

IPAM は適応されたサービス用ロールを介して、あらかじめ指定した複数リージョンにおける VPC/Subnet の IP アドレス使用状況情報を 1 か所のリージョンに集約します。情報が集約されるリージョンのことを Operating Region と呼びます。AWS Organization との連携により、複数 AWS アカウントの情報を 1 か所に集約することも可能です。

- **IPAM operating in AWS Region 1 and AWS Region 2**
  - Private scope
    - Top-level IPAM pool
      - Regional IPAM pool in **AWS Region 2**
        - Development pool
          - Allocation for a VPC in **AWS Region 2**

1. 作業を行う Operating Region を決定し、Amazon VPC IP Address Manager のマネージメントコンソールにアクセスします



2. [IPAM を作成]をおします。複数 AWS アカウント、複数リージョンにおける VPC の IP アドレス使用状況を管理する台帳です。
3. [データレプリケーションを許可]にチェックをつけます

#### 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。

4. [名前]に[Global]と入力し、[運用リージョン]で[すべてのリージョンを選択]にチェックをつけます。注意：ここで指定に含まれたリージョンの VPC で現在使われている EC2 (EIP) や ENI の IP がすべて管理可能となり課金対象となるため、商用環境など大量の IP アドレスを利用しているリージョンは除いてください。

5.

#### 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。

Top

#### 説明 - オプション

IPAM の簡単な説明を記述します。

Top

#### 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 ▼

アジアパシフィック (東京) - ap-northeast-1 ✕

アジアパシフィック (ソウル) - ap-northeast-2 ✕

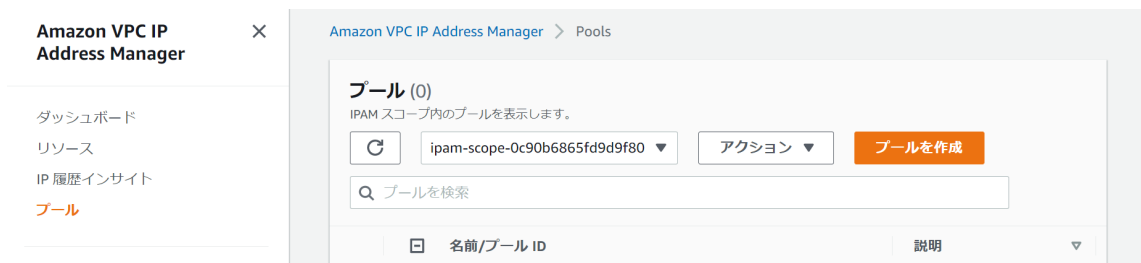
アジアパシフィック (大阪) - ap-northeast-3 ✕

6. [IPAM を作成]ボタンをおします

今までの手順で、Global な管理台帳が作成されました。ここから IP アドレスの管理プールを 3 階層作成します。それぞれ Top レイヤ（複数リージョン、複数アカウント）、Regional レイヤ（単一リージョン、単一アカウント）、特定 VPC レイヤ（単一 VPC）を管理する Pool を作成していきます。

- **IPAM operating in AWS Region 1 and AWS Region 2**
  - Private scope
    - Top-level IPAM pool
      - Regional IPAM pool in **AWS Region 2**
        - Development pool
          - Allocation for a VPC in **AWS Region 2**

7. 左ペインから[プール]をクリックし、[プールの作成]をクリックします。



8. [名前タグ]に Top と入力します

**プールの設定**

IPAM ID

ipam-0d706d324b2fc37cb (Global)

スコープ ID

ipam-scope-0c90b6865fd9d9f80

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。プールが共有されていても、タグは他のアカウントには表示されません。

Top

説明 - オプション

プールの簡単な説明を記述します。

VPC 用のプール

9. 以下の Pool 階層はデフォルトのまま作業を進めます。後ほど 2 次プール、3 次プールの作成では指定します。

**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

10. [新しい CIDR を追加]をおして、[10.0.0.0/8]を入力します

**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。


10.0.0.0/816M IPs削除

<>^v

新しい CIDR を追加

11. [Configure this pool's allocation rule settings]にチェックをつけます

**割り振りルール設定 - オプション** 情報

 **AWS best practice**  
We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize IPAM pools, see [Example IPAM pool plans](#).

