監視の技 1　オンプレミス、マルチクラウド等の様々なログ監視を統合、最適化したい［テキスト・JSON ログ監視］

現状の課題

最近では全ての機能を作り込むシステムは非常にまれであり、共通となる部品を他社から調達し、必要な箇所のみを自社で構築するようになってきた。OS・ミドルウエア・自社アプリケーションそれぞれの稼働状況を監視する必要があるが、そのテキストログファイルはさまざまな種類があり形式も異なる。

一つは文字コードの違いだ。あるアプリケーションはシフト JIS で出力し、あるミドルウエアは UTF-8 で出力するなど、開発ベンダーが異なると使用している文字コードもまちまちとなり、同じサーバー内で複数の文字コードが使われることとなる。

ログファイルの切り替え方（シフト方法）が異なることもある。ファイルをリネームしてから新しいファイルを作成する場合や、ファイルをコピーした後に元のファイルを 0 バイトに切り詰める場合、または最新のログファイル名に当日の日付が入るものもある。

また、パブリッククラウドを使用している場合、クラウドの各種サービス等から出力されるログやアナウンスメントの情報を監視し、異常検知を行う必要がある。これらのログは JSON 形式であるため、テキストログだけでなく JSON ログに対してもフィルタリングし、必要な情報だけ抜き出し監視することが求められる。

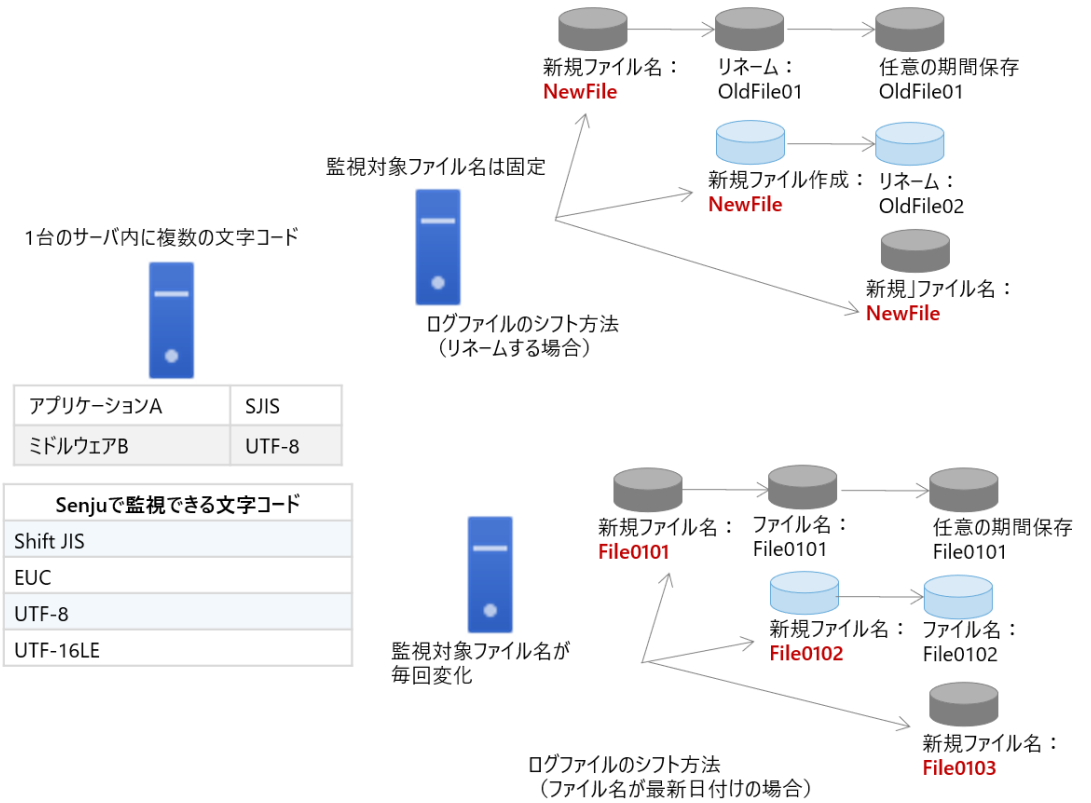
このように一言にログファイルといっても同じ設定では監視できない。それぞれに合った設定が必要となる。

