

コンテナを有効活用したいあなたへ

AWS コンテナサービス入門 2020

Shinichi Hama

Solutions Architect

Amazon Web Services Japan/ Solutions Architecture



Shinichi Hama

 track3jyo

Solutions Architect

Amazon Web Services Japan

- 自宅にいます
- 西日本担当。AWSの大阪オフィスにいます
- Container 関連の業務も担当しています

<好きな AWS サービス>

Amazon Elastic Container Service(Amazon ECS),
Amazon Elastic Kubernetes Service(Amazon EKS), AWS Fargate



本セッションは…

想定聴講者

- docker run はしたことがあるし、コンテナの特性はなんとなく知っている
- AWS 上でコンテナ化したアプリケーション環境構築を検討中
- AWS が提供するコンテナサービスそれぞれの特徴、どういう時に使うものかを知りたい

ゴール

- コンテナ自体が解決する課題、そして AWS の各コンテナサービスが解決しようとしている課題を理解する
- AWS の各コンテナサービスの特徴や利用用途を知り、自身のアプリケーションをコンテナ化して AWS 上で動かす際にどのコンテナサービスが必要か判断できるようになる

Agenda

コンテナとは

コンテナオーケストレーション

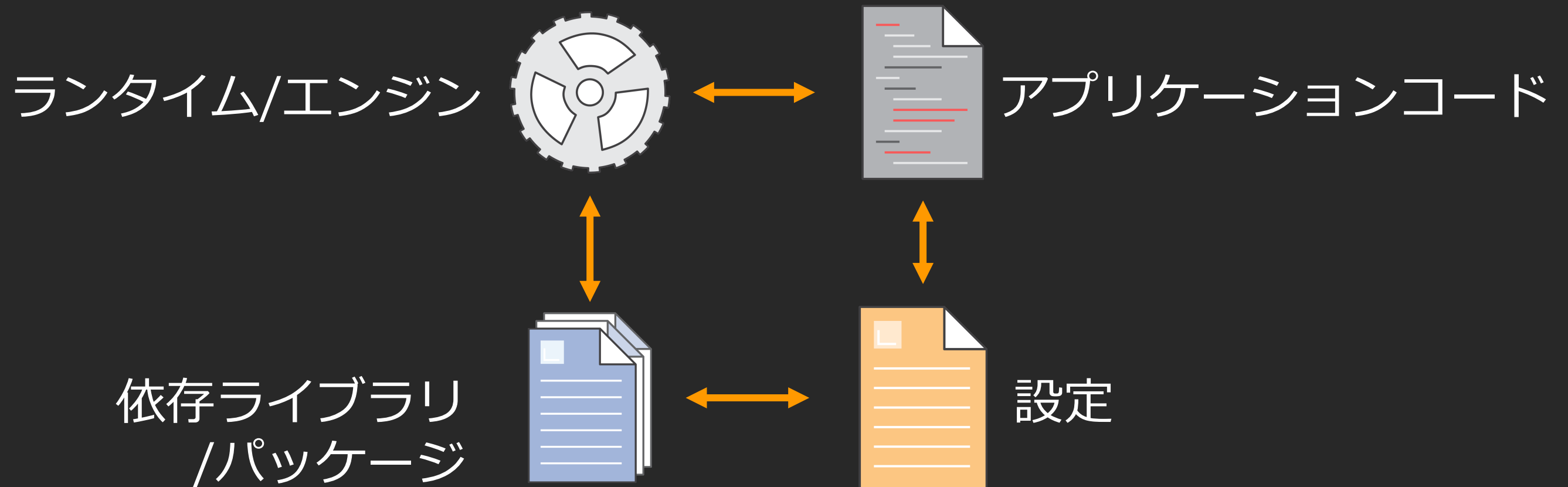
イメージレジストリ

コンテナ実行環境

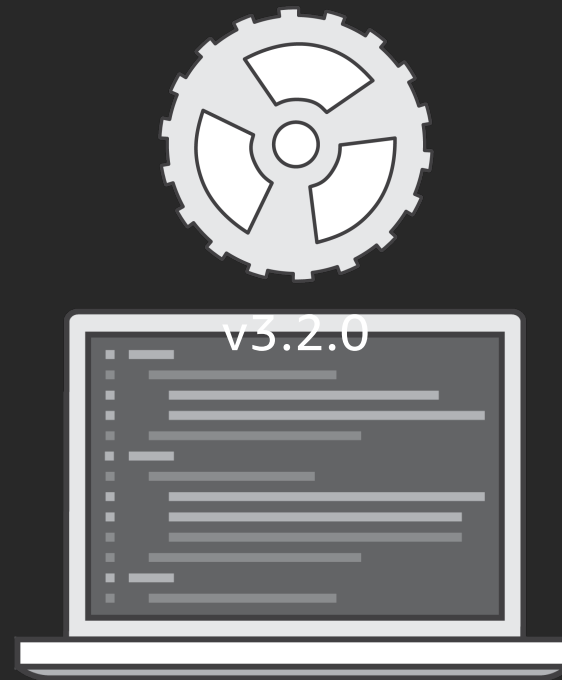
これから始める AWS でのコンテナワークロード

コンテナとは

アプリケーションを構成するコンポーネント



ローカルでは動いたけど、本番で動かない？



ローカルラップトップ

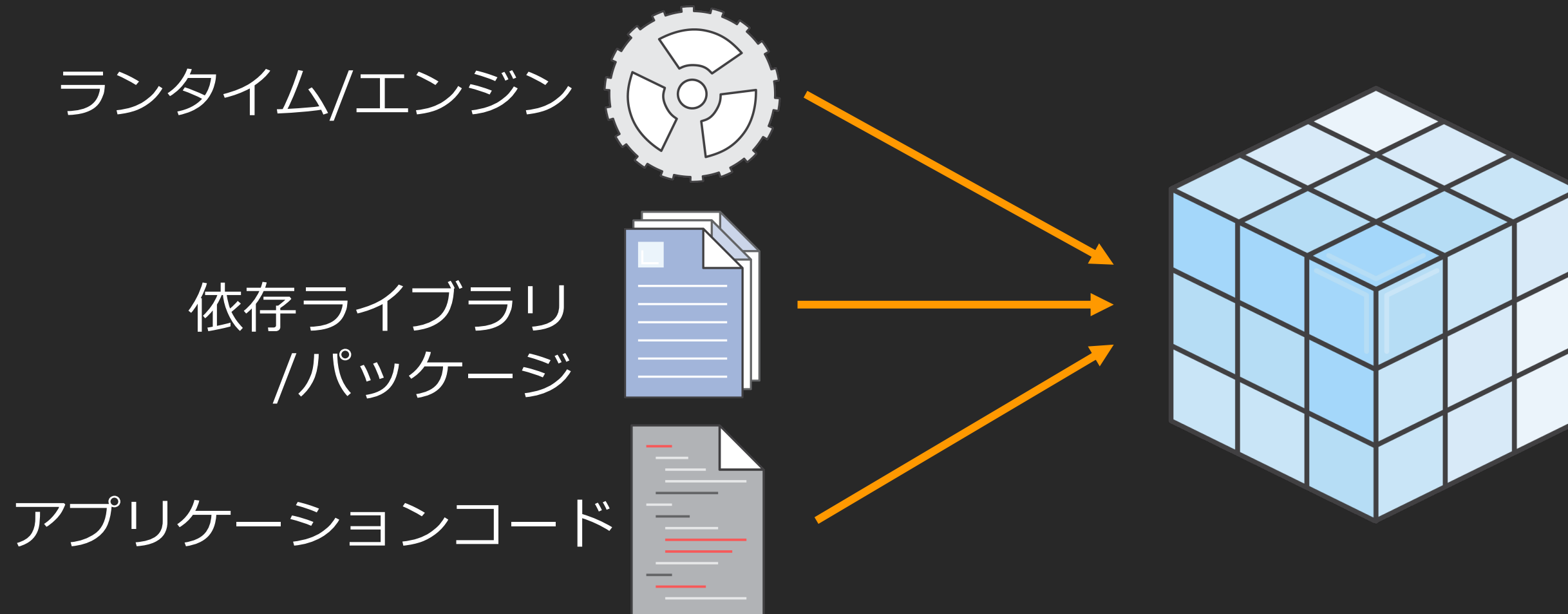


ステージング / QA



本番

「コンテナ」という解決策



Docker

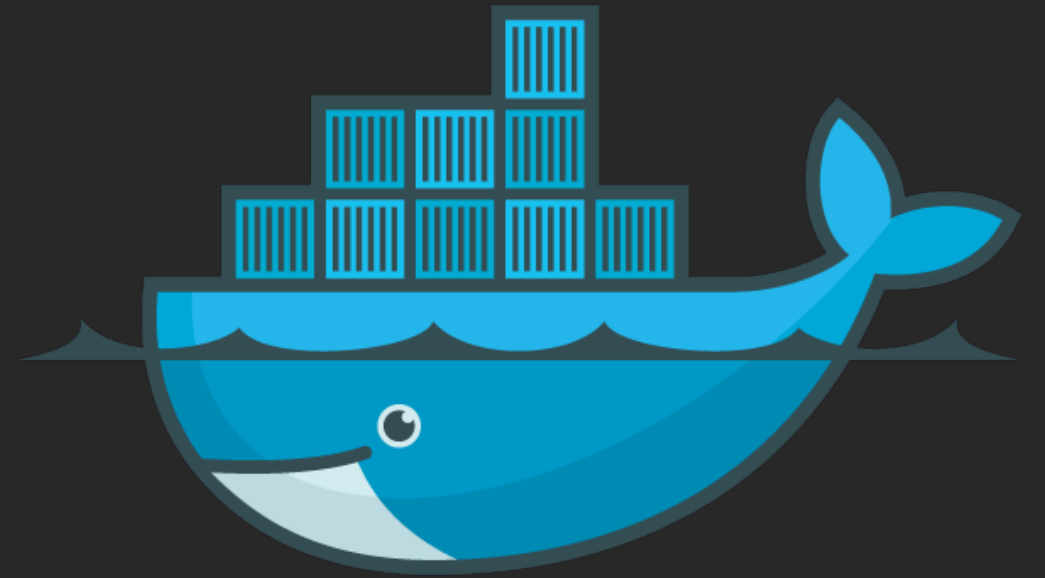
Docker 社が開発

Apache 2.0 ライセンス

2013年3月 OSS リリース

常駐型コンテナ実行エンジン

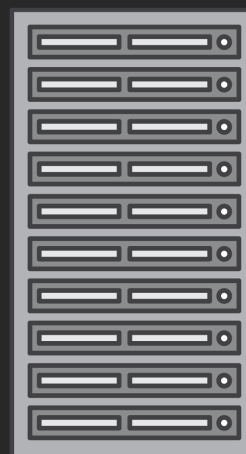
コンテナのライフサイクル管理・デプロイツール



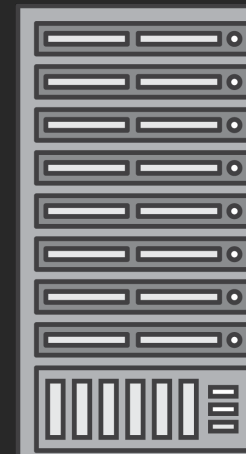
全ての環境で同じコンテナを動かす



ローカルラップトップ

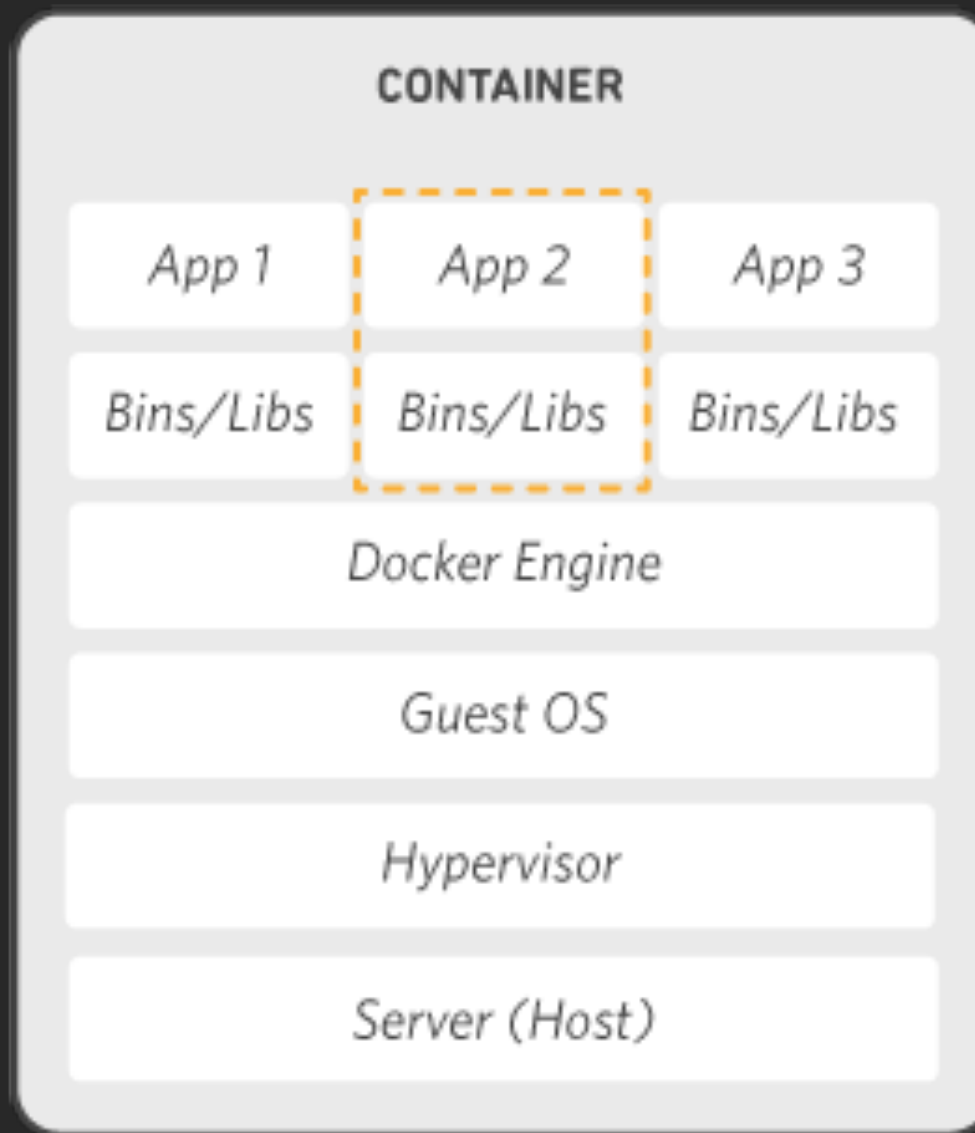
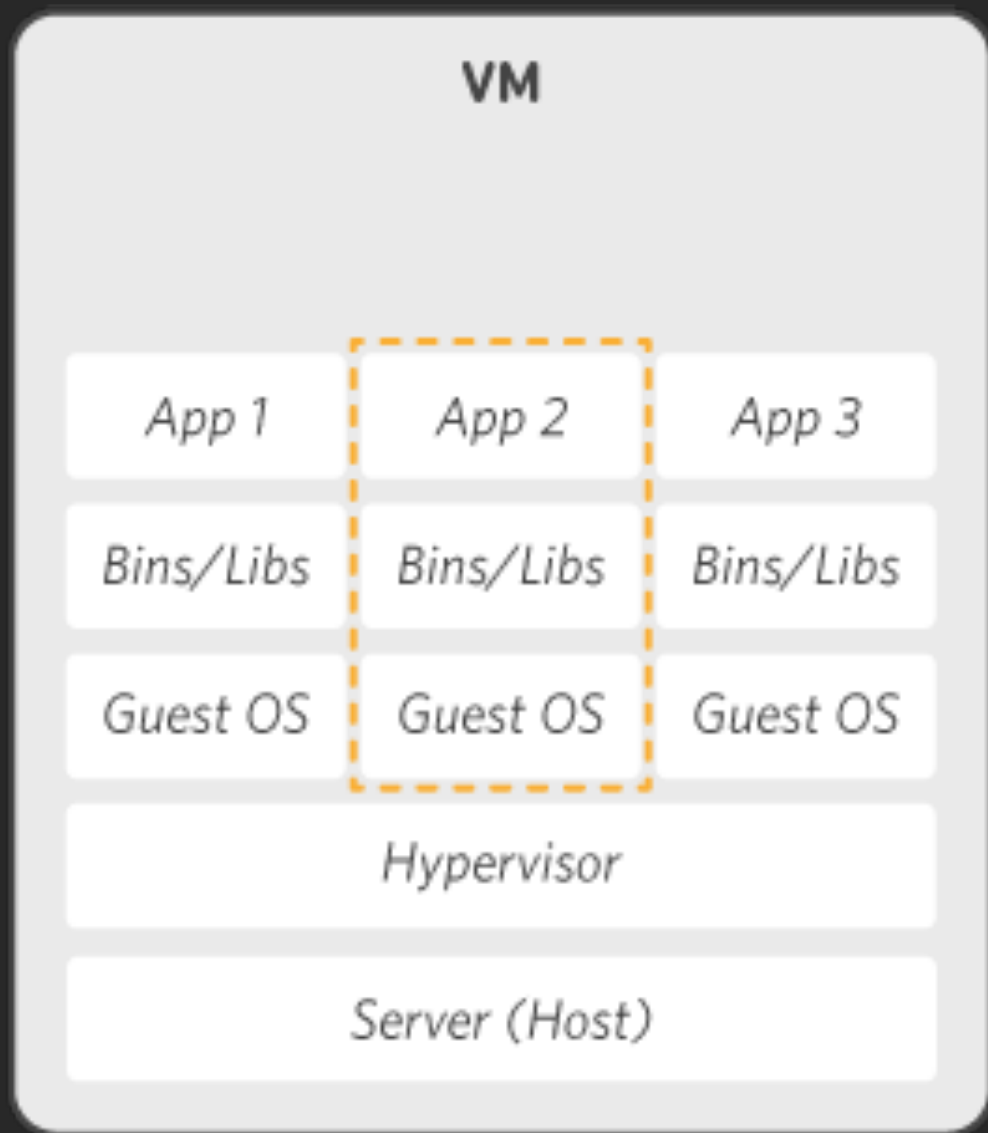


