

AWS Builders Online Series

T1-3

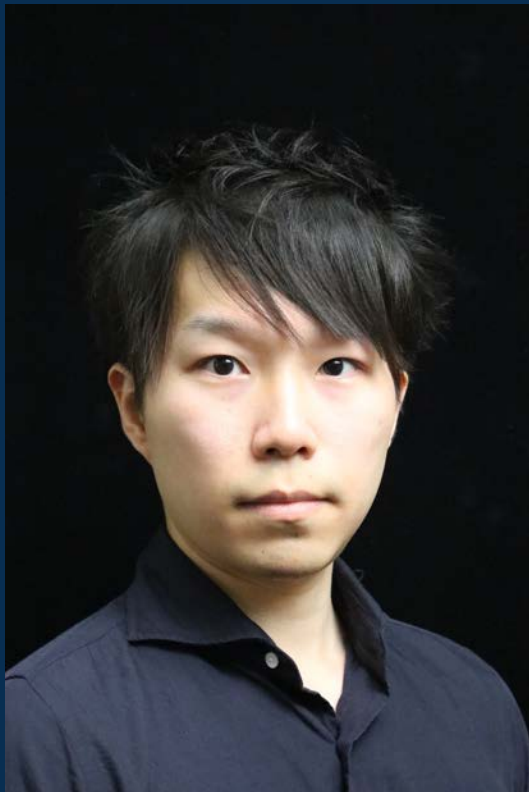
<2024 年版> デモで理解する！ 基本の Web システムアーキテクチャ - 運用編 -

上野 涼平

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



上野 涼平 (うえの りょうへい)

ソリューションアーキテクト

- 業種・業態を問わず、様々なお客様の構成検討を支援
- 前職では、AWS のユーザーの立場として、オンプレミスから AWS への移行、AWS 環境での運用改善に従事

好きな AWS サービス

- AWS Systems Manager

対象者、本セッションで学べること

• 本セッションの対象者

- AWS をこれから触り始めようとする方
- AWS 上のシステムの運用を検討される方
- Amazon EC2 や Amazon RDS を使ったシステムをすでに運用されている方

• 本セッションで学べること

- システムの運用とは？
- AWS サービスを使ったサーバー管理、監視・通知、バックアップ

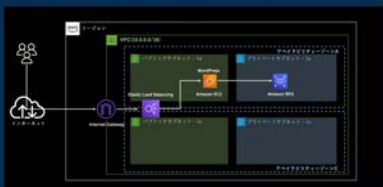
T1 関連セッションについて

本セッションは、基礎編、スケーラビリティ向上編、運用編、セキュリティ編の 4 セッションで構成しています

運用編で例示するアーキテクチャの構築デモは基礎編をご覧ください

本セッションで学べること

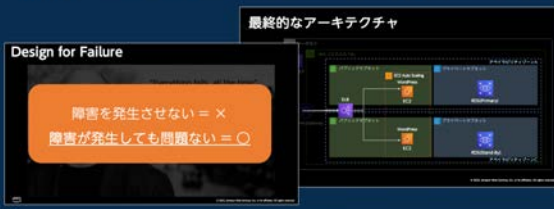
- AWS アカウントと IAM ユーザー作成
- AWS の基本ネットワーク構成とコンポーネントの役割
- 基本の Web システム構築



基礎編

本セッションで学べること

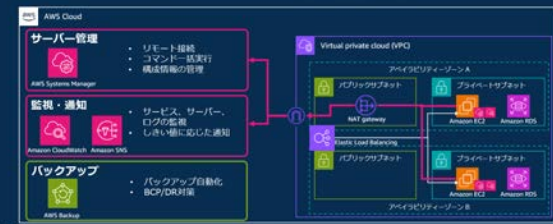
- 可用性とは、スケーラビリティとは？
- AWSサービスを使って、可用性やスケーラビリティを高めるには？



スケーラビリティ向上編

本セッションで学べること

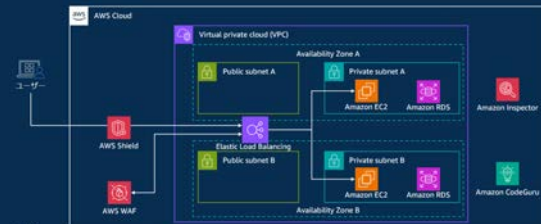
- システムの運用とは？
- AWS サービスを使ったサーバー管理、監視・通知、バックアップ



運用編

本セッションで学べること

- セキュリティ対策の重要性について
- AWS サービスを使った基本的な Web システムのセキュリティ対策



セキュリティ編

アジェンダ

- システム運用とは何か
- AWS サービスを使ったシステム運用
 - サーバー管理（AWS Systems Manager）
 - 監視、通知（Amazon CloudWatch、Amazon SNS）
 - バックアップ（AWS Backup）
- 上記 AWS サービスのデモ
- まとめ



システム運用とは何か



システムは作って終わりではない

システムを動かしていると様々なことが発生する・・・

サービスが利用できない

- ・ サーバーダウン
- ・ サービスダウン
- ・ 通信回線の問題

レスポンスが遅い

- ・ 大量アクセス
- ・ リソース不足

不具合の発生

- ・ ソフトウェアバグ
- ・ パッチが未適用
- ・ 再発防止策が整備できていない

機能追加、改善が進まない

- ・ 継続的なリリース、デプロイの仕組みや体制整っていない
- ・ 運用業務が多くて手が回らない

運用とは ユーザーにサービスを提供し続けるための すべての業務

どのような運用業務が必要になるか？

サービスが利用できない

- ・ サーバーダウン
- ・ サービスダウン
- ・ 通信回線の問題

サーバーに接続して
原因を探ってみよう

設定変更を
しないと

データを復旧
しないと



レスポンスが遅い

- ・ 大量アクセス
- ・ リソース不足

今、サービスは
正常に稼働して
いるのか？

問題があれば
すぐに気付きたい



基本の Web システムを題材にした場合の運用例

サーバー管理

監視・通知

バックアップ

運用例

- サーバーにリモート接続
- サーバーにコマンド実行
- サーバーの構成情報を確認

- サービス、サーバー、ログの監視
- 監視の条件に応じて通知

- データロストに備えたバックアップ取得
- 取得したバックアップの保管、世代管理

課題

- リモート接続用の踏み台サーバー構築、管理業務が発生
- 台数増加による作業負荷増、作業ミスリスク
- 構成管理ドキュメントの更新作業負荷、更新漏れリスク

- 監視、通知の仕組みを用意する必要あり
- 監視、通知用にサーバーを構築した場合、サーバー管理の課題にもつながる

- バックアップジョブの実装やソースコード管理業務が発生
- 定期実行および世代管理の仕組みを用意する必要あり
- バックアップ保管に適した保管場所の用意

AWS サービスを使った システム運用



サーバー管理



AWS クラウド で実行されるアプリケーションとインフラストラクチャの管理に役立つ一連の機能を提供

AWS Systems Manager

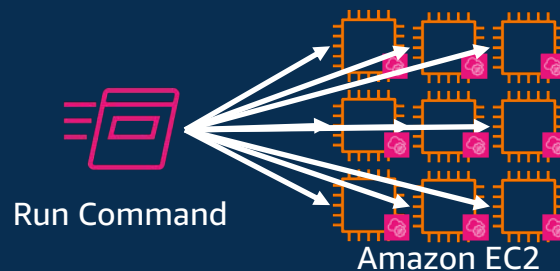
サーバー管理に役立つ Systems Manager の機能

リモート接続 Session Manager



- マネジメントコンソール（ブラウザ）からサーバーにシェルアクセスが可能
- サーバーをプライベートネットワークに配置したまま利用可能
- 踏み台サーバーが不要

コマンド一括実行 Run Command



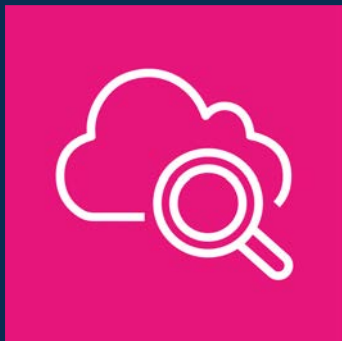
- Bash や Powershell のコマンドを複数のサーバーに対して一括実行可能
- 実行対象はインスタンス、タグ、リソースグループの単位で指定可能

構成情報の管理 Inventory



- サーバーにインストールされている OS、アプリケーション等のインベントリ情報を収集
- 最短 30 分ごとにインベントリデータを定期的に収集し、データを最新状態に保つ

