

Data Science Checklist for AIOps Applications



現代の IT システム運用では、サービス管理システムやツールセットのパフォーマンスを向上させるために、拡張インテリジェンス、機械学習、アナリティクスを導入するケースが増加しています。

これらの技術を、「いつ」、「どのように組み合わせるか」によって、**AIOps が、「障害管理」、「顧客体験」、「サービス保証プロセス」の改善にどれだけ効果をもたらすか？**が決まることになります。

次世代の AIOps アプリケーションが持つべき機能

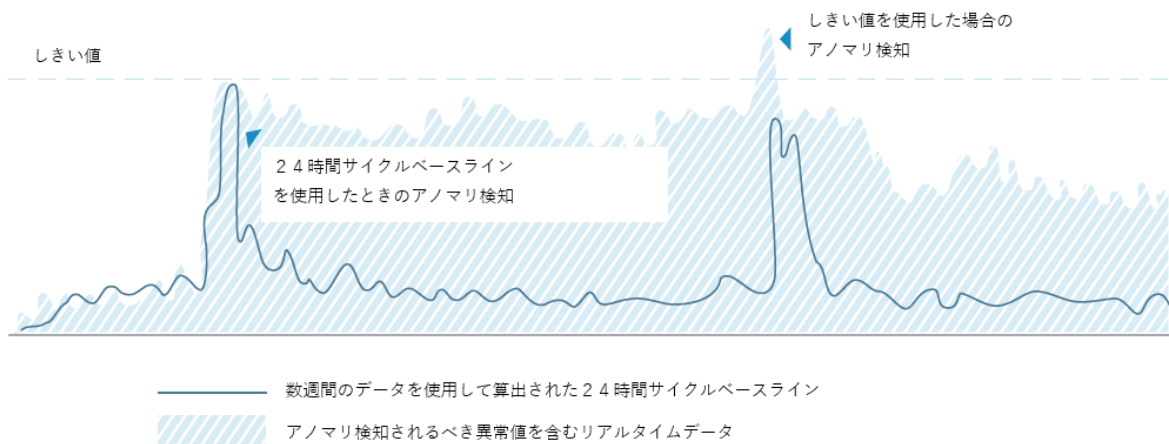
- 1 一日を詳細な時間間隔で分析をし、時間帯特有の変化、全体のトラフィック量の増減、許容範囲内の偏差などに対応可能な**先進的なアノマリ検知**
- 2 ノイズを減らしパフォーマンスの問題や障害を早急に見つける**確率モデル**
- 3 関連するイベントを見つけ、根本原因を定義するために、時間的に近いイベントを関連付けるだけの単純な方法に加えて実行される、**類似性分析**
- 4 現象と根本原因を区別するために、各ディメンジョンごとのメトリクスの重要度、エントロピー、離心率を使用した**推定根本原因**の特定
- 5 性能管理を最適化する**オントロジー推論**

本文書では、これらのデータサイエンスの効能について見ていき、それらがどのように、そしてなぜサービス管理に重要な影響を及ぼすかを解説します。

先進的なアノマリ検知

単純なしきい値を使用したアノマリ検知では、そのしきい値がユーザにより設定されたものであっても、統計値を使用したものであっても、ワークロードや通信量が急激に変化するために複雑化するネットワークや、現在のデータセンターでは十分に機能しません。ネットワーク使用のピーク時や、重いときに偽陽性を検出し、比較的穏やかな時間帯に真陽性を取り逃がしてしまうことがあります。そのため、別のより適したアノマリ検知手法が必要になります。ワークロードや使用率の通常の時間推移を継続的に学習し、そこから算出された期待値からの偏差値を使用した検知にすべきです。

