[AWS Black Belt Online Seminar]

AWS Site-to-Site VPN

サービスカットシリーズ

Solutions Architect 菊地 信明
2021/10

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け、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。

- AWSの技術担当者が、AWSの各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

- 本資料では2021年10月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います。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　ネットワークソリューション部
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
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, AWS Site-to-Site VPN

本セミナーの対象者

- AWS Site-to-Site VPNをこれからご利用予定の方
- オンプレミスやAmazon VPCのネットワーク設定を行う知識をお持ちの方
- VPN接続をすでにご利用の方で、より理解を深めたい技術者の方

本日の目標

- AWS Site-to-Site VPN接続の種類、利用例を理解する
- 設定時に注意するべきポイントを把握する
- 運用時における確認項目、AWS側メンテナンスに対して備えておくべきことを認識する
- 詳細情報・最新情報へのポインタを得る

本セミナーでお話しないこと

- Amazon VPC、AWS Site-to-Site VPNに対するマネージメントコンソール上でのステップバイステップな設定方法
- Amazon VPC、AWS Site-to-Site VPNに関する用語・機能の詳細
- 各構成への移行方法
- オンプレミスとインターネット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

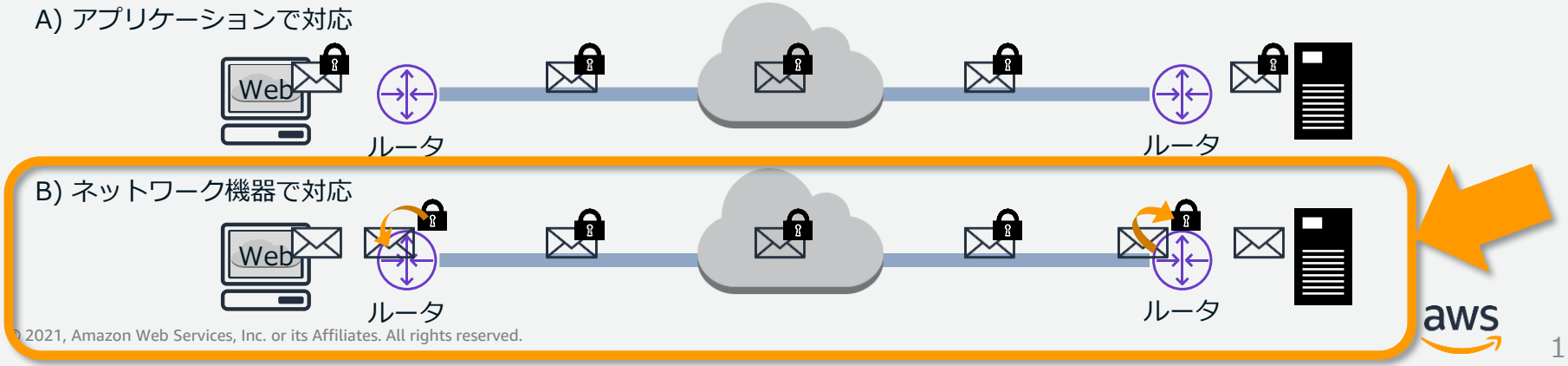
Agenda

- ✓ **オンプレミスからAWSへプライベート接続する方法**
  - ➢ AWSにおけるVPN接続の種類
  - ➢ AWS Site-to-Site VPNとは？
  - ➢ AWS Site-to-Site VPNの設定
  - ➢ 2つのターゲットゲートウェイ - VGW or TGW
- ✓ VPNの冗長化
  - ➢ 仮想プライベートゲートウェイ(VGW)
  - ➢ トランジットゲートウェイ(TGW)
  - ➢ Direct Connectとの併用
- ✓ AWS Site-to-Site VPNを利用した拠点間通信
- ✓ 運用時の確認ポイント
- ✓ よくあるお問合せ
- ✓ まとめ
- ✓ 参考
  - ➢ AWS Site-to-Site VPNにおける直近のアップデート
  - ➢ AWS Site-to-Site VPNの利用料金

オンプレミスからAWSへ
プライベート接続する方法

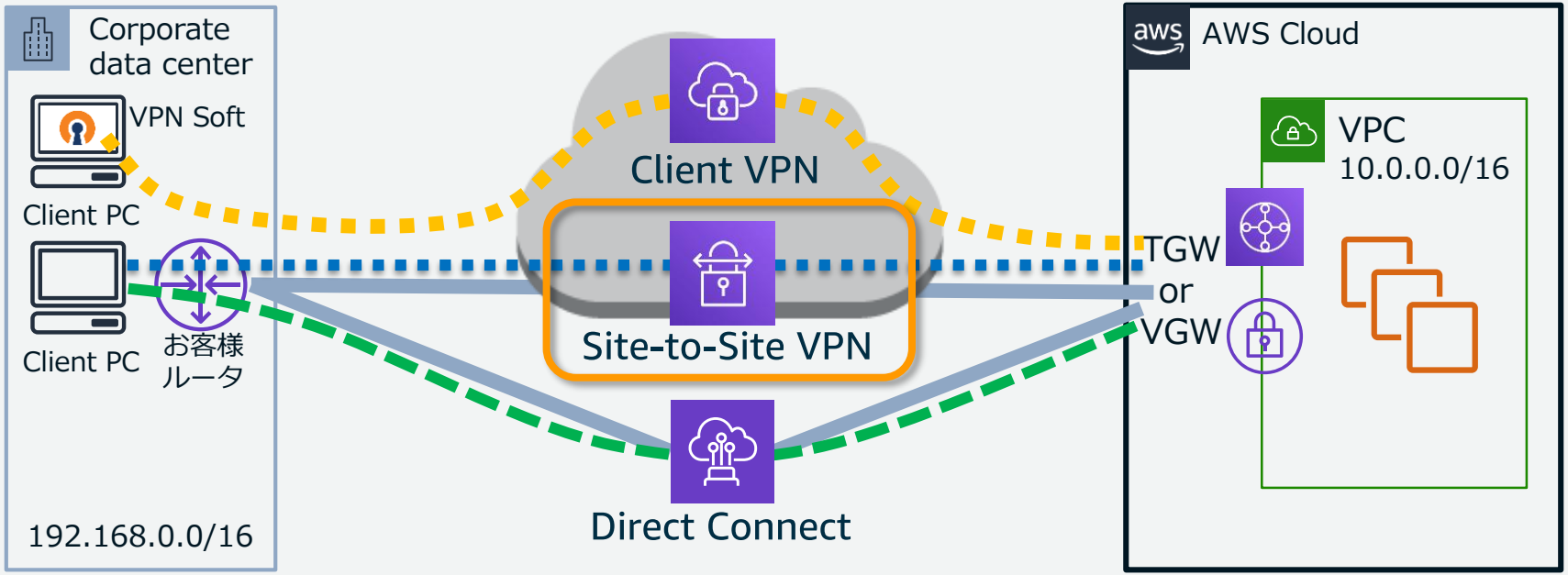
なぜVPNを利用するのか？

クラウドはオンプレミスからインターネット越しに利用する前提で提供されています。インターネットを経由した通信が必要となると、経路上に第三者が管理するデバイスが存在するため、通信の内容を盗み見られてしまう可能性があります。すでに公開されているWebサイトの内容であれば、問題も少ないかもしれません。しかし、顧客情報やクレジット番号などの秘匿情報を含む場合、第三者に見られては困ります。
このような守るべき情報がある場合、内容を暗号化し、プライベート接続する必要があります。



プライベート接続

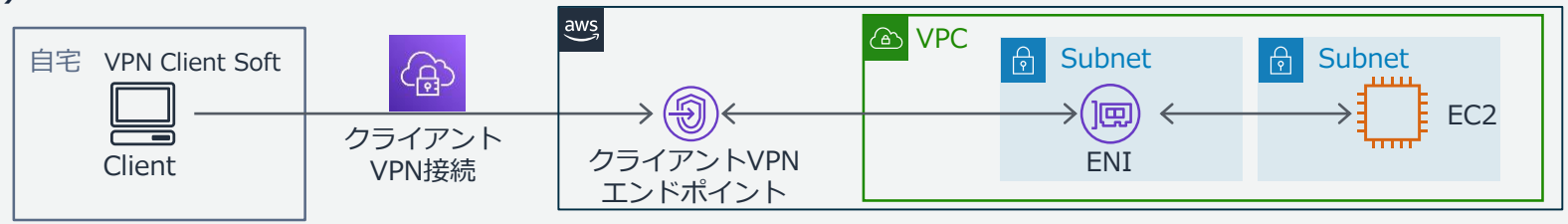
パブリックIPアドレスを使わず、プライベートIPアドレスのみでAWS VPCのリソースへアクセスする場合、以下の3つのパターンがあります。



