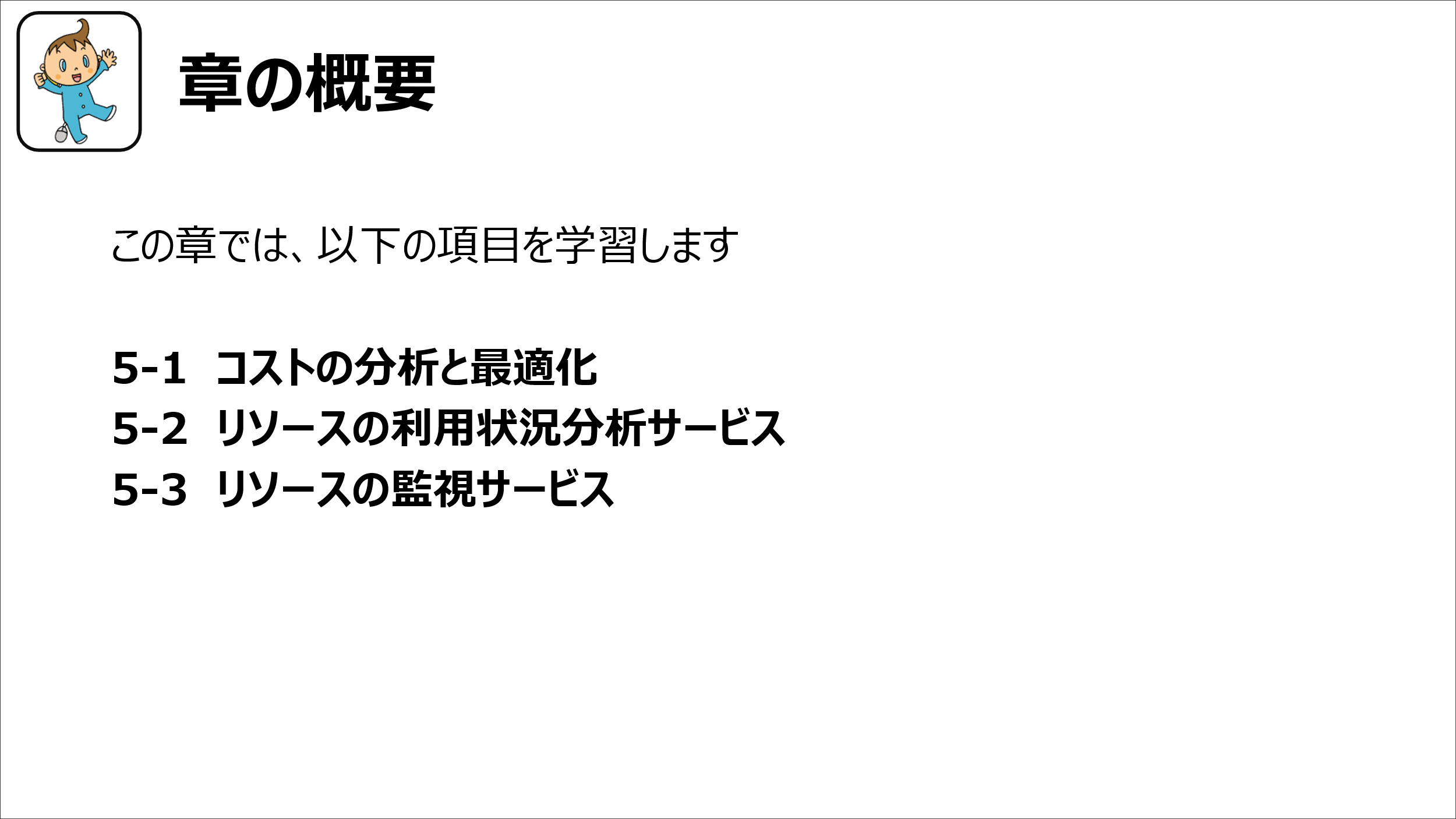
# Chapter5　AWSの利用状況の分析と監視を知りたい



スライド5：章の概要

## コストの分析と最適化



スライド5-1：コストの分析と最適化

* AWS Cost Explorer

AWS Cost Explorer は、Amazon Web Services（AWS）を利用した際に発生するコストと使用状況を時間の流れに沿って管理・分析できる無料ツールで、クラウド支出の可視化に役立ちます。AWSを利用すると、仮想サーバーのEC2、データ保存用のS3、データベースのRDSなど、さまざまなサービスにコストが発生します。

しかし、請求書を見ただけでは「どのサービスにいくら使っているのか」「どのリージョンで費用が増えているのか」がわかりにくいという課題があります。そこで、Cost Explorerを使うことで、利用料金をグラフや表で直感的に確認できます。

* 特徴

リソースの利用状況をグラフや表で可視化できるだけでなく、サービス別・アカウント別・期間別に細かく分析できるため、どこでコストが発生しているかを直感的に把握することが可能です。

また、過去の実績データをもとに将来のコストを予測し、利用傾向を把握することで無駄なリソースを削減でき、効率的なコスト管理につなげることができます。

* AWS Cost Explorerで行う管理と分析

ここではAWSマネジメントコンソールを用いて、Cost Explorerでコストを管理・分析する方法を見ていきましょう。

Cost Explorerにおけるデータの反映には数時間から最大24時間ほどの遅延があるため、直近の利用状況は即時には反映されない点に注意してください。

また、プロジェクト単位や部署単位でコストを管理したい場合は、リソースへのタグ付けをあらかじめ行っておくと、Cost Explorer上での集計やフィルタリングが容易になります。

