オンラインゲーム運用に必要な各種インフラのログを効率的に収集 モニタリング環境の整備とオペレーションの効率化に大きく貢献する Splunk Enterprise

概要

“最高の「物語」を提供することで、世界中の人々の幸福に貢献する。”を企業理念に掲げ、IP（知的財産）を生かした豊富なエンターテインメントコンテンツを世界中に発信している株式会社スクウェア・エニックス。HD（ハイ・ディフィニション）ゲームや大型オンラインゲーム、モバイルゲームなどのゲームを中心とするサービス展開を行うデジタルエンタテインメント事業を中核として、業務用ゲームの企画・開発・販売などを行うアミューズメント事業、コミックやゲーム攻略本などを手掛ける出版事業、フィギュアやキャラクターグッズなどの二次的著作物の企画・制作及びライセンス許諾を行うライツ・プロパティ等事業など幅広い事業を展開しています。

そんな同社が手掛ける主力 IP の 1 つであるファイナルファンタジーシリーズナンバリングタイトル 14 作目にあたる「ファイナルファンタジー XIV（以下、FFXIV）」は、MMORPG（Massively Multiplayer Online Role-Playing Game）としてはシリーズ 2 作目で、6 周年目を迎え人気を博しています。この FFXIV では、オンプレミスやクラウドを有機的に連携させ、グローバルなインフラ基盤を日本やアメリカ、欧州の各データセンターに展開しています。この FFXIV のインフラ基盤におけるモニタリング環境として、そしてオペレーションを効率化するためのツールとして Splunk Enterprise が活躍しています。

オペレーションの効率化や迅速な原因特定に向けた基盤整備が必要に

ゲーム運営に必要なサーバの設計・構築・運用は、掛札 純平氏が所属する情報システム部門が担っていますが、これまでサーバの安定運用に向けたログ分析基盤は整備されていませんでした。障害発生時にはログを確認するために各サーバへのログインが必要であったり、サーバベンダーによって異なるハードウェアのログを解析して障害原因を特定する必要があり、運用管理の負担が大きかったと掛札氏は以前の状況を振り返ります。「サーバへのログインや、サーバ内に点在するログを直接参照していた関係で、障害対応の速度や粒度が個人のスキルに大きく依存していました。障害対応を迅速に行うためにも、オペレーションの効率化が求められていたのです」。

またゲームの切断や遅延といったユーザーからの問い合わせに対応すべく、カスタマーサポート経由で調査のリクエストが情報システム部に寄せられていましたが、当初はリクエストごとにデータフォーマットの整形や分析用のスクリプティングなど手動でオペレーションしている箇所が多く、他の業務と並行して行うために調査だけで数週間を要することも。「緊急性の高いものでは、たとえ数分でも我々にとっては看過しがたい時間になってしまいます。効率的かつ迅速に調査分析できる環境が求められていたのです」と掛札氏は当時の課題について語ります。

さらに、当時アプリケーションレイヤーの分析は別の仕組みで存在していたものの、情報システム部がインフラレイヤーと関連付けて主体的に分析を行うことはありませんでした。コンテンツ配信に利用する CDN（Contents Delivery Network）を監視する仕組みも十分ではなかったといいます。「ログを保存する仕組みは存在していましたが、能動的に分析するような環境ではなかったのです」と掛札氏。

新たな開発に自身のリソースを割きたいと考えていた掛札氏だけに、インフラにおけるモニタリングやオペレーションの効率化、さらにはこれまでできていなかったアプリケーション側の分析も含め、業務の効率化を進めることを決断するのです。

