

2024

オブザーバビリティ の現状

成功への道筋を描く

splunk>
a CISCO company

遂に、エンジニアチームがソフトウェアアプリケーションの最新の機能を完成させました。数カ月におよぶ設計、コーディング、テストを終えて、あとはバグや大きな問題が発生せずに、リリースが成功するのを祈るばかりです。

新しいアップデートを本番環境に追加し、状況を見守ります。そして…問題は何も起こりませんでした。

Slackに新しいチャンネルを立ち上げて、メッセージを慌ただしくやり取りする必要も、深夜に近所のコンビニにエナジードリンクを買いに走る必要も、顧客からの怒りの電話に対応する必要もありません。チームメンバーはそれぞれ平穏の中で普段どおりに仕事をしています。(BGM：静けさを感じさせるコオロギの鳴き声)

エンジニアチームだけでなく、オフィス全体が落ち着いた雰囲気にも包まれています。SREは長年温めてきた自動化プロジェクトに着手し、開発者はバックログから次のリクエストを取り出して新機能を作成し、プラットフォームエンジニアはドキュメントの仕上げに入り、仕事が一区切りついた社員がコーヒーを入れています。

この平和な光景は偶然の賜物ではありません。オブザーバビリティの成し得る技です。オブザーバビリティは、あらゆるデジタルビジネスの成功基盤としてすべてを明るく照らし、平穏な日常をもたらします。システムが大混乱に陥ることを心配する必要がなければ、チームはイノベーションやレジリエンスの構築、強化に集中できます。

目次

- 4 その景色を見るためには苦労して登るだけの価値がある
- 6 先進的なオブザーバビリティプラクティスを構築することのメリット
- 13 テレメトリデータで柔軟な未来を創造する
- 17 プラットフォームエンジニアリングがDevOpsの新たな未来を切り開く
- 21 オブザーバビリティでのAI活用が始まる
- 24 オブザーバビリティを推進してリーダーを目指す
- 27 Splunkでオブザーバビリティのリーダー的組織を目指す

夢のような話に思えるかもしれませんが、私たちが調査したIT運用チームやエンジニアリング担当者のエリートグループにとって、このような成功は現実の話です。

先進的なオブザーバビリティプラクティスを導入していれば、イノベーションとレジリエンスを両立できます。どの組織でも問題の発生は避けられません。しかし、先進的な取り組みを行っている組織は、問題をすばやく、場合によっては数分以内に検出して修正します。開発者は開発と実験に時間を費やし、新しい製品やサービスを短期間で、わずかな期待ではなく自信を持ってリリースしています。リーダー的組織は、データに対する柔軟性と所有権を確保するためにはOpenTelemetryに、そしてインサイトを獲得するためにはAIに価値を見出しています。

昨年のオブザーバビリティ調査レポートで、私たちはオブザーバビリティが定着したと宣言しましたが、今年の調査では、オブザーバビリティがベースラインになっていることがわかりました。先進的なオブザーバビリティプラクティスを実践する組織は、競合他社とは一線を画し、未知の未知を検出して修正し、エンドユーザーに卓越したデジタルエクスペリエンスを提供しています。

こうした組織の取り組みを見てみましょう。

ビギナー的組織と比較したリーダー的組織の優位性

2.8倍

問題の検出スピード



72%

オンデマンドで
プッシュする
コードの量の差



78%

OpenTelemetryの
導入率



その景色を見るためには 苦勞して登るだけの価値がある

「この先、デジタルシステムが生成する
テレメトリデータが減ることはまずありません」

Splunk製品/テクノロジー担当SVP、Tom Casey

オブザーバビリティはもはや、新しいトレンドではありません。調査では、オブザーバビリティツールをすでに2年以上使用していると答えた回答者が約半数(47%)にのぼり、前年の36%から増加しました。また、オブザーバビリティは具体的なメリットをもたらしています。すでにご存知のように、緊急時にすばやいたラブルシューティングが可能になり、アラートの忠実度が向上し、問題を検出するまでの時間が短縮し、開発スピードが上がり、ダウンタイムが減ったことなどが報告されています。リーダー的組織がどのようなメリットを享受して他の組織と差をつけているかについては、後ほど紹介します。

ただし、リーダー的組織であっても、環境の複雑さを完全に克服したわけではありません。これは避けられないことです。

データが中心となる環境で、特に課題となるのは何でしょうか。いずれもデータに関する課題ですが、調査で最も多かったのは、異なるソースのデータを相関付けるのに時間がかかりすぎることです(30%)。2024年の調査では、各課題を挙げた組織の割合が軒並み増加し、データに関する課題が深刻化していることがうかがえます。

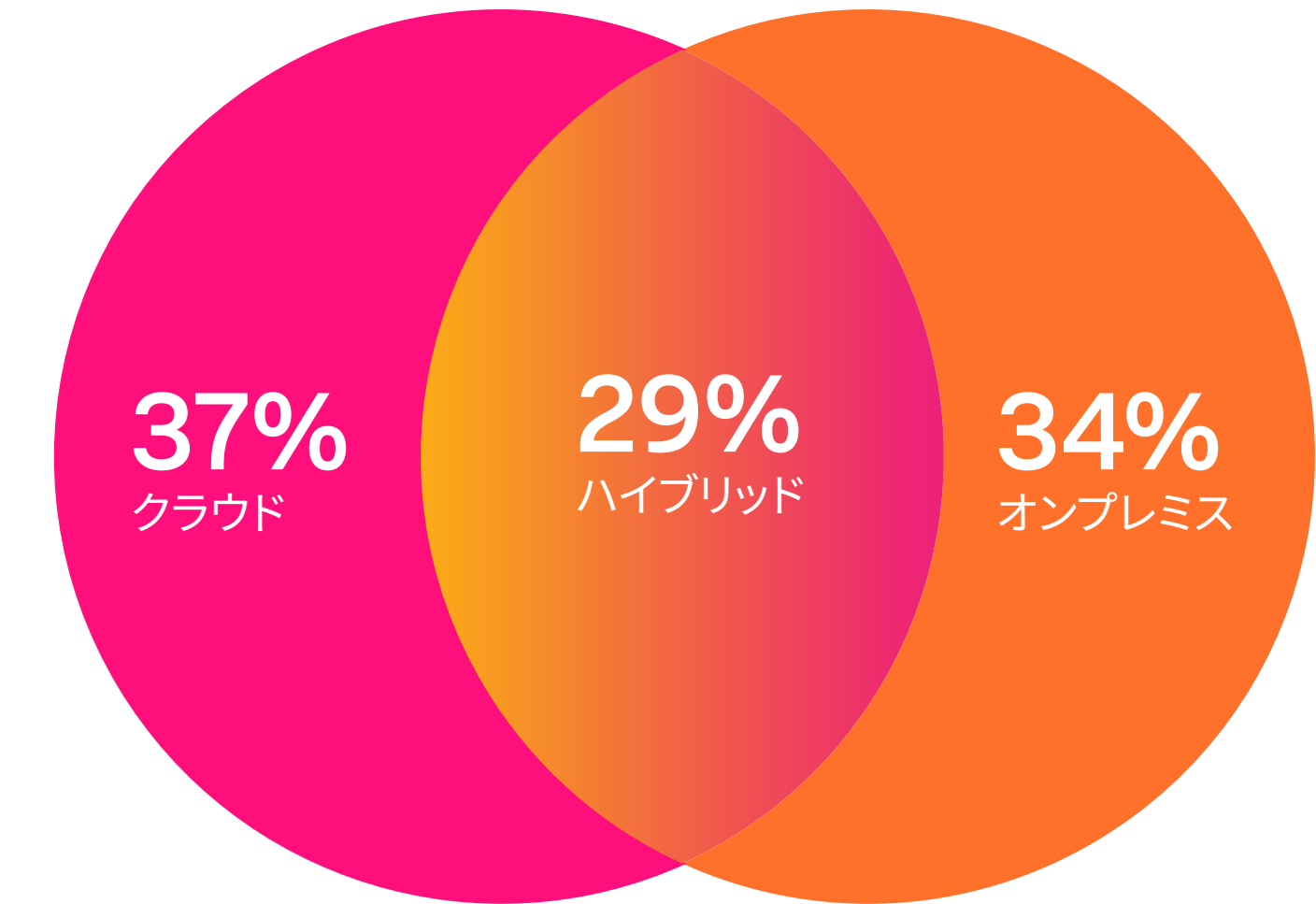
オブザーバビリティの実現

オブザーバビリティを実現すれば、環境全体を可視化できます。これは、今日のテクノロジースタックの複雑さを考えると容易ではありませんが、苦労するだけの価値はありません。対象には、組織が所有するネットワークと外部のネットワーク、オンプレミス、クラウド、ハイブリッドのインフラ、自社開発およびサードパーティのアプリケーション、デジタルサービスのカスタマーエクスペリエンスが含まれます。

