# 東証株式売買システム「arrowhead」の性能解析や キャパシティ監視、ビジネストランザクション分析に貢献 困難だった大量データのリアルタイム可視化を可能にするSplunk Enterprise

## 概要

1878年に東京株式取引所として創立され、日本を代表する金融商品取引所として140年以上にわたって日本の経済成長を支え続けている株式会社東京証券取引所（以下、東証）。日本における証券・金融市場の象徴的な存在であり、ニューヨークやロンドンとともに世界有数の金融市場として位置づけられています。日本取引所グループ（JPX：Japan Exchange Group）の一員として、2019年度から第三次中期経営計画を推進しており、社会を支えるインフラとしての責任を果たす意思と、環境変化に立ち向かう意思を「市場への責任 未来への挑戦」とし、世界でも中心的な市場の一つであり続けるためのさまざまな施策に取り組んでいます。具体的には、新しい上場商品の開発をはじめ、新市場の創設準備や売買取引などマーケット形成に不可欠なシステムへの積極的な投資、海外にある証券取引所との戦略的提携など、攻めの姿勢で新たな時代に求められる市場を創造しています。

そのような東証において、現物商品の売買システムとして2010年から稼働しているのが、世界最高水準の高速性・信頼性・拡張性を兼ね備えた株式売買システム「arrowhead（アローヘッド）」です。arrowheadの取引対象となるのが現物商品としての株式やCB（Convertible Bond：転換社債型新株予約権付社債）で、1日あたりの注文件数は平均5000万件程度、多い日では1億件を超える膨大な件数を処理できる環境が整備されています。2019年には売買制度の見直しによる株価急変動の抑止や、終値での約定成立機会の向上、システム性能の安定化など、市場利用者がより安心して取引できる市場を実現すべく、性能改善も踏まえた全面刷新を実施しています。その際に、arrowheadにおけるサーバリソースを中心としたシステム性能解析やキャパシティ監視、ビジネスデータ解析基盤として、Splunk Enterpriseが採用されています。

## 性能改善を目指すarrowhead刷新においてキャパシティ監視の課題が顕在化

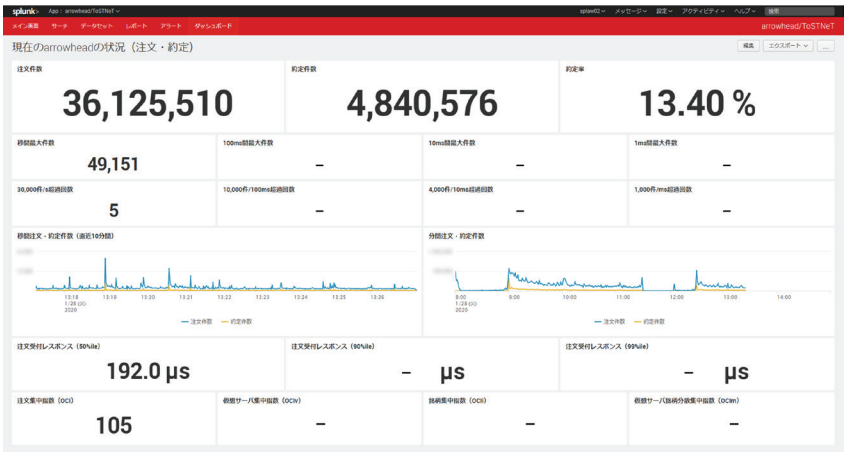
株式などの取引市場を運営する金融商品取引所では、公正・公平な取引を実現するための市場構築が重要であり、東証でも高い公正性・安全性・信頼性を備えた最適な取引の場を提供することが求められています。なかでも、システム利用者に最小限かつ公平なレスポンスを提供することが重要であり、非機能要件であるシステムの性能や信頼性を十分に担保することが欠かせません。IT開発部ではそのような性能要件の確保を始めとした様々なシステムの企画・開発を担当しています。

そのような東証が運用してきたarrowheadの刷新プロジェクトが始動するなかで課題の1つとなっていたのが、arrowheadが稼働するサーバ群のキャパシティ監視でした。「JPX全体としてキャパシティ監視には非常に力を入れており、継続的に投資を行っています。ただし、得られた情報をリアルタイムに取り込むことができる基盤は有していたものの、必要な結果を得るための解析に多くの時間が費やされていました」とIT開発部 課長 トレーディングシステム担当 山本 敦士氏は当時の状況を振り返ります。具体的には、注文受付レスポンスや注文スループット、メモリ使用率やディスク使用率などのキャパシティといった情報を確認するGUIは用意されていたものの、分析結果の表示には長い時間を要していました。「従来の解析ツールでは必要な情報を速やかに取得することができず、C言語やPerlを駆使して解析用のスクリプトを別に開発するなど、個別対応を実施せざるを得ない状況でした」と語るのは同部調査役 トレーディングシステム担当 加藤 圭氏です。そこで、arrowhead刷新のタイミングにあわせ、改めてキャパシティ監視につながる解析基盤を一から見直すことになったのです。

