
aws
INNOVATE
ONLINE CONFERENCE

aws INNOVATE
ONLINE CONFERENCE

多くの選択肢が揃ってきた「オンプレミスとVPC間の接続方法」を整理してみる

菊地 信明
アマゾン ウェブ サービス ジャパン
技術本部 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

門田 梓
アマゾン ウェブ サービス ジャパン
技術本部 ソリューションアーキテクト

Agenda

本セッションの狙い

はじめに

オンプレミスとVPCの接続パターン

1. 拠点からインターネット経由でVPCに接続
2. 複数拠点からセキュアにVPCに接続
3. 拠点からシステム毎に異なるVPCに接続
4. 共通リソースをAWS上に集約

まとめ

オンプレミスとVPCの接続パターン

1. 拠点からインターネット経由でVPCに接続
   → 最も容易だが、通信要件に合わせて暗号化を利用
2. 複数拠点からセキュアにVPCに接続
   → Direct ConnectとVPNを併用してメリハリのある構成
3. 拠点からシステム毎に異なるVPCに接続
   → Direct Connect Gatewayでシステム毎のVPCへ接続
4. 共通リソースをAWS上に集約
   → Transit Gatewayで経路を集中管理、柔軟な経路設計

本セッションの狙い

- 本セッションは、AWS利用を検討されている方や、すでにAWSのご利用を開始している方で、オンプレミスからVPCへの接続を最適化したい要件をお持ちの方などを対象にしています。

- すでに閉域網を利用してVPCへ接続している方で、利用拡張に備えて新サービスへの移行を検討されている方にも、参考となる情報をお伝えしていきます。

対象サービス

各種VPN、Direct Connect、そして、昨年のre:Inventで発表されたTransit Gatewayを取り扱います。

これらのサービスを活用し、オンプレミスとAWS VPCを接続する手段を中心にご説明させていただきます。

各サービスの詳細な設定方法については、各公式ドキュメントを参照ください。

はじめに

aws INNOVATE
ONLINE CONFERENCE

オンプレミスとVPCを接続するサービス一覧


Amazon VPC


AWS Direct Connect


AWS Transit Gateway


AWS Site-to-Site VPN


AWS Client VPN


Router


Direct Connect gateway


Customer gateway


Internet gateway


AWS PrivateLink


NAT gateway


Peering


VPN connection


VPN gateway

Security group

Availability Zone

選択肢がたくさんあってよくわからない...😟😟😟

オンプレミスとVPCを接続するサービス一覧


Amazon VPC


AWS Direct Connect


AWS Transit Gateway


AWS Site-to-Site VPN


AWS Client VPN


Router


Direct Connect gateway


Customer gateway


Internet gateway


AWS PrivateLink


NAT gateway


Peering


VPN connection


VPN gateway

Security group

Availability Zone

整理しましょう😀👍

aws

オンプレミスとVPCの接続パターン

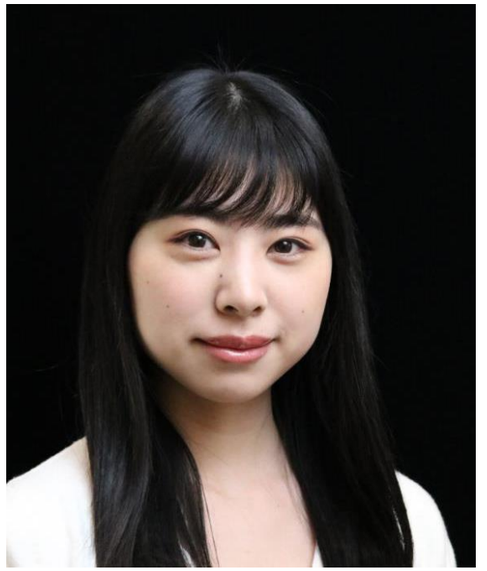
aws INNOVATE
ONLINE CONFERENCE

オンプレミスとVPCの接続パターン

1. 拠点からインターネット経由でVPCに接続
2. 複数拠点からセキュアにVPCに接続
3. 拠点からシステム毎に異なるVPCに接続
4. 共通リソースをAWS上に集約

自己紹介

門田　梓（かどた　あずさ）



所属

技術統括本部ソリューションアーキテクト

経歴

ネットワーク機器メーカーのプリセールスエンジニア

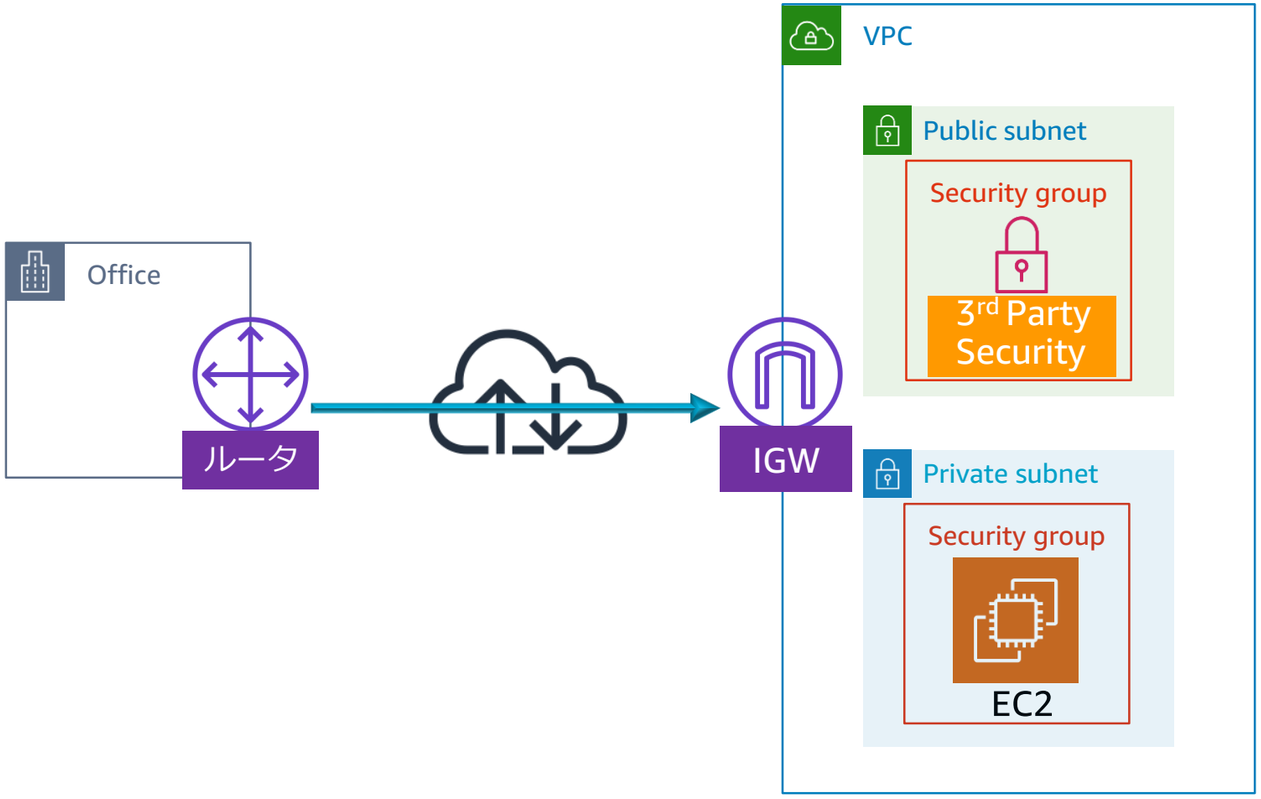
好きなAWSサービス

AWS Media Services, VPC

拠点からインターネット経由でVPCに接続

aws INNOVATE
ONLINE CONFERENCE

拠点からインターネット経由でVPCに接続



通信要件

- 通信要件が特にない
- リモートからVPC上のリソースにアクセスできればよい

メリット

- 安価
- どこからでも接続可能

デメリット

- 別途セキュリティ対策が必要

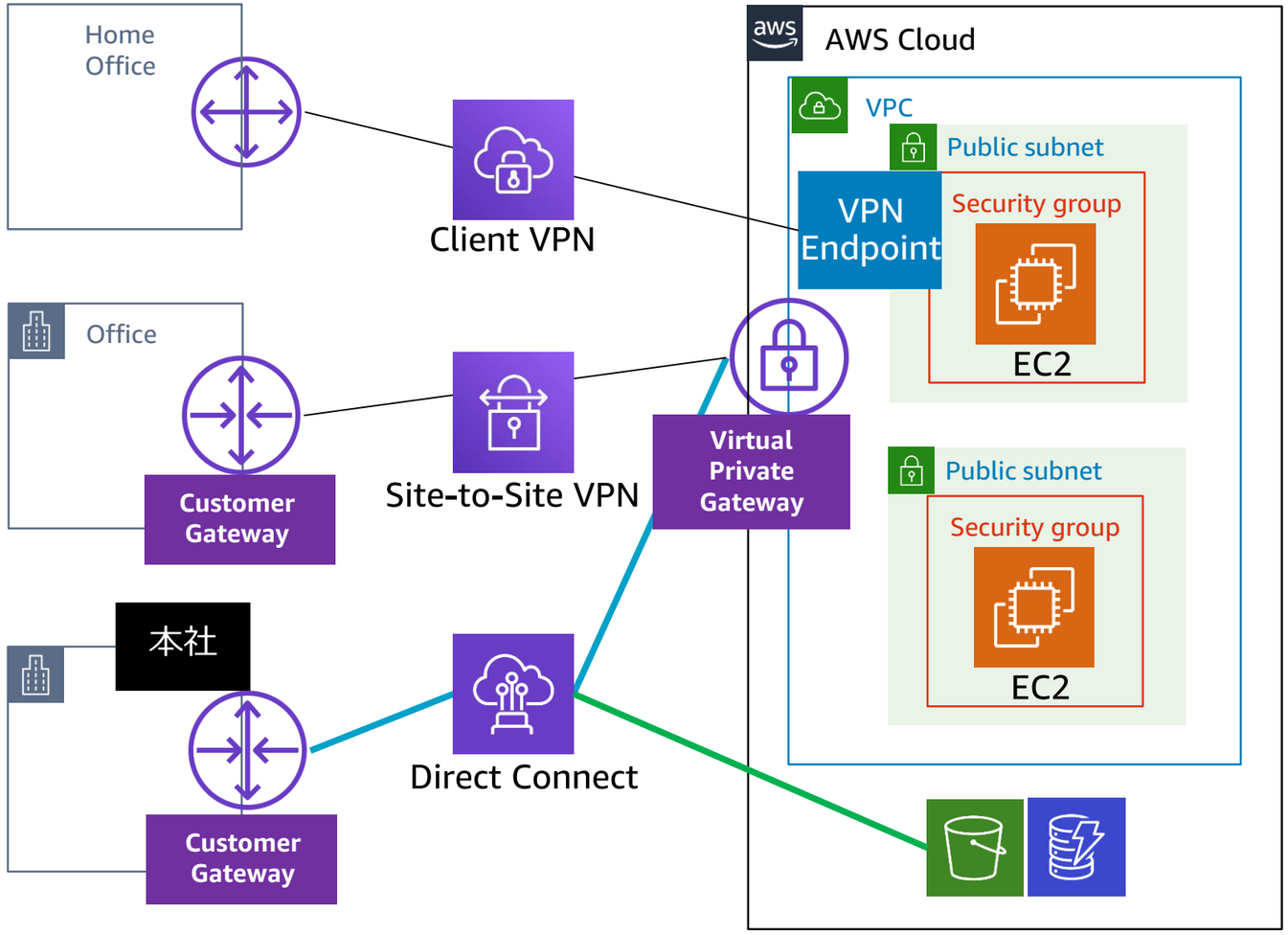
ポイント

- パブリックサブネットは最低限に
- セキュリティグループを設定
- 必要に応じてアプリケーションで暗号化

複数拠点からセキュアにVPCに接続

aws INNOVATE
ONLINE CONFERENCE

複数拠点からセキュアにVPCに接続



通信要件

- セキュアなサイト間接続
- 拠点間通信
- 回線の冗長化

サービス

- **Client VPN**
- **Site-to-Site VPN**
- **Direct Connect**
- **CloudHub**

Client VPN

お客様のクライアントをOpen VPNベースのVPNを介してAWSへプライベートに接続するサービス

ユースケース

- 自宅や出張先からアクセスしたい

ポイント

- Active Directory を使用したクライアント認証と証明書ベースの認証をサポート
- VPCから他のVPC、AWSの各種サービス、オンプレミス、インターネットにシームレスにアクセス