解決策

監視するサーバーの文字コードと異なる文字コードのアプリケーションログを監視する場合は、文字コード変換を行う。その際、特定の範囲の文字コードに関しては事前に任意の文字に変換し、文字コードの変換でエラーが発生するのを防ぐ処理が必要となる。これにより、文字コードにかかわらずサーバー内に出力されるログファイルの監視が可能だ。

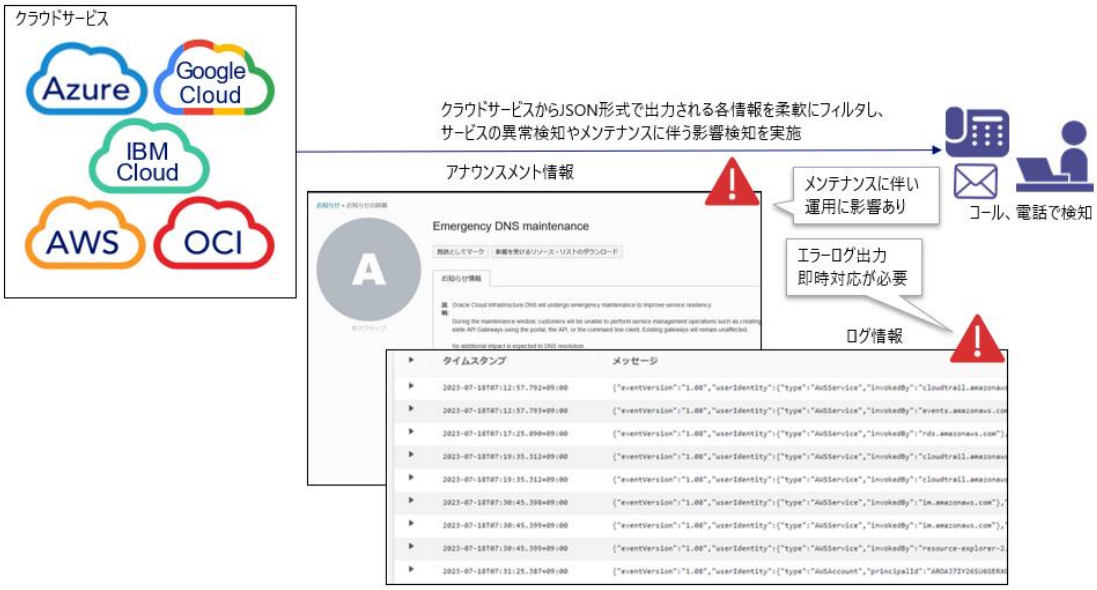
ログファイルのシフト方法は、OS・ミドルウエア・アプリケーションごとの仕様に合わせて設定する。ファイルがリネームされる場合やファイルをコピーする場合は、監視対象ファイル名が常に固定であり特別な設定は不要である。だが、監視対象ファイル名が動的に変化する場合は、毎回新たなファイル名が監視対象に含まれるよう正規表現を使用する。この場合も意図しないログファイルが監視対象とならないように、できる限り条件を絞り込んでおくことが必要だ。

また、テキストログに限らず、JSON 形式のファイルをキーバリューの条件を指定してフィルタリングしたうえで監視することで、クラウド環境のログについても柔軟に監視が可能である。



