OpsRamp

［ホワイトペーパー］

サービス志向の AIOps

OpsRamp OpsQ は IT オペレーションの効率化と対応の迅速化をどう実現するのか

目次

はじめに

IT オペレーションの未来において、効率性の鍵となるのは自動化です。
いまやIT基盤はビジネスやテレワークなど柔軟な働き方の実現において重要な要素であり、IT基盤の安定した運用管理はITチームにとっては大きな課題となっています。大量のデータ、アラート、相反するビジネス上の重要事項に悪戦苦闘するデジタルオペレーションチームにとって、人工知能を活用した自動化は大きな競争優位となります。より多くの作業をより短時間で（しかも、より少ない資源で）処理しなければならない厳しい状況において、IT オペレーション向けの人工知能、すなわち AIOps の活用は理にかなった選択肢です。AI機能に加えて、緊急時に社外からでもリモートで運用管理できるクラウドサービスであることはBCPの観点からも求められる要件になるでしょう。

AIOps は革新的技術であり、まだその初期段階にあります。
クラウドネイティブなサービスやハイブリッドインフラがかつてないほどの複雑性をもたらすなか、AIOps は、IT オペレーション機能のスケーリングに不可欠な要素となります。AIOps に期待できることは、マシンデータ分析からより迅速かつ効率的な IT サービスマネジメントまで多岐にわたります。

それだけではなく、企業の IT チームにとって、サービス中心の AIOps は、インフラの複雑性を管理し、デジタルサービスを維持し、事業のニーズを満たすための真にユニークなソリューションを提供します。AIOps　に対するサービス中心のアプローチは、システムの健全性をプロアクティブに監視し、アラートの嵐を削減し、問題に素早く対応・修復することによって、システムの混乱を防ぎます。

本文書では、機械学習および関連する計算法によって提供され、効率化される 3つのタスク、
①インテリジェントアラート、②アラートの関連付け、③自動修復 & エスカレーション を取り上げます。
OpsRamp OpsQ が、企業の IT 環境全体にまたがる膨大なデータセットを分析、正規化、処理することにより、分野横断的な分析を行い、いっそうの文脈的可視性とプロアクティブな洞察をもたらすことを理解していただけるでしょう。

- **効率性の向上：** 高度な推論モデルにより、複雑なパターンに存在する因果関係を明らかにし、以前は管理できなかった複雑性に対処
- **インシデントの自動検知および解消：** 機械学習を活用した根本原因解析と異常検知により、インシデント解消をスピードアップ。
- **マルチクラウドの最適化：** ダイナミックなクラウド環境におけるインテリジェントな容量分析と継続的最適化。

第1章：インテリジェントアラートとしきい値

ネットワークオペレーションセンター（NOC）のチームは、企業データセンターの仮想または物理デバイスにホストされた最新のデジタルサービス、あるいはパブリッククラウドの IaaS や PaaS サービスから絶え間なく発信されるアラートに直面しています。マネージド IT リソースに関するメトリクスが監視され、所定のしきい値を超えるとアラートが発信されます。
このような監視メトリクスは、IT リソースの容量利用率や性能データを示します。

監視業務の一環として、IT オペレーションチームは、アラートに関連して以下のタスクが発生します。

1. 取り込んだアラートを共通の原因と関連付ける
2. 解決に向けてアラートのトリアージと優先順位付けを行う
3. さらなる根本原因分析が必要な問題についてインシデントチケットを作成するなど、ITSM ツールと連携して問題管理を改善する

アラート受信件数の増加に伴い、取り込んだアラート 1件あたりのタスクフローの平均所要時間は加速度的に増加します。
OpsRamp OpsQ を導入すれば、インテリジェントアラーティングを適用し、各タスクを最大限に自動化することで、**アラート1件あたりに要する人的時間を削減**することができます。

インテリジェントアラートの目的は、ユーザーへの影響が生じる前に容量または性能劣化状況を特定することです。実際によく生じるインテリジェントアラートのユースケースは 2種類あります。

- **既知のしきい値がある状況：** メトリクスの大部分に容量または性能劣化条件を示す既知のしきい値がある場合。たとえば、サーバーの持続的な CPU 使用率が 90% を超える場合、CPU が制約条件下にあることを示します。

- **既知のしきい値がない状況：** ある種のメトリクスは、「正常」な運用範囲がシステムの全体状況によって異なるため、現実的にしきい値を設定することができません。たとえば、ウェブサイトにおけるユーザーの要求に対する応答時間は、サイトの背景にあるウェブ、アプリケーション、データベース構成要素によって異なります。

