Internet Week 2018

S2 クラウド接続もおまかせ、基礎からのネットワーク
クラウドの基礎とオンプレミスネットワークとの接続

アマゾン　ウェブ　サービス　ジャパン株式会社
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
菊池　之裕

2018.11.27

内容についての注意点

- 本資料では2018年11月27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が東京リージョンを使用する場合、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.

プレゼンテーションについて

プレゼンテーションは事後資料にて公開いたします。

> スライドの撮影は不要です。

どうしてもメモ的に取りたいという方はシャッター音の鳴らないカメラアプリで周りの迷惑にならないよう撮影をお願いします。

自己紹介

名前：菊池　之裕(きくち　ゆきひろ)

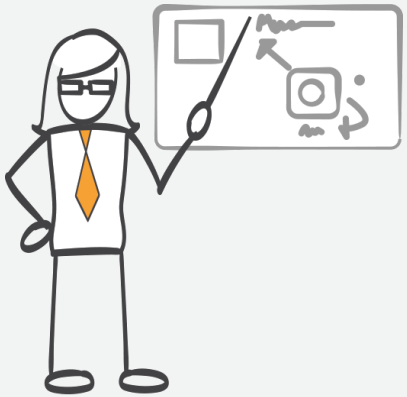
所属：アマゾン ウェブ サービス ジャパン株式会社
　　ソリューションアーキテクト　ネットワークスペシャリスト

ロール：Network系サービスについてのご支援

経歴：ISP,IXP,VPN運用、開発を経てネットワーク機器、仮想ルータ販売会社のプリセールス、プロダクトSEからAWSへ

好きな AWS サービス: ELB,Direct Connect,VPC,Marketplace

このセミナーのゴール



クラウド特有のネットワークに慣れる

従来の設計や運用を見直す

クラウドにあわせたネットワークの作り方を理解する

Agenda

- クラウドとは
  - クラウドのネットワークAmazon Virtual Private Cloud(VPC)
  - VPCにおけるルーティング
- 特性を考えたネットワーク
  - リージョンとアベイラビリティゾーンを理解する
  - 設計を柔軟に考える
  - セキュリティフィルタ、ACLの考え方：セキュリティグループとNetwork ACL
- オンプレミス環境とAWSクラウドの接続
  - Direct Connect　プライベート接続とパブリック接続
  - 高可用性
- よくある落とし穴
- まとめ

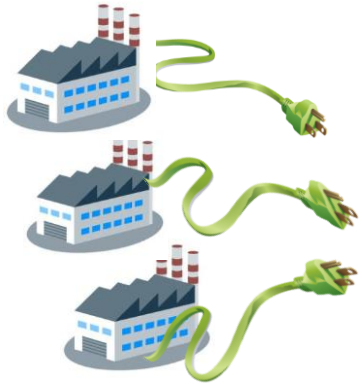
Agenda

- クラウドとは
  - クラウドのネットワークAmazon Virtual Private Cloud(VPC)
  - VPCにおけるルーティング
- 特性を考えたネットワーク
  - リージョンとアベイラビリティゾーンを理解する
  - 設計を柔軟に考える
  - セキュリティフィルタ、ACLの考え方：セキュリティグループとNetwork ACL
- オンプレミス環境とAWSクラウドの接続
  - Direct Connect　プライベート接続とパブリック接続
  - 高可用性
- よくある落とし穴
- まとめ

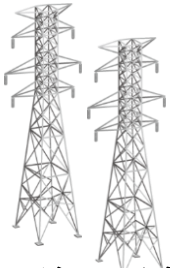
クラウドとは

いつでも、必要なだけ、低価格で

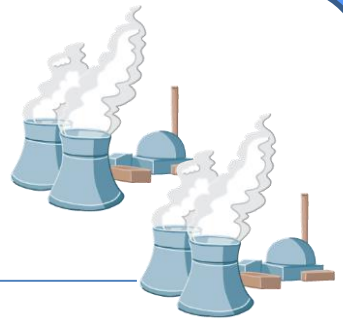
電気



工場



送電線



発電所

コンピュータ

IT部門

インターネット

データセンター

クラウドコンピューティングの特徴

初期投資が
不要

低額な
変動費

実際の使用分
のみ支払い

セルフサービスな
インフラ

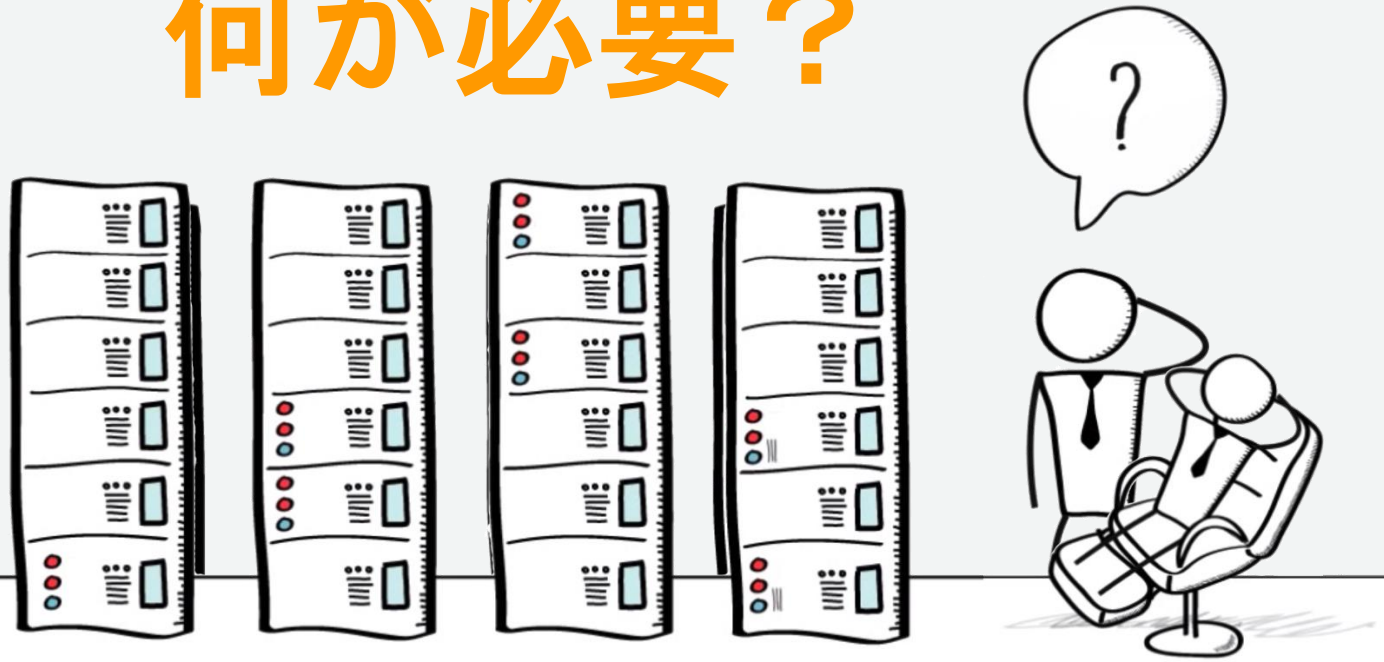
スケールアップ
ダウンが容易

市場投入と
俊敏性の改善

クラウドのネットワーク
Amazon Virtual Private Cloud(VPC)

データセンターをデザインしようとするには・・・

何が必要？



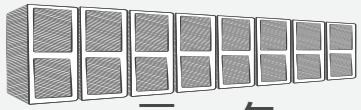
オンプレミス環境でのネットワークのイメージ

土地、電源、UPS、ラック、空調、ラック、ファイバー、パッチパネル、SFP等IFモジュール、スイッチ、ルータ、ストレージ、サーバ、ロードバランサー、ファイアーウォール、WAF、遠隔操作用ターミナルサーバ・・・

Before

従来のITインフラ

データセンター



ラック

ネットワーク機器

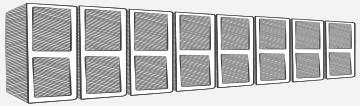
構築するには

時間（＝コスト）がかかる
早くても数ヶ月、長いと半年

After

クラウドで仮想ネットワークを構築

データセンター



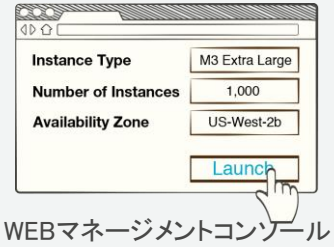
ラック

ネットワーク機器

必要な機能を抽象化
サービスとして
予め用意されている

(Network Function Virtualization)

組み合わせてすぐ利用開始！



WEBマネージメントコンソール

or

クラウドに対する悩み・不安

インターネット接続部分のスケールは大丈夫？

社内業務アプリケーションはミッションクリティカルだから冗長とか大丈夫？

クラウドを使いたいが社内ルール（セキュリティ/ネットワーク）に合わなそう

社内と専用線で接続したいけど、どうやればいいの?

VPC(Virtual Private Cloud)で解決可能

AWS上にプライベートネットワーク空間を構築

- 任意のIPアドレスレンジが利用可能

論理的なネットワーク分離が可能

- 必要に応じてネットワーク同士を接続することも可能

ネットワーク環境のコントロールが可能

- ルートテーブルや各種ゲートウェイ、各種コンポーネント

複数のコネクティビティオプションが選択可能

- インターネット経由
- VPN/専用線(Direct Connect)

aws

VPCに使うアドレスレンジの選択

VPC

VPCに設定するアドレスは既に使っている、もしくは使うであろうネットワークアドレスを避けるのがポイント

172.31.0.0/16

推奨: RFC1918レンジ

推奨:/16
(65,534アドレス)

最初に作成したアドレスブロックは作成後変更はできないので注意が必要
2個目以降は追加、削除ができる

aws

VPC設計のポイント

- CIĐR(IPアドレス)は既存のVPC、社内のĐCやオフィスと被らないアドレス帯をアサイン

  プライベートアドレスで無い場合は100.64.0.0/10 CGNAT　を使うのも手
- 複数のアベイラビリティゾーンを利用し、可用性の高いシステムを構築
- パブリック/プライベートサブネットへのリソースの配置を慎重に検討
- 適切なセキュリティ対策を適用する
- システムの境界を明らかにし、VPCをどのように分割するか将来を見据えてしっかりと検討する

