



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

[AWS Black Belt Online Seminar]

Amazon VPC

サービスカットシリーズ

Archived

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>



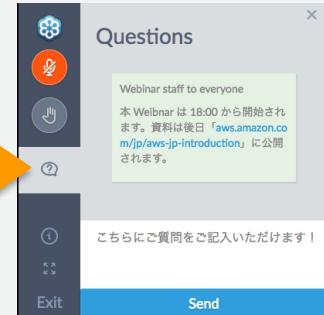
AWS Black Belt Online Seminar とは

「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、Amazon 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

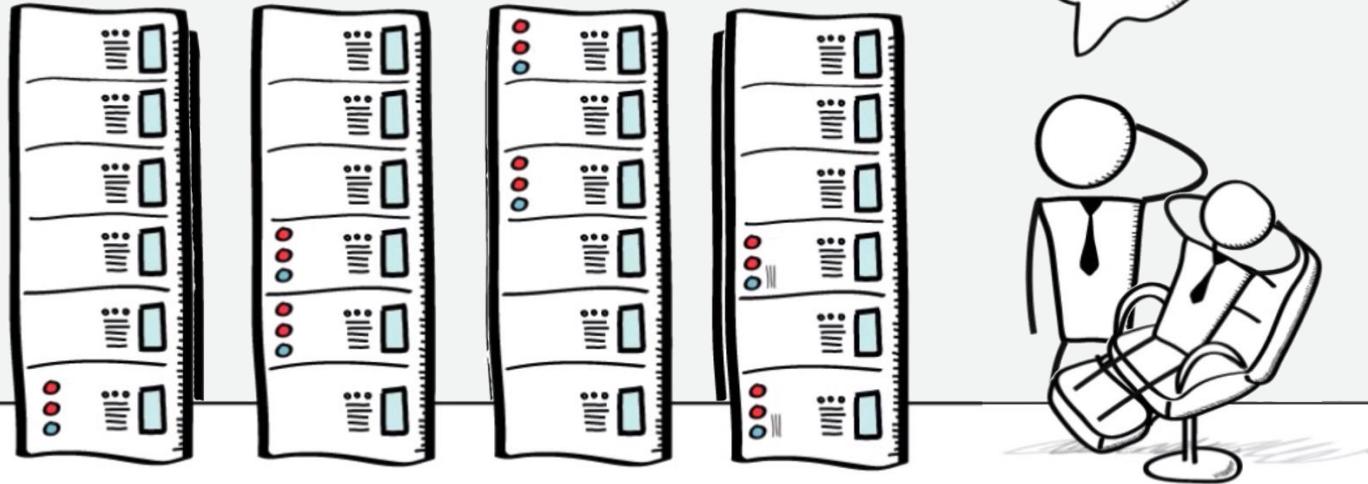
VPCの運用

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

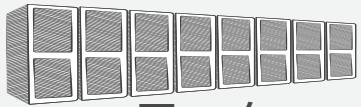


土地、電源、UPS、空調、ラック、ファイバー、パッチパネル、SFP等IFモジュール、スイッチ、ルータ、ストレージ、サーバ、ロードバランサー、ファイアーウォール、WAF、遠隔操作用ターミナルサーバ・・・

Before



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



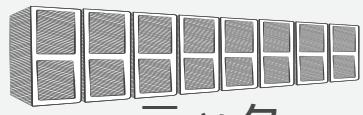
時間（＝コスト）がかかる
早くても数ヶ月、長いと半年

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！



バーチャル
プライベート
ゲートウェイ



Elastic IP



Elastic
ネットワーク
インターフェース



ルート
テーブル



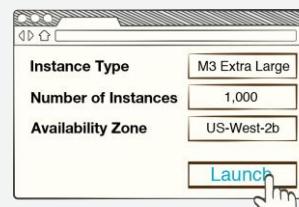
インターネット
ゲートウェイ



仮想ルータ

NAT
ゲートウェイ

+



WEBマネージメントコントール

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



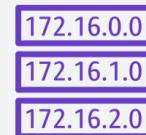
インターネット
ゲートウェイ



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
インターフェース

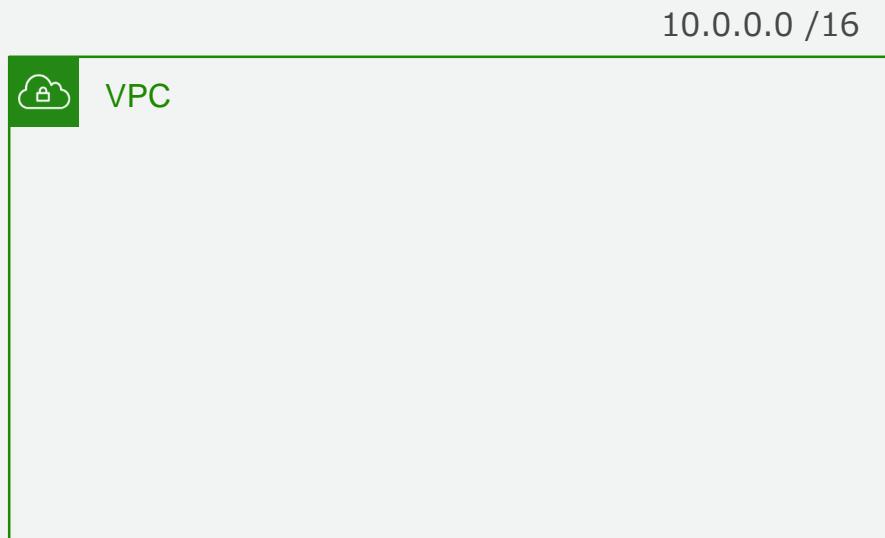


Elastic
ネットワーク
アダプタ

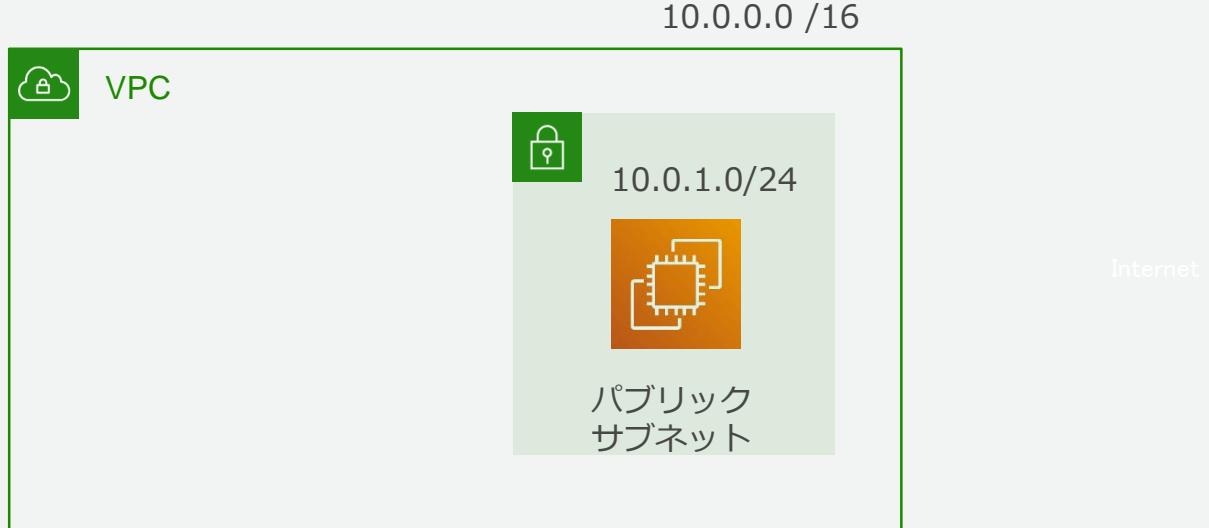


PrivateLink

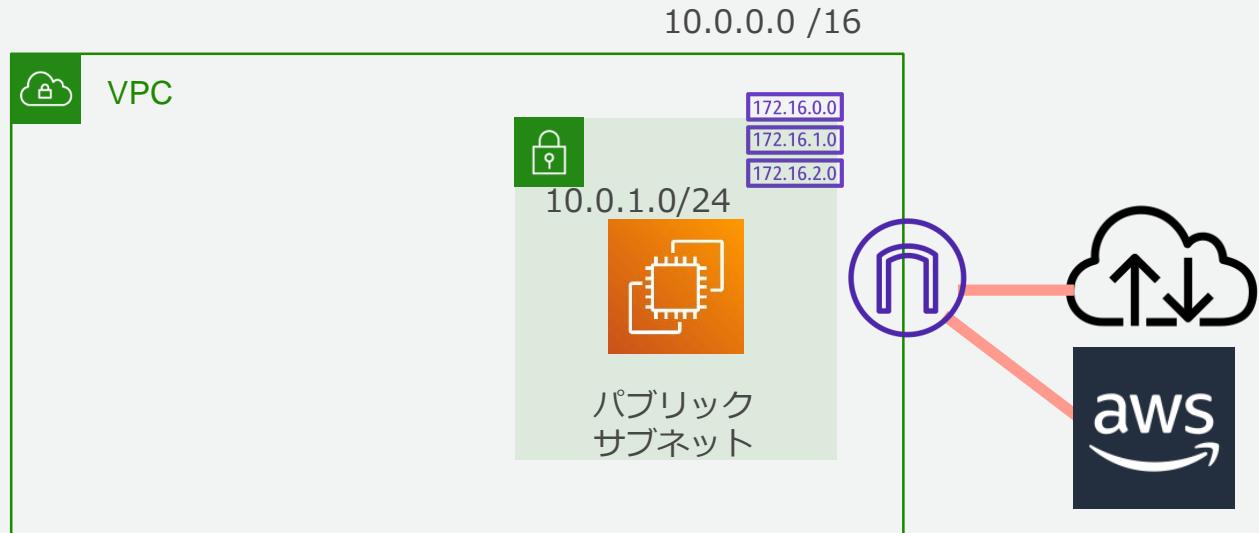
まずは全体のネットワーク空間をVPCとして定義



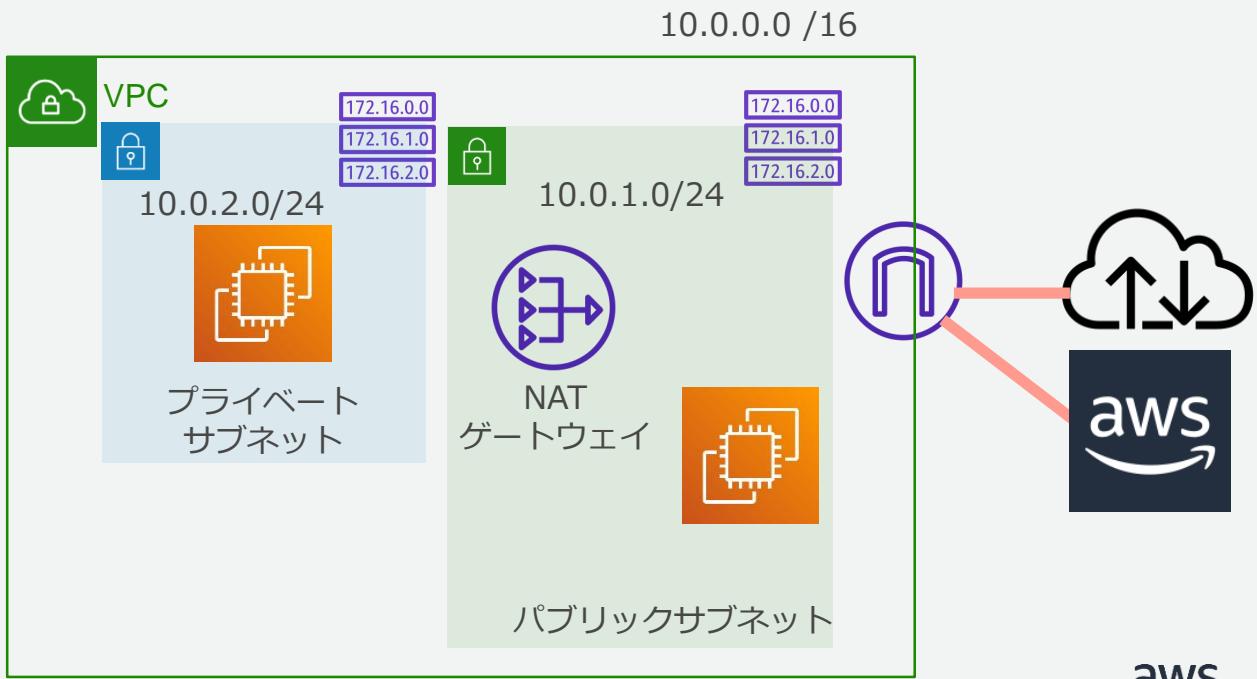
利用するサブネットを定義



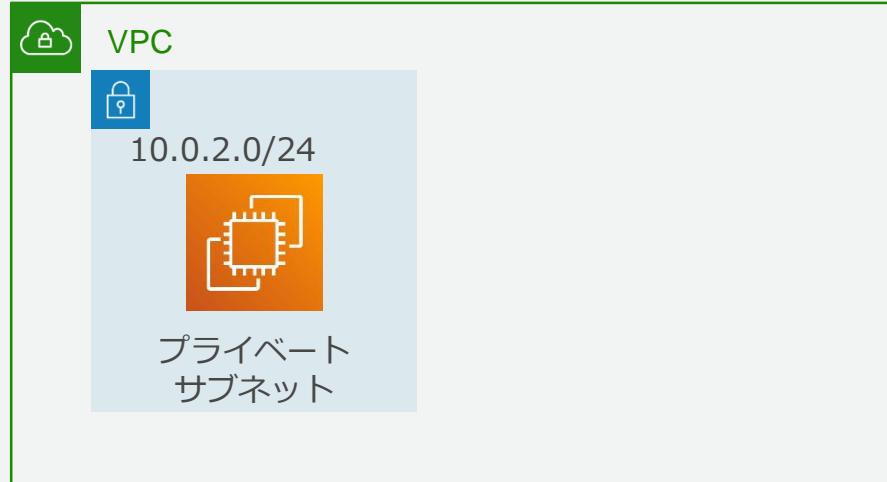
インターネットへの接続を設定



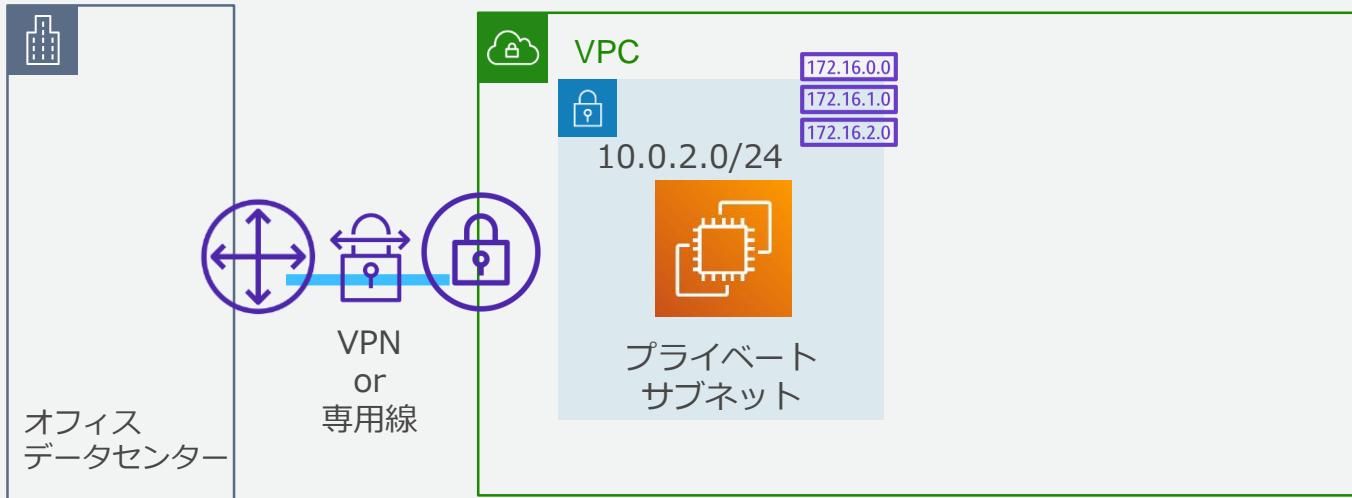
プライベートサブネットを追加



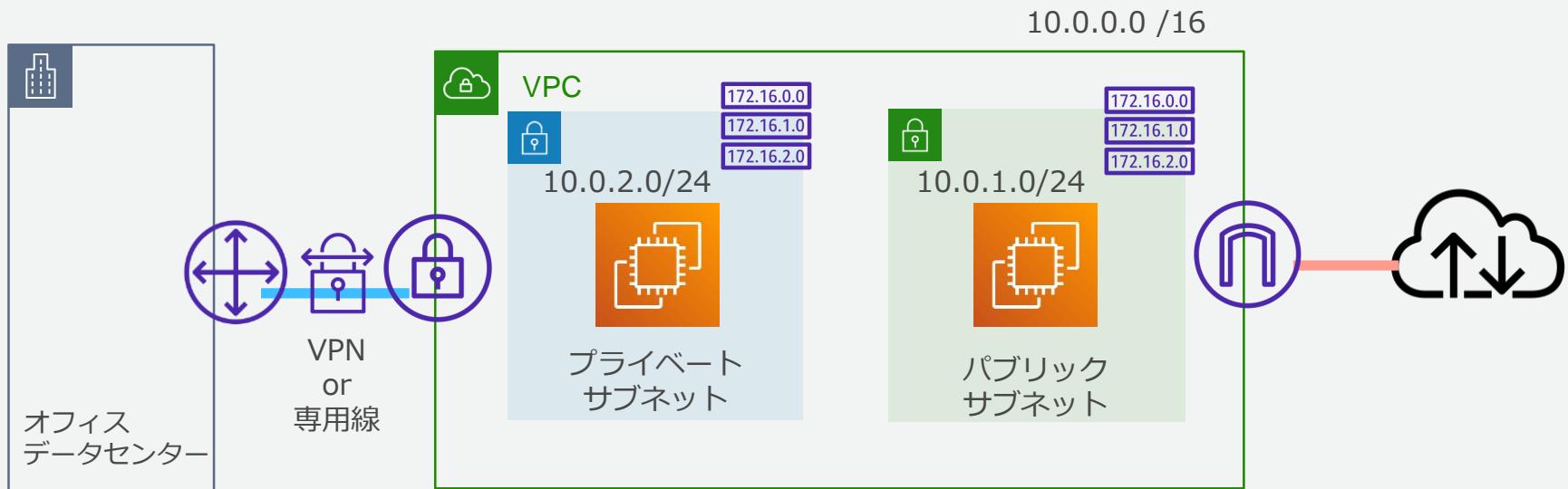
インターネットに接続しないネットワークも作成可能



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

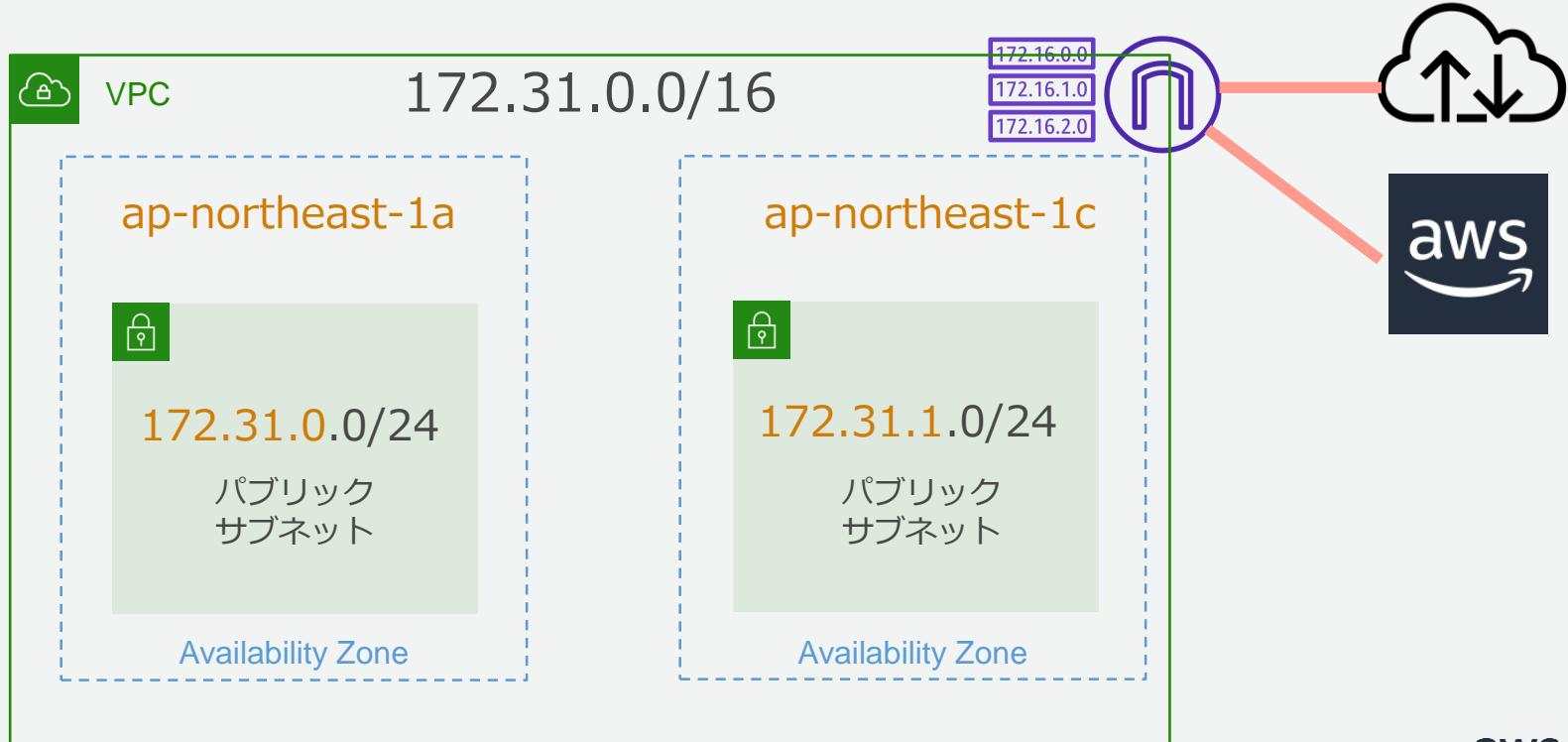


VPC ウィザードで数画面で作成可能

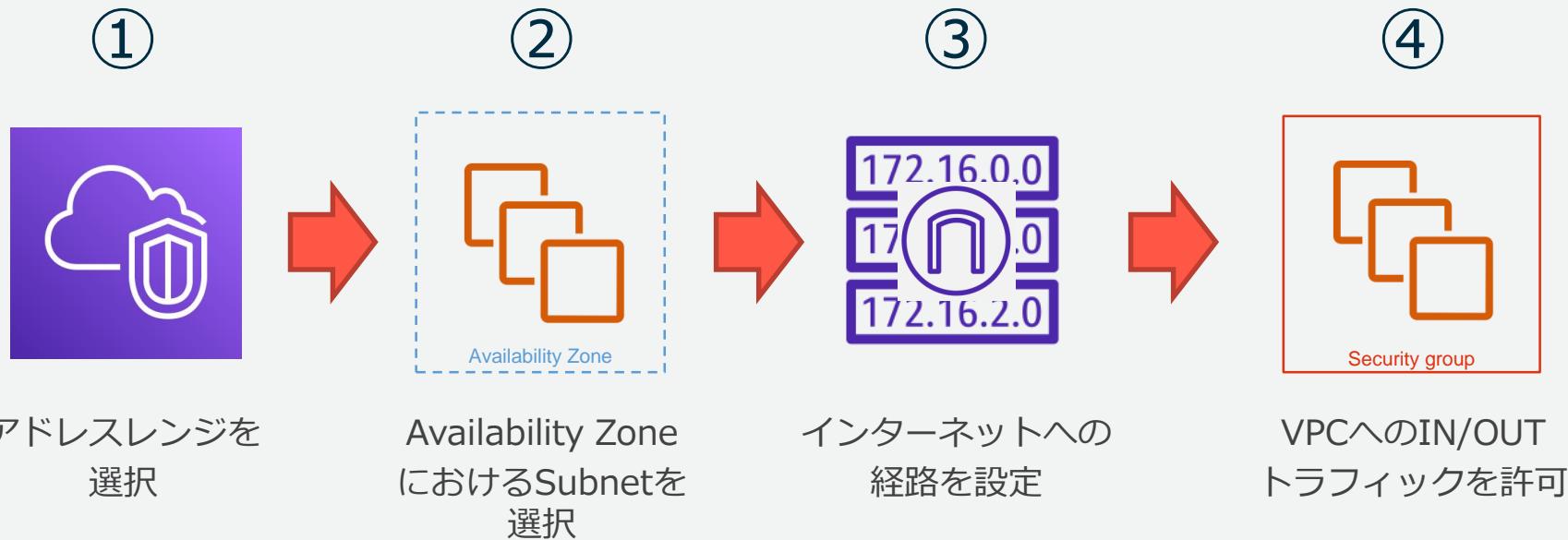


ウォークスルー: インターネット接続VPCセットアップ

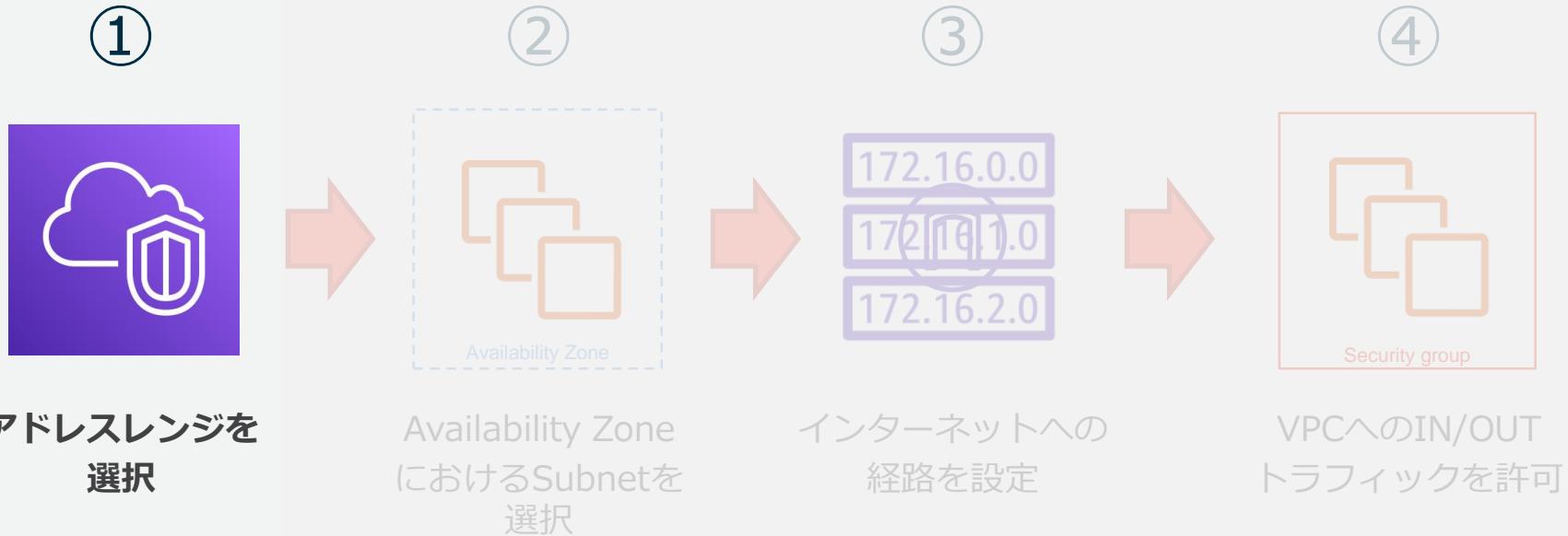
インターネットへの接続を設定するVPCを作成



インターネット接続VPCのステップ^⁹



インターネット接続VPCのステップ^⁹



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

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

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



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

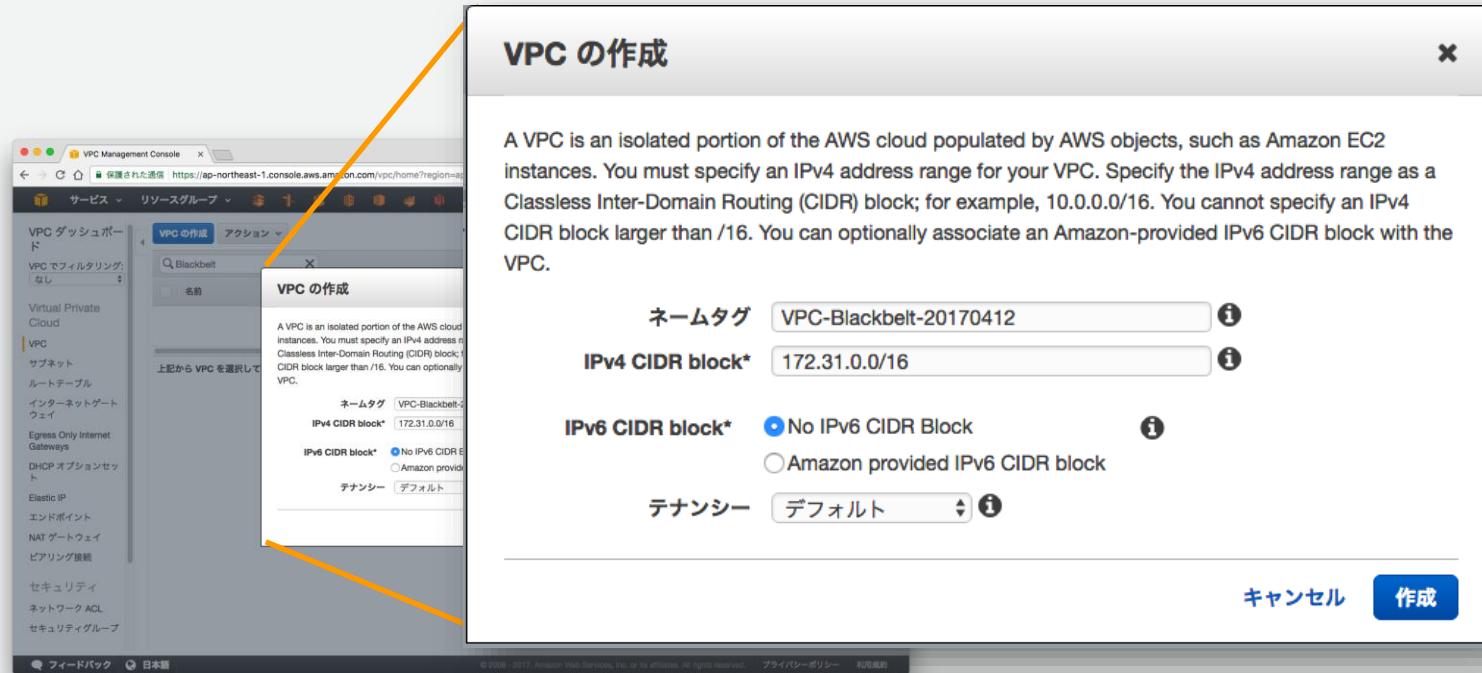
172.31.0.0/16

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)