監視と通知



Amazon CloudWatch

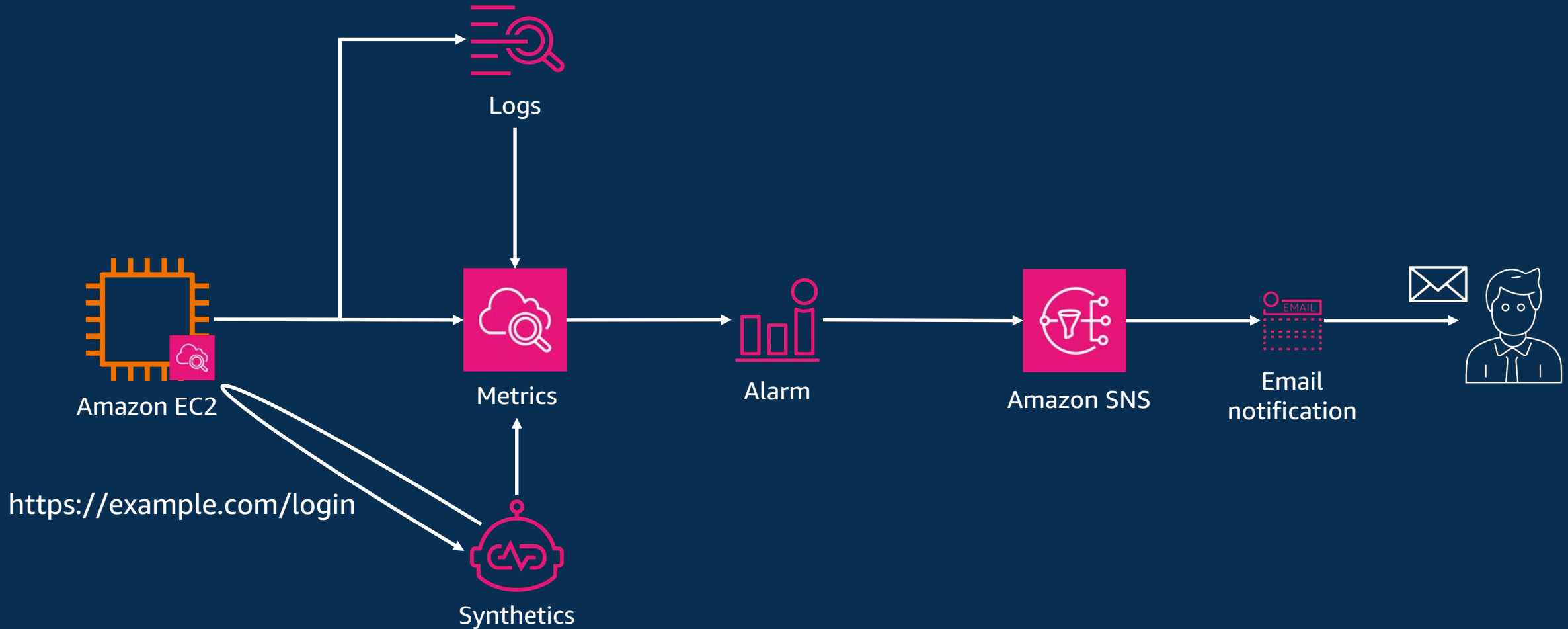
メトリクス(CPU 使用率、ディスク使用率等)、ログ、Synthetics 監視、アラームなどの機能を提供



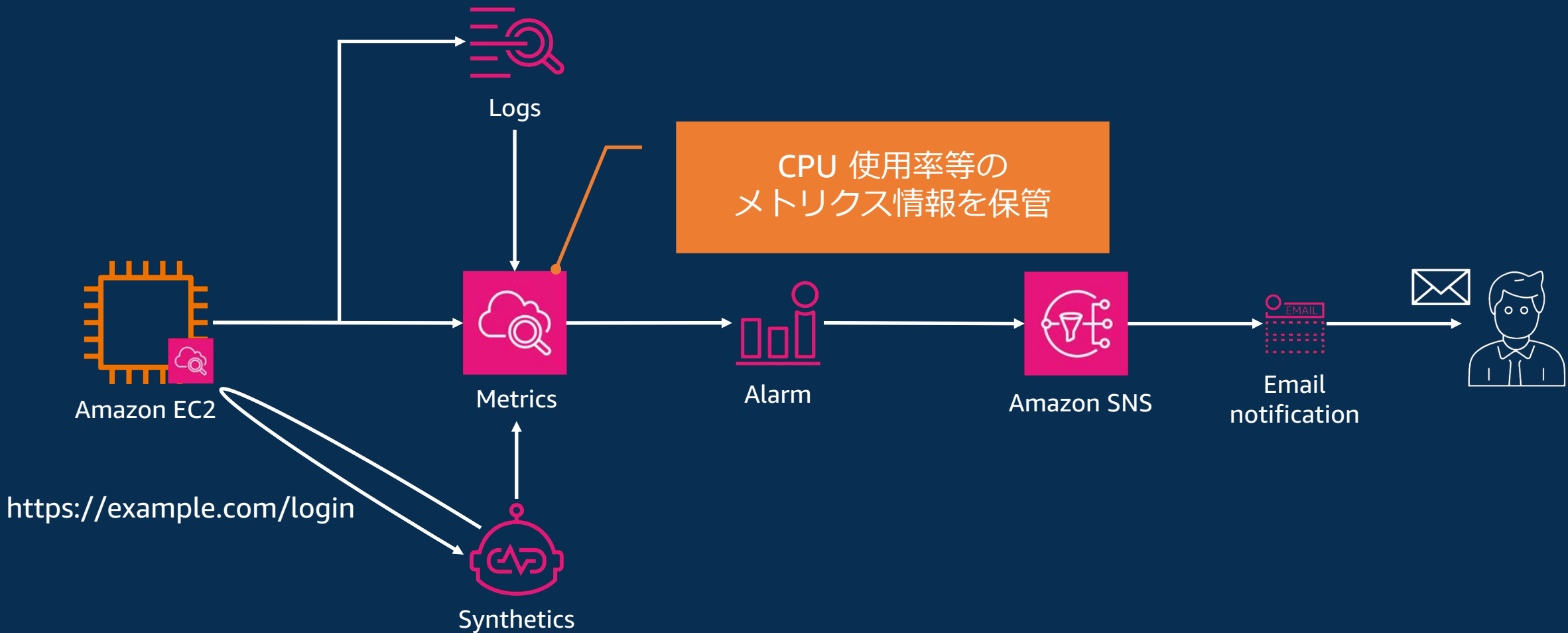
Amazon Simple Notification Service
(Amazon SNS)

