



[AWS Black Belt Online Seminar]

AWS Direct Connect

サービスカットシリーズ

Solutions Architect 菊地 信明
2021/2/9

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



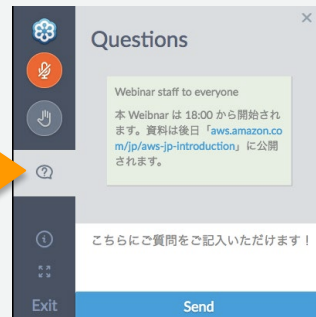
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾンウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
お答えできませんのでご了承下さい

- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2021年2月9日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっております。日本居住者のお客様には別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

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株式会社
技術統括本部 レディネスソリューション本部
Network Solution Architect



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

本セミナーの対象者

- 基本的なネットワークやAmazon VPCの知識をお持ちの技術者
- オンプレミスとAWS Cloudを閉域網で接続する要件をお持ちの方
- すでにAWSをご利用中で、オンプレミスから通信するVPCを効率よく管理したい方
- Direct Connectパートナーに関連するお仕事をされている方

本日の目標

- AWS Direct Connectの機能とメリットを理解する
- AWS Direct Connectの利用パターンを把握する
- 複数のユースケースに対してメリットを知る
- 詳細情報・最新情報へのポイントを得る

本セミナーでお話しないこと

- Amazon VPC、AWS Direct Connectに対するマネージメントコンソール上での具体的な設定方法
- Transit Gatewayに関する用語・機能の詳細
- 各構成への移行方法
- オンプレミスとDirect Connectロケーション間をつなぐ回線の手配方法

関連するAWSサービスについての情報は、本資料後半のリンクをご参照ください

Agenda

- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系



Agenda

- **AWS Direct Connect とは？**
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系



AWS Direct Connectとは？

AWS Direct Connect とは？

Direct Connect = 専用線サービス

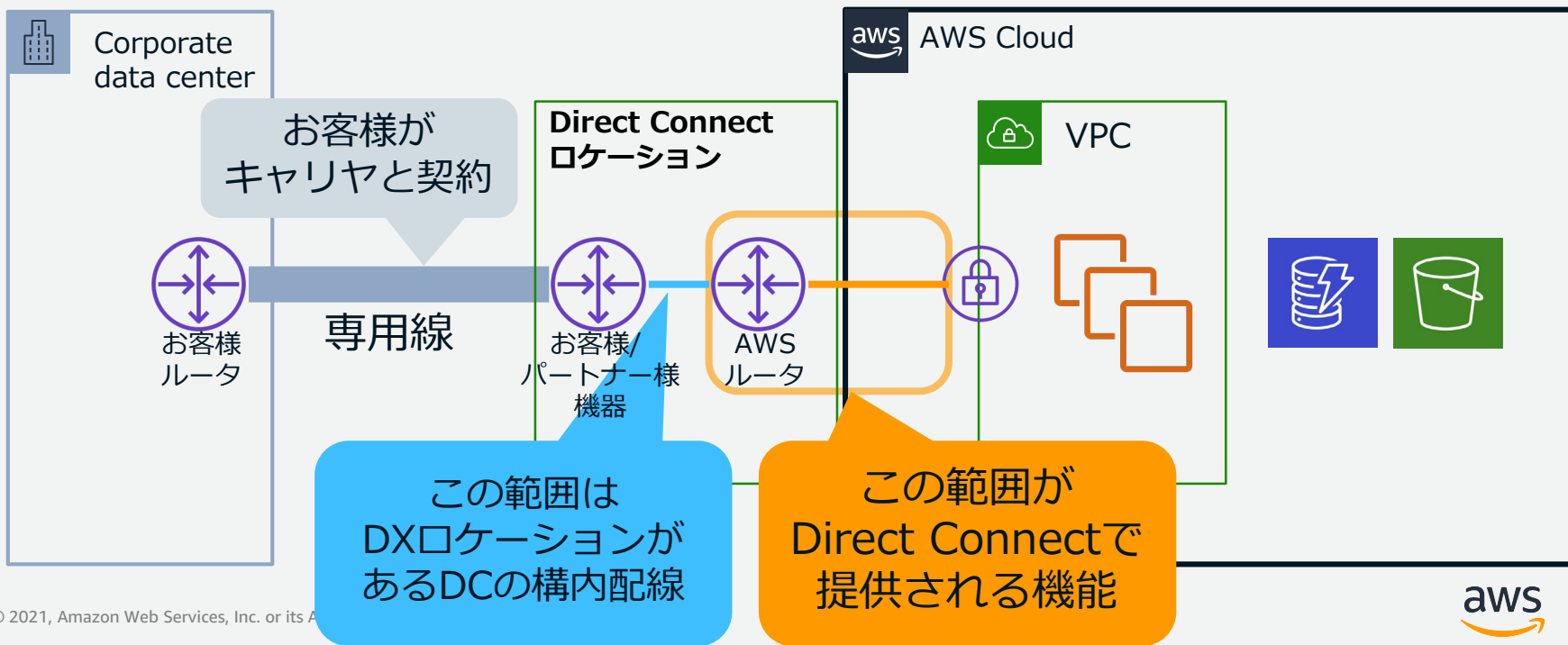
AWS Direct Connect とは？

Direct Connect ≠ 専用線サービス

AWS Direct Connect とは？

AWS Direct Connectは【**オンプレミスと直接接続する専用線サービスではありません**】

お客様がキャリアから調達する専用線の片端とAWS Cloudを、Direct Connectロケーションで接続するサービスです



Agenda

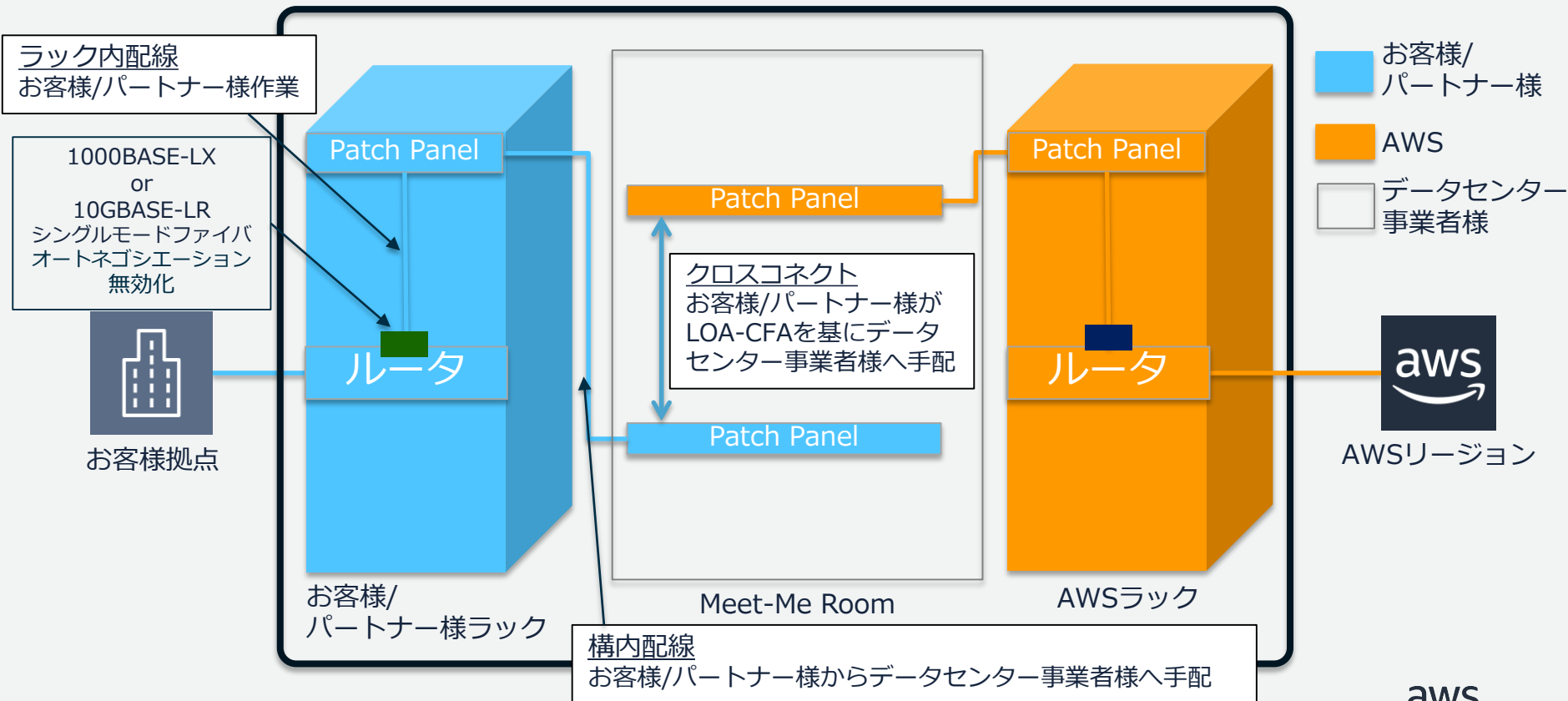
- AWS Direct Connect とは？
- 物理接続/論理接続
 - **物理接続**
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系



物理接續

Direct Connect ロケーションでの接続

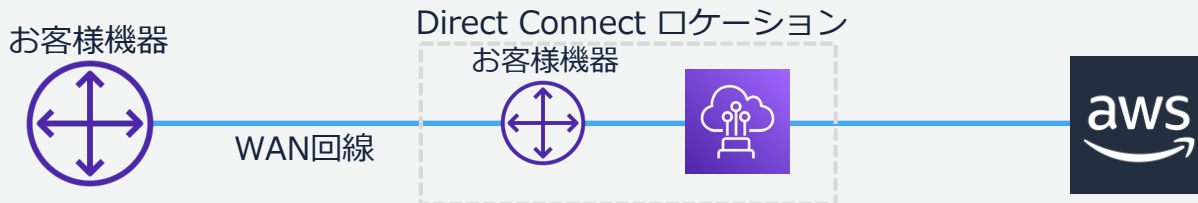
Direct Connect ロケーション



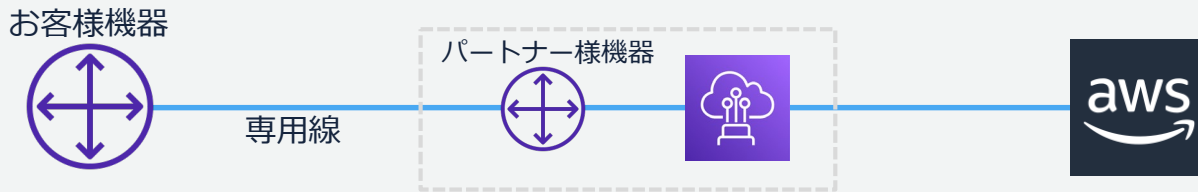
接続のパターン



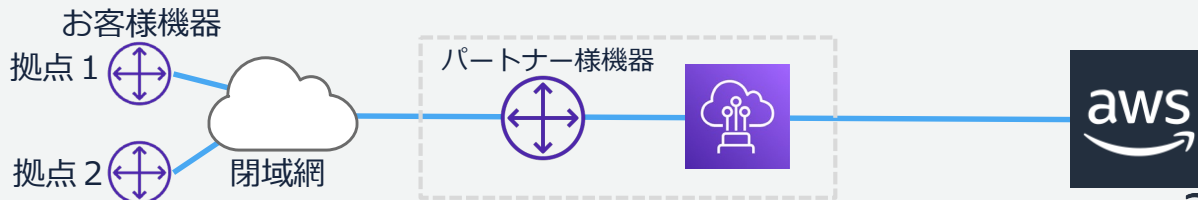
1) Direct Connectロケーションとお客様機器が同じロケーション



2) Direct Connectロケーションからパートナー様専用線で接続



3) パートナー様閉域網(IP-VPN網、モバイル網等)経由で接続

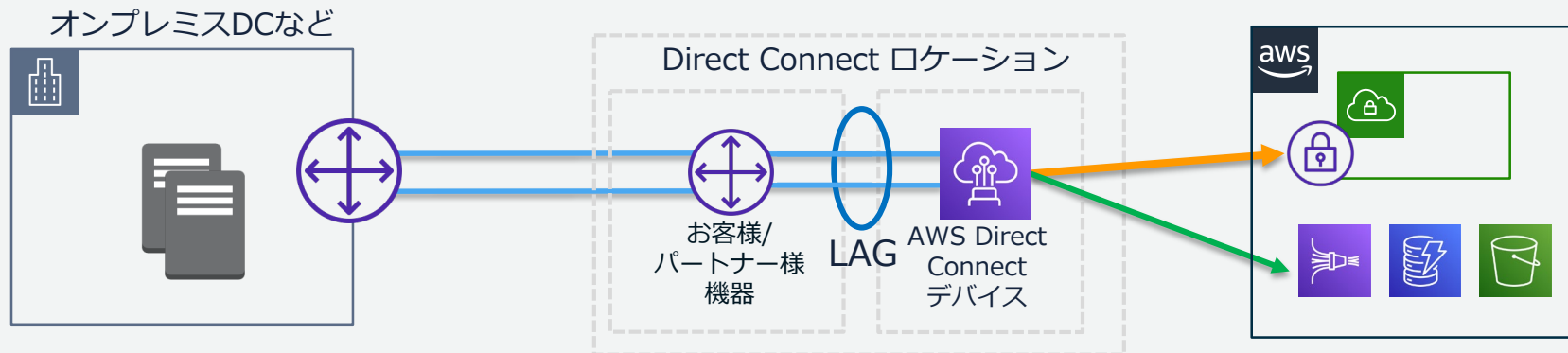


Link Aggregation Group (LAG)

複数の1 Gbpsまたは10 GbpsのConnectionを集約し、一つの論理インターフェイスとして提供

- 同じ速度のConnectionを最大で4つ集約し、各Connectionにトラフィック分散
- Link Aggregation Control Protocol (LACP) を使用

※メンバーポートは同一のAWSデバイスに收容されるため別途冗長化が必要



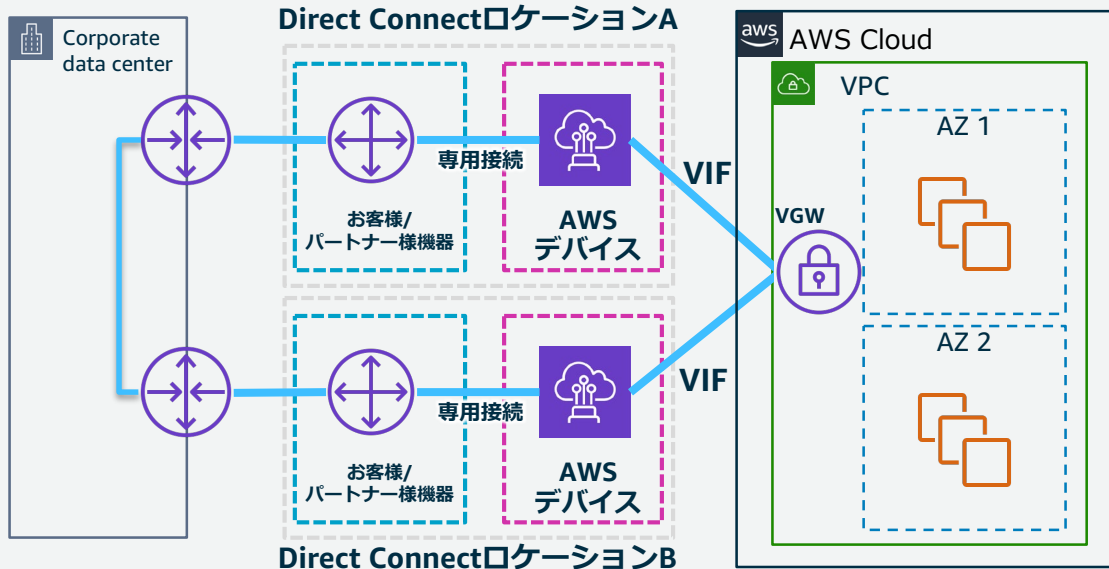
https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/lags.html

ベストプラクティス：クリティカルなワークロードの高い回復性

- AWS Direct Connect の回復性に関する推奨事項

<https://aws.amazon.com/jp/directconnect/resiliency-recommendation>

お客様の大切なワークロードを担うネットワークとして、シングルポイントを作らない事が重要。そのための推奨構成を以下に記載します。



- Active-Active、Active-Standbyは問わない
- Direct Connectゲートウェイ、Transit Gatewayも利用可能

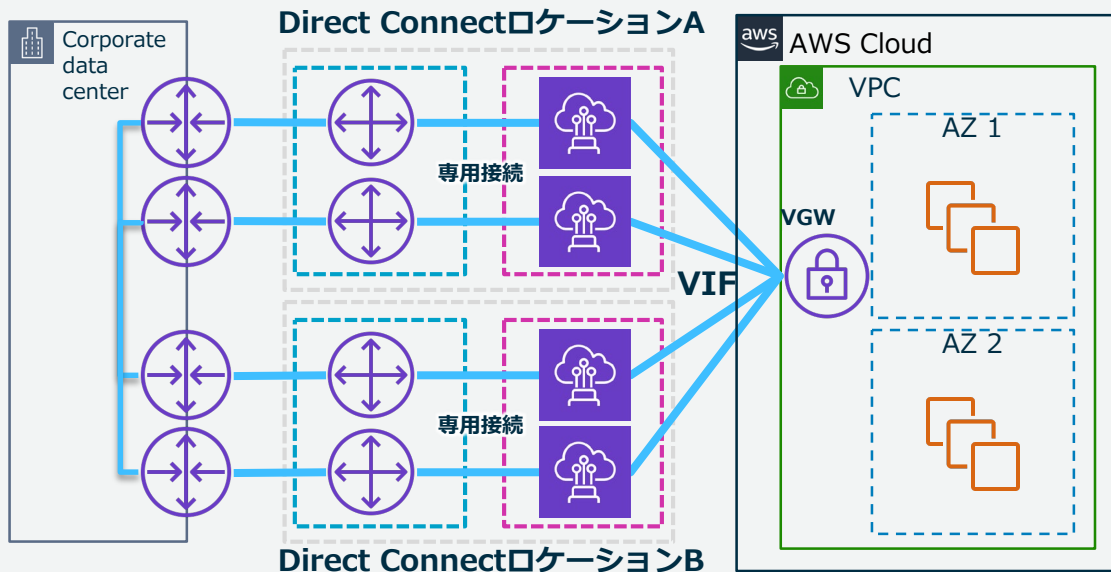
SLA 99.9%要件

- 2つのロケーションに接続を配置
- エンタープライズサポート契約に加入
- AWS上のリソースをマルチAZ化

ベストプラクティス：クリティカルなワークロードの最大回復性

- AWS Direct Connect の回復性に関する推奨事項

<https://aws.amazon.com/jp/directconnect/resiliency-recommendation>



SLA 99.99%要件

- 2つのロケーションに各2つの接続、**合計4つの接続を配置**
- エンタープライズサポート契約に加入
- AWS上のリソースをマルチAZ化
- SAによるW-Aレビュー

