監視の技 12　システムで検知したイベントを統合して インシデントを自動起票したい

現状の課題

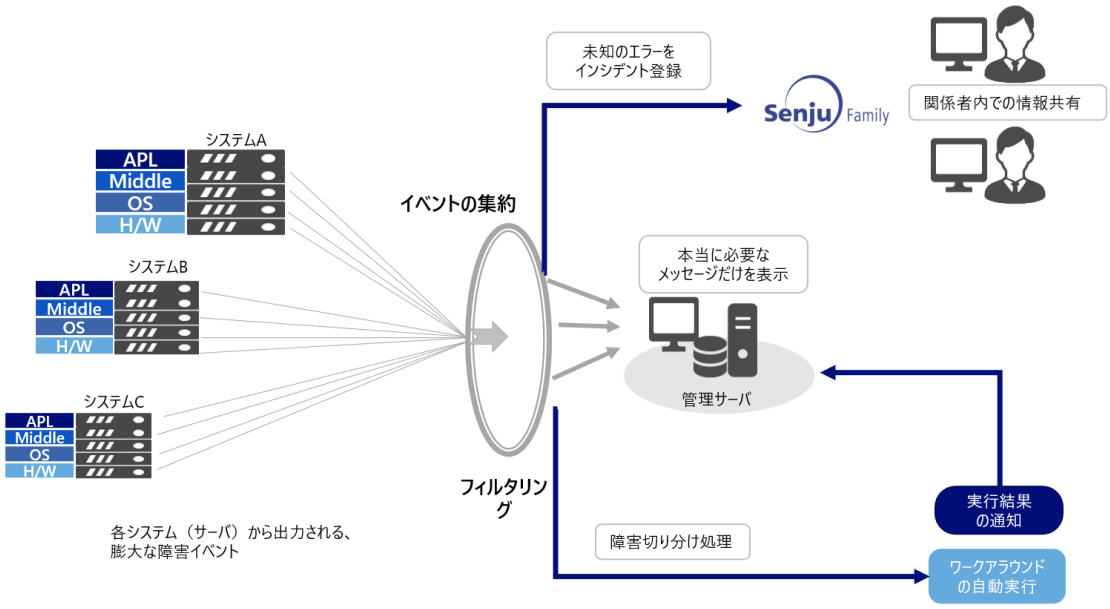
システムからは日々大量のイベントが発行される。障害イベントが発行された場合、①手順書を基に対応を実施、②担当者へ電話やメールで連絡、③対応が完了したらクローズ処理を行う、といった運用を行うケースが多い。だが、複数のシステムからバラバラにイベントが発行されると、システムごとの手順書では運用現場は混乱し、対応ミスを招く。

また、システム運用は 24 時間を交代制で行われるのが一般的であり、シフト交代時には紙による引き継ぎを実施している場合も多く見られる。これでは**対応記録の漏れが発生するリスクが高く、関係者間全体での情報共有は困難**である。

解決策

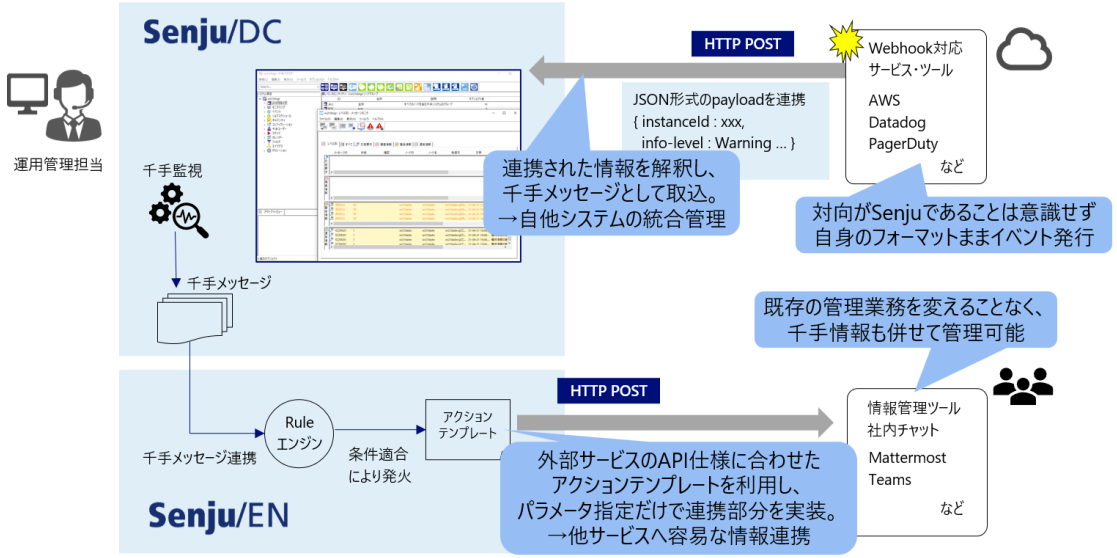
複数のシステムからバラバラに発行されるイベントは全て集約すべきである。一つにまとめた上でイベントの種類に応じた手順を実施する。無視してよいイベントはフィルタリングを行って通知しない。既知の問題にはワークアラウンドを実施しそれぞれの対応記録を通知する。これで現場での対応を一元化でき、不要イベントも通知されなくなるため、作業負荷は大幅に軽減できる。

