監視サービスの運用高度化に向けた新たなアプローチ

富士通エフ・アイ・ピー(株)

■ 執筆者Ｐｒｏｆｉｌｅ ■

渡邊　豪

2006 年　富士通エフ・アイ・ピー（株）入社
　　アウトソーシングサービス部所属
　　アウトソーシング支援業務担当
2007 年　第 5 カスタマサービス部所属
　　アウトソーシング運用業務担当
2016 年　現在 センター基盤開発部所属
　　ITSM ツール開発担当

■ 論文要旨 ■

当社データセンターを利用するアウトソーシングユーザーに対し、国内データセンター事業者では最大規模となる共用型監視サービス（PowerMSP）を提供している。ユーザー数は非常に多く（684 社、18,095 台、2016 年 9 月現在）、発生するアラームは月間 82 万件近くに達し、これをオペレーターが 24 時間 365 日体制で対応を行っている。アラームを的確かつ迅速に対処することが要求される中、アラーム件数が増加し続けており、オペレーターや SE の負荷増大、要員追加によるコスト増のリスクが生じている。本論文では、従来までのフィルタリングのアプローチを見直し、発生メッセージをパターン化・モデル化する技術を開発し、対処不要アラームを自動抽出する取り組みについて論述する。本技術は当社ノウハウに富士通研究所の分析技術を融合させた、新たなアプローチで実現しており、監視運用業務の効率化・負荷軽減に貢献出来ると考える。

■ 論文目次 ■

１．はじめに ……《 3》
１．１　監視サービス（PowerMSP）の概要
１．２　監視サービスを取り巻く環境
１．３　監視サービスの運用状況
１．４　これまでの対策状況

２．問題の分析と課題 ……《 5》

３．対策立案と実施 ……《 6》
３．１　対策立案
３．２　具体的な取り組み

４．取り組みの効果 ……《 11》

５．今後の取り組み ……《 13》

■ 図表一覧 ■

図１　監視システム基盤／オペレーション基盤の全体図 ……《 3》
図２　オペレーター、現場SEの負荷発生箇所……《 4》
図３　現場SE／オペレーターが対処するアラームの内訳……《 5》
図４　対策１アプローチの新旧比較……《 6》
図５　対策２アプローチの新旧比較……《 7》
図６　対策３アプローチの新旧比較……《 7》
図７　共起分析のイメージ……《 8》
図８　ツールの試行結果……《 11》
図９　I社に適用した分析結果 ……《 12》

１．はじめに

１．１　監視サービス（PowerMSP）の概要

当社は富士通所有のデータセンターを核に、アウトソーシング事業を展開しており、ホスティングやハウジング、コロケーション契約の顧客システムに対して、共用型のPowerMSP 監視サービス（以下、PowerMSP）を 2003 年 10 月から提供している。2016 年 9 月時点で、データセンターユーザーの約 8 割にあたる 684 社、18,095 台のサーバを監視しており、国内データセンター事業者の提供するサービスとして最大級の規模となっている。

PowerMSP では、共通サービスであるメリット（共通基盤設備、共用要員体制）を活かしたコスト圧縮に加え、オペレーターによる 24 時間 365 日の確実な監視と、顧客担当 SE（以下、現場 SE）への迅速な障害通知により素早い復旧作業を実現し、顧客業務の継続性と影響度の極小化を図り、高いサービス品質を確保している。

１．２　監視サービスを取り巻く環境

データセンター市場は成熟期を迎えつつあり、競合状態は厳しさを増してきており、監視サービスを取り巻く環境も非常に厳しい状況にある。特に、ベンチャー企業による監視SaaS サービスや Zabbix、Hinemos などの OSS 監視ツールを活用して低価格を全面に出した競合の台頭により、更に競争が激化している。また、技術のコモディティ化により、単純な監視・通報サービスだけでは顧客からの値引き要請を強いられてしまう。

このような状況下で、更なる価格競争力強化を図るとともに、付加価値の高いサービス提供が急務となっている。

１．３　監視サービスの運用状況

PowerMSP を提供する基盤環境は大きく二つの環境に大別される。一つ目は、顧客システムの障害を検知する監視システム基盤環境と、二つ目は、そこで上がったアラームを対処するオペレーション基盤環境である。監視システム環境は、Systemwalker Centric Manager を利用した 10 台の統合監視サーバで構成されており、検知したアラームは約 5,000 行のフィルタリング定義によって自動削除され、フィルタリングを通ったアラームを 6 人 4 班の交代シフトで 24 時間 365 日体制を取るオペレーターにより、電話連絡や定型処理などのオペレーションが行われる。（図１）

