

KPI設定で有識者でなくても状況が把握できる システムステータスの強力な可視化に貢献するSplunk IT Service Intelligence

概要

ソフトバンクグループにおける決済や金融に関する中核企業として、決済代行をはじめとした金融サービスを手掛けているSBペイメントサービス株式会社。EC運営事業者向けにクレジットカード決済やキャリア決済といった様々な決済手段を提供するオンライン決済代行事業をはじめ、ソフトバンク携帯ユーザー向けの通話料合算請求に関する開発・運営、カード加盟店審査や端末決済サービスの提供といったカード加盟店業務、カード発行業務などを行っています。なかでも中核事業であるオンライン決済サービスは、40を超える決済手段を用意しており、コンビニ支払いやプリペイドカード、口座振替、ポイント支払などにも対応可能です。2017年実績で取扱高が2兆5334億円、2018年度 10月実績で100,474店舗の導入実績を誇る、業界屈指の決済サービスを提供しています。

そんな同社においてシステムの運用支援・改善を行っているシステム本部 システム運用統括部 運用課では、運用の課題解決をはじめ、日々の業務改善やシステム開発の支援を行うなどシステムに関連した様々な業務に従事していますが、事業が拡大するなかで運用管理するサーバーの数も急増することに。そこで、ログ収集・分析の早期化やシステムリソースの可視化によって障害対応や問い合わせ対応を円滑に行うべくSplunk Enterpriseを導入。その後、専門家だけでなくシステムステータスが可視化できるようSplunk IT Service Intelligenceを導入し、アプリケーションやDBとの相関関係も含めたシステムの健全性が一目で分かるような仕組みを構築しています。ダッシュボード画面からドリルダウンするだけで該当箇所の詳細情報がすぐに把握できるなど、運用管理の効率化にSplunkが貢献しています。

効率的なログ分析に必要なSplunk Enterprise

同社では、各種決済機関が持つシステムとEC運営事業者をはじめとした加盟店を連携させるための仕組みを運用しており、加盟店側に提供するフロントのアプリケーションサーバーや各種DBサーバーを数多く運用しています。それらサーバー群の運用を行っている担当者は、加盟店からの問い合わせ対応や障害切り分けが発生した場合、それぞれのサーバーがログを抽出し、複数のログを相関的に見ながら調査していく必要があります。「事業の拡大に伴って管理するシステム規模が大きくなるなか、ログを収集して必要な情報を抽出するだけでも多くの工数が必要です。原因を特定して回答するまでの時間を効率的に行うためにも、ログが効率的に分析できるツールが求められていたのです」と運用課 鈴木 彰氏は当時の課題について振り返ります。

社内においては、業務の効率化も含めた新たな技術的アプローチを実践する役割を担っているため、ログ分析のソリューションとして日本では実績のなかったSplunk Enterpriseを2010年にいち早く導入、顧客対応の迅速化に取り組んだ経緯があります。「我々が重視しているのは、その仕組みがデファクトスタンダードであることです。しかも、日本での実績よりも世界的に標準的な仕組みかどうか。その点、Splunk Enterpriseはその時点でも高く評価できたのです」と鈴木氏は選定のポイントを語ります。「ログ収集せずとも調べる時点でSplunk内にログが格納されていますし、SPLと呼ばれる強力な検索コマンドを利用すれば必要な情報にすぐたどり着くことができます。依頼対応だけで1日かかっていたことが、すぐに解決できるようになりました」とその効果を鈴木氏は実感します。

