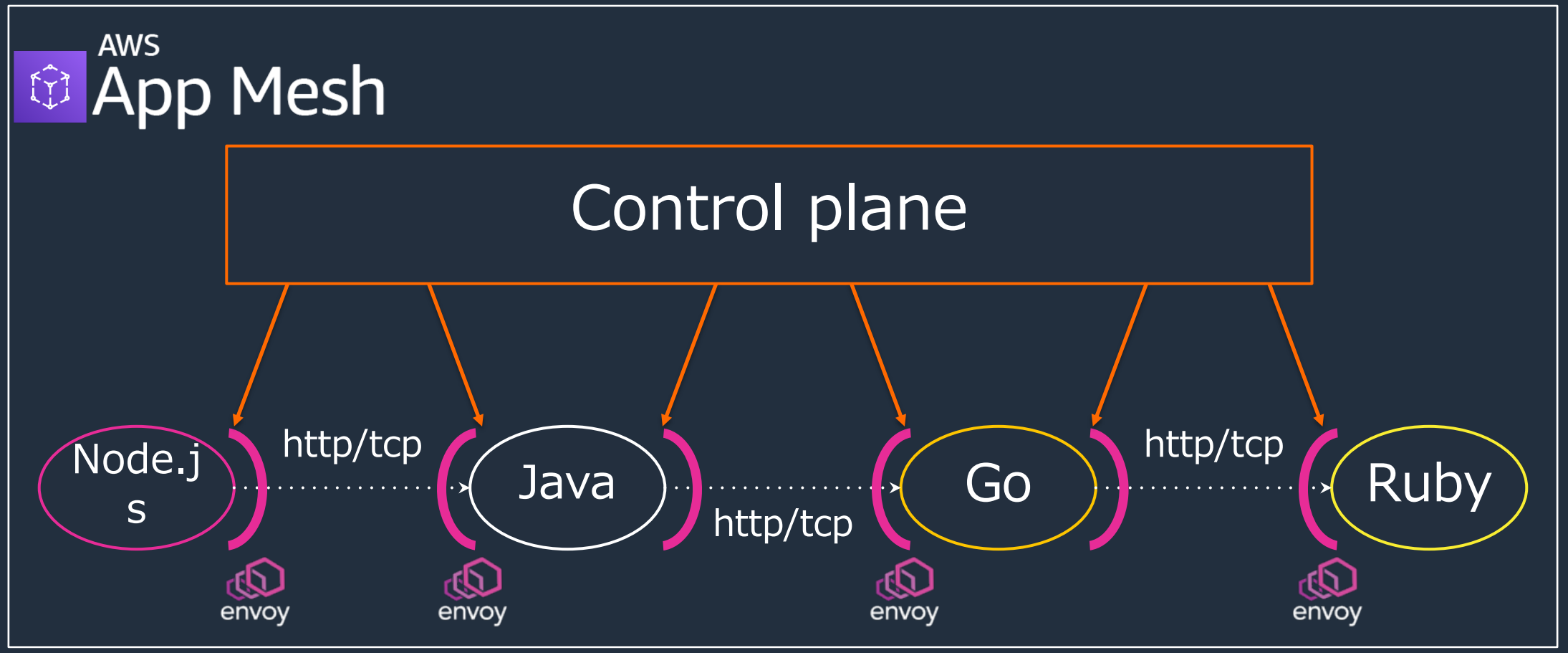
AWS Blackbelt Container

AWS App Mesh

2021-12

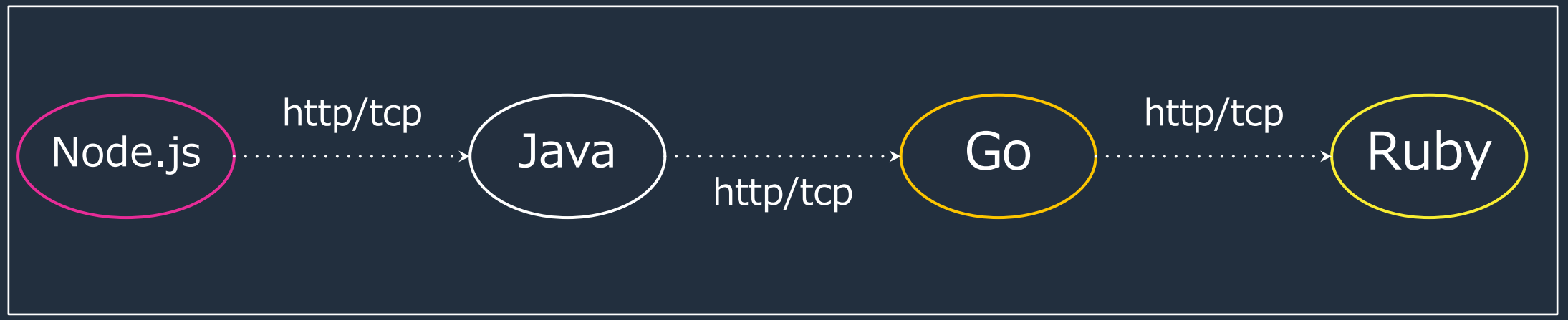
AWS App Mesh とは

Envoy を管理するコントロールプレーンを提供するサービスメッシュ



サービスメッシュとは

- アプリケーションレベルの通信制御を、サービスメッシュの基盤で行うので、アプリケーションに組み込む必要がなくなる
  - HTTP 通信のリトライやタイムアウト
  - 通信のトレーシングやログ、メトリクスの取得
  - TLS を使用した暗号化通信



サービスメッシュが求められるようになった背景

分散システムにおける様々なユースケース解決のため

- 動的サービス構成法の普及（A／Bテスト、カナリアリリース、サービスディスカバリ）
- アーキテクチャ、言語の多様化
- さらにクラウドによる動的サービス作成頻度向上
- 可観測性のために、標準化されたモニタリング要求
- サービス間通信の信頼性を積極的に確保する実装の徹底実施
- セキュリティ

aws

このセッションの前に。。

CON265 サービスメッシュ入門で以下を扱っています

- サービスメッシュとは何か

  アプリケーションレベルの通信を、アプリケーション自身が制御するのではなくインフラストラクチャーで制御できるようにする技術
- サービスメッシュが求められるようになった経緯

  分散システムにおける様々なユースケース解決のため
- サービスメッシュ実装

  AWS App Mesh はEnvoy Proxyをデータプレーンとして、コントロールプレーンと可観測性のために CloudWatch や X-Ray との連携を提供

