



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

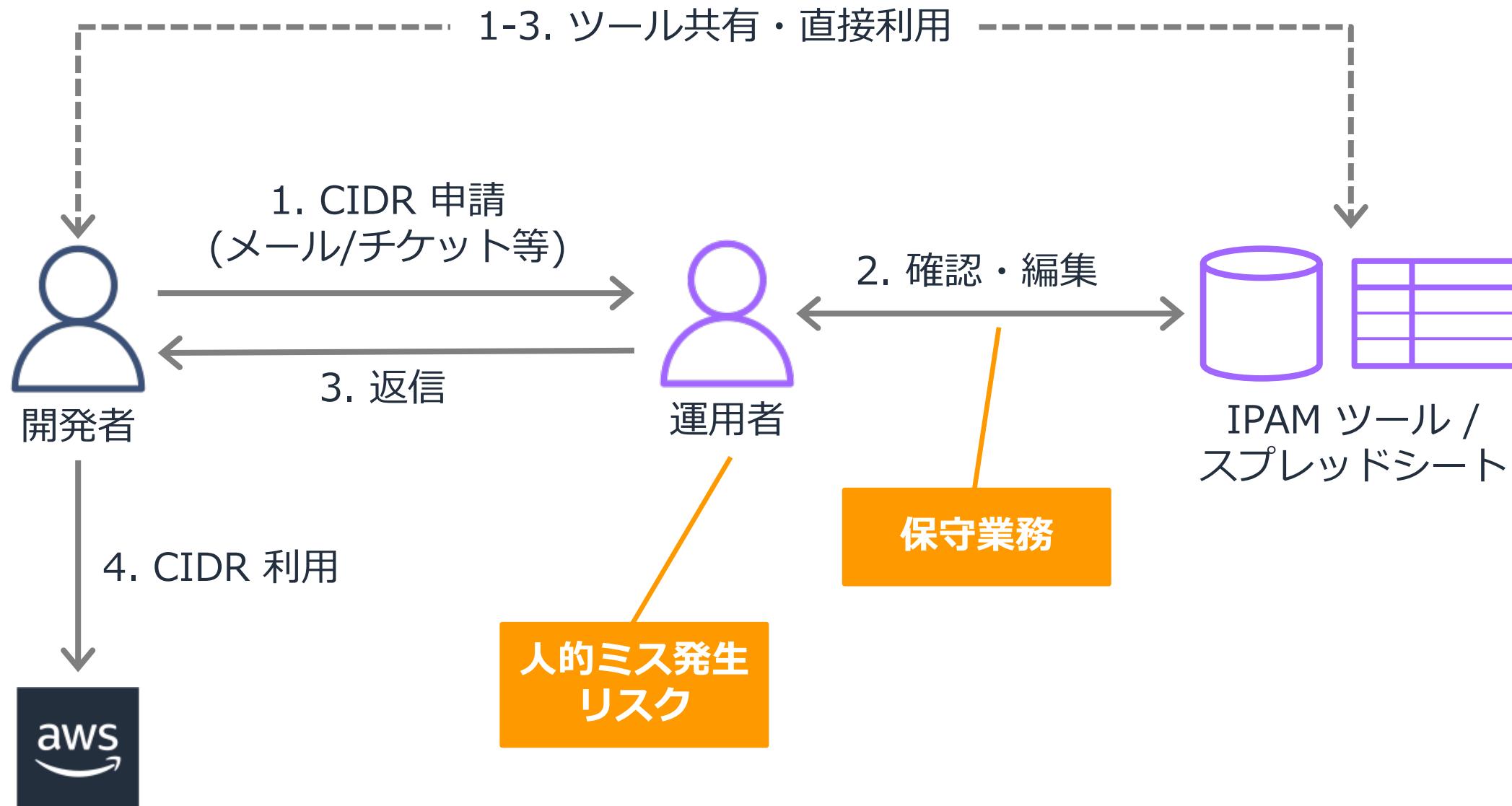
- サービス登場の背景 – IPAM 登場以前の課題
- サービス概要
- サービス導入方法・使い方
 - A. 新規環境への導入
 - B. 既存環境への導入
- クオータ・料金
- まとめ

