数時間を要していたログ確認がわずか5分足らずで可能に 監視業務や障害対応の迅速化に大きく貢献するSplunk

課題

日常業務としてのリソース監視の状況報告がリアルタイムに実施できず、障害発生時にはログ取得から分析、原因特定までに数時間ほど必要。障害復旧だけでなく、日々の監視業務においても、効率的な環境づくりが求められていた。

導入効果

本番環境に影響を与えることなく、スキルに依存せずログ分析から原因特定までが容易に。確認作業だけで2〜3時間が必要だったが、わずか5分程度で確認できるように。日々のリソース監視も複数の環境を紐づけることで、一気通貫で把握できるようになった。

TOYOTA SYSTEMS

業種: ソフトウェア

ソリューション: IT運用, プラットフォーム

トヨタグループの サービス品質向上に貢献するSplunk

2019年にトヨタ自動車の情報子会社3社が合併し、トヨタ自動車並びにトヨタグループ各社に対して開発及び情報領域の各種サービスを提供している株式会社トヨタシステムズ。これまで培ってきた専門スキルを結集し、アプリケーション、インフラ、ネットワークの切れ目なく、かつサービスの企画・提案から、構築・導入・運用に至る一貫したトータルITソリューションを展開、トヨタグループ全体のビジネス基盤の強化を強力に推進しています。「最適解を、ITで」とスローガンに掲げ、先端技術開発から車づくりを支えるエンジニアリング分野やコーポレート・ファイナンス分野、業務支援を行うインフラ分野に至るまで、オールトヨタとしてDX・デジタル化を早急に進めながら、持続可能なモビリティ社会に貢献する活動に取り組んでいます。

そんな同社では、さまざまなシステムを運用しており、そのための基盤として数多くのITインフラを運用しています。そのシステム環境を安全に運用するためにも、日々のサーバおよびアプリケーションの監視業務はもちろん、万一障害が発生した際には迅速な原因究明とその対処が求められます。その環境づくりを通じてトヨタグループのサービス品質向上に貢献しているのが、クラウド環境で利用できるSplunk Cloud Platformであり、ITサービスの健全性を監視するためのSplunk IT Service Intelligence(以下、ITSI)です。

大量のログを分析し、日常的な監視業務の効率化や 障害時の原因特定の迅速化を図りたい

トヨタグループ全体におけるIT 基盤の運用管理を行っている同社は、設計技術や製造、そして販売後のアフターケアに関連した各種システムの運用管理まで幅広い領域をカバー。「サービスが稼働するサーバの監視を行い、万一の障害時にはログを収集したうえでその原因特定を行う作業を日常的に行っており、長年継続して安定稼働に向けた環境整備に取り組んでいます」とカスタマーサービスシステム部 部長 田中 孝蔵氏は説明します。なかでも、自動車から取得するデータをコールセンターに提供し、顧客対応に生かすための仕組みを運用していますが、万一障害が発生した際には、迅速な切り分けから原因特定、早期復旧に向けた環境づくりが求められてきました。

データを取得する対象車両は今やグローバルで1000万台近い数になっており、この情報が日々大量に蓄積されている状況です。「万一の障害時には、これまでは昔ながらの手作業にて直接サーバからログを収集し、分析を行うことで原因特定を行ってきました。本番環境のサーバだけに誰でもすぐにログを取得するわけにもいかず、複数のメンバーでチェックしたうえでデータを収集する必要があります。決して効率的な作業とは言えませんし、分析するだけでもメンバーに大きな負担を強いていました」と同部 GM 伊藤 孝幸氏は当時を振り返ります。もちろん、障害復旧だけでなく、日々の監視業務においても、効率的な環境づくりが求められていたのです。実際に障害が発生した際には、本番環境からログを取得しその内容を詳細に分析していくだけで数時間が必要で、日々行っているリソース監視においては、データを収集してExcelなどでグラフ化するという作業のために週に1回ほどしか報告、共有できない状況でした。

本番環境に影響を与えず、 事前に用意したサーチ文でデータ確認も容易に

新たな環境づくりに向けて検討するなかで注目したのがSplunk Cloud Platformでした。実は同時期にAPM(Application Performance Management)ツールを別途導入してアプリケーションのパフォーマンス分析を行う環境づくりを行っていましたが、APMツールではログ分析の機能が十分でないと考えていたと語ります。「大量のログを分析、検知することはAPMツールでも可能ですが、障害原因の特定から復旧にまでつなげたいと考えていました。リアルタイムにログを収集し、それぞれを関連付けてインサイトを見つけるという観点では、Splunkが適していると考えたのです。クラウド環境のためにサーバの維持管理に負担もなく、急な対応でも自宅からアクセスできる。小さく始めて育てていけることも魅力的でした」と伊藤氏。同部の市川 武人氏も「数多くのサーバを運用しているため、できる限り業務処理に影響を与えないような環境が重要です。本番環境に影響を与えることなくログ分析が可能なSplunkは、我々が求める仕組みとマッチしていたのです。また、作業の平準化が可能な半面、ITスキルの高いメンバーであればより詳細に使いこなすことができるという点も大きなメリットでした」と語ります。