1. AWSマネジメントコンソールと検索するか、以下URLからアクセスします。  
   <https://aws.amazon.com/console/>
2. AWSマネジメントコンソールにログインし、ホームが表示されることを確認します。
3. 上部の検索バーに[Cost Explorer]を入力し、選択します。



図5-1

1. [請求とコスト管理]が表示されていることを確認します。  
   初回利用時は [Cost Explorerを有効化する]ボタンが表示されます。

クリックして有効化してください。

1. 表示画面では、日次・月次・サービス別・アカウント別などにフィルタをかけ、グラフを切り替えることができます。



図5-2

* AWS Budgets

AWS Budgetsは、クラウド利用にかかるコストやリソース使用量の上限をあらかじめ設定して、予算を超えそうになったら通知してくれるサービスです。

似たサービスに AWS Cost Explorer がありますが、こちらは「過去のコストを分析するツール」です。一方、Budgetsは「未来の支出を予測し、超過を防ぐツール」として位置付けられます。両者を組み合わせると、分析と予算管理の両輪でコスト最適化が可能になります。

* 特徴
* 条件別のフィルタリング

サービス、メンバーアカウント、リージョン、タグといった条件で柔軟にフィルタリングできるため、特定の環境や部署ごとの支出を詳細に把握できます。

* 予算超過のアラート通知

予算を超過する見込みがある場合には自動でアラートが送信され、早めの対応を取ることが可能です。

* リソース使用量ベースでの管理

金額ベースの管理だけでなく、リソース使用量に基づく分析にも対応しており、無駄なリソースの削減や効率的な運用につなげられます。

* 予算の種類

AWS Budgetsでは主に次の4種類の予算を設定できます。

|  |  |
| --- | --- |
| **項目** | **説明** |
| コスト予算(Cost Budget) | 月額いくらまでのように「金額」を基準に管理 |
| 使用量予算（Usage Budget） | EC2の時間数やS3のストレージ容量など、利用量で管理 |
| 予約インスタンス利用率予算（RI Budget） | 購入したRIがどのくらい活用されているかを監視 |
| Savings Plans利用率予算（SP Budget） | 長期割引プラン(Savings Plans)の適用状況を管理 |

* AWS Budgetsを用いた予算の作成

実際に予算の作成まで見ていきましょう。

1. AWSマネジメントコンソールにログインし、ホームが表示されることを確認します。
2. 上部の検索バーに[Budgets]を入力し、選択します。また、左上部のメニューから[Billing]-[Budgets]を選択します。
3. [請求とコスト管理]-[予算]が表示されていることを確認します。
4. 右上部の[予算を作成]をクリックします。

