障害イベント対応を自動化するアプローチ
―ランブックオートメーションを利用したイベント管理―

システム運用におけるイベント管理・障害対応業務では、より迅速な対応が求められる一方、コスト削減も要求されている。システムが大規模化・複雑化し、障害イベントが増加するなかで、効率的な「イベント管理」が求められている。本稿では、イベント管理における手作業の対応を自動化するアプローチについて考察する。

迅速な対応が求められるシステム運用

近年、企業におけるITの役割はますます重要となっており、情報システムに障害が発生すると、ビジネスが受けるダメージは非常に大きいものになる。そのため、システム運用にはより確実で迅速なイベント対応・障害対応が求められている。

同時に、イベント対応・障害対応に要するコストは、システムが大規模化・複雑化するにつれて増加するので、システム運用コストの削減も求められる。

イベント管理プロセスの現状と問題点

現状のイベント管理プロセスのフローは、図１の①のように表すことができる。

監視ツールが検出したイベントは、24時間365日待機している運用オペレータによって監視コンソールで検知される。運用オペレータは、イベントの内容とイベント切り分け表を突き合わせて、対応が必要かどうかを確認する。対応が必要なものは、手順書に従って切り分け・対応を行い、必要に応じて開発部門に連絡する。

このように、イベント管理プロセスは障害の切り分けや対応作業などに人による判断が必要なため、依然として手順書による手作業の対応が実施されている。

イベント管理プロセスにおける問題を整理すると以下のようになる。

(1) 対応不要なイベントの増加

システム障害がビジネスに与える影響が大きくなってきたことにより、過度の障害検知が求められる傾向が強くなっている。実際に、システムのわずかな変化でも障害イベントとして通知するアプリケーションが増えてきている。結果として、障害ではないケースでも障害イベントを通知してしまい、運用オペレータのイベント切り分けによって対応不要と判定されるケースが多くなっている。

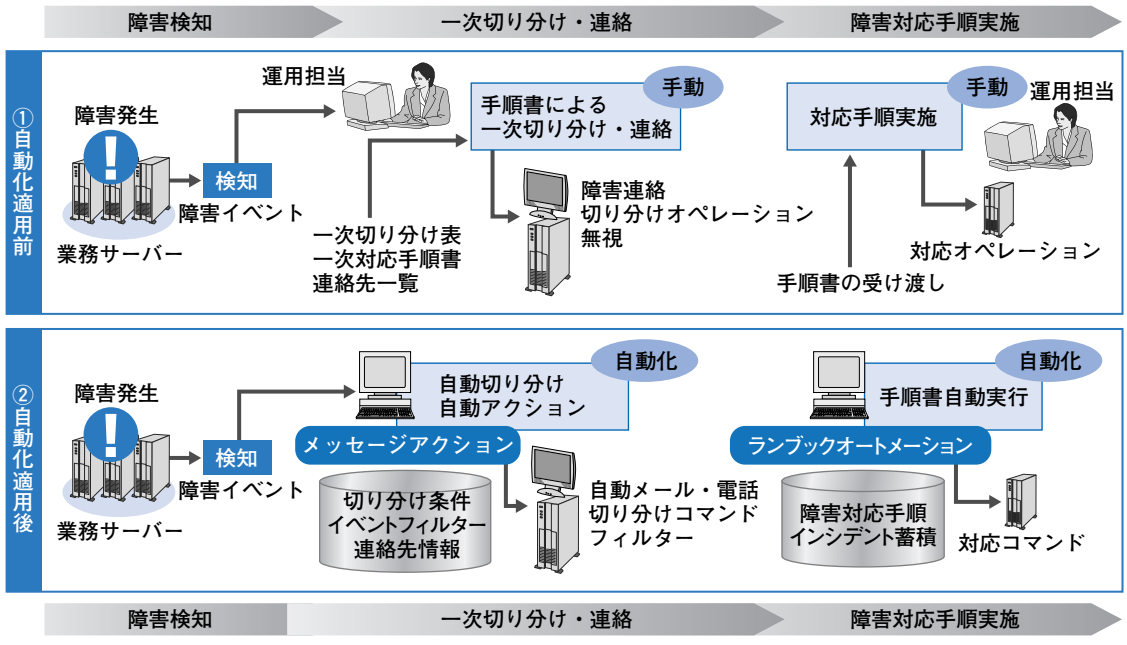
結果として対応不要となったイベントも、運用オペレータによる手作業のイベント切り分けが行われる。このような作業の増加が、運用オペレータの負荷や運用コストの増大につながっている。