Site-to-Site VPN

お客様のデータセンターやオフィスをIPsec VPNを介してAWSへプライベートに接続するサービス

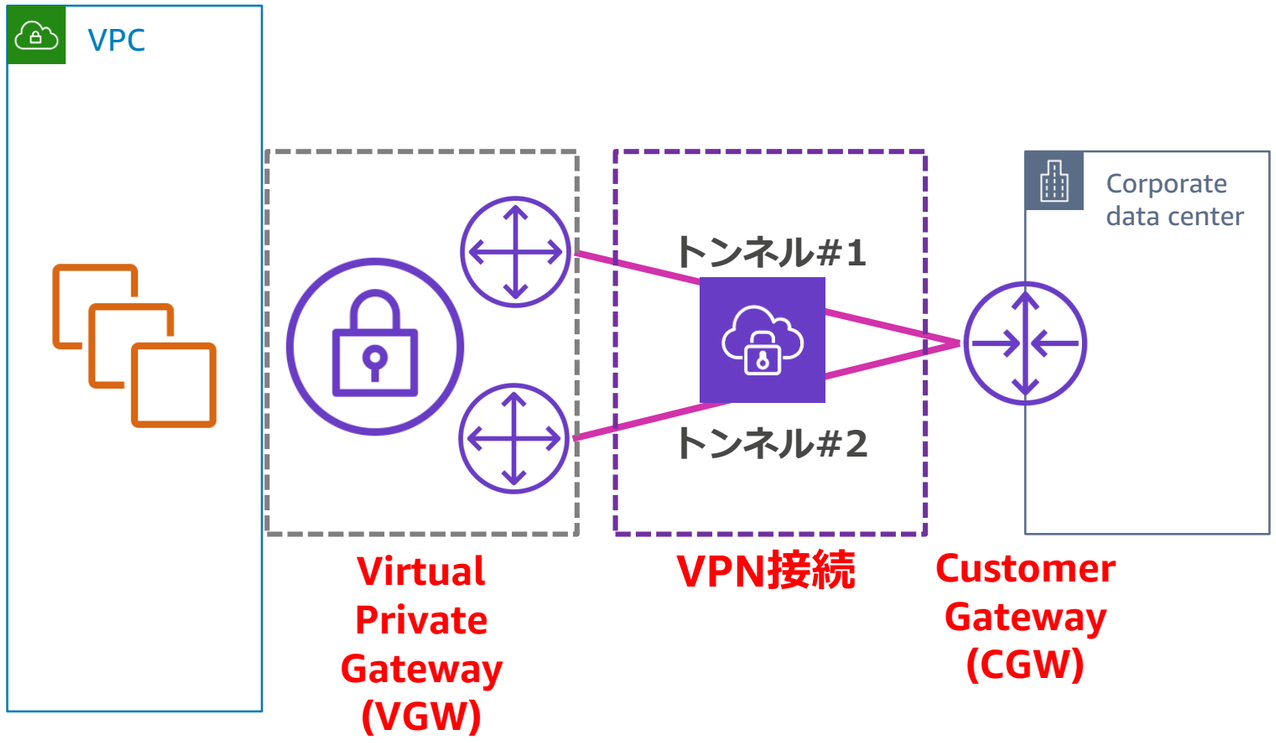
種類

- Classic VPNとAWS VPN
  - （Classic VPNからAWS VPNへの移行については補足参照）
- AWS VPNはVirtual Private GatewayもしくはTransit Gatewayと接続

ユースケース

- 拠点とAWSを簡単に早く接続したい
- 少量のトラフィック
- 価格重視/スモールスタート
- バックアップ回線

Site-to-Site VPNの接続構成



ポイント

- 1つのVPN接続は2つのIPsecトンネルで冗長化
- ルーティングは
  静的(スタティック)
  動的(ダイナミック:BGP)
  が選択可能
- VGWはDirect Connectのエンドポイントとしても利用
- IKEv2対応

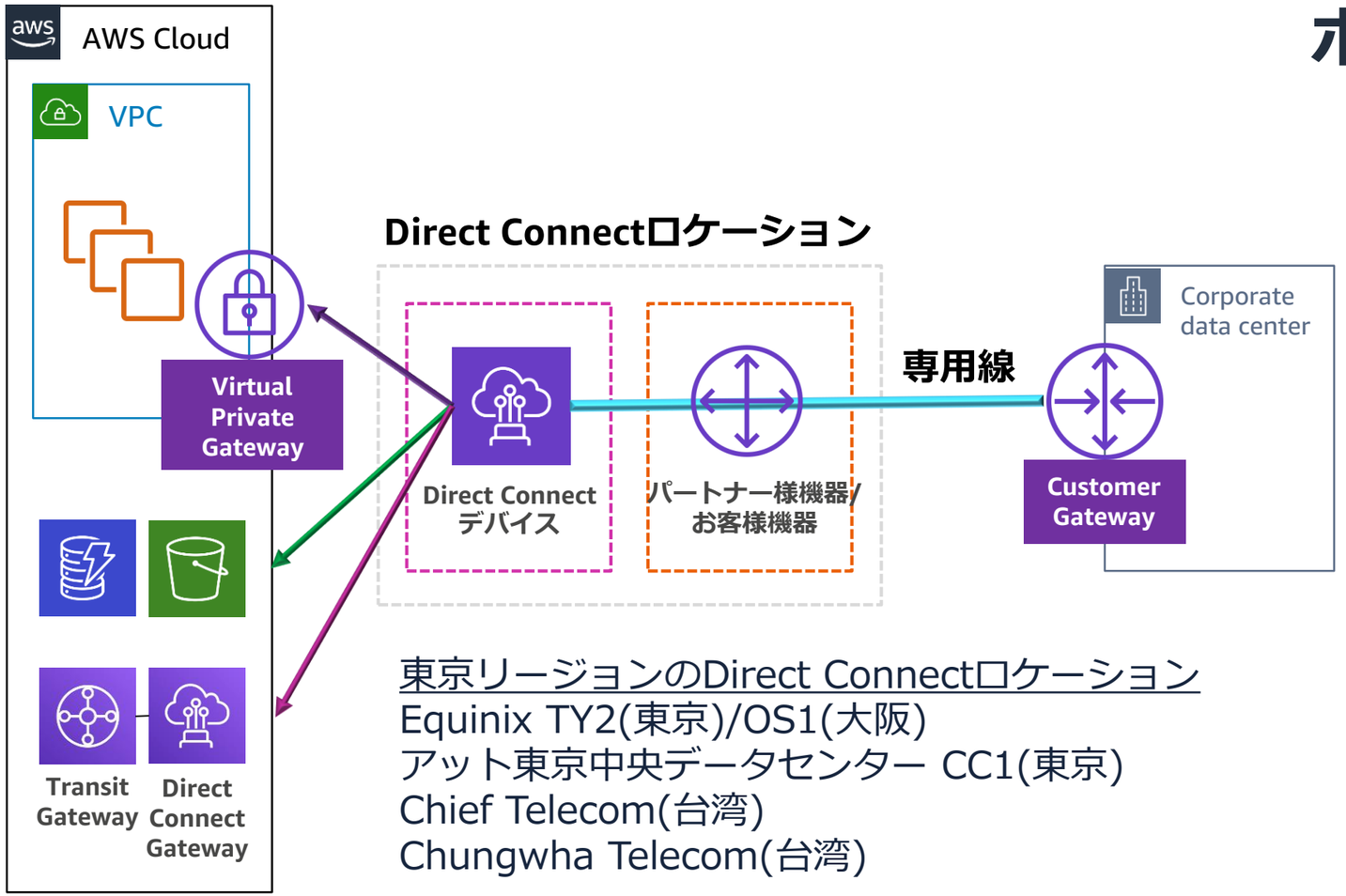
Direct Connect

お客様のデータセンターやオフィスを専用線を介してAWSへプライベートに接続するサービス

ユースケース

- 安定したパフォーマンスが必要
- 閉域網での接続が必要
- 大量のトラフィック
- 主回線
- 一貫性のある管理を実現したい

Direct Connectの接続構成



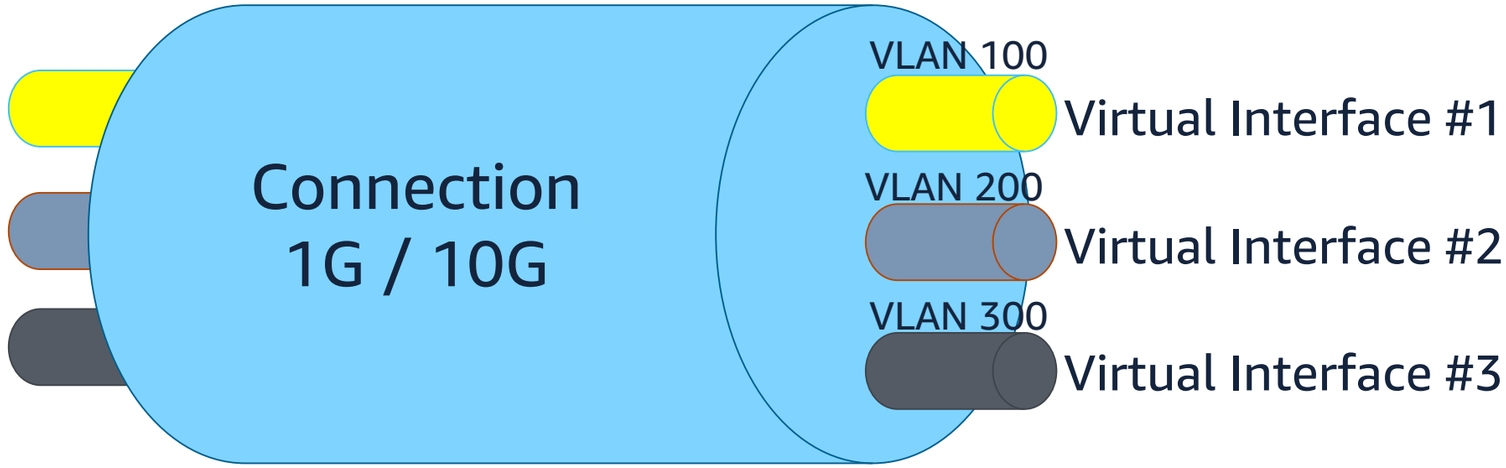
東京リージョンのDirect Connectロケーション
Equinix TY2(東京)/OS1(大阪)
アット東京中央データセンター CC1(東京)
Chief Telecom(台湾)
Chungwha Telecom(台湾)

ポイント

- オンプレミスから専用線を介して Direct Connect ロケーションに接続
- Direct Connect ロケーション ＝AWSクラウドへの物理的な接続を提供する拠点
- 物理接続を“Connections”、または ”接続“と呼ぶ
- Connectionは1Gbpsまたは10Gbpsのポート速度をサポート
- ルーティングはBGPのみ
- 接続先は以下の3つ
  VPC(プライベート接続)
  AWSクラウド(パブリック接続)
  TGW用のDXGW(トランジット接続)

仮想インターフェース（Virtual Interface=VIF）

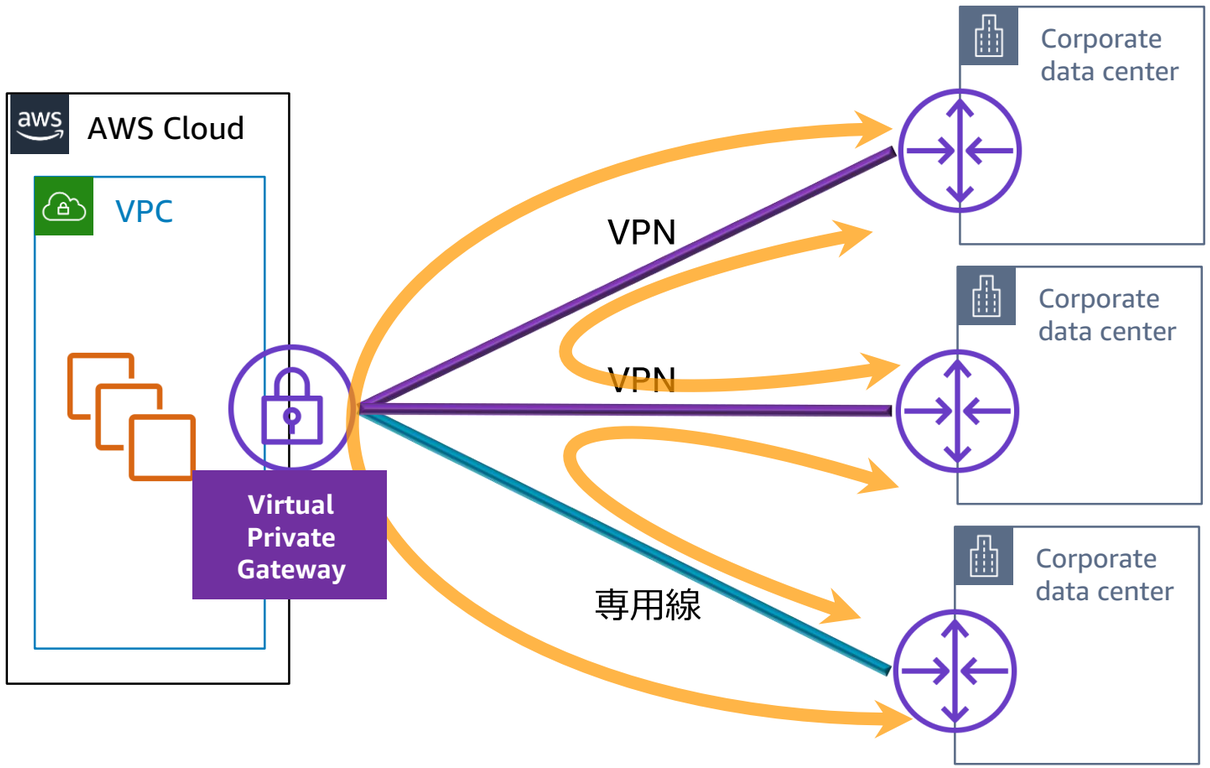
Connection = 物理接続（1G or 10G）
VIF = Connectionを通してAWSリソースにアクセスするための論理インタフェース
- AWSとお客様ルータの間でBGPピアを確立し経路を交換
- VLAN IDを持つ



- VPCへプライベートアドレスを介した接続を提供するのが**Private VIF**
- AWSの全リージョンへパブリックIPを介した接続を提供するのが**Public VIF**
- Transit Gateway用のDirect Connect Gatewayへの接続を提供するのが**Transit VIF**
- 同一Connection上にPublic VIF、Private VIF、Transit VIFの混在が可能

