AWS ホワイトペーパー

ハイブリッド接続

ハイブリッド接続: AWS ホワイトペーパー

Table of Contents

ハイブリッド接続

出版日:2023 年 7 月 6 日 (ドキュメントの改訂)

多くの組織がオンプレミスのデータセンター、リモートサイト、クラウドを接続しなければならない状況にあります。こうした異なる環境は、ハイブリッドネットワークによって接続できます。このホワイトペーパーでは、AWS の構成要素と、どのハイブリッド接続モデルが自分に適しているかを判断する際に考慮すべき主な要件について説明します。ビジネス要件と技術要件に最適なソリューションを決定しやすくするために、論理的な選択プロセスをガイドする決定木を用意しています。

序章

現代の組織では、さまざまな IT リソースが使用されています。以前は、こうしたリソースをオンプレミスのデータセンターまたはコロケーション施設でホストするのが一般的でした。しかし、クラウドコンピューティングの導入が増えるにつれ、クラウドサービスプロバイダーが提供する IT リソースの配信や消費がネットワーク接続を介して行われるようになりました。既存の IT リソースの一部またはすべてをクラウドに移行することもできますが、どちらの場合も、オンプレミスとクラウドのリソースを接続するには共通のネットワークが必要です。オンプレミスとクラウドのリソースが共存している状態をハイブリッドクラウドと呼び、それらを接続する共通のネットワークをハイブリッドネットワークと呼びます。すべての IT リソースをクラウドに保持している場合でも、リモートサイトへのハイブリッド接続が必要な場合があります。

目的に応じて、いくつかの接続モデルを選択できます。選択肢があれば柔軟性が高まりますが、最適な選択肢を特定するには、ビジネス要件と技術要件を分析し、適切でない選択肢を除外しなければなりません。要件は、セキュリティ、導入時間、パフォーマンス、信頼性、通信モデル、スケーラビリティなどを考慮することでまとめられます。要件の入念な、収集、分析、検討が完了したら、ネットワーク設計者とクラウド設計者が、適用可能な AWS ハイブリッドネットワークの構成要素とソリューションを特定できます。最適なモデルを特定し選択するには、設計者が各モデルの利点と欠点を理解する必要があります。また、技術的な制限によって、適切なモデルを除外しなければならない場合もあるでしょう。

このホワイトペーパーでは、選択プロセスを簡略化できるよう、各重要な考慮事項を論理的な順序で解説しています。それぞれの考慮事項には、要件を収集するための質問があります。これにより、設計上の各決定が及ぼす影響と共に、考えられる解決策を特定できます。このホワイトペーパーでは、一部の考慮事項に使用する決定木を紹介しています。これに従うと、意思決定プロセスの推進、選択肢の除外、各決定の影響把握が可能になります。最後に、エンドツーエンドの接続モデルの選択と設計を適用したハイブリッドユースケースのシナリオについて説明します。この例を参考にすると、ど

うすればこのホワイトペーパーで説明されているプロセスを実例に基づいて実行できるかを確認できます。

このホワイトペーパーは、最適なハイブリッド接続モデルの選択と設計を行えるようになることを目的としています。このホワイトペーパーの構成を次に示します。

- ハイブリッド接続の構成要素 - AWS ハイブリッド接続に使用されるサービスの概要。
- 接続性の選択および設計上の考慮事項 - 各接続モデルの定義、各モデルが設計上の決定に与える影響、要件の特定に関する質問、解決策、決定木。
- お客様のユースケース - 考慮事項と決定木を実際に適用する方法の例。

Well-Architected の実現状況の確認

AWS Well-Architected フレームワークは、クラウド内でのシステム構築に伴う意思決定の長所と短所を理解するのに役立ちます。このフレームワークの 6 つの柱により、信頼性、安全性、効率、費用対効果、持続可能性の高いシステムを設計および運用するための、アーキテクチャのベストプラクティスを確認できます。AWS Management Consoleで無料で提供されている AWS Well-Architected Toolを使用すると、柱ごとに一連の質問に答えることで、これらのベストプラクティスに照らしてワークロードを評価できます。

クラウドアーキテクチャに関する専門的なガイダンスやベストプラクティス (リファレンスアーキテクチャのデプロイ、図、ホワイトペーパー) については、AWS アーキテクチャセンターを参照してください。

AWS ハイブリッド接続構成要素

ハイブリッドネットワーク接続アーキテクチャには、次の 3 つの構成要素があります。

- ハイブリッドネットワーク接続: AWS 接続サービスとオンプレミスのカスタマーゲートウェイデバイス間の接続タイプ。
- AWS ハイブリッド接続サービス: 顧客インフラストラクチャと AWS 間の接続とルーティングを提供する AWS サービス。
- オンプレミスのカスタマーゲートウェイデバイス: ハイブリッドネットワーク接続のオンプレミスエンドポイントとなる、既存の顧客ネットワーク内のデバイス。接続タイプが異なれば、これらのデバイスの技術的要件も異なります。これについては次のセクションで説明します。

ハイブリッドネットワーク接続

オンプレミス機器と AWS 間の接続にはいくつかの方法があります。このホワイトペーパーでは、これらのさまざまな方法を全体的なアーキテクチャに組み込む方法に焦点を当てていますが、さまざまなオプション (AWS Direct Connect、サイト間の仮想プライベートネットワーク、および Transit Gateway Connect) の概要も説明しています。

AWS Direct Connect

AWS Direct Connect は、プレミスから AWS への専用ネットワーク接続を確立するサービスです。詳細については、「AWS Direct Connect」を参照してください。

AWS Direct Connect 接続には専用接続とホスト接続の 2 つのタイプがあります。専用接続は AWS デバイスとオンプレミスデバイスを直接リンクするものですが、ホスト接続は接続の詳細を処理できる AWS パートナーがサポートします。詳細については、「AWS Direct Connect 接続」を参照してください。

Direct Connect 接続では、仮想インターフェイス (VIF) を使用してさまざまなトラフィックフローを分離します。複数の VIF は、VLAN (802.1q) タグで区切られた同じ Direct Connect リンクを使用できます。AWS ネットワークに接続する VIF には 3 つのタイプがあります。詳細については、「AWS Direct Connect 仮想インターフェイス」を参照してください。3 つの型を以下に示します。

- プライベート VIF: プライベート VIF は、デバイスと AWS 内部のリソースとの間のプライベート接続です。これらは、AWS 内部で、(単一の VPC をサポートする) 仮想プライベートゲートウェ

イ (VGW) で直接、または複数の VGW に接続する Direct Connect ゲートウェイ経由で終端します。

- パブリック VIF: パブリック VIF により、S3、DynamoDB、パブリック EC2 IP 範囲などのパブリック AWS リソースへの接続が可能になります。パブリック VIF はインターネットに直接アクセスできませんが、Amazon のパブリックリソースはアクセスできるので (他のお客様のパブリック EC2 インスタンスを含む)、お客様がセキュリティ計画を立てる際にはこの点を考慮する必要があります。
- トランジット VIF: トランジット VIF は、Direct Connect ゲートウェイを介した、デバイスと AWS Transit Gateway との間のプライベート接続です。トランジット VIF は、速度が 1 Gbps 未満のリンクでもサポートされるようになりました。詳細については、「発表のお知らせ」をご覧ください。

> **Note**
>
> ホスト型仮想インターフェイス (ホスト型 VIF) はプライベート VIF の一種で、VIF が AWS Direct Connect 接続を所有する AWS アカウントとは別の AWS アカウントに割り当てられます (AWS Direct Connect パートナーが含まれる場合もあります)。AWS では新しいパートナーがこのモデルを提供することはできなくなりました。詳細については、「ホスト仮想インターフェイスを作成する」を参照してください。

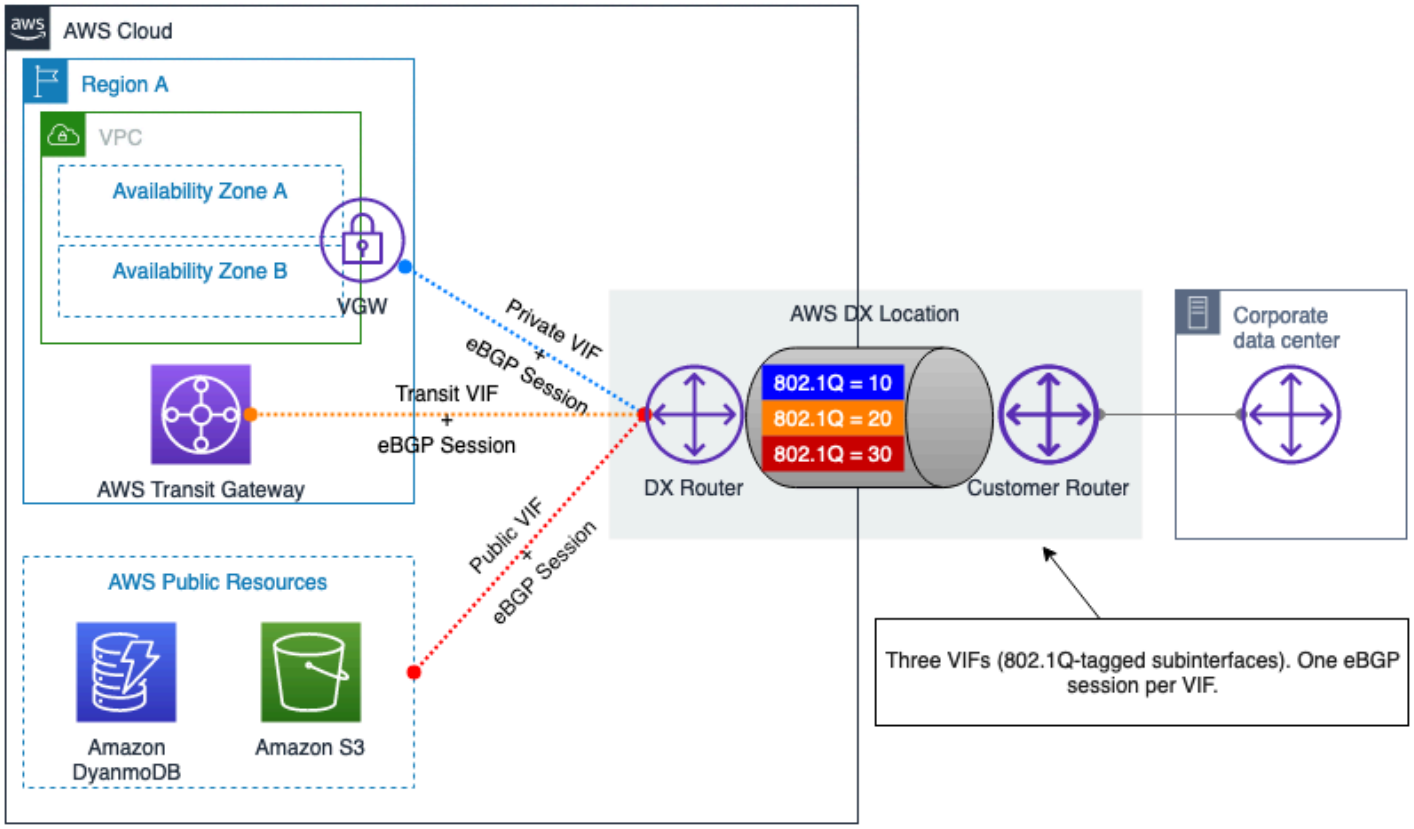

図 1 — AWS Direct Connect プライベート VIF とパブリック VIF

Site-to-Site 仮想プライベートネットワーク (VPN)

Site-to-Site VPN を使用すると、2 つのネットワークが安全に通信でき、インターネットなどの信頼できないトランスポート上でも使用できます。お客様は、次の 2 つのオプションを使用して、オンプレミスサイトと Amazon Virtual Private Cloud (Amazon VPC) 間の VPN 接続を確立できます。

- AWS マネージド Site-to-Site VPN (AWS S2S VPN): これは、IPSec を使用する完全マネージド型の高可用性 VPN サービスです。詳細については、「AWS Site-to-Site VPN Site-to-Site VPN の概要」を参照してください。オプションで、Site-to-Site VPN 接続のアクセラレーションを有効にできます。詳細については、「Site-to-Site VPN 接続の高速化」を参照してください。S2S VPN では、Direct Connect トランジット VIF を使用することでトラフィックがインターネットを経由することを回避できるため、コストが削減され、プライベート IP アドレスを使用できるようになります。詳細については、「AWS Direct Connect とプライベート IP VPN」を参照してください。
- ソフトウェア Site-to-Site VPN (顧客管理 VPN): この VPN 接続オプションでは、通常 EC2 インスタンスで VPN ソフトウェアを実行して、VPN ソリューション全体をプロビジョニングおよび管理する必要があります。詳細については、「ソフトウェア Site-to-Site VPN」を参照してください。

いずれの方法でも、VPN トンネルのオンプレミス側の終端をカスタマーゲートウェイデバイスでサポートする必要があります。このデバイスは、物理デバイスでもソフトウェアアプライアンスにすることもできます。AWS でテストされたネットワークデバイスの詳細については、「カスタマーゲートウェイデバイス」のリストを参照してください。

Transit Gateway Connect (TGW Connect)

Transit Gateway Connect は、AWS Transit Gateway とオンプレミスのゲートウェイデバイス間の GRE トンネルを使用します。ダイナミックルーティングを有効にするために、TGW Connect 上で BGP が使用されます。TGW Connect は暗号化されないことに注意してください。詳細については、「Transit Gateway Connect」を参照してください。

AWS ハイブリッド接続サービス

AWS ハイブリッド接続サービスは、拡張性と可用性に優れたネットワークコンポーネントを提供します。ハイブリッドネットワークソリューションの構築において重要な役割を果たします。このホワイトペーパーの執筆時点では、次の 3 つの主要なサービスエンドポイントがあります。

- AWS 仮想プライベートゲートウェイ (VGW) は、VPC レベルで IP ルーティングと転送を提供する、冗長性の高いリージョナルサービスで、VPC がお客様のゲートウェイデバイスと通信するためのゲートウェイとして機能します。VGW は AWS S2S VPN 接続と AWS Direct Connect プライベート VIF を終端できます。
- AWS Transit Gateway (TGW) は、可用性が高くスケーラブルなリージョナルサービスです。複数の VPC を相互に接続できるほか、単一の集中型ゲートウェイを使用して、Site-to-Site VPN や Direct Connect を介してオンプレミスネットワークを接続できます。概念的には、AWS Transit Gateway は可用性が高く冗長性のある仮想クラウドルーターとして機能します。AWS Transit Gateway は複数の Direct Connect 接続、VPN トンネル、または TGW Connect ピアでの等コストマルチパス (ECMP) ルーティングをサポートします。Transit Gateway は、同じリージョン内とクロスリージョンの両方で相互にピアリングできるため、接続されたリソースはピアリングリンクを介して通信できます。詳細については、「AWS Transit Gateway scenarios」を参照してください。
- AWS クラウド WAN は、支社、データセンター、Amazon VPC 間を接続するための中央ダッシュボードを提供し、数回クリックするだけでグローバルネットワークを構築できます。ネットワークポリシーを使用すると、ネットワーク管理とセキュリティタスクを 1 か所で自動化できます。詳細については、「AWS クラウド WAN documentation」を参照してください。
- Direct Connect Gateway (DXGW) は、ルーティング情報を接続全体に配信するグローバルに利用可能なサービスで、従来のネットワークの BGP ルートリフレクターと同様に動作します。データ

は DXGW を通過せず、ルーティング情報のみを処理します。DXGW は、どの AWS リージョンにも作成でき、他のすべての AWS リージョンからアクセスできます。Direct Connect VIF を DXGW に接続し、その DXGW を VGW (プライベート VIF を使用) または AWS Transit Gateway (トランジット VIF を使用) に関連付けることができます。詳細については、「Direct Connect ゲートウェイ」を参照してください。DXGW はグローバルに利用できるサービスなので、冗長性のために複数の DXGW を作成する必要はありません。ただし、完全に分離しておきたいプロダクションネットワークとテストネットワークなど、ルーティングドメインを分けるために複数の DXGW を使用することもできます。

ハイブリッド接続の種類および設計上の考慮事項

このホワイトペーパーの本セクションでは、オンプレミス環境を AWS に接続するハイブリッドネットワークを選択するうえで、考慮すべき事項について説明しており、論理的な思考プロセスに基づいて、最適なハイブリッド接続ソリューションを選択できるようにしています。設計に影響する考慮事項は、接続タイプに影響する事項と、接続設計に影響する事項に分類されます。接続タイプに関する考慮事項は、インターネットベースの VPN を使用するか、Direct Connect を使用するかの判断に役立ちます。接続設計上の考慮事項は、接続の設定方法を決定する際に役立ちます。

ここでは、接続タイプに影響を与える次の考慮事項について説明します: 導入時間、セキュリティ、SLA、パフォーマンス、コスト。こうした考慮事項とそれらが設計上の選択にどのように影響するかを確認すると、インターネットベースの接続と Direct Connect のどちらを使用した方が要件に対応できるかを判断できます。

ここでは、接続設計に影響する次の考慮事項について説明します: スケーラビリティ、通信モデル、信頼性、サードパーティの SD-WAN 統合。こうした考慮事項とそれらが設計上の選択にどのように影響するかを確認すると、要件を満たす最適な論理設計を判断できます。

次の構成を使用して、選択および設計上の各考慮事項を議論し、分析します。

- 定義 - 考慮すべき事項の簡単な定義を示しています。
- 重要な質問 - 考慮事項に関連する要件を収集するための質問をまとめています。
- 考慮すべき能力 - 考慮事項に関連する要件を満たすためのソリューションを示しています。
- 決定木 - 特定の考慮事項や、一連の考慮事項によっては、最適なハイブリッドネットワークソリューションの選択に役立つ決定木を提示しています。

