
aws
SUMMIT
TOKYO | APRIL 20-21, 2023

AWS-03

AWS ネットワーク管理を ステップアップしたい方に送る、次の一手

菊地 信明
アマゾン ウェブ サービス ジャパン合同会社
技術統括本部ネットワークソリューション部
シニアソリューションアーキテクト ネットワークスペシャリスト

自己紹介

名前： 菊地 信明（きくち のぶあき）

所属： アマゾンウェブサービスジャパン合同会社
ネットワークソリューション部
シニアソリューションアーキテクト
ネットワークスペシャリスト

経歴： 通信キャリアにてホスティングやマネージドFWのサポートを経験
鉄道系IT子会社にて設計・開発・運用に従事
AWSサポートにてDirect Connect/VPNのサポートを対応

好きなAWSサービス：
AWS Direct Connect, AWS Transit Gateway, Amazon Route 53

AWSネットワークを活用いただいてますか？

- 物理的な制約にとらわれず、使いたいときにすぐにネットワークを設定できるクラウドならではの俊敏性

Amazon Virtual Private Cloud (VPC)

AWS Client VPN

- 最大キャパシティを予測する必要が無い、AWSマネージドサービス

Elastic Load Balancer (ELB)

AWS Transit Gateway (TGW)

このセッションの対象者

以下のような課題をお持ちの方を対象としています

- AWSクラウドにシステムを構築したけど、インターネット経由でのアクセスに不安を感じている
- VPC上のシステムと社内システムを連携させたいけど、プライベートIPで通信させるサービスはどれを利用すればよい？
- システムごとにVPCを作っているけど、関連性のあるVPCへ連携するのがたいへん

このセッションでお伝えしたいこと

このセッションを受講された方が、以下のようなことを学んでいただけるようお話しします

- オンプレミスとAWSクラウドを閉域網でつなぐときの考慮ポイントを知る
- AWS側のゲートウェイとなるサービスとその特徴を理解する
- クラウドネットワークの拡張時に困らない設計を把握する

アジェンダ

1. オンプレミスとVPCの接続パターン
- A 拠点からインターネット経由でVPCに接続
- B 複数拠点からセキュアにVPCに接続
- C 要件が異なる拠点からVPCに接続
- D 拠点からシステム毎に異なるVPCに接続

2. VPCが増えてきた時の対応方法
- 2-1. AWS Transit Gatewayを使うには？
- 2-2. “オンプレミス通信”と“VPC間通信”を分けて考える
- 2-3. 構成比較：プライベートVIF + DXGW or トランジットVIF + TGW
- 2-4. より使いやすくなったトランジットVIF

Appendix
- A-1. AWS Transit Gateway構成への移行手順
- A-2. AWSネットワーク関連の情報

1. オンプレミスとVPCの接続パターン

オンプレミスとVPCの接続パターン

A 拠点からインターネット経由でVPCに接続

B 複数拠点からセキュアにVPCに接続

C 要件が異なる拠点からVPCに接続

D 拠点からシステム毎に異なるVPCに接続

皆さんがAWSクラウドを活用するフェーズや要件に合わせて、これらから選択・組み合わせが可能です。

A 拠点からインターネット経由でVPCに接続

インターネットゲートウェイ 

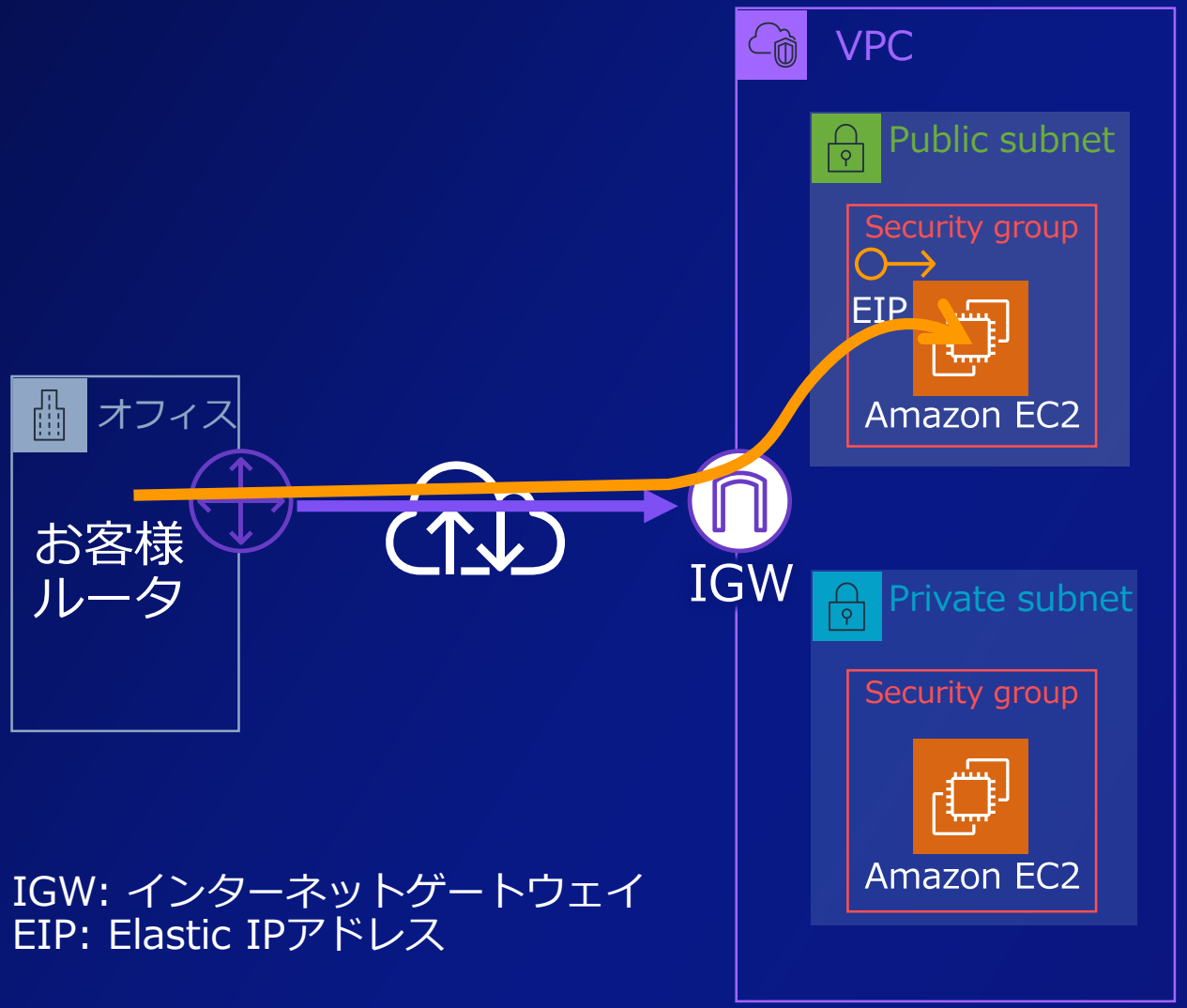
＋

Elastic IPアドレス

Elastic Load Balancing 

AWS アーキテクチャアイコン
https://aws.amazon.com/jp/architecture/icons/

A 拠点からインターネット経由でVPCに接続



IGW: インターネットゲートウェイ
EIP: Elastic IPアドレス

ユースケース

- すぐにVPC上でシステムを構築
- ID/Password入力フォームが暗号化されていればOK

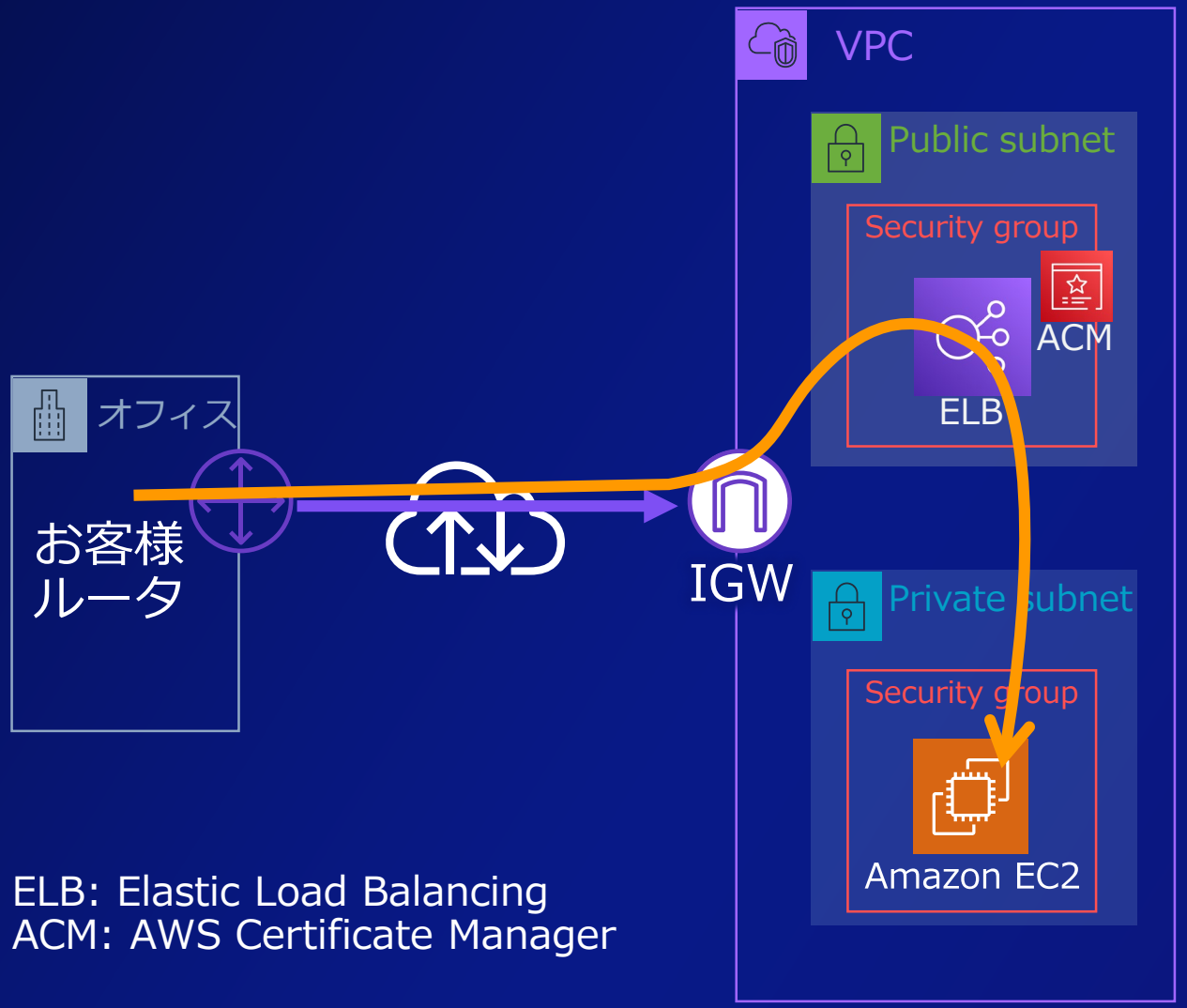
メリット

- 安価でどこからでも接続可能

ポイント

- パブリックサブネットは最低限に
- Elastic IPアドレスで接続先IPを固定化
- セキュリティグループを設定
- アプリケーションで暗号化

A 拠点からインターネット経由でVPCに接続(ELB)



ELB: Elastic Load Balancing
ACM: AWS Certificate Manager

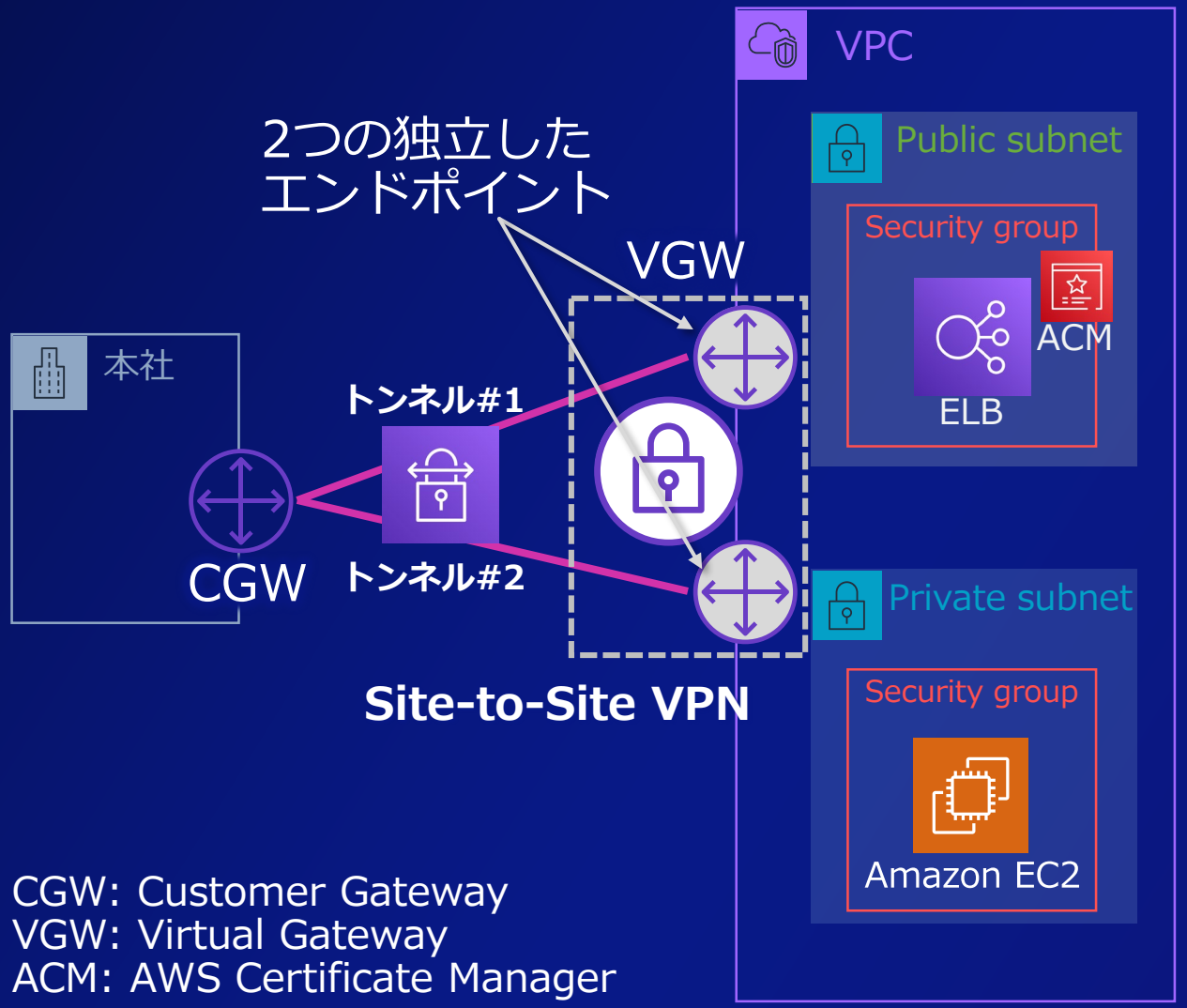
ポイント

- 外部からアクセスさせるパブリックサブネットには、AWSによるマネージドサービスのロードバランサーのみを配置
- AWS Certificate Managerで証明書を発行し、SSL/TLSに対応
- 実際にアプリケーションが稼働するサーバーは、プライベートサブネットで安全に稼働

