クラウド事業のITシステム監視、運用を自動化
障害一次対応の速度向上にSplunkが大きく貢献

課題

事業規模の拡大に伴い監視対象システムが大規模化、アラート通知数も比例して増加傾向にある。従来の運用監視基盤では障害一次対応に時間を要するようになり、基盤の刷新が必要とされていた。

導入効果

従来の運用監視基盤をSplunkに置き換え、周辺のサブ監視システムからのアラートを集約し、構成情報と合わせて解析することにより、影響を受けたシステムの特定や顧客への通知、対応部門へのエスカレーションに至る、障害一次対応の自動化と効率化を実現した。

IDCFrontier

業種・業界: 通信

ソリューション: プラットフォーム, IT運用

データドリブンの成果

- 障害一次対応の所要時間を、従来の6分の1へと短縮
- 運用担当者が必要とする情報を絞り込み、ダッシュボードへの可視化を実現
- アラートと対応手順の関連を自動的に判別可能に

IT運用監視の最適化、障害一次対応のスピード化や品質向上に「Splunk IT Service Intelligence」を採用

データセンター事業、クラウド事業を手がける株式会社IDCフロンティアは、首都圏、東日本、西日本で大規模データセンターを運用し、ネットワークセキュリティや運用監視を含む高品質なデータセンターソリューション、クラウドコンピューティングおよびネットワークサービスを提供しています。

顧客企業におけるITシステムのクラウド化が進むにつれ、同社のクラウド提供基盤も拡張を続け大規模化。ビジネス環境の変化に迅速に対応可能なIT運用監視に対するニーズが高まっていました。

一方で、同社が長年利用してきた従来の運用監視システムでは、老朽化による様々な問題が顕在化していました。たとえば、クラウド提供基盤の大規模化により仮想マシンの台数が増えることで、監視対象のシステムから発せられるログは大量になります。アラートに関連する大量のログをより効率的に集約、整理し、影響範囲を迅速に特定する必要があったのです。

そこで同社は、IT運用監視のさらなるスピード化、障害の初動対応品質の向上等を目的に、「Splunk Enterprise」「Splunk IT Service Intelligence (ITSI)」を導入し、運用を開始しました。

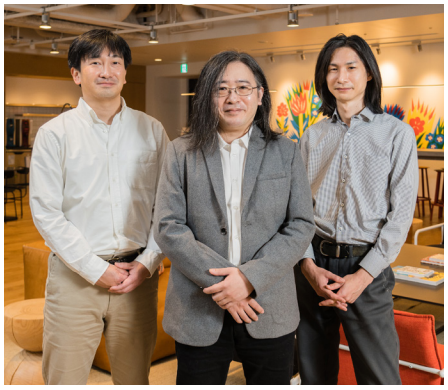
IT運用監視を自動化し、障害一次対応の最適化を図る仕組みが必要だった

既存の運用監視基盤について、同社 エンジニアリング統括本部 クラウドエンジニアリング本部 本部長の松本 和久氏は、「現在の運用システムで運用業務を続けていく中でビジネス環境が大きく変わった。また、サービスシステムの大規模化や高品質な運用が求められる中で、これまで様々な措置を講じてきたが、運用システムのアーキテクチャも運用現場そのものも従来の仕組みでは対応しきれなくなってきた」と課題を話します。

システムが大規模化する中で、障害発生時の対応に時間が掛かっていた状況がありました。同社 エンジニアリング統括本部 クラウドエンジニアリング本部 プラットフォーム開発部 運用基盤グループの阿部 佑介氏は、「従来は障害のアラートに対して、人力による運用でカバーしてきていましたが、監視対象のシステムが増え、大量かつ同時にアラートが通知される状況をカバーしきれなくなった」と話します。

たとえば、障害発生時に、影響を受けているお客様に連絡するために、どのお客様が影響を受けているか、どこに連絡するべきかを調べるのに時間を取られていました。「大量のアラートに対する一次対応のスピード化を実現するためには、人力で対応する領域を増やすのではなく、自動化や効率化を進めていくアプローチが必要だった」と阿部氏は述べています。

そして、そのためには、既存のシステムや運用プロセス、体制では限界があり、「システムに手を入れる必要があり、課題解決に向け、アーキテクチャから運用監視基盤を再設計し直そうと検討を開始することになった」ということです。



