要旨

１．背景

すべての企業がビジネスに IT を利用していると言っても過言ではない昨今、IT は様々なビジネスシーンで使用されている。障害による IT システムの停止は、ビジネス機会に大きな影響を及ぼし、対応する運用担当者にも大きな業務負荷を与えている。IT システムが変化しているにも関わらず、障害対応は変化せず障害発生後に対応する企業がほとんどである。しかしながら、事が起きてからでの対応では対処に時間が掛かり、対応完了後の関係部署への報告や是正処置にも工数が掛かっている。その結果、運用担当者が本来成すべき業務への時間が確保されない状況である。

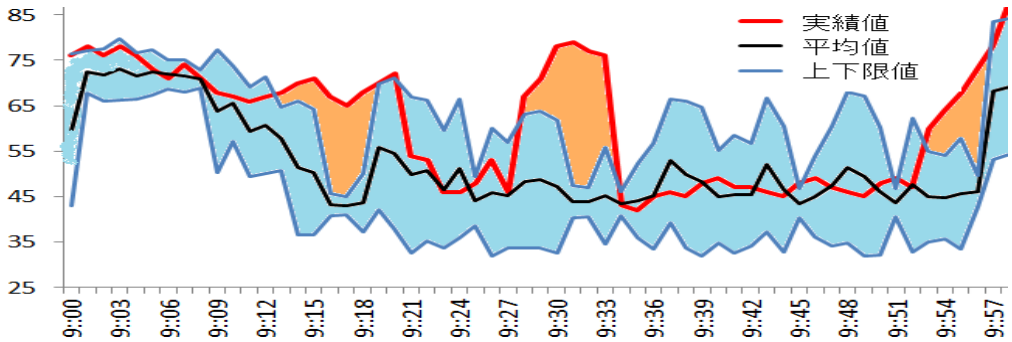
この運用担当者が抱える障害対応の負荷軽減のために、オートメーション化を通じて「障害を予兆し、未然に対処する」プロアクティブな運用管理を本研究で提案する。

２．研究内容

現状の運用では、閾値越えの監視や異常が発生時に如何に早く復旧させるかといった監視が殆どである。私たちは、『閾値は超えないがいつもと異なる状態を検知』し、事が起きる前に障害につながる可能性について分析するスタイルへと変えていく、そんな自動化を目指し、『**外れ値による障害予兆の検知自動化**』を実際に仕組みとして構築し有効性について検証を進めた。

【外れ値】各種リソースの時系列毎の実績値を基にした**平均値**と、許容範囲となる**上下限値**を算出し、ある日の実績値がこの上下限値から外れた値と定義

【上下限値】過去実績から標準偏差を算出し平均値±標準偏差×2 で求めた許容値と定義
±標準偏差×2 は統計的に 95%を網羅。外れた残り 5%を外れ値と設定



（１）構築を進めるうえでの前提条件

① コストを掛けない　※数百～数千万掛ければ実現するツールはあるが非現実的
② 既存の運用を最大限活用　※データレイアウトの違いを意識せず吸収する仕組み
③ 外れ値検知の基となる各リソースの上下限値を実績データから自動更新する
④ 外れ値を検出した際に自動通知させたい

（２）検知対象データの選定

普段から実績を記録し監視対象としているリソースデータを中心に、ディスク、メモリ、CPU、画面レスポンスやクリティカル業務の開始終了時刻・処理時間を対象とした。

要旨

３．実現方法

embulk と G Suite を用い、前提条件の 4 項目すべてを満たす自動化システムを構築。

embulk：入出力・フィルタープラグインを活用し、異形式のデータを自動収集ならびに統一レイアウトへ変換し、G Suite の Spreadsheet に出力

G Suite：自動スケジュールで script を実行し、日次のグラフ生成、外れ値検出、異常時メールを送信。過去 3 ヶ月の実績データから上下限値の自動更新を実現

４．検証結果

今回は CPU 使用量データで検証を実施し、『閾値は超えないがいつもと異なる状態を検知』する自動化検証が行えた。但し、画一的な検知は難しく企業やシステム毎のリソース特性を分析し個々にチューニングが必要であることが分かった。これを踏まえ、“上下限値算出時の係数”と“外れ値検知条件(*1)”をパラメータ化し実用性を高めている。

*1 瞬間的な高負荷が許容できるリソースは、外れ値が複数回続いたとき外れ値として検知

検証結果から見えた課題

外れ値検知の信頼度向上のために標準偏差算出時に除外したい異常値を指定できるとよい。

５．考察

これまで見ていなかった外れ値を知ることで、日々の運用の変化に気付き未然に対処するプロアクティブな運用管理へパラダイムシフトしていけるものと考える。反面、検出した事象を基に複数のデータから相関的に真の原因を分析する必要がある。そのためには普段から運用の変更管理の記録化や、収集しておくべきデータの整備が不可欠である。

本研究での仕組みを利用することで、相関的な分析に必要となるデータを自動的に収集・整理することができ、分析のための時間、延いては新しい取り組みへの時間の確保につながると考え、これを成果と捉えている。

以　上