このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報についてはサービス別資料もしくはサービスのドキュメントをご確認ください

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

サービスカットシリーズ

Solutions Architect 菊地 信明
2020/2/19

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

自己紹介

名前：菊地 信明

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
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

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

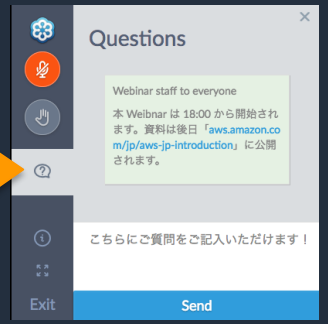
AWS Black Belt Online Seminar とは

「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2020年2月19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.

本日のアジェンダ

1. はじめに
2. 冗長化がなぜ必要か？
3. 冗長化の選択肢
4. より高い可用性を求めるためには
5. 安心して運用するために
6. まとめ

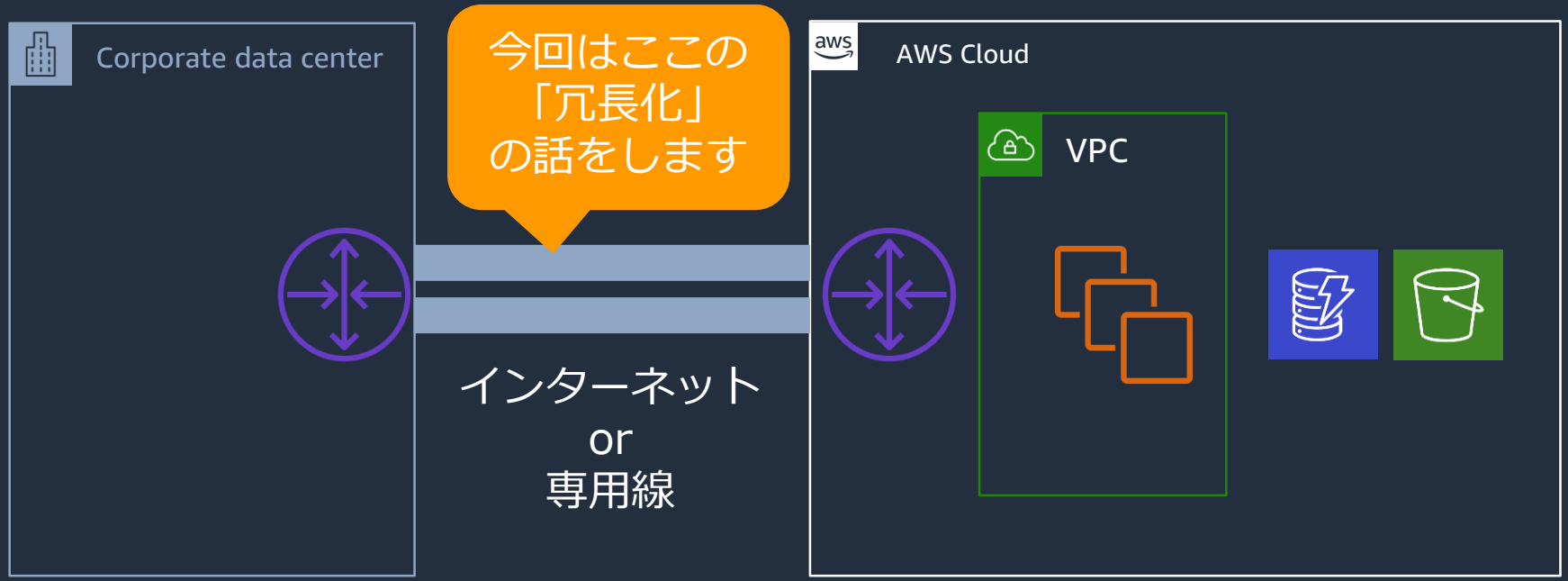
はじめに

AWSへのシフトが高まるにつれて、オンプレミスとAmazon VPC間の接続にはますます重要性が求められてきます。このセミナーでは、そのVPCとお客様のオンプレミス拠点間に信頼性の高い接続環境を構築する際の説明と、様々な要件を踏まえたAWSサービスをご利用いただく際のベストプラクティスやユースケースについてお伝えします。

一方で、オンプレミスとAWSを接続する範囲においては、これまで皆さんが培ってきたネットワーク技術をそのまま利用できる部分が多いのも事実です。これはクラウドと言えども、物理的なネットワーク機器を利用して接続している事に変わりがないからです。本セッションではAWSクラウド特有の事を中心としてお伝えいたしますが、一部、一般的なネットワーク設計に関する事も含まれておりますので、ご承知おきください。

本セッションの対象となる事

オンプレミス環境からAWSを利用するためには、ネットワークが必要
ネットワーク＝インターネット、または、専用線を指す



本セッションの対象外となる事

- ベンダー固有の情報

  登壇者が調査した範囲での知見を共有する目的で、ベンダー様固有の事象をお伝えする事があります。詳細な仕様については、ベンダー様の公開情報などでご確認ください。

- インターネット回線の冗長化

  接続要件がインターネット経由で許容できる場合には、一般的な考え方の元、インターネット接続を冗長化するなどして対応ください。

- 永続的なベストプラクティス

  記載のベストプラクティスは、本日時点で最善と考えられるアーキテクチャを基にしております。今後、発表されるサービスによりベストプラクティスが変更になる可能性もあります。設計を行う際には、最新の情報をAWS公式ドキュメントなどでご確認ください。

本日のアジェンダ

1. はじめに
2. 冗長化がなぜ必要か？
3. 冗長化の選択肢
4. より高い可用性を求めるためには
5. 安心して運用するために
6. まとめ


“Everything fails, all the time”
Werner Vogels
(CTO, Amazon.com)
すべてのものは、
いつでも壊れうる
ed the Turing tes

障害事例 1

米国
工事中の誤った掘削作業で
光ファイバーが切断

AWS内の影響

パケットドロップが

13のみ

障害事例２

ブラジル
ゴミ捨て場の火災で
空中に配線されていた
光ファイバーが焼失

AWS内の影響

お客様より申告無し

AWSによる可用性の取り組み

リージョン内ネットワークにおいても、責任共有モデルに基づき、
AWSが可用性を高める努力を常に実施

ダークファイバー網

低遅延と経路の
多様性に最適化

自社による運用

ファイバーの経路を
定常的に点検

位置のトラッキング

地理空間座標を
用いた配置の分析

キャパシティ拡張

光波長多重化を活用

なぜ冗長化が必要か？

AWS利用時においては、ほとんどの領域でお客様が物理環境の冗長性を意識する必要は無い。しかし、オンプレミス環境とAWSを接続する際には、明確に物理的な接続点が存在する。

- 物理的なリソースである以上、壊れる前提で考える
- メンテナンス等で一時的に利用できない時間帯が発生する

稼働しているサービスが突然停止することを許容していないのなら
通信の冗長化を行い、経路を自動的に切り替える環境を整える

クラウドに限った話ではない

冗長化が不必要なパターン

- 検証環境専用のネットワークで停止が許容される
- 他のネットワーク経由などの代替手段が整備されている
- ネットワークに対する明確な目標復旧時間が定義されていて、復旧時にデータが再送されれば問題ないシステム

あてはまらないなら、冗長化しましょう

本日のアジェンダ

1. はじめに
2. 冗長化がなぜ必要か？
3. 冗長化の選択肢
4. より高い可用性を求めるためには
5. 安心して運用するために
6. まとめ

冗長化の選択肢

十分な予算があれば、メイン回線と同等の回線を複数用意するのが理想的。
どれくらいの投資ができるか？は「そのネットワークが担うシステムが停止した場合に、どれくらいの損失があるのか？」からバランスを見て判断する。

AWSにおける代表的な冗長化を大きく分類すると以下

1. Direct Connectを複数回線接続
   →一貫性のある通信品質、安定した広帯域が必要な場合

2. メイン回線をDirect Connect／バックアップ回線をVPN接続
   →障害時には特性が違う回線利用を許容できる場合

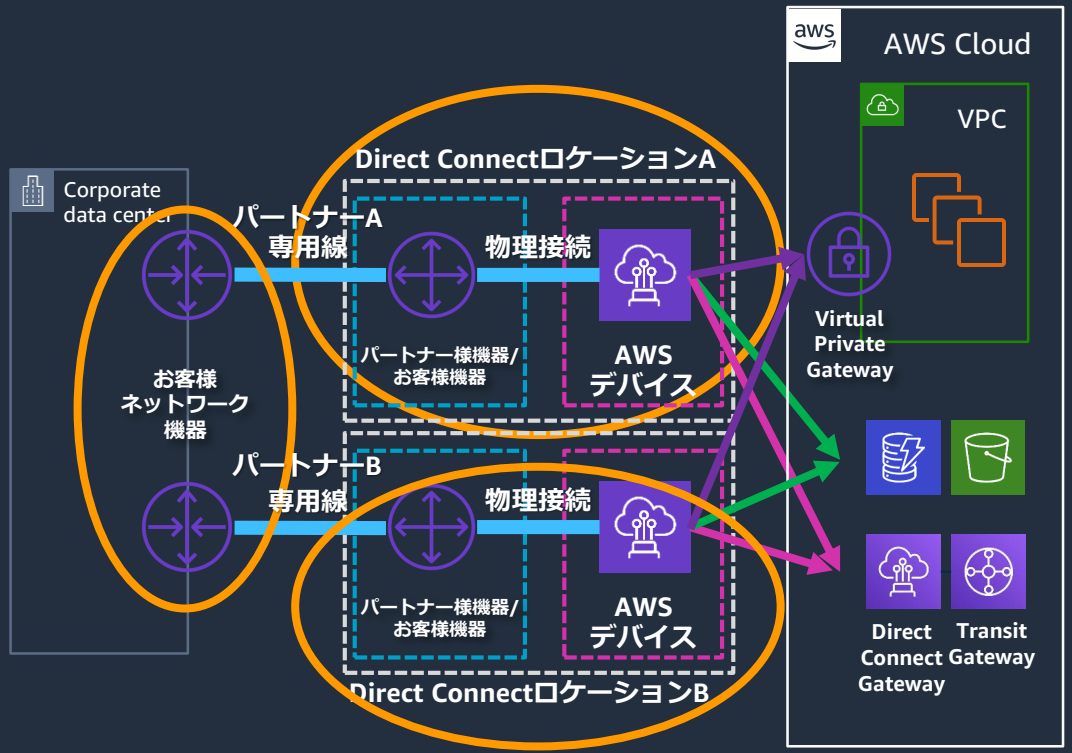
3. インターネット回線を冗長化（本セッションの対象外）
   →閉域網を必要とせず、通信品質の劣化が許容できる場合

