



Amazon Elastic Kubernetes Service (Amazon EKS) での Data Plane 管理

AWS Black Belt Online Seminar

林 政利

Specialist Solutions Architect, Containers

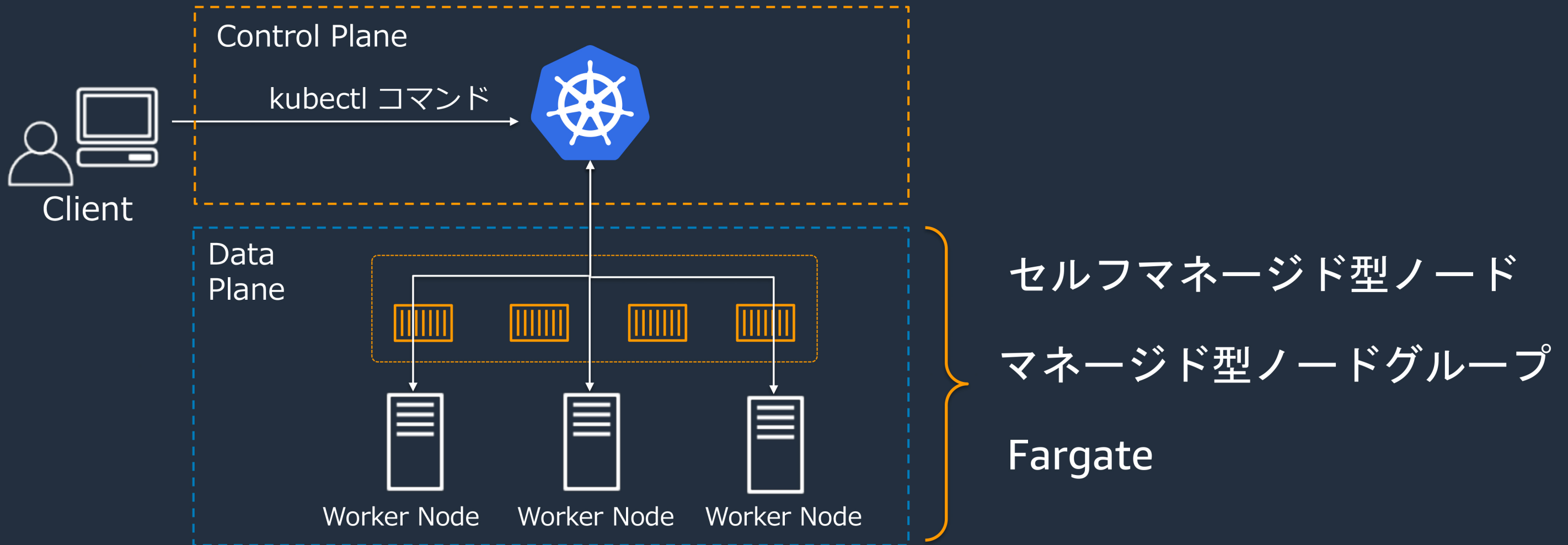
2021/10

アジェンダ

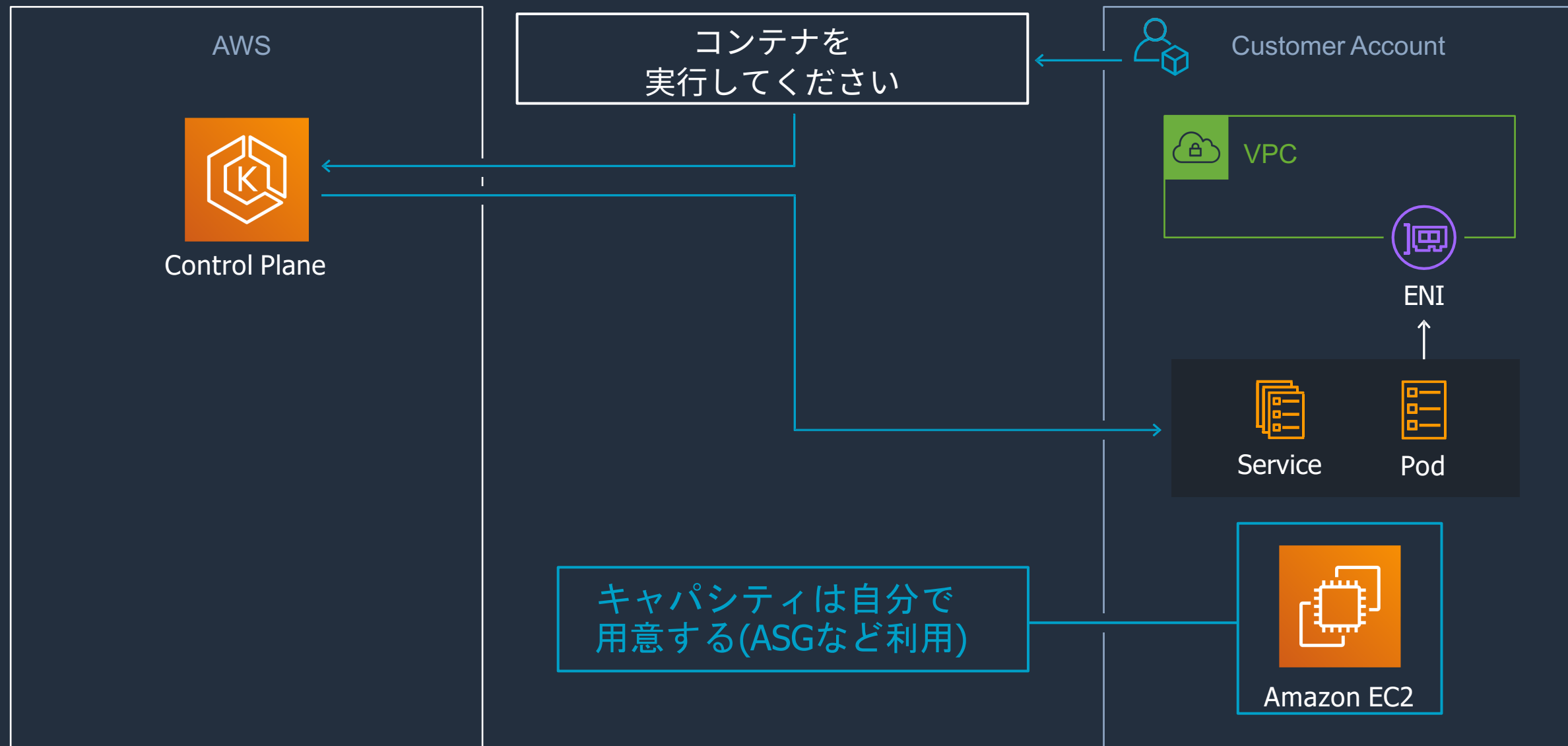
- Amazon EKS での Data Plane 管理オプション
 - セルフマネージド型ノード
 - マネージド型ノードグループ
 - Fargate
- Data Plane 管理の選択方法