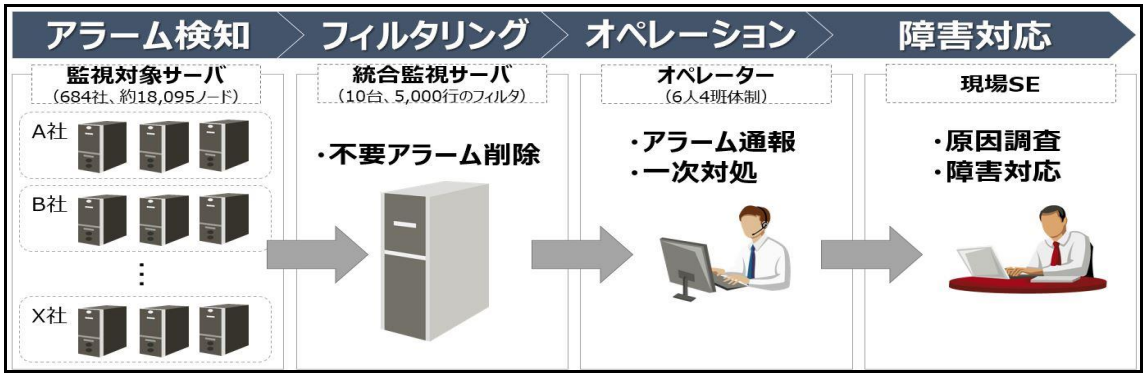

図１　監視システム基盤／オペレーション基盤の全体図

加えて、2012 年には IT サービスマネジメント（以下、ITSM）基盤を導入し、インシデントログを利用した対応履歴の記録や、オペレーション自動化ツールを利用したオペレーション自動化を図るなど、日々PowerMSP のサービス品質の向上や効率化に努めている。

このような状況の中、顧客システムから検知したアラーム件数が増加し続け、月間約 828,000 件にも達しており、オペレーターの目視確認の負荷が増大している。統合監視サーバにてフィルタされ出力されたアラーム約 32,000 件すべてに対し、オペレーターは目視確認を行っているため、アラーム増加に比例し本作業負荷も増加している。（図２）
仮に、1 アラームに対し 2 分（アラームの確認が 1 分、その他、Ping による死活確認や対応履歴の登録作業などで 1 分）の時間を要した場合、1,066 時間もの対応が必要となり、オペレーター6 人中 1.5 人が確認作業のみに費やされることとなる。

この結果、確認作業が膨大になり重要アラームの見落としやアラーム連絡の遅延、もしくはオペレーター増員によるコスト増といったリスクを抱えている。

更に、アラームを受け取り対処する SE も負荷が増大している。SE の勤務体系は平日日中帯だが、アラームはシステム稼働に重大な影響を及ぼしている可能性もあるため、連絡を 24 時間 365 日で受け取らなくてはならない。この件数は合計 2,700 件にも達し、１件ごとの確認で昼夜問わず 30 分以上の時間を要するため、大きな負荷となっている。（図２）
SE は平常時の運用マネジメントや新規提案活動も実施しているが、そちらに注力できないという問題が生じている。

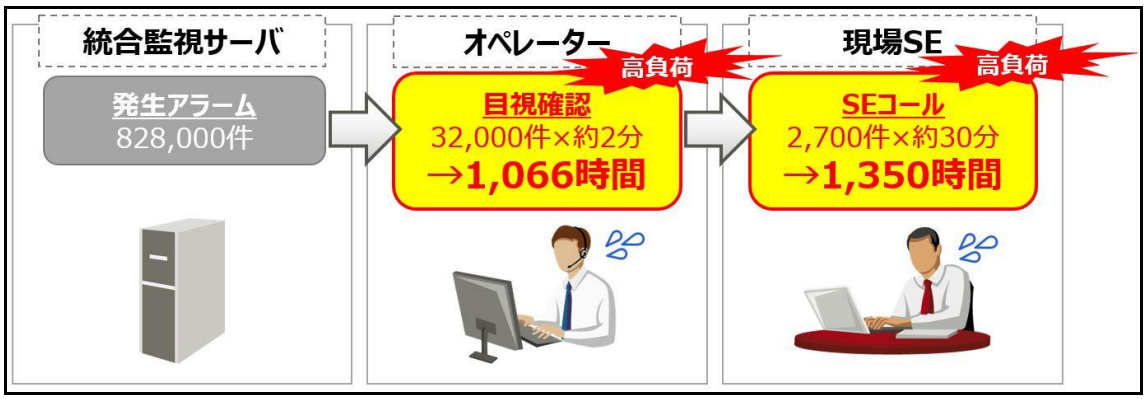

図２ オペレーター、現場 SE の負荷発生箇所

１．４　これまでの対策状況

このリスクに対し、これまでは現場 SE からの不要アラーム無視指示申請に対し、申請書の台帳化や一元管理するツールを作成するなど、目視確認作業の効率化を図ってきた。また、2010 年から SE コール（オペレーターから現場 SE への架電通報）削減に向けた WG 活動を行い、対処不要なアラームの検討を実施し、フィルタリング対応を継続的に推進してきた。

また、SE の負荷軽減策として電話コールのローテーションを徹底させ、特定担当者にアラーム連絡が集中しないよう、負荷軽減を図った。

これらの改善活動は一定の効果を上げており、2013 年度は約 20%の SE コール削減を達成した。だが、近年のアラーム増加ペースが改善割合を上回っており、2014 年度の削減率は 1%程度に落ち込んでおり、効果は鈍化傾向にある。このままの状況が続けば、PowerMSP の