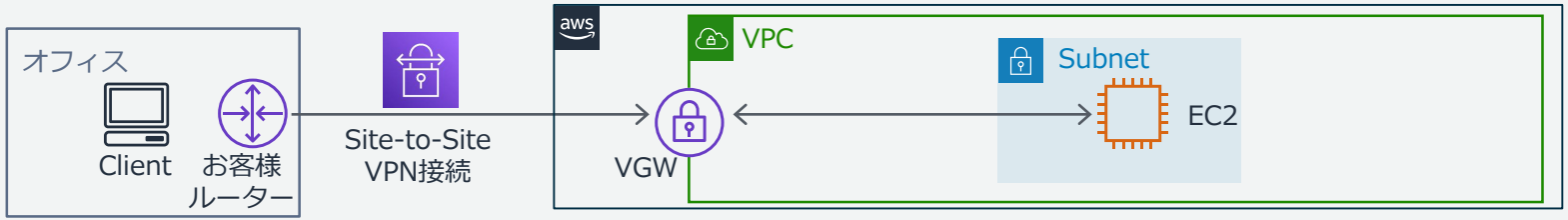
AWSにおけるVPN接続の種類

VPN接続３パターン

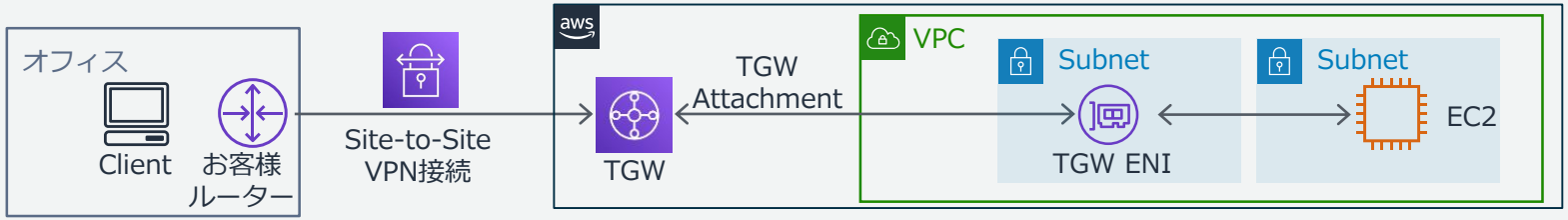
1) AWS Client VPN



2) AWS Site-to-Site VPN 仮想プライベートゲートウェイ(VGW)接続

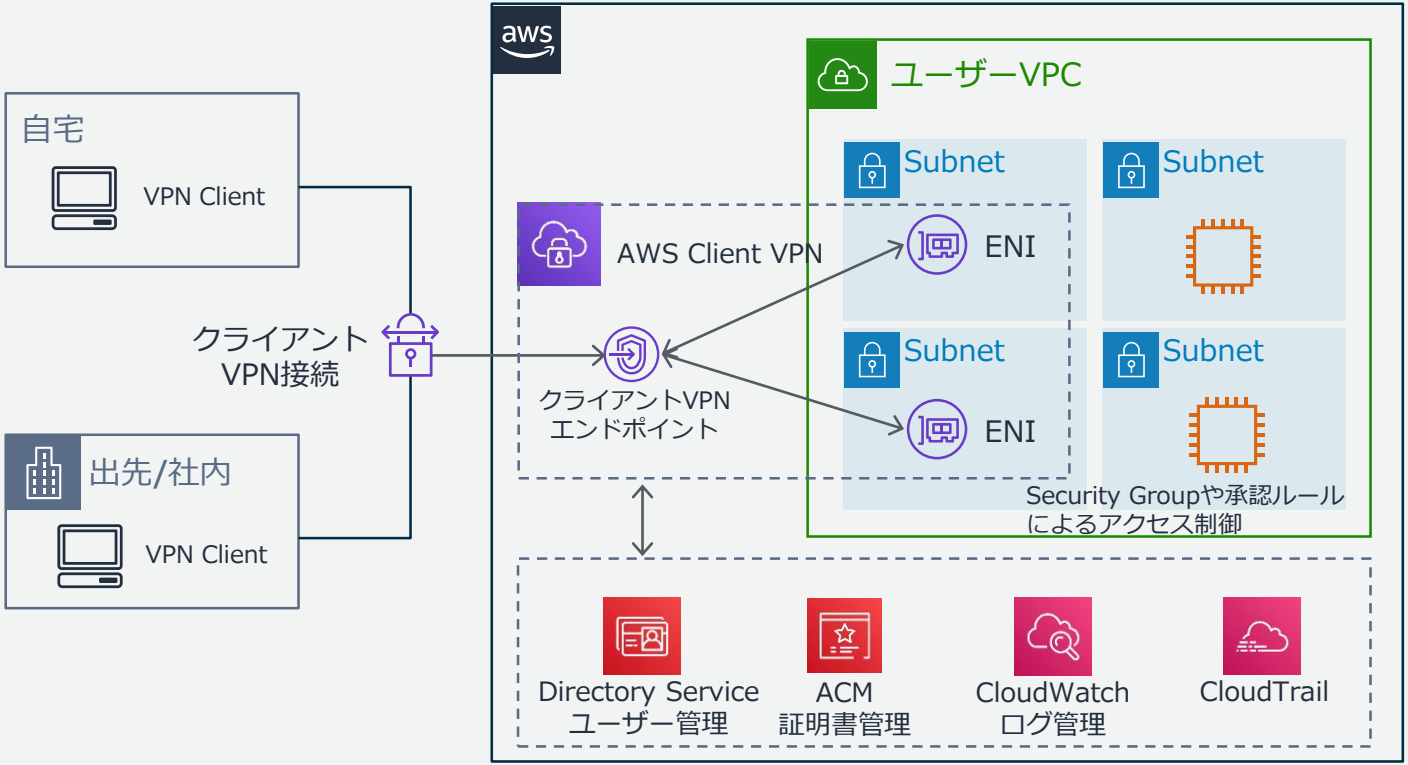


3) AWS Site-to-Site VPN トランジットゲートウェイ(TGW)接続



1) AWS Client VPN

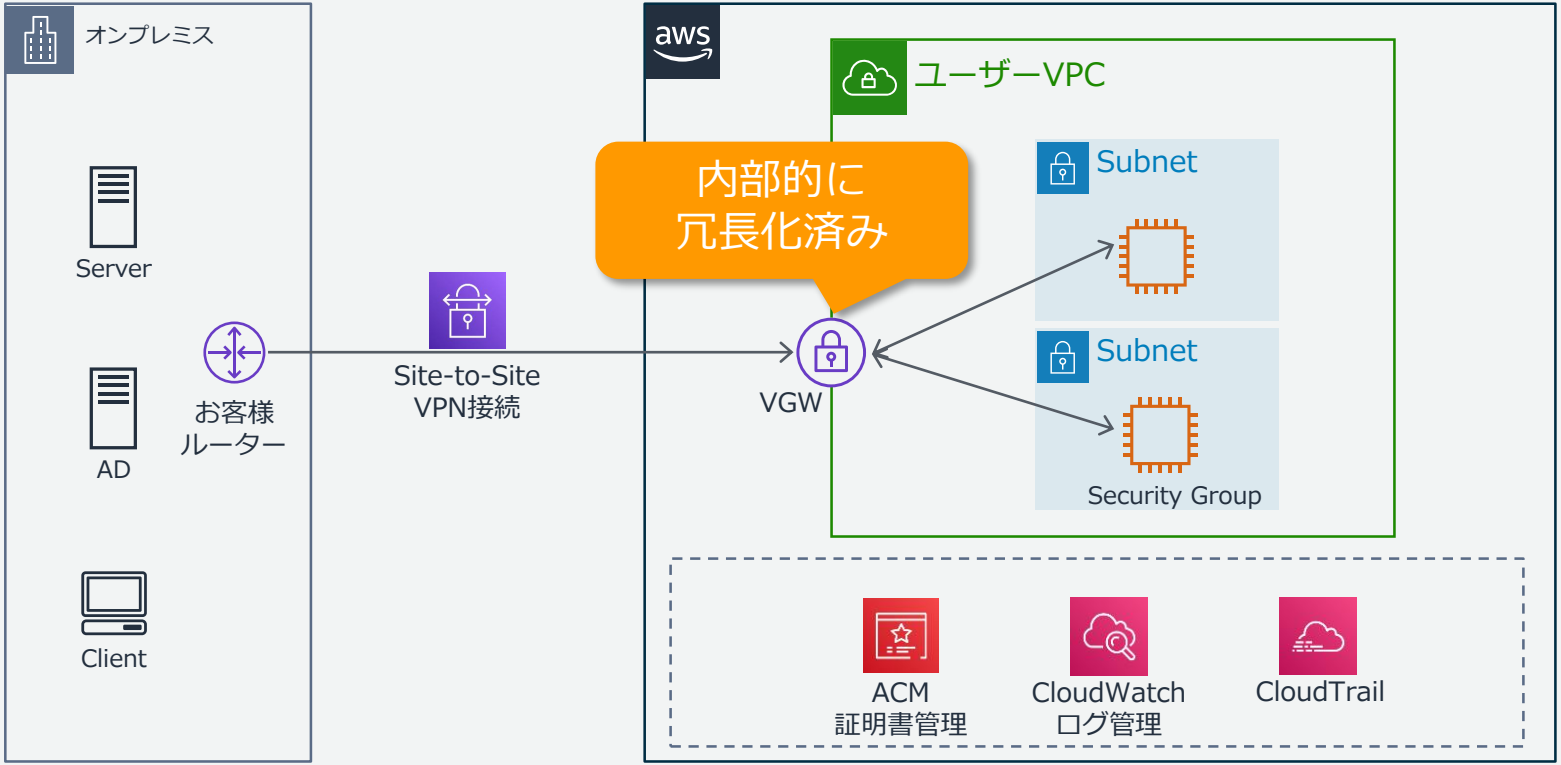
本セッションではご紹介のみ



https://docs.aws.amazon.com/ja_jp/vpn/latest/clientvpn-admin/

2) AWS Site-to-Site VPN VGW接続

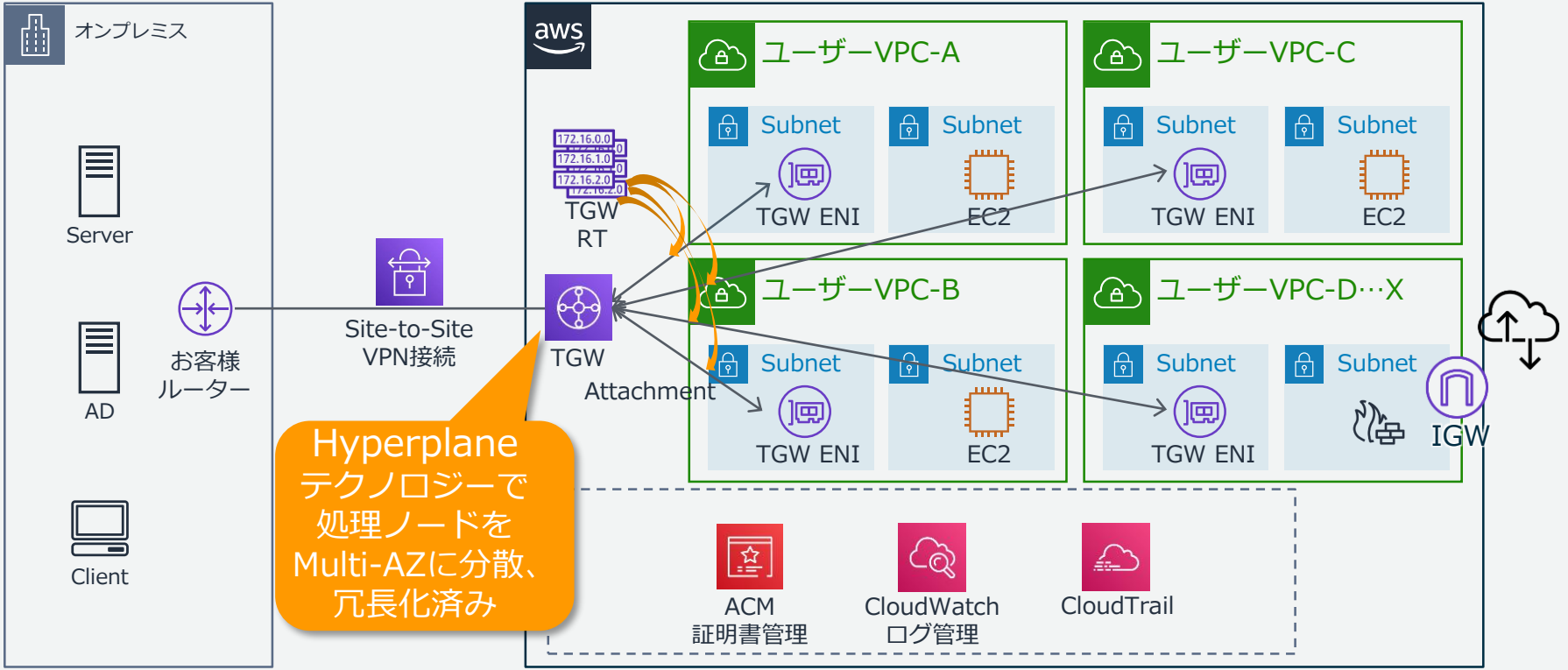
オンプレミスから特定のVPCへ接続する際に有用



https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/

3) AWS Site-to-Site VPN TGW接続

オンプレミスから複数のVPCへ接続する際や、柔軟なルーティング要件に対応

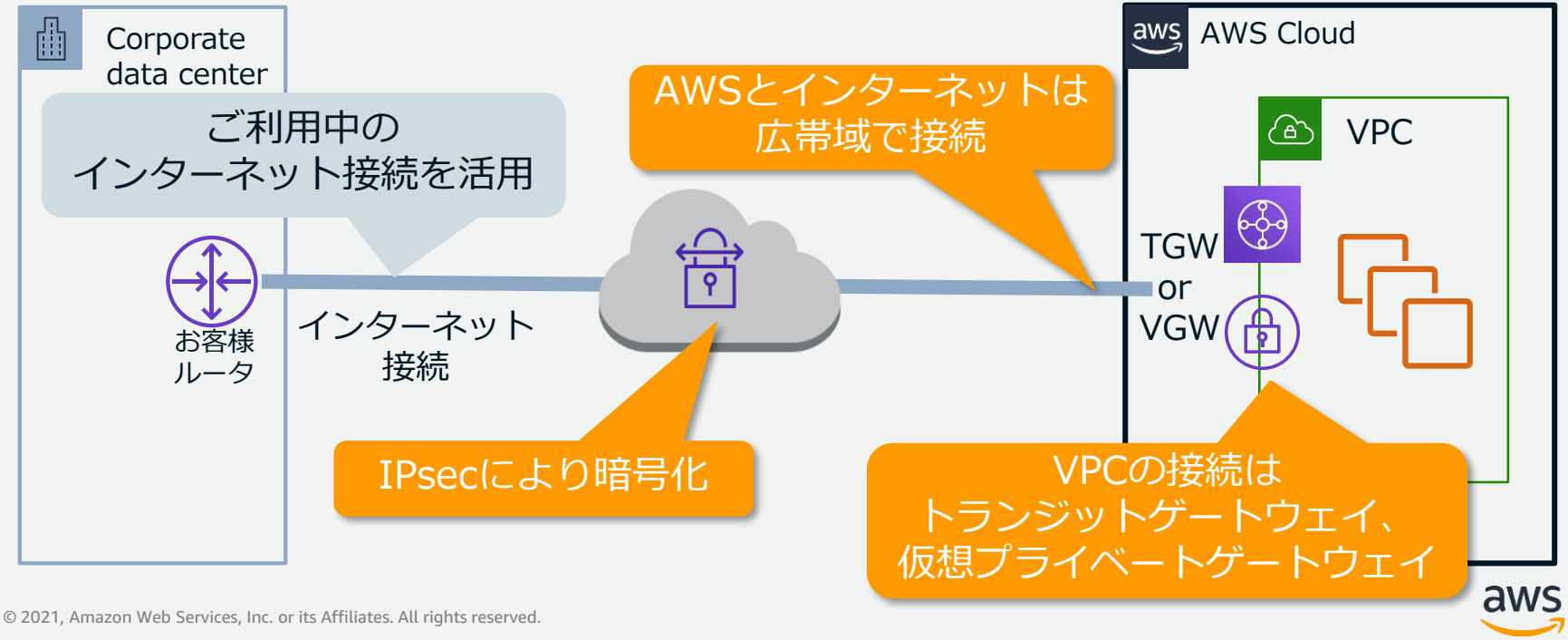


https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/

AWS Site-to-Site VPNとは？

AWS Site-to-Site VPNとは？

AWS Site-to-Site VPNを利用することで、VPCに関連付けられたトランジットゲートウェイ、または、仮想プライベートゲートウェイ（VGW）を経由し、リモートネットワークへの安全なアクセス環境を利用できます。
インターネットプロトコルセキュリティ（IPsec）VPN接続がサポートされています。



AWS Site-to-Site VPN

ユースケース

- 拠点とAWSを簡単に早く接続したい
- 価格重視/スモールスタート
- Direct Connectのバックアップ回線

ポイント

- 用途によって、接続先を使い分け
  - VGW：特定のVPCのみと通信
  - TGW：多くのVPCと通信（VPN料金の他にTGWの料金も発生する）
- IPsec対応ルーターと固定Public IPがあれば、容易に環境構築可能（事前共有キーによる認証方式）
- プライベート証明書による認証の場合、非固定Public IPに対応
- 不要になったらすぐに停止できる（時間課金＋転送量に課金）

https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/vpn-tunnel-authentication-options.html

AWS Site-to-Site VPNの設定

AWS Site-to-Site VPNの設定：主な準備

カスタマーゲートウェイデバイス

- VPN接続のお客様側にある物理デバイスまたはソフトウェアデバイス

カスタマーゲートウェイ(CGW)

- インターネットルーティングが可能な固定の IP アドレスにリソース名を定義し、AWS へ登録（証明書による認証を選択した場合、固定IPアドレスは不要）

ルーティングのタイプ

- 静的または動的が選択可能　デバイスが対応している場合は、動的(BGP)を推奨
- BGPの設計時に拠点ごとにユニークなASN

ターゲットゲートウェイ

- 仮想プライベートゲートウェイ(VGW)、もしくは、トランジットゲートウェイ(TGW)をあらかじめ作成、予め通信対象のVPCと関連付け
- ASNはCGWとは異なる値

カスタマーゲートウェイデバイス（CGW）

カスタマーゲートウェイデバイスの設定

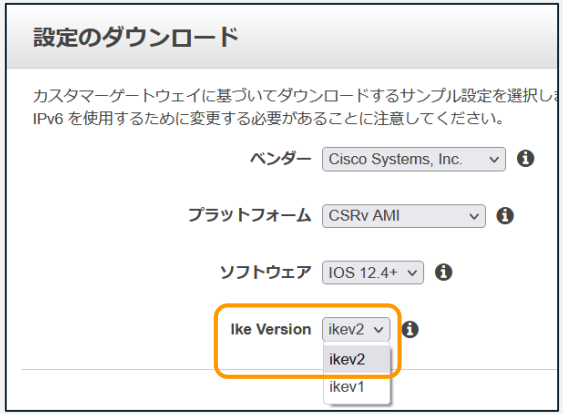
- VPNを利用するためには、オンプレミス環境のデバイスを正しく設定
- 主要ベンダーのサンプルコンフィグは、VPN接続設定後にマネジメントコンソールからダウンロード可能
- デバイスの最新OSに適合した設定は、各ベンダーの公開情報も確認

https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/your-cgw.html

アップデート：設定ダウンロード機能がIKEv2に対応

ご利用デバイスがIKEv2に対応している場合

- 対応するプラットフォームに対して、サンプルコンフィグに予めIKEv2の設定が記載されている状態で入手可能。
- IKEv2ではプロトコルの複雑性が緩和され、セキュリティアソシエーション(SA)ネゴシエーションも簡素化されているため、IKEv2へ移行を推奨。



https://aws.amazon.com/jp/about-aws/whats-new/2019/02/aws-site-to-site-vpn-now-supports-ikev2/

カスタマーゲートウェイデバイス：サンプルコンフィグ利用時の注意

- サンプルコンフィグはVPN接続に関する必要最小限の設定のみが記載。
- お客様のネットワーク環境に合わせて必ず修正すること。
- 可能なら検証環境でのテストを行い、期待通りの動作をするか確認する。
- 特に2つのトンネル間でのトラフィックシフトについては、入念にチェックし、実際に利用するアプリケーションへの影響を確認すること。

カスタマーゲートウェイ(CGW)：動的ルーティング

AWSで接続を確認済みの製品

- Barracuda NextGen Firewall F シリーズ 6.2以降
- Cisco ASA (Cisco ASA 9.7.1以降)
- Cisco IOS (Cisco IOS 12.4以降)
- F5 Networks BIG-IP (v12.0.0以降)
- Fortinet FortiGate 40以降
- H3C MSR800 (バージョン 5.20)
- IIJ SEIL/B1 (SEIL/B1 3.70以降)
- Juniper J-Series (JunOS 9.5以降)
- Juniper SRX (JunOS 11.0以降)
- Juniper SSG または Netscreen series (Juniper ScreenOS 6.1以降)
- Mikrotik RouterOS (6.36以降)
- Palo Alto Networks (PANOS 4.1.2以降)
- SonicWALL (SonicOS 5.9または6.2以降)
- Sophos ASG (V8.300以降)
- Vyatta (Network OS 6.5以降)
- WatchGuard XTM、Firebox (Fireware OS 11.12.2以降)
- Yamaha RT107e、RTX1200、RTX1210、RTX1500、RTX3000、またはSRT100
- Zyxel ZyWALL (ZLD 4.3以降)

その他、CGW要件を満たすデバイスで接続可能
以下のURL参照

カスタマーゲートウェイデバイスの要件
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/your-cgw.html#CGRequirements
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/cgw-dynamic-routing-examples.html

カスタマーゲートウェイ(CGW)：静的ルーティング

AWSで接続を確認済みの製品

- Cisco ASA (Cisco ASA 8.2以降)
- Cisco ASA (Cisco ASA 9.7.1以降)
- Cisco IOS (Cisco IOS)
- Cisco Meraki MX シリーズ (9.0以降)
- Citrix Netscaler CloudBridge (NS 11以降)
- Cyberoam CR15iNG (V10.6.5MR-1移行)
- F5 Networks BIG-IP (v12.0.0以降)
- Fortinet Fortigate 40+ シリーズ (FortiOS 4.0以降)
- H3C MSR800 (バージョン 5.20以降)
- IIJ SEIL/B1 (SEIL/B1 3.70以降)
- Mikrotik RouterOS (6.36以降)
- Openswan (2.6.38以降)
- pfSense (OS 2.2.5以降)
- SonicWALLrunning SonicOS 5.9または6.2以降
- Strongswan Ubuntu 16.04 (Strongswan 5.5.1以降)
- WatchGuard XTM、Firebox (Fireware OS 11.11.4以降)
- Zyxel Zywall (Zywall 4.20以降)

その他、CGW要件を満たすデバイスで接続可能
以下のURL参照

カスタマーゲートウェイデバイスの要件
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/your-cgw.html#CGRequirements
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/cgw-static-routing-examples.html

ルーティングのタイプ：動的 or 静的

特別な要件が無い場合、動的を推奨
カスタマーゲートウェイデバイスが非対応な場合のみ、静的を利用
合わせて、サブネットが参照するルートテーブルでルート伝播を有効化

動的（BGP）選択時のメリット

- 2つのトンネル（後述）間で冗長性が高まる
  片方のIPsecトンネルが利用できない場合、スムーズに切り替わる
- オンプレミスとVPCのCIDR増減時に、自動的に対応
  オンプレミス拠点やVPCでネットワーク追加時、お客様ルーターから経路を広報すると、VPCから疎通可能、VPCのCIDR追加時にも対応か容易
- 複数拠点間の通信をAWSで折り返すCloudHub構成でも柔軟な運用が可能
  他拠点向け経路を自動的に受信でき、変更作業が単一箇所で済む

認証のタイプ：事前共有キー or プライベート証明書

固定パブリックIPアドレスを用意できる場合は事前共有キー(Pre-shared keys)方式を推奨
非固定のパブリックIPアドレスしか用意できない場合のみ、プライベート証明書による認証を検討（コスト面に注意）

認証タイプの検討ポイント

- カスタマーゲートウェイ側で対応の確認
  事前共有キーは多くのベンダーで対応しているが、プライベート証明書については、予め確認が必要
- プライベート証明書利用時には、別途、ACMの費用が追加される
  コストについては以下の公式ドキュメントで確認
  - AWS Certificate Manager の料金
  https://aws.amazon.com/jp/certificate-manager/pricing/
- 拠点の移転などで固定パブリックIPが変更になる場合
  CGWの変更機能が追加されているため、VPN接続の作り直しは不要（パブリックIP変更に伴う、お客様ルーターの設定変更は必要）

設定時の注意：最大送信単位 (MTU)

AWS Site-to-Site VPNでは、パスMTU検出(Path MTU Discovery)に対応していません。このため、予めEnd-to-Endでパケットサイズが1399以下となるよう、ホスト、ネットワーク機器のMTU設定を行う事を推奨。

例：Amazon Linux 2でのMTU設定

```
$ sudo ip link set dev eth0 mtu 1399
```

例：Windows系OSでのMTU設定

```
> Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -RegistryValue 1399
```

Site-to-Site VPN のクォータ
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/vpn-limits.html

EC2 インスタンスのネットワークの最大送信単位 (MTU)
https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/network_mtu.html
https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/WindowsGuide/network_mtu.html#set_mtu_windows