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

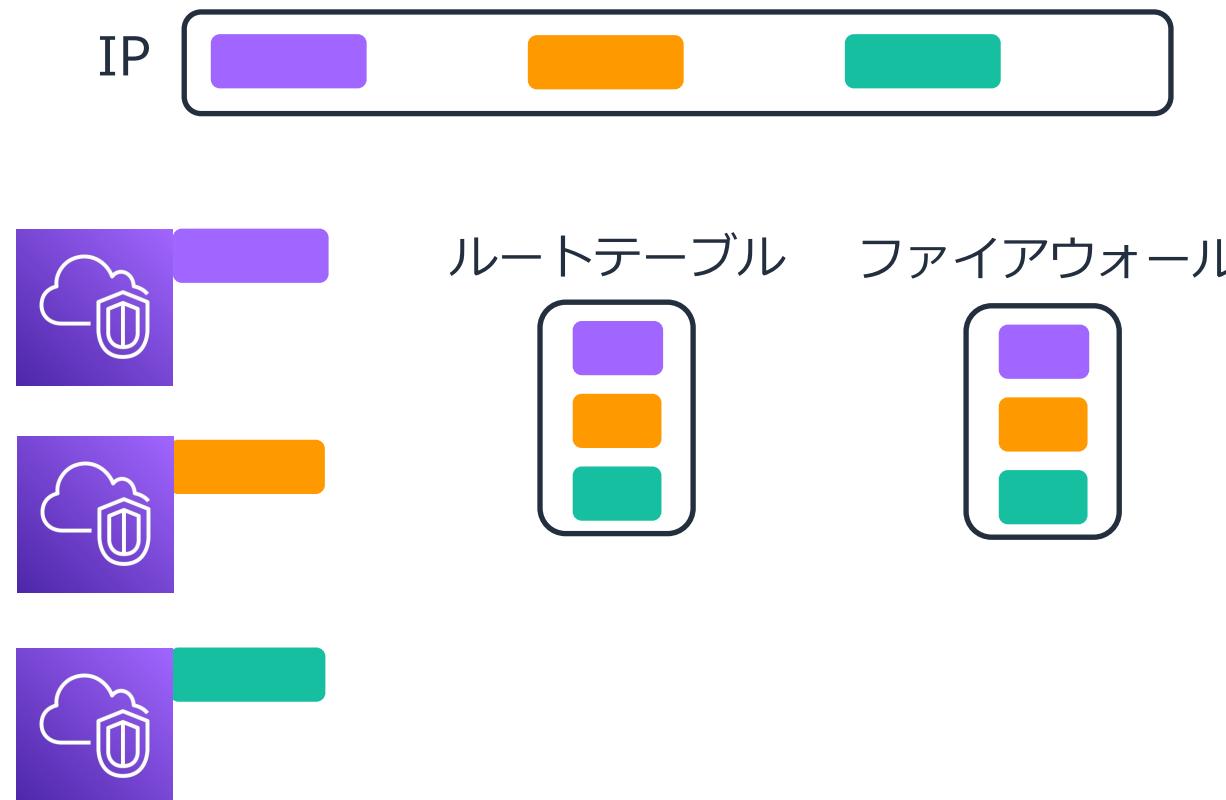
運用者の負担大、管理コストがかかる、人的ミス発生のリスクあり



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**

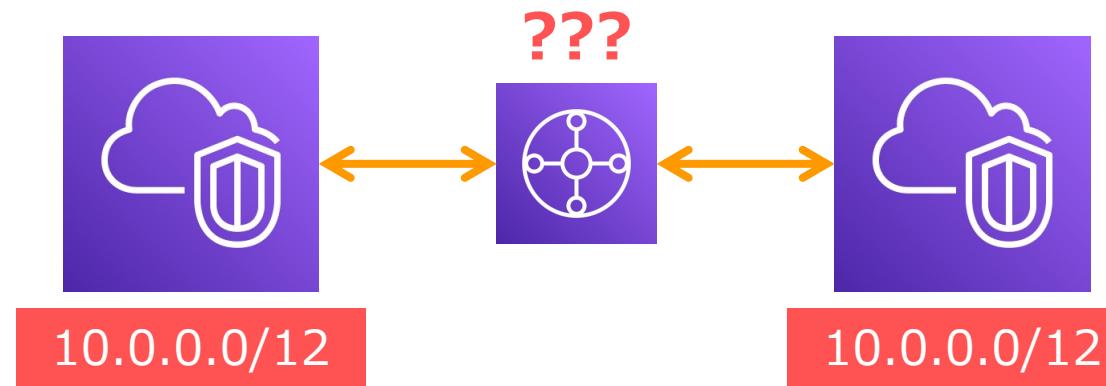
課題 3. IP アドレスのモニタリングが困難

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

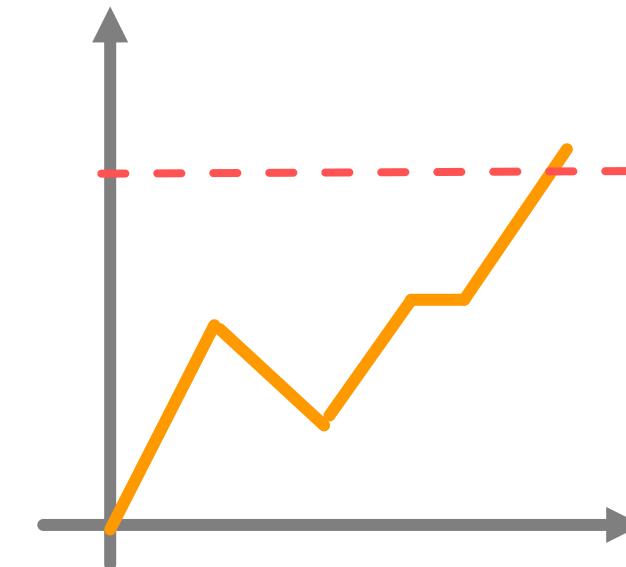
重複した CIDR が放置される可能性



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

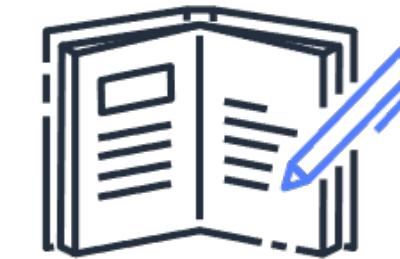
トラブルシュート



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

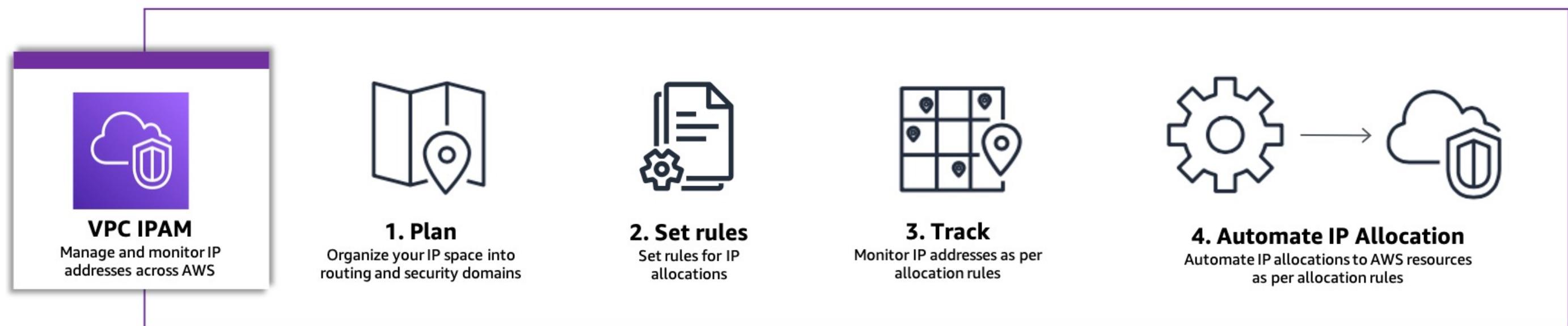
本セッションの流れ（再掲）

- 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

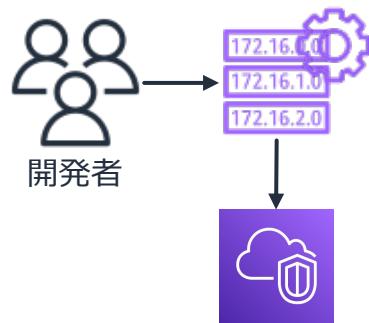
- 大規模ネットワークにおいて、**CIDR を自動的に割り振り**
 - スプレッドシート等によるマニュアル管理が不要になり、アドレス割り当て業務の手間やミスを回避
- **IP アドレス利用のモニタリング、過去に遡った分析、監査**にも対応
- AWS Organizations や AWS Resource Access Manager との連携も可能
- 料金はアクティブな IP アドレス分だけの**従量課金**



