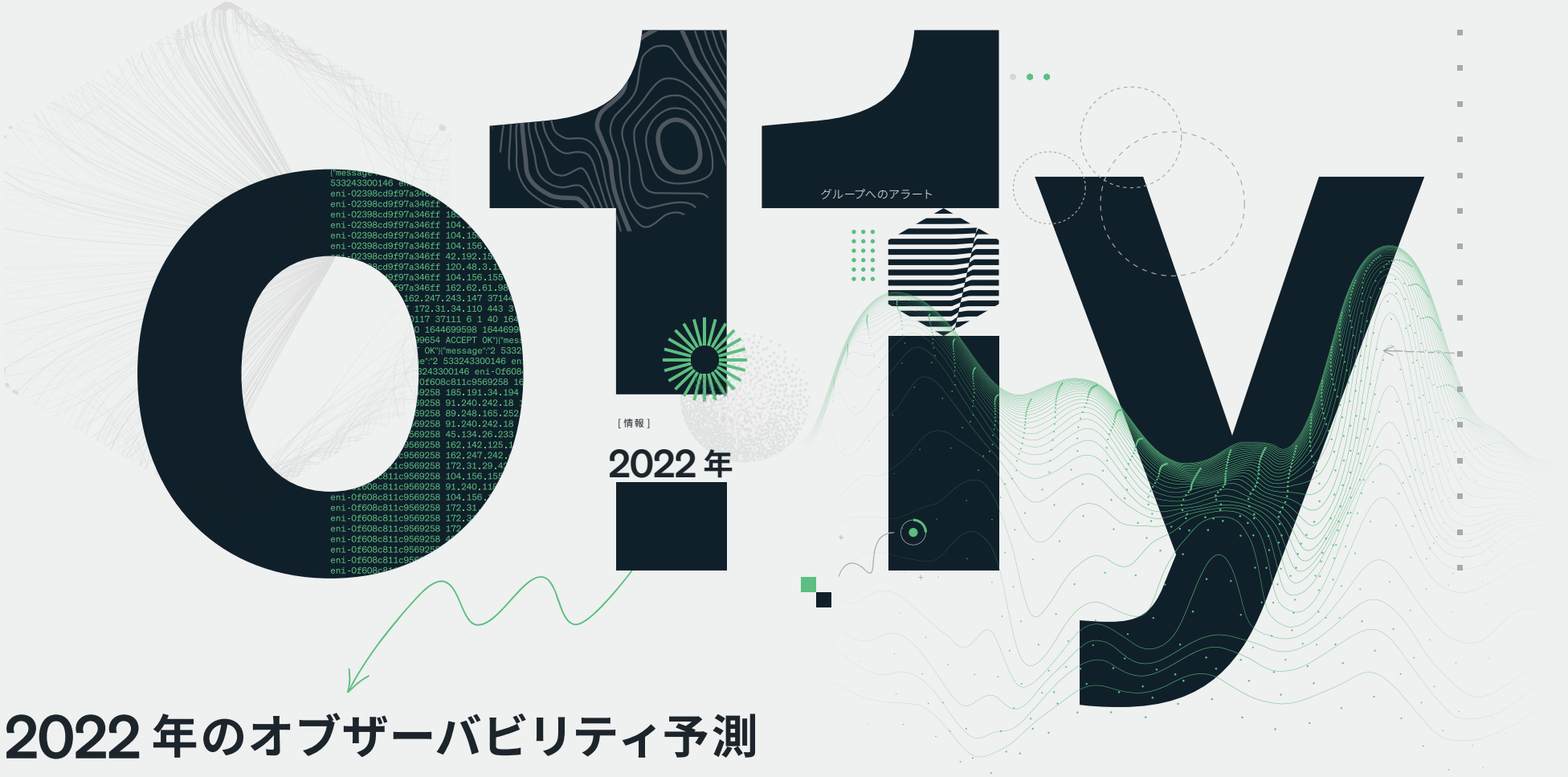
new relic | ETR




# 2022 年のオブザーバビリティ予測

オブザーバビリティの現状と未来への投資に関する調査

年次レポート／ 2022 年 9 月

作成者：

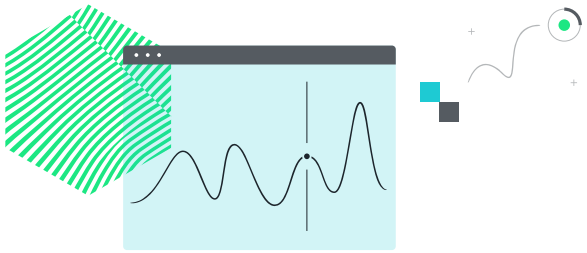
**アリシア・バステリ** New Relic、シニアテクニカル・コンテントマーケティング・マネージャー

共同作成者：

**ダレン・ブラバム、** ETR シニアダイレクター、アナリスト、博士

# 目次

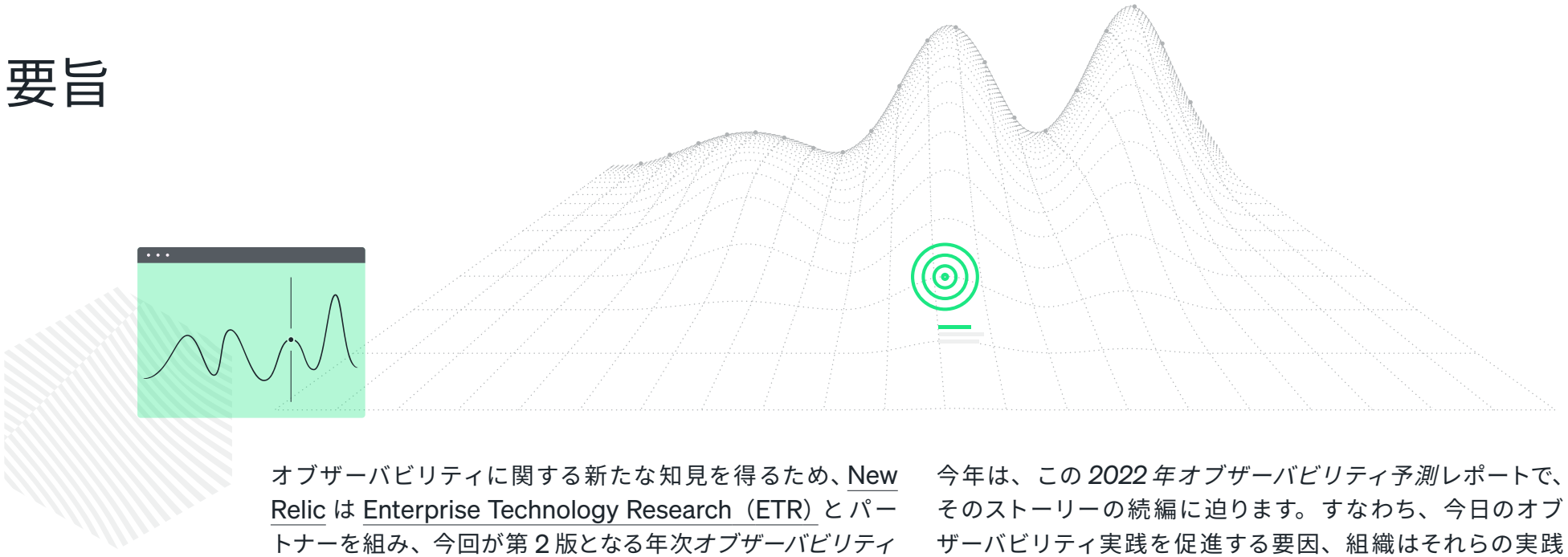
# 図表一覧表



# 本レポートについて

オブザーバビリティの現状と未来に関する、定量化可能なデータポイントと詳細な分析をご覧ください。

# 要旨



オブザーバビリティに関する新たな知見を得るため、New Relic は Enterprise Technology Research（ETR）とパートナーを組み、今回が第 2 版となる年次*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。

昨年、*2021 年オブザーバビリティ予測*レポートにおいて、デジタルトランスフォーメーション（DX）に導かれる形で、あらゆる最新のビジネスにおいてフルスタックオブザーバビリティ（o11y）がいかに必要不可欠なものとなっているかを考察しました。今こそ組織はフルスタックオブザーバビリティに移行し、顧客や従業員、パートナー、サプライヤーの最適化されたデジタルエクスペリエンスを推進する優れたソフトウェアの計画、構築、デプロイ、運用を行えるようになるべきであるという、強力な根拠を提示しました。

今年は、この *2022 年オブザーバビリティ予測*レポートで、そのストーリーの続編に迫ります。すなわち、今日のオブザーバビリティ実践を促進する要因、組織はそれらの実践をどう変容させているのか、そしてオブザーバビリティはどのように技術プロフェッショナルの仕事に影響を与えているのか。さらに、今後 3 年間でオブザーバビリティの必要性が増すであろう新たなテクノロジーについても考察を加えます。

今日、多くの組織は、ツールを寄せ集めてどうにか技術スタックを監視している状態にあります。そこでは、情報技術（IT）システムとビジネス全体に関する分断されたビューでの膨大なマニュアル作業が求められます。それと同時に、調査対象者は、高価値な業務を遂行するための、簡潔かつシームレスに統合された、より効率のよい方法を切望し、計画していました。

## 課題

監視は分断されています。多くの組織は現状、技術スタック全体を監視していません。

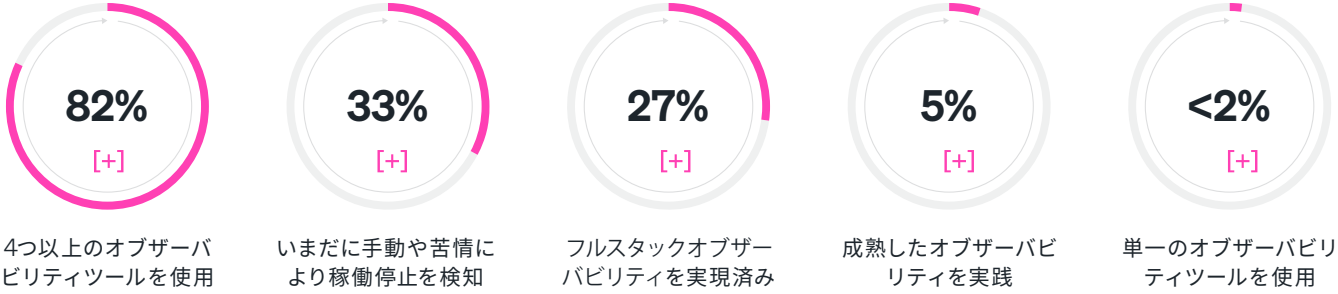



図 01. オブザーバビリティの課題の概要

## 機会

オブザーバビリティはサービスレベルのメトリクスを改善します。組織はその価値を知り、そこへのさらなる投資を予定しています。


図 02. オブザーバビリティの機会の概要

## フルスタックオブザーバビリティの優先／実現

[+]


図 03. オブザーバビリティがいかにサービスレベルのメトリクス改善に役立つかの概要

# 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

調査においては、バイアスを防ぐため、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）とは、システムがどのように機能しているかを測定し、外部出力にもとづき問題やエラーを特定する能力のことです。これらの外部出力とは、テレメトリデータ（メトリクス、イベント、ログ、トレース）のことです。データドリブンなエンジニアリングでは、テレメトリデータによりアクションが促されます。オブザーバビリティは、エラーとその詳細（いつ、なぜ、どのように発生したのか）を特定するアクション可能なデータを確保するため、インストゥルメントシステムを必要とします。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、異なる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 箇所で実現します。チームはそこで、より早いトラブルシューティングや問題解決の共同作業を行い、運用効率を高め、最適化された顧客およびユーザーエクスペリエンスを確実なものとする高品質なソフトウェアの開発を行なうことができます。

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は、複雑なデジタルシステムの挙動を理解し、データを各自に合わせた考察へと変換するために、オブザーバビリティを使用します。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」はリアクティブ（事後対応的）なものであり、何が誤っている（エラー）のか、いつエラーが発生したのかを明らかにします。対してオブザーバビリティは、（何が、いつ、に加えて）なぜ、どのようにエラーが発生したのかをプロアクティブ（事前対策的）に決定します。監視ツールのみだとデータサイロとデータサンプリングに帰結する可能性がありますが、オブザーバビリティ・プラットフォームでは、技術スタック全体をインストゥルメントし、そこから抽出されたテレメトリデータを、1 箇所に統合されたアクショナブル・ビューで相関させる能力を提供します。

| 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 | データ駆動型 |
| 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？ |
| データサイロ（分断） | 1 箇所へのデータ集約 |
| データサンプリング | すべてを計装 |

**表 01.** 監視とオブザーバビリティの主な違い

多くのツールはオブザーバビリティに特化し、以下のような性能を備えています。

- AIOps（ITオペレーション向け人工知能）
- アラート
- アプリケーションパフォーマンス監視（APM）
- ブラウザ監視
- カスタムダッシュボード
- データベース監視
- ディストリビューティッド（分散）トレーシング
- エラー追跡
- インフラストラクチャ監視
- Kubernetes監視
- ログ管理
- 機械学習（ML）モデルパフォーマンス監視（MLOps）
- モバイル監視
- ネットワークパフォーマンス監視
- セキュリティ監視
- サーバーレス監視
- 外形監視

リアルユーザー監視（RUM）には、ブラウザ監視とモバイル監視が含まれます。デジタルエクスペリエンス監視（DEM）には、RUM に加えて外形監視が含まれます。

# 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、全テレメトリデータの包括的なビューにもとづきます。

フルスタックオブザーバビリティにより、エンジニアと開発者は、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。その代わりに、より優先度の高い、ビジネスに影響する、彼らの望むクリエイティブなコード開発業務に集中できるようになります。

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る通り、カスタマーエクスペリエンス監視／DEM（フロントエンド）、サービス監視、ログ管理、環境監視（バックエンド）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。

多くの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をご覧ください。

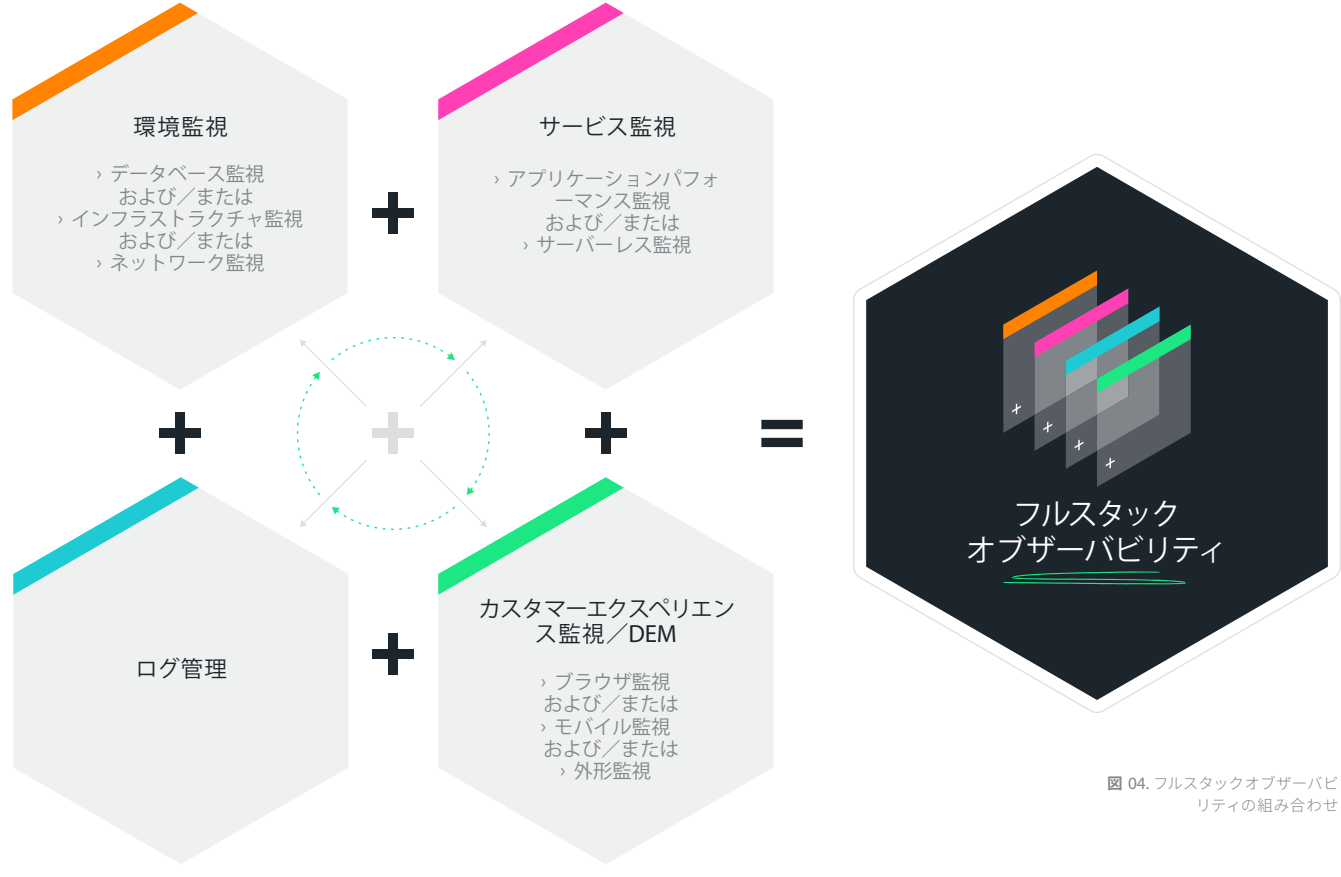



図 04. フルスタックオブザーバビリティの組み合わせ

# 成熟したオブザーバビリティの実践

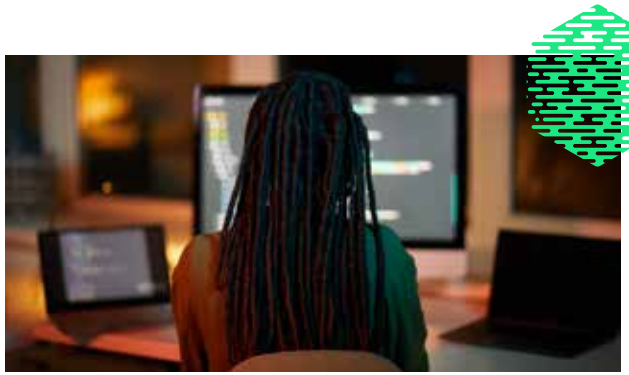
成熟したオブザーバビリティの実践を構成する要素は、やや主観的な問題です。本レポートでは、成熟したオブザーバビリティの実践を、ベストプラクティスに従い、特定の成果を達成することと定義しました。

## ベストプラクティス

- インストゥルメンテーションが自動化されている
- インシデント対応の一部が自動化されている
- インフラストラクチャが自動化ツールを使用して設定、オーケストレーションされている
- テレメトリが技術スタック全体にわたり収集されている
- テレメトリ（メトリクス、イベント、ログ、トレース）が複数チームで活用できるよう単一ペインに統合されている
- ユーザーがテレメトリデータとその可視性に幅広くアクセスできる
- ソフトウェアのデプロイメントに、CI/CD（継続的なインテグレーション、開発およびデプロイメント）の実践が活用されている
- カーディナリティの高いデータの取り込み
- 臨機応変なデータクエリ能力

## 成果

- 開発者（およびエンジニア）の作業時間が、インシデント対応（リアクティブ）からより高価値な作業（プロアクティブ）へ移行
- ソフトウェアスタックに関する判断におけるチーム間の協力体制が強化
- オブザーバビリティによりサービスの中断とビジネスリスクが低減
- テレメトリデータが、ビジネス関連の文脈を考慮してイベントやインシデントのビジネスインパクトを数値化
- オブザーバビリティにより顧客行動への理解が深まることで、収益維持率が向上
- オブザーバビリティにより収益を創出する使用事例を構築



**本レポートの目的に鑑み、成熟したオブザーバビリティの実践は、少なくとも以下の５つの特性を備えるものとします。**

- ✓ テレメトリ（メトリクス、イベント、ログ、トレース）を、複数チームで活用できるよう単一ペインに統合
- ✓ 開発者およびエンジニアの作業時間を、インシデント対応（リアクティブ）からより高価値な作業（プロアクティブ）なものへと移行
- ✓ ソフトウェアスタックに関する判断におけるチーム間の協力体制を強化
- ✓ サービスの中断とビジネスリスクを低減
- ✓ 顧客行動への理解を深めることにより、収益維持率を向上

調査対象者におけるオブザーバビリティの成熟度についてご覧ください。

# 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。

| | 役割 | 役職 | 説明 | 一般的な KPI |
|---|---|---|---|---|
| 実務担当者 | 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 | プロセスを最適化、自動化して、コード設計、ビルド、デプロイを行なう技術チームのメンバー<br><br>新規コーディングの課題や新規技術の導入に前向きに取り組み、最新の高性能ツールについて熟知している | • サイクルタイム（変更実施のスピード）<br>• エンドポイントのセキュリティインシデント<br>• エラー率<br>• リードタイム（発想からデプロイメントまでのスピード）<br>• インシデント間の平均時間（MTBI）<br>• ソフトウェアパフォーマンスの速度<br>• 稼働率 |
| 実務担当者 | 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<br><br>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<br>• デプロイのスピードと頻度<br>• エラーバジェット<br>• エラー率<br>• 平均検出時間（MTTD）<br>• 平均復旧時間（MTTR）<br>• サービスレベル契約（SLA）<br>• サービスレベル指標（SLI）<br>• サービスレベル目標（SLO）<br>• 稼働率 |
| ITDM | 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<br><br>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<br><br>継続的な加速と、サービスの規模化を目指す | • 顧客満足度<br>• MTBI<br>• MTTR<br>• 予定に沿ったプロジェクト完遂<br>• ソフトウェア開発と効率性<br>• デプロイメントの速度<br>• 稼働率 |
| ITDM | 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<br><br>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<br><br>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<br><br>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<br>• 費用対効果<br>• 顧客満足度<br>• 投資利益率（ROI）<br>• デプロイメントの速度<br>• イノベーションの速度<br>• 総所有コスト（TCO）<br>• 稼働率 |

**図 02.** 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）

## 組織の規模

本レポートでは、組織の規模は
従業員数により決定されます。


図 05. 従業員数にもとづく組織の規模

# 手法

ETR が調査対象者に質問表を送付し、調査への回答に対して謝礼を支払いました。

本レポート内の全データは、2022 年 3 月から 4 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もとづいて調査対象者を選定しました。ETR は、回答者のサンプル規模を獲得するのに、彼らが拠点とする国と組織でのロールタイプ（すなわち実務担当者および 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、14 の主要国をターゲットとしました。

本レポート内で提示されるすべてのドルは米国ドル（USD）です。

調査結果をダウンロードする。

# 回答者の属性

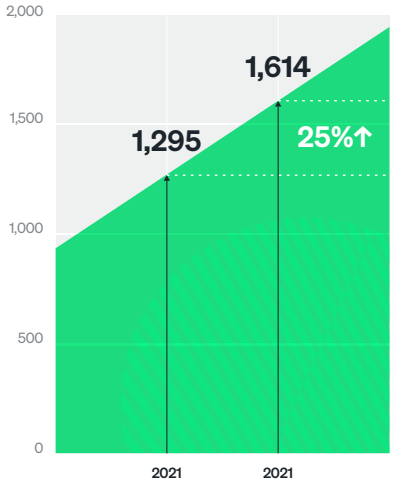
n=1,614

2022 年、ETR は、オブザーバビリティに関するレポートとして最大規模の、かつ 2021 年の調査での 1,295 名から 25% 以上増となる 1,614 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。対象国は昨年同様、アジア太平洋、ヨーロッパ、北米にわたる地域からの 14 カ国で、フランス、ドイツ、アイルランド、イギリスが回答者の 44% を占め、およそ 31% がカナダおよび米国でした。残りの 25% 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、タイを含む、より広いアジア太平洋地域からの回答者でした。地域別のハイライトを見る。

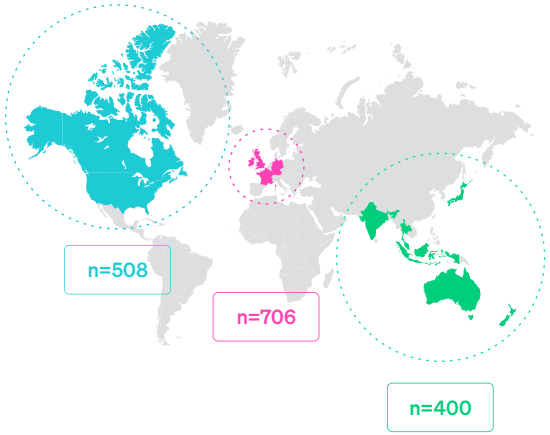
調査対象者の構成は昨年とほぼ同様で、65% が実務担当者、35% が ITDM です。データに共通するテーマは、オブザーバビリティに関する実務担当者の評価と認識および ITDM の評価と認識の分割です。

回答者の年代は 19 歳～ 72 歳に分布し、80% が男性、20% が女性と識別されており、これは（残念ながら）今日の技術プロフェッショナルにおける男女の不均衡を反映するものとなっています。

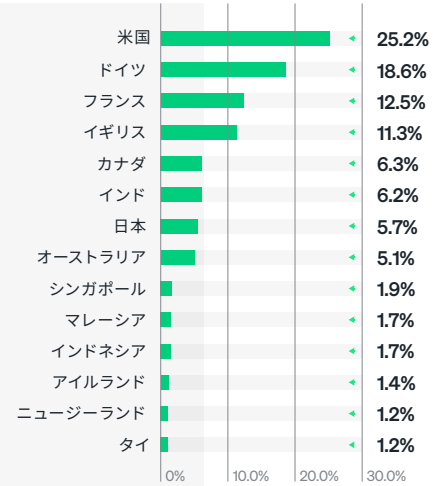
### サンプル規模



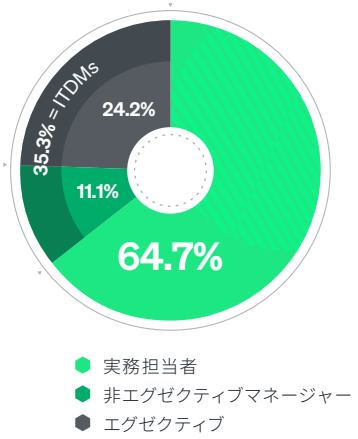

### 地域



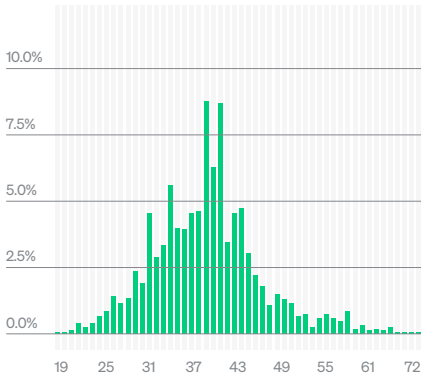

### 国




### ロール




### 年齢




### 性別

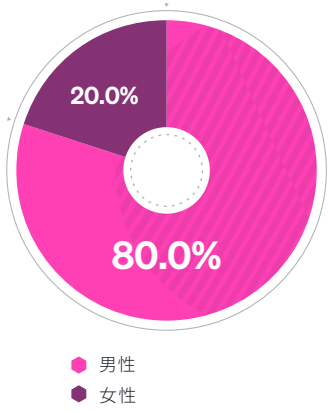



**図 06.** 回答者の属性（サンプル規模、地域、国、役割、年齢、性別）

# 回答者の企業属性

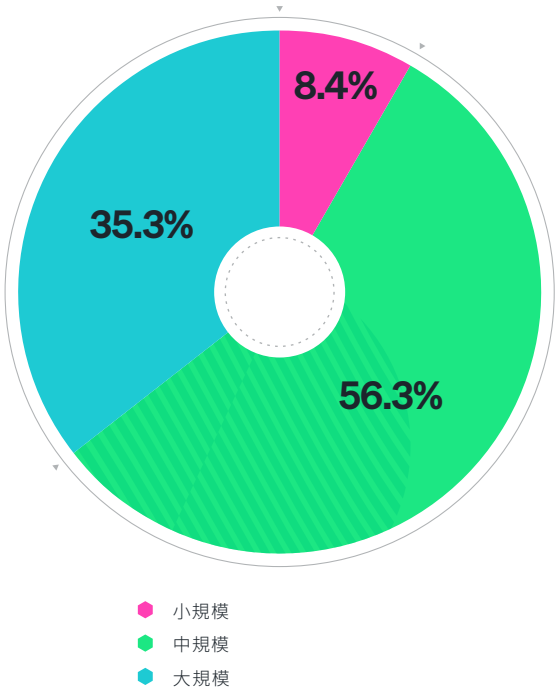
調査対象者の半数以上（56%）が中規模組織、35% が大規模組織、そして 8% が小規模組織に勤務しています。

組織の年間収益は、17% が 100 万ドルから 999 万ドル（うち 35% が小規模組織、55% が中規模組織）、43% が 1,000 万ドルから 9,999 万ドル（うち 76% が中規模組織）、40% が 1 億ドル以上（うち 63% が大規模組織）です。

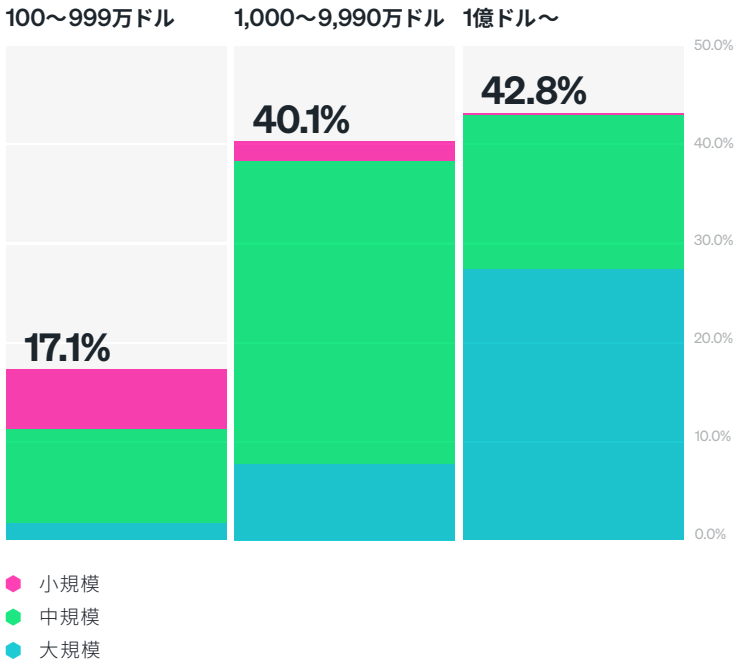
回答者群の業界は、IT ／テレコミュニケーション、金融／保険、工業／原料／製造、小売／消費者、医療／製薬、エネルギー／ユーティリティ、サービス／コンサルティング、教育、NPO ／その他、政府機関など、多様な業界により構成されています。