- オブザーバビリティを実現するために克服すべき問題はいくつかあります。
- ・ **多すぎるノイズ**：オブザーバビリティとは、すべての構成要素について状態を把握することではありません。実際、情報が多すぎると担当者の処理が追いつかず、「オオカミが出た」と叫ぶ少年に振り回される村人のように真実がわからなくなり、情報を信じなくなってしまう恐れがあります。そこで本当にオオカミがやって来たときには、どうやってそれを知ることができるでしょうか。調査では回答者の半数以上(57%)が、過剰なアラートが「ある程度」または「非常に」問題になっていると回答しています。この問題は、燃え尽き症候群から問題の見逃しによるダウンタイムの発生まで、さまざまな実害につながります。実際、66%の回答者が、燃え尽き症候群のためにチームの重要なメンバーが離職したことがあると回答しています。
 - ・ **分散した環境**：組織の資産がどこにあるか、すべて把握できているでしょうか。今日、資産があるのは組織内にとどまりません。調査では、アプリケーション環境全体で「すべて」または「ほぼすべて」のデータを相関付けできていると回答した割合が24%にとどまりました。ビジネスアプリケーションがパブリッククラウド、オンプレミス、ハイブリッドインフラに分散している状況を考えれば無理もないでしょう。すべての資産の状況を可視化することは永遠の課題です。以前から、組織が所有または運用していないネットワークインフラについてインサイトを獲得するのは難しく、その状況は今も続いています。実際、ネットワーク資産をかなり可視化できていると回答した割合は26%にとどまりました。
 - ・ **多すぎるツール**：最新のテクノロジーとレガシーテクノロジーに対して組織が導入しているオブザーバビリティツールは、平均で23個にのぼります。組織によっては、1人の担当者が23種類のツールを切り替えながら監視を行うこともあるでしょう。これは明らかに多すぎます。しかも、23個は平均です。実際、8%の回答者が50個以上のツールを使用していると回答しています。そのすべてを使いこなすのはもはや神業です。
- 調査の回答者は、オブザーバビリティの実現が、今後進むべき道であることを理解しています。オブザーバビリティソリューションがもたらす価値は、そのコストの2.42倍であり、86%が、今後1年間でオブザーバビリティソリューションへの支出を増やすと回答しています。これだけの価値をもたらすのであれば、避けて通る理由はありません。



分散するビジネスアプリケーション



先進的な オブザーバビリティプラクティス を構築することのメリット

「先進的なオブザーバビリティプラクティスを構築することは、顧客に卓越したデジタルエクスペリエンスを提供し、常に顧客目線を取り入れて意思決定を行うということです」

Splunkオブザーバビリティ担当SVP兼GM、Patrick Lin

シャーロック・ホームズは「他の人が知らないことを知るのが私の仕事だ」と言っています。

先進的なオブザーバビリティプラクティスの実践は、組織のデジタル環境を全体から細部に至るまで詳しく監視し理解する点で、探偵業によく似ています。ビジネスを運営していれば、知らないうちにさまざまな謎や障害物が生じるものです。その一つひとつを探り出すには、環境を構成するすべての要素を観察するしかありません。

こうした謎を解くことは、オブザーバビリティの成果を証明するだけでなく、従業員の幸福度、開発者の生産性、顧客の満足度、組織の収益の向上など、さまざまなメリットを生み出し、最終的にビジネスの改善につながります。

では、先進的なオブザーバビリティプラクティスを構築するには何が必要でしょうか。適切なテクノロジーを導入するだけでは不十分です。優れた成果をあげているチームは、オブザーバビリティを向上させるための意欲、知識、能力を持っています。

重要なのは、オブザーバビリティによって単に問題を回避するだけでなく、卓越したデジタルエクスペリエンスを提供することを目指す文化を醸成することです。つまり、現状を維持するのではなく、より良い形に変えていく意識を持つことです。優れたチームは、その目的のために、オブザーバビリティ戦略に関する知識を磨き、適切なツール、トレーニング、プロセスを通じてその知識を行動に移そうと日々努めています。

言い換えれば、オブザーバビリティは、それ自体が成果なのではなく、成果をあげるための優れた手段なのです。



オブザーバビリティプラクティスの成熟度が低い組織では、問題の根本原因を探るために関係者全員を緊急会議に招集しなければなりません。しかし、人が多すぎると解決は遠のくばかりです。リーダー的組織のチームは、このような状況を回避する方法を心得ています。

Splunk AIOps製品マーケティング担当ディレクター、Annette Sheppard

先進的なオブザーバビリティプラクティスを実現するまでの道のり

先進的なオブザーバビリティプラクティスは、最初からあるものではなく、作り上げるものです。Splunkは、このプロセスが、基本的な可視化、インサイトの活用、プロアクティブな対応、ワークフローの統合の4つの段階を経て進化していくと考えています。リーダー的組織がどのようにこの道のりを辿っていくかを深く理解するために、調査では4つの段階ごとに、実状を探るための質問をしました。

基本的な可視化

すべての環境のすべてのテクノロジースタックを可視化できていますか？

リーダー的組織は、オンプレミスインフラから、プライベートクラウド、パブリッククラウド、コンテナ、アプリケーションまで、環境全体を高いレベルで可視化しています。

インサイトの活用

問題の検出時にコンテキストも同時に把握できていますか？

リーダー的組織にとって、アラートは議論や解析が必要になるものではなく、実用的なインサイトを提供してくれるものです。また、根本原因の特定、イベントの相関付け、さらには解決策の提案に、AIや機械学習を活用しています。

プロアクティブな対応

問題に先手で対応できていますか？

レジリエンスが高い組織でもダウンタイムは発生します。しかし、リーダー的組織では発生頻度が少なく、発生しても問題をすばやく解決できるため、状況があまり悪化せず、類似の問題の再発を防ぐこともできます。

ワークフローの統合

組織のプロセスにオブザーバビリティが組み込まれていますか？

リーダー的組織は、プラットフォームエンジニアリングなどの手法を活用して、ソフトウェアの開発、提供、運用方法を標準化し、開発者の生産性と運用効率を向上させています。

可視化のメリット：リーダー的組織が優れている領域

今回の調査では、リーダー的組織が複数の領域で他の組織よりも優れていることがわかりました。

開発者のイノベーション促進と生産性向上

今日、顧客の期待はかつてないほど高まっています。その中で革新的な製品を短いサイクルで提供できる企業は、顧客の要求に応えるだけでなく、競争でも優位に立つことができます。それを支えるのが、強力なエンジニアリングチームです。

リーダー的組織では、開発者の生産性の高さが生産力と収益を押し上げています。リーダー的組織の4分の3以上(76%)が、コードの大部分をオンデマンドでプッシュしています。一方、オブザーバビリティの取り組みが初期段階にある「ビギナー組織」で同様に回答した割合は30%にとどまりました。ユーザーへの新機能の提供については、リーダー的組織の60%が真っ先に市場に投入できていると回答し、ビギナー組織の8.6倍にのびました。

リーダー的組織はスピードがあるだけでなく、コードプッシュの安定性が高く、ミスが少ないという特徴もあります。リーダー的組織では、エンジニアリングチームによる本番環境のアプリケーションコードの変更成功率(DORAの主要メトリクスの1つ)がビギナー組織より22%上回っています。さらに、リーダー的組織の大多数は、変更の成功率が90%以上であると回答しています。

開発者が開発や実験を好むのは、個人的な利益だけが理由ではありません。付箋も、電子レンジも、ペニシリンも、Gmailも、さまざまな実験による偶然の産物です。リーダー的組織の開発者が目指しているのはまさにそれです。リーダー的組織の開発者は、メンテナンス、アラート処理、設定などの日常業務をこなしながら、ビギナー組織よりも38%多くの時間をイノベーションに費やしています。

問題の迅速な検出と修復

リーダー的組織は、開発のスピードだけでなくレジリエンスの高さでも秀でています。レジリエンスが高ければ、ダウンタイムを最小限に抑えることができます。アプリケーションの障害やパフォーマンスの低下が発生してから数分または数秒以内に問題を特定できると回答したリーダー的組織は68%で、そのスピードはビギナー組織の2.8倍にのびます。リーダー的組織では改善も進んでおり、57%が、根本原因を特定するまでの時間が1年前と比べて大幅に短くなったと回答しています。

このスピードには精度の高さが深く関係しています。リーダー的組織が推定するアラートの真陽性率は平均で80%以上でした。そのため、アラートが誤検知でないという確信を持って対応を進めることができます。一方、ビギナー組織では、実際の問題につながるアラートの割合が推定で半数強(54%)にとどまっています。この確率なら、コイン投げと変わりません。表なら実際に問題発生、裏なら誤検知といった具合です。この状態では、憶測や疑念が生じたり、緊急対応が無駄足に終わったりして、最終的にはエンジニアがアラートを完全に無視するようになる可能性もあります。

迅速な検出は迅速な解決につながります。MTTR (平均解決時間)が数分または数時間と回答した割合は、リーダー的組織がビギナー組織の2.3倍にのび、MTTRが数日、数週間、さらには数カ月と回答した割合は、逆にビギナー組織がリーダー的組織の2.4倍にのびました。問題の解決に時間がかかるほど、インシデントの影響が広がります。『[ダウンタイムの隠れたコスト](#)』レポートによると、1時間あたりのダウンタイムコストは54万ドルに達します。その点を踏まえると、問題を数時間で解決するのと数日かかるのには雲泥の差があります。

リーダー的組織で
コードの大部分を
オンデマンドでプッ
シュしている割合は
ビギナー組織の
2.6倍以上

リーダー的組織が
アプリケーションの
問題を検出する
スピードは
ビギナー組織の
2.8倍

AIの導入と活用

リーダー的組織は、オブザーバビリティの向上のために、機械学習、AIOps、生成AIなど、あらゆる形でAIを活用しています。いずれのテクノロジーも導入率が高く、たとえばAIOpsツールを広く活用している割合は64%で、ビギナー組織の10倍にのびります。また、リーダー的組織の65%がAIOpsを活用し、インテリジェンスと自動化を強化しながらインシデントの根本原因の特定や修復を行っています。

