

ミシシッピ州歳入局：Splunk Observabilityで ダウンタイムを防止して数百万ドルを節約

主な課題

ミシシッピ州歳入局(MDOR)ではIT環境が2000%と急激に拡大し、対処を迫られていました。事後対応的なITプラクティスから脱却し、複雑なメトリクスを明確なビジネス成果に変換して幹部に報告できるようにするため、規模拡大とともに断片化した監視システムを一元化されたオブザーバビリティプラットフォームに置き換える必要がありました。

主な成果

Splunkの導入により、州が管理する1.3億ドル規模の新しい酒類物流施設のオブザーバビリティプラクティスを変革しました。その結果、ダウンタイムのリスクを大幅に低減し、透明性の向上を通じて連邦監査を効率化し、問題の発生と修正を繰り返す事後対応的な運用から、データ主導でセキュリティを重視したプロアクティブな運用へと転換しました。



業種：公共部門、製造、リテール

ソリューション：Splunk
Observability、Splunk ITSI

政府機関のITは、稼働の維持だけで済むものではない

ミシシッピ州歳入局(MDOR)が担う重要性は、扱う税金の規模と影響を受ける市民の数に表れます。過去10年間で、同州のIT環境は新しいテクノロジーへの投資や構造改革を通じて2000%拡大し、その中でIT運用チームはこの急成長の舵取りをしてきました。

しかし、同局の規模が拡大しているなか、IT運用チームは持ちこたえるだけで精一杯であり、発生した問題やインシデントに受動的に対応している状態でした。この大規模な成長を支えるには、事後対応的かつ場当たりのIT運用から脱却し、断片化したその場しのぎの監視システムを拡張性が高い一元化されたオブザーバビリティプラットフォームに置き換えて、環境全体を把握し、増え続けるインシデントに後れを取らず対応できる態勢を整える必要があったのです。

そこに登場したのがSplunkです。MDORは、新たな大規模エコシステムを監視および管理するための戦略的パートナーとしてSplunkを選びました。Splunkを導入したことにより、環境全体にわたってサイロを解消し、一元的な可視化、データアクセスの改善、システム全体の健全性の監視を実現しました。これらは、有益なアップタイムを維持し、業務目標を達成するうえで不可欠なものです。

ミシシッピ州歳入局のCTO (最高技術責任者)であるMike Dehaan氏はこう述べています。「障害発生シナリオで主要依存関係のマッピングについて考える場合ですら、まずSplunkインスタンスの稼働を維持することが最優先です。Splunkは、アプリケーションの健全性とパフォーマンスを管理するための中枢です。問題に対応するときは、いつでも真っ先にSplunkを確認します」

成果

- 100万ドル以上：節約
- 2000%：IT環境の成長

オブザーバビリティをゼロから構築

MDORで変革の大きな転換点となったのは、最新テクノロジーを取り入れた新しい酒類物流倉庫の建設です。同局は、ミシシッピ州におけるワインおよび蒸留酒の唯一の卸売業者として年間1.3億ドル規模の事業を運営しています。しかし、以前の施設のネットワークインフラでは最新の運用を十分に支えられませんでした。

コンテナ化プラットフォームを基盤として高度に自動化された新施設に移行することは、最新化に取り組むための「キャリアの中で一度あるかどうか」の機会でした。成功を確実にするため、Dehaan氏はオブザーバビリティを当初から優先事項としました。「オブザーバビリティや監視について初めから考慮しておかなければ、後から無理やり組み込もうとしても、必ず困難に直面することになります」

プロジェクトの複雑さに対処するための戦略的な判断として、チームは監視インフラを優先することにしました。同氏はこう説明します。「最初にSplunkのツールを導入しました。新しいツールを先に導入したことで、導入プロセス全体を通じてその機能が積極的に役立ちました。今回の巨大プロジェクトを少しずつ進めていく中で、Splunkは最初から最後まで手放せないツールです」

Splunk Observabilityの導入を幹部に提案する際に同氏は、障害が発生した場合のコストを厳しい形で示しました。数日間のダウンタイムによって100万ドルを優に超える損失が生じるというものです。オブザーバビリティを優先したおかげで、チームは、今日の業界で一般的となっている「前例のないスピード」でプロジェクトを進めながらも、事業継続性を確実に維持することができました。

Dehaan氏はこう続けます。「ダウンタイムは極めて重大な問題なので、オブザーバビリティを最初から組み込みたいと考えました。それがビジネス成果に直接つながることがわかっていましたからです。その点について試算も行いました。問題の特定や解決に必要なツールがないため出荷がわずかに3日遅れただけでも、損失額はSplunkプラットフォームへの総投資額を上回るのです。この説明によって、ROIが誰の目にも明らかになりました」



障害発生シナリオで
主要依存関係のマッピング
について考える場合ですら、
まずSplunkインスタンスの
稼働を維持することが
最優先です。Splunkは、
アプリケーションの健全性と
パフォーマンスを管理する
ための中枢です。

ミシシッピ州歳入局、
CTO (最高技術責任者)、
Mike Dehaan氏



私たちはみな、午前9時から
午後5時までが勤務時間です。
しかし、自分にとって
Splunkは、勤務時間外の
午後5時から午後9時のもの
と思っています。その時間帯
に自らの意思でオフィスに
残って作業しているのは、
それが楽しいからです。
Splunkは私たちのすべての
業務の中心にあるのです。

ミシシッピ州歳入局、
CTO (最高技術責任者)、
Mike Dehaan氏

セキュリティ運用を強化してコンプライアンスを向上

Splunk Observabilityへの信頼が深まるなかで同局は、このプラットフォームを単なる運用ツールではなく、セキュリティ態勢の支えとしても考えるようになりました。Dehaan氏は、すべての運用担当者のワークフローにセキュリティ意識を高める仕組みを組み込んで、従来のサイロ化されたアプローチを打破しました。