ステージング / QA



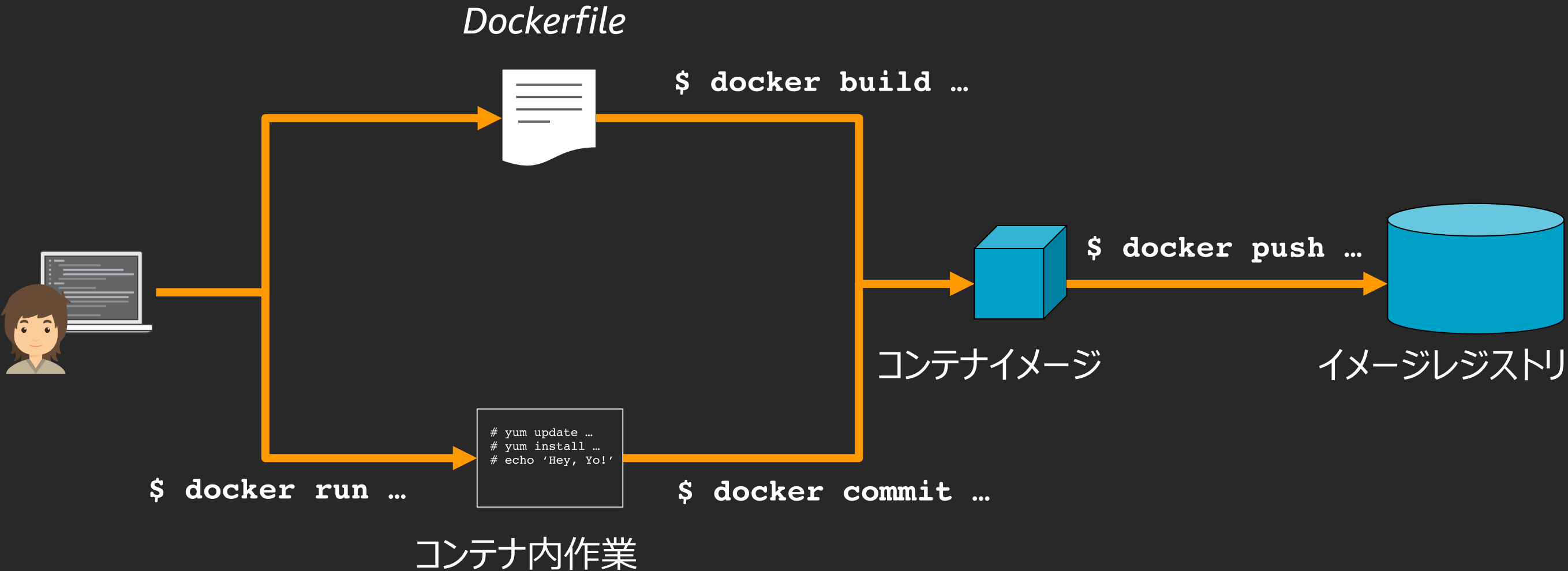
本番

仮想マシンとコンテナ



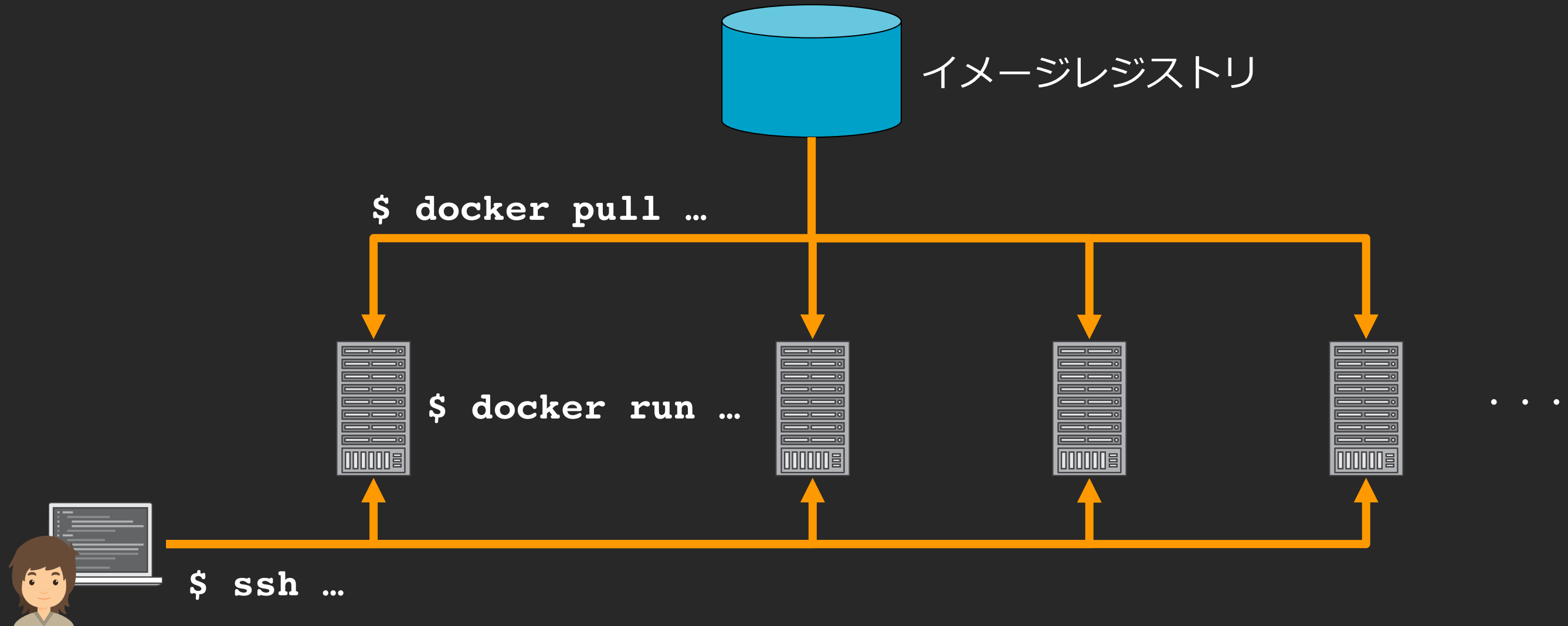
Dockerを利用した基本的ワークフロー

- コンテナイメージ作成 -



Dockerを利用した基本的ワークフロー

- コンテナ実行 -



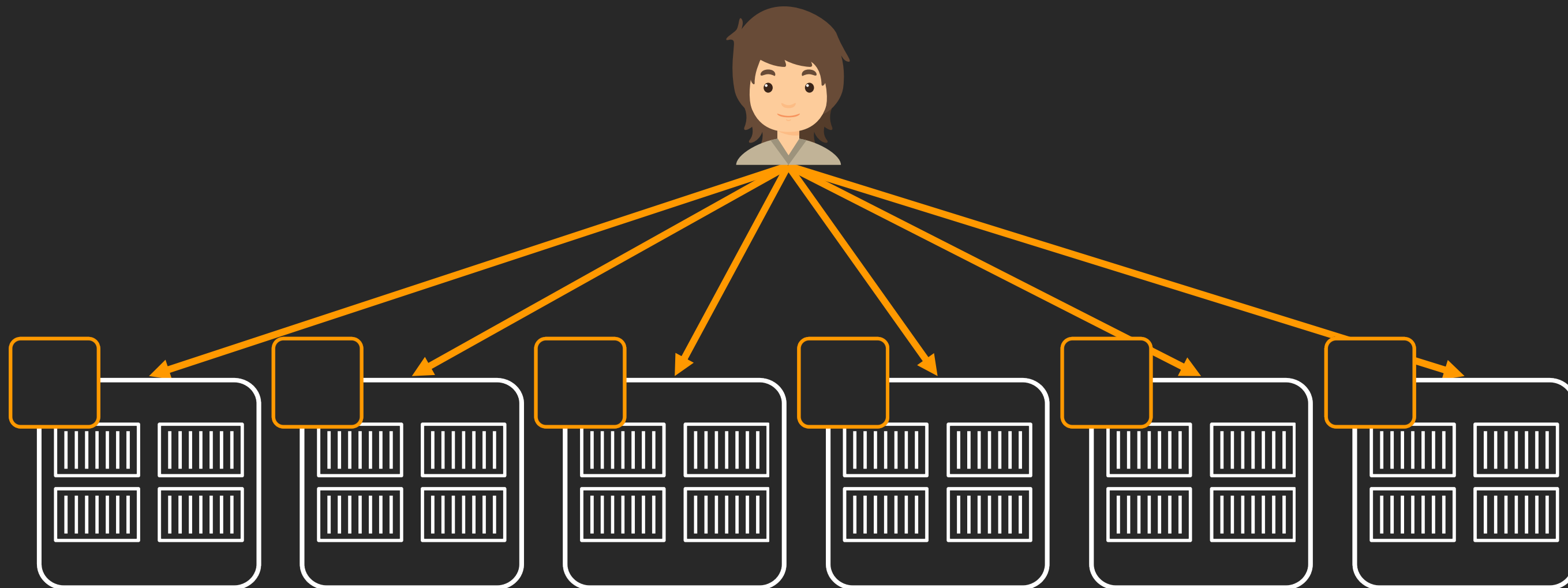
思っていたよりも手作業？



- Docker の責務は**同一サーバ上**のコンテナライフサイクル管理
- **複数サーバやコンテナを束ねた概念**に対するオペレーションは
スコープ外

コンテナオーケストレーション

手作業でのコンテナイメージダウンロードと実行は 非効率かつミスオペレーションを招く



「この EC2 インスタンスの
クラスターでコンテナを
実行したいです」



Amazon ECS

「このコンテナを3つのAZに
分散させて10個デプロイして、
このロードバランサーに
つないでください」



Amazon Elastic Container Service (ECS)

