[AWS Black Belt Online Seminar]
Amazon VPC

サービスカットシリーズ

Solutions Architect 菊池 之裕
2020/10/21

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

過去資料
https://amzn.to/JPArchive

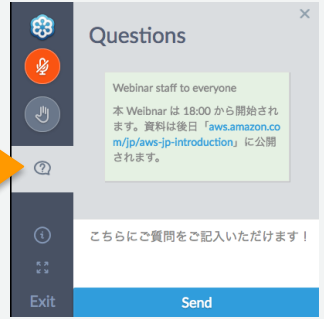
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、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10月21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.

自己紹介

名前：菊池　之裕(きくち　ゆきひろ)

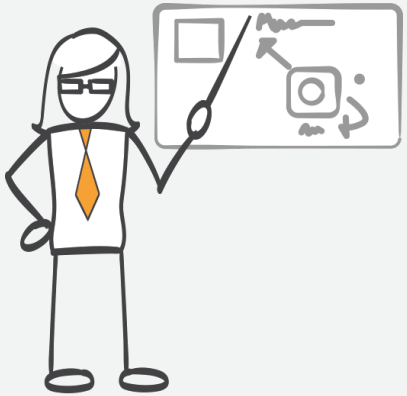
所属：ソリューションアーキテクト ネットワークスペシャリスト

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:Transit Gateway,Direct Connect,Marketplace

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

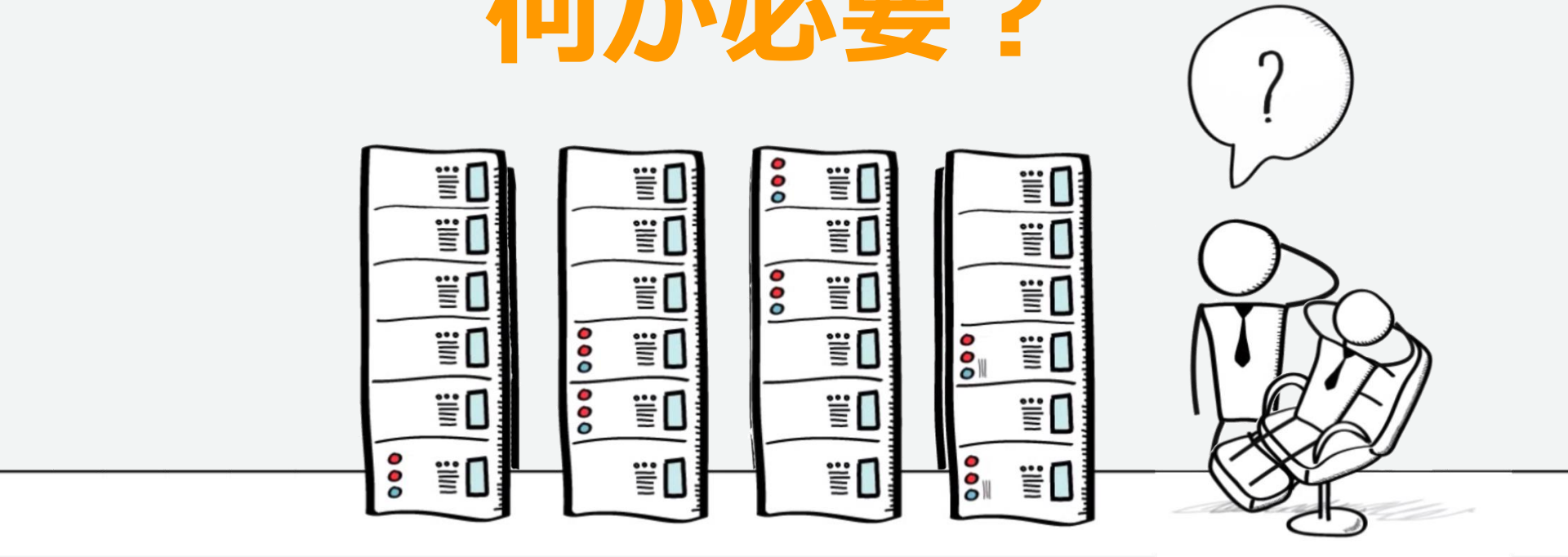
Amazon VPCとは？
VPCのコンポーネント
オンプレミスとのハイブリッド構成
VPCの設計
VPCの実装
VPCの運用
まとめ

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？



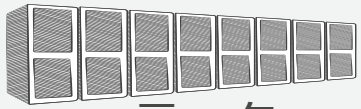
オンプレミス環境でのネットワークのイメージ

土地、電源、UPS、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

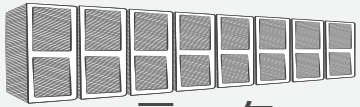
ネットワーク機器

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！

バーチャル
プライベート
ゲートウェイ

インターネット
ゲートウェイ

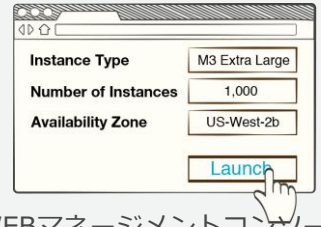
Elastic IP

Elastic
ネットワーク
インタフェース

ルート
テーブル

仮想ルータ

NAT
ゲートウェイ



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

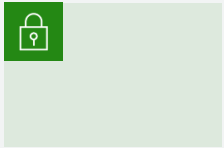
- インターネット経由
- VPN/専用線(Direct Connect)

