# 多くのSaaSを安全に利用するためのSIEM基盤を整備 少数精鋭で運用している企業こそ導入すべきSplunk Cloud

## 概要

日光ケミカルズは、コロイド化学と皮膚科学をベースとしたスペシャリティケミカル分野において専門性を有し、多角的企業グループであるニッコールグループの中核企業。

1946年に創立後、安全性や環境への配慮といった社会的責任を重視しながら、業界の発展に向けた多岐にわたる活動を実施。社員一人ひとりが創造性を育み、発揮することで、化粧品・医薬品・食品などの業界へ、一歩先を考えた製品やサービスを生み出し、マーケットニーズに応じたソリューションを提供しています。

同社では、2011年に発生した東日本大震災を契機に、事業継続の観点から災害復旧可能な基幹システムを構築するべくDR環境の整備を行っています。AWSにて基幹システムとして採用しているSAPを運用しながら、業務システムとしてのG suiteやオンラインストレージのBox、ネットワーク管理のCisco Merakiなど、積極的にSaaSを利用しており、事業継続を実現しながら生産性向上に寄与する環境づくりを推進しています。これら各種サービスを安全に利用するために外部のSOCサービスを利用していますが、このSOCサービスがアラートの抽出から分析までを行う基盤として活用しているのが、基幹システムで利用しているAWSをはじめ、各種SaaS環境のログを集約しているSplunk Cloudです。

## サービスの健全性担保や証跡管理などを強化するための仕組みが必要だった

東日本大震災を契機に、多くの業務システムをクラウド上で利用できるSaaSに移行し、基幹システムをはじめ、社内にはほぼサーバを設置せずにクラウドを中心としたシステム基盤を整備している同社ですが、基幹システムをAWSに移行する以前は、資産管理ツールを用いてクライアント環境の操作ログを中心に取得する程度で、サービスの健全性確保や貴重な情報資産が守られているかどうかの証跡管理などについては十分でない状況が続いていました。「情報セキュリティの重要性は理解していましたが、AWSへの移行プロジェクトが本格化していたこともあり、すぐに着手できなかったのが実態です」と情報セキュリティ管理室 東原 雄一氏は当時の状況を振り返ります。

またAWSへの移行とともに、積極的にクラウドサービスを利活用する方針が採用されたことで、さまざまなクラウドサービスが現場レベルで一気に導入されることに。その結果、企業にとって重要なガバナンスが十分に実現できないという課題も顕在化していたと説明します。グループ内に研究部門を持っているため、企業における貴重な情報資産の持ち出しなどを防ぐ意味でも、これまで以上に状況が可視化できる環境づくりに取り組む機運が高まっていったのです。

そこで、これまで運用してきた資産管理ツールでのクライアントログの収集だけにとどまらない、広範囲なログ収集が可能な仕組みを検討することになったのです。

## 少人数でも運用でき、AWSとの親和性の高さや豊富なAppsが大きな魅力に

そこで東原氏が最初に注目したのが、ビッグデータ分析ソフトウェアのSplunk Enterpriseでした。「2015年当時はSplunk自体を知りませんでしたし、SIEMという概念も理解していませんでした。ちょうどパートナーからの紹介でSplunkに出会ったのがきっかけで興味を持ったのです」と当時を振り返ります。特に大きかったのは、AWSの連携が柔軟にできる点でした。「我々はAWSを業務のプラットフォームとしてフルに使っているため、AWSからの各種ログがAPI経由で柔軟に取得できるのは大きかった」と東原氏。

また大前提として、当時は東原氏が最小限のリソースで仕組みの導入を進めていたこともあり、使いやすさや後々のインテグレーションのしやすさなどは選択の大きなポイントになっていたといいます。「ログ収集までに時間のかかるような仕組みは避けたかった。その点、Splunkにはすぐに業務に適用できるAppsをはじめ、社内のシステムが増えたとしても柔軟に拡張できるAdd onが豊富です。少人数であっても運用しやすいと考えたのです」と評価します。市場的にもSplunkが注目され始めていたことで、その流れに乗っていくことを念頭に導入を決断したのです。「周回遅れのソリューションを導入すると、結局後で保守費用などがかさんでしまうこともあり、時流に乗ることは重要です。Splunkはエコシステムも充実しているため、失敗しにくいと判断しました」と東原氏。

ただし、Splunk Enterpriseを運用するなかでの課題も顕在化してきたと東原氏。「Splunk自

NIKKO CHEMICALS

### 業種

- 化学メーカー

### 活用事例

- 安全なクラウド利用に向けたログ取集基盤

### 課題

- 業務で利用するSaaSの健全性の担保や証跡管理が十分でなかった
- 少人数でも多くのSaaSを安全に活用するための仕組みが必要だった
- バージョンアップなど運用の負担を軽減したかった
- ログ収集するためのサーバのサイジングに苦労した
- 複数のSaaSの利用状況を相関的に分析する基盤が必要だった

### 導入効果

- 業務で採用しているSaaSを安全に利用できる環境が整備できた
- 各SaaSのログを集約、相関的な分析が可能になった
- SOCサービスの監視ポイントを集約、最小限のコストで運用できるようになった
- 運用において足りないログが可視化できるようになった
- 業務に応じたSaaSの利用拡大につながった

### データソース

- AWSにおけるConfigCloudTrail、CloudWatch Logs、S3などの各種ログ
- IDS/IPS
- Cisco Meraki
- Box
- Okta
- G Suite
- Office 365
- Netskope
- Sentinel One