業界別のハイライトを見る。

**組織の規模**




**年間収益**




**業界**

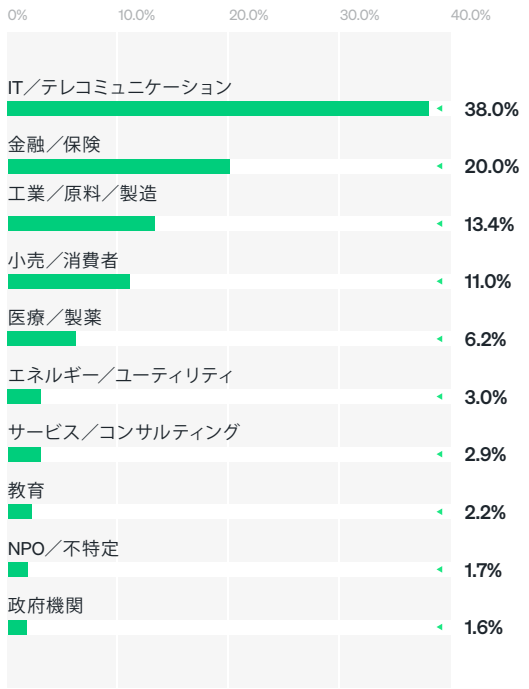
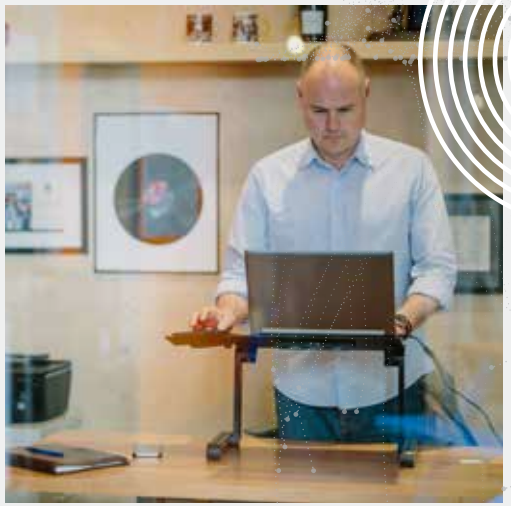



**図 07.** 回答者の企業属性（組織規模、年間収益、業界）

# オブザーバビリティの現状

## 監視は分断されています。多くの組織は現状、技術スタック全体を監視していません。



# 現在のデプロイメント

はじめに、調査実施の時点で導入されていたオブザーバビリティの特性とデプロイ済みの性能について、それらがどのようにデプロイされたか、戦略と組織、得られた利点、オブザーバビリティに割り当てられた IT 予算の割合、価格と請求に関するトレンド、フルスタックオブザーバビリティを優先、実現するための課題について見ていきましょう。

## 成熟したオブザーバビリティの特性

調査対象者に、どの成熟したオブザーバビリティの特性がもっとも重要だと考えるか、また調査後半の別個の質問で、導入済みなのはどれかについて尋ねました。結果は以下の通りです。

- 2% のみが、自社組織で 15 のオブザーバビリティの特性すべてを導入していると回答
- 全く導入していないと回答したのはわずか 1%
- 半数以上（53%）が 3 ～ 5 項目を導入（52% が 1 ～ 4 項目を導入、48% が 5 項目以上を導入、10% が 10 項目以上を導入）

本レポートでの成熟したオブザーバビリティの定義にもとづくと、成熟したオブザーバビリティの実践を行っている調査対象者は 5% にとどまりました。

成熟したオブザーバビリティの実践を行っている回答者ほど、多くのオブザーバビリティの特性を導入している傾向にあり、97% が 9 項目以上、40% が 15 項目すべてを導入していると回答しました。

成熟したオブザーバビリティの実践を行っている回答者の 100% が、オブザーバビリティにより顧客行動への理解が深まり、収益維持率が向上したと回答しました。これに対し、実践の成熟度の乏しい回答者では 34% でした。

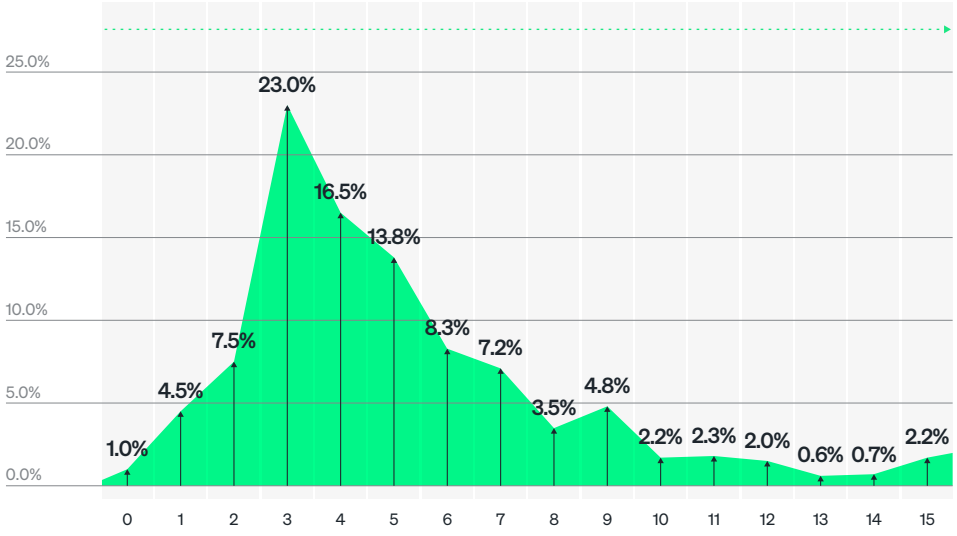



**図 08.** 採用されている成熟したオブザーバビリティの実践の特性の数

### 地域別の考察

成熟したオブザーバビリティの実践を行っているのは北米の組織がもっとも多く（7%）、ヨーロッパの組織がもっとも少ない傾向にありました（4%）。

### 役割別の考察

エグゼクティブはオブザーバビリティにより顧客行動への理解が深まり、収益維持率が向上したと感じていました（トップ回答）。対照的に、その他の回答者においては、収益維持率は非エグゼクティブマネージャーでは下位の 10 位、実務担当者では 6 位でした。

**5%**

未満が、成熟した
オブザーバビリティを実践

成熟したオブザーバビリティの実践において回答者がもっとも重要な特性と考えるものと、彼らが実際に導入している特性については隔たりがありました。

| 成熟した実践の特性 | 上位 5 位のもっとも重要とされた特性 | もっとも重要であるとされ、導入済みの特性 * | その特性を導入済みの回答者の全体の割合 |
|---|---|---|---|
| ソフトウェアのデプロイメントに CI/CD の実践が活用されている | 23.6% | 52.5% | 42.8% |
| ソフトウェアスタックに関する判断におけるチーム間の協力体制が強化 | 27.3% | 52.0% | 45.7% |
| 開発者の作業時間が、インシデント対応（リアクティブ）からより高価値な作業（プロアクティブ）なものへと移行 | 28.4% | 47.7% | 40.3% |
| インフラストラクチャが自動化ツールを使用して設定、オーケストレーションされている | 24.3% | 46.9% | 40.3% |
| テレメトリデータが、ビジネス関連の文脈を考慮してイベントやインシデントのビジネスインパクトを数値化 | 26.7% | 43.6% | 31.8% |
| 臨機応変なデータクエリ能力 | 22.4% | 43.4% | 31.6% |
| オブザーバビリティにより収益を創出する使用事例が構築 | 22.7% | 41.1% | 31.8% |
| オブザーバビリティによりサービスの中断とビジネスリスクが低減 | 27.2% | 41.0% | 33.9% |
| オブザーバビリティにより顧客行動への理解が深まることで、収益維持率が向上 | 28.0% | 40.7% | 37.7% |
| テレメトリ（メトリクス、イベント、ログ、トレース）が複数チームで活用できるよう単一ペインに統合されている | 25.5% | 39.9% | 32.6% |
| ユーザーがテレメトリデータとその可視性に幅広くアクセスできる | 22.2% | 39.8% | 31.8% |
| インストゥルメンテーションが自動化されている | 20.0% | 36.0% | 28.2% |
| インシデント対応の一部が自動化されている | 22.2% | 35.5% | 30.4% |
| テレメトリが技術スタック全体にわたり収集されている | 21.5% | 34.0% | 27.0% |
| カーディナリティの高いデータの取り込み | 17.8% | 31.6% | 24.8% |

**表 03.** 成熟したオブザーバビリティの実践にもっとも重要な特性と、実際に導入済みの特性の比較

*

**この列は、**例えば「CI/CD を活用したソフトウェアデプロイメントが、成熟したオブザーバビリティの実践のもっとも重要な特性の 5 つのうちの 1 つであると答えた 23.6% の回答者のうち、実際にこの特性を導入しているのは 52.5% に過ぎない」ことを意味します。

# デプロイ済みの性能

性能は、特性と混同されるべきではなく、これはオブザーバビリティの特定のコンポーネントを指します。調査対象者に、17 のオブザーバビリティ性能のうち、デプロイ済みのものはどれかを尋ねました。以下に、性能別、また性能数別の結果を概観します。

## 性能別：

調査対象者のうち、最も多いのが 57%（ネットワーク監視）最も少ないものは 34%（Kubernetes 監視）が、自社組織でオブザーバビリティ性能をデプロイしていると回答しました。判明したのは以下のことです。

- 半数余りが、環境監視性能とログ管理をデプロイしていると回答
- DEM およびサービス監視性能は、40% 台
- 新興テクノロジーに対する監視性能はもっともデプロイされておらず、30% 前半台

各性能のハイライトを見る。

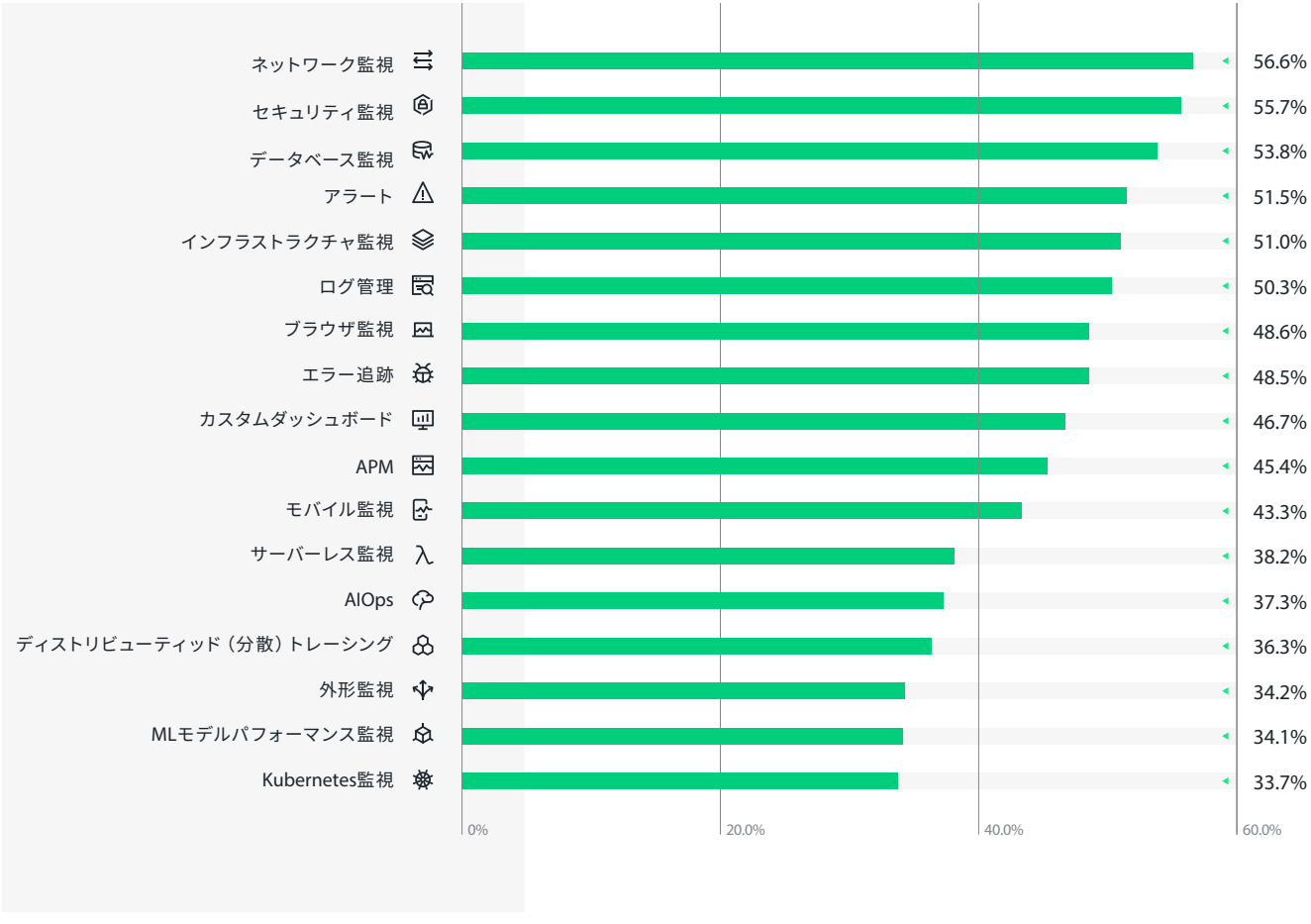



図 09. デプロイ済みの性能

## 性能数別

調査対象者の組織でデプロイされている性能数については、以下のことがわかりました。

- 17 すべてのオブザーバビリティ機能をデプロイしている組織は 3% のみ
- 3% が何もデプロイしていないと回答
- 多数（61%）が 4 ～ 9 項目をデプロイ済み（9% が 1 ～ 3 項目、80% が 5 項目以上、28% が 10 項目以上）

これらの結果は、多くの組織では現状、技術スタック全体は監視していないことを示唆しています。ただし、これは変化しつつあります。今後のデプロイメント計画をご覧ください。

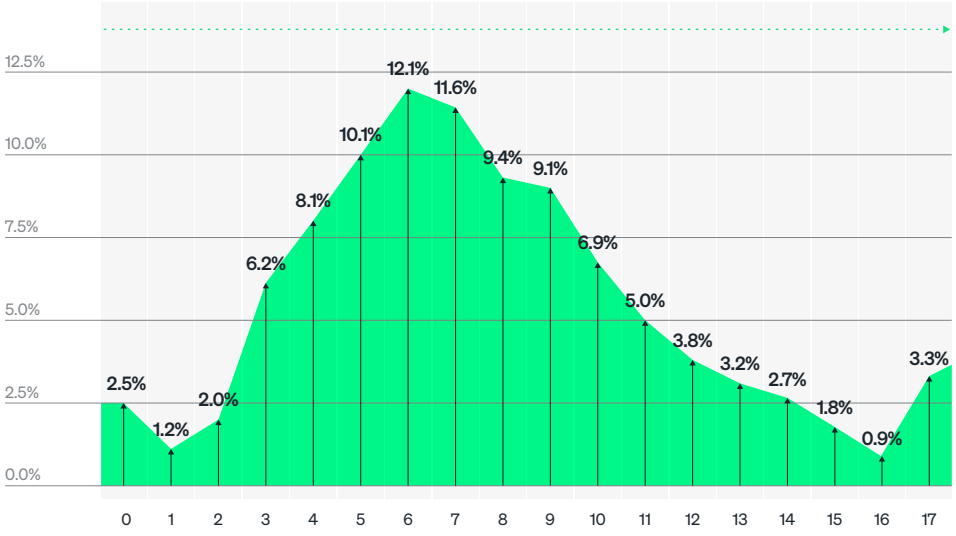



図 10. デプロイ済みの性能数

### 地域別の考察

全般的に、アジア太平洋の組織が多くの性能をデプロイしており、少ないのはヨーロッパの組織でした。

### 役割別の考察

エグゼクティブは、すべてのオブザーバビリティがデプロイされているとの回答がより多く(6%、非エグゼクティブマネージャーが 2%、実務担当者が 3%)、これは何がデプロイ済みで何がデプロイ予定かの知識ギャップを示唆しています。

# フルスタックオブザーバビリティの普及

本レポートでのフルスタックオブザーバビリティの定義にもとづくと、これを実現している調査対象者は 27% のみにとどまりました。さらに、自社組織がフルスタックオブザーバビリティをすでに優先し、実現しているとの回答はさらに少なく、3% のみでした。

これらの結果は、組織の技術スタックの大部分は現状、監視や完全なオブザーブがなされておらず、フルスタックオブザーバビリティの実現を加速させる十分な機会が生まれていることを示唆しています。

特記すべきは、フルスタックオブザーバビリティを実現している組織の 84% が、IT 予算全体の少なくとも 5% をオブザーバビリティツールに割り当てていたということです。

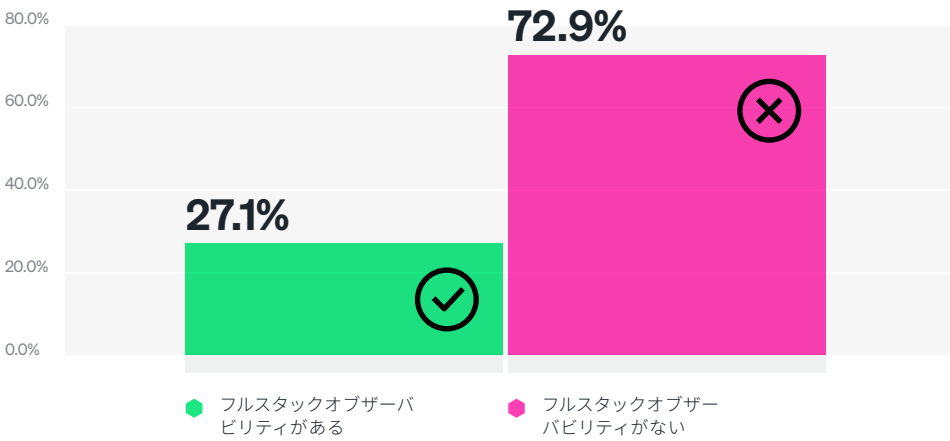



**図 11.** フルスタックオブザーバビリティを持つ／持たない組織の割合

**「日々、私たちのインフラストラクチャとプラットフォーム計算、ストレージサイクルの 33 ～ 35% が、複数のクラウドロケーションに置かれます。それらの多くでは監視が行われていません。これは当社のアプリケーション空間が分散しているためで、学術機関で非常に多いケースです。セキュリティリスク管理の観点から言うと、これはセキュリティリスクの最大領域の一角をなしています。」**

CISO、大手教育企業

### 地域別の考察

フルスタックオブザーバビリティを実現しているのはアジア太平洋の組織にもっとも多く（33%）、ヨーロッパの組織にもっとも少ない傾向にありました（21%）。

### 組織規模別の考察

フルスタックオブザーバビリティを実現している組織のなかで、小規模組織は 7% のみで、中規模組織が 52%、大規模組織が 42% でした。

**73%**

が、フルスタックオブザーバビリティを実現していない

# 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ると、圧倒的多数の調査対象者は複数ツールを使用していると回答しました。

- 大多数（82%）が 4 つ以上のツールを使用（94% が 2 つ以上）
- 5 分の 1 が、もっとも割合の高い 7 つのツール使用を回答
- オブザーバビリティのニーズが 1 つのツールで満たされているのはわずか 2%

ツールの分断化

つまり、今日のオブザーバビリティの現状は、複数のツール使用とそれに伴う分断化が多く、本質的に管理が複雑になっていると言えます。実際、25% の調査対象者は、監視ツールが多すぎることがフルスタックオブザーバビリティの優先と実現を阻む最大の課題であると述べています。

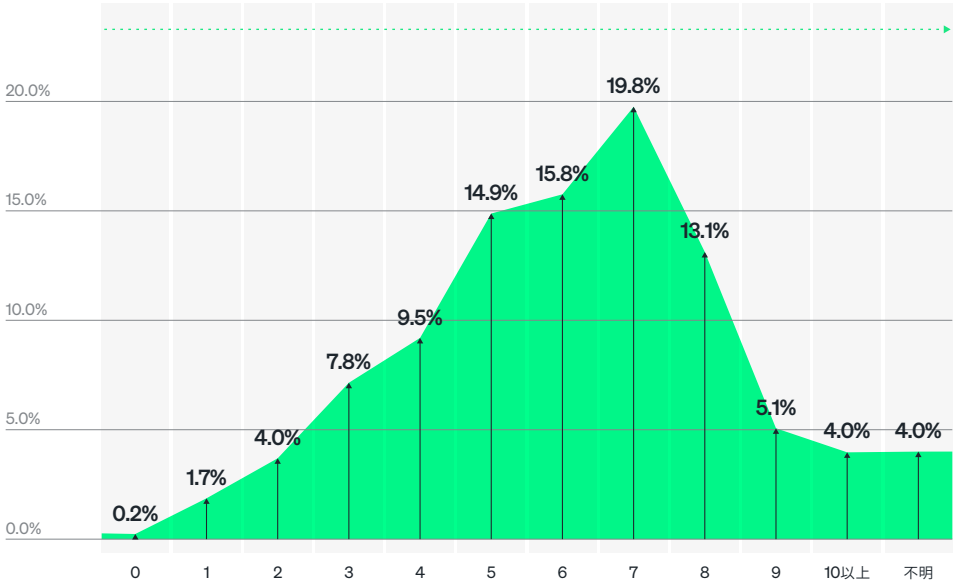



**図 12.** オブザーバビリティ性能に使用されるツール数

**組織規模別の考察**

監視ツールの 1 つのみの使用は、小規模組織でもっとも多い傾向にありました（6%、中規模組織で 2%、大規模組織で 1% のみ）。

**「オブザーバビリティ監視と情報セキュリティは緊密な連携が可能で、同一のプラットフォームを活用できます。重複する部分が多々あります。すべてを提供するのに単一のツールを使用できるという意味で、これはさらに重要性を増していきます。」**

SVP 兼 CTO、大手小売企業

**82%**

が、4 つ以上のオブザーバビリティツールを切り替えて使用

# 統合されたテレメトリ、可視化、ダッシュボードの構築

テレメトリデータと可視化、そのデータのダッシュボード構築は、どのように統合またはサイロ化／異種化されているでしょうか？

## 統合されたテレメトリ

調査対象者の組織のテレメトリデータが、どのように統合またはサイロ化されているかについて、回答は以下の通りです。

- ほぼ半数（49%）がどちらかと言えば統合されている（テレメトリデータを1箇所に統合している）と回答、ただし完全に統合されているのは 7% のみ
- 3分の1が、どちらかと言えばサイロ化されている（テレメトリデータを個別のデータ保管場所に分割している）と回答、そのうち 8% は完全にサイロ化されている
- 5分の1以下（17%）が、統合とサイロがおよそ半々であると回答

データの分断化

興味深いことに、どちらかと言えばサイロ化されていると回答した 51% のうち、47% が実際には単一のプラットフォームを強く望むと回答しました。さらに、完全にデータがサイロ化されているうちの 77% が、単一のプラットフォームを望むと回答しました。

オブザーバビリティに単一のツールを使用しているのは回答者のわずか 2% という状況で、異種の監視ツールとオープンソースのソリューションの使用を考えれば、これらの結果は当然のことと言えます。なぜなら、サイロ化され、分断されたデータは質の悪いユーザーエクスペリエンスを生むため（高価、コンテキストの欠如、トラブルシューティングの遅延）、組織にサイロがあればあるほど連結への要望は高まります。おそらく、多種のサイロからのデータのやりくりにもっとも面倒を感じているであろう回答者が、自社のより簡潔なオブザーバビリティソリューションを切望しています。

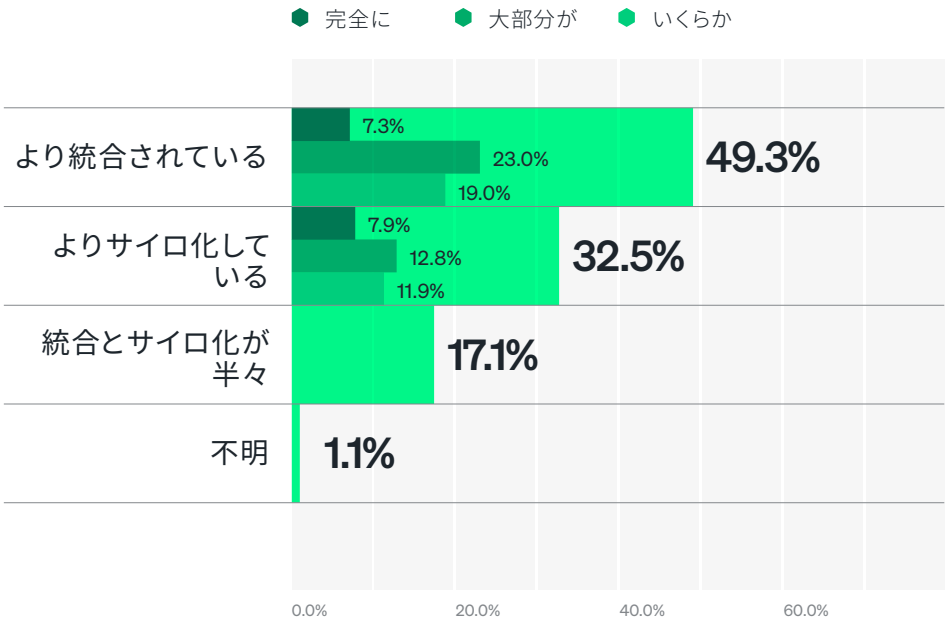



図 13. テレメトリデータの統合 vs サイロ化

### 地域別の考察

ヨーロッパと北米の組織では、統合されたテレメトリデータを保有する傾向が大きく（それぞれ 51% と 56%）、サイロ化データは少ない傾向にありました（それぞれ 31% と 25%）。いっぽう、アジア太平洋の組織は、統合されたテレメトリデータの保有がもっとも少なく (38%)、サイロ化されたデータの保有がもっとも多い傾向にありました (45%)。実際、15% は完全にサイロ化されていました。

### 組織規模別の考察

大規模組織は、統合されたテレメトリデータの保有が若干多く (54%)、サイロ化されたデータの保有が少ない傾向にありました (30%)。対照的に、小規模組織は、統合されたテレメトリデータの保有が少なく (40%)、サイロ化されたデータの保有が多い傾向にありました (45%)。

## 統合された可視化とダッシュボードの構築

データの可視化とダッシュボードの構築についても、同様のことが言えます。調査対象者の組織のテレメトリデータの可視化およびダッシュボード構築が、どのように統合または異種化されているかについての回答は、以下の通りです。

- 3分の2以上（68%）が、どちらかと言えば統合されている（テレメトリデータは単一のダッシュボードソリューションに可視化されている）と回答
- 約4分の1（23%）が、どちらかと言えば異種化されている（複数の可視化ソリューションがクロスコミュニケーションなく使用されている）と回答
- 10分の1以下（8%）が、どちらでもないと回答

オブザーバビリティのニーズを満たすために、複数ツールを使用している、という状況にもかかわらず、回答者の多くは多数のツールから得たデータを統合、可視化しているようです。これらの結果は、統合されたオブザーバビリティエクスペリエンスへの願望を示していると思われます。

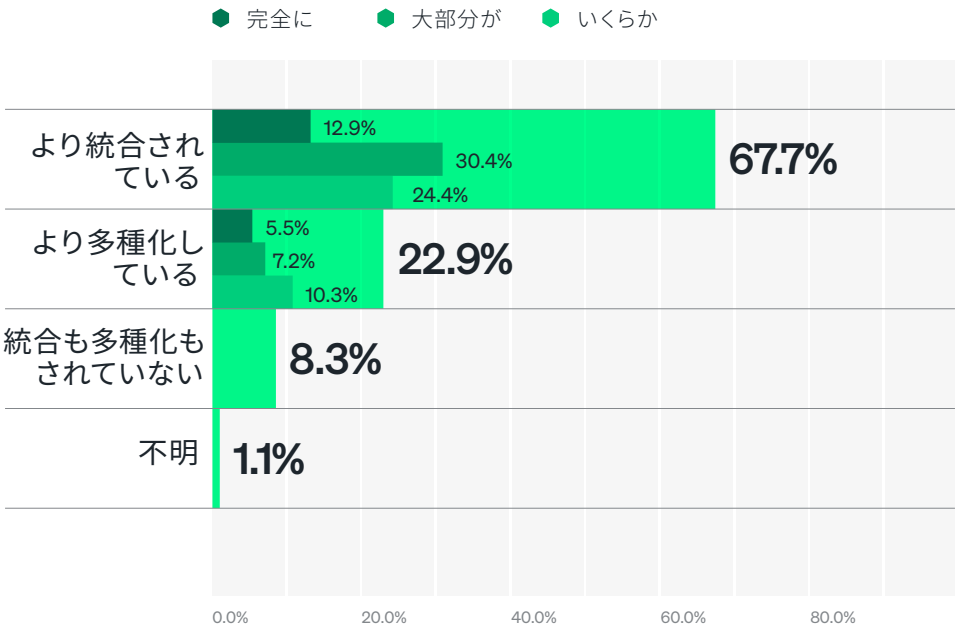



**図 14.** テレメトリデータの可視化／ダッシュボード構築の統合 vs 異種化

### 地域別の考察

北米の回答者は、単一のダッシュボードソリューションに可視化されたテレメトリデータの保有が多く（74%）、クロスコミュニケーションのない複数の可視化ソリューションの保有が少ない傾向にありました（18%）。アジア太平洋の回答者は、単一のダッシュボードソリューションに可視化されたテレメトリデータの保有がもっとも少なく（61%）、クロスコミュニケーションのない複数の可視化ソリューションの保有がもっとも多い傾向にありました（33%）。実際、11%は完全に異種化されていました。

### 役割別の考察

ITDMは、自社のテレメトリデータの可視化とダッシュボード構築はどちらかというと統合されていると考えており（71%）、一方で実務担当者はそう考えている人は少ない傾向にありました（66%）。

### 組織規模別の考察

中規模組織の回答者は、自社のテレメトリデータの可視化とダッシュボード構築はどちらかというと統合されているとの回答がもっとも多く（70%）、一方で小規模組織の回答者ではもっとも少ない傾向にありました（62%）。

**23%**

が、クロスコミュニケーションなしの複数の可視化ソリューションを使用（異種化テレメトリデータ）

# 戦略と組織

次に、調査対象者のオブザーバビリティ戦略とチーム組織について、単一プラットフォームか複数のポイントソリューションかの嗜好性や、ソフトウェアおよびシステム中断の検知方法、オブザーバビリティのニーズを促進するトレンド、役割別のオブザーバビリティの支持、オブザーバビリティの目的に対する認識、ソフトウェア開発ライフサイクルのどの段階でオブザーバビリティを使用するか、どのチームがいつオブザーバビリティを担当するかについて調査しました。