このセッションで扱うこと

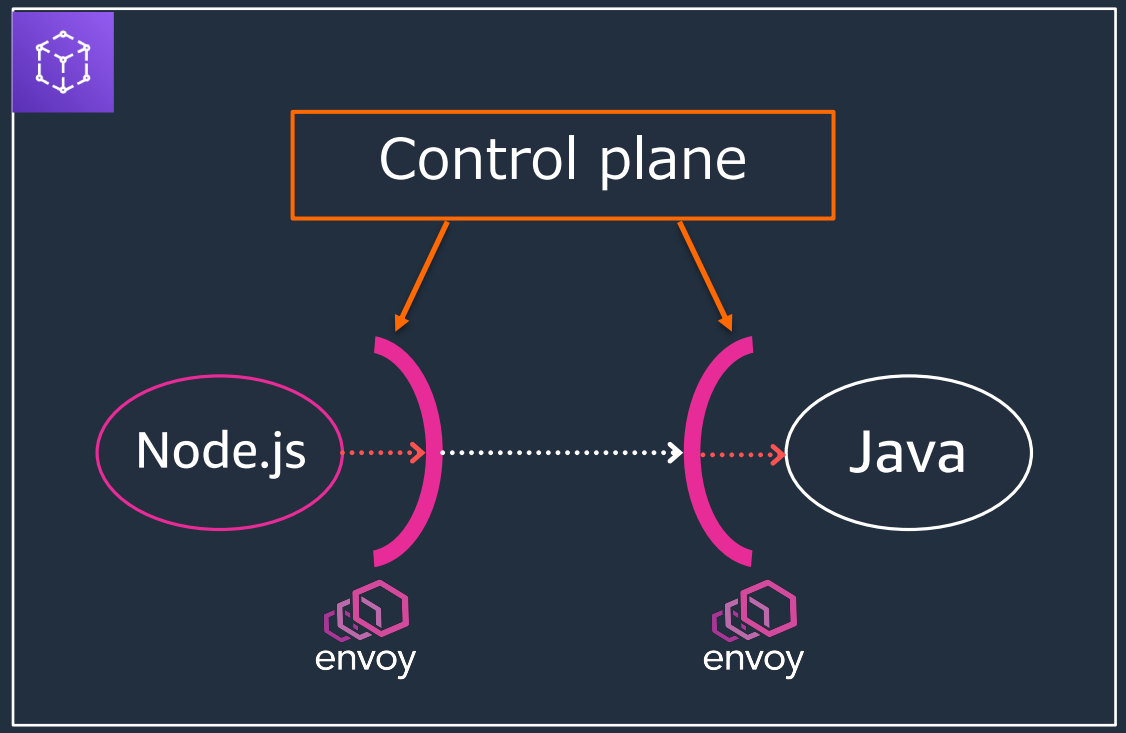
- AWS App Mesh のコア機能
- AWS App Mesh の概念と構成要素
- AWS App Mesh の周辺機能