有識者でなくても原因特定でき、 システムステータスの可視化が容易な仕組みが必要に

ただし、Splunk Enterpriseによる運用では、ログ監視のためのミドルウェアなどから発行されたアラートが上がった段階で確認作業を行うケースが中心でした。そんな運用を続けていくうちに、CPUやメモリの使用率といったリソース周りのリアルタイムなモニタリングに関する課題が顕在化してきたと言います。「本番環境で作業するときは、サーバーのステータスなどを目視で監視しながら作業しますが、監視対象ごとにウィンドウを立ち上げる必要がありますし、すべてがテキスト情報での監視です。集計しないと把握できない事象は、その場では対応が難しい状況でした。もっとわかりやすくシステムリソースが可視化できるようにしたいと考えたのです」と鈴木氏。そこで、これまで取得していなかったサーバーリソースをログ化してSplunk Enterpriseに集約、ダッシュボード画面にてグラフ化することに成功します。「ダッシ

SBペイメントサービス株式会社

業種

- ・ 情報通信業

活用事例

- ・ オンライン取引におけるサービスモニタリングおよびシステムステータスの可視化

課題

- ・ ログを相関的に分析、原因究明までに膨大な工数が発生していた
- ・ サーバステータスを目視で監視せざるを得ず、非効率だった
- ・ システム全体のステータス把握が困難だった
- ・ 有識者でないと障害原因の特定が難しかった

導入効果

- ・ 自動的にログ収集、効率的な分析が容易になり、依頼にも迅速に対応可能になった
- ・ グラフィカルにサーバーリソースが可視化できるようになった
- ・ KPIを設定し、色でステータスが一目で把握できるようになった
- ・ 詳細情報までドリルダウンでき、障害原因のあたりが簡単に付けられるようになった

データソース

- ・ 外部接続用のGW機器のログ
- ・ アプリケーションサーバーログ
- ・ DBサーバーログ
- ・ Webサーバーのログ

スプラック製品

- ・ Splunk Enterprise
- ・ Splunk IT Service Intelligence



SBペイメントサービス株式会社
システム本部
システム運用統括部
運用課
鈴木 彰氏

ュボード上でグラフィカルに表現できたことで、作業中のモニタリングが容易になりました。異常があればすぐに気づきますし、見落とすことがなくなったのは大きい」と鈴木氏は評価します。

そして2017年、新たな課題に取り組むこととなります。それが、システムステータスの可視化です。「ダッシュボード上では、サーバーごとのリソースが把握しやすくなっています。しかし、サービスが不安定になったときなど、システム全体での事象を把握するためには、有識者が原因箇所のあたりを付けた上で調べなければなりません。有識者でないメンバーでも原因特定が進められる環境が必要だと考えるようになったのです」と鈴木氏。しかし、Splunk Enterpriseの基本機能だけでは実現するのは困難でした。そこで紹介されたのが、データドリブン監視システムによるイベント分析によってシステムステータスの可視化が可能なSplunk IT Service Intelligenceだったのです。「Splunk Enterpriseのアドオンで利用でき、費用もさほどかからないことが分かりました。そこでハンズオンを開いていただき、すぐに実装する決断をしたのです」と鈴木氏は語ります。

KPI設定でサービスレベルが一目で分かる

Splunk IT Service Intelligence

現状は、Splunk IT Service Intelligenceにて各システムのモニタリング項目における閾値、いわゆるKPIをそれぞれ設定し、収集先のサーバー群における関係性を示したシステムマップ (Glass Table) をGUIから作成することで、ダッシュボード上に各システムの監視項目を表示しています。色分けされた形でステータスを表現しており、緑であれば正常、黄色は警告、赤は異常な状態だということが一目で分かるようになっています。「経験豊富な有識者でなくとも、誰が見てもどの値が問題になっているのか、サービスレベルの状態が一目で分かるようになりました」と鈴木氏は評価します。なお現在の運用は、Splunkフォワーダーにて各サーバーのリソース情報やログ情報をリアルタイムに収集、1日で収集されるおおよそ100GBのログを数日間保持したうえで、一部はアーカイブしたうえで順次破棄する運用となっています。