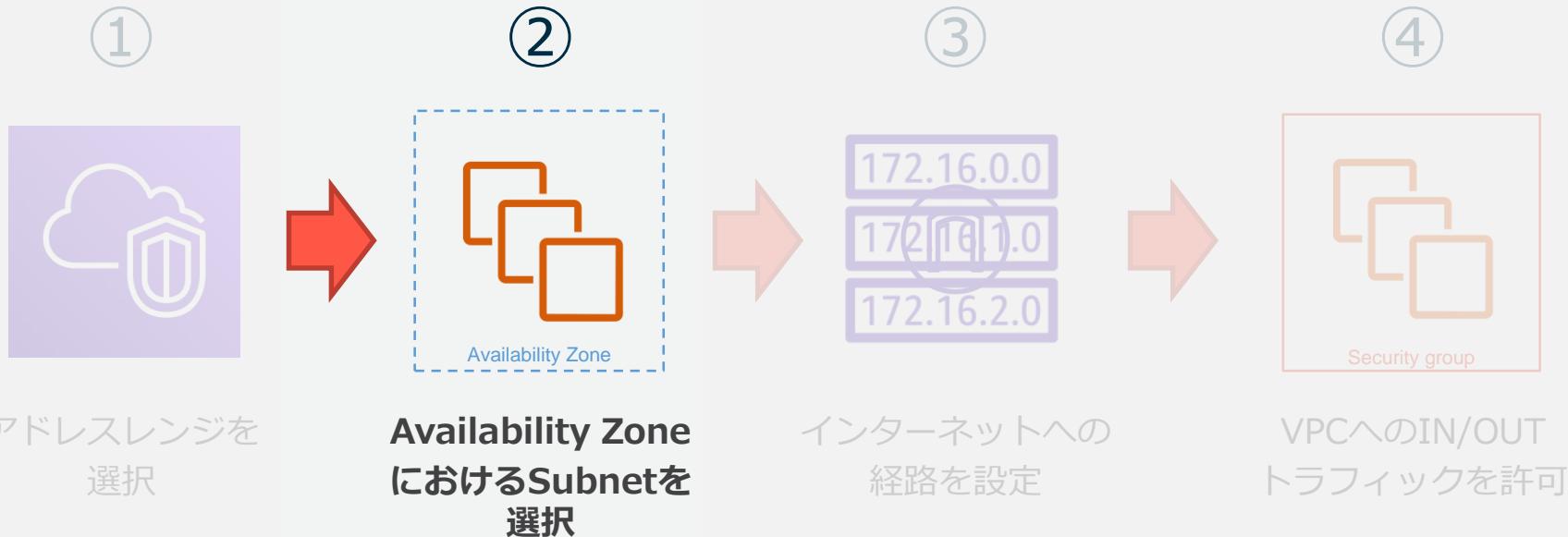
最初に作成したアドレスブロックは作成後変更はできないので注意が必要
2個目以降は追加、削除ができる。

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^⁹



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

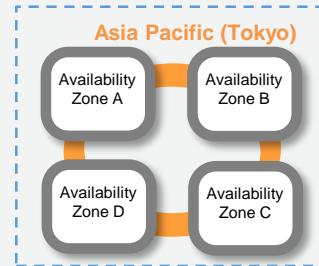
サブネットマスク	サブネット数	サブネットあたりのIPアドレス数
/18	4	16379
/20	16	4091
/22	64	1019
/24	256 ※	251
/26	1024 ※	59
/28	16384 ※	11

※ VPCあたりのサブネット作成上限数はデフォルト 200 個

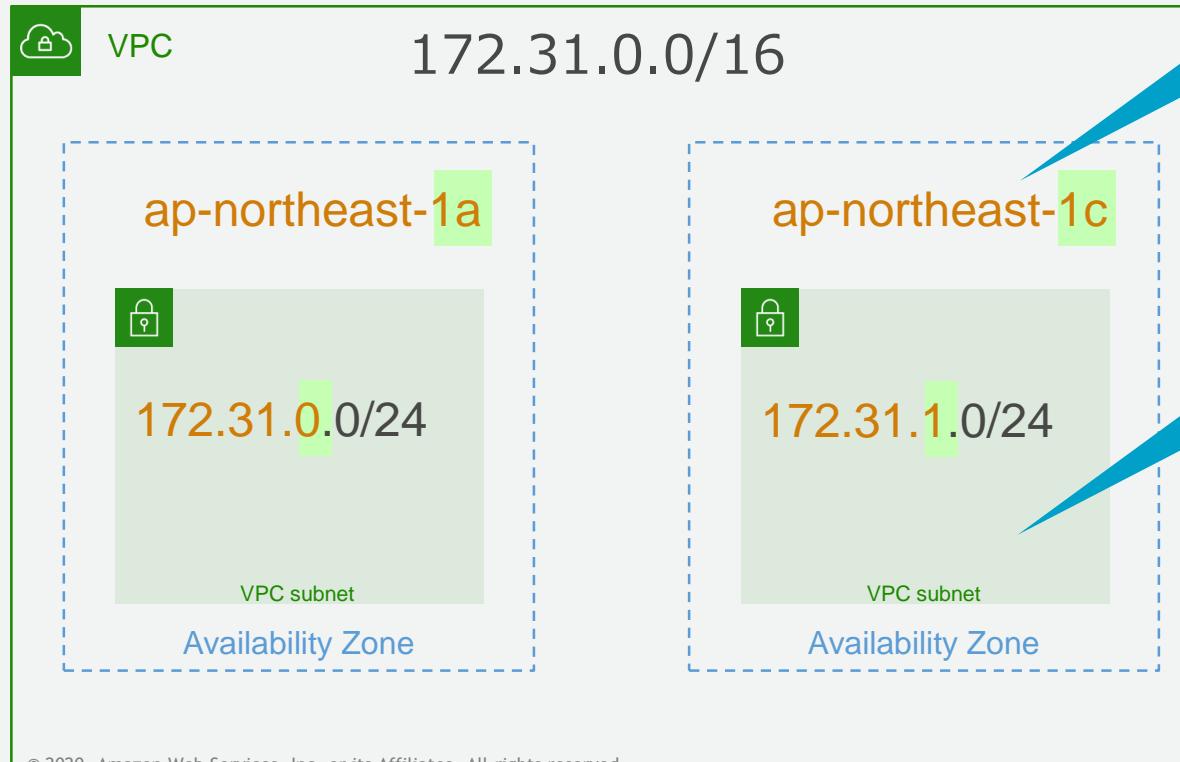
アベイラビリティゾーン

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

The screenshot shows the AWS VPC Management Console with the URL <https://ap-northeast-1.console.aws.amazon.com/vpc/home?region=ap-n...>. The left sidebar is collapsed, and the main area displays the 'Subnet Creation' dialog. The dialog includes fields for Name Tag (Subnet-Public-A), VPC (vpc-9961f2fd | VPC-Blackbelt-20170412), CIDR (172.31.0.0/16), Availability Zone (ap-northeast-1a), and IPv4 CIDR block (172.31.1.0/24). Buttons for 'Cancel' and 'Create' are at the bottom right.

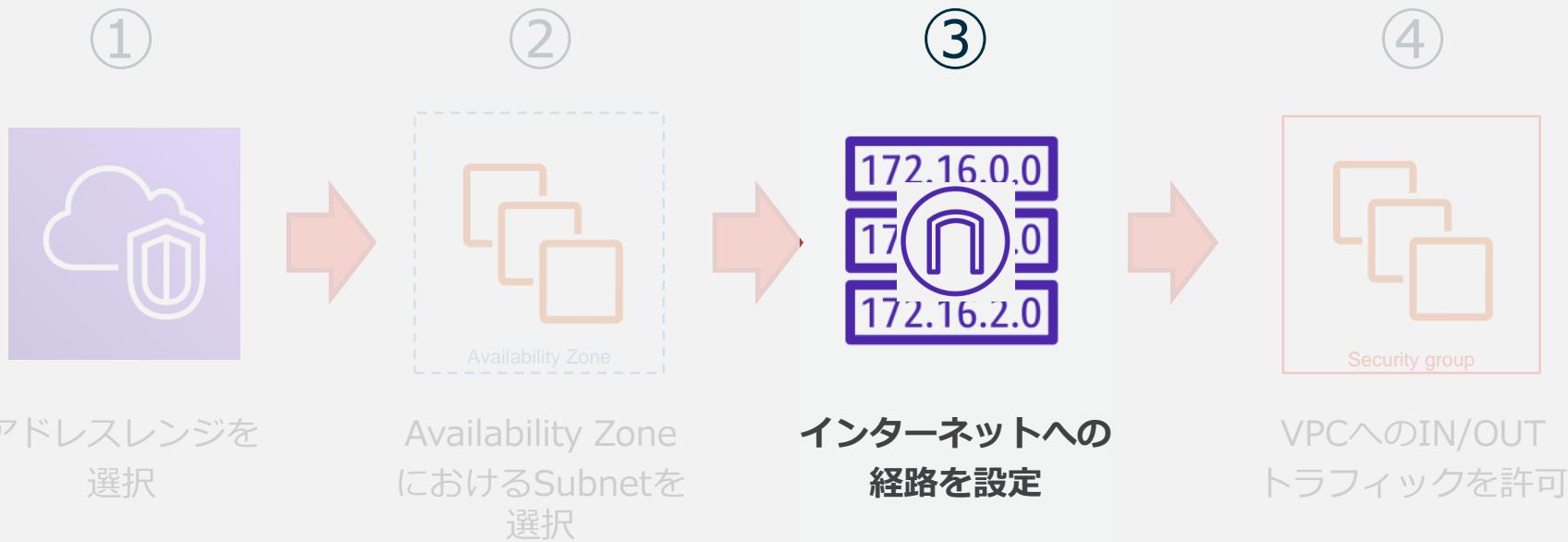
- ・ネームタグ
- ・VPC
- ・アベイラビリティゾーン
- ・IPv4 CIDR block

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ルーター
.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^⁹



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

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 lists various VPC-related services. The main pane displays a table of route tables, with one row selected. A blue callout bubble points to the 'ルート' (Route) tab of the selected route table's details view, highlighting the 'View: All rules' dropdown and the first route entry.

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)

名前	ルートテーブル ID	明示的に関連付け	メイン	VPC
rtb-9c7350f8	0 サブネット	はい	vpc-9961f2fd VPC-Blackbelt-201704...	

rtb-9c7350f8

送信先	ターゲット
172.31.0.0/16	local

ルート

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

要約

インターネットゲートウェイを作成、VPCにアタッチ

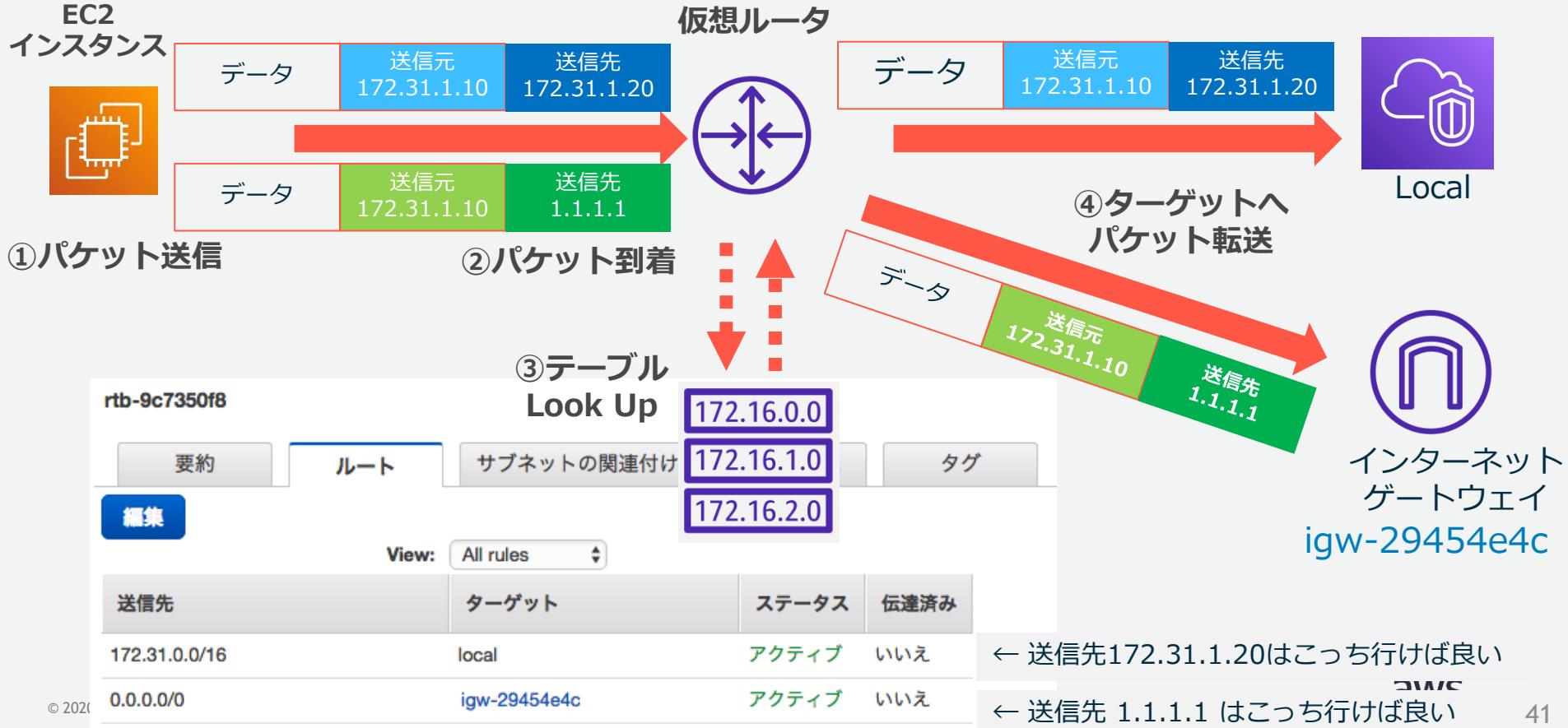
The screenshot shows the AWS VPC Management Console interface. A blue callout bubble points from the bottom left towards the center, containing the text: "VPCからインターネットへの接続がアタッチされた".

Internet Gateway Creation Dialog:
The main dialog is titled "Internet Gatewayの作成". It contains the following text:
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

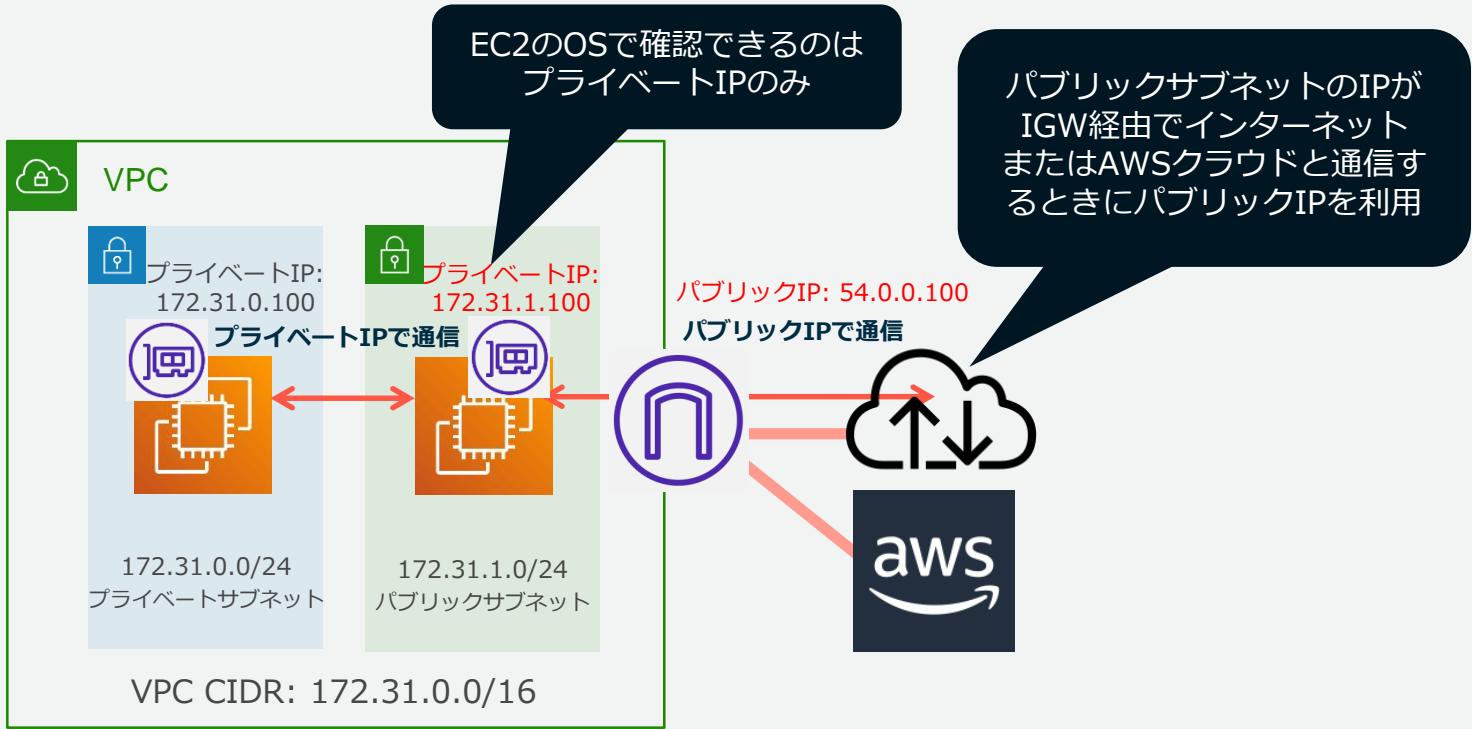
Attach to VPC Dialog:
A smaller dialog titled "VPCにアタッチ" is displayed below. It contains the following text:
インターネットとの通信を有効にするため、インターネットゲートウェイをVPCに接続します。
VPC: vpc-9961f2fd | VPC-Blackbelt-20170412
Buttons: キャンセル, アタッチ

Internet Gateway List:
At the bottom, a table lists the created Internet Gateway.
Name: VPC-Blackbelt-20170412, ID: igw-29454e4c, Status: attached, VPC: vpc-9961f2fd | VPC-Blackbelt-20170412

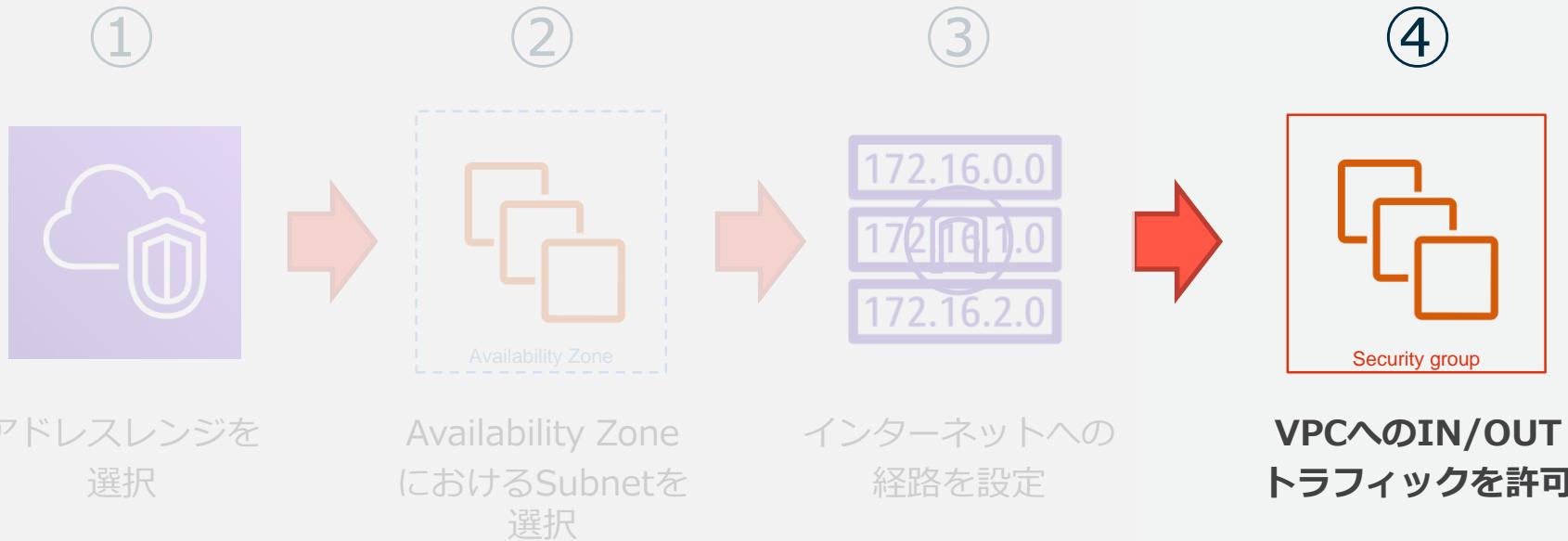
仮想ルータとルートテーブルの関係(ルートLook up)



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^⁹



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 URL <https://ap-northeast-1.console.aws.amazon.com/vpc/home?region=ap-n...>. The left sidebar lists various VPC services. The main area shows the 'Security Groups' section, where a new rule is being created for a security group named 'sg-0fe2e368'. The 'Inbound Rules' tab is selected. A blue callout bubble on the right states: '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)'. Another blue callout bubble at the bottom right states: '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'.

セキュリティグループの作成 セキュリティグループのアクション

要約 インバウンドルール アウトバウントルール

キャンセル 保存

タイプ	プロトコル	ポート範囲	送信元	削除
すべての トラフィック	すべて	すべて	sg-0fe2e368	i x
HTTP (80)	TCP (6)	80	0.0.0.0/0	i x

別のルールの追加

タイプ	プロトコル	ポート範囲	送信元	削除
すべての トラフィック	すべて	すべて	sg-0fe2e368	i
HTTP (80)	TCP (6)	80	0.0.0.0/0	i

別のルールの追加

Network ACLs = ステートレス Firewall

The screenshot shows the AWS VPC Management Console with the Network ACL creation page. On the left, a sidebar lists various VPC-related services. The main area displays a table of Network ACL rules. An orange arrow points from the sidebar's 'セキュリティ' (Security) link to the 'セキュリティ' section of the table header. Another orange arrow points from the sidebar's 'ネットワーク ACL' (Network ACL) link to the 'ルール #' (Rule #) column of the table.

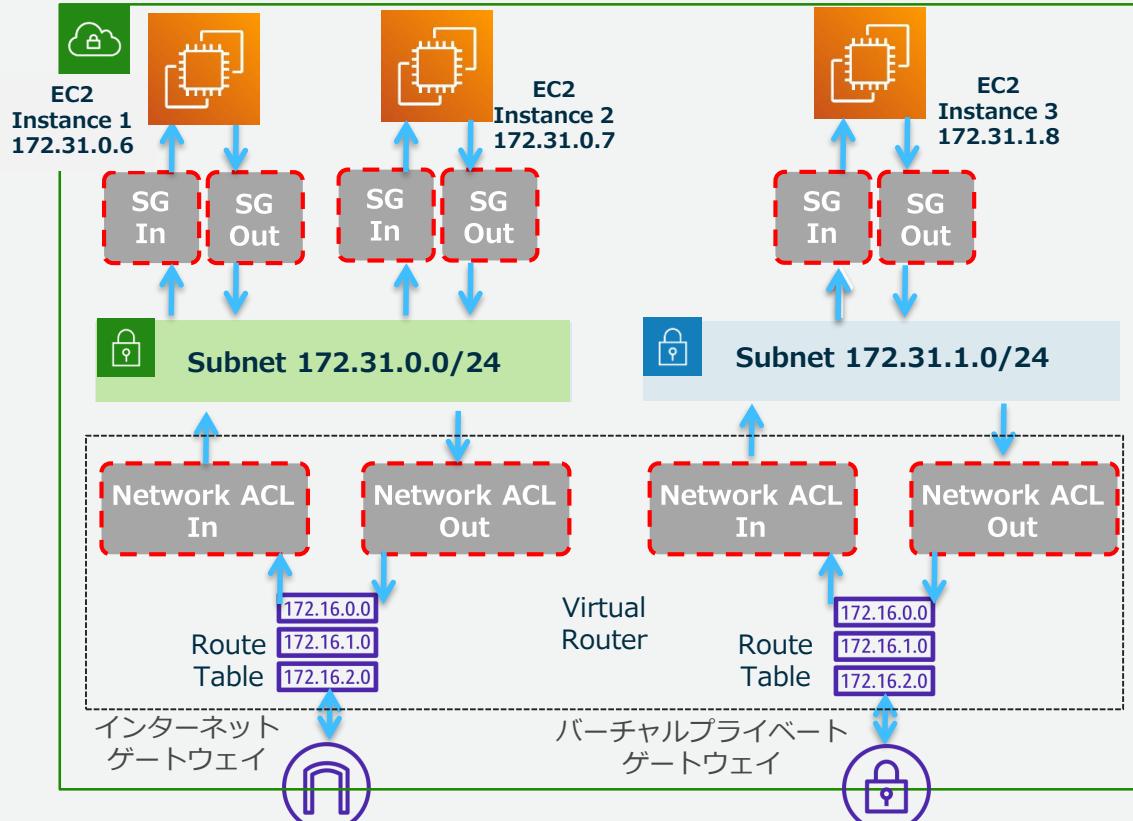
ルール #	タイプ	プロトコル	ポート範囲	送信元	許可/拒否
100	すべての トランザクション	すべて	すべて	0.0.0.0/0	許可
*	すべての トランザクション	すべて	すべて	0.0.0.0/0	拒否

A blue speech bubble on the right contains the text: "サブネット単位で適用される" (Applied at the subnet level) and "デフォルトでは全ての送信元IPを許可" (Default allows all source IP addresses).

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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

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

The screenshot shows the AWS VPC console interface. On the left, there's a sidebar with various navigation options like 'New VPC Experience', 'Elastic IP New', 'マネージドプレフィックスリスト New', 'エンドポイント', 'エンドポイントのサービス', 'NAT ゲートウェイ New', 'ピアリング接続', 'セキュリティ', 'ネットワーク ACL', 'セキュリティグループ New', '仮想プライベートネットワーク (VPN)', 'カスタマーゲートウェイ', '仮想プライベートゲートウェイ', 'サイト間の VPN 接続', and 'クライアント VPN エンドポイント'. The main area is titled 'マネージドプレフィックスリスト (1/3) 情報' and shows a table with one item: 'pl-0b' (prefix-test, 10, IPv4, Create-complete). Below this, a detailed view for 'pl-0b - prefix-test' shows two entries: 'CIDR' (10.0.0.0/16, 10.1.0.0/16) and '説明'.

- 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

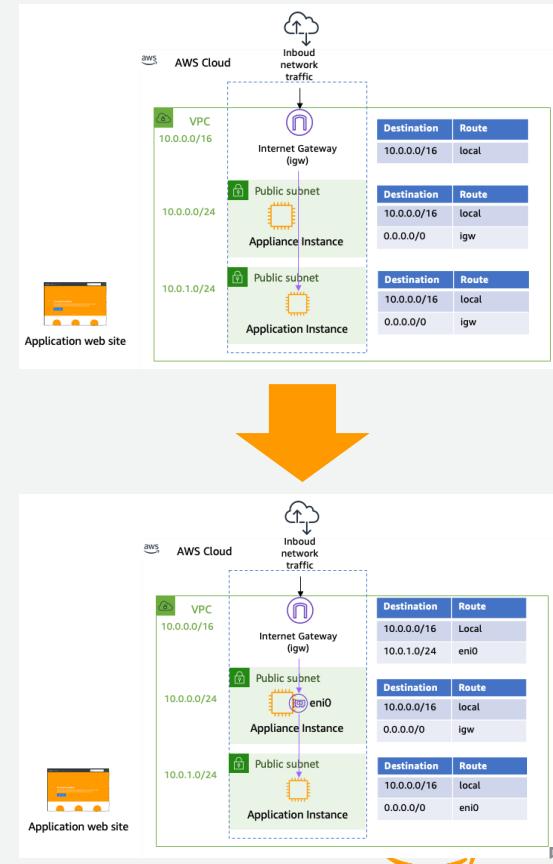
<https://aws.amazon.com/jp/about-aws/whats-new/2020/06/amazon-virtual-private-cloud-customers-use-prefix-lists-simplify-configuration-security-groups-route-tables/>

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

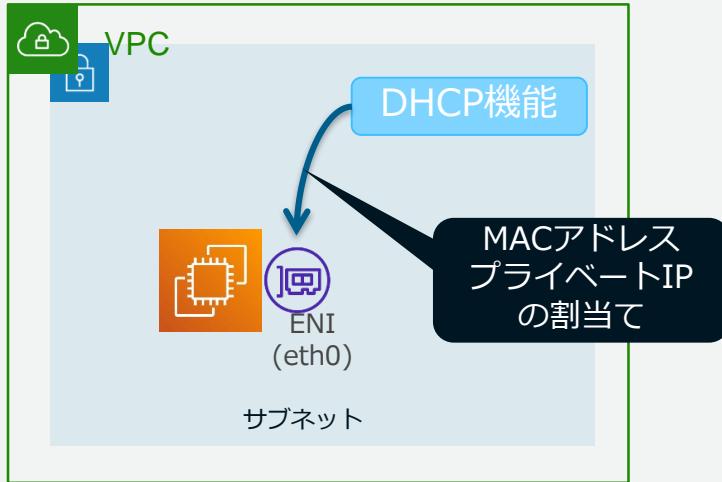
The screenshot shows two CloudFormation stacks being created:

- Stack 1: rtb-1**
 - Outputs:** rtb-1 (Route Table ID)
 - Resources:**
 - rtb-1:** Route Table (Associations: 2 gateways, Main: No, VPC ID: vpc-0)
 - igw-1:** Internet Gateway (Attached to VPC vpc-0)
 - vgw-1:** Virtual Private Gateway (Attached to VPC vpc-0)
 - Outputs:** rtb-1 (Route Table ID)

Stack 2: rtb-0
 - Outputs:** rtb-0 (Route Table ID)
 - Resources:**
 - rtb-0:** Route Table (Associations: 1 gateway, Main: Yes, VPC ID: vpc-0)
 - Outputs:** rtb-0 (Route Table ID)

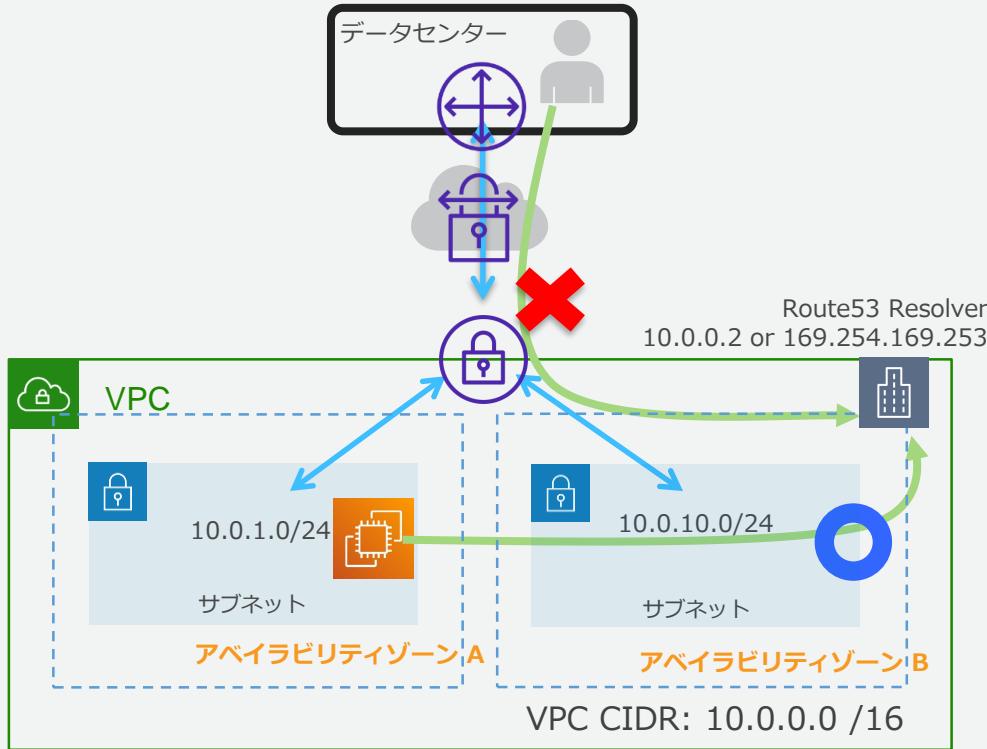
VPCセットアップの補足

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)
- ・EC2インスタンスを再起動しても、割り当てる固定IPは変わらない。