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

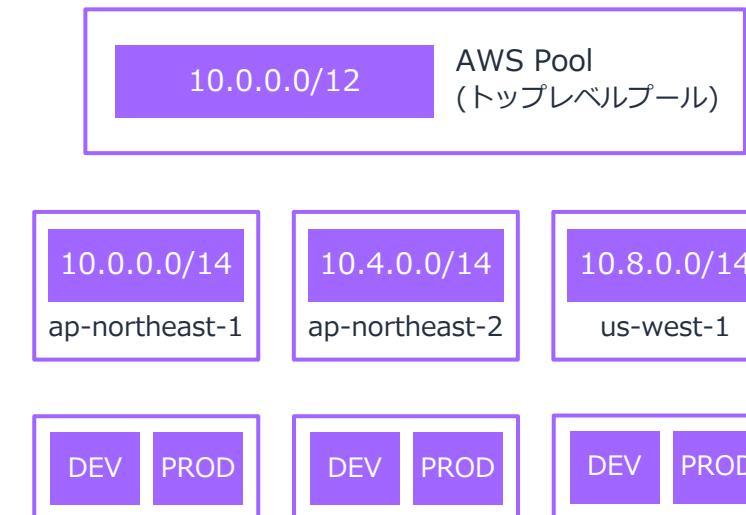
3 ステップで構築します

1 | IPAM の作成



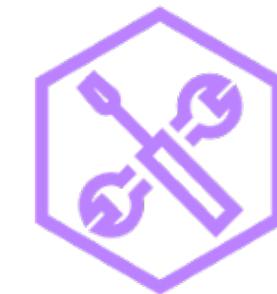
単独の IPAM で
複数リージョン・アカウント管理

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

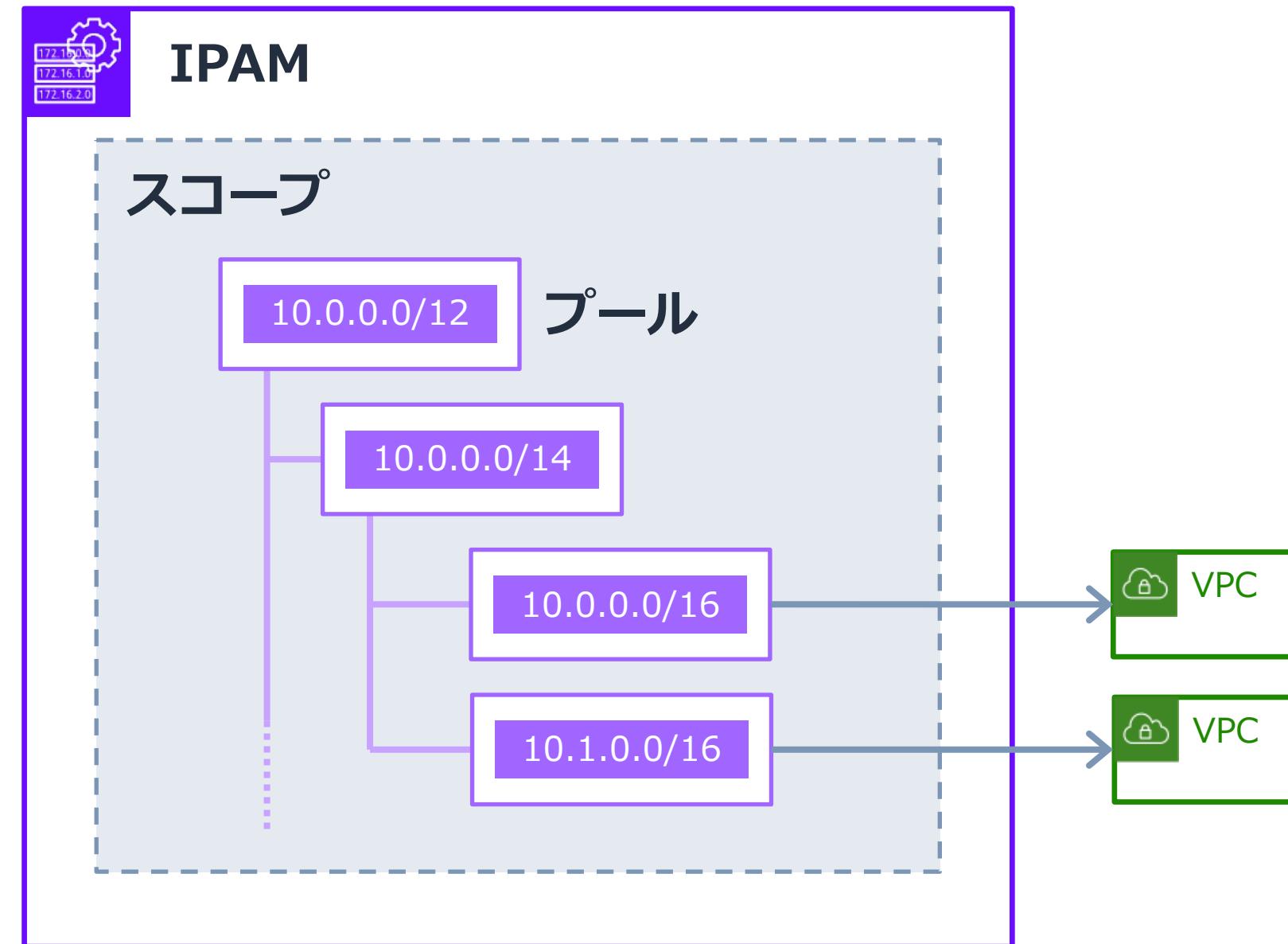


特定の CIDR を使えるアカウントや、
リージョンを制限

プールの作成・編集時に指定

IPAM の基本概念

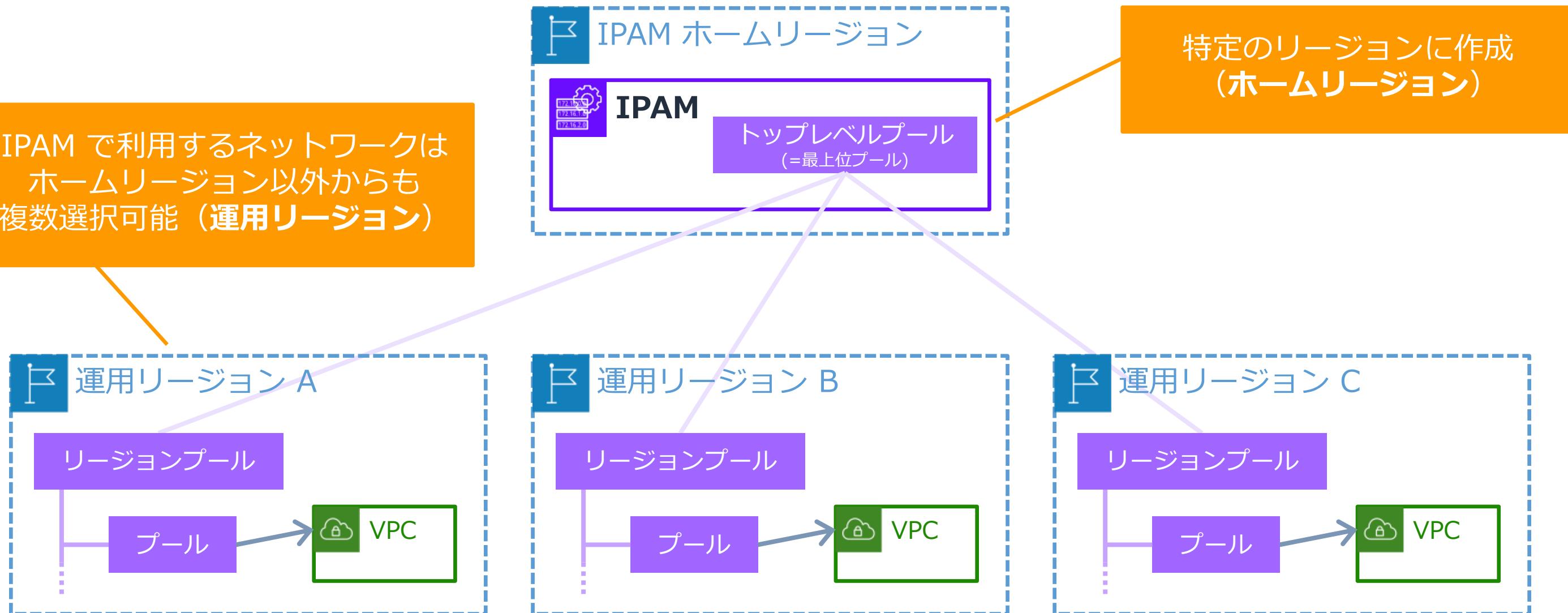
階層構造にある「IPAM」 「スコープ」 「プール」 の 3 つが重要



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

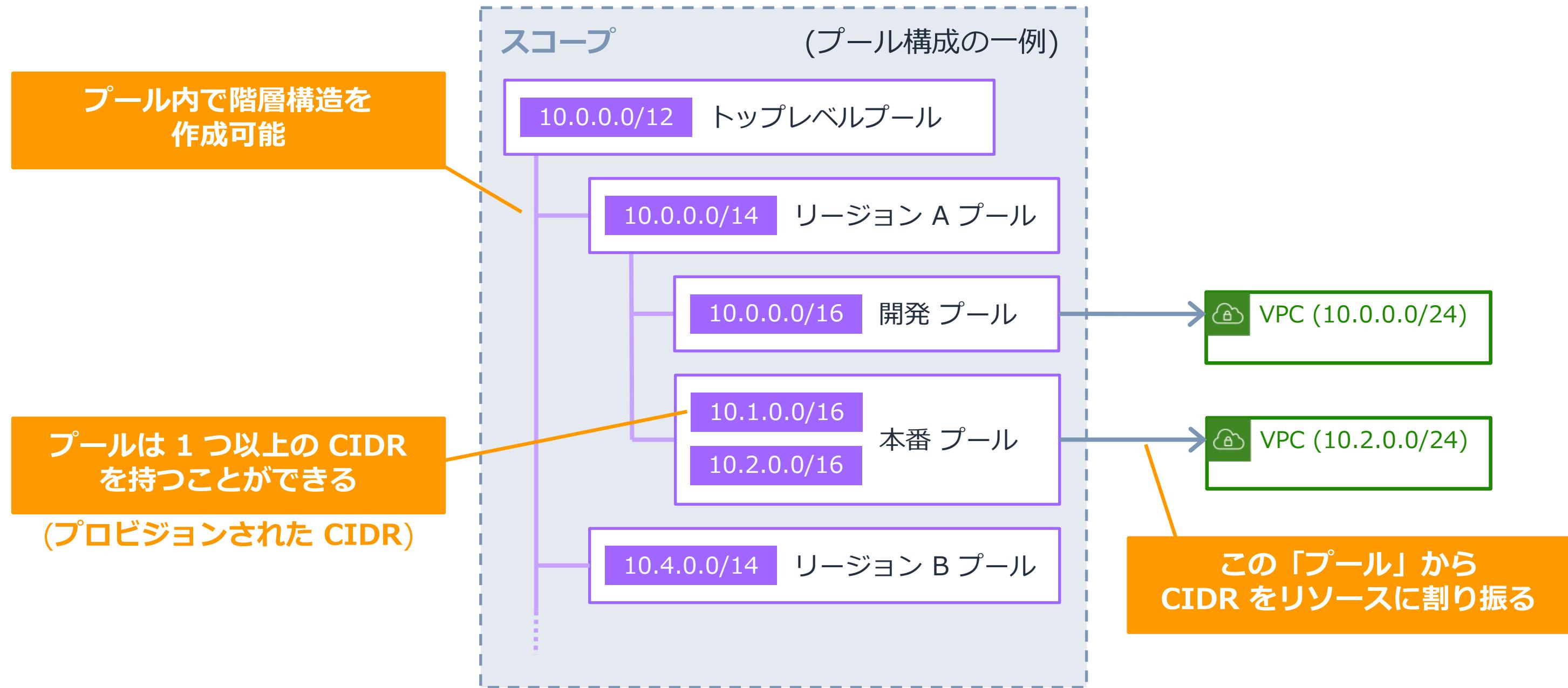
- パブリックスコープ・プライベートスコープの 2 種類が存在
- IPAM 作成時に、1 つずつデフォルトで作成される