サービス品質確保ができず、顧客に対して高品質なサービス提供が困難となるリスクがあるため、対応が急務となっている。

２．問題の分析と課題

アラームが大量発生し、オペレーター/SE の負荷が増大している根本となる問題点は何なのか。684 社のユーザーを担当している各現場 SE へのヒアリング、及び発生したアラームのインシデントログを詳細調査した結果、以下 3 点が問題であることが判明した。

【問題１】目視確認が不要なアラームが多い（オペレーターの負荷増大）

オペレーターが目視確認を行うアラーム件数は月間 32,000 件にもなるが、一方で、サーバ再起動などの一次対処や SE コールを行ったアラーム数は 3,900 件（一次対処 1,200 件、SE コール 2,700 件）であった。（図３左側）　つまり、オペレーターは全体の 87.8%に当たる、毎月 28,100 件もの対処不要なアラームに対し、目視確認を実施していることになる。

【問題２】現場 SE のフィルタリングが進まない（オペレーターの負荷増大）

フィルタリング判断にはシステム全容の把握、アラーム内容・発生パターンの特定、顧客説明など非常に時間を要する。加えて現場 SE は日常的に発生する SE コール対応以外にも、日々の提案活動や運用改善も行う必要があり、フィルタリング対応まで手が回らない状況となっていた。PowerMSP では年間 60～70 社ペースで顧客が増加していることから、現状の人手に依存したやり方だけでは限界があり、新たなアプローチが必須である。

【問題３】現場 SE が対応不要なアラームが多い（SE の負荷増大）

オペレーターが SE コールを行った 2,700 件のアラームのうち、現場 SE が具体的な対処（ログ調査、故障部品交換など）に踏み込んでいたものは、わずか 40%（1,100 件）程度であった。（図３右側）　残りの 60%のアラームについては、顧客や他社ベンダーへ対応依頼を行うのみで、現場 SE は何も対処を実施していなかった。対応不要なアラームも、現場 SE が連絡を受け取っているのである。

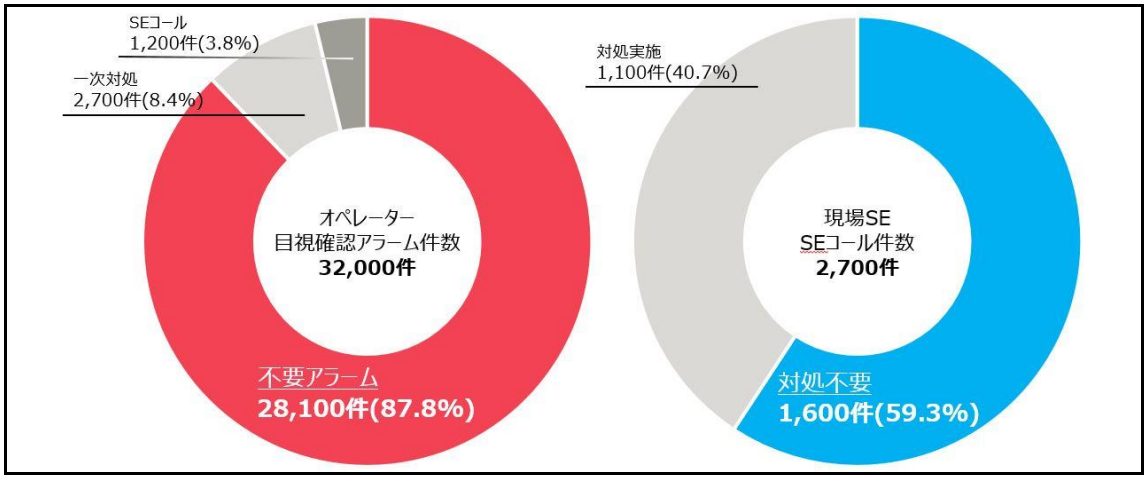

図３　現場 SE／オペレーターが対処するアラームの内訳

これら三つの問題に対し、以下の課題を設定し、状況の改善を図ることとした。

【課題１：アラーム目視作業負荷の軽減】
オペレーターが対処不要なアラームを削減し、目視作業負荷を軽減する
【課題２：フィルタリング判断の軽減】
現場 SE によるフィルタリング判断を軽減する
【課題３：アラーム対応負荷の軽減】
現場 SE が対処不要なアラームを SE コール対象から外し、現場 SE の対応負荷を軽減する

３．対策立案と実施

３．１　対策立案

これまでオペレーターが対処不要なアラームを削減するにはフィルタリングを行なうことで対応してきたが、現場 SE の作業負荷が高まっている現状を踏まえると、これ以上の改善効果は期待できない。そこで課題に対する着眼点を変えることで、現場 SE に依存しないアプローチが実現出来ると考え、二つの方式を立案した。