HTTP、E メール、モバイルプッシュ通知、モバイルテキストメッセージ (SMS) などのメッセージ配信が可能

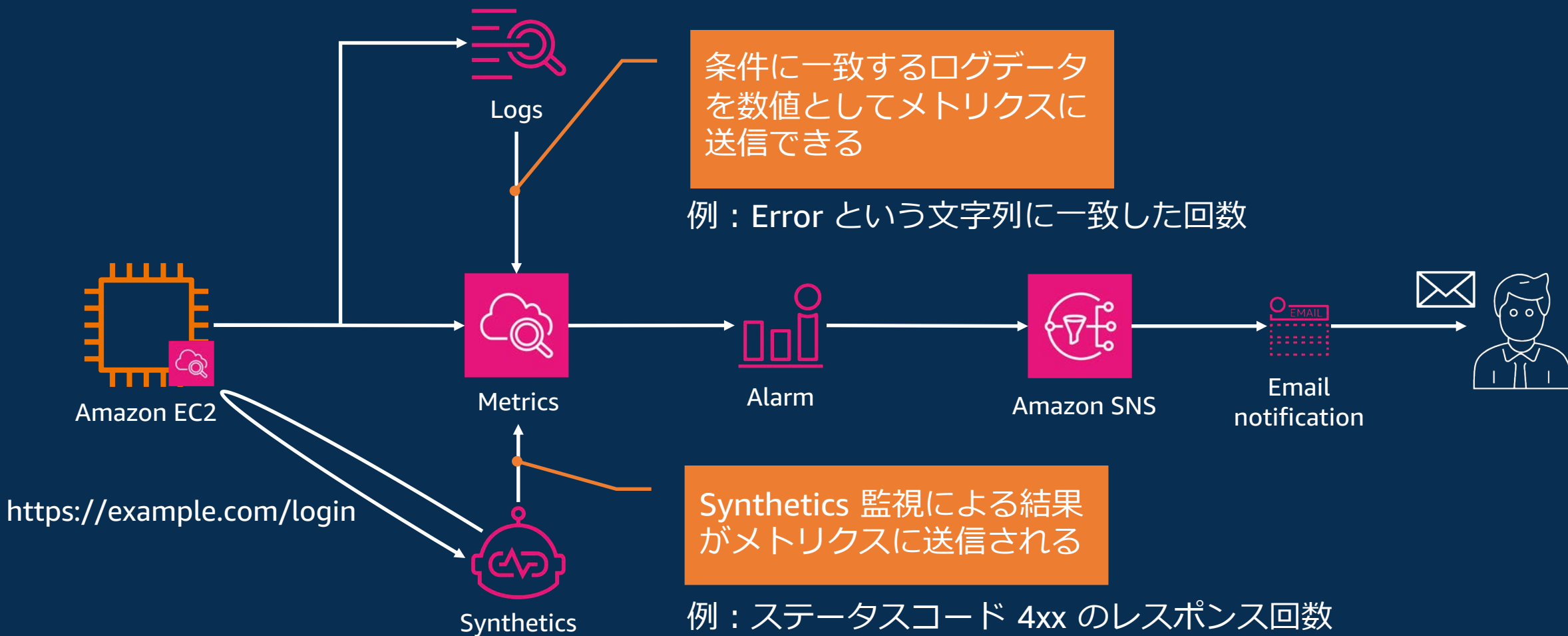
CloudWatch、SNS を使った監視・通知の例



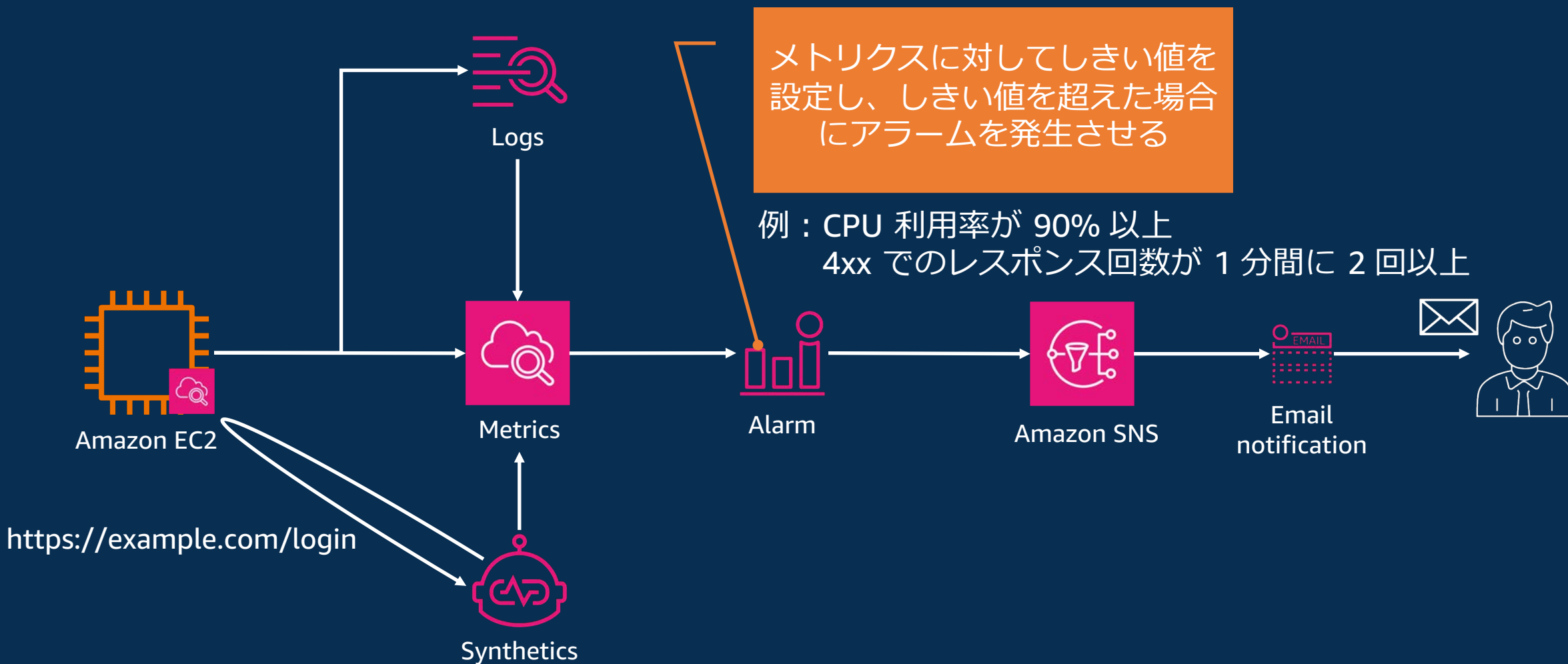
CloudWatch、SNS を使った監視・通知の例



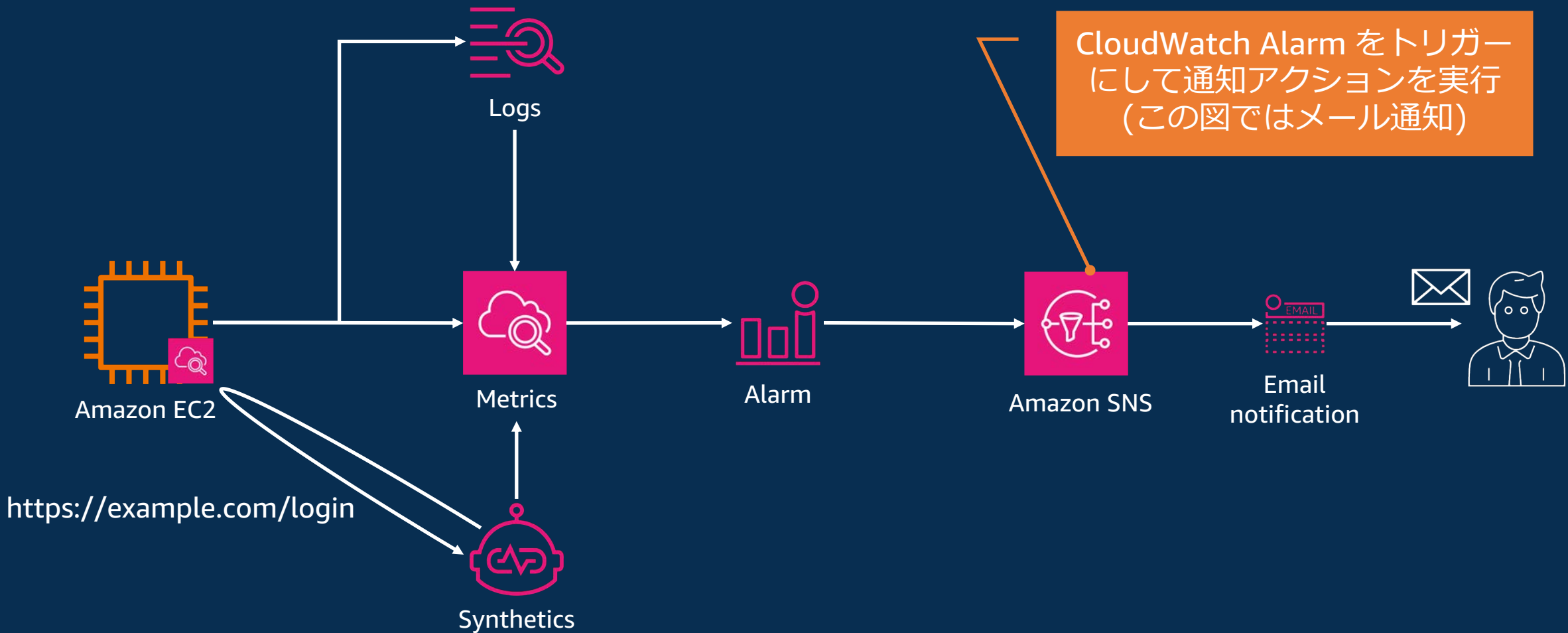
CloudWatch、SNS を使った監視・通知の例



CloudWatch、SNS を使った監視・通知の例



CloudWatch、SNS を使った監視・通知の例



バックアップ

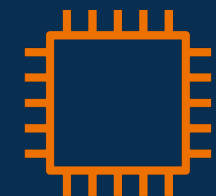


AWS Backup

バックアップスケジュールの自動化やバックアップの保持、
管理を行うフルマネージド型のバックアップサービス

AWS Backup を利用したバックアップ取得

バックアップ取得対象、
取得頻度、保存期間などを
指定



Amazon EC2



Amazon RDS



東京リージョン



AMI



Snapshot

28日間保管



バージニア北部リージョン



AMI



Snapshot

別リージョンに
コピーすることも可能
※対象リソースについてはドキュメントを参照

サポートされているリソース

<https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html#supported-resources>

サーバーまるごとのバックアップではなく
ファイル単位のバックアップはどうするか？

補足：ファイル単位のバックアップ



Amazon Simple Storage Service
(Amazon S3)

- どこからでも簡単に、お好みの量のデータを保存、取得できるオブジェクトストレージサービス
- 99.9999999999% (11 9s) のデータ耐久性

AWS Command Line Interface (AWS CLI)
AWS SDK
Amazon S3 REST API



本セッションにおける全体構成



AWS Cloud

サーバー管理



AWS Systems Manager

- ・ リモート接続
- ・ コマンド一括実行
- ・ 構成情報の管理

監視・通知



Amazon CloudWatch



Amazon SNS

- ・ サービス、サーバー、ログの監視
- ・ しきい値に応じた通知

バックアップ



AWS Backup

- ・ バックアップ自動化
- ・ 別リージョンへのコピー

基礎編 / スケーラビリティ向上編



Virtual private cloud (VPC)