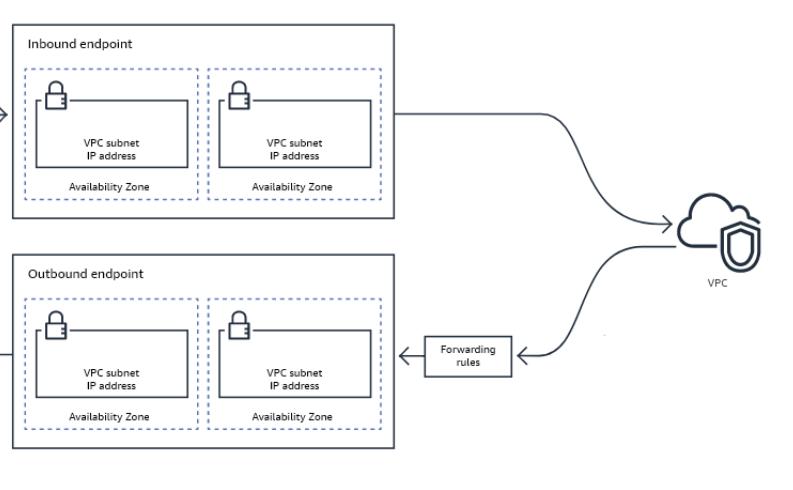
Route53 resolver(AmazonProvidedDNS)



- 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



- ・ 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

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

DNS機能の有効化とホストへのDNS名割当て

vpc-edge.poc1 (10.0.0.0/16) | edge.poc1

Summary Tags

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

Network ACL: acl-edge.poc1
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes

Enable DNS resolution

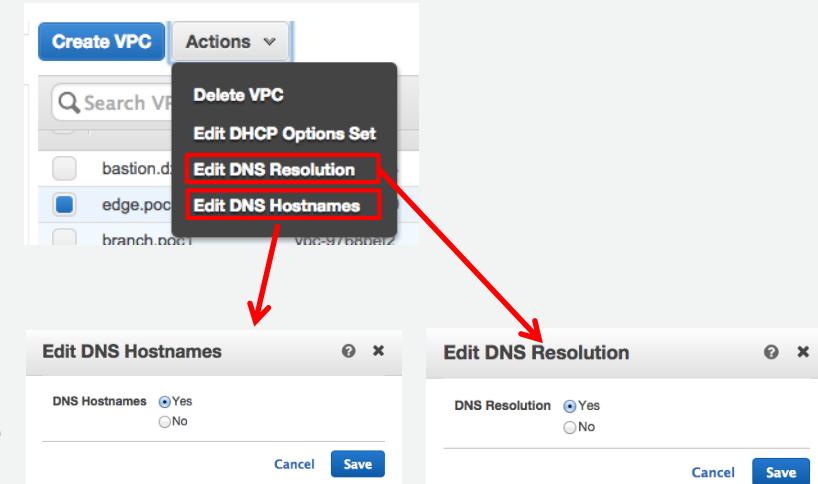
基本はyesとする

NoにするとVPCのDNS機能が無効となる

Enable DNS hostname

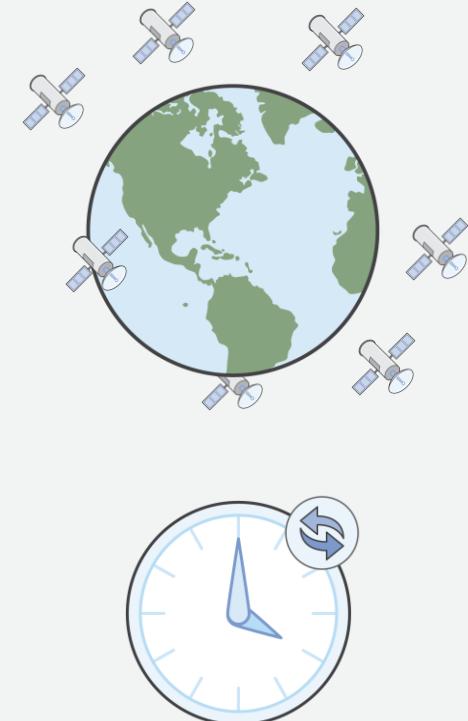
TrueにするとDNS名が割り当てられる

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



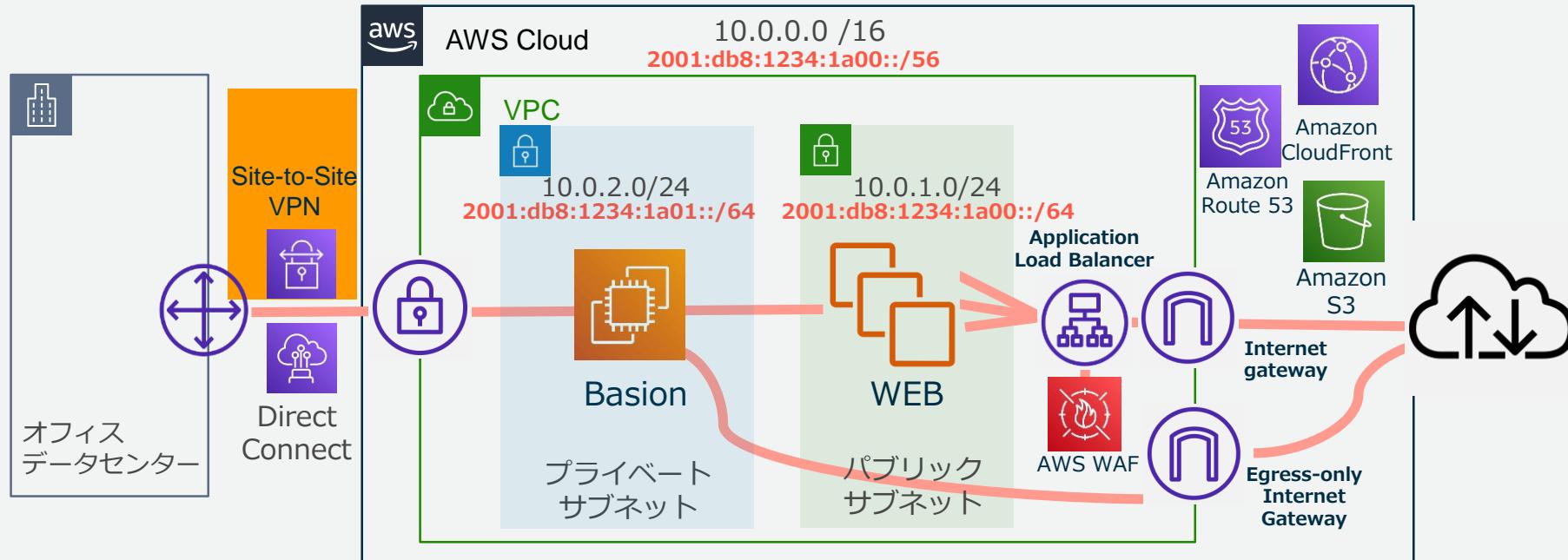
Amazon Time Sync Service

- 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

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、Direct Connect	VPN、Direct Connect

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

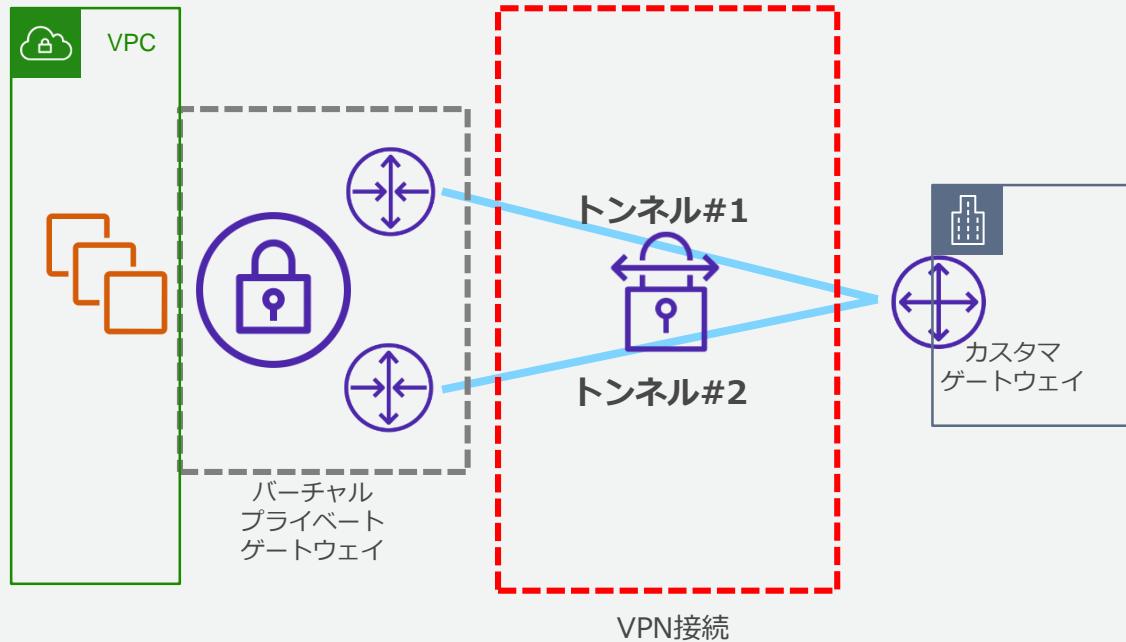
VPN接続

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

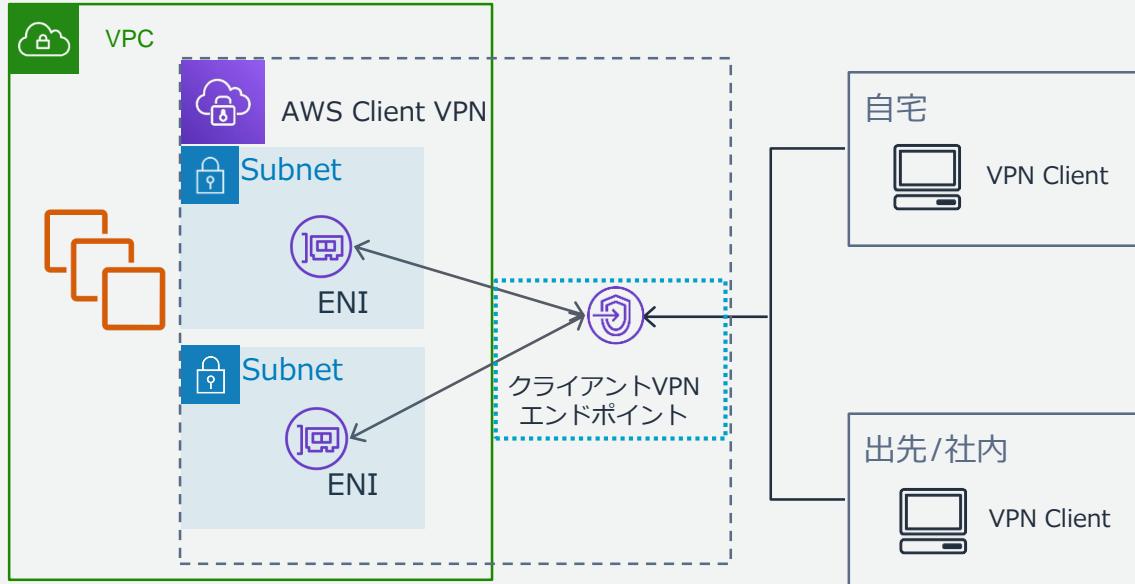
AWS Direct Connectを利用し、一貫性のあるネットワーク接続を実現
本番サービス向け

Site-to-Site VPN接続構成



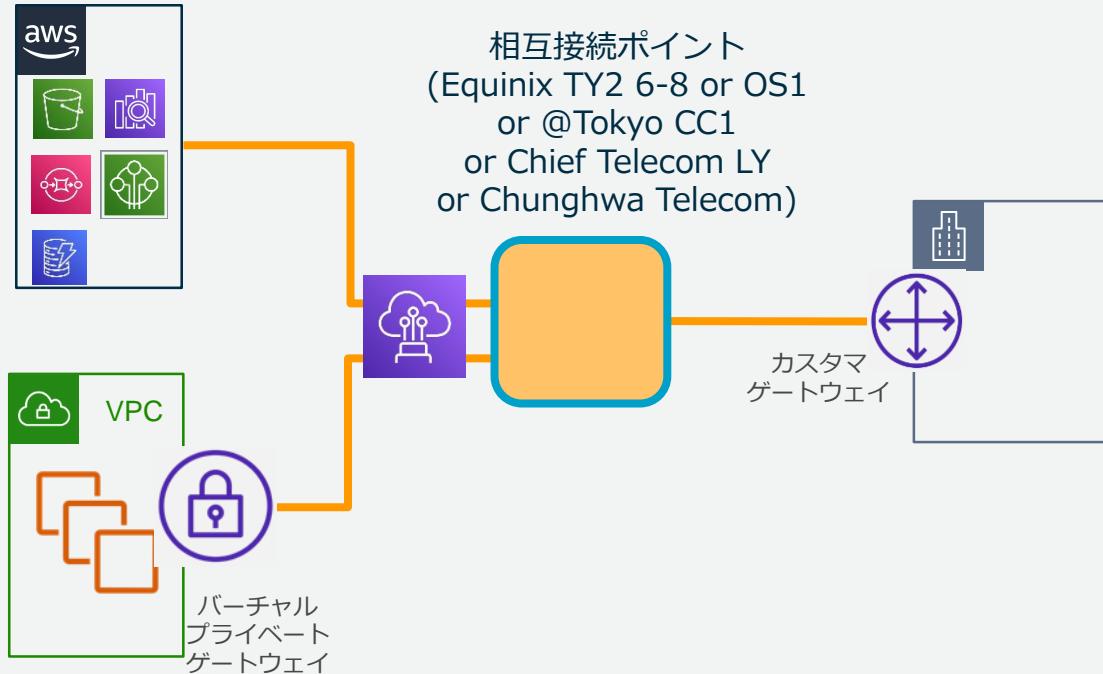
- ・1つのVPN接続は2つのIPsec
トンネルで冗長化
- ・ルーティングは
静的(スタティック)
動的(ダイナミック:BGP)
が選択可能

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

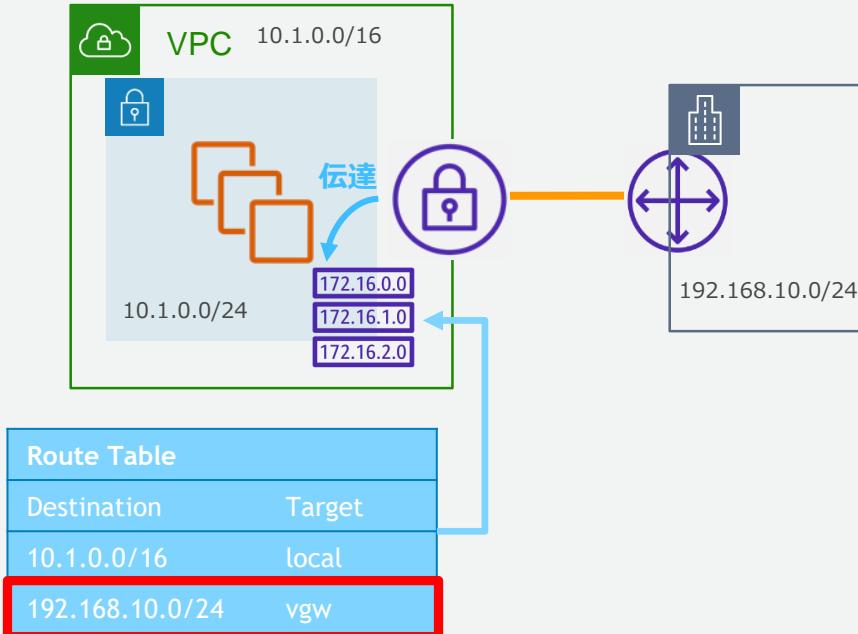
専用線(Direct Connect)接続構成



- 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)

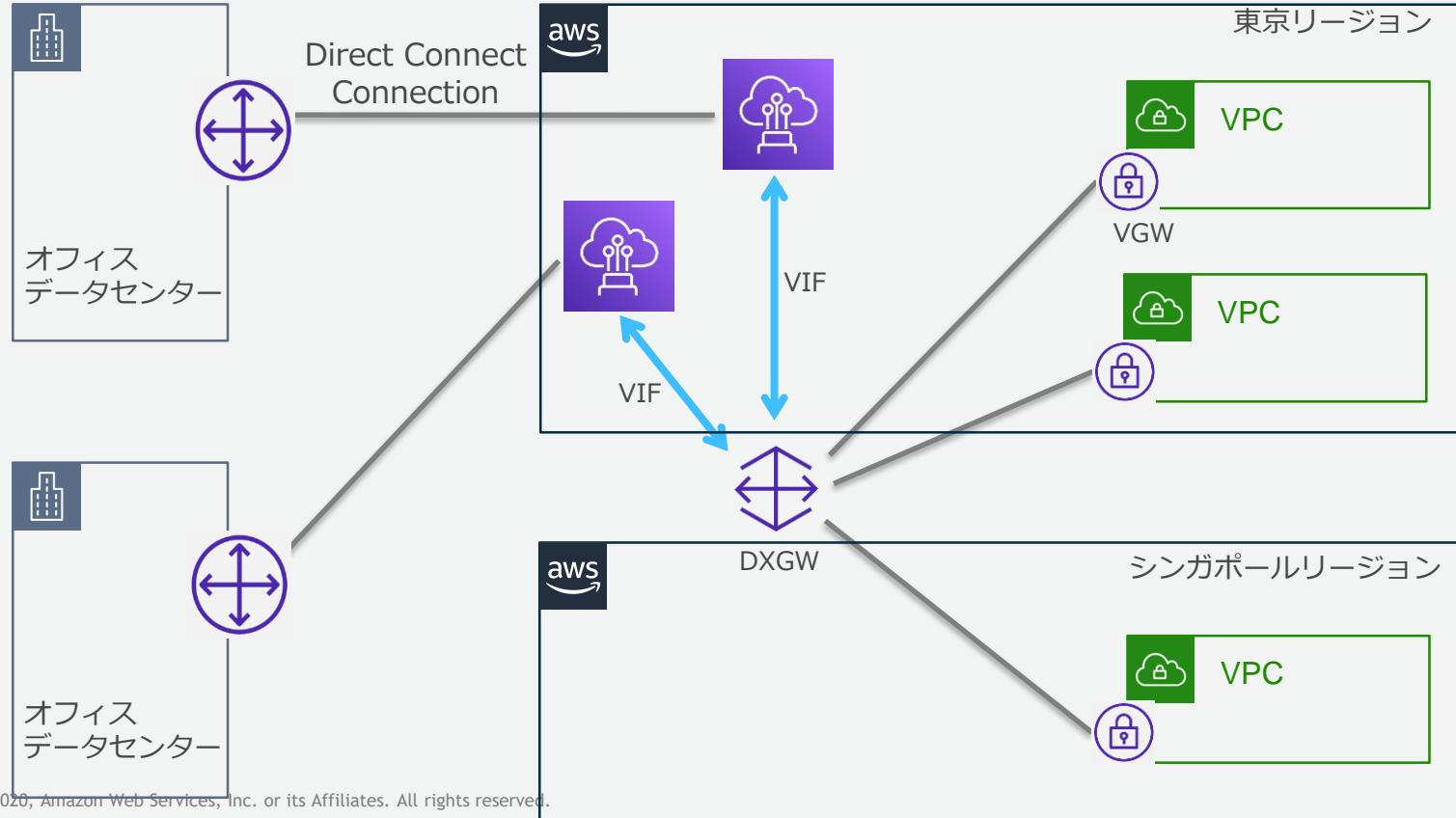
Direct Connect Gateway



- 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

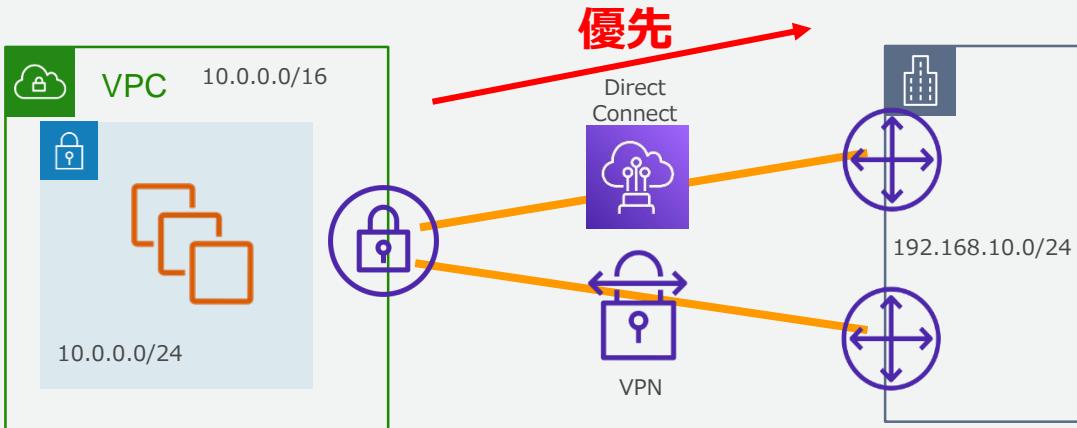
- VPNとDirect Connectを同じVGWに接続することが可能

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

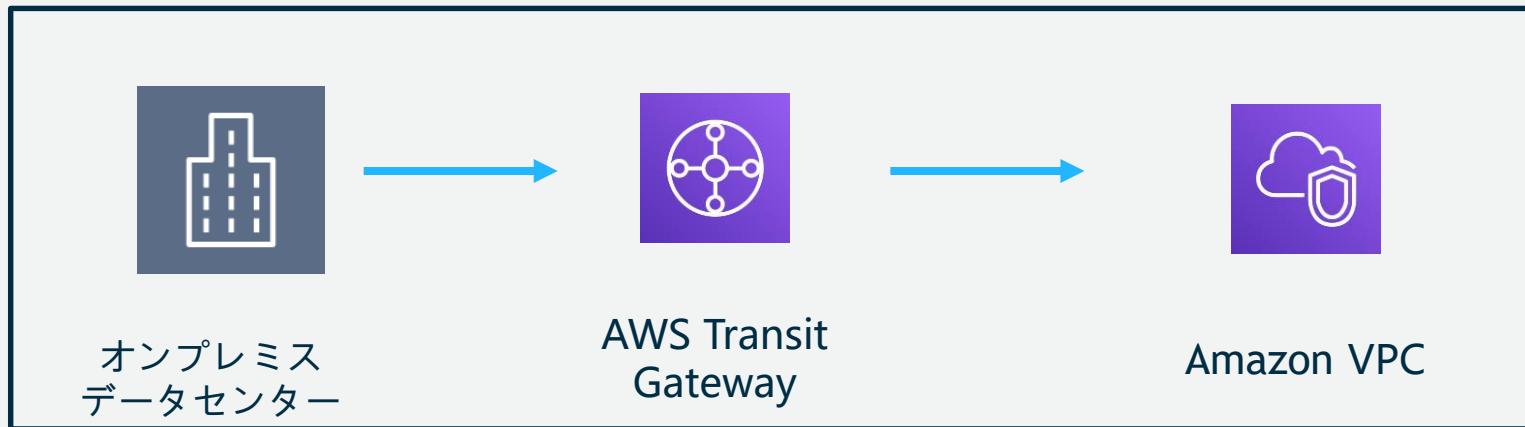
(VPNを優先したい場合はVPNルータからDirect Connectより長いPrefixを広告)

- 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

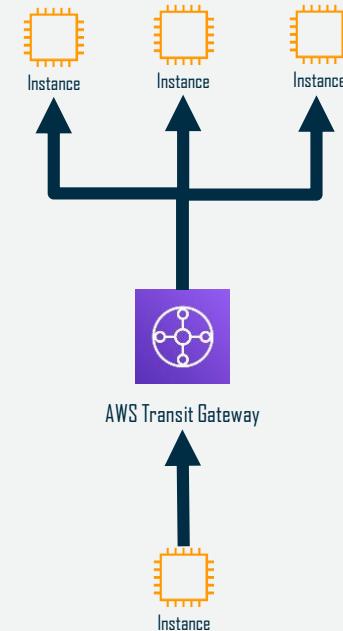


Transit GatewayのMulticast対応

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

管理用アカウント(logging, AWS Organizations, billing, landing zone)

Account

Account

Account

Account

IAM, クロスアカウント ロール

開発

テスト

本番

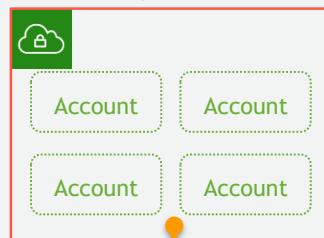
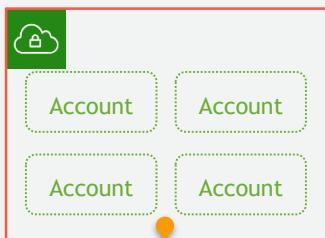
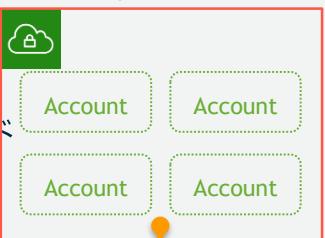
シェアドサービス

アウトバウンド

URL filtering

NAT gateway

DLP / Proxy



エッジサービス

WAF / ADC

SD-WAN

VPN / Firewall



Internal



AWS VPN



AWS Direct Connect



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

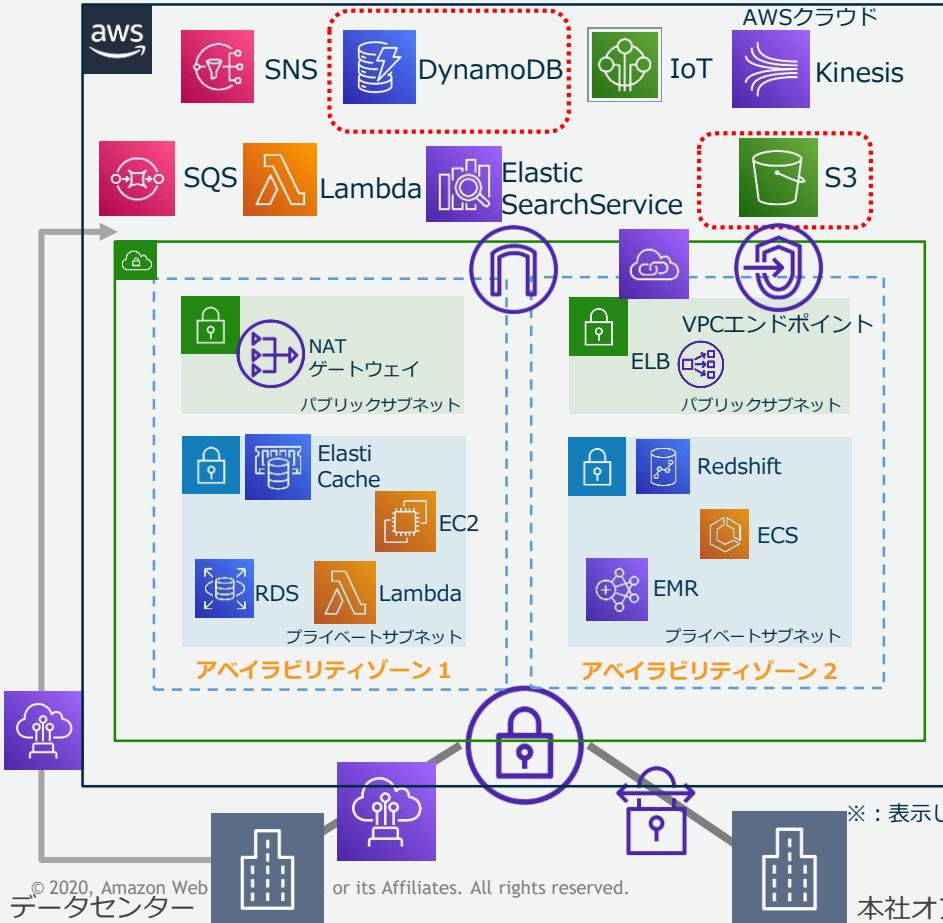
まとめ



VPC設計のポイント

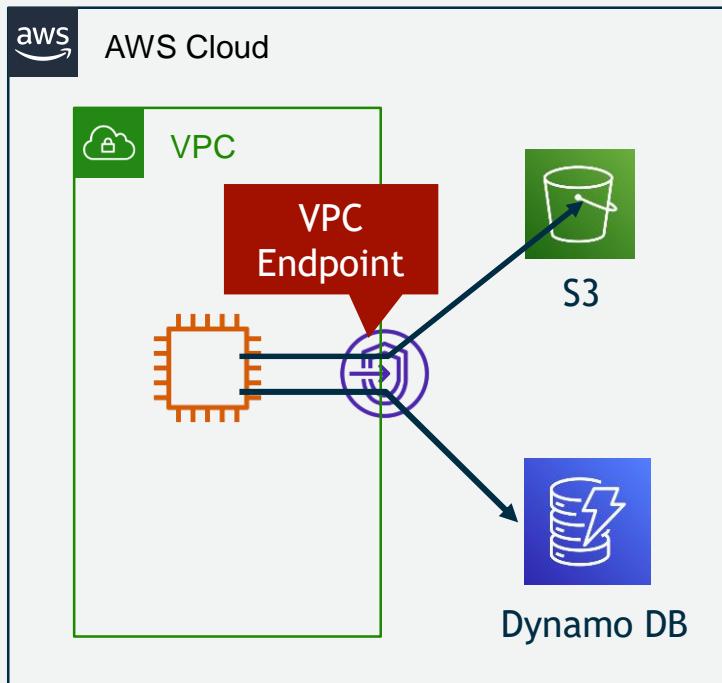
- CIDR(IPアドレス)は既存のVPC、社内のDCやオフィスと被らないアドレス帯をアサイン
プライベートアドレスで無い場合は100.64.0.0/10 CGNAT を使うのも手
- 複数のアベイラビリティゾーンを利用し、可用性の高いシステムを構築
- パブリック/プライベートサブネットへのリソースの配置を慎重に検討
- 適切なセキュリティ対策を適用する
- システムの境界を明らかにし、VPCをどのように分割するか将来を見据えてしっかりと検討する