AWS App Mesh

コア機能

AWS App Mesh

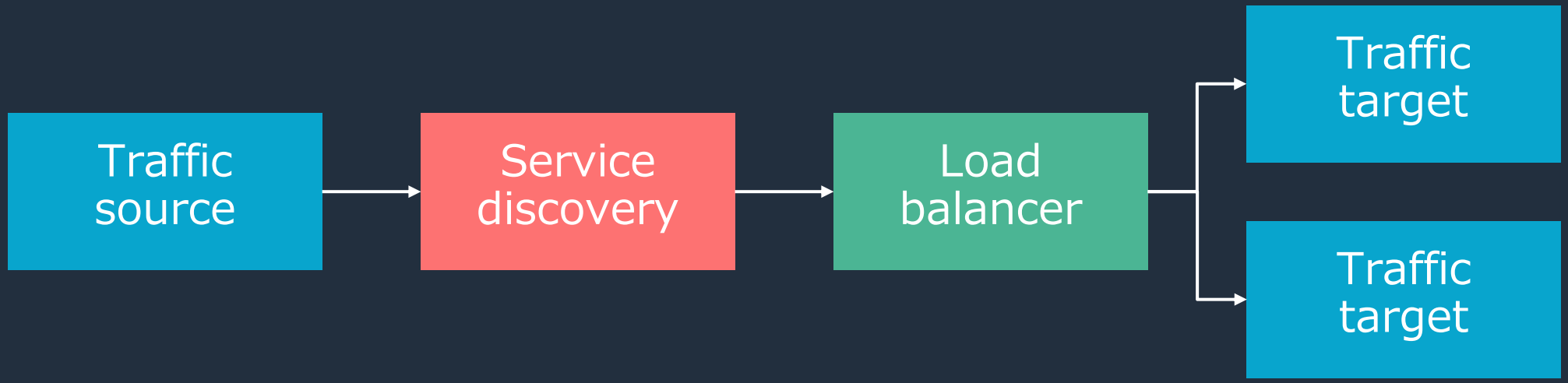
サービスメッシュを管理するコントロールプレーンを提供する



- アプリケーションレベルの通信をネットワークモデルとして定義
- ネットワークモデルを Envoy の設定に変換して配布

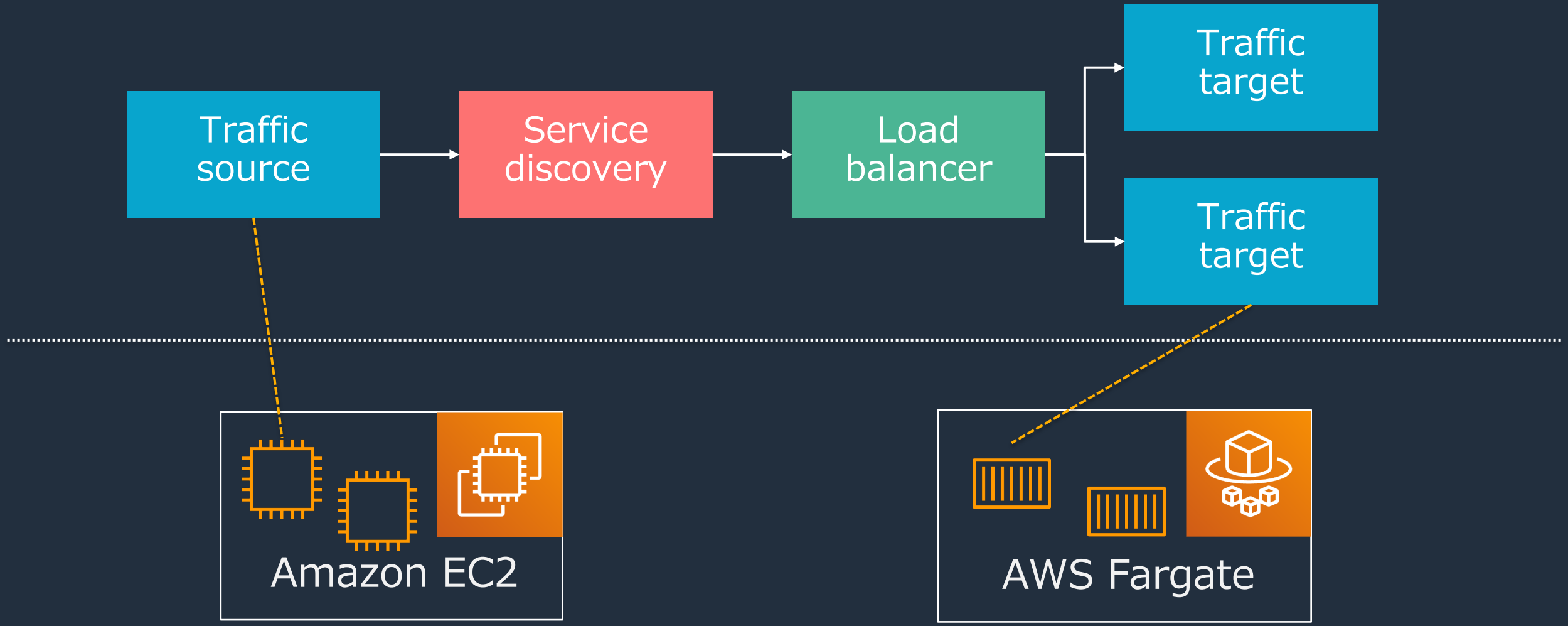
aws

AWS App Mesh のネットワークモデル

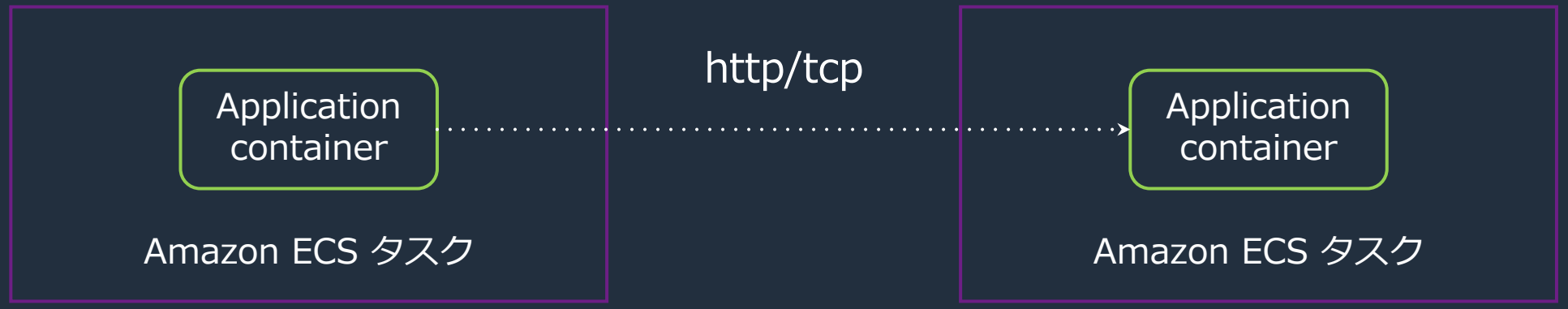


1. 通信元のアプリケーションは、通信先をサービスディスカバリーで発見してリクエストを送信
2. リクエストがロードバランサーに到達
3. ロードバランサーが、複数の通信先にリクエストを振り分け