Amazon EKS での Data Plane 管理オプション

EKS の Data Plane 管理のオプション



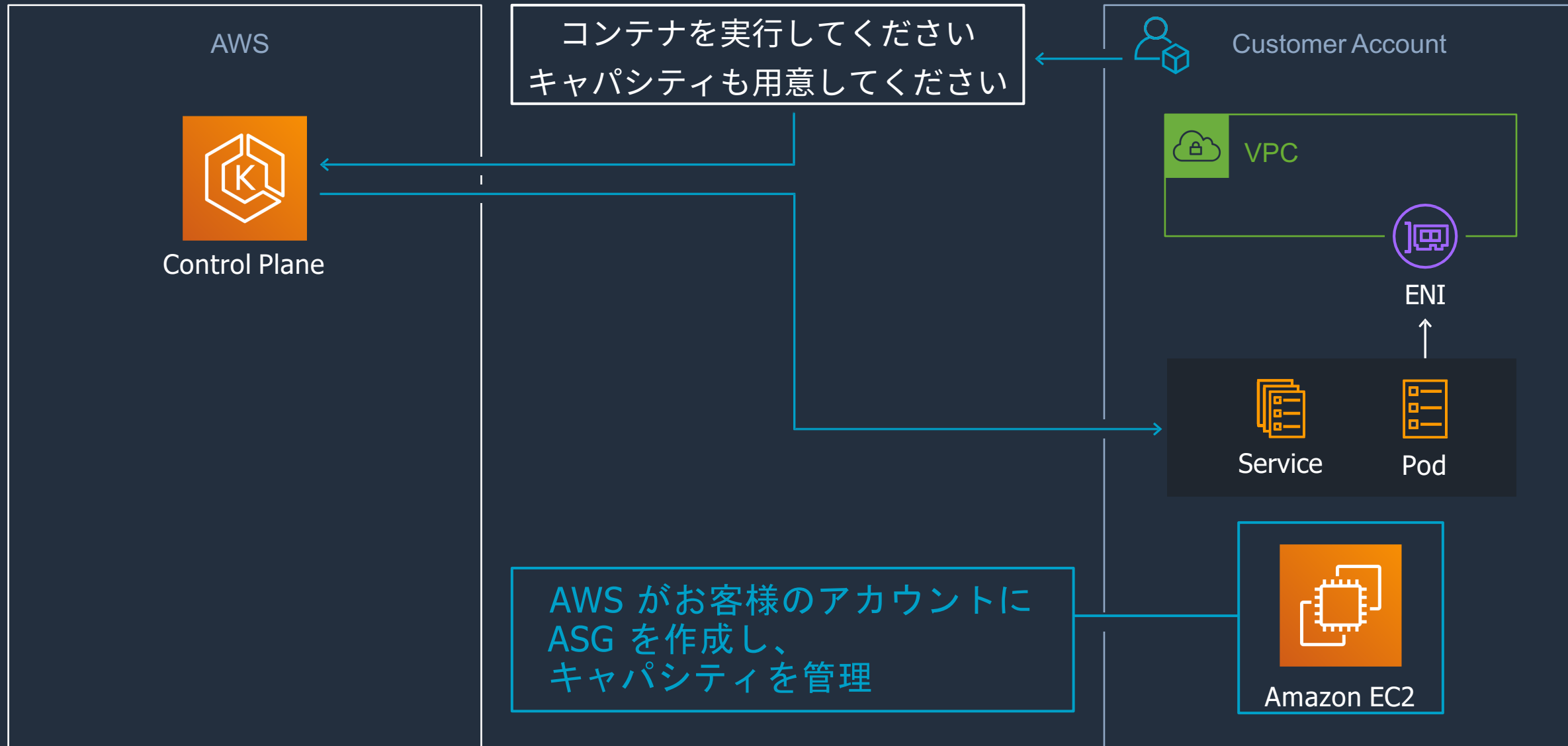
セルフマネージド型ノード



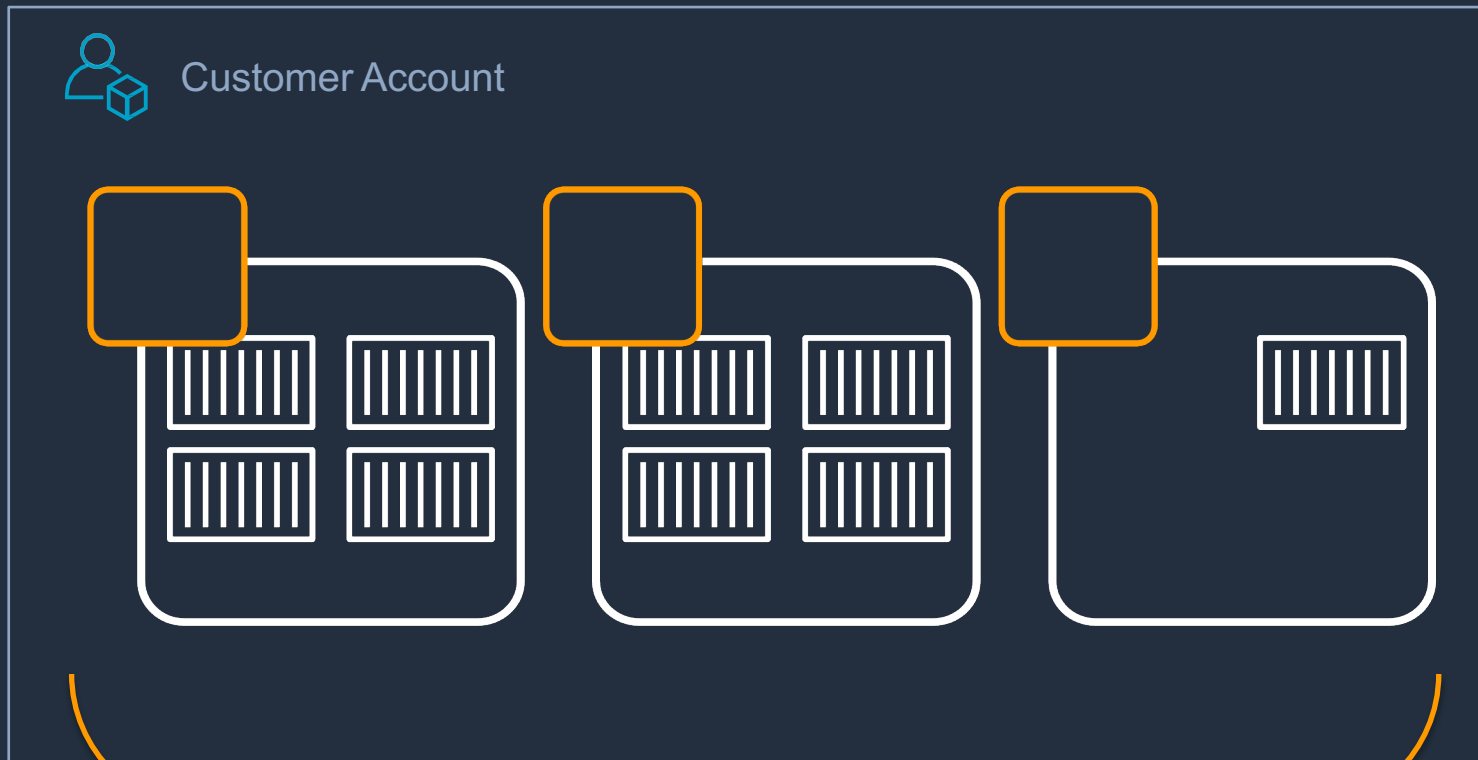
セルフマネージド型ノード

- コンテナを動かすためのキャパシティを完全に制御
 - EC2の運用やAMIの管理
 - EC2のライフサイクル
 - AWSのAuto Scaling Groupを利用
 - またはサードパーティのツールを利用
- kubeletの更新方法を細かく制御