2つのターゲットゲートウェイ
VGW or TGW

ターゲットゲートウェイ: VGW or TGW

主に通信対象VPCの数で判断するが、利用機能の有無などで総合的に検討

仮想プライベートゲートウェイ(VGW)接続時のメリット

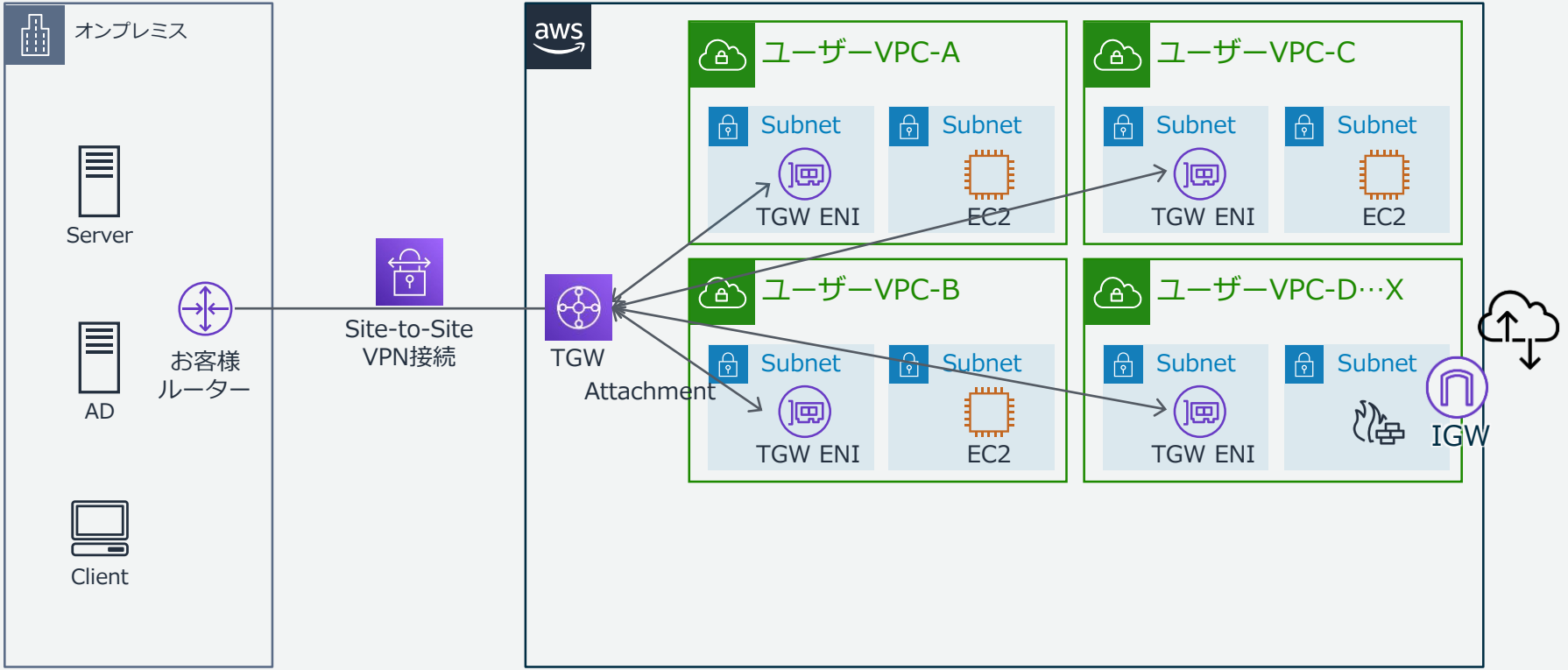
- シンプルな構成
  - 関連リソースが少なく、設定が容易
  - VPC追加毎にVPN接続を追加

トランジットゲートウェイ(TGW)接続時のメリット

- 複数のVPCに同時アクセス
  - 1つのVPN接続で複数のVPCへ接続が可能、VPC追加時にはTGWにアタッチするだけでオンプレミスとの通信が可能
  - 複数のルーティングテーブルを使い分け、柔軟なルーティング設計が可能
- Act-Actやアクセラレーション機能を利用可能

TGW接続のメリット(1): 複数VPCと同時接続

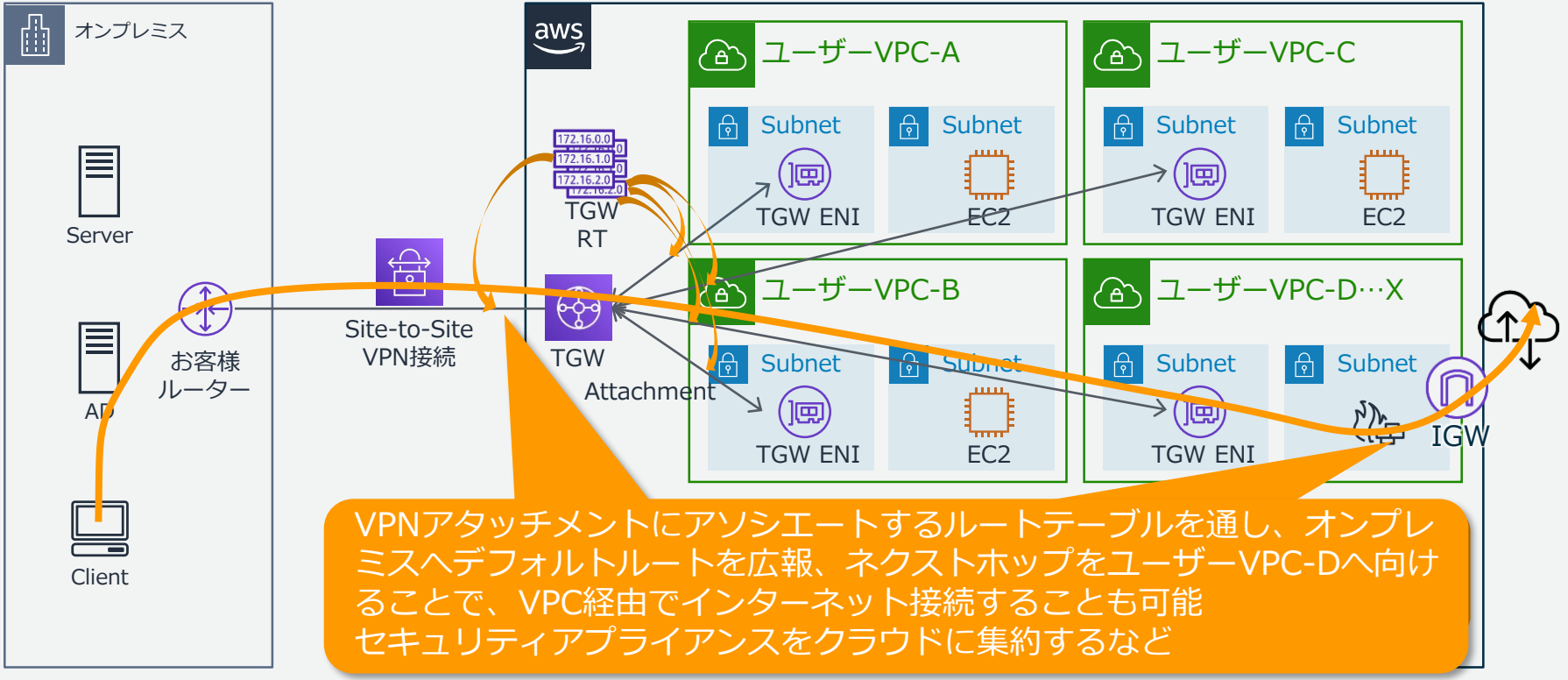
オンプレミスから複数のVPCへ接続する場合でも、1つのVPN接続で通信可能



https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/

TGW接続のメリット(2): 柔軟なルート設計

各アタッチメントにルーティングテーブルを割り当て、柔軟なルート設計が可能

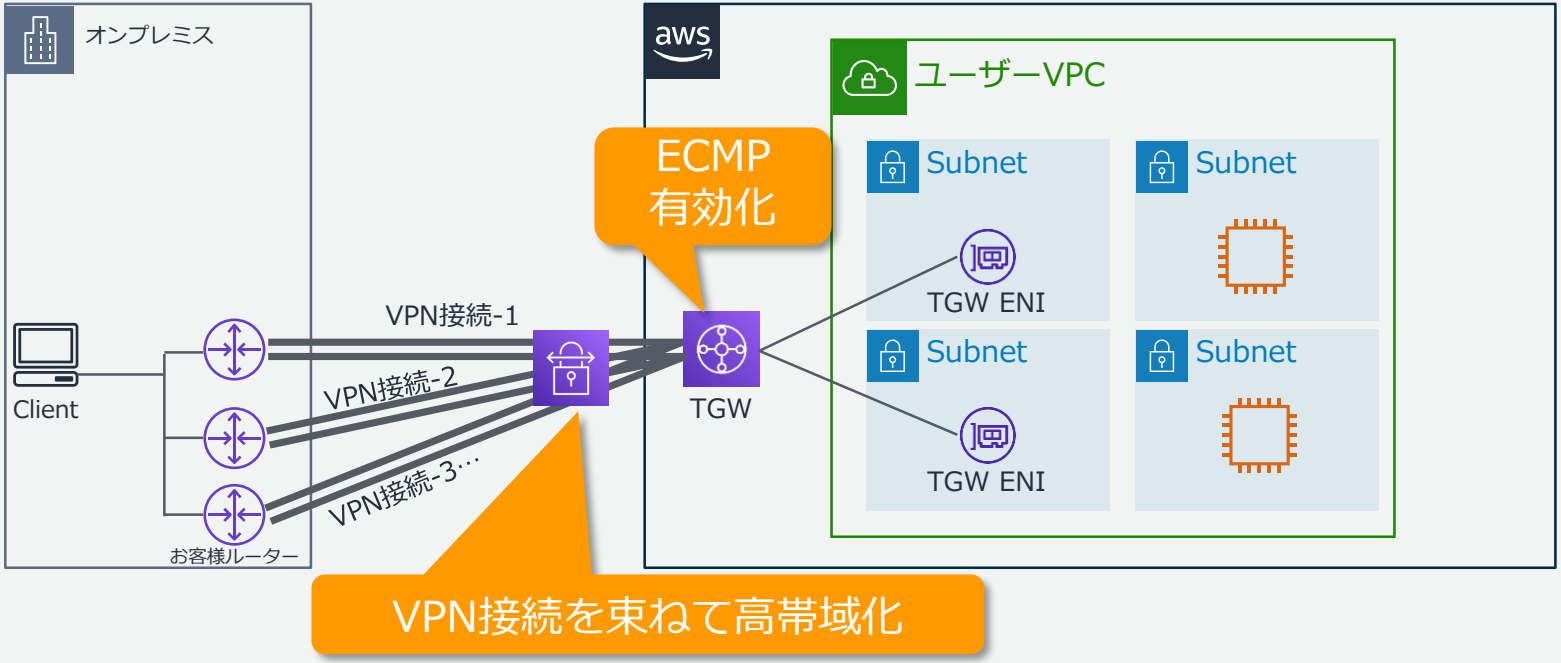


VPNアタッチメントにアソシエートするルートテーブルを通し、オンプレミスへデフォルトルートを広報、ネクストホップをユーザーVPC-Dへ向けることで、VPC経由でインターネット接続することも可能
セキュリティアプライアンスをクラウドに集約するなど

https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/

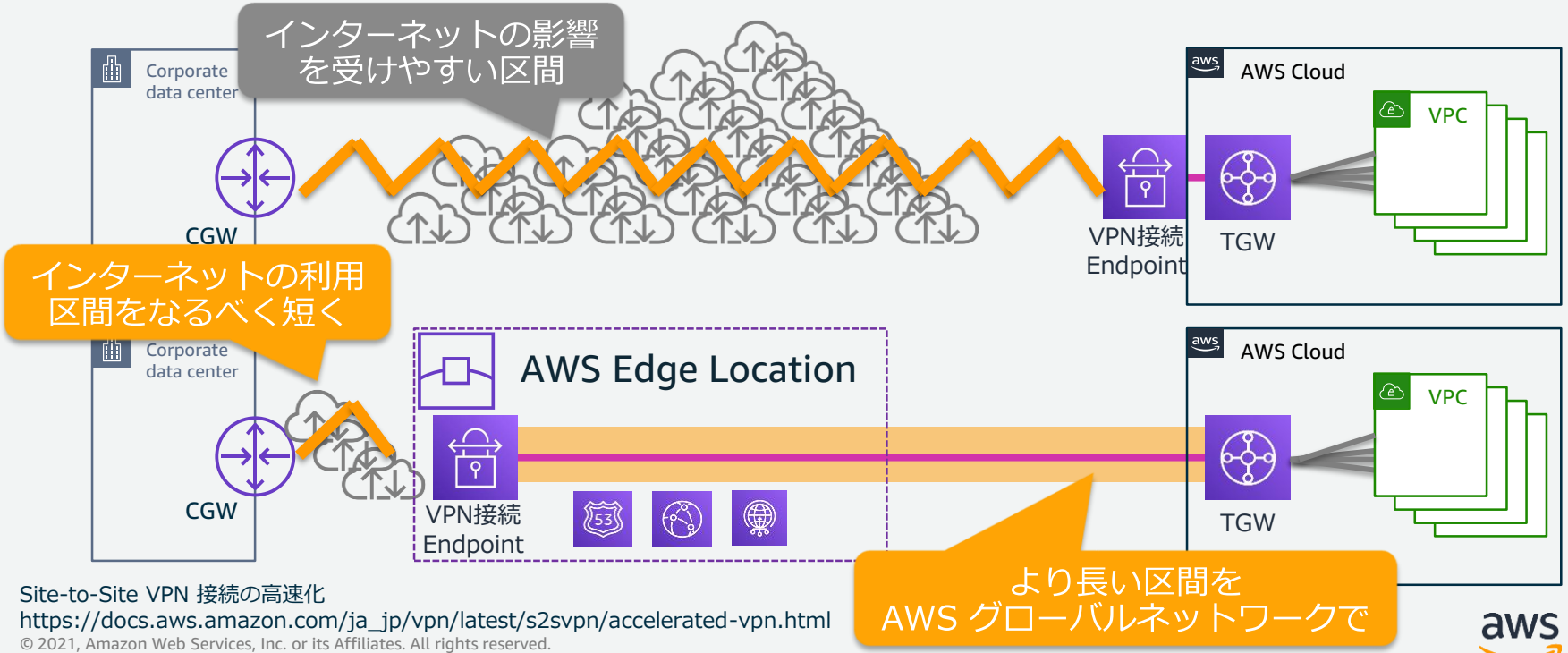
TGW接続のメリット(3): 複数のVPNによるAct-Act通信

複数のVPN接続を束ね、Equal Cost Multi Path(ECMP)を利用し帯域を増す
1つのIPsecトンネル当たり、最大1.25Gbps
VPN接続を増やすことで、最大50Gbpsまでのバーストを検証済み



TGW接続のメリット(4): Acceleratedサイト間VPNオプション

Accelerated VPNオプションを有効化し、AWSバックボーンを利用することで、
海外拠点からのVPN接続時などにインターネットの不安定要素を軽減
事前にテストサイトで効果測定が可能：https://speedtest.globalaccelerator.aws/



Site-to-Site VPN 接続の高速化
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/accelerated-vpn.html

より深い理解：テスト用VPN接続を構築

以下のハンズオン資料では、実際にvyosを利用してご自身のAWSアカウント環境に、AWS VPNの構築を体験できます。

AWS Hands-on for Beginners
Network編#2 Amazon VPC間およびAmazon VPCとオンプレミスのプライベートネットワーク接続

https://pages.awscloud.com/JAPAN-event-OE-Hands-on-for-Beginners-Network2-202009-reg-event-LP.html