## 単一プラットフォームか複数のポイントソリューションか

過去 10 年間にわたり、オブザーバビリティベンダーは、専門のエンジニアリングチームが担当するスタック監視を支援する専用ツールを開発してきました。たとえば、New Relic は、アプリケーション開発者のための APM カテゴリーを開発し、先導してきました。他社は異なる専門ロールを選択し、その部門をうまく支援するための最良のツールを開発してきました。しかし、この慣行により、それぞれのツールで異なるエクスペリエンスとデータ保管が進み、複雑さが増大しました。

オブザーバビリティの威力を十全に実現するために、組織は、すべてのタイプとソースのテレメトリのための、統合された、基礎となるデータ保管を必要としています（まさに現在、New Relic がオブザーバビリティプラットフォームで提供しているものです）。統合されたエクスペリエンスにより、各エンジニアリングチームが全エンティティとその依存関係を 1 箇所で確認し、チームやツール、データのサイロを排除してより緊密に協働することができます。

しかし、オブザーバビリティに使用するツール数に関し、組織が戦略的に望むことは何でしょうか？彼らが望むのは、単一の、連結型のオブザーバビリティプラットフォームなのか、それとも寄せ集めて使用されたり、特定の監視性能のみに使用される、複数ポイントの最高品質のソリューションでしょうか？結果は以下の通りです。

- ほぼ半数（47%）が、単一の、連結型のオブザーバビリティプラットフォームを希望
- 3 分の 1 が複数のポイントソリューションを選択
- 5 分の 1 が、どちらでもよいと回答

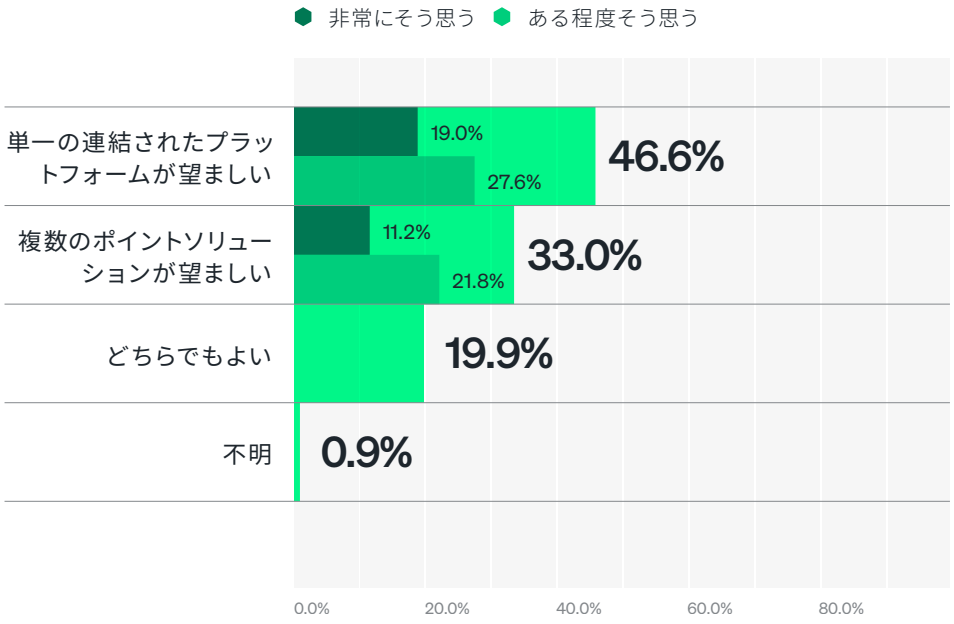



**図 15.** 単一の、連結されたプラットフォーム vs 複数のポイントソリューション

**47%**

が、単一の、連結型のオブザーバビリティプラットフォーム（オールインワン）を希望

これらの結果が示すのは、多くの組織が、オブザーバビリティのニーズを満たすために、単一のツール、オールインワンのアプローチを望んでいるということです。

しかし、多くの回答者が単一の連結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、94% が 2 つ以上の監視ツールを使用しています。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 2% であり、組織のテレメトリデータが完全に統合されているとの回答は 7% にとどまりました。

さらに、フルスタックオブザービリティの優先／実現を阻む主要な課題は何かを尋ねたところ、4 分の 1 が、監視ツールが多すぎることと回答しました。

これらをまとめると、オブザーバビリティの現状は、複数ツールで分断されていることがわかります。ただし、ツールの分断化はフルスタックオブザービリティへの重大な阻害要因であるという認識とともに、単一の、連結オブザーバビリティプラットフォームへの戦略的嗜好性が高まっていることが見てとれます。

**「我々が公表する戦略とビジョンは、より少ないプロバイダーでより多くの領域をカバーするというものです。妥当であれば、各業務にそれぞれベンダーを配するのではなく、複数の業務に対して 1 つのベンダーを利用するようにしています。」**

SVP 兼 CTO、大手小売企業

### 地域別の考察

アジア太平洋地域では、55% の回答者が、単一の、連結プラットフォームが好ましいと回答しました。

### 役割別の考察

約 3 分の 1（32%）の非エグゼクティブマネージャーが、単一の、連結プラットフォームが非常に好ましいと回答し、対してエグゼクティブおよび実務担当者でそう回答したのは 17% でした。

### 業界別の考察

金融／保険・工業／原料／製造業界では、半数以上の回答者が、単一の、連結プラットフォームが好ましいと回答しています（それぞれ 60%、54%）。

# ソフトウェアおよびシステム中断の検知

オブザーバビリティは、組織のパフォーマンスにどのような影響を与えるのでしょうか？調査の結果は以下の通りです。

- ほぼ半数（46%）が、複数の監視ツールを通じて最初に中断を認知
- 約 5 分の 1（21%）のみが、1 つのツールを通じて最初に中断を検知

つまり、回答者の約 3 分の 2（67%）が、1 つ以上のツールを通じて最初に中断を検知すると回答したことになります。これだけ多数が複数の監視ツールを通じて最初の中断を検知するというのは、回答者がオブザーバビリティ目的でデプロイしている監視ツール数の多さについてすでに見てきたことを考えれば、納得の数字です。

しかし、注目すべきは、多くの組織において、いかにプロセスがいまだに手動であるかということです。以下のことが判明しました。

- ほぼ 4 分の 1（22%）が、特定の時間に行われる手動でのシステムチェック／検査を通じて最初に中断を検知
- 約 10 分の 1（11%）が、インシデントチケットおよび顧客や従業員からの苦情を通じて最初に中断を検知

つまり、3 分の 1 の回答者は、いまだに手動のチェックや検査、もしくはインシデントチケットや苦情を通じて最初に中断を検知していました。

さらに、回答者がどのように中断を検知しているかと、彼らのテレメトリデータがどのように統合されているかには、明らかな関連性があります。概して、テレメトリデータが統合されているほど、中断の検知は単一のオブザーバビリティツールを通じてなされていました。

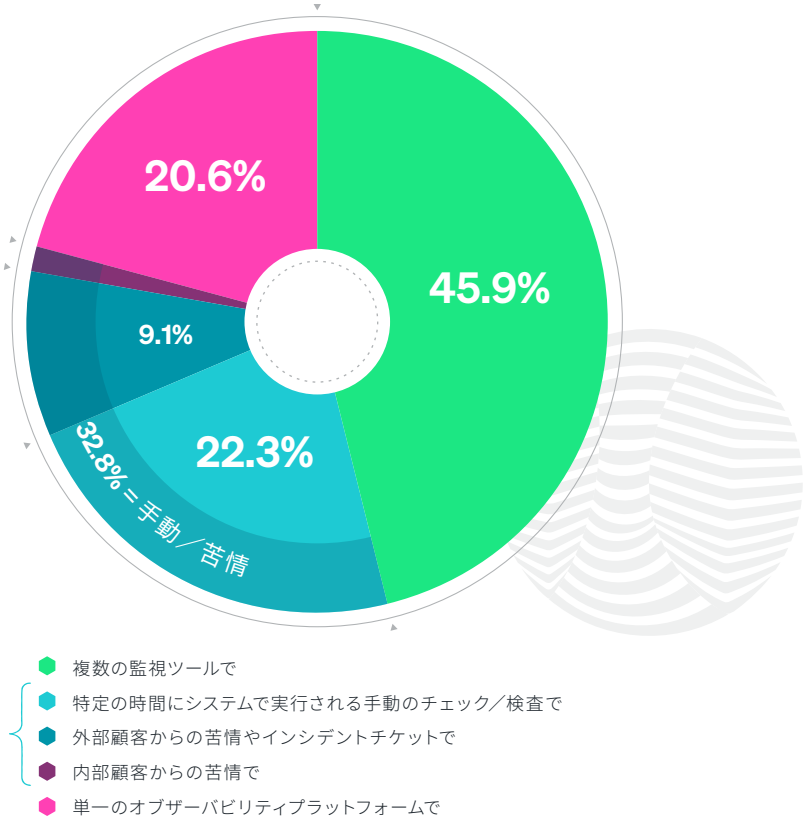



**図 16.** 回答者がどのようにソフトウェアおよびシステム中断を検知しているか

**組織規模別の考察**

大規模組織は、複数のツールを通じて中断を検知している傾向が高く、いっぽうで小規模組織は、マニュアルでのチェックや検査、また複数のツールを使用している傾向にありました。

**33%**
は、手動のチェックや検査、苦情を通じて最初に中断を検知

# オブザーバビリティを促進するトレンド

では、どのようなテクノロジー戦略とトレンドが、オブザーバビリティのニーズを促進しているのでしょうか？

モダンアプリケーションは、通常クラウドで運用され、数百ものコンポーネントに依存しており、その各コンポーネントがさらに監視の課題とセキュリティリスクを生み出します。クラウドの導入、クラウドネイティブなアプリケーションのアーキテクチャーによりサイバーセキュリティの脅威が高まるなかで、セキュリティとガバナンス、リスク、コンプライアンスへの注力が、調査対象の組織においてオブザーバビリティのニーズ促進という点でもっともよく言及される戦略またはトレンドだった（49%）のは当然のことです。

クラウドネイティブなフロントエンドのアプリケーションアーキテクチャーの開発、カスタマーエクスペリエンス管理への注力の強化、マルチクラウドなバックエンド環境への統合についても、いずれも 40% 以上言及されています。

トップの回答ではなかったものの、39% の回答者が、OpenTelemetry などのオープンソースの技術を、36% がサーバレスコンピューティングを、36% がアプリケーションとワークロードのコンテナ化を採用していると回答しました。すべて、オブザーバリティが統合的なアプローチを必要とするトレンドです。

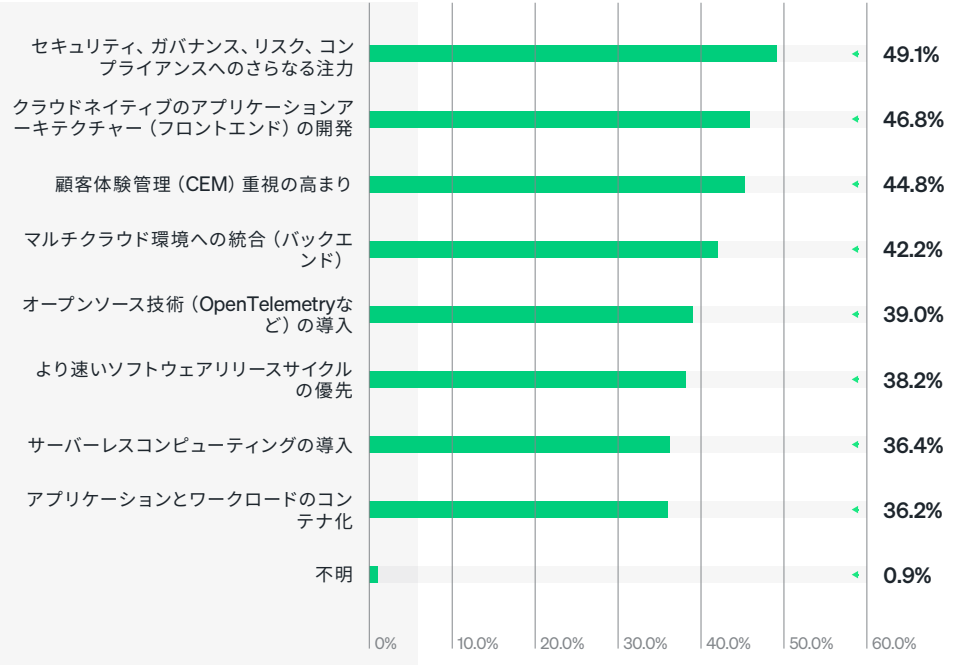



図 17. オブザーバビリティのニーズを促進するテクノロジー戦略とトレンド

### 地域別の考察

クラウドネイティブなアプリケーションアーキテクチャー（フロントエンド）の開発が、アジア太平洋地域においてオブザーバビリティのニーズを促進するトップの戦略でした（53%）。

### 役割別の考察

クラウドネイティブなアプリケーションアーキテクチャー（フロントエンド）の開発は、エグゼクティブにとってトップの促進要因であり（50%）、非エグゼクティブマネージャーおよび実務担当者にとっては第 2 位の促進要因でした（47%）。

### 業界別の考察

エネルギー／ユーティリティおよび NPO 業界では、マルチクラウド環境への統合がトップの促進要因との回答が多かったのに対し、政府機関ではクラウドネイティブなアプリケーションアーキテクチャーとの回答が多く、また医療／製薬業界ではサーバレスコンピューティングの導入との回答が多い傾向にありました。サービス／コンサルティング業界では、トップ要因として、セキュリティ、クラウドネイティブ、マルチクラウドが均等に分かれました。

**「クラウドに移行したため、監視すべきものが増え、追加的なニーズも多くなりました。オブザーバビリティは、標準的な設備の監視というだけでなく、それらすべての異なる側面を確認し、表示するための方法となっています。」**

シニアエンジニア、大手金融企業

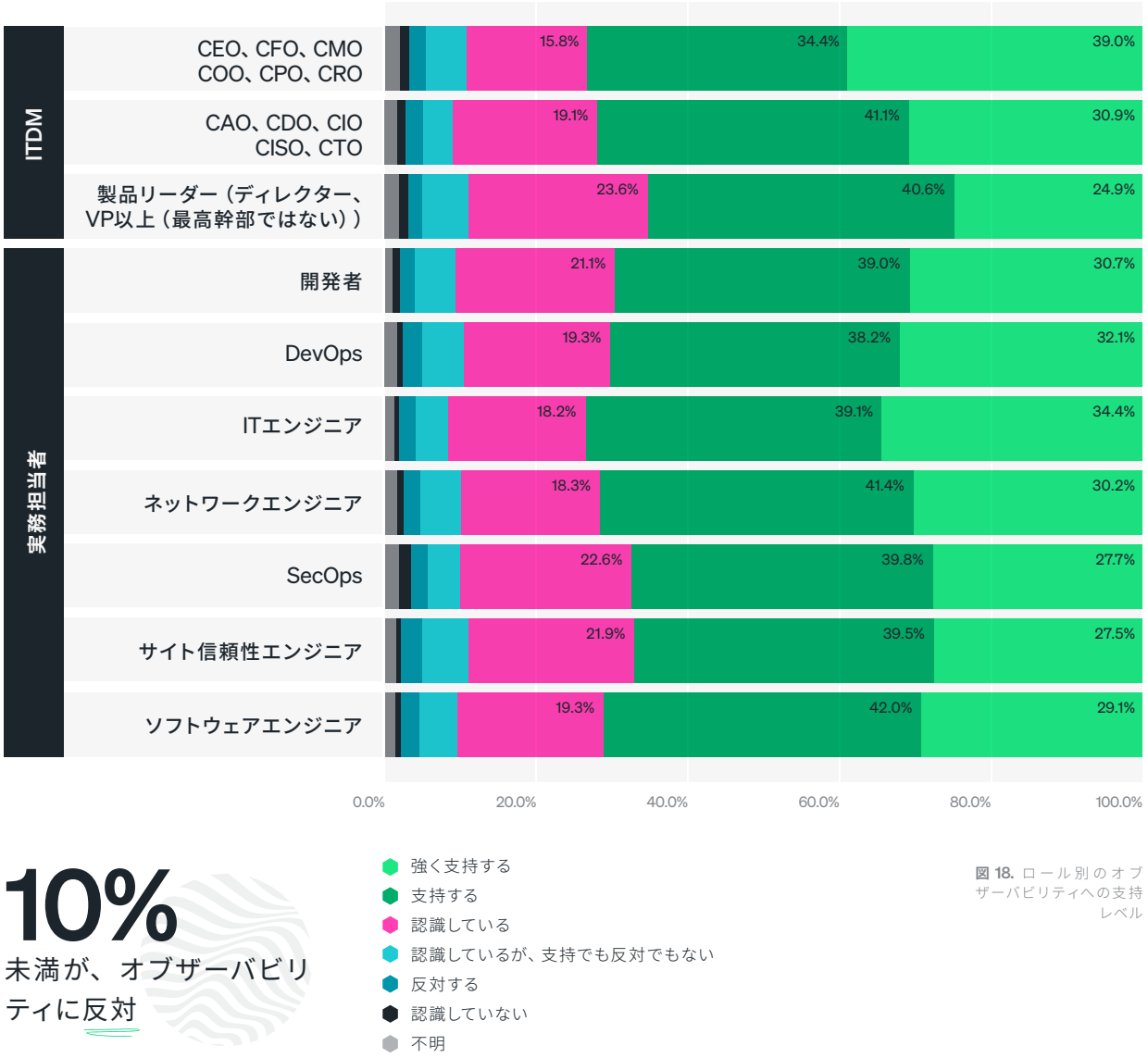
# オブザーバビリティへの支持

回答者の組織において、オブザーバビリティをもっとも熱心に支持していたのは誰でしょうか？調査対象者に、自社組織の複数ロールにおける支持の程度差について尋ねました。

全般的に、調査対象者は、すべてのロールがオブザーバビリティに反対するよりも支持していると回答しました。一見すると、支持の程度に特定の傾向はあまりないように見えます。しかし、もっとも熱心にオブザーバビリティを支持するのは技術に特化しない最高幹部たちであり（39%）、しかも概して技術に特化した最高幹部よりも多い（31%）と調査回答者が考えたことは注目に値します。ほかに特筆すべき点は以下の通りです。

- 全般的にオブザーバビリティへの反対は少ない（10%未満）
- 本レポートの定義においてフルスタックオブザービリティがある、または成熟したオブザーバビリティの実践を行っている回答者は、それらの 2 要素がない回答者に比べ、オブザーバビリティへの強い支持が顕著である
- オブザーバビリティを完全に中核的な事業目標の達成要因であると考えている組織の回答者は、ほぼすべてのロールにおいてオブザーバビリティへの強い支持が顕著である

個別のロールやチームがオブザーバビリティの価値を認め、支持していると、組織はデプロイメント拡張と予算増額を行なう傾向にあるため、これらの結果は、今後のオブザーバビリティデプロイメント計画および予算計画の根拠となると思われます。




**10%**
未満が、オブザーバビリティに反対

図 18. ロール別のオブザーバビリティへの支持レベル

# オブザーバビリティの目的

人々が認識しているオブザーバビリティの目的とは何なのか、すなわち実務担当者と ITDM は、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るのか、もしくはインシデントへの対応や予防強化に必要な要因であると考えているのかについて調査を行いました。結果は以下の通りです。

- 半数が、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る
- 4 分の 1 以上（28%）が、事業目標とインシデント対応のいずれも同様に、組織のオブザーバビリティが達成要因となると考えている
- 5 分 1 あまり（21%）が、オブザーバビリティをインシデントへの対応と予防強化に必要な要因であると回答

4 分 3 以上（78%）が、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事実が、オブザーバビリティが取締役会レベルの保証事項となったことを示唆しています。

**78%** が、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示唆

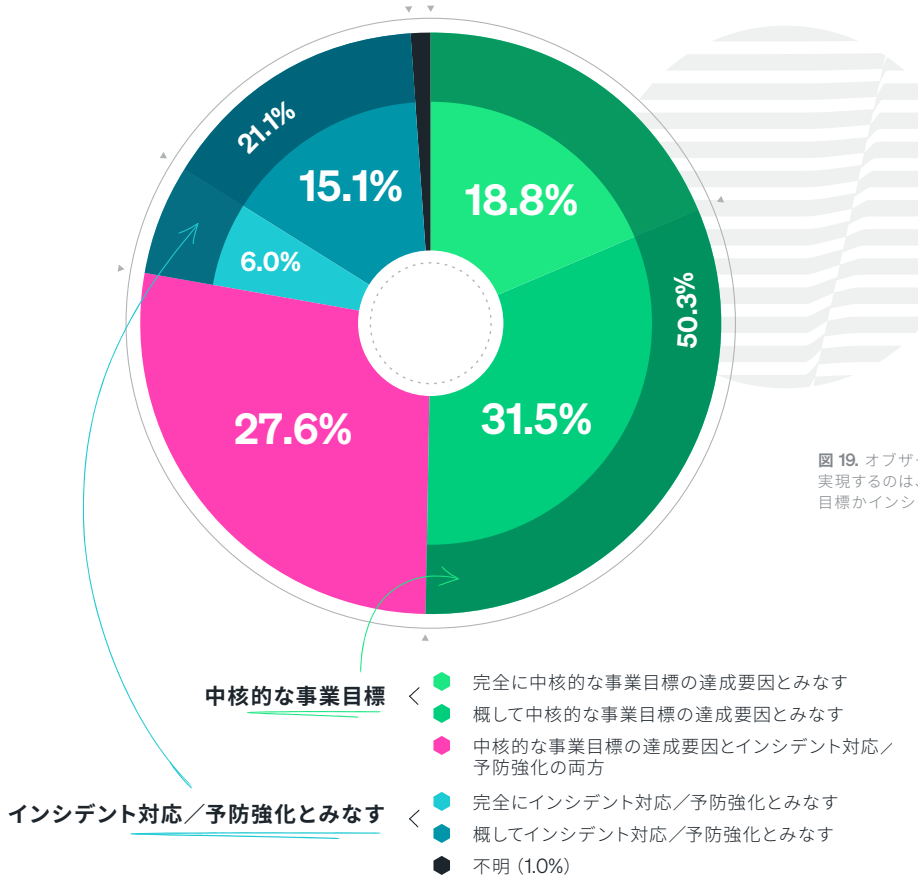



図 19. オブザーバビリティが実現するのは、中核的な事業目標かインシデント対応／予防強化

### 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、アジア太平洋地域の回答者でもっとも多く（58%）、これに対して北米とヨーロッパでは 48% でした。反対に、オブザーバビリティをインシデントへの対応と予防強化に必要な要因であるとする回答は、アジア太平洋地域の回答者でもっとも少なく（15%）、これに対して北米では 22%、ヨーロッパでは 24% でした。

### 役割別の考察

当然のことながら、エグゼクティブは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る傾向が最も高く（56%）、これに対して非エグゼクティブマネージャーでは 51%、実務担当者では 48% でした。反対に、エグゼクティブではオブザーバビリティをインシデントへの対応と予防強化であるとする回答が最も低く(16%)、これに対して非エグゼクティブマネージャーでは 17%、実務担当者では 24% でした。

### 組織規模別の考察

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、中規模組織の回答者で最も多く（54%）、小規模組織では少ない傾向にありました（42%）。また、オブザーバビリティをインシデントへの対応と予防強化であるとする回答は、中規模組織で最も少なく（19 %）、大規模組織では多い傾向にありました（25%）。

### 業界別の考察

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、小売／消費者（57%）、金融／保険（54%）、IT ／テレコミュニケーション（52%）業界でもっとも多い傾向にありました。反対に、オブザーバビリティをインシデントへの対応と予防強化に必要な要因であるとする回答は、エネルギー／ユーティリティ（33%）、サービス／コンサルティング（28%）、NPO ／不特定（26%）業界でもっとも多い傾向にありました。

# オブザーバビリティを使用した SDLC の各段階

元来、監視はソフトウェア開発ライフサイクル（SDLC）の運用（稼働）段階に焦点を当てたものでした。データは SDLC 全体に拡張できる可能性があり、計画、ビルド、デプロイ、運用、保守においてチームのよりデータドリブンな活動を可能にします。これまで、SDLC の前期段階（計画、ビルド、デプロイ）で作業を行なってきた多くのエンジニアは、オブザーバビリティが彼らの作業向上に寄与するとは認識していませんでした。

そうであっても、多くの回答者が、SDLC のすべての段階において、ある程度のデータドリブンなオブザーバビリティによるインサイトを利用してきたことがわかりました。しかし、各段階で完全なオブザーバビリティを活用している回答者は、約 3 分の 1 しかいませんでした。

- **計画：**34% が、計画段階で完全なオブザーバビリティを活用
- **ビルド：**30% が、ビルド段階で完全なオブザーバビリティを活用
- **デプロイ：**34% が、デプロイ段階で完全なオブザーバビリティを活用
- **運用：**37% が、運用段階で完全なオブザーバビリティを活用

成熟したオブザーバビリティの実践（本レポートでの定義による）を行なう回答者では、実践を行っていない回答者に比べ、SDLC の全段階における完全なオブザーバビリティの活用が顕著でした（計画が 53%、ビルドが 46%、デプロイが 51%、運用が 54%）。

フルスタックオブザーバビリティ（本レポートでの定義による）を実践している回答者でも、まだの回答者に比べ、SDLC の全段階において、完全なオブザーバビリティの活用が顕著でした（計画が 38%、ビルドが 36%、デプロイが 42%、運用が 46%）。

開発者は、新機能の提供ではなくデバッグ作業に時間を費やしすぎていることが多々あります。彼らにとって、SDLC 全体を能率化できるオールインワンのオブザーバビリティプラットフォームは不可欠です。

### 地域別の考察

アジア太平洋の回答者は、計画（72%）およびビルド（75%）段階で拡張的または完全なオブザーバビリティを使用している傾向がもっとも高く、北米では、デプロイ（75%）および運用（81%）段階でもっとも活用している傾向にありました。ヨーロッパの回答者では、計画で 63%、ビルドで 65%、デプロイで 67%、運用で 69% と、拡張的または完全なオブザーバビリティの使用が全般的に少ない傾向にありました。

### 業界別の考察

全体としては、金融／保険、小売／消費者業界では、運用段階での 83% をはじめ、SDLC の全段階における拡張的または完全なオブザーバビリティの活用がもっとも多く、次いで IT ／テレコミュニケーション業界が多い傾向にありました。政府機関の回答者は、SDLC の全段階における拡張的または完全なオブザーバビリティの活用がもっとも少なく、次に教育業界が少ない傾向にありました。

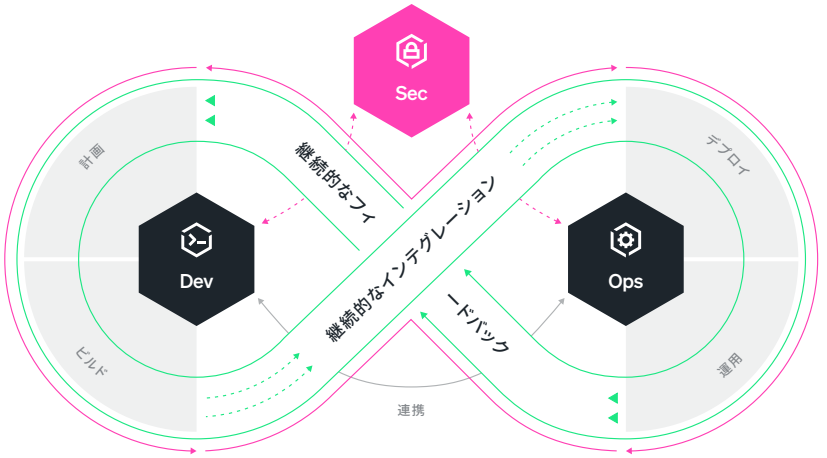



図 20. DevSecOps のソフトウェア開発ライフサイクル

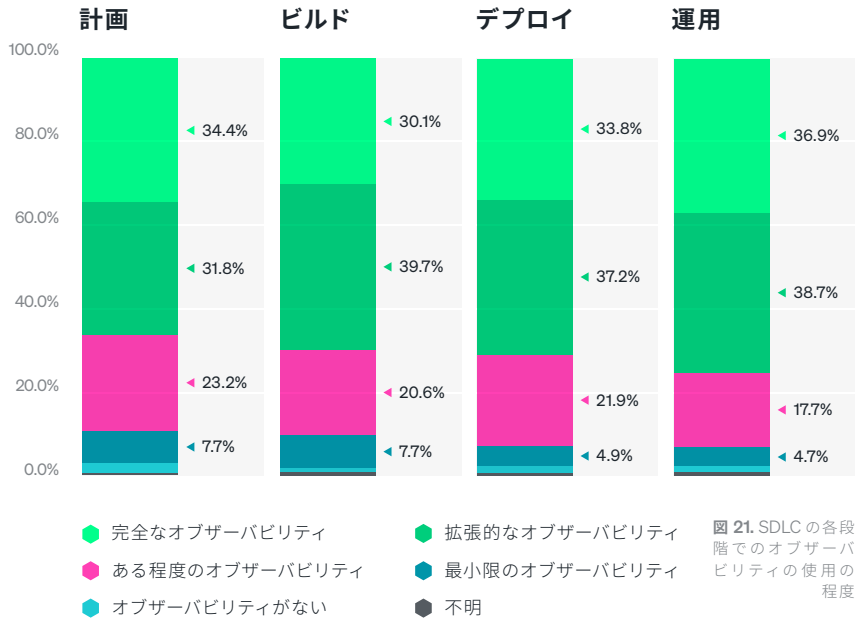



図 21. SDLC の各段階でのオブザーバビリティの使用の程度

# オブザーバビリティを担当するチーム

調査対象者に、自社組織でオブザーバビリティの実施、保守、使用を主に担当するのはどのチームかを尋ねました。結果は以下の通りです。

- IT オペレーションチームがオブザーバビリティを担当することがもっとも多く、次いでネットワークオペレーションと DevOps チームが多い傾向にありました
- アプリケーション開発と SRE チームは、オブザーバビリティの保守、使用よりも実施を担当することがより多い傾向にありました
- SecOps と DevSecOps チームは、オブザーバビリティの実施、保守よりも使用を担当することがより多い傾向にありました

多くの組織に専門の IT オペレーションチームが配備されている一方、オブザーバビリティを主に担当する専門の DevSecOps や SecOps チームがいる組織は少ない傾向にありました。これは、各セキュリティチームが個別のセキュリティ関連オブザーバビリティツールを使用していることを示している可能性があります。包括的な、オールインワンのオブザーバビリティアプローチは、開発、セキュリティ、オペレーションの各チームがシームレスに協働する（DevSecOps）ようになる文化的移行を支援します。組織はセキュリティを優先させるため、今後数年間でこの動きがどのように変化していくかは興味深いところです。