冗長化方法

複数のDirect Connectによる冗長化

複数のDirect Connectによる冗長化

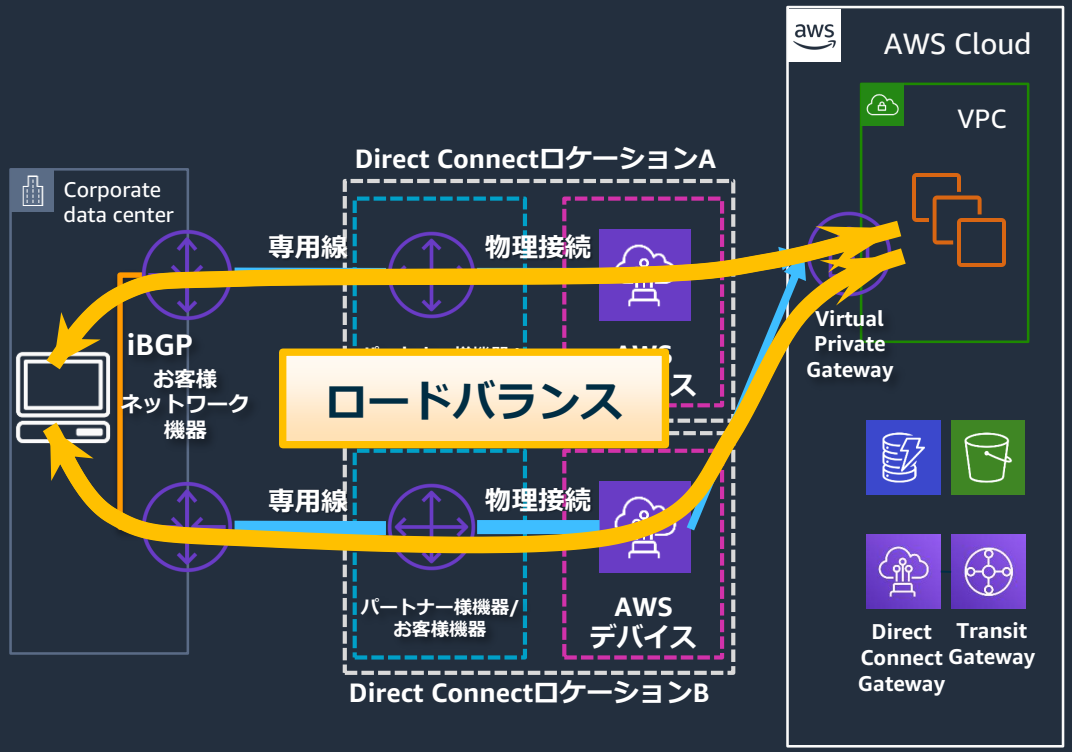
エンタープライズのユースケースで多く取られる方法



- 異なるロケーションに接続
- Active-Active、Active-Standbyをお客様ルーターにて制御
- 異なるパートナー経由で接続して、キャリヤ冗長化を実現する事も可能
- 十分なテストを行う事がとても重要

複数のDirect Connectによる冗長化（Active-Active）

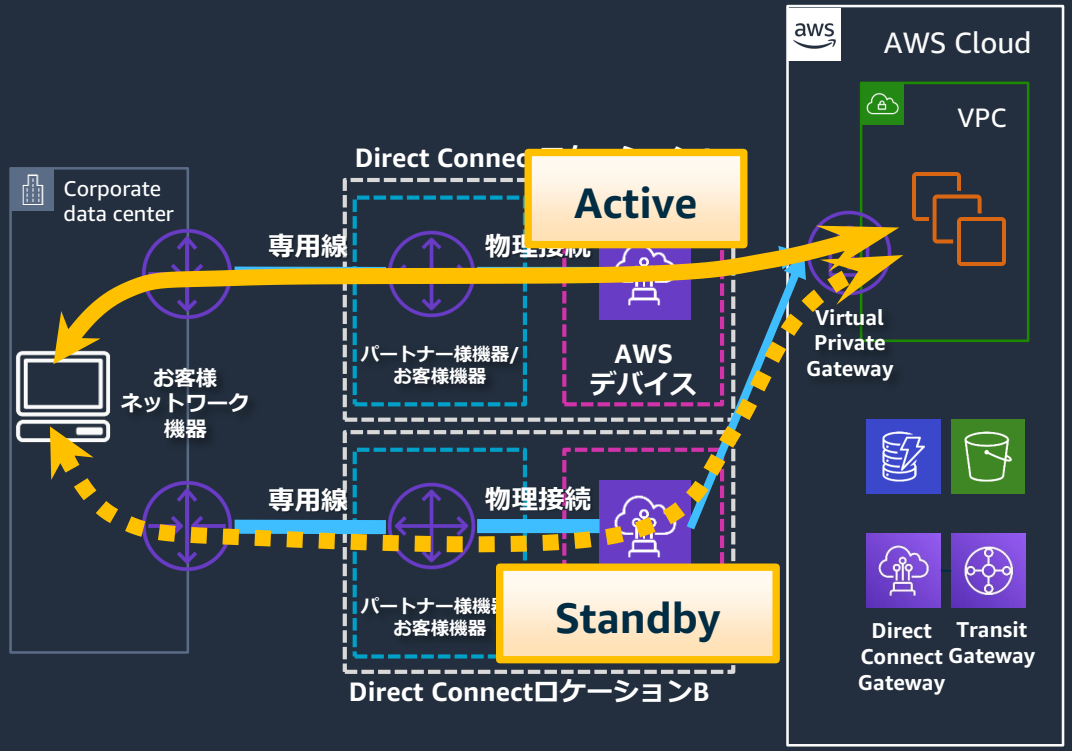
何も設定しなければ、AWSからオンプレミス方向はActive-Activeとなる



- AWSからオンプレミスへ向けたトラフィックはロードバランシングされる
- トラフィックが均等にバランスされない場合もある
- オンプレミスからAWSへ向けたトラフィックは、お客様ネットワーク機器の設定によるので、非対称通信もありえる
- お客様ルーター間はiBGPで経路交換し、ベストパスを選択する

複数のDirect Connectによる冗長化（Active-Standby）

トラフィックを片寄する要件があれば、お客様ネットワーク機器で設定



- Direct Connectによる設定項目は無い
- お客様ネットワーク機器にてBGPのアトリビュートを指定

  通信方向毎に

  オンプレミス→AWS：Local Preference

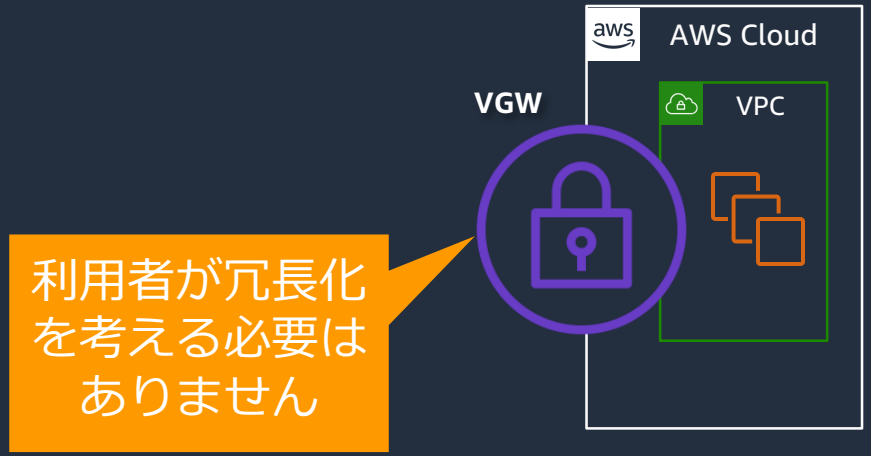
  AWS→オンプレミス：AS Path Prepend

  でそれぞれ指定
- ネットワーク機器によっては、これらの指定に未対応の場合もある
- 現時点ではMEDによる指定で優先制御ができるが、サポート対象では無い

Virtual Private Gateway (VGW) について

オンプレミスとVPC間をつなぐ仮想ルーターの役目を持つ

構成図上は1つのアイコンで示されるが、内部的に冗長化されているため、利用者にて冗長化を意識する必要無い



- 現在のところ、VGWのルートテーブルを利用者が参照する機能は無い
- VGWが持つ経路を確認したい場合は、サポートケースで問い合わせ可能（有償のAWSサポートへの加入が必要、サポートが調査時の経路のみ提供可、過去の経路は確認不可）