フォームより申し込みいただくことで、
いつでも体験できます。
AWSリソース利用に関する費用は、
ご負担いただきますのでご了承ください。

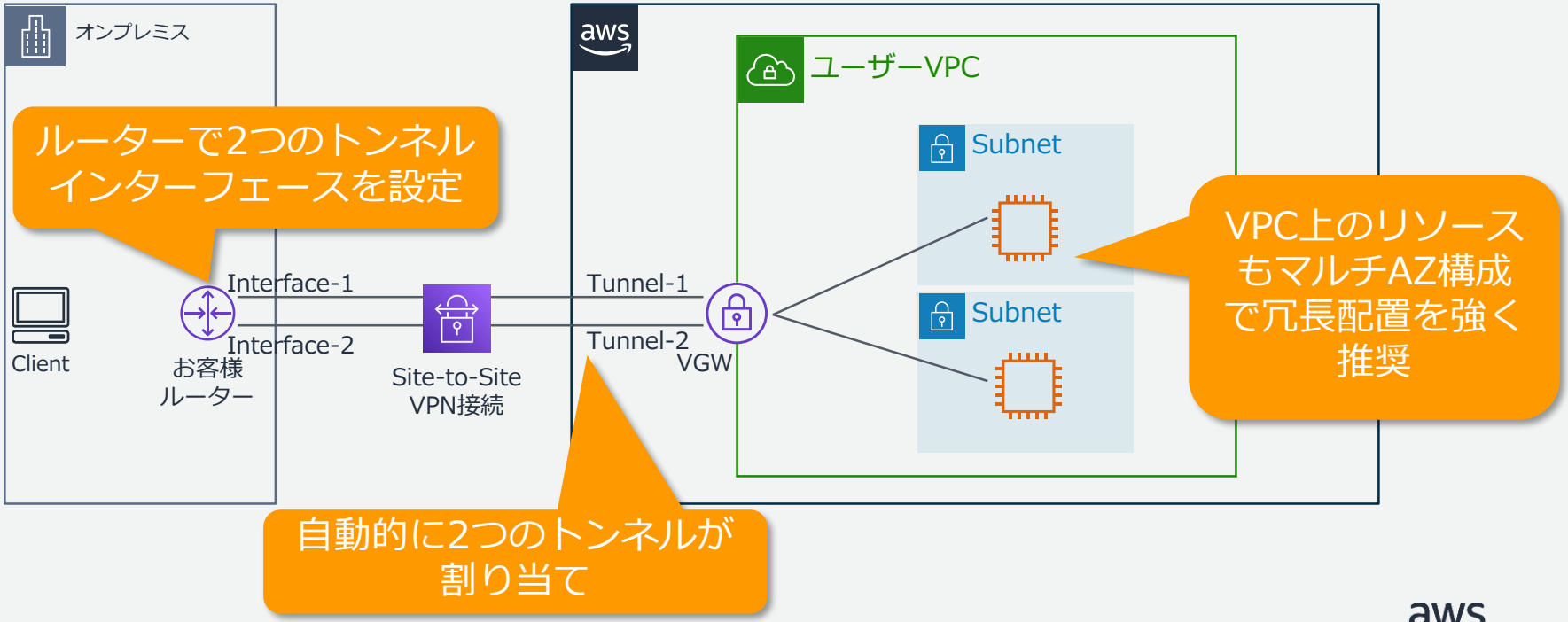
Agenda

- ✓ オンプレミスからAWSへプライベート接続する方法
  - ➢ AWSにおけるVPN接続の種類
  - ➢ AWS Site-to-Site VPNとは？
  - ➢ AWS Site-to-Site VPNの設定
  - ➢ 2つのターゲットゲートウェイ - VGW or TGW
- ✓ **VPNの冗長化**
  - ➢ 仮想プライベートゲートウェイ(VGW)
  - ➢ トランジットゲートウェイ(TGW)
  - ➢ Direct Connectとの併用
- ✓ AWS Site-to-Site VPNを利用した拠点間通信
- ✓ よくあるお問合せ
- ✓ まとめ
- ✓ 参考
  - ➢ AWS Site-to-Site VPNにおける直近のアップデート
  - ➢ AWS Site-to-Site VPNの利用料金

AWS Site-to-Site VPNの冗長化
仮想プライベートゲートウェイ(VGW)

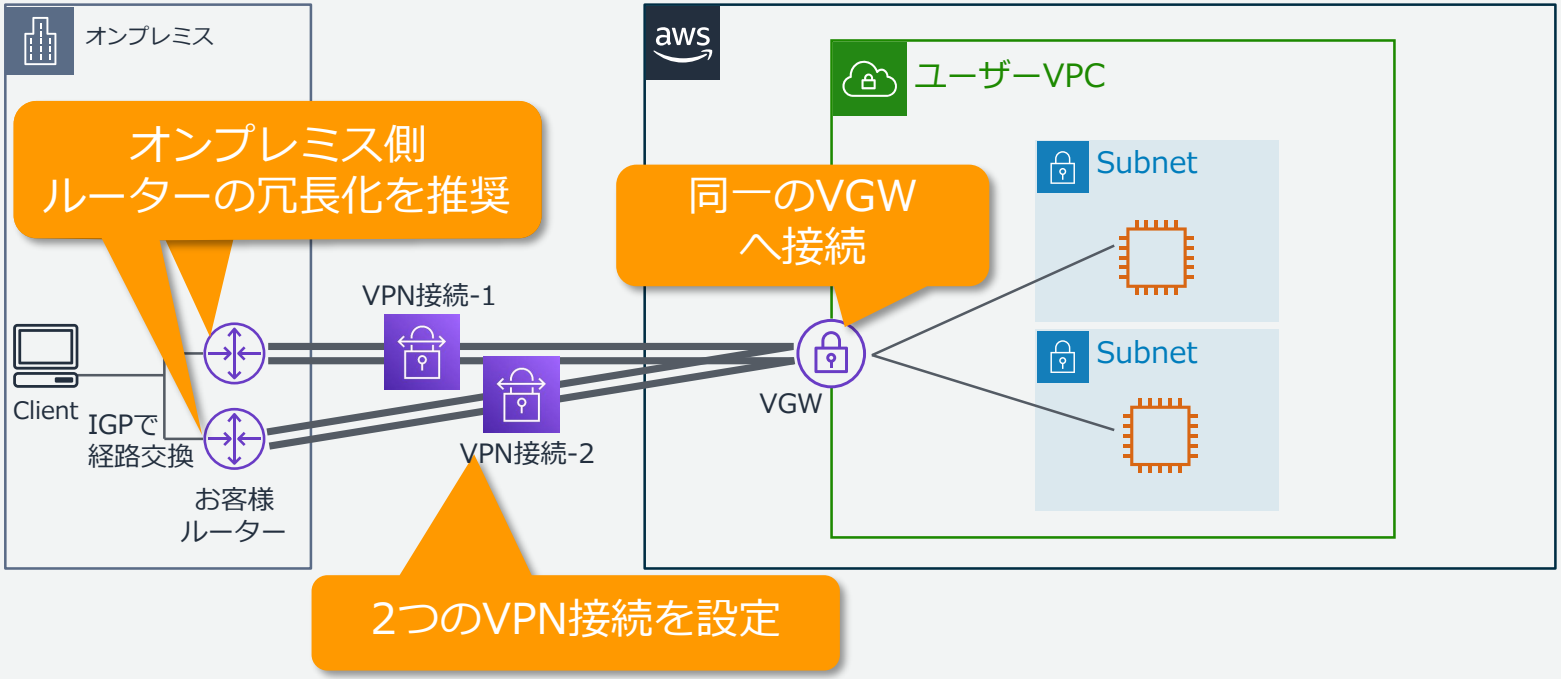
冗長化の考え方：1つのVPN接続で2つのIPsecトンネル

1つのAWS Site-to-Site VPNを作成すると、2つのIPsecトンネルを利用可能。
両方のトンネルをUp状態に保つことが重要。
VGWは内部的に冗長化済み。



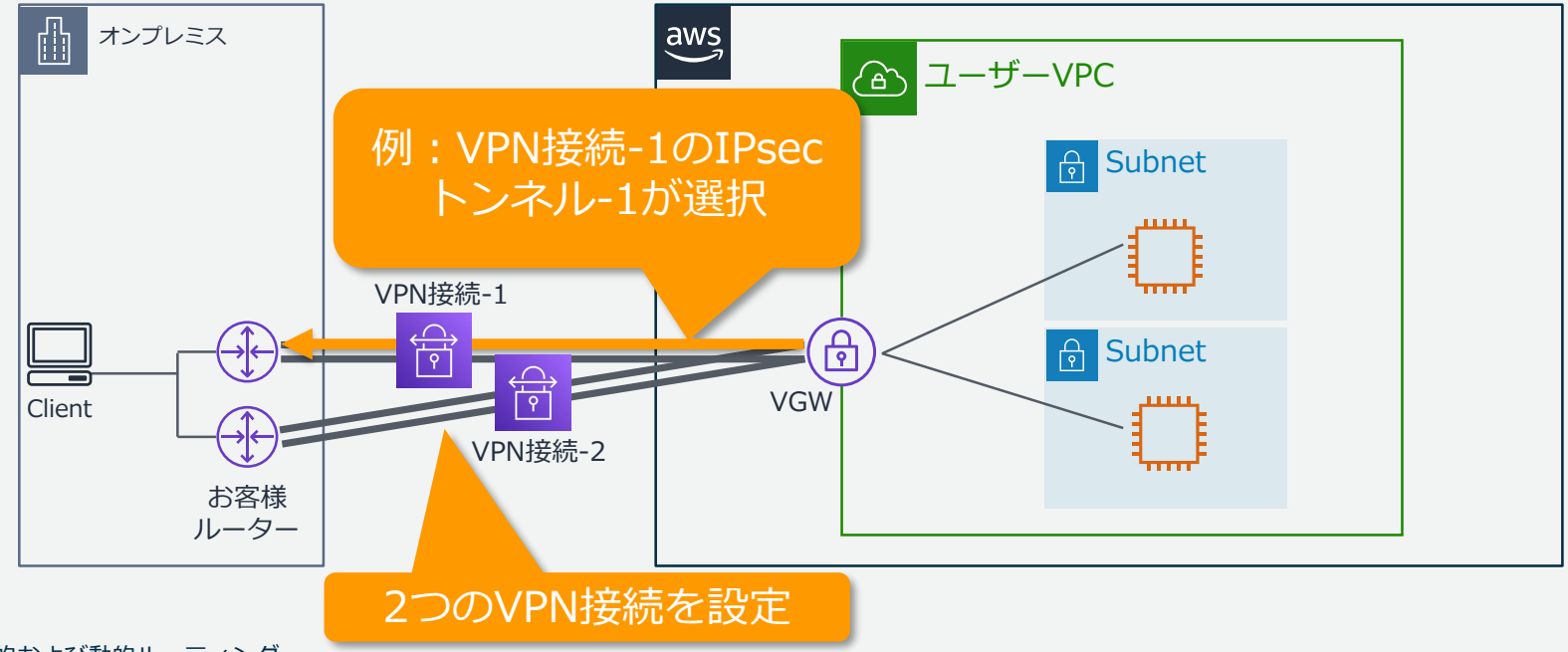
冗長化の考え方：単一障害点となるルーターを冗長化

オンプレミス側のカスタマーゲートウェイ（CGW）を冗長化することで、
単一障害点を無くす事を推奨。
2 IPsecトンネル x 2 VPN接続 = 合計4つのIPsecトンネルで冗長化。



VGW接続の際の優先制御：AWS→オンプレミス

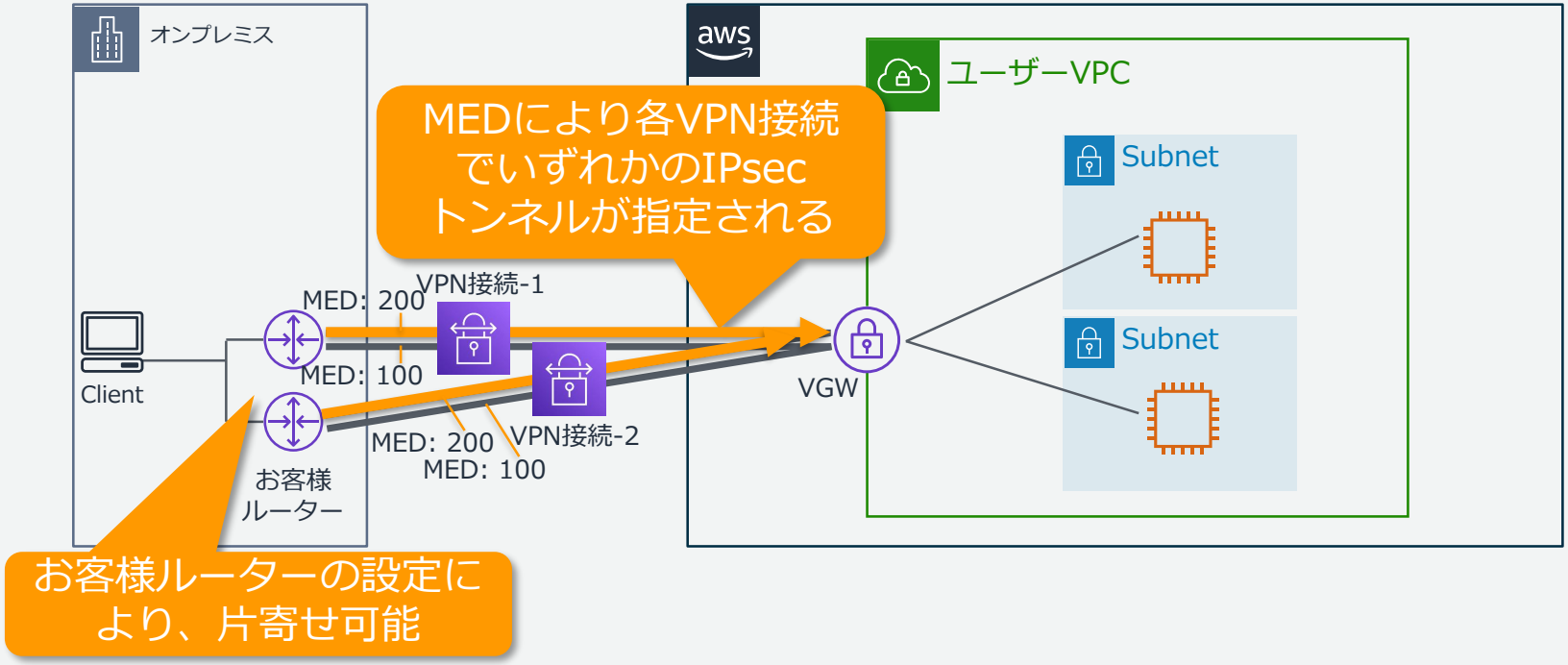
AWSからオンプレミス方向への経路は、AWS側のアルゴリズムにより、冗長化されたIPsecトンネルのうち、いずれか一つが選択される(Active-Standby)。
お客様ルーターでAS Path PrependやMEDを設定することにより制御可能。



静的および動的ルーティング
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/VPNRoutingTypes.html#vpn-route-priority

VGW接続の際の優先制御：オンプレミス→AWS

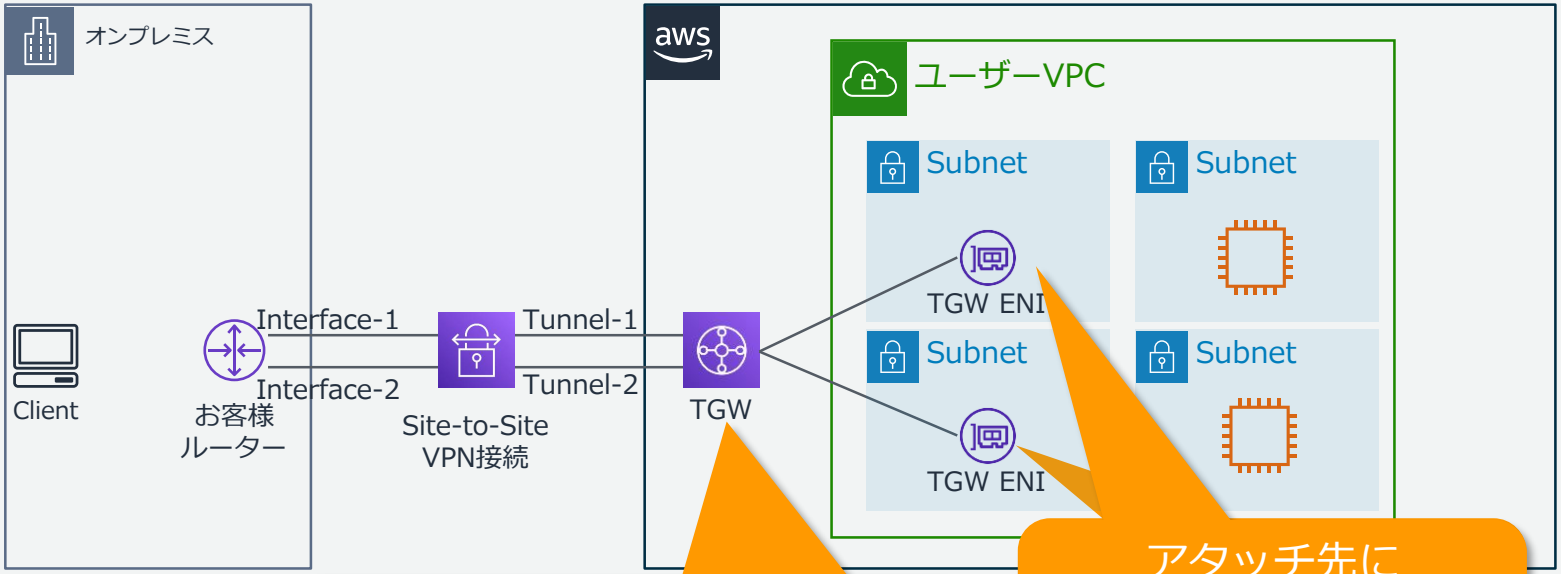
オンプレミスからAWS方向への経路は、お客様ルーターがMEDによる制御に対応している場合、AWSが付与するMED値によって各AWS接続ごとに優先するIPsecトンネルが決定する。



AWS Site-to-Site VPNの冗長化
トランジットゲートウェイ(TGW)