アラートを引き起こすメトリクスは、主に 2種類あります。

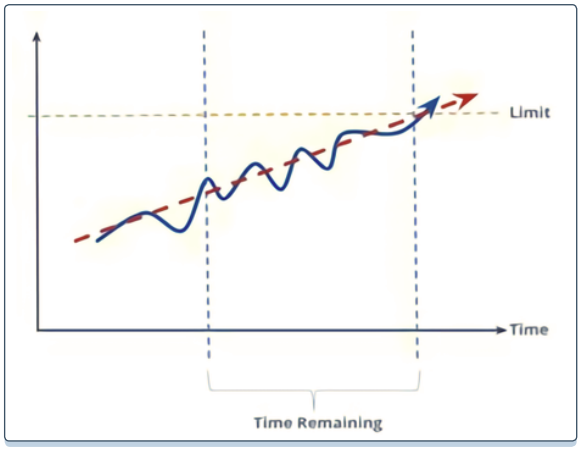
- **性能メトリクス：** ユーザーの要求に対する応答時間、ディスクの入出力の遅延時間
- **容量メトリクス：** ディスクスペースの残量、メモリ使用率

機能

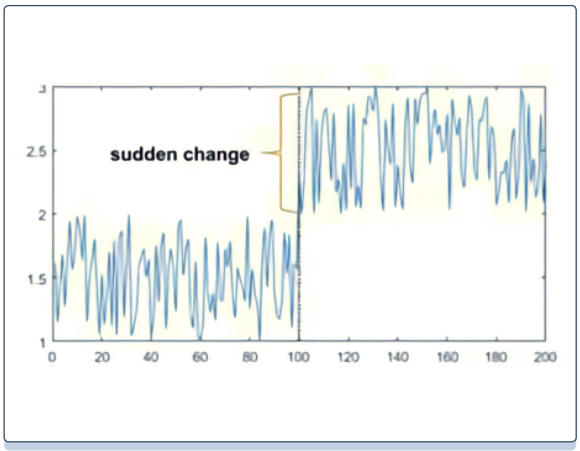
OpsRamp は、インテリジェントアラートの 2通りのユースケースに対応したそれぞれ 3つの特徴があります（図1、図2 を参照）。

ユースケース	**OpsRamp** の機能
既知のしきい値がある状況	**しきい値超過に関するアラート：** メトリックの値が既知のしきい値を超過したときにアラートを生成します。このようなアラートは、明確な傾向を持たずに急速に変動するメトリック（CPU またはメモリ使用率など）に最も効果的です。 **しきい値超過までの予想時間に関するアラート：** 既知のしきい値を超過するまでの予想残り時間に基づいてアラートを生成します。このようなアラートは、明確な傾向を持って徐々に上昇する（または低下する）メトリクスに適しています。
既知のしきい値がない状況	**突然の変化に関するアラート：** 最近の挙動から突然の変化を検知したときにアラートを生成します。変化は、プラスの方向にもマイナスの方向にも起こりえます。このようなアラートは、突然の挙動変化が性能劣化を示すようなメトリクス（応答時間の突然の増大など）に適しています。

図1： アラート対応ワークフロー

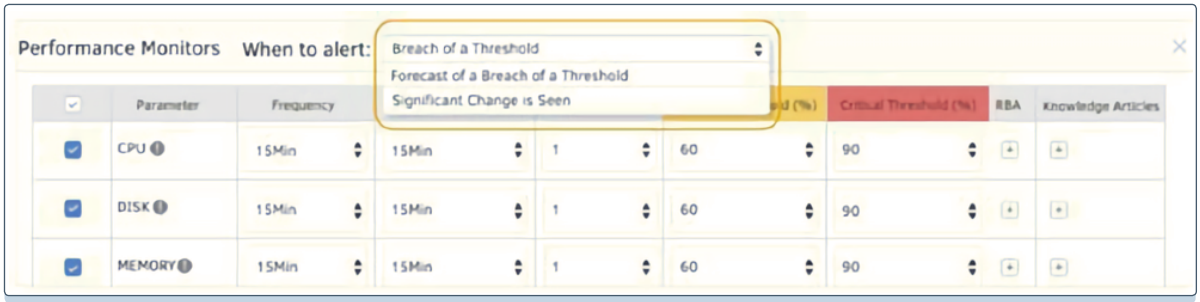


しきい値超過までの予想時間に関するアラート



突然の挙動変化に関するアラート

図2： OpsRamp のしきい値オプション



OpsRamp

第2章： アラートの関連付け

アラートの関連付けルールを用いて、アラートを一次的なものと二次的なものに分類し、それらを関係づけることができます。そのうえでユーザーは、アラートをクラスター化し、因果関係の把握に役立つ推論という上位レベルの情報を生成することができます。

