2023年
オブザーバビリティの現状

グローバル調査：IT環境がますます複雑になる中で、
先進的な組織は可視化を推進し、レジリエンスを
強化して、ROIを大きく向上させている

splunk>

オブザーバビリティが定着

オブザーバビリティ (可観測性)は、かつては最先端の概念でした。それが今では「当たり前」になっています。数年前までは先進的な組織のみが導入していたオブザーバビリティは、今日のIT環境の特徴ともいえる複雑に絡み合ったシステムを可視化する基盤として現代の企業を支えています。

Splunkが2年前にオブザーバビリティに関する調査を開始して以来、オブザーバビリティの向上に取り組む組織の数は大幅に増え、今回の調査ではオブザーバビリティプロジェクト専門の担当者がいると回答した組織が87%にのぼりました。これだけ多くの組織がオブザーバビリティ導入の流れに乗るのには十分な理由があります。

2023年 オブザーバビリティの現状

Splunkは、組織のオブザーバビリティを担う1,750人の現場担当者、マネージャー、エキスパートを対象に、今日までの成果から将来の展望まで、オブザーバビリティを取り巻く状況を調査しました。特に目立った成果は以下のとおりです。

- オブザーバビリティのリーダー的組織では、オブザーバビリティツールのROIが期待をはるかに上回ったと回答した割合がビギナー組織の7.9倍にのぼります。
- リーダー的組織では、アプリケーションの可用性とパフォーマンス要件への対応に100%自信があると回答した割合が89%に達し、ビギナー組織の3.9倍にのぼりました。
- さらにリーダー的組織では、予定外のダウンタイムやサービスの深刻な問題の解決を何時間あるいは何日もかけることなくわずかな時間で完了できると回答した割合も、ビギナー組織の4倍にのぼりました。

オブザーバビリティを体系的に実践している組織は、複雑なIT環境を詳細に可視化することで、障害の防止、問題解決の迅速化、アプリケーションの信頼性向上を実現し、最終的に収益と顧客満足度の向上につなげています。リーダー的組織とビギナー組織の定義については後ほど説明することにして、まずは今日のオブザーバビリティの状況を見ていきましょう。

オブザーバビリティ実践の成熟度を高めることは、信頼性、パフォーマンス、収益、顧客満足度の向上につながります。

羅針盤としてのレジリエンス

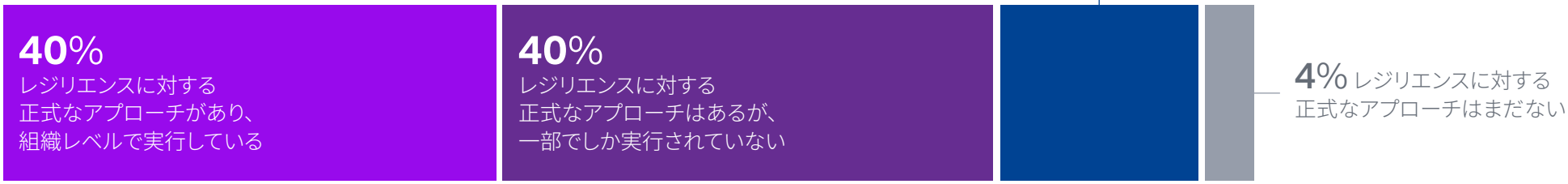
多くの組織がレジリエンスへの投資を強化しています。その背景には、レジリエンスの低さが、障害の頻発による顧客離れ(73%)や生産性の低下に伴うイノベーションの後れ(74%)につながるという不安があります。そのため、全体で95%の組織が、オブザーバビリティリーダーがレジリエンス戦略とその優先順位付けや投資判断についてビジネス部門のリーダーと1年前よりも積極的にコラボレーションしていると回答したのもうなずけます。オブザーバビリティの成熟度の6つの指標すべてが優れているリーダー的組織に限ると、この割合は100%に達します。ただし、リーダー的組織自体の割合は全体の10%にとどまります。成熟度が最も低いビギナー組織は全体の33%を占めます。4段階の成熟度の定義については第2部で詳しくご説明します。

調査では、今後1年間のレジリエンス戦略について、ソリューション投資の具体的な計画があるかどうかを尋ねました。その結果、約半数の回答者が以下の目的を達成するためのソリューションに投資する予定だと回答しました。

- **顧客やユーザー向けのサービスの迅速な復旧**
- **セキュリティインシデントへの迅速な対応と修復**
- **テクノロジー環境全体の可視化**
- **従来の事業継続計画とレジリエンス向上の取り組みの融合**
- **セキュリティインシデントのダウンストリームへの影響の把握**

これらは組織にとって、円滑な事業運営、システムのセキュリティ確保、顧客の満足度維持に欠かせない能力です。ここ数年間の混乱を教訓とすると、この先どのような困難が待ち受けているにせよ、次の嵐に備えてレジリエンス戦略を構築することは必須です。

レジリエンス向上のメリットは明らかでも進捗状況はさまざま



複雑化がオブザーバビリティの追い風に

すべての物事は無秩序へと向かう。これは自然の摂理です。オブザーバビリティのエコシステムも例外ではありません。調査では、IT環境の拡大と複雑化を反映して、過去1年間で使用するオブザーバビリティツールや機能が「増えた」と回答した割合が81%に達し、「大幅に増えた」と回答した割合も32%にのぼりました。

これは自然な成り行きと言えるでしょう。つまり組織は、ツールを増やし、システムを拡張し、より多くのアプリケーションを作って、より多くの収益源を確保しようとした結果、IT環境が無秩序に拡大して収拾がつかなくなり、可視性の向上が急務となって、オブザーバビリティへと行き着いたのです。

ただし、ツールの数が増えているからと言って、必ずしも利用するベンダーが増えているとは限りません。44%の組織がベンダー数が増えた(12%が大幅に増えた)と回答する一方で、40%がベンダー統合を進めていると回答しています。それでも、管理すべきベンダーとツールの数は膨大で、すべてのIT担当者が夢見る「単一画面ですべてを管理」という理想は崩れ、遠のいていくばかりです。

調査方法

Enterprise Strategy Group社が、2022年12月12日 から2023年1月19日 に か け て、従業員数500人以上の組織を対象に、組織のオブザーバビリティ状況に詳しいIT運用/アプリケーション開発/DevOpsのリーダー 1,750人にアンケートを実施しました。

10カ国

対象となった10カ国は次のとおりです：
オーストラリア、カナダ、フランス、ドイツ、インド、日本、ニュージーランド、シンガポール、英国、米国

16の業界

対象となった業界は次のとおりです：航空宇宙・防衛、消費財、教育、エネルギー、金融サービス(銀行、証券、保険)、政府機関(連邦/中央、州/地方)、ヘルスケア、テクノロジー、ライフサイエンス、製造、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

複雑さについて言えば、調査対象の組織が使用する自社製ビジネスアプリケーションの数は平均165個にのぼり、約半分の51%がパブリッククラウド、残り49%がオンプレミスで運用および管理されています。また、これらのアプリケーションのうち56%が全体または一部にクラウドネイティブアーキテクチャを採用し、44%が完全にレガシー/モノリシックアーキテクチャで作られています。

この数年、クラウドこそが近い将来アーキテクチャの世界を制すると言われ続けてきた中で、この結果は驚きです。モノリシックアプリケーションは今も健在で、これらのレガシーアプリケーションをクラウド向けにリファクタリングするのが容易ではないことを考えると、今後もハイブリッドアーキテクチャが共存することは間違いないでしょう。

この先クラウドが衰退することはないものの、レガシーアプリケーションをクラウドネイティブアーキテクチャに積極的にリファクタリングしている組織はわずかながら減少しています。

- **自社製アプリケーションの中でクラウドネイティブアプリケーションが占める割合を今後1年間で増やす予定だと回答した割合は58%で、前年の67%から減少しました。**
- **クラウドネイティブアプリケーションの割合を変える予定はないと回答した割合は40%で、前年の32%から増加しています。**
- **クラウドネイティブアプリケーションの割合を減らす予定だと回答した割合は2%で、昨年の1%からわずかに増加しています。**

クラウドが深く浸透すると同時に、ハイブリッドアーキテクチャが残り続けるならば、複雑さを克服し、異なる環境を一元的に監視するために、オブザーバビリティは今後も重要であり続けるでしょう。

完全クラウド化は現実的ではありません(少なくとも今のところは)。今でもハイブリッド環境が優勢です。

44%：モノリシックアーキテクチャで構築された自社製アプリケーションの割合(平均)

86%：オブザーバビリティソリューションの選定でハイブリッドアーキテクチャに対応する柔軟性を重視している組織の割合(ただし半数の組織はハイブリッドアーキテクチャを改善領域と認識)

仲間の助けを借りて前進

オブザーバビリティツールの導入は進み、調査では73%の組織がオブザーバビリティツールを1年以上使用していると回答しています。それでも、これらのツールはまだ新しい存在であり、3年以上使用している組織は14%にとどまりました。