SLAについて

- AWS Direct Connect Service Level Agreement

<https://aws.amazon.com/jp/directconnect/sla/>

SLAに適用すると・・・

- ➡ アップタイムが目標値を下回った場合、
利用料から定められた割合の返金をリクエスト可能
- ➡ 通信品質は適用前と同等
- ➡ 技術サポートはご契約いただいたプランに即した対応

**重要なのは、ベストプラクティスを参考に
止まらないシステムを作る事！**

Agenda

- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - **仮想インターフェイスの種類**
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系



仮想インターフェースの種類

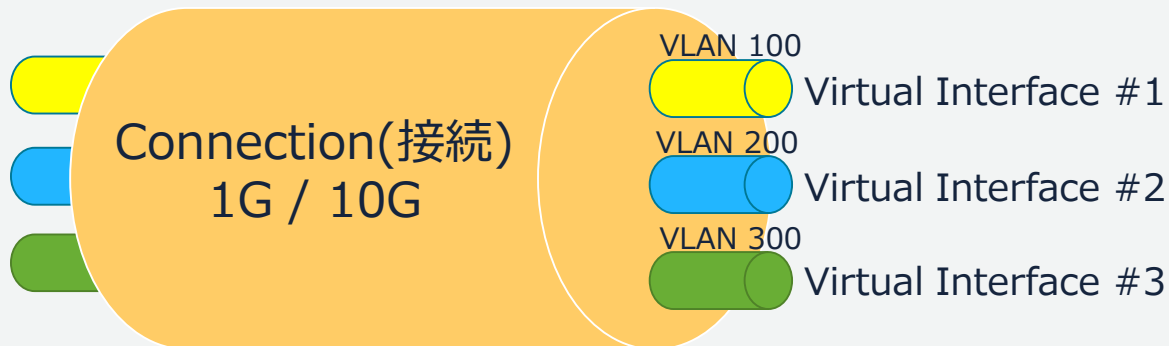
- ・プライベート仮想インターフェース
- ・パブリック仮想インターフェース
- ・トランジット仮想インターフェース

仮想インターフェイス (Virtual Interface = VIF)

Connection(接続) = 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ーフェイス

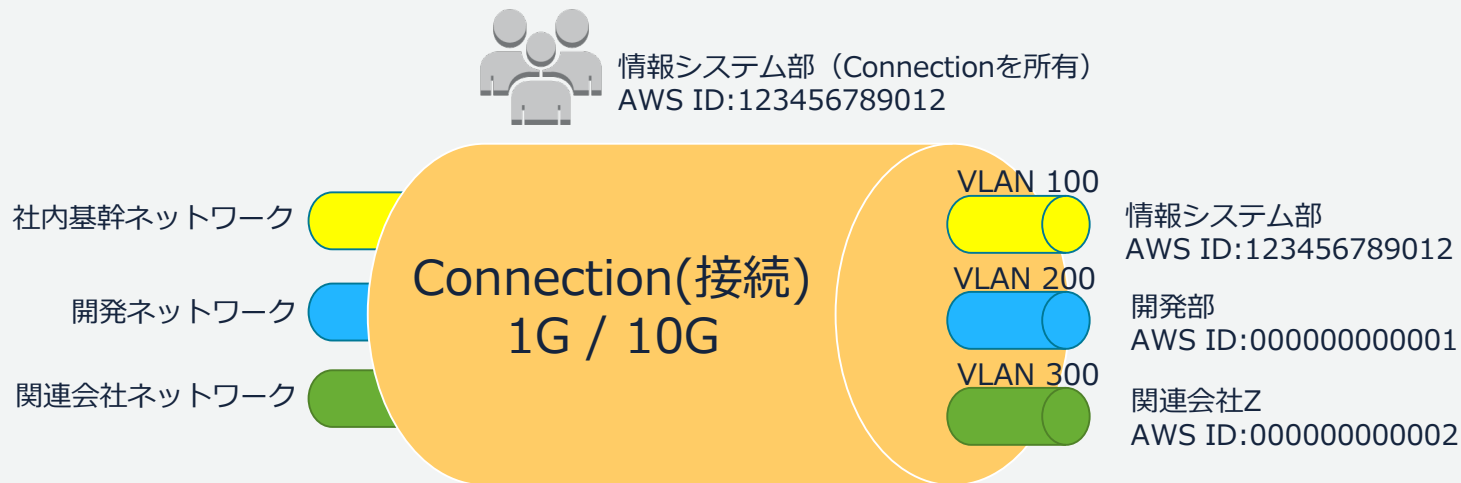
- AWSとお客様ルータの間でBGPピアを確立し経路交換をするために必要
- VLAN IDをもつ



- **プライベートVIF** : VPCへプライベートIPを介した接続を提供
- **パブリック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
- **トランジットVIF** : Transit Gateway用のDirect Connectゲートウェイへ接続を提供

クロスアカウント利用

- Connectionを所有しているAWSアカウントから、他のAWSアカウントに対してVIFを提供することが可能
- データ転送料については、各アカウントに課金

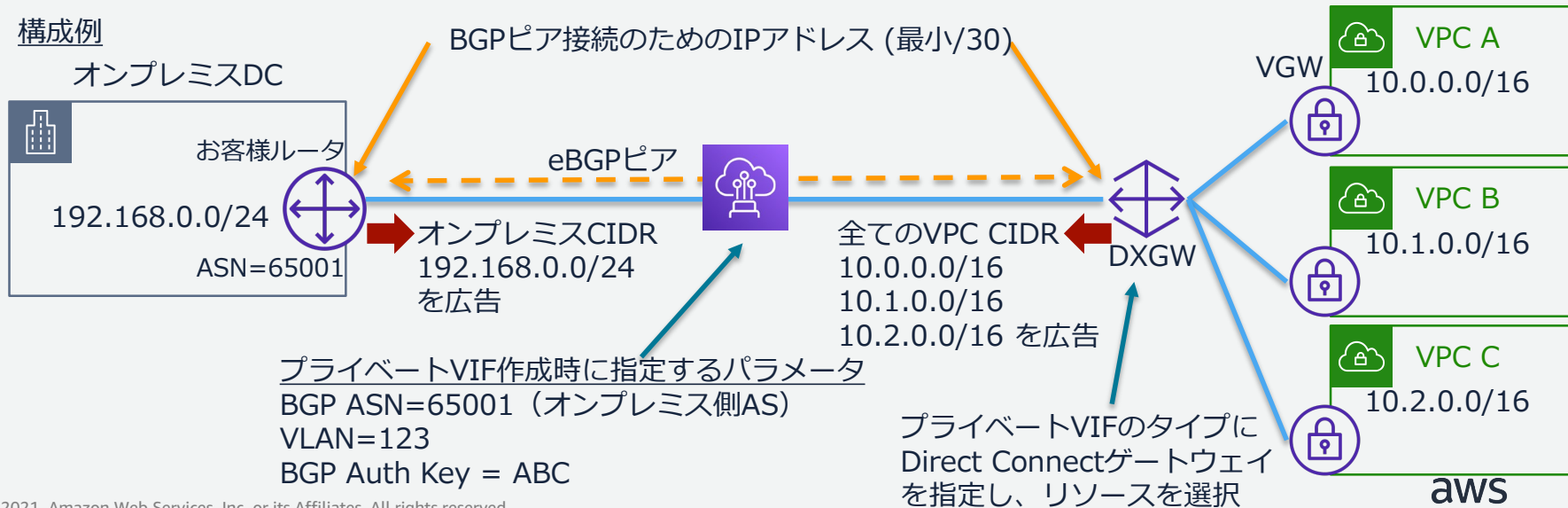


プライベート接続 : Direct Connectゲートウェイ(DXGW)タイプ(推奨)

- **プライベートVIF**を使用して複数のVPCへ接続を提供
- お客様ルータでBGP, MD5認証, IEEE802.1q VLANのサポートが必要
- VPCのCIDR(IPv4,IPv6)がすべてAWSから広告される (フィルタリング可能)
- Jumbo Frame(MTU=9001)をサポート

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

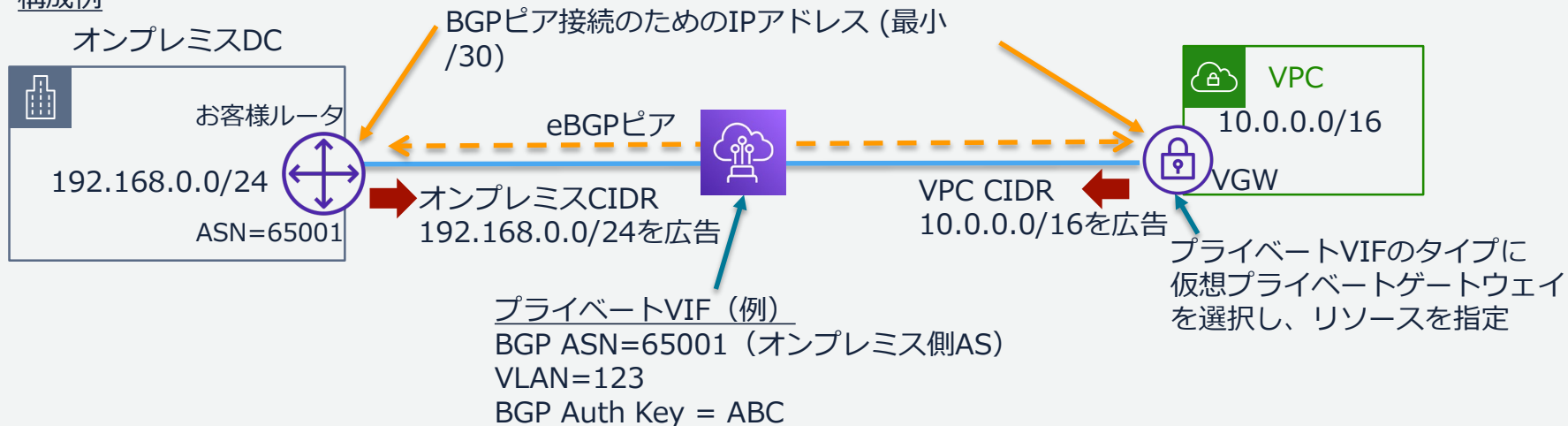
構成例



プライベート接続：仮想プライベートゲートウェイ(VGW)タイプ

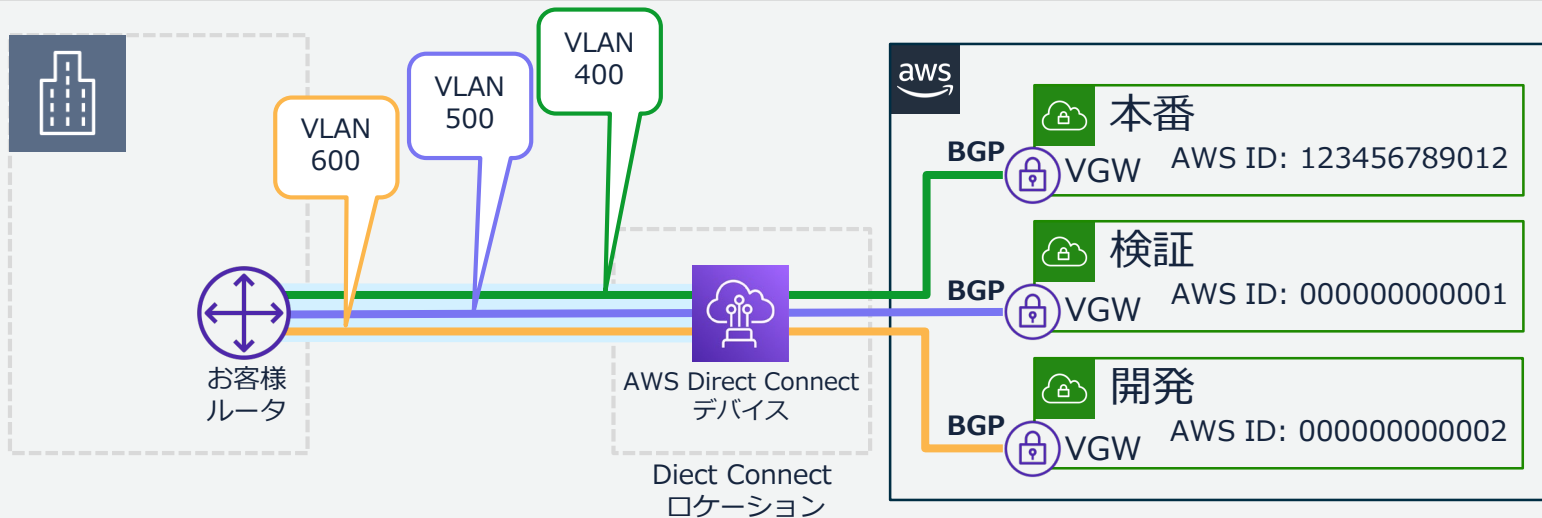
- **プライベートVIF**を使用して単一のVPCへ接続を提供
- 他の要件はDirect Connectゲートウェイタイプと同様
- 後述するCloudHub構成が必要な際に利用

構成例



複数のプライベートVIFによるマルチVPC接続

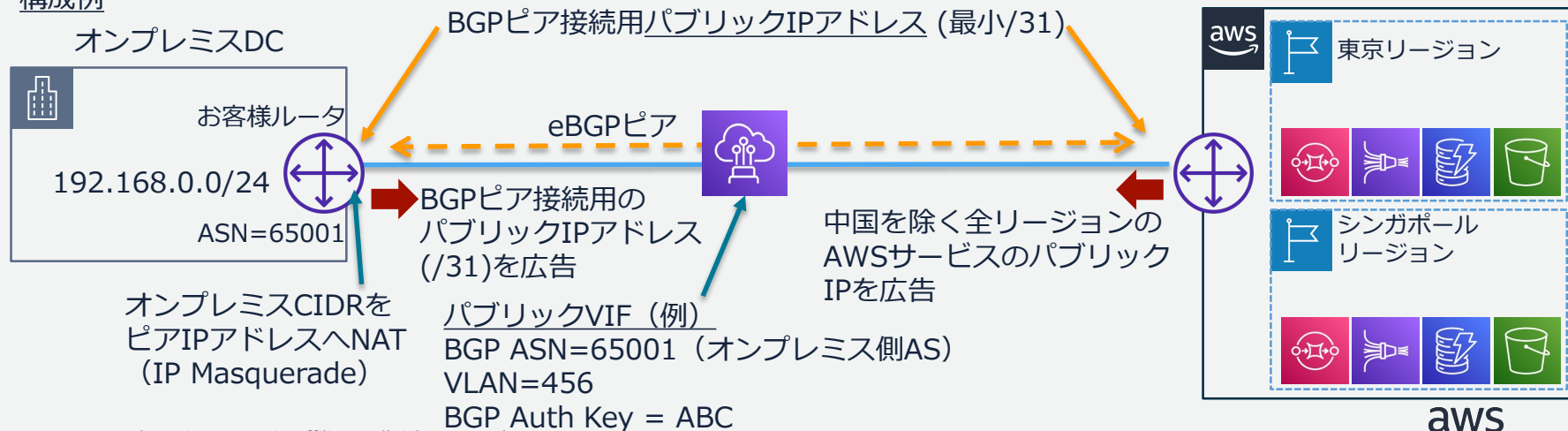
- オンプレミスを複数のVPCへ接続するために複数の**プライベートVIF**を使用
- Direct Connectロケーションに紐づけられたリージョンのVPCにのみ接続可能
- それぞれのVIFで発生するデータ転送の料金は、通信するリソースを所有するAWSアカウントに課金
- お客様ルータで通信対象VPC毎に異なる設定をする場合に採用
- Direct Connectゲートウェイとの混在も可能