CloudHubによるサイト間通信

複数のSite-to-Site VPN/Direct Connect接続がある場合、AWS VPN CloudHubを使用してサイト間の相互通信を実現



ユースケース

- 本社、支社、データセンター間での通信（ハブアンドスポーク構成）

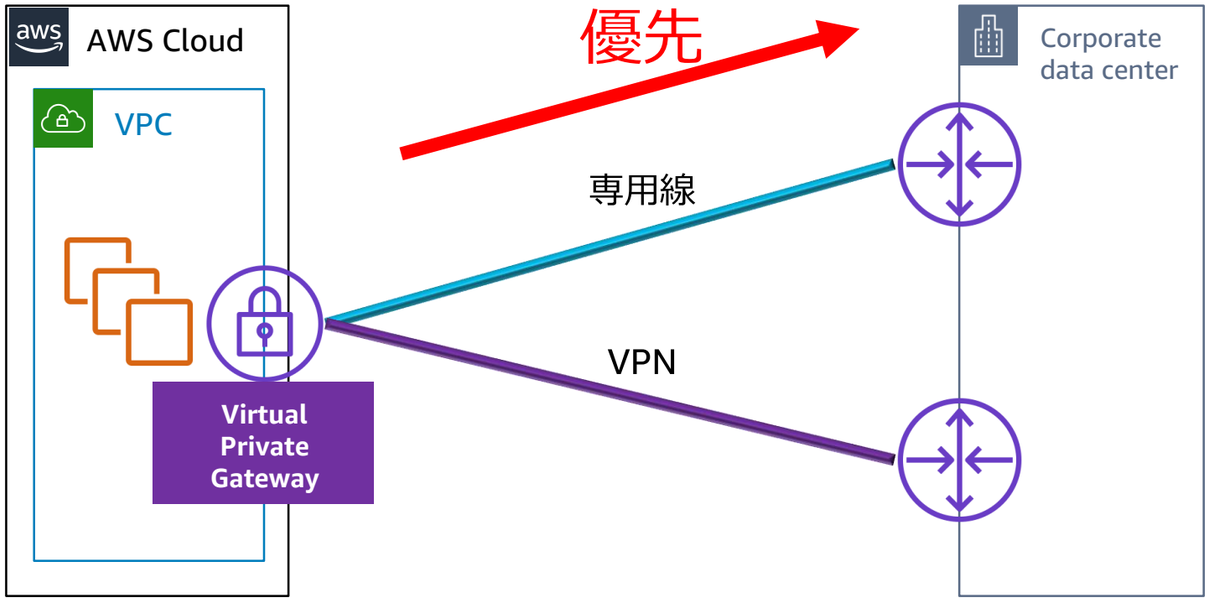
ポイント

- 一つのCloudHubにVPNとDirect Connectを含めることが可能
- 一つのVPCに割り当て
- サイト間での IP 範囲の重複不可
- Direct Connect Gatewayでは非対応

Site-to-Site VPNと専用線の比較

	Site-to-Site VPN	専用線
コスト	安価なベストエフォート回線も利用可能	キャリアの専用線サービスの契約が必要
リードタイム	即時~	数週間~
帯域	暗号化のオーバーヘッドにより制限あり	ポート当たり1G/10Gbps/LAG可能
品質	インターネットベースのため経路上のネットワーク状態の影響を受ける	キャリアにより高い品質が保証されている
障害時の切り分け	インターネットベースのため自社で保持している範囲以外での切り分けが難しい	エンドツーエンドでどの経路を利用しているか把握できているため比較的容易

Site-to-Site VPNと専用線の冗長化



ポイント

- VPCから見たOutboundは必ずDirect Connectが優先される
  - VPNを優先したい場合はVPNルータからDirect Connectより長いPrefixを広告
- VPNとDirect Connectを終端しているルータが別々の場合、両ルータはiBGPによる接続が必要

自己紹介

菊地 信明（きくち のぶあき）

所属

技術統括本部　レディネス＆テックソリューション本部
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
私鉄系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

役割

AWSを利用したネットワーク設計のお手伝い
新サービスの利用提案

好きなAWSサービス

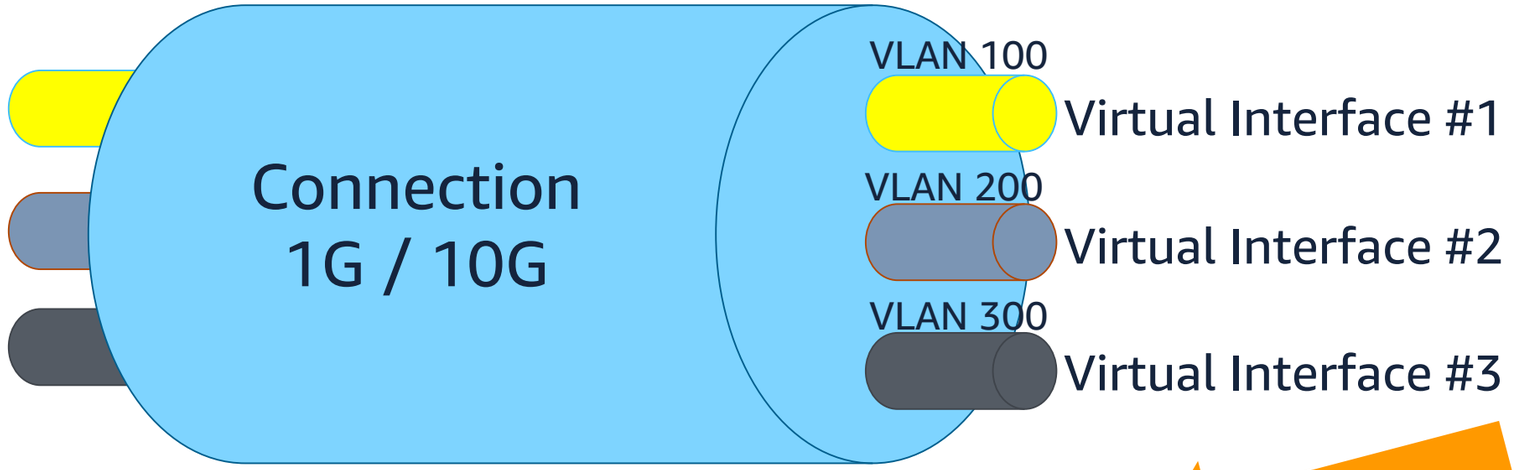
Amazon Direct Connect／AWS VPN／Amazon Route 53

3. 拠点からシステム毎に異なるVPCに接続

aws INNOVATE
ONLINE CONFERENCE

仮想インターフェース（Virtual Interface=VIF）(再掲)

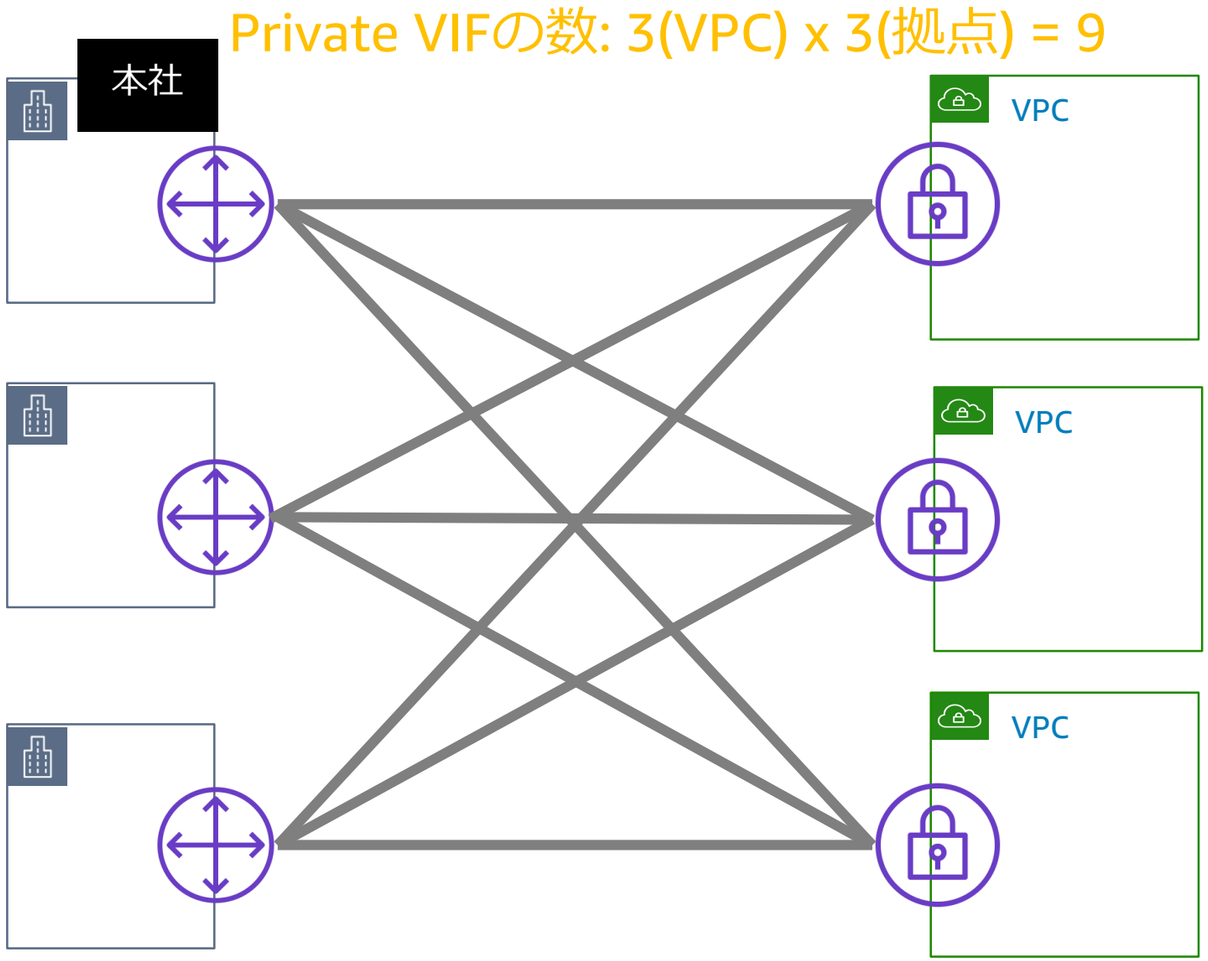
Connection = 物理接続（1G or 10G）
VIF = Connectionを通してAWSリソースにアクセスするための論理インタフェース
- AWSとお客様ルータの間でBGPピアを確立し経路を交換
- VLAN IDをもつ



- VPCへプライベートアドレスを介した接続を提供するのが**Private VIF**
- AWSの全リージョンへパブリックIPを介した接続を提供するのが**Public VIF**
- TransitゲートウェイとDirect Connectゲートウェイの接続を提供するのが**Transit VIF**
- 同一Connection上にPublic VIF、Private VIF、Transit VIFの混在が可能