【対策１：アラーム集約】
対処不要アラームをフィルタリングして削減するのではなく、アラームを集約して目視確認するアラーム件数を削減させる。（図４）

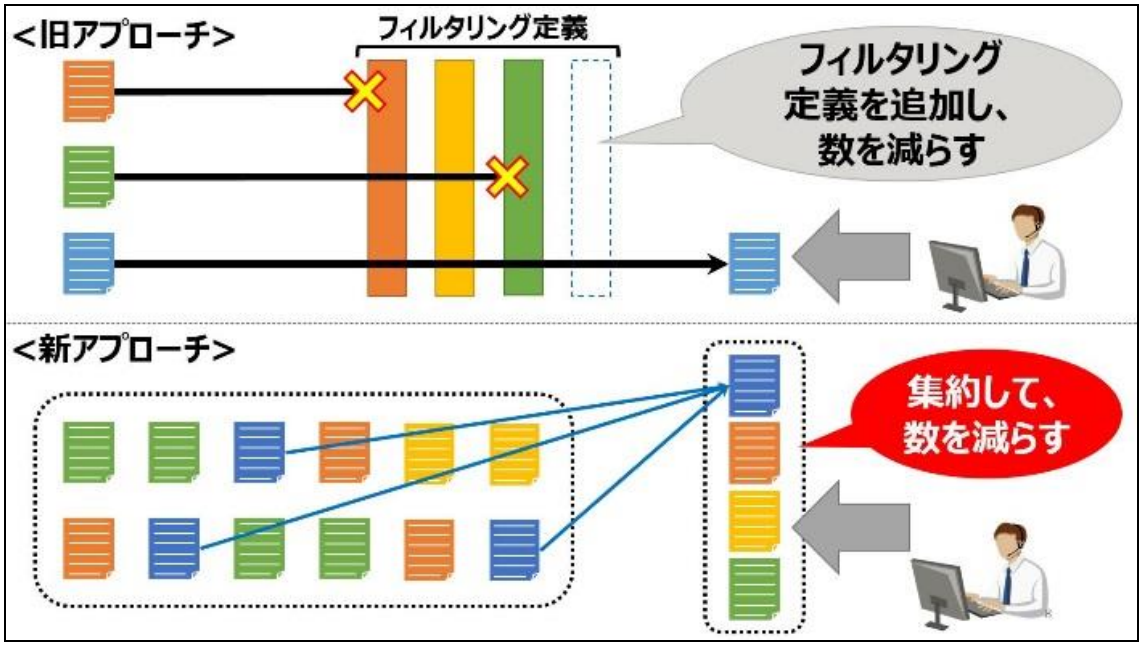

図４　対策１アプローチの新旧比較

【対策２：インシデントログ利活用】
現場 SE がアラームログ（メッセージ）を見てフィルタリング可否を判断するのではなく、インシデントログからフィルタリング候補を自動抽出し、現場 SE の確認件数を激減させる。（図５）

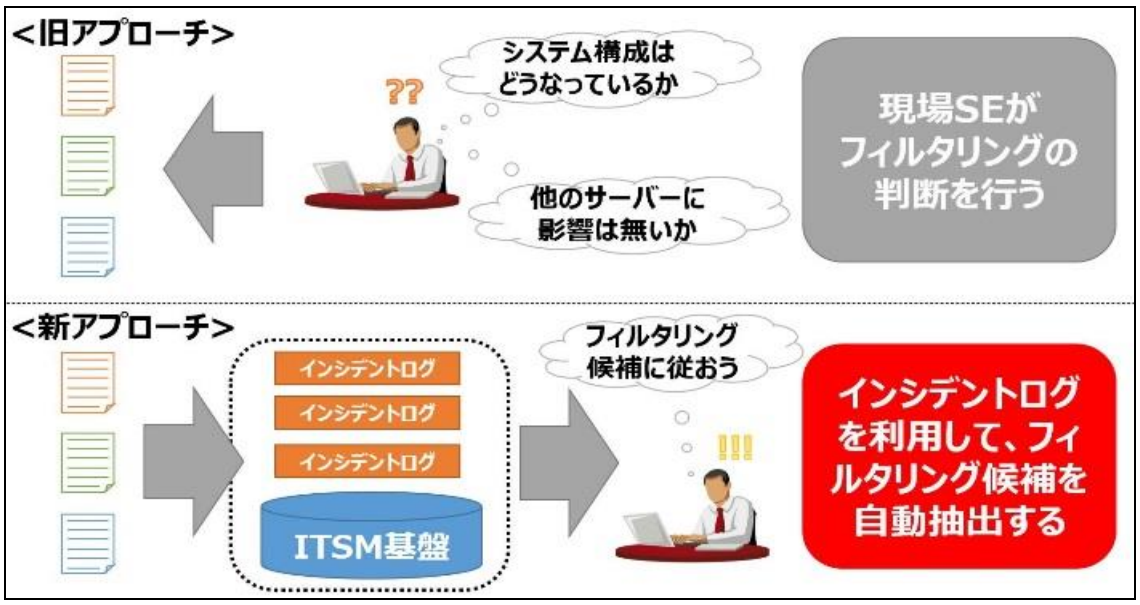

図５　対策２アプローチの新旧比較

また、従来 SE コールでは、オペレーターがメッセージ内容を確認し、現場 SE が予め作成した「切り分け表」と照らし合わせて誰に通報するかを決定する。だが、弊社が運用を行うシステムは、構成、利用するミドルウェアが多岐に渡り、無数の組み合わせから生じるアラームは多種多様であるため、「切り分け表」ですべてのアラームメッセージを網羅することは不可能である。