Tips: Virtual Private Gateway が持つ経路について

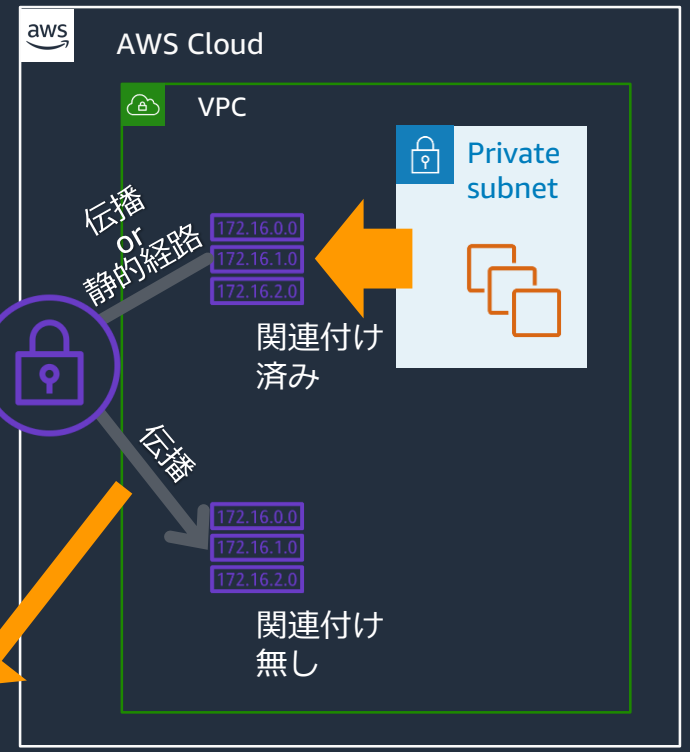
VGWが持つ経路を管理する方法

いずれのサブネットにも関連付けられていないルートテーブルに対し「VGWが持っている経路」を自動的に伝播させることが可能

以下の様なコマンド実行結果を定期的に取得する事で、過去のルートテーブル情報を保存する方法もある

aws ec2 describe-route-tables --route-table-ids

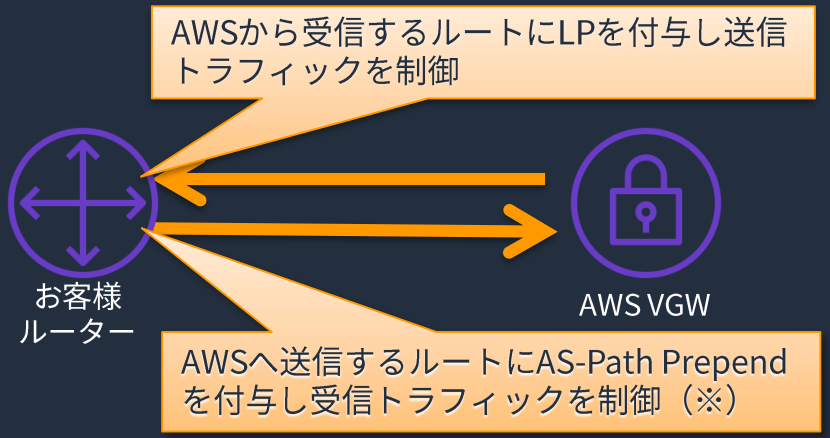
（VPCのCIDRは排除できず、localは除外して考える）

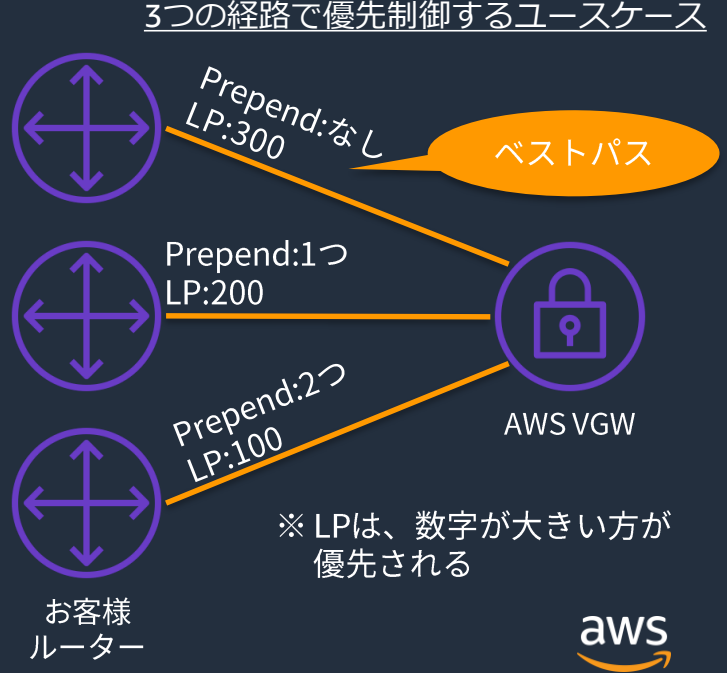


BGPパス属性を用いた経路制御

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

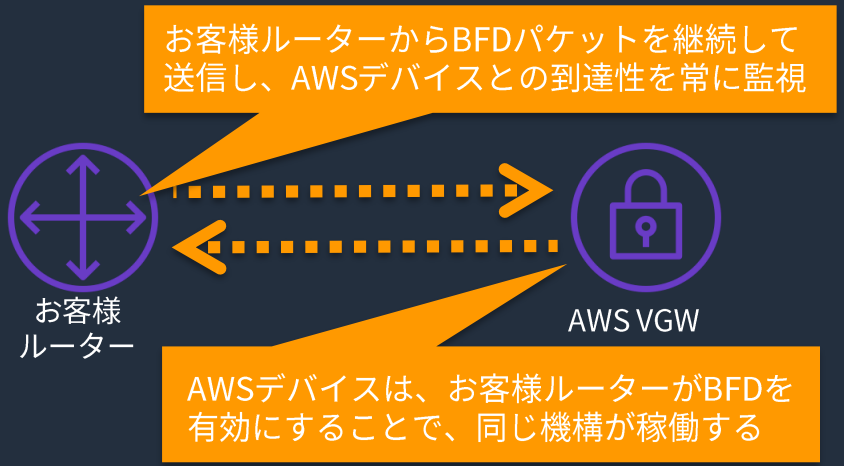
※ LPは、数字が大きい方が優先される

- ルーティングポリシーと BGP コミュニティ
https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/routing-and-bgp.html

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、機能が有効化される
- 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)で、約1秒程度でダウンを検知、インターフェイスを停止する



- 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/

Tips: BFDとGraceful Restartの併用について

一部のルーターOSでは、Graceful Restart*の機能がデフォルトで有効になっている

BFDとGraceful Restartを併用すると、意図した障害検出が出来ず、切り替えに時間がかかるので、無効にしておくことを強く推奨

*Graceful Restart: ルーティングプログラムの再起動などによりネットワークから経路が消えた場合、通信の停止時間を短くするために利用する機能

-参考 Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/unicast/config/cisco_nexus7000_unicast_routing_config_guide_8x/configuring_advanced_bgp.html

====

Configuring a Graceful Restart

DETAILED STEPS

Step 3

switch(config-router)# graceful-restart

Enables a graceful restart and the graceful restart helper functionality. This command is enabled by default.

====

障害時の経路切替時間の短縮：BFD非対応ルーター

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
- Cisco社の公開情報では以下の記載がある
  20秒以下などの極端に短い時間とするとBGPピアが不安定になる可能性がある
- 安定化の為には、Holdtimeを20～30秒程度とすることが適切と考える

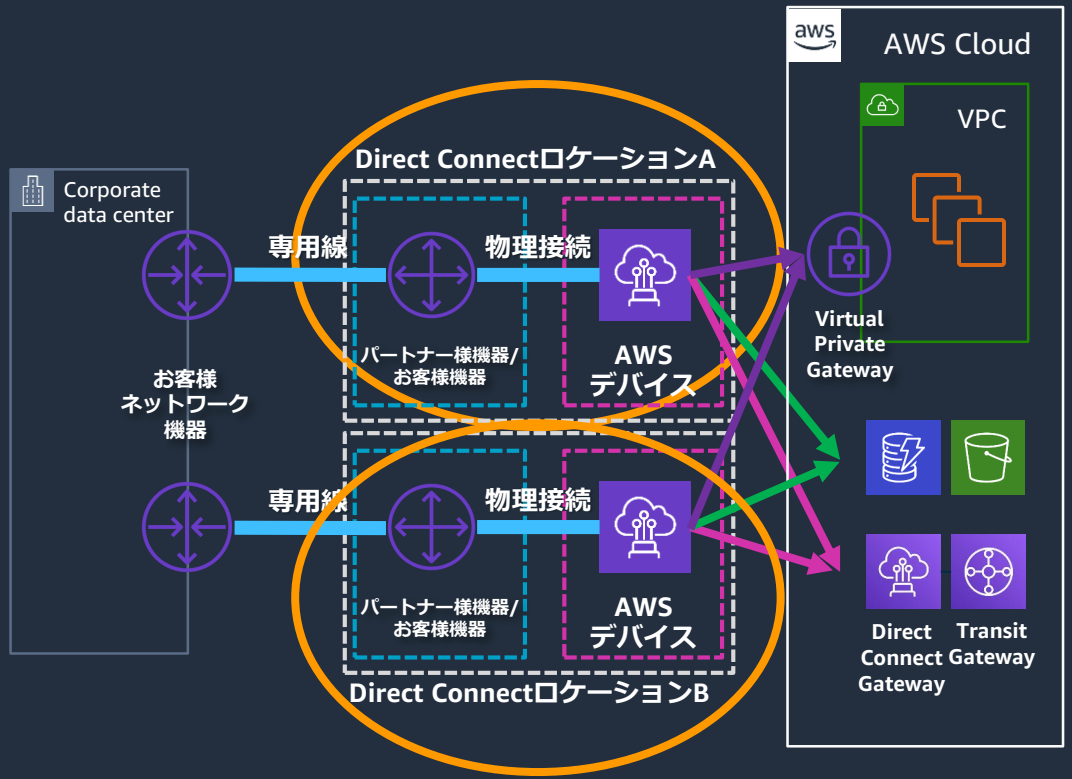
- 参考 Cisco IOS IP Routing: BGP Command Reference (AWS外部サイト)
BGP Commands: neighbor timers through show bgp nsap summary
https://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/command/reference/irg_book/irg_bgp4.html
"neighbor timers" より抜粋
====
Usage Guidelines
When configuring the holdtime argument for a value of less than twenty seconds, the following warning is displayed:
% Warning: A hold time of less than 20 seconds increases the chances of peer flapping
====

冗長化方法

旧来の冗長化方法

複数のDirect Connectによる冗長化(再掲：現在の推奨)

Direct Connectロケーションを分けてAWSへ接続



- 異なるロケーションに接続
  - Active-Active、Active-Standbyをお客様ルーターにて制御
  - 異なるパートナー経由で接続して、キャリヤ冗長化を実現する事も可能
  - 十分なテストを行う事がとても重要

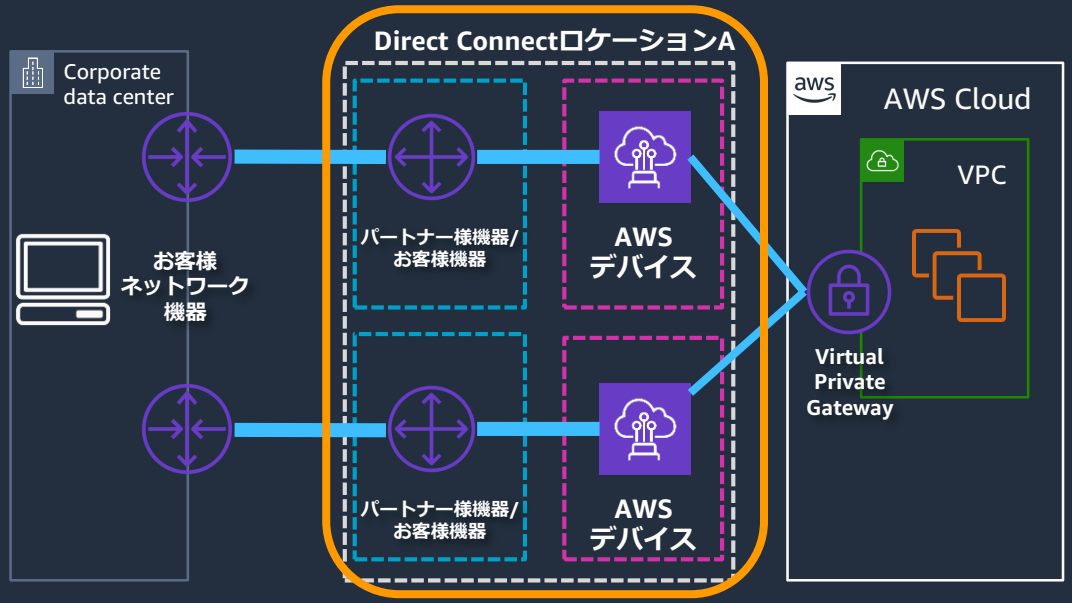
旧来の冗長化方式（過去の経緯）

過去には東京リージョンにDirect Connectロケーションが1つしか存在しない時期もあり、同一ロケーション内に複数の接続を推奨している時期もありました。

現在では東京近郊に2つ目のロケーションが追加されたため、より高い回復性を実現する手段として、ロケーションを分ける事をベストプラクティスとしています。

旧来の冗長化方式：同一ロケーションにおける冗長化

現在では非推奨の「同一ロケーションによる冗長化」の場合、注意が必要。
課題：特定ロケーションの障害により、すべての通信が停止



- マネージメントコンソールの”Direct Connect Resiliency Toolkit “で接続ウィザードを利用すると、適切な冗長性を達成するリクエストを作成可能
- 前述のロケーションを分けた接続へ移行する事を推奨
- 同一ロケーション内冗長の構成については、AWSデバイスが別となっている事を確認（次ページ）

