Microsoft Azure 勉強会 第4回 Azureネットワーク基礎

日本マイクロソフト株式会社
デジタルセールス事業本部

Why Microsoft ?

The only vendor to span devices, traditional software and cloud services …

… and bring you security, management and a unified application development environment

© 2020 Microsoft Corporation. All rights reserved

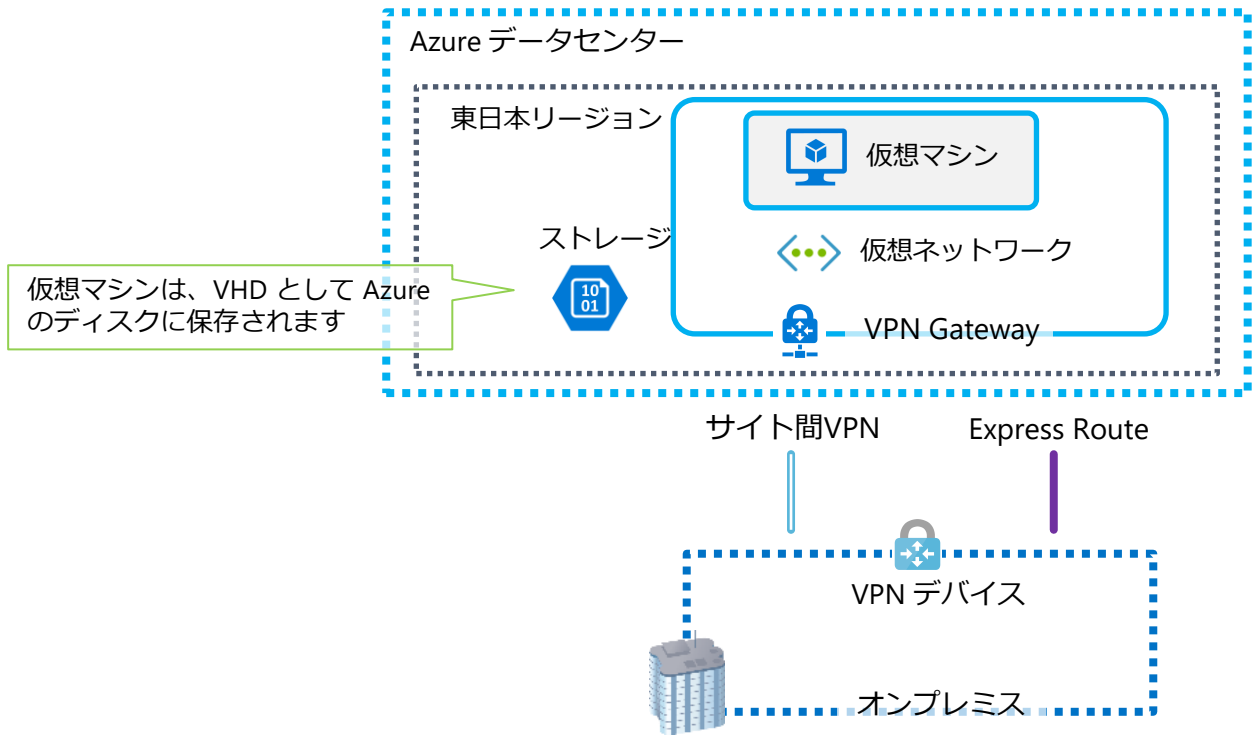
Azure ネットワーク基礎

基礎知識 | 機能 | 参考情報

© 2020 Microsoft Corporation. All rights reserved

Azure IaaS で ネットワークをデザイン

Azure IaaS のパーツを組み合わせる



Azure データセンターのお好きなリージョンを選んでください

仮想ネットワークを作ってください

仮想ネットワークの端に、VPN Gateway を作ってください

仮想ネットワークにお好きな仮想マシンを配置してください

Azure に対応したルーター (VPN デバイス) をご用意ください

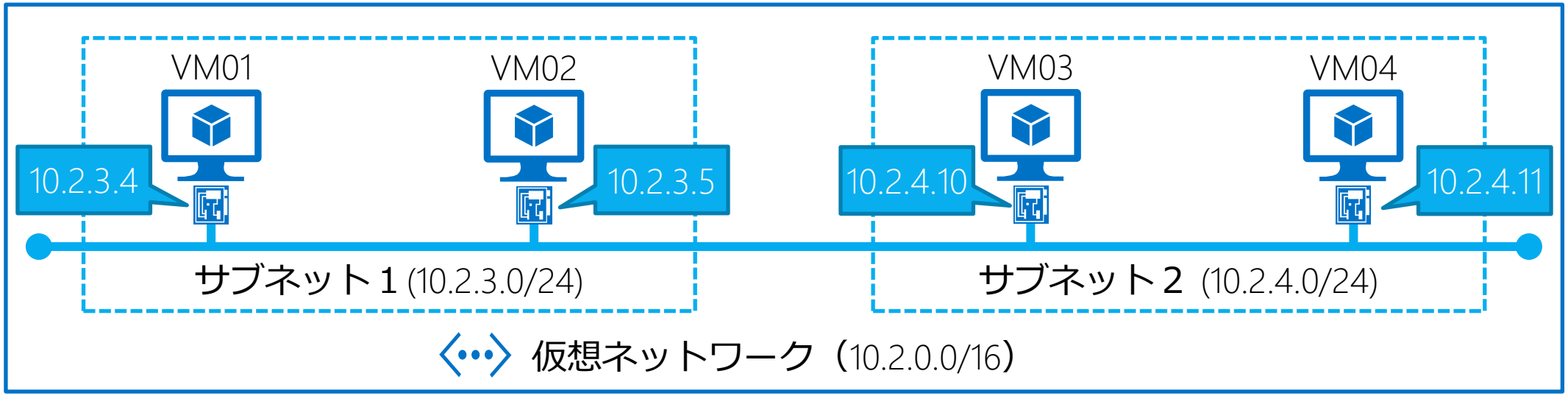
サイト間 VPN か Express Route でオンプレミスと接続してください

お客様の環境に合わせて組み合わせます

© 2020 Microsoft Corporation. All rights reserved

仮想ネットワーク（VNet）

- Microsoft Azure データセンター上にプライベートなネットワークを確保
  - 複数のプライベート アドレス空間・サブネットの定義、アクセス制御ポリシー等、様々な設定が可
- 安全に接続するためのオプションを提供
  - IPSEC VPN による接続（サイト間接続 / ポイント対サイト接続）
  - ExpressRoute（閉域網接続サービス）による Microsoft Azure データセンターとの直接接続

