Amazon VPC Lattice × EKS で実現するアプリケーションネットワーキング

後藤 健汰(Kenta Goto)
Solutions Architect ISV/SaaS

自己紹介

- 名前
  - 後藤 健汰（ Kenta Goto ）
- 所属
  - ISV/SaaS Solutions Architect
- 職歴
  - SIer → Web系（インフラエンジニア）
- 趣味
  - サウナ

@kennygt51

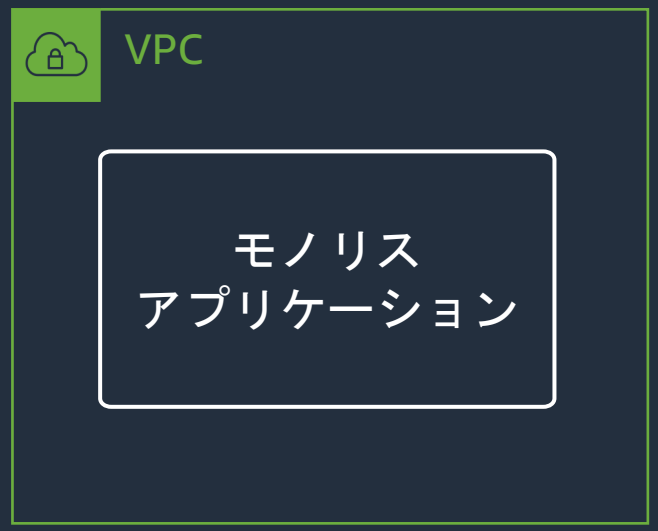
Agenda

- サービス間通信の必要性と課題
- Amazon VPC Lattice とは
- VPC Lattice × EKS のユースケース
- AWS Gateway Controller for Kubernetes
- デモ
- まとめ

