日立ソリューションズ

HITACHI
Inspire the Next

ビッグデータ利活用基盤ソリューション

Splunk

導入事例

株式会社ブロードバンドセキュリティ 様

様々な機器から出力される膨大なログデータから新たな脅威を検知、分析するSIEMとして、セキュリティ運用の現場に「Splunk」を活用。

**お客様のセキュリティ運用をアウトソーシングする「マネージドセキュリティサービス」をはじめとし、様々なセキュリティサービスを提供する、株式会社ブロードバンドセキュリティ。
同社は、SIEM（セキュリティ情報およびイベント管理）機器のサポート切れにともない、新たな機器の選定を開始、拡張性と柔軟性に優れたSIEMとして、ビッグデータ利活用基盤ソリューション「Splunk」を採用しました。**

BBSec

設　　立	2000（平成12）年11月
本社所在地	東京都新宿区西新宿8-5-1 野村不動産西新宿共同ビル4F
事 業 内 容	マネージドセキュリティサービス、セキュアメールサービス、セキュリティ認証取得・準拠支援、脆弱性診断サービス等のセキュリティサービス
U　R　L	http://www.bbsec.co.jp/

従来からの課題

従来のSIEM機器のサポート終了により、同社の新たなサービス基盤となりうるSIEM機器の選定を開始

同社のマネージドセキュリティサービス（MSS）は、SOC（Security Operation Center）によるセキュリティ運用サービスで、お客様のネットワークから収集したログデータを、専門技術者が解析、24時間365日体制で監視し、セキュリティの脅威に備えるサービスです。

「当社のMSSの強みは、SOCの運用で培った最新技術と防御モデルをもとに収集、分析した最新情報を、約100社、300事業部門を超える導入先のお客様にいち早く展開できる点です。また、SOCの運用では、ファイアウォールからWAFまで、約20種類のネットワーク機器を取り扱っており、マルチベンダーで様々な機器を取り扱うことで多くの知見を蓄積している強みがあります」（安藤氏）

「今までSOCで使ってきたSIEMが2014年末でサポート終了になるため、機器を新たに入れ替える必要がありました。SIEMは様々なネットワーク機器やセキュリティと接続され、収集したログ情報に基づいて、異常を検知し、その対策方法を通知する仕組みです。ですから、機器を選定、購入して終わりではなく、既存の環境を新たなSIEMに適用させる必要がありました」（戸崎氏）

「既存の環境に柔軟に適用できる点に加え、課題として挙げられるのが拡張性の問題です。従来のSIEMが上限に近いパフォーマンスで運用していたので、今後のビジネスを考えたときに、監視システムの規模の拡大に対応できる拡張性の高いSIEM機器を選ぶ必要がありました」（安藤氏）

株式会社ブロードバンドセキュリティ
取締役 CTO
安藤　一憲 氏

こうした課題をもとに、2013年夏頃よりSIEM機器の検討を開始しました。

導入の経緯

従来のシステム構成に適用可能な柔軟性と、容易にスケールアウトできる拡張性の高さが決め手

SIEM機器の選定に際しては、複数の競合製品の中から候補を絞りました。

「従来のSIEM機器の後継モデルや、その他にも複数の機器の中からコストや性能面を比較して検討していきました。ポイントとなったのは、上述のような柔軟性や拡張性、そして国内での導入実績です。これらの要素とコスト面を総合的に勘案しました」（戸崎氏）

「現場での選定とは別に、私の方では、Splunkジャパンの中村社長と知り合う機会があり、そこで、SplunkをSIEMとして活用する事例が出はじめている情報をキャッチしていました。Splunkはスケールアウトできる拡張性の高さが魅力的でした。そこで、Splunkを検討候補に加えるようアドバイスしました」（安藤氏）

では、SIベンダーとして日立ソリューションズが選ばれた理由はどのあたりにあるのでしょうか。

「今回の案件は、既存の環境にSplunkを適用させるためのシステム開発に重きを置いていたので、SI力に定評のある日立ソリューションズに相談しました。これまでもメールセキュリティのシステムでお付き合いがありましたので、実機のデモを手配いただくなどスピーディに対応いただきました」（鈴木氏）

「日立ソリューションズには、従来のSIEM機器で可能だった機能を、Splunkで実現できるかどうか、要件に対する技術的な検証にしっかり取り組んでいただきました。従来SIEMの膨大な量の全機能一覧をこちらから提示しました。その機能の一つ一つがSplunkで実現できることがわかり、開発を安心してお任せできました」（戸崎氏）

2014年3月頃に機器とベンダーの選定を終了し、プロジェクトがスタートしました。

導入時の取り組み

短期間での開発を可能にした日立ソリューションズのインテグレーション力

実際の開発が始まったのは2014年6月頃でした。

「開発時に一番力を入れたのが、いかに従来のSIEMの機能をSplunkで実現するかという部分です。MSSは、SIEMだけで運用されているわけではありません。様々なネットワーク機器やセキュリティ機器と接続され、『SOCポータル』と呼ばれるお客様とのやり取りの窓口となる弊社のこれまでのノウハウを結集した独自開発のシステムと連動しています。ですから、従来のシステム構成は変えずに、SIEMだけを入れ替えることに注力しました。