マネージド型ノードグループ



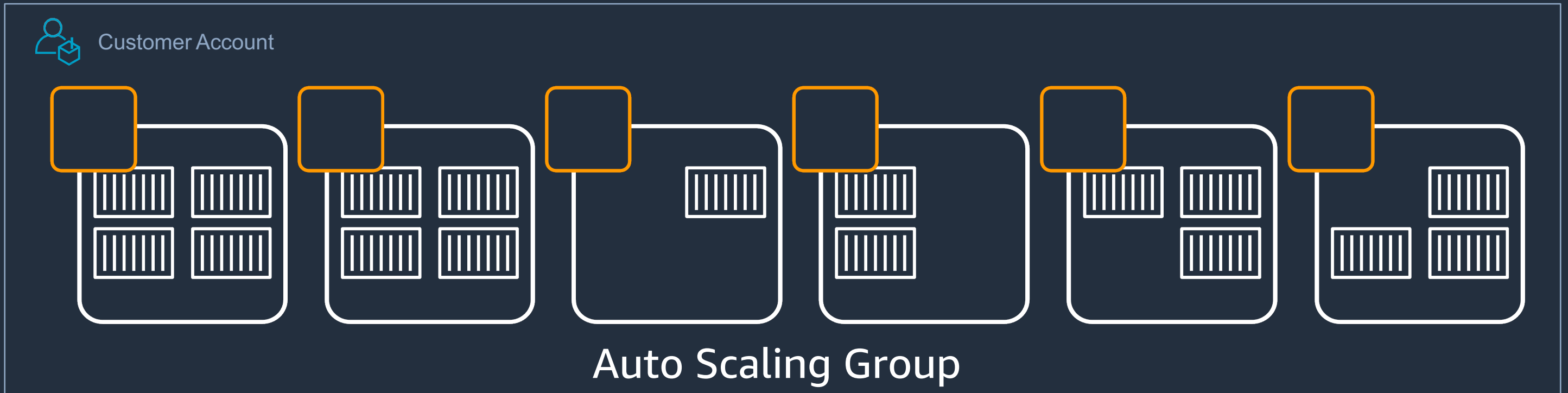
マネージド型ノードグループ



**Amazon
EKS**

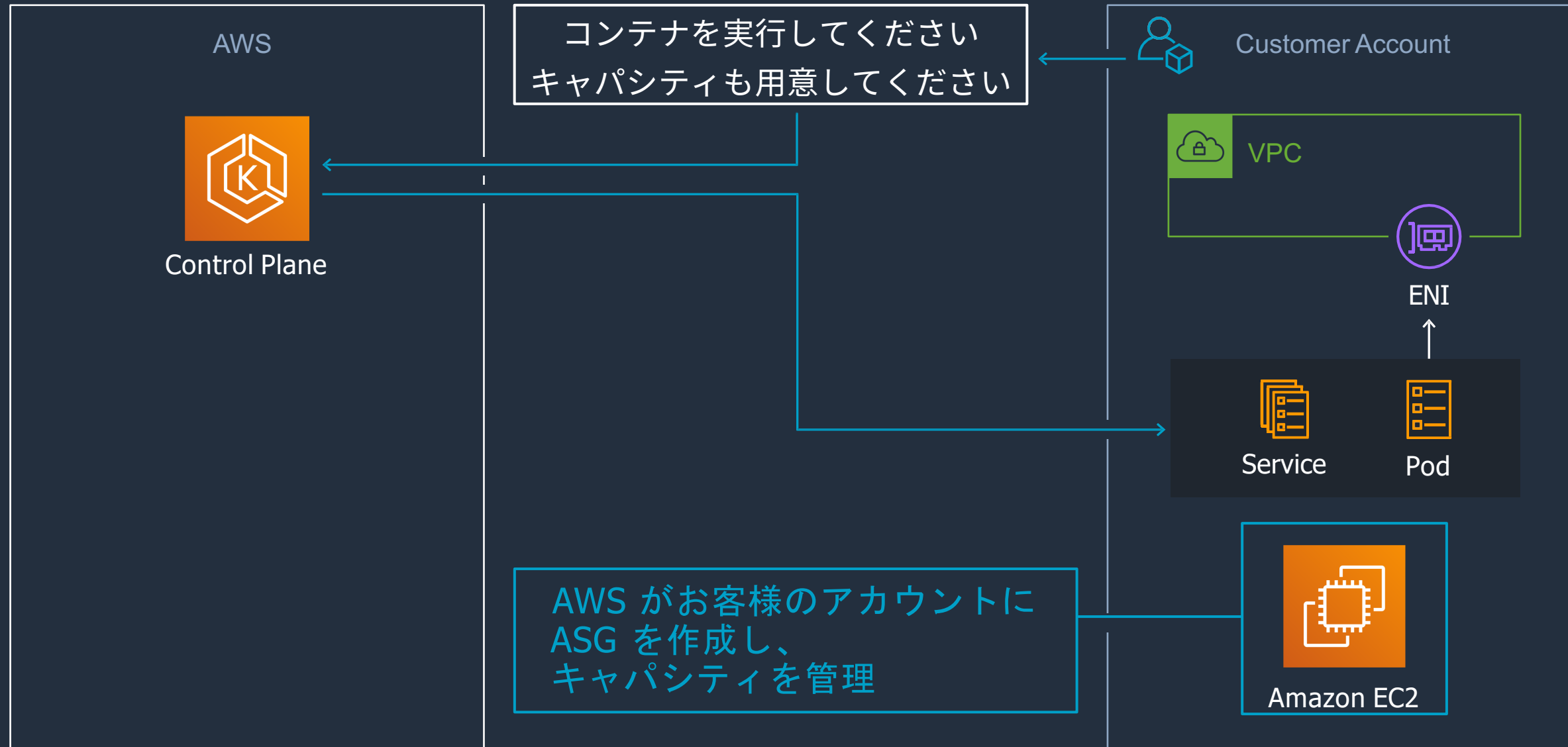
- EKSがお客様のアカウントにASGを作成して管理
- EKSにキャパシティの増減を指示
 - EKSがASGを操作
- Kubernetesのプラクティスを考慮
 - 必要なAWSタグの付与
 - 終了時にノードからPodを退避
 - Spotインスタンスのリバランス・終了通知のハンドリング
