IT資格道場

AZ-700 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

AZ-700 出題範囲(Microsoft Learn 公式 Study guide・Skills measured as of July 27, 2026)準拠
2026年9月版

本書のご利用にあたって

- 本書は「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルであっても著作物です。本書の転載・改変しての再配布・二次販売を禁じます。
- 本書を AI モデルの学習データとして利用すること(学習目的の入力・データセット化を含む)を禁じます。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

不正な配布を見つけた場合は info@shikaku-doujou.com までご連絡ください。

目次

資格道場 購入者限定テキスト／学習用（読む）

このテキストは、Microsoft Learn 公式の **Study guide for Exam AZ-700（Skills measured as of July 27, 2026）** の到達目標をそのまま章立てにしたものです。章・節の並びは公式の並び順と同じで、節見出しの末尾に付いている `[1.1]` のような記号は、公式の到達目標番号（当サイトの台帳 `content/exam-scope/az-700.json` の code）です。

このテキストの役割は「読めば問題が解けるようになること」です。用語の紹介で終わらせず、試験で問われる形――「どちらを選ぶか」「その構成で通信は通るか」「なぜ通らないか」――に答えられるところまで書いています。

進め方の標準は次のとおりです。

① 学習用（このテキスト）を読む → ② 頻出度別で解き方を掴む → ③ 問題演習で腕試し → ④ 頻出度別に戻って再確認（試験直前もここ）。暗記用は本線に入れず並走させ、空き時間の反復と用語の再確認に使ってください。

試験の前提（一次情報）

- 合格ラインは 1,000 点満点中 **700 点**。
- 試験時間は **100 分**。Microsoft の共通案内では、100 分は「ラボを含まないアソシエイト／エキスパート試験」の区分にあたります（ラボを含む区分は 120 分）。ただし Microsoft は「ラボを含む試験の一覧は公開しない」と明言しているため、ラボが絶対に出ないという保証はありません。
- 問題数は Microsoft が公表していません（共通の案内は「多くの試験は 40〜60 問」）。
- 日本語で受験できます。
- 出題形式の内訳も非公表です。公式のサンドボックス（Exam sandbox）で体験できる形式は、択一、複数選択、ドラッグ&ドロップ、並べ替え（build

list)、ホットエリア、アクティブスクリーン、ケーススタディなどです。

5 つの主題と配点（公式は幅で公表）

章	主題	配点
第1章	コア ネットワーク インフラストラクチャの設計と実装	25〜30%
第2章	接続サービスの設計・実装・管理	20〜25%
第3章	アプリケーション配信サービスの設計と実装	15〜20%
第4章	Azure サービスへのプライベート アクセスの設計と実装	10〜15%
第5章	Azure ネットワーク セキュリティ サービスの設計と実装	15〜20%

各節の冒頭には、公式の到達目標（英語原文）とその意味を表で置いています。試験は英語版が先に更新されるため、原文の言い回しに慣れておくと、日本語版の設問で戸惑いません。

第1章 コア ネットワーク インフラストラクチャの設計と実装（25〜30%） [1.1/1.2/1.3/1.4]

Azure ネットワークの土台です。アドレス設計・名前解決・経路・監視の 4 つで、配点はいちばん重い章です。ここが曖昧なままだと、第2章以降（VPN・ExpressRoute・Private Link）の設問がすべて解けなくなります。

1-1 Azure リソースの IP アドレス指定の設計と実装 [1.1]

公式の到達目標（原文）	意味
Plan and implement network segmentation and address spaces	ネットワークの分割とアドレス空間を計画・実装する
Create a virtual network (VNet)	仮想ネットワークを作成する
Plan and configure subnetting for services, including virtual network gateways, private endpoints, service endpoints, firewalls, application gateways, VNet-integrated platform services, and Azure Bastion	各サービス（仮想ネットワーク ゲートウェイ、プライベート エンドポイント、サービス エンドポイント、ファイアウォール、Application Gateway、VNet 統合の PaaS、Azure Bastion）向けのサブネット設計
Plan and configure subnet delegation	サブネット委任の計画と構成
Plan and configure shared or dedicated subnets	共有サブネットと専用サブネットの使い分け
Create a Public IP Prefix	パブリック IP プレフィックスの作成
Choose when to use a public IP address prefix	パブリック IP プレフィックスを使う場面の判断
Plan and implement a Custom IP address prefix (bring your own IP)	カスタム IP アドレス プレフィックス（BYOIP）の計画と実装

公式の到達目標（原文）	意味
Create a public IP address	パブリック IP アドレスの作成
Associate public IP addresses to resources	パブリック IP アドレスをリソースに関連付ける

仮想ネットワーク（VNet）とアドレス空間

VNet は Azure における「自分専用のネットワーク」です。作るときに必ず決めるのが **アドレス空間（address space）** で、CIDR 表記で 1 つ以上指定します。VNet は 1 つのリージョンと 1 つのサブスクリプションに属し、リージョンをまたぐことはできません（またぎたい場合はピアリングや Virtual WAN で繋ぎます）。

アドレス空間には、RFC 1918 のプライベート アドレス（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）を使うのが基本です。技術的にはパブリック アドレス範囲も指定できますが、その範囲へのインターネット向け通信が VNet 内へ吸われるため、原則として避けます。

設計で最初に潰すべき論点は「重複」です。 オンプレミスと VPN／ExpressRoute で繋ぐ予定があるなら、オンプレミスで使っているアドレスと重複してはいけません。VNet 同士をピアリングする予定があるなら、そのアドレス空間同士も重複してはいけません。重複したまま繋ごうとすると、ピアリングの作成やゲートウェイ接続の作成そのものが失敗します。試験では「A 社と B 社の合併で 10.0.0.0/16 同士がぶつかった」といったシナリオが好んで出ます。対処は次のいずれかです。

- どちらかの VNet を作り直してアドレス空間を変更する（VNet 内のリソースを退避する必要があります）。
- 重複しない追加のアドレス空間を足し、そちら側に移す。

- 直接繋がず、Private Link（第4章）や NVA による NAT を挟む。

アドレス空間は、VNet の作成後に**追加・削除ができます**。ただし、既にサブネットが載っている範囲は縮められません。設計時は「将来足す分」を見越して、必要より一段広い範囲（たとえば /16）を確保し、サブネットを /24 単位で切っていく方式が扱いやすくなります。

サブネットと予約アドレス

VNet の中はサブネットに分割します。ここで必ず覚えるのが **Azure は各サブネットで先頭 4 つと末尾 1 つ、合計 5 つのアドレスを予約する** という規則です。10.0.1.0/24 なら次のようになります。

アドレス	用途
10.0.1.0	ネットワーク アドレス
10.0.1.1	既定のゲートウェイ（Azure が使用）
10.0.1.2、10.0.1.3	Azure DNS を VNet 内へマッピングする用途で予約
10.0.1.255	ブロードキャスト アドレス