B 複数拠点からセキュアにVPCに接続

AWS Site-to-Site VPN

AWS Site-to-Site VPN

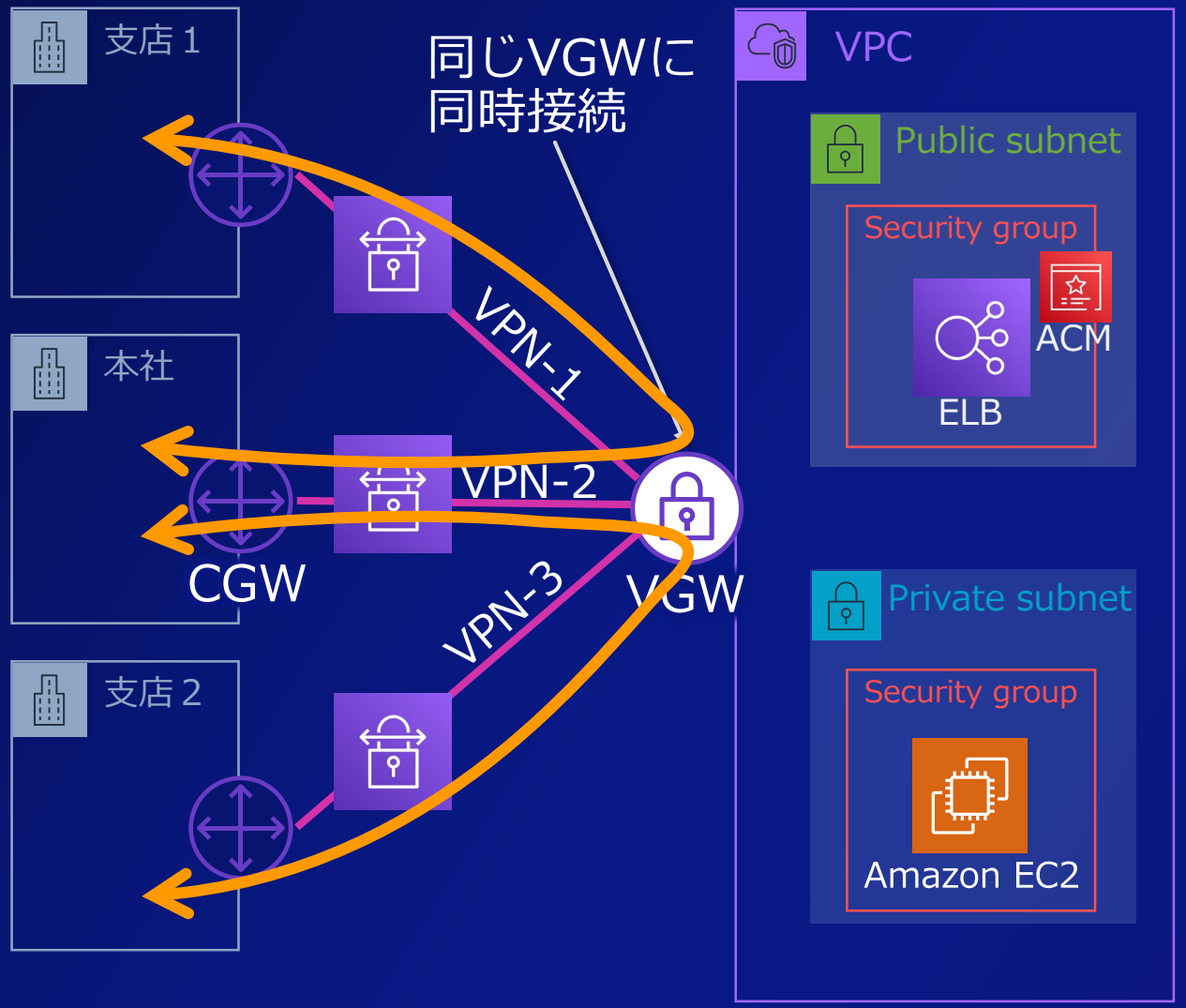


CGW: Customer Gateway
VGW: Virtual Gateway
ACM: AWS Certificate Manager

ポイント

- オンプレミスにパブリックIPアドレスを持つ、IPsec対応のネットワーク機器
- VGW（仮想プライベートゲートウェイ）はそれぞれ別のパブリックIPでエンドポイントを提供
- 2つのIPsecトンネルで冗長化
- ルーティングは動的：BGPを推奨、対応していない場合、静的も可能
- VGWの他にAWS Transit Gatewayへ接続する構成も可能

B 複数拠点からセキュアにVPCに接続



ポイント

- 同じVGWにVPNを接続することで、複数拠点から1つのVPCに同時接続が可能
- アイコンとしては一つに表現されるVGWだが、内部的に冗長化
- VGWをハブとして折り返し通信も可能（CloudHub構成）
- 拠点間通信をさせない場合、拠点のルーターで制御（フィルター、ASNの重複等）

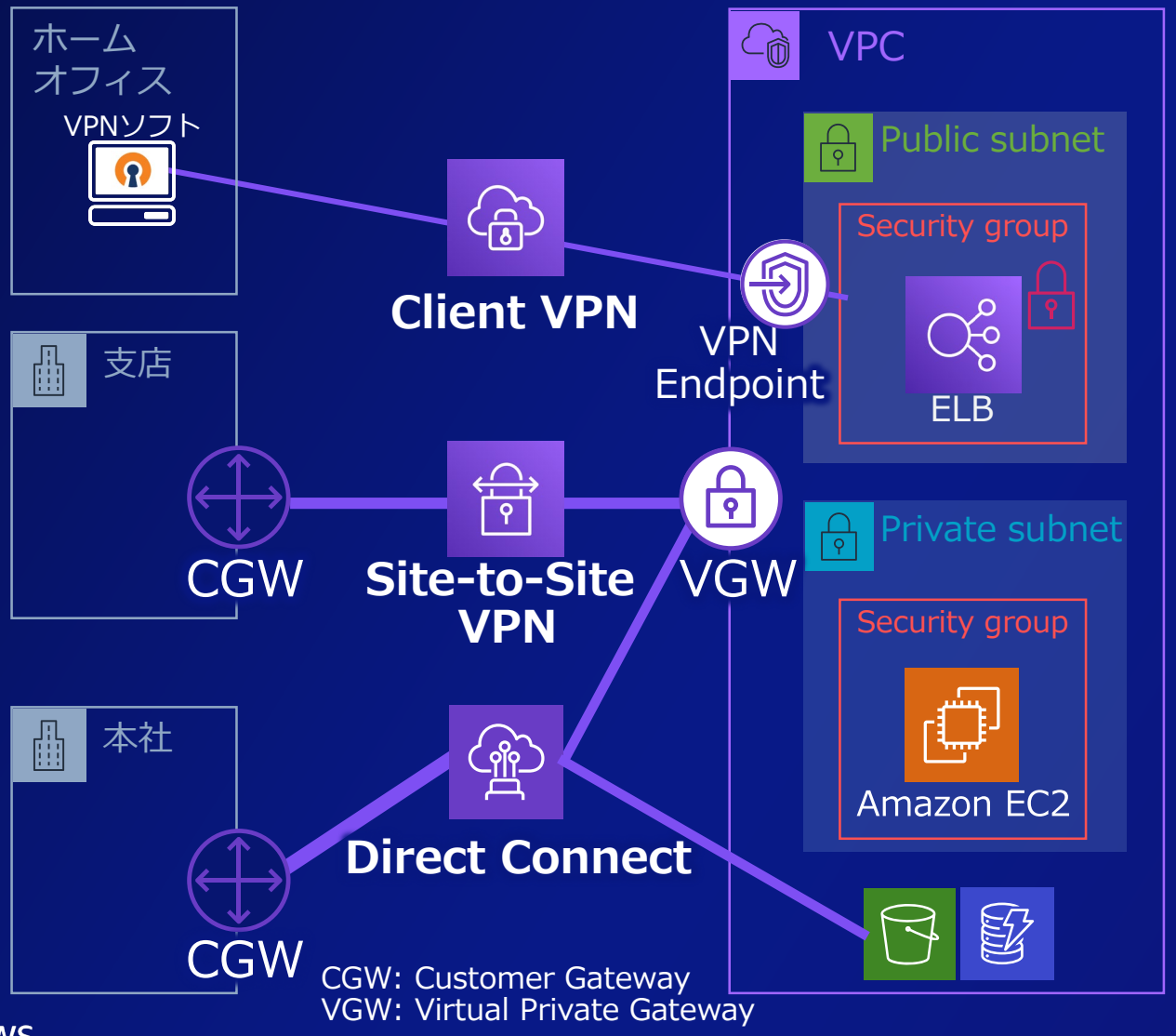
C 要件が異なる拠点からVPCに接続

AWS Client VPN

AWS Site-to-Site VPN

AWS Direct Connect

C 要件が異なる拠点からVPCに接続



ユースケース

- 自宅勤務者の接続
- セキュアなサイト間接続
- 大規模拠点から接続

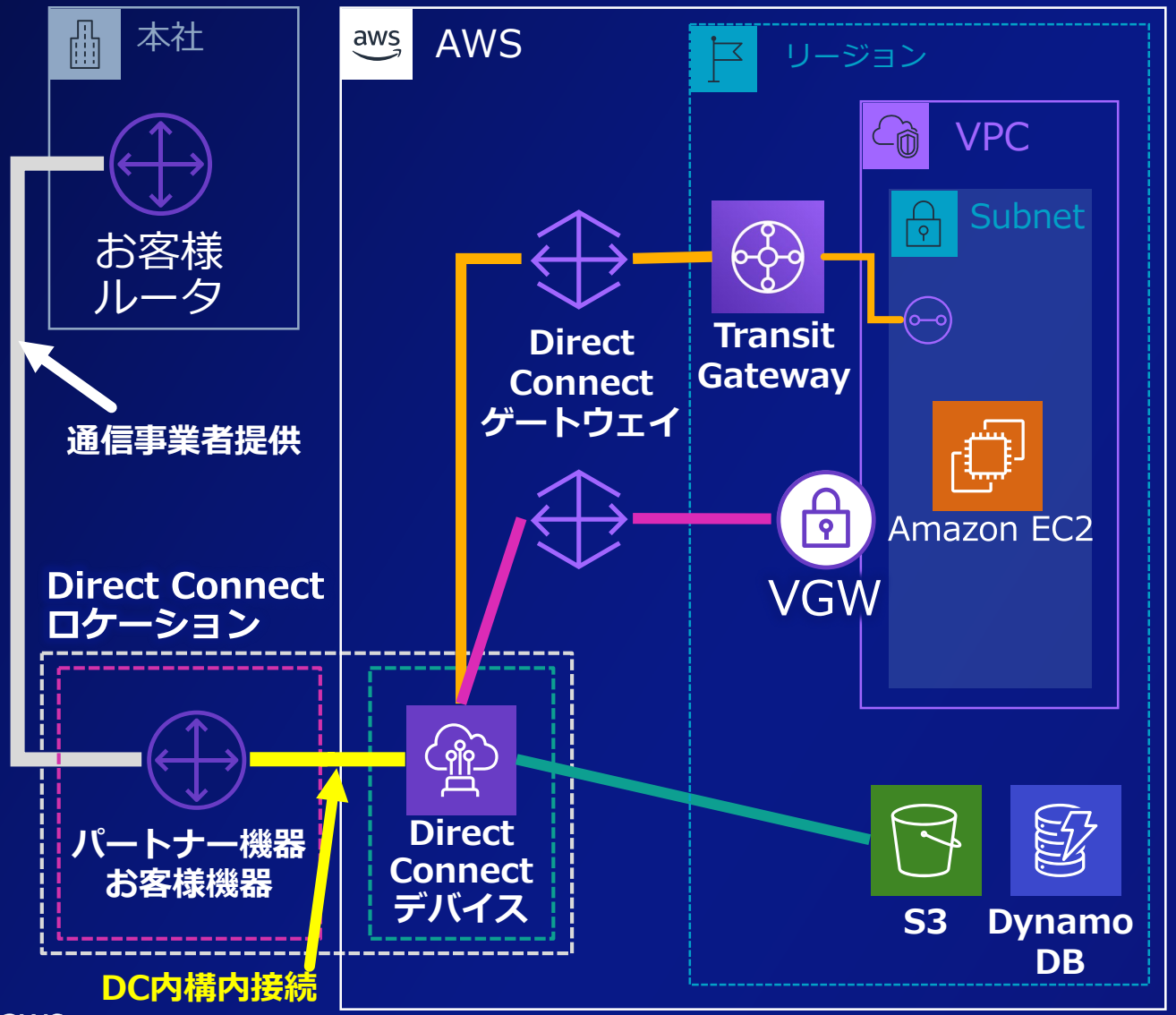
メリット

- 要件に合わせてコストを最適化

選択肢

- AWS Client VPN
- AWS Site-to-Site VPN
- AWS Direct Connect

AWS Direct Connect



ポイント

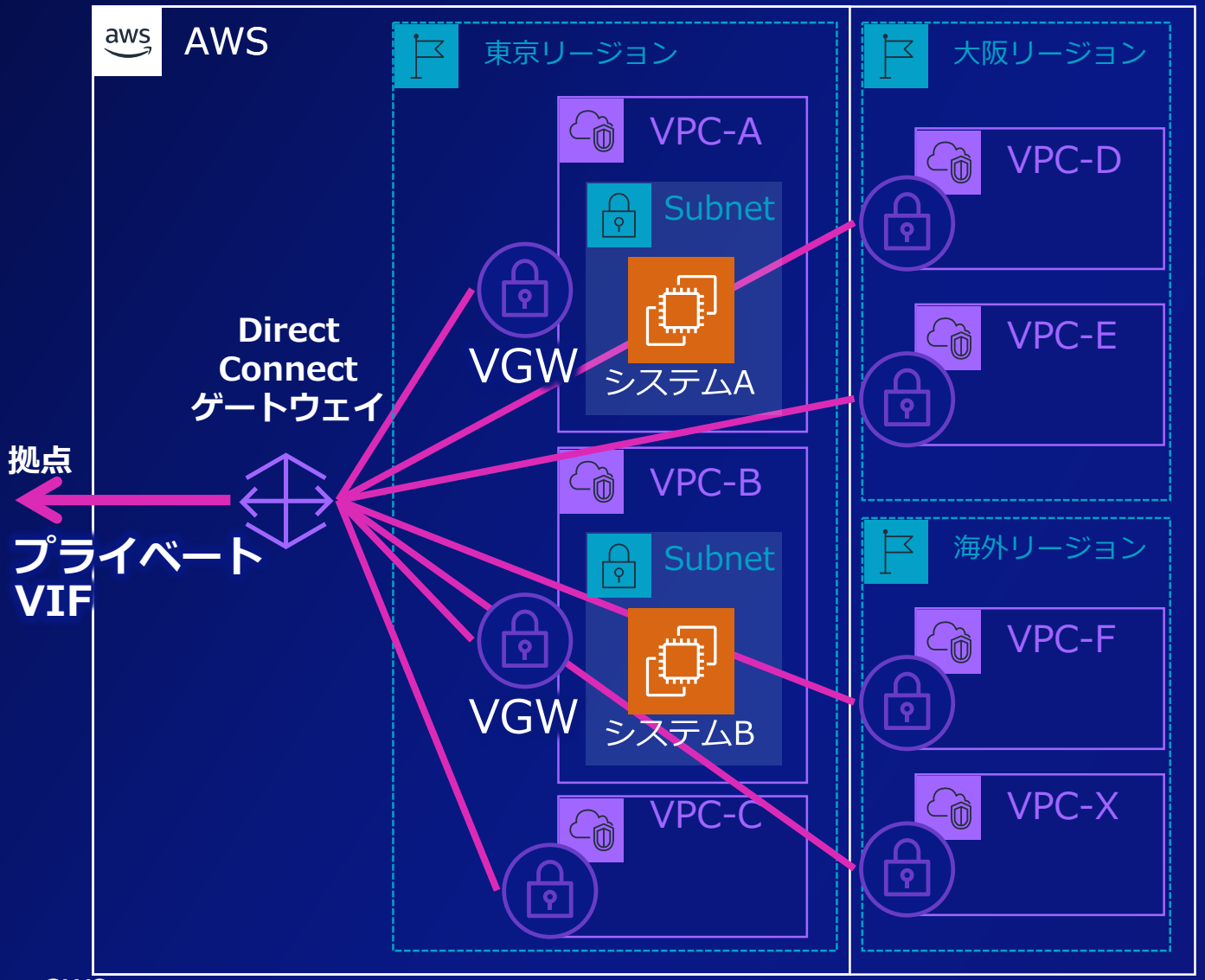
- オンプレミスから専用線でDirect Connectロケーションに接続
- 1, 10, 100Gbpsのポート速度をサポート
- 接続の中に仮想インターフェイス(VIF)を作成
- VIFは接続対象別に3タイプ
  トランジット：TGW用のDXGW
  プライベート：VGW用のDXGW
  パブリック：AWSクラウド
- パートナー経由の利用で多くの選択肢から要件に合わせて選定

D 拠点からシステム毎に異なるVPCに接続

Direct Connectゲートウェイ 

AWS Transit Gateway 

Direct Connectゲートウェイ(DXGW)

