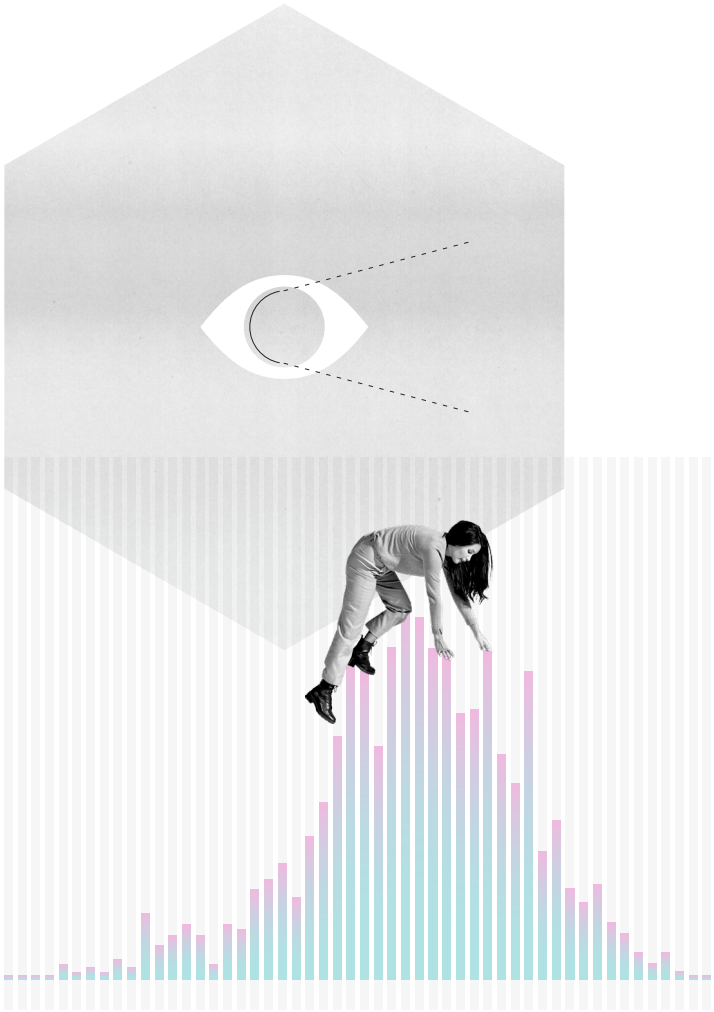
new relic

Observ–ability

FORECAST_2024

年次レポート/ 2024年

目次



エグゼクティブ・サマリー

*2024年オブザーバビリティ予測*は、オブザーバビリティの進化に関する洞察を提供し、主要な成長分野と停滞分野を特定し、外的要因がどのように導入と投資戦略を形成しているかを明らかにします。16カ国の1,700人の技術専門家の意見を取り入れたこの調査は、オブザーバビリティ業界で最大かつ最も包括的な調査です。

デジタルエクスペリエンスとビジネスの成長が企業の最重要課題となっている今、この調査結果は、オブザーバビリティの具体的なビジネス価値を浮き彫りにしています。ITプロフェッショナルは、自動化と障害への予防に対する賢明な投資を通じて主要業績評価指標（KPI）を管理しながら、計画外のダウンタイムを削減し、アップタイムを改善し、信頼性を高める方法を模索しています。このレポートによると、オブザーバビリティを優先する組織は、業務効率と全体的な業績に関して大きな優位性があることを示しています。

今年のデータでは、オブザーバビリティが投資収益率（ROI）において中央値で4倍のリターンをもたらすことが明らかになりました。フルスタックオブザーバビリティを実現している企業では、ダウンタイムが79%減少し、システム停止が48%削減されました。オブザーバビリティへのさらなる投資の必要性がこれまで以上に高まっています。

さらに、ビジネスオブザーバビリティ、つまりテレメトリーデータをビジネス成果とリアルタイムで関連付けることができる機能が最優先事項となっています。ビジネスオブザーバビリティを実現する機能を導入している組織は、そうでない組織と比較して、年間のダウンタイムが40%減少し、時間あたりのシステム停止コストが24%削減され、サービス中断への管理に費やす時間が25%短縮されています。

さらに、AI監視、機械学習（ML）モデル監視、ITオペレーション向けAI（AIOps）などの人工知能（AI）テクノロジーの導入の増加は、イノベーションをサポートする際のオブザーバビリティの重要性の高まりを反映しています。AI主導型オブザーバビリティを導入済みの組織は、全体的なビジネス価値とROIがより高いと報告されています。

要約すると、本レポートは、オブザーバビリティが単なる技術的な話ではなく、ビジネス成果を達成するための戦略的必須事項であることを裏付けています。オブザーバビリティに投資することで、組織はより信頼性の高いデジタル体験を確保し、運用効率を向上し、将来の成長に向けた準備を整えることができます。

主な調査結果

ビジネス影響が大きいシステム停止による年間のダウンタイムの中央値は77時間、1億4,600万ドルに相当

ビジネス影響が大きいシステム停止による年間の合計ダウンタイムの中央値は77時間（約3日）これを合計すると、年間のシステム停止コストの中央値は1億4,600万ドルになります。平均すると、回答者はエンジニアリングチームがサービス中断への対処に費やした時間の中央値を30%と推定しました。これは、週40時間労働とすると12時間に相当します。

フルスタックオブザーバビリティを実現している組織は、年間ダウンタイムが79%削減、毎年4,200万ドルを節約可能

平均すると、フルスタックオブザーバビリティを実現している企業は、実現していない企業に比べて年間ダウンタイムが79%減少し（338時間に対して70時間）、時間あたりのシステム停止コストが48%少なくなります（210万ドルに対して110万ドル）。また、ダウンタイムの短縮とコスト、その他いくつかの要因の間には強い関連性があります。

41%が、来年中にツール統合を予定していると回答

複数のポイントソリューションと比較して、単一の統合プラットフォームが2倍ほど多く優先されています。実際、単一ツールを使用している回答者の数は前年比（YoY）37%増加しました。また、ツールの平均数は前年比11%減少しました。45%が依然として5つ以上のツールを使用していますが、41%は来年中にツールを統合する予定であると回答しています。

オブザーバビリティROIの中央値は4倍、前年比の2倍

オブザーバビリティ年間支出の中央値は、すべての回答者の全体で195万ドルでした。ただし、オブザーバビリティから得られる年間価値の中央値は815万ドルで、ROIの中央値は4倍でした。つまり、ROI中央値が前年比の2倍から4倍に倍増しています。さらに、5つ以上のオブザーバビリティ関連機能を導入済みの企業は、4つ以下しか導入していない企業に比べて、オブザーバビリティへの投資から得られる年間価値とROIが高くなると予想されています。

ビジネスオブザーバビリティを実現する機能を導入している組織では、年間のダウンタイムが40%削減

ビジネス成果をテレメトリーデータと関連付け、リアルタイムでレポートする機能（ビジネスオブザーバビリティ）は、オブザーバビリティベンダーのもっとも重要な基準の1つであり、全体で3番目の選択肢でした。実際、40%がビジネスオブザーバビリティを実現する機能を導入済みでした。平均すると、ビジネスオブザーバビリティを実現する機能を導入済みの企業は、そうでない企業と比較して、年間のダウンタイムが40%減少し、時間あたりのシステム停止コストに費やす時間が24%削減され、サービス中断への対処に費やす時間が25%短縮されています。

組織はAIテクノロジーを十分に活用するためオブザーバビリティを導入している

AIテクノロジーの導入は、オブザーバビリティのニーズを促す戦略やトレンドのトップでした（41%）。約5人に2人（42%）がAI監視、29%が機械学習（ML）モデル監視、24%がAIOps機能を導入していました。注目すべき点は、これらの機能を導入した企業は、導入していない企業に比べて、オブザーバビリティから得られる年間合計価値がより高くなると予想されています。

オブザーバビリティの現状

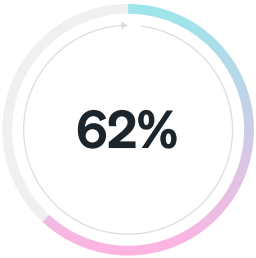
このセクションでは、導入の傾向、組織戦略、システム停止の影響、ダウンタイムのコスト、導入を促進する主な利点について説明します。

オブザーバビリティの現状は、より優れたビジネス成果を推進 するために テクノロジーへの投資を最適化 することがますます重要視されていることを反映しています。組織は、断片的な監視から、統合されたオブザーバビリティプラットフォームに移行しています。

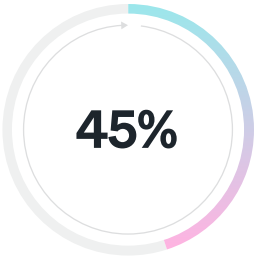
ほとんどの組織はまだフルスタックオブザーバビリティを実現していませんが、オブザーバビリティ関連機能の導入は前年比（YoY）で大幅に増加しました。さらに多くの組織がフルスタックオブザーバビリティに近づいているか、フルスタックオブザーバビリティを実現するようになっており、これがその可能性を最大限に引き出す鍵となります。

システム停止はまだ頻繁でコストがかかる問題ですが、より多くの技術スタックの監視、フルスタックオブザーバビリティの実現、そしてオブザーバビリティのベストプラクティスの実施により、組織はサービスレベル指標を改善し、実施した投資から最大限のビジネス価値を引き出しています。

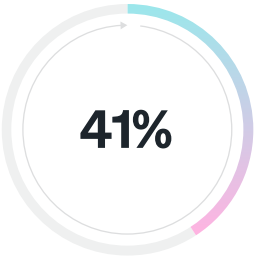
ハイライト：



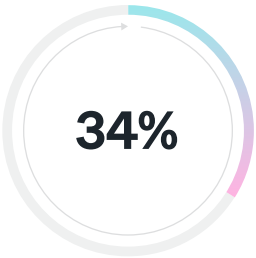
62%がビジネス影響が大きいシステム停止では、ダウンタイム1時間あたりのコストは100万ドル以上と回答



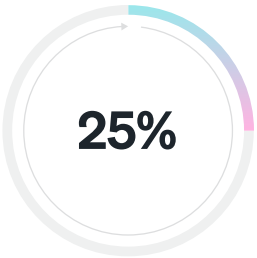
45%がオブザーバビリティに5つ以上のツールを使用



41%がAIテクノロジーの導入によりオブザーバビリティのニーズが高まっていると回答



34%がオブザーバビリティへの投資から年間1,000万ドル以上の価値を得ていると回答



25%がフルスタックオブザーバビリティを実現

導入の現状

このセクションでは、導入済みのオブザーバビリティ関連機能、機能に使用されたツールの数、オープンソースの使用状況、テレメトリーデータが統合されているかサイロ化されているか、どのような種類のデータがテレメトリーデータと統合されているか、導入済みのベストプラクティス、調査時のオブザーバビリティ年間支出、および回答者がオブザーバビリティを使用する頻度について説明します。

ハイライト：

67%
オブザーバビリティに年間で100万ドル以上を支出

51%
1つ以上のオブザーバビリティ関連機能にオープンソースソリューションを使用

45%
オブザーバビリティに5つ以上のツールを使用

導入済みのオブザーバビリティ関連機能

調査対象者は、19のオブザーバビリティ関連機能のうち、導入済みのものを回答してくれました。以下は、機能別、機能数別、フルスタックオブザーバビリティの実現に使用されている数別の調査結果です。

機能別

機能数別

フルスタックオブザーバビリティの実現に使用されている数別

機能別

調査回答者は、自社組織が、最多のもので58%（セキュリティ監視）、最小のもので24%（[AIOps]（ITオペレーション向け人工知能）を導入していることを示唆しています。

- 半数以上が、セキュリティ監視（58%）、ネットワーク監視（57%）、データベース監視（55%）、アラート（55%）、ダッシュボード（54%）、インフラストラクチャ監視（54%）、ログ管理（51%）、アプリケーションパフォーマンス監視（APM、50%）などの、主要なオブザーバビリティ関連機能を導入していました。
- 3分の1以上が、ブラウザ監視（44%）、エラー追跡（43%）、モバイル監視（35%）などの主要なデジタル顧客体験モニタリング（DEM）機能と、AIモニタリング（42%）とビジネスオブザーバビリティ（40%）を導入していました。
- AIOps機能（24%）、外形監視（26%）、ディストリビューティッド（分散）トレーシング（29%）、Kubernetes（K8）監視（29%）、機械学習（ML）モデル監視（29%）、サーバーレス監視（30%）など、より高度な機能をそれぞれ導入していたのは3分の1未満でした。

組織規模別の考察
大規模組織は、AIモニタリング、ビジネスオブザーバビリティ、サーバーレス監視を除くすべての機能を導入する傾向がもっとも高かった。

地域別の考察
アジア太平洋の回答者は、AIモニタリング、AIOps、外形監視を導入する傾向がより高かったが、他のすべての機能を導入する傾向はもっとも低かった。欧州の回答者は、ほとんどの機能を導入する傾向がもっとも高かった。

業界別の考察
IT業界の回答者は一般に、ほとんどの機能を導入する傾向が平均よりも高かった。メディア／エンターテイメントの回答者は、AI関連機能とDEM機能を導入する傾向がもっとも高かった。

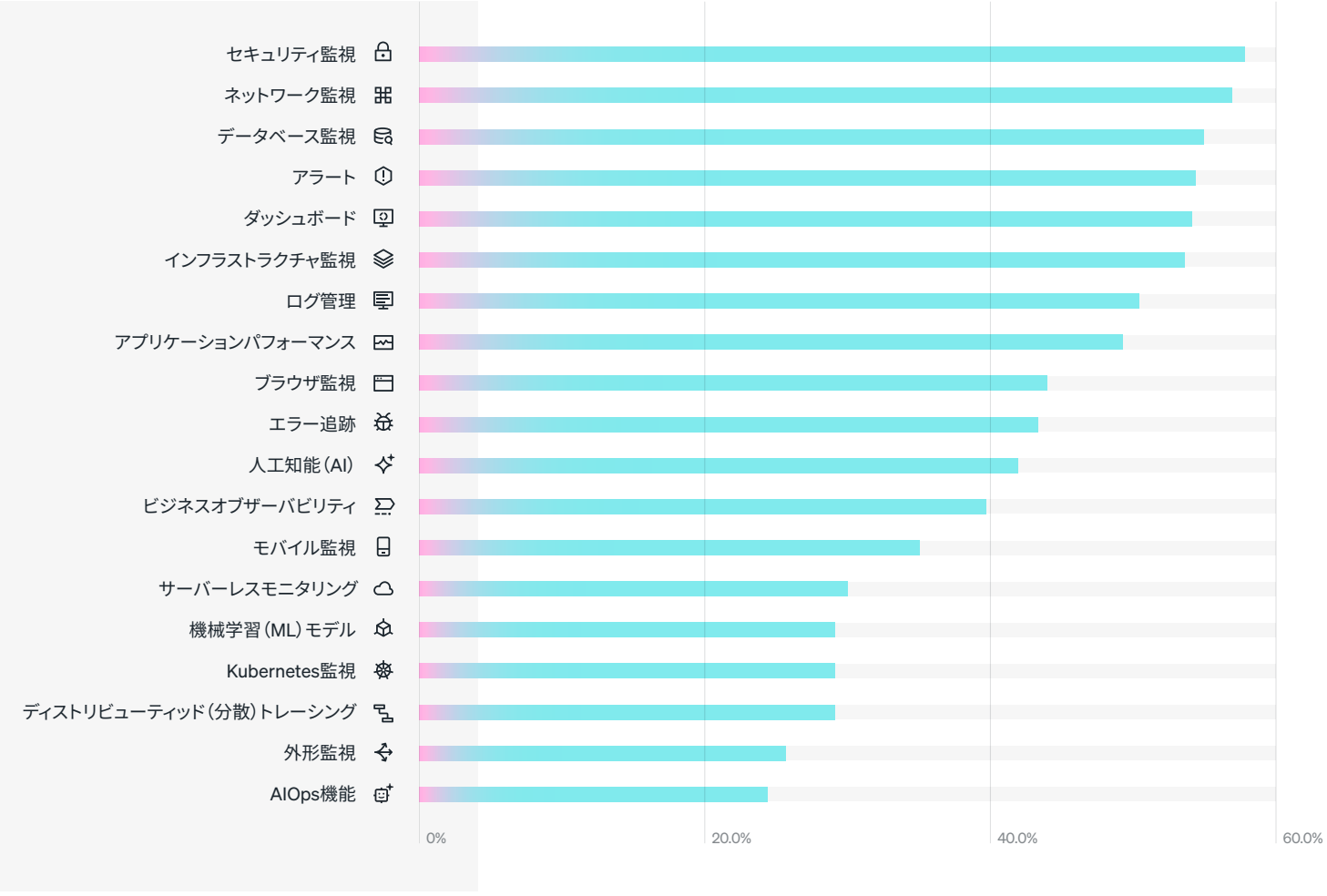


図01. 現状の導入機能

機能数別

調査対象者は、組織が平均8つの機能を導入していると回答しました。4分の3（75%）が5つ以上の機能を導入済みで、そのうち37%は10以上、10%は15以上でした。

組織規模別の考察
大規模組織では、10以上の機能を導入している割合がもっとも高い傾向にありました（40%、中規模組織で35%、小規模組織で27%）。

地域別の考察
欧州の回答者は、10以上の機能を導入している割合が最も高い傾向にありました（46%、南北アメリカで42%、アジア太平洋で29%）。

業界別の考察
IT業界の回答者は、10以上の機能を導入している割合がもっとも高い傾向にありました（53%、医療／製薬で48%、サービス／コンサルティングで43%）。

37%
10以上のオブザーバビリティ関連機能を導入済み

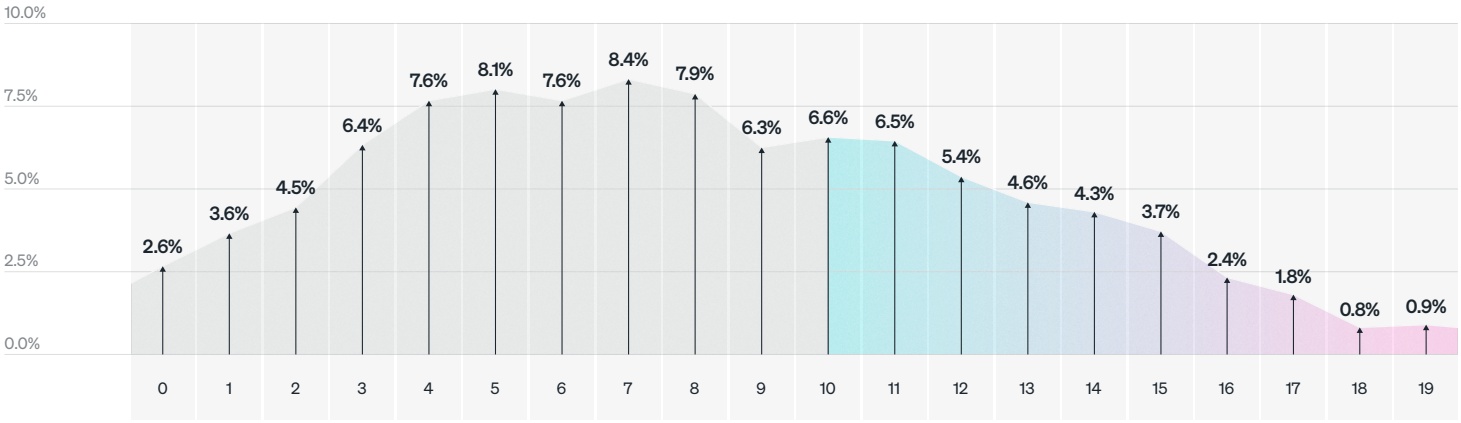


図02. 現在導入済みの機能数

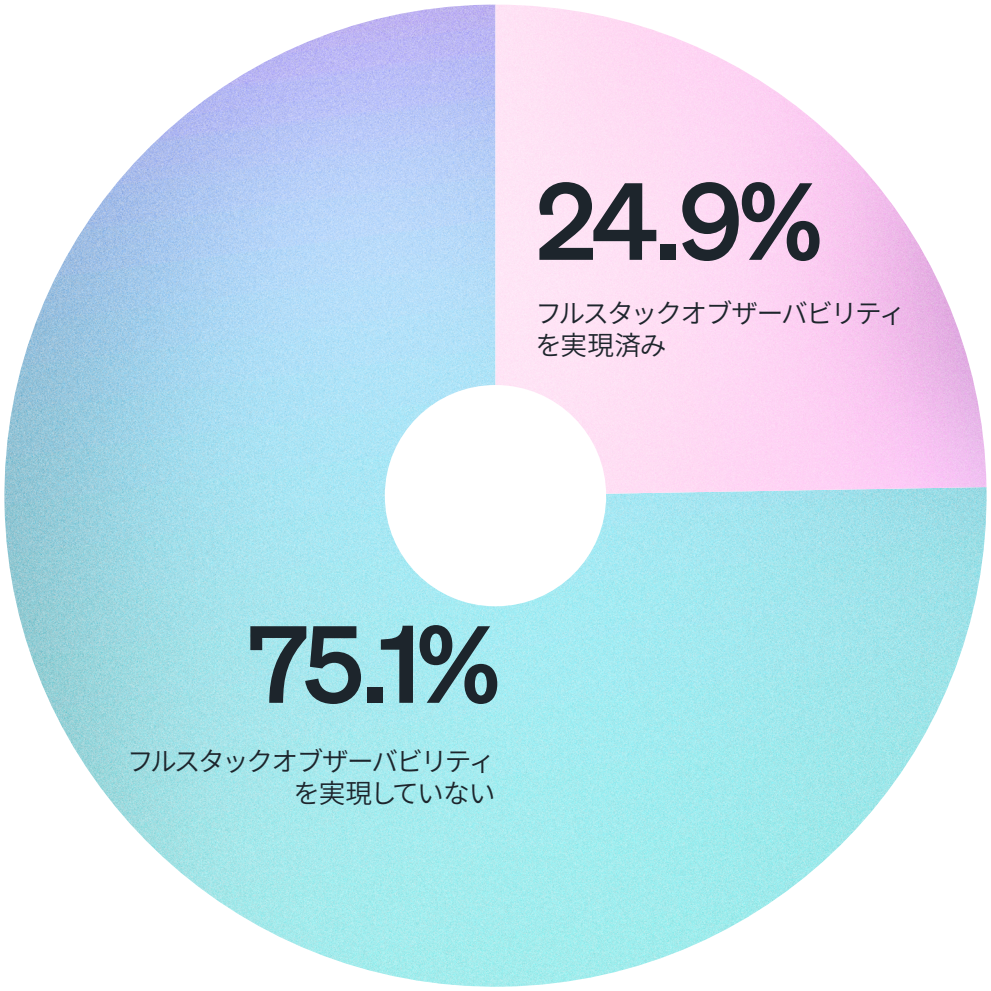
5つの以上の機能を導入済みの企業は、4つ以下を導入した企業に比べて、年間のダウンタイムが短く、年間のシステム停止にかかる費用も少なく、サービス中断への対処に費やす時間も平均より短くなる傾向がありました。

- **5以上の機能：**年間ダウンタイムの中央値が45%減少、サービス中断への対処に費やすエンジニアリング時間が24%短縮
- **10以上の機能：**年間ダウンタイムの中央値が74%減少、時間あたりのシステム停止コストの中央値が32%削減、サービス中断への対処に費やすエンジニアリング時間が41%短縮
- **15以上の機能：**年間ダウンタイムの中央値が80%減少、時間あたりのシステム停止コストの中央値が47%削減、サービス中断への対処に費やすエンジニアリング時間が39%短縮

より多くのオブザーバビリティ関連機能を導入することは、より優れたビジネス成果につながります。

フルスタックオブザーバビリティの普及

フルスタックオブザーバビリティの定義に基づくと、4分の1（25%）の調査対象者がこれを実現しています。



組織規模別の考察
フルスタックオブザーバビリティの実現がもっとも高いのは大規模組織で27%、中規模組織で23%、小規模組織は20%でした。

地域別の考察
欧州の回答者はフルスタックオブザーバビリティの実現がもっとも高い傾向にありました（32%、アジア太平洋29%、南北アメリカ28%）。

業界別の考察
IT業界の回答者は、フルスタックオブザーバビリティの実現がもっとも高い傾向にありました（35%、医療／製薬34%、サービス／コンサルティング31%）。教育業界の回答者は、フルスタックオブザーバビリティの実現がもっとも低い傾向にありました（11%、テレコミュニケーション34%、エネルギー／ユーティリティ15%、政府機関15%）。

図03. フルスタックオブザーバビリティを実現した、または実現しなかった2024人の回答者の割合

特に、フルスタックオブザーバビリティを実現した組織は、実現していない組織と比べて、年間ダウンタイムの中央値が79%減少、時間あたりのシステム停止コストの中央値が48%削減、サービス中断への対処に費やす時間が44%短縮しました。また、オブザーバビリティの年間支出も27%減少、オブザーバビリティを使用した中断を検知する可能性がもっとも高い傾向にありました（51%）。オブザーバビリティに関するベストプラクティスをすべて導入し、ほとんどの利点やビジネス成果を得る可能性がもっとも高い傾向にありました。

フルスタックオブザーバビリティを実現した企業は、通常、より多くのベストプラクティスを導入し、より優れたビジネス成果を得ています。

監視ツール数

システムの健全性を監視するために使用しているツール数を尋ねました。圧倒的多数の調査対象者は複数のツールを使用している、と回答しました。

- ほとんどの回答者（88%）が複数のツールを使用しており、そのうち45%が5つ以上のツールを使用していました（2023年52%、2022年73%）、10以上のツールを使用していたのは3%でした。
- 使用されたツールの平均数は4.5で、2023年（5.1）より11%減少し、2022年（5.9）より24%減少しました。同様に、ツール数の中央値は、2022年で6、2023年で5、2024年には4つになりました。2024年のもっとも一般的な回答（最頻値）はツール3つ（18%）で、次にツール5つ（15%）でした。
- 1つのツールだけを使用していたのはわずか6%でした。ただし、単一のツールを使用している回答者の割合は前年比（YoY）37%増加しました。

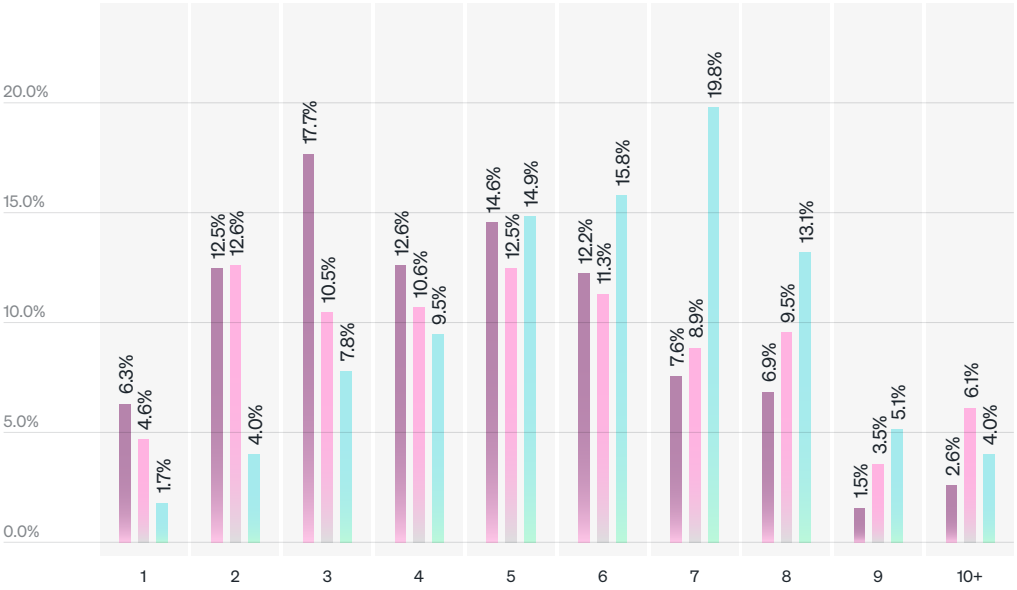


図04. オブザーバビリティの実現のために使用されるツール数、2022、2023、2024年の比較

2024年の回答者
2023年の回答者
2022年の回答者

組織規模別の考察

小規模組織では、中規模組織（7%）、大規模組織（4%）よりも1つのツール（17%）を使用する傾向がきわめて高く、大・中規模の組織では、5つ以上のツールを使用する傾向が多く見られました（小規模組織でわずか26%に対し、両方で47%）。

地域別の考察

欧州の回答者は、単一のツールを使用する傾向がもっとも高く（南北アメリカとアジア太平洋の回答者は6%に対し8%）、アジア太平洋の回答者は、5つ以上のツールを使用する傾向がもっとも高く見られました（55%、欧州では43%、アメリカでは35%）。

業界別の考察

医療／製薬の回答者は、単一のツールを使用する傾向がもっとも高く（13%）、次に教育業界（10%）、エネルギー／ユーティリティ（9%）でした。メディア／エンターテイメントの回答者は、5つ以上のツールを使用する傾向がもっとも高く（60%）、次に金融サービス／保険（57%）、テレコミュニケーション（55%）でした。

45%がオブザーバビリティに5つ以上のツールを使用

オブザーバビリティ性能に複数のツールを使用している場合と比較して、単一のツールを使用すると以下の利点があります。

- オブザーバビリティの年間支出の中央値で65%削減（200万ドルに対して70万ドル）
- 年間ダウンタイムの中央値で18%削減（年間305時間に対して249時間）
- 時間あたりのシステム停止コストの中央値で45%削減（1時間あたり200万ドルに対して110万ドル）
- サービス中断への対処に費やすエンジニアリング時間が50%削減（週40時間労働に基づく13時間に対して7時間）