- ライフサイクルの管理にフォーカス
 - AMIや起動テンプレートの指定は可能
 - デフォルトでは EKS Optimized AMI を利用

ノードを意識するということ

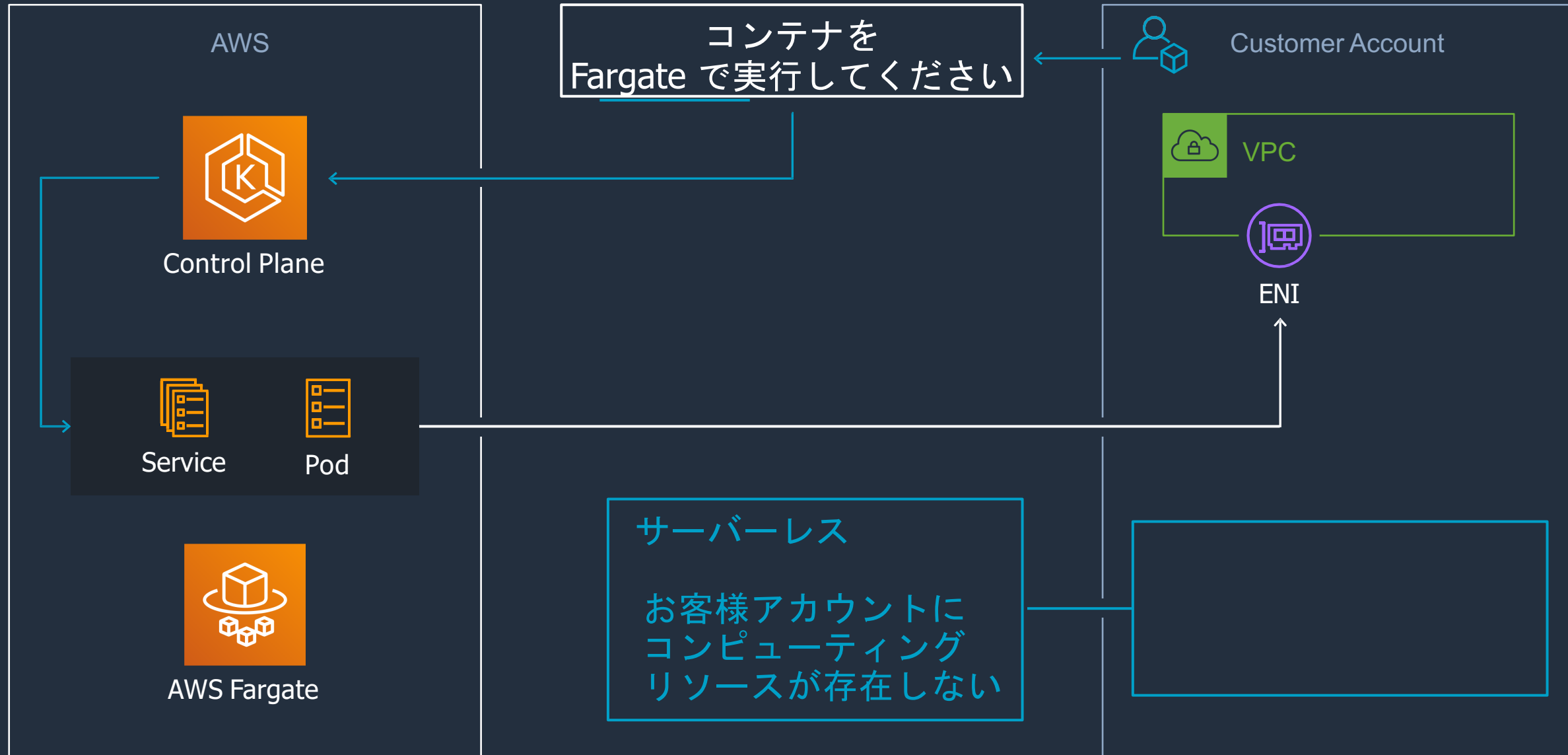


- ノードのサイジング
- ノードのスケールリング
 - Kubernetes Cluster Autoscaler のチューニング
- AMIの管理、更新
 - マネージド型ノードグループではAMI更新はシンプルな作業
 - ノードをローリングアップデートする作業は必要