パブリック接続

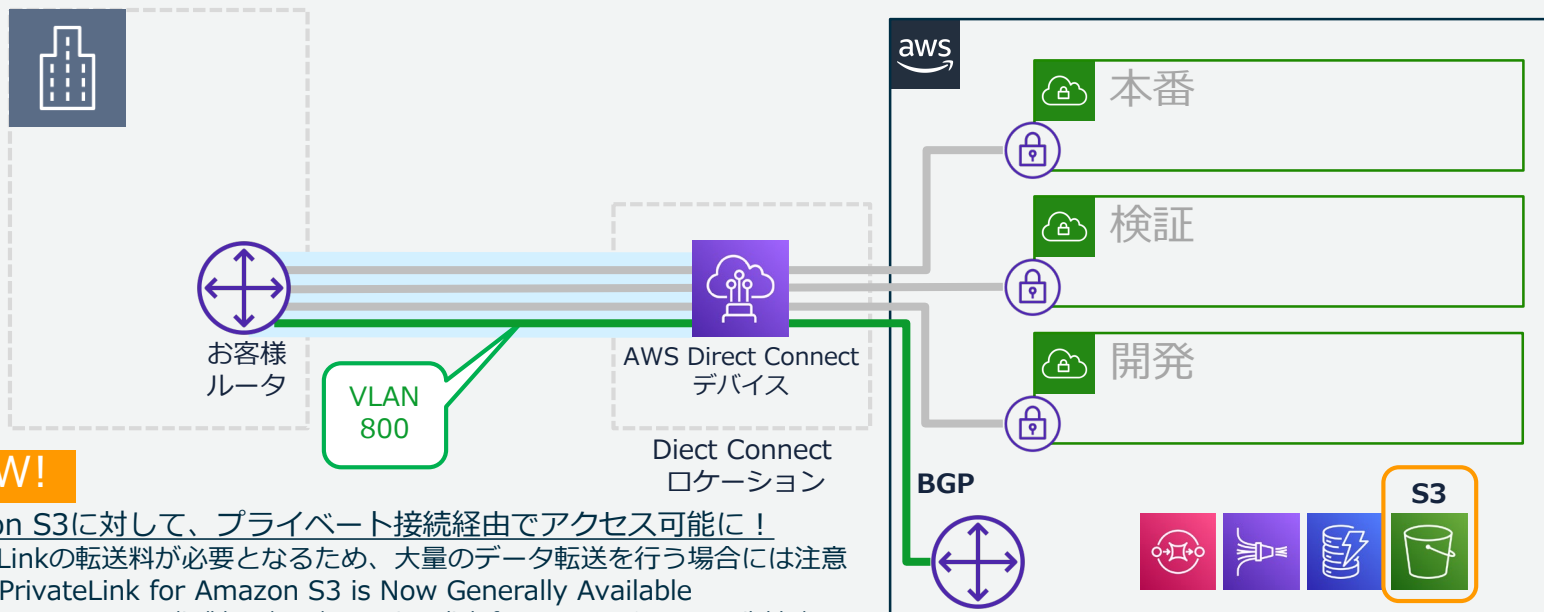
- **パブリックVIF**を使用して中国を除く全リージョンのパブリックサービスへの接続を提供
- オンプレミスのプライベートアドレスをパブリックIPアドレスへNAT
 - ※お客様所有のパブリックIPを利用し、BGPピアを構成
 - ※用意が不可能な場合、AWS所有パブリックIPをAWSサポートへリクエスト可能(状況ヒヤリング)
- 中国を除く全リージョンのAWSサービスのパブリックIPをAWSから広告
 - BGP Communityで経路フィルタし、接続リージョンの経路だけ受け取る事も可能

構成例



パブリックVIFによるパブリックサービスへの接続

- 同一Connection上にパブリックVIFとプライベートVIFの混在が可能
- パブリックVIF追加時、既存プライベート通信に影響を与えない
- パートナーから提供されるサービスでは、利用前に利用可否の確認を推奨



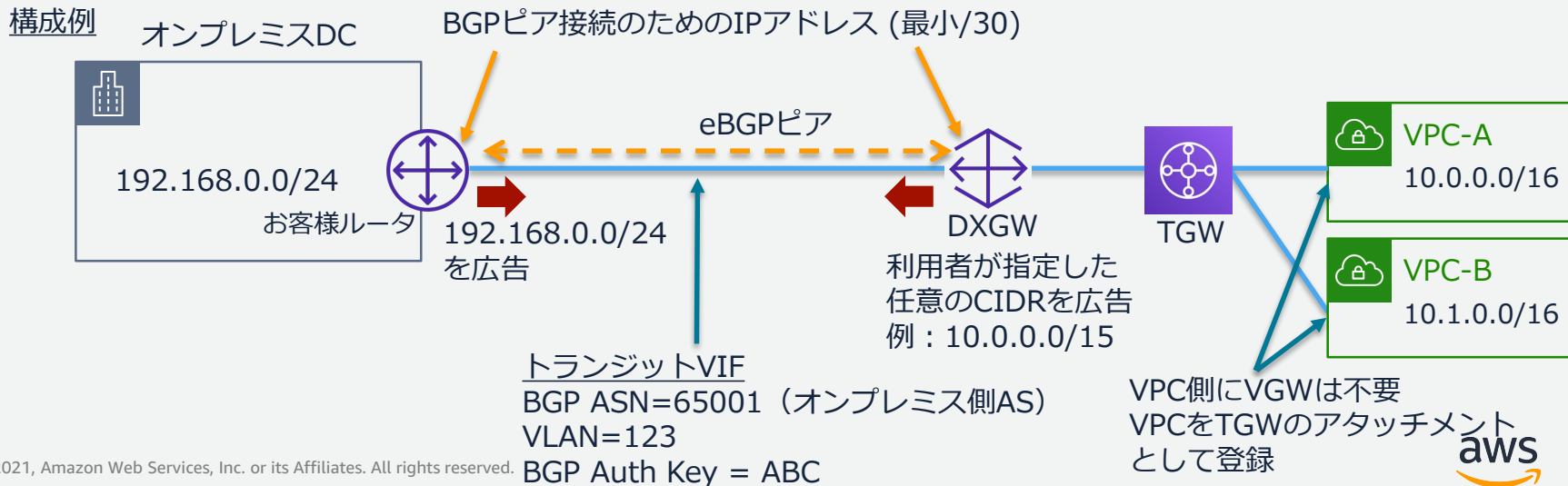
NEW!

Amazon S3に対して、プライベート接続経由でアクセス可能に！
PrivateLinkの転送料が必要となるため、大量のデータ転送を行う場合には注意
- AWS PrivateLink for Amazon S3 is Now Generally Available
<https://aws.amazon.com/jp/blogs/aws/aws-privatelink-for-amazon-s3-now-available/>

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
- 接続要件の多くはプライベートVIFと同等
- 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
- Jumbo Frame (MTU=8500) をサポート

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



Agenda

- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - **AWS Transit Gateway**
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系

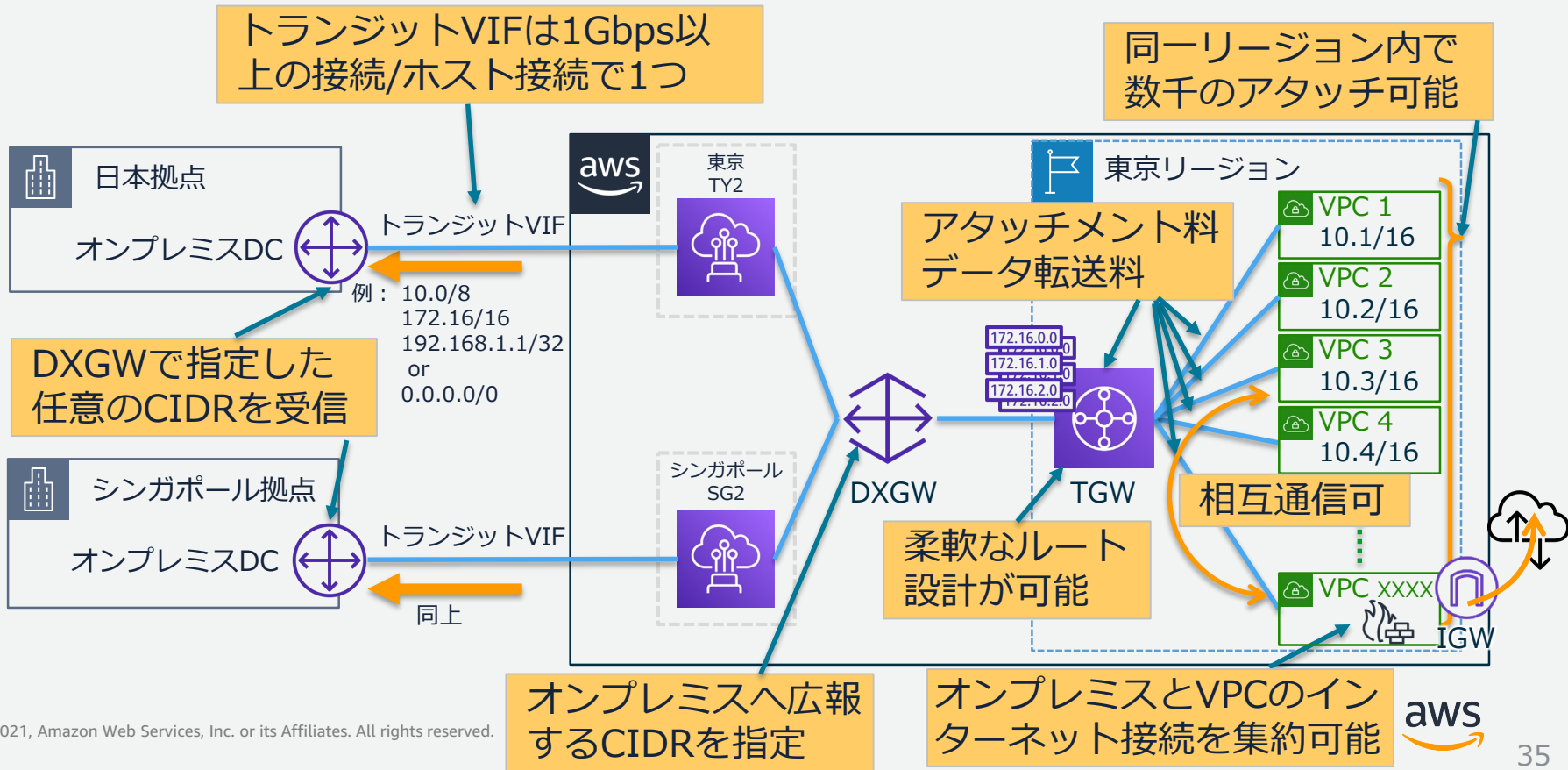


AWS Transit Gateway

トランジットVIF利用時の注意点

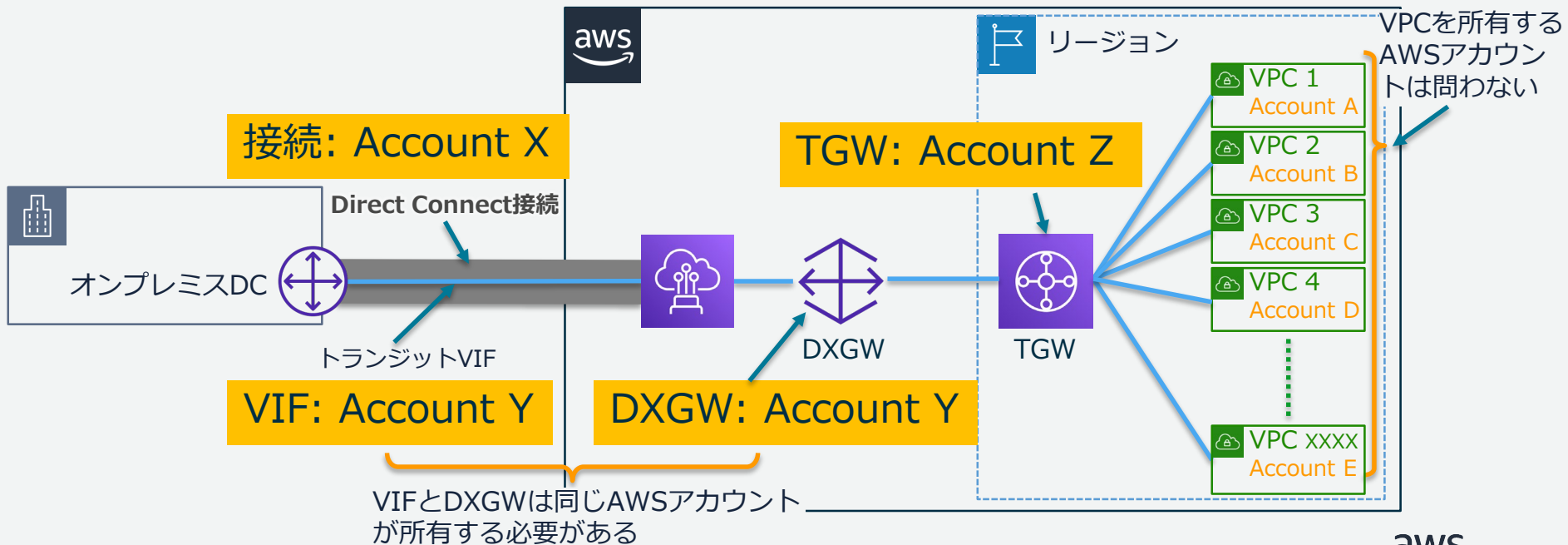
- **トランジットVIFはDirect Connect 1/2/5/10 Gbps接続でのみ作成可能**
 - パートナーを通して提供される共有型接続では利用できない
 - パートナーによって『共有型、専有型』の定義が異なるため、専有型に分類されていても、対応できない場合がある
 - パートナーに確認する際には、サービス名称で判断せず技術窓口にお問い合わせを推奨
- **パートナーのサービスによる制限有無を確認**
 - 多くのパートナーが提供するLayer 3網には利用可能な経路数の上限がある
 - AWSサービスのクォータ（後述）に加え、パートナー網の仕様を把握し全体設計
 - 動的ルーティングを考慮し、初期段階だけではなく運用時に増減する経路数にも注意
- **パートナーが管理するTGWへ接続する際には、サービス仕様を予め確認**
 - VMware on AWSのVMware Managed Transit Gatewayなど、パートナーが提供するTGWに対する接続では、お客様の通信要件がサービス仕様と合致しているか確認

トランジットVIF+TGW : 利用時のポイント



トランジットVIF+TGW : マルチアカウント対応

- 接続とトランジットVIFは、別のAWSアカウントが管理する事が可能
- トランジットVIFとDXGWは同一アカウントが所有
- TGW、VPCを所有するアカウントは問わない



Agenda

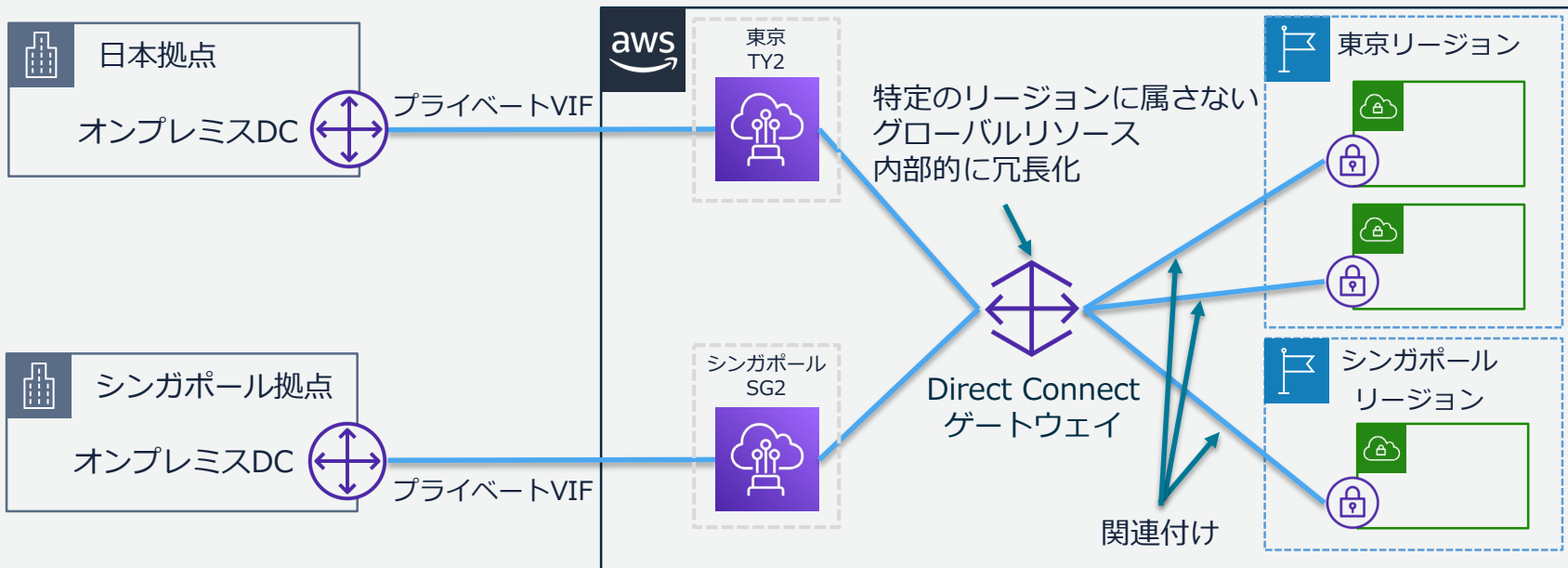
- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - **AWS Direct Connectゲートウェイ**
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系



AWS Direct Connectゲートウェイ

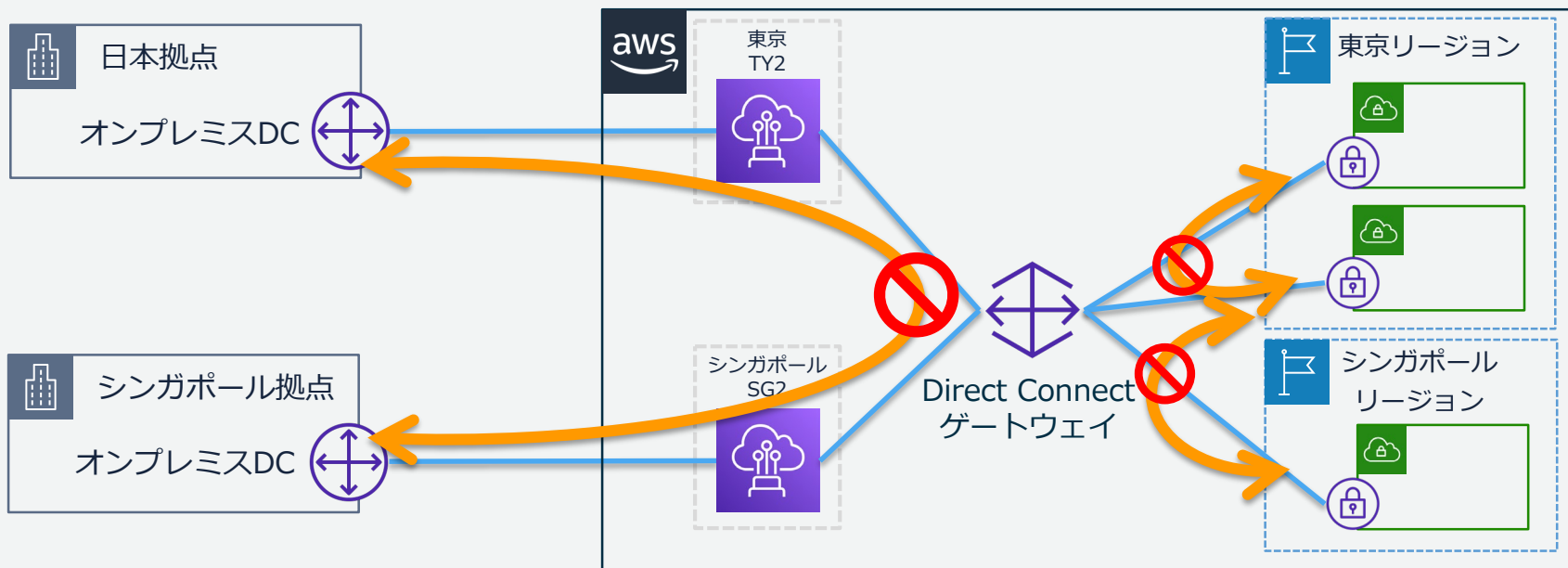
AWS Direct Connectゲートウェイ (DXGW)