- クラウドでコンテナを本番環境利用するためのオーケストレーター
- 各種 AWS サービスとの高度な連携
- 多様なワークロードをサポートする「タスク」「サービス」というシンプルなリソース表現
- Linux/Windows サポート



Amazon ECS

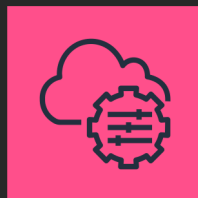
サービス紹介ページ

<https://aws.amazon.com/jp/ecs/>

Amazon ECS と各種AWSサービスの高度な連携



AWS
Secrets Manager



AWS Systems Manager
Parameter Store

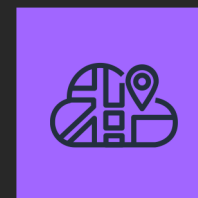


Amazon Simple
Storage Service(S3)

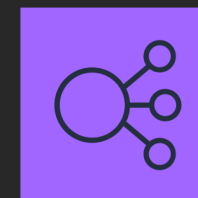
Secrets/Configs



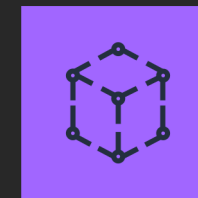
Amazon VPC



AWS Cloud Map

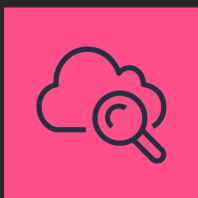


Elastic Load
Balancing(ELB)

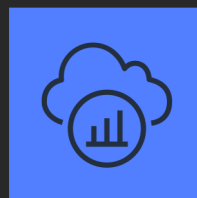


AWS App Mesh

ネットワークング



Amazon
CloudWatch



AWS X-Ray

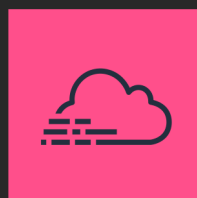
モニタリング



AWS Identity and
Access Management (IAM)



Amazon GuardDuty

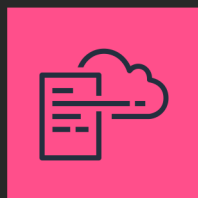


AWS CloudTrail

セキュリティ



Amazon ECS



AWS CloudFormation

laC



Amazon Elastic
File System(EFS)

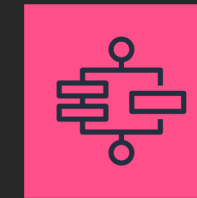
NFS

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

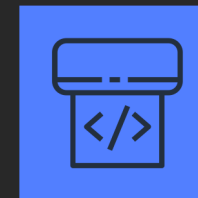


Amazon EventBridge

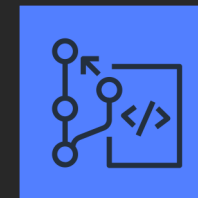
Job実行



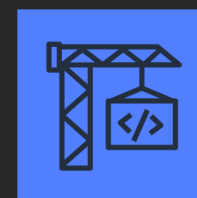
AWS Step Functions



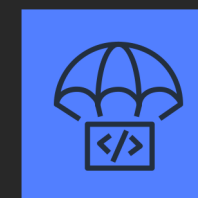
AWS CodePipeline



AWS CodeCommit



AWS CodeBuild



AWS CodeDeploy

CI/CD



kubernetes

- たくさんのお客様が EC2 上にセルフマネージドな Kubernetes を動かしていました
- Kubernetes の周りにおける OSS のエコシステムやその拡張性の高さを望まれていました

Amazon Elastic Kubernetes Service(EKS)

- 運用難易度の高い Kubernetesをマネージドで提供
- エコシステムの OSS やツールを利用できる, CNCF certified
- 各種 AWS サービスとの連携
- EKS サービスチーム、OSS チームによる Kubernetes コミュニティへの貢献
- “Pod”、“Deployment”、“Service”、“Job”などのリソースに代表される高い表現力



