

クラウドシステム向けログ管理システムの開発

飯島 淳一† 宮崎 剛† 大室 善則†

富士電機株式会社†

1 はじめに

近年、クラウドの普及が進み、システムを構築する上でクラウドの利用が選択肢として定着した^[1]。特に、IoT 機器からデータを収集し活用するシステム等はクラウドで構築することが向いており、クラウドの利用が広がっている。

クラウドベンダの提供するサービスと連携させることで、利用者自らの管理範囲や作り込みが減りクラウドの恩恵をより多く得られるが、運用管理をする上においては複数のソフトウェアが連携して動作するため、サービスの安定稼働には各ソフトウェアの稼働ログの監視が必須となる。

本稿では、運用監視作業の効率化や異常発生時の迅速な原因分析を支援することを目的に開発したクラウドシステム向けログ管理システムについて述べる。

2 富士電機での取り組み

富士電機では、クラウドや IoT を活用し、お客様の課題を解決する、新たな価値の提供に向けたサービスに取り組んでいる。

サービスを安定稼働させるため、運用監視を実施しているものの、稼働ログの監視は効率的でない部分があった。そこで、稼働ログを収集し、共通形式に変換した上で統合管理し、発生時刻の相関等をグラフ表示することにより、監視作業の効率化や異常発生時の迅速な原因分析を支援する、ログ管理システムを開発した。

3 適用課題

ログ管理システムを開発する上で、次の課題がある。

- ① ファイルだけでなく、API や専用コマンドにより取得する稼働ログの自動収集対応
- ② 異なるログ形式を同列に取り扱うことが出来るような仕組み
- ③ 監視作業や異常時の原因分析に役立つ表示

Development of log management system for cloud system
Junichi Iijima†, Tsuyoshi Miyazaki†, Yoshinori Oomuro†
†Fuji Electric Co., Ltd.

4 提案手法

図 1にログ管理システムのシステム構成図を示す。ログ管理システムは大きくログ収集、ログ統合、ログ表示の機能で構成される。

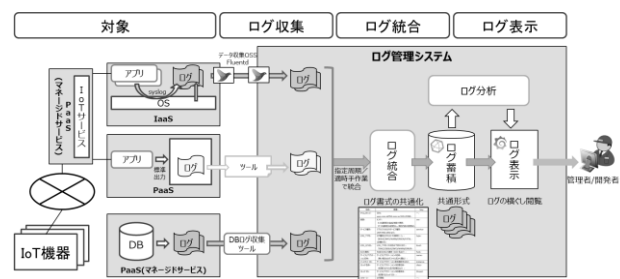


図 1 ログ管理システムの構成図

4.1 ログ収集

ログ収集は、各アプリやサービスから稼働ログを収集しファイルとして保存する機能である。

収集対象とする稼働ログは、次の3種類がある。

- (ア) IaaS(Infrastructure as a Service)上で動作する従来型のアプリが出力する、ファイル形式のもの
- (イ) PaaS(Platform as a Service)上で動作するアプリが出力する、専用コマンドで取得するもの
- (ウ) PaaSが出力する、REST APIでログ取得を行うもの

課題①への対策として、(ア)ファイル形式のものにはオープンソースソフトウェアであるFluentdによる転送、(イ)専用コマンドで取得するもの及び、(ウ)REST APIでログ取得を行うものについてはツールを開発した。これにより、稼働ログを自動収集することが可能となった。また、ログ管理システム以外の監視システムでもログの利用や連携が容易となる。

4.2 ログ統合

ログ統合は、収集したログを共通の形式に変換した上で統合管理する機能である。

収集したログは、対象システムやアプリによって形式が異なっているため、そのままでは同列に取り扱うことができない。そこで、統合管理する

ための共通形式として、ログを標準項目と個別項目に分ける形式で設計した。標準項目は、ログに共通な項目（何時、何処、誰が、何を実施）を格納する。個別項目は、標準項目以外の詳細項目（顧客ID、受信データなど）を格納する。