データを成果に変える

- ログ収集から確認までの作業時間を大幅に短縮
- 教育期間が1か月から1週間ほどに削減
- 業務の自動化で工数削減に貢献

(写真右から)

株式会社トヨタシステムズ
カスタマーサービスシステム部 部長
田中 孝蔵氏

株式会社トヨタシステムズ
カスタマーサービスシステム部 GM
伊藤 孝幸氏

株式会社トヨタシステムズ
カスタマーサービスシステム部
市川 武人氏

株式会社トヨタシステムズ
カスタマーサービスシステム部
近藤 芳樹氏

実際にPoCにて検証してみたところ、SPLにてサーチ文を用意しておくだけで必要なデータが確認でき、必要があればすぐに全体への通知が可能になるなど、これまでできなかったことが簡単に実装できることを実感した同部 近藤 芳樹氏。「設置されたサーバから取得するだけでなく、オンデマンドで配信されてくるものなどさまざまな環境で日々運用しており、受け取ったバイナリデータをテキスト変換した後にバッチ処理するなど、いろいろな処理を経たうえでようやくデータが確認できます。どうしてもログが分断されており、それを一気に確認できるのは魅力的でした」。インターフェースも自身が見やすい形に組み換えが自由に実施できるなど、便利に活用できると考えたと語ります。

同時に試したITSIに関しても、全体の状況を一気通貫でリアルタイムに把握できるようになるなど、状況の可視化による障害の未然防止に非常に役立つと判断。「求めているキーワードだけを抽出したり見たいログだけを部分的に抜き出すなど、必要な情報だけを簡単にグラフ化できます。時系列で並べて見ることも容易で、自由度の高さから使いやすさを実感しました」と同部 池田 健吾氏は評価します。その結果、定常監視業務および障害発生時の状況把握から対処に至る環境づくりにSplunkが採用されることになったのです。

数時間の確認作業がわずか5分ほどで可能に、スキルに関わらず作業の平準化にも貢献

現在は、開発環境含めた22台ほどのサーバのうち、アプリケーションサーバやDBサーバなど計8台ほどを監視対象として設定しており、フォワーダーを経由してSplunk Cloud Platformにログを収集、インデックス化し、いつでも検索できる環境が整備されています。ITSIにて閾値を設定したうえで、稼働するサービスの健全性も監視できるようになっています。1日に取り込むログは100GBに達しており、1年ほどの保存期間を設けて運用している状況です。「事前にSPLにてサーチ文を作成したうえで問題があればアラートが通知されるように設定しており、日常的にはそのアラートを確認し、必要に応じてSplunkにて調査を行うことも。ITSIでは、ダッシュボード上にリソースが一覧で確認できるようになっているため、その変化も確認しています」と近藤氏。これまで2名ほどの体制で定常監視を1日かけて行っていたものが、多くの部分を自動化したことで大きな負担軽減につながっています。

データの不正など問題発生した場合の確認作業は、以前は本番環境からのデータ取得から始めていたことで確認までに2～3時間を要していましたが、今はSplunk側のログを確認するだけで済み、わずか5分程度の時間で確認作業が実施できる状況です。リソース監視もグラフ化して共有するのに週に1度しかできなかったものが、今では複数のログを相関的に紐づけることで全体が一気通貫でリアルタイムに把握でき、異常が発生した場合もすぐに確認、対処できる環境が整備できています。「以前は大量のデータをローカルに保存し、データを準備するだけでも多くの時間がかかるなど、ある意味で職人技が必要でした。今はデータが蓄積された段階で素早く検索できます。メンバーのレベルにかかわらずスクリプトをたたくだけで状況把握が可能です。日々の定常業務で必要な情報をダッシュボード化することにより、資料まとめも不要になり、作業の平準化にも大きく貢献しています」と伊藤氏。

