春の Observability 祭り 2025

Amazon CloudWatch を使ってネットワーク監視を行うには

宮崎 友貴
アマゾンウェブサービスジャパン合同会社
ソリューションアーキテクト

自己紹介

宮崎　友貴

アマゾンウェブサービスジャパン
ソリューションアーキテクト

通信業のお客様を中心にご支援しています。

好きな AWS の observability サービス
Amazon CloudWatch Metrics
Amazon Managed Grafana

Agenda

- ネットワークオブザーバビリティとは
- Network Flow Monitor とは
- Network Synthetic Monitor とは
- Internet Monitor とは
- まとめ

ネットワークのオブザーバビリティとは

ネットワークの健全性、パフォーマンスを包括的に把握
迅速な検出と解決を効率的に行えることで障害発生時の影響を最小化

検出する

問題が発生したらすぐに特定して、調査と修正をできるだけ早く開始できます

調査する

障害発生時のテレメトリーを調べて問題の性質を把握します

修復する

問題による顧客への影響を一時的または恒久的に軽減するための対策を講じます

パフォーマンス

RTT (Round Trip Time) やパケットロスなどのパフォーマンス指標を継続的に測定して異常を特定します

位置特定する

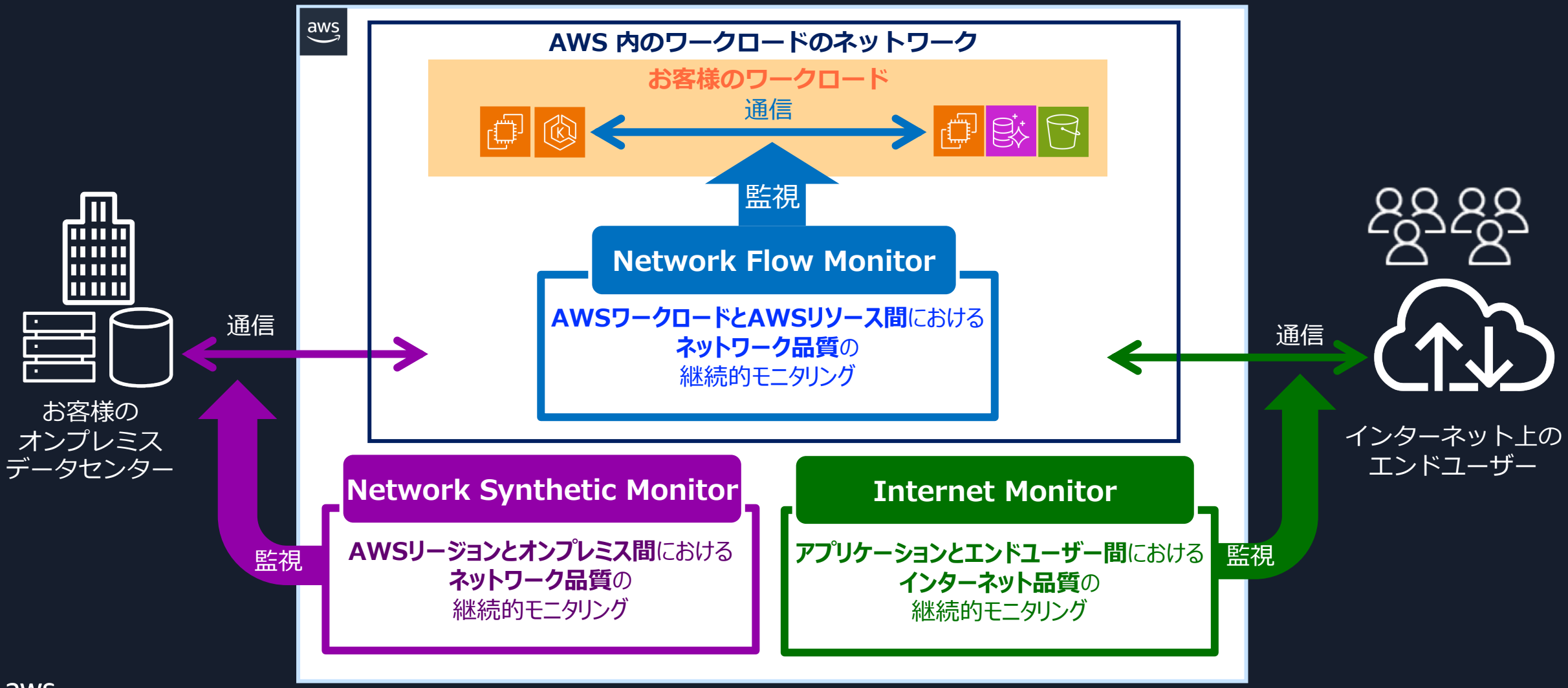
メトリックガイドによるネットワーク障害の故障個所の特定により、トラブルシューティングを迅速化します