また、異常が発生すれば相関分析が可能なDeep Diveへドリルダウンすることで時系列での相関分析が可能となっており、原因究明が迅速に行えるようになっています。「Splunk IT Service Intelligenceが素晴らしいのは、Splunk内だけでなく、別の環境にもドリルダウンできる点です。Splunkはシステム目線に特化していますが、別のサービス目線での可視化ツールも導入しており、そちら側の状況もすぐに把握できます。複数あったダッシュボードの入り口を一つにできたのはとても大きい」と鈴木氏は高く評価します。

Splunk IT Service Intelligenceについては、ほとんどGUIでの設定が可能のため、1度のハンズオンでどんなことができるのかを学び、環境設定はマニュアルを見ながら半日ぐらいですぐに行うことができましたと鈴木氏は語ります。「すでにSplunk Enterpriseを長年利用してきたことで、どのステータスがどんな状態なら警告を出すといったKPIなど指標に関するノウハウは社内にはありましたので、すぐに環境を作ることができました」。

ログ検索の柔軟性が大きな魅力、SPLの使い勝手の良さも大きな利点

Splunkの一番の強みについては、ログ検索の柔軟性だと鈴木氏は断言します。「Splunkのような可視化ツールは他にもありますが、私の知る限り、ログ検索の柔軟性は断トツに優れています。通常であれば、マシンデータを事前に解析したうえでマッピングして取り込む必要がありますが、Splunkはそのまま取り込むだけで、あとから分解して分析に活用できます。わざわざ事前にマッピングやインデックス化する必要がないのがありがたい」。また、サーチ処理言語であるSPLの使い勝手がよく、一般的なエンジニアであればすぐに使えるような代物だと評します。「SQLとUNIXシェルを足して2で割ったような感じです。実際にマニュアルでSQLとの違いも出ていますし、すぐに理解できます。また、厳密に記述せずとも使える点も助かっています。単語だけ検索窓に入力すれば関連したログ情報がすぐに出てくるため、カジュアルな使い方が可能です」とその魅力を語ります。

Splunk IT Service Intelligenceでシステムステータスを可視化したことで、テクニカルなエンジニアではない管理職や経営層であってもパッと見て状態が分かるようになったのも1つの効果だと説明します。

「エンジニア出身の管理職には、相関分析画面となるDeep Diveが好評です。以前はシステムのレポートで時系列を合わせて確認するのが大変で、その微調整を管理職自らやっているケースも。今はDeep Diveで時系列がきちんと把握できるようになりました」と鈴木氏は評価します。個別にレポート作成せずとも、Deep Diveをお互いに見つつ新たな情報を追加するなど、コミュニケーションの基盤として同じ目線で確認することが可能になっています。しかも、これら高度な分析が片手間で行うことができる点もSplunkの見逃せないポイントの1つだと鈴木氏。

ログ収集の範囲を広げながら、機械学習への取り組みも加速

今後については、現在サーバーを中心に収集しているログの範囲をネットワーク機器も含めて拡大させていきたいと鈴木氏は語ります。

「何かあった場合、各アプリケーションのログからでも想像はできるのですが、おそらくネットワークに起因するだろうということで止まってしまうことも。さらに詳しく見ていくためにも、システム全体の可視化を進めていきたい。また、Splunk IT Service Intelligenceが持つ機械学習の機能はまだ十分に使いこなしていないため、今後はうまく取り入れていきたい考えです。各システムのKPIとなる閾値の設定などは過去の知見が生かされていますが、機械学習を使って微調整しながら、システムステータス全体の可視化をさらに進めていきたい」と今後について語っていただきました。

Splunk無料トライアルまたはCloudトライアルをダウンロードしてお試ください。Splunkは、クラウドとオンプレミスのオプションを備えており、ご利用容量の規模に応じて、ご要望に合うデプロイメントモデルをお選び頂けます。



詳細はこちらからお問い合わせください: https://www.splunk.com/ja_jp/talk-to-sales.html

https://www.splunk.com/ja_jp