そこで、こちらも現場 SE の事前情報に依存しない対応を進めることとした。

【対策３：アラームログ自動判別】

現場 SE の事前定義情報と比較するのではなく、システム側でアラームログの内容を自動判別し、SE コール必要有無を判断する。（図６）

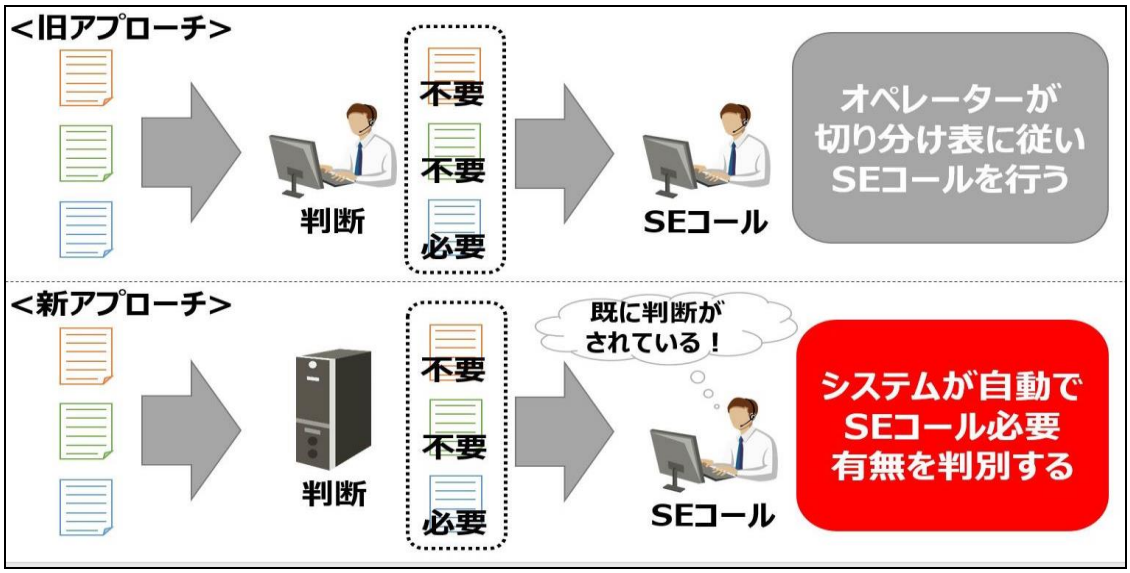

図６　対策３アプローチの新旧比較

上記三つのアプローチにより、オペレーターの作業負荷と、現場 SE の判断・対応負荷を軽減させる方針とした。

問題解決に当たっては、障害時の通報スピードアップや迅速な復旧などサービス品質向上を最優先事項と捉え、【課題１】から対処することとし、次に【課題２】【課題３】を解決することで、対象不要アラームの削減と効率的なフィルタリングという好循環のシナジー効果を実現する。

３．２　具体的な取り組み

【対策１：アラーム集約】の取り組み

これまで発生したアラームを詳細分析すると特定パターンでアラームが発生しているケースが多いことが分かった。例えば、Windows や Linux などの OS 再起動では決まったメッセージが連続で発生する。Web－AP－DB に代表される 3 階層モデルのシステムでは、DB サーバの負荷が上がり処理性能が低下すると、AP サーバのキューが溜まりプロセス数が増加するなど、相関関係のあるアラームが発生する傾向がある。これら、単一または複数ホストでの事象を捉えることでアラームを集約可能と判断し、ツール化に取り掛かった。

実施に当たっては富士通研究所と連携し、共起分析技術を用いて、スピード感を持って対応することとした。

【共起分析技術とは】

富士通研究所が保有する共起分析技術とは、発生したアラーム内のメッセージ（単語）と発生時間を元に、アラーム間の出現パターンを自動抽出する分析技術である。重複やパターン化されているメッセージは、法則性（例えば、1 分以内に同様のメッセージが 100 件発生や、A というメッセージの後に必ず B、C、D というメッセージが発生する、など）を持つので、複数メッセージからこれらのパターンを洗い出し、関連性を判断する。（図７）