ここ数年に渡って、使用するツール数が減少する傾向が明らかです。41%が来年中にツールを統合する予定であると回答しているため、この傾向は続くと予想されます。

オープンソースの使用状況

上記19のオブザーバビリティ関連機能のそれぞれについて、独自のソリューションに加えてオープンソースソリューションを使用しているかどうかを調査回答者に尋ねたところ、以下のことがわかりました。

- 回答者の半数以上（51%）が、1つ以上のオブザーバビリティ関連機能にオープンソースソリューションを使用していました。ただし、*オープンソースのみ*を使用していたのはわずか約1%でした。
- 調査に含まれた3つのオープンソースソリューションのうち、1つ以上のオブザーバビリティ性能にGrafana（38%）、Prometheus（23%）、OpenTelemetry（19%）を使用していました。
- 4分の1以上が、AIモニタリング（31%）、外形監視（28%）、ディストリビューティッド（分散）トレーシング（28%）、K8モニタリング（27%）、APM（27%）、AIOps機能にオープンソースソリューション（26%）を使用していました。

組織規模別の考察

大規模組織では、1つ以上のオブザーバビリティ関連機能の実装にオープンソースソリューションの使用がもっとも高い傾向にありました（55%、中規模組織で46%、小規模組織で39%）。

地域別の考察

また、アジア太平洋の回答者は、1つ以上のオブザーバビリティ関連機能の実装にオープンソースソリューションの使用がきわめて高い傾向にありました（61%、南北アメリカ44%、欧州42%）。

業界別の考察

政府機関の回答者は、1つ以上のオブザーバビリティ関連機能の実装にオープンソースソリューションの使用がもっとも高い傾向にありました（65%、テレコミュニケーション65%、金融サービス／保険61%）。サービス／コンサルティングの回答者がもっとも低い傾向にありました（37%、エネルギー／ユーティリティ43%、医療／製薬45%）。

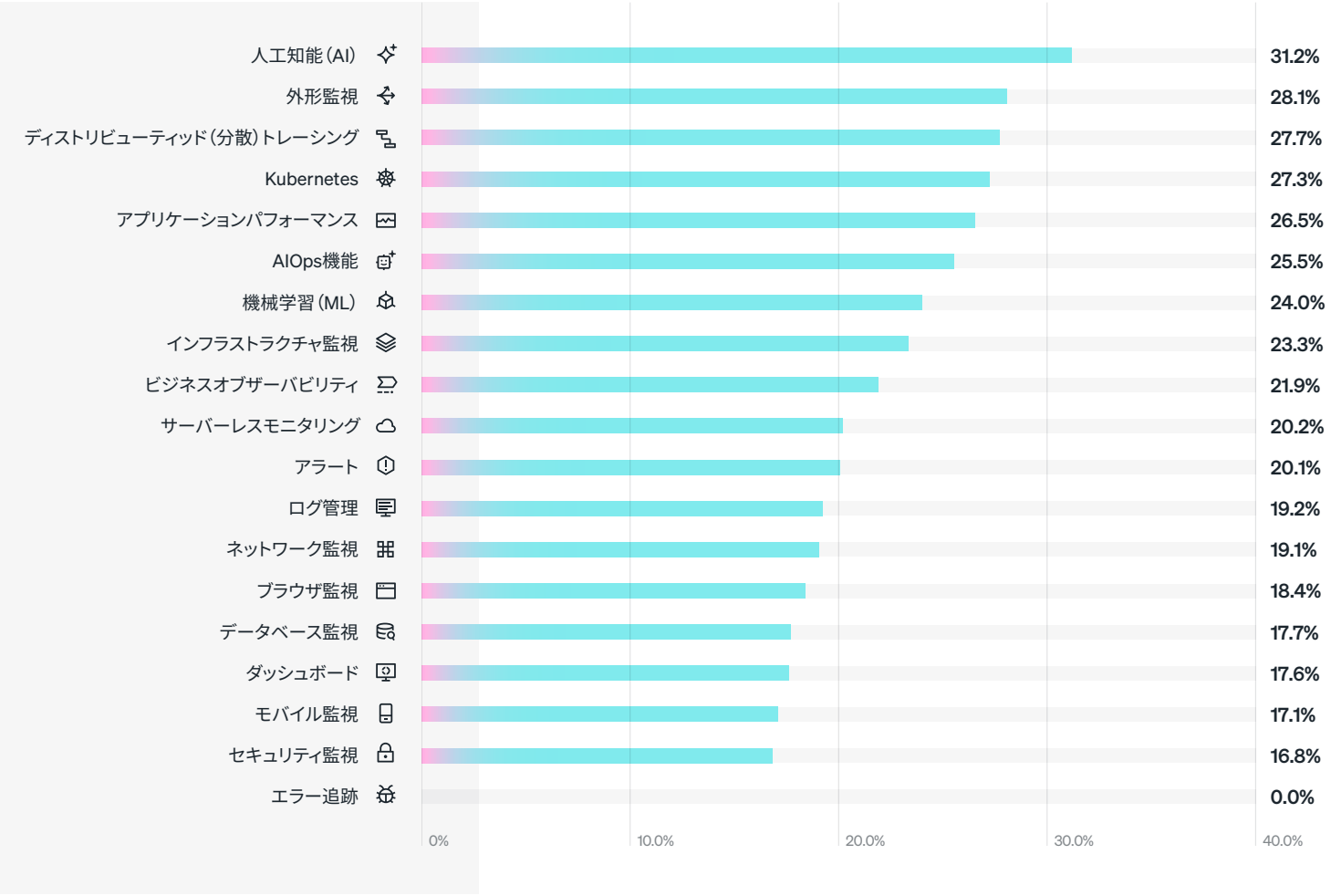


図05. オブザーバビリティの実現に使用されるオープンソースソリューション

51%

1つ以上のオブザーバビリティ関連機能の実装にオープンソースソリューションを使用していました。ただし、オープンソースのみを使用していたのはわずか約1%でした。

回答者は、オブザーバビリティベンダーのもっとも重要な基準としてオープンソースのサポート（移植性）を選択する可能性がもっとも低く（16%）、オープンソース技術の導入がオブザーバビリティの必要性を促進する戦略または傾向であると回答したのは21%のみでした。しかし、24%はオブザーバビリティへの投資からの価値を最大化するために、来年はオープンソースを使用する可能性がもっとも高いと回答しました。

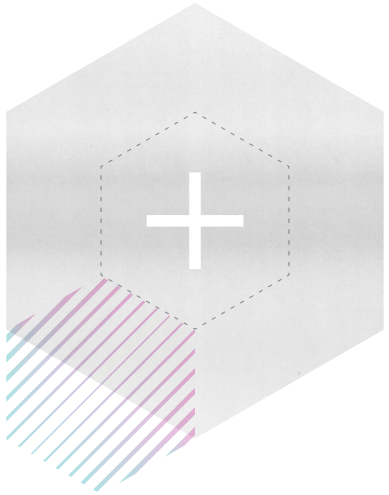
多くの組織は、ライセンスコストをかけずに、活発なコミュニティによる広範な導入とサポートの恩恵を受けるために、オブザーバビリティにオープンソースソリューションの使用を開始しています。ただし、ほとんどの場合、オープンソースと独自のオブザーバビリティソリューションを併用しています。

もっともよく使われるオープンソースソリューションは、そのソリューションが市場に登場してからの期間と主な機能に関連しています。

たとえば、ダッシュボードソリューションでよく知られているGrafanaは、もっとも使用されているオープンソースソリューションで、もっとも長く（2014年から）使用されています。

2番目に使用されているのはPrometheus（ユビキタスな時系列データベースおよびメトリクス監視ツール）で、2016年から使用されています。

また、OpenTelemetry（テレメトリーデータを収集し、独自のオブザーバビリティソリューションや視覚化ツールにエクスポートする一連のAPI、SDK、ツール）は、最新（2019年から）であまり使用されていませんが、オープンソーステレメトリーの標準プロトコルになるにつれて、大幅な成長と導入が見られます。



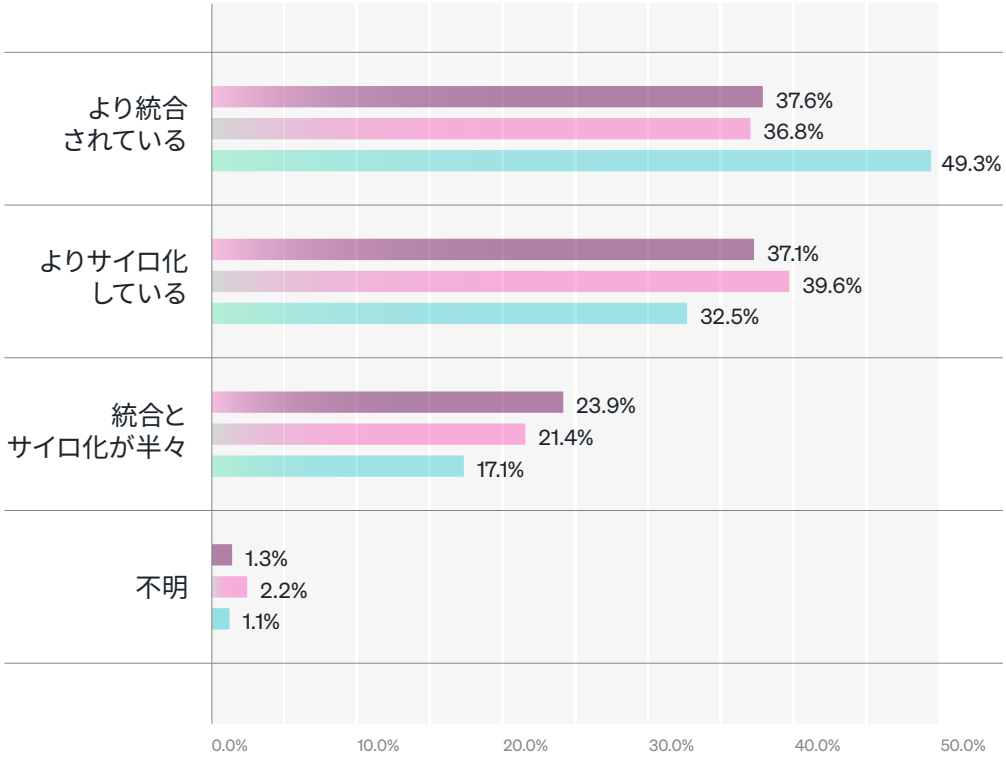
「業界はeBPFやOpenTelemetryタイプのアプローチに移行しているため、私はより多くのオープンソース技術を管理しています。ただし、そのためにはコレクターを使用する必要があります。OpenTelemetryのコレクターとしてNew Relicを使用していますが、New RelicではAIOps機能も提供してくれます。」

ITインフラストラクチャ担当シニアディレクター
米国の大手フィンテック企業

テレメトリーデータの統合とサイロ

調査対象者に、組織のテレメトリーデータ（MELT: メトリクス、イベント、ログ、トレース）がどのように統合、またはサイロ化されているかについて尋ねました。回答は以下の通りです。

- 全体として、38%がより統合されたテレメトリーデータ（2023年から2%増）、対して37%がよりサイロ化されたテレメトリーデータ（2023年から6%減）を保持しており、大まかに二分されている
- 12%がほぼ統合されたテレメトリーデータ（テレメトリーデータを1か所に統合）、対して11%がほぼサイロ化されたテレメトリーデータ（テレメトリーデータを個別のデータストアに分割して置いている）と回答
- 約4分の1（24%）は、テレメトリーデータは統合とサイロ化がおよそ半々と回答（2023年から12%増）



5つ以上のツールを使用している回答者は、1〜4つのツールを使用する回答者（57%）に比べて、ある程度サイロ化されたテレメトリーデータを保持している、と回答する傾向が13%多く見られました（64%）

平均して、よりサイロ化されたテレメトリーデータを持つ回答者と比較して、より統合されたテレメトリーデータを持つ回答者には以下の利点があります。

- 年間ダウンタイムで78%削減（年間488時間に対して107時間）
- サービス中断への対処に費やすエンジニアリング時間が11%削減（32%に対して28%）
- ROIの中央値が4%向上（290%に対して302%）

組織規模別の考察
大規模組織では、サイロ化されたテレメトリーデータがもっとも多い傾向にありました（38%、中規模組織で37%、小規模組織で33%）。

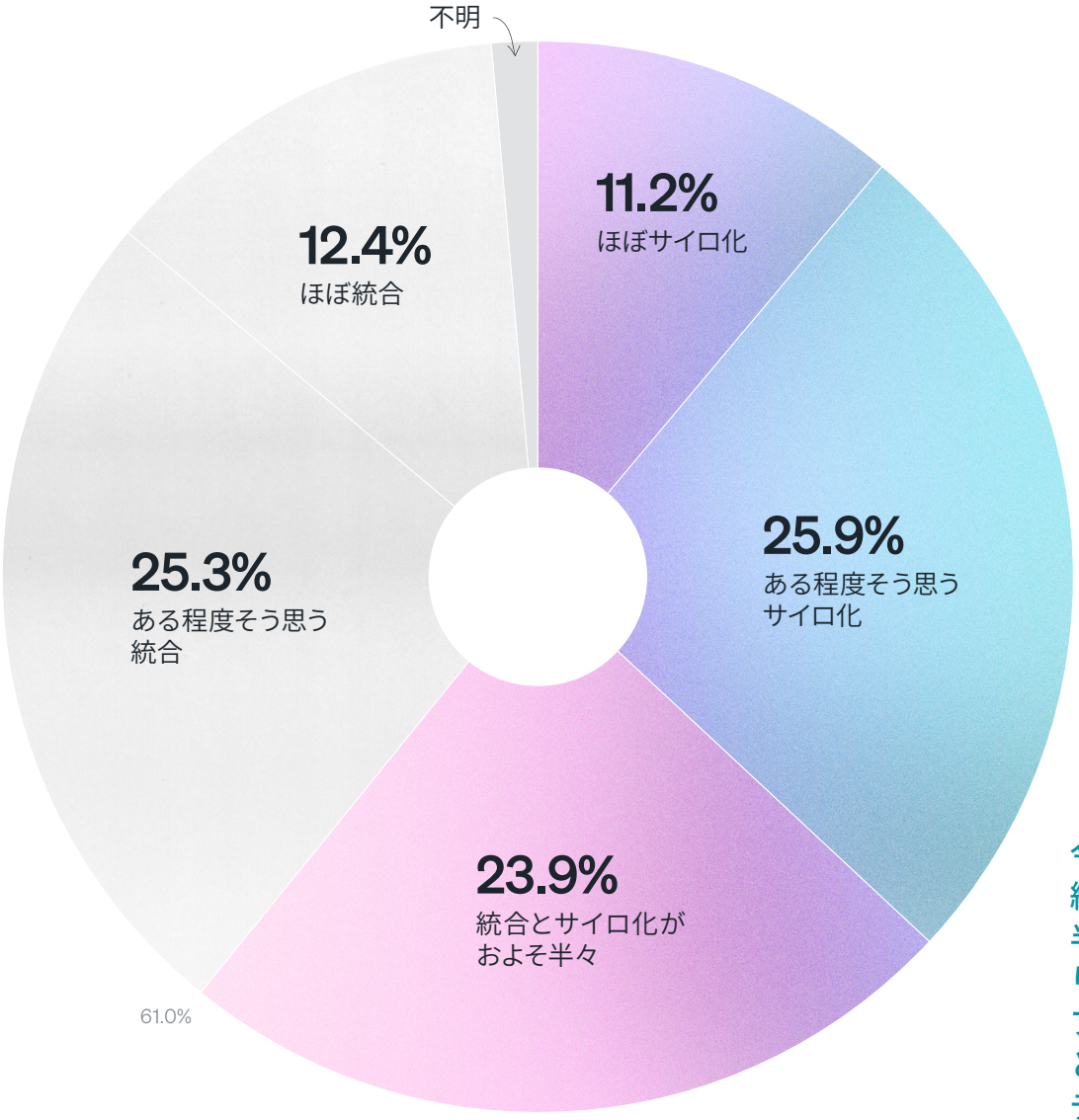
地域別の考察
アジア太平洋の回答者は、欧州（39%）や南北アメリカ（30%）よりもサイロ化されたテレメトリーデータ（42%）が多いと報告されています。

業界別の考察
サイロ化されたテレメトリーデータの割合がもっとも高い業界は、政府機関（53%）、メディア／エンターテイメント（47%）、教育（45%）でした。統合テレメトリーデータの割合がもっとも高い業界は、テレコミュニケーション（53%）、小売／消費者（52%）、サービス／コンサルティング（41%）でした。

図06. テレメトリーデータの統合vsサイロ化、2022、2023、2024年の比較

2024年の回答者
2023年の回答者
2022年の回答者

61%
自社のテレメトリーデータはある程度サイロ化していると回答



今年、テレメトリーデータは統合とサイロ化がおよそ半々です。このデータは、より多くのツールを使用してオブザーバビリティを高めることと、よりサイロ化されたデータを保持することとの間に関連性を示しています。また、より統合されたデータがダウンタイムの減少やROIの向上など、より望ましいビジネス成果につながることも示唆しています。

図07. 2024年にテレメトリーデータを統合

データの統合

真のビジネスオブザーバビリティを実践するには、組織はビジネス関連データをテレメトリーデータ（MELT）と統合する必要があります。ビジネス関連データの種類を確認したところ、現在統合されているのは以下のとおりと報告されています。

- ほとんど（87%）が1つ以上のビジネス関連データの種類をテレメトリーデータと統合していました。2つ以上の統合は77%、5つ以上の統合は35%でした。10のデータすべてを統合していたのはわずか4%でした。
- 統合される可能性がもっとも高かったのは、運用データ（43%）と顧客データ（41%）でした。
- 統合される可能性がもっとも低かったのは、製品研究と人事データ（両方32%）でした。

地域別の考察

欧州の回答者は、5種類以上のビジネス関連データをテレメトリーデータと統合する傾向がもっとも高くなっています（39%に対し、南北アメリカとアジア太平洋の両方で34%）。

業界別の考察

IT回答者は、テレメトリーデータと統合された5種類以上のビジネス関連データを保持している可能性がもっとも高くなっています（47%、メディア／エンターテイメント41%、医療／製薬38%）。教育業界の回答者がもっとも低い傾向にありました（19%、エネルギー／ユーティリティ25%、政府機関27%）。

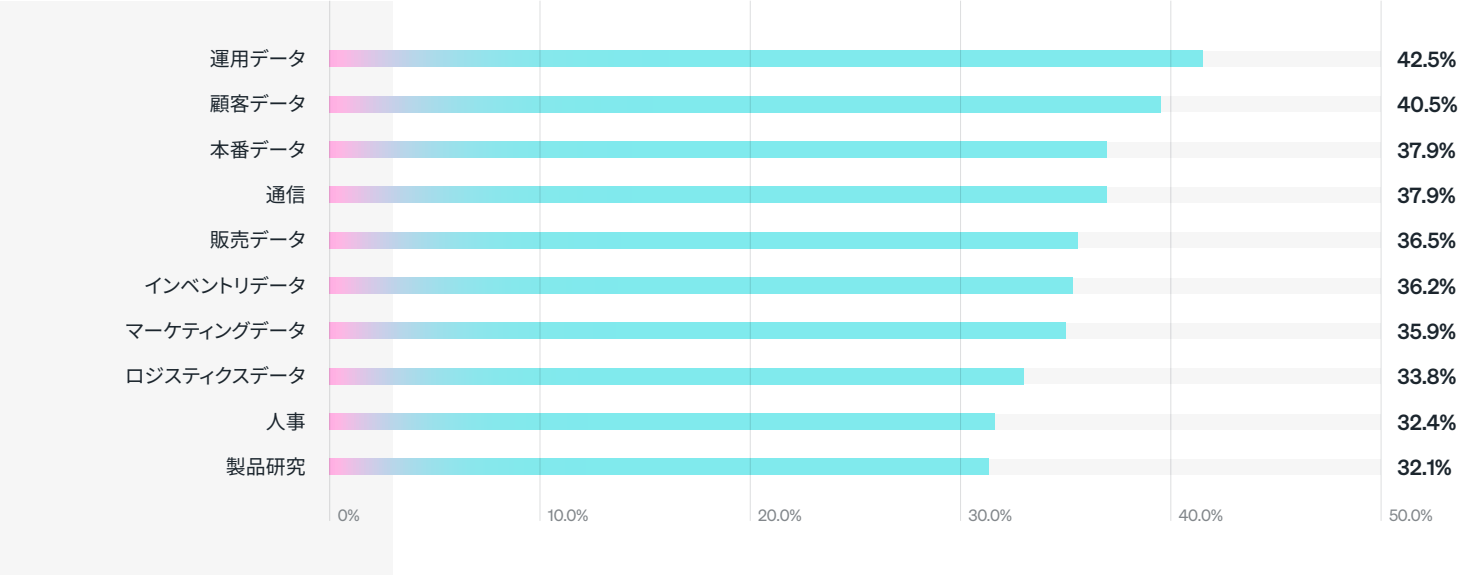


図08. 現在のテレメトリーデータと統合されているビジネス関連データの種類

現在テレメトリーデータと統合されているビジネス関連データの種類が5つ未満である企業と比較して、5つ以上を統合している企業では以下のメリットがありました。

- 時間あたりのシステム停止コストが32%削減（220万ドルに対して150万ドル）
- 年間ダウンタイムが63%削減（370時間に対して139時間）
- サービス中断への対処に費やすエンジニアリング時間が27%削減（週40時間労働に基づく15時間に対して11時間）

35%
5種類以上のビジネス関連データをテレメトリーデータと統合

ITエキスパートは、ビジネス成果に対する現実世界の影響（ビジネスオブザーバビリティ）をより深く理解するために、テレメトリーデータを使用することの重要性を認識しています。

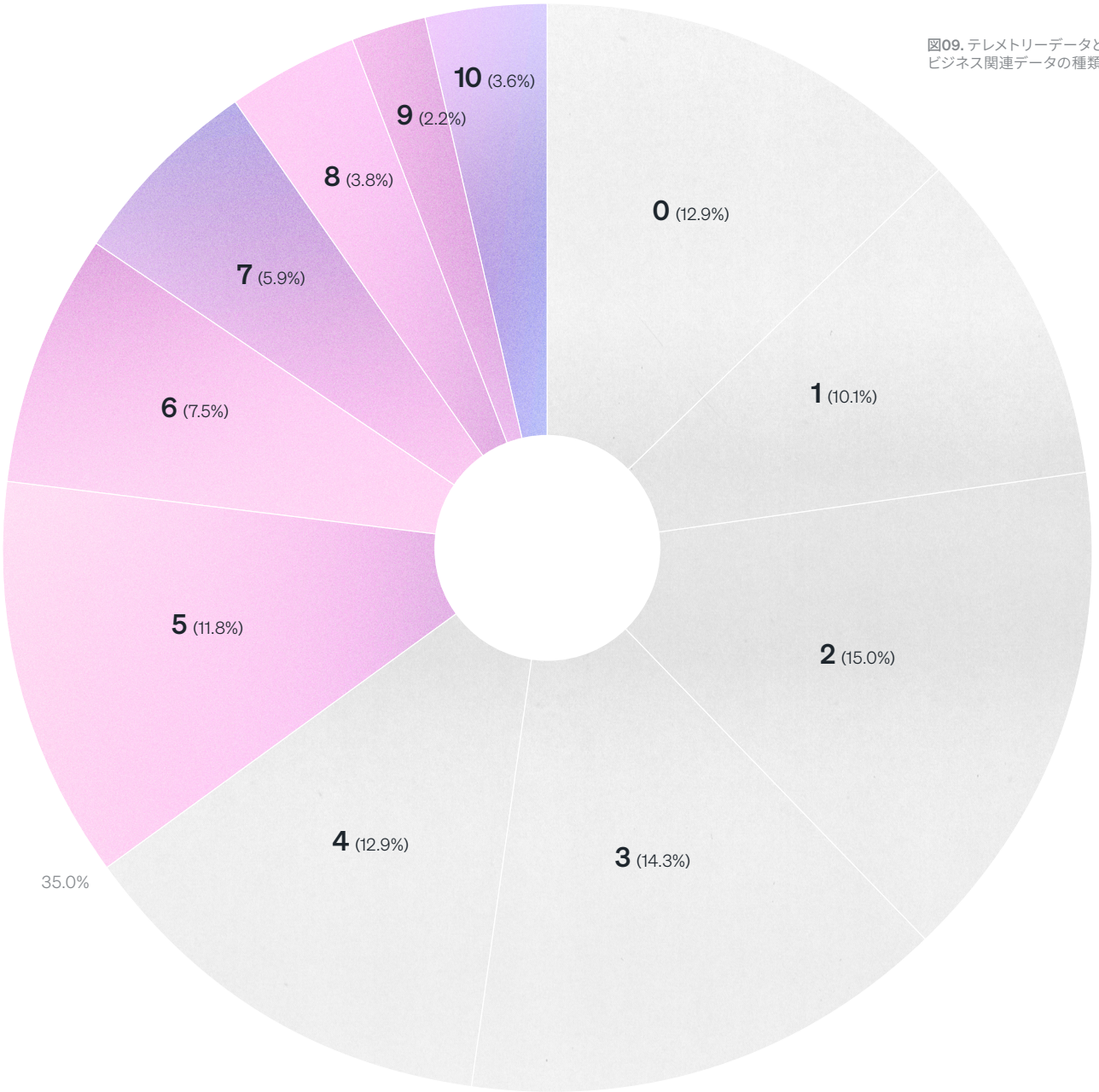


図09. テレメトリーデータと統合されているビジネス関連データの種類の数

導入済みのベストプラクティス

調査回答者に、再度以下の表にリストされている9つの異なるオブザーバビリティのベストプラクティスのうち、どれを導入済みかと尋ねました。結果は以下の通りです。

- ほとんどの回答者（83%）が2つ以上のベストプラクティスを導入していましたが、5つ以上の企業は16%だけでした。
- 回答者は、自社のソフトウェア導入にはCI/CDプラクティスを使用（40%）、自動化ツールを使用してプロビジョニングおよびオーケストレーションされているインフラストラクチャを使用（39%）と回答する傾向がもっとも高かったものの、その傾向は前年に比べて低くなりました。
- 昨年と比較して、テレメトリーデータにはイベントやインシデントのビジネスへの影響を定量化するための豊富なメタデータとビジネスコンテキストが含まれていると回答（24%増）、ユーザーがテレメトリーデータと視覚化に広くアクセスできると回答（18%増）、テレメトリーデータが複数チームで使用できる単一ペインに統合されていると回答（13%増）、テレメトリーが技術スタック全体にわたってキャプチャされていると回答（8%増）、柔軟にデータをクエリできると回答（2%増）しました。

組織規模別の考察

小規模組織は、5つ以上のベストプラクティスを導入済み（24%）と回答する傾向が、大規模組織（17%）、中規模組織（11%）に比べて高くなりました。

地域別の考察

南北アメリカの回答者（21%）は、アジア太平洋（13%）、欧州（12%）に比べ、5つ以上のベストプラクティスを導入済みとの回答がもっとも多い傾向にありました。

業界別の考察

サービス／エンターテイメントの回答者は、5つ以上のベストプラクティスを導入済みの傾向がもっとも多い傾向にありました（23%、金融サービス／保険21%、医療／製薬20%）。