サービス間通信の必要性と課題

背景：サービス間通信の必要性

- モノリスアプリケーションは、機能数や複雑さに応じて、様々な課題が生じうる

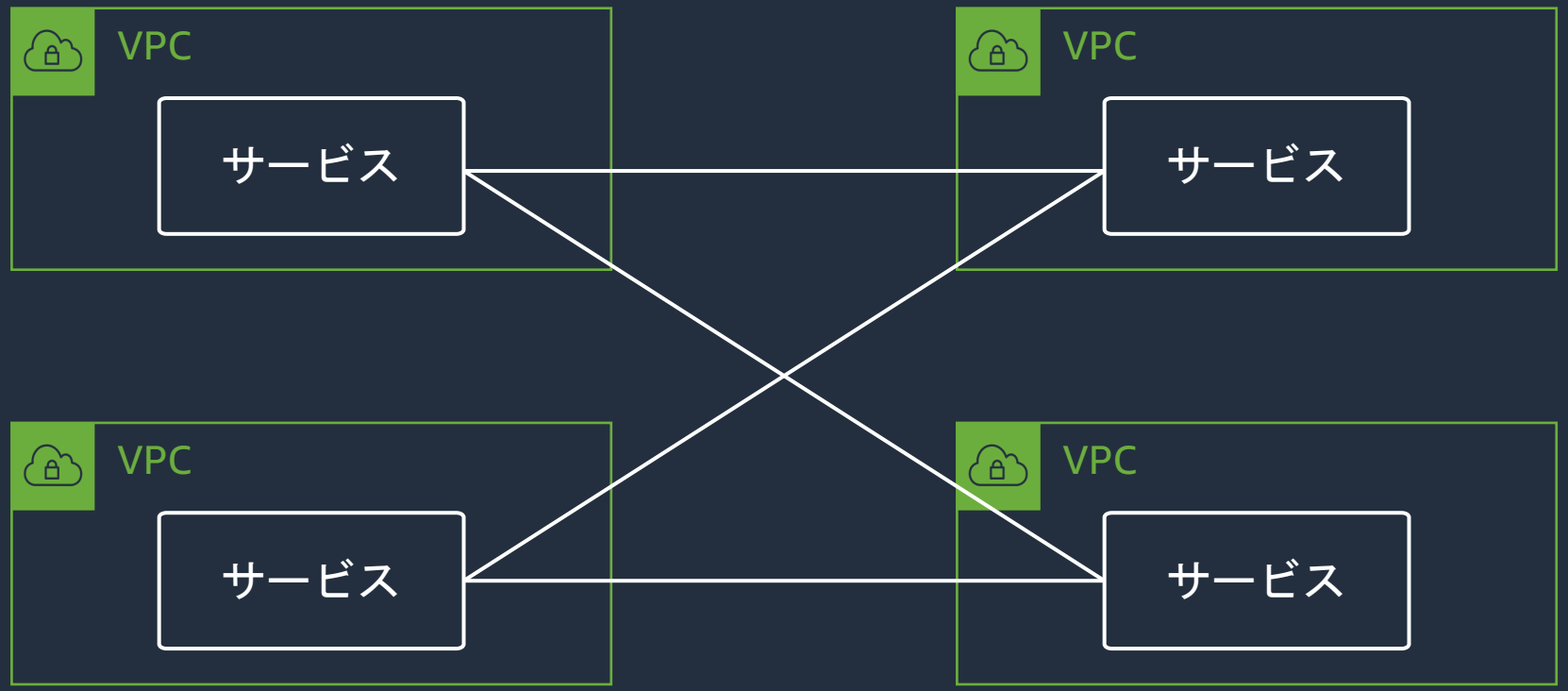


モノリスの課題

- 開発速度の遅さ
- 大きなデプロイ範囲
- 信頼性
- 新規テクノロジーの導入
- スケーラビリティ

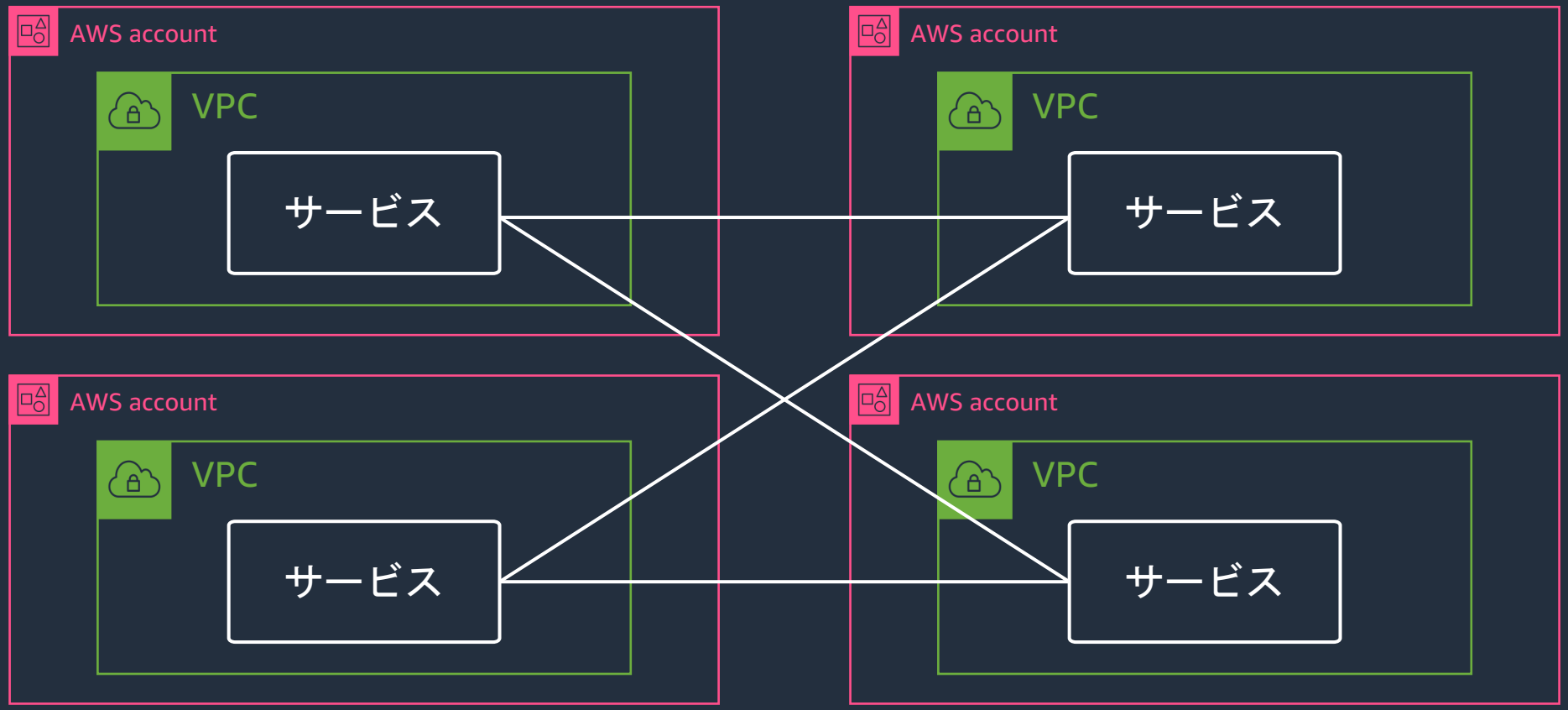
背景：サービス間通信の必要性

- 複数の（マイクロ）サービスに分解。サービスチームはAPIを提供し、APIを通じてやり取りする



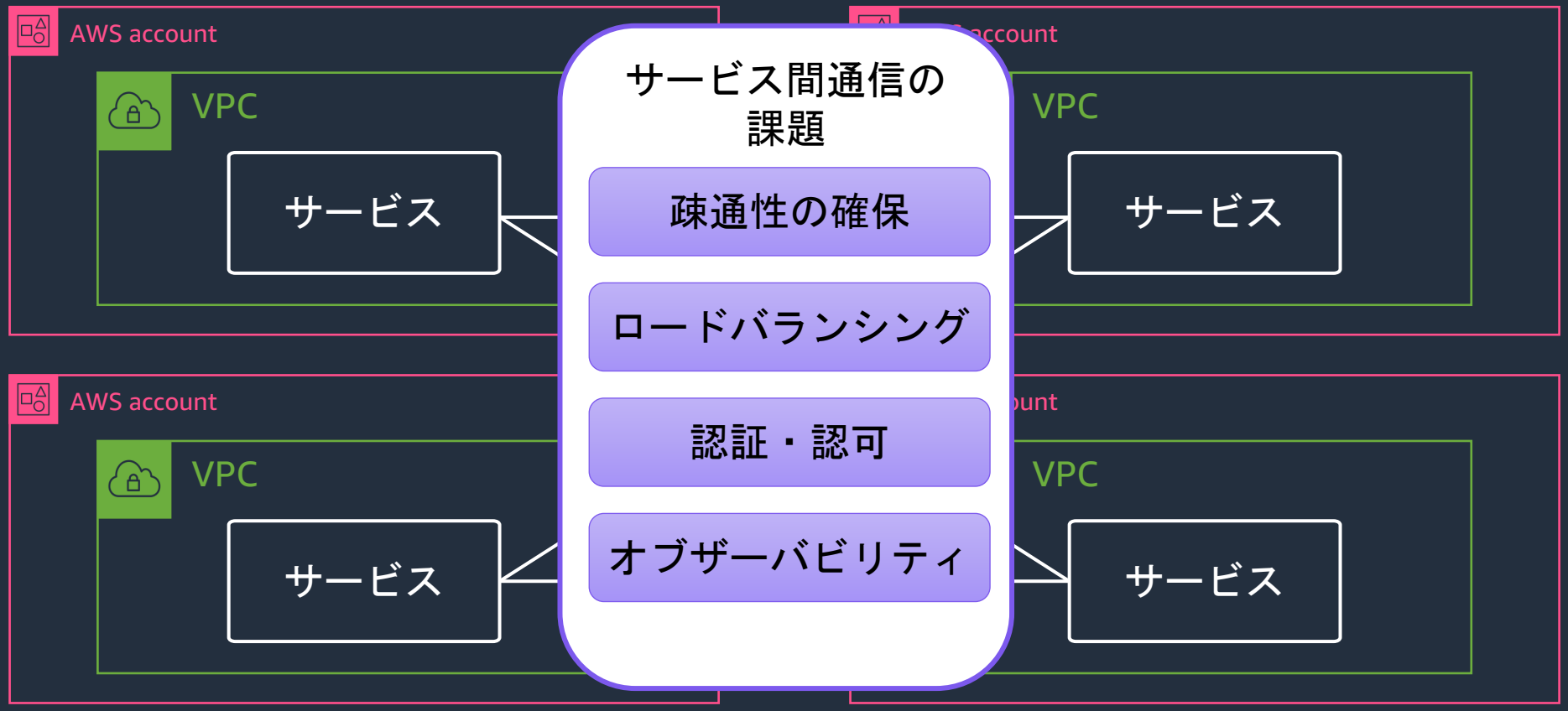
背景：サービス間通信の必要性

- 複数のサービスは、複数のVPC・アカウントで構成されうる