種類別に見ると、以下のツールが多くの組織で導入されています。

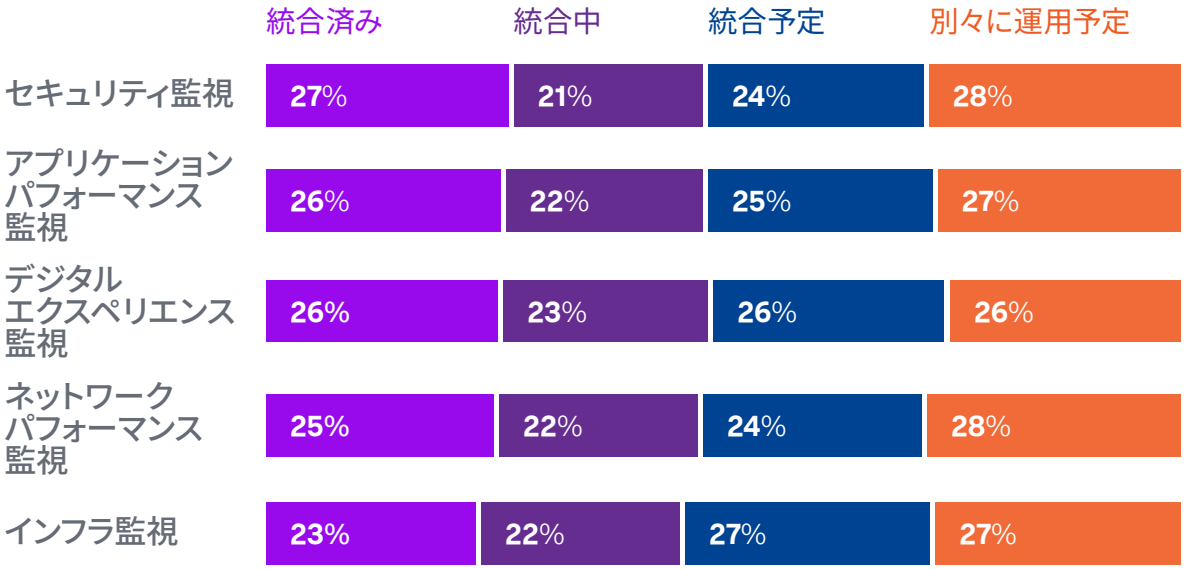
- **ネットワークパフォーマンス監視(79%)**
- **セキュリティ監視(78%)**
- **アプリケーションパフォーマンス監視(78%)**
- **デジタルエクスペリエンス監視(72%)**
- **インフラ監視(70%)**

これらのツールを使用する組織は昨年と比べて全体的に増えており、使用するオブザーバビリティツールや機能が増えたと回答した割合が81%にのぼったことと一致します。さらに、ツールの統合も進んでおり、オブザーバビリティツールをその他の監視プラクティスと統合する組織の割合が昨年よりも増えています。後ほど詳しく取り上げますが、リーダー的組織ではすべてのカテゴリでオブザーバビリティツールとの統合が進んでいます。

ただし、一口に「ツール」と言っても、その実態はさまざまです。調査では80%の組織が、オブザーバビリティに関する機能が追加されていないにもかかわらずベンダーが「オブザーバビリティツール」と呼び名を変えている従来型の監視ツールに遭遇したことがあると回答しています。こうした卑怯な手口、言うなれば「見せかけのオブザーバビリティ」は、組織が新しいツールを評価する時点で「明白な危険」と判断されても仕方ないでしょう。

統合のメリット

約75%の組織が最終的にすべての監視ツールやチームをオブザーバビリティと統合する予定だと回答していますが、目標の達成度はさまざまです。



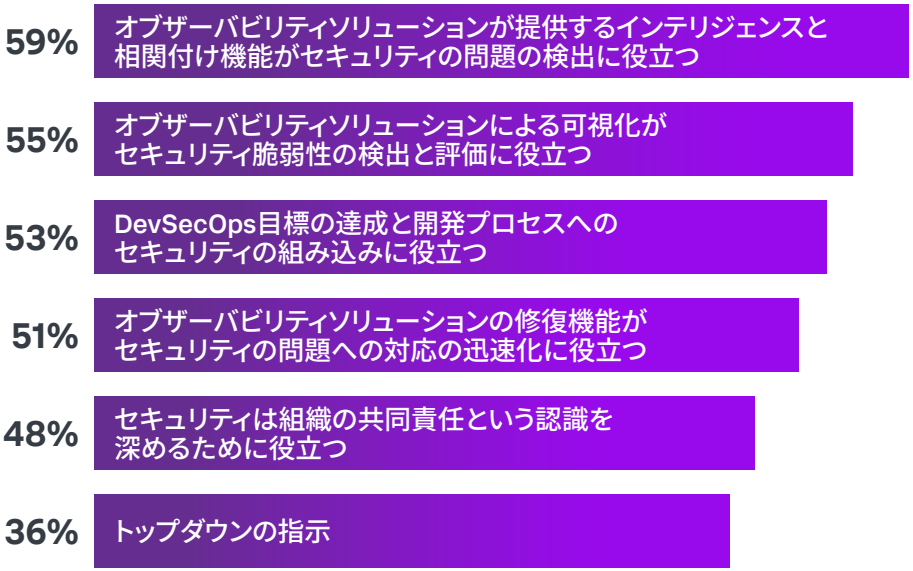
オブザーバビリティと最も統合されているのがセキュリティ監視です。昨年と比べると、セキュリティとオブザーバビリティの統合を推進する組織が増えています。この統合は相乗効果を発揮して可視性をさらに向上させ、インシデントに関する豊富なコンテキストを提供して、問題解決を加速します。

調査では、そもそもセキュリティとオブザーバビリティを統合しようと思った理由についても尋ねました。その結果、オブザーバビリティソリューションによる可視化は、セキュリティの脆弱性をより正確に検出および調査し、すばやく対応して修正するために有効である点が挙げられました。逆に、統合の理由として一番少なかったのは、トップダウンの指示です。つまり、セキュリティとオブザーバビリティの統合は、上から命令でやらされるよりも、自然な流れとして行われるケースが多いと言えます。

オブザーバビリティツールは、環境をより深く詳細に可視化できるように進化しています。この流れは当然、セキュリティとオブザーバビリティの統合に有利に働き、問題の未然の防止と特定、システムの円滑かつ安全な24時間運用といったさらなるメリットをもたらすでしょう。

相乗効果

オブザーバビリティとセキュリティ監視を統合する理由



AIや機械学習もオブザーバビリティツールとの相性は抜群です。ChatGPTがAIを世に広めるずっと以前から、オブザーバビリティチームはAI/機械学習を活用してオブザーバビリティツールを補強してきました。調査でも、AI/機械学習をすでに使用している組織は66%にのぼりました。一方、導入段階の組織は26%にとどまり、こうした新しい技術に興味がないと回答した組織はわずか1%でした。

また、AIOpsツールの評価も高く、従来のソリューションを上回る点として、問題の技術的な根本原因を自動的に特定できる(34%)、問題の発生を予測して顧客に影響が及ぶ前に対処できる(31%)、問題の影響が実際にどのくらい深刻であるかをより正確に判断できる(30%)ことなどが挙げられています。

これらのメリットは、問題を迅速に解決し効率をさらに向上させるためにも非常に効果的です。ただし、ここにもあの卑劣な手口が蔓延していることに注意が必要です。調査では76%の組織が「見せかけのAIOps」に遭遇したことがあると回答し、「見せかけのオブザーバビリティ」と並ぶ高い割合になりました。

91%：オブザーバビリティ目標の達成にAIOpsが重要だと考えている組織の割合

64%：AIOpsツールのROIが期待を上回った組織の割合

AIOpsの加速：AIOpsの一番のメリットとして、MTTD (平均検出時間)の短縮と根本原因分析の迅速化が挙げられています。

人材の潮目が変化

オブザーバビリティが一過性の流行ではないことが明らかになるにつれて、人材の状況も良い方向に向かっています。オブザーバビリティに詳しい人材を集めて専門チームを立ち上げ、ツールの標準化に取り組んでいると回答した組織は58%で、同人材がアプリケーション開発チームに参加するだけの組織の42%を上回りました。

昨年のレポートでは、オブザーバビリティ人材の確保が数とスキルの両方で深刻な課題になっていました。全体として人材不足はまだ続いており、IT運用チームのメンバーが足りないと回答した組織は85%、SRE/DevOpsエンジニアが足りないと回答した組織は86%にのぼります。

それでも今年は、一部とはいえ状況が好転しています。

- **十分な数のIT運用人材を確保できないと回答した割合が昨年の36%から今年は22%に減少しました。ただし、適切なスキルを持つ人材を確保できないと回答した割合は昨年の13%から21%に増加しています。**
- **71%の組織が、人員削減や一時解雇(約3分の1はそれが複数回発生した)が原因でチームの人手不足が続いていると回答しています。**
- **ただし、こうした大量解雇が市場の人材プールを充足させている可能性があります。数とスキルのどちらの面でも人材確保の課題はないと回答した組織が昨年の5%から今年は15%に増加したのはそのためかもしれません。**

リーダー的組織の35%が人材に関する課題はないと回答し、オブザーバビリティの成熟度が高い組織ほど優れた人材を十分に確保できていることがわかります。

専門人材の確保が多くの成果を生み、オブザーバビリティが一過性の流行ではないことが明らかになっています。

87%：オブザーバビリティプロジェクト専門の担当者がいる組織の割合

完全な可視化は目前に迫り ROIはすでに達成

アプリケーションの信頼性とパフォーマンス目標の達成に100%自信があると回答した割合は43%で、半分に届きませんでした。残りの約48%も多くの組織はある程度自信があると回答しましたが、それは逆に言うと、不安が残っているということです。オブザーバビリティのリーダー的組織では、100%自信があると回答した割合は89%にのぼります。ということは、この不安はオブザーバビリティツールが未成熟であることが原因ではなく、組織内の受け入れ態勢やマインドセットの問題かもしれません。

環境を構成する各要素(オンプレミスのレガシーインフラ、プライベートクラウドインフラ、セキュリティ態勢、コンテナなど)を「かなり可視化できている」と回答した組織の割合は52%にとどまりました。オブザーバビリティ向上の主な目的が可視化であることを考えると、これは憂慮すべき数字です。つまり、この点こそが重要な改善領域であり、多くのチームがパフォーマンス目標の達成に不安を感じている要因を探るヒントになるかもしれません。