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。

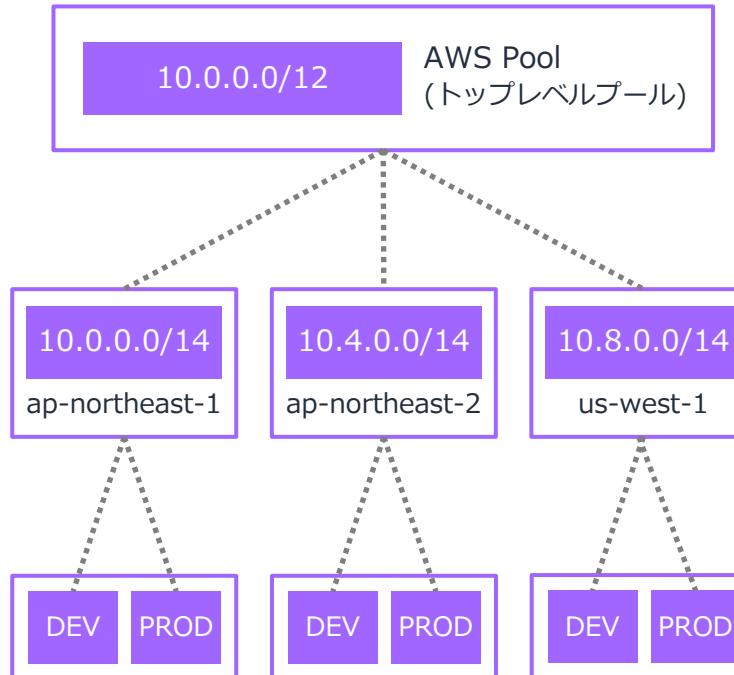
新しいタグを追加

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

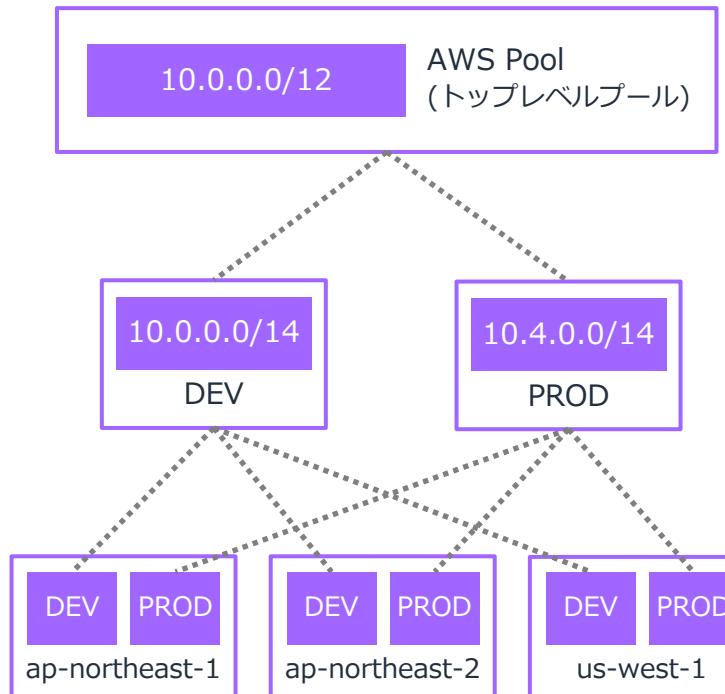
例 1

リージョンごとに統合して管理



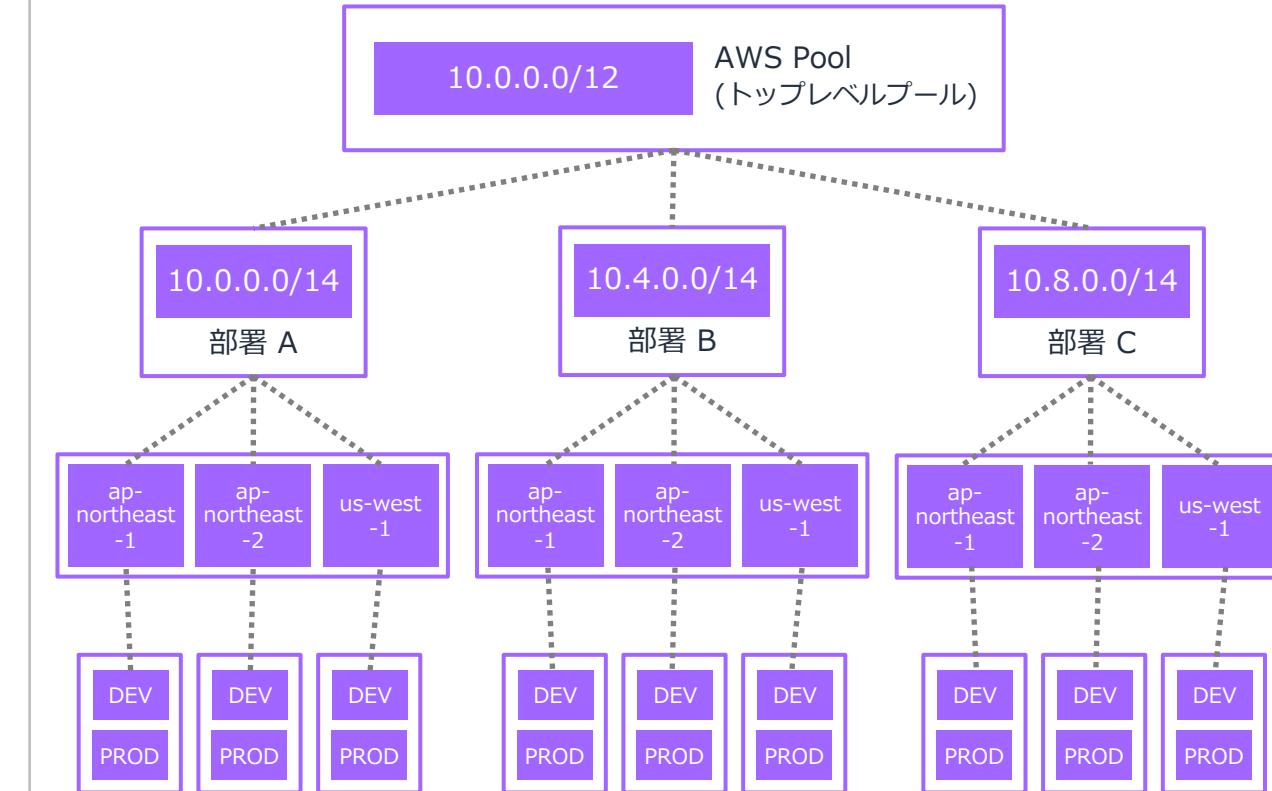
例 2

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

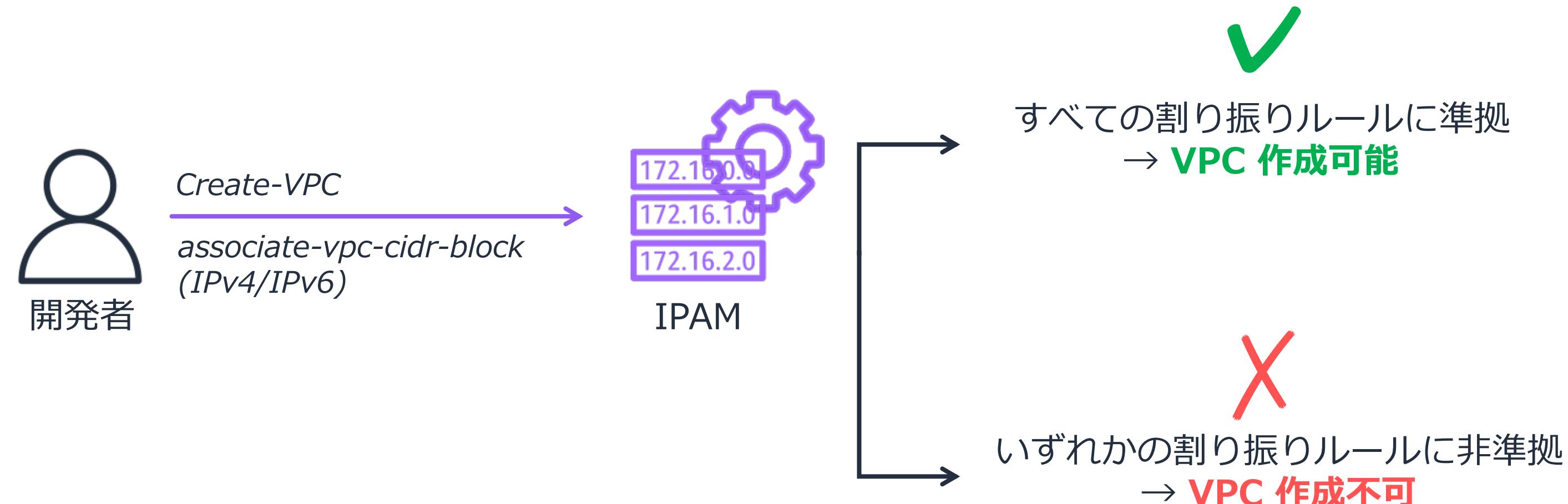
割り振りルール設定 | 仕組み

IPAM 作成

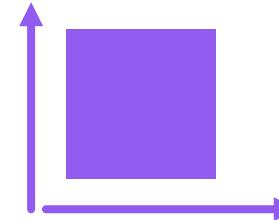
IP 空間設計

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

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ケ

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
```



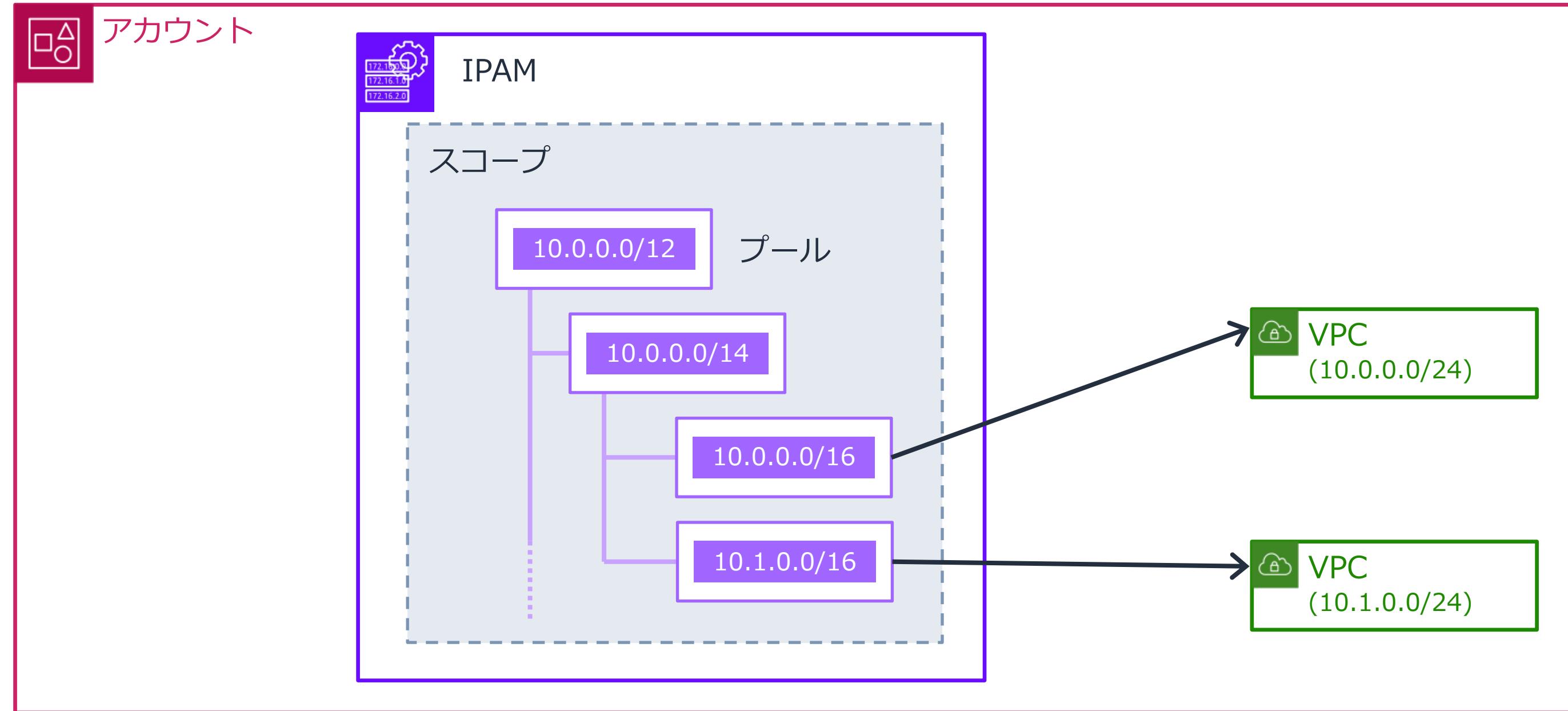
```