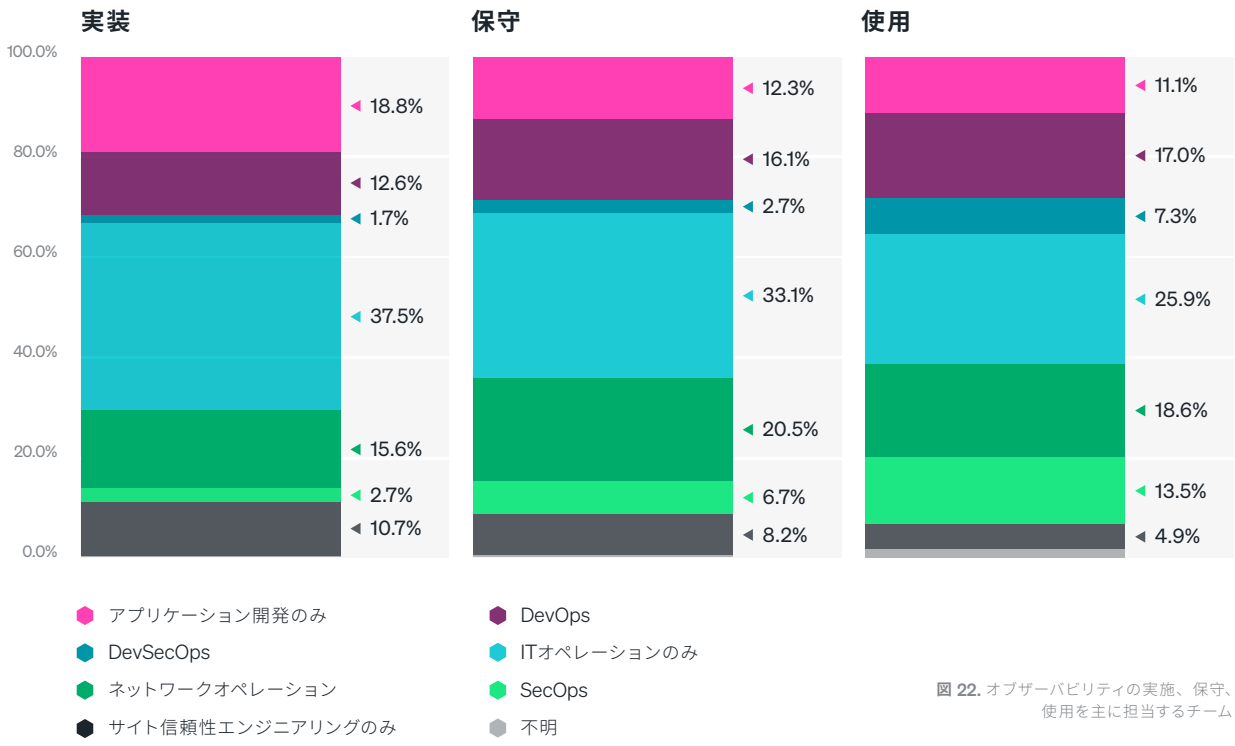



**図 22.** オブザーバビリティの実施、保守、使用を主に担当するチーム

### 地域別の考察

北米では、IT オペレーションチームのオブザーバビリティへの関与がほかの地域よりやや高い傾向にありました。一方で、アジア太平洋では、DevSecOps チームのオブザーバビリティへの関与がほかの地域よりやや高い傾向にありました。

# 価格、請求、支出

オブザーバビリティツールに関する予算配分と、価格および請求の嗜好性について調査を行いました。

## 予算配分

調査対象者に、現在オブザーバビリティツールに配分している IT 予算の割合を尋ねたところ、結果は以下の通りとなりました。

- もっとも多数（69%）が 5% 超～ 15% 未満、14% が 15% 超を配分
- 3% のみが 20% 超を配分
- 配分が 5% 未満なのは 16% のみ

つまり昨年同様に、オブザーバビリティツールへの IT 予算配分は、多くの組織において 20% 未満でした。

より成熟したオブザーバビリティの実践（本レポートでの定義による）を行っている組織は、オブザーバビリティにより多額を支出している傾向にありました。その 4 分の 1 以上（29%）が 15% 超を配分しており、これに比べて、成熟度の少ない組織では 14% でした。

また、多くの性能をデプロイしている組織は、最大のオブザーバビリティ予算を配分している傾向にありました。20% 超を配分するうちのほぼ 4 分の 3（73%）が、また 15% 超を配分するうちの半数以上（57%）が、9 つ以上の性能をデプロイしていました。

来年度の予算計画について確認する。

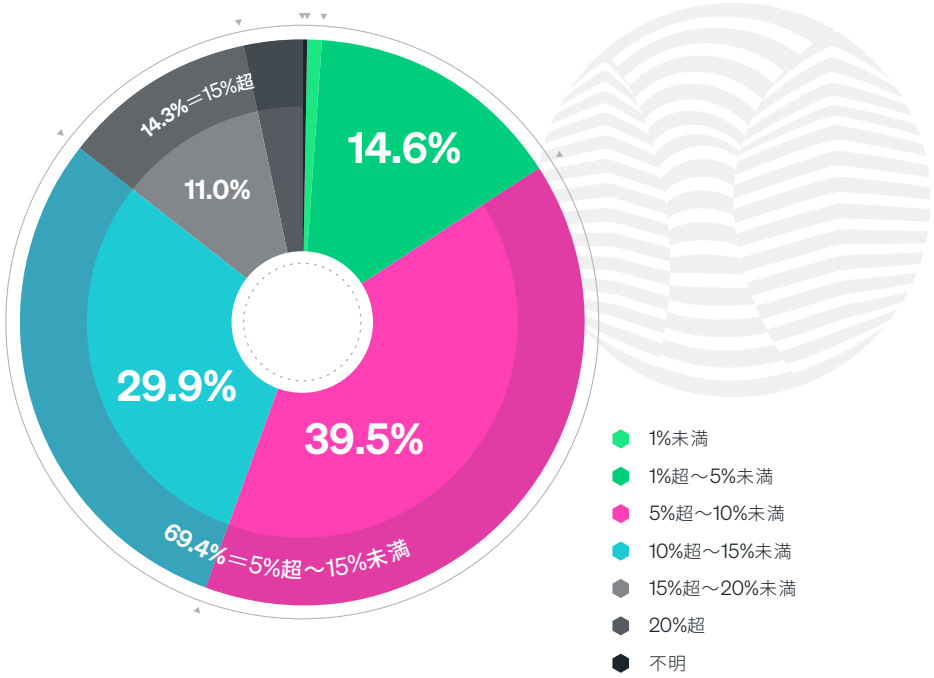



図 23. オブザーバビリティツールへの IT 予算配分の割合

### 地域別の考察

アジア太平洋地域の回答者は、オブザーバビリティツールに 10% 超の IT 予算を配分している傾向が高く（50%）、いっぽうでヨーロッパおよび北米の回答者では 10% 未満との回答が多くなりました（それぞれ 60% と 54%）。また、アジア太平洋の回答者の 21% が 15% 以上を配分しており、これに比べて北米の回答者は 14%、ヨーロッパの回答者は 11% でした。

### 業界別の考察

エネルギー／ユーティリティ、工業／原料／製造業界の回答者では、オブザーバビリティツールに IT 予算の 10% 超～ 15% 未満を配分しているとの回答がトップで、その他の全業界では 5% 超～ 10% 未満を選択する傾向にありました。これは、エネルギー／ユーティリティおよび工業／原料／製造業界ではダウンタイムにより敏感であること、規制が厳しいこと、また AI、ML、IoT などの技術を使用している傾向が高いことが理由として考えられます。

# 価格設定の特性

オブザーバビリティツール／プラットフォームに関し、価格設定モデルへの嗜好性に加え、どんな価格設定の特性が回答者とその組織にとって重要性が高いかを調査しました。結果は以下の通りです。

- 全体として、予算に見合う価格設定がもっとも重要であるとされ、価格設定の透明性、全テレメトリにわたるシングルライセンスのメトリクス、開始時点の低価格も多く言及
- ハイブリッドな価格設定モデルが、ユーザー／ホスト／エージェントベースのみの価格設定モデルよりも高くランク付け
- 単一 SKU と SKU バンドルのアプローチは同程度

2 種のハイブリッド価格設定モデル（ハイブリッドユーザー＆データ取り込みの価格設定、およびハイブリッドホスト＆データ取り込みの価格設定）が市場で優勢な価格設定モデルであり、これらのオプションが調査では上位にランク付けされました。回答者は、データ取り込みの使用ベースの価格設定への嗜好性が顕著でした。

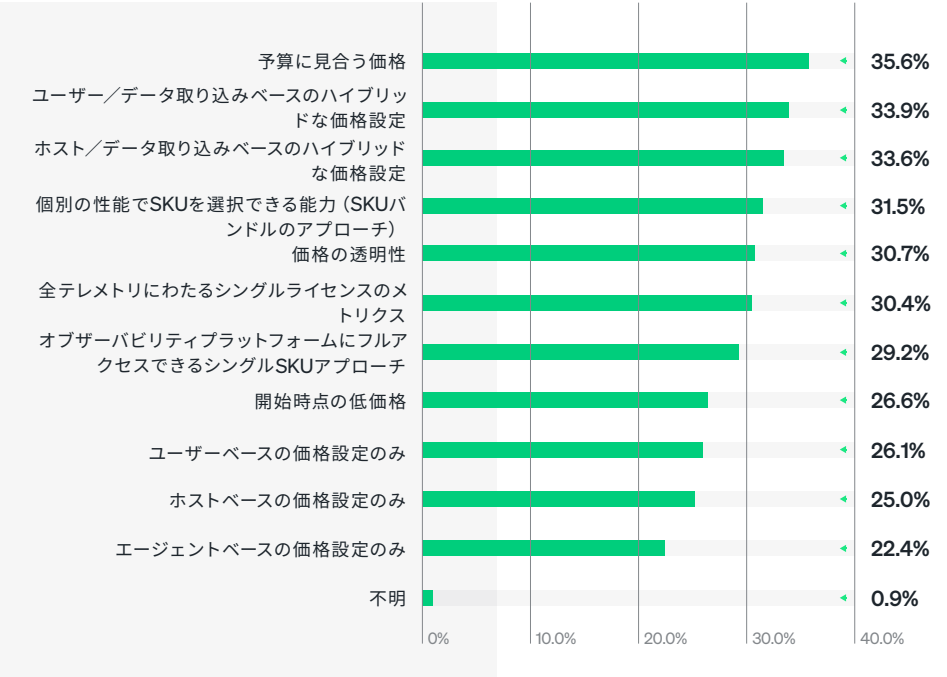



**図 24.** 価格設定の特性に関する嗜好

### 地域別の考察

北米の回答者では、予算に見合う価格設定の選択がもっとも多く、また全テレメトリにわたるシングルライセンスのメトリクスも他の地域に比べて好まれる傾向にありました。一方で、アジア太平洋の回答者は、ハイブリッドな価格設定モデルをもっとも好む傾向が見られました。

### 役割別の考察

役割別の考察：興味深いことに、実務担当者は、トップの回答として予算に見合う価格設定を選択する傾向にありました。また、開始時点の低価格も選択する傾向が見られました。しかし、エグゼクティブは、予算に見合う価格設定を 6 番目に重要であるとし、代わりにハイブリッドな価格設定モデルをもっとも好ましいと回答しました。非エグゼクティブマネージャーでは、SKU バンドルのアプローチ、全テレメトリへのシングルライセンスのメトリクス、ホスト／エージェントベースのみの価格設定モデルへの嗜好性がもっとも低くなりました。

### 組織規模別の考察

小規模組織では、シングル SKU アプローチ（34%、中規模と大規模では 29%）、開始時点の低価格（31%、中規模と大規模では 26%）への嗜好性がやや高くなりました。大規模組織では、価格設定の透明性（33%、小規模で 31%、中規模で 29%）がやや高くなりました。

# 請求の特性

調査対象者にとってどのような請求モデルと特性がもっとも重要かについても、調査を行いました。結果は以下の通りです。

- 最低月額のない従量課金制の、使用量を拡大できる柔軟性が全体のトップ
- 従量課金制の請求モデル（使用が月ごとの規定量または実使用量にもとづく）が、サブスクリプションベースのモデルより好まれる
- あらゆるテレメトリデータタイプを取り込める能力、ペナルティなしのオートスケール、予測可能な支出も上位にランク付け

本調査の実施期間に ETR が ITDM に対して行った補足的な聞き取り調査では、調査対象者は価格と請求の予測可能性をもっとも望んでいました。技術的な設計や価格設定、請求モデルにかかわらず、ITDM は請求額の正確な事前予測能力を欲していました。

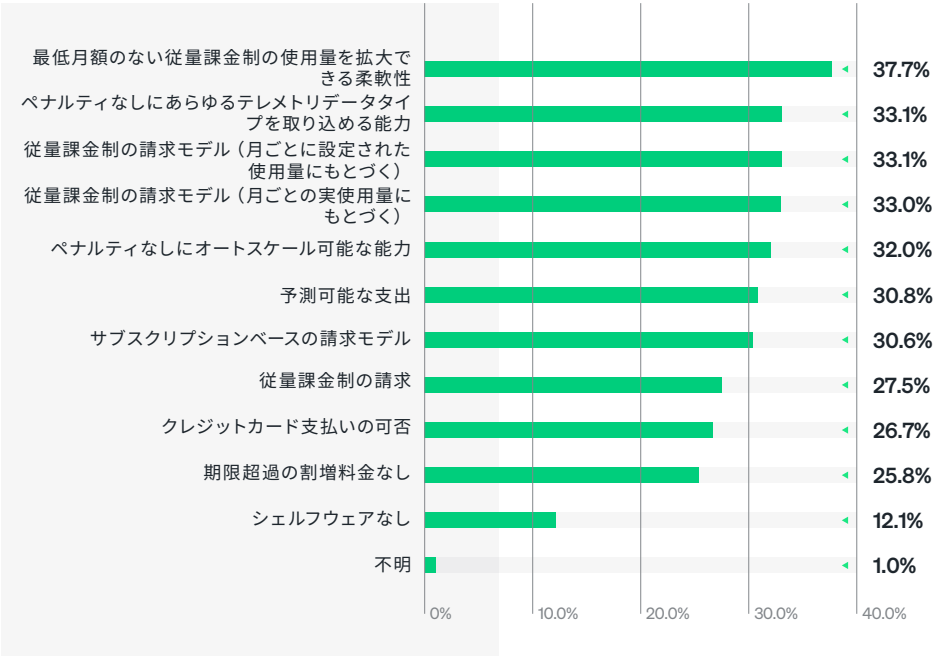



図 25. 請求の特性に関する嗜好

### 地域別の考察

ヨーロッパの回答者は、請求モデルのタイプや、最低月額のない従量課金制の使用量拡大の柔軟性をもっとも考慮しない傾向にありました。アジア太平洋の回答者は、ペナルティなしでオートスケールする機能を気にする人が少ない傾向にありました。北米の回答者は、クレジットカード支払いの可否と、プレミアムの割増料金やシェルフウェアをより考慮する傾向にありました。

### ロール別の考察

実務担当者は、予測可能な支出をもっとも考慮していました。非エグゼクティブマネージャーは、サブスクリプションベースの請求モデル、従量課金制、シェルフウェアなしへの嗜好性がもっとも低い傾向にありました。

### 組織規模別の考察

小規模組織は、アクティブな設定使用量ではなく月ごとに設定された使用量にもとづく従量課金制モデルをより好む傾向にありました。中規模組織は、ペナルティなしであらゆるテレメトリデータタイプを取り込める能力（34%、対して小規模は 32%、大規模は 33%）と従量課金制（34%、対して小規模は 32%、大規模は 29%）についての考慮がやや高い傾向にありました。大規模組織は、最低月額のない従量課金制の使用量を拡大できる柔軟性（42%、対して中規模は 35%、小規模は 33%）、また予測可能な支出（36%、対して中規模は 32%、小規模は 29%）をもっとも考慮する傾向にありました。

**「実際に支出が行われる 16 ～ 18 か月前に予算を組まないといけないことは多々あります。正確に予測ができる限り、明らかにそれが好ましい方法です。」**

SVP 兼 CTO、大手小売企業

# オブザーバビリティの利点

ここからは、良い点について見ていきましょう。オブザーバビリティの主な利点全般について、またどんな使用事例で活用されているか、サービスレベルのメトリクス改善に役立っているか、どんな点でソフトウェアエンジニアや開発者の生活の向上にもっとも貢献しているかについて、調査を行いました。

回答者は、現在のオブザーバビリティのデプロイメントの結果として、明らかに利点を感じていることがわかりました。オブザーバビリティは、明白な、ポジティブなビジネスインパクトを生み出し続けています。以下が改善された点です。

- アップタイム、パフォーマンス、信頼性
- 運用効率
- カスタマーエクスペリエンス
- イノベーション
- ビジネスと収益の成長

これらの結果は、オブザーバビリティがいかに組織のビジネス、テクノロジー、そして収益を変革しているかを示しています。

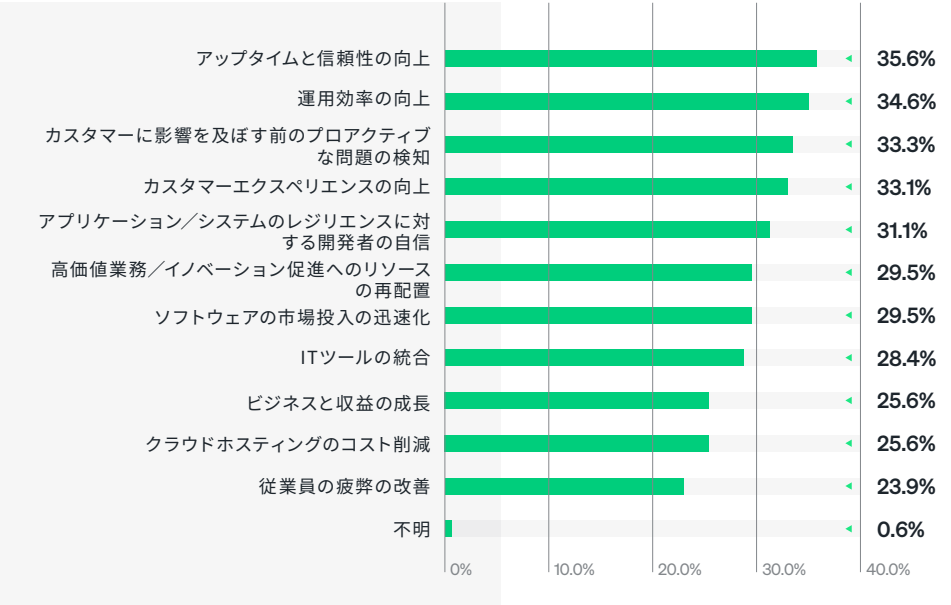



**図 26.** オブザーバビリティのデプロイメントにより得られる主な利点

### 地域別の考察

ヨーロッパの回答者は、オブザーバビリティの利点として、アップタイムと信頼性の改善（32%）と、顧客に影響を及ぼす前のプロアクティブな問題の検知（28%）との回答がもっとも少ない傾向にありました。アジア太平洋の回答者では、オブザーバビリティの利点は顧客に影響を及ぼす前のプロアクティブな問題の検知との回答が最も多く（40%）、IT ツール構築の連結（25%）とクラウドホスティングのコスト削減（22%）との回答が少ない傾向にありました。

### 役割別の考察

エグゼクティブは、組織の運用効率の向上との回答が少なく（31%）、実務担当者では多い傾向にありました（36%）。非エクゼクティブマネージャーは、顧客に影響を及ぼす前のプロアクティブな問題の検知に組織が恩恵を受けているとの回答が最も多く（40%）、ビジネス／収益の成長との回答が最も少ない傾向にありました（19%）。

### 組織規模別の考察

小規模組織の回答者は、オブザーバビリティの利点は IT ツール構築の連結（38%）、ビジネス／収益の成長（32%）との回答が最も多く、顧客に影響を及ぼす前のプロアクティブな問題の検知（26%）である、との回答が最も少ない傾向にありました。中規模組織の回答者は、アップタイムと信頼性の改善（33%）とビジネス／収益の成長（23%）との回答が少ない傾向にありました。大規模組織の回答者は、運用効率の向上（39%）、顧客に影響を及ぼす前のプロアクティブな問題の検知（38%）、カスタマーエクスペリエンスの向上（36%）との回答が多い傾向にありました。

### 業界別の考察

エネルギー／ユーティリティ業界の回答者は、オブザーバビリティの利点として、アプリケーション／システムのレジリエンスに対する開発者の自信の高さとの回答が多い傾向にありました（51%）。政府機関の回答者は、従業員の疲弊の改善との回答が多い傾向にありました（55%）。医療／製薬業界の回答者は、カスタマーエクスペリエンスの向上（43%）、ビジネスと収益の成長（39%）との回答が多い傾向にありました。IT ／テレコミュニケーション業界の回答者は、高価値業務／イノベーション促進へのリソースの再配置との回答が多い傾向にありました（35%）。NPO ／不特定業界の回答者は、運用効率の向上（52%）との回答が多い傾向にありました。サービス／コンサルティング業界の回答者は、アップタイムと信頼性の改善との回答が多い傾向にありました（49%）。

# 使用事例

回答者にとってオブザーバビリティが最も重要だった技術的な使用事例／目的について、調査を行いました。その結果、多岐にわたる使用事例のなかに、以下の共通点が示されました。

1. クラウドリソースの使用と支出の最適化 (31%)
2. デジタルカスタマーエクスペリエンスの競争優位性の改善、獲得に向けた DX の取り組みの支援 (31%)
3. コンテナ化とサーバーレス環境の管理 (29%)
4. 新製品／サービスの市場投入の迅速化 (29%)
5. DevOps への組織的な IT 移行の支援 (29%)

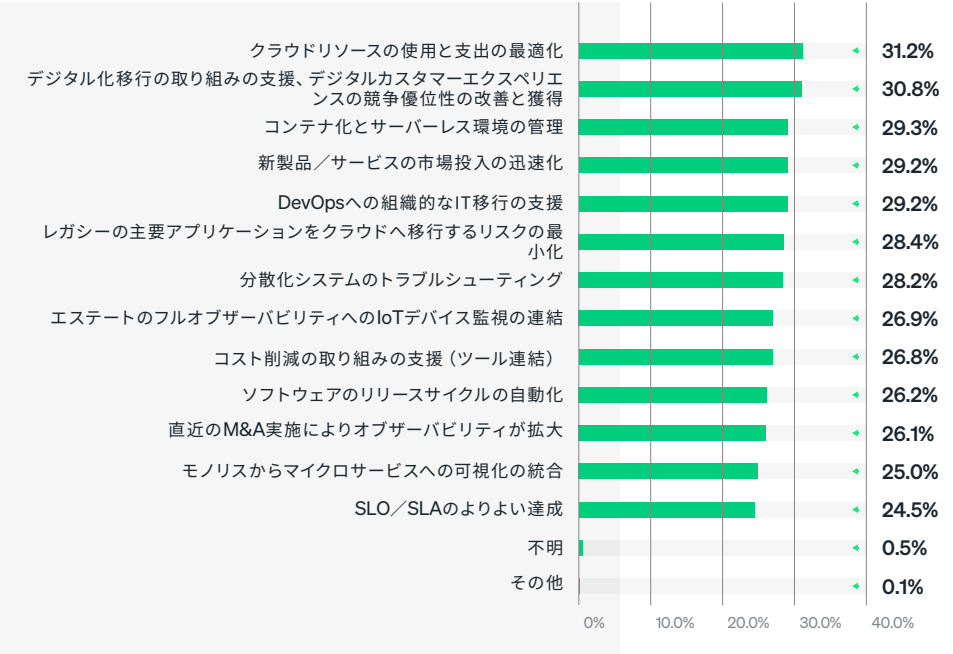



**図 27.** オブザーバビリティの使用事例／目的

### 地域別の考察

アジア太平洋の回答者では、DX の取り組みの支援がトップの回答で、次いで新製品／サービスの市場投入の迅速化、中核的なレガシーアプリケーションのクラウド移行のリスク最小化、コンテナ化とサーバーレス環境の管理でした。北米の回答者では、DevOps への組織的な IT 移行の支援が 2 番目の回答でした。ヨーロッパでの回答は、全地域での平均的な結果と同様でした。

### 役割別の考察

エグゼクティブは、自社組織が、DevOps への組織的な IT 移行の支援 (34%)、自社エステートのフルオブザーバビリティへの IoT デバイス監視の連結 (30%)、コストカットの取り組みの支援 (29%) にオブザーバビリティを活用しているとの回答がもっとも多い傾向にありました。非エグゼクティブマネージャーは、自社組織が、分散化システムのトラブルシューティング (31%)、SLO/SLA のよりよい達成 (27%) にオブザーバビリティを活用しているとの回答がもっとも多い傾向にありました。実務担当者は、自社組織が、中核的なレガシーアプリケーションのクラウド移行のリスク最小化にオブザーバビリティを活用しているとの回答がもっとも多い傾向にありました (30%)。

### 組織規模別の考察

小規模組織の回答者は、コストカットの取り組みの支援 (34%) にオブザーバビリティを活用しているとの回答がもっとも多く、いっぽうで大規模組織ではもっとも少ない傾向にありました (26%)。大規模組織の回答者は、コンテナ化とサーバーレス環境の管理 (35%)、DevOps への組織的な IT 移行の支援 (33%)、ソフトウェアのリリースサイクルの自動化 (32%) にオブザーバビリティを活用している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

教育業界の回答者は、クラウドリソースの使用と支出の最適化 (63%) と DX の取り組みの支援 (47%) にオブザーバビリティを活用しているとの回答がもっとも多い傾向にありました。エネルギー／ユーティリティ業界の回答者は、コストカットの取り組みの支援 (40%)、新製品／サービスの市場投入の迅速化 (40%)、中核的なレガシーアプリケーションのクラウド移行のリスク最小化 (38%)、直近の M&A 実施によりオブザーバビリティが拡大 (36%)、コンテナ化とサーバーレス環境の管理 (34%、サービス／コンサルティング業界と同様) にオブザーバビリティを活用しているとの回答がもっとも多い傾向にありました。政府機関の回答者は、分散化システムのトラブルシューティングへの活用がもっとも多い傾向にありました (50%)。工業／原料／製造業界の回答者は、DevOps への組織的な IT 移行の支援への活用がもっとも多い傾向にありました (35%)。サービス／コンサルティング業界の回答者は、ソフトウェアのリリースサイクルの自動化への活用がもっとも多い傾向にありました (40%)。

# インシデント対応

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オブザーバビリティをよく利用します。

- ↓ **ダウンタイムの短縮**
- ↓ **レイテンシの短縮**
- ↑ **効率の向上**

稼働停止の頻度、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。調査の結果から、フルスタックオブザーバビリティを実践している組織では、オブザーバビリティによりサービスレベルのメトリクスが改善され、オブザーバビリティを優先／実現している組織では稼働停止の頻度が減少し、MTTD と MTTR が短縮されることがわかりました。


**図 28.** オブザーバビリティを優先／実現すると、稼働停止の頻度は減少し、MTTD と MTTR は短縮される

## 稼働停止の頻度

では、顧客とエンドユーザーに影響する稼働停止は、どの程度頻繁に発生しているのでしょうか？調査結果は以下の通りです。

- 稼働停止が頻繁に発生（52～72%が週に1回以上と回答）
- ビジネスインパクトの少ない稼働停止がもっとも頻発（72%が週に1回以上と回答）
- ビジネスインパクトが大きい稼働停止の発生はもっとも少ない（月に2～3回以下）ものの、それでも半数以上（52%）が週に1回以上の発生を経験

| | 稼働停止の頻度がもっとも高い（週に1回以上） | 稼働停止の頻度がもっとも低い（月に2～3回以下） |
|---|---|---|
| ビジネスインパクトが大きい | 51.9% | 45.8% |
| ビジネスインパクトが中程度 | 62.9% | 35.3% |
| ビジネスインパクトが小さい | 71.6% | 26.8% |

表 04. ビジネスインパクトの程度（大・中・小）別に見た稼働停止の頻度の比較

稼働停止の相対的頻度を考えると、手動の作業やインシデントチケットがどの程度これらの稼働停止の検知ソースであるかについての考察は注目に値します。

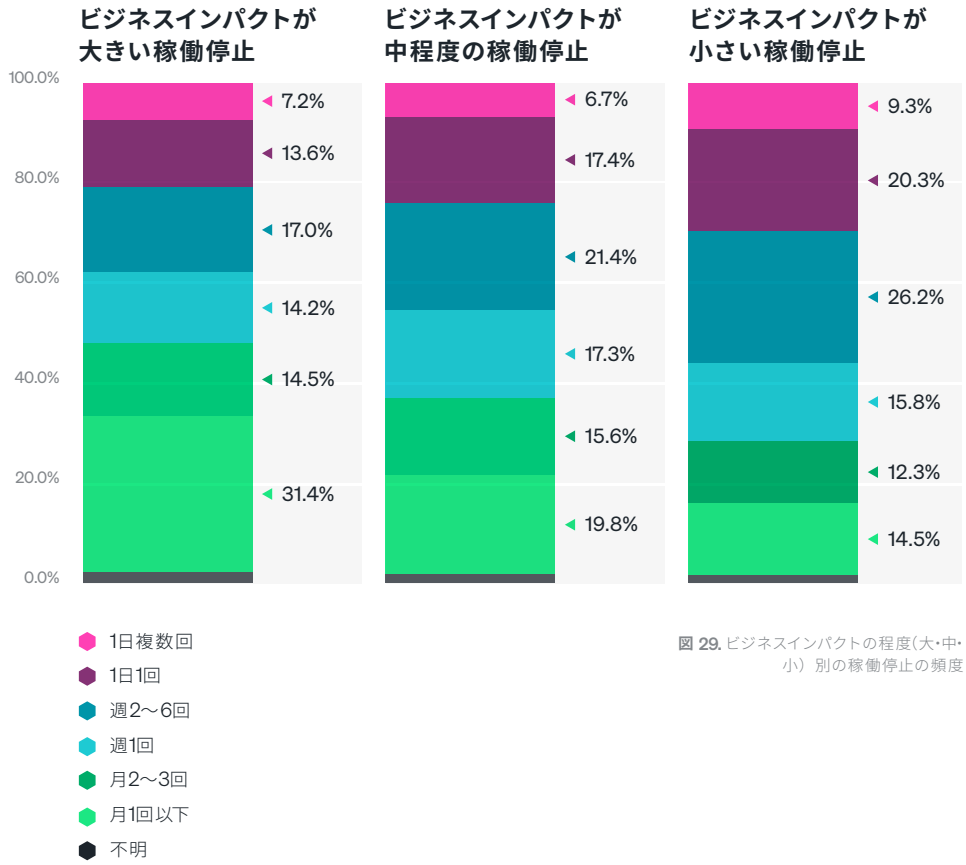



図 29. ビジネスインパクトの程度（大・中・小）別の稼働停止の頻度

### 地域別の考察

北米の回答者は、自社組織の稼働停止の頻度は低い（月に2～3回以下）と回答し、いっぽうでヨーロッパの回答者はより頻度が高い（週に1回以上）と回答する傾向にありました。