様々なコンポーネントを用意


インターネット
ゲートウェイ


サブネット


仮想ルータ

ルート
テーブル


VPC
Peering


NAT
ゲートウェイ


VPC
エンドポイント
for
Amazon S3


Elastic
IP


バーチャル
プライベート
ゲートウェイ


VPN
コネクション

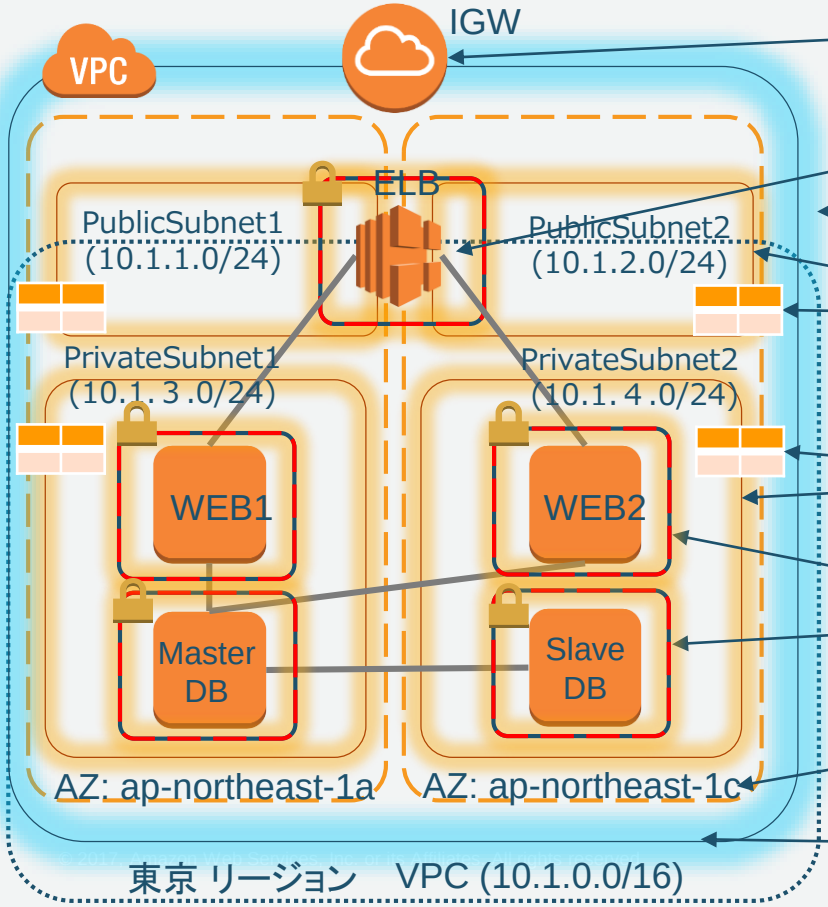

カスタマ
ゲートウェイ


Elastic
ネットワーク
インタフェース


Elastic
ネットワーク
アダプタ

aws

AWSでのネットワーク設計例



インターネットゲートウェイ

ロードバランサ

仮想プライベートネットワーク（VPC）

パブリックサブネットとルートテーブル
（インターネットへの経路設定あり）

プライベートサブネットとルートテーブル
（インターネットへの経路設定なし）

セキュリティグループ
（ステートフルファイアウォール）

アベイラビリティゾーン（DC群）を選択

東京のリージョンを選択

IPアドレス空間の設計

- VPCを作成するリージョンを選択
  - 必要なロケーションのリージョンを選択

- VPCに付与するCIDRブロックの決定
  - 大きさは /28 から /16
  - オンプレミス環境との接続も考慮し、被らないCIDRを選択

ポイント

VPCはリージョンに存在

VPCはリージョン内のアベイラビリティゾーンすべてに及ぶ

VPC (10.1.0.0/16)
東京 リージョン

サブネット設計

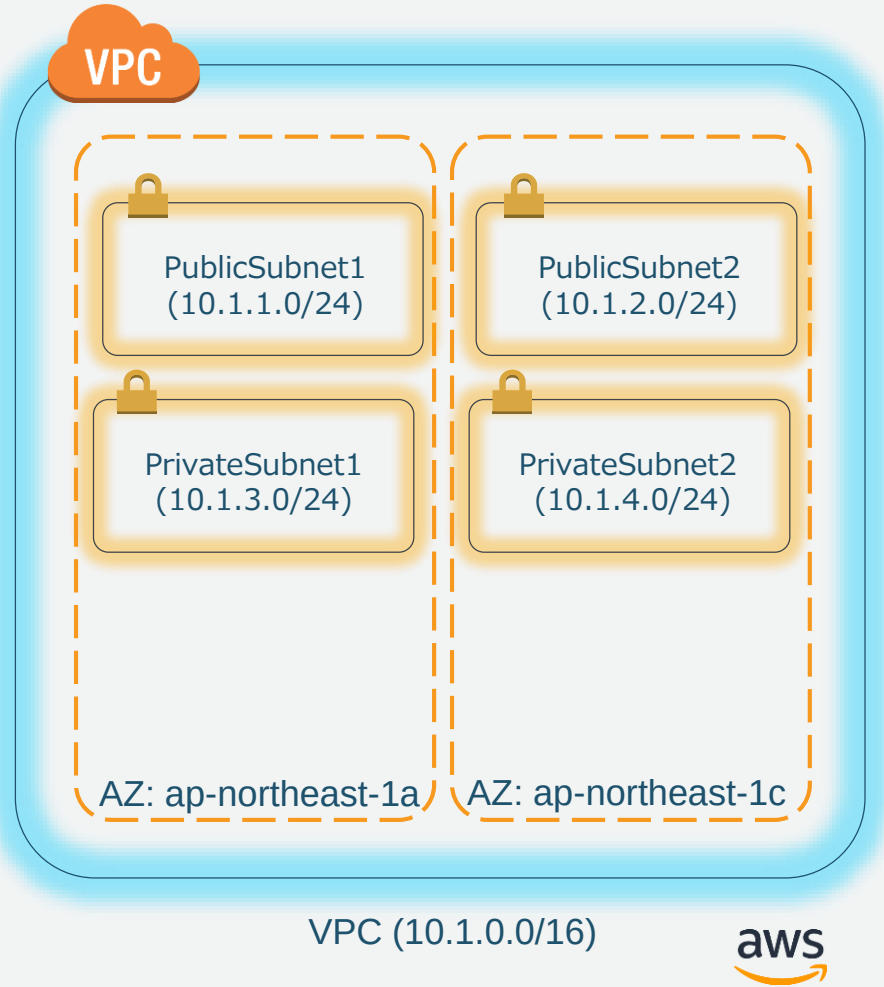
- ルーティングポリシーごとにサブネットを分割
  - 例：インターネットアクセスの有無で分割

    有：Public Subnet

    無：Private Subnet
- サブネットを設置するAZ（アベイラビリティゾーン）を選択
  - 例：高可用性のために2つのAZにサブネットを分けて配置（右図）
- サブネットのCIDRを選択

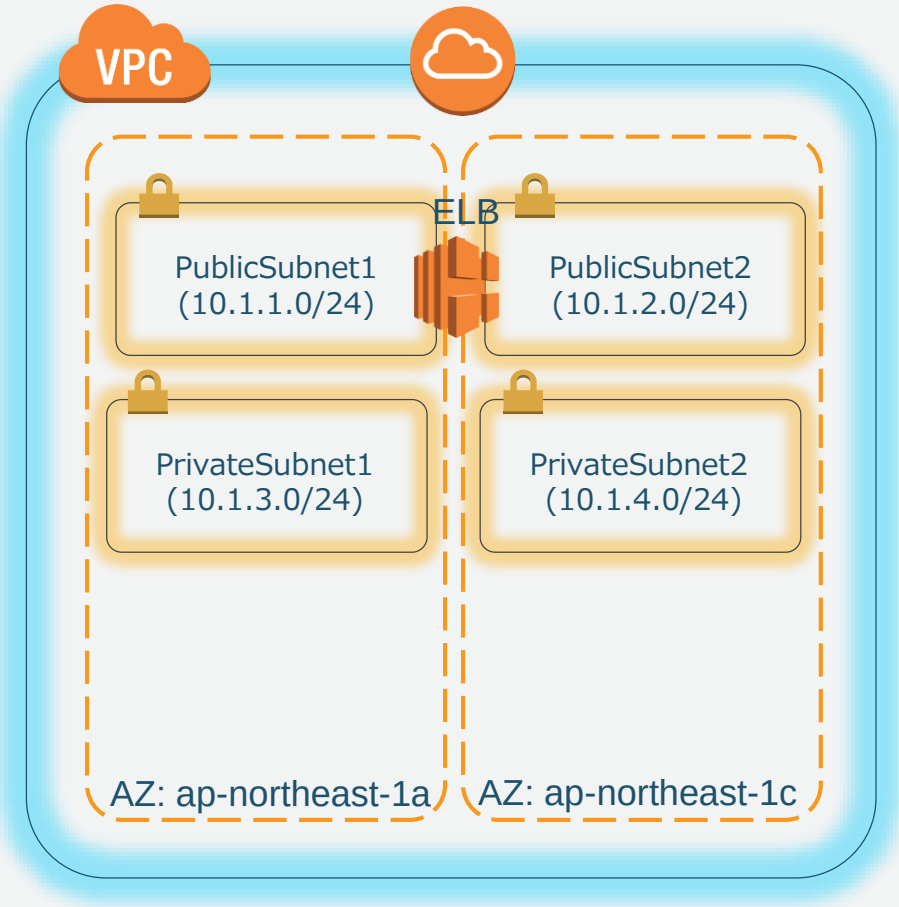
<u>ポイント</u>

サブネットはアベイラビリティゾーンに存在



コンポーネントの配置

- インターネットゲートウェイ（IGW）
  - VPCにアタッチして使用
  - 自動スケーリング
  - 単一障害点無し
- Elastic Load Balancing（ELB）
  - 仮想ロードバランサとしてVPC内で使用
  - 自動スケーリング
  - 単一障害点無し
  - パブリックIPを付与



参考:
https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html
https://aws.amazon.com/jp/elasticloadbalancing/

VPC (10.1.0.0/16)
東京 リージョン

ルーティング設計

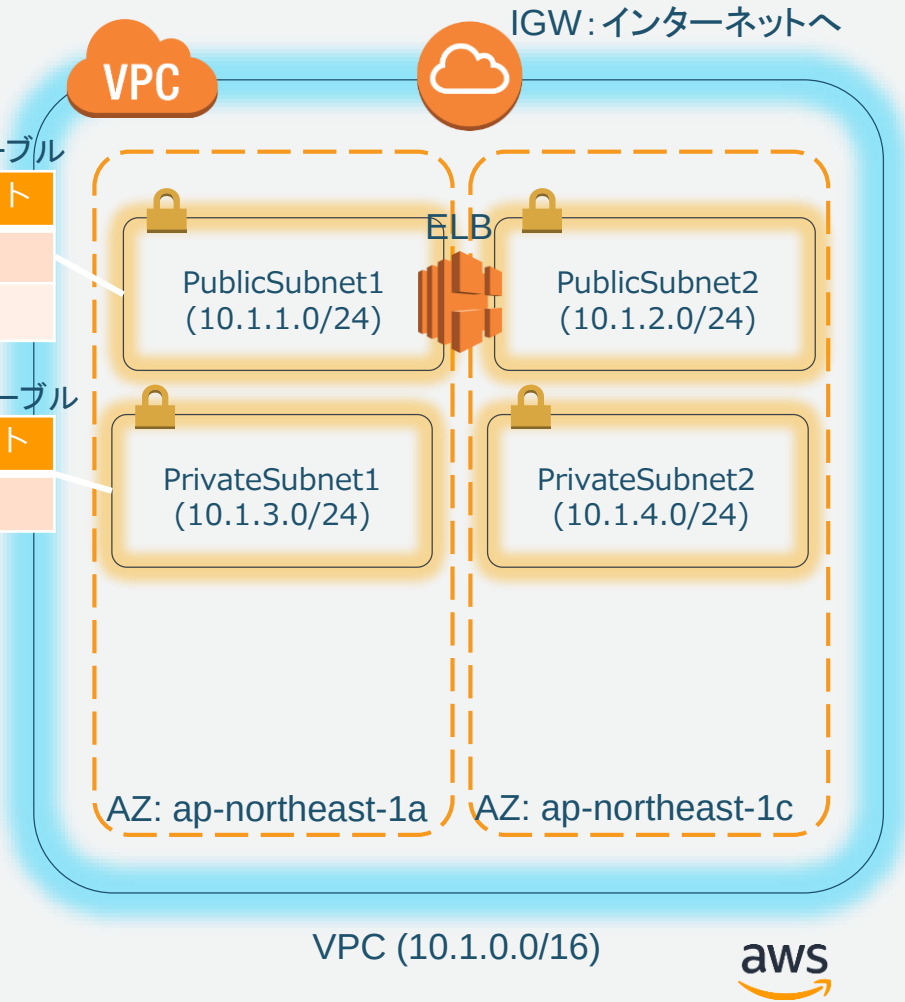
- VPC内のサブネット間はデフォルトで互いにルーティング可能
- ここではIGW向けにデフォルトルート0.0.0.0/0を追加（赤字）
- 必要な送信先への経路を設定可能