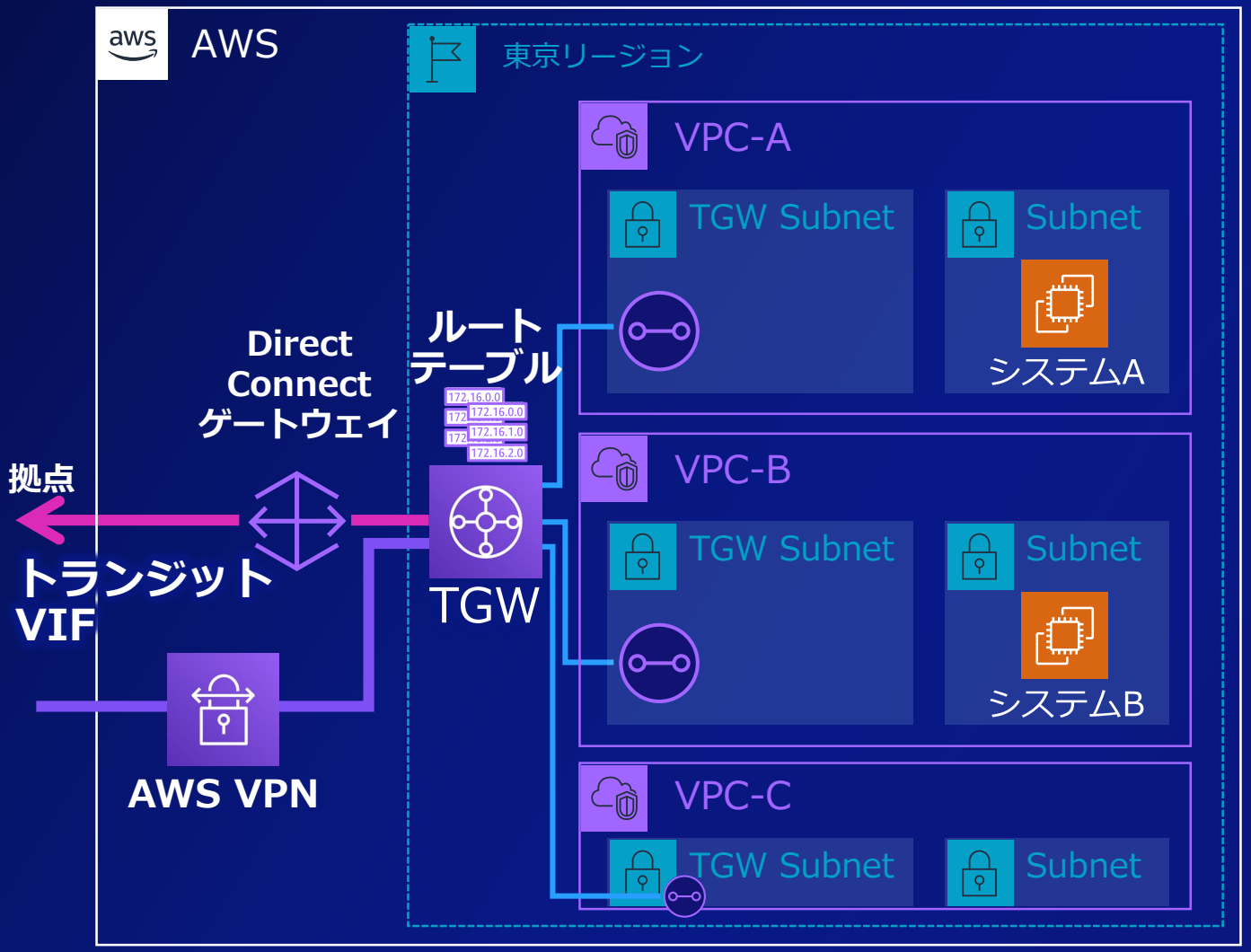


ポイント

- Direct Connectゲートウェイを利用することで、1つのプライベート接続から20のVPCに同時アクセス可能
- 互いに影響を受けない、システムごとに異なるVPCを平行稼働
- Direct Connectゲートウェイの利用料は無料、経由した転送の量に応じて課金
- 異なるリージョンのVPCにも関連付け可能

注: 2023年4月末にQuotaの見直しが行われました
最新情報は以下をご確認ください
https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

AWS Transit Gateway (TGW)



ポイント

- リージョン内のコアルーターとして通信を集約する役割
- TGWは数千のVPCと通信可能
- TGWルートテーブルを複数作成し、柔軟なルーティングに対応
- AWS Site-to-Site VPNも接続
- 複数のリージョン間通信時にはAWS Cloud WANを検討

オンプレミスとVPCの接続パターン（再掲）

A　拠点からインターネット経由でVPCに接続
☞別途セキュリティを保ち迅速に通信

B　複数拠点からセキュアにVPCに接続
☞IPsecトンネルでVPN接続し、CloudHub構成を活用

C　要件が異なる拠点からVPCに接続
☞ネットワークサービスを使い分け要件/コストに最適化

D　拠点からシステム毎に異なるVPCに接続
☞規模によってDXGWとTGW、Cloud WANを検討

皆さんがAWSクラウドを活用するフェーズや要件に合わせて、これらから選択・組み合わせが可能です。

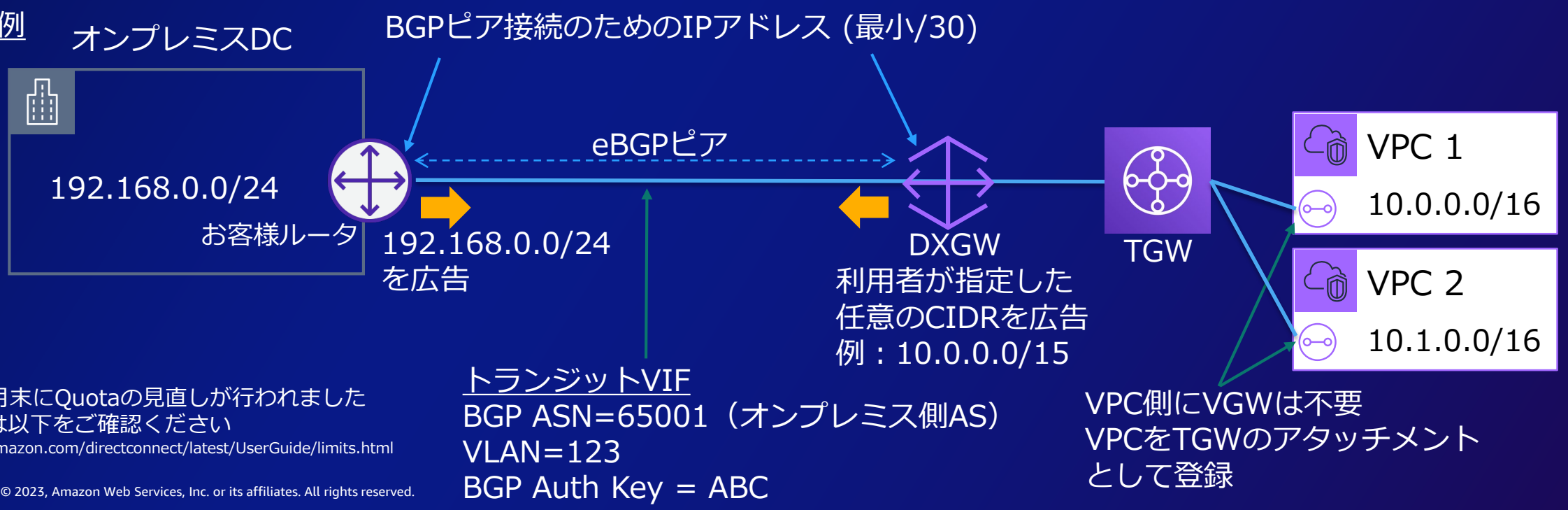
2. VPCが増えてきた時の対応方法

2-1. AWS Transit Gatewayを使うには？

トランジットVIFによるTransit Gateway(TGW)への接続

- トランジットVIFを使用してDirect Connectゲートウェイ(DXGW)経由でTGWへ接続
- オンプレミスルーターとBGPピアを確立する
- VPC CIDRはそのまま広告されず、Direct Connectゲートウェイの「許可されたプレフィックス」で指定した任意のCIDRが広告される：合計200 CIDR
- Jumbo Frame (MTU=8500) をサポート

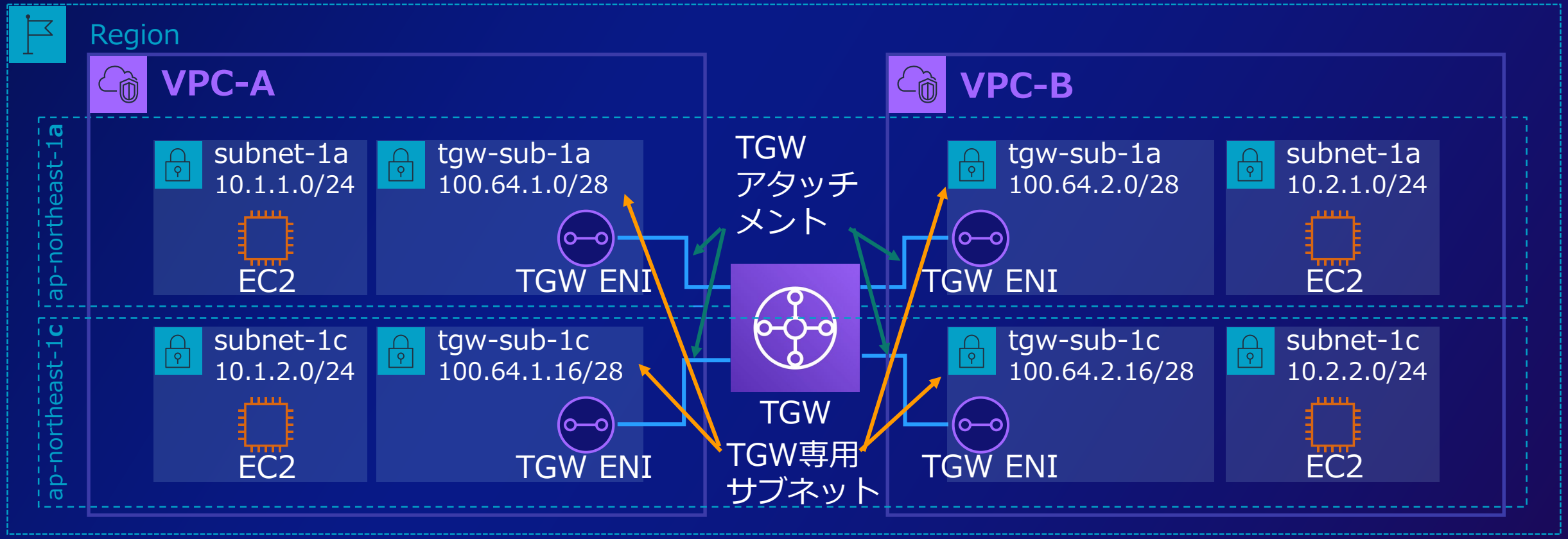
  https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/set-jumbo-frames-vif.html



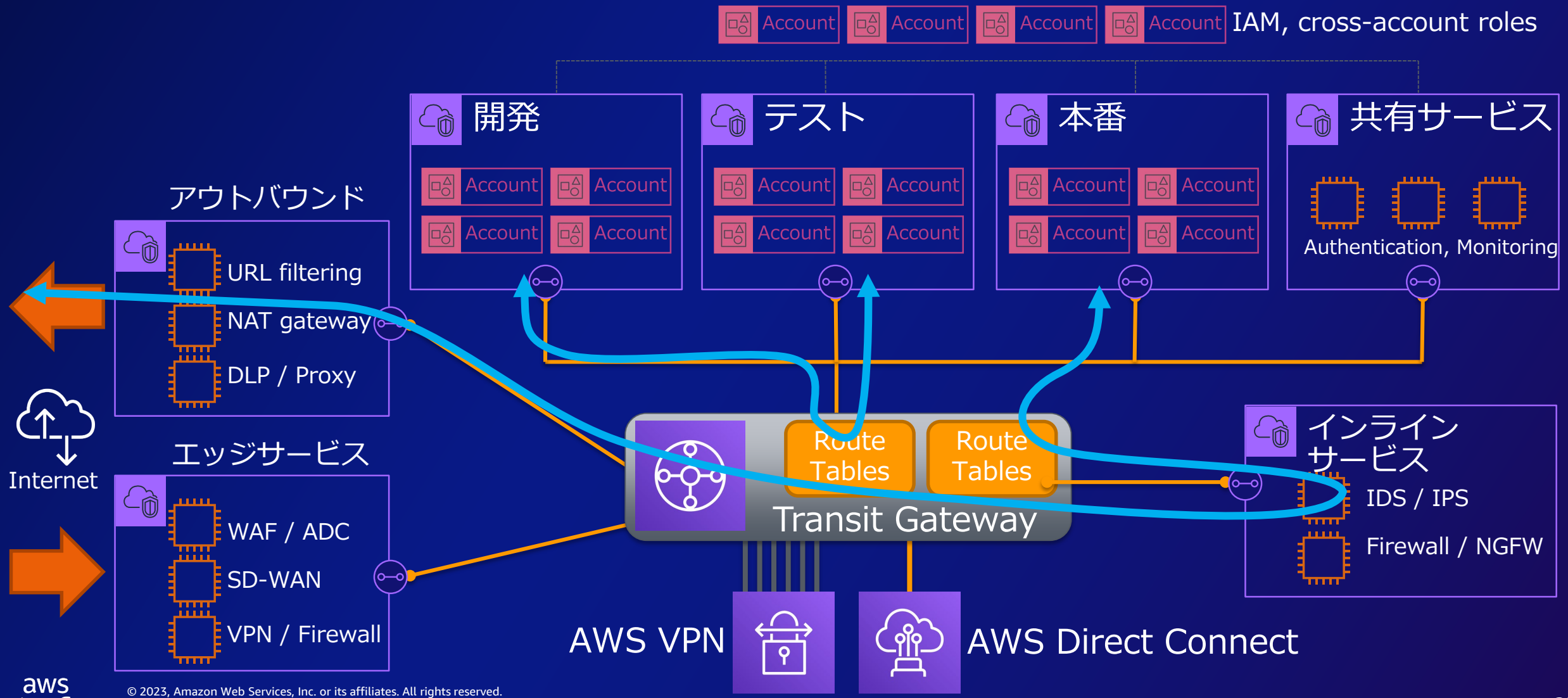
注: 2023年4月末にQuotaの見直しが行われました
最新情報は以下をご確認ください
https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

Transit Gatewayのベストプラクティス: アタッチメント

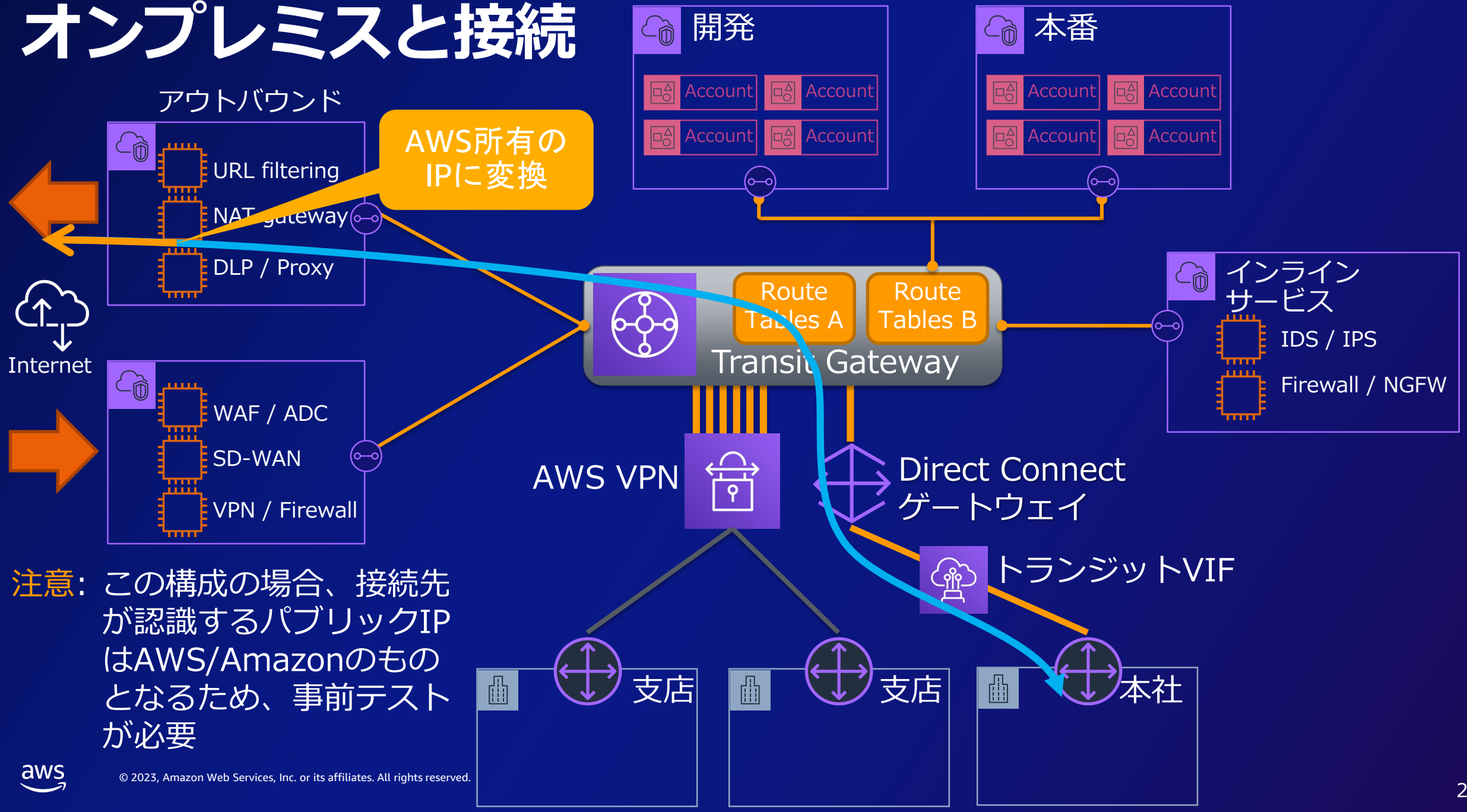
- Transit Gateway(TGW)をアタッチするサブネットは、専用の/28(IPアドレス:16個)を用意し、EC2インスタンスなど、ワークロードを配置するサブネットとは別にする
- ルートテーブルの柔軟性や、ネットワークアクセスコントロールリストを分けて管理することが可能になる