柔軟性、拡張性が決め手となり Splunk Enterpriseを前提とした 「Splunk IT Service Intelligence」を採用

次期運用監視基盤の選定は2020年7月ごろより本格化しました。阿部氏によれば、「従来システムはITIL (Information Technology Infrastructure Library) をベースに構築していたため、当初はITILを中心にインシデント管理や構成管理データベース (CMDB) といったカテゴリーで運用監視基盤を探していた」と話します。

一方で、松本氏は、「次期運用監視基盤のコンセプトを検討していく中で、サブ監視システムから通知されたアラートをルールに従って分類し、構成情報を関連付け、運用者が必要とする情報に加工し伝えるというプロセスの本質を考えたときに、ログ分析プラットフォームをシステムに組み込むことで新しい運用のあり方を実現できるのではないか

株式会社IDCフロンティア
エンジニアリング統括本部
クラウドエンジニアリング本部
本部長
松本 和久 氏

株式会社IDCフロンティア
エンジニアリング統括本部
クラウドエンジニアリング本部
プラットフォーム開発部
運用基盤グループ
阿部 佑介 氏

株式会社IDCフロンティア
エンジニアリング統括本部
クラウドエンジニアリング本部
プラットフォーム開発部
運用基盤グループ
渡邉 一雄 氏

と考えた」と述べています。

では、Splunk 選定の決め手となったポイントはどのあたりにあるのでしょうか。阿部氏は、大きく「機能面」「ライセンス体系」「拡張性」の3点を挙げます。

まず、「機能面」については、「従来システムでできていた機能をSplunkでも実現できることがPoCなどを通じて検証できた」と説明します。Splunkのエンジニアの対応、手厚いサポートも選定の一因となりました。

2つめの「ライセンス体系」は、従来製品は管理対象の台数に応じた課金体系だったということです。同社のようなクラウドサービス事業者では、日々、管理対象のノードが増減する状況にあるため、次年度の予算化が難しい状況でした。「その点、Splunkのライセンスはデータ量に応じた課金だったため、ある程度計算が立てやすく、その点も大きな魅力だった」と阿部氏は話します。

そして、3つめの「拡張性」については、Splunk Enterpriseを前提としたプレミアム製品「Splunk IT Service Intelligence」（ITSI）が挙げられます。監視対象のシステムから収集したデータの相関付け、機械学習によるインテリジェンスにより、予測分析と効率的なアラート管理を実現するものですが、「今後、運用の自動化、効率化で新たに取り組みたい要件が出てきたときに、柔軟性、拡張性といった部分で可能性を感じた」と阿部氏は述べています。

2021年6月に正式にSplunkの採用が決定し、同7月より本番環境の構築が開始されました。構築時に注力した点について、阿部氏は、「旧システムから新システムへの移行は単に機能をエクスポートしてインポートすれば済むものではない」として、要件を整理し設計に落とし込む上で、「サーチ言語（SPL）の基礎的な部分から理解、習得するのに十分な時間をかけた」と話します。また、運用担当者にとって操作に違和感が生じないよう、UIにも配慮しました。

また、機能面について、同社 エンジニアリング統括本部 クラウドエンジニアリング本部 プラットフォーム開発部 運用基盤グループの渡邉 一雄 氏 は、「導入にあたり注力した点としては相関サーチの開発で、蓄積されてきた運用対応手順やナレッジを継続利用できるよう、既存システムの監視アラート表示を踏襲してエピソードが生成されるようにしました。また、既存システムには無い、新たな機能として監視イベントから通知先を紐付けて抽出できるようにしました」と話します。

監視基盤には周辺のサブ監視システムが複数存在しており、アラートのベースとなるメッセージが多数発せられます。「多様なアラートを処理するためにSPL開発は高度なスキルが必要とされます」SPL開発には、Splunkのプロフェッショナルサービスによる支援のもと、「自分達でも継続して改善していけるように、SPLの処理内容に関するスキルトランスファーも手厚く対応いただきました」と渡邉氏は話します。

> 分散していた各種データをシームレスに操作できる環境が整ったことで、今後の継続的な改善につなげていくことができると考えています”
>
> 株式会社IDCフロンティア
> エンジニアリング統括本部
> クラウドエンジニアリング本部
> プラットフォーム開発部
> 運用基盤グループ
> **渡邉 一雄 氏**