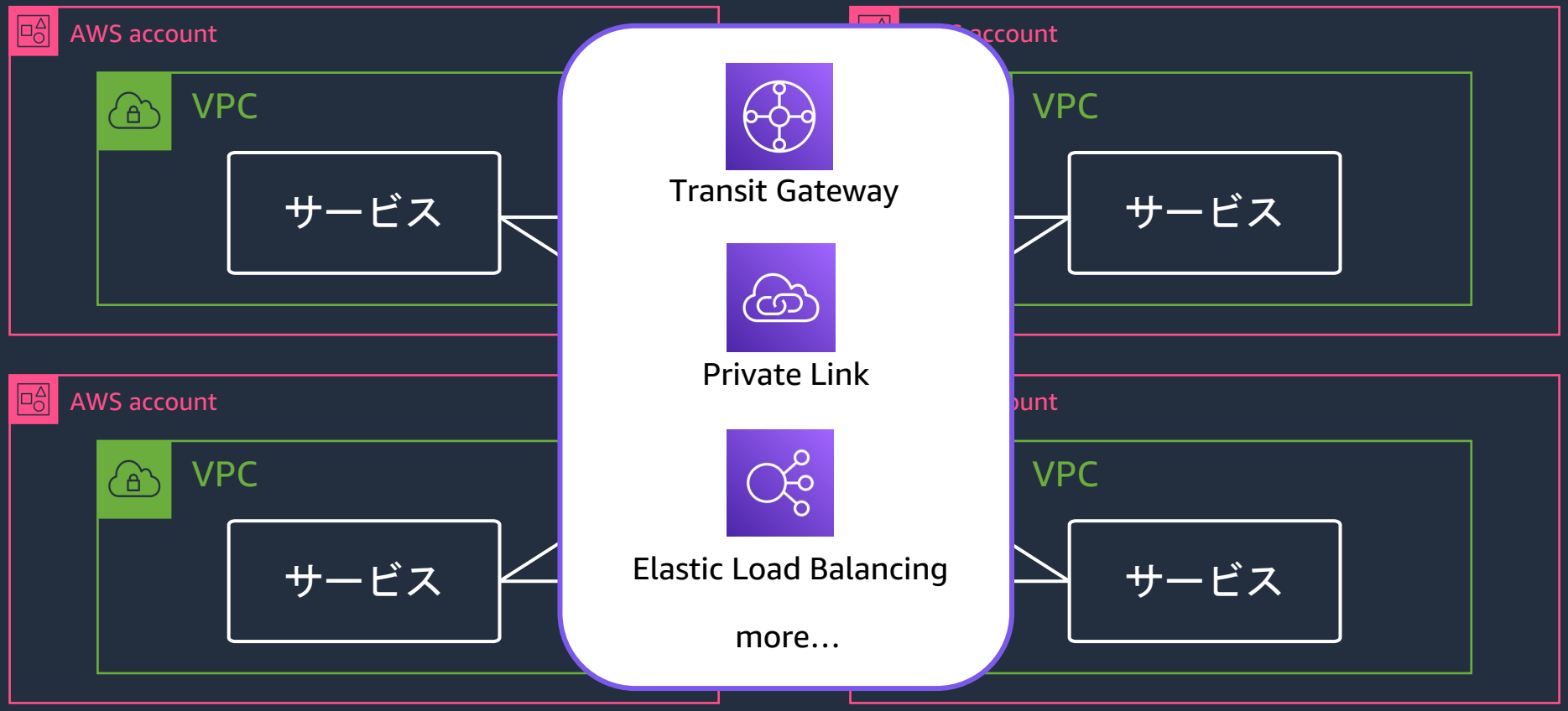
背景：サービス間通信の課題

- サービス間通信に求められる要件は多種多様



背景：サービス間通信の課題

- アカウントやVPCが分離すると、疎通性の確保やサービス間通信の課題解決のため、構成が複雑になりがち



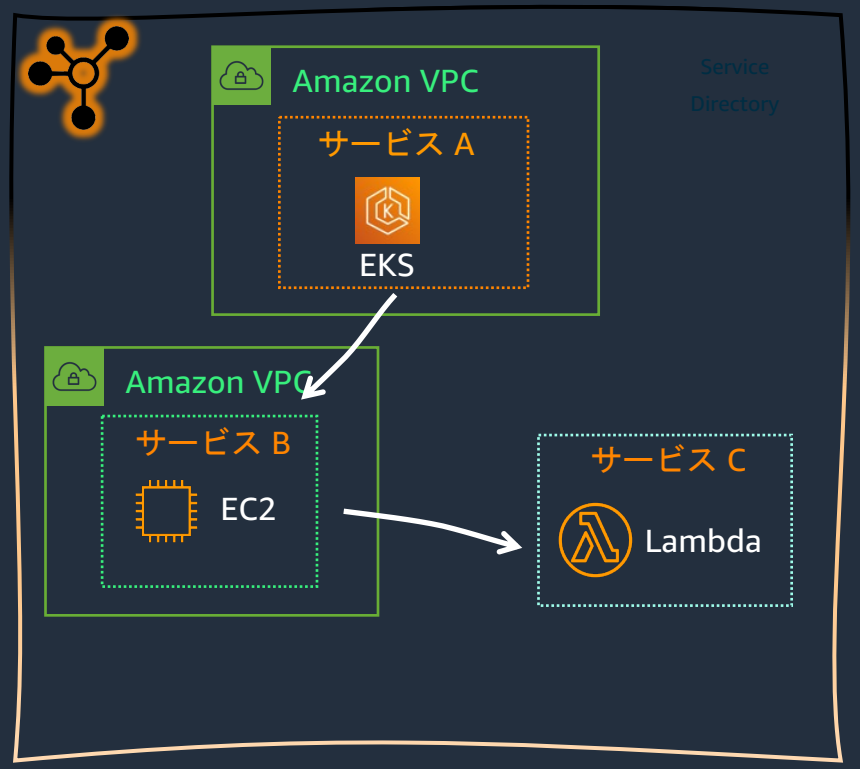
Amazon VPC Lattice とは

Amazon VPC Lattice とは

様々なサービス間通信を、特定の技術（コンテナなど）に依存せず、
Amazon VPC のネットワークサービスのみでシンプルに実現するサービス

- 接続性
  - アカウント、VPCをまたいだ接続
  - CIDR が重複する VPC 間での接続が可能
- コンピューティングサービスの一貫性