Amazon EKS

サービス紹介ページ

<https://aws.amazon.com/jp/eks/>

多種多様な OSS との連携

各種コミュニティにより開発された多種多様なエコシステムとの連携

モニタリング



Prometheus



Grafana

CI/CD



Argo CD



Spinnaker

サービスメッシュ



Istio



LINKERD

ネットワーキング



CNI



CoreDNS



- Kubernetes のパッケージマネージャ
- 各 OSS のインストールやパッケージの展開が可能

コントロールプレーン



Client

kubectl コマンド



Amazon EKS



mycluster.eks.amazonaws.com

データプレーン



Availability
Zone 1



Availability
Zone 2



Availability
Zone 3

Phase 1

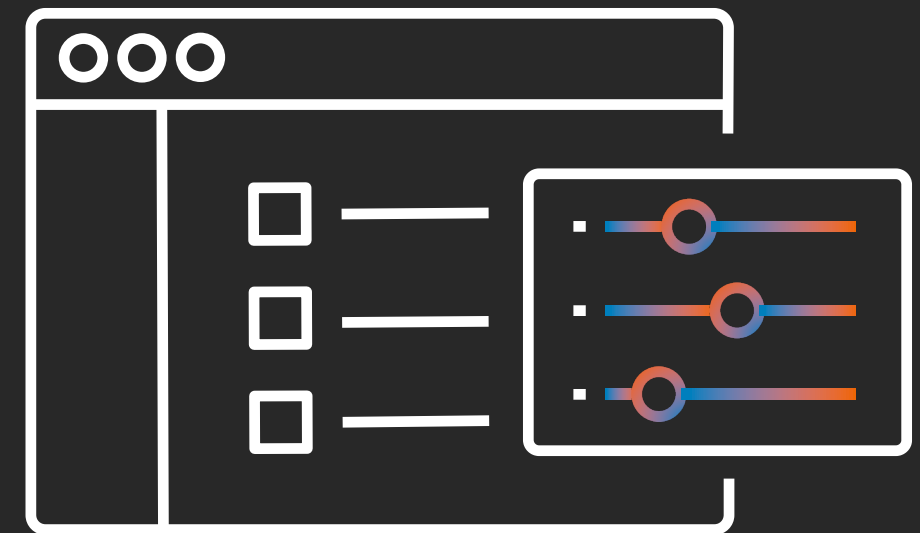
Kubernetes

コントロールプレーンの管理

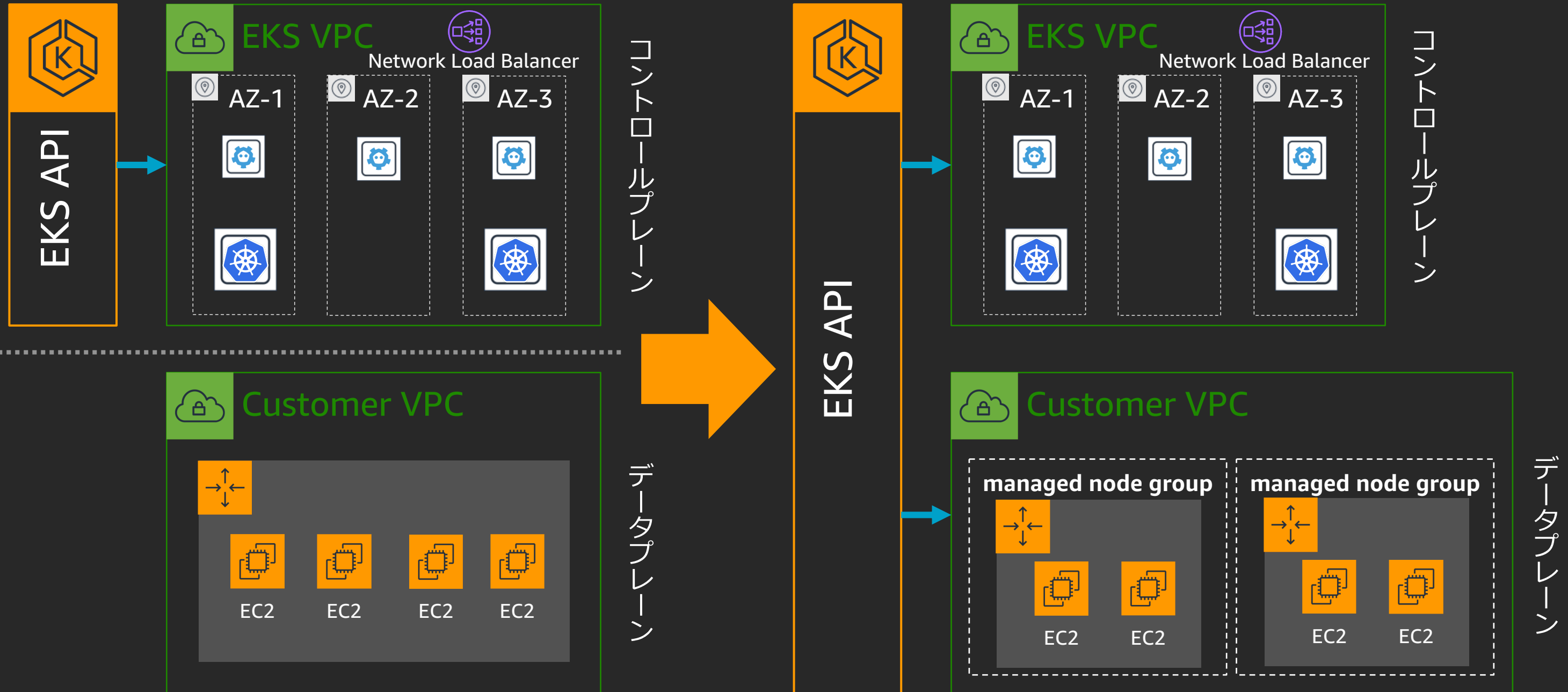
Phase 2

Kubernetes

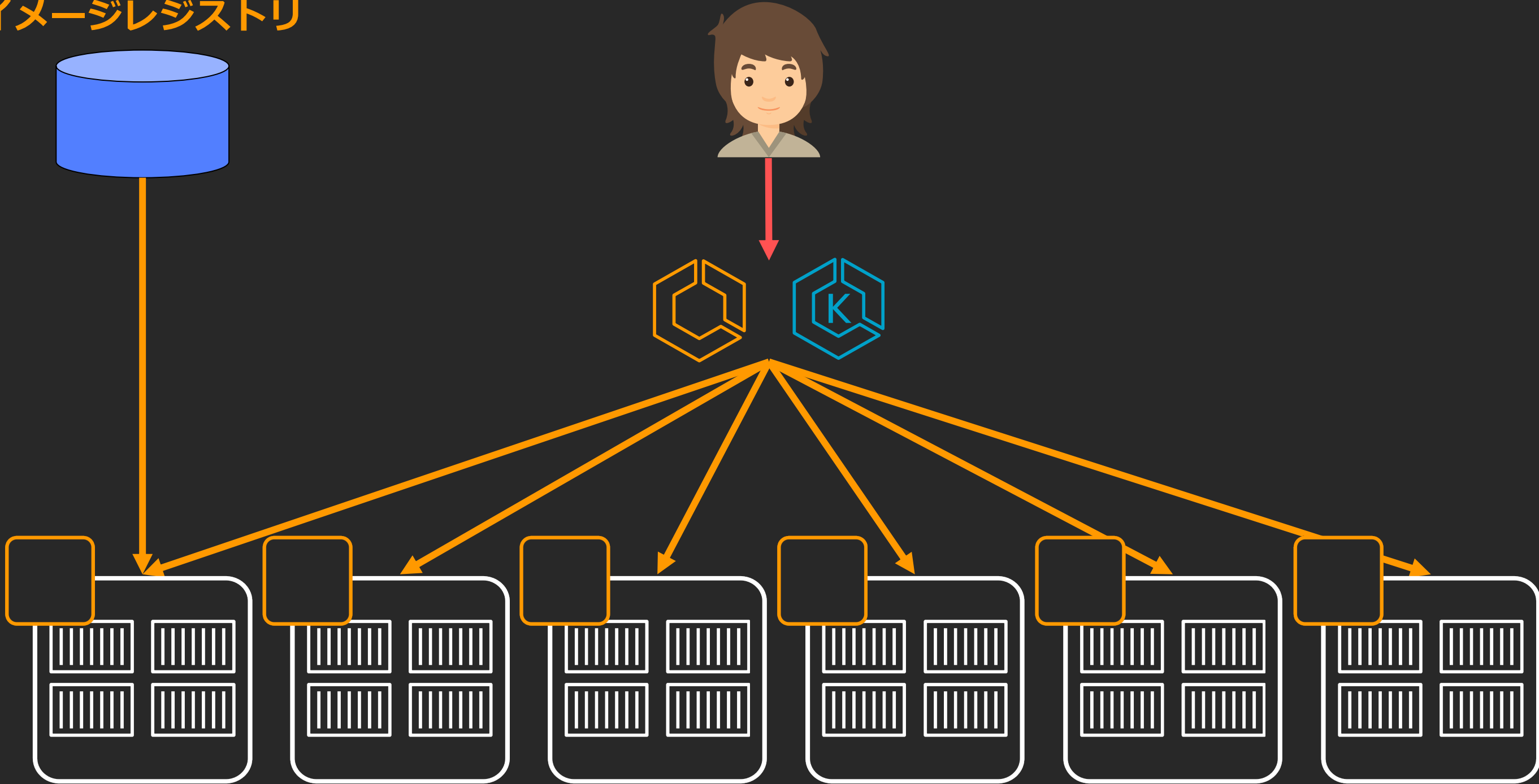
データプレーンの管理



Amazon EKS Managed Node Groups



イメージレジストリ



イメージレジストリ

Amazon Elastic Container Registry (ECR)

- フルマネージドなプライベートコンテナイメージレジストリ
- セキュア – 保管イメージの自動的な暗号化、IAM 連携
- スケーラブルかつ高い可用性
- Docker CLI からの利用
- ECS/EKS/Kubernetes だけでなく、その他コンテナオーケストレーションツールからも利用可能



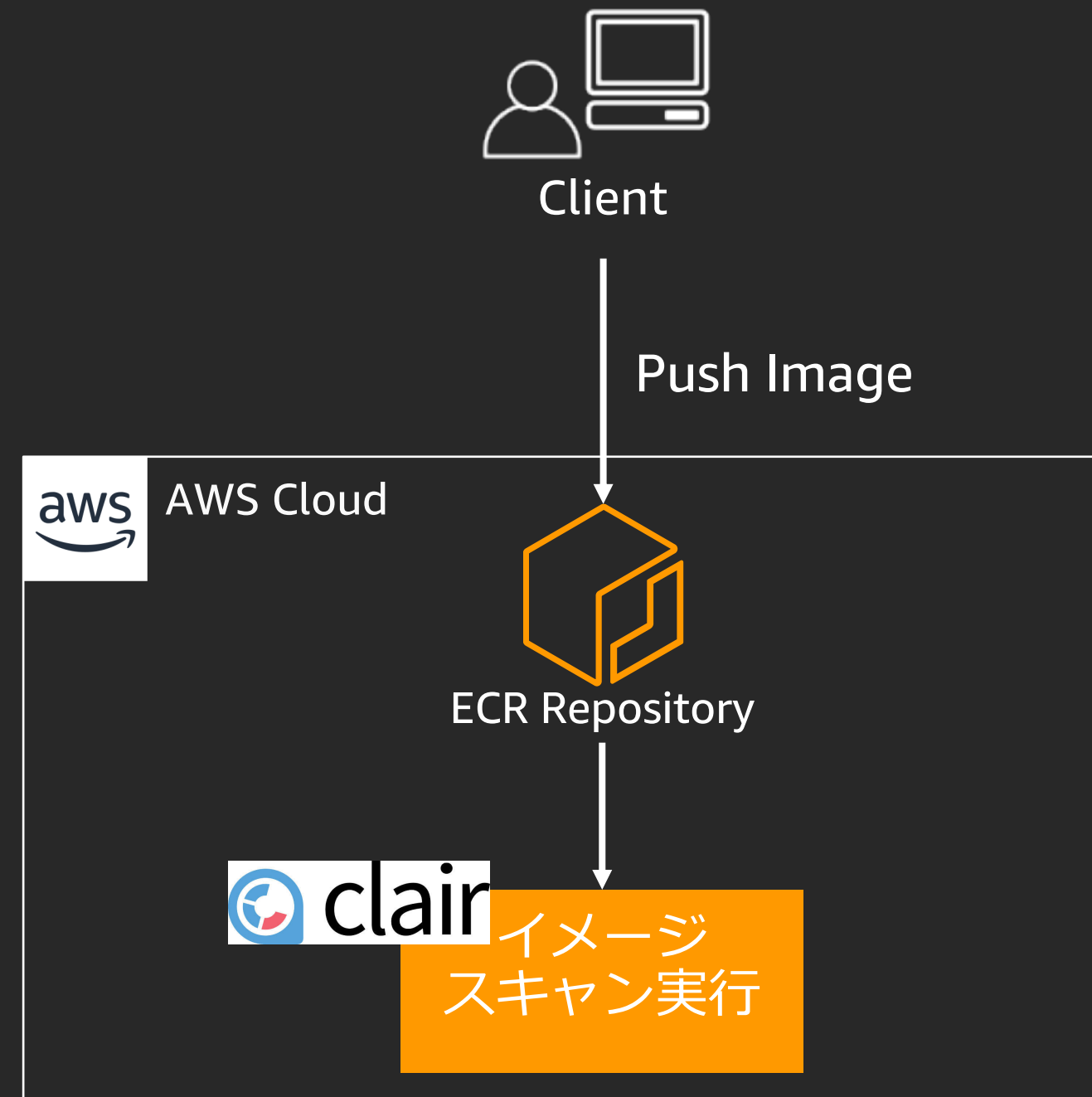
Amazon ECR

サービス紹介ページ

<https://aws.amazon.com/jp/ecr/>

Amazon ECR のイメージスキャン機能

- ECR ネイティブの機能として提供される脆弱性 (CVEs) の静的スキャン機能
- OSS の CoreOS Clair を利用
- コンテナイメージ Push 時の自動スキャンが可能
- スキャンにかかる費用は無料



