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。

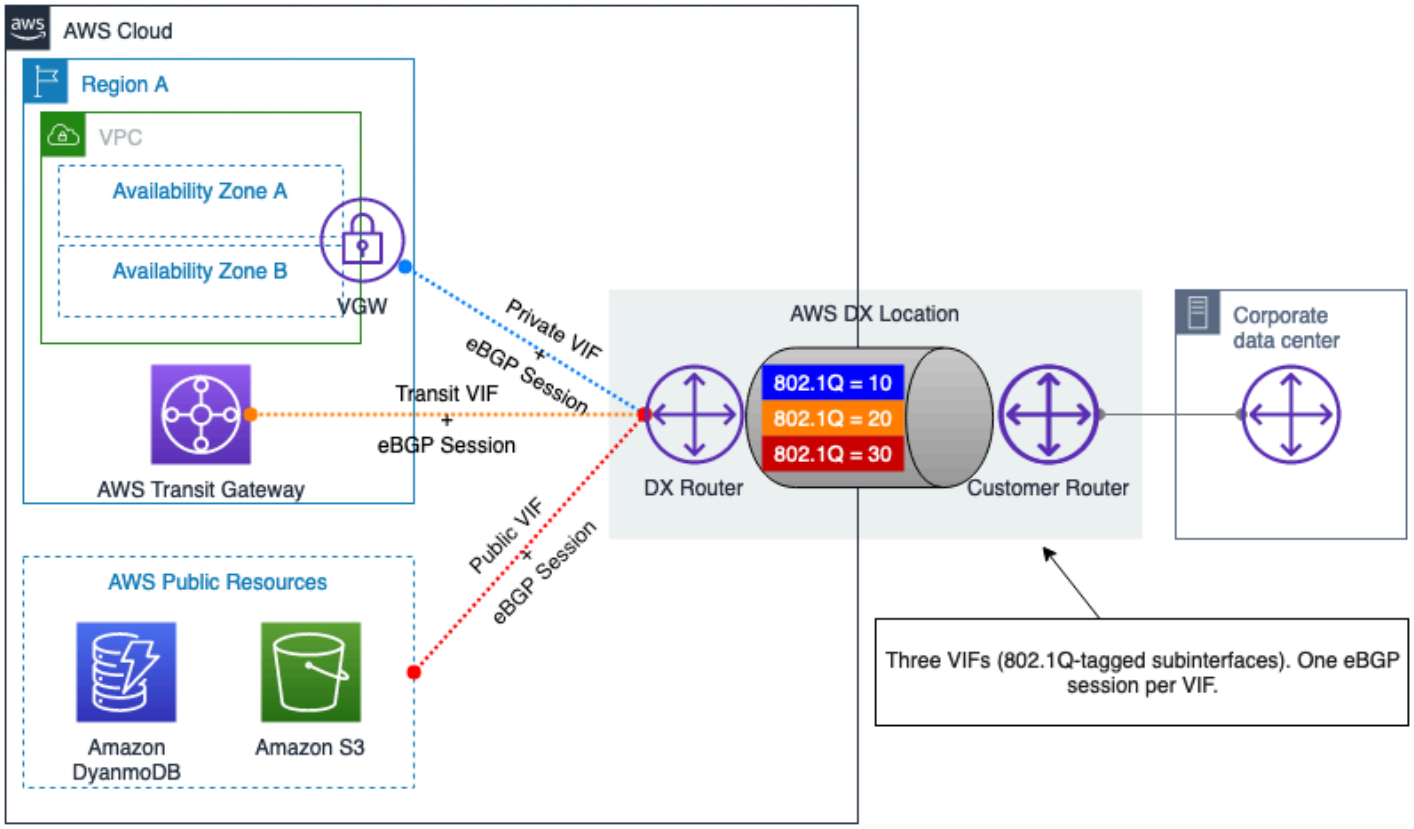

図 1 — AWS Direct Connect プライベート VIF とパブリック VIF

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。

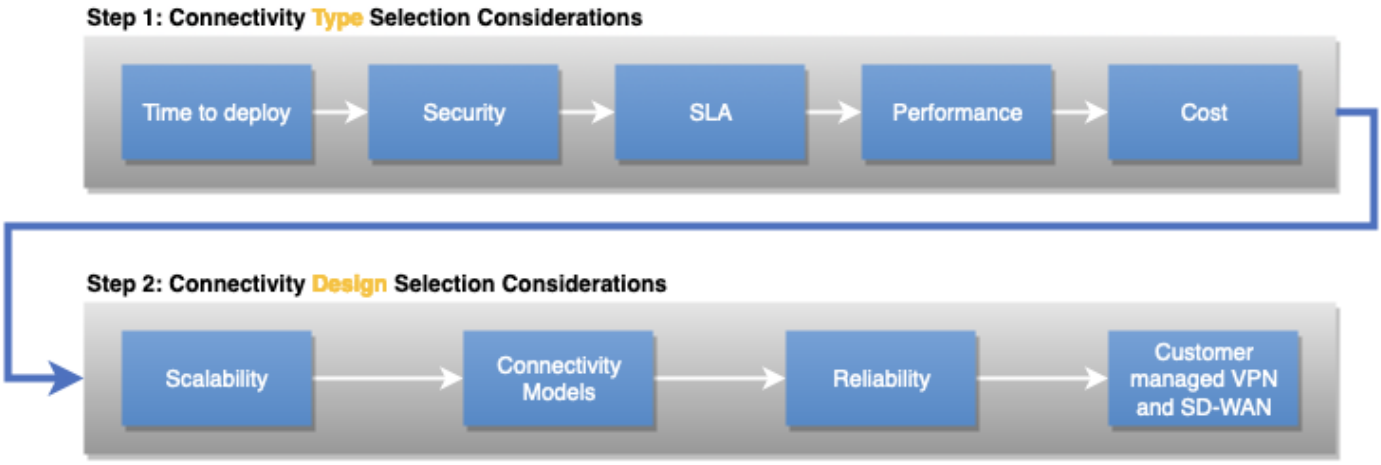

図 2 – 考慮事項のカテゴリ、個々の考慮事項、各項目間の論理的な順序を示す図

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。これには、デプロイまでの時間、セキュリティ、SLA、パフォーマンス、コストが含まれます。

考慮事項

- デプロイするまでの時間
- セキュリティ
- サービスレベル契約 (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。これにより、インターネットベースの接続、プライベート専用接続、または AWS Direct Connect パートナーによってマネージドサービスとして提供されるプライベートホスト接続を使用するかどうかの決定に影響します。

重要な質問

- デプロイ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に AWS 接続が必要な場合は、ほとんどの場合、既存のネットワーク接続を使用する必要があります。これは多くの場合、パブリックインターネット経由で への AWS VPN 接続を確立することを意味します。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、数時間以内に新しいホスト接続をプロビジョニングできます。

数日から数週間の場合は、 AWS Direct Connect パートナーと協力して へのプライベート接続を確立できます AWS。 AWS Direct Connect パートナーは、 AWS Direct Connect ロケーションとデータセンター、オフィス、またはコロケーション環境間のネットワーク接続を確立するのに役立ちます。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。ホスト接続は、多くの場合、Dedicated Connections よりも迅速に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。

数週間から数か月の場合は、 との専用プライベート接続の確立を調べることができます AWS。サービスプロバイダーと AWS Direct Connect パートナーは、 AWS Direct Connect Dedicated Connections を促進します。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 ロケーションが存在するのと同じコロケーション施設に既にネットワーク機器がインストールされている場合は、コロケーションサイトでクロスコネクトを介して Dedicated Connection をすばやく確立 AWS Direct Connect できます。接続をリクエストすると、 AWS は認可と接続ファシリティ割り当てのレター (LOA-CFA) をダウンロードできるようにするか、詳細をリクエストして E メールで送信します。LOA-CFA は、 に接続する認可であり AWS、クロスコネクトを注文するためにネットワークプロバイダーによって必要です。

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。 AWS Direct Connect パートナーから正確なプロビジョニング時間について通知されます。

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

- セキュリティ要件とポリシーでは、インターネット経由で暗号化された接続を使用して接続することを許可していますか AWS、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

セキュリティ要件とポリシーでは、インターネットの使用を許可したり、 AWS と会社のネットワーク間のプライベートネットワーク接続の使用が必要になる場合があります。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。

インターネットを活用できる場合、 AWS Site-to-Site VPN を使用して、インターネット経由でネットワークと Amazon VPCs または AWS Transit Gatewayの間に暗号化されたトンネルを作成できます。インターネットベースの接続を活用する場合、SD-WAN ソリューションをインターネット経由で に AWS 拡張することもオプションです。このホワイトペーパーの後半の「カスタマーマネージド型 VPN と SD-WAN」セクションでは、SD-WAN に関する具体的な考慮事項について説明します。

AWS と会社のネットワークとの間でプライベートネットワーク接続が必要な場合は、 では AWS Direct Connect Dedicated Connections または Hosted Connections の使用 AWS を推奨します。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 経由の Word (パブリック VIFVPN またはトランジット VIF) を確立するか、10Gbps または 100Gbps の専用接続で MACsec を使用することを検討する必要があります。

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	はい	DX 経由の S2S VPN、トランジット VPN 経由の S2S VIF、または 10Gbps または 100Gbps 専用接続の MACsec が必要です

サービスレベル契約 (SLA)

定義

エンタープライズ組織は、組織が消費するサービスごとに SLA を満たすことをサービスプロバイダーに要求することがよくあります。次に、組織は独自のサービスを上に構築し、独自のコンシューマーに SLA を提供する場合があります。SLA は、サービスがどのように提供および運用されるかを説明するために重要であり、可用性などの特定の測定可能な特性を含むことがよくあります。サービスが定義された SLA を破った場合、サービスプロバイダーは通常、契約で指定された金銭的補償を提供します。SLA は、測定のタイプ、要件、測定期間を定義します。例として、 AWS Direct Connect SLA のアップタイムターゲット定義を参照してください。

重要な質問

- サービスクレジットを含むハイブリッド接続接続 SLA は必要ですか？
- 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 は、さまざまな ISPs セットを使用して複数のリンクを配置することに細心の注意を払っていますが、インターネットの管理は単に AWS または単一のプロバイダーの管理ドメインの外部にあります。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 エンドポイントの可用性ターゲットを提供する AWS Site-to-Site VPN SLA があります。

AWS Direct Connect は、SLA が満たされなかった毎月の請求サイクルで利用できなくなった該当する接続に対してお客様が支払ったポートアワー料金の合計に対するパーセンテージとして計算されたサービスクレジットを含む正式な SLA を提供します。 AWS Direct Connect これは、SLA が必要な場合に推奨される転送です。 は、 AWS Direct Connect 場所の数、接続、その他の設定の詳細など、各アップタイムターゲットの特定の最小設定要件を AWS Direct Connect 一覧表示します。要件を満たさない場合、サービスが定義された SLAs を切断してもサービスクレジットを提供できません。

重要なのは、ハイブリッド接続を提供するように選択されたサービスが SLA 要件を満たすように設定されている場合でも、ネットワークの残りの部分では同じレベルの SLA が提供されないことがあります。 AWS 責任は AWS Direct Connect 、ポート AWS Direct Connect の場所で終了します。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、接続は、該当する場合、ユーザーとサービスプロバイダーの間で SLA の対象となります。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 パートナーは AWS Direct Connect 接続を提供します。パートナーは、 とのデマケーションポイントまでの製品提供に基づいて、サービスクレジットを含む SLA を提供することができます AWS。オプションは APN Partners で評価し、さらに詳しく調べる必要があります。AWS は検証済みの配信パートナーのリストを発行します。

