監視メッセージの最適化

IBM イベント相関解析ツールによるイベント・アナリティクスと適用事例

1. データセンター運用監視における課題

データセンターの運用管理作業において、監視メッセージへの対応は非常に重要です。ITIL のイベント管理プロセスとインシデント管理プロセスに相当する活動として、オペレーターはコンソールに通知される監視メッセージに応じた対応作業を実施します。しかし多くの現場では、対応不要なメッセージが大量に表示されていたり、あるメッセージに対応したら、実際には別の根本原因がメッセージ通知されていて対応が無駄骨になったり、といった顕著な課題を抱えています。

2. 監視メッセージの最適化要件

このような課題に対し、監視メッセージへの対応を最適化するための代表的な要件を考察します。

まず、「**対応が必要な監視メッセージだけが表示される**」ようにすることが挙げられます。監視メッセージは、対応が必要なもののみを表示し、不要なメッセージの確認に費やす時間を削減します。

次に「**適切な優先度が設定されている**」ことも重要です。設計段階でそれぞれの監視メッセージの優先度を適切に設定し、本番稼働後も、設計時の想定から変化したものや、コンポーネント間で優先度が異なるものを継続的に調査し、再設定します。

さらに、「**監視メッセージが標準化されている**」ことが対応作業を効率化します。監視メッセージのフォーマットを標準化することで、起きていることを短時間で把握でき、対応作業が実施しやすくなります。

3. イベント・アナリティクス

前述の要件に対し、通知された監視メッセージの特性をイベント・アナリティクス手法によって把握するアプローチが有効です。セキュリティーやパフォーマンスなど特定の目的に応じた各種アナリティクス手法がありますが、ここでは発生パターンを把握するための代表的な2つの手法「**時系列分析**」と「**相関分析**」を説明します。これらの手法は 5 章で説明する事例でも適用しています。

(1) 時系列分析

数日～１カ月程度の間の監視メッセージを時系列に並べ、反復パターンや発生順序のパターンを分析します。具体的には 10 分間ごとのイベント数をグラフ化し、大量イベントの発生傾向と反復の周期を把握します。**図1**は実際の分析結果ですが、この事例では、５回の不定期なバースト（大量発生）と１０回の反復パターンが発見されました。そのほとんどが対応不要で、本当に対応が必要なものはイベント全量の１５%程度であることが明らかになりました。

(2) 相関分析

相関分析は、複数のイベントの因果関係を特定する手法で、一般に障害対応に長けた技術者や熟練のオペレーターが、時間をかけて経験的に見つけ出すような属人的な分析に頼っています。そこで IBM ワトソン研究所は Event Relationship Network 手法を応用した EMM（Event Monitoring & Management）ツール［1］を開発し、「タイムスタンプ」「ホスト名」「メッセージ ID」の3つのイベント情報をキーに、イベント・アナリティクス技術によって、同じパターンで出現する相関イベント群を発見できるようにしました。

図2は、EMM ツールの特徴を示していますが、数百のイベント種別の中から出現順序と出現間隔を手掛かりに、「A の次に B が起き、その後 C が起きる」「D が起き、その後 E が起きる」という2種類の因果関係のパターンを発見しています。

4. 分析結果による改善対応アプローチ

分析で、バーストや反復、相関など顕著なパターンが発見されたら、パターンそれぞれに改善対応を施します。

【バーストの改善対応】

バーストの多くは、ハードウェア障害に起因し、メッセージに応じて修理対応されますが、同一イベントでコンソールが埋め尽くされる場合もあるので、イベント管理製品の「重複イベントの表示抑止」機能などで、表示されるイベント数を低減します。また、対応不要なものとしてコンソール非表示にしているイベントがバーストしていることもあり、それらは定期的な時系列分析で発見し、発生自体を抑制するようにします。