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

VPC Endpoint概要

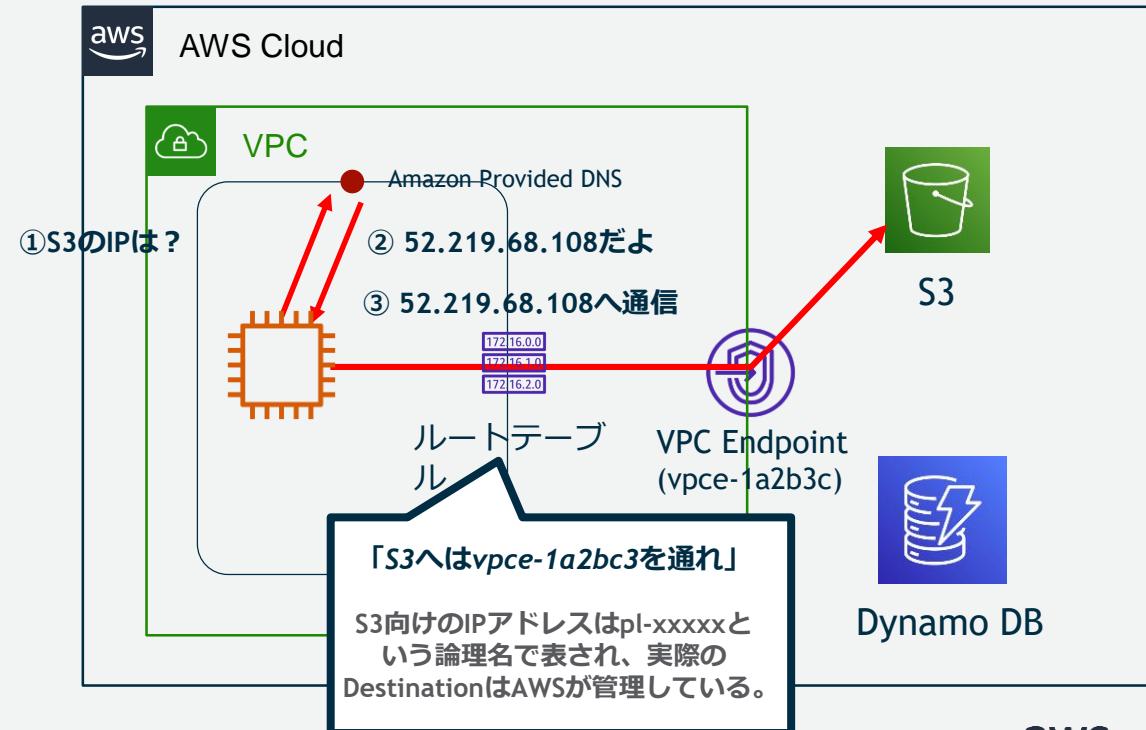


VPC Endpointは、グローバルIPをもつAWSのサービスに対して、VPC内部から直接アクセスするための出口

動作比較

Gateway型の動作

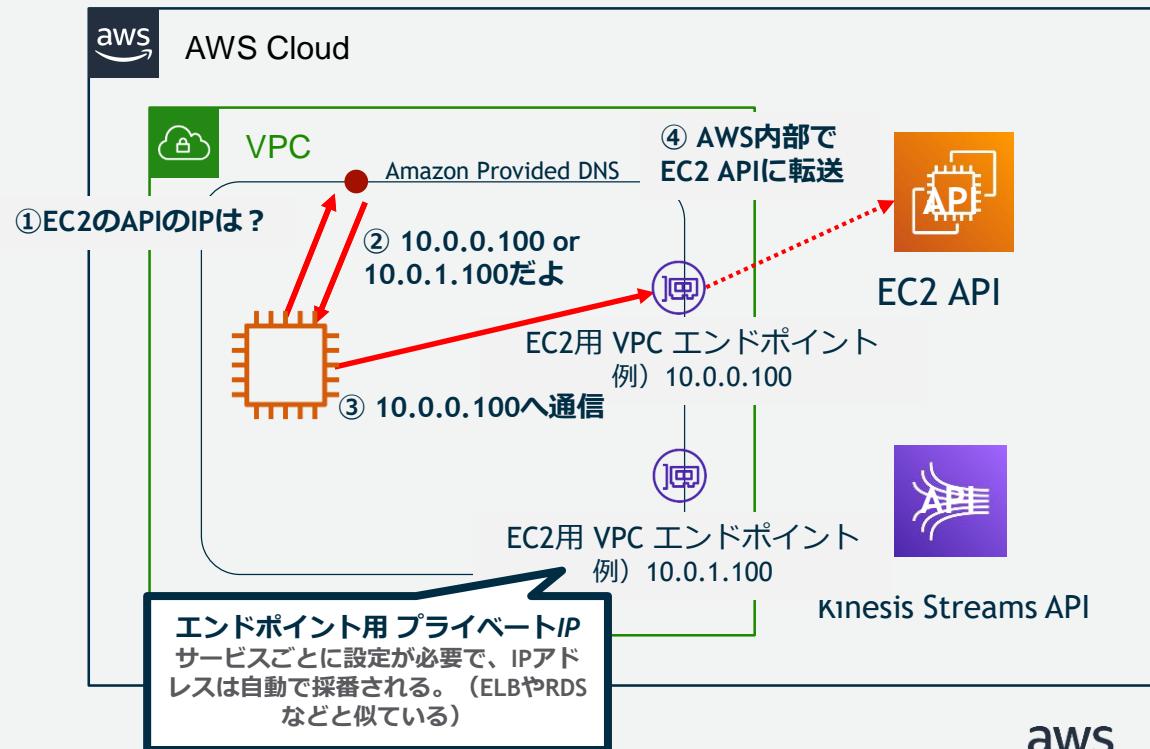
- サブネットに特殊なルーティングを設定し、VPC内部から直接サービスと通信する。
- 通信先のIPアドレスはグローバルIPアドレス



動作比較

PrivateLink (Interface型)の動作

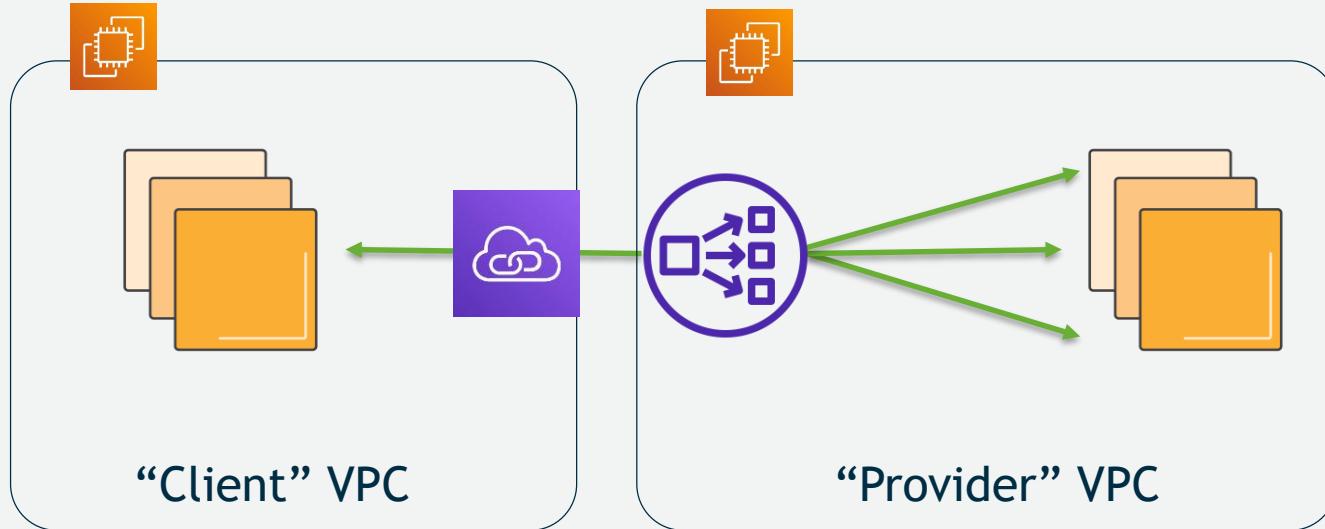
- サブネットにエンドポイント用のプライベートIPアドレスが生成される。
- VPC内部のDNSがエンドポイント向けの名前解決に対してしてプライベートIPアドレスで回答する。
- エンドポイント用プライベートIPアドレス向け通信が内部的にサービスに届けられる。



機能比較

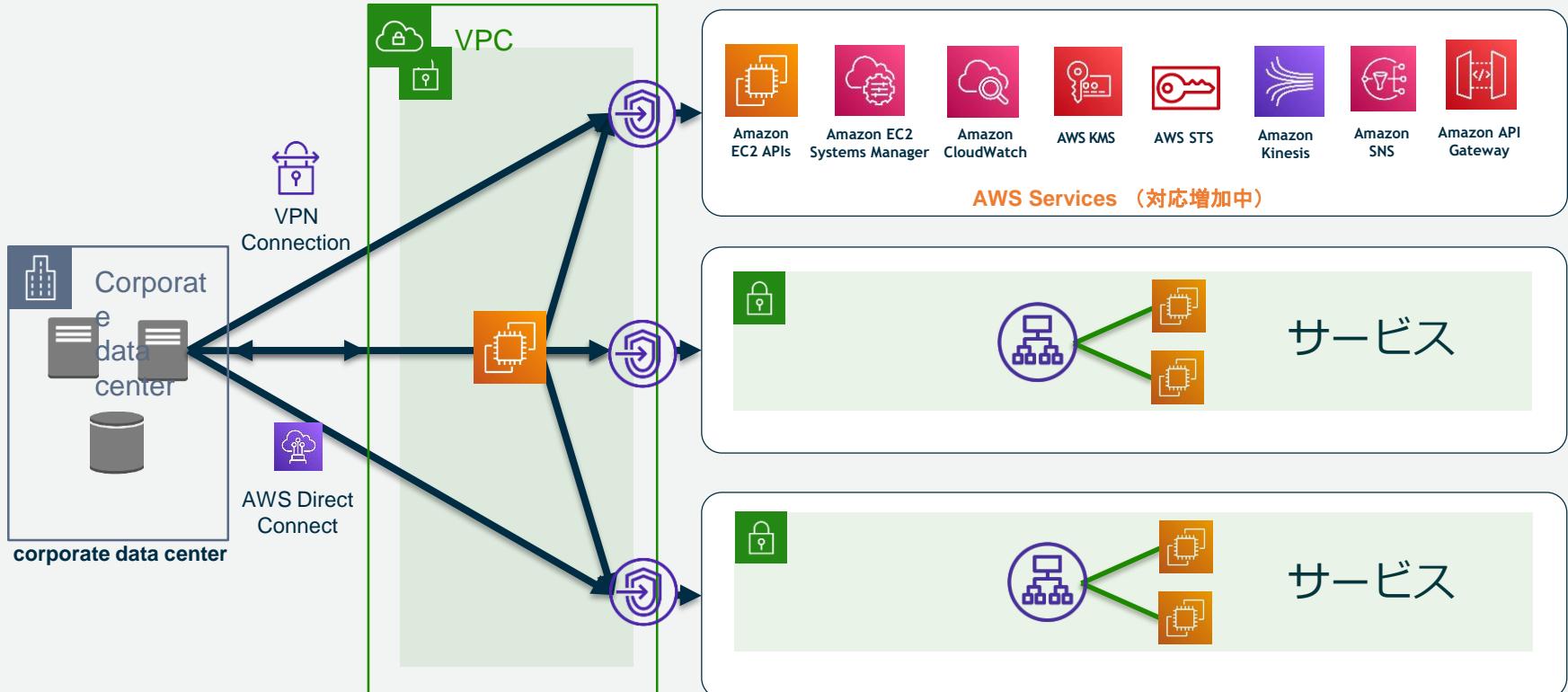
	Gateway型	PrivateLink(Interface型)
アクセス制御	エンドポイントポリシー IAM Policyと同じ構文でアクセス先のリソースを制限可能。	セキュリティグループ セキュリティグループでアクセス元IP、ポートを制御可能。対象のサービスの特定のリソースへのアクセス制御は不可。
利用料金	無料	有料 サービスごとに、1プライベートIP毎に下記の料金。 0.014 USD/時間（東京）+ 0.01 USD/ GB https://aws.amazon.com/jp/vpc/pricing/
冗長性	ユーザー側で意識する必要なし	マルチAZ設計 マルチAZで配置するように設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

PrivateLink for Customers and Partners

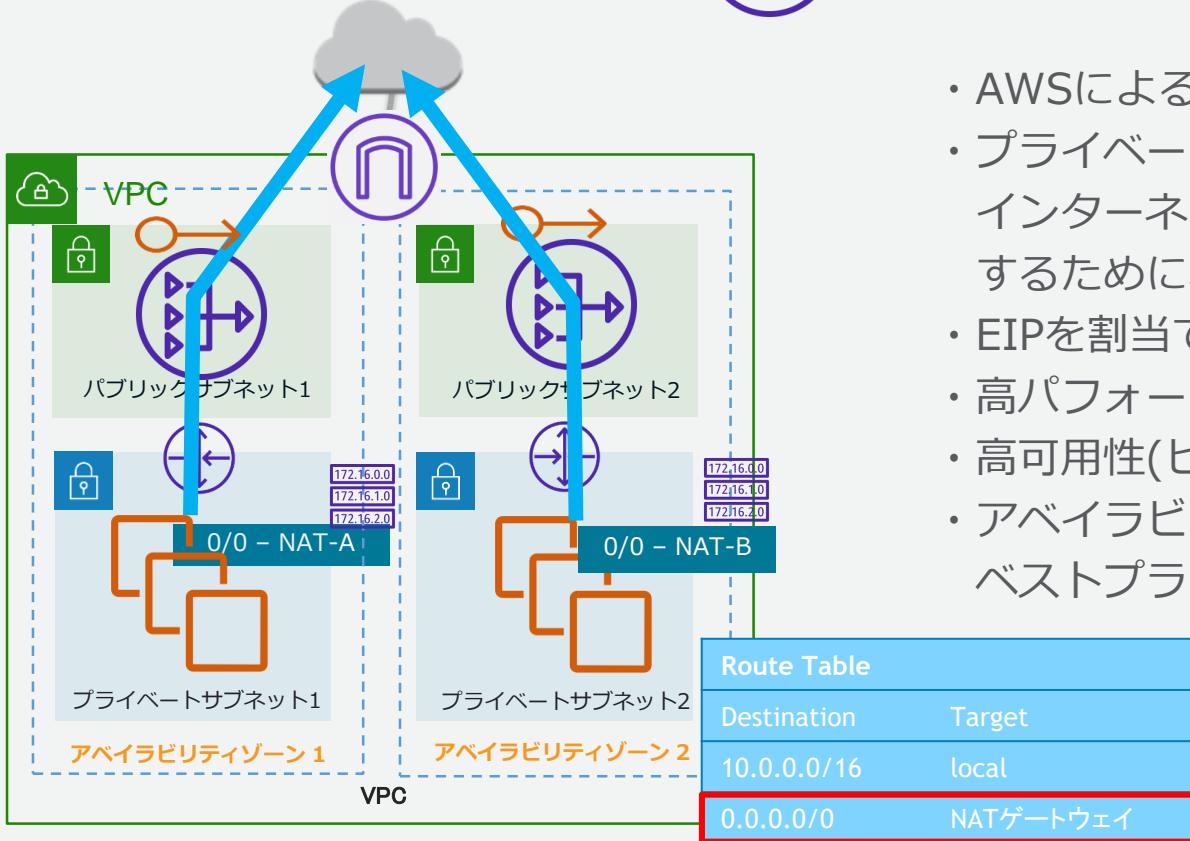


PrivateLinkはユーザが自分で作ることもできる

PrivateLinkはオンプレミスにネイティブ対応



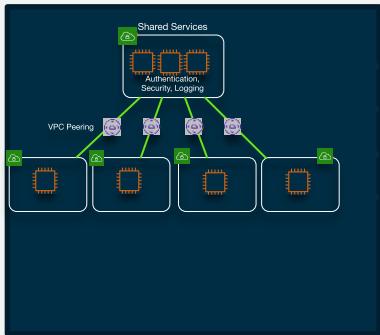
NATゲートウェイ



- ・ 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

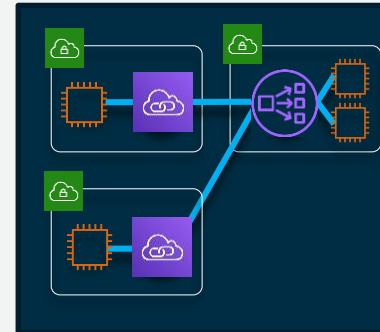
VPCの接続バリエーション

VPC peering



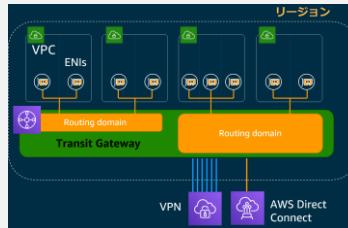
- 1 vs 1 の関係
- 100 VPCまで
- VPC間のSecurity groups
- Inter-region対応

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

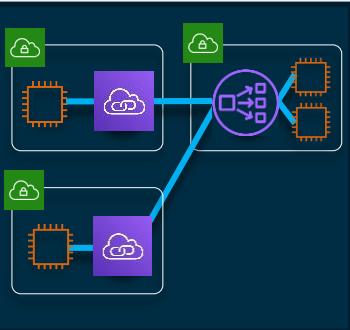
AWS Transit Gateway



- 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

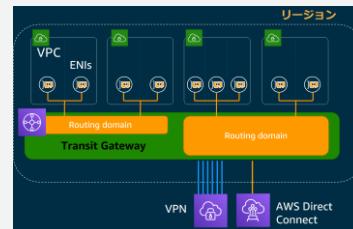
Transit Gateway と PrivateLinkはスケーラブル

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

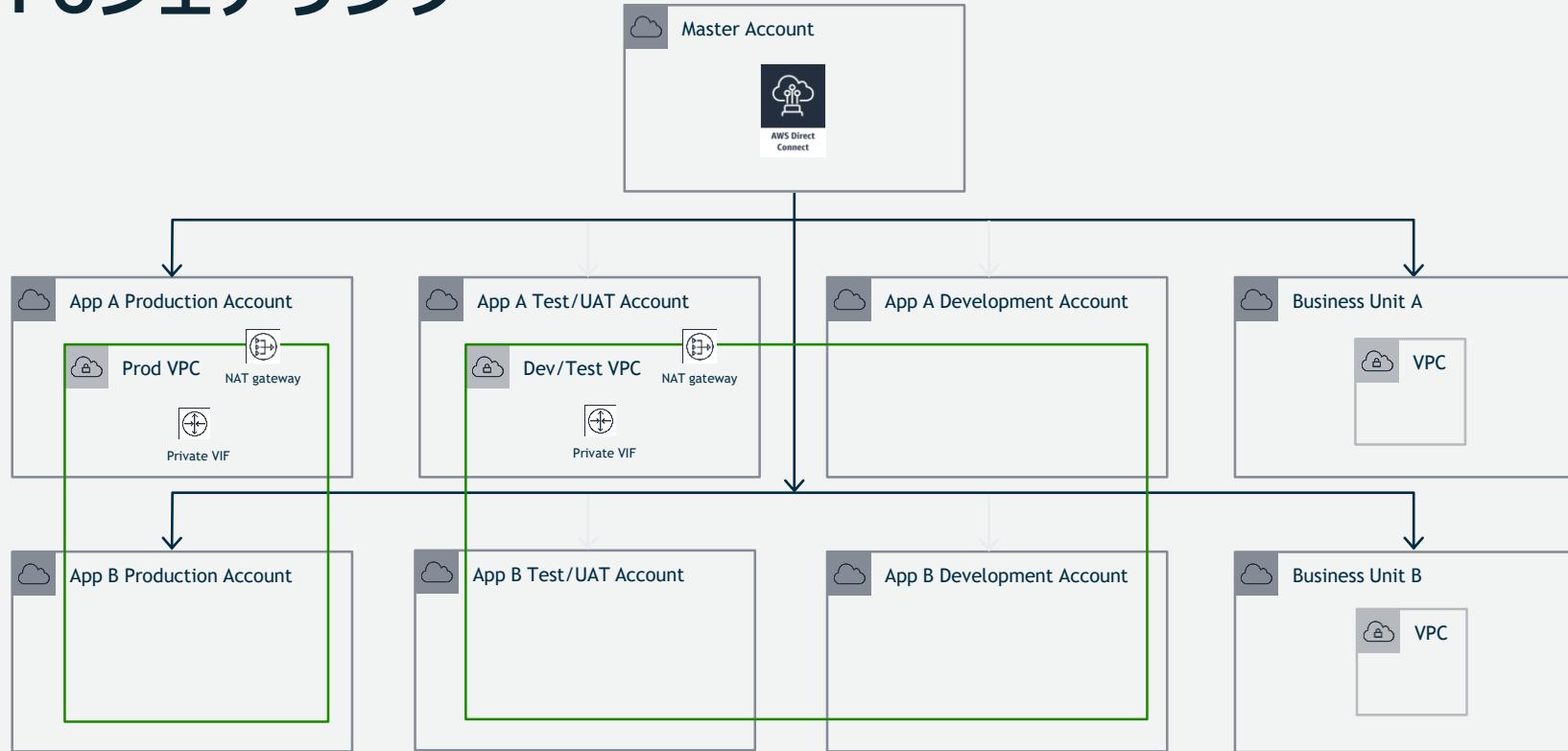
Scope: ネットワークの共用

Trust model: VPC間の信頼を集中管理

Dependencies: Transit Gateway

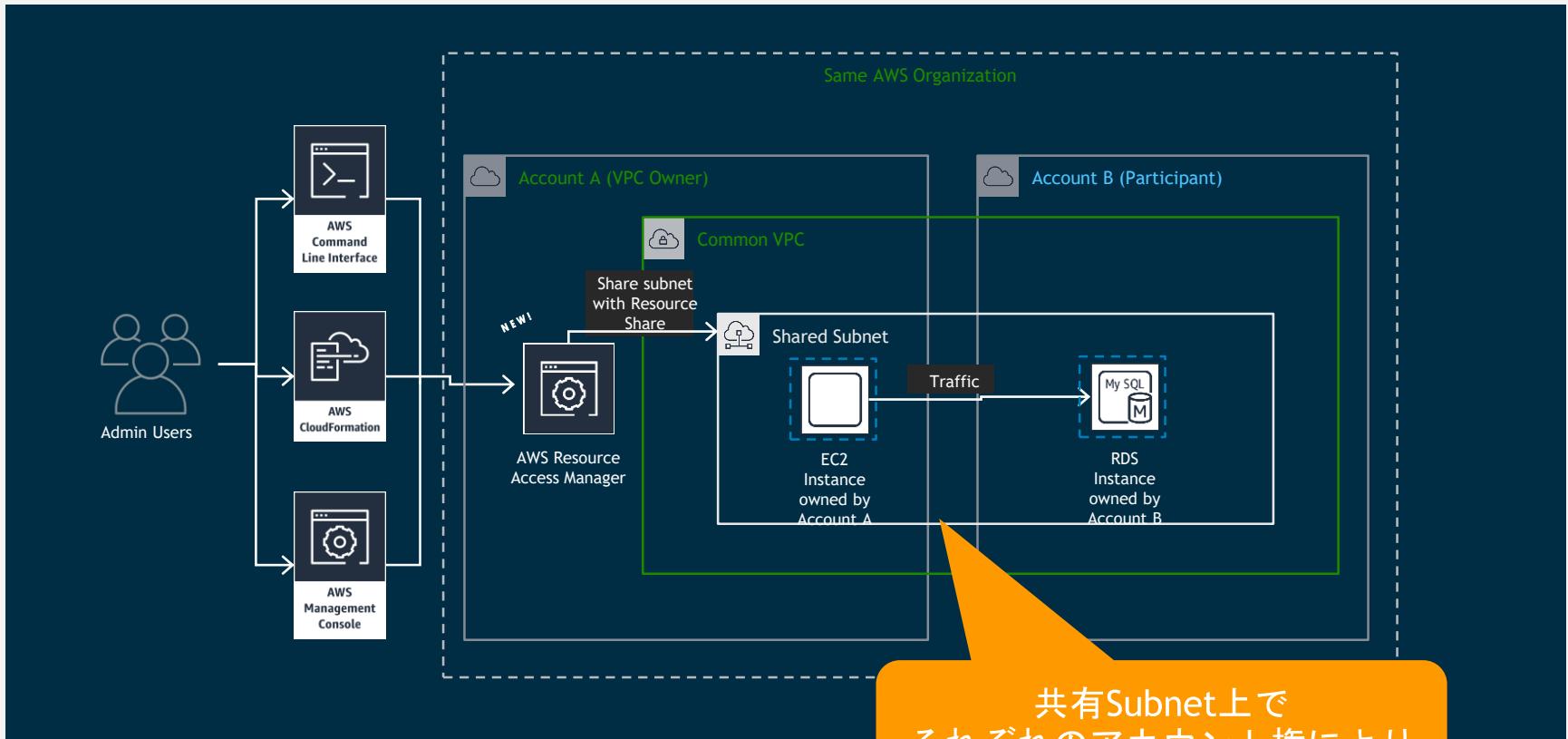
Scale: 数千のVPCに対応

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



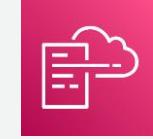
```
aws ec2 create-vpc  
--cidr-block 10.0.0.0/16
```

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

サードパーティツール



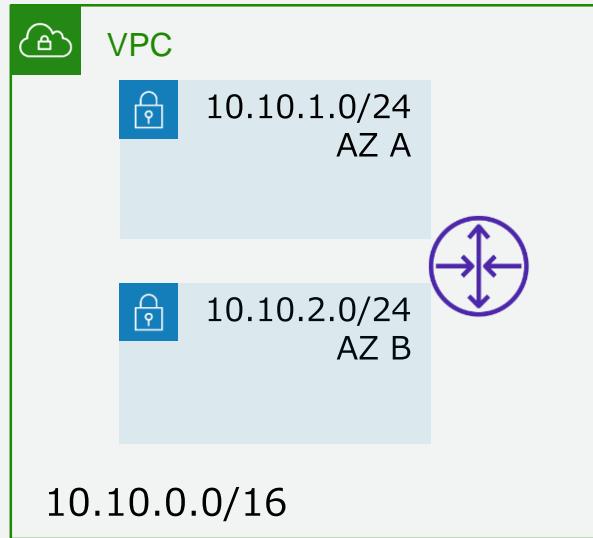
AWS CloudFormation



```
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



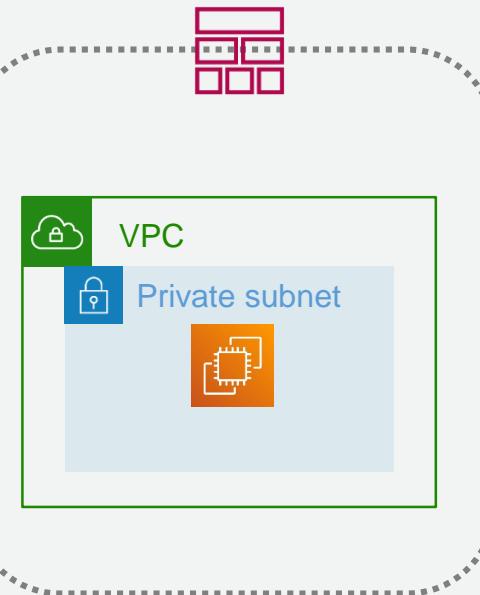
```
aws ec2 create-vpc --cidr 10.10.0.0/16
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.1.0/24 --a us-west-2a
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.2.0/24 --a us-west-2b
```

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"
      } ]
    }
  }
}
```



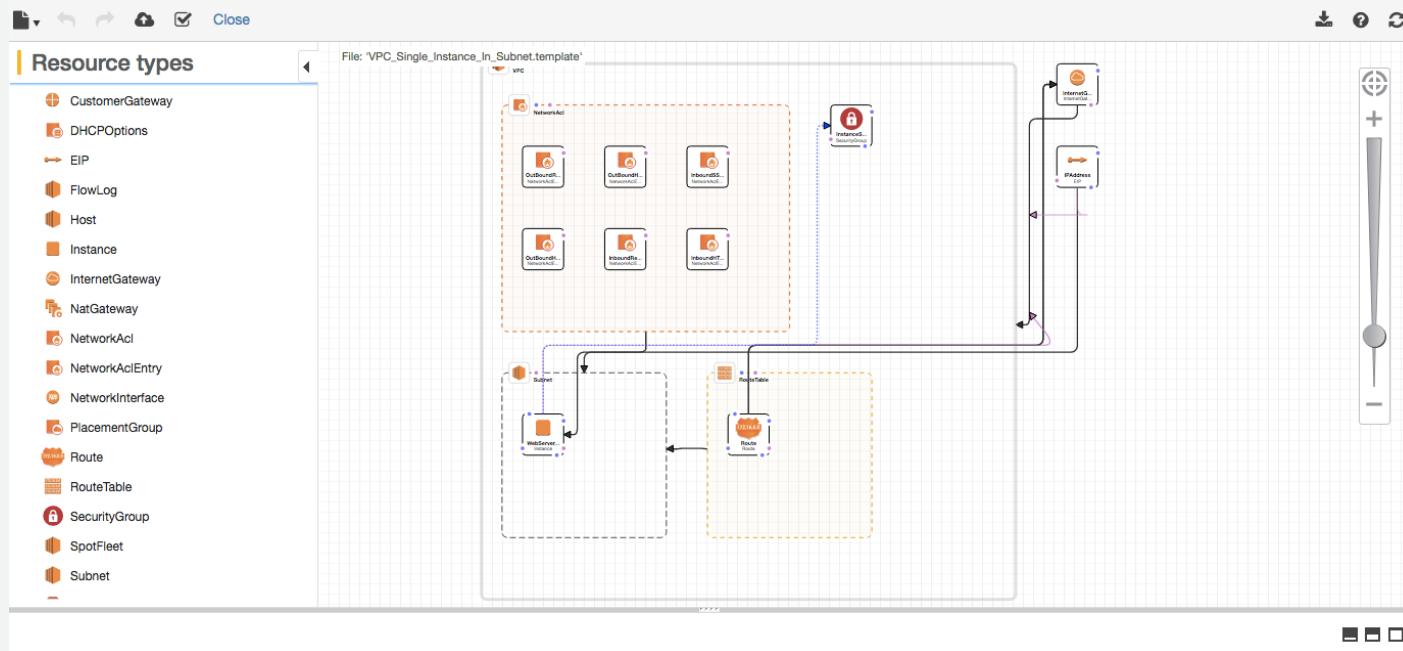
テンプレート
(JSON形式)

CloudFormation

AWS環境(スタック)が完成

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

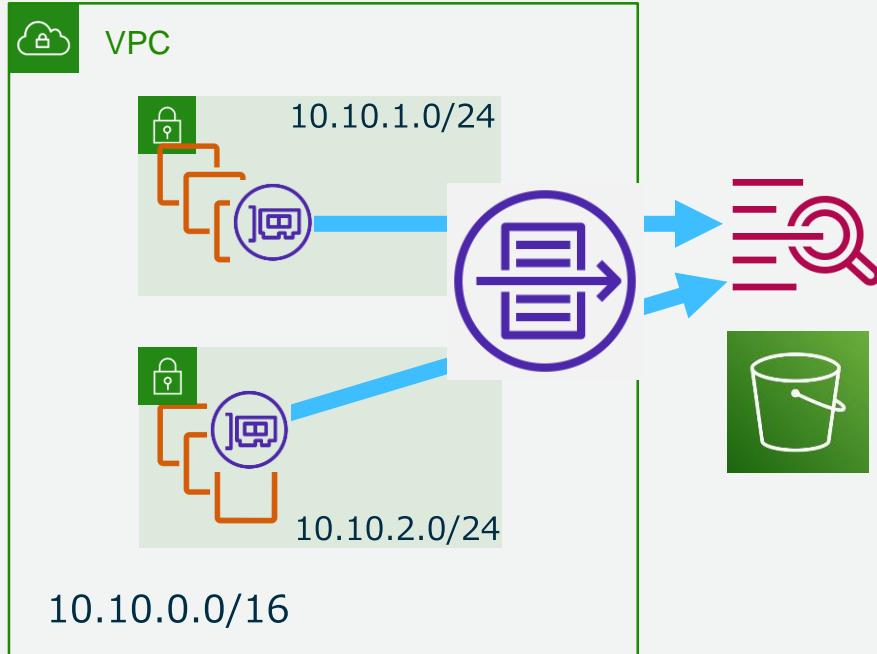
VPCの設定

VPCの運用

まとめ



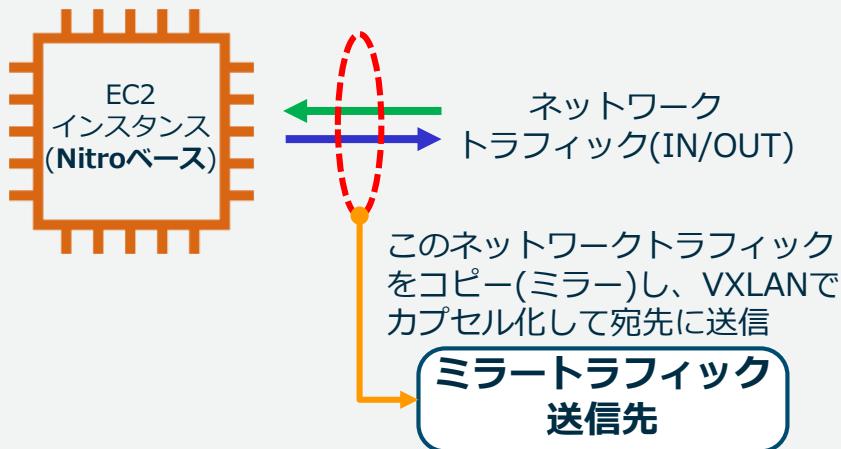
VPC Flow Logsとは



- ・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,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]