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には独自の SLA があり、AWS S2S VPN も同様です。セキュリティ上の理由から、をスケールおよび AWS S2S VPN AWS Transit Gateway に使用している可能性がありますが、各サービスでサービスクレジットの対象となるには、各 SLAs と一致する方法で両方を設計する必要があります。

「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。

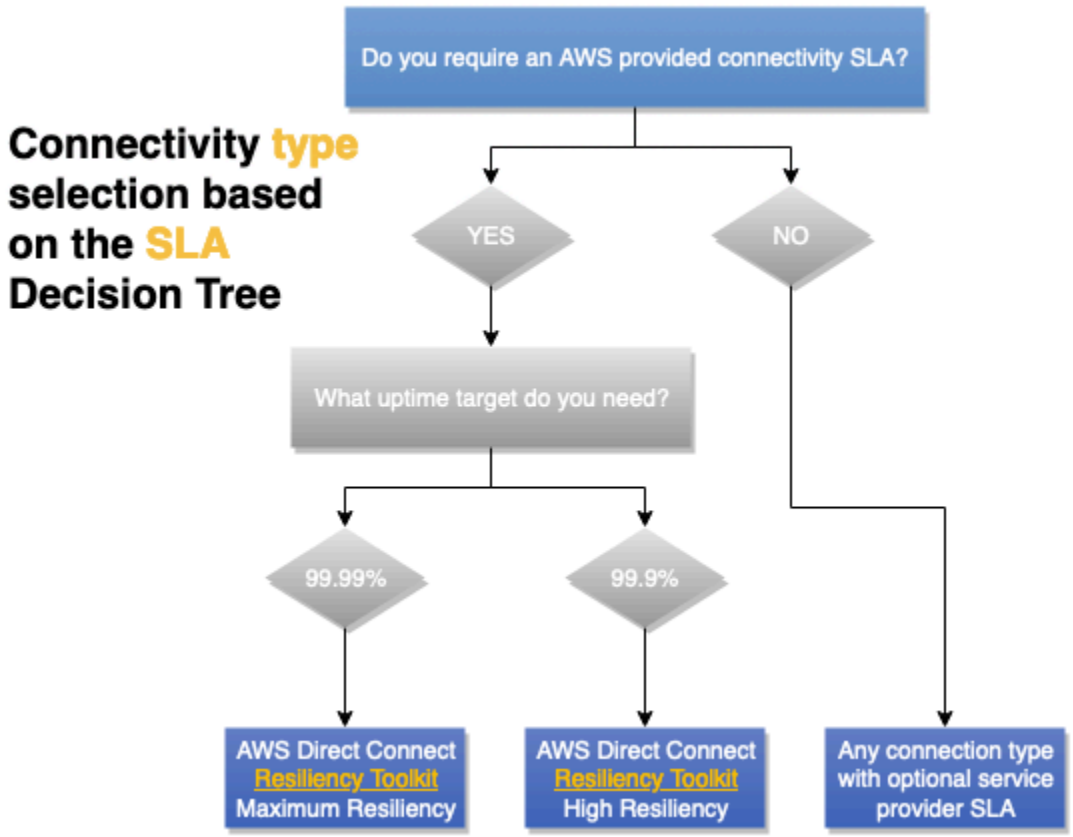

図 3 – SLAの検討決定ツリー

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。VPNsヘッドのトンネリング、MTU の制限の引き下げ、ハードウェア帯域幅の制限により、Word はスループットを制限できます。

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。

TCP を使用してトラフィックをトランスポート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。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、それに対して非常に敏感である可能性があります。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。一部の VPN ソリューションには、トラフィックの伝送に使用するネットワーク上のパケット損失から復旧するための独自のメカニズムが含まれています。

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必要な場合は、決定的なパフォーマンスを提供するため、AWS Direct Connect が推奨されます。帯域幅はスループット要件に基づいて選択できます。インターネットベースの接続よりも一貫したネットワークエクスペリエンス AWS Direct Connect が必要な場合は、 を使用する AWS ことをお勧めします。プライベートVIFsとトランジットVIFsはジャンボフレームをサポートしているため、ネットワーク経由のパケット数を減らし、オーバーヘッドを減らすことでスループットを向上させることができます。 AWS Direct Connect SiteLinkはバック AWS ボーンを使用してロケーション間の接続を提供し、オンデマンドで有効にできます。Direct Connect 帯域幅の選択には、 SiteLink で使用される帯域幅を考慮する必要があります。

VPNオーバーを使用すると、暗号化 AWS Direct Connect が追加されます。ただし、これにより MTU の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 managed Site-to-Site (S2S) VPN の機能については、AWS Site-to-Site VPN ドキュメントを参照してください。接続を介した暗号化が主要な暗号化要件である場合、多くの直接接続ロケーションで MACsec がサポートされています。MACsec には、VPN 接続と同じ MTU Site-to-Site または潜在的なスループットに関する考慮事項はありません。 は、等価コストのマルチパスルーティング (ECMP) を使用して VPN 接続の数を水平方向にスケーリングし、それに応じてスループットを向上させることをお客様に AWS Transit Gateway 許可します。 AWSの Managed Site-to-Site VPN、プライベート接続に Direct Connect トランジットVIFsの使用をサポートしています。詳細については、 のプライベート IP VPN AWS Direct Connectを参照してください。

もう 1 つのオプションは、インターネットVPN経由で AWS Managed Site-to-Site を使用することです。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。インターネットの気象イベント、輻輳、レイテンシー期間の増加は予測不可能である可能性があります。 AWS は、インターネットパスの使用に伴ういくつかの欠点を軽減できる AWS Accelerated S2S VPN を備えたソリューションを提供します。Accelerated S2S VPN は AWS Global Accelerator を使用します。これにより、VPN トラフィックはカスタマーゲートウェイデバイスにできるだけ早く、できるだけ近くに AWS ネットワークに入ることができます。これにより、輻輳のない 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、トラフィックを最高のパフォーマンスを提供するエンドポイントにルーティングします。高速 VPN 接続を使用すると、トラフィックがパブリックインターネット経由でルーティングされるときに発生する可能性のあ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。その他のコストには、 AWS ネットワークポイントオブプレゼンスへの接続コストが含まれます。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、サービスプロバイダーまたは APN Direct Connect パートナーのコストが発生します。

重要な質問

- 施設とインターネットから AWS 毎月 に送信される予定のデータ量はどのくらいですか。

- 1 か月 AWS あたりに、 から施設およびインターネットに送信するデータ量はどのくらいになると思われますか。
- 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

実行する帯域幅負荷の高いワークロードがある場合 AWS、 AWS Direct Connect は 2 AWS つの方法でネットワークコストを と との間で削減できます。まず、 との間で AWS 直接データを転送することで、インターネットサービスプロバイダーに支払う帯域幅コストを削減できます。次に、専用接続を介して転送されるすべてのデータは、インターネット AWS Direct Connect データ転送レートではなく、データ転送レートが引き下げられます。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 では、 AWS Direct Connect SiteLink を使用して AWS バックボーンを使用してサイトを相互接続できます。詳細については、 SiteLink 起動ブログを参照してください。この機能を活用すると、通常の Direct Connect データ転送コストと 1 時間あたりの料金 SiteLink が有効になります。オンデマンドで SiteLink を有効または無効にできます。インターネットまたはプライベートネットワーク接続が関与する障害シナリオには、このオプションが適している場合があります。

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 ネットワーク上のあらゆる場所から中国 AWS リージョン を除く にトラフィックを配信できます。この機能は、インターネットを使用してリモートにアクセスするよりも多くの技術的利点がありますが AWS リージョン、コストがかかります。詳細については、EC2 Data Transfer 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。

最適なアプリケーション設計は、データ処理を内部に保持 AWS し、不要なデータ出力料金を最小限に抑えます。へのデータ入力 AWS は無料です。

> **Note**
>
> 全体的な接続ソリューションの一環として、 AWS 接続コストに加えて、DX ロケーション内のサービスプロバイダーのコスト、クロスコネクト、ラック、機器 (必要な場合) など、 end-to-end 接続のコストも考慮する必要があります。

インターネットを使用するべきかプライベート接続を使用するべきかわからない場合は、インターネットを使用するよりも安価 AWS Direct Connect になる損益分岐点を計算します。データ量により AWS Direct Connect が安価になり、永続的な接続が必要な場合は、 が最適な接続オプション AWS Direct Connect です。

接続が一時的なものであり、インターネットが他の要件を満たしている場合、インターネットの弾力性により、インターネット経由で AWS S2S VPN を使用する方が安価になる場合があります。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 リストは Direct Connect ウェブサイトで入手可能) である 施設内にいる場合は、 へのクロスコネクトを確立できます AWS。つまり、専用接続を 1、10、または 100Gbps で使用するということです。 AWS Direct Connect パートナーは、より多くの帯域幅オプションとより小さな容量を提供するため、接続コストを最適化できます。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。

を使用すると AWS Transit Gateway、VPN と Direct Connect の接続を多くの VPCs と共有できます。1 時間 AWS Transit Gateway あたりに行う接続数と通過するトラフィック量に対して課金されますが AWS Transit Gateway、管理を簡素化し、必要な VPN 接続数と VIFs 数を減らします。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。オプションで、 AWS Transit Gateway がほとんどの VPCs へのトラフィックパスにある設計を検討できますが、すべてではありません。このアプローチにより、大量のデータを転送する必要があるユースケースの AWS Transit Gateway データ処理料金を回避できます AWS。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 AWS Direct Connect としてインターネット上の AWS S2S VPN をバックアップ/フェイルオーバーパスとして組み合わせることです。技術的に実行可能で費用対効果が高い一方で、このソリューションには技術的な欠点があり (このホワイトペーパーの「信頼性」セクションで説明されています)、管理がより難しい場合があります。 AWS 非常に重要なワークロードや重要なワークロードには、これをお勧めしません。

最後のアプローチは、Amazon VPN インスタンス (複数可) にWANデプロイされたカスタマー管理の Word または SD-EC2 です。これは、S2S VPN と比較して数十から数百のサイトがある場合、 AWS 大規模に安価になる可能性があります。ただし、仮想アプライアンスごとに考慮すべき管理オーバーヘッド、ライセンスコスト、EC2 リソースコストがあります。

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型 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	あり	はい	はい	いいえ	なし
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
Transit Gateway	オプションです。	オプションです。	必須	オプションです。	オプションです。
AWS データ処理コスト	該当なし	のみ AWS Transit Gateway	はい	のみ AWS Transit Gateway	のみ AWS Transit Gateway
上書きできますか AWS Direct Connect ?	あり	はい	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、カスタマー管理VPNおよび SD- に関する考慮事項について説明しますWAN。

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型と 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またはサイトへの接続VPCsを必要とする現在の数と予想される数を教えてください。
- 単一 AWS リージョン または複数のリージョンにVPCsデプロイされていますか？

- 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 にアドバタイズされる予定のルートの数VPCsと AWS 、側から受信される予定のルートの数を教えてください。
- 時間の AWS 経過とともに帯域幅を に増やす必要がありますか？