ネットワークモデルとアプリケーションの関係

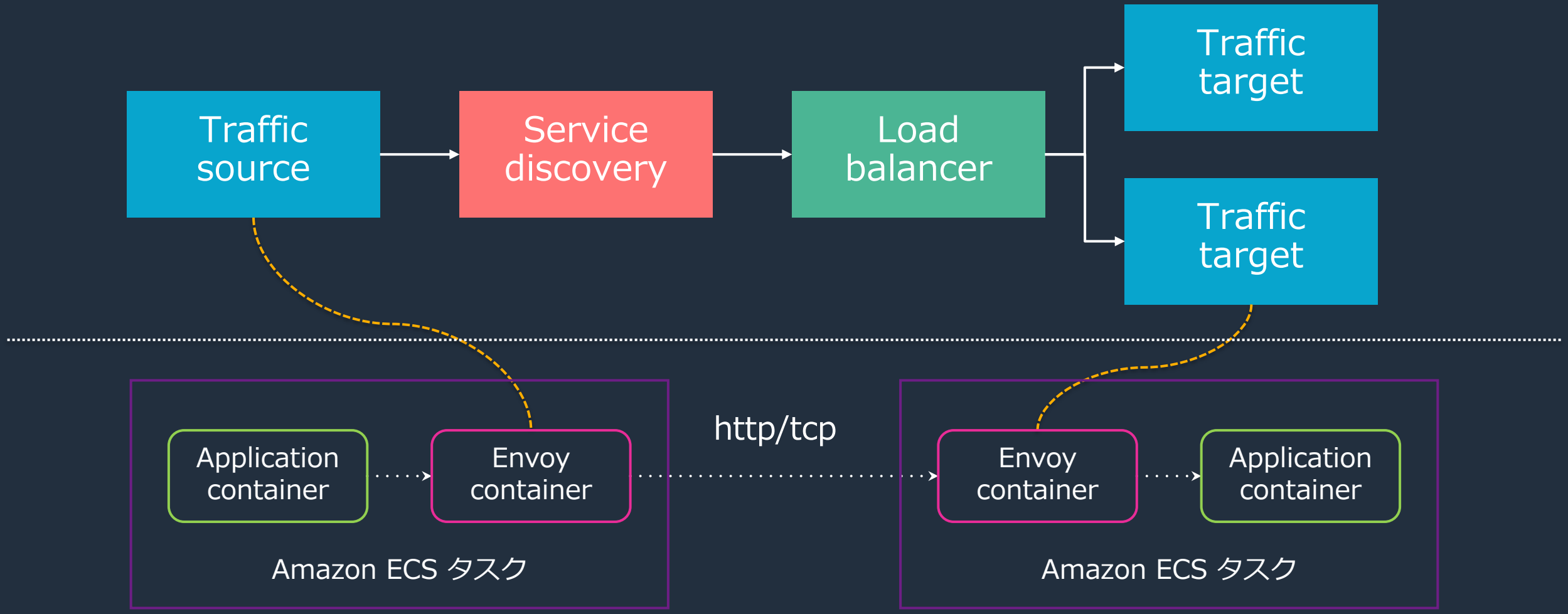


AWS App Mesh の動作イメージ



AWS App Mesh の動作イメージ: Envoy proxy の導入

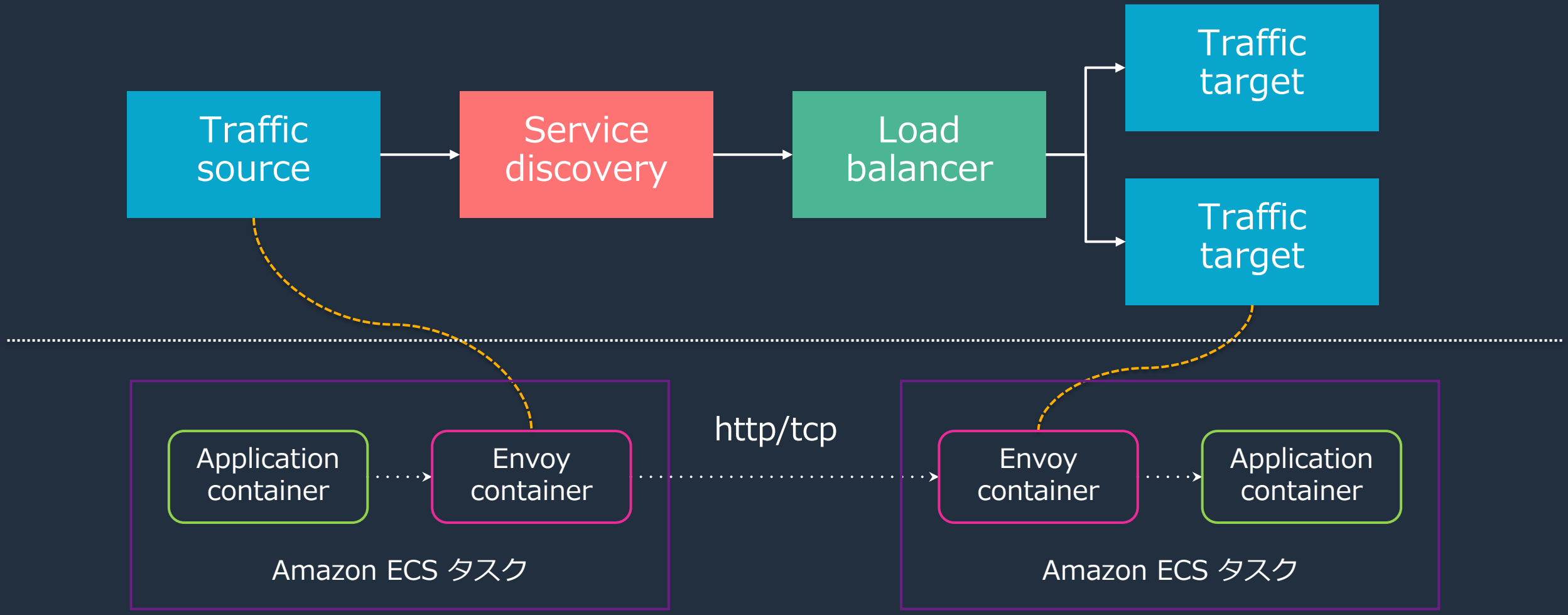
AWS App Mesh の動作イメージ: ネットワークモデルとの関係



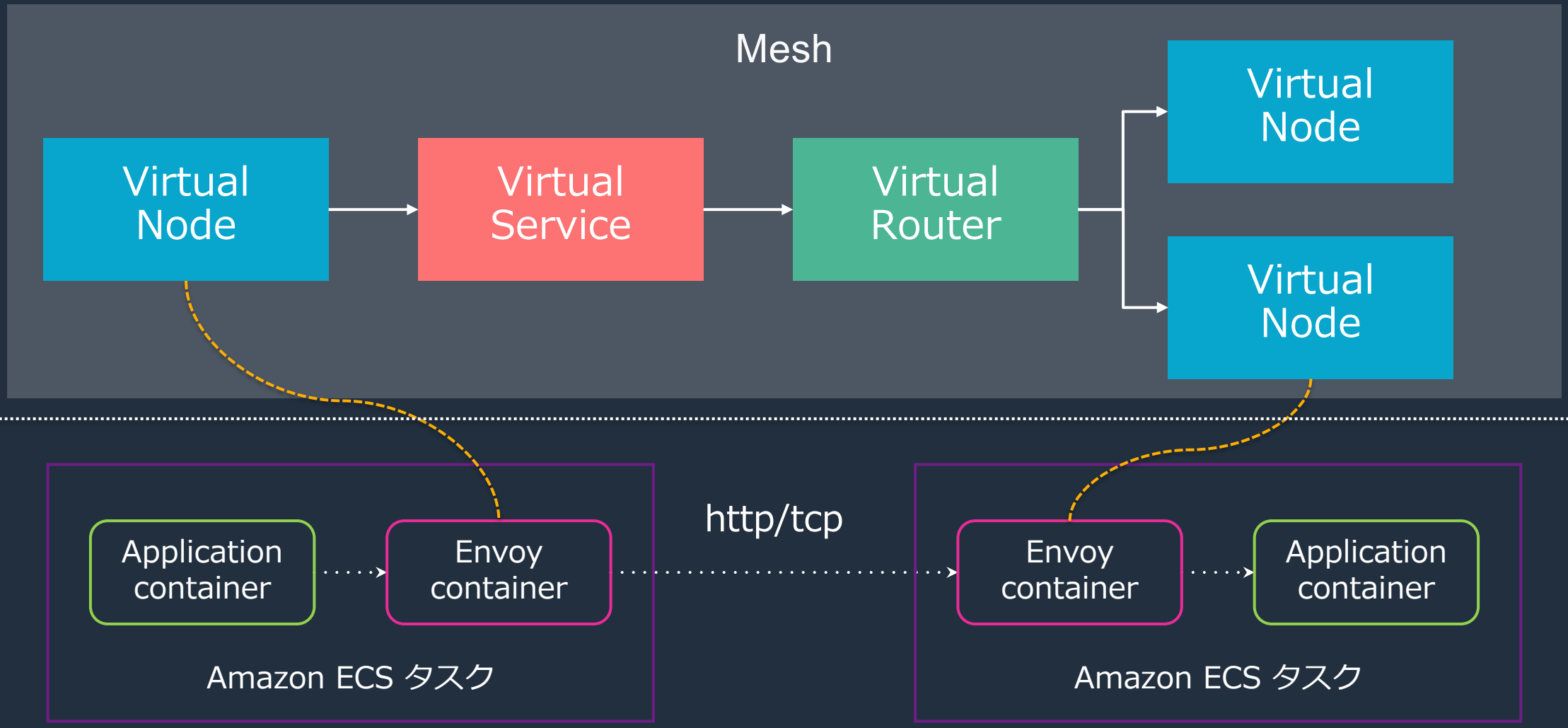
AWS App Mesh

概念と構成要素

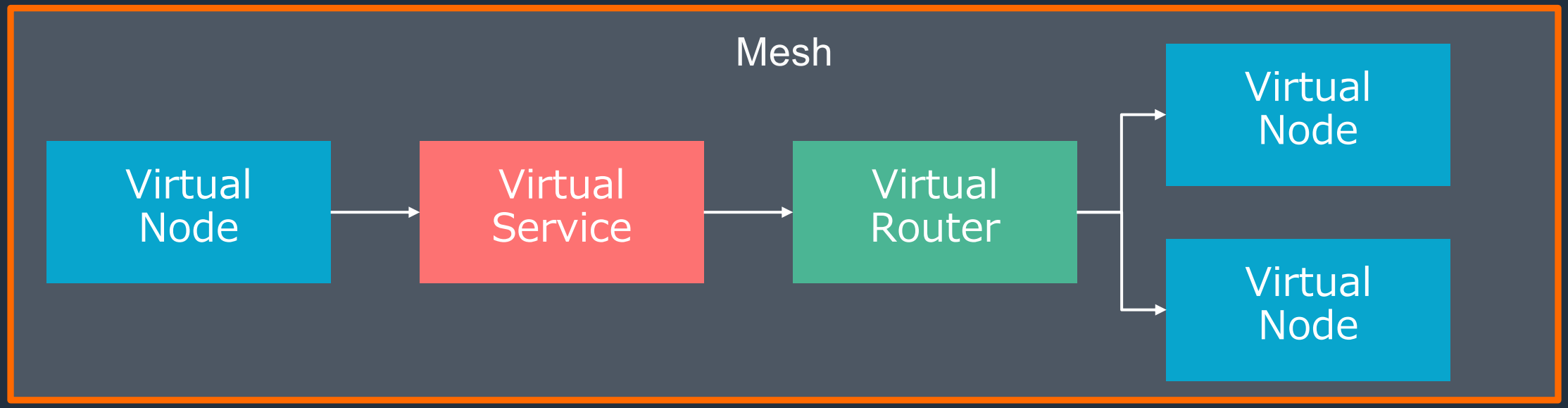
AWS App Mesh の動作イメージ: トップレベルの概念



AWS App Mesh の動作イメージ: トップレベルの概念



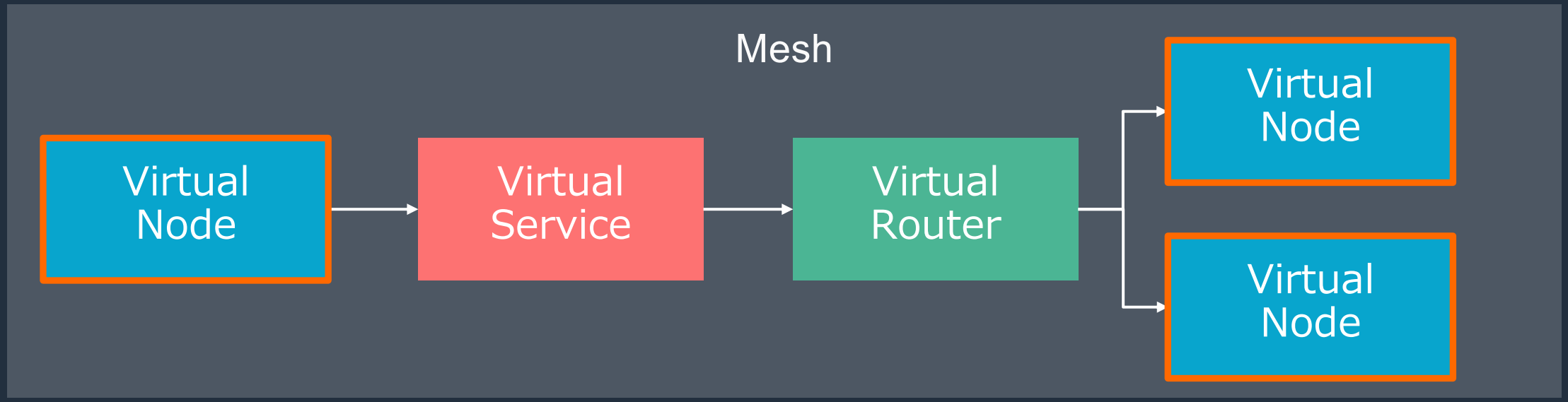
トップレベルの概念: Mesh



- サービス間の通信制御を行う論理的な境界