### ロール別の考察

エグゼクティブは、自社組織の稼働停止の頻度は低い（月に2～3回以下）と回答し、いっぽうで実務担当者はより頻度が高い（週に1回以上）と回答する傾向にありました。

### 組織規模別の考察

小規模組織では、ビジネスインパクトが低い稼働停止は週1回以上、ビジネスインパクトが中程度および大きい稼働停止の発生は月に2～3回以下の傾向にありました。中規模および大規模組織では、稼働停止は週1回以上発生する傾向にありました。

**52%**

で、ビジネスインパクトの大きい稼働停止が週1回以上発生

フルスタックオブザーバビリティの実現と稼働停止の頻度の低さには、明確な関連性が見られます。フルスタックオブザーバビリティを実現している組織（本レポートでの定義による）の回答者は、稼働停止の頻度がもっとも低い（月に 2 ～ 3 回以下）との回答が多く、稼働停止の頻度がもっとも高い（週 1 回以上）との回答が少ない傾向にありました。

| | 稼働停止の頻度がもっとも高い（週 1 回以上） | | 稼働停止の頻度がもっとも低い（月に 2 ～ 3 回以下） | |
|---|---|---|---|---|
| | フルスタックオブザーバビリティを実践している | フルスタックオブザーバビリティがない | フルスタックオブザーバビリティを実践している | フルスタックオブザーバビリティがない |
| ビジネスインパクトが大きい | **41.3%** | 55.9% | **56.4%** | 41.9% |
| ビジネスインパクトが中程度 | **51.2%** | 67.3% | **46.4%** | 31.2% |
| ビジネスインパクトが小さい | **59.6%** | 76.1% | **38.2%** | 22.5% |

**表 05.** ビジネスインパクトの程度（大・中・小）別に見た稼働停止の頻度の比較と、フルスタックオブザーバビリティの有無

すでにフルスタックオブザーバビリティを優先／実現していると答えた回答者は、稼働停止の頻度がもっとも低い（月に 2 ～ 3 回以下）との回答が多く、また稼働停止の頻度がもっとも高い（週 1 回以上）との回答が少ない傾向にありました。

このデータは、フルスタックオブザーバビリティと稼働停止の頻度の少なさとの強い関連性を裏付けるものです。

| | 稼働停止の頻度がもっとも高い（週 1 回以上） | | 稼働停止の頻度がもっとも低い（月に 2 ～ 3 回以下） | |
|---|---|---|---|---|
| | フルスタックオブザーバビリティを優先／実現している | フルスタックオブザーバビリティを優先／実現していない | フルスタックオブザーバビリティを優先／実現している | フルスタックオブザーバビリティを優先／実現していない |
| ビジネスインパクトが大きい | **34.1%** | 52.4% | **65.9%** | 45.3% |
| ビジネスインパクトが中程度 | **36.4%** | 63.6% | **63.6%** | 34.5% |
| ビジネスインパクトが小さい | **34.1%** | 72.7% | **63.6%** | 25.7% |

**表 06.** ビジネスインパクトの程度（大・中・小）別に見た稼働停止の頻度の比較と、フルスタックオブザーバビリティの優先／実現の有無

## MTTD

稼働停止の平均検知時間と、セキュリティ、IT インシデント管理に使用される一般的なサービスレベルでのメトリクスについて、調査結果により以下のことが示されました。

- 大多数が、5 分超だが 60 分未満の MTTD を経験
- 一般に、ビジネスインパクトが大きい稼働停止のほうが、インパクトが小さい停止より検知に時間がかかる
- 5 分の 1 以上（22%）が、ビジネスインパクトの大きい稼働停止の検知に 1 時間以上かかっている

| | 最速の MTTD（30 分未満） | 最遅の MTTD（30 分超） |
|---|---|---|
| **ビジネスインパクトが大きい稼働停止** | 44.5% | 53.1% |
| **ビジネスインパクトが中程度の稼働停止** | 49.1% | 49.1% |
| **ビジネスインパクトが小さい稼働停止** | 58.6% | 39.5% |

**表 07.** ビジネスインパクトの程度（大・中・小）別に見た最速の MTTD と最遅の MTTD の比較

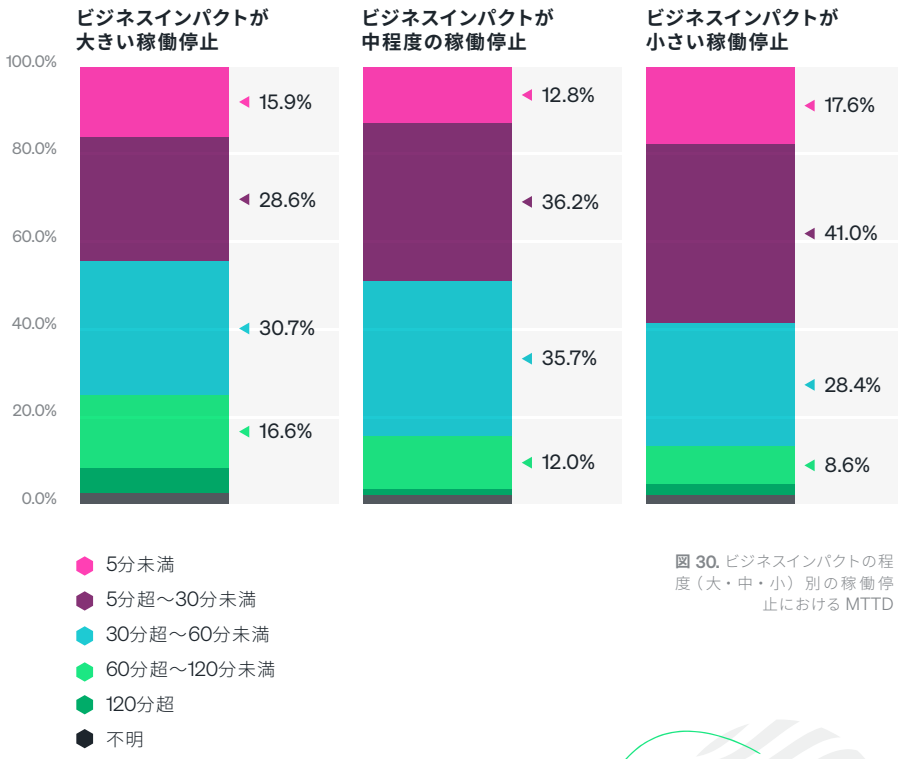



**図 30.** ビジネスインパクトの程度（大・中・小）別の稼働停止における MTTD

### 地域別の考察

ビジネスインパクトが大きい稼働停止に関し、ヨーロッパの回答者は、60 分を超える MTTD が最も少ない傾向にありました（19%、対してアジア太平洋の回答者は 26%、北米の回答者は 24%）。ビジネスインパクトが中程度の稼働停止に関し、アジア太平洋の組織ではより速い MTTD が多く（55%）、北米の組織では最も少ない傾向にありました（53%）。ビジネスインパクトが小さい稼働停止に関し、北米の組織ではより速い MTTD が多く（62%）、ヨーロッパの組織では最も少ない傾向にありました（57%）。

### ロール別の考察

ビジネスインパクトが小さい稼働停止に関し、エグゼクティブと実務担当者は、非エグゼクティブマネージャーに比べて MTTD の速さについてより楽観的でした。ビジネスインパクトが大きい稼働停止に関し、ITDM は実務担当者より楽観的な傾向が見られました。

### 組織規模別の考察

小規模組織では、ビジネスインパクトが大きい稼働停止の 30 分以内での検知が最も多い傾向にありました（48%、対して中規模で 44%、大規模で 45%）。

**22%**

が、ビジネスインパクトが大きい稼働停止の検知に 1 時間超費やしている。

その他の興味深い結果は、フルスタックオブザーバビリティを実現している組織（本レポートでの定義による）の回答者と、すでにフルスタックオブザーバビリティを優先／実現していると答えた回答者も、最速の MTTD（5 分未満）を経験している傾向にあったということです。

| | 最速の MTTD（5 分未満） | | | |
|---|---|---|---|---|
| | フルスタックオブザーバビリティを実践 | フルスタックオブザーバビリティがない | フルスタックオブザーバビリティを優先／実現している | フルスタックオブザーバビリティを優先／実現していない |
| ビジネスインパクトが大きい稼働停止 | **20.1%** | 14.3% | **25.0%** | 15.6% |
| ビジネスインパクトが中程度の稼働停止 | **16.9%** | 11.3% | **31.8%** | 12.3% |
| ビジネスインパクトが小さい稼働停止 | **24.2%** | 15.1% | **34.1%** | 17.1% |

**表 08.** ビジネスインパクトの程度（大・中・小）別の稼働停止に関する、フルスタックオブザーバビリティの有無およびフルスタックオブザーバビリティを優先／実現しているかどうかによる最速の MTTD

すでにフルスタックオブザーバビリティを優先／実現していると答えた回答者は、MTTD が最速（30 分未満）であることが多く、MTTD が最遅（30 分超）であることは少ない傾向にありました。

このデータは、フルスタックオブザーバビリティと MTTD 短縮との強い関連性を示しています。

| | 最速の MTTD（30 分未満） | | 最遅の MTTD（30 分超） | |
|---|---|---|---|---|
| | フルスタックオブザーバビリティを優先／実現している | フルスタックオブザーバビリティを優先／実現していない | フルスタックオブザーバビリティを優先／実現している | フルスタックオブザーバビリティを優先／実現していない |
| ビジネスインパクトが大きい稼働停止 | **68.2%** | 43.8% | **31.8%** | 53.7% |
| ビジネスインパクトが中程度の稼働停止 | **65.9%** | 48.6% | **34.1%** | 49.5% |
| ビジネスインパクトが小さい稼働停止 | **65.9%** | 58.4% | **31.8%** | 39.7% |

**表 09.** ビジネスインパクトの程度（大・中・小）別の稼働停止別の、フルスタックオブザーバビリティの有無およびフルスタックオブザーバビリティを優先／実現しているかどうかによる最速の MTTD と最遅の MTTD の比較

## MTTR

セキュリティおよび IT インシデント管理におけるもう 1 つの一般的なサービスレベルのメトリクスである MTTR についても、同様の傾向が見られます。

- 大多数が、5 分超だが 60 分未満の MTTR を経験
- 一般に、ビジネスインパクトが大きい／中程度の稼働停止のほうが、インパクトの小さい停止より解決に時間がかかる
- 3 分の 1 近く（29%）が、ビジネスインパクトの大きい稼働停止の解決に 1 時間超かかっている

| | 最速の MTTR（30 分未満） | 最遅の MTTR（30 分超） |
|---|---|---|
| **ビジネスインパクトが大きい稼働停止** | 38.2% | 59.7% |
| **ビジネスインパクトが中程度の稼働停止** | 43.6% | 54.6% |
| **ビジネスインパクトが小さい稼働停止** | 54.0% | 44.2% |

**表 10.** ビジネスインパクトの程度（大・中・小）別に見た最速の MTTR と最遅の MTTR の比較

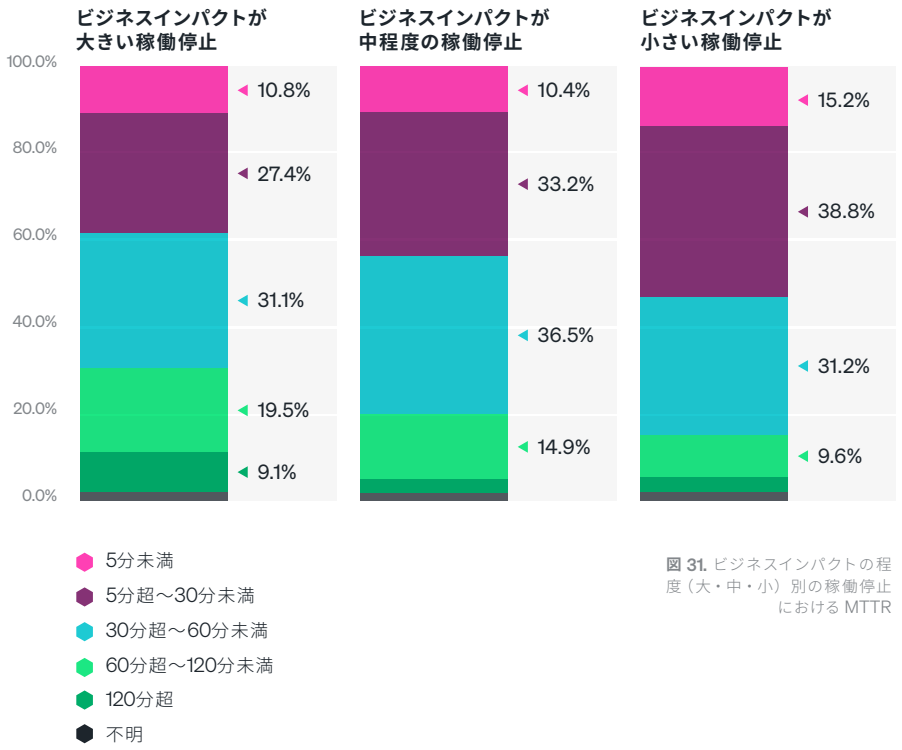



**図 31.** ビジネスインパクトの程度（大・中・小）別の稼働停止における MTTR

### 地域別の考察

ビジネスインパクトが大きい／中程度の稼働停止に関し、ヨーロッパの回答者は、MTTR が 5 分未満であることが MTTR が 1 時間超であることが少ない傾向にありました。

### ロール別の考察

ビジネスインパクトが大きい／中程度の稼働停止に関し、非エグゼクティブマネージャーは、エグゼクティブや実務担当者に比べて MTTR が 1 時間超との回答が多い傾向にありました。ビジネスインパクトが小さい稼働停止に関し、エグゼクティブと実務担当者は、非エグゼクティブマネージャーよりも MTTR の時間について楽観的である傾向にありました。

### 組織規模別の考察

大規模組織では、ビジネスインパクトが大きい／中程度の稼働停止の検知に 1 時間以上かかることがもっとも多い傾向にありました。

**29%**

が、ビジネスインパクトが大きい稼働停止の解決に 1 時間以上かかっている

フルスタックオブザーバビリティを実現している組織（本レポートでの定義による）の回答者と、すでに優先／実現していると答えた回答者も、最速の MTTR（5 分未満）を経験している傾向にありました。

| | 最速の MTTR（5 分未満） | | | |
|---|---|---|---|---|
| | フルスタックオブザーバビリティ実装済み | フルスタックオブザーバビリティがない | フルスタックオブザーバビリティを優先／実現している | フルスタックオブザーバビリティを優先／実現していない |
| ビジネスインパクトが大きい稼働停止 | **13.0%** | 9.9% | **25.0%** | 10.4% |
| ビジネスインパクトが中程度の稼働停止 | **10.7%** | 10.3% | **22.7%** | 10.1% |
| ビジネスインパクトが小さい稼働停止 | **18.7%** | 13.9% | **34.1%** | 14.7% |

**表 11.** ビジネスインパクトの程度（大・中・小）別の稼働停止に関する、フルスタックオブザーバビリティの有無および優先／実現しているかどうかによる最速の MTTR

すでにフルスタックオブザーバビリティを優先／実現していると答えた回答者も、MTTR が最速（30 分未満）であることが多く、一方で優先／実現していない回答者は MTTR が最遅（30 分超）でした。

このデータは、フルスタックオブザーバビリティと MTTR の短縮との強い関連性を示しています。明らかに、フルスタックオブザーバビリティと稼働停止頻度の少なさ、MTTD、MTTR の最良のパフォーマンス指標には関連性が見られます。

MTTR の短縮についての方針はこちら。

| | 最速の MTTR（30 分未満） | | 最遅の MTTR（30 分超） | |
|---|---|---|---|---|
| | フルスタックオブザーバビリティを優先／実現している | フルスタックオブザーバビリティを優先／実現していない | フルスタックオブザーバビリティを優先／実現している | フルスタックオブザーバビリティを優先／実現していない |
| ビジネスインパクトが大きい稼働停止 | **61.4%** | 37.5% | **38.6%** | 60.3% |
| ビジネスインパクトが中程度の稼働停止 | **59.1%** | 43.2% | **40.9%** | 55.0% |
| ビジネスインパクトが小さい稼働停止 | **65.9%** | 53.6% | **29.6%** | 44.6% |

**表 12.** ビジネスインパクトの程度（大・中・小）別の稼働停止に関する、フルスタックオブザーバビリティを優先／実現しているかどうかによる最速の MTTR と最遅の MTTR の比較

## 性能別の MTTD ／ MTTR の予測要因

加えて、データから、特定の性能（AIOps、ディストリビューティッド（分散）トレーシング、セキュリティ監視、カスタムダッシュボード、外形監視、APM、データベース監視、アラート、インフラストラクチャ監視）と MTTD ／ MTTR の短縮（30 分未満）には、明らかな関連性があることが予測されます。これらの性能のうち、AIOps **は有意水準** 10% **の範囲で統計的に有意です。**

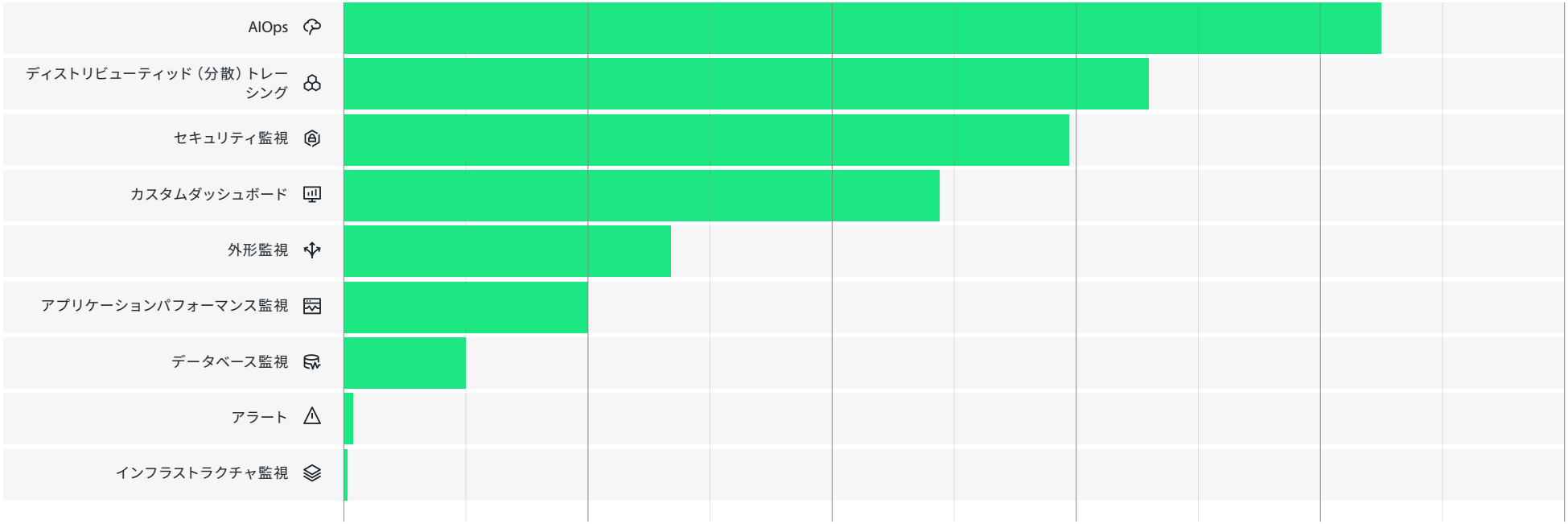



図 32. 30 分未満の MTTD/MTTR が予測される性能

# 開発者とエンジニアの日々の業務

オブザーバビリティは、開発者とエンジニアにとってどのような点でもっとも役立つかを、実務担当者自身と ITDM に尋ねました。結果は以下の通りです。

- 少なくとも 30% が、生産性を向上させ、チーム間の連携を可能にし、複雑で分散した技術スタックの管理において推測に基づいた作業を減らすと回答
- 約 10 分の 3 が、開発者とエンジニアの日々の業務が楽になり、ワークライフバランスが改善され、スキルセットと雇用可能性が高まると回答
- およそ 4 分の 1 が、推測を裏付け／反証し、私見を打破し、情報の不足を補うのに役立つと回答

これらの結果は、開発者とエンジニアが労力を削減し、チーム間の連携を高め、生産的な業務に時間を使えるようになるための解決策を求めていることを示しています。エンジニアリングへのデータドリブンなアプローチと、オールインワンのオブザーバビリティプラットフォームにより、開発者とエンジニアの生活は、以下を通じて、よりよい快適なものになります。

- コンテナ、マルチクラウド、複数ツールなどの複雑で分散した技術スタックの管理において、推測に基づいた作業が減る
- 何が起こったかだけでなく、なぜそのインシデントが発生したのかの理解において、雑音を減らしより多くの有意なデータを得る
- 不具合をより迅速に解消し、より生産性が高くビジネスインパクトのある、彼らの望む創造的なコード作業のための時間を確保する

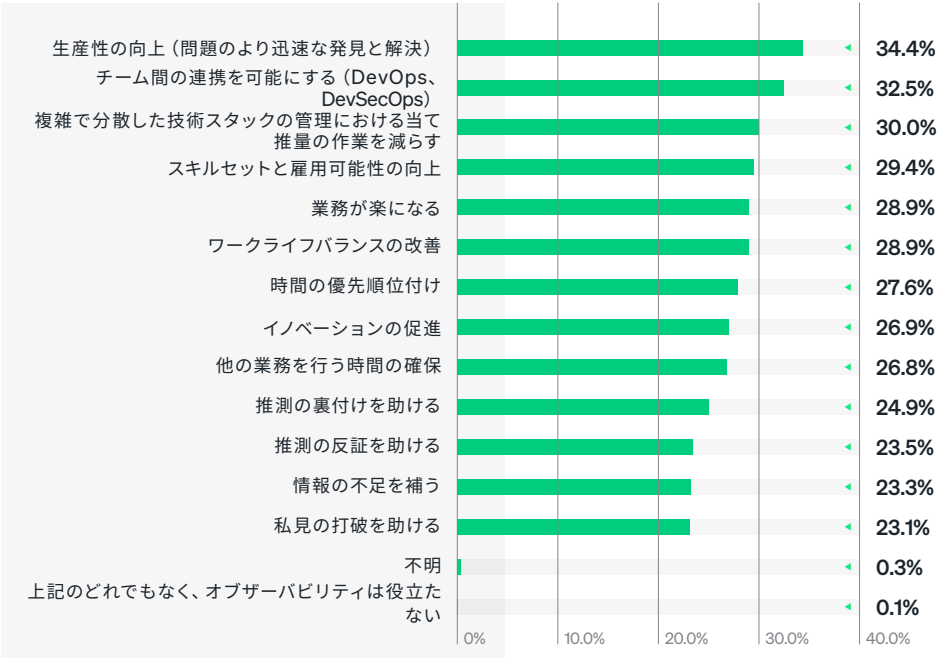



図 33. オブザーバビリティはどのような点で開発者とエンジニアの生活向上にもっとも役立つか

### 地域別の考察

アジア太平洋の回答者では、生産性の向上との回答がもっとも多い傾向にありました（41%、対してヨーロッパでは 30%、北米では 35%）。ヨーロッパの回答者では、開発者／エンジニアの日々の業務が楽になるとの回答がトップでした（31%）。一方、北米の回答者では、イノベーションの促進（32%、対してアジア太平洋では 24%、北米では 25%）、他の業務を行う時間の確保（30%、対してアジア太平洋では 27%、ヨーロッパでは 24%）との回答がもっとも多い傾向にありました。

### 役割別の考察

エグゼクティブでは、オブザーバビリティは実務担当者のワークライフバランスを改善させる（32%）との回答が実務担当者自身（28%）より多い傾向にありました。一方、非エグゼクティブマネージャーは、実務担当者が他の業務を行う時間を確保できる（34%）との回答がもっとも多く、彼らの業務を楽にする（22%）、イノベーションを促進する（23%）、チーム間の連携を可能にする（26%）との回答はもっとも少ない傾向にありました。

### 業界別の考察

教育業界の回答者は、オブザーバビリティは推測に基づいた作業を減らす（43%）、業務を楽にする（40%）、推測を裏付ける（37%）、スキルセットと雇用可能性を高める（37%）との回答が、他のほとんどの業界より多い傾向にありました。エネルギー／ユーティリティ業界の回答者も、推測に基づいた作業を減らす、ワークライフバランスが改善される（いずれも 42%）との回答が多い傾向にありました。政府機関の回答者でも、推測に基づいた作業を減らす（42%）との回答が上位でした。また、サービス／コンサルティング業界の回答者は、スキルセットと雇用可能性を高める（36%）、時間の優先順位付けが可能になる（38%）、チーム間の連携を可能にする（43%）との回答が他業界より多くなりました。

**29%**

が、オブザーバビリティは開発者／エンジニアの業務を楽にし、ワークライフバランスを改善し、スキルセットと雇用可能性を高めると回答

# フルスタックオブザーバビリティを阻む課題

では、フルスタックオブザーバビリティがそれほど多くの利点をもたらすのであれば、組織がそれを優先／実現させるのを阻むものは何でしょうか？結果は以下の通りです。

- 利点の理解不足と、既存の IT パフォーマンスで十分であるという心理が、もっとも多く指摘された要因（いずれも 28%）
- 4 分の 1 以上の回答者（27%）が、予算がないことに言及
- 4 分の 1 が、監視ツールが多すぎると回答
- ほぼ 4 分の 1 が、販売サイクルの長さ、インストゥルメントされていないシステム、戦略の欠如、多種からなる技術スタックに苦労
- 5 分の 1 近く（19%）が、スキルの欠如と回答

加えて、自社 IT パフォーマンスは十分である（現状のパフォーマンスの改善は必要ない）と回答したうちの 51% が、予算の 20% 超をオブザーバビリティツールへ配分していると答えました。

まとめると、この結果は、フルスタックオブザーバビリティを追求する上で、複数の異なる障壁と問題があることを示しています。フルスタックオブザーバビリティを実現するには、技術プロフェッショナルがその利点についてより明確な理由付けを示し、特に大規模組織においては、その理由付けを明確なビジネス戦略へと組み込む必要があります。

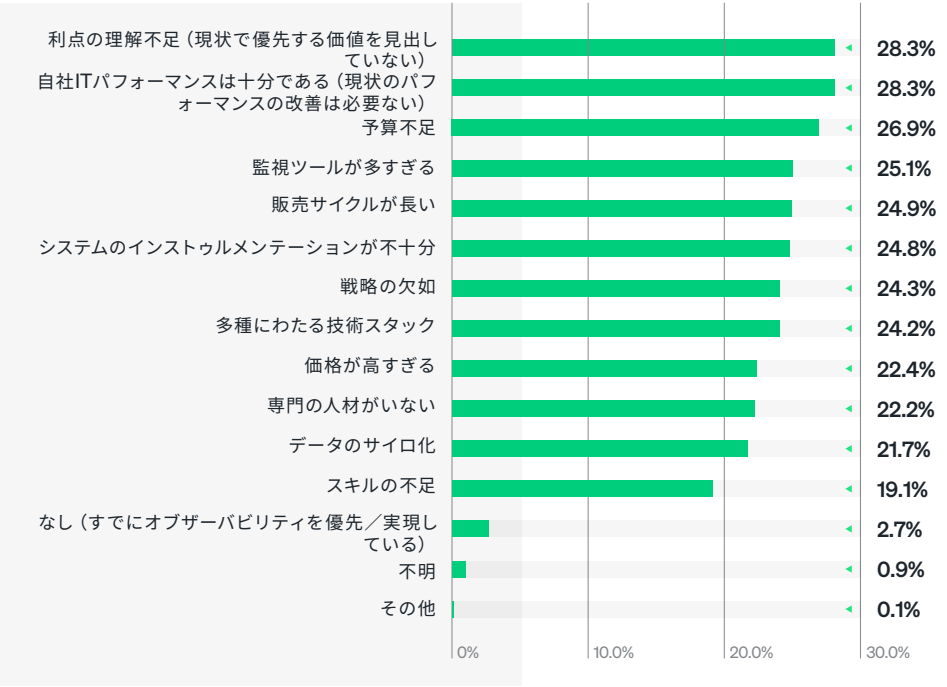



**図 34.** フルスタックオブザーバビリティの優先／実現を阻む主な課題

### 地域別の考察

55% が単一の連結プラットフォームを望ましいとするアジア太平洋地域では、もっとも大きな障壁は、彼らのシステムのインストゥルメンテーションが不十分なこと、また監視ツールが多すぎること（いずれも 28%）となりました。一方ヨーロッパの回答者は、予算不足（29%）との回答が若干多く、戦略の欠如（21%）、自社システムのインストゥルメンテーションが不十分なこと（22%）との回答は少ない傾向にありました。北米の回答者は、利点の理解不足（32%）と十分な IT パフォーマンス（31%）との回答が多い傾向にありました。

### 役割別の考察

多くの実務担当者とエグゼクティブは、フルスタックオブザーバビリティのメリットを十分に理解できていないことが、導入の主な課題であると感じていました（29%）が、非エグゼクティブマネージャーは、既存の自社 IT パフォーマンスは十分である（31%）と考える傾向にありました。実務担当者は、自社 IT パフォーマンスは十分である（26%）、スキルの欠如（17%）との回答はもっとも少なく、多種からなる技術スタック（26%）、データのサイロ化（23%）との回答が多い傾向にありました。

### 組織規模別の考察

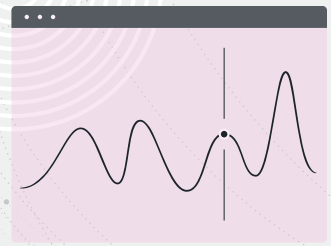
小規模組織は、最大の課題として、価格が高すぎること（33%）、次いで予算不足（29%）を挙げました。中規模組織は、利点の理解不足（30%）にもっとも苦労していました。大規模組織は、自社 IT パフォーマンスは十分である（32%）との回答がもっとも多く、一方で従業員 5,000 名以上の大規模組織では、戦略の欠如（34%）との回答がもっとも多い傾向にありました。

**3%**

が、すでにフルスタックオブザーバビリティを優先／実現していると回答

# オブザーバビリティの未来

## 組織はオブザーバビリティのビジネス価値を見据え、さらなる投資を予想しています。



# MTTR の短縮

調査対象者に、MTTR の短縮にもっとも貢献する要因は何かを尋ねました。これは、44 ～ 60% が稼働停止の解決に 30 分以上かかっていることを考えると、非常に重要な質問です。全体として、上位の回答は以下の通りでした。

1. よりよい DevOps の実践（39%）
2. 自動化されたインシデント対応のワークフロー（38%）
3. オブザーバビリティツールに関するスタッフのトレーニング（36%）

フルスタックオブザーバビリティを既に実装している回答者は、MTTR 短縮には自動化されたインシデント対応のワークフローが必要に対するの回答（42%）が、フルスタックオブザーバビリティを実装していない回答者（36%）に比べて顕著でした。