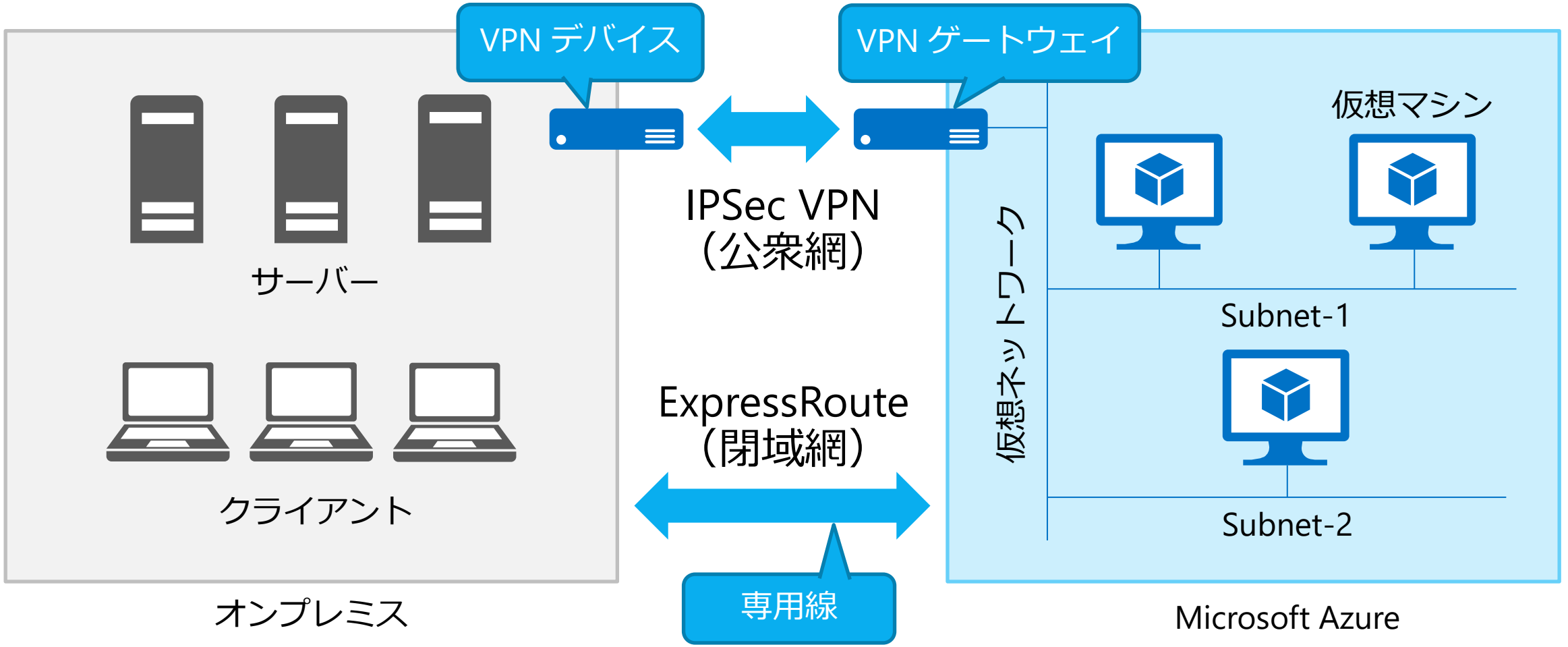


- 仮想マシンは「仮想ネットワーク」に配置（仮想マシン作成においては仮想ネットワークは必須）

© 2020 Microsoft Corporation. All rights reserved

オンプレミス環境と Microsoft Azure との接続