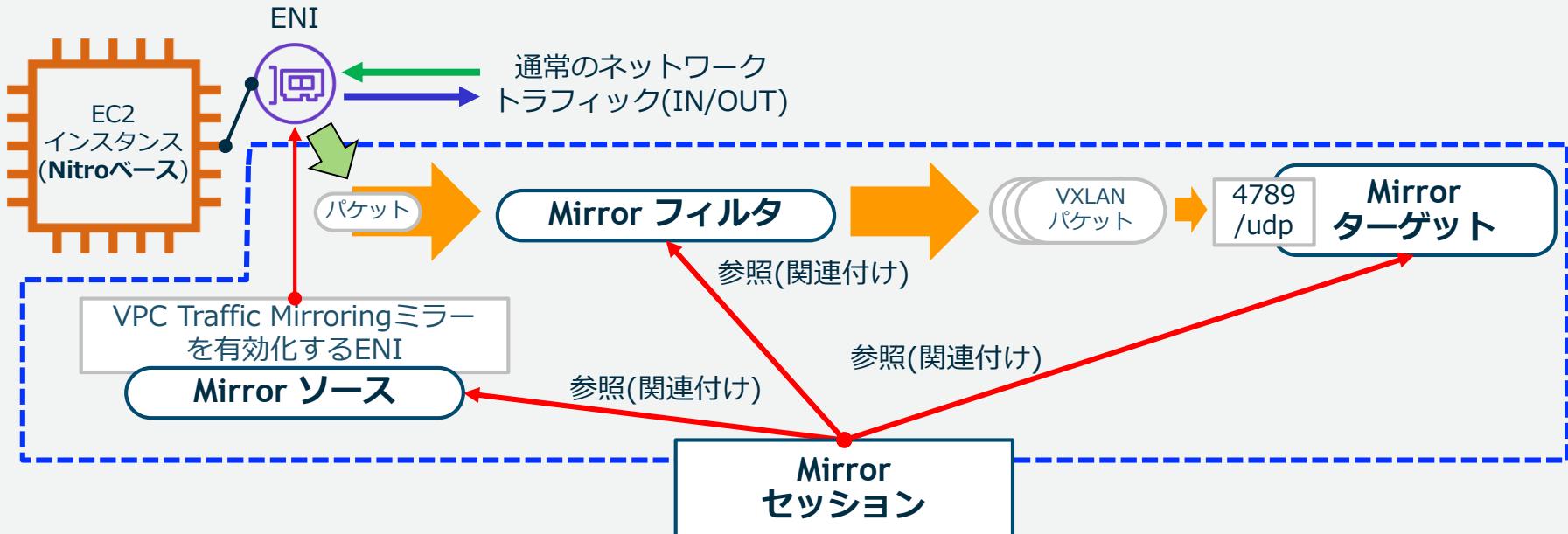
- 脅威検出(フォレンジック)
- コンテンツモニタリング
- 問題判別

- 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

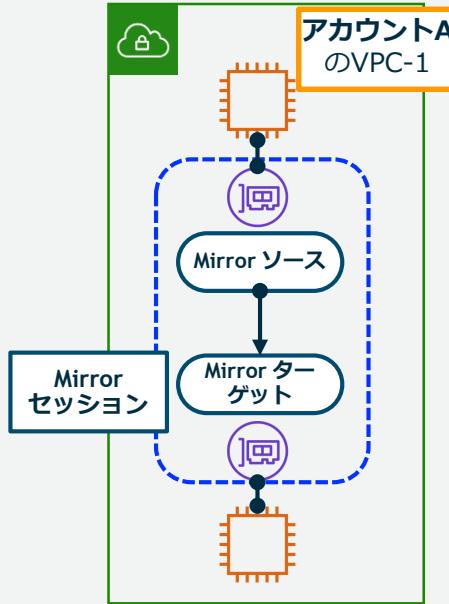


<https://aws.amazon.com/jp/about-aws/whats-new/2019/06/announcing-amazon-vpc-traffic-mirroring-for-amazon-ec2-instances/>

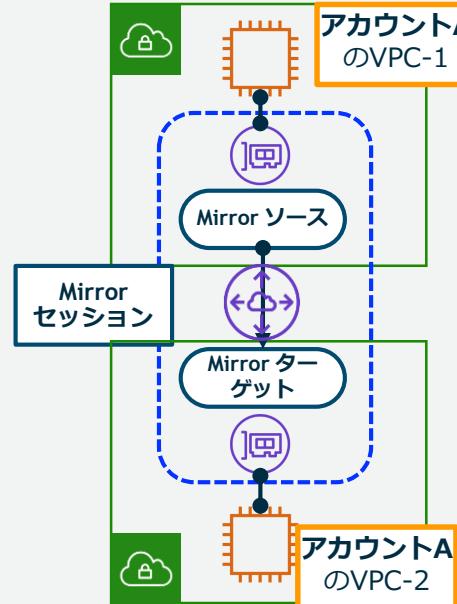
Mirror ソース/フィルタ/ターゲット/セッション

同一リージョンを前提として、下図の構成が可能

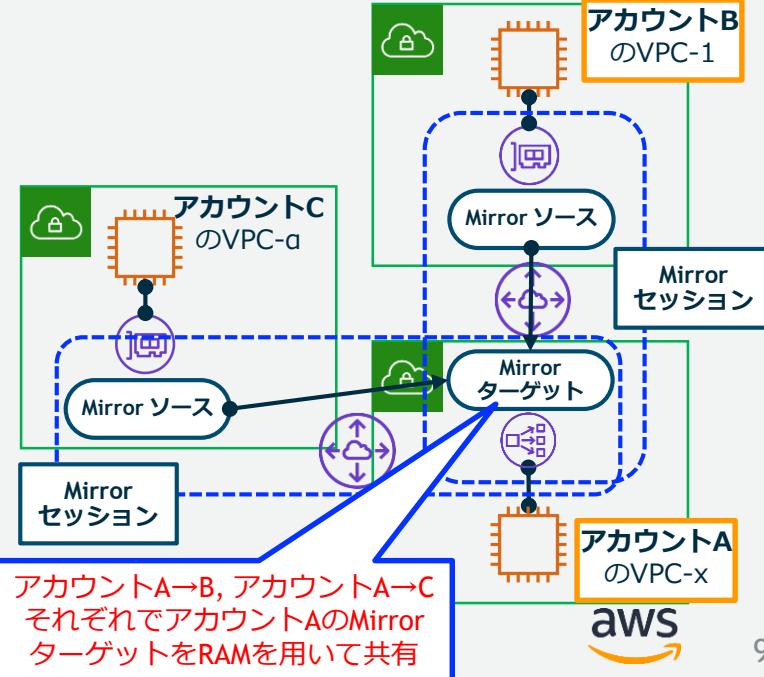
同一アカウント&同一VPC内



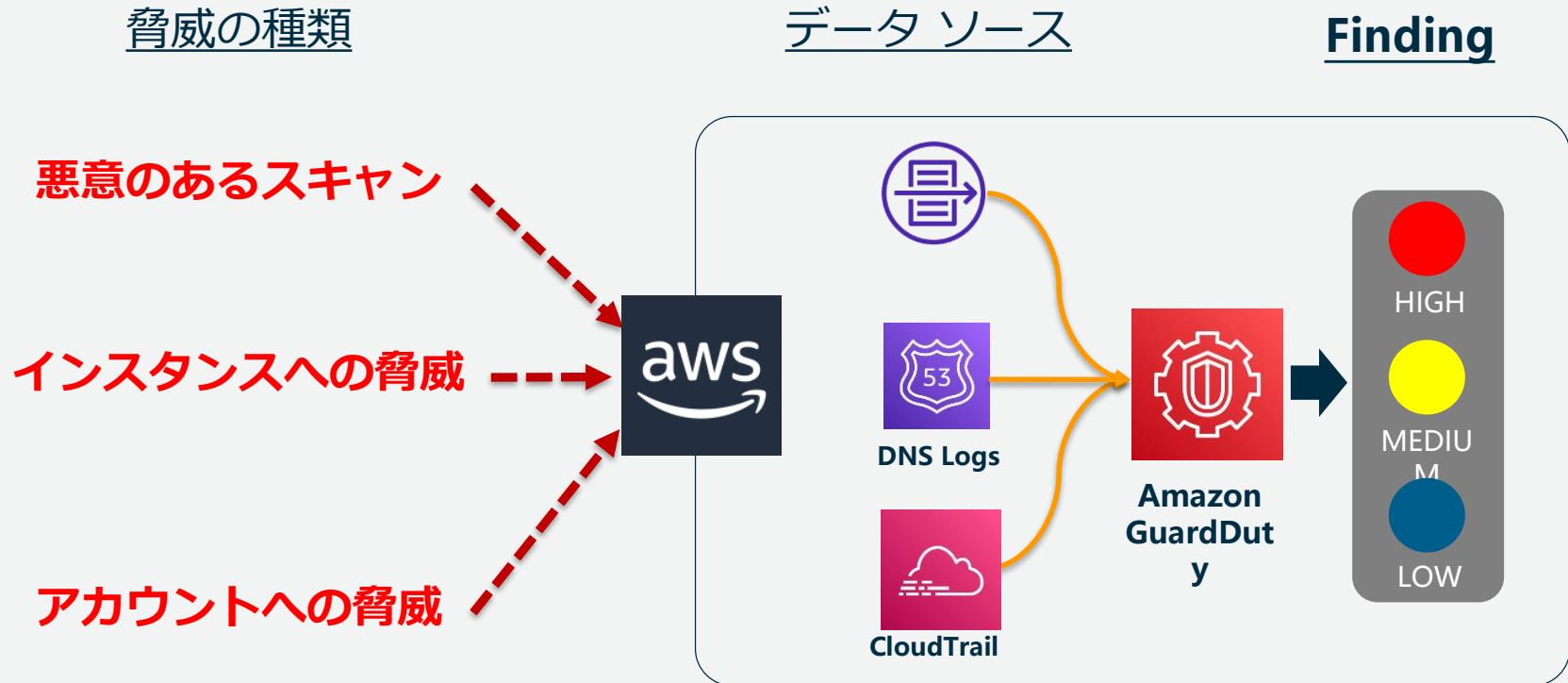
同一アカウント&異なるVPC間



異なるアカウント&異なるVPC間



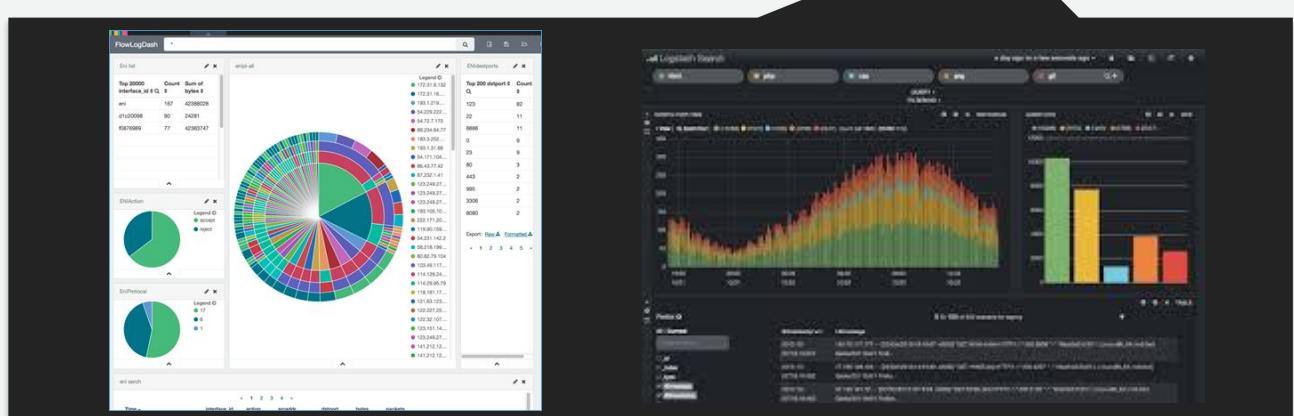
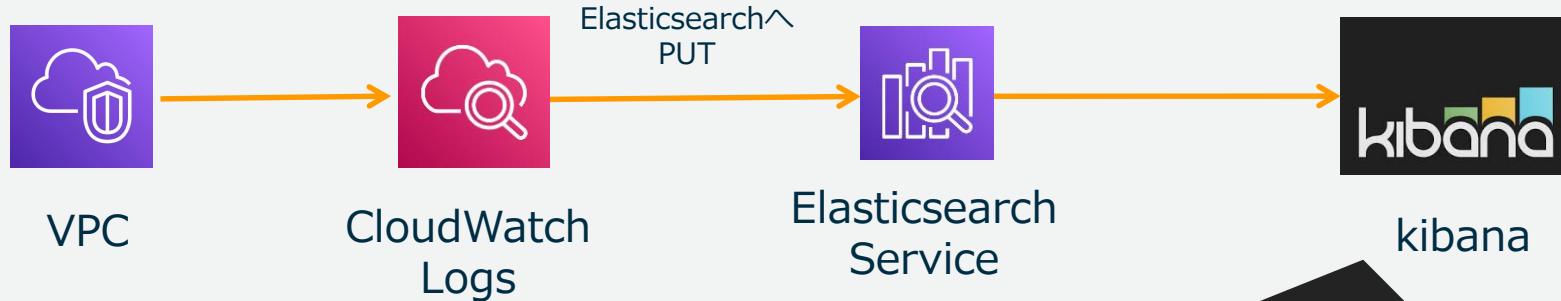
GuardDuty による脅威の検知と通知



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



Amazon VPC のクオータ関連

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



The screenshot shows the AWS Japan Language Resources page. At the top, there's a navigation bar with the AWS logo, search bar, and links for "日本担当チームへお問い合わせ", "サポート", "日本語", "アカウント", and "コンソールにサインイン". Below the navigation is a main menu with links for "製品", "ソリューション", "料金", "ドキュメント", "学習", "パートナー", "AWS Marketplace", "その他", and a search icon. The main content area features a large title "AWS クラウドサービス活用資料集トップ" and a descriptive paragraph about the service. At the bottom, there are four buttons: "AWS Webinar お申込", "AWS 初心者向け", "業種・ソリューション別資料", and "サービス別資料".

AWS クラウドサービス活用資料集トップ

Amazon Web Services (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

AWS Webinar お申込 »

AWS 初心者向け »

業種・ソリューション別資料 »

サービス別資料 »

<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>





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

Amazon VPC IP Address Manager(IPAM)

AWS Black Belt Online Seminar

安藤 慎太郎

Solutions Architect

Archived



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け、Amazon ウェブ サービス ジャパン 合同会社が主催するオンラインセミナーシリーズです
- AWS の技術担当者が、AWS の各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

- 本資料では **2022 年 4 月**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

安藤 慎太郎

役職

Solutions Architect

好きな AWS サービス



AWS Direct Connect



Amazon Transcribe など

本セッションの対象者

- re:Invent 2021 で発表された
Amazon VPC IP Address Manager (IPAM) に興味をお持ちの方
 - **AWS 上での IP アドレス管理の良い方法**を知りたい方
-
- Amazon Virtual Private Cloud (VPC) の基礎については、
事前に別途セミナーのご視聴をおすすめいたします。
 - 【AWS Black Belt Online Seminar】Amazon VPC
https://www.youtube.com/watch?v=JAzsGRS_o4c

本セッションのゴール

以下を理解し、Amazon VPC IP Address Manager (IPAM)
の要点を押さえていただくこと

- Amazon VPC IP Address Manager (IPAM) の概要
- IPAM のメリット (IPAM が解決するこれまでの課題)
- IPAM の主要コンポーネント・機能と、活用方法

本セッションの流れ

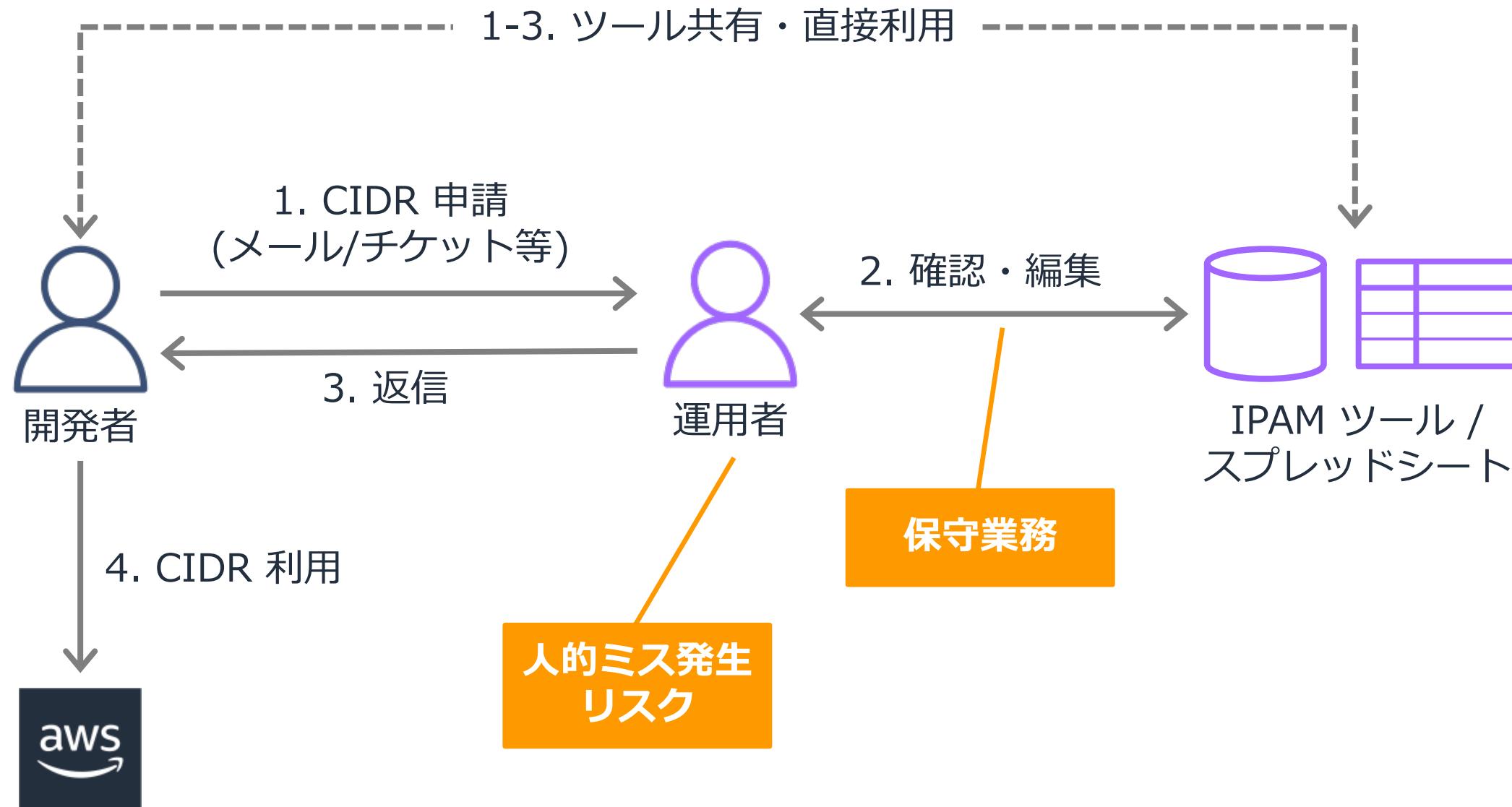
- サービス登場の背景 – IPAM 登場以前の課題
- サービス概要
- サービス導入方法・使い方
 - A. 新規環境への導入
 - B. 既存環境への導入
- クオータ・料金
- まとめ

本セッションの流れ

- サービス登場の背景 – IPAM 登場以前の課題
- サービス概要
- サービス導入方法・使い方
 - A. 新規環境への導入
 - B. 既存環境への導入
- クオータ・料金
- まとめ

課題 1. IP アドレス割り振りの手動管理の手間・リスク

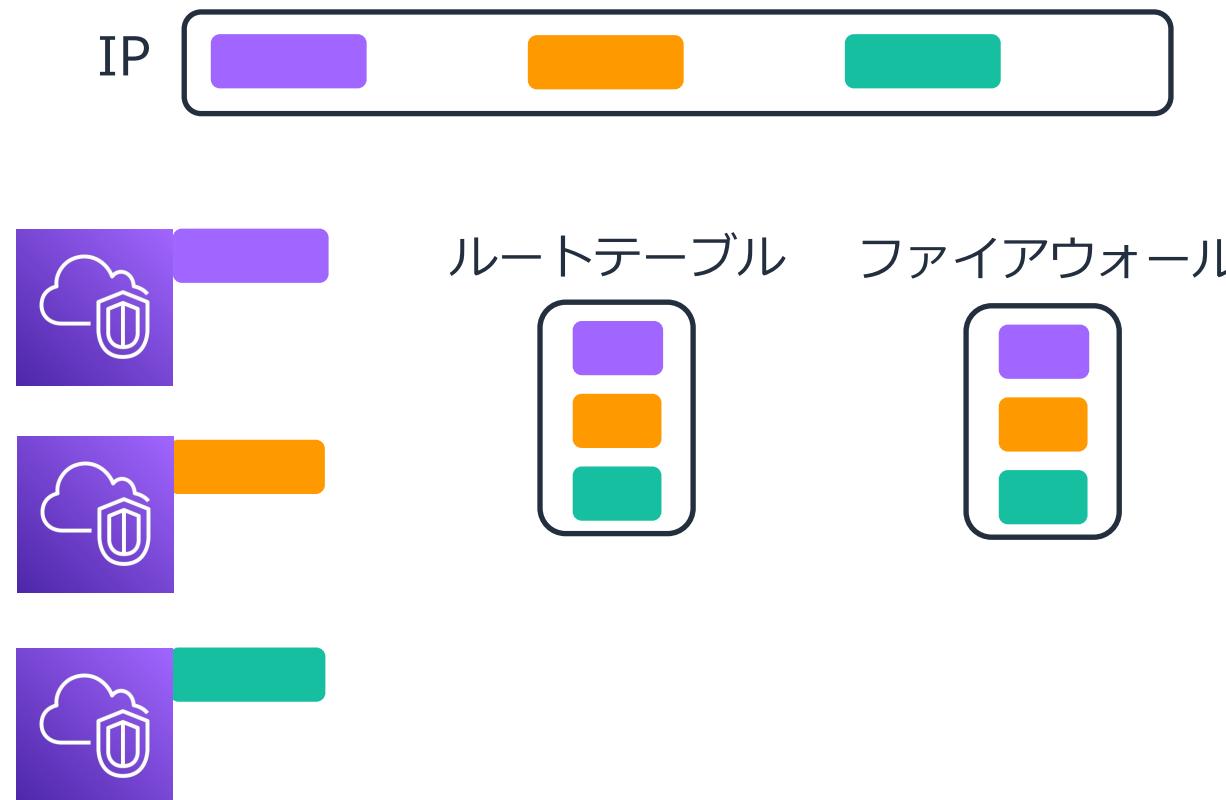
運用者の負担大、管理コストがかかる、人的ミス発生のリスクあり



課題 2. ルーティング・セキュリティ要件の管理

システムの拡大 → IP アドレス空間が分割 → 管理が煩雑に

管理・設計不足の IP アドレス空間



ルーティング・セキュリティ要件の管理が**煩雑**

理想的な IP アドレス空間



ルーティング・セキュリティ要件の管理が**容易**

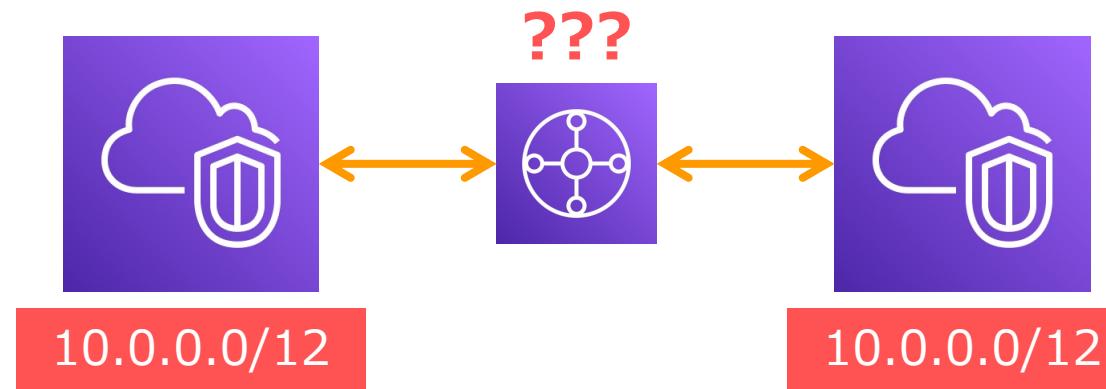
課題 3. IP アドレスのモニタリングが困難

VPC、リージョン、アカウントを跨いでモニタリング、不測の事態を回避したい

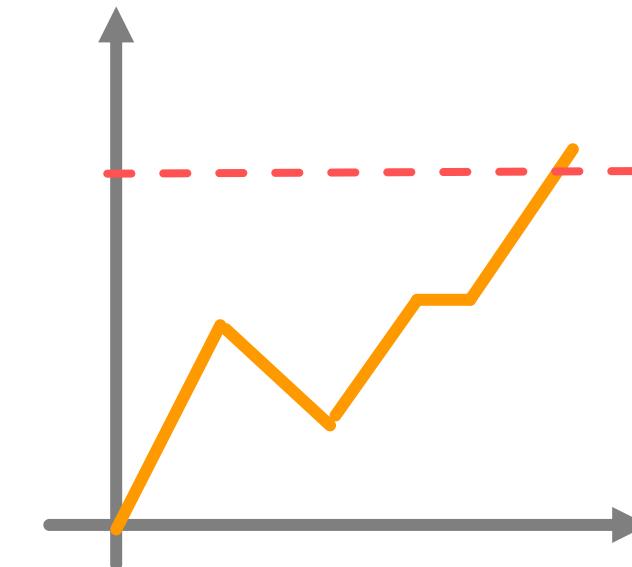
重複した CIDR が放置される可能性



VPC 間の接続を試みて、はじめて問題が発覚



IP アドレス不足の検知が困難



VPC の IP アドレスが枯渇する前に
CIDR を追加できるよう、事前にアラートが必要

課題 4. IP アドレスに関するトラブルシュートが困難

IP アドレスに関するトラブルシュート・時間を遡った分析を実施したい

トラブルシュート



ネットワークの接続で問題が発生したとき・・・

そもそも IP アドレスの利用は適切だったのか？

監査



ルーティングのセキュリティ・コンプライアンス

特定の IP アドレスがアプリケーションで使われているのか？

特定の IP アドレスがいつ、どのように割り振られていたか？

課題 5. BYOIP したアドレスの複数アカウントでの利用不可

AWS の仕様上、BYOIP した IP アドレスは単独アカウント利用のみだった

- BYOIP = Bring Your Own IP
 - お客様が所有されているパブリック IP アドレスを、AWS 上で利用すること
 - 以下などの地域インターネットレジストリに対応
 - American Registry for Internet Numbers (ARIN)
 - Réseaux IP Européens Network Coordination Centre (RIPE)
 - Asia-Pacific Network Information Centre (APNIC)
 - 参照：https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-byoip.html
 - 2022/4 月現在、JPNIC から取得した IP アドレスには非対応

IPAM 登場以前の IP アドレス管理の課題まとめ

以下の課題を解決するサービスこそが **Amazon VPC IPAM**

1. **IP アドレス割り振りの手動管理**による手間、人的ミス発生のリスク
2. ネットワーク規模拡大に伴う**ルーティング・セキュリティ要件の管理の煩雑化**
3. **CIDR 重複や IP アドレスの枯渇**をモニタリングできない
4. **IP アドレスに関するトラブルシュート**が困難
5. BYOIP したアドレスが単独アカウントでしか使えない

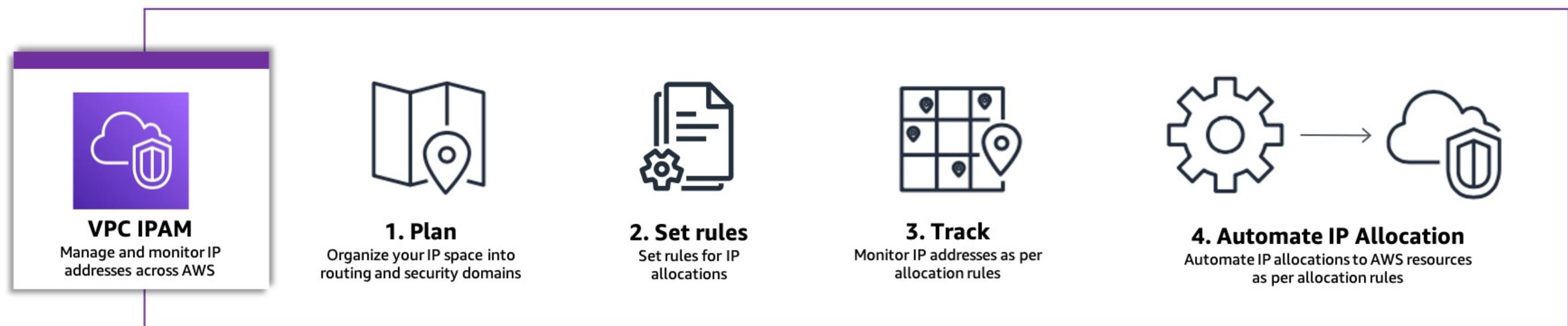
本セッションの流れ（再掲）

- サービス登場の背景 – IPAM 登場以前の課題
- サービス概要
- サービス導入方法・使い方
 - A. 新規環境への導入
 - B. 既存環境への導入
- クオータ・料金
- まとめ

Amazon VPC IP Address Manager (IPAM) とは

VPC 上の IP アドレスを整理し、割り当て状態を管理

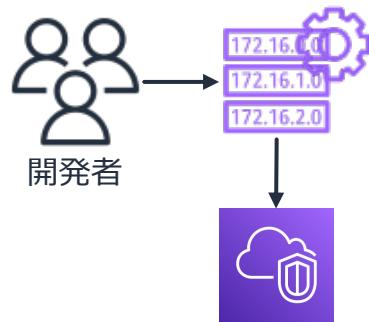
- 大規模ネットワークにおいて、**CIDR を自動的に割り振り**
 - スプレッドシート等によるマニュアル管理が不要になり、アドレス割り当て業務の手間やミスを回避
- **IP アドレス利用のモニタリング、過去に遡った分析、監査**にも対応
- AWS Organizations や AWS Resource Access Manager との連携も可能
- 料金はアクティブな IP アドレス分だけの**従量課金**



IPAM の機能

大きく分けると機能は以下の 3 つ

CIDR 割り振りの自動化



開発者が IPAM を直接利用するだけで
事前に設定したビジネスルールに基づき
CIDR が割り当てられる。

社内チケットやメールによる
CIDR 管理が不要に。

※単一 IP ではなく、VPC に割り当てる
CIDR 単位での管理

モニタリング



IP アドレス利用のトラッキング。
利用率のモニタリングや、
重複する CIDR によるアラート通知
が可能。

監査



最大で 3 年間データを保持。
監査やコンプライアンスチェック
に活用可能。

IPAM の導入方法

IPAM は新規・既存からの移行の両方で活用可能

- A. 新規環境への導入 (Greenfield Deployment)
- B. 既存環境への導入 (Brownfield Deployment)

本セッションの流れ（再掲）

- サービス登場の背景 – IPAM 登場以前の課題
- サービス概要
- サービス導入方法・使い方
 - **A. 新規環境への導入**
 - **B. 既存環境への導入**
- クオータ・料金
- まとめ