Public Sunbnetのルートテーブル

送信先	ターゲット
10.1.0.0/16	local
0.0.0.0/0	**IGW**

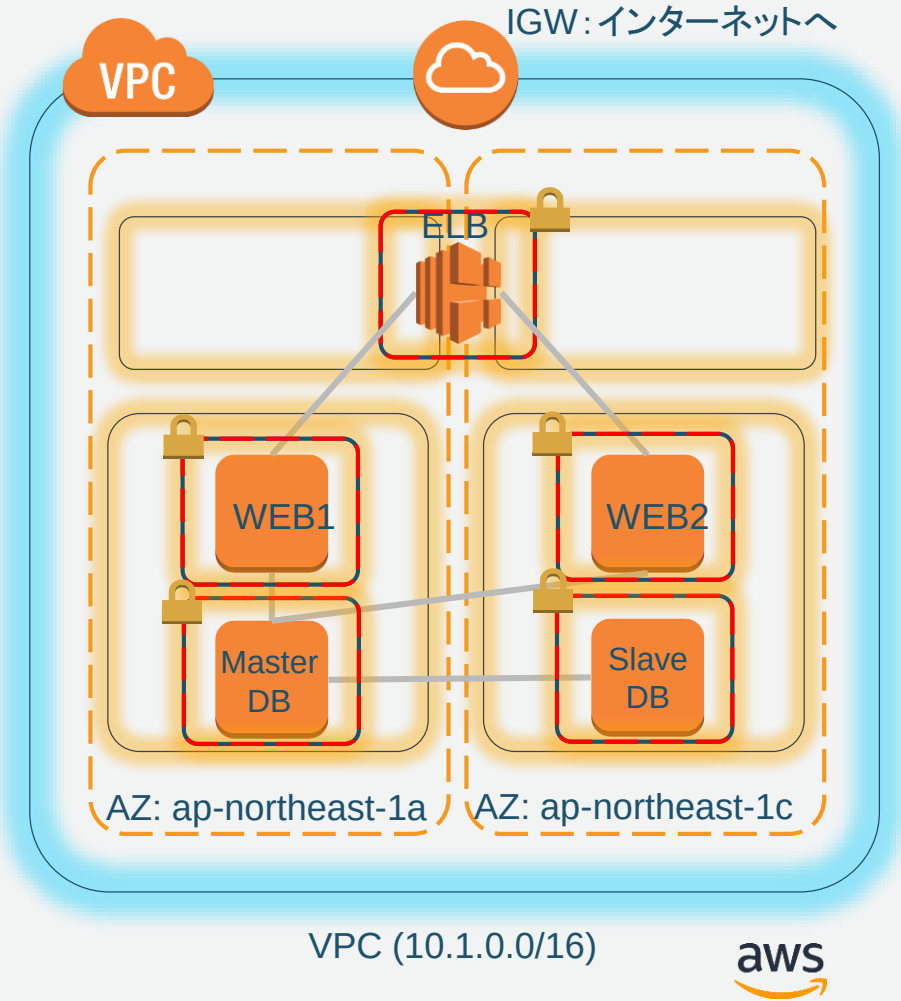
Private Sunbnetのルートテーブル

送信先	ターゲット
10.1.0.0/16	local



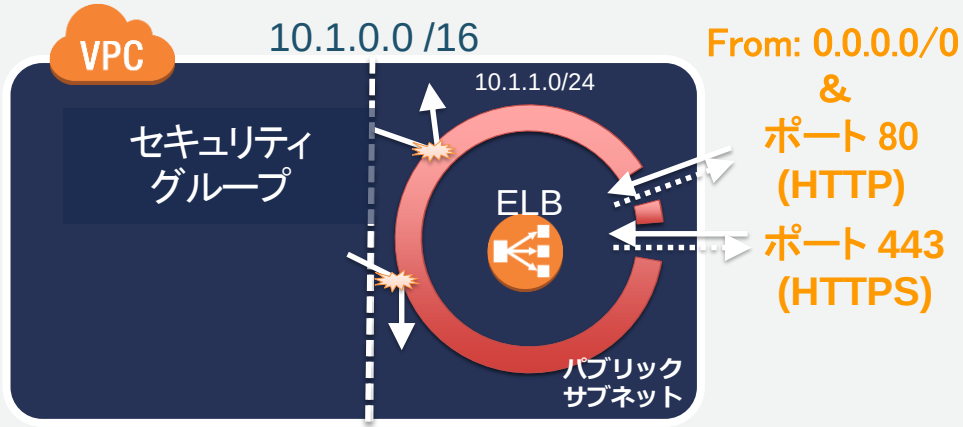
セキュリティ設計

- セキュリティグループ（右図の赤点線）
  - お客様のポリシーに従って必要な通信のみを許可
  - 一種のステートフルファイアウォール



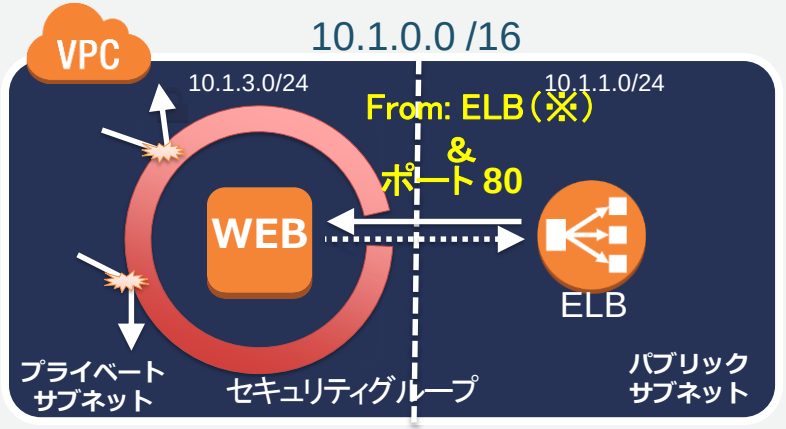
セキュリティグループの例

ルール：ELBは インターネットからサービスポート HTTP(80) と HTTPS(443) 宛だけ受信



セキュリティグループの例（つづき）

ルール：WEBサーバはELBからのHTTP通信 だけ許可



※IPアドレスではなく、ELBのセキュリティグループをソースとして指定可能
※ELBのセキュリティグループは描画を省略しています

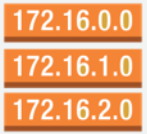
OSではなくインフラのレイヤで確実に通信を制御

参考：https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

VPCにおけるルーティング

VPC内におけるルーティング

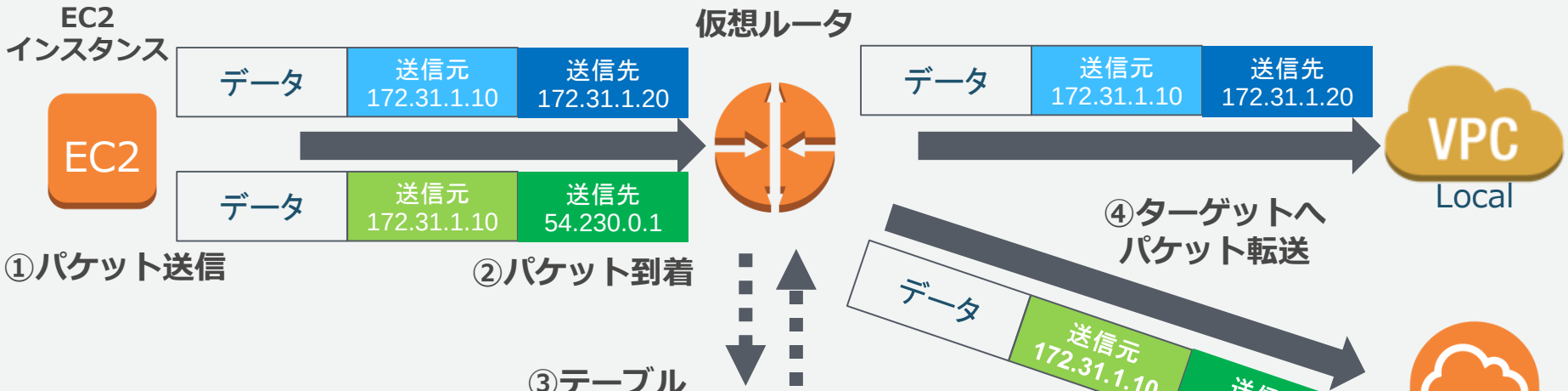
- ルートテーブルはパケットがどこに向かえば良いかを示すもの
- VPC作成時にデフォルトで１つルートテーブルが作成される
- VPC内は作成時に指定したCIDRアドレス（プライベートアドレス）でルーティングされる



ルートテーブルの確認

インターネットゲートウェイを作成、VPCにアタッチ

仮想ルータとルートテーブルの関係(ルートLook up)



rtb-9c7350f8

要約 | ルート | サブネットの関連付け | タグ

編集

View: All rules

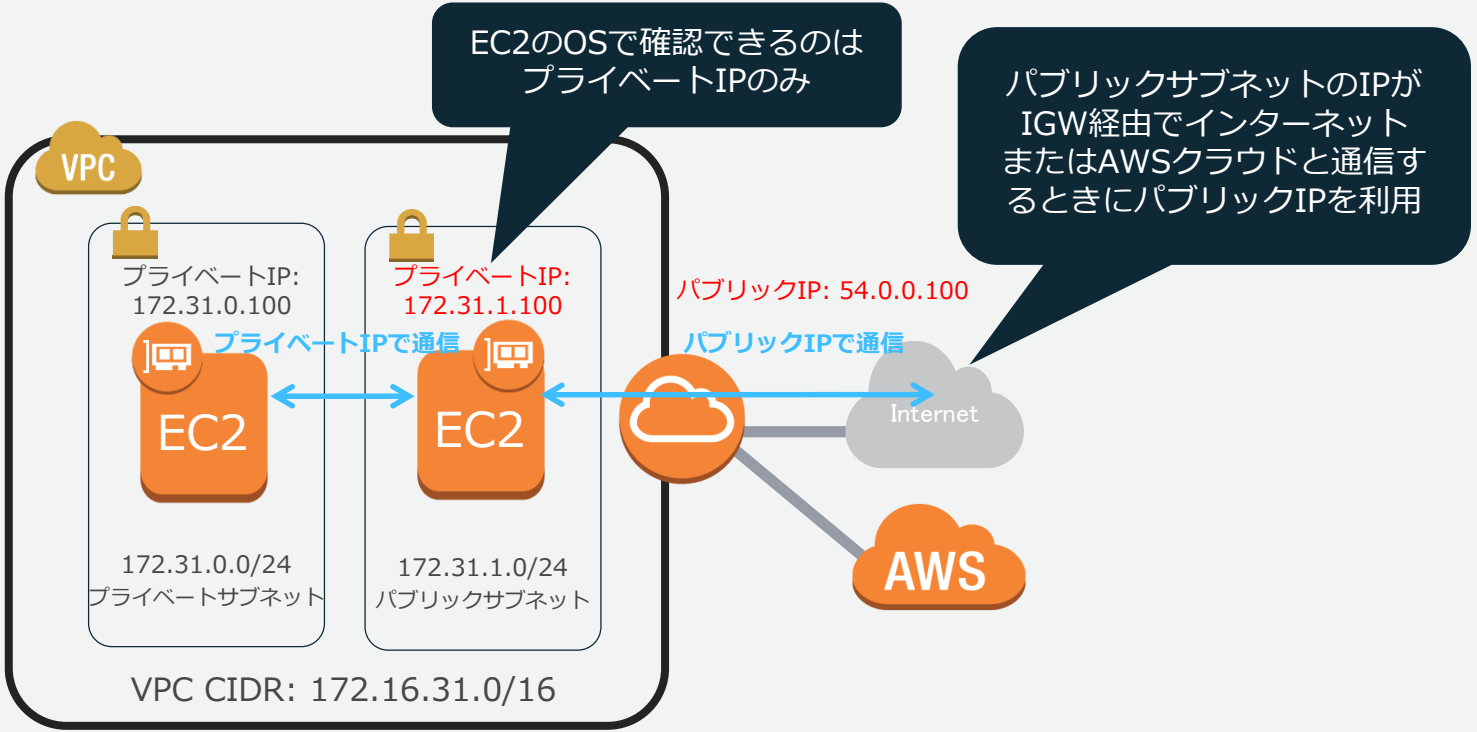
送信先	ターゲット	ステータス	伝達済み
172.31.0.0/16	local	アクティブ	いいえ
0.0.0.0/0	igw-29454e4c	アクティブ	いいえ

← 送信先172.31.1.20はこっち行けば良い

← 送信先 54.230.0.1 はこっち行けば良い

ルートテーブルにインターネットゲートウェイを追加

パブリックサブネットとプライベートサブネット



Agenda

- クラウドとは
  - クラウドのネットワークAmazon Virtual Private Cloud(VPC)
  - VPCにおけるルーティング
- 特性を考えたネットワーク
  - リージョンとアベイラビリティゾーンを理解する
  - 設計を柔軟に考える
  - セキュリティフィルタ、ACLの考え方：セキュリティグループとNetwork ACL
- オンプレミス環境とAWSクラウドの接続
  - Direct Connect　プライベート接続とパブリック接続
  - 高可用性
- よくある落とし穴
- まとめ

