【Azure VPN Gateway】トラブルシューティング

2026年3月31日

改訂履歴

版数	発行日	改訂内容
第1版	2026年2月20日	初版発行

本資料の内容は 2026/2/20 時点のものです。製品のアップデートにより変更となる場合があります旨ご了承ください。

Agenda

1. 前提情報
    1. 本資料の目的
    2. 用語集
2. Azure VPN Gateway 概要
    1. Azure VPN Gateway とは
    2. 利用する理由・背景
    3. 接続の仕組み
    4. 冗長構成時に事前に確認すべき要点
3. 運用サイクル
    1. Azure VPN Gateway が定期的に更新される理由
    2. 更新時に起こりやすいこと
4. 運用管理と監視方法
    1. Azure Monitor（メトリック監視）
    2. Azure Monitor（リソースログ / 診断ログ）
    3. Network Watcher（Connection Monitor）
5. トラブルシューティングの切り分け手順
    1. 切り分けの考え方
    2. 切り分けのフローチャート
    3. ① トンネル確立前：VPN 接続自体ができない
    4. ② 認証エラー：認証方式（PSK / 証明書 / Entra ID）で失敗
    5. ③ ルーティングエラー：接続はできるが通信が届かない
    6. ④ 運用・変更起因：設定変更・期限切れ・環境変更による影響

1. 前提情報

1.1. 本書の目的

目的

本資料は、以下を目的とします。

- **Azure VPN Gateway の基本的な仕組みおよび構成要素に関する理解を深める**
- **発生しやすいトラブル（ネットワーク疎通不良や権限設定の問題など）に対する基本的な切り分け方法を整理し、原因特定および初期対応が行える状態を目指す**

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	通信トンネル	インターネット上に暗号化した仮想専用経路を作る仕組み。
2	IPsec/IKE	IP 通信を暗号化して保護する技術。IKE は暗号鍵を自動的に交換する仕組み。
3	クライアント証明書	ユーザーや端末が正当であることを証明するデジタル証明書。
4	OpenVPN	安全なVPN接続を実現するオープンソースの VPN ソフトウェア。
5	ルート証明書	他の証明書の正しさを保証する、信頼の最上位にある証明書。
6	動的ルーティング	ネットワーク状況を自動で判断し、最適な経路に切り替える仕組み。
7	BGP	インターネット間で経路情報を交換する主要なルーティングプロトコル。
8	SSTP	TCP 443番ポートで接続できる、安全な VPN プロトコル。
9	ExpressRoute	Azure と企業ネットワークを専用線で接続する高速・安定のサービス。
10	ネットワークコンポーネント	ネットワークを構成する機器や要素。ルーター、スイッチ、Firewall（以後 FW）など。
11	プロトコル	機器同士が通信するための共通ルール。例：TCP/IP、HTTP。
12	冗長構成	障害に備え、同じ機能を複数用意して止まらない仕組み。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
13	サブネット	ネットワークを小さく分割し、管理しやすくするための区分。
14	再ネゴシエーション	通信中に暗号方式などを再確認し、設定を更新する仕組み。
15	暗号スイート互換性	通信する両者が同じ暗号方式を使えるかどうかの互換性。
16	トラフィック	ネットワーク上を流れるデータ量のこと。
17	パケットロス	送信したデータが途中で消失する現象。遅延や通信品質低下の原因。
18	MFA	複数の認証方法で安全性を高める仕組み。 多要素認証のこと。
19	Active-Active	複数機器を同時稼働させ、負荷分散しつつ停止しない構成。
20	ハブ＆スポーク構成	中心（ハブ）となるネットワークが交通の中心地のようにすべてを管理し、そこから放射状（スポーク）に他のネットワークが接続される構成。
21	Microsoft バックボーン	Microsoft が世界中に持つ高速・高信頼の専用ネットワーク網。
22	スループット	一定時間に処理できる通信量。性能を示す指標。
23	エントリポイント	通信が最初に入る場所。ゲートウェイや入口サーバーなど。
24	CPU	コンピュータの計算処理を担当する中心的なハードウェア。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
25	ルーティングテーブル	各パケットをどの経路へ送るかを示した一覧表。
26	BGP ピアリングイベント	BGP 間の接続確立や切断など、経路交換に関するイベント。
27	Log Analytics Workspace	Azure のログを集約・分析するための格納先サービス。
28	KQL	Azure のログ検索に使うクエリ言語。高速で柔軟な分析が可能。
29	Storage Account	Azure のデータ保管サービス。Blob や File など多用途に利用。
30	Event Hub	大量データをリアルタイムで受け取り処理するイベント基盤。
31	PSK	事前共有鍵方式。接続前に共有した共通鍵で認証する仕組み。
32	Service Account Authentication	サービスやアプリが自動処理するためのアカウント認証方式。
33	Shared Key	共有鍵方式。ストレージへのアクセス制御に用いる鍵。
34	ポート（UDP 500 / 4500、ESP）	VPN(IPsec)で使う主要ポート。500 / 4500 は IKE、ESP は暗号化データ。
35	Yamaha、FortiGate、Cisco	代表的なネットワーク機器メーカー。VPN / FW などで広く利用。
36	Firewall	不正通信を遮断するネットワーク保護装置。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
37	UTM	Firewall（以後 FW ）に加え、侵入防止など複数のセキュリティ機能を統合した装置。
38	UDR（ユーザー定義ルート）	Azure で独自のルートを設定し、通信経路を制御する機能。
39	ローカルネットワークゲートウェイ	Azure VPN で “オンプレミス側情報” を登録する設定項目。
40	Azure ASN	Azure が BGP で使う自律システム番号（ ASN ）。経路交換に必要。
41	BGP ピア IP	BGP でルーター同士がピアリングするために使われる相手先の IP アドレス。
42	仮想アプライアンス (NVA)	Azure 上に置く仮想ネットワーク機器。FW やルーター機能を提供。
43	MTU （Maximum Transmission Unit）	一度に送れるパケットの最大サイズ。
44	Keepalive	接続が生きているか確認するための定期的な信号。
45	DPD	Dead Peer Detection。VPN 相手の生存を確認し、死活を検出。
46	静的ルート	管理者が手動で経路を指定するルート設定。変化しない固定経路で安定した通信を実現。
47	オンプレミス VPN Gateway	オンプレミス環境とクラウドをつなぐため、VPN 経由で安全に通信を中継する役割を持つ接続ゲートウェイ。
48	リージョン	Azure がデータセンターをまとめて配置している “地理的なエリア” のこと。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
49	社内 LAN	会社や組織の建物内で使われる内部専用のネットワーク。
50	Entra ID 認証	Microsoft が提供するクラウドの ID 管理サービスである Microsoft Entra ID がユーザーの “本人確認” を行い、クラウドサービスへ安全にアクセスできるようにする仕組み。
51	OpenVPN パッケージ	P2S 接続で OpenVPN プロトコルを使うために、ユーザー端末へ配布される設定構成パッケージ。
52	strongSwan	IPsec を使って安全な VPN接続を構築できるオープンソースのソフトウェア。
53	IKE_SA（phase1）	VPN 接続で使う暗号鍵を安全に交換し、通信相手を認証するための最初のセキュリティ交渉プロセス。