IPAM のセットアップ

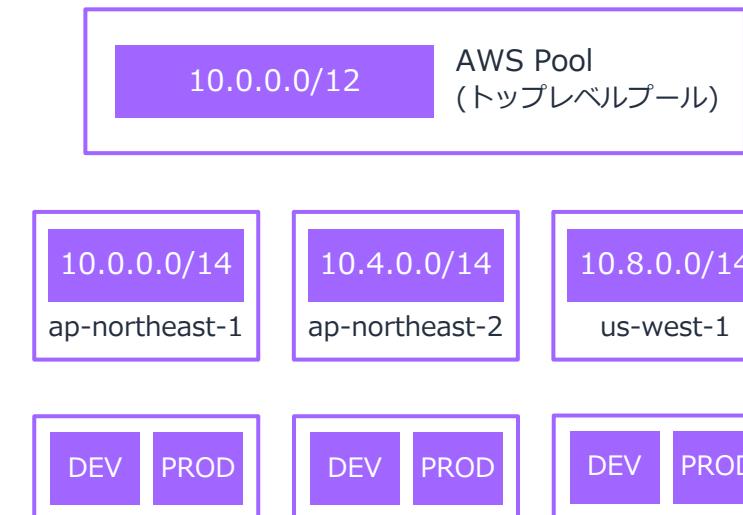
3 ステップで構築します

1 | IPAM の作成



単独の IPAM で
複数リージョン・アカウント管理

2 | IP アドレス空間の設計



ルーティングやセキュリティの要件に従って
ネットワークを設計

3 | 割り振りルール設定

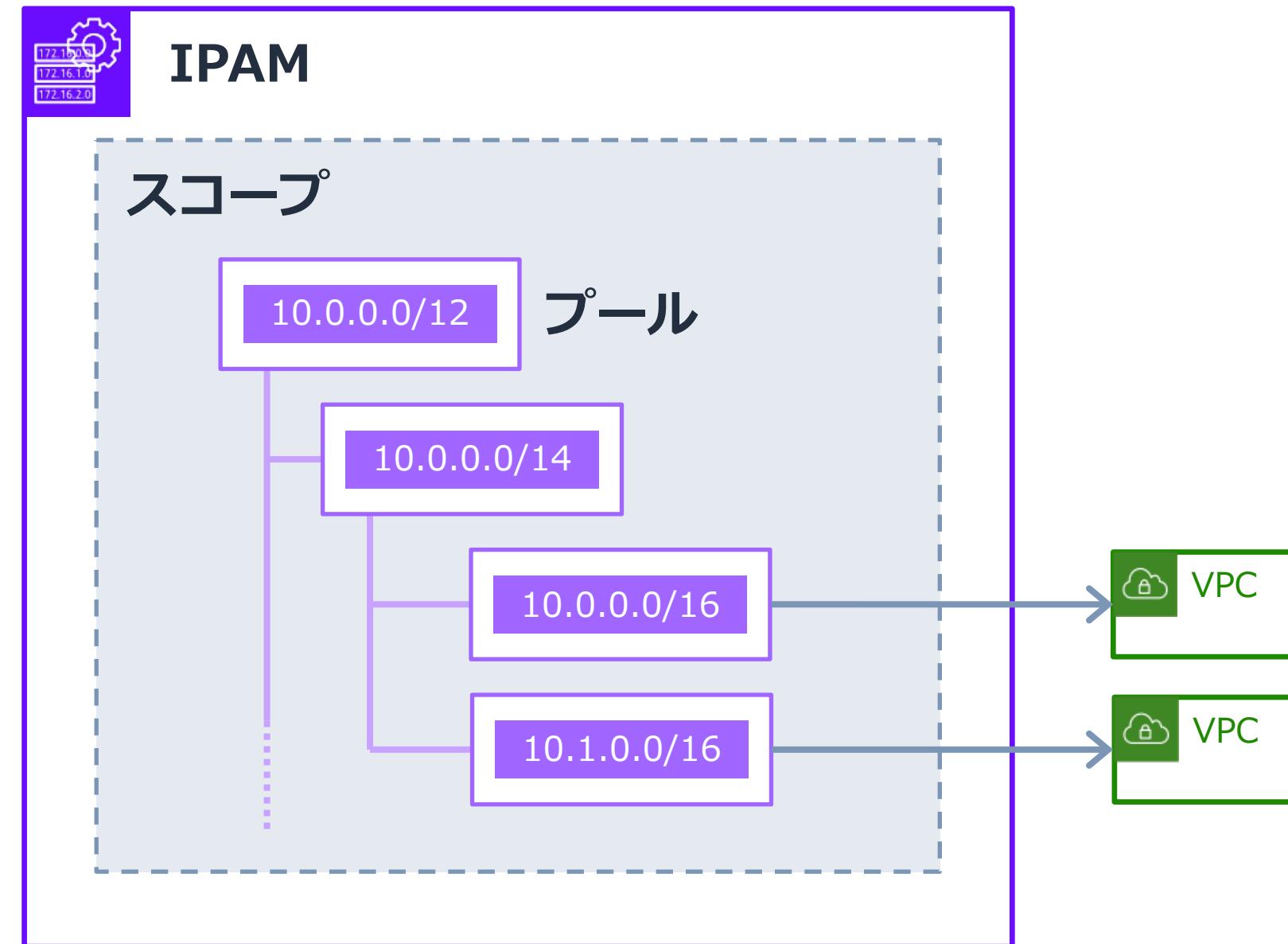


特定の CIDR を使えるアカウントや、
リージョンを制限

プールの作成・編集時に指定

IPAM の基本概念

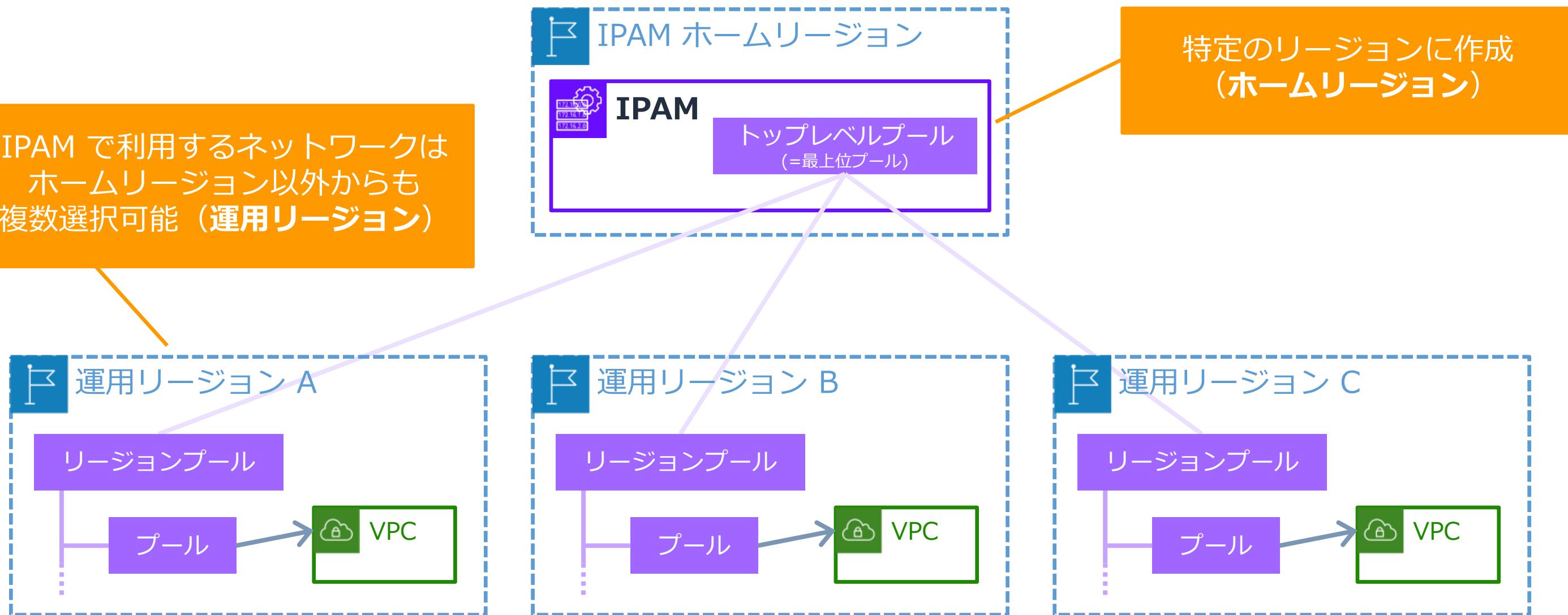
階層構造にある「IPAM」 「スコープ」 「プール」 の 3 つが重要



IPAM の基本概念 | IPAM

組織やアカウントに対応する、IP アドレス管理の単位

IPAM で利用するネットワークは
ホームリージョン以外からも
複数選択可能（運用リージョン）



ホームリージョンと可用性についての関連については本資料末尾の補足 p.58-p.60 をご参照ください

IPAM の基本概念 | スコープ

IPAM の中に作成するもので、IPAM 内での最上位概念

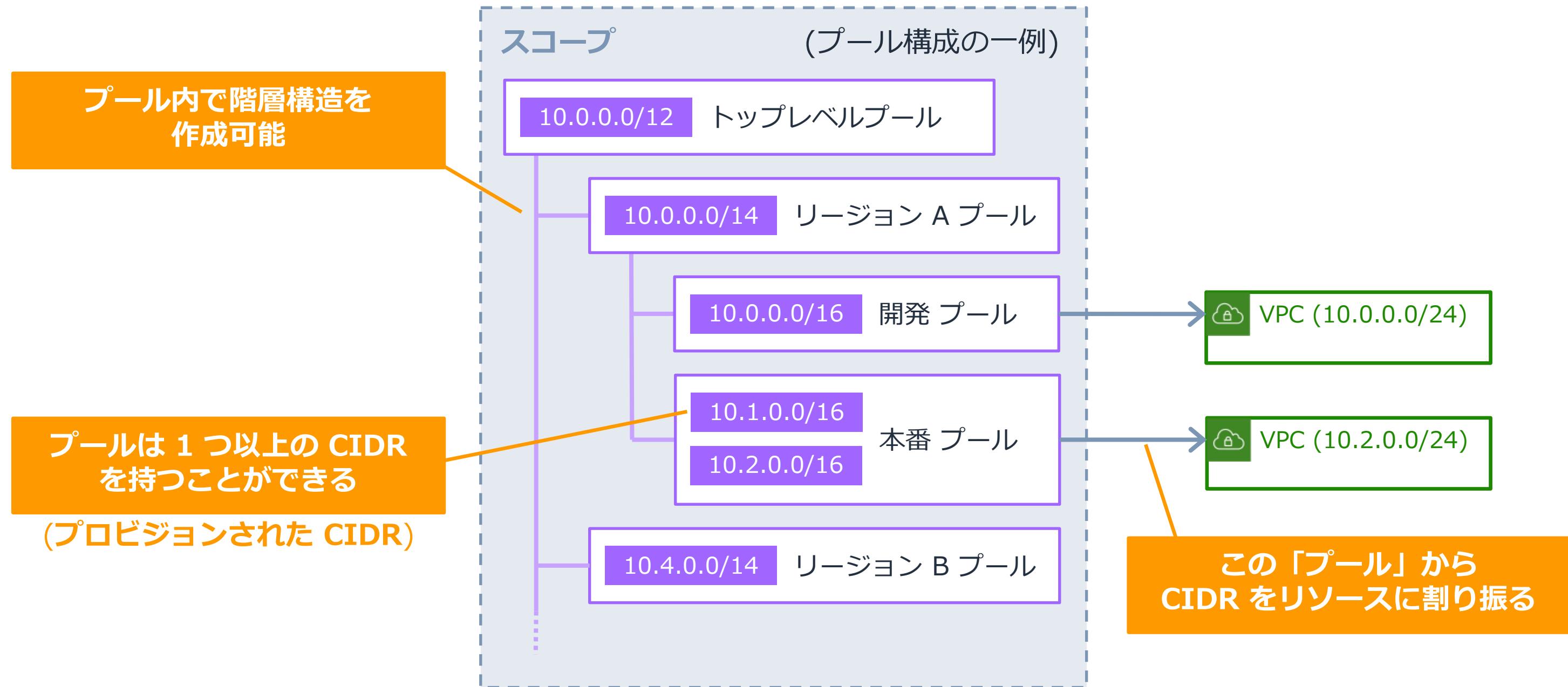
- パブリックスコープ・プライベートスコープの 2 種類が存在
- IPAM 作成時に、1 つずつデフォルトで作成される

基本的にこちらを利用

	パブリックスコープ	プライベートスコープ
IPAM でのデフォルト数	1	1
IPAM への追加作成	不可	可 (デフォルトのクォータで最大 5 個, 調整可) →接続されないプライベートスコープの ネットワーク間で CIDR の重複が可能
用途	BYOIP	プライベートネットワーク

IPAM の基本概念 | プール

スコープの中に作成するもので、連続する IP アドレス範囲 (CIDR) の集合



IPAM の基本概念 | プール - 用語の補足

プールに関する用語「プロビジョン」「割り振り」の違いに注意

プロビジョン (Provision)

プールの詳細	モニタリング	CIDR	割り振り	リソース	コンプライアンス	リソース共有	タグ
CIDR (1) 情報							
<input type="button" value="CIDR のプロビジョンを解除"/>	<input type="button" value="CIDR をプロビジョン"/>	< 1 >	①				
<input type="text"/> 結果をフィルタリング							

CIDR (1) 情報

CIDR	状態
10.1.0.0/16	プロビジョン済み

プールに CIDR を追加 (準備) すること
プロビジョンされた CIDR のみプールから利用可能になる

設定方法 (マネジメントコンソールの場合)

- ・プール作成時：「プロビジョンする CIDR」
- ・プール作成後：プールの詳細画面「CIDR」タブ

割り振り/割り当て (Allocation)

プールの詳細	モニタリング	CIDR	割り振り	リソース	コンプライアンス	リソース共有	タグ
割り振り (2) 情報							
<input type="button" value="Ignore and release CIDRs"/>	<input type="button" value="CIDR の割り振りを解除"/>	< 1 >	②				
<input type="text"/> 結果をフィルタリング							
CIDR	割り振り ID	リソースの...	説明	リソース ID	リソースのリージョン	所	
10.1.0.0/24	ipam-pool-all...	vpc	-	vpc-0020880...	ap-northeast-3	20	
10.1.1.0/24	ipam-pool-all...	vpc	-	vpc-05f69d1...	ap-northeast-3	20	

プールにプロビジョンされた CIDR (の一部)を
VPC などのリソースに実際に割り振ること

設定方法 (マネジメントコンソールの場合)

- ・VPC 作成：CIDR として IPAM プールを指定
- ・VPC 以外：プールの詳細画面「割り振り」タブ

IPAM の作成や設定を行う手段は以下の 4 通り

- AWS マネジメントコンソール
- AWS CLI
- AWS SDK
- クエリ API
 - 直接 IPAM にアクセスして様々な操作が可能だが、アプリケーション側でリクエストする際に署名用ハッシュ計算やエラーハンドリングが必要。
 - <https://docs.aws.amazon.com/AWSEC2/latest/APIReference/>

単独アカウント/複数アカウントによって事前に必要な設定が異なる

- **単独アカウント**

- AWS Identity and Access Management (IAM) でサービスにリンクされたロールの手動作成が必要
 - https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/using-service-linked-roles.html#create-service-linked-role

- **複数アカウント (AWS Organizations と統合)**

- 組織内のアカウントに IPAM の管理者を委任する必要がある
 - これにより、サービスにリンクされたロールが、組織内の全てのアカウントで自動的に作成される
 - IPAM 関連の操作は、管理者となった IPAM 管理アカウントから実施
- 組織内でのプール共有や、組織内の IP アドレスの使用状況を俯瞰したモニタリングが可能

IPAM 作成 | 設定項目

IPAM 作成

IP 空間設計

割り振りルール設定

Amazon VPC IP Address Manager > IPAMs > 作成

IPAM を作成 情報

データレプリケーションを許可 情報

Amazon VPC IP Address Manager には、ソースアカウントから委任されたアカウントにデータをレプリケートするための許可が必要です。委任されたアカウントは、各ソースアカウントと、それらのソースアカウントによって選択された AWS リージョンのリソースおよび IP 使用状況の詳細にアクセスできます。

Amazon VPC IP Address Manager が、ソースアカウントから Amazon VPC IP Address Manager 委任アカウントにデータをレプリケートすることを許可します。
IPAM の作成を続行するには、このチェックボックスをオンにする必要があります。

IPAM の設定 情報

Using IPAM with a single account

If you are creating an IPAM for a single account (not an organization), in order for IPAM to monitor your resources, you must create a service-linked role. [Learn more](#).

名前タグ - オプション

「Name」のキーと指定した値を持つタグを作成します。

グローバル名

説明 - オプション

IPAM の簡単な説明を記述します。

自分の IPAM

運用リージョン

IPAM がリソースを検出し、IP を管理するリージョンを選択します。

リージョンを選択

2つのデフォルトのスコープが作成されます

IPAM の作成時には、プライベートスコープとパブリックスコープの 2 つのデフォルトのスコープも作成されます。

タグ

タグは、AWS リソースに割り当てるラベルです。各タグは、キーとオプションの値で構成されます。タグを使用して、リソースを検索してフィルタリングしたり、AWS のコストを追跡したりできます。

リソースにタグが関連付けられていません。

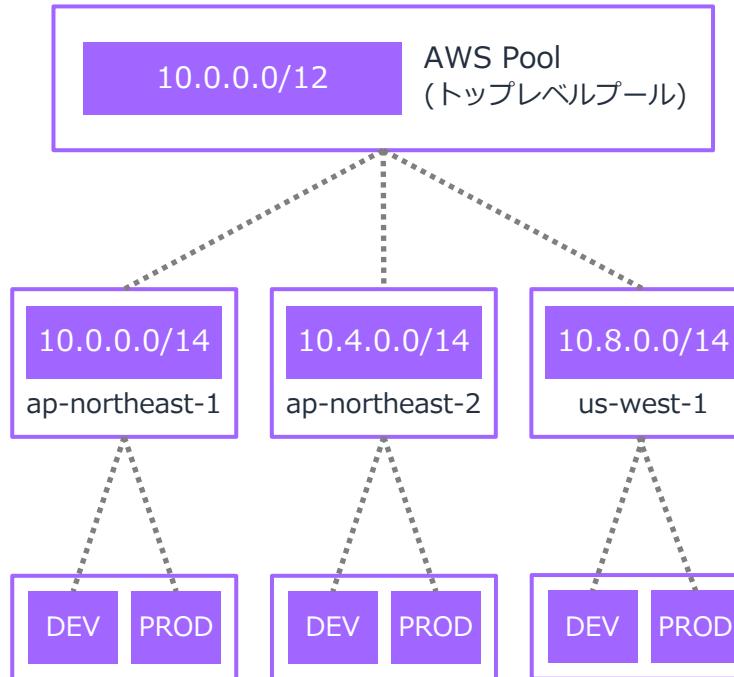
新しいタグを追加

さらに 50 個のタグを追加できます。

ベストプラクティス：トップレベルプールを作成、配下の階層を要件に応じて設計

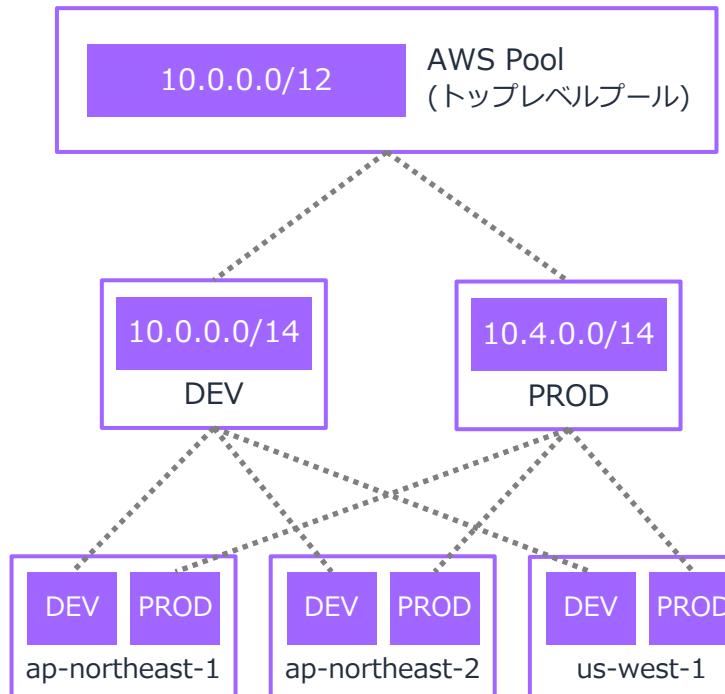
例 1

リージョンごとに統合して管理



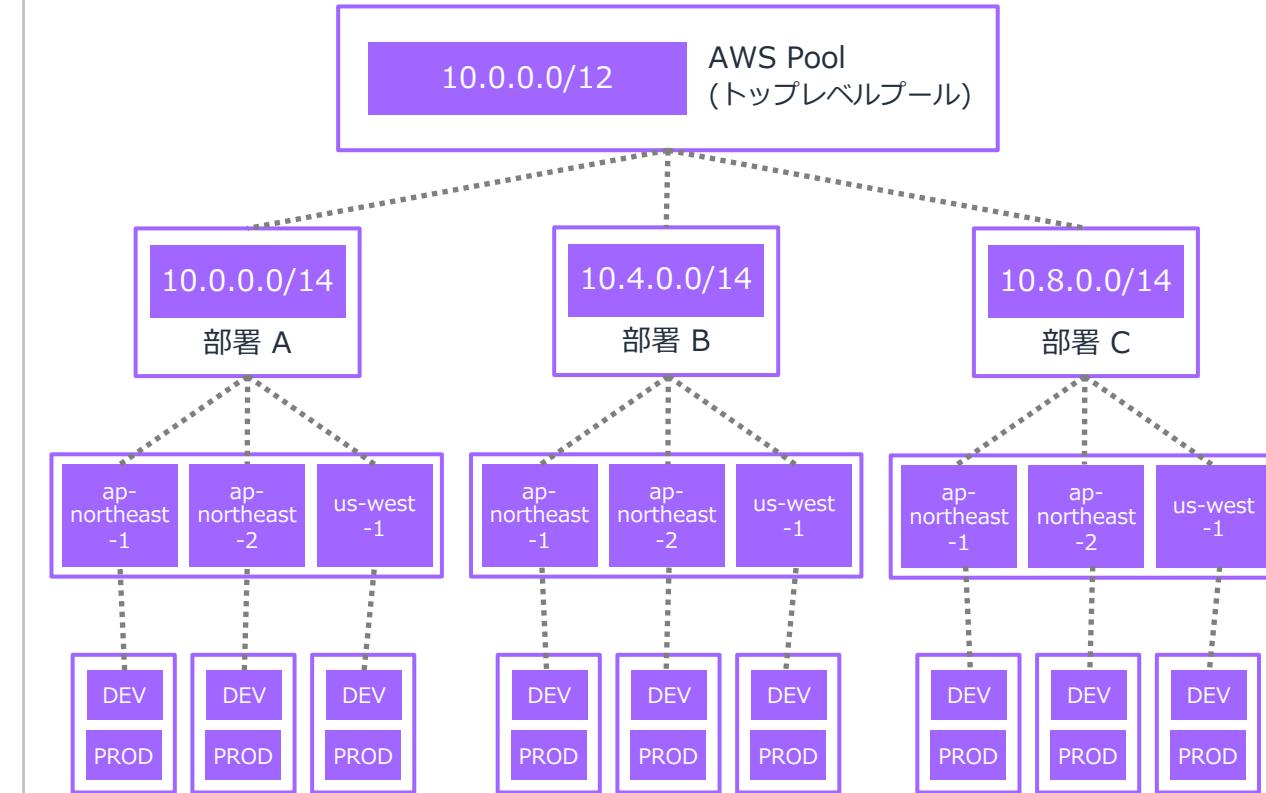
例 2

ワークロードごとに統合して管理



例 3

部署ごとに統合して管理



IP 空間の設計 | プール作成画面

IPAM 作成

IP 空間設計

割り振りルール設定

Amazon VPC IP Address Manager > Pools > 作成

次でプールを作成: ipam-scope-088307f7ce790b230

プールの設定

IPAM ID
ipam-0008686caac19cbc4

スコープ ID
ipam-scope-088307f7ce790b230

名前タグ - オプション
「Name」のキー

VPC プール

説明 - オプション
プールの簡単な説明

VPC 用のプール

- トップレベルプールを作成する場合**
- ソースプール: 無し (No source pool)
 - ロケール: 無し (None)

プール階層 情報

ソースプール

このプールに CIDR をプロビジョンするには、その CIDR がソースプールで使用可能である必要があります。ソースプールが選択されていない場合は、その空間がスコープ内で使用可能である必要があります。

No source pool

アドレスファミリー

このプールのアドレスファミリーを選択します。

IPv4

ロケール

このプールが存在するロケールを選択します。

None

プロビジョンする CIDR 情報

プロビジョン先の CIDR は、ソースプールのスペースで、またはソースプールがない場合はスコープのスペースで、使用可能である必要があります。

CIDR 1/1

CIDR

プロビジョンする CIDR を追加します。

10.0.0.0/12

1M IPs

削除

< > ^ v

新しい CIDR を追加

割り振りルール設定 - オプション 情報

AWS best practice

ソースプールが設定されている場合
/16 など、サイズ別の CIDR 追加も可能

CIDR 1/1

CIDR

プールの作成後にプロビジョンする CIDR を追加します。正確な CIDR を入力するか、ネットマスク長を指定できます。

転送する CIDR ネットマスク長を選択

削除

特定の CIDR を追加

サイズ別に CIDR を追加

新しいタグを追加

さらに 50 個のタグを追加できます。

キャンセル

プールを作成

IP 空間の設計 | プール一覧画面

IPAM 作成

IP 空間設計

割り振りルール設定

Amazon VPC IP Address Manager

ダッシュボード

リソース

IP 履歴インサイト

プール

IPAM
スコープ
設定

Amazon VPC IP Address Manager > Pools

スコープ

プール (7)

IPAM スコープ内のプールを表示します。

プールを検索

名前/プール ID	説明	CIDR	状態
top-level-global-pool (ipam-pool-026175a7cf6d15e22)	Top-level pool	10.0.0.0/12	プロビジョン済み 修正完了
osaka-pool (ipam-pool-0255546d88ccf311)	-	10.0.0.0/14	プロビジョン済み 作成完了
osaka-dev (ipam-pool-0da4d02d36d94376b)	-	10.0.0.0/16	プロビジョン済み 作成完了
osaka-prod (ipam-pool-0fd447f311755db7d)	Prod pool in Osaka	10.1.0.0/16	プロビジョン済み 修正完了
tokyo-pool (ipam-pool-078e9029d344ad8a1)	-	10.4.0.0/14	プロビジョン済み 作成完了
tokyo-prod (ipam-pool-01dc0fefbf1cd62ed)	-	10.5.0.0/16	プロビジョン済み 作成完了
tokyo-dev (ipam-pool-0c1f8279000786798)	-	10.4.0.0/16	プロビジョン済み 作成完了

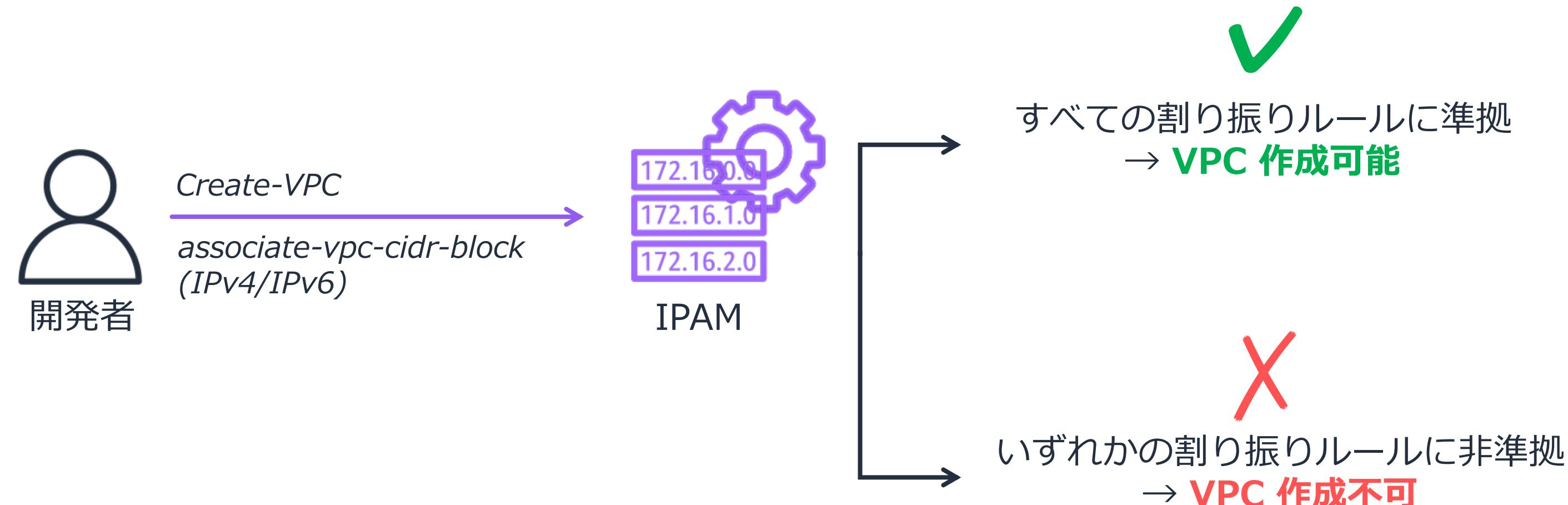
割り振りルール設定 | 仕組み

IPAM 作成

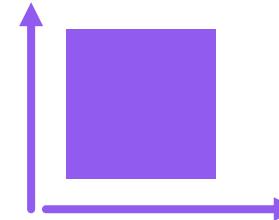
IP 空間設計

割り振りルール設定

各プールでの CIDR の割り振りについてルールを設定
CIDR 申請時/利用検知時に、IPAM がチェックを行う



この設定項目を「コンプライアンス」として、プール内の VPC を判定



ネットマスク (サイズ)

プール内で利用可能な CIDR のサイズ
例) /24 以上のサイズは作成不可



タグ

プールから CIDR を利用する際にリソースに必要なタグ
例) タグ environment=dev を持つリソースのみ許可



リージョン

プールを利用可能なリージョン



プリンシパル

プールを利用可能な組織単位 (OU) / アカウント
※ AWS Resource Access Manager (RAM) で設定

割り振りルール設定 | プール作成画面

IPAM 作成

IP 空間設計

割り振りルール設定

Amazon VPC IP Address Manager > Pools > 作成

次のプールを

このプールの割り振りルール設定を構成

プールの設定

IPAM ID
ipam-0008686caac19

名前タグ - オプション
「Name」のキーと指定し

VPC プール

説明 - オプション
プールの簡単な説明を記述

VPC 用のプール

プール階層 情報

ソースプール
このプールに CIDR をプロ

場合は、その空間がスコ

No source pool

アドレスファミリー
このプールのアドレスファ

IPv4

ロケール
このプールが存在するロク

None

CIDR 管理

リソースの自動インポート

検出されたリソースを自動的にインポート

このプールを使用して VPC などのリソースに CIDR を割り振る場合は、自動インポートを許可することをお勧めします。

- 自動インポートを許可
 許可しない

ネットマスクコンプライアンスネットマスク

ネットマスクの最小長

プール内でリソースを割り振るためのネットマスクの最小長。

/0 (4,294M IPs)

デフォルトのネットマスク長

IPAM がこのプールから CIDR をリソースに割り振るときに使用されるデフォルトのネットマスク長。

デフォルトのネットマスク長を選択

ネットマスクの最大長

プール内でリソースを割り振るためのネットマスクの最大長。

/32 (1 IP)

タグコンプライアンス

タグ

タグ付け要件

このプールのリソースのタグ付け要件を追加します。

新しい必須タグを追加

さらに 50 個のタグを追加できます。

ロケールコンプライアンス

ロケール (リージョン) ※ソースプールから継承

ロケール

ロケールはプールロケールによって設定されます。

ap-northeast-1

プロビジョンする CIDR 情報

プロビジョン先の CIDR は、ソースプールのスペースで、またはソースプールがない場合はスコープのスペースで、使用可能である必要があります。

CIDR 1/1

CIDR

プロビジョンする CIDR を追加します。

10.0.0.0/12

1M IPs

削除

新しい CIDR を追加

割り振りルール設定 - オプション 情報



AWS のベストプラクティス

最上位のプールを作成してから、最上位のプールの下にリージョン別のプールを作成することをお勧めします。リージョン別のプールの下に、開発プールを作成します。開発プールから割り当てるルールを設定して、これらのプールの CIDR を使用できるリソースを制御できます。IPAM プールを整理する方法の例については、次を参照してください: [IPAM プールプランの例](#).

