AWS
Black Belt
Online Seminar

【AWS Black Belt Online Seminar】
発注者のためのAWSネットワーク入門

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

2018.05.15

内容についての注意点

- 本資料では2018年05月15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.

自己紹介

名前：菊池　之裕(きくち　ゆきひろ)

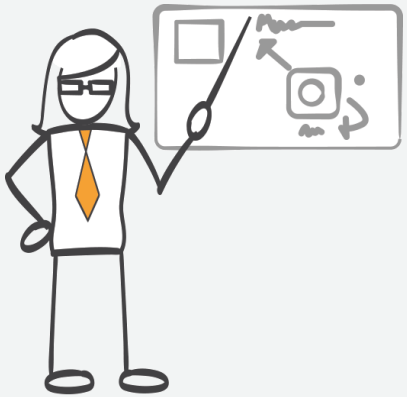
所属：アマゾン ウェブ サービス ジャパン株式会社
　　ソリューションアーキテクト　ネットワークスペシャリスト

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,Market Place

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

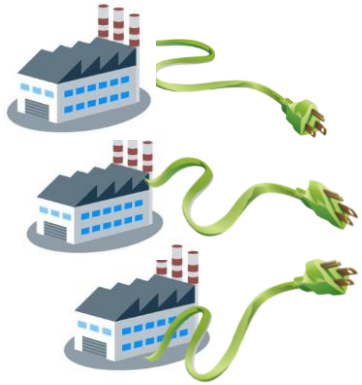
Agenda

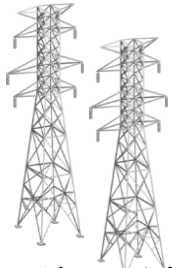
クラウドとは
クラウドのネットワーク
Amazon Virtual Private Cloud(VPC)
発注を考えたときのネットワーク
    特性を考えたネットワーク
    設計を柔軟に考える
    専用線の考え方
まとめ

