

2025年



オブザーバビリティ 予測レポート



過去20年間における
テクノロジーの飛躍が

ソフトウェアのルールを変えてきました。

SaaSとモバイルの登場により、アプリケーションは企業ファイアウォールから解放されました。クラウドコンピューティングとマイクロサービスはデジタルトランスフォーメーションを加速させた一方で、複雑さも増大させました。

私たちは今、人のあらゆる活動にAIが組み込まれるという次の大変革期を迎えようとしています

単純な監視から真のオブザーバビリティへの移行が求められたこれまでの変化と同様に、AI時代にはそれを超えるインテリジェントオブザーバビリティが求められます。これは、稼働中のAIモデルを単に監視するという意味ではありません。熟練したエンジニアからIT分野以外の専門家に至るまで、誰もが数分でアプリケーションを構築し、導入できるというソフトウェアのカンブリア爆発に備えることを意味します。今後待ち受けている変化の規模、速度、複雑さ、多様さは、私たちがこれまで経験したことのないものとなるでしょう。

従来のオブザーバビリティでは不十分となるでしょう。バイブコーディングに対応するには、オブザーバビリティそのものが誰にでも利用できるようになる必要があります。今後は、インシデントの影響が顧客に及ぶ前に、人間とエージェントが問題をリアルタイムで診断して解決し、技術的イベントをビジネス成果に結び付け、インテリジェントなアクションを自動で実行することが求められます。

現代のオブザーバビリティは、メトリクス・イベント・ログ・トレース（MELT）というテレメトリーの柱を超えて拡大しています。高いパフォーマンスを発揮するチームは「MELTx」を活用しています。「x」とは、セキュリティシグナル、コストやパフォーマンスデータ、構成の変更、ランブック、依存関係など、完全なオブザーバビリティに必要なその他のすべての要素を指します。このような状況を受け、New Relicをはじめとするプラットフォームは、AIと確定的な洞察を組み合わせたインテリジェンスエンジンを搭載し、予測アラート、自動是正、既存ツールとシステム全体のシームレスな統合を可能にしています。

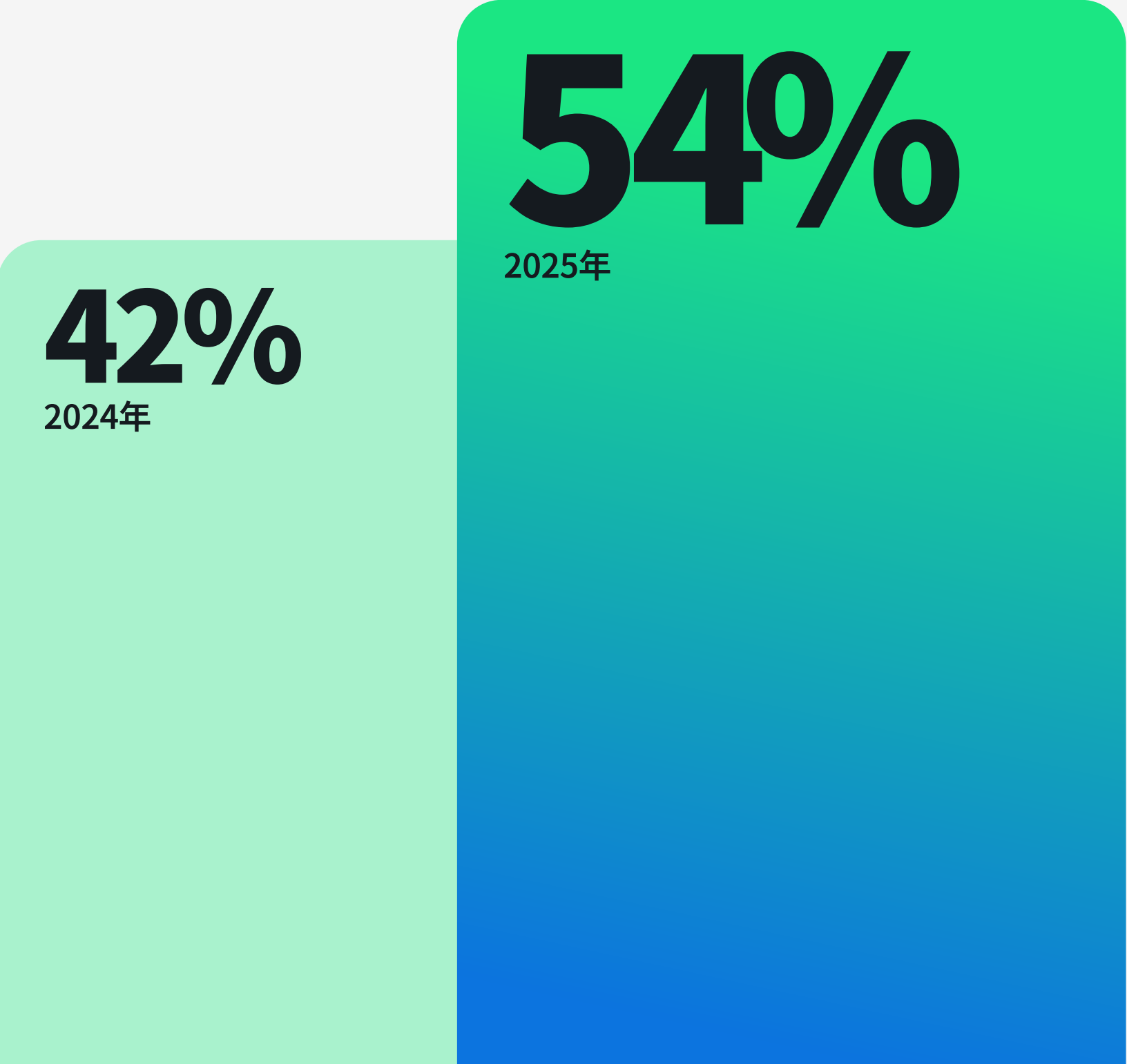
今年のオブザーバビリティ予測レポートでは、エンジニアリングおよびIT分野のリーダー1,700人を対象に調査を実施し、この新時代の成功を決定付ける機能、ビジネス成果、運用面の課題を明らかにしました。先行する組織がどのように断片化したツールを統合し、ダウンタイムを低減し、テレメトリーデータのビジネス価値を最大限に引き出しているのか、そして、インテリジェントオブザーバビリティがいかにAI駆動型企業の基盤となっているかを解明しています。

主な調査結果

AI監視

AIにより運用および開発業務が大きく変革しています。現在の導入状況では、AI監視の利用率は2024年の42%から2025年には54%に増加しており、前年比で2桁成長を達成しています。

企業はAIの試験段階を超え、実際の顧客が関わる環境やビジネスプロセスでの導入を進めています。



ダウンタイムに伴うコスト



最上位モデルのNVIDIA CPUを60秒ごとに焼き捨てるのと同等のコストです。デジタルシステムの停止による経済的損失は、ビジネスリソースを大きく圧迫します。運用のレジリエンスを高めることは、収益と市場の信頼を守るための実効性のある手段です。

ツールの統合

27% ツール数減少

利用ツールの平均数は2年間で27%減少していますが、組織あたりのオブザーバビリティツール数は平均4.4個であり、まだ改善の余地があります。統合されたオブザーバビリティプラットフォームへの移行を計画している組織は52%に上っており、この重要な動きは今後も続くと予想されます。

フルスタックオブザーバビリティ

フルスタックオブザーバビリティ（FSO）のギャップ：調査対象組織の73%がフルスタックオブザーバビリティを備えておらず、技術スタックとアプリケーションの大部分が依然として監視の対象外となっています。深刻なシステム停止に伴う平均コストは、フルスタックオブザーバビリティ¹を導入している組織では1時間あたり100万ドル、未導入の組織では1時間あたり200万ドルに上ります。リーダーにとってのメリットは明快です。フルスタックオブザーバビリティの実現により、運用リスクを減らし、インシデント対応を迅速化し、具体的な財務リターンを得られます。

