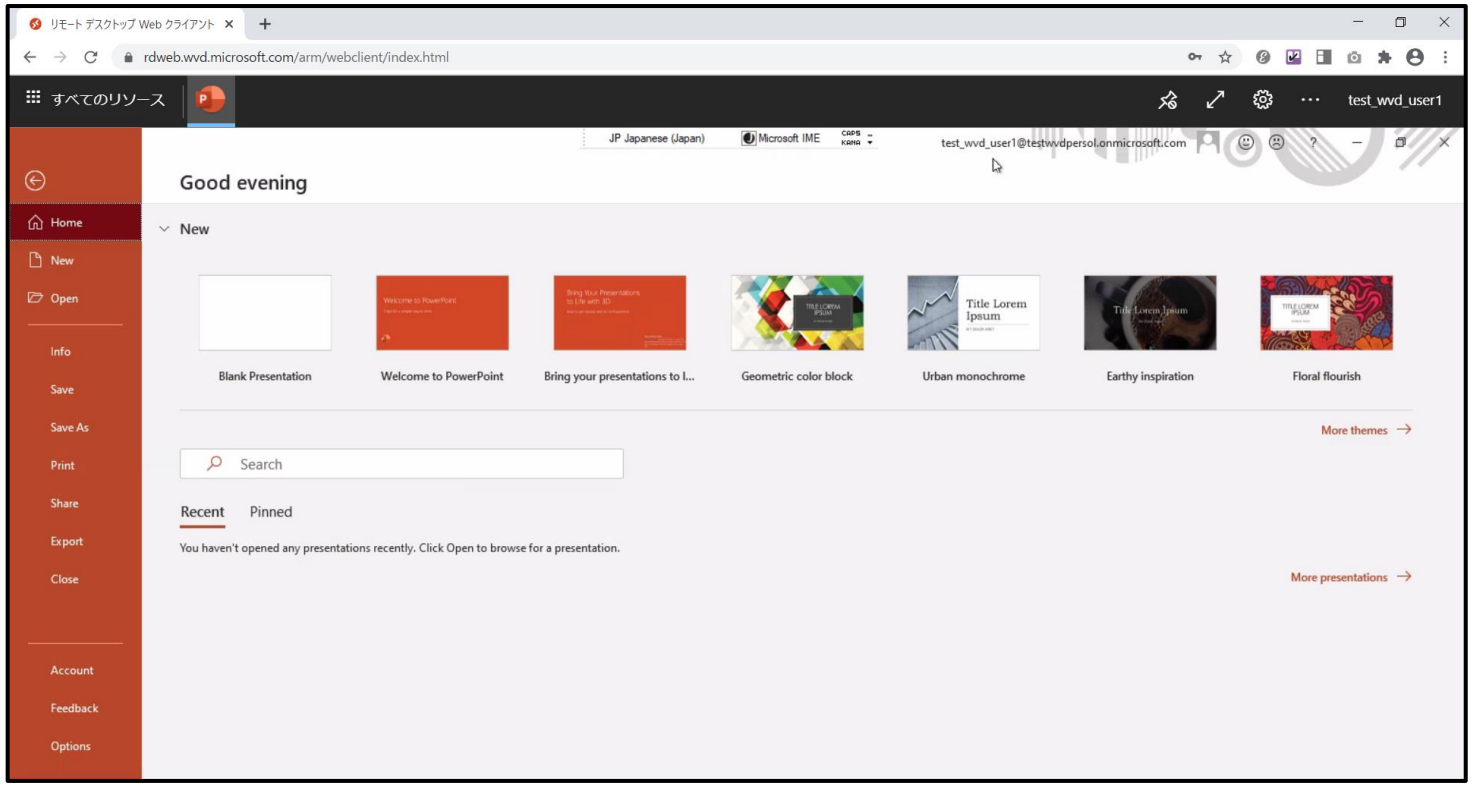
6. 続いて、右記画面から、
リモートアプリ(今回はPowerPoint)をクリック。



7. 右記サインイン画面が表示されるので、
2. で入力した認証情報と同じ情報を入力。
※但し、ユーザ名については、ドメイン名を
Azure ADのものではなく、
オンプレADのドメインを指定すること。

WVDの接続（ブラウザアプリ）

8.　右記のようにPowerPointの画面が表示されたら、成功。



2. 基本操作

ユーザの割り当て

ユーザ割り当て（ハンズオン内容）

ハンズオン環境のホストプールにご自身のアカウントを割当てます。設定の前後で表示が異なることをご確認ください。

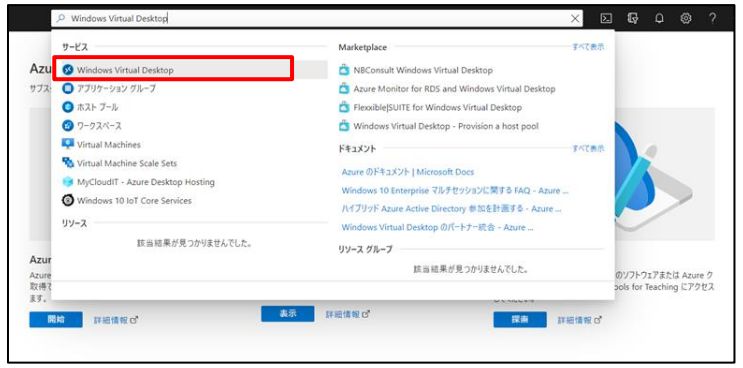
・ユーザの割り当てを設定する場所を確認。

・ユーザの割り当てを実施。
→割り当てたユーザでログインし、ログイン可能なことを確認。

・ユーザの割り当て解除を実施。
→割り当て解除したユーザでログインし、ログイン不可なことを確認。

各種WVDリソースへのユーザ割り当て

1. Azureポータル画面から
「Windows Virtual Desktop」と検索し、
表示されたその項目をクリック。

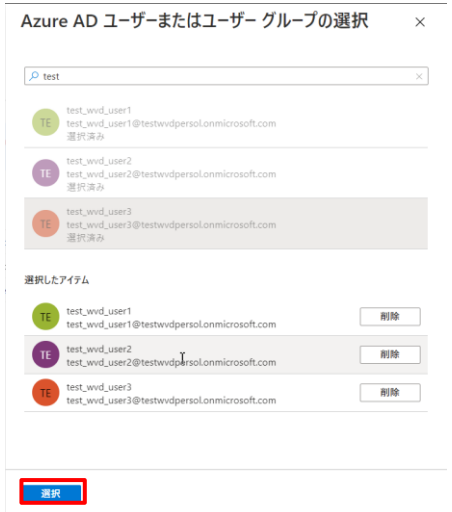


2. 右記画面が表示されるので、
「アプリケーショングループ」
→「<ホストプール名>＋'-DAG'」
をクリック

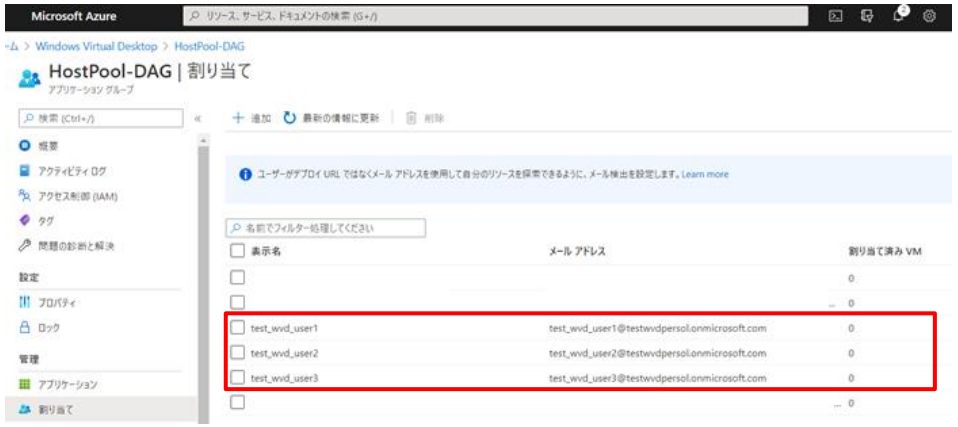
3. 右記画面が表示されるので、
「割り当て」→「追加」をクリック

各種WVDリソースへのユーザ割り当て

4. 右記画面が表示されるので、
   追加するユーザを追加し、「選択」をクリック。
   ※オンプレミスからAzureADへ
   同期されたユーザーを選択すること。
   ここで追加可能なユーザ全てがWVDで
   使用できわけではないので注意。