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


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

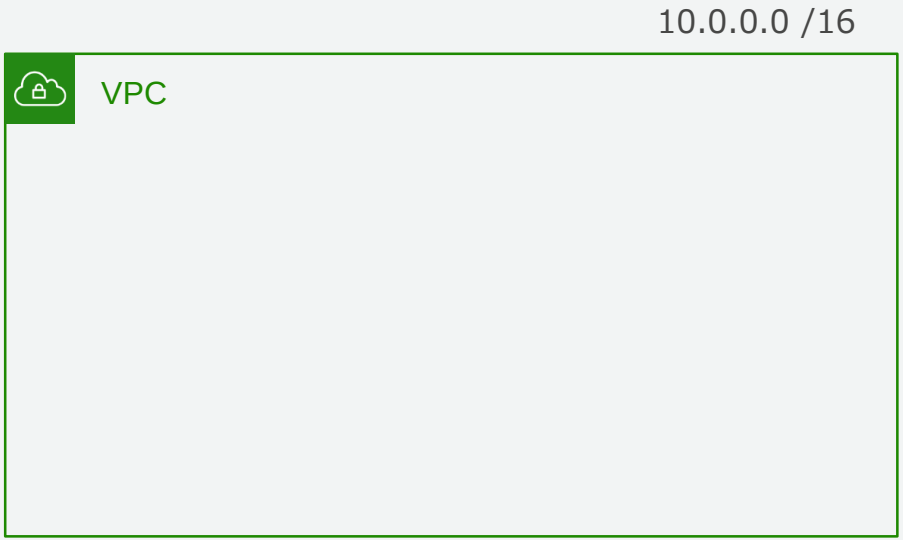

カスタマ
ゲートウェイ


Elastic
ネットワーク
インタフェース

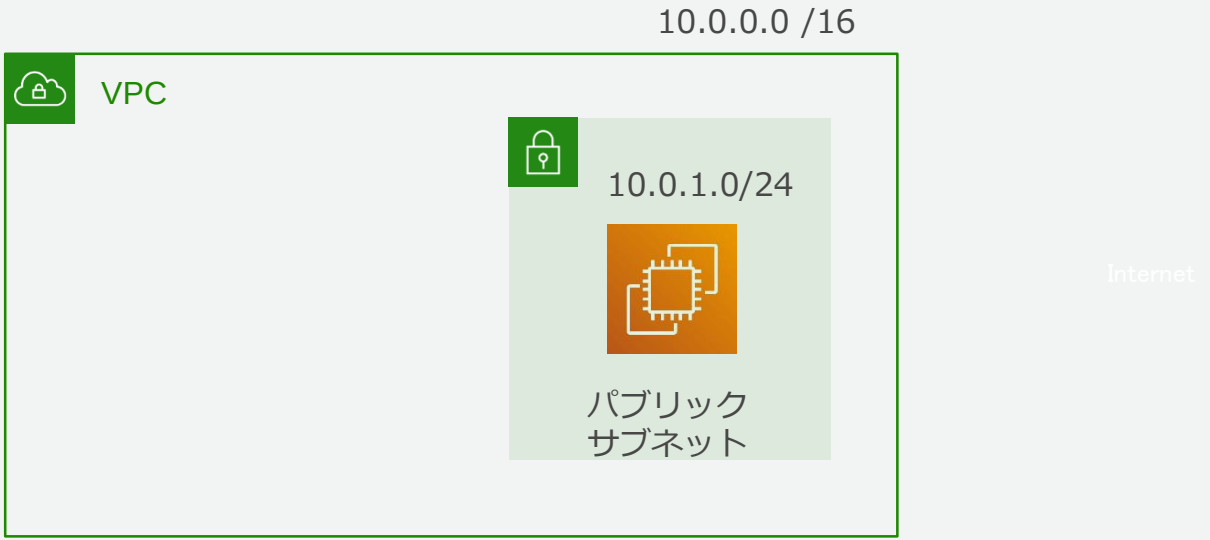

Elastic
ネットワーク
アダプタ


PrivateLink

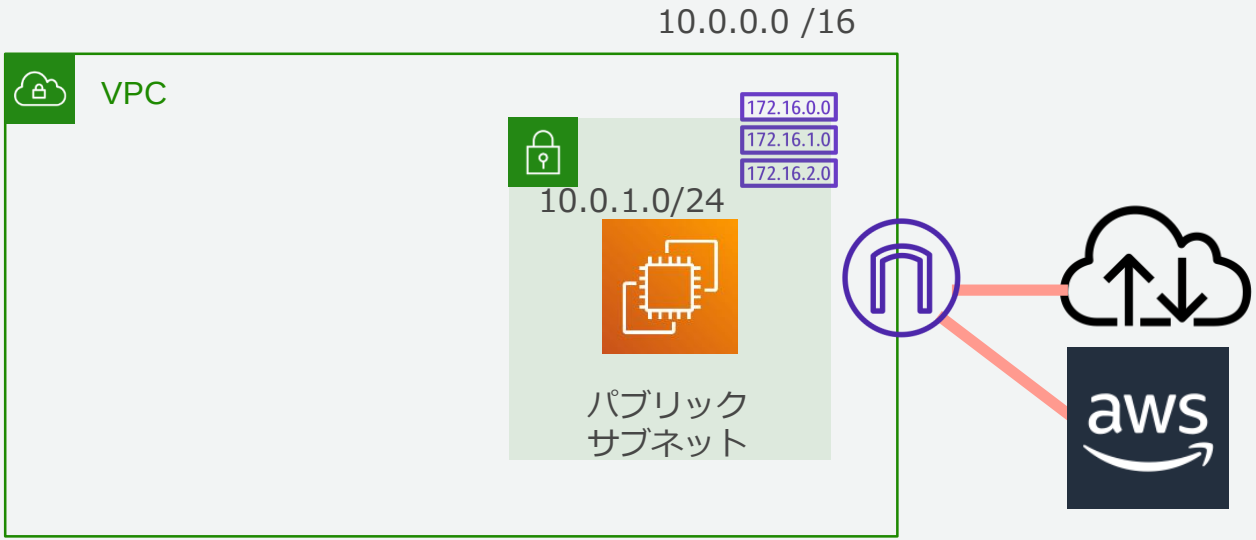
まずは全体のネットワーク空間をVPCとして定義



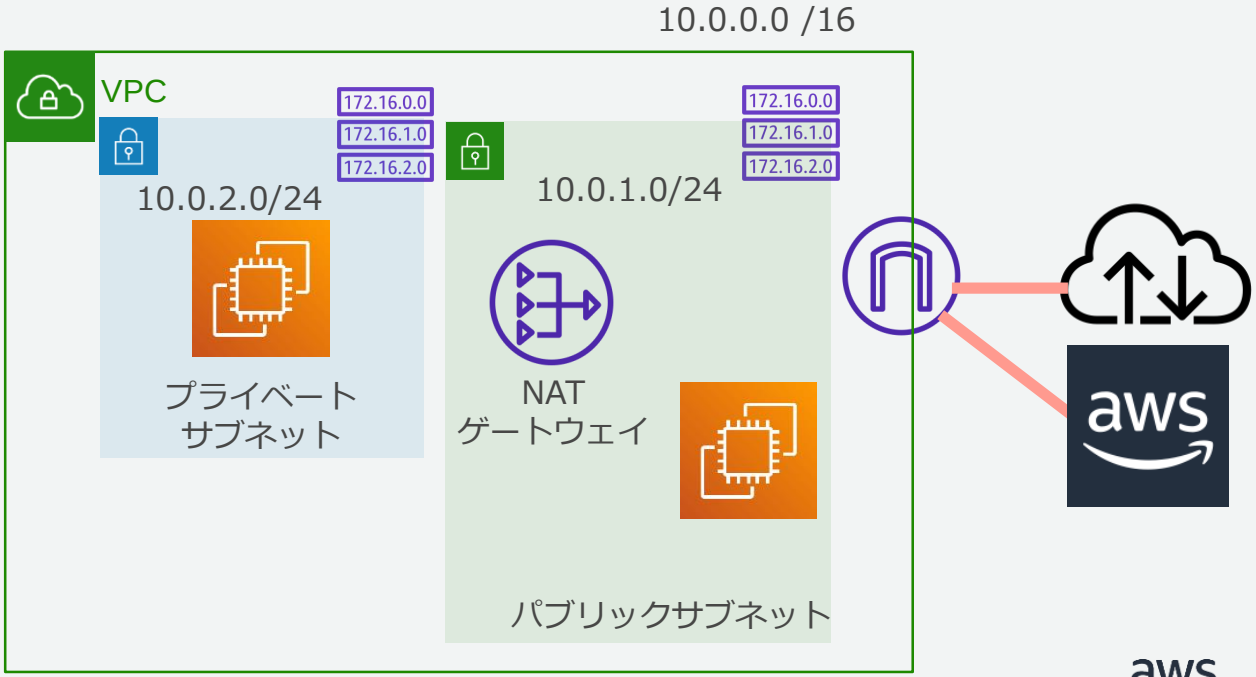
利用するサブネットを定義



インターネットへの接続を設定

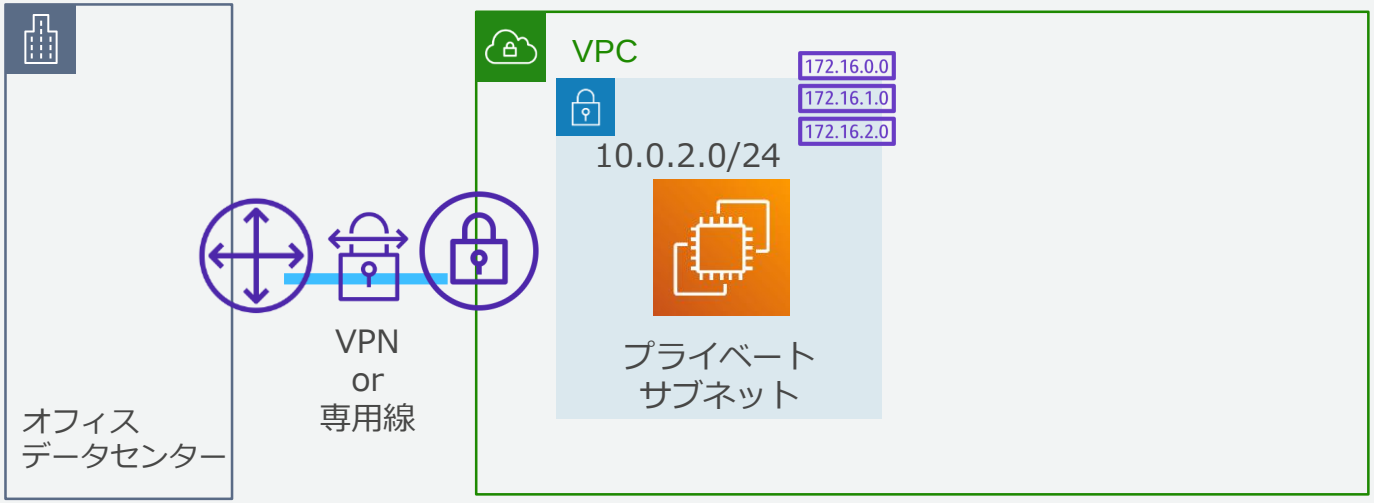


プライベートサブネットを追加

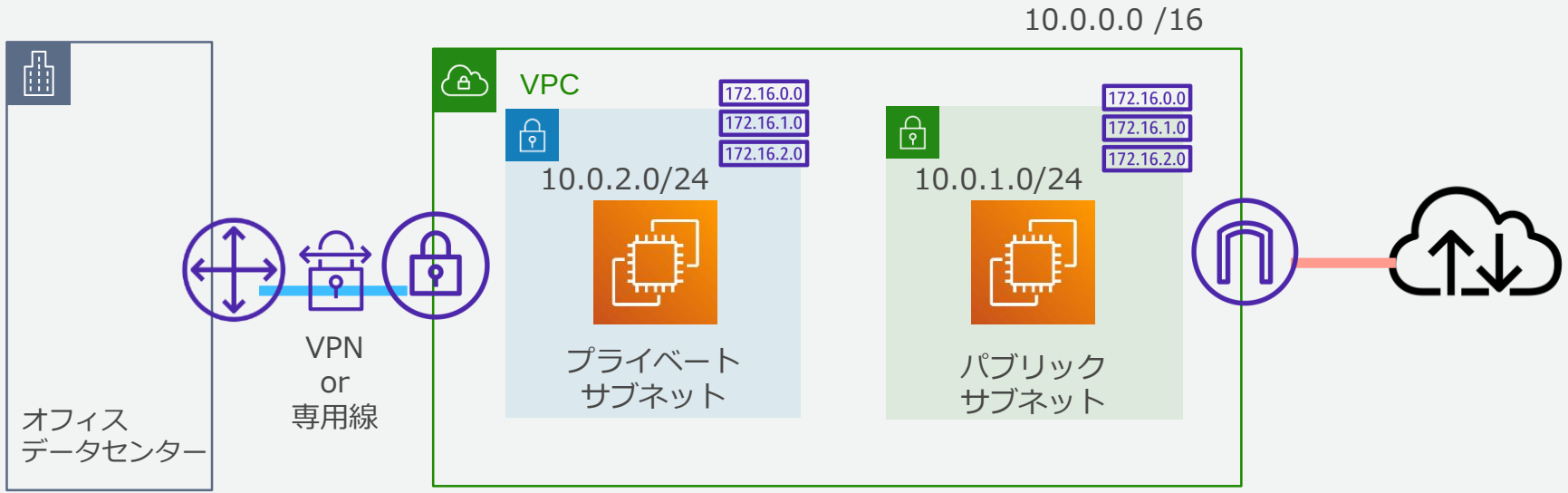


インターネットに接続しないネットワークも作成可能

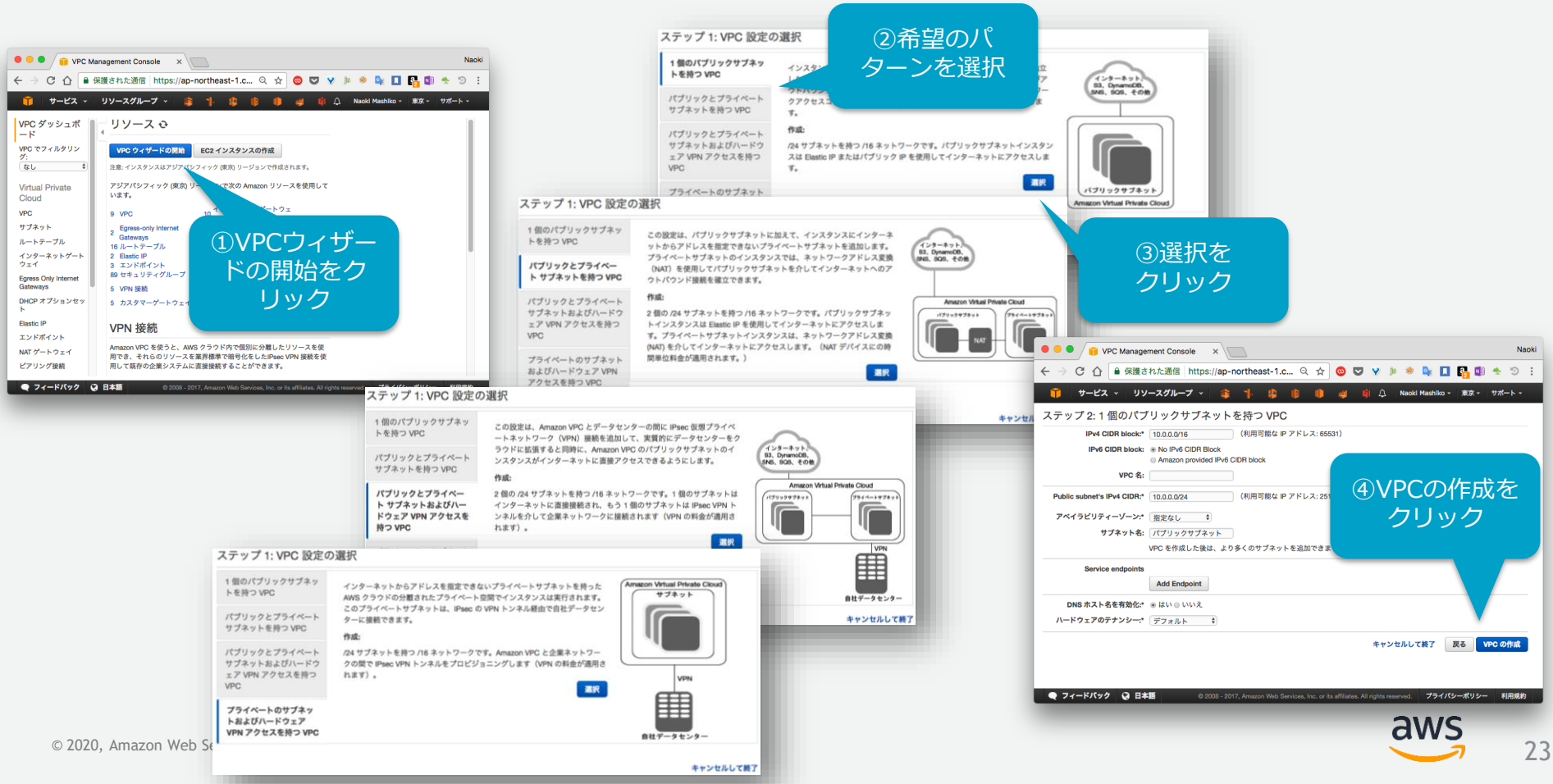
オンプレミスとの接続



ネットワーク要件に応じて自由に設定可能

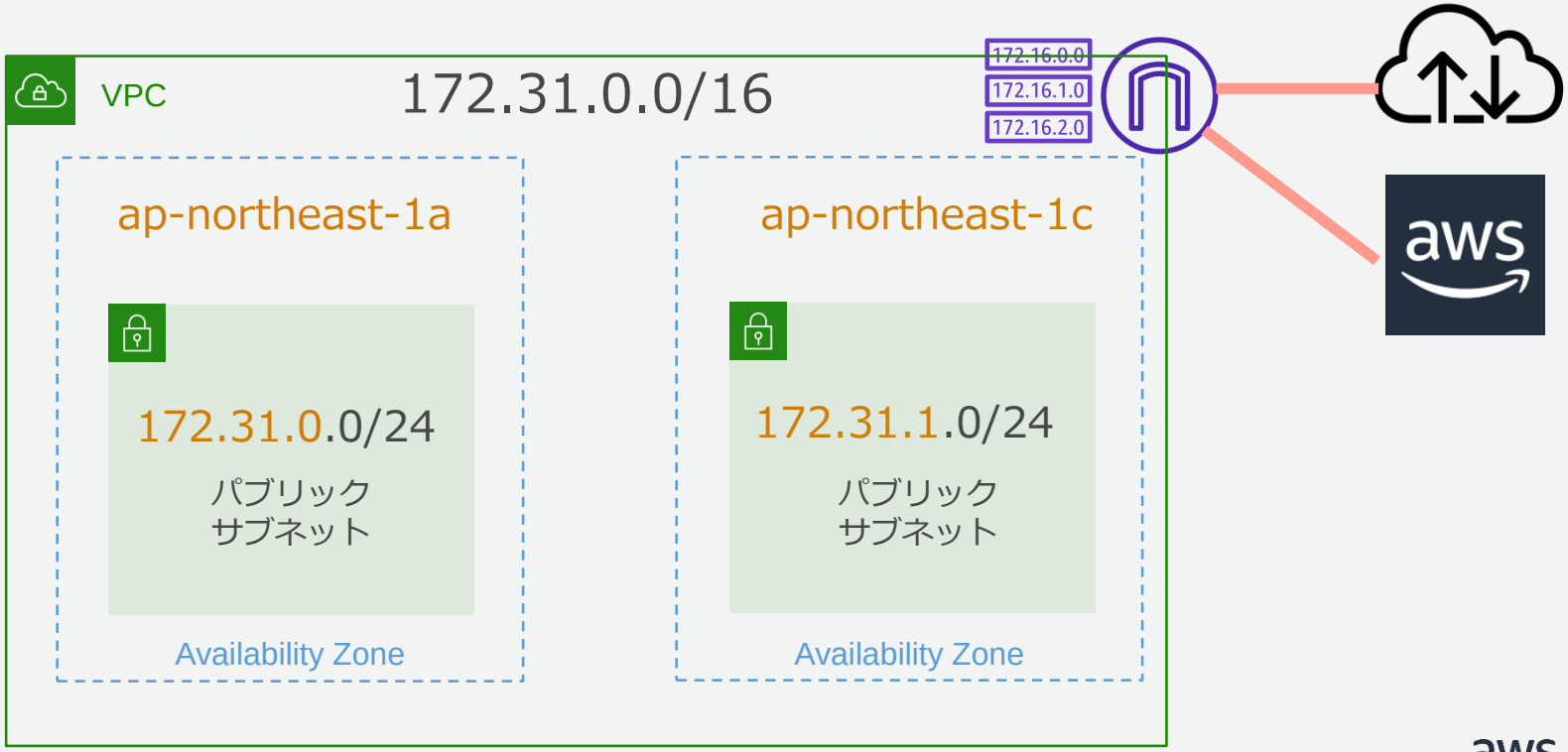


VPCウィザードで数画面で作成可能

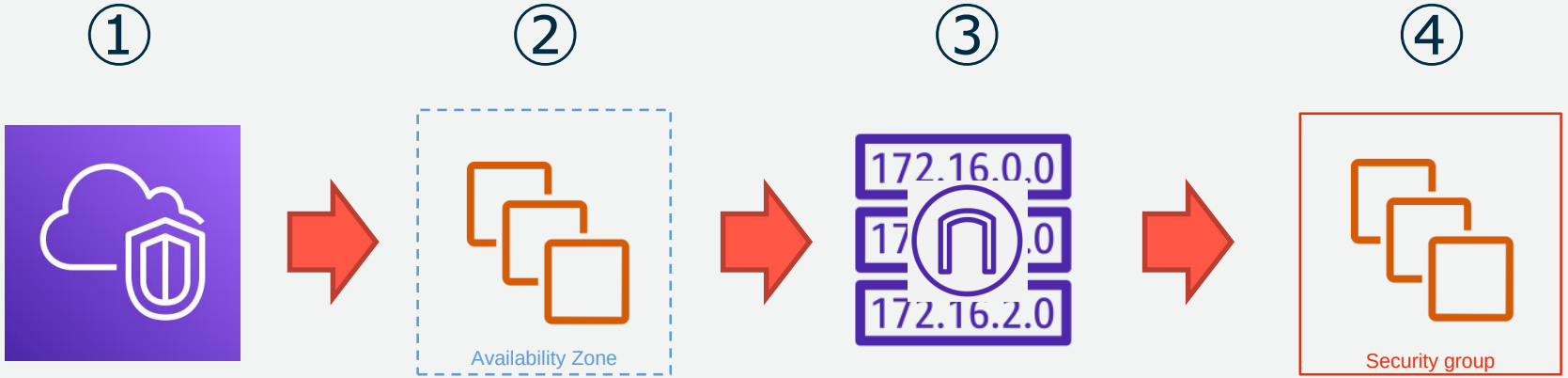


ウォークスルー:
インターネット接続VPCセットアップ

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



アドレスレンジを選択

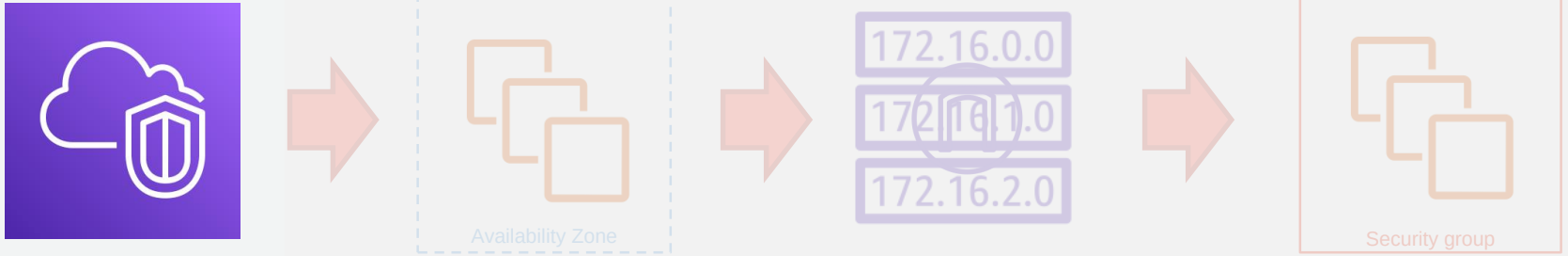
Availability Zoneにおける Subnetを選択

インターネットへの経路を設定

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

① ② ③ ④



アドレスレンジを選択

Availability Zoneにおける Subnetを選択

インターネットへの経路を設定

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

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

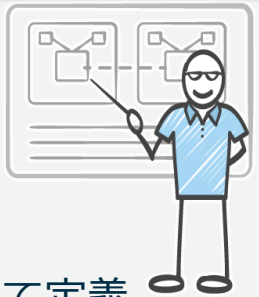
CIDR レンジのサンプル:

172.31.0.0/16

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

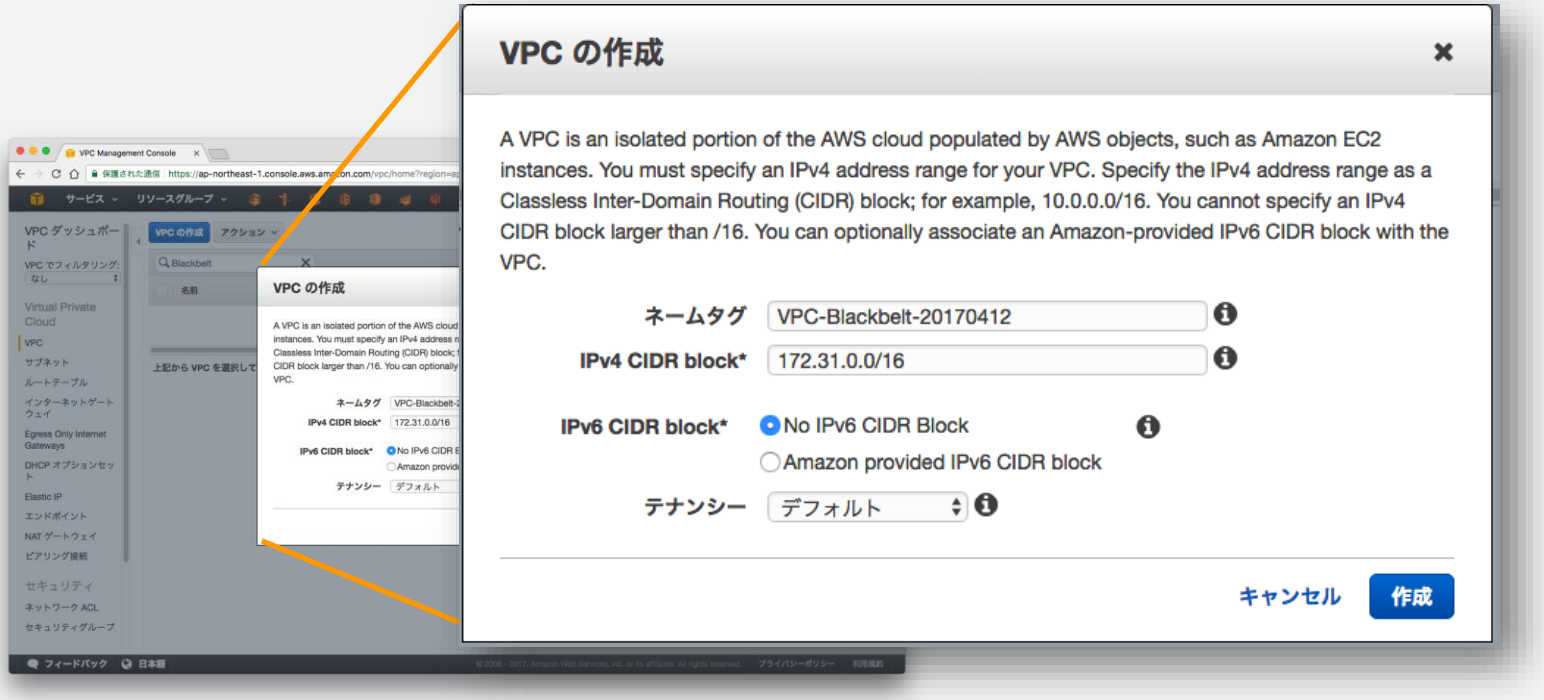
172.31.0.0/16

推奨: RFC1918レンジ
衝突で使えない場合は
RFC6598(100.64.0.0/10)

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。

VPCの作成



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

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 CIDR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

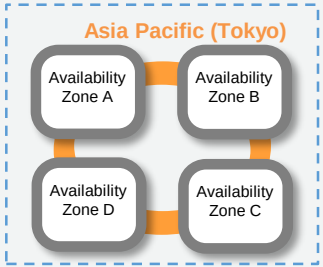
サブネットマスク	サブネット数	サブネットあたりのIPアドレス数
/18	4	16379
/20	16	4091
/22	64	1019
/24	**256 ※**	**251**
/26	1024 ※	59
/28	16384 ※	11

※ VPCあたりのサブネット作成上限数はデフォルト２００個

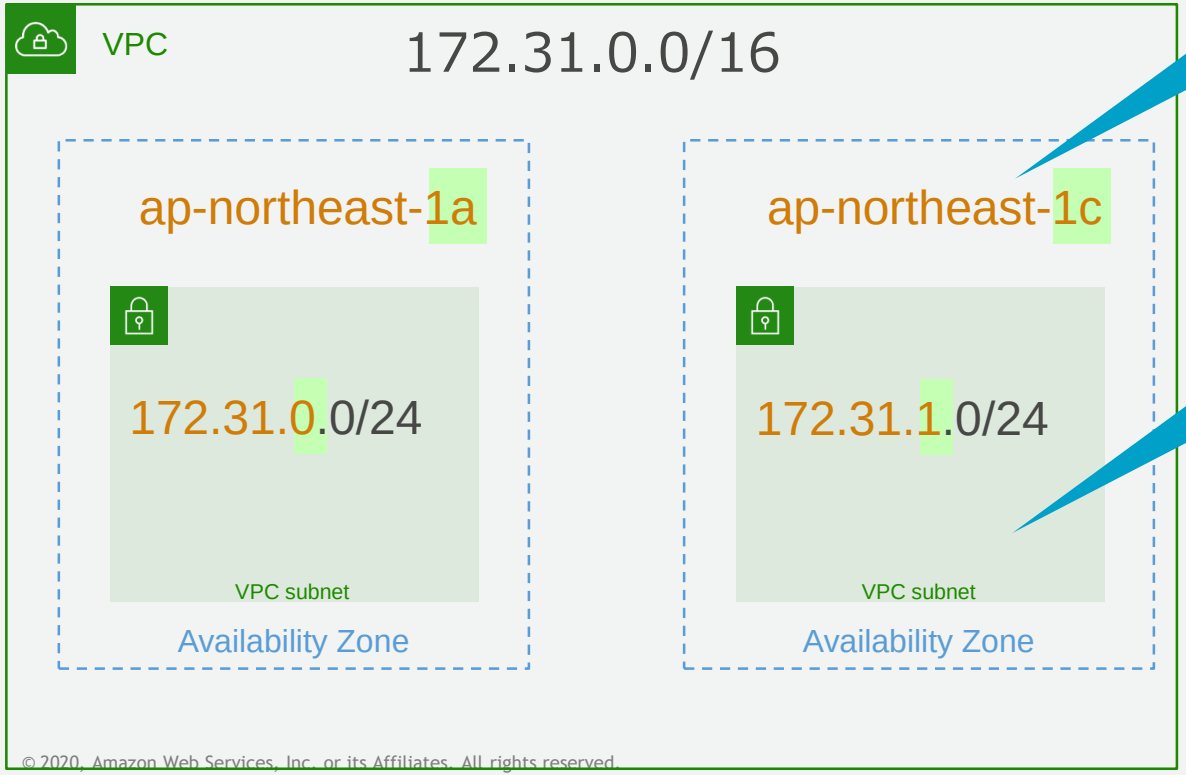
アベイラビリティゾーン

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（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）