AWS リファレンスアーキテクチャー



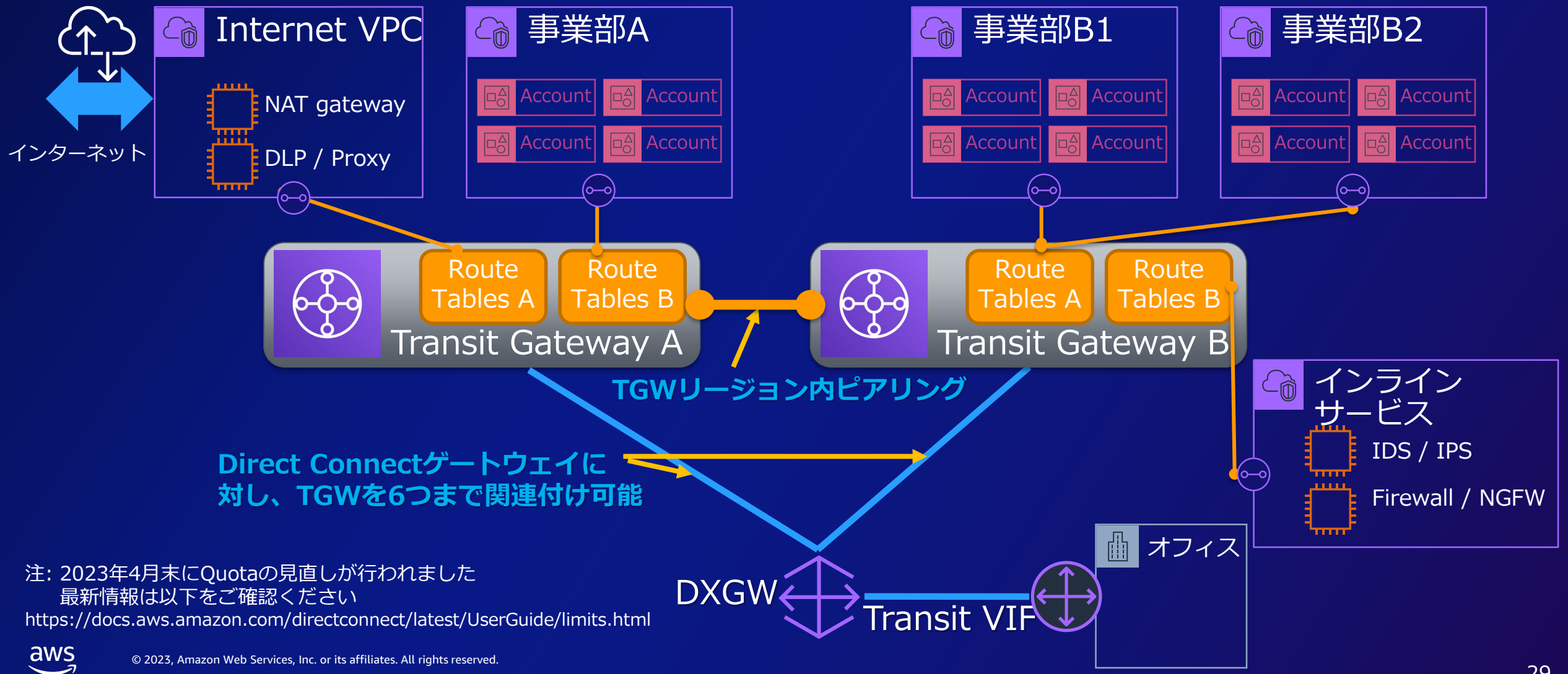
オンプレミスと接続



注意：この構成の場合、接続先が認識するパブリックIPはAWS/Amazonのものとなるため、事前テストが必要

VPC内の多彩なルーティング要件（パターン1）

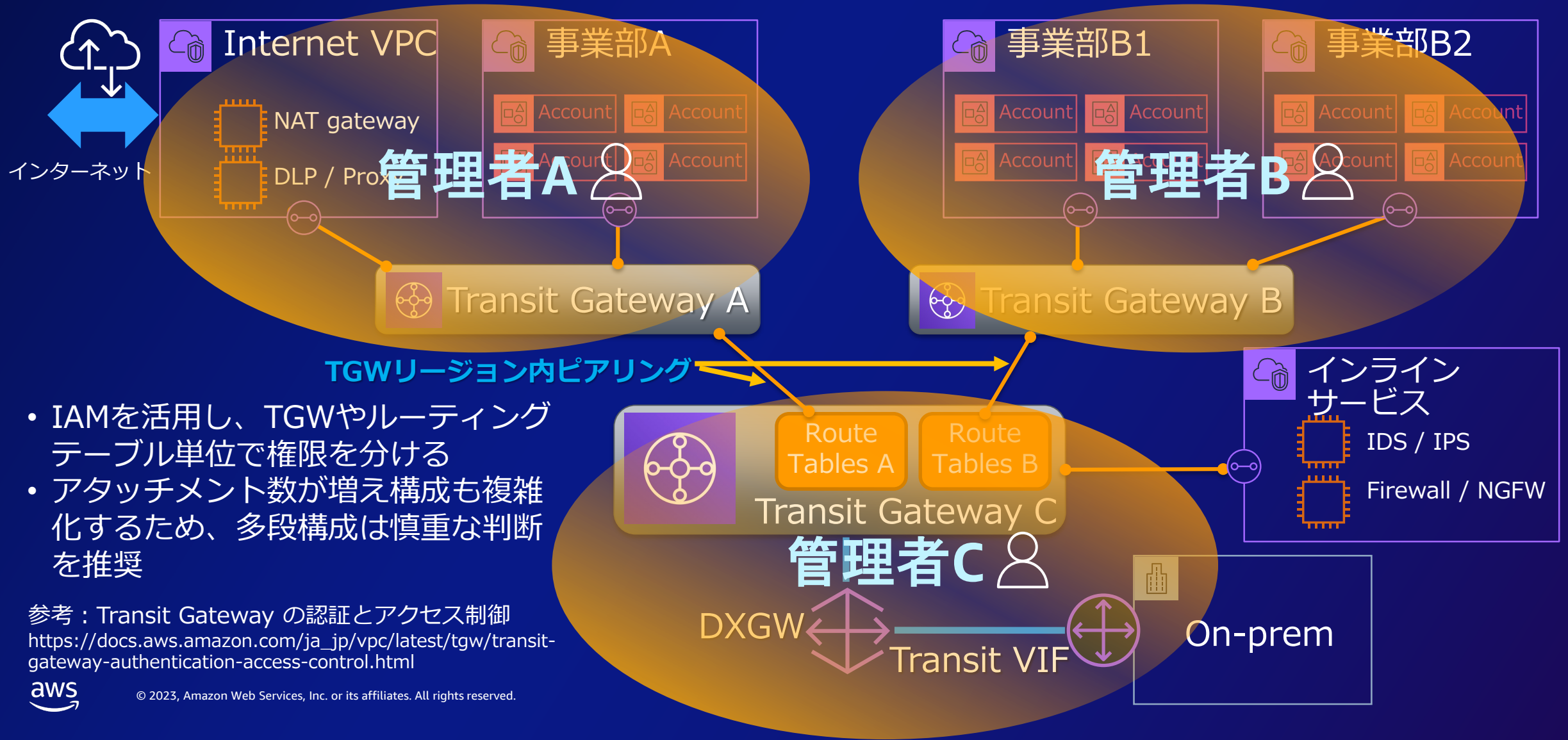
DXGWから複数のTGWに関連付け、必要な通信のみをピアリング経由で通信



注: 2023年4月末にQuotaの見直しが行われました
最新情報は以下をご確認ください
https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

VPC内の多彩なルーティング要件（パターン2）

TGWリージョン内ピアリングを利用して多段構成も可能



- IAMを活用し、TGWやルーティングテーブル単位で権限を分ける
- アタッチメント数が増え構成も複雑化するため、多段構成は慎重な判断を推奨

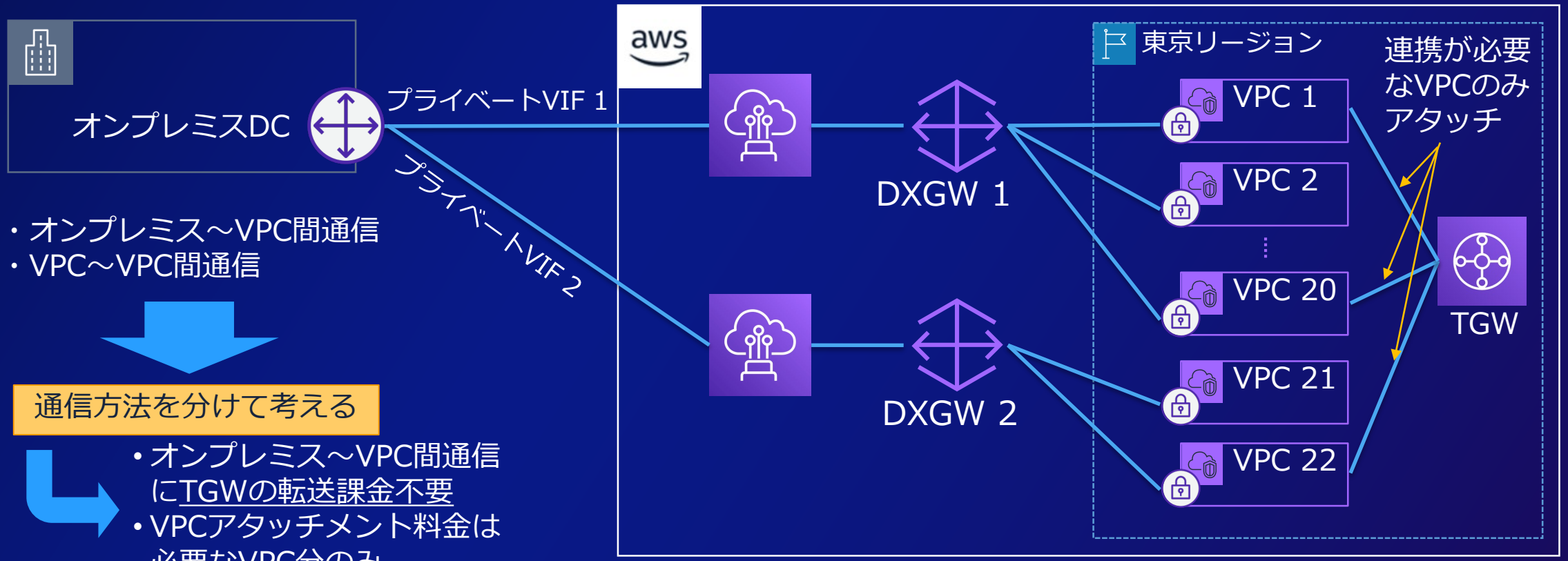
参考：Transit Gateway の認証とアクセス制御
https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/transit-gateway-authentication-access-control.html

2-2. “オンプレミス通信”と “VPC間通信”を分けて考える

Direct Connectゲートウェイの Tips

AWS Direct Connectゲートウェイ：Tips

- Direct Connectゲートウェイ(DXGW)あたりのVGW数は**20**まで。それを超える数のVPCを接続する場合は**プライベートVIFとDXGWのペアを追加**する
- VPC間の通信はDXGWを経由できないため、**連携が必要なVPCのみ**Transit Gateway(TGW)をアタッチして経路を確保する



注: 2023年4月末にQuotaの見直しが行われました
最新情報は以下をご確認ください
https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

2-3. 構成比較

AWS Direct Connect
プライベートVIF or トランジットVIF

オンプレミスとVPC間の閉域網接続における プライベートVIF(DXGW)とトランジットVIF(DXGW+TGW)の比較

検討項目	プライベートVIF（DXGW）	トランジットVIF（DXGW+TGW）
用途	オンプレミスとVPCを1対多で接続する	オンプレミスとVPC間に**コアルーター**としてTGWを配置し、全ての通信を1か所で管理する
VPCの拡張性	VPCは1つのプライベートVIF+DXGWで20まで関連付け可能、21以上にはプライベートVIF+DXGWのペアを追加	**VPCを5,000まで接続可能**
通信対象IP	オンプレミスとVPC間のCIDRみ通信	オンプレミスとDXGWに指定する任意のIPで通信（上限：200 Prefix、デフォルトルート指定可能）
ルーティング	DXGWから広報するVPC CIDRに対し、経路フィルタリングが可能 VPC間の折り返し通信不可	TGWで複数のルートテーブルを作成し、柔軟な設計が可能　VPC間の折り返し通信可能 TGW Connectと連携しSD-WANとシームレス接続
費用	DXGWの利用は無料、転送料は仮想プライベートゲートウェイのみ利用時と同等	TGWの転送料(従量制)、アタッチメント料(時間課金)が加算
接続の要件	パートナーから提供される**豊富なメニューから選択可能**	接続/ホスト接続(**1G未満でも利用可**)が必要（引き続き、共有型接続では不可）

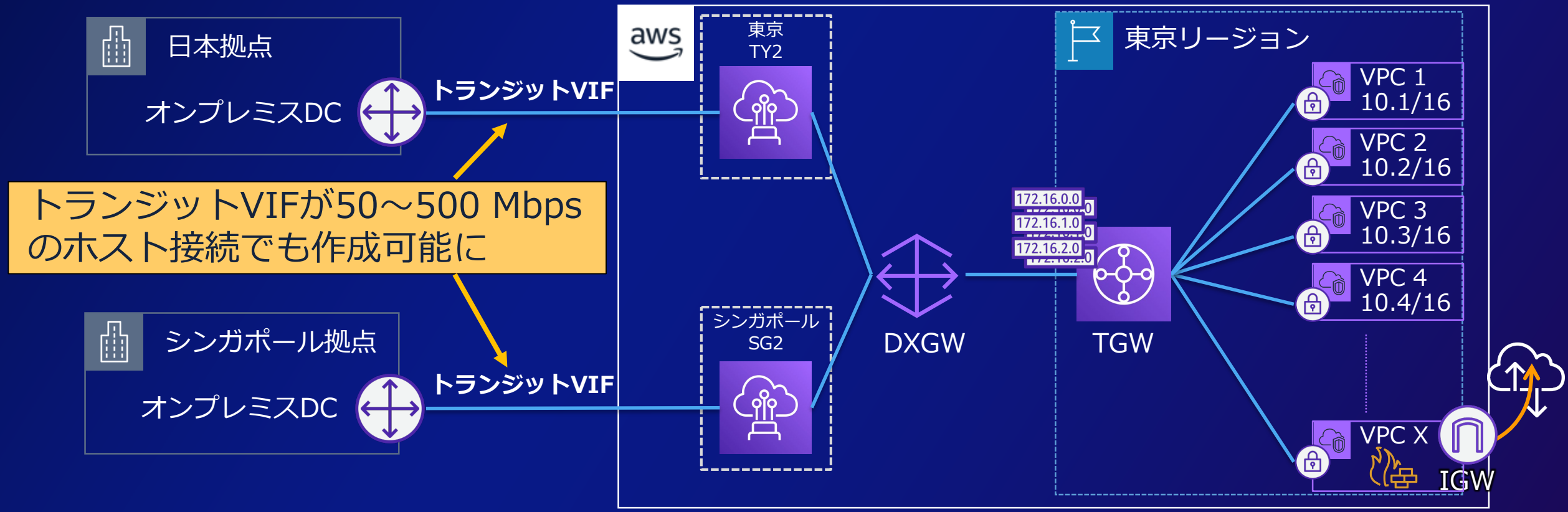
注: 2023年4月末にQuotaの見直しが行われました
最新情報は以下をご確認ください
https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