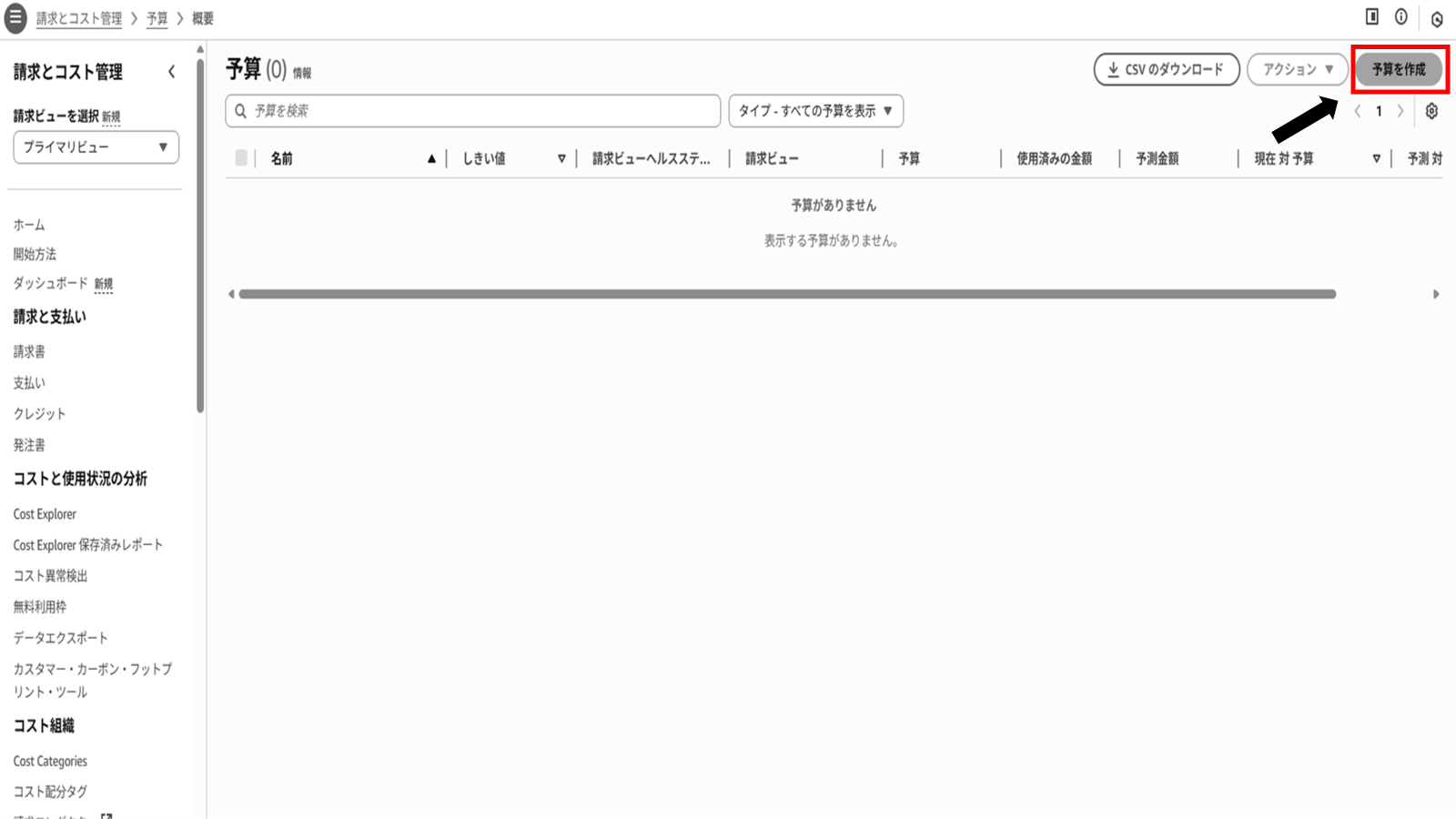


図5-3

1. まずは[月次コスト予算]を選択して、予算額「例:100ドル/月」と入力します。
2. 通知設定でメールアドレスを登録し、アラート通知を誰に送るか設定します。



図5-4

1. スクロールし右下に[予算を作成]をクリックし、予算が正常に作成されることを確認します。

グラフィカル ユーザー インターフェイス, アプリケーション

AI 生成コンテンツは誤りを含む可能性があります。

図5-5

次に作成した予算がダッシュボードに表示されることを確認します。

1. 作成した予算名をクリックします。
2. 現在の使用量やコスト、設定した予算額が比較グラフで表示されていることを確認します。

* AWS Trusted Advisor

AWS Trusted Advisorは、AWSが提供するアカウント診断サービスです。クラウド環境を安全かつ効率的に利用するためのチェックを自動で行い、改善点を「アドバイス」として提示してくれます。

* Trusted Advisor で確認できる内容

Trusted Advisorでは、診断結果を次の5つのカテゴリで表示します。

|  |  |
| --- | --- |
| **項目** | **説明** |
| コスト最適化（Cost Optimization） | 利用していないEBSボリュームやIdleなロードバランサーなどを削除してコストを削減 |
| パフォーマンス（Performance） | 不適切なインスタンスタイプの利用や、リソース不足の可能性を指摘 |
| セキュリティ（Security） | ルートアカウントのMFA設定やセキュリティグループの開放設定を確認 |
| 信頼性（Reliability） | マルチAZ構成が取られているか、障害対策が十分かをチェック |
| サービス制限（Service Limits） | EC2やRDSなどのリソース数が上限に達しそうな場合に通知 |

これらの診断結果をもとに、コスト削減・セキュリティ強化・パフォーマンス改善といった具体的な改善策を実施できます。

* Trusted Advisor の利用手順

1. AWSマネジメントコンソールにログインし、ホームが表示されることを確認します。
2. 検索バーで[Trusted Advisor]と入力して選択します。
3. ダッシュボードが表示され、コスト最適化、セキュリティ、パフォーマンス、フォールトトレランス、サービス制限の5つのカテゴリでチェック結果が確認できます。

グラフィカル ユーザー インターフェイス, アプリケーション

AI 生成コンテンツは誤りを含む可能性があります。

図5-6

## リソースの利用状況分析サービス



スライド5-2：リソースの利用状況の分析

* Amazon CloudWatch Logs

　Amazon CloudWatch Logsは、AWSのいろいろなサービスから出るログを集めて保存し、後から確認できるサービスです。たとえばEC2やLambdaの動作ログをまとめて確認できるので、エラーの原因を探しシステムがちゃんと動いているかをチェックするのに便利です

具体的に3つを紹介します。

* ログ収集と保存

　CloudWatch Logsは、さまざまなAWSサービスやアプリケーションからログを収集し、クラウド上に保存できます。

* EC2インスタンスのシステムログは、CloudWatch Agentを導入すれば自動的に取り込むことが可能です。
* Lambda関数の実行ログを自動で保存され、エラーや処理状況を把握できます。
* 保存期間を1日から無期限まで柔軟に設定でき、長期的な運用監査にも利用可能です。
* 検索と分析

収集したログは、CloudWatchコンソール上で検索やフィルタリングが可能です。

* 特定のキーワード(例：ERROR)でログを素早く検索できます。
* フィルタ条件を使って、発生時間や対象リソースごとに絞り込むことができます。
* Logs Insightsを使えばSQLライクなクエリで集計・分析が可能で、障害対応や不具合の調査に役立ちます。
* 可視化とアラート連携

CloudWatch Logsは、他のサービスと連携して可視化や通知にも活用できます。

* ログからメトリクスフィルターを作成し、CloudWatchダッシュボードでグラフ表示が可能です。
* CloudWatchアラームと組み合わせ、エラー発生時にSNS通知（メールやSMS、Lambda呼び出しなど）を受け取ることができます。
* 定常的に監視することで、問題の早期発見と運用効率化につながります。
* 操作

ここでは、EC2 インスタンスのログをCloudWatch Logs で確認する方法を例として紹介します。

1. AWSマネジメントコンソールにログインします。
2. 上部の検索バーに[CloudWatch Logs]を入力し、選択します。
3. 左メニューから[ログ]を選択し、一覧の中の[ロググループ]をクリックします。

グラフィカル ユーザー インターフェイス, アプリケーション

AI 生成コンテンツは誤りを含む可能性があります。

図5-7

1. 確認したいロググループ[例：/aws/ec2/instance]をクリックします。自動的に作成された[ログストリーム]をクリックすると、ログが時系列で表示できます。
2. 上部の検索バーにキーワード[ERROR]を入力すると、エラー箇所だけ抽出できます。