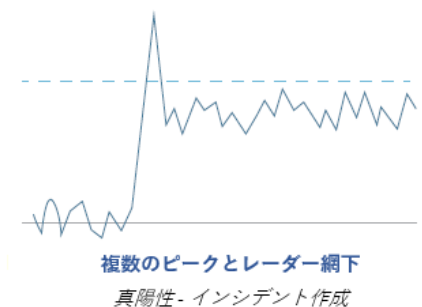
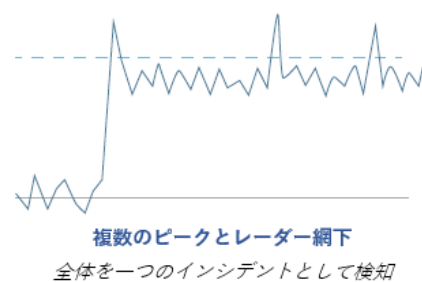
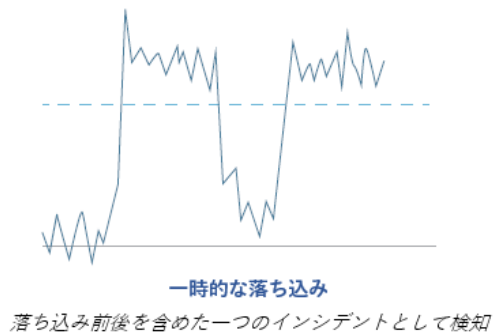
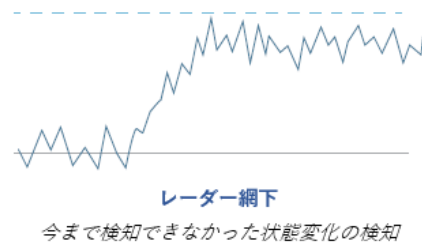
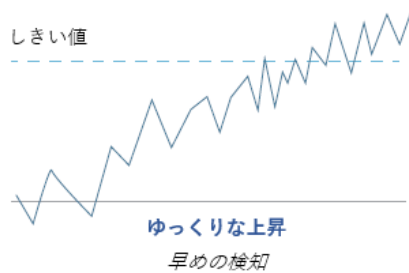
この先進的なアノマリ検知は、教師なし機械学習を採用しており、時間軸上で変化するメトリクスと属性のベースラインを学習データとしています。ベースラインはデータが取り込まれるときに学習され、より多くのデータが収集されるにつれてそれらは継続的に更新されます。学習したベースラインからの偏差によりアラートを発生させる方法は、より精密なアラート発生手段です。つまり、使用量の少ない期間に発生する重大な異常を検知すると同時に、ピーク期間に頻繁に発生する誤検知ノイズを削減します。



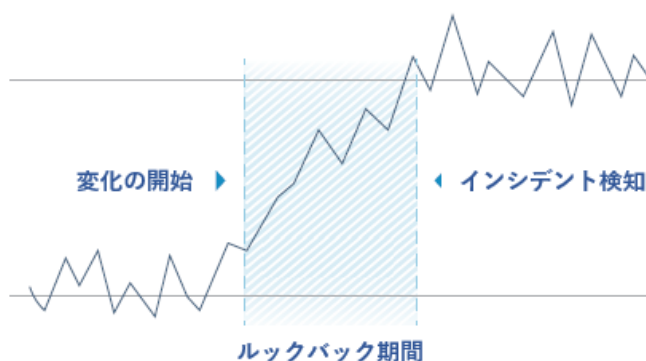
確率モデル

監視対象のさまざまなイベントおよびメトリクスから検知されるシグナル（異常）は、一時的な使用量の急増または統計計算によるノイズに起因する一過性のものであることがよくあります。このような一過性のシグナルは、必ずしも永続的な問題を示しているわけではありません。重要で、かつ一過性でないシグナルを特定することができれば、運用チームは本当に修正が必要な問題に集中でき、その結果、運用効率が向上します。

確率モデルは、シグナルとノイズを区別するのに優れています。そのため、ウォール街では、一見ランダムに見える市場動向のゆらぎや局所性をモデル化するのに広く使用され、市場の状況がいつ変化するかを予測しています。同様の理由で、これらのモデルはノイズの多いデータセンターや IT 運用の分野でも活用されています。確率モデルにより、すべてのメトリクスや、イベント、エンティティの動作を継続的に監視、評価し、非一過性、かつ対処が必要な「インシデント」を見つけることができます。確率モデルでは、他の手法では分類を誤ったり、発見が遅れたり、あるいは完全に見逃してしまうようなパターンを正しく検出することができます。