### ご利用製品

- Splunk Cloud

日光ケミカルズ株式会社
情報セキュリティ管理室
**東原 雄一氏**

体のバージョンアップが頻繁に発生することは、実は非常にいいことではあります。ただし、私一人で運用しなくてはならないため、手間のかかる作業はできるだけ避けたいと考えていたのです」。実際にバージョンアップ自体が進められない事態も発生していたことで、心理的な負荷もあったと語ります。また、サイジングに関しても心理的な負担が大きなものになっていたと東原氏。「Amazon EC2における仮想サーバのスペックがギリギリの状態が続いていたものの、なかなか手を付けることができずにいたため、いつも引っかかっていたのです。この負担を何とか軽減できる環境が欲しいと考えていました」。

そこで選んだのが、Splunkの機能がSaaSとして利用できるSplunk Cloudでした。「SaaSとして利用できるサービスがあることを聞き、今の課題に応えてくれるものだと考えたのです」。実はIaaS環境としてのAWS上で運用していたころは、スペック上の課題もあって最小限のログ取得にとどまっていましたが、SaaSによってサイジングの課題が解消でき、多くのログが負担なく収集できる環境が整備できるようになりました。SaaSであればバージョンアップのためにシステムを止める必要がなく、メンテナンスフリーになる点も高く評価したのです。

結果として、AWS上で運用してきたSplunk Enterpriseから、SaaSとして利用できるSplunk Cloudに移行することで、これまで以上に広範囲なログ取得が可能な環境を整備することに成功するのです。

## 利用するSaaSのログをSIEMに集約、外部のSOCによる監視サービスを活用

現在は、基幹システムが稼働するAWSの各種ログをはじめ、グループウェアとして活用しているG SuiteおよびOffice 365、オンラインストレージのBoxや無線有線含めたネットワーク管理が統合できるCisco Meraki、仮想デスクトップ環境を実現するAmazon WorkSpaces、シングルサインオンのOkta、クラウドセキュリティとしてのNetskope、エンドポイント対策としてのSentinel Oneなど、セキュリティに関連したさまざまなログをSplunk Cloudにて取得しています。このSplunk Cloudに収集されたログを外部のSOCサービスを利用して24時間対応で監視、分析しており、何かあればアラートがメールやSlackにて通知される運用です。ログ自体は全て合わせると1日10GBほどのサイズとなっており、ログを保持する期間も用途に応じた形で運用しています。Splunk Cloudに直接流し込めないログは、AWS上にSyslogサーバを設置して運用していますが、今後はSplunkがクラウド上にインスタンスを用意しているInput Data Managerと呼ばれるフォワーダを経由して取得していく計画です。

## 相関的な分析が可能になり、現場が求めるSaaSの利用拡大も容易になった

Splunk Cloudに多くのログを集約できたことで、SOCサービスが監視するノードが1か所になることでコストを最小限におさえつつ、利用しているSaaS を相関的に分析、判断できるようになり、これまで以上にセキュアな形で運用できるようになったと東原氏は高く評価しています。「利用しているSaaSのログを横串で見ることができるため、インシデントの検知も迅速になるだけでなく、SOCサービスからのアラートも相関的な状況からチューニングできるようになったのは大きい」。また、SIEMであるSplunk Cloudにログを集めることで、ログの過不足が判断できるようになったことも評価の1つに挙げています。「当初はAWSのログだけで十分だと考えていましたが、実際にはネットワーク側の問題でアラートになっていたケースが明らかに。そこでCisco MerakiのログもSplunk Cloudに入れるようになるなど、不足したログが明確になったのは大きな効果です」と東原氏。Splunk Cloudがあることで、現場の要望に応える新たなSaaSも安全に展開できるようになったと評価します。「今では、Splunk Cloudでログが取れないSaaSは導入しないというのが判断基準になっています」。

## 少数精鋭で運用するからこそSplunk Cloudが有効なツールに

Splunkが提供するソリューションについては、安定して利用できるだけでなく、使いやすさについても高く評価しています。「クラウド環境であってもAppsが自分で導入でき、サイジングやバージョンアップに関する心理的な負担もなくなっています」と東原氏。タスクの自動化が可能なSplunk Phantomや機械学習によってスコアリングすることでリスクが軽減できるSplunk UBAなど、Splunkの企業ビジョンにも共感が持てると東原氏は評価します。「SaaSを積極的に利用する我々にとって、SIEMは安全を担保するために欠かせないプラットフォームといっても過言ではありません。AWSをプラットフォームとして選択したような感覚でSplunkを利用しているといえます」。

特にSIEMというソリューションについては、少数精鋭で運用している企業こそ導入すべきだと東原氏は力説します。「DXや働き方改革などがもてはやされていますが、それらを進めるためには安全の担保が必要で、まさにSIEMは欠かせないソリューションの1つ。運用人数が多ければSaaSそれぞれに担当を付けて監視することはできるかもしれませんが、それではとても非効率。我々のような人数規模の企業だからこそ、Splunkの価値は高いものになるはずで、決して高いソリューションではないことがわかるはず」と東原氏。

## 運用監視などオペレーション系のログも集約していく

今後については、まだログを集約していないWeb会議をはじめ、Microsoft IntuneおよびJamfなどモバイルセキュリティなどについても集約していく予定となっています。また、リアルタイム性が求められる運用監視などのオペレーション系のログは別の仕組みで運用していますが、いずれはSaaS型の監視プラットフォームとしてSplunkが買収したSignalFxへの切り替えも視野に入れていると語ります。

またログについては、取得しすぎてしまうと当然コストに影響するだけでなく、従業員のプライバシー配慮も考慮し、精査していく必要があると指摘します。「情報のマスキングも含め、ログの取得についてはさらに検討が必要だと考えています」と東原氏に語っていただきました。



20-13742-Splunk-IT-Nikou Chemical-A4-102-CS-JP