監視の技 10　イベントの種類に応じて対応手順を自動的に切り替えたい

現状の課題

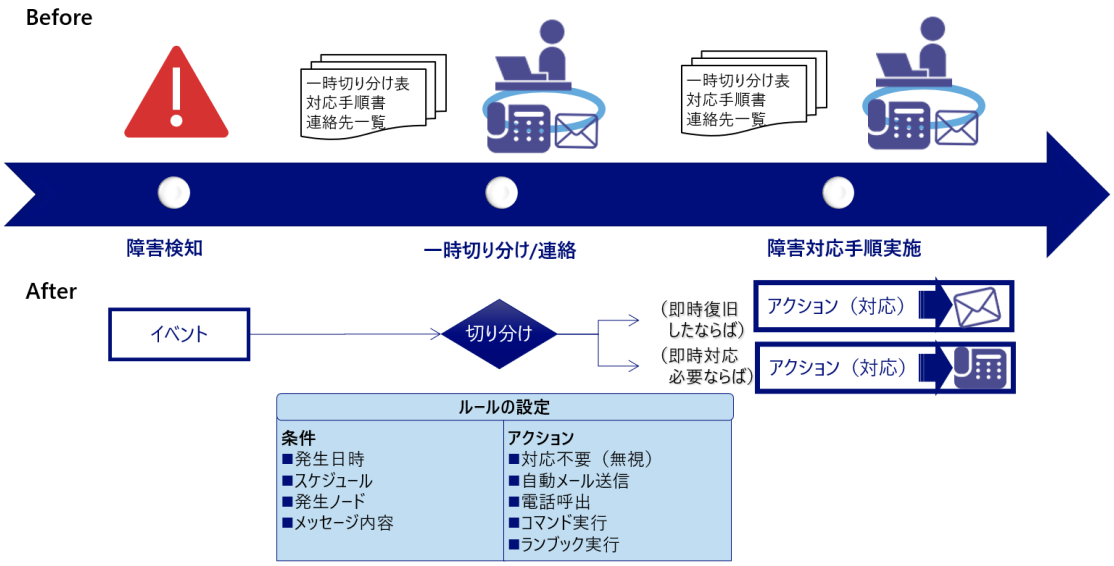
一口に障害といってもそれぞれに内容は異なり、その対応方法もさまざまだ。例えばハードウエア障害やジョブスケジュールでのバッチ障害は、即座に対応しなければならないため電話でのコールが必要となる。一方、リソース警告のような障害の場合は、即座に対応する必要はなくメール通知だけでよい。また対応方法が明確になっている既知事象のものは自動復旧コマンドを実行し、復旧した場合は対応履歴を残してクローズする。

アプリケーション担当者や基盤担当者にとって、障害内容に応じた手順書を常に最新にしておくのは大きな負担である。だからといって、運用担当者が障害のたびに対応方法を、アプリケーション担当者や基盤担当者に確認するのでは作業効率が悪い。

解決策

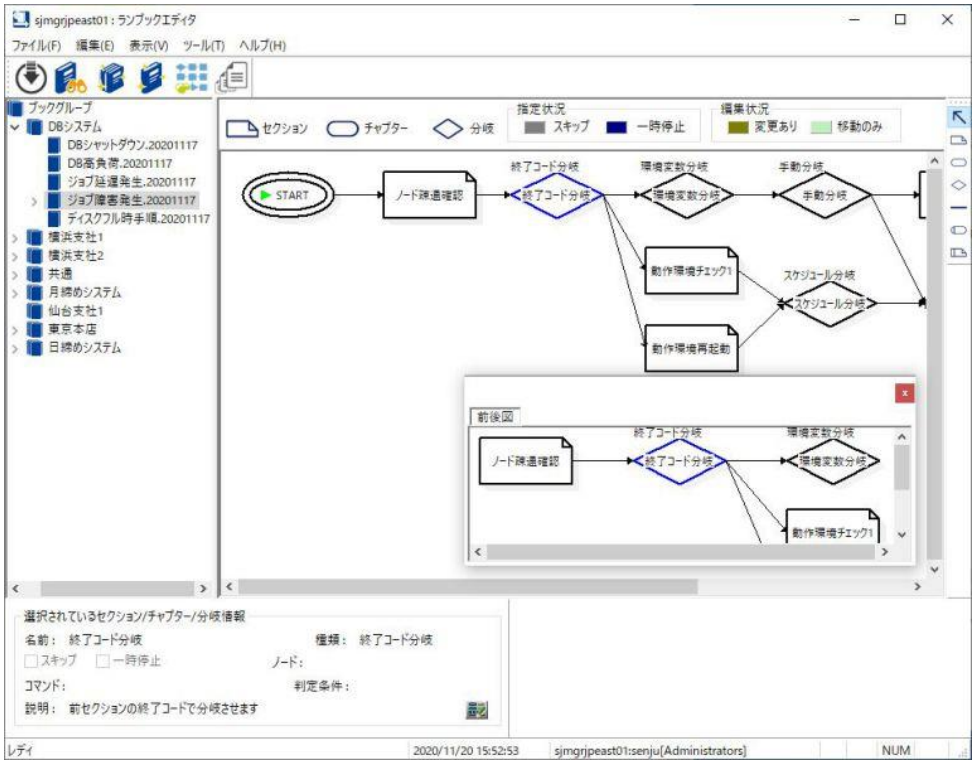
アプリケーション担当者や基盤担当者は、発生する障害ごとに対応方法を電子化した手順書にする。「いつ」「〇〇サーバーから」「〇〇という障害」が発生した場合はこの対応方法というように、障害内容と対応方法を明確にしておく。障害発生時はツールが自動的に判断し、手順書の該当箇所へ導くようにしておく。手順書の更新も簡略化する仕組みが必要だ。

ツールが導いた対応手順書に従い、運用担当者は障害を切り分けて対応手順を実行する。この時点で障害発生時の対応方法を確認する作業はなくなり、作業負荷は軽減されている。どうしても手動で対応しなければならないものは仕方がないが、それを除いた作業をできるだけ自動化しておけば、オペレーションミスを防止するとともに、運用品質も向上する。



Senju Family での実践方法

Senju DevOperation Conductor では「メッセージアクション」機能を提供している。**発生したイベントの切り分けを行い、切り分けた結果に応じたアクション（対応）を自動で行うことが可能**だ。切り分け条件に一致した場合、メール送信や電話呼び出し、コマンドなどを自動実行する。どの条件にも一致しなかった場合は、メッセージモニタに「対応不要」や「エスカレーション要」などを表示することも可能である。オペレーションエンジニアの作業は軽減されるとともに、いま何をしなければならないのかを容易に把握することができる。

障害が発生した際、該当するサーバーの切り分けを実施するときなど複雑な手順が必要になる場合には、「ランブックオートメーション」機能を利用することで障害対応を自動で実施することも可能になる。

イベントに対する手順は、定義データをツールに読み込むだけで最新になる。アプリケーション担当者や基盤担当者が行っていた手順書の更新作業は、大幅に軽減できる。