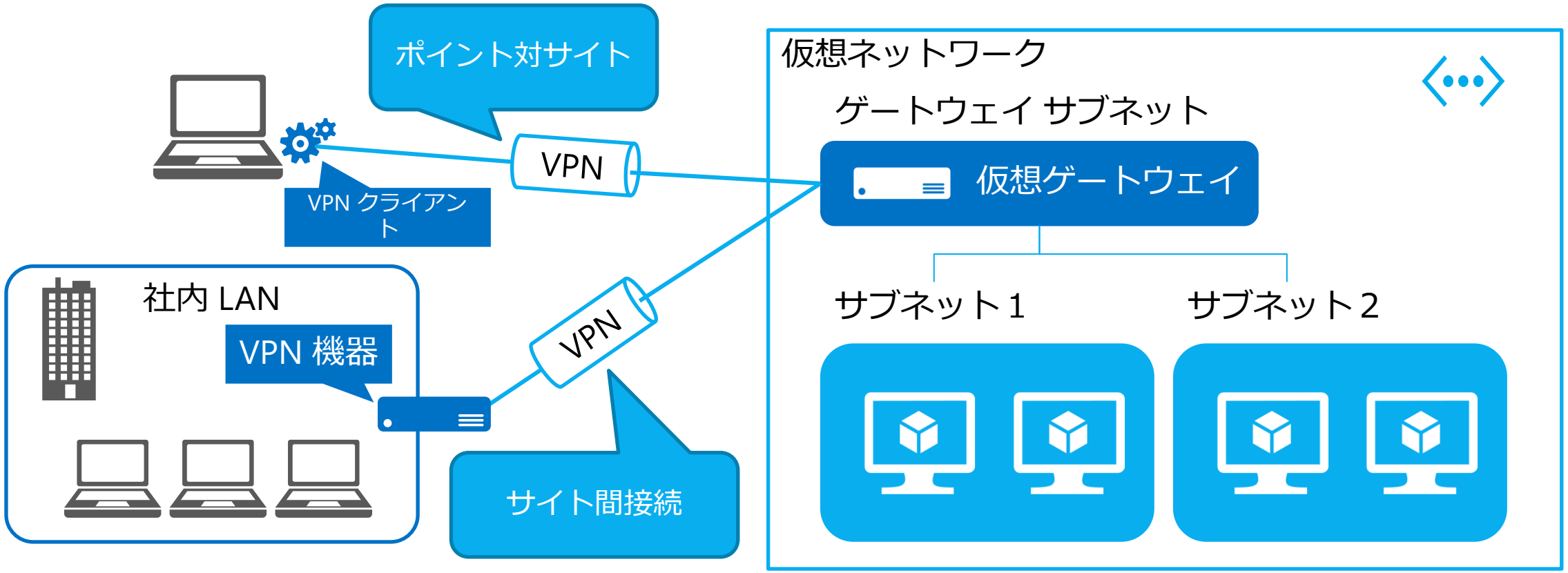
■ 仮想ネットワークでオンプレミスと安全に通信



© 2020 Microsoft Corporation. All rights reserved

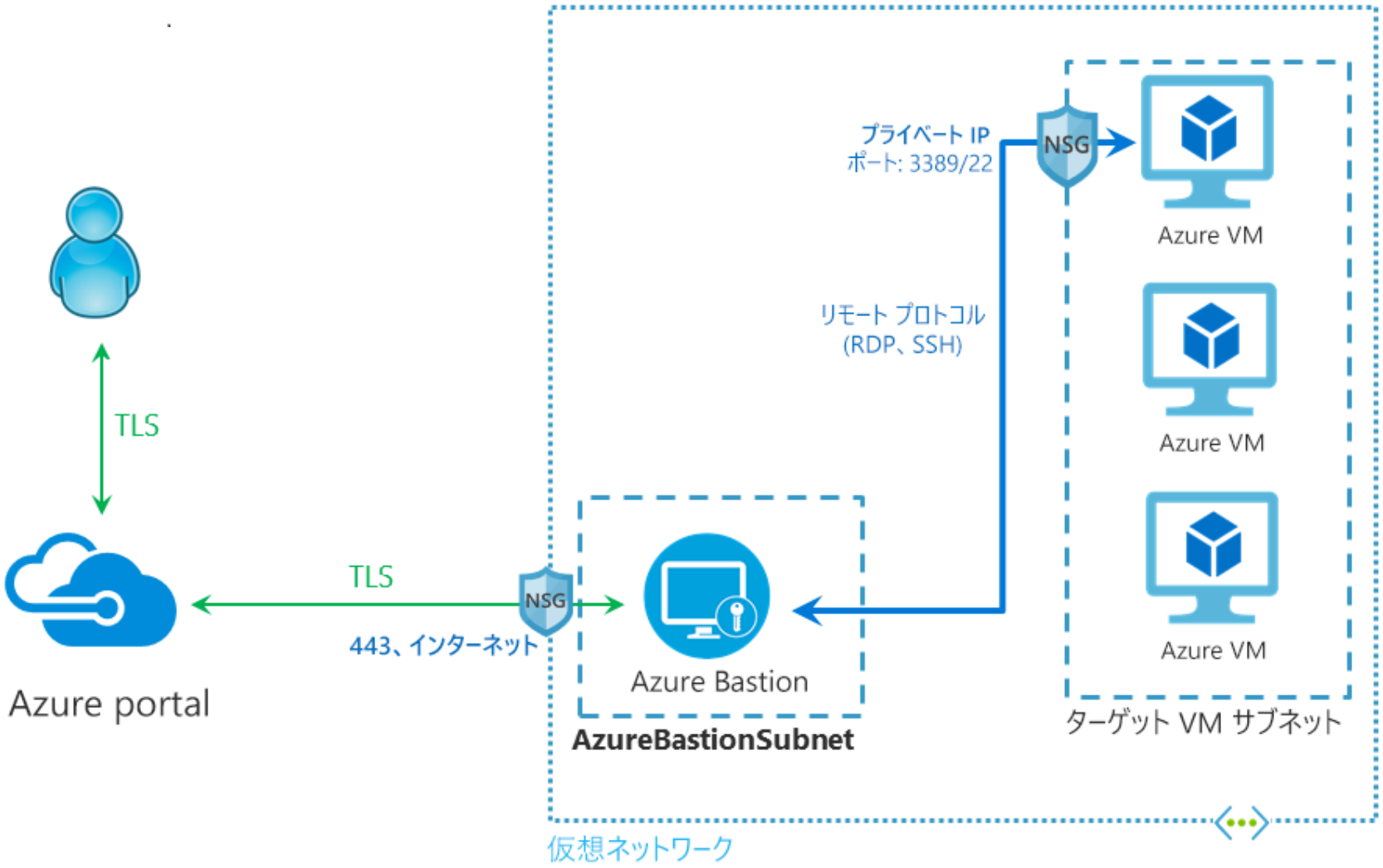
IPSec VPN による接続

- Azure 仮想ネットワークに対する VPN 接続機能を提供
  - サイト間接続：オンプレミスのサイトと仮想ネットワーク間にセキュリティで保護された接続を作成
    オンプレミスのネットワークに VPN デバイスが必要
  - ポイント対サイト接続：各クライアントから個別にセキュリティで保護された接続を作成
    VPN クライアント パッケージのインストールが必要