☒ Configure this pool's allocation rule settings

12. 以下のように Netmask Compliance に全て/16 を指定します。これにより、2 次プールは/16 のアドレス空間のみが作成可能となります。

## Netmask compliance

### 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。

/16 (65K 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。

/16 (65K IPs)

### 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。

/16 (65K IPs)

13. [プールの作成]をおします
14. 作成が完了したら、プール詳細画面の[CIDR]タブをクリックします。10.0.0.0/8 が管理配下になったことがわかります。（作業完了まで数分間かかりますのでしばらく待ちます）

[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](#)

**CIDR (1) 情報** [CIDR のプロビジョンを解除](#) [CIDR をプロビジョン](#)

🔍 結果をフィルタリング [1](#) ⚙️

<input type="checkbox"/>	CIDR	▼	状態	▼
<input type="checkbox"/>	10.0.0.0/8		🟢 プロビジョン済み	

**プールの詳細 情報**

**状態**  
🟢 作成完了

**アドレスファミリー**  
📄 IPv4

**ロケール**  
📄 None

**CIDR**  
📄 10.0.0.0/8 🟢 プロビジョン済み

検出されたリソースを自動的にインポート  
🔍 いいえ

**プール使用率**

16M  
プロビジョンド IP

☒ プールに割り振り済み  
☒ リソースに割り当て済み  
☒ 利用可能な IP

**コンプライアンスのステータス**  
このプールにはリソース CIDR がありません。

**ソースプール**  
-

**ソースプールの使用率**  
-

15. 再度[プールの作成]をおして 2 次プール（Region 用）を作成します。 ここで指定する

リージョンは、10.0.0.0/8 IP アドレス帯の VPC が存在しないリージョンを選択してください。すでに存在している VPCIP アドレス帯と 10.0.0.0/8 が重複する場合、エラーとなります。(10.0.0.0/24 や 10.0.0.0/16 も 10.0.0.0/8 の中に含まれているので重複します)

16. Tokyo 等後ほど VPC を作成するリージョンの名前を入力します

次でプールを作成: ipam-scope-0c90b6865fd9d9f80

### プールの設定

IPAM ID ipam-0d706d324b2fc37cb (Global)	スコープ ID ipam-scope-0c90b6865fd9d9f80
--	---

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。プールが共有されていても、タグは他のアカウントには表示されません。

Tokyo

説明 - オプション  
プールの簡単な説明を記述します。

VPC 用のプール

17. プール階層で先程作成した[Top]を選択します

### 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。

Top (ipam-pool-06b55a6efbb096cde) ▼

### ソースプールの概要

CIDR 10.0.0.0/8  プロビジョン済み	プール ID ipam-pool-06b55a6efbb096cde
プロビジョンド IP アドレス 16M	名前 Top

18. [ロケール]で後ほど VPC を作成するリージョンを選びます

ロケール  
このプールを常駐させるロケールを選択します。ロケールは、ソースプールのロケールが [なし] の場合にのみ変更できます。

ap-northeast-1 ▼

19. [プロビジョンする CIDR]で[特定の CIDR を追加]をおします

**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。

特定の CIDR を追加サイズ別に CIDR を追加

20. [10.0.0.0/16]を入力します

**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。

65K IPs削除

<>^v

特定の CIDR を追加サイズ別に CIDR を追加

21. [Configure this pool's allocation rule settings]にチェックを付けます
22. [検出されたリソースを自動的にインポート]にチェックを付けます。これにより既存及び新規作成された VPC の IP アドレス情報が IPAM 上で確認できるようになります。