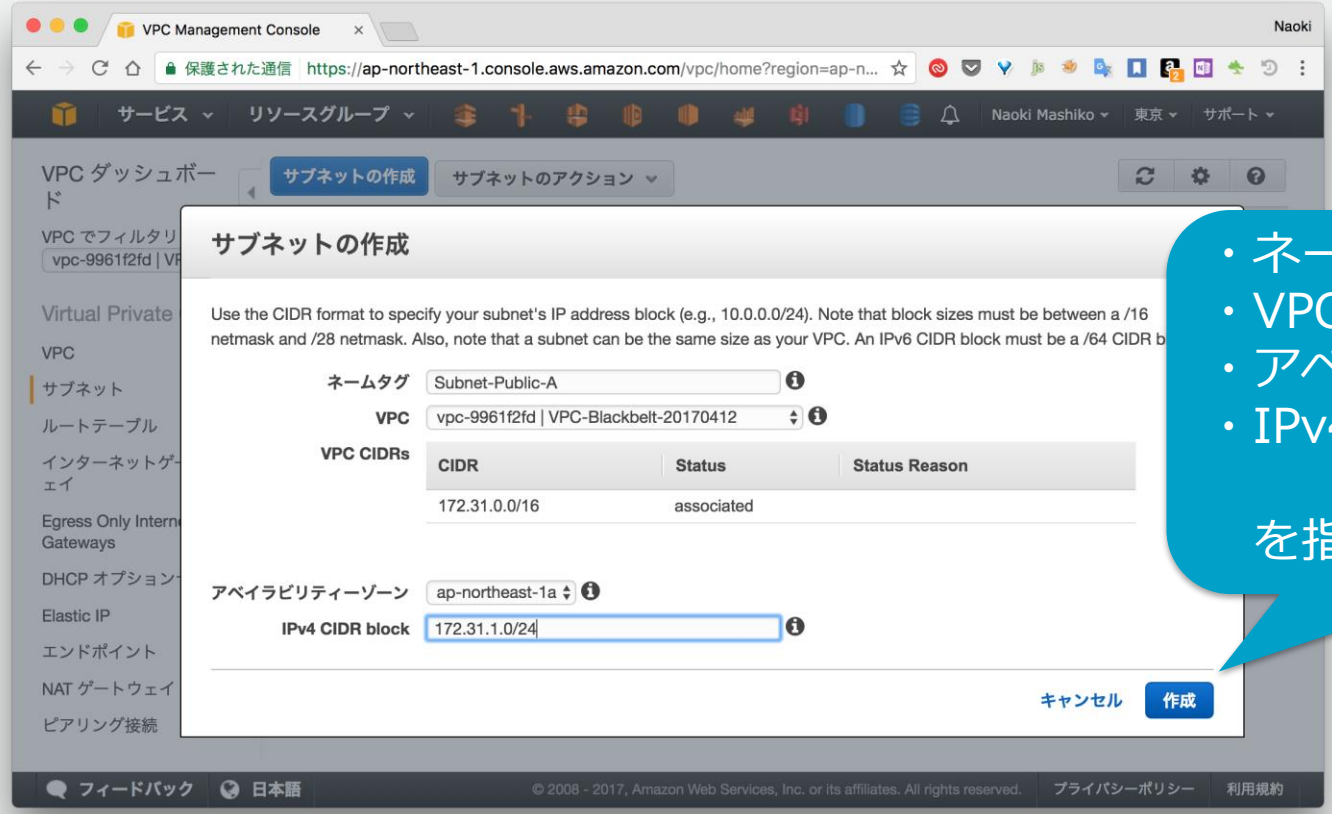
サブネットに対してAZとアドレスを選択



推奨：各AZにSubnetを設定

推奨：Subnetに/24設定（251個）

サブネットを作成



- 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(/24の例)

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

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

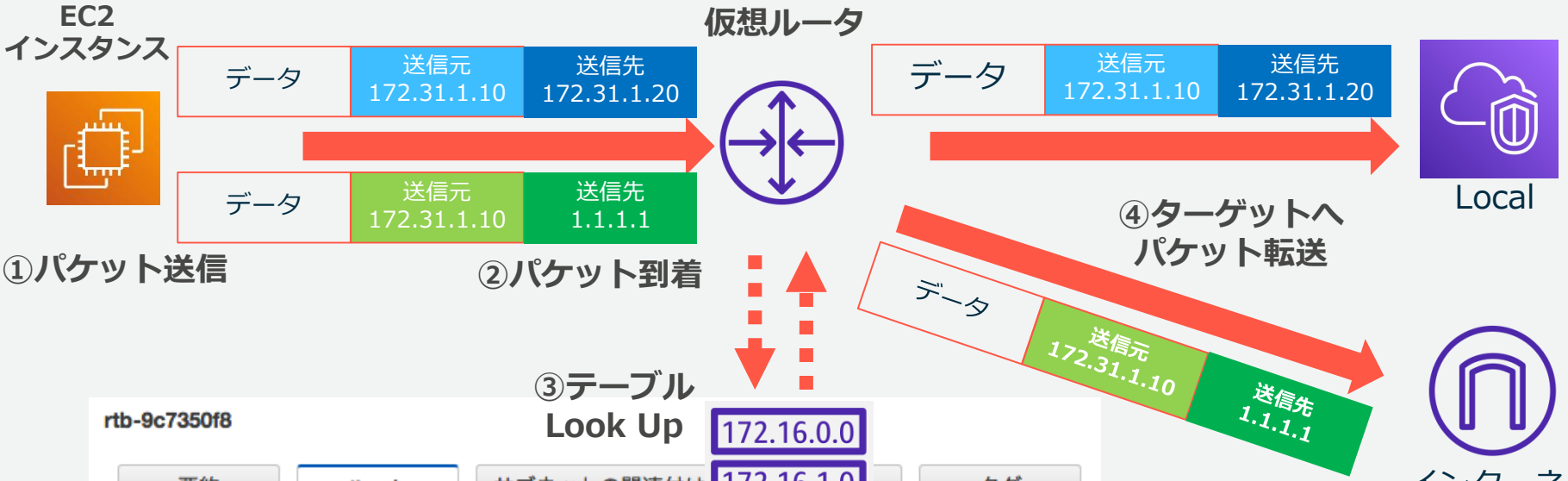
VPC内におけるルーティング

- 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

172.16.0.0
172.16.1.0
172.16.2.0

要約 | ルート | サブネットの関連付け | タグ

編集

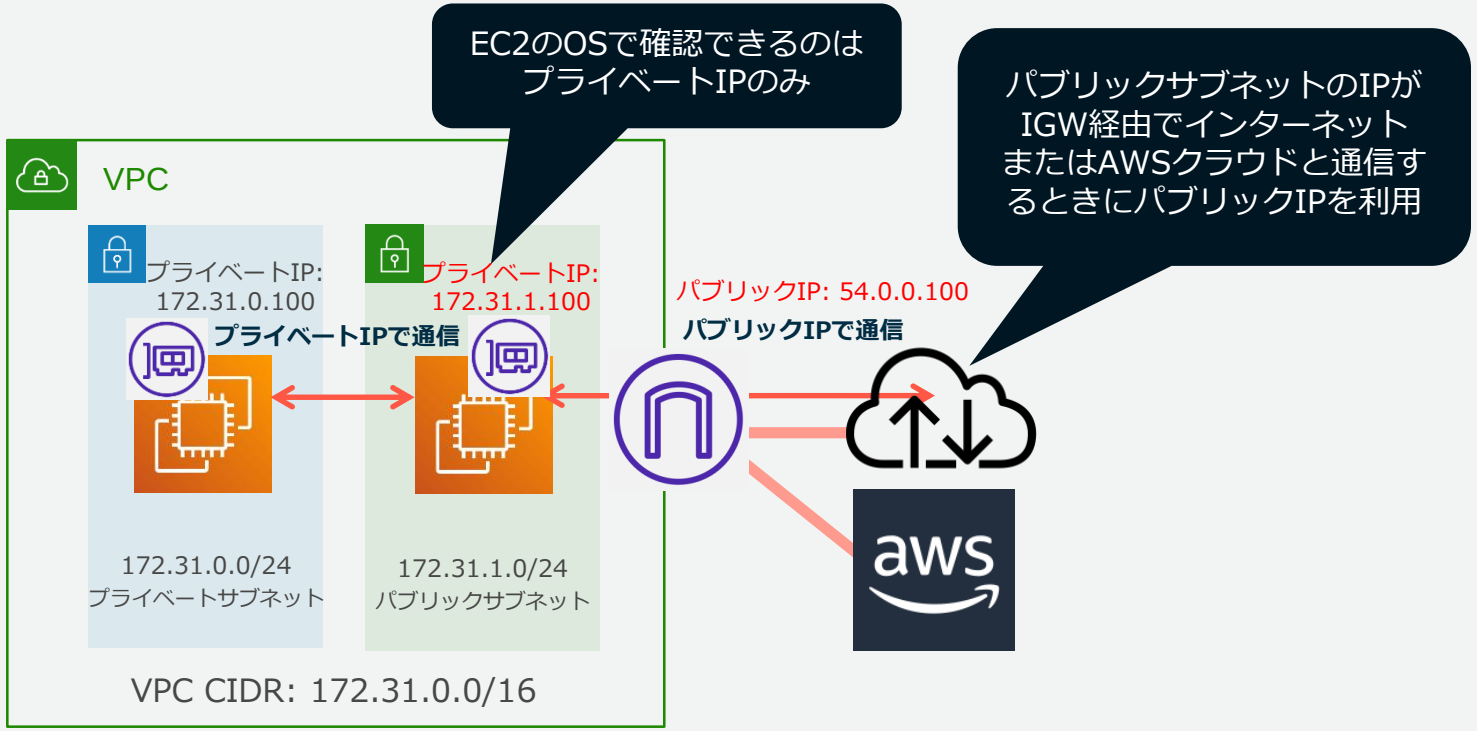
View: All rules

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

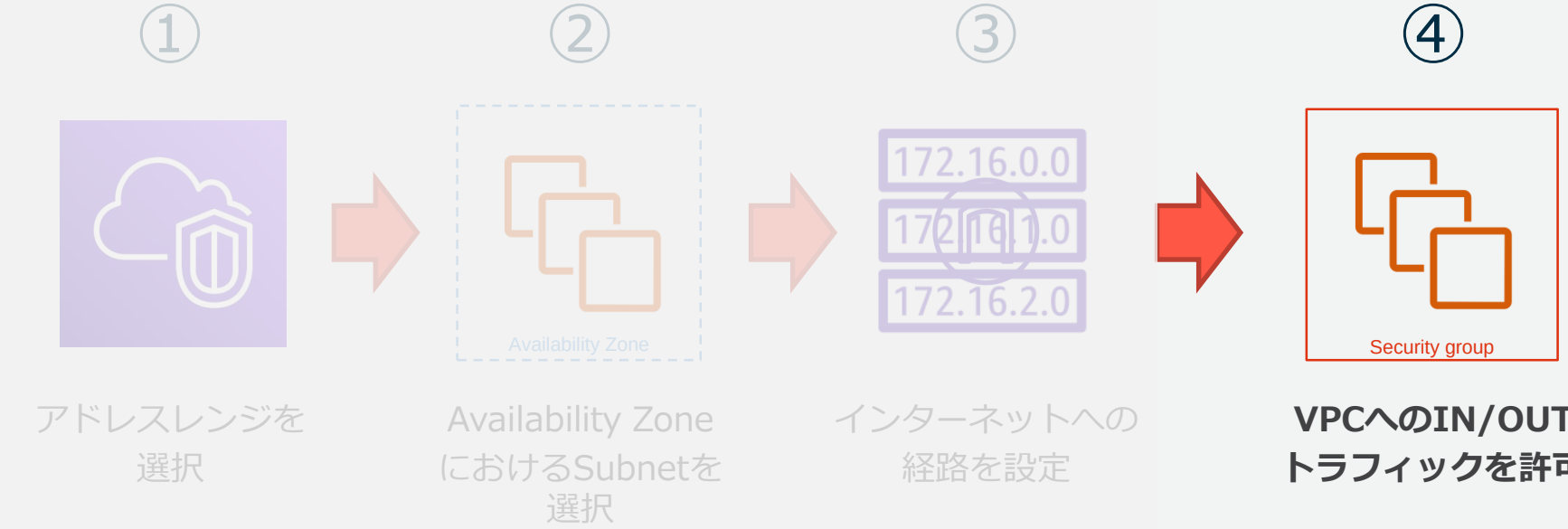
← 送信先172.31.1.20はこっち行けば良い

← 送信先 1.1.1.1 はこっち行けば良い

パブリックサブネットとプライベートサブネット



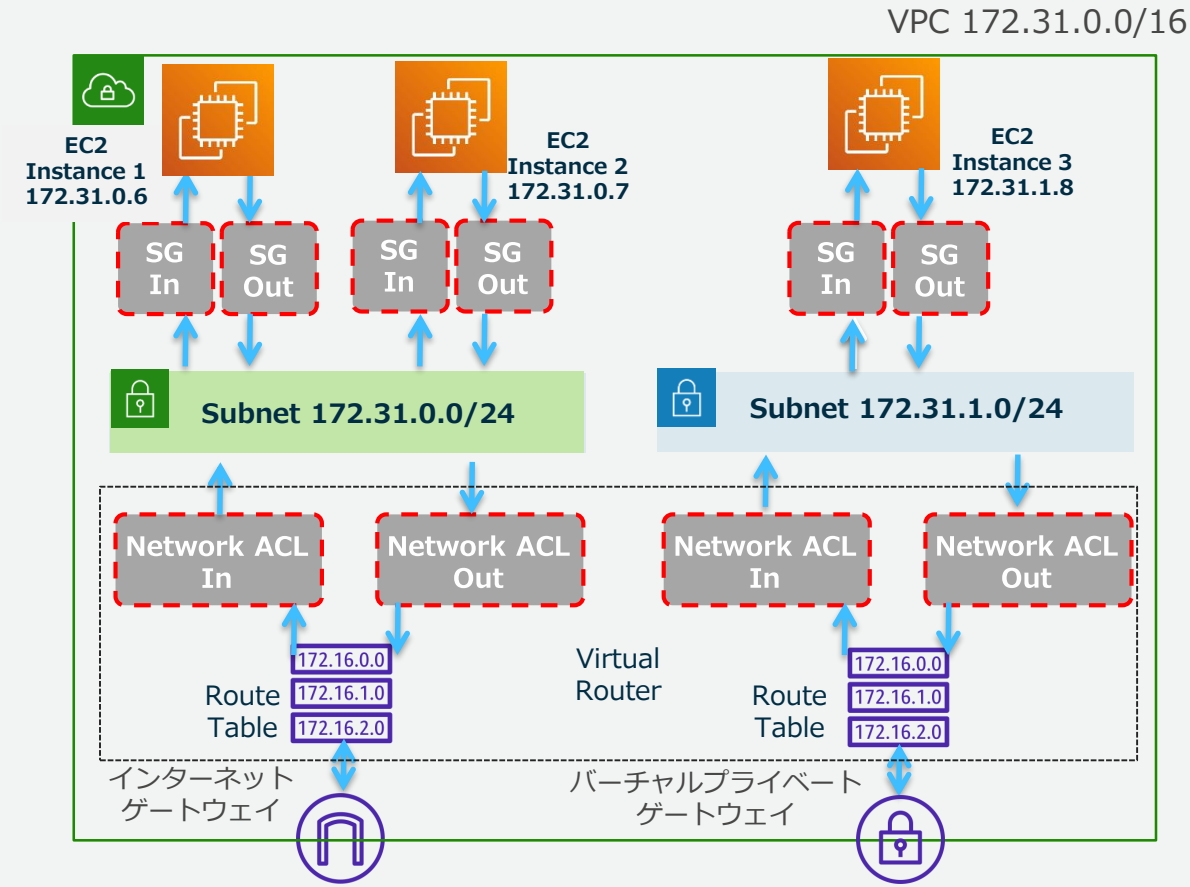
インターネット接続VPCのステップ



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



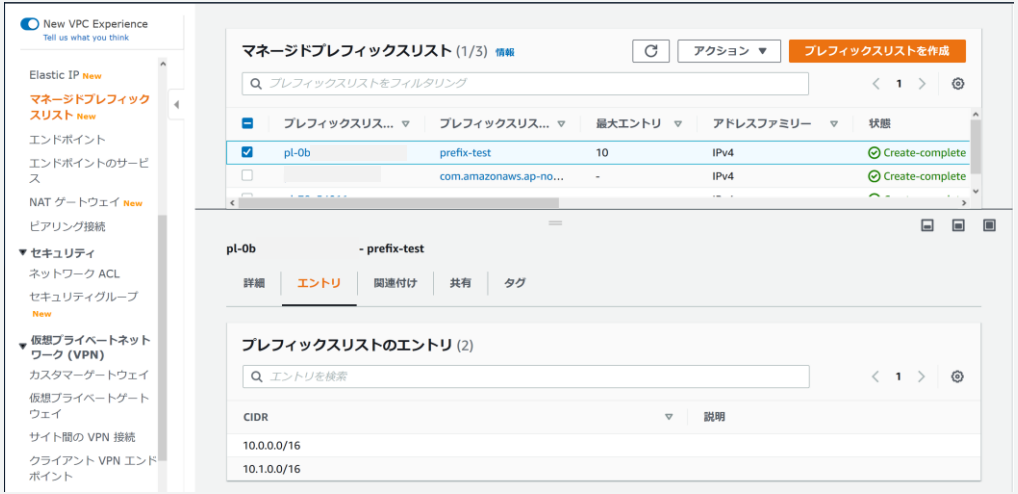
ネットワークACL vs セキュリティグループ

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

NEW

カスタマーマネージド プレフィックスリスト

カスタマーマネージドプレフィックスリスト



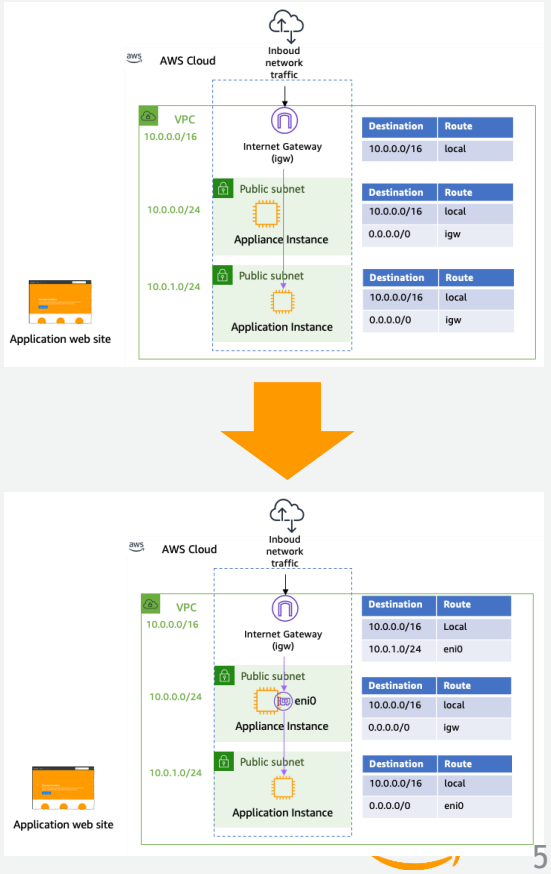
- お客様自身で複数のアドレスブロックをまとめてプレフィックスが設定可能に
- セキュリティグループ、サブネットおよびTransit Gatewayのルーティングテーブルで利用可能
- 作成したプレフィックスリストはRAMで他アカウントから参照可能

https://aws.amazon.com/jp/about-aws/whats-new/2020/06/amazon-virtual-private-cloud-customers-use-prefix-lists-simplify-configuration-security-groups-route-tables/