リーダー的組織は、AIの導入率が高いだけでなく、それによって大きなメリットを得ています。AIOpsツールのROIが期待をはるかに上回ったと回答した割合は40%にのびりました。これに対して、ビギナー組織ではわずか6%にとどまっています。

生成AIはオブザーバビリティの領域でも存在感を増しており、リーダー的組織はそのユースケースを開拓し始めています。オブザーバビリティツールに組み込まれた生成AI機能を活用している割合は3分の1にのびり、ビギナー組織の6%を大幅に上回りました。生成AIベースのチャットボットによるオブザーバビリティプラクティスの強化にも積極的で、85%がデータ分析、81%が問題の解決策の提案に利用しています。

テレメトリパイプライン管理における優先順位付け

データは、優れたオブザーバビリティプラクティスを支える基盤です。テレメトリパイプライン管理戦略は競争上の差別化要因であり、テレメトリデータが増え、コンプライアンス規則が変わり、ユースケースが増大するとともに、その重要性が増します。

先進的なオブザーバビリティプラクティスを実践している組織は、コストの抑制策としてデータ管理の技法を重視する傾向があり、階層化は57%、集約は55%が「非常に重要」だと考えています。こうした組織はおそらく、オブザーバビリティの取り組みが進んでいない組織と比べて、リリースする製品の数、管理するアプリケーションの数、保存するデータの量が多いため、コストが急速に膨らむと考えられます。どの組織にとっても、ある日予期せず法外な額のサービス利用請求書が届くのは避けたいものです。

リーダー的組織でのAIOpsの導入率はビギナー組織の**10倍以上**

リーダー的組織でコスト抑制にデータの階層化が重要であると回答した割合はビギナー組織の**2倍以上**

データとリソースの共有

セキュリティ運用チーム、IT運用チーム、エンジニアリングチームは、問題の根本原因を解決するために同じコンテキストを共有する必要があります。たとえば、ネットワークトラフィック急増のアラートが届いた場合、特別セールの実施、新機能のリリース、DDoS攻撃など、さまざまな要因が考えられます。データを共有できなければ、各チームが十分なコンテキストを得られないまま調査に無駄な労力を費やし、互いに責任をなすり付け合うことになりかねません。

チーム間の壁をなくしてダッシュボードを共有すれば、発生した問題をどのチームが担当すべきか、それはセキュリティインシデントなのかアプリケーションのパフォーマンスの問題なのかといった基本的な判断をすばやく行って、問題の根本原因に短時間でたどり着くことができます。リーダー的組織では約4分の3 (73%)が、セキュリティとオブザーバビリティのツールやワークフローを統合することによってMTTRを短縮しています。一方、ビギナー組織で同様に回答したのは39%にとどまりました。

「ウォールーム(作戦司令室)には常にセキュリティ担当者が参加するのが理想的です」と、SplunkのフィールドCTOであるCory Mintonは言います。「統合されたプラットフォームで経営幹部レベルの情報を可視化する場合でも、セキュリティチームとオブザーバビリティチーム間で基本的な知識を共有するだけの場合でも、共通の言語がなければうまくいきません」

先進的なオブザーバビリティプラクティスの実践に取り組む組織は、意図的であってもそうでなくても、プロセスの一環としてセキュリティとオブザーバビリティのデータやツールを統合することになります。この2つの重要な領域では、まず「分かち合いは思いやり」の精神を持つことが大切です。リーダー的組織では70%が、トラブルシューティングの際にデータとツールを共有し、80%が、ソフトウェア開発ライフサイクル(SDLC)全体でソフトウェアエンジニアがセキュリティ脆弱性の検出を通常業務として行う習慣を築いています。

オブザーバビリティがもたらす価値の拡大

ダウンタイムの削減、解決時間の短縮、イノベーションの推進は、あらゆる組織が目指す目標です。リーダー的組織は年間で支出の2.67倍の利益を得ており、成果を収益に直接結び付けています。

リーダー的組織は他の組織と比べて、オブザーバビリティソリューションからより多くのメリットを得ています。オブザーバビリティソリューションの導入によって問題の検出時間が短縮されたと回答した割合は、ビギナー組織が67%であったのに対して、リーダー的組織ではほぼすべての95%にのぼります。問題の迅速な検出は、システムをすばやく復旧させてダウンタイムを最小限に抑えるために重要です。また、オブザーバビリティの向上によってアプリケーションの開発期間が短縮されたと回答した割合も、ビギナー組織の64%に対して、リーダー的組織では92%にのぼりました。開発サイクルを短縮できれば、新製品や新しいエクスペリエンスを市場にすばやく投入できます。

リーダー的組織の73%がオブザーバビリティとセキュリティのツールやワークフローを統合して**MTTRを短縮**

リーダー的組織ではオブザーバビリティソリューションの導入によって得られた年間利益が**支出の2.67倍**におよぶ

オブザーバビリティの リーダー的組織が 享受しているメリット

リーダー的組織は次の領域で大きな成果を
あげています。

- ビギナー組織
- 成熟度が中程度の組織
- 成熟度が高い組織
- リーダー的組織



38% 42% 46% 52%

開発者がイノベーションに
費やす時間の割合



3% 7% 14% 28%

問題を数秒以内に
検出



6% 16% 37% 64%

AIOpsツールを
広く活用



39% 48% 62% 73%

オブザーバビリティと
セキュリティの
ワークフローを統合して
MTTRを短縮

テレメトリデータで 柔軟な未来 を創造する

「エンジニアはこれまで、オブザーバビリティデータの収集、変換、活用方法を自由に管理できませんでした。ベンダーに依存しないオープンソースのOpenTelemetryは、こうした柔軟性に対するニーズに対処します」

Splunk製品管理担当シニアディレクター兼OpenTelemetry共同創設者
Morgan McLean

オブザーバビリティが次に目指すのは柔軟性です。今後、データの所在地要件が厳しさを増し、新しいデータソースが次々に生まれ、ツールがさらに増えるのに伴って、データユースケースも拡大していくでしょう。こうしたユースケースを取り入れて、テレメトリデータの真価を引き出すには、データを効果的に管理および活用する体制を整える必要があります。データの収集方法、保存先、変換方法を組織が自由に決められることが重要です。このセクションでは、組織でデータを管理するためにお勧めの方法を紹介します。

OpenTelemetryが新たなスタンダードに

OpenTelemetry (OTel)は、オブザーバビリティデータを収集するための業界標準のオープンソースのアプローチです。データに関するすべての問題をたちまち解決する魔法の杖というわけではありませんが、一部の呪縛を解いてくれます。Cloud Native Computing Foundation (CNCF)のサポートにより、データの詳細な管理に役立つAPIやSDKが十数種類の言語で提供されているため、ベンダーロックインや専用エージェントの導入を回避できます。

そして、これだけははっきりと言えます。OpenTelemetryはオブザーバビリティの未来を支える基盤です。テレメトリデータを収集するための標準的な方法として、急速に認知されつつあります。今回の調査では、半数以上(58%)の回答者が、主に使用しているオブザーバビリティソリューションでOpenTelemetryが使われていると回答しています。OpenTelemetryへの対応がイノベーションの1つの原動力と広く認識されるようになり、当然、リーダー的組織は導入を進めており、78%が適切なプラットフォームをすでに導入しています。

また、リーダー的組織は、OpenTelemetryのメリットをよく理解しています。そのメリットとして「データに対する主導権と所有権を向上させることができる」を選択した回答者は65%で上位に入りました。一方で1位になったのは「より広範なテクノロジーエコシステムを活用できる」で、72%にのびりました。OpenTelemetryを導入すると、柔軟性とカスタマイズ性が飛躍的に向上します。一般的なプログラミング言語のほぼすべてに対応するライブラリが提供されているため、開発者が使用するテクノロジースタックに関係なくアプリケーションのインストルメンテーションが可能です。また、さまざまなフレームワークやライブラリと統合できるため、既存のアプリケーションへのオブザーバビリティの追加も簡単に行えます。

リーダー的組織はOpenTelemetryのメリットを享受している

● リーダー的組織 ● ビギナー組織

より広範なテクノロジー
エコシステムを活用できる

データの所在地要件に
対応できる



最新のクラウドフレームワークを
簡単に導入できる

オブザーバビリティの
コストを低減できる



データに対する主導権と所有権を
向上させることができる

ベンダーロックインを
回避できる



OpenTelemetryの 潜在能力を引き出す

一般的にOpenTelemetryのような強力なテクノロジーはシンプルではありませんが、その難しさを克服するだけの価値があります。早期に導入した組織は、最終的に得られるメリットが、それまでの苦労に十分値することを理解しています。リーダー的組織がOpenTelemetryの課題をより深刻に捉えているのは、期待する価値が大きいためと考えられます。調査では、OpenTelemetryの導入を「非常に困難」と評価した割合は、ビギナー組織で21%であったのに対して、リーダー的組織では44%にのばりました。リーダー的組織が最も課題と考えているのは、習得の難しさ、つまりOpenTelemetryに精通した人材の不足で、55%がこの点を挙げました。ただし、今は厳しくても、OpenTelemetryに関するトレーニングが増えるにつれてこの課題は解消していくと考えられます。