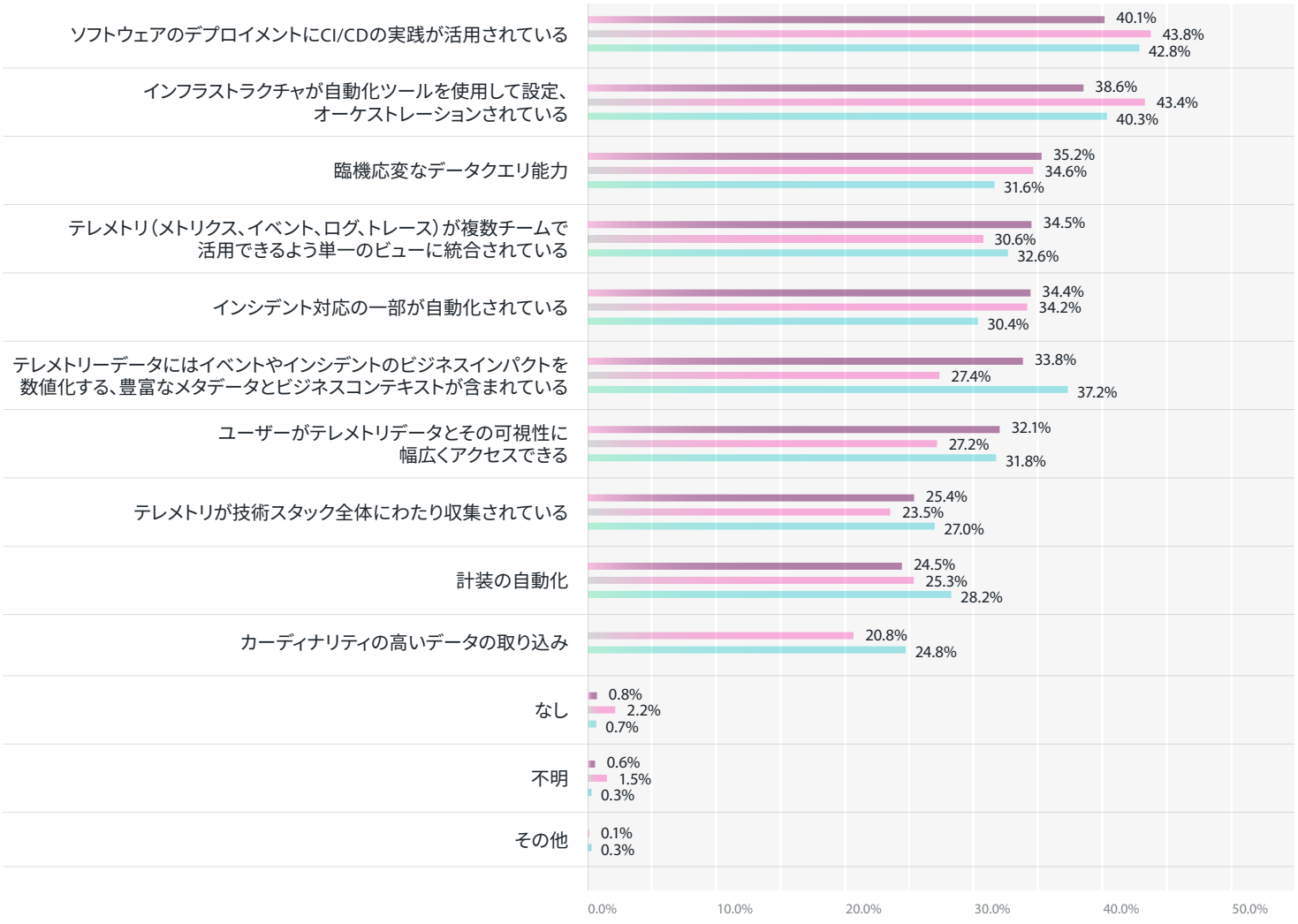
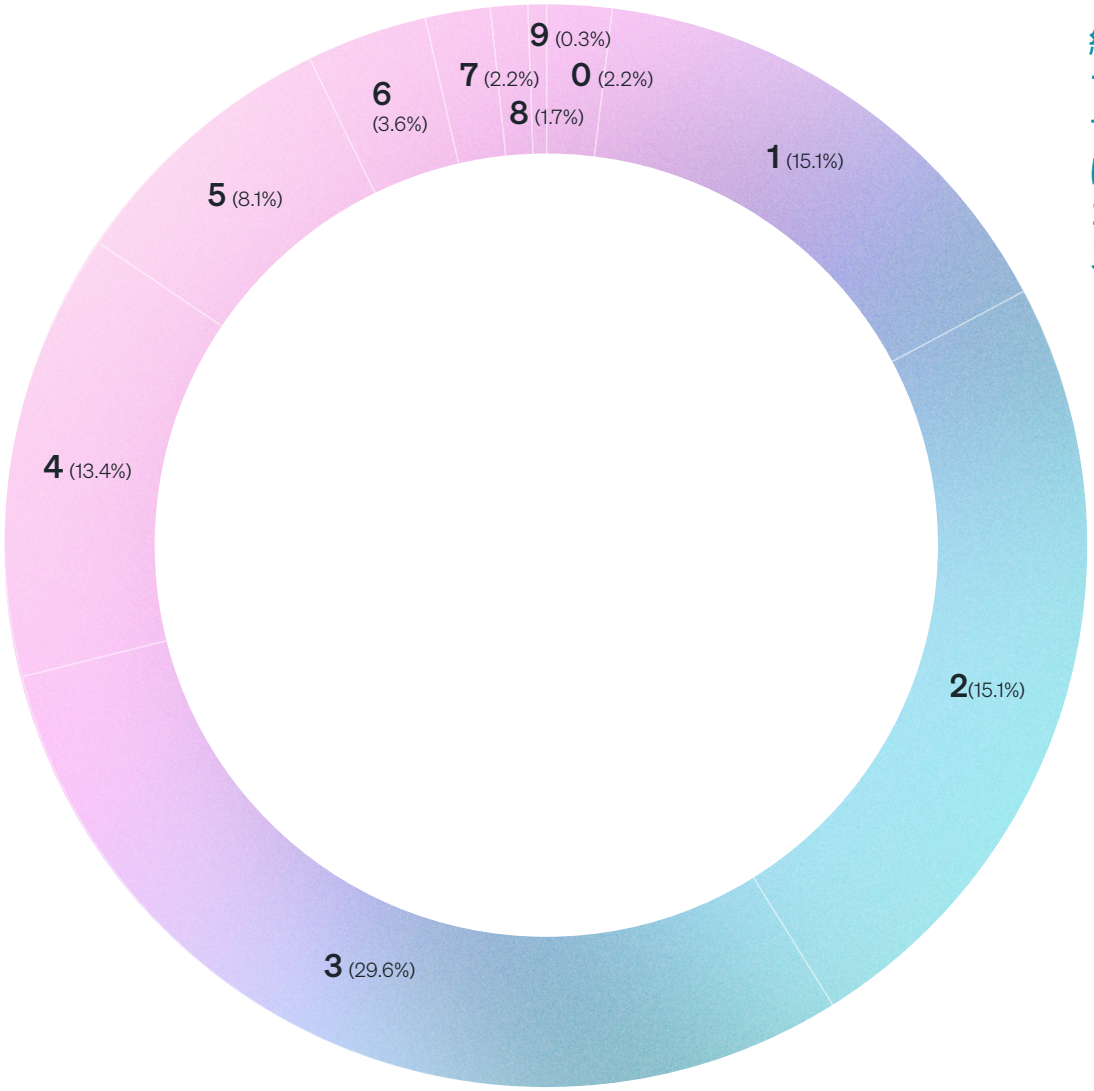


図10. 導入済みのベストプラクティス

平均して、1 ～4つを導入済みの企業と比較して、5つ以上のオブザーバビリティのベストプラクティスを導入済みの企業の利点は以下のとおりです。

- 年間ダウンタイムが19%削減 (294時間に対して239時間)
- 時間あたりのシステム停止コストが35%削減 (200万ドルに対して130万ドル)
- サービス中断への対処に費やすエンジニアリング時間が38%削減 (34%に対して21%)
- オブザーバビリティソリューションを導入してからMTTDがある程度改善したと回答 (53%に対して72%)
- オブザーバビリティソリューションを導入してからMTTRがある程度改善したと回答 (56%に対して77%)
- オブザーバビリティに対する年間支出が20%削減 (200万ドルに対して160万ドル)



組織は、さらに多くのベストプラクティスの導入を検討する必要があります。これは、ダウンタイムの短縮やコストの削減など、ビジネス成果の向上に大きく関係しているからです。

図11. 2024年に導入されたオブザーバビリティのベストプラクティスの数

オブザーバビリティの年間支出

オブザーバビリティへの年間支出の中央値は**195万ドル**でした。3分の2以上（67%）がオブザーバビリティに年間少なくとも100万ドルを費やしており、500万ドル以上を費やしているのはわずか2%でした。年間支出額が50ドル未満だったのはわずか13%でした（縦軸は回答企業の年間収益となります）。

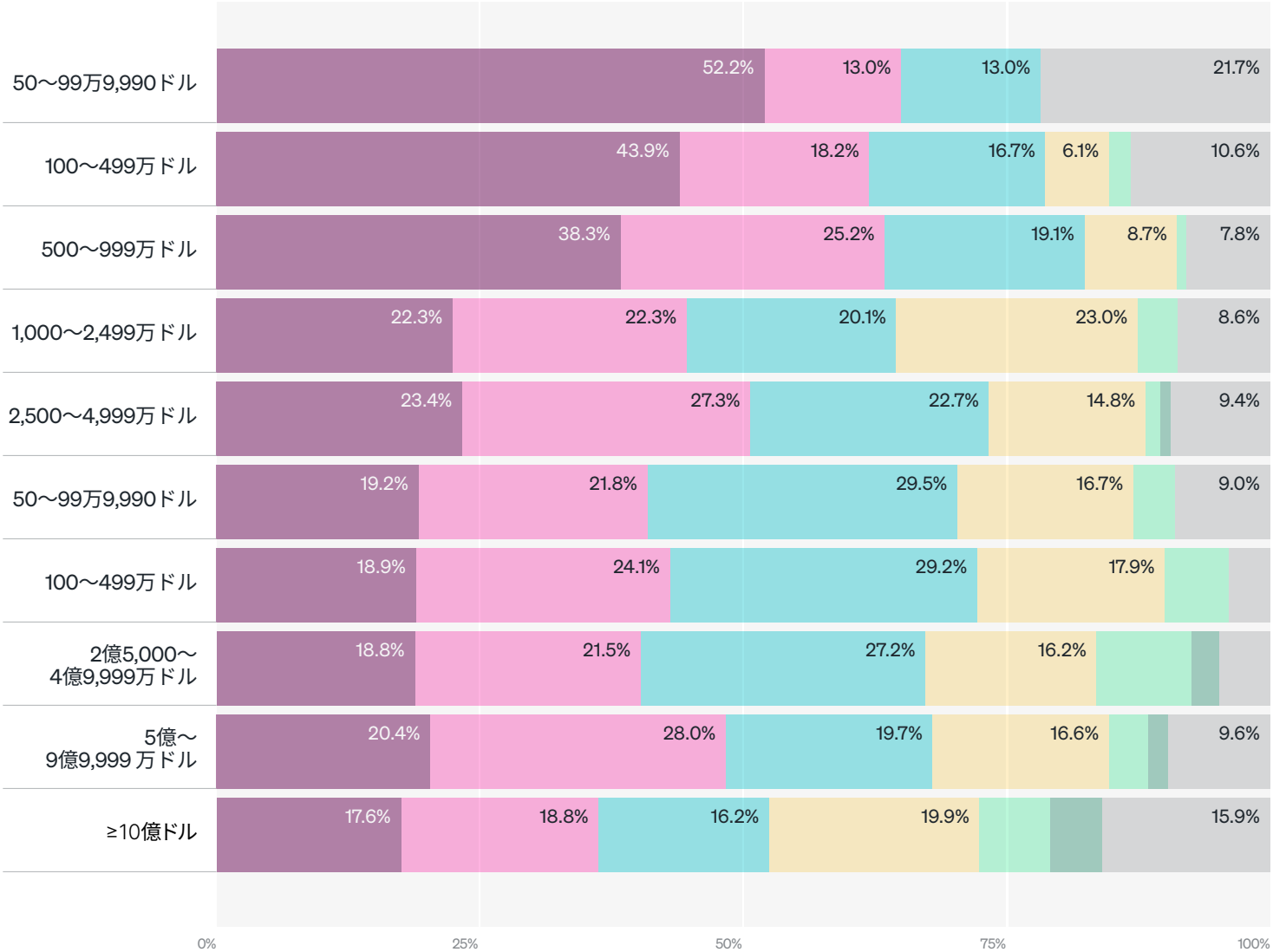


図12. 年間収益別のオブザーバビリティの年間支出

- <100万ドル
- <100万ドル〜199万ドル
- <200万ドル〜299万ドル
- <300万ドル〜399万ドル
- <400万ドル〜499万ドル
- ≥500万ドル
- 不明

67%
オブザーバビリティに年間で100万ドル以上を支出している

次の7つの要因がオブザーバビリティ年間支出の中央値の低下に関連していました。

- ✓ **オブザーバビリティに1つのツールを使用：**オブザーバビリティに1つのツールを使用している企業は、2つ以上のツールを使用している企業に比べて、オブザーバビリティに対する支出が67%少なくなりました（200万ドルに対して70万ドル）。
- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、オブザーバビリティに費やす費用が減少します。たとえば、5つ以上のオブザーバビリティ関連機能を導入した企業は、4つ以下の企業に比べて、オブザーバビリティへの年間支出が13%少なくなりました（218万ドルに対して190万ドル）。10個以上のオブザーバビリティ関連機能を導入した企業は、9個以下の企業に比べて、オブザーバビリティへの年間支出が30%少なくなりました（215万ドルに対して150万ドル）。
- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現している組織は、フルスタックオブザーバビリティを実現していない組織に比べ、オブザーバビリティへの年間支出額が27%少なくなりました（205万ドルに対して150万ドル）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した企業は、検知していない企業に比べて、オブザーバビリティへの年間支出額が23%少なくなりました（220万ドルに対して170万ドル）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、オブザーバビリティへの年間支出額が20%少なくなりました（200万ドルに対して160万ドル）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、オブザーバビリティへの年間支出額が10%少なくなりました（205万ドルに対して185万ドル）。
- ✓ **より統合されたテレメトリーデータの保持：**より統合されたテレメトリーデータを保持している企業は、よりサイロ化されたテレメトリーデータを保持している企業に比べて、オブザーバビリティへの年間支出額が5%少なくなりました（200万ドルに対して190万ドル）。

組織規模別の考察
予想通り、大規模組織では、中規模組織（185万ドル）や小規模組織（65万ドル）よりも高い支出の中央値（220万ドル）を報告しています。

地域別の考察
アジア太平洋の回答者は、欧州（175万ドル）や南北アメリカ（130万ドル）よりも高い支出の中央値（250万ドル）を報告しています。

業界別の考察
メディア／エンターテイメントの回答者は、オブザーバビリティの年間支出の中央値がもっとも高い（260万ドル）、次に金融サービス／保険（250万ドル）、テレコミュニケーション（235万ドル）。教育業界の回答者は支出額がもっとも低い（100万ドル）、次に医療／製薬（120万ドル）、サービス／コンサルティング（140万ドル）。

より多くの技術スタックを監視し、オブザーバビリティのベストプラクティスをより多く導入し、オブザーバビリティに単一のツールを使用し、オブザーバビリティにより中断を検知している企業は、実際にはオブザーバビリティに費やす費用が少なくなります。

戦略と組織

このセクションでは、単一の統合プラットフォームまたは複数ポイントソリューションの優先順位、オブザーバビリティベンダーまたはソリューションを選択する際のもっとも重要な基準、オブザーバビリティの必要性を促進する戦略と傾向、オブザーバビリティが中核的なビジネス目標を達成するための重要な鍵となるのか、それともインシデント対応／予防強化のためであるのか、フルスタックオブザーバビリティを阻む課題について考察します。

ハイライト：

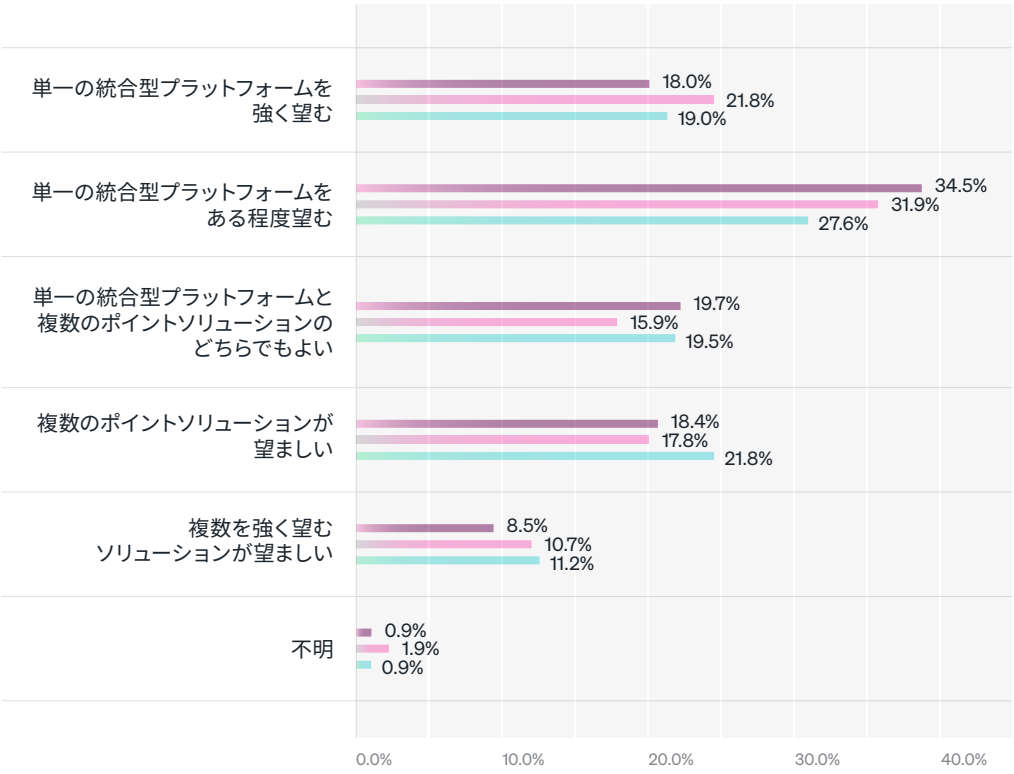
53%
単一の統合型オブザーバビリティプラットフォームを好む

41%
AIテクノロジーの導入によりオブザーバビリティのニーズが高まっていると回答

32%
広範な機能がオブザーバビリティベンダーのもっとも重要な基準であると回答

単一プラットフォームか複数ポイントソリューションか

オブザーバビリティに使用されているツールの数に関しては、半数以上（53%）がある程度単一の統合プラットフォームを選択しています。これは昨年とほぼ同じです。4分の1以上（27%）がある程度複数のポイントソリューションを選択し、これは昨年より6%減少で、また5人に1人（20%）は特に好みがないため、昨年より24%増加しました。



組織規模別の考察

小規模組織（56%）は、中規模組織（53%）や大規模組織（52%）の企業よりも、ある程度単一の統合プラットフォームを好む傾向が高く見られました。

地域別の考察

欧州の回答者（58%）は、南北アメリカ（52%）やアジア太平洋（51%）よりも、ある程度単一のプラットフォームを好む傾向が高く見られました。

業界別の考察

教育機関の回答者は、単一の統合されたオブザーバビリティプラットフォームを好む傾向がもっとも高く（64%）、続いてITと政府機関（両方60%）でした。医療／製薬の回答者は複数のポイントソリューションを好む傾向がもっとも高く（36%）、次にサービス／コンサルティング（34%）、テレコミュニケーション（33%）でした。

図13. オブザーバビリティの嗜好性、2022、2023、2024年の比較

- 2024年の回答者
- 2023年の回答者
- 2022年の回答者

53%

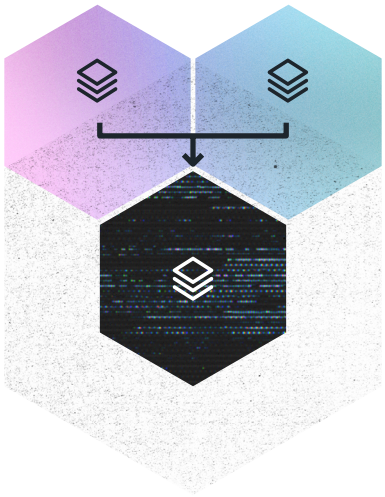
単一の統合型オブザーバビリティプラットフォームを好む

2年連続、ほぼ2対1の割合で、複数のポイントソリューションよりも単一のプラットフォームが好まれています。オブザーバビリティに単一のツールを使用することと、オブザーバビリティへの支出の削減、ダウンタイムの減少、システム停止コストの削減、中断への対処時間の削減との間に関連性があったため、これは理にかなっています。

多くの回答者が単一の統合型プラットフォームが好ましいとしているにもかかわらず、88%が2つ以上の監視ツールを使用しており、オブザーバビリティに単一ツールを使用しているのはわずか6%でした。

フルスタックオブザーバビリティの実現を妨げている課題は何かとの質問に、3分の1以上（34%）が、監視ツールが多すぎてデータがサイロ化されていると回答しました。

ツールの分散が続いている一方で、ここ数年、使用するツールの数が減りつつあります。実際、単一ツールを使用している回答者の数は前年比（YoY）37%増加しました。また、ツールの平均数は前年比11%減少しました。さらに、41%が来年中にツールを統合する予定であると回答しています。



オブザーバビリティベンダーの基準

回答者の3分の1近くが、オブザーバビリティベンダーまたはソリューションを選択する際のもっとも重要な基準は、広範な機能（32%）と手頃な価格（31%）であると回答しました。さらに、4分の1以上がビジネスオブザーバビリティ（27%）、デプロイメントモデル（27%）、学習とヘルプ（26%）を挙げています。

32% 広範な機能がオブザーバビリティベンダーのもっとも重要な基準であると回答

全体としては、広範な機能、手頃な価格、ビジネスオブザーバビリティがオブザーバビリティベンダー基準の上位3つでしたが、上位の選択肢は役割、組織の規模、地域、業界によって大きく異なりました。

組織規模別の考察

中規模および大規模組織（両方32%）では、小規模組織（24%）よりもコストをもっとも重要な基準として挙げる傾向が高かった。

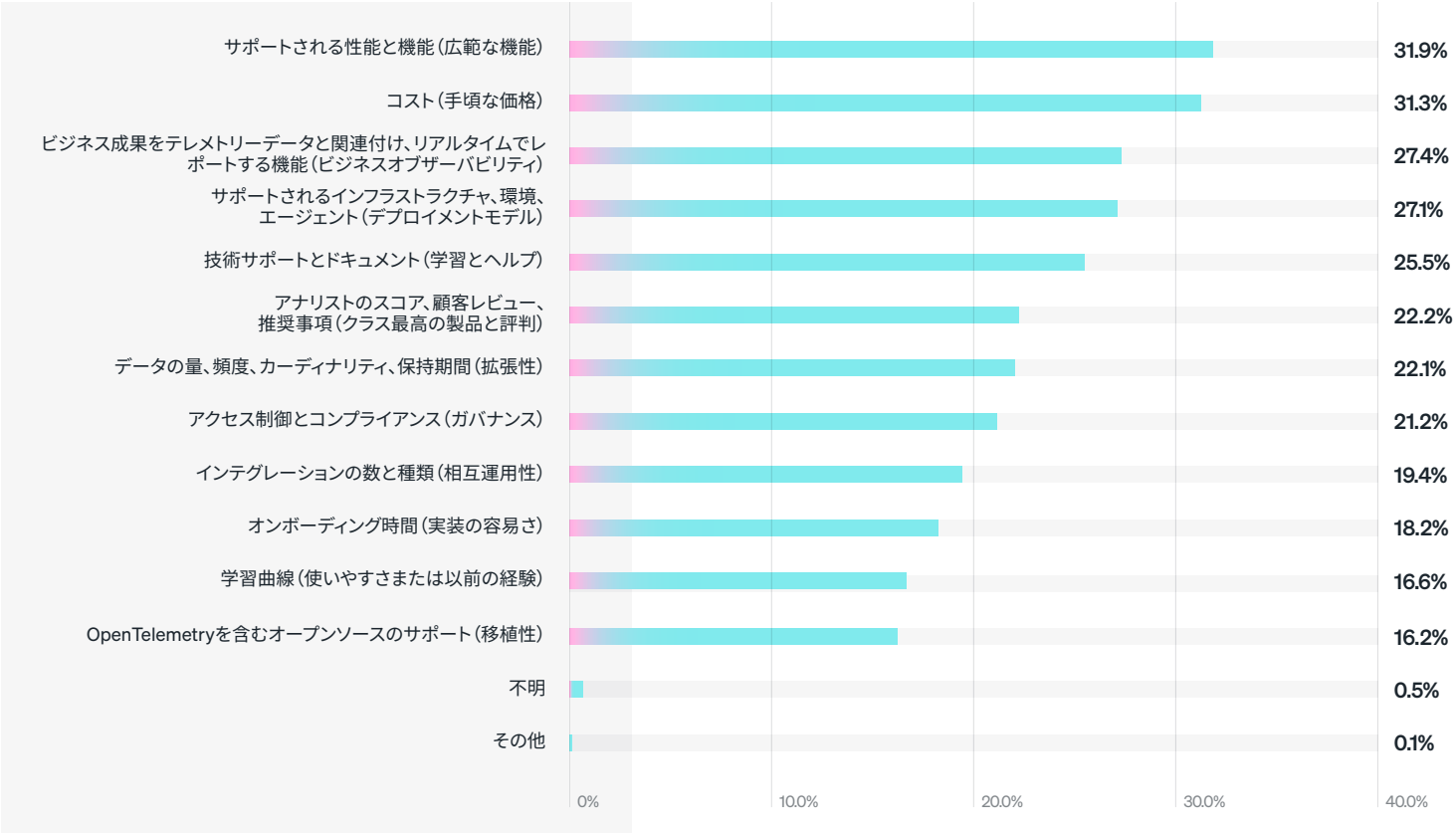
地域別の考察

欧州（39%）と南北アメリカ（38%）の回答者では、コスト（手頃な価格）が最優先の選択肢でしたが、アジア太平洋（22%）の回答者は、優先順位が特に低かった（7番目の選択肢）ことが顕著でした。アジア太平洋の回答者（32%）では、ビジネスオブザーバビリティが第1位の選択肢であったのに対し、南北アメリカ（25%）では第5位、欧州（21%）では第7位でした。

業界別の考察

教育（43%）、サービス／コンサルティング（43%）、IT（38%）、エネルギー／ユーティリティ（32%）、小売／消費者（31%）の回答者では、コスト（手頃な価格）がトップでした。テレコミュニケーションの上位2つの基準は、ビジネスオブザーバビリティとクラス最高のサービスと評判でした（両方39%）。広範な機能とともにビジネスオブザーバビリティも、金融サービス／保険でもトップの回答でした（両方34%）。メディア／エンターテイメントでは、拡張性とともに広範な機能もトップの回答となっています（両方34%）。政府機関では、実装とデプロイメントモデルの容易さが最上位の基準でした（両方28%）。

図14. もっとも重要なオブザーバビリティベンダーの基準



オブザーバビリティを促進するトレンド

データによると、人工知能（AI）テクノロジーの導入と、セキュリティ、ガバナンス、リスク、コンプライアンスの重視が、オブザーバビリティの推進要因としてもっともよく挙げられている（両方とも41%）ことが示されています。調査対象者の約3分の1は、ビジネスアプリのワークフローへの統合（35%）、コスト管理（33%）、クラウドネイティブのアプリケーションアーキテクチャーの開発（31%）を挙げています。

41% AIテクノロジーの導入によりオブザーバビリティのニーズが高まっていると回答

組織規模別の考察

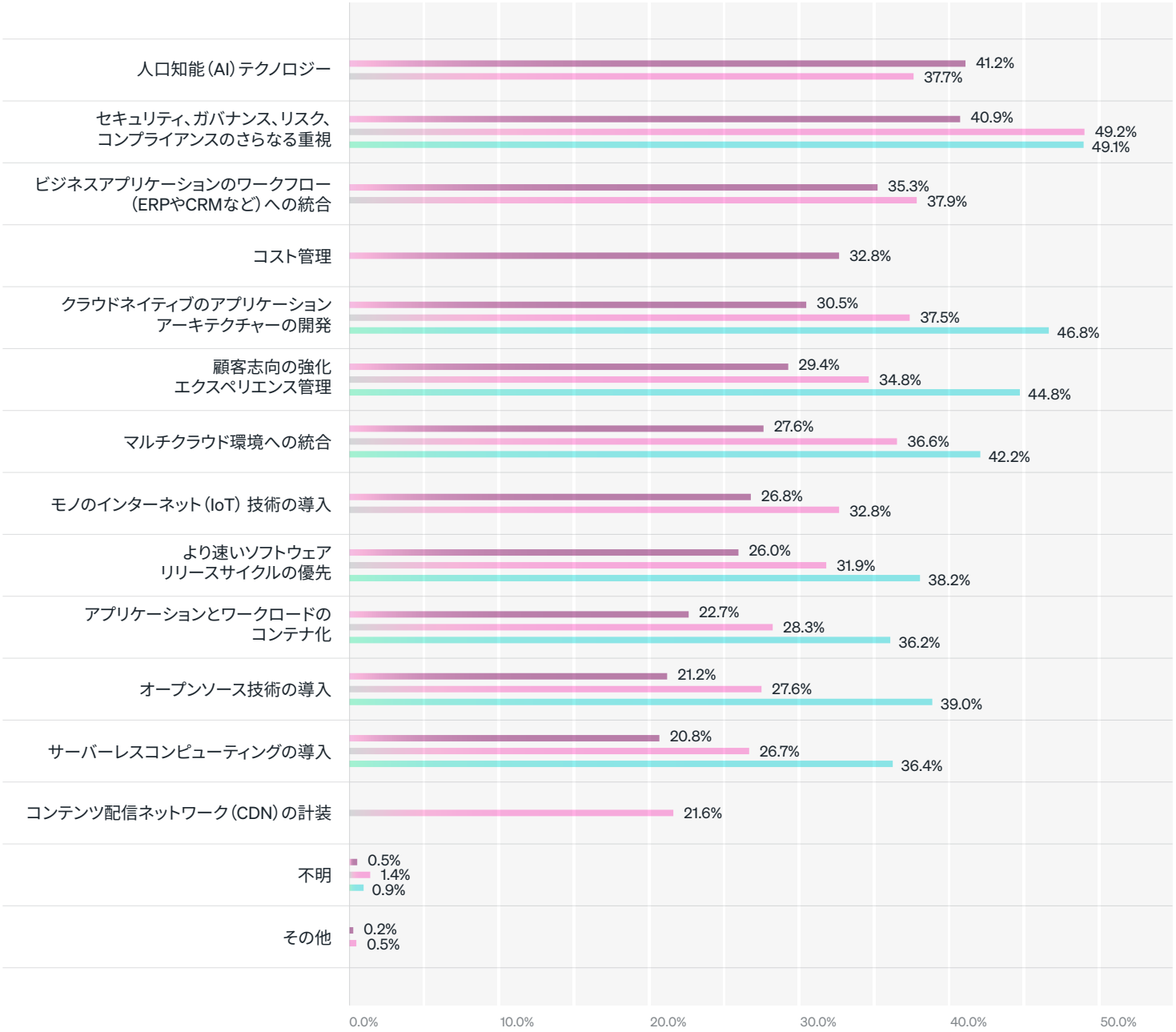
小規模組織の回答者は、マルチクラウド環境への移行（中規模25%、大規模31%に対して17%）やコスト管理（大規模33%、中規模34%に対して27%）を挙げる傾向が低く、AIテクノロジーの導入（大規模41%、中規模44%に対して34%）や、セキュリティ、ガバナンス、リスク、コンプライアンスへの重視が高まっているという回答でした（中規模39%、大規模44%に対して31%）。

地域別の考察

アジア太平洋の回答者は、コスト管理（欧州35%、南北アメリカ42%に対して25%）やAIテクノロジーの導入（欧州41%、南北アメリカ48%に対して36%）を挙げる傾向が低く、一方で、セキュリティ、ガバナンス、リスク、コンプライアンスへの重視が高まっているという回答でした（欧州の43%、南北アメリカの48%に対して34%）。