拠点からシステム毎に異なるVPCに接続

オンプレミスから複数のVPCへアクセスするため、メッシュ型にVIFを利用
管理者が異なる複数のVPCに対し、それぞれのオンプレミス環境からアクセス



通信要件：Direct Connectを効率よく活用し、異なるAWSアカウントが管理する複数のVPCへオンプレミスから通信する

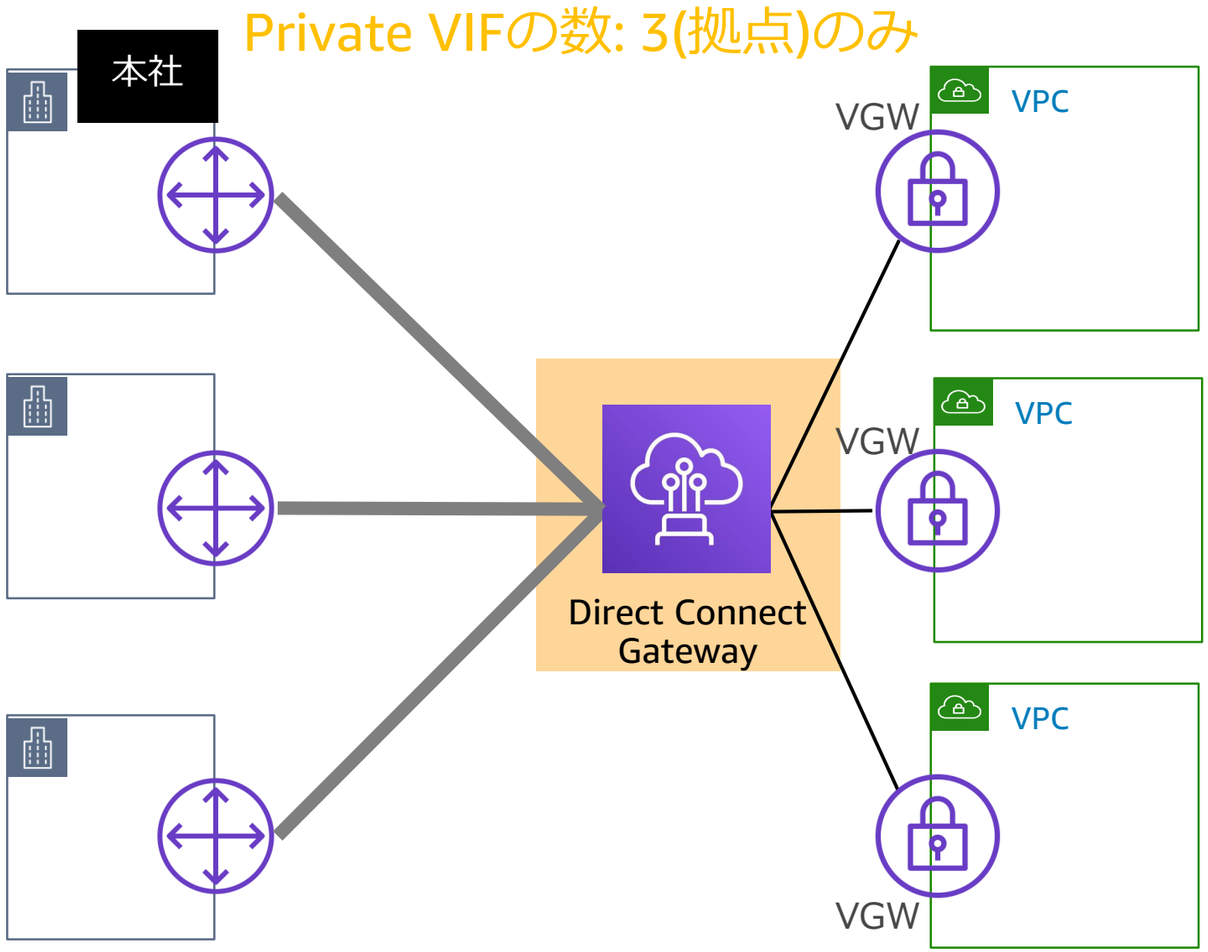
AWS Direct Connect Gateway

オンプレミスネットワークとVPCの間をよりスケーラブルに

aws INNOVATE
ONLINE CONFERENCE

拠点からシステム毎に異なるVPCに接続

オンプレミスから複数のVPCへ効率的にアクセス
管理者が異なるVPCに対しても、アクセス可能

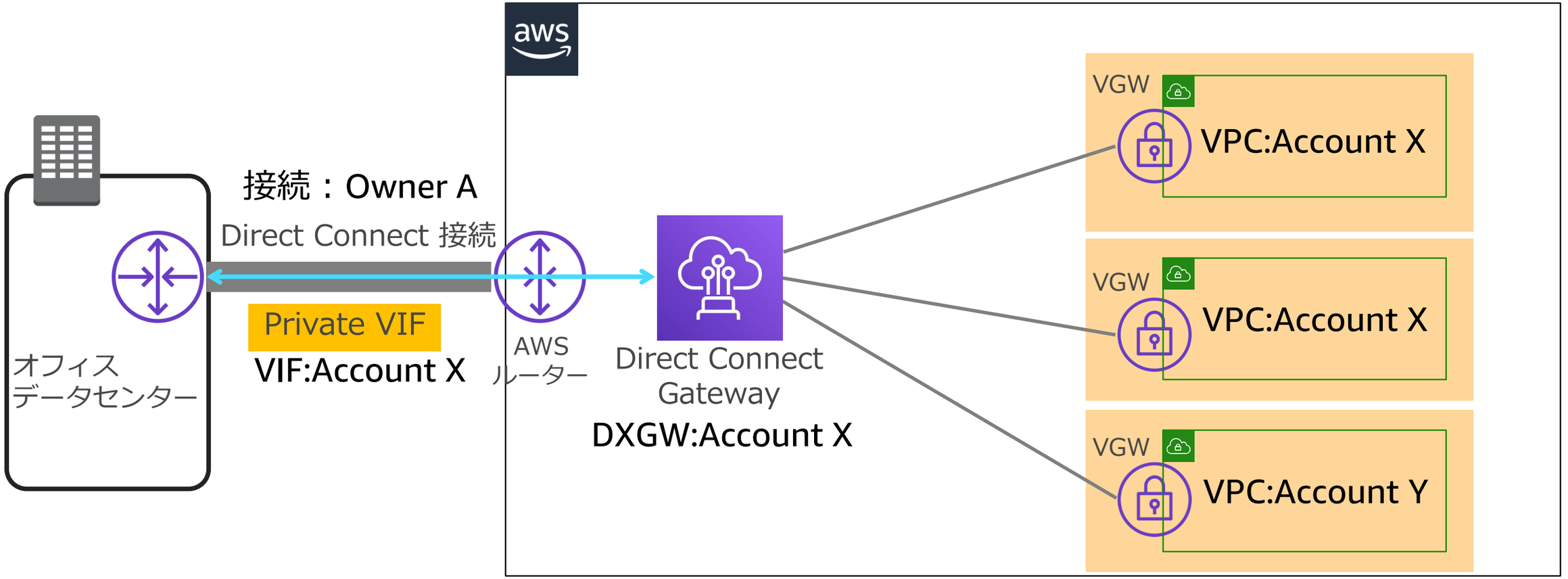


通信要件：Direct Connectを効率よく活用し、異なるAWSアカウントが管理する複数のVPCへオンプレミスから通信する

サービス：Direct Connect Gateway

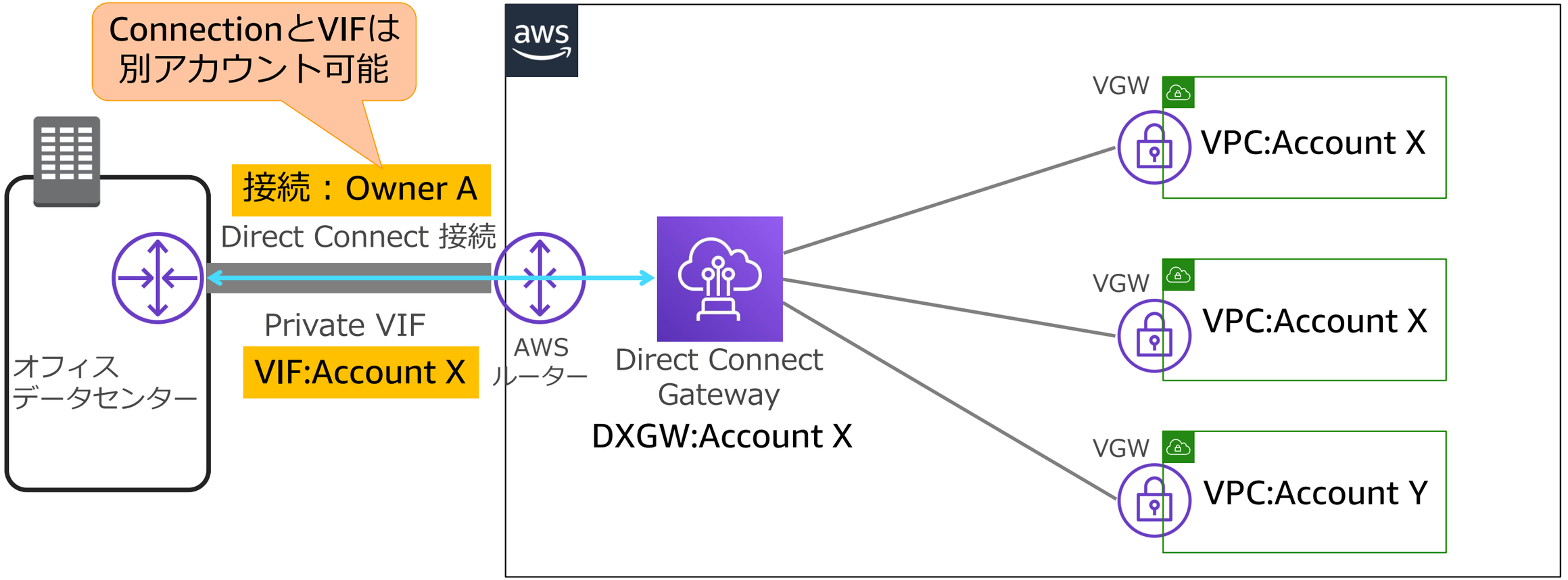
Direct Connect Gateway ユースケース

オンプレミスから複数のVPCに対し、プライベート仮想インターフェイス(VIF)を利用して容易に接続



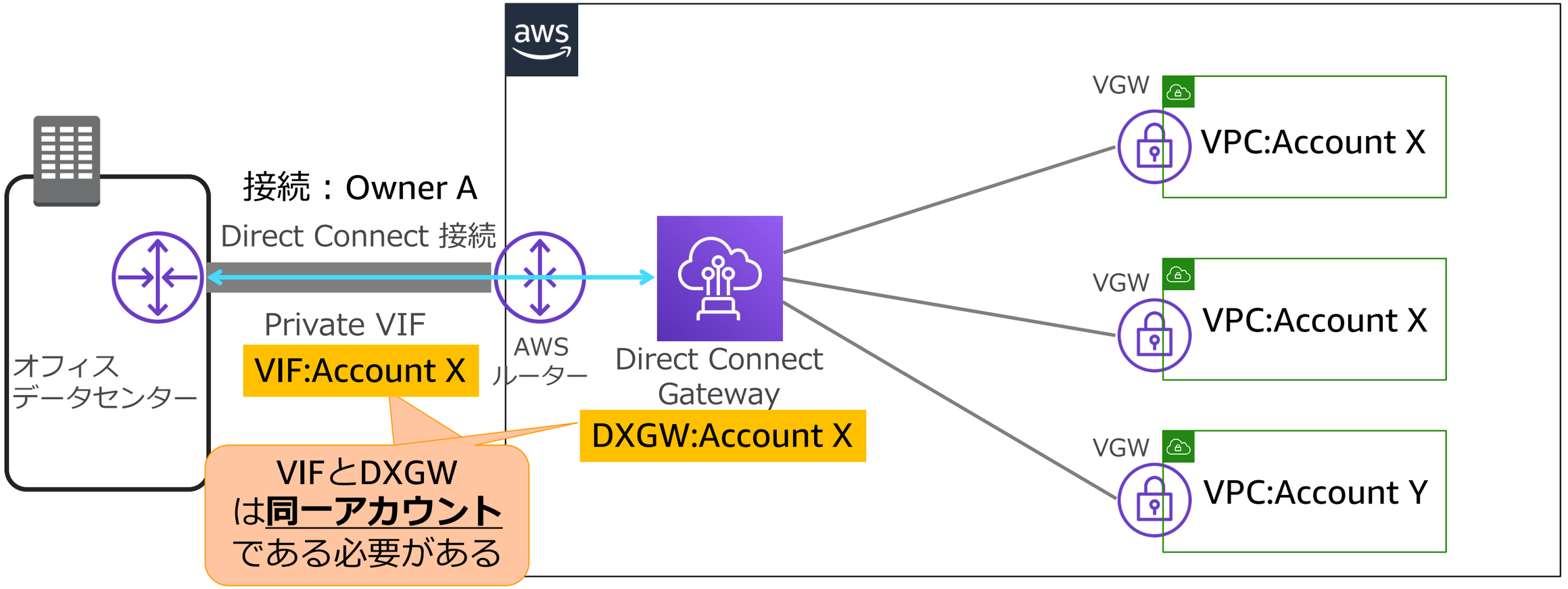
Direct Connect Gateway ユースケース

接続(Connection)と仮想インターフェイス(VIF)は、別のAWSアカウントが管理する事が可能



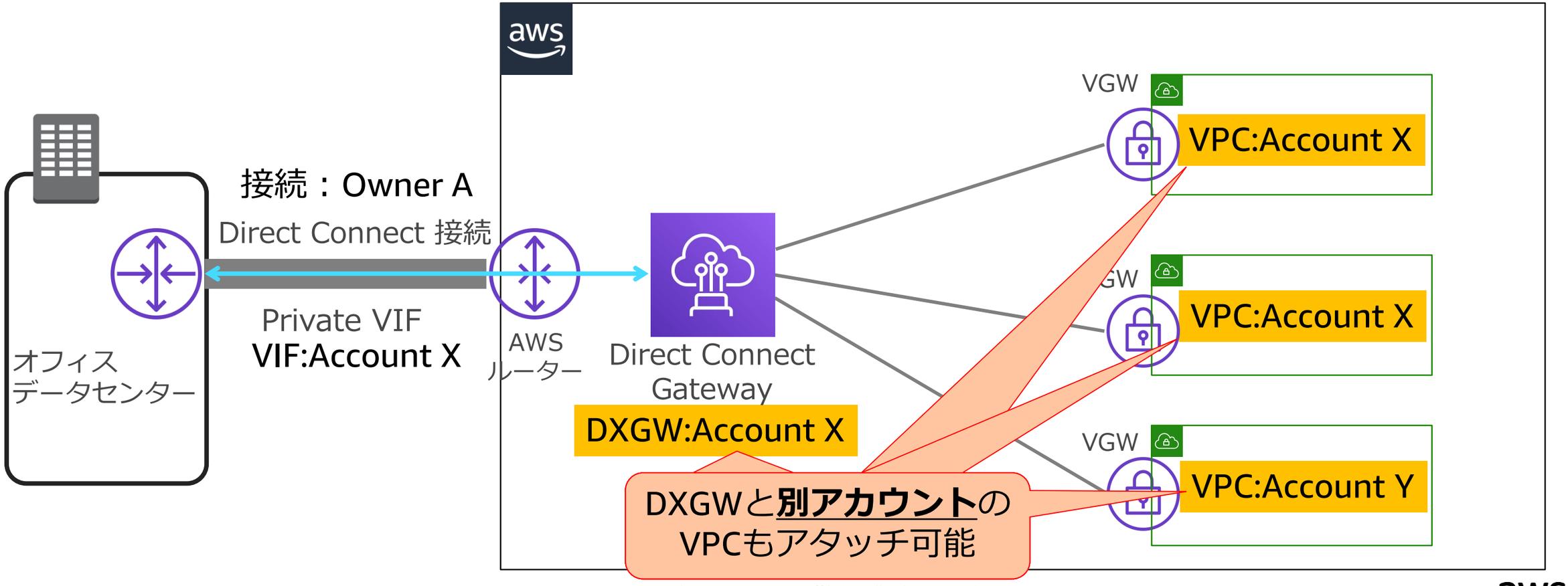
Direct Connect Gateway ユースケース

VIFとDirect Connect Gatewayは同一アカウントが所有している必要がある



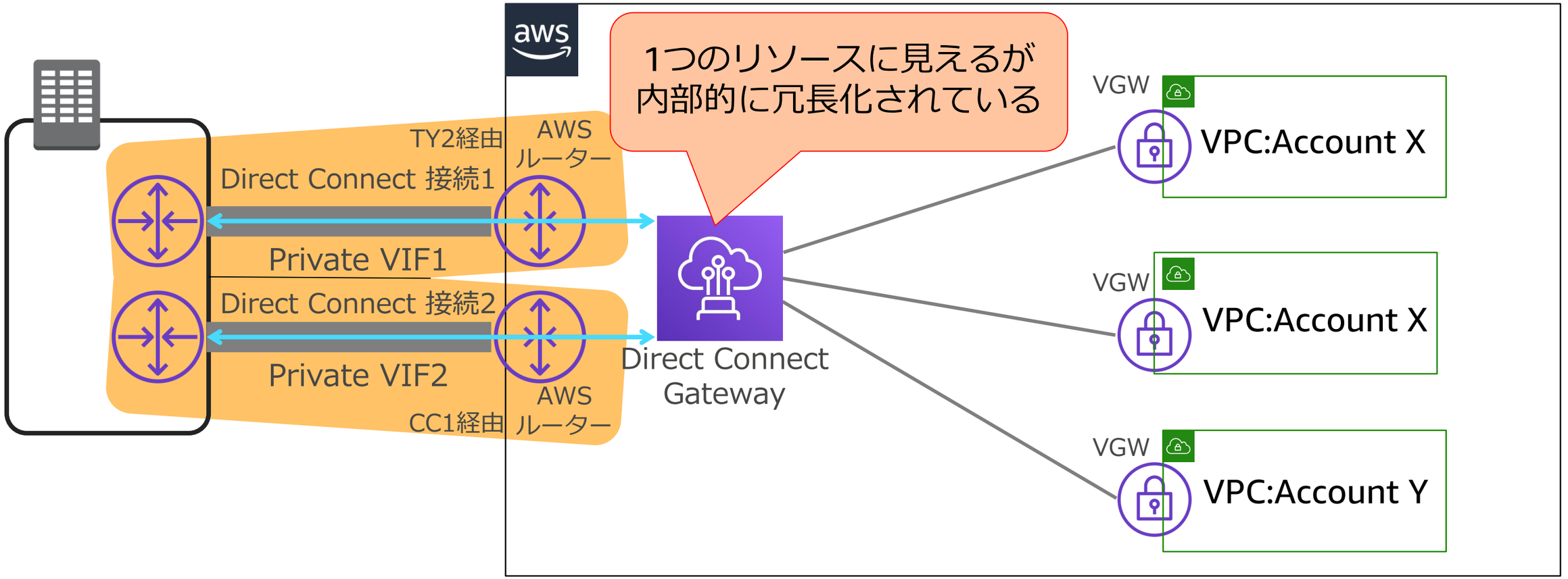
Direct Connect Gateway ユースケース

Direct Connect GatewayとVPCは~~同一支払いアカウントであれば~~、
別のアカウントでもアタッチ可能（2019/10/4 制限削除）