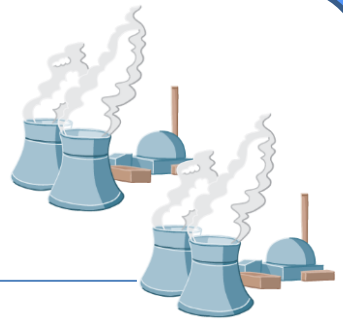
クラウドとは

いつでも、必要なだけ、低価格で

電気







コンピュータ

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

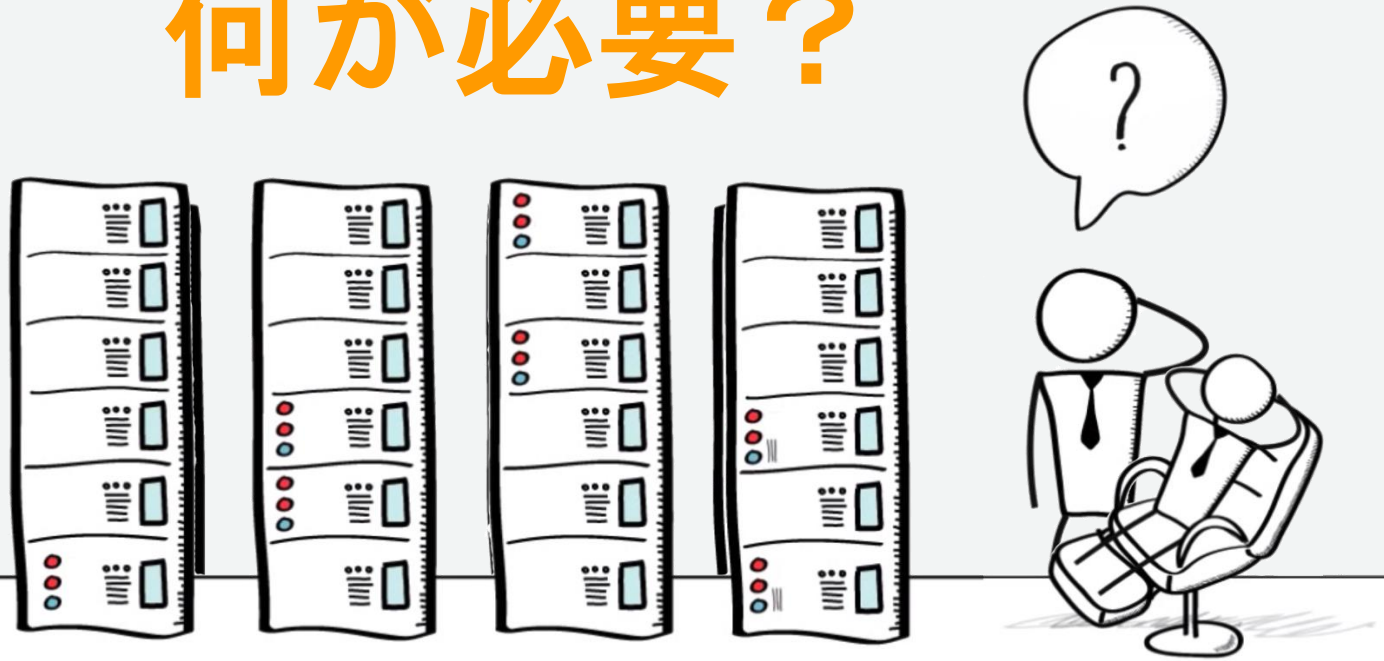
スケールアップ
ダウンが容易

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？



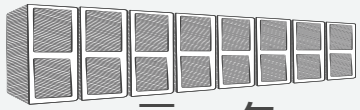
オンプレミス環境でのネットワークのイメージ

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

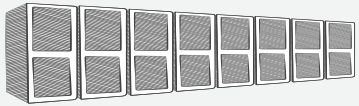
構築するには

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



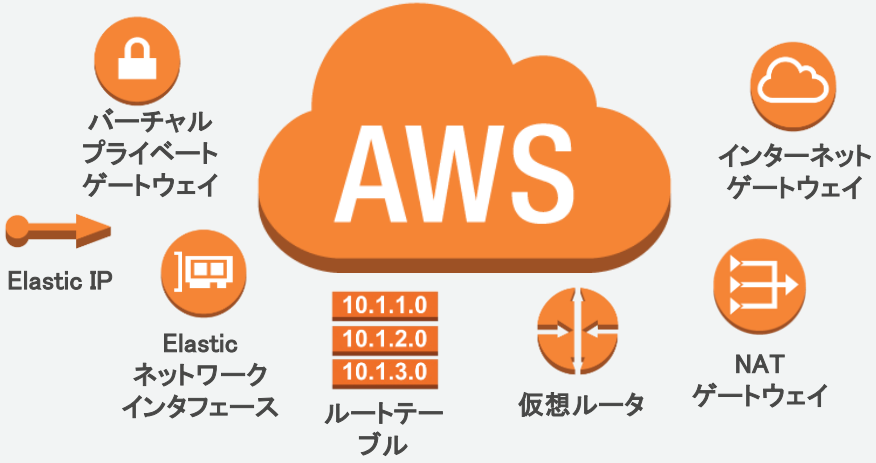
ラック

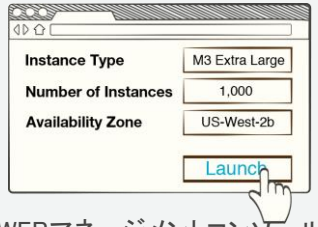
ネットワーク機器

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)