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。

- ルートの概要を使用して、 にアドバタイズされ、 から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。
- VGW または DXGWを使用してBGPピアリングセッションの数を最小限に抑えます。1 つのBGPセッション AWS Transit Gatewayで複数の に接続できますVPCs。
- WAN 複数のオンプレミスサイト AWS リージョン を一緒に接続する必要がある場合は、クラウドを検討してください。

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。複数のリージョンにVPCsまたがる 1 AWS リージョン つまたは複数の Amazon VPC 内にクラウドリソースをデプロイできます。また AWS 、Amazon S3 や DynamoDB AWS リージョンなどの 1 つまたは複数の にパブリックエンドポイントがある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でのVPC相互通信の要件はありますか？

- オンプレミスから直接 AWS パブリックエンドポイントにアクセスする要件はありますか？
- オンプレミスの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要件はありますか？

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。を相互接続する設計の詳細についてはVPCs、「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 高速化 Site-to-Site VPN – AWS Transit Gateway、単一 AWS リージョン
- AWS DX – DXGW、VGW単一リージョン
- AWS DX – VGW、マルチリージョン、 AWS パブリックピアリングDXGWを使用
- AWS DX – AWS Transit Gateway、マルチリージョン、 AWS パブリックピアリングDXGWを使用
- AWS DX – AWS Transit Gateway、マルチリージョン (3 つ以上) DXGWを使用

AWS 高速化 Site-to-Site VPN – AWS Transit Gateway、単一 AWS リージョン

このモデルは以下で構成されます。

- 単一 AWS リージョン。
- AWS とのマネージド Site-to-SiteVPN接続 AWS Transit Gateway。
- 高速化VPNが有効になりました。

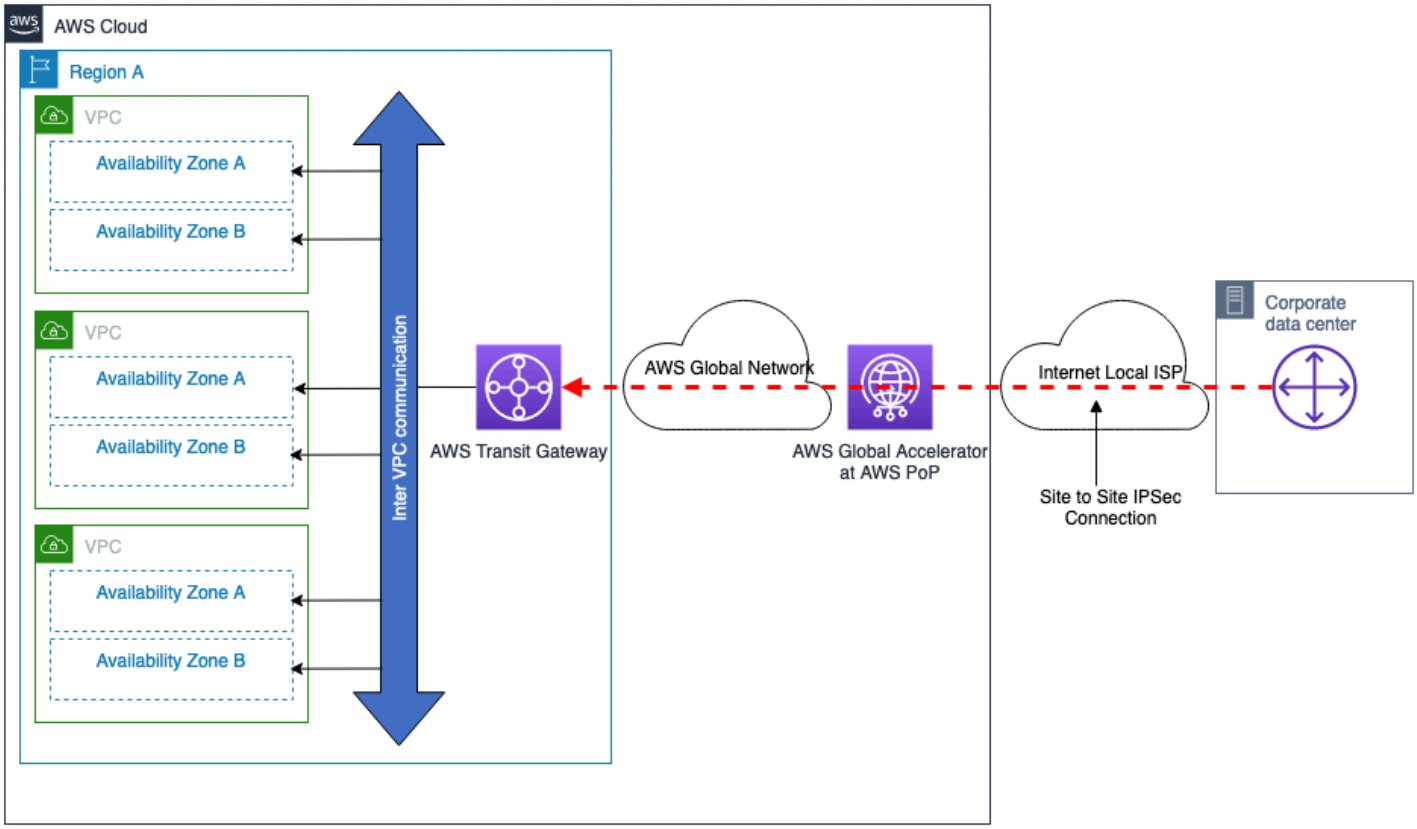

図 4 – AWS 管理対象 VPN – AWS Transit Gateway、単一 AWS リージョン

接続モデル属性:

- 高速VPN接続 を使用して、パブリックインターネット経由で最適化された接続を確立する機能を提供します。 AWS Site-to-Site VPN
- で複数のVPNトンネルを設定することで、より高いVPN接続帯域幅を実現する機能を提供しますECMP。
- 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 () による自動フェイルオーバーを提供しますBGP。
- AWS Transit Gateway に接続されている ではVPCs、接続されているすべての が同じVPN接続VPCsを使用できます。間で目的の通信モデルを制御することもできます。詳細についてはVPCs、「How Transit Gateways Work」を参照してください。
- サードパーティーのセキュリティおよび 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。およびオンプレミスから VPC-to-VPCVPCトラフィックへの一元化されたネットワークセキュリティを参照してください。

スケールの考慮事項:

- 複数のIPsecトンネルがあり、ECMP設定済みの帯域幅は最大 50 Gbps (各トラフィックフローはVPNトンネルあたりの最大帯域幅に制限されます)。
- 1 https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-quotas.htmlつあたり数千 を接続VPCsできます AWS Transit Gateway。
- ルートの数など、他のスケール制限については、Site-to-Site VPNクォータを参照してください。

その他の考慮事項:

- 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 AWS Transit Gateway 処理コストAWS。
- リモートのセキュリティグループは で参照VPCできません AWS Transit Gateway 。ただし、VPCこれはピアリングでサポートされています。

AWS DX – DXGW、VGW単一リージョン

このモデルは以下で構成されます。

- 単一 AWS リージョン。
- 独立した DX ロケーションへのデュアル AWS Direct Connect 接続。
- AWS DXGW VPCsを使用して に直接アタッチされますVGW。
- 通信 AWS Transit Gateway VPC間の のオプションの使用。

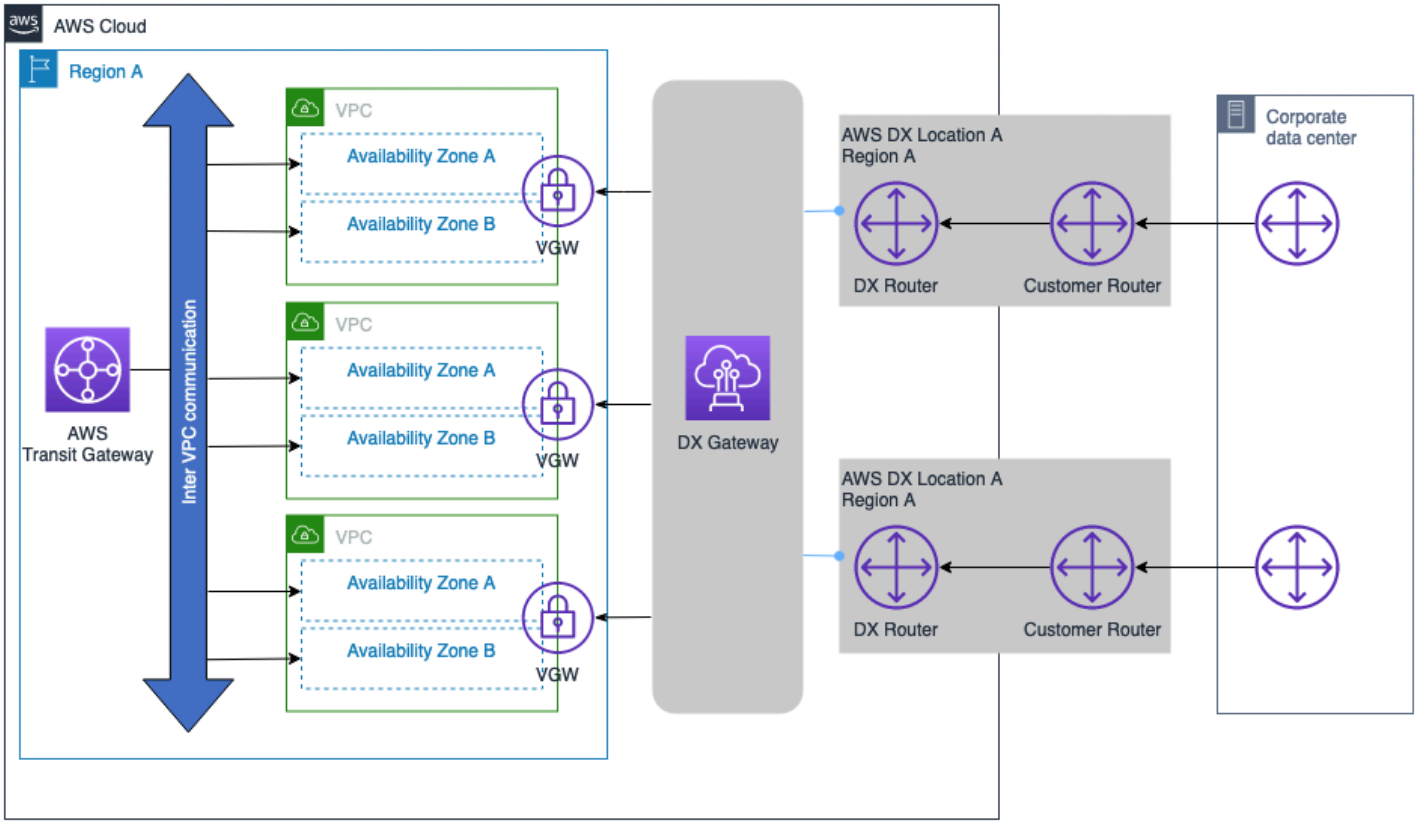

図 5 – AWS DX – DXGWと VGW、シングル AWS リージョン

接続モデル属性:

- 将来、他のリージョンの VPCsおよび DX 接続に接続できるようになります。
- 動的ルーティング () による自動フェイルオーバーを提供しますBGP。
- AWS Transit Gateway を使用すると、 間で目的の通信モデルを制御できますVPCs。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:

サポートされているプレフィックスの数、DX 接続タイプ (専用、ホスト) VIFsあたりの数など、他のスケール制限の詳細については、AWS Direct Connect 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:

- プライベートのBGPセッションVIFは、 IPv4と に対してそれぞれ最大 100 個のルートをアドバタイズできますIPv6。

- 1 回のBGPセッションDXGWで 1 人あたり最大 20 個まで接続VPCsできます。20 個以上VPCsが必要な場合は、大規模な接続を容易にするために追加することも、Transit Gateway 統合の使用を検討DXGWsすることもできます。
- 必要に応じて AWS Direct Connectを追加できます。

その他の考慮事項:

- とオンプレミスネットワーク間の AWS データ転送には AWS Transit Gateway 、関連する処理コストは発生しません。
- リモートのセキュリティグループは、 で参照VPCすることはできません AWS Transit Gateway （VPCピアリングが必要です）。
- VPC ピアリングはVPCs、 間の通信を容易に AWS Transit Gateway するために の代わりに使用できますが、これにより、大規模な多数のVPC point-to-pointピアリングを構築および管理するための運用の複雑さが増します。
- 通信VPCが不要の場合、この接続モデルではVPCピアリング AWS Transit Gateway も必要ありません。

AWS DX – VGW、マルチリージョン、 AWS パブリックピアリングDXGWを使用

このモデルは以下で構成されます。

- へのデュアル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 ロケーションへのデュアル AWS Direct Connect 接続。
- AWS DXGW VPCsを使用して 10 個以上に直接アタッチされVGW、 VPCsを使用して最大 20 個までアタッチされますVGW。
- リージョンVPC間およびリージョン間の通信 AWS Transit Gateway のための のオプションの使用。

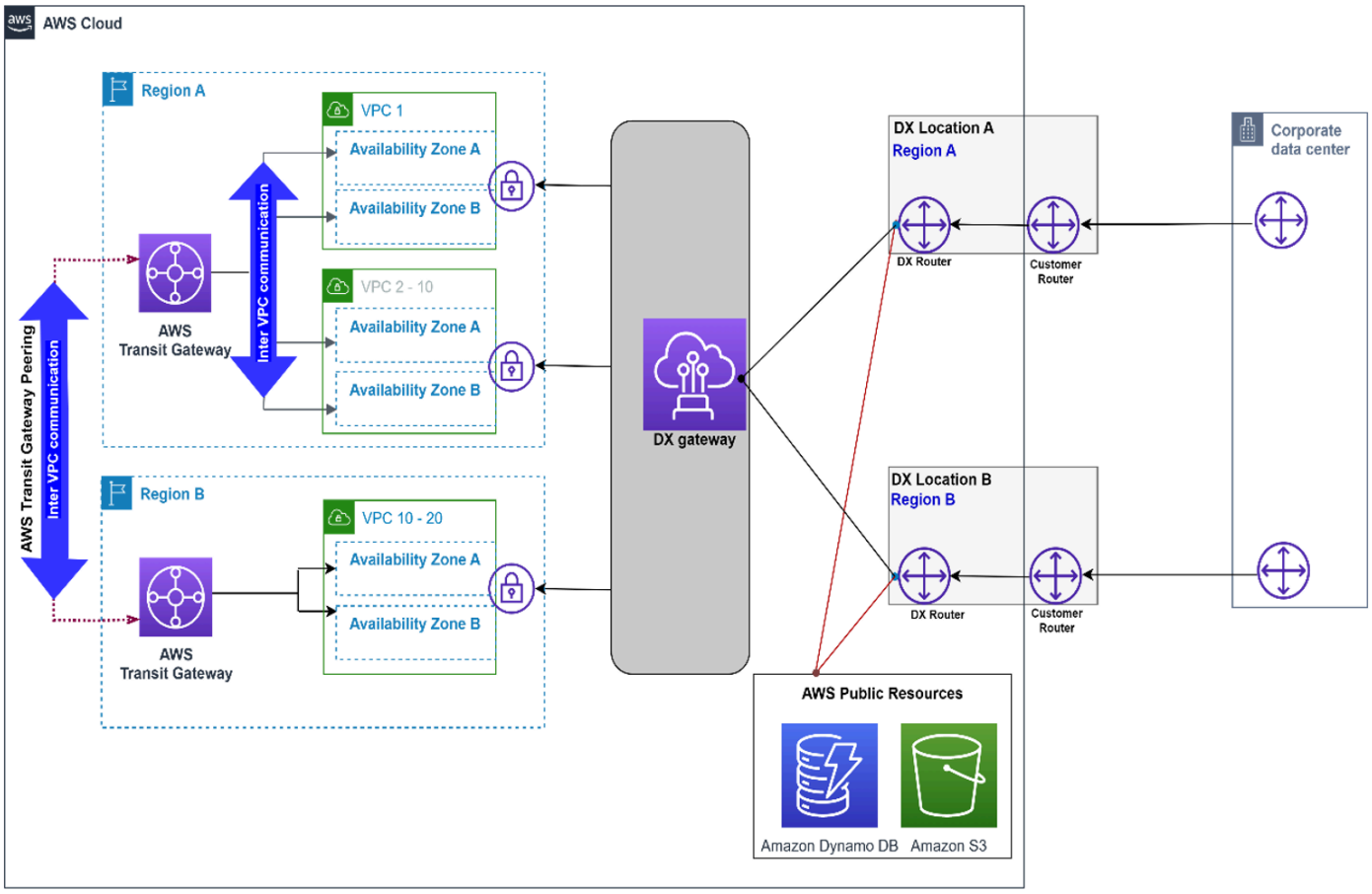

図 6 – AWS DX – DXGW VGW、マルチリージョン、パブリック VIF

接続モデル属性:

- AWS DXGW VPCsを使用してVGW最大 20 VPCs個を使用して 10 個を超える に直接アタッチされますVGW。
- AWS DX パブリックVIFは、 AWS DX 接続を介して Amazon S3 などの AWS 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。
- 今後、他のリージョンの VPCs および DX 接続に接続できるようになります。
- および Transit Gateway ピアリングによって促進されるリージョン間VPC AWS Transit Gateway およびリージョン間のVPC通信。

スケールの考慮事項:

サポートされているプレフィックスの数、DX 接続タイプ (専用、ホスト型) VIFsあたりの数など、他のスケール制限の詳細については、AWS Direct Connect 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:

- プライベートのBGPセッションでは、 IPv4と に対してそれぞれ最大 100 のルートをアドバタイズVIFできますIPv6。
- 各プライベート では 1 回のBGPセッションDXGWで 1 人あたり最大 20 個VIF、 VIFsあたり最大 30 個のプライベート に接続VPCsできますDXGW。
- 必要に応じて AWS Direct Connectを追加できます。

その他の考慮事項:

- とオンプレミスネットワーク間の AWS データ転送には AWS Transit Gateway 、関連する処理コストは発生しません。
- リモートのセキュリティグループは AWS Transit Gateway （ VPCピアリングが必要) によって参照VPCできません。
- VPC ピアリングは、 間の通信を容易に AWS Transit Gateway するために の代わりに使用できますVPCsが、これにより、大規模な多数のVPC point-to-pointピアリングを構築および管理するための運用の複雑さが増します。
- 通信VPCが不要の場合、この接続モデルではVPCピアリング AWS Transit Gateway も必要ありません。

AWS DX – AWS Transit Gateway、マルチリージョン、 AWS パブリックピアリング DXGWを使用

このモデルは以下で構成されます。

- 複数の AWS リージョン。
- 独立した DX ロケーションへのデュアル AWS Direct Connect 接続。
- へのデュアル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VPCsあたりの の高スケール。

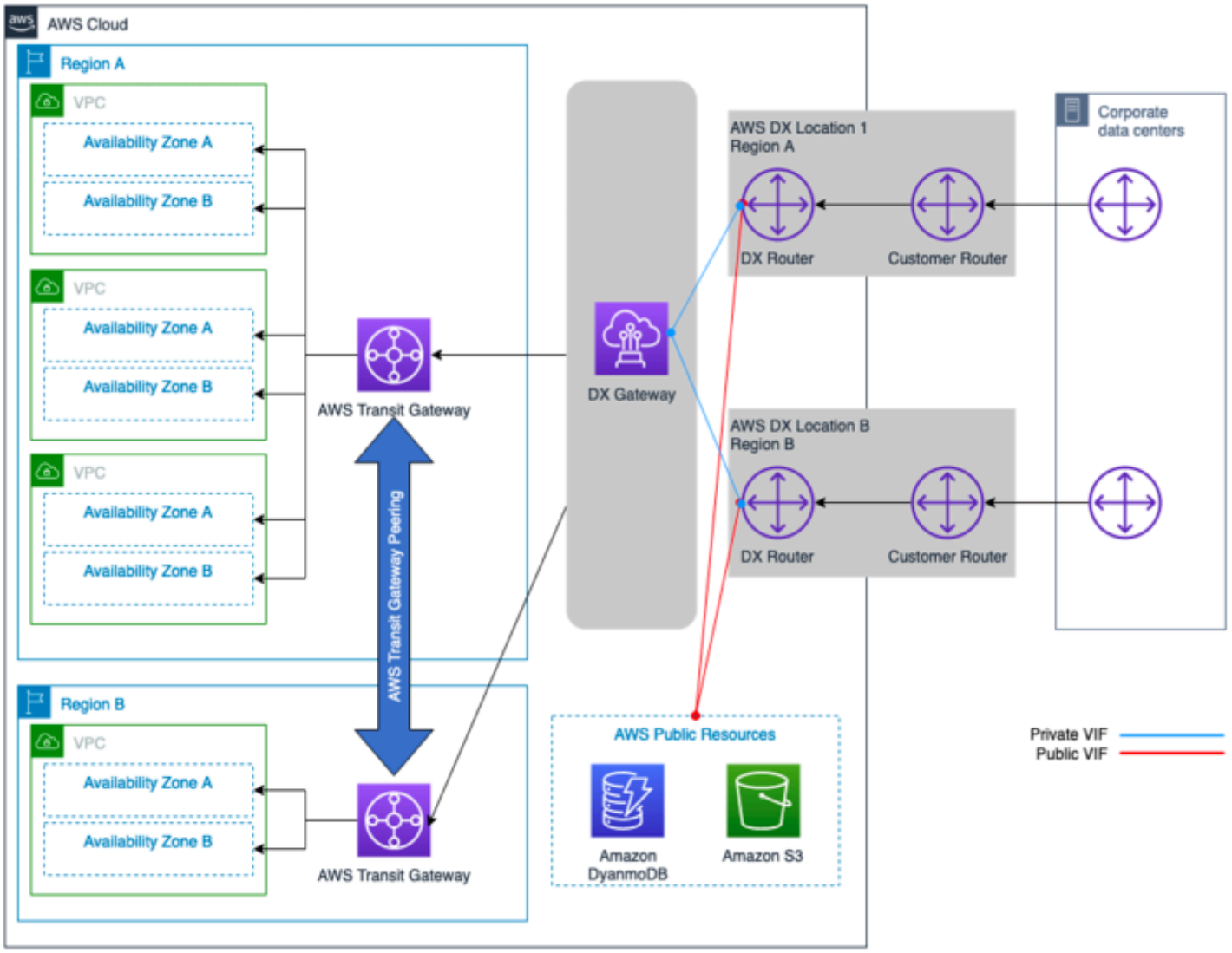

図 7 – AWS DX – DXGW AWS Transit Gateway、マルチリージョン、パブリック AWS VIF

接続モデル属性:

- AWS DX パブリックVIFは、 AWS DX 接続を介して S3 などの AWS 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。
- 今後、他のリージョンで VPCs や DX 接続に接続できるようになります。
- AWS Transit Gateway に接続するとVPCs、 間でメッシュの完全接続または部分接続を実現できますVPCs。
- AWS Transit Gateway ピアリングによりリージョン間VPCおよびリージョン間のVPC通信が容易になります。

- サードパーティーのセキュリティアプライアンスと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。「」を参照してください。 およびオンプレミスから VPC-to-VPCVPCトラフィックへの一元的なネットワークセキュリティ。

スケールの考慮事項:

- との間のルート数は AWS Transit Gateway 、トランジットでサポートされているルートの最大数に制限されます VIF (インバウンドとアウトバウンドの番号は異なります)。スケール制限とサポートされているルート数と の詳細については、AWS Direct Connect クォータを参照してくださいVIFs。
- 1 回のBGPセッション AWS Transit Gateway で VPCs1 人あたり最大数千 までスケールできます。
- AWS DX VIFあたりの単一トランジット。
- 必要に応じて、追加の AWS DX 接続を追加できます。

その他の考慮事項:

- AWS とオンプレミスサイト間のデータ転送には、追加の AWS Transit Gateway 処理コストが発生します。
- リモートのセキュリティグループは AWS Transit Gateway （ VPCピアリングが必要) によって参照VPCできません。
- VPC ピアリングは、 間の通信を容易に AWS Transit Gateway するために の代わりに使用できますVPCsが、これにより、大規模な多数のVPC point-to-pointピアリングを構築および管理するための運用の複雑さが増します。

AWS DX – AWS Transit Gateway、マルチリージョン (3 つ以上) DXGWを使用

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 ロケーションへのデュアル AWS Direct Connect 接続。
- AWS DXGW と AWS Transit Gateway。
- リージョンVPCsあたりの の高スケール。

- 間のピアリングの完全なメッシュ AWS Transit Gateway。

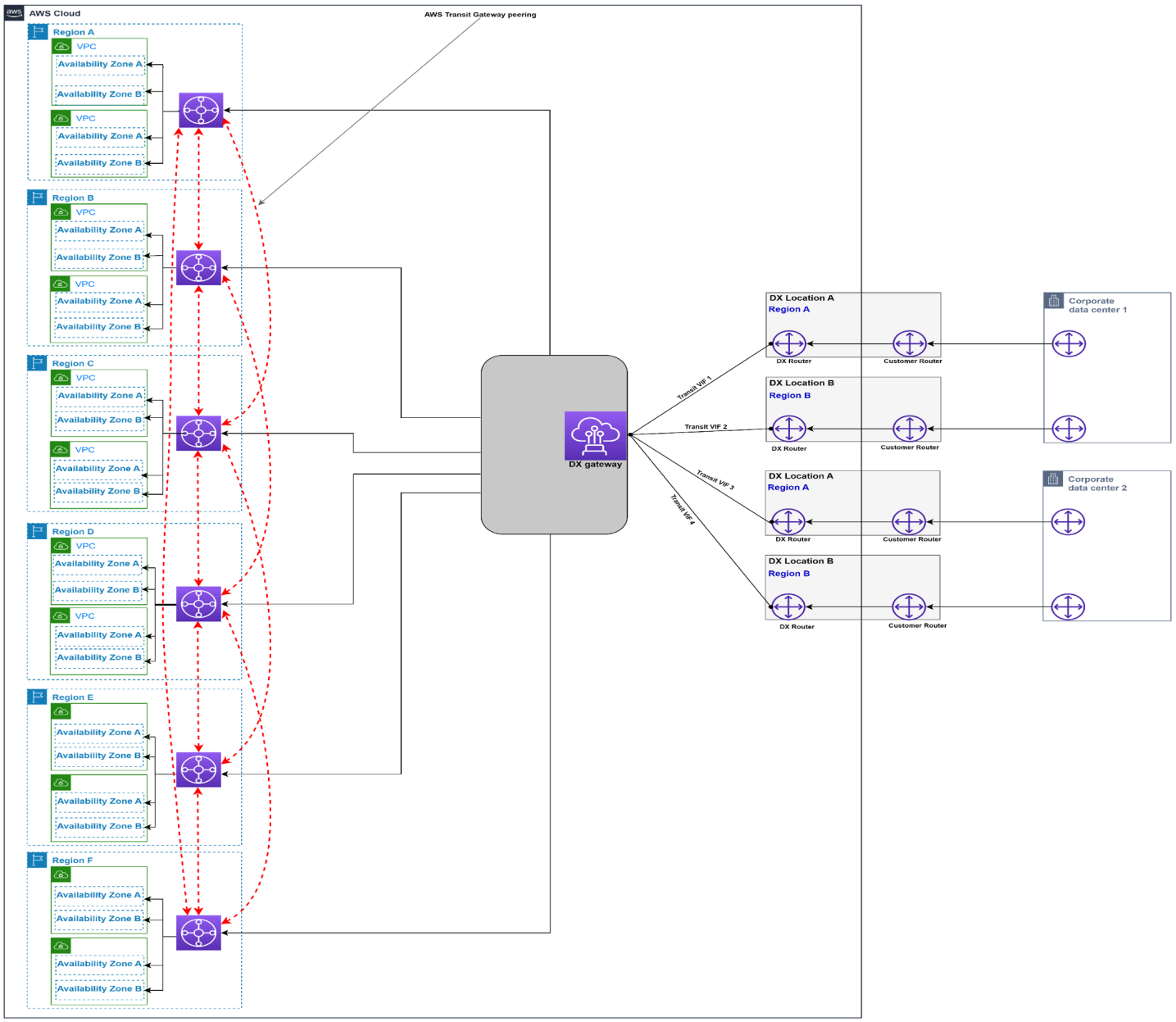

図 8 – AWS DX – AWS Transit Gateway、マルチリージョン (3 つ以上) DXGWを使用

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、 AWS DX 接続を介して S3 などの AWS 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。

- 今後、他のリージョンの VPCs および DX 接続に接続できるようになります。
- AWS Transit Gateway に接続するとVPCs、 間でメッシュの完全接続または部分接続を実現できますVPCs。
- リージョン間のVPC通信は AWS Transit Gateway ピアリングによって促進されます。
- サードパーティーのセキュリティアプライアンスと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。「」を参照してください。 およびオンプレミスから VPC-to-VPCVPCトラフィックへの一元的なネットワークセキュリティ。

スケールの考慮事項:

- との間のルート数は AWS Transit Gateway 、トランジットでサポートされているルートの最大数に制限されます VIF (インバウンドとアウトバウンドの番号は異なります)。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。
- 1 回のBGPセッション AWS Transit Gateway で VPCs 1 回あたり数千 までスケールできます DXGW (プロビジョニングされた AWS DX 接続によって提供されるパフォーマンスで十分であると仮定します)。
- 1 つあたり最大 6 AWS Transit Gatewayつの を接続できますDXGW。
- 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 DXGWsリージョンが必要です。
- AWS DX VIFあたりの単一トランジット。
- 必要に応じて、追加の AWS DX 接続を追加できます。

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、追加の AWS Transit Gateway 処理コストが発生します AWS。
- リモートのセキュリティグループは AWS Transit Gateway （ VPCピアリングが必要) によって参照VPCできません。
- VPC ピアリングはVPCs、 間の通信を容易に AWS Transit Gateway するために の代わりに使用できますが、これにより、大規模な多数のVPC point-to-pointピアリングを構築および管理するための運用の複雑さが増します。

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。

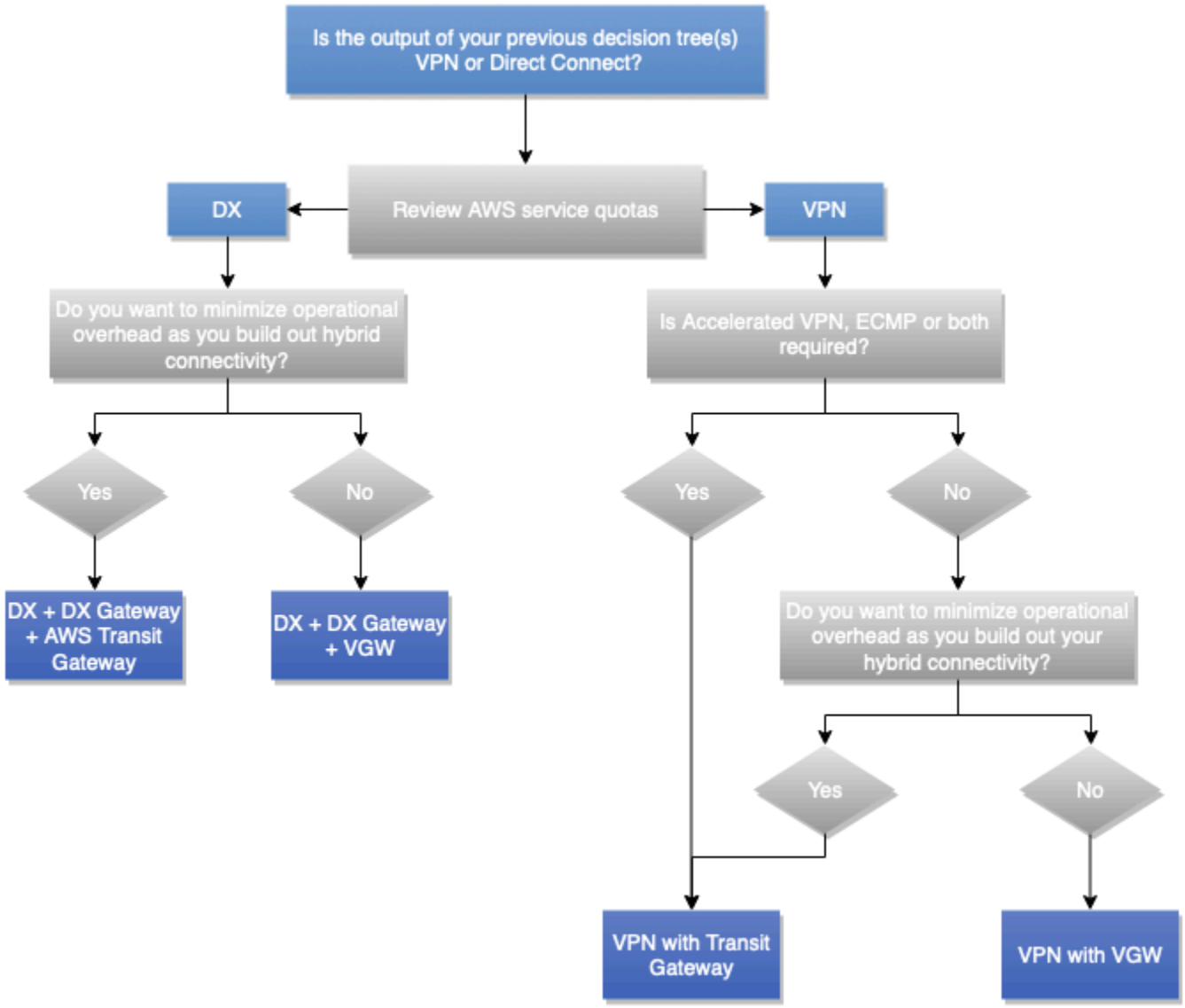

図 9 - スケーラビリティと通信モデルの決定木

> **Note**
>
> 選択した接続タイプが の場合VPN、通常はパフォーマンスを考慮して、VPN終了ポイントが AWS VGW か AWS Transit Gateway AWS S2S VPN接続かを決定する必要があります。まだ作成されていない場合は、 間の必要な通信モデルVPCとVPN、接続への接続VPCに必要な数 (複数可) を考慮して、意思決定に役立てることができます。