- Direct Connect Resiliency Toolkit で使用を開始する方法
https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/resiliency_toolkit.html

旧来の冗長化方式：AWSデバイスの確認について

同一のロケーションで二つのDirect Connectを利用した冗長化を行っている場合、二つのConnectionが「別のAWSデバイス」にアサインされている事をマネージメントコンソールで確認

1つ目の仮想インターフェイスID

2つ目の仮想インターフェイスID

旧来の冗長化方式：AWSデバイスの確認について(続き)

AWS デバイス項目に記載されてたIDを確認
前半はロケーション名のキーワードが表記され、続くキーワードはランダム

1つ目の仮想インターフェイス

AWS デバイス
EqTY2-2xviw1vk3rhgl

2つ目の仮想インターフェイス

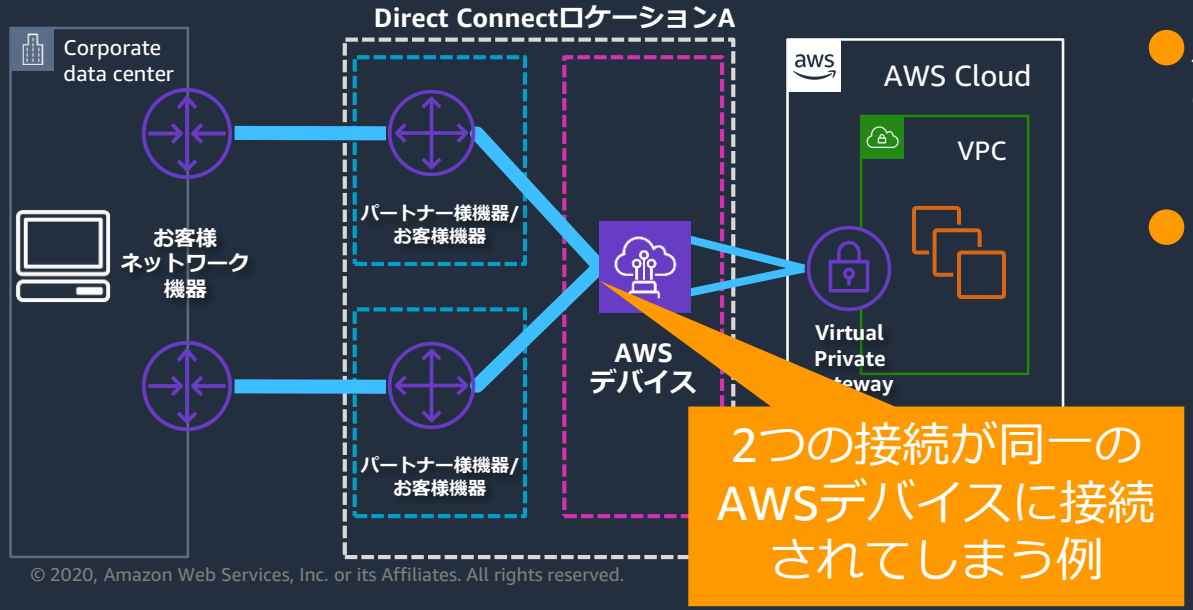
AWS デバイス
EqTY2-qu3riajamatx

二つを比較して異なっていれば別のAWSデバイスに収容されている

注意点：旧来の冗長化方式

通常は、同一ロケーションにおいて複数のDirect Connect接続をリクエストすると、自動的に別のAWSデバイスへアサインされる

特定の条件で同じAWSデバイスへアサイン・接続される事例もあるので、前述のAWSデバイスIDを確認し、重複していた場合には以下の対応を



- パートナー経由の共有VIF、Sub1/10-gのホスト接続の場合
  - パートナー様窓口へ確認
- コネクションを自社保有で、直接接続を利用している場合
  - AWSサポートへ確認
    必要に応じ、新たな接続をリクエストの上、別のAWSデバイスにアサインされたことを確認の上、改めてクロスコネクト依頼
    （古い接続は削除）

注意点：旧来の冗長化方式(続き)

結果としてAWSデバイスが重複してしまう例：

1. 期間を空けてリクエスト
   開発期間中に最初のリクエスト、本番リリース時に2つ目のリクエストをした場合、それらを冗長化目的と認識できず、同一AWSデバイスにアサイン

2. 複数のペアを同時にリクエスト
   本番用環境に2本、開発環境用に1本/2本の合計3～4つの接続をリクエストした場合、正しいペアでお客様ルーターへ接続しないと、同一AWSデバイスへアサインされたペアで利用してしまう可能性がある

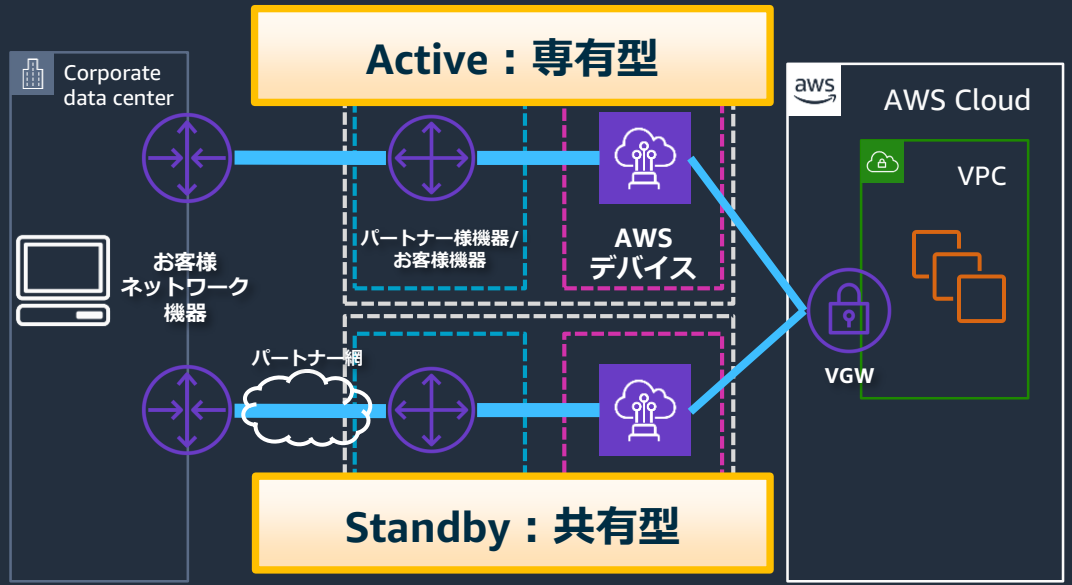
3. 同一ロケーションで異なるパートナー様からDirect Connectを調達
   パートナー様間では冗長化の調整しないので、事前に冗長化目的であることを相談

冗長化方法

コスト抑制条件に適用した冗長化

コスト抑制条件に適用した冗長化：異なるサービスを併用

基本的には、同一品質の回線を利用する事が理想だが、コスト抑制のため、通常利用しないStandby回線には、共有型を併用する事も可能



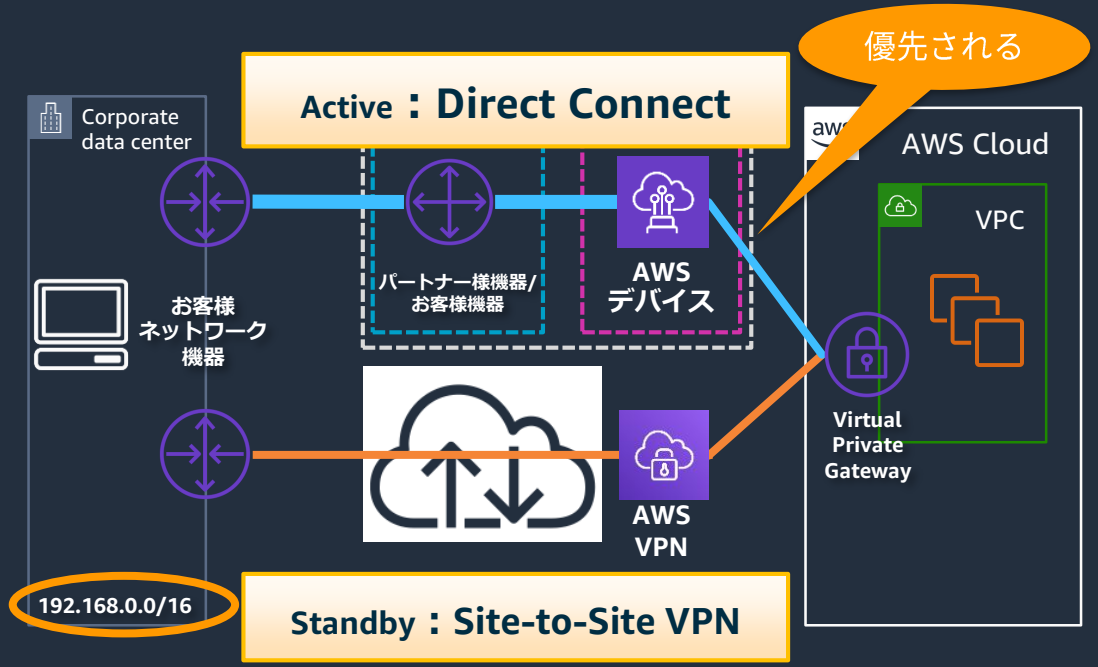
- Standbyへ切り替わり時には、通信品質の劣化を許容することも必要
- パートナーのサービスによっては、意図する経路設計が出来ない事もあるので、事前に確認が必要

  例： お客様ルーターから広報される経路が集約される、経路数の上限がある

  デフォルトルートのみ広報可能

コスト抑制条件に適用した冗長化：VPN接続を併用

Direct Connectのバックアップとして、AWS Site-to-Site VPNを利用し、同じVGWに接続する



- オンプレミスのCIDRとして同じプレフィックスを指定した場合、必ずDirect Connect経由が優先される
- BGPのASパス属性でVPN側を優先したとしても、AWS→オンプレミス方向の通信は、必ずDirect Connectが優先される
- メンテナンス時などVPN側を優先したい場合には、経路を分割して広報する