Update

3-4. より使いやすくなったトランジットVIF

より多くの接続速度で トランジット仮想インターフェイスをサポート

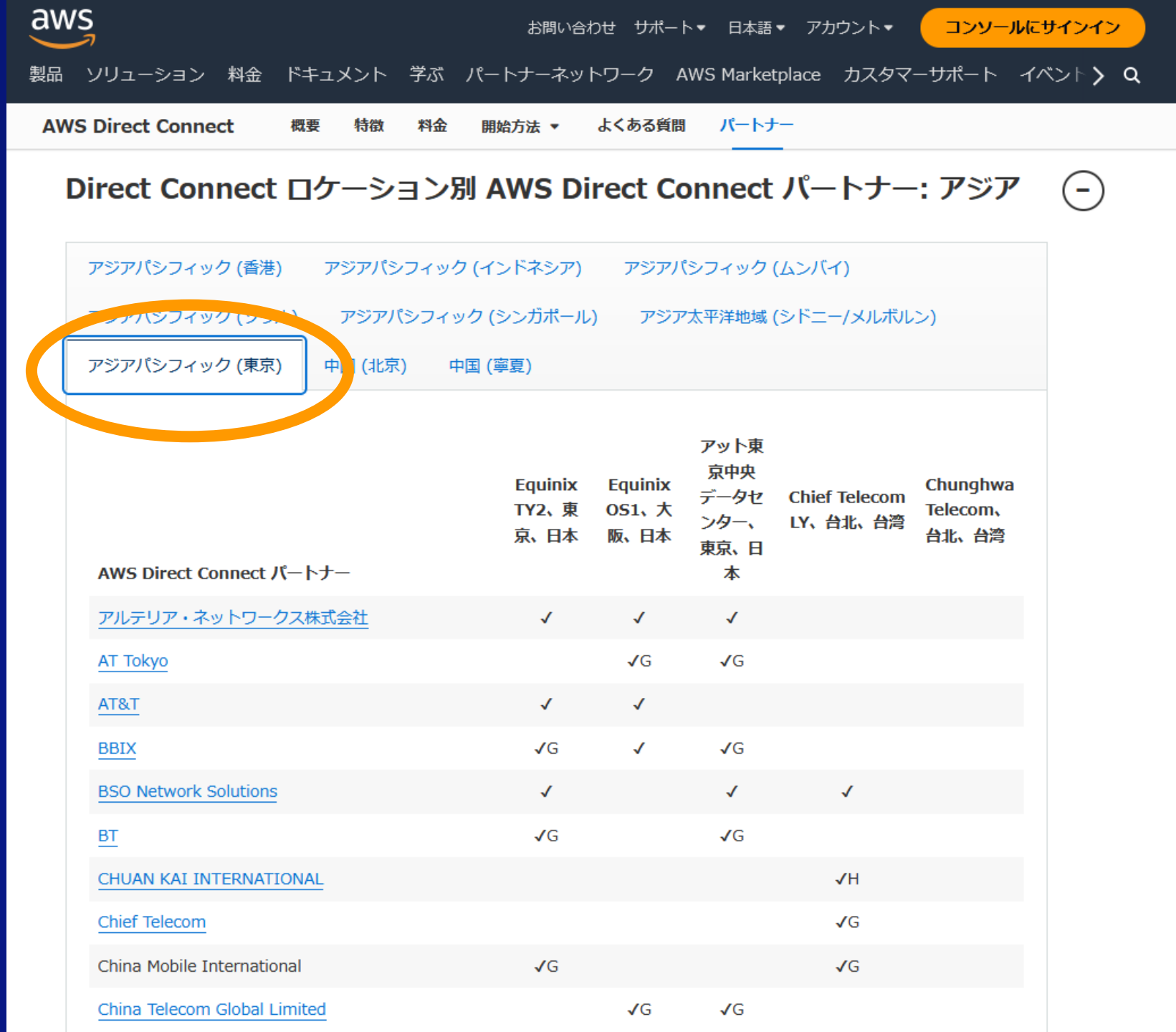
- パートナーから提供されるすべての**ホスト接続**で、トランジット仮想インターフェイス（トランジットVIF）が利用可能になりました。



参考：

公開URLでパートナー様一覧と利用可能なロケーションを確認可能

https://aws.amazon.com/jp/directconnect/partners/



AWS Direct Connect パートナー	Equinix TY2、東京、日本	Equinix OS1、大阪、日本	アット東京中央データセンター、東京、日本	Chief Telecom LY、台北、台湾	Chunghwa Telecom、台北、台湾
アルテリア・ネットワークス株式会社	✓	✓	✓		
AT Tokyo		✓G	✓G		
AT&T	✓	✓			
BBIX	✓G	✓	✓G		
BSO Network Solutions	✓		✓	✓	
BT	✓G		✓G		
CHUAN KAI INTERNATIONAL				✓H	
Chief Telecom				✓G	
China Mobile International	✓G			✓G	
China Telecom Global Limited		✓G	✓G		

まとめ

まとめ

- オンプレミスとAWSクラウドを閉域網でつなぐときの考慮ポイントを知る

要件ごとに複数のネットワークサービスを選択・組み合わせ

- AWS側のゲートウェイとなるサービスとその特徴を理解する

仮想プライベートゲートウェイ(VGW)、Direct Connectゲートウェイ(DXGW)、Transit Gateway(TGW)の特性、使い方

- クラウドネットワークの拡張時に困らない設計を把握する

拡張性に優れたアーキテクチャ、その考え方

Thank you!

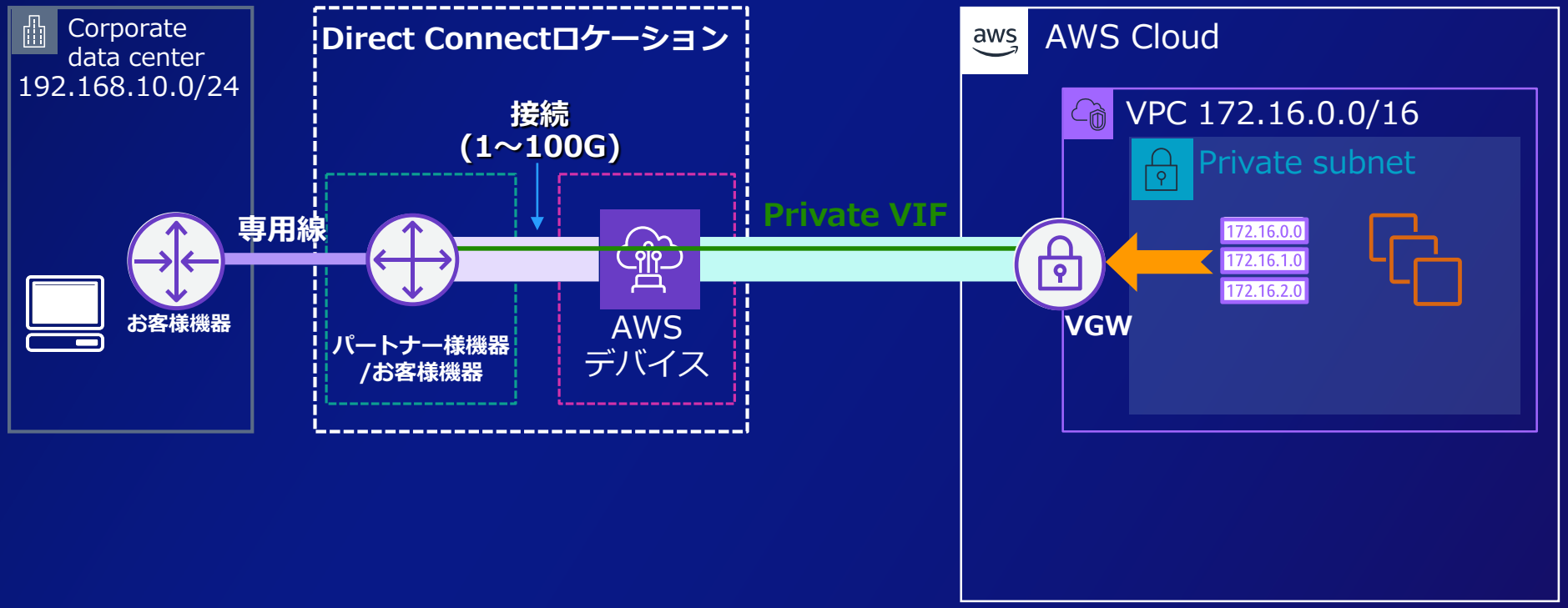
菊地 信明
アマゾン ウェブ サービス ジャパン合同会社
ネットワークソリューション部
シニアソリューションアーキテクト
ネットワークスペシャリスト

Appendix

A-1. AWS Transit Gatewayへの移行方法

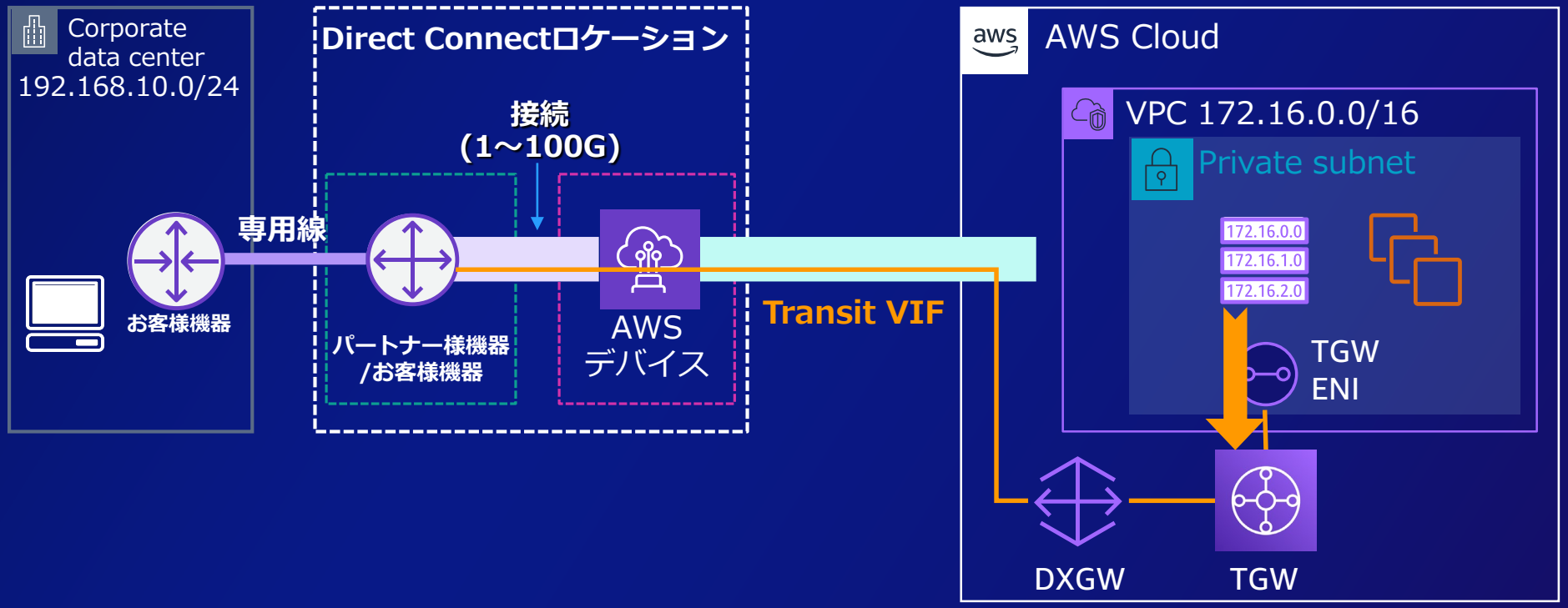
移行元環境について

- 本資料では、移行元環境として以下のような構成を前提とする。
- 冗長化については考慮しません。実際の移行時には冗長化を考慮した作業手順を検討。



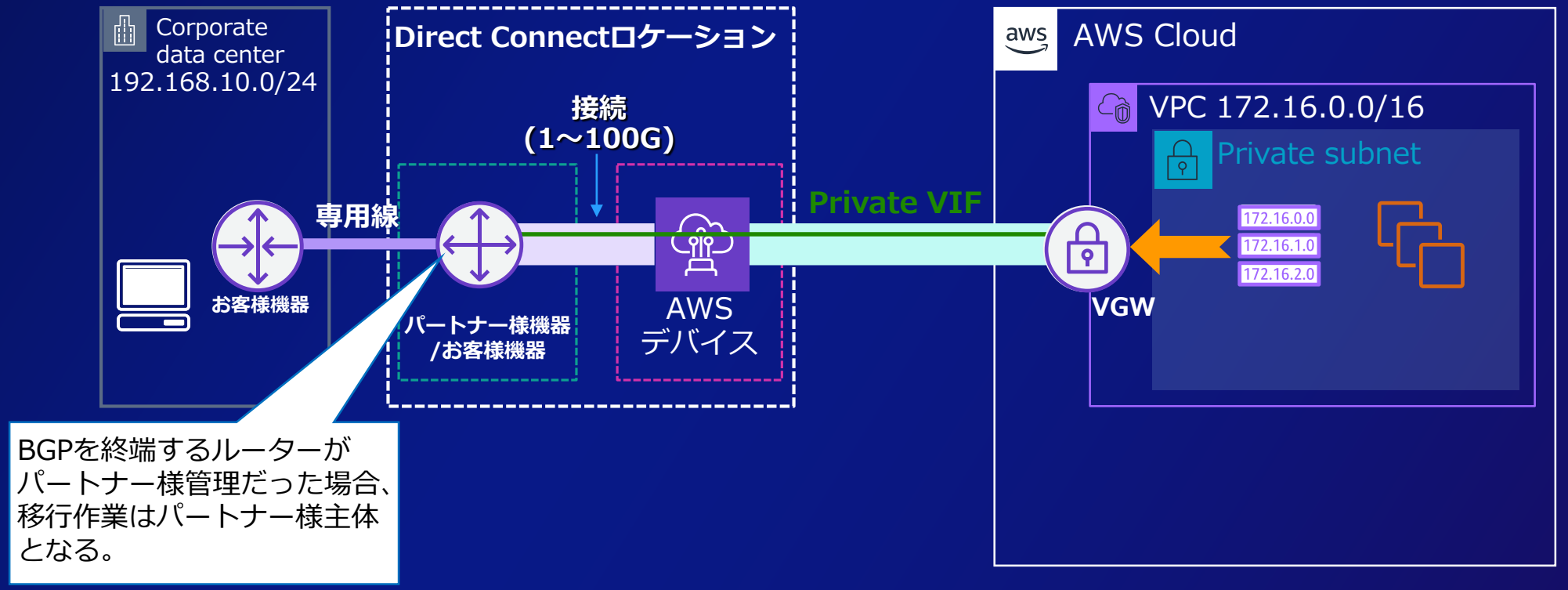
移行後環境について

- 最終的な構成は以下。
- Transit VIFを利用できるDirect Connect 接続が必要です。



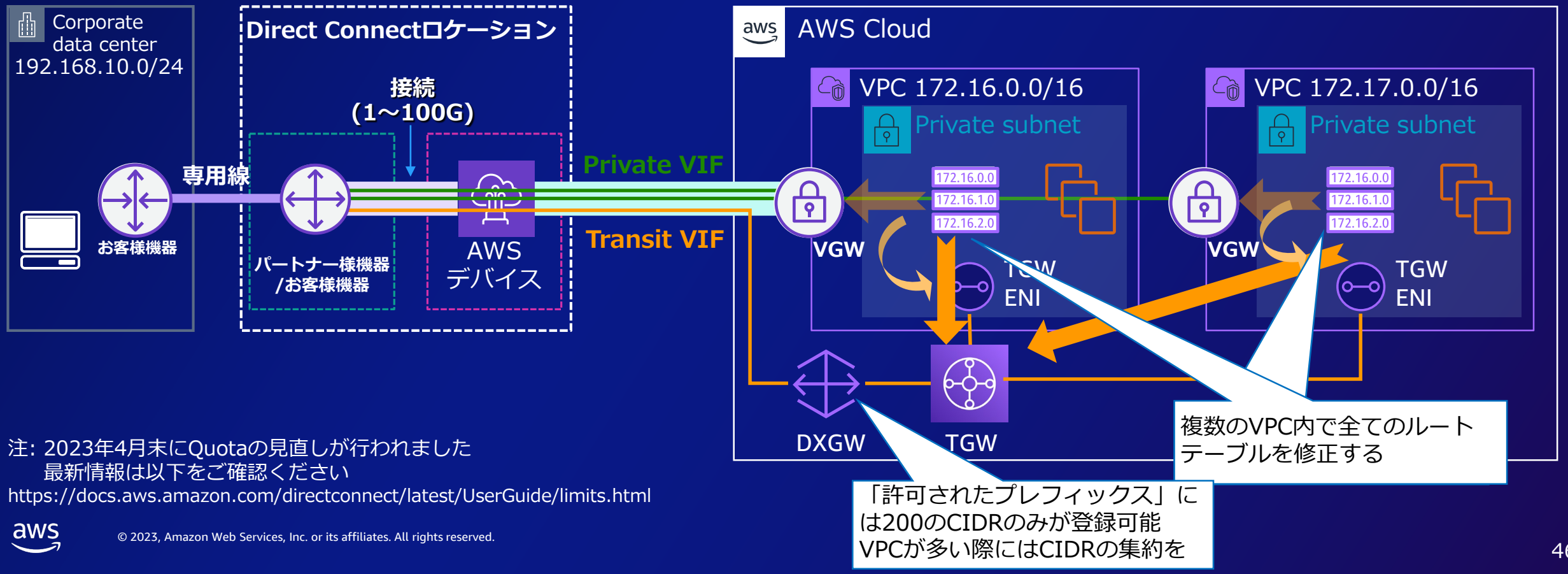
オンプレミス環境における注意点

BGPを終端するルーターは、Direct Connectロケーションに設置されている場合や、L2網を通してオンプレミス側に設置されている。パートナー様機器が終端して、経路を再配信している構成などがある。現状の構成を正しく理解しておくことが大切。



VPC環境における注意点

複数のVPCを同時に移行する場合、それぞれのVPC内でSubnetが参照しているルートテーブルを変更。一度に移行する、またはVPC毎に移行を分ける等、事前に移行計画を作る。「許可されたプレフィックス」の200レコード制限に注意。