  - Amazon EC2、AWS Lambda、Amazon EKS との統合
- オブザーバビリティ・トラフィックコントロール
  - Amazon S3、Amazon CloudWatch、Amazon Kinesis Data Firehose へのログ出力
- セキュリティ
  - IAM による認証

Amazon VPC Lattice の主要コンポーネント



サービス

- 単一のアプリケーションユニット
- 1つのサービスコンポーネント（マイクロサービス）を「サービス」として定義する

サービスネットワーク

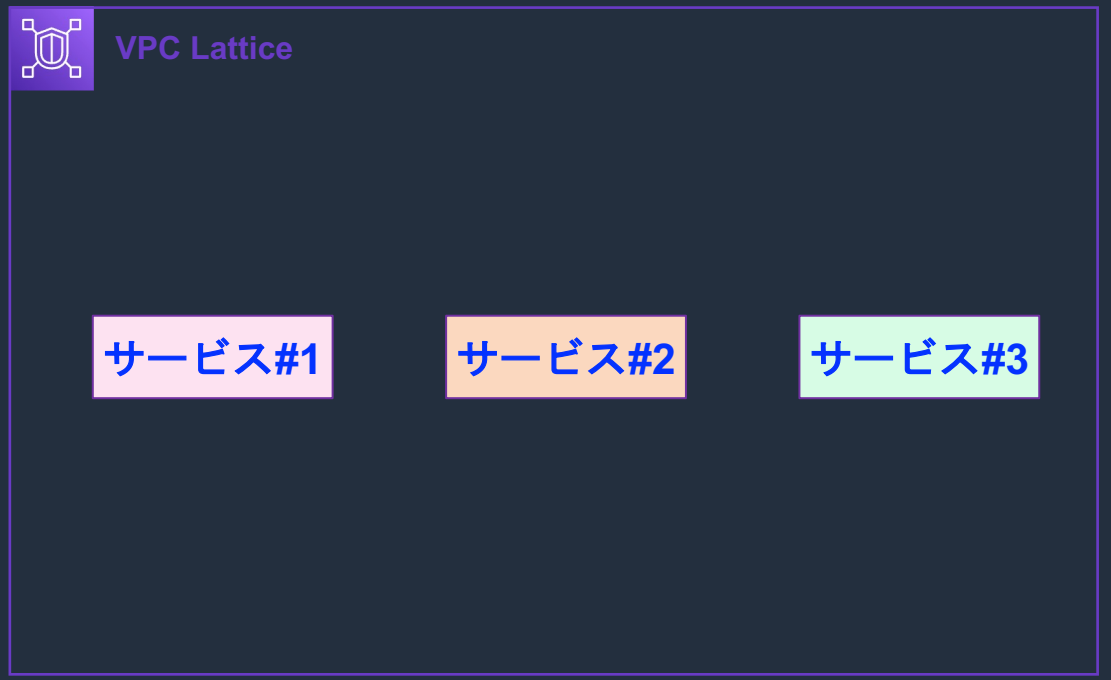
- 論理的なアプリケーション層ネットワークの境界
- VPC やアカウントをまたいでクライアントとサービスを接続