アベイラビリティーゾーン A



パブリックサブネット



プライベートサブネット



NAT gateway



Amazon EC2



Amazon RDS



Elastic Load Balancing



パブリックサブネット



プライベートサブネット



Amazon EC2



Amazon RDS

アベイラビリティーゾーン B



デモ



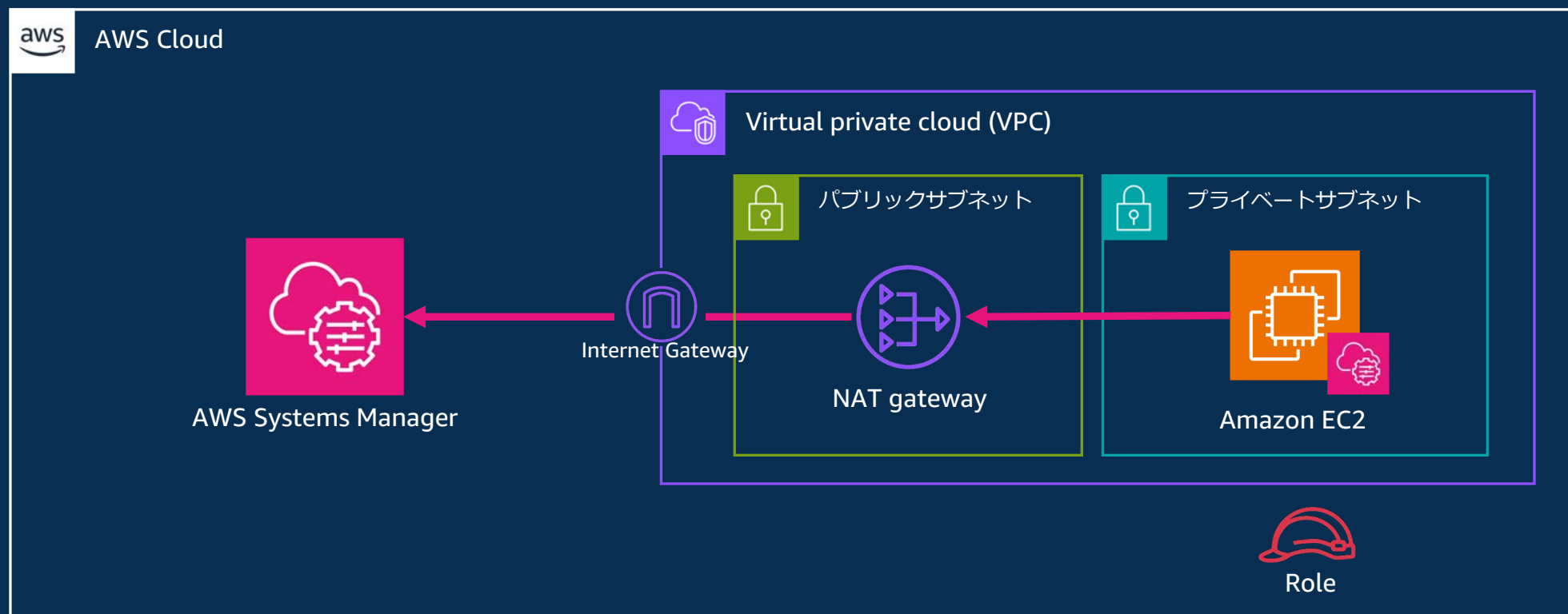
Systems Manager を利用したサーバー管理



サーバーをマネージドノードにする

Systems Manager で管理されている状態のサーバーを**マネージドノード**と呼びます

Systems Manager の一部の機能を利用するためには、サーバーをマネージドノードにする必要があります



サーバーをマネージドノードにする

1 Systems Manager Agent の導入

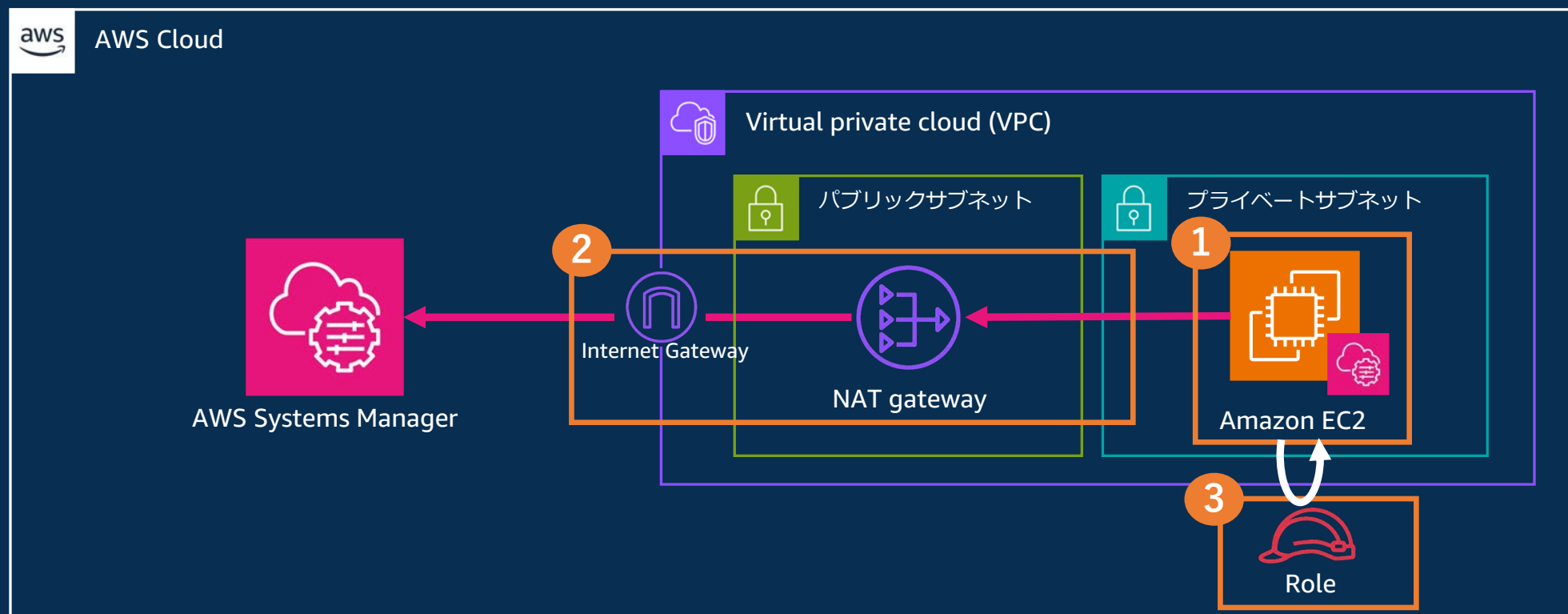
- ✓ 手動インストール
- ✓ プリインストール済みの AMI を利用する (Amazon Linux 2023 など)

2 アウトバウンド経路の確保

- ✓ Internet Gateway 経由
- ✓ VPC エンドポイント経由

3 必要な権限を付与

- ✓ IAM ロールのアタッチ
- ✓ デフォルトのホスト管理設定を行う



サーバーをマネージドノードにする

1 Systems Manager Agent の導入

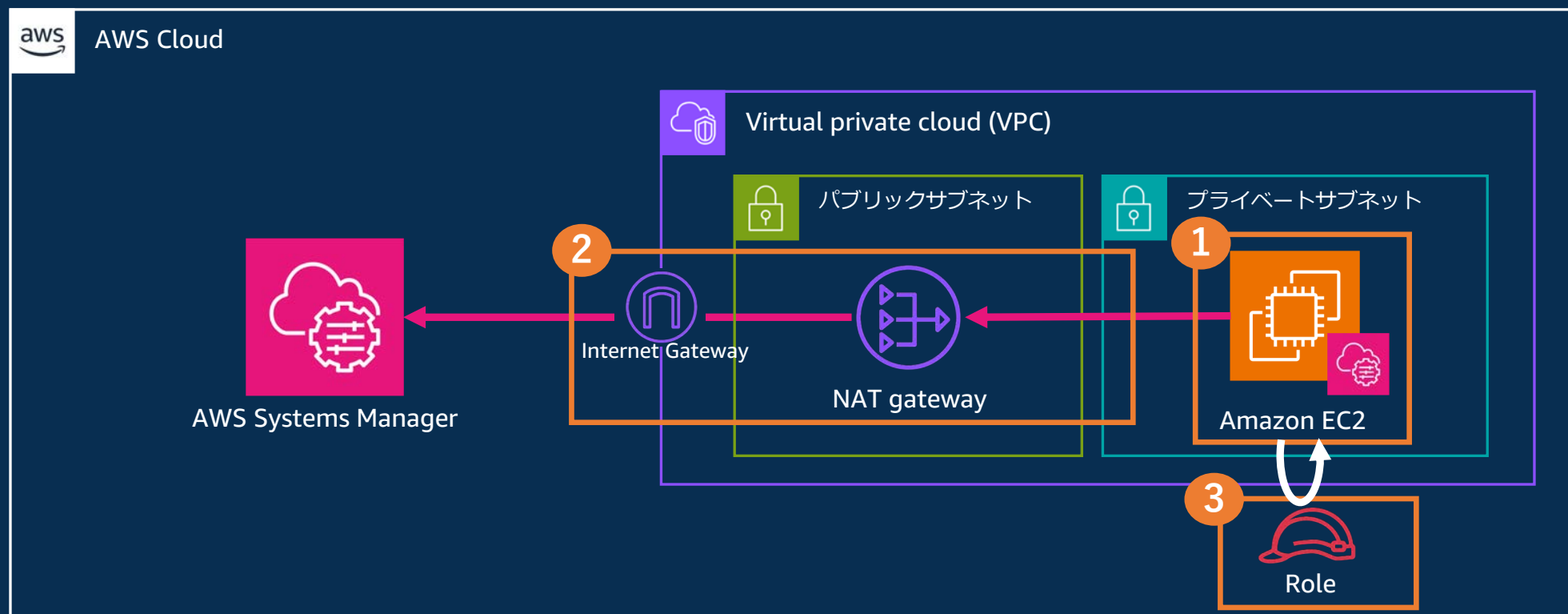
- ✓ 手動インストール
- ✓ プリインストール済みの AMI を利用する (Amazon Linux 2023 など)