2. Azure VPN Gateway 概要

2.1. Azure VPN Gateway とは

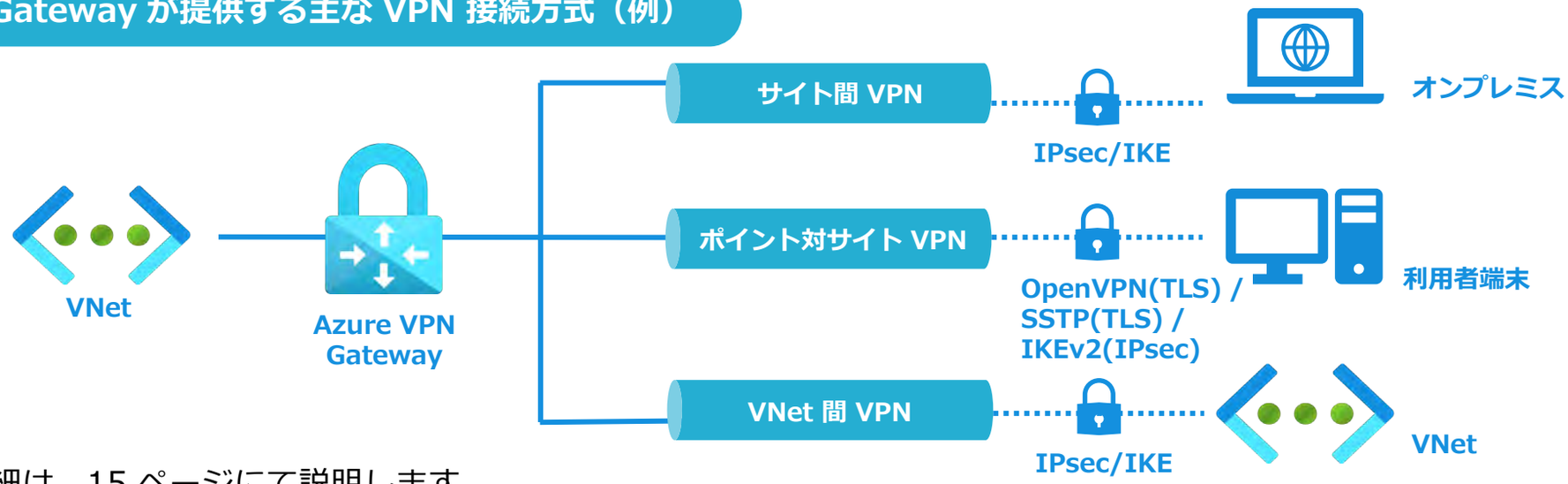
本ページでは Azure VPN Gateway について説明します。

Azure VPN Gateway の概要

Azure VPN Gateway は、Azure 仮想ネットワーク（以下、VNet）とオンプレミス環境、または複数の VNet 間における**セキュアな接続を提供する VPN Gateway サービス**です。

VNet に配置される専用のネットワーク ゲートウェイが VPN 接続の終端として動作し、**暗号化された通信トンネル（IPsec/IKE など）を確立し**制御を行います。
また、1 つの Azure VPN Gateway に対して複数の VPN 接続を設定できるため、複数のオンプレミス拠点や他の VNet など、**さまざまなネットワークと同時に接続が可能**です。

Azure VPN Gateway が提供する主な VPN 接続方式（例）



※接続方式の詳細は、15 ページにて説明します。

2.2. 利用する理由・背景

以下は、Azure VPN Gatewayを導入する際の基本的な背景を整理したものです。

Azure VPN Gatewayの利用背景

■オンプレミスとの安全なハイブリッドクラウド構成

Azure VPN Gateway は IPsec/IKE により、オンプレミスとVNetを暗号化通信で接続します。既存ネットワークを活かしたハイブリッド構成が可能で、常時接続と強固な認証・暗号化により安全なクラウド連携を実現します。

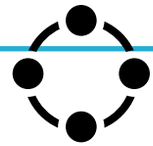
■モバイル／リモートワーカーの安全なアクセス

ポイント対サイト VPN（P2S）により、PC やモバイル端末からVNetへ安全に接続できます。証明書認証や Entra ID、OpenVPN に対応し、社外からでも安全なリモートアクセス環境を提供します。

■マルチクラウド環境との安全な接続

AWS や GCP など他クラウドとの間を VPN で安全に接続し、システム連携やデータ通信を暗号化して行うマルチクラウド構成が可能です。

■ExpressRoute 併用による冗長化



ExpressRoute 障害時のバックアップとして Azure VPN Gateway を併用することで、通信継続性を確保できます。これにより、可用性と耐障害性を高めたネットワーク構成が実現します。

2.3. 接続の仕組み

本項目では、Azure VPN Gatewayで利用できる三種類の接続方法について、それぞれの特徴や主な用途を紹介します。
拠点間接続や各デバイスからのリモートアクセスなど、用途に応じた使い分けがポイントです。各接続方法の詳細は、次のページで解説します。

接続方法の種類

■ポイント対サイト VPN
（Point-to-Site　以後：P2S）

ユーザーのデバイスから VNet へ個別に接続する方式で、クライアント証明書や OpenVPN を使用してリモートワーカーの安全なアクセスを提供します。

■仮想ネットワーク間接続
（VNet間）

複数の VNet を 通信トンネルで相互接続し、リージョン間でもセキュアな通信を可能にします。これにより、システムの分割配置や災害対策構成が柔軟に実現できます。

■サイト間 VPN
（Site-to-Site　以後：S2S）

オンプレミスの VPN デバイスと Azure VPN Gateway を IPsec/IKE を用いて接続し、拠点ネットワーク同士を安全に延長する仕組みです。
拠点間を常時接続するため、企業ネットワークと VNet を一体のネットワークとして扱えます。

以下の表では、接続時に必要となるゲートウェイや仮想ネットワークなどの構成要素を整理して説明しています。

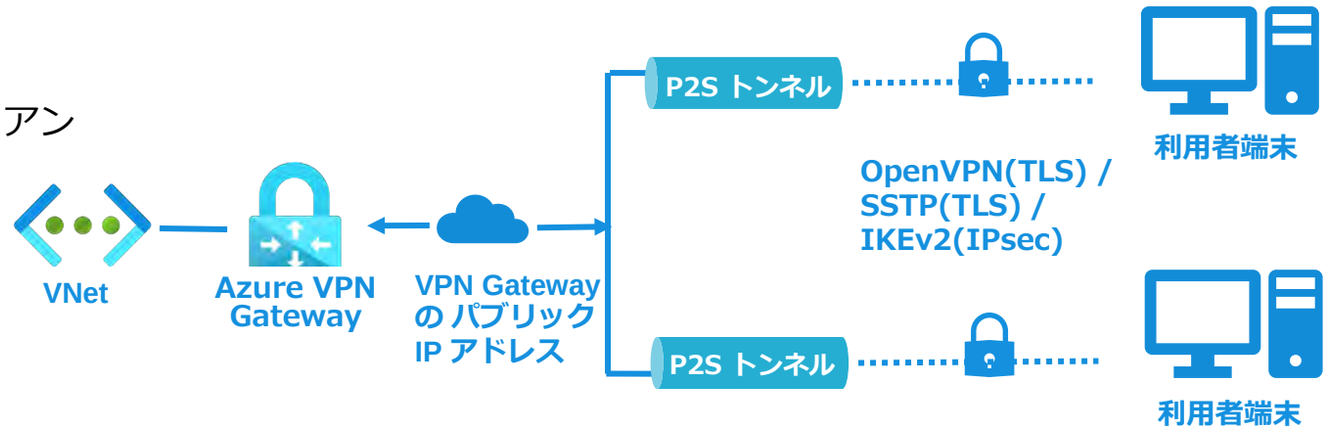
接続方法	構成要素	説明
共通	**VPN Gateway のパブリック IP アドレス**	Azure 側の VPN Gateway がインターネット上で通信するために使う公開 IP アドレス
ポイント対サイト VPN（ P2S ）	**P2S トンネル**	個々のクライアント端末が VNet に直接 VPN 接続するための方式
	VPN クライアント	ユーザーの PC などから VPN 接続を行うためのアプリケーションまたは設定