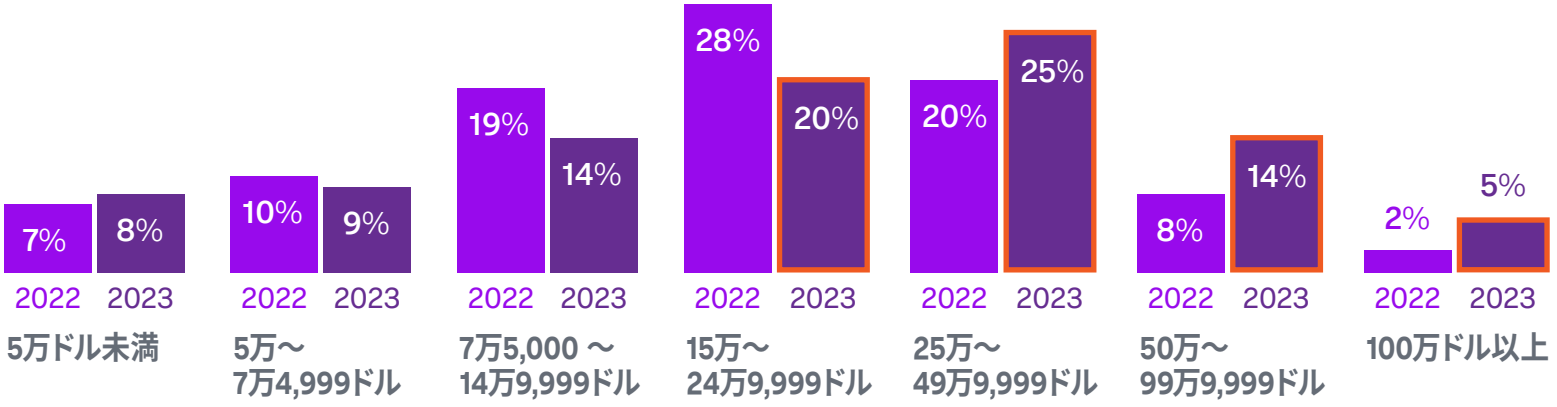
実際、ダウンタイムのように多大なコストがかかるインシデントにいまだ多くの組織が悩まされています。自社製のアプリケーションで過去1～2年に起きた、サービスに影響が及んだ問題について、ビジネス面への影響を尋ねた結果は以下のとおりです。

- **顧客満足度が低下した：49%**
- **収益が下がった：45%**
- **顧客を失った：38%**
- **評判が低下した：36%**
- **ビジネスへの影響はなかった：12%**

これらの問題の社内への影響についても尋ねたところ、多かった回答が、チームメンバーの離職者が増えたことと、オブザーバビリティ関連業務のアウトソースが増えたことで、ともに38%でした。

ダウンタイムのコストが上昇

約3分の2の組織でダウンタイムの1時間あたりのコストが15万ドル以上にのぼっています。

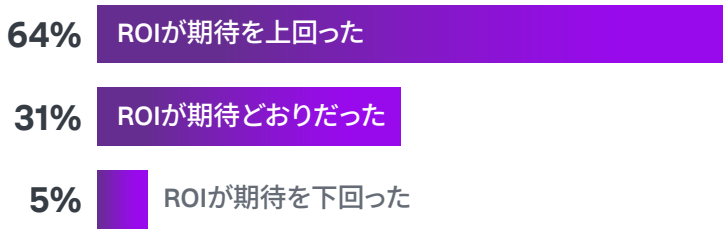


一方で、オブザーバビリティ向上の取り組みは見返りも大きく、成果として、問題の検出スピードの向上(83%)、問題の修復スピードの向上(82%)、ハイブリッドシステムの可視化(81%)、アプリケーションのセキュリティ向上(81%)が挙げられています。

これらの重要なメリットは、ツール自体のコストを上回っているようです。ほとんどの組織がオブザーバビリティ投資の収支がプラスまたは大幅にプラスになったと回答し、ROIが期待を上回ったと回答した組織は64%、リーダー的組織に限定すると86%にのぼりました。全体で、ROIが期待を下回った組織はわずか5%でした。

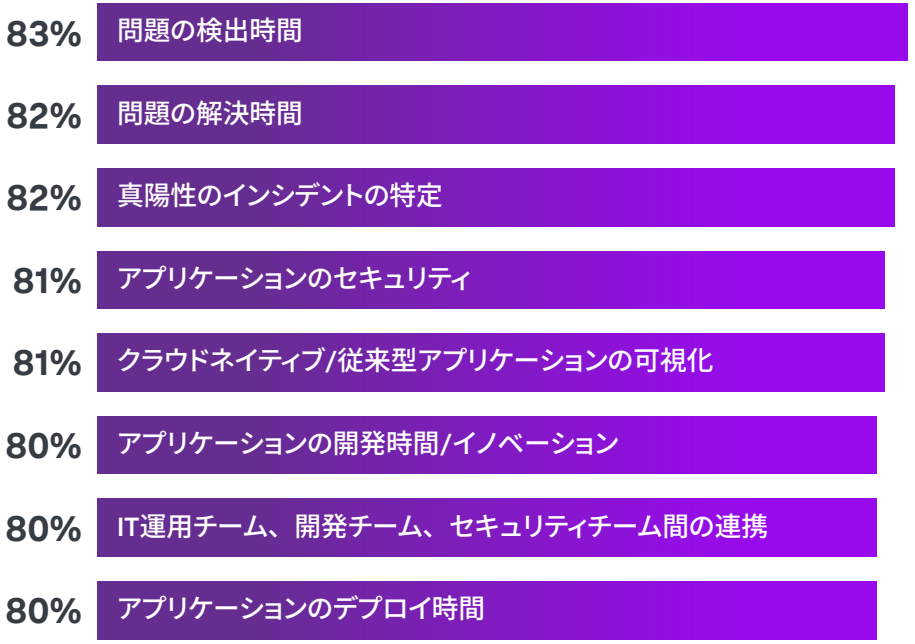
右の図からもわかるとおり、組織はオブザーバビリティがもたらすメリットを明確に実感しています。その中には、ハイブリッドアプリケーションの可視性の向上や、アプリケーションの開発期間の短縮などもありますが、特に大きな成果として挙げられるのが、アプリケーションのセキュリティ向上とMTTR (平均解決時間)の短縮です。この2つは、今日のIT運用チームとエンジニアリングチームにとって優先度の高い目標です。

オブザーバビリティ投資のROI



オブザーバビリティは幅広く大きなメリットをもたらす

オブザーバビリティソリューションは幅広い領域にメリットをもたらしています。



リーダー的組織が得るメリット

オブザーバビリティがさまざまな効果を生む中で、ビギナーレベルの組織が今後得る価値はリーダー的組織を大きく上回ることになるでしょう。ただし、リーダー的組織は、ROIの向上、イノベーションの加速、パフォーマンス目標の達成に対する自信の高さなど、成功を一足早く掴んでいます。

オブザーバビリティのリーダー的組織になることは重要です。それは、組織の評判や収益の向上といった実際の利益につながるからです(周りに自慢できるというボーナス付きです)。

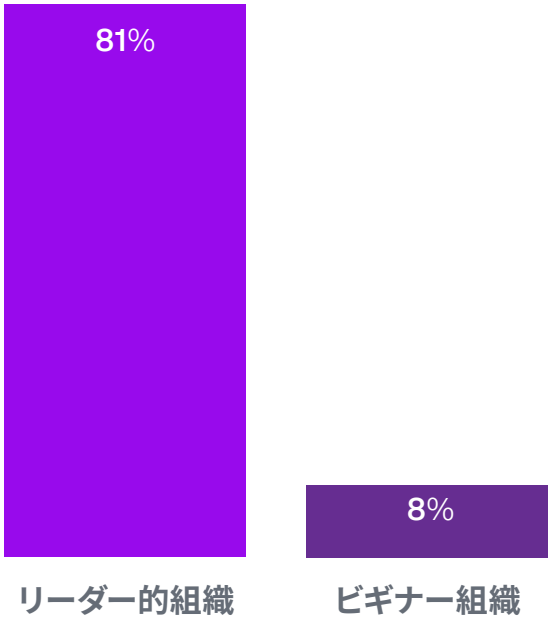
リーダー的組織では、オブザーバビリティとそれがもたらす可視化が定着し、複雑なエコシステムの状況の詳細な把握、障害発生率の低下、問題の迅速な解決、イノベーションの拡大、人材の獲得のしやすさといった優位性を得ています。

リーダー的組織はさまざまな点でその他の組織を凌駕しています。前述のとおり、信頼性とパフォーマンス目標の達成に100%自信があると回答した割合は約90% (2021年の48%、2022年の71%から増加)、オブザーバビリティツールのROIが期待を上回った割合も約90%にのぼります。ほかにも以下の優位性があります。

- **ダウンタイムの年間発生回数が、平均でビギナー組織の3分の1に抑えられています。**
- **予定外のダウンタイムやサービスの深刻な問題の解決を何時間あるいは何日もかけることなくわずかな時間で完了できる割合が、ビギナー組織の4倍にのぼります。**
- **新しい製品/収益源の開拓数が平均で34%上回っています。**

パフォーマンスやイノベーションに対する期待が年々高まる中でこれらの優位性を獲得することは非常に大きな利益につながります。つまり、オブザーバビリティを幅広く実践してビジネス全体を可視化すれば、競争において極めて有利な立場に立てるということです。

リーダー的組織はレジリエンスを重視



リーダー的組織の多くが、レジリエンスについて、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答しています。