2 アウトバウンド経路の確保

- ✓ Internet Gateway 経由
- ✓ VPC エンドポイント経由

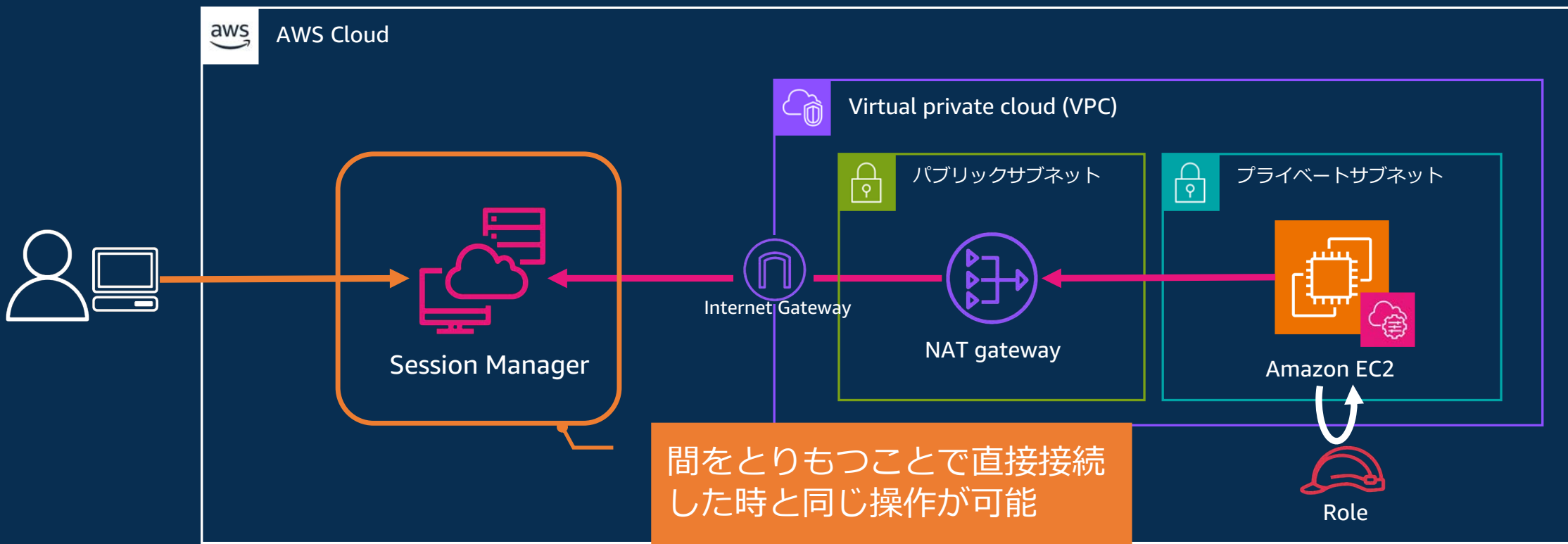
3 必要な権限を付与

- ✓ IAM ロールのアタッチ
- ✓ デフォルトのホスト管理設定を行う

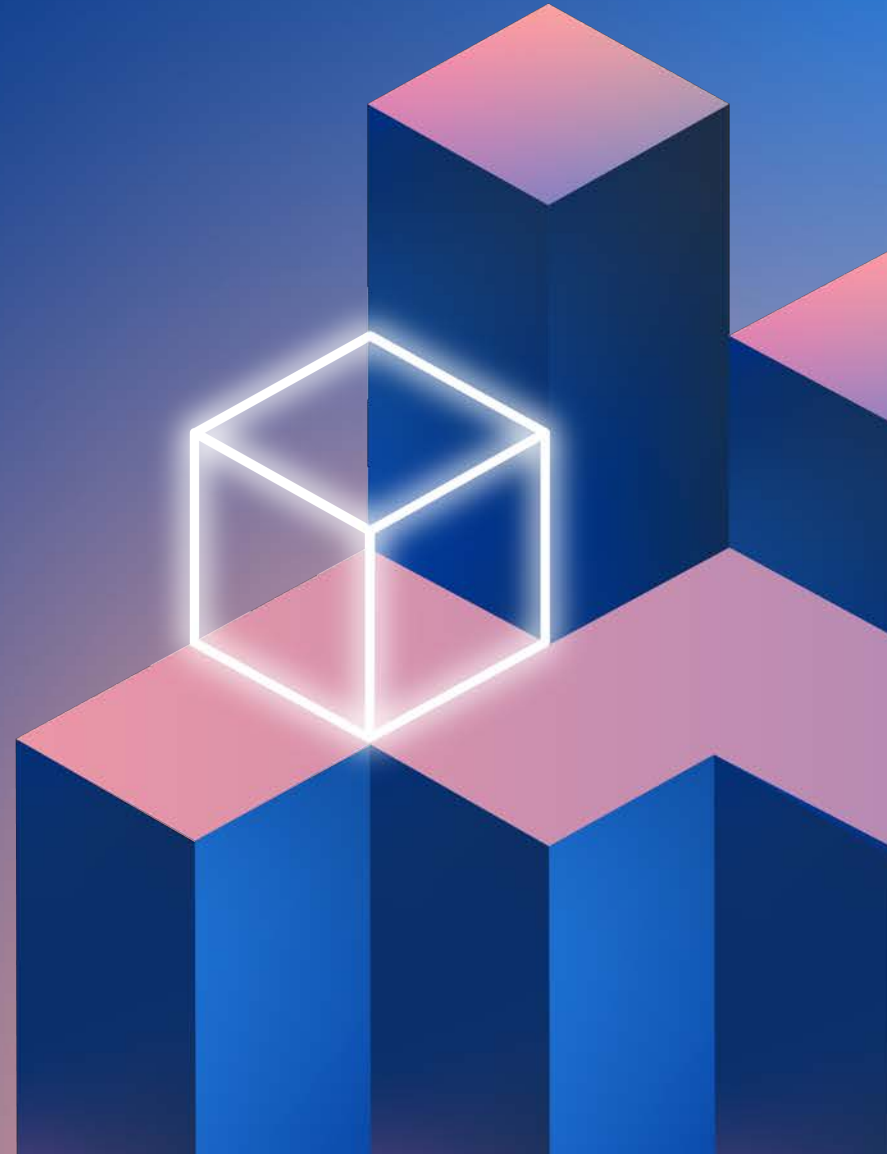


補足 : Session Manager を使ったサーバー接続

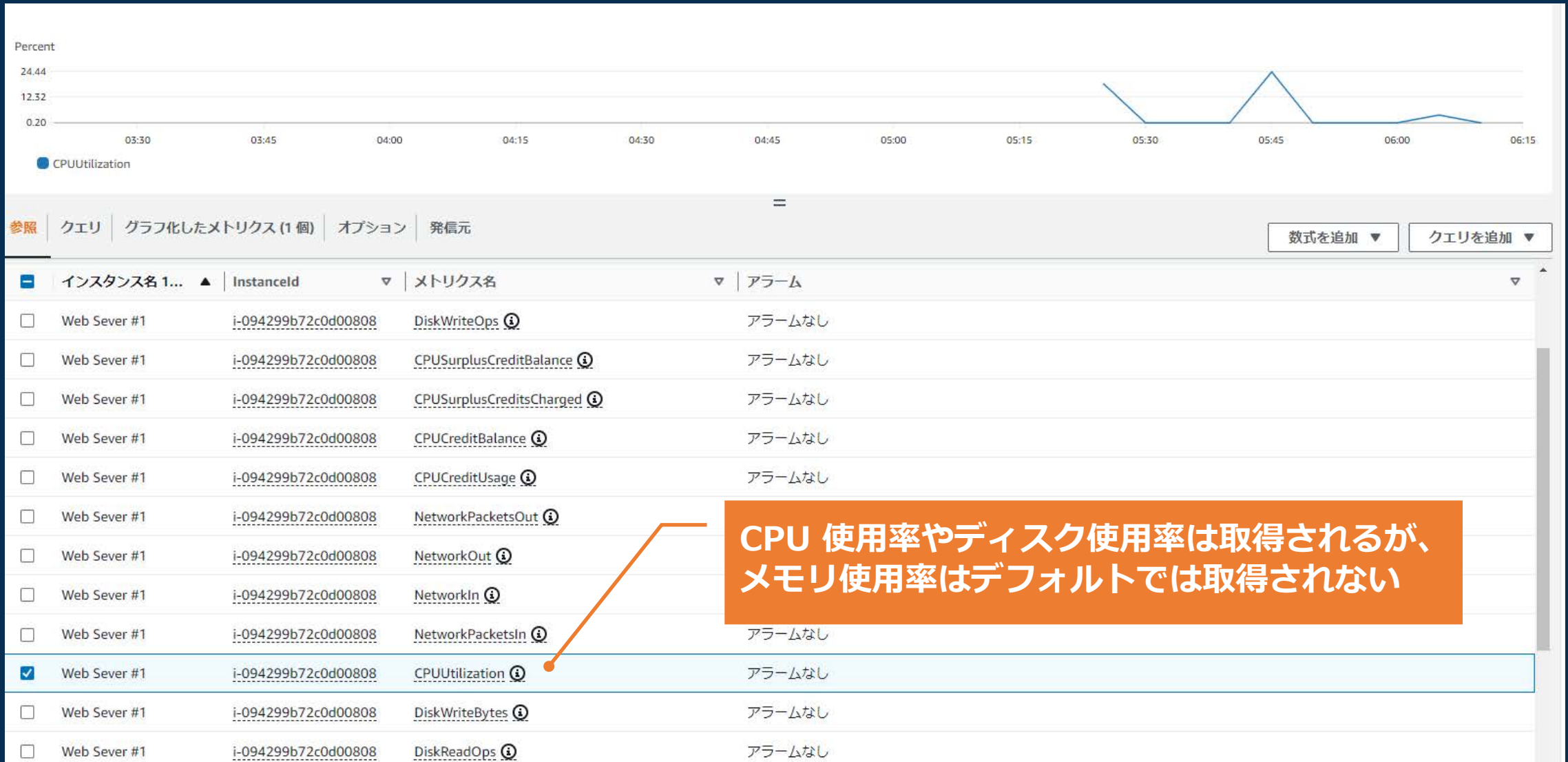
マネージドノード自ら Systems Manager やその機能である Session Manager にアウトバウンド通信を行う仕組みのため、サーバーは**プライベートネットワークに構築可能**で、**インバウンドの開放も不要**