{
  "IpamPoolAllocation": {
    "Cidr": "10.0.0.0/24",
    "IpamPoolAllocationId": "ipam-pool-alloc-018ecc28043b54ba38e2cd99943cebfbd",
    "ResourceType": "custom",
    "ResourceOwner": "123456789012"
  }
}
```

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

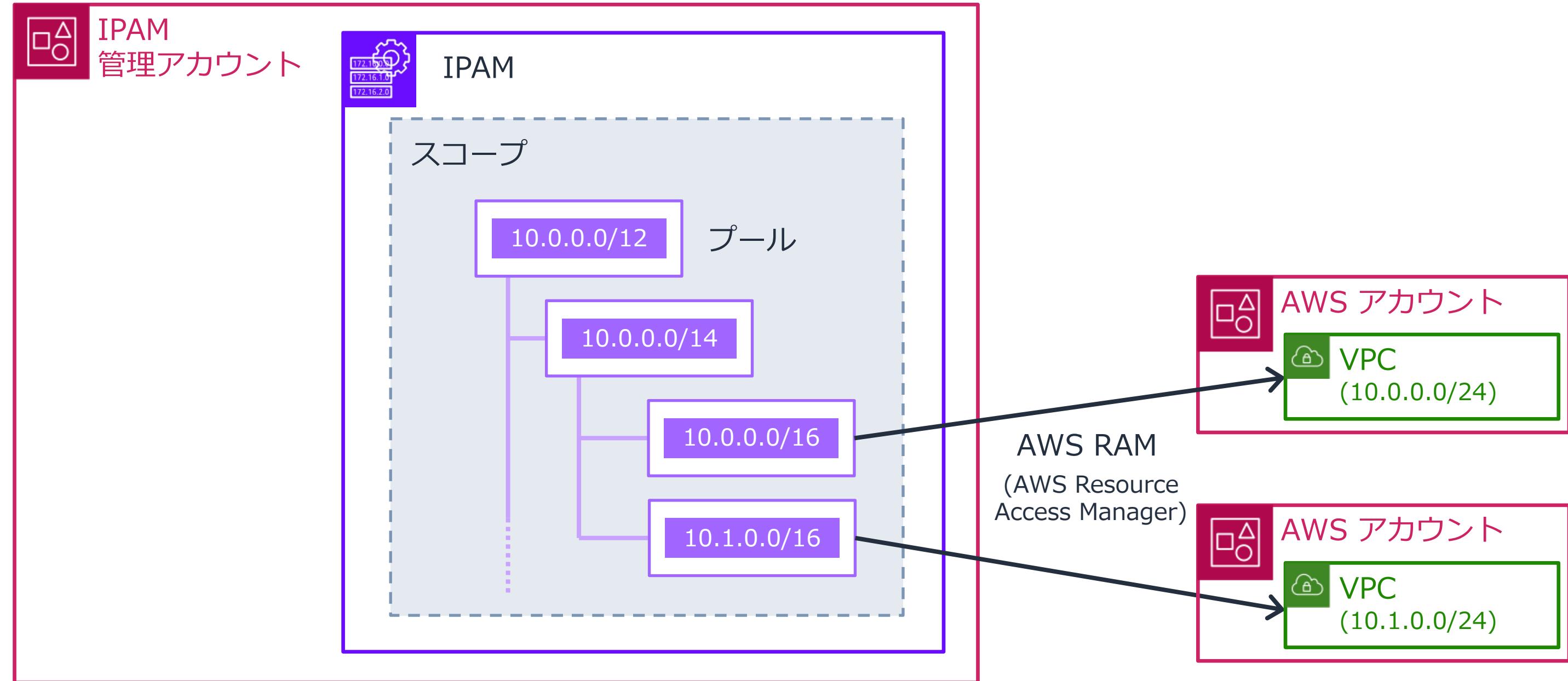
IPAM 利用イメージ | 単独アカウントの場合

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:

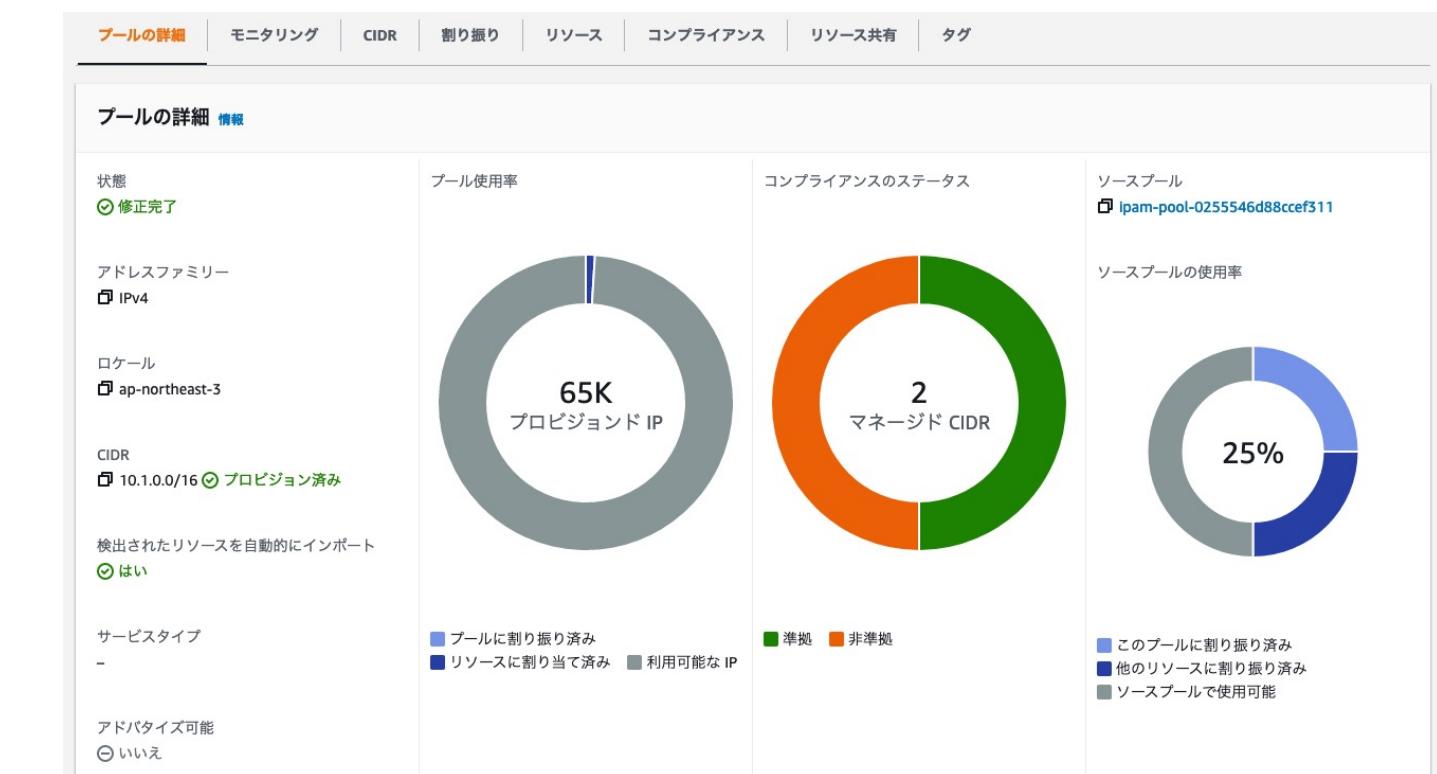
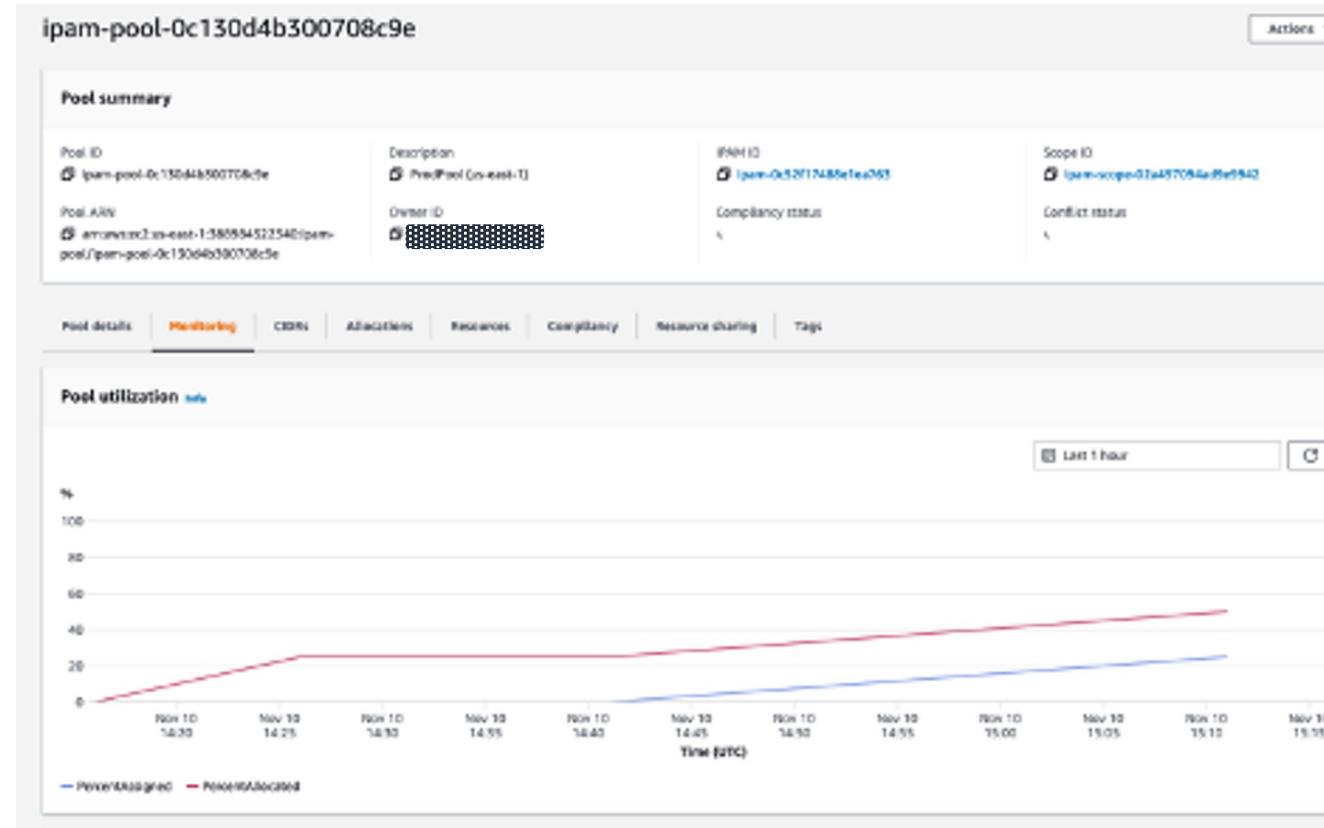
- A yellow box highlights the 'Compliance Status' column header and the first few rows.
- A purple box highlights the 'Redundancy Status' column header and the last few rows.