- 一つのプライベートVIFを用いたプライベート接続で、中国を除く世界の**全リージョン**の**複数のVPC**と閉域で通信することが出来る (AWS中国アカウントを利用し、中国リージョンに閉じた環境では、複数のVPCに接続可能)
- 無料で利用でき、ロケーションと同一リージョンへは遅延などの心配はない



AWS Direct Connectゲートウェイ利用時の注意

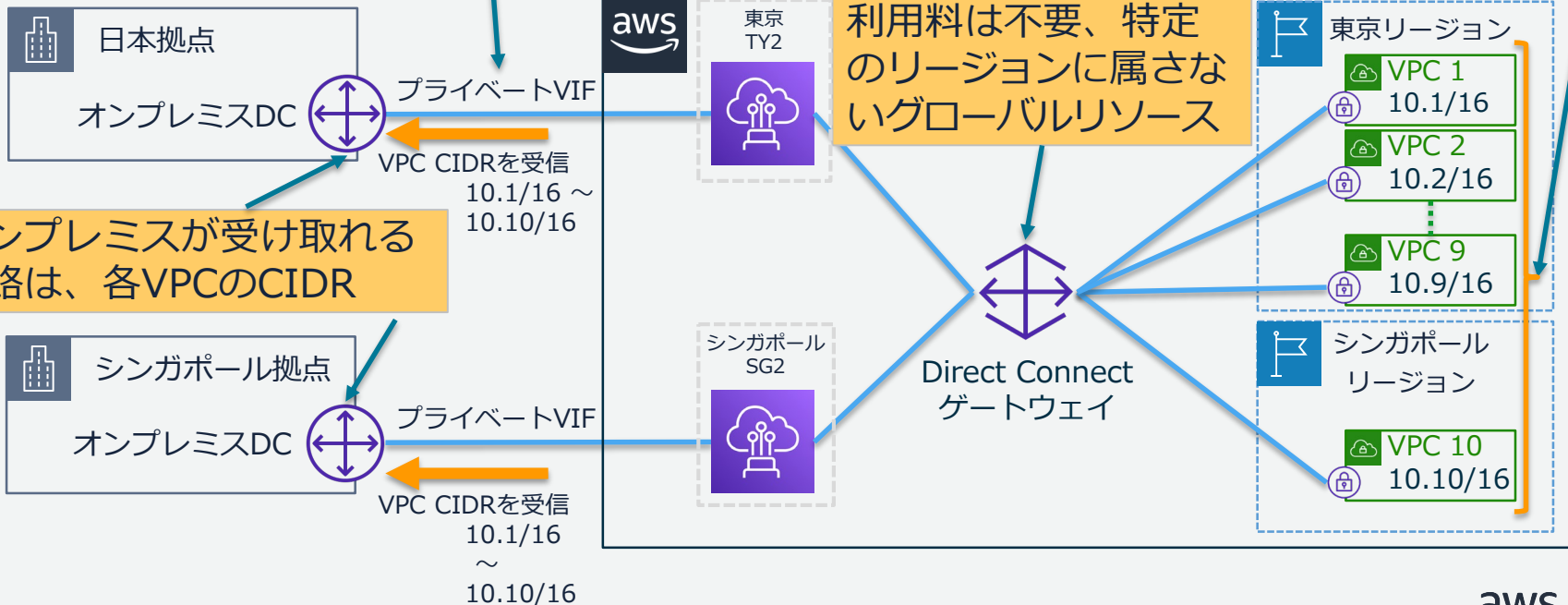
- オンプレミスからオンプレミス、VPCからVPCへ折り返し通信は不可
 - CloudHubと呼ぶオンプレミス間通信が必要な場合、VGWへ接続
- VPC間の通信が必要な場合、リージョン内であればPrivateLink、Transit Gatewayなど、リージョンをまたぐ場合にはVPCピアリングで対応



プライベートVIF + DXGW : 利用時のポイント

パートナーが提供する共有型プライベートVIFを利用可能

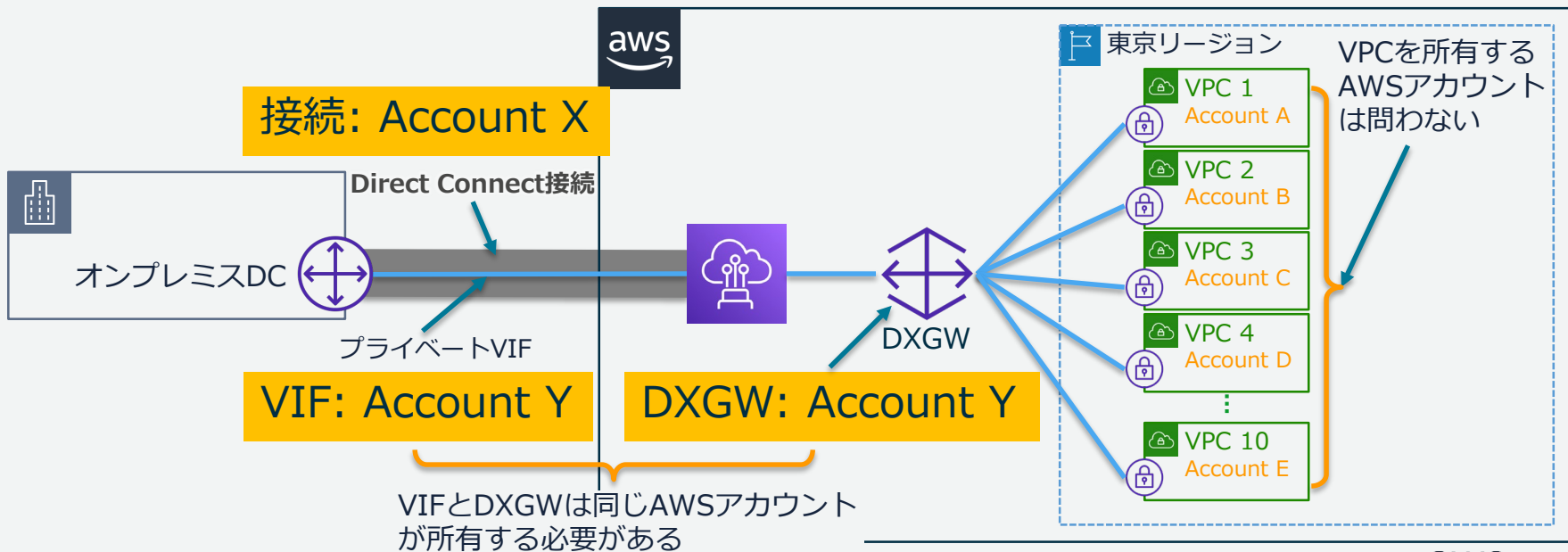
1つのDXGWから最大10のVPCへ通信可能



オンプレミスが受け取れる経路は、各VPCのCIDR

AWS Direct Connectゲートウェイ : マルチアカウント対応

- 接続とプライベートVIFは、別のAWSアカウントが管理する事が可能
- プライベートVIFとDXGWは同一アカウントが所有
- VPCを所有するアカウントは問わない

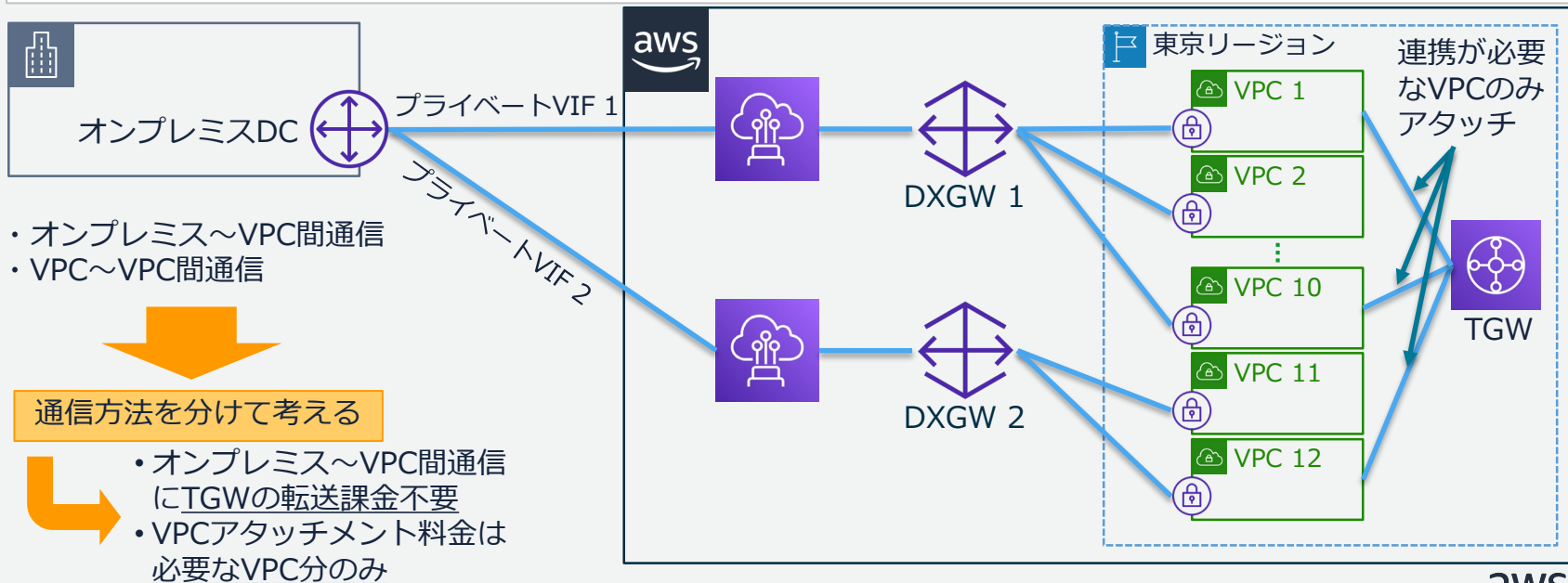


オンプレミスとVPC間の閉域網接続における プライベートVIF(DXGW)とトランジットVIF(DXGW+TGW)の比較

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 10 まで関連付け可能、11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	オンプレミスとVPC間のみ通信	オンプレミスと DXGWに指定する任意のIPで通信 (上限：20、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
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	1Gbps以上の接続/ホスト接続が必要

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10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



Agenda

- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - **パートナー経由のDirect Connect**
- 高い回復性/モニタリング
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系



パートナー経由のDirect Connect

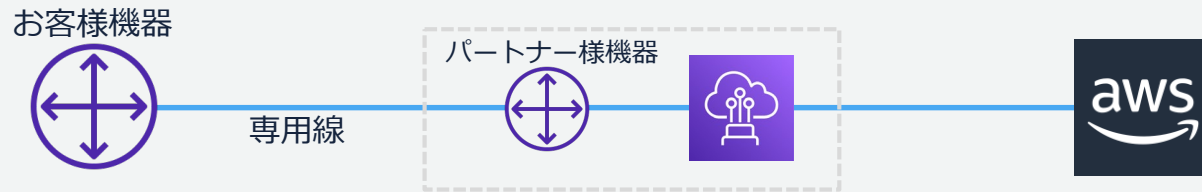
接続のパターン（再掲）



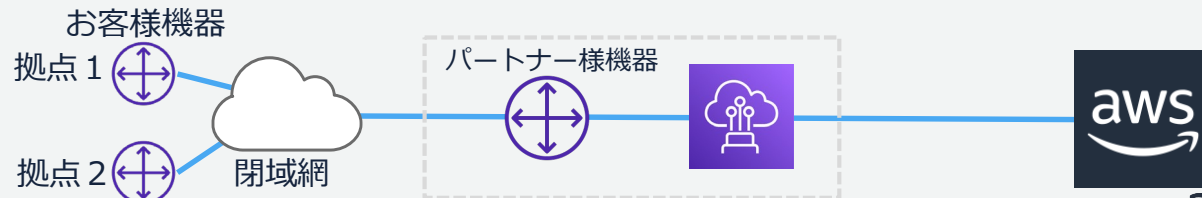
1) Direct Connectロケーションとお客様機器が同じロケーション



2) Direct Connectロケーションからパートナー様専用線で接続

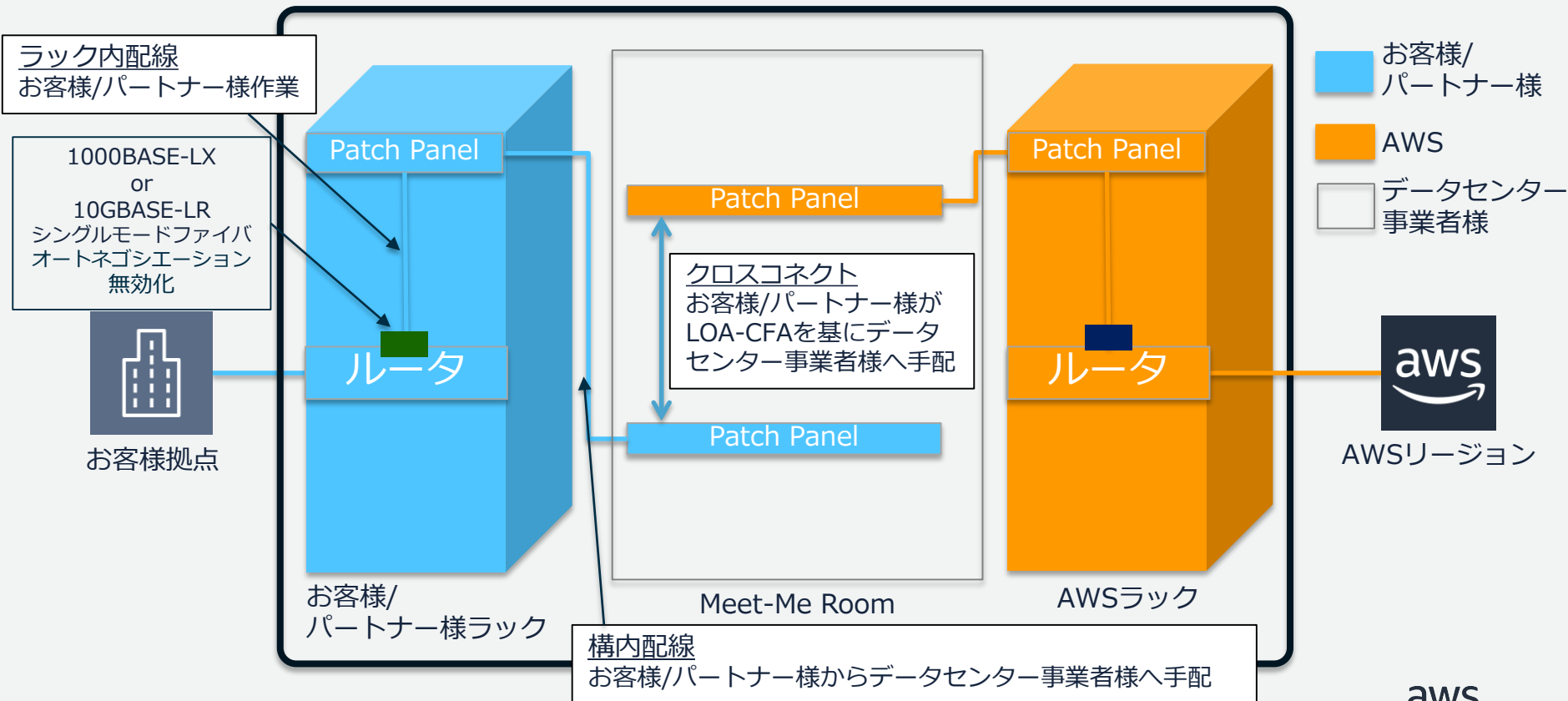


3) パートナー様閉域網(IP-VPN網、モバイル網等)経由で接続



Direct Connect ロケーションでの接続（再掲）

Direct Connect ロケーション



Direct ConnectをサポートするAPNパートナー様

東京リージョンにてAWS Direct Connectロケーションへ接続するための回線を提供することのできるAWSパートナー抜粋

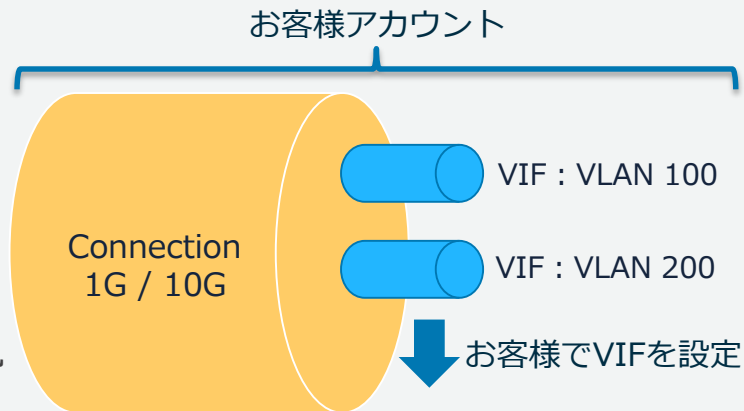
AWS Direct Connect パートナー	Equinix TY2、東京、 日本	Equinix OS1、大阪、 日本	アット東京中 央データセン ター、東京、 日本	Chief Telecom LY、 台北、台湾	Chunghwa Telecom、台 北、台湾
アルテリア・ネットワークス株式会社	✓	✓	✓		
AT Tokyo		✓G	✓G		
AT&T	✓V	✓			
BSO Network Solutions	✓		✓	✓	
BT	✓H		✓		
CHUAN KAI INTERNATIONAL				✓H	
Chief Telecom				✓G	
China Mobile International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