特に走行している世界中の自動車から24時間365日送られるデータを確認しなければならないため、いつでも全員で監視できる環境が整備できたことで、特定のメンバーが疲弊するような環境からも脱却できています。「障害が発生すると時間を意識して焦ってしまう場面もありますが、今はいつでもすぐに確認できるという安心感があるのは大きい」と池田氏。教育面でも、月に1度程度しか行わない作業もあるため、覚えるまでに1か月程度を要していましたが、今はアラートメールを判断して対処するフローが中心となり、1週間程度ですぐに戦力として活躍できるようになった点も見逃せないと近藤氏。

Splunkのサポートについても、監視に最適なGUIの使い方アドバイスや無料セミナーによるSPL学習、検索を効率よく行うための記載方法の助言など、学びの機会も多く得ている状況です。「やりたいことに対して実現する方法はもちろん、適したアドインの提案などもいただけており、とても助かっています」と池田氏。全体を管理する田中氏もSplunkの効果を実感しています。「残業時間を減らすことでメンバーのモチベーション向上にも貢献しており、職場の雰囲気もよくなっています。我々の取り組みを社内にアピールすることで、他部署も含めて全社的にSplunkに興味を持っており、活用の輪が広がっていると感じています」と高く評価します。

> 残業時間を減らすことでメンバーのモチベーション向上にも貢献しており、職場の雰囲気もよくなっています”
>
> 株式会社トヨタシステムズ
> カスタマーサービスシステム部
> 部長
>
> **田中 孝蔵氏**

> メンバーのレベルにかかわらずスクリプトをたたくだけで状況把握できます。リソース監視のための資料まとめも不要になり、作業の平準化、迅速化だけでなく、ムダな作業の削減にも大きく貢献しています”
>
> 株式会社トヨタシステムズ
> カスタマーサービスシステム部
> GM
>
> **伊藤 孝幸氏**

> ユーザの動きを自分たちの手元で先んじてチェックできるような環境づくりに向けて、Splunk Real User Monitoringに期待したい”
>
> 株式会社トヨタシステムズ
> カスタマーサービスシステム部
>
> **市川 武人氏**

> 以前は業務を覚えるまでに1か月程度を要していましたが、新人でも1週間程度ですぐに戦力として活躍できるようになっています”
>
> 株式会社トヨタシステムズ
> カスタマーサービスシステム部
>
> **近藤 芳樹氏**

> 障害が発生すると時間を意識して焦ってしまう場面もありますが、今はいつでもすぐに確認できるという安心感があるのは大きい”
>
> 株式会社トヨタシステムズ
> カスタマーサービスシステム部
>
> **池田 健吾氏**

AI技術の活用や早期の事象察知へ向けた環境づくりも進めたい

これまで同社では、新たなシステム環境を整備する際に運用ツールを手作業で構築してきましたが、今回クラウド環境にてSplunkをベースに運用環境が整備できたことで、新たに適用していく環境も増えていくと期待を寄せています。「今後はコンテナ実装やクラウド環境で基盤を構築する機会も出てきますが、Splunkのようなツールで運用の自動化を図っていくことで要員が共有できるだけでなく、システムの共通化にもつながってくる。その意味での期待は高い」と伊藤氏。

ITSIについては、現状は機械学習によるプロアクティブな異常検知までの仕組みが整備されていないため、AIOpsプラットフォームとしてのSplunk活用をさらに進めていきたい考えです。「過去の実績から閾値を設けて検知するようなことは実際に行っていますが、AI技術を活用することで、複数のログの動きから障害の予兆検知といったことにまで発展させていきたい」と近藤氏。池田氏も「ログだけでなく、例えばDB内のブロックを見る機能を使って、想定外のデータが入っていないかどうかといった動きの検知などにも活用してみたい」と語ります。

また、現場から問い合わせが来る前に、システム保守側でいち早く事象に気づけるような環境づくりを進めていきたいと語ります。「ユーザの動きを自分たちの手元で先んじてチェックできるような環境を整えていきたい。その点では、先行して導入しているAPMツールの活用はもちろんですが、導入当時はなかったSplunk Real User Monitoringの検証を始めています。既存APMツールのSplunkへの置き換えも含め、自分たちが管理するネットワークの先も含めて手が届くような環境づくりを進めていきたい」と市川氏。運用の自動化についてもある程度整いつつありますが、無人化によるさらなる省力化や開発と運用を考慮したDevOpsの環境づくりに向けても活用していきたいと語ります。

トヨタグループ全体を支えている基盤を運用している同社だけに、今後もSplunkを活用してグループ全体の安心安全な業務運用に貢献していきたいと最後に田中氏に語っていただきました。

22-Fix-Splunk-TOYOTASYSTEMS-A4-101-CS