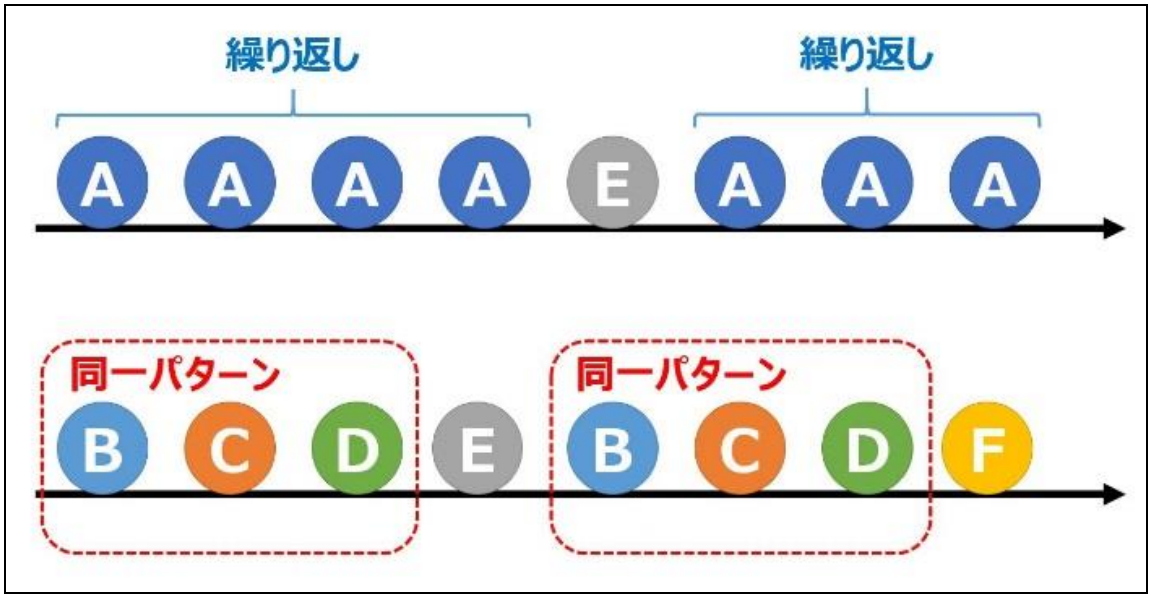

図７　共起分析のイメージ

PowerMSP では、684 社の全ユーザーのアラーム情報を一元管理して保存しているため、研究所の共起分析エンジンをそのまま利用してしまうと、他社の情報まで分析対象となり、アラーム集約結果の精度が低下してしまう。一方で、アラーム情報をユーザー単位に分割し分析することも可能だが、事前の分析加工処理に最低でも 3.5 時間を要すため非効率である。そこでアラーム内に含まれる、ユーザー固有識別子（PowerMSP ユーザーコード）が記録されているフィールドを活用し、ユーザーごとに分析領域を分けることにした。更に、OS が固定文字として出力するタイムスタンプやプロセス ID 以外の、分析に有効な可変情報だけを対象とするように改善した。この結果、アラームの単独発生パターンや複数ホストに跨るパターンを瞬時に（平均 10 分）自動抽出した。

実際のアラーム内のメッセージでは、同じ事象を表していても、ユーザー名や使用率などの数値が異なる場合もあるため、これらも同一のメッセージとして判別する必要がある。そこで、これら「ゆらぎ」要素も考慮し、ツール抽出精度を向上させた。
一般的にこのようなツールは、分析条件などを事前設定する必要があるが、本ツールはこれらが不要である。そのため、操作する人のスキルに依存せず容易に分析が可能となり、また分析結果の品質が均一化される。

加えて、現場 SE が実施結果を手軽に判別出来るよう、Excel ツール化を行い、レポーティング機能も実装した。レポーティングでは、個々のパターン結果を出力するほかに、総アラーム数に対する期待削減効果も数値化／見える化しアラーム集約の設定作業を促すことで、オペレーターの負荷改善の早期化を図った。

【対策２：インシデントログ利活用】の取り組み

これまで当社の ITSM 基盤は、オペレーターや現場 SE の運用プロセスとして定着しており、障害通知漏れの防止や対応遅延の早期発見に役立っている。
この ITSM で管理する情報には、アラーム内容やそれに紐づく対処履歴、各種構成情報（CI）が存在するため、これらを活かすことで解決するのではないかと考え、以下のような取り組みを実施した。

(1) オペレーターの判断が不要となる情報の抽出

ITSM の各管理項目の詳細を調査していくと、「対応欄」という項目に、”オペレーターが誰に連絡し、現場 SE がどのような復旧作業を行ったか”、という情報があり、対応のエビデンスとして活用されている。この欄はフリーフォーマットであるが、オペレーターは記入作業を効率化するため表記が統一されており、詳細情報と併せて「対処不要」「対処済み」といった４つの対処状況サマリーも記載されていた。

当社では、現場 SE へ障害通知をした際、電話越しに対処不要として指示を受けた場合、オペレーターは「対処不要」と記載するルールになっている。そこで、この情報を使うことで、現場 SE のフィルタリング可否判断の代替と成り得ると捉えた。

(2) 判断支援となる情報の抽出

また、「発生日時」「対応完了日時」という項目があり、それぞれ、アラーム発生時刻、アラーム対処時刻を記載しているため、「対処完了日時」から「発生日時」を引くことで、アラーム対処に要した時間が把握出来る。

通常、オペレーターが現場SEへ障害通知した場合、アラーム内容の説明で平均3分、現場SEが対処内容を記録するのに、平均2分を要する。このため、アラーム対処に要した時間が 5 分前後の場合は、全く対処をしていないと間接的に判断出来る。この仮説を確認するため、月間アラーム件数の多い上位 10 社の現場 SE にヒアリングを掛けたところ、全員正しいとの回答であった。

上述の結果、ITSM 管理項目を上手く利活用することで、これまでの現場 SE に依存したフィルタリング判断を、（１）では判断レス化、（２）では判断を強力に支援することを可能とした。