## 素早く解析でき、内部で使いこなせる仕組みとして高く評価

新たな環境として求めたのは、可能な限り素早く解析できること、そして社内で使いこなせることでした。「私が明言していたのは（解析対象のデータ量には因るが）概ね1分以内に解析ができること。使いこなし

現在の arrowhead の状況（注文・約定）




注：画面内データは実際のデータとは異なります

### 業種

- その他金融業

### 活用事例

- 東証株式売買システム「arrowhead」の性能解析/キャパシティ監視およびビジネストランザクションデータ解析

### 課題

- 大量のログから必要な情報を得るための解析に時間がかかっていた
- CやPerlなど解析用のスクリプトを作成するなど個別対応が必要に
- 性能向上したarrowheadにも対応できるデータ解析基盤の構築が急務に
- 解析プロセスの簡素化を目指したい
- データ量が多く、部分的な解析しかできなかった
- リアルタイムにシステム状況を把握できる環境を整備したい

### 導入効果

- ミリ秒単位の解析も可能となり、内部で起きていることの可視化に成功
- 周辺システムとAPIで容易に連携
- 数十倍のスピードで解析結果が表示
- データ解析までのプロセスを簡素化、必要な情報をリアルタイムに把握
- arrowheadに対して行った投資の効果測定ツールとして活用
- 素早くグラフ化、役立つデータかどうかのトライ&エラーがしやすい
- プロアクティブな基礎情報を解析するためのツールとして重宝

### データソース

- Linux OSのSyslogログ
- ミドルウェアのログ
- 株式売買システムのログ

### ご利用製品

- Splunk Enterprise

株式会社東京証券取引所
IT 開発部
課長
トレーディングシステム担当
**山本 敦士氏**

株式会社東京証券取引所
IT 開発部
調査役
トレーディングシステム担当
**加藤 圭氏**

については、自社のメンバーでも柔軟な解析ができるような仕組みであることを希望したのです」と山本氏。実は当初は、旧来のツールを利用し続けることを前提に検討を進めていましたが、性能改善を実現した新生arrowheadへの移行に伴って従来以上の処理能力の向上が求められ、既存ツールでは対応できないことが判明しました。

そこで注目したのが、ビッグデータ分析ソフトウェアのSplunk Enterpriseでした。以前は、サーバから必要なログデータをダウンロードするために、まずはシステム運用を担う部署であるITサービス部に申請を行った上で、大量のデータをダウンロードし、その後、性能解析用のマシンにアップロードして個別のスクリプトにて解析を行っていました。「解析結果が出るまでのプロセス全体で見れば、数日の時間を要していました。また、例えば1ミリ秒間毎の注文件数の推移を一日分評価するとなると、2,700万行というExcelで扱えないような行数になってしまいます。それゆえ部分的な時間帯の分析に終始せざるを得ないなど、気軽に解析すること自体が難しい状況だったのです」と加藤氏。Splunk Enterpriseであれば、必要な情報が自動的にインデクサーに蓄積され、Splunkが持つ独自の検索言語であるSPLにてサーチ文を用意しておけば、リアルタイムに欲しい情報を手に入れることができる、と評価します。「秒間でいえば多いときで8万件を超える注文件数が発生しますが、それがリアルタイムに把握できます。実はarrowheadからすれば1秒間というのは長い時間で、一つの注文を200マイクロ秒で処理するような状況です。1ミリ秒での処理件数などもSplunk Enterpriseであればすぐに表示できます」と山本氏。

社内で使いこなせるかどうかは、検索言語であるSPLの使いやすさとともに、周辺システムとの連携が容易で多様なAPIを備えていることもメリットで、例えば人手でExcelにダウンロードするような処理も自動化できる点が大きいと山本氏。「GUIでもスマートな運用は可能ですが、APIを使ってSPLにてサーチ文を用意しておくだけで、必要な情報がExcelシートに自動的に入手できます。データ活用という面でも、使いやすい仕組みです」。

結果として、大容量のデータを高速処理する必要がある東証のarrowheadにおけるキャパシティ監視やログ解析のソリューションとして、Splunk Enterpriseが採用されました。