(2) 切り分け・対応手順の複雑化・属人化

現在、情報システムはますます複雑化しており、さまざまなベンダーのサーバー、ネットワーク機器、アプリケーションでシステムが構成される。そのため、１つの障害に対し

野村総合研究所
システムマネジメント事業本部
運用自動化推進部
主任システムエンジニア
勝碕　繁（かつざきしげる）
専門は運用管理システムの設計・開発

図1　イベント管理プロセスフロー



て、切り分け・対応のために確認すべき部位・項目が多く、また専門性も要求されるようになってきている。

このように切り分け・対応手順が複雑化したことにより、MTTR（平均復旧時間）が増加したり、あるいは運用オペレータでは対応しきれず、システムに詳しい開発担当者が切り分け・対応を行うケースが多くなったりしている。

(3) 手順書を維持管理する負荷の増大

開発と運用の職務分離が行われている現場では、イベントの切り分け・対応の手順書は開発部門で作成されたものを運用部門が受け入れる形となる。

手順書は、システムのリリースのたびに、また新たな障害が発生するたびに改訂される。システム運用の現場では、障害時の切り分け・対応手順書、定常業務を遂行するための手順書など、さまざまな手順書が存在する。そのため、手順書のメンテナンスや実績の確認など、手順書に関する維持管理の負荷が高まっている。

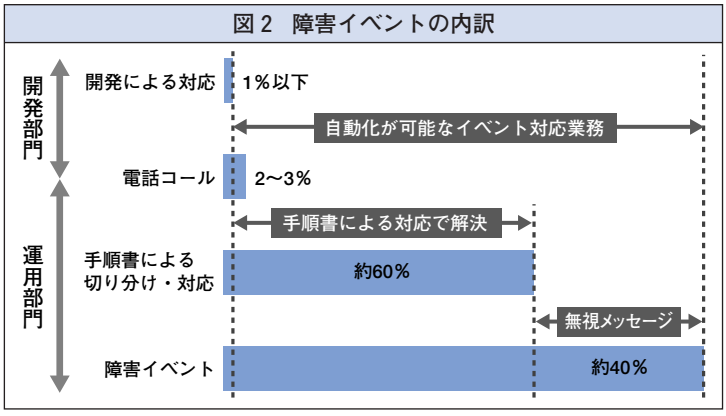
期待されるイベント管理の自動化

実例としてNRIのデータセンターをあげると、ここでは、IT全般統制の観点から開発と運用の職務分離が行われ、イベント管理は運用部門が24時間365日待機して対応している。障害イベントが発生すると、運用部門で切り分けと一次対応までを行い、解決しないもの

だけを開発部門へ回付する。

図２は、NRIのデータセンターで検出されるイベントの月間件数に対する対応内容の内訳を示したものである。

イベントの総件数は数十万件で、その約40％は運用オペレータによって対応不要と判定される「無視メッセージ」である。残りのイベントは、手順書に従って運用オペレータが切り分け・対応を行うが、これによって全体の90％以上が解決される。ここでも解決しないものが開発部門へ回付される。



「無視メッセージ」を含めて運用オペレータの対応は、メッセージ切り分け表や対応手順書に従って行われるオペレーションであり、システム化・自動化が可能な作業である。この部分をシステム化・自動化することは、イベント対応の迅速化・コスト削減を行う近道である。その鍵を握るアプローチとして注目を集めているのが「ランブックオートメーション」である。

