FUJITSU

お客様企業
富士通株式会社

本社所在地
東京都港区

業種
ITサービス

製品
Elasticsearch

ユースケース
ログ管理

サブスクリプション
Platinum

富士通：国内トップクラスのクラウド基盤の運用を支えるElasticsearch。運用品質に多大な効果を発揮、セキュリティにも活用

富士通の「FUJITSU Hybrid IT Service FJcloud-O」は、オープンソースソフトウェアをベースに自社で設計・構築・運用しているクラウドサービスだ。クラウドではワークロードも基盤も常に変わり続けるため、要件や問題を事前に把握しきれず、未知の問題に直面する場面も少なくない。しかも、APIには非同期のものが多く、一連の処理のどこに問題があるか容易に分からなかったり、そもそも問題であることを認知することが難しいケースも多い。そこで、Elasticsearchで全ログの分析を行うことで、問題点を迅速に検出し、いつでもトラブルシュートできるようにしている。またクラウド基盤全体のセキュリティ管理にもElastic SIEMを導入し役立てている。

約4TB/日
Elasticsearchで
分析するログの量

約80台
Elasticsearchサーバ

富士通について

さまざまなハードウェア、ソフトウェア、サービスを手掛ける、国内有数の大手 IT ベンダー。クラウドサービス事業においては、グループ会社の富士通クラウドテクノロジーズ株式会社と合わせ日本市場シェア 3 位で、国内事業者としては首位に立つ。
https://www.fujitsu.com/jp/

OSS ベースのクラウドサービスを主力に、国内事業者ではトップのクラウド事業を展開

日本のクラウドサービス市場では近年、いわゆる「メガクラウド」に加え、国内の事業者が存在感を増している。その国内事業者の中でも日本市場シェア 3 位、国内事業者としては首位に立つのが富士通株式会社だ。同社は関東・関西を中心に全国 12 箇所のデータセンターを有し、グループ企業も合わせるとエンジニア約 5 万人の体制で、約 400 種類のサービス、約 100 もの実行基盤を運営、8,000 社を超えるユーザーにクラウドサービスを提供している。

富士通の多彩なクラウドサービスラインアップを代表する「FUJITSU Hybrid IT Service FJcloud-O」（以下、FJcloud-O）は、オープンソースソフトウェア（OSS）をベースに自社で設計・構築・運用しているクラウドサービスだ。2015 年に「FUJITSU Cloud Service K5」としてサービス提供を開始し、アーキテクチャ刷新やサービス名称変更などを経て現在に至る。

サービス基盤の構築・運用においては業務の継続性を追求し、数々の公的認証・規格にも対応、基幹系システムの移行に最適なクラウドという。富士通は日本の政府向けクラウド事業に 2020 年から本格的に参入しており、政府向けクラウド事業において重要な ISMAP（政府情報システムのためのセキュリティ評価制度）のクラウドサービスリストにも

elastic

FJcloud-O が登録されている。

「OSS ベースへのこだわりは、ソースコードが公開されている透明性の高さが理由です。ブラックボックスとなっている商用ソフトとは違い、何かあったときにも我々が対処できるため、事業継続性につながります。FJcloud-O が主なターゲットとしている顧客は金融系や政府系などで、クラウドリフトの商談も多いです」と説明するのは、クラウド基盤統括部 シニアディレクター 兼 クラウド基盤開発部 部長の岩松昇氏だ。

岩松氏は富士通研究所で OS や仮想化、クラウドなどの技術を研究し、OSS にも数多く貢献してきた経歴の持ち主で、クラウド基盤統括部へ移ってからはアーキテクトとして第 2 世代プラットフォームを立ち上げた。このプラットフォームが、今の FJcloud-O へと続いている。