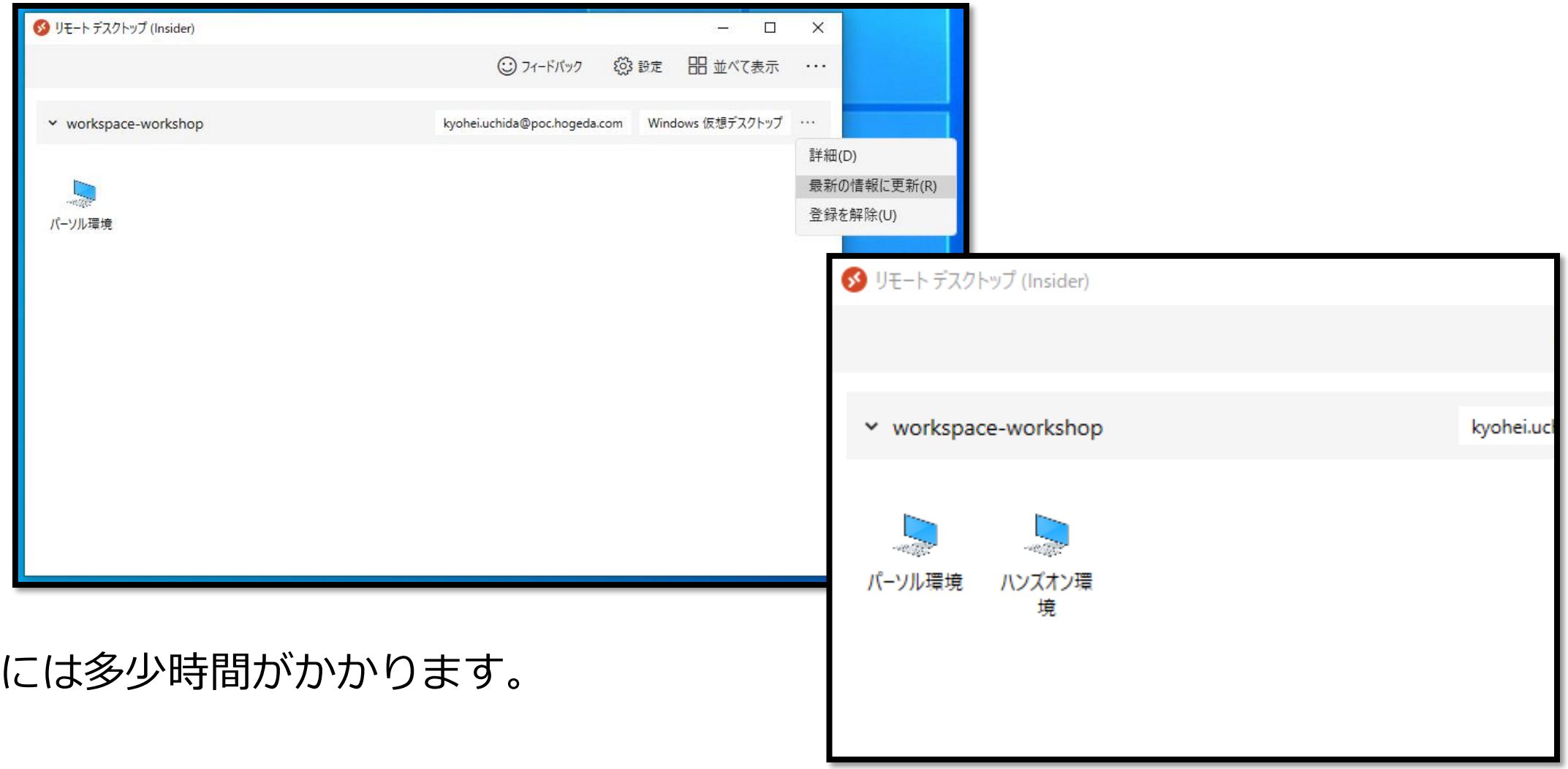


5. 右記画面のようにユーザが追加されたら成功。



各種WVDリソースへのユーザ割り当て

- 設定が反映されていることを確認

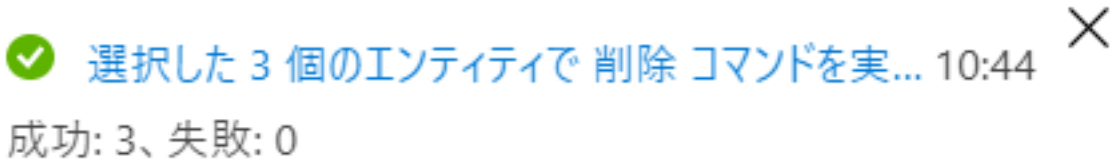


※反映には多少時間がかかります。

各種WVDリソースへのユーザ割り当て

6. 右記画面に遷移、割り当て解除対象の
ユーザにチェックを入れ、
「削除」→「OK」をクリック。

7. 右記ポップアップ画面が表示されたら成功。



ホストプールの設定変更

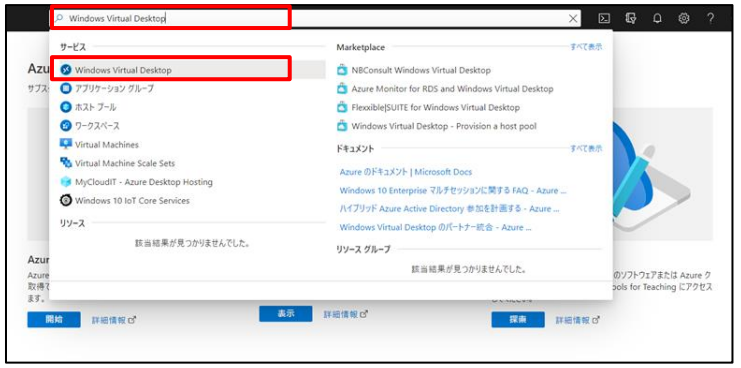
ホストプールの設定変更（ハンズオン内容）

ホストプールの設定を変更し、ユーザーの操作が制限されることをご確認ください。

・ホストプールの設定を変更する場所を確認。
・RDPプロパティの設定。
　クリップボードのリダイレクトの禁止。
　→設定後、各ユーザーがクリップボードを使えないことを確認。

ホストプールの設定

1. Azureポータル画面から
「Windows Virtual Desktop」と検索し、
表示されたその項目をクリック。



2. 右記画面が表示されるので、
「ホストプール」
→対象のホストプールをクリック

3. 右記画面が表示されるので、
「プロパティ」をクリック

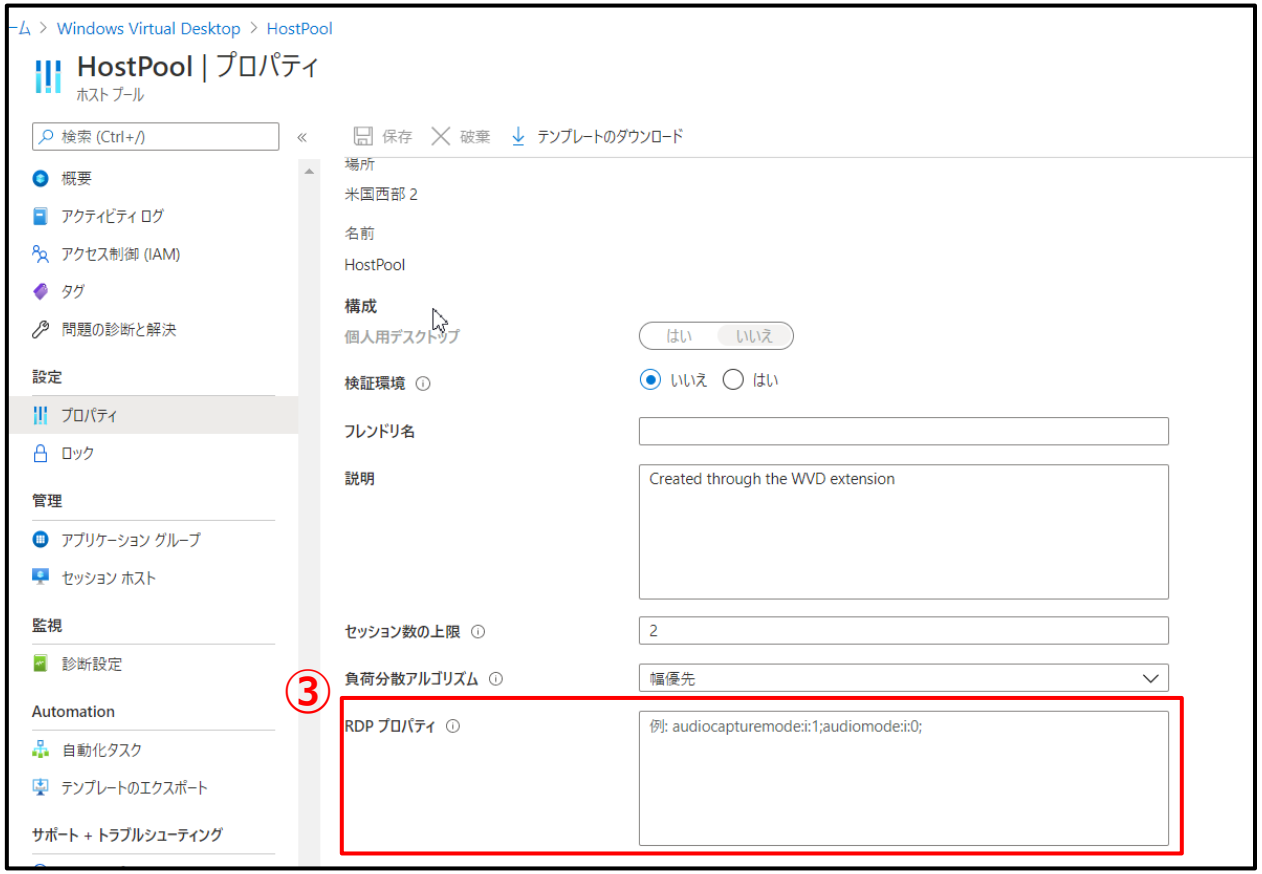
ホストプールの設定

4. 右記画面が表示される。
   ここでは、以下内容などを設定可能

① セッション数の上限
セッションホスト1台に
ログインできるユーザ数の上限

② RDPプロパティ
以下を制御可能。
・リダイレクト
(USB,クリップボード,プリンター)
・マルチモニター
・画面サイズ
・帯域幅　など

詳細な設定内容については以下を参照
(https://docs.microsoft.com/ja-jp/windows- server/remote/remote-desktop-services/clients/rdp-files)




只今、休憩時間です。
再開はHH:MMを予定しています。

3. 管理系操作

条件付きアクセス（多様素認証）

条件付きアクセス（ハンズオン内容）

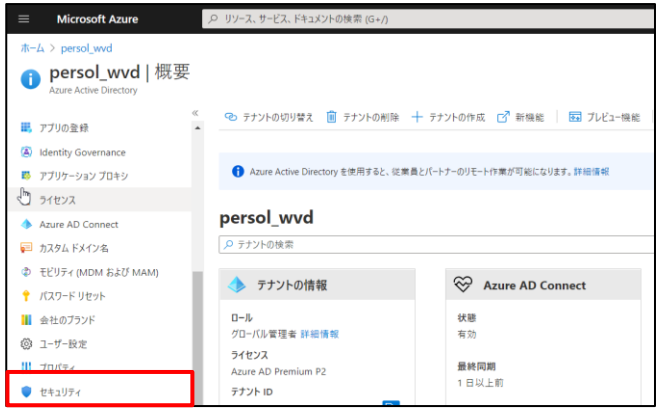
Azure ADの条件付きアクセスを構成し、WVD接続時に多要素認証を要求されることをご確認ください。なお、条件付きアクセスの設定変更は弊社にて実施いたします。