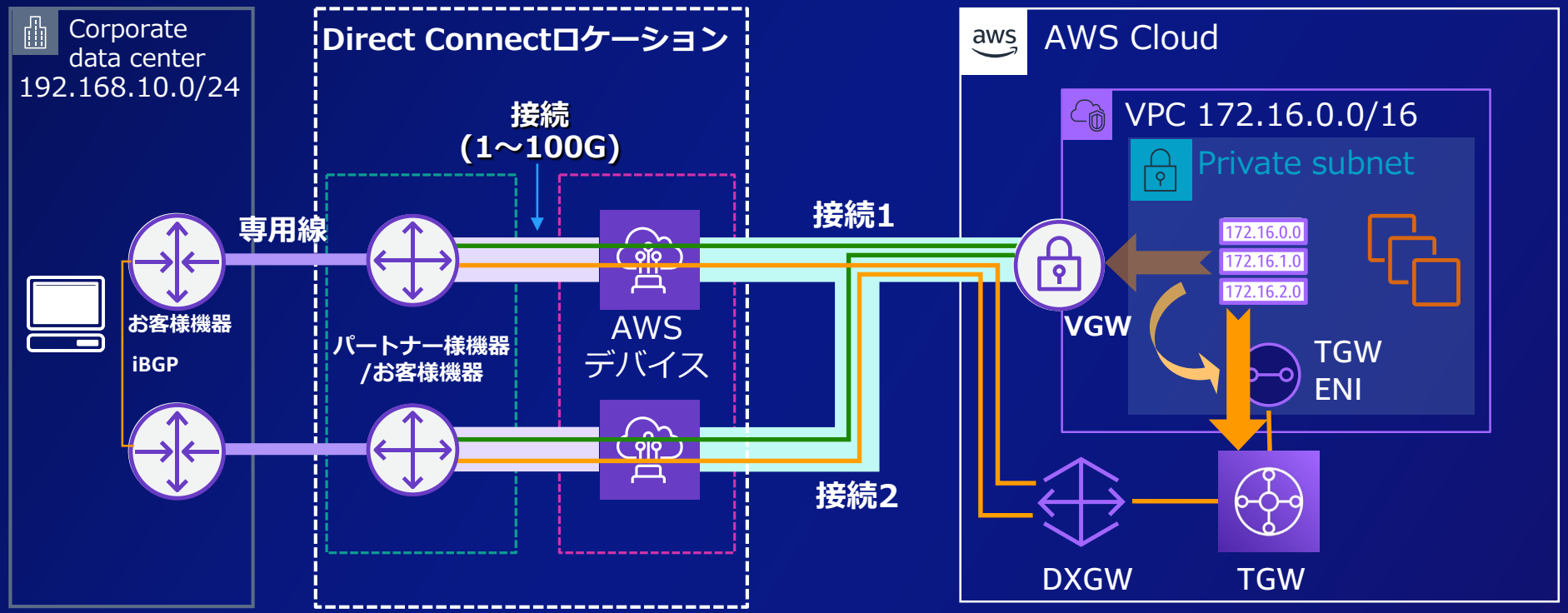


注: 2023年4月末にQuotaの見直しが行われました
最新情報は以下をご確認ください
https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

本番環境における移行作業について

本資料では、冗長化については考慮していません。実際の移行時には冗長化を考慮した作業手順をご検討ください。

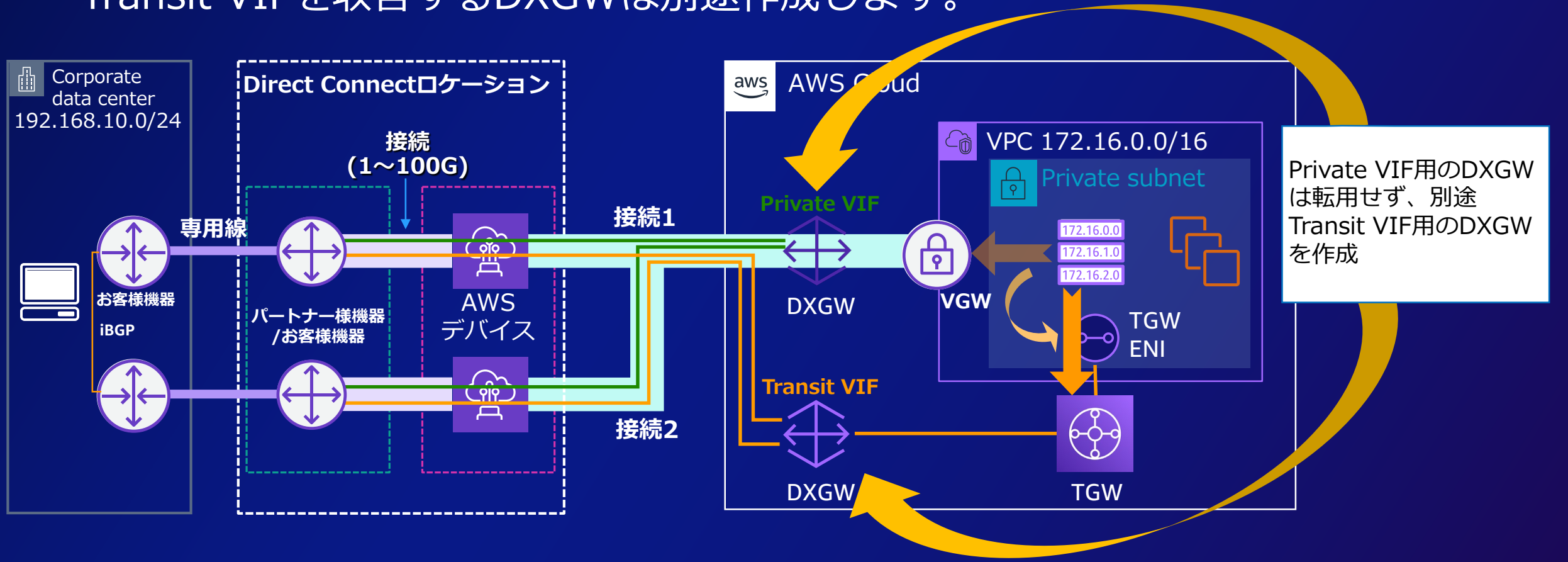
【冗長化例】



移行元でDirect Connect Gateway(DXGW)を利用

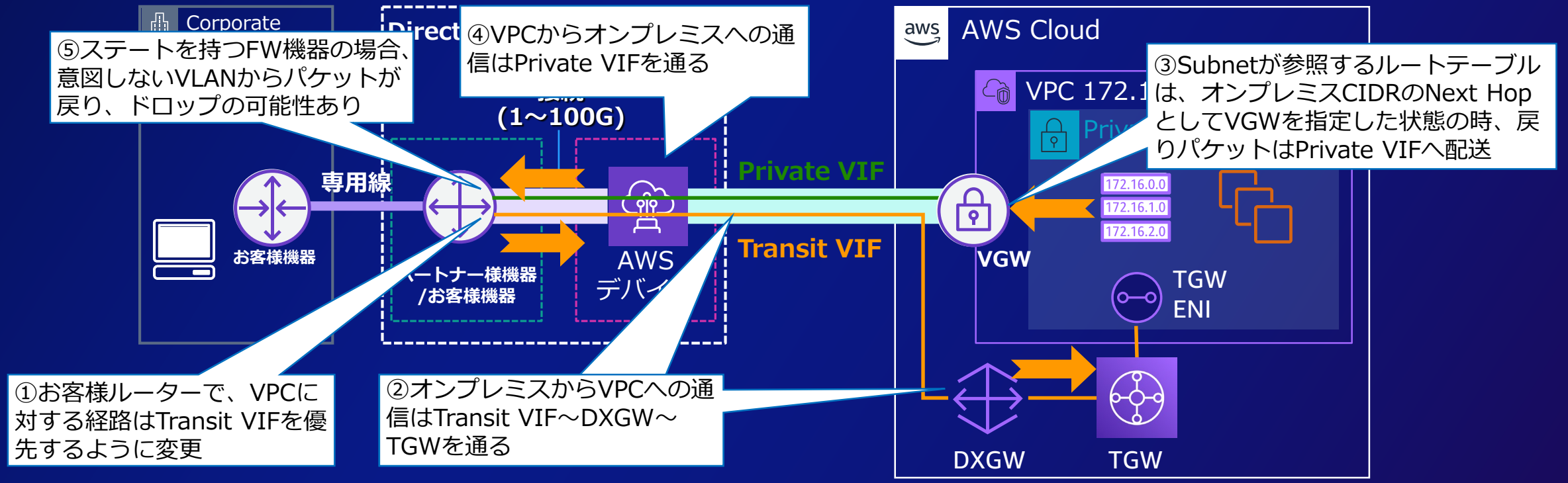
以降のページでは、移行元が直接VGWへ接続されている前提ですが、DXGWを利用している場合にも同様の処理が可能です。

Transit VIFを収容するDXGWは別途作成します。



非対称ルーティングについて

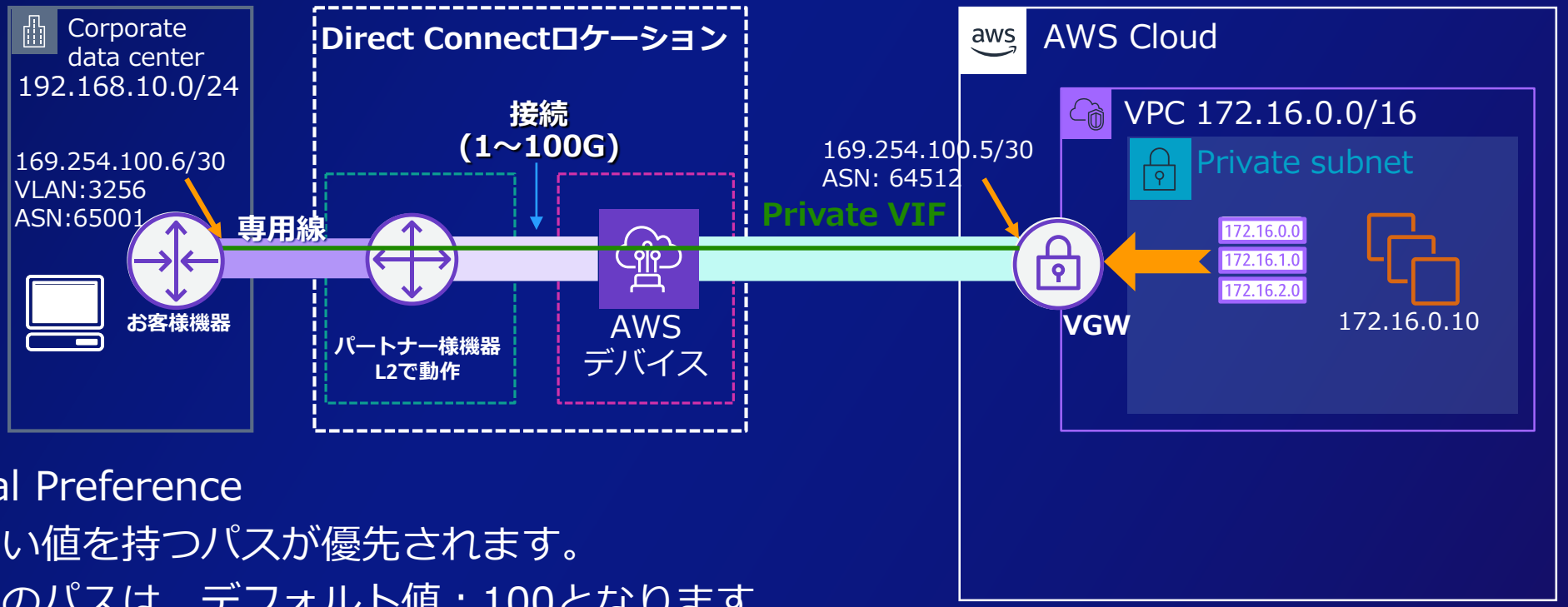
移行作業時に「非対称ルーティング」となる場合がある。この状況でも各リソースはパケットを転送しつづける。お客様機器の仕様によっては、意図しないVLANからパケットが戻り、ドロップの可能性あり。



デモ環境：移行元

Private VIF側のBGPピアのLocal Preference設定※

作業前：　100 (Cisco Default)
移行準備：　200
移行作業：　50

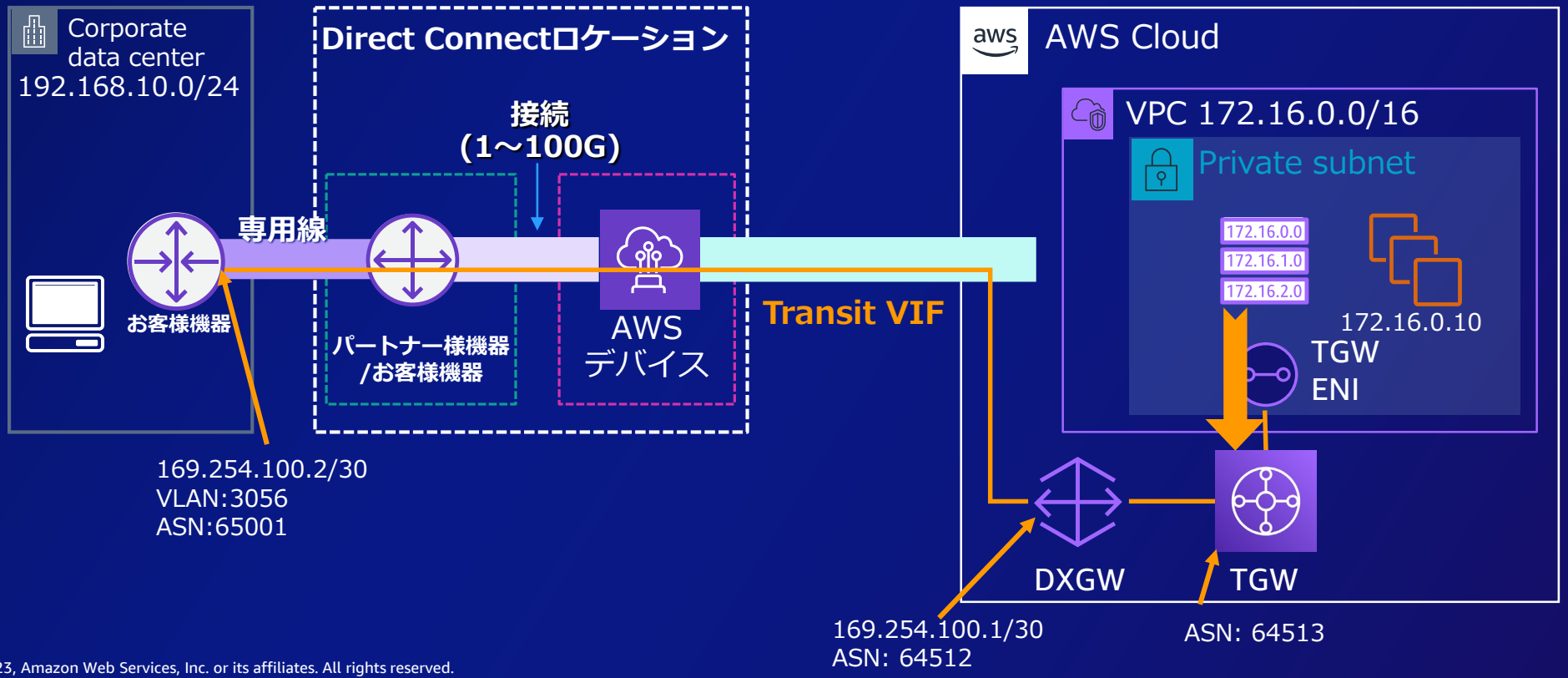


※Local Preference
最も高い値を持つパスが優先されます。
未設定のパスは、デフォルト値：100となります。

デモ環境：移行後

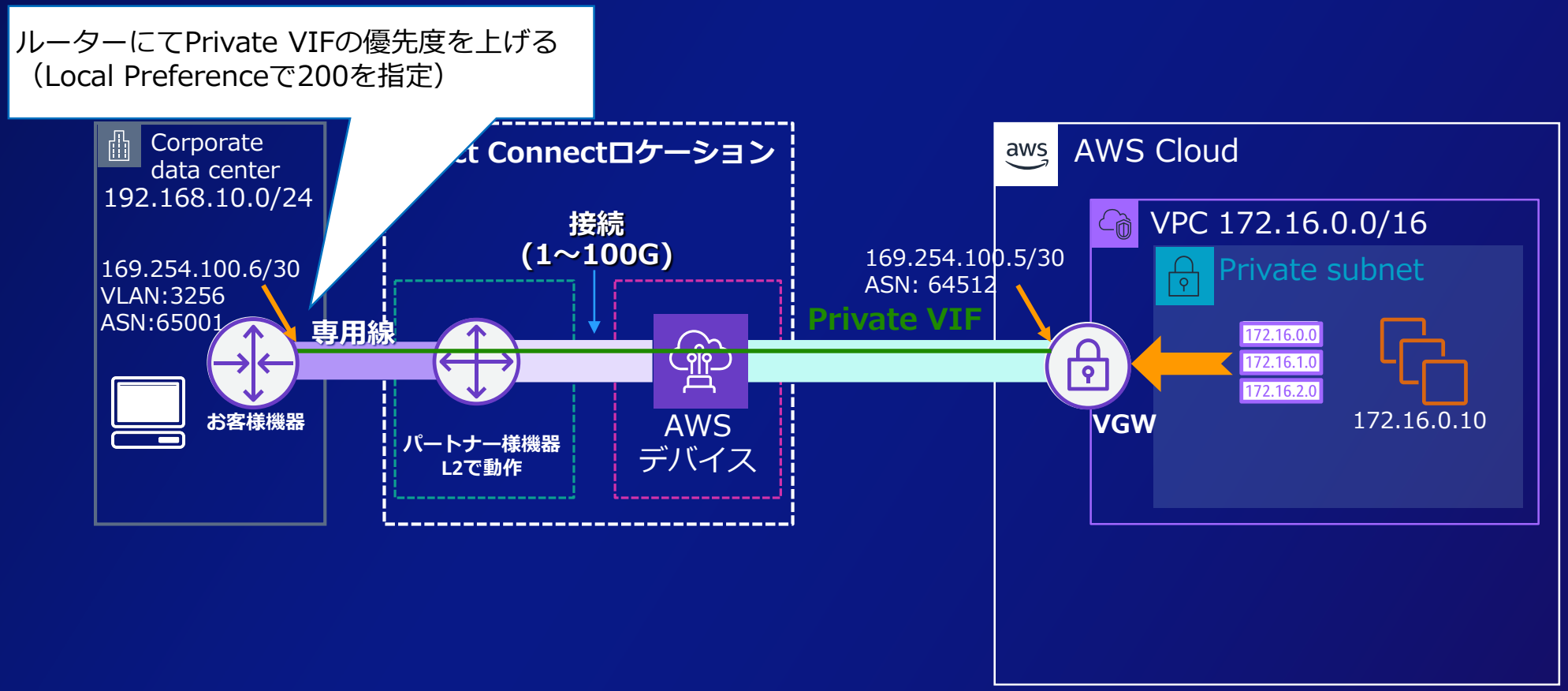
Transit VIF側のBGPピアのLocal Preference設定

作業前後で変更せず： 100 (Cisco Default)