また、確率モデルでは、動的な「ルックバック」期間（前の期間を遡って検索する機能）を使用して、システムが最初に有害な変化を示した時点を持定することもできます。この「ルックバック」期間を使用することで、多くの障害・パフォーマンス管理システムより早く「インシデント」を持定することができます。「ルックバック」期間により、変化がゆっくりでサービスへの影響が現れるまでに時間がかかるような事象「スローライザー」も検知することが可能です。

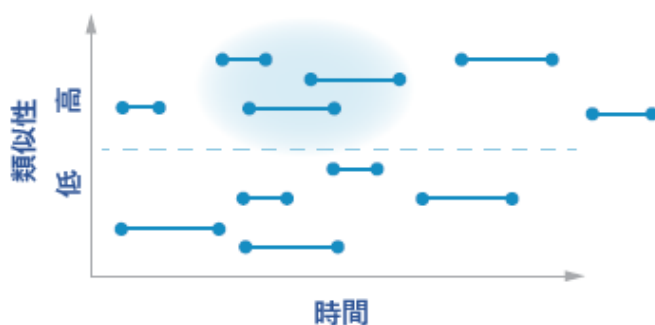


変化を検知した時点で動的に作成される「ルックバック」期間により、問題発生 of 正確な時間を特定し、サービス品質の低下と適切に関連付けることができます。

類似性 – 時刻による関連付けを改善する方法

既存の障害/パフォーマンス管理システムは同じ時間帯に発生した異常シグナルをグループ化しています。しかし、システムコンポーネントや属性値（特徴）の類似性に基づいて分析し、グループ化することはできません。VIA AIOps は、Jaccard 類似性係数などの統計的に厳密な類似性指標と、シグナル間の類似性スコアに基づいてグループ化を行います。この方法と時間的相関とを組み合わせることで、異常が関連しているかどうか、異常をグループ化すべきか、または別々に扱うべきかをより適切に判断することができます。時間的相関に類似性分析をプラスすることにより、根本原因を持定するための分析が強化されます。

これは、障害やパフォーマンスの問題により、複数の異なるレイヤーで複数のアラームが発生するような場合に特に重要です。このような場合に類似性分析を使用すると、シグナルをグループ化して単一のインシデントとし、1枚のチケットに集約することができます。サイロ化されて運用されているサービスレイヤーを横断して障害やパフォーマンスを管理することで、運用効率とサービスアシュアランスが大幅に向上します。



図のように、グルーピングは時間上の重なりと類似性により決まります。

推定根本原因（Probable Cause）

推定根本原因の分析にはいくつかのアルゴリズムが使用されます。最も優れたアルゴリズムの一つは、重要度（Severity）、離心率（Eccentricity）、エントロピー（Entropy）の組み合わせに基づくランキングスコアを使用するものです。

重要度：システムコンポーネントや要素がインシデントにより受ける悪影響の度合いを表す指標。

離心率：インシデントによる影響の不均衡度を表す指標で、あるインシデントによる特定コンポーネントへの影響度と、別のコンポーネントへの影響度を比較することにより計算されます。

エントロピー：システム（またはコンポーネント）の無秩序さを表す指標であり、完全に動作しているシステムのエントロピーは 0 に近く、機能不全のシステム（またはコンポーネント）は高いエントロピーを持ちます。エントロピーは、イベントの希少性に直接関係しています。障害が発生している状態は、障害が発生していない状態よりも稀です。重大度の高い障害はさらに稀であるため、エントロピーも高くなります。

重要度と離心率の両方が高いコンポーネント、つまり、他のコンポーネントと比較して障害やパフォーマンスの問題の影響を最も受けるコンポーネントは、エントロピーが最も高くなります。実際には、エントロピーは、重要度と離心率およびその他の主要な指標から算出されます。エントロピーの高いコンポーネントは、根本原因を特定する上で非常に高い診断的価値を持っています。

典型的なユースケース

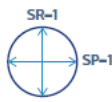
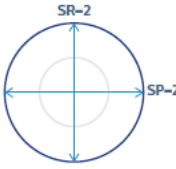
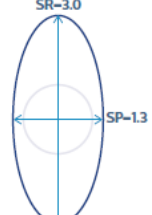
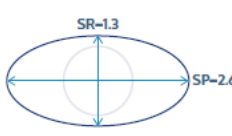
推定根本原因を決定する際に重要度、離心率、エントロピーが果たす役割をよりよく理解するために、典型的な使用例を考えてみましょう。