システム停止コストの中央値（ビジネス影響大）



ビジネス影響

75% ROIを報告

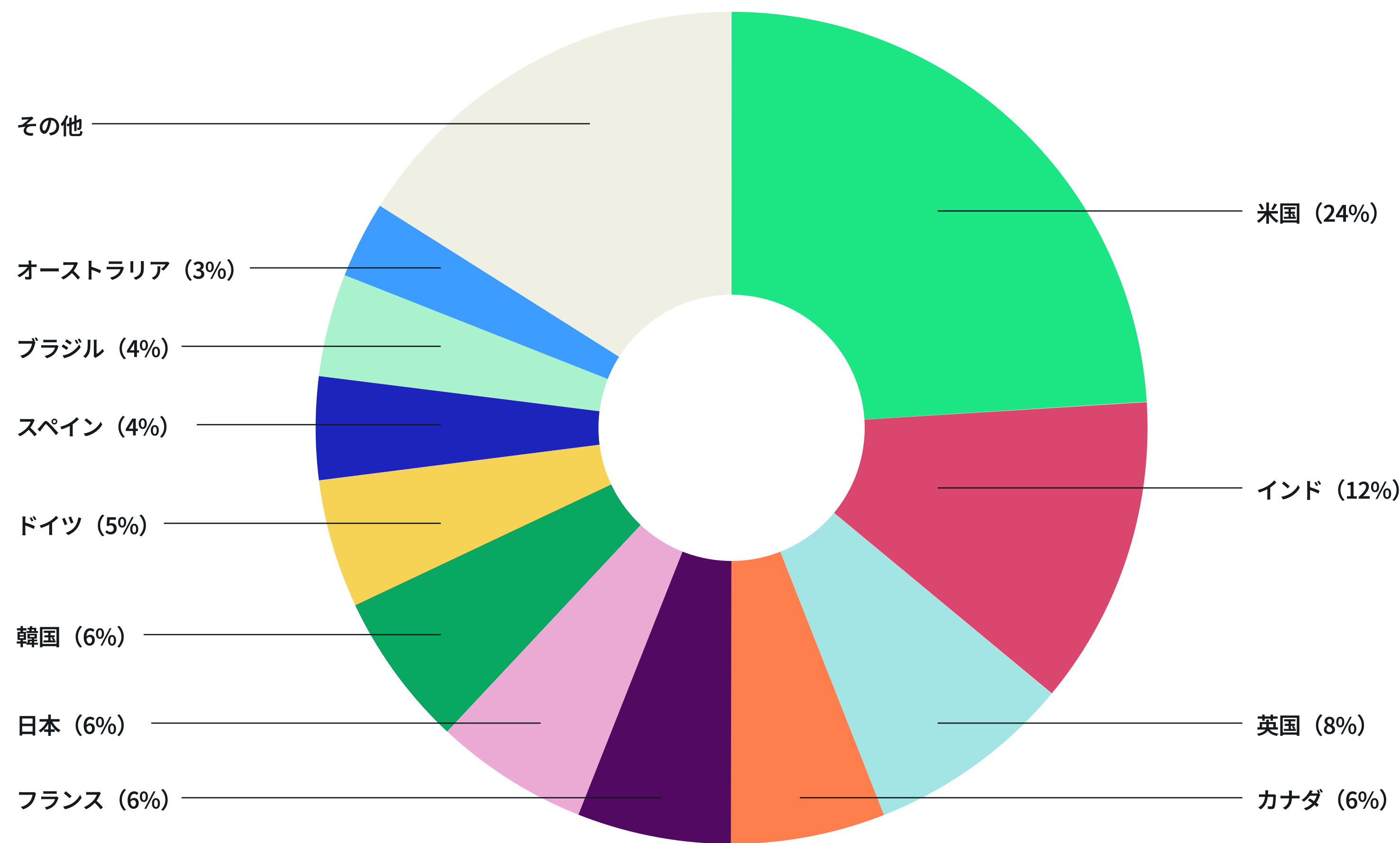
オブザーバビリティは大きなビジネス価値をもたらします。オブザーバビリティへの投資が望ましい利益をもたらしていると報告した企業は全体の75%に上り、約5分の1（18%）が3〜10倍のROIを実現していると回答しています。

¹ 本レポートにおいて、フルスタックオブザーバビリティ（FSO）とは、インフラストラクチャ、アプリケーションおよびサービス、セキュリティ監視、デジタルエクスペリエンスモニタリング（DEM）、ログ管理という5つの主要カテゴリにおける可視化の実現を指します。

調査の方法

New RelicはEnterprise Technology Research（ETR）と共同で、世界中のITおよびエンジニアリング分野のチームやリーダー1700人を対象に調査を実施しました。回答者は幅広い業界と規模組織から構成されています。

回答者の内訳
国



組織の年間収益： 調査対象組織の21%が10億ドル以上、11%が5億ドル～9億9,999万ドル、14%が2億5,000万ドル～4億9,900万ドル、54%が2億4,999万ドル未満

従業員数： 14%の組織が1万人以上の従業員を抱える
企業特性： 実務担当者65%、経営幹部11%、管理職24%

1,700人
IT分野のリーダー

20以上
国

10億ドル以上
調査対象者のうち21%の組織の年間収益

AI搭載オブザーバビリティの台頭

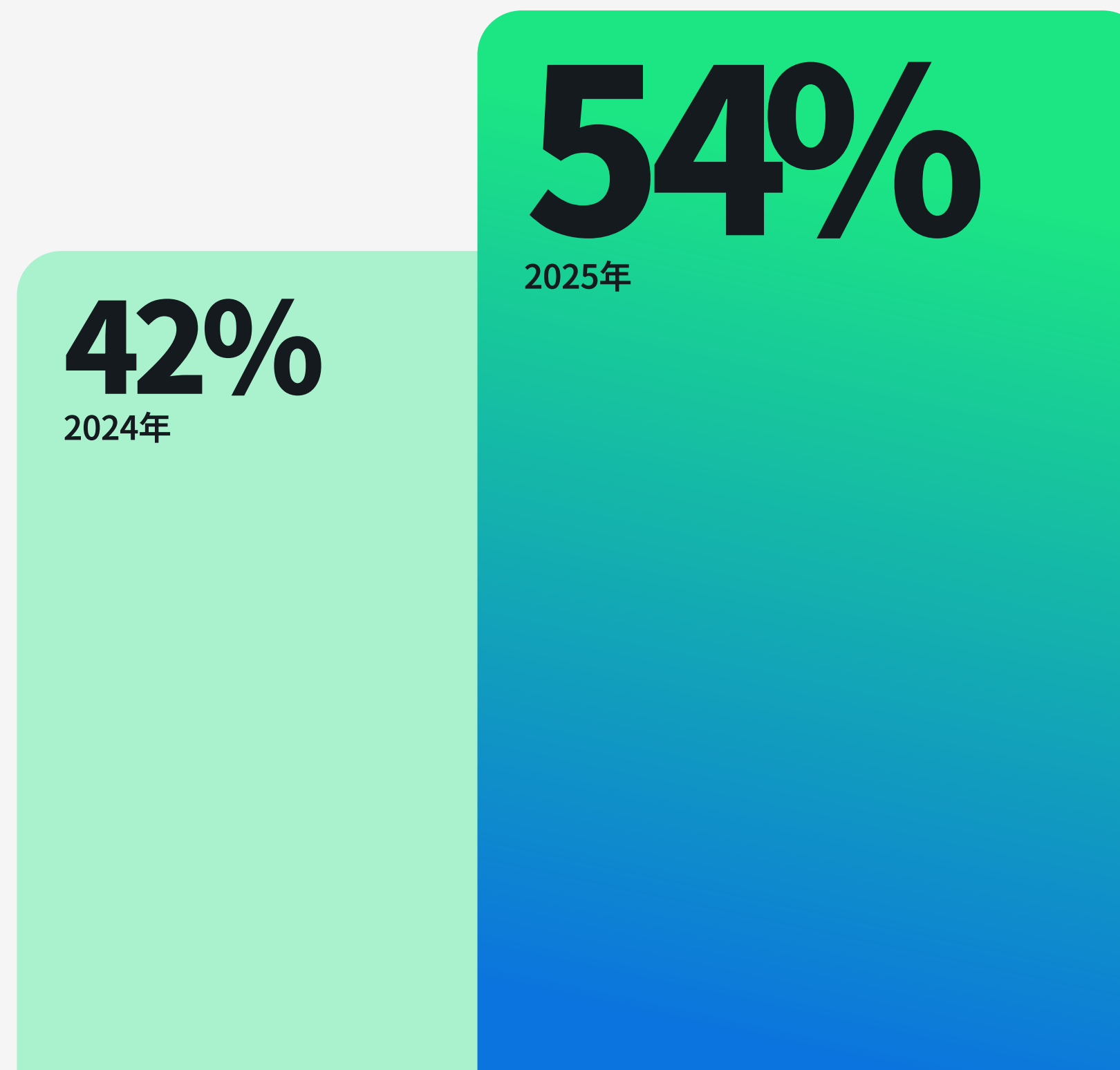
この移行は今まさに起こっています。
生成AIやエージェントAIのオブザーバビリティスタックへの統合がますます進んでいます。

AI強化型の監視機能は以前から利用可能でしたが、大半の組織はオブザーバビリティの成熟が不十分で、その機能を最大限に活用できていませんでした。その状況が変わりつつあります。組織はAIをフルスタックテレメトリー（MELTx）に適用することで、受け身の体制から事前対応・予測型の体制へとIT運用を移行させています。

AI監視の導入と影響

AI監視の利用率は2024年の42%から2025年の54%へと、**前年比で2桁成長を遂げており、導入組織が初めて過半数に達しました。**

AI監視機能を導入している組織の割合



この結果が示すこと

製品やワークフローにおけるAI導入の広がりにより、組織は隠れた障害を防ぐため、複雑な分散システムの動作や相互関係に関するリアルタイムの洞察を必要としています。その結果、より深いオブザーバビリティへの需要が高まっています。