経路変更

障害が発生したネットワークセグメントを迂回するよう、アラート生成し、トラフィックをシフトします。

ネットワークパフォーマンス監視を提供する AWS マネージドサービス

それぞれモニタリング対象が異なる 3つ の サービス を提供
目的に応じて 使い分け や 組み合わせ



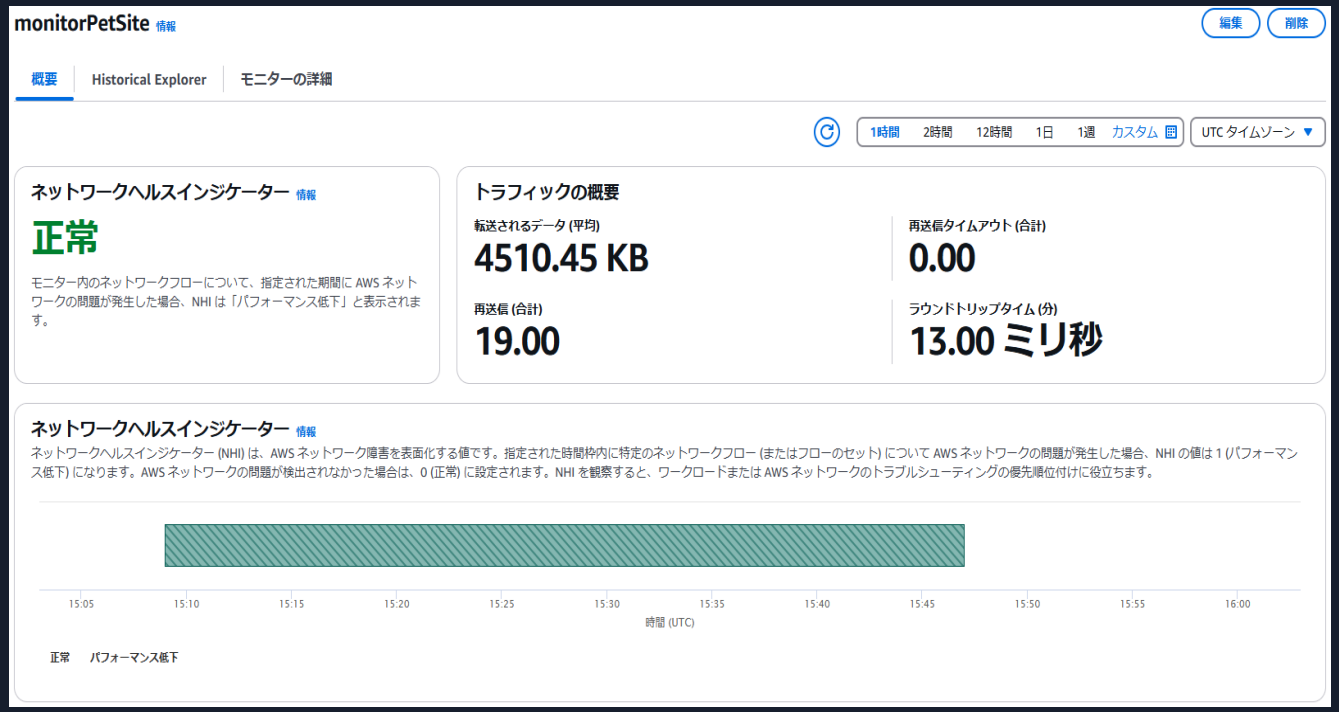
Network Flow Monitorとは

Network Flow Monitor とは

AWSワークロードとAWSリソース間のネットワークを監視するマネージメントサービス

Network Flow Monitor

- Amazon EC2 や Amazon EKS などのコンピューティングインスタンスとAWS サービス間のトラフィックを監視
- エージェントを使用してパケットロス(%)とレイテンシー(ms) などのメトリクスをほぼリアルタイムで可視化