したがって /24 のサブネットで使えるのは 251 個です。/29 なら 8 − 5 = **3 個**しか使えません。「/29 のサブネットに 5 台の仮想マシンを置けるか」という設問は、この 5 つの予約を知っているかどうかを問うています（置けません）。

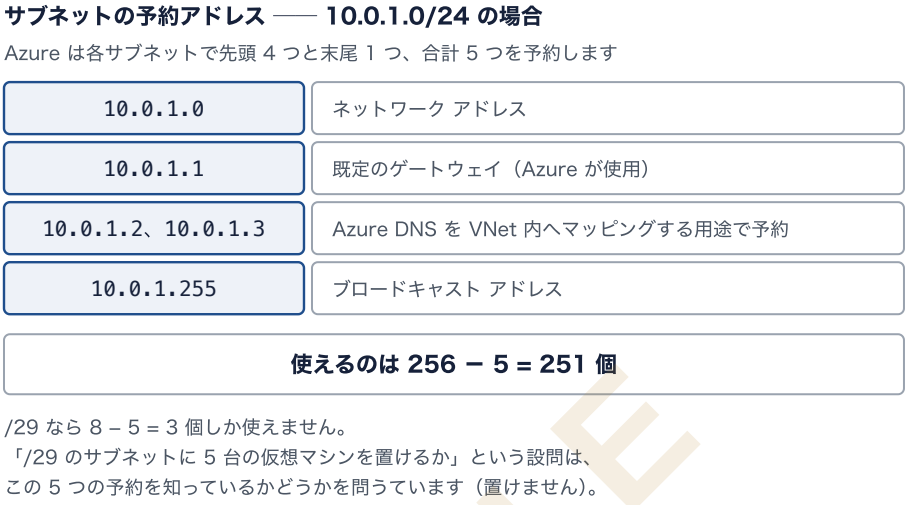


図 1-1　サブネットの予約アドレス —— 10.0.1.0/24 の場合

サブネットの大きさは **/29 から /2 まで**です。小さすぎるサブネットを切ると後で拡張できずに詰みます。逆に、サブネットは後から拡大・縮小できますが、その範囲にリソースが載っていない部分に限られます。

サービスごとに必要な専用サブネット

AZ-700 で頻出なのが「このサービスにはどの名前・どの大きさのサブネットが要るか」です。名前が固定されているものは、その名前でないと配置できません。

サービス	サブネット名	最小サイズの目安
仮想ネットワーク ゲートウェイ（VPN／ExpressRoute）	**GatewaySubnet**（固定）	/29 が最小だが **/27 以上を推奨**。ExpressRoute と VPN を共存させる場合や FastPath などを見込むなら /27 以上が必要

サービス	サブネット名	最小サイズの目安
Azure Bastion	**AzureBastionSubnet**（固定）	**/26 以上**
Azure Firewall	**AzureFirewallSubnet**（固定）	**/26**
Azure Firewall の強制トンネリング用管理サブネット	**AzureFirewallManagementSubnet**（固定）	**/26**
Azure Route Server	**RouteServerSubnet**（固定）	**/27 以上**
Azure DNS Private Resolver（受信エンドポイント／送信エンドポイント）	任意の名前（委任が必要）	/28 以上
Application Gateway	任意の名前だが **専用**（他のリソースと同居不可）	/24 を推奨

ポイントは 3 つです。

1. **名前が固定のサブネットは、その名前でしか機能しない。** `GatewaySubnet` を `gw-subnet` という名前で作ると、ゲートウェイの配置に失敗します。
2. **これらは専用サブネットである。** GatewaySubnet や AzureFirewallSubnet に仮想マシンを置くことはできません。Application Gateway のサブネットも、他の種類のリソースと共有できません。
3. **サイズは後から広げにくい。** 特に GatewaySubnet を /29 で切ってしまうと、後から ExpressRoute を足すときに空きアドレスが足りず、作り直しになります。

名前が固定の専用サブネット ―― その名前でないと配置できない

サービス	サブネット名	最小サイズの目安
仮想ネットワーク ゲートウェイ	`GatewaySubnet`	/29 最小・/27 以上を推奨
Azure Bastion	`AzureBastionSubnet`	/26 以上
Azure Firewall	`AzureFirewallSubnet`	/26
Azure Firewall の管理サブネット	`AzureFirewallManagementSubnet`	/26
Azure Route Server	`RouteServerSubnet`	/27 以上
Azure DNS Private Resolver	任意の名前（委任が必要）	/28 以上
Application Gateway	任意の名前だが専用	/24 を推奨

GatewaySubnet を gw-subnet という名前で作ると、ゲートウェイの配置に失敗します。
これらは専用サブネットで、仮想マシンを置くことはできません。

図 1-2　名前が固定の専用サブネット ―― その名前でないと配置できない

「共有サブネット（shared subnet）」か「専用サブネット（dedicated subnet）」かの判断は、**同じサブネットに置くリソースへ同じネットワーク ポリシー（NSG やルート テーブル）を当てて問題ないか**で決めます。役割が違うもの（Web 層・アプリ層・DB 層）は分けるのが基本です。分けておけば、NSG とルート テーブルをサブネット単位で当てられ、後述する強制トンネリングやサービス チェイニングもサブネット単位で切り替えられます。

サブネット委任（subnet delegation）

一部の Azure PaaS は、VNet の中に自分の管理下のリソースを注入します。このとき使うのが **サブネット委任** です。サブネットに対して「このサービスに委任する」と設定すると、そのサービスだけがそのサブネットへリソースを配置できるようになり、必要なポリシーもサービス側が自動で構成します。

代表的な委任先は次のとおりです。

- `Microsoft.Web/serverFarms`（App Service の VNet 統合）
- `Microsoft.ContainerInstance/containerGroups`（Azure Container Instances）
- `Microsoft.Sql/managedInstances`（SQL Managed Instance）
- `Microsoft.Network/dnsResolvers`（Azure DNS Private Resolver）

委任したサブネットは、そのサービス専用になります。仮想マシンを混ぜることはできません。試験では「App Service の VNet 統合が構成できない」というシナリオで、委任漏れ・サブネットの共有が原因、という形で問われます。

パブリック IP アドレス

パブリック IP アドレスは、それ自体が 1 つの Azure リソースです。作成時に決める主な項目は次のとおりです。

項目	選択肢	押さえどころ
SKU	**Standard** / Basic	Basic は廃止が公式に告知済み。新規設計は Standard 一択
割り当て	静的 / 動的	Standard は **静的のみ**。Basic は動的も可
バージョン	IPv4 / IPv6	デュアル スタック構成では両方を作る
可用性ゾーン	ゾーン冗長 / 特定ゾーン / なし	Standard のみ選択可。ゾーン冗長にすると単一ゾーンの障害を跨げる