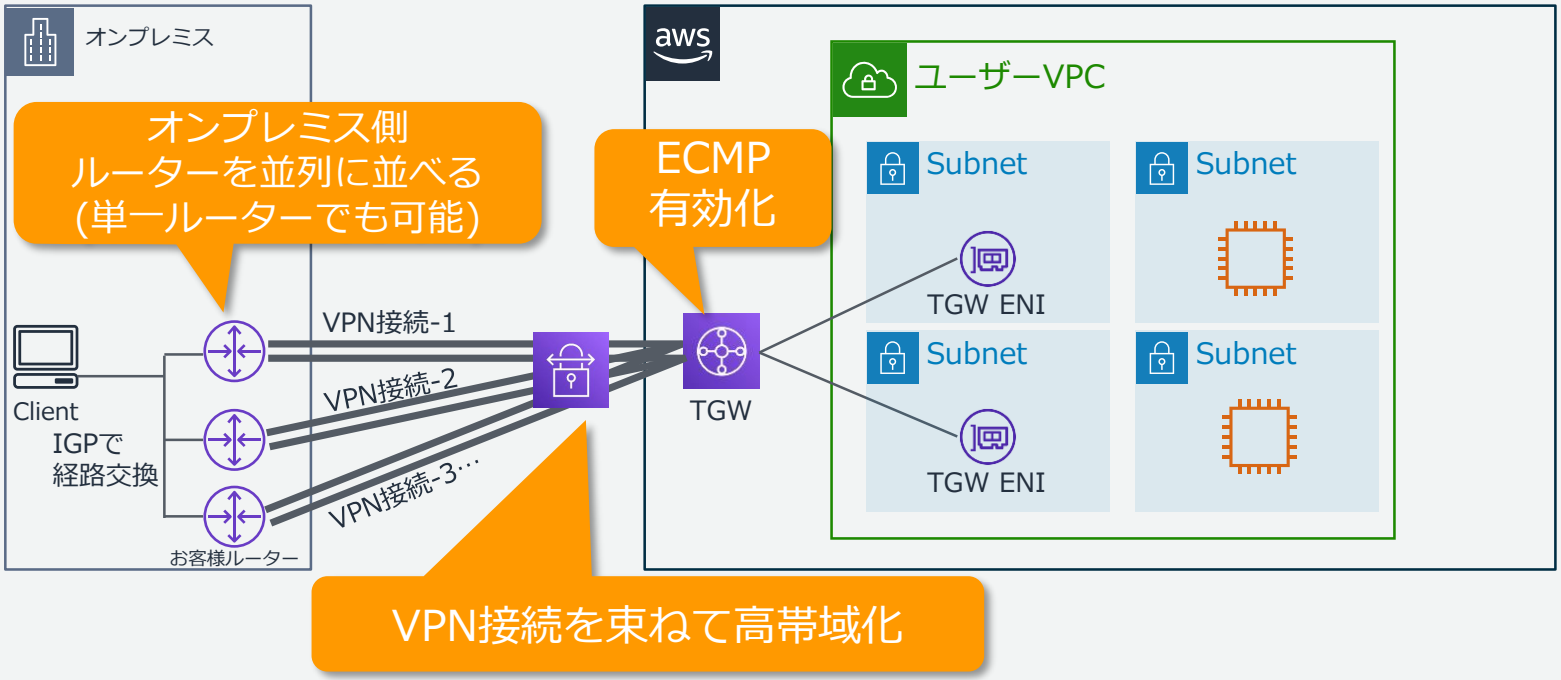
冗長化の考え方：1つのVPN接続で2つのIPsecトンネル

VGW接続と同様に1つのVPN接続で2つのIPsecトンネルが提供される。
TGWはHyperplaneテクノロジーにより、大量の計算ノードで冗長構成済み。
アタッチ先に二つのSubnetを指定し、単一AZ障害時に他方のAZで通信を継続。



冗長化の考え方：複数のVPN接続に通信を分散するECMP

CGWを冗長化し、TGWでEqual Cost Multi Path(ECMP)を有効化することで、
複数のIPsecトンネルを等価で利用することが可能。



冗長化の考え方：ECMP利用時の考慮ポイント

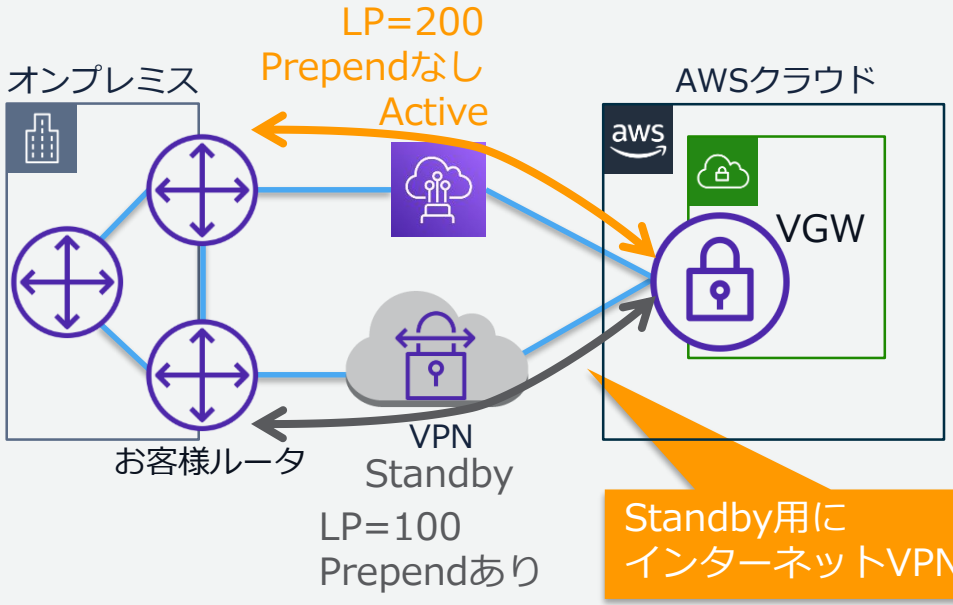
- TGWでEqual Cost Multi Path(ECMP)を有効化すると、同じTGWに接続しているすべてのVPN接続に対し、ECMPが有効となる。
- Internetを経由するため、レイテンシーに一貫性を求めない場合に利用。恒久的に広帯域を必要とする場合、Direct Connect利用を推奨。
- オンプレミス→VPC方向への通信は、お客様ルーターへ適切な設定を行うことで通信が分散するようにする。
- 行きと帰りのトラフィックが異なる経路を通る「非対称ルーティング」となる可能性がある。お客様ルーターがセキュリティ機能やセッション管理を実装している場合、パケットをドロップしてしまう可能性がある。回避するには、ルーターベンダーが公開している非対称ルーティングを許容する設定を行う必要がある。

  参考：What is the default setting for 'set flow tcp-syn-check' and how do you check
  https://kb.juniper.net/InfoCenter/index?page=content&id=KB4444

AWS Site-to-Site VPNの冗長化
Direct Connectとの併用

経路制御：Direct Connect/VPN(BGP)

- Direct Connectのバックアップとしてインターネット VPNを利用
- VPN接続は動的経路制御(BGP)を利用することを推奨
- 予算面で、同等のDirect Connect回線を用意できない際の代替手段



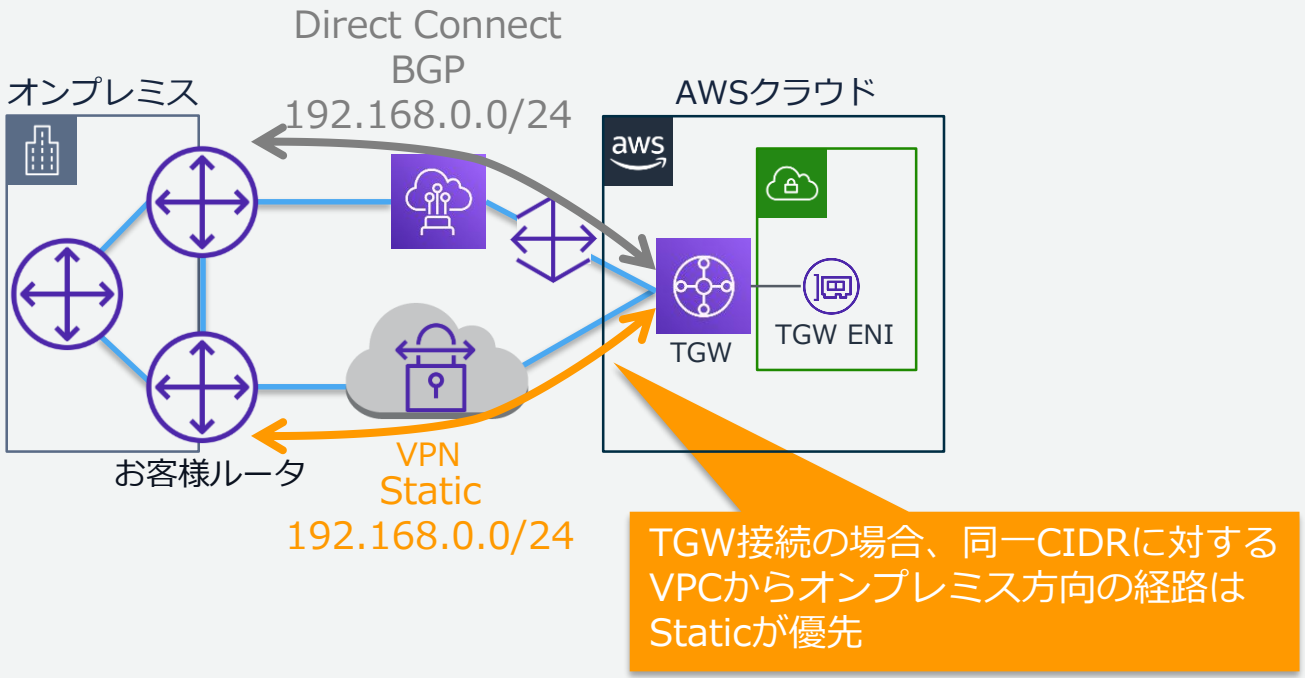
フェールオーバー時にはDirect Connectとインターネット VPNとの性能差からパフォーマンスに影響が出る場合があるため注意

※ 仕様上、AWSからオンプレミス方向への通信は(AS Path Prependの有無によらず)常にDirect Connectを優先経路となる

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/

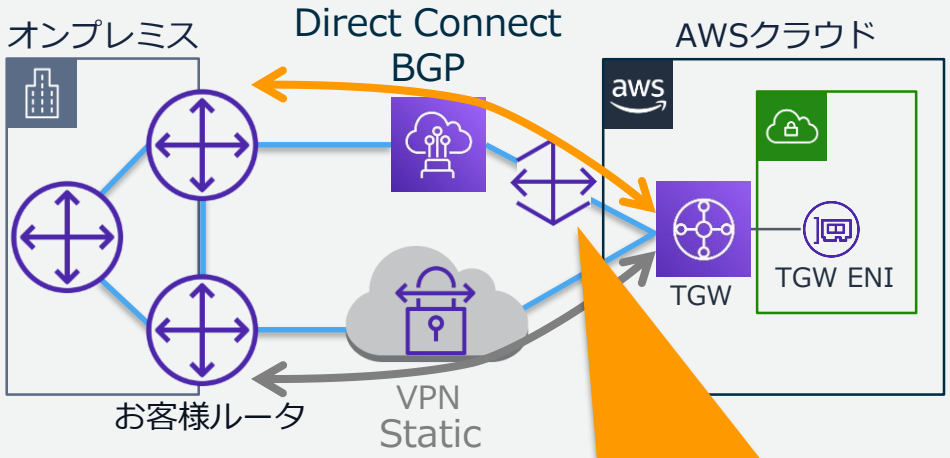
注意点：TGW接続のDirect Connect/VPN(Static)

- TGW接続でVPNで静的経路制御(Static)を利用し、同一のCIDRを利用した場合、VPNの経路が優先される



注意点： TGW接続のDirect Connect/VPN(Static) 続き

- 可能ならBGPの利用を推奨するが、やむを得ない場合、Direct Connect側で広報する経路を分割し、より詳細な経路を広報する

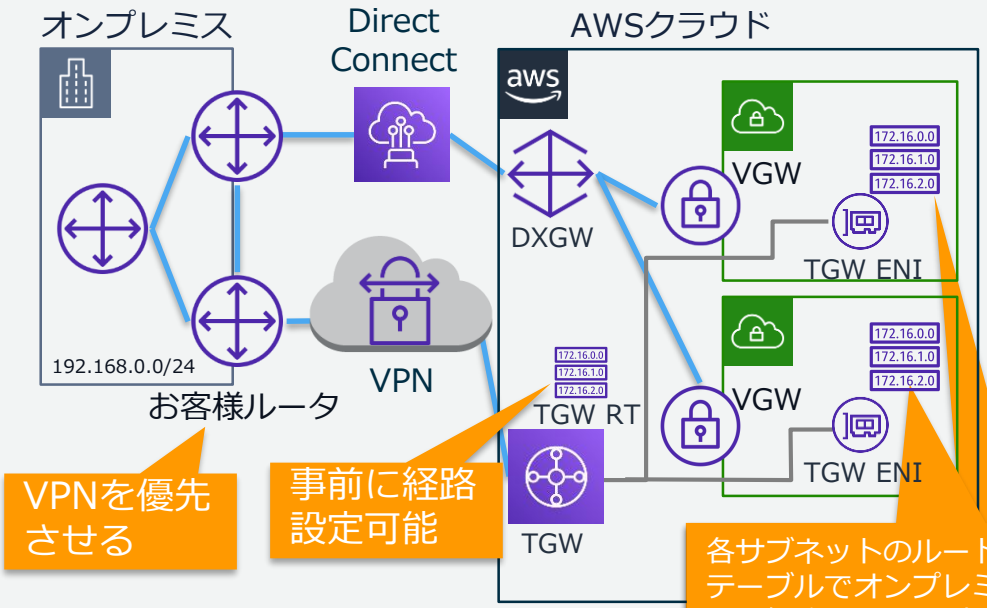


バックアップ用途として、VPNでStatic接続を利用し、Direct Connectを優先する場合の例：
- Direct Connectで2経路を広報する
  192.168.0.0/25
  192.168.128.0/25
- VPNでオンプレミスCIDRを1つ設定
  192.168.0.0/24

Direct Connect側経路をより詳細な経路とすることで、VPNをバックアップ用途として利用

複数VPCに対するバックアップ用途のSite-to-Site VPN

- VPCが複数ある場合、迂回用のTransit Gateway(TGW)にVPN接続し、VPCからオンプレミスへの経路をVGWからTGWへ手動で切り替える
- 各VPCのサブネットルートテーブルで切り替えが必要（TGWルートテーブルは事前設定可能）
- オンプレミスルーター側でも、Direct ConnectからVPNへ経路切り替えが必要



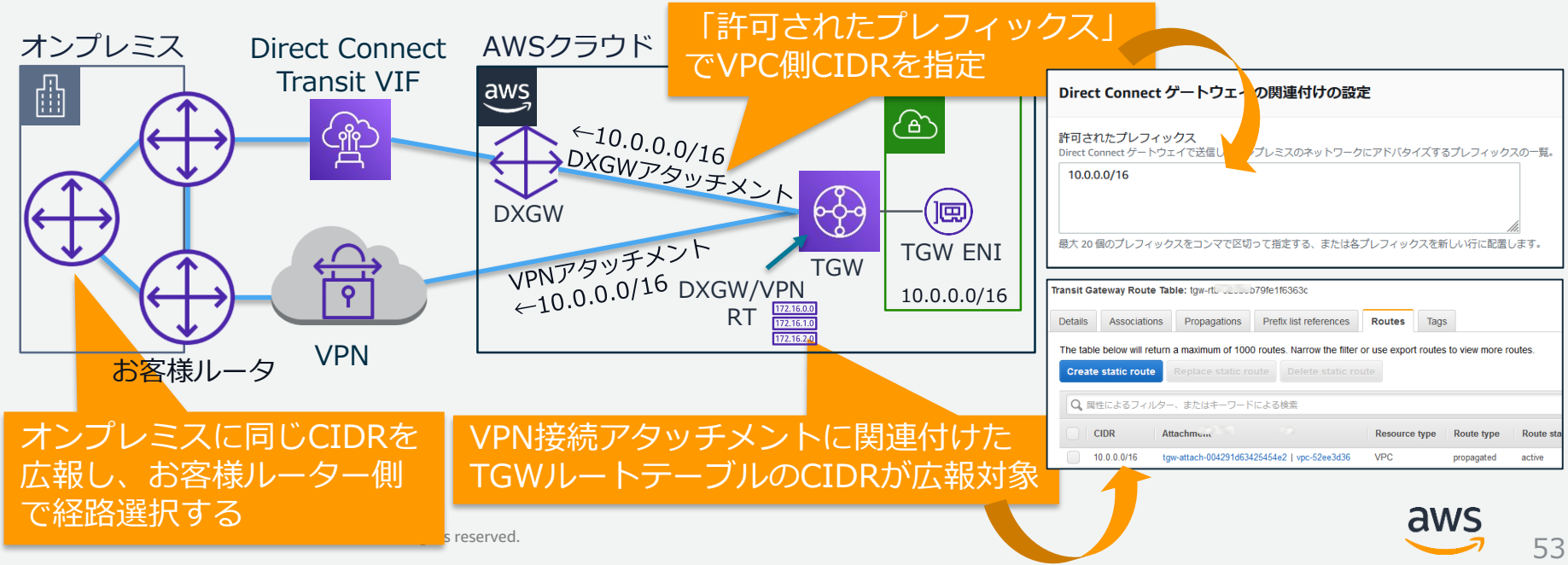
VPCサブネットルートテーブルの操作

通常時はオンプレミス向け経路をVGWへ設定
- VGWのルート伝播(Propagation)を有効時
  192.168.0.0/24のターゲット VGW #自動追加
- VGWのルート伝播(Propagation)を無効時
  192.168.0.0/24のターゲット VGW #手動追加

