elastic

InfoTrace360

「正確性・スケーラビリティ」に強みを持つ検索エンジンで、業務環境を効率的に見える化 | Elasticsearch × InfoTrace 360

目次

近年、DX推進やテクノロジーの進歩によって、ITシステムの活用が進んでいます。業務が効率化する一方で、扱うデータ量が格段に増加することによりITシステム運用のコストが上昇してしまっているという企業も多いでしょう。また、これに加えて監視・分析段階においても、スピードや正確性といった様々な課題が顕在化しつつあります。

その課題に「検索」の技術を用いて向き合い、ソリューションを提供してきたのが、Elasticsearch株式会社（以下、Elastic社）です。2012年、オランダで設立されて以来、グローバルで事業を拡大。現在では、世界40か国以上に拠点を構え、プロダクトのダウンロード数が40億に到達するなど、世界を代表する企業です。

この記事では、Elastic社の福田氏へのインタビューを通して、企業がITシステム運用で抱えている課題や、Elastic社のソリューションで期待できる効果、株式会社ソリトンシステムズ（以下、ソリトン）が提供するソリューションへの活用状況について紹介します。

ITシステムの複雑化により、運用コストが増大

DXの推進やテクノロジーの進化を背景に、ITシステムも変化しつつあります。オンプレミスとクラウドの並立や、両形態を接続するためのハイブリッドネットワークの構築、アジャイル開発の浸透による継続的なアップデートなど、様々なレイヤーにおいてITシステムの構築環境が複雑化しているのです。

その結果、以前よりもITシステムの運用にかかるコストが増大。情報システム部門の人材リソースも不足しているため、いかに効率的にシステムを運用できるかが大きな課題となっています。

福田氏は、平時のみならず、問題発生時にかかる対応コストにも目を向ける必要があると語ります。

“ITシステム自体が複雑化しているため、トラブルが起きた際、原因を特定するのに時間がかかるようになってきています。その結果、サービスが使えない時間も長くなり、ビジネスに機会損失を生んでしまうのです。不測の事態に対応するコストを削減するには、即座に課題を発見し、サービスのダウンタイムを最小限に抑える必要があるといえるでしょう。”

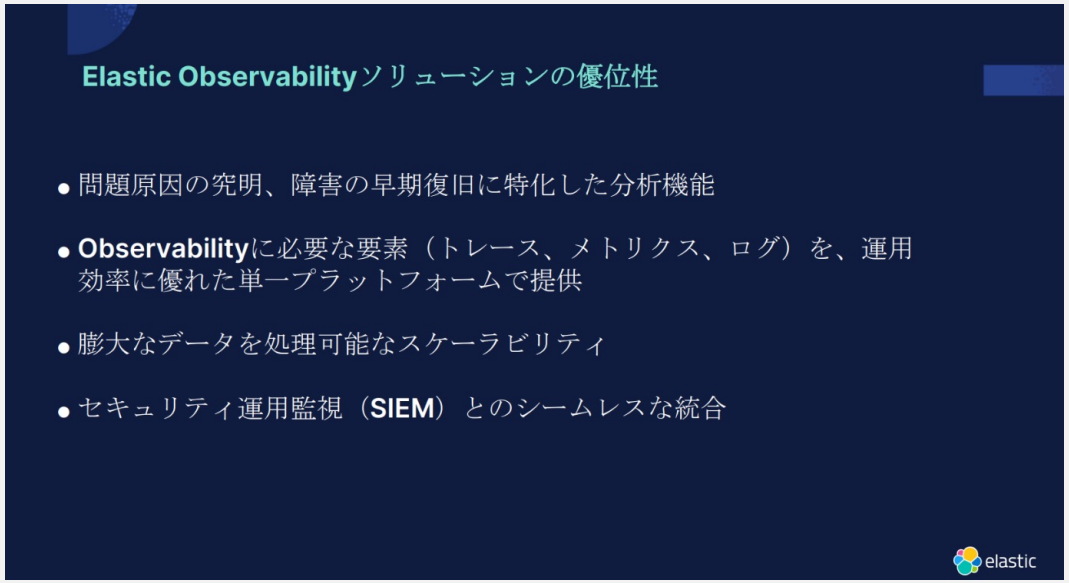
Elasticsearchの検索技術が、ITシステム運用の効率化に貢献

ITシステム運用の効率化を図るのに有効なのが、ITシステム・セキュリティの監視です。

特に近年、レスポンス時間などの「トレース」と、インフラのCPU・メモリ使用率といった「メトリクス」、システム上のアクション履歴である「ログ」という三要素のデータを用いてシステムの現状を把握する”Observability（オブザーバビリティ）”が注目を集め、その方法論に基づいて様々な監視ソリューションが開発されてきました。IT環境に関わる多様なデータを見える化することで、障害原因の早期特定や障害の予兆検知を期待できるようになったのです。

ところが福田氏は、従来の監視ソリューションには大きな課題もあると話します。

図 1



“可視化されたデータによって、異常発生に素早く気づけたとしても、根本的な原因を特定するには、結局のところ、膨大なログデータを見返さなくてはなりません。手探りで多岐にわたるデータソースから問題に関連するログデータを収集して整理し、原因を分析するには、数日単位の時間がかかることもあります。“

このような課題を解決するために、Elastic社が提案しているのが、検索エンジン「Elasticsearch」の機能をObservability分野に拡張した「Elastic Observability」です。「Elastic Observability」は、Elasticsearchの強みである「スピード・正確性・スケーラビリティ」を引き継いだObservabilityソリューションです。