  例：192.168.0.0/16

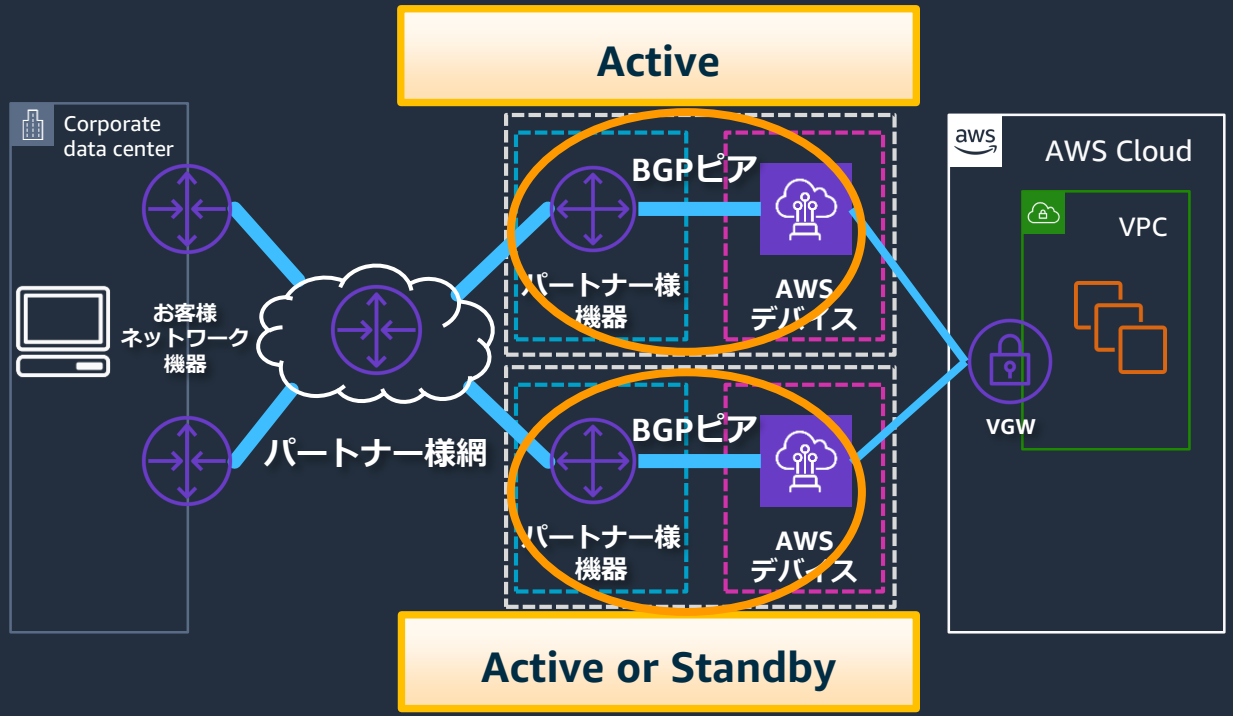
  →192.168.0.0/17
  →192.168.128.0/17

冗長化方法

パートナー網を経由した冗長化

パートナー網経由の冗長化

広域イーサ網を経由して効率的にAWSへ閉域網接続を行う場合、パートナーの設備が冗長化を行っている場合がある



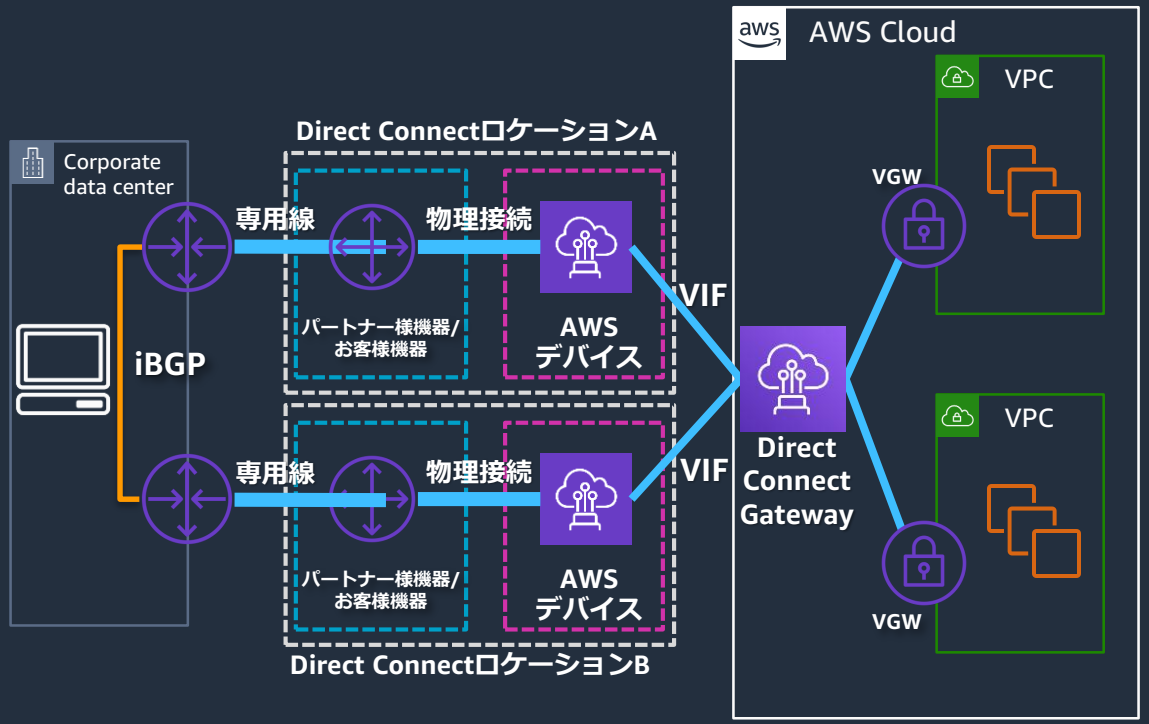
- お客様ネットワーク機器は、パートナー様網の仕様により、L2、L3による接続を行う
- L3接続の場合、AWSデバイスとのBGPピアはパートナー様機器が行う
- 冗長化の設計についてはパートナー様の仕様によるところが大きいので、詳細はパートナー様窓口へ確認ください

冗長化方法

Direct Connect Gatewayに対する冗長化

Direct Connect Gateway(DXGW)に対する冗長化

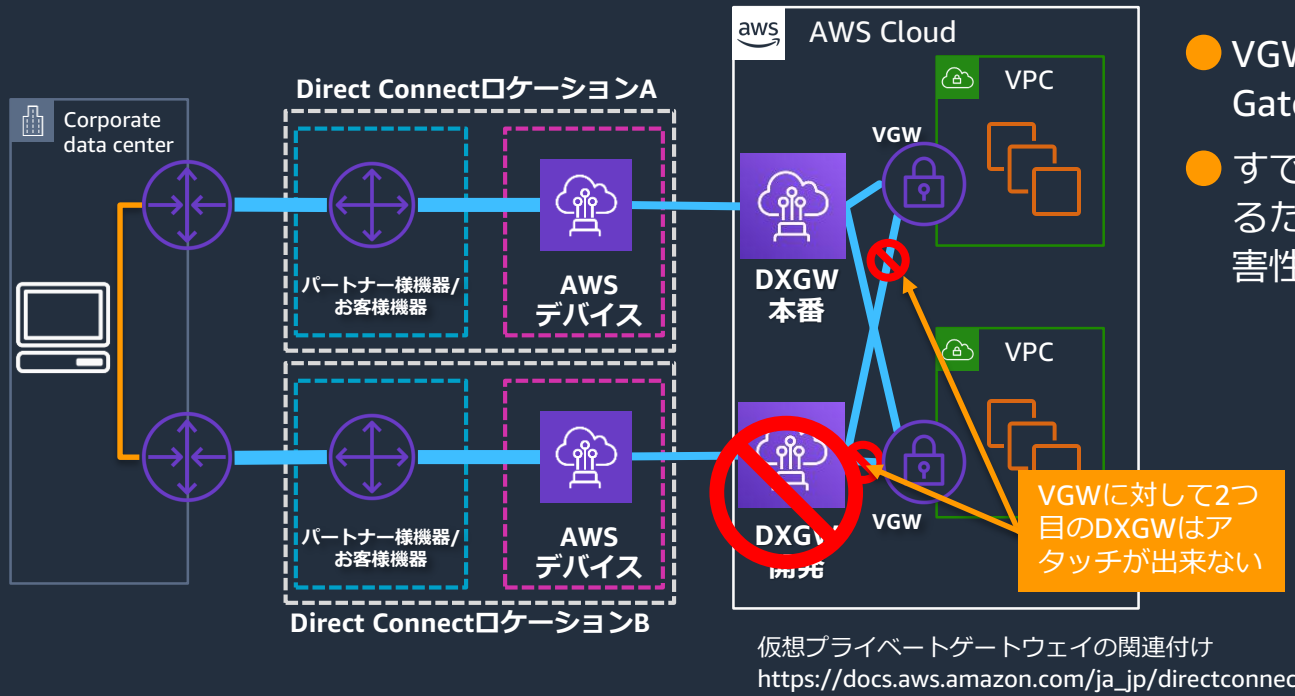
基本的にはDirect Connectで直接VGWに接続する場合と同様



- Direct Connect Gatewayは単一のリソースに見えるが内部で冗長化
- 構成上は1ホップ増えるように見えるが、オーバーヘッドの心配は不要
- 同時にアタッチ可能なVIFは30
  (冗長化しても15拠点が収容可能)

Direct Connect Gateway(DXGW)に対する冗長化：注意点

本番と開発のリソースを分ける観点から、DXGWを分けたい要望があるが、
VGWアタッチの制約で不可



- VGWは二つ目のDirect Connect Gatewayにアタッチできません
- すでに内部的に冗長化されているため、DXGWを分けても耐障害性の向上は期待できない

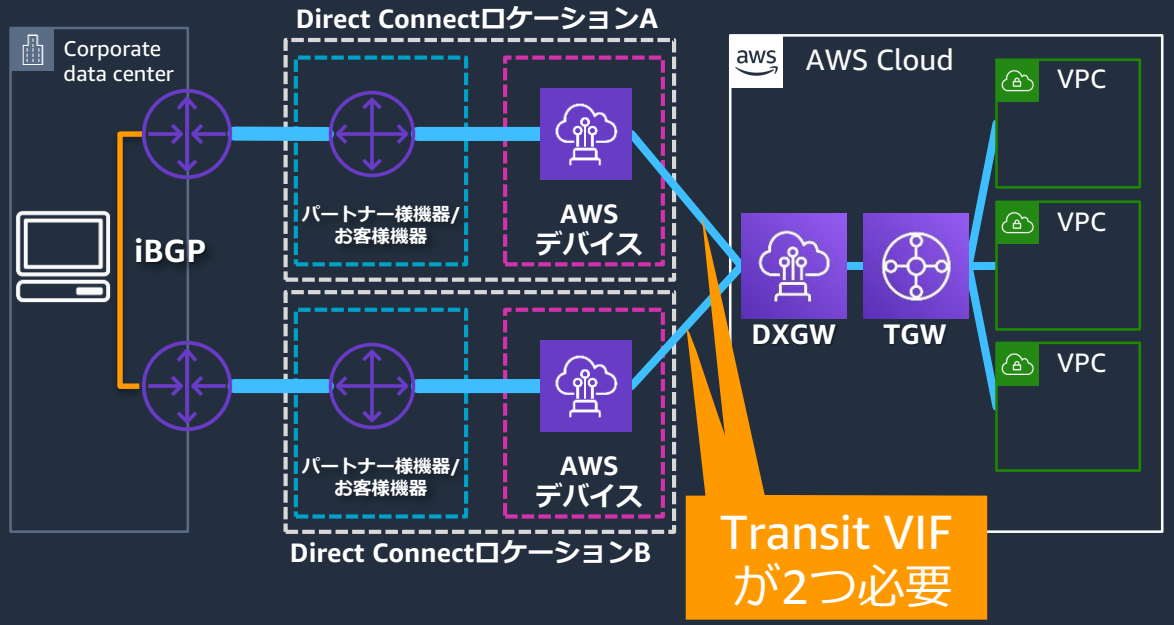
仮想プライベートゲートウェイの関連付け
https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/virtualgateways.html