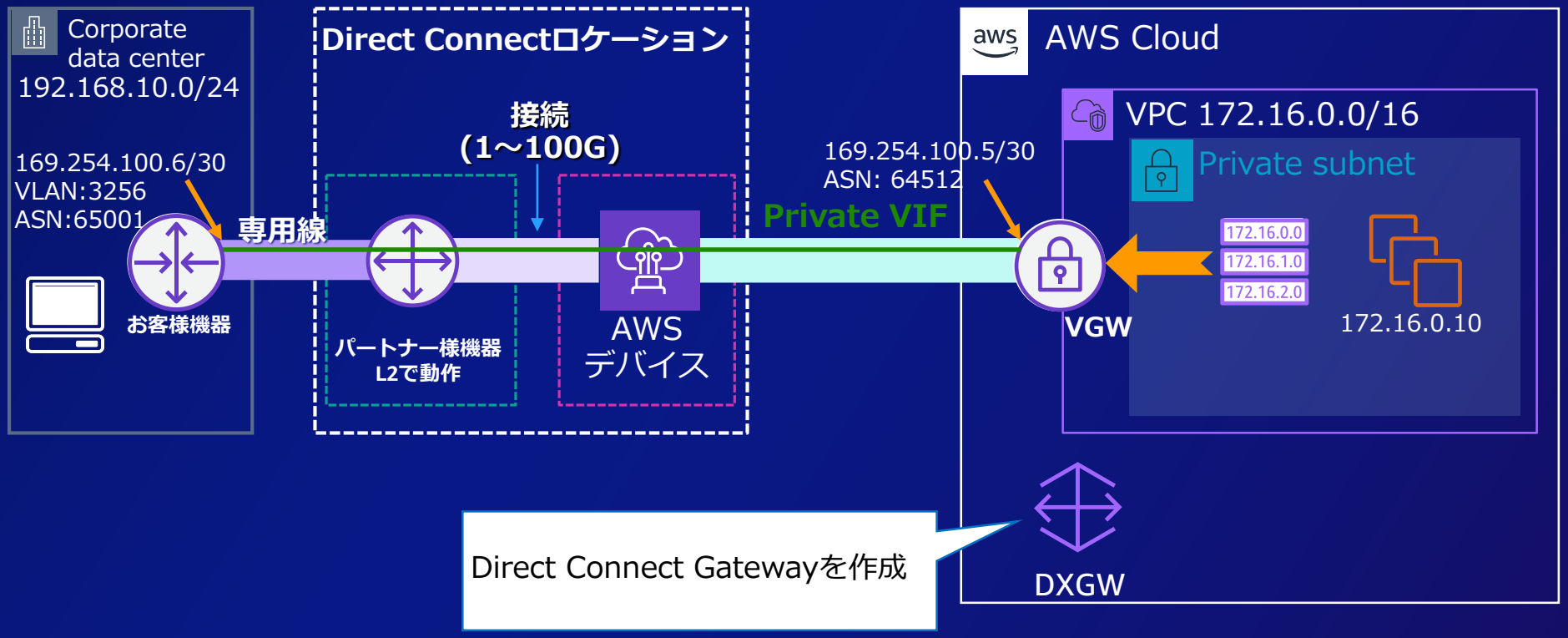
Step:1 【事前準備】

オンプレミス側ルーターにて、Transit VIF開通後もPrivate VIF側で通信をするようにLocal Preferenceを設定。



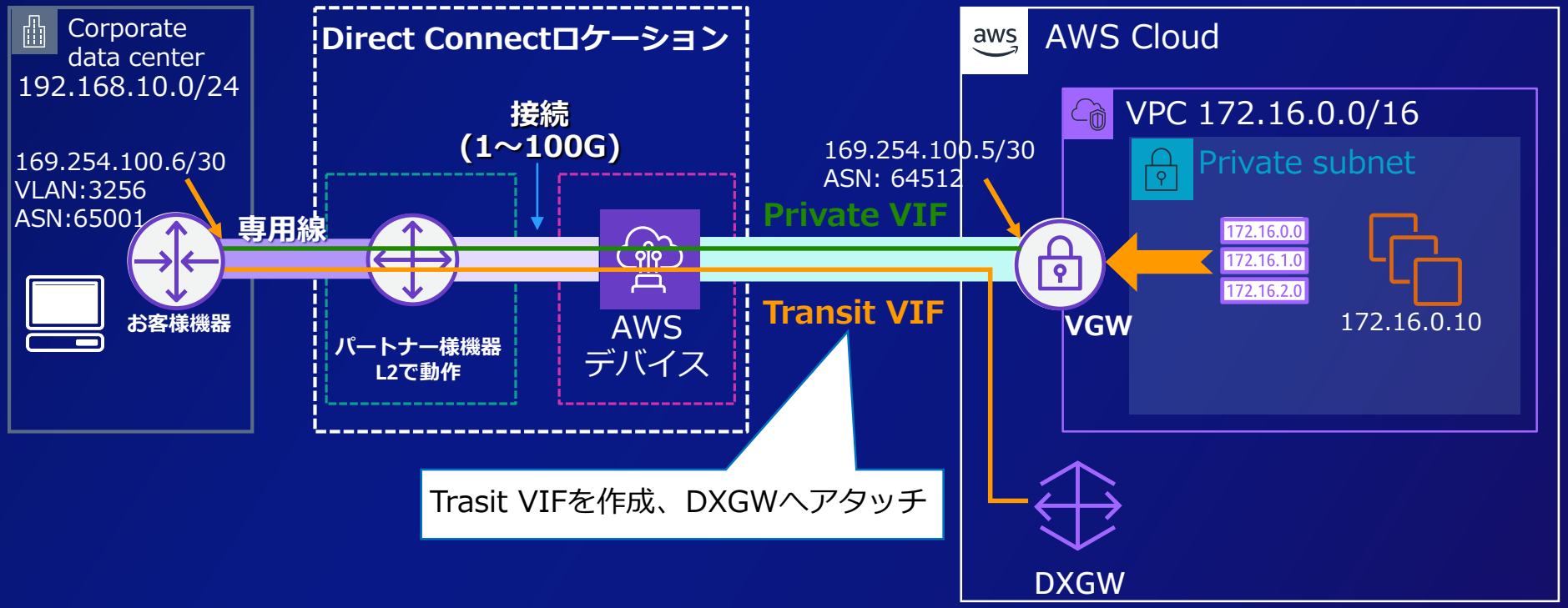
Step:2

- 新たにDirect Connect Gateway(DXGW)を作成する。
- 元の構成がDXGWを利用していた場合でも、使いまわさずに新たなDXGWを作成する。



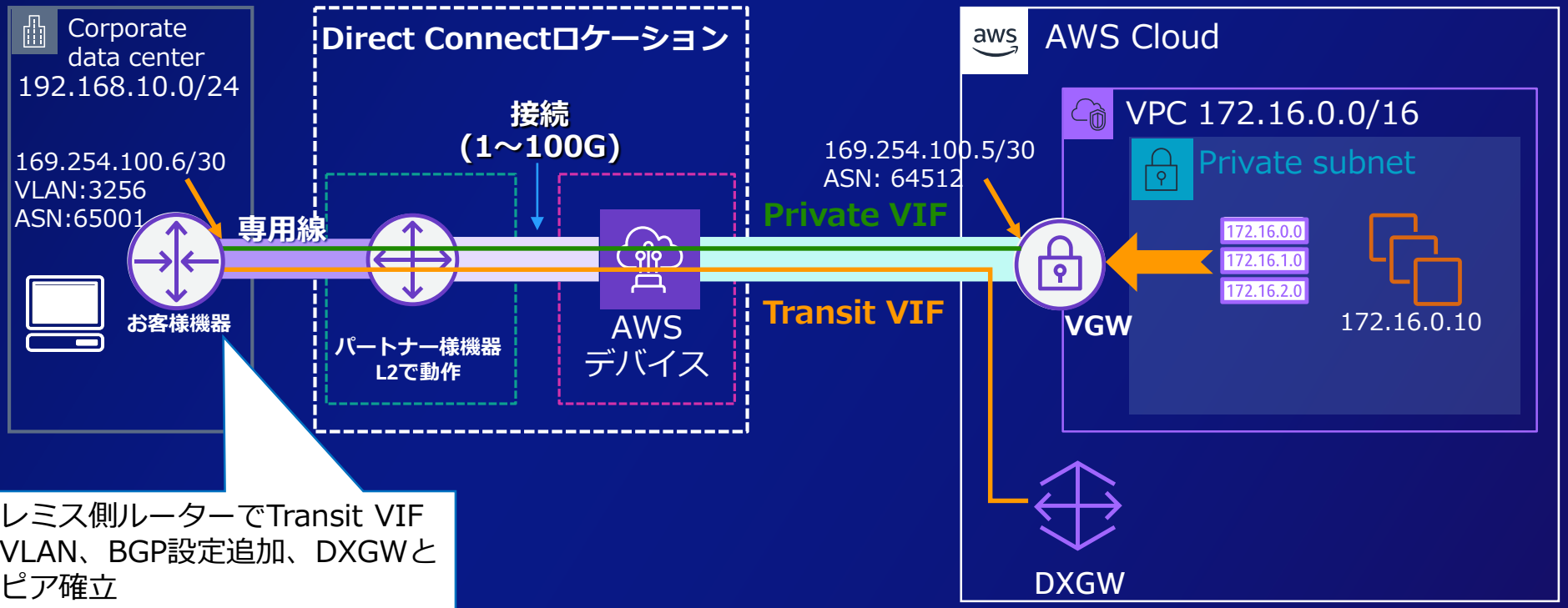
Step:3

- Transit VIFを作成し、DXGWにアタッチする。



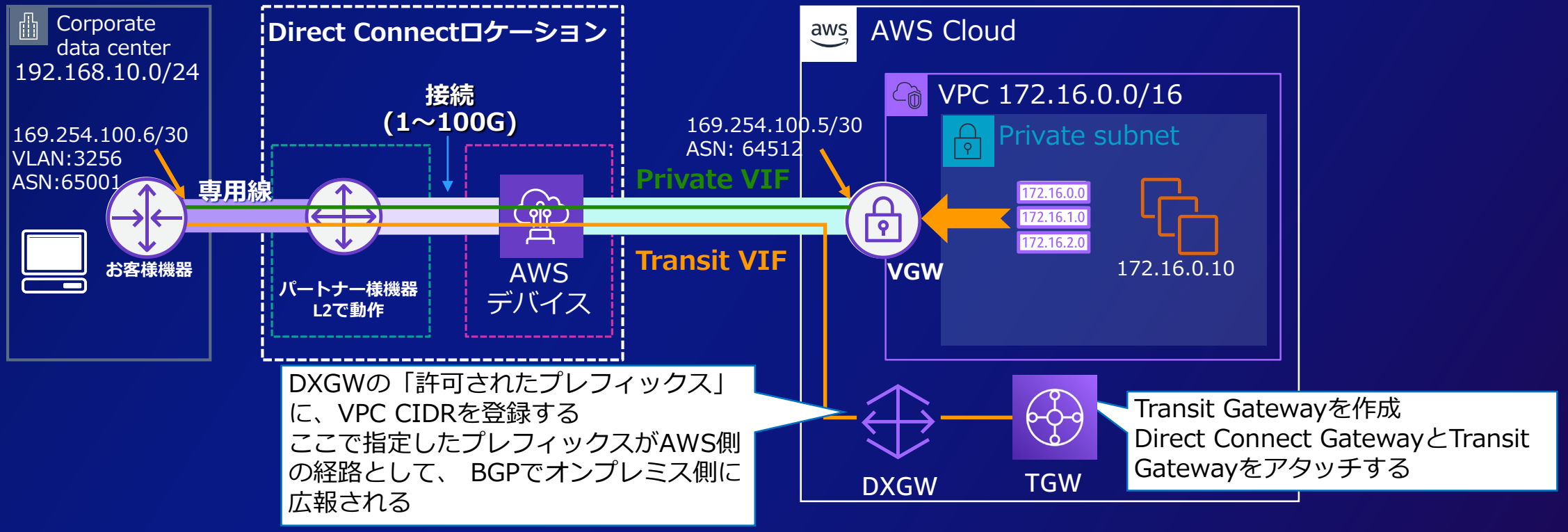
Step:4

- オンプレミス側ルーターにTransit VIF用の設定を投入し、BGPピアをUp状態にする。



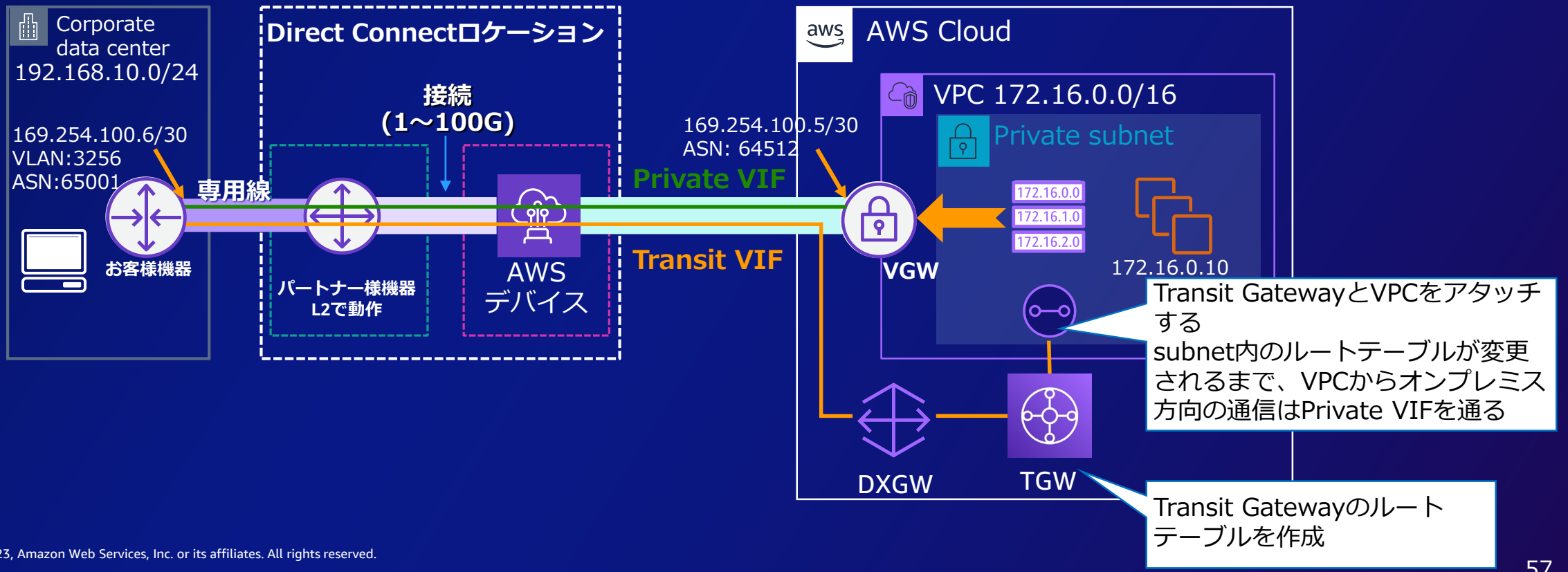
Step:5

- Transit Gateway(TGW)を作成し、DXGWとアタッチする。
- 「許可されたプレフィックス」にはVPC CIDRを登録。必要に応じてCIDRを集約する。同じ経路が広報されるがLocal Preferenceの設定を済ませているので、Private VIFが優先される。