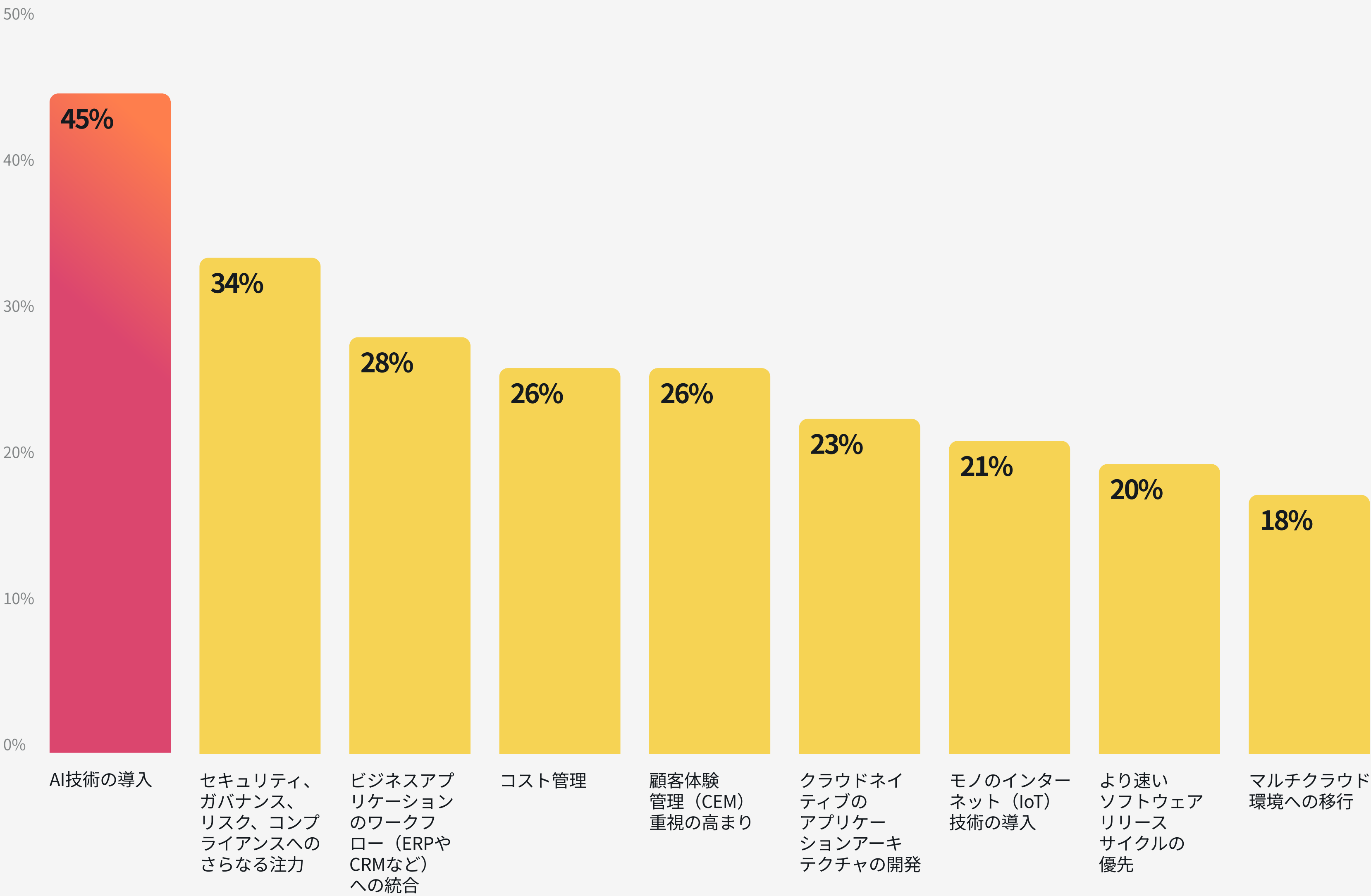
LLMを活用したアプリケーションやエージェントAIの導入が広がるにつれ、可視性に関する新たな課題が生じています。これらのモデルは確率的に動作し、動的な分散環境に依存しており、多くの場合、従来の監視方法では見えにくい形で障害を引き起こします。依存関係の特定がより困難です。障害の発見もより困難です。適切なオブザーバビリティを備えていない場合、隠れた問題が気付かないうちにシステム全体に波及するおそれがあります。

AIを大規模に導入する組織では、コードの追跡やインフラストラクチャの監視にとどまらない、より深いレベルのシステム洞察が必要となっています。場合によっては、AIをモニターするためのAIの導入が必要となり得ます。言い換えると、AIを搭載したオブザーバビリティプラットフォームを活用し、AIモデルとパイプライン、API、下流のアプリケーションとの相互作用をリアルタイムで把握することが求められます。

この傾向は、オブザーバビリティを欠くとAIの導入がもたらす影響が運用体制の整備を上回りかねないという重要なリスクも浮き彫りにしています。機械学習モデルのドリフト、隠れた障害、レイテンシを検出できない場合、ユーザー体験が低下し、ビジネスチャンスを逃すおそれがあります。成長を加速させるためにAIに投資する組織にとって、運用面でのリスクはすぐに顕在化し、具体的な影響をもたらします。

AI導入がオブザーバビリティの需要を牽引

オブザーバビリティの需要を押し上げている最大の要因はAI技術の導入であり、調査では経営幹部の45%がこれを挙げており、他の要因を上回っています。



この結果が示すこと

システムが複雑化し、人間だけでの追跡が難しくなる中、AI強化型オブザーバビリティが不可欠となりつつあります。AIによって問題の早期検出と自動対応が可能になり、ダウンタイムを減らし、復旧までの時間を早め、ユーザーへの影響を防ぐことができます。

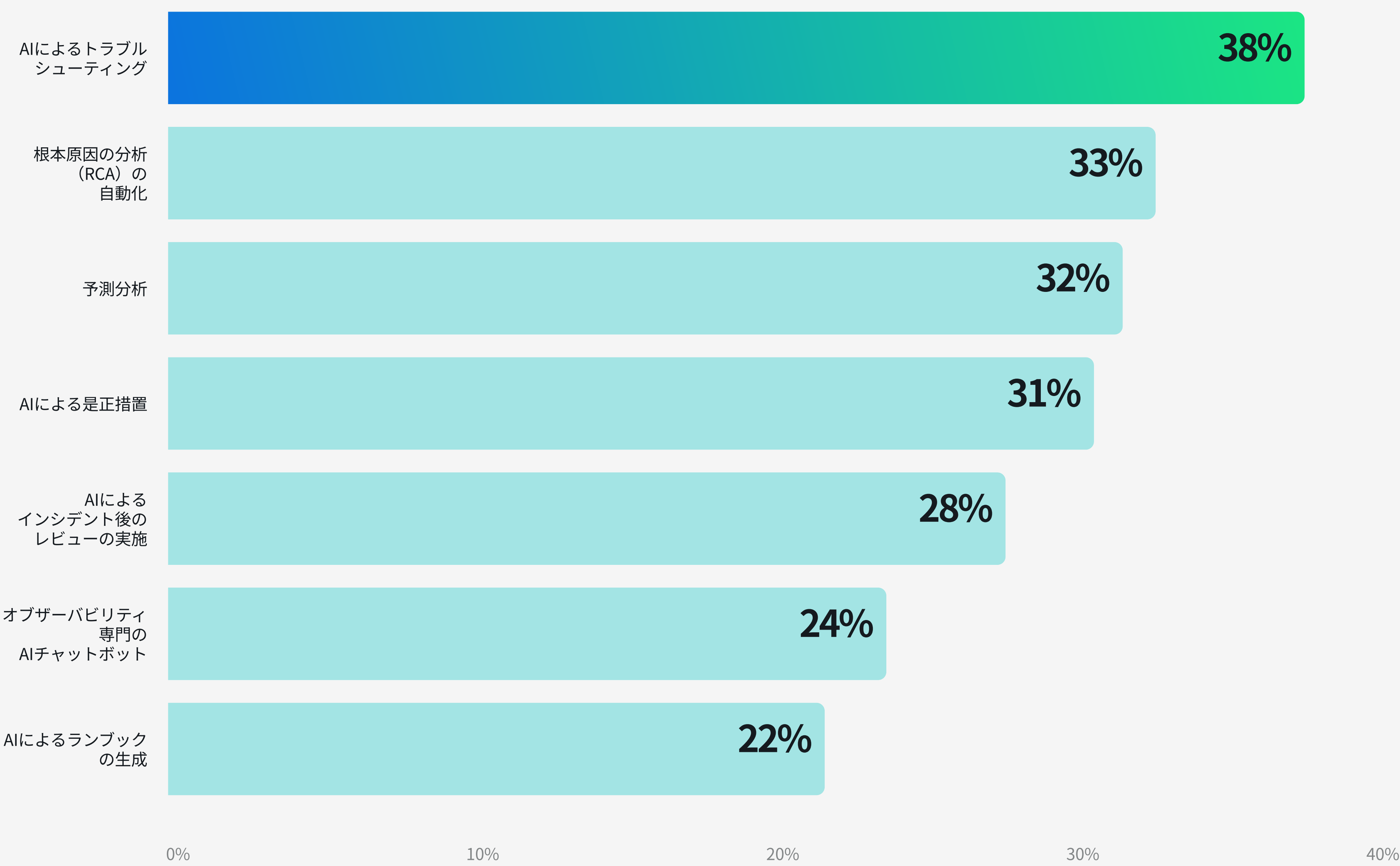
AI監視とオブザーバビリティの急速な発展は、運用担当者が合理的に追跡できないほどにシステムが複雑化しているという単純な現実を映し出しています。現在、細かに分散した変化の速い環境でサービスが実行されており、膨大なテレメトリーが生成されています。インテリジェントな支援がない場合、重大な異常がデータの海に埋もれてしまい、ビジネス影響を引き起こすインシデントに発展する可能性があります。

調査の結果、AIによってオブザーバビリティを強化できる最大の機会が明らかになりました。経営幹部とIT分野のリーダーは、最も有効な機能としてAIによるトラブルシューティング（38%）を挙げており、これによりチームは問題が拡大する前に診断できます。次いで、根本原因分析の自動化（33%）や、ロールバックや構成更新などのAIによる是正措置（31%）が挙げられており、これらの機能により平均解決時間（MTTR）を大幅に短縮し、インシデントの影響範囲を抑えることができます。また、予測分析（32%）も上位にあり、ユーザーに影響が及ぶ前に問題を予測できる機能が求められていることを示しています。

この技術は運用戦略を大きく変えるものです。これまでシステム停止への対応に追われていたチームが、今ではユーザーが気付く前に問題を解決し始めています。ダウンタイムの低減と復旧の迅速化は財務的リスクの低減に直結し、エンジニアはアラートの追跡ではなく製品開発などのより価値の高い取り組みに注力できるようになります。

この進化の次の段階では、AIが検出を超えて積極的に介入するようになり、システムの自動化がさらに進むと予想されます。適応の速い組織が、レジリエンスの強化、インシデントコストの削減、人員を同じペースで増やさずに拡張できる自由といった構造上の利点を得られます。