**CIDR management**

**Automatically import discovered resource**

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。

☒ 検出されたリソースを自動的にインポート

☐ Don't allow

23. [Netmask Compliance]に[/24]を指定します。3 次プール（VPC 用）に/24 を割り振ることが出来るようになります。

**Netmask compliance**

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。

/24 (256 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。

/24 (256 IPs) ▼

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。

/24 (256 IPs) ▼

24. [プールを作成]をおします
25. 以下の通り 2 次プールが作成されています

Amazon VPC IP Address Manager > Pools

**プール (2)**  
IPAM スコープ内のプールを表示します。

🔄 ipam-scope-0c90b6865fd9d9f80 ▼ アクション ▼ **プールを作成**

🔍 プールを検索

	名前/プール ID	説明	CIDR
○	📁 Top (ipam-pool-06b55a6efbb096cde)	-	📦 10.0.0.0/8 ✓
○	📁 Tokyo (ipam-pool-08e6832e88c38f929)	-	📦 10.0.0.0/16 ✓

26. ここから個別 VPC 用の 3 次プールを作成します。なおこのハンズオンの手順は以下の構造に従っていますが、階層構造は自由です。プロジェクト用プールの下に、個別リージョンごとのプールを作成することも可能です。単一プールの下に複数 VPC を割り当てることも可能です。

- **IPAM operating in AWS Region 1 and AWS Region 2**
  - Private scope
    - Top-level IPAM pool
      - Regional IPAM pool in **AWS Region 2**
        - Development pool
          - Allocation for a VPC in **AWS Region 2**



27. [プールを作成]をおして、名前に[Dev]と入力します

次でプールを作成: ipam-scope-0c90b6865fd9d9f80

### プールの設定

IPAM ID ipam-0d706d324b2fc37cb (Global)	スコープ ID ipam-scope-0c90b6865fd9d9f80
--	---

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。プールが共有されていても、タグは他のアカウントには表示されません。

Dev

説明 - オプション  
プールの簡単な説明を記述します。

VPC 用のプール

28. 2 次プール（Region 用）を指定します

### 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。

Tokyo (ipam-pool-08e6832e88c38f929) ▼

#### ソースプールの概要

CIDR 10.0.0.0/16  プロビジョン済み	プール ID ipam-pool-08e6832e88c38f929
-------------------------------	---------------------------------------

29. [特定の CIDR を追加]をおし、[10.0.0.0/24]を入力します

### 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。


10.0.0.0/24 256 IPs 削除

< > ^ v

特定の CIDR を追加 サイズ別に CIDR を追加

30. [Configure this pool's allocation rule settings]にチェックをつけます

割り振りルール設定 - オプション 情報

 **AWS best practice**  
We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize IPAM pools, see [Example IPAM pool plans](#).

☒ Configure this pool's allocation rule settings

31. [検出されたリソースを自動的にインポート]にチェックをつけます

CIDR management

Automatically import discovered resource  
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。

☒ 検出されたリソースを自動的にインポート  
☐ Don't allow

32. [Netmask Compliance]で[/24]を設定します。これにより、2 次プールから 3 次プールに割り当てられた[/24]CIDR ブロックを全て割り当て可能となります。