ここでは、同一原因により多重のアラートが引き起こされる状況が見られるカスケードインパクトとパラレルインパクトという 2つのユースケースを分析します。

カスケードインパクト（垂直方向の連鎖障害）

カスケードインパクトは、上流で生じたひとつの障害（およびそれがもたらすアラート）が下流に伝播していき、やがて依存関係によって連鎖するアラートをシステム全体に引き起こすというユースケースを指します。その場合、根本原因である上流のアラートを特定することが重要になります。

図3 および 4は、カスケードインパクトの 2つの事例を示しています。

図3 では、スイッチ1がダウンし、スイッチへのネットワーク接続に依存する下流デバイスへのアラート伝播を引き起こしています。「シグナル」を示すアラートは、スイッチ1 のアラートのみです。それ以外のアラートは、原因条件に関連する「ノイズ」です。

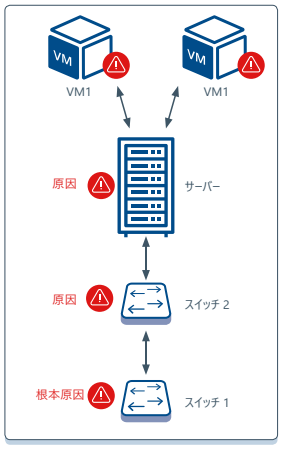


図3：
ネットワークにまたがる
カスケードインパクト

アラート

ID	Subject	Device	Status	Related Alerts
12789	インターフェイスif-1がダウン	スイッチ 1	重要	--
34578	デバイスに到達不可能	スイッチ 1	重要	--
78657	ホストがダウン	Server	重要	--
...	...	...	...	--

推論

ID	Subject	Device	Status	Related Alerts
12789	インターフェイスif-1がダウン	スイッチ 1	重要	10

図4 では、マイクロサービスD がダウンし、それに依存する他の 3つのマイクロデバイスの可用性に影響を及ぼしています。ここでは、どのマイクロサービスが問題を引き起こしているかを理解するためには、正しい文脈が不可欠です。

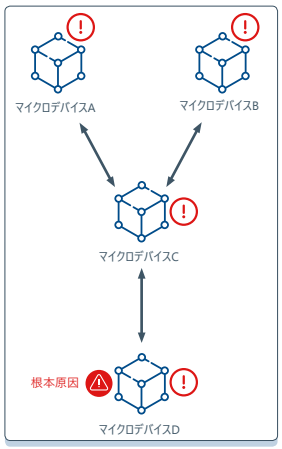


図4：
アプリケーションコン
ポーネントにまたがる
カスケードインパクト

アラート

ID	Subject	Resource
12789	マイクロサービスAがダウン	マイクロサービスA
34578	マイクロサービスBがダウン	マイクロサービスB
78657	マイクロサービスCがダウン	マイクロサービスC
78657	マイクロサービスDがダウン	マイクロサービスD

推論

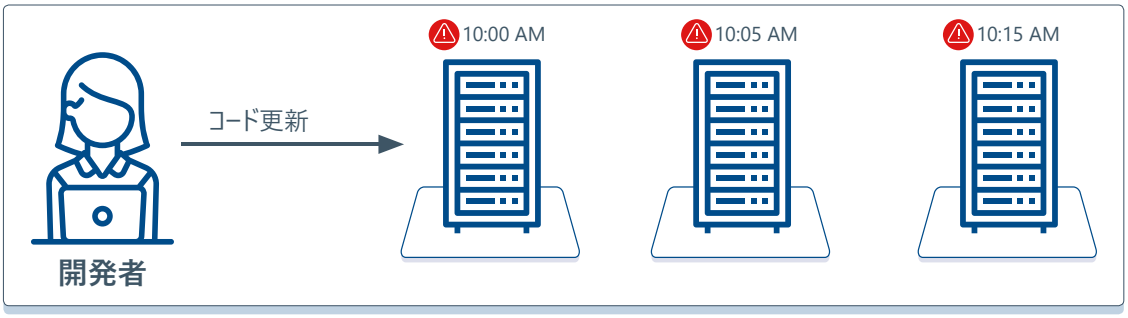
ID	Subject	Resource	Correlated Alerts
78657	マイクロサービスDがダウン	マイクロサービスD	3

パラレルインパクト（並列方向の障害連鎖）

パラレルインパクト型のアラートは、通常、複数の要素に同時に適用される単一のソースから始まります。カスケードインパクト型のアラートと同様、結果は、ひとつの根本原因がアラートの洪水を発生させます。