オブザーバビリティのリーダー的組織の定義

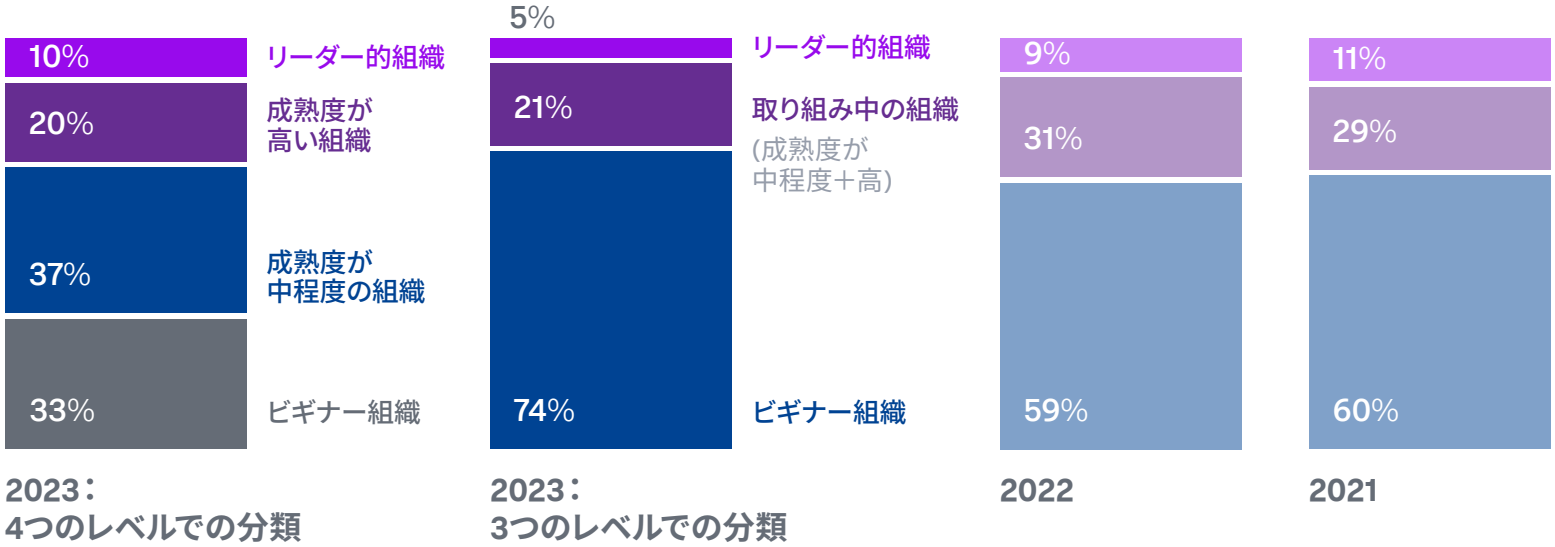
今年は回答者数が昨年の1,250人から1,750人に増え、より多くのデータが得られたことで、成熟度をさらに詳しく分析できるようになりました。そのため、2022年の「ビギナー組織」、「取り組み中の組織」、「リーダー的組織」というレベル分けを見直して、今年は「ビギナー組織」、「成熟度が中程度の組織」、「成熟度が高い組織」、「リーダー的組織」の4つのレベルに分類しました。

組織のオブザーバビリティ実践の成熟度は6つの指標で評価しています。そのうち3つは昨年と同じ「経験」(24カ月以上がリーダー、12カ月未満がビギナー)、オブザーバビリティツール全体での「データの相関付け」の規模、オブザーバビリティツールでの「AI/機械学習の活用」の度合いです。残りの新しい3つは、オブザーバビリティ専門の担当者数を基準とする「専門スキル」、クラウドネイティブと従来型の両方のアプリケーションアーキテクチャへの対応度合いを評価する「ソリューションレベル」、そして「AIOpsの導入」の状況です。今年は「ベンダー統合」は指標から外しました。

6つすべてのカテゴリで最高レベルに達していた組織を「リーダー」、5つの場合を「成熟度が高」、3 ～ 4つの場合を「成熟度が中程度」、2つ以下の場合を「ビギナー」に分類しました。

成熟度の分類を細分化したことで、多くの組織がいまだオブザーバビリティジャーニーの前半にあることがわかりました(ビギナー組織33%、成熟度が中程度の組織37%)。昨年の3つのレベルの分類に当てはめると、ビギナー組織が全体の74%を占めることになります。ビギナー組織が増えているということは、オブザーバビリティの導入が急速に進んでいるということであり、今から取り組みを始めても決して遅くはないともいえます。

このレポートでは、趣旨に照らし合わせて主にリーダー的組織とビギナー組織を比較しています。2つの「取り組み中」の組織は常にリーダー的組織とビギナー組織の中間の結果で、ほぼすべてのカテゴリにおいて成熟度が高い組織が成熟度が中程度の組織を上回っています。

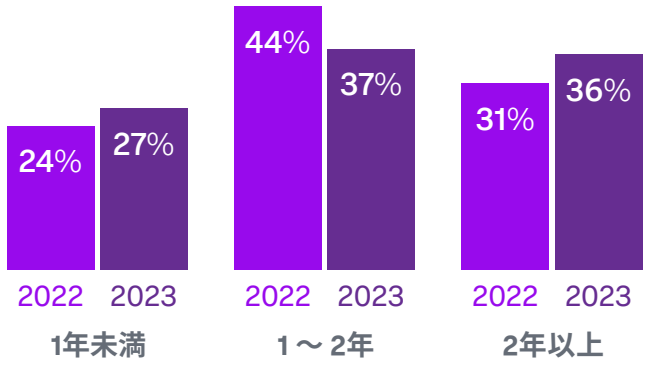


6つの指標を詳しく分析すると、成熟度の分類を細分化した効果が見えてきます。

- **データの相関付け：ITシステム全体でどのくらいのデータを相関付けできているか**
  - ビギナー組織：ほとんどまたはまったくできていない(14%、2022年は19%、2021年は15%)
  - 成熟度が中程度の組織/高い組織：ある程度できている(45%、取り組み中の組織として2022年は44%、2021年は51%)
  - リーダー的組織：かなりできている(39%、2022年は36%、2021年は33%)
- **AI/機械学習の活用：AI/機械学習機能が搭載されたオブザーバビリティツールを使用しているか**
  - ビギナー組織：検討していない/導入していない(8%、2022年は11%、2021年は13%)
  - 成熟度が中程度の組織/高い組織：導入の最中(26%、2022年は26%、2021年は33%)
  - リーダー的組織：ある程度/幅広く活用している(66%、2022年は62%、2021年は52%)
- **専門スキル：オブザーバビリティプロジェクトを専門で受け持つ担当者がいるか**
  - ビギナー組織/成熟度が中程度の組織：専門スキルがあまり浸透していない(12%が「いない」または「わからない」と回答)
  - 成熟度が高い組織/リーダー的組織：専門スキルが広く浸透している(87%が「いる」と回答)
- **ソリューションレベル：クラウドネイティブと従来型の両方のアプリケーションアーキテクチャに対応するオブザーバビリティツールを重視/導入しているか**
  - ビギナー組織：重要だと思わない(14%)
  - 成熟度が中程度の組織/高い組織：重要だと思うが導入予定はない(49%)
  - リーダー的組織：重要だと考え活用している(37%)
- **AIOpsの導入：オブザーバビリティの実践にAIOpsツールを活用しているか**
  - ビギナー組織：AIOpsツールの導入予定はない/関心がない(7%)
  - 成熟度が中程度の組織/高い組織：AIOpsツールを導入中/一部で活用している(60%)
  - リーダー的組織：AIOpsツールを広く活用している(32%)

経験の差

オブザーバビリティの実践経験の長さ



可視化が自信につながる

リーダー的組織では環境の可視化が進んでいます。些細な問題でもすばやく察知して修正できるため、大きなインシデントに発展する前に対処できることもよくあります。

可視化が後れているビギナー組織とは対照的に、リーダー的組織では「かなり可視化できている」と回答した割合が調査対象のすべての領域で過半数を優に超えました。

- **コンテナ：リーダー的組織71%、ビギナー組織32%**
- **パブリッククラウドのIaaS：リーダー的組織71%、ビギナー組織38%**
- **セキュリティ態勢：リーダー的組織70%、ビギナー組織37%**
- **オンプレミスのインフラ：リーダー的組織66%、ビギナー組織34%**
- **アプリケーション(コードレベル)：リーダー的組織66%、ビギナー組織31%**

これだけ環境を可視化できていると、問題が起きていないときは安心して製品のリリースに集中でき、それがパフォーマンス目標達成の自信につながります。

- **リーダー的組織のほとんど(89%)が、アプリケーションのパフォーマンス要件の達成に100%自信があると回答し、2022年の71%、2021年の48%から増加しています。**
- **リーダー的組織の過半数(55%)が、オブザーバビリティツールのROIが期待を上回ったと回答し、ビギナー組織の7%を大きく上回っています。**
- **リーダー的組織では、ソフトウェアエンジニアリングチームが開拓した新しい製品/収益源の数がビギナー組織を34%上回っています。**

新しい収益源を開拓するという方法で目標を達成し効率的に価値を創出したチームは、満足度が高い傾向があります。前述のとおり、十分なオブザーバビリティ人材を確保できている、または適切なスキルを持つ人材を確保できていると回答したリーダー的組織は35%にのぼり、成功が成功を呼んでいることがわかります。