「ランブックオートメーション」とは、手作業によって行われているシステムやネットワークの運用オペレーションをワークフロー化し、ワークフローの実行・管理・レポートを自動化することにより、運用の効率を高める技術およびその仕組みのことである。

イベント管理プロセスにおける「ランブックオートメーション」とは、障害の検知から切り分け・対応までの一連のフローを自動化することである。

現在、「ランブックオートメーション」への関心は世界的に高まっている。米国においてはシステムマネジメントにおける１つのトレンドとなっており、2008年頃から多くの企業で取り組みが始まっている。

「Senju Operation Conductor」によるオペレーションの自動化

2009年６月にリリースされた、野村総合研究所（NRI）の統合システム運用管理ツール「Senju Operation Conductor Ver.10.0」には、手作業で行われてきたオペレーションを自動化する２つの機能が実装されている。メッセージアクション機能とランブックオートメーション機能である。（図１の②）

(1) イベントを自動切り分け

メッセージアクション機能とは、運用オペレータが手作業で行っている、イベント内容とイベント切り分け表の突き合わせ作業を自

動化する機能である。

「切り分け条件」として、「発生ノード・発生プロセス」「スケジュール（時間帯・曜日）」「メッセージID」「メッセージ内容」など、イベントに関するさまざまな項目を指定しておくと、発生したイベント（メッセージ）が自動的に切り分けられる。イベントごとに「メールを送信する」「電話を発信する」「ランブックを実行する（後述）」といったアクション（対応）を指定しておくことで、対応が自動される。

(2) 複雑な対応手順を自動実行

ランブックオートメーション機能とは、システム障害時の診断・復旧作業、サーバー維持管理作業など、手順書に従って実施する必要のあるオペレーション（出力内容やタイミングなどで人の判断を要していた部分）を自動実行する機能である。

オペレーションの内容は、図3のようなビジュアルなインターフェース画面でワークフローを作成するだけで簡単に設計できるようになっている。ワークフローには、コマンドを実行する部品や、切り分け結果に応じて後続処理を分岐する部品を配置し、先行・後続関係を設定する。このワークフローを自動実行することで、手順書の自動化が実現される。たとえば、日中のオンライン中はオペレータAに、夜間バッチ中はオペレータBに電話するというような柔軟な設計も可能である。手順書実行の自動化・システム化により、複雑な手順でもヒューマンエラーを起こすことなく迅速な対応が可能となる。

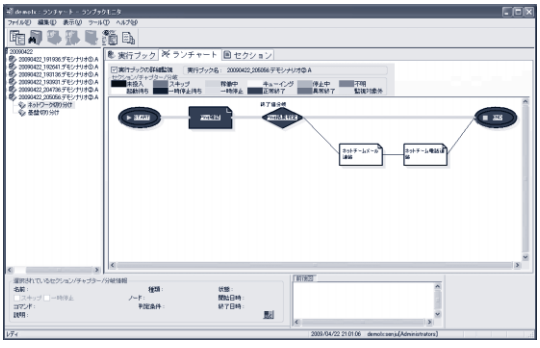


図3　ワークフロー設計のインターフェース画面例

イベント管理自動化の効果

検出した障害イベントはメッセージアクション機能で処理され、イベント内容の切り分けを自動的に行う。連絡が必要なイベントは自動的にメールまたは電話で連絡される。そして、手順書による障害原因の切り分け・対応が必要なイベントは、ランブックオートメーション機能により自動的にワークフローが実行される。

障害の検知から解決までの一連のフローを手作業で実施した場合、1つのイベントの対応時間は平均20分であった。これを自動化することにより、数秒にまで短縮することが可能となる。

以上のように、イベント管理の自動化は、運用オペレータの負荷の削減およびオペレーションミスの防止を可能とし、「属人性のない迅速な対応」と「コスト削減」という2つの効果をもたらす。■