VPC設計のポイント

- CIDR(IPアドレス)は既存のVPC、社内のDC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

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

発注を考えたときのネットワーク

クラウドを新たに発注するには？

- いままでのオンプレミスのRFPやRFIを流用？
- サーバとストレージ、ネットワークだけを考える？

クラウドを新たに発注するには？

- いままでのオンプレミスのRFPやRFIを流用？
- サーバとストレージ、ネットワークだけを考える？

特性に合わせた新しい考え方を取り入れることが必要

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

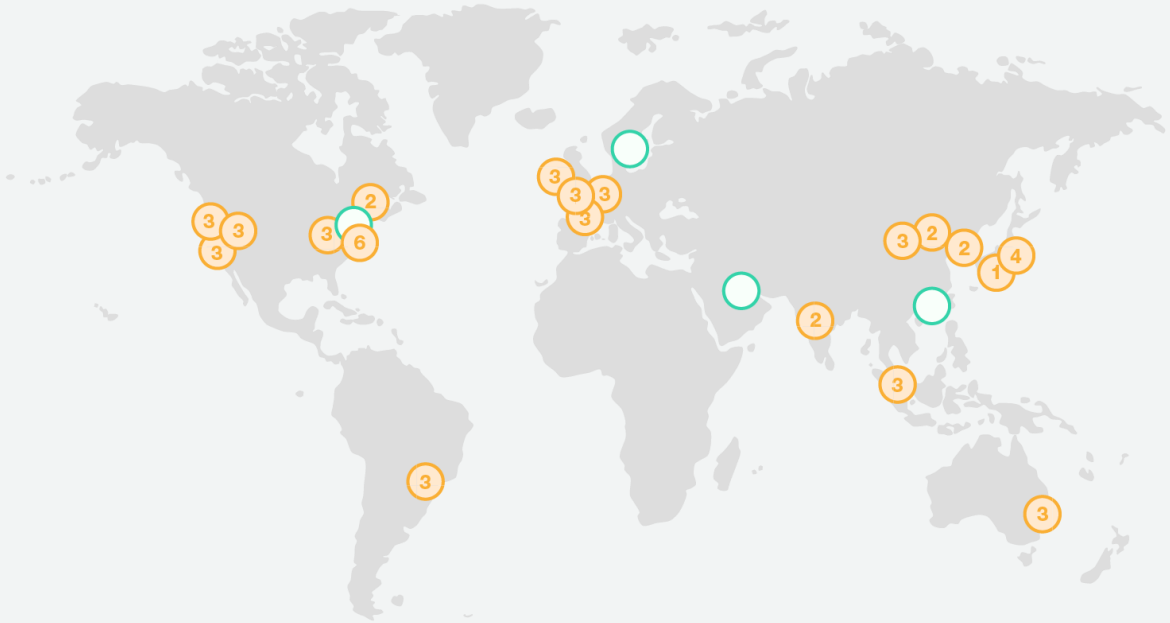
リージョン

18+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
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)**

＊GovCloudは米国政府関係企業用です。

55のアベイラビリティ・ゾーン（データセンター群）
105 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