89%：アプリケーションの可用性とパフォーマンス要件の達成に100%自信があると回答したリーダー的組織の割合

86%：オブザーバビリティツールのROIが期待を上回ったと回答したリーダー的組織の割合

リスクの抑制、修正の迅速化、障害の防止

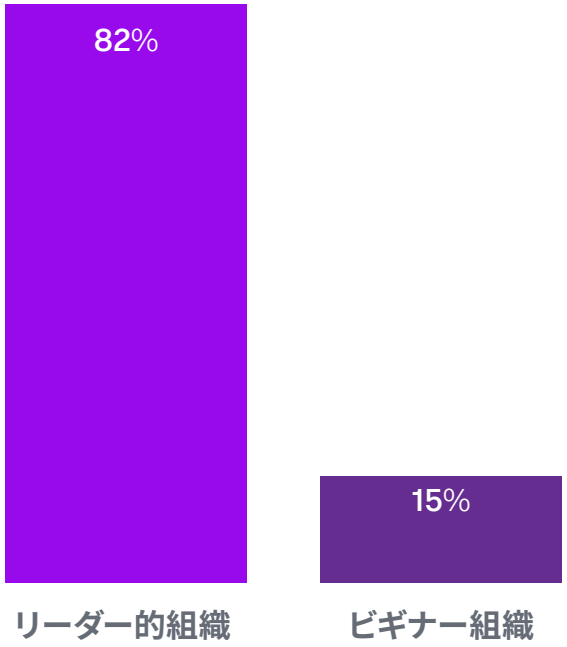
オブザーバビリティのリーダー的組織は、アプリケーション開発と信頼性に関する複数のKPIでビギナー組織をはるかに上回っています。

- **自社製アプリケーションの多くのコードを本番環境にオンデマンドでプッシュできる割合は3.8倍にのぼります(リーダー的組織は47%、ビギナー組織は15%)。**
- **根本原因の特定スピードが大幅に向上したと回答した割合は6.3倍にのぼります(リーダー的組織は63%、ビギナー組織は10%)。**
- **リーダー的組織のアラートは実用性が高く、アラートの半数以上が自動修復システムによってトリアージされていると回答した割合が62%にのぼります。**
- **リーダー的組織は、コードを本番環境にプッシュする頻度が高い一方でダウンタイムの発生率が低く、ビジネスクリティカルな自社製アプリケーションのダウンタイム発生頻度は57%の組織で数四半期に1回以下でした。**
  - 年間のダウンタイム発生数の中央値は、リーダー的組織が2回、ビギナー組織が6回でした。
- **リーダー的組織は問題の解決も速く、ビジネスクリティカルな自社製アプリケーションで発生した予定外のダウンタイムまたは深刻なパフォーマンス低下を数分以内に解決できると回答した割合がビギナー組織の4倍でした。逆に、解決に数日かかると回答したビギナー組織の割合はリーダー的組織の2倍でした。**

これらのKPIは、ソフトウェア開発とデリバリーの品質を測定するためのDORA (DevOps Research and Assessment)メトリクスをほぼ網羅しています。

リーダー的組織はセキュリティとオブザーバビリティの統合で大きなメリットを得ている

リーダー的組織の多くが、セキュリティ監視ツールやチームとオブザーバビリティを統合することで、リスク管理やインシデント対応の面で「大きな成果を得た」と回答しています。



オブザーバビリティソリューションによる改善でもリーダー的組織とビギナー組織の間には差がありました。

- **開発時間が大幅に短縮した：リーダー組織は59%、ビギナー組織は25%**
- **デプロイ時間が大幅に短縮した：リーダー組織は63%、ビギナー組織は25%**
- **クラウドネイティブ/従来型アプリケーションの可視性が大幅に向上した：リーダー組織は60%、ビギナー組織は25%**
- **問題検出までの時間が大幅に短縮した：リーダー組織は59%、ビギナー組織は24%**
- **問題解決までの時間が大幅に短縮した：リーダー組織は65%、ビギナー組織は25%**

これだけの差、特にクラウドネイティブ/従来型アプリケーションの可視性向上で35ポイントの差が出たことは注目に値します。しかも、すべてのカテゴリで昨年よりも差が広がっています。どの組織もハイブリッドやマルチクラウドの課題に直面しており、今後、環境全体を可視化する必要に迫られることは明らかです。

調査では、オブザーバビリティソリューションがチーム間の連携に役立っていることもわかりました。オブザーバビリティソリューションのおかげでIT運用チーム、開発チーム、セキュリティチーム間の連携が強化されたと回答したリーダー的組織は60%で、ビギナー組織の26%を大きく上回りました。また、雇用状況が改善した割合も55%にのぼり、ビギナー組織の23%を上回っています。

リーダー的組織はオブザーバビリティソリューションを活用して、ハイブリッドアーキテクチャの可視化を大きく向上させていると同時に、開発、デプロイ、インシデント検出、問題解決を迅速化しています。

リーダー的組織に学ぶ教訓

リーダー的組織になれば多くのメリットが得られることは明らかです。では、リーダー的組織はどのようにして今日の成功を掴んだのでしょうか。実践経験の長さ以外に、リーダー的組織はいくつかの面で、際立った成果をあげるための一貫した姿勢を貫いています。

想定外の事態に備える

需要の急増、サイバー脅威の増加、地政学的緊張、自然災害など、この数年間にはさまざまな混乱が起き、どの組織もこれを免れることはできませんでした。しかし、これらの問題とどのように向き合ったかは組織によって大きく異なります。

リーダー的組織にとってレジリエンスは基本です。リーダー的組織の97%がレジリエンスに対する正式なアプローチをすでに確立しているだけでなく、実に81%もの組織が、重要なシステムを保護するための組織レベルの戦略を策定済みです。ビギナー組織では、レジリエンスに対する組織レベルの正式なアプローチを策定している割合がわずか8%にとどまり、今後に向けた重要な改善課題を浮き彫りにしています。

また、多くのリーダー的組織が将来を見据えて、今後1年間でレジリエンスをさらに強化するためのソリューションに投資する意志を明確にする一方で、それを最優先事項にあげたビギナー組織は少数派でした。では、リーダー的組織の最優先事項は何でしょうか。

- **リーダー的組織では、テクノロジー環境全体をより詳細に可視化することが今後の最優先事項のトップで、その割合はビギナー組織を15ポイント上回りました。**
- **僅差で2位になったのは、技術系以外のビジネスプロセスでの脆弱性調査とリスク緩和で、こちらもビギナー組織を18ポイント差で大きく上回りました。**

ビジネスについてもオブザーバビリティについても、将来何が起きるかを正確に予測することはできません。それでも、レジリエンスの向上に必要な戦略やソリューションに投資すれば、問題にすばやく対処して、大規模なインシデントに発展する事態を回避できる可能性が高まります。

チーム全体の取り組み：**100%のリーダー的組織**が、レジリエンス戦略とその投資や、保護すべき重要なビジネスシステムの判断について、ITリーダーが他のビジネス部門(セキュリティ、財務、マーケティング、オペレーションなど)のリーダーと積極的にコラボレーションしています。

力を合わせて目の前の壁を乗り越える

事態は悪化しています。環境やアプリケーションはますます複雑になり、マイクロサービスのような、容易には理解できない最新のデリバリー手法が次々と登場しています。同時に、リーダー的組織の45%が、利用するオブザーバビリティベンダーの数が急増していると回答しています。こうした現実は、雑音をはねのけてインシデントの根本原因を特定したり、パフォーマンス低下の問題を解決しようとするときに壁となって立ちはだかります。

環境全体にはびこる複雑さに対抗するために、オブザーバビリティのリーダー的組織は、ツールの共通化やデータセットの共有を通じてチーム間のコラボレーションを強化し、システムの状況把握、認識の共有、問題の診断、パフォーマンスの最適化を推進しています。各種のツールやチームをオブザーバビリティと統合しているかを尋ねる質問では、リーダー的組織は6つのカテゴリ(AIOps、アプリケーションパフォーマンス監視、インフラ監視、デジタルエクスペリエンス監視、ログ管理、ネットワークパフォーマンス監視)すべてで「統合済み」の割合が高くなりました。

これらの業務を統合すれば、チーム間のコラボレーションを効率化し、重複作業を排除するだけでなく、プロアクティブな監視を実現できるよう結束を固めることができます。

リーダー的組織の75%が、オブザーバビリティツールやチームと他の業務をある程度以上統合しています。

自分の頭で考える

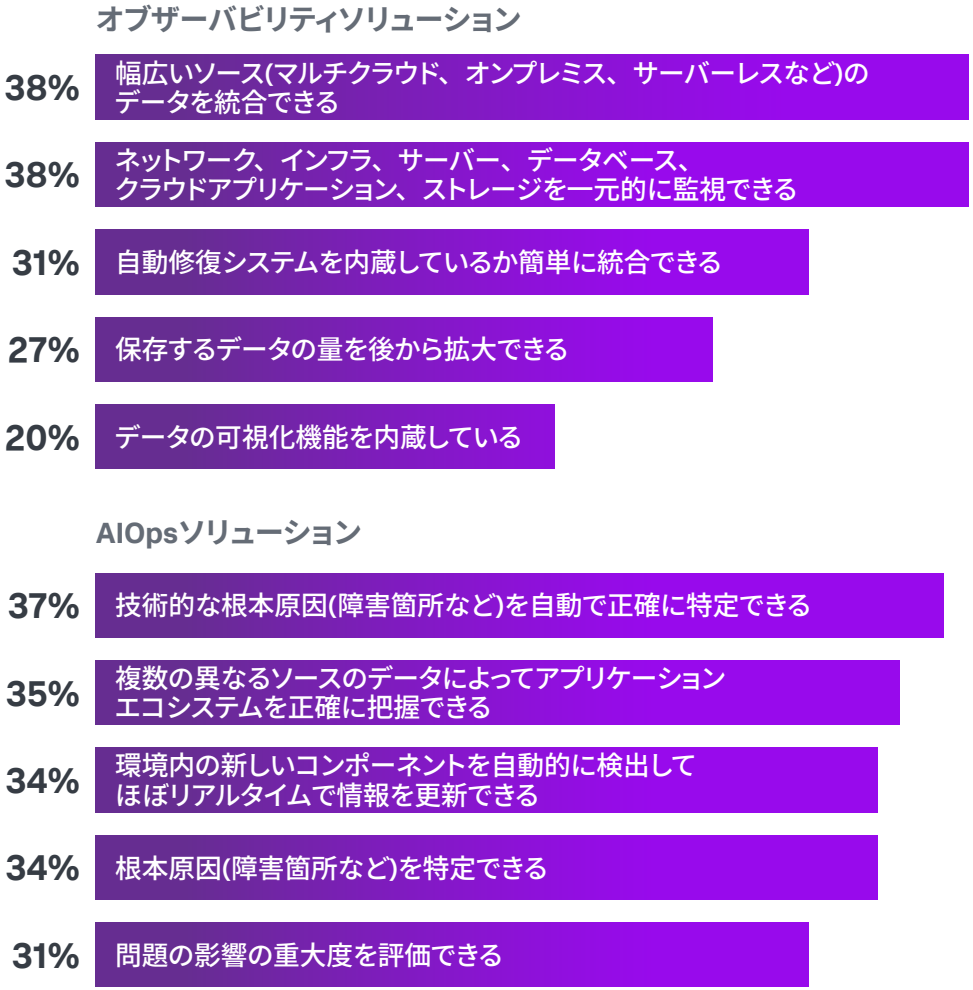
オブザーバビリティのリーダー的組織は、厳しい目で製品の選定に臨みます。「見せかけのオブザーバビリティ」に遭遇したことがあると回答した割合は68% (ビギナー組織は29%)、「見せかけのAIOps」に遭遇した割合は56% (同25%)にのぼりました。