- Mesh の中に Virtual Node や Virtual Service などを組み合わせて
  ネットワークモデルを構築する

aws

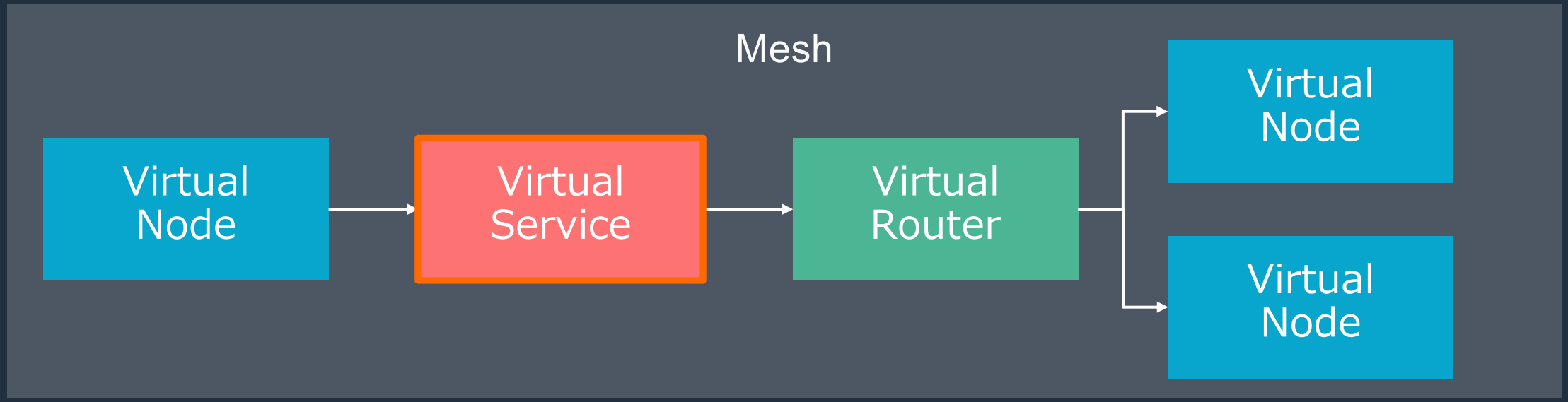
トップレベルの概念: Virtual Node



- 実際のアプリケーションへの論理的なポインタ
  - 例) ECS サービス、Kubernetes デプロイメント
- Envoy の実行時パラメータ (環境変数など) で Virtual Node 名を設定し、アプリケーション (Envoy) と Virtual Node を関連づける

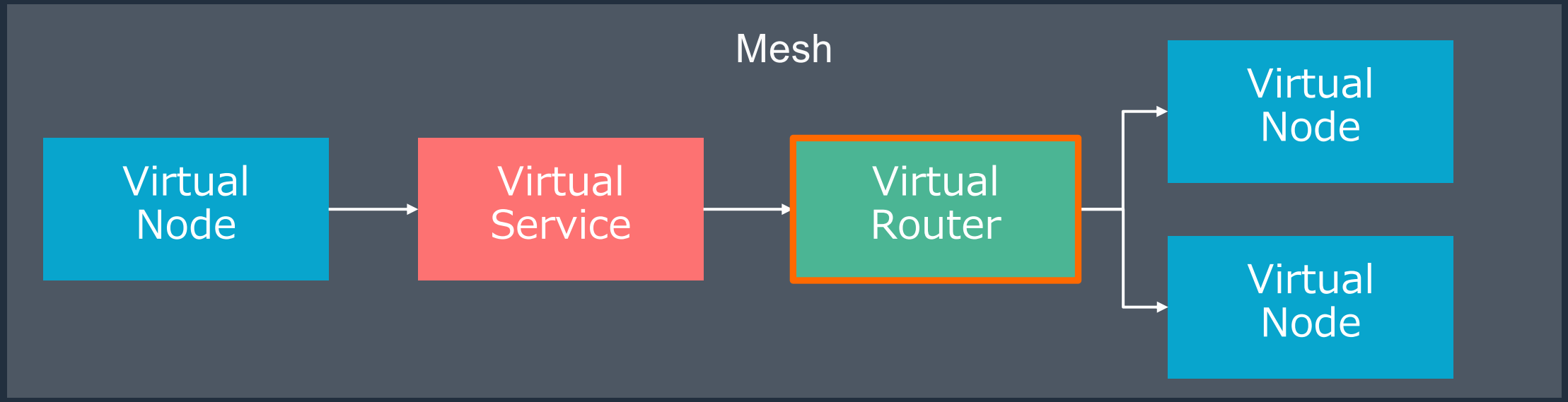
aws

トップレベルの概念: Virtual Service



- アプリケーションの通信先を表す
- リクエストは Virtual Router または Virtual Node にルーティングされ、実際のアプリケーションに到達する