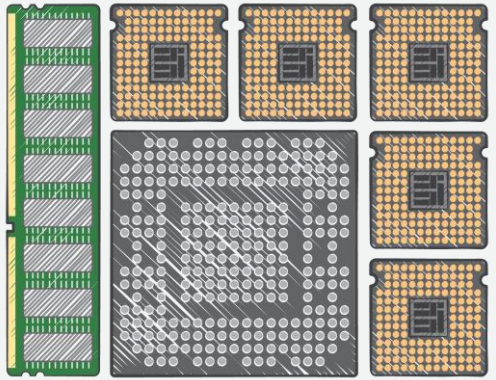
Design for Failureの考え方

- 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

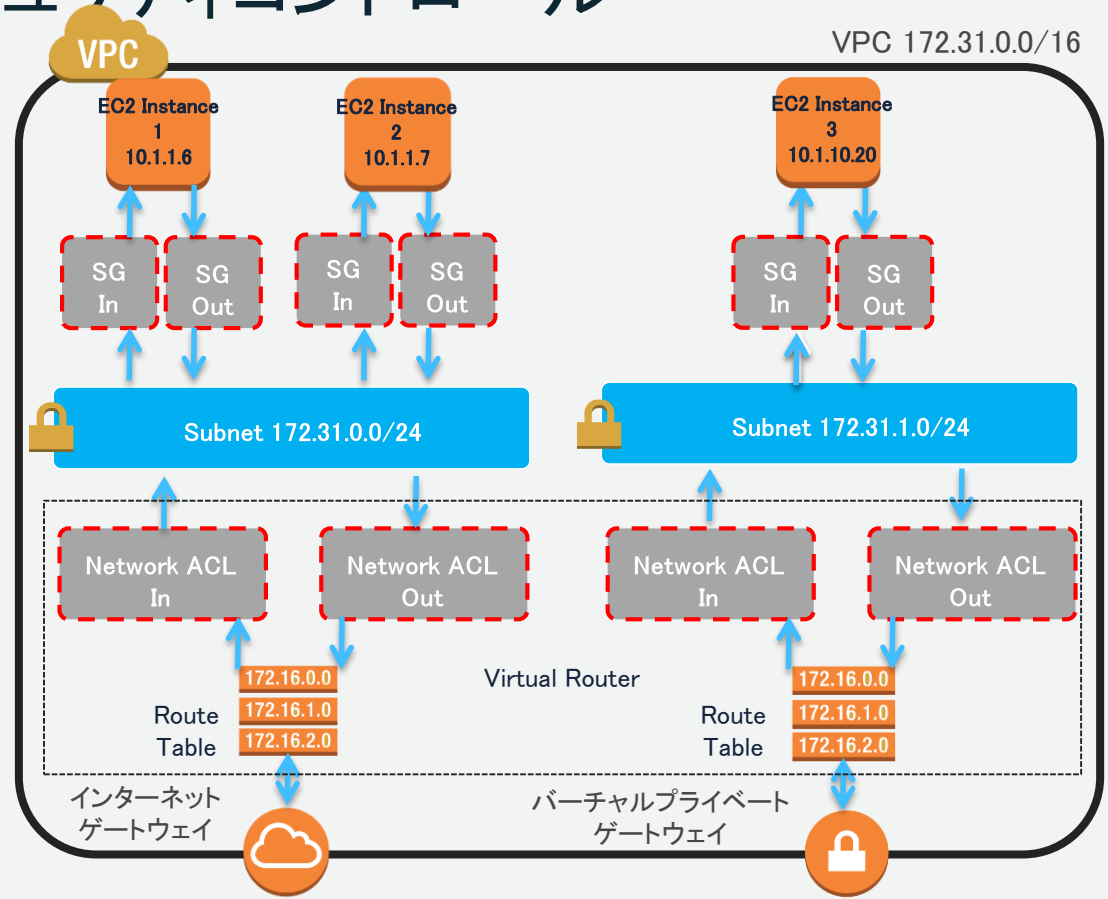
特性に合わせた新しい考え方を取り入れる

- 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がターゲットにできるのでIPを意識しない運用が可能

セキュリティグループ = ステートフル Firewall

Network ACLs = ステートレス Firewall

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 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 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 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 ればその管理下になる

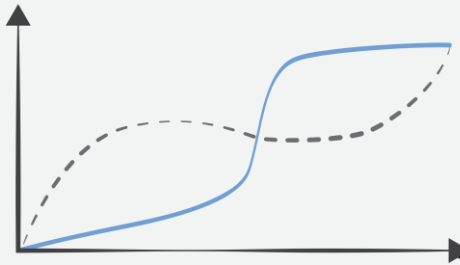
再掲：特性に合わせた新しい考え方を取り入れる

- 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

専用線の考え方

専用線(Direct Connect)はカジュアルに引ける

- フレッツを使ったサービスも存在
  - 開通に時間がかからない
- ルータの設定が面倒
  - SI込みのパートナーもある
- そんなに帯域を使わない
  - パートナーにより帯域を絞ったプランも提供

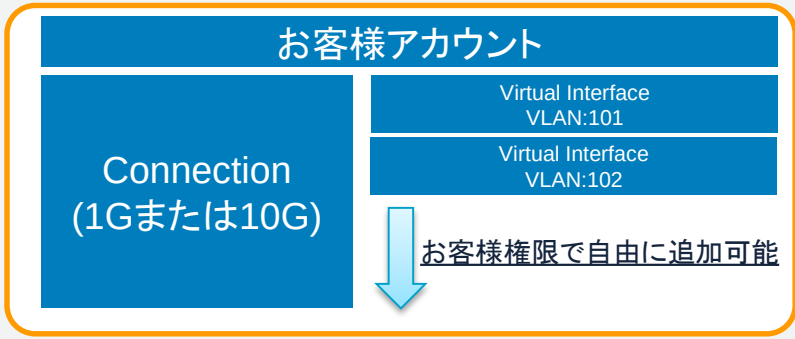


Direct Connect の提供形態とパートナー

パートナーの提供サービス(占有型・共有型)