ここでは、ハイブリッドネットワークの設計に影響する考慮事項について、ある項目の結果が、次に続く項目の入力情報となる順序で説明しています。図 2 に示すように、最初のステップで接続タイプを決定し、次のステップでそのタイプを設計選択の考慮事項に基づいて調整します。

図 2 は、2 つの考慮事項カテゴリ、個々の考慮事項、各項目の論理的な順序を示しており、各項目については、以降のサブセクションで説明します。ハイブリッドネットワーク設計の決定には、こうした項目の検討が不可欠です。対象の設計に、これらすべての考慮事項が必要でない場合は、要件に当てはまる事項の検討に注力しても構いません。

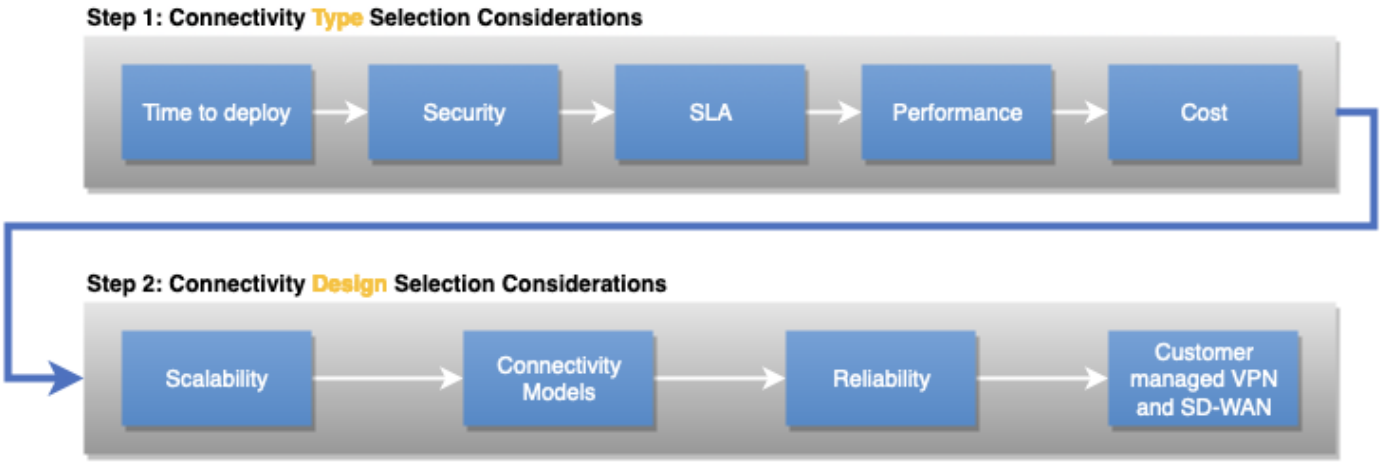

図 2 – 考慮事項のカテゴリ、個々の考慮事項、各項目間の論理的な順序を示す図

接続タイプの選択

このセクションでは、ワークロードに選択する接続タイプに影響を与える考慮事項について説明します。ここでは、導入時間、セキュリティ、SLA、パフォーマンス、コストの各項目に触れます。

考慮事項

- デプロイするまでの時間
- セキュリティ
- サービスレベルアグリーメント (SLA)
- パフォーマンス
- コスト

デプロイするまでの時間

定義

導入にかかる時間は、ワークロードに適した接続タイプを選択するうえで重要な要素となる場合があります。接続タイプやオンプレミス拠点によっては、数時間以内で接続を確立できますが、追加の回線を設ける必要がある場合は数週間から数か月かかることもあるでしょう。これに応じて、インターネットベースの接続、プライベート専用接続、AWS Direct Connect パートナーが管理サービスとして提供するプライベートホスト接続のどれを使用するかを判断することになります。

重要な質問

- 導入にはどの程度のタイムライン (数時間、数日、数週間、数か月など) が必要となりますか。
- この接続は、どのくらいの期間必要ですか。短期間のプロジェクト、あるいは、恒久的なインフラストラクチャととらえるべきでしょうか。

考慮すべき機能

数時間または数日以内での AWS 接続が要件の場合、一般的に、既存のネットワーク接続を使用する必要があります。この場合は通常、パブリックインターネット経由で AWS への VPN 接続を確立することになります。既存の AWS DX パートナーがプライベート AWS 接続を提供している場合は、新しいホスト接続を数時間以内にプロビジョニングできることもあります。

数日から数週間が要件の場合は、AWS Direct Connect パートナーと協力して、AWS へのプライベート接続を確立できます。AWS Direct Connectパートナーの協力を得ることで、AWS Direct Connect のロケーションと、データセンター、オフィス、コロケーション環境との間にネットワーク接続を確立できます。特定の AWS Direct Connect パートナーは、Direct Connect ホスト接続の提供が承認されています。多くの場合、ホスト接続は、専用接続よりも早くプロビジョニングできます。AWS Direct Connectパートナーは、AWS バックボーンに接続されている既存のインフラストラクチャを使用して各ホスト接続をプロビジョニングします。

数週間から数か月が要件の場合は、AWS との専用プライベート接続の確立について検討すると良いでしょう。サービスプロバイダーや AWS Direct Connect パートナーの協力を得ることで、AWS Direct Connect 専用接続を確立できます。サービスプロバイダーは通常、Direct Connect 専用接続を簡単に確立できるよう、お客様の敷地内にネットワーク機器を設置します。サービスプロバイダー、サイトの場所、その他の物理的要因によっては、Direct Connect 専用接続の環境導入に、数週間から数か月かかる場合があります。

AWS Direct Connect ロケーションと同じコロケーション施設にネットワーク機器を設置済みの場合は、コロケーションサイトでのクロスコネクトを介して AWS Direct Connect 専用接続を迅速に確立できます。AWS に接続をリクエストすると、Letter of Authorization and Connecting Facility Assignment (LOA-CFA) がダウンロードできるようになるか、詳細情報の提供を求める電子メールが届きます。LOA-CFA は AWS に接続するための認可で、ネットワークプロバイダーがクロスコネクトを代行注文するために必要です。

表 1 - 費用対効果の比較

	インターネットベースの接続	DX 専用接続 (DX ロケーション内の既存機器を使用)	DX 専用接続 (新規リソースを使用)	DX ホスト接続 (DX パートナーの既存ポートを使用)	DX ホスト接続 (新規リソースを使用)
プロビジョニング時間	数時間から数日	日間	数週間から数か月	数時間から数日	数日から数週間または数か月

> **Note**
>
> ここで説明しているプロビジョニング時間のガイドラインは、実際の考察に基づいていますが、例示にすぎません。サイトの場所、ダイレクトコネクトロケーションまでの近さ、既存のインフラストラクチャなどを考慮した場合、どの要因もプロビジョニング時間に影響を与えます。正確なプロビジョニング時間については、AWS Direct Connect の担当パートナーからアドバイスを得られます。

セキュリティ

定義

セキュリティ要件は、ハイブリッド接続タイプに影響を与えます。主な考慮事項を次に示します。

- 転送タイプ - インターネット接続またはプライベートネットワーク接続
- 暗号化の要件

重要な質問

- セキュリティの要件とポリシーでは、AWS への接続についてインターネット経由の暗号化接続の使用を許可していますか。それともプライベートネットワーク接続の使用を義務付けていますか。
- プライベートネットワーク接続を利用する場合、ネットワーク層での転送中に暗号化を行える必要がありますか。

テクニカルソリューション

セキュリティの要件とポリシーによっては、インターネットの使用を許可したり、AWS と企業ネットワーク間でプライベートネットワーク接続の使用を要求したりすることになるでしょう。こうした点は、ネットワーク転送中での暗号化を可能にする必要があるかや、アプリケーション層での暗号化を容認するかなどの判断にも影響を与えます。

インターネットを利用できる場合は、AWS Site-to-Site VPN を使用して、ネットワークと Amazon VPC または AWS Transit Gateway の間にインターネット経由の暗号化トンネルを確立できます。インターネットベースの接続を利用している場合は、SD-WAN ソリューションをインターネット経由で AWS に拡張することも可能です。このホワイトペーパーでは、後半の「カスタマー管理の VPN および SD-WAN」セクションで、SD-WAN に関する具体的な考慮事項について説明します。

AWS と企業ネットワークの間にプライベートネットワーク接続が必要な場合、AWS では AWS Direct Connect 専用接続またはホスト接続の使用をお勧めしています。プライベートネットワーク接続で、転送中の暗号化が必要な場合は、Direct Connect (パブリック VIF またはトランジット VIF のいずれか) で VPN を確立するか、10 Gbps または 100 Gbps の専用接続で MACsec を使用することを検討してください。

表 2 - Example Corp. Automotive の接続タイプ要件

	Site-to-Site VPN	Direct Connect
トランスポート	インターネット	プライベートネットワーク接続
転送中の暗号化	Yes	DX 経由の S2S VPN、トランジット VIF 経由の S2S VPN、もしくは 10 Gbps または 100 Gbps の専用接続を介した MACsec が必要

サービスレベルアグリーメント (SLA)

定義

企業は、多くの場合、利用するサービスごとに、サービスプロバイダーに SLA の遵守を要求します。さらに、それに基づいて、独自のサービスを構築し、自社の利用者に SLA を提示する場合もあ

ります。SLA には、サービスの提供および運用方法を規定するという重要な役割があり、可用性など、特定の測定可能な特性が記述されることも少なくありません。サービスを定めた SLA に違反したサービスプロバイダーは通常、契約で規定された金銭的な補償を提示します。また、SLA では、測定の種類、その要件、測定期間も定められます。規定の例は、「AWS Direct Connect SLA」の稼働時間目標の定義でご覧いただけます。

重要な質問

- ハイブリッド接続の SLA では、サービスクレジットも定める必要がありますか。
- ハイブリッドネットワーク全体で、稼働時間目標を遵守する必要がありますか。

考慮すべき機能

接続タイプ: インターネット接続を確立できるかどうかは、予測できない場合もあります。AWS では、さまざまな ISP との複数リンクに細心の注意を払っていますが、インターネットは、AWS や単一プロバイダーの管理対象ドメイン外で管理されています。そのため、管理対象のネットワークを離れたトラフィックについては、クラウドプロバイダーで制御できるルートエンジニアリングとトラフィックに限界があります。ただし、AWS Site-to-Site VPN SLA には、AWS Site-to-Site VPN エンドポイントの可用性目標が規定されています。

AWS Direct Connect では、サービスクレジットを定めた正式な SLA が提供されます。このクレジットは、SLA を満たしていない月次請求サイクルの間に利用できなかった接続に対してお客様が支払った AWS Direct Connect 総ポート時間料金に基づいて、パーセンテージを計算したものです。SLA が必要な場合は、このネットワーク接続をお勧めします。また、AWS Direct Connect では、稼働時間目標ごとに、AWS Direct Connect のロケーション数、接続数、その他の構成詳細といった最小構成要件が具体的に定められています。こうした要件を満たしていないと、定義済みのサービス SLA が遵守されなかった場合のサービスクレジットを得られないことになります。

ここで重要なのは、ハイブリッド接続のために選択したサービスの構成が SLA 要件を満たしていても、それ以外のネットワークで、同レベルの SLA が遵守されない場合があることです。AWS の責任範囲は、AWS Direct Connect ロケーションの AWS Direct Connect ポートまでです。AWS の責任範囲を離れ、組織のネットワークに入ったトラフィックは、AWS の管理対象外と見なされます。AWS とオンプレミスネットワークの間でサービスプロバイダーを使用する場合、この接続には、お客様とサービスプロバイダー間で定めた SLA が適用されます (該当する場合)。ハイブリッド接続の設計時には、ハイブリッドネットワーク全体の品質は、その中で最も品質の低いネットワークと同程度である点に留意してください。

AWS Direct Connect パートナーの協力を得れば、AWS Direct Connect 接続を確立できます。こうしたパートナーとは、AWS との間に設定された境界点までの製品提供に基づいて、サービスクレジットが定められた SLA を締結できることもあります。この選択肢については、APN パートナーと共に、直接的な評価と綿密な調査を行う必要があります。AWS では、検証済みデリバリーパートナーのリストを公開しています。

論理設計: 接続タイプの他にも、設計を進める中で考慮すべき構成要素があります。例えば、AWS Transit Gateway と AWS S2S VPN には独自の SLA があります。AWS Transit Gateway による規模拡大や、AWS S2S VPN によるセキュリティ確保を目指している場合にも、各サービスでサービスクレジットの対象となるには、各 SLA に準拠して、それらの両方を設計しなければなりません。

「AWS Direct Connect の回復性に関する推奨事項」と「Resiliency Toolkit」をご確認ください。

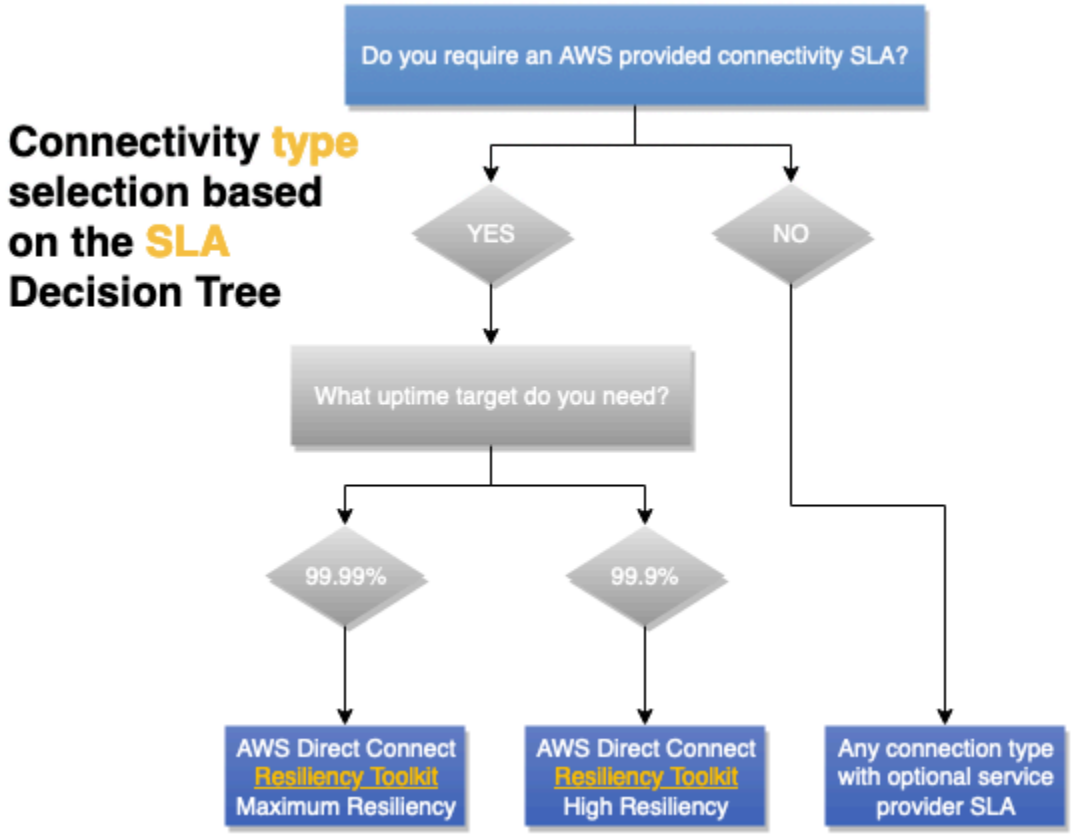

図 3 - SLA を考慮する際の決定木

パフォーマンス

定義

遅延、パケット損失、ジッター、帯域幅など、ネットワークパフォーマンスにはさまざまな要因が影響を与えます。それぞれの要素がいかに重要かは、アプリケーションの要件によって異なる場合があります。

重要な質問

アプリケーションの要件に基づいて、アプリケーションの動作とユーザーエクスペリエンスに影響が及ぶネットワークパフォーマンス要因を特定し、優先順位を付ける必要があります。

帯域幅

帯域幅は、接続時のデータ転送速度を意味し、通常はビット/秒 (bps) で測定されます。メガビット/秒 (Mbps) とギガビット/秒 (Gbps) が一般的な尺度であり、基数には、よく使用される 2 (2^10) ではなく、10 (1,000,000 ビット/秒 = 1 Mbps) が使用されます。

アプリケーションの帯域幅上のニーズを評価するときは、その要件が時間と共に変化しうる点に留意してください。クラウドへの最初のデプロイ、通常運用、新規ワークロード、フェイルオーバーなどの各シナリオには、異なる要件が設定される場合があります。

アプリケーション固有の帯域幅を考慮しなければならない場合もあります。例えば、広帯域接続で確定的なパフォーマンスを得られることが要件の場合もあれば、パフォーマンスと広帯域幅の両方が確定的であることが要件の場合もあるでしょう。アプリケーションがトラフィックフローごとの帯域幅制限に達していると、場合によっては、特別な構成を行い、複数のトラフィックフロー (ストリームまたはソケットとも呼ばれる) を並行して使用する必要があります。これにより、多くの接続帯域幅を使用できます。また、VPN を使用すると、トンネリングのオーバーヘッド、MTU の上限低下、ハードウェア帯域幅の制限によって、スループット上の制約が生じることもあります。

レイテンシー

レイテンシーは、パケットがネットワーク接続を介して送信元から宛先に移動するために必要な時間を意味します。通常はミリ秒 (ms) 単位で測定されますが、低レイテンシーが要件の場合は、マイクロ秒 (µs) で表されることもあります。光の速度の関係上、距離が長くなれば、レイテンシーも増大します。

アプリケーションのレイテンシー要件は、さまざまな形式で設定されることがあります。仮想デスクトップなど、非常にインタラクティブなアプリケーションの場合、ユーザーの入力に仮想デスクトップが反応するまでの時間がレイテンシー目標に設定されることがあります。一部の Voice over