* VPC Flow Logs

VPC Flow Logsは、AWSの仮想ネットワーク(VPC)内でやり取りされる通信の記録を収集するサービスです。誰が(送信元IP)、どこに(宛先IP)、どのポートを使って、通信が許可されたのか拒否されたのか、どれくらいのデータ量をやり取りしたのかといった情報を自動的にログとして保存します。これにより、普段は目に見えないネットワークの挙動を「見える化」できるため、通信トラブルの原因調査やセキュリティ監査に大きく役立ちます。

VPC Flow Logsの機能は大きく分けて4つの観点で整理できます。

* 監視
* 診断
* メトリック
* ログ

これらを組み合わせることで、セキュリティ強化からコスト最適化まで幅広く活用できます。

* 監視
* 通信ログ収集

C、サブネット、またはネットワークインターフェースごとに、送信元/宛先IP・ポート番号・許可/拒否・データ量などを 自動的に記録 します。

* 通信可否の確認

セキュリティグループやネットワークACLのルールで 通信がブロックされていないか を調べられます。

* トラフィックの傾向把握

特定の時間帯にアクセスが集中していないか、夜間に異常な通信がないかを分析できます。

* 診断
* 許可、拒否トラフィックの見分け

通信が届かない原因が「セキュリティグループの設定か？ACLの設定か？」を切り分けられます。

* 不審な通信の検出

想定外のIPやポートへのアクセスを見つけ、セキュリティリスクを早めに察知できます。

* トラフィック経路の確認

　Flow Logs自体はルート情報を直接出しませんが、他の情報と合わせることでルーティングの問題調査に活用できます。

* メトリック
* 通信量の集計

　パケット数やデータ量を確認し、どの通信がネットワークを多く使っているか把握できます。

* CloudWatchメトリクス化

　ログをCloudWatchのグラフやアラームに変換し、リアルタイムに監視できます。

* ログ
* 保存

　CloudWatch LogsまたはS3に出力して保存できます。

* 検索・可視化

CloudWatch Logsではフィルタで特定のエラーやIPをすぐ探せます。

S3に保存すればAthenaでSQL検索ができ、大量データを効率的に分析できます。

* 保存期間の管理

CloudWatch Logsでは1日から無期限まで保存期間を自由に設定できます。

* VPC Flow Logs を作成して CloudWatch Logs に出力する手順

　ここでは、VPC全体を対象にFlow Logsを作成してCloudWatch Logsに出力する手順を説明します。

1. AWSコンソールにログインし、上部の検索バーに[VPC]と入力し選択します。
2. 左メニューから[仮想プライベートクラウド]-[お使いのVPC]をクリックします。
3. 中央下部の[フローログ]をクリックし、右下部にでてきた[フローログを作成]をクリックします

グラフィカル ユーザー インターフェイス, アプリケーション, PowerPoint

AI 生成コンテンツは誤りを含む可能性があります。

図5-8

1. トラフィックタイプを選択します。[承諾][拒否][すべて]の3項目がありますが、学習や検証では[すべて]がおすすめです。
2. 集約間隔を選びます。[1分][10分]がありますが通常は[10分]で十分です。
3. 送信先を選びます。[CloudWatch Logs]はログを検索・可視化するのに便利で、[Amazon S3]は長期保存やAthenaでの分析に適しています。ここでは[CloudWatch Logs]を選びましょう。
4. 送信先ロググループの指定では未選択で自動でCloudWatch Logsの ロググループが作成されます。
5. サービスアクセスでは[新しいサービスロールを作成して使用]を選べば必要な権限が付与されたIAMロールが自動で作成されます。

グラフィカル ユーザー インターフェイス, アプリケーション

AI 生成コンテンツは誤りを含む可能性があります。

図5-9

1. 以上を設定し、[フローログを作成]をクリックすると設定完了です。
2. 最後にフローログが作成されているか[フローログ]を確認します。

* AWS X-Ray

　AWS X-Rayは、アプリケーションに送られたリクエストの処理経路を可視化する「分散トレーシングサービス」です。

　クラウド環境では、1つのリクエストがAPI Gateway→Lambda→DynamoDBなど複数のサービスを経由するのが一般的です。このようなマイクロサービス構成では、遅延やエラーの原因を従来のログだけで追うのは困難です。

X-Ray を使えば、リクエストがどのサービスを通過し、どこで時間がかかったのか、どこで失敗したのかを エンドツーエンドで追跡できます。

　さらに、サービス間の関係性を自動的に図示する「サービスマップ」により、システム全体の構造やボトルネックを直感的に把握することができます。

* 特徴
* 分散システム対応

マイクロサービスやサーバーレスなど、複数のサービスが関わる環境でも一貫したトレースが可能です。全体像を俯瞰できるため、複雑なシステムでも状況を正しく理解できます。

* トレースの収集

ユーザーのリクエストがどのAWSサービスを通過したかを「足跡」として記録します。これにより、1回のリクエストがアプリ全体でどのように処理されたのかを一貫して追跡できます。

* サービスマップの生成

アプリを構成する各サービス間の呼び出し関係を自動的に図示します。API GatewayからLambda、DynamoDBといった連携の流れを俯瞰でき、依存関係や処理のつながりを直感的に把握できます。

* 遅延の分析

処理ごとの実行時間を分解し、どの段階で時間がかかっているかを数値やグラフで確認できます。ボトルネックを特定し、性能改善の手がかりを得ることが可能です。

* エラーの可視化

処理が失敗した箇所は自動的に強調表示されます。問題のあるサービスや処理を素早く把握でき、トラブルシューティングの効率が向上します。

* サンプリングによる効率化

全てのリクエストを詳細に記録するとコストが増加するため、X-Rayは一部のリクエストを自動的に抽出して保存します。これにより、必要な情報を確保しつつコストを抑えることができます。