- ネットワークヘルスインジケーター (NHI) によりAWS ネットワークの正常性を確認可能
- AWSサポートにも提供されるため、ネットワークの問題のトラブルシューティングを迅速化

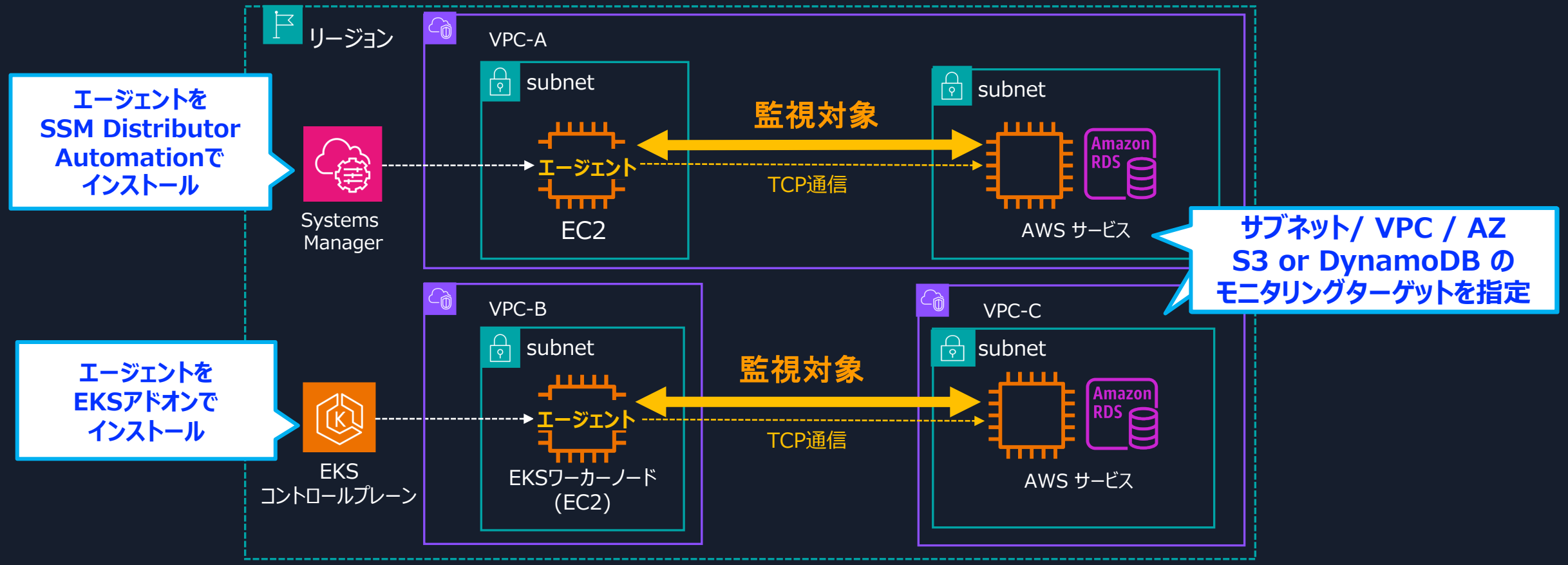


AWS サービス間のネットワークパフォーマンスを監視、可視化

障害時にAWS側かアプリケーション側かの問題の切り分けにより迅速な解決が可能に

Network Flow Monitor のアーキテクチャ

Network Flow Monitor



- エージェントから指定したサブネット/VPC/AZ の範囲内リソースもしくは S3/DynamoDB への TCP 通信を監視
- エージェントは、TCP 接続に関連するイベントを受信し、eBPF を使用してTCP トラフィックを分析
- パフォーマンスメトリクスを Network Flow Monitor サービスのバックエンドに約30秒ごとに送信

