elastic | HINO Computer System

（写真左から）
サーバー基盤部 部長
横山 和尊 氏
サーバー基盤部 インフラサーバー基盤 グループリーダー
金田 侑大 氏

SUCCESS STORY

検索　製造業

日野コンピューターシステム、ネットワークのログデータを集約し、可視化された運用を実現

日野自動車グループのシステム開発会社である日野コンピューターシステム株式会社（以下、日野コンピューターシステム）では、本社や工場内の様々なネットワーク機器から出力されるログが分散し、障害検知や対応に支障をきたしていた。そこで、ログ監視基盤の刷新を決断。目標としたのは、管理者が見たいデータを掘り下げて検索し、問題箇所の特定と分析を高速化することだった。同社は、分散していたログデータを集約することで、安全な環境下における実用的な形式での利用を実現し、全体的な可視性の向上を成し遂げた。

ログ検索時間を30分から数秒へ短縮

Elastic Cloudの導入により、各事業部の機器内に点在していたログデータを本社サーバー基盤部に一元集約。ログ検索の時間を大幅に短縮した。

Microsoft Azureとの閉域網接続でセキュアな環境構築

Microsoft Azureと閉域網で接続し、ログデータをインターネットに晒すことなく、セキュアな環境で集約することに成功。

現場主導の「データの民主化」と自律的活用

Elastic Cloudの導入により、各部門の現場担当者が自律的にデータを活用する「データの民主化」を実現。

ネットワークのログ分散が障害対応に支障をきたす

日野自動車のシステム子会社である日野コンピューターシステム。同社のサーバー基盤部は、セキュリティ環境の構築などグループ全体のネットワークインフラを支えている。しかしグループの事業拡大に伴い、ネットワーク環境が複雑化し、システムごとの負荷状況の把握や、各部門でのログ管理は限界を迎えていた。

サーバー基盤部でインフラサーバー基盤グループリーダーを務める金田 侑大氏は、従来のインフラ管理基盤について「ログ情報はシステムごとに収集、蓄積されていましたが、基本的には各システムを動かすサーバーに散在していました。そのため、どこで何が発生したかを把握するためには、まず各所に置かれたサーバーや機器に直接アクセスし、ログを集める必要がありました」と説明する。

障害が発生した際には、問題の原因を1秒でも早く特定する必要がある。しかし、従来のインフラ管理基盤では、まず分散していたログを集める作業に時間がかかり、集めたログを分析するシステムの反応も悪かった。「1時間分のログを分析して結果を表示するまでに20〜30分かかる状態でした」（金田氏）

さらに、分散したサーバー内に膨大なログデータを長期保存することは難しく、古いログデータは別のメディアに移動していたり、最悪の場合、ログが上書きされていたりすることもあった。そのため、障害発生時に過去のログを照合して分析することも難しかった。

Elasticの柔軟性と拡張性に着目

こうした課題を打破するため、同社は2024年末からElasticの導入に向けた検討を開始した。選定の過程では他社製品との比較も行われた。数あるソリューションの中からElasticを選定した理由は、ログ管理における豊富な実績と、膨大なデータを高速検索できる基盤としての強さである。特に、1日数百GB発生するネットワークログを、コストを抑えつつ長期保管し、かつ即座に検索できる点が決め手の一つとなった。

Elasticの柔軟性と拡張性も重要な要素となった。同社サーバー基盤部の部

スモールスタートで導入し、利用拡大に対応できる拡張性の高さがElastic Cloudのメリットでした。

横山 和尊 氏
サーバー基盤部
部長

elastic

長を務める横山 和尊氏は、「自分たちでダッシュボードをカスタマイズし、必要な情報を自在に可視化できる点は、他社のパッケージ製品にはない魅力だった。また、スモールスタートで導入し、成功すれば適用範囲を拡大していきたいという我々の考えにも合致していた」と振り返る。加えて、ログデータの管理について、セキュリティ上の要件をクリアすることも主要な選定材料となった。日野自動車グループの厳格なセキュリティ基準を満たすため、外部のクラウド環境にログデータを置くことは極力避ける必要があった。

この懸念に対して、Elasticのクラウドサービスである「Elastic Cloud」は、同社グループが利用するMicrosoft Azureのクラウド環境と「Azure Private Link」で接続し、インターネットを経由せずに閉域網内でデータを転送できる仕組みを備えていた。「外部にデータを晒さないセキュアな環境を構築できることが、クラウド型での導入を後押ししました」と金田氏は説明する。