IP (VoIP) アプリケーションにも同様の要件が見られる場合があります。考慮すべき 2 番目のタイプのワークロードは、トランザクションの頻度が高く、次の処理の前に、サーバーからの応答が必要なワークロードです。例えば、キーと値を格納するデータベースなどは、ネットワークレイテンシーの増大によって、かなりの影響を受ける可能性があります。

Jitter

ジッターとは、ネットワーク遅延の一貫性を示す値であり、一般的に、レイテンシーと同様、ミリ秒 (ms) 単位で測定されます。

アプリケーションのジッター要件は、通常、ビデオや音声配信などのリアルタイムストリーミングアプリケーションに設定されます。こうしたアプリケーションのデータフローには、少量のバッファによる低ジッターの補正が可能で、速度と遅延が一定であることが求められる傾向があります。

パケットロス

パケット損失とは、配信されなかったネットワークトラフィックのパーセンテージを測定した値です。どのようなネットワークでも、トラフィックの急増、ネットワーク機能の低下、ネットワーク機器の障害などにより、ある程度のパケット損失が発生することがあります。そのため、ある程度のパケット損失を許容する必要がありますが、どの程度までそれが可能かは、アプリケーションによって異なります。

トラフィックを TCP で転送するアプリケーションには、再送信によってパケット損失を修正する機能があります。しかし、IP 上で UDP または独自のプロトコルを使用するアプリケーションは、パケット損失を処理する独自の手段を実装する必要があり、そうした損失の影響を非常に受けやすい性質があります。Voice over IP アプリケーションでは、パケット損失が発生した通話部分を無音にすることがあり、再送信は試行されません。また、一部の VPN ソリューションでは、トラフィック伝送用のネットワークでパケット損失が生じた場合、独自のメカニズムで回復を行います。

考慮すべき機能

予測可能なレイテンシーとスループットが要件の場合は、AWS Direct Connect を選択肢として検討すると良いでしょう。これなら、確定的なパフォーマンスを得られ、スループット要件に基づいて、帯域幅を選択できます。AWS では、インターネットベースの接続以上に安定したネットワークエクスペリエンスが必要な場合、AWS Direct Connect の使用をお勧めしています。これにより、ジャンボフレームに対応したプライベート VIF とトランジット VIF を使用できるため、ネットワークを流れるパケットの数が減り、オーバーヘッド削減によってスループットも向上します。AWS Direct ConnectSiteLink は、AWS バックボーンを使用した拠点間接続を可能にし、オンデマンドで有効になります。Direct Connect の帯域幅を選択する際には、SiteLink に使用する帯域幅を考慮する必要があります。

AWS Direct Connect 経由で VPN を使用すると、暗号化を行えるようになりますが、MTU サイズが小さくなり、スループットが低下する可能性があります。AWS が管理するサイト間 (S2S) VPN 機能については、「AWS Site-to-Site VPN」のドキュメントを参照してください。接続中の暗号化を主な暗号化要件とするお客様に配慮して、Direct Connection ロケーションの多くは、MACsec に対応しています。MACsec の実装では、サイト間 VPN 接続のような MTU サイズ上のスループット低下は考慮する必要はありません。AWS Transit Gateway を導入すると、等コストマルチパスルーティング (ECMP) によって VPN 接続数が水平方向に増加するため、スループットが向上します。AWS のマネージド Site-to-Site VPN では、プライベート接続に Direct Connect トランジット VIF を使用できます。詳細については、「AWS Direct Connect とプライベート IP VPN」を参照してください。

もう 1 つの選択肢は、AWS が管理するサイト間 VPN をインターネット経由で使用することです。低コストで広く利用できるため、魅力的な選択肢になり得ます。ただし、インターネット上のパフォーマンスはベストエフォートであることに留意してください。インターネットでの環境変化、混雑、遅延状態の増加などは、予測できないこともあります。AWS では、AWS 高速 S2S VPN を使用したソリューションにより、インターネットパスの使用で生じる欠点の一部を軽減しています。高速 S2S VPN で AWS Global Accelerator を使用することにより、カスタマーゲートウェイデバイスに可能な限り近い場所から、最も早いタイミングで、AWS ネットワークにトラフィックを送り込むことができます。こうすることで、混雑のない AWS グローバルネットワークを使用してネットワークパスを最適化し、最良のパフォーマンスを実現しているエンドポイントにトラフィックをルーティングします。高速 VPN 接続を使用すると、パブリックインターネット経由のトラフィックルーティングで発生し得るネットワークの中断を回避できます。

コスト

定義

このクラウドでは、ハイブリッド接続のコストに、プロビジョニング済みリソースと使用量のコストが含まれます。プロビジョニング済みリソースのコストは、時間単位 (通常は 1 時間単位) で測定され、データ転送と処理の利用量は通常、ギガバイト (GB) 単位で測定されます。その他に、AWS ネットワークのポイントオブプレゼンス (POP) への接続コストがかかります。ネットワークが同じコロケーション施設内にある場合は、相互接続の同じくらい低料金になることもあるでしょう。ネットワークが別の場所にある場合は、サービスプロバイダーや APN Direct Connect パートナーの費用が発生します。

重要な質問

- 施設およびインターネットから AWS へは、毎月どれくらいの量のデータが送信されると予想していますか。

- AWS から施設およびインターネットへは、毎月どれくらいの量のデータが送信されると予想していますか。
- こうしたデータ量は、どれくらい頻繁に変化しますか。
- 障害シナリオでは、どのような変更点が生じますか。

考慮すべき機能

多くの帯域幅が必要なワークロードを AWS で稼働させる場合、AWS Direct Connect を使用すると、AWS に出入りするトラフィック上かかるネットワークコストを 2 つの方法で削減できます。1 つ目は、AWS との間でデータを直接転送し、インターネットサービスプロバイダーにかかる帯域幅のコストを削減することです。2 つ目は、専用接続を介して転送するすべてのデータが、インターネットのデータ転送速度ではなく、割引後の AWS Direct Connect データ転送速度で課金されることです。詳細については、「Direct Connect の料金」ページを参照してください。

AWS Direct Connect を導入すると、AWS Direct Connect SiteLink を使用した AWS バックボーン経由でサイトを相互接続できます。詳細については、SiteLink ローンチに関するブログを参照してください。この機能を利用すると、通常の Direct Connect データ転送コストのほか、SiteLink が有効になっている間の料金 (1 時間単位) が発生します。SiteLink は、オンデマンドで有効または無効にできるため、インターネットまたはプライベートネットワークの接続に関連する障害シナリオに適した選択肢と言えるでしょう。

オンプレミスと Direct Connect ロケーション間の接続にネットワークサービスプロバイダーを利用する場合、帯域幅のコミットメント変更が可能かどうかや、変更に必要な時間は、サービスプロバイダーとの契約に従って規定されます。

AWS バックボーンは、AWS ネットワークの任意のポイントオブプレゼンスから、中国を除く任意の AWS リージョン にトラフィックを配信する機能を備えています。この機能には、インターネットを介したリモート AWS リージョン リージョンへのアクセスよりも多くの技術的利点がありますが、コストが生じます。詳細については「EC2 データ転送」の料金ページを参照してください。トラフィックパスに AWS Transit Gateway がある場合、GB あたりのデータ処理コストが追加されますが、2 つの Transit Gateway 間でリージョン間ピアリングを使用している場合、Transit Gateway のデータ処理への課金は一度のみ行われます。

アプリケーション設計を最適化すると、AWS 内でデータ処理を維持でき、不要なデータ送信料金を最小限に抑えられます。AWS へのデータ入力は、課金されません。

> **Note**
>
> 接続ソリューション全体を検討する中で、AWS の接続に加え、エンドツーエンド接続にかかるコストも考慮しなければなりません。例えば、サービスプロバイダー、相互接続、ラック、DX ロケーション内の機器 (必要な場合) などのコストも発生します。

インターネット接続とプライベート接続のどちらを使用すべきか判断できない場合は、インターネットよりも AWS Direct Connect の方が低コストとなる損益分岐点を計算します。データ量の観点でいうと AWS Direct Connect の方が安価と判断され、永続的な接続を要件にしている場合は、AWS Direct Connect が、接続上の選択肢として最適です。

一時的な接続が要件であり、その他の要件をインターネット接続によって満たすことができれば、柔軟性のあるインターネット経由で AWS S2S VPN を使用する方が安価な場合があります。ただし、これにはオンプレミスネットワークからのインターネット接続を十分に行える必要がある点に注意してください。

AWS Direct Connect を備えた施設 (リストは Direct Connect Web サイトで入手可能) で運用を行っている場合、AWS への相互接続を確立できます。これにより、1、10、または 100 Gbps の専用接続を使用できます。AWS Direct Connect パートナーの協力を得ると、さまざまな帯域幅オプションや小規模なキャパシティを利用して、接続コストを最適化できる可能性があります。例えば、1 Gbps の専用接続ではなく、50 Mbps のホスト接続を最初に導入できます。

AWS Transit Gateway を導入すると、VPN 接続と Direct Connect 接続を多数の VPC と共有できます。AWS Transit Gateway への 1 時間あたりの接続数と、AWS Transit Gateway を通過するトラフィック量に応じて課金が発生しますが、管理が簡素化されると同時に、必要な VPN 接続と VIF の数が減少します。こうした運用オーバーヘッドの削減によるメリットとコスト削減によって、データ処理の追加コストを帳消しにできる可能性があります。選択肢として、必ずしも VPC へのトラフィックパスのすべてに AWS Transit Gateway を配置しないという設計も検討できます。こうした方法により、大量のデータを AWS に転送する必要があるユースケースで AWS Transit Gateway のデータ処理課金を回避できます。この設計の詳細については、「接続モデル」セクションを参照してください。もう 1 つの方法は、プライマリパスとしての AWS Direct Connect と、バックアップ/フェイルオーバーパスとしてのインターネット上の AWS S2S VPN を組み合わせることです。このソリューションは技術的に実現可能で、かなりのコスト効率を得られますが、技術的な欠点 (このホワイトペーパーの「信頼性」セクションで説明) があるため、管理がさらに難しくなる可能性があります。きわめて重要なワークロードまたは重要なワークロードの場合、AWS では、この方法を推奨していません。

最後にご紹介する方法は、カスタマーマネージドの VPN または SD-WAN を Amazon EC2 インスタンスにデプロイすることです。数十から数百のサイトがある場合、この方法を取ると、AWS S2S VPN の使用よりも大幅なコスト削減につながる可能性があります。ただし、仮想アプライアンスごとに、管理上のオーバーヘッド、ライセンスコスト、EC2 リソースコストが生じる点を考慮しなければなりません。

ディシジョンマトリックス

表 3 - Example Corp. Automotive の接続設計に関する入力情報

カテゴリ	カスタマーマネージド VPN または SD-WAN	AWS S2S VPN	AWS 高速 S2S VPN	AWS Direct Connect ホスト接続	AWS Direct Connect 専用接続
インターネット接続が必要	はい	Yes	Yes	No	No
プロビジョニング済みリソースのコスト	EC2 インスタンスとソフトウェアライセンス	AWS S2S VPN	AWS S2S VPN と AWS Global Accelerator	ポートコストの該当キャパシティスライス	専用ポートのコスト
データ転送コスト	インターネットの料金	インターネットまたは Direct Connect の料金	インターネットおよびデータ転送プレミアムの料金	Direct Connect の料金	Direct Connect の料金
トランジットゲートウェイ	任意	任意	必須	任意	任意
AWS データ処理コスト	該当なし	AWS Transit Gateway と併用する場合のみ	Yes	AWS Transit Gateway と併用する場合のみ	AWS Transit Gateway と併用する場合のみ

カテゴリ	カスタマーマネージド VPN または SD-WAN	AWS S2S VPN	AWS 高速 S2S VPN	AWS Direct Connect ホスト接続	AWS Direct Connect 専用接続
AWS Direct Connect を介した利用	はい	Yes	いいえ	該当なし	該当なし

接続設計の選択

ホワイトペーパーのこのセクションでは、接続設計の選択に影響する考慮事項について説明します。接続設計には、論理的な側面だけでなく、ハイブリッド接続の信頼性を設計して最適化する方法も含まれます。

スケーラビリティ、接続モデル、信頼性、顧客管理の VPN と SD-WAN などの考慮事項について説明します。

考慮事項

- スケーラビリティ
- 接続モデル
- 信頼性
- カスタマーマネージド VPN と SD-WAN

スケーラビリティ

定義

スケーラビリティとは、要件の変化に応じて接続ソリューションが時間と共に成長し、進化する能力を指します。

ソリューションを設計する際には、現在の規模と予測される成長を考慮する必要があります。この成長は、有機的な成長である場合もあれば、合併や買収のような急速な拡大に関連する場合もあります。

注: 対象となるソリューションアーキテクチャによっては、前述の要素をすべて考慮する必要がない場合もあります。ただし、一般的なハイブリッドネットワークソリューションのスケーラビリティ

要件を特定するための基礎要素としては役立ちます。このホワイトペーパーでは、ハイブリッド接続の選択と設計に焦点を当てています。VPC ネットワークアーキテクチャに関するハイブリッド接続の規模も考慮することをお勧めします。詳細については、「スケーラブルで安全なマルチ VPC AWS ネットワークインフラストラクチャの構築」ホワイトペーパーを参照してください。

重要な質問

- オンプレミスサイトへの接続を必要とする VPC の現在数および予想数はいくつですか。
- VPC は 1 AWS リージョン つのリージョンにデプロイされているのか、それとも複数のリージョンにデプロイされているのか?
- AWSに接続する必要があるオンプレミスサイトはいくつですか。
- サイトごとに AWSに接続する必要のあるカスタマーゲートウェイデバイス (通常はルーターまたはファイアウォール) はいくつありますか。
- Amazon VPC にアドバタイズされると予想されるルートの数と、側から受信されると予想されるルートの数はいくつですか? AWS
- AWS 帯域幅を徐々に増やす必要はありますか?

考慮すべき機能

スケールは、ハイブリッド接続設計の重要な要素です。その点について、以降のセクションでは、対象とする接続モデル設計の一部としてスケールを組み込んでいきます。

ハイブリッドネットワーク接続設計のスケールの複雑さを最小限に抑えるために推奨されるベストプラクティスを以下に示します。

- ルート集約を使用して、アドバタイズされるルートと受信されるルートの数を減らす必要があります。 AWSそのため、IP アドレッシングスキームは、ルート集約を最大限に活用できるように設計する必要があります。トラフィックエンジニアリングは全体的に重要な考慮事項です。トラフィックエンジニアリングの詳細については、「Reliability」セクションの「Traffic engineering」サブセクションを参照してください。
- DXGW と VGW を組み合わせて使用するか、単一の BGP セッションで複数の VPC AWS Transit Gatewayに接続できる場合は、BGP ピアリングセッションの数を最小限に抑えます。
- 複数のオンプレミスサイトを同時に接続する必要がある場合は、クラウド WAN を検討してください AWS リージョン 。

接続モデル

定義

接続モデルとは、オンプレミスネットワークと AWS内のクラウドリソース間の通信パターンを指します。Amazon VPC 内のクラウドリソースは、 AWS リージョン 複数のリージョンにまたがる単一または複数の VPC 内にデプロイできます。また、Amazon S3 や DynamoDB など AWS リージョン、 AWS 単一または複数のパブリックエンドポイントを持つサービスもデプロイできます。

重要な質問

- リージョン内およびリージョン間の VPC 間通信の要件はありますか。
- AWS オンプレミスからパブリックエンドポイントに直接アクセスする必要はありますか?
- オンプレミスから VPC AWS エンドポイントを使用してサービスにアクセスする必要はありますか?