特性を考えたネットワーク

リージョンとアベイラビリティゾーンを理解する

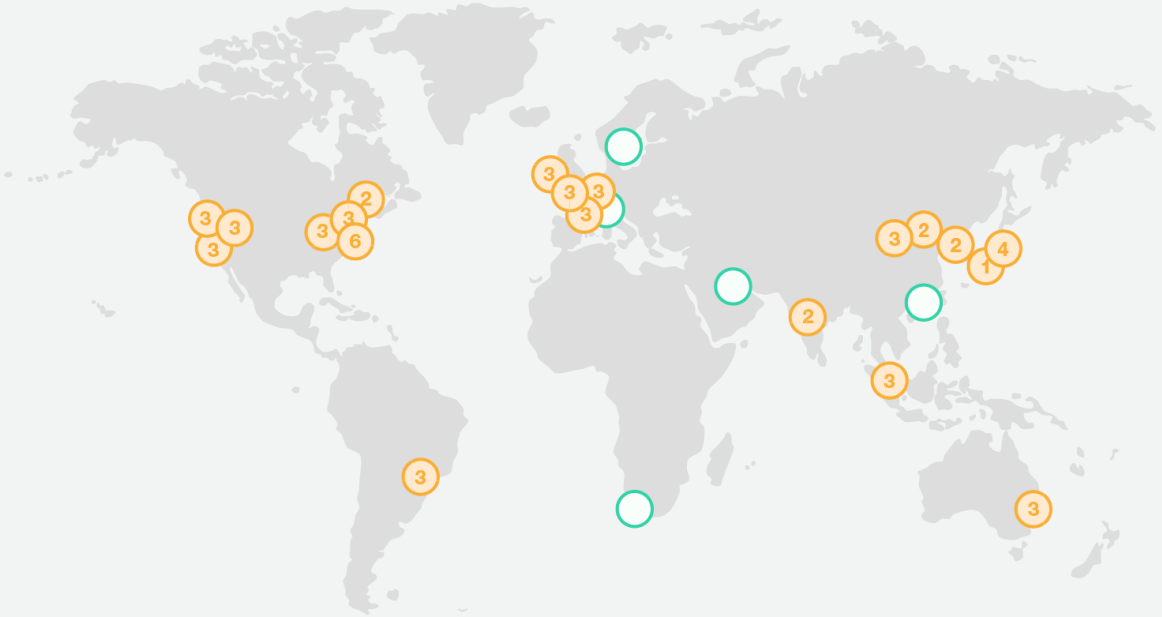
リージョン

19＋1のリージョン（国・地域）

1. US EAST (Virginia)
2. US WEST (N. California)
3. US WEST 2 (Oregon)
4. EU WEST (Ireland)
5. JAPAN (Tokyo)
6. South America (Sao Paulo)
7. Singapore
8. Sydney
9. GovCloud(West)
10. BJS 1 (Beijing China)
11. EU (Frankfurt)
12. Korea
13. India
14. OHIO
15. MONTREAL
16. UK
17. **NINGXIA**
18. **France**
19. **Osaka(Local)**
20. **GovCloud(East)**

* GovCloudは米国政府関係企業用です。

57のアベイラビリティ・ゾーン（データセンター群）
150 のエッジロケーション



データ保管先を明示的に指定可能。

アベイラビリティゾーン

AZは１つ以上のデータセンターで構成される

- １リージョン内にAZが複数存在（大阪ローカルリージョンを除く）
- AZはお互いに地理的・電源的・ネットワーク的に分離
- 2つのAZを利用した冗長構成を容易に構築
- リージョン内のAZ間は高速専用線で接続（リージョン間も可能な限り高速専用線で接続）

アベイラビリティゾーン

AZは１つ以上のデータセンターで構成される

- １リージョン内にAZが複数存在（大阪ローカルリージョンを除く）
- AZはお互いに地理的・電源的・ネットワーク的に分離
- 2つのAZを利用した冗長構成を容易に構築
- リージョン内のAZ間は高速専用線で接続（リージョン間も可能な限り高速専用線で接続）

複数のデータセンターをまたいだネットワークを簡単に構築可能

冗長の考え方を変えてみる

- よくある要求仕様
  - TCPのセッションは障害時に即座にバックアップ機に引き継がれること

  → データセンターを跨いだ時点で不可能
  - システムの正常性の定義を考え直してみる
  - 1パケット落としてもTCPでは再送がかかる
  - 全体のシステム全体でリカバリができていれば良しとする

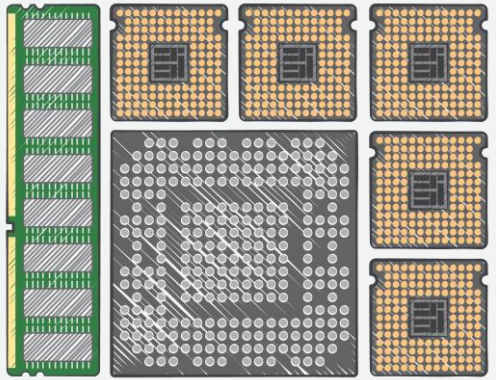
Design for Failureの考え方

- ゼッタイに落ちないシステムはない
  - EC2インスタンスやデータベースが落ちたときに問題がないようにシステムを作る
  - 疎結合や、水平に展開できるシステムを目指す
  - IPアドレスに依存しない。DNSを活用
    - 単一IPがシングルポイント、DNSで複数エントリを書くようにする（マネージドサービスは最初から考慮）
    - 詳しくは**AWSを用いた耐障害性の高いアプリケーションの設計** https://www.slideshare.net/kentamagawa/aws-7991623 を参照

設計を柔軟に考える

帯域保証を聖域と考えない

- 帯域は増やせる
  - EC2インスタンスタイプで帯域が選択できる
  - POCをすることで必要な帯域が求められる
  - どうしてもギャランティしたい場合はギャランティされているインスタンスタイプを選択する



従来の設計を踏襲する前にPOCをしよう

- 実際のワークロードを乗せてシミュレートしてみる
- 必要な容量や帯域がわかる。
- 物理とくらべて安価で作ったり壊したりが容易

- クラウドは、柔軟
  - インスタンスタイプの変更や水平展開ができることを意識してみる。
  - ネットワークアドレスも潤沢に用意しておくと、ビジネスが順調に伸びた場合や急なサーバー追加にも対応可能
    - IPアドレスやサブネットを大きめに作っておく

セキュリティフィルタ、ACLの考え方：
セキュリティグループと
Network ACL

特性に合わせた新しい考え方を取り入れる

- いままでのフィルタ
  - L2スイッチで1台ごとにフィルタをポートに記述
  - 大量のフィルタ行と戦うはめに
- クラウドの機能を有効利用
  - セキュリティグループという概念を使う
  - 1台ごとに管理ができ、グループ化も可能
  - セキュリティグループ自身をターゲットにできるのでIPを意識しない運用が可能

aws

セキュリティグループ = ステートフル Firewall

デフォルトで許可されているのは同じセキュリティグループ内通信のみ
（外からの通信は禁止）

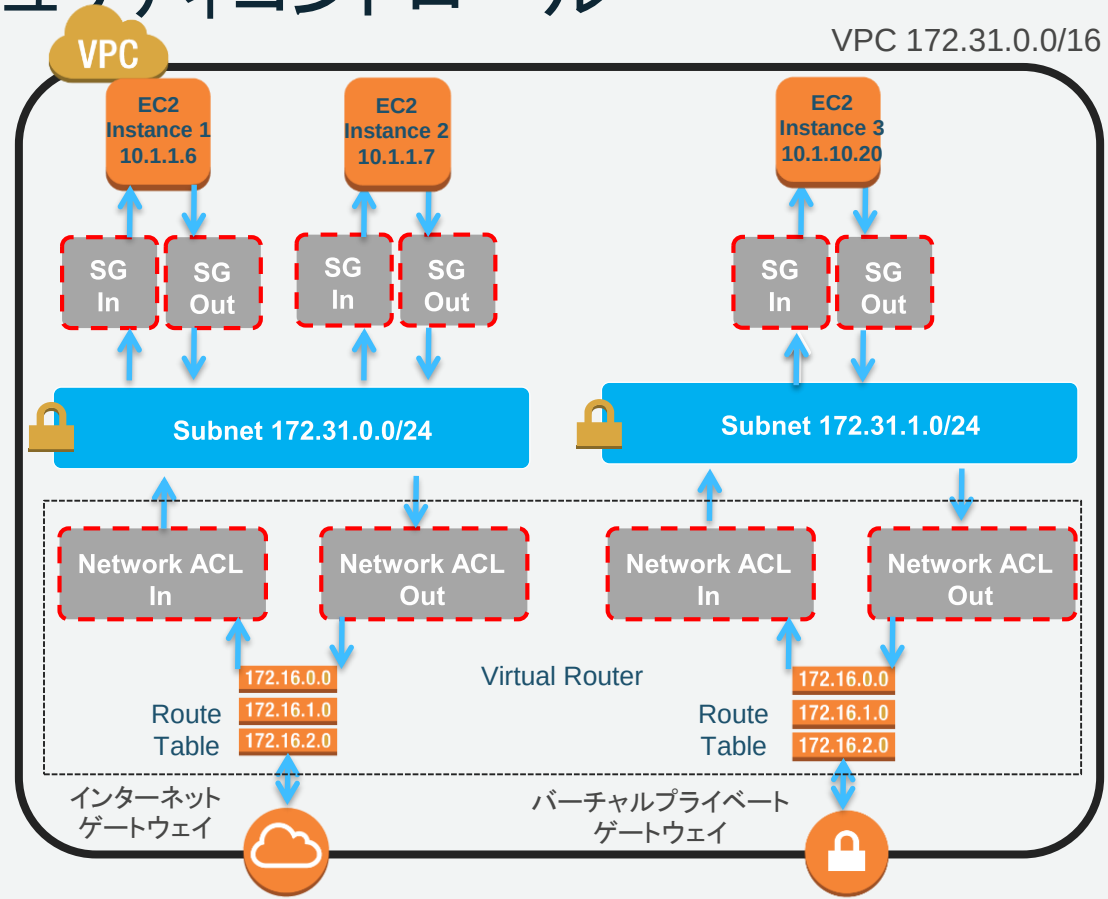
その為、必要な通信例えば、
WEB公開する場合は
インターネット(0.0.0.0/0)から80
ポートを許可

Network ACLs = ステートレス Firewall

サブネット単位で
適用される

デフォルトでは全ての
送信元IPを許可

VPCセキュリティコントロール



ネットワークACL vs セキュリティグループ

ネットワークACL	セキュリティグループ
サブネットレベルで効果	サーバレベルで効果
Allow/DenyをIN・OUTで指定可能 (ブラックリスト型)	AllowのみをIN・OUTで指定可能 (ホワイトリスト型)
ステートレスなので、戻りのトラフィックも明示的に許可設定する	ステートフルなので、戻りのトラフィックを考慮しなくてよい
番号の順序通りに適用	全てのルールを適用
サブネット内のすべてのインスタンスがACLの管理下に入る	インスタンス管理者がセキュリティグループを適用すればその管理下になる

再掲:特性に合わせた新しい考え方を取り入れる

- いままでのフィルタ
  - L2スイッチで1台ごとにフィルタをポートに記述
  - 大量のフィルタ行と戦うはめに
- クラウドの機能を有効利用
  - セキュリティグループという概念を使う
  - 1台ごとに管理ができ、グループ化も可能

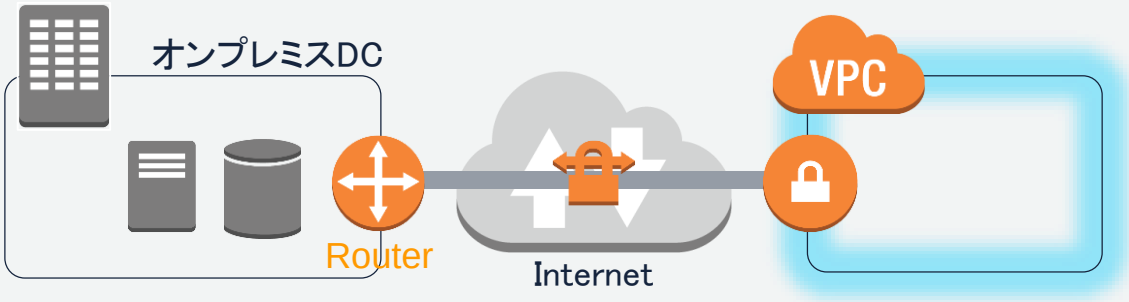
Agenda

- クラウドとは
  - クラウドのネットワークAmazon Virtual Private Cloud(VPC)
  - VPCにおけるルーティング
- 特性を考えたネットワーク
  - リージョンとアベイラビリティゾーンを理解する
  - 設計を柔軟に考える
  - セキュリティフィルタ、ACLの考え方：セキュリティグループとNetwork ACL
- オンプレミス環境とAWSクラウドの接続
  - Direct Connect　プライベート接続とパブリック接続
  - 高可用性
- よくある落とし穴
- まとめ