このほかにも、特定のインフラまたはフレームワークに対するサポート不足も課題であると、リーダー的組織の半数以上(54%)が同意しています。ただしこの課題は、OpenTelemetryのサポートに対する需要があることを認識するベンダーが増えるにつれて解消していくでしょう。実際、OpenTelemetryは登場からわずか5年の間に急速に普及しています。今日では、新しい製品やフレームワークの多くがOpenTelemetryにネイティブで対応しています。また、新しいシグナルタイプとして[プロファイリングのサポート](#)が追加され、ベンダーに関係なくリソースの使用状況をコードレベルで把握できるようになるなど、OpenTelemetry自体の進化もまだ続いています。

OpenTelemetryの導入が比較的容易だと考える回答者は、その理由として、充実したサポートを挙げています。プログラミング言語やクラウドネイティブのテクノロジーにサポートが組み込まれているほか、ユーザーコミュニティからも支援を得ることができます。十分な支援があれば、何かわからないことがあっても誰かが答えを教えてくれるため、早期の習得が可能です。



オープンソースプロジェクトは
常に進化しています。今こそ
OpenTelemetryを導入するのに
最適なタイミングです。

Splunk製品管理担当シニアディレクター兼OpenTelemetry共同創設者
Morgan McLean

テレメトリパイプラインを使いこなす

データはストーリーを語ります。ログ、メトリクス、トレースはいずれも、いつ、どこで、誰が、何を、なぜ行ったかを示すため、インシデント調査には欠かせません。クラウドやマイクロサービスが登場し、現在ではAIも普及し始めた中、オブザーバビリティチームは、複雑に絡み合ったテレメトリデータを解明してそのストーリーを読み取ろうと奮闘しています。

このデータの迷宮を攻略するには、高度なツールに加えて、データの所有権を中心とした戦略が必要です。データ量とコストが増加し続ける中、テレメトリデータをより詳細に管理するための技法が注目されています。リーダー的組織は特に、管理の必要性を感じています。

- ・ **変換と加工**：1行900文字のログとその関連メタデータを50文字のタイムスタンプとメトリクスに変換するなど、データを変換することにより、量を削減し、効率的に保存して、分析を簡素化できます。調査では全体の91%が、オブザーバビリティデータのコスト抑制には変換が重要だと回答し、特にリーダー的組織では「非常に重要」だと回答した割合が高くなりました。
- ・ **データの階層化**：データの価値はさまざまです。監査のためのデータはコールドストレージに保存するなど、アクセス頻度に応じて最適な保存先を選択することで、不必要に高価なストレージに費用をかけるのを回避できます。調査では全体の90%がこのアプローチを高く評価し、データの階層化がコスト抑制の方法として「重要」だと回答しています。
- ・ **集約**：このアプローチでは、統計的手法を使って複数のデータポイントを集約します。さまざまなソースのデータを組み合わせ、実用的な情報に変換することで、パターンやインサイトを抽出できます。また、ストレージの削減にも有効で、調査では全体の92%がコスト抑制に「重要」または「非常に重要」だと回答しています。

これらのデータ管理機能は、専用のポイントソリューションでも、より広範なオブザーバビリティスイートでも利用できるため、最適な方法を柔軟に選択できます。

リーダー的組織は明らかに「少ないほど良い」という考え方を持っています。これらの組織のオブザーバビリティチームは、その他の組織よりもツールの増加を問題視しており、データの階層化(63%)、変換(62%)、集約(61%)の3つすべての機能を提供する単一のスイートを好む傾向があります。

「テレメトリパイプライン管理は1つの製品ではなく、いくつかの機能の集まりです」と、Splunkの製品/テクノロジー担当SVPであるTom Caseyは説明します。「ツールセットに統合された製品にパイプライン機能が組み込まれている場合は、個別のソリューションを管理する負担を軽減して運用を合理化し、より深いインサイトを得ることができます」

スタックに新しいツールを追加するのは、ジェンガでタワーが倒れないようにブロックを引き抜くようなもので、巧みな手腕が求められます。これには、新しいシステムに慣れるためのスタッフのトレーニングや、管理の後継者育成計画の作成、場合によっては認定プログラムへの投資なども含まれます。また、専用のポイントソリューションを導入した場合、確認すべきダッシュボードの数が増えるため、その分、インシデント対応に時間がかかる可能性があります。

A person wearing a grey jacket and black leggings is adjusting a large black backpack on a rocky trail. The person's hands are visible, securing the straps. The background shows a sunset over a mountain range. The text is overlaid on the image.

プラットフォームエンジニアリングが DevOpsの新たな未来 を切り開く

「組織にプラットフォームエンジニアリング部門があれば、先駆者を目指す優秀な人材を惹きつけることができます。問題は、このまったく新しいチームを作る価値があることをCTOにどのように理解してもらうかです」

Splunk AIOps製品マーケティング担当ディレクター、Annette Sheppard

今まさに、プラットフォームエンジニアリング革命が起きています。調査では、回答者の約4分の3 (73%)が、プラットフォームエンジニアリングを広範囲に、または一部のプロジェクトで実践しており、さらに20%が、今後1年のうちに実践する予定だと回答しています。

この流れは、業務の範囲が拡大し続けるIT運用チームやエンジニアリングチームにとって朗報です。トラブルシューティングのプレッシャーにさらされてやる気が出る人もいれば、新しい仕事を探し始める人もいます。調査では、66%が、過去1年間でチームの重要なメンバーが燃え尽き症候群により離職したと回答し、70%が人手不足を訴えています。

プラットフォームエンジニアリングとは何か

プラットフォームエンジニアリングは基本的に、ツールチェーン、ワークフロー、セルフサービス型のプラットフォームを構築するためのアプローチの1つです。このアプローチにより、ソフトウェアエンジニアはツールの管理に費やす時間を減らして、より実用的で信頼できるソフトウェアの開発に集中することができます。

プラットフォームエンジニアリングに関する以下の噂は間違いです。

- ・ サイトリライアビリティエンジニアリングの別称である。
- ・ DevOpsの終焉を意味する。
- ・ すべての問題を解決する特効薬である。

プラットフォームエンジニアの日常業務には以下のものがあります。

- ・ ソフトウェアをVMにデプロイするまでのプロセスを定義する。
- ・ コーディング基準を定め、テスト環境を整備して、ソフトウェアの開発方法を規定する。
- ・ アプリケーションのインストールメンテーションの方法を標準化する。

なんとなくイメージできたでしょうか？

プラットフォームエンジニアリングの対象領域は幅広く、今のところ、DevOpsエンジニアの登場時にSREが困惑した状況とよく似ています。今後、プラットフォームエンジニアリングの有用性に対する認識が高まるにつれて、その役割と責任は自然に固まっていくでしょう。しかし、それまで待つのは組織にとって得策ではありません。



現在の開発プロセスで最も混乱が生じている領域、たとえばデプロイパイプライン、バベルの塔のようにばらばらのプログラミング言語、オブザーバビリティに関する標準化の欠如などの問題を把握し、その解消にプラットフォームエンジニアリングチームの労力を集中させます。

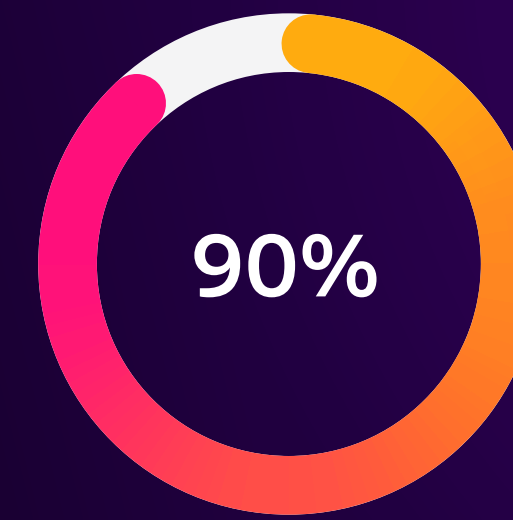
Splunk開発者エバンジェリズム担当ディレクター、Greg Leffler

プラットフォーム エンジニアリング革命の 原動力

プラットフォームエンジニアリングチームを持つ組織の55%が、その最大の成果として、IT運用の効率が向上し、スケーリング、監視、トラブルシューティングなどの業務が改善したことを挙げています。また、開発者の効率と生産性が向上したと回答した割合も40%にのぼり、効率の向上はプラットフォームエンジニアリングがもたらす代表的なメリットと言えます。

「開発者は、付随的な事柄、たとえば、アプリケーションを監視可能にする方法、データベースとの通信に使用するフレームワーク、FedRAMPへの準拠状況、実行時のプロファイリング方法などの詳細に悩まずに済みます」とLefflerは言います。「プラットフォームエンジニアリングチームがいれば、こうした作業をすべて引き受けてくれるため、開発者は成果物の提供に専念できます」

標準化は効率化につながります。大規模な組織では、複数の開発チームが異なるプロジェクトに取り組み、それぞれ独自のツールセットとプロセスを使用することがよくあります。プラットフォームエンジニアがソースコードリポジトリやCI/CDパイプラインなどを標準化すれば、コラボレーションの強化とデプロイ時間の短縮に大いに役立ちます。そして、プラットフォームエンジニアリングの導入効果が最も大きい領域はセキュリティとコンプライアンスです。ソフトウェアを構築およびデプロイするための確実な方法を厳密に定めることで、HIPAAやFedRAMPなど、需要の高い法規制や認証に準拠できます。