<http://aws.amazon.com/jp/directconnect/partners/>
※最新情報は APN パートナー様にお問い合わせください

パートナーの提供サービス (占有型・共有型)

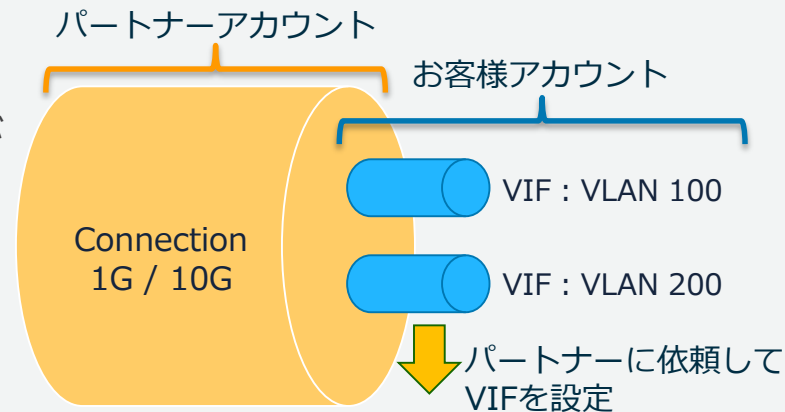
Direct Connect (占有型)

- Connectionをお客様へ提供
- VIFはお客様側で自由に設定可能
- 物理帯域(1G,10G)を占有
- 各VIFは物理帯域をシェア
- 帯域制御が必要な場合、お客様機器で実現



Direct Connect (共有型)

- Connectionはパートナーが所有
- お客様のリクエストベースでパートナーがVIFを設定
- 各VIFは物理帯域をシェア
- パートナー様の機能拡張で、帯域保証型、ベストエフォートなどさまざま



AWS Direct Connect サービスデリバリープログラム(SDP)

AWS Direct Connectサービスデリバリーパートナーは、このサービス特有の技術面の審査を受け、大容量のホスト接続の提供が可能。

これにより、サービス利用者がより豊富なメニューから要件にあった帯域を選択できる。ホスト接続をお客様アカウントで保持し、VIFを作る権限が委譲され運用に柔軟性が増す。

ホスト接続を利用することで効率化される作業例：

- VGWからDXGWへの切り替え時、既存VIFを削除し新たなVIFを作成後、DXGWへ関連付け
- 一時的に異なるDXGWへ経路を変更し、検証環境用VPCへ通信を切りかえる

要件に見合うパートナーを探す



AWS Direct Connect パートナー

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



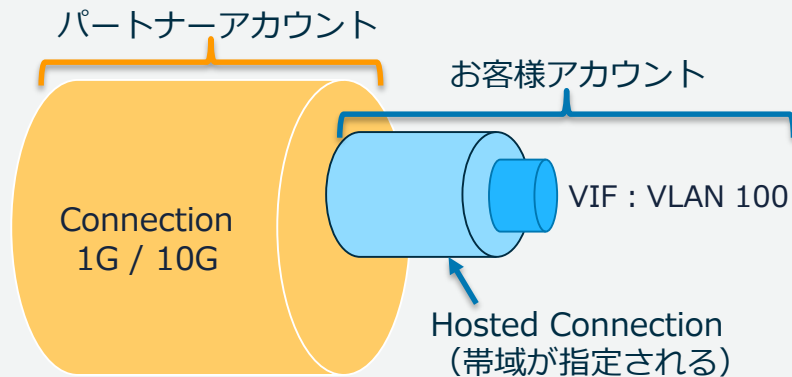
service delivery

提供可能サービスメニューについては各パートナー様窓口へお問い合わせください。

パートナーの提供サービス (ホスト接続: Hosted Connection)

Hosted Connection(ホスト接続)と呼ぶ仮想的なConnectionをパートナーがお客様へ提供

- 50,100,200,300,400,500 Mbps、1,2,5,10 Gbpsの帯域をConnectionの中で占有
- ホスト接続の作成方法はパートナーによる (AWSマネジメントコンソールからは不可)
- Hosted Connectionの中にVIFを一つだけ、お客様アカウントの権限で作成可能
- VIFの削除・再作成ができる



<https://aws.amazon.com/jp/premiumsupport/knowledge-center/direct-connect-types/>
https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/accept-hosted-connection.html

パートナー経由のDirect Connectの注意点

- パートナーのサービスによってVPCへの経路広報のタイプが異なる場合がある
例：
 - ✓ オンプレミスルータから広報している経路情報に集約をかけるもの
 - ✓ ユーザーがパートナーに申告した経路情報が集約されるもの
 - ✓ パートナー網からAWSに対してデフォルトが広報されるもの
 - ✓ パートナー網からAWSに対してプライベートCIDR全てが広報されるもの



異なる回線サービスで冗長を取る場合、回線ごとに経路広報のタイプが異なると予期せぬ経路の偏りや、意図する冗長設計の妨げの原因となり得ます
あらかじめ、パートナーのサービス提供条件のご確認をお願いします

Agenda

- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- **高い回復性/モニタリング**
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系

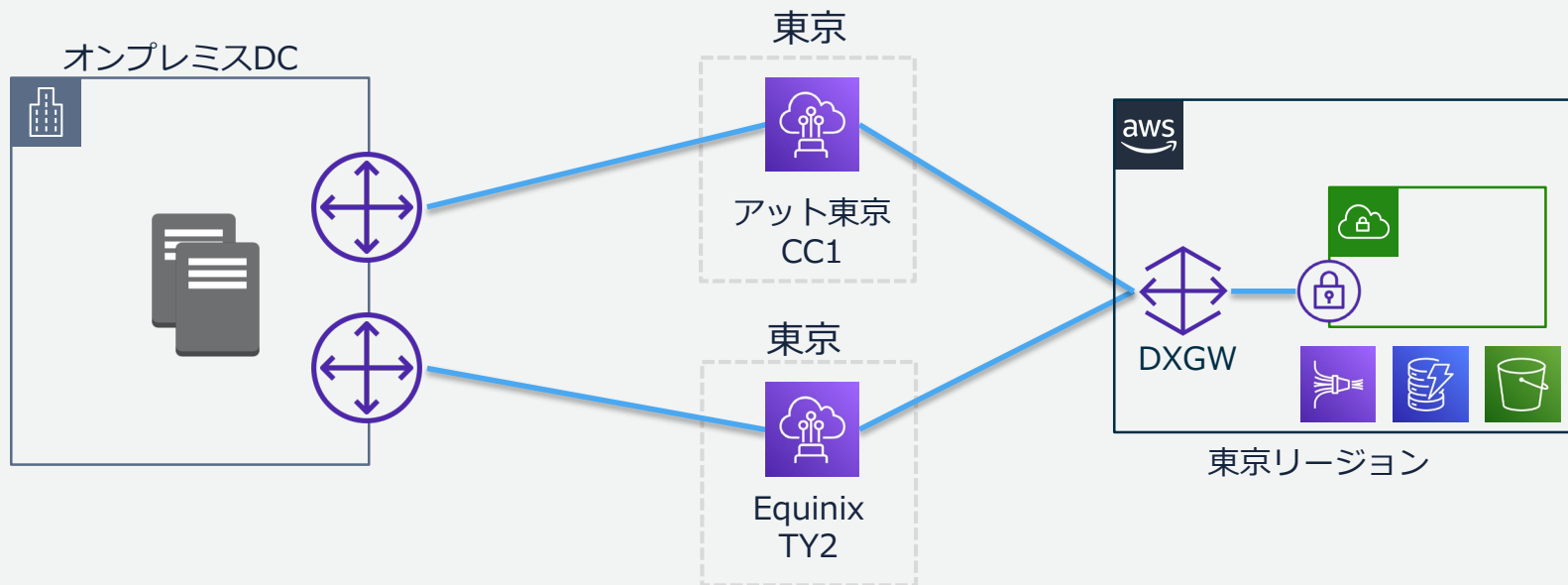


高い回復性/モニタリング

デュアルロケーション (リージョン内で分散)

高い回復性のためにDirect Connectを冗長化する場合は異なるロケーションへの分散が基本

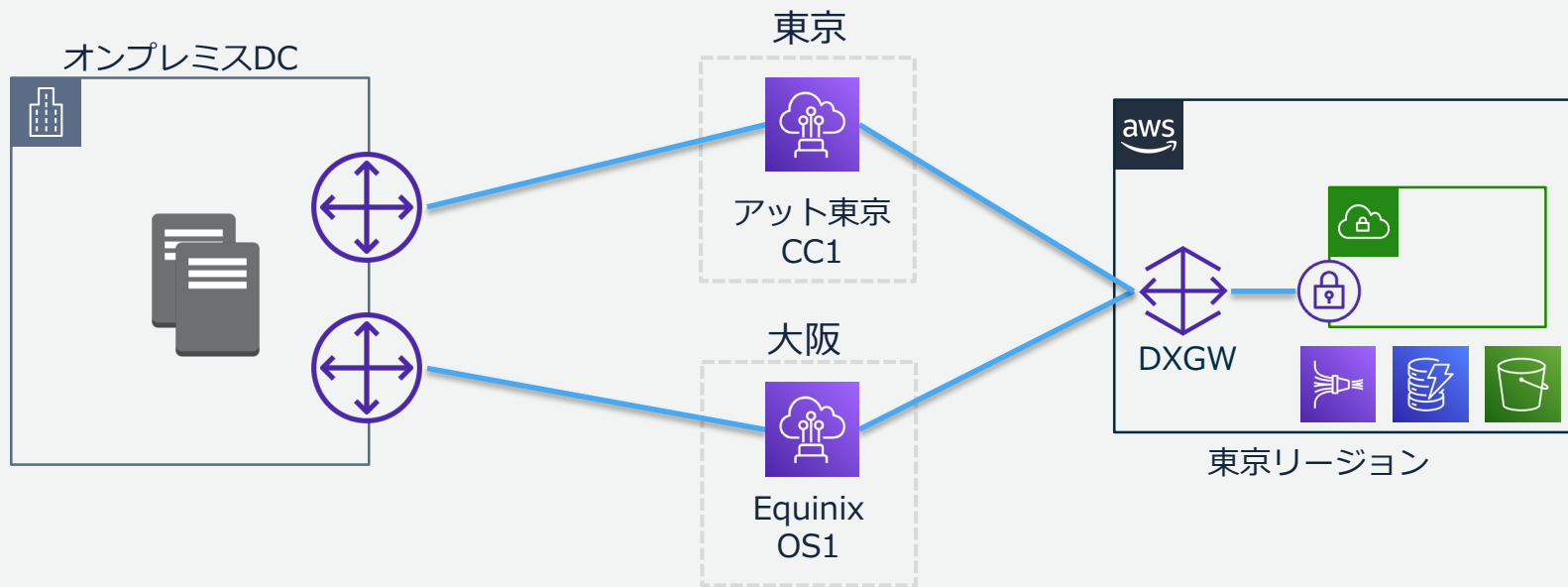
東京リージョンの異なるDirect Connectロケーションを用いた冗長構成の例



<https://aws.amazon.com/jp/directconnect/resiliency-recommendation/>

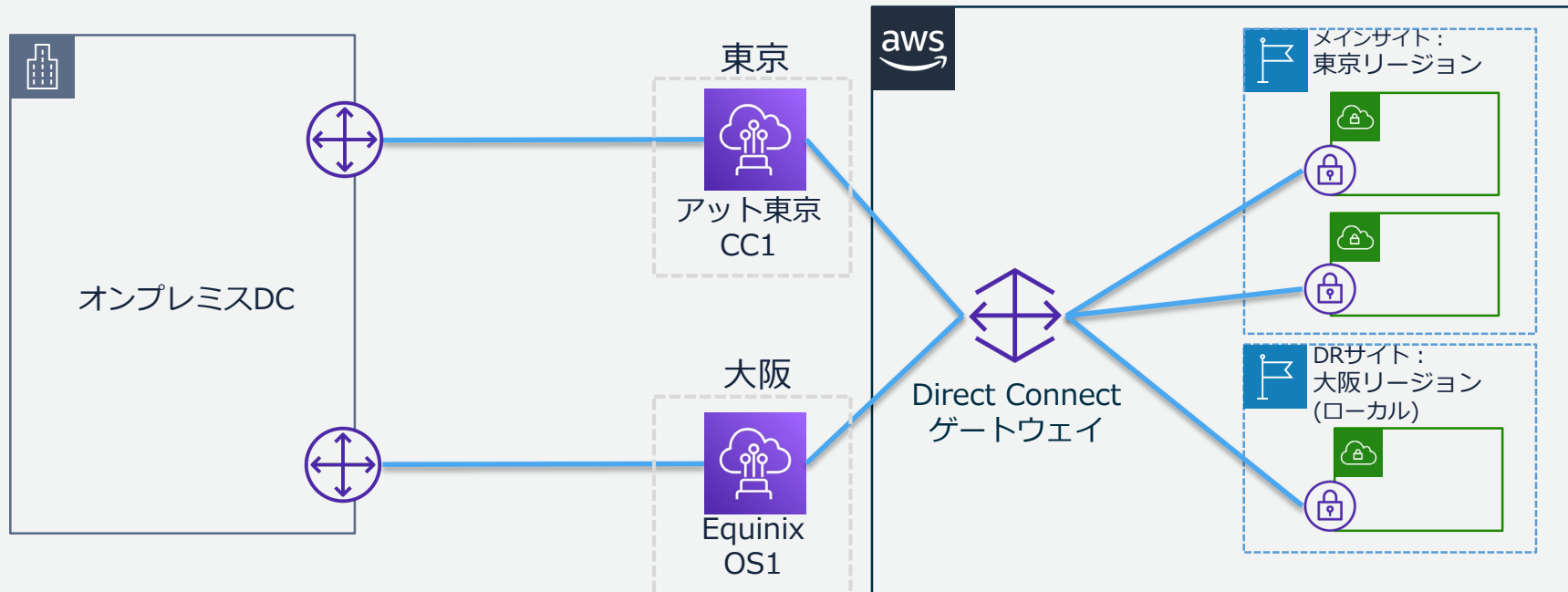
デュアルロケーション (東京・大阪で分散)

東京と大阪に分散したDirect Connectロケーションを用いた冗長構成の例



デュアルロケーション [東阪分散+大阪リージョン(ローカル)]

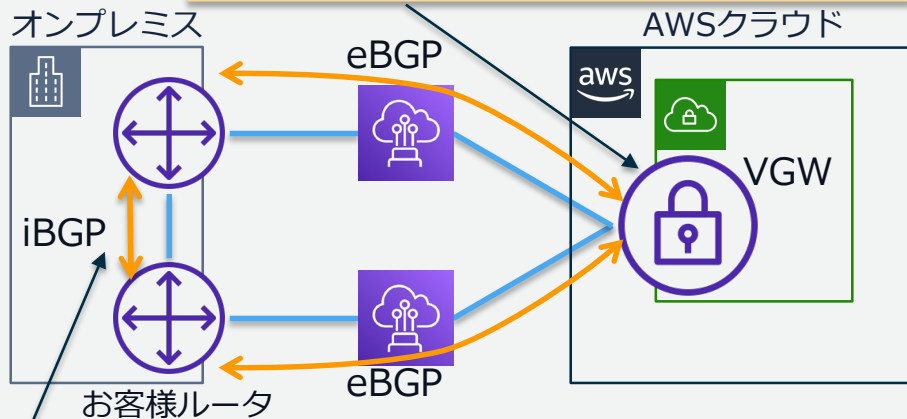
Direct Connectゲートウェイを用いて大阪リージョンへ接続する構成例



冗長構成における経路制御

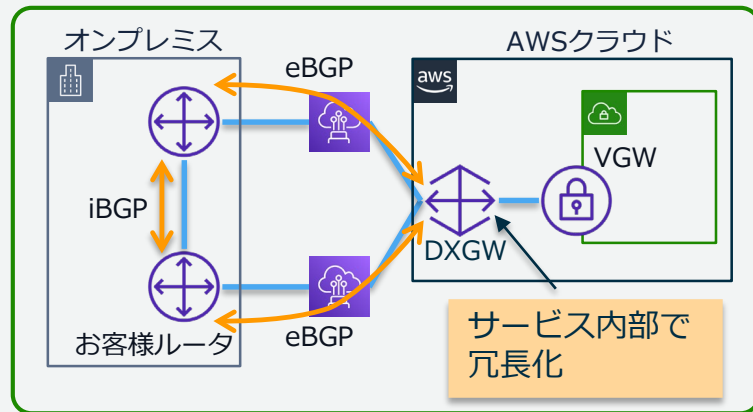
- VPC上のVGW(Virtual Private Gateway)に複数のVIFを終端
- BGPのパス属性を用いて経路を制御する
- AWS上の設定ではなく、お客様ルータの設定により経路制御を行う