業界別の考察

AIテクノロジーの導入、セキュリティ、ガバナンス、リスク、コンプライアンスへの重視が、1つを除くすべての業界の回答者にとって最大の推進力でした。エネルギー／ユーティリティの回答者にとっては、ビジネスアプリケーションのワークフローへの統合が最大の推進力でした（43%）。



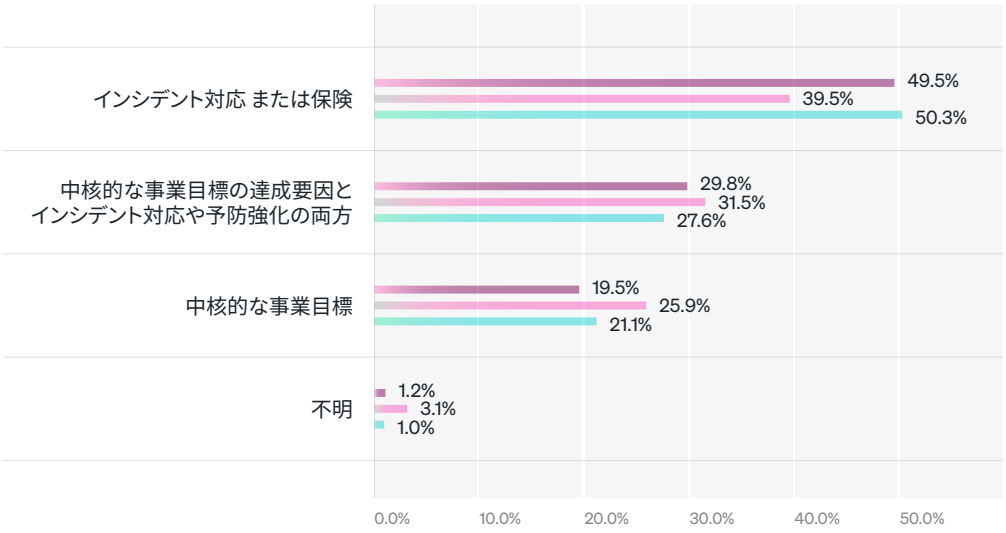
AIテクノロジーの導入とコスト管理を除いて、オブザーバビリティを推進する他のすべての戦略とトレンドは前年比で減少しました。このデータは、AIへの関心の高まりを反映しています。

図15. オブザーバビリティのニーズを促進するテクノロジー戦略とトレンド、2022、2023、2024年の比較

- 2024年の回答者
- 2023年の回答者
- 2022年の回答者

オブザーバビリティの目的

調査回答者の半数（50%）が、どちらかというとオブザーバビリティを中核的な事業目標の達成要因であると考えています（対前年比で25%増加）。さらに、ほぼ3分の1（30%）が、オブザーバビリティにより組織内でビジネス目標とインシデント対応が同等に可能になると回答しました（対前年比で5%減少）。また、5人に1人（20%）が、オブザーバビリティをインシデント対応または予防強化とみなしていると回答しています（対前年比で25%減少）。



総合すると、79%がある程度オブザーバビリティを中核的な事業目標の達成要因であると考えています（2023年71%、2022年78%）。一方、49%がある程度のインシデント対応または予防強化のためだと回答しています（2023年57%、2022年49%）。

組織規模別の考察

小規模組織（59%）は、オブザーバビリティは中核的な事業目標の達成要因であると回答する傾向がもっとも高く、中規模組織（51%）と大規模組織（47%）が続きました。

地域別の考察

オブザーバビリティを中核的な事業目標の達成要因であるとする回答は、アジア太平洋の回答者がもっとも多く（57%）、次いで欧州（47%）、南北アメリカ（42%）でした。

業界別の考察

オブザーバビリティは中核的な事業目標の達成要因であると回答する可能性がもっとも高かったのは政府機関の回答者（65%）で、次いでメディア／エンターテイメント（62%）、IT（59%）でした。教育の回答者は、インシデント対応または予防強化のためであると回答する可能性がもっとも高く（32%）、次いで医療／製薬、エネルギー／ユーティリティの回答者（両方27%）でした。

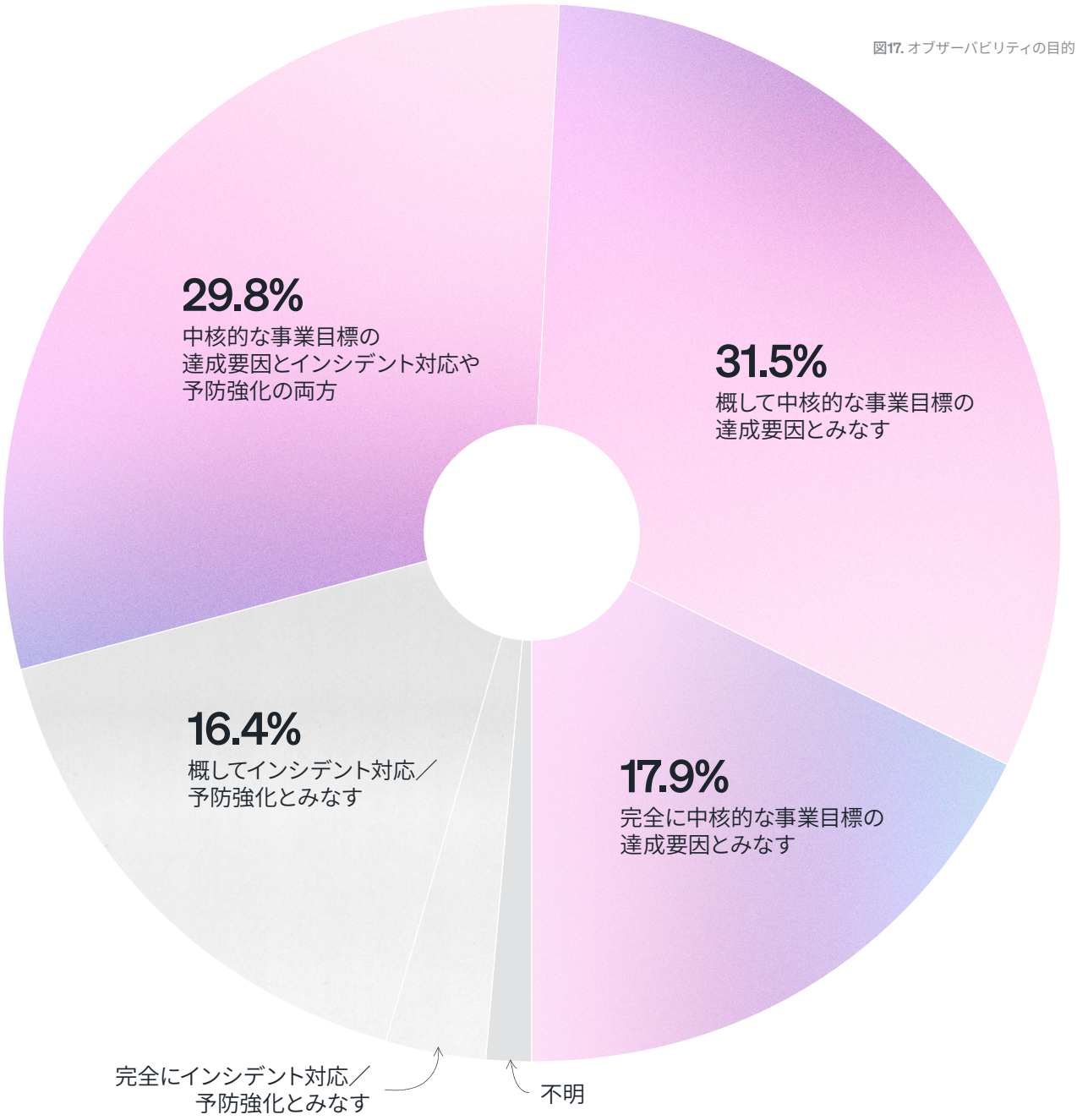
図16. テレメトリーデータの統合 vs. サイロ化、2022、2023、2024年の比較

2024年の回答者
2023年の回答者
2022年の回答者

79% オブザーバビリティをある程度中核的な事業目標を達成するための重要な実現要因とみなす

これらの結果は、オブザーバビリティを単なるインシデント対応や予防強化のためではなく、中核的な事業目標を達成するための重要な実現要因とみなす、回答者の間で明らかな変化が生じていることを示しています。

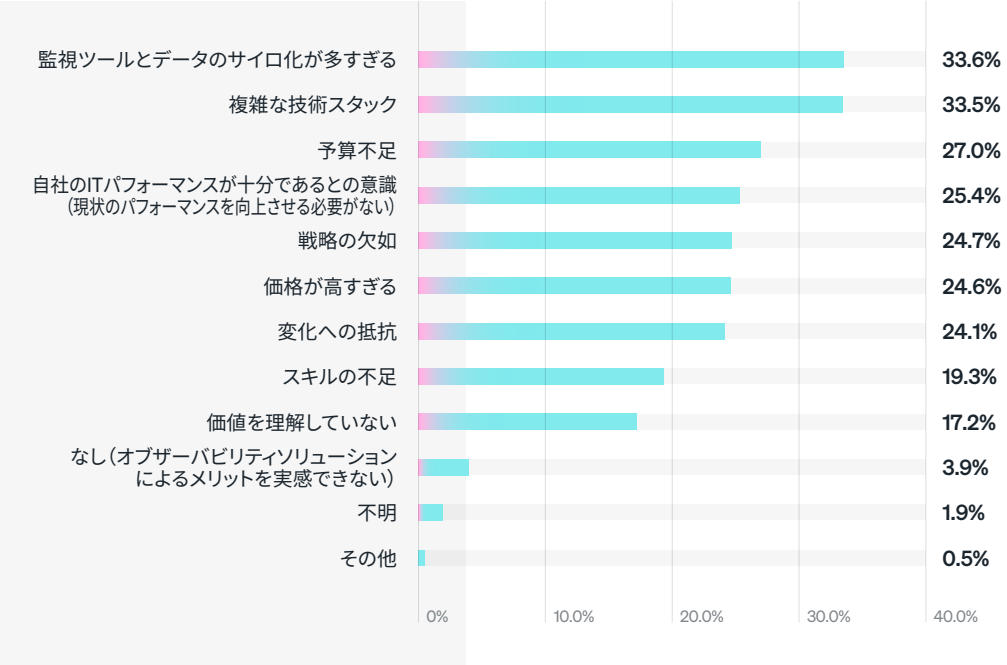
図17. オブザーバビリティの目的



フルスタックオブザーバビリティを阻む課題

組織にフルスタックオブザーバビリティの実現を阻むものは何かと調査したところ、回答者の3分の1以上が、複雑な技術スタック、多すぎる監視ツール、サイロ化されたデータを挙げています（両方34%）。約4分の1が、予算不足（27%）、十分なITパフォーマンス（25%）、戦略の欠如（25%）、価格が高すぎる（25%）、変化への抵抗（24%）を挙げており、すでにフルスタックオブザーバビリティを実現していると主張していたのははわずか4%でした。

34% フルスタックオブザーバビリティを実現する上での障害として、**多すぎる監視ツールとサイロ化されたデータと回答**



注：この質問では、2023〜2024年にかけて回答のオプションにいくつかの変更があったため、前年比、同一条件での比較を行うことはできません。

組織規模別の考察

大規模組織の回答者は、多すぎる監視ツールやサイロ化されたデータ、複雑な技術スタックが最大の課題と回答しました。中規模組織では、価格が高すぎると答える傾向がもっとも多く見られました。小規模組織の最大の課題は予算不足でした。

地域別の考察

欧州の回答者は、価格が高すぎると回答する傾向がもっとも高い一方で、監視ツールが多すぎることやデータがサイロ化されていたと回答する傾向はもっとも低く見られました。南北アメリカとアジア太平洋の回答者は、戦略の欠如と変化への抵抗が課題と答える傾向がより高く見られました。アジア太平洋では、自分にスキルはないが、ITパフォーマンスは十分であると答える傾向が高く見られました。

業界別の考察

ほとんどの業界の企業にとって、上位2つの課題は、複雑な技術スタック、多すぎる監視ツールとサイロ化されたデータでした（いくつかの例外を除く）。教育業界の回答者は、最大の課題に予算不足（51%）と費用（35%）を挙げています。政府機関（32%）、テレコミュニケーション（32%）、サービス／コンサルティング（28%）の回答者にとっても予算不足を2番目に挙げています。メディア／エンターテイメントの2番目の選択肢は、戦略の欠如でした（34%）。

図18. 組織でのフルスタックオブザーバビリティ実現を阻む主な課題

これらの結果は、ツールの分散の拡大、データのサイロ化、複雑な技術スタックがリストの上位を占めており、フルスタックオブザーバビリティを実現するには、複数の異なる障壁と問題があることを示しています。

システム停止、ダウンタイムとシステム停止にかかるコスト

開発者とエンジニアは、3つの重要なビジネス、および技術的な課題の解決によくオブザーバビリティを使用します。ダウンタイムの短縮、レイテンシの短縮、そして効率性の向上です。

システム停止の頻度、平均検出時間（MTTD）、平均復旧時間（MTTR）が、セキュリティおよびITインシデント管理で使用される一般的なサービスレベルのメトリクスです。

このセクションでは、システム停止の原因、頻度、コスト（MTTDとMTTRの傾向）について説明します。

ハイライト：

62%

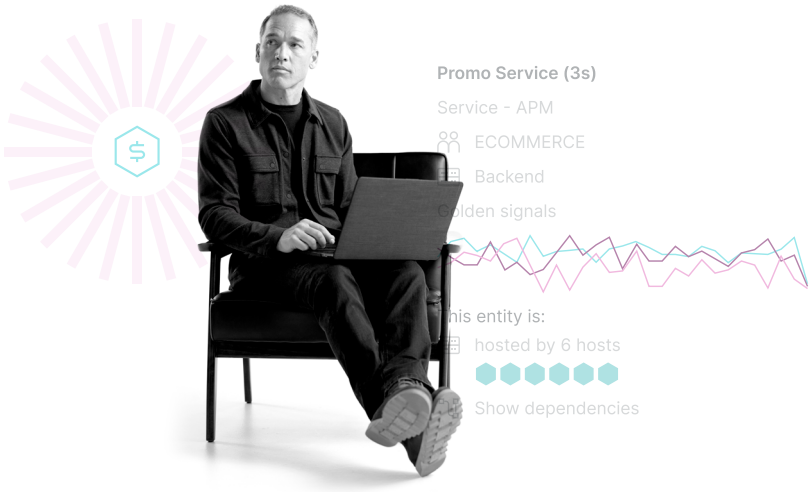
ビジネス影響が大きいシステム停止では、ダウンタイム1時間あたりのコストは100万ドル以上と回答

59%

オブザーバビリティを導入してからMTTRがある程度改善したと回答

38%

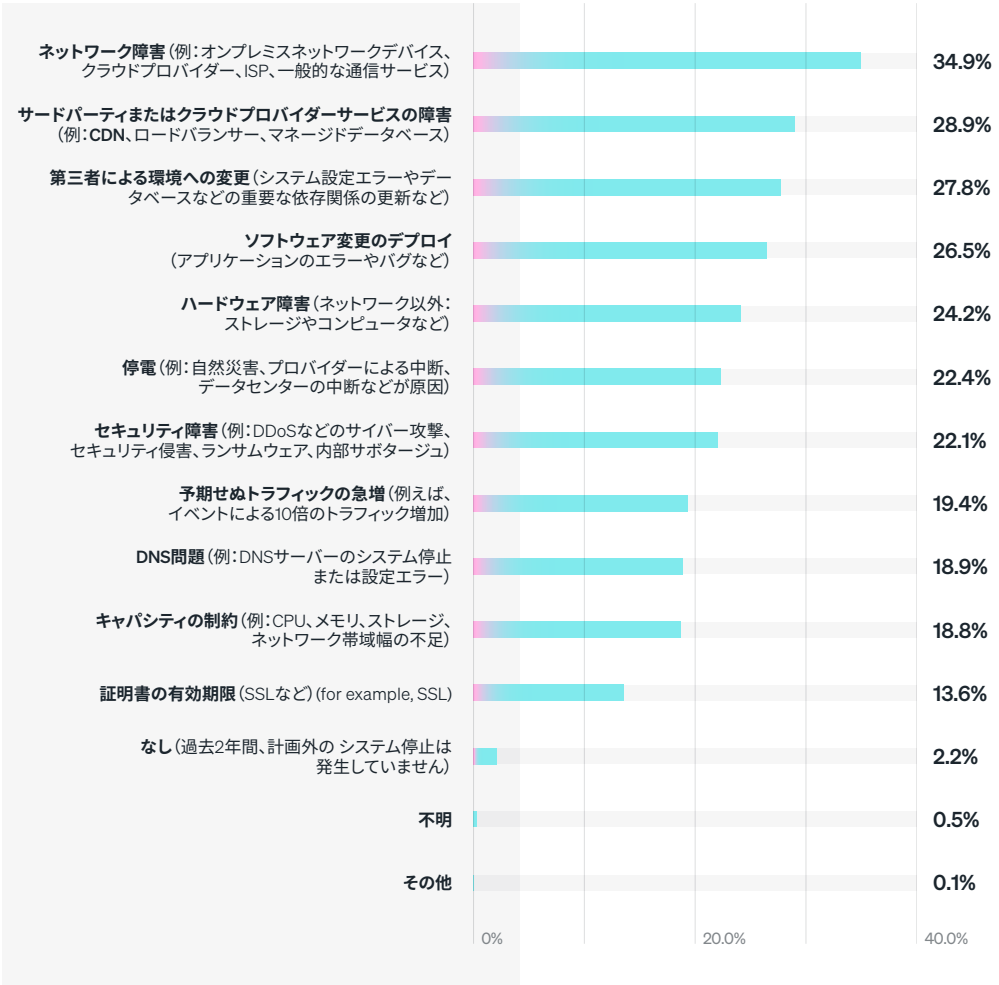
ビジネスインパクトの大きいシステム停止が週1回以上発生したと回答



システム停止の原因

回答者の3分の1以上（35%）が、過去2年間に組織で計画外停止が発生したもっとも一般的な原因はネットワーク障害であると回答しました。4分の1以上が、もっとも一般的な原因として、サードパーティまたはクラウドプロバイダーのサービス障害（29%）、第三者による環境への変更（28%）、ソフトウェアの変更のデプロイ（27%）を挙げています。

35% 過去2年間の計画外停止のもっとも一般的な原因はネットワーク障害であると回答



組織規模別の考察

大規模組織では、第三者による環境への変更が主な原因であると回答する傾向が高く見られました（31%、中小規模では24%）。小規模組織では、キャパシティの制約を挙げる傾向が高く見られました（26%、大規模19%、中規模16%）。

地域別の考察

欧州と南北アメリカの回答者は、第三者による環境への変更が共通の原因であると回答する傾向が高く見られました（それぞれ32%と31%、アジア太平洋では23%）。アジア太平洋の回答者は、キャパシティの制約（南北アメリカ18%と欧州の15%に対して21%）や、予期せぬトラフィックの急増（南北アメリカ18%と欧州の16%に対して22%）に対処している傾向が多く見られました。

業界別の考察

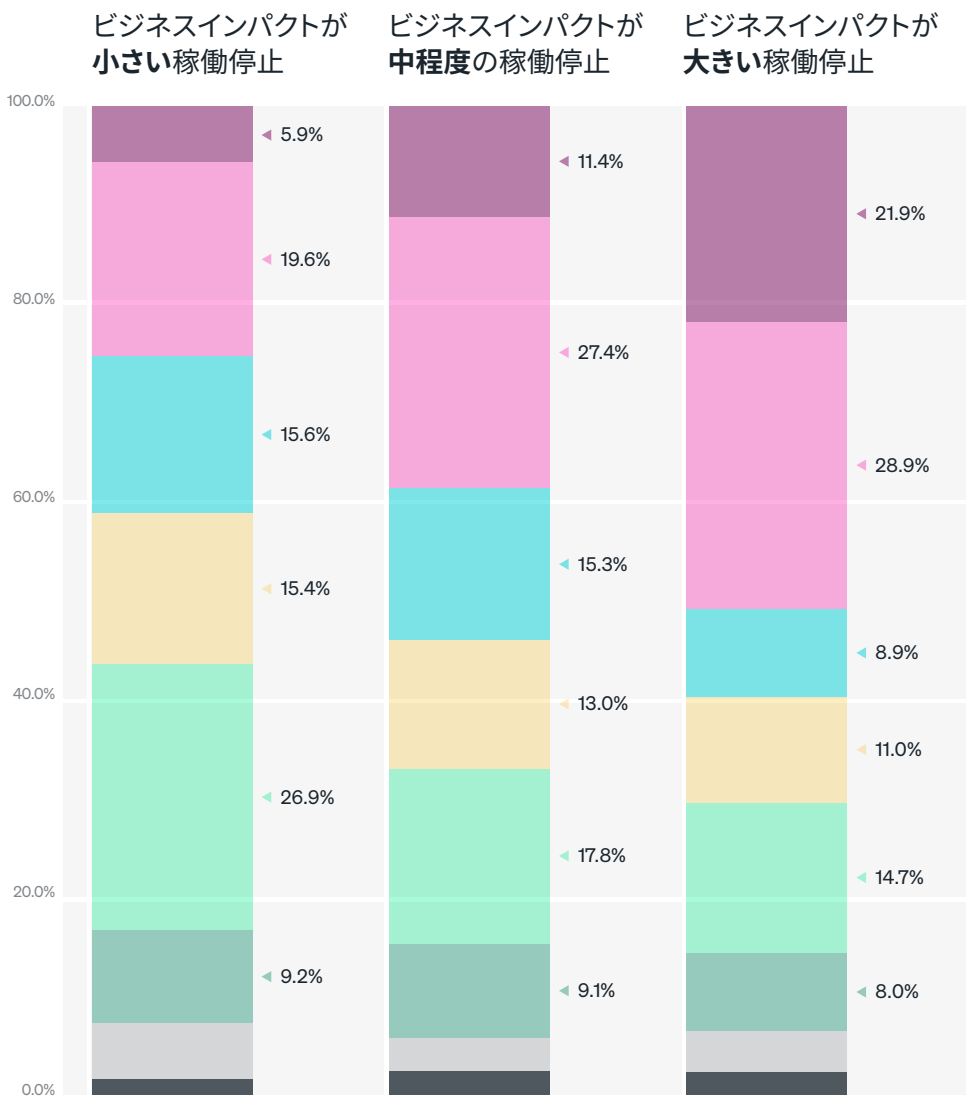
ネットワーク障害は、すべての業界にとって最優先の選択肢ではありませんでした。政府機関の回答者はセキュリティ障害（34%）、メディア／エンターテイメントでは停電（32%）と同率1位でした。エネルギー／ユーティリティの回答者（35%）にとっても停電がトップの選択肢でした。

図19. 過去2年間の計画外停止のもっとも一般的な原因

過去2年間に組織で計画外停止が発生したもっとも一般的な原因は、4分の1以上が人的ミス（第三者による環境への変更や、ソフトウェアの変更のデプロイ）によるものであると回答しました。しかし、ほとんどの回答者は、これらのシステム停止は自分たちでは制御できないものだと考えています。

システム停止の頻度

調査回答者に、ビジネスインパクトが小さい、中程度、または大きいシステム停止がどのくらいの頻度で発生するかを尋ねたところ、すべてのビジネスインパクトのレベルにおける年間停止頻度の中央値は**232回**でした。ビジネスインパクトが小さいシステム停止がもっとも頻繁に発生し、半数以上（57%）が少なくとも週に1回停止を経験し、15%は毎日停止に対処していました。ビジネスインパクトが大きいシステム停止の発生頻度はもっとも低いものの、38%が週に1回以上の停止を経験しており、12%は1 日に1 回以上の停止が発生していると回答しました。



組織規模別の考察
小規模組織は、大規模組織（234件）や中規模組織（183件）に比べて、年間でかなり多くのシステム停止（410件）を経験しました。

地域別の考察
南北アメリカの回答者は、欧州（207件）やアジア太平洋（272件）と比較して、年間のシステム停止件数（94件）が最小でした。

業界別の考察
年間でもっとも多くのシステム停止が発生したのは政府機関（419件）、次いでメディア／エンターテイメント組織（413件）でした。サービス／コンサルティング組織が年間システム停止の発生件数がもっとも少なく（55件）、次いで小売／消費者組織（118件）でした。

図20. すべてのビジネス影響レベル全体のシステム停止の頻度

38%
ビジネス影響の大きいシステム停止が週1回以上発生

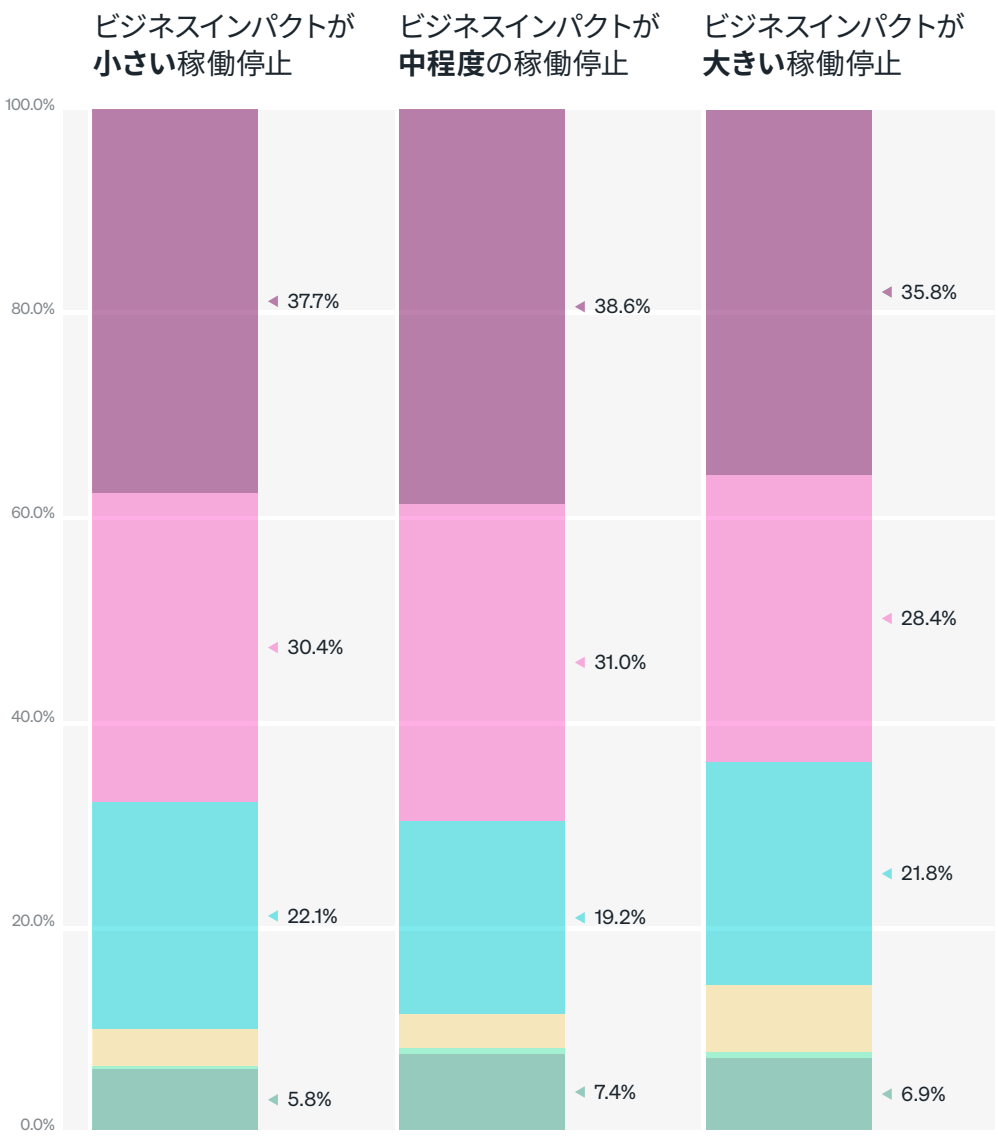
次の7つの要因がシステム停止頻度の低下に関連していました。

- ✓ **より統合されたテレメトリーデータの保持：**より統合されたテレメトリーデータを保持している企業は、よりサイロ化されたテレメトリーデータを保持している企業に比べて、年間のシステム停止回数が77%減少しました（409回の停止回数に対して96回）。
- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現した企業は、実現しなかった企業に比べて、年間のシステム停止回数が71%減少しました（252回の停止回数に対して74回）。
- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、年間で発生するシステム停止の数は少なくなります。たとえば、5つ以上のオブザーバビリティ性能を導入済みの企業は、4つ以下の企業に比べて年間のシステム停止回数が47%減少しました（370回のシステム停止回数に対して196回）。10個以上を導入済みの企業は、9個以下の企業に比べて、年間のシステム停止回数が62%減少しました(25回の停止回数に対して96回）。また、15個以上を導入済みの企業は、14個以下の企業に比べて、年間のシステム停止回数が69%減少しました（234回の停止回数に対して74回）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した企業は、より手動による検知方法を使用した企業に比べて、年間のシステム停止回数が69%減少しました（366回の停止回数に対して114回）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、年間のシステム停止回数が47%減少しました（252回の停止回数に対して134回）。
- ✓ **オブザーバビリティに1つのツールを使用：**オブザーバビリティに1つのツールを使用している企業は、2つ以上のツールを使用している企業に比べて、年間のシステム停止回数が9%減少しました（234回の停止回数に対して214回）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、年間のシステム停止回数が8%減少しました（232回の停止回数に対して214回）。

システム停止はかなり頻繁に発生しますが、フルスタックオブザーバビリティやその他の要因が停止頻度に多大なプラスの影響をもたらします。

平均検出時間 (MTTD)

システム停止を検出するまでの平均時間は、セキュリティとITインシデント管理で使用される一般的なサービスレベル指標です。このデータは、すべてのビジネス影響レベル全体でMTTDに費やされる年間時間の中央値が**134時間、約6日であることを示しています。**ビジネス影響が大きいシステム停止のMTTDの中央値は37分で、回答者の4分の1以上 (29%) は、1時間以上であると回答しました。