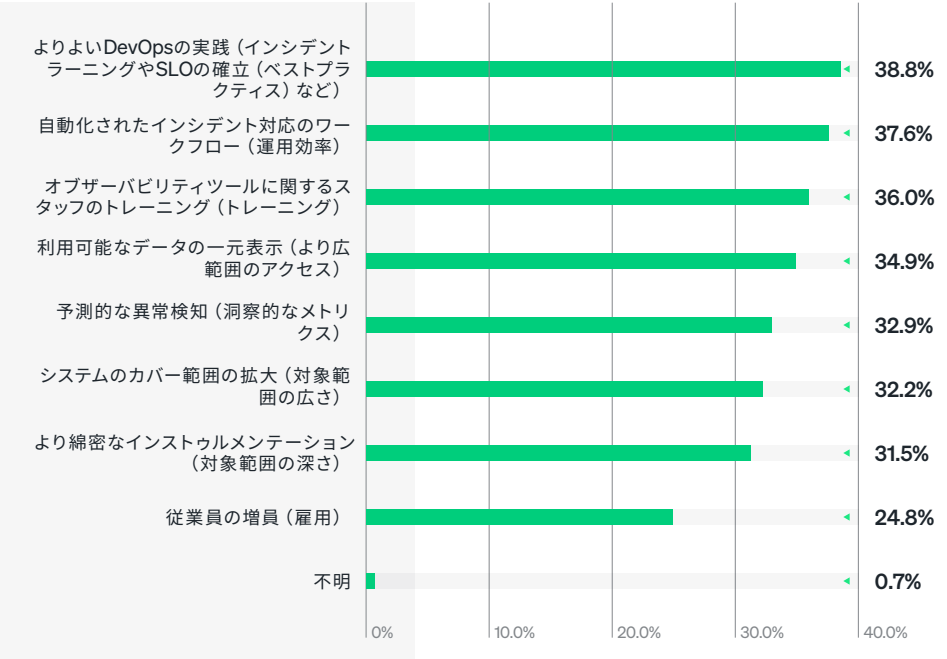



**図 35.** 稼働停止の MTTR を短縮する最大の貢献要因

### 地域別の考察

アジア太平洋やヨーロッパの回答者と異なり、北米の回答者は、MTTR 短縮の方法としてオブザーバビリティツールに関するスタッフのトレーニングとの回答がもっとも多く（40%）、よりよい DevOps の実践との回答は第 4 位でした。一方、アジア太平洋の回答者は、よりよい DevOps の実践との回答がもっとも多い傾向にありました（42%）。

### ロール別の考察

実務担当者では、オブザーバビリティツールに関するスタッフのトレーニングとの回答がもっとも多くなりました（37%）。エグゼクティブでは、スタッフの補充との回答がもっとも少なくなりました（22%）。また、非エグゼクティブマネージャーでは、利用可能なデータの一元表示（32%）、予測的な異常検知（30%）との回答がもっとも少なくなりました。

### 組織規模別の考察

小規模組織の回答者では、オブザーバビリティツールに関するスタッフのトレーニング（40%）、より綿密なインストゥルメンテーション（36%）、予測的な異常検知（35%）が上位の回答になりました。一方、中規模および大規模組織での上位回答は、全体結果と同様でした。

### 業界別の考察

スタッフの補充がトップの回答だったのは、政府機関および医療／製薬業界のみでした。教育、エネルギー／ユーティリティ、金融／保険、小売／消費者業界では、いずれも自動化されたインシデント対応のワークフローがトップの回答となりました。NPO ／不特定、サービス／コンサルティング業界では、オブザーバビリティツールに関するスタッフのトレーニングがトップでした。一方、工業／原料／製造 JT ／テレコミュニケーション業界では、よりよい DevOps の実践がトップでした。

# デプロイメント計画

先を見据える企業のリーダーたちは、ビジネスの必須事項としてオブザーバビリティを実施しています。回答者が、来年と今後 3 年間でどれほど積極的に多くの性能をデプロイする予定かについては、興味深いものがあります。

## 来年

来年は、さらなるオブザーバビリティ性能をデプロイするための重要な年になるでしょう。2023 年の終わりまでに、回答者は 72 ～ 86% の性能がデプロイされると予想しています。

- ほぼ 3 分の 1（32%）が、1 ～ 5 の新規性能をデプロイする予定
- 半数以上（56%）が、6 ～ 10 の新規性能をデプロイする予定
- 11 ～ 14 の新規性能をデプロイする予定なのは 5% のみ
- 新規性能をデプロイする予定がないのはわずか 8%

注目すべきは、来年には 40% 以上が ML モデルパフォーマンス監視と AIOps をデプロイする予定であることです。

1 年後を見ると、ネットワーク監視、セキュリティ監視、ログ管理、データベース監視、アラート、インフラストラクチャ監視などの性能のデプロイメントは、80% 台半ばになります。

たとえ来年にデプロイが予定されている傾向が少ない性能であっても（Kubernetes 監視、外形監視、ディストリビューティッド（分散）トレーシングなど）、70% 台半ばという数字になります。

## 今後 3 年間

2025 年へと目を向けると、ほぼすべての回答者が、ネットワーク監視、セキュリティ監視、ログ管理その他のオブザーバビリティ性能のデプロイを予定していました。

回答者の多くが、2025 年までにほとんどの性能（88 ～ 97%）を得るつもりであると回答しています。今後 2 ～ 3 年の見込みは以下の通りです。

- 多く（60%）が 1 ～ 5 の新規性能をデプロイする予定
- 6 つ以上の新規性能のデプロイを予定しているのは 8% のみ
- 約 3 分の 1（32%）が、新規性能のデプロイを予定していない（おそらくすでにデプロイ済みとなるため）
- ある回答者は、17 すべての性能をデプロイ予定と回答

Kubernetes 監視など、もっともデプロイされていることが少ない性能であっても、圧倒的な 88% もの回答者がすでにデプロイ済み、または今後 3 年間でデプロイ予定と回答しています。

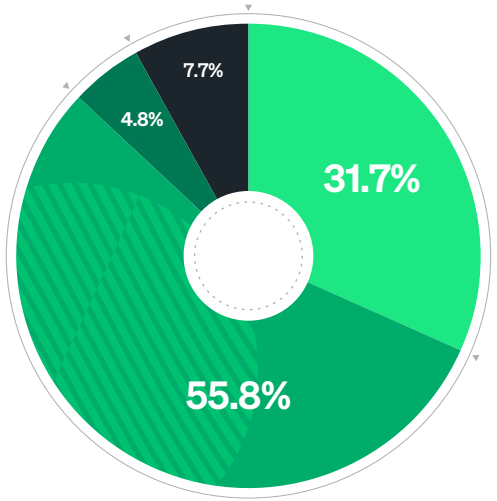



図 36. 来年度にデプロイメントが予定される性能

**88 ～ 97%**
の 17 のオブザーバビリティ性能が、2025 年までにデプロイ予定

# 性能のデプロイメントのまとめ

2025 年までに、17 のオブザーバビリティ性能のうち 88 ～ 97% がデプロイされる見込みです。これらのオブザーバビリティ性能のデプロイを予定していない回答者はわずかでした（2 ～ 7%）。

- 未デプロイ、追加予定なし（%）
- デプロイ済み（%）
- 2023年までにデプロイ予定（%）
- 2025年までにデプロイ予定（%）

多数のオブザーバビリティ性能をデプロイするというこの意向の表明は、本調査においてもっとも驚くべき結果の 1 つでした。これは、多くの組織が、2025 年までに堅牢なオブザーバビリティの実践を実施するようになる可能性を示唆しています。この結果は、オブザーバビリティの現状と、近い将来の成長の可能性を浮き彫りにするものです。

**「リモートワークでは、さらなる監視と自動アラートの必要性があります。すべての側面を完全に監視し、すばやくアラートするツールが必要です。この割合はどんどん高くなっていくと思います。90% が監視されているという状態に行き着くのも、時間の問題ではないでしょうか。」**

シニアエンジニア、金融企業

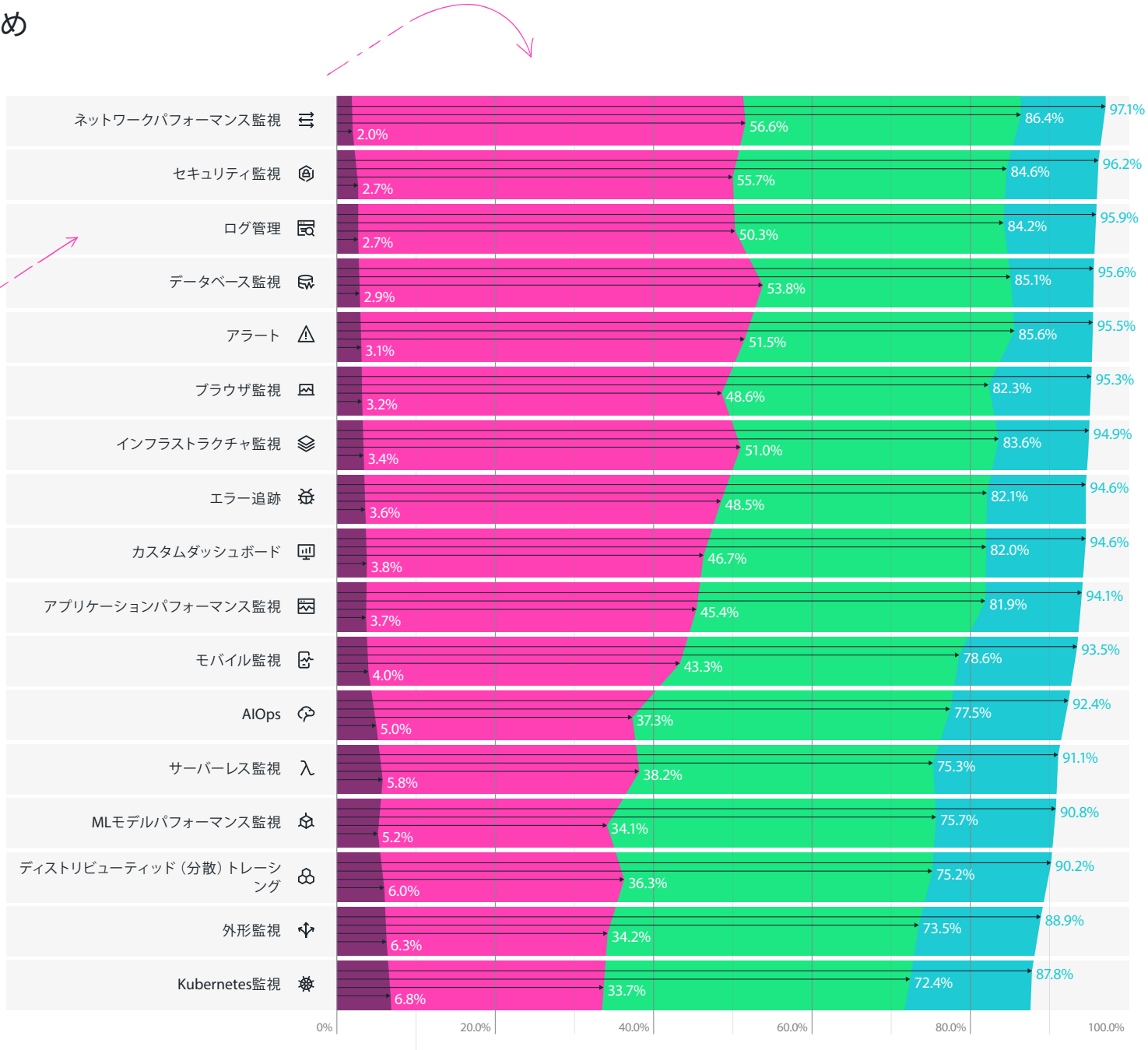



図 37. 2022 年から 2025 年にかけての性能のデプロイメント概要

# 予算計画

では、調査対象者の予算計画は、先に述べた積極的なオブザーバビリティ性能のデプロイメント計画とどのように一致しているのでしょうか？調査対象者に、来年度のオブザーバビリティ予算計画について尋ねました。結果は以下の通りです。

- 半数以上（52%）が、オブザーバビリティ予算の増額を予定（38% がある程度、14% が大幅にまたは広範囲に）
- 5 分の 1 が、オブザーバビリティ予算の現状維持を予定（増減 5% 以内）
- 27% のみが、オブザーバビリティ予算の削減を予定（12% がある程度、15% が大幅にまたは広範囲に）

驚くべきことに、来年、デプロイ予定の機能数がもっとも少ない（0 ～ 3）と答えた回答者が、オブザーバビリティ予算を増額または維持するとの回答がもっとも多い傾向にありました（80% 台）。一方、デプロイ予定の性能が多い（4 ～ 14）回答者は、その多くが、オブザーバビリティ予算を削減すると回答しました。これは、何をデプロイするかの意思決定者の意向が予算決定者の意向と一致していないか、意思決定者が各性能に対する追加料金を設定しないオブザーバビリティベンダー（New Relic のように）の使用を予定している可能性を示しています。

フルスタックオブザーバビリティを実現している（本レポートでの定義による）回答者は、フルスタックオブザーバビリティを実現していない回答者（69%）に比べて、来年のオブザーバビリティ予算を増額また維持するとの回答が多い傾向にありました（79%）。

また、成熟したオブザーバビリティの実践を行っている（本レポートでの定義による）回答者も、成熟したオブザーバビリティの実践を行っていない回答者（71%）に比べて、来年のオブザーバビリティ予算を増額または維持するとの回答が多い傾向にありました（86%）。

興味深いことに、オブザーバビリティを完全にインシデントの対応／予防強化とみなす回答者も、来年のオブザーバビリティ予算を増額または維持するとの回答が多い傾向にありました（83%）。一方で、オブザーバビリティを完全に中核的な事業目標の達成要因とみなす回答者は、オブザーバビリティ予算を増額または維持するとの回答が少ない傾向にありました（70%）。

全体として、オブザーバビリティは組織にとって今後も予算の優先度が高いと言えます。

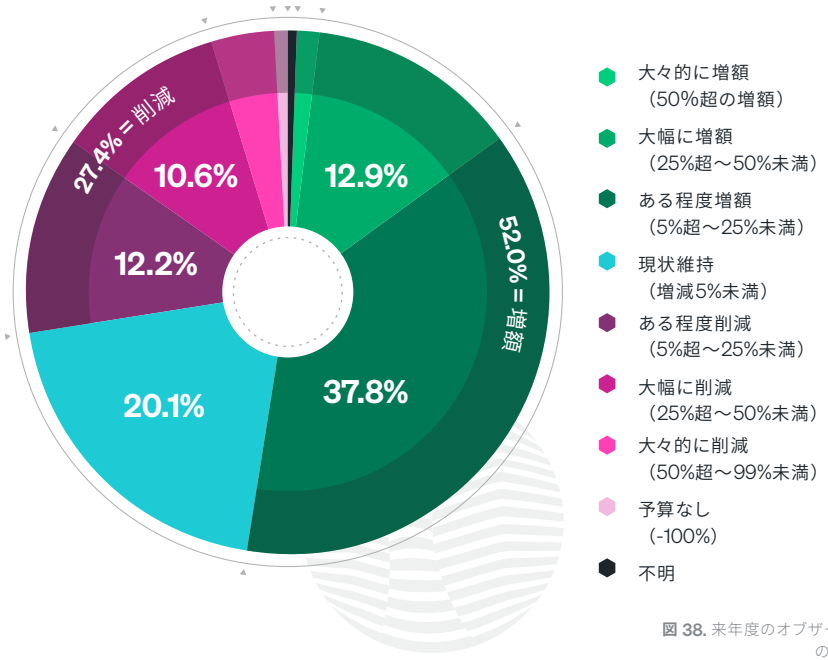



図 38. 来年度のオブザーバビリティツールの予算変更の見込み

### 地域別の考察

北米の回答者は、来年の予算を増額予定との回答が、他地域よりも多い傾向にありました（63%、対してアジア太平洋で 51%、ヨーロッパで 45%）。

### ロール別の考察

来年にかけて、57% のエグゼクティブがオブザーバビリティツールへの予算増額を予定しており、そのうち 16% は、大幅なまたは広範囲にわたる増額を見込んでいます。

### 組織規模別の考察

大規模組織の回答者は、来年のオブザーバビリティ予算を増額するとの回答が多く（57%）、中規模は削減（30%）、小規模は維持（28%）との回答が多い傾向にありました。

**72%**

が、来年のオブザーバビリティ予算を増額または維持

# 市場機会

また、今後 3 年間で、回答者が自社組織でオブザーバビリティがもっとも必要であると予測するのは、他にはどんなタイプのテクノロジーかについても調査しました。結果は以下の通りです。

- 人工知能（AI）やモノのインターネット（IoT）をはじめ、エグゼクティブが優先するロードマップに含まれるであろうより確立されたテクノロジーが、上位の回答として突出していました（40% 台）
- ビジネスアプリケーション、5G、ブロックチェーン、エッジコンピューティングなどの、第 2 波のテクノロジーや古くなりつつあるテクノロジーは、すべて 30% 台前半から中盤のポイント数になりました
- クラウドゲーミング、パーソナライゼーション技術、スーパーアプリ、Web3、メタバースなどの、新興テクノロジーや今後発展するであろうテクノロジーは、すべて 20% 台前半かそれを若干下回るポイント数でした

オブザーバビリティは、AI や 5G、ブロックチェーンなどのより新しいテクノロジーをデプロイし競争上の強みとして、より活用しやすくするため、これらの優先順位は当然のことと言えます。

これらの 11 のテクノロジーの詳細についてはこちら。

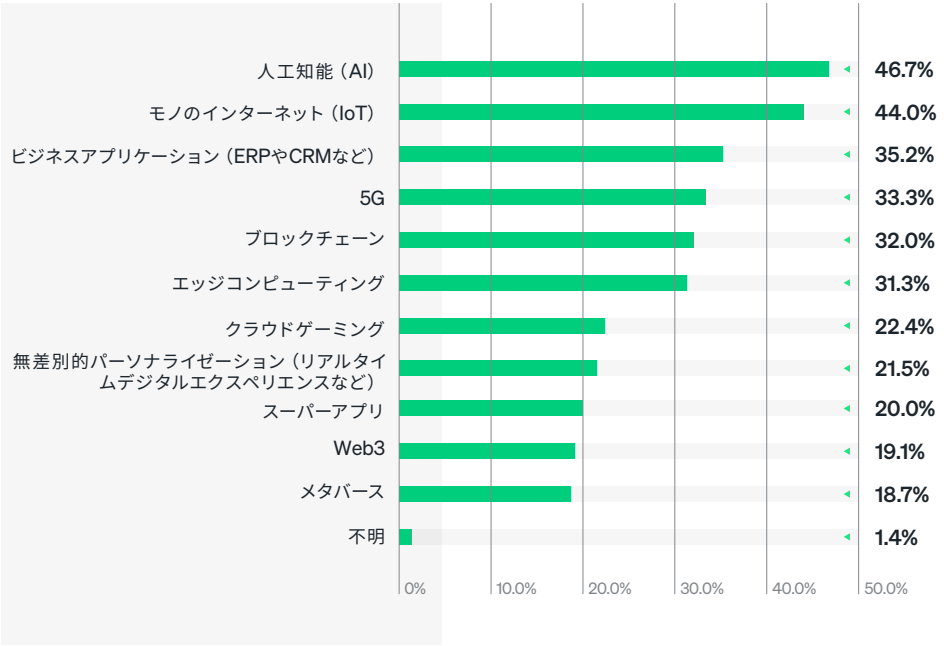



図 39. 今後 3 年間でもっともオブザーバビリティを必要とするテクノロジー

### 地域別の考察

北米の回答者は、今後 3 年間で AI 向けのオブザーバビリティの必要性を多く予測する傾向にありました（52%、対してアジア太平洋では 46%、ヨーロッパでは 43%）。アジア太平洋の回答者は、リアルタイムのデジタルエクスペリエンスなどの無差別的パーソナライゼーション技術の選択が若干多い傾向にありました（26%、対してヨーロッパでは 19%、北米では 22%）。一方、ヨーロッパの回答者はブロックチェーンの選択が少ない傾向にありました（29%、対してアジア太平洋が 35%、北米が 34%）。

### 役割別の考察

今後 3 年間で、エグゼクティブは AI 向けのオブザーバビリティ（51%、対して非エグゼクティブマネージャーは 41%、実務担当者は 46%）、エッジコンピューティング（38%、非エグゼクティブマネージャーは 31%、実務担当者は 29%）の必要性を多く予測する傾向にありました。

### 業界別の考察

IoT は、教育(51%)、エネルギー／ユーティリティ(61%)、金融／保険（42%）、医療／製薬（47%）、工業／原料／製造（43%）をはじめ、複数の業界でトップの回答でした。工業／原料／製造業界は、企業リソース計画（ERP）や顧客関係管理（CRM）などのビジネスアプリとの回答がトップだった唯一の業界でした（43%、IoT と同率）。一方、これは小売／消費者業界では第 2 位でした（40%）。

エネルギー／ユーティリティとサービス／コンサルティング業界は、エッジコンピューティングとの回答が他の業界よりも多い傾向にありました（それぞれ 42% と 45%）。エネルギー／ユーティリティ業界は、メタバースとの回答も他の業界より多い傾向にありました（31%）。一方、5G は、IT ／テレコミュニケーション業界で第 3 位でした（36%）。

# まとめと結論、要点

データ、チーム、ツールの分断が課題ではあるものの、
オブザーバビリティの利点は明白です。

# データ、ツール、チームが分断されている

今日の技術プロフェッショナルは、複雑に継ぎ合わされたデータとツールを駆使して監視を行い、技術ポートフォリオの維持、運用、保守を行っています。オブザーバビリティは現状、複数ツールであることが多く、エンジニアは複数のシステムとデータの流れのなかで多大な手動作業と調整を強いられています。多くの組織にとって、オブザーバビリティの現状は以下のような状態にあります。

- 大多数が複数ツール
- 技術スタック全体はカバーしていない
- データストリームとシステムの間で膨大な調整と複雑さが発生
- 問題の検知に手動の作業とインシデントチケットが必要
- 改善可能な稼働停止頻度および MTTD ／ MTTR パフォーマンスが存在

回答者は明らかに、より高価値なプロジェクトを追求できる自由が手に入る、簡潔な単一のツールを望んでいるようです。調査結果は、シームレスな、統合された未来への強い関心を示唆しています。

組織は、皆の業務遂行を遅らせるデータ、ツール、チームの分断に立ち向かう必要があります。このような分断化は、最適ではないカスタマーエクスペリエンス、IT コストの急増、事後対応的な手間のかかる業務でのエンジニアの時間の浪費、非効率なリソース配分、競争相手の脅威の拡大、セキュリティの脆弱化その他、ダウンストリームで多くの課題を生み出します。

私たちは、多種からなるシステムとツール、情報ソースを単一のオブザーバビリティプラットフォームに連結することで、最高のデジタルカスタマーエクスペリエンスを実現できると信じています。デジタルエクスペリエンスの一貫性と可用性、そして安全性を確保することが、成功への鍵です。

# オブザーバビリティはサービスレベルのメトリクスを改善する

フルスタックオブザーバビリティの優先／実現は、以下に寄与します。

↓ 稼働停止の頻度を低減
↑ 平均検出時間（MTTD）の短縮
↑ 平均復旧時間（MTTR）の短縮

# 組織はオブザーバビリティに投資している

多くの調査対象者がオブザーバビリティの利点の理解不足を優先／実現への主な課題として挙げているにもかかわらず、全体的な結果としては、彼らは収益に関する利点を認識しています。回答者はオブザーバビリティの実践に投資を行い、より多くの、よりよい、よりシンプルなオブザーバビリティを望んでいます。組織は、今後 3 年間で大胆なオブザーバビリティの性能強化と大幅な予算増加を予定し、近い将来のより成熟したフルスタックのオブザーバビリティの獲得を示唆しています。

すべてのエンジニアが、ソフトウェアライフサイクルの全段階でオールインワンのオブザーバビリティプラットフォームを利用できる可能性は、ますます明らかになっています。私たちは、この領域のちょうど境界線、すなわち組織が、複雑さを減らし、さまざまな方法で業務を楽にする熟慮された統合オブザーバビリティの実践に踏み出そうとしている、その転換点に立っているのです。数年のうちに、多くの組織が過去を振り返り、フルスタックオブザーバビリティ無しに一体どうやって対処していたのかと疑問に思うようになるかもしれません。

# オブザーバビリティの理想的な状態を得るためのヒント

調査結果から、オブザーバビリティの理想的な状態とは、組織が SDLC の全段階の技術スタック全体を監視でき、成熟したオブザーバビリティの実践の特性が導入され、統合されたテレメトリデータと統合されたダッシュボードまたはデータの可視化を、理想的には単一の連結プラットフォームとして実現している状態であると考えられます。では、組織はどうすれば、このオブザーバビリティの理想的な状態を得られるのでしょうか？まずは、それを阻んでいる課題に取り組むことから始めればよいのです。

| 課題 | ソリューション |
|---|---|
| **認識の低さ**<br>• 利点の理解不足（現時点で優先すべき価値を見出していない）<br>• IT パフォーマンスが十分であるとの意識（現状のパフォーマンスを向上させる必要がない） | **IT パフォーマンスの向上をはじめとするオブザーバビリティの利点と価値をユーザーに教育する。例として使用事例の提示など：**<br>• クラウドリソースの使用と支出の最適化<br>• デジタルカスタマーエクスペリエンスの競争優位性を改善、獲得するための DX の取り組みの支援<br>• コンテナ化とサーバーレス環境の管理<br>• 新製品／サービスの市場投入の迅速化<br>• DevOps への組織的な IT 移行の支援<br>• 主要なレガシーアプリケーションのクラウド移行のリスク最小化<br>• 分散化システムのトラブルシューティング |
| **ツールの分断**<br>• 監視ツールが多すぎる<br>• 多種にわたる技術スタック | **オールインワンのオブザーバビリティプラットフォームへ移行する：**<br>• 監視ツールを単一プラットフォームへ連結<br>• 利用可能なデータの一元表示を提供（アクセスのしやすさ）<br>• テレメトリデータを複数チームで活用できるよう単一ペインに統合 |
| **データの分断**<br>• システムのインストゥルメンテーションが不十分<br>• データのサイロ化 | **フルスタックオブザーバビリティを優先／実現させる：**<br>• 技術スタック全体にわたるテレメトリデータを収集<br>• システムのカバー範囲を拡大（対象範囲の広さ）<br>• より綿密なインストゥルメンテーション（対象範囲の深さ）<br>• 計装の自動化<br>• ユーザーにテレメトリデータとその可視化への幅広いアクセスを提供 |
| **組織による支援の不足**<br>• 戦略の欠如<br>• 予算不足<br>• 専門的人材の不足<br>• スキルの欠如 | **オブザーバビリティの目標への支援を計画する：**<br>• 包括的なオブザーバビリティ戦略の策定<br>• 現在と今後のオブザーバビリティのニーズにもとづく十分な予算の配分<br>• 必要に応じた追加人材の雇用<br>• スタッフに対するオブザーバビリティツールのトレーニング |
| **チームの分断**<br>• 各チームが異なるツールを使用<br>• 連携不足 | **オブザーバビリティを SDLC の全段階（シフトレフトを含む）に組み込む：**<br>• インシデントラーニングや SLO など、よりよい DevOps のベストプラクティスの確立<br>• インシデント対応のワークフローの自動化（運用効率）<br>• 予測的な異常検知の導入（洞察的なメトリクス）<br>• 可能な限りのインシデント対応の自動化<br>• 自動化ツールを使用したインフラストラクチャの設定とオーケストレーション<br>• ソフトウェアデプロイメントへの CI ／ CD の実践の活用<br>• 他チームとの連携 |
| **購買、価格、請求の懸念**<br>• 価格の高さ<br>• 販売サイクルの長さ<br>• 予測可能性の欠如 | **適正なオブザーバビリティプラットフォームとベンダーを選択する。上位 10 項目の検討項目は以下の通り：**<br>• カバーされる性能（現在と今後）<br>• 予算に見合う価格<br>• 価格の透明性<br>• 全テレメトリにわたるシングルライセンスのメトリクス<br>• 最低月額のない従量課金制の使用量を拡大できる柔軟性<br>• ペナルティなしにあらゆるテレメトリデータタイプを取り込める能力<br>• ペナルティなしにオートスケール可能な能力<br>• 予測可能な支出<br>• 従量課金制の請求<br>• 期限超過の割増料金なし |

**表 13.** オブザーバビリティの理想的な状態を得るための課題と解決策

# 期待される成果

ひとたび組織がこの理想的なオブザーバビリティの状態を獲得すれば、多くのポジティブな成果が得られることをデータは示しています。

### アップタイム、パフォーマンス、信頼性の改善

- サービスの中断とビジネスリスクの低減
- サービスレベルのメトリクスの改善
- カスタマーエクスペリエンスの向上

### 運用効率

- テレメトリデータにビジネス関連の文脈を組み込んでイベントやインシデントのビジネスインパクトを数値化
- 複雑で分散した技術スタックを管理する場合の当て推量を低減
- 生産性の向上（開発者とエンジニアが問題をより迅速に検出、解決）
- 時間の優先順位付け
- 情報不足の補填、推測の裏付け、推測や私見の打破を促す

### ビジネスと収益の成長

- 顧客行動への理解を深めることによる収益維持率の向上
- 収益を創出する使用事例の構築

### チーム間の連携

- ソフトウェアスタックに関する判断におけるチーム間の連携強化（DevOps、DevSecOps）
- SDLC の全ステージに対するフィードバックの提供

### 開発者とエンジニアの満足度向上

- 開発者とエンジニアの業務を、インシデント対応（リアクティブ）からより高価値な作業（プロアクティブ）へと移行
- スキルセットと雇用可能性の向上
- 業務が楽になる
- ワークライフバランスの改善
- イノベーションの促進

New Relic のプラットフォームについて知る

# 付録

オブザーバビリティ性能別、市場機会別、業界別、
地域／国別の重要なトレンドをご確認ください。

# 各性能のハイライト

17 のオブザーバビリティ性能について、調査の時点で回答者がデプロイ済みのものは何か、来年から今後 2 ～ 3 年間にかけて何をデプロイする予定かなど、豊富な情報を掘り下げました。

## AIOps

*プロセスを改善し、インサイトを得るために AI（人工知能）を活用する。*

AIOps をデプロイ済みの回答者は、37% のみでした。しかし、**40% が来年のデプロイを予定し（来年にデプロイ予定の性能の第 2 位）**、15% が今後 2 ～ 3 年のうちにデプロイ予定であると回答しました。これは、AIOps はデプロイされていることがもっとも少ない性能の 1 つだったものの、78% が 2023 年までに、**92% が 2025 年までに AIOps をデプロイ予定であることを意味します。**AIOps のデプロイを予定していないのは、わずか 5% でした。

