



# 【AWS Black Belt Online Seminar】

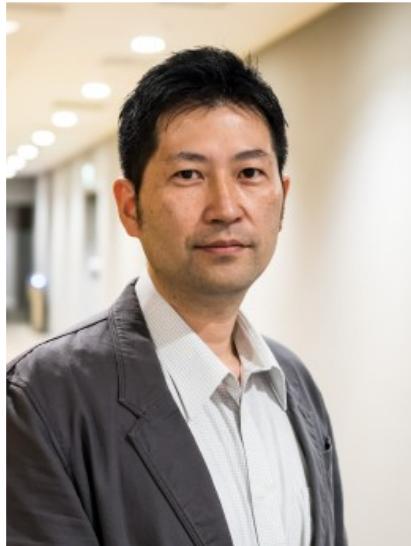
## Amazon Virtual Private Cloud (VPC)

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 益子 直樹

2017.04.12

# 自己紹介



名前：益子 直樹（ましこ なおき）

所属：アマゾンウェブサービスジャパン  
ソリューションアーキテクト

ロール：製造業、製薬業界のお客様を中心にご支援

経歴：通信キャリアで広域イーサやISPの  
バックボーン設計開発や運用を担当

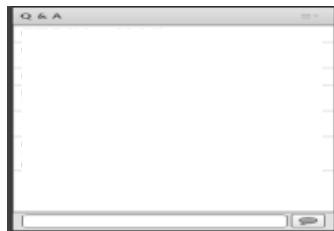
好きなAWSサービス： VPC  
Direct Connect  
CloudFormation

# AWS Black Belt Online Seminar へようこそ！

質問を投げることができます！

- Adobe ConnectのQ&Aウィンドウから、質問を書き込んでください。  
(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ください。
- Twitterへツイートする際はハッシュタグ **#awsblackbelt** をご利用ください。

①Q&Aウィンドウ  
右下のフォームに  
質問を書き込んで  
ください



②吹き出しマークで  
送信してください

# AWS Black Belt Online Seminar とは

AWSJのTechメンバがAWSに関する様々な事を紹介するオンラインセミナーです

## 【火曜 12:00~13:00】

主にAWSのソリューションや  
業界カットでの使いどころなどを紹介  
(例：IoT、金融業界向け etc.)

## 【水曜 18:00~19:00】

主にAWSサービスの紹介や  
アップデートの解説  
(例：EC2、RDS、Lambda etc.)



※開催曜日と時間帯は変更となる場合がございます。

最新の情報は下記をご確認下さい。

オンラインセミナーのスケジュール&申し込みサイト

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

# 内容についての注意点

- 本資料では2017年4月12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.

# このセミナーのゴール

- VPCのコンセプトに慣れる
- 基本的なVPCのセットアップが出来るようになる
- 自社の要件にあった仮想ネットワークの作り方を理解する



# Agenda

- Amazon VPCとは？
- VPCのコンポーネント
- オンプレミスとのハイブリッド構成
- VPCの設計
- VPCの実装
- VPCの運用
- まとめ



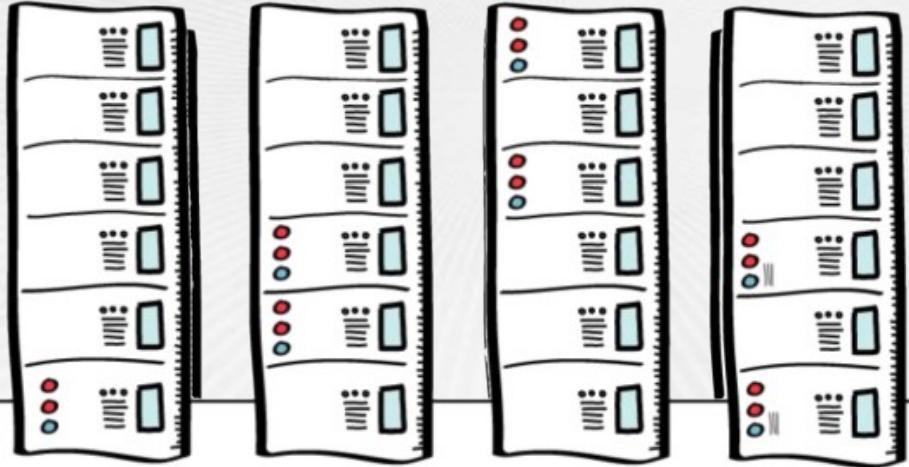
# Agenda

- **Amazon VPCとは？**
- VPCのコンポーネント
- オンプレミスとのハイブリッド構成
- VPCの設計
- VPCの実装
- VPCの運用
- まとめ



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

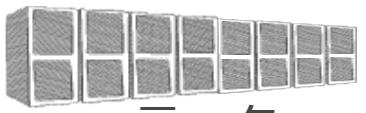


土地、電源、UPS、ラック、空調、ラック、ファイバー、パッチパネル、SFP等IFモジュール、スイッチ、ルータ、ストレージ、サーバ、ロードバランサー、ファイアーウォール、WAF、遠隔操作用ターミナルサーバ・・・・

# Before



データセンター

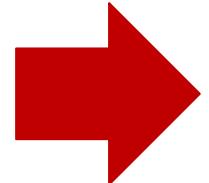


ラック

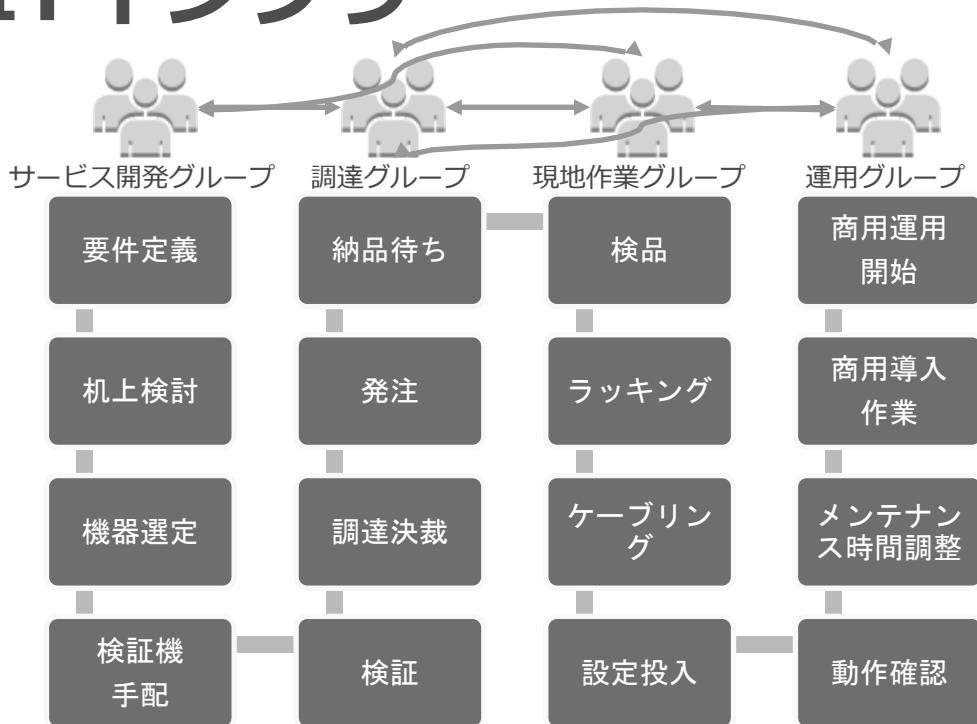


ネットワーク機器

## 従来のITインフラ



構築するには



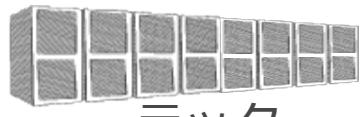
時間（＝コスト）がかかる  
早くても数ヶ月、長いと半年

# After

## クラウドで仮想ネットワークを構築



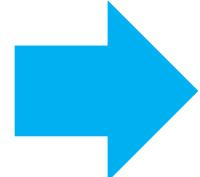
データセンター



ラック



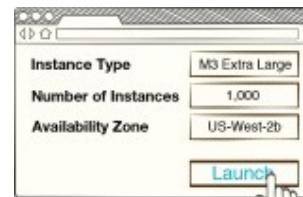
ネットワーク機器



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アウトは大丈夫？

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)

# Agenda

- Amazon VPCとは？
- **VPCのコンポーネント**
- オンプレミスとのハイブリッド構成
- VPCの設計
- VPCの実装
- VPCの運用
- まとめ