プラットフォームエンジニアによる
運用の標準化の取り組みが
成果をあげている

プラットフォームエンジニアリングを導入する メリットトップ5

55% IT運用の効率向上



42% アプリケーションの信頼性/パフォーマンスの向上



40% 開発者の生産性向上



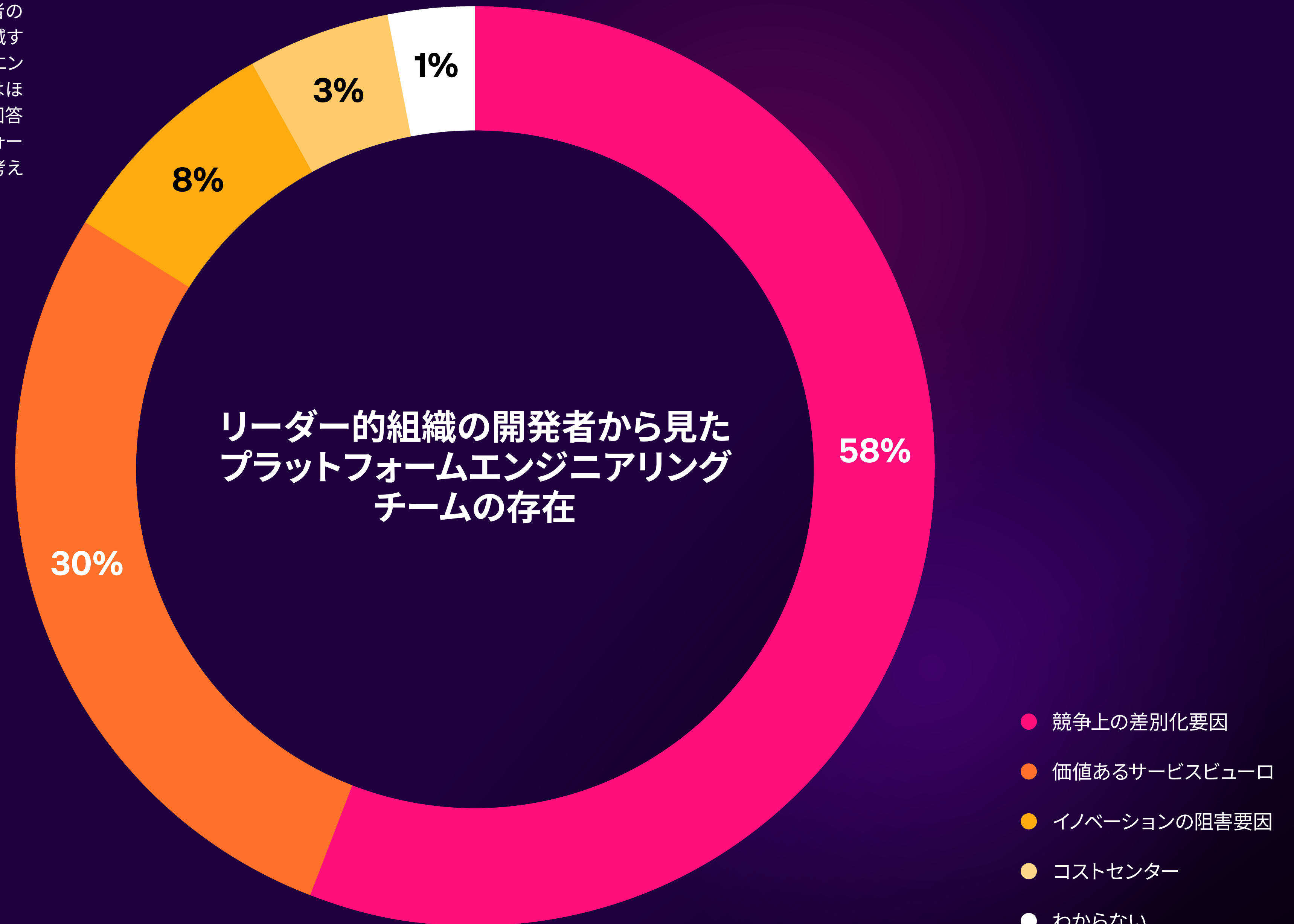
38% 新たなワークロードに対応したインフラの最適化



31% 技術負債の削減



プラットフォームエンジニアリングの最終目標は、開発者の生産性とコードの品質を向上させ、負担を全体的に軽減することです。そのため、開発者は当然、プラットフォームエンジニアリングチームを好意的に受け止めており、調査ではほぼ半数(47%)が「価値あるサービスビューロ」であると回答しました。さらに、リーダー的組織では58%がプラットフォームエンジニアリングチームを「競争上の差別化要因」と考えており、ビギナー組織の18%を大きく上回りました。



オブザーバビリティでのAI活用 が始まる

「生成AIアシスタントは、オブザーバビリティに関する知識を
民主化するための鍵です。自然言語で質問ができれば、
新たなレベルのインサイトとインテリジェンスを獲得できます」

Splunk AI担当VP、Hao Yang

エンジニアであれば、多くのグラフやダッシュボードを見比べて状況を把握する代わりに、仮想のウォールルームでスタック全体に関する情報をすばやくチェックし、てきぱきと指示メッセージを送りたいと思うでしょう。この数十年の間、機械学習、従来型のAI、AIOps、そして今日の生成AIなどの新しいテクノロジーが登場するたびに、開発者やエンジニアはこの理想の実現を期待してきました。それは実現したのでしょうか？

AIや機械学習が効率を向上させる

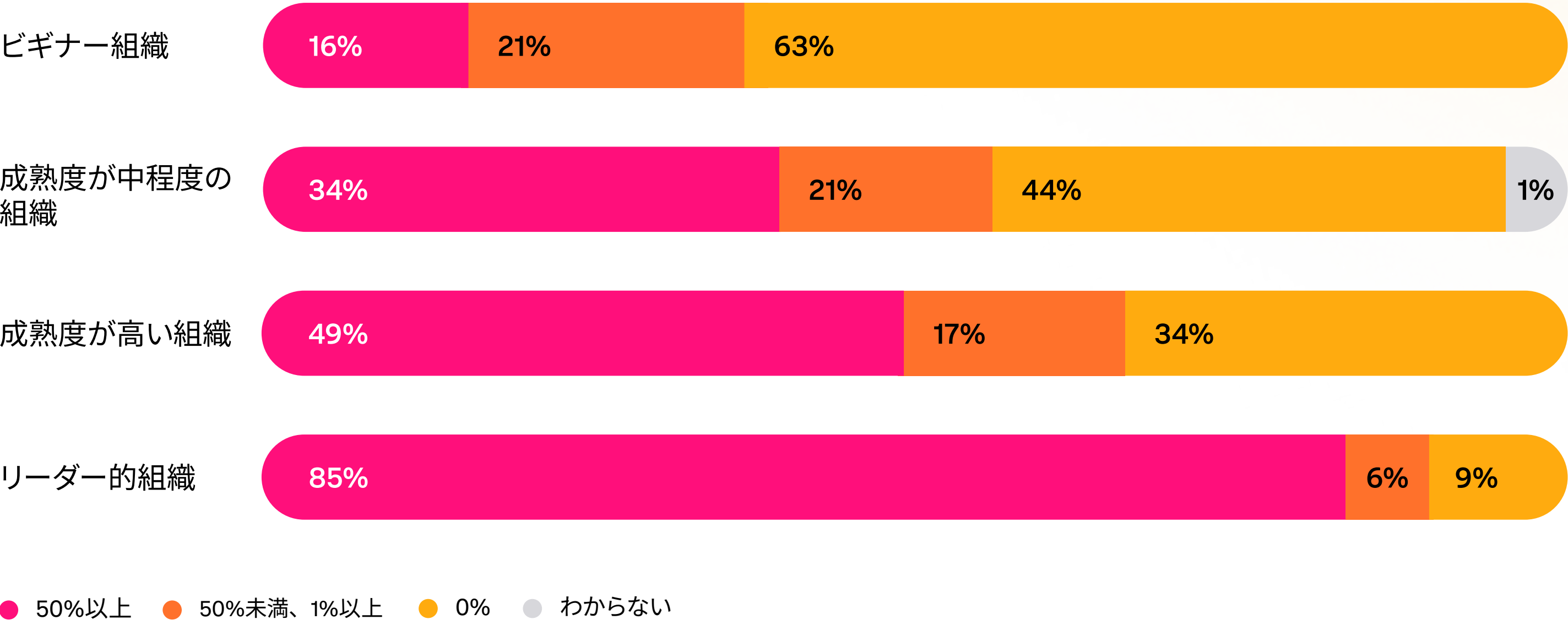
オブザーバビリティツールでのAIと機械学習の活用は、すでに当たり前になっています。調査ではほぼすべての回答者(97%)が、AIや機械学習を組み込んだシステムを利用してオブザーバビリティの運用を拡張しており、昨年の66%から大幅に増加しました。

回答者、特にリーダー的組織は、従来型のAIと機械学習を活用して業務の効率を向上させ、大きな成果をあげています。具体的には、56%がイベントの相関付けとアラートの優先順位付け、53%が解決策の提案に利用しています。リーダー的組織では解決策の提案での利用率が高く、その割合は91%にのびりました。

SREの方はよくご存知のとおり、アラート疲れは現実起きています。AIと機械学習は、その緩和に役立ちます。調査では、全体の57%がアラートの量が問題になっていると回答しています。AIと機械学習の相関付け機能はその打開策になり得ます。多くの組織がすでに、AIや機械学習を組み込んだシステムを問題の修復に利用し、34%が、1カ月に発生するオブザーバビリティ関連のアラートのうち半数以上をこの方法で解決しています。ここでもリーダー的組織は突出しており、85%がアラートの半数以上をAIや機械学習で解決していると回答しています。ビギナー組織で同様に回答した割合はわずか16%でした。