論理的には一つのオブジェクトに見えるが、実際には物理的に冗長化されている



iBGPにより同AS内の隣接ルータにBGPのパス属性値を伝達し、どちらの経路を選択するかAS内で総合的に判断

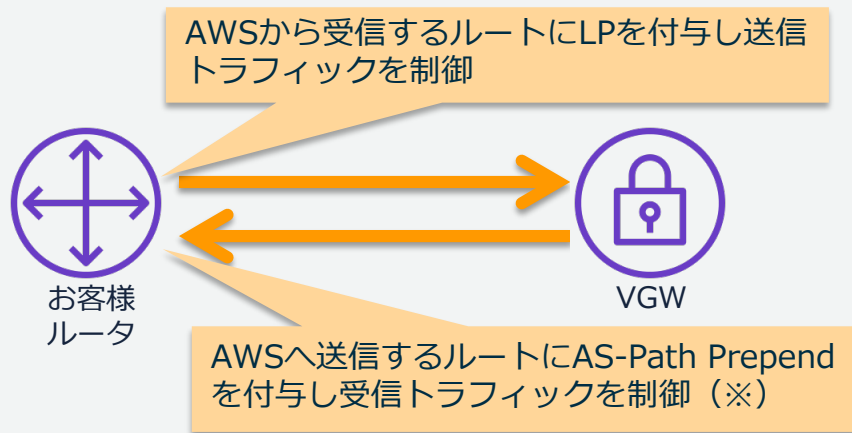
Direct Connectゲートウェイ(DXGW)利用の場合



サービス内部で冗長化

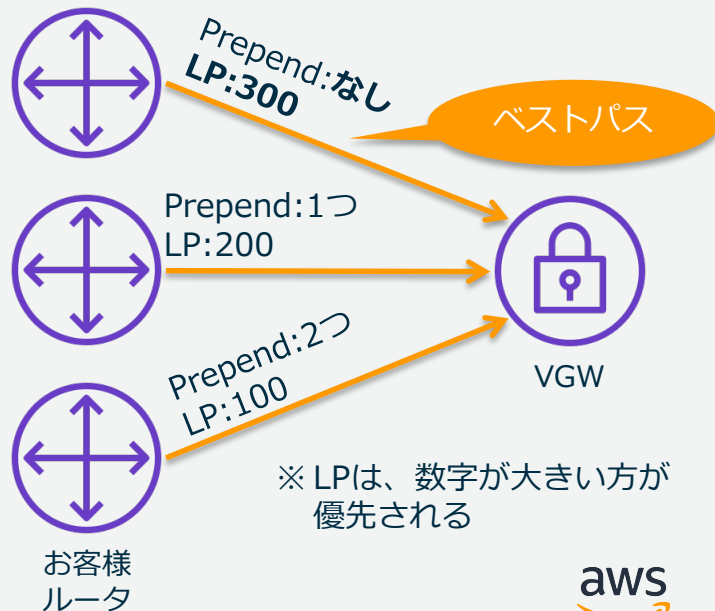
BGPパス属性を用いた経路制御：LP+AS-Pathの例

- 同じ宛先を持つ複数のBGPルートから、ベストパスを選択するためにルータによって評価される属性値
- 以下の例ではLP(Local Preference)とAS-Path Prependを利用



※ AWSに広告する経路のLocal Preferenceを制御するためのBGPコミュニティでも同様に受信トラフィックをコントロール可能

3つの経路で優先制御するユースケース



※ LPは、数字が大きい方が優先される

冗長構成における経路制御：注意点

- AWS上の設定ではなく、お客様ルータの設定により経路制御を行う
- AWSからオンプレミスへの通信は、以下の順に評価される

最初

1. より詳細な(サブネットマスクが小さな)ルート

2. BGP Local Preference Communityタグ

最後

3. BGP AS Path属性

オンプレミス環境の経路制御方針に合わせ、いずれかの方法を選択
1つの機能で制御する場合、他のパラメーターは同一にする

ルーティングポリシーと BGP コミュニティ - AWS Direct Connect

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html#private-routing-policies>

BGPコミュニティ（1）

パブリック接続で使用可能なもの

AWSに広告するプレフィックスの伝播を制御するためのBGP コミュニティ

- 7224:9100—ローカル AWS リージョン内のみ伝播
- 7224:9200—同じ大陸のすべての AWS リージョン (例：北米全域)に伝播
- 7224:9300—グローバル (すべてのパブリック AWS リージョン)に伝播
- デフォルト = すべてのパブリック AWS リージョン (グローバル) に伝播

AWSが広告するプレフィックスに付与されるBGP コミュニティ

- 7224:8100— AWS Direct Connect のプレゼンスポイントが関連付けられている AWS リージョンと同じリージョンから送信されるルート
- 7224:8200—AWS Direct Connect のプレゼンスポイントが関連付けられている大陸と同じ大陸から送信されるルート
- タグなし—グローバル (すべてのパブリック AWS リージョン)

https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/routing-and-bgp.html

BGPコミュニティ（2）

プライベート接続で使用可能なもの

AWSに広告する経路のローカルプリファレンスを制御するためのBGPコミュニティ

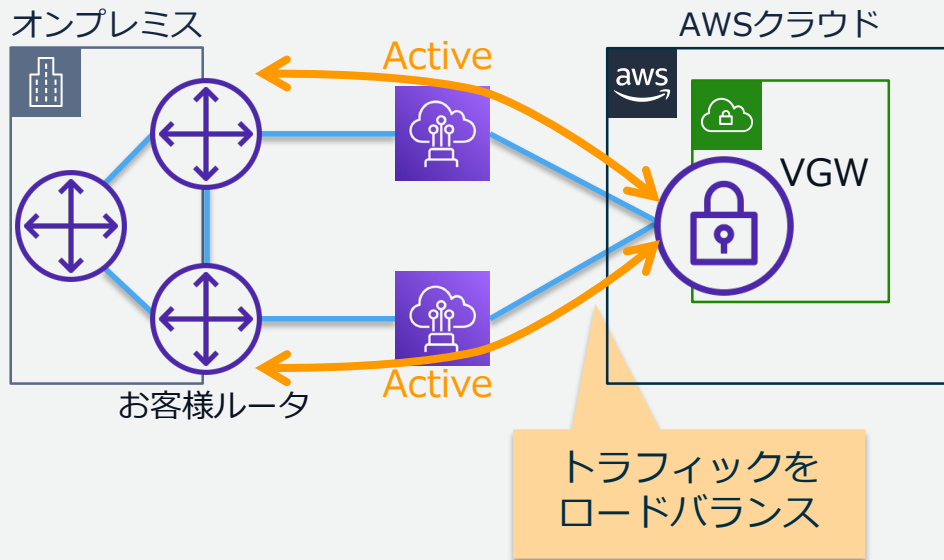
- 7224:7100—優先設定：低
- 7224:7200—優先設定：中
- 7224:7300—優先設定：高

ご参考：AS-PATHプリペンドでもAWSからお客様ルータ向けのトラフィックの優先度を制御可能

https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/routing-and-bgp.html

経路制御 (Active/Active)

- お客様ルータで何も設定しなければ、AWSからオンプレミスへの通信は2本のDirect Connectの間でトラフィックをロードバランスし、Active/Activeとなる
- オンプレミスからAWSへの通信は、お客様ルータの設定による



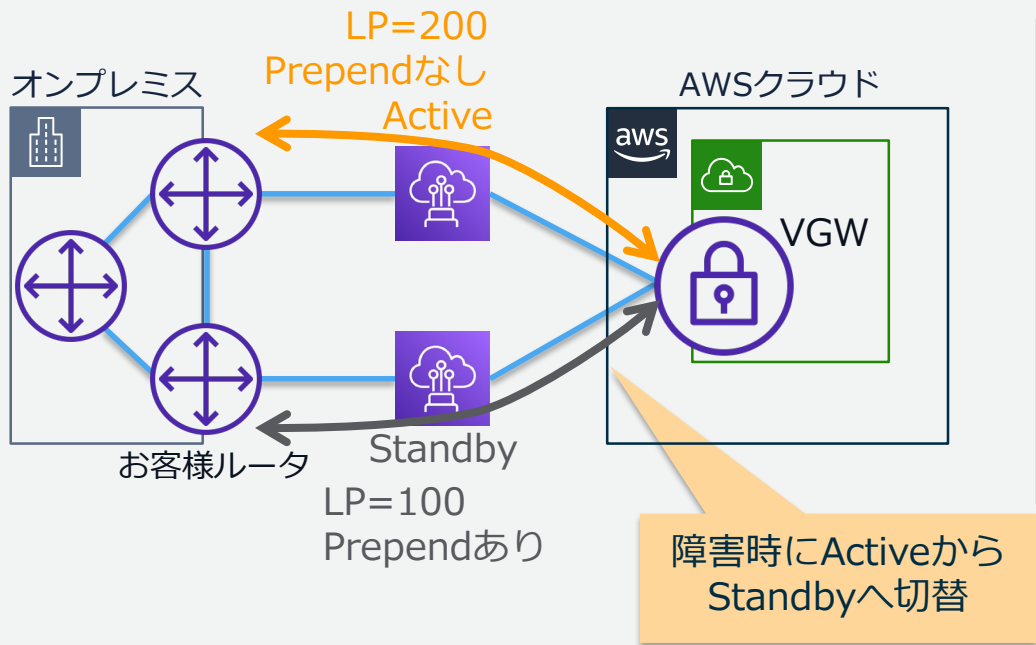
それぞれのルータで以下が等しくなるようにする必要がある。

- AWSへ送信するBGPルートのASパス長、LPコミュニティ、MED
- AWSから受信するBGPルートに付与するLP値

- ※ 片系障害時にトラフィックが迂回した場合でも迂回先で輻輳が発生しないように帯域管理が必要
- ※ 通信形態によってはトラフィックが均等にバランスされない場合もある

経路制御 (Active/Standby)

- 2本のDirect Connectどちらかを通常利用し、障害時はStandby側へ自動切り替えを行う
- AWSの機能では、Active/Standbyを指定する機能は無い

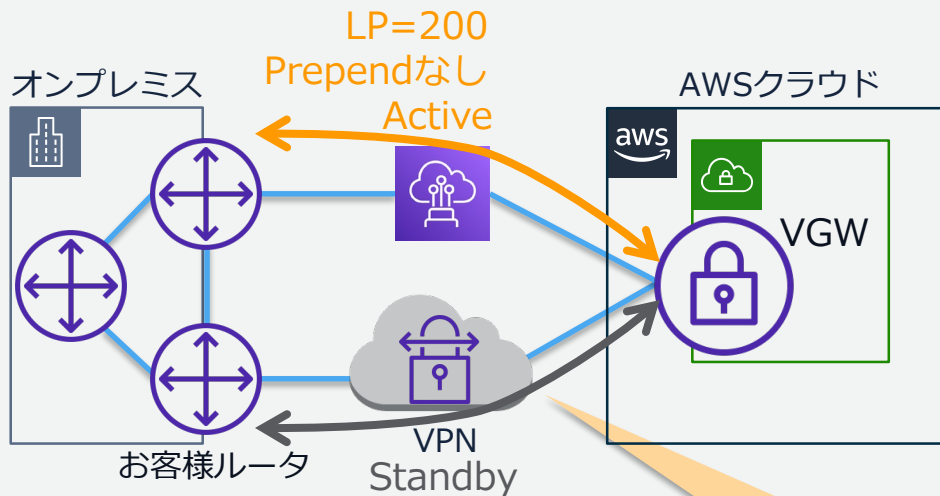


お客様ルータでBGP属性値を以下のように設定しActive/Standbyを制御

- AWSへ広告するBGPルート of ASパス長をAS-Path Prepend を使ってStandby側が長くなるようにする
- AWSから受信するBGPルートに付与するLP値をStandby側で小さくなるようにする

経路制御 (Direct Connect/VPN)

- Direct Connect障害時のバックアップとしてインターネットVPNを利用
- 予算面で、同等のDirect Connect回線を用意できない際の代替手段



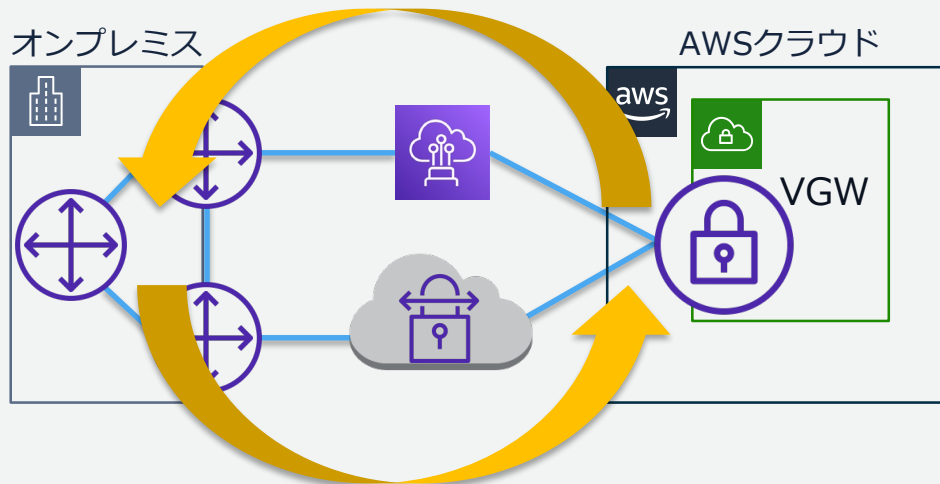
フェールオーバー時にはDirect ConnectとインターネットVPNとの性能差からパフォーマンスに影響が出る場合があるため注意

※ 仕様上、AWSからオンプレミス方向への通信は(パス属性によらず)常にDirect Connectを優先経路となる

Standby用に
インターネットVPN
を利用

非対称ルーティング時の注意

- 冗長構成のDirect Connectにおいて非対称ルーティング（上りと下りで経路が異なる）が発生する事があるが、AWSサービスとしては問題なく通信可能
- この状態が発生しないようにするためには、お客様ルータ側で制御する必要がある



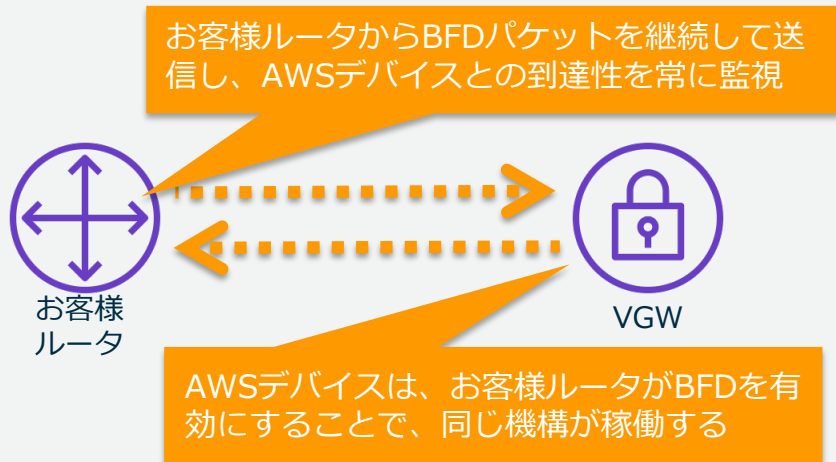
ファイアウォール利用時には非対称ルーティングに対応していないクラスタを利用するとパケットが破棄されるので注意

StandbyでVPNを利用している場合には非対称ルーティングは避ける
（送受信パケットにおけるレイテンシーの違いを避ける）

VPN を AWS Direct Connect 接続のバックアップとして設定する方法を教えてください。
<https://aws.amazon.com/jp/premiumsupport/knowledge-center/configure-vpn-backup-dx/>

障害時の経路切替時間の短縮：推奨方法

- BFD(Bidirectional Forwarding Detection)を利用し、高速に障害を検知
- AWSデバイス側はお客様ルータで設定した値に合わせ、機能が有効化
- AWSデバイスの状態検出の間隔は最低300ミリ秒、乗数は3
- 300ミリ秒 × 3回 (+作動時間)の約1秒程度でダウンを検知、インターフェイスを停止



Cisco

```
bfd interval 50 min_rx 50 multiplier 3
```

```
router bgp CUSTOMER_BGP_ASN  
neighbor NEIGHBOR_IP_ADDRESS fall-over bfd
```

Juniper

```
edit interfaces ge-0/0/1  
edit bfd-liveness-detection  
set minimum-interval 50  
set multiplier 3
```

DX 接続で BFD を有効にする方法を教えてください

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/enable-bfd-direct-connect/>

障害時の経路切替時間の短縮：BFD非対応ルーター 対策：BGPのkeepalive/Hold Timerのチューニング

お客様ルーターがBFDに対応していない場合にのみ、BGPのkeepalive/Hold Timeをチューニングして切替時間を短縮する

- AWSデバイス側はお客様ルーターで設定した値に合わせて稼働する
- AWSデバイスにおけるHoldtime時間の定義は内部的に管理、公開情報は無し
- 安定化の為に、Holdtimeを20～30秒程度とすることが適切と考える

Ciscoルーターの場合

```
router bgp CUSTOMER_BGP_ASN  
neighbor NEIGHBOR_IP_ADDRESS timers 10 30
```

デフォルト値 Keepalive=60秒 Hold Timer=180秒

Juniperルーターの場合

```
edit protocols bgp group ebgp  
set hold-time 30
```

デフォルト値 Keepalive=30秒 Hold Timer=90秒

参考 Cisco IOS IP Routing: BGP Command Reference (AWS外部サイト)

BGP Commands: neighbor timers through show bgp nsap summary

https://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/command/reference/irg_book/irg_bgp4.html

Amazon CloudWatchによるDirect Connectのモニタリング

NEW!