同氏は言います。「私は大きな賭けに出ました。運用担当者の一人ひとりにセキュリティ意識を根付かせる必要がありました。チームメンバーのミスがあった場合、コンプライアンス担当者が運用実態よりもスプレッドシートでの監査に集中しては、見落としてしまう可能性があるからです」

チームは、Splunkを活用してセキュリティ運用を「生存メカニズム」として組み込むことにより、急成長に対応しました。Dehaan氏は説明します。「扱うデータ量が膨大になったことで、セキュリティリスクも劇的に増大しました。この規模拡大に対応できる唯一の方法は、セキュリティ意識を高めることです」

このセキュリティ戦略は、規制当局による監査の際に真価を問われることになりました。監査では、3〜4カ月の準備期間を経て、2週間にわたる現地監査を受けます。しかし、Splunkによる可視化機能と文書作成機能のおかげで、MDORのチームは万全の態勢で臨むことができました。監査官はその取り組みにとっても好印象を持ち、チームの優れたパフォーマンスを称賛する書簡を長官に送るとともに、監査を予定よりも早く終了させました。「私たちの努力は、単に監査に合格させる以上の価値があると評価されたのだと思います」と、同氏は振り返ります。

ITSIによって価値を幹部にまで拡大

Dehaan氏が上級管理職の役割を担うようになると、スイッチの脆弱性やエラーログといった技術的な話題に関心のない長官や非技術系のステークホルダーに対して組織のインフラの健全性を伝える方法が必要になりました。そこで大きな役割を果たしたのが、Splunk ITSI (IT Service Intelligence)です。

Dehaan氏は次のように指摘します。「長官が知りたいのは、アプリケーションの全体的な健全性であり、技術的な詳細には興味がありません。簡潔にまとめられた統計データを求めているのです。ITSIのおかげで、膨大なデータセットを具体的に理解しやすいインサイトへと凝縮できるようになりました」

チームは、技術的なパフォーマンスとビジネス成果を関連付けて、組織のミッション達成にIT投資がどのように貢献しているかを定期的に報告しています。これにより、コストセンターだったIT部門は、州の最重要サービスの健全性をリアルタイムで可視化するパートナーとしての地位を確立しました。

「私たちは、幹部が組織に貢献する成果に直接焦点を当てています。ITSIは、その取り組みを強力に支援してくれています」と、Dehaan氏は述べています。

事後対応から運用の拡大へ

Splunkの導入前は、問題の発生と修正を繰り返す事後対応的な運用から抜け出せず、障害の追跡に何時間もかかっていました。

今や、状況は一変しました。Splunkを導入したことで、アナリストのデータに対する認識が根本的に変わり、受動的なものだったのが、包括的かつ戦略的なものになりました。この変化は、運用チームに加わったアナリストが取り組むあらゆる仕事に反映されています。MDORのリードインフラエンジニアであるJustin Dennis氏は次のように説明します。「運用チームに新たに加わったメンバーは、まず、Splunk 4 Rookies (初心者向けSplunk講座)を受講します。クラウドサービスからオンプレミスのネットワーク、それらの間のあらゆる要素まで、Splunkの基礎を学ぶことで、エンジニアはそれぞれの役割をより効果的に果たせるようになります」

チームメンバーは、運用におけるSplunkの活用方法を熟知しているだけでなく、その用途を積極的に拡大しています。このプラットフォームは当初、インフラ監視のための技術的なツールとして導入されましたが、今では開発チーム、QAチーム、さらには組織内のさまざまな事業部門で情報源として利用されています。今後数年間の目標は、Splunkインスタンスへのビジネスロジックの組み込みを継続することです。

Dehaan氏はこう助言します。「まずは小さなことから、好奇心を持って始めましょう。すべてはレゴブロックのようなものであり、1つずつ積み上げていくのです。初めは、手に負えないように思えるかもしれませんが、しかし、最初の一步を踏み出せば、想像以上に早く使いこなせるようになります」

Splunkで好奇心を探究する

政府機関は、予算もリソースも縮小する中で最新化を絶えず迫られる環境にあります。そうした状況の中でミシシッピ州歳入局が証明したのは、レジリエンスを生み出すのはデータの力、そしてコードと同じくらい好奇心を重んじる文化を築く勇気だということです。

「私たちはみな、午前9時から午後5時までが勤務時間です。しかし、自分にとってSplunkは、勤務時間外の午後5時から午後9時のものと思っています。その時間帯に自らの意思でオフィスに残って作業しているのは、それが楽しいからです。Splunkは私たちのすべての業務の中心にあるのです」とDehaan氏は述べ、最後にこう締めくくります。「好奇心をくすぐってみましょう。データの中には、まだ活用されていない大きな価値が眠っています。それを掘り起こし始めると、データを活かすことがとても楽しい作業だとわかります」



運用チームに新たに加わったメンバーは、まず、Splunk 4 Rookies (初心者向け Splunk講座)を受講します。クラウドサービスからオンプレミスのネットワーク、それらの間のあらゆる要素まで、Splunkの基礎を学ぶことで、エンジニアはそれぞれの役割をより効果的に果たせるようになります。

ミシシッピ州歳入局、
リードインフラエンジニア、
Justin Dennis氏

Splunkを無料でダウンロードするか、[Splunk Cloudの無料トライアル](#)をお試しください。Splunkは、クラウドかオンプレミスか、また組織の規模の大小などにかかわらず、お客様のニーズに最適な導入モデルでご利用いただけます。