CloudWatch、SNS を利用した監視と通知



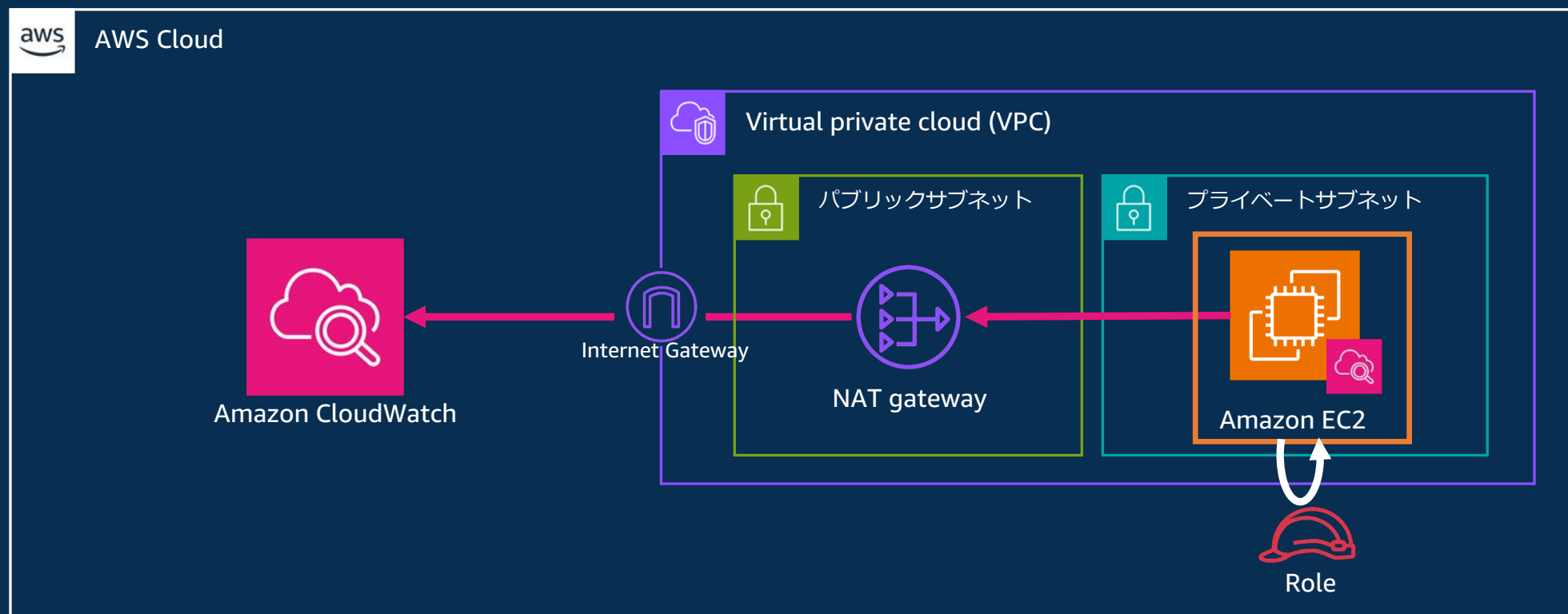
Amazon EC2 のメトリクス画面（一部抜粋）



CPU 使用率やディスク使用率は取得されるが、メモリ使用率はデフォルトでは取得されない

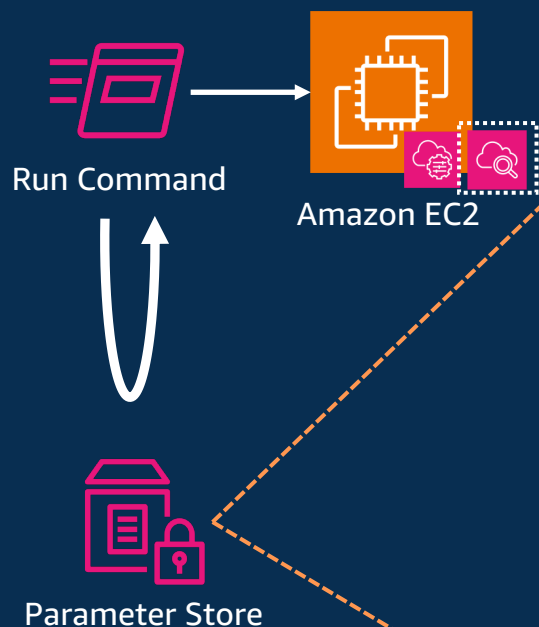
CloudWatch Agent の導入

カスタムメトリクスやログの機能を利用するためには、サーバーに **CloudWatch Agent** の導入が必要
アウトバウンド経路の確保や必要な権限の付与は Systems Manager と同様に必要



Run Command を利用して CloudWatch Agent のインストールおよび設定を行う

設定値の一部抜粋

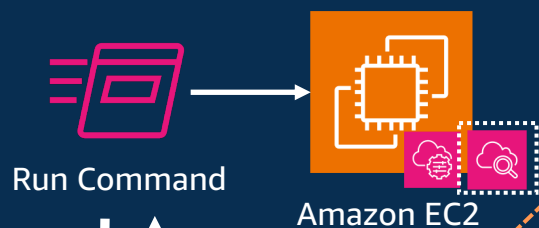


```
"agent": {
  "metrics_collection_interval": 10,
  "logfile": "/opt/aws/amazon-
cloudwatch-agent/logs/amazon-
cloudwatch-agent.log"
},
"metrics": {
  "namespace": "DemoCustomMetrics",
  "metrics_collected": {
    "mem": {
      "measurement": [
        "mem_used",
        "used_percent",
        "mem_cached",
        "mem_total"
      ],
      "metrics_collection_interval": 10
    }
  }
}
```

```
"logs": {
  "logs_collected": {
    "files": {
      "collect_list": [
        {
          "file_path": "/etc/httpd/logs/access_log",
          "log_group_name": "wp-access-log",
          "log_stream_name": "wp-access-log",
          "timezone": "UTC"
        }
      ]
    },
    "log_stream_name": "wp-access-log",
    "force_flush_interval": 15
  }
}
```