迂回時はオンプレミス向け経路をTGWへ変更
- VGWのルート伝播(Propagation)を有効時
  192.168.0.0/24のターゲット VGW #自動追加
  192.168.0.0/24のターゲット TGW #手動追加 (有効)
- VGWのルート伝播(Propagation)を無効時
  192.168.0.0/24のターゲット TGW #手動変更

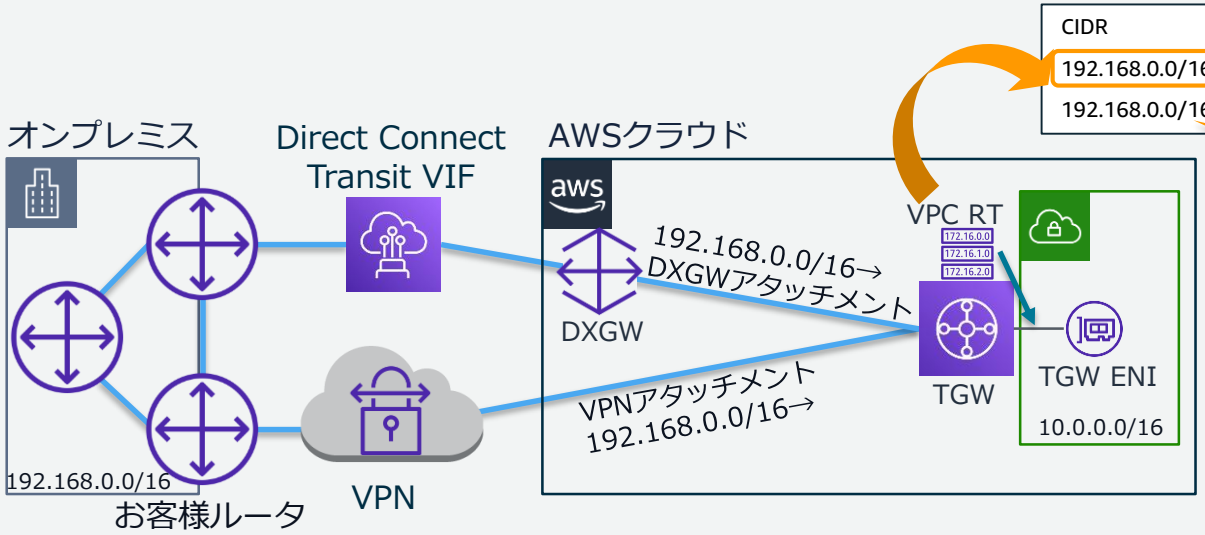
経路制御：TGW接続のDirect Connect/VPN(BGP)

オンプレミスからAWSへ通信する際の経路選択
- Transit VIF + Direct Connect Gateway(DXGW)でTGW接続の場合、DXGWのTGWアタッチメントで「許可されたプレフィックス」にオンプレミスへ広報するVPC側CIDRを指定する
- VPNでTGW接続の場合、TGWのルートテーブルのCIDRがオンプレミスへ広報される



経路制御：TGW接続のDirect Connect/VPN(BGP)

AWSからオンプレミスへ通信する際の経路選択
- TGWのルートテーブル内で、同じCIDRに対して別のアタッチメントの経路が重複した場合、Direct Connect Gatewayアタッチメントから伝達した経路が優先される



CIDR	Attachment	Resource Type	Route Type	
192.168.0.0/16	tgw-attach-xx	DXGW	propagate	<優先
192.168.0.0/16	tgw-attach-xx	VPN	propagate	

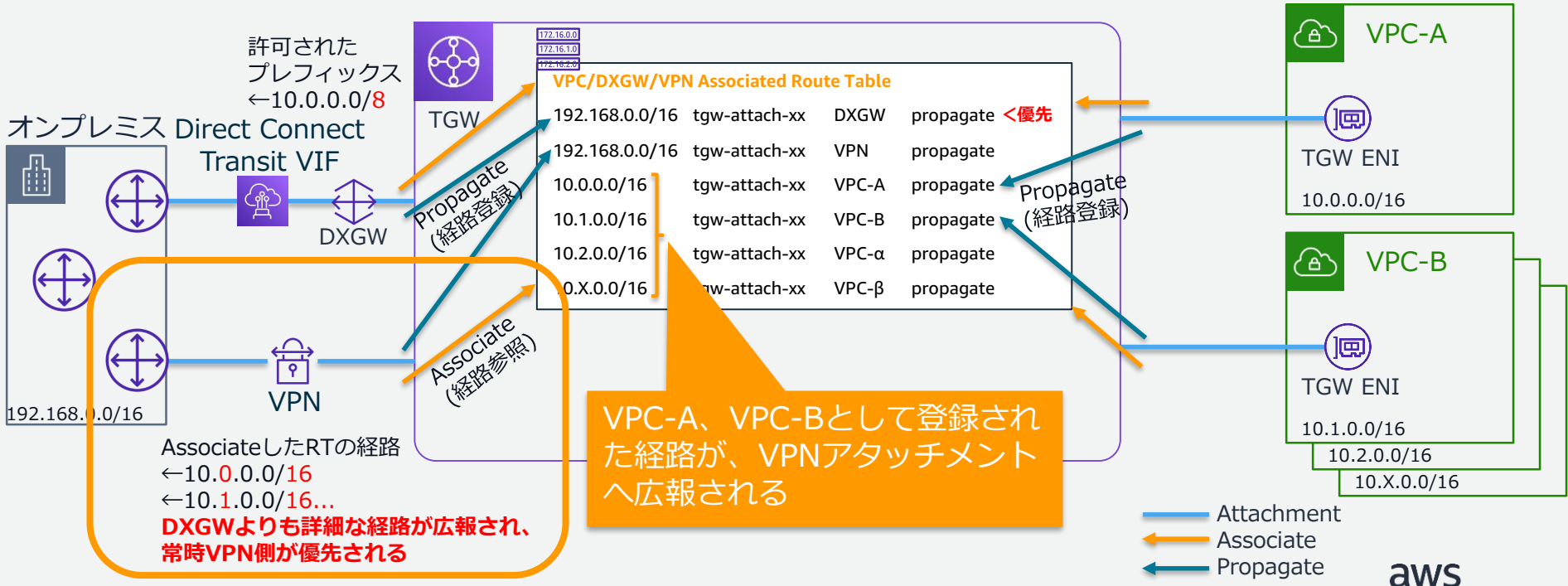
オンプレミスから同じCIDRが広報され、1つのルートテーブル内で重複

参考：トランジットゲートウェイのルートの評価順序
A) 送信先アドレスの最も具体的なルート
B) 送信先 IP アドレスが同じでもターゲットが異なるルートの場合、ルートの優先順位は以下です
1. 静的ルート (例：Site-to-Site VPN 静的ルート)
2. プレフィックスリスト参照ルート
3. VPC が伝達したルート
4. Direct Connectゲートウェイが伝達したルート
5. トランジットゲートウェイピア接続 が伝達したルート
6. Site-to-Site VPN 伝達ルート

トランジットゲートウェイの動作 > ルートの評価順序
https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/how-transit-gateways-work.html

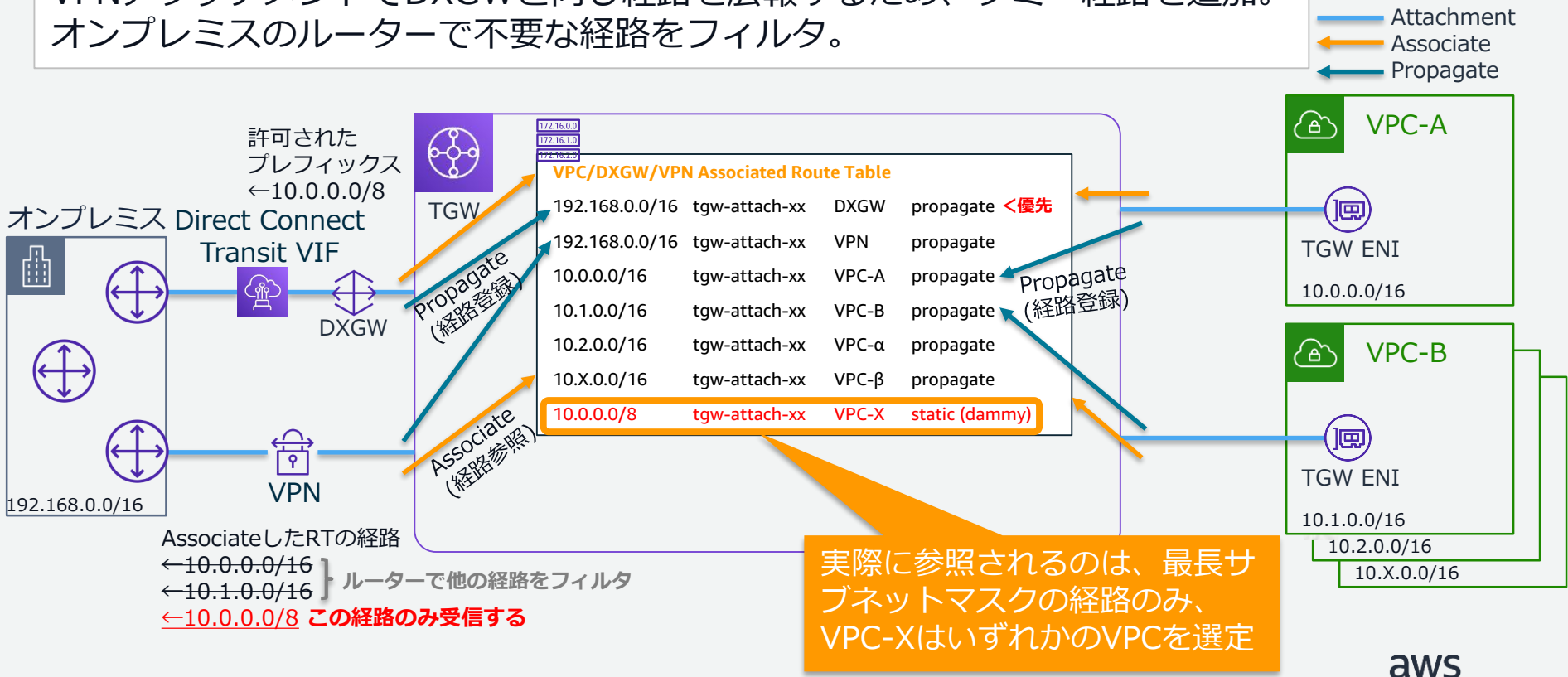
経路制御：ルート設計上の課題

TGW終端のVPN接続では、関連付けられたルートテーブルの経路が、オンプレミスルーターへ広報される。 VPC CIDR数が20を超え、 Direct Connect GatewayアタッチメントでVPC CIDRを集約した場合、ロンゲストマッチにより、常時、VPN接続の経路が優先される。



経路制御：ルート設計例-オンプレミスルーターでフィルタ

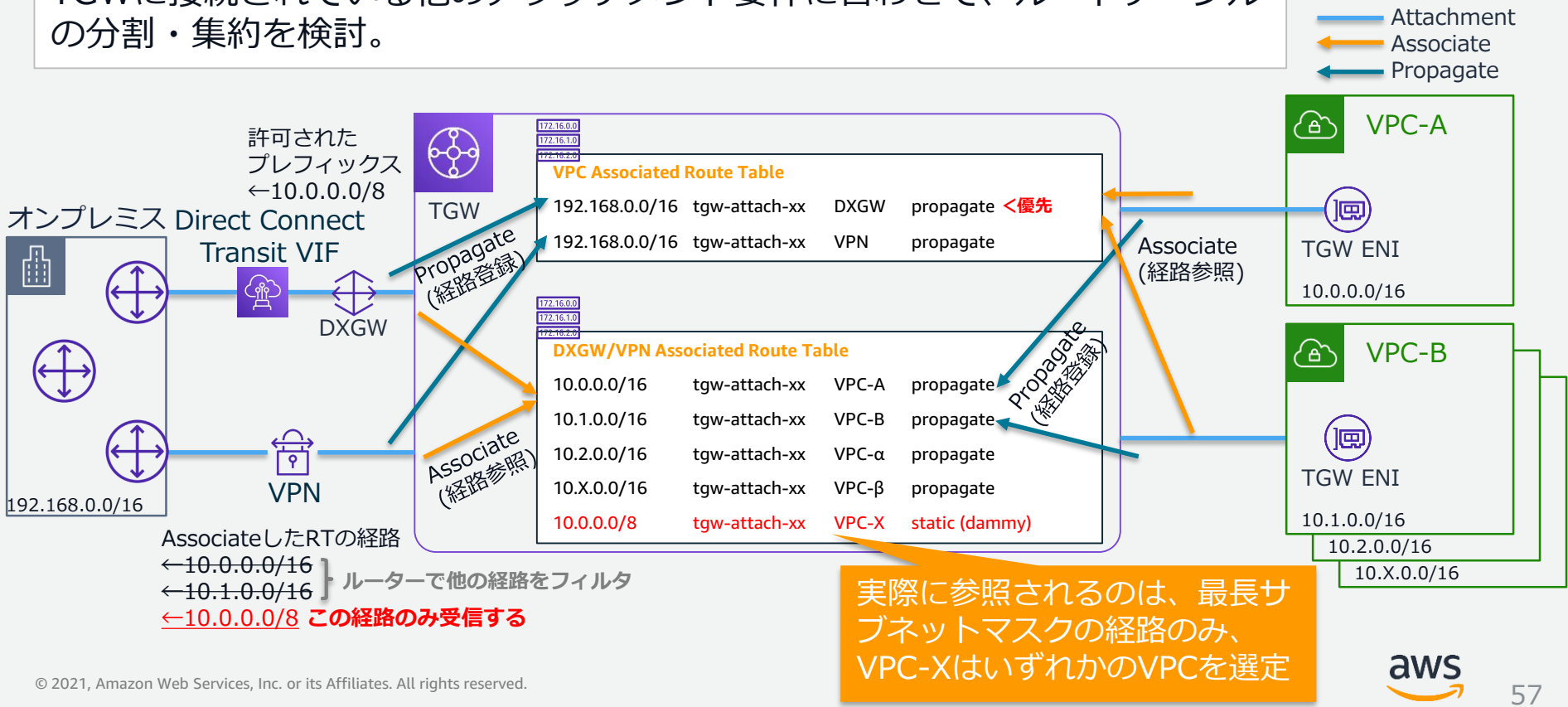
1つのルートテーブルですべてのアタッチメントを利用する設計。
VPNアタッチメントでDXGWと同じ経路を広報するため、ダミー経路を追加。
オンプレミスのルーターで不要な経路をフィルタ。



56

経路制御：ルート設計例-オンプレミスルーターでフィルタ

ルートテーブルを2つに分けて管理することも可能。
TGWに接続されている他のアタッチメント要件に合わせて、ルートテーブルの分割・集約を検討。



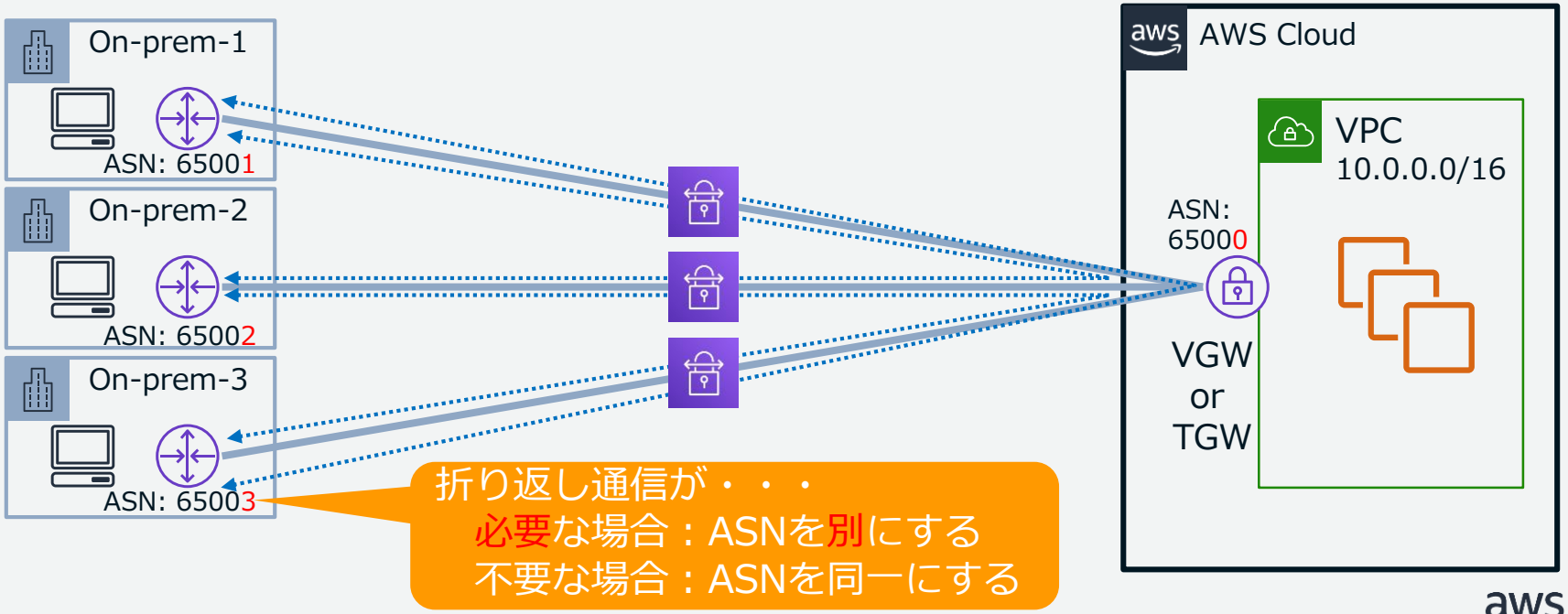
Agenda

- ✓オンプレミスからAWSへプライベート接続する方法
  - ➢AWSにおけるVPN接続の種類
  - ➢AWS Site-to-Site VPNとは？
  - ➢AWS Site-to-Site VPNの設定
  - ➢2つのターゲットゲートウェイ - VGW or TGW
- ✓VPNの冗長化
  - ➢仮想プライベートゲートウェイ(VGW)
  - ➢トランジットゲートウェイ(TGW)
  - ➢Direct Connectとの併用
- ✓**AWS Site-to-Site VPNを利用した拠点間通信**
- ✓運用時の確認ポイント
- ✓よくあるお問合せ
- ✓まとめ
- ✓参考
  - ➢AWS Site-to-Site VPNにおける直近のアップデート
  - ➢AWS Site-to-Site VPNの利用料金