・条件付きアクセスを設定する場所を確認。
・条件付きアクセスを用いて、特定のユーザに多要素認証を要求するよう設定
→設定後、各ユーザーで多要素認証が実施されることを確認。

条件付きアクセス（手順の紹介になります）

1. Azureポータル画面から
「Azure Active Directory」と検索し、
表示されたその項目をクリック。

2. 右記画面が表示されるので、
「セキュリティ」→
「条件付きアクセス」をクリック



3. 右記画面が表示されるので、
「新しいポリシー」をクリック

条件付きアクセス（手順の紹介になります）

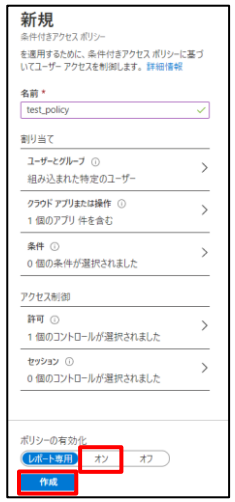
4. 右記画面が表示されるので、
以下のように設定。

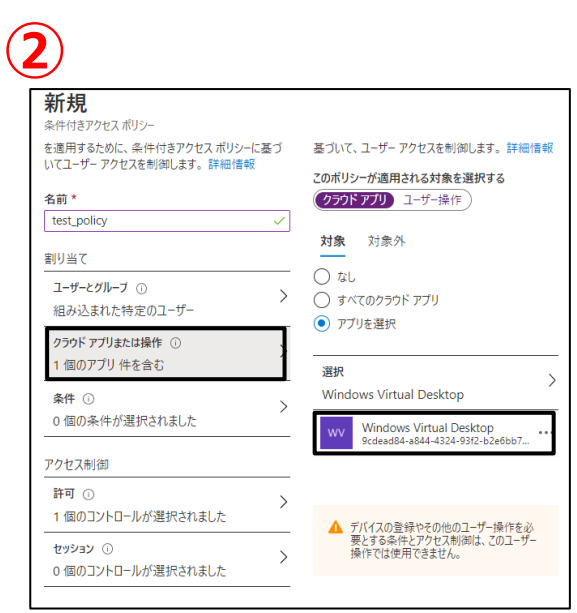
①「ユーザとグループ」で
対象ユーザーを追加。

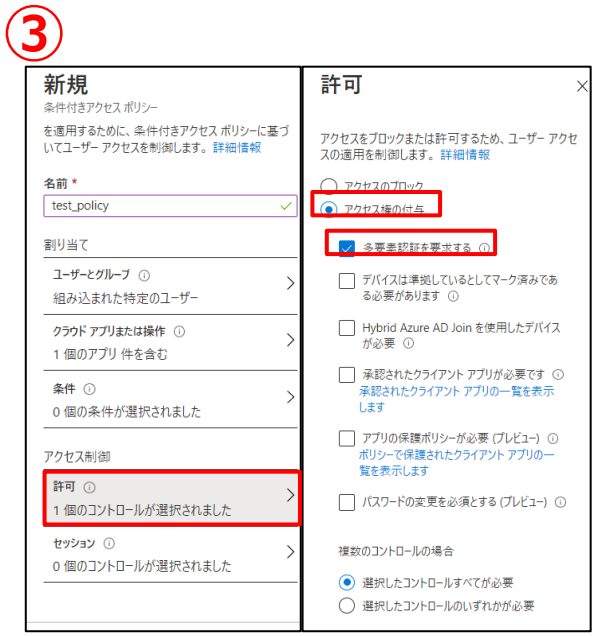
②「クラウドアプリまたは操作」で
「Windows Virtual Desktop」を追加。

③「許可」で「アクセス権の付与」と
「多要素認証を要求する」をチェック。

④ 一番下にある「ポリシーの有効化」を
「ON」に設定し、「選択」をクリック。



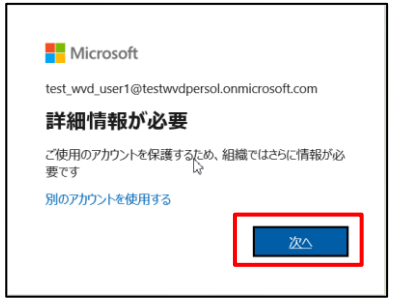




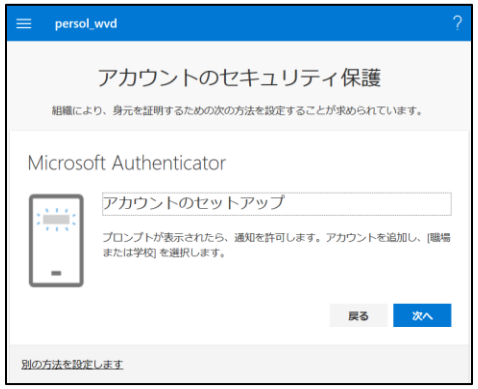
条件付きアクセス（手順の紹介になります）

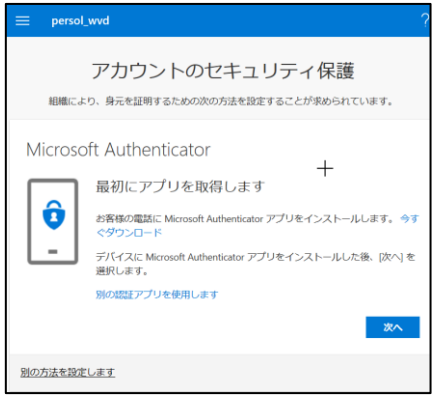
5. 以下画面のように表示されたら、成功。

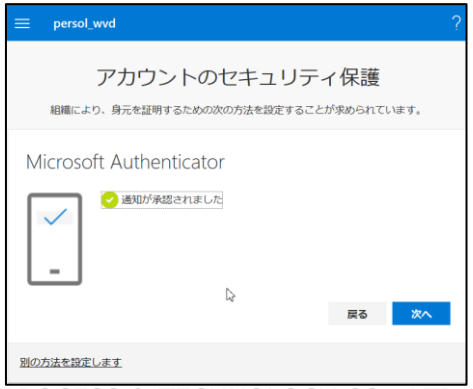
6. WVDクライアントアプリケーションから
再度登録を実施すると、右記画面が表示されるので、
「次へ」をクリック。

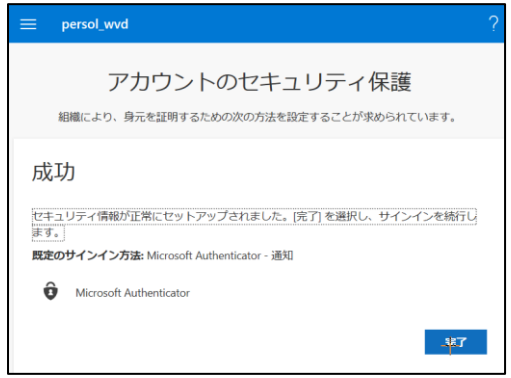


7. 多様素認証時に使用する「Microsoft Authenticator」のセットアップ画面に遷移するので、記載されている内容に従って、セットアップを完了させる。