## アラート

*エラーなどの重要なイベントによりトリガーされる通知を提供する。*

調査対象者の半数以上（52%）がアラートをデプロイ済みで、これは**デプロイ済みの性能の第 4 位**でした。さらに、34% が来年のデプロイを予定し、10% が今後 2 ～ 3 年でのデプロイを予定していました。これは、86% が 2023 年までに、**96% が 2025 年までにアラートをデプロイする予定である**ことを意味します。アラートのデプロイを予定していないのは、わずか 3% でした。

## APM

*パフォーマンスとエラーのアプリケーションを監視する。*

半数近く（45%）の調査対象者が APM をデプロイ済みであると回答し、37% が来年のデプロイを、12% が今後 2 ～ 3 年でのデプロイを予定していました。これは、82% が 2023 年までに、**94% が 2025 年までに APM をデプロイする予定である**ことを意味します。APM のデプロイを予定していないのは、4% のみでした。

## ブラウザ監視

*ブラウザとウェブアプリケーションのアクティビティとパフォーマンスを追跡する。*

ほぼ半数近く（49%）の調査対象者がブラウザ監視をデプロイ済みで、34% が来年のデプロイを、13% が今後 2 ～ 3 年でのデプロイを予定していました。これは、82% が 2023 年までに、**95% が 2025 年までにブラウザ監視をデプロイ予定である**ことを意味します。ブラウザ監視のデプロイを予定していないのは 3% のみでした。

## カスタムダッシュボード

*重要な監視メトリクスの概要を提供する。*

ほぼ半数（47%）の調査対象者がカスタムダッシュボードをデプロイ済みで、35% が来年のデプロイを、13% が今後 2 ～ 3 年でのデプロイを予定していました。これは、82% が 2023 年までに、**95% が 2025 年までにカスタムダッシュボードをデプロイ予定である**ことを意味します。カスタムダッシュボードのデプロイを予定していないのは、4% のみでした。

## データベース監視

*データベースのパフォーマンスを測定、最適化するための基幹的なパフォーマンスメトリクスを収集する。*

半数余り（54%）の調査対象者がデータベース監視をデプロイ済みで、これは**デプロイ済みの性能の第 3 位**でした。さらに、31% が来年のデプロイを、11% が今後 2 ～ 3 年でのデプロイを予定していました。これは、85% が 2023 年までに、**96% が 2025 年までにデータベース監視をデプロイする予定**であることを意味します。データベース監視のデプロイを予定していないのは、わずか 3% でした。

## ディストリビューティッド（分散）トレーシング

*ディストリビューティッド（分散）システムを通過するサービスリクエストを追跡、監視する。*

ディストリビューティッド（分散）トレーシングをデプロイ済みの調査対象者は 36% にとどまり、39% が来年のデプロイを、15% が今後 2 ～ 3 年でのデプロイを予定していました。これは、ディストリビューティッド（分散）トレーシングはデプロイされていることがもっとも少ない性能の 1 つだったものの、75% が 2023 年までに、**90% が 2025 年までにディストリビューティッド（分散）トレーシングをデプロイ予定である**ことを意味します。ディストリビューティッド（分散）トレーシングのデプロイを予定していないのは、6% のみでした。

## エラー追跡

*エラーを追跡、トレースして問題のトラブルシューティングを行う。*

ほぼ半数(49%) の調査対象者がエラー追跡をデプロイ済みで、34% が来年のデプロイを、13% が今後 2 ～ 3 年でのデプロイを予定していました。これは、82% が 2023 年までに、**95% が 2025 年までにエラー追跡をデプロイ予定である**ことを意味します。エラー追跡のデプロイを予定していないのは、4% のみでした。

## インフラストラクチャ監視

*データベースやサーバーと同様にネットワークインフラストラクチャの監視を行う。*

半数余り（51%）の調査対象者がインフラストラクチャ監視をデプロイ済みで、これは**デプロイ済みの性能の第 5 位**でした。さらに、33% が来年のデプロイを予定し、11% が今後 2 ～ 3 年でのデプロイを予定していました。これは、84% が 2023 年までに、**95% が 2025 年までにデータベース監視をデプロイする予定である**ことを意味します。インフラストラクチャ監視のデプロイを予定していないのは、わずか 3% でした。

## Kubernetes 監視

*クラスターやワークロードへの可視性を提供し、Kubernetes デプロイメントの監視を行う。*

Kubernetes 監視をデプロイ済みの調査対象者は 34% にとどまり、39% が来年のデプロイを、16% が今後 2 ～ 3 年でのデプロイを予定していました。これは、Kubernetes 監視はデプロイされていることがもっとも少ないものの、72% が 2023 年までに、**88% が 2025 年までに Kubernetes 監視をデプロイ予定である**ことを意味します。Kubernetes 監視のデプロイを予定していないのは、7% のみでした。これらの結果は、36% がアプリケーションとワークロードをコンテナ化しているという事実と一致しています。

## ログ管理

*エラーとイベントログを保管、検索する。*

半数（50%）の調査対象者がログ管理をデプロイ済みで、これは**デプロイ済みの性能の第 6 位**でした。さらに、34% が来年のデプロイを予定し、12% が今後 2 ～ 3 年でのデプロイを予定していました。これは、84% が 2023 年までに、**96% が 2025 年までにログ管理をデプロイする予定である**ことを意味します。ログ管理のデプロイを予定していないのは、わずか 3% でした。

## ML モデルパフォーマンス監視

*機械学習モデルのパフォーマンスを監視する。*

ML モデルパフォーマンス監視（MLOps）をデプロイ済みの調査対象者は 34% にとどまり、**42%（第 1 位）が来年のデプロイを**、15% が今後 2 ～ 3 年でのデプロイを予定していました。これは、ML モデルパフォーマンス監視はデプロイされていることがもっとも少ない性能の 1 つだったものの、76% が 2023 年までに、**91% が 2025 年までに ML モデルパフォーマンス監視をデプロイ予定である**ことを意味します。ML モデルのパフォーマンス監視デプロイを予定していないのは、5% のみでした。

## モバイル監視

*モバイルアプリケーションとデバイスパフォーマンスを監視する。*

モバイル監視をデプロイ済みの調査対象者は半数以下（43%）で、35% が来年のデプロイを、15% が今後 2 ～ 3 年でのデプロイを予定していました。これは、79% が 2023 年までに、**94% が 2025 年までにモバイル監視をデプロイ予定である**ことを意味します。モバイル監視のデプロイを予定していないのは、4% のみでした。

## ネットワーク監視

*ネットワークトラフィックとパフォーマンスメトリクスを監視する。*

半数を超える（57%）の調査対象者がネットワーク監視をデプロイ済みで、これが**もっともデプロイされている性能**でした。さらに、30% が来年のデプロイを、11% が今後 2 ～ 3 年でのデプロイを予定していました。これは、86% が 2023 年までに、**97% が 2025 年までにネットワーク監視をデプロイする予定である**ことを意味します。ネットワーク監視のデプロイを予定していないのは、わずか 2% でした。

## セキュリティ監視

*潜在的なセキュリティの脅威に関する脆弱性の指標を収集し、分析する*

半数以上（56%）の調査対象者がセキュリティ監視をデプロイ済みで、これは**デプロイ済みの性能の第 2 位**でした。さらに、29% が来年のデプロイを予定し、12% が今後 2 ～ 3 年でのデプロイを予定していました。これは、85% が 2023 年までに、**96% が 2025 年までにセキュリティ監視をデプロイする予定である**ことを意味します。セキュリティ監視のデプロイを予定していないのは、わずか 3% でした。

## サーバーレス監視

*サーバーレスアプリケーションのパフォーマンスメトリクスとエラーを監視する。*

サーバーレス監視をデプロイ済みの調査対象者は 38% にとどまり、37% が来年のデプロイを、16% が今後 2 ～ 3 年でのデプロイを予定していました。これは、サーバーレス監視はデプロイされていることがもっとも少ない性能の 1 つだったものの、75% が 2023 年までに、91% **が 2025 年までにサーバーレス監視をデプロイ予定である**ことを意味します。サーバーレス監視のデプロイを予定していないのは、6% のみでした。これらの結果は、36% の回答者がサーバーレスコンピューティングを導入しているという事実と一致しています。

## 外形監視

*パフォーマンスを予測するため、シミュレーションされる使用を監視する。*

外形監視をデプロイ済みの調査対象者は 34% にとどまり、**39% が来年のデプロイを（来年にデプロイ予定の第 3 位）**、15% が今後 2～3 年でのデプロイを予定していました。これは、外形監視はデプロイされていることがもっとも少ない性能の 1 つだったものの、74% が 2023 年までに、89% **が 2025 年までに外形監視をデプロイ予定である**ことを意味します。外形監視のデプロイを予定していないのは、6% のみでした。

# 市場機会のハイライト

調査対象者が今後 3 年間でもっともオブザーバビリティを必要とする 11 のテクノロジーについても、詳細を分析しました。

## 5G

*モバイルブロードバンド通信の第 5 世代テクノロジー規格*

3 分の 1 の回答者が、自社組織において今後 3 年間でもっとも必要になるのは、5G 向けのオブザーバビリティであると予測しています（全体で 4 番目）。実務担当者は、5G との回答がやや高い傾向にありました（35% で 4 番目、対して ITDM では 30% で 6 番目）。小規模および大規模組織の回答者は、5G との回答がより多い傾向にありました（38% で 3 番目、対して中規模組織では 30% で 6 番目）。これは、医療／製薬（44%）、教育（40%）、IT ／テレコミュニケーション（36%）業界において 3 番目に多い回答でした。興味深いことに、AI を選択した 47% の回答者のうち半数以上（52%）が、トップの回答として 5G も選択しました。

## 人工知能

*機械による人間の知能プロセスのシミュレーション*

ほぼ半数の回答者（47%）が、自社組織において今後 3 年間でもっとも必要になるのは、AI 向けのオブザーバビリティであると予測しています（全体で 1 番目）。北米の回答者（52%）、エグゼクティブ（51%）、また複数の業界（サービス／コンサルティング（62%）、エネルギー／ユーティリティ（60%）、政府機関（58%）、IT ／テレコミュニケーション（51%）など）の回答者において、半数以上となりました。興味深いことに、AI を選択した 47% の回答者のうち半数以上が、5G、ブロックチェーン、IoT もトップの回答として選択しました。

## ブロックチェーン

*暗号通貨に用いられることの多い、非中央集権の仕組みにもとづく技術*

ほぼ 3 分の 1（32%）の回答者が、自社組織において今後 3 年間でもっとも必要になるのは、ブロックチェーン向けのオブザーバビリティであると予測しています（全体で 5 番目）。非エグゼクティブマネージャーは、この必要性を回答する傾向がもっとも低く（26%、対してエグゼクティブが 36%、実務担当者が 32%）、ヨーロッパの回答者も同様でした（29%、対してアジア太平洋で 35%、北米で 34%）。この必要性を回答した回答者は、エネルギー／ユーティリティ（40%）、IT ／テレコミュニケーション（35%）業界で多い傾向にありました（4 番目）。興味深いことに、AI を選択した 47% の回答者のうち半数以上（52%）が、ブロックチェーンも選択しました。

## ビジネスアプリケーション

*ERP や CRM などの、業務遂行において重要性の高いアプリケーション*

3 分の 1 以上の回答者（35%）が、自社組織において今後 3 年間でもっとも必要になるのは、ビジネスアプリケーション向けのオブザーバビリティであると予測しています（全体で 3 番目）。ビジネスアプリケーションをトップと回答したのは工業／原料／製造業界（43%、IoT と同率）のみで、小売／消費者業界においては 2 番目（40%）でした。興味深いことに、ビジネスアプリケーションを選択した 35% の回答者のうち 42% が、トップ回答として無差別的パーソナライゼーションも選択しました。

## クラウドゲーミング

*データセンターのリモートサーバでホストされるビデオゲームで、ゲームオンデマンド、サービスとしてのゲームとも呼ばれる*

4 分の 1 以下（22%）の回答者が、自社組織においてもっとも必要になるのは、クラウドゲーミング向けのオブザーバビリティであると予測しています（全体で 7 番目）。IT ／テレコミュニケーション業界の回答者がもっとも多く予測する傾向にありました（27%）。クラウドゲーミングはエッジコンピューティングを使用することが多いですが、今後数年間におけるオブザーバビリティの予測に関しては、この 2 つに明確な相関性は見られませんでした。

## エッジコンピューティング

*IoT デバイスなどの、クラウドからローカルのロケーションへとプロセスを移行するアーキテクチャー*

エッジコンピューティングとの回答は 6 番目でした（31%）。実際、IoT を選択した回答者の 41% が、エッジコンピューティングも選択しました。エネルギー／ユーティリティ、サービス／コンサルティング業界の回答者は、エッジコンピューティングとの回答が他の業界よりも多い傾向にありました（それぞれ 42%、45%）。エグゼクティブも、エッジコンピューティング向けのオブザーバビリティの必要性を予測する回答が多い傾向にありました（38%、対して非エグゼクティブが 31%、実務担当者が 29%）。

## 無差別的パーソナライゼーション

*パーソナライズされた、リアルタイムのデジタルエクスペリエンス*

約 5 分の 1 の回答者（22%）が、無差別的パーソナライゼーション向けのオブザーバビリティがもっとも必要になると予測しました（全体で 8 番目）。アジア太平洋の回答者に、この必要性を予測する傾向が多く（26%、対してヨーロッパで 19%、北米で 22%）、また教育、小売／消費者業界の回答者も同様でした（それぞれ 34%、26%）。一方、もっとも回答が少なかったのは、小規模組織（18%、対して中規模組織で 21%、大規模組織で 24%）、またサービス／コンサルティング（17%）、医療／製薬（13%）、NPO ／不特定（11%）の各業界でした。興味深いことに、ビジネスアプリケーションを選択した 35% の回答者のうち 42% が、トップ回答として無差別的パーソナライゼーションも選択しました。

## モノのインターネット（IoT）

*インターネットや他のネットワークに接続されたデバイスのシステム*

IoT は、調査対象者が自社組織において今後 3 年間でオブザーバビリティがもっとも必要になると予測するテクノロジーとして、全体の第 2 位でした（44%）。ただし、IoT は、エネルギー／ユーティリティ（61%）、教育（51%）、医療／製薬（47%）、工業／原料／製造（43%）、金融／保険（42%）などの複数の業界においてトップの回答でした。大規模組織も、IoT を多く選択する傾向にありました（48%、対して小規模組織で 39%、中規模組織で 43%）。興味深いことに、AI を選択した 47% の回答者のうち半数以上（52%）が、トップ回答として IoT も選択しました。

## メタバース

*AI、IoT、エッジコンピューティング、ブロックチェーン、Web3、仮想現実（VR）、拡張現実（AR）で仮想的に構築された生活のシミュレーション*

メタバースは、もっとも回答が少ない選択肢でした。今後 3 年間でオブザーバビリティが必要になると予測したのは、回答者の 19% にとどまりました。回答が多い傾向にあったのは、アジア太平洋（22%、対してヨーロッパでは 18%、北米では 17%）、小規模組織（22%、対して中規模と大規模では 18%）、エネルギー／ユーティリティ（31%）、医療／製薬（23%）、サービス／コンサルティング（21%）の各業界です。興味深いことに、5G を選択した 33% の回答者のうち 39% が、トップ回答としてメタバースも選択しました。さらに、ブロックチェーンを選択した 32% の回答者のうち 38% が、トップ回答としてメタバースも選択しました。

## スーパーアプリ

*複数の使用事例に 2 つ以上のコアビジネスアセットを活用するデジタルプラットフォーム*

今後 3 年間でスーパーアプリ向けのオブザーバビリティが必要になると予測したのは、回答者の 20% のみでした。スーパーアプリは、モバイルファーストが支配的な国（日本と米国のみがブラウザファースト）の、複数の事業部門を持つ大規模組織においてより適用される傾向にあります。特にアジア太平洋、南米、東欧、アフリカ、中東において優勢です。スーパーアプリを使用する組織は多くありませんが、使用組織においては、オブザーバビリティが絶対的に必要になる、包括的な巨大プロジェクトとなります。

## Web3

*ブロックチェーン技術にもとづく、インターネットの第 3 世代と称されるアプローチ*

約 5 分の 1（19%）の回答者が、Web3 向けのオブザーバビリティが今後 3 年間でもっとも必要になると予測しています（全体では下から 2 番目）。アジア太平洋では最下位でした（17%）が、ヨーロッパではやや多い傾向にありました（21%）。エネルギー／ユーティリティ業界の回答者では多く（25%）、政府機関と NPO ／不特定業界の回答者ではもっとも少ない傾向にありました（それぞれ 15%、14%）。Web3 はブロックチェーン技術を使用するものの、オブザーバビリティの予測に関してこの 2 つに明確な相関性は見られませんでした。

# 業界のハイライト

調査において示された 10 の業界の各データを比較すると、
興味深い相違が浮き彫りになりました。

## 教育

教育業界の回答者には、以下の傾向が**もっとも多く**見られました。

- クラウドリソースの使用と支出の最適化（63%）、DX の取り組みの支援（47%）にオブザーバビリティを使用
- 予測可能な支出に関心が高い（54%）
- 自社組織において、今後 3 年間で IoT 向けのオブザーバビリティがもっとも必要だと予測（51%）
- 自動化されたインシデント対応のワークフローが、MTTR の短縮にもっとも有効と回答（49%）
- オブザーバビリティの最大の利点はカスタマーエクスペリエンスの向上と示唆（47%）
- ユーザー／データ取り込みベースのハイブリッドな価格設定モデルが好ましい（40%）
- オブザーバビリティに単一のツールを使用（9%）

以下のような傾向が**より多く**見られました。

- 予算不足（51%）、価格が高すぎる（31%）ことが、フルスタックオブザーバビリティの優先／実現の最大の障壁であると回答
- オブザーバビリティは、当て推量の作業を減らす（43%）、業務を楽にする（40%）、推測を裏付ける（37%）、スキルセットと雇用可能性を高める（37%）という点で、エンジニア／開発者の生活の向上にもっとも役立つと回答
- ビジネスインパクトが小さい／中程度の稼働停止の検知と解決にかかる時間は 30 分未満

SDLC の全段階での拡張的または完全なオブザーバビリティの使用は**少ない傾向**にありました。

## エネルギー／ユーティリティ

エネルギー／ユーティリティ業界の回答者には、以下の傾向が**もっとも多く**見られました。

- マルチクラウド環境への移行がオブザーバビリティの最大の促進要因であると回答（60%）
- 自社組織において、今後 3 年間で AI 向けのオブザーバビリティがもっとも必要だと予測（60%）
- 自社アプリ／システムのレジリエンスに対する開発者の自信がオブザーバビリティの主な利点であると回答（51%）
- ペナルティなしのオートスケール能力に関心が高い（42%）
- システムが十分にインストゥルメンテーションされていないことが、フルスタックオブザーバビリティの優先／実現の最大の障壁であると回答（38%）
- オブザーバビリティをどちらかというとインシデント対応／予防強化とみなしている（33%）
- 17 の性能すべてをデプロイしていると回答（10%）
- 本レポートでの定義による成熟したオブザーバビリティの実践を実施（10%）

以下のような傾向が**より多く**見られました。

- 統合されたテレメトリデータがあると回答（54%）
- インシデント対応のワークフローの自動化とよりよい DevOps の実践が MTTR の短縮にもっとも有効と回答（いずれも 44%）
- 自社組織が、IT 予算の 10%超～ 15%未満をオブザーバビリティツールに配分していると示唆（43%）
- オブザーバビリティは、当て推量の作業を減らす、ワークライフバランスを改善する（いずれも 42%）という点でエンジニア／開発者の生活の向上にもっとも役立つと回答
- 自社組織において、今後 3 年間でエッジコンピューティング向け（42%）およびメタバース向け（31%）のオブザーバビリティがもっとも必要だと予測
- 稼働停止が週 1 回以上発生
- ビジネスインパクトが小さい／中程度の稼働停止の検知には 30 分未満、ビジネスインパクトが大きい稼働停止の検知には 30 分超を費やすと回答

オブザーバビリティツール／プラットフォームに関するもっとも重要な価格設定の特性として、予算に見合った価格との回答が**もっとも少ない傾向**にありました（27%）。

## 金融／保険

金融／保険業界の回答者には、以下の傾向が**もっとも多く**見られました。

- 単一の、連結プラットフォームが好ましい（60%）
- フルスタックオブザーバビリティの優先／実現の最大の障壁は、利点の理解不足であると回答（28%）
- 運用段階の 83% をはじめ、SDLC の全段階で拡張的または完全なオブザーバビリティを使用

以下のような傾向が**より多く**見られました。

- オブザーバビリティをどちらかというと中核的な事業目標の達成要因であるとみなしている（54%）
- 自社組織において、今後 3 年間で IoT 向けのオブザーバビリティがもっとも必要だと予測（42%）
- オブザーバビリティツール／プラットフォームのもっとも重要な価格特性として、従量課金制の請求とペナルティなしであらゆるテレメトリデータタイプを取り込める能力を好む（いずれも 31%）
- オブザーバビリティツール／プラットフォームのもっとも重要な価格特性として、特にハイブリッドなユーザーベースの価格設定を好む（29%）
- 単一のオブザーバビリティプラットフォームでソフトウェアとシステムの中断を検知（24%）
- 稼働停止が週 1 回以上発生

この業界の回答者は、本レポートでの定義にもとづくフルスタックオブザーバビリティの実現が**もっとも少ない傾向**にありました（17%）。

## 政府機関

政府機関の回答者には、以下の傾向が**もっとも多く**見られました。

- オブザーバビリティの主な利点として、従業員数の削減（55%）、IT ツールの統合（40%）と回答
- オブザーバビリティを分散化システムのトラブルシューティングに使用（50%）
- 本レポートでの定義によるフルスタックオブザーバビリティを実現している（42%）
- 従業員の増員が MTTR の短縮にもっとも有効と回答（41%）

以下のような傾向が**より多く**見られました。

- クラウドネイティブなアプリケーションアーキテクチャーの開発がオブザーバビリティのニーズを促進と回答（58%）
- 予測可能な支出に関心が高い（50%）
- オブザーバビリティは、複雑な分散した技術スタックの管理において当て推量の作業を減らすという点で、エンジニア／開発者の生活の向上にもっとも役立つと回答（42%）
- 予算に見合う価格、価格の透明性、ハイブリッドな価格設定モデルを、オブザーバビリティツール／プラットフォームのもっとも重要な価格特性とみなす（いずれも 39%）
- フルスタックオブザーバビリティの優先／実現の障壁として、価格が高すぎる（35%）、予算不足（31%）と回答
- ビジネスインパクトが中程度／大きい稼働停止の発生は月に 2 ～ 3 回以下

以下が**もっとも少ない傾向**にありました。

- SDLC の全段階で拡張的または完全なオブザーバビリティを使用
- 組織の DevOps への IT 移行の支援、コスト削減の取り組み（ツールの統合）、新製品／サービスの市場投入の迅速化にオブザーバビリティを使用（すべて 15%）

## 医療／製薬

医療／製薬業界の回答者には、以下の傾向が**もっとも多く**見られました。

- サーバーレスコンピューティングの導入がオブザーバビリティの最大の促進要因であると回答（49%）
- オブザーバビリティのもっとも大きな利点としてカスタマーエクスペリエンスの向上（43%）、またオブザーバビリティの主な利点の一つとしてビジネス／収益の成長（39%）と回答
- 成熟したオブザーバビリティの実践のもっとも重要な特性は、サービスの中断とビジネスリスクの低減と回答（33%）

以下のような傾向が**より多く**見られました。

- 統合されたテレメトリデータがあると回答（54%）
- オブザーバビリティツール／プラットフォームのもっとも重要な価格特性として、予算に見合う価格設定と回答（47%）
- 自社組織において、今後 3 年間で IoT 向けのオブザーバビリティが必要だと予測（47%）
- オブザーバビリティは、チーム間の連携を可能にするという点で開発者／エンジニアの生活の向上にもっとも役立つと回答（42%）
- オブザーバビリティツールに関するスタッフのトレーニングが MTTR の短縮にもっとも有効と回答（40%）
- 予算不足、システムが十分にインストゥルメンテーションされていないことが、フルスタックオブザーバビリティの優先／実現の最大の障壁であると回答（いずれも 31%）
- 本レポートでの定義による成熟したオブザーバビリティの実践を実施（7%）
- 稼働停止が週 1 回以上発生

## 工業／原料／製造

工業／原料／製造業界の回答者には、以下の傾向が**もっとも多く**見られました。

- 自社組織において、今後 3 年間で ERP や CRM などのビジネスアプリ向けのオブザーバビリティがもっとも必要だと予測（43%、IoT と同率）
- オブザーバビリティを組織の DevOps への IT 移行の支援に使用（35%）
- ソフトウェアスタックに関する判断におけるチーム間の連携強化が、成熟したオブザーバビリティの実践のもっとも重要な特性と回答（34%）
- 販売サイクルの長さが、フルスタックオブザーバビリティの優先／実現の最大の障壁であると回答（27%）

以下のような傾向が**より多く**見られました。

- 単一の、連結プラットフォームが好ましい（54%）
- よりよい DevOps の実践が MTTR の短縮にもっとも有効であるとの回答がトップ（42%）
- オブザーバビリティツール／プラットフォームのもっとも重要な価格特性として、価格の透明性を選択（36%）
- IT 予算の 10%超～ 15%未満をオブザーバビリティツールに配分（30%）
- すでにフルスタックオブザーバビリティを優先／実現していると回答（5%）
- ビジネスインパクトが小さい稼働停止の検知には 30 分以内、ビジネスインパクトが大きい稼働停止の検知と解決には 30 分超を費やすと回答

## IT ／テレコミュニケーション

IT ／テレコミュニケーションの回答者は、オブザーバビリティの主な利点は、高価値業務／イノベーション促進へのリソースの再配置であるとの回答が**もっとも多い傾向**にありました（35%）。

以下のような傾向が**より多く**見られました。

- オブザーバビリティをどちらかというと中核的な事業目標の達成要因とみなしている（52%）
- 統合されたテレメトリデータがあると回答（52%）
- ソフトウェアデプロイメントに CI ／ CD の実践を活用していると回答（52%）
- よりよい DevOps の実践が MTTR の短縮にもっとも有効であるとの回答がトップ（41%）
- 従量課金制が好ましい（35%）
- 自社 IT パフォーマンスは十分であると認識（34%）
- 単一のオブザーバビリティプラットフォームでソフトウェアとシステムの中断を検知（24%）
- 稼働停止が週 1 回以上発生

## NPO ／不特定

NPO ／不特定業界の回答者には、以下の傾向が**もっとも多く**見られました。

- オブザーバビリティツール／プラットフォームのもっとも重要な価格特性として、予算に見合う価格設定を選択（54%）
- 運用効率の向上がオブザーバビリティの主な利点であると回答（52%）
- 成熟したオブザーバビリティの実践のもっとも重要な特性は、臨機応変なデータクエリ能力であると回答（39%）
- オブザーバビリティツール／プラットフォームに関するもっとも重要な請求特性として、従量課金制を選択（39%）
- テレメトリデータの可視化／ダッシュボード構築は多種化されていると回答（36%）

以下のような傾向が**より多く**見られました。

- マルチクラウド環境への移行がオブザーバビリティの最大の促進要因であると回答（43%）
- オブザーバビリティは、チーム間の連携を可能にするという点で開発者／エンジニアの生活の向上にもっとも役立つと回答（43%）
- オブザーバビリティツールに関するスタッフのトレーニングが MTTR の短縮にもっとも有効であると示唆（39%）
- 価格が高すぎることがフルスタックオブザーバビリティの優先／実現の最大の障壁であると回答（39%）
- オブザーバビリティツール／プラットフォームのもっとも重要な価格特性の 1 つとして、価格の透明性を選択（39%）
- 稼働停止の発生は月に 2 ～ 3 回以下
- ビジネスインパクトが小さい／大きい稼働停止の検知は 30 分以内と回答

## 小売／消費者

小売／消費者業界の回答者には、以下の傾向が**もっとも多く**見られました。

- テレメトリデータは統合されており（60%）、そのデータの可視化／ダッシュボード構築は統合されている（79%）と回答
- オブザーバビリティをどちらかというと中核的な事業目標の達成要因であるとみなしている（57%）
- 成熟したオブザーバビリティの実践のもっとも重要な特性は、ソフトウェアスタックに関する判断におけるチーム間の連携強化と回答（31%）
- 運用段階の 83% をはじめ、SDLC の全段階で拡張的または完全なオブザーバビリティを使用
- 10 以上のオブザーバビリティツールを使用（7%）

以下のような傾向が**より多く**見られました。

- インシデント対応のワークフローの自動化と、よりよい DevOps の実践が、MTTR の短縮にもっとも有効であると回答（いずれも 42%）
- 今後 3 年間で、ERP や CRM などのビジネスアプリ向けのオブザーバビリティがもっとも必要だと予測（40%）
- オブザーバビリティの利点を理解していないと回答（34%）
- 本レポートでの定義による成熟したオブザーバビリティの実践を実施（6%）
- 従量課金制の請求が好ましい
- 稼働停止の検知は 30 分未満と回答

## サービス／コンサルティング

サービス／コンサルティング業界の回答者には、以下の傾向が**もっとも多く**見られました。

- ソフトウェアデプロイメントに CI ／ CD の実践を活用していると回答（57%）
- アップタイムと信頼性の改善が、オブザーバビリティの主な利点であると回答（49%）
- 自社のテレメトリデータはサイロ化していると回答（45%）
- オブザーバビリティをソフトウェアのリリースサイクルの自動化に使用（40%）
- すでにフルスタックオブザーバビリティを優先／実現していると回答（6%）

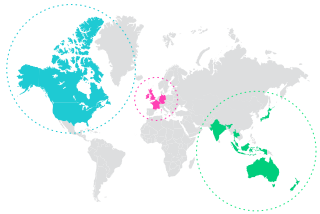
以下のような傾向が**より多く**見られました。

- 自社組織において、今後 3 年間で、エッジコンピューティング向け（45%）と、ERP や CRM などのビジネスアプリ向け（40%）のオブザーバビリティがもっとも必要だと予測
- オブザーバビリティツールに関するスタッフのトレーニングが、MTTR の短縮にもっとも有効であると回答（43%）
- オブザーバビリティツール／プラットフォームのもっとも重要な価格特性の 1 つとして、価格の透明性を選択（43%）
- オブザーバビリティは、チーム間の連携を可能にするという点で開発者／エンジニアの生活の向上にもっとも役立つと回答（43%）
- 価格が高すぎる（34%）、予算不足（30%）が、フルスタックオブザーバビリティの優先／実現の最大の障壁であると回答
- ビジネスインパクトが中程度／大きい稼働停止の発生は月に 2 ～ 3 回以下
- 稼働停止の解決にかかる時間は 30 分超