項目	選択肢	押さえどころ
ルーティング設定	Microsoft ネットワーク / インターネット	「インターネット」は Azure のバックボーンを早期に出る（コールド ポテト）。既定は Microsoft ネットワーク

Standard SKU のパブリック IP は **既定でインバウンドが閉じています**。NSG で明示的に許可しない限り、外から届きません。Basic は既定で開いています。この差はセキュリティ設問の定番です。

関連付けられる先は、仮想マシンのネットワーク インターフェイス、Standard Load Balancer のフロントエンド、Application Gateway、Azure Firewall、VPN ／ ExpressRoute ゲートウェイ、NAT Gateway、Bastion などです。**Standard SKU のリソースには Standard SKU のパブリック IP しか付けられません**（SKU を混ぜられない）。

パブリック IP プレフィックス

パブリック IP プレフィックス（Public IP Prefix） は、連続したパブリック IP アドレスの範囲をまとめて確保する仕組みです。/28（16 個）から /31（2 個）といった単位で予約し、その中から個々のパブリック IP アドレスを切り出します。

使う場面は、**送信元アドレスを相手先のファイアウォールで許可リストに入れてもらう必要があるとき**です。個別に取ると、リソースを作り直すたびにアドレスが変わり、相手先の許可リストを毎回更新してもらうことになります。プレフィックスで連続範囲を確保しておけば、「この /28 を許可してください」と一度伝えるだけで済み、範囲内のどのアドレスに変わっても影響がありません。

制約として、プレフィックスから切り出したアドレスは **Standard SKU・静的**になります。プレフィックスはリージョンとサブスクリプションに紐づき、ゾーン冗

長にもゾーン指定にもできます。

カスタム IP アドレス プレフィックス（BYOIP）

カスタム IP アドレス プレフィックス（Custom IP address prefix、BYOIP ＝Bring Your Own IP） は、自社が保有しているパブリック アドレス範囲を Azure に持ち込み、Azure から広告してもらう仕組みです。移行時に「今のグローバル アドレスを変えずに Azure へ移りたい」という要件を満たします。

手順の骨子は次のとおりです。

1. 対象範囲について、**ROA（Route Origin Authorization）** を発行し、Azure の AS 番号（8075）を許可する。
2. WHOIS／RDAP の登録情報で保有者であることを確認できる状態にする。
3. 自分の秘密鍵で**署名済みメッセージ**を作り、範囲の所有権を証明する。
4. Azure 側でカスタム IP プレフィックス リソースを作成し、検証（provisioning）を待つ。
5. 検証が済んだら **コミッション（commission）** して広告を開始し、その範囲からパブリック IP プレフィックス／パブリック IP を切り出す。

持ち込める最小サイズは IPv4 で /24（グローバルに広告できる最小単位）です。BYOIP を使うと、アドレスの所有権は自社のままで、Azure のリソースに割り当てられるようになります。

この節のまとめ（試験で効く形）

- サブネットの利用可能数 = 総数 − **5**。
- 名前固定サブネット：GatewaySubnet、AzureBastionSubnet（/26 以上）、AzureFirewallSubnet（/26）、AzureFirewallManagementSubnet

（/26）、RouteServerSubnet（/27 以上）。

- 委任したサブネットは、そのサービス専用。
- 「相手先の許可リストを固定したい」→ **パブリック IP プレフィックス**。「今のアドレスをそのまま Azure で使いたい」→ **カスタム IP プレフィックス（BYOIP）**。
- Standard パブリック IP は既定で閉じている・静的のみ・SKU を混ぜられない。

1-2 名前解決の設計と実装 [1.2]

公式の到達目標（原文）	意味
Design name resolution inside a VNet	VNet 内部の名前解決の設計
Configure DNS settings for a VNet	VNet の DNS 設定
Design public DNS zones	パブリック DNS ゾーンの設計
Design private DNS zones	プライベート DNS ゾーンの設計
Configure public and private DNS zones	パブリック／プライベート DNS ゾーンの構成
Link a private DNS zone to a VNet	プライベート DNS ゾーンの VNet へのリンク
Design and implement Azure DNS Private Resolver	Azure DNS Private Resolver の設計と実装

VNet の既定の名前解決

VNet を作ると、何も設定しなくても **Azure 提供 DNS（Azure-provided DNS）** が使えます。実体は **168.63.129.16** という特別なアドレスで、すべての VNet から到達できる Azure のプラットフォーム アドレスです。このアドレス

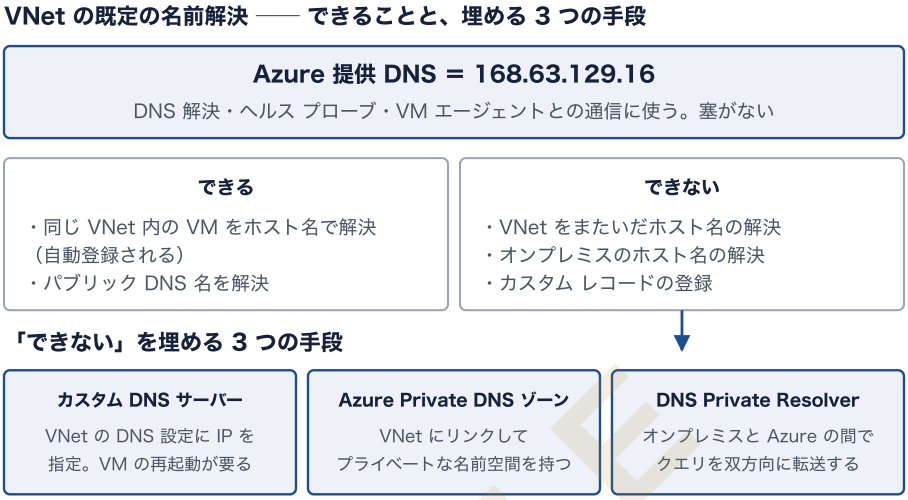
は DNS 解決のほか、ロード バランサーのヘルス プローブや VM エージェントとの通信にも使われます。**NSG や UDR でこのアドレスへの通信を止めると、名前解決だけでなくヘルス プローブも壊れます。** 試験の定番の引っかけです。

Azure 提供 DNS でできること・できないことは、はっきり分かれます。

- **できる**：同じ VNet 内の仮想マシン同士を、ホスト名で解決する（自動登録される）。パブリック DNS 名を解決する。
- **できない**：**VNet をまたいだホスト名の解決**（ピアリングしていても、Azure 提供 DNS だけでは別 VNet の VM 名は引けません）。オンプレミスのホスト名の解決。逆引き（PTR）の細かな制御。カスタム レコードの登録。