考慮すべき機能

最も一般的な接続モデルのシナリオの一部を以下に示します。各接続モデルには、要件、属性、考慮事項が含まれます。

注意: 前述のとおり、このホワイトペーパーではオンプレミスネットワークと AWS間のハイブリッド接続に焦点を当てています。VPC を相互接続する設計の詳細については、「スケーラブルで安全なマルチ VPC AWS ネットワークインフラストラクチャの構築」ホワイトペーパーを参照してください。

モデル

- AWS 高速Site-to-Site VPN —、シングル AWS Transit GatewayAWS リージョン
- AWS DX — DXGW と VGW、シングルリージョン
- AWS DX — VGW、マルチリージョン、パブリックピアリングを備えた DXGW AWS
- AWS DX — DXGW、マルチリージョン、パブリックピアリング AWS Transit GatewayAWS
- AWS DX — DXGW あり AWS Transit Gateway、マルチリージョン (3 つ以上)

AWS 高速Site-to-Site VPN —、シングル AWS Transit GatewayAWS リージョン

このモデルは以下で構成されます。

- シングル。 AWS リージョン
- AWS とのマネージドSite-to-Site VPN 接続。 AWS Transit Gateway
- 高速 VPN が有効。

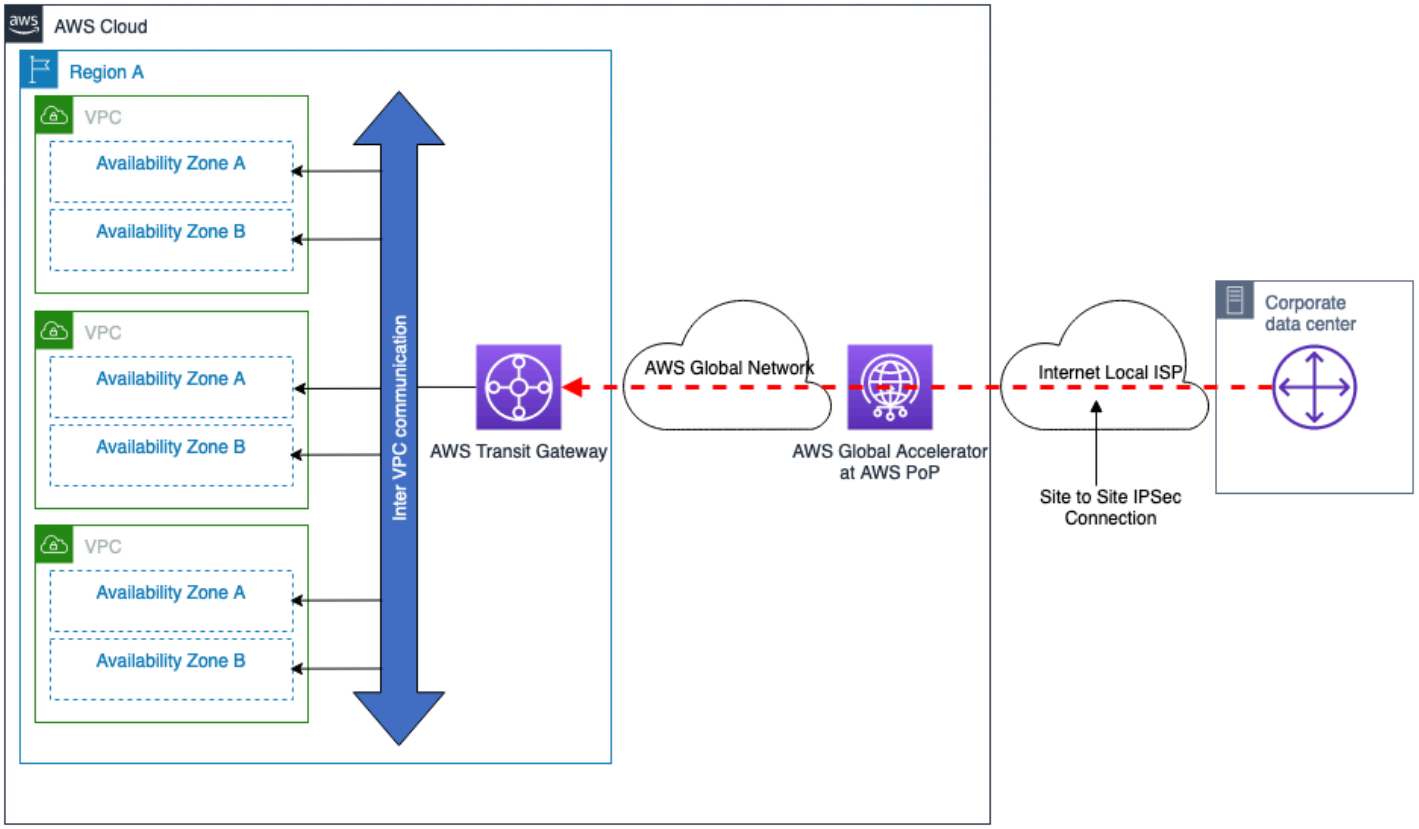

図 4 — AWS マネージド VPN — AWS Transit Gateway、シングル AWS リージョン

接続モデル属性:

- AWS 高速 Site-to-Site VPN 接続を使用して、パブリックインターネット上で最適化された VPN 接続を確立する機能を提供します。
- ECMP を使用して複数の VPN トンネルを構成することで、VPN 接続帯域幅の拡大を実現する機能を提供します。
- 複数のリモートサイトからの接続に使用できます。
- 動的ルーティング (BGP) による自動フェイルオーバーを提供します。
- VPC AWS Transit Gateway に接続すると、接続されているすべての VPC が同じ VPN 接続を使用できます。VPC 間で必要な通信モデルを制御することもできます。詳細については、「Transit Gateway の動作」を参照してください。

- サードパーティのセキュリティと SD-WAN 仮想アプライアンスをと統合するための柔軟な設計オプションを提供します。 AWS Transit Gateway「VPC 間のトラフィックおよびオンプレミスから VPC へのトラフィックのネットワークセキュリティの一元化」を参照してください。

スケールの考慮事項:

- 複数の IPSec トンネルと ECMP を設定した場合、最大 50 Gbps の帯域幅 (各トラフィックフローは VPN トンネルごとの最大帯域幅に制限されます)。
- 1 台あたり数千の VPC を接続できます。 AWS Transit Gateway
- ルート数など、その他のスケール制限については、「Site-to-Site VPN のクォータ」を参照してください。

その他の考慮事項:

- AWS Transit Gateway オンプレミスデータセンターと間のデータ転送にかかる追加の処理コスト。 AWS
- リモート VPC のセキュリティグループは参照できません。ただし、VPC AWS Transit Gateway ピアリングではサポートされています。

AWS DX — DXGW と VGW、シングルリージョン

このモデルは以下で構成されます。

- シングル。 AWS リージョン
- 独立した DX AWS Direct Connect ロケーションへのデュアル接続。
- AWS DXGW は VGW を使用して VPC に直接接続されます。
- VPC AWS Transit Gateway 間通信でのオプションの使用。

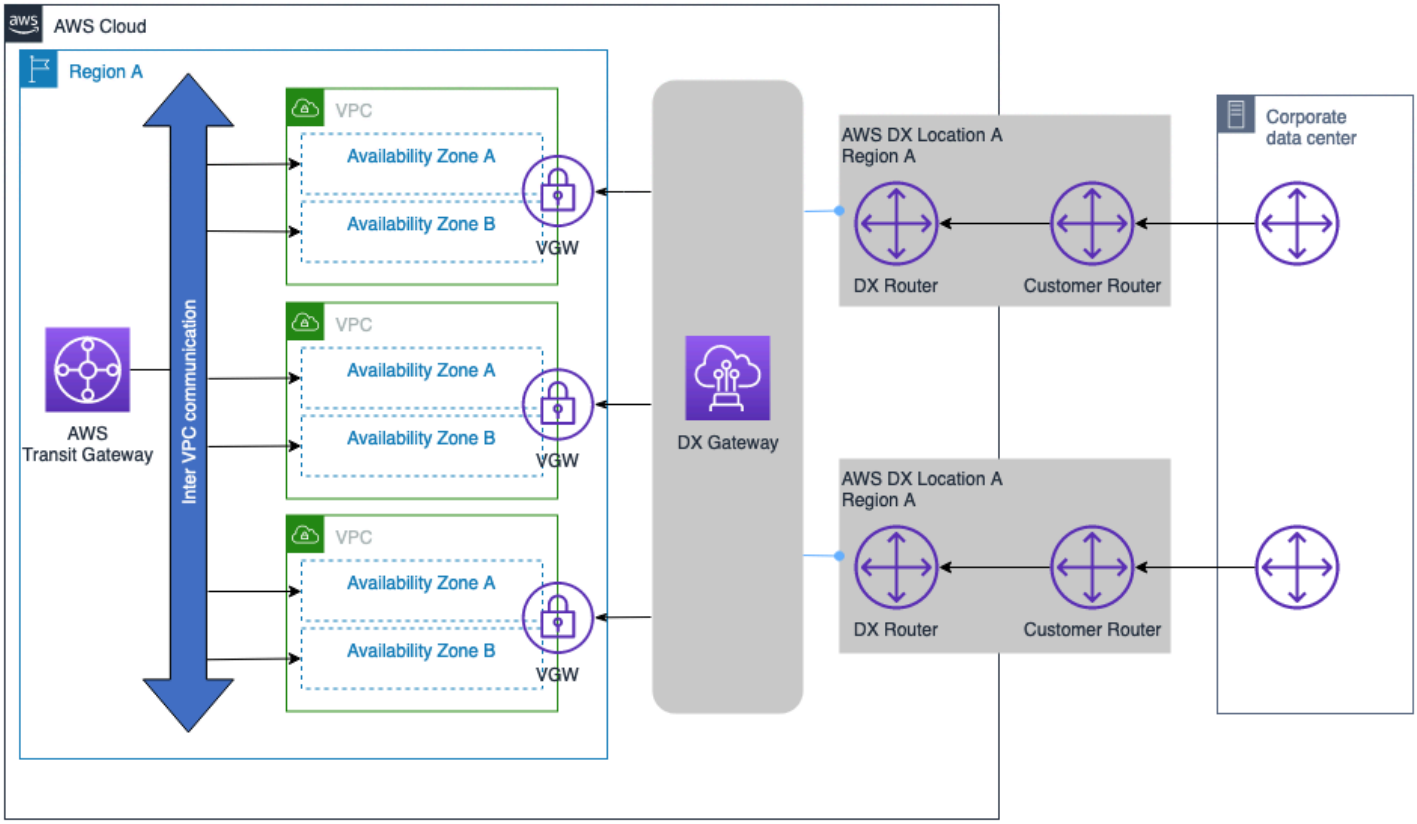

図 5 — AWS DX — DXGW と VGW、シングル AWS リージョン

接続モデル属性:

- 将来的には、他のリージョンの VPC および DX 接続に接続できる機能を提供します。
- 動的ルーティング (BGP) による自動フェイルオーバーを提供します。
- AWS Transit Gateway を使用すると、VPC 間の必要な通信モデルを制御できます。詳細については、「Transit Gateway の動作」を参照してください。

スケールの考慮事項:

サポートされるプレフィックスの数、DX 接続タイプ (専用、ホスト) ごとの VIF の数など、その他のスケール制限の詳細については、「AWS Direct Connect のクォータ」を参照してください。いくつかの重要な考慮事項:

- プライベート VIF の BGP セッションは、IPv4 と IPv6 のそれぞれについて最大 100 のルートをアドバタイズできます。

- 1 つの BGP セッションで DXGW あたり最大 20 の VPC を接続できます。20 以上の VPC が必要な場合は、DXGW を追加して大規模な接続を容易にするか、Transit Gateway 統合の使用を検討してください。
- AWS Direct Connect必要に応じてさらに追加できます。

その他の考慮事項:

- AWS Transit Gateway AWS オンプレミスネットワークとオンプレミスネットワーク間のデータ転送に関連する処理コストは発生しません。
- リモート VPC のセキュリティグループは参照できません AWS Transit Gateway (VPC ピアリングが必要)。
- VPC AWS Transit Gateway 間の通信を円滑にする代わりに VPC ピアリングを使用することもできますが、これにより、大量の VPC point-to-point ピアリングを大規模に構築および管理するための運用が複雑になります。
- VPC 間通信が不要な場合は、この接続モデルでは VPC AWS Transit Gateway ピアリングも必要ありません。

AWS DX — VGW、マルチリージョン、パブリックピアリングを備えた DXGW AWS

このモデルは以下で構成されます。

- への二重接続を備えた複数のオンプレミスデータセンター。 AWS
- 独立した DX AWS Direct Connect ロケーションへのデュアル接続。
- AWS DXGW は VGW を使用して 10 台以上の VPC に直接接続され、VGW を使用する最大 20 台の VPC に直接接続されます。
- VPC AWS Transit Gateway 間およびリージョン間通信でのオプションの使用方法。

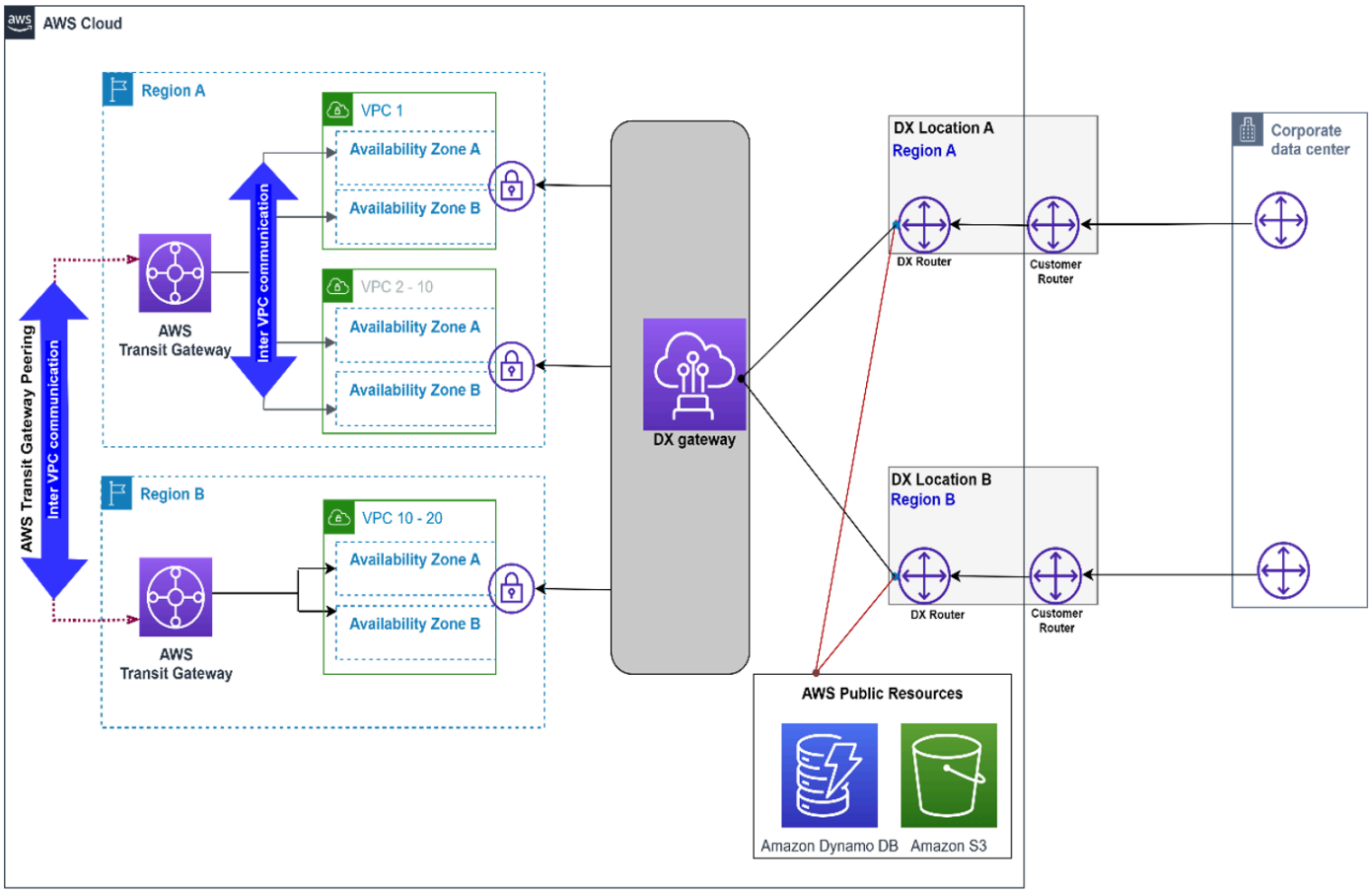

図 6 — AWS DX — VGW、マルチリージョン、パブリック VIF を使用した DXGW

接続モデル属性:

- AWS DXGW は VGW を使用する 10 台以上の VPC、VGW を使用する最大 20 台の VPC に直接接続されています。
- AWS DX パブリック VIF は、 AWS DX 接続を介して Amazon S3 AWS などのパブリックサービスに直接アクセスするために使用されます。
- 将来的には、他のリージョンの VPC および DX 接続に接続できる機能を提供します。
- VPC間およびリージョン間のVPC 通信は、Transit Gateway ピアリングによって促進されます。AWS Transit Gateway

スケールの考慮事項:

サポートされるプレフィックスの数、DX 接続タイプ (専用、ホスト) ごとの VIF の数など、その他のスケール制限の詳細については、「AWS Direct Connect のクォータ」を参照してください。いくつかの重要な考慮事項:

- プライベート VIF の BGP セッションは、IPv4 と IPv6 のそれぞれについて最大 100 のルートをアドバタイズできます。
- 各プライベート VIF の 1 つの BGP セッションを介して DXGW ごとに最大 20 の VPC を接続でき、DXGW ごとに最大 30 のプライベート VIF を接続できます。
- 必要に応じて追加できます。 AWS Direct Connect

その他の考慮事項:

- AWS Transit Gateway AWS オンプレミスネットワークとオンプレミスネットワーク間のデータ転送に関連する処理コストは発生しません。
- リモート VPC のセキュリティグループは参照できません AWS Transit Gateway (VPC ピアリングが必要)。
- VPC AWS Transit Gateway 間の通信を円滑にする代わりに VPC ピアリングを使用することもできますが、これにより、大量の VPC point-to-point ピアリングを大規模に構築および管理するための運用が複雑になります。
- VPC 間通信が不要な場合は、この接続モデルでは VPC AWS Transit Gateway ピアリングも必要ありません。

AWS DX — DXGW、マルチリージョン、パブリックピアリング AWS Transit GatewayAWS

このモデルは以下で構成されます。

- 複数。 AWS リージョン
- 独立した DX AWS Direct Connect ロケーションへのデュアル接続。
- への二重接続を備えた単一のオンプレミスデータセンター。 AWS
- AWS DXGW と。 AWS Transit Gateway
- リージョンごとの大規模な VPC。