* X-Rayのアーキテクチャ

　X-Rayは、アプリケーションから送られるトレースデータを収集し、可視化する仕組みを提供します。流れは以下のとおりです。

1. アプリケーションやサービスに X-Ray SDK または OpenTelemetry（ADOT）を組み込みます。
2. リクエストごとの情報がトレースデータとして生成されます。
3. 収集されたデータが X-Ray サービスに送信され、保存・分析されます。
4. コンソールでサービスマップやトレースを閲覧ができます。

代表的な統合対象としては 、API Gateway、ALB、Lambda、ECS、EKS、RDS、DynamoDB、Step Functions などが挙げられます。

* X-Rayの主要な用語

|  |  |
| --- | --- |
| **項目** | **説明** |
| トレース（Trace） | 1つのリクエスト全体の流れを記録したもの |
| セグメント（Segment） | サービスごとの処理単位 |
| サブセグメント（Subsegment） | 外部APIやデータベース呼び出しなど、さらに細かい処理単位 |
| サービスマップ（Service Map） | 各サービス間の関係を可視化した図 |
| アノテーション | 検索やフィルタに使うキー/値データ |
| メタデータ | 参考情報として記録される追加データ |

* AWS CloudTrail

　AWSでは、すべての操作がAPIという仕組みを通じて実行されます。コンソールでボタンをクリックした場合も、CLIでコマンドを打った場合も、その裏側では必ずAPIが呼び出されています。CloudTrailは、このAPIの呼び出し履歴を記録し、後から参照できるようにするサービスです。

言い換えると、CloudTrailは「AWSで行った行動を残す日誌」のような役割を担っており、「いつ、誰が、何をしたか」を確認でき、運用の安全性や透明性を保つことができます。

* 特徴

　CloudTrailは「イベント」として記録します。イベントには、操作の種類、実行者、対象のリソース、時刻などの情報が含まれています。

イベントには大きく3つの種類があります。

|  |  |
| --- | --- |
| **項目** | **説明** |
| 管理イベント | IAMの設定変更やリソース作成・削除など、管理作業に関する記録 |
| データイベント | S3オブジェクトへのアクセスやLambda関数の呼び出しといった、リソースへの直接的な操作 |
| インサイトイベント | 通常と異なるパターンが見られた場合に生成される特別な記録 |

これらはJSON形式で保存され、S3やCloudWatch Logsに出力できます

* イベント履歴

アカウントを作成した時点で、CloudTrailは自動的に有効になっています。これにより、直近90日分の管理イベントを「イベント履歴」から確認できます。追加設定を行わなくても利用可能です。

* Trailの作成

より長期的に記録を残すには「Trail(証跡)」を作成します。Trailを有効化すると、操作履歴が指定したS3バケットに保存され、後からAthenaなどを使って検索・分析できるようになります。

Trail作成の流れは次のとおりです。

1. AWSマネジメントコンソールにログインします。
2. 上部検索バーに[CloudTrail]と入力して、CloudTrailコンソールを開きます。
3. 左メニューから[Trail]をクリックします。
4. [Trailを作成]を選択します。
5. Trail名を入力し、ログ保存先のS3バケットを指定します。
6. 必要に応じてCloudWatch Logsとの連携を設定し[作成]をクリックします。

## リソースの監視サービス



スライド5-3：リソースの監視サービス

* Amazon CloudWatch Metrics

　CloudWatch Metricsは、リソースの状態を数値化したもので、「データポイント」と呼ばれる値の集まりです。AWSの各リソースは、自動的にさまざまなメトリクスを収集しています。

たとえばEC2、RDS、Lambdaなどの数値を確認することで、リソースの健康状態を把握できます。

* 名前空間とディメンション

CloudWatchメトリクスは 「名前空間」 と 「ディメンション」 で整理されており、名前空間がどのサービスなのかを意識するとわかりやすいです。

* 名前空間：サービスごとに分けられた分類（例：AWS/EC2、AWS/RDS）
* ディメンション：同じサービスでも対象を細かく指定するもの（例：EC2インスタンスIDごとにCPU使用率を確認）
* 基本メトリクス

まずは、以下の基本メトリクスから確認することをおすすめします。

|  |  |
| --- | --- |
| **項目** | **説明** |
| EC2 | CPU使用率、Network In/Out |
| RDS | CPU使用率、Database Connections |
| ELB | リクエスト数、5XXエラー数 |



図5‑10

* Amazon CloudWatch Alarms

CloudWatch Alarmsは、あらかじめ設定したしきい値に基づいてリソースの状態を見守り、条件を満たしたときに自動的に通知やアクションを実行してくれるサービスです。メトリクスの値を一定期間モニタリングし、異常が続いた場合に検知する仕組みを提供します。

* アラームのステート

アラームには3つの状態があります。

|  |  |
| --- | --- |
| **項目** | **説明** |
| OK | 正常範囲内 |
| アラーム状態 | しきい値を超えた状態 |
| データ不足 | データ不足で判断できない状態 |

* Amazon SNS

Amazon SNS（Simple Notification Service）は、AWSが提供するメッセージの通知サービスです。クラウド上で発生したイベント（例：CloudWatch Alarms）を受け取り、あらかじめ登録された宛先に通知する役割をもちます。

* 特徴
* 複数の受信者に同時配信できる：Publish（メッセージを送信する側）/Subscribe（メッセージを受け取る側）モデルを採用しています。これにより、Publisherがトピック（配信先を管理する論理的なグループ）にメッセージを送信するとトピックに登録されたすべてのSubscribe宛に配信されます。
* 配信方法を自由に選択できる：Eメール、SMS、モバイルプッシュ通知、HTTP/HTTPSエンドポイント、Lambda関数など
* スケーラブルが安心：数百万件の通知にも対応可能