更に、ITSM 内の構成情報も活用することで、フィルタリングが十分に設定され、アラーム件数の少ない顧客システムをリファレンスモデル化し、類似構成のシステムへ横展開することで、PowerMSP 全体の品質底上げ（対処不要アラームの更なる削減）にも役立てられると考えた。

このため、以下のような指標が類似している場合、類似構成と判断し、発生アラーム件数が少ない場合はアラームが多いシステムへのリファレンス例として適用出来るようにした。これは当社の 684 社のアカウントベースを保有しているからこそ実施可能であり、他社では真似できない独自性を持つ。

・サーバ台数（システム規模）
・監視種別ごとのアラーム数
・機種ごとのアラーム数

ここで開発した機能を、【対策 1】にて取り組んだ共起分析エンジンを用いたツールへ組込み、フィルタリングの統合分析ツールとしてブラッシュアップした。

【対策３：アラームログ自動判別】の取り組み

アラーム内容判別に向け、過去に発生した80万件超のアラームを確認し、発生元のプロダクトや発生の規則性など、特徴があるかを調査した。この結果、アラームは大きくインフラ関連(ハードウェア、OS)／アプリ関連(アプリケーション、Web/AP 基盤・DB などのミドルウェア)の2種類に分類されることが分かった。

この特徴を踏まえて各アラームの対応内容を見ると、現場SEが具体的な対処（障害復旧、原因調査）を行ったアラームは、インフラ関連が殆どであった。アプリ関連の場合は対処を行わず、顧客／ベンダーへ連絡し完了としていた。

これは、弊社アウトソーシングサービスの運用形態に起因している。システム開発において、顧客がアプリケーションを開発し、搭載する基盤についてはデータセンターへ委託するケースが殆どである。運用もこの分担と同様となっているため、現場SEの対応は殆どインフラ関連に該当する。

このことから、システム側で自動的にアラームメッセージをインフラ、非インフラに判別することができれば、現場SEへのSEコール判断に繋げられると判断した。

本ツールは【対策１】と同様、富士通研究所と協調し、アラームメッセージ中の「単語」「文脈」を元に判断するロジックを開発した。

本ロジックを利用する際、ベースとなる教師データ（人がアラームを事前に仕分けた結果）が必要となる。教師データを作成するには、アラーム調査～判断まで、1 件ごとで 5 分掛かるため、必要数が多いと本来の目的である現場 SE の負荷軽減に反し、負荷が高まってしまう。これを回避するため、教師データ数を変動させ、仕分け結果に大きく差異が出ない最適値を算出した。

この検証の際、教師データ数に比例して精度も高まるかと想定したが、実際は比例しなかった。更に調べていくと、教師データとして重要なのは、数量ではなくカバー範囲（多種多様な単語、文脈が含まれているか）ということである。

上記に合致した教師データを揃えるため、前述の共起分析ツールにて重複を排したメッセージ一覧を作成し、それに対して正解を付与し、教師データとして利用するようにした。これにより、従来 60%前後だった仕分け正解率が、80%近くまで向上した。

また、結果と併せて判断根拠（どの単語、文脈が判定に大きく影響したか）も表示し、利用者側が納得感を得られるようにした。

本ツールはフィルタリング統合分析ツールとは別の、アラーム仕分けツールとしてリリースし、利用を開始した。

４．取り組みの効果

フィルタリング統合分析ツールを、アラーム件数が多い上位 5 社へ試行し、実際のアラーム情報を分析した。この結果、最大で 79.8%、効果が低いものでも 41.6%のアラーム削減が可能であるという結果を得た。（図８）

ユーザ名	アラーム発生件数		削減率
	削減前	削減後	
A社	13,465	7,862	41.6%
B社	10,241	2,072	79.8%
C社	4,879	1,649	66.2%
D社	1,743	830	52.4%
E社	1,686	664	60.6%

図８　ツールの試行結果

また、従来現場 SE のフィルタリング判断に、数時間を要していたが、本ツールを利用することで、わずか 7 分で完了し、分析作業が大幅に向上した。更に、今まで数百行というアラーム情報からフィルタリング可否を判断しなければならなかったが、こちらも 30 行程度に集約され、現場 SE による判断が圧倒的に軽減された。

また、共起分析エンジンのみを利用した分析結果は、現場 SE のフィルタリング判断と比較し誤差が発生していたが、ITSM の情報と組み合わせたレポートでは、ほぼ 100%の確率まで上昇した。

これらの結果を元に、2016 年度から当社が運用を実施する受注済の I 社向けシステムに対し、実際の適用を行った。I 社は当社移行前からアラームが大量発生しており、フィルタリング未整備のまま当社にて運用を引き継ぐとアラーム対処に忙殺されることが予想されたため、対策が急務であった。事前に取得した 30 日分の 114,450 件のアラームに対し今回のツールを適用したところ、49,022 件(42.8%)が削減可能という算出結果を得ることができた。（図９）　また、想定外の副次効果として、出力されたレポートからアラーム内容精査が容易になったことで、ハードウェア故障のアラームも発見することができた。現在はこれらの算出結果を元に、現場 SE がフィルタリング適用を進めており、高品質な監視サービスが提供出来る見込みである。