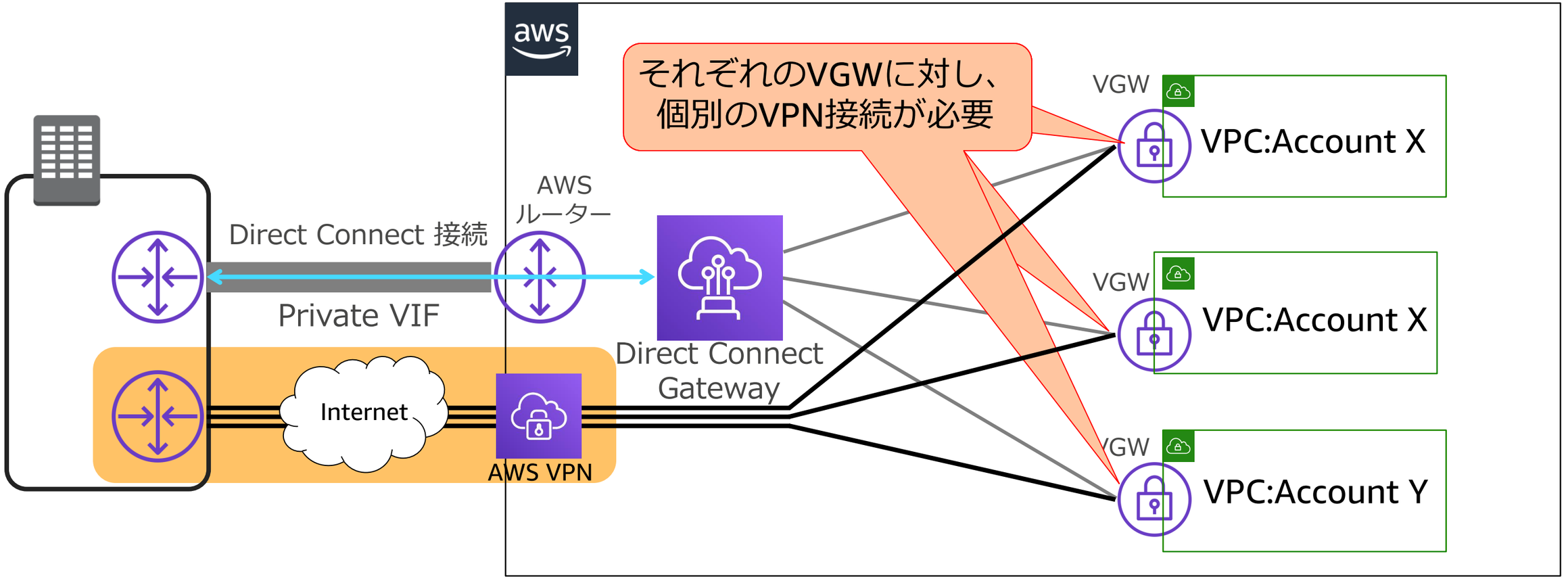
Direct Connect Gateway: 冗長化 Private VIF x 2

2つ目の接続を異なるロケーションに配置、Private VIFを追加し、同一のDirect Connect Gatewayへアタッチする事で、単一障害点を無くす



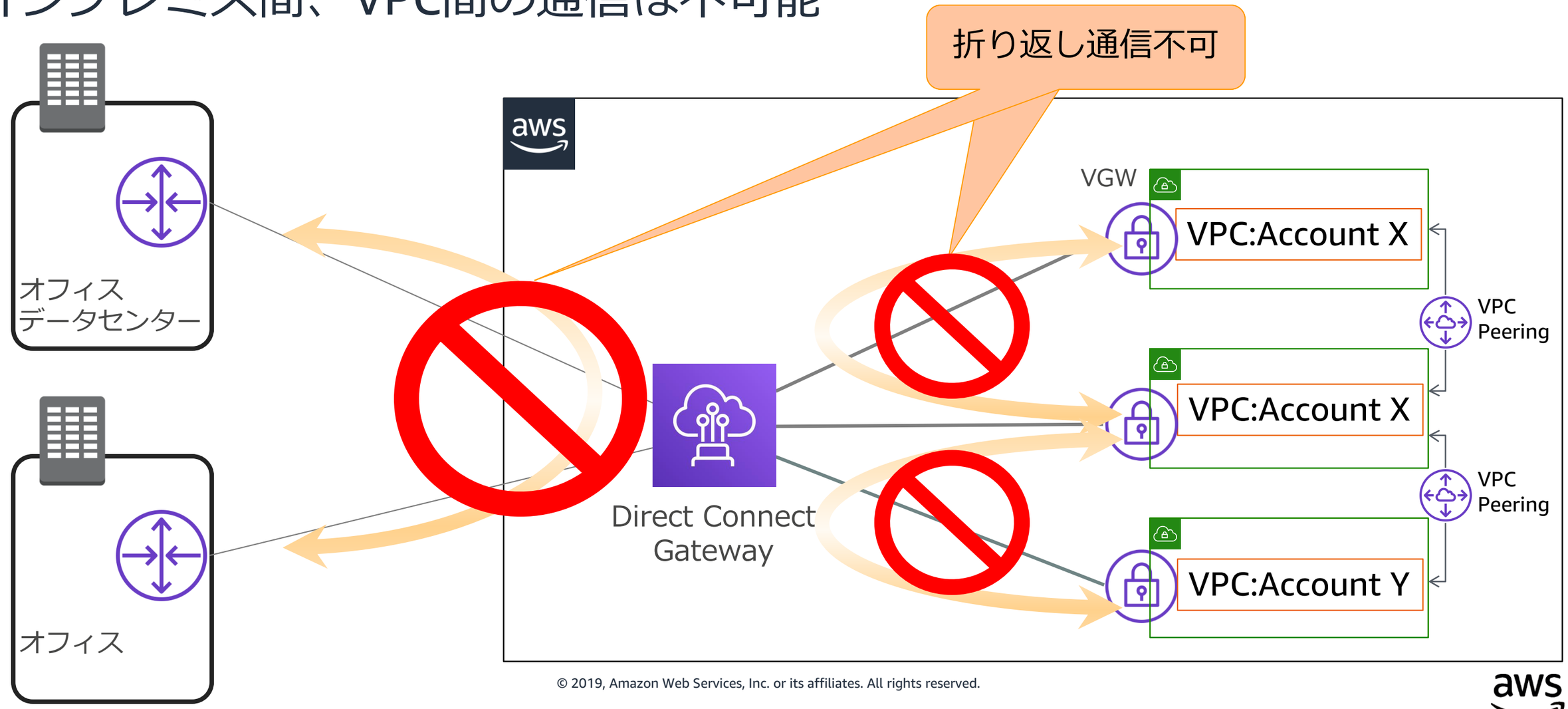
Direct Connect Gateway: 冗長化 AWS VPN

バックアップ回線としてAWS VPNを利用する事も可能だが、VGWごとにVPN 接続を設定する必要がある



Direct Connect Gateway 注意点

オンプレミス間、VPC間の通信は不可能



Direct Connect Gateway メリット

- 仮想インターフェイス(VIF)の数を節約可能
- VPC増加時には、新たな仮想プライベートゲートウェイ(VGW)をDirect Connect Gatewayにアタッチするだけで通信可能
- 既存Direct Connect環境からの移行が容易
  - 新規のVIFが必要、VPCのルートテーブルは変更不要、切り替え時にお客様ルーターにてBGPのアトリビュート（Local Preference、AS Path Prepend）を設定し、優先する経路を選択
- Direct Connect Gatewayの利用自体は無料（仮想インターフェイスの転送料金のみ）
- 複数リージョンのVPCにAWSバックボーンを利用して閉域接続可能

Direct Connect Gateway 利用時のポイント

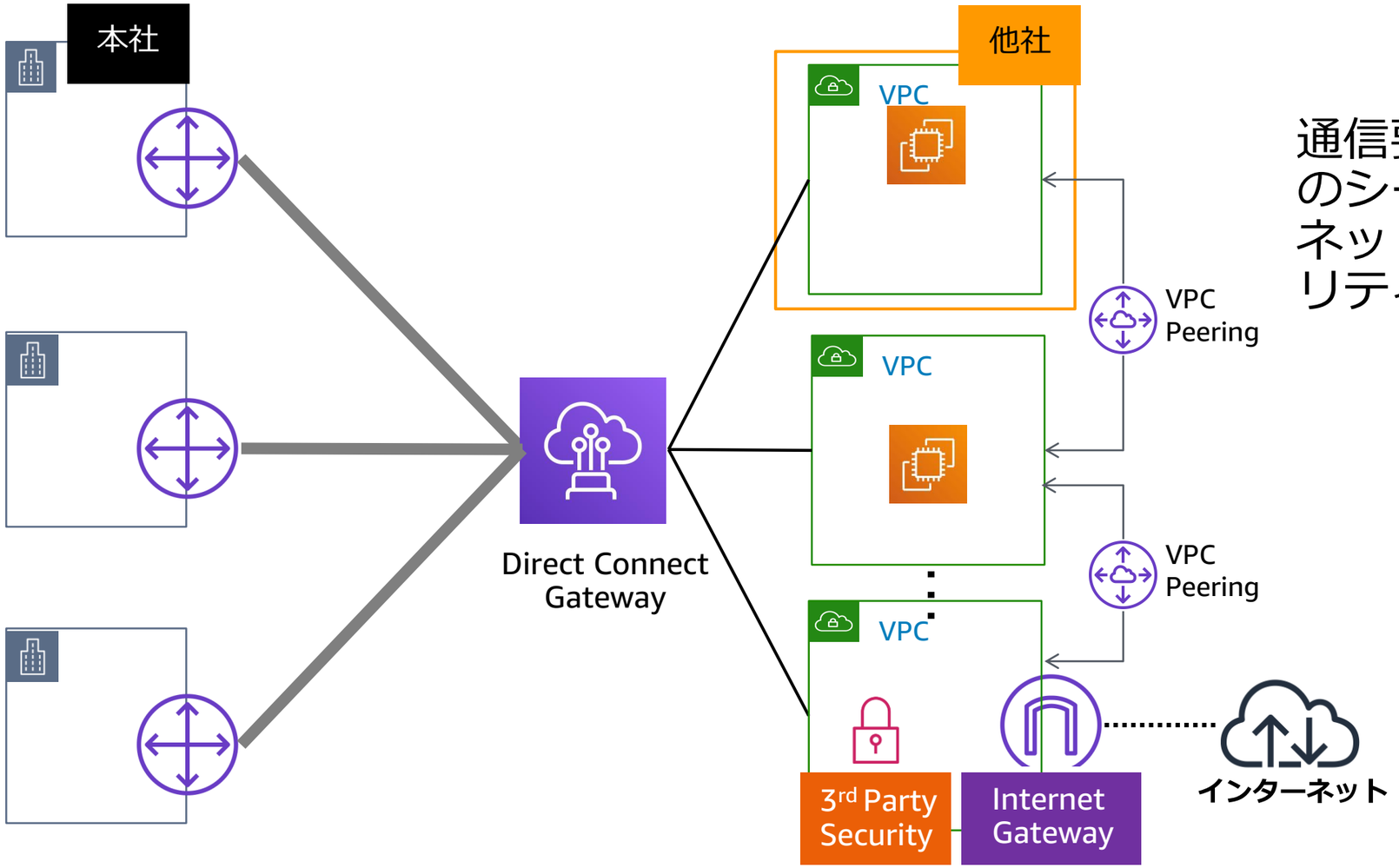
- 通常のDirect Connectと比較し、利用に際するデメリットは特に無し
  - 導入によるオーバーヘッドはありません
- 通常のDirect Connect仮想インターフェイス利用時には、VPCの数に関わらず「とりあえず間に挟む」事で後の拡張性が格段に増す
- 移行時に、現在のプライベートVIFを使いまわしする事はできない
- 設定時には、すべてのVPC CIDRをお客様ルーターにBGPで広報する
- 特定のVPC CIDRのみと通信させたい場合「許可されたプレフィックス」にて、フィルターを設定することができる