Ingress Routing

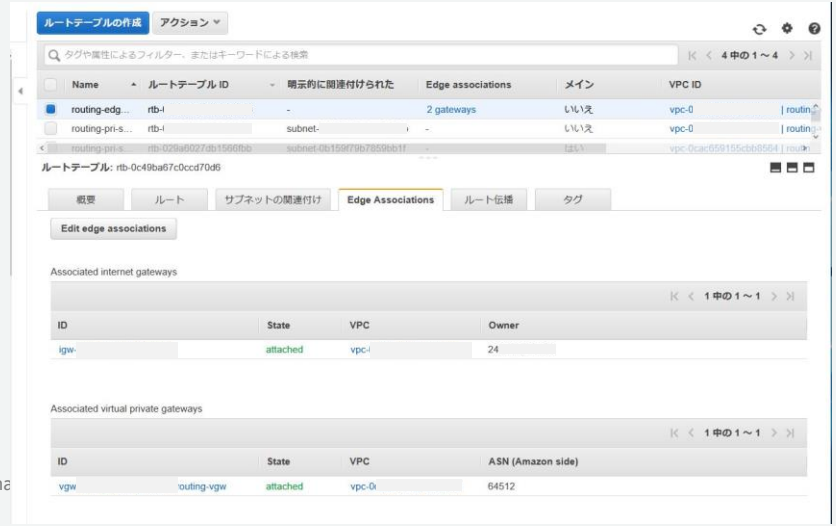
Ingress Routing

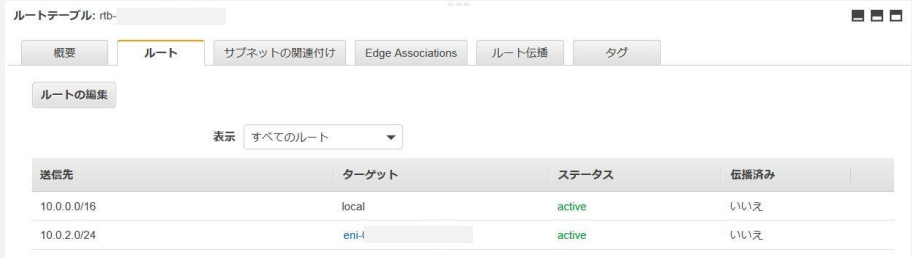
- Internet Gateway/VGWに対するアウトバウンド・インバウンド双方のトラフィックを特定EC2インスタンスのENIに向ける事ができる
- VPCに出入りする全トラフィックが特定EC2インスタンスを通過することを強制するため、IDS/IPSやFirewallによる監視・通信制御を効果的に実行可能
- Ingress Routingは全てのリージョンで利用可能



Ingress Routing 注意点

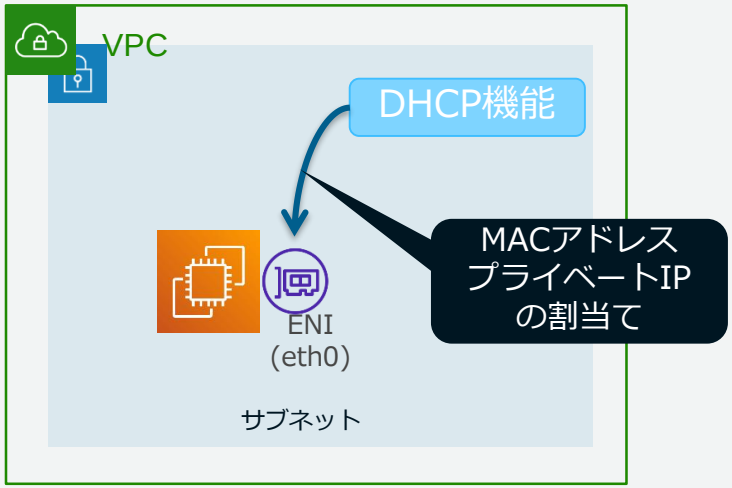
- IGW/VGW用のルーティングテーブルを作成し、それをIGW/VGWにアタッチする。
- サブネットに関連付けたルーティングテーブルやVPC作成時のルーティングテーブルはIngress Routingには紐付けできない。
- ENIをターゲットにするのでAZ/インスタンス障害時にlambdaなどでルーティングテーブルを切り替える仕組みが必要（TGWのインライン監査と同じ）
- 他のサブネットのIGW/VGW向けのルーティングは指定したENIに向けること（非対称になる）
- 指定できるCIDRはすでに作成されているサブネットと完全一致が必要





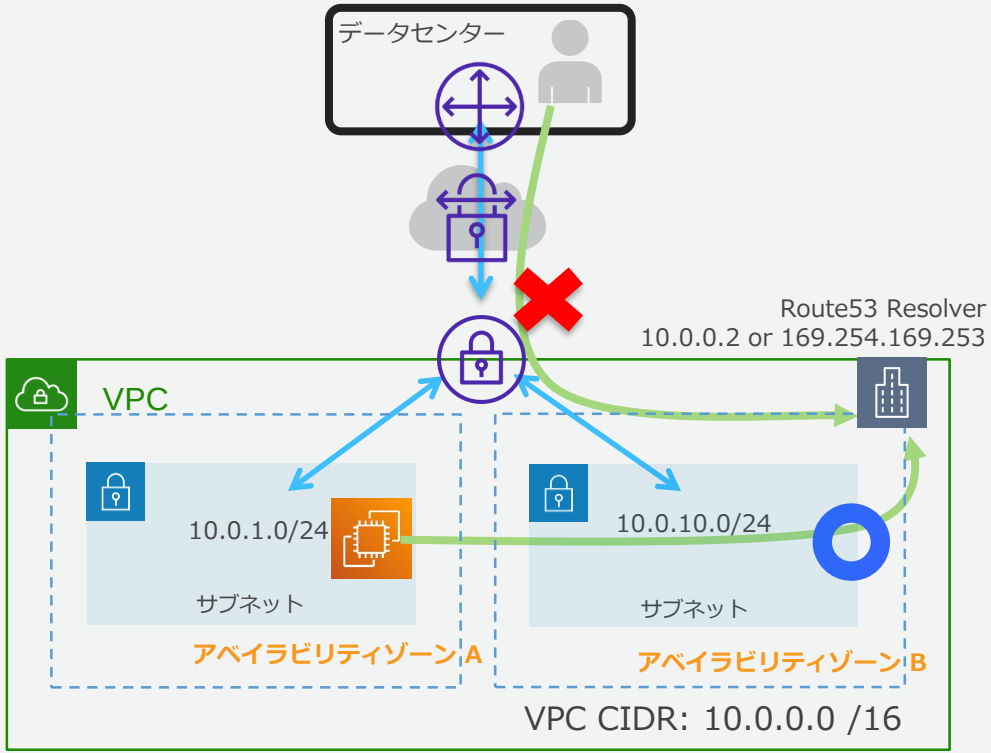
VPCセットアップの補足

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フェース)にIPを自動割当て
- プライベートIPを固定にした場合はDHCP経由で該当のIPが割当てられる
  （EC2インスタンスのOS上のNIC設定はDHCP設定とする)
- EC2インスタンスを再起動しても、割り当てられた固定IPは変わらない。

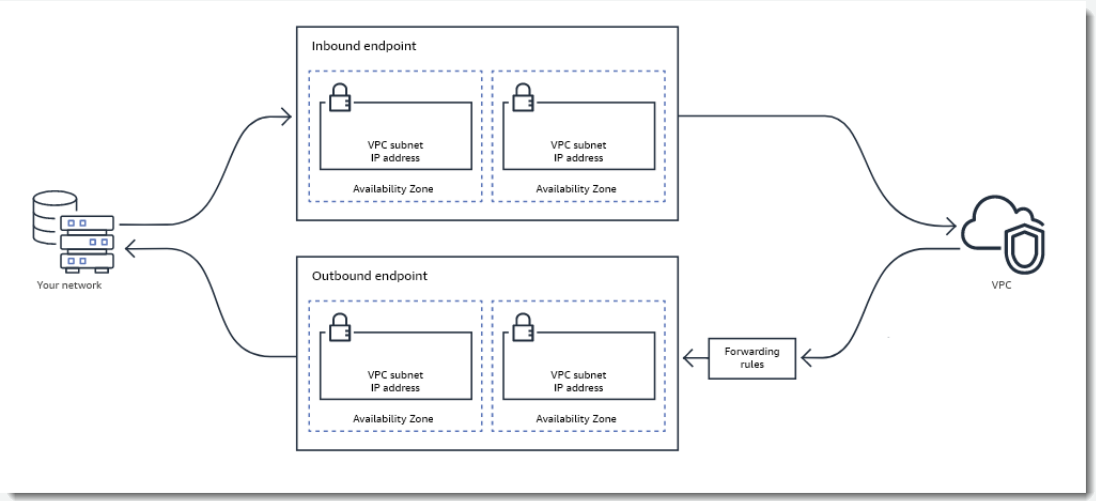
Route53 resolver(AmazonProvidedDNS)



- 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）
  - **Route 53 Resolver for Hybridsで解決**

http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#AmazonDNS

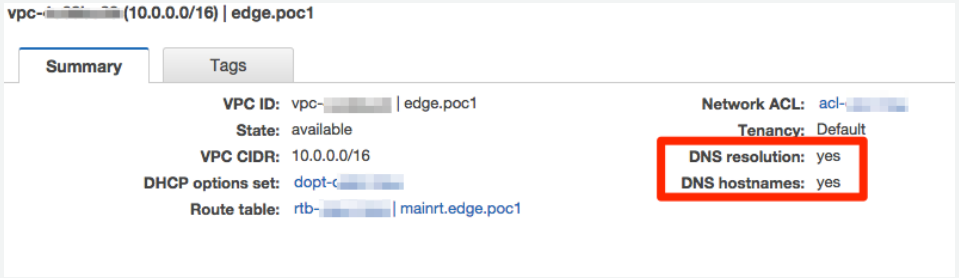
Route 53 Resolver for Hybrid Clouds

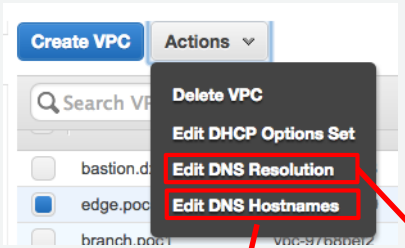


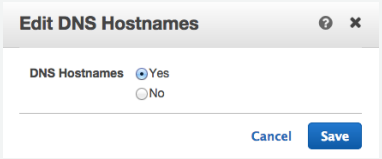
https://aws.amazon.com/jp/blogs/aws/new-amazon-route-53-resolver-for-hybrid-clouds/

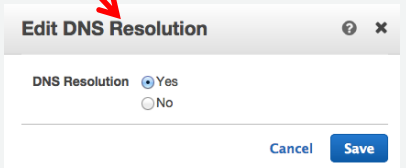
- オンプレミスからDirect Connect/VPN経由によるVPC Provided DNSへの直接アクセス可能なDNSエンドポイントを提供
- 逆方向（VPC内からオンプレミスへの特定ドメイン参照）も可能
- 複数AZに跨ったエンドポイント設定による冗長

DNS機能の有効化とホストへのDNS名割当て









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

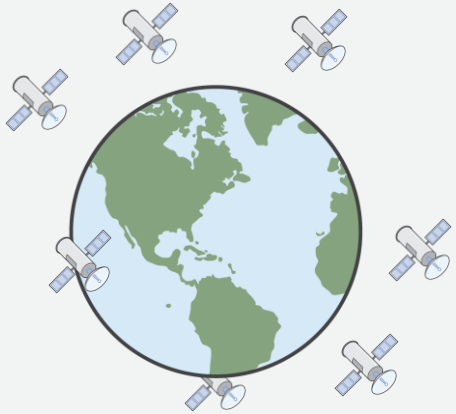
Enable DNS hostname

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

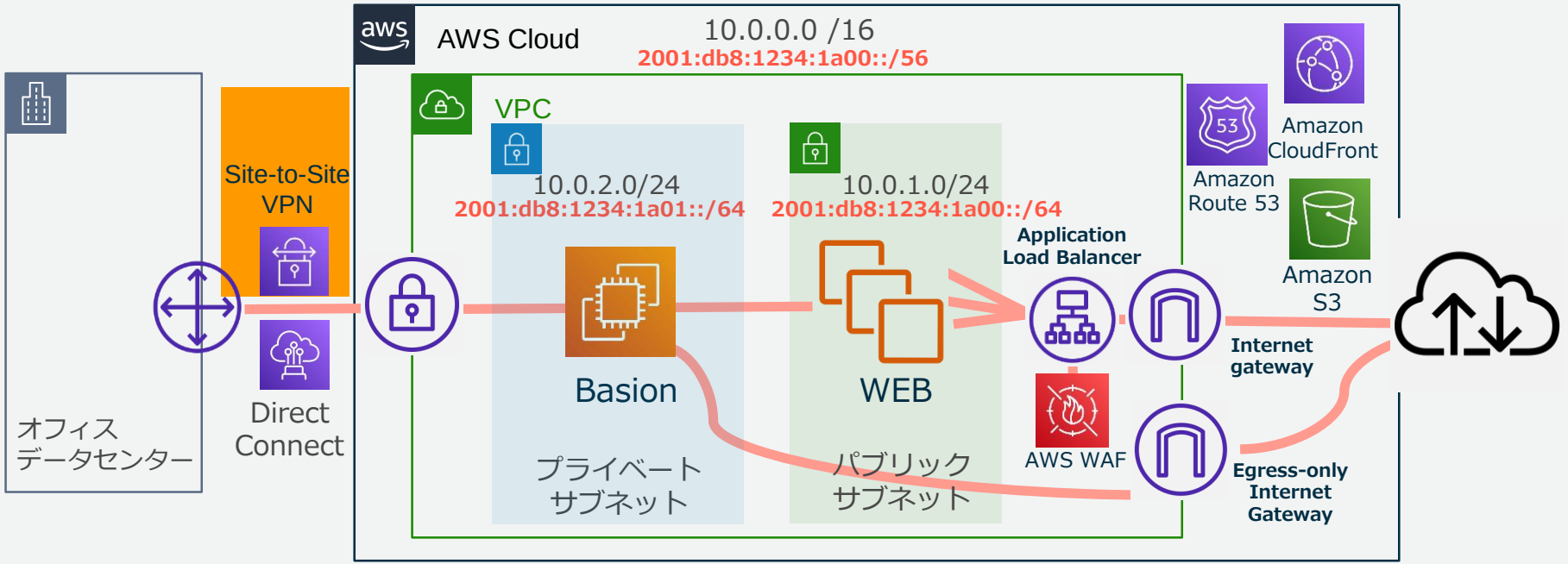
Amazon Time Sync Service

- VPC内で稼働する全てのインスタンスからNTPで利用できる高精度な時刻同期サービス
- EC2インスタンス内でNTPサーバのIPアドレスとしてとして169.254.169.123を設定するだけで利用できる
  - このアドレスはリンクローカルアドレスなので、外部インターネットへのアクセスは不要。プライベートサブネット内でも利用できる
- Leap Smearingによる「うるう秒」への対策が実装済み
- 無料で全リージョンで利用可能



IPv6の対応

Site-to-Site VPNでIPv6対応開始



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

https://aws.amazon.com/jp/blogs/news/new-ipv6-support-for-ec2-instances-in-virtual-private-clouds/

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）
インスタンスタイプ	全てのインスタンスタイプ	M3、G2を除く全ての現行世代の インスタンスタイプでサポート
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、Direct Connect	VPN、Direct Connect

http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html

Agenda

Amazon VPCとは？
VPCのコンポーネント
VPCのセキュリティ
オンプレミスとのハイブリッド構成
VPCの設計
VPCの設定
VPCの運用
まとめ

VPCとのプライベートネットワーク接続

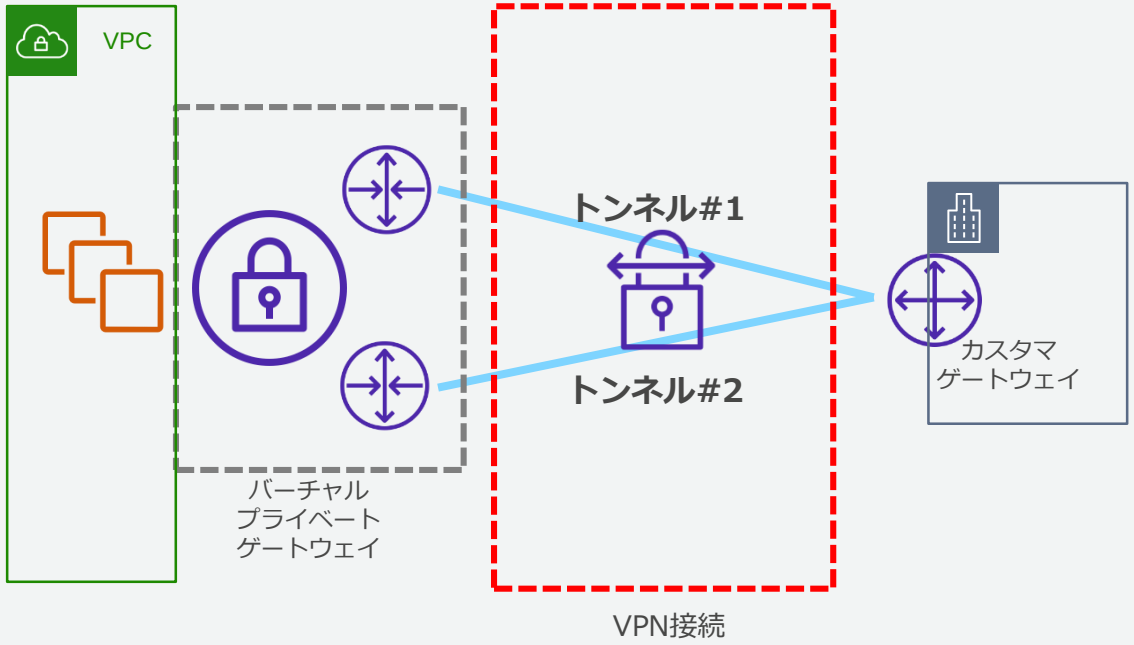
VPN接続

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
エンドポイントを利用したClient VPN

専用線接続

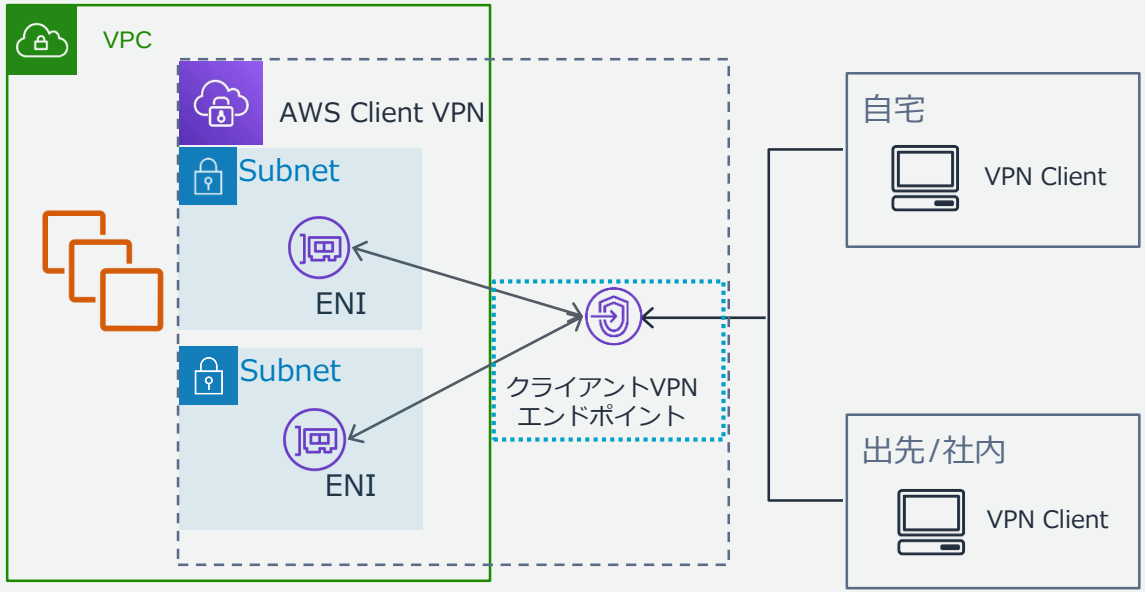
AWS Direct Connectを利用し、一貫性のあるネットワーク接続を実現
本番サービス向け