組織規模別の考察
平均すると、中規模の組織は、大規模な組織 (138時間) や小規模な組織 (163時間) よりも、年間システム停止の検知に費やす時間が短くなっています (101時間)。

地域別の考察
平均すると、アジア太平洋の回答者が年間システム停止の検知にもっとも多くの時間を費やし (219時間) 、次いで欧州 (110時間) 、南北アメリカ (42時間) でした。

業界別の考察
年間システム停止の検知にもっとも時間がかかっていた業界には、サービス／コンサルティング (23時間) 、小売／消費者 (61時間) 、教育 (64時間) が挙げられます。年間システム停止の検知にもっとも時間を費やした業界には、メディア／エンターテイメント (331時間) 、政府 (269時間) 、金融サービス／保険 (227時間) が挙げられます。

図21. ビジネス影響レベル別のシステム停止におけるMTTD

29%
ビジネス影響が大きいシステム停止の検知に1時間超費やしている

次の7つの要因がMTTDの短縮に関連していました。

- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現した企業は、実現しなかった企業に比べて、年間のシステム停止の検知に費やす時間が85%減少しました（155時間に対して23時間）。
- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、年間のシステム停止の検知に費やす時間が短縮されます。たとえば、5つ以上のオブザーバビリティ関連機能を導入済みの企業は、4つ以下の企業に比べて、年間のシステム停止の検知に費やす時間が52%減少しました（195時間に対して95時間）。10個以上を導入済みの企業は、9個以下の企業に比べて、年間のシステム停止の検知に費やす時間が77%減少しました（170時間に対して39時間）。また、15個以上を導入済みの企業は、14個以下の企業に比べて、年間のシステム停止の検知に費やす時間が84%減少しました（138時間に対して22時間）。
- ✓ **より統合されたテレメトリーデータの保持：**より統合されたテレメトリーデータを保持している企業は、よりサイロ化されたテレメトリーデータを保持している企業に比べて、年間のシステム停止の検知に費やす時間が79%減少しました（225時間に対して28時間）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した企業は、より手動による検知方法を使用した企業に比べて、年間のシステム停止の検知に費やす時間が78%減少しました（216時間に対して48時間）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、年間のシステム停止の検知に費やす時間が65%減少しました（162時間に対して57時間）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、年間のシステム停止の検知に費やす時間が35%減少しました（138時間に対して90時間）。
- ✓ **オブザーバビリティに1つのツールを使用：**オブザーバビリティに1つのツールを使用している企業は、2つ以上のツールを使用している企業に比べて、年間のシステム停止の検知に費やす時間が15%減少しました（138時間に対して117時間）。

すべてのビジネス影響レベルのシステム停止を検知するにはほぼ同じ時間がかかりますが、フルスタックオブザーバビリティやその他の要因により、MTTD時間を大幅に短縮できます。

平均復旧時間 (MTTR)

セキュリティとITインシデント管理で使用される一般的なサービスレベル指標であるMTTRにも同様のパターンがあります。すべてのビジネス影響レベル全体でMTTRに費やされる年間時間の中央値が**141時間、つまり約6日であることを示しています。**ビジネス影響が大きいシステム停止のMTTRの中央値は51分で、回答者の3分の1以上 (39%) は、1時間以上であると回答しました。

組織規模別の考察
中規模組織のMTTR中央値 (118時間) は、大規模組織 (155時間) や小規模組織 (167時間) と比較してもっとも低く見られました。

地域別の考察
アジア太平洋の回答者のMTTR中央値がもっとも高く (245時間) 、次いで欧州 (125時間) 、南北アメリカ (53時間) でした。

業界別の考察
MTTRの中央値がもっとも低い業界には、サービス／コンサルティング (48時間) 、小売／消費者 75時間) 、教育 (97時間) が挙げられます。MTTRの中央値がもっとも高い業界には、政府 (302時間) 、メディア／エンターテイメント (284時間) 、金融サービス／保険 (277時間) が挙げられます。

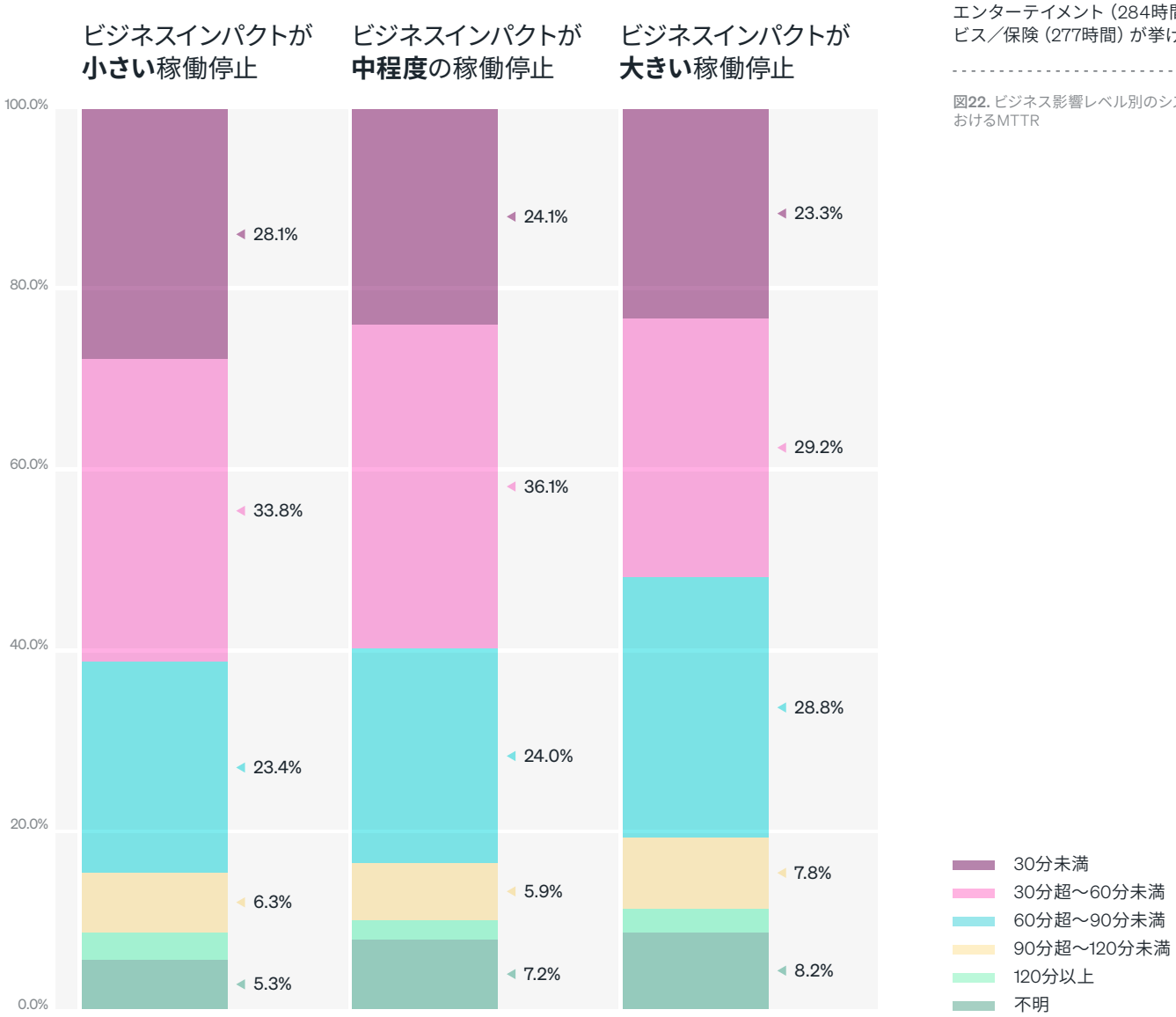


図22. ビジネス影響レベル別のシステム停止におけるMTTR

39%
ビジネス影響が大きいシステム停止の解決に1時間超費やしている

次の7つの要因がMTTRの短縮に関連していました。

- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現した企業は、実現しなかった企業に比べて、年間のシステム停止の解決に費やす時間が76%減少しました（168時間に対して41時間）。
- ✓ **より統合されたテレメトリーデータの保持：**より統合されたテレメトリーデータを保持している企業は、よりサイロ化されたテレメトリーデータを保持している企業に比べて、年間のシステム停止の解決に費やす時間が76%減少しました（258時間に対して62時間）。
- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、年間のシステム停止の検知に費やす時間が短縮されます。たとえば、5つ以上のオブザーバビリティ関連機能を導入済みの企業は、4つ以下の企業に比べて、年間のシステム停止の解決に費やす時間が41%減少しました（191時間に対して113時間）。10個以上を導入済みの企業は、9個以下の企業に比べて、年間のシステム停止の解決に費やす時間が70%減少しました（179時間に対して53時間）。また、15個以上を導入済みの企業は、14個以下の企業に比べて、年間のシステム停止の解決に費やす時間が75%減少しました（150時間に対して38時間）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した企業は、より手動による検知方法を使用した企業に比べて、年間のシステム停止の解決に費やす時間が74%減少しました（240時間に対して63時間）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、年間のシステム停止の解決に費やす時間が57%減少しました（178時間に対して77時間）。
- ✓ **オブザーバビリティに1つのツールを使用：**オブザーバビリティに1つのツールを使用している企業は、2つ以上のツールを使用している企業に比べて、年間のシステム停止の解決に費やす時間が20%減少しました（155時間に対して124時間）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、年間のシステム停止の解決に費やす時間が10%減少しました（145時間に対して130時間）。

ビジネス影響が大きいシステム停止は、解決にもっとも時間がかかります。ただし、フルスタックオブザーバビリティやその他の要因により、すべてのビジネス影響レベルのシステム停止をより迅速に解決できる可能性があります。

合計ダウンタイム

前述されたシステム停止の頻度と、その検出と解決にかかる時間を考慮すると、組織ではかなりのダウンタイムが起きていることになります。データによると、すべてのビジネス影響レベル全体の年間ダウンタイムの中央値は**77時間、約3日です。**

次のような要因が年間ダウンタイムの減少に関連していました。

- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、年間のシステム停止の検知に費やす時間が短縮されます。たとえば、5つ以上のオブザーバビリティ関連機能を導入済みの企業は、4つ以下の企業に比べて、年間のシステム停止の検知に費やす時間が45%減少しました（409時間に対して223時間）。10個以上を導入済みの企業は、9個以下の企業に比べて、年間のシステム停止の検知に費やす時間が74%減少しました（371時間に対して95時間）。また、15個以上を導入済みの企業は、14個以下の企業に比べて、年間のシステム停止の検知に費やす時間が80%減少しました（299時間に対して60時間）。
- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現した企業は、実現しなかった企業に比べて、年間ダウンタイムで79%を削減しました（338時間に対して70時間）。
- ✓ **より統合されたテレメトリーデータの保持：**より統合されたテレメトリーデータを保持している企業は、よりサイロ化されたテレメトリーデータを保持している企業に比べて、年間ダウンタイムで78%を削減しました（488時間に対して107時間）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した企業は、より手動による検知方法を使用した企業に比べて、年間ダウンタイムで73%を削減しました（445時間に対して118時間）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、年間ダウンタイムが63%減少しました（370時間に対して139時間）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、年間ダウンタイムが19%減少しました（294時間に対して239時間）。
- ✓ **オブザーバビリティに単一のツールを使用：**オブザーバビリティに1つのツールを使用している企業は、2つ以上のツールを使用している企業に比べて、年間ダウンタイムが18%減少しました（305時間に対して249時間）。

組織規模別の考察

年間ダウンタイムの中央値は小規模組織（372時間、約16日）がもっとも高く、次いで大規模組織（300時間、約13日）、中規模組織（230時間、約10日）でした。

地域別の考察

アジア太平洋の回答者の年間ダウンタイムの中央値がもっとも高く（467時間、約19日）、次いで欧州（227時間、約9日）、南北アメリカ（97時間、約4日）でした。

業界別の考察

年間ダウンタイムの中央値がもっとも高い業界には、メディア／エンターテイメント（608時間、約25日）、政府（564時間、約24日）、金融サービス／保険（528時間、約22日）が挙げられます。年間ダウンタイムの中央値がもっとも低い業界には、サービス／コンサルティング（80時間、約3日）、教育（158時間、約1週間）、小売／消費者（164時間、約1週間）が挙げられます。

ダウンタイムの短縮といくつかの要因（フルスタックオブザーバビリティの実現や一般により多くの機能の導入など）の間には強い関連性があります。

ダウンタイムは高くつきます。適切なツールが導入されていない場合は、人的資本の観点から、特定の問題を解決するためにより多くの時間を費やすかもしれません。

ITインフラストラクチャ担当シニアディレクター
米国大手フィンテック企業

システム停止コスト

ビジネス影響が小さいシステム停止の場合、ダウンタイム1時間あたりのシステム停止コストの中央値は130万ドルで、ビジネス影響が中程度の場合は160万ドル、ビジネス影響が大きい場合は**190万ドル**でした。

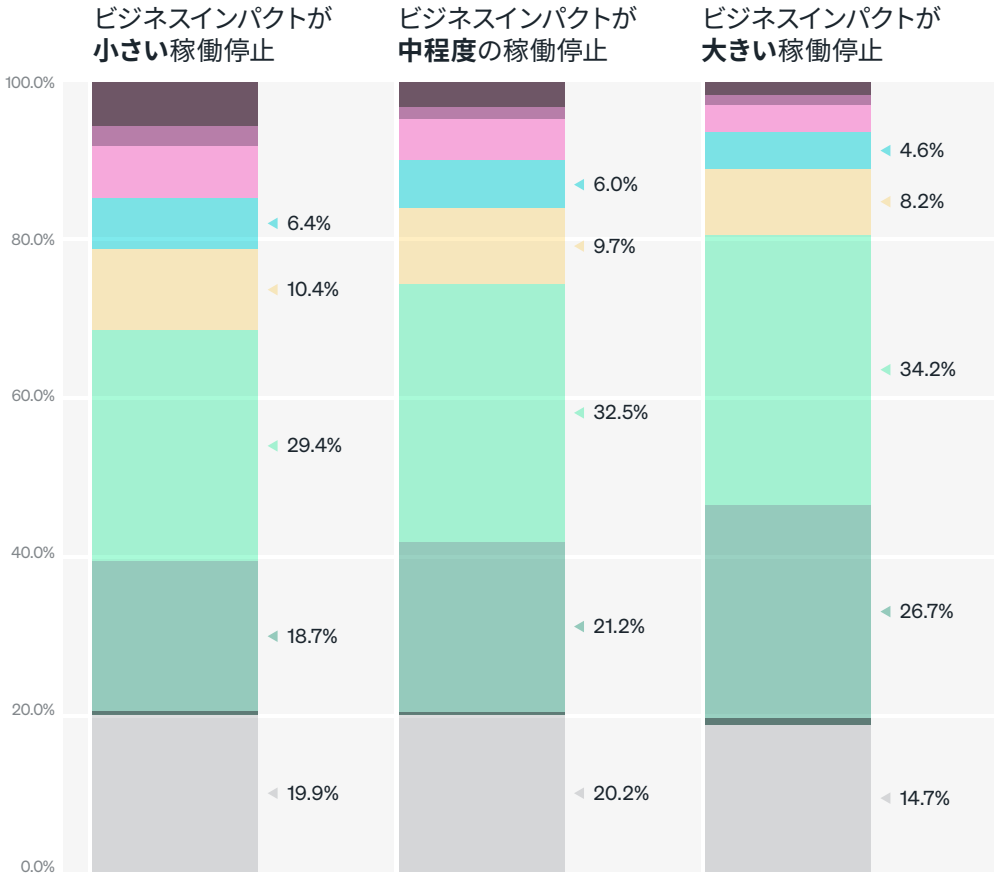


図23. ビジネス影響レベル別の時間あたりのシステム停止コスト

- %0（組織の収益に影響なし）
- 1〜9万9,990ドル
- 10〜24万9,990ドル
- 25〜49万9,990ドル
- 50〜99万9,990ドル
- 100〜249万ドル
- 250〜499万ドル
- ≥500万ドル
- 不明

62% ビジネス影響が大きいシステム停止では、ダウンタイム**1時間あたりのコストは100万ドル以上**と回答

次の6つの要因がビジネス影響が大きいシステム停止コストの中央値の低下に関連していました。

- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、時間あたりのシステム停止コストが削減されます。たとえば、5つ以上のオブザーバビリティ関連機能を導入済みの企業は、4つ以下の企業に比べて、時間あたりのシステム停止コストが5%減少しました（200万ドルに対して190万ドル）。10個以上を導入済みの企業は、9個以下の企業に比べて、時間あたりのシステム停止コストが41%減少しました（220万ドルに対して130万ドル）。10個以上を導入済みの企業は、9個以下の企業に比べて、時間あたりのシステム停止コストが50%減少しました（200万ドルに対して100万ドル）。
- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現した企業は、実現しなかった企業に比べて、時間あたりのシステム停止コストが48%減少しました（210万ドルに対して110万ドル）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した企業は、より手動による検知方法を使用した企業に比べて、時間あたりのシステム停止コストが19%減少しました（210万ドルに対して170万ドル）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、時間あたりのシステム停止コストが32%減少しました（220万ドルに対して150万ドル）。
- ✓ **オブザーバビリティに1つのツールを使用：**オブザーバビリティに1つのツールを使用している企業は、2つ以上のツールを使用している企業に比べて、時間あたりのシステム停止コストが45%減少しました（200万ドルに対して110万ドル）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、時間あたりのシステム停止コストが35%減少しました（200万ドルに対して130万ドル）。

組織規模別の考察

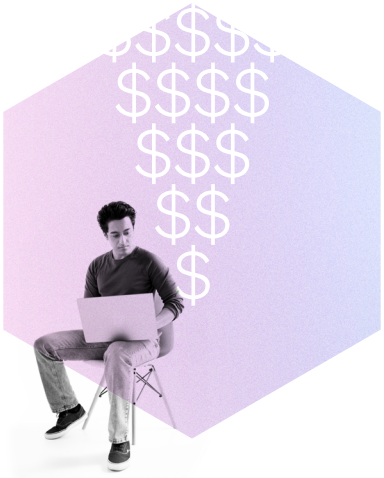
大規模組織では、ビジネス影響が大きいシステム停止に対する時間あたりシステム停止コストの中央値（210万ドル）が、中規模組織（200万ドル）や小規模組織（130万ドル）よりも高く見られました。

地域別の考察

アジア太平洋の回答者は、ビジネス影響が大きいシステム停止に対する時間あたりシステム停止コストの中央値（230万ドル）が、欧州（170万ドル）や南北アメリカ（140万ドル）よりも高く見られました。

業界別の考察

ビジネス影響が大きいシステム停止に対する時間あたりシステム停止コストがもっとも高い業界には、政府（230万ドル）、メディア／エンターテイメント（220万ドル）、テレコミュニケーション（220万ドル）、金融サービス／保険（220万ドル）が挙げられます。年間のシステム停止コストの中央値がもっとも低い業界には、サービス／コンサルティング（130万ドル）、教育（130万ドル）、医療／製薬（130万ドル）が挙げられます。

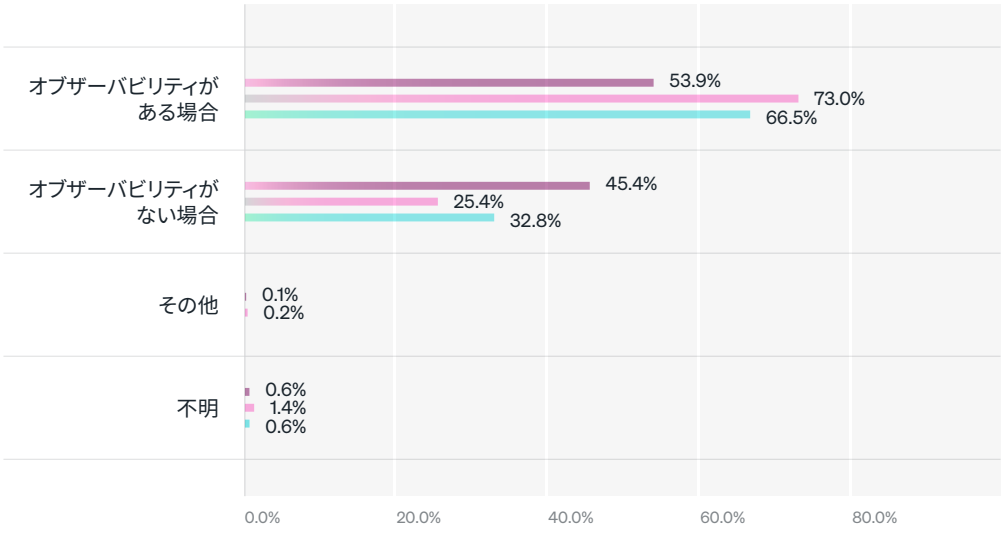


「平均すると、1分のダウンタイムで10,000ドル以上の費用がかかる可能性があると言えます。1分ごとのダウンタイムで企業は収益を損失する可能性があります。1時間ダウンした場合は、数百万ドルの損害が発生する可能性があります。」

ITインフラストラクチャ担当シニアディレクター
米国大手フィンテック企業

システム中断の検知

回答者は、オブザーバビリティがない場合（45%）よりもオブザーバビリティがある場合（54%）に中断を検知すると回答する傾向が依然として高かったものの、これは昨年より26%減少しました。また、単一のオブザーバビリティプラットフォームで中断を検知すると回答した企業は、昨年と比べて12%増加しました（2023年の15%に対して17%）。



地域別の考察

南北アメリカの回答者は、オブザーバビリティによる中断を検知した可能性がもっとも高く見られました（63%、欧州55%、アジア太平洋46%）。逆に、アジア太平洋の回答者は、オブザーバビリティなしで検知した可能性がもっとも高く見られました（54%、欧州44%、南北アメリカ36%）。

業界別の考察

サービス／コンサルティングの回答者は、オブザーバビリティで中断を検知する傾向がもっとも高く見られました（74%、医療／製薬で60%、ITで58%）。メディア／エンターテイメントの回答者は、オブザーバビリティなしで検知した可能性がもっとも高く（57%）、次いでエネルギー／ユーティリティ（56%）、テレコミュニケーション（53%）でした。

図24. 回答者がどのようにソフトウェアおよびシステムの中断を検知しているか、2022年、2023年、2024年の比較

- 2024年の回答者
- 2023年の回答者
- 2022年の回答者

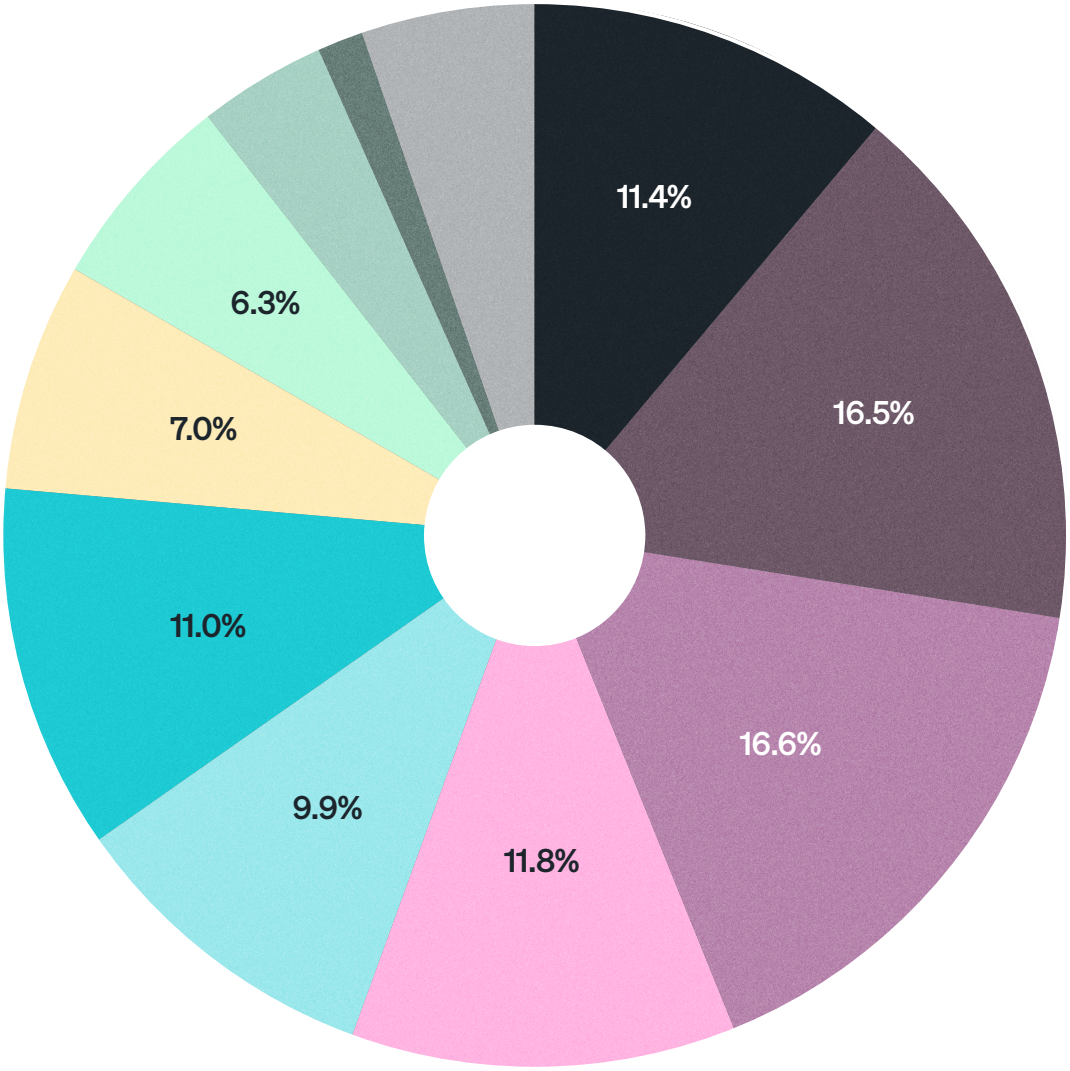
45% 未だに効率の低い方法で**中断を検知**

オブザーバビリティなしで中断を検知した企業と比較して、オブザーバビリティがある場合の中断を検知した企業のメリットは次のとおりです。

- 年間ダウンタイムで73%削減（445時間に対して118時間）
- 時間あたりのシステム停止コストで19%削減（210万ドルに対して170万ドル）
- サービス中断への対処に費やすエンジニアリング時間が28%削減（週40時間労働に基づく16時間に対して10時間）

システム中断への対処に費やした時間

エンジニアリングチームがシステム中断への対処に費やした時間の中央値の割合は30%で、週40時間労働とすると12時間に相当します。回答者のほぼ半数（45%）は、エンジニアリングチームがシステム中断への対処に費やした時間は30%未満、つまり週40時間労働とすると12時間未満であると回答しました。



組織規模別の考察
中規模と大規模組織は、小規模組織（25%）よりもシステム中断への対処に多くの時間を費やしています（それぞれ32%と31%）。

地域別の考察
アジア太平洋の回答者は、システム中断への対処にもっとも多くの時間を費やしたと推定し（41%）、次いで欧州（30%）、南北アメリカ（20%）でした。

業界別の考察
システム中断への対処に費やした時間がもっとも長い業界には、メディア／エンターテイメント（49%）、政府（43%）、金融サービス／保険（40%）が挙げられます。システム中断への対処に費やした時間がもっとも短い業界には、教育（20%）、サービス／コンサルティング（20%）、医療／製薬（24%）が挙げられます。

図25. エンジニアリングチームがシステム中断への対応に費やした時間の割合は、年間ダウンタイムと相関していました（相関値0.516）。

- 0%〜9%
- 10%〜19%
- 20%〜29%
- 30%〜39%
- 40%〜49%
- 50%〜59%
- 60%〜69%
- 70%〜79%
- 80%〜89%
- 90%〜99%
- 不明

次の7つの要因がエンジニアリングチームがサービス中断への対処に費やす時間の割合の低下に関連していました。

- ✓ **オブザーバビリティに単一のツールを使用：**オブザーバビリティに1つのツールを使用している企業は、複数のツールを使用している企業に比べて、サービス中断への対処に費やすエンジニアリング時間が50%減少しました（33%に対して17%、あるいは週40時間労働に基づくと13時間に対して7時間）。
- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現した企業は、実現しなかった企業に比べて、サービス中断への対処に費やすエンジニアリング時間が44%減少しました（36%に対して20%、あるいは週40時間労働に基づくと14時間に対して8時間）。
- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、年間のエンジニアリング時間が短縮される傾向がありました。たとえば、5つ以上のオブザーバビリティ関連機能を導入済みの企業は、4つ以下の企業に比べて、サービス中断への対処に費やす時間が24%減少しました（38%に対して29%、あるいは週40時間労働に基づくと15時間に対して12時間）。10個以上を導入済みの企業は、9個以下の企業に比べて、サービス中断への対処に費やす時間が41%減少しました（38%に対して22%、あるいは週40時間労働に基づくと15時間に対して9時間）。また、15個以上を導入済みの企業は、14個以下の企業に比べて、サービス中断への対処に費やす時間が39%減少しました（33%に対して20%、あるいは週40時間労働に基づくと13時間に対して8時間）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、サービス中断への対処に費やす時間が38%減少しました（34%に対して21%、あるいは週40時間労働に基づくと14時間に対して8時間）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した企業は、より手動による検知方法を使用した企業に比べて、年間のシステム停止に費やす時間が38%減少しました（40%に対して25%、あるいは週40時間労働に基づくと16時間に対して10時間）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、年間のシステム停止の対処に費やすエンジニアリング時間が27%減少しました（37%に対して27%、あるいは週40時間労働に基づくと15時間に対して11時間）。
- ✓ **より統合されたテレメトリーデータの保持：**より統合されたテレメトリーデータを保持している企業は、よりサイロ化されたテレメトリーデータを保持している企業に比べて、年間のシステム停止の対処に費やすエンジニアリング時間が11%減少しました（32%に対して28%、あるいは週40時間労働に基づくと13時間に対して11時間）。