自動スケール

稼働管理の必要性

WVDランニングコスト：

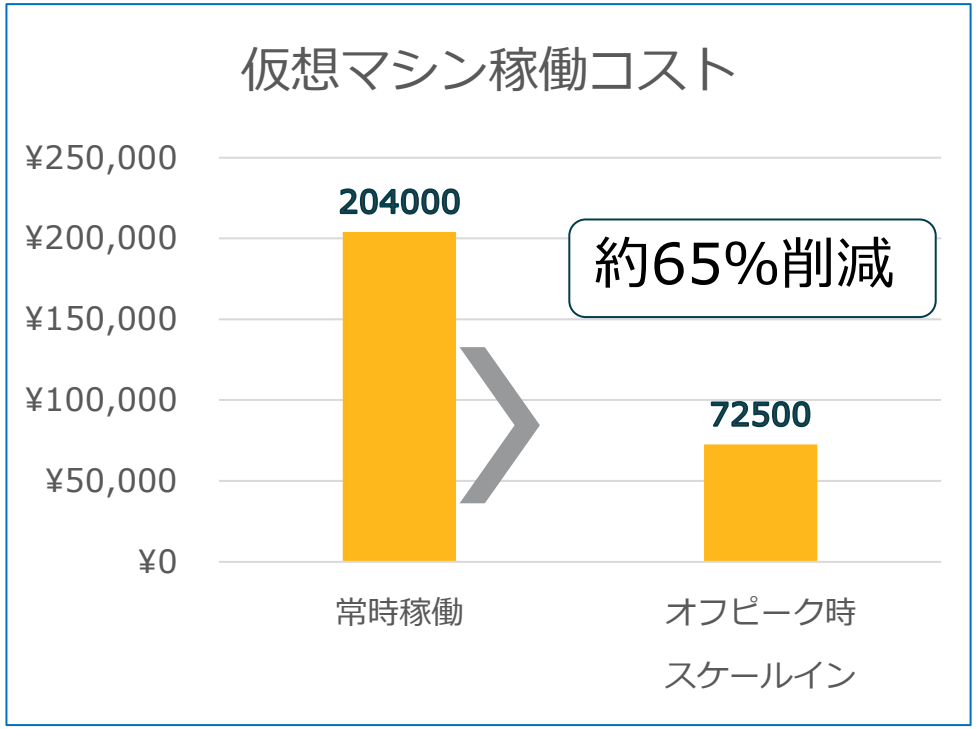
・ライセンス

・ストレージ

・ネットワーク

・仮想マシン

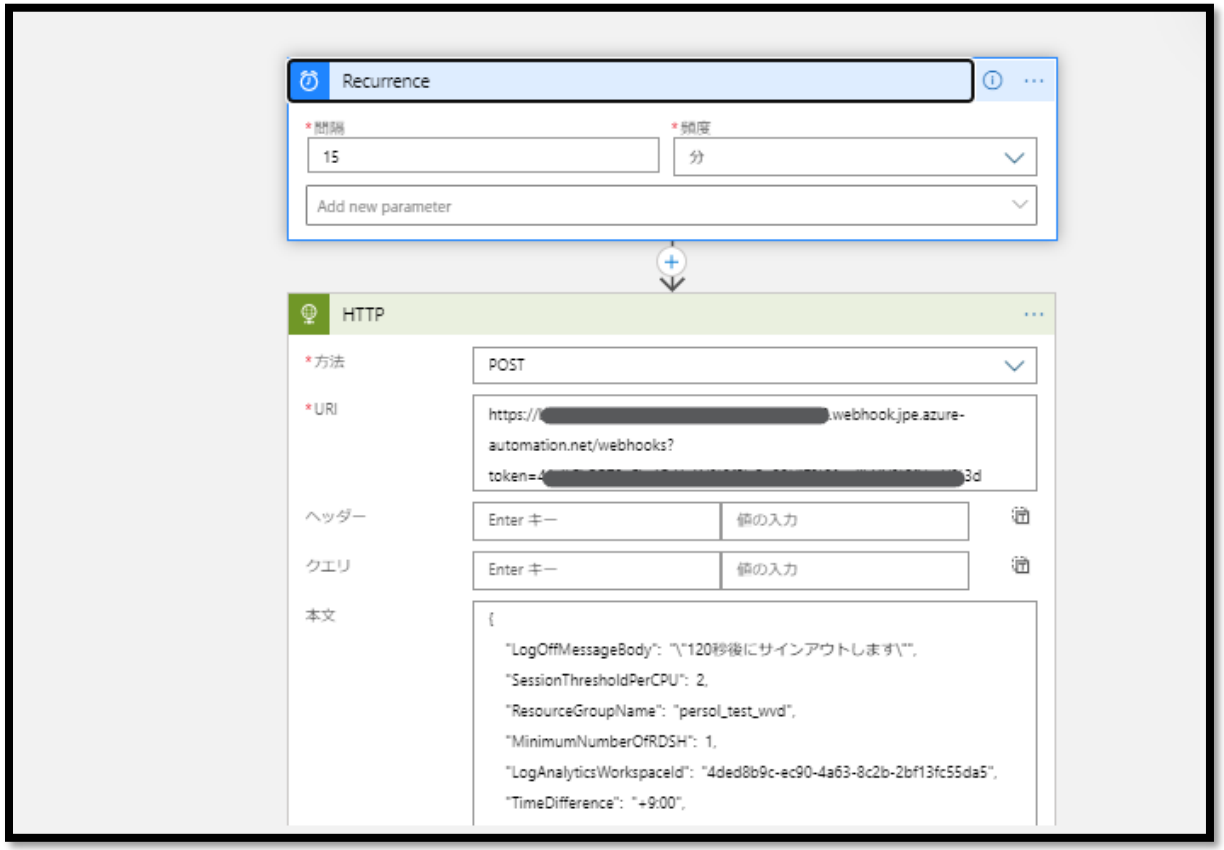
← ・コストの大部分を占める
・時間単位で従量課金
：コスト削減の余地が大きい



※仮想マシンサイズD4sv3（4vcpu16GB）
100ユーザ
vcpuあたり2セッションを想定
ピーク時間を220時間/月とし、
オンピークには全ユーザが使用
オフピーク時はユーザの５%が利用する想定
（オンピーク→オフピークで13台→1台にスケールイン）

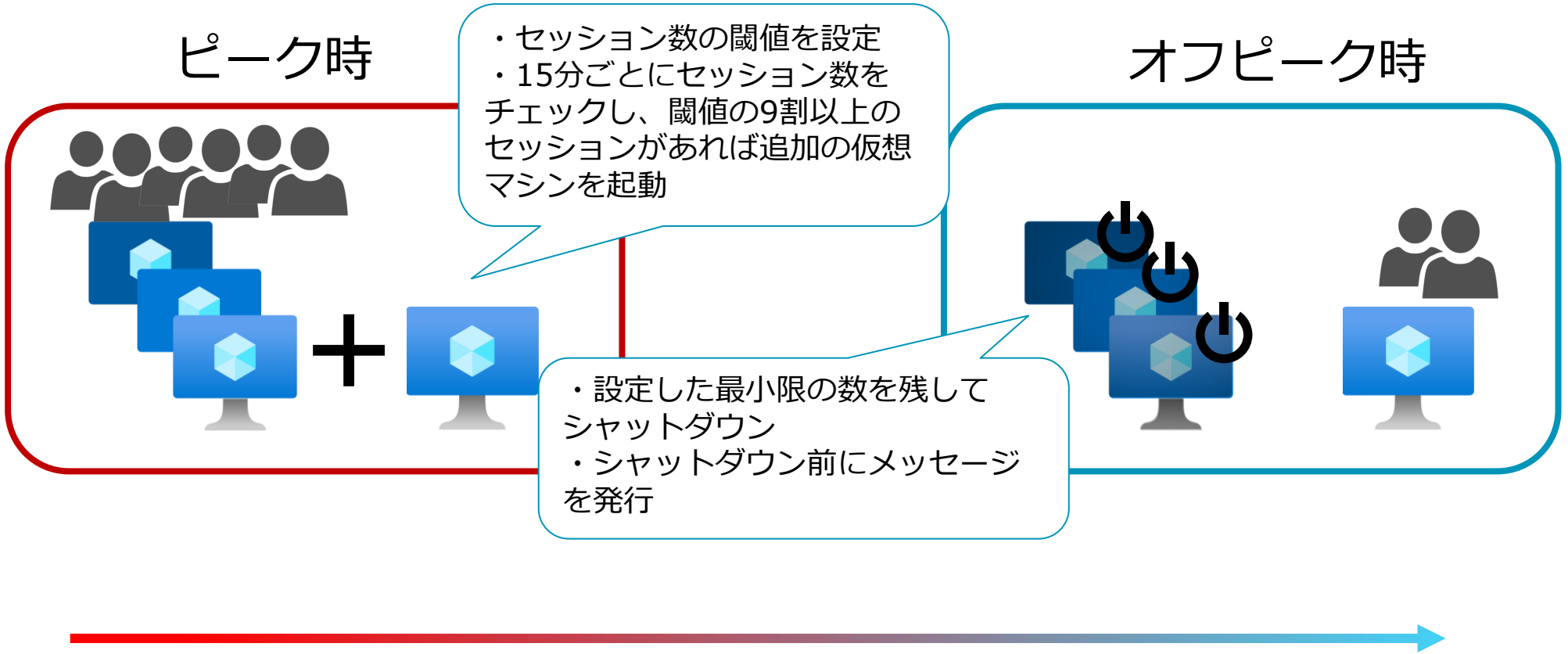
自動スケールソリューション

- Microsoft公開のWVDスケーリングツールが利用可能
- Azure Automation＋Webhook＋Logic App
- による稼働管理サービスを簡単に構築可



自動スケールソリューションの仕様

- ピーク時間の設定にもとづき、仮想マシンの起動停止をスケジュール
- ・ピーク時はコアCPUごとのセッション数に応じてスケールアウト
- ・ピーク時以外は最小限の数の仮想マシンのみ起動



自動スケール（ハンズオン内容）

パーソル環境のWVDに接続いただき、セッション数が閾値を超えた時のオートスケール動作をご確認ください。

なお、設定変更は弊社にて行います。（設定画面を閲覧することは可能です）

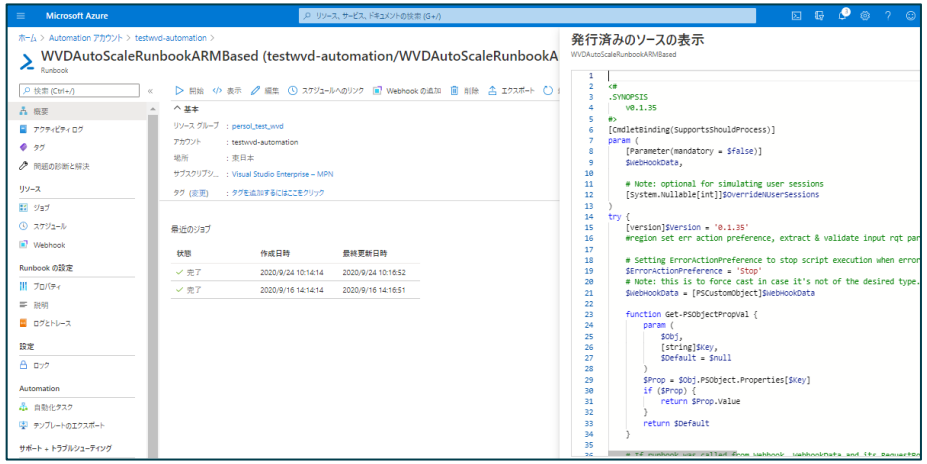
- 自動スケールツールを設定する場所を確認
- 自動スケールツールの動作内容を確認
  →有効化後に、仮想マシンの電源状態が自動的に変更することを確認

