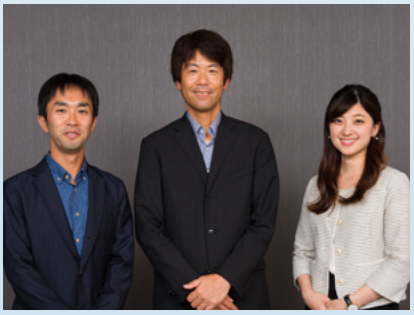
splunk>
大容量ログデータ分析ツール

SCSK

セキュリティ、運用監視、業務の可視化など、多様な活用が行えるログ解析ツールSplunkの実力

SCSK株式会社

2011 年 10 月、住商情報システム株式会社と株式会社 CSK との合併により誕生した IT サービスベンダー。システム開発から IT インフラ構築、IT マネジメント、BPO（Business Process Outsourcing）、IT ハード・ソフト販売まで、ビジネスに求められるすべての IT サービスをフルラインアップで提供。ビジネスの新価値創造とグローバル展開をサポートしている。お客様の求める未来を「共に創る」ことで、未来に向けて成長し続ける企業となることを目指している。



SCSK株式会社
プラットフォームソリューション事業部門
事業推進グループ
ミドルウエア技術部長
ITエンジニアリング事業本部
営業推進部　第三課長
内野 靖之 氏 （写真中央）

SCSK株式会社
プラットフォームソリューション事業部門
ITエンジニアリング事業本部
営業推進部 第三課 課長代理
事業推進グループ
開発技術部 第一課
樋口 貴志 氏 （写真左側）

SCSK株式会社
プラットフォームソリューション事業部門
ITエンジニアリング事業本部
ミドルウェア部　第六課
西岡 加奈 氏 （写真右側）

SCSK は、自社で独自に開発したソフトウェアプロダクトサポートサービス「CarePlus Software Product Support Service」（以下 CarePlus SPSS）のコアとなるテクノロジーとして、ログ解析ツール「Splunk Enterprise」（以下、Splunk）を採用している。データ分析・解析に注目が集まる中、膨大なマシンデータを収集、監視、分析、可視化することが容易に行えるというSplunkを使うことによって、どのようなことが可能となるのだろうか。実際に CarePlus　SPSS で Splunk を利用している内野 靖之氏と樋口 貴志氏、Splunk の製品担当である西岡 加奈氏に話を伺った。

サポートプラットフォームの中核として採用されているSplunk

CarePlus　SPSS は、多くの製品を扱っている SCSK が顧客の利便性を向上させる為に、、クラウド上で製品サポートサービスを提供するプラットフォームとして 2015 年 6 月にリリースし、2017 年 1 月からは、社外のソフトウェアベンダーなどにも CarePlus　Cloud として販売が開始されている製品だ。「これまでは電話やメールで行っていたサポートを、もっと効率的にクラウドを使って行えないかと考えたのが CarePlusCloud のプロジェクトの始まりです」と話す内野氏は、Splunk はログを収集することによって、可視化やリアルタイム分析の機能を持っており、セキュリティ、運用、可視化などの課題を解決できる製品だと説明する。CarePlusCloud では、Splunk を全面的に採用することによって、障害発生時に原因を短時間で発見したり、セキュリティのインシデントが発生したときに進入経路などを分析したり、アプリケーションの操作ログを使って行動パターンを分析するといったことに活用しているという。

一方、数年前から Splunk を利用していたと話す樋口氏は、Splunk が導入しやすく、ログだけでなく、データベースの分析を行えることが採用の決め手となったと話す。「内部システムの監視、アプリケーションの操作ログ、セキュリティなど、さまざまな用途で Splunk を使えることが最も便利ですね。それぞれのシステムを別々に入れてしまうと、管理や運用が煩雑となってしまいますが、Splunk だけでさまざまなことが行えることが一番の魅力だと思います」。

実際に、社内利用で Splunk を搭載した CarePlus SPSS を使うことによって、大きな効果を得ることができたと樋口氏は話を続ける。「SCSK では、約 400 ほどの製品を扱っていますが、それぞれの部署がサポートを行っており、保守や運用のやり方も微妙に異なっていました。CarePlus SPSS を利用することによって、保守や運用を統一して行うことができるようになり、問い合わせの数や応対にかかった時間を分析することによって、ピークに合わせて人を配置したり、チーム内の人に対する負荷を均一化することができるようになりました。たとえば、ERP などの製品では、年末調整に伴って 11 月くらいから問い合わせが殺到することがわかったので、それに合わせて年末調整に関する FAQ を用意することで、問い合わせが 20 ～ 30%減り、サポートの負荷を低減させることができました」。