トップレベルの概念: Virtual Router

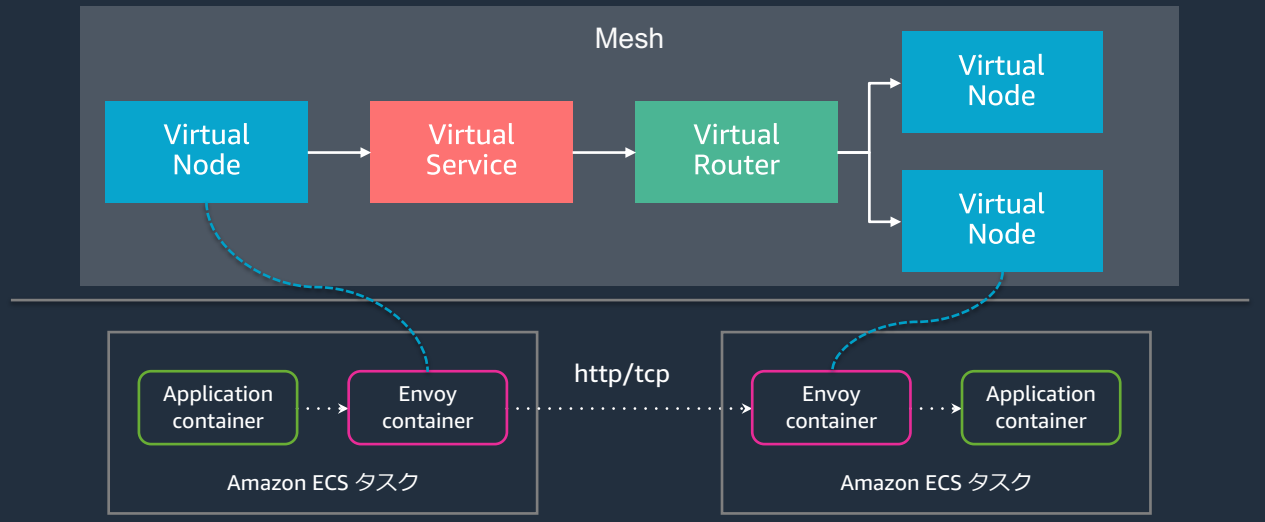


- リクエストのルーティングを管理するロードバランサー
- 単一または複数の Virtual Node にルーティングされる

aws

トップレベルの概念まとめ

- Mesh
  - サービスメッシュの論理的な境界
- Virtual Node
  - アプリケーションのポインタ
- Virtual Service
  - アプリケーションの通信先
- Virtual Router
  - ルーティング管理



AWS App Mesh

周辺機能

App Mesh のカバーする周辺機能

オブザーバビリティ

- Metrics
- Logs
- Traces

セキュリティ

- Network Controls
- Encryption
- Authentication
- Authorization

その他のサポート

- Cross-cluster
- Cross-account
- Multiple compute options

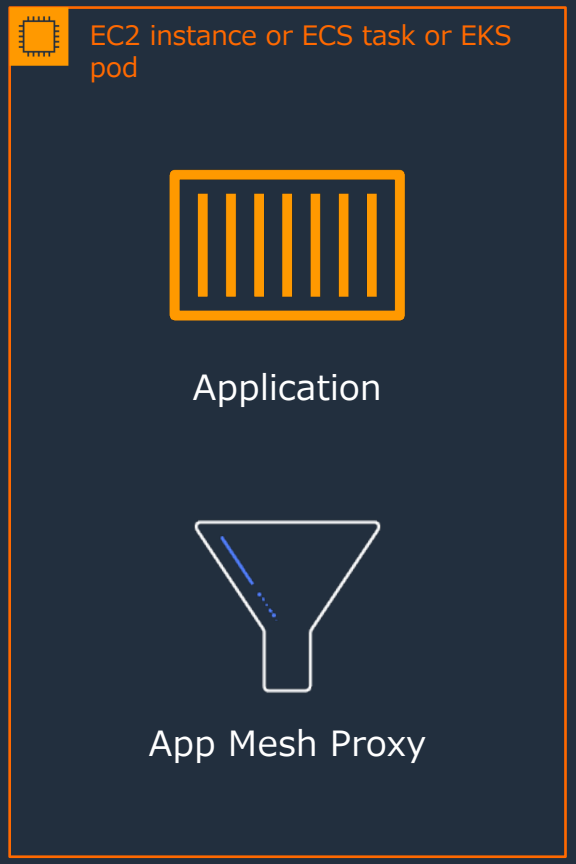
aws

オブザーバビリティ

Metrics

Logs

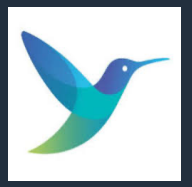
Traces



CloudWatch Metrics

Managed Service for Prometheus

CloudWatch Logs



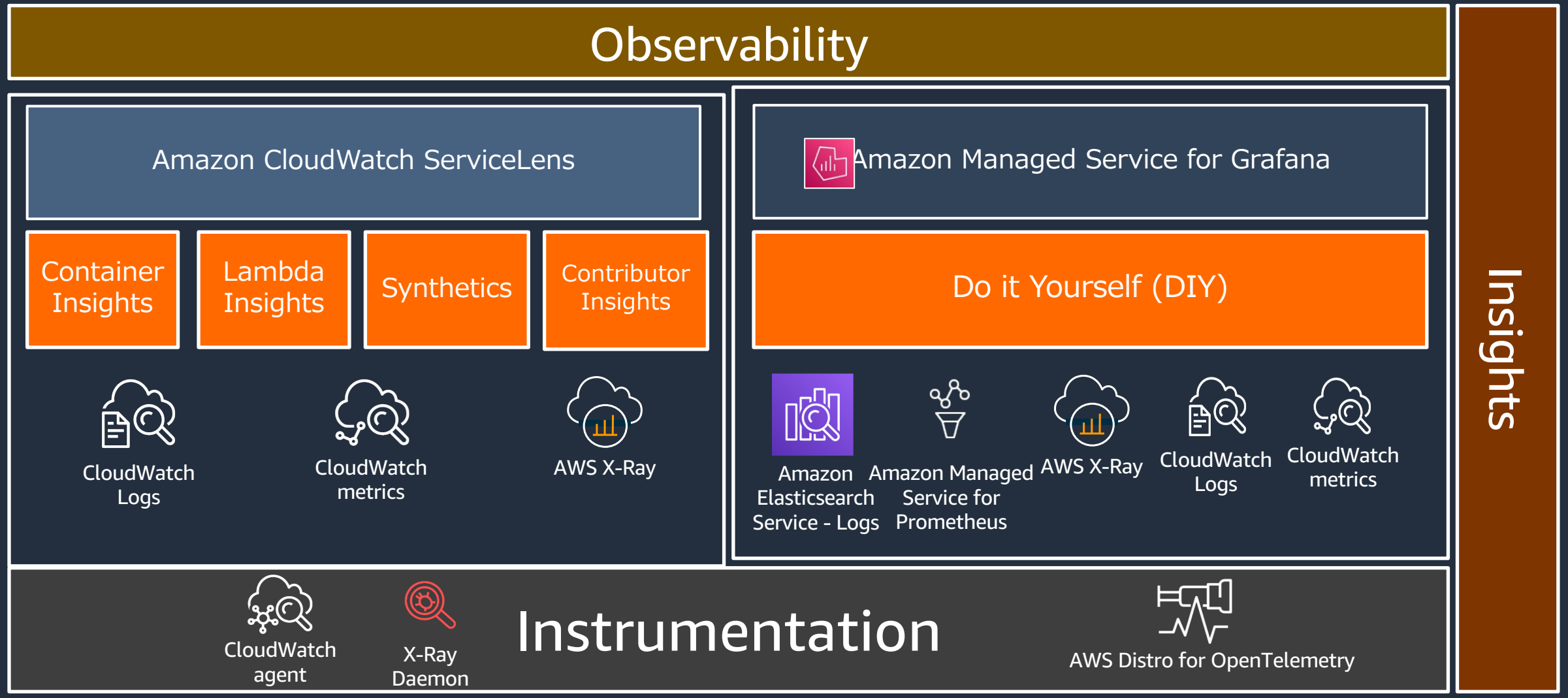
FireLens (Fluent Bit)