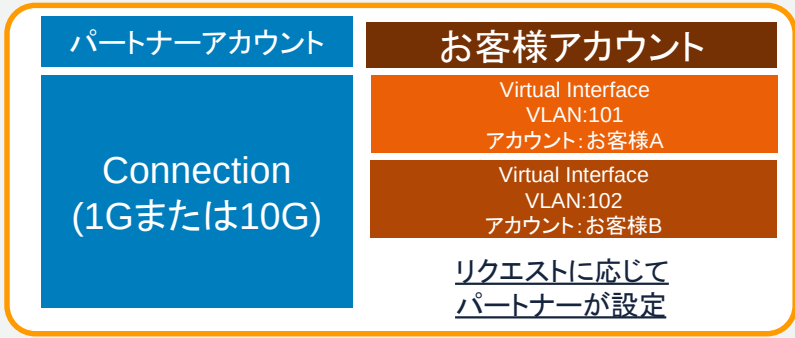
Direct Connect(占有型)

- Connectionをお客様へ提供
- Virtual Interfaceはお客様側で自由に設定可能



Direct Connect(共有型)

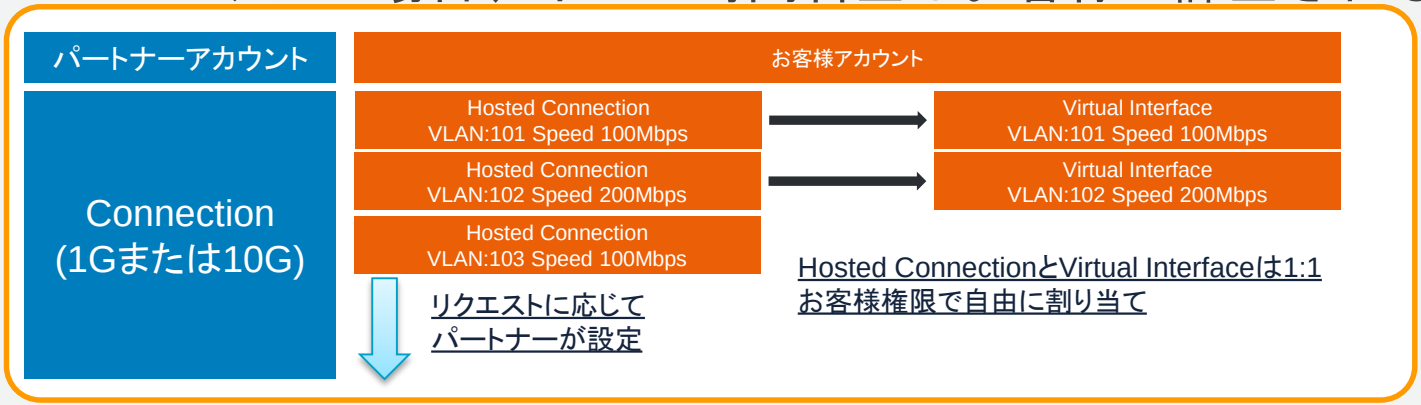
- Connectionはパートナーのアカウントで持つ
- Virtual Interfaceはお客様のリクエストベースでパートナーが設定



パートナーの提供サービス(共有型 Sub 1G)

Direct Connect(共有型　Sub 1G)

- Connectionはパートナーのアカウントで持つ
- Hosted Connectionと呼ぶ仮想的なConnectionをお客様へ提供
- Virtual InterfaceはHosted Connectionに紐付けされ追加可能
- このモデルの場合、ポート時間料金はお客様に課金される