根本原因分析も、データのグループ化に手間がかかり、あまり楽しい仕事ではありません。そしてここでも、AIと機械学習が活躍します。調査では、全体の4分の1が、根本原因分析の中で特に大変な作業としてデータの相関付けと分析を挙げ、次いで22%が、データの収集と集約を挙げています。AIと機械学習はこの両方に役立つため、回答者の半数以上(55%)が、AIや機械学習を組み込んだツールを調査と根本原因の特定に活用しているのは当然と言えるでしょう。

リーダー的組織はアラートの解決にAIや機械学習を活用



生成AIへの興味は尽きない

生成AIはオブザーバビリティの新たな希望の光であり、オブザーバビリティチームはそれが自分たちの業務をどのように変えてくれるかに興味津々です。多くの人がまず思いつくのはチャットボットやAIアシスタントでしょう。AIアシスタントは、山のようなデータをくまなく調べて、最も関連性の高い情報を見つけ出し、有用な分析を実行したり、解決策を提案したりしてくれます。ユーザーが平易な言葉で質問するだけで、その情報を深く掘り下げ、コンテキストを取得し、最終的には根本原因を特定します。クエリ言語を習得する必要がないため、経験の浅いチームメンバーやビジネスユーザーでも、必要なときにインサイトを取得できます。

調査では、回答者の84%が、オブザーバビリティプラットフォームに組み込まれた生成AI機能、特にチャットボットやAIアシスタントの利用を検討しています。用途としては、データ分析(66%)と問題の解決策の提案(60%)が多く挙げられました。ただし、興味はあるものの、実際に導入している組織は13%にとどまっています。

評価はしているものの実際の導入につながらないのには、それなりの理由があります。最も大きな理由は、生成AIを組み込んだオブザーバビリティソリューションが市場でもまだ新しいことです。ベンダーは準備を進めているものの、一般提供されている製品はごくわずかです。そのため、オブザーバビリティチームは、どのように生成AI機能を活用し、日常業務のワークフローに組み込むかをまだ明確に決められずにいます。AIモデルを自社で作成してオブザーバビリティプラットフォームに組み込むという方法もありますが、これにはかなりの時間、費用、労力が必要になります。

さらに、多くの組織がまだ内部ポリシーと手順の作成に取り組んでいる段階であるため、オブザーバビリティチームにとっては、生成AIの使用が組織で許可されるかどうかすら定かではありません。Splunkのレポート『[2024年セキュリティの現状：競争が激化するAIの活用](#)』では、セキュリティ担当者の34%が、生成AIに関する組織の正式なポリシーが確立されていないと回答しています。

多くの組織が生成AIを探索しているものの、頂点まで到達した組織はごくわずか

13%

これらの機能を実際に導入している

84%

興味がある、評価中、オブザーバビリティツールに組み込まれた生成AIを試験導入中

3%

興味がない/わからない

オブザーバビリティを推進して リーダーを目指す

「オブザーバビリティのリーダー的組織に仲間入りするには、現状を維持するだけでなく、先陣を切ってイノベーションを推進することが重要です。データを実用的なインサイトに変えることができれば、業界をリードするだけでなく、再定義することも可能です」

Splunkオブザーバビリティ担当SVP兼GM、Patrick Lin

リーダー的組織は、環境全体を包括的に可視化することでダウンタイムを削減しています。仮にダウンタイムが発生した場合でも、すばやく復旧できます。また、開発者が大量の定型業務に忙殺されることなくイノベーションに取り組み、製品を短いサイクルでリリースすることで、ビジネスの成長につながっています。ほかにも、リーダー的組織が秀でている点はたくさんあります。ここからは、リーダー的組織がどのように他の組織を凌駕し、先進的なオブザーバビリティプラクティスを実現しているかを紹介します。

1. エンジニアリングチーム内でOpenTelemetryの推進者を見つける

リーダー的組織でOpenTelemetryの導入率が高い(78%)ことは、この標準に投資価値があることを示しています。実際、データ管理の向上、ベンダーロックインの回避、より広範なテクノロジーエコシステムの活用など、さまざまなメリットが得られます。ただし、導入は容易ではありません。その大きな理由が、OpenTelemetryに精通した人材がいないことです。その解決策の1つが既存の人材の活用です。この方法なら、組織が最新テクノロジーの導入や従業員の教育と成長に前向きであることを開発者に示すとともに、組織内のエンジニアをOpenTelemetryのエキスパートとして育てることで、導入の成功率を上げることができます。また、イノベーション精神を浸透させることで、将来的に新しい人材を惹きつけることもできます。

開発チームによるOpenTelemetryの学習意欲を高めるには、オブザーバビリティベンダーを頼る方法もありますが、お勧めは社内トレーニングプログラムを構築することです。そのためにはまず、チームの中で、OpenTelemetryの導入に積極的でやる気のある推進者を見つけます。推進者には、OpenTelemetryプロジェクトのWebサイトやGitHubで学んでもらい、CNCF Slackグループなどのコミュニティに参加してもらうとよいでしょう。

2. プラットフォームエンジニアリングを組織全体のドリームチームとして位置付ける

プラットフォームエンジニアリングは、すべてのチームにオブザーバビリティプラクティスを浸透させ、ソフトウェアエンジニアとSREがツールチェーンについての口論に時間を無駄にすることなく、コードの記述とリリースに全力を尽くせるようにするための鍵です。その価値を見過ごすのは大きな損失です。調査では、全体の4分の3 (73%)の回答者がプラットフォームエンジニアリングを導入していると答えました。ただし、専門のチームを作ることは第一歩にすぎません。経営幹部、マネージャー、担当者の賛同を得て、プラットフォームエンジニアリングチームを支援することも重要です。

リーダー的組織の58%は、開発者がプラットフォームエンジニアリングを競争上の差別化要因と考えていると回答しています。この差別化要因を活かすには、まず、プラットフォームエンジニアリングチームが付加価値をもたらすという認識を持つ必要があります。エンジニアや開発者にとっては、効率と生産性の向上という価値があります(リーダー的組織の48%が同意)。経営幹部にとっては、市場投入までの時間の短縮、技術的負債の削減、コードの信頼性の向上などのビジネス成果という形で価値がもたらされます。

3. オブザーバビリティデータとセキュリティデータを共有して強力な成果を生み出す

リーダー的組織の約4分の3 (73%)が、オブザーバビリティとセキュリティのワークフローおよびツールを統合してMTTRを短縮しています。オブザーバビリティチームとセキュリティチームの両方が質の高いコンテキストとデータを利用できれば、インシデントの根本原因をより簡単に特定できます。

ただし、この2つのチームの目標は異なり、その目標が相反する場合もあることを理解する必要があります。コラボレーションを段階的に進めることで、チーム間の摩擦を和らげることができます。まずは、両方のチームが共通して使用するデータソースとワークフローを洗い出します。最終的にはツールの統合を検討しますが、当面は優先度が高いデータソースをいくつか統合し、それらのデータソースに関連するワークフローを調整するのが最善の方法です。ネットワークチームがこれらすべてのデータにアクセスできるようにすれば、トラブルシューティングの際に、すべてのチームがさらに多くのコンテキストを利用できるようになります。

4. ビジネスに影響が出る前にテレメトリパイプラインのコストを抑制する

データ管理にこだわるのは良いことです。データの収集量、送信方法、送信先を管理すれば、準備(ラングリング)のコストを節約し、既存のデータからより多くの価値を引き出すことができます。

リーダー的組織は、重要なコスト抑制策として階層化(57%)などのデータ管理技法を取り入れています。データの階層化は、メトリクス、ログ、トレースのいずれでも、すべてのデータが同じ価値を持つわけではないという考え方に基づいています。そのため、優先度の低いデータを低コストのコールドストレージに移動することでコストを削減できます。そのデータが必要になったときは、統合分析などの機能を使うことでデータを移動することなく利用できます。

5. AIを活用してアラート疲れを軽減し、未知の未知を発見する

調査では、全体の57%が、オブザーバビリティソリューションで生成される過剰なアラートが問題になっていると回答しています。そこで役立つのがAIと機械学習です。AIや機械学習を組み込んだツールを使えば、異常の検出やイベントの相関付けの精度と効率を向上させて、この問題を緩和できます。実際、リーダー的組織の85%が、アラートの半数以上をAIや機械学習によって処理しています。AIを組み込んだツールでは、同じインシデントに関連する複数のアラートをグループ化したり、高度な分析を適用して、生成されるアラートの量を全体的に抑えるなど、いくつかの方法でノイズを減らすことができます。

AIOpsの主なユースケースの1つに対処することで、根本原因分析の迅速化や「未知の未知」のプロアクティブな検出、または潜在的な問題の予測による顧客側のインシデントの防止などの他のユースケースにも焦点を当てることができます。

6. 外部運用のネットワークを含むネットワーク全体を可視化する

エンドツーエンドのオブザーバビリティを実現するにはインフラ全体を可視化する必要がありますが、コンテナ、パブリッククラウド、分散ネットワークなど、近年普及しているテクノロジーの可視化は容易ではありません。リーダー的組織では可視化が進んでおり、パブリッククラウド環境は77%、オンプレミスインフラは74%、アプリケーションは71%が「かなり可視化できている」と回答していますが、組織が所有および運用していないネットワークインフラは例外で、かなり可視化できていると回答した割合は45%にとどまりました。