コンテナ実行環境



Amazon ECS



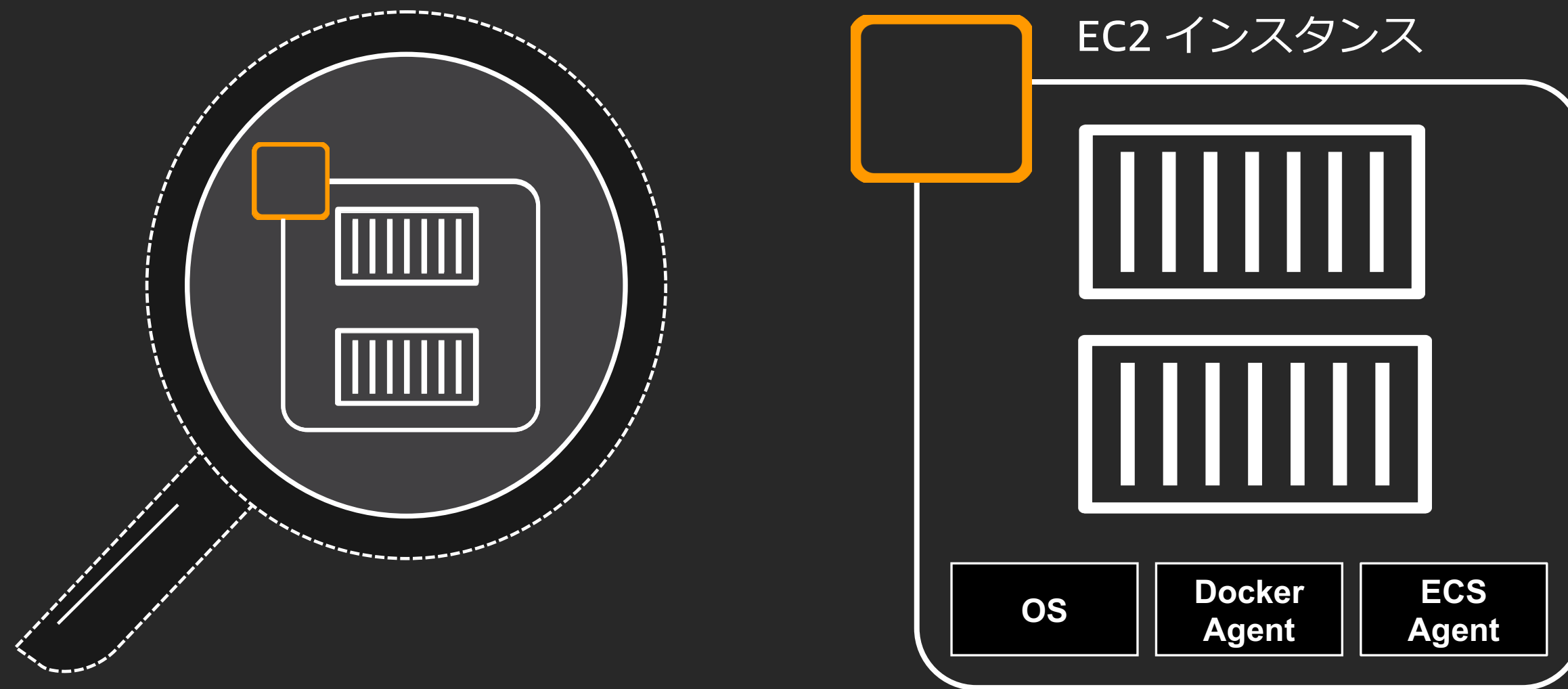


Amazon ECS

コンテナ実行環境



実行環境 EC2 インスタンスの運用業務



- OS やエージェント類へのパッチ当て・更新
- 実行中のテナ数に基づく、最適なリソース使用率を保つための EC2 インスタンス数のスケーリング

AWS Fargate



AWS マネージド

EC2 インスタンスのプロビジョン、スケール、管理不要

コンテナネイティブ

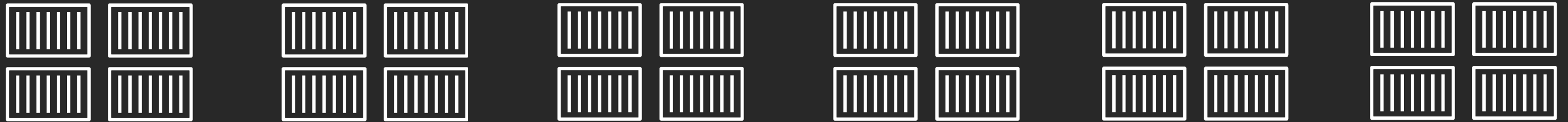
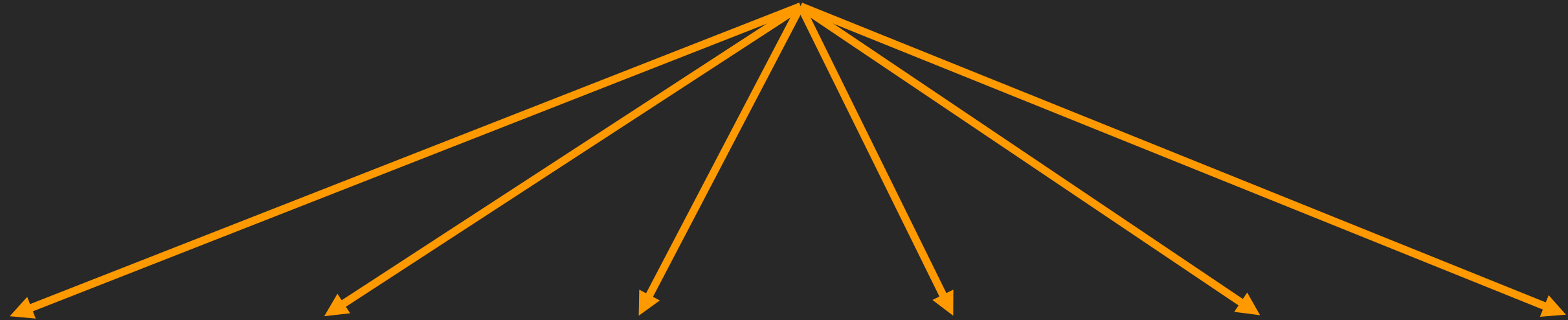
仮想マシンを意識しないシームレスなスケールリング
コンテナの起動時間・使用リソースに応じた料金設定

AWS サービスとの連携

VPC ネットワーキング、Elastic Load Balancing、IAM、
CloudWatch、etc.