AWS Site-to-Site VPNを利用した拠点間通信

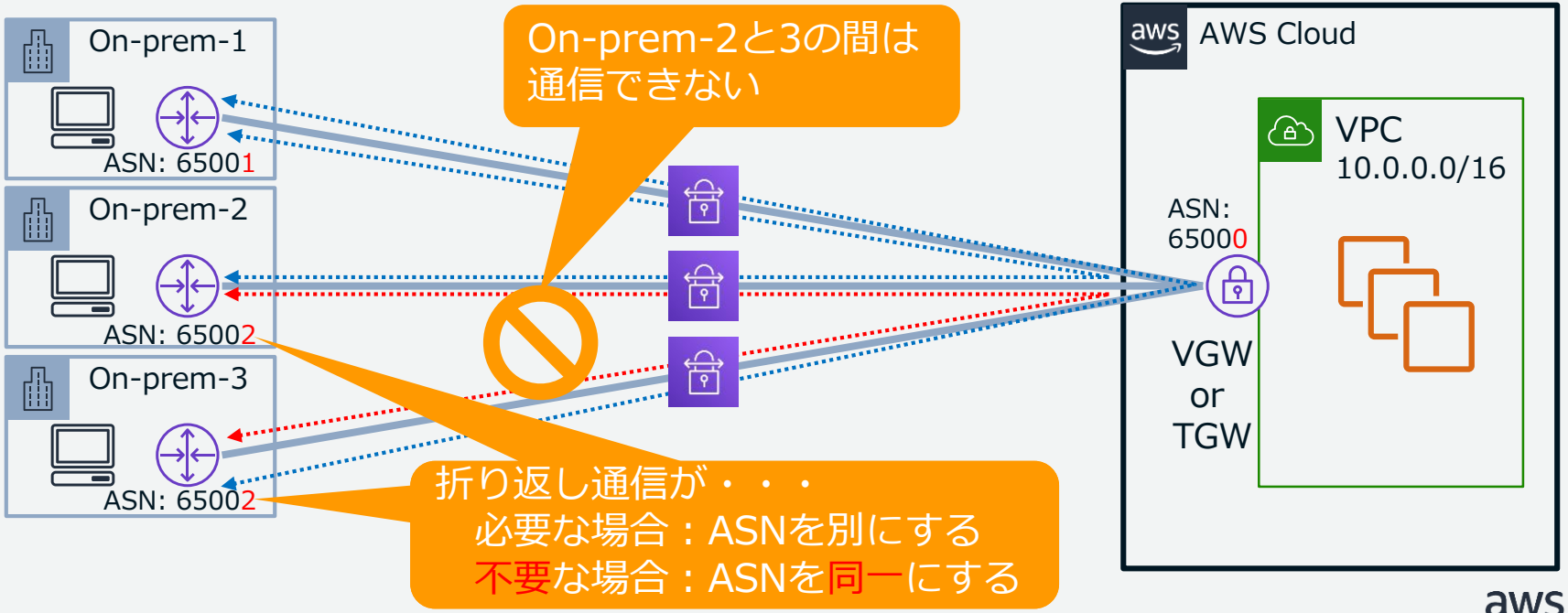
AWS VPNを使った拠点間通信: AWS VPN CloudHub

同一のVGW/TGWに接続された動的AWS VPN間でASNをユニークにすることで、折り返し通信が可能。AWS VPN CloudHubと称し、特別な設定は不要。AWS側の設定で無効化する機能は無い。



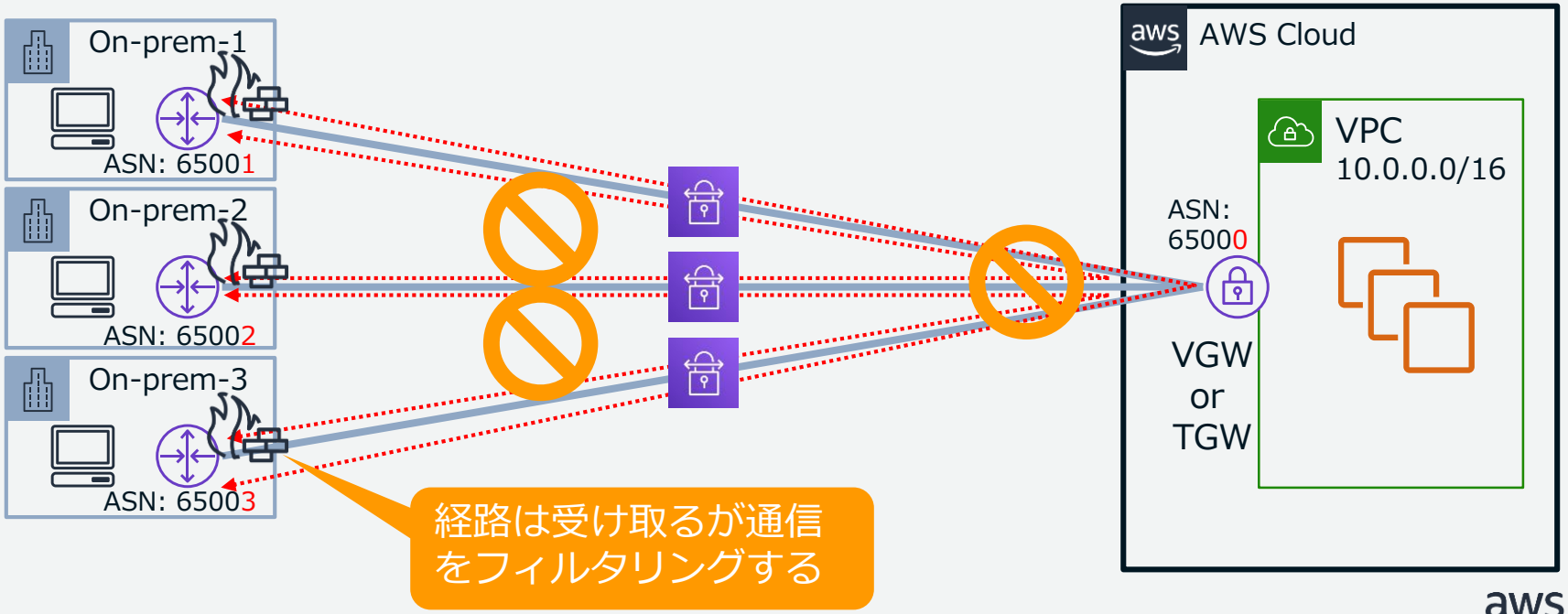
折り返し通信の制限：同一ASNを利用

他の組織間で折り返し通信を制限したい場合、同一ASNから受け取った経路をルートテーブルに反映しないBGPの特性を活用。
各拠点は引き続きVPCと通信可能。



折り返し通信の制限：より厳密に制限

拠点間通信をより厳密に制限したい場合、各オンプレミスのお客様ルーターでフィルタリングすることを推奨。
VPC CIDRに対してのみ、許可ルールを設定。



Agenda

- ✓オンプレミスからAWSへプライベート接続する方法
  - ➢AWSにおけるVPN接続の種類
  - ➢AWS Site-to-Site VPNとは？
  - ➢AWS Site-to-Site VPNの設定
  - ➢2つのターゲットゲートウェイ - VGW or TGW
- ✓VPNの冗長化
  - ➢仮想プライベートゲートウェイ(VGW)
  - ➢トランジットゲートウェイ(TGW)
  - ➢Direct Connectとの併用
- ✓AWS Site-to-Site VPNを利用した拠点間通信
- **✓運用時の確認ポイント**
- ✓よくあるお問合せ
- ✓まとめ
- ✓参考
  - ➢AWS Site-to-Site VPNにおける直近のアップデート
  - ➢AWS Site-to-Site VPNの利用料金

運用時の確認ポイント

運用時の確認ポイント：マネージメントコンソール

- 通信に問題が発生した場合、以下の項目を確認

マネジメントコンソール：VPCダッシュボード＞サイト間のVPN接続
　＞対象のVPN接続設定選択
　　＞画面下の[トンネル詳細]タブ

[正常時]

VPN 接続: vpn-0b83[redacted]a879

詳細 | トンネル詳細 | タグ

トンネルの状態

2 中の 1 ～ 2

トンネル番号	外部 IP アドレス	内部 IPv4 CIDR	内部 IPv6 CIDR	ステータス	ステータスの最終変更日	詳細	証明書 ARN
Tunnel 1	52.[redacted]0	169.254.79.236/30	-	アップ	2021年8月[redacted]:48 UT…	3 BGP ROUTES	
Tunnel 2	52.[redacted]9	169.254.209.240/30	-	アップ	2021年8月[redacted]:09 UT…	3 BGP ROUTES	

各トンネルの状態

[非正常時]

ステータス	ステータスの最終変更日	詳細
ダウン	2021年7月[redacted]:46 UTC+9	IPSEC IS DOWN
アップ	2021年8月[redacted]:09 UT…	3 BGP ROUTES

この時間帯に何らかの問題がなかったかを確認する

オンプレミスからAWSへ広報しているCIDRの数

運用時の確認ポイント：Amazon VPC Reachability Analyzer

ネットワークが目的どおりに設定されているかを確認する手段
パケットを一切送信せずに2つのエンドポイント間での到達性を解析可能
インスタンスから仮想プライベートゲートウェイまでの通信確認などに利用

運用時の確認ポイント：VPCフローログ

EC2などのネットワークインターフェイスを通過する情報をキャプチャする機能

Amazon CloudWatch Logs、またはAmazon S3に保存

ログを取得した際、オリジナルの通信に対してスループットやレイテンシーなどの影響はない

取得単位はVPC、サブネット、ENI

すべてのトラフィック、許可、拒否から選択可能

- フロー元/先のAWSサービス名を確認
- 通過するゲートウェイを確認

  例：1-同じVPC、3-VGW経由、4-VPCピア など

フィールド	内容
version	3
account-id	384767312456
interface-id	eni-0b62d5e000e412345
srcaddr	108.56.192.231
dstaddr	172.31.0.202
srcport	50565
dstport	80
protocol	6
packets	7
bytes	751
start	1573704396
end	1573704455
action	ACCEPT
log-status	OK
vpc-id	vpc-0af48868ceeb12345
subnet-id	subnet-02ab634d2e4c12345
instance-id	i-0a998a68301112345
tcp-flags	3
type	IPv4
pkt-srcaddr	108.56.192.231
pkt-dstaddr	172.31.0.202
region	ap-northeast-1
az-id	apne1-az1
sublocation-type	-
sublocation-id	-
pkt-src-aws-service	-
pkt-dst-aws-service	EC2
flow-direction	ingress
traffic-path	3

運用時の確認ポイント：その他の情報

- **お客様ルーターのログ**
  状況を正確に把握するため、タイムスタンプ付きのログを保管、通信断につながる情報を確認

ない場合
不要
board
術サポートへ

- **Internetサービスプロバイダへ問合せ**
  回線不具合やVPNエンドポイント※へのリーチャビリティに影響する経路上での問題有無を確認（※マネジメントコンソールに記載の”外部IPアドレス”）

https://aws.amazon.com/jp/premiumsupport/technology/personal-health-dashboard/
https://status.aws.amazon.com/

Agenda

- ✓オンプレミスからAWSへプライベート接続する方法
  - ➢AWSにおけるVPN接続の種類
  - ➢AWS Site-to-Site VPNとは？
  - ➢AWS Site-to-Site VPNの設定
  - ➢2つのターゲットゲートウェイ - VGW or TGW
- ✓VPNの冗長化
  - ➢仮想プライベートゲートウェイ(VGW)
  - ➢トランジットゲートウェイ(TGW)
  - ➢Direct Connectとの併用
- ✓AWS Site-to-Site VPNを利用した拠点間通信
- ✓運用時の確認ポイント
- **✓よくあるお問合せ**
- ✓まとめ
- ✓参考
  - ➢AWS Site-to-Site VPNにおける直近のアップデート
  - ➢AWS Site-to-Site VPNの利用料金

AWS Site-to-Site VPNに関する
よくある問合せ

YAMAHA社製ルーターについて

Q: IPsecトンネルはアップしても、BGPがDownのまま

A: BGPの設定を反映させるため、”bgp configure refresh“を実行してください。

参考：http://www.rtpro.yamaha.co.jp/RT/docs/bgp/bgp4-command.html#bgp_configure_refresh

Q: AWSからオンプレミス方向への通信を制御するため、AS Path Prependの利用を推奨されたが、対応していない

A: BGPのアトリビュートであるMEDをご利用ください。

参考：http://www.rtpro.yamaha.co.jp/RT/docs/bgp/bgp4-command.html#bgp_neighbor

Q: ipsec ike local id / remote idの指定で”/0”とマスク指定するとエラーとなる

A: お使いのルーターでOSを最新版にアップデートすることで対応ください。

オンプレミスとVPCのCIDR設計

Q: オンプレミスCIDRとVPC CIDRが重複しているが、通信する方法はないか？

A: VPC CIDRを変更することが不可能な場合、お客様ルーターでSource NATとDestination NATを併用し、重複を回避ください。

Q: VPCのPrivate NAT Gatewayを使い、オンプレミスCIDRと重複したVPC CIDRに通信させることは可能か？

A: Privte NAT Gatewayでは、Destination NATを実装しておりません。オンプレミスホストがVPC内のIPに到達するためには、VPNで利用するお客様ルーターを超える必要がありますが、オンプレミス内にも存在するIPアドレスに対しては、これが不可能です。

Q: オンプレミスのCIDRからL2延伸してVPCにVPN接続したい

A: AWS VPNではLayer 2接続をサポートしていません。

メンテナンスの影響について

Q: AWS VPNにおけるAWS側メンテナンス時に連絡はありますか？

A: 特別な理由が無い限り、メンテナンスにおいてお客様への通知は行われません　このため、 冗長性を確保するために２つのトンネルを設定しUp状態とすることが重要です。

Q: 片方のトンネルがダウンしましたがメンテナンスですか？

A: 片側だけのトンネルがダウンした後、自動的に復旧した場合、AWS側のメンテナンスが行われていた可能性があります。自動的に両方のトンネルがUp状態へ復帰していれば、お客様側で特に必要なアクションはありません。いずれかのトンネルが復旧しない場合、お客様ルーター操作により、IPsecトンネルや論理/物理インターフェイスのDown/Up、（可能であれば）ルーターの再起動をお試しください。

Q: 定期的にIPsecトンネルがDown/Upを繰り返すのはメンテナンスの影響ですか？

A: 途中経路で扱えるMTUサイズが小さく、IPsecの鍵を更新する際に必要なパケットが破棄されている可能性があります。IKE SA/IPsec SAのlifetimeを短くすることで改善できることがあります。

クォータについて

Q: AWS VPN接続を利用して1つのVPCに最大でいくつの拠点からアクセスできますか？

A: 以下にクォータの情報が記載されておりますので、「仮想プライベートゲートウェイあたりの Site-to-Site VPN 接続の数」をご確認ください。本資料作成時点では、10となります。より多くの拠点をVPCに接続する要件の場合、トランジットゲートウェイの利用を推奨いたします。各数値について、引き上げをリクエスト出来る場合がありますが、引き上げ可能であることをお約束するものではございません。

参考：Site-to-Site VPN のクォータ

https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/vpn-limits.html

VPNトンネルエンドポイントについて

Q: AWS側エンドポイントが更新された時に通知されますか？

A: AWS側のVPNトンネルエンドポイントの一方または両方が交換されたときに、AWS Personal Health Dashboardにトンネルエンドポイント交換通知が表示されます。

参考：AWS Health イベントを使用した VPN 接続のモニタリング
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/monitoring-vpn-health-events.html#tunnel-replacement-notifications

Q: AWS側エンドポイントが更新された時にVPN通信に影響しますか？

A: AWS Site-to-Site VPNはマネージドサービスである特性上、AWSにより定期的に更新処理を行います。この際、VPN接続は自動的に2番目のトンネルにフェイルオーバーして、アクセスが中断されないようにします。このため、カスタマーゲートウェイを設定するときは、両方のトンネルを設定することが重要です。