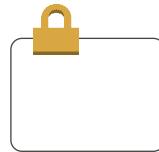




# 様々なコンポーネントを用意



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

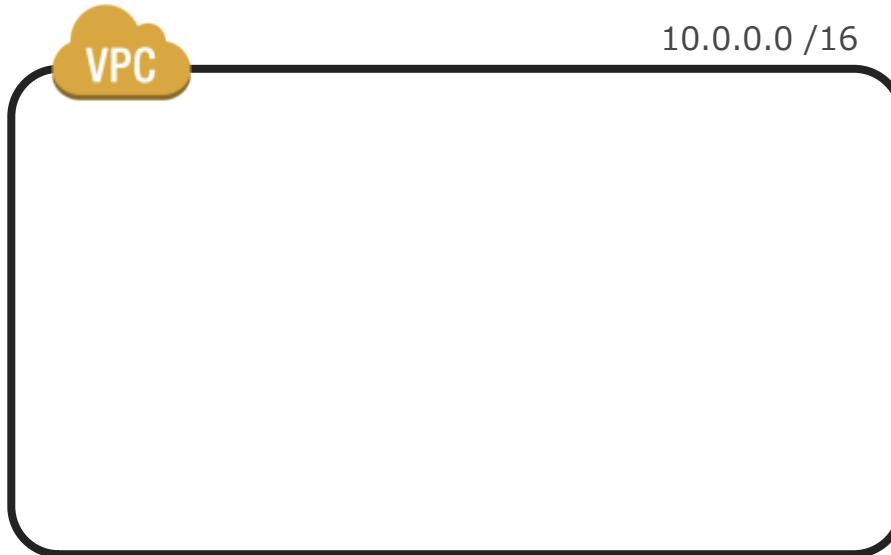


Elastic  
ネットワーク  
インターフェース



Elastic  
ネットワーク  
アダプタ

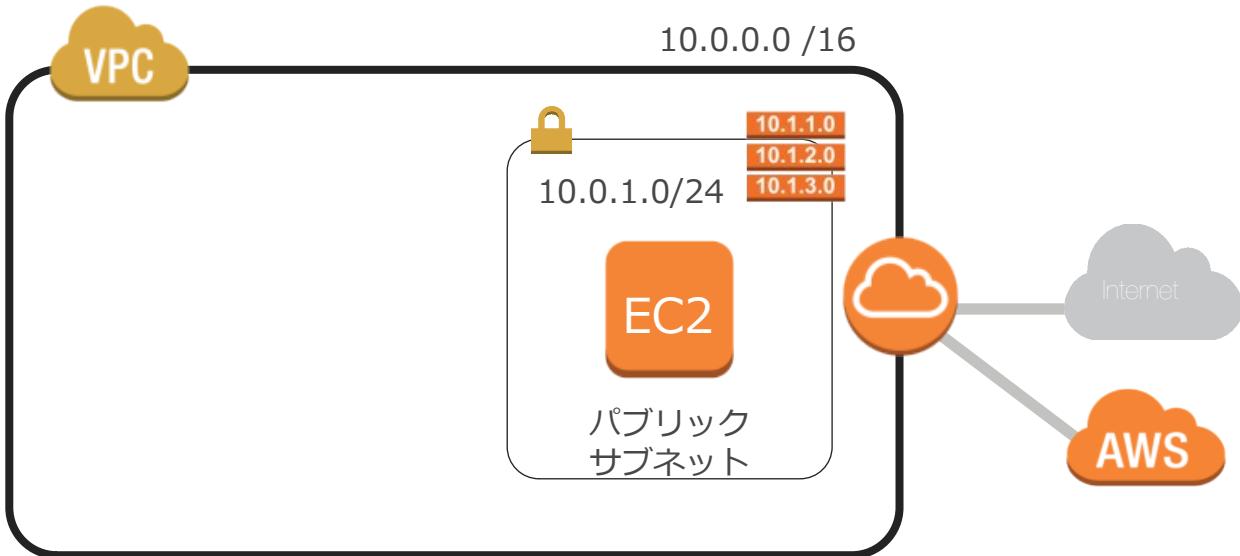
# まずは全体のネットワーク空間をVPCとして定義



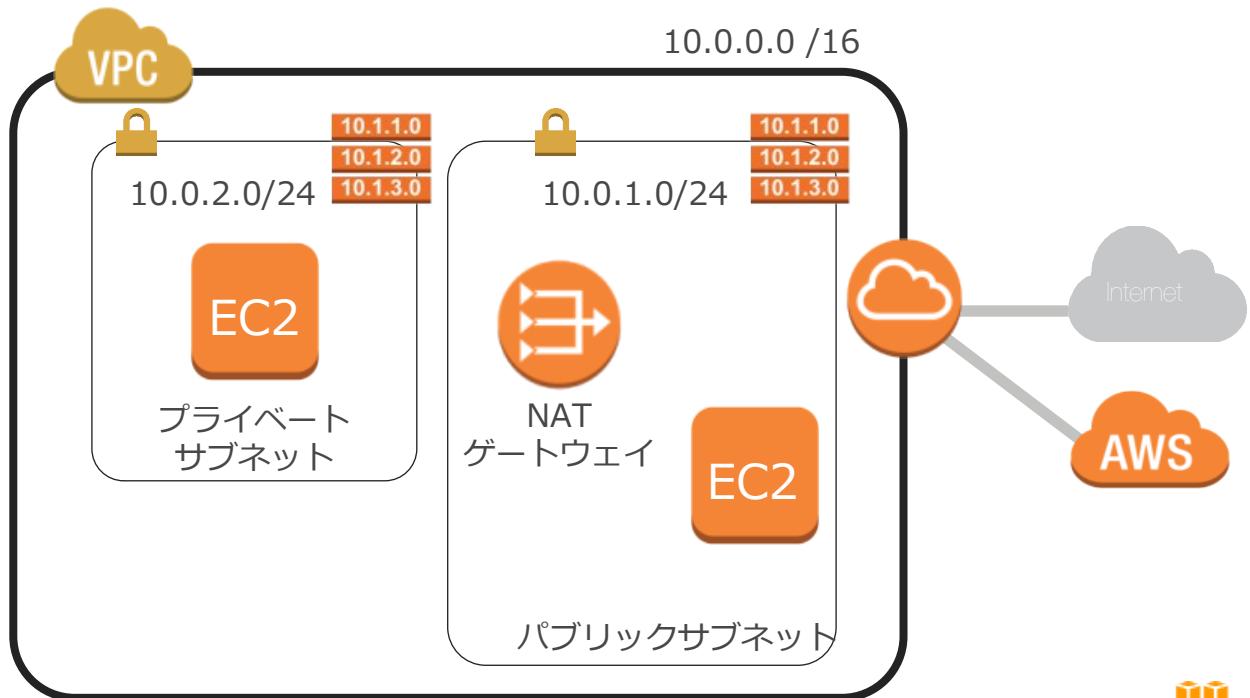
# 利用するサブネットを定義



# インターネットへの接続を設定



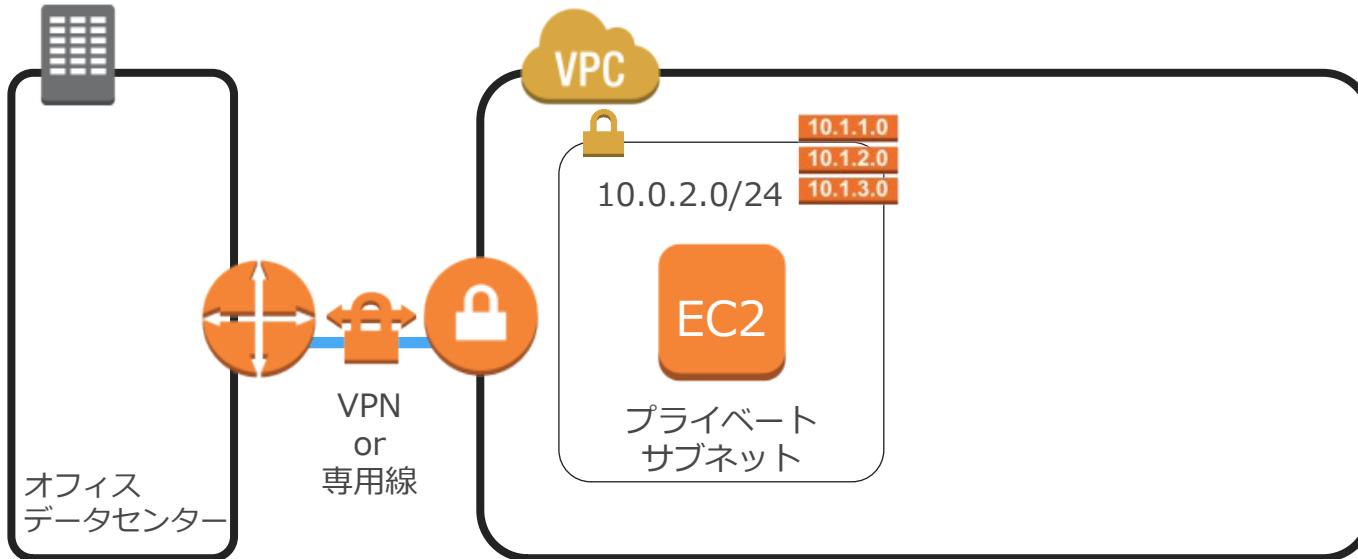
# プライベートサブネットを追加



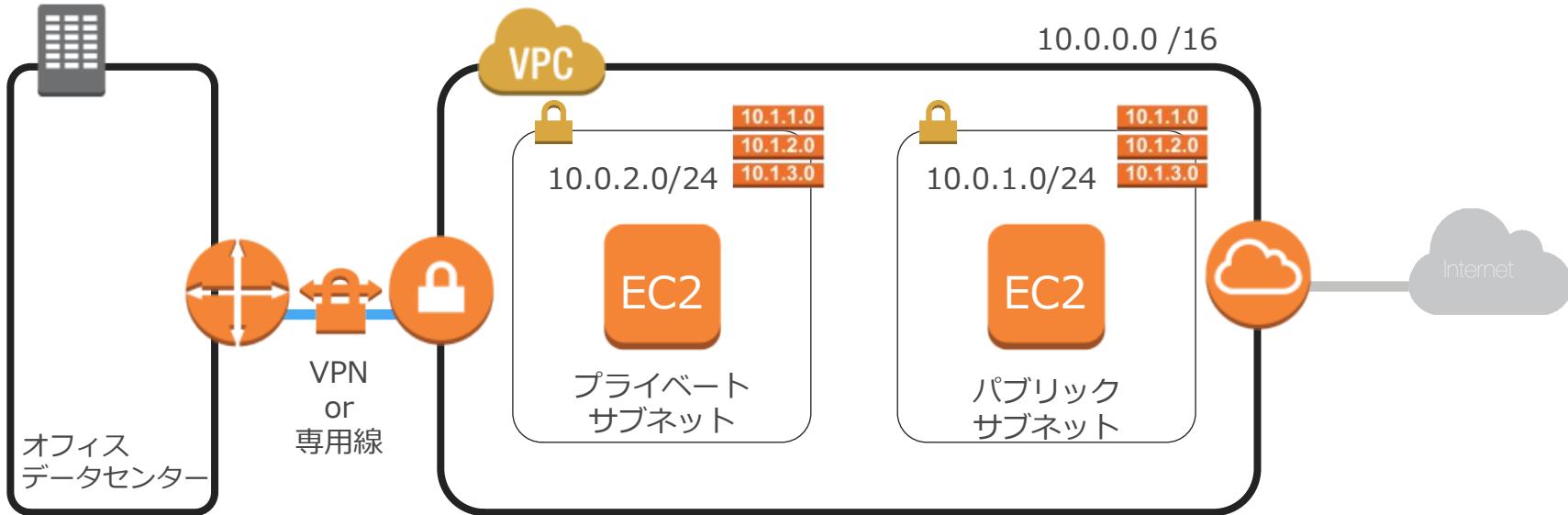
# インターネットに接続しないネットワークも作成可能



# オンプレミスとの接続



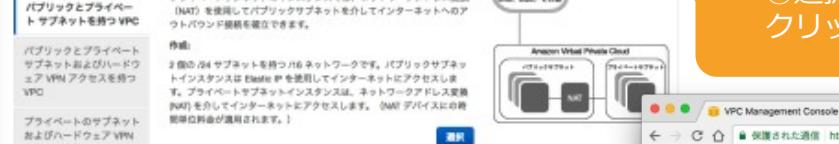
# ネットワーク要件に応じて自由に設定可能



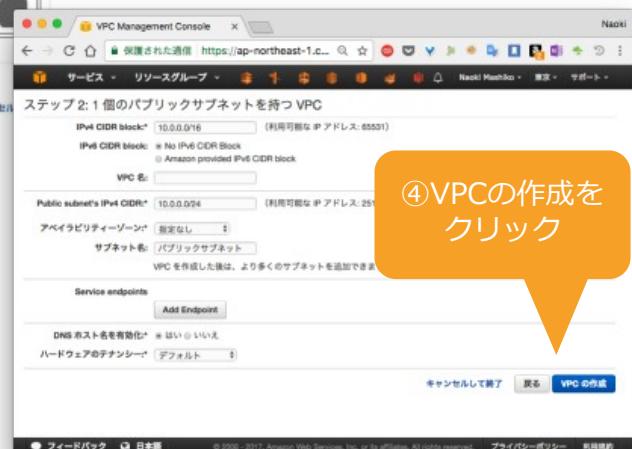
# VPC ウィザードで数画面で作成可能



②希望のパターンを選択



③選択をクリック

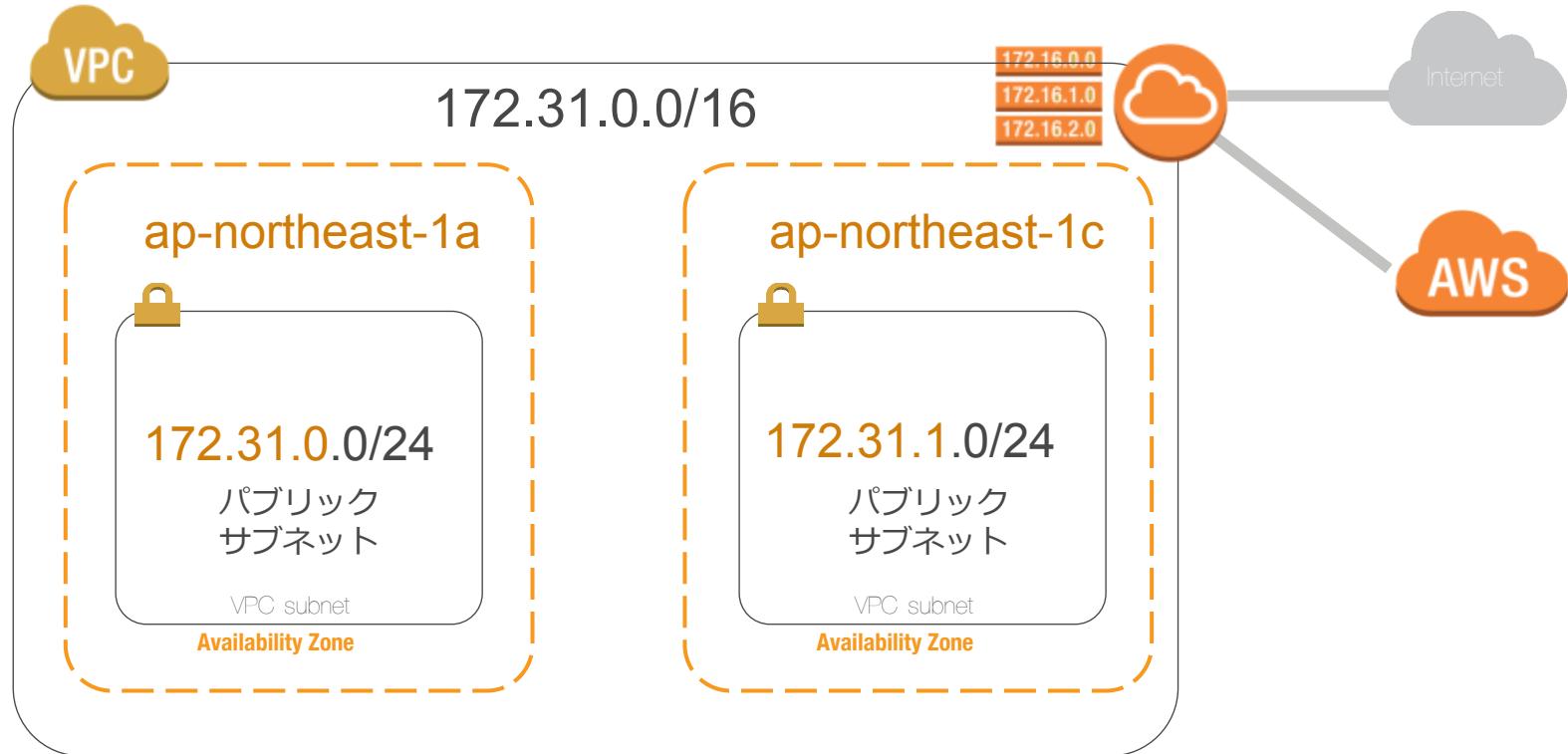


④VPCの作成をクリック



# ウォークスルー： インターネット接続VPCセットアップ<sup>®</sup>

# インターネットへの接続を設定するVPCを作成



# インターネット接続VPCのステップ<sup>°</sup>

①



アドレスレンジを  
選択

②



Availability Zone  
におけるSubnetを  
選択

③



インターネットへの  
経路を設定

④



VPCへのIN/OUT  
トラフィックを許可

# インターネット接続VPCのステップ<sup>°</sup>

①



アドレスレンジを  
選択

②



Availability Zones  
におけるSubnetを  
選択

③



インターネットへの  
経路を設定

④



VPCへのIN/OUT  
トラフィックを許可

# CIDR表記の再確認（Classless Inter-Domain Routing）

以前のアドレス体系はクラスフルだった（IPv4の32ビットアドレス空間を8ビットで区切る）

クラスA・・・16,777,214個 ( $2^{24}-2$ )

クラスB・・・65,534個 ( $2^{16}-2$ )

クラスC・・・254個 ( $2^8-2$ )

クラスBだと多過ぎ、クラスCだと少な過ぎる場合など実際の組織のホスト数に柔軟合わせたい

CIDR レンジのサンプル:

172.31.0.0/16

8/16/24のいずれかではなく、可変長のビットマスクで必要に応じたアドレッシングが可能になった



10101100 00011111 11000000 00000000

ネットワークアドレス部

ホストアドレス部

※RFC(1518/1519を経て4632)にて定義

# 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

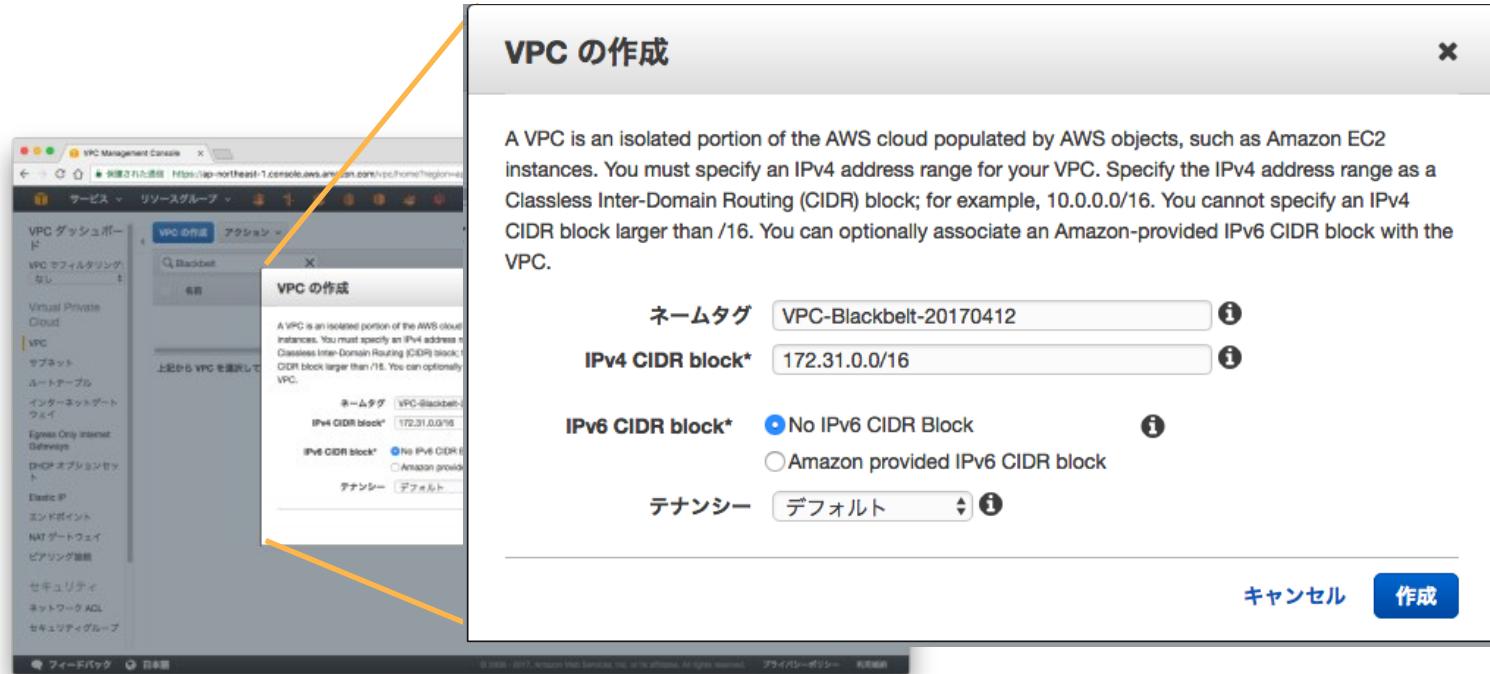
172.31.0.0/16

推奨: RFC1918レンジ

推奨:/16  
(65,534アドレス)

作成後変更はできないので注意が必要

# VPCの作成



The screenshot shows the AWS VPC Management Console interface. On the left, there's a sidebar with various VPC-related options like 'Virtual Private Cloud', 'Subnets', 'Route Tables', etc. In the center, a modal window titled 'VPC の作成' (Create VPC) is open. The modal contains the following information:

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Form fields:

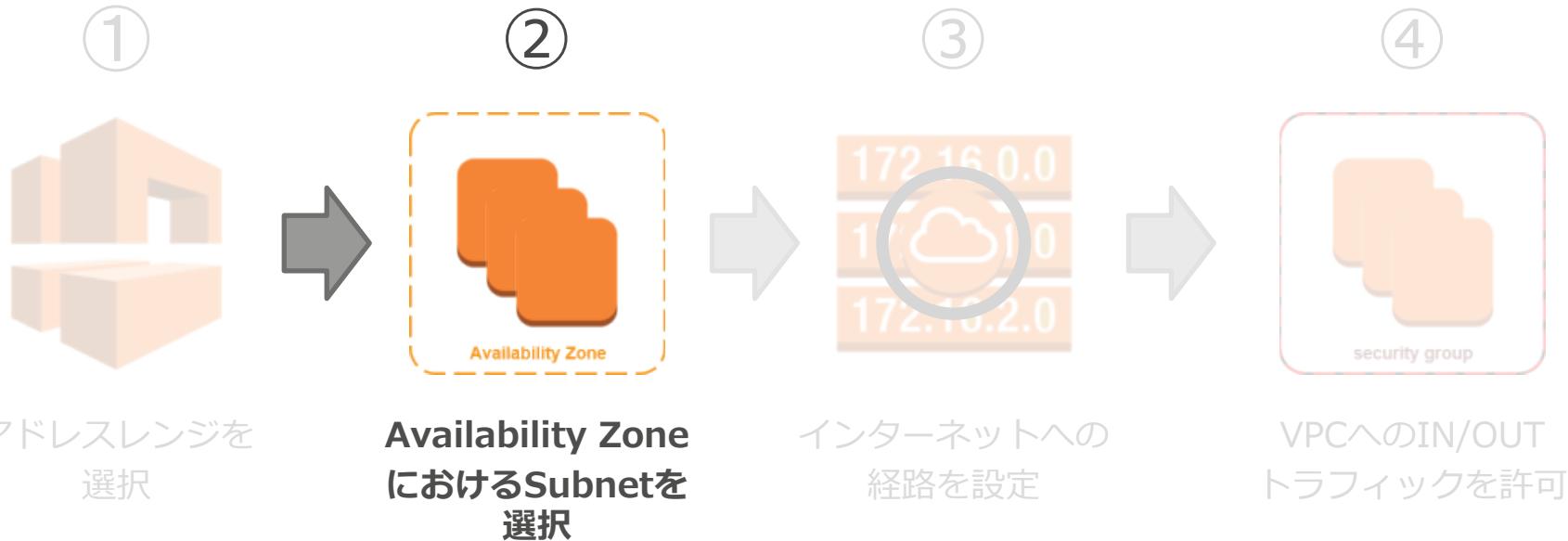
- 名前タグ: VPC-Blackbelt-20170412
- IPv4 CIDR block\*: 172.31.0.0/16
- IPv6 CIDR block\*:  No IPv6 CIDR Block  
 Amazon provided IPv6 CIDR block
- テナント: デフォルト

Buttons at the bottom: キャンセル (Cancel) and 作成 (Create)

IPv4 CIDR block にアドレスレンジを入力して作成



# インターネット接続VPCのステップ<sup>°</sup>



# VPC CIRDとサブネット数

CIDRに/16 を設定した場合の各サブネット数と使えるIPアドレス数

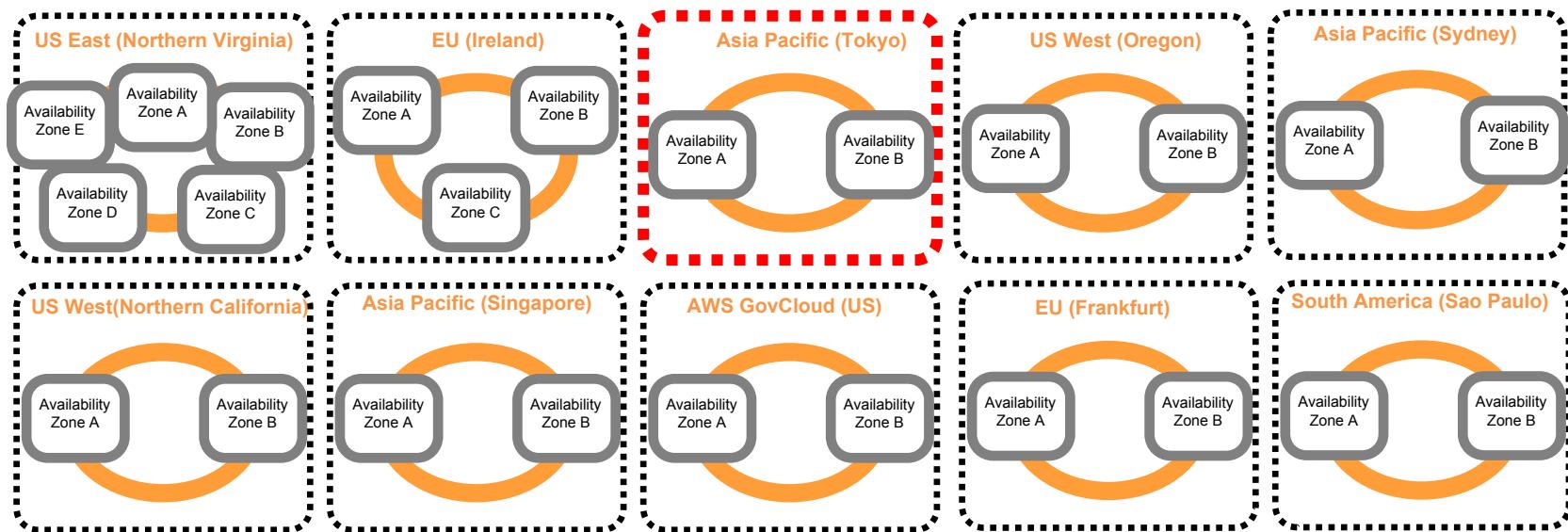
サブネットマスク	サブネット数	サブネットあたりのIPアドレス数
/18	4	16379
/20	16	4091
/22	64	1019
<b>/24</b>	<b>256</b> ※	<b>251</b>
/26	1024 ※	59
/28	16384 ※	11

※ VPCあたりのサブネット作成上限数はデフォルト200個

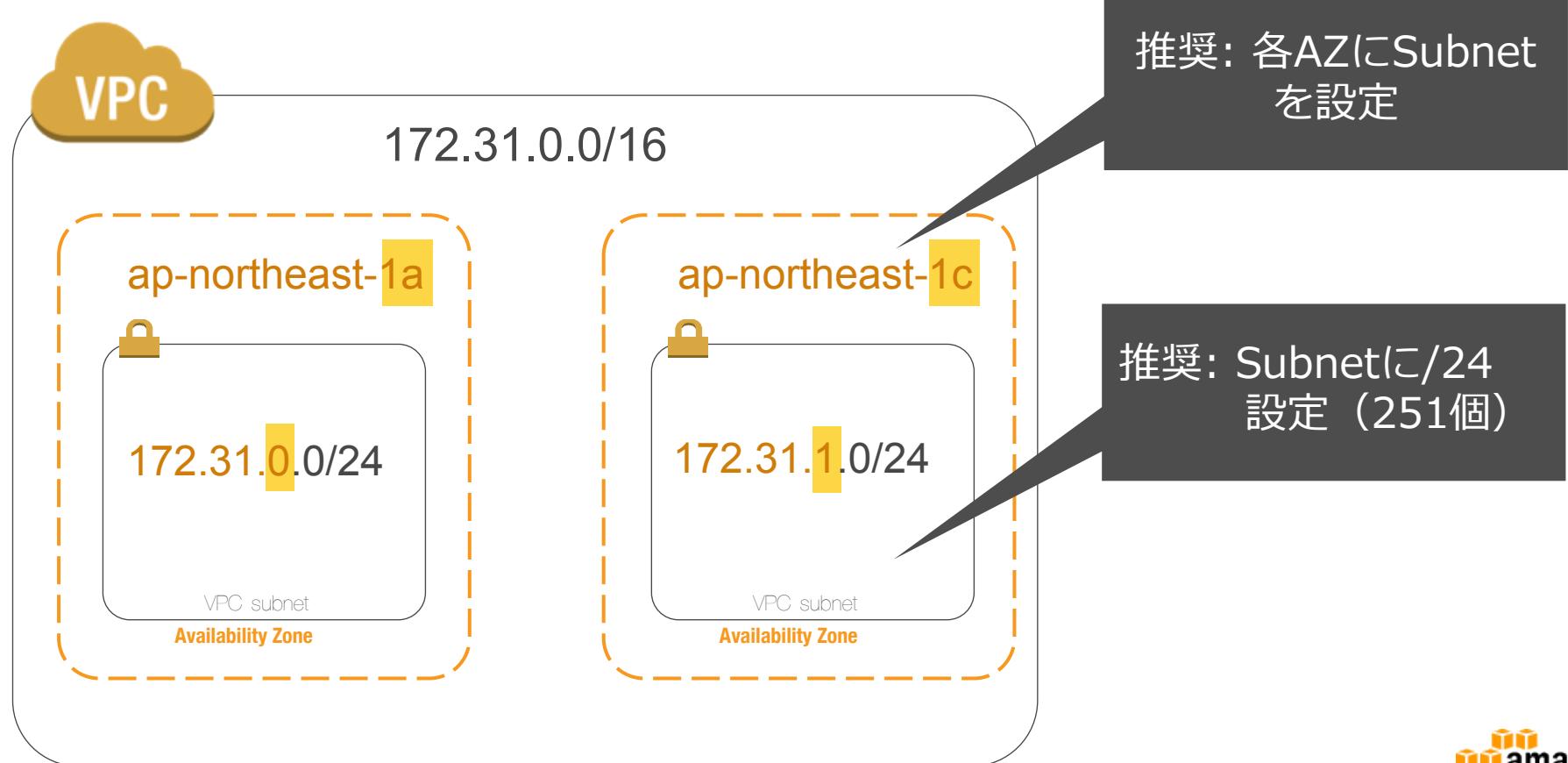
# アベイラビリティゾーン

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
- 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（リージョン間はインターネット経由）



# サブネットに対してAZとアドレスを選択



# サブネットを作成

The screenshot shows the AWS VPC Management Console with the 'Create Subnet' wizard open. The left sidebar shows navigation options like Virtual Private Cloud, Subnets, Route Tables, and more. The main form has the following fields:

- ネームタグ: Subnet-Public-A
- VPC: vpc-9961f2fd | VPC-Blackbelt-20170412
- VPC CIDRs: CIDR 172.31.0.0/16, Status: associated
- アベイラビリティーゾーン: ap-northeast-1a
- IPv4 CIDR block: 172.31.1.0/24

At the bottom right are 'キャンセル' (Cancel) and '作成' (Create) buttons.

- ・ネームタグ
- ・VPC
- ・アベイラビリティゾーン
- ・IPv4 CIDR block

を指定して作成



# サブネットで利用できないIPアドレス

ホストアドレス	用途
.0	ネットワークアドレス
.1	VPCルータ
.2	Amazonが提供するDNSサービス
.3	AWSで予約
.255	ブロードキャストアドレス (VPCではブロードキャストはサポートされていない)

# インターネット接続VPCのステップ<sup>°</sup>

①



アドレスレンジを  
選択

②



Availability Zone  
におけるSubnetを  
選択

③



インターネットへの  
経路を設定

④



VPCへのIN/OUT  
トラフィックを許可

# 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

172.16.0.0  
172.16.1.0  
172.16.2.0

# ルートテーブルの確認

The screenshot shows the AWS VPC Management Console with the URL <https://ap-northeast-1.console.aws.amazon.com/vpc/home?region=ap-northeast-1#routetables>. The left sidebar is collapsed, and the main area displays the Route Table details for 'rtb-9c7350f8'.

**Route Table Details:**

Name	Route Table ID	Explicit Association	Main	VPC
rtb-9c7350f8	0 Subnet	Yes	vpc-9961f2fd   VPC-Blackbelt-201704...	

**Route Table Rules:**

View:	All rules
From:	172.31.0.0/16
To:	local

A large orange speech bubble points to the 'To' column of the first rule, containing the text:

送信先が同一のセグメントであれば同一セグメントに送信（VPC作成時にデフォルトで作成）



# インターネットゲートウェイを作成、VPCにアタッチ

The screenshot shows the AWS VPC Management Console interface. A yellow callout bubble points from the bottom left towards the 'VPCにアタッチ' (Attach to VPC) button in the 'VPCにアタッチ' dialog box.