組織のインシデント対応や
オブザーバビリティ業務を
最も向上させるAI機能は
どれだと思いますか？



ビジネス成果

オブザーバビリティの具体的な価値

AIの導入はオブザーバビリティを変革する強力な原動力ですが、それは全体像の一部に過ぎません。

オブザーバビリティは重要なビジネスメトリクスに直接影響し、さまざまなパフォーマンス指標にわたり明確な投資利益を実証しています。調査回答者は、運用のレジリエンス、エンジニアリングの効率、ビジネスの成長という3つの主要領域で、オブザーバビリティの効果を認識しています。



ダウンタイムによる 莫大なコスト

オブザーバビリティはシステムの
安定性と可用性を直接向上させ、
インシデント解決の迅速化と
ダウンタイムの短縮により収益と
ブランドの評判を保護できます。

200万ドル 米ドル/時間

調査対象組織における深刻な
ビジネス停止に伴うコストの
中央値。

この結果が示すこと

オブザーバビリティの導入により運用の
レジリエンスが直接向上し、重大なシス
テム停止による対応時間と財務的影響を
大幅に抑制できます。

ダウンタイムは、IT部門の懸念から、今や取締役会レベル
のリスクへと変わりました。調査によると、組織が報告し
た**深刻なシステム停止によるコストの中央値は1時間あた
り200万ドル**であり、短時間の停止であっても多大な経済
的リスクを伴うことを示しています。収益、顧客からの信
頼、ブランドの評判のすべてがリスクにさらされている場
合、システムの停止が1分続くごとにビジネス影響が累積
していきます。

この累積効果を例示すると、報告されたコストとシステム
停止の平均頻度を年間換算した場合、**深刻なビジネスシ
ステム停止によるリスクは年間7,600万ドル**に上ります。
これが取締役会レベルのリスクであることにお気づきで
しょうか。

経済効果は明白です。システム停止の期間と頻度が減る
ことで、数百万ドルのコスト削減となります。オブザー
バビリティを導入した組織は、平均検出期間（MTTD）
およびMTTRの両方で明らかな改善を見せたと報告して
います。問題の検出と解決が迅速化することで、リスク
にさらされる期間が短縮し、個々のインシデントが連鎖
的なビジネス障害に発展することを防止できます。

“

ダウンタイムは直接コストと
なります。私たちは
New Relicを利用して
**全インシデントの
ダウンタイムを
算定しています。**

New Relicのメトリクスを確認することで、
影響を受けたトランザクションの数を
正確に把握し、インシデントの重大度と
コストを適切に判断できます。

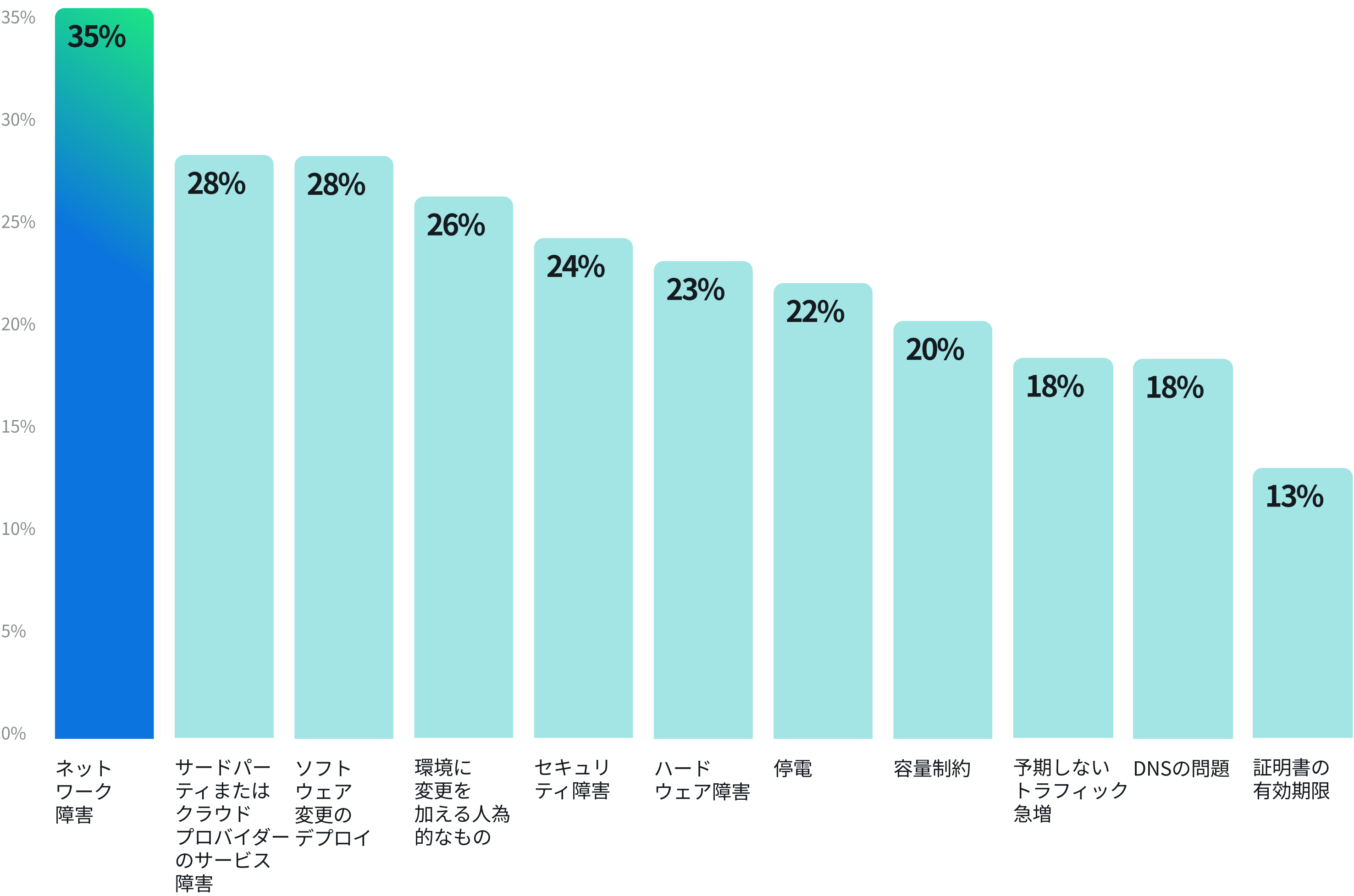
Tibi Guiu
ITガバナンス部門責任者



オブザーバビリティの導入後にMTTDが改善したと報告した調査対象組織は約7割（68%）に上り、可視性と速度が技術的な成果であるだけでなく、財務的にも不可欠であることを裏付けています。

このようなコストのかかるシステム停止の根本原因は、現代のデジタル環境の複雑さを物語っています。依然としてネットワーク障害（35%）とサードパーティプロバイダーの問題（28%）が主な原因となっており、相互接続が進むシステムの脆弱性を浮き彫りにしています。そのほか、ソフトウェアの導入（28%）や計画外の環境変化（26%）をきっかけとして予防できるはずのインシデントが発生し続けており、その多くは導入前の可視性の不足や監視の断片化が原因です。分散アーキテクチャでは、一つの構成ミスが数十ものサービスに波及する可能性があり、この脆弱性には多大な代償を伴います。