参考：Site-to-Site VPN トンネルエンドポイントの置換

https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/endpoint-replacements.html

途中経路、障害検知について

Q: AWS VPN接続でパスMTU検出(Path MTU Discovery)できますか？

A: AWS Site-to-Site VPNではパスMTU検出をサポートしていません。あらかじめお客様ルーターの論理インターフェイスのMTUを1399バイトに設定してください。

参考：Site-to-Site VPN のクォータ
https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/vpn-limits.html

Q:冗長化のトンネル間で障害検知を早めるためにBFD使えますか？

A: AWS Site-to-Site VPNではBFDによる障害検知をサポートしていません。より早く障害を検知するためには、お客様ルーターにてデッドピア検出（dead peer detection: DPD）を設定してください。

参考：カスタマーゲートウェイデバイスの VPN トンネルの非活動性、不安定性、またはトンネルダウンをトラブルシューティングするにはどうすればよいですか?

https://aws.amazon.com/jp/premiumsupport/knowledge-center/vpn-tunnel-instability-inactivity/

Agenda

- ✓オンプレミスからAWSへプライベート接続する方法
  - ➢AWSにおけるVPN接続の種類
  - ➢AWS Site-to-Site VPNとは？
  - ➢AWS Site-to-Site VPNの設定
  - ➢2つのターゲットゲートウェイ - VGW or TGW
- ✓VPNの冗長化
  - ➢仮想プライベートゲートウェイ(VGW)
  - ➢トランジットゲートウェイ(TGW)
  - ➢Direct Connectとの併用
- ✓AWS Site-to-Site VPNを利用した拠点間通信
- ✓運用時の確認ポイント
- ✓よくあるお問合せ
- **✓まとめ**
- ✓参考
  - ➢AWS Site-to-Site VPNにおける直近のアップデート
  - ➢AWS Site-to-Site VPNの利用料金

まとめ

AWS Site-to-Site VPN接続の種類、利用例を理解する

＞VGW接続/TGW接続の使い分け、TGWのみ利用可能なオプション

設定時に注意するべきポイントを把握する

＞サンプルコンフィグレーションを入手し環境に合わせ修正

運用時における確認項目、AWS側メンテナンスに対して備えておくべきことを認識する

＞2つのIPsecトンネルを常時Up状態に保つ
＞各トンネルのステータスをマネジメントコンソールで確認

詳細情報・最新情報へのポインタを得る

＞各説明ページ下部の公開ドキュメントURL、後述の直近アップデートも参照

Agenda

- ✓オンプレミスからAWSへプライベート接続する方法
  - ➢AWSにおけるVPN接続の種類
  - ➢AWS Site-to-Site VPNとは？
  - ➢AWS Site-to-Site VPNの設定
  - ➢2つのターゲットゲートウェイ - VGW or TGW
- ✓VPNの冗長化
  - ➢仮想プライベートゲートウェイ(VGW)
  - ➢トランジットゲートウェイ(TGW)
  - ➢Direct Connectとの併用
- ✓AWS Site-to-Site VPNを利用した拠点間通信
- ✓運用時の確認ポイント
- ✓よくあるお問合せ
- ✓まとめ
- ✓**参考**
  - ➢AWS Site-to-Site VPNにおける直近のアップデート
  - ➢AWS Site-to-Site VPNの利用料金

参考：AWS Site-to-Site VPNにおける直近のアップデート

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
2019/2	AWSサイト間VPNがIKEv2に対応	セキュリティ対策として、新しいプロトコルを使用してVPNを確立
2019/8	AWSサイト間VPNで証明書による認証のサポートを開始	IKE認証にデジタル証明書をサポート
2019/8	AWSサイト間VPNに、VPNトンネルのセキュリティアルゴリズムおよびタイマー設定の環境設定機能を追加	セキュリティアルゴリズムを制限することや、新規および既存のVPN接続のタイマー設定が可能
2019/12	Acceleratedサイト間VPNにより、VPNパフォーマンスを改善することを発表	AWS Global Acceleratorテクノロジを利用し、VPN接続のパフォーマンスを向上
2020/2	AWSサイト間VPNがAWS Transit Gatewayへの接続に対する証明書による認証のサポートを開始	セキュリティと柔軟性を高めるデジタル証明書を利用
2020/7	AWSサイト間VPNが作成時のリソースのタグ付けとリソースレベルのアクセス許可のサポートを開始	タグによるリソース管理がより柔軟、正確に

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

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
2020/8	AWS Site-to-Site VPNが新たにIpv6トラフィックをサポート	カスタマーゲートウェイデバイスとAWS内のリソース間におけるトラフィックにIpv6アドレス指定可能に
2020/8	AWSサイト間VPNが追加の暗号化、整合性、キー交換アルゴリズムのサポートを開始	より高いセキュリティを提供してデータを保護
2020/8	AWS Site-to-Site VPNがInternet Key Exchange (IKE)の開始をサポート	AWS側からIKEネゴシエーションを開始することが可能に
2020/10	AWSサイト間VPNが正常性に関する通知のサポートを開始	Personal Health Dashboardを介してトンネルの異常状態を通知
2021/3	AWSサイト間VPNがルート制限のサービスクォータを増やす	TGWにおけるルート制限を以下に拡張 オンプレミス→AWS: 1,000 AWS→オンプレミス: 5,000
2021/9	AWS Site-to-Site VPN、Download Configurationユーティリティの最新版をリリース	一部デバイスでIKEv2のパラメータを含むサンプルコンフィグがダウンロード可能に

https://aws.amazon.com/jp/about-aws/whats-new/2020/
https://aws.amazon.com/jp/about-aws/whats-new/2021/

参考：AWS Site-to-Site VPNの利用料金

料金体系：VGW接続

AWS Site-to-Site VPNの月額利用料＝

VPN接続ごとの時間課金 ＋ データ転送料

時間課金は、VPN接続をプロビジョニングして利用可能となっている各VPN接続IDに対してそれぞれ支払い。各IPsecトンネルのDown/Up状態は加味されない。課金停止にはVPN接続IDの削除が必要。

データ転送料は、EC2オンデマンド料金と同様で従量制。AWSからインターネットへのデータ転送(アウト)が課金対象となり、1 GB/月まで無料。東京リージョンでは、次の9.999 TB/月まで0.114USD/GBとなる。詳細は下記の料金説明ページを参照。

https://aws.amazon.com/jp/vpn/pricing/
https://aws.amazon.com/jp/ec2/pricing/on-demand/

料金体系：TGW接続

AWS Site-to-Site VPNの月額利用料＝

VPN接続ごとの時間課金 ＋ データ転送料

＋ VPNアタッチメント時間課金 ＋ TGWデータ処理料金

TGW接続を利用した場合、通常のVPN接続料金、データ転送料に加え、TGWに対するアタッチメント料、TGWデータ処理料金が必要となります。
VPNアタッチメント料は1つのアタッチメントに、2つのIPsecトンネル接続が含まれます。また、1つのVPN接続ごとにVPNアタッチメント時間課金が必要です。

https://aws.amazon.com/jp/vpn/pricing/
https://aws.amazon.com/jp/global-accelerator/pricing/

料金体系：TGW接続＋Acceleratedサイト間VPNオプション

AWS Site-to-Site VPNの月額利用料＝

VPN接続ごとの時間課金 ＋ データ転送料

＋ VPNアタッチメント時間課金 ＋ TGWデータ処理料金

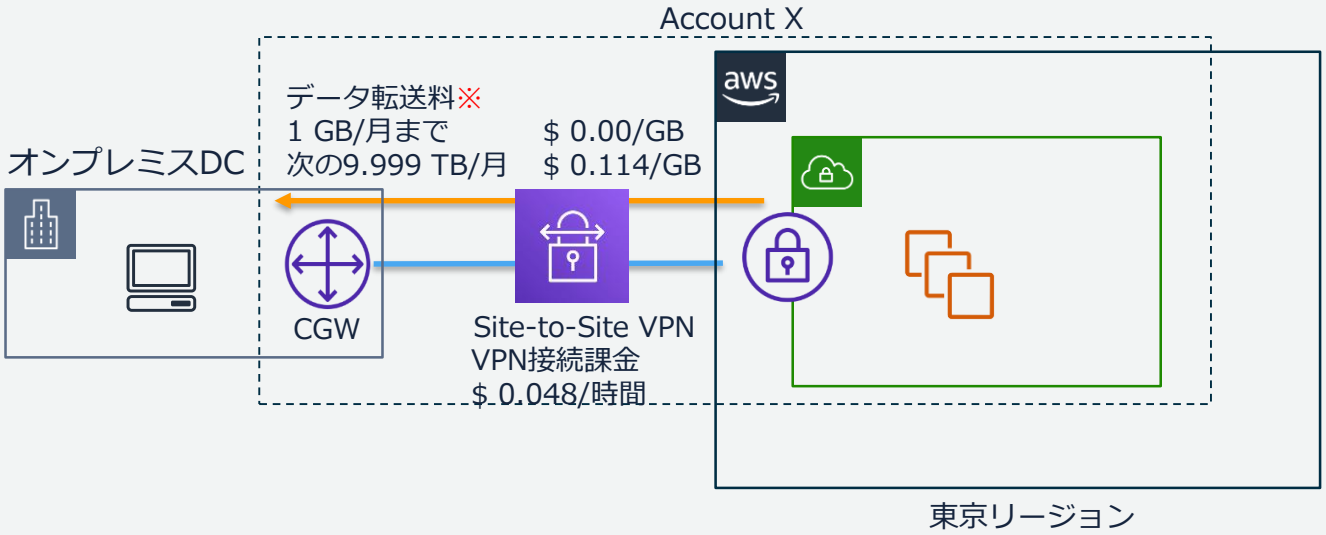
＋ Global Accelerator の時間料金 x 2 ＋ プレミアムデータ転送料

Acceleratedサイト間VPNオプションを利用した場合、通常のVPN接続料金、データ転送料、TGWに関連する課金に加え、Global Accelerator(GA)の時間課金が2つのIPsecトンネル分、GAのプレミアムデータ転送料が必要となります。

https://aws.amazon.com/jp/vpn/pricing/
https://aws.amazon.com/jp/transit-gateway/pricing/
https://aws.amazon.com/jp/global-accelerator/pricing/

料金　シナリオ１（例：同一AWSアカウントでVGW接続）

オンプレミスからAWS Site-to-Site VPNを利用し、1つのVPCにアクセスする例。

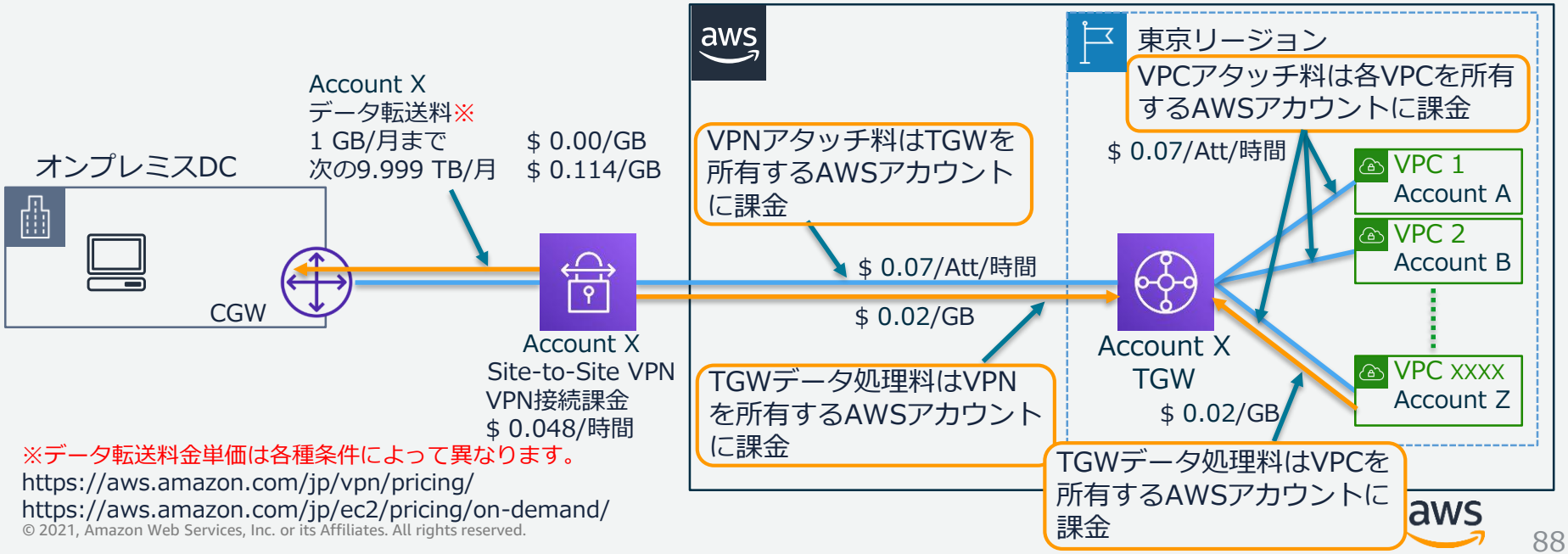


※データ転送料金単価は各種条件によって異なります。詳しくは以下をご参照ください。
https://aws.amazon.com/jp/vpn/pricing/
https://aws.amazon.com/jp/ec2/pricing/on-demand/

備考：オンプレミスからのインターネット接続の回線・サービスにかかる費用は別途発生します。

料金　シナリオ２（例：TGW接続において、TGWとVPCが別アカウント）

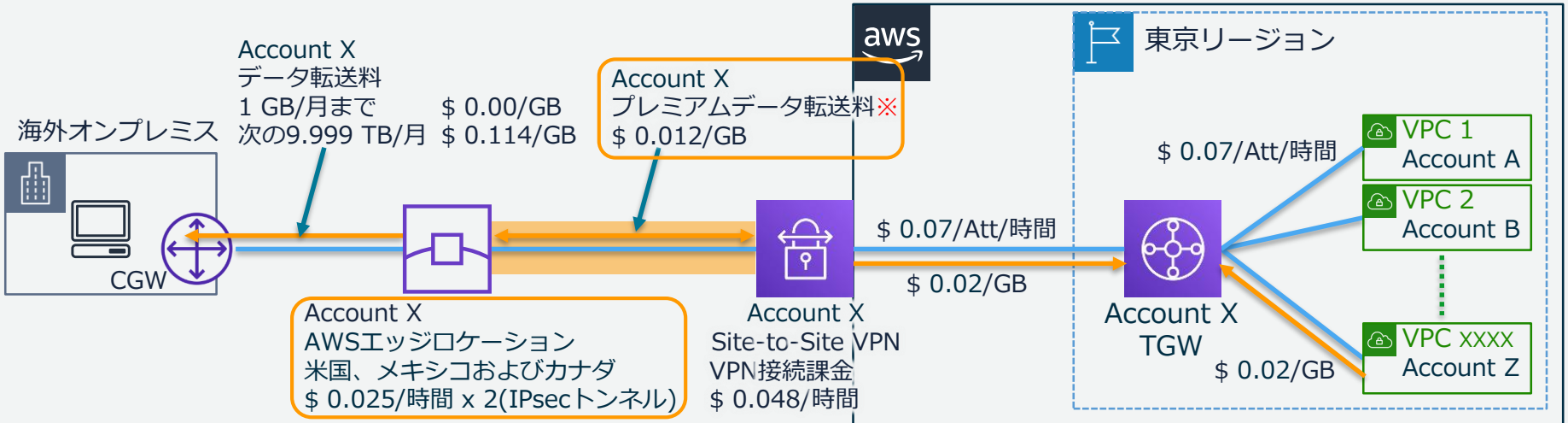
- VPN接続の時間課金、データ転送料金、TGWのVPNアタッチメント料金、VPNアタッチメントを通過するTGWデータ処理料はTGWを所有するアカウントに課金
- VPCアタッチ料金、VPCアタッチメントを通過するTGWのデータ処理料金はトラフィックをTGWに送信するVPCを所有するAWSアカウントに課金



※データ転送料金単価は各種条件によって異なります。
https://aws.amazon.com/jp/vpn/pricing/
https://aws.amazon.com/jp/ec2/pricing/on-demand/

料金　シナリオ３　（例：TGW接続＋Acceleratedサイト間VPNオプション）

- TGW料金に加え、AWS Global Accelerator時間あたり料金、プレミアムデータ転送料がVPN/TGWを所有するAWSアカウントに課金
- プレミアムデータ転送料金は、エッジロケーションを通る主要なデータ転送方向のみ課金



※プレミアムデータ転送料は主要な方向のトラフィック量に応じ課金され、
単価は通信先エッジロケーションによって異なります。
https://aws.amazon.com/jp/global-accelerator/pricing/

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

[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/

[AWS Hands-on for Beginners] Network編#2 Amazon VPC間およびAmazon VPCとオンプレミスのプライベートネットワーク接続
https://pages.awscloud.com/JAPAN-event-OE-Hands-on-for-Beginners-Network2-202009-reg-event-LP.html

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へお問い合わせください
https://aws.amazon.com/jp/premiumsupport/

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）
https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service

具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWS の日本語資料の場所「AWS 資料」で検索

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　　検索]

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