© 2020 Microsoft Corporation. All rights reserved

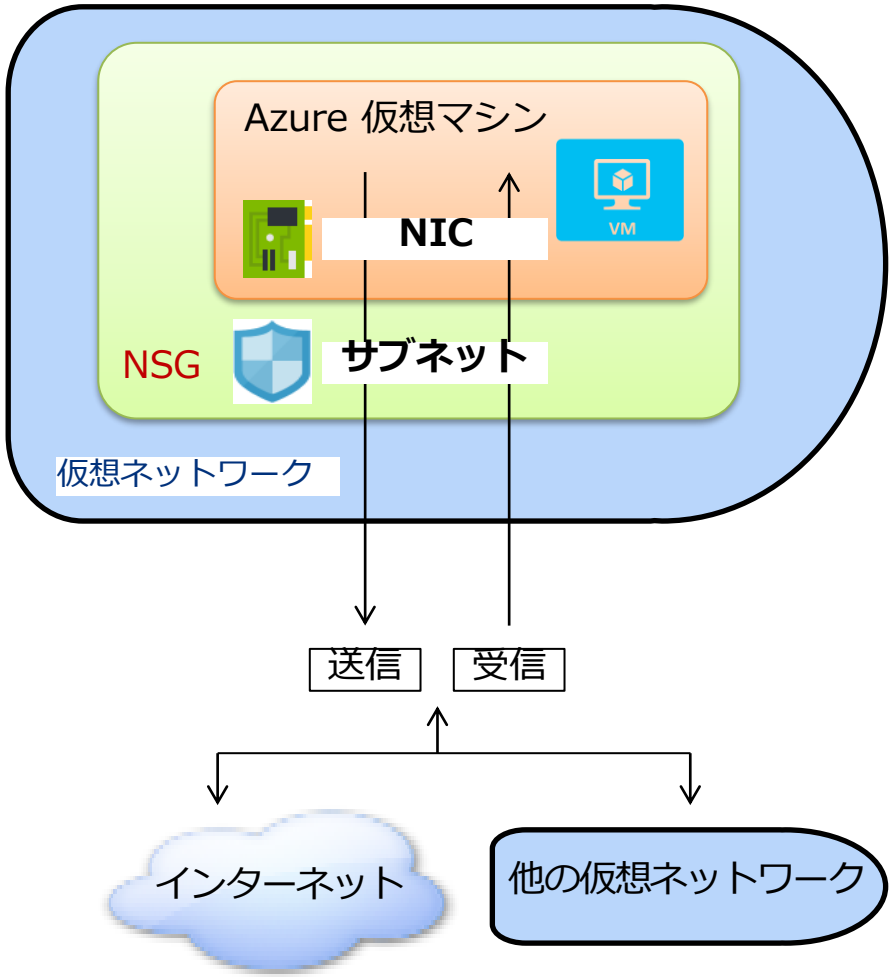
セキュアな接続方式 - Bastion アーキテクチャ



© 2020 Microsoft Corporation. All rights reserved

ネットワーク セキュリティ グループ（NSG）

- 受信/送信トラフィックに対する、アクセス制御ルールの集合
- Azure 仮想マシンの ”ネットワーク インターフェイス”、または、サブネットに対して設定できる
- 送信元 IP アドレス、宛先 IP アドレス、ポート（範囲も可）、プロトコルを指定して、送受信両方向の通信を許可/禁止する