**Internet Gateway Creation Dialog:**

- Top navigation bar: VPC Management Console, URL: https://ap-northeast-1.console.aws.amazon.com/vpc/home
- Left sidebar: VPCダッシュボード, サービス (VPC, Virtual Private Cloud, VPC), リソースグループ (vpc-9961f2fd | VPC-Blackbelt-20170412)
- Main area: インターネットゲートウェイの作成 (Create Internet Gateway)
  - Description: インターネットゲートウェイは、VPC をインターネットに接続する仮想ルーターです。
  - Name Tag: VPC-Blackbelt-20170412
  - Buttons: キャンセル, 作成

**VPC Attachment Dialog:**

- Title: VPCにアタッチ (Attach to VPC)
- Description: インターネットとの通信を有効にするため、インターネットゲートウェイを VPC に接続します。
- VPC Selection: VPC vpc-9961f2fd | VPC-Blackbelt-20170412
- Buttons: キャンセル, アタッチ

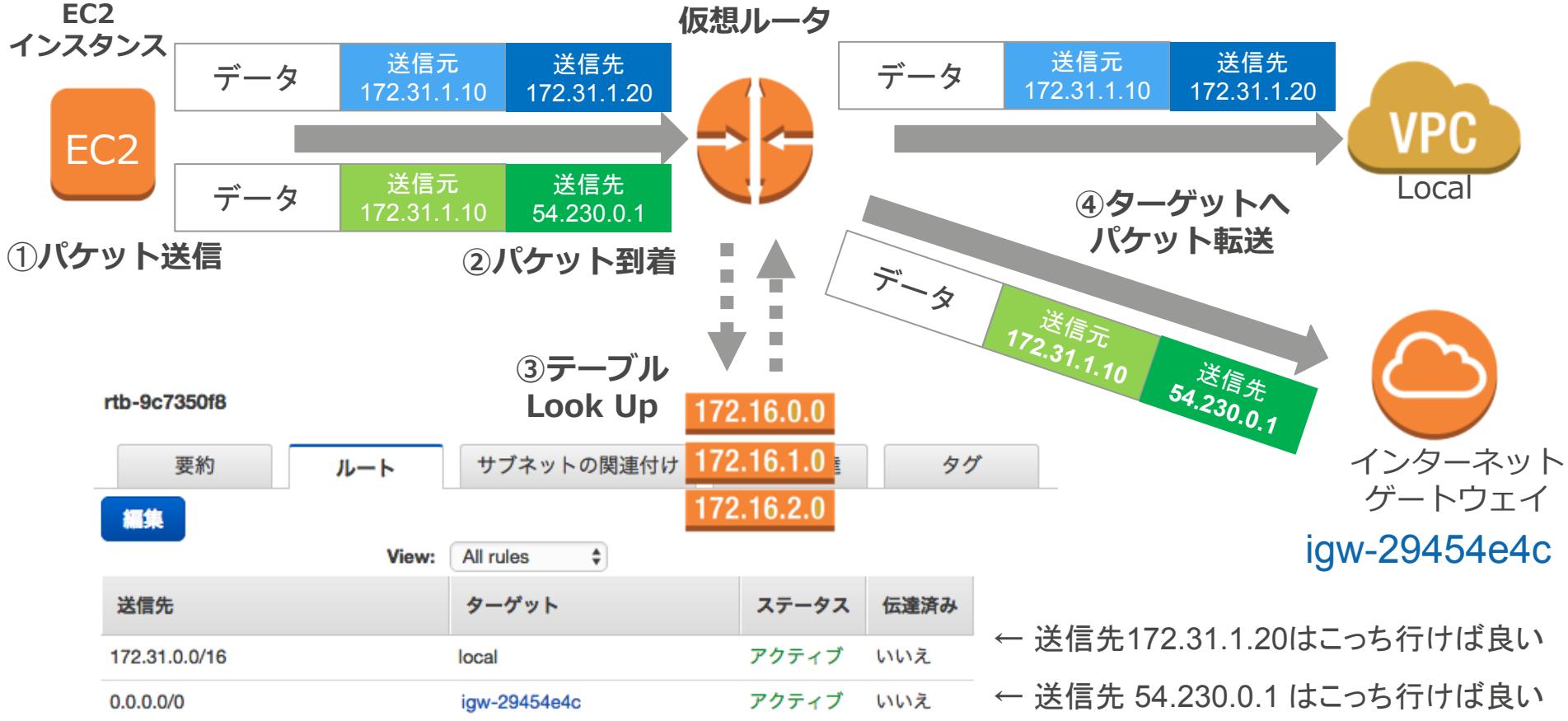
**Internet Gateway List:**

- Header: インターネットゲートウェイの作成 (Create Internet Gateway), 削除 (Delete), VPCにアタッチ (Attach to VPC), VPCからデタッチ (Detach from VPC)
- Search bar: Blackbelt
- Table:

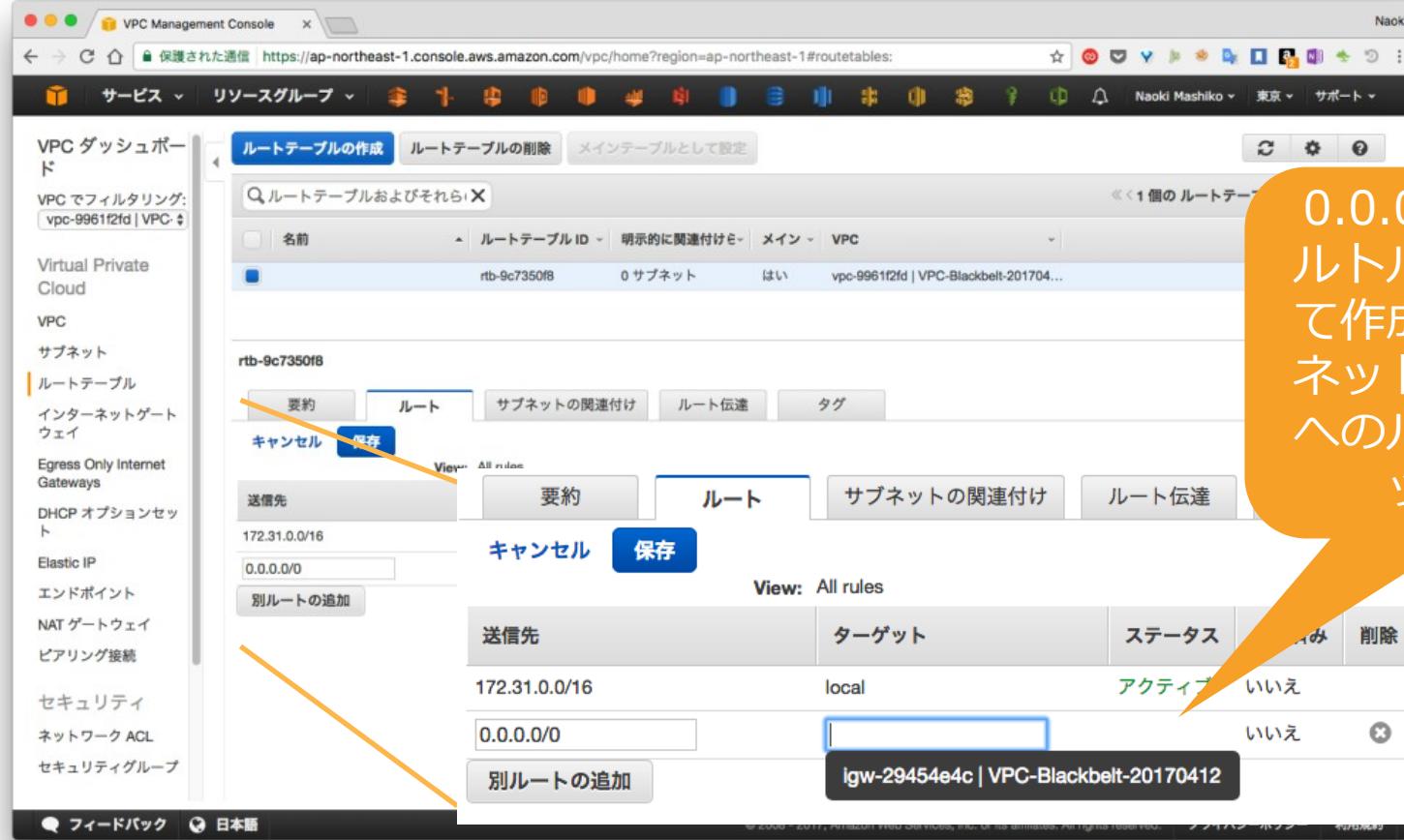
名前	ID	状態	VPC
VPC-Blackbelt-20170412	igw-29454e4c	attached	vpc-9961f2fd   VPC-Blackbelt-201704...

VPCからインターネットへの接続がアタッチされた

# 仮想ルータとルートテーブルの関係(ルートLook up)

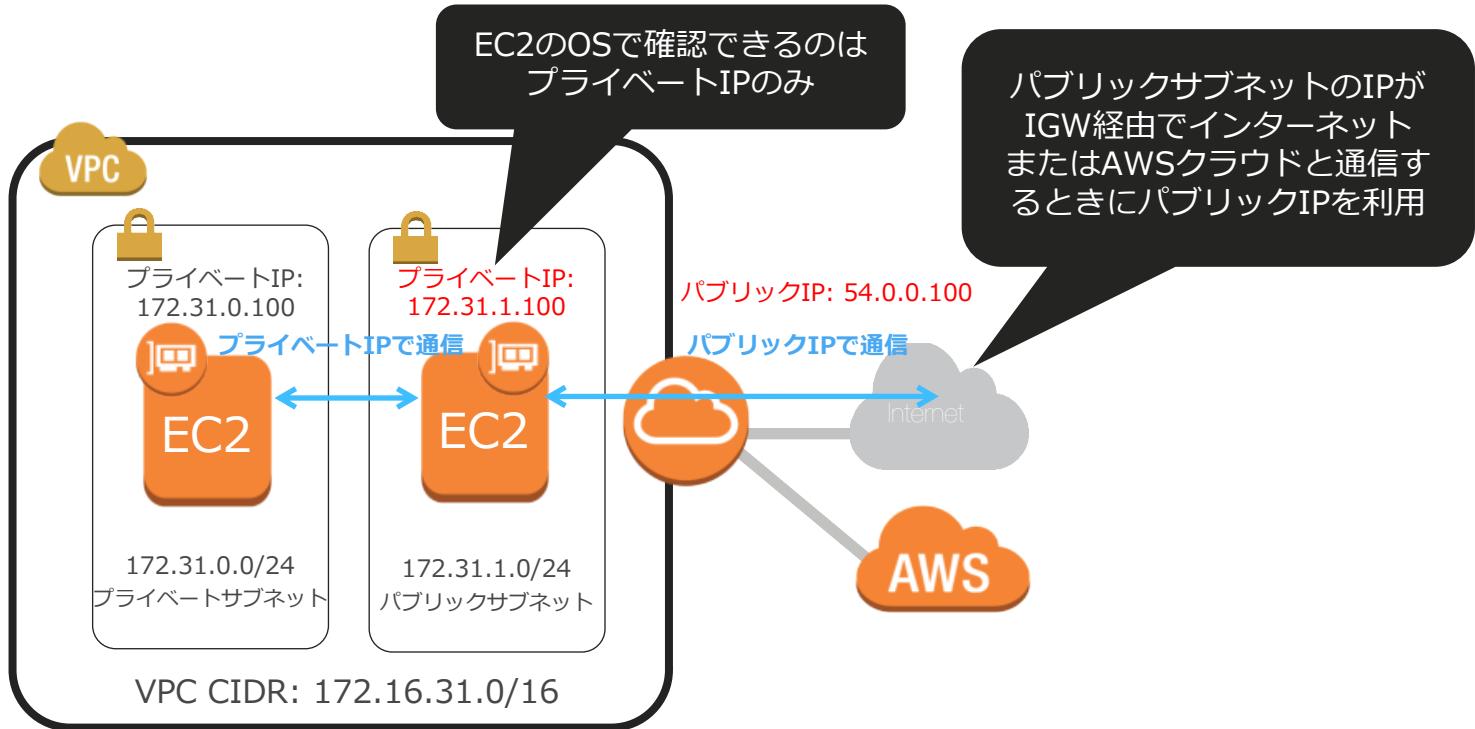


# ルートテーブルにインターネットゲートウェイを追加

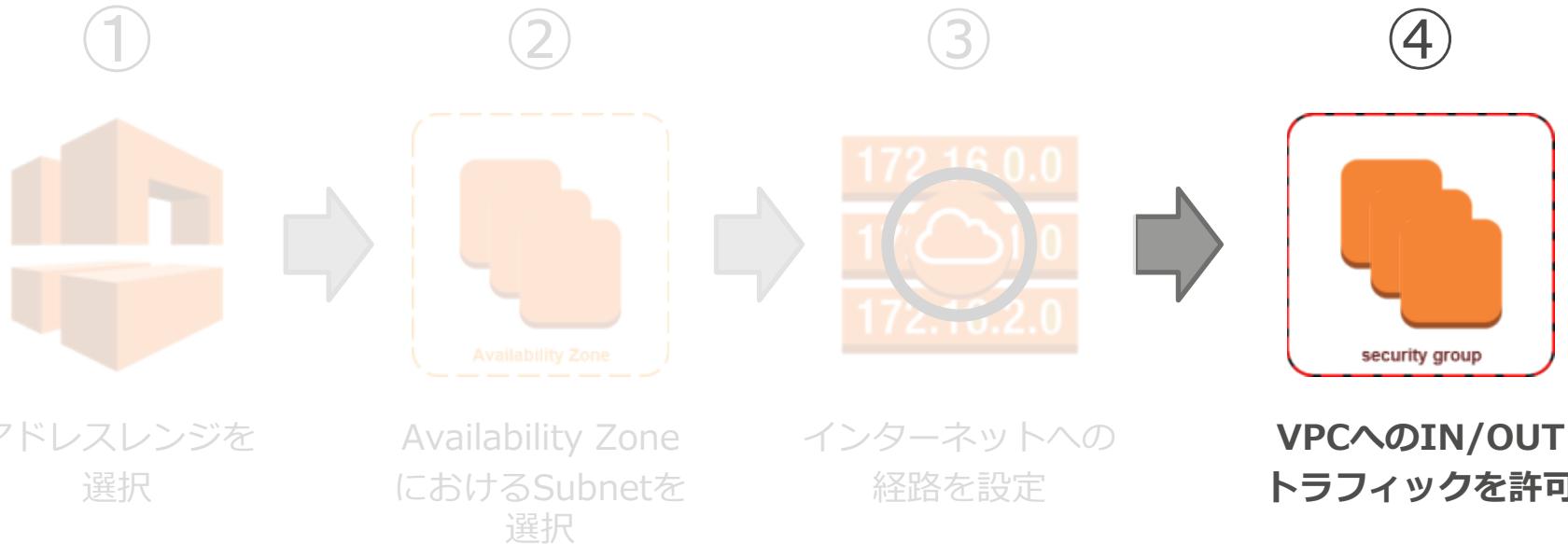


0.0.0.0/0 (デフォルトルート) に対して作成したインターネットゲートウェイへのルートをターゲットに追加

# パブリックサブネットとプライベートサブネット



# インターネット接続VPCのステップ<sup>°</sup>



# セキュリティグループ = ステートフル Firewall

The screenshot shows the AWS VPC Management Console with the 'Security Groups' tab selected. A specific security group, 'sg-0fe2e368', is being edited. The 'Inbound Rules' tab is active, showing two rules:

Type	Protocol	Port Range	Source
すべての トラフィック	すべて	すべて	sg-0fe2e368
HTTP (80)	TCP (6)	80	0.0.0.0/0

Below the main table, there's a smaller preview table showing the same rules.

A large orange callout bubble points to the top rule with the text: "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)".

A second orange callout bubble points to the bottom rule with the text: "その為、必要な通信例えは、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".

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、必要な通信例えは、  
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

The screenshot shows the AWS VPC Management Console with the URL <https://ap-northeast-1.console.aws.amazon.com/vpc/home?region=ap-northeast-1#aclc:>. The left sidebar lists various VPC-related services. The main area is titled "ネットワーク ACL の作成" (Create Network ACL) and shows a single network ACL named "acl-aef07ec2". The interface includes tabs for "要約" (Summary), "インバウンドルール" (Inbound Rules), "アウトバウンドルール" (Outbound Rules), "サブネットの関連付け" (Associate with Subnet), and "タグ" (Tags). The "インバウンドルール" tab is selected, displaying two rules:

ルール #	タイプ	プロトコル	ポート範囲	送信元	許可/拒否
100	すべての トraフィック	すべて	すべて	0.0.0.0/0	許可
*	すべての トraフィック	すべて	すべて	0.0.0.0/0	拒否

A yellow arrow points from the text "サブネット単位で適用される" to the "サブネットの関連付け" tab. Another yellow arrow points from the text "デフォルトでは全ての送信元IPを許可" to the first rule in the table.

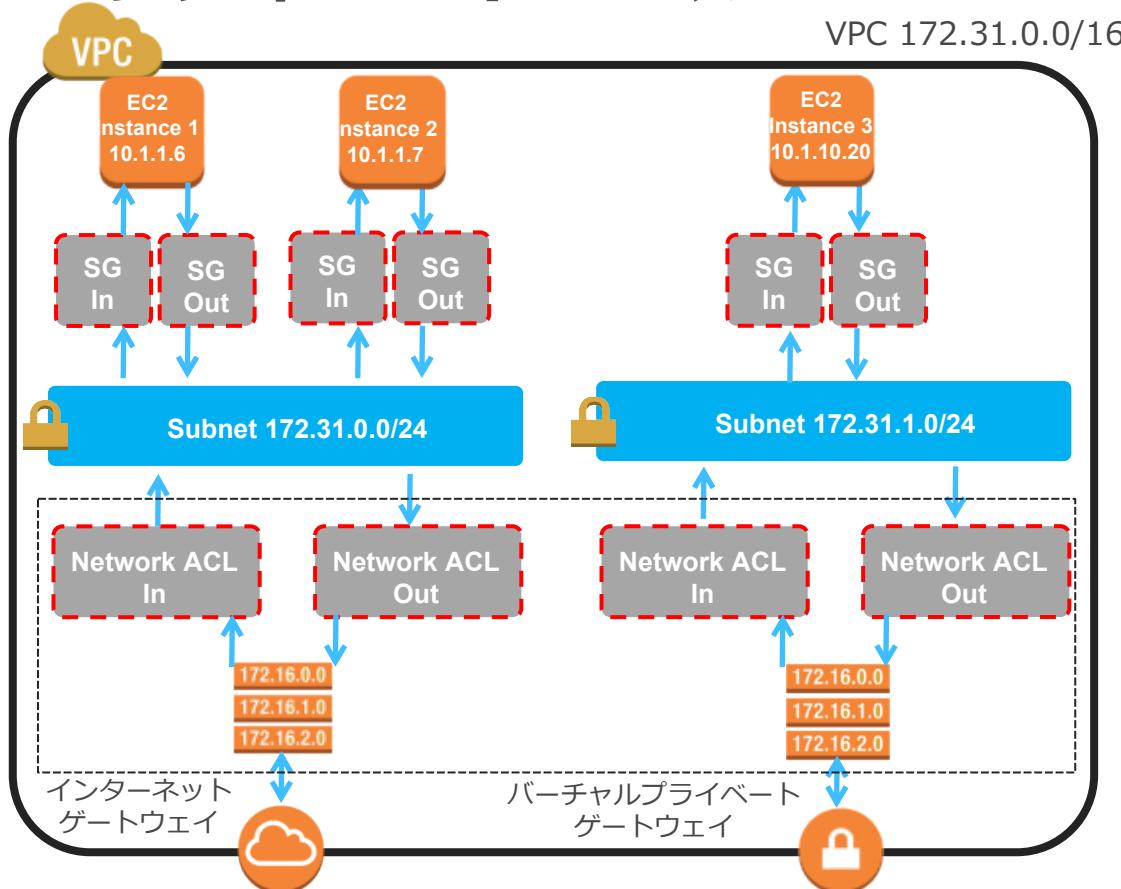
サブネット単位で適用される

デフォルトでは全ての送信元IPを許可

Amazon web services

# VPCセキュリティコントロール

VPC 172.31.0.0/16

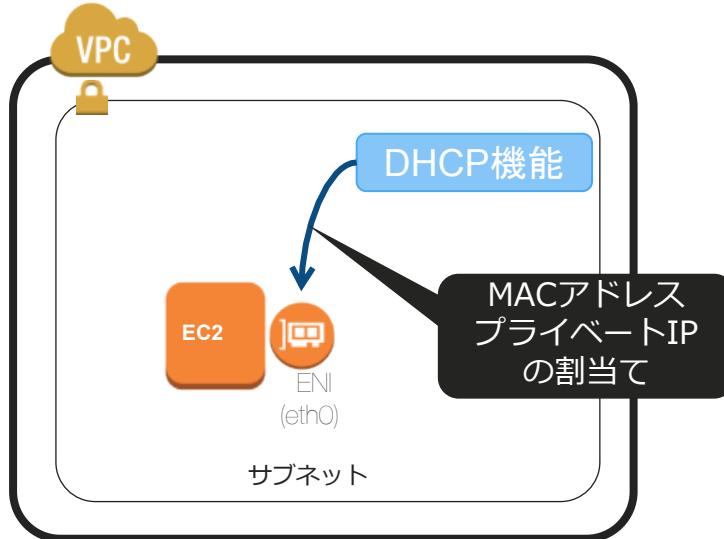


# ネットワークACL vs セキュリティグループ

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

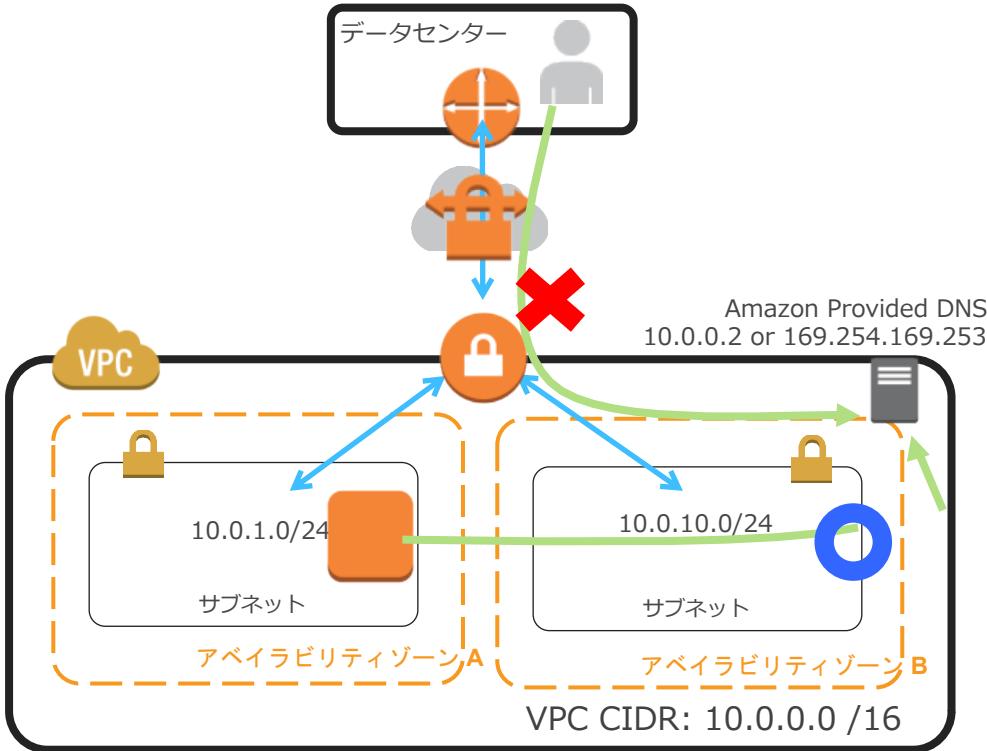
# VPCセットアップの補足

# サブネット内のDHCP



- ・サブネット内のENI(Elasticネットワークインターフェース)にIPを自動割当てる
- ・プライベートIPを固定にした場合はDHCP経由で該当のIPが割当てる(EC2インスタンスのOS上のNIC設定はDHCP設定とする)

# Amazon DNS サーバー



- Amazonが提供するDNSサービス
- 以下の2つのアドレスが利用可能
  - ①VPCのネットワーク範囲(CIDR)のアドレスに+2をプラスしたIP  
(10.0.0.0/16の場合は10.0.0.2)
  - ②169.254.169.253
- **VPC内のEC2インスタンスからのみ参照可能  
(VPNや専用線経由では参照できない)**

[http://docs.aws.amazon.com/ja\\_jp/AmazonVPC/latest/UserGuide/VPC\\_DHCP\\_Options.html#AmazonDNS](http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#AmazonDNS)

# DNS機能の有効化とホストへのDNS名割当て

vpc-[REDACTED] (10.0.0.0/16) | edge.poc1

Summary Tags

VPC ID: vpc-[REDACTED] | edge.poc1  
State: available  
VPC CIDR: 10.0.0.0/16  
DHCP options set: dopt-[REDACTED]  
Route table: rtb-[REDACTED] | mainrt.edge.poc1