Netmask compliance

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。  

/24 (256 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。  

/24 (256 IPs) ▼

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。  

/24 (256 IPs) ▼

33. [プールを作成]をおします

34. 以下のように 3 階層構造となっています。



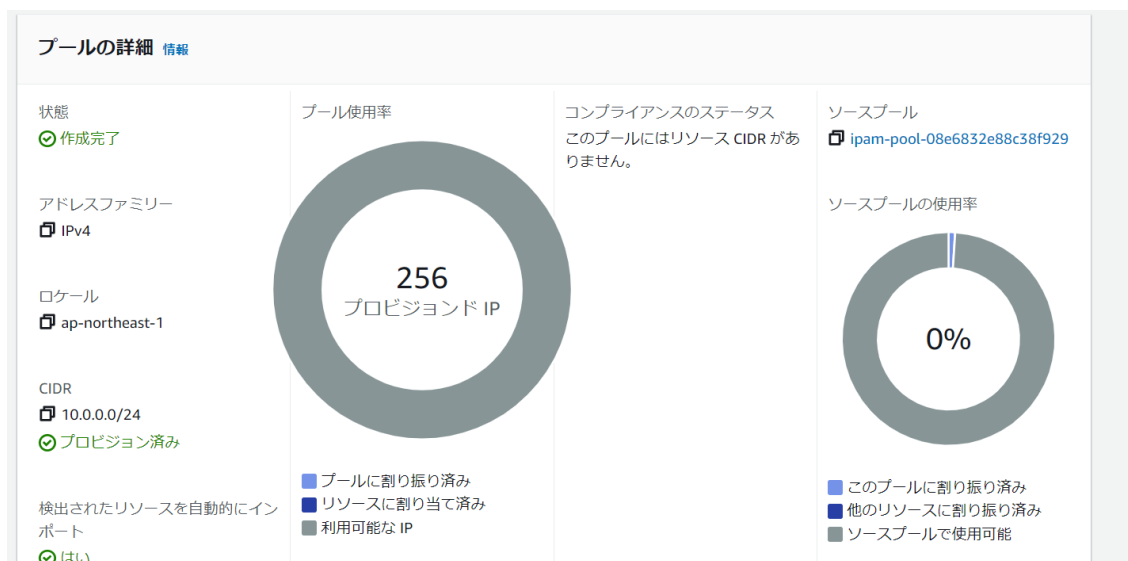
35. Dev プールの詳細画面で[CIDR]タブをクリックすると以下のように正しく 10.0.0.0/24 がプロビジョニングされているかを確認します。



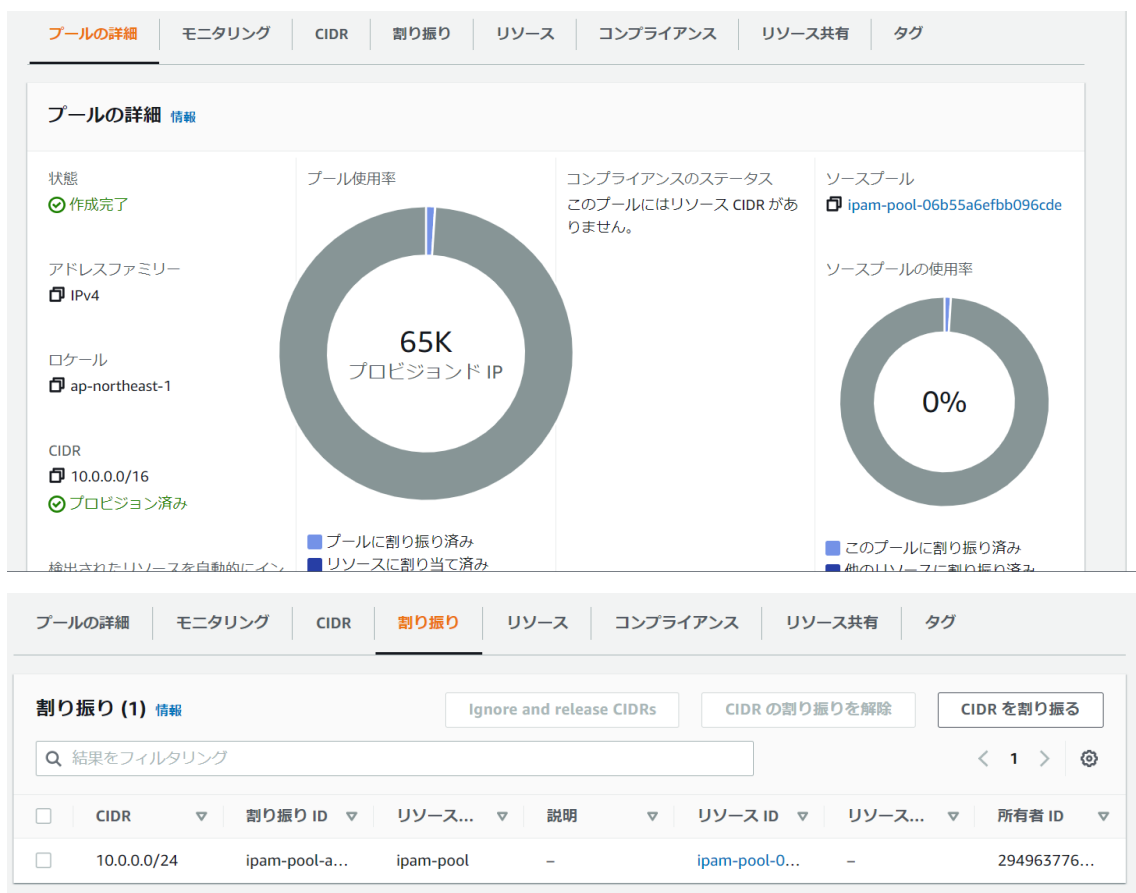
36. [割り振り]タブを確認すると、管理可能な CIDR IP アドレス帯がまだ何も割り振られていないことがわかります。