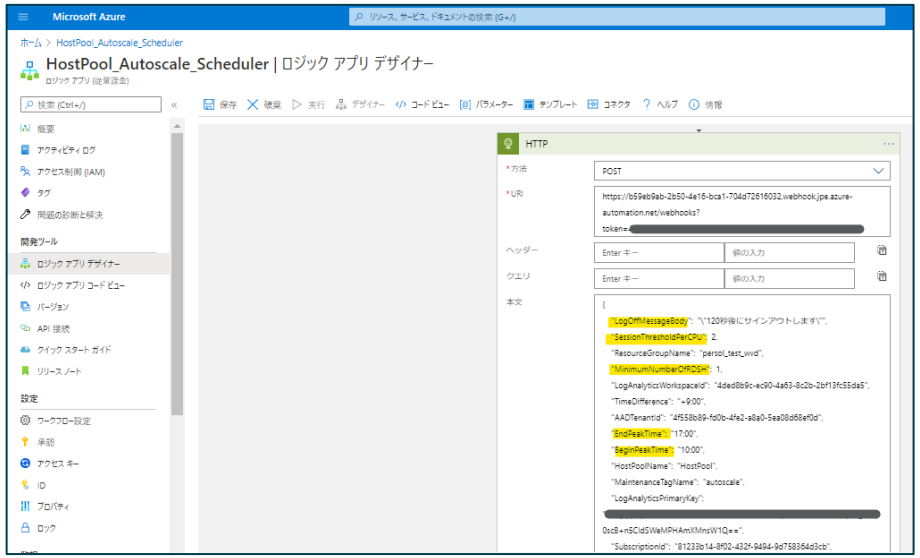
自動スケールツール（手順の紹介になります）

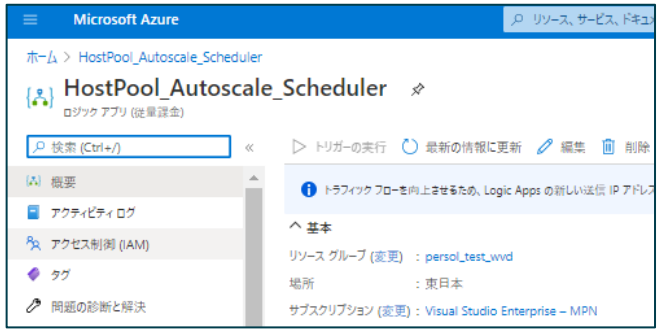
１．Automation確認
（WVDAutoScaleRunbookARMBased）

２．Logic App確認
（Hostpool_Autoscale_Scheduler）
[ロジックアプリデザイナー]から
ピーク時間やメッセージ等設定可能

３．Logic App トリガー手動実行
ピーク時、オフピーク時において
設定通りの動作確認







ログ・監視

WVDパフォーマンス監視

WVD運用で考慮すべき事項

- 稼働状況
- サインイン状況
- CPU負荷
- ネットワーク
- ディスクIO、スループット、・・・

→Log Analyticsで一元的にログを管理
→Azure Monitorで監視を構成

ログ・監視（ハンズオン内容）

WVDにおけるログ・監視サービスの実装方法についてご確認ください。
なお、設定変更は弊社にて行います。（※クエリを発行することは可能です）

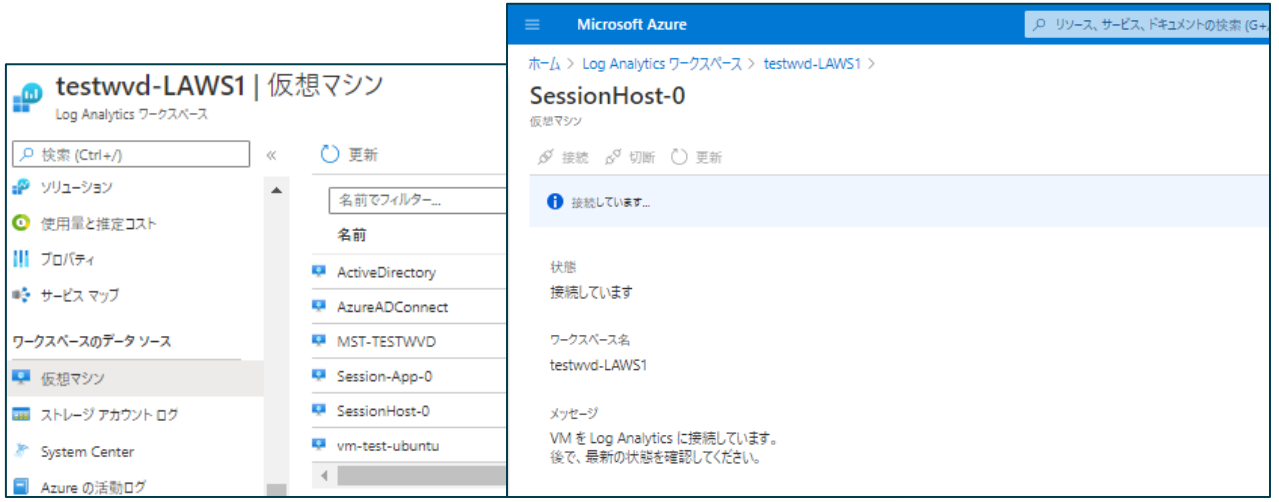
- ログ・監視の構成方法の確認
- ログの閲覧
  →Log Analyticsにて検索クエリを発行し、どのようにログを閲覧することができるかを確認
  →ダッシュボードにピン止めして、一覧表示する方法を確認

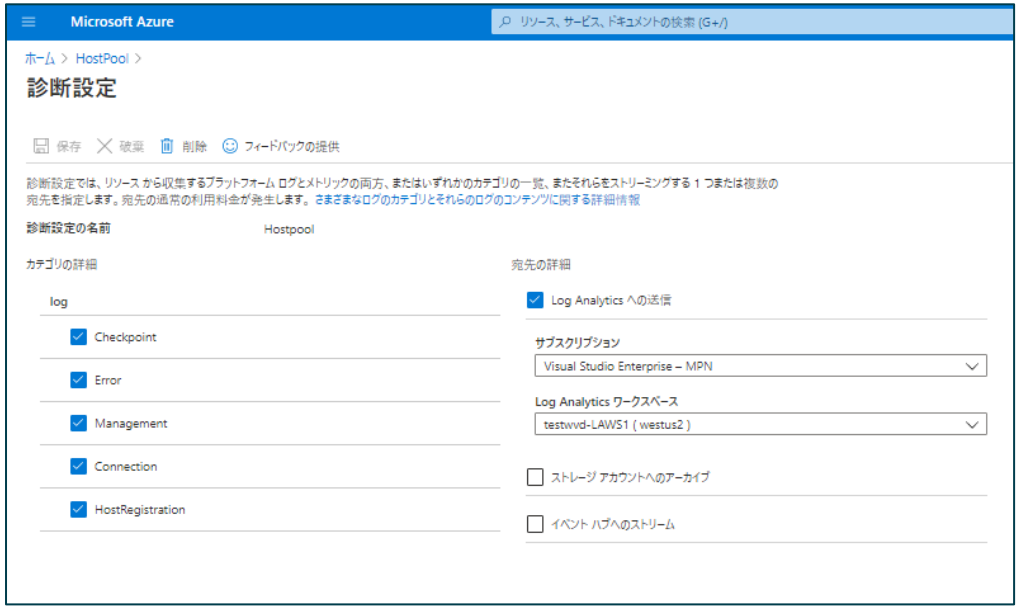
構成手順（手順の紹介になります）

1. Log Analytics ワークスペースを作成

2. ワークスペース>データソース>
仮想マシンから監視対象の
セッションホストVMを接続

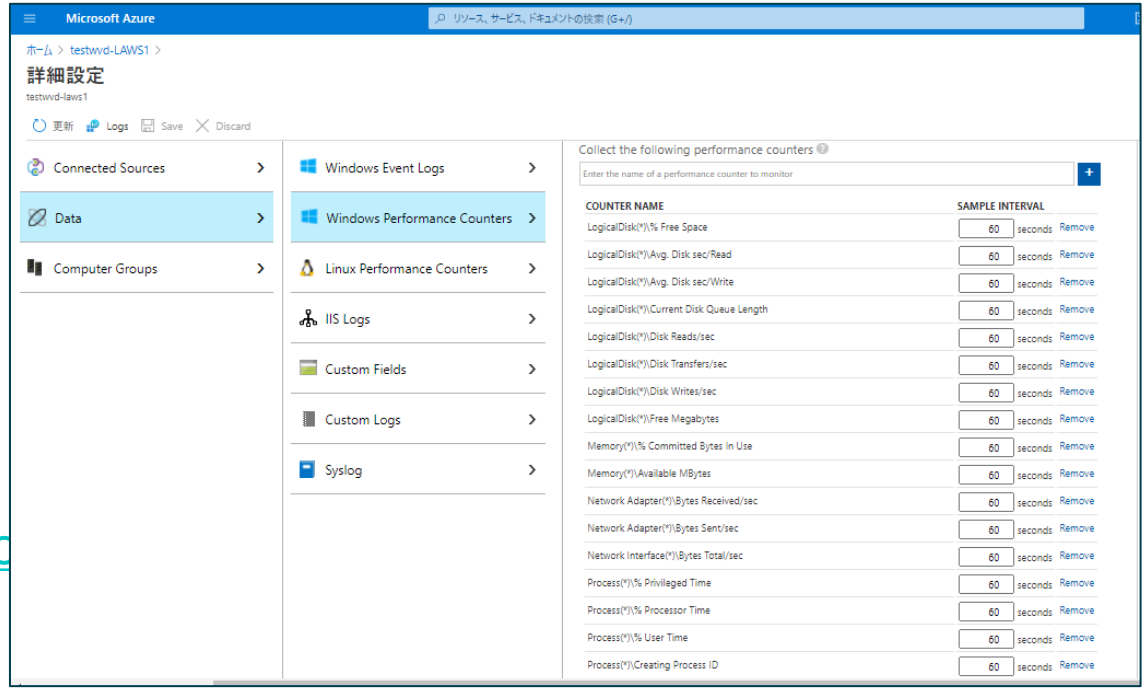
3. 監視対象のホストプール画面で
[診断設定]をクリックし、
ログを有効化





構成手順（手順の紹介になります）

4. パフォーマンスカウンターを登録
詳細設定>Data>Windows Performance Counter
から論理ディスクや
ネットワークインターフェイス、
ターミナルサービスの
パフォーマンスカウンターを設定