本ツールを利用した現場 SE へ感想をヒアリングしたところ、「削減対応が容易になった」「視覚的にレポーティングされるため、顧客や他社ベンダーへの対応説明に活用し易い」といった声が上がり、概ね好評であった。一方で「レポートの情報量が多すぎて必要な情報が何か判別し辛い」といった意見も出ており、今後のツール改版で改善を行う予定である。

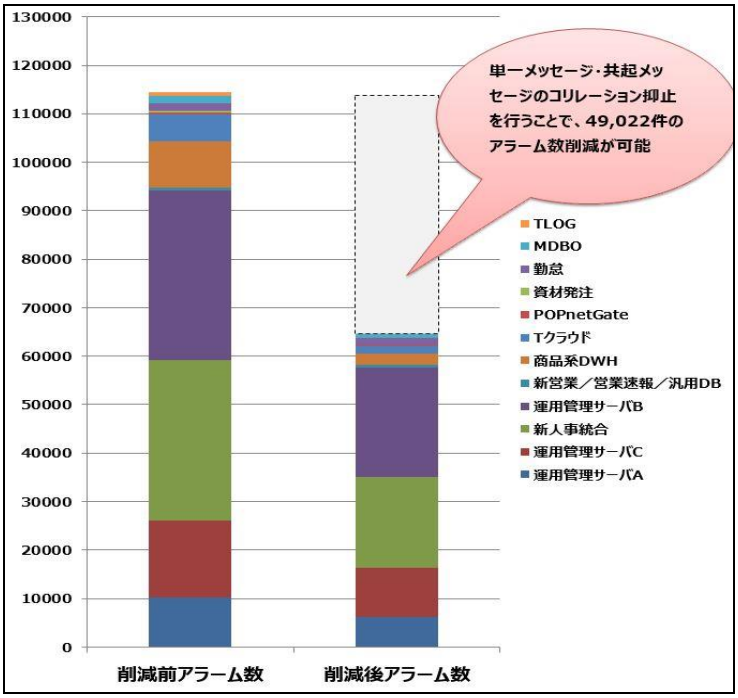

図９　I 社に適用した分析結果

一方、アラーム仕分けツールについて、顧客連絡のみで完了するインシデントの多いユーザーへ試行した。実際の 3 ヶ月分のデータ（2,232 件）を抽出、及び運用を担当する現場 SE がすべてのアラームへインフラ／アプリの仕分けを行い、ツール結果との比較を行った。

この結果、79.3%（1,770 件）のメッセージが人の仕分けと同一となった。「ツールにて判別不可能（この場合人が確認を行うため、不正解ではない）」という仕分け結果も含めると、実に 98.4%(2,197 件)が意図どおりの動作となった。

本ユーザーでは、現場 SE が受け取る SE コールの 6 割が顧客連絡のみで完了しており、現場 SE の対応時間は月間で 40 時間近くに達する。ツールの判別結果に従いオペレーターが顧客に直接連絡することで、対応時間がほぼ削減されるため、効果は非常に大きい。

ただし、人がアプリ関連のアラームと判別したものを、ツールがインフラと判別する真逆のパターンも多少見られた。実運用においては、顧客へ 1 件誤報するだけで大きなクレームに発展するリスクがあり、その場合の対応工数は非常に甚大なものとなる。そのため、今後更なる精度改善が必要である。

改善案として、人間がアラームの判別をする重み付けの要素を加える予定である。メッセージを人間が判別する際、メッセージ冒頭のキーワードや、実際の実行ファイル名などをまずは参照し、その上で詳細なメッセージを確認する。これらは判別材料としての比重が大きい。

現行のツールにこのような重みの考え方を取り込み、逆判別の解消、判断できなかった件数の減少を図る予定である。

５．今後の取り組み

今回開発したツールによって、対処不要なメッセージを効率的に集約し、オペレーターの目視件数を激減させた。更に、インシデント情報を活用し現場 SE によるフィルタリング可否判断を自動化、及び今後の改善の余地はあるが、アラーム判別の自動化も行い、これによって、監視サービスの運用高度化と運用負荷の軽減を実現した。

現在スタンドアロンツールとして提供し、オフラインで利用しているが、2017 年度に現行の監視システム基盤環境のリプレースを予定しており、今後はユーザーへの個別適用を通じて精度向上を図りつつ、これらの機能をリプレース後の基盤環境へ組込む予定である。これにより、発生したアラームをオンラインで自動的にフィルタリング、自動仕分けを行い、更なる品質向上とコスト削減を実現し、監視サービスの全体最適化を図る。

従来のユーザー観点で見た監視サービスは、あくまで「異常を検出し、通知する」までがスコープ範囲であったが、今回のアプローチを盛り込むことで、顧客業務システムの改善分析までもカバー出来るサービスへと刷新出来る可能性を秘めている。他社にこのような製品は無いため、監視サービス展開における、他社優位性確保に繋げられる。加えて本改善の結果、オペレーターや現場 SE の対応品質が向上することで顧客満足度を高め、更なるビジネス拡大にも貢献出来ると期待している。

参考文献

特になし