オブザーバビリティツールを評価する際に重視する点については、異なるソースのデータを統合する能力と、ネットワーク、インフラ、サーバー、データベース、クラウドアプリケーション、ストレージを一元的に監視する能力の2つが同率1位で、数ポイント差で他の選択肢を上回りました。

この2つはともに、統合と可視化に要約することができます。多くの組織にとって、当面はハイブリッド環境を維持することが現実的な選択肢です。それならば、マルチクラウド環境、オンプレミス環境、ハイブリッドアプリケーション、それらをつなぐすべての要素を一元的に監視できるツールは必須です。オブザーバビリティソリューションを選定するときは、リーダー的組織の姿勢を手本に、組織の可視化要件に合っているかどうかをしっかりと見極めましょう。

ツール選定に関するリーダー的組織からのアドバイス

オブザーバビリティソリューションとAIOpsソリューションのどちらでも、選定時には以下の機能を重視することを勧めています。



強固な基盤を築く

オブザーバビリティの実践と言われても、何をすべきか戸惑う人がほとんどでしょう。最適な可視化を実現するにはどうすればよいでしょうか。問題をすばやく検出して解決するには何が必要でしょうか。そもそも何から始めればよいのでしょうか。

最後の疑問については、リーダー的組織とビギナー組織で答えが一致しました。それは、標準化されたメトリクス、ログ、トレースに基づいてオブザーバビリティパイプラインを構築することです。そのためにお勧めするのがOpenTelemetryです。OpenTelemetryの導入から始めれば、以降の作業が容易になります。また、標準のフレームワークを取り入れることで、一貫性を維持しやすくなり、将来を見据えた拡張性も確保できます。

オブザーバビリティの実践を始めるうえで重要な取り組みとして、リーダー的組織で上位に入り、ビギナー組織では入らなかった回答もありました。それは、フィードバックループの構築です。インシデントの発生原因を評価するインシデント事後レビューを含め、フィードバックループは、あらゆる運用において効果を高めるために重要なプラクティスの1つです。しかし他の基本機能に比べると重要性は低いのかもしれません。ここで疑問に思うのは、リーダー的組織はオブザーバビリティジャーニーの先を進みすぎていて、ビギナー組織の参考にはならないのでしょうか。

リーダー的組織とビギナー組織のいずれも、オブザーバビリティを実践するうえで重要な最初のステップの1つは、組織全体でメトリクス、ログ、トレースを標準化し、それに基づいてオブザーバビリティパイプラインを構築することだと考えています。

推奨される取り組み

1.レジリエンスを優先する

システム障害、システムを取り巻く環境の変化、有害事象など、問題が発生するのは避けられません。重大な問題に先手を打って対応すると同時に、新たな難題に直面してもセキュリティと信頼性を維持できる体制を築くには、レジリエンス戦略の策定と実行が不可欠です。それは顧客満足度の向上にもつながります。

リーダー的組織の成功が物語るように、正式なレジリエンス戦略は策定して終わりではなく、組織全体で実行することが重要です。リーダー的組織は、あらゆる面にレジリエンスを組み込むことによって、インシデントの発生時に迅速に対応し、マクロ環境の変化にすばやく適応する能力を高めています。

2.標準を定める

オブザーバビリティの導入を始めたばかりか、実践が進んでいるかを問わず、あらゆる成熟度の組織が重要な最初のステップとして挙げたのが、メトリクス、ログ、トレースの標準化です。これは、すべてのシステムでデータの一貫性を保つとともに、効率と相互運用性を向上させるために役立ちます。

リーダー的組織は、専門のオブザーバビリティチームを立ち上げて、ツールの標準化に集中的に取り組む傾向があります。このアプローチが適切かどうかは組織によりますが、組織全体におけるオブザーバビリティ担当者の位置づけを明確にするうえで重要な戦略です。

専門のオブザーバビリティチームを作る場合でも、オブザーバビリティの専門家を各アプリケーション開発チームに配置する場合でも、標準を定めて適切なデータパイプラインを構築することが重要です。標準化したメトリクスを基準として使用すれば、ニーズの変化に応じて柔軟にデータパイプラインを拡張し、実践の成熟度に合わせて適切なオブザーバビリティツールを選択できます。

3.ソリューションの選定は慎重に行う

見せかけのオブザーバビリティやAIOpsが蔓延する中、ベンダーから適切な製品を購入するには、事前にすべてのソリューションを綿密に調査する必要があります。あらゆる成熟度の組織に言えますが、特にリーダー的組織は、オブザーバビリティソリューションを選定する際に、さまざまなソースのデータを統合できることと、インフラからクラウドアプリケーションまでのすべてを一元的に監視できることを重視します。今後もハイブリッド環境を維持するならば、すべてのシステムを可視化するオブザーバビリティソリューションを導入する必要があります。

購入するソリューションを評価する際は、ベンダーにその製品独自の機能を紹介してもらい、従来の監視ソリューションとどこが違うのか、クラウドとオンプレミスの両方の環境を可視化できるか、ネットワーク、インフラ、データベースも一元監視できるかを確認します。躊躇する必要はありません。購入後に後悔することのないように、聞きたいことはすべて聞いておきましょう。

4.フィードバックループを構築する

物事が悪い方に進むのは、避けては通れない現実です。もちろん、強力なオブザーバビリティプラクティスを確立すれば、そうしたリスクを緩和し、問題を早期に修正して障害やシステム停止を回避できます。しかし、オブザーバビリティプラクティスをどれだけ高度なものにしても、すべてのインシデントを完璧に防ぐことはできません。オブザーバビリティのリーダー的組織とビギナー組織の違いの1つは、失敗から学べるかどうかです。オブザーバビリティプラクティスを確立するためにリーダー的組織が重視する項目としてフィードバックループの構築が上位に入ったことがそれを証明しています。

インシデントの解決後、インシデント事後レビューを実施して問題の根本原因を詳しく評価することで、どこにどのような問題があったかを明確にし、適切な再発防止策を立てることができます。この追加ステップは、システムの信頼性を高め、アラートを調整して邪魔なノイズを低減するとともに、将来同じようなインシデントが発生するのを防ぐことができます。

また、フィードバックループを構築することは、オブザーバビリティチーム内に継続的な改善の文化を育むためにも役立ちます。継続的な改善によってオブザーバビリティを強化し続ければ、成功への道を着実に歩むことができます。

付録

国別の特徴

オブザーバビリティへの取り組みに関する国別の状況

オーストラリアおよびニュージーランド

オーストラリアとニュージーランド(ANZ)の組織はオブザーバビリティの成熟度が高く、ビギナー組織の割合は全体の25%にとどまり(世界の他国の平均は34%)、成熟度が高い組織が36%で最も多いという結果になりました(同19%)。

レジリエンスを重視する組織が多いのも特徴で、レジリエンスについて、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答した割合は55%にのぼります(世界の他国の平均は39%)。また、技術系以外のビジネスプロセスでの脆弱性調査とリスク緩和のために、レジリエンスソリューションへの投資を予定している組織も55%にのぼりました(同44%)。

プロセスの点では、専門のITチームが主体となってオブザーバビリティツールを導入していると回答した割合が48%と高く(世界の他国の平均は26%)、逆に、プラットフォームエンジニアリングチームが開発チームや運用チームにツールを提供していると回答した割合は19%でした(同35%)。

オブザーバビリティの専門知識や専門スキルに重きを置く傾向もあります。オブザーバビリティプラクティス導入のアドバイスをするなら何を勧めるかという質問で、「オブザーバビリティのオーナーシップを持つ専門のオブザーバビリティチームを設置する」と回答した割合が40%で、世界の他国の平均(30%)を上回りました。

オブザーバビリティに対してはプラットフォームのアプローチを重視する組織が多数派です。53%の組織が、オブザーバビリティツールセットの機能数が増加していると回答した一方で(世界の他国の平均は31%)、34%が、オブザーバビリティベンダーをかなり統合していると回答しています(同13%)。

カナダ

カナダの組織はオブザーバビリティの成熟度が中央に集中し、リーダー的組織が5%と少ない一方で(世界の他国の平均は10%)、ビギナー組織も25%にとどまりました(同34%)。つまり、成熟度が中程度の組織と高い組織が70%を占めます。