Use this pool to allocate CIDRs to resources such as VPCs

タグ

タグは、AWS リソースに割り当てるラベルです。各タグは、キーとオプションの値で構成されます。タグを使用して、リソースを検索してフィルタリングしたり、AWS のコストを追跡したりできます。

リソースにタグが関連付けられていません。

新しいタグを追加

さらに 50 個のタグを追加できます。

キャンセル

プールを作成

組織での CIDR 払い出しの制限

IPAM 作成

IP 空間設計

割り振りルール設定

(補足)

- AWS Organizations の Service Control Policy (SCP) で、指定した IPAM プール以外からは CIDR を払い出せないよう設定可能

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Deny",  
      "Action": ["ec2>CreateVpc", "ec2:AssociateVpcCidrBlock"],  
      "Resource": "arn:aws:ec2:*:*:vpc/*",  
      "Condition": {  
        "StringNotEquals": {  
          "ec2:Ipv4IpamPoolId": "ipam-pool-0123456789abcdefg"  
        }  
      }  
    }  
  ]  
}
```

IPAM の利用方法 | VPC 作成

VPC の設定

作成するリソース 情報
VPC リソースのみを作成するか、VPC やサブネットなどを作成します。

VPC のみ VPC、サブネットなど

名前タグ - オプション
「Name」のキーと、ユーザーが指定する値でタグを作成します。
my-vpc-01

IPv4 CIDR ブロック 情報
 IPv4 CIDR の手動入力 IPAM 割り当ての IPv4 CIDR ブロック -

IPv4 IPAM プール
osaka-prod (ipam-pool-0fd447f311755db7d)
ap-northeast-3 Prod pool in Osaka

The locale of the IPAM pool must be equal to the current region.

ネットマスク
ネットマスクを選択

IPv6 CIDR ブロック 情報
 IPv6 CIDR ブロックなし IPAM 割り当ての IPv6 CIDR ブロック - Amazon 提供の IPv6 CIDR ブロック IPv6 CIDR 所有 (ユーザー所有)

♦ 2022/4 月現在、BYOIPv6 のみ IPAM 管理可能

テナント 情報
デフォルト



- IPAM で割り当てられた IPv4/IPv6 CIDR ブロックを指定して VPC を作成可能
- プールから選択
- 割り振りルールによるチェックが実施される
 - ネットマスク：設定された最小・最大の範囲からのみ選択可
 - リソースタグ
 - プリンシパル

注意！

2022/4 月現在・・・

- ※ 特定の作成方法でのみ IPAM プールを選択可能
- ※ VPC 作成以外で、明示的に IPAM プール等を選択することはない
 - VPC 内にサブネット等のリソースを作成すると、IPAM が自動で検知する仕組み

IPAM の利用方法 | VPC 作成以外 – コンソール オーバーレイネットワーク、VPN 等用に CIDR の事前割り振り

The diagram illustrates the process of pre-allocating CIDR blocks. It shows a large grey arrow pointing from the left-hand 'Pool Overview' screen to the right-hand 'Pre-Allocation Configuration' screen.

Left Panel: IPAM Pool Overview (ipam-pool-0fd447f311755db7d)

- Pool ID:** ipam-pool-0fd447f311755db7d
- 説明:** Prod pool in Osaka
- 所有者 ID:** [REDACTED]
- IPAM ID:** ipam-0008686caac19cbc4
- スコープ ID:** ipam-scope-088307f7ce790b230
- コンプライアンスのステータス:**
 - 1 準拠リソース CIDR
 - 1 非準拠リソース CIDR
- 競合ステータス:**
 - 2 重複しないリソース CIDR

Bottom Navigation: プールの詳細 | モニタリング | CIDR | **割り振り** | リソース | コンプライアンス | リソース共有 | タグ

Allocation Table:

CIDR	割り振り ID	リソースのタイプ	説明	リソース ID
10.1.0.0/24	ipam-pool-alloc-02...	vpc	-	vpc-0020880e7ea8...
10.1.1.0/24	ipam-pool-alloc-0d...	vpc	-	vpc-05f69d1fd33a...

Buttons: Ignore and release CIDRs | CIDR の割り振りを解除 | **CIDR を割り振る**

Right Panel: Pre-Allocation Configuration

次で割り当て: ipam-pool-0fd447f311755db7d

割り振りを作成して、後で使用するために IPAM プール内の空間を手動で予約します。例えば、オンプレミスネットワークで CIDR 用の空間を予約できます。IPAM は予約を管理し、オンプレミスの IP 空間と重複する CIDR があるかどうかを示します。

割り振り設定

CIDR 別
割り当てる CIDR を指定します。

ネットマスクの長さ別
割り当てるスペースのサイズを選択します。

CIDR: 割り振る CIDR を入力します。
CIDR を入力 - IPs
< > ^ v

説明 - オプション: この割り振りの説明を入力します。
自分のデータセンター

Buttons: キャンセル | **割り当てる**

IPAM の利用方法 | VPC 作成以外 – CLI/API

オーバーレイネットワーク、VPN 等用に CIDR の事前割り振り