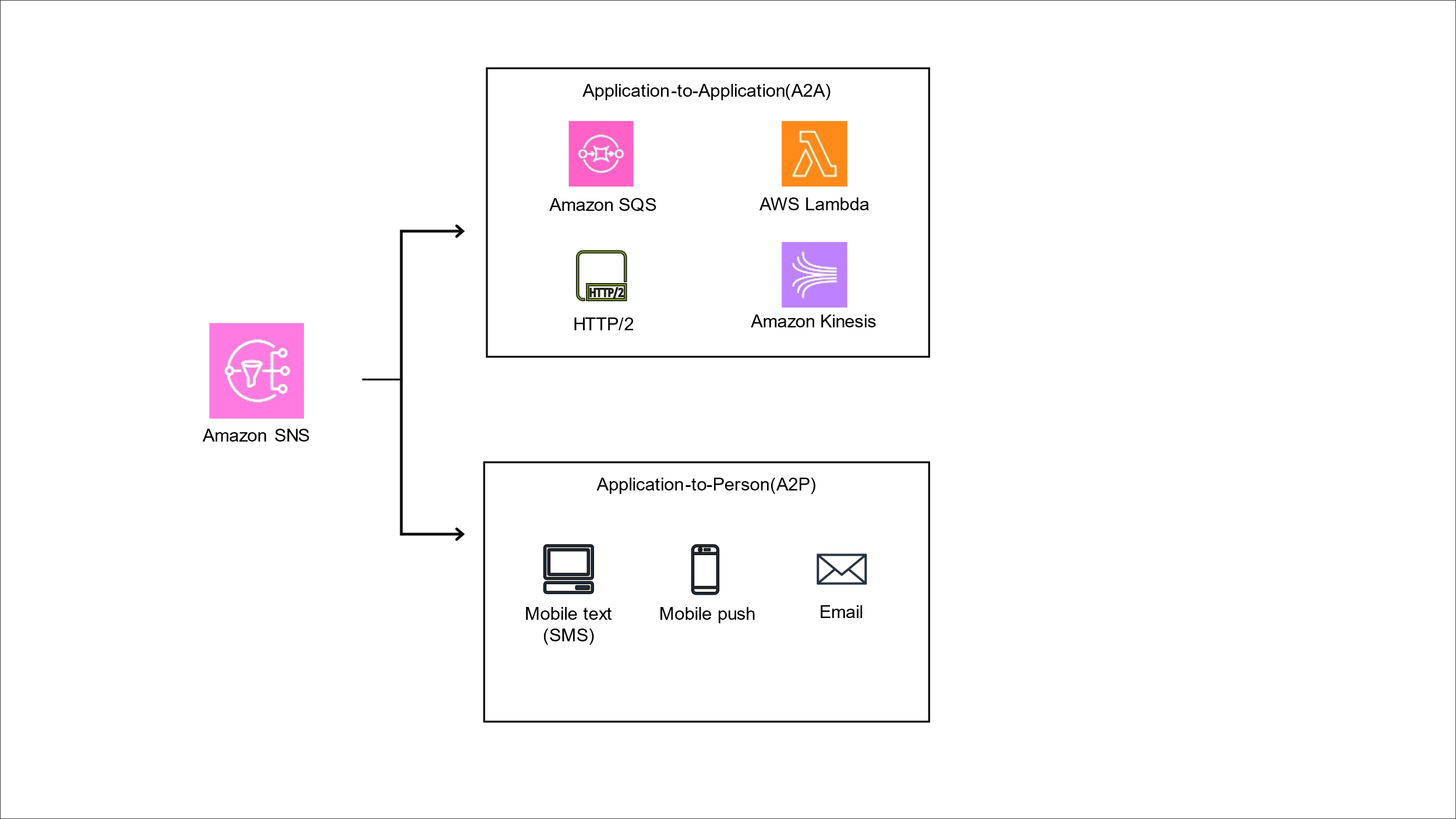
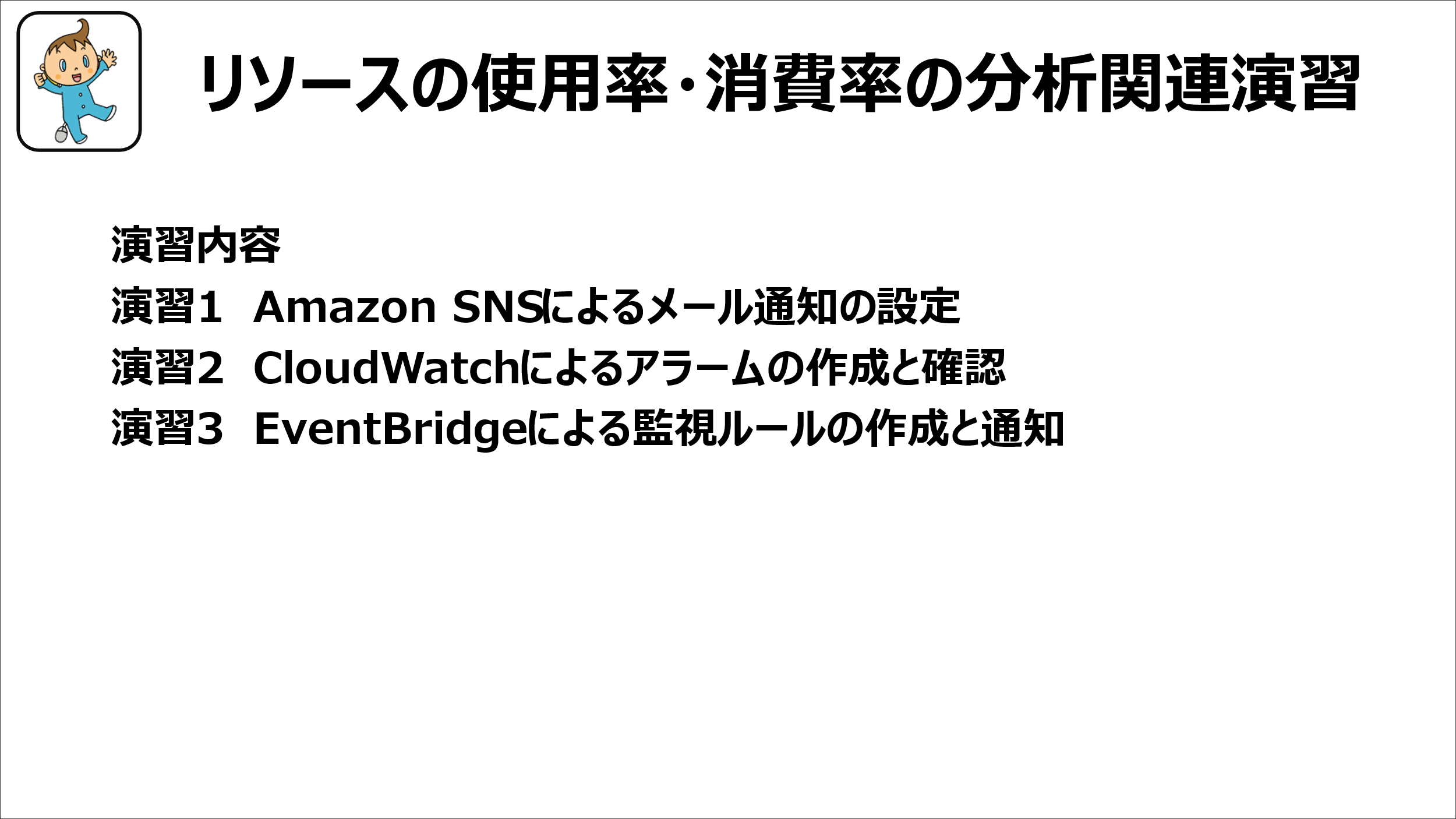