ストリーミングビデオサービスの加入者の例で考えてみましょう。あるコンテンツを視聴しようとして、ストリーミングデバイス（Apple TV、Roku、Chromecast など）を使用してビデオサービスに接続しようとしたときに、多くのユーザが「認証エラー」になりました。この問題はシステムのどの場所でも発生する可能性があります。ユーザデバイスからデータセンターの認証サーバーまでの間、認証サービスの前にあるネットワークやロードバランサーなど、すべてのコンポーネントで発生する可能性があります。根本原因を正しく診断するためには、ユーザデバイスから認証サービスまでのトポロジにおけるすべてのコンポーネントを分析する必要があります。

これらのコンポーネントの多くは、根本的な障害の影響を受けているため、さまざまな重要度の異常な動作を示している可能性があります。推定根本原因を特定するには、それら異常を示しているコンポーネントからのアラームやメトリクスデータを、コンポーネントを特徴付ける属性（ディメンジョン）を含め、非常に細かいレベルで分析する必要があります。例えば、ユーザデバイスは、モデルやファームウェアなどの特徴

(ディメンジョン) に分類されて分析されます。すべてのモデルとファームウェアで同じ重要度の認証エラーを示している場合、問題はユーザデバイス以外の場所で発生している可能性があります。なぜなら、ユーザデバイスで問題が発生している場合、すべてのモデルとファームウェアで同時にエラーになる可能性は非常に稀だからです。逆に、特定のモデルやファームウェアで他のデバイスよりも著しく深刻な（重要度の高い）障害が発生している場合、それらは推定根本原因の候補となります。実際の原因ではない場合でも、最も深刻な影響を受けているコンポーネントは、実際の原因へ導く重要な症状である可能性があります。いずれにしても、推定根本原因であれ、重要な症状（Key Symptom）であれ、深刻な影響を受けているコンポーネントには、高い診断価値があります。

上記の例や、重要度、離心率、エントロピー、診断的価値の関係は、幾何学的に説明することが可能です。ここでは、ビデオストリーミングの問題が Roku デバイスに関連しているか、他の場所にあるかの検討を例として取り上げます。

シナリオ	原因
Roku デバイスとその他 (Apple TV、Chrome 等) の通常の状態。 1 は通常状態を表します。 	Roku の重要度 (SR) = 1 他のデバイスの重要度 (SP) = 1 離心率 = 1 エントロピー ≈ 0
Roku とその他のデバイスが重要度 2 の状態 	Roku の重要度 (SR) = 2 他のデバイスの重要度 (SP) = 2 離心率 = 1 エントロピー $\approx$ 低 診断的価値 = 低 プロバブルコース = 可能性低 Roku 自体がプロバブルコースである可能性は低い。その他のデバイスが受けているのと同じ原因による影響を受けている可能性が高い
Roku が他のデバイスより不釣り合いに大きくインシデントからの影響を受けている 	Roku の重要度 (SR) = 3.0 他のデバイスの重要度 (SP) = 1.3 離心率 = 2.3 エントロピー $\approx$ 高 診断的価値 = 高 プロバブルコース = 可能性高 重要度と離心率の両方が高く、Roku がプロバブルコースであるか、分析上重要な現象である可能性が高い
Roku が他のデバイスよりインシデントから受ける影響が小さい 	Roku の重要度 (SR) = 1.3 他のデバイスの重要度 (SP) = 2.6 離心率 = 0.5 エントロピー $\approx$ 中 診断的価値 = 中 プロバブルコース = 可能性低 中程度の重要度で、かつ中より低い離心率であることから、Roku はプロバブルコースではないが、診断的価値のある現象である可能性はある。