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使用して信頼性を測定する方法の詳細については、 AWS Well-Architected フレームワーク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、全体的なソリューションやアプリケーションの可用性とは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。

- オンプレミス AWS リソースと通信できない場合、リソースは引き続き運用できますか？ 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。
- 分散サービス拒否 (DDoS) イベントに対する脆弱性は何ですか？

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 Connect 設計に対する高いAWS Direct Connect 耐障害性を確保するためのベストプラクティスを説明するため、耐障害性に関する推奨事項を参照することをお勧めします。 AWS

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： 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間の冗長性、DX ロケーション、デバイス電源、ファイバーパス AWS リージョン、オペレーティングシステムなど、ハイブリッドネットワーク接続パスの単一障害点を排除することを目指します。このホワイトペーパーの目的と範囲について、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、 AWS リージョン （マルチリージョンアーキテクチャの場合) に焦点を当てています。
- 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。リンクにはデッドピア検出 (DPD) 、VPNリンクには双方向転送検出 (BFD) を使用して、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時間は、非常に短い場合 (これらの接続が常にアクティブである場合) 、短い時間枠 (事前設定済みのVPN接続を有効にする必要がある場合) 、または長い場合 (物理リソースを移動する必要がある場合、または新しいリソースを設定する必要がある場合) です。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。AWS Direct Connect ルーティングのセクションと ではBGP、トラフィックフロー (コミュニティ、BGPローカル設定、AS パス長) に影響を与えるためのいくつかのトラフィックエンジニアリングオプションについて説明します。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、各 AWS ネットワークコンポーネントがルートの評価と選択の観点から IP ルーティングをどのように処理するか、およびルートの選択に影響を与える可能性のあるメカニズムを十分に理解する必要があります。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、「Transit Gateway Route Evaluation Order 」、Site-to-Site VPN「Route Priority 」、および必要に応じて Direct Connect Routing とBGP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、適用すると特定のルートエントリに展開されます。

より具体的なルートを含むデュアル Site-to-SiteVPN接続の例

このシナリオは、インターネット経由で への冗長な単一の AWS リージョン VPN接続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 AWS Transit Gateway。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。

- 回復力のあるハイブリッド接続: 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) を使用して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して接続障害の検出を高速化します。
- パフォーマンス効率: 両方のVPN接続ECMPで を設定することで、 AWS Transit Gateway VPN接続帯域幅全体を最大化できます。または、サイト概要ルートとともに異なる、より具体的なルートをアドバタイズすることで、2 つのVPN接続間で負荷を独立的に管理できます。

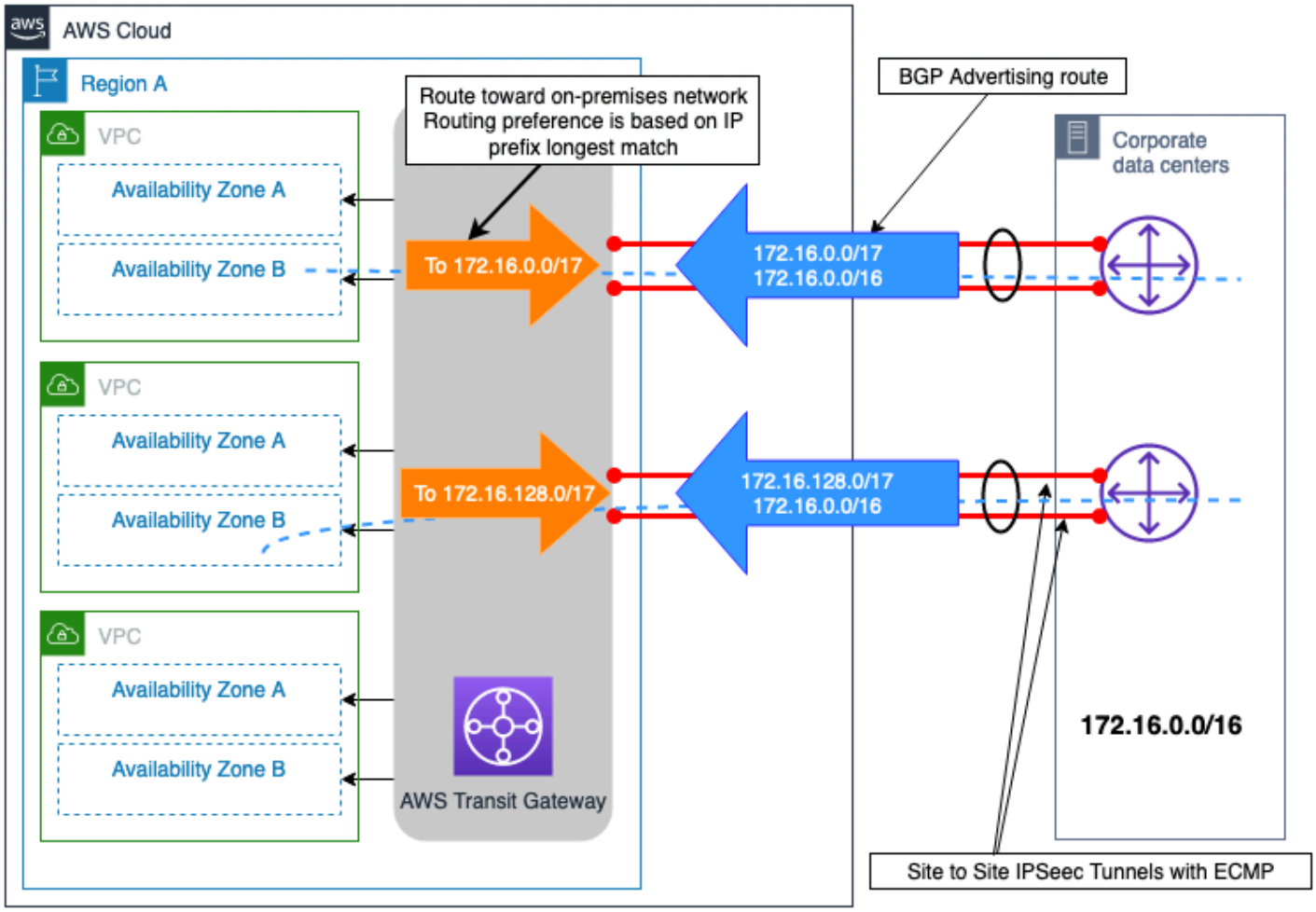

図 10 – より具体的なルートを含むデュアル Site-to-SiteVPN接続の例

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 に示すシナリオは、異なる地理的リージョンにあり、 と AWS を使用して最大耐障害性接続モデル (AWS Direct Connect「耐障害性に関する推奨事項」に記載) AWS Direct Connect DXGW を使用して に接続されている 2 つのオンプレミスデータセンターサイトを示していますVGW。これらの 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相互接続されます。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 にアドバタイズされたルートに関連付けることで AWS DXGW、エグレスパスの選択を横から AWS DXGW行うことができます。これらのコミュニティ属性は、アドバタイズされたルートに割り当てられた AWSのBGPローカル設定属性を制御します。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 レベルでの接続の信頼性を最大化するために、各 AWS DX 接続ペアは、各オンプレミスサイトと 間のデータ転送に両方を同時に利用できるECMPように を設定します AWS。

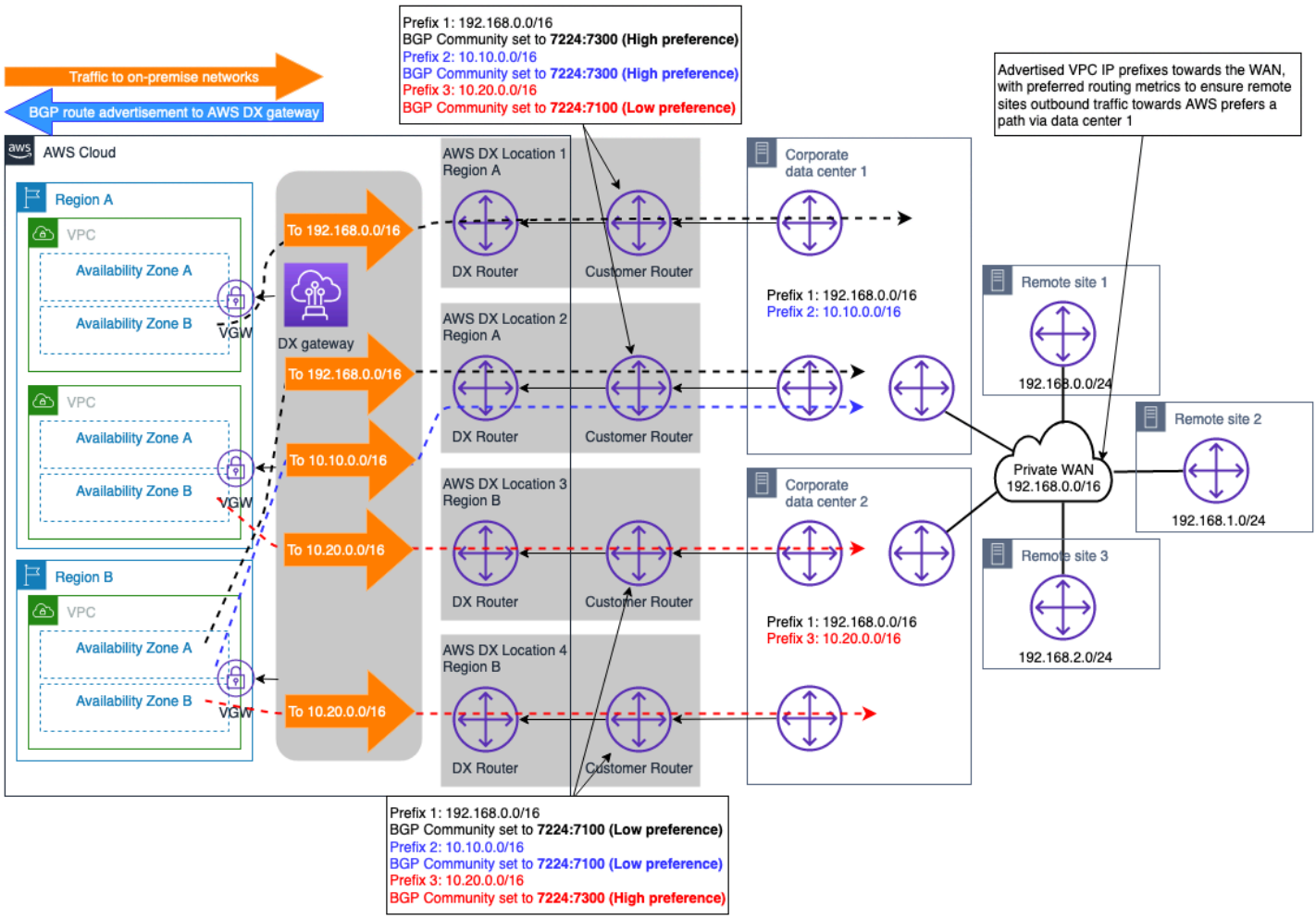

図 11 – 複数の DX 接続を使用するデュアルオンプレミスサイトの例

この設計では、オンプレミスネットワーク (アドバタイズされたプレフィックスの長さとBGPコミュニティが同じ) 宛てのトラフィックフローは、 を使用してサイトあたりのデュアル DX 接続に分散されますECMP。ただし、DX 接続全体で が必要ECMPでない場合は、先に説明し、Routing ポリシーとBGPコミュニティ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 接続レベルでパス選択をさらに設計できます。