2.3. 接続の仕組み

ポイント対サイト VPN（ P2S ）

■特徴
・利用者端末から OpenVPN / IKEv2 / SSTP 対応の VPN クライアントを用いて Azure に接続
・証明書認証および Entra ID 認証に対応
・オンプレミス側に VPN 機器を必要としない構成

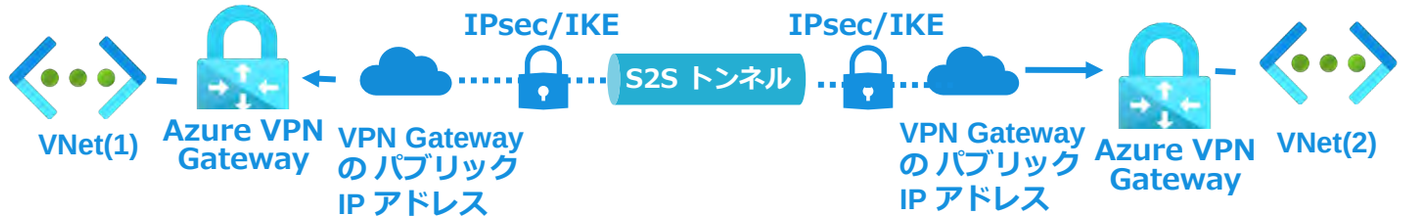
■主な用途
・在宅勤務や外出先から Azure 環境へ安全にアクセス
・管理者の運用作業や開発・検証環境への一時的な接続



仮想ネットワーク間接続（ VNet 間）

■特徴
・Azure リージョン間を含む VNet 同士の接続が可能
・BGP（動的ルーティングの仕組み）を使用し複数の VNet 同士の経路設定を手動ではなく、自動化することが可能
・中心となる VNetを挟み、別々の VNet 同士が通信できる構成が可能

■主な用途
・Azure 内で分離したネットワーク間の安全な接続
・ハブ＆スポーク構成や本番・検証など複数環境間の接続



2.3. 接続の仕組み

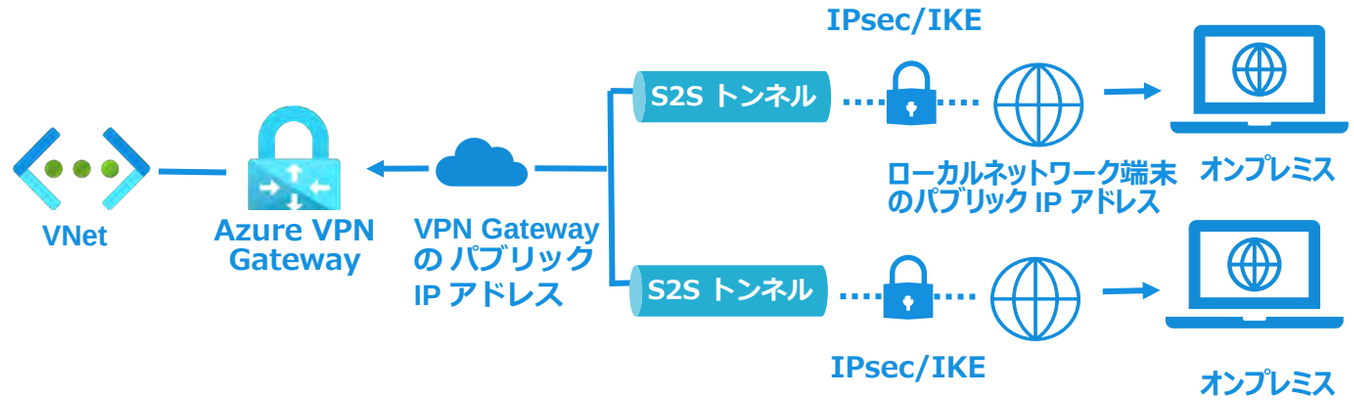
サイト間 VPN（ S2S ）

■特徴

・Azure VPN Gateway とオンプレミス VPN 機器を IPsec/IKE で常時接続し、VNet を社内 LAN の延長として利用可能
・静的ルートおよび BGP による動的ルーティングに対応
・Active-Active 構成により高可用な冗長接続が可能

■主な用途

・オンプレミスと Azure を接続するハイブリッドクラウド構成
・オンプレミス環境から Azure 上の業務システムへの常時アクセス



接続方法	構成要素	説明
サイト間 VPN（S2S）	**オンプレミス**	企業が自ら保有・管理する社内ネットワークやサーバー環境
	IPsec IKEv2 S2S トンネル	Azure とオンプレミスを拠点間（ S2S ）VPN で安全に結ぶ際に使われる暗号化トンネル方式であり、VNet が拠点の場合（ VNet 間）でも利用される
	ローカルネットワーク端末のパブリック IPアドレス	オンプレミス側の VPN 装置がインターネットへ接続するときに使う公開 IP アドレス

2.3. 接続の仕組み

■**VPN クライアントの最新バージョン確認（ P2S 接続）**
Azure VPN Gateway の P2S 接続では、利用するトンネル方式や OS によって対応クライアントが異なります。
設計時には、トンネル方式と OS の対応関係を確認するとともに、VPN クライアントが最新バージョンで利用されていることを事前に確認します。
これにより、暗号化の非互換や OS アップデートとの不整合による接続トラブルを防ぐことができます。

トンネル方式	OS	利用クライアント	最新版の確認場所
OpenVPN（推奨）	Windows 10 / 11	Azure VPN Client（ UWP ）	Microsoft store
	macOS	Azure VPN Client for macOS	Microsoft store
	iOS / iPadOS	OpenVPN Connect	App Store
	Android	OpenVPN Connect	Google Play
	Linux	OpenVPN パッケージ	各ディストリビューションの公式リポジトリ
IKEv2	Windows 10 / 11	Windows OS標準VPN	Windows Update
	macOS	OS標準 IKEv2 クライアント	macOS アップデート
	iOS / iPadOS	OS標準 IKEv2 クライアント	iOS アップデート
	Android	strongSwan等	Google Play
	Linux	strongSwan	strongSwan サイト
SSTP（Windows専用）	Windows 10 / 11	Windows OS標準 SSTP	Windows Update
	macOS / iOS / Android / Linux	非対応	—

注意事項

Azure VPN Gateway では、VNet とオンプレミスの IP アドレス空間が重複すると正常なルーティングができないため、重複がないことを前提に設計を行ってください。

2.4. 冗長構成時に事前に確認するべき要点

以下は、Azure VPN Gatewayの冗長構成時に事前に確認すべき要点を整理したものです。冗長構成の選択、VPNクライアント要件、アドレス設計やSKU・接続数などの前提条件を明確にし、構成不備や要件不足による問題発生を防ぐことを目的としています。