※ eBPF は、Linuxカーネル内でトラフィック分析、フロー追跡などを行う機能

Network Flow Monitor の料金

Network Flow Monitor は、以下2つの料金がかかります。

Amazon CloudWatch Network Flow Monitor 料金

①監視リソース(エージェント)

監視リソースあたり
0.0069 USD/時間

※「監視リソース」は
稼働中のエージェント毎に
1つ計上されるリソース

＋

②CloudWatchメトリクス

最初の10,000
メトリクスまで
0.30 USD/metric/月

※1つのモニターは
5つのメトリクス を発行

- DataTransferred
- Retransmissions
- タイムアウト
- RoundTripTime
- ヘルスインジケータ(NHI)

＋

(関連サービス利用料)

Amazon CloudWatch
(アラーム, …)

＋

AWS Lambda

＋

⋮

※2025/4 時点での東京リージョンの場合
https://aws.amazon.com/jp/cloudwatch/pricing/

デモ：Network Flow Monitor を使ってみよう

Network Flow Monitor

マネージドエージェントをインストールするだけで簡単に開始可能

Step1

インスタンスリソース にエージェントをデプロイ

EC2はSSMを、EKSはEKSアドオンを使用して簡単にデプロイ

Step2

ワークロードインサイトを確認

エージェントが自動収集したワークロードのパフォーマンスを確認

Step3

モニターを作成

特定のワークロードのネットワーク品質を継続的にモニタリング

Step4

Historical Explorer から再送信の発生を確認

ネットワークフローのトポロジを表示し、トラブルシューティング

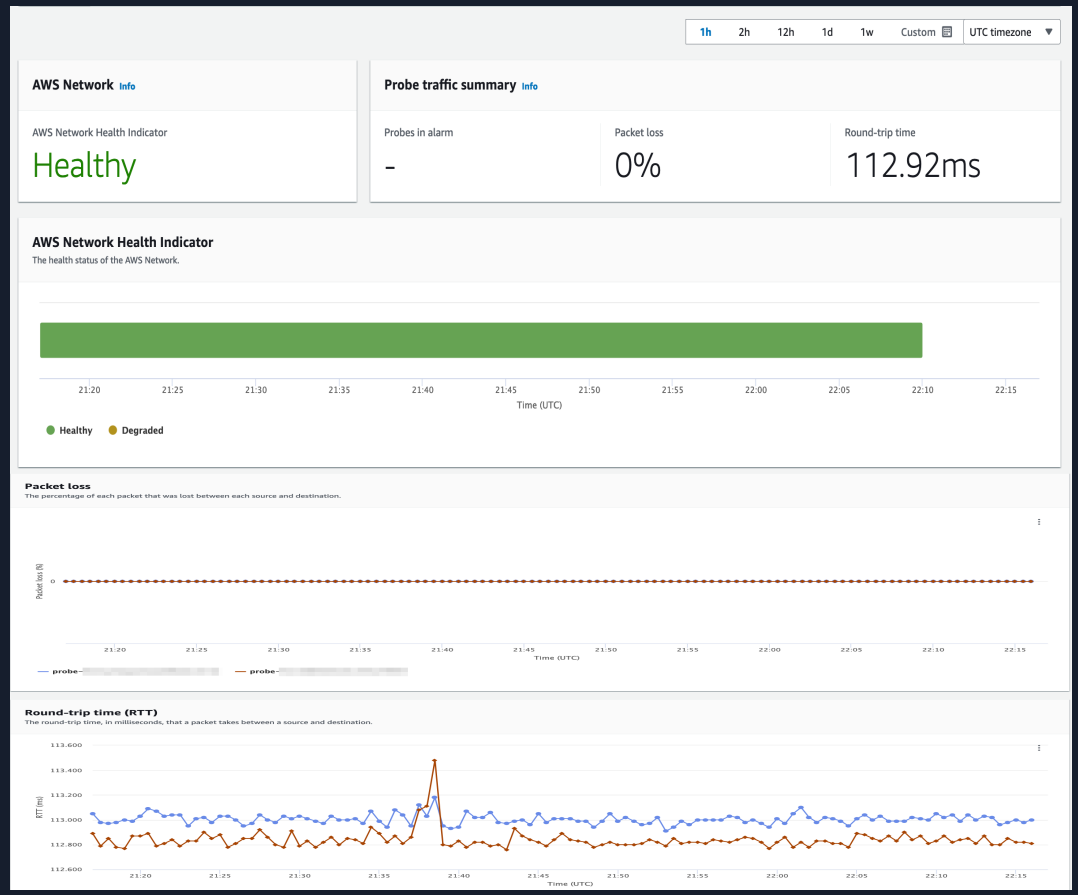
Network Synthetic Monitor とは

Network Synthetic Monitor とは

Network Synthetic Monitor

DirectConnect や VPN 等を経由した AWS とオンプレミス間のネットワーク品質を監視

- パケットロスとレイテンシー(RTT) メトリクスを
  リアルタイムで可視化
- AWS 管理のネットワークの正常性を示す
  AWS Network Health Indicator （NHI）を
  使用して問題を切り分け
- エージェントレスで、VPC のサブネットとエンドポイントを指定
  するだけで開始可能
- サブネットに配置したプローブにより、10 PPS
  (packets per second) でトラフィックが生成
- TCP/ICMPプロトコルをサポート