## 5000万件/日の注文電文と各種リソースを収集、いつでも解析

Splunk Enterpriseの運用については、arrowheadの統合ログ管理の仕組みからフォワーダーを経由し、各サーバのCPUやメモリの使用率といったリソース系のログを取得。さらにarrowheadで処理された1日平均5000万件ほどの注文電文ログをSplunkインデクサーに取り込むことで、可視化および解析に必要な情報の蓄積が行われています。検索などを行うサーチヘッドサーバ上に作成されたWeb GUI上には、リソース系の情報やキューの滞留状況がリアルタイムに表示されるダッシュボードを用意。注文の秒間処理件数や相場情報の秒間配信件数、注文受付レスポンスや相場情報配信レイテンシーなど業務的な情報もリアルタイムに表示でき、運行管理システムのアラートに対する解析ツールとしても活用されています。

現在の arrowhead のリソース状況


注：画面内データは実際のデータとは異なります

現状はIT開発部のメンバー5名程度が主に利用していますが、欲しい情報があるメンバーにSplunk Enterpriseを紹介するなど、少しずつ利用者が増えていると加藤氏は説明します。「例えば4000ほどある銘柄の取引がそれぞれ秒間で何件ずつ発生しているのか、数十の取引参加者が数千ある発注ルートをどう使っているのかなど、アプリケーションデータ/ログを解析することで必要な情報が欲しい場合に、Splunk Enterpriseが活躍しています」と加藤氏。プロアクティブな基礎情報を解析するためのツールとして役立っている状況です。

## ミリ秒単位の解析も可能に、arrowhead内部の可視化を実現

Splunk Enterpriseを導入したことで、情報がスピーディに解析できるようになったのは大きいと語ります。「これまでのデータ量が多く局所的な解析しかできなかった環境から脱却し、あきらめるしかなかったミリ秒単位での電文やリソース推移の動きまで可視化できるようになったのは大きい。arrowhead内部で起きていることを、より具体的に把握できるようになり、ボトルネックの究明と解消にも役立てることができます。また、SPL内には計測値の分布を示すパーセンタイルを評価する関数なども用意されており、必要な情報がSPLだけで容易に手に入るのはとても助かっています」と加藤氏は高く評価します。

感覚的にも数十倍のスピードで解析結果が表示できるようになり、今では事前にSPLにてサーチ文を用意しておくだけで解析が可能です。「サマリーインデックスを使って事前に値を抽出しておける機能があることで、時間をかけずに必要な情報が入手できる環境が手に入るのもSplunk Enterpriseの魅力的な機能です」と山本氏は評価します。

コスト面での効果も高いと山本氏。「あれだけの高速性をもって大量のデータを処理するのに、わずか4台のサーバで実現できています。しかも、インデクサーサーバは容易にスケールアウトできるため、拡張性も高い。以前は高速なストリーミング処理のためのミドルウェアが構成上必要でしたが、今はSplunk Enterpriseだけでその環境が構築できています」と評価しています。

Splunk Enterpriseによってリソース系の情報や業務系の状況がリアルタイムに把握できることで、新生arrowheadに対する投資効果を測定するツールとしても役立っていると山本氏は力説します。また、Splunk Enterpriseであれば集まった情報を素早くグラフ化できる点も大きいと語ります。「集めた情報の業務への有用度は玉石混交です。そのような情報もボタン1つでグラフ化すれば、情報の有用性が一目で判断できます。わざわざExcelなどを経由せず可視化できるため、トライ&エラーしやすい」と加藤氏。

他にも、充実したマニュアルとともに、コミュニティサイトの存在も有益だと語ります。「Splunkのユーザが多いこともあり、新しい情報や不明点も多くのユーザから声が集まるコミュニティサイト上から探すことが可能です。リファレンスが充実しているのは見逃せません」と山本氏。

## データソースを拡大し、さらなる高度な分析にも活用したい

今後については、充実したSplunkのプラグインを積極的に活用し、各種ミドルウェアやBIツールなどとの連携を進めていきたいと語ります。ほかにも「現状取り込めていないネットワーク機器のログ情報や、注文の値段やどれだけの約定数などが起きているのかといった業務的な情報も取り込んで、これまで見えなかった新たな情報も可視化できるはず」と加藤氏は期待を寄せています。「arrowheadの運行に直接かかわる部分のために難しいかもしれませんが、個人的にはサーバ間の相関関係などが可視化できるSplunk IT Service Intelligenceにも非常に興味を持っています。システム構成を把握しながら、各サーバで何が起きているのかの可視化によってサービス全体の可用性を高めるといったことにも挑戦してみたい」と語っていただきました。