この「できない」を埋める手段が、次の 3 つです。

1. **カスタム DNS サーバー**：VNet の DNS 設定に、自分で立てた DNS サーバー（VM）やオンプレミスの DNS サーバーの IP を指定します。設定は VNet 単位（またはネットワーク インターフェイス単位）で、**変更後は各 VM の再起動（またはネットワーク インターフェイスの再取得）が必要**です。カスタム DNS を指定すると Azure 提供 DNS は使われなくなるため、パブリック名も解決できるよう、フォワーダーとして 168.63.129.16 を指しておくのが定石です。
2. **Azure Private DNS ゾーン**：Azure のマネージド サービスとして、プライベートな名前空間を持ちます（後述）。
3. **Azure DNS Private Resolver**：オンプレミスと Azure の間で、DNS クエリを双方向に転送します（後述）。



カスタム DNS を指定すると Azure 提供 DNS は使われなくなるため、
パブリック名も解決できるよう 168.63.129.16 をフォワーダーに指すのが定石です。

図 1-3　VNet の既定の名前解決 —— できることと、埋める 3 つの手段

Azure DNS のパブリック ゾーン

Azure DNS のパブリック ゾーンは、インターネットに公開する権威 DNS です。`contoso.com` のようなゾーンを作り、A／AAAA／CNAME／MX／TXT／NS／SOA／SRV／PTR／CAA レコードを持たせます。

設計の要点は次のとおりです。

- ゾーンを作ると Azure が **4 つのネーム サーバー**を割り当てます。レジストラ側の NS レコードをこの 4 つに向けて初めて権威が移ります（**委任**）。
- **エイリアス レコード セット（alias record set）** を使うと、A／AAAA／CNAME レコードから Azure リソース（パブリック IP、Traffic Manager プロファイル、Front Door、別のゾーン内のレコード）を直接参照できます。参照先のアドレスが変わっても自動で追随し、参照先が消えるとレコード

も自動で除去されるため、いわゆる「ダングリング DNS（宙ぶらりんの DNS）」による乗っ取りを防げます。ゾーン頂点（apex、`contoso.com` そのもの）に CNAME は置けませんが、エイリアス A レコードなら置けます。**「apex を Front Door に向けたい」→ CNAME ではなくエイリアス A レコード** という論点で出ます。

- 分割ホライズン（split-horizon／split-brain）：同じ名前を、社内からはプライベート IP、社外からはパブリック IP に解決させたいときは、**同名のパブリック ゾーンとプライベート ゾーンを両方作ります**。VNet にリンクされたプライベート ゾーンが優先されるため、内部からはプライベート IP が返ります。逆に、同名のプライベート ゾーンを作らずパブリック ゾーンだけで構成すると、社内からの問い合わせにもパブリック ゾーンのレコード（パブリック IP）が返り、内部の宛先には向きません。

Azure Private DNS ゾーン

プライベート DNS ゾーンは、VNet の中だけで有効な名前空間です。インターネットからは引けません。

- **仮想ネットワーク リンク（virtual network link）** で VNet に結び付けて初めて、その VNet から引けるようになります。リンクは複数の VNet に張れ、**リンクした VNet 同士がピアリングされていなくても、それぞれのリンクがあれば解決できます**。
- リンク時に **自動登録（auto-registration）** を有効にすると、その VNet の仮想マシンの A レコードが自動で作られ、VM の削除時に自動で消えます。**自動登録を有効にできるリンクは、1 つのゾーンにつき VNet 1 つあたり 1 つ**で、逆に 1 つの VNet が自動登録できるゾーンも 1 つだけです。
- プライベート ゾーンは **サブスクリプションやリージョンをまたいでリンクできます**（ゾーン自体はグローバル リソース）。ハブ&スポーク構成では、ハ

ブのサブスクリプションにゾーンを 1 つ置き、全スポーク VNet からリンクするのが定石です。

Private Link との関係（詳細は第4章）：プライベート エンドポイントを作ると、`privatelink.blob.core.windows.net` のような専用のプライベート ゾーンが必要になります。パブリック名（`mystorage.blob.core.windows.net`）は CNAME で `mystorage.privatelink.blob.core.windows.net` を指しており、そのプライベート ゾーンがリンクされている VNet からはプライベート IP が、リンクされていない環境からはパブリック IP が返ります。**「オンプレミスから private endpoint 名がパブリック IP に解決されてしまう」というトラブルは、ほぼすべてこの DNS の設計漏れです。**

アプリケーションは接続文字列を変えずに済み、DNS の見え方だけで経路が変わります。
「オンプレミスから private endpoint 名がパブリック IP に解決されてしまう」は、
ほぼすべてこの DNS の設計漏れです。

図 1-4　privatelink 名の解決 —— リンクの有無で返る IP が変わる

Azure DNS Private Resolver

Azure DNS Private Resolver は、DNS サーバーの VM を自前で立てずに、オンプレミスと Azure の間で DNS を橋渡しするマネージド サービスです。VM

のパッチ当てや冗長化から解放されるのが最大の利点です。

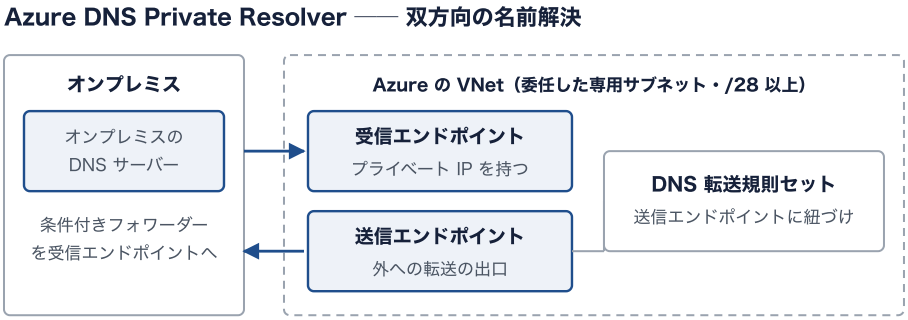
構成要素は次の 3 つです。

構成要素	役割
受信エンドポイント（inbound endpoint）	オンプレミスから Azure へ向かうクエリの受け口。VNet 内のプライベート IP を持ち、オンプレミスの DNS サーバーの条件付きフォワーダーの転送先にする
送信エンドポイント（outbound endpoint）	Azure からオンプレミス（や他の DNS）へクエリを転送する出口
DNS 転送規則セット（forwarding ruleset）	「このドメインはこの DNS サーバーへ転送する」という規則の集合。送信エンドポイントに紐づけ、VNet にリンクして適用する

エンドポイントを置くサブネットは、`Microsoft.Network/dnsResolvers` **へ委任した専用サブネット**である必要があり、他のリソースと共有できません（/28 以上が目安）。Private Resolver 自体は 1 つの VNet に配置し、他の VNet からはピアリングとリンクで利用します。