Network ACL: acl-[REDACTED]  
Tenancy: Default  
**DNS resolution: yes**  
**DNS hostnames: yes**

## Enable DNS resolution.

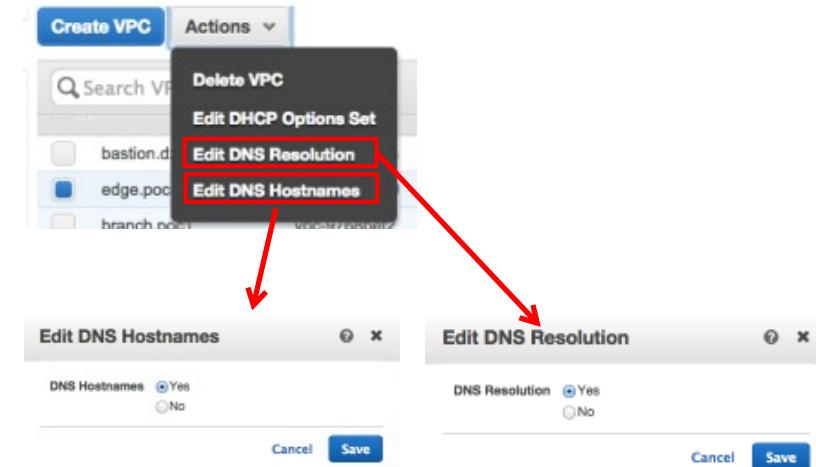
基本はyesとする

NoにするとVPCのDNS機能が無効となる

## Enable DNS hostname

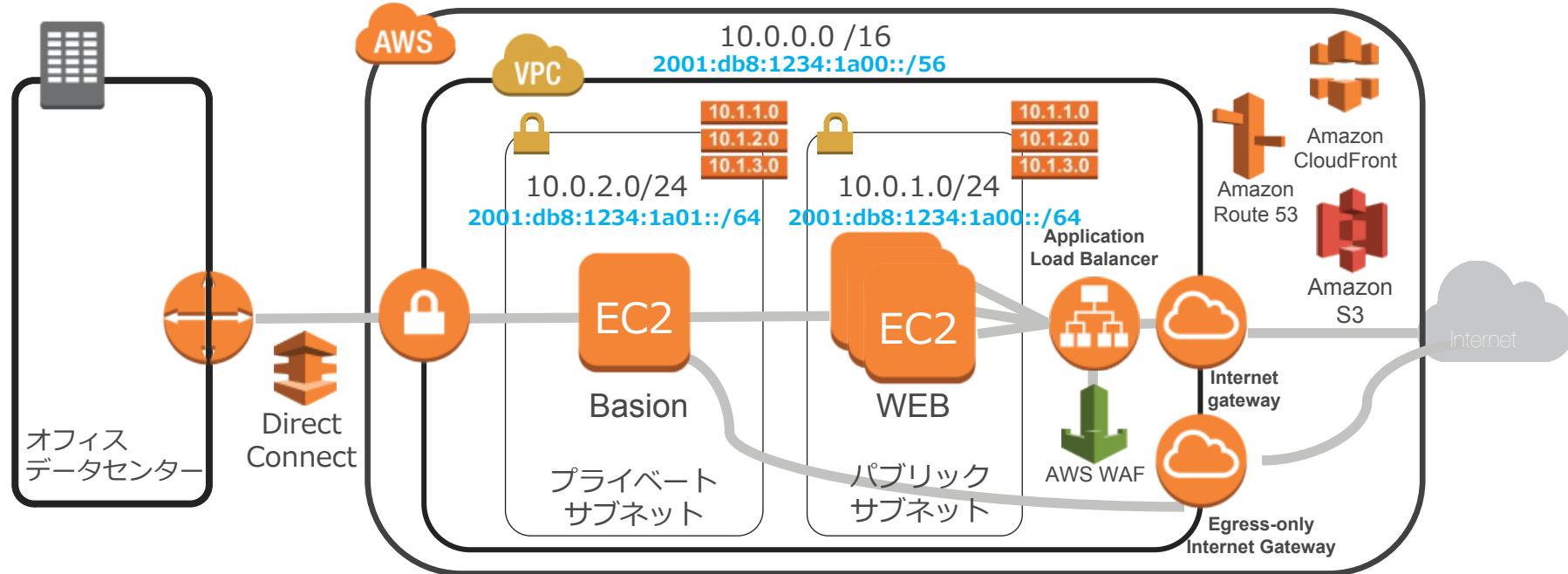
TrueにするとDNS名が割り当てられる

“Enable DNS resolution”をtrueにしないと有効にならない



# IPv6の対応

S3、CloudFront、WAF、Route53に続きVPC、ALBがIPv6対応



Egress-only Gateway(EGW) を利用して  
IPv6においてもプライベート利用が可能

上記のような構成をIPv4/IPv6デュアルスタックで構築可能

# VPCにおけるIPv4とIPv6の特徴と制限

	IPv4	IPv6
アドレス体系	32bit	128bit
VPCでの利用	デフォルトで適用	オプトイン (自動適用ではなく任意)
CIDRブロックサイズ	16~28bitで選択 自分で任意のアドレスを設定可能	56bit固定 かつ自動で56bit CIDRが アサインされる (選べない)
サブネット ブロックサイズ	16~28bitで選択	64bit固定
パブリックIP/ プライベートIP	それぞれ存在 (NATを介してパブリックIPをプライマリプライ ベートIPにMAP)	パブリックのみ (プライベートにするにはEgress-only Internet Gatewayを利用)
インスタンスタイル	全てのインスタンスタイル	M3、G2を除く全ての現行世代の インスタンスタイルでサポート
アマゾン提供DNS	プライベートIP、Elastic IPに対する それぞれのDNSホスト名を受信	提供されるDNSホスト名はなし
閉域接続	VPN、DirectConnect	DirectConnectのみ

# Agenda

- Amazon VPCとは？
- VPCのコンポーネント
- オンプレミスとのハイブリッド構成
- VPCの設計
- VPCの実装
- VPCの運用
- まとめ



# VPCとのプライベートネットワーク接続

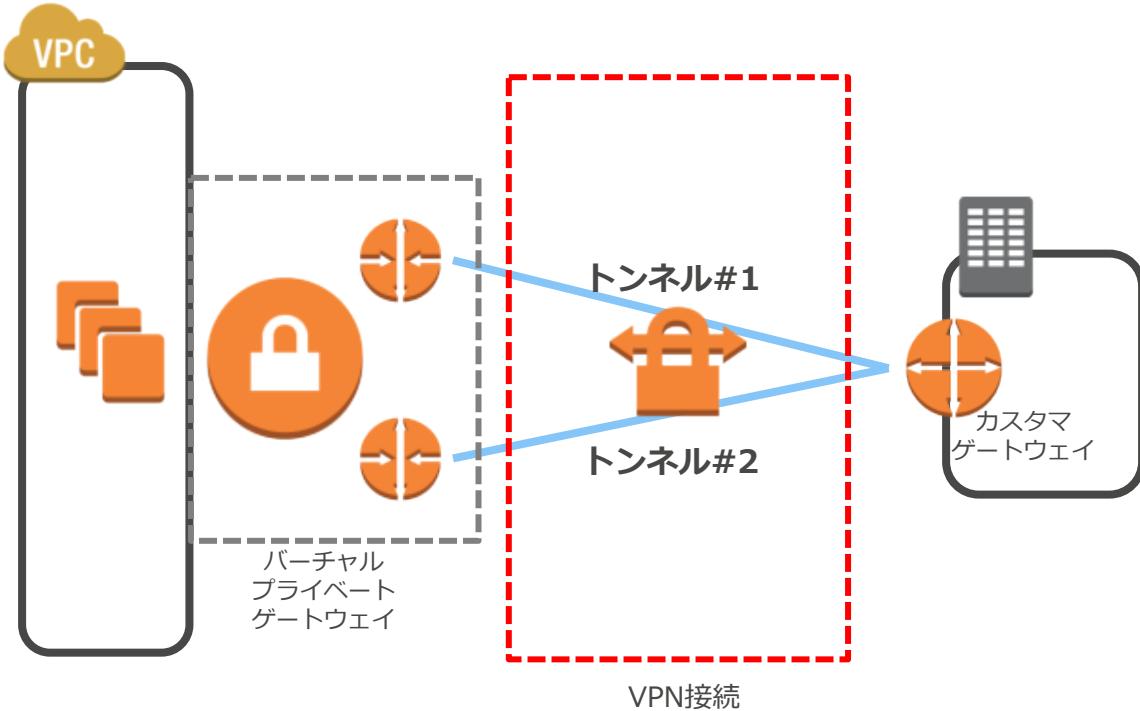
## VPN接続

バーチャルプライベートゲートウェイを利用したサイト間VPN

## 専用線接続

AWS Direct Connectを利用し、一貫性のあるネットワーク接続を実現  
本番サービス向け

# VPN接続構成



- ・1つのVPN接続は2つのIPsec  
トンネルで冗長化
- ・ルーティングは  
静的(スタティック)  
動的(ダイナミック:BGP)  
が選択可能

# カスタマゲートウェイの要件

機能	RFC	機能	RFC
Pre-shared キーを使用して、IKE セキュリティ接続を確立する	RFC2409	トンネルを論理インターフェイスに結合する (経路ベースのVPN)	-
トンネルモードで、IPsec セキュリティ接続を確立する	RFC4301	暗号化前に IP パケットをフラグメント化する	RFC4459
AES 128 ビット暗号化または AES 256 ビットの暗号化機能を使用する	RFC3602	(オプション) BGP ピアを確立する	RFC4271
SHA-1 または SHA-256 のハッシュ機能を使用する	RFC2404	VPN トンネルに入る TCP パケットの最大セグメントサイズを調整する	RFC4459
Diffie-Hellman Perfect Forward Secrecy を使用します。以下のグループがサポートされます。 フェーズ 1 グループ: 2,14~18,22,23,24 フェーズ 2 グループ: 1,2,5,14~18,22,23,24	RFC2409	パケットの "フラグメント化しない" フラグをリセットする	RFC791
IPsec Dead Peer Detection の利用	RFC3706		

# VPN対応機器リスト

## ■ 静的ルーティングを使用する場合

Cisco ASA 500シリーズ バージョン8.2移行

Cisco ISR (IOS 12.4以降)

SonicOS5.8以降を実行するDell SonicWALL次世代ファイアウォール(TZ,NSA,SuperMassiveシリーズ)

Juniper Jシリーズサービスルーター (JunOS 9.5以降)

Juniper SRXシリーズサービスゲートウェイ (JunOS 9.5以降)

ScreenOS 6.1もしくは6.2(またはそれ以降)のJuniper SSG/ISG

Microsoft Windows Server 2008 R2 以降

ヤマハ RTX1200 ルーター

## ■ 動的ルーティングを使用する場合

Astaro Security Gateway/Security Gateway Essential Firewall Edition バージョン8.3以降

Cisco ISR (IOS 12.4以降)

SonicOS5.9以降を実行するDell SonicWALL次世代ファイアウォール(TZ,NSA,SuperMassiveシリーズ)

Fortinet Fortigate 40+シリーズ (FortiOS 4.0以降)

Juniper Jシリーズサービスルーター (JunOS 9.5以降)

Juniper SRXシリーズサービスゲートウェイ (JunOS 9.5以降)

ScreenOS 6.1もしくは6.2(またはそれ以降)のJuniper SSG/ISG

Palo Alto Networks PAシリーズ (PANOS 4.1.2以降)

Vyatta network OS 6.5以降

ヤマハ RTX1200 ルーター

掲載機器以外でも要件を満たせば利用可能  
最新情報はWebのドキュメントを参照

<https://aws.amazon.com/jp/vpc/faqs/#C9>



# カスタマゲートウェイのコンフィグレーション

VPC Dashboard

Create VPN Connection Delete Download Configuration

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Name	VPN ID	State	Virtual Private Gateway
vpn-xxxxxx	available	vgw-xxxxxx	vgw.poc



Download Configuration

Please choose the configuration to download based on your type of customer gateway.

Vendor Cisco Systems, Inc.

Platform ISR Series Routers

Software IOS 12.4+

Cancel Yes, Download



```
! -----
! IPSec Tunnel #1
! -----
! #1: Internet Key Exchange (IKE) Configuration
!
! A policy is established for the supported ISAKMP encryption,
! authentication, Diffie-Hellman, lifetime, and key parameters.
!
! Note that there are a global list of ISAKMP policies, each identified by
! sequence number. This policy is defined as #200, which may conflict with
! an existing policy using the same number. If so, we recommend changing
! the sequence number to avoid conflicts.
!
crypto isakmp policy 200
    encryption aes 128
    authentication pre-share
    group 2
    lifetime 28800
    hash sha
exit

! The ISAKMP keyring stores the Pre Shared Key used to authenticate the
! tunnel endpoints.
!
```

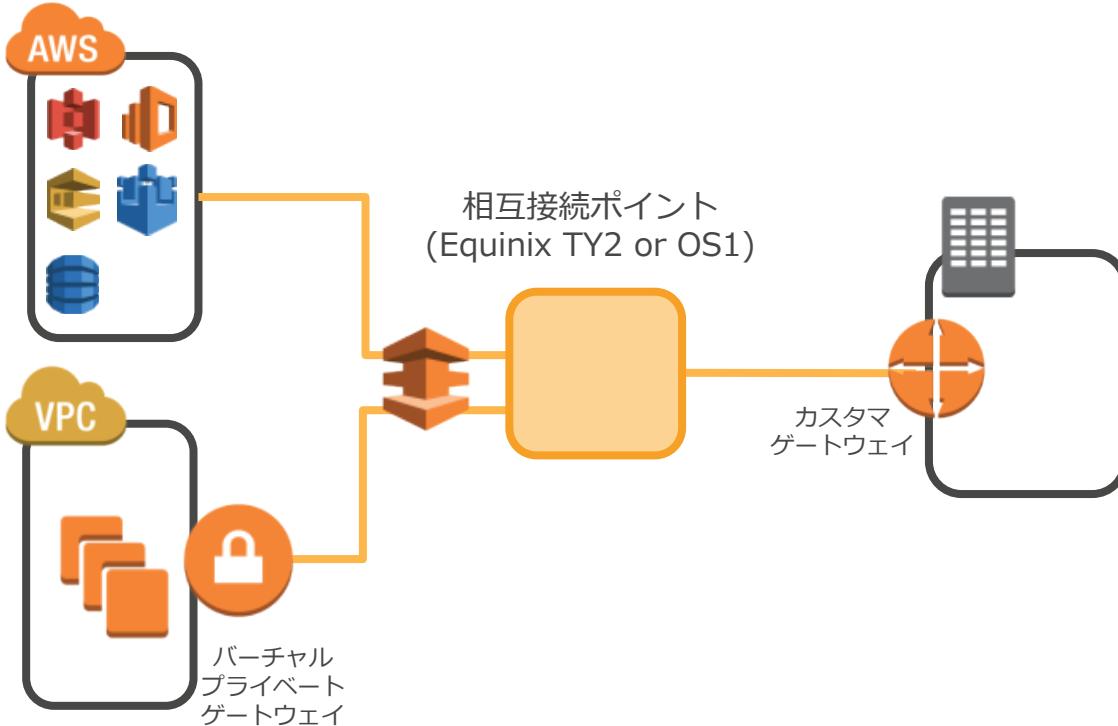
[http://docs.aws.amazon.com/ja\\_jp/AmazonVPC/latest/NetworkAdminGuide/Introduction.html](http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/NetworkAdminGuide/Introduction.html)

# VPNのアップデート(2015/10)

- カスタマゲートウェイのIPアドレスが再利用可能に
- NATトラバーサルが利用可能に
  - NATルータの背後にカスタマゲートウェイが設置可能
- 新しい暗号化オプション
  - AES-256
  - フェーズ1: DH groups 2, 14-18, 22, 23, and 24
  - フェーズ2: DH groups 1, 2, 5, 14-18, 22, 23, and 24

[http://aws.typepad.com/aws\\_japan/2015/10/vpc-vpn.html](http://aws.typepad.com/aws_japan/2015/10/vpc-vpn.html)

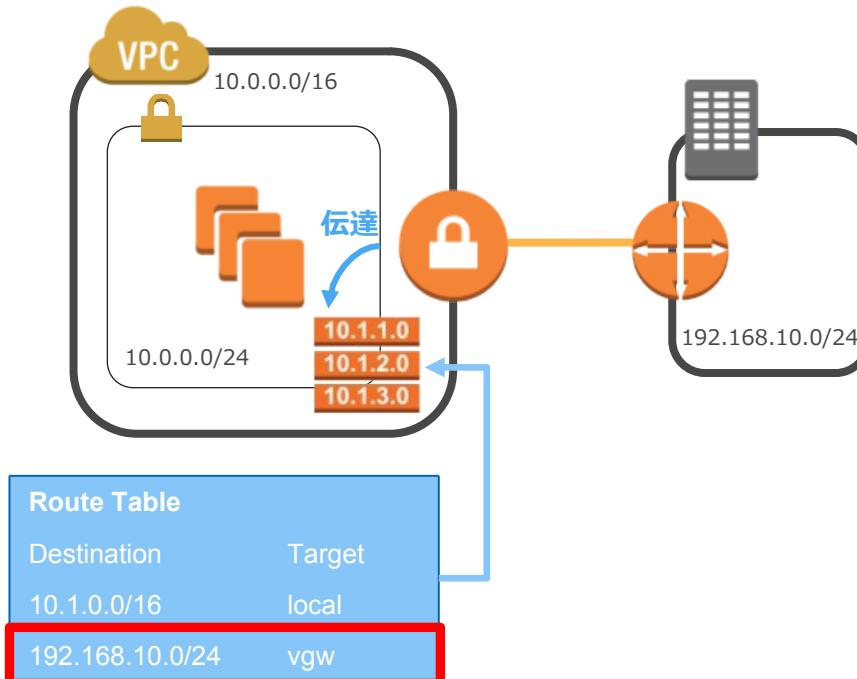
# 専用線(Direct Connect)接続構成



- ・ AWSとお客様設備を専用線でネットワーク接続
- ・ 相互接続ポイントへ専用線を敷設し、AWSのルータと相互接続
- ・ 日本の相互接続ポイントは東京(Equinix TY2)  
大阪(Equinix OS1)
- ・ ルーティングはBGPのみ
- ・ 接続先は以下の2つ  
VPC(プライベート接続)  
AWSクラウド(パブリック接続)
- ・ VPNよりも一貫性がある
- ・ 帯域のパフォーマンスも向上
- ・ ネットワークコストも削減

# VPCからオンプレミスへのルート設定

- VPCからオンプレミスへの通信をするためには各サブネットのルートテーブルの設定が必要



宛先: オンプレミスのIP  
ターゲット : VGWのID

- ルートテーブルで“ルート伝達(プロパゲート)”を有効にするとVGWで受信したルート情報をルートテーブルに自動的に伝達(頻繁にオンプレのルートが更新される場合はこちらを利用)

# インターネットVPN vs 専用線

	インターネットVPN	専用線
コスト	安価なベストエフォート回線も利用可能	キャリアの専用線サービスの契約が必要
リードタイム	即時～	数週間～
帯域	暗号化のオーバーヘッドにより制限あり	~10Gbps
品質	インターネットベースのため経路上のネットワーク状態の影響を受ける	キャリアにより高い品質が保証されている
障害時の切り分け	インターネットベースのため自社で保持している範囲以外での切り分けが難しい	エンドツーエンドでどの経路を利用しているか把握できているため比較的容易

# VPNとDirect Connectの冗長化

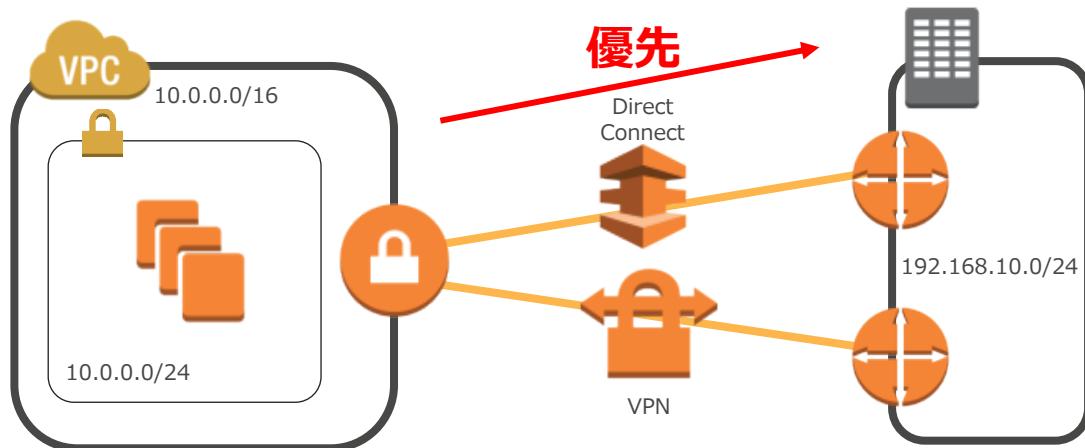
- VPNとDirect Connectを同じVGWに接続することが可能

Direct Connect =アクティブ  
VPN =スタンバイ

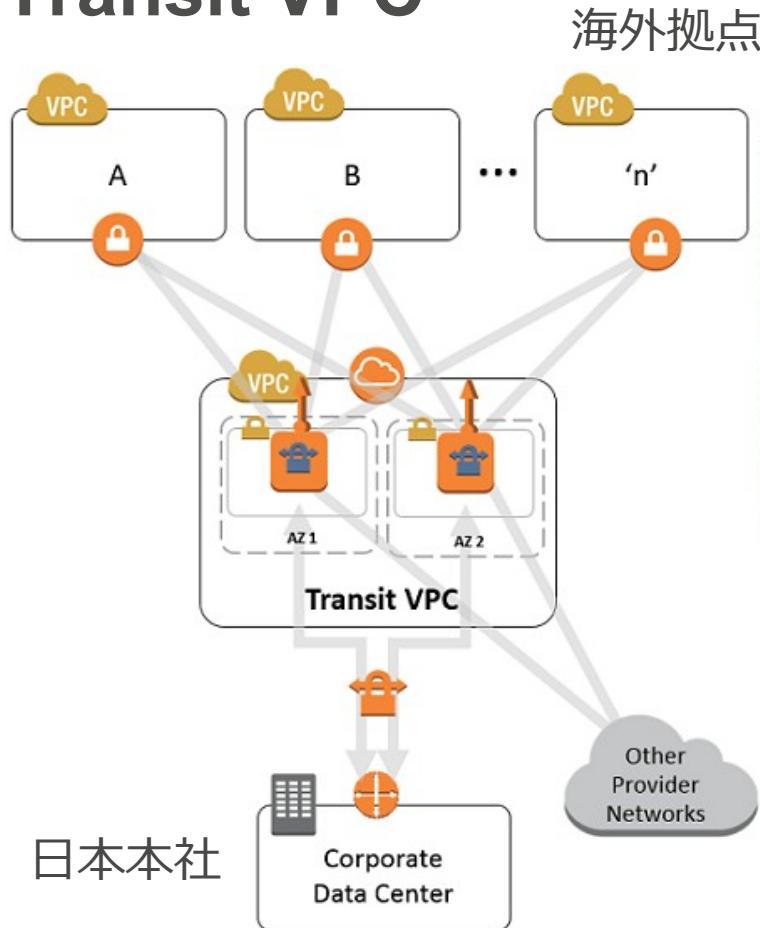
- この場合VPCから見たOutboundは必ずDirect Connectが優先される