冗長化方法

Transit Gatewayに対する冗長化

Transit Gateway(TGW)に対する冗長化

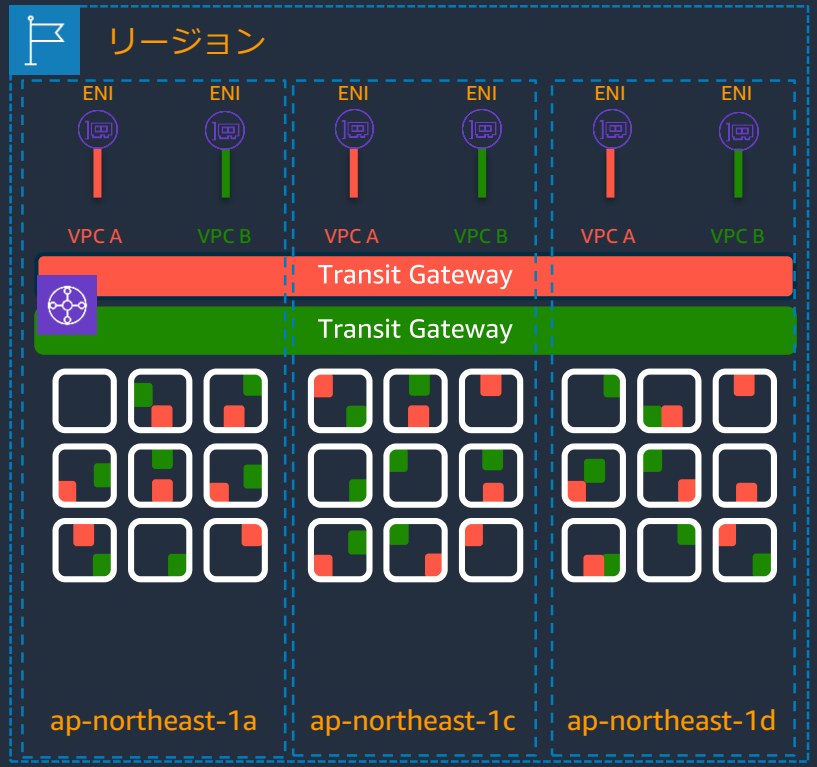
ロケーション冗長は、Direct Connectで直接VGWに接続する場合と同様
バックアップ用にもTransit VIFが必要（特性の異なる共有型サービス利用不可）



- DXGWから広報されるAWS側経路はDXGWの”許可されたプレフィックス”に登録のCIDRが両方のVIFに対して広報される
- DXGWとTGWは内部的に冗長化されているため、考慮不要

TGWを分ける必要が無い理由：HyperPlane

TGWはHyperPlane技術を使って、大量のリソースを仮想的に分割して提供



アタッチメント

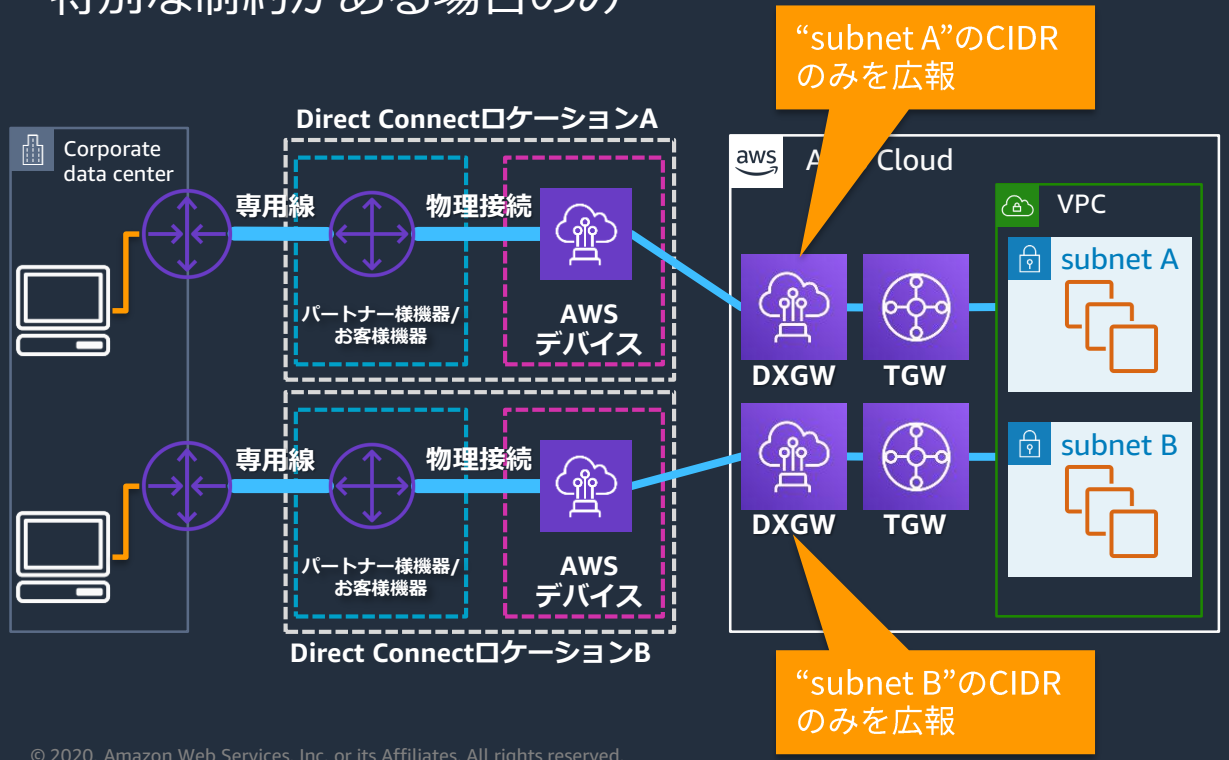
- AZごとに1つのENI(Elastic Network Interface)
  ➡つまりAZ内の1つのサブネットにのみアタッチ可能
- AZごとの高信頼性
- ネットワーク容量のシャーディングによる確保
- 数十マイクロ秒の低レイテンシー

AWS HyperPlane

- 水平方向に拡張可能なステートマネジメント
- Tbpsを超えるマルチテナンシーのサポート
- NLB、NAT Gateway、Amazon EFSのサポート、さらにTransit Gatewayをサポート

Tips: TGWを分ける必要がある場合

TGWを分ける事で、利用するVPC CIDRごとに使う物理線を分割可能
特別な制約がある場合のみ



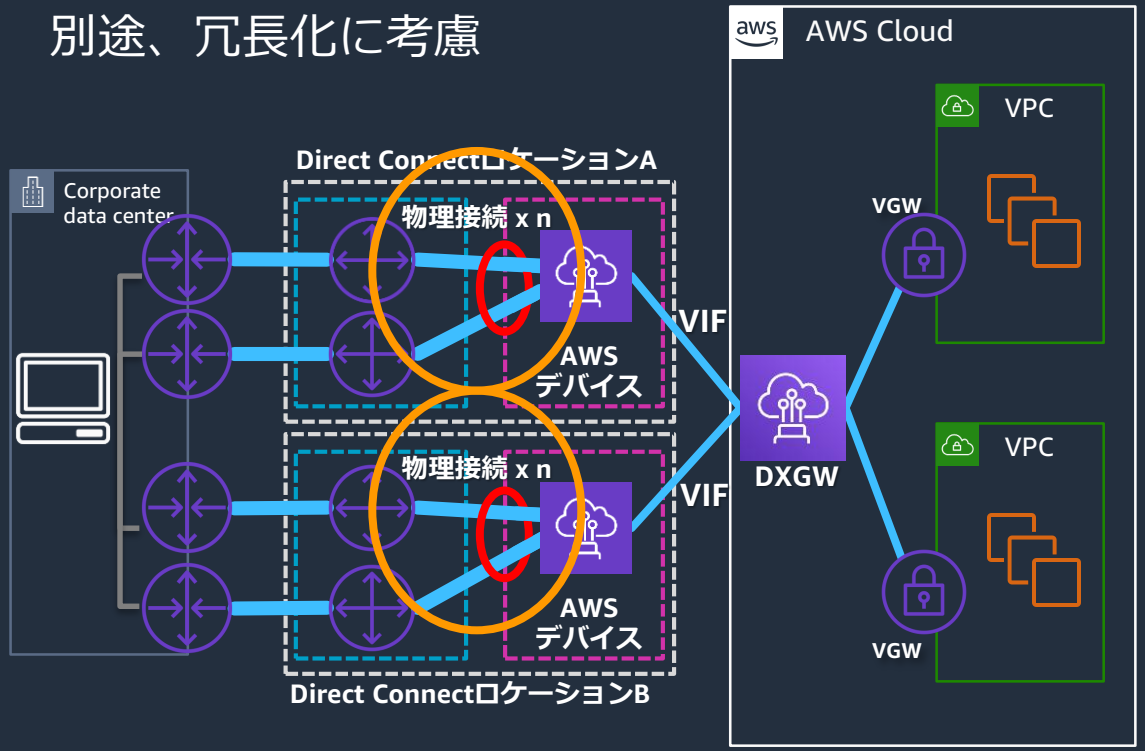
- パートナーのサービスにおいて、1つしかVPCが利用できない場合、かつ、複数の接続がお互いに干渉しない要件をクリアする場合
- 別途冗長化を検討