ANZと同様にレジリエンスを重視する傾向があり、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答した割合は50%にのぼりました(世界の他国の平均は39%)。また、レジリエンスの低さの大きなデメリットとして、50%が顧客離れ(同33%)、54%がイノベーションの後れ(同33%)を挙げています。

自社製アプリケーションについてはクラウドネイティブアーキテクチャを採用する組織が多く、クラウドネイティブアーキテクチャのアプリケーションが占める割合を今後1年間で増やす予定だと回答した割合は70%にのぼりました(世界の他国の平均は57%)。

ツールセットの機能を積極的に増やすと同時に、ベンダー統合を進める組織が多いのも特徴です。42%の組織が、オブザーバビリティ関連の機能数が大幅に増加していると回答した一方で(世界の他国の平均は32%)、51%がベンダーを統合していると回答しています(同39%)。

専門のオブザーバビリティチームの設置が今日の大きな課題と思われます。ベンダーを統合して簡素化を進める組織が多いのはそのためかもしれません。さらに、数とスキルの両方でIT運用担当者を十分に確保できないことを課題に挙げた組織が53% (世界の他国の平均は42%)、アプリケーション開発者を十分に確保できないことを課題に挙げた組織も56%にのぼりました。

フランス

フランスの組織のオブザーバビリティの成熟度は世界平均をわずかに下回り、ビギナー組織が39%に対して(世界の他国の平均は33%)、リーダー的組織が9% (同10%)、成熟度が高い組織が19% (同20%)でした。

ほかにいくつかの領域で後れが見られます。

- オブザーバビリティツールセットでAI/機械学習を活用している：23% (世界の他国の平均は31%)
- クラウドネイティブアーキテクチャと従来のアプリケーションアーキテクチャの両方に対応したオブザーバビリティソリューションを導入している：25% (同38%)

逆に、他国を上回っている点もいくつかあります。まず、オブザーバビリティを確保するために、データ形式にオープンスタンダードを採用している組織が46%にのぼりました(世界の他国の平均は35%)。これは、データの統合、可視化、相関付けに効果的です。

また、すべてのアプリケーションスタックに対応したオブザーバビリティツールを導入している割合が高く、ネットワークから、インフラ、サーバー、データベース、クラウドのアプリケーションまで、すべてを一元的に監視できる環境が整っています。これだけの可視性を確保できれば、盲点をなくすと同時に、インサイトをすばやく獲得できるメリットもあります。

複雑化とデータのサイロ化に関する課題の緩和策として、オブザーバビリティベンダーを統合するか、少なくともベンダー数を増やさないようにする組織が67%と多いのも特徴です(世界の他国の平均は54%)。

ドイツ

ドイツの組織のオブザーバビリティの成熟度は世界平均を大幅に下回り、ビギナー組織が42%を占める一方で(世界の他国の平均は32%)、成熟度が高い組織とリーダー的組織が19%にとどまりました(同31%)。

成熟度の低さを決定づける要因ではないものの、レジリエンスの構築にも後れが見られます。レジリエンスについて、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答した割合は32%にとどまりました(世界の他国の平均は41%)。また、レジリエンスソリューションに対する投資意欲も低く、テクノロジー環境全体の可視性を向上させるための投資予定がある組織は39% (同50%)、データを既知の正常な状態に戻せるようにするための投資予定がある組織は35% (同45%)でした。

ドイツの成熟度を低くしている重要な要因の1つが、オブザーバビリティツールと監視ツールで収集されるデータを広範に相関付けている組織の割合が31%と低調であったことです(世界の他国の平均は39%)。また、オブザーバビリティ環境に関係するベンダーが増加していると回答した組織が64%にのぼります(同42%)。ベンダーの増加は複雑さと統合の課題を悪化させます。つまり、成熟度が低い直接の原因は複雑さと言えるかもしれません。

アラートの精度の低さは、成熟度の低さが原因と考えられます。オブザーバビリティソリューションや監視ソリューションで生成されるアラートのうち、真陽性のアラートが半数に満たないと回答した組織は78%にのぼりました(世界の他国の平均は44%)。

一方で、現在の課題を克服するために包括的で拡張性の高いオブザーバビリティソリューションが必要であることは多くの組織が認識しており、クラウドネイティブアーキテクチャと従来のアプリケーションアーキテクチャの両方に対応した単一のオブザーバビリティソリューションを導入することが、重要かつ必要であると回答した割合は59%にのぼりました(世界の他国の平均は48%)。

インド

インドの組織はオブザーバビリティの成熟度ではトップクラスです。リーダー的組織が23%を占め(世界の他国の平均は9%)、ビギナー組織は18%にとどまりました(同34%)。

オブザーバビリティの成熟度が高いためか、自社製アプリケーションのポートフォリオ改革に非常に積極的で、今後12カ月間でクラウドネイティブアプリケーションの割合を大幅に増やす予定だと回答した組織が82%にのぼりました(世界の他国の平均は56%)。

また、レジリエンスも重視しており、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答した割合は52%にのぼりました(同39%)。しかも、それにとどまりません。レジリエンスソリューションへの投資意欲が高く、インシデント対応と修復を迅速化するための投資予定がある組織は65% (同49%)、顧客やユーザー向けのサービスを迅速に復旧するための投資予定がある組織は62% (同50%)と、いずれも他国の平均を上回っています。

オブザーバビリティツールについては良い意味で懐疑的で、66%の組織が「見せかけのオブザーバビリティ」に遭遇したことがあると回答しています(世界の他国の平均は42%)。オブザーバビリティツールの選定で何を重視するかという質問では、マルチクラウド環境、オンプレミス環境、サーバーレス関数などのさまざまなソースのデータを統合できる点を挙げた組織が45%にのぼりました(同35%)。また、可視化の統合機能を重視する組織も27%と高めでした(同19%)。

日本

日本の組織はオブザーバビリティの成熟度でかなり後れを取っており、ビギナー組織が48%を占め(世界の他国の平均は31%)、リーダー的組織はわずか1%でした(同11%)。

特に後れが見られる領域がいくつかあります。

- オブザーバビリティソリューションを2年以上使用している：18% (世界の他国の平均は38%)
- オブザーバビリティツールと監視ツールから収集したすべてのデータを相関付けている：11% (同42%)
- オブザーバビリティツールセットでAI/機械学習を活用している：15% (同33%)
- クラウドネイティブアーキテクチャと従来のアプリケーションアーキテクチャの両方に対応したオブザーバビリティソリューションを導入している：12% (同40%)

一方で、自社製アプリケーションのモダナイズには積極的で、今後1年間でクラウドネイティブアプリケーションの割合を増やす予定だと回答した組織は67% (世界の他国の平均は57%)、大半のアプリケーションをオンデマンドでアップデートできると回答した組織は41% (同29%)にのぼりました。

全体として、アプリケーションの監視やトリアージに必要なツールとプロセスの整備は万全でなくても、アプリケーション開発の領域では前進を続けている様子がうかがえます。

シンガポール

シンガポールの組織のオブザーバビリティの成熟度は世界平均を下回り、ビギナー組織は41% (世界の他国の平均は33%)、リーダー的組織はわずか6% (同10%)でした。

ビギナー組織の割合が高いすべての国に言えることですが、ビギナー組織の間で監視ツールやチームのサイロ化が大きな課題になっています。オブザーバビリティと他の業務を統合している組織が少なく、インフラ監視との統合は9% (世界の他国の平均は24%)、デジタルエクスペリエンス監視との統合は14% (同36%)、ネットワークパフォーマンス監視との統合は10% (同26%)、セキュリティ監視との統合は13% (同28%)と、軒並み低い結果になりました。

人材不足も大きな悩みで、数とスキルの両方でIT運用担当者を十分に確保できないことを課題に挙げた組織が57%にのぼりました(世界の他国の平均は41%)。さらに、「Quiet Quitting」(仕事をがんばりすぎず最低限のことだけをこなす働き方)をするスタッフが増えて効率が下がっていることを課題に挙げた組織も45%にのぼります(同31%)。

これらの課題がアプリケーションパフォーマンスのKPIや成果の低さにつながっていると考えられます。

- アプリケーションの信頼性とパフォーマンス目標の達成に100%自信がある：30% (世界の他国の平均は44%)
- 新しいコードの変更失敗率(Change Failure Rate)が30%以上である：54%(同36%)

一方で、業務をサポートするためのAIOpsツールの導入には積極的で、AIOpsソリューションを導入中と回答した組織は36%にのぼりました(世界の他国の平均は24%)。また、AIOpsを早期導入した組織のうち64%が、問題の根本原因の診断スピードが上がったと回答しています(同50%)。

英国

英国の組織のオブザーバビリティの成熟度は世界平均をわずかに下回り、ビギナー組織が38%で、世界の他国の平均32%をやや上回る一方、リーダー的組織が10%、成熟度が高い組織が20%で、いずれも他国の平均と同率でした。

監視ツールやチームとオブザーバビリティプラクティスとの統合が進んでおり、インフラ監視との統合が30% (世界の他国の平均は22%)、ログ管理との統合が35% (同23%)、ネットワークパフォーマンス監視との統合が33% (同23%)と、いずれも世界平均を上回っています。

専門のプラットフォームエンジニアリングチームが、セルフサービス型のオブザーバビリティツールやその他のソフトウェアデリバリーツールを、開発チームやSRE/DevOpsエンジニアに提供すると回答した割合が42%にのぼったのも特徴的です(世界の他国の平均は32%)。逆に、オブザーバビリティツールの選定と活用のためにSREやDevOpsエンジニアが開発チームに参加すると回答した割合は12%と低めでした(同20%)。