ログ共通形式の構成を図 2 に示す。

課題②への対策として、異なるログ形式を同列に取り扱うことが出来るような仕組みとした。

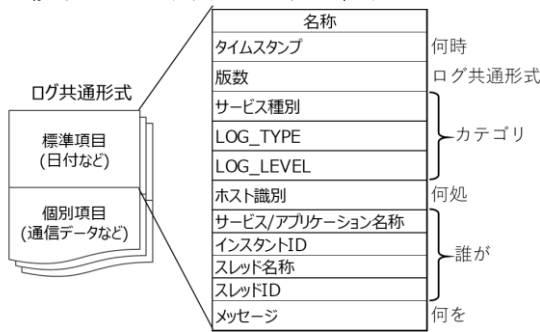


図 2 ログ共通形式の構成

4.3 ログ表示

ログ表示は、統合管理しているログを時系列のグラフや発生時刻と処理時間を表現するグラフとして表示する機能である。

課題③を実現するためのグラフ表示の一つとして、集約したログを時系列で表示した例を図 3 に示す。

図 3 の上部には縦軸を単位時間当たりのログ件数、横軸を時間としたグラフを表示している。図 3 の下部にはあるタイミングでのログ詳細を表示している。図 3 の例では、あるタイミングで DB の CPU が高負荷状態となり、システム全体としてログが急増したことや高負荷状態となる直前に実行された処理が確認できる。

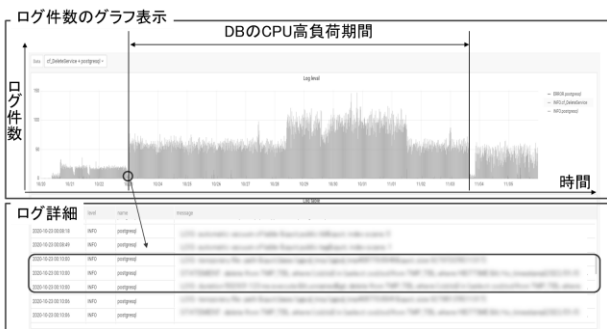


図 3 集約したログを時系列で表示した例

課題③を実現するためのグラフ表示の一つとして、処理時間を表現したタイムチャートの例を図 4 に示す。図 4 では、縦軸に処理の開始時刻の古いものから並べ、横軸に処理の開始時刻から終了時刻までの線を引いている。これにより、長時

間実行した処理やそれに影響を受け時間のかかった処理が確認できる。

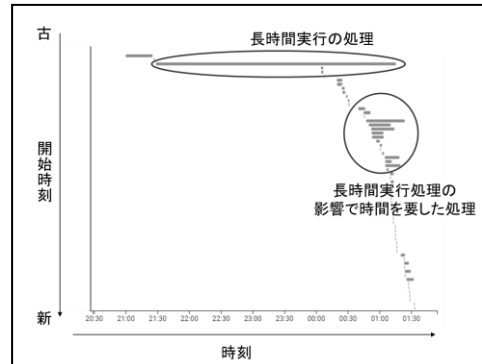


図 4 処理時間を表現したタイムチャートの例

5 効果

ログ管理システムの適用効果について、インシデント対応を行う部門にて評価を実施した。同一のインシデントに対しシステムの有無で評価はできないため想定によるところはあるが、一例としてアラート検知から原因特定までの所要時間が、従来の 4.5 時間から 1.5 時間へと 66% の削減が見込めるという結果となった。

表 1 インシデント発生時の想定効果

現状 所要時間		適用後 所要時間		想定効果
運用部門	開発部門	運用部門	開発部門	
3.5 時間	1 時間	1 時間	0.5 時間	3 時間 (66%) 削減

6 おわりに

本稿では、クラウド上で動作するシステムの稼働ログを自動収集し、共通形式に変換した上で統合管理し、さらに発生時刻の相関等をグラフ表示することにより、監視作業の効率化や異常発生時の迅速な原因分析を支援する、ログ管理システムについて述べた。

今後は、本技術の適用を推進し、クラウド上で動作するシステムの安定稼働に貢献する。

参考文献

[1] IDC Japan. “国内クラウド需要調査結果を発表”.
IDC Japan. 2022 年 12 月 1 日.
<https://www.idc.com/getdoc.jsp?containerId=prJPJ49914322>, (参照 2023-01-06)