変化し続けるサービス基盤を安定稼働させるため、Elasticsearch で全ログを分析

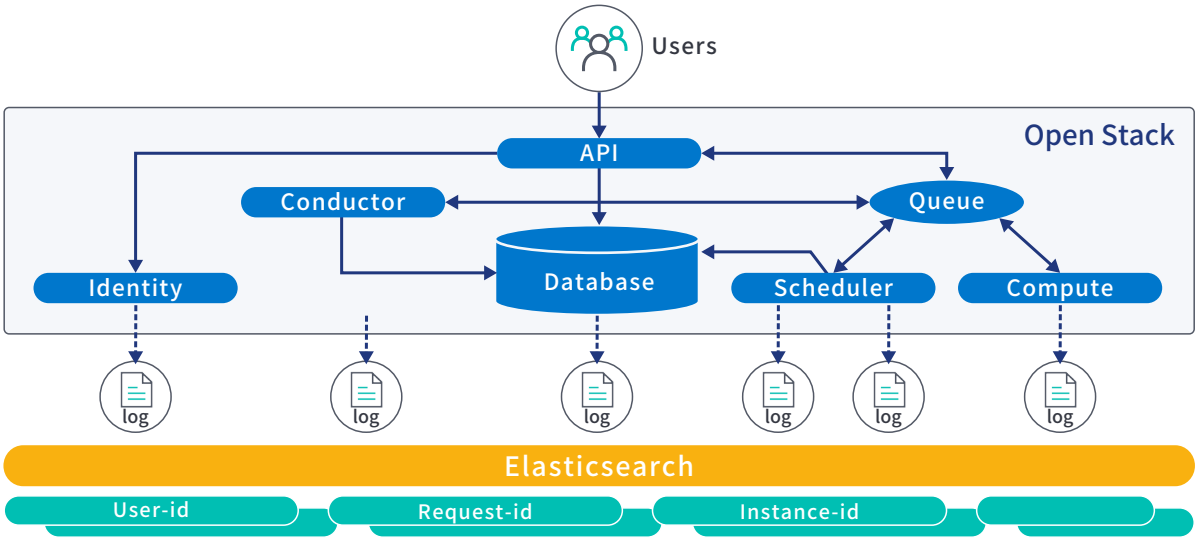
現在の FJcloud-O は、アーキテクチャこそ立ち上げ当初から連続しているものの、プラットフォームを構成する数々の OSS の度重なるアップデートや、プラットフォーム自体の改良などもあって、立ち上げ当初とは大きく異なるものとなっている。

「クラウドではワークロードも基盤も常に変わり続けるため、これまでの SI 案件と違って要件や問題を事前に把握しきれませんし、未知の問題に直面する場面も少なくないのです。しかも、シンプルな指標で問題を検知してアラートを出せるような箇所ばかりとは限りません。クラウドの API には非同期のものが多いので、一連の処理のどこに問題があるか容易に分からなかったり、そもそも問題であることを認知することが難しいケースも多いのです。問題点を迅速に検出して修正し続けることが重要という考えから、いつでもトラブルシュートできるよう Elasticsearch で全ログの分析を行っています」（岩松氏）

Elasticsearch で分析する対象は、顧客向けサービスはもちろん、管理用サービスや、ファイアウォールなど物理機器も合わせた全てのログ、さらにメトリックも含まれる。データ量は全体で 4TB/ 日、最も大きなリージョンだけでも約 2TB/ 日に達し、それをサーバ約 80 台で稼働する Elasticsearch でインデックス化しており、固有 ID などでクエリを実行してサービス間の連携を追いつつ問題箇所を突き止めることが可能だ。クエリはインシデント時に手動で実行するだけでなく、アラートを受けての自動実行や定期ジョブとして実行されるものもあり、問題の早期発見につなげられている。その結果によっては、さらに Ansible などを用いて不整合が発生した DB のレコードを修正するといったセルフヒーリングも自動で行わ

Elasticsearchは、オペレーションの品質向上、そして顧客に対する説明責任を果たす上で役立っており、今後ますます規模が大きくなっていく中ではスケーラビリティに期待しています。運用のさらなる改善に向けて、Machine Learningの活用も進めることにしました

クラウド基盤統括部 シニアディレクター
兼 クラウド基盤開発部 部長
岩松昇氏



図：クラウド基盤を構成する 100 種類以上、数百コンテナのログを Elasticsearch に集約

れる。現状では約 800 項目を監視しており、それに基づく自動化ジョブは 300 あまりに及ぶ。

岩松氏は、Elasticsearch が本格採用されるまでの経緯について、「前の世代のプラットフォームでは、手動でログを収集して調べ、対処する必要がありました。運用を改善するため、前世代の後半からは Elasticsearch でログを分析し、Ansible による自動対処まで行う仕組みをパイロット的に構築しています。これがトラブルシュートに大いに役立ち、Elasticsearch を知らなかった人たちもその効果を実感、第 2 世代では最初から Elasticsearch を組み込むことにしました」と説明している。

Elasticsearch は SOC チームも活用、Elastic SIEM のほか自社開発 SIEM も併用

第 2 世代プラットフォームでは、管理用サービス基盤を docker コンテナによるマイクロサービスで構築、Ansible を中心とした運用自動化の仕組みや、Elasticsearch によるログ収集・分析機能も、最初から組み込まれた。前世代の途中から取り入れられたことで、それまで Elasticsearch を知らなかったエンジニアたちにも効果や活用方法が認知され、定着していった。