- Two specific rows are circled with purple boxes:
 - The first circled row shows 'dx-lab-test-vpc' with two red 'Duplicate' markers 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

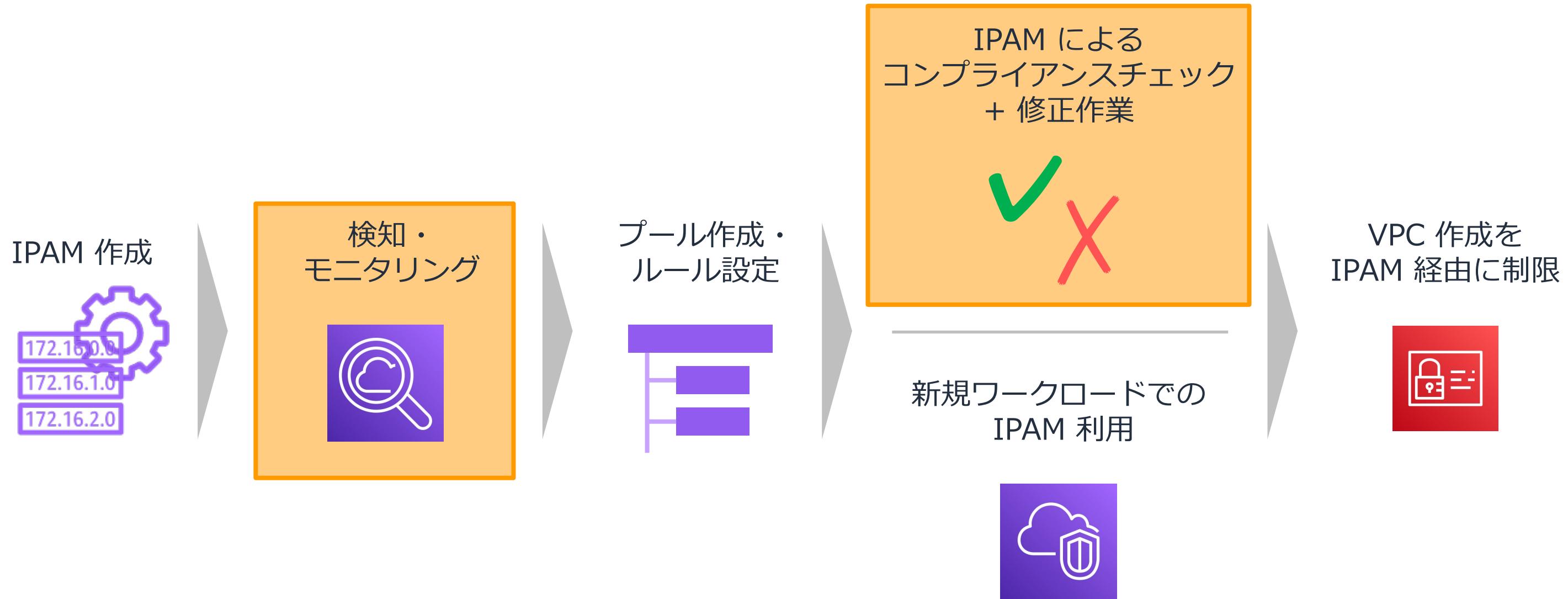
- サブネット
- VPC
- Elastic IP
- EC2 インスタンス
- ENI

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

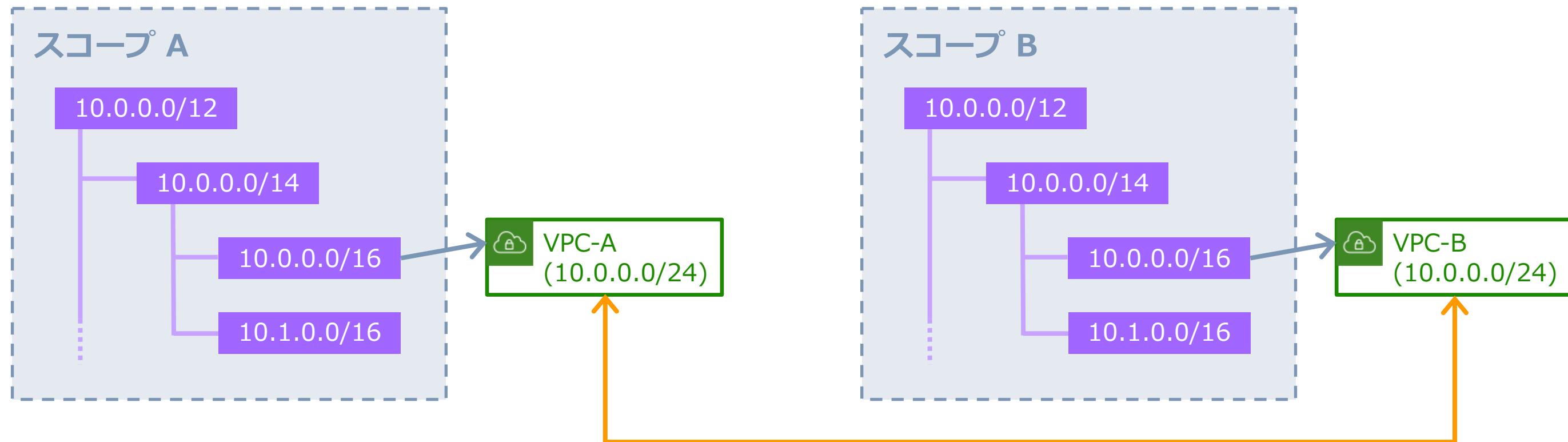
「2つのVPCを相互接続する予定の有無」により対処法が異なる

- 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

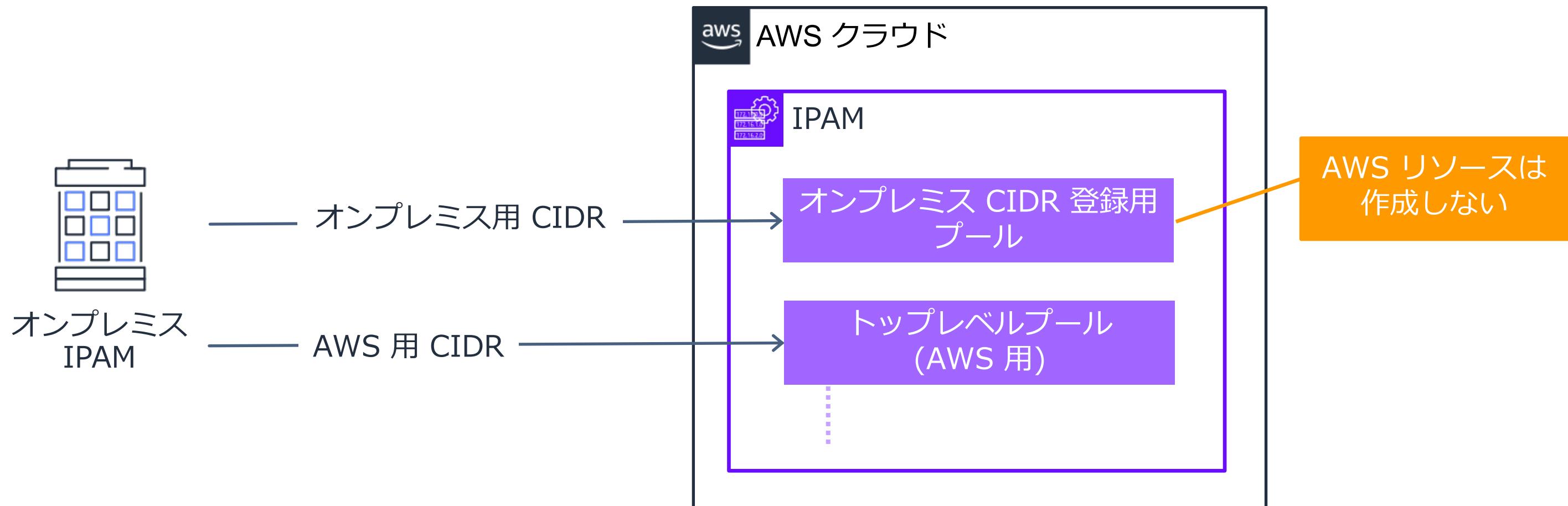
リソース ID コンプライアンスのス... 重複ステータス リソース名 IP 使用状況 CIDR リージ...

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

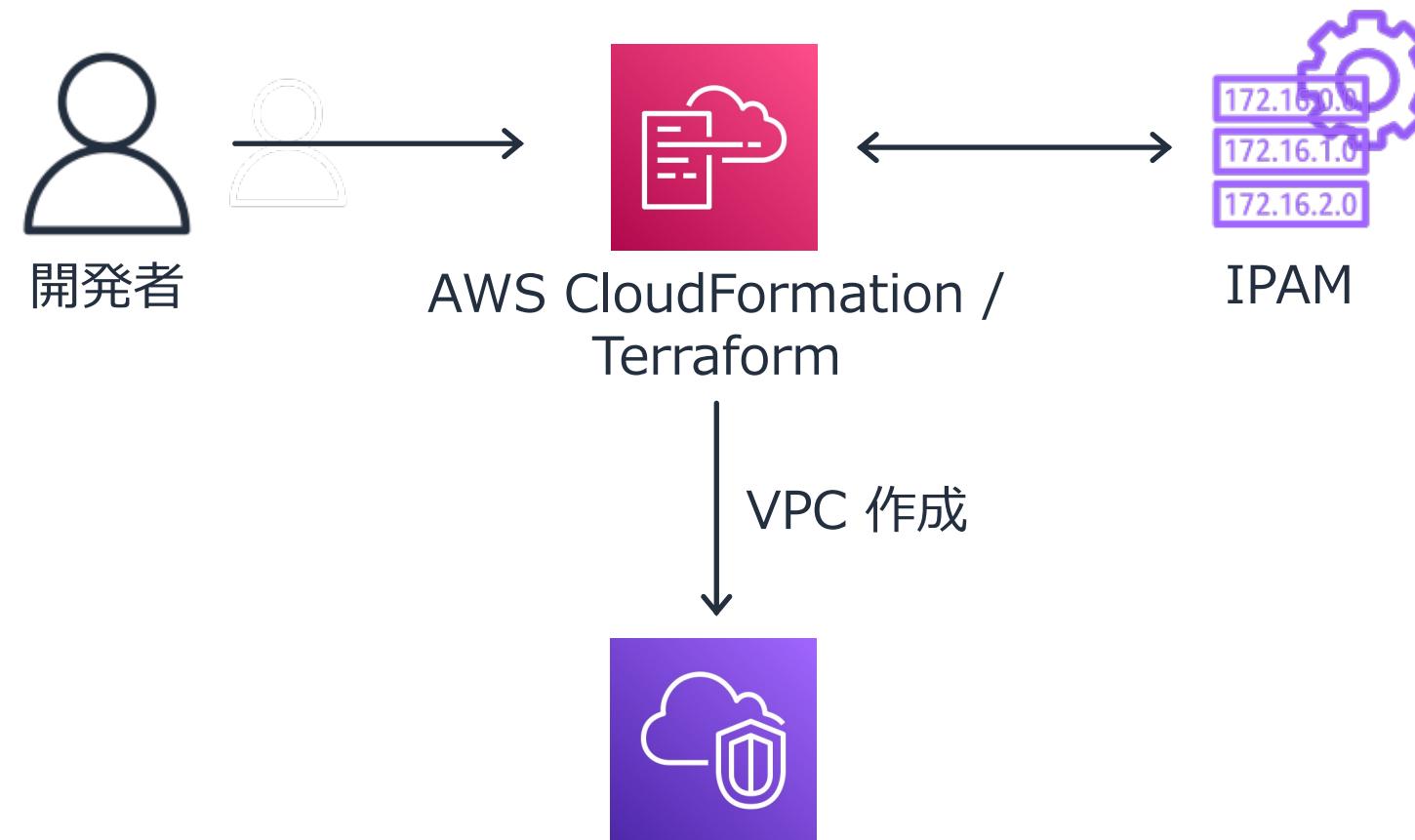
オンプレミス IPAM とのハイブリッド運用