システム停止の主な原因

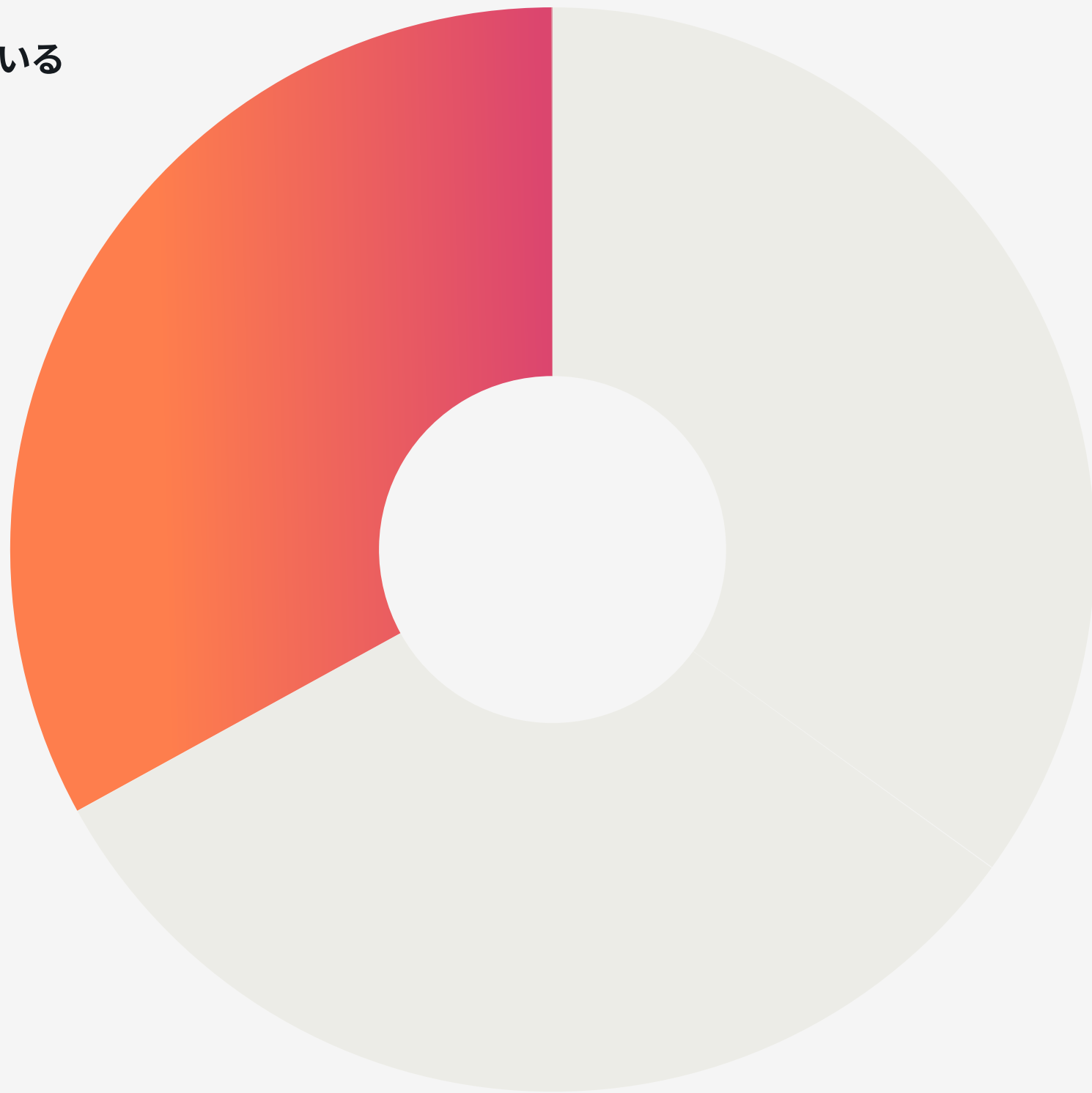


エンジニアリングの生産性と満足度の向上

オブザーバビリティツールの導入により、エンジニアリングチームは緊急対応に追われることなくイノベーションに注力できるようになり、生産的でやりがいのある職場環境を育みます。

33%

のエンジニアの労働時間が
緊急対応
や障害対応に費やされている



この結果が示すこと

エンジニアリングチームは依然として事後的な対応に縛られており、それが士気を低下させ、ひいては収益にも影響を与えています。現在、エンジニアがプラスのビジネス影響をもたらすプロジェクトに取り組めるようにすることが、これまで以上に重要となっています。

AI強化型オブザーバビリティはイノベーションへの注力と士気の向上に向けた明確な道筋を示します。

エンジニアリング業務の3分の1は依然として事後対応や緊急対応に費やされています。エンジニアリング業務のさらに33%が保守や技術的負債に費やされていることから、現時点では、エンジニアの業務時間のうち3分の2以上が新機能の開発や革新的なコーディング以外の作業に費やされていることになります。

経営幹部と実務担当者のどちらも、より優れた高度に自動化されたオブザーバビリティには大きなメリットがあると認識しています。経営者が挙げたオブザーバビリティのメリットで最も多かったのは「予期しないダウンタイムの低減」（リーダーの55%が回答）で、次いで「業務全体の効率化」（50%）と「セキュリティリスクの軽減」（46%）が続きます。

実務担当者が挙げたメリットで最も多かったのは「アラート疲れの軽減」で、エンジニアとSREの59%が回答しています。実務担当者のメリットの上位3つのうち残りは「トラブルシューティングと根本原因分析の迅速化」（58%）と「チーム間連携の向上」（52%）でした。

AI支援などの機能により、オブザーバビリティワークフローが向上することで、エンジニアは問題を迅速に特定できるようになり、複雑なシステムのデバッグに伴う認知的な負荷やフラストレーションが軽減されます。

エンジニアリングチームは、事後的な対応にかかる時間が減ることで、新機能の開発、既存製品の改善、イノベーションにさらに専念できるようになります。

これは実務担当者の満足度やワークライフバランスの向上に直接貢献するため、離職率の低下や優秀な人材の獲得につながります。

“

New Relicを活用して、244件の問題を5時間で解決できました。プロアクティブな監視により、

年間1,600万ドルの削減になったと推計しています。

インシデントの予防が可能になれば、顧客体験と顧客満足度を高められます。

Cody Chandler
クラウドエンジニアリング担当
シニアディレクター

 **BLACKLINE**



オブザーバビリティは企業に具体的なROIをもたらす

オブザーバビリティの影響はIT運用にとどまらず、ビジネスパフォーマンス、顧客体験、事業成長にも直接及んでいます。



75%

の企業が、オブザーバビリティへの投資が望ましい利益をもたらしていると報告しており、約5分の1（18%）の企業が3～10倍のROIを実現していると回答しています。

この結果が示すこと

オブザーバビリティの価値はITの領域にとどまらず、アップタイムの向上や運用コストの削減といった中核的なビジネス目標の達成に直接貢献します。

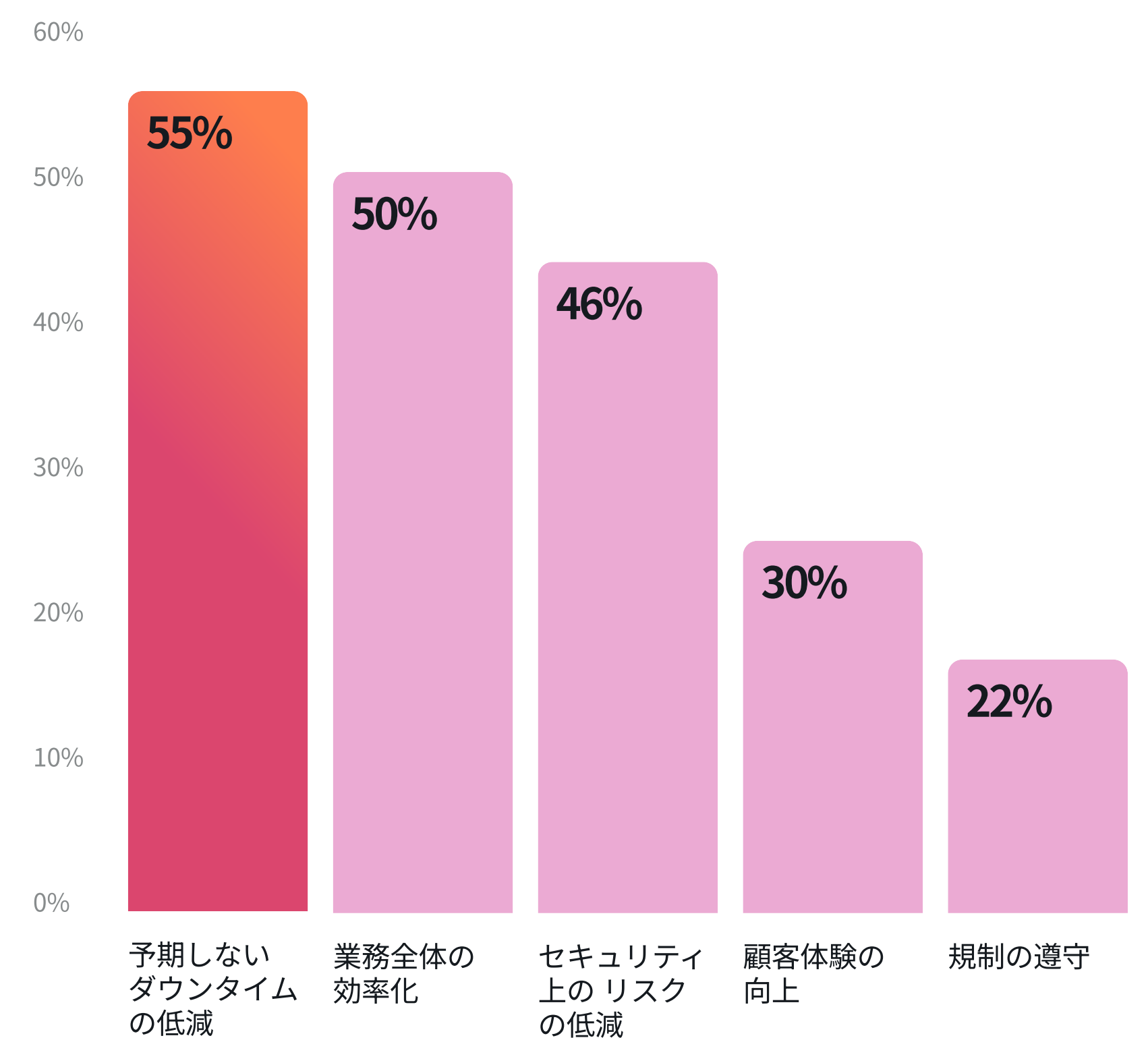
信頼性が高く高性能なデジタルサービスは、良好な顧客体験を築く基盤となります。オブザーバビリティは、障害を最小限に抑え、最適なアプリケーションパフォーマンスを確保することで、このような顧客体験を直接支えます。

オブザーバビリティが企業にもたらす最大のメリットとして、リーダーの55%が「予期しないダウンタイムの低減」を挙げています。問題の特定と解決を迅速化することで、重大なビジネスアプリケーションのダウンタイムを減らし、顧客の定着率と満足度を高めることができます。

さらに、オブザーバビリティのビジネス上のメリットとして、50%が運用効率の向上、30%が顧客体験の向上を挙げています。これは当然の結果であり、オブザーバビリティから得られる洞察により、チームはレジリエンスとパフォーマンスに優れた製品を初期段階から開発できるようになります。

オブザーバビリティは継続的に投資を回収できる技術カテゴリの一つとして注目が集まっています。予算が精査され、すべての投資に価値の裏付けが求められる市場において、これは大きな強みとなります。さらに、業績の高い企業では、次のイノベーションの波への投資を可能にする大きなリターンを生み出しています。