参考：Windowsパフォーマンスカウンター
https://docs.microsoft.com/ja-jp/azure/azure-mo
counters#windows-performance-counters

ログの検索

1. Log Analytics Workspaceにアクセスします。
2. ログを開きます。
3. クエリを選んで、フィルターから「カテゴリ：Windows Virtual Desktop」を選択。

ログの検索

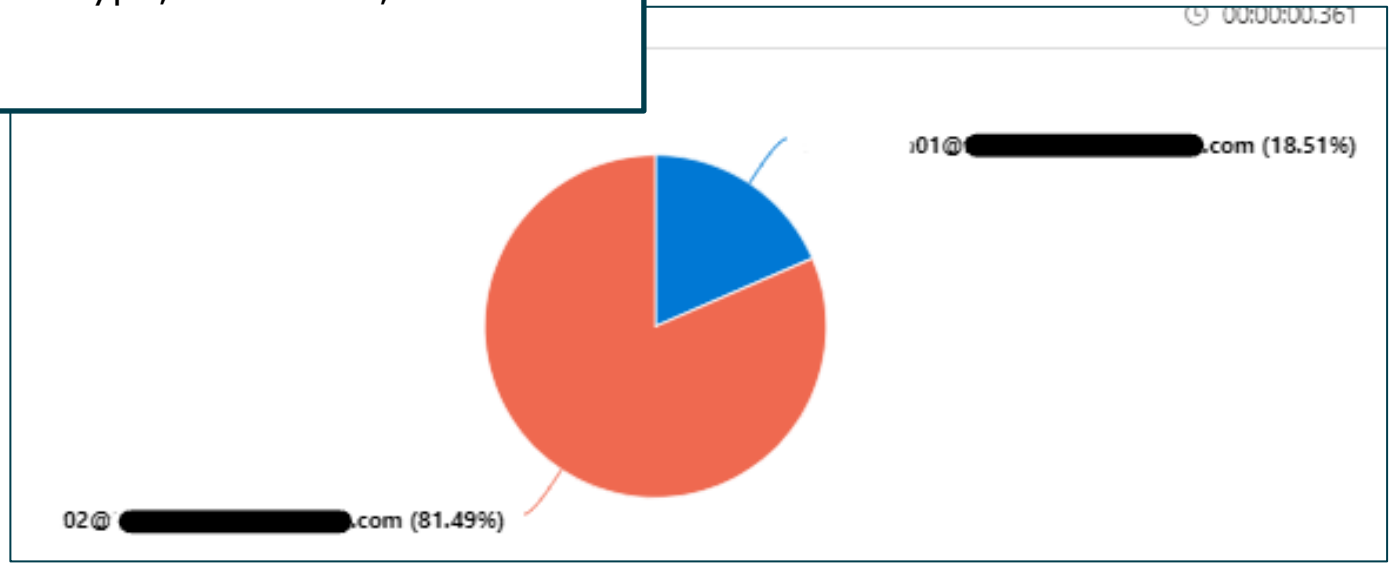
4. サンプルクエリを選択して実行します。
5. クエリをカスタマイズして、保存することも可能です。

ログクエリ（サンプル）：WVD使用状況

- クエリ対象：ユーザーサインイン状況

ログクエリ：ユーザー別合計セッション時間

```
WVDConnections
|where TimeGenerated >ago(1d)
|where State == “Connected”
|Project CorrelationId, username, ConnectionType, StartTime=TimeGenerated
|Join (WVDConnections
            | where State == “Completed”
            | project EndTime = Timegenerated, CorrelationId)
            on  CorrelationId
|Project Duration = (EndTIme-StartTime)/1m, ConnectionType, UserName, StartTime
|summarize sum(Duration) by username
|render piechart;
```

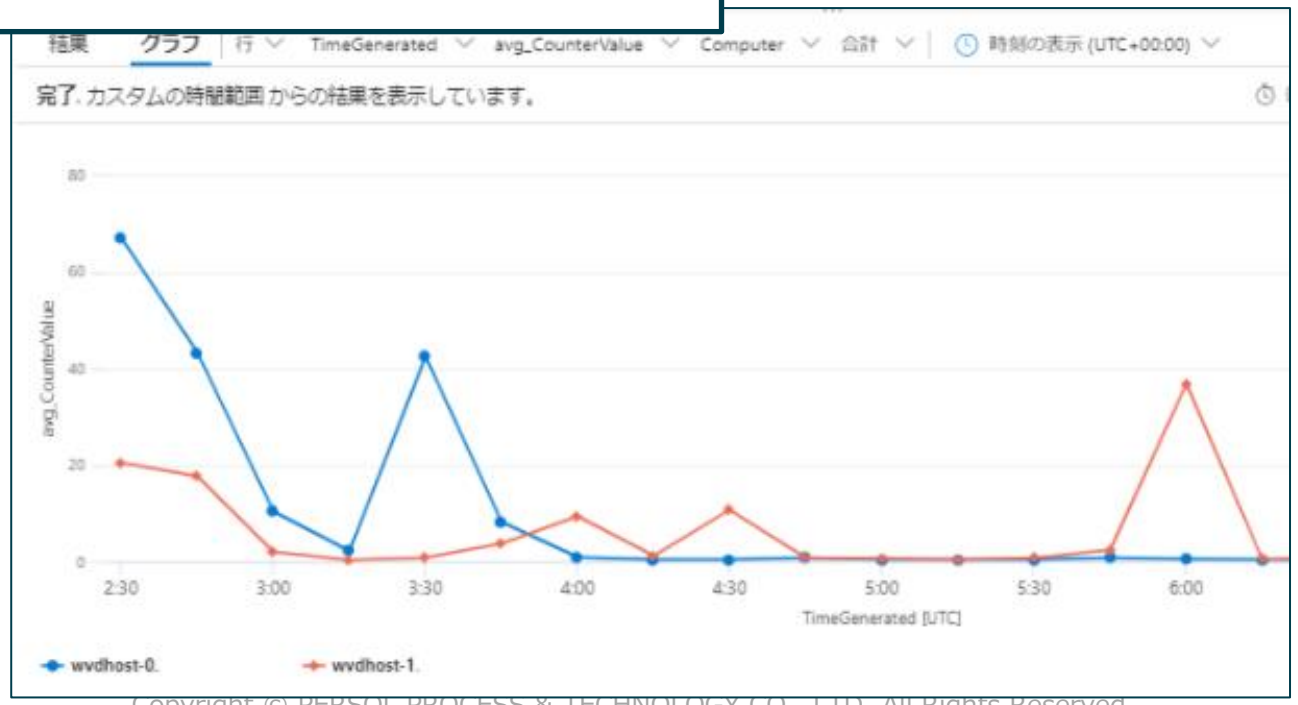


ログクエリ（サンプル）：各種パフォーマンス

- クエリ対象：CPU使用率

ログクエリ：全コンピューターの CPU 使用率の平均値 (15mごと)

```
Perf
| where CounterName == "% Processor Time"
| where objectName == “Processor"
| summarize  avg(CounterValue) by Computer,  bin(TimeGenerated, 15m)
|render timechart;
```



ログクエリ（サンプル）：エラーログ

- クエリ対象：WVDエラー,セッションホストVM死活状況

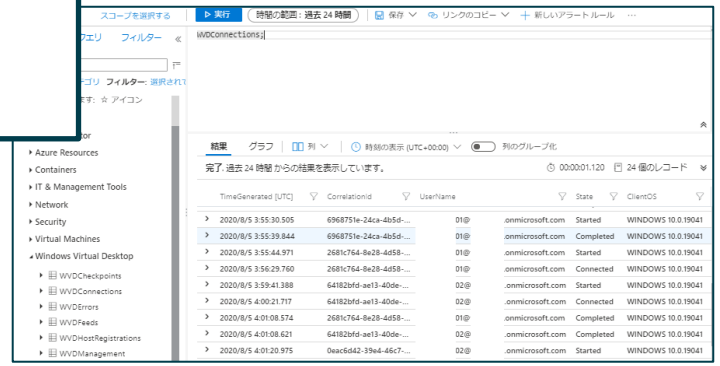
ログクエリ：WVDエラー

```
WVDErrors
|where TimeGenerated > ago(7d);
```

ログクエリ：VM死活状況

```
Heartbeat
|where TimeGenerated >ago(7d)
|summarize heartbeat_count=count() by computer, bin(TimeGenerated,1h)
|sort by computer, TimeGenerated asc;
```

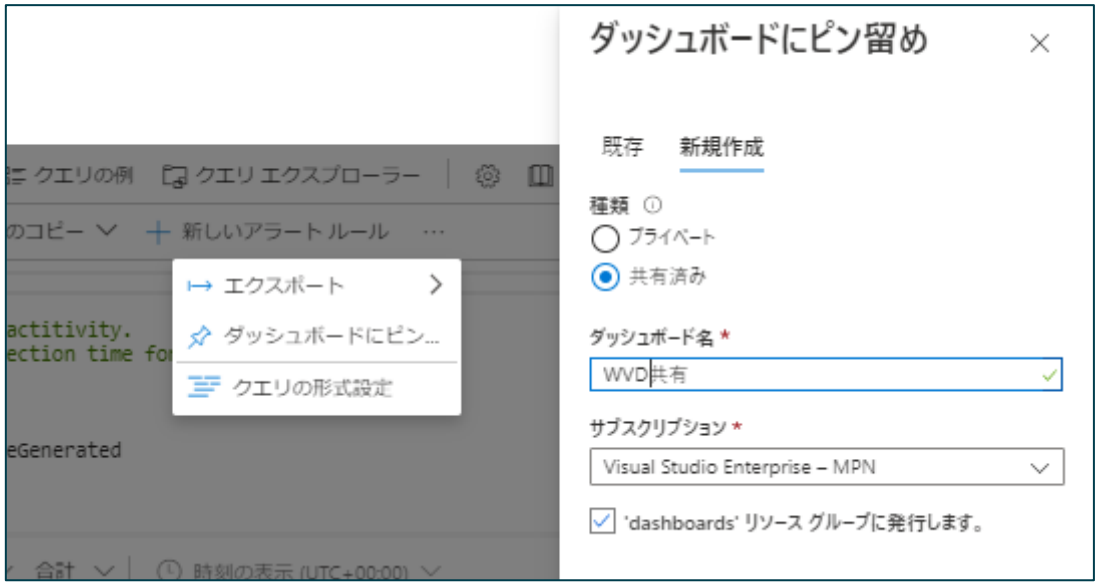
WVDErrors においてServiceError = “true” の場合、
問題を Microsoft にエスカレートする必要があります。
当該エラーの CorrelationID をお伝えください。