それらの強みの中でも、特にスピードに関しては、他の監視ソリューションと比べても抜きんでています。検索エンジン”であるElasticsearchは、収集したデータをインデックスと呼ばれる大きなテーブルに格納します。そしてデータを格納する際、そのドキュメントをのちの検索処理が高速に行えるように、すべての「ワード」をその意味を理解したうえで適切なフィールドに格納します。この機能をベースに稼働するElastic Observabilityは、障害原因の特定のためにログやその他のメトリクスデータを調査する際、データ量が増えても高速で分析、可視化を行うことが可能です。福田氏は続けて次のように説明します。

“ITシステム監視においてはとにかくスピードが命です。障害が発生した場合、いかに早くその原因を特定するかが重要なポイントです。しかし従来の監視ソリューションではログからのキーワード抽出に長時間かかったり、ログの分析に数時間かかってしまい、結果的に原因の特定が遅れてしまうケースが多くありました。”

また、正確性もITシステム監視においては重要です。Elastic Observabilityは上記のとおりデータをインデックスに格納しますが、その際すべてのデータを同じスキーマで保持するよう作られています。つまり、トレース、メトリクス、そしてログがすべてひとつのテーブルに格納されており、どのデータとどのデータが関連しているかを瞬時に分析することが可能です。このような機能は、Observabilityという新しい監視形態を実現するのにうってつけだと福田氏は言います。

“Observabilityが求める監視形態は、単にトレース、メトリクス、ログのデータが収集できるというだけでなく、これらが互いにどう関係しているのかを可視化する必要があります。これは監視対象となるシステムが複雑化しているため、人の力で問題の原因を特定するのが困難になり、その分析のために監視ソリューション側が「ある特定の時刻におけるトレースとログの相関関係」といった視点で可視化することが求められるようになりました。その意味で従来の監視ソリューションが苦手にしていたログを100%可視化できるElastic Observabilityは Observabilityを実現するという意味において最も優れたソリューションです。”

さらに、スケーラビリティも高く、膨大な量のデータを処理することが可能です。数十台のサーバーを用いた並列処理を行っても、パフォーマンスが落ちません（図1）。

Elasticソリューションは、「Elasticsearch」を核に、ITシステム監視を行う「Elastic Observability」、セキュリティ監視を行う「Elastic Security」へとサービスを拡大。全てのサービスは、一つのプラットフォーム上で使用することが可能なため、ネットワークの安定性やシステムの利用状況など、ITに関する様々な問題を迅速に解決できるようになっています。

図 2

連携ソリューション「InfoTrace 360」でIT課題の解決に貢献する

Elastic社の検索エンジン「Elasticsearch」は、ソリトンが提供する業務環境を可視化するレポートサービス「InfoTrace 360」のダッシュボード部分で、メインエンジンとして採用されています。

ソリトンは、もともと個人情報保護法対策としてオンプレミスでPC操作ログを管理するための製品を販売してきましたが、より幅広いユーザーに利用してもらえるよう、SaaS形態で提供することを検討。ソリトンの持っていたログ記録・管理のノウハウと「Elasticsearch」のデータ抽出・分析の能力を組み合わせ「InfoTrace 360」が誕生しました。同製品は、コンピューターの稼働状況やファイルの利用状況など、業務環境に関わる幅広いデータの保管・分析を通して、各企業のセキュリティリスクの把握や働きやすい環境づくりに貢献しています（図2）。

福田氏は、ソリトンの「InfoTrace 360」との連携について、以下のように語ります。

“日本のITシステムは、独自のログや運用方法が目立つため海外の監視ツールをそのまま適用することは難しい傾向にあります。一方「 Elasticsearch 」は、あらゆる形態のデータを分析することができ、検索を強みにしているという性質上、どの業界・業種でも活用できる汎用性があるため、日本のITシステム監視に大いに役立つと自負しています。今回いただいた連携の機会を活かし、今後も既存サービスの改善や、新規サービス・新規ビジネスの開発を一緒に行っていきます。“

これを受けて、ソリトンの「InfoTrace 360」のプロダクトマネージャーを担当する池田は、以下のように締めくくりました。

“テレワークの浸透やクラウド利用の増加など、企業の業務環境が変化する中、情報漏洩や内部不正、働き過ぎなどのリスクも上昇しています。適切な企業運営のために、異常を察知し、迅速に対応することがますます求められるようになってきました。それらのニーズにITシステム・セキュリティの監視を通して応えるのが「InfoTrace 360」です。現在、他よりも多くの切り口の分析レポートに強みを持っていますが、今後も環境変化に伴う新たな情報漏洩経路・リスクの可視化や、早期検知機能を追加したりすることで、さらに顧客のニーズに応えられる製品に改善できればと考えています。”

Elasticsearch株式会社

お問い合わせはこちら

https://www.elastic.co/jp/contact

謝 辞

Elasticsearch株式会社様、インタビューにご協力いただき誠にありがとうございました。

テレワーク・クラウドシフトなど、業務環境が大きく変化している今、働き方の「モニタリング」は、業務効率を下げずにセキュリティ強化を実現する手段の一つです。

ソリトンは、「安全性」と「利便性」を両立したITソリューションをこれからも提供していきます。

ネットアテスト

「ネットアテスト」は、企業ネットワークに関わる全ての方のためのサイトです。安心・安全な環境を実現したい情報システム担当者様、確かなシステムを提案されたいインテグレータ様に向けて、運用の効率化やセキュリティ強化の方法などをお届けしていきます。

サイトはこちら