4. 共通リソースをAWS上に集約

aws INNOVATE
ONLINE CONFERENCE

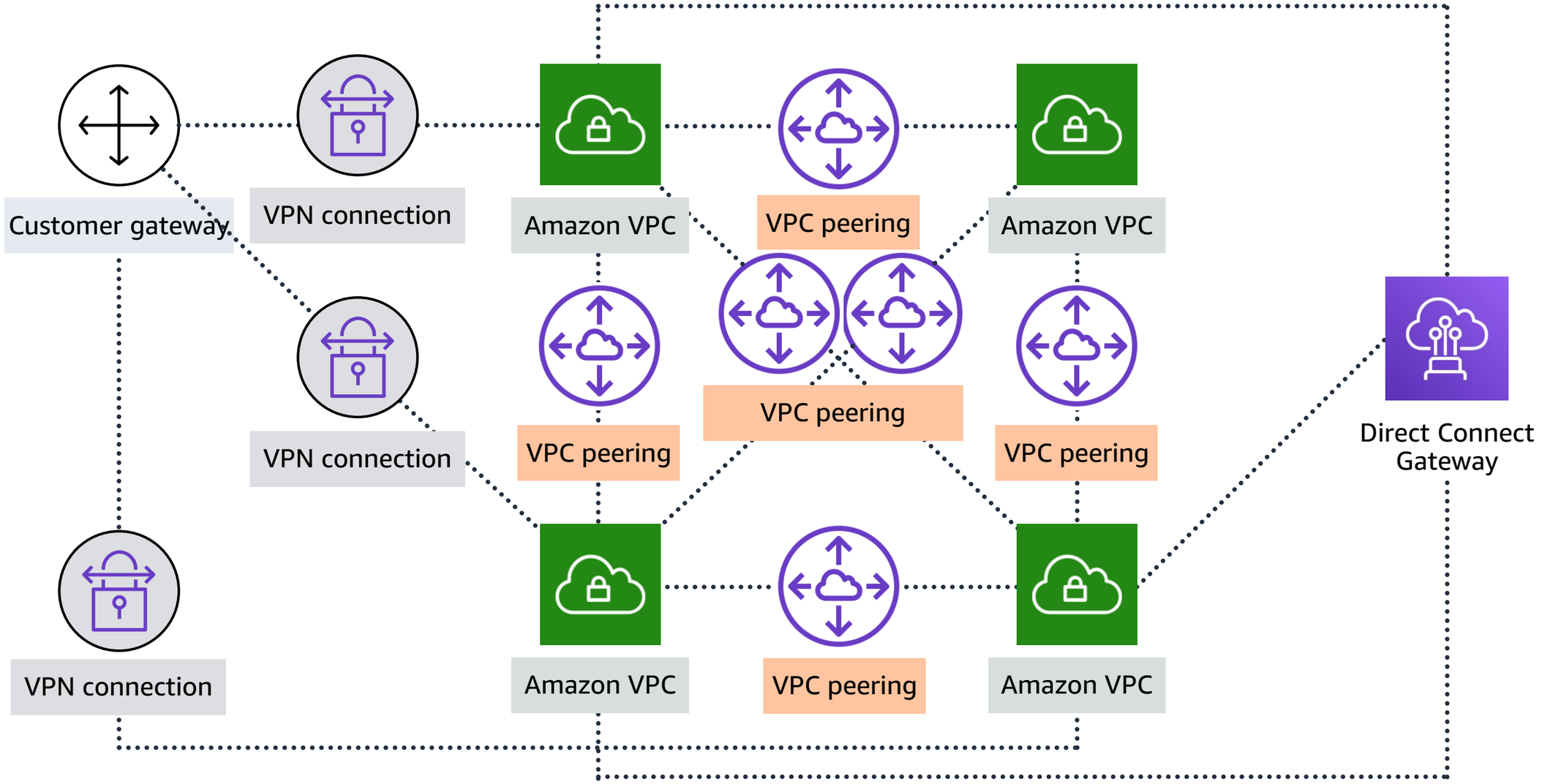
共通リソースをAWS上に集約

管理・連携するVPCの数が増え、VPC Peeringのメッシュ化によりAWS上の構成が複雑化
多くのオンプレミス拠点がVPCへ接続

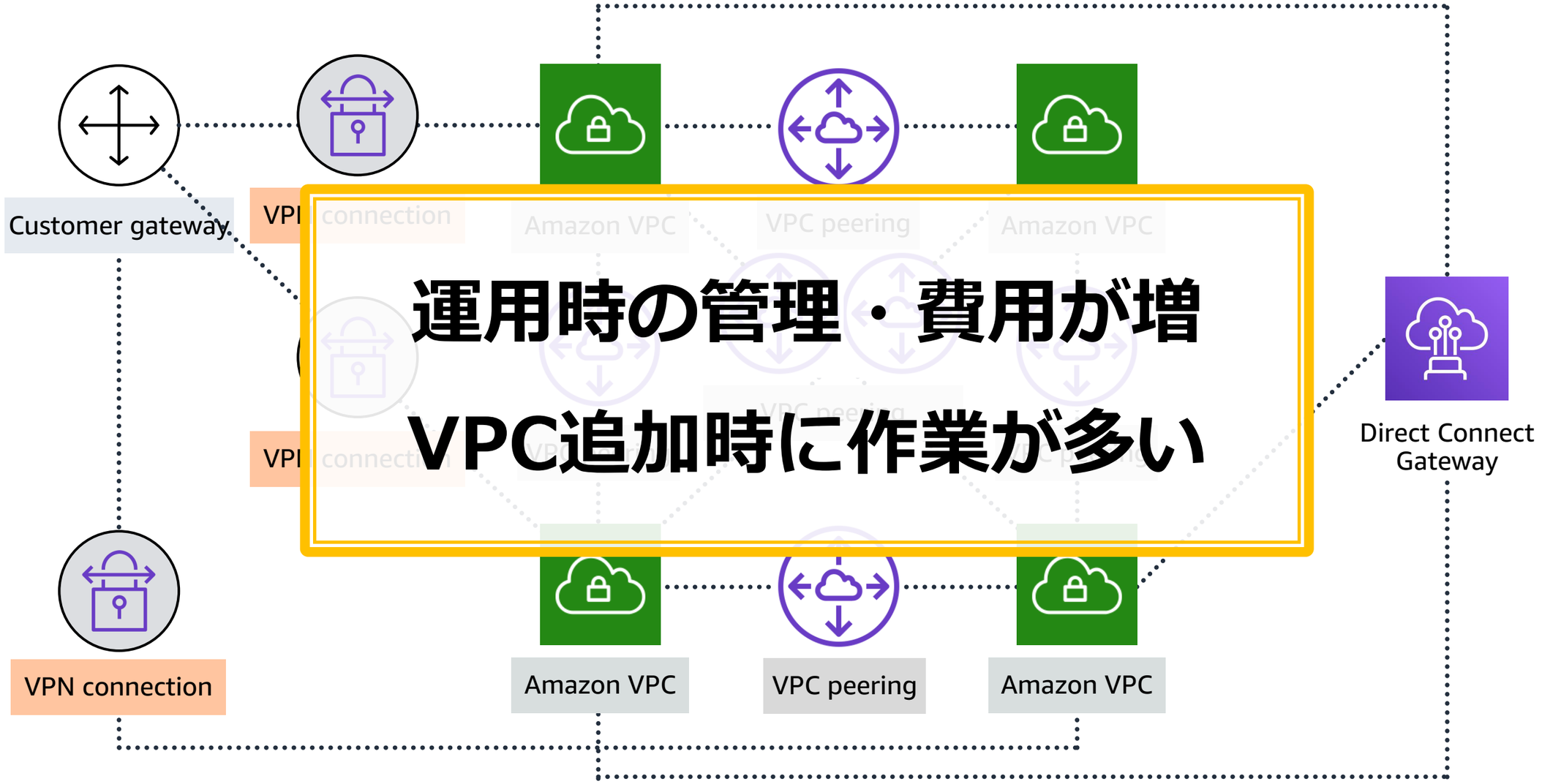


通信要件：オンプレミス、VPC間のシームレスな連携、インターネット接続環境をAWS上のセキュリティアプライアンスに集約

VPC Peeringのメッシュ化



個別のVPN接続



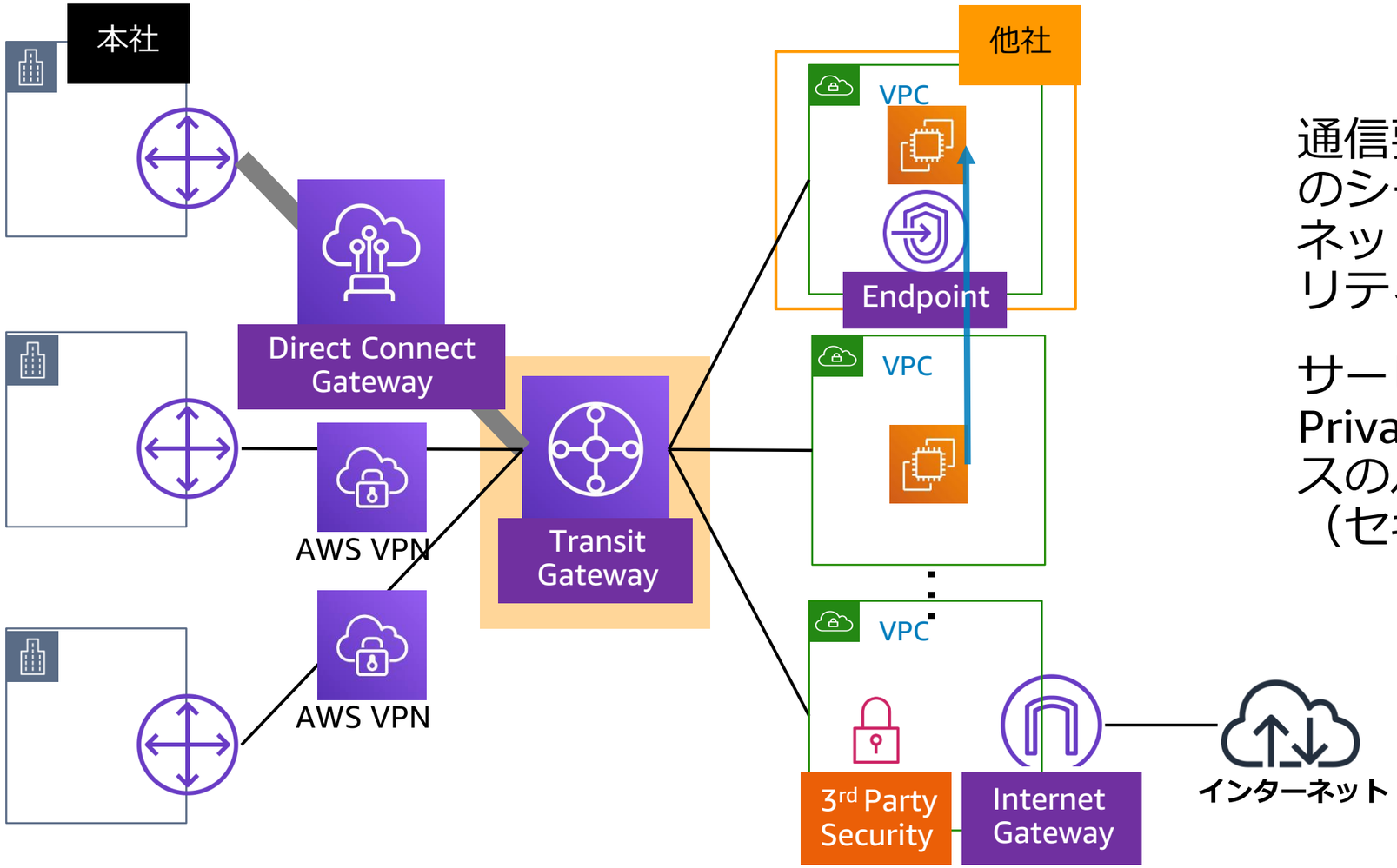
AWS Transit Gateway

Amazon VPC、AWS アカウント、オンプレミスネットワーク間の
数千規模の接続を簡単にスケールする

aws INNOVATE
ONLINE CONFERENCE

共通リソースをAWS上に集約

管理・連携するVPCの数が増え、VPC Peeringのメッシュ化によりAWS上の構成が複雑化
多くのオンプレミス拠点がVPCへ接続
→Transit Gatewayを中心に配置し、リージョナルルーターとして経路を集中管理