オンプレミス環境とAWSクラウドの接続

オンプレミス環境とAWSクラウドの接続（１）

VPN接続

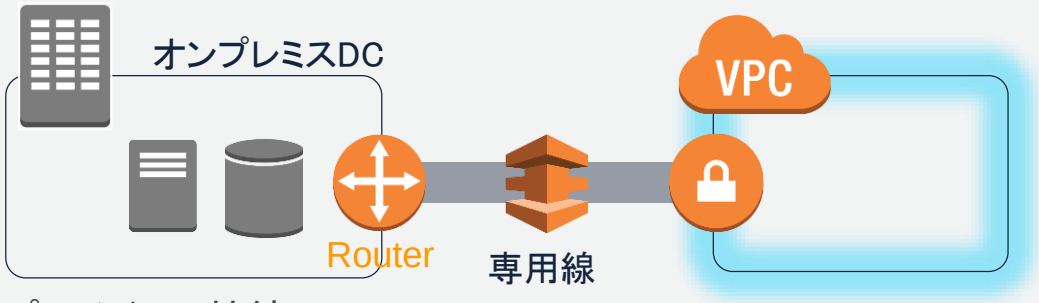


- インターネットVPNによるプライベート接続
- オンプレミス環境からのデータ移行やハイブリッド環境の構築に利用
- オンプレミスからのユーザー端末からのプライベートなアクセス経路としても利用

参考：
https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpn-connections.html

オンプレミス環境とAWSクラウドの接続（２）

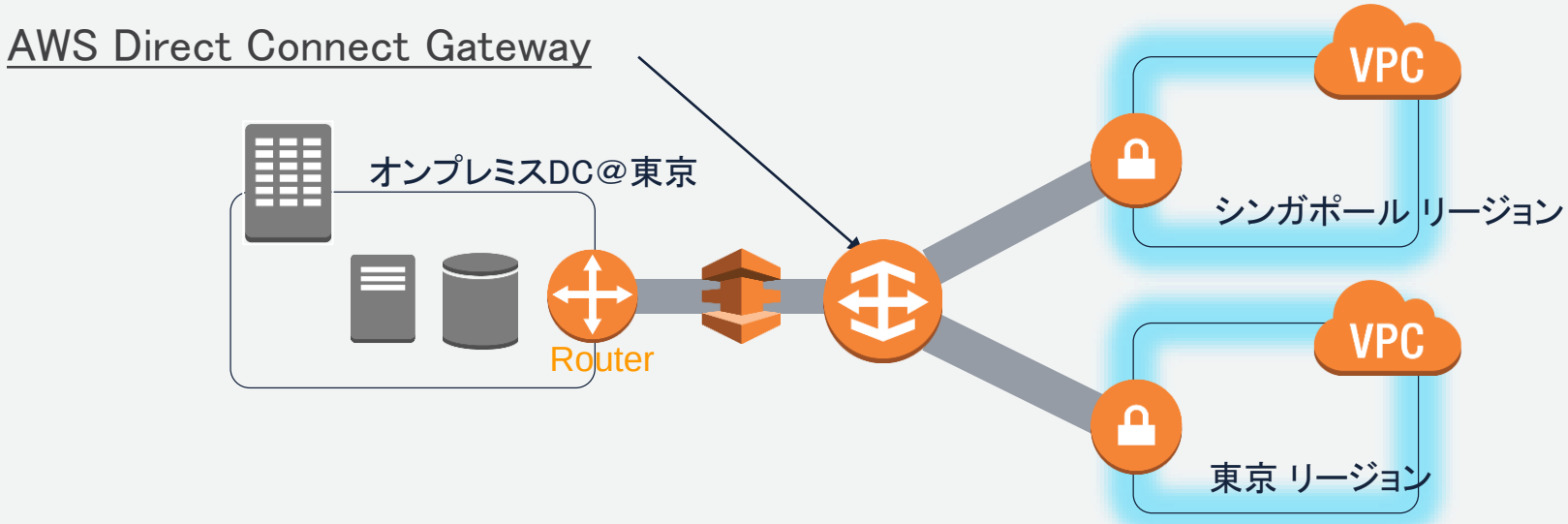
AWS Direct Connect



- 専用線接続によるプライベート接続
- 安定したスループット、レイテンシ
- オンプレミス環境からのデータ移行やハイブリッド環境の構築に利用
- オンプレミスからのユーザー端末からのプライベートなアクセス経路としても利用

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

オンプレミス環境とAWSクラウドの接続（３）



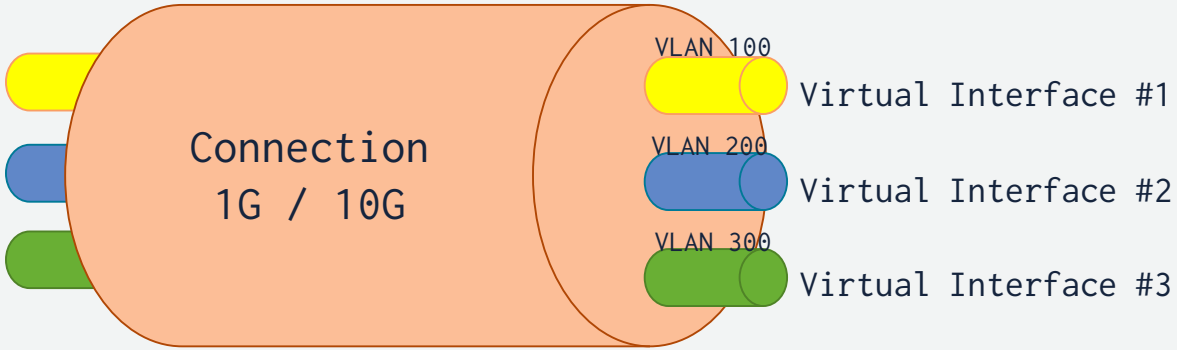
- Direct ConnectでAWSクラウドへ接続するだけでそこから世界の全リージョン（中国を除く）のVPCに閉域網で接続することが出来る

参考：
https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/direct-connect-gateways.html

Direct Connect
プライベート接続とパブリック接続

仮想インタフェース（Virtual Interface = VIF）

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



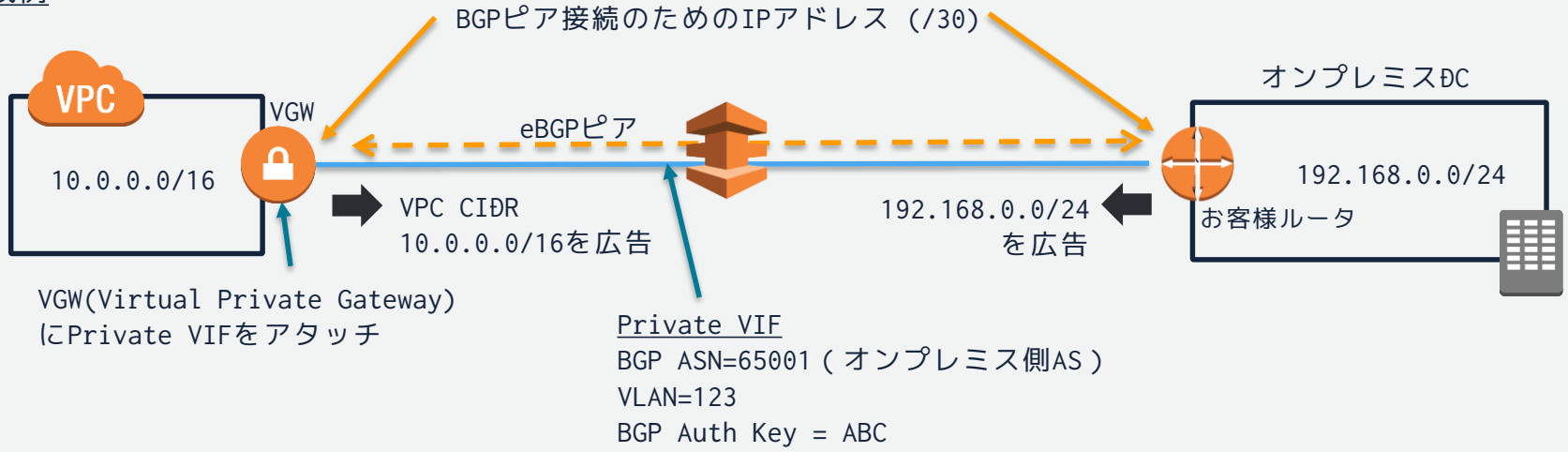
- VPCへプライベートアドレスを介した接続を提供するのが**Private VIF**
- AWSの全リージョンへパブリックIPを介した接続を提供するのが**Public VIF**

プライベート接続

- Private VIFを使用してVPCへの接続を提供
- 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AWSから広告される
- Jumbo Frame(MTU=9001)をサポート

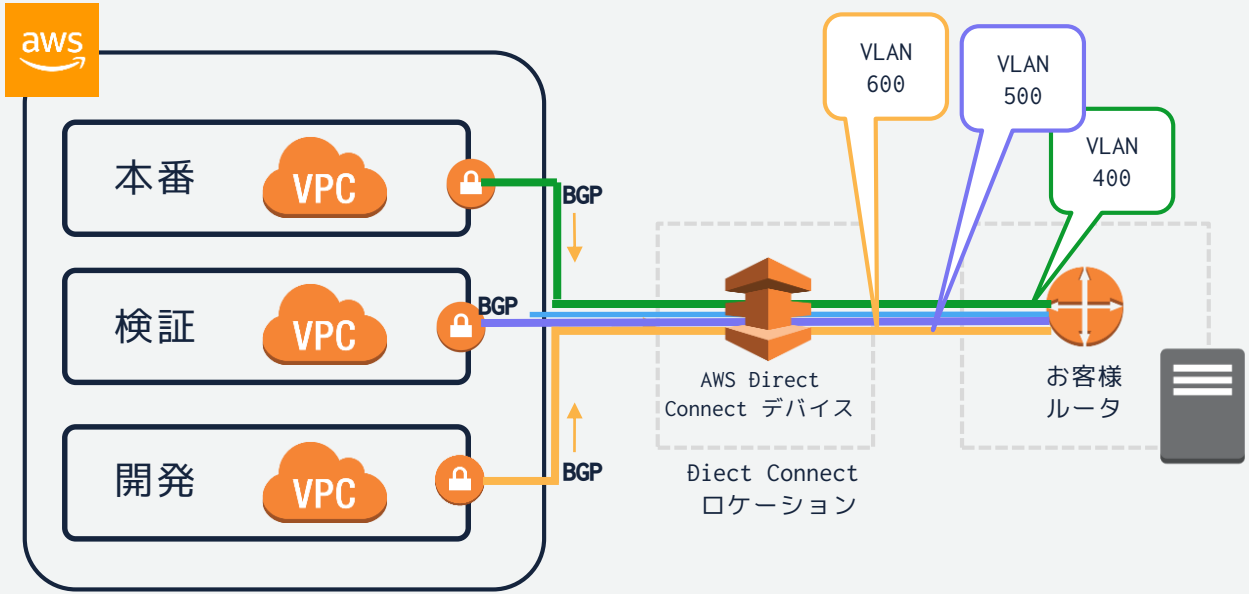
  https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/set-jumbo-frames-vif.html