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

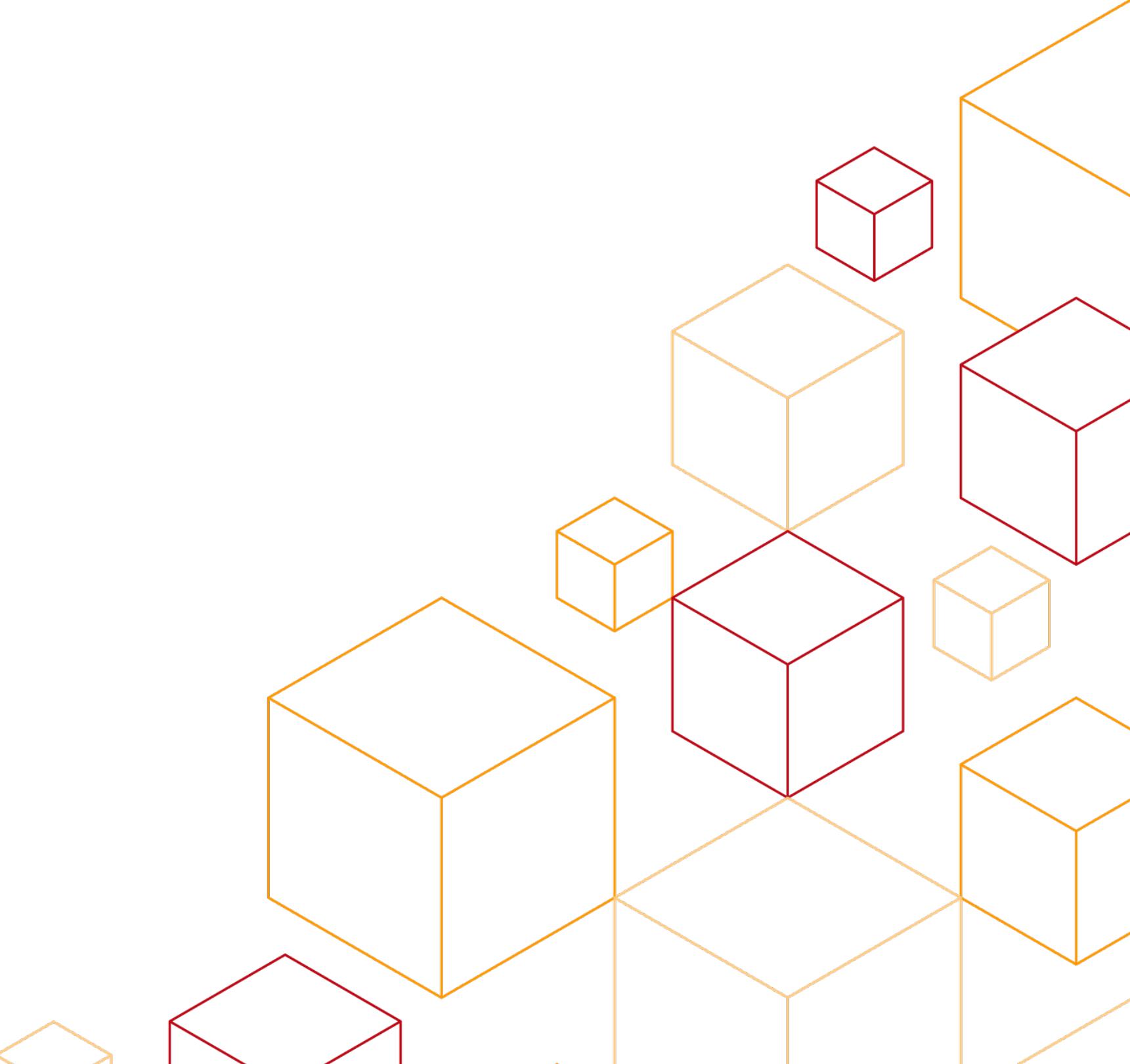
- Amazon VPC IP Address Manager (IPAM) は
VPC の IP アドレスを整理し、割り当て状態を管理できるサービス
 - 大規模ネットワークで CIDR を自動で割り当てることが可能
 - スプレッドシートなどによる手動管理が不要
 - アドレス割り当て業務の手間やミスを回避可能
 - CIDR 割り当てに対するルール設定
- IP アドレス利用状況のモニタリングや、過去に遡った分析に対応
 - トラブルシュートや監査に活用可能
- AWS Organizations や AWS Resource Access Manager との連携により
複数アカウント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

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)



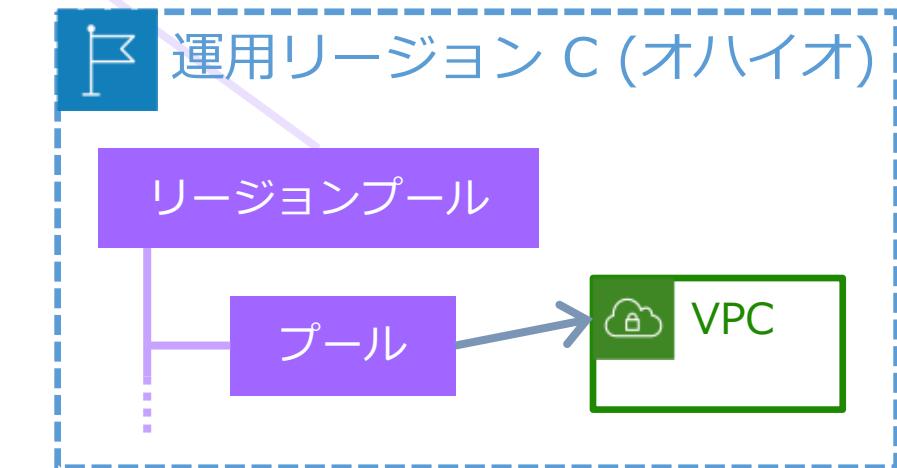
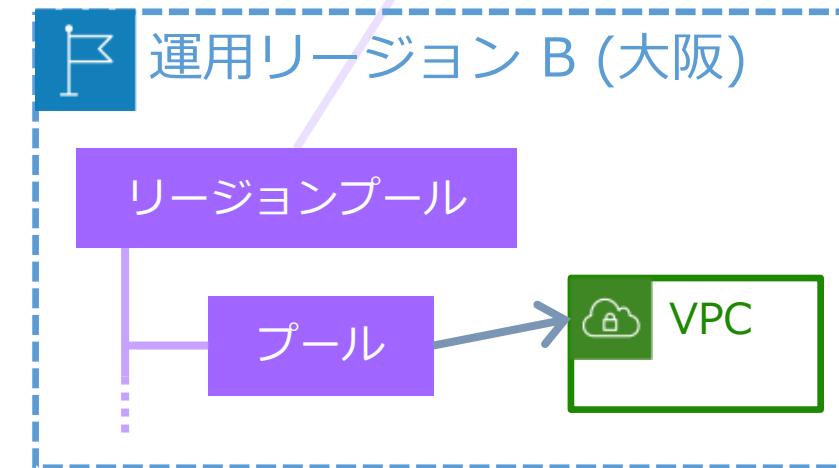
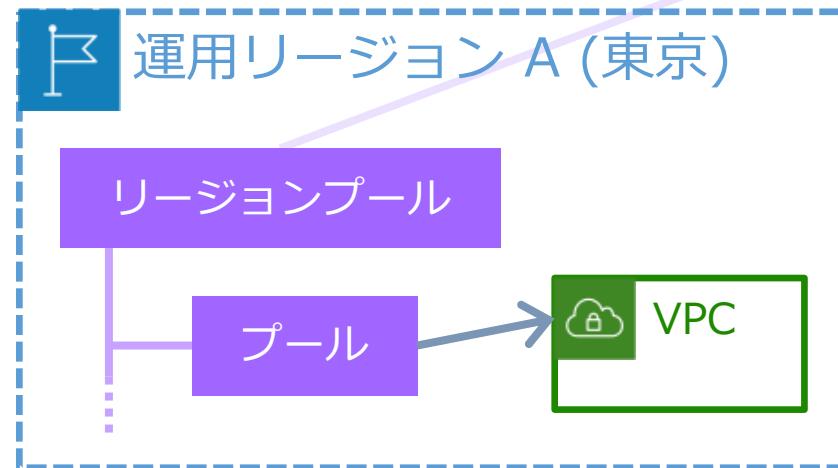
補足