(VPNを優先したい場合はVPNルーティング表からDirect Connectより長いPrefixを広告)

- VPNへのフェールオーバー時はレイテンシなど回線品質に注意



# Transit VPC



- CloudFormationテンプレートとして提供
- VPCをグローバルネットワーク転送センターとして機能
- 2つ以上のAWSリージョンに渡るプライベートネットワークを構築可能
- すべてのAWSリージョンを定期にスキャンし、VPN接続がないスポークVPCで適切にタグされた仮想プライベートゲートウェイを探す
- 発見すると各VPCとTransitVPC (Cisco CSR on EC2)間に自動でVPN作成およびBGP接続を行う
- 通常のインスタンスとネットワークの料金に加え、Cisco CSRのライセンス料金が課金される(BYOLも可能)

日本本社

# Agenda

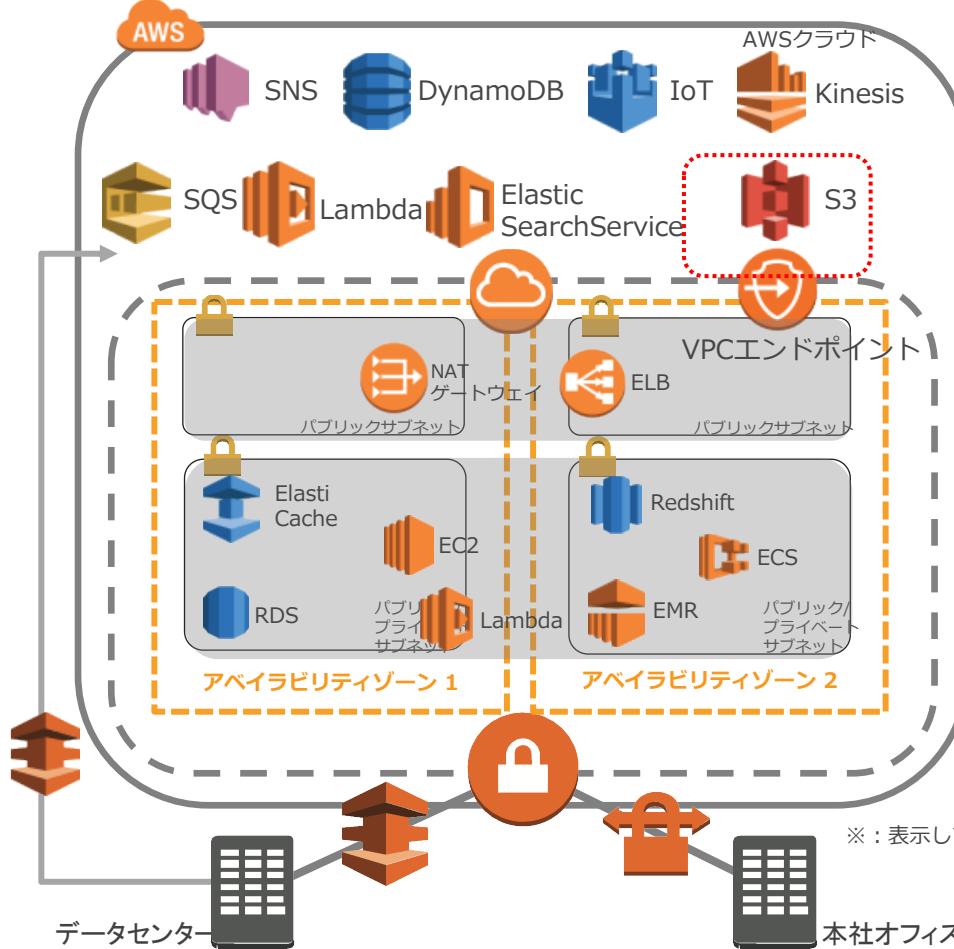
- Amazon VPCとは？
- VPCのコンポーネント
- オンプレミスとのハイブリッド構成
- **VPCの設計**
- VPCの実装
- VPCの運用
- まとめ



# VPC設計のポイント

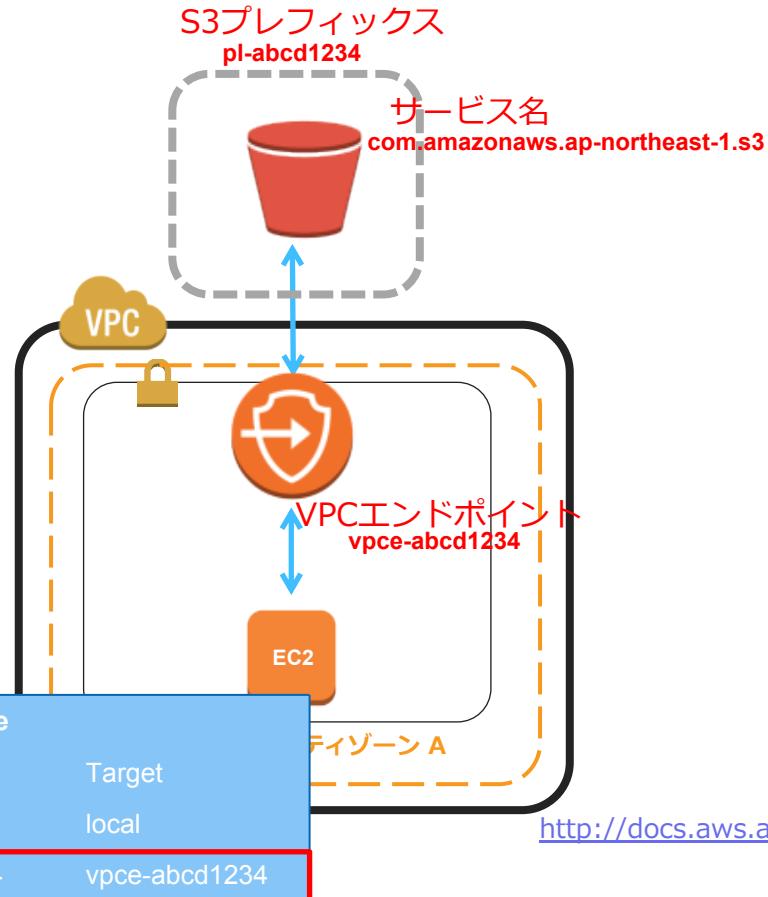
- CIDR(IPアドレス)は既存のVPC、社内のDCやオフィスと被らないアドレス帯をアサイン
- 複数のアベイラビリティゾーンを利用し、可用性の高いシステムを構築
- パブリック/プライベートサブネットへのリソースの配置を慎重に検討
- 適切なセキュリティ対策を適用する
- システムの境界を明らかにし、VPCをどのように分割するか将来を見据えてしっかりと検討する

# AWSクラウドとVPC



- VPC内と外のどちらにリソースやエンドポイントが存在するかサービスによって異なる
- VPCからAWSクラウドへのリソースはIGW経由の通信となる  
プライベートサブネットからは→  
NATゲートウェイ  
S3であればVPCエンドポイントの利用も可能  
パブリックサブネットからは→  
自動割当てまたはEIPのパブリックIPから直接アクセス
- S3へのアクセスはVPCエンドポイント利用可能

# VPCエンドポイント for S3



- VPCエンドポイントをVPCに作成し、プライベートサブネットからAWSクラウド上のS3バケットにアクセスが可能
- VPCエンドポイントを作成すると、ルートテーブルの宛先にS3のプレフィックス、ターゲットにVPCエンドポイントが自動で設定されS3への通信がVPCエンドポイント

経由となる

- VPCエンドポイントポリシーでアクセス制御が可能
- 追加費用なし（トラフィック課金もなし）

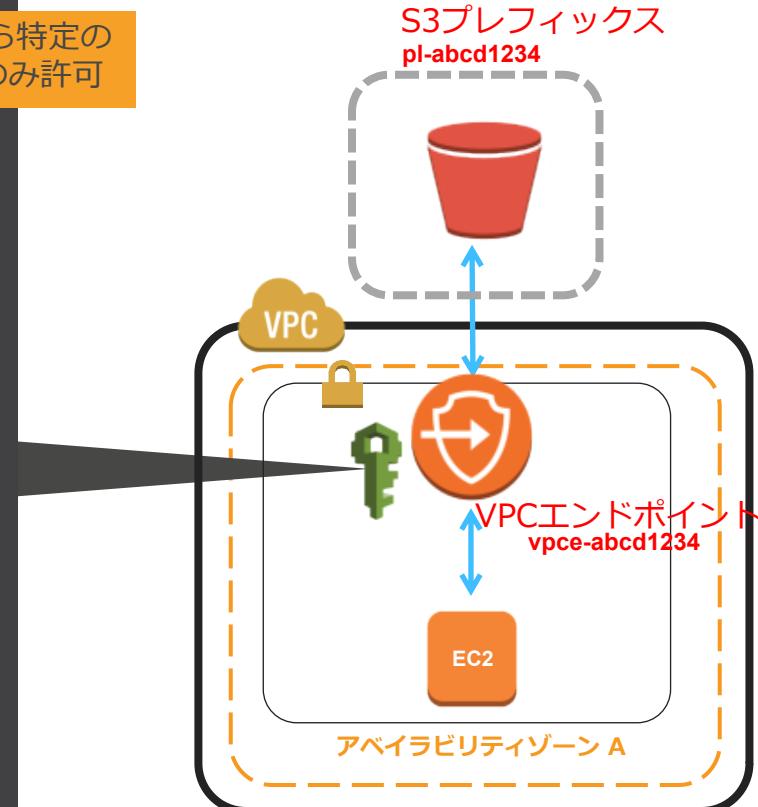
[http://docs.aws.amazon.com/ja\\_jp/AmazonVPC/latest/UserGuide/vpc-endpoints.html](http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpc-endpoints.html)

# VPCエンドポイントポリシー

```
{ "Statement": [ { "Sid": "specific-bucket-only", "Principal": "*", "Action": [ "s3:GetObject", "s3:PutObject" ], "Effect": "Allow", "Resource": [ "arn:aws:s3:::mypics", "arn:aws:s3:::mypics/*" ] } ] }
```

VPCエンドポイントから特定の  
バケットへのPut/Getのみ許可

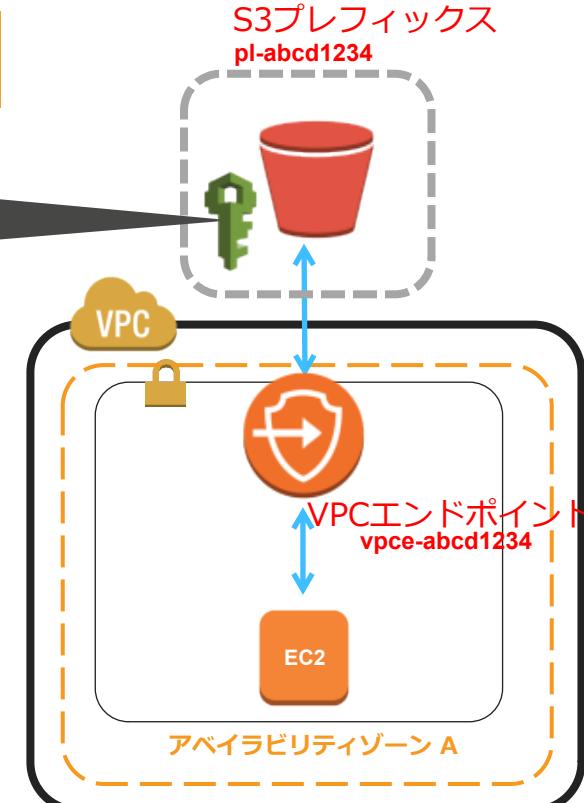
S3プレフィックス  
pl-abcd1234



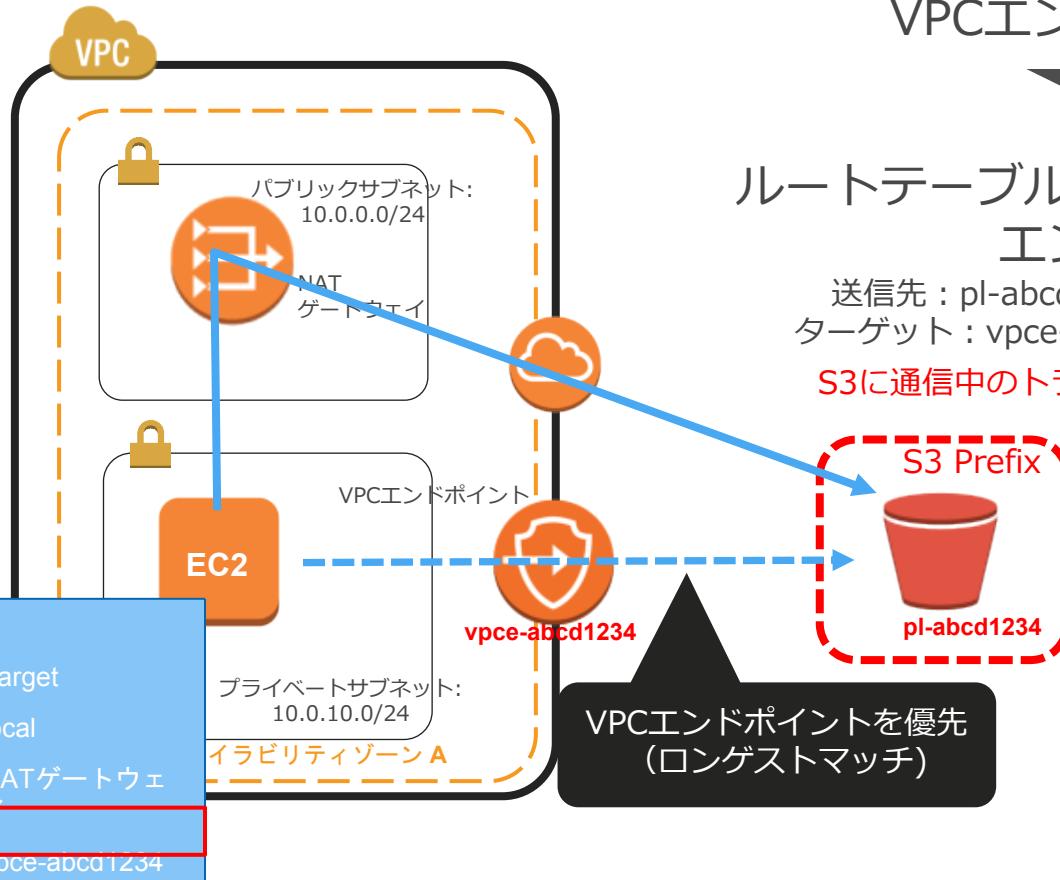
# S3バケットトポリシー(VPCエンドポイント指定)

```
{  
    "Version": "2012-10-17",  
    "Id": "Policy1415115909152",  
    "Statement": [  
        {  
            "Sid": "Access-to-specific-VPCE-only",  
            "Principal": "*",  
            "Action": "s3:*",  
            "Effect": "Deny",  
            "Resource": ["arn:aws:s3:::mypics",  
                        "arn:aws:s3:::mypics/*"],  
            "Condition": {  
                "StringNotEquals": {  
                    "aws:sourceVpce": "vpce-abcd1234"  
                }  
            }  
        }  
    ]  
}
```

特定のVPCエンドポイントからの  
アクセスを許可



# 移行について



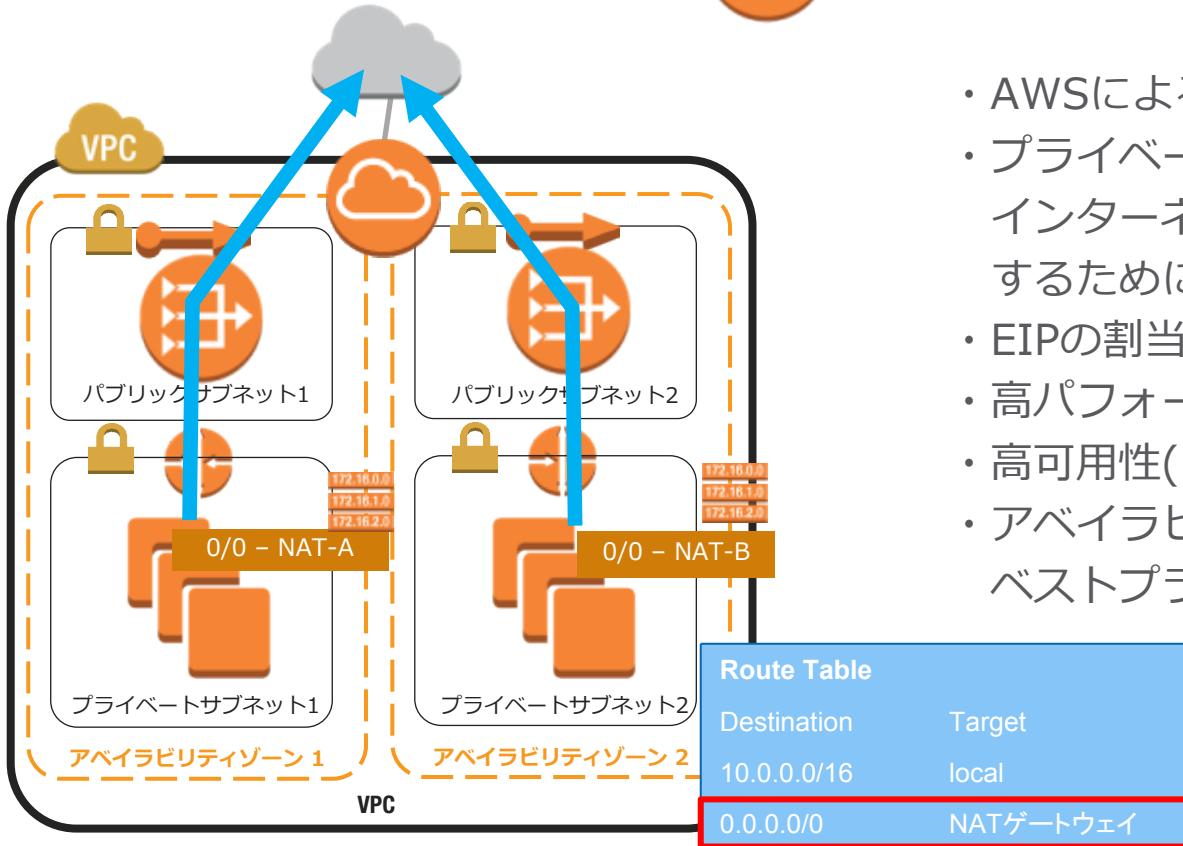
VPCエンドポイント追加

ルートテーブルにVPCエンドポイントのエントリを追加

送信先 : pi-abcd1234(プレフィックスリスト)  
ターゲット : vpce-abcd1234(VPCエンドポイント)

S3に通信中のトラフィックに影響が出るので注意！

# NATゲートウェイ



- ・ AWSによるマネージドNATサービス
- ・ プライベートサブネットのリソースがインターネットまたはAWSクラウドへ通信するために必要
- ・ EIPの割当て可能
- ・ 高パフォーマンス(最大10Gbpsバースト)
- ・ 高可用性(ビルトインで冗長化)
- ・ アベイラビリティゾーン毎に設置するのがベストプラクティス

# VPCを分割するケース(例)

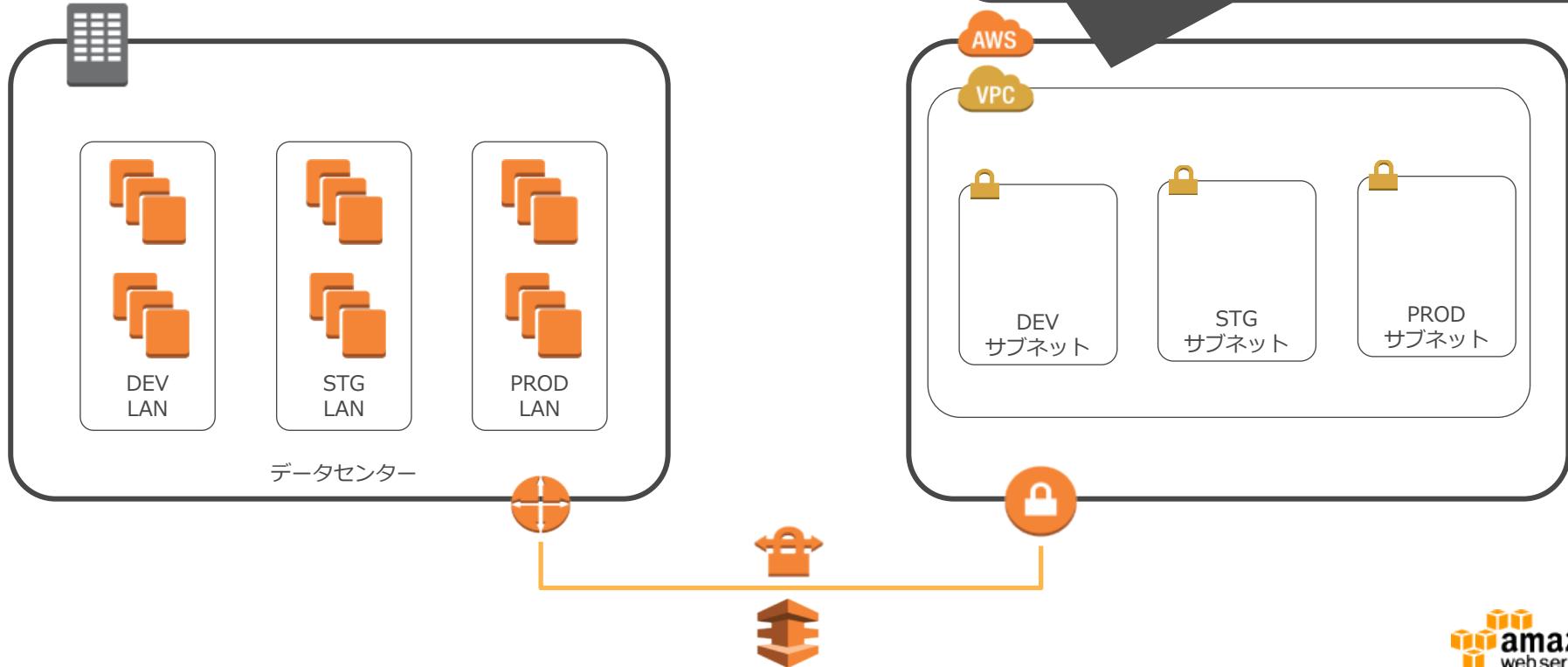
- アプリケーションによる分割
- 監査のスコープによる分割
- リスクレベルによる分割
- 本番/検証/開発フェーズによる分割
- 部署による分割
- 共通サービスの切り出し