Amazon ECS

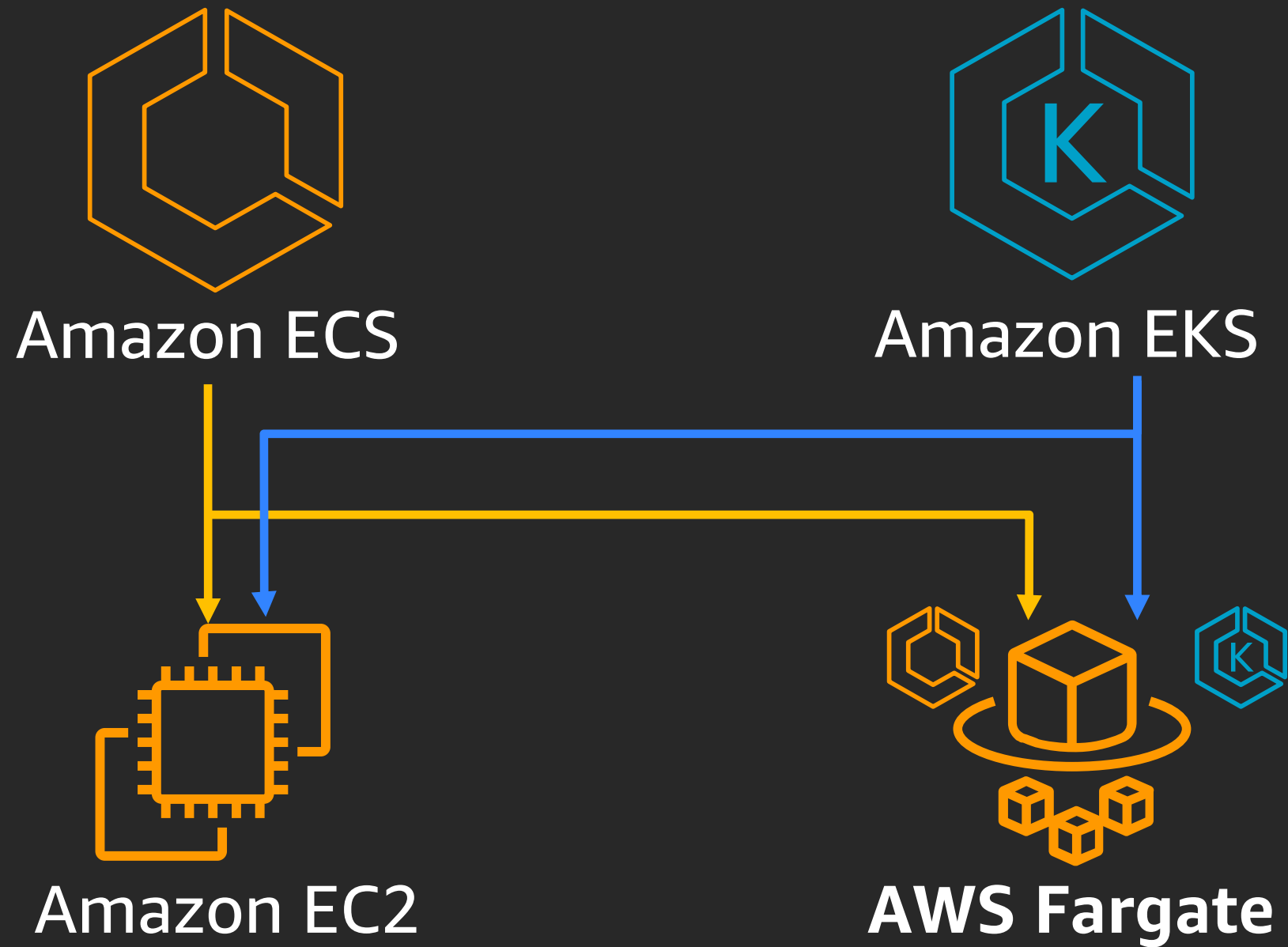


AWS Fargate

Amazon EKS on AWS Fargate



AWS 上でのコンテナ実行における幅広い選択肢

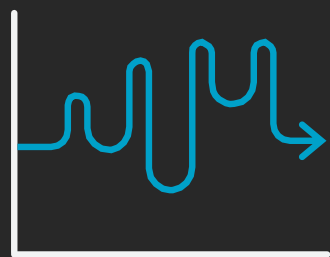


AWS Fargate 購入オプション

Fargate の価格面での障壁を取り除いてきました

Fargate

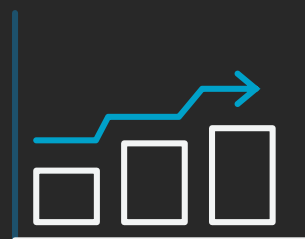
長期的なコミットなしで、コンテナに割り当てたリソースの秒単位での従量課金



短期的・スパイクのある・予測不可能なワークロードに最適

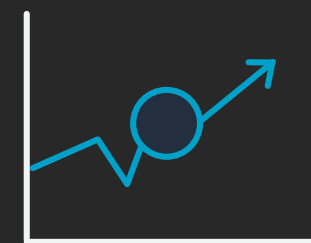
Compute Savings Plans (new) Fargate Spot (new)

1年もしくは3年間の1時間あたりの利用金額をコミットすることで、大幅な割引を受けます



長期的・予測可能なワークロードに最適

空きキャパシティのリソースを Fargate の標準価格の最大 70% 割引で利用できます

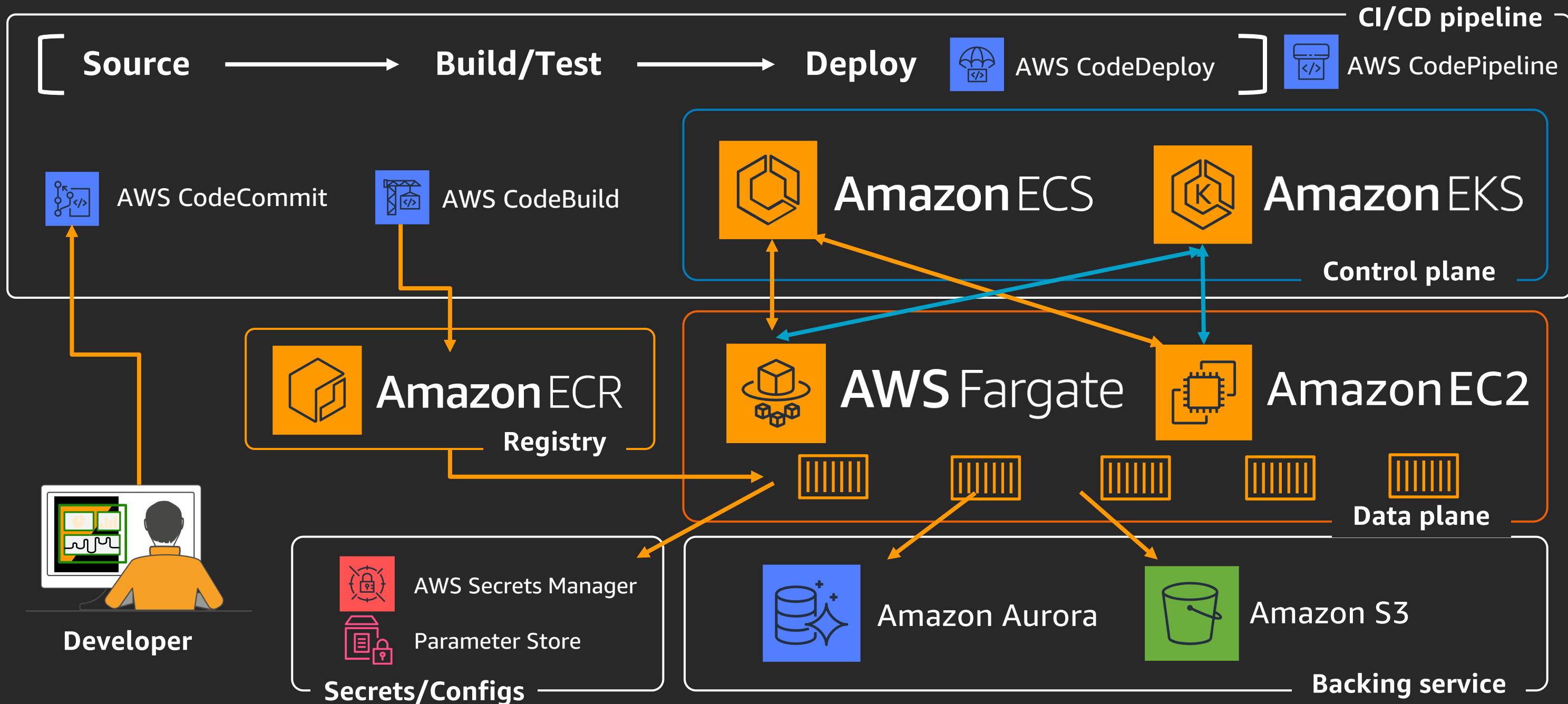


中断への耐性があるワークロードに最適

2019年1月に Fargate の価格を50%値下げしました

これから始める
AWSでのコンテナワークロード

周辺を支えるサービス群



選定指針のエッセンス

- Fargate は AWS でのコンテナ実行における最初の選択肢
- マネージドサービスがあるものをコンテナサービスでやろうとしていないか？
 - 全てをコンテナでやろうとしていませんか？

サーバレス・仮想マシンも含めて、自分たちのワークロードにあうコンピューティングを適宜使い分けましょう

AWSコンテナサービスを数字で見る

80%

クラウドのすべてのコンテナ化された実行中のアプリケーションのうち
AWS で実行されている割合

150%

AWS コンテナサービスの
前年比の成長

10倍

1 年間の EKS 使用量の増加

3倍

1 年間の Fargate 使用量の増加
毎週 1 億タスクを実行

20億以上

ECR を使用した毎週 Pull される
Image の数

<https://aws.amazon.com/jp/containers/>

コンテナ関連サービスの公開ロードマップ

The screenshot displays the AWS Containers Roadmap on GitHub, organized into five columns based on project status:

- Researching (53 items):** Includes requests for IPv6 support in Fargate, increasing container disk space, enhancing FireLens reliability, and unified observability solutions.
- We're Working On It (60 items):** Features work on Fluent Bit logs, AWS Service Operator, ephemeral volume encryption, capacity providers, and EKS AMI release processes.
- Coming Soon (11 items):** Announces support for Fargate in all regions, Kubernetes v1.13 end of support, KMS encryption for ECR, and CloudFormation integration for ECR scanning.
- Developer Preview (4 items):** Shows development progress for ECS in IDEs, ECS CLI v2, support for ARM nodes, and task-placement constraints.
- Just Shipped (160 items):** Celebrates the release of offline private subnet support, ASG capacity deletion, EC2 Inf1 instances, ephemeral volume encryption, CloudFormation version upgrades, and new EKS regions.

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

まとめ: AWS のコンテナ関連サービス

オーケストレーション

デプロイメント、スケジューリング、スケーリング



Amazon ECS



Amazon EKS

イメージレジストリ

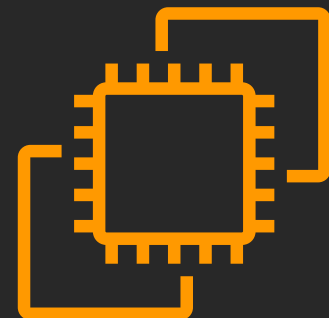
コンテナイメージの格納



Amazon ECR

ホスティング

コンテナ実行環境



Amazon EC2



AWS Fargate

関連セッション

AWS-21: モダンアプリケーションのためのアーキテクチャデザイン
パターンと実装

清水 崇之, Sr. Solutions Architect, Manager, Amazon Web Services Japan

AWS-26: AWSの継続的インテグレーション/デリバリー総まとめ！
モダンアプリケーション構築のためのCI/CDベストプラクティス！

福井 厚, Sr. Specialist SA, Serverless, Amazon Web Services Japan

AWS-34: 最高の "Kubernetes on AWS" を実現するために

Tori Hara, Sr. Product Developer Advocate, Containers Product, Amazon Web Services

Thank you!