図5 は、パラレルインパクト型ユースケースの例を示しています。開発者が、クラスター内の異なるサーバーに対してコード更新を行います。更新にはバグがあり、各サーバーにアラートを引き起こします。「シグナル」を示すアラートはひとつもありません。これらすべてのサーバーに生じた他のアラートは、すべて同じ情報を伝えるものなので、「ノイズ」です。オペレーションチームは、的確に障害対応を行うため、複数のアラートから適切な「シグナル」を推論する必要があります。

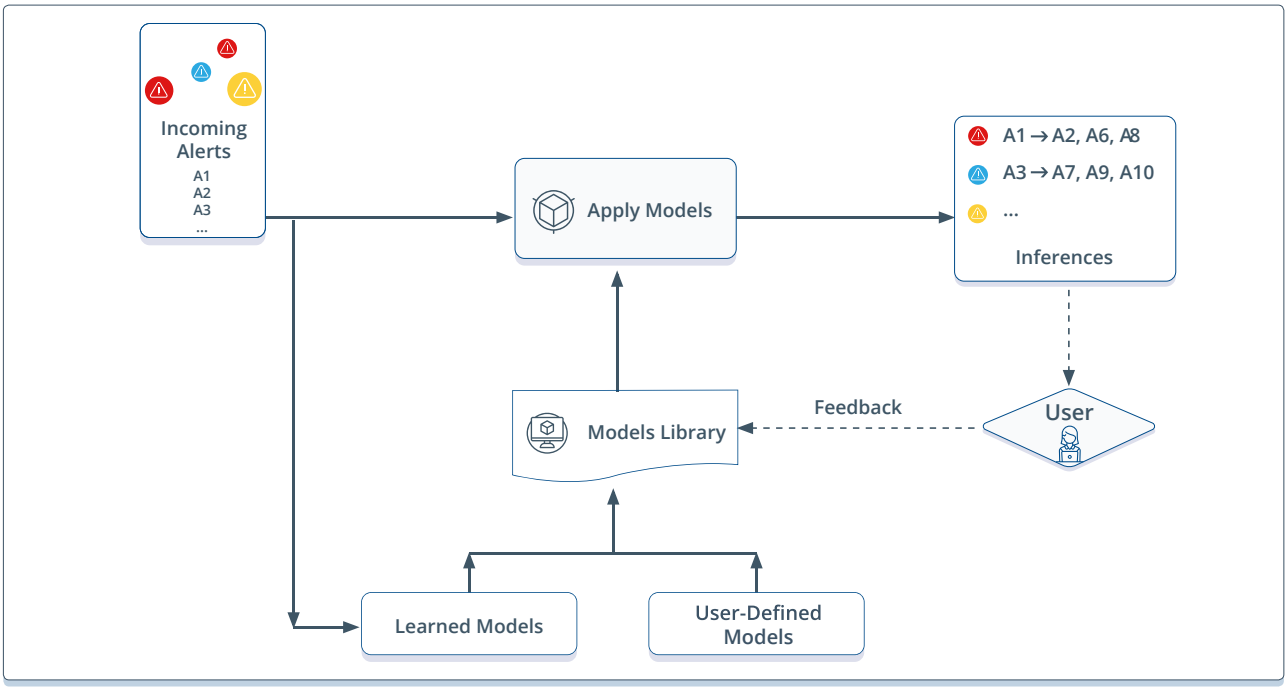
図5：アプリケーションコンポーネントにまたがるカスケードインパクト



OpsRamp がどう問題を解決するか

OpsRamp OpsQ は、機械学習や他のデータ駆動型アプローチを適用して、同一の原因条件から生じるアラートを関連付け、推論します。OpsQ は、常にパターンを学習し、学習したモデルを受信アラートストリームに適用して、カスケードインパクトやパラレルインパクトが意味するものを解明します。また、学習モデルに基づき、関連するアラートをグループ化して推論を形成します。その結果、ITチームは、個々のアラートに対処する代わりにこれらの推論を管理することで、ユーザーが日常業務の中で取捨選択しなければならない「ノイズ」を減らすことができます。図6 は、OpsQ のアルゴリズムに基づくアラート関連付けを示しています。