AWSアカウントとVPC分割パターンはお客様のITオペレーションモデルに沿ったものである必要がある。

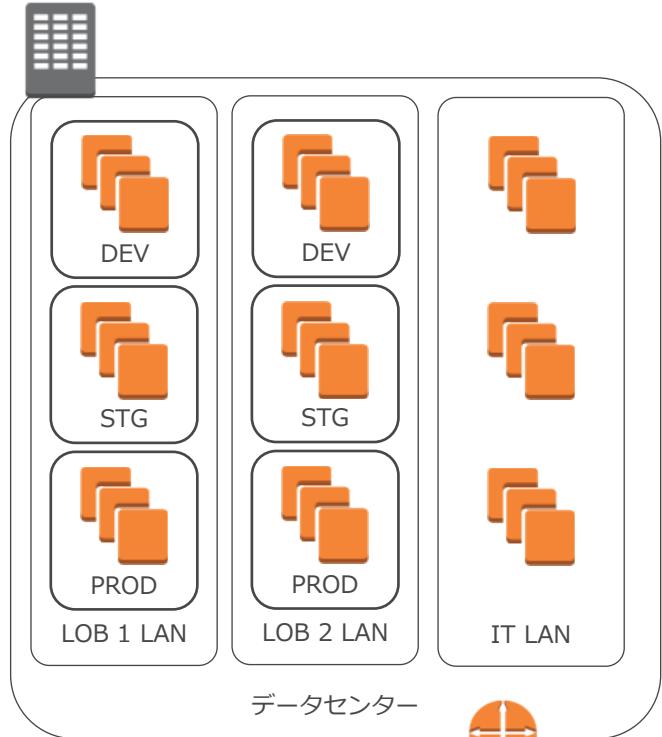


# フェーズによるVPC分割

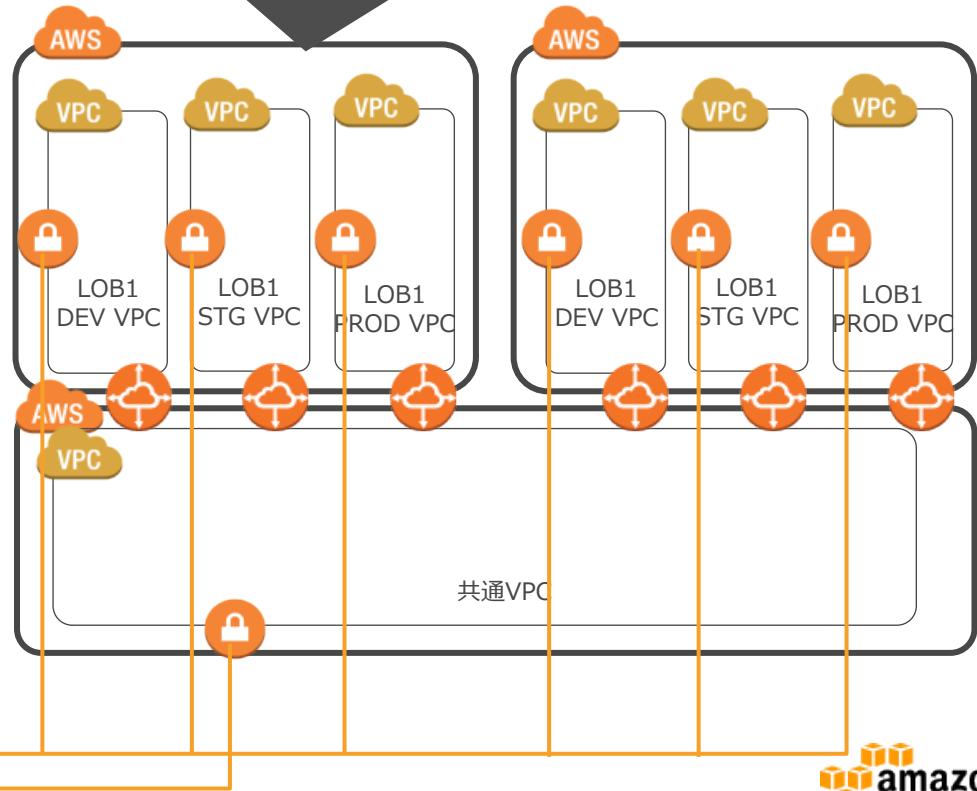
- ・シングルアカウント・シングルVPC
- ・IAMによる権限分離
- ・タグによるコスト管理



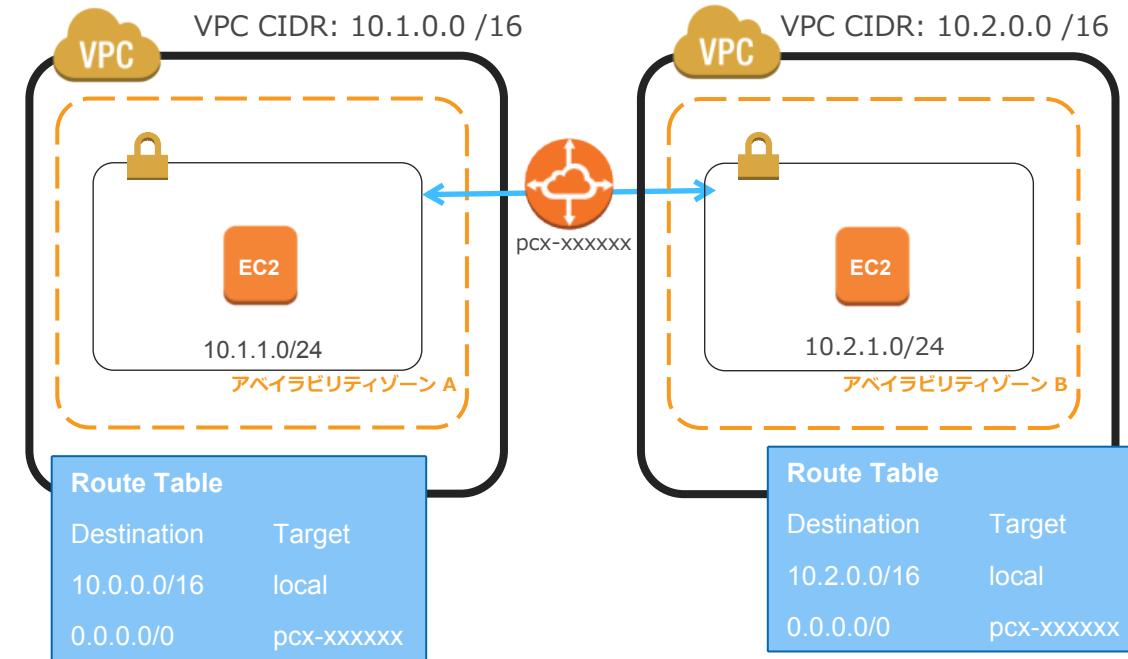
# 組織ごとのVPC分割



- ・マルチアカウント・マルチVPC
- ・モニタリングや認証などのコアサービスは共通VPCとVPCピアリングで接続

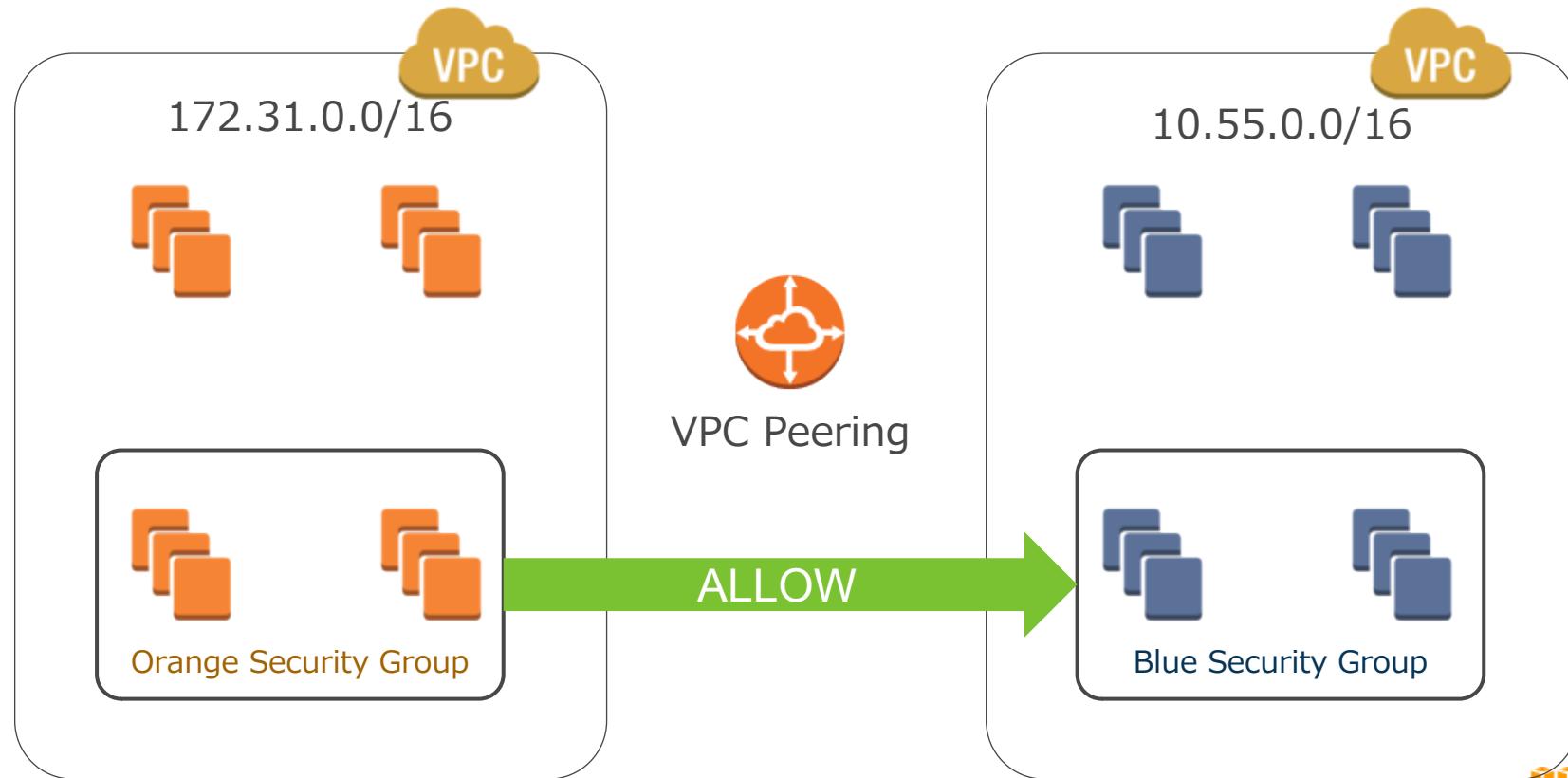


# VPC Peering (VPCピア接続)



- 2つのVPC間でトラフィックのルーティングが可能
- 同一のAWSアカウントはもちろん、異なるAWSアカウント間(クロスアカウント)のVPC間をピア接続することも可能
- 単一障害点や帯域幅のボトルネックは存在しない
- 以下の点に注意
  - MTU (VPC Peering 1,500byte)
  - 直接PeeringしているVPCとのみ通信可能 (2HOPは不可)
  - Regionは跨げない

# VPCピアリング先のセキュリティグループが指定可能



# Agenda

- Amazon VPCとは？
- VPCのコンポーネント
- オンプレミスとのハイブリッド構成
- VPCの設計
- **VPCの実装**
- VPCの運用
- まとめ



# VPCの実装方法

## マネージメント コンソール



## AWS CLI AWS SDK



```
aws ec2 create-vpc  
--cidr-block 10.0.0.0/16
```

```
from vpc.boto import VPCConection  
c = VPCConection()  
vpc = c.create_vpc('10.0.0.0/16')
```

## サードパーティツール



## AWS CloudFormation

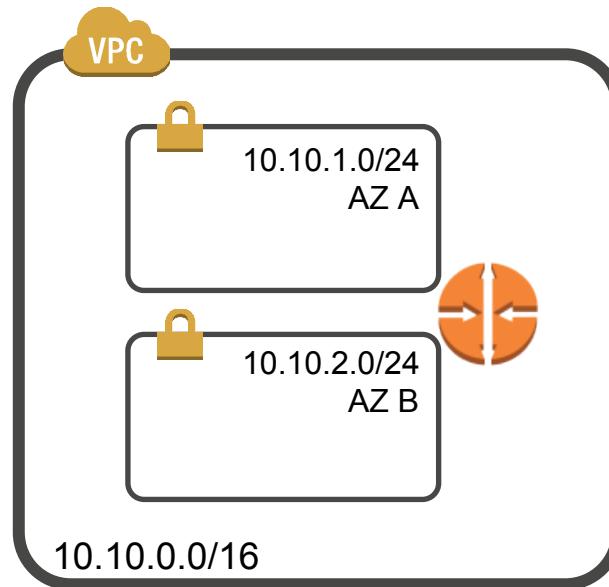


```
resource "aws_vpc" "main" {  
    cidr_block = "10.0.0.0/16"  
    tags {  
        Name = "main"  
    }  
}
```

```
{  
    "AWSTemplateFormatVersion" : "2010-09-09",  
    "Resources" : {  
        "myVPC" : {  
            "Type" : "AWS::EC2::VPC",  
            "Properties" : {  
                "CidrBlock" : "10.0.0.0/16",  
                "EnableDnsSupport" : "false",  
                "EnableDnsHostnames" : "false",  
                "InstanceTenancy" : "dedicated",  
                "Tags" : [ {  
                    "Key" : "foo",  
                    "Value" : "bar"  
                } ]  
            }  
        }  
    }  
}
```



# CLI - VPC作成



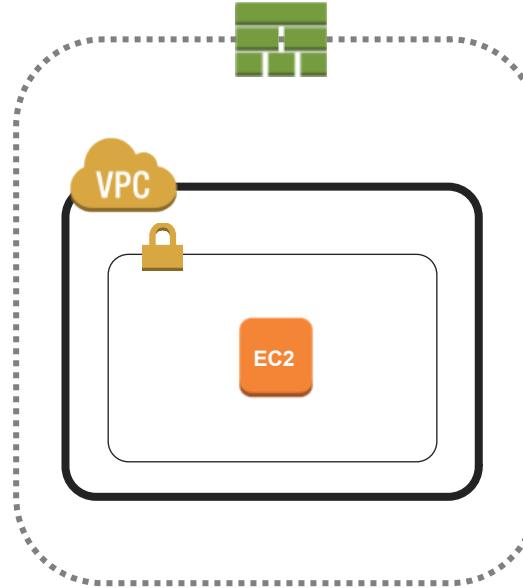
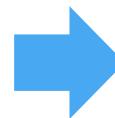
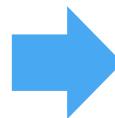
```
aws ec2 create-vpc --cidr 10.10.0.0/16
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.1.0/24 --a us-west-2a
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.2.0/24 --a us-west-2b
```

# AWS CloudFormation

JSON/YAMLテンプレートを元にAWS環境を構築



```
"AWSTemplateFormatVersion" : "2010-09-09",
"Resources" : {
  "myVPC" : {
    "Type" : "AWS::EC2::VPC",
    "Properties" : {
      "CidrBlock" : "10.0.0.0/16",
      "EnableDnsSupport" : "false",
      "EnableDnsHostnames" : "false",
      "InstanceTenancy" : "dedicated",
      "Tags" : [ {
        "Key" : "foo",
        "Value" : "bar"
      } ]
    }
  }
}
```



テンプレート  
(JSON形式)

CloudFormation

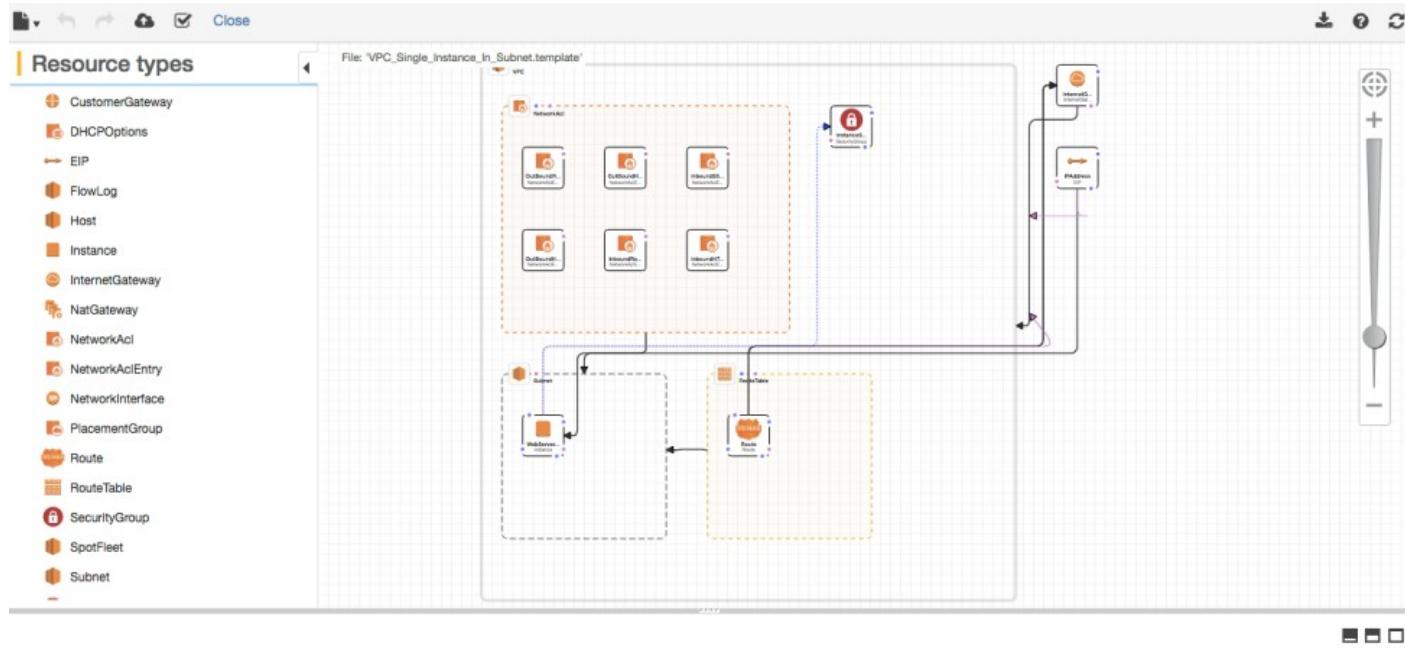
AWS環境(スタック)が完成

テンプレートサンプル : [http://docs.aws.amazon.com/ja\\_jp/AWSCloudFormation/latest/UserGuide/CHAP\\_TemplateQuickRef.html](http://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/CHAP_TemplateQuickRef.html)



# AWS CloudFormationデザイナー

GUIでテンプレートの作成が可能

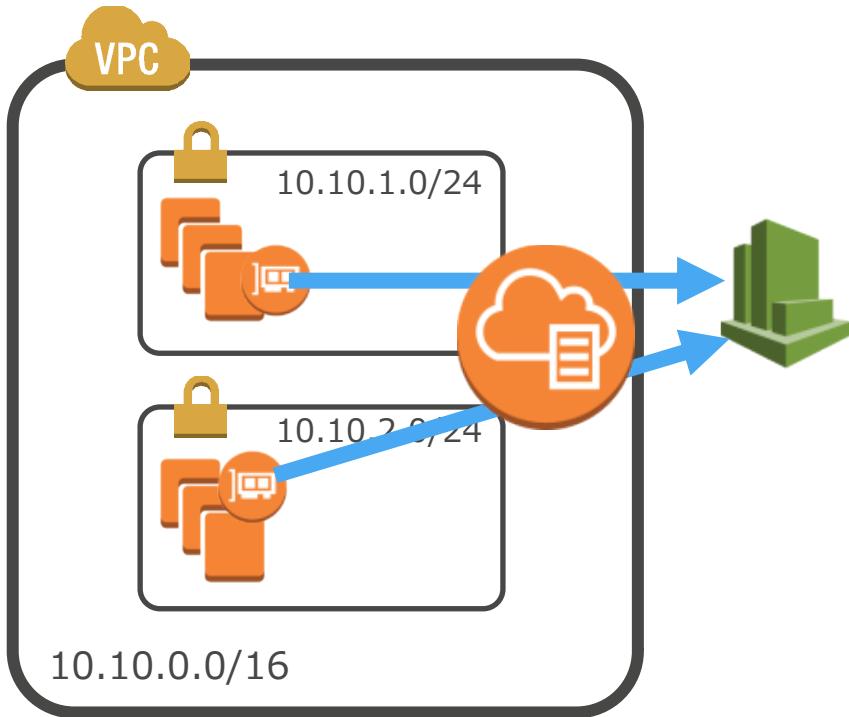


# Agenda

- Amazon VPCとは？
- VPCのコンポーネント
- オンプレミスとのハイブリッド構成
- VPCの設計
- VPCの実装
- **VPCの運用**
- まとめ



# VPC Flow Logsとは



- ・ネットワークトラフィックをキャプチャし、CloudWatch LogsへPublishする機能
- ・ネットワークインターフェースを送信元/送信先とするトラフィックが対象
- ・セキュリティグループとネットワークACLのルールでaccepted/rejectされたトラフィックログを取得
- ・キャプチャウインドウと言われる時間枠(約10分間)で収集、プロセッシング、保存
- ・RDS, Redshift、ElasticCache WorkSpacesのネットワークインターフェーストラフィックも取得可能
- ・追加料金はなし(CloudWatch Logsの標準料金は課金)