オープンソース由来であるElasticは「調べればわかる」素性が強み

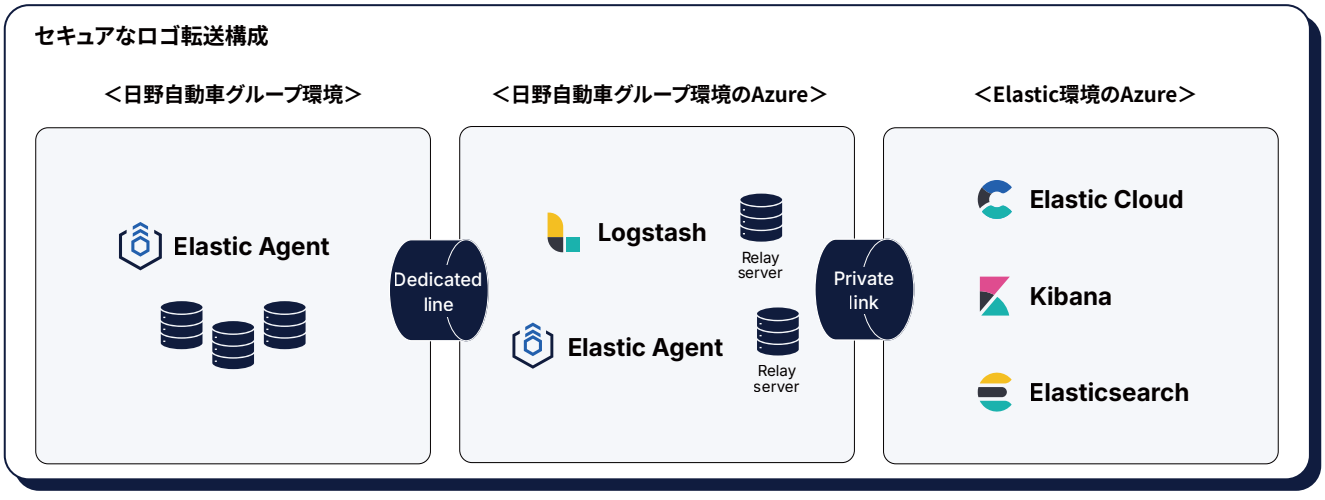
導入プロジェクトは、まず「ログデータ基盤の構築」から始まり、次に「既存環境のリプレース」、そして最終的な「最適化」という3つのステップで進められた。また、単にログを収集するだけでなく、実務で使用できる形にするためのデータ加工にも工夫を凝らした。例えば、ネットワークログをバイト単位からビット単位に変換して可視化するなど、現場エンジニアが直感的に理解できる形式に書き換える作業を積み重ねた。

これら、開発時に直面した粒度の異なるさまざまな課題に際して、金田氏のチームではパートナー企業やElasticからの支援を受けながらプロジェクトを進めた。さらに、Elasticが持つ豊富な公開ドキュメントも開発の助けとなったという。「Elasticはオープンソースを源流としているため、自分で調べればかなり深いところまで解決策が見つかります。不明な点があっても、コミュニティやドキュメントを頼りに自力で答えにたどり着けるベースがあることは、内製化を進める上で非常に心強く感じました」と金田氏は評価する。

現場管理者が自律的にダッシュボードをカスタマイズ

導入後、最も大きな変化をもたらしたのはログ検索時間の圧倒的な短縮である。以前は30分近くかかっていた1時間分のログ表示が、今では数秒から数分で検索可能となった。これにより、障害発生時の対応が飛躍的にスピードアップした。金田氏は、「検索が速くなったことで、現場の運用担当者の負担を大幅に軽減することができました。トラブルの発生時でも、瞬時に状況を可視化し、条件を変えながら、多角的に理解できるまで原因を探ることができると好評です」と手応えを口にする。

ログ管理基盤の運用面でも大きな成果が得られている。Elastic Cloudが備える「Hot/Frozenアーキテクチャ」というデータの階層管理を活用することで、コスト効率と利便性を両立させている。この階層管理は、直近のデータを高速なストレージに置き、過去のデータは安価なオブジェクトストレージに移動させるという構成。時間が経つにつれて利用頻度が激減するログデータの管理には極めて合理的で相性が良い。



さらに金田氏は、「コストを重視したフローズン階層のデータであっても、検索速度に全く不満はない」と話す。これにより、コストを抑えつつ、例えば3カ月前のトラブルを遡って調査するといった分析も容易になった。

Elastic Cloudによるログ管理が稼働したことで、横山氏と金田氏が想定していなかった効果も生まれている。当初は事前構築済みのダッシュボードを利用していた事業部門の運用担当者が、自部署の業務に合わせてダッシュボードをカスタマイズするなど、自主的に新たな機能を作り始めたのだ。

「ネットワークの技術者ではない現場の担当者が管理ツールの設定を勉強して、自ら検索式を書くようになりました。まさに『データの民主化』が起きたと感じました」（金田氏）

現場が開発した機能には、ログデータを読みやすく変換して、特定の機器の利用が帯域の80%を超えると自動的にメールを送る仕組みなどがある。Elasticのデータ基盤を現場が自律的に活用することでログの有用性は一層高まっている。

ログ監視以外の領域にも展開を計画

サーバー基盤部では今後、Elastic Cloudによるログデータの運用体制を、他の領域を含めたグループ全体へ拡大する構想を描いている。日野自動車は三菱ふそうトラック・バス株式会社との経営統合を控えており、統合後のネットワークインフラ管理の効率化も視野に入れる。

一方、進化が著しいAIの応用についても検討している。「AIは機械学習による過去のログデータ分析に使えると考えています。例えば、現在のネットワークの異常値を過去の障害や攻撃のパターンと照合し、先回りしたセキュリティ対策を講じることもできると期待しています」と金田氏は語る。

また横山氏は、「現場支援の一環として、サーバー基盤部が主導して社内向けにElastic Cloudの勉強会やトレーニングも実施していきたいと考えています。また、これまでと同様にElasticからのサポートにも期待しています」と話す。

ネットワークログだけでなく、アプリケーションレベルでの運用管理や、セキュリティログを監視・分析する「セキュリティ情報とイベント管理（SIEM）」への応用など、可能性は広がる。

「Elasticの基盤は、作ろうと思えば何でも作ることができる、無限の可能性を秘めた製品だと思っています」と金田氏は最後に語った。

Elasticはオープンソース由来の技術で、豊富な技術情報がネット上に豊富に存在するという点は、開発担当として非常に魅力的でした。

金田 侑大氏
サーバー基盤部
インフラサーバー基盤
グループリーダー

SOLUTION

Elasticsearch | Elastic Cloud | Kibana

elastic