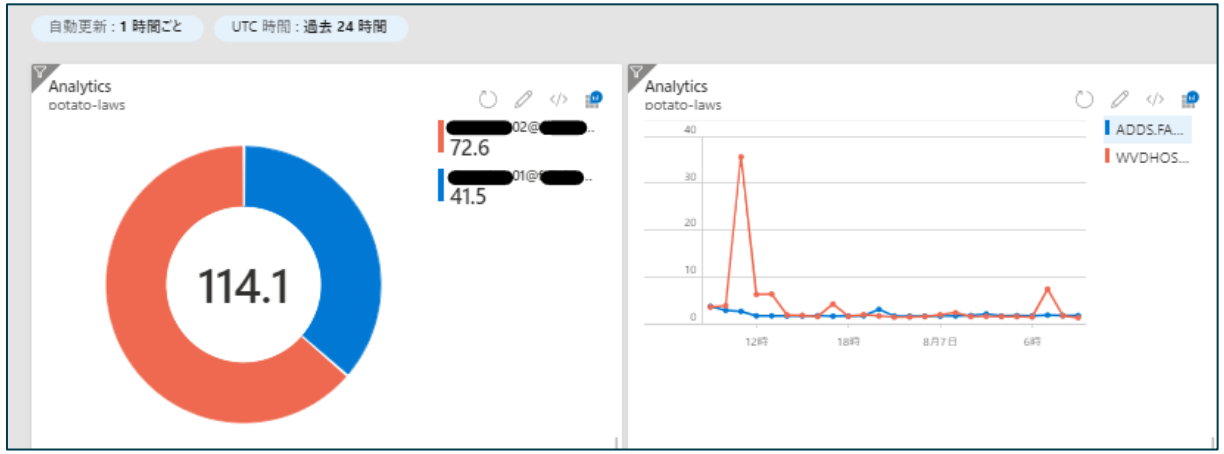


ログ共有（ダッシュボードの活用）

- 集計結果はAzure Portalの
  ダッシュボード上で共有可能

- ログクエリ画面のメニューから
  […]をクリック
  「ダッシュボードにピン留め」を
  選択し、共有ダッシュボードの
  新規作成・ピン留めを選択





アラートの構成（手順の紹介になります）

1. Azure Monitorにてアラートルールを構成します。

2. 下記の項目を設定します。
   - スコープ：監視対象となるリソース
     Log Analyticsを指定することで、そこに転送したログを元にアラートを構成することが可能
   - 条件：アラートルールをトリガーするタイミング
     クエリを指定することが可能
   - アクション：アラートルールがトリガーされた時に通知を送信する（メール発報）ことが可能
     ※Webhookをキックすることも可能

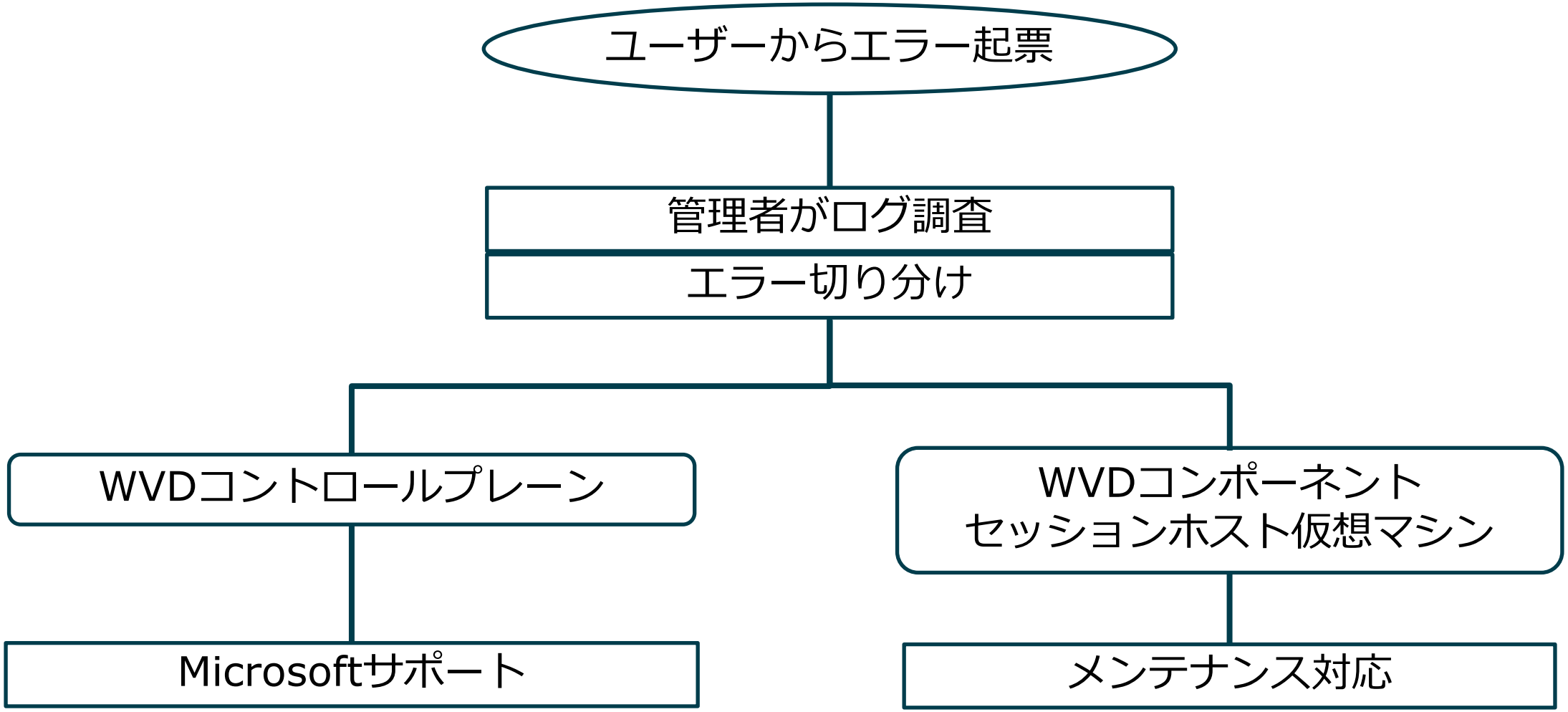
障害対応

障害対応（ハンズオン内容）

障害が発生した際のメンテナンス方法についてご確認ください。

- エラーの切り分けの確認
  →MS側 or ユーザー側
- ユーザー側エラーの場合のメンテナンス方針の確認
- ユーザーへのメッセージ送信
- ユーザーの強制ログオフ
- ドレインモードの有効化
  →一時的に新規セッションが禁止されることを確認
  →管理者だけが接続する方法を確認