サービスとして顧客に提供する基盤だけに、そのログを扱う Elasticsearch も権限設定を分けるなどセキュリティ上の配慮が施されており、またクラウド基盤全体のセキュリティ管理にも Elasticsearch が活用されている。

「セキュリティ管理においては、Elastic SIEM を導入しているほか、Elasticsearch を使って自分たちで開発した SIEM・ダッシュボードもあり、両方を SOC チームの担当者たちがインシデント時などに状況を把握するため使っています。自作の SIEM と Elastic SEIM を併用しているのは、当時の Elastic SIEM だけでは我々が見たい情報に対応できない部分がいくつかあったので、それを補足するのが目的です」と、クラウド基盤開発部 マネージャーの本田亮弘氏は説明する。

なお、SIEM による状況確認・監視を行うきっかけとして、Elastic の Watcher で検知したアラートも用いられている。こうしたセキュリティ運用体制は、各種セキュリティ標準、例えば金融系の PCI DSS や政府系の ISMAP などの認証に伴う監査でも説明し、認定を受けた。

運用品質に多大な効果、 今後は Machine Learning の効果に期待し本格的な活用に着手

Elasticsearch を全面的に取り入れた運用は、サービスの品質に大きな効果を発揮していると岩松氏らは評価している。

「Elasticsearch の効果は広範囲に渡ります。例えば、クラウド基盤を維持するという観点でいえば、やはりオペレーションの品質向上、そして顧客に対する説明責任を果たす上で役立っていると言えます。インシデントの解析をより迅速に行うなどは、Elasticsearch がなければできなかったでしょう。これまでやってこられたのも Elasticsearch あってこそですし、今後ますますビジネスが成長し、どんどん規模も大きくなっていくことが予想されるため、Elasticsearch のスケーラビリティには期待しています」（岩松氏）

FJcloud-O は、第 2 世代プラットフォームとして構築されて以来のアーキテクチャを受け継ぎつつ、改良を繰り返しながら使われている。Elasticsearch も、バージョンアップや新たなモジュールの追加などが行われてきた。今、新たに導入しようと岩松氏らが検討しているのは、Machine Learning だ。すでに簡単な試用を行ったことがあるとのことで、岩松氏は次のように期待を示している。

「運用の経験上、例えば『いつもとは違うログが出ていた』『急に大量のログを出すようになった』など通常と違う挙動が、後で振り返ってみるとトラブルの予兆を示していることが多いのです。そういったアノマリの発生を検出するのに、Machine Learning が役立つのではないかと考えています。現状では事後にログを調べて帰納的に把握していますが、そういったことができる人も限られますし、監視ではなかなか分かりません。どんな人でも、その異常が起きたタイミングで見つけられるようになれば、運用も非常に楽になるのではないかと期待しています。また、FJcloud-O の基盤には、一部ですがベンダー製品も含まれており、その中身はブラックボックスです。そういった箇所の監視を強化するのにも、Machine Learning が役立つと考えています」

なお、過去に Machine Learning を試用した際には、その試行期間が短かったことや、ライセンスの都合により検証用環境で使っていたことなどから、岩松氏らが期待するようなアノマリ検出にはつながらなかった。学習させるデータの種類や量、学習期間や、検出しようとしていたイベントの発生頻度などが足りず、効果を実感できなかったと考えられている。

「やはり本番環境で長期間使っていかないと、なかなか Machine Learning の効果が分かるような事象に遭遇しないのでしょうね。そこで 2022 年 5 月には、本格的に Machine Learning を使えるライセンスにしました。試行した時点のバージョンに比べると Machine Learning の機能も劇的に良くなっていると聞くので、今後は社内的な環境で実績を積んでいき、本格的な活用を進めたいと考えています」（岩松氏）

お問い合わせ
Email: elastic-japan@elastic.co

全文検索エンジンを提供する企業、Elastic は Elastic Stack（Elasticsearch、Kibana、Beats、Logstash の製品群）の開発元です。検索、ログ、セキュリティ、分析などのユースケースで大規模データをリアルタイムに処理するサービスを、オンプレミスと SaaS で提供しています。Elastic のコミュニティは 10 万人規模に成長しています。Elastic Stack は Cisco、eBay、Goldman Sachs、Microsoft、The Mayo Clinic、NASA、The New York Times、Wikipedia、Verizon を含む世界中の企業や組織で採用され、ミッションクリティカルなシステムを支えています。Elastic は、世界各国から社員が働く「分散型企業」として 2012 年に設立されました。詳しくは、elastic.co/jp/ をご覧ください。