自動化により障害一次対応の時間は6分の1に短縮を見込む、運用現場の様々な要求に応えることが可能に

2022年9月からは既存システムとSplunkの並行稼動が始まりました。松本氏は「Splunkに取り込む1つ1つのイベントが意味を持ち、IT運用監視においてはそのイベントの取りこぼしが運用業務にクリティカルな影響を及ぼすため、旧システムで検知できていることが新システムでも検知可能な状態にするための地道な作業を行った」と述べています。

そして、2022年11月からはSplunkによる本格稼働が開始されました。阿部氏によれば、「日常的な運用監視、障害一次対応やエスカレーションを行うエンジニアなど、延べ40名のエンジニアがSplunkを使った運用業務にあたっている」ということです。

Splunkの導入効果について、阿部氏は「これまで様々なDBに散在していたデータがSplunk上に集約されたことにより、障害発生時の一次対応に要する時間は、理論値では、従来システムでの約30分が5分以内に短縮されている」と話しました。アラートが出たシステムがどの顧客のシステムで、誰に、どのような手段で通知するかを整理、対応するために「これまでは人手で調べて目視確認を行っていたものが、Splunkと既存の監視ツールなどを組み合わせることで、ほぼ自動化に成功した」と阿部氏は続けます。

また、渡邉氏は、「特定の顧客IDの特定のアラートのみを表示させたいという運用現場の要望に対しても、キーワードで絞り込むことによりダッシュホードに可視化できる。また、既存システムでは対応しきれずに、運用担当者がアラートから影響範囲の特定や対応手順の関連付けをおこなっていたが、新システムでは自動的に判別可能な仕組みが整備できた」と話します。

> 今後も、IT運用のさらなる自動化、最適化にSplunkを活用していきたいです。ビジネスチャンスにつなげる “攻めのツール” として社内でのSplunk活用が進んでいくよう、さらなるご協力に期待したいです”
>
> 株式会社IDCフロンティア
> エンジニアリング統括本部
> クラウドエンジニアリング本部
> 本部長
> **松本 和久 氏**

> Splunkは運用監視ツールではないものの、従来システムでできていた機能をすべて実現できることが確認できました。Splunkのエンジニアの迅速な対応、手厚いサポートも選定の一因となりました。今もカスタマーサクセスマネジャーと定例をしてもらっている。プロジェクトは一段落ついたが、今後、Splunkを使い倒すということに注力していく。自分達がやりたいことをどうやってSplunkで実現できるかについて今議論しているが、引き続きご協力いただきたい。また、海外での活用事例などについても情報提供してもらえると嬉しい”
>
> 株式会社IDCフロンティア
> エンジニアリング統括本部
> クラウドエンジニアリング本部
> プラットフォーム開発部
> 運用基盤グループ
> **阿部 佑介 氏**

対象業務範囲を拡大し、Splunkの強みである「データ活用」を実現していきたい

今後の課題や展望について、阿部氏は「Splunkの強みである『データの利活用』にも注力していきたい」と話します。たとえば、「100人のユーザーそれぞれが違うダッシュボードを使うこともSplunkでは可能なので、その人にとって最も必要で、有用なデータを表示させることができないか、特定のサービスでダッシュボードを作ってみるところからアプローチを開始している」ということです。

さらに、セキュリティ分野での活用など「今のところ未着手の分野もSplunkに集約していけるとよいと考えている」として、そのためのユースケースなどの情報提供などに今後も期待したいと阿部氏は述べました。

松本氏は、IT運用の観点で「アラート分析から障害復旧対応に至るIT運用のさらなる自動化、スピード化に取り組んでいきたい」とした上で、「SplunkをIT運用システムの中心にし、運用自動化システムとの連携やサブ監視システムの高度化など、ゼロタッチオペレーションに向けたIT運用全体の最適化を実現していきたい」と展望を述べました。

また、今回のプロジェクトでは「Splunkプロフェッショナルサービスからナレッジトランスファーをしっかり受けたことが大きなポイントだった」と話します。内製での運用が実現できなければ、今後のビジネス変化に対応しながら運用現場からの要望に答えることはできないと考えています。

松本氏は、「今後も、ビジネスチャンスにつなげる “攻めのツール” としてSplunkを活用していきたい」とし、そのために社内でのSplunk活用が進んでいくよう、さらなる情報提供やアドバイスなどの協力に期待したいと締めくくりました。

23-job#-Splunk-IDCfrontier-CS-104