オブザーバビリティが企業にもたらす主なメリット



フルスタック オブザー バビリティを 実現する上での 課題

導入が急速に広がる一方で、多くの組織は真のフルスタックオブザーバビリティ（FSO）の実現に苦慮しています。

課題の多くは構造的なものであり、技術スタックの分散、監視ツールの重複や余剰、テレメトリデータのサイロ化によって死角が生まれ、インシデントの解決が遅れます。一部のチームはツールの統合やデータフローの標準化に着手していますが、オブザーバビリティ全体の成熟度は、現代のデジタル環境の複雑さにまだ追いついていないのが現状です。

フルスタックオブザーバビリティのギャップ



73%

の調査対象組織がフルスタックオブザーバビリティを備えておらず、その結果、技術インフラとアプリケーションの大部分で障害が起きやすくなり、運用や顧客体験を損なうリスクが高まっています。

この結果が示すこと

フルスタックオブザーバビリティの導入により、インフラストラクチャ、アプリケーションおよびサービス、セキュリティ監視、デジタルエクスペリエンスモニタリング（DEM）、ログ監視における可視性が統合されます。これがない場合、チームは重大な死角を残したまま作業を行うことになり、不具合の原因検出の遅れ、システム停止の長期化、コストの上昇を招きます。

フルスタックオブザーバビリティを導入していない場合、組織は運用上のリスクと財務上のリスクの両方にさらされることになります。監視ツールが分散し、データがサイロ化されるため、エンジニアはインシデントの調査時に断片的な洞察をつなぎ合わせる必要があり、対応時間の遅れやシステム停止コストの増加を招きます。それに対し、フルスタックオブザーバビリティを導入した組織では、フロントエンドのユーザー体験からバックエンドのインフラやAPIに至るまで、エンドツーエンドで問題を追跡できるため、より迅速な解決とよりの確な意思決定が可能になります。

フルスタックオブザーバビリティには、パフォーマンスとコストの面で大きなメリットがあります。導入したチームでは、システム停止の発生回数が減少しています（深刻なシステム停止が週1回以上発生している割合はわずか23%で、未導入の場合の40%を大きく下回っています）。また、MTTDは28分となっており、未導入の場合より7分短縮されます。最も際立っているのは金銭的な差で、**深刻なシステム停止に伴う平均コストはフルスタックオブザーバビリティ導入時が1時間あたり100万ドルであるのに対し、未導入時は1時間あたり200万ドルです。**

リーダーにとってのメリットは明快です。フルスタックオブザーバビリティの実現により、運用リスクを減らし、インシデント対応を迅速化し、具体的な財務リターンを得られます。

少なくとも週に1回のシステム停止が発生（ビジネス影響が大きいシステム停止）

23%

フルスタック
オブザーバビリティ
導入済み

40%

フルスタック
オブザーバビリティ
未導入

システム停止MTTDの中央値（ビジネス影響が大きいシステム停止）

28分

フルスタック
オブザーバビリティ
導入済み

35分

フルスタック
オブザーバビリティ
未導入

システム停止コストの中央値（ビジネス影響大）

100万ドル

1時間あたり

フルスタック
オブザーバビリティ
導入済み

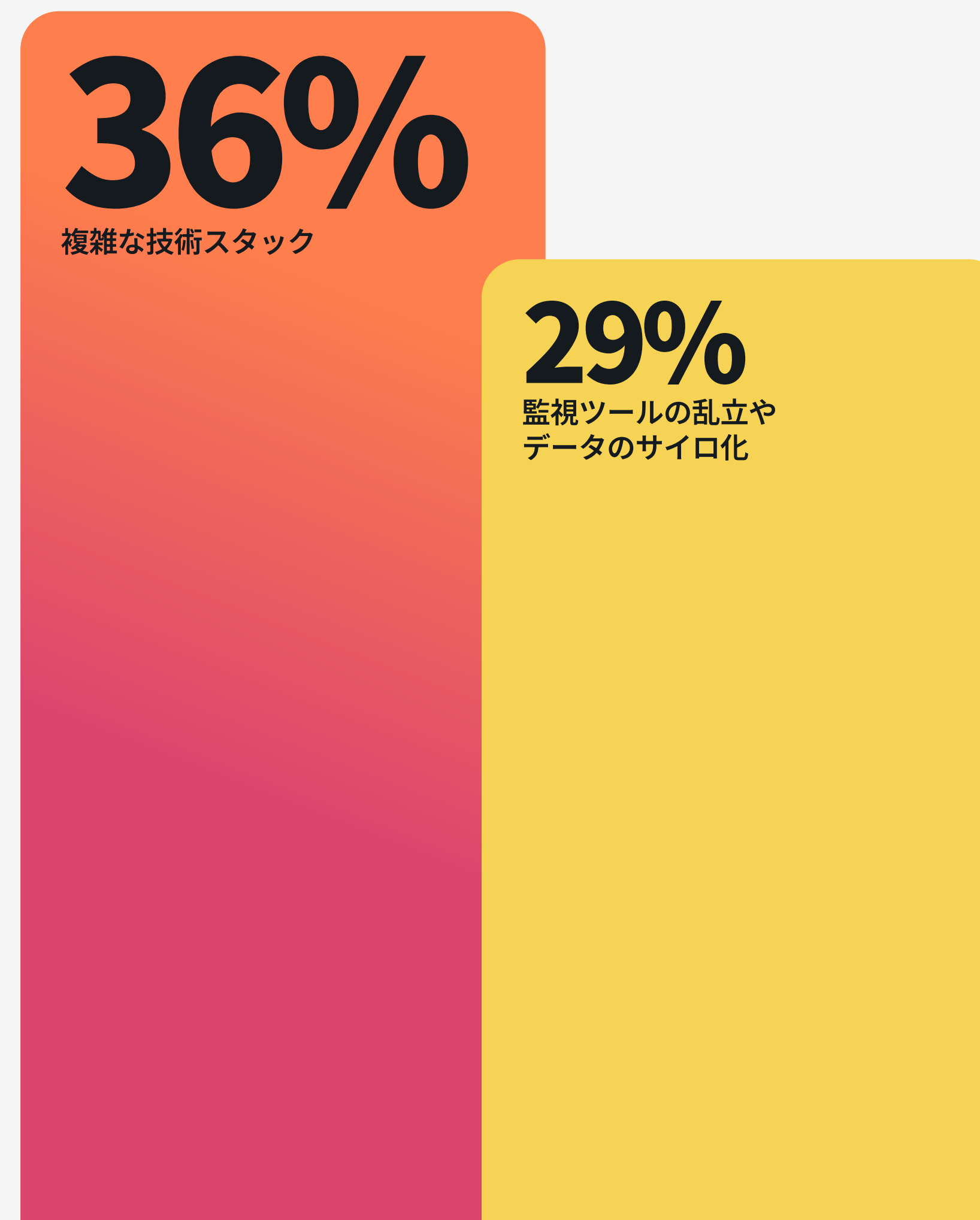
200万ドル

1時間あたり

フルスタック
オブザーバビリティ
未導入

複雑な技術スタック とサイロ化された データ

36%が「複雑な技術スタック」、
29%が「監視ツールの乱立や
データのサイロ化」を
最大の課題として挙げています。



この結果が示すこと

複雑で断片化した技術スタックとデータのサイロ化により、チームがシステムの健全性を適切に把握することが難しくなっています。ツールを統合し、データを統一することが、レジリエンスを高め、真の全体像を可視化するための鍵となります。

現代のデジタル環境は肥大化と断片化が進んでおり、フルスタックオブザーバビリティを実現する上での大きな障壁となっています。最大の課題として、リーダーの3分の1以上（36%）が「複雑な技術スタック」、29%が「監視ツールの乱立やデータのサイロ化」を挙げています。多くの場合、これらは表裏一体の問題です。新しいサービス、クラウド、フレームワークを導入するたびにテレメトリーが増大し、最終的には連携されていないツール間に分散してしまいます。

その結果、システムの健全性の把握が断片的になります。エンジニアは複数のダッシュボードを切り替えてインシデントの全容をつなぎ合わせる必要がありますが、重要な兆候は孤立したデータサイロに隠れたままです。また、テレメトリーに一貫性がないため、包括的で相関するデータに依存している異常検出や自動根本原因分析といったAI機能の有効性が制限されます。

このような運用上の足かせにより、多くの組織が監視エコシステムを徹底的に見直すとともに、複雑さそのものがレジリエンスの障害となっていることを認識しています。オブザーバビリティの取り組みの次のステップは統合です。ツール群の簡素化とデータフローの統一によってサイロを解消し、システムの健全性の真の全体像を可視化します。

組織によるオブザーバビリティツールの統合が進む

企業はオブザーバビリティツールの統合がもたらす価値を把握しています。統合されたオブザーバビリティプラットフォームは、運用を効率化し、複雑さを解消し、システム全体の健全性を可視化します。

この結果が示すこと

オブザーバビリティツールの乱立が負担となっていた組織が改善を進めた結果、ツールの組織あたりの平均数は2023年の6個から4.4個へと減少しています。中央値はさらに低く、現時点で組織あたり4個となっています。

27%↓

2023年から2025年にかけて、組織が利用しているオブザーバビリティツールの数の平均が減少しています。

組織はツールの分散の抑制に積極的に取り組んでいます。オブザーバビリティツールの組織あたりの平均数は2023年の6個から4.4個へと27%減少しており、特に注目すべき点として、一部のリーダーはさらに少ない数で運用しています。この傾向は、ツールの乱立により、解決できる問題と同じくらい多くの問題（データの断片化、オーバーヘッドの増加、インシデント対応の遅延）を引き起こすという認識の広がりを反映しています。

コスト面の考慮も常に議論となっています。オブザーバビリティプラットフォームの選定時に最も優先する基準として、リーダーの37%がコストを挙げており、財務上の圧力が統一ソリューションへの移行を加速させていることを示しています。