認証ポリシー

- IAM を活用した認証
- サービスネットワークや個々のサービスに関連付けることで、アクセス制御をおこなう

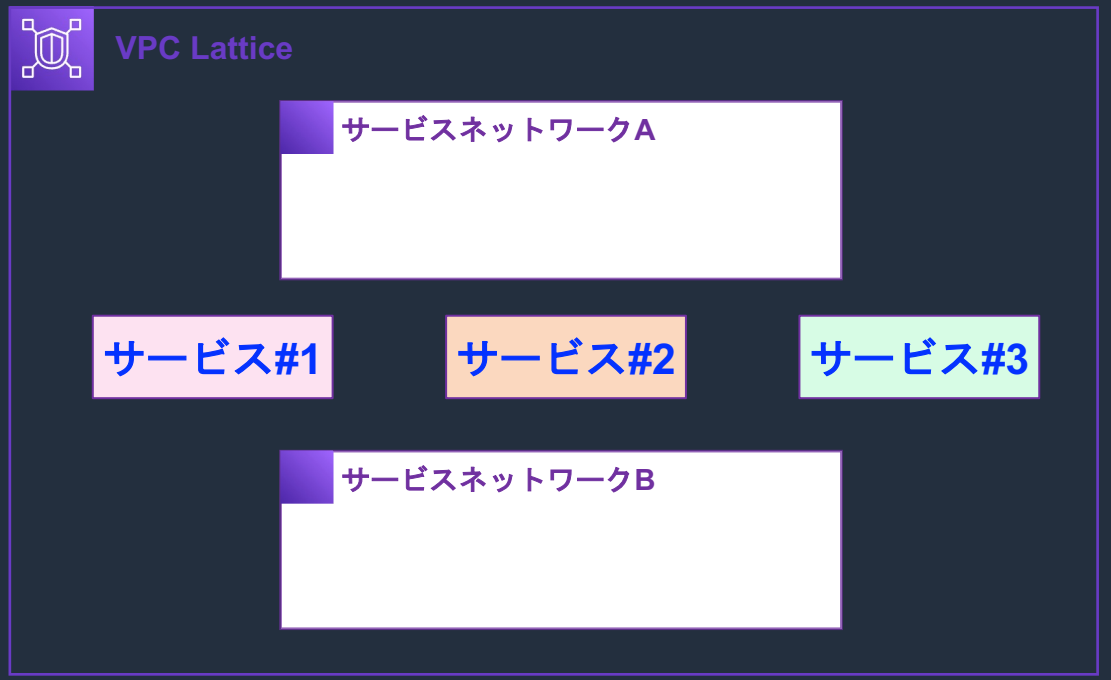
VPC Lattice サービス

- 1 つのサービスコンポーネント (マイクロサービス) を VPC Lattice の「サービス」として定義する



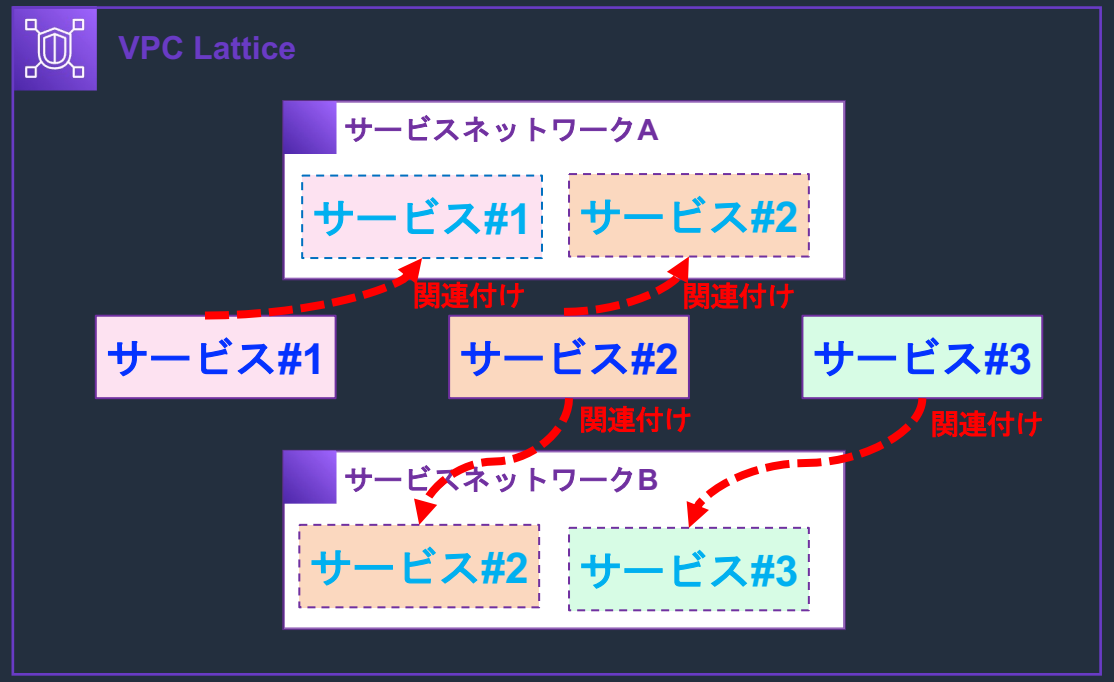
VPC Lattice サービスネットワーク

- サービスの集合としての論理境界を「サービスネットワーク」として定義する



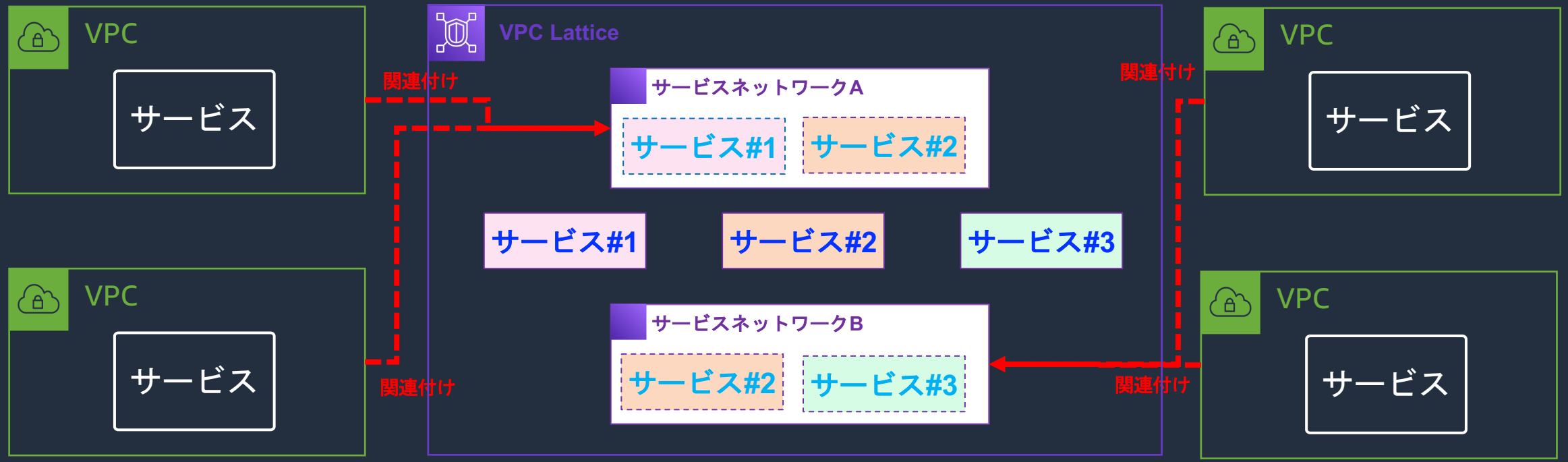
VPC Lattice サービスネットワークとサービス

- サービスを、サービスネットワークに関連付ける



VPC Lattice サービスネットワークと VPC

- VPC をサービスネットワークに関連付けることで、サービスと接続可能になる

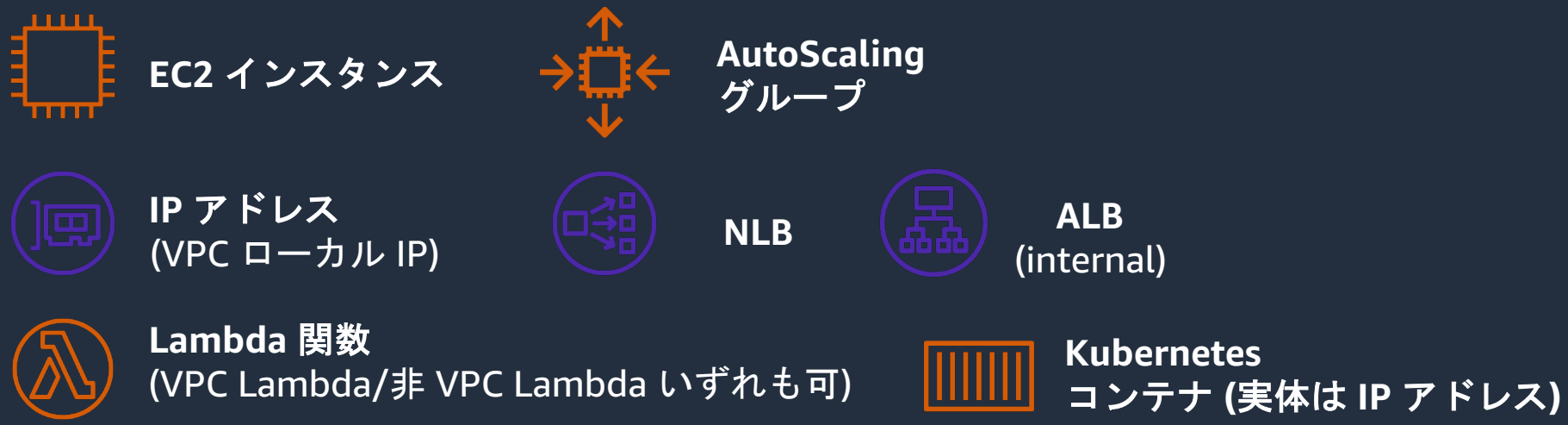


Amazon VPC Lattice で実現できること

- 疎通性の確保
  - アカウント、VPC をまたいだ接続
- サービスディスカバリ
  - DNS 名によるシンプルな名前解決
- ロードバランシング
  - ルールやターゲットグループによる柔軟な負荷分散
- アクセス制御
  - IAMと統合されたアクセス制御 (認証ポリシー)
- モニタリング
  - メトリクスやログの集中管理

疎通性の確保

- アカウント、VPC をまたいだ HTTP/S、gRPC での通信を実現
  - Transit Gateway や VPC Peering は不要
- ターゲットとして EC2 インスタンスや Lambda 関数、Kubernetes コンテナなど複数のリソースに対応