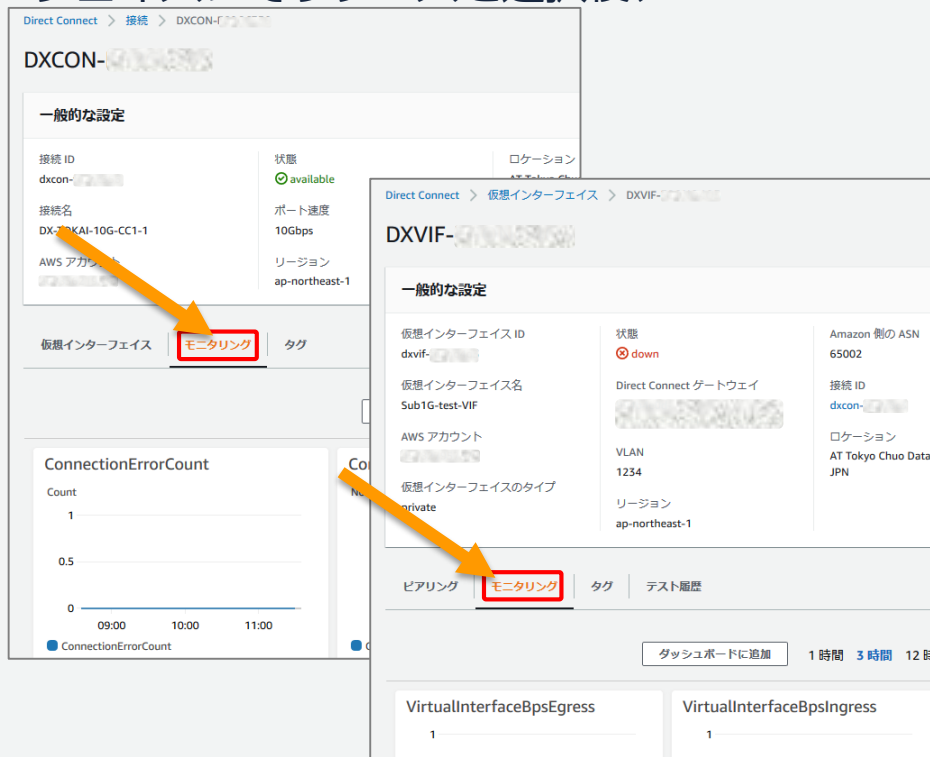
マネジメントコンソールの接続/仮想インターフェイスにてリソースを選択後、“モニタリング”タブから確認可能

接続のメトリクス(ホスト接続を除く)

- Connectionのアップ/ダウン
- Connectionの送受信データ転送量
- Connectionの送受信パケットレート
- MACレベルエラー (CRCエラーを含む)
- AWS側で送受信される光レベル

仮想インターフェイス(=VIF)のメトリクス

- VIFの送受信データ転送量
- VIFの送受信パケットレート

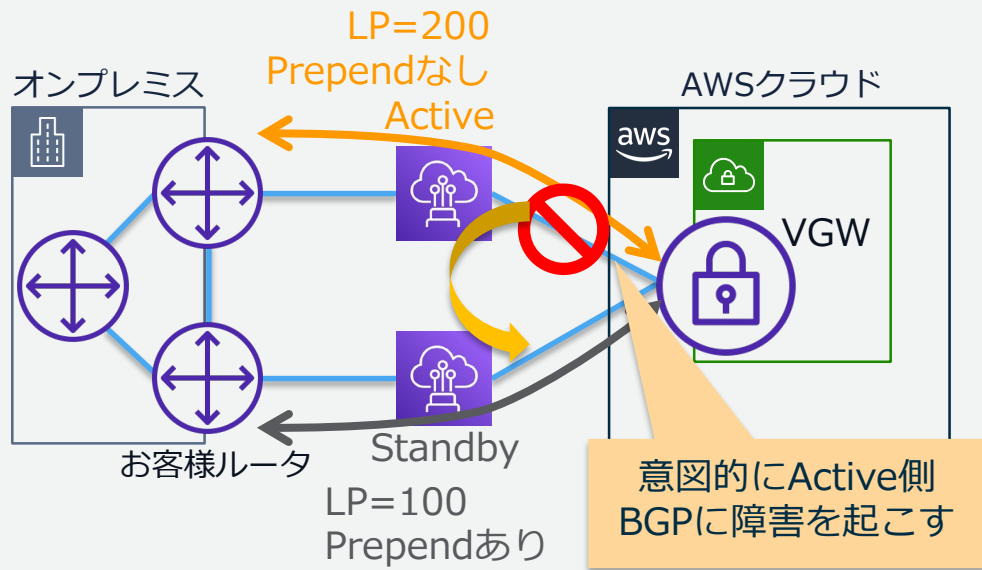


https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/monitoring-cloudwatch.html

Direct Connect フェイルオーバーテスト

NEW!

冗長化構成における切り替えテストを実施する際、AWS側の操作のみでVIFのBGPピアを一定時間ダウンできるようになりました。これにより、AWSルーターのメンテナンス等の影響を予めテストしやすくなりました。



【注意】

パートナー経由のVIFを利用している場合、パートナー側で監視している可能性があるため、予めご確認ください。

<https://aws.amazon.com/jp/about-aws/whats-new/2020/06/aws-direct-connect-enables-failover-testing/>

参考 : Direct Connect フェイルオーバーテスト : 実施例

The screenshot shows the AWS Direct Connect console interface. At the top, the breadcrumb navigation reads "Direct Connect > ... > DXVIF-**[redacted]**". Below this, the main header displays "DXVIF-**[redacted]**". To the right of the header are three buttons: "Actions ▲", "Edit", and "Delete". The "Actions" dropdown menu is open, showing the following options: "Download", "Sample configuration", "Failover test", "Bring down BGP", and "Cancel test". An orange arrow points from the "Failover test" option to the "State" field in the configuration table below. The configuration table has two columns: "General configuration" and "State".

General configuration	State
Virtual interface ID dxvif- [redacted]	✔️ available
Virtual interface name dxlab-maint	
AWS account [redacted]	
	Virtual private gateway vgw- [redacted]
	VLAN 10

参考 : Direct Connect フェイルオーバーテスト : 実施例

Start failure test ×

⚠ Failure testing puts the virtual interface in a down state and will cause an outage if you have not configured redundancy. Failure testing will put virtual interface dxvif-fh8pi7u8 in an induced failure state by putting its BGP peerings into a down state.

Test maximum time (minutes) - *optional*

Valid ranges are 1 - 180. Default is 180 minutes.

To confirm test, type *Confirm* in the field below.

Cancel **Confirm**

参考 : Direct Connect フェイルオーバーテスト : 実施例

The screenshot displays the AWS Direct Connect console interface. At the top, a green notification banner states "BGP failure testing successfully started". Below this, a warning message with a red triangle icon reads "Disable BGP test starting" and explains that the test is starting, causing the virtual interface to lose connectivity. The interface name "DXVIF-" is visible, along with "Actions", "Edit", and "Delete" buttons. The "General configuration" section shows the "Virtual interface ID" as "dxvif-" and the "State" as "testing", with an information icon next to the state label. Three orange arrows point to the notification banner, the warning message, and the "testing" state label.

✓ BGP failure testing successfully started

Disable BGP test starting
A test to put BGP peerings into a down state for this virtual interface is starting now. This virtual interface will lose connectivity during the course of this test.

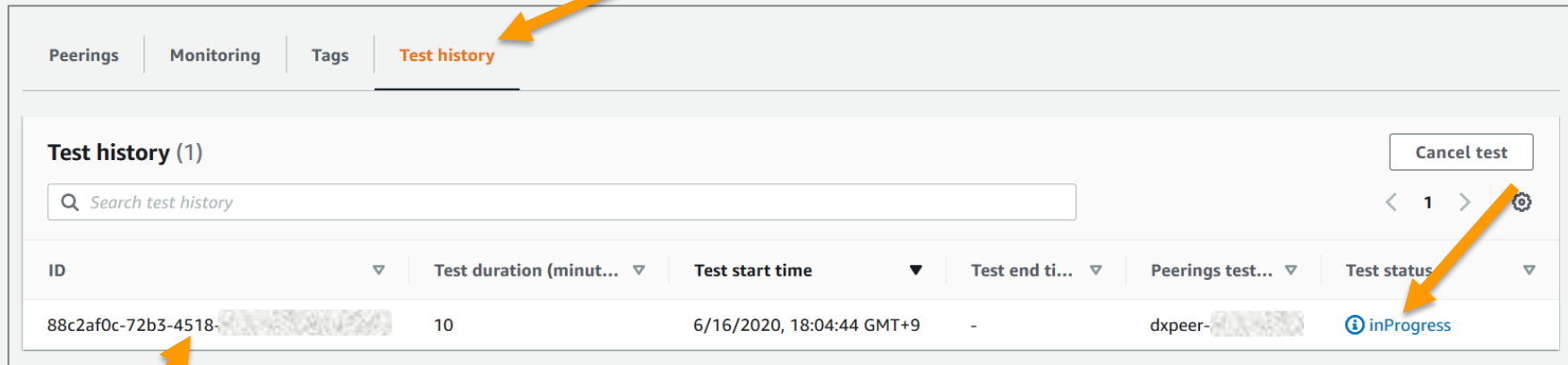
DXVIF- [redacted]

Actions ▼ Edit Delete

General configuration

Virtual interface ID	State
dxvif-[redacted]	testing

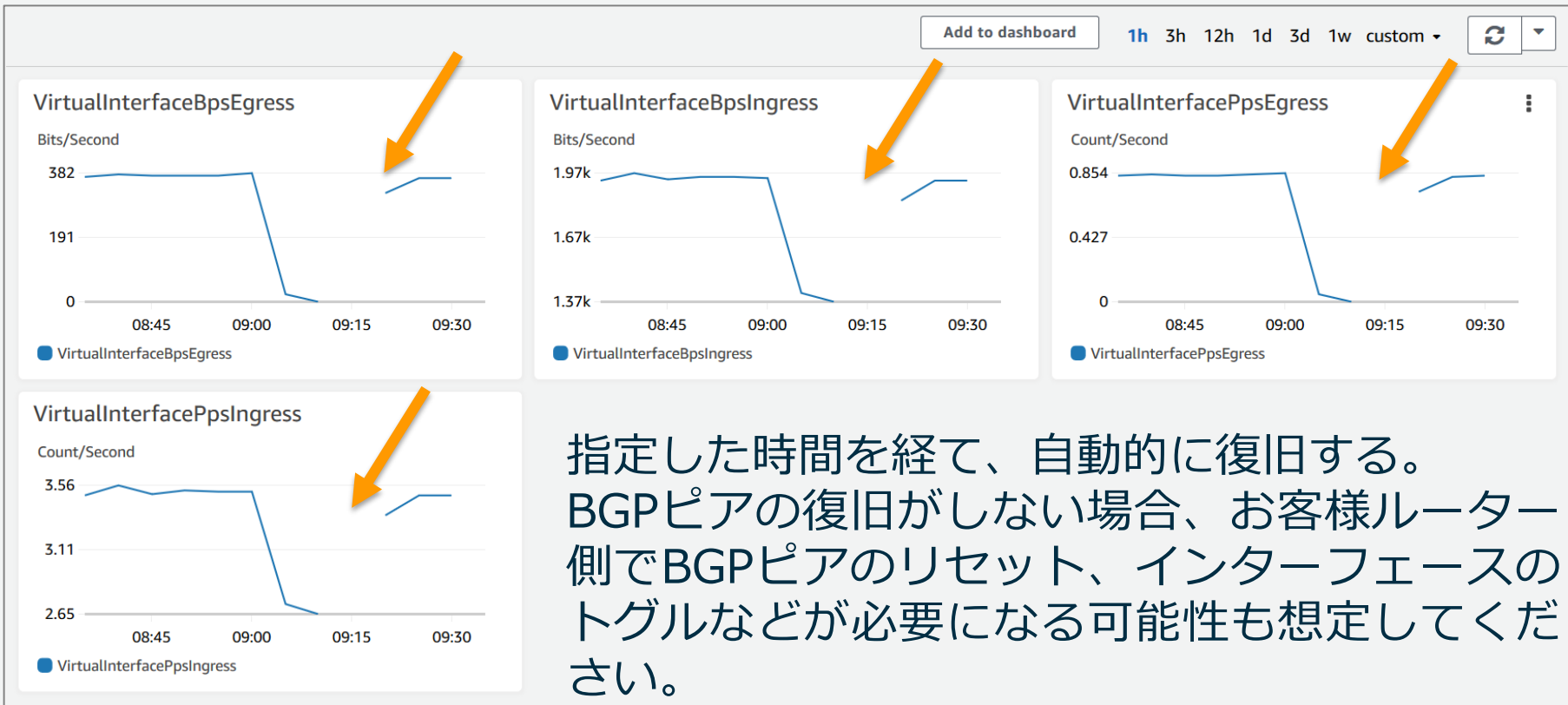
参考 : Direct Connect フェイルオーバーテスト : 実施例



The screenshot displays the AWS Direct Connect console interface. At the top, there are navigation tabs: Peering, Monitoring, Tags, and Test history. The Test history tab is selected. Below the tabs, there is a section titled "Test history (1)" with a search bar and a "Cancel test" button. A table below shows the test history with columns: ID, Test duration (minut...), Test start time, Test end ti..., Peering test..., and Test status. The table contains one entry with ID 88c2af0c-72b3-4518-..., a duration of 10 minutes, a start time of 6/16/2020, 18:04:44 GMT+9, and a status of inProgress. An orange arrow points to the "Test history" tab, another points to the "Cancel test" button, and a third points to the "inProgress" status in the table row.

ID	Test duration (minut...)	Test start time	Test end ti...	Peering test...	Test status
88c2af0c-72b3-4518-...	10	6/16/2020, 18:04:44 GMT+9	-	dxpeer-...	inProgress

参考 : Direct Connect フェイルオーバーテスト : 実施例



Agenda

- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- **クォータについて**
- What's New (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系



クォータについて

各種クォータについて

Direct Connectに関するクォータの一覧

コンポーネント	制限	コメント
AWS Direct Connect 専用接続あたりのプライベートまたはパブリック仮想インターフェイス数	50	この制限を増やすことはできません
AWS Direct Connect 専用接続あたりのトランジット仮想インターフェイス数	1	この制限を増やすことはできません
AWS Direct Connect ホスト接続あたりのプライベート、パブリック、またはトランジット仮想インターフェイス数※1	1	この制限を増やすことはできません
1つのアカウントで、リージョンごとのアクティブな AWS Direct Connect 接続	10	
Link Aggregation Group (LAG) あたりの仮想インターフェイスの数	50	
プライベート仮想インターフェイスのボーダーゲートウェイプロトコル (BGP) セッションあたりのルート BGP セッションで 100 を超えるルートにアダプタイズしている場合、BGP セッションはアイドル状態になり BGP セッションは DOWN になります。	100	この制限を増やすことはできません
パブリック仮想インターフェイスのボーダーゲートウェイプロトコル (BGP) セッションあたりのルート数	1,000	この制限を増やすことはできません
Link Aggregation Group (LAG) ごとの専用接続数	4	
リージョンごとの Link Aggregation Group (LAG) の数	10	
アカウントあたりの AWS Direct Connect ゲートウェイ	200	
AWS Direct Connect ゲートウェイあたりの仮想プライベートゲートウェイの数	10	この制限を増やすことはできません
AWS Direct Connect ゲートウェイあたりの Transit Gateway 数	3	この制限を増やすことはできません
AWS Direct Connect ゲートウェイあたりの仮想インターフェイス (プライベートまたはトランジット)	30	
オンプレミスからトランジット仮想インターフェイスの AWS へのプレフィックス数	100	この制限を増やすことはできません
AWS からトランジット仮想インターフェイスの AWS への AWS Transit Gateway ごとのプレフィックス数	20	この制限を増やすことはできません

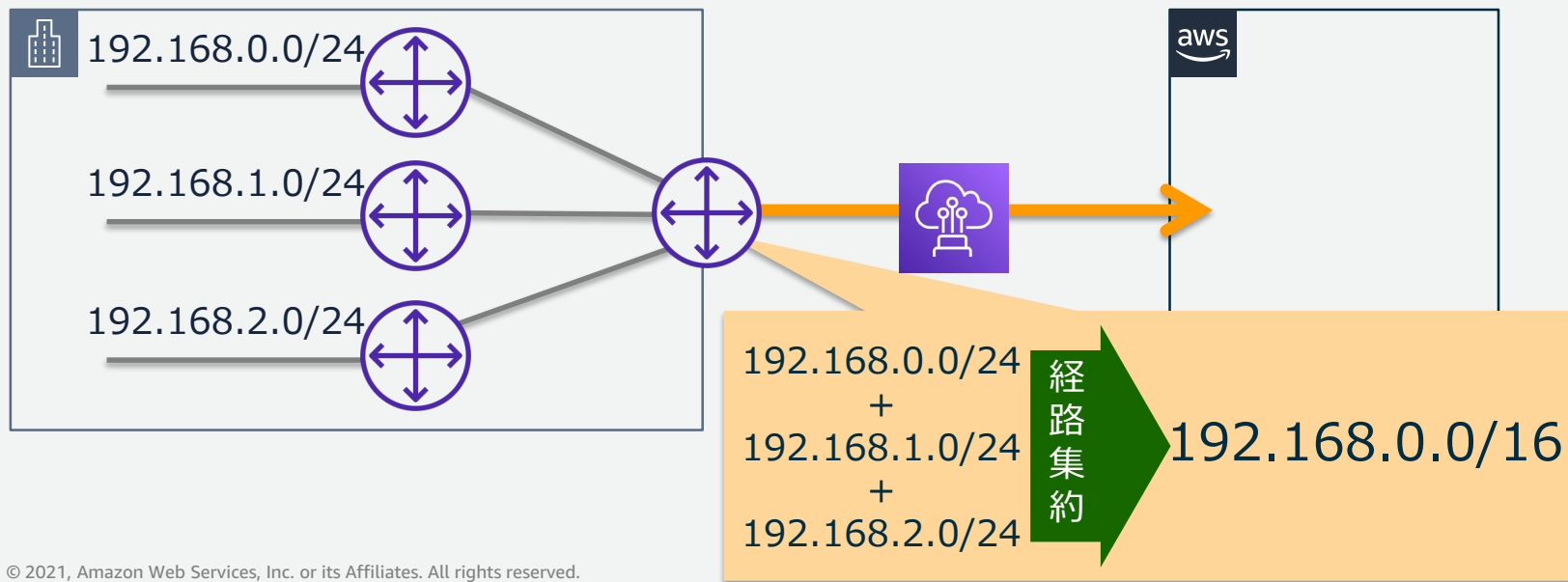
※1: キャパシティが 1 Gbps 未満のホスト接続で、トランジット仮想インターフェイスを作成することはできません。

https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/limits.html

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

経路集約の必要性

- お客様ルータから広告できるネットワーク数はBGPセッションあたり**100 (プライベート/トランジットVIF) または1,000 (パブリックVIF)** が上限
- 経路数の上限を超えるとBGPピアがシャットダウンされる (注意!)
- 普段から経路集約やフィルタリングを意識する設計を!
- デフォルトルートの広告が有効な場合もあり