■冗長構成（Active-Active）を設計する場合の検討事項
Active-Active を構成する場合は、以下の 3 つの観点で事前確認が必要です。

①Active-Activeを採用する必要性の確認
コストや設計工数が増えるため、導入目的に立ち返り必要性を明確にします。

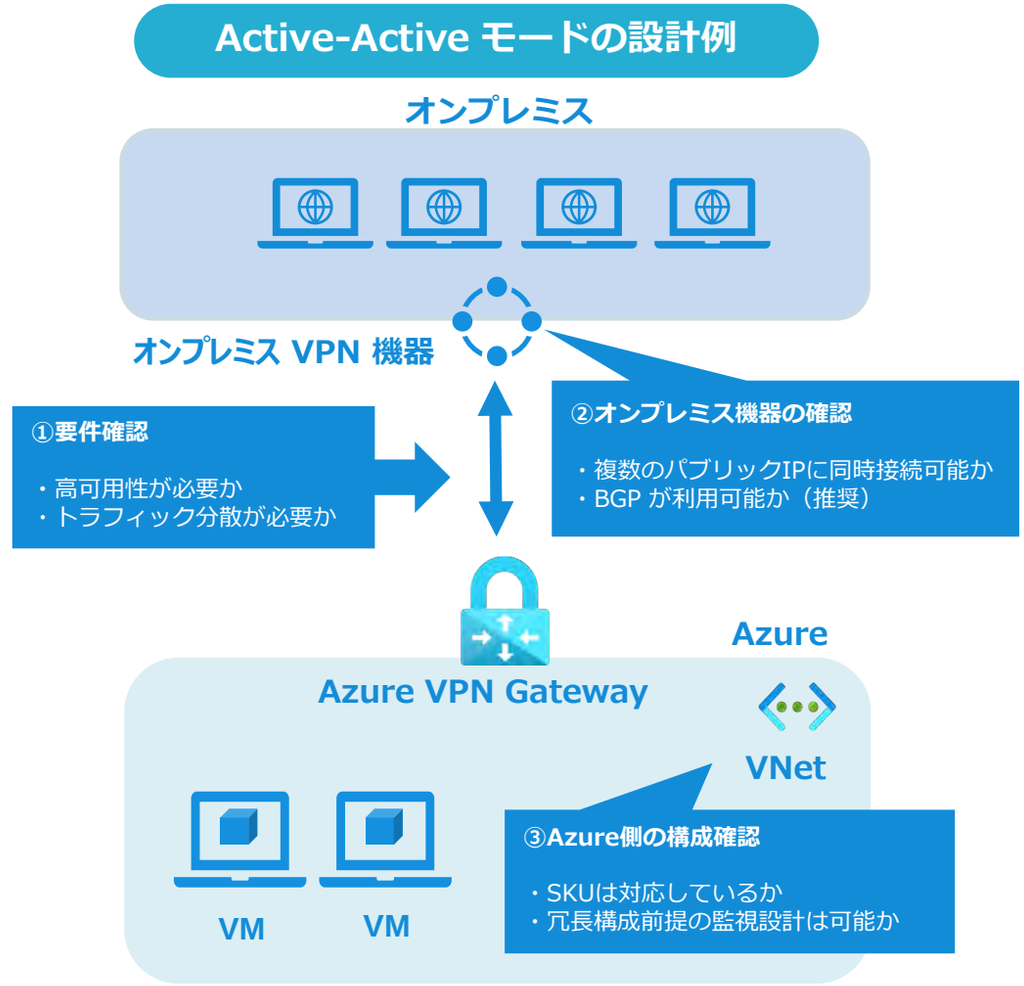
・障害発生時も通信を継続するための高可用性が必要か
・通信量や同時接続数の要件から、性能面でトラフィック分散が必要か

②オンプレミス機器が対応しているか確認
S2S、P2S 接続の場合オンプレミスのネットワーク機器が対応しているか確認します。

・Azure の 2 つのパブリック IP に同時接続できるか
・2 本の VPN トンネルを同時にアクティブ状態で維持できる機能があるか
・BGP が使えるか（ Active-Active構成での経路制御・自動切替のため推奨）

③Azure 側の前提条件の確認
構成要件および運用設計を確認します。

・Active-Active 対応の SKU か（参考リンク）
・Active-Active 前提の監視・障害対を行っているか
（例：片系のトンネルが切断された場合でも通信が継続するため、
冗長性が失われたことを検知できるよう各トンネルを個別に監視する仕組みを導入するなど）



3. 運用サイクル

3.1. Azure VPN Gateway が定期的に更新される理由

Azure VPN Gateway は、サービス品質の維持・向上を目的として定期的に更新されます。本項目では、可用性設計や運用判断の前提知識として、Azure VPN Gatewayが定期的に更新される理由を整理します。更新の目的や背景を理解することで、影響最小化設計や運用サイクル全体の意図を明確にします。

Azure VPN Gatewayが更新される理由

■機能・信頼性・パフォーマンス・セキュリティの継続的向上

Azure VPN Gateway は機能強化、信頼性向上、性能改善、セキュリティ強化を目的として定期的に更新されます。更新には、ソフトウェアパッチ適用、ネットワークコンポーネントのアップグレード、老朽化ハードウェアの廃止などが含まれます。

■クラウド基盤進化とSKU・機能のライフサイクル管理

Azure 基盤の進化に伴い、Azure VPN Gateway でも新機能の追加、既存機能の改善、旧 SKU や構成の非推奨・廃止が計画的に実施されます。

■セキュリティ脅威や標準仕様への対応

Azure VPN Gateway は IPsec/IKE などの業界標準プロトコルを用いるため、暗号アルゴリズムの強化や脆弱性対応が継続的に必要です。ネットワークの重要なエントリポイントであるため、最新のセキュリティ基準を維持する目的で更新が行われます。

■計画メンテナンスとしての更新

Azure VPN Gateway はマネージドサービスとして、安定したサービス提供を維持するため、計画メンテナンスの一環として定期的な更新が実施されます。
これらの更新は業務影響を最小化するよう計画されていますが、一時的な瞬断等は避けられないため、更新の発生を前提とした可用性設計や運用計画が重要となります。

3.1. Azure VPN Gateway が定期的に更新される理由

Azure VPN Gateway の最新情報は、ユーザー自身で公式サイトや実際の画面上から確認できます。以下の表では、主に利用する確認場所と、それぞれで把握できる情報の概要を整理しています。

アップデート・メンテナンス情報の確認方法

確認場所	主に確認できる内容
Microsoft Learn（日本語） 「Azure VPN Gateway の新機能」（リンク）	・新機能 / 一般提供（ GA ）・先行提供（ Preview ）情報 ・非推奨・廃止予定（ SKU / パブリックIP など） ・今後の変更予定と影響
Azure の更新情報（リンク）	・VPN Gateway の新機能 / 一般提供（ GA ）情報 / 提供終了（ Retirement ） 情報 ・他 Azure サービスと横断的に確認可能
Azure の状態（リンク）	・リージョン単位の大規模障害のみ（簡易）
Azure Service Health（ Azure portal 画面）	・自サブスクリプションに影響する障害 ・計画メンテナンス / 事後報告
Azure portal（ VPN Gateway の構成画面）	・メンテナンス通知 ・SKU / 構成変更時の注意・移行案内

3.2. 更新時に起こりやすいこと

Azure VPN Gatewayの更新では、通信断や再接続対応が発生することがあります。本項目では、更新時に起こりやすい代表的な事象と、その背景を整理しています。