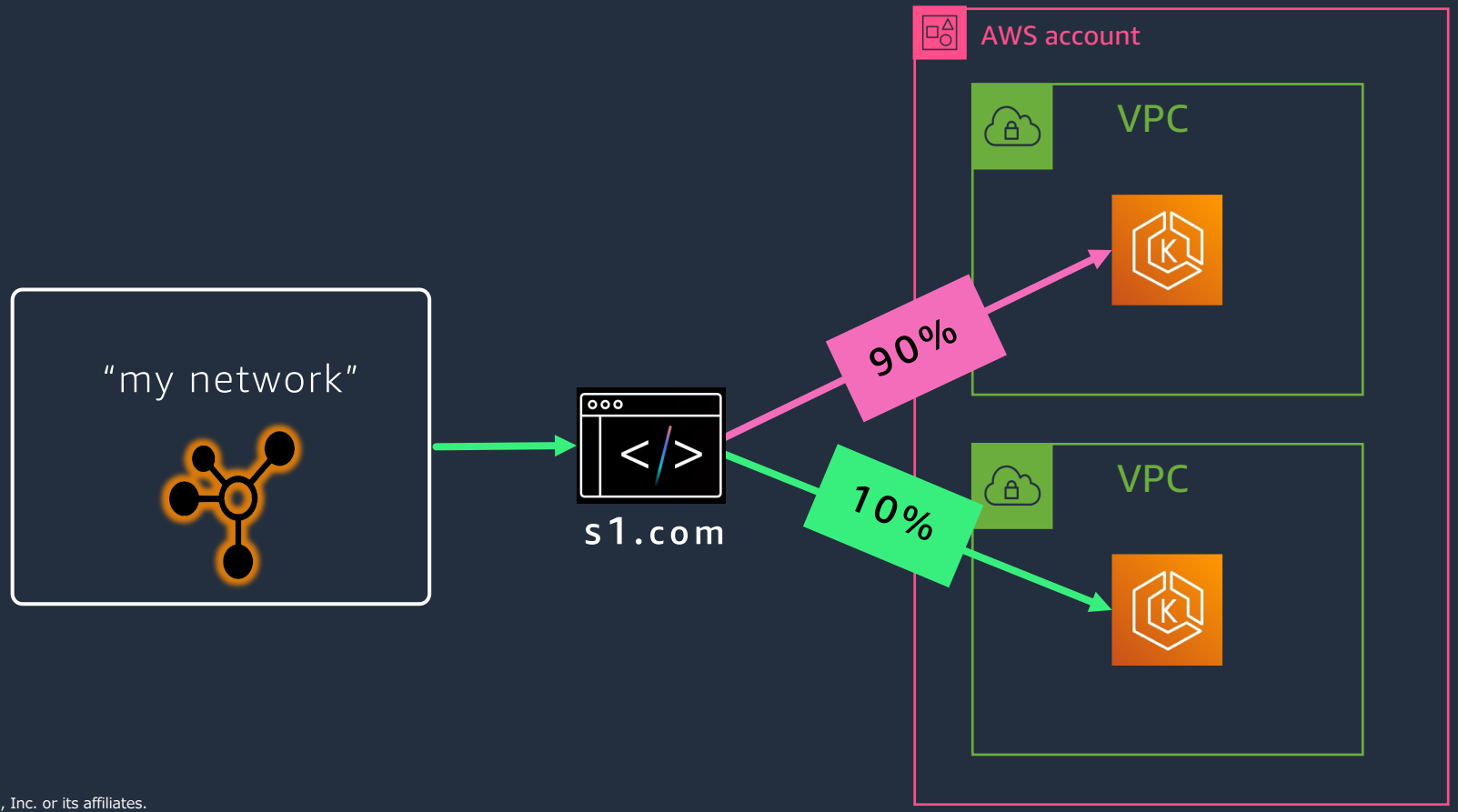


サービスディスカバリ

- サービスは、それぞれに固有の DNS 名が払い出される。カスタムドメイン名を設定することも可能

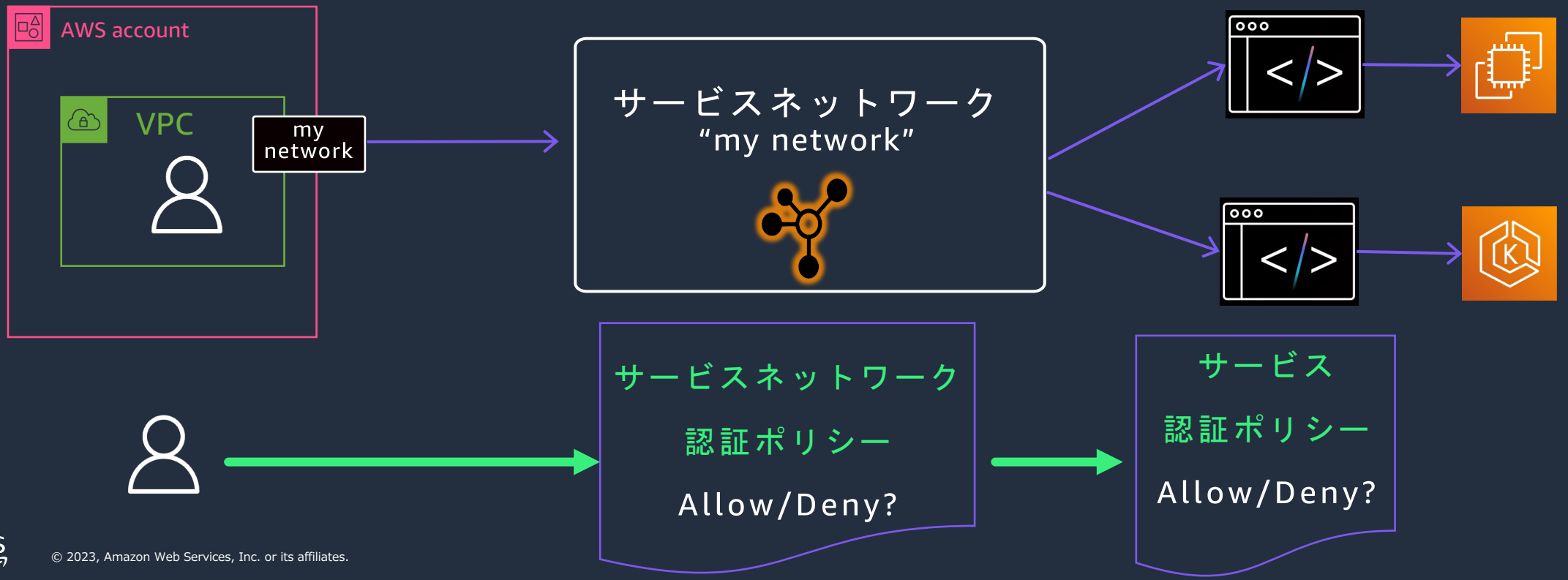
ロードバランシング

- ルールや条件評価、重みに基づいて、転送先のターゲットを決定できる



アクセス制御

- 認証タイプ「AWS_IAM」を選択することで、認証ポリシーを設定し、IAM を使用してアクセスコントロールを実現できる。



モニタリング

- サービスへのアクセスログの出力、CloudWatch メトリクスの発行をサポート

アクセスログ

CloudWatch Logs

S3 バケット

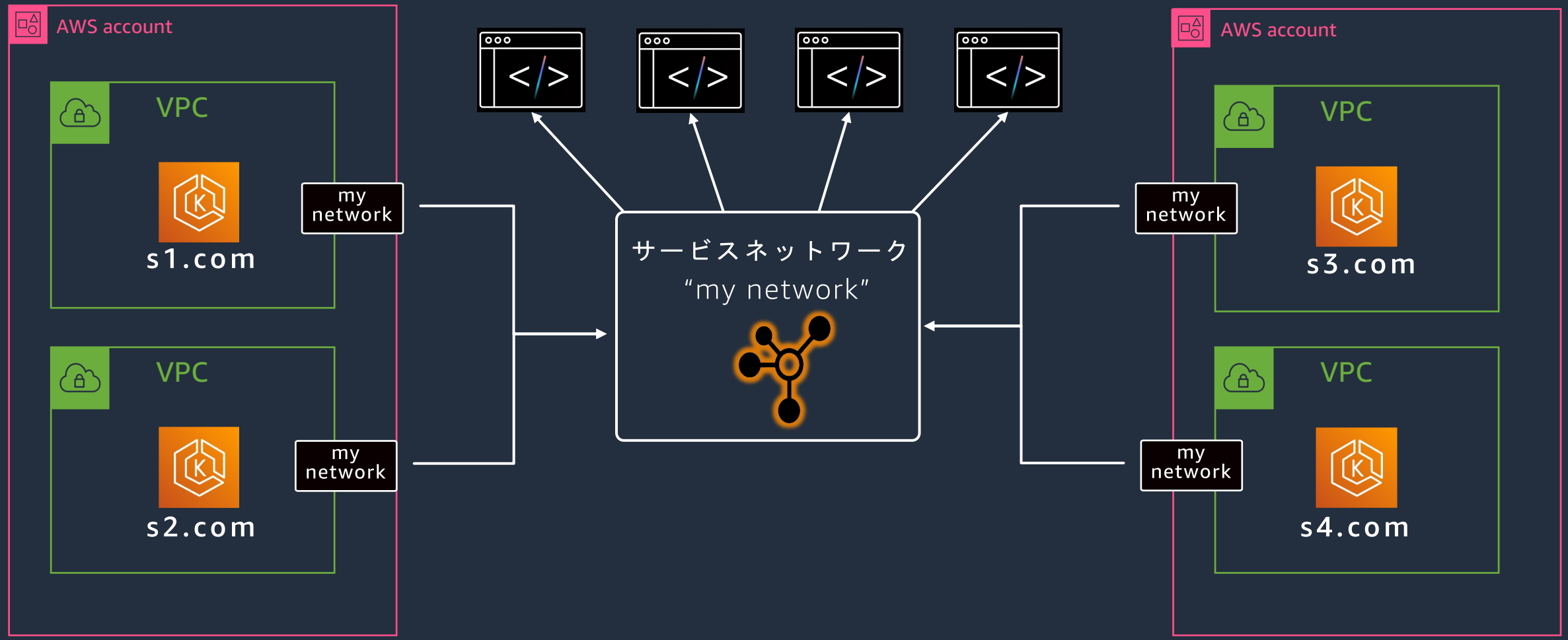
Kinesis Data Firehose

メトリクス