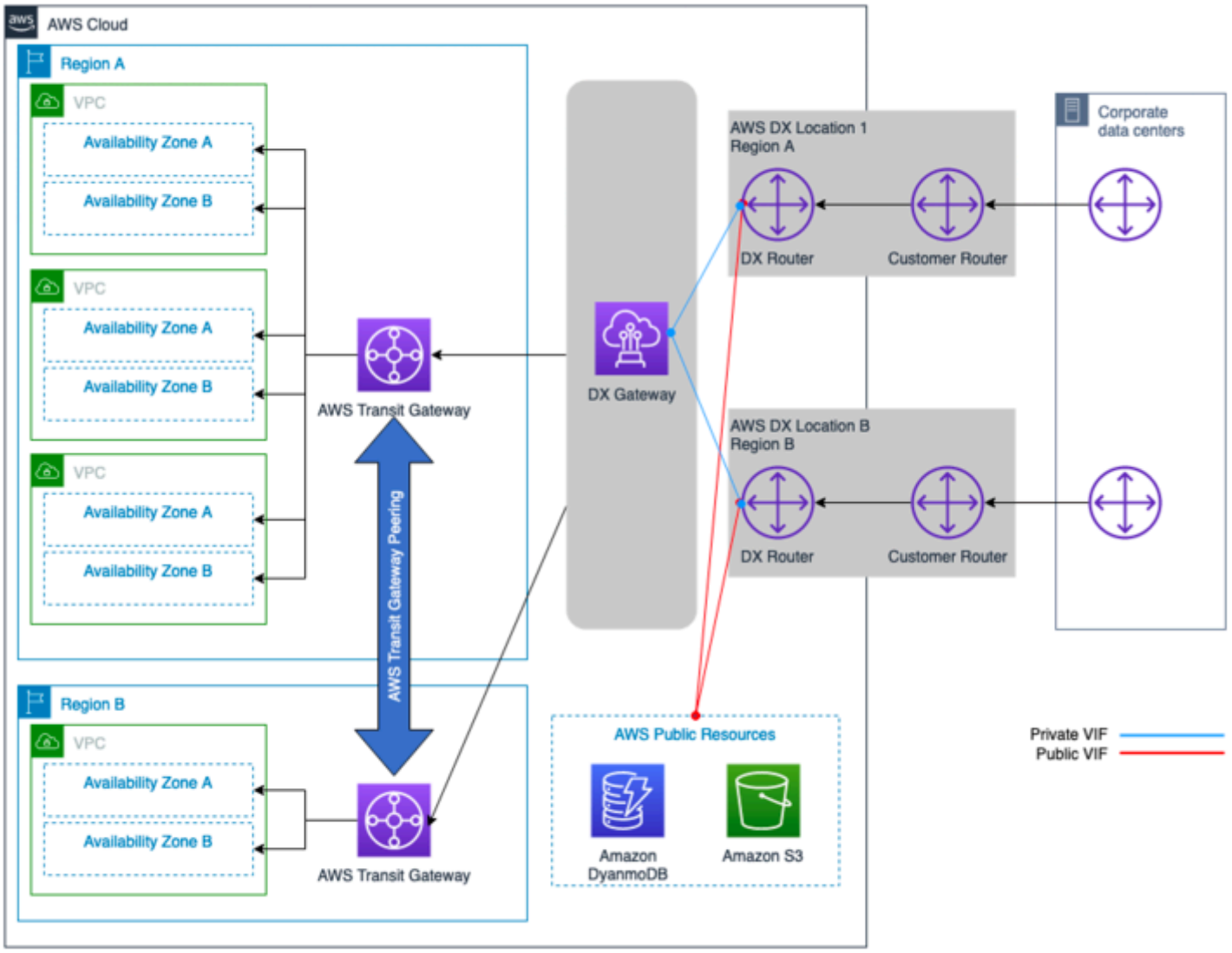

図 7 — AWS DX — DXGW あり、マルチリージョン、パブリック VIF AWS Transit Gateway AWS

接続モデル属性:

- AWS DX パブリック VIF は、DX 接続を介して S3 AWS などのパブリックリソースに直接アクセスするために使用されます。 AWS
- 将来的には、他のリージョンの VPC や DX 接続に接続できる機能を提供します。
- VPC AWS Transit Gateway に接続すると、VPC 間の完全または部分的なメッシュ接続を実現できます。
- VPC 間およびリージョン間 VPC 通信は、ピアリングによって促進されます。 AWS Transit Gateway

- サードパーティのセキュリティと SDWAN 仮想アプライアンスをと統合するための柔軟な設計オプションを提供します。 AWS Transit Gateway「VPC 間のトラフィックおよびオンプレミスから VPC へのトラフィックのネットワークセキュリティの一元化」を参照してください。

スケールの考慮事項:

- 送受信ルートの数は、Transit VIF 上でサポートされるルートの最大数に制限されます (インバウンドとアウトバウンドの数は異なります)。 AWS Transit Gateway スケールの制限とサポートされるルートと VIF の数について詳しくは、「AWS Direct Connect のクォータ」を参照してください。
- 1 つの BGP セッションで、1 つの AWS Transit Gateway VPC を数千までスケールアップできます。
- DX ごとに 1 つのトランジット VIF。 AWS
- AWS DX 接続は必要に応じて追加できます。

その他の考慮事項:

- AWS Transit Gateway AWS オンプレミスサイト間のデータ転送には追加の処理コストが発生します。
- リモート VPC のセキュリティグループは参照できません AWS Transit Gateway (VPC ピアリングが必要)。
- VPC AWS Transit Gateway 間の通信を円滑にする代わりに VPC ピアリングを使用することもできますが、これにより、大量の VPC point-to-point ピアリングを大規模に構築および管理するための運用が複雑になります。
- 3 AWS Transit Gatewayつ以上必要な場合は、DXGW を追加できます。次の接続モードを参照してください。

AWS DX — DXGW あり AWS Transit Gateway、マルチリージョン (3 つ以上)

このモデルは以下で構成されます。

- 複数 AWS リージョン (3 つ以上)。
- デュアルオンプレミスデータセンター。
- リージョンごとに独立した DX AWS Direct Connect ロケーションにまたがるデュアル接続。
- AWS DXGW と。 AWS Transit Gateway
- リージョンごとの大規模な VPC。

- s 間のピアリングのフルメッシュ。 AWS Transit Gateway

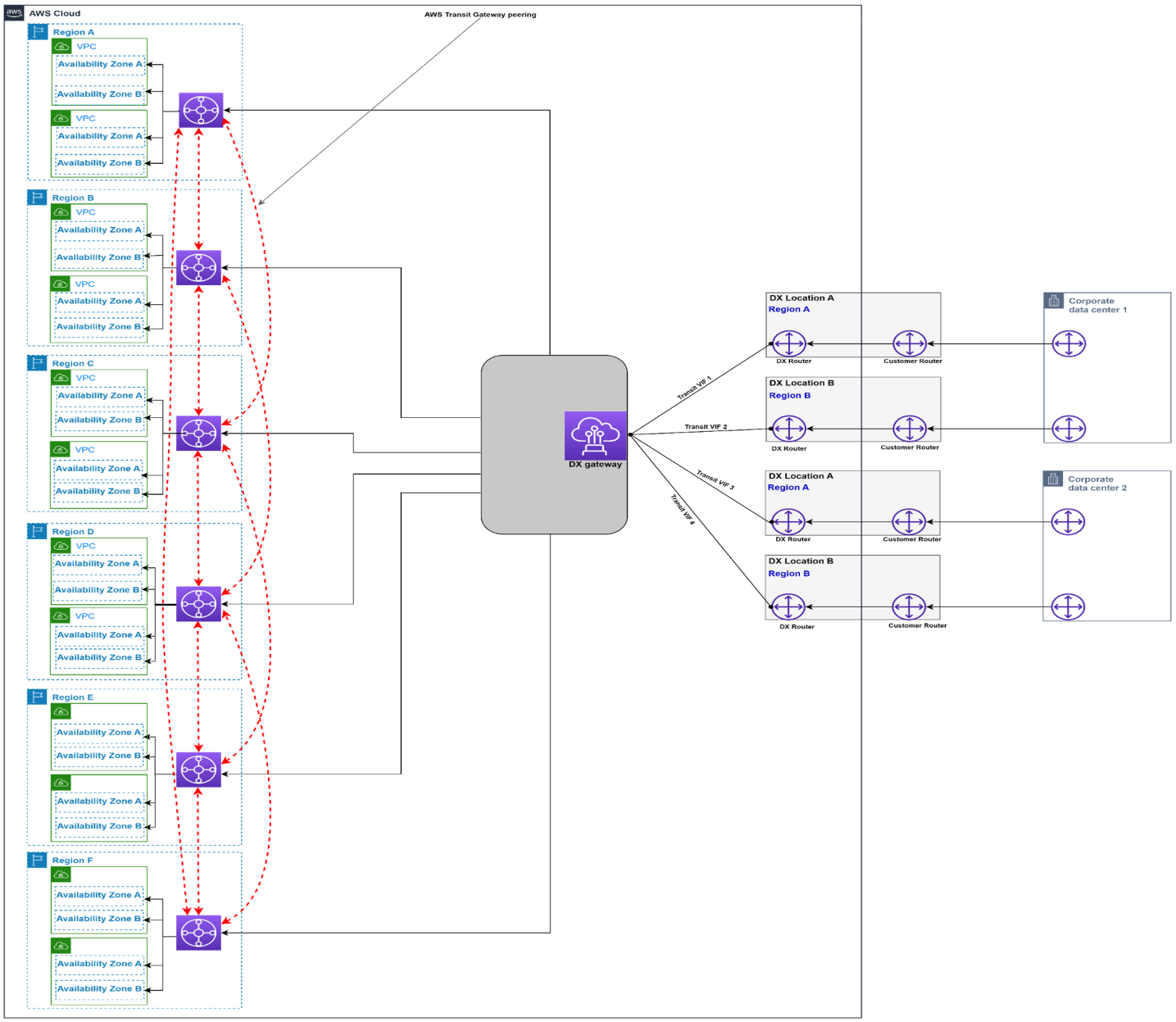

図 8 — AWS DX — DXGW あり AWS Transit Gateway、マルチリージョン (3 つ以上)

接続モデル属性:

- 運用上のオーバーヘッドが最も低い。
- AWS DX パブリック VIF は、DX 接続を介して S3 AWS などのパブリックリソースに直接アクセスするために使用されます。 AWS

- 将来的には、他のリージョンの VPC および DX 接続に接続できる機能を提供します。
- VPC AWS Transit Gateway に接続すると、VPC 間の完全または部分的なメッシュ接続を実現できます。
- リージョン間の VPC 通信は、ピアリングによって促進されます。 AWS Transit Gateway
- サードパーティのセキュリティと SDWAN 仮想アプライアンスをと統合するための柔軟な設計オプションを提供します。 AWS Transit Gateway「VPC 間のトラフィックおよびオンプレミスから VPC へのトラフィックのネットワークセキュリティの一元化」を参照してください。

スケールの考慮事項:

- 送受信ルートの数は、Transit VIF 上でサポートされるルートの最大数に制限されます (インバウンドとアウトバウンドの数は異なります)。 AWS Transit Gateway スケールの制限について詳しくは、「AWS Direct Connect のクォータ」を参照してください。ルート数を減らす必要がある場合は、ルート集約を検討してください。
- DXGW ごとに AWS Transit Gateway 1 つの BGP セッションで数千の VPC までスケールアップできます (プロビジョニングされた DX 接続によって提供されるパフォーマンスが十分であると仮定します)。 AWS
- DXGW ごとに 6 AWS Transit Gatewayつまで接続できます。
- を使用して 3 つ以上のリージョンを接続する必要がある場合は AWS Transit Gateway、追加の DXGW が必要です。
- DX ごとに 1 つのトランジット VIF。 AWS
- AWS DX 接続は必要に応じて追加できます。

その他の考慮事項:

- オンプレミスサイトと間のデータ転送には、 AWS Transit Gateway 追加の処理コストが発生します。 AWS
- リモート VPC のセキュリティグループは参照できません AWS Transit Gateway (VPC ピアリングが必要)。
- VPC AWS Transit Gateway 間の通信を円滑にする代わりに VPC ピアリングを使用することもできますが、これにより、大量の VPC point-to-point ピアリングを大規模に構築および管理するための運用が複雑になります。

以下の決定木では、スケーラビリティと通信モデルに関する考慮事項について説明します。

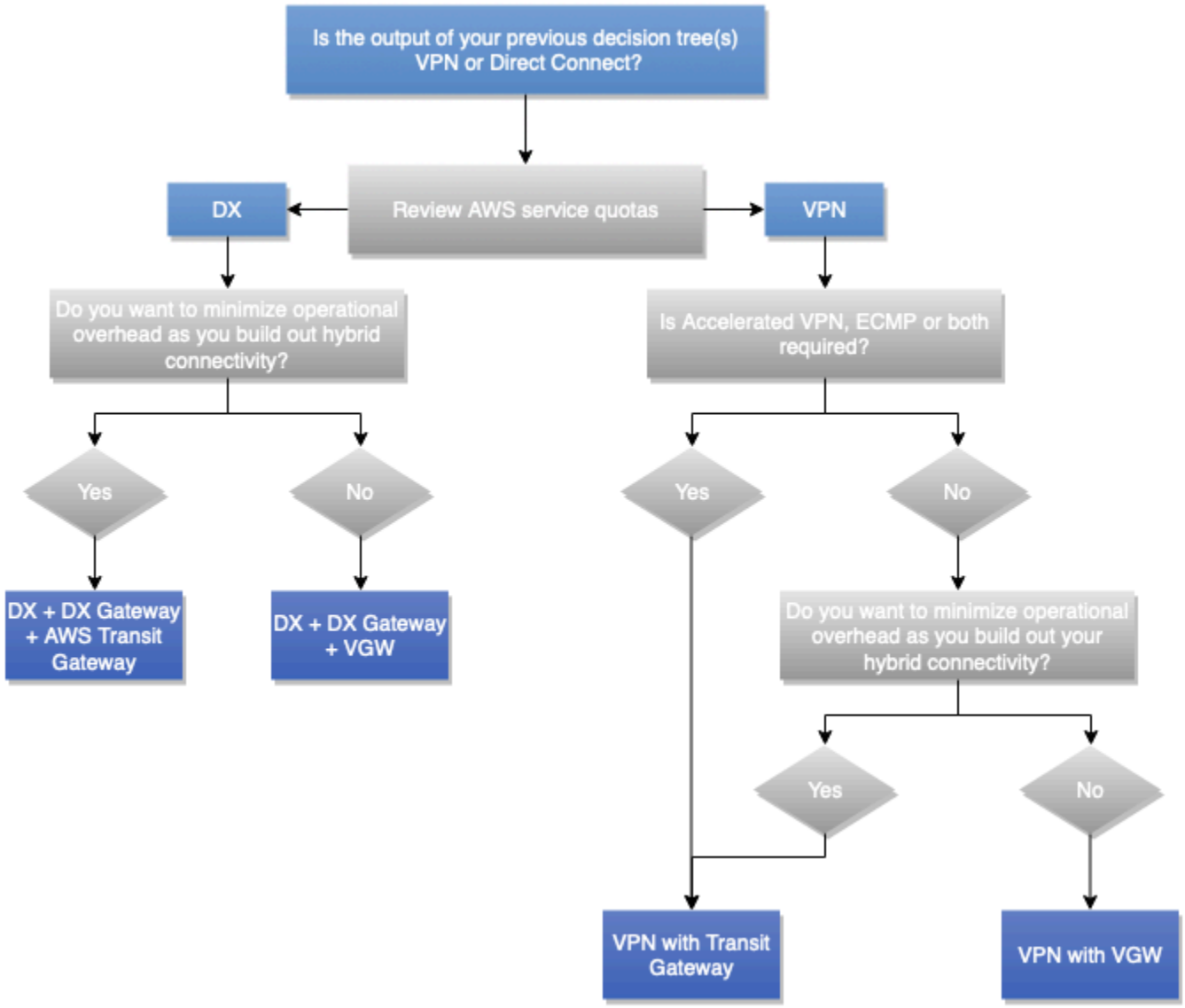

図 9 - スケーラビリティと通信モデルの決定木

> **Note**
>
> 選択した接続タイプが VPN の場合、通常はパフォーマンスを考慮して、VPN ターミネーションポイントが AWS VGW 接続か S2S VPN 接続かを判断する必要があります。 AWS Transit Gateway AWS まだ決まっていない場合は、VPC 間で必要な通信モデルと、VPN 接続に接続する必要のある VPC の数を検討して、判断に役立ててください。

信頼性

定義

信頼性とは、サービスまたはシステムが必要に応じて期待どおりの機能を実行する能力を指します。システムの信頼性は、特定の期間における運用品質のレベルによって測定できます。これを回復性と比較してください。回復性とは、インフラストラクチャやサービスの中断から動的かつ確実に回復するシステムの能力を指します。

可用性と耐障害性を利用して信頼性を測定する方法の詳細については、 AWS Well-Architected Frameworkの信頼性の柱を参照してください。

重要な質問

可用性

可用性は、ワークロードが使用可能な時間の割合です。一般的な目標としては、99% (年間に許容されるダウンタイムの日数 3.65 日)、99.9% (8.77 時間)、99.99% (52.6 分) があり、そのうち 9 の数字を省略しています (「ツーナイン」は 99%、「スリーナイン」は 99.9% など)。 AWS とオンプレミスのデータセンター間のネットワークソリューションの可用性は、ソリューション全体またはアプリケーションの可用性と異なる場合があります。

ネットワークソリューションの可用性に関する重要な質問には以下があります。

- AWS オンプレミスのリソースと通信できなくても、リソースは稼働し続けることができますか? その逆も可能ですか。
- 計画的なメンテナンスのための予定されたダウンタイムは可用性指標に含めるべきですか、それとも除外すべきですか。
- アプリケーション全体の状態とは別に、ネットワーク層の可用性を測定する方法を教えてください。

Well-Architected フレームワーク信頼性の柱の「可用性」セクションには、計算の可用性に関する提案と公式が掲載されています。

回復性

回復性は、インフラストラクチャまたはサービスの中断から復旧し、需要に合わせて動的にコンピューティングリソースを取得し、設定ミスや一時的なネットワーク問題のような障害を軽減する

ワークロードの能力です。冗長ネットワークコンポーネント (リンク、ネットワークデバイスなど) がそれ自体では期待どおりの機能を提供するのに十分な可用性を備えていない場合、障害に対する回復性は低くなります。その結果、ユーザーエクスペリエンスが低下します。

ネットワークソリューションの回復性に関する重要な質問には以下があります。

- 同時に発生する個別の障害はいくつまで許容すべきですか。
- 接続ソリューションと社内ネットワークの両方で単一障害点を減らすにはどうすればよいでしょうか。
- 分散型サービス拒否 (DDoS) イベントに対する脆弱性はどのようなものですか。