複数クラスタでもコストを最小限に、スキーマレスによる柔軟性を評価

そこで掛札氏が目を付けたのが、データプラットフォームの Splunk Enterprise でした。「ネットワーク機器のログを集約してセキュリティ分析を行うデータプラットフォームとして隣のチームが導入していたのが Splunk Enterprise でした。こんなツールがあると上司から紹介を受けたのがきっかけです」と掛札氏。実は、スクリプトを駆使する環境から脱却するべく、周囲のコミュニティ界隈で利用されていたオープンソースのログ分析基盤を構築し、活用していたこともありましたが、プロダクション環境に展開することを想定して Enterprise レベルのサポートが得られる有償版を検討したところ、ライセンス体系が FFXIV のインフラ環境に適していないことが判明したのです。「ネットワーク要件を確認したところ、ログ分析基盤を物理データセンターごとに設置する必要がありましたが、比較していた製品はクラスタ

SQUARE ENIX®

業種

- 情報・通信業

活用事例

- オンラインゲームにおけるインフラ関連のモニタリング基盤

課題

- サーバの安定運用に向けたモニタリングのための統合的なログ分析基盤が未整備だった
- サーバログインやトラップ解析など非効率な運用管理を強いられていた
- 利用者からの問い合わせ調査に数週間を要することも
- アプリケーション側のログ分析が十分に行われていなかった
- 新たな開発のために自身のリソースを振り分けたかった

導入効果

- ホストにログインせずともログ確認を迅速に行うことが可能になった
- 各種ログを相関的に見て分析、新たな気付きが得られるようなった
- 障害予兆検知などプロアクティブにログ活用できるようになった
- ダッシュボードを活用することでレポート作成作業の自動化を実現
- 自身のリソースを新たな開発に振り分けることができるようになった
- ワールドごとのユーザー傾向の可視化にも大きく貢献
- 障害発生時にも告知情報を詳細かつ迅速に行うことができるようになった
- サービスの印象悪化を防ぐことにも役立っている

データソース

- Syslog
- Linux OSの監査ログ
- BMCログ
- 内製アプリケーションの独自形式ログ
- CDNトラフィックログ
- IT管理サービスログ
- その他各種Saas関連ログ

ご利用製品

- Splunk Enterprise

株式会社
スクウェア・エニックス
情報システム部
掛札 純平氏

ごとに費用が掛かるため、大きな投資になってしまう。対して Splunk Enterprise であれば、クラスタが異なっても費用が発生することはありません。当時スモールスタートしたかった我々の環境に適したソリューションだったのです」と掛札氏。

また、これまで利用していたオープンソースのソリューションでは、データを取り込む前の事前のスキーマ定義がパフォーマンスを得る上で必要でした。「Splunk Enterprise であれば事前にスキーマ定義を行う必要はなく、今あるログを手軽に収集して分析を行うことが可能でした。フォーマットの異なる多種多様なログを扱う我々にとって、手離れの良い Splunk Enterprise はとても魅力的だったのです」と掛札氏は評価します。

複数台の Indexer を 3 か国に分散、インフラ運用に必要な各種ログを収集

現在は、50名ほどのメンバーが Splunk Enterprise を利用しており、ログデータをインデックス化する複数台の Indexer を日米欧の物理環境および仮想環境に展開しています。実際に収集しているのは、Syslog や Linux OS の監査ログ、ハードウェアの監視やイベント記録を行う BMC（Baseboard Management Controller）のログといった IT インフラに関わるログをはじめ、内製アプリケーションから取得するレイテンシ関連のログやセッションログなど、そしてコンテンツデータ配信時に活用している CDN のトラフィックデータや ID 管理サービス、GitHub をはじめとした各種 SaaS 監査ログ、SaaS 自体が API で提供しているヘルスチェック情報などエンドポイント監視に使うログなどです。それぞれの用途や目的に応じてログのリテンション期間や要件は異なっており、リアルタイムなものから定期取得するものまでさまざまです。