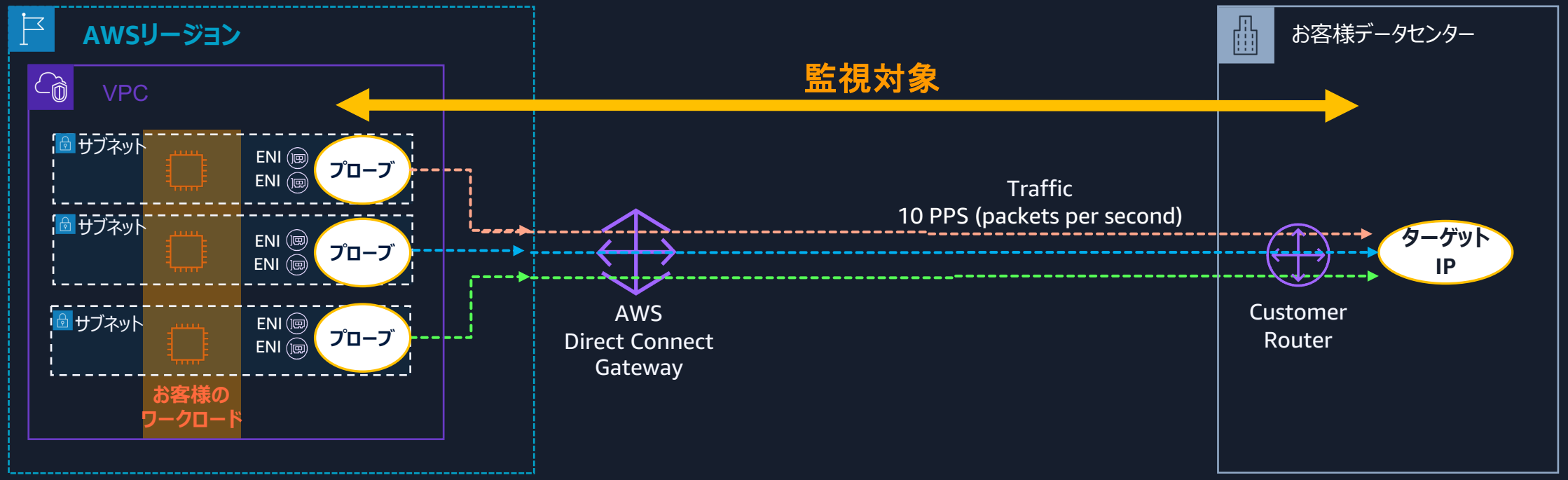


AWS とオンプレミス間のネットワークの状態を監視、通知、可視化

AWS管理のネットワークの問題かどうかの切り分けが可能に

Network Synthetic Monitor のアーキテクチャ

Network Synthetic Monitor



- 送信元サブネット、宛先IP、アドレスファミリ (IPv4/IPv6)、プロトコル (ICMP/TCP)、パケットサイズのすべての組み合わせに対して、**プローブ(AWS ホストリソースからオンプレミスの宛先 IP アドレスに送信されるトラフィック)** を作成
- エンドツーエンドの監視を行うには、ミッションクリティカルなワークロードが設定されている各AZに**プローブ**を配備し、ワークロードの通信先であるオンプレミス内の宛先(IP Address)をターゲットに設定

Network Synthetic Monitor の料金

Network Synthetic Monitor

Network Synthetic Monitor は、以下2つの料金がかかります。

Amazon CloudWatch Network Synthetic Monitor 料金

①監視リソース(プローブ)

4つのプローブあたり
0.11 USD/時間

※「監視リソース」は
稼働中のエージェント毎に
1つ計上されるリソース

＋

②CloudWatchメトリクス

最初の10,000
メトリクスまで
0.30 USD/metric/月

※1つのプローブは
3つのメトリクス を発行

- ラウンドトリップ時間
- パケットロス
- Network Health Indicator (NHI)

＋

(関連サービス利用料)

Amazon CloudWatch
(アラーム, …)