AWS X-Ray

OpenTracing

aws

AWSの監視サービス群 全体像

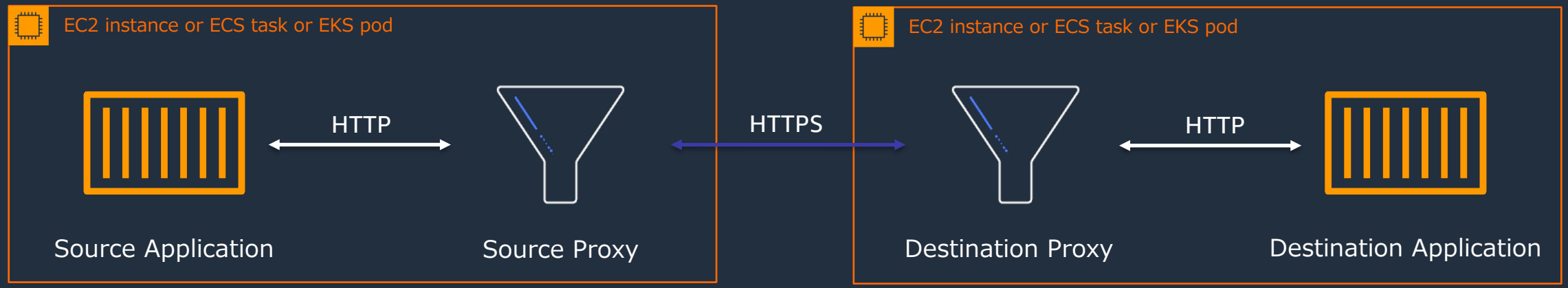


セキュリティ

- サービス間のネットワーク接続を定義
- 透過的な暗号化
- 透過的な認証
- 透過的な認可

SPIFFE/SPIRE

AWS Certificate Manager

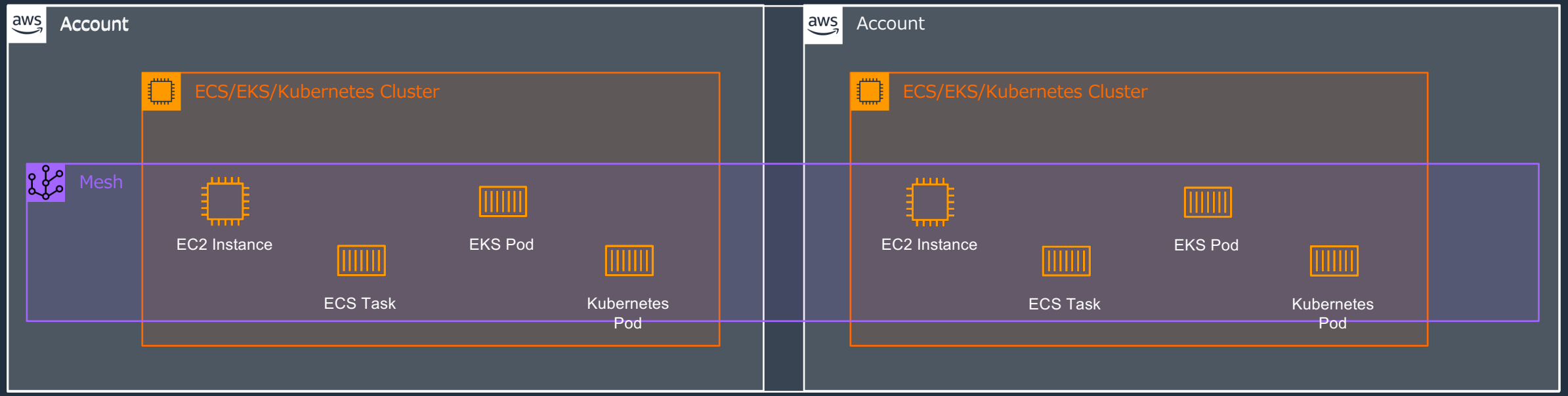


その他のサポート

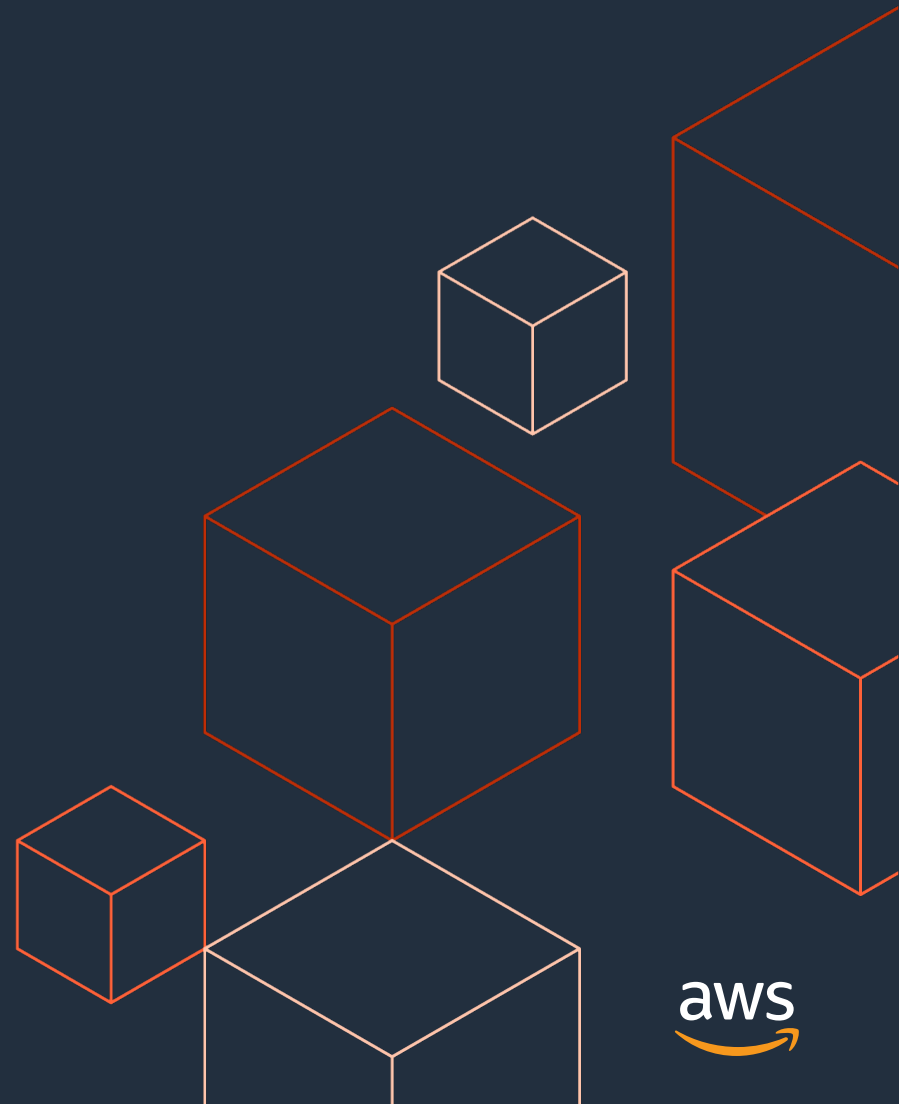
- クロスクラスタ
- クロスアカウント
- 様々な計算オプション

AWS Resource Access Manager

AWS Organizations



まとめにかえて

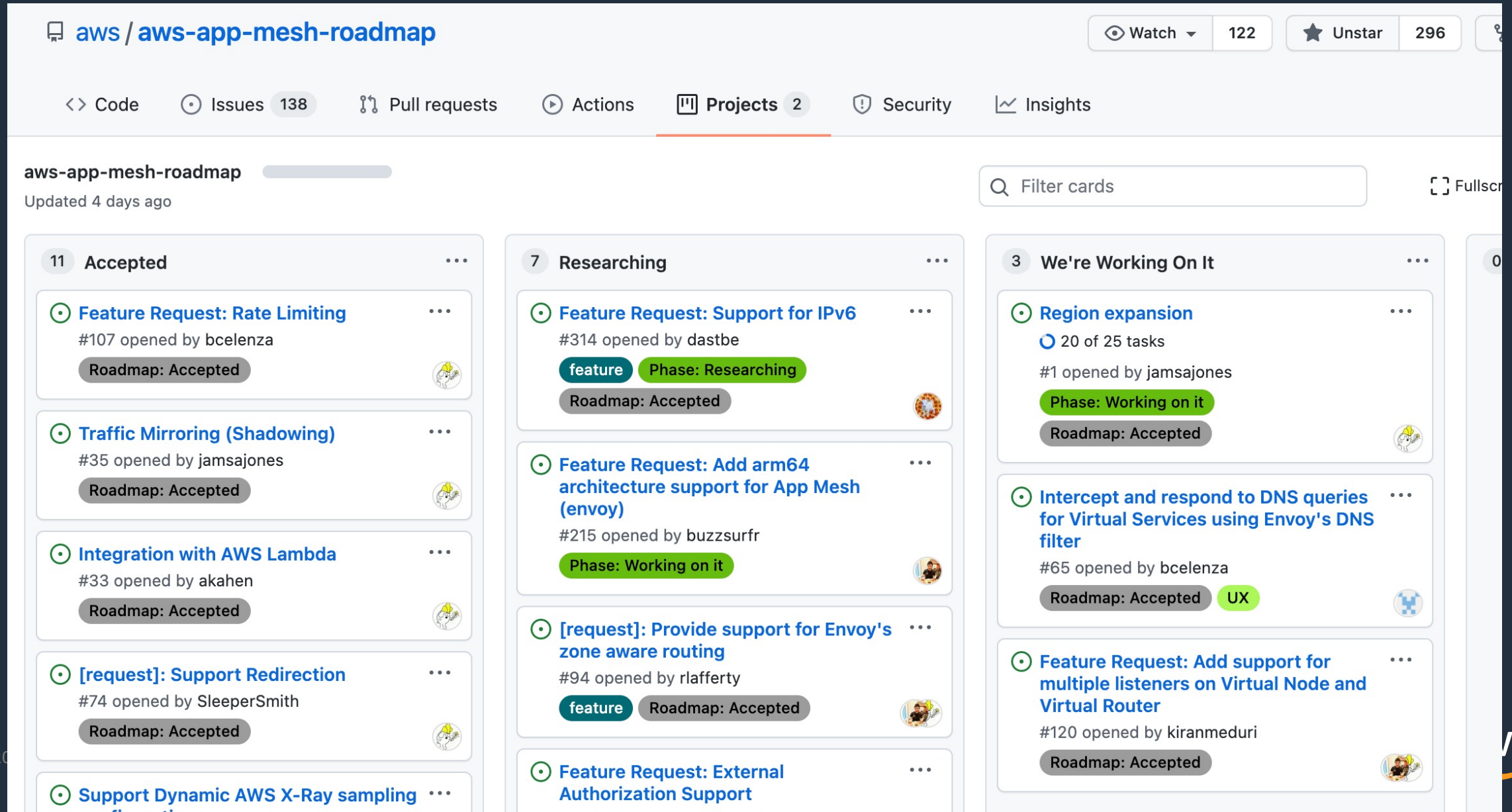


このセッションで扱ったこと

- AWS App Mesh のコア機能
  - アプリケーションレベルの通信をネットワークモデルとして定義
  - ネットワークモデルを Envoy の設定に変換して配布
- AWS App Mesh の概念と構成要素
  - Mesh / Virtual Node / Virtual Service / Virtual Router
- AWS App Mesh の周辺機能
  - オブザーバビリティ
  - セキュリティ