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

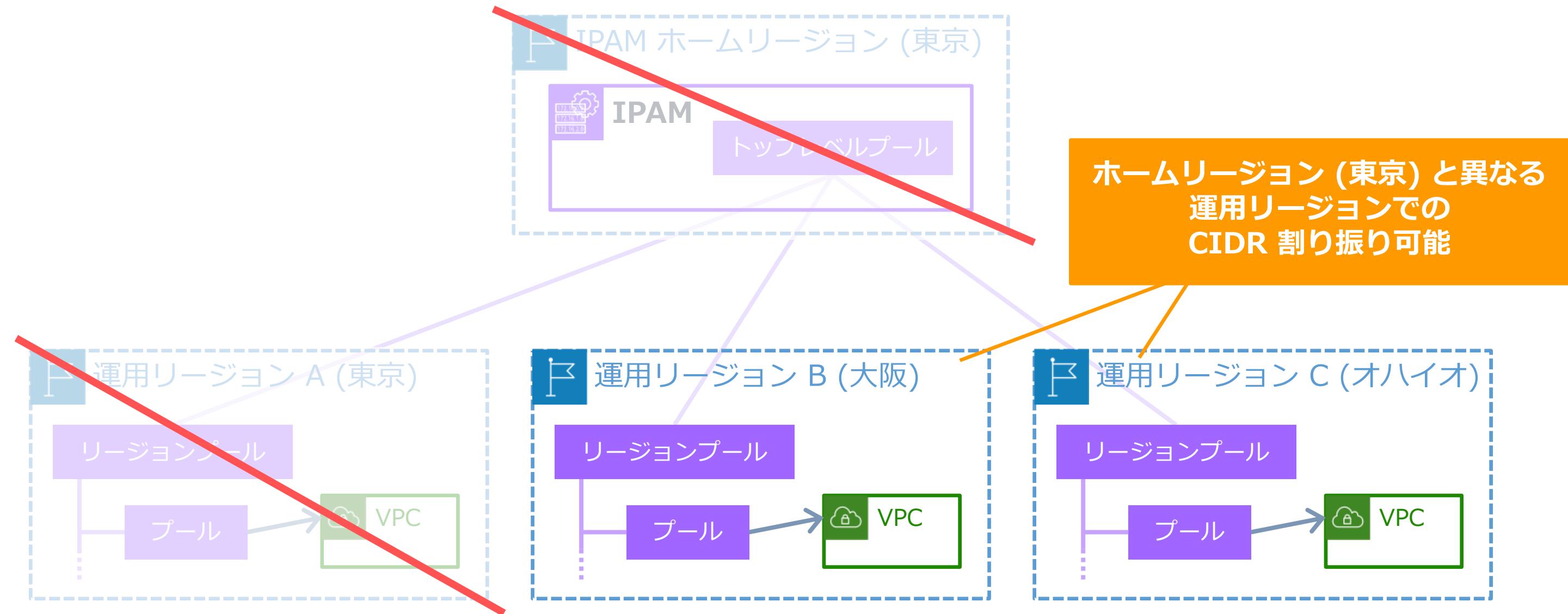
各運用リージョン内のプールは、別リージョンに非依存



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

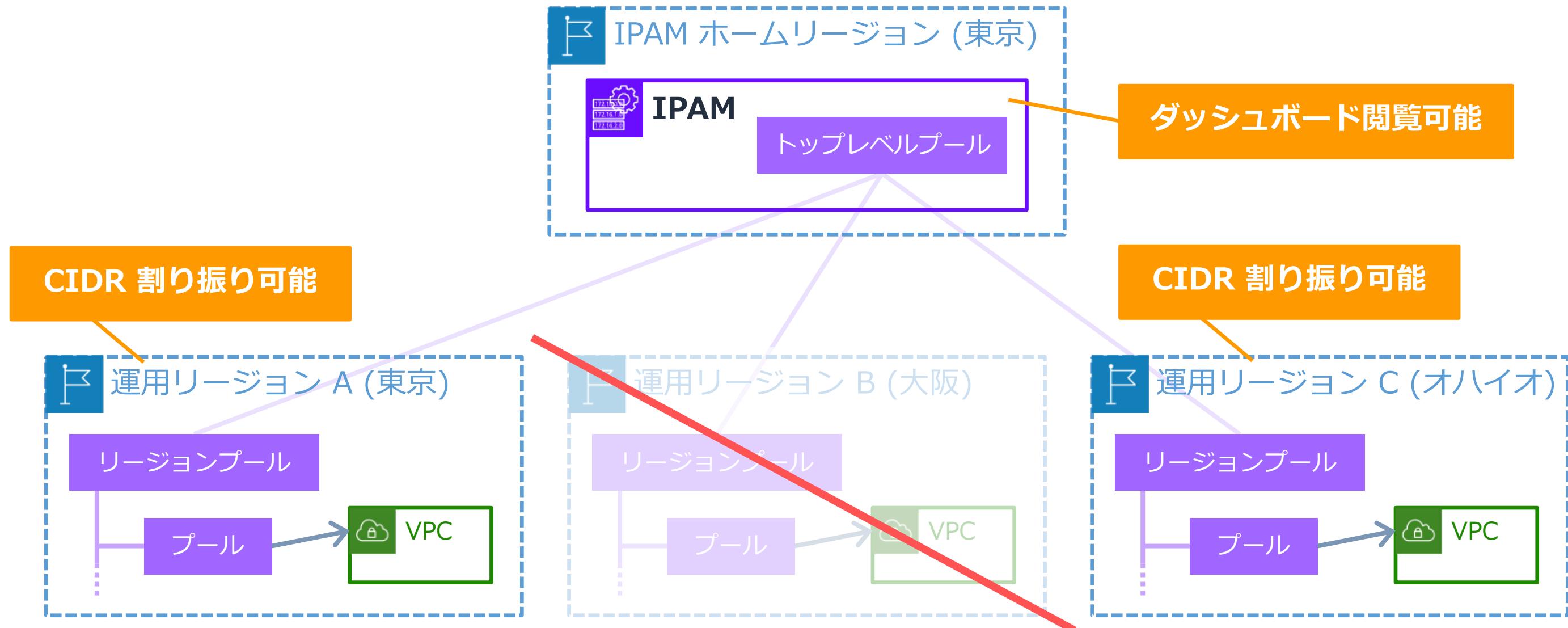
IPAM のリージョンと可用性 | シナリオ 1

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

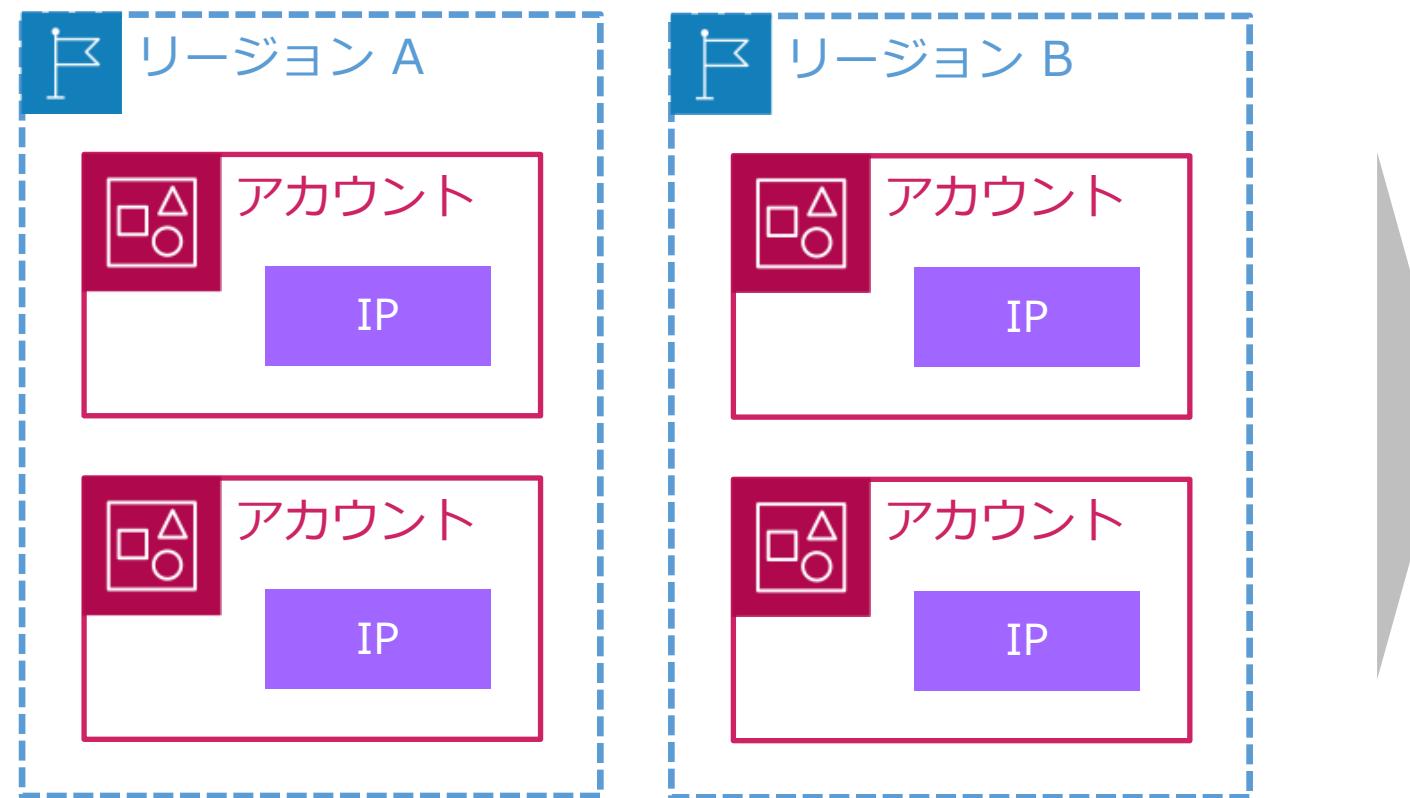
ある運用リージョンが利用できなくなった場合 → その他のリージョンは平常



BYOIP | アドレスのアカウント間共有

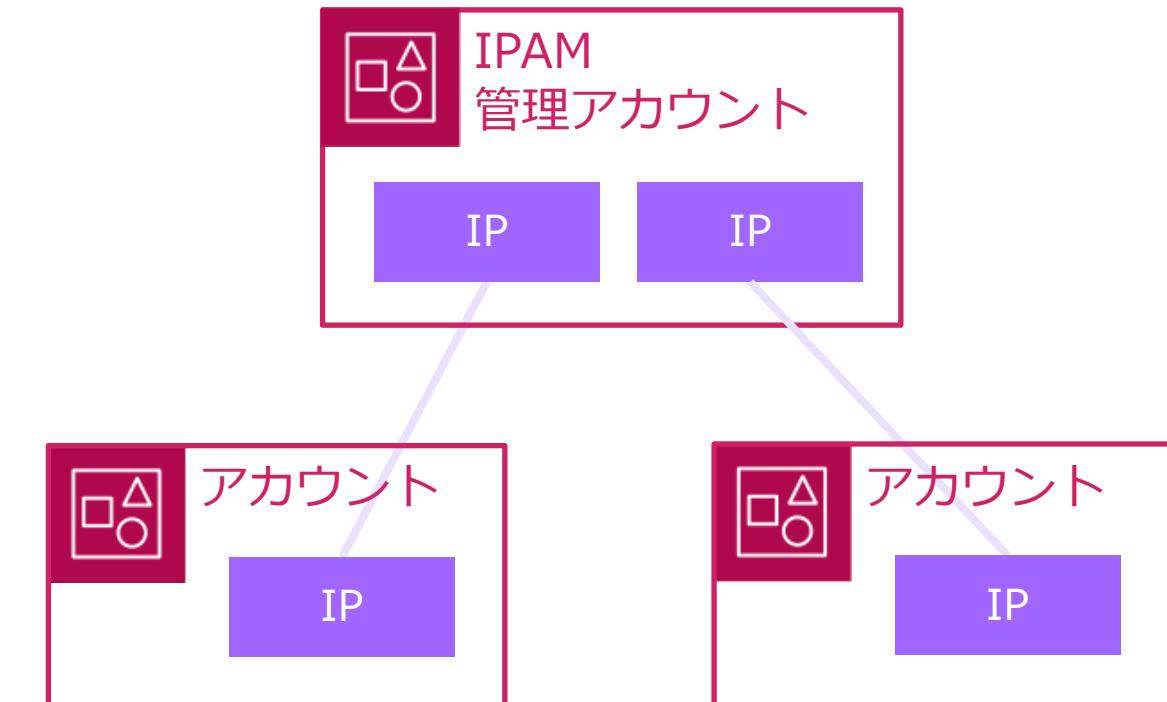
BYOIP したアドレスの利用開始手順を簡素化可能

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

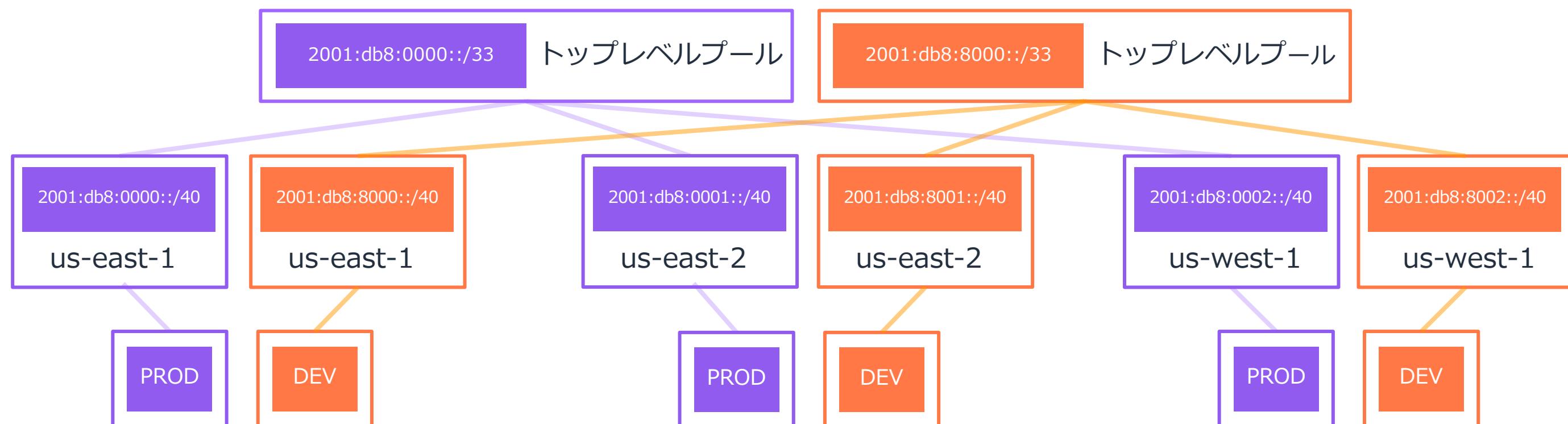
パブリックにアドバタイズ可能にすることを許可する
(インターネットまたは DX 経由で経路広告)

- 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