典型的な双方向構成はこうなります。

- **オンプレミス → Azure**：オンプレミスの DNS で `privatelink.database.windows.net` などの条件付きフォワーダーを作り、転送先を **受信エンドポイントのプライベート IP** にする。
- **Azure → オンプレミス**：転送規則セットに `corp.contoso.com → オンプレミス DNS の IP` を登録し、送信エンドポイント経由で転送する。規則セットは VNet にリンクして有効化する。



オンプレミス → Azure：オンプレミスの DNS で privatelink.database.windows.net などの条件付きフォワーダーを作り、転送先を受信エンドポイントのプライベート IP にする。
Azure → オンプレミス：転送規則セットに corp.contoso.com → オンプレ DNS の IP を登録し、送信エンドポイント経由で転送する。規則セットは VNet にリンクして有効化する。

図 1-5　Azure DNS Private Resolver —— 双方向の名前解決

この節のまとめ

- 168.63.129.16 は DNS だけでなくヘルス プローブにも使う。**塞がない**。
- Azure 提供 DNS は **VNet をまたげない**。またぐならプライベート DNS ゾーン＋リンク。
- プライベート DNS ゾーンは **リンクしないと引けない**。自動登録リンクは VNet ごとに 1 つ。
- 分割ホライズンは、同名のパブリック ゾーンとプライベート ゾーンを併用する。
- オンプレミスとの双方向解決は **DNS Private Resolver**（受信エンドポイント＋送信エンドポイント＋転送規則セット）。
- ゾーン頂点を Azure リソースへ向けるのは **エイリアス レコード**。

1-3 VNet の接続とルーティングの設計と実装 [1.3]

公式の到達目標（原文）	意味
Design service chaining, including gateway transit	ゲートウェイトランジットを含むサービス チェイニングの設計
Implement VNet peering	VNet ピアリングの実装
Implement and manage virtual network connectivity by using Azure Virtual Network Manager	Azure Virtual Network Manager による接続の実装と管理
Design and implement user-defined routes (UDRs)	ユーザー定義ルートの設計と実装
Associate a route table with a subnet	ルート テーブルのサブネットへの関連付け
Configure forced tunneling	強制トンネリングの構成
Diagnose and resolve routing issues	ルーティング問題の診断と解決
Design and implement Azure Route Server	Azure Route Server の設計と実装
Identify appropriate use cases for Azure NAT Gateway	Azure NAT Gateway の適切なユース ケースの判断
Implement Azure NAT Gateway	Azure NAT Gateway の実装

システム ルートとルーティングの優先順位

Azure は、VNet を作った時点で **システム ルート（既定のルート）** を自動生成します。同じ VNet 内の通信、ピアリング先、ゲートウェイ経由、そして 0.0.0.0/0 のインターネット向けが含まれます。

経路が競合したときの優先順位は、**次の順**で決まります。これは AZ-700 で最も問われるルールの 1 つです。

1. **ユーザー定義ルート（UDR）**
2. **BGP で学習したルート**（VPN／ExpressRoute／Route Server 経由）
3. **システム ルート**

同じ優先度の中では、**より長い（詳細な）プレフィックスが勝ちます**（最長一致）。したがって、BGP で 0.0.0.0/0 を受け取っていても、UDR で 0.0.0.0/0 を書けば UDR が勝ちます。逆に、UDR で 10.0.0.0/8 を書いていても、BGP で 10.1.2.0/24 を学習していればそちらが勝ちます（プレフィックスが長いため）。

図 1-6　経路が競合したときの優先順位

UDR の **次ホップの種類** は次のとおりです。

次ホップ	用途
仮想アプライアンス（Virtual appliance）	NVA や Azure Firewall の内部 IP を指定して経由させる

次ホップ	用途
仮想ネットワーク ゲートウェイ（Virtual network gateway）	VPN／ExpressRoute ゲートウェイへ向ける。強制トンネリングで使う
仮想ネットワーク（Virtual network）	VNet 内で経路を上書きする
インターネット（Internet）	インターネットへ直接出す
なし（None）	**その宛先への通信を破棄する**（ブラック ホール）

ルート テーブルは **サブネットに関連付けます**（VNet 全体や NIC には付けません）。1 サブネットに付けられるルート テーブルは 1 つ、1 つのルート テーブルは複数のサブネットに付けられます。単位がサブネットである以上、同じサブネットの中で仮想マシンごとに経路を変えることはできません。**特定の仮想マシンだけ別の経路にしたいときは、その仮想マシンを別のサブネットへ分け、そのサブネットにルート テーブルを関連付けます。**

ルート テーブルには **「ゲートウェイ ルートの伝達（BGP route propagation）」**のスイッチがあります。これを無効にすると、そのサブネットは VPN／ExpressRoute ゲートウェイから BGP で学習した経路を受け取らなくなります。ハブ&スポークで「オンプレミス向けの通信を必ずファイアウォール経由にしたい」ときに、伝達を無効化し、UDR でファイアウォールを指す、という組み合わせを使います。

VNet ピアリング

VNet ピアリングは、2 つの VNet を Azure のバックボーンで直結する仕組みです。同一リージョン同士は「VNet ピアリング」、リージョンをまたぐ場合は「グローバル VNet ピアリング」と呼びますが、設定項目は同じです。

覚えるべき性質は 4 つです。

1. **非推移的（non-transitive）**。A–B と B–C をピアリングしても、A–C は通信できません。ハブ&スポークでスポーク同士を通信させたいなら、ハブに NVA／Azure Firewall を置いて UDR で経由させるか、スポーク同士も直接ピアリングします。
2. **アドレス空間が重複していると作れない。**
3. **双方向の合意が要る。** 実体は各 VNet 側に 1 つずつのピアリング リソースで、両方が作られて初めて状態が「Connected」になります。片方だけだと「Initiated」のまま繋がりません。
4. **低遅延・高帯域。** ゲートウェイや公衆網を経由せず、帯域は VM の性能に依存します。

ピアリングの設定スイッチは、試験でそのまま問われます。

スイッチ	意味
仮想ネットワーク アクセスを許可する	ピアリング先との通信そのものを許可（通常は有効）
転送されたトラフィックを許可する（Allow forwarded traffic）	**ピアリング先が発信元でないトラフィック**（NVA が転送してきたもの）を受け入れる。サービス チェイニングに必須
ゲートウェイ トランジットを許可する（Allow gateway transit）	**自分側のゲートウェイ**を相手に使わせる（ハブ側で有効化）
リモート ゲートウェイを使用する（Use remote gateways）	**相手側のゲートウェイ**を使う（スポーク側で有効化）

ゲートウェイ トランジットは、ハブ VNet の VPN／ExpressRoute ゲートウェイを、スポーク VNet が共用するための仕組みです。ハブ側で「ゲートウェイ トランジットを許可する」を有効に、スポーク側で「リモート ゲートウェイを使用