29%

エンジニアリングチームは、時間の半分以上をサービス中断への対処に費やしていると報告

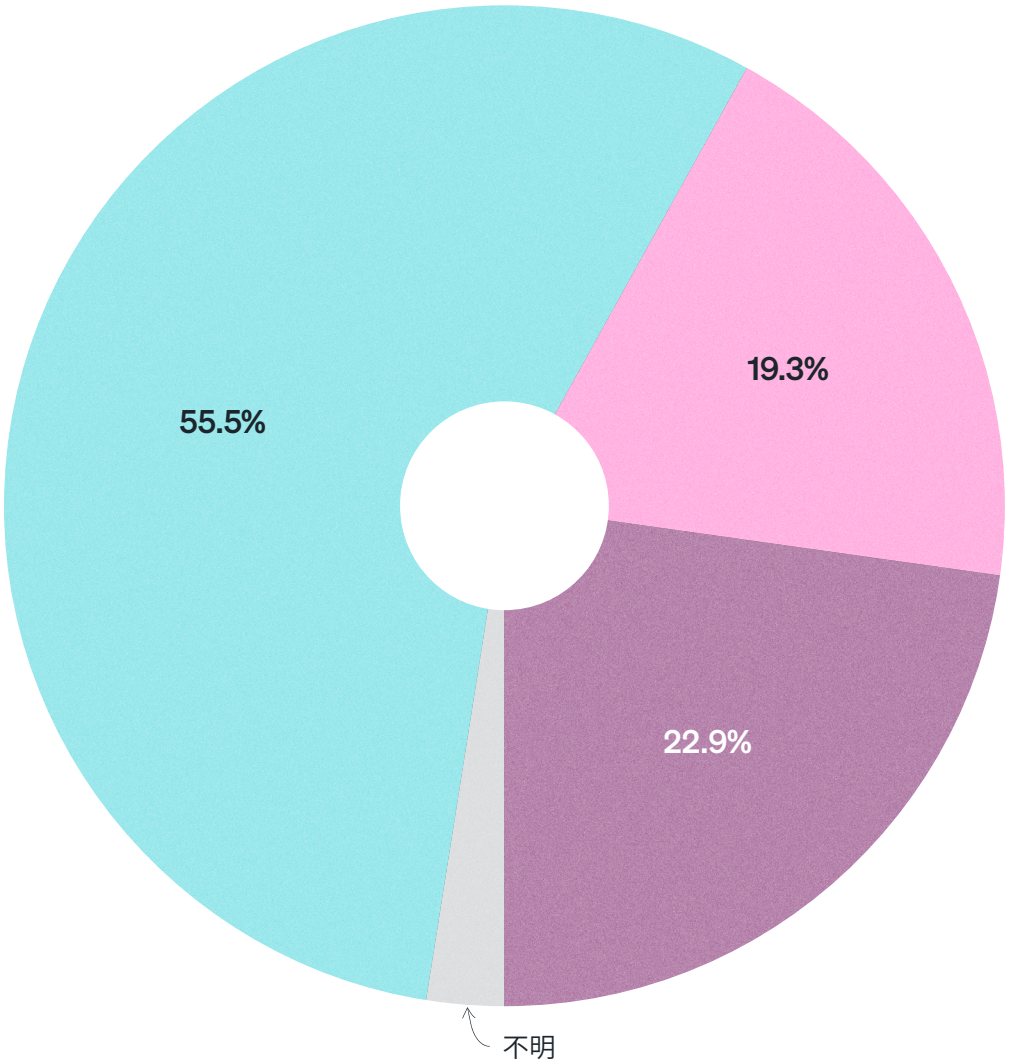
エンジニアはシステム中断への対処にかなりの時間を費やします。ただし、フルスタックオブザーバビリティやその他の要因により、エンジニアの時間が解放され、より高価値な作業に集中できるようになります。

MTTxの変化

オブザーバビリティソリューション導入以降、自社組織のシステム停止のMTTx（MTTDとMTTR）がどのように変化したかについても、調査を行いました。

MTTDの変化

MTTDについては、データによると、回答者の半数以上（56%）が、オブザーバビリティソリューションの導入以来、MTTDがある程度改善されたと回答しています。そのうち29%の回答者が25%以上改善したと回答しました。約5人に1人（19%）が変わらないと回答しました。



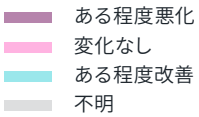
地域別の考察

南北アメリカの回答者は、オブザーバビリティを導入してからMTTDがある程度改善されたと回答する傾向がきわめて高く見られました（69%、アジア太平洋と欧州では48%）。

業界別の考察

サービス／コンサルティングの回答者は、オブザーバビリティを導入してMTTDがある程度改善されたと回答する傾向がもっとも高く見られました（65%、小売／消費者63%、医療／製薬63%、メディア／エンターテイメント60%）。

図26. オブザーバビリティ導入以降のMTTDの変化



ほとんどの回答者は、オブザーバビリティを導入後、システム停止をより迅速に検出しました。また、フルスタックオブザーバビリティの実現やより多くのベストプラクティスの導入など、いくつかの要因によりMTTDがさらに短縮されます。

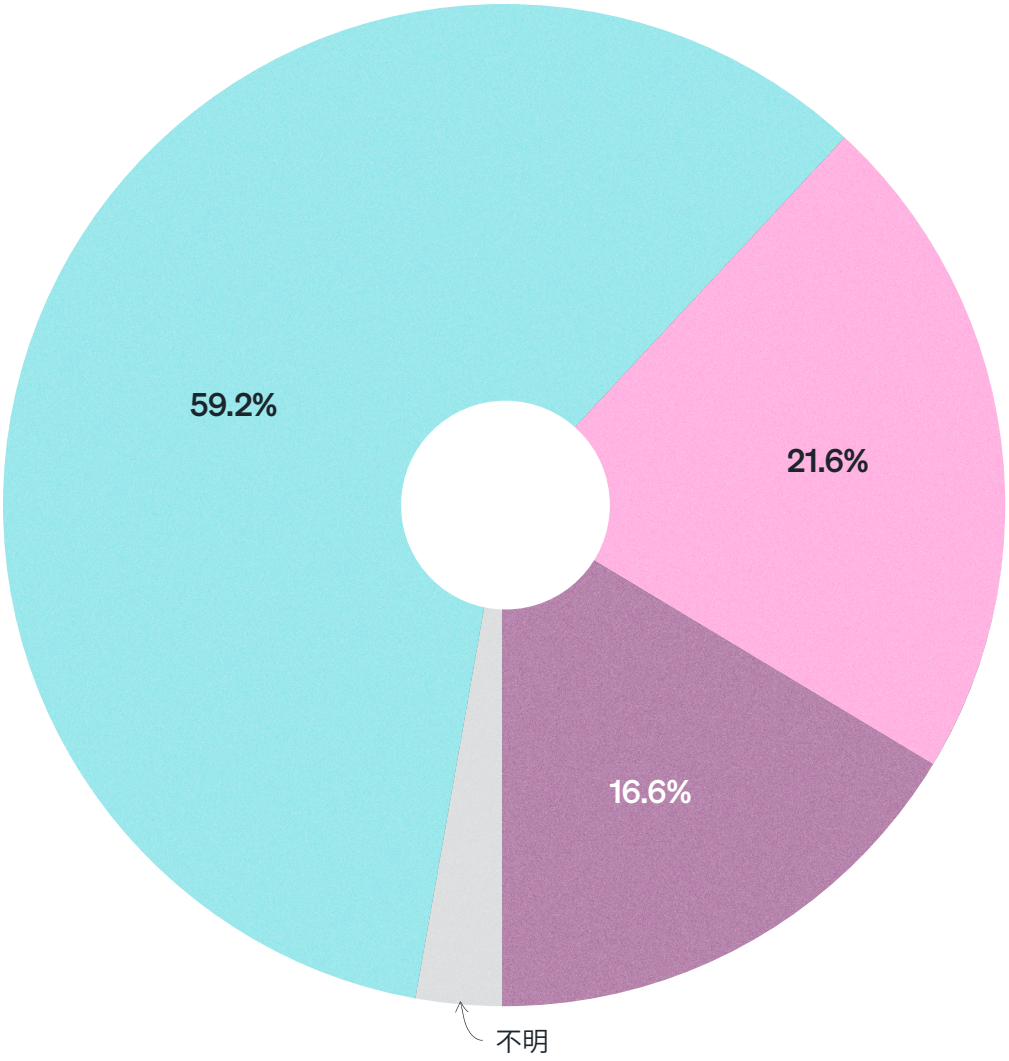
56% オブザーバビリティを導入してからMTTDがある程度改善したと回答

次の6つの要因がMTTDの改善に関連していました。

- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、MTTDがある程度改善したと回答する傾向が高くなります。たとえば、5つ以上のオブザーバビリティ関連機能を導入済みの企業は、4つ以下の企業に比べて、改善したと回答する傾向が62%高くなりました（38%に対して61%）。10個以上を導入済みの企業は、9個以下の企業に比べて、改善したと回答する傾向が44%高くなりました（48%に対して69%）。また、15個以上を導入済みの企業は、14個以下の企業に比べて、改善したと回答する傾向が34%高くなりました（54%に対して72%）。
- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現した企業は、実現しなかった企業に比べて、MTTDがある程度改善したと回答する傾向が37%高くなりました（51%に対して70%）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、MTTDがある程度改善したと回答する傾向が37%高くなりました（53%に対して72%）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した中断を検知した企業は、より手動による検知方法を使用した企業に比べて、MTTDがある程度改善したと回答する傾向が35%高くなりました（47%に対して63%）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、MTTDがある程度改善したと回答する傾向が33%高くなりました（50%に対して66%）。
- ✓ **より統合されたテレメトリーデータの保持：**より統合されたテレメトリーデータを保持している企業は、よりサイロ化されたテレメトリーデータを保持している企業に比べて、MTTDがある程度改善したと回答する傾向が15%高くなりました（55%に対して63%）。

MTTRの変化

MTTRについては、オブザーバビリティソリューションの導入以来、回答者の大多数（59%)がMTTRにある程度の改善が見られたと回答し、変わらないと答えたのは4分の1未満（22%）でした。



組織規模別の考察

小規模組織と大規模組織は、中規模組織（55%）よりもMTTRの改善が見られたと回答する傾向が高かった（それぞれ64%と61%）。

地域別の考察

南北アメリカの回答者は、オブザーバビリティを導入してからMTTRがある程度改善したと回答する傾向がきわめて高く見られました（67%、アジア太平洋59%、欧州では47%）。

業界別の考察

メディア／エンターテイメントの回答者は、オブザーバビリティを導入してからMTTRがある程度改善したと回答する傾向がもっとも高く（73%）、次いで教育（71%）、医療／製薬（66%）、サービス／コンサルティング（65%）、金融サービス／保険（62%）でした。

図27. オブザーバビリティ導入以降のMTTDの変化

- ある程度悪化
- 変化なし
- ある程度改善
- 不明

ほとんどの回答者は、オブザーバビリティを導入後、システム停止をより迅速に解決しました。また、単一のツールを使用してオブザーバビリティを実現したり、より多くのベストプラクティスを導入したりするなど、いくつかの要因によりMTTRがさらに短縮されます。

59% オブザーバビリティを導入してから MTTRがある程度改善したと回答

次の7つの要因がMTTRの改善に関連していました。

- ✓ **より多くのオブザーバビリティ関連機能の導入：**導入する機能が増えるほど、MTTRがある程度改善したと回答する傾向が高くなります。たとえば、5つ以上のオブザーバビリティ関連機能を導入済みの企業は、4つ以下の企業に比べて、改善したと回答する傾向が30%高くなりました（48%に対して63%）。10個以上を導入済みの企業は、9個以下の企業に比べて、改善したと回答する傾向が27%高くなりました（54%に対して69%）。また、15個以上を導入済みの企業は、14個以下の企業に比べて、改善したと回答する傾向が23%高くなりました（58%に対して71%）。
- ✓ **オブザーバビリティのベストプラクティスの導入：**5つ以上のオブザーバビリティのベストプラクティスを導入した企業は、4つ以下の企業と比べて、MTTDがある程度改善したと回答する傾向が36%高くなりました（56%に対して77%）。
- ✓ **フルスタックオブザーバビリティの実現：**フルスタックオブザーバビリティを実現した企業は、実現しなかった企業に比べて、MTTRがある程度改善したと回答する傾向が23%高くなりました（56%に対して69%）。
- ✓ **より多くの種類のビジネス関連データをテレメトリーデータと統合：**5種類以上のビジネス関連データをテレメトリーデータと統合した企業は、1〜4種類のデータを統合した企業に比べて、MTTRがある程度改善したと回答する傾向が20%高くなりました（57%に対して67%）。
- ✓ **より統合されたテレメトリーデータの保持：**より統合されたテレメトリーデータを保持している企業は、よりサイロ化されたテレメトリーデータを保持している企業に比べて、MTTRがある程度改善したと回答する傾向が14%高くなりました（57%に対して65%）。
- ✓ **オブザーバビリティによる中断の検知：**オブザーバビリティにより中断を検知した企業は、より手動による検知方法を使用した企業に比べて、MTTRがある程度改善したと回答する傾向が13%高かった（55%に対して63%）。
- ✓ **オブザーバビリティに1つのツールを使用：**オブザーバビリティに1つのツールを使用している企業は、複数のツールを使用している企業に比べて、MTTRがある程度改善したと回答する傾向が11%高かった（59%に対して65%）。

機能別にみたMTTx低下のインフルエンサー

本データは、平均よりも低いMTTDおよびMTTRと、11のオブザーバビリティ関連機能の間に正の相関があることを示しています。

- **ビジネスオブザーバビリティとエラー追跡は、有意水準5%の範囲で統計的に有意です**
- アラートとダッシュボードは、3年連続で有意な関連性を示しています（2022〜2024年）
- エラー追跡とログ管理は、2年連続で有意な関連性を示しています（2023年と2024年）
- APM、データベース監視、およびセキュリティ監視は、2年連続で有意な関連性を示しています（2022年と2024年）
- AI監視（今年の新機能）、ブラウザ監視、ビジネスオブザーバビリティ（今年の新機能）、ネットワーク監視は、今年初めて有意な関連性を示しました

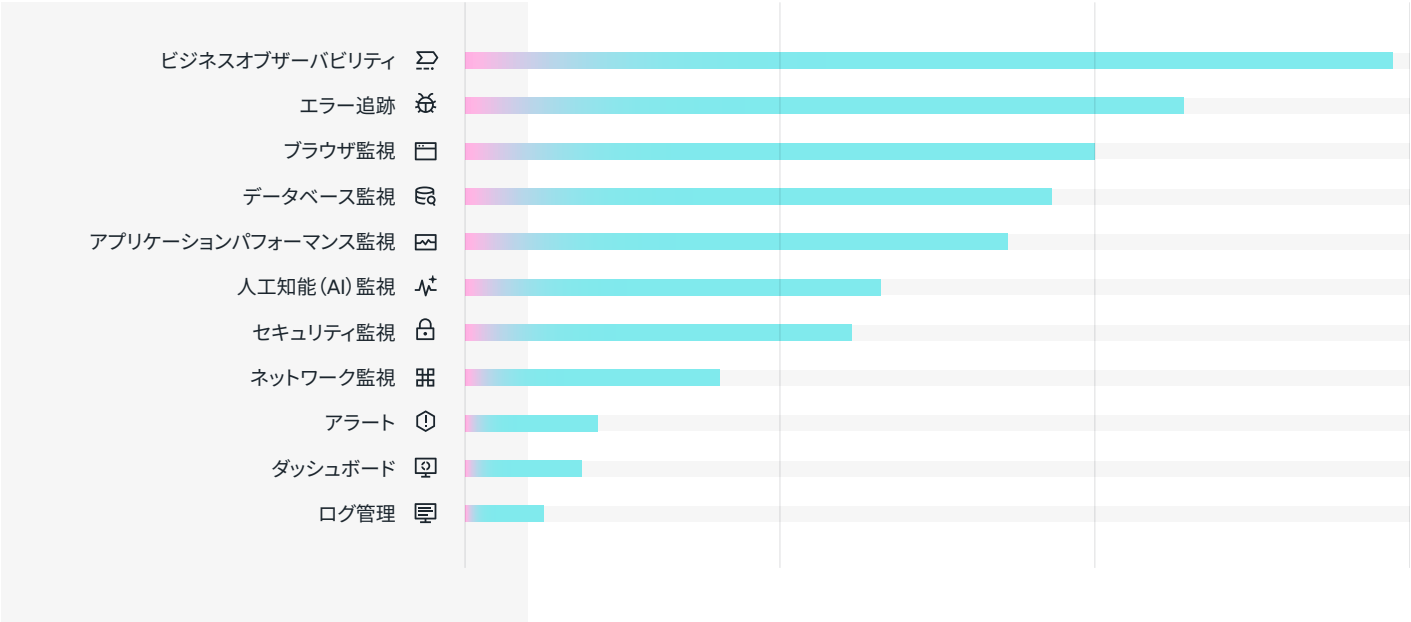


図28. 平均より低いMTTDとMTTRに関連するオブザーバビリティ関連機能

MTTxの削減を目指している組織は戦略的オブザーバビリティ関連機能、特にビジネスオブザーバビリティとエラー追跡の導入を優先することで、確率を高める可能性があります。

ダウンタイムの削減

回答者の3分の1以上が、根本原因の分析（RCA）とインシデント後のレビュー（37%）、DORA（DevOps Research and Assessment）メトリクスの監視（34%）、ゴールデンシグナルの監視（33%）を行っていると同時に、MTTxの追跡、レポート作成と奨励（33%）が、組織のダウンタイムの削減に役立ったと回答しています。

約4分の1が、サービスレベル管理の導入（28%）、組織全体にオブザーバビリティデータへのアクセス提供（26%）、ダッシュボードを使った詳細なパフォーマンスと健全性KPIの報告（22%）、重大なインシデントに対する自動アラート設定（22%）が、組織のダウンタイムの削減に役立ったと回答しています。

37%

根本原因の分析とインシデント後のレビューの実施がダウンタイムの削減に役立ったと回答

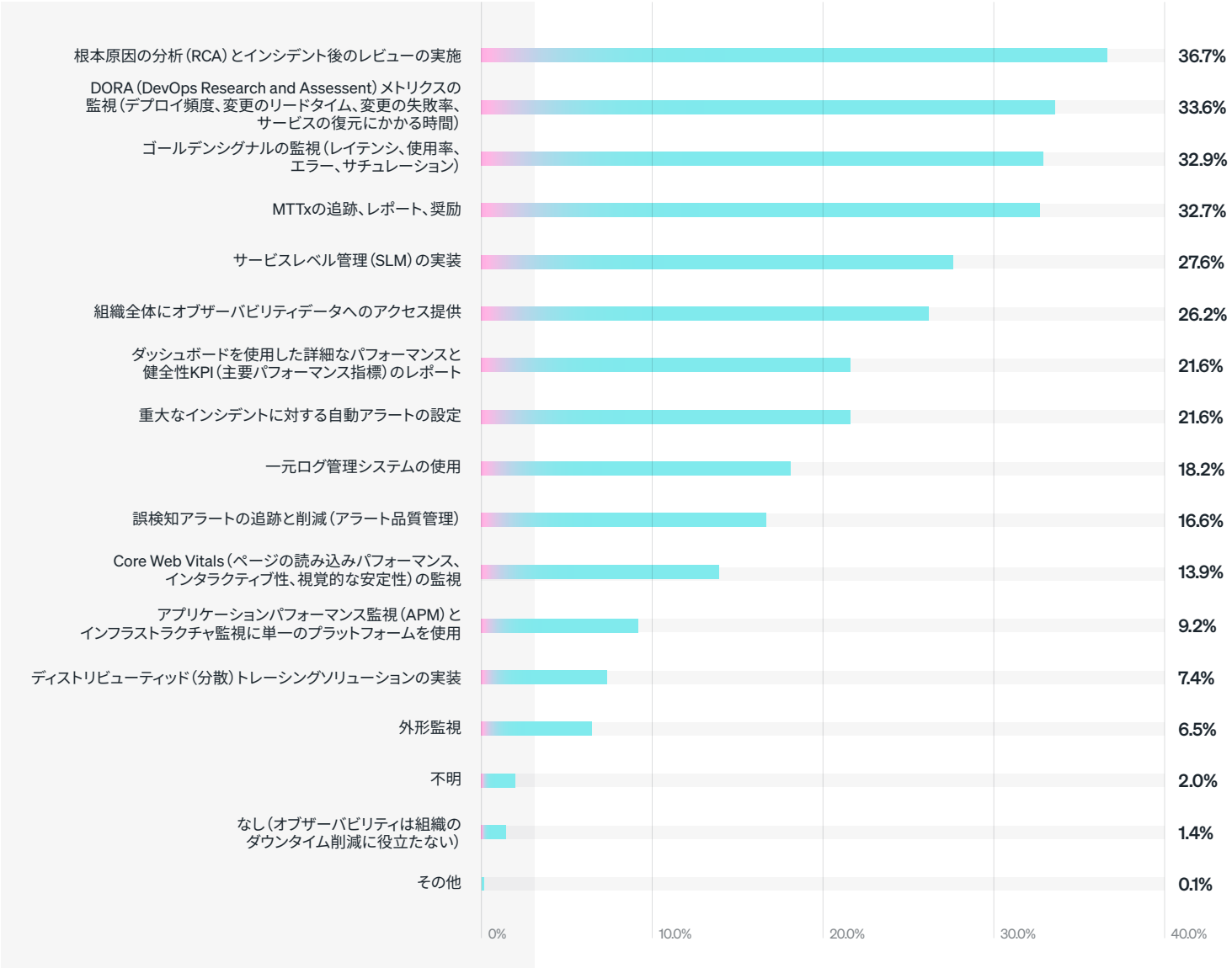


図29. 組織のダウンタイム削減に貢献したオブザーバビリティの実践

開発者とエンジニアは、稼働時間と信頼性を向上させるための対策を積極的に講じています。

組織規模別の考察

大規模組織の回答者は、中規模と小規模組織よりも、RCAとインシデント後のレビューの実施、DORAメトリクスの監視、ゴールデンシグナルの監視を行うと回答する傾向が顕著に高く見られました。

地域別の考察

アジア太平洋の回答者は、DORAメトリクスの監視がダウンタイムの削減に役立ったと回答する傾向が非常に高く見られました。南北アメリカの回答者は、ゴールデンシグナルを監視し、一元ログ管理システムを使用していると回答する可能性がきわめて高く見られました。

業界別の考察

半数近くが、DORAメトリクスの監視がダウンタイム削減に役立ったと回答：（メディア／エンターテイメント48%、テレコミュニケーション47%、政府機関44%、金融サービス／保険42%）。3分の1以上が、ゴールデンシグナルの監視がダウンタイム削減に役立ったと回答：（教育39%、金融サービス／保険39%、小売／消費者37%、メディア／エンターテイメント35%、テレコミュニケーション35%、エネルギー／ユーティリティ35%、工業／原料／製造33%）。

オブザーバビリティの利点

このセクションでは、オブザーバビリティの主な利点、フルスタックオブザーバビリティを実現する利点、組織がオブザーバビリティへの年間投資から得ている総価値、オブザーバビリティの投資利益率（ROI）の中央値について説明します。

ハイライト：

58%

オブザーバビリティへの投資から年間総額500万ドル以上を受け取っていると回答

34%

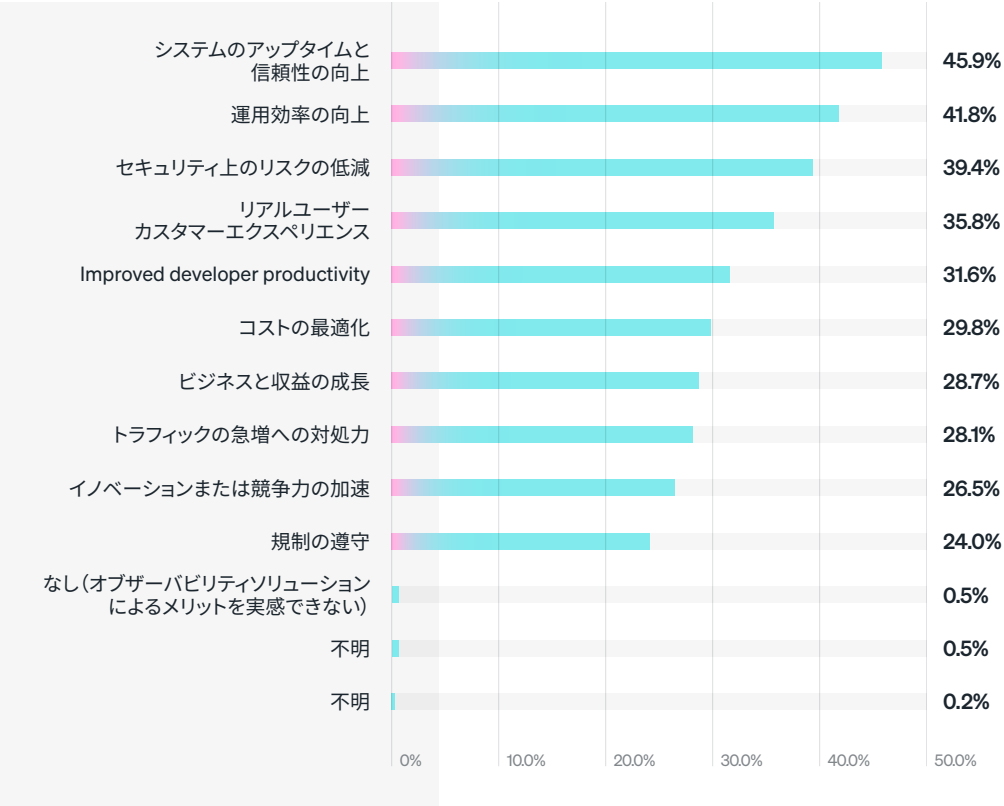
オブザーバビリティへの投資から年間1,000万ドル以上の価値を得ていると回答

28%

AIOps機能を導入した際、オブザーバビリティへの投資からより高い年間価値を得たと回答

オブザーバビリティの主な利点

回答者は、現在のオブザーバビリティソリューションの結果として確実に利点を感じており、ほぼ半数（46%）がシステムの稼働時間と信頼性の向上を挙げています。3分の1以上が、運用効率の向上（42%）、セキュリティリスクの軽減（39%）、実際のユーザー（顧客）体験の向上（36%）を挙げています。3分の1近く（32%）が、開発者の生産性の向上、コストの最適化（30%）、ビジネスと収益の成長（29%）、トラフィックの急増への対応力（28%）が見られたと回答しています。



フルスタックオブザーバビリティを実現した組織は、実現していない組織よりも以下のように多くの利点を得ています。

- システムの稼働時間と信頼性が51%向上する可能性が高い（41%に対して62%）
- 運用効率が向上する可能性が44%高い（38%に対して55%）
- コストを最適化する可能性が30%高い（28%に対して36%）
- セキュリティリスクを軽減する可能性が26%高い（37%に対して47%）
- 実際のユーザー（顧客）体験が向上する可能性が15%高い（35%に対して40%）

組織規模別の考察

一般に、大規模組織の回答者はオブザーバビリティの利点をそれぞれ挙げる傾向が高く、次いで中規模組織、小規模組織と続きます。

地域別の考察

南北アメリカ大陸の回答者は、一般的に恩恵を経験したと回答する可能性がもっとも高く見られました。アジア太平洋の回答者は、トラフィックの急増、ビジネスと収益の成長、イノベーションや競争上の優位性の加速に対応する能力を挙げる可能性がもっとも高く見られました。欧州の回答者は、コストの最適化と規制遵守を挙げる可能性がもっとも高く見られました。

業界別の考察

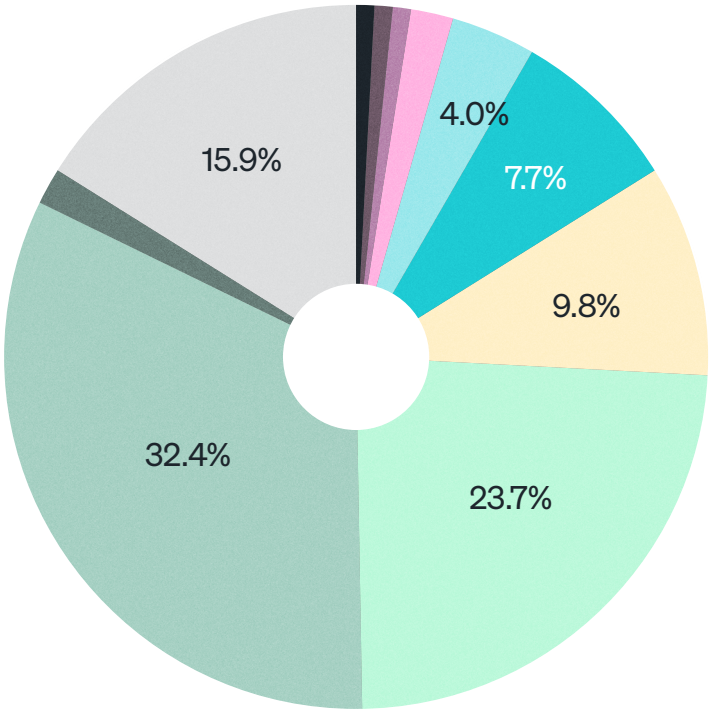
ほとんどの業界では、システムの稼働時間と信頼性の向上が最優先の選択肢でした。ただし、メディア／エンターテイメント（46%）、IT（45%）、エネルギー／ユーティリティ（39%）では、運用効率の向上がトップの選択肢でした。教育業界の最大の選択肢はセキュリティリスクの軽減（54%）でした。