# 実際のレコード

2 123456789010 eni-abc123de

Version

account-id

interface-id

172.168.1.12 172.168.1.11

srcaddr

dsraddr

49761 3389 6 20 4249

srcport

dstport

protocol

packet

bytes

1418530010 1418530070 REJECT OK

start

end

action

log-status

# Flow Log レコードの項目

フィールド	説明
version	VPC flow logsのバージョン
account-id	flow logを取得したAWSアカウント
interface-id	ログストリームが適用されているネットワークインターフェースのID
srcaddr	送信元アドレス（※）
dsraddr	送信先アドレス（※）
srcport	送信元ポート
dsrport	送信先ポート
protocol	IANAで定義されたプロトコル番号
packets	キャプチャウインドウの中で取得したパケット数
bytes	キャプチャウインドウの中で取得したバイト数
start	キャプチャウインドウ開始時のUNIX時間
end	キャプチャウインドウ終了時のUNIX時間
action	トラフィックのアクション (ACCEPT/REJECT)
log-status	ログステータス (OK/NODATA/SKIPDATA)

Flow Log レコード:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html#flow-log-records>



# VPC Flow Logsで取得できない通信

- Amazon DNS サーバーへのトラフィック  
(独自の DNS サーバーを使用する場合は、その DNS サーバーへのすべてのトラフィックが記録される)
- Amazon Windows ライセンスのアクティベーション用に Windows インスタンスによって生成されたトラフィック
- インスタンスマタデータ用に 169.254.169.254 との間を行き来するトラフィック
- DHCP トラフィック
- デフォルトの VPC ルーターの予約済み IP アドレスへのトラフィック

# 利用例：CloudWatch メトリックフィルターとアラート作成

22/tcp(SSH)でREJECTされた通信をフィルタ

```
[version, account, eni, source, destination, srcip, destip="22",
 protocol="6", packets, bytes, windowstart, windowend,
 action="REJECT", flowlogstatus]
```

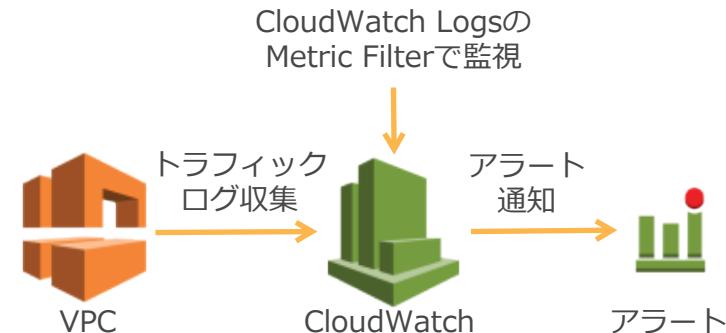
## CloudWatch Logs Metric Filter作成

Log Groups > Filters for flowlogsdemo

Add Metric Filter

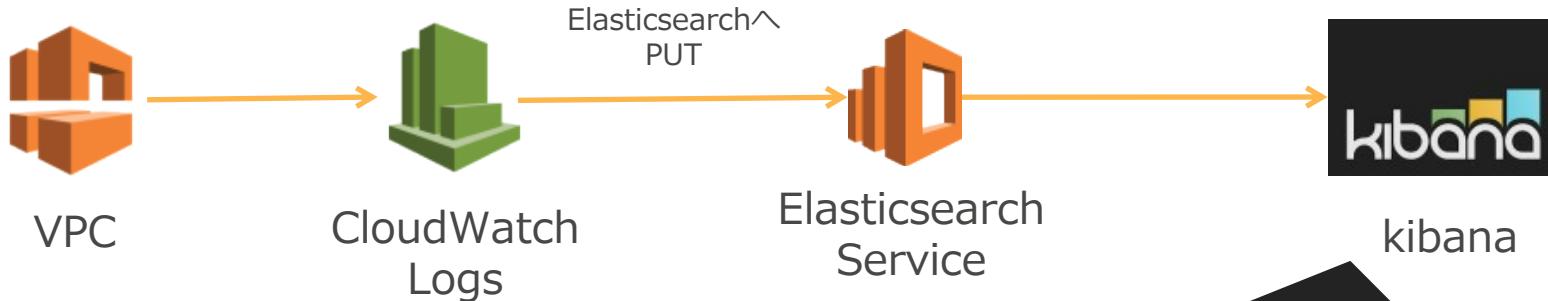
Filter Name: ssh\_login\_reject  
Filter Pattern: [version, account, eni, source, destination, srcip, destip="22", protocol="6", packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]  
Metric: flowlogs / ssh\_login\_alert  
Metric Value: 1

Create Alarm



[http://docs.aws.amazon.com/ja\\_jp/AmazonVPC/latest/UserGuide/flow-logs.html#flow-logs-cw-alarm-example](http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html#flow-logs-cw-alarm-example)

# 利用例：Elasticsearch Service + kibanaによる可視化



<https://blogs.aws.amazon.com/security/post/Tx246GOZNFIW79N/How-to-Optimize-and-Visualize-Your-Security-Groups>



# VPCのリミット関連

代表的なVPCのリミット

リソース	数
リージョン当たりの VPC の数	5
VPC 当たりのサブネットの数	200
AWS アカウント当たり、1 リージョン内の Elastic IP 数	5
ルートテーブル当たりのルートの数	100
VPCあたりのセキュリティグループの数	500
セキュリティグループあたりのルール数(In/Out)	50
ネットワークインターフェースあたりのセキュリティグループ	5
VPC当たりのアクティブなVPCピア接続	125
VPCあたり(仮想プライベートゲートウェイ)のVPN接続数	10

- デフォルトの上限値が増加したのもあります
  - [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Appendix\\_Limits.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html)
- Webサイトから制限解除申請可能
  - <http://aws.amazon.com/jp/contact-us/vpc-request/>
- 不明点はAWSサポートや担当営業までお問い合わせください。

# まとめ

- VPCにより、さまざまな要件に合わせたネットワークを簡単に作成可能
- 設計時には将来の拡張も見据えたアドレッシングや他ネットワークとの接続性も考慮する
- VPC構成は自社のITオペレーションモデルに合わせる
- VPC単体ではなくVPC全体の関係性も視野に入れる
- 実装や運用を補助するツールも有効利用

# Q&A



# 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
  - <http://aws.amazon.com/jp/aws-jp-introduction/>



サービス別資料	ソリューション別資料	業種別資料	その他の資料
無料オンラインセミナー 「Black Belt Online Seminar」のサービスカット資料他、AWSのTechメンバーによる各サービスの解説資料がご覧いただけます。	無料オンラインセミナー 「Black Belt Online Seminar」のソリューションカット資料他、特定のソリューションについてのAWS活用方法がご覧いただけます。	無料オンラインセミナー 「Black Belt Online Seminar」のインダストリーカット資料他、特定の業界のユースケースがご覧いただけます。	イベントに関する資料やアップデート情報などがご覧いただけます。

- 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
  - <http://aws.typepad.com/sajp/>

# AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は以下のリンクよりお気軽にご相談ください

<https://aws.amazon.com/jp/contact-us/aws-sales/>

The screenshot shows a web page with a sidebar on the left and a main content area on the right.

**\_sidebar:**

- 問い合わせ
- 日本担当チームへのお問い合わせ**
- 関連リンク
- フォーラム

**main content:**

## 日本担当チームへのお問い合わせ

AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。

※ご請求金額またはアカウントに関する質問は[こちらからお問い合わせください](#)。  
※Amazon.com または Kindle のサポートに問い合わせは[こちらからお問い合わせください](#)。

アスタリスク (\*) は必須情報となります。

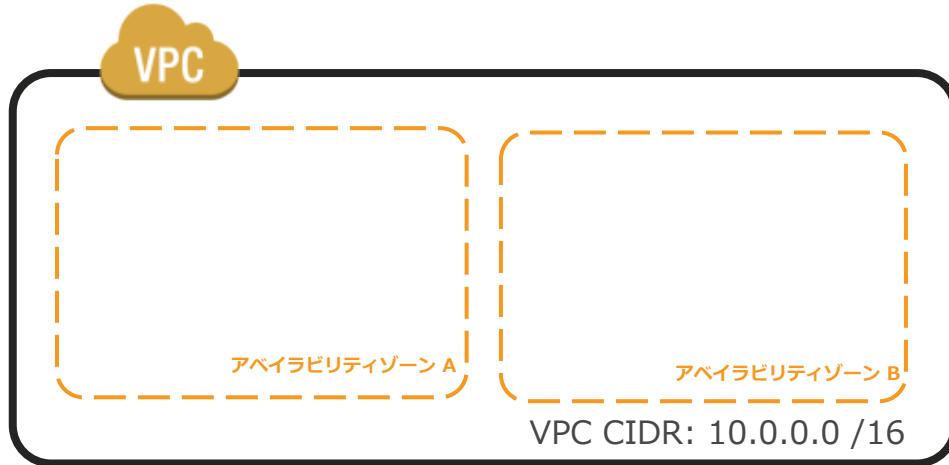
姓\*

名\*

※「AWS 問い合わせ」で検索してください

ご参加ありがとうございました

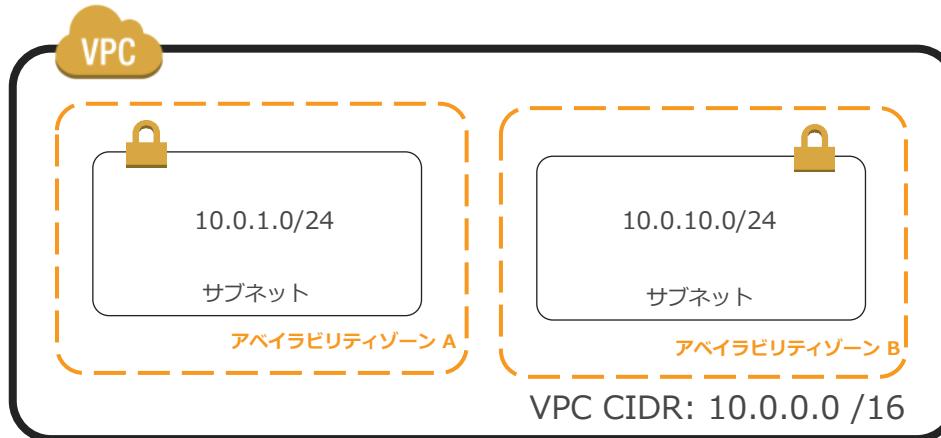
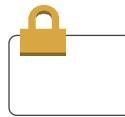




- ・仮想データセンターをAWS上に設定
- ・VPC内で利用するIPアドレスのブロックを設定
  - 通常であればプライベートアドレス(RFC1918)を利用
  - /28から/16のネットマスクを利用する
- ・複数のアベイラビリティゾーンを利用可能

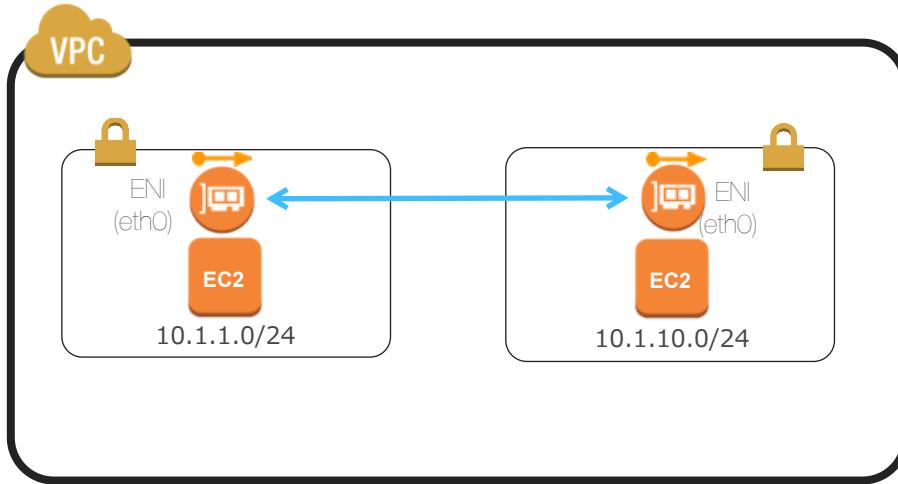
**作成後はVPCアドレスブロックは変更できないので注意！**

# サブネット



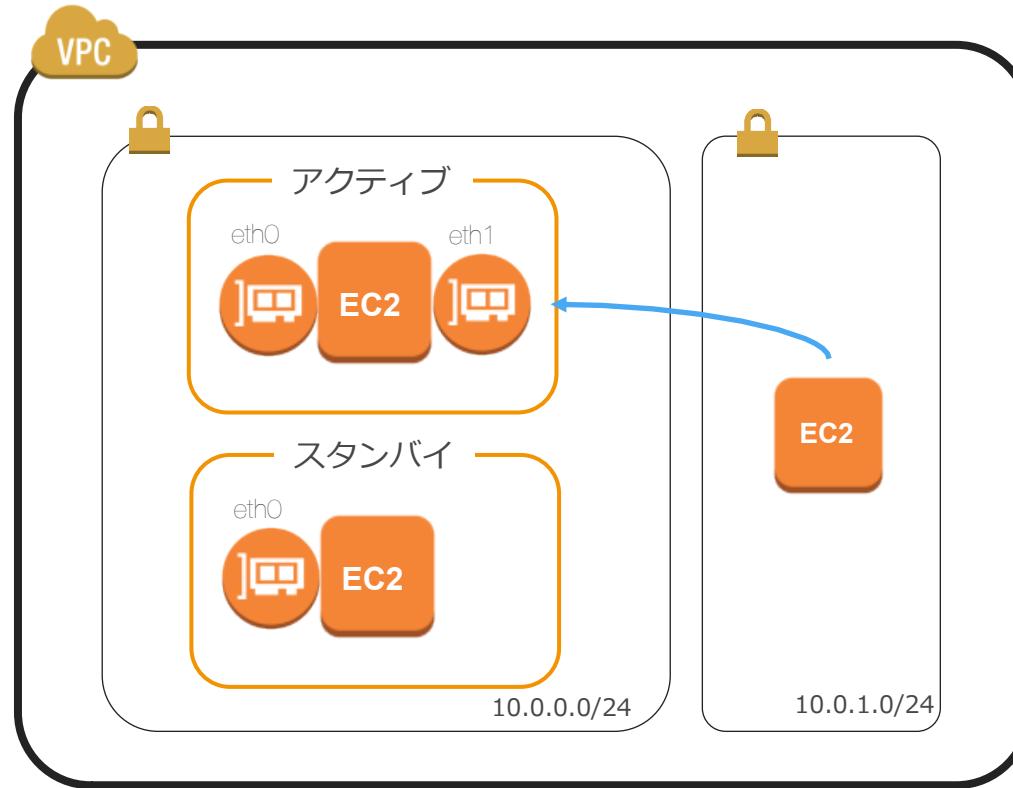
- ・VPCのIPアドレス範囲(CIDR)の中で設定
- ・アベイラビリティゾーン毎に設定
- ・ネットワークACL(アクセスリスト)でネットワークレベルでのセキュリティを設定
- ・サブネット毎にルーティングを設定
- ・最小は/28(14IP)

# Elastic ネットワークインターフェース

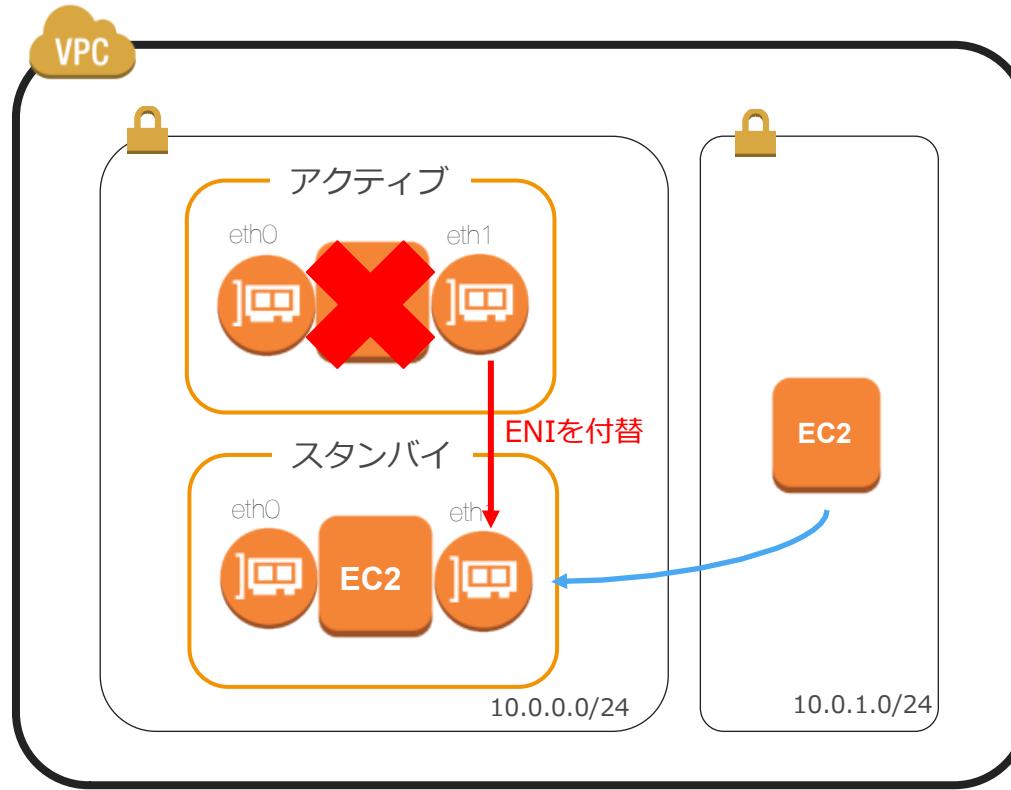


- EC2で利用するネットワークの仮想インターフェース
- EC2インスタンス毎に仮想ネットワークインターフェースを複数持つことが可能
- 以下をENIに紐づけて維持可能  
プライベートIP  
Elastic IP  
MACアドレス  
セキュリティグループ
- 固定のプライベートIPを設定することが可能
- VPC内のマネージドサービスでも暗黙的に利用されている

# ENIを使ったフェールオーバー(Floating IP)



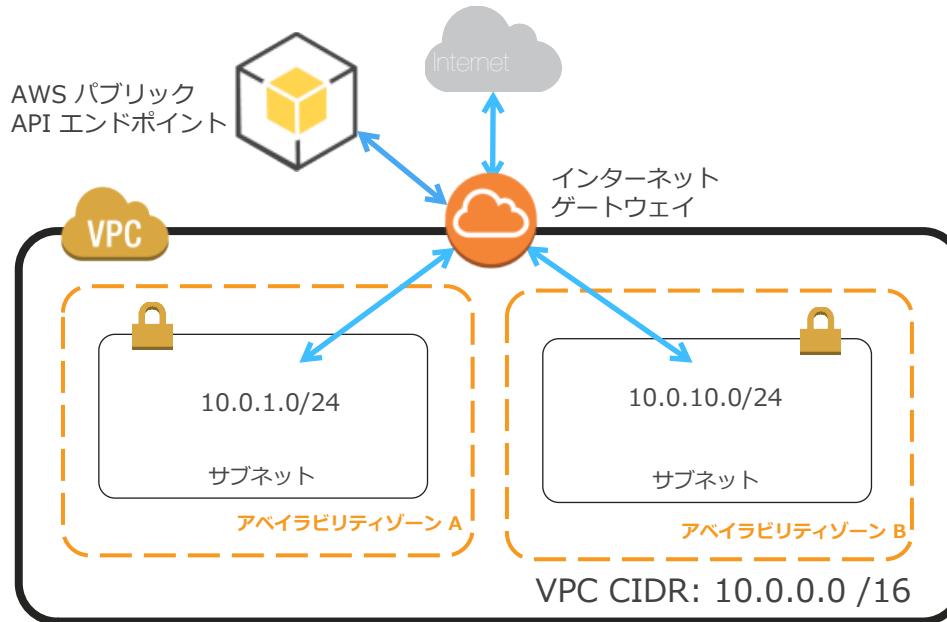
# ENIを使ったフェールオーバー(Floating IP)



[http://aws.clouddesignpattern.org/index.php/CDP:Floating\\_IP](http://aws.clouddesignpattern.org/index.php/CDP:Floating_IP)

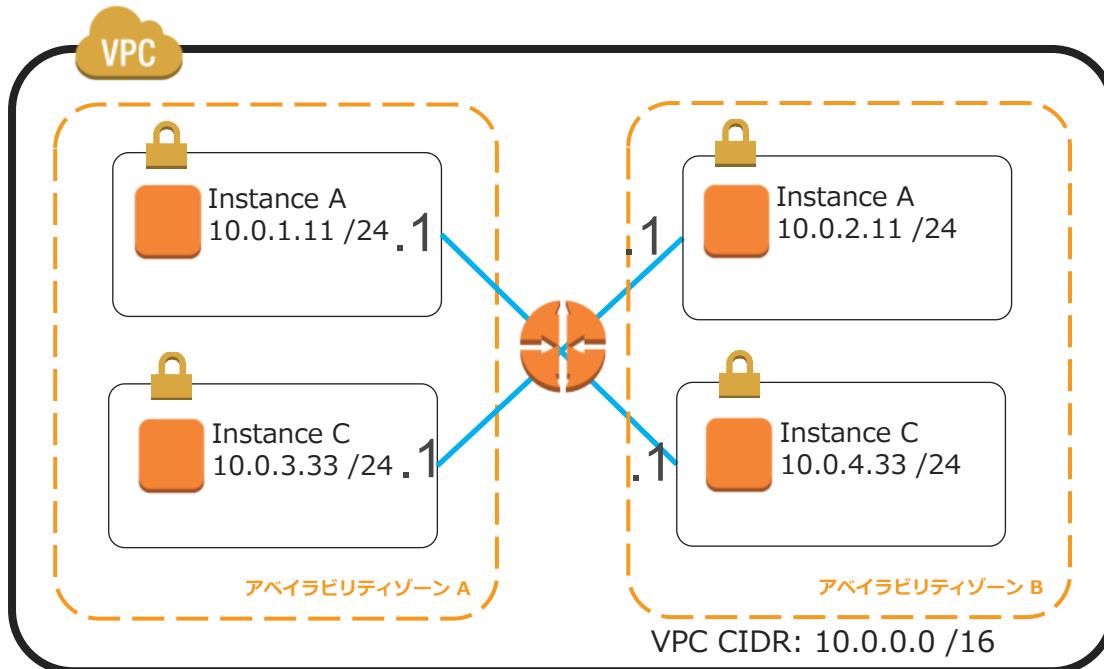


# インターネットゲートウェイ(IGW)



- ・VPC内のリソースにインターネットへの接続を提供
- ・VPCにアタッチすることで利用可能
- ・サブネットでルーティング指定
- ・単一障害点や帯域幅のボトルネックは存在しない