する」を有効にします。**スポーク側に自前のゲートウェイがあると、「リモートゲートウェイを使用する」は有効にできません。**これも定番の設問です。

サービス チェイニング

サービス チェイニング（service chaining）は、UDR で次ホップを NVA に向けることで、トラフィックを意図した装置に通す設計です。ハブ&スポークの標準形はこうなります。

- スポーク A のサブネットに UDR：`0.0.0.0/0 → 仮想アプライアンス（ハブの Azure Firewall の内部 IP）`
- スポーク B のサブネットにも同じ UDR
- ハブとスポークはピアリングし、**双方で「転送されたトラフィックを許可する」を有効化**
- 結果として、スポーク A ↔ スポーク B の通信もインターネット向け通信もハブのファイアウォールを通る

NVA を仮想マシンで自前実装する場合、**その VM の NIC で「IP 転送（IP forwarding）」を有効化**する必要があります。有効化しないと、自分宛でないパケットを VM が破棄します。Azure Firewall はマネージド サービスなので、この設定は不要です。

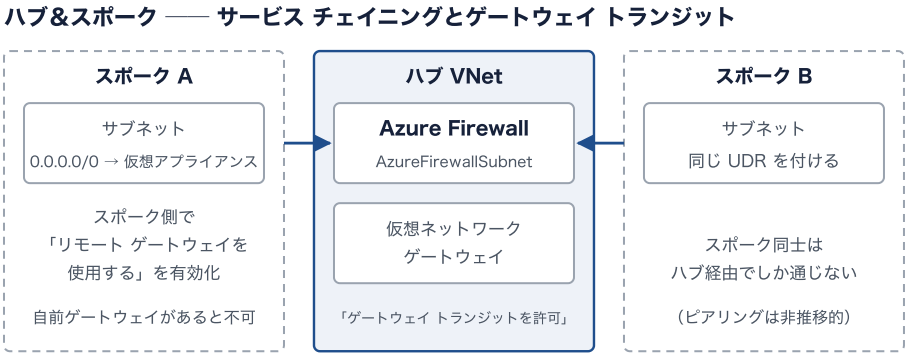


図 1-7　ハブ&スポーク —— サービス チェイニングとゲートウェイ トランジット

強制トンネリング

強制トンネリング（forced tunneling） は、Azure からインターネットへ直接出る通信を禁止し、すべてオンプレミス経由（またはファイアウォール経由）にする構成です。監査要件で「出口を 1 か所に集約せよ」と言われたときの答えです。

実装は 2 通りです。

- **UDR で実装**：対象サブネットに `0.0.0.0/0 → 仮想ネットワーク ゲートウェイ` の UDR を付ける。
- **BGP で実装**：オンプレミス側から既定ルート（0.0.0.0/0）を広告する。

注意点として、**GatewaySubnet に 0.0.0.0/0 の UDR を付けてはいけません**。ゲートウェイ自身の制御通信が壊れ、接続が落ちます。また Azure Firewall で強制トンネリングを行う場合は、専用の

AzureFirewallManagementSubnet が別途必要で、管理トラフィックだけはインターネットへ直接出します。

ルーティング問題の診断

トラブル シューティングは道具の使い分けで解きます。

症状	使う道具
どこへ送られているか分からない	Network Watcher の **次ホップ（Next hop）**
許可／拒否が NSG のどれで起きたか知りたい	**IP フロー検証（IP flow verify）**、**NSG 診断（NSG diagnostics）**
サブネットに実際に効いている経路の一覧が見たい	NIC の **有効なルート（effective routes）**
実パケットを見たい	**パケット キャプチャ**
特定の宛先へ到達できるか継続的に見たい	**接続モニター（Connection Monitor）**

よくある原因は、①UDR の次ホップが落ちている NVA を指している、②BGP 伝達を無効化したままオンプレ経路が消えた、③非対称ルーティング（行きは NVA・戻りは直接）でステートフル装置がパケットを落とす、④アドレス空間の重複、です。

Azure Route Server

Azure Route Server は、VNet 内の NVA と Azure のソフトウェア定義ネットワークとの間で **BGP をやりとりする**マネージド サービスです。これが無い時代は、NVA が学習した経路を UDR に手で書き写す必要がありました。Route Server を置くと、NVA が広告した経路が VNet のサブネットへ自動で反映さ

れ、逆に VNet のアドレス空間や ExpressRoute／VPN から学んだ経路が NVA へ広告されます。

要点は次のとおりです。

- 専用サブネット **RouteServerSubnet（/27 以上）** が必要。
- **ルーティングのみを担当し、データ パスには入りません**（パケットは Route Server を通らない）。
- 高可用性のため、2 つの BGP ピア IP を持ちます。NVA からは両方とピアリングします。
- ASN は **65515**（Azure 側の固定値）。NVA 側は任意のプライベート ASN を使います。
- **ブランチ間トラフィック（branch-to-branch）** を有効にすると、ExpressRoute と VPN／NVA の間で経路を相互に交換し、拠点間の通信が成立します。無効なら経路交換は行われません。

Azure NAT Gateway

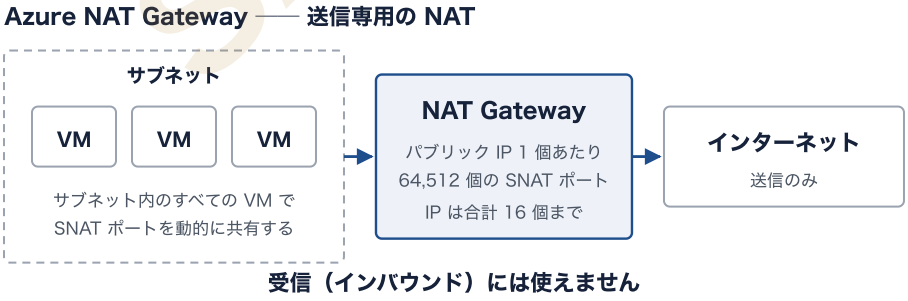
Azure NAT Gateway は、サブネットからインターネットへ出る **送信専用（アウトバウンド専用）** の NAT です。サブネットに関連付けると、そのサブネットの送信通信は必ず NAT Gateway のパブリック IP から出て行きます。

なぜ使うのか、が試験の中心です。Azure の既定の送信（default outbound access）やロード バランサーの送信規則では、**SNAT ポートの枯渇**が起きます。多数の VM が同じ宛先へ大量の接続を張ると、ポートが足りなくなり接続が失敗します。NAT Gateway は、パブリック IP 1 個あたり **64,512 個の SNAT ポート**を持ち、**サブネット内のすべての VM で動的に共有**します。必要なところへ必要なだけ割り当てられるため、枯渇に圧倒的に強くなります。