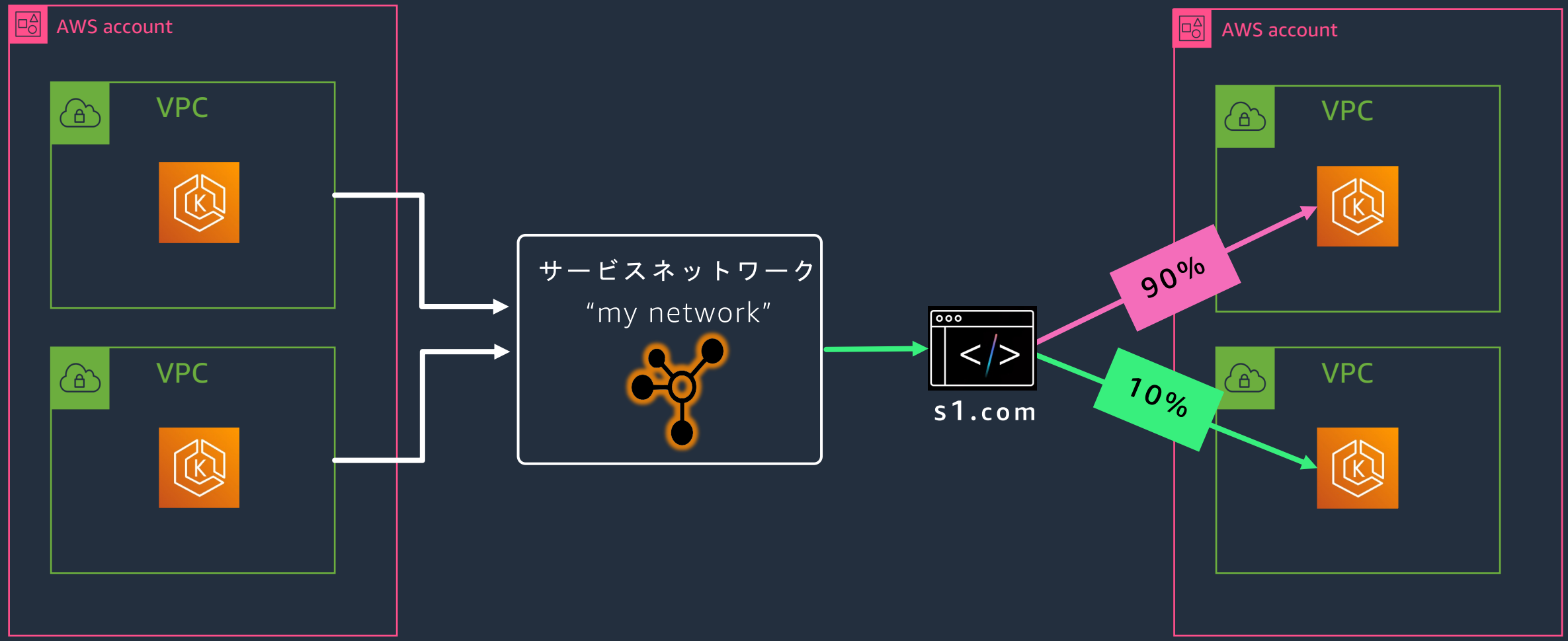
CloudWatch

VPC Lattice × EKS のユースケース

シングルテナント（マルチクラスター）間通信



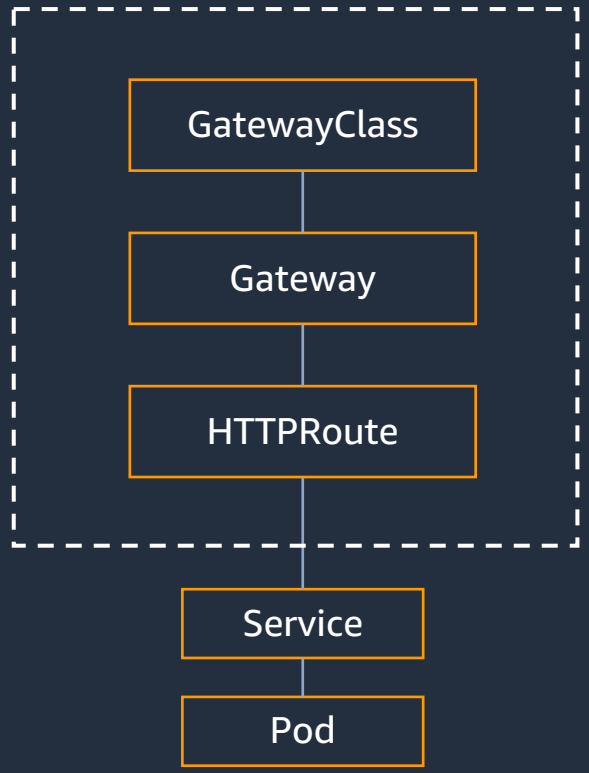
加重ルーティングによるクラスターアップグレード



AWS Gateway Controller for Kubernetes

Kubernetes Gateway API とは

- Kubernetes Gateway API は SIG-NETWORK コミュニティを中心に開発が行われている API リソース
- クラスター外部からのトラフィックを制御するためのもので、Ingress リソースが抱える各種課題の解決を目的として開発された
- GatewayClass、Gateway、HTTPRoute といった複数のリソースから構成される