Site-to-Site VPN接続構成



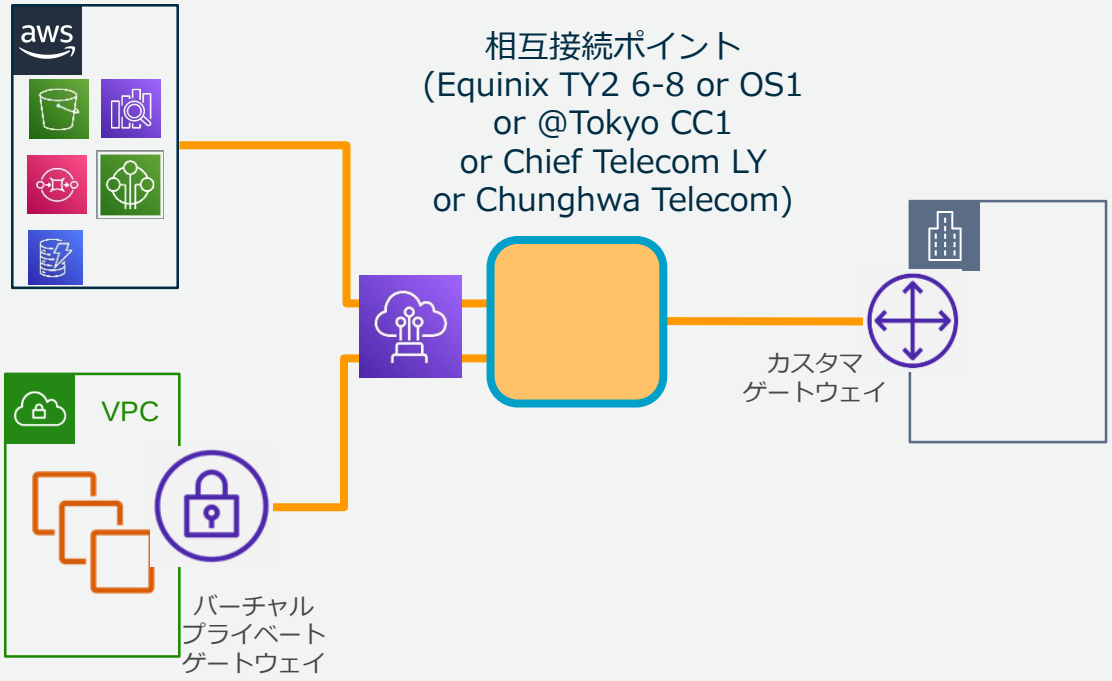
・1つのVPN接続は2つのIPsec
トンネルで冗長化
・ルーティングは
静的(スタティック)
動的(ダイナミック:BGP)
が選択可能

Client VPN接続構成



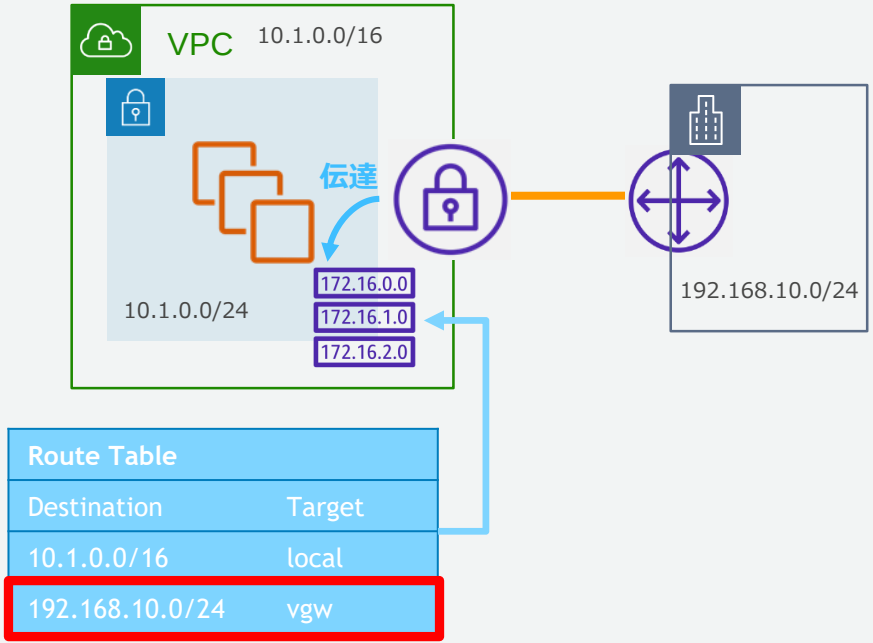
- OpenVPNベースでのクライアントVPN接続を提供するマネージドサービス
- どこからでもAWS・オンプレミス上リソースへの安全なアクセスを提供
- AWS上に配置されたClient VPNのエンドポイントを経由し、オンプレミス内のシステムへ接続可能

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
- 東京リージョンの相互接続ポイントは
  - 東京(Equinix TY2 6-8,@Tokyo CC1)
  - 大阪(Equinix OS1)
  - 台北(Chief Telecom LY, Chunghwa Telecom)
- ルーティングはBGPのみ
- 接続先は以下の3つ
  - VPC(プライベート接続)
  - AWSクラウド(パブリック接続)
  - Transit Gateway(トランジット接続)
- 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)

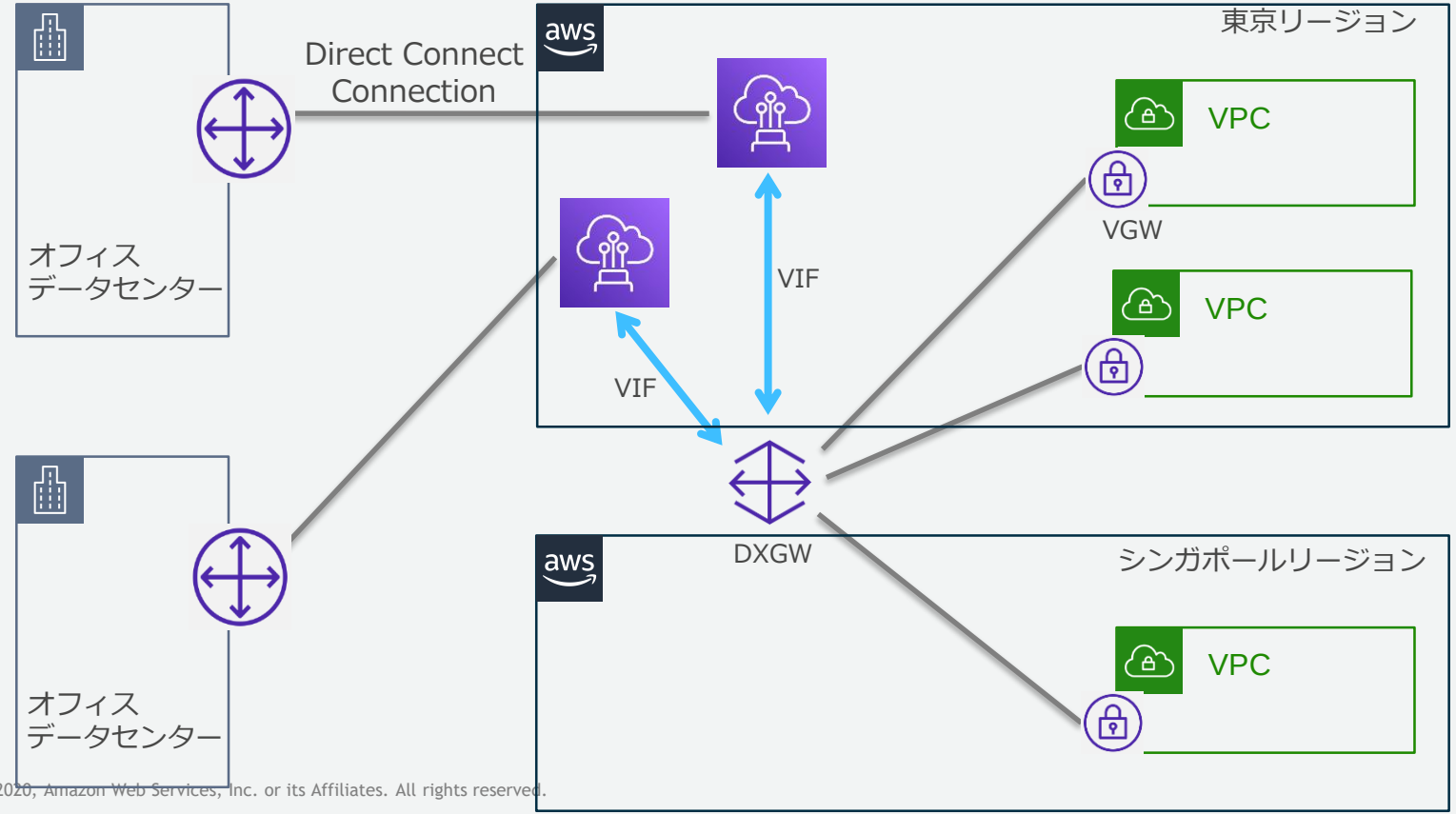
Direct Connect Gateway

- 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

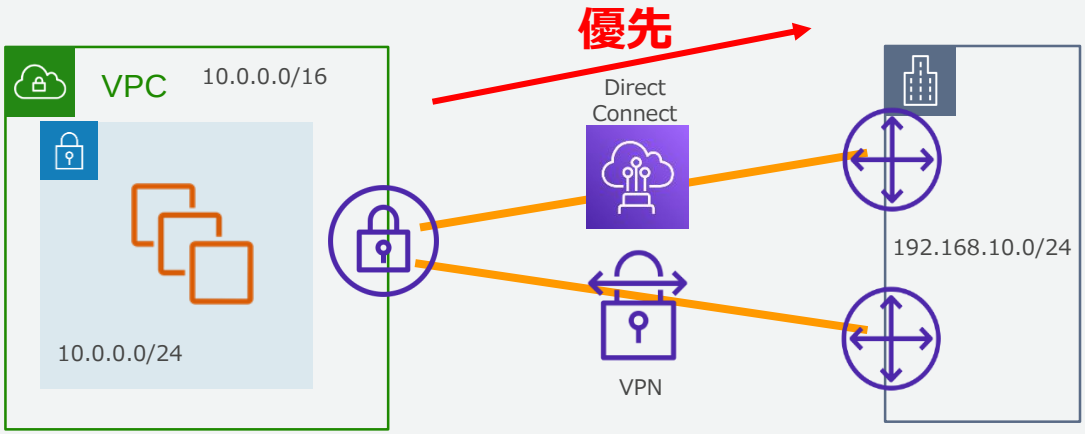
Direct Connect Gatewayの接続例



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	ポート当たり1G/10Gbps/LAG可能
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

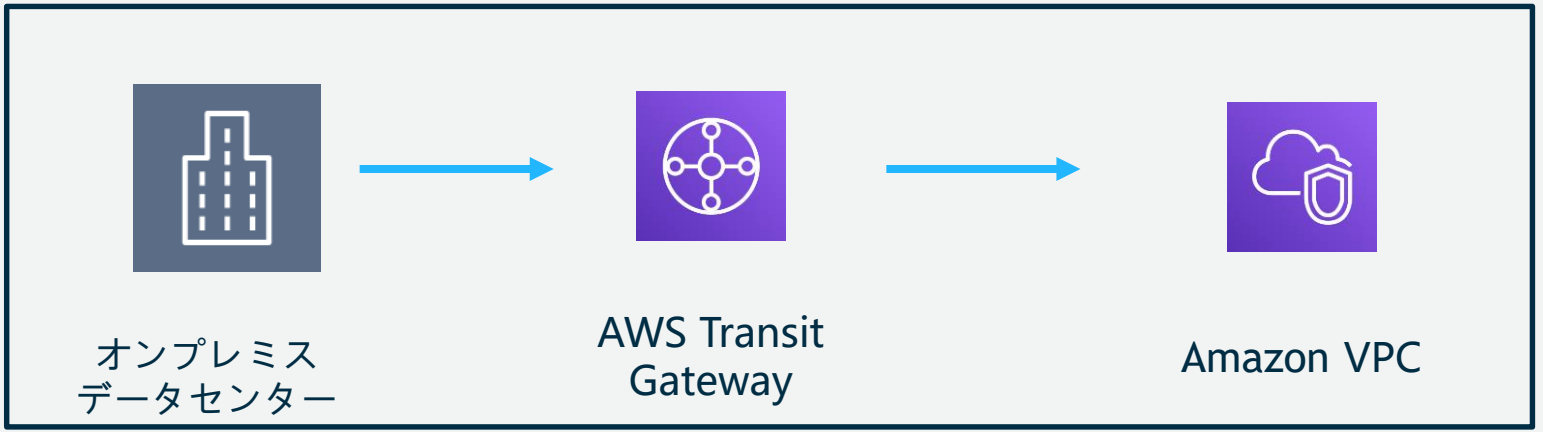
VPNとDirect Connectの冗長化



- 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ルータから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

AWS Transit Gateway

1000以上のVPCとオンプレミス間の相互接続を簡単に

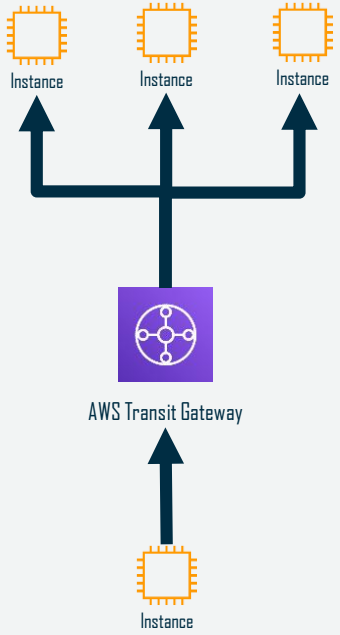


Transit GatewayのMulticast対応

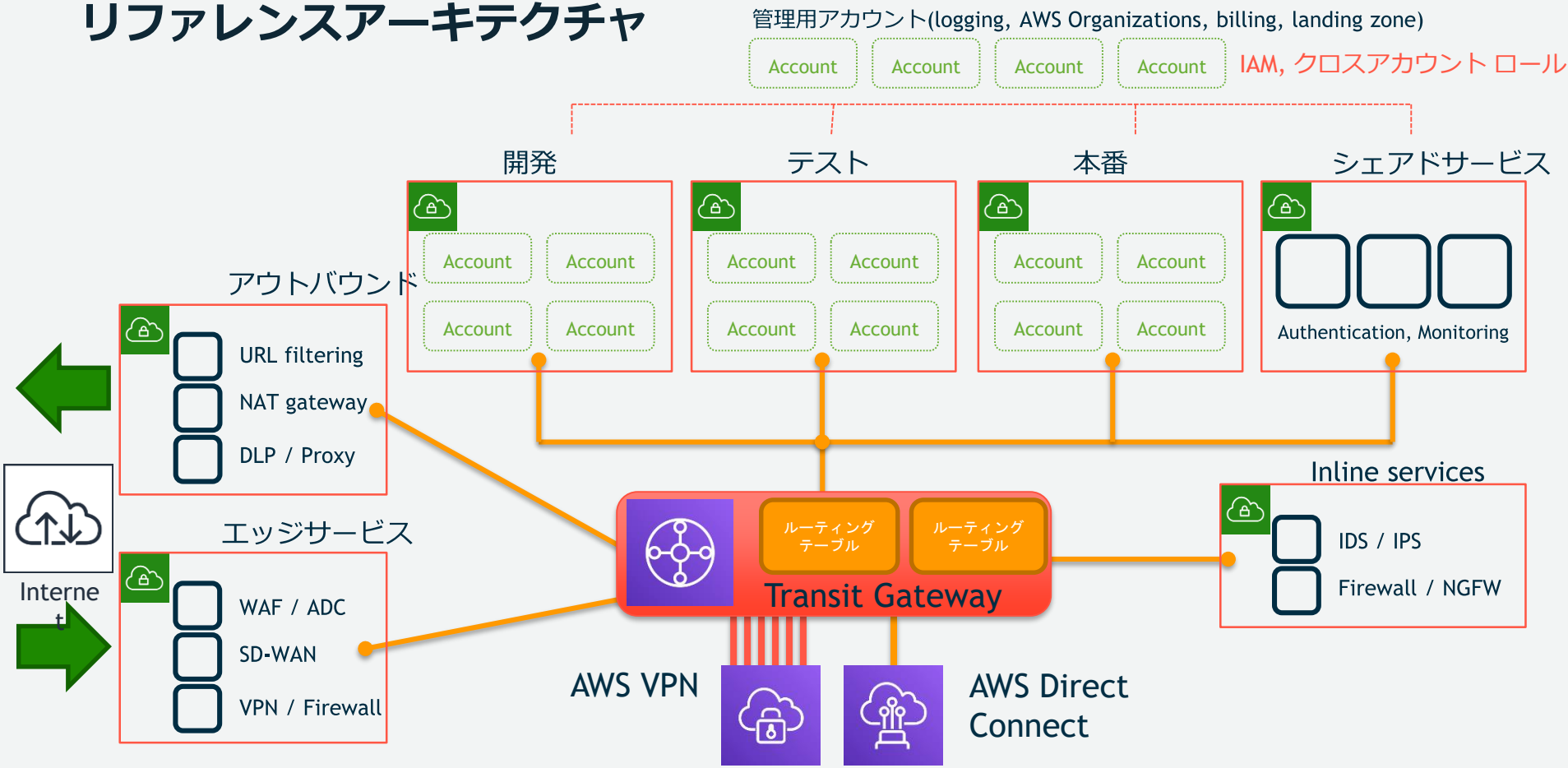
NEW

Multicast

- AWS Transit Gatewayの機能として、データストリームを仮想的に複数のアプリケーションに配信することが可能に
- 株価配信やマルチメディアコンテンツ配信など、データを購読者にストリームする際に最適
- バージニア、フランクフルト、サンパウロ、バーレーン、香港、ソウルリージョンで利用可能