© 2020 Microsoft Corporation. All rights reserved

ネットワークセキュリティグループ（NSG）

受信セキュリティ規則

送信セキュリティ規則

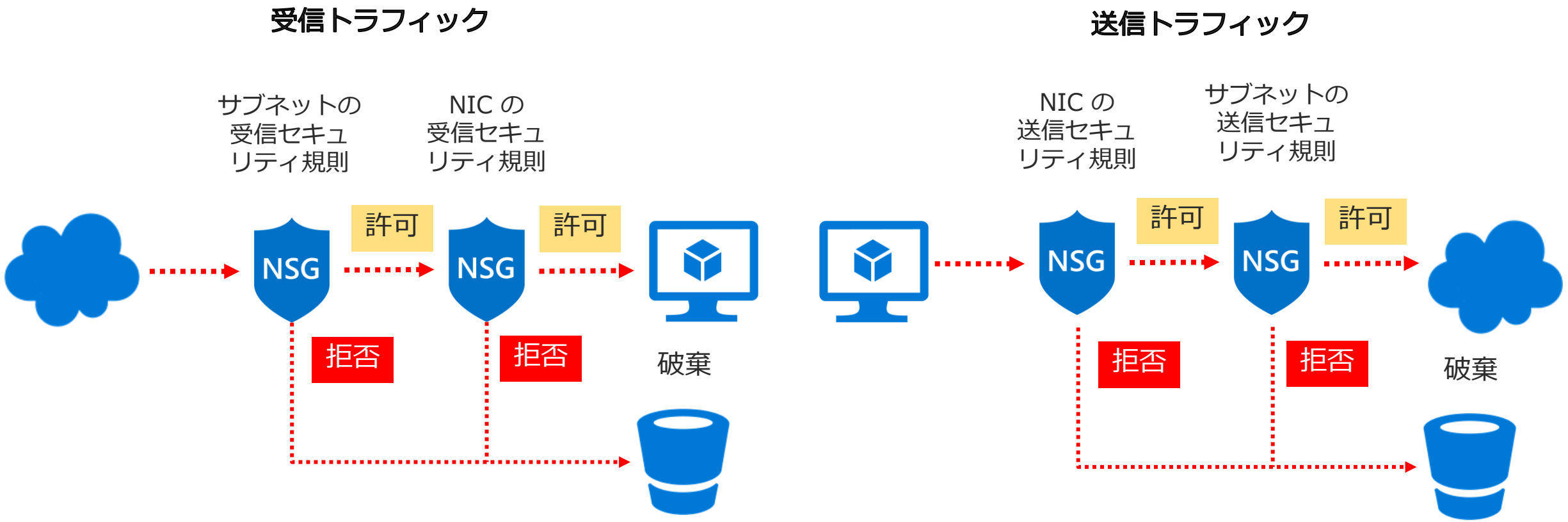
優先度	名前	ポート	プロトコル	ソース	宛先	アクション
1000	default-allow-rdp	3389	TCP	任意	任意	許可
65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork	許可
65001	AllowAzureLoadBalancerInBound	任意	任意	AzureLoadBalancer	任意	許可
65500	DenyAllInBound	任意	任意	任意	任意	拒否

優先度	名前	ポート	プロトコル	ソース	宛先	アクション
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

© 2020 Microsoft Corporation. All rights reserved

NSG の適用順

■ 仮想マシンの NIC または仮想ネットワーク内のサブネットに割り当て可能



© 2020 Microsoft Corporation. All rights reserved

NSG サービスタグ

VirtualNetwork	仮想ネットワークの同一サブネット、仮想ネットワークの異なるサブネット、 仮想ネットワークピアリングで接続された異なる仮想ネットワーク※ Express Route接続されたオンプレミスネットワーク S2S接続されたオンプレミスネットワーク P2S接続されたクライアントネットワーク
AzureLoadBalancer	LBの正常性プローブIP
インターネット	パブリックIP（Azure PaaSを含む）
AzureTrafficManager	Traffic Manager のプローブIP
Storage	Azure Storage サービスのIP
Sql	Azure SQL Database, Azure SQL Data Warehouse サービスのIP
AzureBackup	Azure Backup Storage タグと AzureActiveDirectory タグに依存
AzureMonitor	Log Analytics、Application Insights、AzMon、およびカスタム メトリック