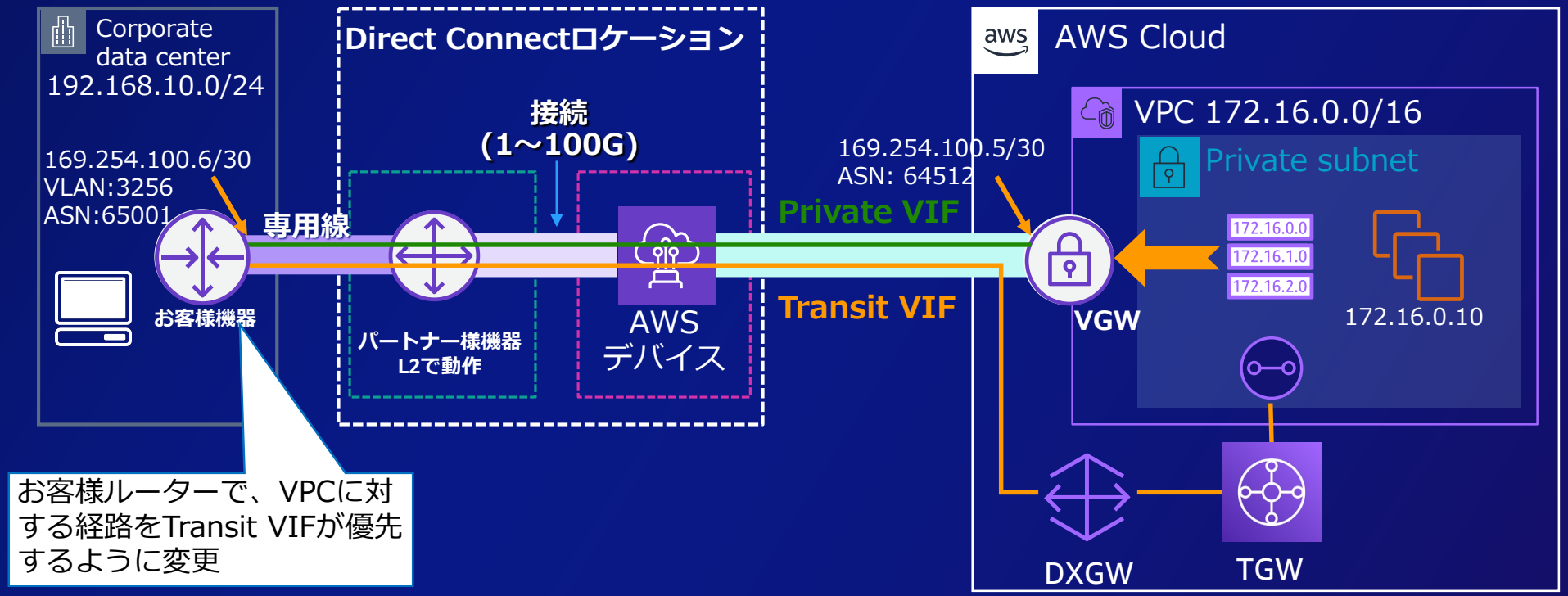
Step:6

- TGWのアタッチメントとしてVPCを指定。TGW側のルートテーブルを作成、VPCアタッチメントをアソシエートする。
- ここまでのStepで切り替え前準備が完了。



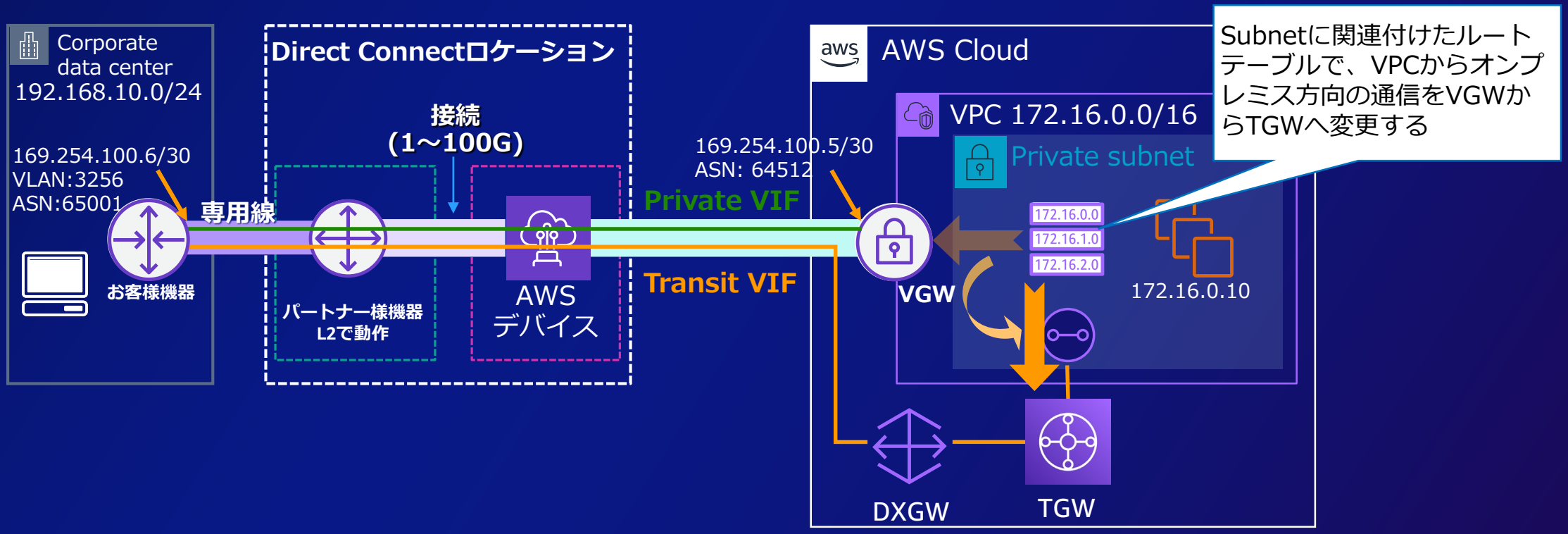
Step:7【切り替え開始】

- お客様ルーターにてLocal Preferenceの設定を変更し、VPC向け経路をTransit VIFへ切り替え。
- この時点で、非対称ルーティング発生。



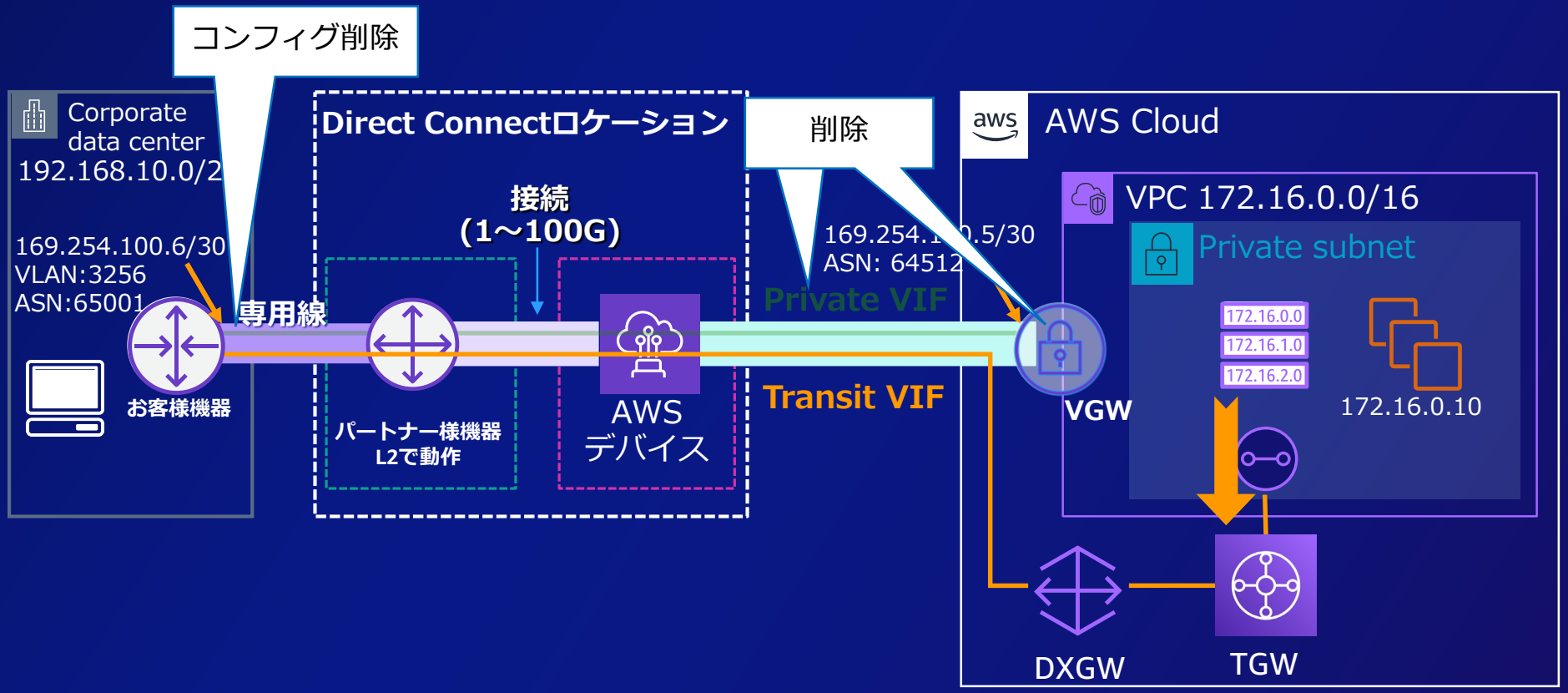
Step:8 【切り替え完了】

- Subnetが参照しているルートテーブルで、オンプレミス向け経路をTGWに変更。
- 全ての通信がTransit Gateway経由に切り替わる。



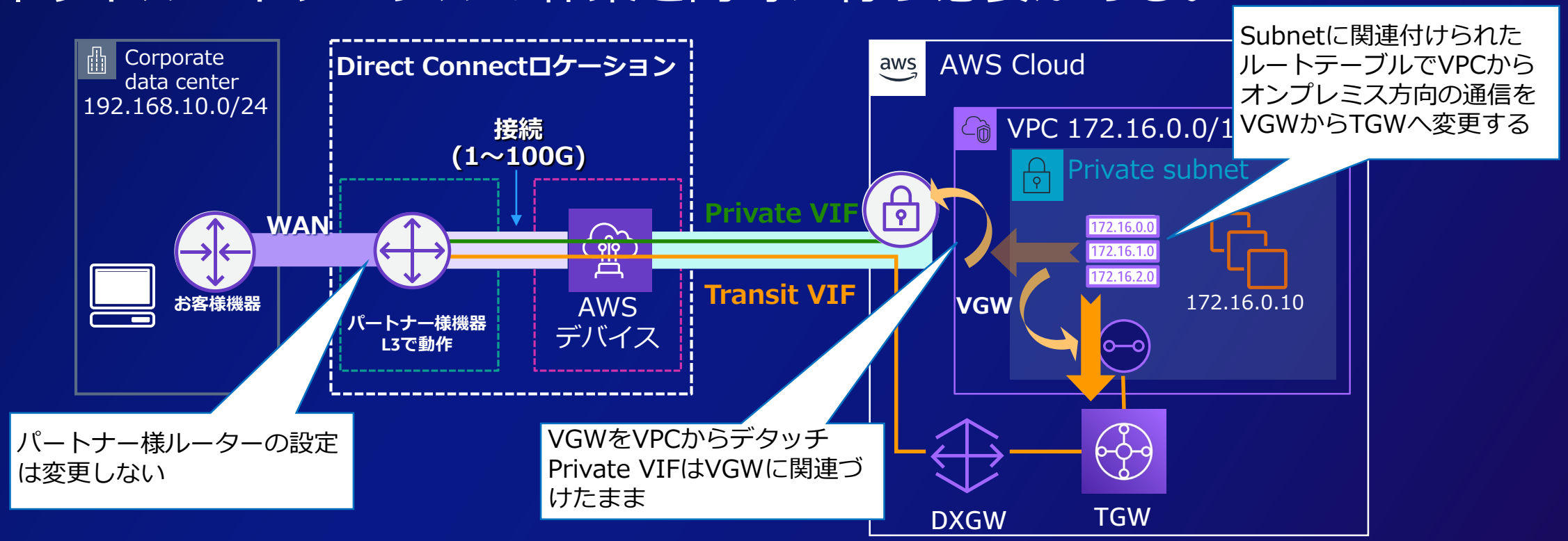
Step:9 【不要リソース削除】

- 通信確認後、不要となったPrivate VIF、VGWを削除。
- オンプレミス側ルーターで、Private VIFに関するコンフィグ削除。



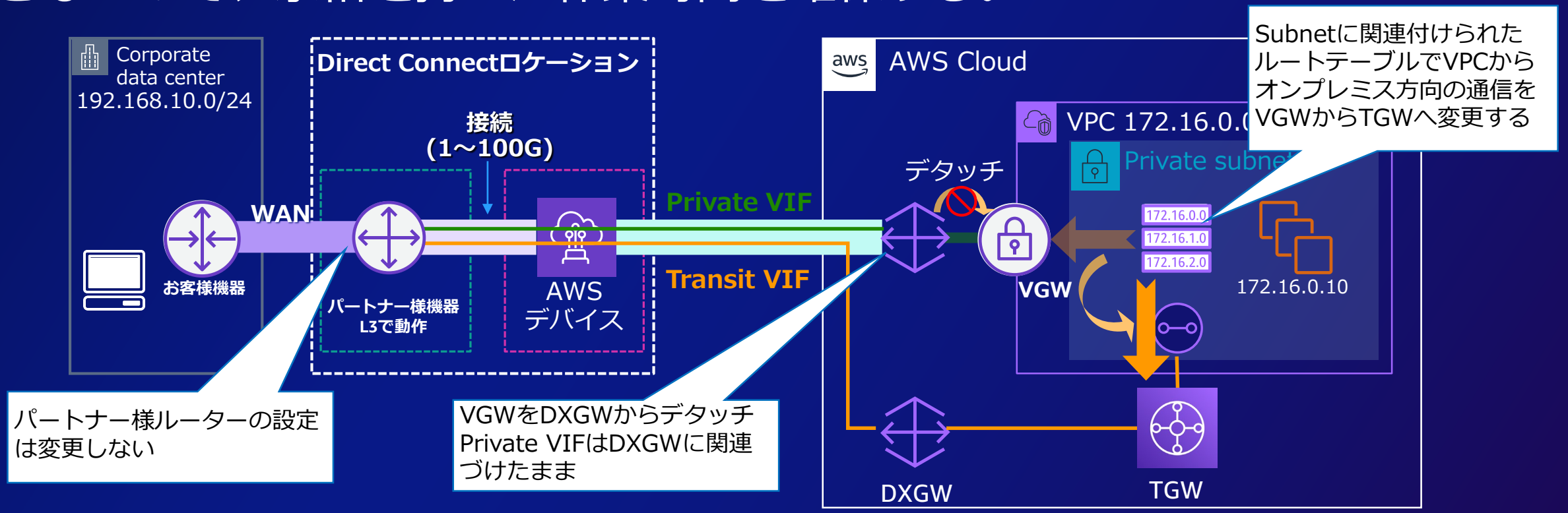
参考①：Step:7/8の代替【切り替え開始】

パートナー様経由の接続を利用時に、お客様ルーターのBGPアトリビュートを変更できない場合、VGWをVPCからデタッチする方法も選択可能。ただし、非対称ルーティングが成立しないため、VPCサブネットルートテーブルの作業を同時に行う必要がある。



参考②：Step:7/8の代替【切り替え開始】

Private VIFをDXGW経由で利用している場合、DXGWからVGWをデタッチすることで、オンプレミスからVPCへの経路を強制的にTransit VIFへ切り替えることが可能。ただし、デタッチに必要な時間は定義できないので、余裕を持った作業時間を確保する。



まとめ

- ✓ 事前準備として、Transit VIF、Direct Connect Gateway、Transit Gatewayを作成、BGPピアを確立する
- ✓ Transit GatewayのVPCアタッチメントを設定するが、Subnetのルートテーブルは切り替え作業まで変更しない
- ✓ 新旧VIFの経路制御：
  - ✓ オンプレミス→VPC = オンプレミス側ルーターのLocal Preference
  - ✓ VPC→オンプレミス = VPC Subnetが参照するルートテーブル
- ✓ 切り替え時の非対称ルーティングが発生するが、AWS側リソースは対応可能（オンプレミス側機器で問題になる可能性あり）
- ✓ パートナーサービス利用の場合、どの手法が採用できるか事前に確認
- ✓ 通信確認後、不要リソースを削除
- ✓ 本番環境の切り替えでは冗長化を考慮した手順を検討

Appendix

A-2. AWSネットワーク関連の情報

AWS アーキテクチャアイコン
https://aws.amazon.com/jp/architecture/icons/

【AWS Tech 再演】AWS のネットワーク設計入門｜AWS Summit Tokyo 2017
https://www.youtube.com/watch?v=pyaiWqjNz-A

Black Belt VPN
https://pages.awscloud.com/rs/112-TZM-766/images/202110_AWS_Black_Belt_Site-to-Site_VPN.pdf

Black Belt Direct Connect
https://pages.awscloud.com/rs/112-TZM-766/images/20210209-AWS-Blackbelt-DirectConnect.pdf

Black Belt Transit Gateway
https://pages.awscloud.com/rs/112-TZM-766/images/20210209-AWS-Blackbelt-DirectConnect.pdf