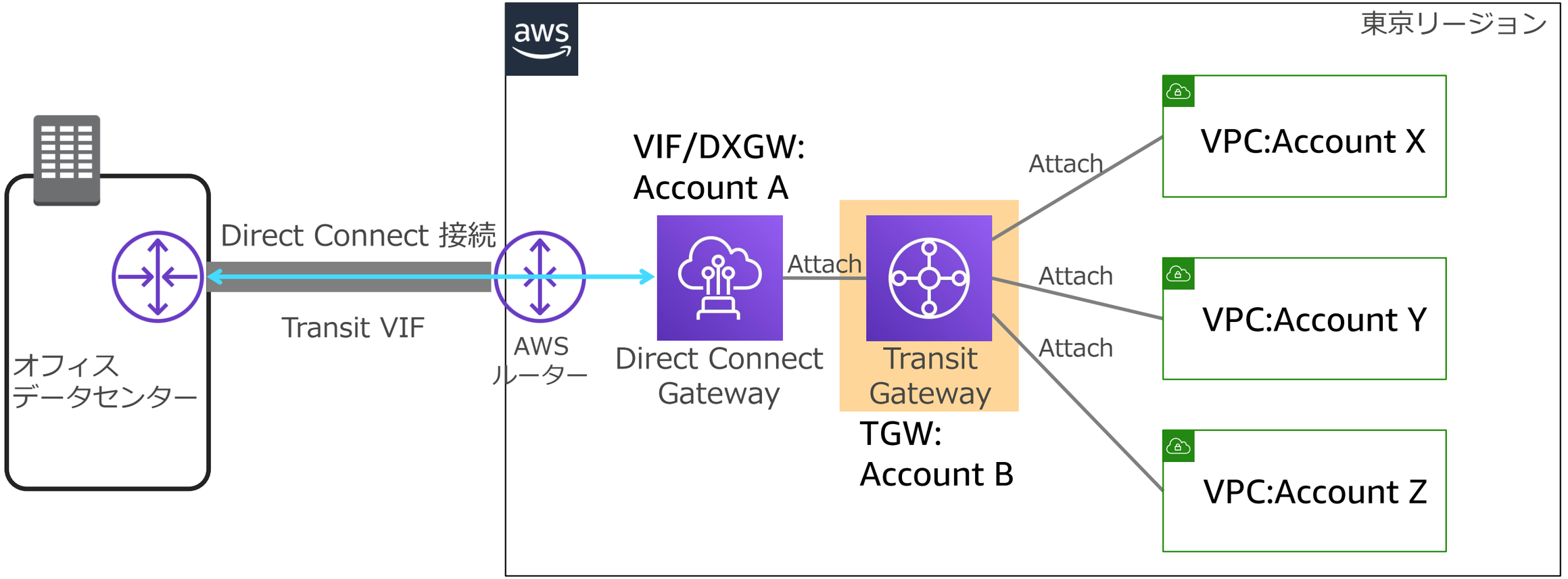


通信要件：オンプレミス、VPC間のシームレスな連携、インターネット接続環境をAWS上のセキュリティアプライアンスに集約

サービス： Transit Gateway、Private Link、マーケットプレイスのパートナーアプライアンス（セキュリティ関連）

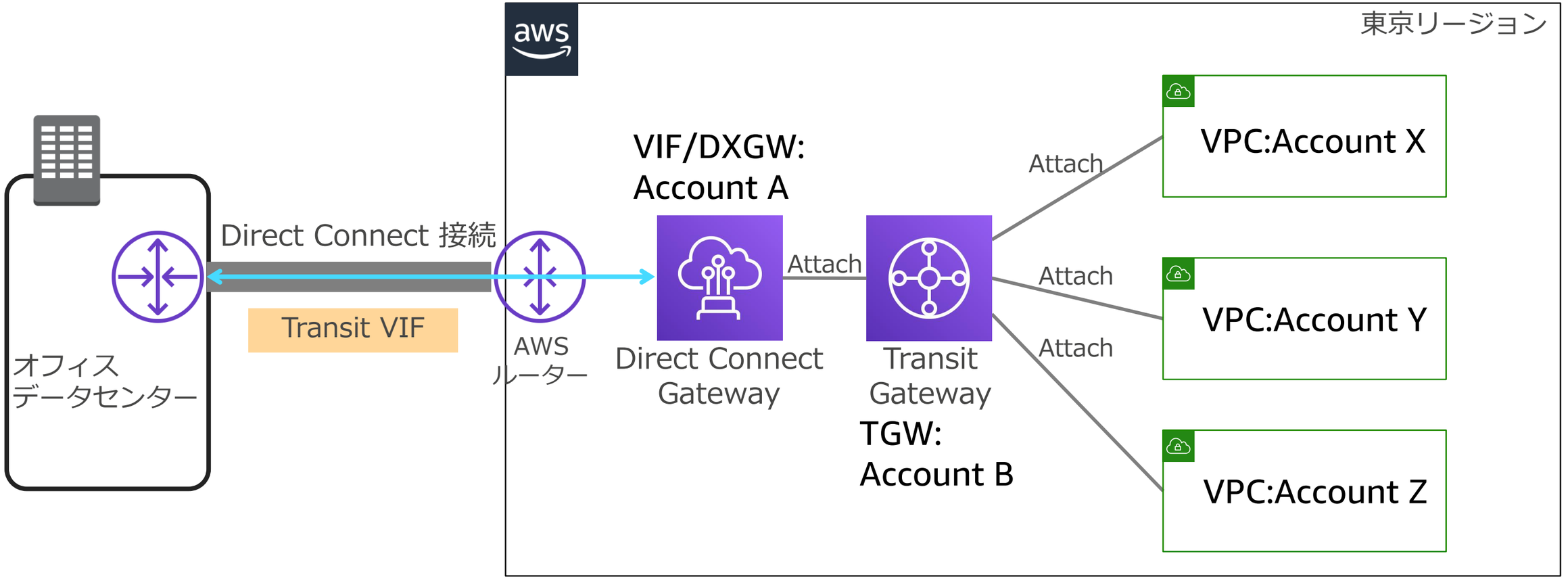
Transit Gateway 接続概要

Direct Connect GatewayとVPCの間に入る構成、VGWは不要
Transit仮想インターフェイス(VIF)を利用する点に注意



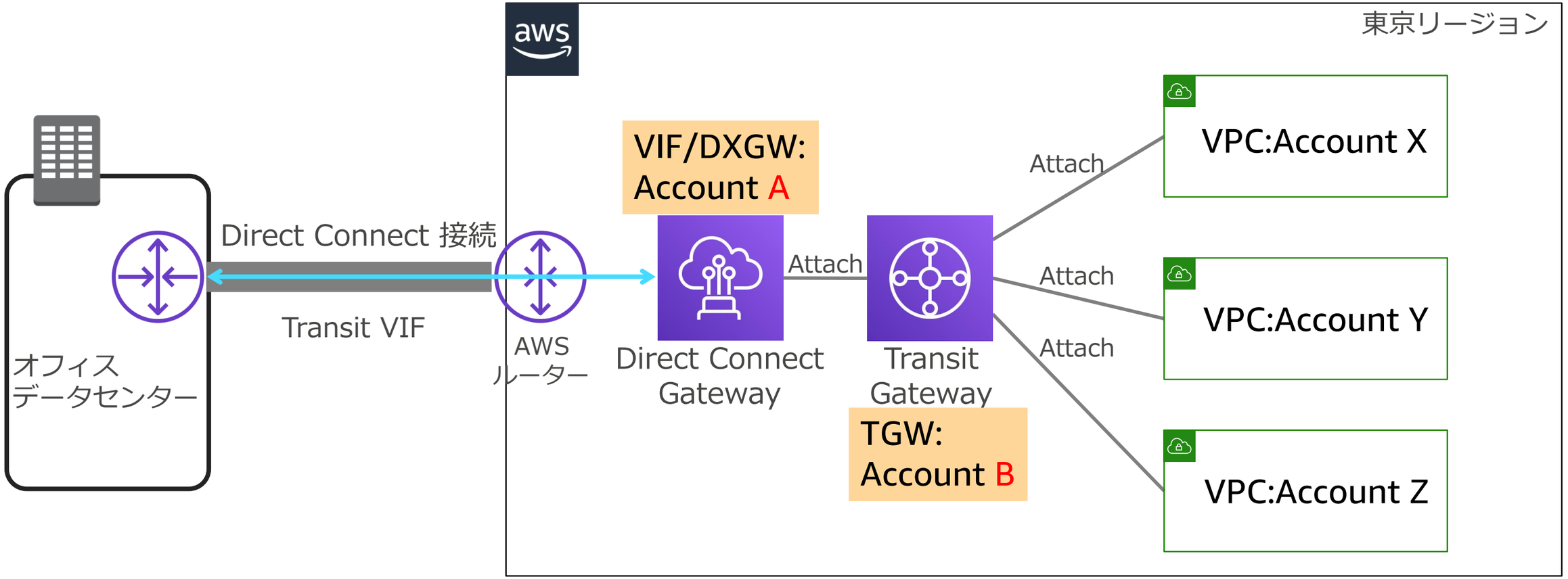
Transit Gateway 接続概要

Direct Connect GatewayとVPCの間に入る構成、VGWは不要
Transit仮想インターフェイス(VIF)を利用する点に注意



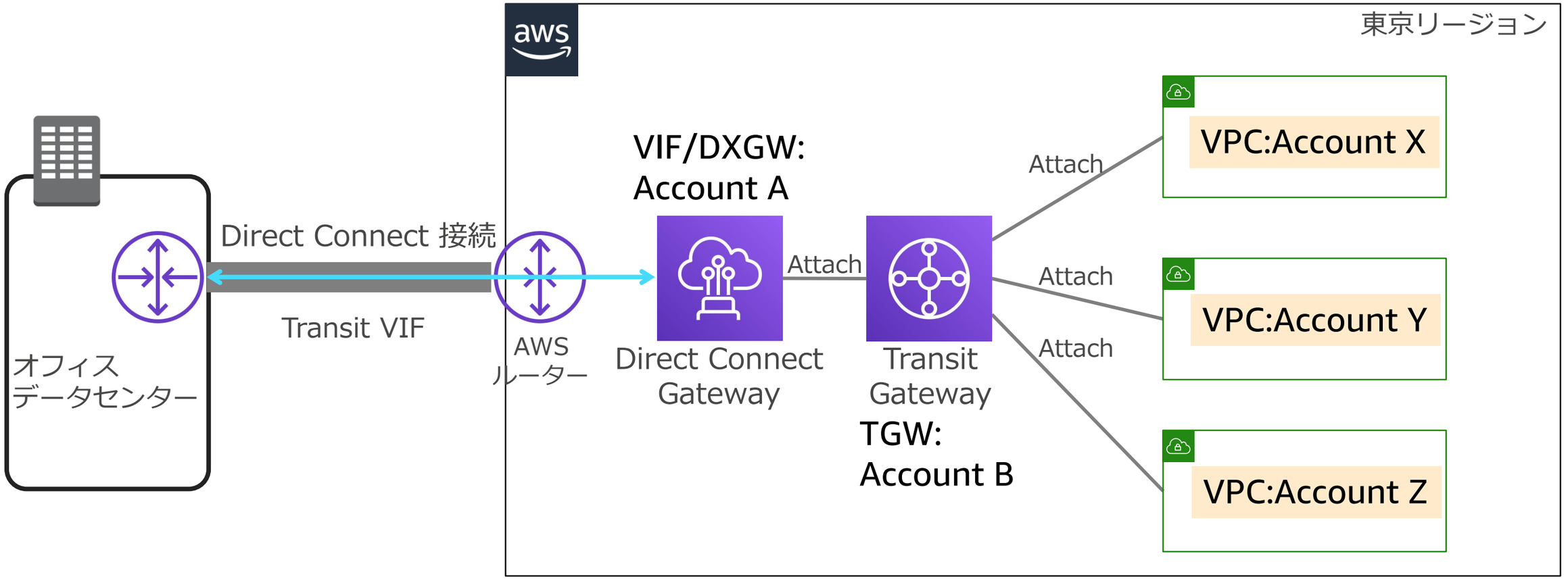
Transit Gateway 接続概要

Direct connect GatewayとTransit Gatewayは~~同じ支払いアカウントに属している必要がある~~別のアカウントでもアタッチ可能（2019/10/4 制限削除）