更新時に起こりやすいこと

事象	詳細と背景
短時間の通信中断（フェールオーバー）	Azure VPN Gateway は既定で冗長構成（ Active / Standby ）ですが、計画メンテナンスや更新時にはフェールオーバーが発生し、稼働系から待機系へ切り替わる際に10~15秒程度の瞬断が起きる可能性があります。更新作業において想定外の障害発生時には最大数分かかる場合もあります。
P2S 接続の再接続要求	ポイント対サイト（ P2S ）VPN では、更新時にクライアント接続が切断され、ユーザー側手動再接続が必要になります。 常時接続を前提とする用途では影響が生じやすいため注意が必要です。
SKU 移行時の構成確認不足	旧 SKU（Basic、非 AZ SKU 等）から新 SKU への移行時には、パブリック IP の種別変更（Basic → Standard）や Gateway サブネットサイズ、Active-Active 対応可否などの構成要件について、事前に十分な確認が必要です。確認が不十分な場合、想定外の追加作業や一時的なダウンタイムが発生する可能性があります。
一時的な構成制約・操作制限	更新中は、Azure VPN Gateway の構成変更（接続追加・削除、設定変更）が一時的に制限されることがあります。 Microsoft では、変更失敗のリスクがあるため基盤更新中の構成変更操作を避けることを推奨しています。
オンプレミス側機器との再ネゴシエーション	IPsec/IKE トンネルは、更新後に再ネゴシエーションが発生します。 オンプレミス VPN 機器の設定や暗号スイート互換性によっては、再接続に時間がかかる場合があります。

4. 運用管理と監視方法

4.1. Azure Monitor（メトリック監視）

4章では、Azure サービスを利用したAzure VPN Gateway の運用管理と監視方法についてそれぞれ説明いたします。

本項目では、Azure VPN Gateway の運用管理や監視（稼働状況、通信量、負荷状況、異常の兆候）をすることができる **Azure Monitor のメトリック監視**について説明します。

Azure Monitor

Azure Monitor のメトリック監視とは？

Azureのリソース（VM、ストレージ、Azure VPN Gateway など）の 「CPU 使用率」「トラフィック量」「エラー数」などを 時系列グラフ で表示するサービスです。

Azure VPN Gateway における代表的なメトリック項目

項目	メトリック	内容
トラフィック量・データ量関連	Ingress Bytes / Egress Bytes	Ingress：受信したデータ量（バイト） Egress ：送信したデータ量（バイト）
	Ingress Packets / Egress Packets	パケット数（通常時と比較した通信回数の傾向や、DoS 攻撃のような異常な増加が発生していないかを確認）
接続数・セッション関連	Tunnel Count / Connection Count	有効な VPN トンネル数・接続数
	Failed Connections	VPN 接続が失敗した回数
ゲートウェイ全体の状態に関わるもの	CPU / Processor Time	Azure VPN Gateway の CPU 負荷イメージ
	P2S（ Point-to-Site ）接続関連メトリック	同時接続ユーザー数など

必要に応じて Log Analytics へエクスポートし、リソースログ（ Gateway / Tunnel / IKE / P2S ）と相関分析できます。
次ページでリソースログ / 診断ログについて説明します。

4.2. Azure Monitor（リソースログ / 診断ログ）

本項目では、Azure VPN Gateway のトラブルシュートや原因調査のためにより詳しい内部ログを取得**する Azure Monitor のリソースログや診断ログ**について説明します。

Azure Monitor のリソースログ / 診断ログとは？

Azure のリソースが「内部でどんな処理をしたか」を、詳細なログとして記録・保存する仕組みです。
エラー内容や接続処理の流れ、VPN のトンネル確立・切断のイベントなど、
数値では見えない “動作の中身” を把握するためのログを取得できます。

Azure VPN Gateway における代表的なログ項目

ログ	内容	例
GatewayDiagnosticLog	ゲートウェイ内部のイベントログ	• ゲートウェイの起動 / 停止 • 設定変更 / 更新 • ルーティングのイベント、障害の発生、エラー情報
TunnelDiagnosticLog	IPsec トンネル・IKE のイベントログ	• トンネル確立 / 切断 / 再試行 • IPsec/IKE のエラーメッセージ
RouteDiagnosticLog	ルート（経路）に関するログ	• ルーティングテーブルの更新、学習した経路 • BGP ピアリングイベント（BGP を使う場合）
IKEDiagnosticLog	P2S や S2S の IKE（鍵交換・認証）ログ	• 認証成功 / 失敗 • 証明書・パラメータ不一致（暗号方式違いなど）
P2SDiagnosticLog	クライアントユーザー単位のログ	• 接続 / 切断したユーザー名 • 接続元 IP • 認証方式（証明書・Entra ID など）

ログの保存先

Azure Monitor の診断ログは、一般的には **Log Analytics Workspace** に保存し、KQL を使って検索・分析・可視化することができます。
また必要に応じて、Storage Account や Event Hub に保存することも可能です。

4.3. Network Watcher（Connection Monitor）

本項目では、Azure VPN Gateway を経由した 主にAzure とオンプレミス間の通信が問題なく行われているかを確認することができる **Network Watcher（Connection Monitor）** について説明します。

Network Watcher

Network Watcher（Connection Monitor）とは？

Azure とオンプレミス / 他拠点間の ネットワークの疎通を監視し、通信がどこで止まっているのかを可視化する監視サービスです。
Azure VPN Gateway を経由した Azure とオンプレミス間の通信が正常に行われているかを監視し、遅延・パケットロス・通信断などの発生箇所を特定することができます。

できること

✓ **通信テスト（疎通チェック）を自動で実行**
- Azure ⇔ オンプレミス
- 複数の拠点が Azure を経由して相互に通信する場合の、拠点同士などの到達性テストを行うことができます。

✓ **「どの区間で失敗したか」を可視化**
以下のような**切断区間を可視化**できます。
- Azure 側 / オンプレミス側 / インターネット区間 / VPN トンネル / ルート

✓ **遅延・パケットロスの測定**
- Latency (遅延) / Packet loss (損失)
  Hop ごとの状況（通信経路上で、どの区間・中継点に問題があるか）
  → パフォーマンス問題の原因調査をすることが可能です。

✓ **アラートの作成**
- 異常時にメール / Teams に通知することができます。

メトリック、ログ、Network Watcherの比較

種類	主な目的	参考Microsoft社記事
メトリック	VPN Gatewayの状態を数値化し監視する	Azure Monitor メトリックの概要
リソースログ / 診断ログ	VPN Gatewayの処理内容を記録	Azure Monitor のリソース ログ
Network Watcher	VPN Gatewayとオンプレ間のネットワークの到達性そのものを監視	Azure Network Watcher とは