図5-11

## リソースの使用率・消費率の分析関連演習



スライド5-4:リソースの使用率・消費率の分析関連演習

※　以下にリソースの使用率・消費率の分析関連演習の前提条件を示します。

1. 「AWSアカウント」を作成していること。
2. 「AWS 無料利用枠プログラム」が適用済みであること。
3. Amazon Web Servicesアカウントを作成済みであること。

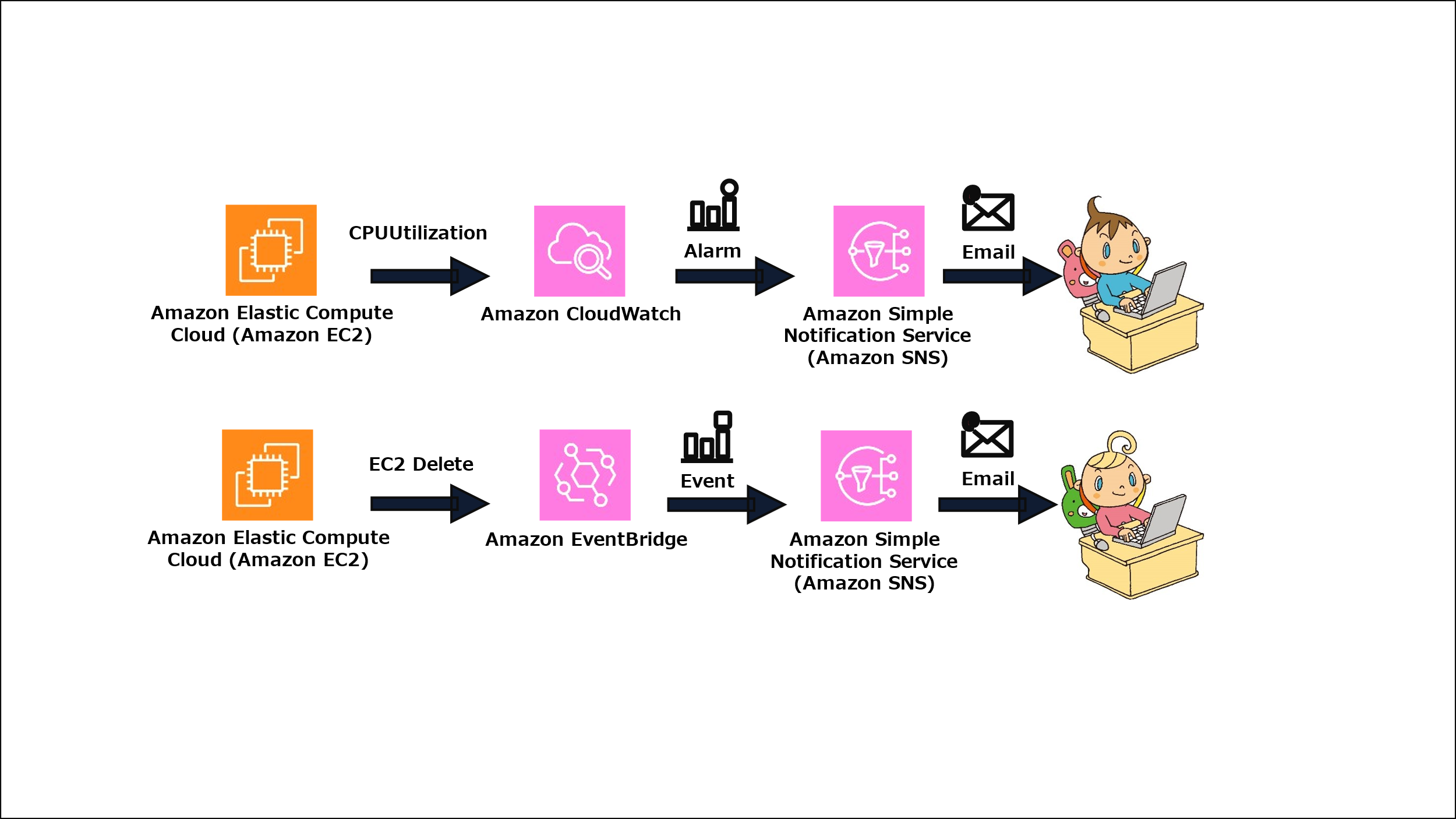
　※　メールアドレスを使った、Amazon Web Servicesアカウントのことをルートユーザーと記載します。