＋

AWS Lambda

＋

⋮

※2025/4 時点での東京リージョンの場合

https://aws.amazon.com/jp/cloudwatch/pricing/

Network Synthetic Monitor を使ってにみよう

Network Synthetic Monitor

ソースとなるAWS側のサブネットとオンプレミス側の宛先IPを指定するだけで簡単に開始可能

Step1

モニターを作成

AWS側のソースとオンプレミス側の宛先を指定し、プローブを作成

Step2

自動生成されたダッシュボードを確認

プローブにより収集されたメトリクスを確認および継続的に監視

Step3

問題のトラブルシューティング

問題の原因のトラブルシューティングに役立てる

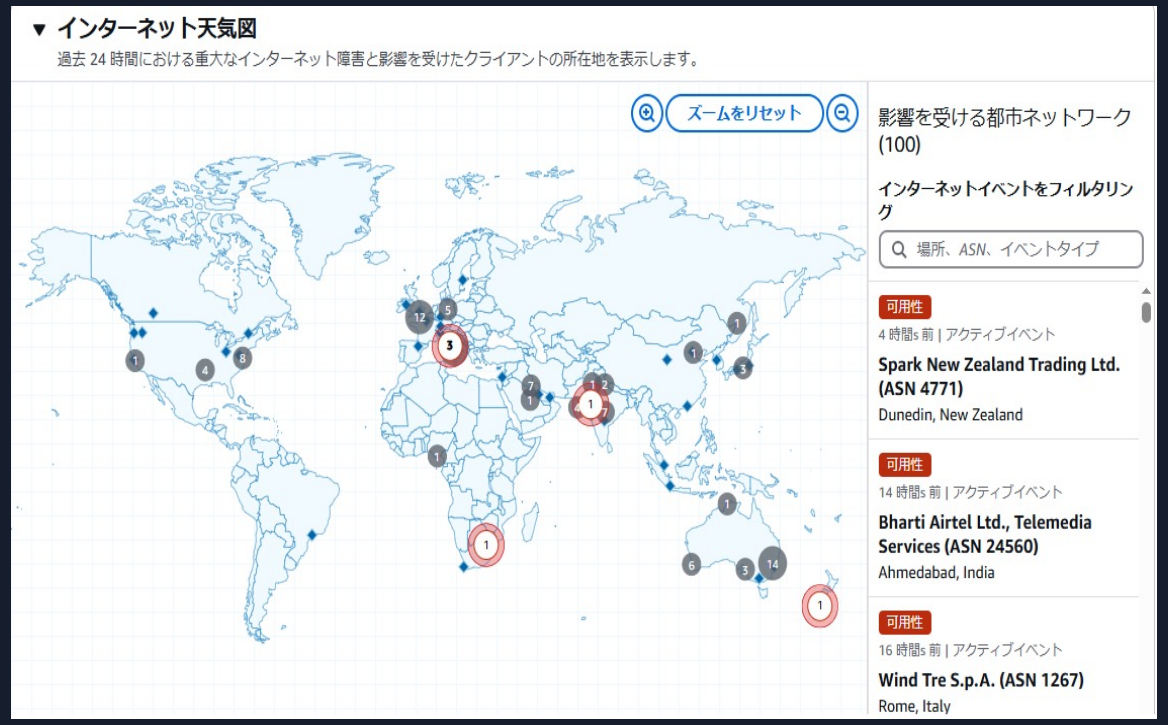
Internet Monitor とは

Internet Monitor

Internet Monitor

アプリケーションとエンドユーザー間のインターネットパフォーマンスを監視するマネージメントサービス

- 継続的にインターネット通信（送受信）時の
  可用性とレイテンシ(RTT) などのメトリクスを収集
- インターネット天気図で過去24時間以内に発生した
  インターネットの問題を世界地図で可視化
- アプリケーションを利用するクライアントの
  インターネットパスを監視し、パフォーマンスを可視化
  監視対象：VPC/Workspaces/CloudFront/NLB
- クライアントやアプリケーションへの影響はなし
- パフォーマンスを最適化する方法を提案
- 測定値は CloudWatch Logs に発行されるので
  詳細の追跡や分析が可能