パートナーにより拡張されたAWS Direct Connectサービス

相互接続ポイントにおける接続装置等の設置場所

- 専用線とのパッケージ提供する場合も

10Mbps, 100Mbps等1Gbps よりも狭帯域のサービス

お客様指定の場所から相互接続ポイントまでのアクセス

広域WANで複数拠点からAWSへの接続

パートナーの提供サービス

- Direct Connectが使えるデータセンターの提供
- 相互接続ポイントにおけるコロケーション提供
- 相互接続ポイント込みの専用線サービス提供
- 相互接続ポイント込みの広域ネットワークサービス提供
- 相互接続ポイント込みのモバイル網への接続

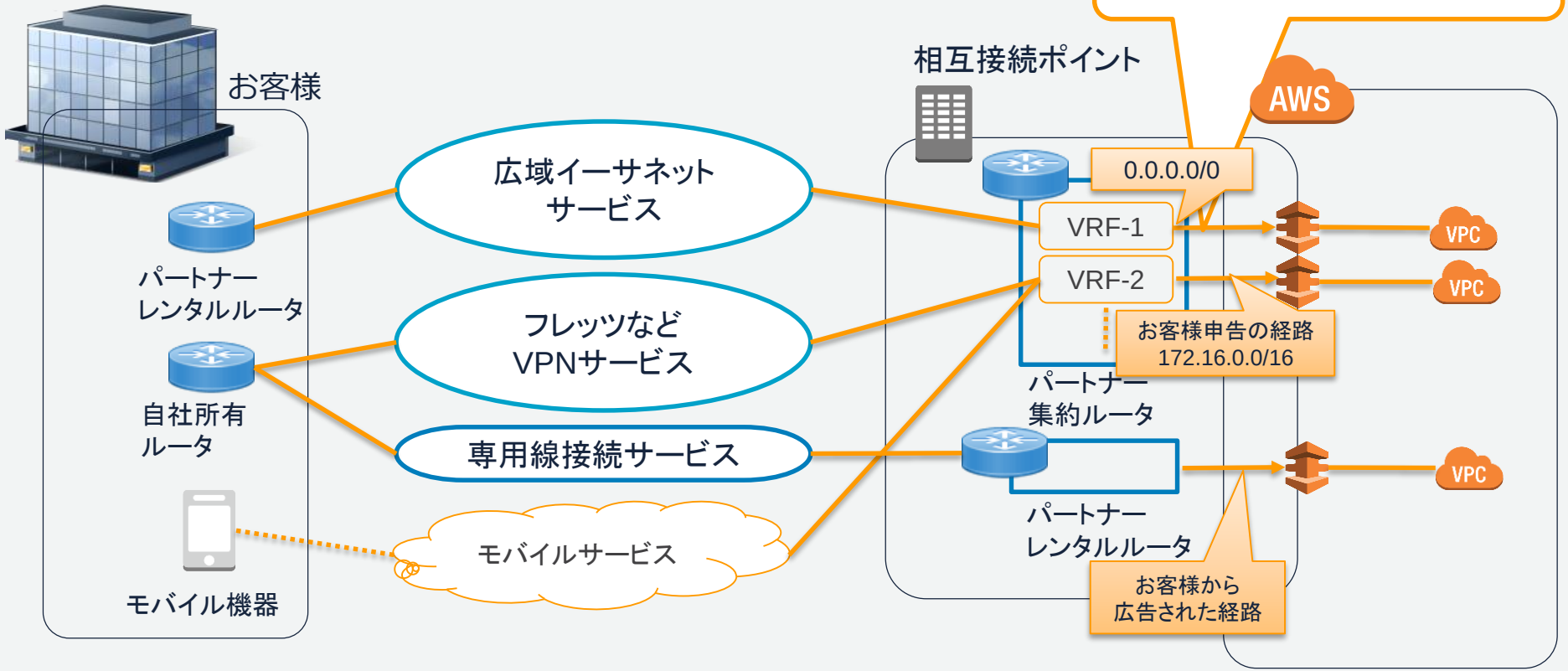
ルータレンタル、マネージドサービスなど各社により提供

https://aws.amazon.com/jp/directconnect/partners/#apac

パートナー経由のDirect Connect

- 共有モデル
  - 1契約あたり1バーチャルインターフェイスが基本
    - 冗長化では2バーチャルインターフェイスが必要
  - ベストエフォートとギャランティ
  - 通信料固定のものと従量のものがある
    （別途パートナーへご確認ください）
  - Sub1Gでは従量課金になる
- 専有モデル
  - 1契約で複数のバーチャルインターフェイスへの接続が可能（最大50）
  - 1Gもしくは10G
  - 接続料金は従量でAWSアカウントに請求される

パートナー経由のDirect Connect



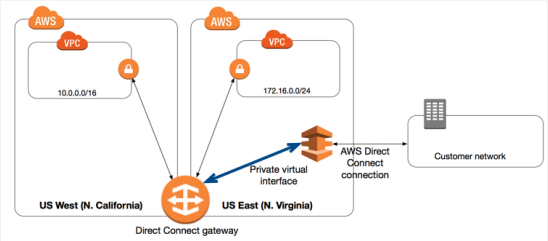
パートナー経由のDirect Connectの注意点

- VPCへの経路広報のタイプが異なる
  - エッジルータからの経路情報をVPCへそのままフォワードせず、ある程度の集約がかかるサービスがある
  - デフォルトが広報されるもの
  - 申告した経路が集約されるもの

冗長を取る場合、経路の偏りの原因となるので、サービスの確認を

Direct Connect Gateway

- Direct Connect GatewayがHubになり、同一アカウントに所属する**複数のリージョン**の**複数のロケーション**から**複数リージョン**の**複数のVPC**に接続できる機能。
    - Direct Connectから世界の全リージョン（中国除く）のVPCに接続することができる。
    - 1つのDirect Connectの仮想インターフェイスから複数のVPCに接続することができる。