以下のように詳細画面のトップのグラフでは、/24 が利用可能な IP として認識されています。



37. 2 次プールを見ると、一部の IP がプールに割り振り済みとなっています。



IPAM では、その IP アドレスが実際使用されているかどうか(EC2 や ELB、EIP 等が利用しているか)ではなく、その IP アドレスが VPC に割り当てられているか、下位 Pool に割り振っているか、を IP アドレスが利用可能かどうかとして判断していますので注意して下さい。2022/02/04 現在、IPAM は VPC 及び Subnet の IP アドレス割り

当て状況の管理に対応していますが、VPC 内部のリソース(EC2 や ELB、EIP 等が利用しているか)の IP アドレス利用状況の管理には対応していません。

いままでの手順で作成された 3 次プールに割り当てられた CIDR IP アドレスブロック [10.0.0.0/24] を VPC に割り振り、VPC を作成します。

38. マネージメントコンソールから VPC の画面に移動します。2 次プールで作成したリージョンで作業を行います。
39. 左ペインから[VPC]をクリックし、[VPC を作成]をおします
40. 適当な名前をつけます
41. [IPv4 CIDR ブロック]で[IPAM 割り当ての IPv4 CIDR ブロック]を選択します

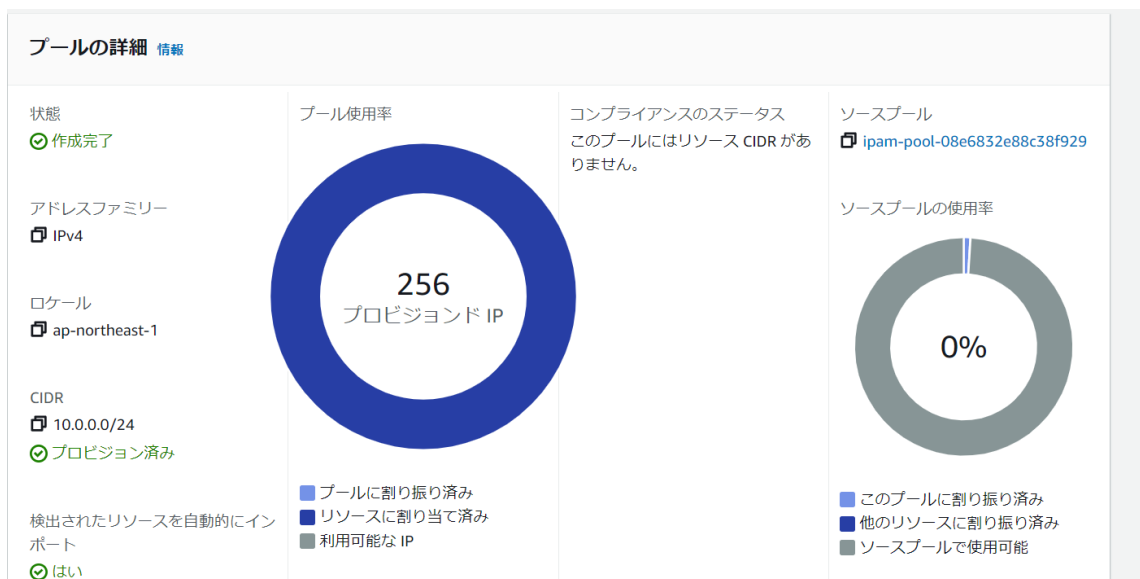
IPv4 CIDR ブロック [情報](#)  
☐ IPv4 CIDR の手動入力  
☒ IPAM 割り当ての IPv4 CIDR ブロック - 新規