エラー対応の流れ



メンテナンス対応

- 管理者で対応できる事象の場合、以下手順でメンテナンス実施

1．ドレインモード

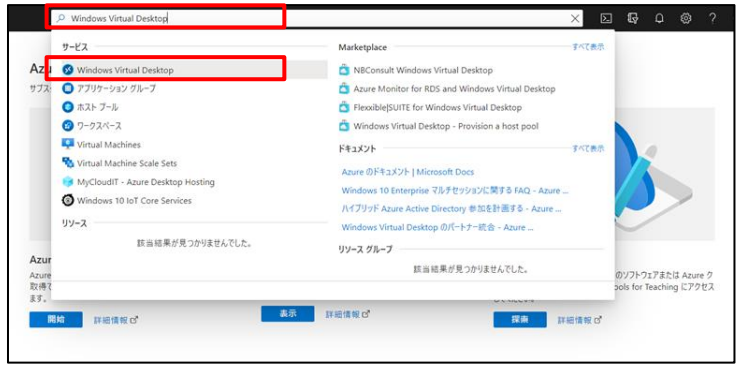
2．メッセージ発行・セッション解放

3．RDP接続

4．作業実施

メンテナンス対応：セッションホストの操作

1. Azureポータル画面から
「Windows Virtual Desktop」と検索し、
表示されたその項目をクリック。



2. 右記画面が表示されるので、
「ホストプール」
→「＜ホストプール名＞」をクリック

3. 右記画面が表示されるので、
「セッションホスト」→
対象のセッションホストをクリック

メンテナンス対応：セッションホストの操作

4. 右記画面が表示される。
ここでは、以下内容などを実施可能

① メッセージの送信
このセッションホストに接続している
ユーザのデスクトップ上に
メッセージを送信。

② Log of all users
このセッションホストにログインしている
ユーザー全員をログオフ。

③ ドレインモードの変更
新しい接続の許否を設定。
ドレインモードオンにした場合、
新しい接続はそのセッションホスト以外
に接続。

メンテナンス対応：管理者が接続するには

ドレインモードはあくまでWVDの管理コントロールプレーン経由での接続を禁止します。
管理者は対象の仮想マシンに直接RDP接続することで、メンテンナスが可能です。

1. Virtual Machineページで IPアドレスを確認
2. mstscアプリケーションでRDP接続

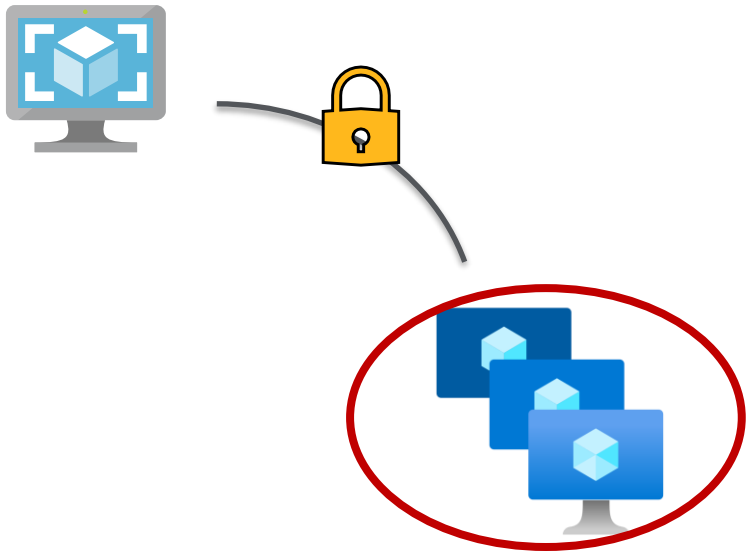
マスタ更新

WVDマスタ更新のポイント

ポイント：

OSイメージとホストプールは固定的に紐づく

ホストプール内でのイメージ更新・配布は不可



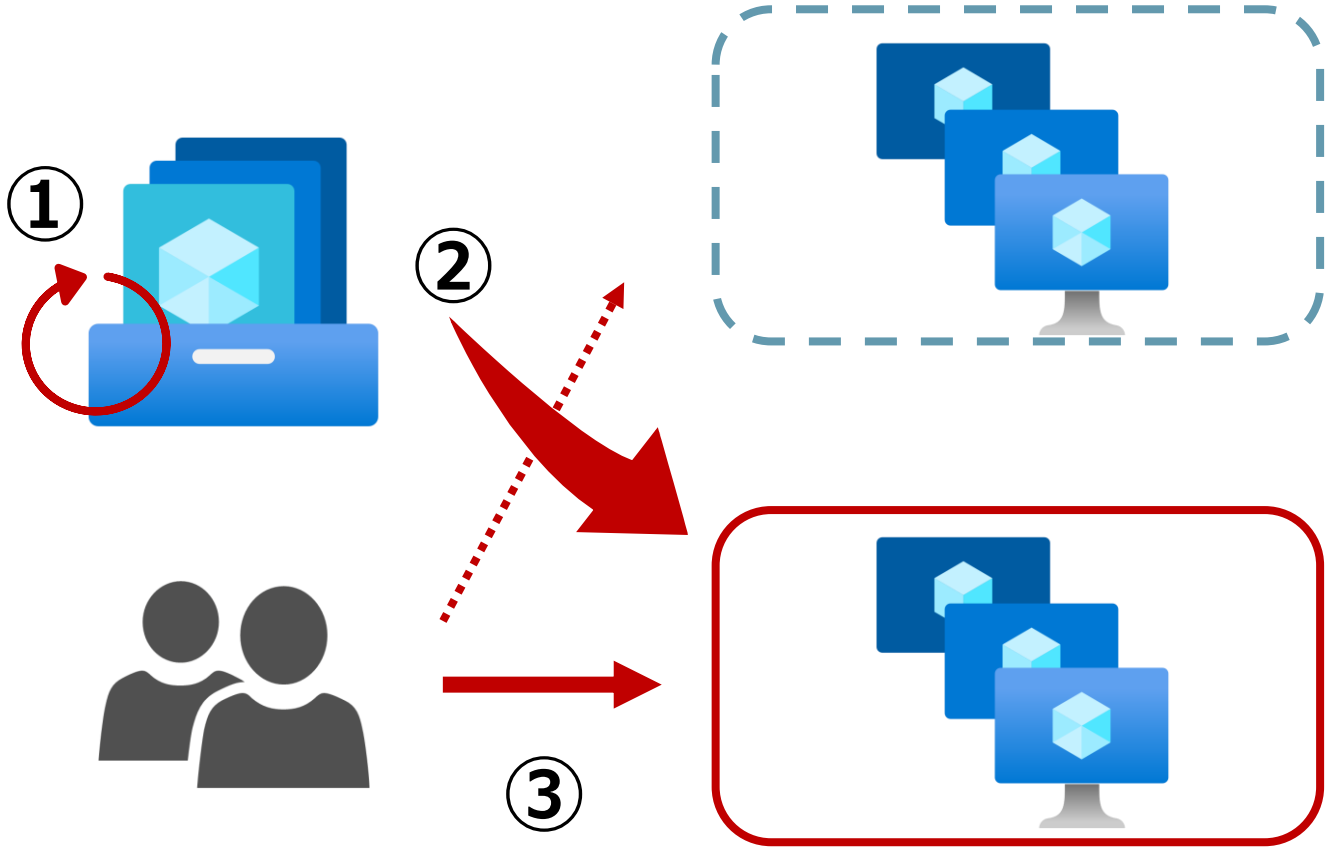
対応：

イメージ管理とホストプール管理を区別

イメージごとにホストプールを作成し移行

マスタ更新の流れ（ブルーグリーンデプロイメント）

- ホストプールに対するイメージ更新機能がないため、
- 基本的にイメージ更新ごとに新規ホストプールを作成し環境



※プロファイルはFSLogix管理により
　自動的に移行される

1．マスタイメージ更新

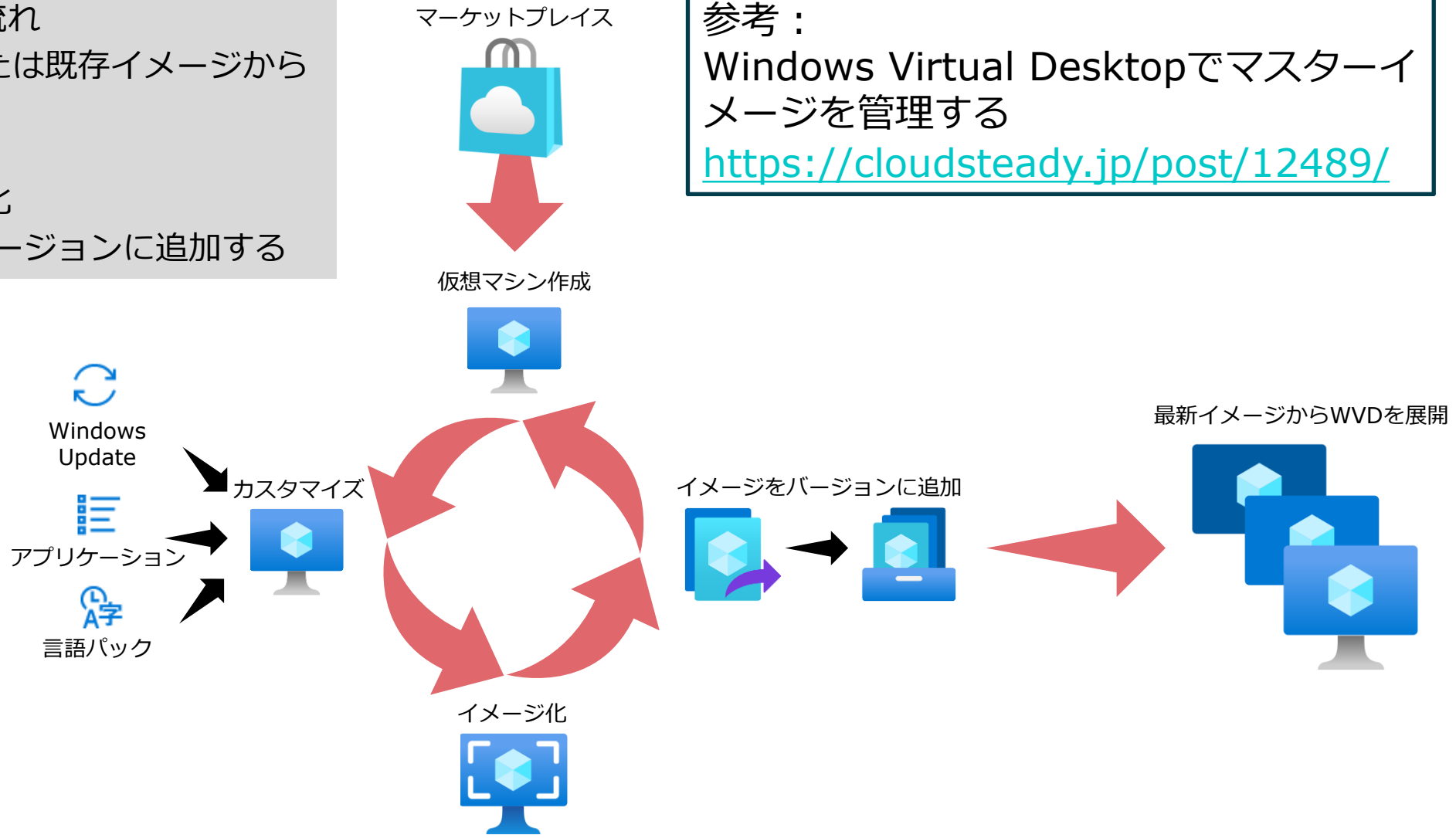
2．新規ホストプールデプロイ

3．ユーザー周知＆割当切り替え

4．旧ホストプール削除

イメージ更新：Shared Image Gallery

イメージ更新の大まかな流れ
- マーケットプレイスまたは既存イメージから仮想マシンを作成
- カスタマイズを実施
- 仮想マシンをイメージ化
- イメージをイメージ バージョンに追加する



参考：
Windows Virtual Desktopでマスターイメージを管理する
https://cloudsteady.jp/post/12489/