構成例



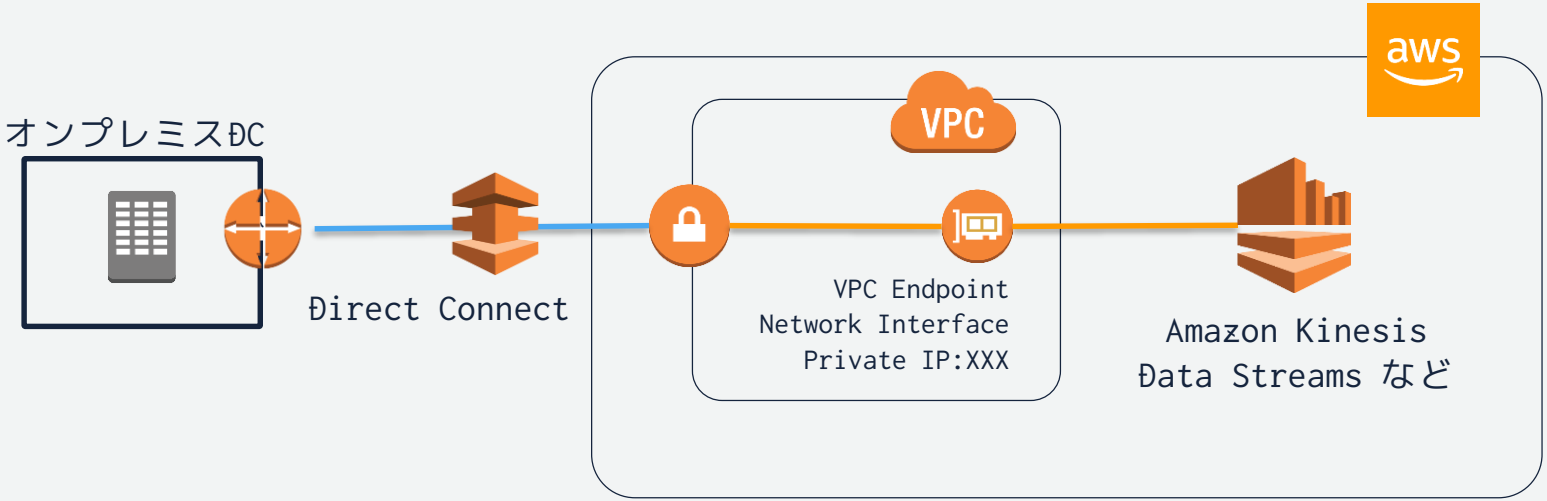
Private VIFによるマルチVPC接続

- オンプレミスを複数のVPCへ接続するために複数のPrivate VIFを使用
- 複数の異なるAWSアカウントのVPCへオンプレミスから接続可能
- 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



オンプレミスからAWS PrivateLinkへの接続（1）

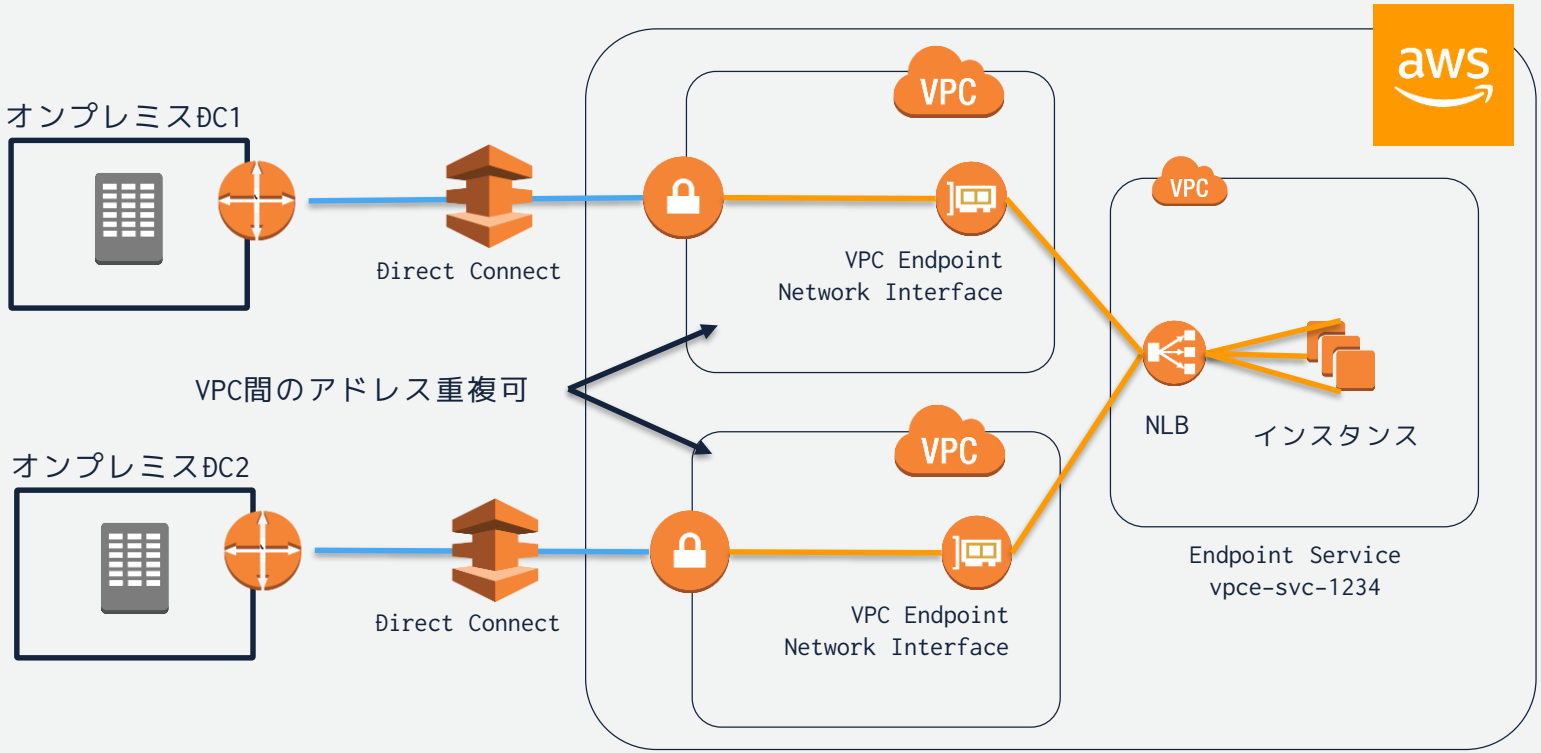
インタフェース型VPCエンドポイント（＝PrivateLink）を使用するAWSサービスへダイレクトコネクト経由でアクセスする構成の例



https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/vpce-interface.html

オンプレミスからAWS PrivateLinkへの接続（２）

エンドポイントサービスを公開し、Direct Connect経由でアクセスする例

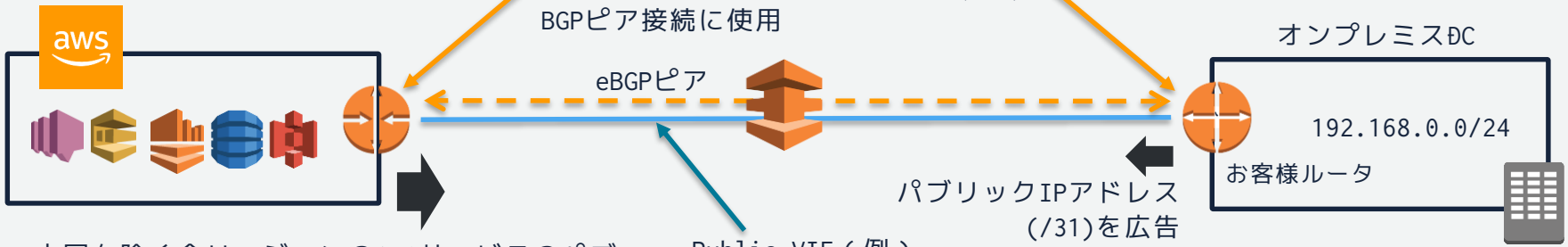


https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/vpce-interface.html

パブリック接続

- Public 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AWS提供のパブリックIPアドレスへNAT
  ※お客様所有のパブリックIPの持ち込みも可能
- 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で自リージョンの経路だけをフィルタ可能