```
$ aws ec2 allocate-ipam-pool-cidr \
--ipam-pool-id ipam-pool-0533048da7d823723 \
--netmask-length 24
```



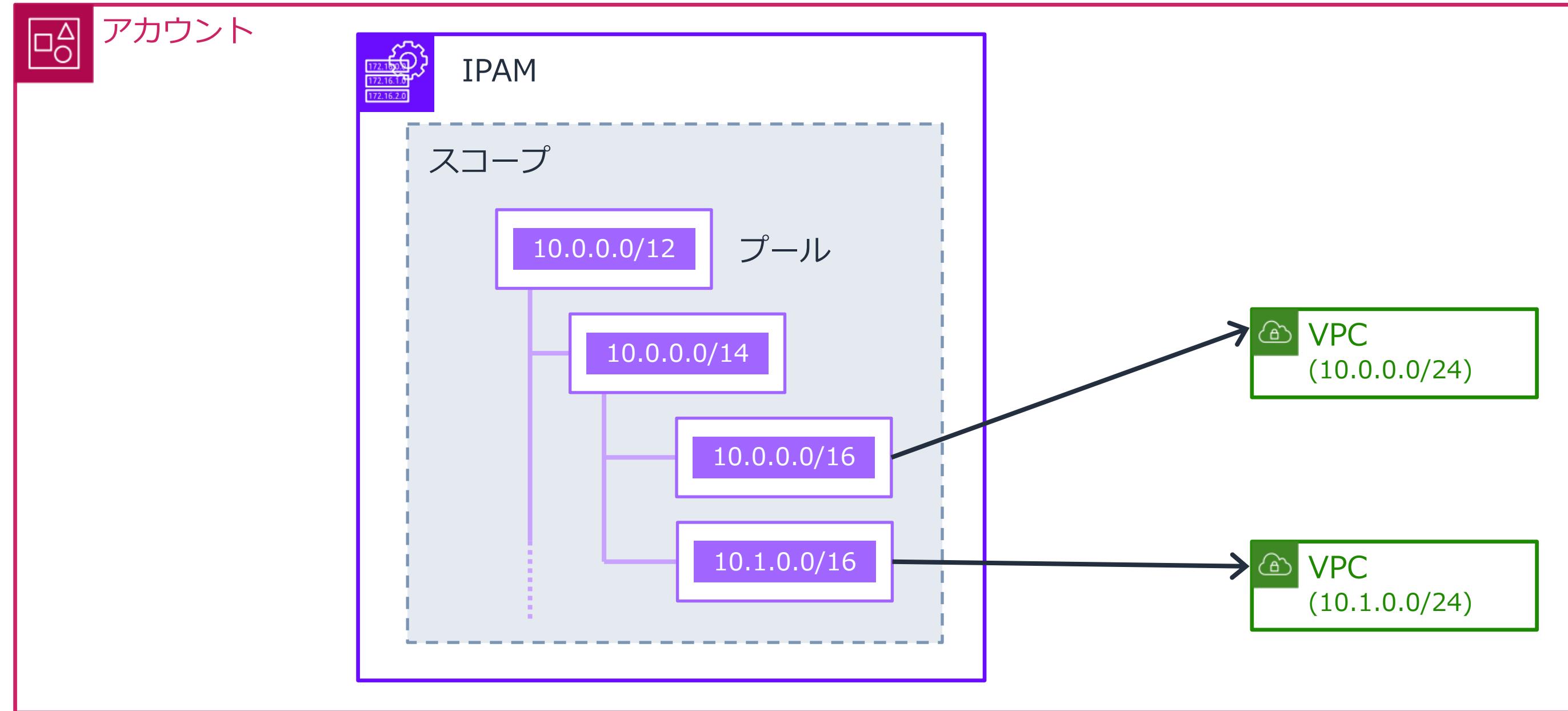
```
{
  "IpamPoolAllocation": {
    "Cidr": "10.0.0.0/24",
    "IpamPoolAllocationId": "ipam-pool-alloc-018ecc28043b54ba38e2cd99943cebfbd",
    "ResourceType": "custom",
    "ResourceOwner": "123456789012"
  }
}
```

CLI: <https://docs.aws.amazon.com/cli/latest/reference/ec2/allocate-ipam-pool-cidr.html>

API: https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/APIReference/API_AllocateIpamPoolCidr.html

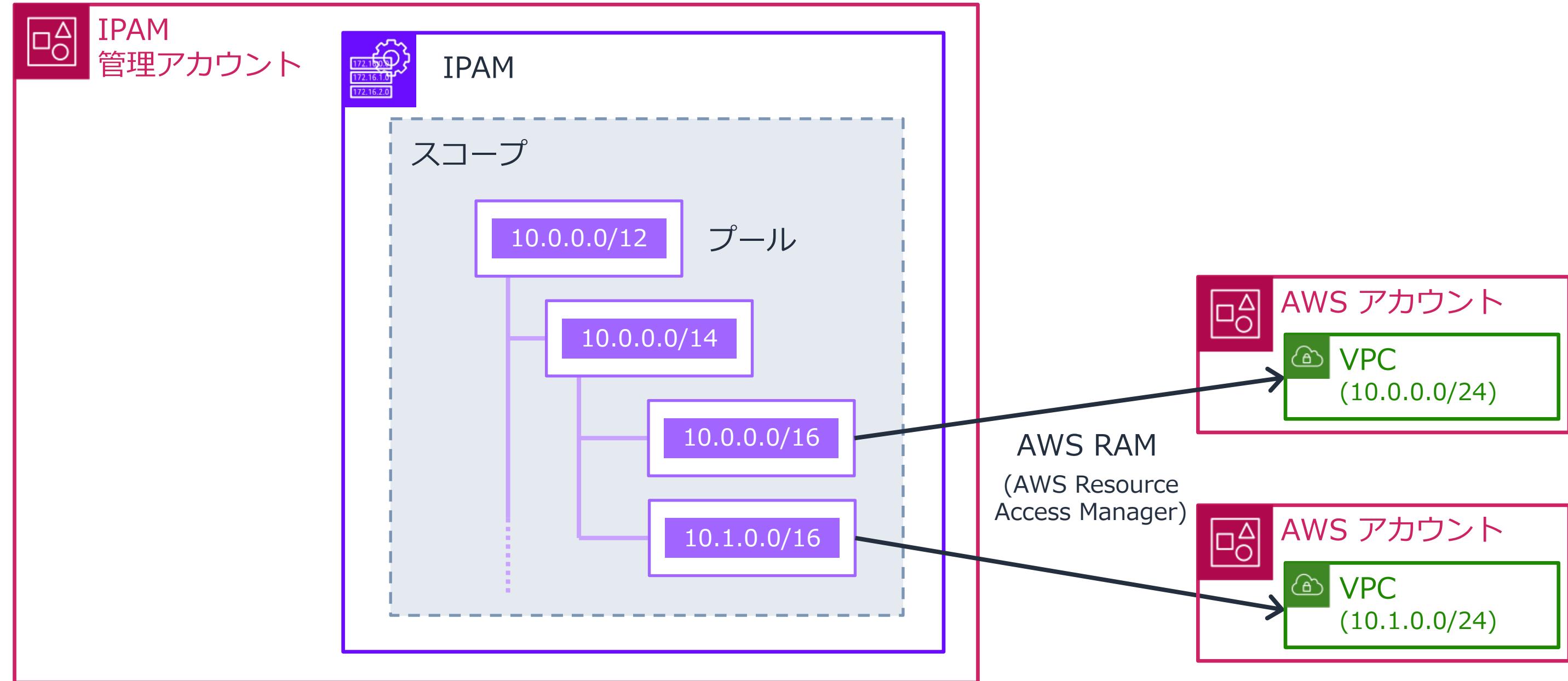
IPAM 利用イメージ | 単独アカウントの場合

アカウント内で、プールの作成から CIDR の割り振りまで完結



IPAM 利用イメージ | 複数アカウントの場合

IPAM 管理アカウントがプール等を作成。AWS RAM によりプールを共有。



モニタリング | リソース

リソースを発見し、重複、コンプライアンスのステータスを報告

The screenshot shows the 'Resources' page of the Amazon VPC IP Address Manager. The table lists various resources with columns for Resource ID, Compliance Status, Redundancy Status, Resource Name, Usage Status, CIDR, Region, Owner ID, and Pool ID. Several rows are highlighted with colored boxes and arrows:

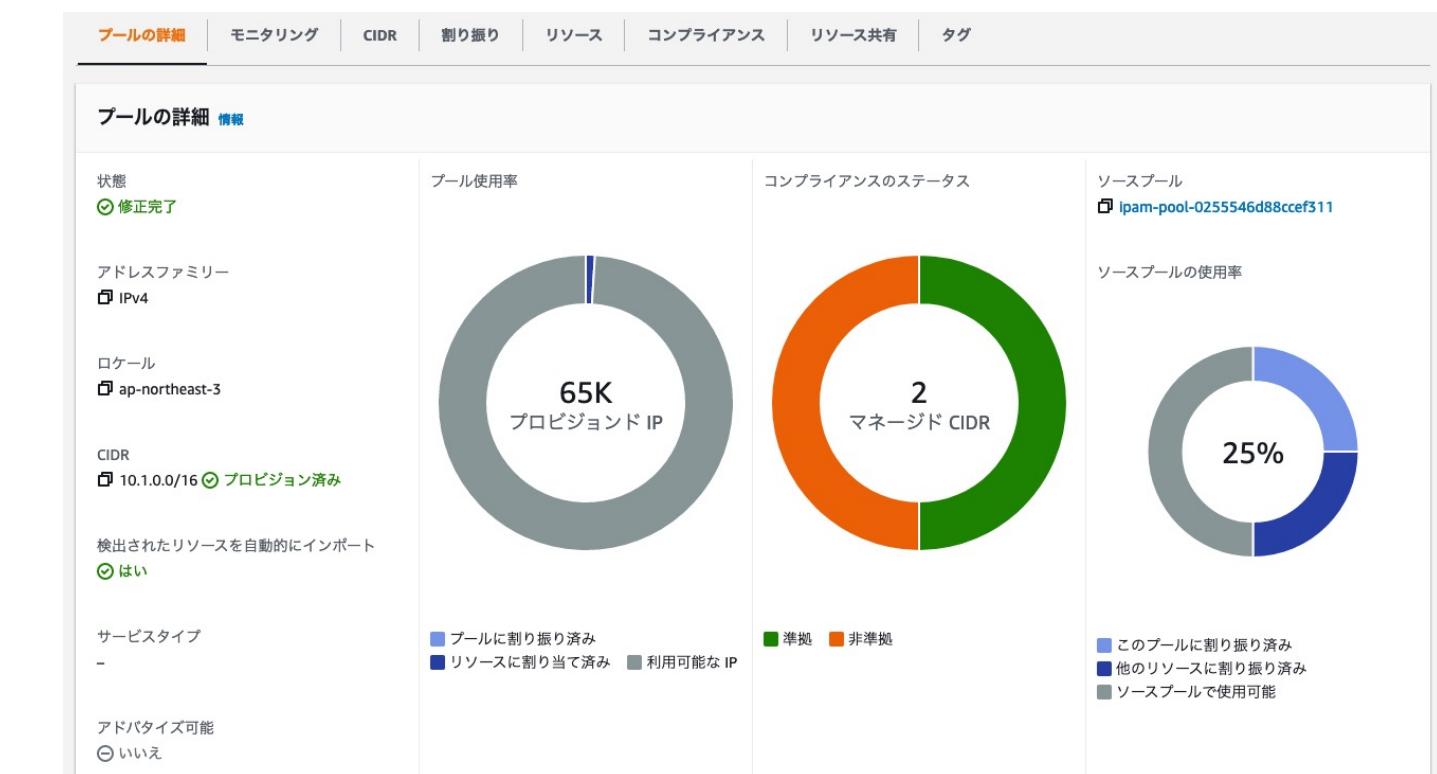
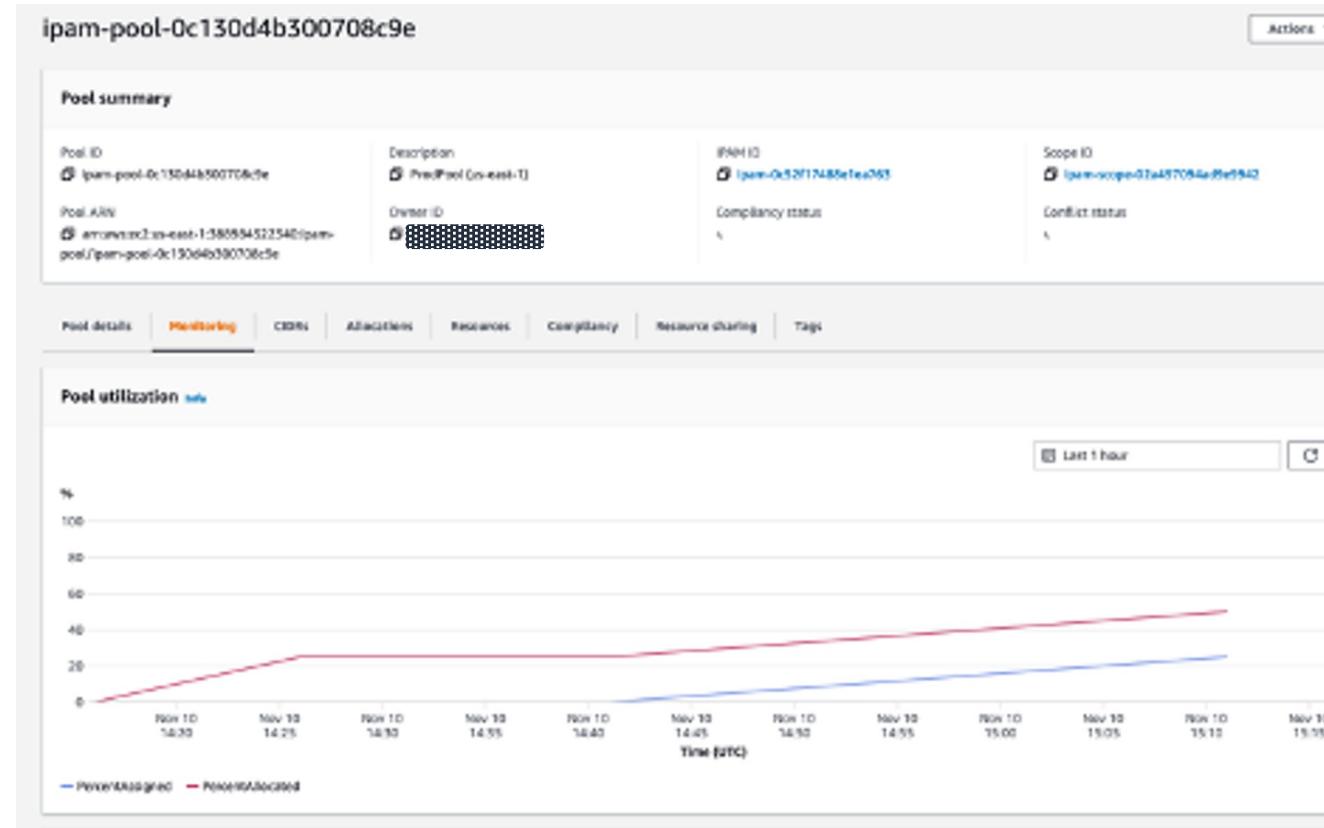
- A yellow box highlights the 'Compliance Status' column header and the first few rows.
- A purple box highlights the 'Redundancy Status' column header and the last few rows.
- Two specific rows are circled with purple boxes:
 - The first circled row shows 'dx-lab-test-vpc' with two red 'Duplicate' markers pointing to the same CIDR range '10.0.0.0/20'.
 - The second circled row shows 'SandboxVPC01' with two red 'Duplicate' markers pointing to the same CIDR range '10.0.0.0/16'.
- Two other rows have purple boxes around their CIDR ranges:
 - 'ipam-osaka-pr...' has a box around '10.1.1.0/24'.
 - 'Default VPC' has a box around '172.31.0.0/16'.

サブネット・VPC・Elastic IP・
パブリック IPv4 アドレスプール

* EC2, ENI は表示されない (IP 履歴インサイトとの違い)

モニタリング | プール > モニタリング

プールの利用率などをモニタリングし、CloudWatch Alarms も設定可能



IP 履歴インサイト

時間を遡った利用状況を確認し、トラブルシュートや監査に活用可能

The screenshot shows the 'Amazon VPC IP Address Manager' interface with the 'IP History Insights' tab selected. The search criteria are set to CIDR 10.1.0.0/24, IPAM Scope ID ipam-scope-088307f7ce790b230, and a time range of 'Recent 12 hours'. The search results table shows one entry: a sampling completed at 2022-01-13T06:40:16.537Z for resource ID vpc-00208... with name ipam-osaka-pr... status compliant and no duplicates. The 'Resource Type' column is highlighted with a yellow box, showing 'VPC'.

サンプリングされた終了時刻	サンプリングされた開始時刻	リソース ID	名前	コンプライアンスのステータス	重複ステータス	リソースのタイプ	VPC ID
-	2022-01-13T06:40:16.537Z	vpc-00208...	ipam-osaka-pr...	準拠	重複なし	VPC	vpc-0020880e7

* 指定の CIDR に完全一致のリソースのみ表示される
/24 を指定した場合、配下の /32 などは表示されない

検出対象

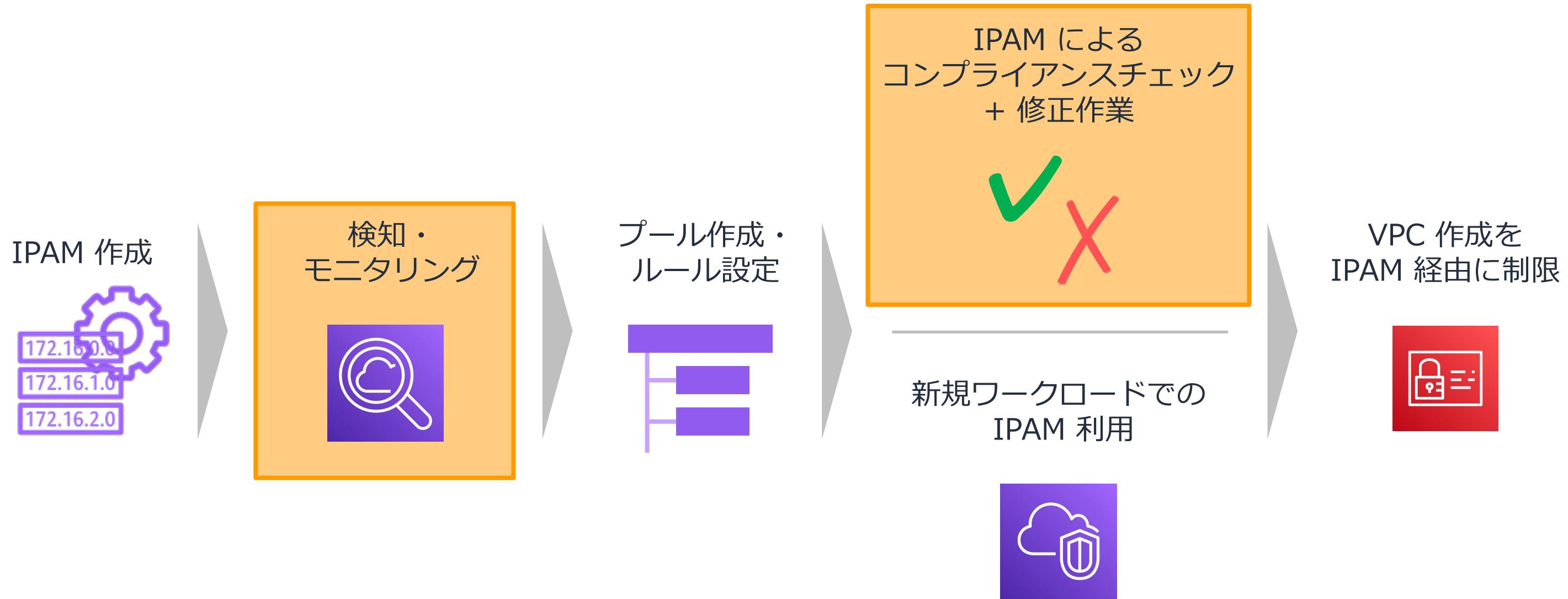
- サブネット
- VPC
- Elastic IP
- EC2 インスタンス
- ENI

本セッションの流れ（再掲）

- サービス登場の背景 – IPAM 登場以前の課題
- サービス概要
- サービス導入方法・使い方
 - A. 新規環境への導入
 - **B. 既存環境への導入**
- クオータ・料金
- まとめ

基本的な移行の流れ

基本的な利用方法は新規導入と同じ。移行にあたり再設計・修正等が必要。



CIDR 重複 | 対処の方針

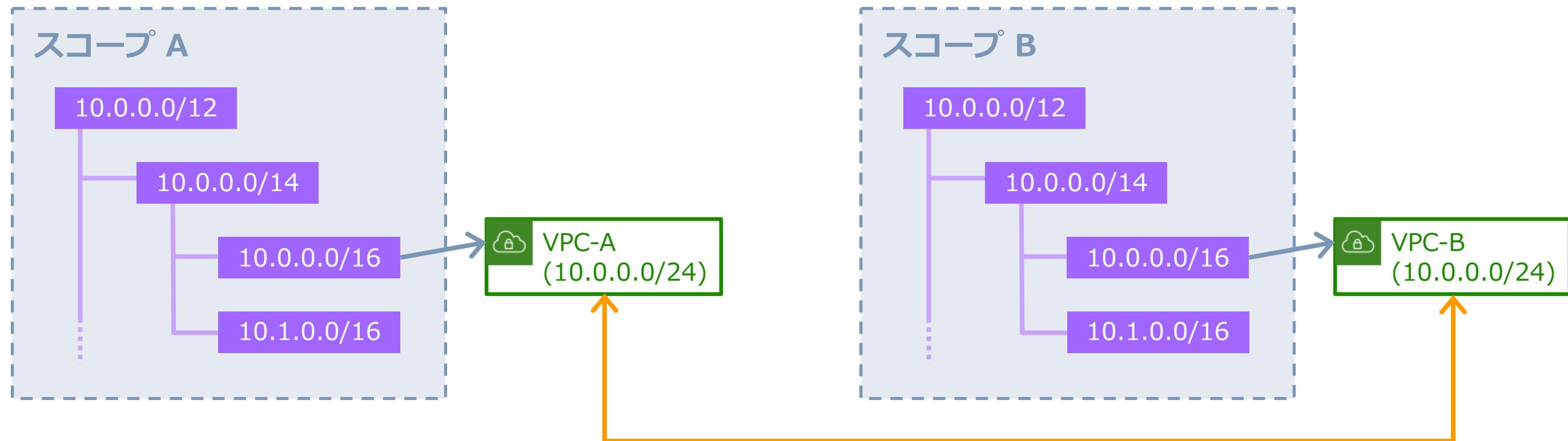
「2つのVPCを相互接続する予定の有無」により対処法が異なる

- 相互接続の予定あり → アーキテクチャを変更
 - 基本方針：相互接続するVPCは別CIDRにする
 - 重複しないCIDRで新しくVPCを作成し、新VPCに、これまでCIDRが重複していたVPCのうち片方のリソースを移行
 - 困難な場合は、NAT等による回避を検討
 - 参考：<https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-solve-private-ip-exhaustion-with-private-nat-solution/>
 - IPAM上では、下記対処(a), (b)のいずれかを実施し、エラーを回避
- 相互接続の予定なし → IPAMの機能を利用し対処
 - 対処(a): スコープの分割
 - 対処(b): スコープ内で「CIDRを無視」としてマーク
 - 新規導入で、意図的にCIDRを重複させる場合も対処法は同様

CIDR 重複 | IPAM での対処(a) スコープの分割

プライベートスコープを分けることで、重複は検出されない

- CIDR の管理はスコープごとに行われる
→ 別スコープであれば CIDR が重複していてもエラーは発生しない



- CIDR の重複は検出されない
- コンプライアンス準拠/非準拠も各 VPC の所属プールの割り振りルールで判定

CIDR 重複 | IPAM での対処(b) CIDR を無視としてマーク

特定のスコープ内で「関連づけられているすべてのCIDR を無視としてマーク」

Amazon VPC IP Address Manager > Resources

リソース (1/18) 情報

IPAM スコープ内のリソースを表示します。

リソースをフィルタリング

リソース ID コンプライアンスのス... 重複ステータス リソース名 IP 使用状況 CIDR リージ...

リソース ID	コンプライアンスのス...	重複ステータス	リソース名	IP 使用状況	CIDR	リージ...
vpc-0020880e7...	準拠	重複	ipam-osaka-prod-vpc	19%	10.1.0.0/24	ap-northe...
<input checked="" type="checkbox"/> vpc-0b71f014c1...	アンマネージド	重複	ipam-osaka-prod-vpc-...	0%	10.1.0.0/24	ap-northe...
vpc-05f69d1fd3...	非準拠	重複なし	ipam-osaka-prod-vpc-...	0%	10.1.1.0/24	ap-northe...

数分で反映

リソース (18) 情報

IPAM スコープ内のリソースを表示します。

リソースをフィルタリング

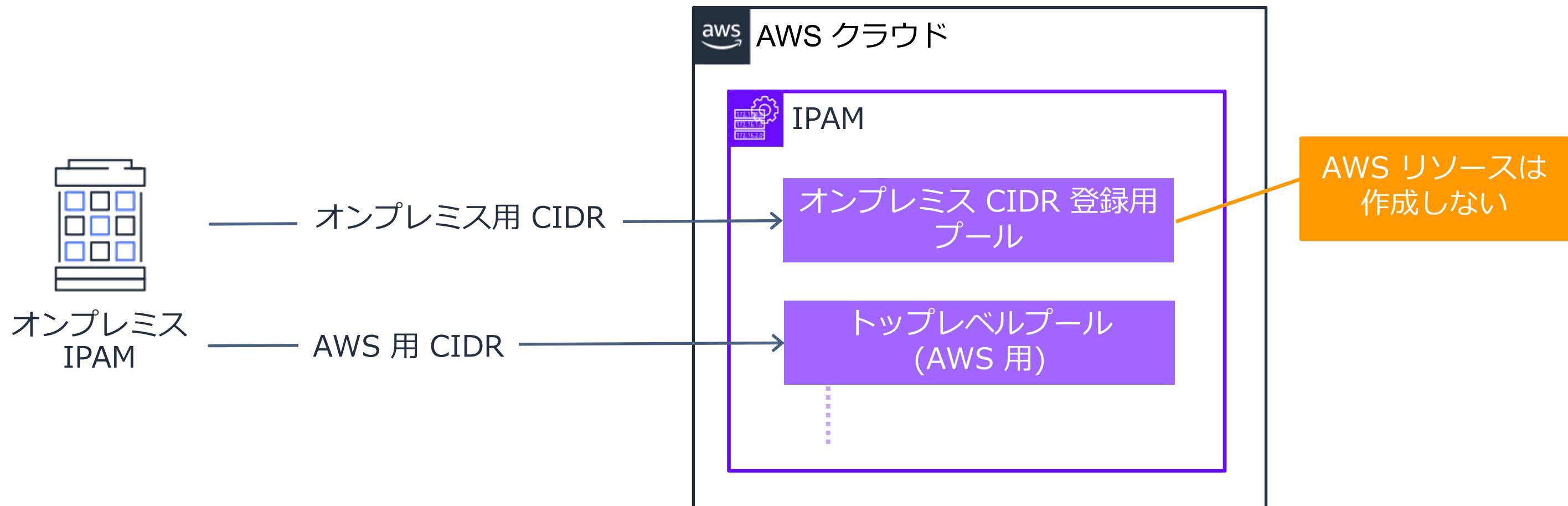
リソース ID コンプライアンスのス... 重複ステータス リソース名 IP 使用状況 CIDR リージ...

リソース ID	コンプライアンスのス...	重複ステータス	リソース名	IP 使用状況	CIDR	リージ...
vpc-0020880e7...	準拠	重複なし	ipam-osaka-prod-vpc	19%	10.1.0.0/24	ap-northe...
<input type="checkbox"/>	無視	無視	ipam-osaka-prod-vpc-...	0%	10.1.0.0/24	ap-northe...
vpc-05f69d1fd3...	非準拠	重複なし	ipam-osaka-prod-vpc-...	0%	10.1.1.0/24	ap-northe...

* コンプライアンスのステータスも無視される

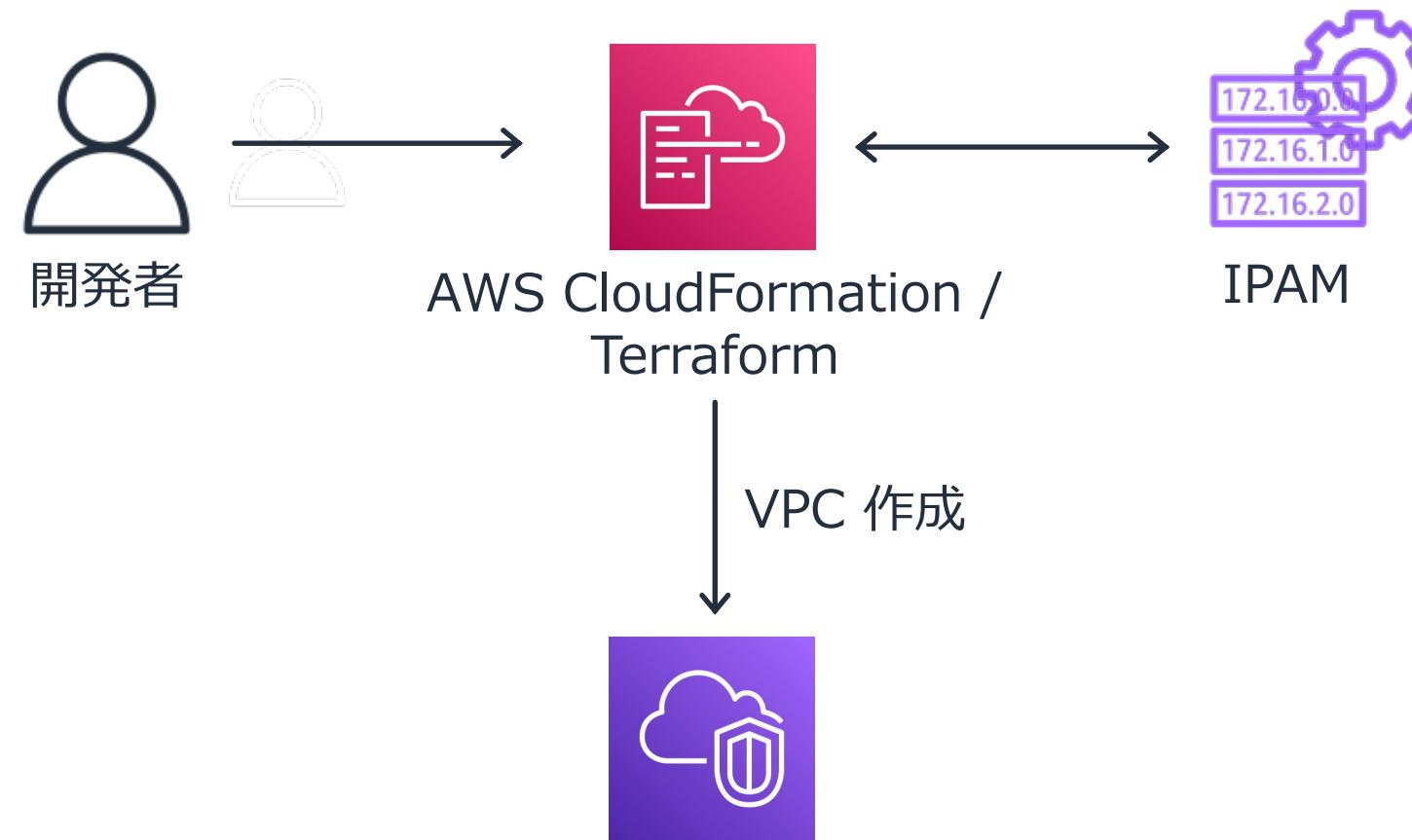
オンプレミス IPAM とのハイブリッド運用

VPC IPAM では、オンプレミスでの CIDR を登録するプールを作成する。
オンプレミス IPAM で AWS 用 CIDR を取得し、VPC IPAM で利用。



VPC への CIDR 割り振りの完全自動化

新規・既存に関わらず、AWS Cloud Formation, Terraform 経由で
完全自動化も可能



AWS CloudFormation: https://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/AWS_EC2.html

Terraform: https://registry.terraform.io/providers/hashicorp/aws/latest/docs/resources/vpc_ipam

Terraform モジュール: <https://github.com/aws-ia/terraform-aws-ipam>

本セッションの流れ（再掲）

- サービス登場の背景 – IPAM 登場以前の課題
- サービス概要
- サービス導入方法・使い方
 - A. 新規環境への導入
 - B. 既存環境への導入
- クオータ・料金
- まとめ

クオータ

	デフォルト	調整 (上限緩和申請) 可能
組織あたりの IPAM 管理者の数	1	いいえ
1 リージョンあたりの IPAM の数	1	はい
1 IPAM あたりのスコープの数	5	はい
1 スコープあたりのプールの数	50	はい
1 プールあたりの CIDR の数	50	はい
プールの階層の深さ	10	はい

料金

シンプルな従量課金：「IPAM が管理するアクティブな IP アドレス / 時間」

- アクティブな IP アドレス : EC2 や ENI などのリソースに実際にアタッチされた IP
- 例えば /16 の CIDR (65536 IP アドレス)が VPC に割り当てられていて、EC2 インスタンスでそのうち 5,000 の IP アドレスを利用している場合、5,000 IP アドレス分の料金のみが発生
 - 2022/4 月時点の東京リージョン (0.00027 USD/IP/時間) では 30 日間でアクティブな IP 5,000 個 × 30 日 × 24 時間 × 0.00027 USD 時間料金 = 972 USD
- マネジメントコンソール、CLI、API で IPAM を削除すれば利用停止もすぐに可能

注意！ IPAM 運用リージョンの全てのアクティブな IP アドレス に対し料金が発生

プールに所属しているかどうかとは無関係に

「リソースとして検知されている VPC (サブネット)」内のアクティブな IP アドレス に課金

例えば東京リージョンに 10 個の EC2 インスタンスが既に存在するアカウントで、運用リージョンに東京リージョンを含めるよう設定した IPAM を作成した場合、インスタンスが存在する VPC がプールに所属しているか否かとは無関係に 10 個の EC2 インスタンスは課金対象となる。

本セッションの流れ（再掲）

- サービス登場の背景 – IPAM 登場以前の課題
- サービス概要
- サービス導入方法・使い方
 - A. 新規環境への導入
 - B. 既存環境への導入
- クオータ・料金
- まとめ

まとめ

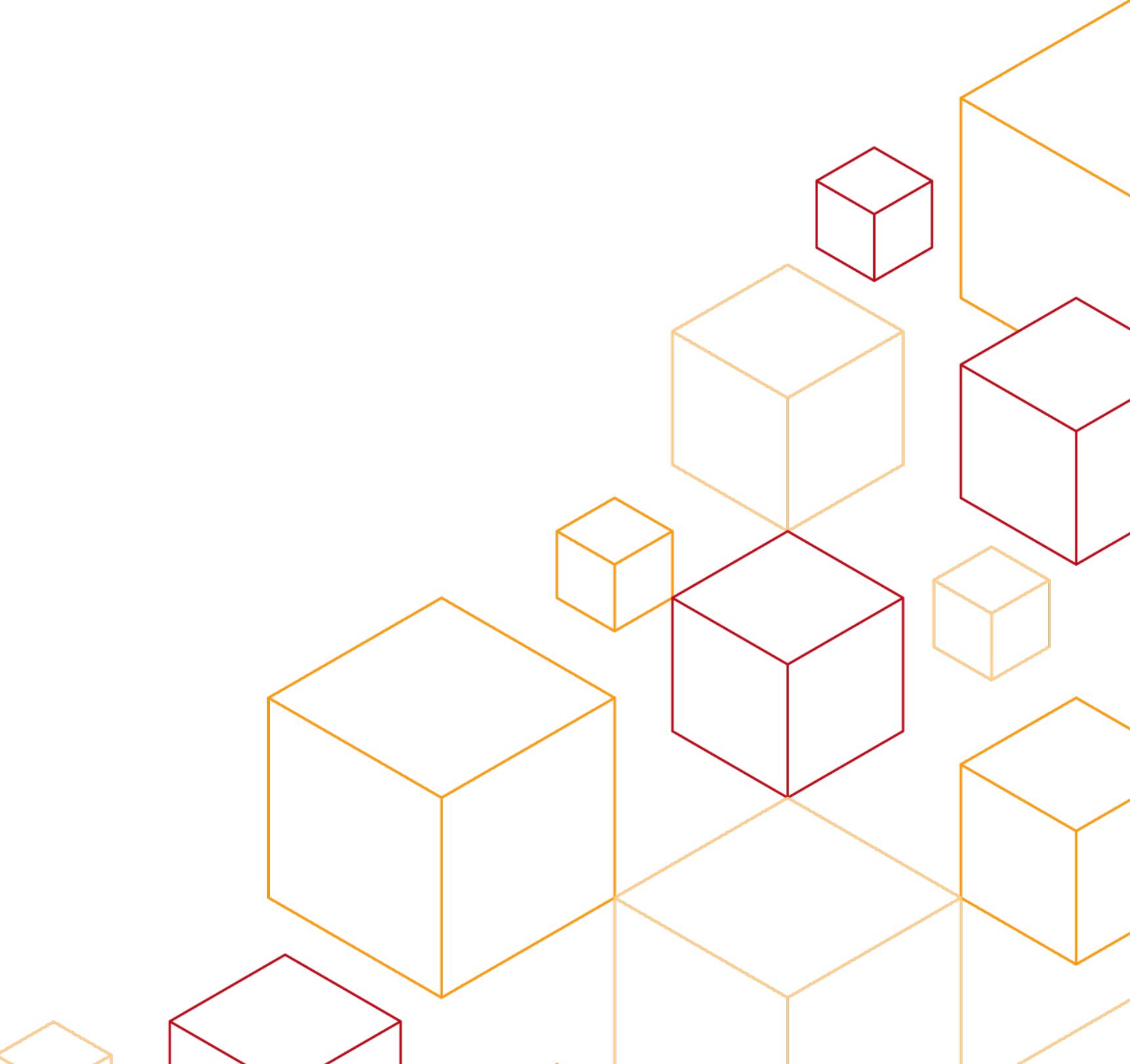
- Amazon VPC IP Address Manager (IPAM) は
VPC の IP アドレスを整理し、割り当て状態を管理できるサービス
 - 大規模ネットワークで CIDR を自動で割り当てることが可能
 - スプレッドシートなどによる手動管理が不要
 - アドレス割り当て業務の手間やミスを回避可能
 - CIDR 割り当てに対するルール設定
- IP アドレス利用状況のモニタリングや、過去に遡った分析に対応
 - トラブルシュートや監査に活用可能
- AWS Organizations や AWS Resource Access Manager との連携により
複数アカウントでの利用も可能

参考資料

- 公式ドキュメント
 - https://docs.aws.amazon.com/ja_jp/vpc/latest/ipam/what-it-is-ipam.html
- re:Invent 2021 “Manage our IP addresses at scale on AWS”
 - <https://www.youtube.com/watch?v=xtLJgJfhPLg&t=5s> (英語)
- Managing IP pools across VPCs and Regions using Amazon VPC IP Address Manager
 - <https://aws.amazon.com/blogs/networking-and-content-delivery/managing-ip-pools-across-vpcs-and-regions-using-amazon-vpc-ip-address-manager/> (AWS ブログ, 英語)



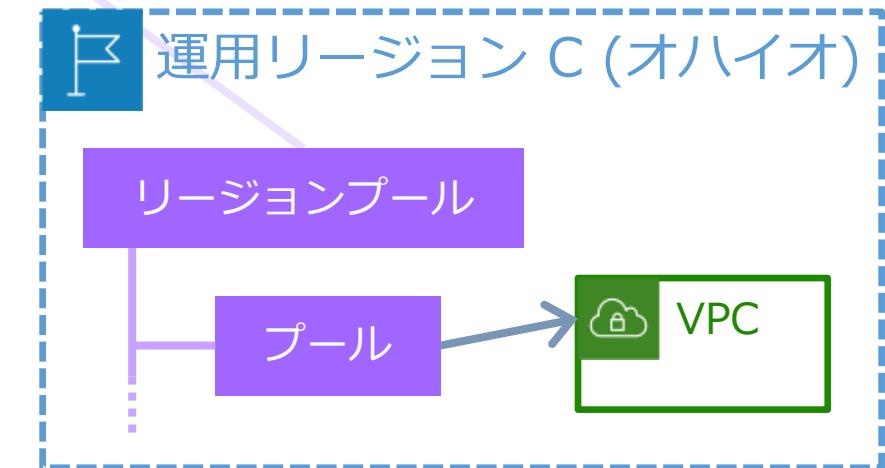
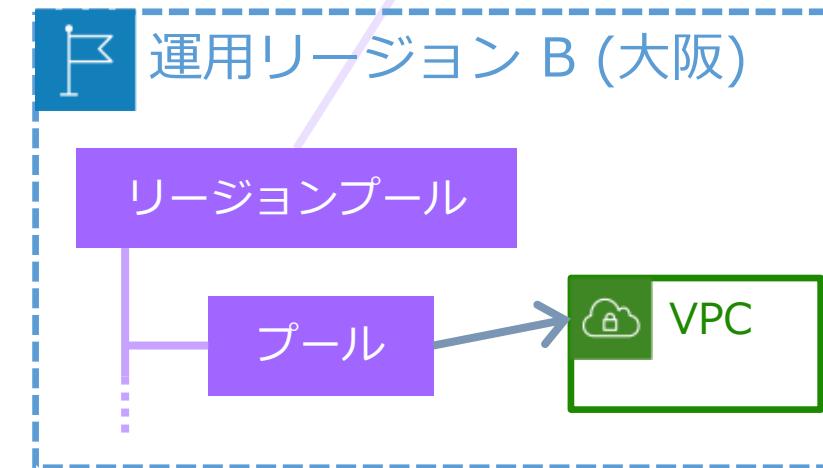
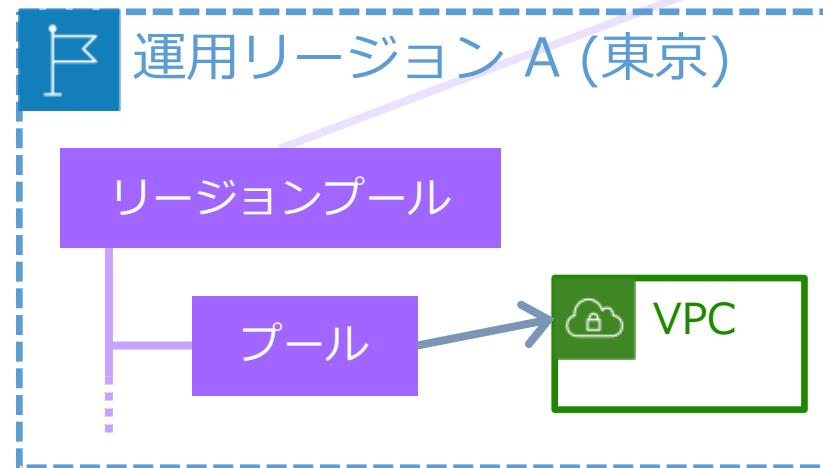
補足



IPAM のリージョンと可用性

ホームリージョン/運用リージョンは互いに非依存

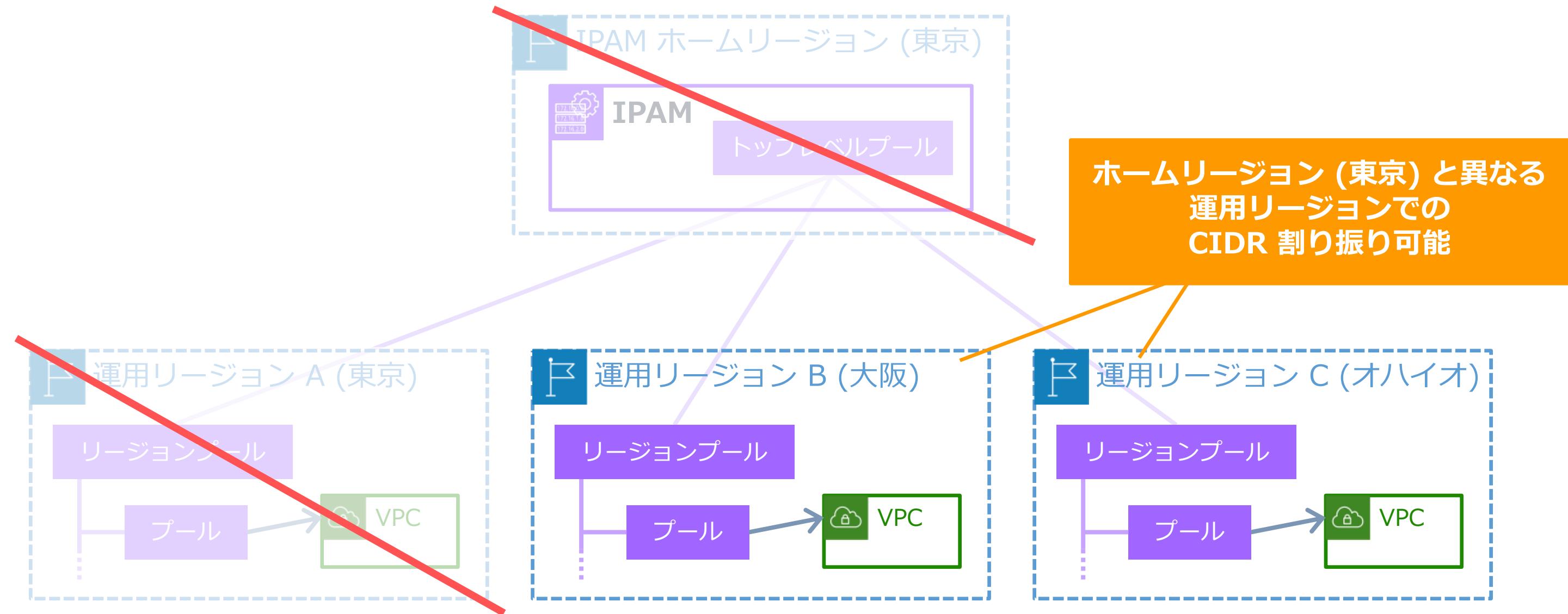
各運用リージョン内のプールは、別リージョンに非依存



ダッシュボードの運用
IPAM 配下の各プールの管理と、
IP のモニタリング

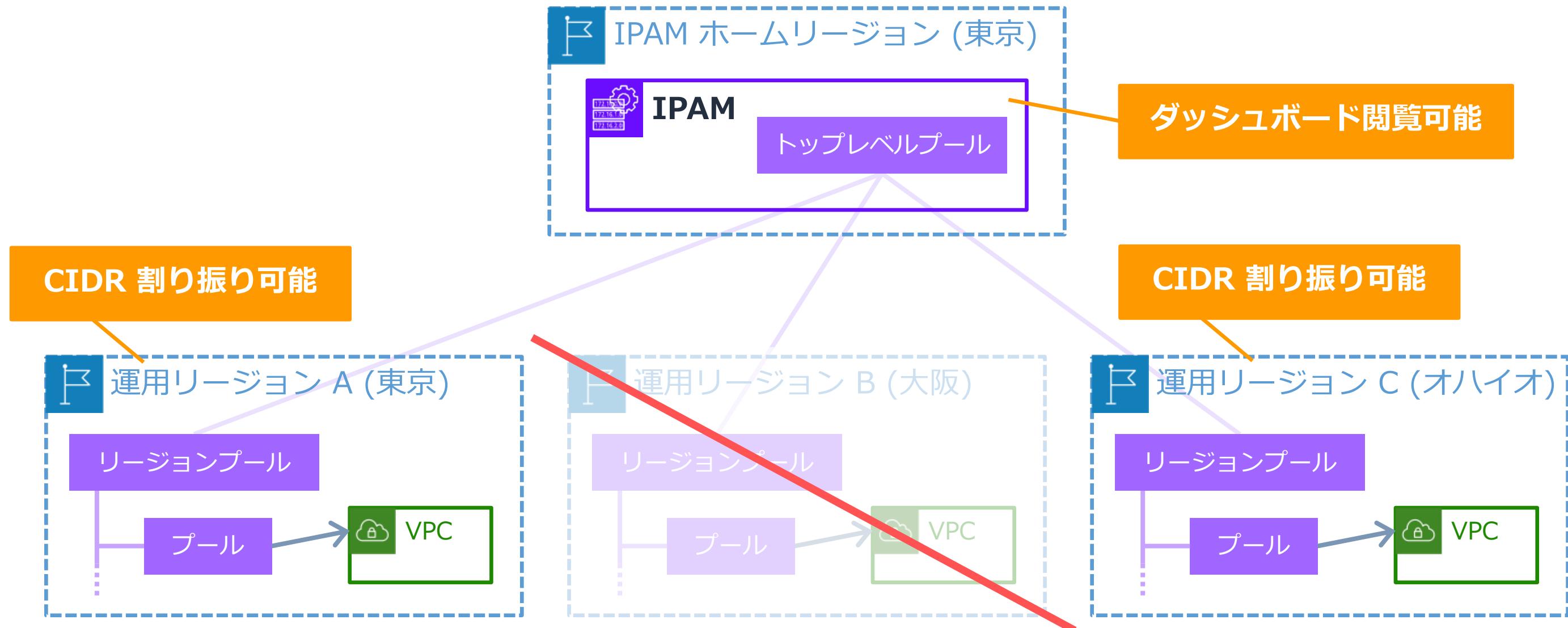
IPAM のリージョンと可用性 | シナリオ 1

ホームリージョンが利用できなくなった場合 → 他リージョンで IP 割り振り可能



IPAM のリージョンと可用性 | シナリオ 2

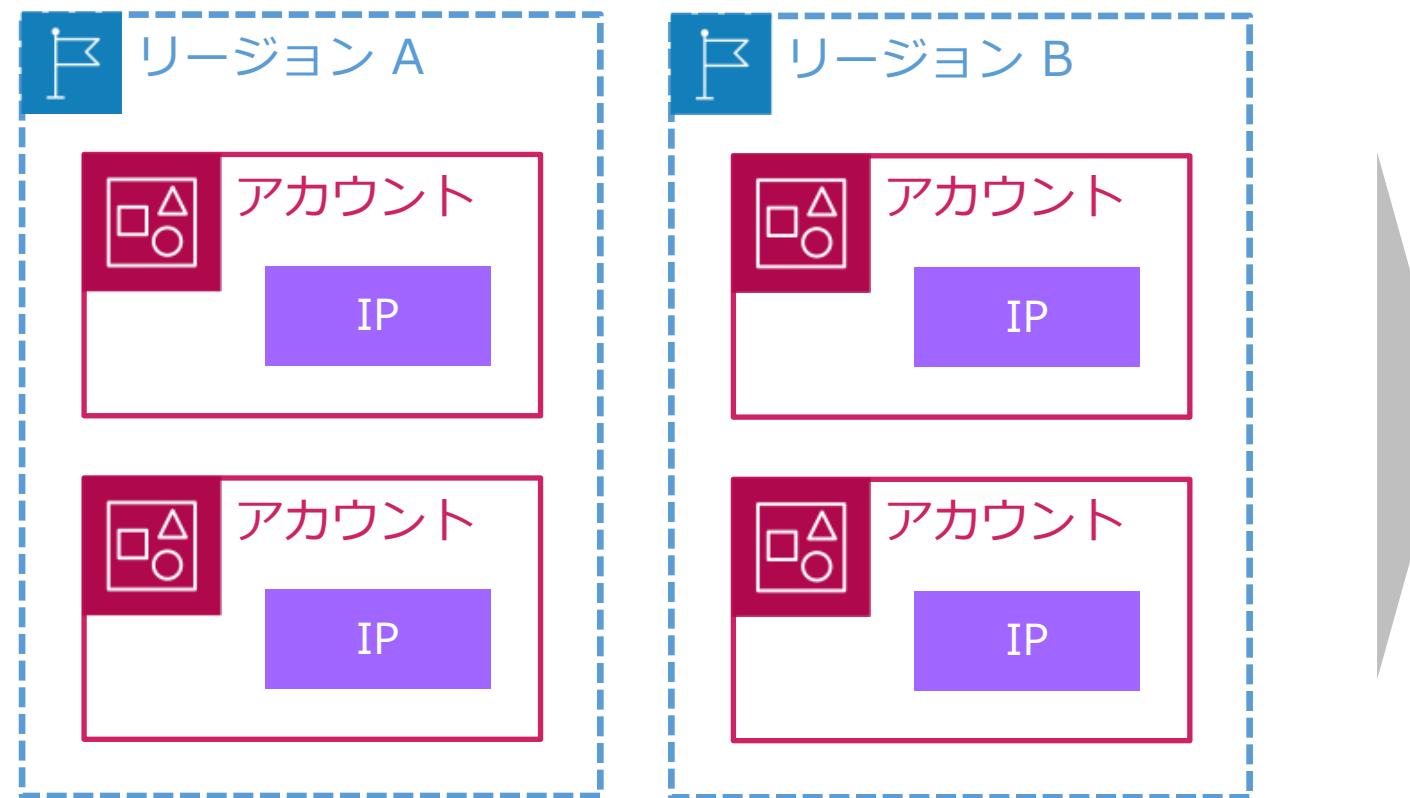
ある運用リージョンが利用できなくなった場合 → その他のリージョンは平常



BYOIP | アドレスのアカウント間共有

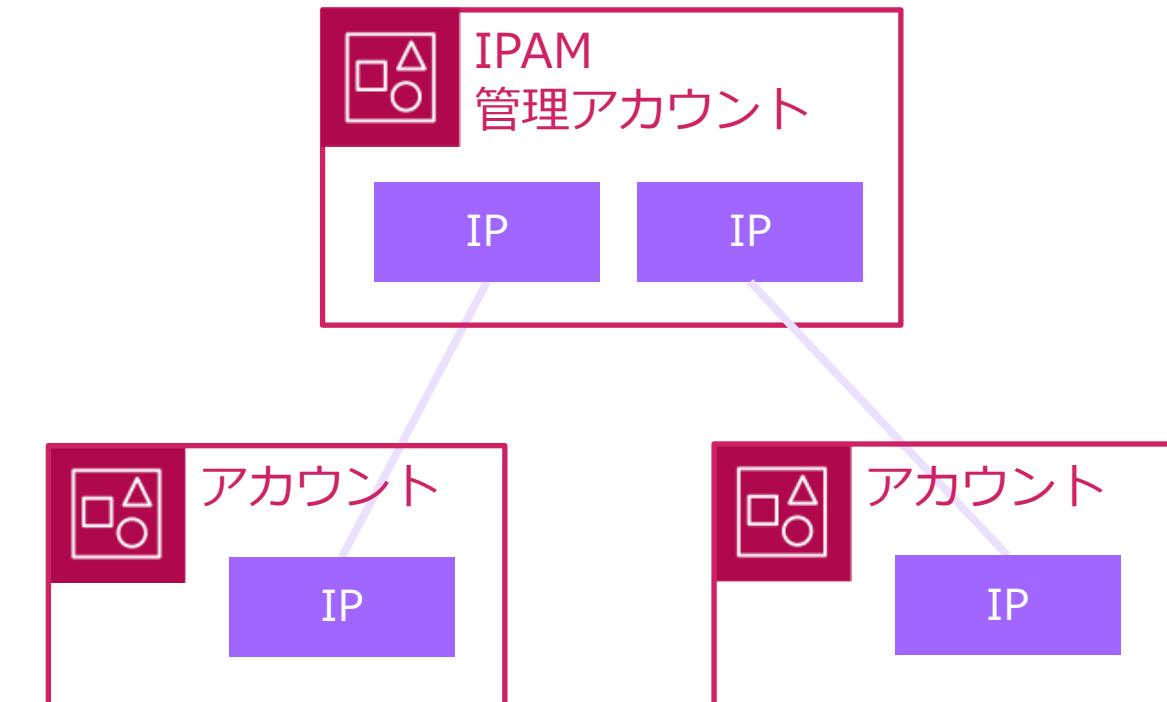
BYOIP したアドレスの利用開始手順を簡素化可能

IPAM 利用なし



各リージョンやアカウントで証明書等による設定が必要

IPAM 利用あり



IPAM 管理アカウントで一度設定すれば
組織内のアカウントで IP アドレスを利用可能

BYOIP | BGP 経路広告の制御

各プールで経路広告の許可 (パブリック/非パブリック) を制御可能

--publicly-advertisable

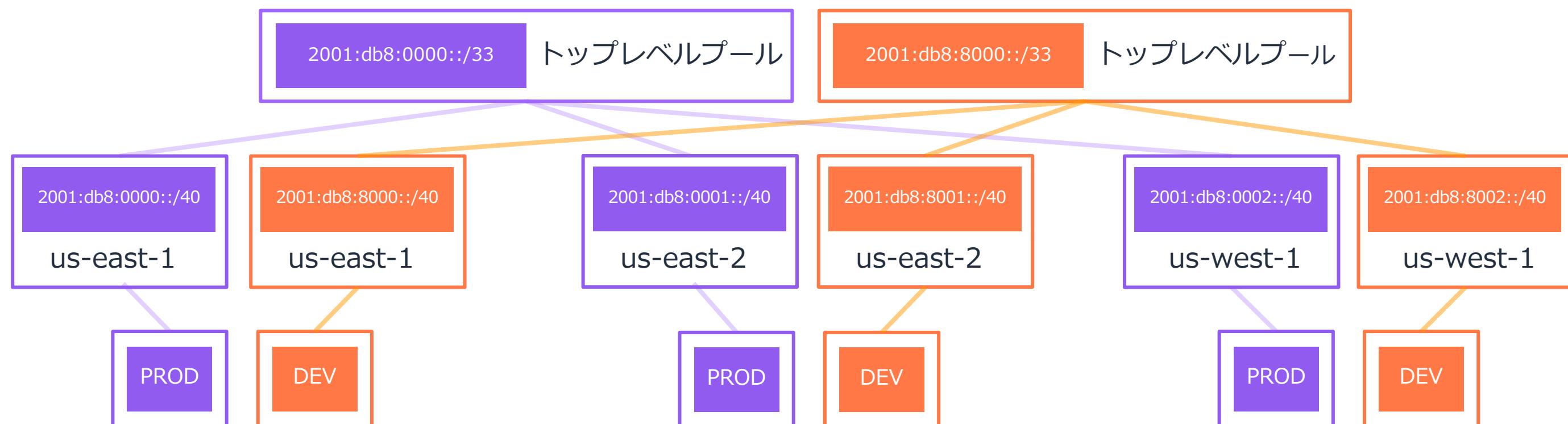
パブリックにアドバタイズ可能にすることを許可する
(インターネットまたは DX 経由で経路広告)

- ROA が必要 (インターネット経由の場合)
- プール内の最小 CIDR 長: /48

--no-publicly-advertisable

パブリックにアドバタイズ可能にすることを許可しない
(DX 経由でのみ経路広告)

- ROA が不要
- プール内の最小 CIDR 長: /56



※ DX: Amazon Direct Connect, ROA: Route Origin Authorization