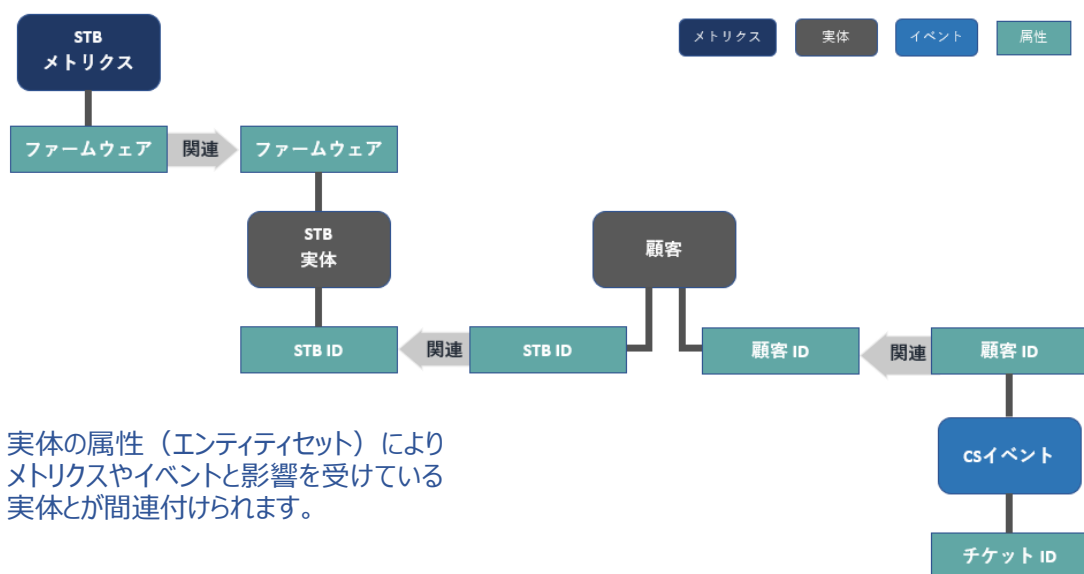
オントロジー推論

システムとは、すべてのシステムコンポーネントと監視対象のエンティティ、および監視に使用される指標値、イベント、インシデントなどの成果物の組み合わせであると定義します。エンティティには、デバイスや特定の顧客が含まれることもあります。

システムのオントロジーとは、デバイス、インフラ、顧客、その他すべてのシステムコンポーネントやエンティティ間の論理的、トポロジ的、物理的な特性に関する情報です。拡張知能や機械学習により、システムのオントロジーを自動的に検出することができます。オントロジーは、より深くリッチなメタデータを提供し、システムやサブシステム間の自動分析と診断を加速します。オントロジーは、前述の類似性分析で使用され、コンポーネントやサービスレイヤー間のインシデントのグループ化をサポートします。また、影響を評価したり、パフォーマンス関連の問題を深く理解するためにも使用されます。

前述のビデオストリーミングの例では、オントロジー推論を使用することで、問題の範囲、影響を受ける人の範囲、影響によるコストを判断しています。

オントロジー推論の影響定義



ファームウェア X は、118,733 台のクライアント機器に影響を与えています。

これは、全クライアント機器の 0.427%にあたります。

これにより、118,733 台（0.213%）のお客様が影響を受けています。

1,598 人のお客様は、最近何かしらのサービスの問題による影響を受けました。

117,135 人のお客様は問題なくサービスを利用しています。

サービスに影響を与える問題への推定対応コスト：\$14,382。

影響を受ける可能性のある 118,733 人のお客様にかかる潜在コスト：\$1,068,597。

結論

次世代の AIOps アプリケーションを検討する際には、データサイエンスが明確な差別化要因となります。データサイエンスがどのように活用されるかによって、次の点に違いが現れます。

どのようなプロセスやユースケースを
最適化できるか。

根本原因を見つけ、サービスを提供する
全ての技術要素から、
症状と原因とを分別する能力

レスポンスだけでなく
解決を早めるために提供される
洞察力

パフォーマンスの問題や障害を
検知するスピード

AIOps アプリケーションを導入する際は、この文章で取り上げた点を考慮し、
最終的な判断をすることをお勧めします。

VIA AIOps について

VIA AIOps は、サービス提供に関わるすべてのレイヤーにインテリジェントな自動化を実現し、顧客体験の向上とオペレーションの最適化をもたらす、次世代の AIOps です。

VIA AIOps は、統合的なエコシステムのオブザーバビリティを提供し、自動化に対する信頼性を高める説明的な AI を提供します。

VIA AIOps は、「ノイズの低減」、「相関関係」、「サイロを越えたインテリジェントな自動化」を実現し、より迅速な問題の検出、緩和措置、解決を可能とします。それにより顧客体験の向上と運用コストの削減が実現できます。