IPv4 IPAM プール

ipam-pool-04f93d034b4261e81

42. [IPv4 IPAM プール] から Dev 用 3 次プールを選びます
43. [VPC を作成]をおします
44. VPC 作成後しばらく待つと、IPAM マネージメントコンソールの Dev プールの詳細画面ですべての IP アドレスが割り当て済となっていることがわかります。

割り振り (1) <a href="#">情報</a>							
<div>ignore and release CIDRs</div> <div>CIDR の割り振りを解除</div> <div>CIDR を割り振る</div>							
<div>Q 結果をフィルタリング</div> <div>&lt; 1 &gt; ⚙</div>							
<input type="checkbox"/>	CIDR	割り振...	リソー...	説明	リソース ID	リソースのリー...	所有者 ID
<input type="checkbox"/>	10.0.0.0/24	ipam-pool...	vpc	-	<a href="#">vpc-005a3a04088661882</a>	ap-northeast-1	294963...



この割り振りタブから、プロビジョンされている CIDR IP アドレス帯を分割してより小さい CIDR ブロックを VPC 以外のリソースに利用目的で割り振りを行うことができます。(Direct Connect Gateway 経由のオンプレミス IP アドレスブロック等)

45. しばらく（10-分程度待つと）リソースタブから、このプールが管理している IP アドレスブロックを保有するリソース（今回の手順だと VPC）が確認できるようになります。

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
<b>リソース (1) 情報</b> IPAM スコープ内のリソースを表示します。							
<input type="text" value="リソースをフィルタリング"/>							
<input type="checkbox"/>	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
<input type="checkbox"/>	vpc-005a3a04088661882		準拠	重複なし	dev		

46. IPAM マネージメントコンソール左ペインの[リソース]をクリックすると、Global の IP アドレス利用状況（初期の IPAM 設定時に指定した全リージョン）が一元管理できます。

Amazon VPC IP Address Manager > Resources

**リソース (4) 情報** 🔄 10.0.0.0/8 16M IPs ipam-scope-0c90b6865fd9d9f80 ▼ アクション ▼

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 < 1 > ⚙️

<input type="checkbox"/>	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
<input type="checkbox"/>	subnet-0a69c4605a979a51b	-	-	-	<div></div>
<input type="checkbox"/>	subnet-0e4ff8382fb35a423	-	-	-	<div></div>
<input type="checkbox"/>	vpc-005a3a04088661882	🟢 準拠	🟢 重複なし	dev	<div></div>
<input type="checkbox"/>	vpc-0f0d617f7d7662471	⊖ アンマネージド	🟢 重複なし	-	<div></div>

VPC 内部に作成された Subnet の IP アドレスブロックが管理が可能です。注意：  
2022/02/04 個別プール詳細画面では Subnet に割り振った I P アドレスブロックの管  
理が行えません。

お疲れ様でした！

以下を削除してください

- ・ V P C
- ・ 3 次プールの割り振り（5 分程度待ちが発生します）→ C I D R
- ・ 3 次プール
- ・ 2 次プールの C I D R
- ・ 2 次プール
- ・ 1 次プールの→ C I D R
- ・ 1 次プール
- ・ IPAM