Run Command を利用して CloudWatch Agent のインストールおよび設定を行う

設定値の一部抜粋



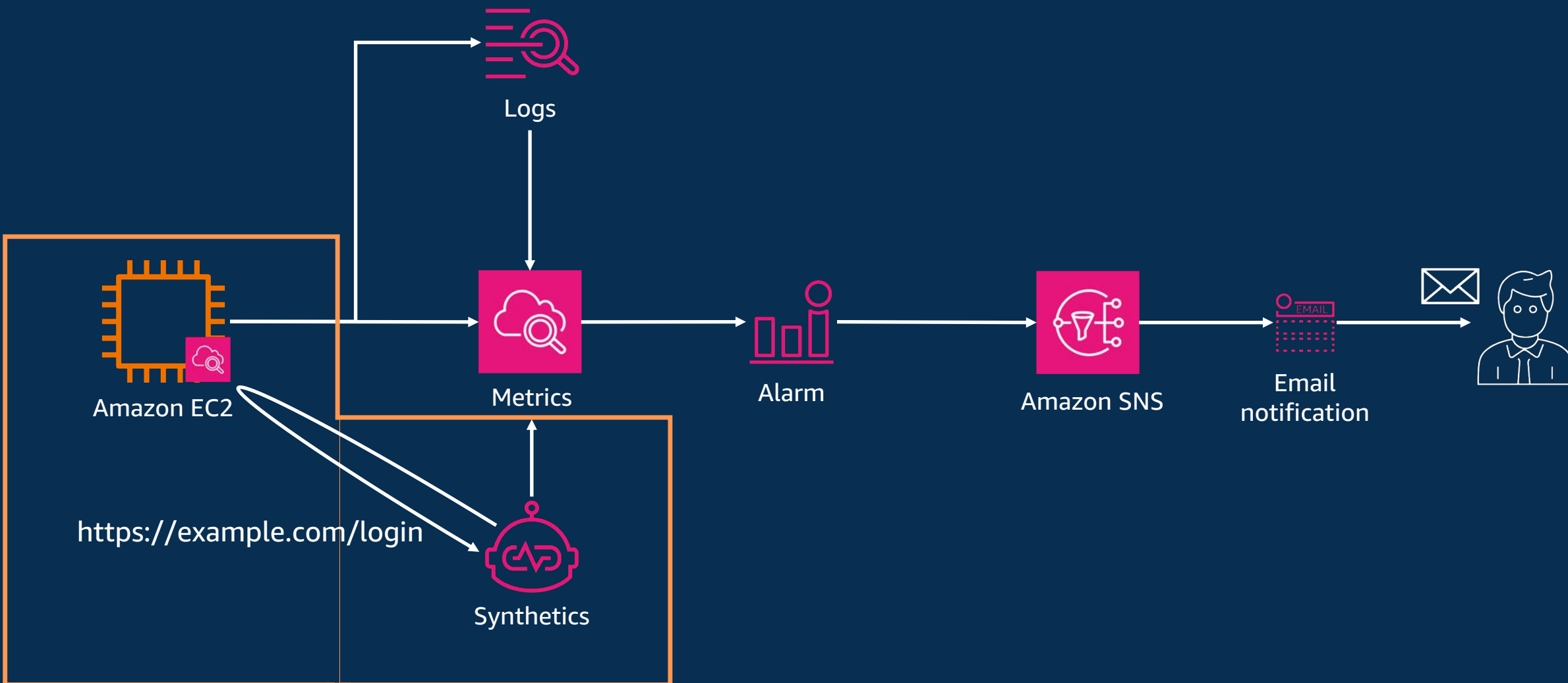
メモリ使用量、メモリ使用率などをカスタメトリクスとして送信

```
"agent": {
  "metrics_collection_interval": 10,
  "logfile": "/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log"
},
"metrics": {
  "namespace": "DemoCustomMetrics",
  "metrics_collected": {
    "mem": {
      "measurement": [
        "mem_used",
        "used_percent",
        "mem_cached",
        "mem_total"
      ],
      "metrics_collection_interval": 10
    }
  }
}
```

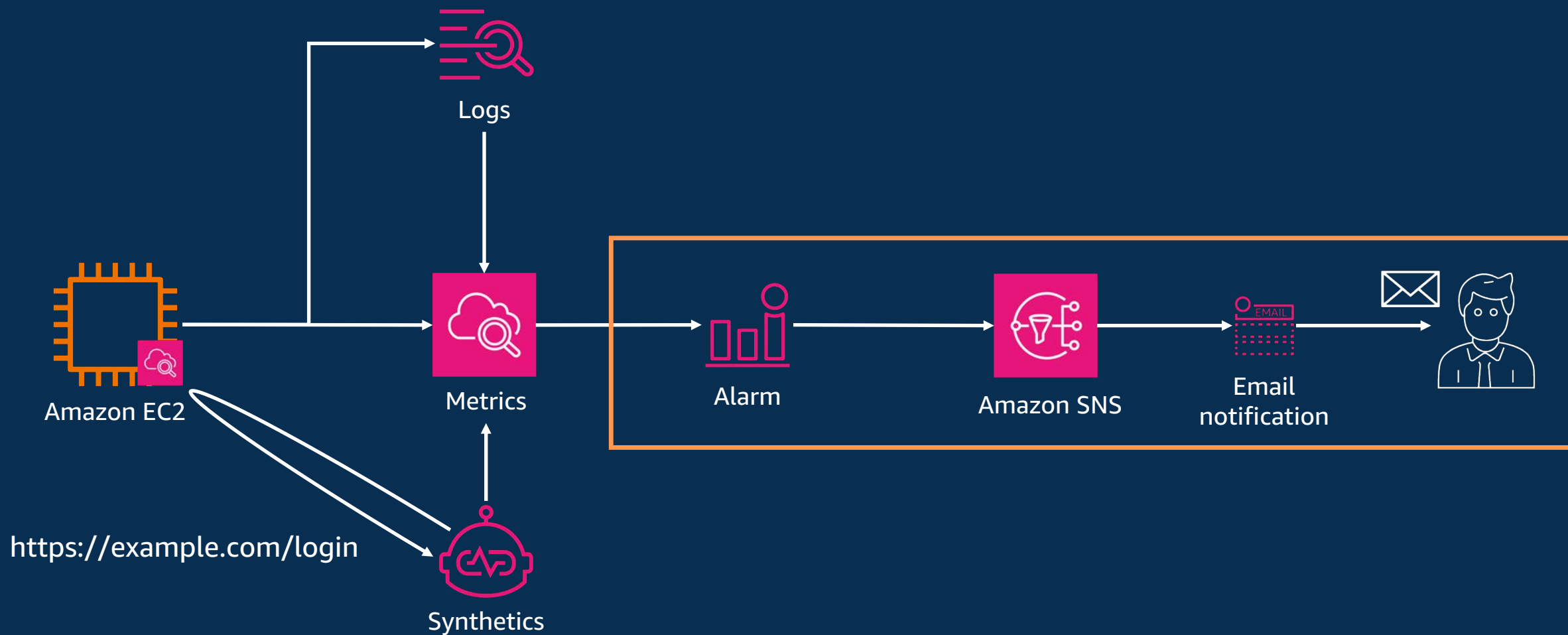
```
"logs": {
  "logs_collected": {
    "files": {
      "collect_list": [
        {
          "file_path": "/etc/httpd/logs/access_log",
          "log_group_name": "wp-access-log",
          "log_stream_name": "wp-access-log",
          "timezone": "UTC"
        }
      ]
    },
    "log_stream_name": "wp-access-log",
    "force_flush_interval": 15
  }
}
```