Fargate



Fargate



Fargate



AWS Fargate



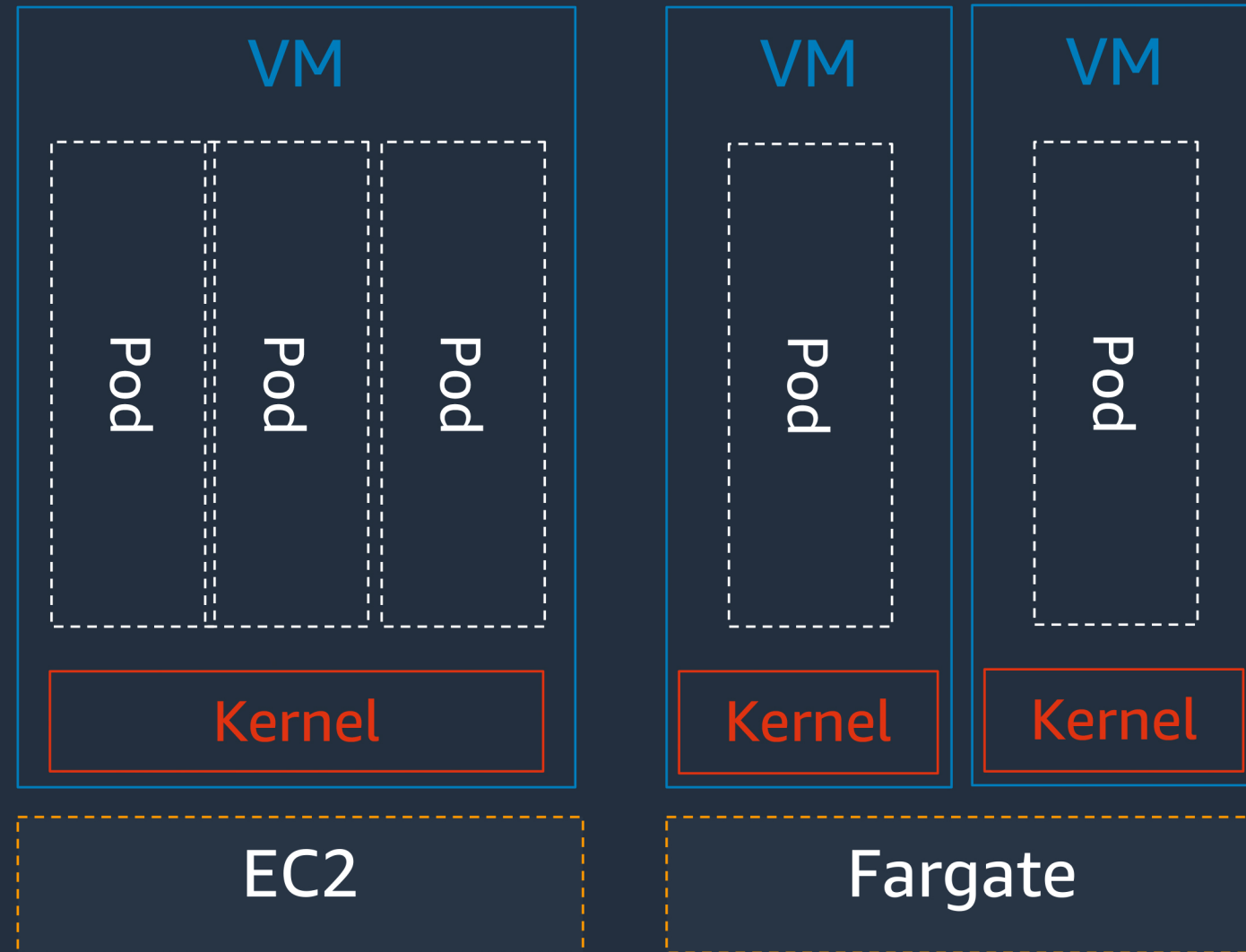
オンデマンドに
リソースを用意



Amazon
EKS

- コンピューティングリソースが
オンデマンドに起動
 - コンテナのサイズに合わせた
リソース
- ワーカーノードのリソース管理が不要
 - スケールイン、アウトの仕組みや
調整
 - インスタンスサイズを選択