この問題への対応策の1つは、組織が運用するネットワークだけでなく、組織のユーザーが利用するすべてのアプリケーションとサービスについてもインサイトを提供するツールを導入することです。インフラ自体は管理できなくても、サードパーティ API、ISPネットワーク、BGP (Border Gateway Protocol)のいずれに問題があるかを把握するなど、可視性を高めることで、パフォーマンス低下といった問題を特定し、適切に対応できます。ただし、その場合、特定のワークロードを他の環境に移行したり、SDN (ソフトウェア定義ネットワーク)を使ってトラフィックを再ルーティングしたりする必要が生じることもあります。

Splunkで オブザーバビリティの リーダー的組織 を目指す



日本語ブログ

オブザーバビリティのトレンドについて、さまざまな業界のリーダーが、AI、データ管理、開発者のイノベーションなど、今日の喫緊の課題にどのように取り組んでいるかを紹介します。

[詳細はこちら](#)



ダウンタイムの隠れたコスト

世界中の企業が直面している4,000億ドルの問題を、レジリエンスの高い組織がどのように回避しているかを紹介します。

[ダウンロードはこちら](#)

業界別の特徴

世界共通の代表的な4つの業界について、主要なインサイトを紹介します。

製造

製造業は、効率化への投資に関して他の業界をリードしています。イベントのグループ化とアラートの相関付けをほとんどまたは完全に自動化している企業は40%にのぼります(全業界の平均は32%)。また、アラートの処理にAIや機械学習テクノロジーを活用している企業も多く、異常検出の55%をはじめ、さまざまなユースケースで導入企業が半数を超えています。

効率の向上は具体的な形でメリットをもたらしています。たとえば、80%の企業が、アプリケーションの問題を数時間で検出できると回答しています。アプリケーションの信頼性とパフォーマンスの目標を達成する自信は、競争優位性の確立につながります。製造業では半数の企業が「非常に自信がある」と回答し、全業界の平均である41%を上回っています。

オブザーバビリティに関する主な課題については、3分の1の企業が、大量のデータを処理しきれないことを挙げています。ただし、少なくとも、データに関する問題の解決策の見込みはあるようです。製造業では、他の業界と比べて、データの集約(44%)とデータの階層化(43%)がコスト管理に不可欠と考える企業が多く見られました。

通信・メディア

通信・メディア業界は、オブザーバビリティプラクティスの成熟度が高く、約4分の1 (24%)の企業が「成熟度が高い組織」で(全業界平均は17%)、10%が「リーダー的組織」でした。

驚くべきは、多くの企業がオブザーバビリティプラクティスを最近導入したばかりで、59%が過去2年以内に導入していることです。しかも、その2年間でツールの数は平均24.6個に増え(全業界の平均は23.1個)、オブザーバビリティへの投資から得た1年あたりのビジネス価値は平均390万ドルにのぼります。この金額は、全業界の平均である340万ドルを50万ドルも上回っています。

この成功の要因の1つは、プラットフォームエンジニアリングが広く浸透していることです。75%の企業が専門チームを作り、そのうち35%がプラットフォームエンジニアリングを幅広く取り入れていると回答しています(全業界の平均は27%)。そのため、76%の企業が、新製品や新機能がリリースされたら真っ先に導入する、または早期に導入する「アーリーマジョリティ」に入っていると回答し、全業界の平均である66%を大きく上回っているのも納得できます。

行政・公共機関

行政・公共機関は、オブザーバビリティの導入で後れをとっており、半数以上(54%)がビギナー組織に該当します(全業界の平均は45%)。その大きな要因は、以下のように組織の環境をかなり可視化できていると回答した割合が低いことです。

- ・プライベートクラウド：38% (全業界の平均は47%)
- ・パブリッククラウド：35% (同47%)

可視性の向上はオブザーバビリティの成功の基盤であるため、オブザーバビリティのメリットを享受している組織も少なく、アプリケーション開発の迅速化が23% (全業界の平均は34%)、問題の検出時間の短縮が19% (同34%)にとどまりました。

実際、行政・公共機関の約3分の1 (29%)が、オブザーバビリティ関連のツールやテクノロジーに対する投資不足を感じています(全業界の平均は15%)。今後、行政・公共機関は、オブザーバビリティプラクティスを進化させ、成熟させていく必要があります。というのも、現在の投資がすでに測定可能なメリットを生み出しているためです。この業界の組織は、オブザーバビリティのツールやソリューションに毎年平均120万ドルを投資し、240万ドルのビジネス価値を生み出しています。

金融サービス

金融サービス業界は、他の業界よりも可視化が進んでいます。すべてのタイプのインフラで「可視化がかなり進んでいる」と回答した割合が全業界の平均を上回りました。

- ・組織が所有および運用しているネットワークインフラ：53% (全業界の平均は49%)
- ・パブリッククラウドインフラ：50% (同47%)

これらの基本的な機能を確立した金融サービス企業の多くは、AIOpsなど、他の領域への投資を進めています。57%がAIOpsツールを活用し、複数の監視システムのデータを統合して可視性を向上させるなどのユースケースを実践しています。こうした先進的な取り組みが功を奏し、67%の企業が、ROIが期待を上回っていると回答しています。

金融サービス業界の企業は、オブザーバビリティプラクティスの成熟とともに、OpenTelemetryを導入する際の互換性の課題に直面しており、57%の企業が互換性の問題に直面していると回答しています(全業界の平均は46%)。ただし、この互換性の問題は、プロジェクトが成熟し、ベンダーがOpenTelemetryとの連携を強化するにつれて、自然に解決していくでしょう。OpenTelemetryの成長に伴う課題がある中でも、金融サービス企業はすでにメリットを享受しています。たとえば、半数近く(45%)が、データに対する主導権と所有権が向上したと回答しています。

国別の特徴

世界の10カ国についての主要なインサイトを紹介します。

オーストラリアおよびニュージーランド

オーストラリアおよびニュージーランド(ANZ)では、4分の1以上 (26%)の組織がリーダー的組織に該当します(すべての国の平均は11%)。オブザーバビリティツールへの投資は年間230万ドルで、調査対象となった他のすべての国を上回りました。そのため、実現したビジネス価値は年間560万ドルにのぼり、他のすべての国の平均である340万ドルを200万ドル以上も上回っています。

「可視化がかなり進んでいる」と回答した組織も全体的に多く、プライベートクラウド環境が61% (すべての国の平均は47%)、所有も運用もしていないネットワークインフラが44% (同26%)でした。また、問題の検出数が多いだけでなく、アラートの忠実度が高いと回答した組織が67%で、すべての国の中で最多でした。

65%の組織が、オブザーバビリティとセキュリティの両方を担う役職を設けています(すべての国の平均は53%)。オブザーバビリティとセキュリティのワークフローやデータを統合すれば、より多くのリソースを活用してインシデントをすばやく解決できます。そのため、MTTRが数時間または数分と回答した組織が86%にものぼるのも、納得の結果です。

開発者が業務時間の56%をイノベーションや実験に費やしている点も、他のすべての国を上回ります。その効果は、アプリケーション開発チームが新しいデジタル製品やサービスを年間で平均13.3件リリースし、他のほとんどの国を上回っていることに表れています。

フランス

フランスでは、オブザーバビリティへの取り組みが全体的に初期段階にあり、約半数がビギナー組織に該当します。オブザーバビリティプラクティスが十分に確立していない場合、インシデントが発生したときの検出、対応、復旧手段が十分に備わっていない可能性があります。これは、36%の組織がデジタルレジリエンスに関する正式なアプローチをまだ策定していないという結果と一致しています。

オブザーバビリティソリューションへの投資によって実現したビジネス価値は年間平均260万ドルで(すべての国の平均は340万ドル)、調査対象の国の中で最も低い結果になりました。

フランスの組織がオブザーバビリティプラクティスを強化するには、まず、大量のデータの処理と相関付けの課題に対応する必要があります。31%の組織が、収集するデータの量が多すぎて人手で処理しきれず、複数のソースのデータを相関付けるのに時間がかかりすぎると回答しています。

オブザーバビリティ強化のもう1つの鍵がOpenTelemetryです。OpenTelemetryを導入すれば、データの管理能力が向上し、ベンダーロックインを回避して、より広範なテクノロジーエコシステムを活用できます。オブザーバビリティソリューションでOpenTelemetryを利用していない組織は現時点で半数以上(56%)ありますが、その価値に対する認識は確実に広がっており、92%の組織が、オブザーバビリティベンダーがOpenTelemetryに対応することが「非常に重要」または「重要」と回答しています。

ドイツ

ドイツでは、組織がオブザーバビリティのアプローチに積極的に対応しており、使用するツールの数が少なく、ポイントソリューションよりもプラットフォームソリューションを好む傾向があります。使用しているオブザーバビリティツールは平均17.8個で、すべての国の平均である23.1個を大幅に下回っています。一方で半数以上が、データの変換(57%)や階層化(62%)などのオブザーバビリティ機能に単一のプラットフォームを使用する傾向があります。

ツールの数が少なければ、一般的にコンテキストの切り替えが少なくなるため、調査の効率が向上します。そのため、85%の組織が、今後MTTDを短縮することに「強い自信がある」と回答しています(すべての国の平均は78%)。また、年間のダウンタイム発生頻度が平均5.9件で、調査対象の他のすべての国の平均である8.5件を大幅に下回りました。