構成例



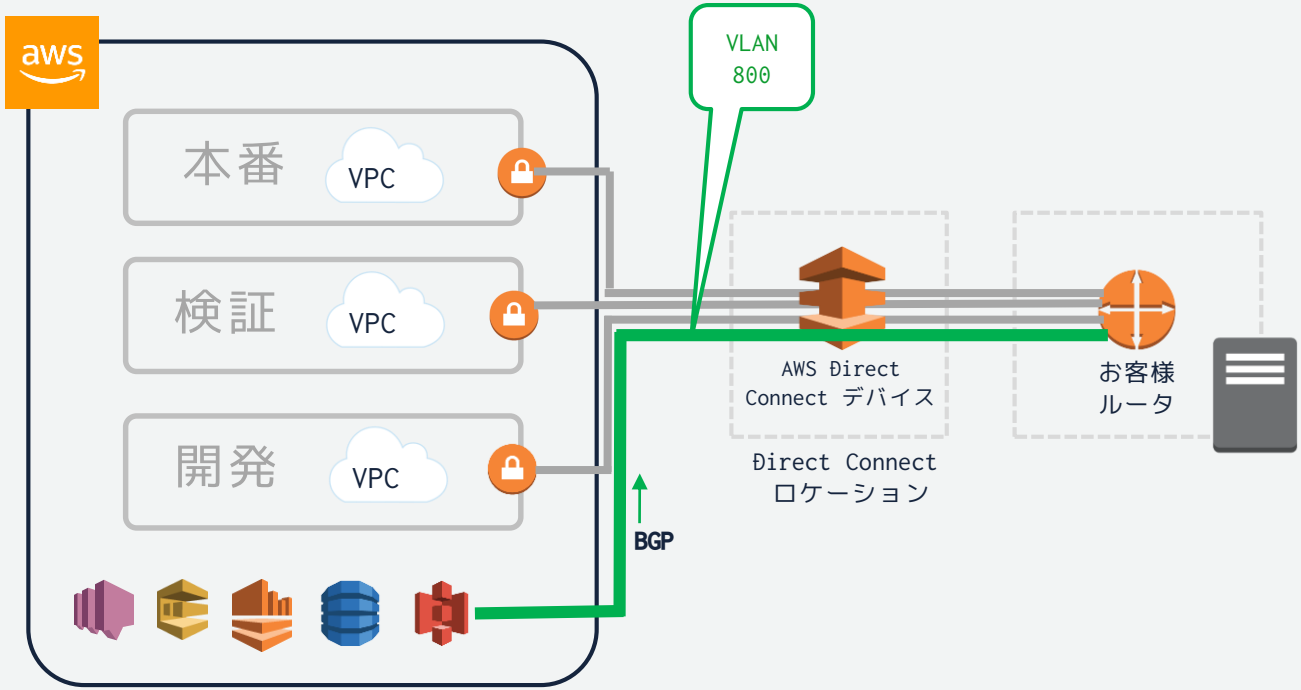
中国を除く全リージョンのAWSサービスのパブリックIPを広告

広告される経路について
https://forums.aws.amazon.com/ann.jspa?annID=2391

Public VIF（例）
BGP ASN=65001（オンプレミス側AS）
VLAN=456
BGP Auth Key = ABC

Public VIFによるパブリックサービスへの接続

- 同一Connection上にPublic VIFとPrivate VIFの混在が可能

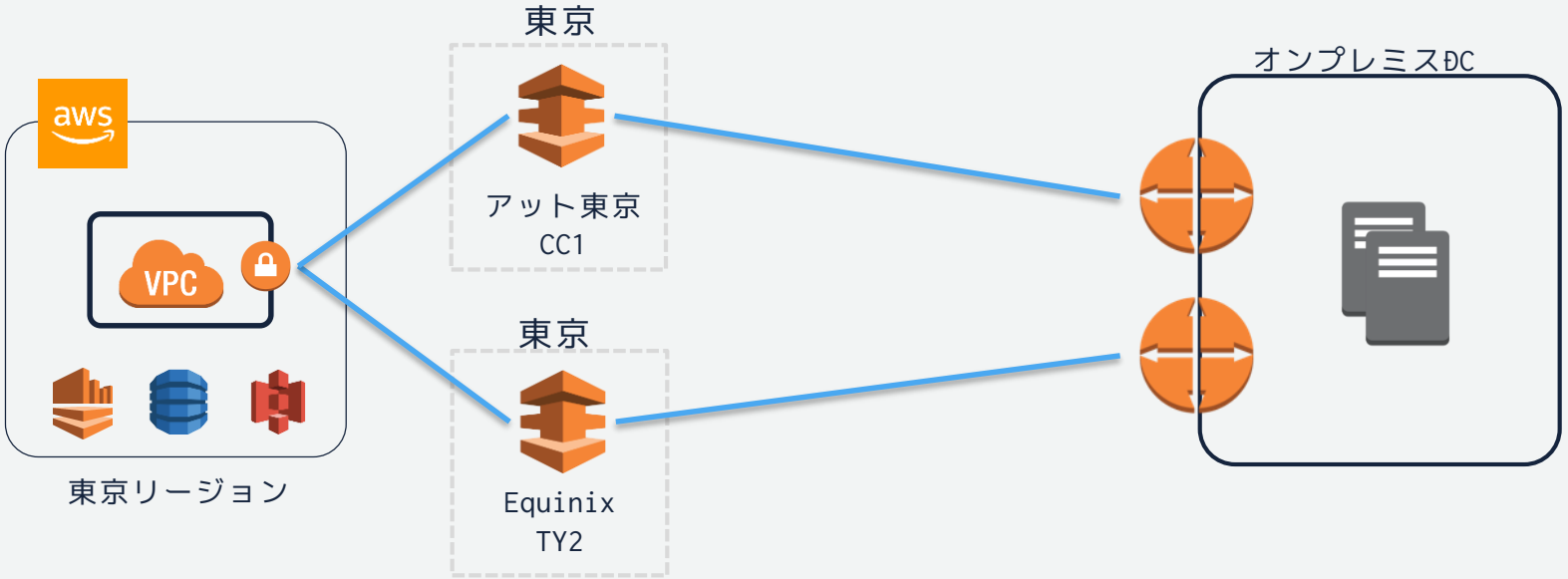


高可用性

デュアルロケーション（東京内で分散）

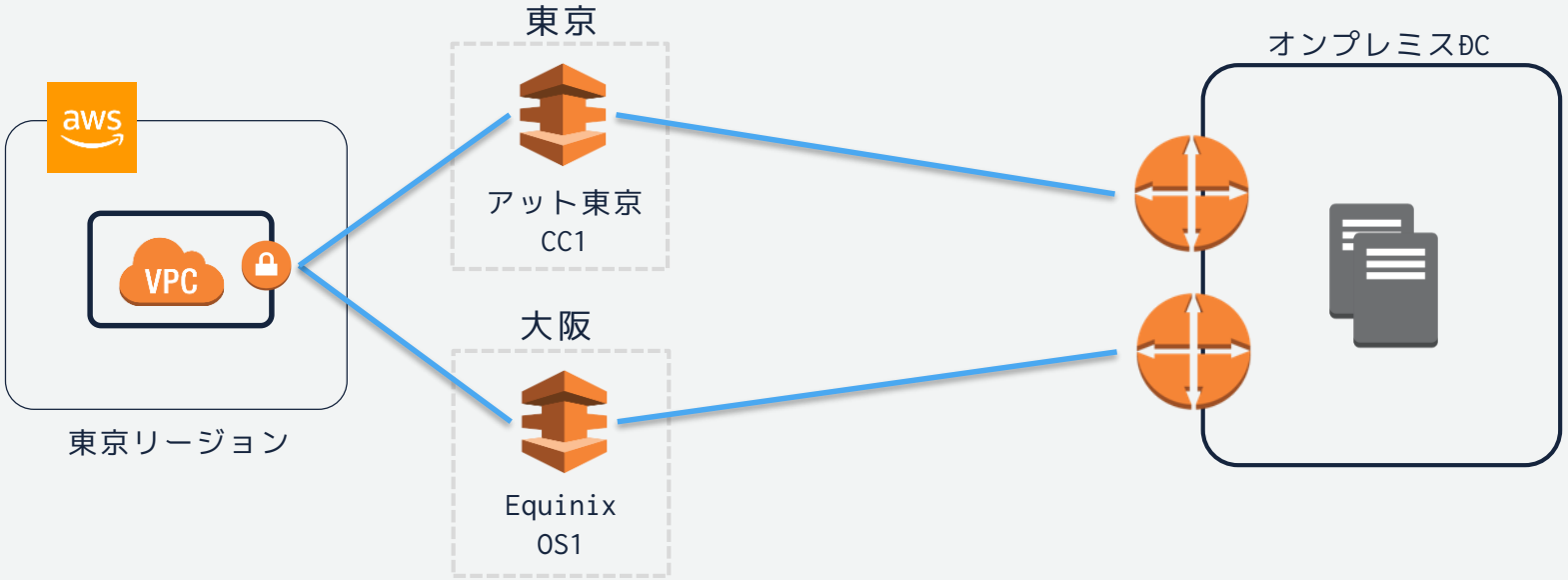
高可用性のためにDirect Connectを冗長化する場合は**異なるロケーションへの分散**が基本

東京内の異なるDirect Connectロケーションを用いた冗長構成の例



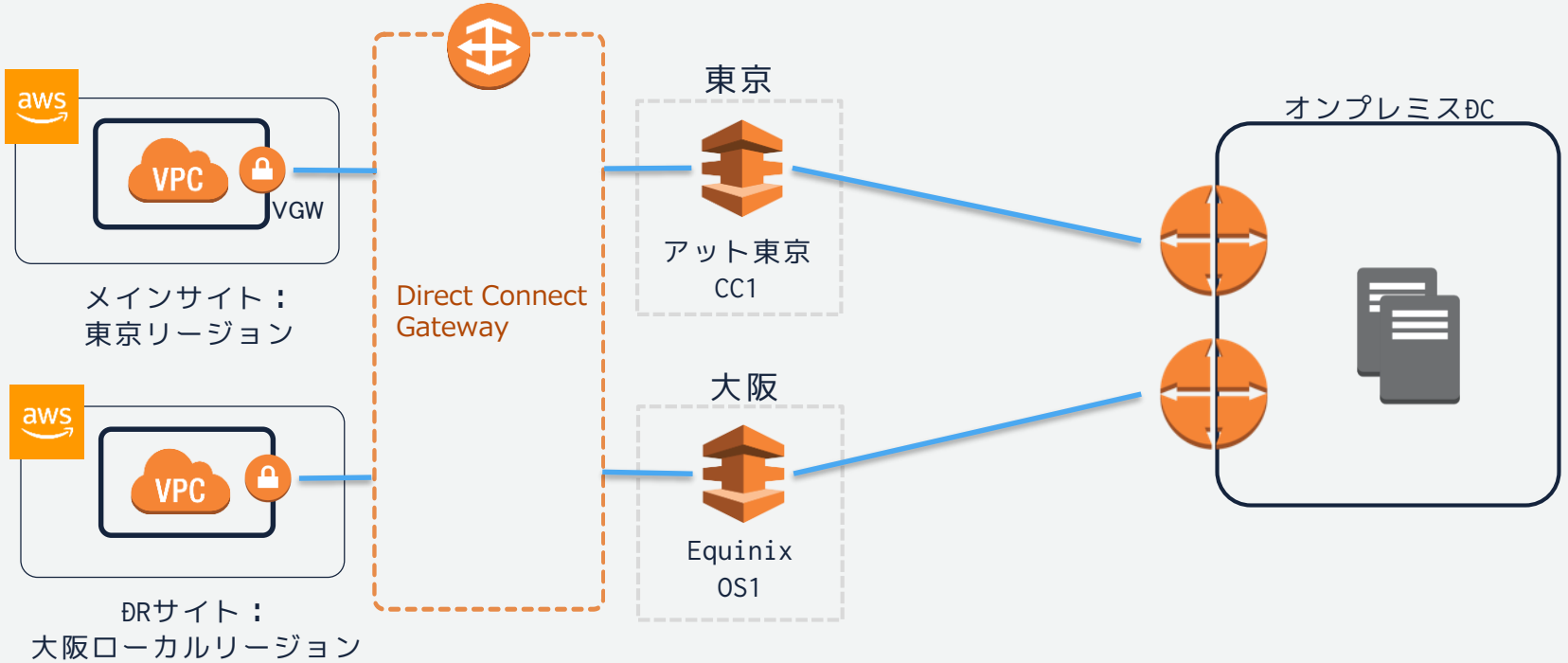
デュアルロケーション（東阪で分散）

東阪に分散したDirect Connectロケーションを用いた冗長構成の例



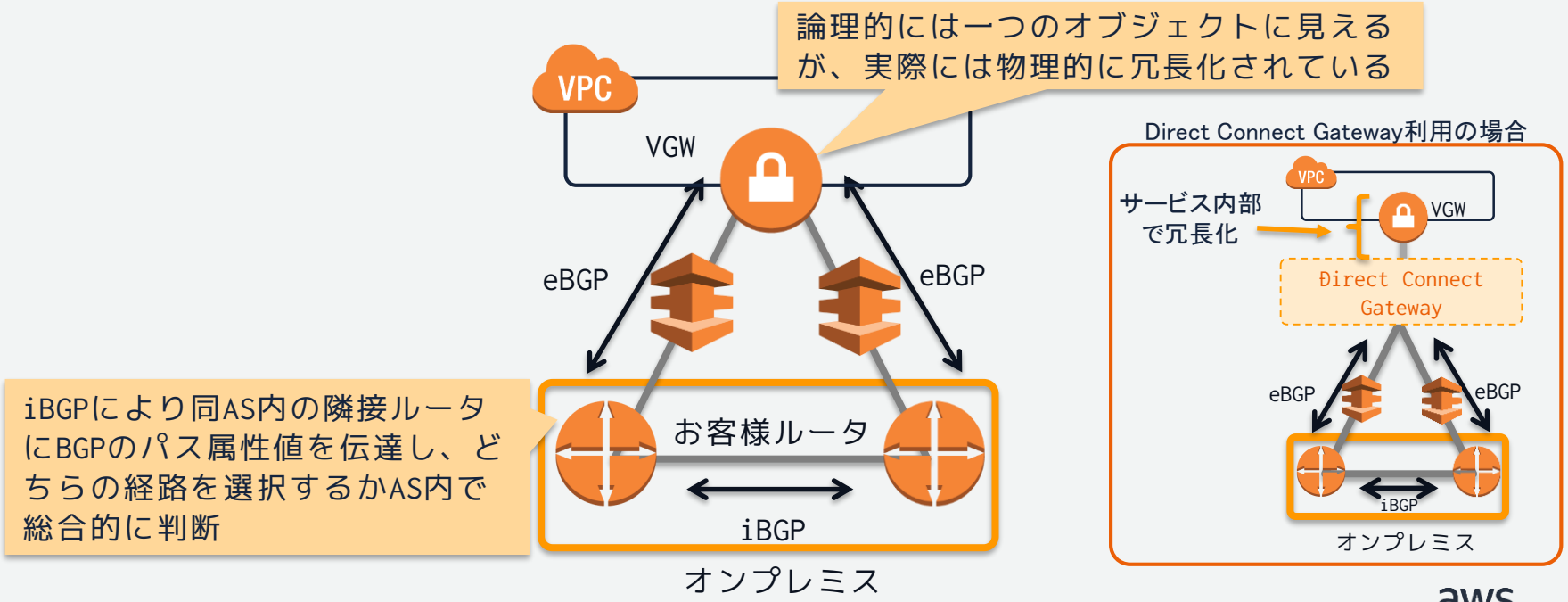
デュアルロケーション（東阪分散＋大阪ローカルリージョン）

ダイレクトコネクトゲートウェイを用いて大阪ローカルリージョンへ接続する構成例



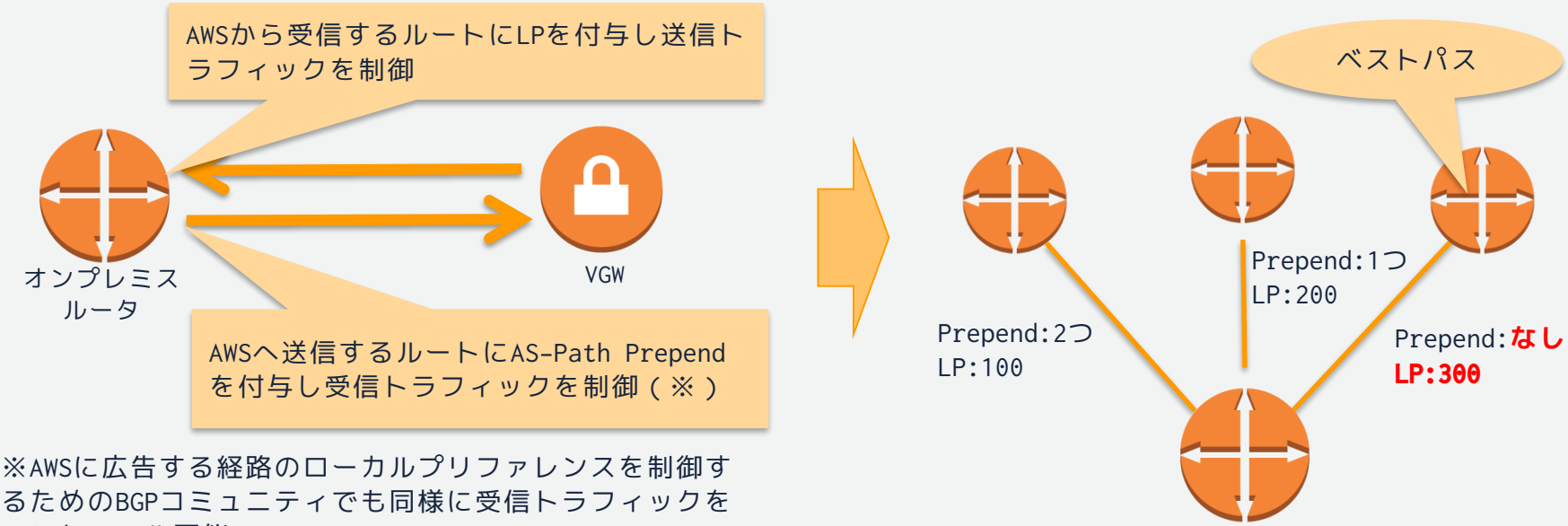
冗長構成における経路制御

- VPC上のVGW(Virtual Private Gateway)に複数のVritual Interface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