Fargateのセキュリティ面でのメリット

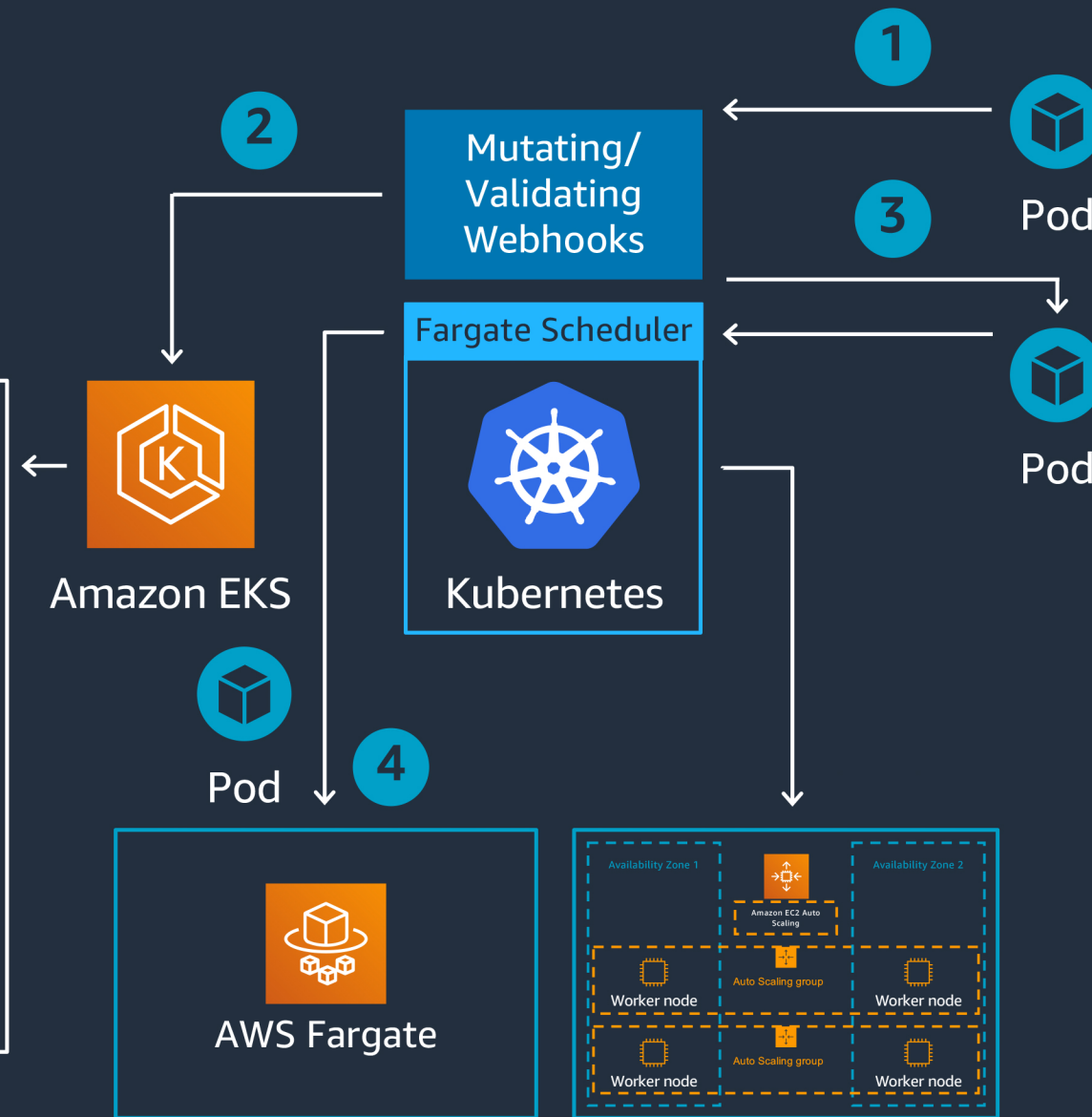


- コンテナは**カーネルを共有**
 - カーネルに脆弱性 -> コンテナから「エスケープ」できるリスク
- **AWS Fargate**
 - Podごとのオンデマンドでリソースを用意
 - VM 分離環境でコンテナ実行

Fargateへのデプロイ方法

Fargate profile

```
{  
  "name": profile-a,  
  "clusterName": mycluster,  
  "podExecutionRole": role-xyz,  
  "subnets": subnet-0ad888345,  
  "selectors": [  
    {  
      "namespace": prod,  
      "labels": {  
        stack: blue  
      }  
    }  
  ]  
}
```

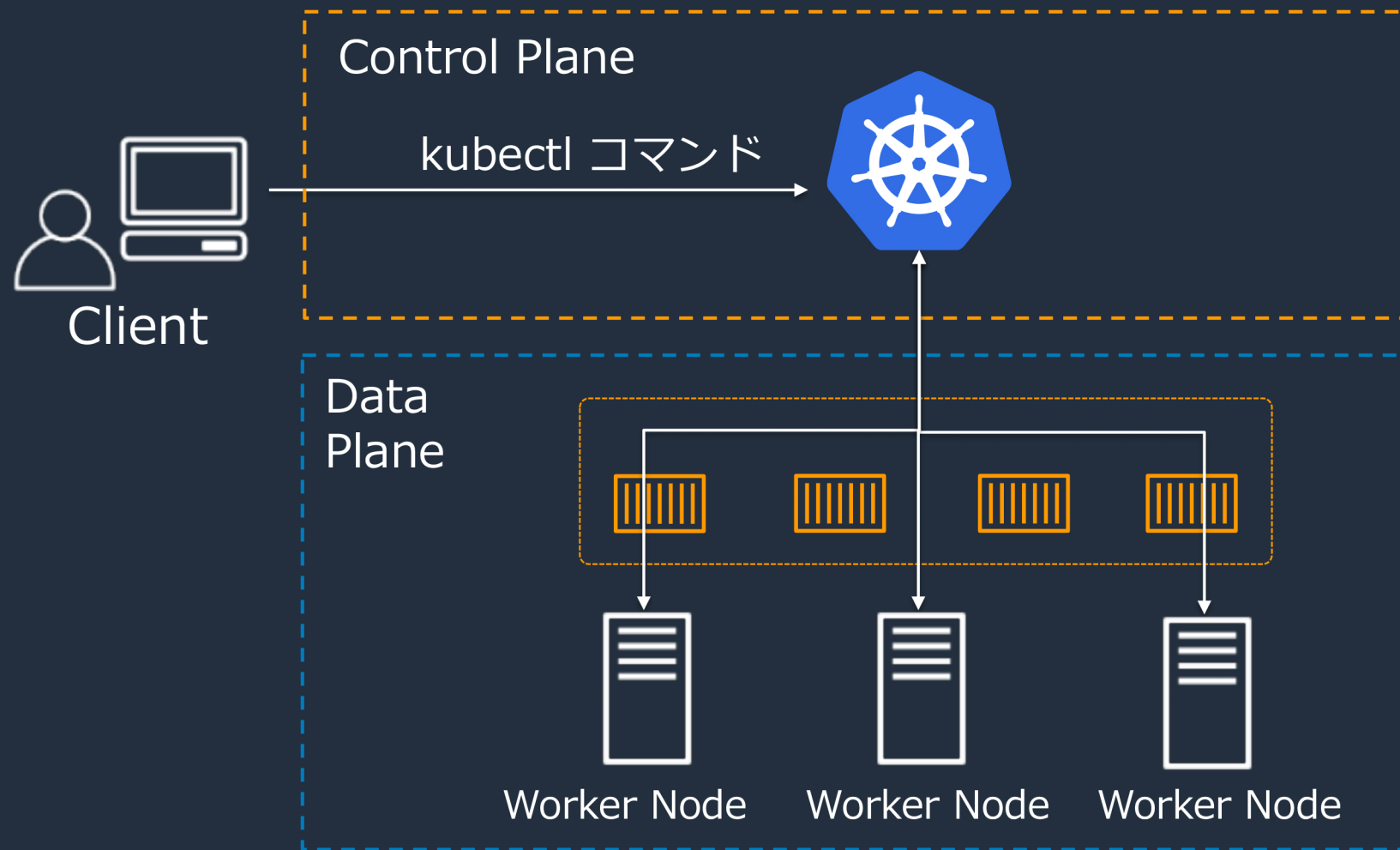


```
namespace: prod  
labels:  
- stack: blue
```

```
namespace: prod  
labels:  
- stack: blue  
- profile = profile-a  
- schedulerName = fargate-scheduler
```