また、未知のエラーは原因や対応を関係者内で情報共有することが重要である。エラー発生時にはインシデントの起票を行い、適切な担当者にエスカレーションしなければならない。その結果、関係者内での情報共有がスムーズとなり対応漏れを防ぐことになる。



Senju Family での実践方法

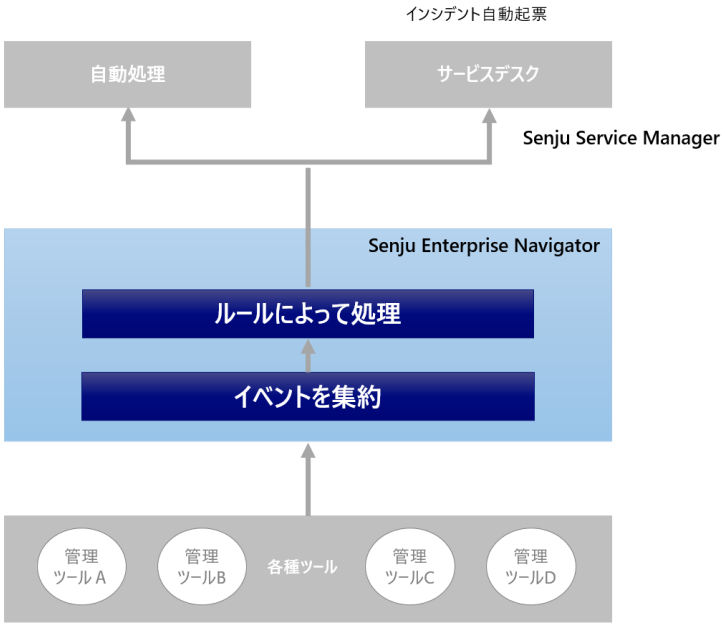
イベントの集約には「Senju Enterprise Navigator」を利用する。これはさまざまなシステムからのイベントを集約し、ルール処理により自動対応を実現する機能を実装するツールである。ルールエンジンによりイベントの種類に応じて対応手順を自動的に判断し、切り分けを行う。既知の問題については、ワークアラウンドについても自動実行し、対応記録の通知のみを行うことが可能だ。



集約する対象として、HTTP によるイベント情報の受付・変換・発信により Webhook 対応の外部システム・サービス、例えば JP1 や Zabbix からのイベントも統合して取り込み、情報管理ツールや社内チャット等、他サービスへの連携も可能である。

Senju/EN ではキューイング機能を利用し、各ツールのアラート形式(ノードのカラム位置、メッセージ ID 等)に合わせた特定のフィルタ条件にマッチしたパターンごとにアラート集約(分類、件数管理)が可能であり、管理不可を軽減することができる。

未知のエラーが発生した場合は、Senju Enterprise Navigator からサービスデスクツールである「Senju Service Manager」へインシデントが自動起票される。適切な担当者へエスカレーションすることで、関係者内での情報共有もスムーズとなる。


インシデント自動起票
自動処理
サービスデスク
Senju Service Manager
Senju Enterprise Navigator
ルールによって処理
イベントを集約
管理
ツール A
管理
ツールB
各種ツール
管理
ツールC
管理
ツールD