Splunk では、さまざまな分析が行えるため、たとえば、特定のユーザーがログインエラーを頻発させているなどの不正アクセスの兆候などをリアルタイムで監視することが可能だ。また、よく読まれる FAQ や読まれない FAQ を分析して、より役に立つ FAQ に再編することで問い合わせの件数などを減らすことにも利用できる。さらに、保守の売上高の伸び率や顧客数などをダッシュボードで可視化することによって、伸びているプロダクトの人員を増やしたり、伸びていないプロダクトを縮小化するなどの経

splunk>

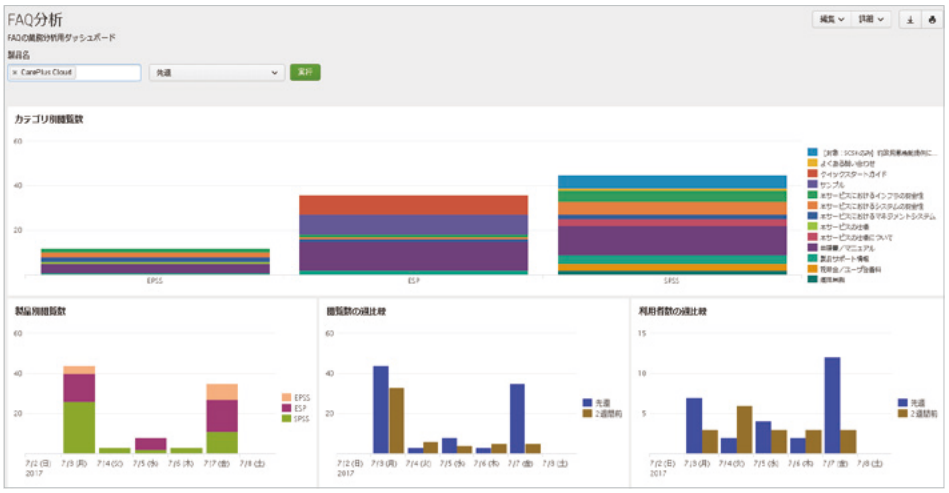
大容量ログデータ分析ツール

営判断を行うためにも、Splunkは役に立つという。「Splunkのインストールは非常に簡単で、フリー版のSplunkを活用されている企業もあります。我々は、導入だけでなく、要望に合わせてダッシュボード画面を作りこんだり、アラートの設定を行うなどのご支援を行っています。また、トレーニングなどを受けていただくことで、導入後も新たな分析を行えるようにし、運用の負荷がかからないようにするメニューも用意しています。セキュリティやサーバの死活監視といった用途だけでなく、工数監視などのビジネスよりの分析も行え、お客様が取り込むデータの使い方次第で、さまざまな分野で活用できることがSplunkの一番の魅力ですね」と西岡氏は説明している。

データの準備に手間をかけずにダッシュボードで可視化できる

優れた分析ツールを用意できても、分析するためのデータを準備するのに時間がかかってしまうようでは、分析をできるようになっても古いデータを使うことになり、最適な分析を行うことはできない。Splunkでは、データの準備も行いやすく、すぐにダッシュボードで可視化できると内野氏は説明する。「課題解決のために分析を行おうとするときには、どのようなインプットが必要となるかが問題になります。Splunkのサーチコマンドは使いやすく、理解しやすくなっているため、イメージしたものを形にするのに非常に役に立ちます。また、ダッシュボードを自由に作れるBI製品などがありますが、ダッシュボードを作るためのデータを加工するための手間がかかるものがほとんどです。Splunkでは、生のデータを正規化するなどの手間をかけずにダッシュボードに取り込んで活用できるほか、データの意味づけも文字や数字の配列を見てある程度自動的に行ってくれるため、手間をかけずにすぐに分析を行うことができます。ダッシュボードを更新する際も、再加工などを行う必要がなく、すぐに最新のデータを使った可視化が行えるため、非常に便利ですね」。

SplunkによるFAQ分析の画面例



今後について樋口氏は、「お客様にSplunkを使った役に立つ情報を、どれだけ提供していけるかが課題ですね。要望に応じたダッシュボードを提供したり、製品側やユーザーだけでなく、その間に立つ代理店にも有益な情報を提供できるようにしていきたいと考えています。ステークホルダー全員に、可視化されたリアルタイムの価値ある情報を提供していきたいですね」と話す。また、西岡氏は、Splunkに興味を持っている人に対して、次のようなメッセージを話してくれた。「Splunkは、セキュリティ対策のために導入されるケースが多いのですが、特定の用途のためだけに導入するのではなく、用途を絞らずにさまざまな課題解決に役立つ分析ツールとして導入することをお勧めしています。我々も、セキュリティや運用監視だけでなく、ビジネスの課題の可視化や人的リソースの最適化などのさまざまな活用方法があることを示していく必要があります。Splunkには、Appsというダッシュボードのテンプレートがあるので、業界や業種、個々の課題に合わせた独自のAppsを作成し、SCSKならではの価値を付加させSplunkを提供していこうと考えています」。

Splunk（スプランク）

あらゆるITシステムから生成されるマシンデータを収集し、インデックス化することによって、シンプル、スピーディ、フレキシブルに検索、分析、可視化できるツール。リアルタイムデータとヒストリカルデータの両方を同じインターフェースで検索し、必要な情報を高速にピックアップでき、検索結果から簡単にグラフや表を作成して、収集した既存データから想定される傾向の分析、予兆を行うことが可能となっている。複数の分析レポートをまとめた、グラフィカルでインタラクティブなダッシュボードを作成でき、マルチテナント機能でユーザーごとに利用するダッシュボードを設定できる。

SCSK SCSK株式会社

プラットフォームソリューション事業部門
ITエンジニアリング事業本部 ミドルウェア部
〒135-8110 東京都江東区豊洲3-2-20 豊洲フロント
e-mail: splunk-sales@ml.scsk.jp　TEL: 03-5166-1673　Web: https://www.scsk.jp/product/common/splunk/