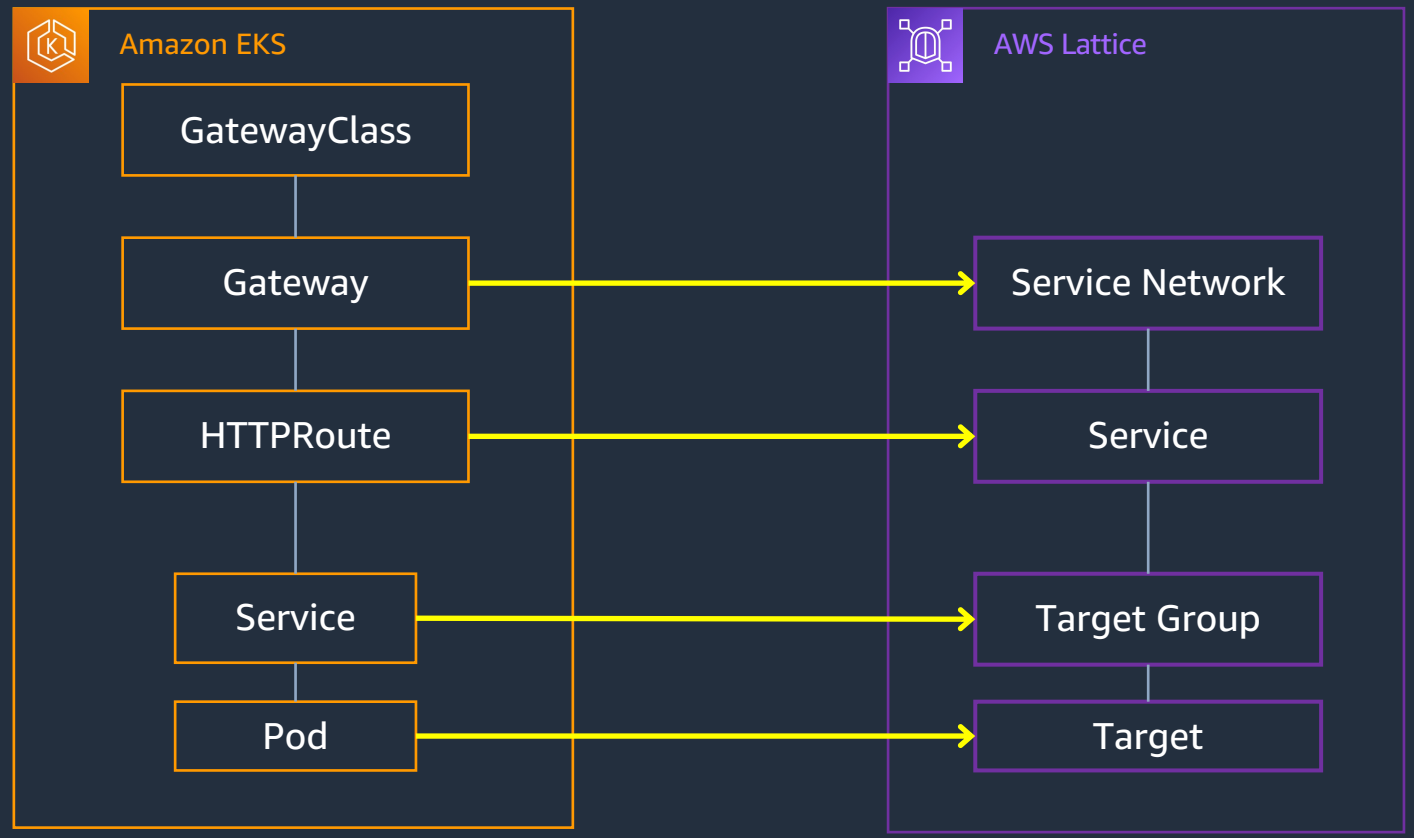


AWS Gateway Controller for Kubernetes とは

- Kubernetes Gateway API を実装するコントローラー
- AWS Gateway Controller for Kubernetes は、Gateway API で定義されたカスタムリソースに対応する VPC Lattice のリソースを作成する
  - Gateway や HTTPRoute といった Kubernetes のリソースを作成することで、VPC Lattice のサービスといった AWS のリソースを作成する
- EKS 上のワークロードで VPC Lattice を使う場合は、このコントローラーをクラスターにデプロイする

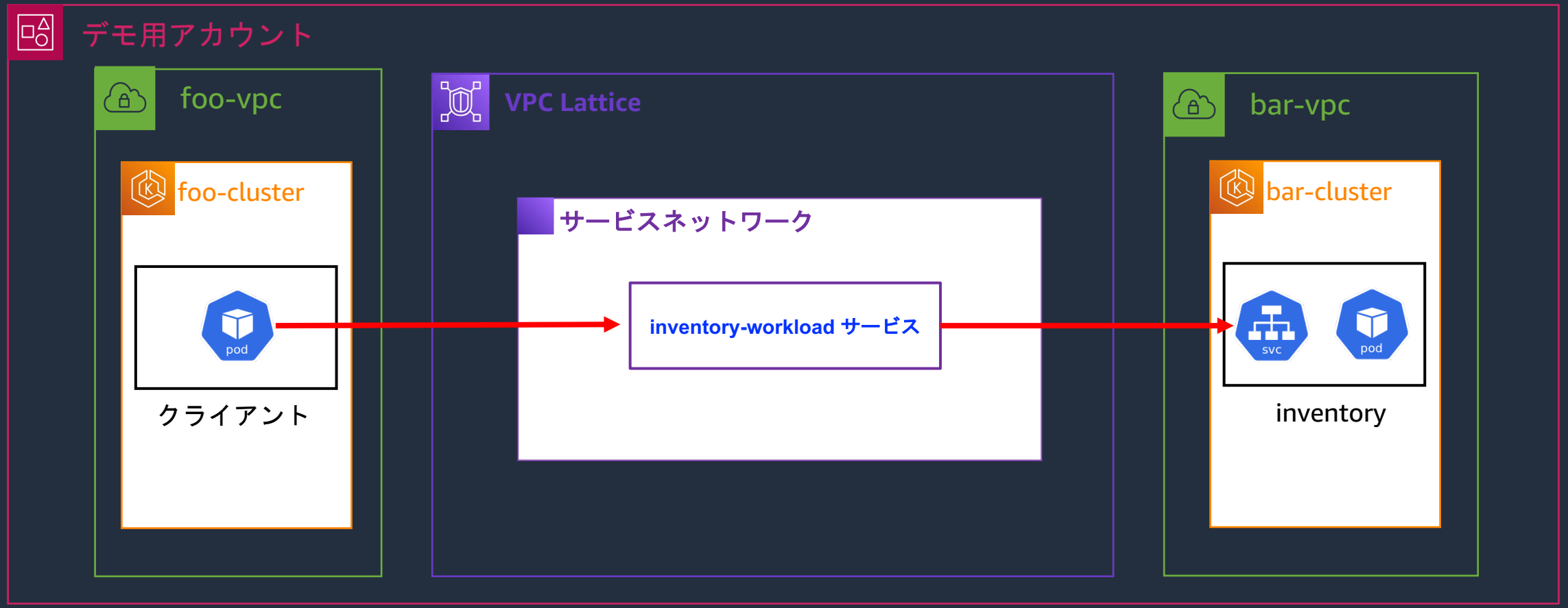
AWS Gateway Controller for Kubernetes とは

- Kubernetes Gateway API リソースと VPC Lattice のリソースは、以下のように対応する



デモ

デモ



まとめ

まとめ

- 様々なサービス間通信を、特定の技術（コンテナなど）に依存せず、Amazon VPC のネットワークサービスのみでシンプルに実現するサービス
- EKS を利用している場合、マルチクラスター間の通信、クラスターアップグレードなどで活用できる
- EKS 上のワークロードで VPC Lattice を使用する場合は AWS Gateway Controller for Kubernetes を利用する

Thank you!