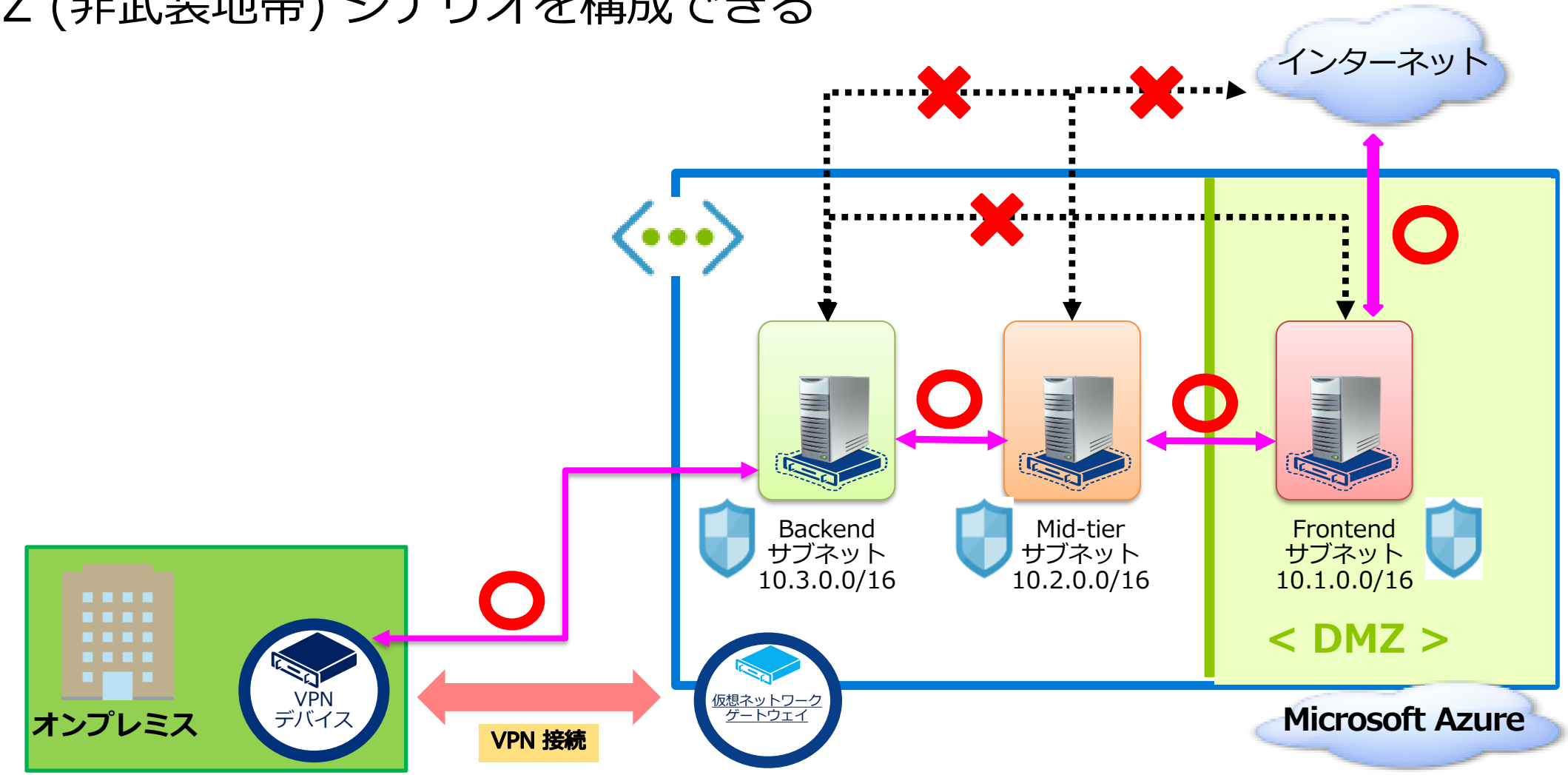
※ピアリング時に「仮想ネットワークアクセスを許可する」を有効にした場合

サービスタグ
https://docs.microsoft.com/ja-jp/azure/virtual-network/service-tags-overview

© 2020 Microsoft Corporation. All rights reserved

例）”ネットワーク セキュリティ グループ” の構成

■ DMZ (非武装地帯) シナリオを構成できる



© 2020 Microsoft Corporation. All rights reserved

免責

本資料には、マイクロソフトの秘密情報が含まれます。本資料は、合理的に知る必要のある貴社内の関係者のみ閲覧できるものとし、マイクロソフトの承諾がない限り、それ以外の第三者に対して、開示、共有等してはならず、また複製も禁じられます。

本資料は情報提供のみを目的としており、本資料に記載されている情報は、本資料作成時点でのマイクロソフトの見解を示したものです。状況等の変化により、内容は変更される場合があります。本資料に表記されている内容（提示されている条件等を含みます）は、貴社との有効な契約を通じて決定されます。それまでは、正式に確定するものではありません。従って、本資料の記載内容とは異なる場合があります。また、本資料に記載されている価格はいずれも、別段の表記がない限り、参考価格となります。貴社の最終的な購入価格は、貴社のリセラー様により決定されます。マイクロソフトは、本資料の情報に対して明示的、黙示的または法的な、いかなる保証も行いません。

© 2020 Microsoft Corporation. All rights reserved

© 2019 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.