図6：アプリケーションコンポーネントにまたがるカスケードインパクト



OpsQ は、機械学習に基づいて自動的に推論モデルを構築し、ユーザーが実際に見られる環境固有のパターンを包含する独自のモデルを定義するための枠組みを提供します。

下表は、OpsRamp によるアラート関連付けの特徴をまとめたものです。

OpsRamp の特徴	概要
トポロジーの検出	トポロジーエクスプローラー： アラートの関連付けに重要な情報は、（ネットワークおよびアプリケーションレイヤー上の）IT 要素間のトポロジー的関係です。 「何が何につながっているか」と「何が何に話しかけているか」を知ることは、アラートの関係を理解するために不可欠です。 OpsRamp は、自動的にネットワークおよびアプリケーションのトポロジーを検出します。ユーザーは、OpsRamp の関連付けアルゴリズムに使われるトポロジーマップを見ることができます。ネットワークおよびアプリケーションのトポロジーマップの例として、図7 および図8 をご覧ください。
推論モデル	図9 は、OpsRamp が現在提供している 3タイプのモデルを示しています。 **下流インパクトモデル：** このユーザー定義モデルは、（図3および4に示した）カスケードインパクト型ユースケースに適しています。このモデルでは、上流および下流のデバイスと、それらのトポロジー的関係に沿って伝播するアラートのタイプをインプットとします。 **アラート類似性モデル：** このユーザー定義モデルは、図5 に示したようなパラレルインパクト型ユースケースに有効です。このモデルでは、アラート間の関連性が認められるために「おおむね」一致しなければならない属性をインプットとします。 **統計的共起モデル：** この機械学習モデルは、カスケードインパクト型とパラレルインパクト型のいずれのユースケースにも適しています。このモデルは、ユーザーのインプットを必要とせず、特定のアラートシーケンスが発生する実績頻度を使用します。高頻度に発生するアラートシーケンスは、相関アラートとして表示されます。 推論モデルは、SaaS としての OpsRamp が持つ主要な利点を生かせる可能性があります。機械学習モデルは、（将来的に）さまざまマネージド環境にまたがる無数のデータベースから学習することが可能です。
推論のライフサイクルマネジメント	図6 に示したとおり、OpsRamp は、相関アラートをグループ化して推論を生成します。ユーザーは、個々のアラートに対処する代わりに推論のライフサイクルを管理すればよいため、イベント関連付けの所要時間を大幅に短縮することができます。1回のアクションで、推論を確認および抑制し、チケットを作成することができます。図10 は、推論を示しています。