構成と制約は次のとおりです。

- 関連付けられるパブリック IP／パブリック IP プレフィックスは **合計 16 個まで**（＝最大約 100 万ポート）。
- **アイドル タイムアウトは既定 4 分**、最大 120 分まで設定可能。
- **ゾーン リソース**です。ゾーン冗長にはできないため、可用性ゾーンごとにサブネットと NAT Gateway を分けるのが推奨構成。
- 1 つの NAT Gateway を **同じ VNet 内の複数サブネット**に関連付けられますが、**1 つのサブネットに付けられる NAT Gateway は 1 つ**です。
- **受信（インバウンド）には使えません。** 外から入る通信はロード バランサーやパブリック IP で受けます。
- NAT Gateway があるサブネットでは、**送信の優先順位が NAT Gateway 最優先**になります（インスタンスのパブリック IP やロード バランサーの送信規則より先）。
- Basic SKU のロード バランサーやパブリック IP とは併用できません。

「送信元 IP を固定したい」「SNAT ポート枯渇を解消したい」「送信だけをまとめたい」――この 3 つが出たら NAT Gateway、と結び付けてください。



ゾーン リソースです。ゾーン冗長にはできないため、可用性ゾーンごとに分けるのが推奨構成。
アイドル タイムアウトは既定 4 分、最大 120 分。
1 つのサブネットに付けられる NAT Gateway は 1 つ。送信の優先順位は NAT Gateway が最優先。

図 1-8　Azure NAT Gateway ―― 送信専用の NAT

Azure Virtual Network Manager

Azure Virtual Network Manager（AVNM） は、多数の VNet の接続とセキュリティ規則を、**中央から宣言的に管理**するサービスです。VNet が数十〜数百に増えると、ピアリングを 1 本ずつ張る運用が破綻するため、その解になります。

構成の流れは次のとおりです。

1. **ネットワーク マネージャー** を作り、**スコープ**（管理グループまたはサブスクリプション）を決める。スコープの外の VNet は扱えません。
2. **ネットワーク グループ** を作り、対象の VNet を入れる。入れ方は 2 通りで、**静的メンバーシップ**（手で選ぶ）と **動的メンバーシップ**（Azure Policy の条件式で自動的に入る）。タグや名前で条件を書けるので、新しい VNet が条件に合えば自動で加わります。
3. **構成（configuration）** を作る。
   - **接続構成（connectivity configuration）**：**メッシュ**（グループ内の全 VNet を相互接続）か **ハブ&スポーク**（ハブを指定し、スポークを接続）。ハブ&スポークでは「直接接続（direct connectivity）」を有効にするとスポーク同士も通信でき、「グローバル メッシュ」でリージョンをまたげます。
   - **セキュリティ管理構成（security admin configuration）**：後述（5-1）の **セキュリティ管理規則**。
4. **デプロイ（deployment）** する。**構成は作っただけでは効きません。リージョンを指定してデプロイして初めて反映されます。** ここが試験でよく問われます。

メッシュ接続は、ピアリングを 1 本ずつ張るのと違い、**接続されたグループ（connected group）** という仕組みで実現され、ピアリングの上限に縛られ

にくくなります。

この節のまとめ

- 経路の優先順位は **UDR ＞ BGP ＞ システム ルート**、同順位なら最長一致。
- ピアリングは **非推移的**。スポーク間はハブの NVA／Firewall 経由か直接ピアリング。
- ゲートウェイ トランジット＝ハブで「許可」、スポークで「リモート ゲートウェイを使用」。**スポークに自前ゲートウェイがあると不可**。
- NVA を VM で作るなら **IP 転送を有効化**。
- 強制トンネリングは `0.0.0.0/0 → 仮想ネットワーク ゲートウェイ`。**GatewaySubnet には付けない**。
- Route Server は **ASN 65515**、RouteServerSubnet /27 以上、データ パスには入らない。
- NAT Gateway は **送信専用・ゾーン リソース・IP 最大 16・1 IP あたり 64,512 ポート・既定タイムアウト 4 分**。
- AVNM は **デプロイして初めて効く**。

1-4 ネットワークの監視 [1.4]

公式の到達目標（原文）	意味
Configure monitoring, network diagnostics, and logs in Azure Network Watcher	Network Watcher の監視・診断・ログの構成
Monitor and troubleshoot network health by using Azure Network Watcher	Network Watcher によるネットワーク正常性の監視とトラブルシューティング

公式の到達目標（原文）	意味
Monitor and troubleshoot networks by using Azure Monitor for Networks	Azure Monitor for Networks（ネットワーク分析情報）による監視
Activate and monitor distributed denial-of-service (DDoS) protection	DDoS 保護の有効化と監視
Evaluate network security recommendations identified by Microsoft Defender for Cloud Secure Score	Defender for Cloud のセキュア スコアの推奨事項の評価
Evaluate network security recommendations identified by Microsoft Defender for Cloud attack path analysis	攻撃パス分析の推奨事項の評価
Identify network resources by using Cloud Security Explorer in Microsoft Defender for Cloud	クラウド セキュリティ エクスプローラーによるネットワーク リソースの特定

Azure Network Watcher

Network Watcher はリージョン単位のサービスで、VNet を持つリージョンでは自動的に有効化されます。道具は「診断」「監視」「ログ」の 3 群に分かれます。

診断ツール

ツール	何が分かるか
IP フロー検証（IP flow verify）	指定した 5 タプル（送信元／宛先 IP・ポート・プロトコル・方向）が、**NIC に効く NSG の規則と、VNet に適用された Azure Virtual Network Manager のセキュリティ管理規則の両方で**許可されるか拒否されるか。拒否ならどの規則が拒否したかまで返る。テストできるのは **TCP と UDP** のみ
NSG 診断（NSG diagnostics）	IP フロー検証の強化版。NSG **とセキュリティ管理規則**の両方を評価し、通過した規則の連鎖を返す。**ICMP** や**仮想マシン スケール セット**に効く規則もテストできる
次ホップ（Next hop）	指定した宛先へのパケットが **次にどこへ行くか**（インターネット／仮想アプライアンス／仮想ネットワーク ゲートウェイ／なし）とルートの出所
有効なセキュリティ規則（Effective security rules）	NIC・サブネットに実際に効いている NSG 規則の合成結果
接続トラブルシューティング（Connection troubleshoot）	送信元から宛先への到達性を **その場で 1 回テスト**し、遅延とホップを返す
パケット キャプチャ（Packet capture）	VM 上でパケットをキャプチャし、ストレージ アカウントかローカルへ保存。フィルターと時間・サイズの上限を指定
VPN トラブルシューティング（VPN troubleshoot）	ゲートウェイと接続の診断を実行し、結果とログをストレージへ出力

監視ツール

- **接続モニター（Connection Monitor）**：到達性を**継続的に**測ります。Azure VM 同士、Azure↔オンプレミス、Azure↔外部 URL を、エージェン