複数のツールの利用には複数のライセンス、統合作業、管理サイクルを伴いますが、統合により、そのすべての面で負担軽減が期待できます。

利用するツールが減ることで、エンジニアリングはダッシュボードや統合作業に煩わされず、問題の解決に専念できます。統合の実現により認知的負荷が軽減し、インシデントの解決が迅速化するとともに、保守やライセンス、重大なシステム停止時の対応遅延リスクなど、断片化したシステムに起因する隠れたコストも削減できます。



Skyscannerは、**New Relicの導入により、12を超える監視ツールを置き換えることができました。**

これまで、10人の経験豊富なエンジニアが監視ソリューションの維持管理に専念する必要がありました。それが現在では、導入や活用の促進に専念できています。

Skyscannerエンジニアリングチーム

組織はオブザーバビリティ成熟への途上にあります。



41%

のリーダーは、サービスの停止（システム障害など）が発生した際に、いまだに顧客からの苦情、インシデントチケット、手動での確認などの非効率な手段によって、初めてその事実を知ることがあると回答しています。

この結果が示すこと

これはフルスタックオブザーバビリティによって実現されるものとは真逆の状況を表しています。多くの組織が依然として後手に回っており、問題の発見を顧客からの苦情や手動での確認に頼っています。

組織はオブザーバビリティに投資しているものの、依然として多くの組織がフルスタックの可視性の実現にはほど遠い状況にあります。顧客からの苦情、インシデントチケット、手動チェックなど、依然として非効率な手段でサービスの停止を把握していると回答したリーダーは41%に上ります。このような受動的な情報に頼っている現状は、多くの組織にとってオブザーバビリティがインシデントの早期検出や予防の面で期待どおりの成果を出せていないことを示しています。

手動チェックや外部からの報告に依存すると、チームがリスクにさらされることになります。システム停止が必要以上に長期化するおそれがあり、ユーザー体験が低下し、インシデント対応が適切に管理されたデータドリブンのプロセスではなく、緊急時のような場当たりの対応に陥ってしまいます。これは名ばかりのオブザーバビリティであり、真の洞察を欠いた可視性だけを提供するダッシュボードやアラートの寄せ集めに過ぎません。

これに対し、成熟したオブザーバビリティ（フルスタックオブザーバビリティ）では、アプリケーション、インフラ、サービス全体のテレメトリデータを相関し、ユーザーが気付く前に異常を検出します。その結果、チームはインシデントの追跡から予防へと移行し、インテリジェントなアラートや予測分析といった最新の手法を活用できるようになります。

2025年において、成熟度のギャップは、レジリエンスを備えた革新的なリーダーと、依然として場当たりの対応にとどまっているリーダーとを分ける明確な境界線となっています。

2025年以降に 向けた戦略的 優先課題

オブザーバビリティ予測の調査結果を見ると、ITおよびデータ分野のリーダーにとっての明確な優先課題が浮き彫りになります。

システムの健全性を一元的に
可視化する統合プラットフォーム
を重視する

オブザーバビリティ駆動型の
文化を育む

AIを活用し、プロアクティブに
対応できる運用を実現する

統合プラットフォームを優先する動きが進む

調査データは、ツールの分散に対処し、全体像を可視化するための重要な戦略として、オブザーバビリティツールを統合されたプラットフォームに統合する必要性を明確に示しています。

52%

の組織が今後12〜24か月以内にオブザーバビリティツールを単一のプラットフォームへ統合することを計画しています。

組織のオブザーバビリティ戦略（今後12〜24か月）

オブザーバビリティツールの統合プラットフォームへの統合



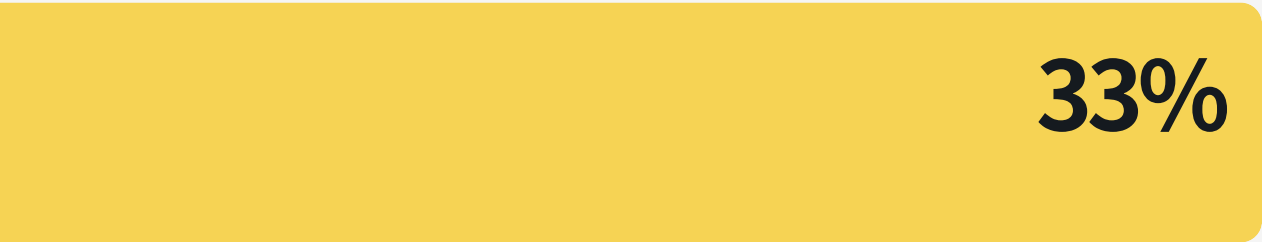
AIOps/ML機能への投資拡大



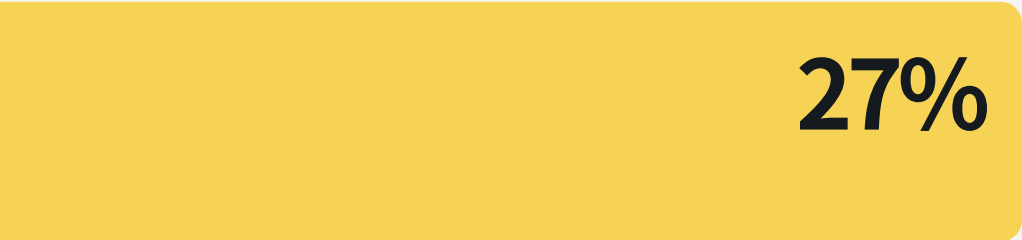
使用量ベースの価格設定モデルの採用



フルスタックオブザーバビリティへの注力



OpenTelemetry導入の優先



0% 10% 20% 30% 40% 50% 60%

この結果が示すこと

業界では、ツールの分散への対処、可視性の向上、包括的な洞察の取得といった明確なニーズに後押しされ、統合されたオブザーバビリティプラットフォームへの移行が本格化しています。

大多数の組織が近い将来にオブザーバビリティツールを単一のプラットフォームに統合する計画を立てており、このことは、ポイントソリューションやツールの分散からの脱却を目指す業界の強い動きを表しています。

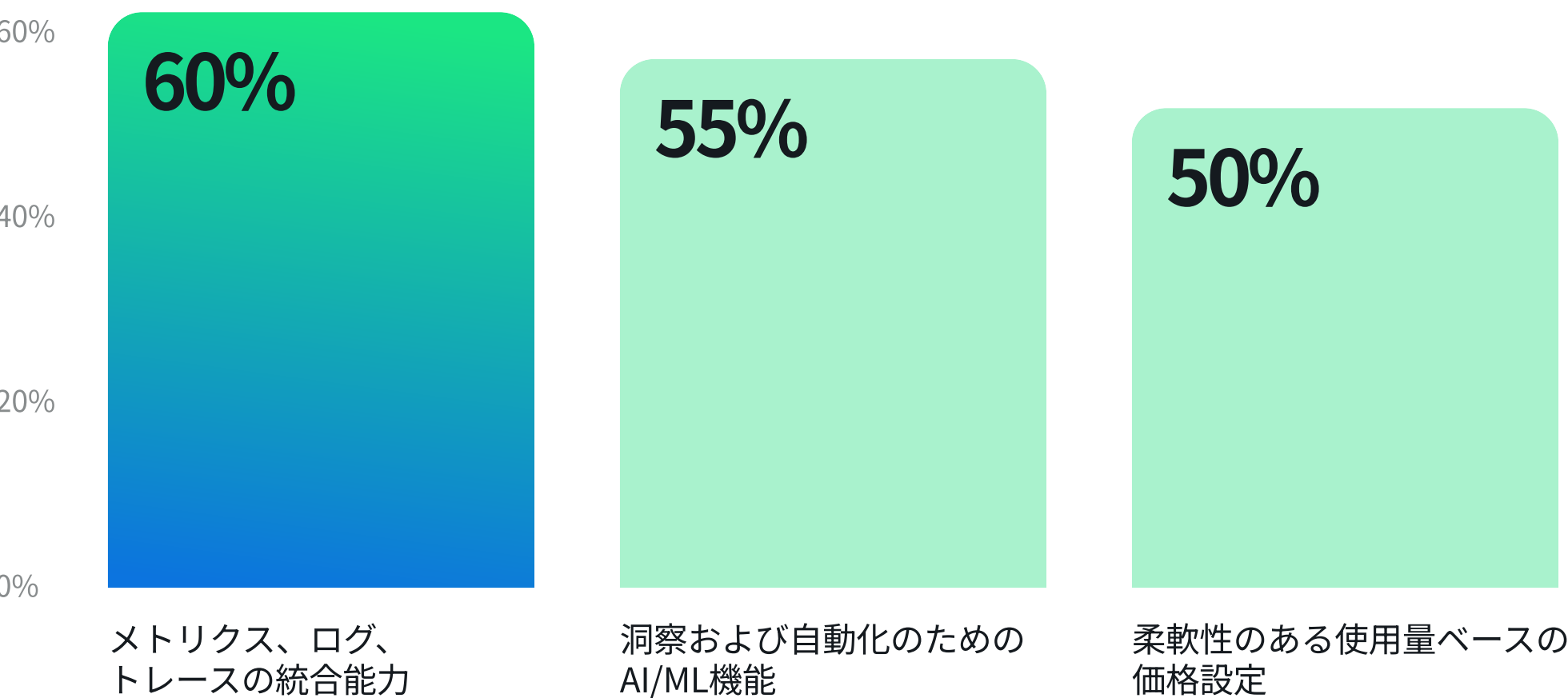
オブザーバビリティツールのベンダーを選定する際の最も多い決め手として、過半数（60%）がメトリクス、ログ、トレースの統合能力を挙げています。