Agenda

- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- クォータについて
- **What's New** (最近の主なアップデートをクイックにチェック)
- まとめ
- 参考：料金体系



What's new 主要アップデート抜粋 (2019年以降)

投稿日	タイトル	備考・関連ページ
Sep 25, 2019	AWS Direct Connect の AWS Transit Gateway サポートが新たに 6 つのリージョンで利用可能に	トランジットVIFが東京リージョンに対応
Oct 4, 2019	AWS Direct Connect では、詳細なコスト配分のサポートと、Direct Connect ゲートウェイの関連付けの支払人 ID 制限の解除を発表します	Direct Connectゲートウェイによる柔軟なマルチアカウント対応と、データ転送料を課金するAWSアカウントを明確化
Oct 7, 2019	AWS Direct Connect が Resiliency ツールキットを発表し、AWS への接続の回復性を強化した接続の注文を容易に	Direct Connect 接続のリクエスト時に便利な、ウィザード形式のインターフェイスを提供開始
Nov 25, 2019	AWS Direct Connect は、AWS 中国リージョンの Direct Connect ゲートウェイを有効にします	AWS中国リージョンでDXGWに対応
May 11, 2020	AWS Direct Connect の強化されたモニタリング機能	これまでのDirect Connect接続に加え、仮想インターフェイスがCloudWatchメトリクスに対応
Jun 3, 2020	AWS Direct Connect でフェイルオーバーのテストが可能に	お客様が指定した時間、BGPセッションをシャットダウンし、回復性をテスト可能

<https://aws.amazon.com/jp/about-aws/whats-new/2019/>
<https://aws.amazon.com/jp/about-aws/whats-new/2020/>

Agenda

- AWS Direct Connect とは？
- 物理接続/論理接続
 - 物理接続
 - 仮想インターフェイスの種類
 - AWS Transit Gateway
 - AWS Direct Connectゲートウェイ
 - パートナー経由のDirect Connect
- 高い回復性/モニタリング
- クォータについて
- What's New (最近の主なアップデートをクイックにチェック)
- **まとめ**
- 参考：料金体系



まとめ

AWS Direct Connectと関連するサービスの機能とメリットを理解する

＞ 接続、仮想インターフェイス、パートナー経由のサービス利用

複数の選択肢から用途に合わせて組み合わせる

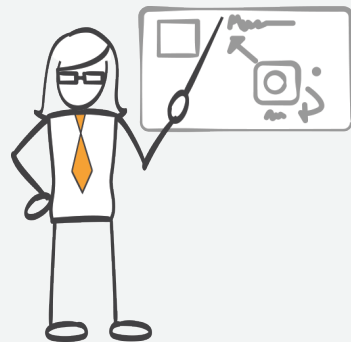
＞ DXGW、TGW、冗長化方法、VPCの数に合わせた構成

最近のアップデートにキャッチアップ

＞ フェイルオーバーテスト、CloudWatchメトリクスの活用

詳細情報・最新情報へのポイントを得る

＞ 各説明ページ下部の公開ドキュメントURL、後述の参考を参照



参考：料金体系

料金体系

AWS Direct Connectの月額利用料 =

ポート使用料

+

データ転送料

データ転送料は

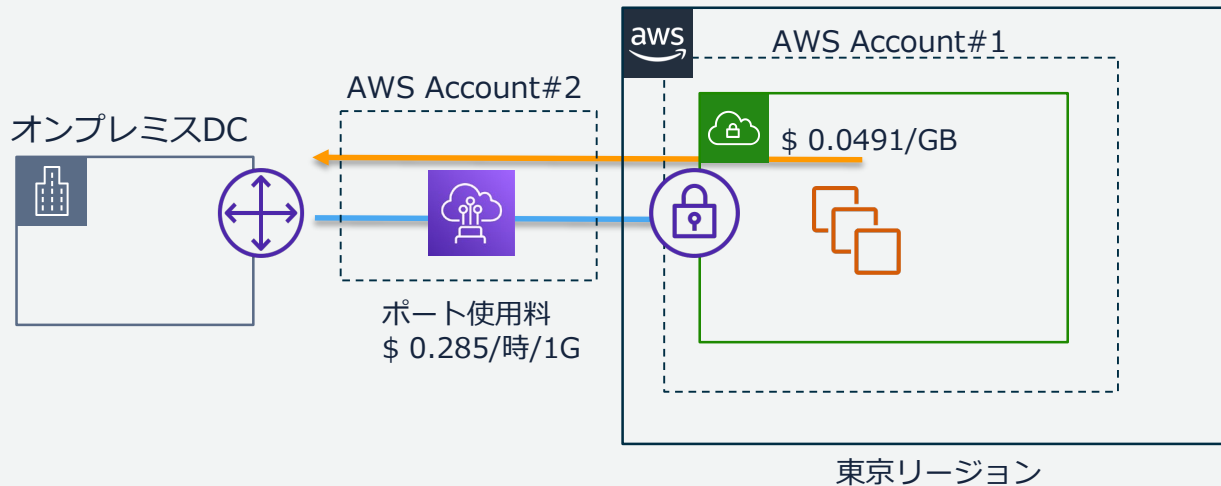
- AWSからのデータアウトに課金
- 仮想インターフェイス(=VIF)、通信対象リソースを持つオーナーアカウントに課金(更新)
- パブリック接続の場合、パブリック上のリソースを所有するオーナーアカウントに課金
- インターネット接続のデータ転送料の数分の一と**安価**

上記のほか、キャリアサービス利用の場合は別途費用必要

<https://aws.amazon.com/jp/directconnect/pricing/>

料金 シナリオ 1 (例 : ConnectionとVIFのAWSアカウントが異なる)

Direct ConnectのConnectionとVIFのオーナーアカウントが異なる場合、ポート使用料はConnectionのオーナーに、VIFのデータ転送料はVPC内のリソースのオーナーアカウントに課金される



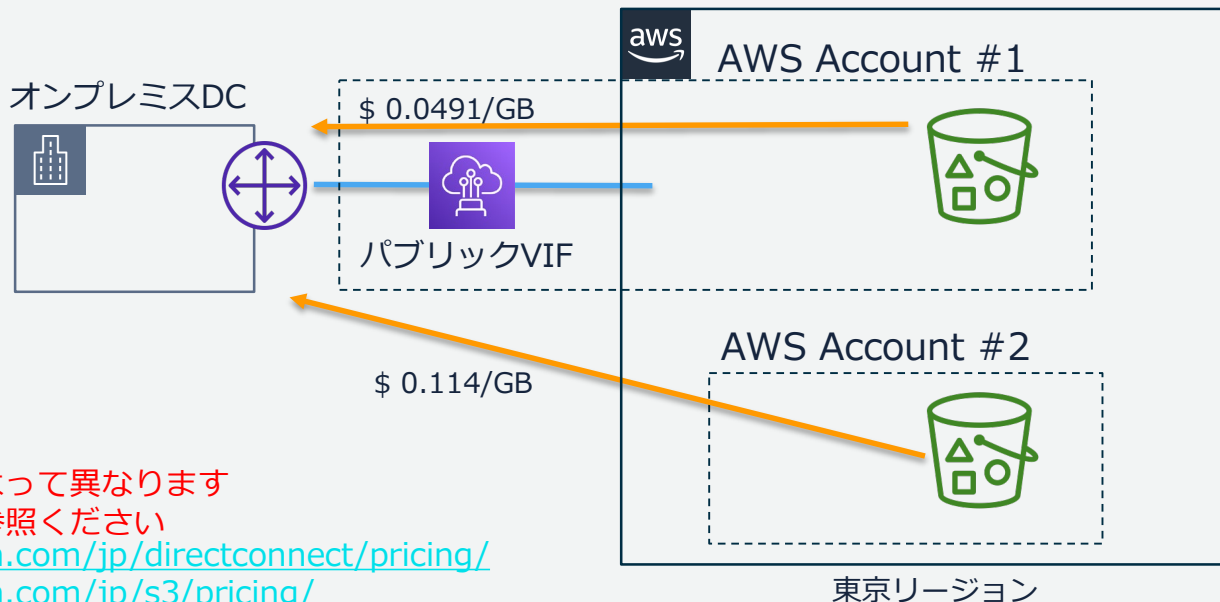
※ 料金は各種条件によって異なります。詳しくは以下をご参照ください。

<https://aws.amazon.com/jp/directconnect/pricing/>

<https://aws.amazon.com/jp/s3/pricing/>

料金 シナリオ 2 (例: パブリックVIFとS3のAWSアカウントが異なる)

- データ転送料金はパブリック上のリソースを所有するオーナーアカウントに課金される
- VIFとパブリック上のリソースのオーナーが同アカウント、もしくは一括請求の対象の場合はDirect Connectの転送料金が適用される
- そうでない場合はインターネットへのデータ転送料金が適用される

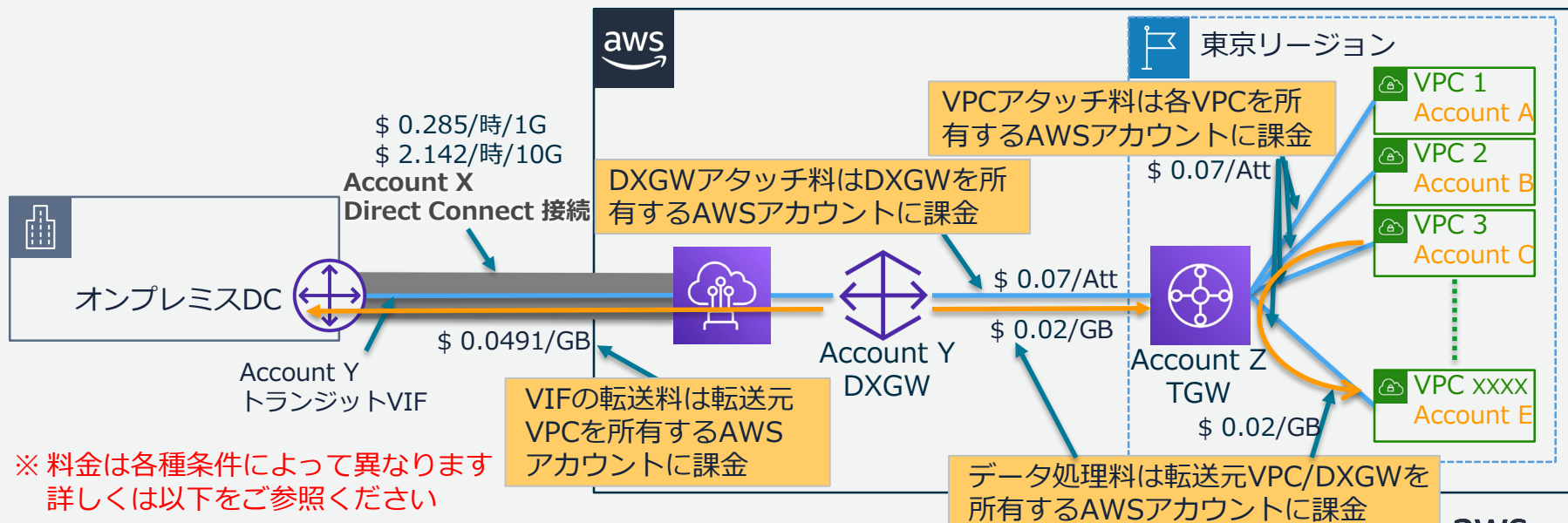


※ 料金は各種条件によって異なります
詳しくは以下をご参照ください

<https://aws.amazon.com/jp/directconnect/pricing/>
<https://aws.amazon.com/jp/s3/pricing/>

料金 シナリオ3 (例: トランジットVIF+TGWにおけるマルチアカウント)

- 接続のポート使用料は接続/ホスト接続を所有しているAWSアカウントに課金
- VIFの転送料はTGWにアタッチされたVPCを所有するAWSアカウントに対して課金
- TGWのデータ処理料金はトラフィックをTGWに送信するVPC/DXGWを所有するAWSアカウントに課金
- TGWのアタッチ料は各アタッチ先のリソースを所有するAWSアカウントに課金



※ 料金は各種条件によって異なります
詳しくは以下をご参照ください

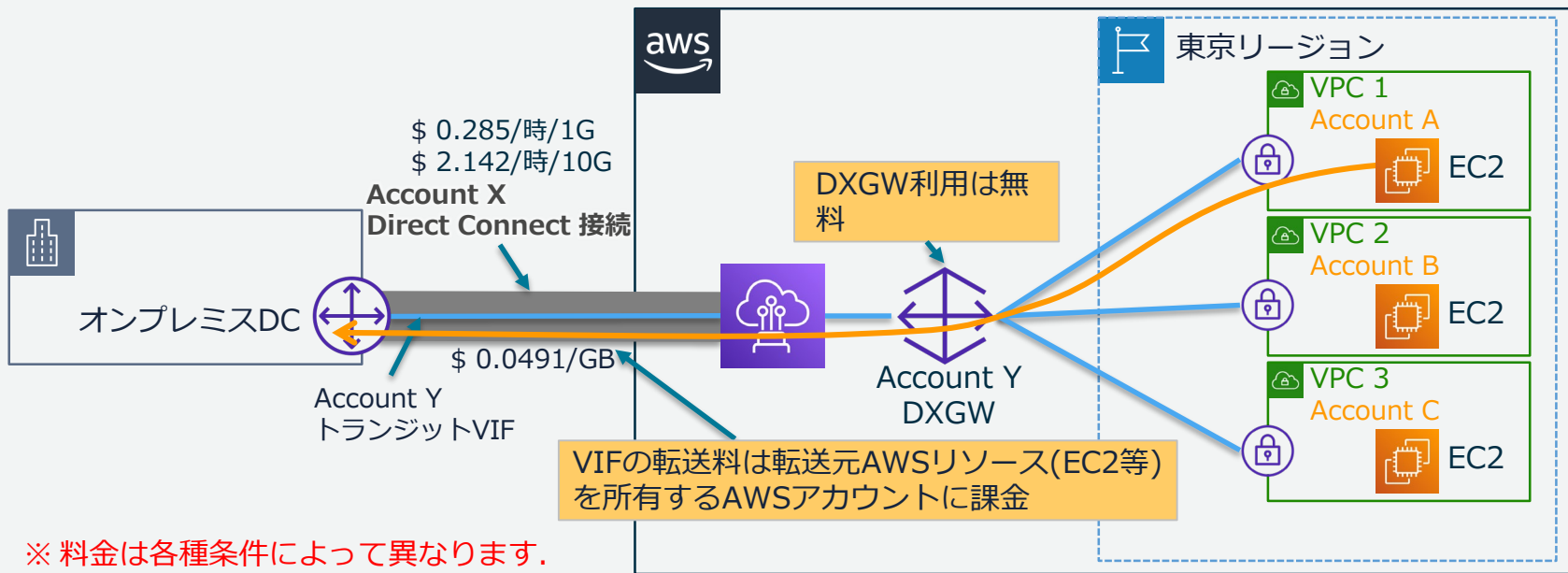
<https://aws.amazon.com/jp/directconnect/pricing/>
<https://aws.amazon.com/jp/transit-gateway/pricing/>

備考: オンプレミスとDirect Connect ロケーション間の回線にかかる費用は別途発生します。



料金 シナリオ 4 (例: プライベートVIF + DXGWにおけるマルチアカウント)

- 接続のポート使用料は接続/ホスト接続を所有しているAWSアカウントに課金
- VIFの転送料はデータ送信を行うAWSリソースを所有しているAWSアカウントに課金
- DXGWの利用に費用は発生しない



※ 料金は各種条件によって異なります。
詳しくは以下をご参照ください。

<https://aws.amazon.com/jp/directconnect/pricing/>

備考: オンプレミスとDirect Connect ロケーション間の回線にかかる費用は別途発生します。

参考 : AWSネットワーク関連サービスの資料

[AWS Black Belt Online Seminar] Amazon VPC

<https://www.slideshare.net/AmazonWebServicesJapan/20201021-aws-black-belt-online-seminar-amazon-vpc>

[AWS Black Belt Online Seminar] AWS Transit Gateway

<https://www.slideshare.net/AmazonWebServicesJapan/20191113-aws-black-belt-online-seminar-aws-transit-gateway>

[AWS Black Belt Online Seminar] オンプレミスとAWS間の冗長化接続

<https://www.slideshare.net/AmazonWebServicesJapan/20200219-aws-black-belt-online-seminar-aws>

[AWS Black Belt Online Seminar] 発注者のためのネットワーク入門

<https://www.slideshare.net/AmazonWebServicesJapan/20180515-aws-black-belt-online-seminar>

[Digital Course] Transit Gateway Networking and Scaling (英語版Eラーニング)

<https://www.aws.training/Details/eLearning?id=40275>

[Amazon Web Servicesブログ] “共有型”AWS DirectConnectでも使えるAWS Transit Gateway

<https://aws.amazon.com/jp/blogs/news/aws-transit-gateway-with-shared-directconnect/>

Q&A

お答えできなかったご質問については

AWS Japan Blog 「<https://aws.amazon.com/jp/blogs/news/>」にて

後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索



The screenshot shows the AWS Japanese website header with the logo, navigation links for '日本語', 'アカウント', and 'サポート', and a 'サインイン' button. The main content area features the title 'AWS クラウドサービス活用資料集トップ' and a paragraph of introductory text. Below the text are four buttons: 'AWS Webinar お申込', 'AWS 初心者向け', '業種・ソリューション別資料', and 'サービス別資料'.

aws

日本語 日本担当チームへお問い合わせ サポート アカウント

コンソールにサインイン

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

AWS Webinar お申込 »

AWS 初心者向け »

業種・ソリューション別資料 »

サービス別資料 »

<https://amzn.to/JPArchive>

AWS Well-Architected 個別技術相談会

毎週“W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に
対策などを相談することも可能

- 申込みはイベント告知サイトから

(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント で[検索]



AWS Well-Architected



ご視聴ありがとうございました

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>