図30. オブザーバビリティソリューションにより得られる利点

オブザーバビリティの総価値

組織がオブザーバビリティへの投資から得た年間価値の中央値は815万ドルでした。半数以上 (58%) がオブザーバビリティへの投資から年間500万ドル以上の価値を得ていると回答し、3分の1 以上 (34%) が1,000万ドル以上の価値を得ていると回答しました。

5つ以上のオブザーバビリティ関連機能を導入済みの企業は、1〜4つを導入した企業（793万ドル）よりも、オブザーバビリティへの投資からより高い年間価値 (820万ドル) を得ていました。



さらに、次のオブザーバビリティ関連機能の導入に関連して、より高い年間合計額が得られました。

- AIOps (ITオペレーション向け人工知能) 機能を導入済みの企業では28%高い (導入していない企業では770万ドルに対して985万ドル)
- 外形監視を導入済みの企業では17%高い (導入していない企業では783万ドルに対して915万ドル)
- AI監視を導入済みの企業では14%高い (導入していない企業では765万ドルに対して875万ドル)
- Kubernetes (K8) の監視を導入済みの企業では14%高い (導入していない企業では793万ドルに対して900万ドル)
- 機械学習 (ML) モデル監視を導入済みの企業では5%高い (導入していない企業では805万ドルに対して843万ドル)
- モバイル監視を導入済みの企業では3%高い (導入していない企業では813万ドルに対して835万ドル)

組織規模別の考察

大規模組織の回答者が年間得た金額がもっとも高く (915万ドル)、次いで中規模組織 (815万ドル)、小規模組織 (265万ドル) でした。

地域別の考察

アジア太平洋の回答者は、欧州 (705万ドル) や南北アメリカ (540万ドル) の回答者と比較して、年間で得られる価値の中央値 (1,008万ドル) がはるかに高いと報告されています。

業界別の考察

オブザーバビリティから得た年間中央値がもっとも高かった業界は、金融サービス／保険 (1,015万ドル)、政府機関 (1,008万ドル)、メディア／エンターテイメント (1,000万ドル) でした。

図31. オブザーバビリティソリューションにより得られる利点

- 0ドル (オブザーバビリティ投資から価値を得ていない)
- 1ドル以上10万ドル未満
- 10万ドル以上25万ドル未満
- 25万ドル以上50万ドル未満
- 50万ドル以上100万ドル未満
- 100万ドル以上250万ドル未満
- 250万ドル以上500万ドル未満
- 500万ドル以上1,000万ドル未満
- 1,000万ドル以上2,000万ドル未満
- 2,000万ドル以上
- 不明

組織はオブザーバビリティへの投資から大きな価値を得ています。この合計値には、ダウンタイムの回避、ツールの最適化、従業員の生産性など、すべての利点が含まれます。

オブザーバビリティの投資利益率（ROI）

ROIの中央値の計算は、年間のオブザーバビリティ支出と得た年間価値の推定に基づいています。

全回答者のオブザーバビリティに対するROIの中央値は**4倍**（295%）でした。言い換えると、1ドル支出するごとに、回答者は4ドルの価値を得ていると考えられます。

地域別の考察

南北アメリカの回答者のROI中央値（3.8倍）は、アジア太平洋または欧州の回答者（両方とも4倍）よりもわずかに低く見られました。

業界別の考察

ROIの中央値がもっとも高かったのは政府機関（4.1倍）で、次いでテレコミュニケーション、小売／消費者、IT、金融サービス／保険（いずれも4倍）でした。教育の回答者のROI中央値がもっとも低く（3.7倍）、次いでエネルギー／ユーティリティ、医療／製薬（両方とも3.8倍）でした。

「投じた費用に対してどれくらいの利益が得られるかということは、常に注目されています。本当に複雑な環境を維持しなければならないことは認めますが、ROIも考慮しなければなりませんし、BtoCのような環境であることを考えると、どこまで妥協してもいいのかとも思います。つまり、私たちは顧客、小売側と向き合っているということです。稼働時間の回復力は非常に重要で、ダウンタイムやMTTRにさらに時間がかかることについては妥協できません。」

ITインフラストラクチャ担当シニアディレクター
米国大手フィンテック企業

オブザーバビリティの未来

このセクションでは、来年と今後2〜3年間のオブザーバビリティの導入計画とデータ統合の計画、投資したオブザーバビリティから最大の価値を得るために、組織が来年実行を計画するであろう方策について考察します。

ハイライト：

83%
来年までに6つ以上の
オブザーバビリティ関連機能を
導入予定

59%
今後1〜3年以内に、5種類以上の
ビジネス関連データを
テレメトリーデータと統合予定

41%
来年中にオブザーバビリティツール
統合を予定

オブザーバビリティの導入計画

既存のオブザーバビリティの導入に関する質問に加え、来年と今後2〜3年の導入計画について、調査回答者に尋ねました。

2025年については、大部分（91%）が来年中に1つ以上の新機能の導入を考えており、半数以上（59%）は1〜5つの機能を導入、3分の1以上（37%）は7つ以上の機能を導入すると考えています。

1年間の概要を見ると、セキュリティ監視やネットワーク監視などの導入が予定される機能が80%以上となっています。3分の1以上が、AIOps（ITオペレーション向け人工知能）機能（39%）、AI監視（36%）、機械学習（ML）モデル監視（34%）、ディストリビューティッド（分散）トレーシング（33%）、サーバーレス監視（33%）を導入すると予想されます。

組織規模別の考察
小規模組織（64%）は、中規模組織（60%）や大規模組織（58%）よりも、来年5つ以上のオブザーバビリティ関連機能を導入する可能性が高くなります。

地域別の考察
アジア太平洋の組織（74%）は、欧州（45%）や南北アメリカ（49%）よりも、来年までに5つ以上のオブザーバビリティ関連機能の導入を予定しています。

業界別の考察
メディア／エンターテイメントの回答者の4分の3以上（77%）が、他のどの業界よりも多く、来年までに5つ以上のオブザーバビリティ関連機能の導入を予定しています。

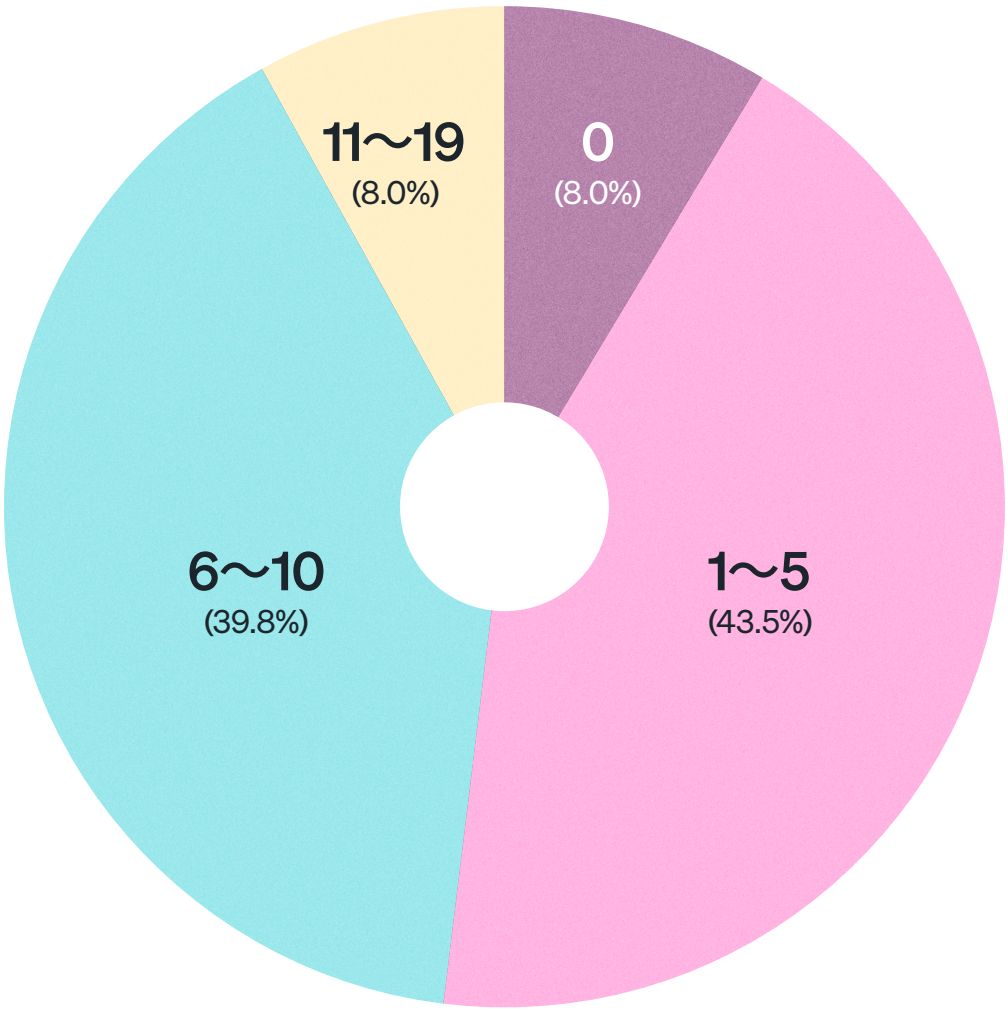


図32. 来年計画されているオブザーバビリティ関連機能の数

- 0個の新規ビジネスオブザーバビリティ関連機能
- 1〜5個の新規ビジネスオブザーバビリティ関連機能
- 6〜10個の新規ビジネスオブザーバビリティ関連機能
- 11〜19個の新規ビジネスオブザーバビリティ関連機能

2027年半ばまでに、75%以上の回答者が19のオブザーバビリティ関連機能のそれぞれについて導入を計画しています。本調査において、これらのオブザーバビリティ関連機能の導入を計画していない回答者はごくわずかでした（最大13%）。

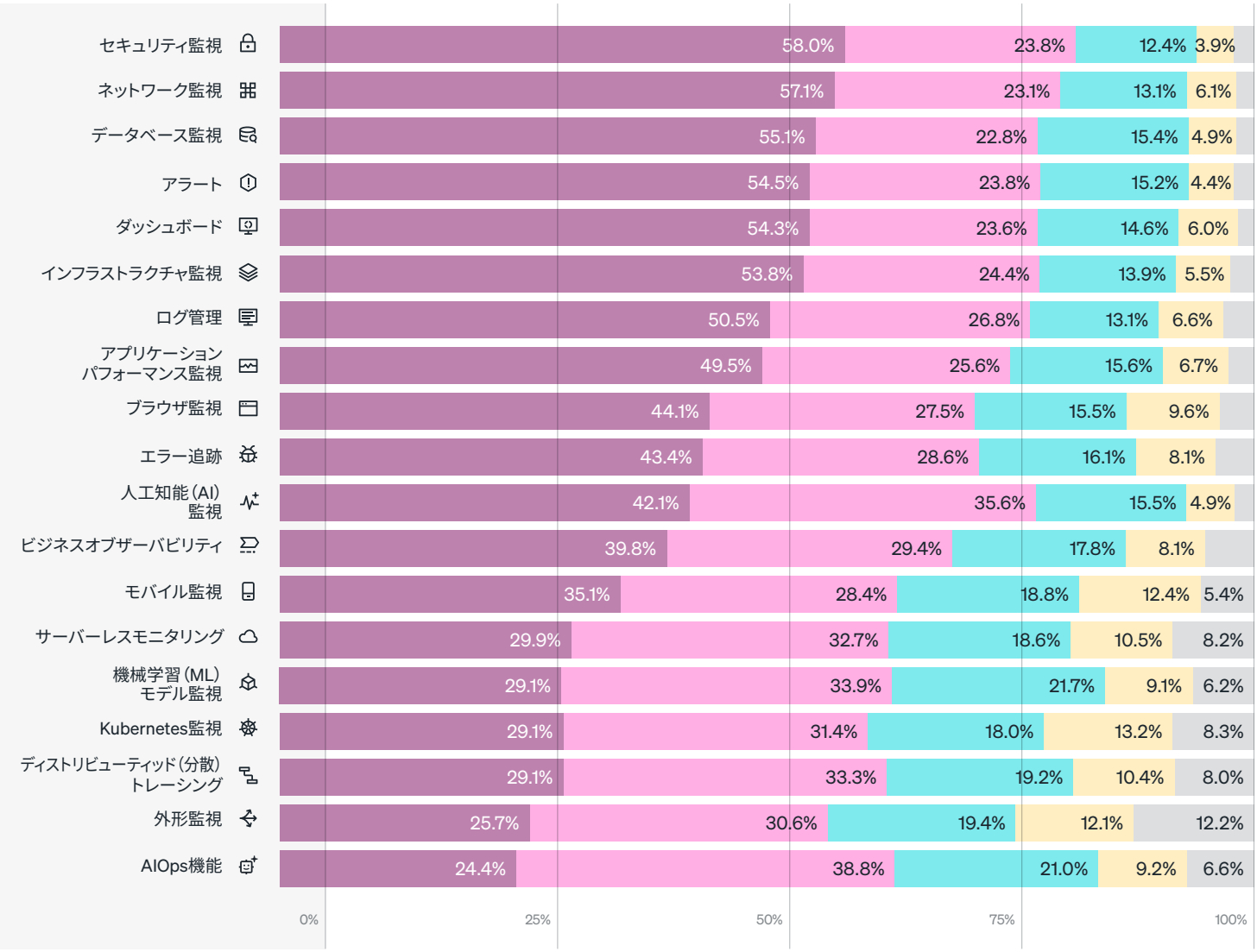


図33. 2024年から2027年のオブザーバビリティ関連機能の導入概要

- 導入済み
- 現在は導入していないが、来年には追加予定
- 現在は導入していないが、今後2〜3年以内に追加予定
- 現在は導入していないが、追加予定もない
- 不明

データの統合計画

真のビジネスオブザーバビリティを実践するには、組織はビジネス関連データをテレメトリーデータ（MELT）と統合する必要があります。現在統合されているデータの種類は既に確認したので、今後1〜3年以内に統合する予定のビジネス関連データの種類を確認してみましょう。

- 約半数が、今後1〜3年以内に各データの種類を統合する予定
- 大多数（89%）が1つ以上のデータの種類を統合する予定、59%は5つ以上を統合する予定ビジネス関連データとテレメトリーデータの統合予定がないと回答したのは11%のみ
- これらの結果は、2027年までに89%が5つ以上のビジネス関連データの種類を統合し、57%が10種類すべてを統合することを表しています。

地域別の考察

アジア太平洋の回答者は、今後1〜3年以内に5種類以上のビジネス関連のテレメトリーデータを統合する予定であると回答する傾向がもっとも高かった（南北アメリカ50%、欧州46%に対して72%）

業界別の考察

メディア／エンターテイメントの回答者は、今後1〜3年以内に5種類以上のビジネス関連のテレメトリーデータを統合する予定であると回答する傾向がもっとも高く（75%、エネルギー／ユーティリティ72%、テレコミュニケーション66%）IT回答者がもっとも低く（45%）、医療／製薬（49%）、教育（52%）でした。

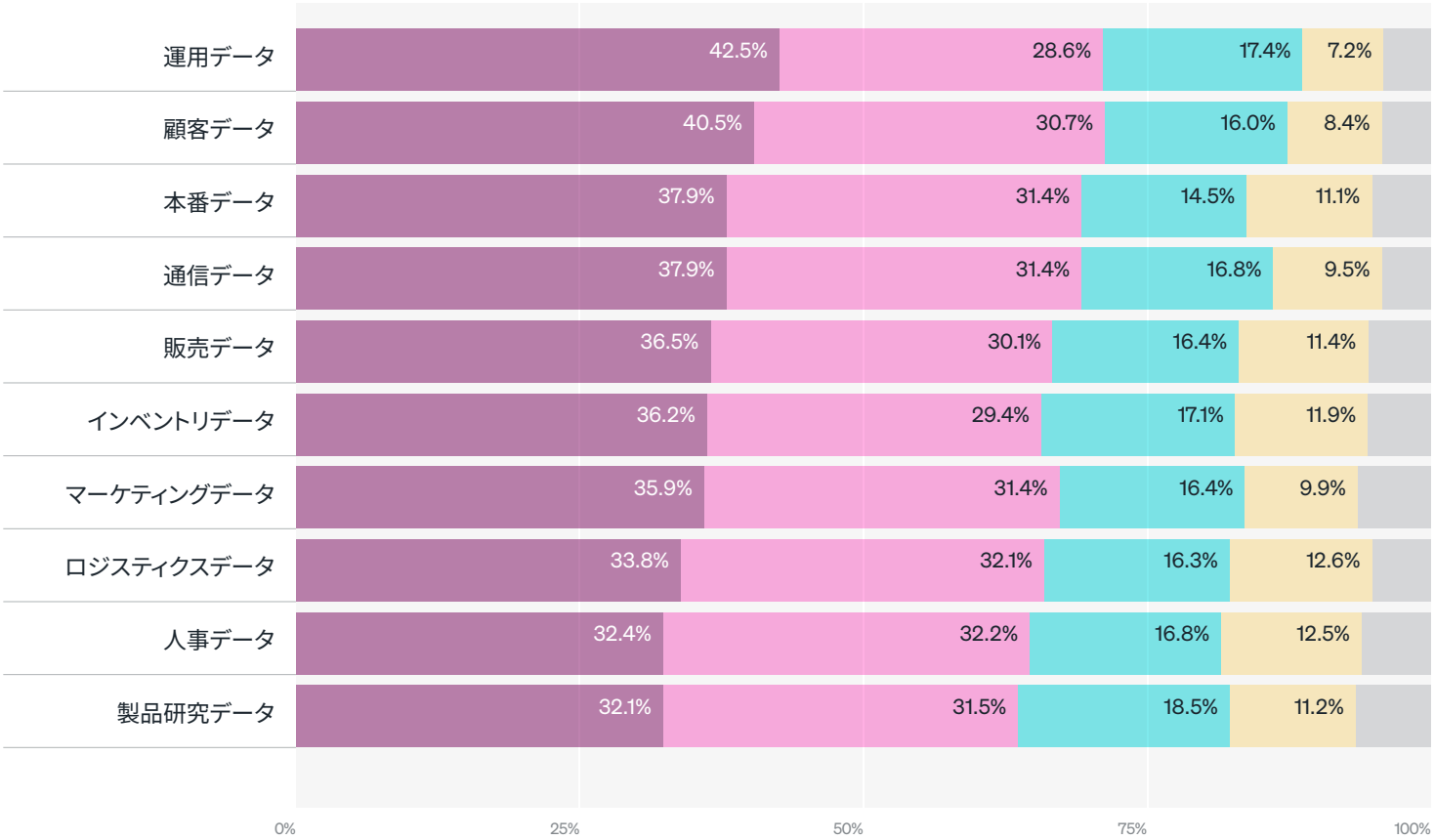


図34. 現在統合されている、または2027年までにテレメトリーデータと統合予定のビジネス関連データの種類

- テレメトリーデータと統合済み
- 現在、テレメトリーデータと統合していないが、来年には統合予定
- 現在、テレメトリーデータと統合していないが、今後2〜3年以内に統合予定
- 現在、テレメトリーデータと統合していないが、統合予定もない
- 不明

59% 今後1〜3年以内に、5種類以上のビジネス関連データをテレメトリーデータと統合予定

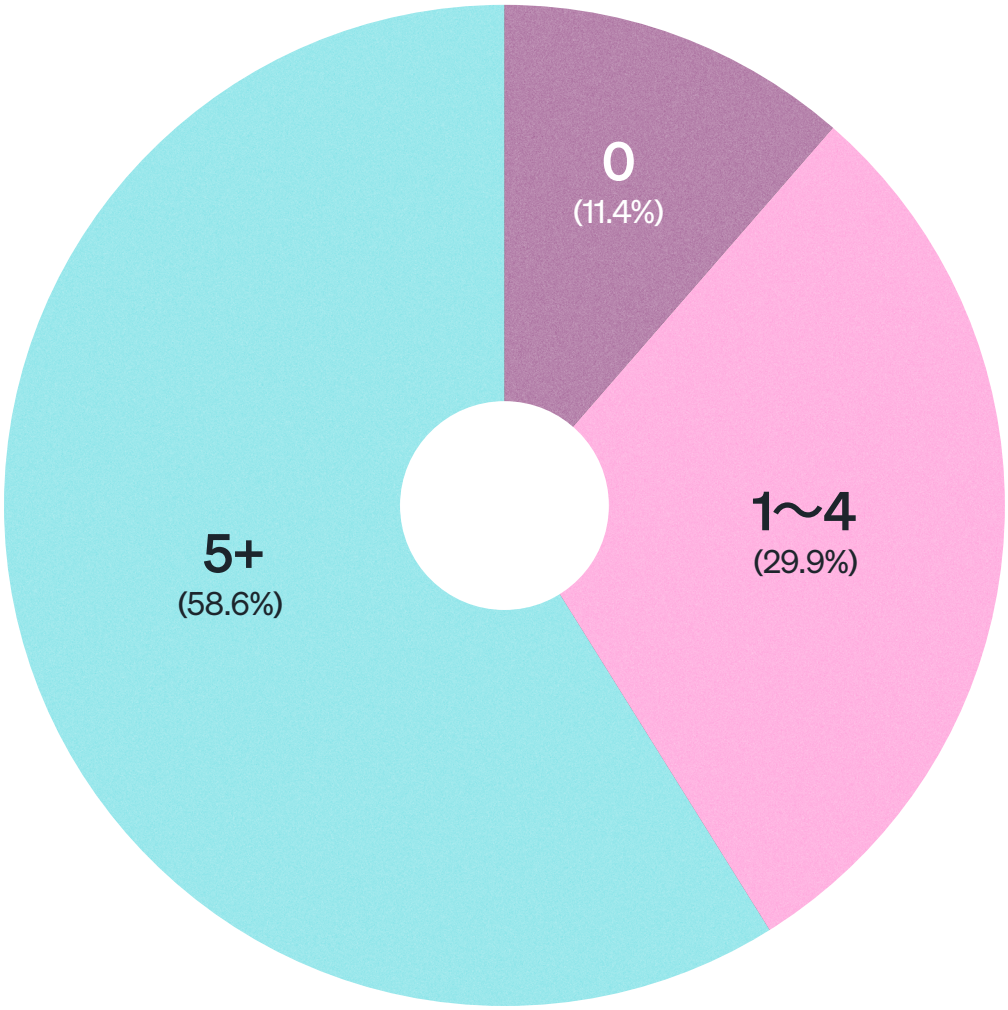


図35. 今後1〜3年間のテレメトリーデータ統合計画

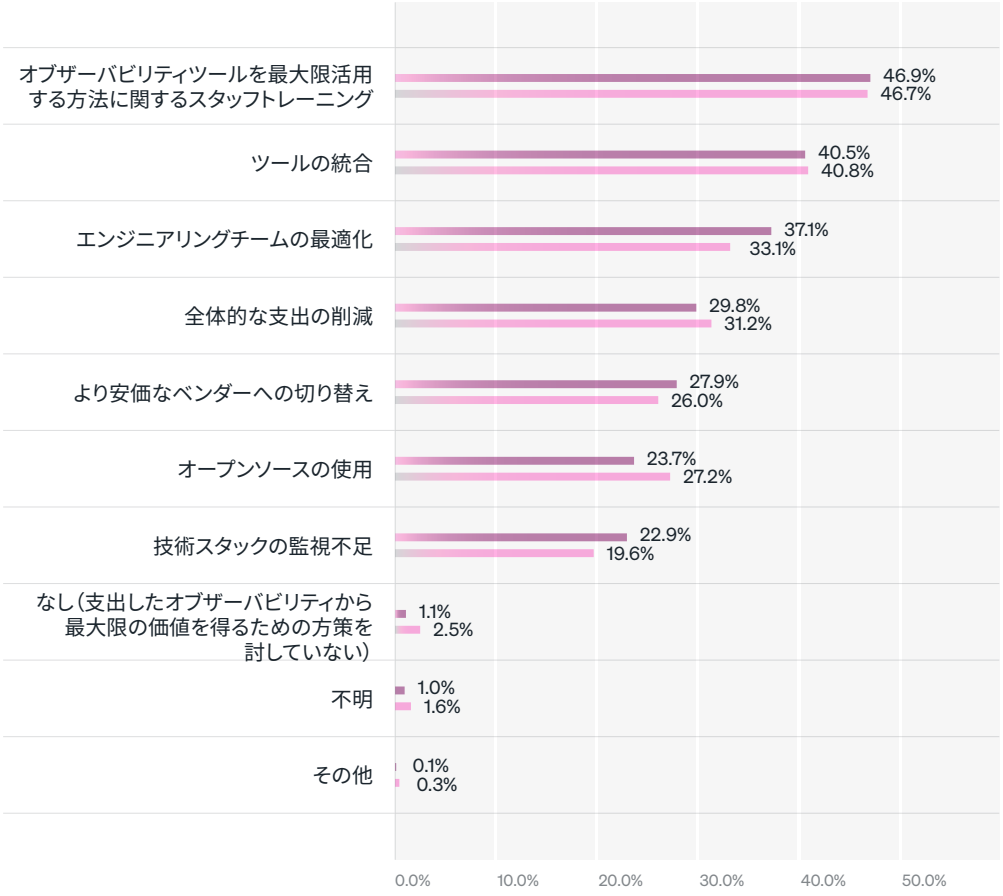
- 0個のビジネス関連データの種類
- 1〜4個のビジネス関連データの種類
- 5個以上のビジネス関連データの種類

今後数年間で、組織はオブザーバビリティの実践に統合するデータの種類を多様化することを予定しています。

オブザーバビリティの価値を最大化する計画

オブザーバビリティから最大の価値を得るため、組織が実施するであろう方策は何かについて調査を行いました。調査の結果は以下の通りです。

- 約半数（47%）が、オブザーバビリティツールを最大限活用する方法に関するスタッフトレーニングを計画
- 約5人に2人（41%）が、ツール統合を検討
- 3分の1以上（37%）がエンジニアリングチームの規模の最適化を計画
- ほぼ3分の1（31%）が全体的な支出の削減を計画
- 残りは、より価格を抑えたベンダーへの切り替え（28%）、オープンソースの使用（24%）、または技術スタックの監視を削減（23%）を計画
- 支出したオブザーバビリティから最大の価値を得るための方策を検討していないとの回答はわずか1%



地域別の考察

アジア太平洋の回答者は、今後1〜3年以内に5種類以上のビジネス関連のテレメトリーデータを統合する予定であると回答する傾向がもっとも高かった（南北アメリカ50%、欧州46%に対して72%）

業界別の考察

メディア／エンターテイメントの回答者は、今後1〜3年以内に5種類以上のビジネス関連のテレメトリーデータを統合する予定であると回答する傾向がもっとも高く（75%、エネルギー／ユーティリティ72%、テレコミュニケーション66%）IT回答者がもっとも低く（45%）、医療／製薬（49%）、教育（52%）でした。

図36. 現在統合されている、または2027年までにテレメトリーデータと統合予定のビジネス関連データの種類

2024年の回答者
2023年の回答者

「ほとんどの場合、私は単一のツールだけを使用したいと考えています。こうすることで、社員全員が全体的に統一された方法で報告することになります。」

インドの大規模小売／消費者企業、
エンジニアリング担当シニアマネージャー

41%
来年中にオブザーバビリティツール統合を予定

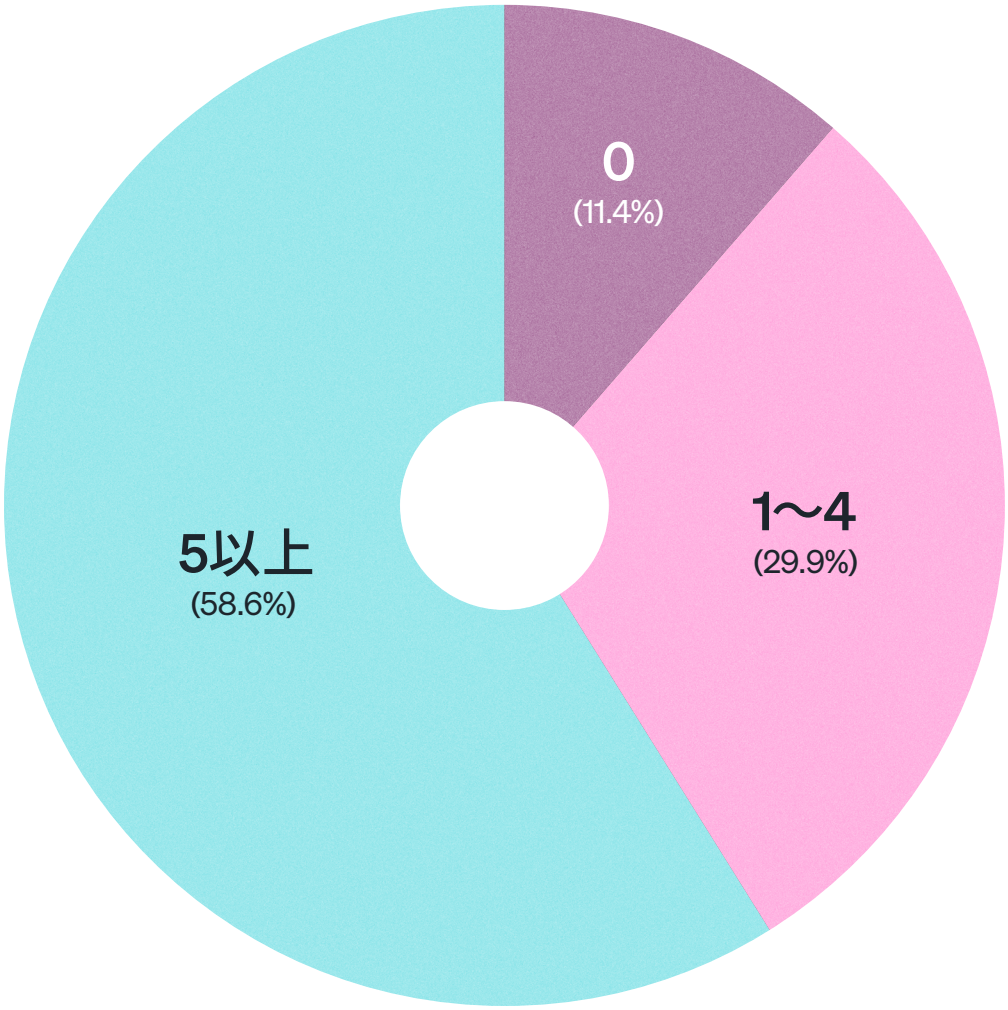


図37. 今後1〜3年間のテレメトリーデータ統合計画

- 0個のビジネス関連データの種類
- 1〜4個のビジネス関連データの種類
- 5個以上のビジネス関連データの種類

今後数年間で、組織はオブザーバビリティの実践に統合するデータの種類を多様化することを予定しています。

まとめ

オブザーバビリティの利点は明確になりつつあり、調査対象者のほぼ半数（46%）がシステムのアップタイムと信頼性の向上を最大の利点として挙げています。その他の主な利点には、運用効率の向上（42%）、セキュリティリスクの軽減（39%）、顧客体験の向上（36%）が含まれます。組織はまた、開発者の生産性、コストの最適化、ビジネス成長、トラフィックの急増への対応力の向上を報告しています。特に、フルスタックオブザーバビリティを実現した企業では、システムの稼働率が向上する可能性が51%高く、運用効率が向上する可能性が44%高いなど、さらに大きな利点が得られました。