アプリケーションA	SJIS
ミドルウェアB	UTF-8

Senjuで監視できる文字コード
Shift JIS
EUC
UTF-8
UTF-16LE



Senju Family での実践方法

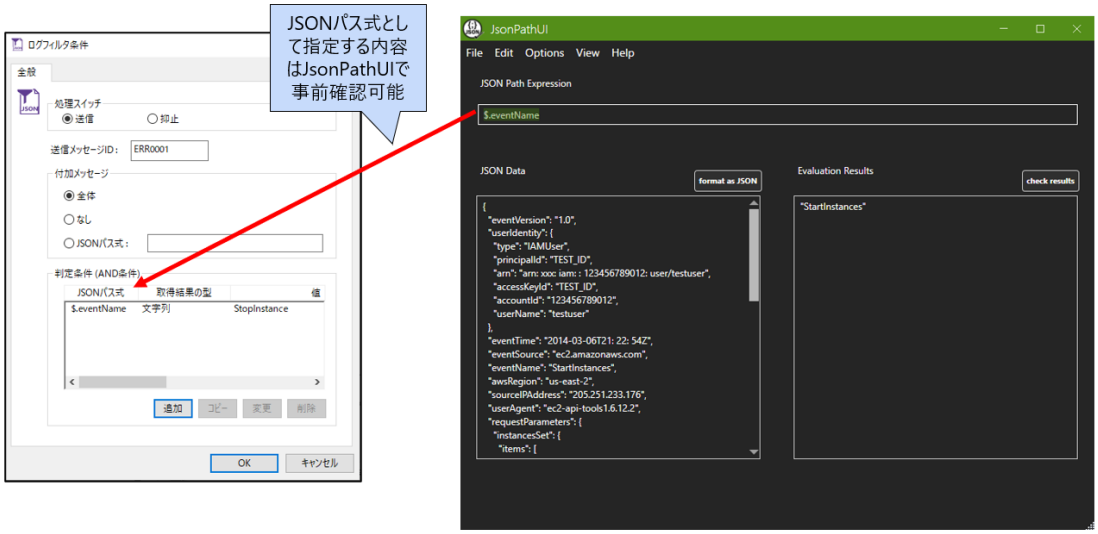
ログ監視は漏れなくダブりなく行うことが重要である。前述のようにファイルのリネームやコピーに追随し監視するとともに、新しく作成されるファイルの中身も監視すべきである。これらは Senju DevOperation Conductor の「文字コード指定」「ログのシフト方法」機能により可能となる。

文字コード指定機能は、文字コード変換時にエラーがあっても、次の文字からコード変換を行う。その他、リトライ回数も詳細に設定することが可能である。ログファイルのシフト方法のいずれにも対応している。

また、アプリケーションの出力ファイル名が次々と変わるような場合、「正規表現でのファイル監視」機能を利用することにより、最新のファイルにも追随した監視を実現できる。

また、パブリッククラウドやコンテナを利用したシステムを運用している場合、Senju/DC Extension Pack を利用することでクラウドサービス（AWS、Azure、Google Cloud、Oracle Cloud Infrastructure、IBM Cloud）のログ、アナウンスメント情報等の収集が可能である。収集が可能な情報はログ、アナウンスメント情報に限らず、Amazon SQS に出力されたメッセージや Amazon Athena でクエリした S3 ファイル内容、Azure Data Explorer のメッセージ、OCI Streaming のメッセージ等、多岐にわたるサービスを対象としている。

これらのクラウド環境で発生した JSON 形式のイベント情報や設定情報のファイルを、イベントログやテキストログと同様に監視対象としてサポートし、JSON ログフィルタによって JSON パス式を指定して絞り込みの指定を行うことができる。また、JSON パス式で取得できる値を事前に確認できるツール「JsonPathUI」もあわせて提供しており、千手ブラウザでの設定前に正しくフィルタリングの指定が行えるか確認することができる。




コンソール上で指定できるフィルタと同様
に千手のログフィルタでも指定可能
ログイベント
下のフィルターバーを使用して、
フィルターパターンの詳細
アクション
メトリクスフィルターを作成
{$.eventName = "AssumeRole"}
Enter キーを押して検索
クリア
1m
30m
1h
12h
カスタム
表示
タイムスタンプ
メッセージ
2023-07-18T07:12:57.792+09:00
2023-07-18T07:12:57.793+09:00
2023-07-18T07:17:25.090+09:00
2023-07-18T07:19:35.312+09:00
2023-07-18T07:19:35.312+09:00
2023-07-18T07:30:45.398+09:00
2023-07-18T07:30:45.399+09:00
2023-07-18T07:30:45.399+09:00
2023-07-18T07:31:25.387+09:00
2023-07-18T07:31:25.387+09:00
2023-07-18T07:31:25.387+09:00
2023-07-18T07:31:25.388+09:00
2023-07-18T07:33:05.417+09:00
2023-07-18T07:33:05.417+09:00