  - その他（クロスアカウント、クロスクラスタ、様々な計算オプション）

App Mesh のロードマップ

https://github.com/aws/aws-app-mesh-roadmap/projects/1

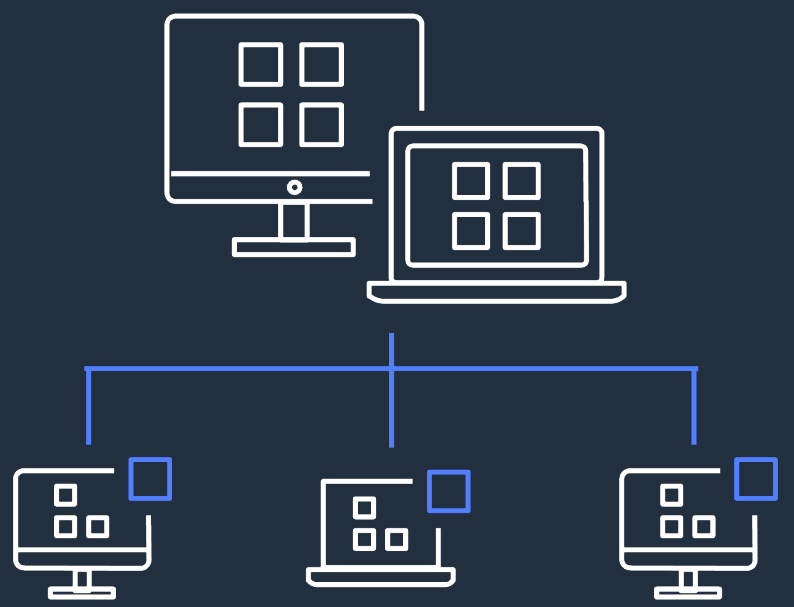


Getting started

クロスアカウント、gRPC、リトライ、Header ベースルーティングなど、活用例を確認可能なコードサンプル
https://github.com/aws/aws-app-mesh-examples

Issues, roadmap, beta channel
https://github.com/aws/aws-app-mesh-roadmap

Amazon EKS 上の AWS App Mesh での SPIFFE/SPIRE による mTLS の使用
https://aws.amazon.com/jp/blogs/news/using-mtls-with-spiffe-spire-in-app-mesh-on-eks/



aws

関連アイテム

- AWS Black Belt Container 2021
  - CON246 Observability – ログ入門
  - CON247 Observability – メトリクス入門
  - CON248 Observability – トレース入門
  - CON265 サービスメッシュ入門