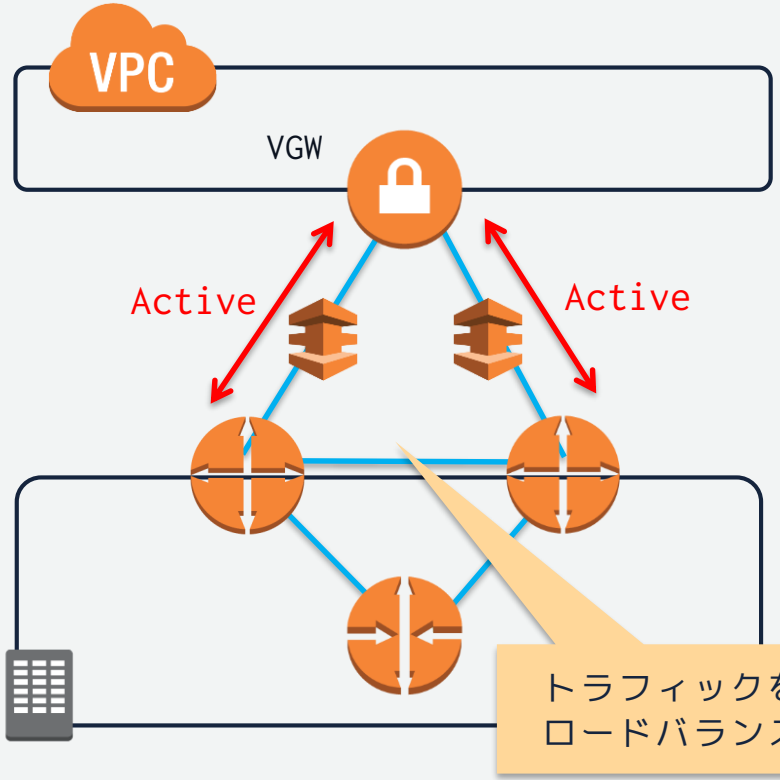
BGPパス属性を用いた経路制御

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コミュニティでも同様に受信トラフィックをコントロール可能

経路制御（Active/Active）



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として利用

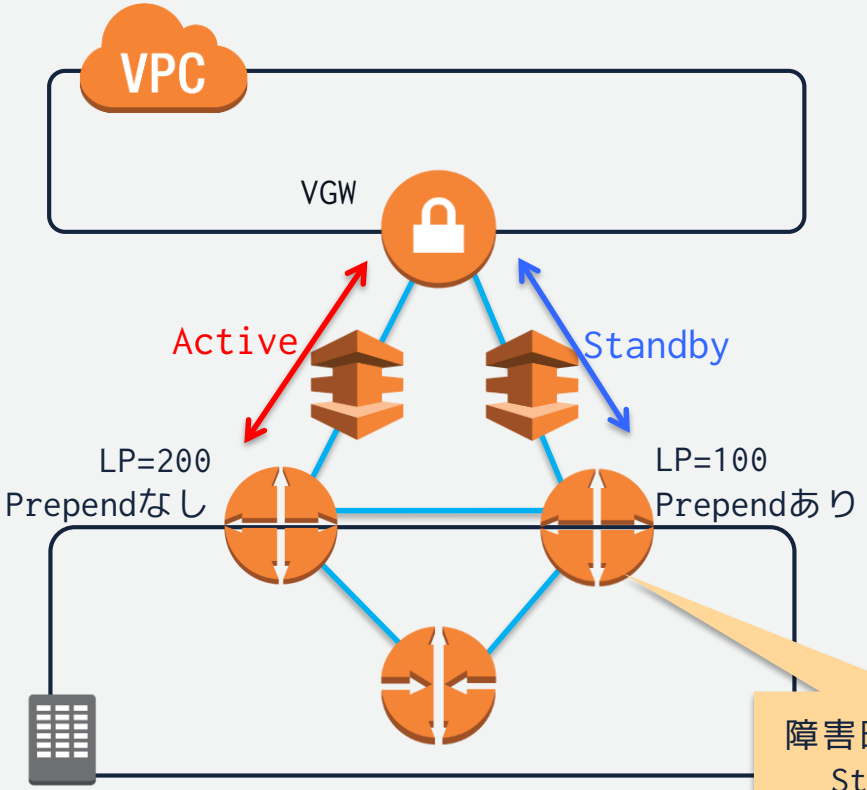
それぞれのルータで以下が等しくなるようにする必要がある.

- 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

https://aws.amazon.com/jp/directconnect/faqs/ Q.Direct Connect プライベート仮想インターフェイスでは、どのようなローカルプリファレンスコミュニティがサポートされていますか?

経路制御（Active/Standby）

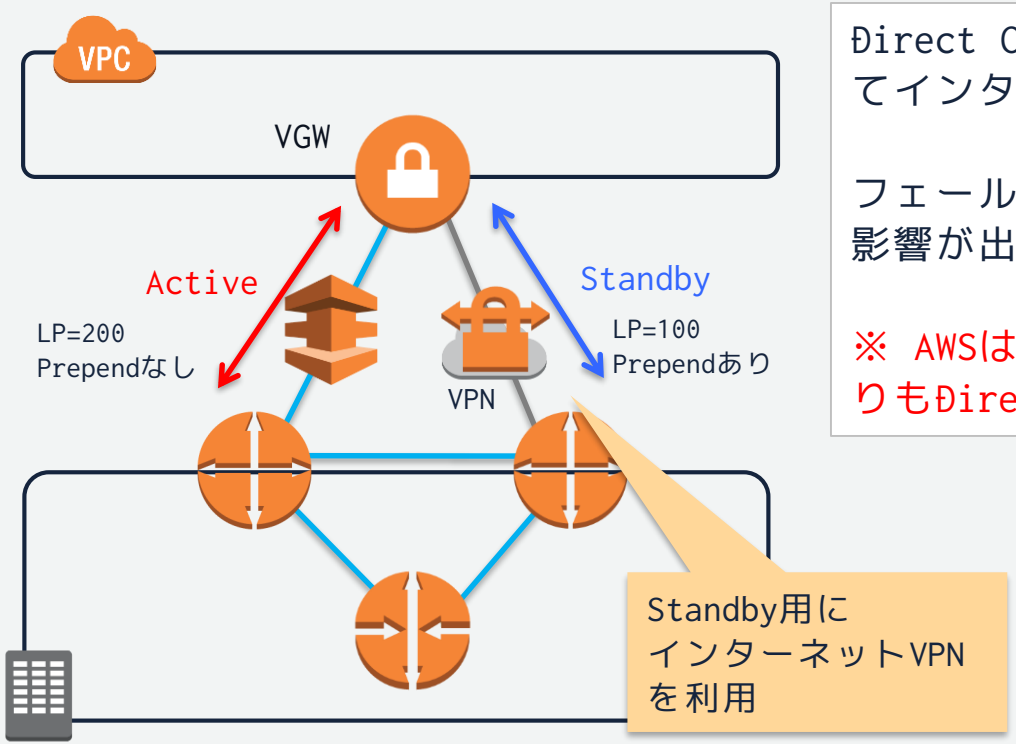


Direct Connect２本のどちらかを通常利用とし、障害時はStandby側へ自動切り替えを行う

それぞれのルータで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ルートの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）

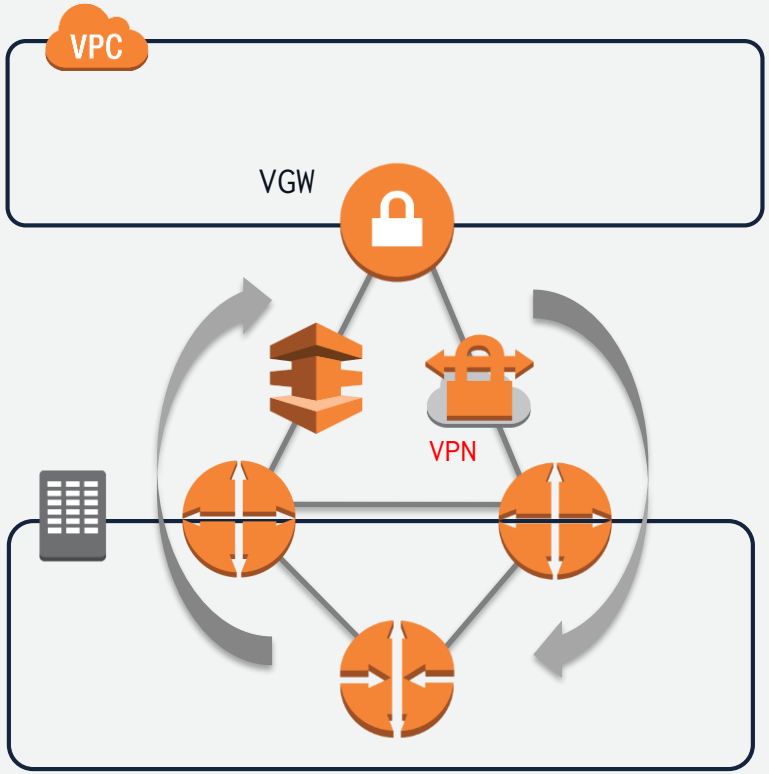


Direct Connect障害時のバックアップとしてインターネットVPNを利用

フェールオーバー時にはパフォーマンスに影響が出る場合があるため注意

※ AWSは（パス属性によらず）常にVPNよりもDirect Connectを優先経路とする

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）は問題なく通信可能

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（パケット破棄）

https://aws.amazon.com/jp/premiumsupport/knowledge-center/configure-vpn-backup-dx/

Agenda

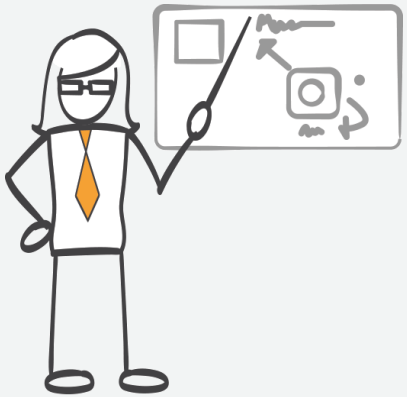
- クラウドとは
  - クラウドのネットワークAmazon Virtual Private Cloud(VPC)
  - VPCにおけるルーティング
- 特性を考えたネットワーク
  - リージョンとアベイラビリティゾーンを理解する
  - 設計を柔軟に考える
  - セキュリティフィルタ、ACLの考え方：セキュリティグループとNetwork ACL
- オンプレミス環境とAWSクラウドの接続
  - Direct Connect　プライベート接続とパブリック接続
  - 高可用性
- よくある落とし穴
- まとめ

よくある落とし穴

よくある落とし穴

- OSPFやVRRPで冗長化したい
  - VPCではマルチキャストは未サポート
  - サービス自身が冗長化していたり他の方法で冗長できるのでホワイトペーパーを見る
- L2延伸をしたい
  - VPCはLayer3で構成される。L2延伸はサポートしない
  - 基本的にL3前提で組み直す。
  - どうしても必要な場合はトンネルやVMware Cloud on AWSの検討を

まとめ



クラウド特有のネットワークに慣れる

従来の設計や運用を見直す

クラウドにあわせたネットワークの作り方を理解する

という訳でオンプレミス側を篠宮さんへ