リファレンスアーキテクチャ



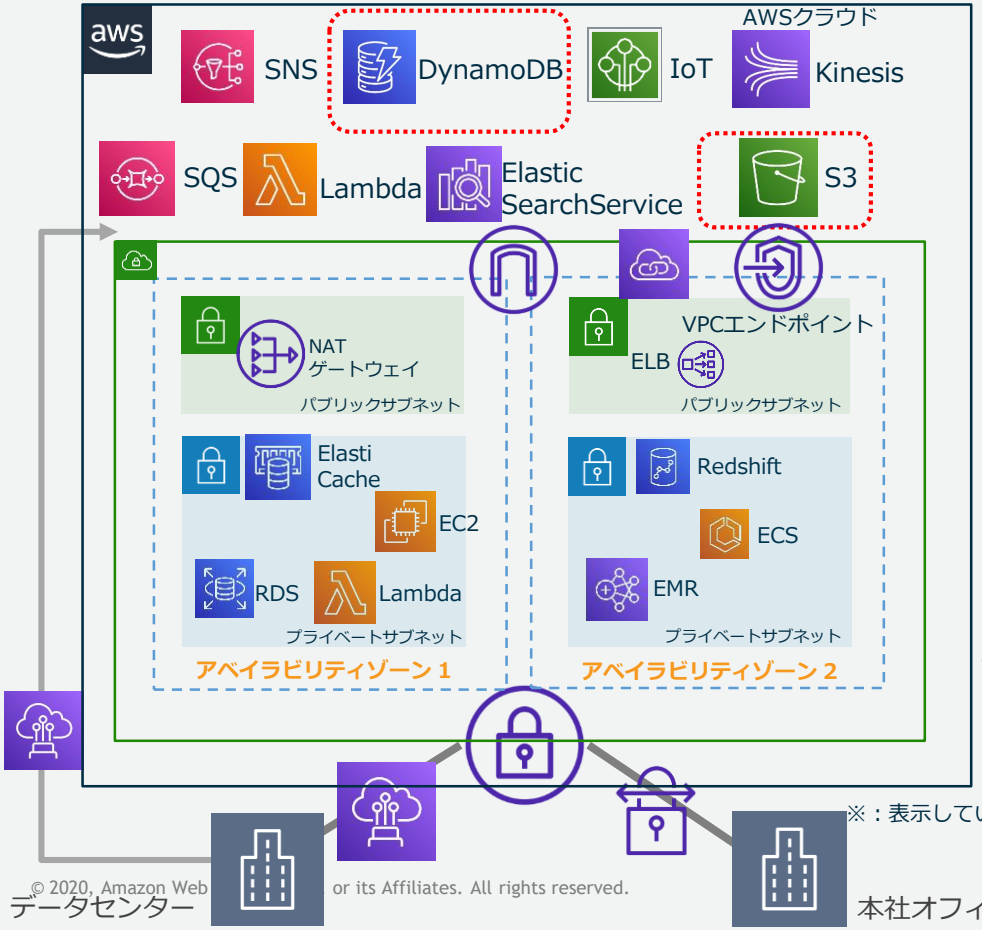
Agenda

Amazon VPCとは？
VPCのコンポーネント
VPCのセキュリティ
オンプレミスとのハイブリッド構成
VPCの設計
VPCの設定
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
  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

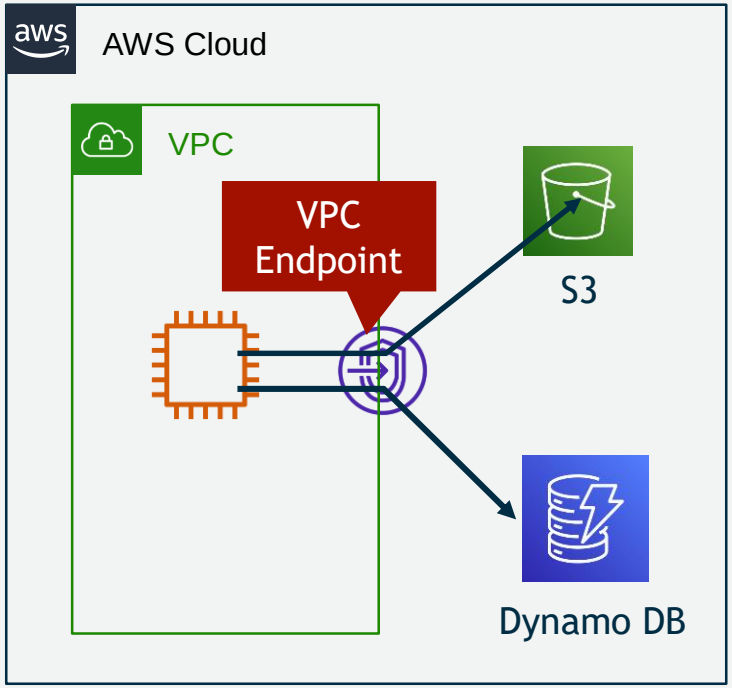
AWSクラウドとVPC



- 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,DynamoDBへのアクセスはVPCエンドポイント(Gateway型)が利用可能

※：表示しているサービスは一部のみです。

VPC Endpoint概要

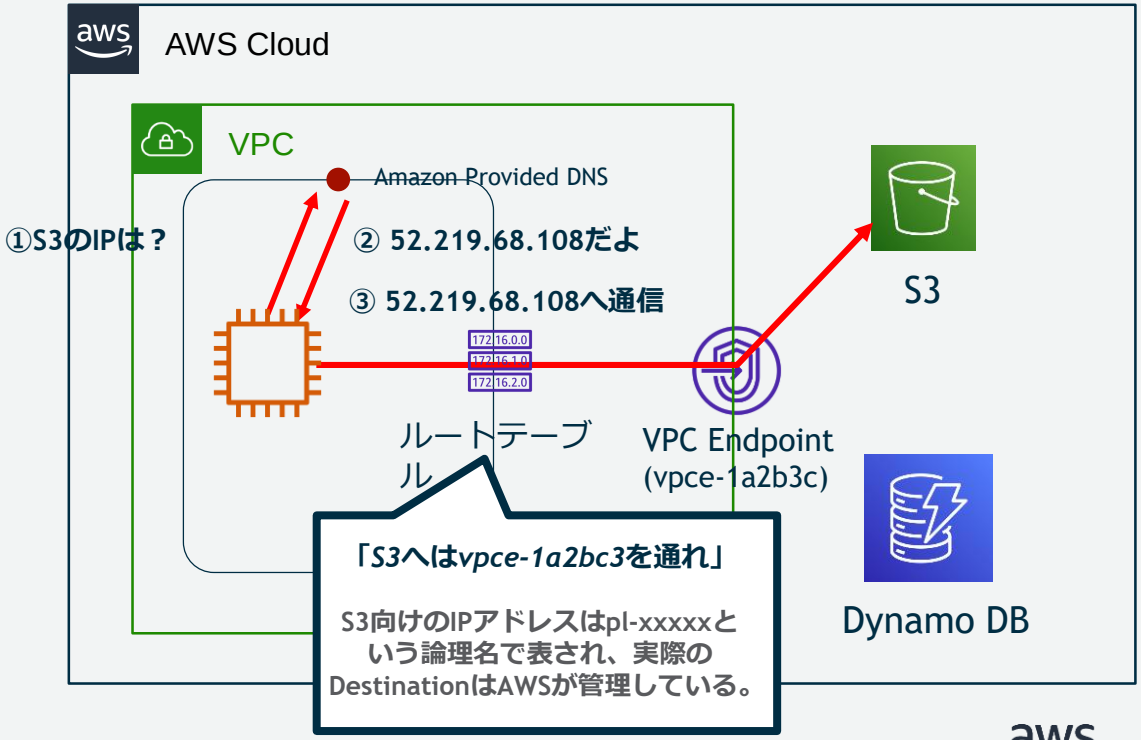


VPC Endpointは、グローバルIPをもつAWSのサービスに対して、VPC内部から直接アクセスするための出口

動作比較

Gateway型の動作

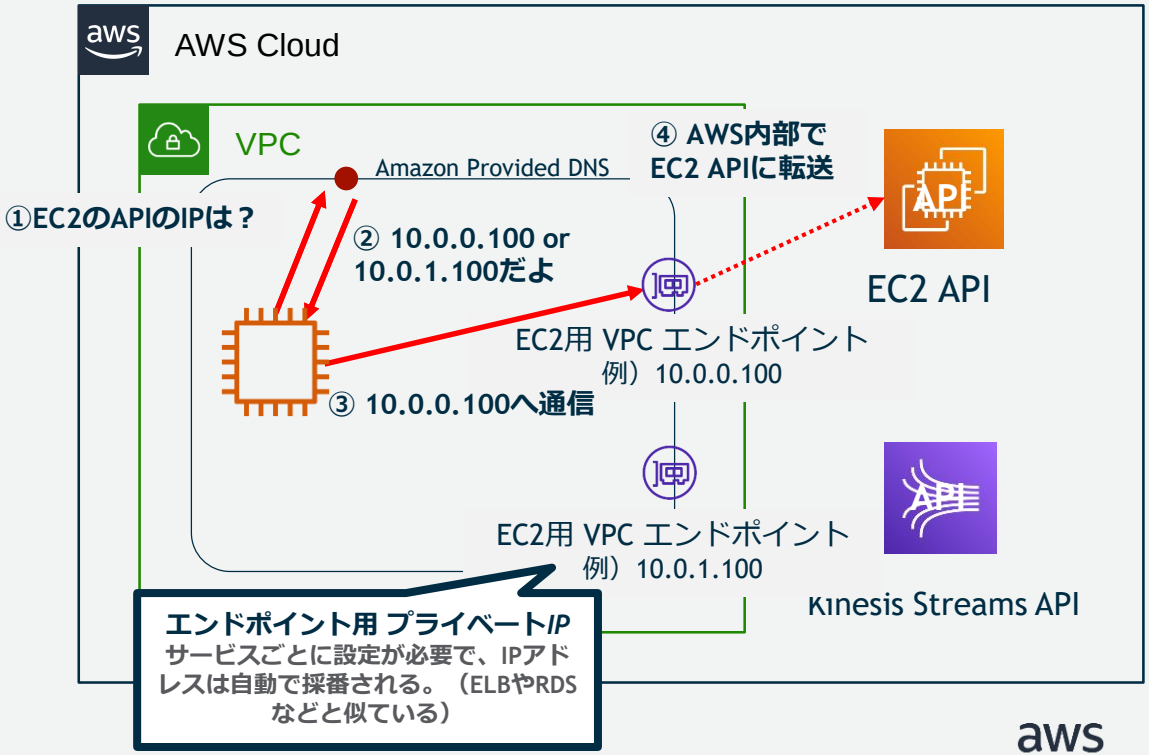
- サブネットに特殊なルーティングを設定し、VPC内部から直接サービスと通信する。
- 通信先のIPアドレスはグローバルIPアドレス



動作比較

PrivateLink (Interface型)の動作

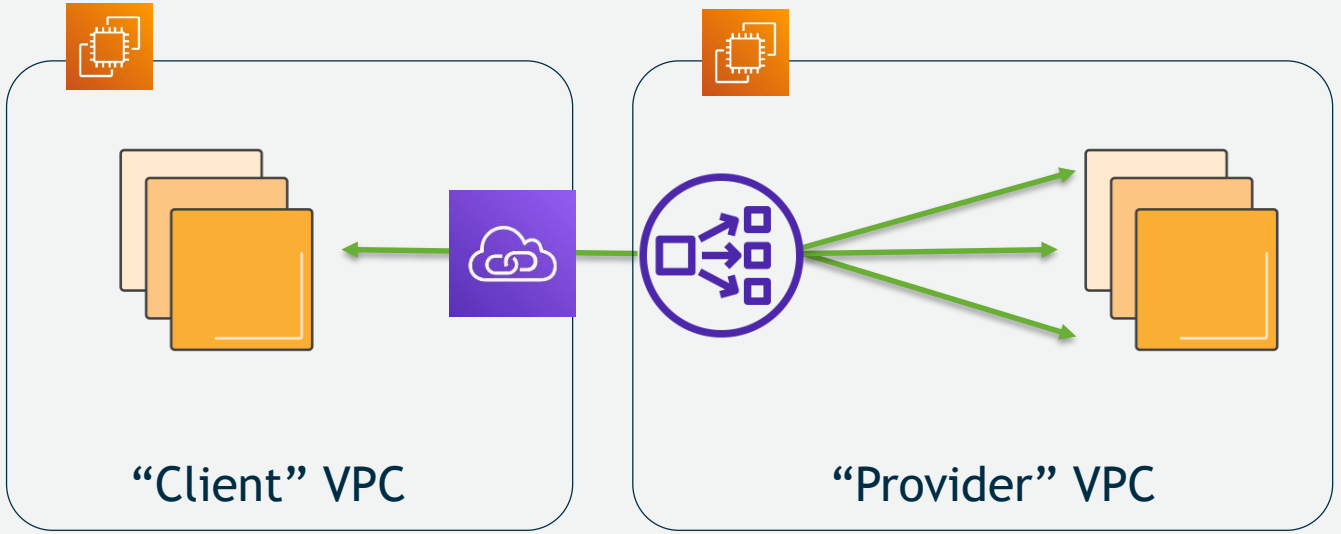
- サブネットにエンドポイント用のプライベートIPアドレスが生成される。
- VPC内部のDNSがエンドポイント向けの名前解決に対してしてプライベートIPアドレスで回答する。
- エンドポイント用プライベートIPアドレス向け通信が内部的にサービスに届けられる。



機能比較

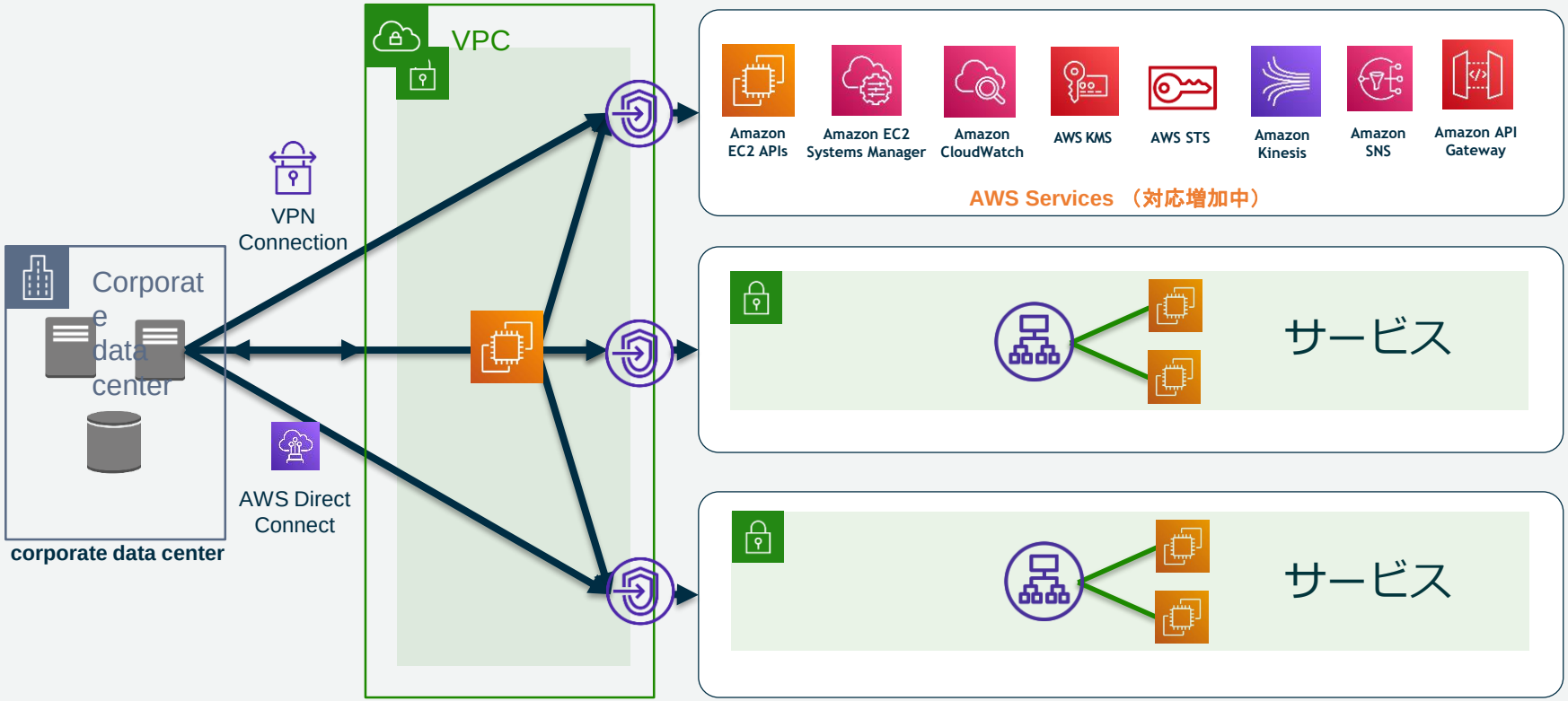
	Gateway型	PrivateLink(Interface型)
アクセス制御	エンドポイントポリシー IAM Policyと同じ構文でアクセス先のリソースを制限可能。	**セキュリティグループ** セキュリティグループでアクセス元IP、ポートを制御可能。対象のサービスの特定のリソースへのアクセス制御は不可。
利用料金	無料	有料 サービスごとに、1プライベートIP毎に下記の料金。 0.014 USD/時間（東京）+ 0.01 USD/ GB https://aws.amazon.com/jp/vpc/pricing/
冗長性	ユーザー側で意識する必要なし	マルチAZ設計 マルチAZで配置するように設定する。