これら 3 つの監視ツールを組み合わせることで、通信の状態把握から原因切り分けまでを段階的かつ効率的に行うことができます。

５．トラブルシューティングの切り分け手順

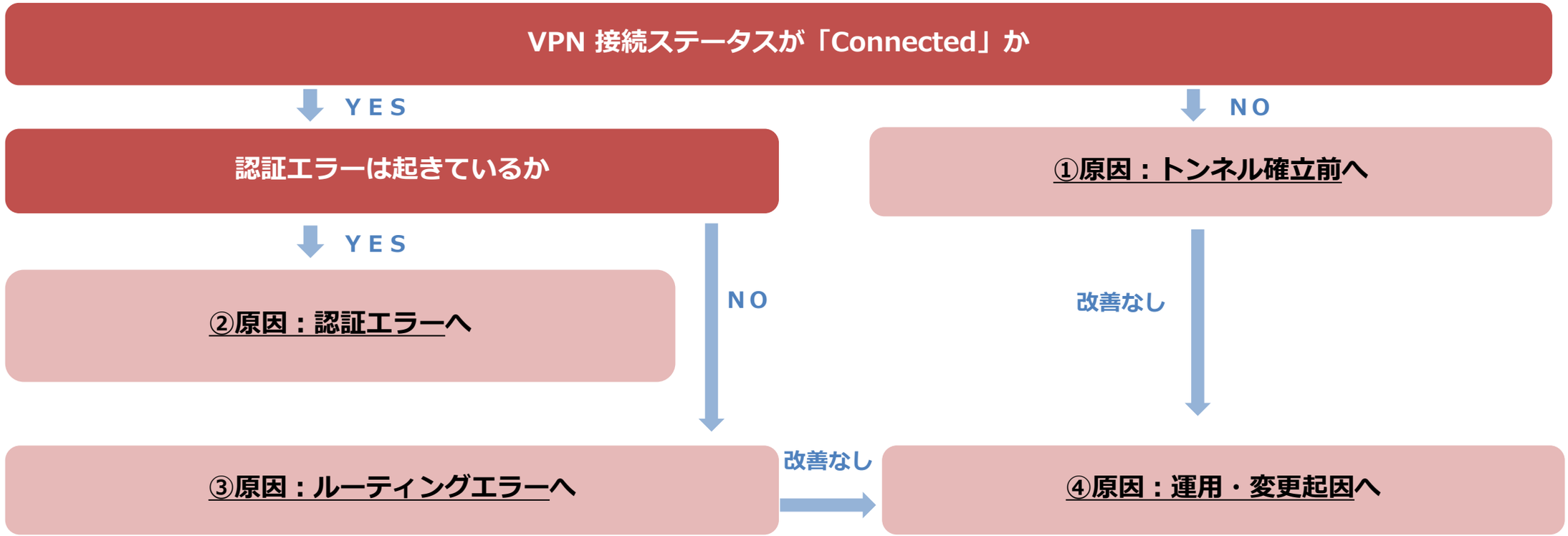
5.1. 切り分けの考え方（4分類）

5章では、Azure VPN Gateway におけるトラブルを迅速に特定するため、原因を以下の4つの観点に分類し、それぞれの切り分け手順を紹介いたします。
次のページ以降でそれぞれの**概要、原因、実際にあった事例、対処法**を解説いたします。

切り分けの考え方（4分類）	内容
① 原因：トンネル確立前 →VPN 接続自体ができない	IKE（VPN の接続の最初の段階）が始まらない、または途中で止まってしまっている状態。 Azure portal では接続状態が 「Not connected」 と表示され、IKE_SA（phase1）の確立ができていない。 この場合の多くは “通信経路の問題” や “基本設定のミス” が原因となる。
② 原因：認証エラー →認証（PSK / 証明書 / Entra ID）ができない	IKE の接続は始まっているが、認証で失敗している状態。 Azure 側には “Authentication failed（認証失敗）” などと表示され、 相手の装置は見えているけれど、正しい相手だと信頼できない状態。
③ 原因：ルーティングエラー →接続はできるが通信が届かない	VPN の接続ステータスは 「Connected」 だが、Azure の VM とオンプレミス間で通信ができない状態。 暗号化部分は問題なく、“ルーティング（経路設定）” や “ファイアウォール（通信の許可設定）” といった設定が原因となるケースが多い。
④ 原因：運用・変更起因 →設定変更・期限切れ・環境変更による影響	明確なエラーが出ないケースも多く、 設定変更・期限切れ・環境変更が原因となる。

5.2. 切り分けのフローチャート

Azure VPN Gateway のトラブルを、「接続不可 → 認証エラー → ルーティング → 運用変更」の順に切り分けるための総合フロー図です。



5.3. ① トンネル確立前：VPN 接続自体ができない

本項目では、VPN接続が「Connected」にならない、トンネルが確立しない場合の原因、過去事例、対処法について紹介いたします。

トラブル概要

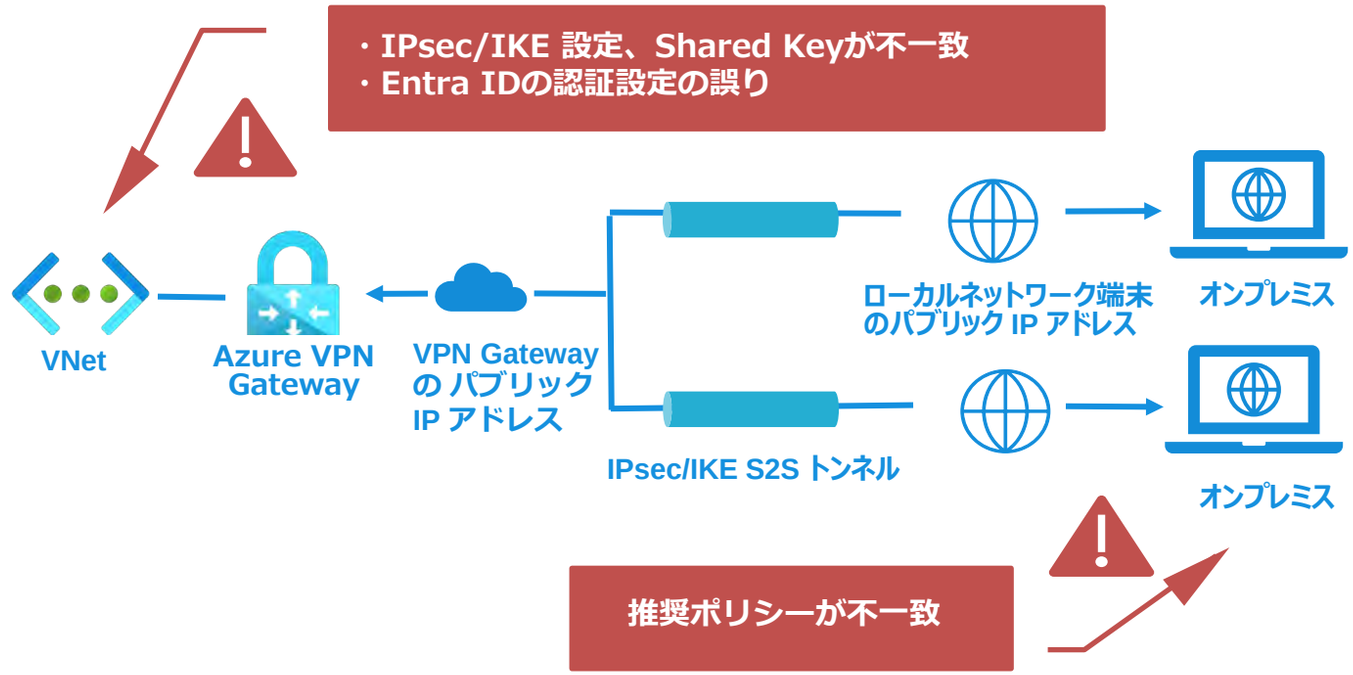
・VPN接続が「Connected」にならない
・トンネルが確立しない

過去の事例

Azure ポータルで VPN 接続の状態が「Connected」にならずトンネルが確立できない。
調査した結果 Azure 側から送信された Service Account Authentication に対してオンプレミスの VPN デバイスが認証失敗の応答を返していなかったことが原因。
そのため、IPsec/IKE 設定や Shared Key の不一致などオンプレミス側の構成を確認いただくことで解決。