図7： OpsRamp の自動検出ネットワークトポロジー

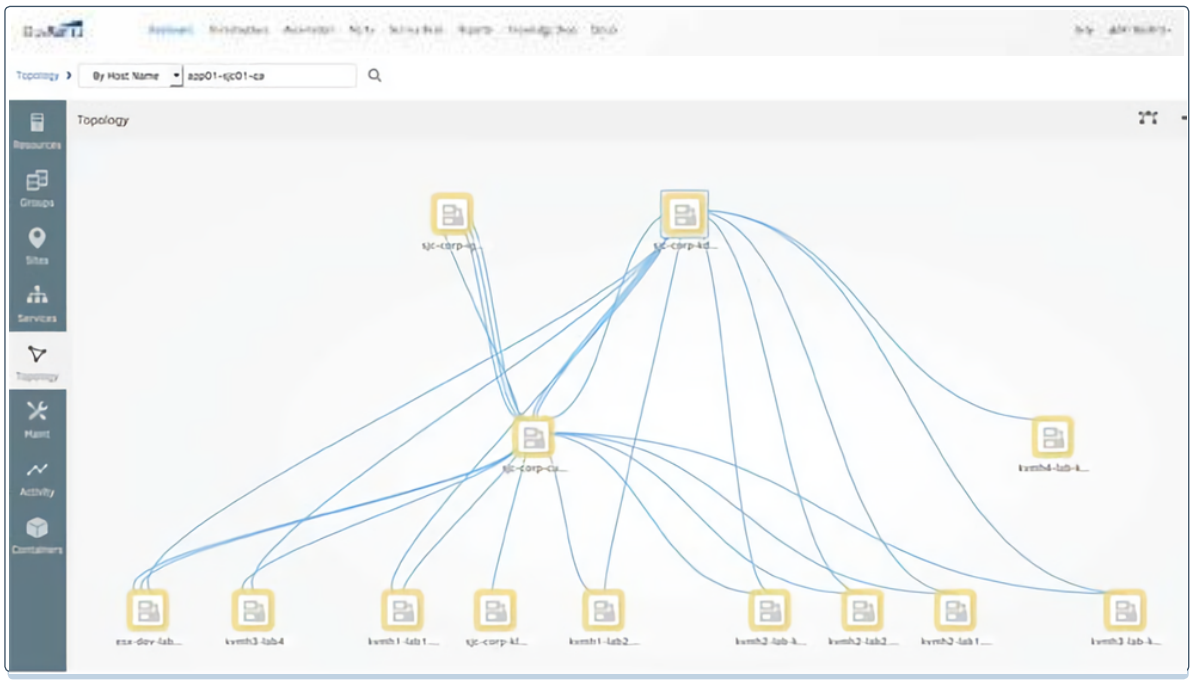


図8： OpsRamp の自動検出アプリケーショントポロジー

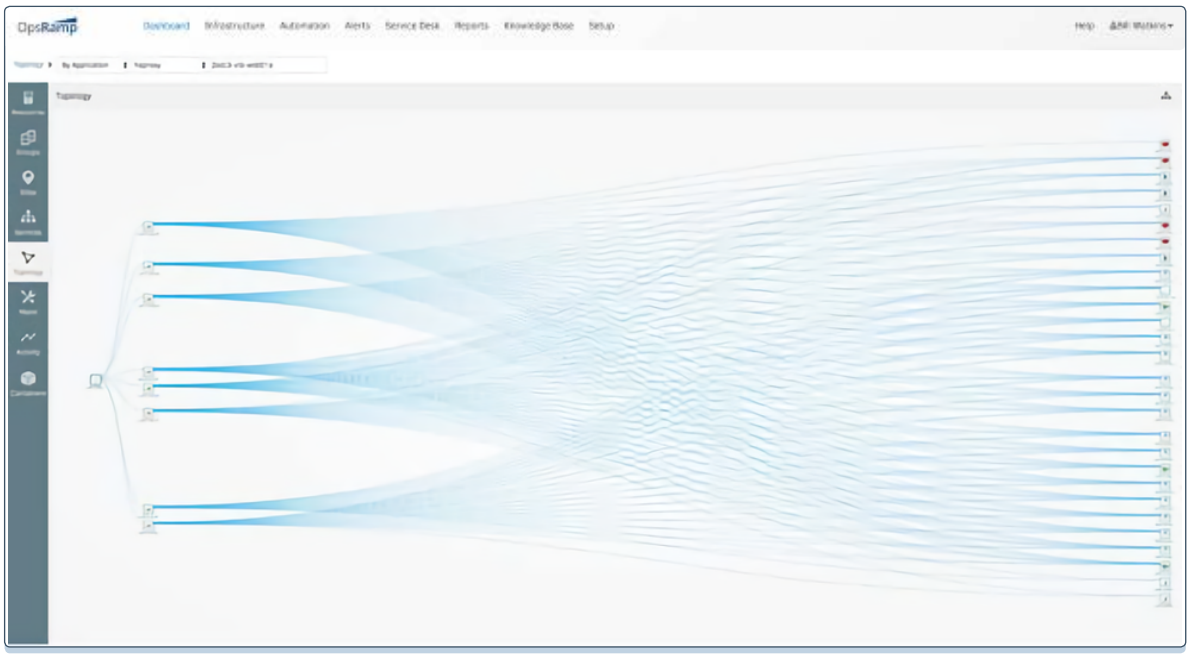


図9： OpsRamp の推論モデル

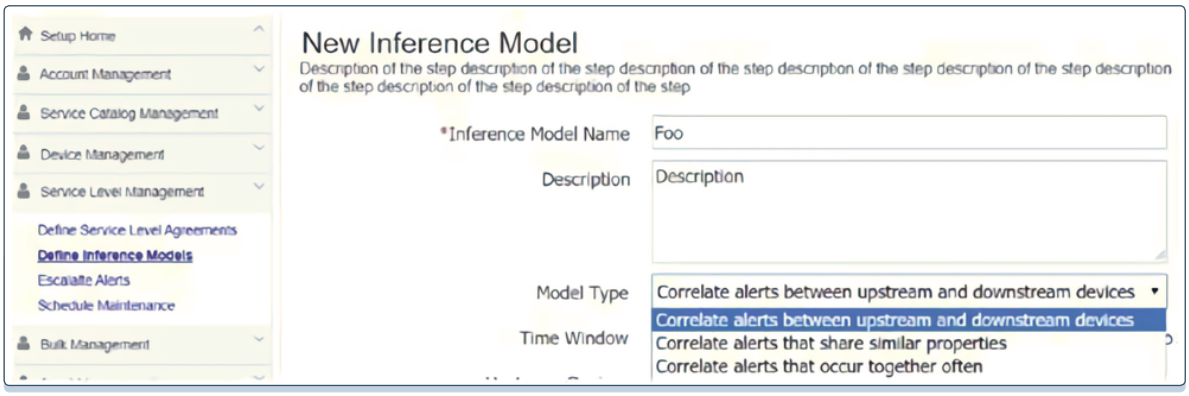
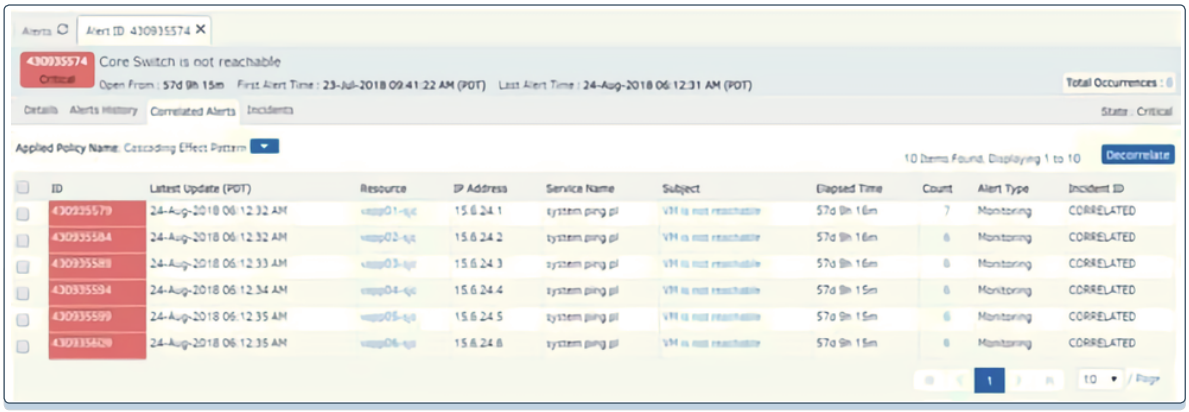