過去 24 時間に世界中で発生した主要なインターネットイベントの概要

インターネット経由の通信状態を一か所で監視、可視化、通知

問題の原因がインターネット、AWS ネットワーク、またはエンドユーザーアプリケーションか、切り分け可能

Internet Monitor を使ってみよう

Internet Monitor

監視対象とするリソースを指定するだけで簡単に開始可能

Step0

インターネット天気図を確認

インターネットの可用性とパフォーマンス問題を確認

Step1

モニターを作成

監視対象となるリリースを指定

Step2

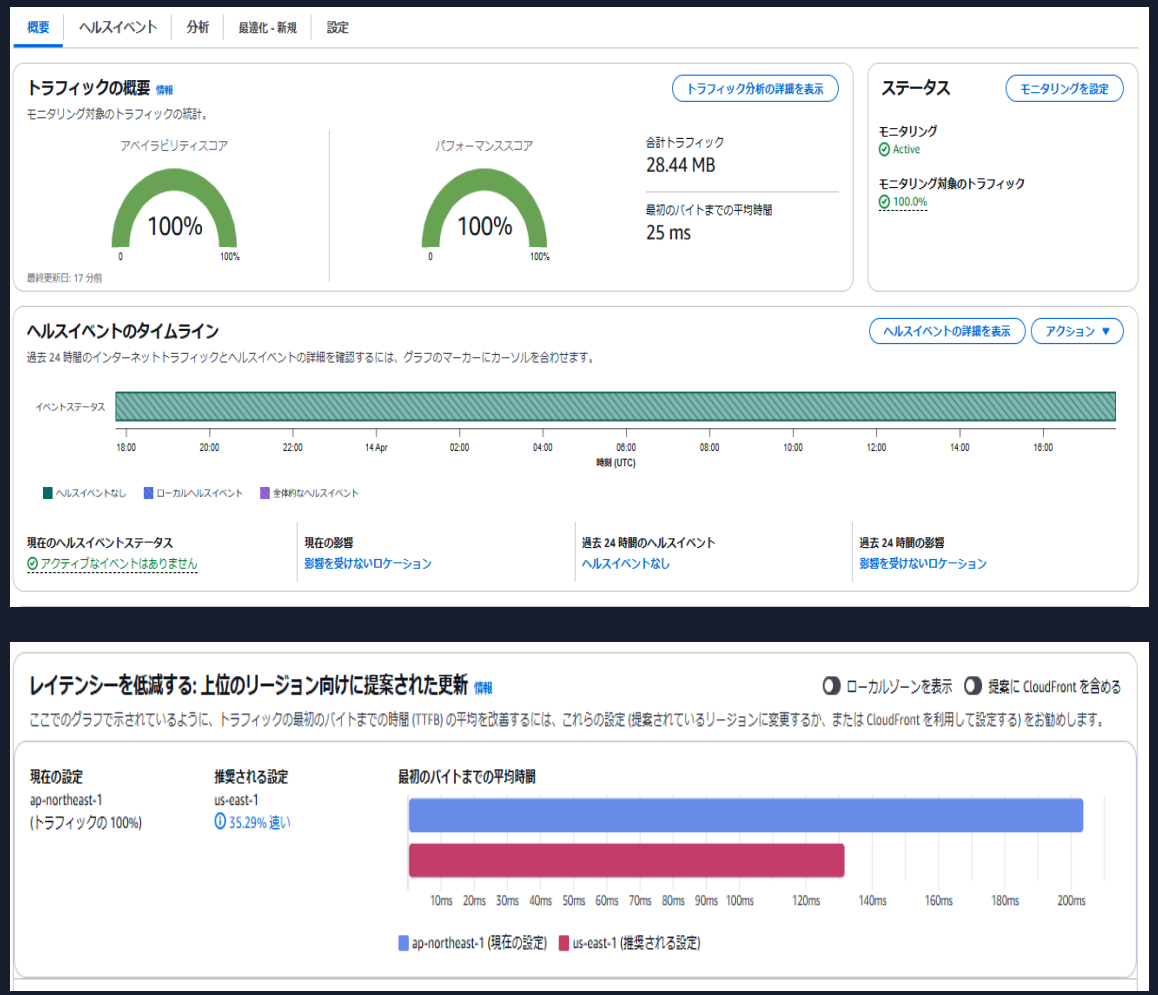
ダッシュボードを確認

インターネットトラフィックの分析結果を確認

Step3

レイテンシーを改善するための提案を取得

クライアントが最適なパフォーマンスを得ることのできる提案を確認



Internet Monitor の料金

Internet Monitor は、以下3つの料金がかかります。

Internet Monitor

Amazon CloudWatch Internet Monitor 料金

①モニタリング対象リソース

監視対象リソースあたり
0.01 USD/時間

※「監視対象リソース」は
VPC, CloudFrontディストリビューション,
WorkSpaces ディレクトリなどの
モニタリングするアプリケーションリソース

＋

②モニタリング対象都市ネットワーク

10,000 個の
モニタリング対象の
都市ネットワークあたり
0.74 USD/時間