指定したパスのアクセスログを「wp-access-log」という名前で CloudWatch logs に出力

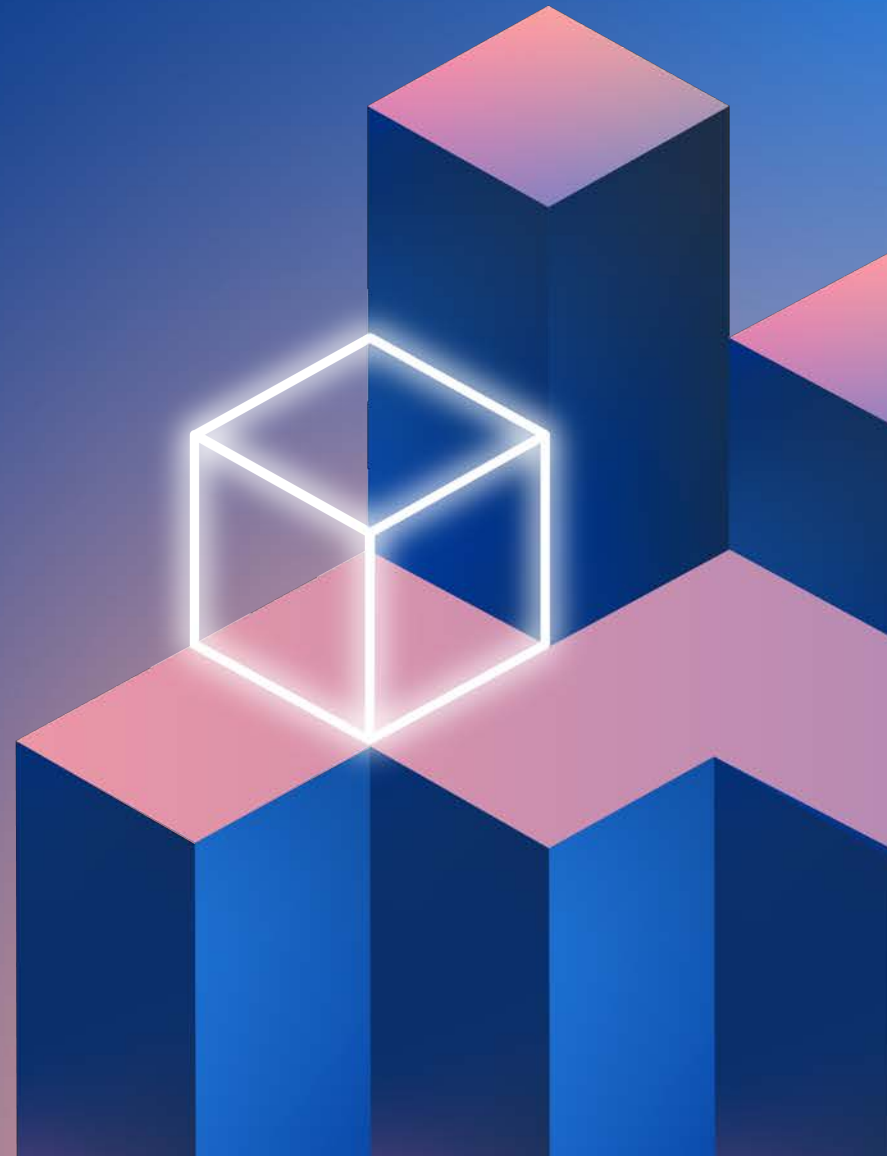
Synthetics 監視



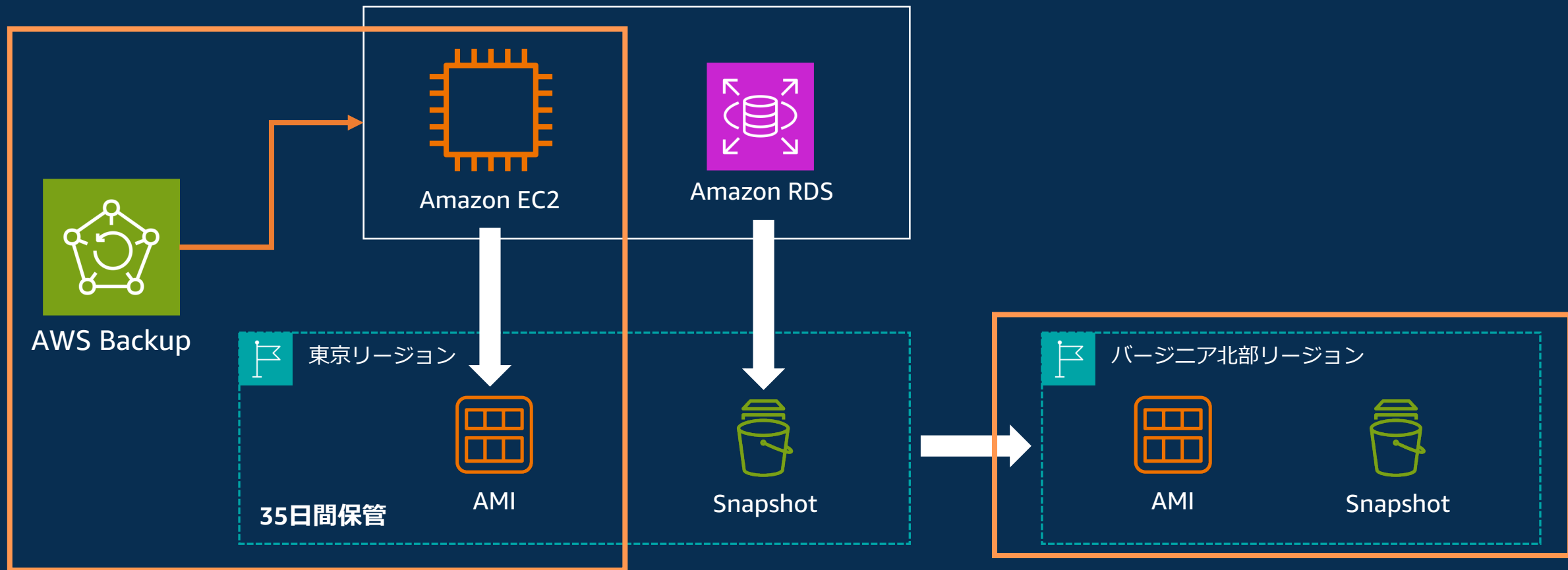
SNS を利用したメール通知



AWS Backup を利用したバックアップ°



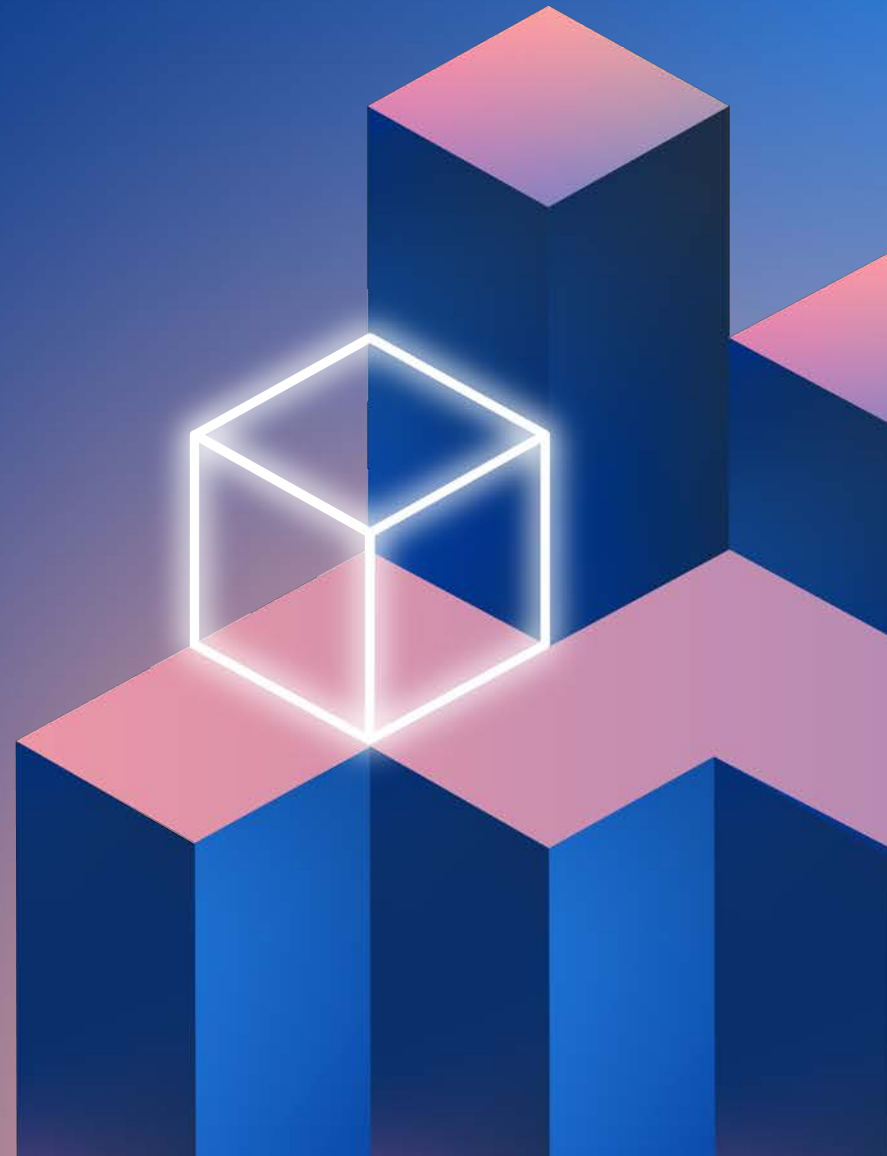
AWS Backup を利用したバックアップ取得



サポートされているリソース

<https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html#supported-resources>

まとめ



料金

本セッションで登場するサービス・機能で料金が発生する要素について概要レベルでご紹介
詳細は各サービスの料金ページをご確認ください

AWS Systems Manager

なし
(本セッションでご紹介した範囲)

Amazon CloudWatch

- ログ
- カスタムメトリクス
- メトリクスを送信する API
- アラーム
- Synthetics (Canaries)

AWS Backup

- Amazon EBS ボリューム
スナップショット
- Amazon RDS データベース
スナップショット

AWS Systems Manager 料金ページ

<https://aws.amazon.com/jp/systems-manager/pricing/>

Amazon CloudWatch 料金ページ

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

AWS Backup 料金ページ

<https://aws.amazon.com/jp/backup/pricing/>



まとめ

- **運用**とはユーザーにサービスを提供し続けるための**すべての業務**
- 運用業務は **AWS** サービスを使うことで**効率化**できる
 - サーバー管理 : AWS Systems Manager
 - 監視、通知 : Amazon CloudWatch 、 Amazon SNS
 - バックアップ : AWS Backup

今後に向けて

本セッションご紹介した内容を具体的な画面を見ながら進めることができるハンズオンです
AWS Builders Online Series の Web ページ内にある **(関連資料) ハンズオン** から
お試しください

- **AWS Systems Manager を使ったサーバー管理はじめの一步編**
- **監視編 サーバーのモニタリングの基本を学ぼう**



Thank you!



AWS TRAINING & CERTIFICATION

600+ ある AWS Skill Builder の無料デジタルコースで学ぼう

30 以上の AWS ソリューションの中から、自分にもっとも関係のあるクラウドスキルとサービスにフォーカスし、自習用のデジタル学習プランとランプアップガイドで学ぶことができます。

自分に合ったスキルアップ方法で学ぼう

EXPLORE.SKILLBUILDER.AWS »



あなたのクラウドスキルを AWS 認定で証明しよう

業界で認められた資格を取得して、スキルアップの一步を踏み出しましょう。AWS Certified の取得方法と、準備に役立つ AWS のリソースをご覧ください。

受験準備のためのリソースにアクセスしよう »



AWS Builders Online Series にご参加いただきありがとうございます

楽しんでいただけましたか? ぜひアンケートにご協力ください。
本日のイベントに関するご意見/ご感想や今後のイベントについてのご希望や改善のご提案などがございましたら、ぜひお聞かせください。



aws-apj-marketing@amazon.com



twitter.com/awscloud_jp



facebook.com/600986860012140



<https://www.youtube.com/user/AmazonWebServicesJP>



<https://www.linkedin.com/showcase/aws-careers/>



twitch.tv/aws