Shinichi Hama
hamashi@amazon.co.jp

 track3jyo

Appendix : その他のコンテナ関連サービス

AWS Cloud Map



AWS
Cloud
Map

クラウドリソースのためのサービスディスカバリ

各リソースに対する継続的なヘルスチェック

ディスカバリ対象サービスの変更に合わせた動的な更新

開発生産性の向上

全アプリケーションリソースをディスカバリ可能な単一のレジストリ

ユーザーフレンドリーな名前の設定

AWS コンテナサービスとの連携

AWS Fargate、Amazon ECS、Amazon EKS

AWS App Mesh



アプリケーションレベルのネットワーク (サービスメッシュ)

ログ・メトリクス・トレース情報の容易な出力
クライアントサイドのトラフィック・ルーティングポリシー
データプレーンに Envoy proxy を利用

単一のクラスタやコンテナサービスを超えて動作

Amazon ECS、Amazon EKS、Kubernetes on EC2、
AWS Fargate、Amazon EC2

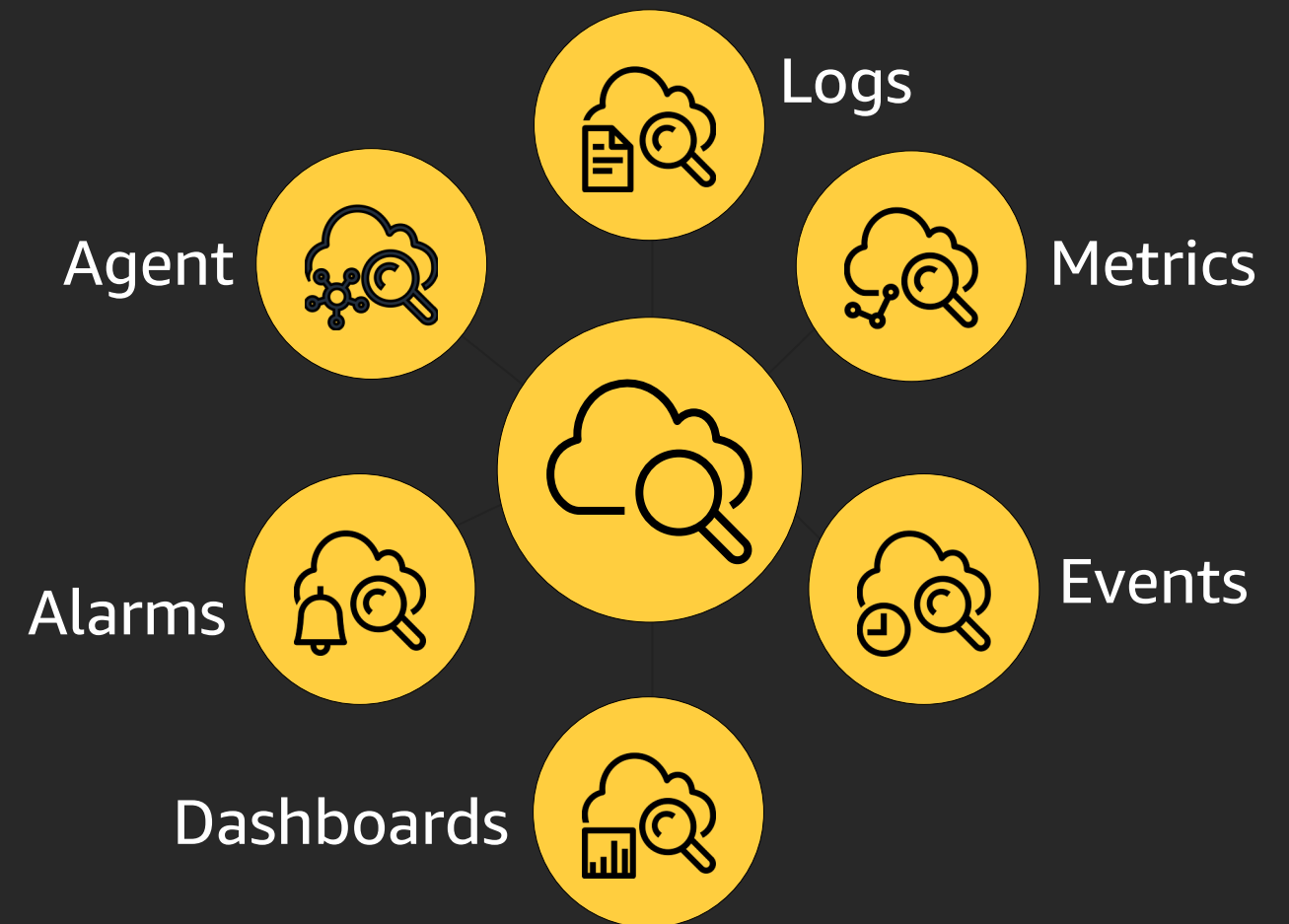
マネージド

コントロールプレーンの管理不要
容易なオペレーション
高いスケーラビリティ

Amazon CloudWatch Container Insights

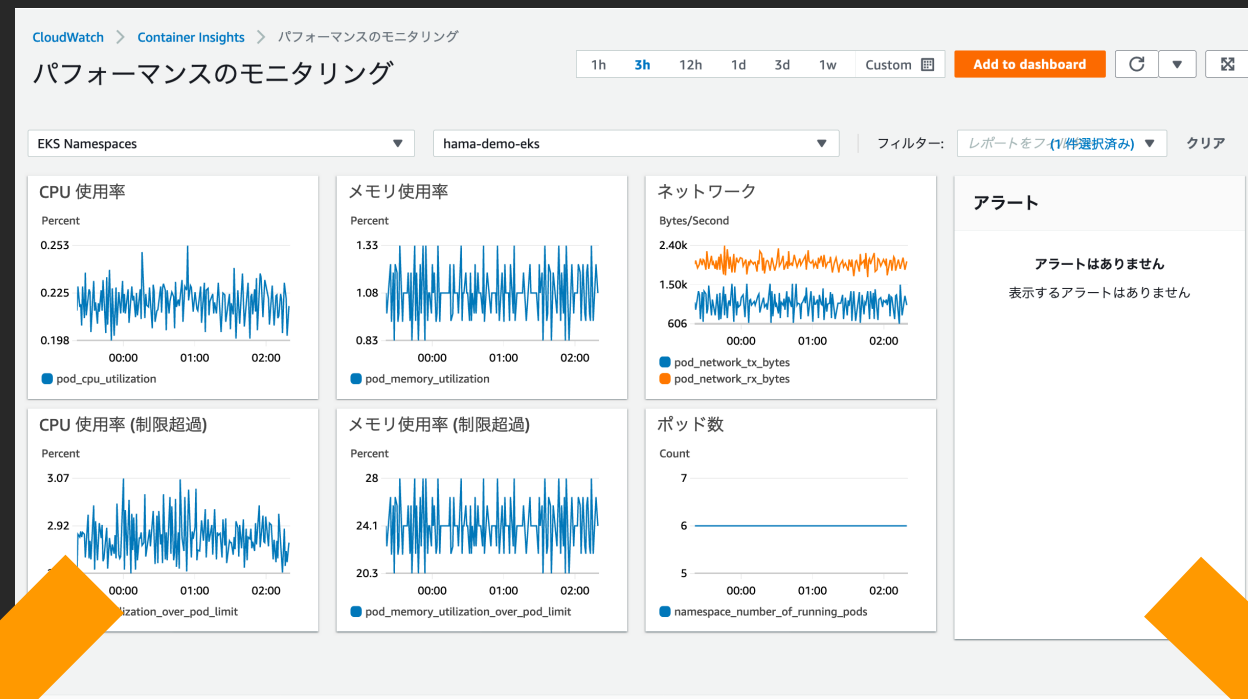
AWS 上でコンテナ化されたアプリケーションに特化した監視・トラブルシューティングおよびアラームのためのモニタリングサービス

- ✓ 自動ダッシュボードによる可視化、分析
- ✓ CloudWatch Logs Insights やX-Rayを利用した詳細なドリルダウンが可能
- ✓ Amazon ECS およびAmazon EKS、Amazon EC2 の Kubernetes にてご利用可能



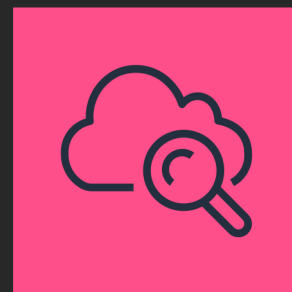
Amazon CloudWatch Container Insights

- Container Insights のダッシュボードを起点により詳細な分析が可能
 - CloudWatch Logs Insights や X-Ray



CloudWatch Logs Insights の要件の例

- グラフのより詳細な値を見たい
- ログに対し分析クエリを発行したい



Amazon CloudWatch
Logs Insights

X-Ray を使う要件の例

- タスク間の通信をトレースしたい



AWS X-Ray

CloudWatch Container Insights Map 表示

β版