※都市ネットワークとは、
クライアントがアプリケーションにアクセスする都市
およびインターネットサービスプロバイダーなどの
ネットワーク（ASN）のこと

＋

③CloudWatch Logs の料金

収集するデータ量に対して
0.76 USD/GB
クエリされたデータ量に対して
0.0076 USD/GB

※モニターは、トラフィック量上位の
都市ネットワーク (最大 500) の診断ログを
5 分ごとに CloudWatch Logs に生成

※収集はスタンダード料金
アーカイブ保存やLive Tail分析など
使用する場合は別途料金がかかります

※2025/4 時点での東京リージョンの場合

https://aws.amazon.com/jp/cloudwatch/pricing/

まとめ

まとめ - ネットワークモニタリングを提供するAWSサービス

それぞれモニタリング対象が異なる 3つ の サービス を提供
目的に応じて 使い分け や 組み合わせ

ネットワークのモニタリング
マネージドサービス

CloudWatch Network Flow Monitor	CloudWatch Network Synthetic Monitor	CloudWatch Internet Monitor
AWSワークロードとAWSリソース間における **ネットワーク品質**の 継続的モニタリング	**AWSリージョンとオンプレミス間**における **ネットワーク品質**の 継続的モニタリング	**アプリケーションとエンドユーザー間**における **インターネット品質**の 継続的モニタリング