テクニカルソリューション

まず、すべてのハイブリッドネットワーク接続ソリューションが高レベルの信頼性を必要とするわけではなく、信頼性のレベルが上がるとそれに応じてコストも増加することに注意することが重要です。シナリオによっては、ダウンタイムがビジネスに与える影響が大きいため、プライマリサイトには信頼性の高い (冗長で耐障害性のある) 接続が必要になることがあります。一方、地域のサイトでは、障害発生時のビジネスへの影響が少ないため、同じレベルの信頼性を必要としない場合があります。AWS Direct ConnectAWS 設計によって高い耐障害性を確保するためのベストプラクティスを説明しているので、レジリエンシーに関する推奨事項を参照することをお勧めします。 AWS Direct Connect

回復性の観点から信頼性の高いハイブリッドネットワーク接続ソリューションを実現するには、設計時に次の点を考慮する必要があります。

- 冗長性:ハイブリッドネットワークの接続経路における単一障害点を排除することを目指します。これには、ネットワーク接続、エッジネットワークデバイス、アベイラビリティーゾーン、DX ロケーション間の冗長性、デバイスの電源 AWS リージョン、ファイバーパス、オペレーティングシステムなどが含まれますが、これらに限定されません。このホワイトペーパーの目的と範囲において、冗長性はネットワーク接続、エッジデバイス (カスタマーゲートウェイデバイスなど)、 AWS DX ロケーション、および AWS リージョン (マルチリージョンアーキテクチャの場合) に重点を置いています。
- 信頼性の高いフェイルオーバーコンポーネント: シナリオによっては、システムが機能していても、必要なレベルでその機能を実行していない場合があります。このような状況は、単一の障害イベントで、計画された冗長コンポーネントが非冗長的に動作していたことが判明したときによく見られます。つまり、使用状況により、ネットワーク負荷が他に行き場がなく、その結果ソリューション全体の容量が不十分になります。

- フェイルオーバー時間: フェイルオーバー時間は、セカンダリコンポーネントがプライマリコンポーネントの役割を完全に引き継ぐまでにかかる時間です。フェイルオーバー時間には、障害を検出するまでにかかる時間、セカンダリ接続を有効にするまでの時間、変更をネットワークの残りの部分に通知する期間など、複数の要因があります。VPN リンクにはデッドピア検出 (DPD) を使用し、リンクには双方向転送検出 (BFD) を使用することで、障害検出を改善できます。 AWS Direct Connect セカンダリ接続を有効にするまでの時間は、非常に短い場合や (接続が常にアクティブな場合)、短い場合 (事前設定された VPN 接続を有効にする必要がある場合) もあれば、長くなる場合もあります (物理リソースの移動や新しいリソースの設定が必要な場合)。ネットワークの残りの部分への通知は、通常、お客様のネットワーク内のルーティングプロトコルを介して行われ、それぞれコンバージェンス時間と設定オプションが異なります。これらの設定はこのホワイトペーパーの範囲外です。
- トラフィックエンジニアリング: 回復性に優れたハイブリッドネットワーク接続設計におけるトラフィックエンジニアリングは、通常のシナリオと障害シナリオにおいて、利用可能な複数の接続上でトラフィックがどのように流れるかを扱うことを目的としています。さまざまな障害シナリオでソリューションがどのように動作するか、またそれがビジネスで受け入れられるかどうかを検討する必要がある、障害に備えた設計の概念に従うことが推奨されます。このセクションでは、ハイブリッドネットワーク接続ソリューションの全体的な回復性レベルを高めることを目的とした、一般的なトラフィックエンジニアリングのユースケースについて説明します。ルーティングと BGP に関するAWS Direct Connect のセクションでは、トラフィックフローに影響を与えるいくつかのトラフィックエンジニアリングオプション (コミュニティ、BGP ローカルプリファレンス、AS パス長) について説明しています。効果的なトラフィックエンジニアリングソリューションを設計するには、ルートの評価と選択の観点から、 AWS 各ネットワークコンポーネントが IP ルーティングをどのように処理するかを十分に理解する必要があります。また、ルートの選択に影響を与える可能性のあるメカニズムについても理解しておく必要があります。これについての詳細は、このドキュメントの対象外です。詳細については、必要に応じて、Transit Gateway のルートの評価順序、Site-to-Site VPN のルーティングの優先度、および Direct Connect のルーティングと BGP に関するドキュメントを参照してください。

> **Note**
>
> VPC ルートテーブルでは、追加のルート選択ルールを含むプレフィックスリストを参照できます。このユースケースの詳細については、「プレフィックスリストのルート優先度」を参照してください。 AWS Transit Gateway ルートテーブルはプレフィックスリストもサポートしていますが、一度適用すると特定のルートエントリに拡張されます。

より具体的なルートを使用したデュアル Site-to-Site VPN 接続の例

このシナリオは、インターネット経由で AWS Transit Gatewayへの冗長 VPN 接続を介して単一の AWS リージョン リージョンに接続する小規模なオンプレミスサイトに基づいています。図 10 に示すトラフィックエンジニアリング設計は、次のような方法でパスの選択に影響を与え、ハイブリッド接続ソリューションの信頼性を高めることができることを示しています。

- 回復性に優れたハイブリッド接続: 冗長 VPN 接続はそれぞれ同じパフォーマンス容量を提供し、動的ルーティングプロトコル (BGP) による自動フェイルオーバーをサポートし、VPN デッドピア検出を使用することで接続障害検出を高速化します。
- パフォーマンスの効率性: AWS Transit Gateway への両方の VPN 接続に ECMP を設定すると、VPN 接続全体の帯域幅を最大化できます。あるいは、サイトサマリールートと共に、より具体的な異なるルートをアドバタイズすることで、2 つの VPN 接続間の負荷を個別に管理できます。

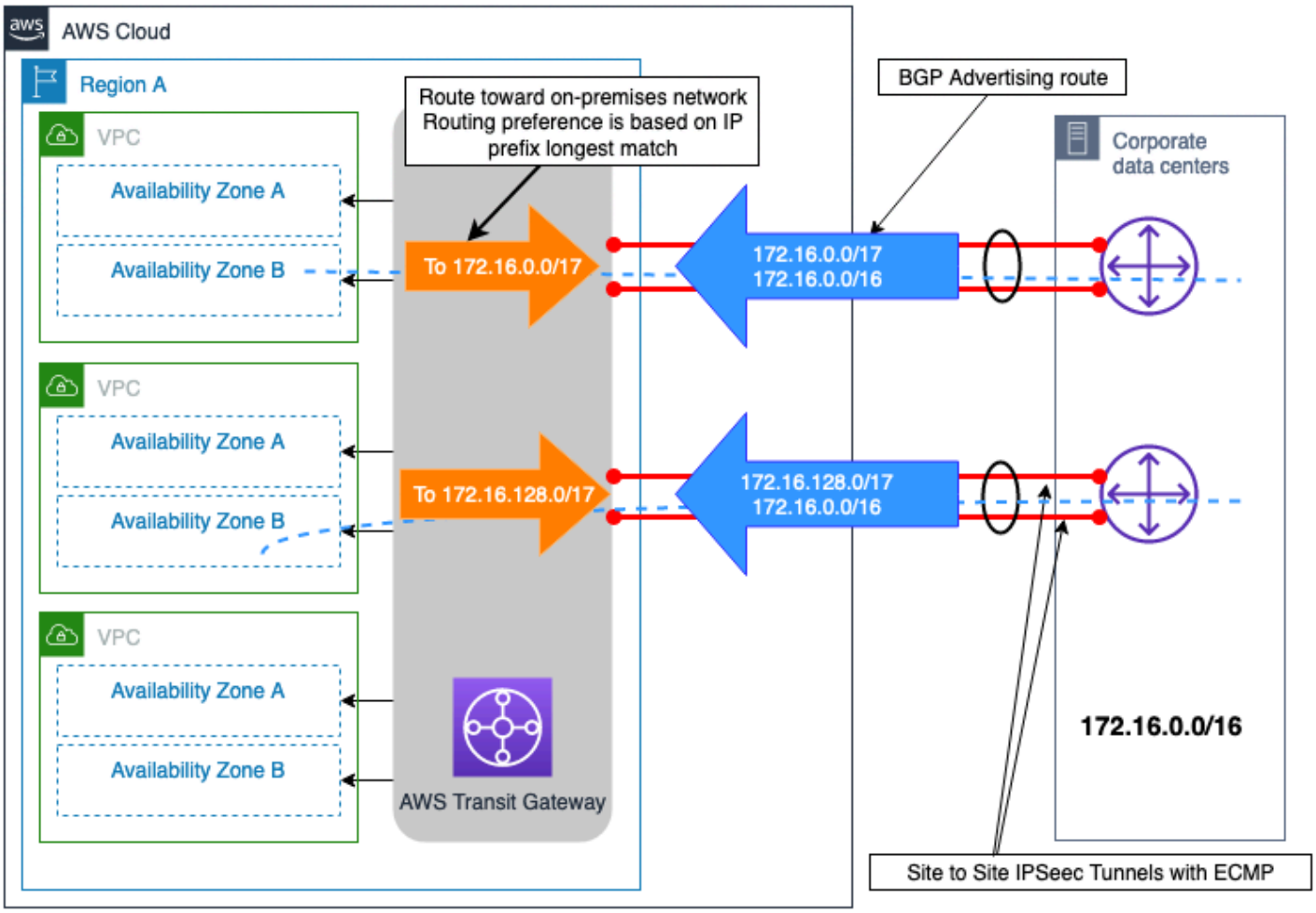

図 10 – より具体的なルートを使用したデュアル Site-to-Site VPN 接続の例

複数の DX 接続を使用するデュアルオンプレミスサイトの例

図 11 に示すシナリオでは、地理的に異なる地域にある 2 つのオンプレミスデータセンターサイトが、DXGW と VGW AWS を使用して Maximum Resiliency 接続モデル (復元力に関する推奨事項に記載) AWS Direct Connect を使用して接続されています。AWS Direct Connect これら 2 つのオンプレミスサイトは、データセンター相互接続 (DCI) リンクを介して相互に接続されています。リモートブランチサイトに属するオンプレミス IP プレフィックス (192.168.0.0/16) は、両方のオンプレミスデータセンターサイトからアドバタイズされます。このプレフィックスのプライマリパスはデータセンター 1 でなければなりません。データセンター 1 または両方の DX ロケーションで障害が発生すると、リモートブランチサイトに出入りするトラフィックはデータセンター 2 にフェイルオーバーされます。また、各データセンターにはサイト固有の IP プレフィックスがあります。これらのプレフィックスには直接アクセスする必要があります。また、両方の DX ロケーションに障害が発生した場合はもう一方のデータセンターサイトからアクセスする必要があります。

BGP コミュニティ属性を DXGW にアドバタイズされたルートに関連付けることで、 AWS DXGW 側からの出力パスの選択に影響を与えることができます。 AWS これらのコミュニティ属性は、AWSアドバタイズされたルートに割り当てられる BGP ローカルプリファレンス属性を制御します。詳細については、「 AWS DX ルーティングポリシーと BGP コミュニティ」を参照してください。

AWS リージョン このレベルでの接続の信頼性を最大化するために、 AWS DX接続の各ペアはECMPを構成し、両者をオンプレミスサイトと間のデータ転送に同時に利用できるようにします。 AWS

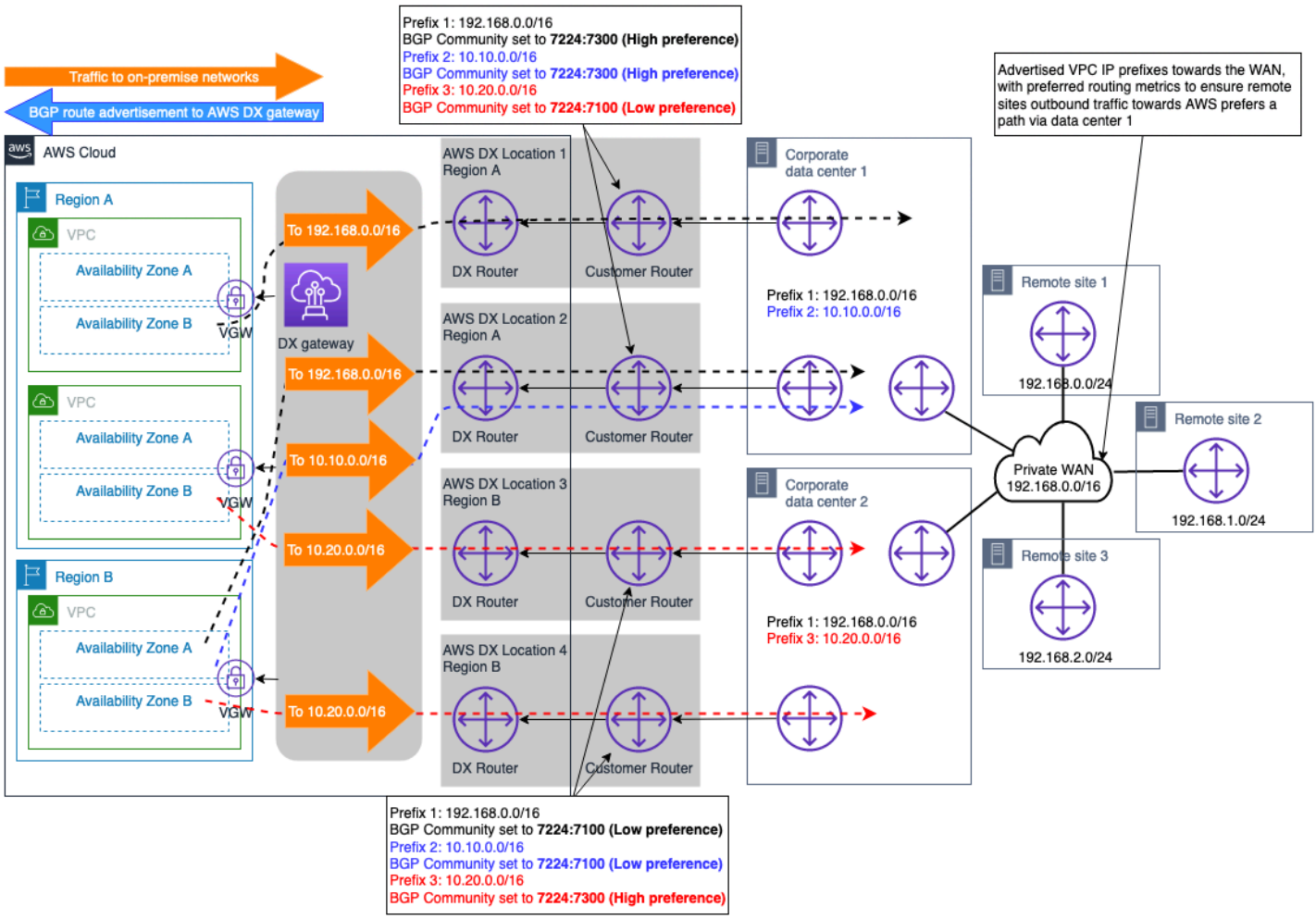

図 11 – 複数の DX 接続を使用するデュアルオンプレミスサイトの例

この設計では、(アドバタイズされるプレフィックス長と BGP コミュニティが同じである) オンプレミスネットワーク宛のトラフィックフローが、ECMP を使用してサイトごとのデュアル DX 接続に分散されます。ただし、DX 接続全体で ECMP が必要ない場合は、前述の「ルーティングポリシーと BGP コミュニティ」のドキュメントで説明されているのと同じ概念を使用して、DX 接続レベルでのパス選択をさらに調整できます。

注: オンプレミスデータセンター内のパスにセキュリティデバイスがある場合は、これらのデバイスを、同じデータセンターサイト内の 1 つの DX リンク経由で送信され、別の DX リンク (両方とも ECMP で使用されるリンク) から受信されるトラフィックフローを許可するように設定する必要があります。

DX 接続のバックアップとしての VPN 接続 (例) AWS

VPN を選択して、 AWS Direct Connect 接続へのバックアップネットワーク接続を提供できます。通常、このタイプの接続モデルはコストに左右されます。というのも、インターネット上のパフォーマンスは不確定であるため、ハイブリッド接続ソリューション全体の信頼性のレベルが低くなり、パブリックインターネット経由の接続では取得できる SLA がないためです。これは有効で費用対効果の高い接続モデルであり、コストが最優先で予算が限られている場合や、セカンダリ DX をプロビジョニングできるようになるまでの暫定的なソリューションとして使用できます。図 12 は、この接続モデルの設計を示しています。VPN 接続と DX 接続の両方がで終端となるこの設計で考慮すべき重要な点の 1 つは AWS Transit Gateway、VPN 接続は、接続先の DX 接続を介してアドバタイズできるルートよりも多くのルートをアドバタイズできることです。 AWS Transit Gatewayこれにより、最適なルーティング状況にならない可能性があります。この問題を解決するには、カスタマーゲートウェイデバイス (CGW) で VPN 接続から受信したルートにルートフィルタリングを設定し、サマリールートのみを受け付けるようにする方法があります。

注:でサマリールートを作成するには AWS Transit Gateway、ルートテーブル内の任意のアタッチメントへのスタティックルートを指定して、 AWS Transit Gateway サマリーがより具体的なルートに沿って送信されるようにする必要があります。

AWS Transit Gateway ルーティングテーブルから見ると、オンプレミスプレフィックスのルートは AWS DX 接続 (DXGW 経由) と VPN の両方から同じプレフィックス長で受信されます。のルート優先順位ロジックに従うと AWS Transit Gateway、Direct Connect 経由で受信したルートは、Site-to-Site VPN AWS Direct Connect で受信したルートよりも優先されます。したがって、オンプレミスネットワークに到達するには、経由のパスが優先されます。