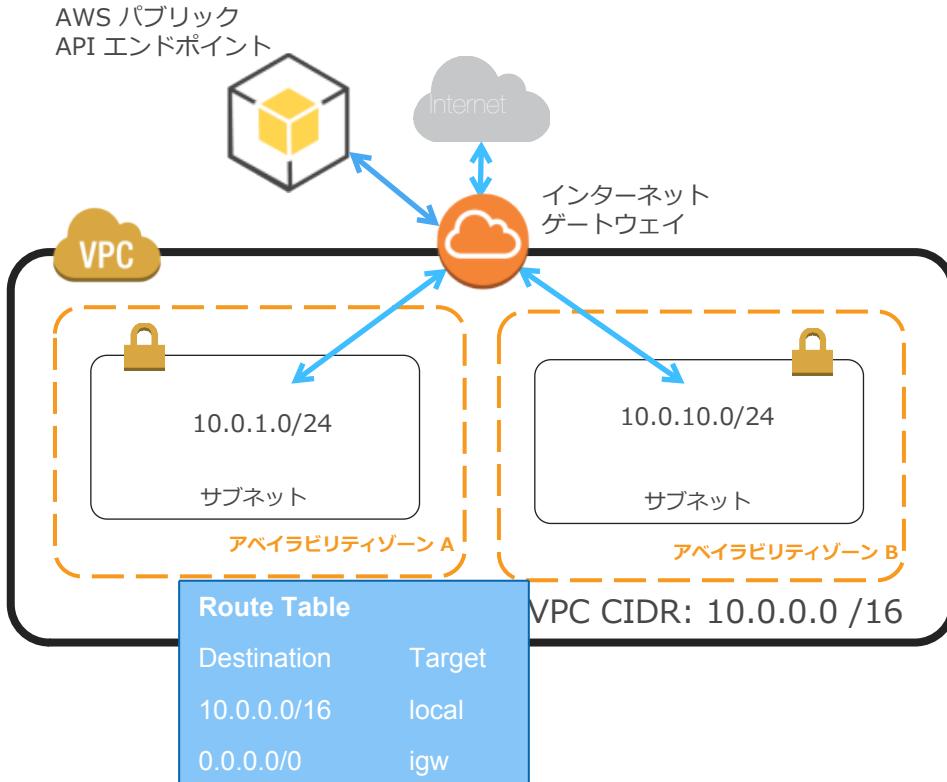
# 仮想ルータ



- ・VPC内のすべてのサブネット間はネットワーク的に疎通可能  
(制御したい場合はネットワークACLを利用)
- ・サブネットのネットワークアドレス+1(.1)がすべてのサブネットのゲートウェイとなる
- ・ユーザが操作するコンポーネントではなく、暗黙的に動作している

# ルートテーブル

10.1.1.0  
10.1.2.0  
10.1.3.0



- サブネット内の通信がどの宛先のネットワークに対してどのコンポーネントに転送されるべきかの定義を記述  
(例: インターネットへの通信はIGW)
- 各サブネットに1つ設定
- 1つのルーティングテーブルには複数のサブネットがマッピング可能
- 必ずVPCのCIDRが"local"として登録されている
- サブネットのデフォルト状態ではメインルートテーブルが設定されている

[http://docs.aws.amazon.com/ja\\_jp/AmazonVPC/latest/UserGuide/VPC\\_Route\\_Tables.html](http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html)



# メインルートテーブルとカスタムルートテーブル

## メインルートテーブル



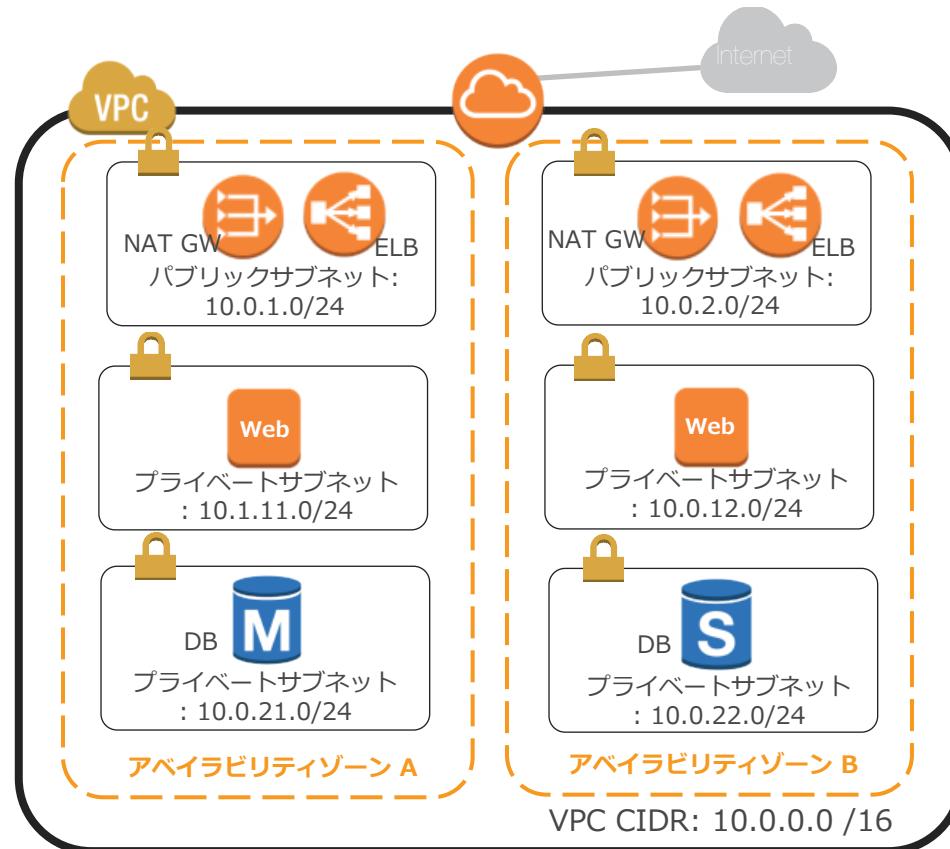
VPCを作成したときに自動的に割当てられるルートテーブル。  
サブネットでルートテーブルの指定が無い場合はメインルートテーブルが割当てられる。

## カスタムルートテーブル



任意で作成したルートテーブル。  
明示的に各サブネットへ割り当てることが可能。  
カスタムルートテーブルをメインルートテーブルに変更することが可能。

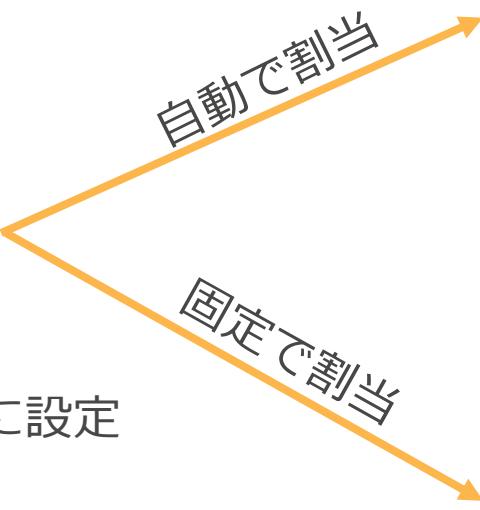
# Webサービスの構成例



# パブリックサブネットの設定

172.16.0.0
172.16.1.0
172.16.2.0
<b>Route Table</b>
Destination      Target
10.1.0.0/16      local
0.0.0.0/0      igw

デフォルトルートをigwに設定

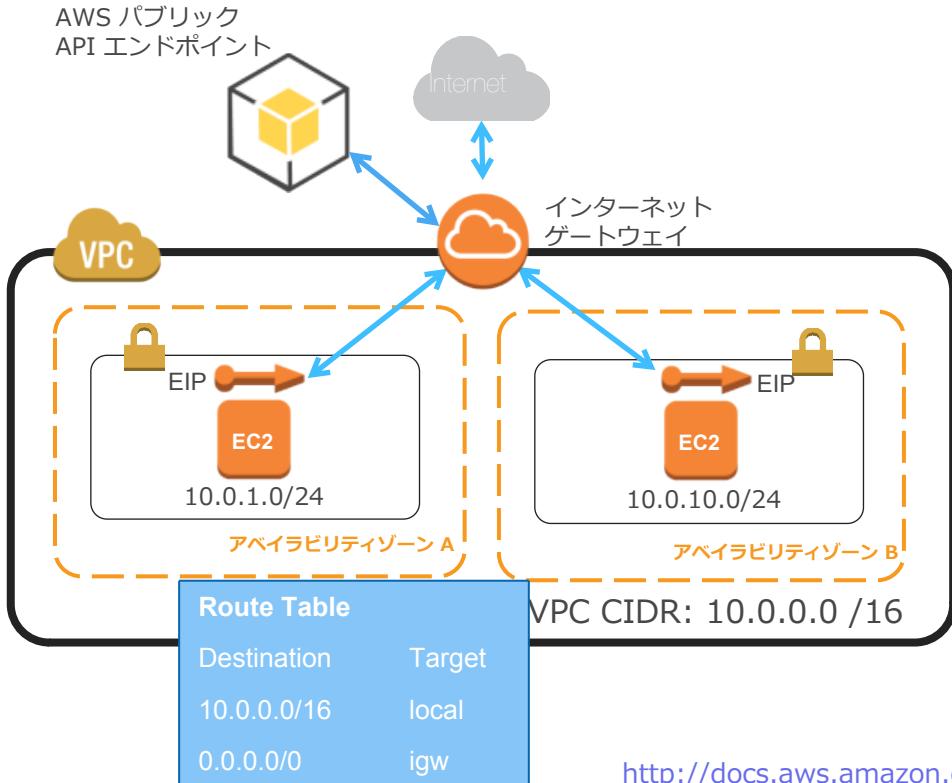


サブネットに自動割当てを設定



ElasticIPをアタッチ

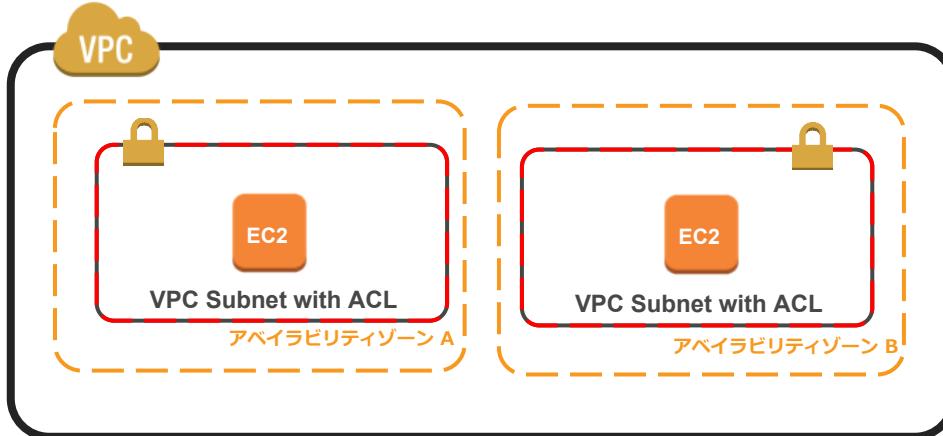
# Elastic IP ➔



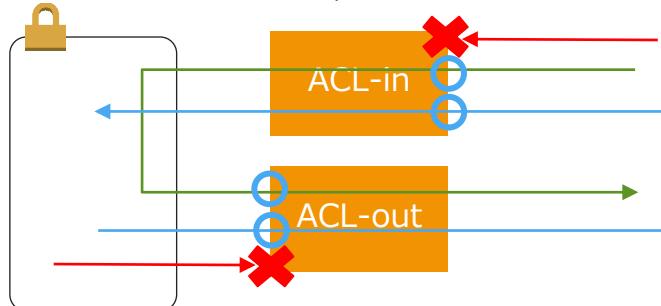
- ・アカウントに紐付けられる固定のパブリックIP
- ・EC2インスタンスに割り当て可能
- ・インスタンスあたり1EIPは無料
- ・費用がかかるのは以下のケース
  - 追加でEIPを利用する場合
  - 起動中のEC2インスタンスに割当てられていない場合
  - アタッチされていないENIに割当てられている場合
  - 1ヶ月間でリマップ(割当て、取り外し)が100回を超えた場合

[http://docs.aws.amazon.com/ja\\_jp/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html](http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html)

# □ ネットワークアクセスコントロールリスト



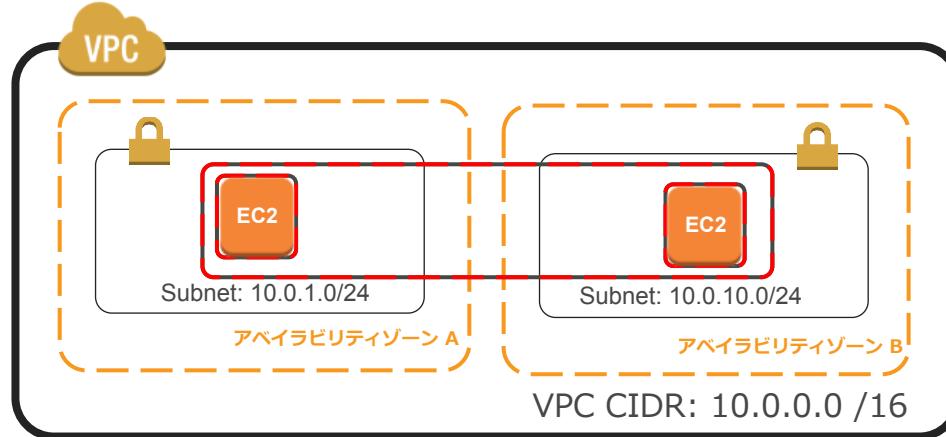
ステートレスなのでinに対するout, outに対するinも設定が必要



- ・サブネット毎に設定するフィルタ機能
- ・インバウンド、アウトバウンドをサブネット毎に制御
- ・ステートレス
- ・デフォルトはすべて許可

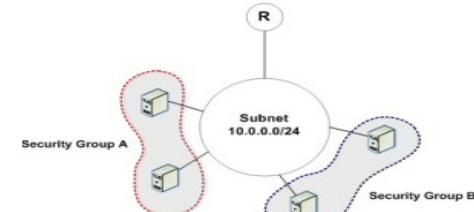
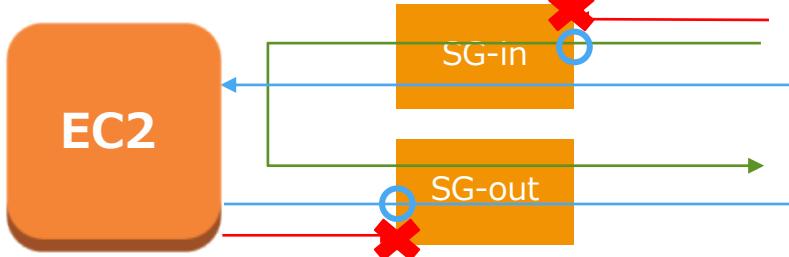


# セキュリティグループ



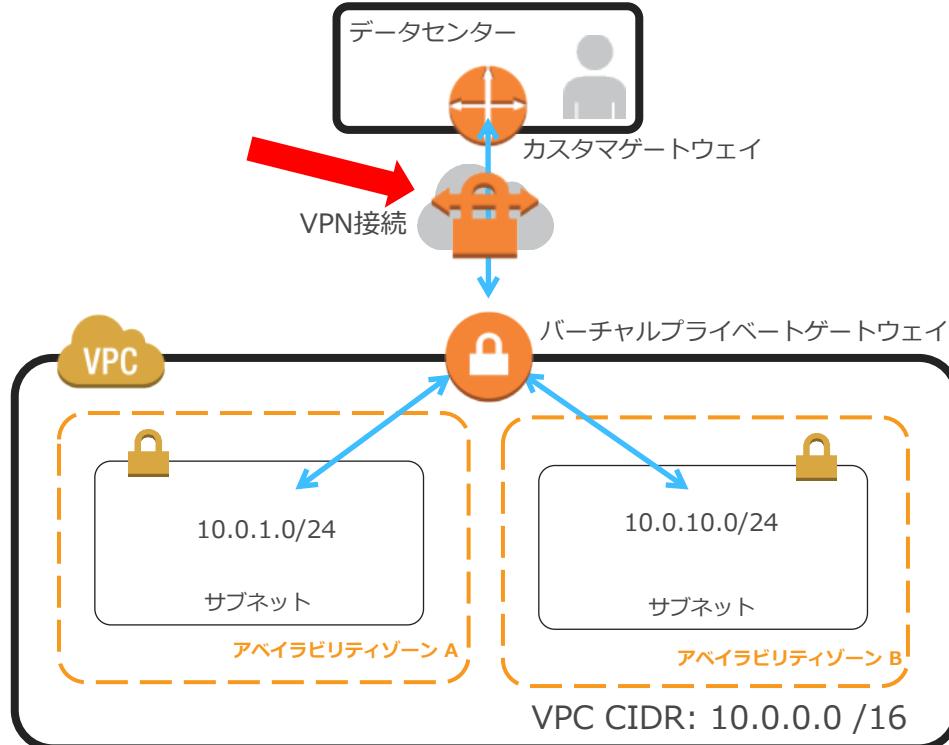
- EC2インスタンスの仮想ファイアウォールとして機能
- 1つのEC2インスタンスあたり5つのセキュリティグループを設定可能
- ステートフル
- デフォルトですべての通信は禁止
- 複数のEC2インスタンスをグルーピング可能

ステートフルなのでinに対するout, outに対するinは設定しなくてOK



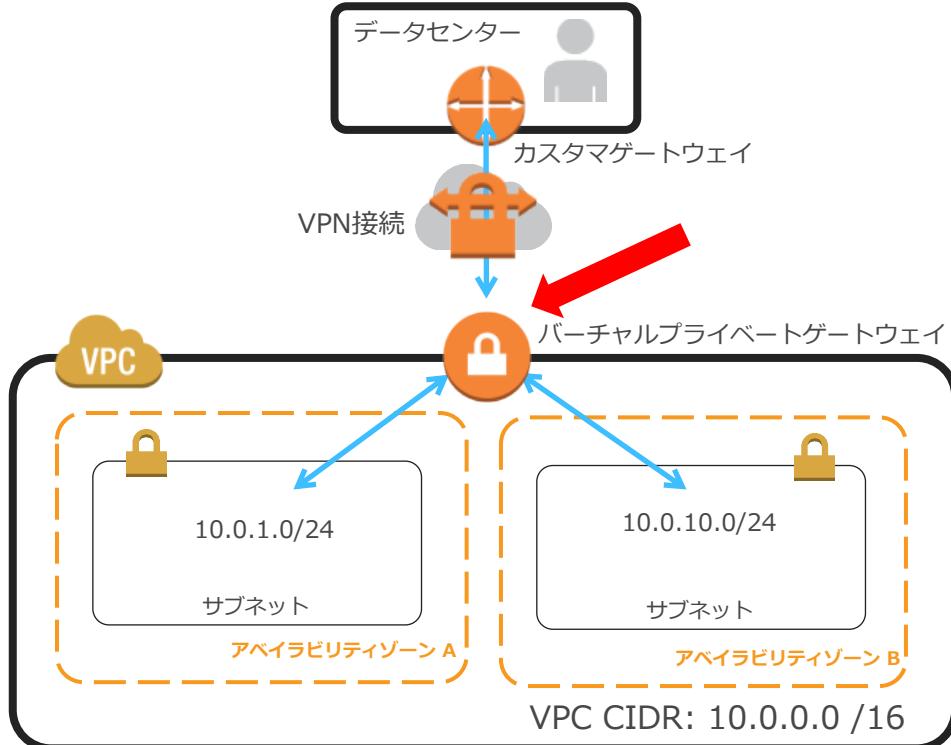
[http://docs.aws.amazon.com/ja\\_jp/AmazonVPC/latest/UserGuide/VPC\\_SecurityGroups.html](http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

# VPN接続



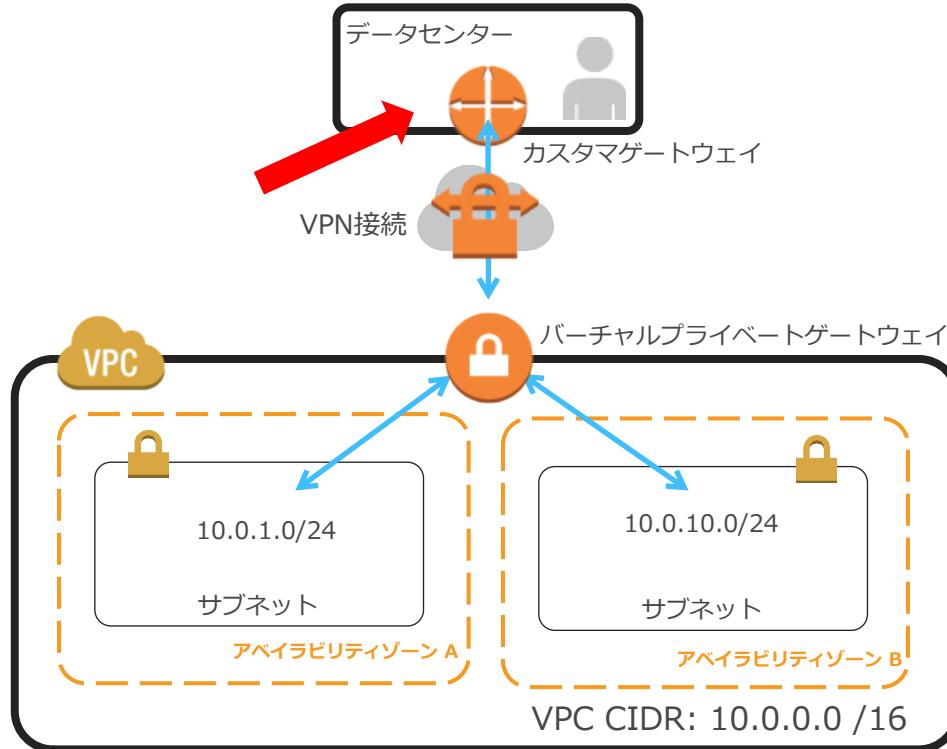
- ・VPCとオンプレミス間のVPN接続
- ・CGWとVGWの間でIPsecトンネルが設定される

# バーチャルプライベートゲートウェイ(VGW)



- ・オフィスやデータセンターなどのオンプレミスとのVPN接続のためのエンドポイントとなる仮想ルータ
- ・Direct Connect(専用線)のエンドポイントとしても利用
- ・1つのVPCあたり1つのVGWのみアタッチ可能
- ・1つのVGWで複数のVPN、Direct Connectのコネクションを終端
- ・单一障害点や帯域幅のボトルネックは存在しない

# カスタマゲートウェイ(CGW)



- AWSとのVPNを接続する物理的または仮想的なルータ
- VGWとVPN接続を行なう
- お客様にて準備/設定いただく
- サンプルコンフィグをダウンロード可能

[http://docs.aws.amazon.com/ja\\_jp/AmazonVPC/latest/NetworkAdminGuide/Introduction.html](http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/NetworkAdminGuide/Introduction.html)

# リージョン間のVPC間接続例