トを入れて監視し、チェックの失敗率・往復時間・ホップ単位のトポロジを可視化します。「1 回だけ調べる」のが接続トラブルシューティング、「ずっと見張る」のが接続モニター、という対比で覚えます。

- **トポロジ（Topology）**：VNet・サブネット・NIC・接続の関係を図示します。

ログ

- **仮想ネットワーク フロー ログ（VNet flow logs）**：**VNet 単位**でフロー（許可／拒否されたトラフィックの 5 タプル、バイト数、パケット数）を記録します。現在の推奨はこちらです。
- **NSG フロー ログ（NSG flow logs）**：NSG 単位の従来型。**廃止が公式に告知されており、VNet フロー ログへの移行が案内されています。**「新規で作るならどちらか」→ **VNet フロー ログ**。
- **トラフィック分析（Traffic Analytics）**：フロー ログを Log Analytics ワークスペースに取り込み、上位の通信相手・悪意ある IP との通信・オープンポートなどを分析します。フロー ログ単体は生データ、可視化と洞察はトラフィック分析、という関係です。

フロー ログの出力先は**ストレージ アカウント**で、保持期間を設定できます。トラフィック分析を使う場合は Log Analytics ワークスペースも必要です。

Azure Monitor for Networks（ネットワーク分析情報）

Azure Monitor のネットワーク分析情報（Network Insights） は、サブスクリプション内のネットワーク リソースを、種類別・正常性別に一覧できるダッシュボードです。個々のリソースへ入らずに、Application Gateway・ロード バランサー・ExpressRoute 回線・VPN ゲートウェイ・Firewall の状態と主要メトリックをまとめて見られます。依存関係ビューでは、リソース間の関係と、それぞれのメトリック・ログへの導線が得られます。

メトリックとアラートの設計も出ます。代表的なものは次のとおりです。

- VPN ゲートウェイ：トンネルの帯域、トンネルの出入りバイト数、BGP ピアの状態、**トンネル接続数**。
- ExpressRoute：回線の入出力ビット数、BGP 可用性、Global Reach の帯域、ARP 可用性。
- ロード バランサー：**データ パスの可用性（Data path availability）**、ヘルス プローブの状態、SNAT 接続数（SNAT ポート枯渇の検知に使う）。
- Application Gateway：**正常なホスト数（Healthy host count）**、応答状態、スループット。
- Azure Firewall：**SNAT ポートの使用率**、スループット、ファイアウォールの正常性状態。

Azure DDoS Protection

Azure は、すべてのパブリック IP に対して **DDoS ネットワーク保護（インフラストラクチャ保護）** を無償で提供しています。これは Azure 全体を守るための基礎保護で、テナント個別のチューニングは行いません。

有償の保護は 2 つの階層です。

階層	単位	特徴
DDoS ネットワーク保護（Network Protection）	**VNet 単位**（DDoS 保護プランを VNet に関連付ける）	VNet 内のすべてのパブリック IP を保護。適応型チューニング、攻撃メトリックとレポート、攻撃時のログ、迅速な対応（Rapid Response）チームへのアクセス、コスト保護

階層	単位	特徴
DDoS IP 保護（IP Protection）	**パブリック IP 単位**	保護対象を個別に選ぶ。小規模向け。迅速な対応やコスト保護は含まれない

保護の中身は **適応型リアルタイム チューニング**です。通常時のトラフィックパターンを学習し、しきい値（TCP SYN／TCP／UDP のパケット毎秒）を自動で調整します。攻撃が始まると、しきい値を超えたトラフィックを緩和し、**攻撃緩和レポート**と**緩和フロー ログ**を出します。

監視では、`Under DDoS attack or not`（攻撃を受けているか）というメトリックにアラートを設定するのが定石です。**保護されるのはパブリック IP を持つ L3/L4 のリソースであり、アプリケーション層（L7）の攻撃は WAF（第5章）で守ります。**「SQL インジェクションや HTTP フラッドはどちらで守るか」→ **WAF**、という切り分けが問われます。

図 1-9　Azure DDoS Protection —— 単位の違いと、守る層の切り分け

Microsoft Defender for Cloud

セキュア スコア（Secure Score） は、推奨事項の達成度を点数で示すものです。ネットワーク関連では「インターネットに面した VM に NSG を関連付ける」「管理ポート（RDP／SSH）をインターネットに開かない（Just-in-Time アクセスを使う）」「サブネットに NSG を関連付ける」「IP 転送を無効にする」といった推奨が並びます。点数は**推奨事項を修復すると上がる**ため、優先順位付けの指標として使います。

攻撃パス分析（attack path analysis） は、個々の設定不備ではなく、**攻撃者が実際に辿れる経路**をグラフで示します。「インターネットに公開された VM に重大な脆弱性がある → その VM の管理 ID が機密データを持つストレージへアクセスできる」といった連鎖を提示し、**その連鎖を断ち切る 1 手（choke point）** を推奨します。個別の推奨事項が大量にあるとき、どれから直すべきかを決めるための道具です。

クラウド セキュリティ エクスプローラー（Cloud Security Explorer） は、クラウド セキュリティ グラフに対する**検索**です。「インターネットに公開されていて、かつ重大な脆弱性があり、かつ機密データに触れられる VM」のような条件を組み立てて、該当リソースを列挙できます。ネットワーク観点では、「公開されているリソース」「特定のポートが開いているリソース」を洗い出す用途で使います。

3 つの関係は、**セキュア スコア＝どれだけ直せているかの指標／攻撃パス分析＝どこから直すべきかの優先順位／クラウド セキュリティ エクスプローラー＝条件を指定して探す道具**、と整理して覚えてください。

この節のまとめ

- 1 回だけ試す＝**接続トラブルシューティング**、継続監視＝**接続モニター**。

- どの規則で落ちたか＝**IP フロー検証**／**NSG 診断**（どちらも **NSG とセキュリティ管理規則の両方**を評価する。ICMP と仮想マシン スケール セットは **NSG 診断**）。どこへ行くか＝**次ホップ**。
- 新規のフロー ログは **VNet フロー ログ**（NSG フロー ログは廃止告知済み）。可視化は **トラフィック分析**。
- DDoS は **ネットワーク保護＝VNet 単位**／**IP 保護＝パブリック IP 単位**。L7 は WAF の担当。
- Defender for Cloud：**セキュア スコア＝指標**／**攻撃パス分析＝優先順位**／**クラウド セキュリティ エクスプローラー＝検索**。

サンプルはここまでです

続き(第2章〜巻末)は、AZ-700 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

AZ-700 学習用テキスト(無料サンプル)

版

2026年9月版(AZ-700 出題範囲(Microsoft Learn 公式 Study guide・Skills measured as of July 27, 2026)準拠)

発行

IT資格道場(https://www.shikaku-doujou.com)

お問い合わせ

info@shikaku-doujou.com