    - 複数のDirect Connectの仮想インターフェイスをDirect Connect Gatewayに接続することができる。



1つ以上のDirect Connect ロケーションに繋げば
全世界の全リージョン（中国除く）に閉域網接続でき
同一リージョンまたは世界の複数リージョンをまたいで複数のVPCに接続できる機能

Direct Connect選択のポイント

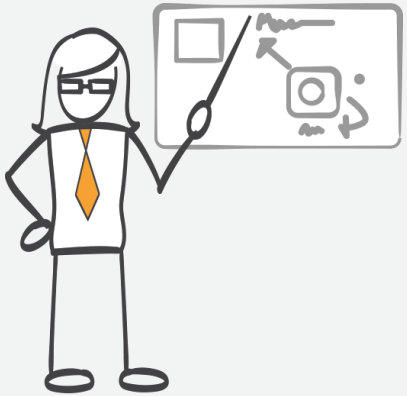
- 占有型は高価ではない
  - 3本以上共有型を引くと価格が逆転する場合も
- Direct Connect Gatewayを活用しよう
  - 複数のVPCを1つの仮想インターフェイスに集約できる
  - 全世界のリージョンが使えるので、専用線費用の節約も
  - レイテンシを気にしなければ、海外リージョンを使う
    - インスタンスが安かったり、東京リージョンにないサービスが使える

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 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

オンラインセミナー資料の配置場所

AWS クラウドサービス活用資料集

- https://aws.amazon.com/jp/aws-jp-introduction/

AWS Solutions Architect ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています。
- https://aws.amazon.com/jp/blogs/news/
- http://aws.typepad.com/sajp/

公式Twitter/Facebook
AWSの最新情報をお届けします

@awscloud_jp

もしくは
http://on.fb.me/1vR8yWm

最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！

お問い合わせ先

AWS導入に関しての問い合わせ
http://aws.amazon.com/jp/contact-us/aws-sales

(ご利用者様向け)課金・請求内容、アカウントに関するお問い合わせ
https://aws.amazon.com/jp/contact-us/

AWS技術サポート
https://aws.amazon.com/jp/premiumsupport/