図10： OpsRamp における推論



第3章： 自動修復とエスカレーション

アラートのエスカレーションと障害対応は、アラート管理で一般的なタスクであり、人の手によって処理されることもよくあります。昔ながらのやり方では、初期対応者が根本原因のアラートを認識し（人の手による関連付けにより）、修復と対応完了のため、対象事項の専門家にそのアラートをエスカレートしていました。

OpsRamp では、シーケンスまたはポリシーによって障害修復を自動化することができます。自動修復できないアラートの場合は、OpsQ がアラートを適切なチームにエスカレートすることができます。

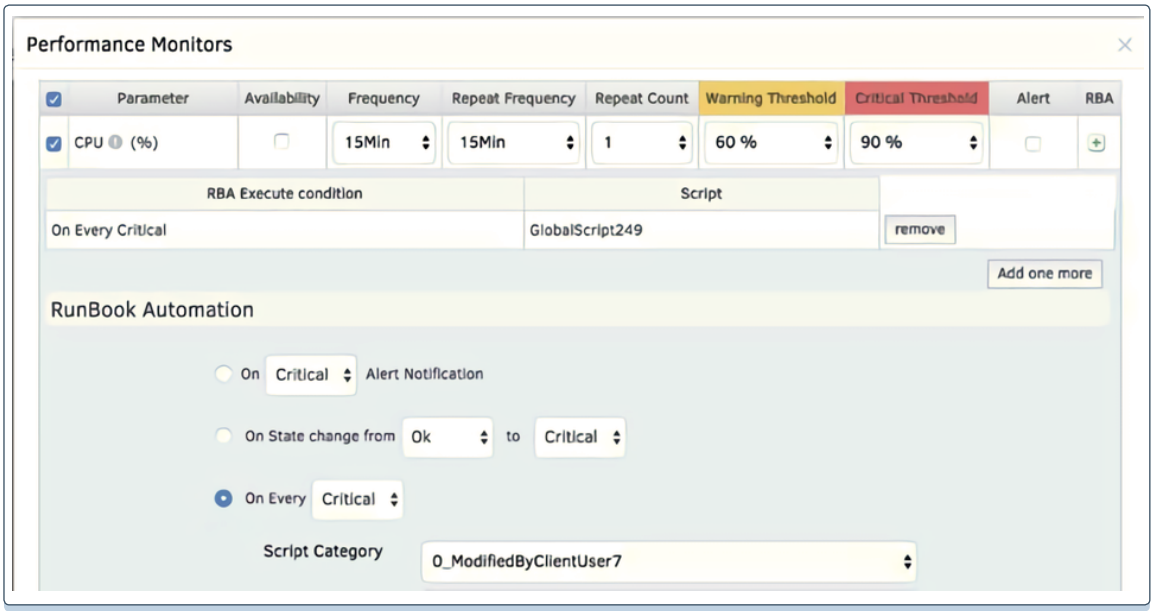
2つのユースケースはいずれも、受信アラートへの初期対応を自動化します。自動化することにより、人間のオペレーターがそのアラートに対して行うことを模倣することができます。