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、これらのデバイスは、トラフィックフローが 1 つの DX リンクを経由し、同じデータセンターサイト内の別の DX リンク (で使用されているリンクの両方ECMP) から送信されるように設定する必要があります。

VPN AWS DX 接続へのバックアップとしての接続の例

VPN は、接続への AWS Direct Connect バックアップネットワーク接続を提供するように選択できます。通常、このタイプの接続モデルは、インターネットを介した不確定なパフォーマンスによりハイブリッド接続ソリューション全体の信頼性が低く、パブリックインターネットを介した接続で取得SLAできるものがないため、コストによって駆動されます。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。この設計では、 VPN と DX 接続の両方が で終了する場合 AWS Transit Gateway、VPN接続は に接続された DX 接続を介してアドバタイズできるルートと比較して、より多くのルートをアドバタイズできるという重要な考慮事項があります 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オプションは、VPN接続から受信したルートに対してカスタマーゲートウェイデバイス (CGW) で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入れることです。

注: で概要ルートを作成するには AWS Transit Gateway、概要がより特定のルートに沿って送信されるように、 AWS Transit Gateway ルートテーブル内の任意のアタッチメントへの静的ルートを指定する必要があります。

AWS Transit Gateway ルーティングテーブルの観点からは、オンプレミスプレフィックスのルートはVPN、同じプレフィックス長の AWS DX 接続 (経由DXGW) と の両方から受信されます。のルート優先度ロジック AWS Transit Gatewayに従って、Direct Connect 経由で受信されたルートは、 経由で Site-to-Site受信されたルートよりも優先されるためVPN、 経由のパスがオンプレミスネットワーク (複数可) に到達するのが優先 AWS Direct Connect されます。

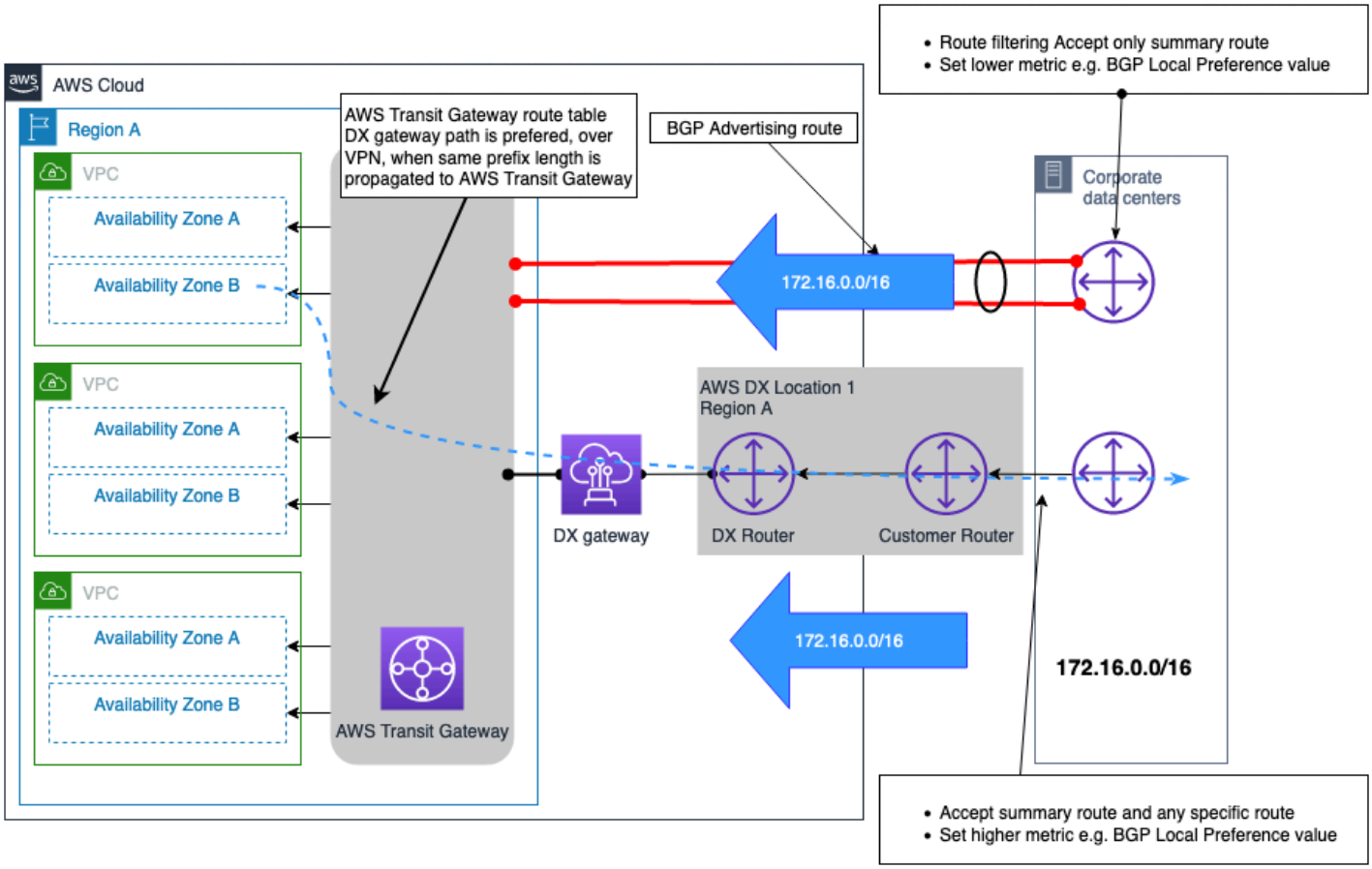

図 12 – AWS DX VPN接続へのバックアップとしての接続の例

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。

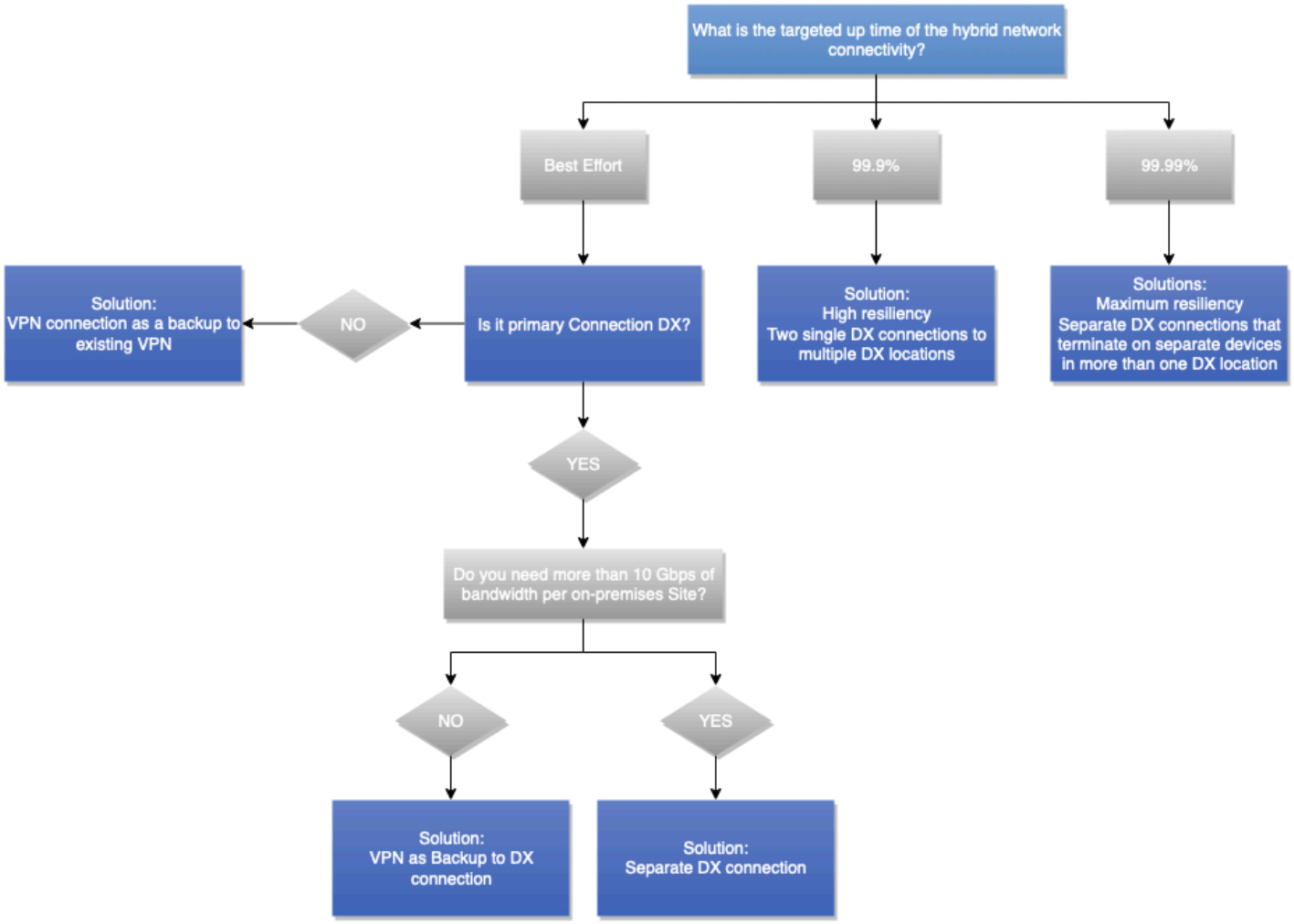

図 13 - 信頼性の決定木

カスタマーマネージドVPN型と 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。一部のお客様は、プライベート を構築して運用するのではなく、インターネットWAN上に仮想 を構築することを選択しますWAN。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WANして、この仮想を一元的に迅速にプロビジョニングおよび管理できます。他のお客様は、従来のセルフマネージドサイトをサイト に採用することを選択しますVPNs。

設計上の決定への影響

SD WANとカスタマー管理は、インターネットまたは 経由で実行VPNsできます AWS Direct Connect。SD-WAN (またはソフトウェア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考慮事項は、ここで適用できます。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、 経由で構築されている場合と同じ信頼性は得られません AWS Direct Connect。