Data Plane 管理の選択方法

EKS の Data Plane 管理のオプションの選択



セルフマネージド型ノード
マネージド型ノードグループ
Fargate

Fargate

- まずFargateが利用できないか検討
- 以下を考慮
 - 未サポート
 - DaemonSets
 - GPU
 - Windowsコンテナ
 - AWS Region外 (AWS Outposts / AWS Wavelength / AWS Local Zones)での運用
 - 利用できるコスト最適化オプション
 - Savings Plans (Compute)
 - Spot は未対応

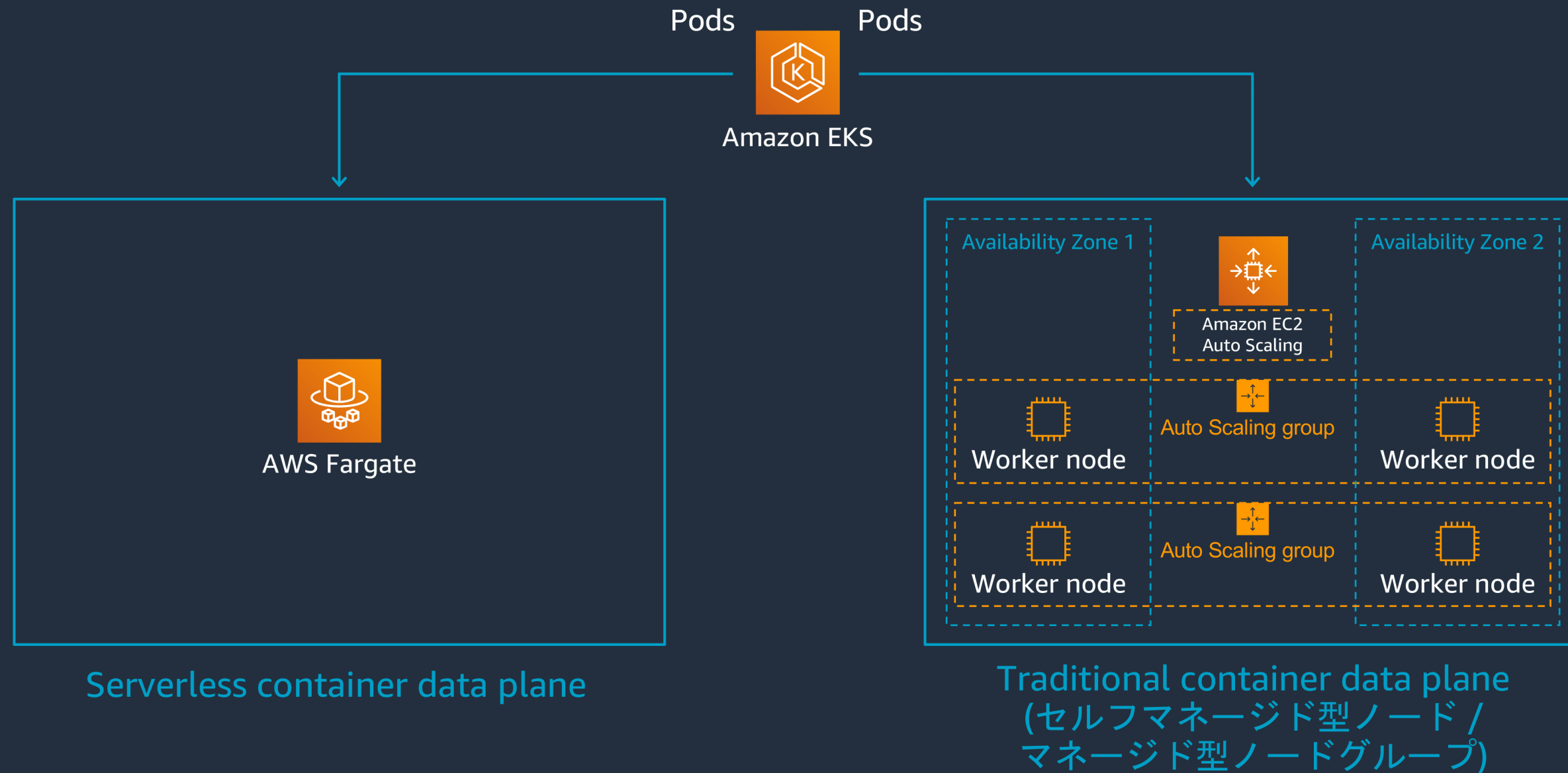
Fargate考慮事項

https://docs.aws.amazon.com/ja_jp/eks/latest/userguide/fargate.html#fargate-considerations