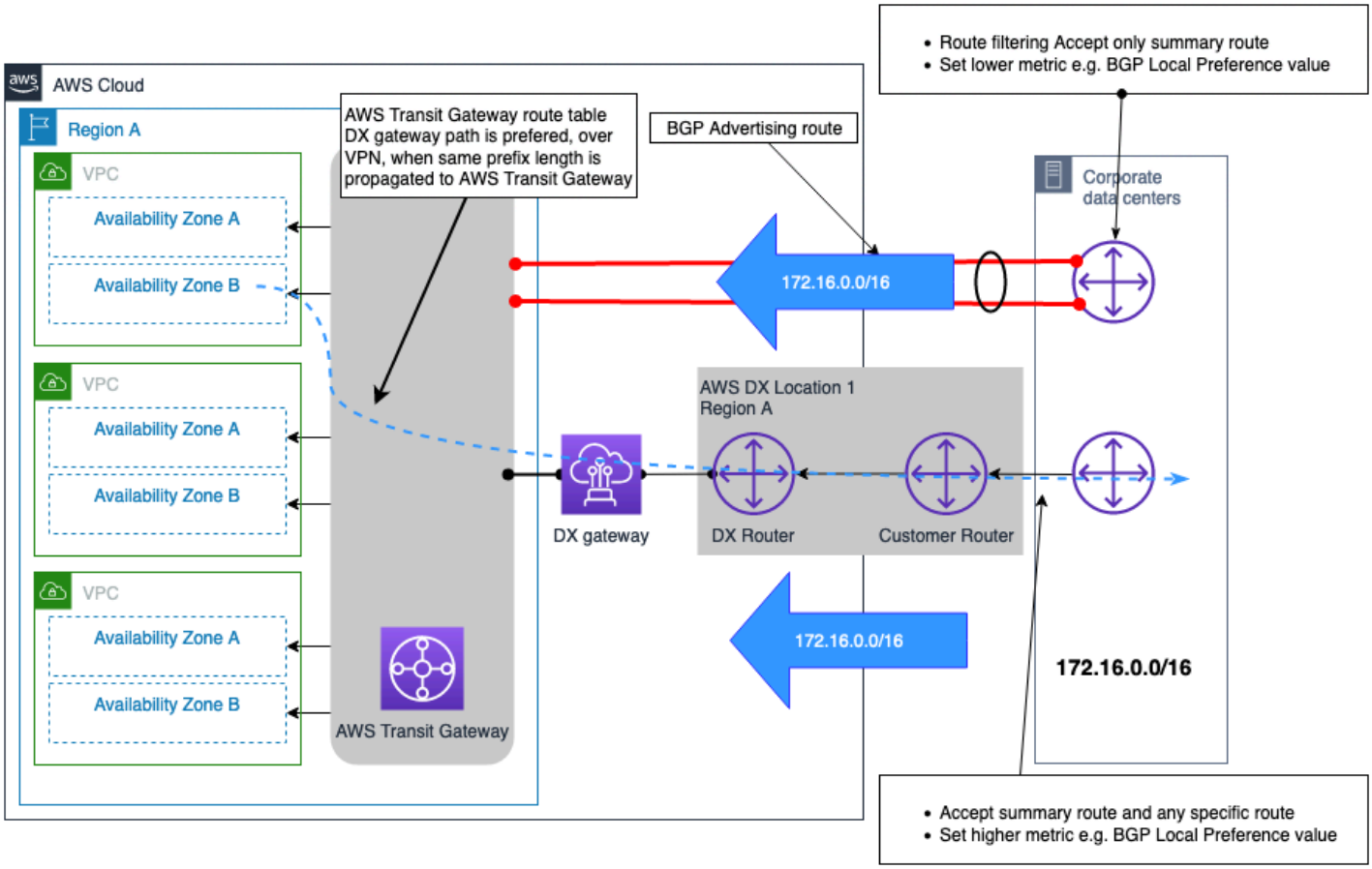

図 12 — AWS DX へのバックアップとしての VPN 接続の例

以下の決定木では、回復性のある (その結果として信頼性の高い) ハイブリッドネットワーク接続を実現するための必要な決定を下す手順を示しています。詳細については、「AWS Direct Connect Resiliency Toolkit」を参照してください。

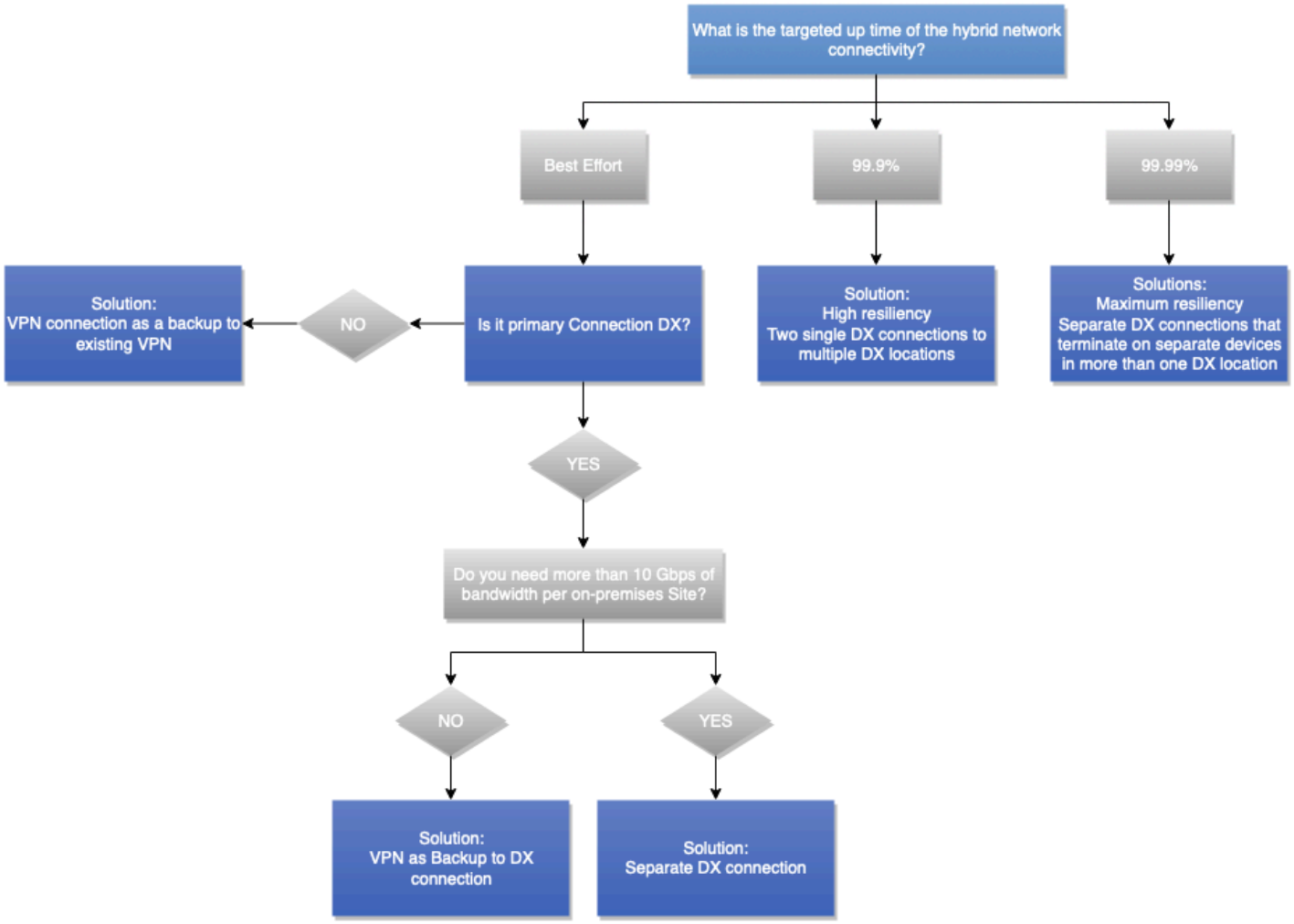

図 13 - 信頼性の決定木

カスタマーマネージド VPN と SD-WAN

定義

インターネットへの接続は必需品であり、利用可能な帯域幅は年々増加し続けています。プライベート WAN を構築して運用する代わりに、インターネット上に仮想 WAN を構築することを選択するお客様もいます。ソフトウェア定義のワイドエリアネットワーク (SD-WAN) を使用すると、企業はソフトウェアを巧みに使用することで、この仮想 WAN を迅速にプロビジョニングして一元管理できます。また、従来の自己管理型のサイト間 VPN を採用するお客様もいます。

設計上の決定への影響

SD-WAN と顧客管理 VPN は、インターネット経由または AWS Direct Connect経由で実行できます。SD-WAN (または任意のソフトウェア VPN オーバーレイ) は、基盤となるネットワークトラン

スポートと同じくらい信頼性があります。したがって、このホワイトペーパーで前述した信頼性と SLA に関する考慮事項は、ここでも当てはまります。例えば、インターネット経由で SD-WAN オーバーレイを構築しても、 AWS Direct Connect上に構築した場合と同じ信頼性は得られません。

要件の定義

- オンプレミスネットワークで SD-WAN を使用していますか。
- VPN 終端に使用される特定の仮想アプライアンスでのみ使用できる、必要な特定の機能はありますか。

テクニカルソリューション

AWS SD-WAN との統合を推奨し AWS Transit Gateway、統合をサポートするベンダーのリストを公開しています。 AWS Transit Gateway AWS SD-WAN サイトのハブまたはスポークサイトとして機能できます。 AWS バックボーンは、導入されているさまざまな SD-WAN ハブを、信頼性が高くパフォーマンスの高いネットワークに接続するために使用できます。 AWS SD-WAN ソリューションは、利用可能なあらゆる経路での自動フェイルオーバー、追加の監視、オブザーバビリティ機能を単一の管理画面でサポートします。自動構成と自動化を多用することで、従来の WAN と比較して迅速なプロビジョニングと可視化が可能になります。ただし、トンネリングと暗号化の使用のオーバーヘッドは、プライベート接続で使用される専用の高速ファイバーリンクとは比較になりません。

場合によっては、VPN 機能を備えた仮想アプライアンスを使用することもできます。自己管理型の仮想アプライアンスを選択する理由には、技術的な特徴やネットワークの他の部分との互換性などがあります。EC2 インスタンスにデプロイされた仮想アプライアンスを使用する自己管理型 VPN または SD-WAN ソリューションを選択する場合、そのようなアプライアンスの管理はお客様の責任となります。また、仮想アプライアンス間の高可用性とフェイルオーバーについても責任があります。このような設計は運用上の責任を増大させますが、柔軟性が向上する可能性があります。ソリューションの機能と能力は、選択する仮想アプライアンスによって異なります。

AWS Marketplace には、お客様が Amazon EC2 にデプロイできる VPN 仮想アプライアンスが多数含まれています。 AWS AWS マネージド S2S VPN から始め、要件を満たさない場合は他のオプションを検討することをお勧めします。仮想アプライアンスの管理オーバーヘッドはお客様の責任です。

Example Corp. Automotive のユースケース

このホワイトペーパーの本セクションでは、考慮事項、要件定義の質問、決定木をどのように活用すると、最適なハイブリッドネットワーク設計を決定できるかについて説明します。決定木への入力情報には要件を使用するため、それらを特定し、定義しておくことが重要です。要件を前もって定義しておけば、設計を何度も繰り返す必要がなくなります。設計の見直しが必要な場合にプロジェクトを完全に停止し、貴重なリソースを保留するなどの事態を最小限に抑えるには、あるいは、そうした事態の回避を理想とするなら、要件を把握しておくと良いでしょう。

このセクションでは、Example Corp. Automotive を説明用の顧客名として使用します。同社は、最初の分析プロジェクトを AWS にデプロイすることを検討しています。この分析プロジェクトで重点を置くのは、同社製の自動車から取得したデータに加え、自社のデータセンターにあるその他の既存データセットを分析することです。同社のアーキテクチャグループは当初、本番環境と開発環境をホストするには、AWS アカウント アカウント、Amazon VPC、少数のサブネットが必要になると考えていました。一方で、着手に意気込むプロジェクトチームは、可能な限りすぐにアクセスできる開発環境を求めていました。同社の目標は、3 か月後に本番環境での稼働を開始することです。

Example Corp. Automotive は、今後その他のプロジェクトでも AWS を使用する予定です。例えば、ERP システムと、仮想デスクトップインフラストラクチャ (VDI) に加え、20 のアプリケーションを、今後 6 か月間でオンプレミスから AWS に移行するなどを想定しています。追加するプロジェクトの要件の一部は、定義中の段階にありますが、AWS クラウド の利用が拡大することは明らかです。

アーキテクチャチームは、このホワイトペーパーで概説されている方法を活用することにし、各考慮事項で示されている要件定義の質問を使用して、設計上の意思決定に必要な入力情報を収集しました。

チームはまず、接続タイプ関連の要件を考察しました。次の表はそれらを大まかに示しています。

表 4 – Example Corp. Automotive の信頼性に関する入力情報

接続タイプの選択に関する考慮事項	要件定義の質問	回答
デプロイ完了までの時間	デプロイ完了までに、どれくらいの期間が必要か。数時間、数日、数週間、数か月	• 開発/テスト: 1 か月 • 本番: 3 か月

接続タイプの選択に関する考慮事項	要件定義の質問	回答
セキュリティ	セキュリティの要件とポリシーでは、AWS への接続についてインターネット経由の暗号化接続の使用を許可しているか。それともプライベートネットワーク接続の使用を義務付けているか。	• 開発/テスト: Site-to-Site VPN を使用可能 • 本番: プライベートネットワークが必要
	プライベートネットワーク接続を利用する場合、ネットワーク層での転送中に暗号化を行える必要がありますか。	不要。アプリケーション層の暗号化を使用する
SLA	ハイブリッド接続の SLA では、サービスクレジットも定める必要があるか	• 開発/テスト: 定める必要はない • 本番: 定める必要がある
	どの程度の稼働時間目標を設定するか。	• 開発/テスト: 設定しない • 本番: 99.99%
	ハイブリッドネットワーク全体で、稼働時間目標を遵守する必要があるか。	• 開発/テスト: 設定しない • 本番: 定める必要がある
パフォーマンス	必要なスループットはどれくらいか。	• 開発/テスト: 100 Mbps • 本番: 500 Mbps から 2 Gbps に拡大
	AWS とオンプレミスネットワーク間では、最大で、どの程度のレイテンシーを許容するか。	• 開発/テスト: 厳しい要件は設定しない • 本番: 30 ミリ秒未満

接続タイプの選択に関する考慮事項	要件定義の質問	回答
	最大で、どの程度のネットワークジッターを許容するか。	• 開発/テスト: 厳しい要件は設定しない • 本番: 可能な限り最小にする
コスト	1 か月あたり、どれくらいの量のデータを AWS に送信するか。	• 開発/テスト: 2 TB • 本番: 20 TB から 50 TB に増量
	1 か月あたり、どれくらいの量のデータを AWS から送信するか。	• 開発/テスト: 1 TB • 本番: 10 TB から 25 TB に増量
	この接続は永続的なものか。	Yes

要件を受け取ったアーキテクチャチームは、それを基に、図 9 の接続タイプの決定木に従って検討を進め、開発環境、テスト環境、本番環境の接続タイプを決定しました。本番環境については、当面の要件だけでなく将来の要件も考慮しました。開発およびテスト環境向けには、インターネット上にサイト間 VPN を確立します。また、本番環境構築のために、サービスプロバイダーと協力して、自社ネットワークを AWS Direct Connect に接続します。当初は、Direct Connect ホスト接続の使用を検討していましたが、AWS が示す SLA の要件を理由に、Direct Connect 専用接続を選択しました。

接続タイプ決定後の次のステップは、接続設計の選択に影響を与える要件を明確に示すことです。このプロセスは、ビジネスおよび技術上の要件に対応するにはどのように接続を構成し、どの AWS サービスを利用すべきかといった論理設計に関係があり、そうした設計に影響を与えます。

スケーラビリティと通信モデルの要件を明確にしようと、アーキテクチャチームは、このホワイトペーパーの関連セクションにある要件定義の質問を使用しました。次の表に、これら 2 つの考慮事項に関連する要件を大まかに示します。

表 5 - 要件定義に関する質問

接続設計の選択に関する考慮事項	要件定義の質問	回答
スケーラビリティ	オンプレミスサイトへの接続が必要な VPC の現在数または想定数は、どれくらいか。	当初は 2。6 か月で 30 に増加すると想定
	これらの VPC は、1 つの AWS リージョン にデプロイされているか。あるいは、複数のリージョンにデプロイされているか。	1 つのリージョン
	AWS に接続する必要があるオンプレミスサイトはいくつですか。	2 か所のデータセンター
	AWS への接続が必要なカスタマーゲートウェイデバイスは、サイトごとに何台あるか。	データセンターごとに 2 台のルーター
	AWS VPC にアドバタイズするルートの数と、AWS 側から受信するルートの数はどれくらいになると想定しているか。	• AWS にアドバタイズするルート: 20 ルート • AWS から受信するルート: 1/16 ルート
	近い将来、AWS への接続に必要な帯域幅の拡大を検討する予定はあるか。	• 開発/テスト: 100 Mbps • 本番: 500 Mbps から 2 Gbps に拡大
接続設計モデル	VPC 間通信を (リージョン内および/またはリージョン間で) 有効にする必要はあるか。	AWS リージョン 内での有効化が必要
	オンプレミスから AWS パブリックエンドポイントサービ	Yes

接続設計の選択に関する考慮事項	要件定義の質問	回答
	スに直接アクセスする必要はあるか。	
	オンプレミスから VPC エンドポイントを使用して AWS サービスにアクセスする必要はあるか。	No