人材不足の緩和策では、オブザーバビリティチームメンバー以外の従業員のリスキリングに力を入れている組織が45%にのぼりました(世界の他国の平均は38%)。また、IT運用担当者や開発者のオブザーバビリティトレーニングへの投資を重視している組織も52%と高めでした(同44%)。このように従業員トレーニングに力を入れる理由は、マクロ経済の悪化を見込んで人材獲得競争が厳しさを増すと予想する組織が49%と多いためと思われます(世界の他国の平均は37%)。

米国

米国の組織は他国と比べてオブザーバビリティの導入がかなり進んでおり、リーダー的組織が13%にものぼり(世界の他国の平均は9%)、ビギナー組織は25%にとどまりました(同36%)。

レジリエンスを重視する組織が多く、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答した割合は50%にのぼります(世界の他国の平均は36%)。アラート機能でも優れており、約3分の1の組織が、監視システムのアラート精度が75%以上だと回答しています(同22%)。

オブザーバビリティツールやチームと他の業務との統合も比較的進んでいて、アプリケーションパフォーマンス監視との統合が32% (世界の他国の平均は24%)、ネットワークパフォーマンス監視との統合が30% (同23%)、インフラ監視との統合が28% (同22%)でした。

製品の調達では、IT運用チームが主体となって行う組織が32% (世界の他国の平均は26%)、経営層からのトップダウンの指示で行う組織が18% (同9%)という結果でした。

アプリケーションをオンデマンドでアップデートできると回答した組織は少なめです。

- 本番環境にコードをオンデマンドでプッシュしてアップデートできる自社製アプリケーションは10%未満である：24% (世界の他国の平均は15%)
- 自社製アプリケーションの大半をオンデマンドでアップデートできる：25% (同33%)

ただし、アプリケーションのアップデートによってサービスに影響する問題が発生し、修復が必要になることは少なく、アプリケーションパフォーマンスの低下を引き起こしたコード変更が30%以上あると回答した組織は31%と、世界の他国の平均39%を下回りました。

業界別の特徴

4つの業界の特徴的なデータポイント

金融サービス

金融サービス業界はオブザーバビリティの成熟度が低めで、リーダー的組織はわずか8%にとどまる一方、ビギナー組織は43%にのぼりました。調査対象の組織には2つの傾向が見られました。

1. まずはマイナス面として、環境を構成する各要素について「かなり可視化できている」と回答した割合が低く、レガシーインフラが41% (他の全業界の平均は49%)、プライベートクラウドが42% (同52%)、パブリッククラウドインフラが53% (同44%)、全体的なセキュリティ態勢が38% (同53%)という結果でした。このことが自信の低さにつながっているとみられ、アプリケーションの信頼性とパフォーマンス目標の達成に100%自信があると回答した組織は26%にとどまりました(同45%)。
2. プラス面では、監視ツールの導入が進んでおり、調査対象になったすべてのツール(AIOps、アプリケーションパフォーマンス監視、ネットワークパフォーマンス監視、インフラ監視、デジタルエクスペリエンス監視、ログ管理、セキュリティ監視)を使用している組織が45%にのぼりました(他の全業界の平均は30%)。また、オブザーバビリティツールやチームと他の業務との統合を推進している組織が多く、AIOpsとの統合が36% (同23%)、インフラ監視との統合が33% (同22%)、デジタルエクスペリエンス監視との統合が36% (同24%)、ログ管理との統合が37% (同23%)、ネットワークパフォーマンス監視との統合が33% (同24%)と、いずれも他業界の平均を上回りました。

さまざまな監視ツールを導入する弊害として、データのサイロ化が課題になっています(ツールやチームの統合だけでは埋め合わせできないと考えられます)。オブザーバビリティに関する主な課題として、32%の組織が、複数のソースからのデータの相関付けを挙げています(他の全業界の平均は24%)。

製造

製造業ではオブザーバビリティの成熟度が中間に集中し、リーダー的組織が8%、ビギナー組織が38%でした。特徴としては以下の3点が挙げられます。

1. 調査対象となったすべての監視ツールを使用している組織は24%にとどまりました(他の全業界の平均は33%)。使用率が特に低かったのがAIOpsツールの51% (同59%)と、ネットワークパフォーマンス監視ツールの72% (同80%)です。
2. オブザーバビリティの実践においてデータの統合と専門チームの設置を重視する傾向があります。
   - オブザーバビリティプラクティスの導入についてアドバイスをするなら何を勧めるかという質問では、34%の組織が、推奨する取り組みのトップ3にデータの統合を挙げました(他の全業界の平均は27%)。
   - チーム体制については、オブザーバビリティ担当者を集めて、組織全体のソフトウェアデリバリーツールの標準化を専門とするチームを作る組織が65%と多く(他の全業界の平均は57%)、逆に、各アプリケーション開発チームのニーズに合ったオブザーバビリティツールを体系的に導入するためにオブザーバビリティ担当者を各チームに配置する組織は35%にとどまりました(同43%)。
3. 問題の検出に時間がかかる傾向もあります。自社製アプリケーションの問題を適切なチームが検出するのに平均で数日かかると回答した組織が40%にのぼりました(他の全業界の平均は30%)。ただし、製造業の各組織はその課題を自覚しているようです。障害やダウンタイムが原因で顧客を失うのを避けるためにレジリエンスを強化する必要があると考えている組織は41%にのぼりました(同33%)。また、95%の組織が、オブザーバビリティリーダーがレジリエンスについてビジネス部門のリーダーと積極的にコラボレーションしていると回答しています。

通信・メディア

通信・メディア業界はオブザーバビリティの成熟度が高く、リーダー的組織が13%にのぼり、ビギナー組織は26%にとどまりました。成熟度が高い理由として次の2点が考えられます。

1. オブザーバビリティの導入時期が早く、オブザーバビリティソリューションを3年以上使用している組織が28%にのぼりました(他の全業界の平均は12%)。ツールセットの整備にも積極的で、40%の組織が、使用するツールと機能の数が大幅に増えたと回答しています(同31%)。データサイロの解消にも熱心に取り組み、異なるツールで収集したすべてまたはほぼすべてのオブザーバビリティデータを相関付けできていると回答した割合が46%にのぼります(同38%)。
2. 監視チームとの統合が進んでおり、AIOpsとオブザーバビリティの統合が進行中と回答した割合が28%にのぼりました(他の全業界の平均は18%)。アプリケーションパフォーマンス監視、デジタルエクスペリエンス監視、ネットワークパフォーマンス監視でも統合が進み、セキュリティ監視との統合は37%の組織が完了しています(同26%)。

オブザーバビリティの成熟度が高いことによるメリットは明らかで、特に、アラートの精度と自動化の2つの領域で顕著です。監視アラートの精度が75%以上と回答した組織は35% (他の全業界の平均は24%)、アラートのトリアージと修復を自動化している組織は55% (同48%)にのぼります。

行政・公共機関

行政・公共機関はオブザーバビリティの成熟度が低く、リーダー的組織はわずか4%にとどまる一方、ビギナー組織は過半数の53%にのぼりました。この業界が直面している課題には以下のものがあります。

1. 監視ツールやチームがサイロ化しています。現時点で、アプリケーションパフォーマンス監視ツールとチームをオブザーバビリティプラクティスと統合している組織の割合は14%にとどまりました(他の全業界の平均は27%)。AIOpsとの統合にいたってはわずか3%でした(同26%)。

   業務統合が遅れてはいるものの、その意欲は高く、今後オブザーバビリティとアプリケーションパフォーマンス監視の統合に取り組む予定だと回答した割合は37% (同25%)、AIOpsとの統合に取り組む予定だと回答した割合は40% (同24%)にのぼりました。これは、行政・公共機関が業務統合の重要性を理解し、民間企業に追いつくための努力をしていることを示します。
2. レジリエンスに関する正式なアプローチの策定が後れています。行政・公共機関はレジリエンスに対する姿勢でも民間企業に後れを取っています。レジリエンスは、主要なビジネスプロセス、サービス提供、テクノロジーへのアクセスが中断される可能性のあるイベントを防止し、対応して、迅速に復旧する能力です。レジリエンスに関する正式なアプローチがあると回答した割合は、民間企業で40%であったのに対して、行政・公共機関では26%にとどまりました。
3. 人材不足が深刻です。行政・公共機関では、オブザーバビリティチームの有能な人材が引き抜かれて離職する「頭脳流出」が多く報告されています。過去12カ月間に頭脳流出が複数回発生したと回答した組織は49%にのぼります(他の全業界の平均は34%)。また、景気後退が見込まれる中で悲観的な組織が多く、59%が、景気が後退したら必要なオブザーバビリティスキルを持つ人材を確保するのが難しくなると予想しています(同43%)。

これらの課題は悪影響を生んでいます。自社製アプリケーションの根本原因分析にかかる時間について、民間企業では77%が過去12カ月間で短くなったと回答しているのに対して、行政・公共機関では48%が12カ月前と変わらないか前よりも長くなったと回答しています。

それでも希望はあります。使用するオブザーバビリティ機能が増えたと回答した割合が74%にのぼりました。しかも、ベンダーの増加を抑えて環境がこれ以上複雑化しないように注意を払っていると考えられ、77%が、エコシステムに新しいオブザーバビリティベンダーを追加していないと回答しています(民間企業では55%)。このように、複雑さの課題を悪化させないようにしながらオブザーバビリティを強化することは、特に人材不足の深刻化への備えとして大きな意味を持ちます。

Splunkの統合セキュリティ/オブザーバビリティプラットフォームで、組織のレジリエンスを向上させましょう。大規模な環境でもすばやく包括的に可視化して効果的なアクションにつなげることができます。あらゆるデジタルリスクに動じない安定した組織運用を支援するSplunkのソリューションをぜひご確認ください。

詳細はこちら

23-144642-Splunk-State of Obs 2023-EB-JA-202305

splunk>