PrivateLink for Customers and Partners

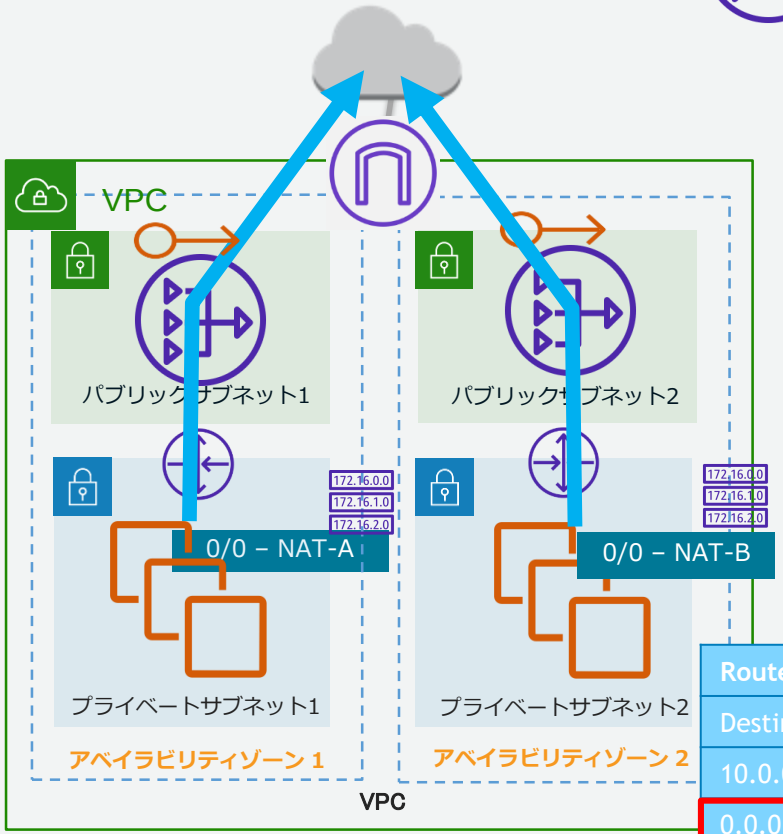


PrivateLinkはユーザが自分で作ることもできる

PrivateLinkはオンプレミスにネイティブ対応



NATゲートウェイ

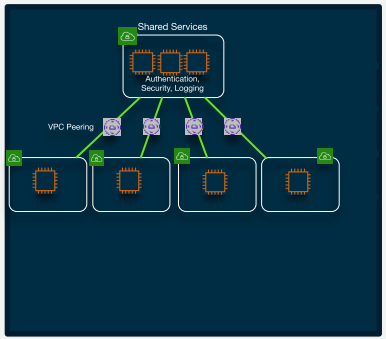


Route Table	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NATゲートウェイ

- 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を割当て
- 高パフォーマンス(45Gbpsまで自動的に拡張)
- 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

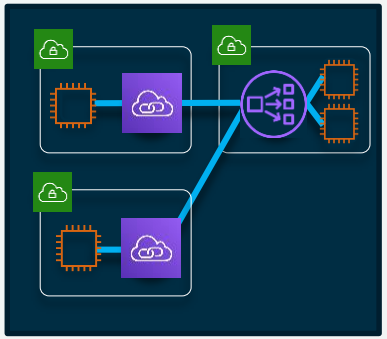
VPCの接続バリエーション

VPC peering



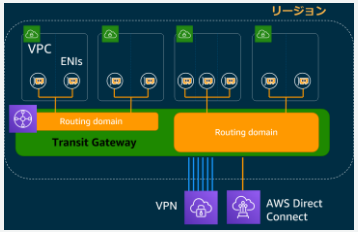
1 vs 1 の関係
100 VPCまで
VPC間のSecurity groups
Inter-region対応

AWS PrivateLink



- 1 vs Nの関係
- スケーラブル
- IPアドレス重複でもOK
- NLBとエンドポイント費用
- Inter-region対応

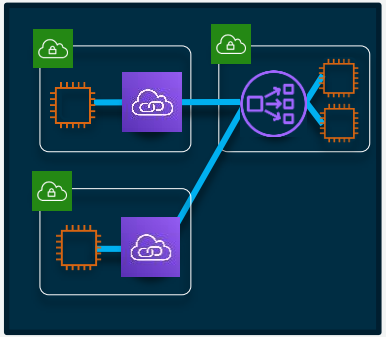
AWS Transit Gateway



- 1vs1でも1vsNでもroute table次第
- スケーラブル
- AZごとのエンドポイント費用
- Inter-region対応

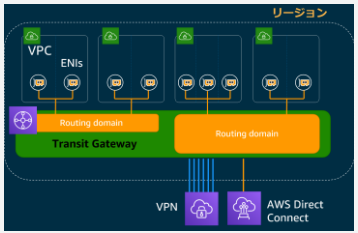
Transit Gateway と PrivateLinkはスケーラブル

AWS PrivateLink



- 1 vs Nの関係
- スケーラブル
- IPアドレス重複でもOK
- NLBとエンドポイント費用

AWS Transit Gateway



- 1vs1でも1vsNでもroute table次第
- スケーラブル
- AZごとのエンドポイント費用

Scope: アプリケーションの共用

Trust model: 相互信頼不要

Dependencies: NLB

Scale: 数千のVPCに対応

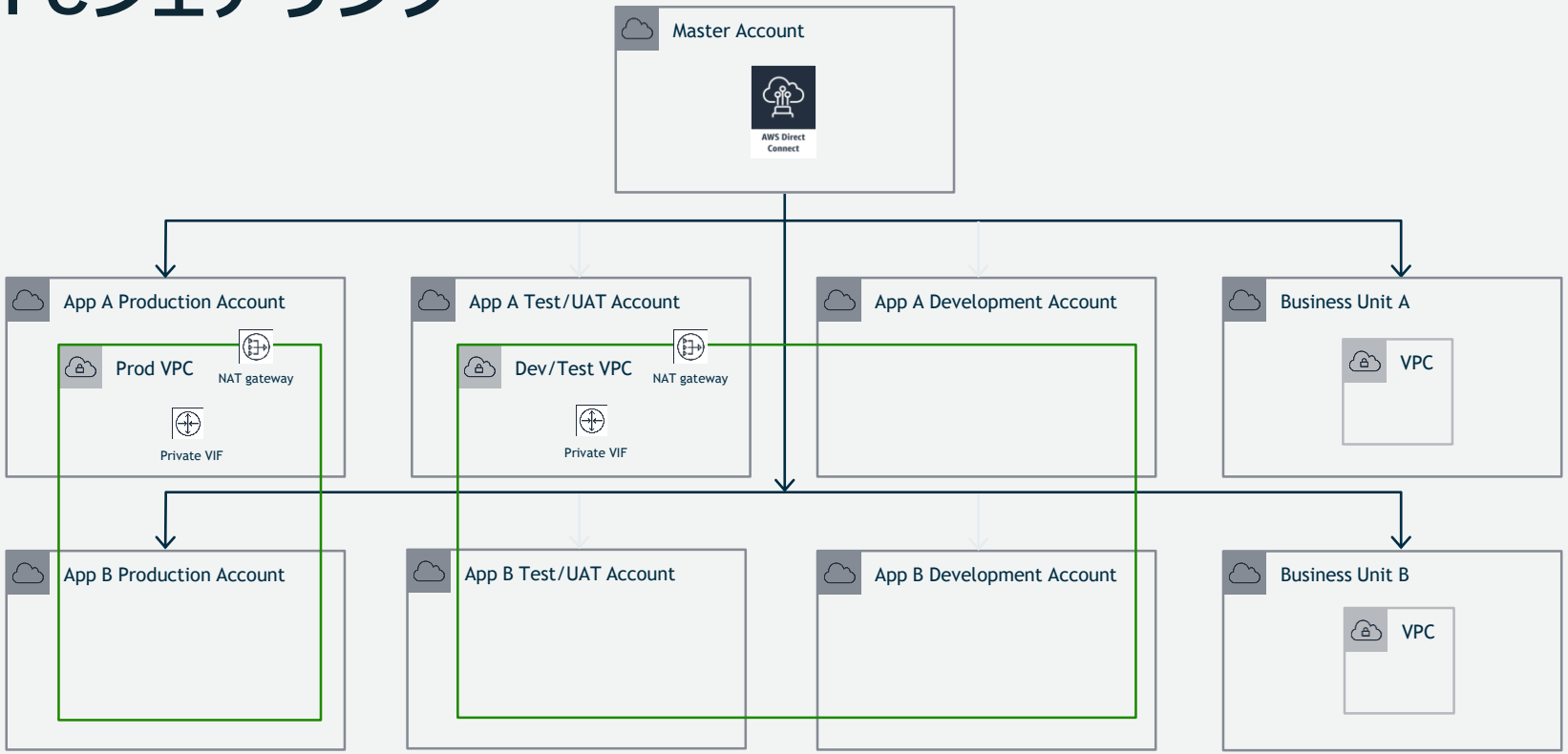
Scope: ネットワークの共用

Trust model: VPC間の信頼を集中管理

Dependencies: Transit Gateway

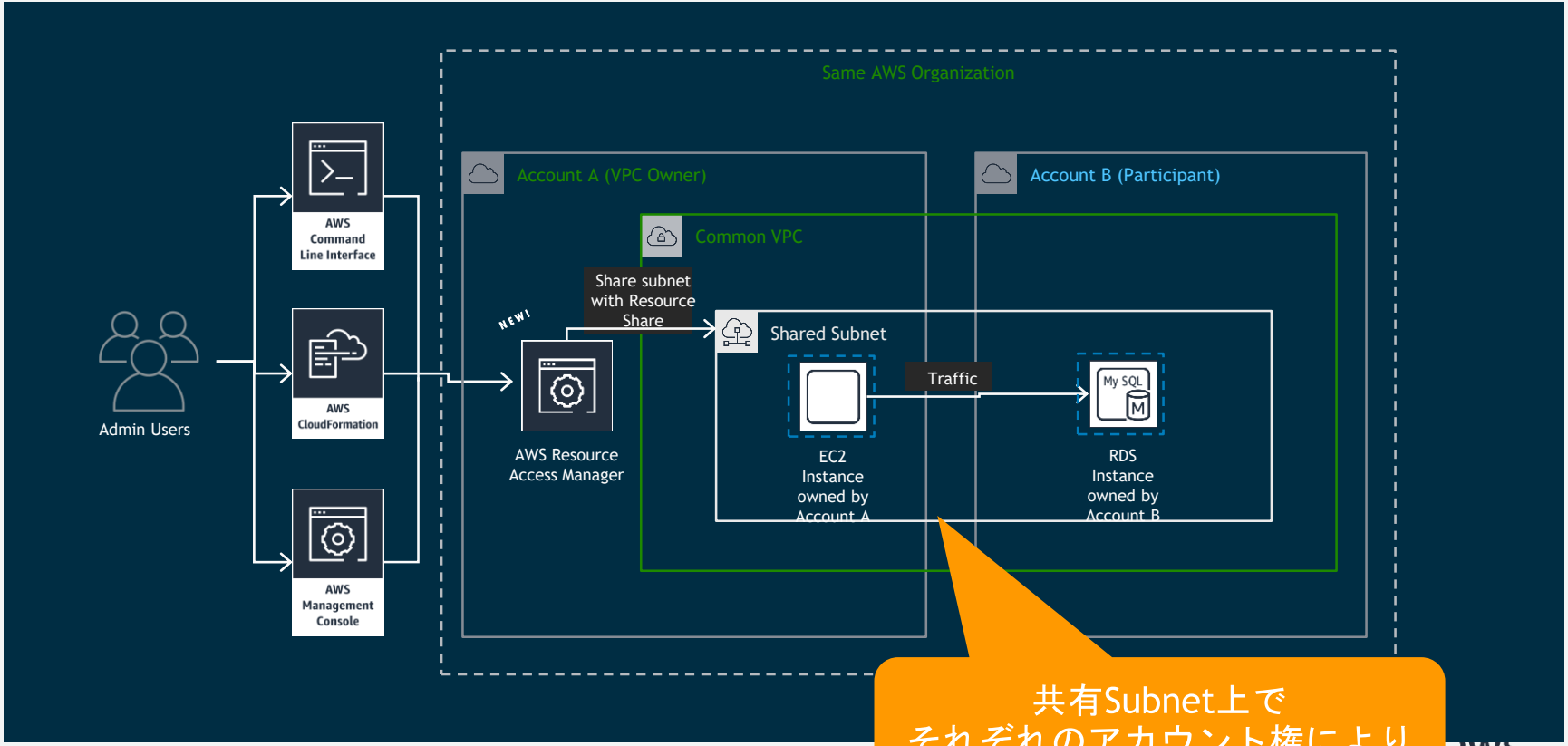
Scale: 数千のVPCに対応

VPCシェアリング



アカウントをまたいだVPCシェアリングにより VPC数を削減

実際の動作



Agenda

Amazon VPCとは？
VPCのコンポーネント
VPCのセキュリティ
オンプレミスとのハイブリッド構成
VPCの設計
VPCの設定
VPCの運用
まとめ

VPCの設定方法

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 VPCConnection
c = VPCConnecction()
vpc = c.create_vpc('10.0.0.0/16')
```

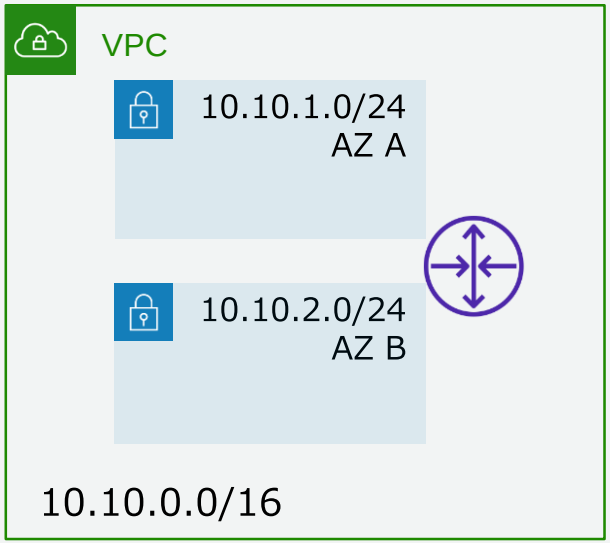
サードパーティツール

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

AWS CloudFormation

```
{
  "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"
      } ]
    }
  }
 }
}
```

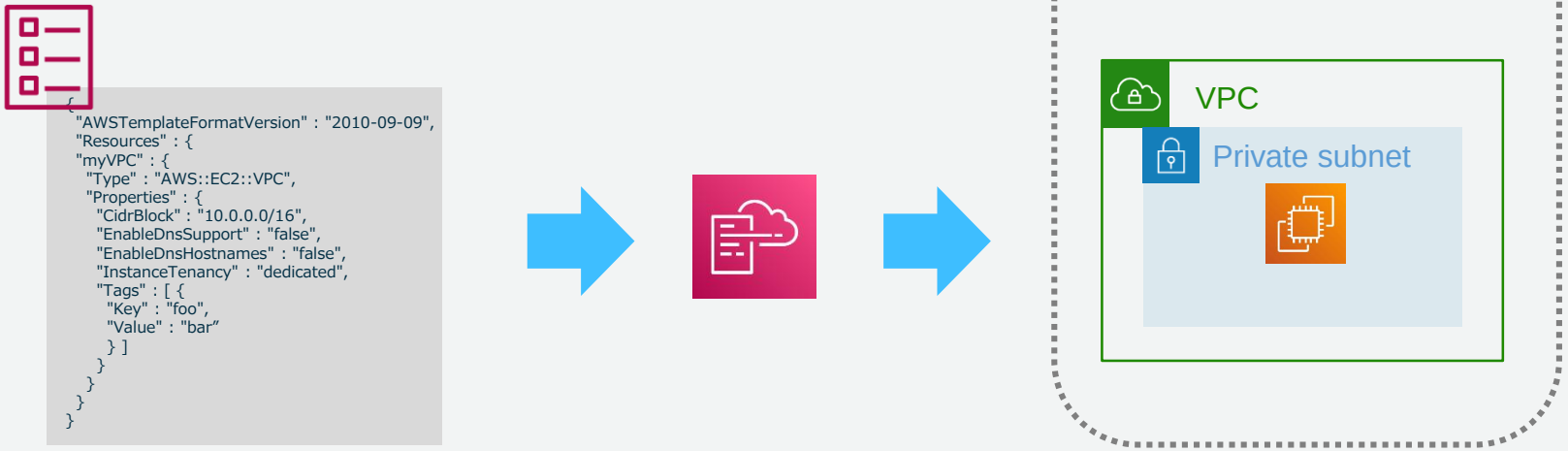
CLI - VPC作成




```
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



テンプレート
(JSON形式)