ベンダー選定理由の上位3つの残りの項目として、55%が洞察と自動化のためのAI/ML機能、50%が柔軟性のある使用量ベースの価格設定を挙げました。

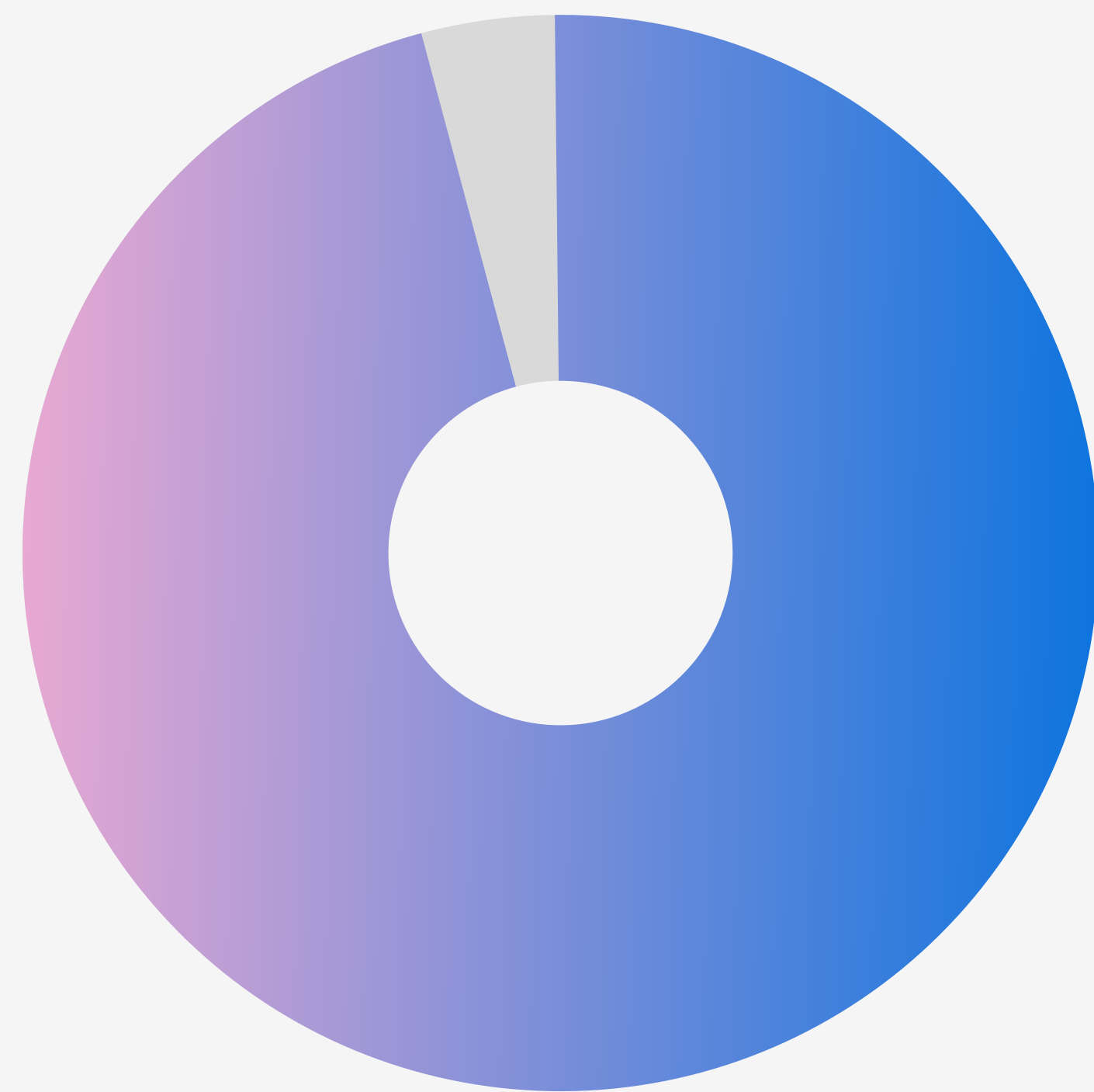
要するに、オブザーバビリティの購入者は統合、AI機能、柔軟な価格設定モデルを優先しています。これらすべての項目が、ツールの分散と高コストという組織の主要な課題に直結しています。

統合されたプラットフォームは、メトリクス、ログ、トレースを単一の画面で提供することで、コンテキストの切り替えをなくし、関連データによって迅速な問題解決を可能にします。

オブザーバビリティベンダーの主な選定基準



オブザーバビリティにおけるAIの活用機会



96%

AI監視機能を導入済みまたは
投資を計画している企業の割合

この結果が示すこと

AI監視は急速に一般化しています。AI監視を導入しておらず、計画もしていない企業はわずか4%であり、投資を怠る組織は運用のレジリエンスとAIによる収益獲得競争の両面で後れを取るリスクがあります。

AIは組織の運営やイノベーションを根本から再構築し、段階的な改善にとどまらず、まったく新しい可能性を生み出します。AIはすでに労力の削減やリリースサイクルの短縮を実現していますが、最も革新的な進展は、人間では考えつかないような、AIが生成するソリューションから生まれるでしょう。そのような革新は従来の製品ロードマップに沿ったものではなく、人間の認知的制約にとらわれずに探求、学習、最適化を行う自律システムから創造されます。

ITおよびエンジニアリング分野のリーダーにとって、これは従来の予想を覆すイノベーションの波に備えることを意味します。真の競争優位性は、常識にとらわれないAI搭載ソリューションを競合他社よりも早く発見、評価、実用化できるチームが握ることになります。そのためには、馴染みの薄いAIシステムの挙動をリアルタイムで監視し、解釈できる堅牢なオブザーバビリティフレームワークが必要となります。

これには大きなリスクを伴います。リーダーは、既存モデルに適合しないという理由で画期的なイノベーションを無視するか、内部構造が不明なために信頼できないという、いずれかのリスクを負うことになります。オブザーバビリティは重要な橋渡し役となり、AI搭載システムがどのように結論を導くかを把握し、現実世界での結果を測定し、大規模導入を確信をもって判断するために必要なテレメトリ、コンテキスト、分析を提供します。

先を見据えている組織は、オブザーバビリティへの投資を単なる障害検知にとどまらない領域へと拡大しています。具体的には、AIネイティブアーキテクチャを監視し、人間の論理から逸脱するパターンを分析し、次世代のソフトウェア開発を形作る革新の価値を捉えるという、未知のものを解釈する能力の開発です。最終的に勝利を収めるには、こうした機会が顕在化する前に見極めて活用することが求められます。

結論 / オブザーバビリティの展望

予測的行動、AI、レジリエンス

組織は、ビジネスを行う代償としてツールの分散や1時間あたり数百万ドルに上るシステム停止コストを受け入れ続けるか、戦略的な代替策としてAI強化型フルスタックオブザーバビリティを導入するかを選択を迫られています。

この移行はすでに進行しており、それを後押しするのは、「システムやサービスの信頼性は全員の責任である」という、近年再構築された文化です。プラットフォームの統合とAIの活用により、従来の「どこが壊れたのか？」という問いから「次に壊れる可能性があるのはどこか？」という問いへの転換が求められます。AIアプリケーションがビジネスの中心となるにつれ、統合されたオブザーバビリティの視点からAIの挙動を把握することは、レジリエンスとイノベーションの両面で不可欠となっています。

成熟の次の段階では、段階的な成果よりも、先を見越した効率的でインテリジェントな運用モデルへの根本的な移行が重視されます。New Relicのようなプラットフォームは、このような未来に備えるリーダーに対し、確信をもって構築、運用、拡張するために不可欠な一元的な可視性とAIによる洞察を提供しています。

ETRについて

ETRは、対象とするIT意思決定者のコミュニティから得た専有データを活用し、投資計画や業界トレンドに関するアクション可能なインサイトを提供するテクノロジー市場のリーディングファームです。2010年以来、ETRは1つの目標に向かって着実に実績を重ねています。すなわち、企業リサーチにおいて、不完全でバイアスのかかった、統計的に有意ではないデータから形成されることの多い意見の必要性を排除することです。ETRの扱うIT意思決定者のコミュニティは、業界で最高クラスの顧客／評価者の視点を提供できる独自のポジションを占めています。このコミュニティから得た専有データとインサイトは、機関投資家やテクノロジー企業、IT意思決定者が、拡張する市場における複雑な企業テクノロジーの展望を概観する上で、大きな役割を果たしています。

NEW RELICについて

New Relicのインテリジェントオブザーバビリティプラットフォームは、企業がデジタルエクスペリエンスにおける断絶を解消できるように支援します。New Relicはテレメトリデータを統合・関連し、デジタル資産の全体像を可視化できる唯一のプラットフォームです。当社は、適切なデータを適切なタイミングで処理して、価値を最大化し、コストを管理することで、問題解決を事前対応（プロアクティブ）から予測対応（プレディクティブ）へと移行させます。だからこそ、世界中の企業（Adidas Runtastic、American Red Cross、Domino's、GoTo Group、Ryanair、Topgolf、William Hillなど）がNew Relicを利用してイノベーションを推進し、信頼性を向上させ、優れた顧客体験を提供して成長に向けて邁進しています。

本レポートについて

このレポートのすべてのデータは、2025年オブザーバビリティ予測レポートの発行に向けた研究や取り組みの一環として行われた調査に基づいています。アジア太平洋地域は全回答者のうち575人（34%）を占めています。すべての金額は米ドルです。

© Copyright 2025, New Relic, Inc. 禁無断転載。本書で言及されたすべての商標および商号、サービスマーク、ロゴはそれぞれの所有者に帰属します。
2025年10月



New Relicのプラットフォームについて知る