財務上の影響に関して、組織がオブザーバビリティへの投資から得た年間価値の中央値は815万ドルで、回答者の半数以上が年間価値500万ドル以上と報告しています。5つ以上のオブザーバビリティ関連機能を導入した企業は、さらに高い収益を実現し、年間平均で820万ドルに達しました。AIOps（ITオペレーション向け人工知能）や外形監視などの特定のオブザーバビリティ機能は、得られた合計価値をさらに拡大し、これらのテクノロジーを導入している組織は、導入していない組織に比べて年間価値が最大28%高くなりました。

フルスタックオブザーバビリティ、統合されたテレメトリーデータ、単一のオブザーバビリティプラットフォームを備えた企業は、システム停止の発生が著しく少なく、分断化またはサイロ化されたオブザーバビリティの実践を行っている企業よりも年間停止が最大77%削減した企業もありました。

本レポートについて

New Relicは、Enterprise Technology Research（ETR）とパートナーを組み、今回が第4回となる年次*オブザーバビリティ予測*レポート作成に向けて調査と分析を実施しました。

新たな試み

ブラジルを対象に加え、地域的分布を更新しました。質問項目について、昨年度の質問項目を多用して対前年比（YoY）の傾向比較を行い、同時に7つの新規項目を追加してさらなる知見を得ました。

業界については、メディア／エンターテイメントを分離し、ITをテレコミュニケーションから分離し、不特定のものを削除しました。

人工知能（AI）監視とビジネスオブザーバビリティという2つのオブザーバビリティ性能を追加し、本年度のレポートで対象となるオブザーバビリティ性能の総数が19になりました。また、より明確にするために、調査回答者に各オブザーバビリティ関連機能の簡単な定義を提供し、これは、新興地域や競合地域では特に必要であると考えられていました。これらの定義を提供することで、本質的に、調査回答者の各性能についての解釈を制約していました。

調査には、システム停止時のビジネス影響のレベル（低、中、高）ごとに、ダウンタイムの時間あたりの平均収益コストに関するセクションを含めました。

通貨、時間、数量に関連するすべての質問の回答形式を、範囲ではなくスライダーに更新しました。スライダーを使用すると、調査回答者がより正確な金額を選択できるようになり、これを基に質問に対する全回答者の中央値を表にしました。オブザーバビリティ年間支出の中央値、年間ダウンタイムの中央値、年間のシステム停止コストの中央値、オブザーバビリティへの投資による年間合計価値の中央値、サービス中断への対処に費やしたエンジニアリング時間の中央値、投資利益率（ROI）の中央値などの表を作成しました。

平均復旧時間（MTTR）に加えて、オブザーバビリティソリューションを導入して以来、組織のサービス中断の平均検出時間（MTTD）がどのように変化したかについて、調査回答者に尋ねました。

定義

本レポートで使用される一般的な用語と概念は、以下のように定義されています。

オブザーバビリティ

調査回答者においては、バイアスを避けるため、オブザーバビリティについての定義を行いませんでした。

オブザーバビリティ（可観測性）により、組織はシステムがどのように機能しているかを測定し、アウトプットされるデータにもとづき問題やエラーを特定できるようになります。これらのデータは、テレメトリーデータ（メトリクス、イベント、ログ、トレース：MELT）と呼ばれています。オブザーバビリティとは、さまざまな役割のための知見を明らかにし、顧客体験やサービスに影響するアクションを即座に実行するために、システムを計装化することです。また、オブザーバビリティは、アップタイムとパフォーマンス向上のため、データの収集、分析、変更、相関付けを行います。

オブザーバビリティが達成されると、さまざまなソースからの全データが結合したリアルタイムビューが、理想的には1か所で実現します。チームはそこで、より迅速なトラブルシューティングと問題解決に向けて連携し、問題の発生を防ぎ、運用効率を確保し、最適化された顧客およびユーザー体験と競争優位性を高める高品質なソフトウェアを開発することができます。

ソフトウェアエンジニアリング、開発、サイト信頼性エンジニアリング、運用、その他の各チーム、さらに経営者やエグゼクティブは、オブザーバビリティを使用して、複雑なデジタルシステムの挙動を理解し、データから知見を導きます。オブザーバビリティにより、より迅速に問題を特定し、根本原因を理解してインシデントにすばやく簡潔に対応し、ビジネス成果に合わせてデータをプロアクティブに調整できます。

オブザーバビリティの一部である監視は、一連の条件（既知の未知）として表現される、これまでの経験にもとづいた環境内の問題を特定するために組織に使用されます。組織は、監視によってこれらの条件に対応できるようになり、潜在的な問題の数と複雑さが限定される状況において問題の解決を導くことができます。

組織は、想定外のことがなぜ（何が、いつ、どのように、に加えて）起こったかを判断するために、オブザーバビリティを使用します。特に、問題の潜在的範囲や、システムとサービスのインタラクションが大規模で複雑な環境において、威力を発揮します。重要な違いは、オブザーバビリティは、すべての問題を解決するための条件の定義において、これまでの経験に依存しない（未知の未知）ということです。また組織は、環境の最適化と強化のために、オブザーバビリティをプロアクティブに使用します。

多くのツールがオブザーバビリティに特化して構築され、以下のような性能を備えています。

分析とインシデント管理
- AIOps（ITオペレーション向け人工知能）機能
- アラート
- エラー追跡

アプリとサービス
- アプリケーションパフォーマンスモニタリング（APM）
- ディストリビューティッド（分散）トレーシング
- サーバーレス監視

人工知能（AI）
- AI監視
- 機械学習（ML）モデル監視

ビジネスへの影響と可視性
- ビジネスオブザーバビリティ
- ダッシュボード

デジタル エクスペリエンス モニタリング（DEM）
- ブラウザ監視
- モバイル監視
- 外形監視

インフラストラクチャ
- データベース監視
- インフラストラクチャ監視
- Kubernetes（K8）監視
- ネットワークパフォーマンス監視

ログ管理

セキュリティ監視

監視ツールのみの場合、データサイロとデータサンプリングが発生することがあります。それとは対照的に、オブザーバビリティプラットフォームは、技術スタック全体を計装し、そこから取得したテレメトリーデータを1か所に集約して、統合的かつアクション可能な一元化されたビューとして相関させることができます。

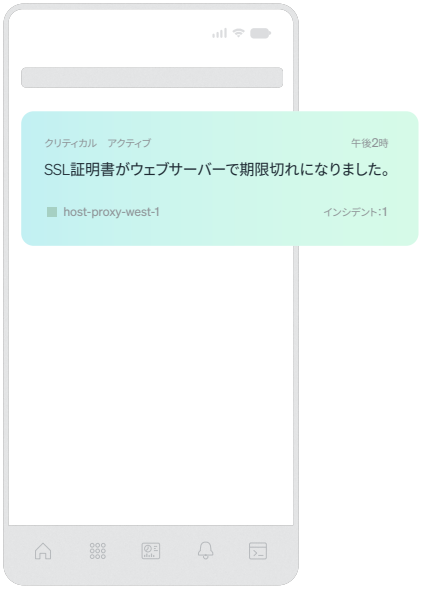
監視	オブザーバビリティ
リアクティブ（事後対応的）	プロアクティブ（事前対策的）
状況的	予測的
推測ベース	データドリブン
いつ、何が起きたのか？	いつ、何が、なぜ、どのように起きたのか？
想定内の問題（既知の未知）	想定外の問題（未知の未知）
データサイロ	1箇所でのデータ集約
データサンプリング	すべてを計装

ビジネスオブザーバビリティは、包括的な可視性を提供し、ビジネスへの影響を数値化する点で、さらに一歩進んでいます。

★ ☆ ☆

監視：良い

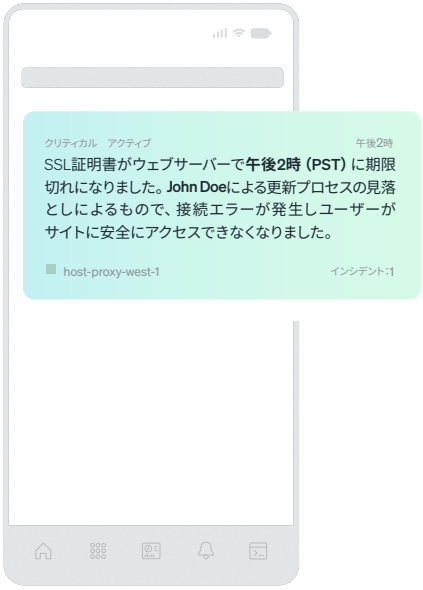
ITチーム



★ ★ ☆

オブザーバビリティ：より良い

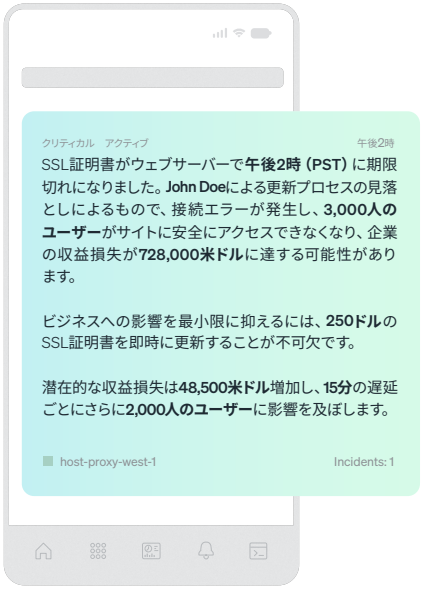
運用チーム



★ ★ ★

ビジネスオブザーバビリティ：もっとも良い

経営者



フルスタックオブザーバビリティ

カスタマーエクスペリエンスに影響しうる技術スタックのすべてを把握する性能を、フルスタックオブザーバビリティ、またはエンドツーエンドのオブザーバビリティと呼びます。これは、全テレメトリーデータを完全に把握することが前提となります。

エンドツーエンドのオブザーバビリティに向けてデータドリブンなアプローチを採用することで、エンジニアと開発者は全テレメトリーデータの完全なビューを獲得します。これにより、彼らはデータサンプリングをしたり、技術スタックの可視性を妥協したり、サイロ化されたデータの切り替えに時間を費やす必要がなくなります。代わりにエンジニアや開発者は、彼らが好む、より優先度が高くビジネスに影響を与えるクリエイティブなコーディング作業に集中できます。また、エグゼクティブや経営者にビジネスの包括的なビューを提供し、サービス中断がもたらすビジネスへの影響を理解できるようにします。

フルスタックオブザーバビリティは、本レポートで使用されているとおり、アプリとサービス、ログ管理、インフラストラクチャ（バックエンド）、DEM（フロントエンド）、セキュリティ監視などの、オブザーバビリティ性能の特定の組み合わせをデプロイする組織により実現されます。

どれほど多くの調査回答者がフルスタックオブザーバビリティを実現させたか、またフルスタックオブザーバビリティを実現させる利点についてご覧ください。

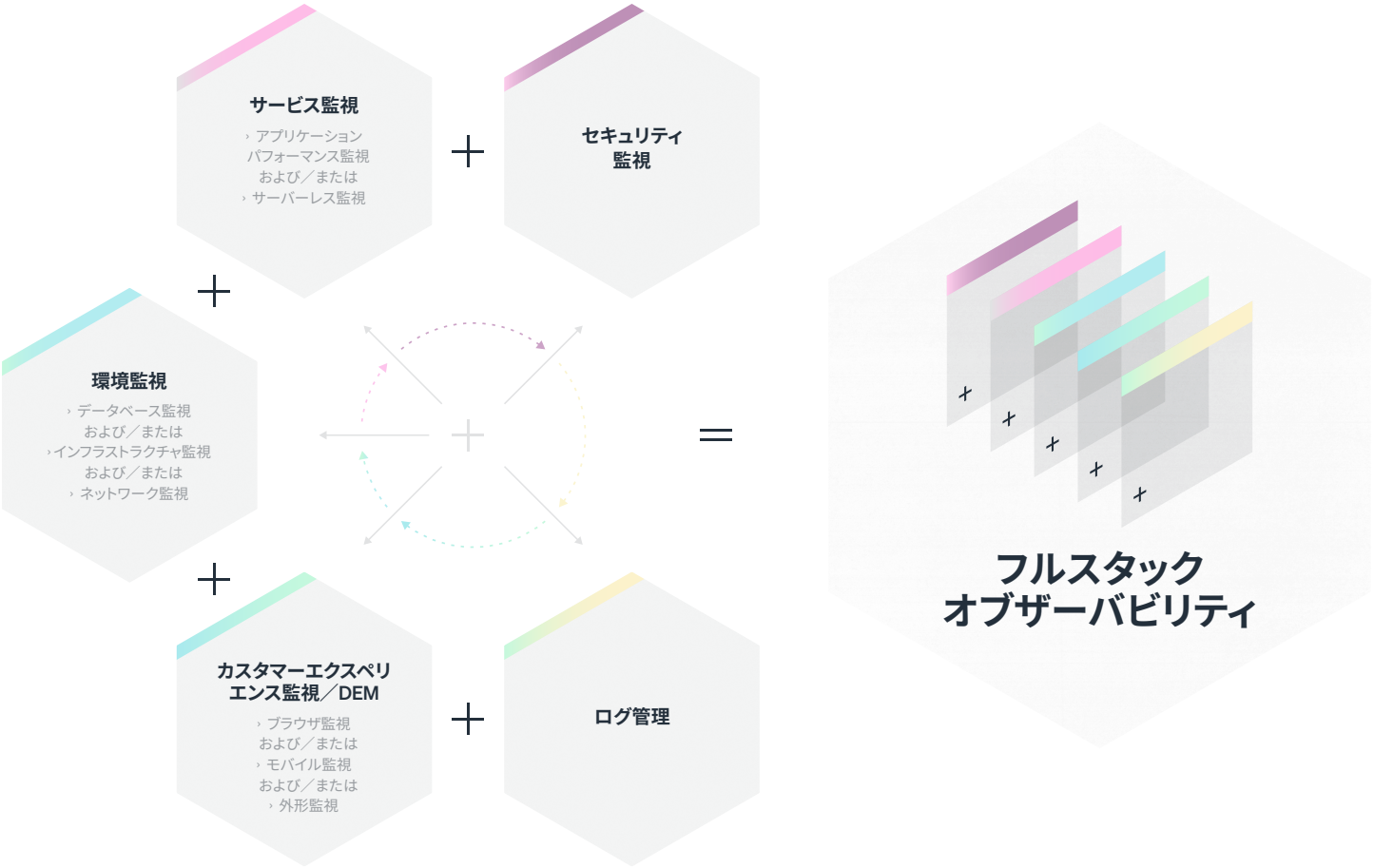


図38. フルスタックオブザーバビリティの定義

MTTx

MTTxには、検出または発見までの平均時間（MTTD）、識別までの平均時間（MTTI）、確認応答までの平均時間（MTTA）、および解決または修復までの平均時間（MTTR）が含まれます。

組織の規模

本レポートでは、特に記載がない限り、組織の規模は従業員数に準じて表記しています（以下参照）。

小規模：1〜100
中規模：101〜1,200
大規模：1,201+

役割

調査の参加者は、実務担当者とIT領域の意思決定者（ITDM）でした。実務担当者とは通常、オブザーバビリティツールを日常業務で使用するユーザーを指します。

実務担当者およびITDMの役割、役職、一般的な主要パフォーマンス指標（KPI）：

役割	役職	説明	一般的なKPI
開発者	アプリケーション開発者、ソフトウェアエンジニア、設計者、フロントラインの担当マネージャー	コード設計、ビルド、デプロイを行い、可能な場合にはプロセスを最適化、自動化する技術チームのメンバー	• サイクルタイム（変更実施のスピード） エンドポイントセキュリティインシデント • エラー率 • リードタイム（発想からデプロイメントまでのスピード） • インシデント間の平均時間（MTBI） • ソフトウェアパフォーマンスの速度 • 稼働率
運用のプロフェッショナル	ITオペレーションエンジニア、ネットワークオペレーションエンジニア、DevOpsエンジニア、DevSecOpsエンジニア、SecOpsエンジニア、サイト信頼性エンジニア（SRE）、インフラストラクチャオペレーションエンジニア、クラウドオペレーションエンジニア、プラットフォームエンジニア、システムアドミニストレーター、設計者、フロントラインの担当マネージャー	インフラストラクチャとアプリケーションの健全性と安定性の全般を担当する技術チームのメンバー 監視ツールを使用してインシデントを検知、解決し、コードパイプラインを構築、強化し、最適化と規模化の取り組みをリードする	• 可用性 • 導入のスピードと頻度 • エラーバジェット • エラー率 • 平均検出時間（MTTD） • 平均復旧時間（MTTR） • サービスレベル契約（SLA） • サービスレベル指標（SLI） • サービスレベル目標（SLO） • 稼働率
非エグゼクティブマネージャー	エンジニアリング、オペレーション、DevOps、DevSecOps、SecOps、サイト信頼性、分析担当のディレクター、シニアディレクター、副社長（VP）、上級副社長（SVP）	顧客向け、社内システム、プラットフォームの構築、運用開始、管理に関する実務担当チームのリーダー 高レベルのビジネス戦略を運用可能なものにし、技術戦略を戦術的実施へと変換するプロジェクトを統括する 継続的な加速とサービスの規模化を目指す	• 顧客満足度 • MTBI • MTTR • 予定に沿ったプロジェクト完遂 • ソフトウェア開発と効率性 • デプロイメントの速度 • 稼働率
エグゼクティブ（最高幹部）	技術に特化：最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）、最高技術責任者（CTO）、最高データ責任者（CDO）、最高アナリティクス責任者（CAO）、チーフアーキテクト 技術に特化しない：最高経営責任者（CEO）、最高執行責任者（COO）、最高財務責任者（CFO）、最高マーケティング責任者（CMO）、最高収益責任者（CRO）、最高製品責任者（CPO）	ビジネスインパクト、技術戦略、組織文化、企業の名声、コスト管理を担当する、技術インフラとコスト全般のマネージャー ビジネスの目標を達成するため、組織の技術関連のビジョンとロードマップを定義する デジタル技術を利用してカスタマーエクスペリエンスと収益性を向上させ、その結果として企業の名声を高める	• コンバージョン率 • 費用対効果 • 顧客満足度 • 投資利益率（ROI） • デプロイメントの速度 • イノベーションの速度 • 総所有コスト（TCO） • 稼働率

方法論

本レポート内の全データは、2024年4月から5月に実施された調査から得られたものです。

ETRは、関連する専門性に基づき調査対象者を選定しました。ETRは、回答者のサンプルサイズを獲得するのに、彼らが拠点とする国と組織でのロールタイプ（実務担当者およびITDM）にもとづき、割当法と呼ばれる非確率サンプリングタイプを実施しました。地理的分配の割当には、16の主要国をターゲットとしました。

業界による結果の偏りを避けるため、本レポートではn<10のサブサンプルが一部の分析から除外されています。

すべてのコメントは、ETRがオブザーバビリティを使用するIT専門家に実施したインタビューから得られたものです。

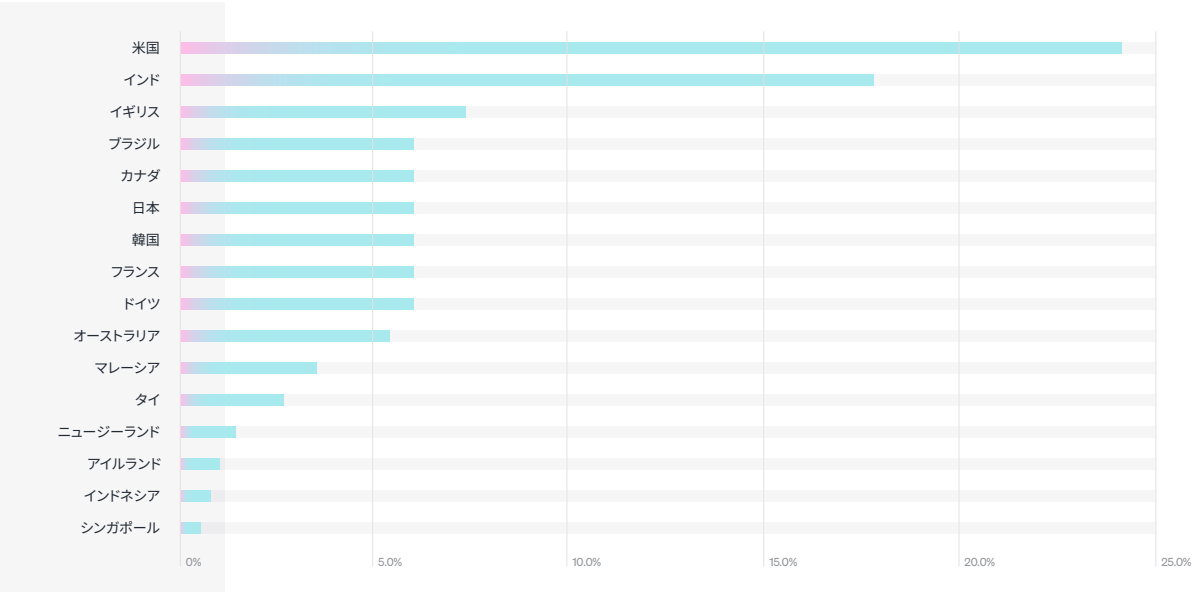
本レポート内で提示されるすべてのドル表記は米国ドル（USD）です。

デモグラフィック

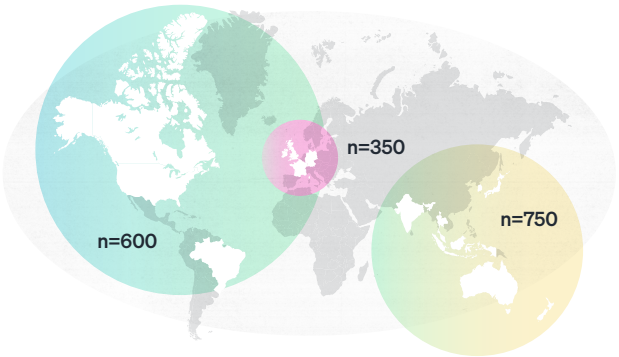
2024年、ETRは他のオブザーバビリティ調査よりも規模が大きい、南北アメリカ、アジア太平洋、欧州の16か国で1,700名の技術プロフェッショナルを対象に調査を実施しました。約35%はブラジル（今年新規）、カナダ、アメリカの回答者でした。フランス、ドイツ、アイルランド、英国が回答者の21%を占め、残りの44%は、オーストラリア、インド、インドネシア、日本、マレーシア、ニュージーランド、シンガポール、韓国、タイを含む、より広域のアジア太平洋からの回答者でした。地域別ハイライトをご覧ください。

調査対象者の構成は2021年、2022年、2023年とほぼ同様で、65%が実務担当者、35%がITDMでした。

国



地域



役割

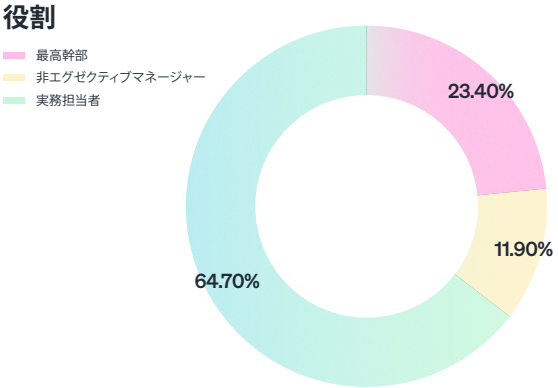


図40. 回答者の属性、地域、国、役割

企業属性

調査対象者の半数以上 (57%) が大規模組織、次いで中規模組織 (34%) 、小規模組織 (9%) に所属していました。

年間収益は、4分の1未満 (17%) が50万ドル～999万ドル、26%が1,000万ドル～9,999万ドル、57%が1 億ドル以上でした。

回答者群の業界は、IT、金融サービス／保険、工業／原料／製造、小売／消費者、医療／製薬、エネルギー／ユーティリティ、サービス／コンサルティング、テレコミュニケーション、教育、政府機関、メディア／エンターテイメント (今年新規) 、非営利など、多様な業界により構成されています。

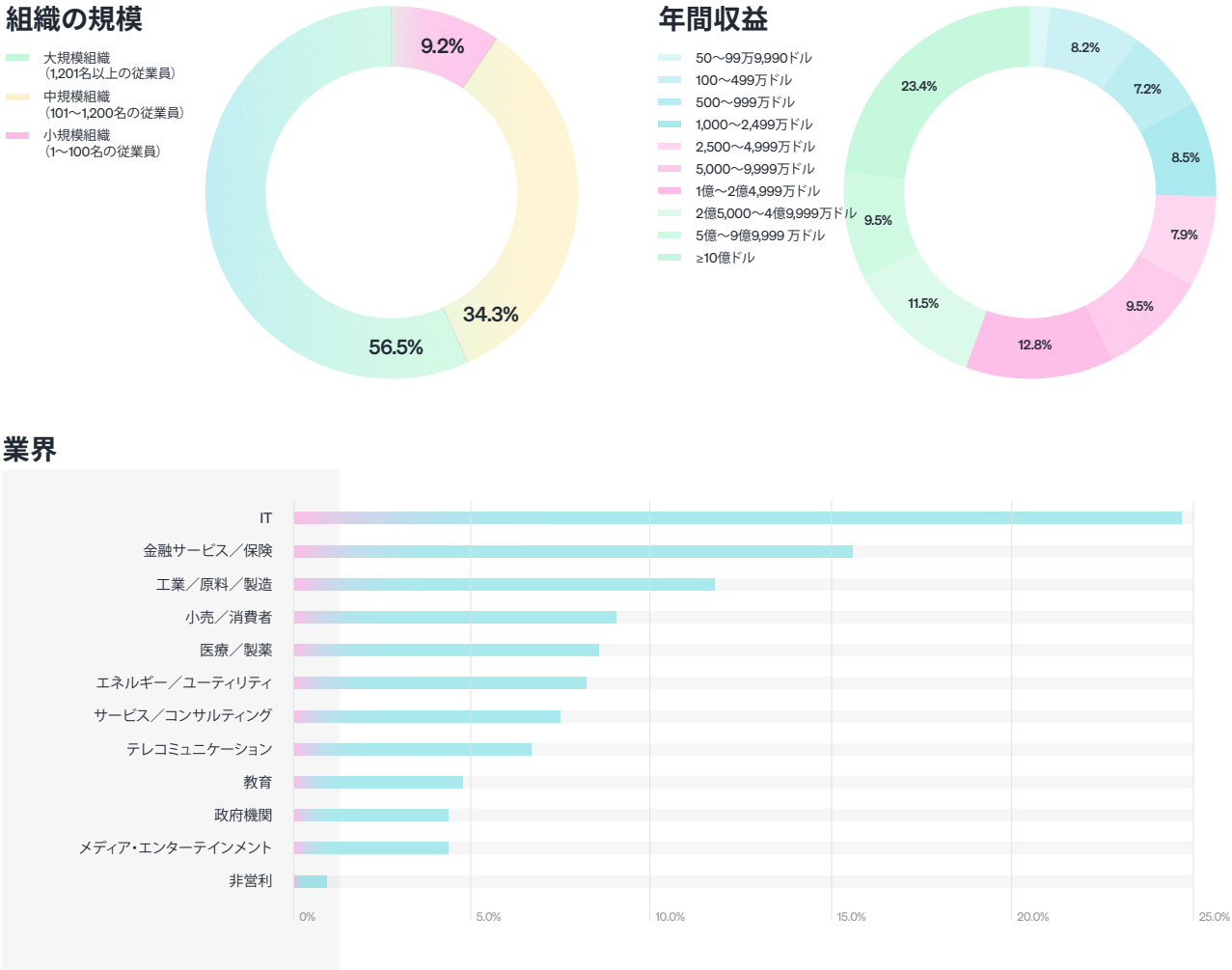


図41. 回答者の組織規模、年間収益、業界

ETRについて

ETRは、対象とするITDM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サーチファームです。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ITDM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、ITDM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なオブサーバビリティプラットフォームは、デジタル体験の中断を解消できるように企業を支援します。New Relicは、テレメトリーデータを統合およびペアリングしてデジタル資産全体を明確にする、唯一のプラットフォームです。当社では、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、コストを抑制して、問題解決をプロアクティブかつ予測可能なものへと移行します。そのため、世界中の企業（Adidas Runtastic、American Red Cross、Domino's、GoTo Group、Ryanair、Topgolf、William Hillなど）が、New Relicを使用してイノベーションを推進し、信頼性を向上させ、成長を促す優れた顧客体験を提供しています。www.newrelic.com/jpをご覧ください。

New Relicのプラットフォームについて知る