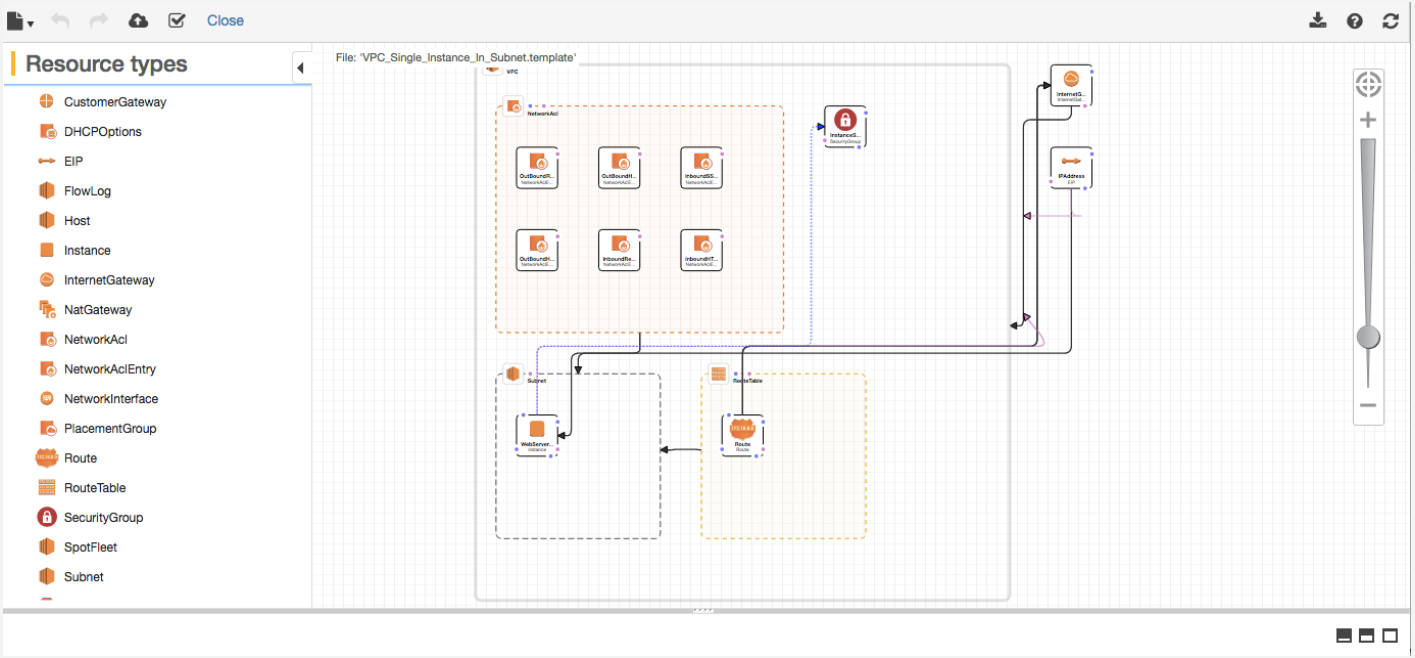
CloudFormation

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

AWS CloudFormationデザイナー

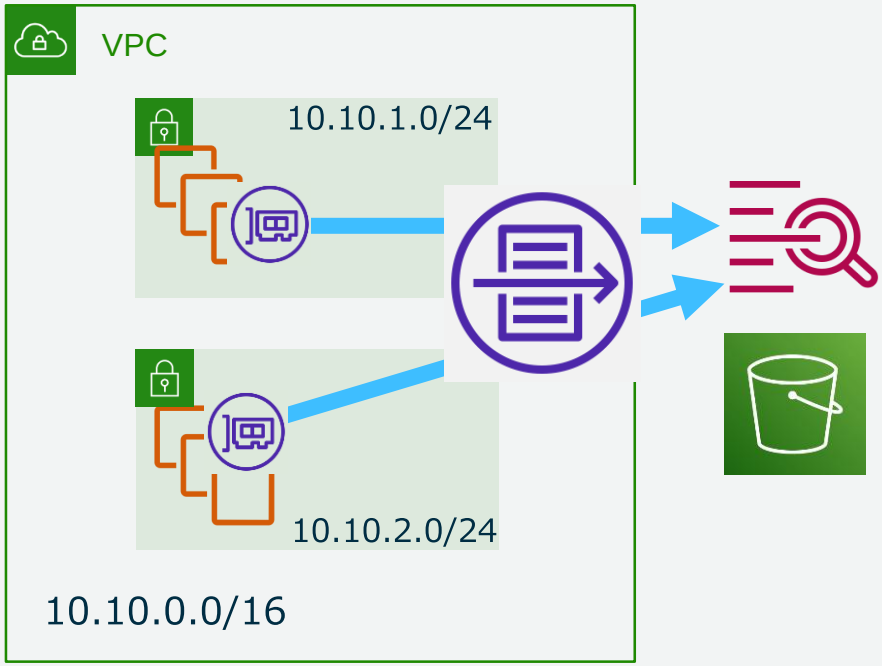
GUIでテンプレートの作成が可能



Agenda

Amazon VPCとは？
VPCのコンポーネント
VPCのセキュリティ
オンプレミスとのハイブリッド構成
VPCの設計
VPCの設定
VPCの運用
まとめ

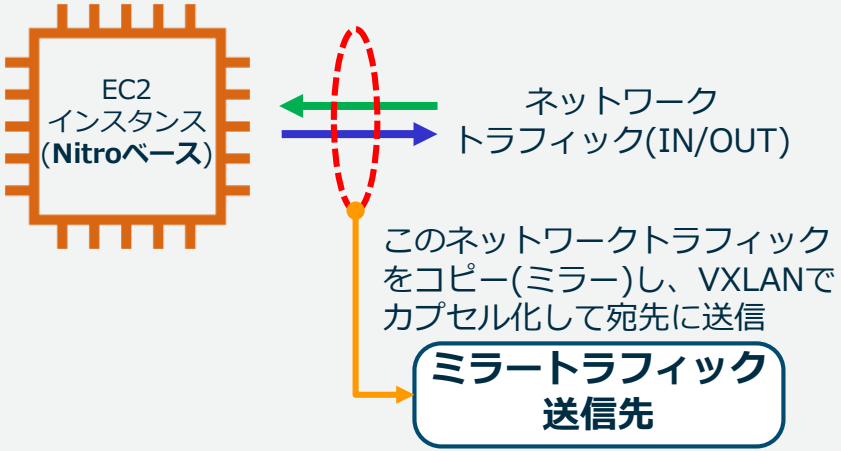
VPC Flow Logsとは



- ネットワークトラフィックをキャプチャし、CloudWatch Logs、S3へPublishする機能
- ネットワークインタフェースを送信元/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フェーストラフィックも取得可能
- 追加料金はなし(CloudWatch Logs,S3の標準料金は課金)

VPC Traffic Mirroring

EC2インスタンスのENIからネットワークトラフィックをミラーリングする機能



[VPC Traffic Mirror機能のユースケース]

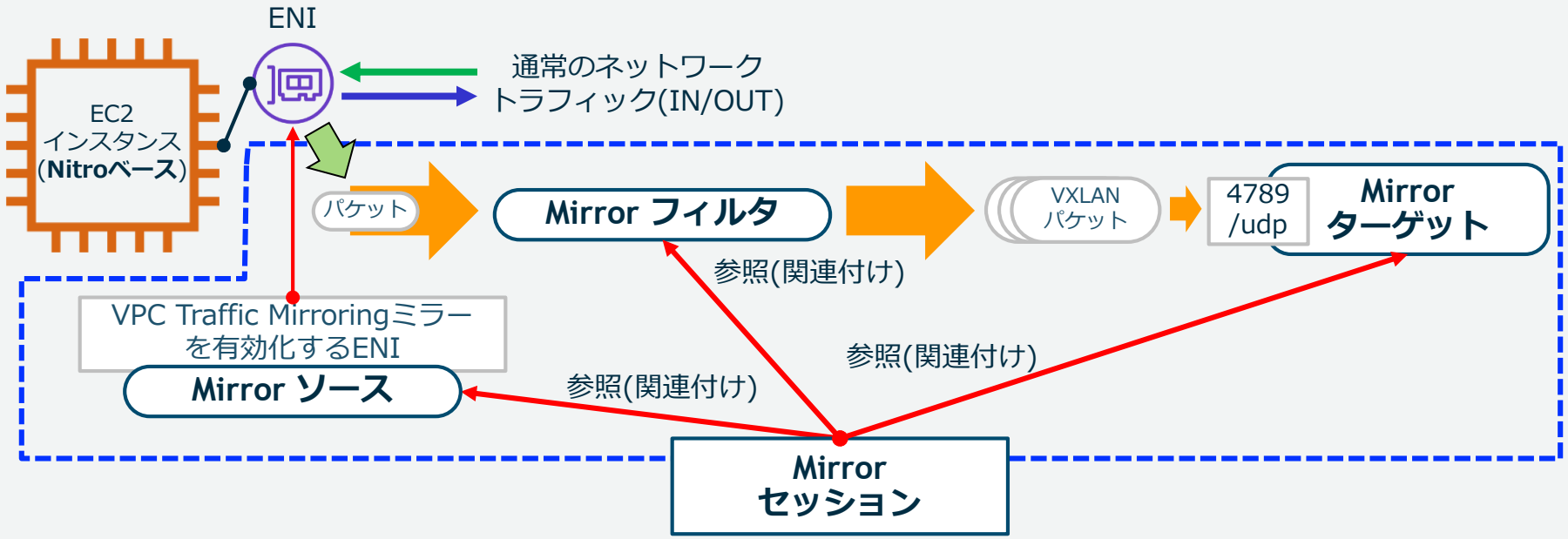
1. **脅威検出(フォレンジック)**
2. **コンテンツモニタリング**
3. **問題判別**

- **VPCフローログには含まれない、パケット内容の取得が可能**

https://aws.amazon.com/jp/about-aws/whats-new/2019/06/announcing-amazon-vpc-traffic-mirroring-for-amazon-ec2-instances/

VPC Traffic Mirroring機能の設定要素(リソース)

VPC Traffic Mirroringは「ソース」「フィルタ」「ターゲット」とそれらを結びつける「セッション」の4つのリソースで構成される

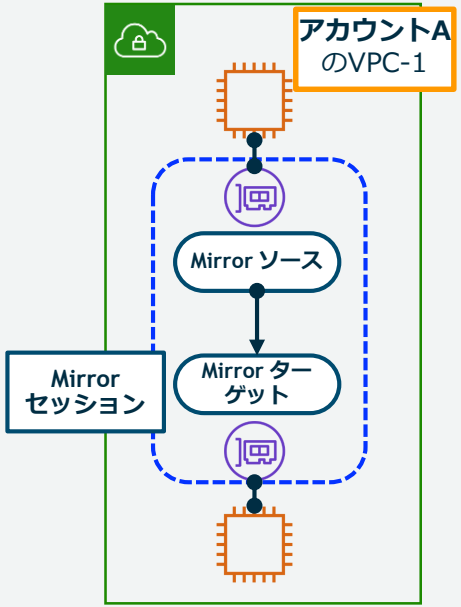


https://aws.amazon.com/jp/about-aws/whats-new/2019/06/announcing-amazon-vpc-traffic-mirroring-for-amazon-ec2-instances/

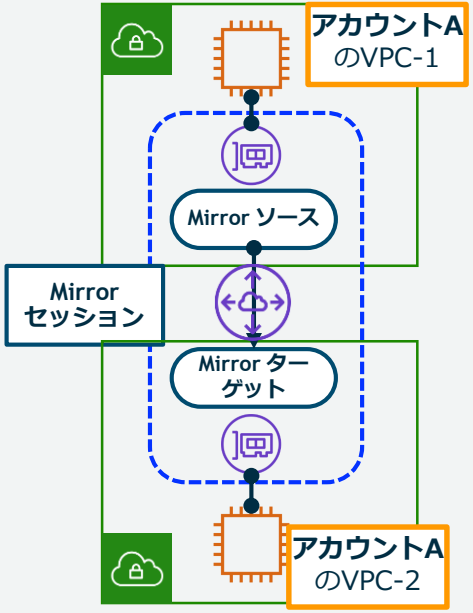
Mirror ソース/フィルタ/ターゲット/セッション

同一リージョンを前提として、下図の構成が可能

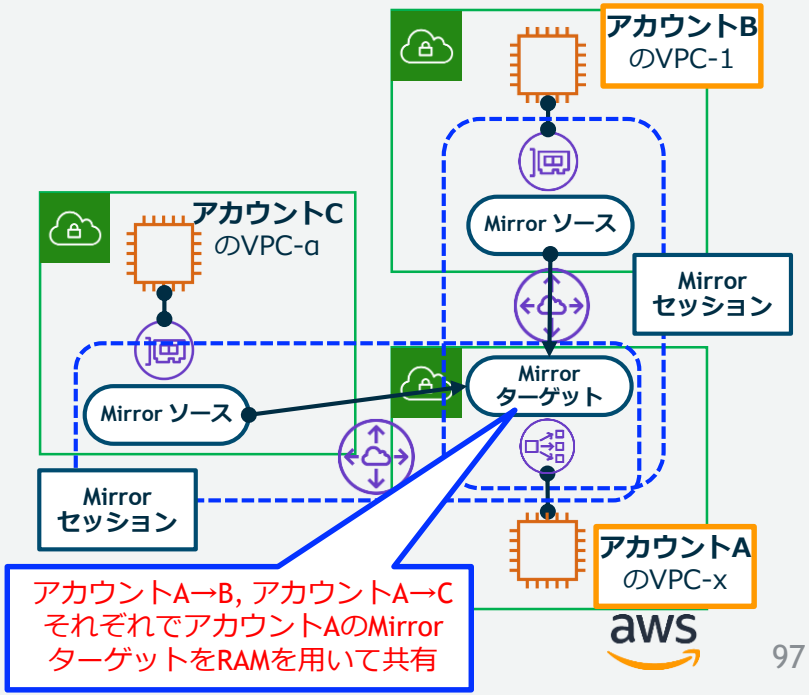
同一アカウント&同一VPC内



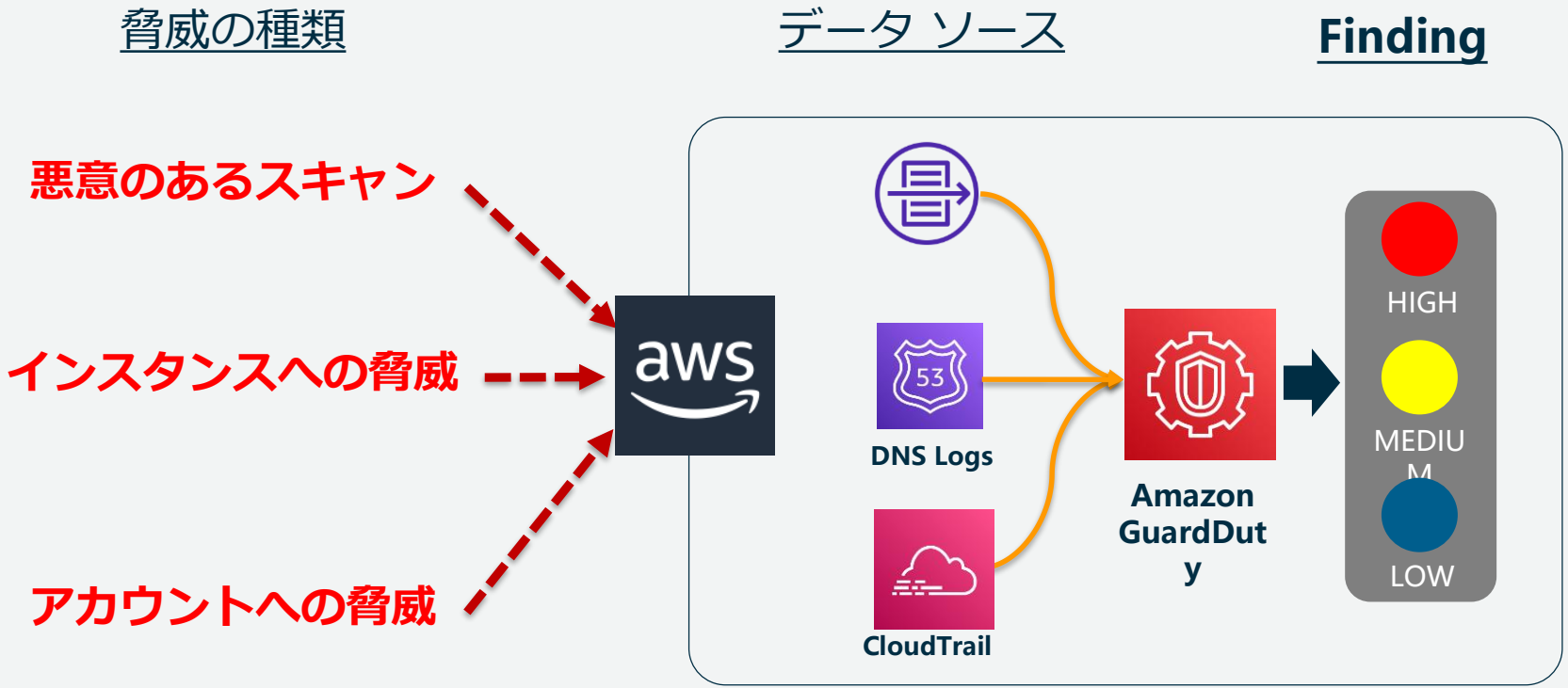
同一アカウント&異なるVPC間



異なるアカウント&異なるVPC間



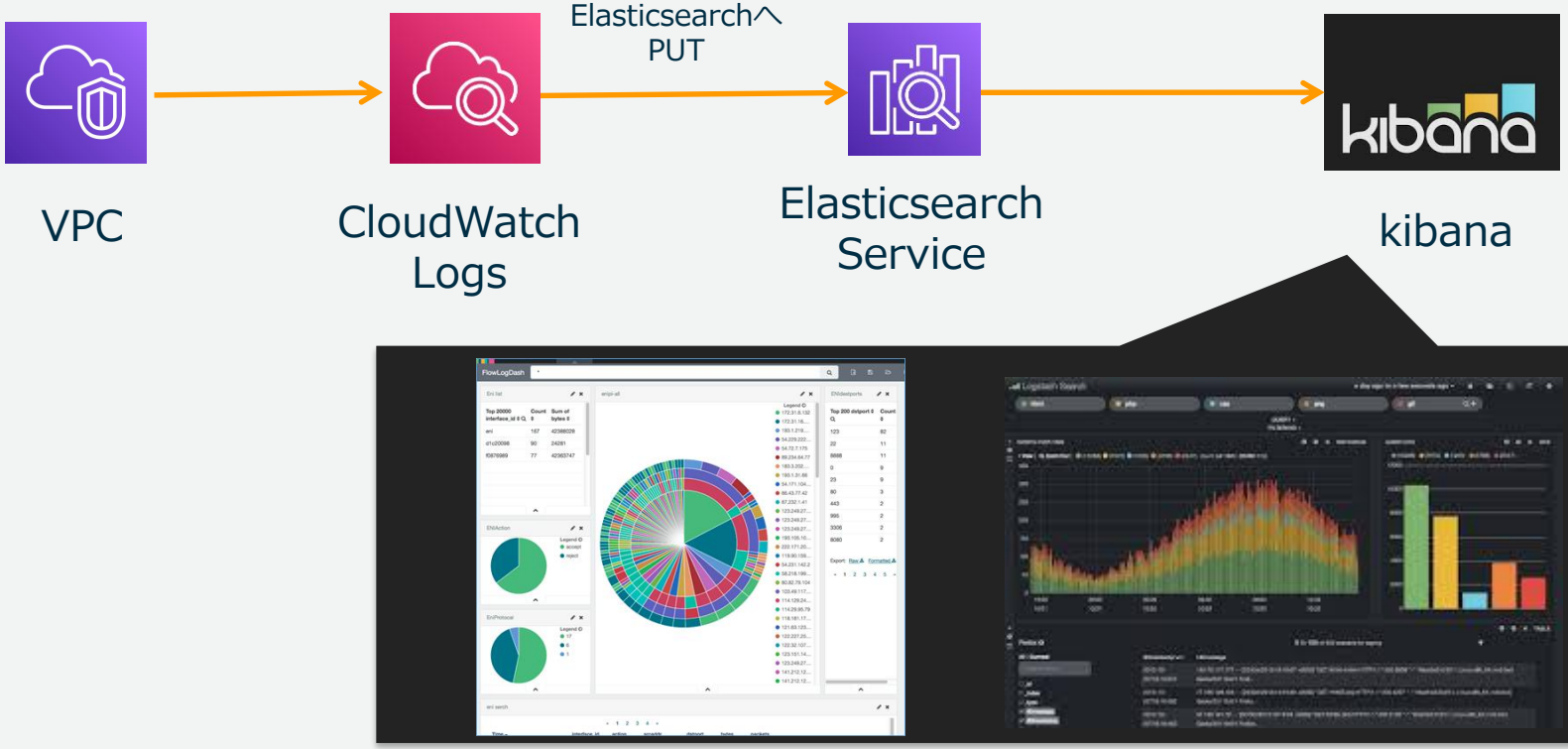
GuardDuty による脅威の検知と通知



Amazon GuardDuty

- AWS環境における、脅威検出を目的としたマネージドサービス
- **EC2**または**IAM**における脅威を検出
- 機械学習による、異常検知の仕組み
- エージェント、センサー、ネットワーク アプライアンス等は不要
- エコシステムの充実
- シンプルなコスト形体と30日間の無料枠

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

Amazon VPC のクォータ関連

代表的なVPCのクオータ

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ものもあり
  - 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

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 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