具体的には4点あります。1つ目はログの取り込み機能。多種多様な機器と接続されるので、ログ取り込みのルールが多く、この部分の機能の開発です。2点目は、アラート検知機能。ログを見てこれはアラートと判断する、しないというBBSecの運用経験から導き出した細かいルールが200種類以上あります。これを1つずつ丹念に移植しました。3点目は、アラートを通知する機能。検知したアラートをSOCポータルに通知する機能を作り込みました。そして、4点目がレポーティング機能。ログを集計してSOCポータルに出力する機能です」(鈴木氏)

結果的に、4つのシステム開発のうち3つを標準機能で、残りの1つは個別開発で再現することに成功しました。これは、Splunkの最大の特長でもある柔軟性による大きなメリットでした。

「日立ソリューションズには、多種多様な機器を取り扱っている実績があるため、私たちが従来使っていたSIEM機器にも精通しており、非常にきめ細かく対応していただきました。これだけの短期間の開発スケジュールでリリースできたのは、Splunkの柔軟性と、日立ソリューションズのSI力が遺憾なく発揮されたおかげだと考えています」(戸崎氏)

株式会社ブロードバンドセキュリティ
マネジメント・サービス ビジネスユニット
ディレクター　戸崎　節雄 氏

2014年10月、Splunkは、従来機器との並行運用という形でリリースされ、2015年1月から、正式にSplunkに切り替えられ運用が続けられています。

導入の効果

担当者の負荷低減と作業標準化、お客様の利便性提供とシステム安定稼働に寄与

「業務効率化という点では2点あります。1点目は、アラート通知の除外設定です。これは複雑なルールの組み合わせで対応するため、従来機器ではSOCのエンジニアでないと対応できませんでしたが、今ではSOCのオペレーター人員でも除外設定が対応可能になりました。

2点目が、ログ検索とログ統計です。従来のSIEM機器では、生ログを出力して、これをExcelで加工、集計する作業が必要でした。これが、Splunk上で集計から統計作業まで行うことが可能となり、オペレーターによる対応が可能になったため、業務効率化と即時レスポンスというお客様への利便性提供につながっています」(鈴木氏)

株式会社ブロードバンドセキュリティ
マネジメント・サービス ビジネスユニット
MSテクノロジー部 エンジニアリンググループ
マネージャー　鈴木　暢 氏

「オペレーターでも対応できる業務が増えたことにより、エンジニアやアナリストは、Splunkをより高度に活用して、セキュリティをより強固にするために、有効な情報収集や解析ができないかという発想ができるようになりました。いわば、Splunkを触媒にして、私たちのサービスが変化してきています」(安藤氏)

「Splunkのアラート通知は安定しており、スペック的にも余裕があるため、システム負荷を心配することなく安心して運用できます。」(戸崎氏)

「Splunkはコマンドラインによるオペレーションなので、GUIのインターフェースに慣れた担当者には、導入当初は戸惑いがあったようです。これについては、業務に携わる約20名の担当者に対し、事前に日立ソリューションズに操作レクチャーをしていただくなどして、スムーズに移行することができました。また、コマンドラインの良いところは、作業や機能を定型化し再利用できるところです。定型作業を標準化することが容易にできるため、結果的に作業ミスの軽減にもつながるメリットがあります」(鈴木氏)

今後の展望

テキストで出力されるあらゆる情報を「資産」として管理、統合できる基盤として

「今後は、複数の機器からの出力内容を組み合わせて、相関、傾向分析からアラート通知を出したり、過去の傾向と比較して異常を検知したりといった、一つ上のレベルの分析の可能性を模索しています」(鈴木氏)

「Splunkは、私たちのサービス基盤になりうる技術だと思っています。新たな適用範囲や、お客様への付加価値提供にSplunkが一役買っています。また、Splunkは、SIEMに限らず、あらゆるテキストの情報をデータ資産として蓄積、管理、統合できるのではというビジョンを持っています」(安藤氏)

「日立ソリューションズとは、当社がカバーできない国内地域のお客様をサポートしていただいたり、得意のインテグレーション領域で、私たちの事業をお手伝いしていただくなど、連携して案件を担当していくパートナーとして、今後も協業していきたいと思います」(戸崎氏)

こちらのQRコードより、本事例の詳細ページをご覧いただけます。
http://www.hitachi-solutions.co.jp/splunk/case01/

商品・サービスに関するお問い合わせ・ご相談受付

【電話による受付】
0120-421-126 [通話料無料]
受付時間 10:00～17:30　月曜日～金曜日(祝日、弊社休業日を除く)

【メールによる受付】
webmaster@hitachi-solutions.com

本カタログ掲載商品・サービスの詳細情報
http://www.hitachi-solutions.co.jp/splunk/

このカタログは資源保護の為、再生紙を使用しています。

H27K-04-00	2015.06

株式会社 日立ソリューションズ
http://www.hitachi-solutions.co.jp/