マネージド型ノードグループ

- 幅広い機能をサポート
- 以下を考慮
 - 未サポート
 - Windowsコンテナ
 - AWS Region外 (AWS Outposts / AWS Wavelength / AWS Local Zones)での運用
 - 利用できるコスト最適化オプション
 - Savings Plans (Compute / Instance)
 - Amazon EC2 リザーブドインスタンス
 - Amazon EC2 スポットインスタンス
 - AWS Graviton2

Data Planeの管理オプションは併用可能



AWS Containers Roadmap

<https://github.com/aws/containers-roadmap/projects/1>

aws / containers-roadmap

Watch 710 Star 3.9k Fork 211

Code Issues 897 Pull requests Actions Projects 1 Security Insights

containers-roadmap Updated 2 days ago

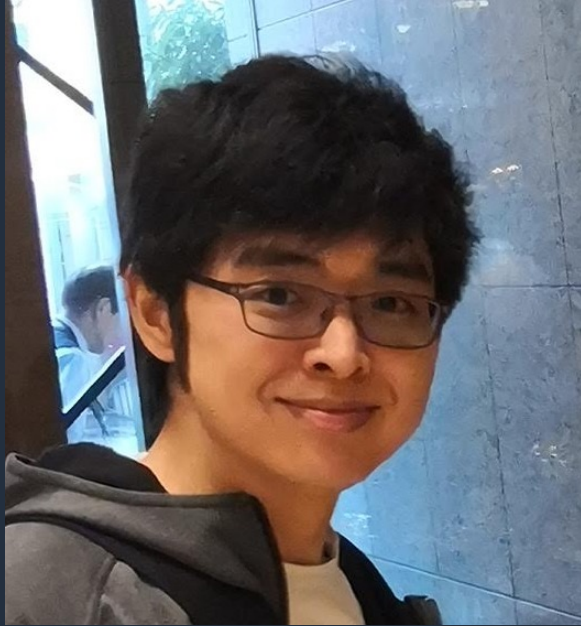
Filter cards Fullscreen Menu

- 85 Researching**
 - [Fargate] [request]: Enhance the reliability of FireLens on Fargate #700 opened by PettitWesley (Fargate, FluentBit, Proposed, Under consideration)
 - [EKS/Fargate] Support for Wildcard * Namespaces #621 opened by tabern (EKS, Fargate)
 - [EKS] [request]: Notifications / More control over EKS Master Node Patch Rollouts #604 opened by johnpemberton (EKS, Proposed)
 - [EKS] [request]: On create: only return ACTIVE when endpoint actually usable #654 opened by dpiddockcmp (EKS, Proposed)
- 50 We're Working On It**
 - [EKS/Fargate] support for Fargate in all regions #620 opened by tabern (EKS)
 - [Fargate] : Ephemeral volume encryption using CMK managed through AWS Key Management Service (KMS) #915 opened by akshayram-wolverine (Fargate, Proposed)
 - [EKS] [request]: A reliable EKS AMI release process #319 opened by max-rocket-internet (EKS, Proposed)
 - [Fargate/ECS] [Image caching]: provide image caching for Fargate. #696 opened by matthewcumplings (ECR, ECS, Fargate, Work in Progress)
- 9 Coming Soon**
 - [ECS] [Fargate Task Storage]: Allow permission configuration of Fargate bind mounts #938 opened by Alex-Richman (Fargate PV1.4, Fargate, Proposed)
 - [EKS][Fargate]: Cannot enrich logs with Parser filter in Fargate logging with fluentbit #1203 opened by itsprds (EKS, Fargate, Issue/Bug)
 - [ECR] [request]: Improve scanning #798 opened by runningman84 (Coming Soon, ECR)
 - [EKS] [request]: Managed Nodes scale to 0 #724 opened by mikestef9 (EKS Managed Nodes, EKS)
 - [EKS]: Kubernetes v1.16 End of
- 2 Developer Preview**
 - [ECS] ECS Development in IntelliJ, PyCharm, and Visual Studio Code #272 opened by cbbbarclay (Developer Preview, ECS, Fargate)
 - [ECS] [request]: Ability to update task- placement constraints and strategy of a service that has already been created #136 opened by mhumeSF (ECS, Proposed)
- 287 Just Shipped**
 - [EKS] [request]: Provide safe transition from managed to self managed add-on deployments #1415 opened by ben-mccown (Add-Ons, EKS, Proposed)
 - [EKS] Increased pod density on smaller instance types #138 opened by tabern (EKS)
 - [EKS] [request]: Support Kubernetes 1.21 #1334 opened by billinghamj (EKS, Proposed)
 - [EKS] [CRI]: Support for Containerd CRI #313 opened by paavan98pm (EKS)
 - [EKS] [request]: Managed Node

まとめ

- Amazon EKS での Data Plane 管理オプション
 - セルフマネージド型ノード
 - マネージド型ノードグループ
 - Fargate
- Data Plane 管理オプションの選択方法

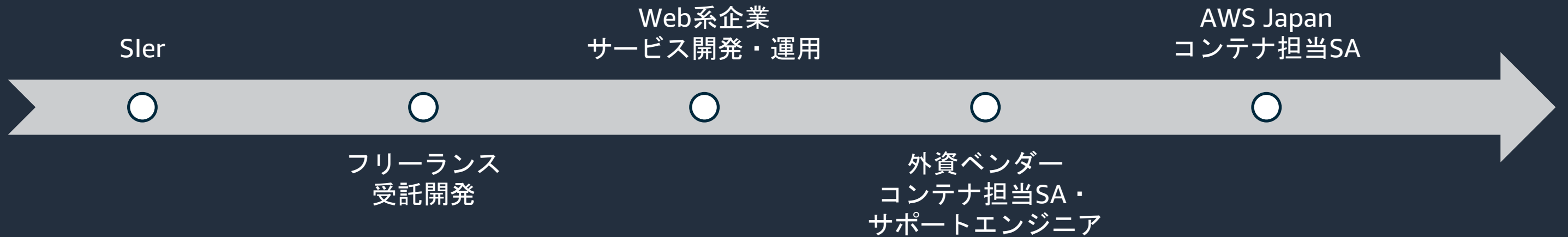
自己紹介



Specialist Solutions Architect, Containers

好きなサービス

Amazon Elastic Kubernetes Service (Amazon EKS)
AWS Certificate Manager



Thank you