原因

・Azure VPN Gateway と 対向デバイスの IPsec/IKE 設定、Shared Key、推奨ポリシーが不一致
・Azure VPN Gateway と 対向ルーター間の通信経路で、必要ポート（UDP 500 / 4500、ESP）が許可されていない
・Entra ID の認証ポリシー不一致



5.3. ① トンネル確立前：VPN 接続自体ができない

対処法

① Shared Key の設定確認 （S2S/VNet間）

Azure

Azure portal ＞ VNet Gateway ＞ 接続 ＞
対象VPN選択 ＞ ［共有キー］または［事前共有キー］の表示が正しいか確認

オンプレミス

VPN デバイス（Yamaha、FortiGate、Cisco など）で
VPN 接続プロファイルに設定されている Pre-shared keyが
Azure側の［共有キー］または［事前共有キー］と一致しているか確認

② IPsec/IKE SA の設定再確認 （S2S/VNet間）

Azure

Azure portal＞VNet Gateway＞接続＞
対象VPN選択＞IPsec/IKE ポリシーの表示

オンプレミス

VPN デバイス（Yamaha、FortiGate、Cisco など）で
VPN 接続プロファイルに設定されているIKE_SA（Phase 1）
IPsec（Phase 2）がAzureのIPsec/IKE ポリシーと
一致しているか確認

③ Azure VPN Gateway 推奨ポリシーへの統一 （S2S/VNet間）

Azure とオンプレミスの VPN 暗号設定（IPsec/IKE）を “Azure 推奨値” に揃えて、トンネルの安定性と互換性を確保する
※Microsoft社公式の推奨ポリシーを参照（リンク）

④必要ポートの疎通確認（ Firewall / UTM ） （共通）

オンプレミス→ Azure 方向（Outbound）に必要ポート（UDP 500 / 4500、ESP）が許可されているか確認
ログ（Firewall / UTM）のブロック履歴を確認

⑤認証設定の見直し（P2Sのみ）

P2S特有の認証設定の見直しについては、次のページで解説します

ポイント

Phase とは、IPsec VPN における暗号化設定の交渉段階を指します。

Phase 1（IKE_SA）では VPN 接続の土台となる認証・鍵交換を行い、
Phase 2（IPsec）では実際にデータ通信を行うための暗号化方式を決定します。
Azure 側とオンプレミス側で Phase 1 / Phase 2 の設定が一致していない場合、
VPN 接続は確立できません。

5.4. ② 認証エラー：認証方式（証明書／Entra ID）で失敗

本項目では、認証関連のエラーが起きた場合の原因、過去事例、対処法について紹介いたします。
認証まわりのトラブルはユーザー端末側で認証を行うP2S特有のものとなります。

トラブル概要

・接続試行はできるが認証段階でエラーが発生する
・Entra IDのログインが通らない

原因

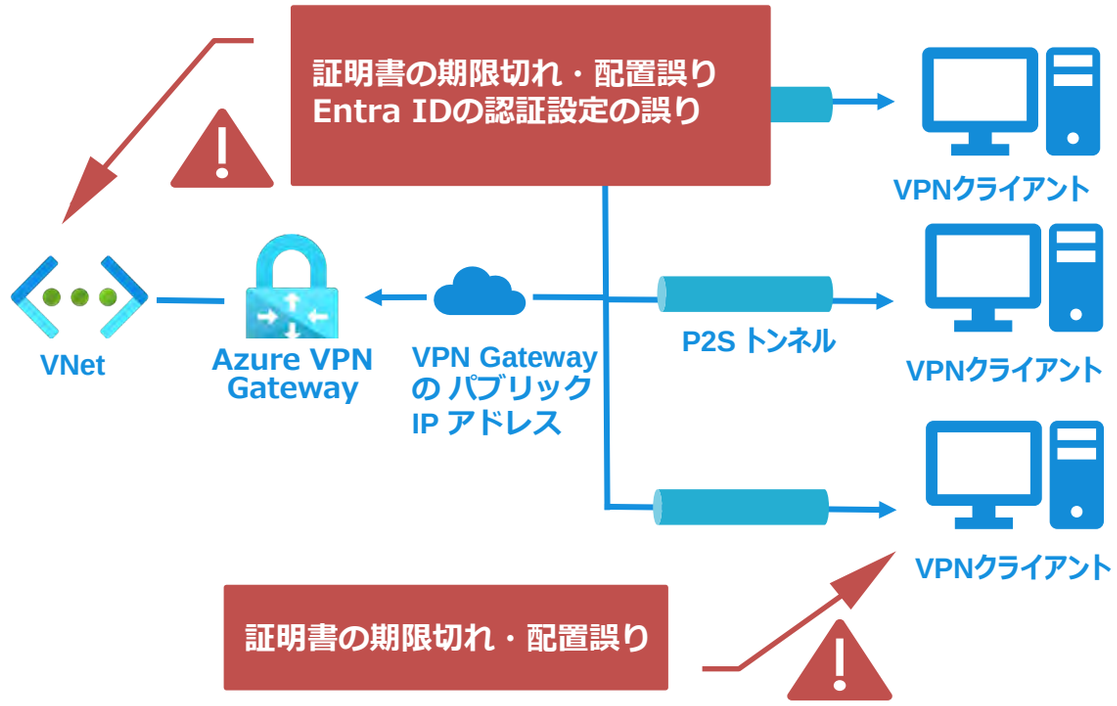
・Entra IDの認証設定の誤り
・Azure VPN Gateway と 対向デバイスの証明書の期限切れ・配置誤り

過去の事例

Azure VPN への接続時にクライアント側で接続エラーが発生する。

調査した結果、Azure に保存されている認証情報とクライアント側から送信された認証情報が一致していなかったことが原因。

証明書の期限切れや配置ミスが考えられたため、認証関連の設定を確認いただくことで解決。



5.4. ② 認証エラー：認証方式（Key／証明書／Entra ID）で失敗

対処法

Entra ID で認証をしている場合（P2Sのみ）

①アプリ登録（App Registration）の設定を再確認

Azure portal ＞Entra ID＞アプリの登録で
Client ID、TenantIDを確認

②Azure VPN Gateway の Entra ID情報が正しいか確認

Azure portal ＞VNet Gateway＞認証＞Entra IDで
TenantID、Application ID、Issuer URLが
アプリの登録と一致しているか確認