相関的な分析が容易になり、数週間かかっていた調査がわずか30秒で可能に

Splunk Enterprise を導入したことで、ホストにログインせずともログ確認を迅速に行うことが可能になり、各種ログを横断的に分析することも可能になったのは大きいと掛札氏は語ります。「当時分析の都度作成や修正を行っていたスクリプトでは、複数のログを横断的に分析することが困難でした。Splunk Enterprise では大量のデータセットを手軽に扱うことができるため、新たな気づきが得られるようになったのです」。また障害発生時にしか確認しなかったログを日常的な監視の際にも活用することで、障害予兆検知などプロアクティブに動けるようになったと評価しています。さらに、手作業で作成していたレポート作成が、今では Splunk Enterprise のダッシュボード上で時系列データとしてシンプルに確認できるようになっています。「レポート作成作業が自動化できたことも大きな効果で、今では欲しかった情報に誰でもダッシュボード経由でアクセスできるようになっています。以前は調査に数週間かかるケースもありましたが、今は Splunk にログインするだけ。30秒程度ですぐに状況確認できるようになっています」と高く評価します。モニタリングやオペレーションの業務が省力化できたことで、自身のリソースを新たな開発に振り分けることができるようになった点も見逃せません。

複数のログが横断的に分析できるようになったことで、ワールド（論理的に分割された FFXIV のユーザーが実際にゲームプレイをする場所）ごとのコミュニティや新規ユーザーの多さなどを可視化するなど、これまで見えていなかったユーザー傾向の可視化にも大きく貢献しています。「FFXIV では負荷分散のために内部的に存在している論理データセンターを分割することがありますが、その際に得られたデータを活用することで、最適なユーザー体験を維持したままインフラ拡張が可能になると考えています」と掛札氏。

Splunk Enterprise については、機能の面やレスポンスの面で高く評価しているだけでなく、SIEM として利用しているチームからの評価も良好です。「SPL も、SQL に触れたことがある方であれば困ることはありません。学習コストも非常に少なく利用することができます」。問い合わせへの迅速な回答が行われるなど、サポート面でも期待に応える真摯な対応に満足していると掛札氏は評価します。

なお、万一 DDoS 攻撃やそれに類するネットワーク障害などの影響でユーザー切断が発生した場合でも、原因の切り分けに Splunk Enterprise を活用することで、告知情報を詳細かつ迅速に行うことができるようになっています。「サーバーレイヤを中心に検知しているため、例えば DDoS 攻撃かどうかの検知や判別は Splunk Enterprise だけでは難しいものの、ネットワークレイヤーの調査や上位の ISP 事業者への問い合わせなど、Splunk Enterprise と連携させた具体的なアクションにつなげることができるようになりました。これまでは単純な告知でさえも掲載するのに時間がかかっていましたが、今ではより詳細な情報を迅速に告知できるようになったのは大きい。サービスの印象悪化を防ぐという効果にも役立っているはず」と利用者への価値提供にも Splunk Enterprise が貢献していると掛札氏は評価します。

ログの取り込み範囲を拡大させながら、継続的にデリバリーできる CI/CD 化を推進

現在はサーバを中心としたログの取得となっていますが、今後はネットワーク機器やアプリケーションレイヤーのログなど、Splunk Enterprise へのログ取り込みの範囲を拡大していきたいと語ります。「今は IP アドレスベースでの分析しかできませんが、ゲーム内のキャラクタ名やキャラクタ ID での分析ができるようになれば、不正アクセスの検知をはじめ、利用規約で禁止されている現実の通貨でアイテムを売買する RMT（Real Money Trade）への対策、チート分析などにも応用できるはず」と掛札氏は期待を寄せています。また、各国に設置している Splunk Enterprise の Indexer は独立した形で運用していますが、これらを有機的に連携させてグローバル全体でのデータ分析にも活用していきたいと語ります。

新たなソリューションとしては、ローカルにキャッシュだけを残してデータをオブジェクトストレージに保存する Splunk Smart Store などにも興味を持っていると掛札氏。また、Splunk Enterprise の運用についてもコード化できるような環境づくり取り組んでいきたいといいます。「今は Indexer 関連の設定を手作業で変更することが多いですが、長期運用していくうえではコード化を行い、システム的に変更履歴が見える状態にしていきたい」と今後について語っていただきました。

20-13742-Splunk-IT-Square Enix-A4-102-CS-JP