アーキテクチャチームは、入力情報に従って、接続設計セクションの決定木をたどりました。今後 6 か月で VPC の数が 2 から 30 に増加すると予想した同チームは、接続および VPC 間のルーティングに使用する終端ゲートウェイとして AWS Transit Gateway の導入を決定しました。各 AWS Transit Gateway は、開発およびテスト環境用 VPN 接続と、AWS Direct Connect との本番環境用 VPN 接続で、独立した終端装置として機能します。独立した AWS Transit Gateway を使用すると、変更管理が簡素化されると共に、開発/テスト環境と本番環境との境界が明確になります。本番環境には AWS Direct Connect があるため、AWS Transit Gateway ゲートウェイが必要です。AWS パブリックエンドポイントサービスへのアクセスには、パブリック VIF を使用します。図 14 は、収集した要件に基づいて決定木をどのようにたどったかを示しています。

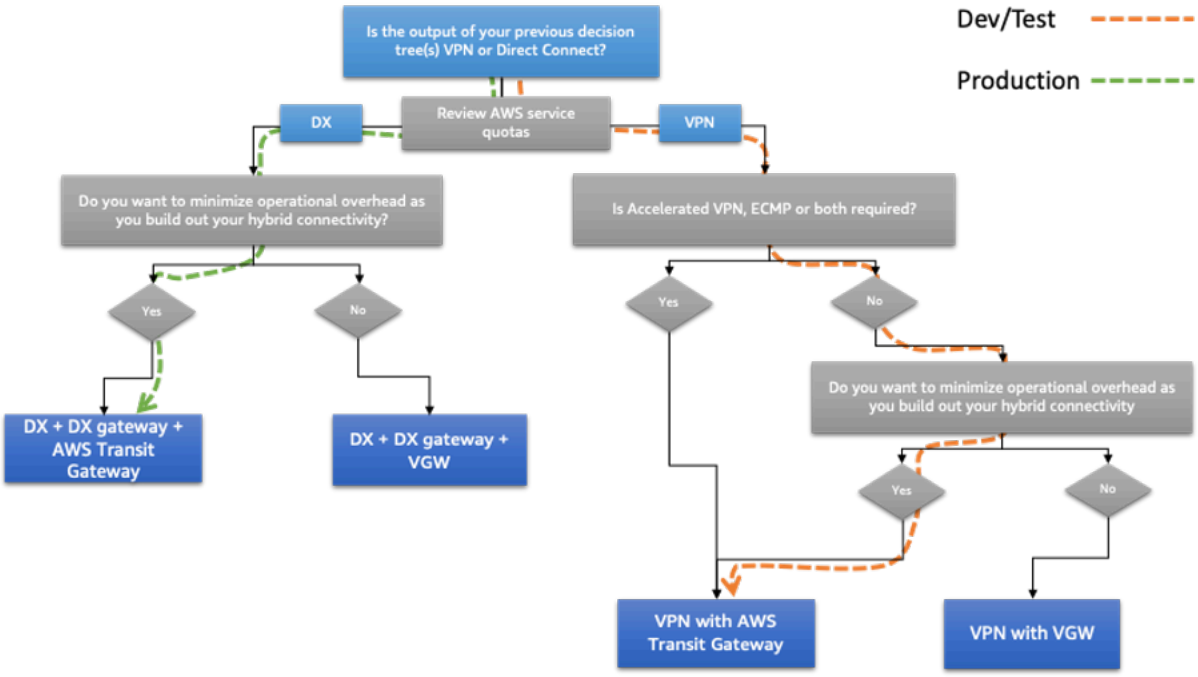

図 14 – Example Corp. Automotive の接続設計の決定木

スケーラビリティと通信モデルの要件を満たすソリューションを決定したら、次のステップは、信頼性に関連する要件を明確に示すことです。このプロセスは、可用性と耐障害性がどの程度必要かに影響を与えます。

信頼性要件を明確にしようと、アーキテクチャチームは、このホワイトペーパーの関連セクションにある要件定義の質問を使用しました。次の表は、それらの要件を大まかに示しています。

表 6 - 信頼性要件に関する質問

接続設計の選択に関する考慮事項	要件定義の質問	回答
信頼性	AWS への接続で障害が発生した場合、ビジネスにどの程度の影響が及ぶか。	• 開発/テスト: 影響は小さい • 本番: 影響は大きい
	ビジネスの観点から考えると、AWS への接続で障害が発生した場合のコストは、高信頼性の接続モデルを AWS に展開するコストを上回るか。	• 開発/テスト: 定める必要はない • 本番: 定める必要がある

受け取った入力情報に基づいて、アーキテクチャチームは、このホワイトペーパーに示されている「信頼性に関する考慮事項」セクションの決定木をたどりました。本番環境向け接続の 99.99% という稼働時間目標と、サービスが中断した場合のビジネスへの大きな影響を考慮した結果、2 か所の Direct Connect ロケーションを使用し、各オンプレミスデータセンターから各 Direct Connect ロケーションに 2 つのリンクを設けることにしました (合計 4 リンク)。開発およびテスト環境用 VPN 接続でも、冗長性を高めるために 2 つの VPN 接続を使用します。接続は、「信頼性」セクションで説明したルートエンジニアリング手法を使用して、次のように構成します。

- 開発およびテスト環境: プライマリデータセンターに向かう 2 つのトンネルで、ECMP によってトラフィックを負荷分散し、スループットを向上させます。セカンダリデータセンターに向かうトンネルは、プライマリトンネルに障害が発生した場合に使用します。
- 本番環境: オンプレミスのレイテンシーと、いずかの Direct Connect ロケーション経由で AWS に接続するときのレイテンシーは、ほぼ同じです。この事例では、AWS とオンプレミス間のトラフィックをロードバランスすることにしました。ロードバランスは、プライマリデータセンターに向かう 2 つの接続で行い、これらのトラフィックを、プライマリデータセンター内に展開したオ

ンプレミスシステムで使用します。同様に、セカンダリデータセンターで稼働するオンプレミスシステム向けにも、そのデータセンターまでを結ぶ 2 つの接続をロードバランスします。接続上の障害が発生した場合、BGP を利用して自動的にフェイルオーバーさせます。

図 15 は、収集した要件に基づいて決定木をどのようにたどったかを示しています。

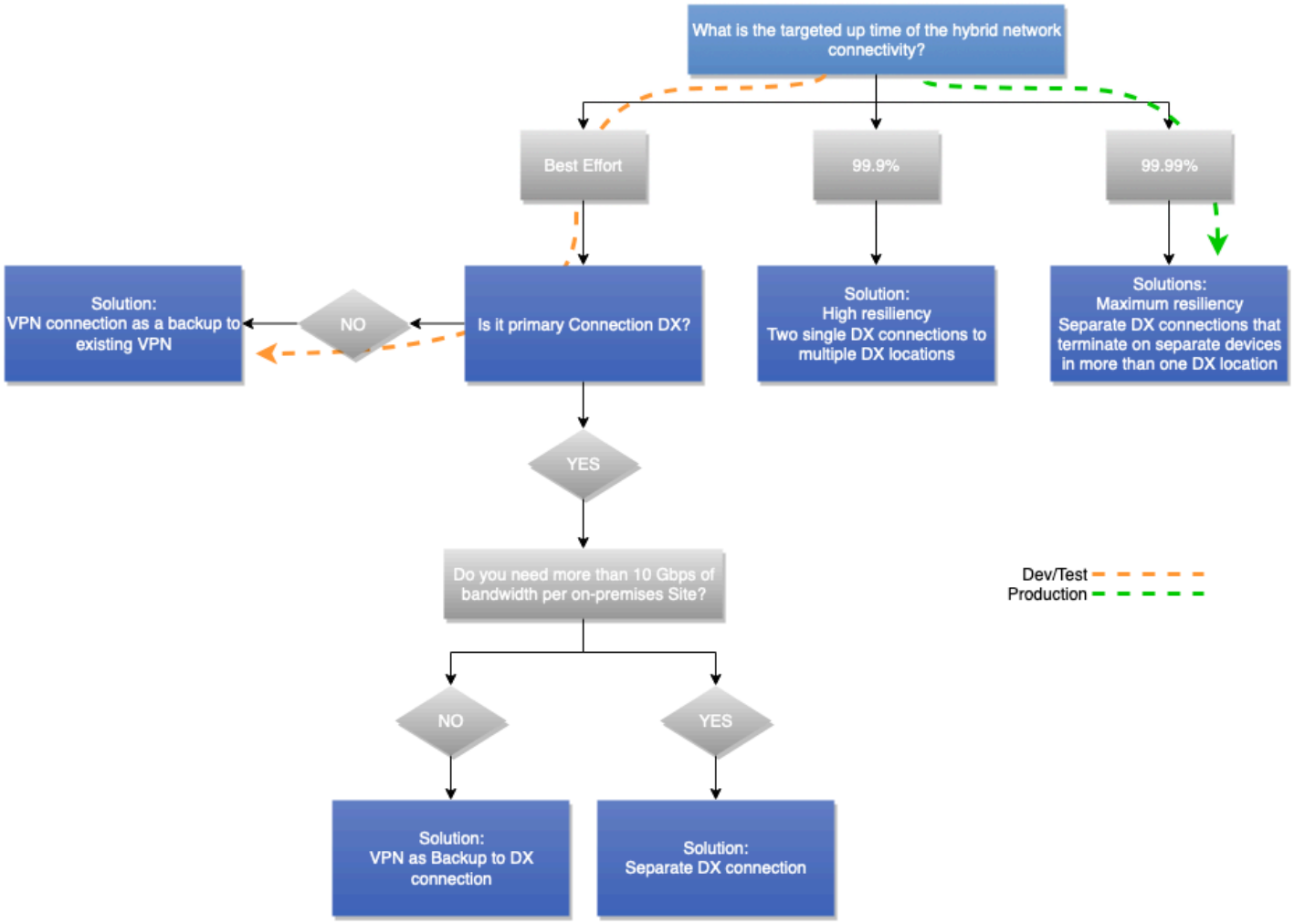

図 15 - Example Corp. Automotive の信頼性の決定木

Example Corp. Automotive が選択したアーキテクチャ

Example Corp. Automotive は、要件を収集し、このホワイトペーパーの前のセクションで示された決定木をたどった後に、アーキテクチャを選択しました。それを次の図に示します。

このアーキテクチャでは、開発およびテスト環境向けに、AWS Transit Gateway を終端とするインターネット経由で AWS S2S VPN を使用します。本番環境のトラフィックには、Direct Connect

ゲートウェイと 2 番目の AWS Transit Gateway を経由する AWS Direct Connect を使用します。AWS Transit Gateway は VPC 間のルーティングに使用します。データパスの観点で言えば、プライマリデータセンターの VPN トンネルは、開発およびテスト環境用のプライマリパスとして使用し、セカンダリデータセンターへのトンネルは、フェイルオーバー時のパスとして使用します。本番環境のトラフィックには、すべての接続を同時に使用します。AWS からのトラフィックには、オンプレミスシステムが配置されているデータセンターに基づいて、最良のネットワーク接続が優先的に選択されるようにします。また、同様のルートエンジニアリング技術を使用して、トラフィックが AWS に向かうときに、適切なパスが優先され対称的なパスが使用されるよう設計します。これにより、オンプレミスのプライマリおよびセカンダリデータセンター間の自社ネットワークの使用を最小限に抑えます。

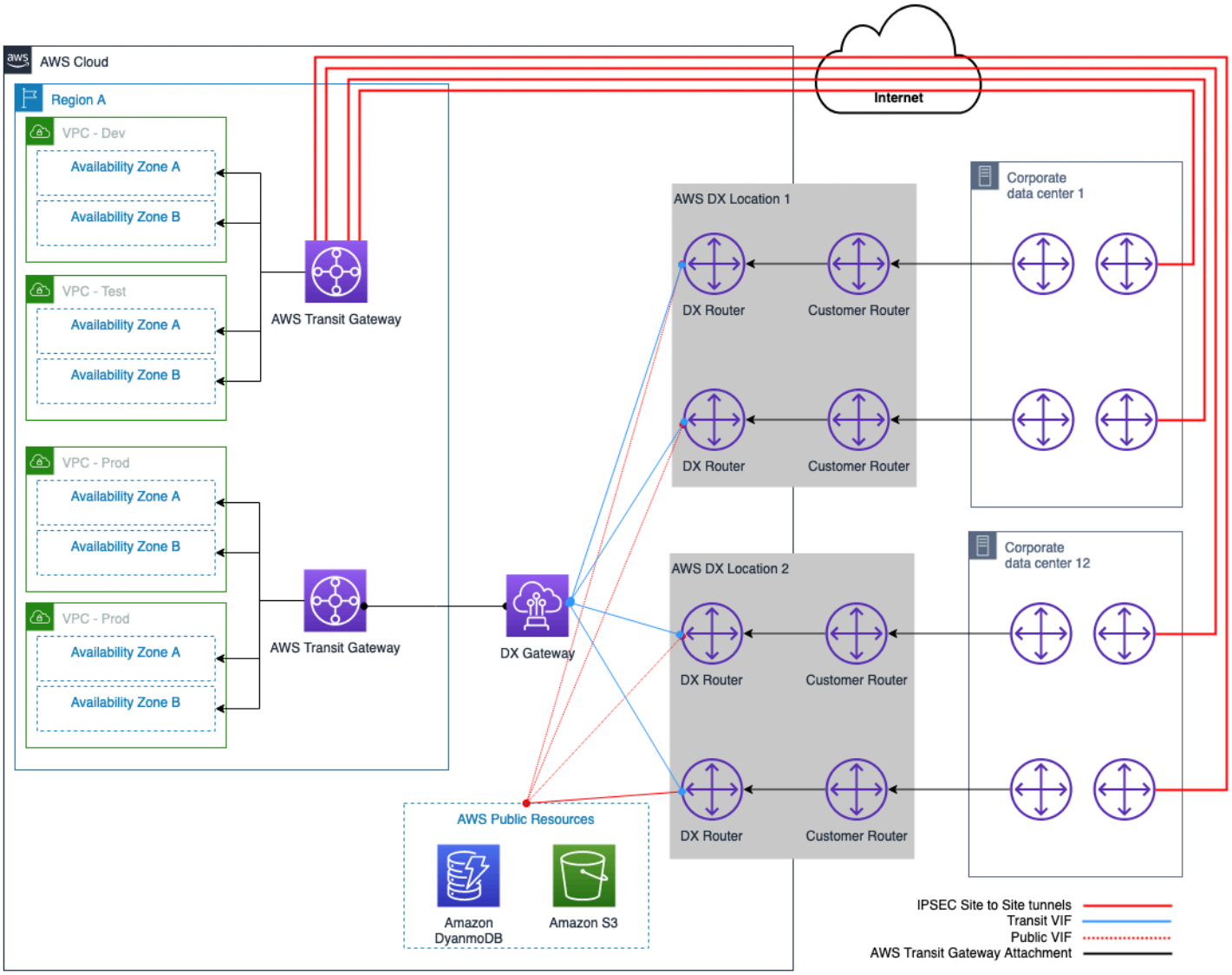

図 16 - Example Corp. Automotive が選択したハイブリッド接続モデル

結論

ハイブリッド接続モデルは、クラウドコンピューティングを採用するための基本的な出発点の 1 つです。ハイブリッドネットワークは、このホワイトペーパーで説明されている接続モデルの選択プロセスに従って、最適なアーキテクチャで構築できます。

このプロセスは、論理的な順序で整理された検討事項で構成されています。この順序は、経験豊富なネットワーク設計者やクラウド設計者が従うメンタルモデルによく似ています。それぞれの検討事項の中で、ディシジョンツリーを使うと、入力要件が限られていても接続モデルを迅速に選択できます。いくつかの考慮事項とそれに対応する影響が、異なる解決策を示していることに気付くかもしれません。このような場合、意思決定者はいくつかの要件について妥協し、ビジネス要件と技術要件を満たす最適なソリューションを選択する必要があるかもしれません。

寄稿者

本ドキュメントの寄稿者は次のとおりです。

- Amazon Web Services、プリンシパルソリューションアーキテクト、James Devine
- Amazon Web Services、プリンシパルソリューションアーキテクト、Andrew Gray
- Amazon Web Services、シニアソリューションアーキテクト、Maks Khomutskyi
- Amazon Web Services、ソリューションアーキテクト、Marwan Al Shawi
- Amazon Web Services、技術責任者、Santiago Freitas
- Amazon Web Services、スペシャリストソリューションアーキテクト - ネットワーキング、Evgeny Vaganov
- Amazon Web Services、スペシャリストソリューションアーキテクト - ネットワーキング、Tom Adamski
- Amazon Web Services、ソリューションアーキテクト、Armstrong Onaiwu

詳細情報

- スケーラブルでセキュアなマルチ VPC の AWS ネットワークインフラストラクチャの構築
- Hybrid Cloud DNS Options for Amazon VPC
- Amazon Virtual Private Cloud Connectivity Options
- Amazon Virtual Private Cloud ドキュメント
- AWS Direct Connect ドキュメント
- ホスト型仮想インターフェイス (VIF) とホスト型接続の違いは何ですか?

ドキュメントの改訂

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードにサブスクライブしてください。

変更	説明	日付
マイナーな更新	DX クォータの上限の引き上げが反映されるよう更新しました。	2023 年 7 月 10 日
メジャーな更新	最新のベストプラクティス、サービス、機能が記載されるよう更新しました。	2023 年 7 月 6 日
マイナーな更新	DX クォータの変更が反映されるよう、リファレンスアーキテクチャの図を更新しました。	2023 年 6 月 27 日
マイナーな更新	リンク切れを修正しました。	2022 年 3 月 22 日
初版発行	ホワイトペーパーの初回発行	2020 年 9 月 22 日

注意

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤー、またはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または黙示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は AWS 契約によって規定されます。本書は、AWS とお客様との間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。