成熟度に関しては、中程度の組織が最多(32%)でした。AIOpsを導入すると、データの相関付けなどに効果があり、オブザーバビリティプラクティスのさらなる成熟につながります。ドイツでは、異なるソースタイプのデータを相関付けるためにAIOpsを利用する組織の割合が38%で、他の国を下回っています(すべての国の平均は46%)。一部のデータしか相関付けできていないと回答した組織が37%にのぼることを考えると(すべての国の平均は28%)、AIOpsの導入が今後の課題と言えるでしょう。

インド

インドでは、リーダー的組織の割合が20%で、すべての国の平均である11%の約2倍にのぼります。これはイノベーションに対する熱心な取り組みの成果と考えられ、96%の組織がソリューションに投資し、開発者がインシデントやアラートの処理に費やす時間を削減し、新しい製品や機能の開発に費やせる時間を増やしています。

インドの組織は新しいテクノロジーの導入にも積極的です。オブザーバビリティツールに組み込まれた生成AI機能を17%の組織がすでに利用し、14%が試験的に導入しています。また、67%が、主に使用するオブザーバビリティソリューションでOpenTelemetryが使われていると回答し、すべての国の平均である58%を上回っています。その効果はすでに現れており、61%が、データに対する主導権と所有権が向上したと回答しています。

インドの組織は、イノベーションに注力し、新しいテクノロジーを導入することで、アプリケーションの稼働時間と品質を最大限に向上させています。アプリケーションの信頼性とパフォーマンスの目標達成に「非常に自信がある」と回答した組織は、半数を超える52%にのぼりました(すべての国の平均は41%)。

イタリア

イタリアでは3分の2がビギナー組織で、リーダー的組織はわずか5%でした。オブザーバビリティプラクティスの導入が進んでおらず、MTTRの短縮やイノベーションの推進など、リーダー的組織が実現しているメリットをあまり享受していません。オブザーバビリティの向上によって問題の解決時間が大幅に短縮したと回答した割合は22%で、すべての国の平均である34%をかなり下回りました。また、新しいデジタル製品がリリースされてもなかなか導入しない「レイトマジョリティ」が11%を占め、すべての国の平均(6%)のほぼ2倍にのぼりました。

イタリアの組織は世界に後れをとっており、その差は拡大し続けています。過去12カ月間で根本原因の特定にかかる時間が短縮したと回答した割合は59%にとどまりました(すべての国の平均は71%)。また、今後MTTRを短縮できるかどうかについて「自信がある」と回答した割合も68%にとどまっています(すべての国の平均は80%)。

さらに、すべての領域に必要な資金が行き渡っていると回答した割合はわずか15%でした(すべての国の平均は28%)。オブザーバビリティの成熟度を向上させるには、まず、チームがこれまでのオブザーバビリティ投資のROIを強調し、経営幹部にその価値を証明して、資金不足を解消する必要がありますでしょう。

日本

日本では、3分の2 (66%)がビギナー組織に該当します。一方で、リーダー的組織の割合が12%にのぼるのは特筆すべき点です。

オブザーバビリティの成功を阻む要因の1つとして、特にビギナー組織において、アラートの忠実度に対する自信の低さが挙げられます。アラートが実際の問題につながると回答した割合は49%にとどまりました(すべての国の平均は61%)。アラートの忠実度が低ければ、オブザーバビリティソリューションがインシデントを報告する前に、エンドユーザーが報告することが多くなります。実際、顧客からの指摘を受けて気づくインシデントの割合が平均で51%にのぼり、他のどの国よりも高い結果になりました。

日本の組織では、オブザーバビリティチームが人員不足に陥ったことが複数回あると回答した割合が55%にのぼり、人材の確保に苦労していることがうかがえます。ただし、その対策は始まっています。約3分の2 (63%)の組織が、今後1年間でオブザーバビリティ人材を確保するための予算を増額する予定で、AIや機械学習の導入による効率化にもリソースを投入しています。すでに60%の組織が、異常の検出にAIや機械学習を活用し、すべての国の平均である51%を上回っています。昨年調査では、日本はこの点で後れをとり、オブザーバビリティツールに組み込まれたAIや機械学習機能を利用する組織がわずか15%であったことを考えると、目覚ましい進歩です。

シンガポール

シンガポールでは、18%がオブザーバビリティのリーダー的組織に該当します(すべての国の平均は11%)。そのため、イノベーションと進化の点で非常に優れています。アプリケーション開発チームが過去1年間にリリースした新しいデジタル製品やサービスの数は平均13.5件で、他のすべての国を上回っています。

イノベーションのペースを維持するために、シンガポールの組織は、オブザーバビリティチームの負担の軽減に取り組む必要があるかもしれません。チームの重要なメンバーが燃え尽き症候群によって離職したと回答した割合は82%にのぼります。アラートの忠実度の低さもチームの負担になっていると考えられ、31%の組織が、誤検知の数が「非常に深刻」だと回答しています(すべての国の平均は13%)。

チームのさらなる負担軽減策として、オブザーバビリティツールの数を減らすことも検討すべきでしょう。シンガポールの組織は平均で28個のツールを使用しています。また、現時点でプロセスが完全に手作業であると回答した割合が20%にのぼるため(すべての国の平均は7%)、イベントのグループ化とアラートの相関付けの自動化も有効です。

英国

英国では、3分の1以上(34%)の組織がオブザーバビリティジャーニーで成熟度が中程度の段階にあり、ビギナーの段階から前進しているのは明るい兆しです。一方で改善の余地もあり、リーダー的組織は8%にとどまりました。

オブザーバビリティプラクティスの成熟度が低いため、イノベーションに遅れが見られます。新しい製品やサービスのリリース数は年間で平均10.8件で、イノベーションのペースに関しては調査対象の他のほとんどの国よりも後れをとっている結果になりました。

全体として、英国の組織は、すでに具体的なメリットが出ているオブザーバビリティへの投資を続ける必要があります。オブザーバビリティツールへの投資は年間で平均130万ドルで、そこから生じたビジネス価値は350万ドル(すべての国の平均以上)にのぼります。

英国の組織に効果的だと考えられる投資領域は、根本原因の特定です。過去1年間で根本原因の特定にかかる時間が短縮したと回答した割合は65%にとどまりました(すべての国の平均は71%)。インシデントをより迅速に検出するには、AIOpsの導入も効果的です。これにより、調査を自動化し、インテリジェンスを強化できます。現時点でAIOpsを導入している組織は46%にとどまります(すべての国の平均は52%)。

米国

オブザーバビリティの成熟度に関しては、米国はすべての国の平均と一致しています。

米国の組織が優れている点の1つは、チームの効率化への投資です。オブザーバビリティチームの生産性向上のために生成AIを試験的に導入している組織は93%にのぼり、そのうち84%がすでに大きな効果をあげていると回答しています(すべての国の平均は74%)。

また、ツールに組み込まれたAIOps機能をオブザーバビリティチームが使用していると回答した割合が60%にのぼり(すべての国の平均は52%)、根本原因の特定やインシデントの修復などのユースケースによく使われています。そのため、73%の組織が、ROIが期待を上回ったと回答しています。

オブザーバビリティプラクティスの効果を評価する指標の1つが、顧客が気づく前に問題を検出できるかどうかです。その点で米国の組織は高い成果をあげています。顧客からの指摘ではなくオブザーバビリティソリューションによって検出したインシデントの割合は平均で58%にのぼり、調査対象となった他のすべての国を上回りました。その要因として、AIOpsの導入が進み、優れたインテリジェンスを活用して根本原因の特定とインシデントの修復を強化できることが考えられます。

調査方法

調査は、2024年5月から6月にかけて、IT運用の現場担当者、マネージャー、経営幹部、開発者、エンジニア、アーキテクト、SREを含む合計1,850人を対象に行われました。対象となった国は、オーストラリア、フランス、ドイツ、イタリア、インド、日本、ニュージーランド、シンガポール、英国、米国の10カ国です。対象となった業界は、航空宇宙・防衛、ビジネスサービス、消費財、教育、金融サービス、政府機関、ヘルスケア、ライフサイエンス、製造、テクノロジー、メディア、石油・ガス、

リテール(小売り)・卸売り、通信、運輸・輸送・物流、公益の16種類です。

20種類の自己報告データポイントを評価する、4つのレベルで構成された新しいオブザーバビリティ成熟度フレームワークに基づいて、回答者の組織をオブザーバビリティ成熟度の4つの段階のいずれかに分類しました。

各段階に分類された組織の内訳は次のとおりです。

- ・第1段階：ビギナー組織(45%)
- ・第2段階：成熟度が中程度の組織(27%)
- ・第3段階：成熟度が高い組織(17%)
- ・第4段階：リーダー的組織(11%)

Splunkについて

シスコの一員であるSplunkは、組織のデジタルレジリエンス向上を支援します。世界の名だたる組織がデジタルシステムのセキュリティと信頼性を維持するために、Splunkのセキュリティとオブザーバビリティの統合プラットフォームを利用しています。Splunkのソリューションを導入すれば、インフラ、アプリケーション、セキュリティに関するインシデントが大規模な問題に発展する前に防止し、障害の発生時にはデジタルシステムを迅速に復旧して、新しいビジネスチャンスをつばやく掴むことができるため、Splunkは多くの組織から信頼されています。

SplunkのSNS



splunk>
a **CISCO** company

© 2024 Splunk LLC. 無断複写・転載を禁じます。Splunk, Splunk>, および Turn Data Into Doing は、米国およびその他の国における Splunk LLC の商標または登録商標です。他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。

24_CMP_report_state-of-observability_v18_JP