自動障害修復

個々のアラートは、最終的には解決されなければならない問題状況を表しています。十分に定義された一連のアクションによってインシデントに対処できる場合は、対応を自動化することができます。たとえば、主要なアプリケーションプロセス（Apache など）が動作を停止してサーバーが利用不可能になった場合、そのプロセスを再始動することが、サーバーを再び起動するための十分に定義された自動化可能なアクションとなりえます。

OpsQ は、アラートトリガー関するスクリプトを呼び出し、自動障害修復アクションを実行することができます。
図11 は、自動修復アクションの構成を示しています。

図11： OpsRamp の自動修復機能



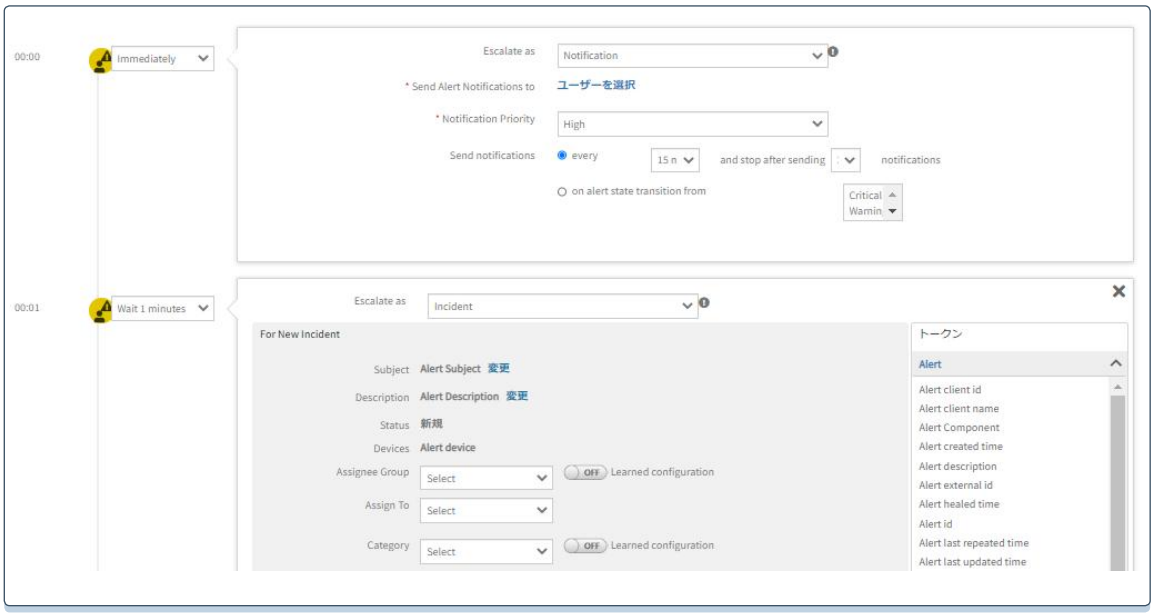
エスカレーションおよびインシデントのルーティング

自動修復できないアラートは、人による調査を必要とします。エスカレーションには、適切なユーザーにアラートを通知し、インシデントチケットを作成し、適切なユーザーにチケットをルーティングする必要があります。通知やルーティングの決定は、問題のデバイスやアラートによって決まります。

たとえば、業務上不可欠な IT サービスをサポートするデバイスに関するアラートの場合、アラート受信から 5分以内にレベル1のサポートスタッフに通知する必要があります。アラートがサーバーからのもので、特定のアプリケーションに関するものの場合、インシデントを作成し、それを該当するアプリケーションチームにルーティングする必要が生じます。

OpsQ は、アラートエスカレーションワークフローを自動作成し、通知とインシデント自動作成を行う初期対応のプログラムを支援します。図12 は、オンコール管理におけるアラートエスカレーションポリシーを示しています。

図12： OpsRamp のアラートエスカレーションポリシー



おわりに

さまざまなプラットフォームやマネジメントツールの導入に伴って IT オペレーション環境が複雑化するなか、自動化と AI の必要性はますます重要になるばかりです。サービス中心の AIOps は、インシデントによる事業の混乱を防ぎ、より迅速に修復するために、AI と機械学習を活用する最も効率的な手段です。OpsRamp OpsQ は、増え続けるイベントデータや性能データに対応するために構築された、インテリジェントなイベント管理、アラートの関連付け、修復を行うソリューションです。

OpsQ やサービス中心の AIOps について詳しくは、www.OpsRamp.com/solutions/service-centric-aiops をご覧ください。

OpsRamp

詳しくはこちら
https://pages.jbs.co.jp/opsramp_index.html