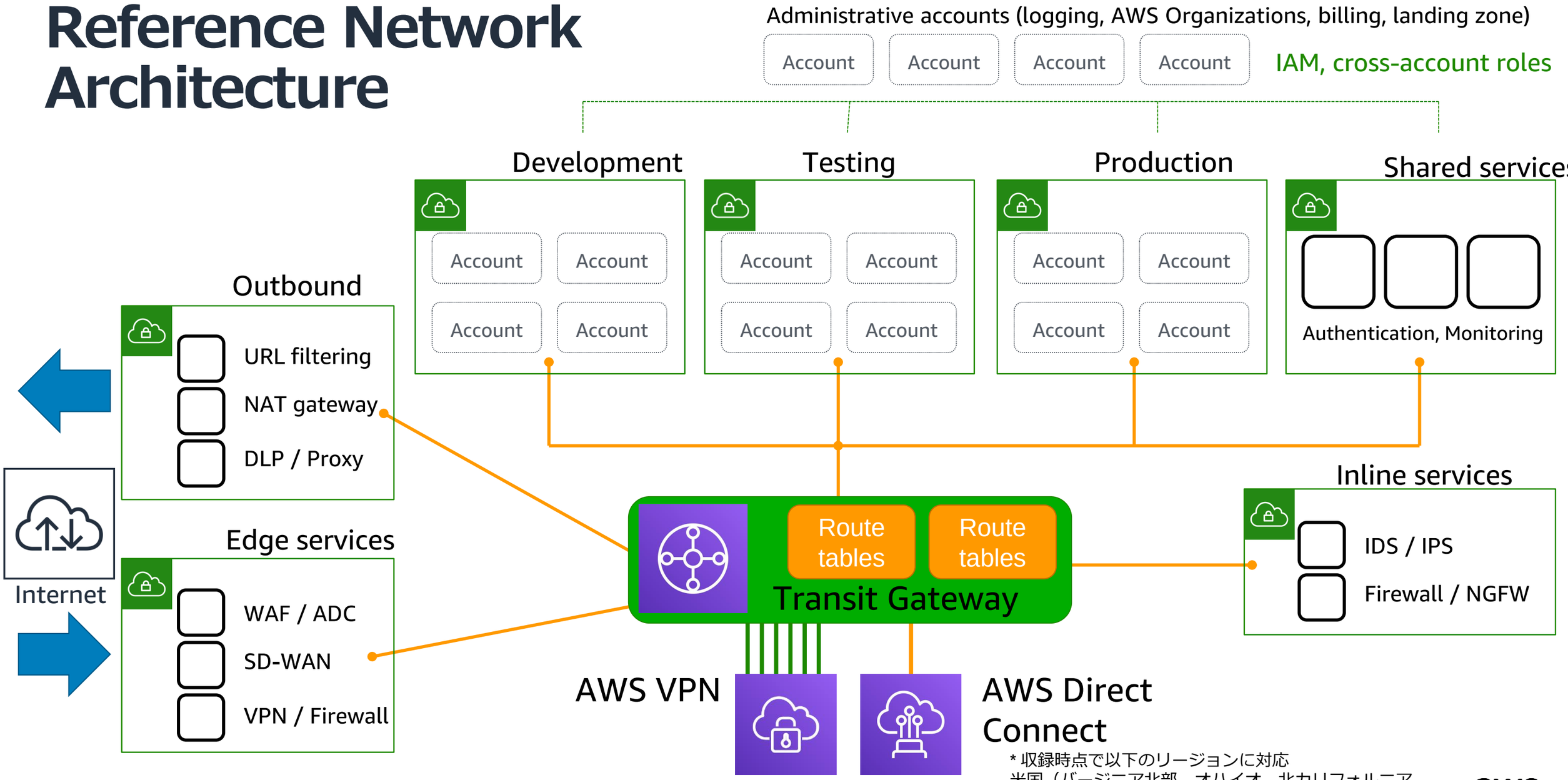


Transit Gateway 接続概要

Transit Gatewayにアタッチするvpcは他のAWSアカウントで管理されていてもよい



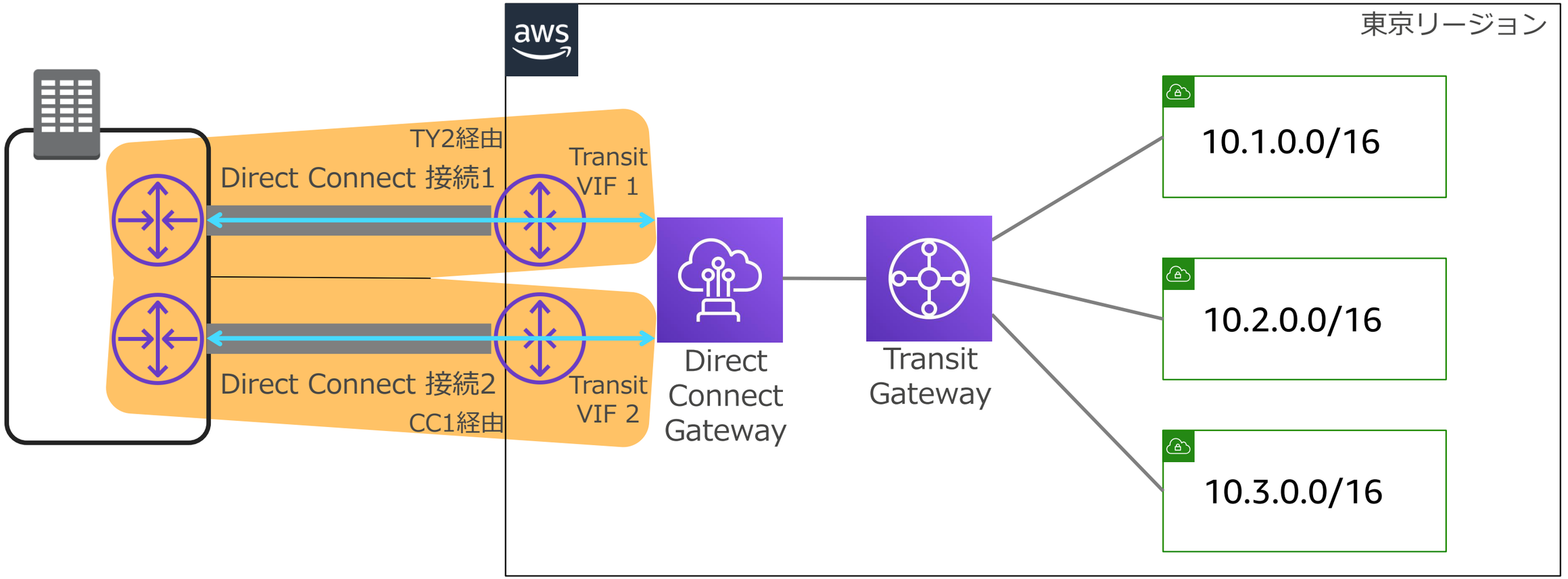
Reference Network Architecture



* 収録時点で以下のリージョンに対応
米国（バージニア北部、オハイオ、北カリフォルニア、オレゴン)、カナダ (中部)、欧州 (アイルランド、ロンドン、フランクフルト) 、 AWS GovCloud (米国東部/西部)

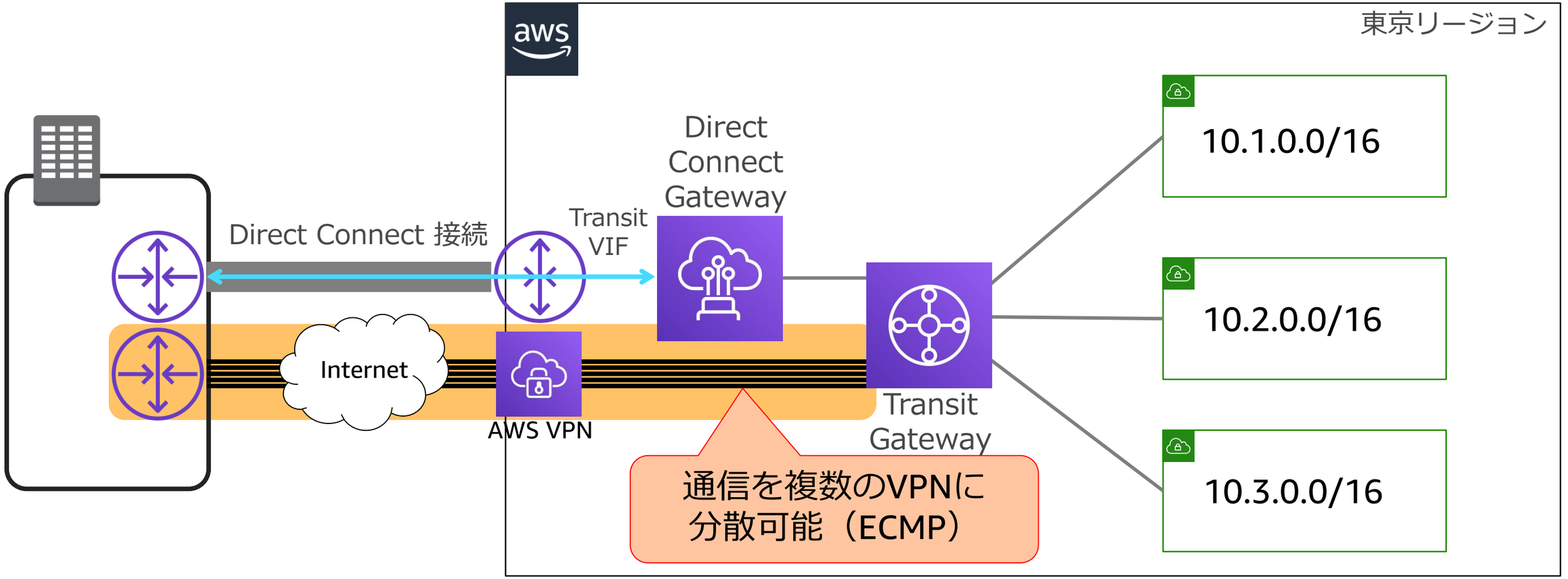
Transit Gateway 冗長化: Transit VIF x 2

回線冗長化の考え方は、Direct Connect Gatewayと同じ



Transit Gateway 冗長化: AWS VPN

AWS VPNをバックアップとして利用する事も可能
Site-to-Site VPNでTransit Gatewayへ直接接続



Transit Gateway メリット

- リージョナルゲートウェイとして利用し、VPC間接続を簡単に管理
- VPC Peeringで複雑になった構成をシンプルにできる
- 数千のVPC、VPNを接続し、大規模な構成を作れる
- アタッチメントごとのルーティング管理を可能にする「ルーティングドメイン」のサポート
- 各アタッチ間の通信を、パートナーが提供するアプライアンスにルーティングする事が可能

Transit Gateway 注意点

- DXGWにアタッチする回線には、Transit仮想インターフェイスが必要
- オンプレミスとの通信には、仮想インターフェイスの転送料に加え、Transit Gatewayの転送料、各アタッチメント毎の時間課金を考慮
- 複雑な構成を組む際には、しっかりとした経路設計を行い、構築後にもEnd-to-Endで「通信出来る事・出来ない事」をテストする事を推奨
- VPC間通信時にはいくつかの制限がありますので、公式ドキュメントに記載の内容をご確認ください
- DXGW+TGWの構成で指定する「許可されたプレフィックス」は、DXGW単独で利用する際と考え方が異なり、記載したCIDRがそのままお客様ルーターへ広報されます

[参考] Transit Gatewayの料金について

英語の表記となりますが、以下にて詳細を説明しております。

Transit Gateway Pricing Points

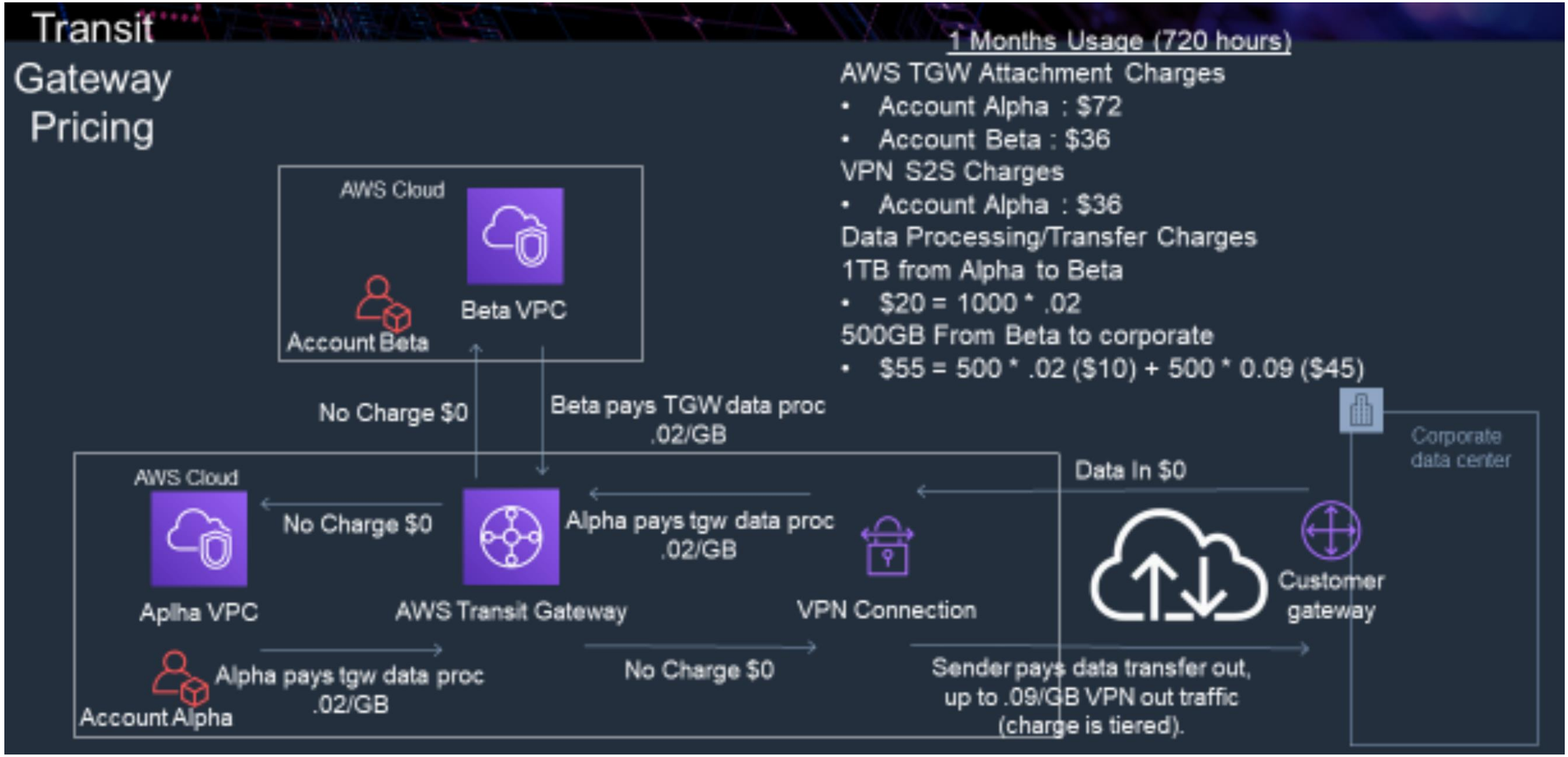
Hourly Attachment Charges

1. Owner (account) of attachment the hourly TGW attachment charge, whether VPC or VPN or soon DXG.

Data Charges

1. Owner (account) of attachment pays the TGW data processing charge for data sent to the TGW.
    1. The receiver of the traffic doesn't pay TGW data processing (no double charge).
    2. Data "sent" to TGW could be data coming in from on premise, i.e. over VPN. There is no EC2 data in (data in is still free), but data "sent" to TGW incurs data processing charge.
2. DATA OUT – Sender (VPC) of data pays the VPN data out charges, not the owner of the VPN attachment.
3. Cross AZ – If sender and receiver instances are in the same AZ, no charge. If receiving EC2 is in different AZ, receiving pays nominal cross AZ charge (.01/GB).

[参考] Transit Gatewayの料金について(続き)



[参考] Classic VPN リタイヤメントについて

aws INNOVATE
ONLINE CONFERENCE

[参考] Classic VPNのリタイヤメントについて

対象者には個別にリタイヤ予定をアナウンス済み

現時点で利用している場合、速やかに後続のAWS VPNへ移行する事を強く推奨します

移行時には、以下のいずれかの方法をご検討ください。

1. すべてのVPN設定を削除し、しばらく置いてから再作成
2. (Direct Connectを併用していない際、既存のClassic VPNは利用したまま) 新規のVGWを作成し、VPCに未アタッチの状態で新規作成したAWS VPNで接続をテストする　全てのVPNがUpした後、新旧のVGWを入れ替え（VPCから旧VGWをデタッチ、新VGWをアタッチ）

資料： AWS Classic VPN から新しい AWS VPN に移行する方法を教えてください

https://aws.amazon.com/jp/premiumsupport/knowledge-center/migrate-classic-vpn-new/

[参考] Classic VPNのリタイヤメントについて

“VPN”であれば対象外

“VPN-Classic”であれば対象

まとめ

多くの選択肢が揃ってきた「オンプレミスとVPC間の接続方法」を整理してみる

aws INNOVATE
ONLINE CONFERENCE

オンプレミスとVPCの接続パターン（再掲）

1. 拠点からインターネット経由でVPCに接続
   → 最も容易だが、通信要件に合わせて暗号化を利用
2. 複数拠点からセキュアにVPCに接続
   → Direct ConnectとVPNを併用してメリハリのある構成
3. 拠点からシステム毎に異なるVPCに接続
   → Direct Connect Gatewayでシステム毎のVPCへ接続
4. 共通リソースをAWS上に集約
   → Transit Gatewayで経路を集中管理、柔軟な経路設計

[参考] 公開資料

AWS Summit Tokyo

・ネットワークデザインパターン Deep Dive　資料　動画

AWS Summit Tokyo

・Transit Gateway Deep Dive アーキテクチャガイド　資料　動画

Transit Gateway 公式ドキュメント

・Amazon Virtual Private Cloud > Transit Gateways

Thank you!

菊地 信明　門田 梓

aws INNOVATE
ONLINE CONFERENCE

Event info - https://amzn.to/JP**Events**

Webinar - https://amzn.to/JP**Webinar**

Archive - https://amzn.to/JP**Archive**