③ユーザーがアプリにアクセスできる状態になっているか確認

該当ユーザー（またはグループ）にライセンス割り当て済み か確認

④条件付きアクセスの影響を確認

Entra ID＞条件付きアクセスで「MFA 必須」「準拠デバイス必須」
が有効な場合、VPN が弾かれることがあるため、確認

⑤Azure VPN Client のプロファイルを最新化

最新版のAzure VPN Clientのダウンロード＞
Azure VPN Client にクライアントプロファイル構成ファイルをインポート

証明書 で認証をしている場合（P2Sのみ）

①登録したルート証明書が正しいか確認

Azure portal＞証明書で接続先の証明書となっているか確認

②ルート、クライアント証明書の有効期限を確認

Azure portal＞証明書＞証明書の有効期限 を確認

③クライアント側に正しくインストールされているか確認

Windows の「証明書マネージャー」を開き、
ルート、クライアント証明書を確認

④必要であれば証明書を再発行する

ポイント

利用している認証方式をAzure portal で確認し、その方式に合わせて適切なトラブルシューティングを実施してください。

5.5. ③ ルーティングエラー：接続はできるが通信が届かない

本項目では、接続はできるが通信が届かない場合の原因、過去事例、対処法について紹介いたします。

トラブル概要

・トンネル内のトラフィックが通らない

過去の事例

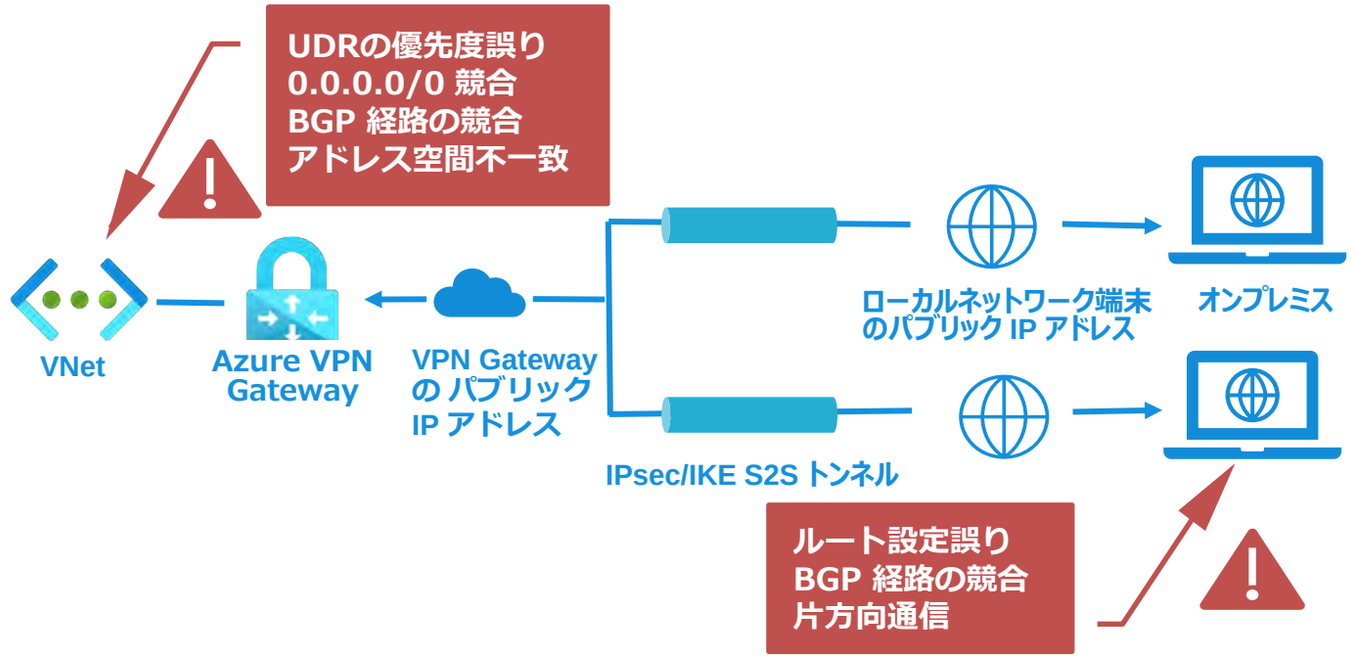
VPN Gateway の P2S 機能を利用して Azure 環境にログインしているが VPN が頻繁に接続できない。

調査した結果、リモート側ネットワーク機器（ルーターなど）が VPN 接続を許可する設定になっておらず、その結果リモートサーバーが応答せず接続が確立できていないことが原因。

ルート設定の誤りが疑われたため、ネットワーク機器側の設定を確認いただくことで解決。

原因

・Azure 側 VNet／サブネット と 対向ネットワーク側 のルート設定誤り
・Azure 側のUDR （ユーザー定義ルート）の優先度誤り
・Azure VNet の有効ルート と ローカルネットワークゲートウェイ側の 0.0.0.0/0 の競合
・Azure VPN Gateway と 対向ルーター間 のBGP 経路の競合
・ローカルネットワークゲートウェイのアドレス空間不一致
・Azure から対向ネットワークへの戻りルート の欠落（片方向通信）



5.5. ③ ルーティングエラー：接続はできるが通信が届かない

対処法

①Azure VM の「有効なルート」を確認（共通）

Azure

Azure portal＞仮想マシン＞ネットワーク＞
有効なルートで宛先を確認

オンプレミス

オンプレミスルーターの ルーティングテーブルでVPN接続
を許可するように設定されているかを確認

②戻りルートの確認（共通）

Azure

Azure portal＞VM ＞ネットワーク＞
ネットワークインターフェイス＞効果的なルート
でルートが 「Virtual network Gateway」になっているか
を確認

オンプレミス

オンプレミスルーターのルーティングテーブルに
Azure VNet あてのルートが存在するかを確認

③ローカルネットワークゲートウェイのアドレス空間 や「0.0.0.0/0」の競合を確認　（S2S/VNet間）

Azure portal ＞ローカルネットワークゲートウェイで以下を確認
- オンプレミスのネットワークが全て入っているか
- “アドレス空間”に 0.0.0.0/0 を入れていないか確認

④BGP 経路の競合の確認　（S2S/VNet間）

Azure portal>仮想ネットワークゲートウェイ＞VPN Gateway＞
BGPで以下がオンプレミス側と一致しているかを確認
- Azure ASN
- BGP ピア IP

⑤UDR（ユーザー定義ルート）の優先度の確認（共通）

Azure portal ＞ルートテーブルで以下を確認
- 0.0.0.0/0 が ネットワーク仮想アプライアンス (NVA) に送られていないか
- Azure VNet 内の経路が正しいか

5.6. ④ 運用・変更起因：設定変更・期限切れ・環境変更による影響

本項目では、運用・変更起因：設定変更・期限切れ・環境変更による影響がある際の原因、過去事例、対処法について紹介いたします。

トラブル概要

・突然 VPN が切断される
・定期的に切れたり、環境変更後に不調が出る

過去の事例

AD サーバーへリモートデスクトップ接続を行いたいが、クライアント PC に設定していた接続が証明書エラーとなり接続できない。

調査した結果、VPN 接続に使用している証明書の有効期限が切れていたことが原因と判明しました。

ルート証明書およびクライアント証明書を再生成いただくことで解決。

原因

・対向ネットワーク間のMTU （Maximum Transmission Unit）のサイズ不足
・対向ルーター（S2S）／クライアント端末（P2S）側 の Keepalive 不足
・Azure 側または対向ネットワーク側 の運用中の設定変更（FW、ルート、Entra ID設定変更）
・AzureVPN Gateway に登録したルート証明書 または クライアント端末に配置した
クライアント証明書 の期限切れ・配置誤り

対処法

MTU 調整 （S2S/P2S）

オンプレミス側のルーター / FW の MTU を引き下げる
※Azure VPN GatewayのMTUは固定のため、オンプレミス側を合わせる

Keepalive 値の調整（S2S/P2S）

オンプレミス側のKeepalive 値を推奨値に変更

直前に行った変更の棚卸し （共通）

Azure portal> アクティビティログで変更や更新を確認

証明書期限の確認 （P2Sのみ）

5.4.にて記載