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 終了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 は SD-WAN と の統合を推奨し AWS Transit Gateway、統合をサポートする AWS Transit Gateway ベンダーのリストを発行します。 AWS は SD-WAN サイトのハブまたはスポークサイトとして機能します。 AWS バックボーンを使用して、 にデプロイされたさまざまな SD WANハブ AWS を、高い信頼性とパフォーマンスを備えたネットワークに接続できます。SD WANソリューションは、1 つの管理ペインで、利用可能なパス、追加のモニタリング、オブザーバビリティ機能による自動フェイルオーバーをサポートします。自動設定と自動化を幅広く使用すると、従来の と比較して迅速なプロビジョニングと可視性が可能になりますWANs。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を選択できます。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セルフマネージドソリューションVPNまたは SD-WAN ソリューションを選択する場合、その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 にデプロイできる多くのVPN仮想アプライアンスが含まれていますEC2。 AWS では、 AWS マネージド S2S から開始VPNし、要件を満たしていない場合は他のオプションを調べ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。

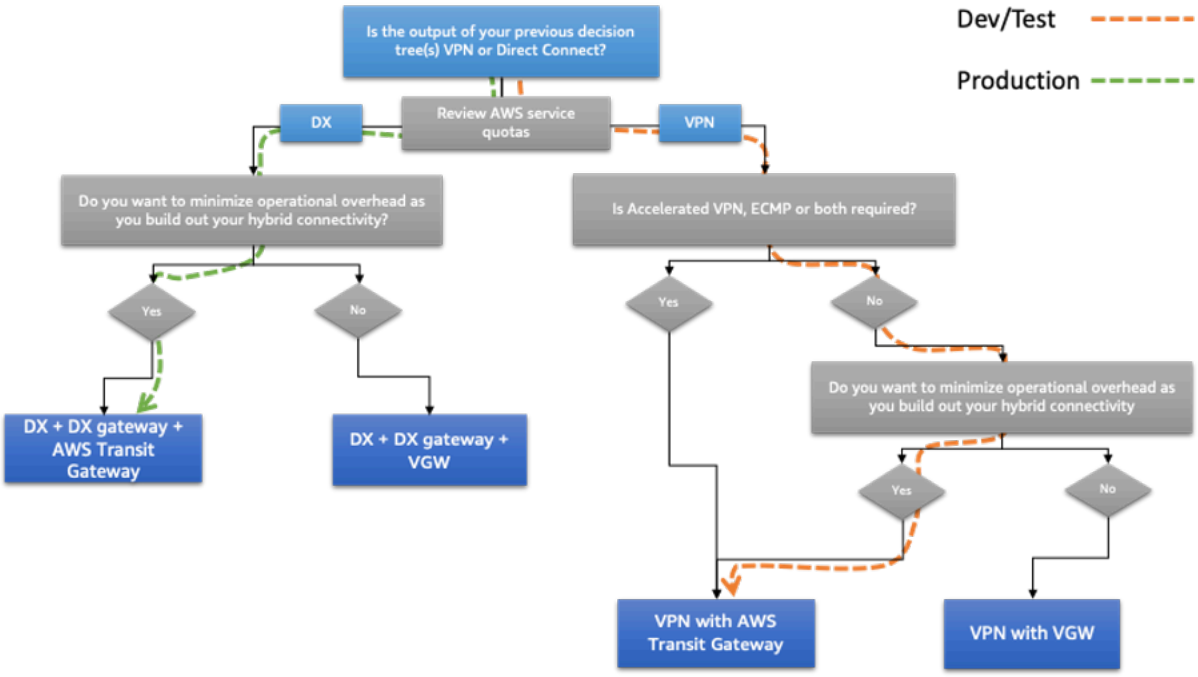

図 14 – Example Corp. Automotive の接続設計の決定木

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。

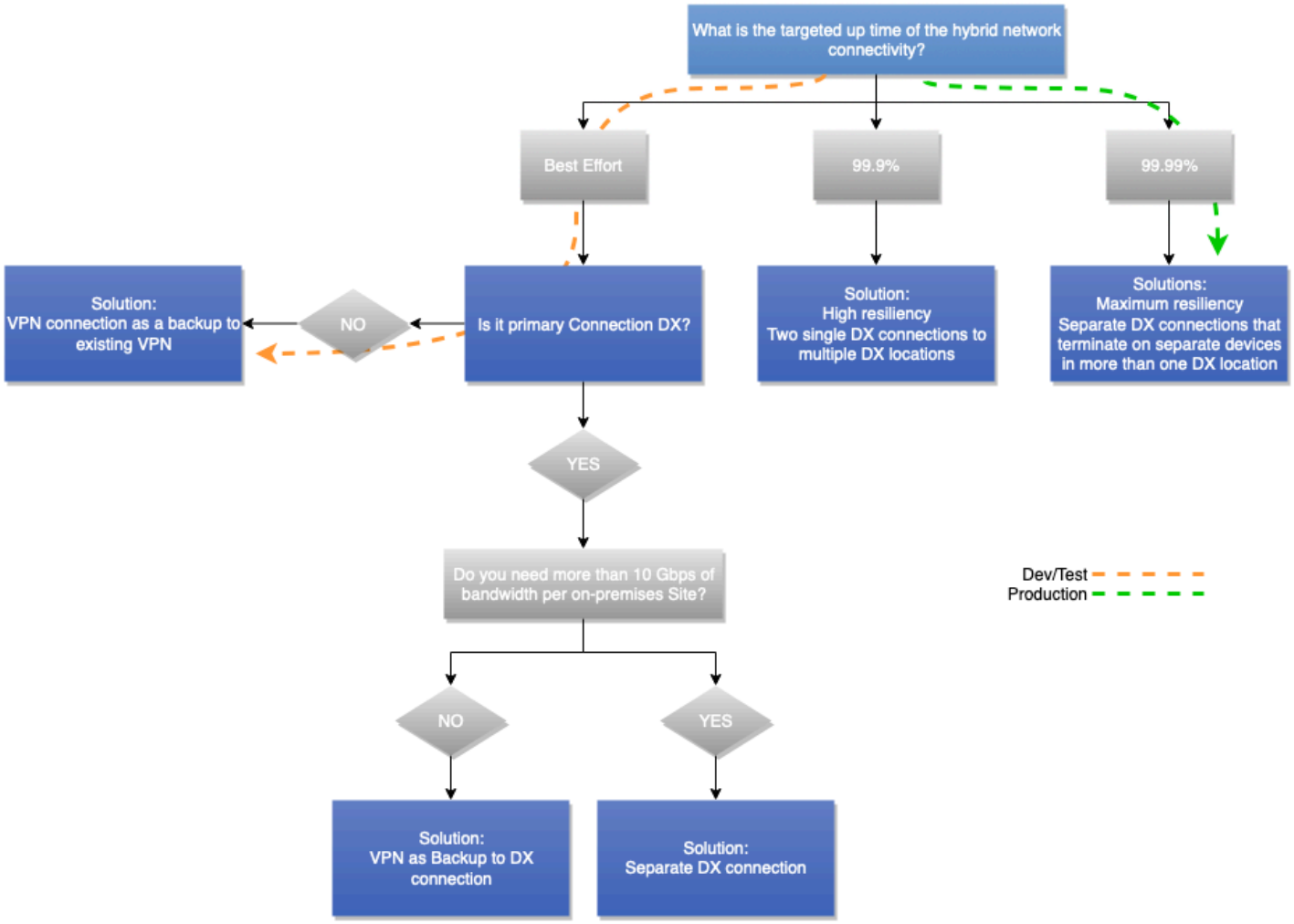

図 15 - Example Corp. Automotive の信頼性の決定木

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。

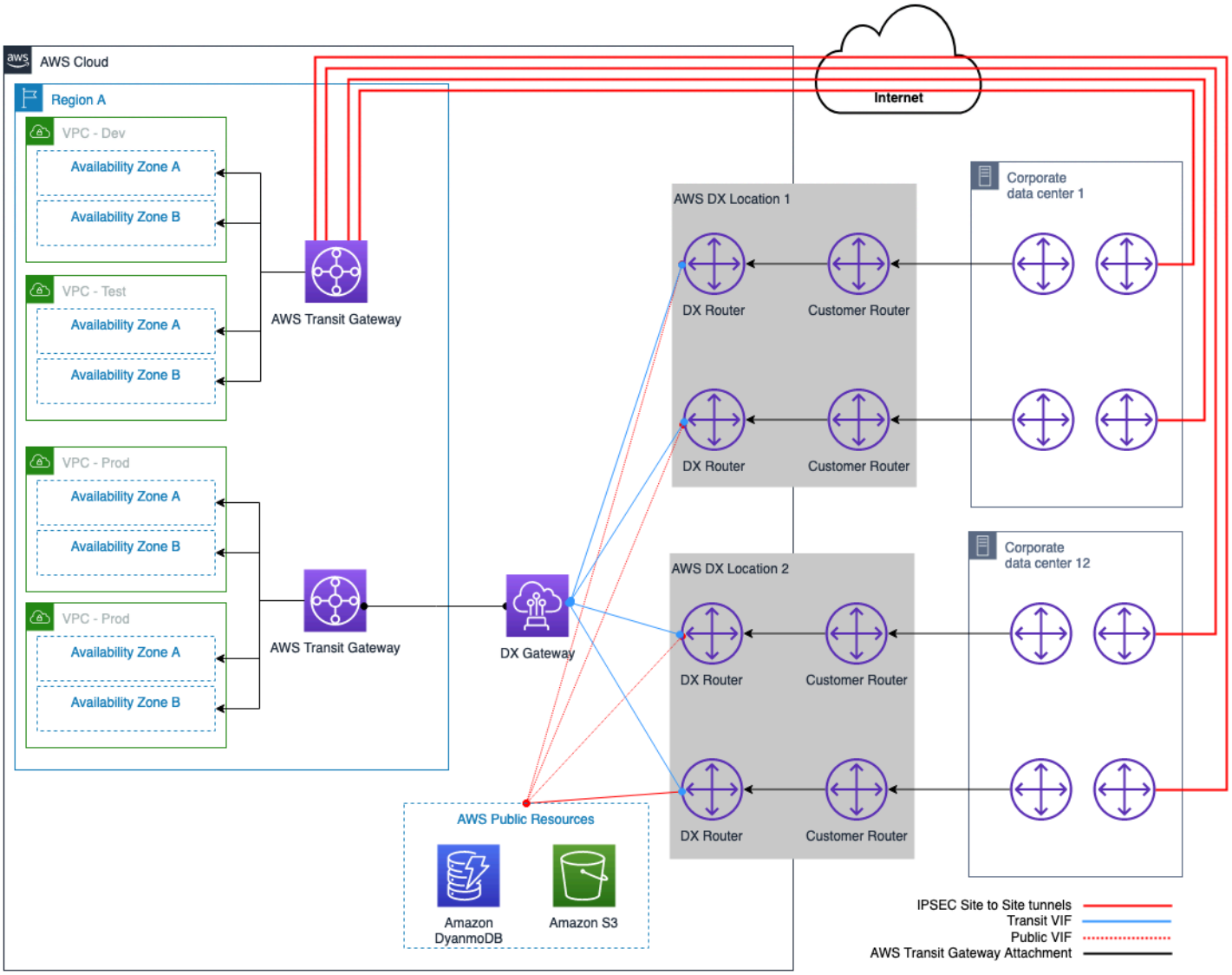

図 16 - Example Corp. Automotive が選択したハイブリッド接続モデル

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。