1. リージョンで「アジアパシフィック(東京)- ap-northeast-1」が選択されていること。

※　本演習の記載情報は2025年8月時点の情報です。Amazon Web Servicesはクラウドサービスのため、仕様が変更されている場合があります。

※　Amazon Web Servicesのリソースは稼働時間に対して課金が発生するため、演習が終了したらリソースを削除することを推奨します。

※以下に、リソースの使用率・消費率の分析関連演習の構成図を示します。



演習1 Amazon SNSによるメール通知の設定

1. AWSマネジメントコンソールにログインします。
2. 画面上部の検索バーに[sns]と入力し、検索候補から[Simple Notification Service]をクリックします。
3. 左メニューから[トピック]-[トピックの作成]をクリックします。
4. 下記のとおり選択、入力し、[トピックの作成]をクリックします。

タイプ：スタンダード

名前：test-Notification

1. 左メニューから[サブスクリプション]-[サブスクリプションの作成]をクリックします。
2. 下記のとおり選択、入力し、[サブスクリプションの作成]をクリックします。

トピック ARN：test-Notification

プロトコル：Eメール

エンドポイント：通知を受け取りたいメールアドレス（例：name@example.com）

1. 入力したメールアドレスに確認メールが届くので、メール内のリンクをクリックして確認します。

※この確認を行わないと、SNS通知は送信されません。

以上で、「Amazon SNSによるメール通知の設定」演習は終了です。

演習2 CloudWatchによるアラームの作成と確認

1. AWSマネジメントコンソールにログインします。
2. 画面上部の検索バーに[EC2]と入力し、検索候補から[EC2]をクリックします。
3. [インスタンスを起動]をクリックします。
4. 下記のとおり選択します。

Amazon マシンイメージ (AMI)：Amazon Linux 2023 kernel-6.1 AMI

インスタンスタイプ：t3.micro

キーペア：MSItest-key

[ネットワーク設定]-[編集]-[VPC]：MSItest

1. [インスタンスを起動]をクリックし、起動完了を待ちます。
2. AWSマネジメントコンソールで画面上部の検索バーに[CloudWatch]と入力し、検索候補から[CloudWatch]をクリックします。
3. 左メニューから[アラーム]-[すべてのアラーム]-[アラームの作成]を選択します。
4. [メトリクスの選択]-[EC2]-[インスタンス別メトリクス]をクリックし、作成したインスタンスの[CPUUtilization]を選択し、[メトリクスの選択]をクリックします。
5. [メトリクスと条件の指定]画面で下記のとおり選択し、[次へ]をクリックします。

しきい値の種類：静的

CPUUtilization が次の時...：より大きい

... よりも：80

1. [アクションの設定]画面で下記のとおり選択し、[次へ]をクリックします。

アラーム状態トリガー：アラーム状態

次のSNSトピックに通知を送信：既存のSNSトピックを選択

通知の送信先：test-Notification

1. [アラームの詳細の追加]画面で下記のとおり入力し、[次へ]をクリックします。

アラーム名：test-Alarm

1. [プレビューと作成]画面で[アラームの作成]をクリックします。
2. CloudWatchの[アラーム]画面に戻ります。
3. 作成したアラームが[OK]、[アラーム]、[データ不足]などの状態で表示されていることを確認します。

以上で、「CloudWatchによるアラームの作成と確認」演習は終了です。

演習3 EventBridgeによる監視ルールの作成と通知

1. AWSマネジメントコンソールにログインします。
2. 画面上部の検索バーに[EventBridge]と入力し、検索候補から[Amazon EventBridge]をクリックします。
3. 左メニューから[バス]-[ルール]-[ルールの作成]を選択します。
4. [ルールの詳細を定義]画面で下記のとおり入力し、[次へ]をクリックします。

名前：test-Rule

ルールタイプ：イベントパターンを持つルール

1. [イベントパターンを構築]画面のイベントパターンで下記のとおり選択し、[次へ]をクリックします。

作成のメソッド：パターンフォームを使用する

イベントソース：AWSのサービス

AWSのサービス：EC2

イベントタイプ：EC2 Instance State-change Notification

イベントタイプの仕様 1：特定の状態

特定の状態：terminated

1. [ターゲットを選択]画面で下記のとおり選択し、[次へ]をクリックします。

ターゲットを選択：[SNSトピック]

トピック：test-Notification

1. [タグを設定 - オプション]画面で[次へ]をクリックします。
2. [レビューと作成]画面で[ルールの作成]をクリックします。
3. AWSマネジメントコンソールで画面上部の検索バーに[EC2]と入力し、検索候補から[EC2]をクリックします。
4. 左メニューから[インスタンス]をクリックし、演習2で作成したインスタンスを選択し、[インスタンスの状態]-[インスタンスを終了]をクリックします。
5. 削除操作を確認し、インスタンスを終了します。
6. SNS経由で送信されたメールを確認します。

以上で、「EventBridgeによる監視ルールの作成と通知」演習は終了です。