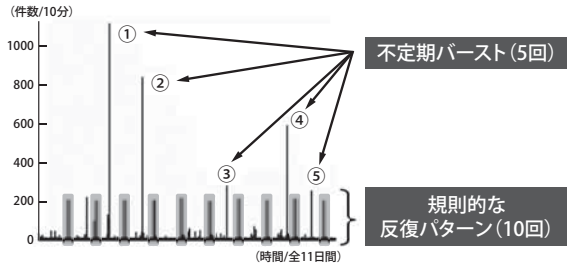

図 1. 時系列分析

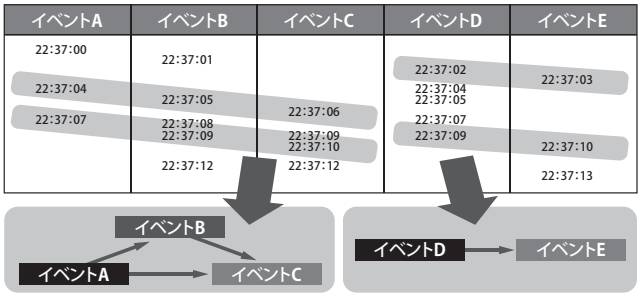

図 2. EMM ツールによる相関分析

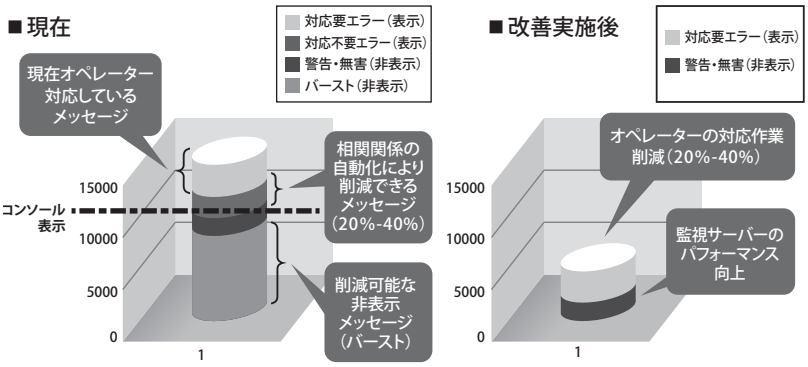

図 3. メッセージ削減効果

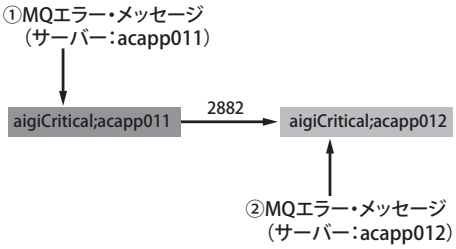

図 4. MQ の相関イベント

【一定間隔で反復するイベント群の改善対応】

これらの多くは定期リブートなどで発生する対応不要なイベント群ですが、通常時は対応が必要なイベントであるため、目視確認で意図的に対応しないようにする「無視対応」と呼ばれる作業が発生し、多くの運用部門で負担のかかる作業となっています。

時系列分析によって無視対応イベントの発生パターンを把握し、通知切替え技法（スイッチを切っている間はイベントを通知しないプログラム的な対策）などにより、イベント発生自体の抑止策を検討します。

【相関イベントの改善対応】

イベント管理製品に「相関付け」の機能がある場合は、イベントに対して自動的に「原因」「副次」の相関を付けて、優先度を動的に変更し、原因イベントから対応するようにします。製品機能がない場合は、手順を改善し、原因イベントが存在している場合としていない場合で、副次イベントへの対応手順を分岐させるようにします。抜本的な対応には、副次イベント生成時に、原因事象のチェック処理を組み込みます。

5. イベント・アナリティクス適用事例

イベント・アナリティクスを適用した事例を2例ご紹介します。

事例1: メッセージ削減による運用コスト削減

この事例 [2] では、対応不要なメッセージが多いという漠然とした課題認識に対し、**図3**の左側のように障害以外のメッセージが数多く通知されていたことが分析により判明しました。メッセージ出力の設定を変更する改善対応により、エラーや警告のメッセージを従来に比べ 80% 以上抑制し、運用担当者のメッセージ出力に伴う対応作業の負荷をお客様による試算で 40% 以上削減できることが見込まれています（**図3**）。

事例 2: 相関分析による障害初期診断の高度化

2 例目は初期診断に時間がかかるという課題に対し、相関分析の結果で顕著な改善効果が見られた例です。**図4**のように、同じエラー・メッセージが、2つのサーバーから別々に通知されていることが EMM ツールの相関分析で発見されました。②のエラー通知はすべて①が原因であることが判明したので、コンソール表示を抑制するフィルター対応を実施しました。このエラーは月間25回発生していましたが、1次サポートが②のエラーから最初に診断して原因が判明せず、その後の2次サポートで原因は①のエラーと特定されることがしばしばありました。対応後は1次サポートだけで診断と対応ができ、初期診断時間を大幅に短縮しました。

6. まとめ

ご紹介した事例からも分かるように、イベント・アナリティクスの持つ次の効果によって、運用部門はよりプロアクティブな活動に取り組めるようになります。

(1) 高度なイベント相関分析が短時間で可能

ベテランの技術者が数週間かけていた分析作業を、EMM ツールで瞬時に終わらせます。世界的に実績を積んだ検出ロジックによって、イベントの相関を正確に把握できるので、技術者は最適な改善対応に注力できるようになります。

(2) 継続的な分析と改善対応による高度な予兆検知

分析と改善対応を継続的に実施することで、障害に起因する一連のイベント発生パターンを逐次把握できます。これにより、障害予兆の検知と予防対策をいち早く講じることができるようになり、サービスの可用性向上に貢献します。

［参考文献］

［1］ IBM：IBM IT Lifecycle Management and Governance Services - event management and monitoring , http://public.dhe.ibm.com/common/ssi/ecm/en/msd03001usen/MSD03001USEN.PDF

［2］ IBM：プレスリリース「監視メッセージ最適化サービス」, http://www-06.ibm.com/jp/press/2011/09/0101.html

岩村 郁雄
Ikuo Iwamura

日本アイ・ビー・エム・システムズエンジニアリング株式会社
サービスマネジメント・エバンジェリスト

増田 みさお
Misao Masuda

日本アイ・ビー・エム株式会社
GTS事業　ITSソリューション
クラウド&データセンター
Certified Architect

※ 本コラムは、IMO（ITSM Management Office）のメンバーにより執筆されています。IMOは、ITサービスマネジメントおよびITILの活用促進と日本での展開への貢献を目的として、日本IBM社内に2004年に設立されたバーチャル組織です。