帯域増強方法

LAGによる広帯域確保

LAG(Link Aggregation)による高帯域確保

複数の接続を1つの接続に集約する技術
別途、冗長化に考慮



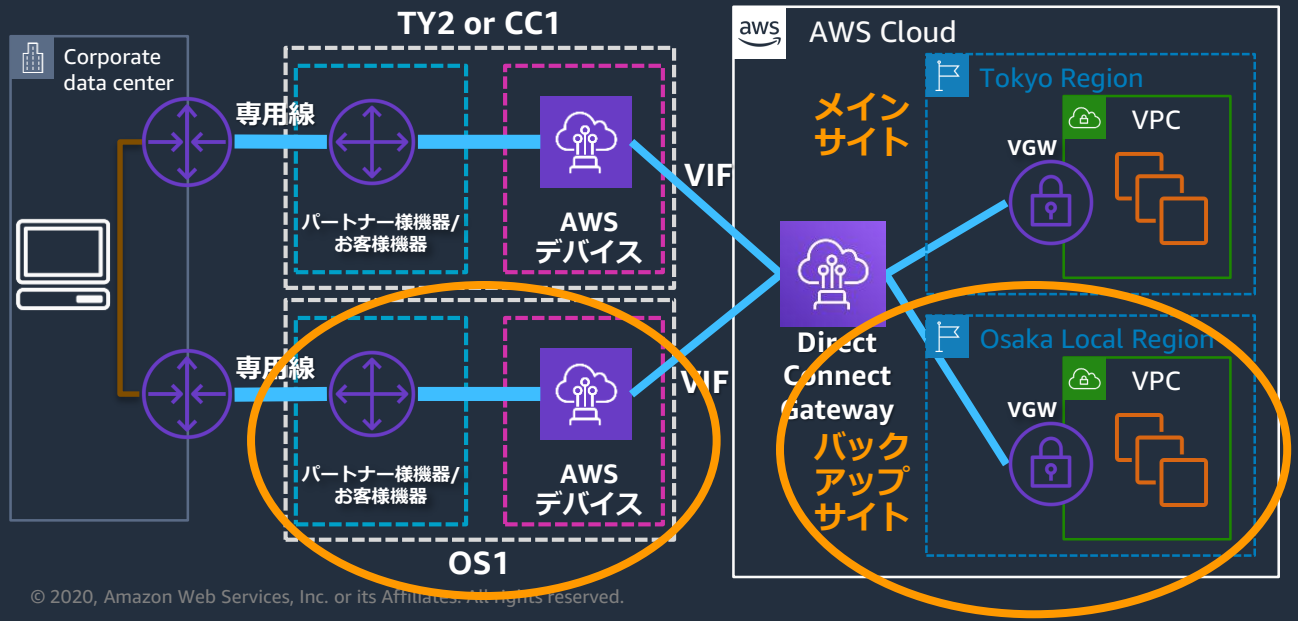
- 標準で1つのLAGで4までの接続を集約
  1 Gbps x 4 = 4 Gbps
  10 Gbps x 4 = 40 Gbps
- マルチシャーシLAGはサポートされず、同一AWSデバイスに収容された接続のみで構成可能
- 冗長化用の接続は、別のロケーションに配置する
- 費用要件から2つの接続のみが利用可能な場合、LAGよりもロケーション冗長を優先する事を推奨

本日のアジェンダ

1. はじめに
2. 冗長化がなぜ必要か？
3. 冗長化の選択肢
4. より高い可用性を求めるためには
5. 安心して運用するために
6. まとめ

より高い可用性を求めるためには：マルチリージョン冗長

大阪ローカルリージョンにバックアップサイトを構築、これに加えて
大阪にあるEquinix OS1と東京にあるEquinix TY2もしくは@Tokyo CC1に
Direct Connectロケーションを冗長化することで、可用性が増す



- グローバルリソースのDirect Connect Gatewayを利用して、東京、大阪ローカルリージョンへ同時に接続
- オンプレミスが東京だった場合、大阪までの専用線接続が高価になりがち
  キャリヤの広域イーサ網などでコスト効率を検討

大阪フルリージョンへ

Amazon Web Services ブログ

AWS 大阪ローカルリージョンをフルリージョンへ拡張中

by Harunobu Kameda | on 22 JAN 2020 | in News | Permalink | Share

大阪でのサービスに対するお客様からの大きなご要望にお応えし、大阪のローカルリージョンが 2021 年初頭までに 3 つのアベイラビリティーゾーンを持つ完全な AWS リージョンに拡大することになりました。 他のすべての AWS リージョンと同様、アベイラビリティーゾーンはそれぞれ独自の電源、冷却システム、物理的セキュリティにより分離されます。また、可用性に影響を与える単一のイベントのリスクを大幅に減らすため離れて配置されますが、高可用性アプリケーションの低レイテンシーは維持されます。

AWS はインフラストラクチャを継続的に拡張しており、お客様が拡大できる十分な能力と、可用性と堅牢性を高めるためのさまざまなシステムを設計するために必要なツールを提供しています。AWS は現在、22 のリージョンと 69 のアベイラビリティーゾーンをグローバルに運用しています。

2011 年 3 月に、2 つのアベイラビリティーゾーンを持つ 5 番目の AWS リージョンとして AWS 東京リージョンを立ち上げました。その後、2012 年に 3 番目の東京のアベイラビリティーゾーン、2018 年に 4 番目のアベイラビリティゾーンを立ち上げました。

2018 年 2 月には大阪ローカルリージョンを立ち上げました。単一のデータセンターに含まれるインフラストラクチャは分離されかつ対障害性のある設計で、既存の AWS リージョンを補完する新しいリージョン構成となりました。東京リージョンから 400 キロ離れた大阪ローカルリージョンは、東京リージョンだけでは難しい災害対策の提供を目指して、国内のさまざまな場所で必要とされるアプリケーションを持つお客様をサポートしてきました。

AWS 大阪ローカルリージョンをフルリージョンへ拡張中
https://aws.amazon.com/jp/blogs/news/in-the-works-aws-osaka-local-region-expansion-to-full-region/

より高い可用性を求めるためには：大阪ロケーション

東京全域が被災しても、大阪ロケーションに接続されたDirect Connectは独立したバックボーンに接続されているため、継続利用可能

ディザスタリカバリーのための接続ポイントとして活用

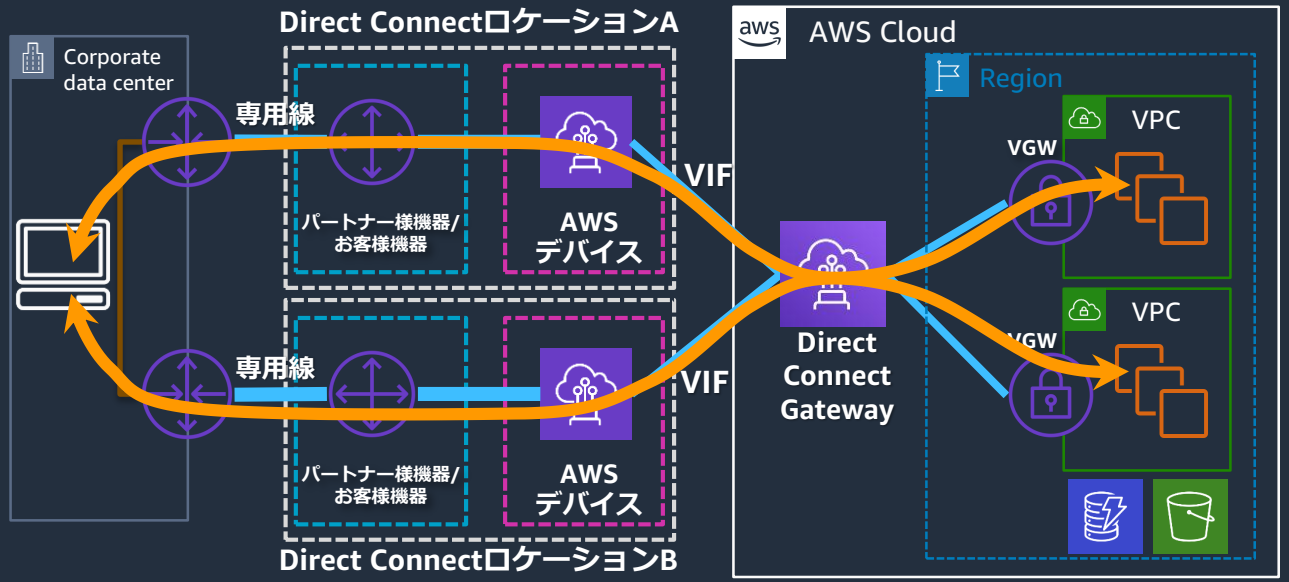
AWS Global Infrastructure Components
https://www.infrastructure.aws/

本日のアジェンダ

1. はじめに
2. 冗長化がなぜ必要か？
3. 冗長化の選択肢
4. より高い可用性を求めるためには
5. 安心して運用するために
6. まとめ

安心して運用するために

【質問】 いつ問題が発生してもシステムが自律的に問題を回避し、影響を最小限に留めるための仕組みは出来ていますか？



AWS Well-Architected Frameworkで点検を！

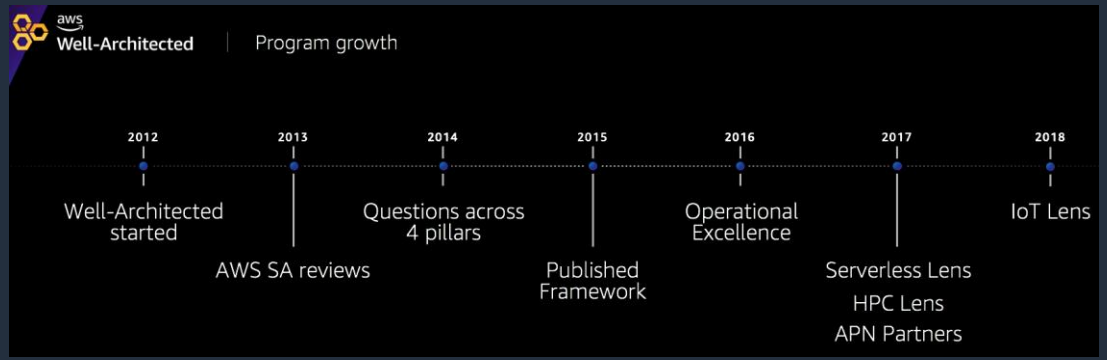
ベストプラクティス

AWS Well-Architected Framework

AWS Well-Architected (W-A) Framework とは？

クラウド設計・運用のベストプラクティス集

- AWSのソリューションアーキテクト(SA)とお客様が長年にわたり数多くの経験から作り上げたもの
- AWSを利用するお客様の成長と共に、W-Aも常に進化し続けている



W-Aホワイトペーパー

W-Aを日本語で説明、PDFまたはWeb形式でご覧いただけます

障害を予想する

障害の考えられる原因を除去または軽減できるように、原因を特定する「プレモータム」演習を実施します。障害シナリオをテストし、その影響に関する理解を検証します。対応手順をテストし、手順が効果的で、チームが手順の実行を十分に理解していることを確認します。定期的な**ゲームデー**を計画し、ワークロードと、シミュレートされたイベントに対するチームの応答をテストします。

AWS Well-Architected
https://aws.amazon.com/jp/architecture/well-architected/

ネットワークにおけるW-A ゲームデー例：

ネットワークに対して発生するイベントを予測する

実際にそれを発生させた際に、システムが影響を受けるか？を検討する

リスクがあるなら、冗長化設計に課題がある ➡ 課題を整理し改善

ゲームデーを実施

検証環境が用意できれば理想

可能なら本番環境でメンテナンス時間を設けて実施

➡ システム全体を確認、問題が発生したら見直し、サイクルを継続

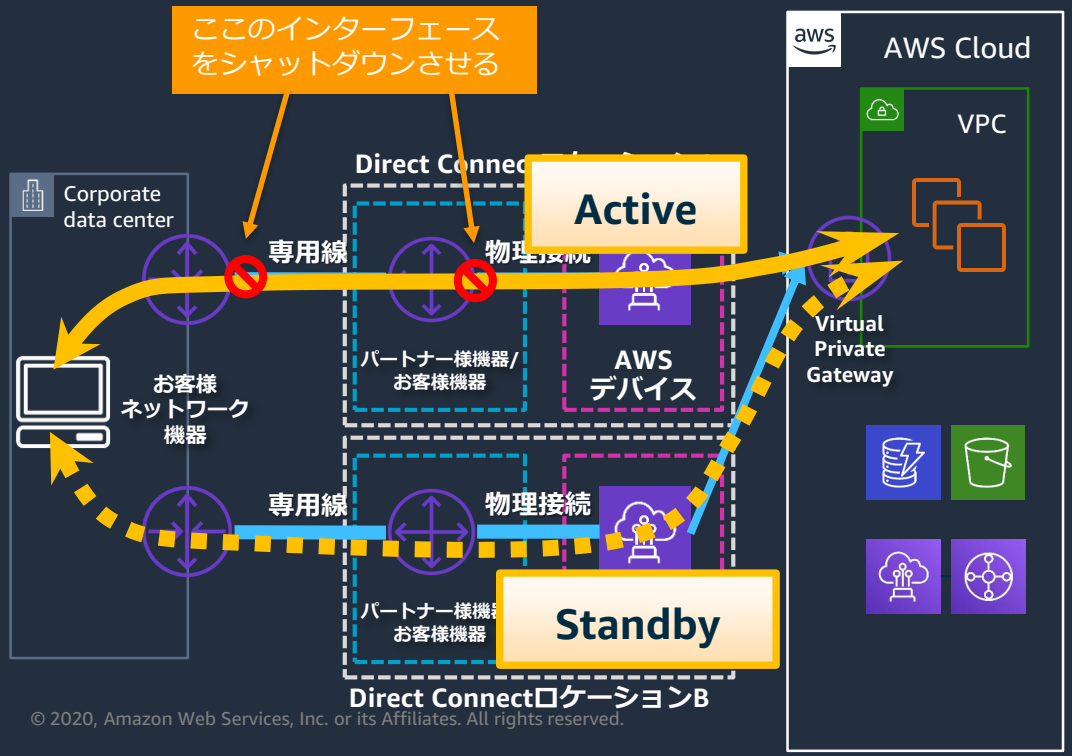
ゲームデーのメリット

定期的なゲームデーを実施することにより、以下のメリットがある

- 障害発生時でも慌てる必要が無い
- サービス提供側のメンテナンス通知で特別対応をとる必要が無い
- 自社の取り組みに対してパッチあてなどの改善が迅速に可能

AWS Direct Connectでのテスト例：

お客様ルーターの物理・論理インターフェースをシャットダウンするか、フィルターによる通信をブロックする事で試す



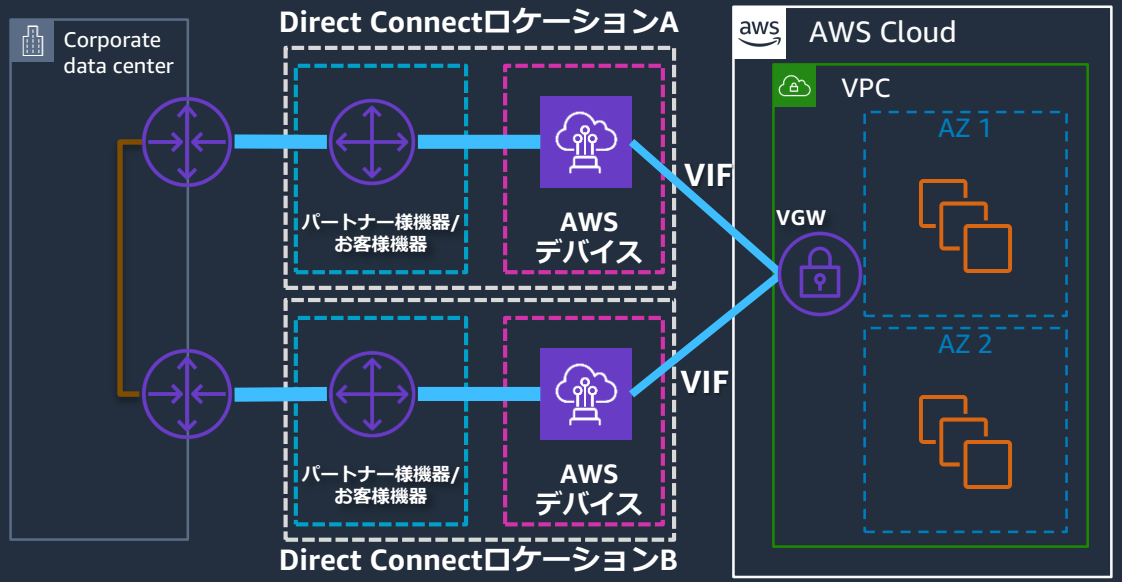
- AWS側の仕組みで障害を疑似する機能の提供は無い
- ゲートウェイにアタッチ済みのVIFを一時的にデタッチする事はできない
- BGPピアを能動的にダウンさせると経路切り替えがスムーズにいくが、厳密な障害再現にならない
- テスト手法としてVIFリソースを削除することも有効
  - ➢ 同一パラメーターでVIFを再作成すれば、通信復旧可（再作成可能な環境に限る）

ベストプラクティス

Direct Connect 回復性向上

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



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

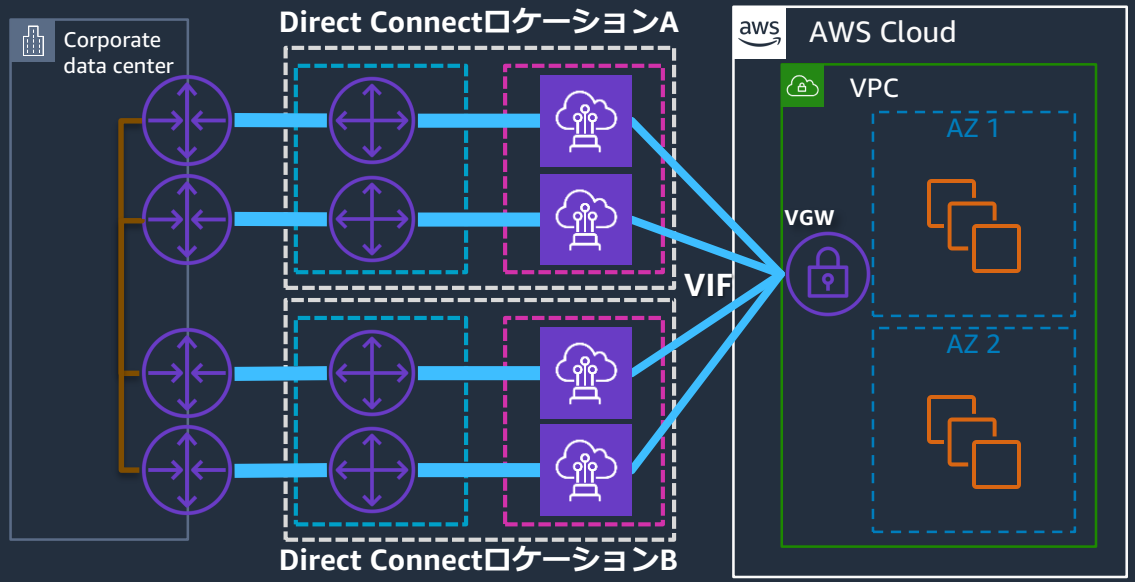
AWS Direct Connect Service Level Agreement
https://aws.amazon.com/jp/directconnect/sla/

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

・Active-Active、Active-Standyは問わない

・Direct Connect Gateway、Transit Gatewayも利用可能



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

AWS Direct Connect Service Level Agreement
https://aws.amazon.com/jp/directconnect/sla/

Direct Connect SLAの注意点

SLA認定を受けたとしても、AWS側システム・設備が特別な機器に収容されることなどは無い

➡認定を受けると、SLA基準を下回った場合に、返金のリクエストが出来る

大事なのは、W-Aに即した堅牢性のある構成とする事

本日のアジェンダ

1. はじめに
2. 冗長化がなぜ必要か？
3. 冗長化の選択肢
4. より高い可用性を求めるためには
5. 安心して運用するために
6. まとめ

まとめ

- ✓ 本番システムをAWS上で利用する際、ネットワークの冗長性は必須
- ✓ どれだけ投資できるかは、システム停止時の損失とのバランスで検討
- ✓ 要件に合わせて冗長化手段を選択
- ✓ Direct Connect接続は、複数のロケーションに分けて冗長化
- ✓ より高い可用性を求めるため、大阪ロケーション経由の冗長化とリソースもマルチリージョン化
- ✓ W-Aを活用し、適正な構成になっているかを確認
- ✓ SLAに適用する構成・定義

参考資料

[AWS Black Belt Online Seminar] AWS Direct Connect
https://aws.amazon.com/jp/blogs/news/webinar-bb-aws-direct-connect-2018/

[AWS Black Belt Online Seminar] AWS Transit Gateway
https://aws.amazon.com/jp/blogs/news/webinar-bb-aws-transit-gateway-2019/

AWS Direct Connect Service Level Agreement
https://aws.amazon.com/jp/directconnect/sla/

Direct Connect Resiliency Toolkit で使用を開始する方法
https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/resiliency_toolkit.html

AWS Well-Architected
https://aws.amazon.com/jp/architecture/well-architected/

Q&A

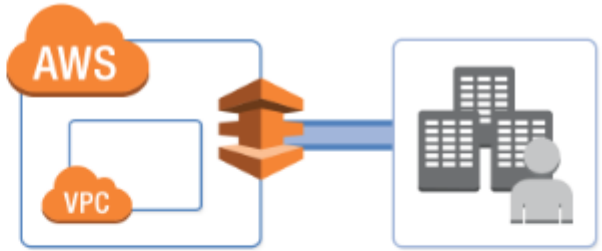
お答えできなかったご質問については
AWS Japan Blog 「https://aws.amazon.com/jp/blogs/news/」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS 専用線アクセス体験ラボトレーニング

AWS専用線アクセス体験ラボ



AWS 専用線アクセス体験ラボでは、オンプレミス環境と AWS 東京リージョンを複数の専用線で接続したシステム構築の検証に必要な環境をご提供いたします。お使いのハードウェア、アプライアンスとの動作検証も可能です。

AWS 専用線アクセス体験ラボは、以下の協賛企業からご支援を頂いております。

Coltテクノロジーサービス株式会社（旧KVH株式会社）、アルテリア・ネットワークス株式会社、株式会社TOKAIコミュニケーションズ、東日本電信電話株式会社

https://aws.amazon.com/jp/dx_labo/

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]

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