この業界の回答者は、クラウドリソースの使用と支出の最適化のためのオブザーバビリティの使用が**もっとも少ない傾向**にありました（17%）。

# 各地域のハイライト

ここでは、調査結果の地域別の相違について詳しく見ていきましょう。



| | アジア太平洋 | ヨーロッパ | 北米 |
|---|---|---|---|
| **現在のデプロイメント** | 多くの性能がデプロイ済みで、フルスタックオブザーバビリティの実現と、SDLC の計画およびビルド段階での拡張的または完全なオブザーバビリティの使用がもっとも多い傾向にありました | デプロイされている性能がもっとも少なく、フルスタックオブザーバビリティの実現と、成熟したオブザーバビリティの実践、SDLC の全段階での拡張的または完全なオブザーバビリティの使用がもっとも少ない傾向にありました | 成熟したオブザーバビリティの実践と、SDLC のデプロイと運用段階での拡張的または完全なオブザーバビリティの使用がもっとも多い傾向にありました |
| **テレメトリデータ** | データのサイロ化（15% の完全なサイロ化を含む）、クロスコミュニケーションのない複数の可視化ソリューション（11% の完全な多種化を含む）がもっとも多い傾向にありました | 統合されたテレメトリデータ、単一のダッシュボードソリューションに可視化されたテレメトリデータがより多い傾向にありました | 統合されたテレメトリデータ、単一のダッシュボードソリューションに可視化されたテレメトリデータがもっとも多い傾向にありました |
| **戦略** | オブザーバビリティを、どちらかというと中核的な事業目標の達成要因であるとみなす傾向がもっとも高い | オブザーバビリティを、どちらかというとインシデント対応／予防強化とみなす傾向がもっとも高い | オブザーバビリティを、どちらかというと中核的な事業目標の達成要因とみなす傾向がより高い |
| **予算配分** | IT 予算の 15% 超をオブザーバビリティツールに配分する傾向がもっとも高く、来年の増額を予定しているとの回答がより多い | IT 予算の 10% 未満をオブザーバビリティツールに配分する傾向がもっとも高く、来年の増額を予定しているとの回答がもっとも少ない | IT 予算の 10% 未満をオブザーバビリティツールに配分する傾向がより高く、来年の増額を予定しているとの回答がもっとも多い |
| **サービスレベルのメトリクス** | 稼働停止が 1 日に複数回発生する傾向がもっとも高く、稼働停止の検知に 60 分超かかる傾向がより高い | 稼働停止が週 1 回以上発生する傾向がもっとも高く、稼働停止の解決にかかる時間は 30 分未満である傾向がもっとも高い | 稼働停止の発生がもっとも少なく、稼働停止の検知にかかる時間は 30 分未満である傾向がもっとも高い |
| **オブザーバビリティの最大の利点** | 問題が顧客に影響を及ぼす前のプロアクティブな検知と、開発者／エンジニアの生産性の向上 | 運用効率の向上と、開発者／エンジニアの業務を楽にする | アップタイムと信頼性を改善し、チーム間の連携を可能にする（DevOps、DevSecOps） |
| **オブザーバビリティの上位の使用事例** | DX の取り組みの支援 | クラウドリソースの使用と支出の最適化 | DevOps への組織的な IT 移行の支援と、クラウドリソースの使用と支出の最適化（同率） |
| **フルスタックオブザーバビリティの優先／実現の主な課題** | 監視ツールが多すぎること、システムのインストゥルメンテーションが不十分であること（同率） | 予算不足 | 利点の理解不足 |

**表 14.** 地域別の調査結果の主な違い

# アジア太平洋

アジア太平洋は、多様な文化とビジネス慣行が存在する地域ですが、その他の地域と比較すると、依然として興味深い相違が見られます。たとえば全体として、アジア太平洋の回答者は、ヨーロッパや北米の回答者と比べてもっとも多くのオブザーバビリティ性能をデプロイしていることが明らかになりました。アジア太平洋の組織は、本レポートでの定義によるフルスタックオブザーバビリティをもっとも実現している傾向にあり（33%）、加えて、オブザーバビリティをどちらかというと中核的な事業目標の達成要因であるとみなす傾向がもっとも多く見られました（58%）。

**連結されたプラットフォームへの移行**

他の地域と比べ、単一の連結プラットフォームを好む傾向がもっとも多く（55.3%）、ただしフルスタックオブザーバビリティの優先／実現を阻む最大の障壁として、監視ツールが多すぎること、システムが十分にインストゥルメンテーションされていないことが挙げられました（いずれも 28%）。また、IT ツールの統合（25%）の経験はもっとも少なく、データのサイロ化（45%、15% の完全なサイロ化を含む）、クロスコミュニケーションのない複数の可視化ソリューション（33%、11% の完全な多種化を含む）がもっとも多い傾向にありました。概して、アジア太平洋の調査対象者は、単一の連結プラットフォームを望んでいるものの、フルスタックオブザーバビリティを得るためのシステムのインストゥルメンテーションを欠いていました。

**プロアクティブな検知とよりよい DevOps の実践**

彼らは、問題が顧客に影響を及ぼす前のプロアクティブな検知を行っているとの回答がもっとも多い傾向にありました（40%）。しかし同時に、稼働停止が 1 日に複数回発生することがもっとも多く、稼働停止の検知に 60 分超かかることがより多い傾向にありました。彼らは、MTTR の短縮に有効なのはよりよい DevOps の実践であるとの選択がもっとも多い傾向にありました（42%）。

**より多くのオブザーバビリティ性能のデプロイ**

今後については、62% が 5 つ以上の性能をデプロイ予定であることを含め、大多数（91%）が、来年に追加的なオブザーバビリティ性能をデプロイする予定であると回答しました。そのなかで、今後のデプロイメントとしてもっとも多い性能は、ML モデルパフォーマンス監視（43%）であり、次いで APM（39%）、Kubernetes と外形監視（38%）、AIOps とディストリビューティッド（分散）トレーシング（37%）でした。追加的な性能のデプロイを予定していないのは 10% のみでした。約半数（51%）が、今後のデプロイメント計画に合わせて来年の予算増加を予定していると回答しました。

**国別のハイライト**

各国の結果を見ると、オブザーバビリティの導入をどう活用するかの違いにおいて、アジア太平洋地域の多様性が見えてきます。

**オーストラリア**🇦🇺 と**ニュージーランド**🇳🇿は、ツールの統合とコスト削減に注力

**インド** 🇮🇳と**インドネシア** 🇮🇩は、オブザーバビリティを DevOps への IT 移行の支援に活用

**日本** 🇯🇵は、サーバーレスおよびコンテナ化への移行の支援にオブザーバビリティを主に使用と示唆

**マレーシア** 🇲🇾の技術チームは、まだ DX と分散化システムに取り組んでいる

**シンガポール** 🇸🇬の組織は、オブザーバビリティをソフトウェアのリリースサイクルの自動化に適用

**タイ** 🇹🇭は、IoT デバイス監視のフルオブザーバビリティエステートへの連結、クラウドリソースの使用と支出の最適化、DX の取り組みの支援に注力

# アジア太平洋

## 東南アジア諸国連合（ASEAN）

インドネシア、マレーシア、シンガポール、タイからなる東南アジア諸国連合（ASEAN）では、オブザーバビリティは主に、DX の取り組みの支援、デジタルカスタマーエクスペリエンスの向上、AI と IoT の今後の展開計画の支援のための必須ツールとして使用されていました。

**インドネシア** 🇮🇩：DevOps、IoT、リスクの低減が優先事項

**マレーシア** 🇲🇾：セキュリティ、リスク、コンプライアンスがオブザーバビリティ戦略を促進する主要な要因

**シンガポール** 🇸🇬：オブザーバビリティのソフトウェアのリリースサイクルの自動化への適用が重要

**タイ** 🇹🇭：AI、IoT、クラウドネイティブなアプリケーションアーキテクチャーの開発が優先事項

### デジタルトランスフォーメーション（DX）とカスタマーエクスペリエンス

ASEAN の調査対象者は、オブザーバビリティを主に、DX の戦略支援、デジタルカスタマーエクスペリエンスの向上に使用していました。

ASEAN では、回答者の 43% が、デジタルカスタマーエクスペリエンスの競争優位性の改善と獲得に向けた DX の取り組みの支援にオブザーバビリティを適用していると回答しました。

3 分の 1 以上（34%）が、ソフトウェアのリリースサイクルの自動化、新製品／サービスの市場投入の迅速化、クラウドリソースの使用と支出の最適化にオブザーバビリティを適用していると回答しました。

### 教育と AI の機会

データでは、オブザーバビリティの潜在能力について技術チームを教育する機会と、明確なオブザーバビリティ戦略の重要性が示されています。ASEAN のほぼ 3 分の 1（32%）の回答者が、フルスタックオブザーバビリティの優先／実現に関する主な課題は、戦略の欠如であると回答しました。

SLO ／ SLA の達成にオブザーバビリティを活用しているとの回答は、26% にとどまりました。

今後 3 年間で、彼らは AI にもっとも注力する予定であり、半数以上（51%）が AI 向けのオブザーバビリティの必要性を予測しました。

### ツールの分散

ツールの分散は、技術チームにとって統一性が欠如する問題が生じます。

ASEAN の半数の回答者が、ソフトウェアおよびシステムの中断を複数のツールを通じて検知していると回答し、いっぽうで 39% が、いまだに手動のチェック／検査、インシデントチケット、苦情を通じて最初に検知すると回答しました。

単一のオブザーバビリティプラットフォームを通じて最初に中断を検知するとの回答は、11% のみでした。

### 今後のオブザーバビリティ計画

ASEAN の回答者は、来年に外形監視と ML モデルパフォーマンス監視のデプロイを予定しているとの回答がもっとも多く（41%）、次いで APM（37%）、Kubernetes 監視（36%）、AIOps（33%）、サーバーレス監視（32%）となりました。

大多数が、2025 年までにほとんどのオブザーバビリティ性能（90 ～ 99%）を得るだろうと予測しています。しかし、自社のデプロイメント計画に合わせて来年の予算を増額すると答えたのは 39% のみで、これはアジア太平洋地域でもっとも低く、いっぽうで 27% は現状維持、34% は削減するとの回答でした。

**26%**

が、SLO ／ SLA の達成にオブザーバビリティを活用

# アジア太平洋

## オーストラリアとニュージーランド

オーストラリアとニュージーランド（ANZ）では、オブザーバビリティ使用の主な促進要因は、コスト削減とツールの統合でした。ANZ の回答者の 3 分の 1 近く（28%）は、フルスタックオブザーバビリティの実現の主な課題として、予算不足を挙げました。また、ニュージーランドの回答者は、オブザーバビリティを組織の DevOps への移行の支援に使用し、またオーストラリアの回答者は、今後 3 年間で AI 向けのオブザーバビリティの使用を予測していました。

**ツールの統合**

オーストラリアの 3 分の 1、またニュージーランドの 4 分の 1 以上（28%）の回答者は、オブザーバビリティをコスト削減の取り組みの支援に使用していると回答しました。

オーストラリアの半数以上（57%）の回答者は、オブザーバビリティに 6 ～ 7 つのツールを使用していました。特筆すべき点として、1 つのツールを使用しているとの回答はありませんでした。

オーストラリアの半数以上（52%）の回答者が、複数のツールを通じて最初にソフトウェアとシステムの中断を検知すると回答し、これに対して単一のオブザーバビリティプラットフォームでの検知は 21% にとどまりました。また 27% が、いまだに手動のチェック／検査、インシデントチケット、苦情を通じて最初に検知すると回答しました。

ANZ のほぼ 4 分の 1 の回答者が、監視ツールが多すぎること（24%）、データのサイロ化（23%）がフルスタックオブザーバビリティの優先／実現を阻む主な課題であると回答しました。

**DevOps、AI、最高幹部の支持**

ニュージーランドは DevOps の状態を目指しているいっぽうで、オーストラリアでは少し状況が異なります。ニュージーランドの回答者の半数近く（44%）が、オブザーバビリティを DevOps への組織的な IT 移行の支援に適用すると回答したのに対し、オーストラリアの回答者では 22% のみでした。

オーストラリアの回答者のほぼ半数（49%）は、自社組織において今後 3 年間で AI 向けのオブザーバビリティの必要性を予測しているのに対し、ニュージーランドの回答者では 35% でした。

最高幹部はオブザーバビリティを強く支持していました。ANZ の回答者の多くは、技術に特化していない幹部の 83%、技術に特化した幹部の 75% を含め、最高幹部のオブザーバビリティへの支持は高いと示唆しています。

**予算と専門人材の不足**

フルスタックオブザーバビリティの優先／実現への最大の課題は、低いパフォーマンスレベルと予算または人材の不足に集約されました。

自社の IT パフォーマンスが十分である（現状のパフォーマンスの改善は必要ない）と答えたのは、オーストラリアの回答者の 30% のみでした。

ニュージーランドの回答者の 3 分の 1 以上（35%）は、予算不足がフルスタックオブザーバビリティの優先／実現への最大の課題であると回答しました。

ANZ の回答者のほぼ 3 分の 1（29%）が、専門の人材不足をフルスタックオブザーバビリティの優先／実現への最大の課題として挙げました。

**今後のオブザーバビリティ計画**

ANZ の回答者は、来年に APM と ML モデルパフォーマンス監視のデプロイを予定しているとの回答がもっとも多い傾向にあり（45%）、次いで外形監視（39%）、サーバーレス監視およびカスタムダッシュボード(いずれも 37%)、ディストリビューティッド（分散）トレーシング（36%）となりました。

ANZ の回答者の大多数は、2025 年までにほぼすべてのオブザーバビリティ性能（86 ～ 99%）を得るだろうと予測しています。したがって、ほぼ半数（47%）が、自社のデプロイメント計画に合わせて来年の予算を増額すると答えいっぽうで、21% は現状維持、31% は削減予定と回答しました。

**29%**

が、フルスタックオブザーバビリティの優先／実現のための専門人材が不足していると回答。

# アジア太平洋

## インド

カスタマーエクスペリエンスを非常に重視しながらも、インドの調査対象者では、自社の IT パフォーマンスが十分であるとの回答は 35% のみにとどまり、IT パフォーマンスが課題であると考えていました。さらに、ほぼ半数（48%）が、複数ツールを通じて最初に稼働停止を検知しており、またほぼ 3 分の 1（31%）は、ソフトウェアとシステムの中断を手動のチェック／検査やインシデントチケット、苦情によって最初に検知していると回答しました。

**標準以下の IT パフォーマンス**

IT パフォーマンスには改善の余地があります。

インドの回答者では、自社の IT パフォーマンスが十分である(現状のパフォーマンスの改善は必要ない）との回答は 35% のみでした。

ほぼ半数（48%）が、複数ツールを通じて最初にソフトウェアとシステムの中断止を検知しており、また 31% は、いまだに手動のチェック／検査やインシデントチケット、苦情によって最初に検知していると回答しました。それらの中断を、単一のオブザーバビリティプラットフォームを通じて検知しているとの回答は、21% のみでした。

**開発者の自信**

オブザーバビリティのニーズを促進する要因は、開発者の自信とリスクの低減でした。

インドの半数以上（56%）の回答者が、オブザーバビリティのニーズを促進する主要な戦略として、セキュリティ、ガバナンス、リスク、コンプライアンスへのさらなる注力と回答しました。

さらに、半数以上（51%）が、アプリケーション／システムのレジリエンスに対する開発者の自信、次いで顧客に影響を及ぼす前のプロアクティブな問題の検知（44%）が、オブザーバビリティデプロイメントの主な利点であると回答しました。

DevOps と AI

DevOps と AI が注目を集めています。

インドの回答者の半数近く（44%）が、オブザーバビリティを DevOps への組織的な IT 移行の支援に適用すると回答しました。

また 54% が、自社組織において今後 3 年間で AI 向けのオブザーバビリティが必要になると予測しました。いっぽう 53% が、自社組織において今後 3 年間で IoT 向けのオブザーバビリティが必要になると予測しました。

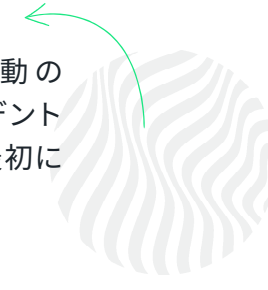
**今後のオブザーバビリティ計画**

インドの回答者は、来年に Kubernetes 監視と ML モデルパフォーマンス監視をデプロイ予定であるとの回答がもっとも多く（いずれも 44%）、次いでディストリビューティッド（分散）トレーシング（42%）、AIOps（40%）、外形監視（38%）、モバイル監視（35%）が多い傾向にありました。

大多数が、2025 年までにほとんどのオブザーバビリティ性能（83 ～ 97%）を得るだろうと予測しています。また、彼らはアジア太平洋地域の他の国と比べて予算の増額が顕著で、70% が来年のオブザーバビリティ予算を増額、13% が現状維持、17% が減額予定であると回答しました。

**31%**

**が、いまだに障害を手動のチェック／検査やインシデントチケット、苦情によって最初に検知**



# アジア太平洋

## 日本

アジア太平洋地域の他の国と比較して、ツールの分散がもっとも顕著に見られたのが日本の調査対象者でした。半数以上（52%）が単一の連結プラットフォームを望むとしながらも、4分の3がオブザーバビリティ戦略の一環として5～8のツールを習慣的に使用していました。しかし同時に、彼らはアジア太平洋地域でもっとも少ない数の性能をデプロイ済みでした。ほぼ3分の1（30%）が、オブザーバビリティをコンテナ化とサーバーレス環境の管理に使用すると回答し、これをオブザーバビリティのもっとも一般的な使用事例として挙げたのはアジア太平洋で日本のみでした。

**コンテナ化とサーバーレス**
コンテナ化とサーバーレスが、日本の回答者にとって主要な優先事項でした。

ほぼ3分の1（30%）が、オブザーバビリティのもっとも一般的な使用事例として、コンテナ化とサーバーレス環境の管理への使用を挙げました。

2番目に一般的な使用事例は、主要なレガシーアプリケーションのクラウド移行のリスク最小化でした（27%）。

オブザーバビリティのデプロイメントにより実現される主な利点は、ソフトウェアの市場投入の迅速化（36%）、次いでカスタマーエクスペリエンスの向上（34%）、顧客に影響を及ぼす前のプロアクティブな問題の検知（32%）でした。

**オブザーバビリティの利点の理解の低さ**
オブザーバビリティの威力については、日本の組織に周知する余地があります。

日本の回答者のほぼ4分の1（24%）が、自社組織のフルスタックオブザーバビリティの優先／実現を阻む主な課題として、自社のITのパフォーマンスは十分だとする利点の理解不足を挙げました。

この結果は、フルスタックオブザーバビリティの価値と威力について日本市場を教育する機会があることを示唆しています。

**ツールの分散**
単一の、連結プラットフォームを好む傾向にもかかわらず、ツールの分散は顕著でした。

日本の回答者の半数以上（52%）が、単一の連結プラットフォームを望むとしながらも、4分の3はオブザーバビリティ戦略の一環として5～8のツールを習慣的に使用していました。

**今後のオブザーバビリティ計画**
日本の回答者は、来年にAPMをデプロイ予定であるとの回答がもっとも多く（50%）、次いでMLモデルパフォーマンス監視とネットワーク監視（それぞれ42%）、ログ管理とカスタムダッシュボード（それぞれ41%）が多い傾向にありました。

大多数が、2025年までにほとんどのオブザーバビリティ性能（89～95%）を得るだろうと予測しています。予算については、47%が来年のオブザーバビリティ予算を増額、16%が現状維持、38%が減額予定と回答しました。

**75%**
が、オブザーバビリティ戦略の一環として5～8の監視ツールを使用

# ヨーロッパ

ヨーロッパでは、「一般データ保護規則（GDPR）」や「決済サービス指令（PSD2）」など、データとソフトウェアに関する新たな規制が導入されています。そのため、本調査が対象とするヨーロッパの 4 カ国すべて（フランス、ドイツ、アイルランド、イギリス）の回答者が、オブザーバビリティの促進要因としてセキュリティ、リスク、コンプライアンスを挙げているのは当然のことと言えます。ヨーロッパの回答者は、他の地域に比べてオブザーバビリティの実践の成熟度が低いとされるものの、来年のオブザーバビリティ予算を増額し、今後 3 年間でより多くの性能のデプロイを予定しています。

**フルスタックオブザーバビリティへ、徐々に移行**

他の地域に比べ、デプロイ済みの性能はもっとも少なく、本レポートの定義によるフルスタックオブザーバビリティの実現（21%）、本レポートの定義による成熟したオブザーバビリティの実践（4%）、また SDLC の全段階での拡張的または完全なオブザーバビリティの使用はもっとも少ない傾向にありました。また、すでにオブザーバビリティを優先／実現しているとの回答もやや少ない傾向にありました（2%）。統合されたテレメトリデータ（51%）、単一のダッシュボードソリューションに可視化されたテレメトリデータ（67%）を持つ傾向は高く、自社システムのインストゥルメンテーションが不十分であるとの回答はやや少ない傾向にありました（22%）。

**インシデント対応への注目**

週 1 回以上の稼働停止がもっとも多く発生しているいっぽうで、それらの検知と解決はかなり速く処理していました。実際、彼らは 30 分未満での稼働停止の解決がもっとも多い傾向にありました。また、オブザーバビリティのデプロイメントの結果として、アップタイムと信頼性の向上（32%）、カスタマーに影響を及ぼす前のプロアクティブな問題の検知（28%）との回答がもっとも少ない傾向にありました。しかし、オブザーバビリティを、どちらかというとインシデント対応／予防強化とみなすことがもっとも多い傾向にありました（52%）。

**野心的なデプロイメント計画だが、予算に見合うか？**

他の地域に比べ、IT 予算のオブザーバビリティツールへの配分が少ない傾向にあり（10% 未満がもっとも多数）、来年の予算増額を予定しているとの回答はもっとも少ない傾向にありましたが（45%）、デプロイメントの予定については野心的でした。フルスタックオブザーバビリティの優先／実現の課題として、予算不足（29%）との回答がやや多い傾向にありました。

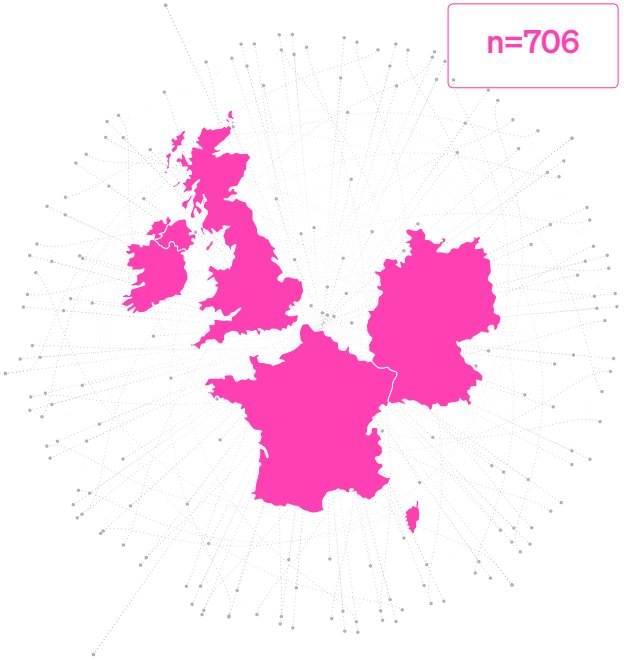
**国別のハイライト**

調査対象のヨーロッパ各国の、オブザーバビリティの重要ポイントのまとめは以下の通りです。

**フランス** 🇫🇷は、セキュリティ、オープンソース、マルチクラウド、IoT のニーズにもとづくオブザーバビリティ強化に注力

**ドイツ** 🇩🇪は、オブザーバビリティをクラウドリソースの使用と支出の最適化と DX の取り組みの支援に適用

**アイルランド** 🇮🇪と**イギリス**🇬🇧は、デプロイ済みのオブザーバビリティ性能の数は高いものの、コストの高さと予算不足に苦慮



# ヨーロッパ

## フランス

全般的に、フランスの調査対象者は、多くのオブザーバビリティの利点を実感しているとの結果が示されました。アップタイムと信頼性の向上（37%）、カスタマーエクスペリエンスの向上（35%）、アプリケーション／システムのレジリエンスに対する開発者の自信（32%）、運用効率の向上（31%）などが挙げられています。30% 以上が、オブザーバビリティは、私見の打破、チーム間の連携、ワークライフバランスの改善という点で開発者／エンジニアの生活の向上に役立つと回答しました。4 分の 3（74%）が、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考えていました。オブザーバビリティへの抵抗は少なく（15% 以下）、技術に特化していない最高幹部によるオブザーバビリティへの強い支持がもっとも多い傾向にありました（34%）。

**頻繁な稼働停止と MTTD ／ MTTR の遅さ**

フランスの回答者は、頻繁な稼働停止（最大 78% が週 1 回以上、また最大 29% が 1 日 1 回以上）を報告しています。それらの稼働停止の検知と解決に関しては、最大 62% が 30 分超の MTTD、最大 66% が 30 分超の MTTR と回答しました。これらの結果にもかかわらず、31% が自社の IT パフォーマンスは十分であると考えていました。

しかし、フルスタックオブザーバビリティがある（本レポートでの定義による）、またすでに自社組織がオブザーバビリティを優先／実現しているとした回答者では、稼働停止の少なさと MTTD ／ MTTR の短さが顕著でした。実際、52% がオブザーバビリティをインシデント対応／予防強化のための要素であると示唆しました。また、31% がオブザーバビリティによりサービス中断とビジネスリスクが低減したと回答しました（成熟したオブザーバビリティの実践におけるもっとも重要な特性のトップ回答）。

**ツールの分散**

フランスの回答者のほとんど（95%）が、オブザーバビリティのニーズに複数のツールを使用していると回答しました（79% が 4 ～ 8 のツールを使用）。43% が単一の連結オブザーバビリティプラットフォームを好むと回答したにもかかわらず、単一のツールを使用しているのはわずか 2% でした。

加えて 48% が、自社の IT チームは複数の監視ツールを通じて中断を最初に検知すると回答しました。4 分の 1 以上が、オブザーバビリティの主な利点は IT ツールの統合であるとし（29%）、監視ツールが多すぎることがフルスタックオブザーバビリティの優先／実現を阻んでいると回答しました（26%）。

このツールの分散が、彼らの報告する頻繁な稼働停止と、その検知／解決に時間がかかることの原因である可能性があります。

**技術スタック全体が監視／観察されていない**

フランスのほぼ 3 分の 2（64%）の回答者が、4 ～ 8 の性能をデプロイ済みでした。調査を行った他の多くの国と比べて、アラート、データベース監視、インフラストラクチャ監視、ログ管理、セキュリティ監視、外形監視をデプロイしているとの回答が少ない傾向にありました。

すでにフルスタックオブザーバビリティを優先／実現しているとの回答は 2% にとどまり、本レポートの定義にもとづくフルスタックオブザーバビリティを実現していたのは 18% でした。本レポートにもとづく成熟したオブザーバビリティの実践を行っているのは 3% のみでした。

**今後のオブザーバビリティ計画と傾向**

今後のデプロイメント計画を支援するため、69% が来年のオブザーバビリティ予算の増額または維持を予定していました。

オブザーバビリティのニーズを促進するための最優先事項は、セキュリティ、ガバナンス、リスク、コンプライアンスへのさらなる注力（44%）、次いでオープンソース技術の導入とマルチクラウド環境への統合が拮抗していました（いずれも 43%）。ヨーロッパの他の国と比べ、フランスの回答者のみが、オブザーバビリティのニーズの促進要因として上位 3 位にオープンソース技術を選択しました。

また、IoT デバイスの監視を不動産の完全な監視につなげる（33%）という回答も、監視のユースケースのトップとして選ばれています。加えて 43% が、自社組織において今後 3 年間で IoT 向けのオブザーバビリティがもっとも必要であると予測しました。

**43%**

**が、自社組織は今後 3 年間で IoT 向けのオブザーバビリティがもっとも必要であると予測**

# ヨーロッパ

## 🇩🇪 ドイツ

ドイツの調査対象者は、頻繁な稼働停止と MTTD ／ MTTR の遅さ、データとツールの分散を経験しているものの、オブザーバビリティのビジネス上の利点を明確に実感しており、特に技術に特化していない最高幹部からの高いレベルの支持がありました。本レポートの定義にもとづくまた、フルスタックオブザーバビリティを優先／実現しているとの回答はわずか 3% だったいっぽうで、2025 年までにほとんどの性能のデプロイを予定していました。

**頻繁な稼働停止と MTTD ／ MTTR の遅さ**

ドイツの回答者は、調査を行ったヨーロッパの国々でもっとも頻繁な稼働停止（最大 82% が週 1 回以上、最大 33% が 1 日 1 回以上）を経験していました。

それらの稼働停止の検知と解決に関しては、最大 50% が 30 分超の MTTD、最大 51% が 30 分超の MTTR と回答しました。

これらの結果にもかかわらず、23% が自社の IT パフォーマンスは十分であると考えていました。

しかし、フルスタックオブザーバビリティを実現している（本レポートでの定義による）、またすでに自社組織はオブザーバビリティを優先／実現しているとした回答者は、稼働停止が少なく、MTTD ／ MTTR が短いという結果になりました。

実際、51% がオブザーバビリティをインシデント対応／予防強化のための要素であると示唆し、31% がオブザーバビリティによりサービス中断とビジネスリスクが低減したと回答しました。

**データとツールの分散**

ドイツの回答者の 4 分の 1 以上が、自社組織のテレメトリデータはよりサイロ化しており、多種からなる技術スタックとデータのサイロ化がフルスタックオブザーバビリティの優先／実現を阻んでいると回答しました。

また、ツールの分散も一般的でした。4 分 3 が、オブザーバビリティのニーズに 5 つ以上のツールを使用していると回答しました。42% が単一の連結プラットフォームが好ましいと回答し、29% が IT ツールの統合がオブザーバビリティの主な利点であると回答したにもかかわらず、単一のオブザーバビリティツールを使用しているのは 2% のみでした。

5 分の 2 が、自社の IT チームが複数の監視ツールを通じてソフトウェアやシステムの中断を最初に検知すると回答しました。単一のオブザーバビリティプラットフォームで中断を最初に検知すると回答したのは 21% のみでした。また、4 分の 1 以上が、オブザーバビリティの主な利点は IT ツールの統合であると考え（29%）、監視ツールが多すぎることがフルスタックオブザーバビリティの優先／実現を阻んでいると回答しました（27%）。

**ビジネス上の利点**

ドイツの回答者の 30% 以上が、オブザーバビリティを、クラウドリソースの使用と支出の最適化と DX の取り組みの支援に適用していると回答しました。

また 30% 以上が、運用効率の向上と、アップタイムと信頼性の向上を報告しています。実際、79% が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しました。ほぼ 3 分の 1（31%）が、オブザーバビリティは開発者／エンジニアの業務を楽にすると回答しました。

すべてのグループで、オブザーバビリティへの高い支持がありました。特に 45% が、技術に特化していない最高幹部が他のどのグループよりもオブザーバビリティを強く支持していると回答しました。

**今後のオブザーバビリティ計画**

ドイツの 40% 以上の回答者が、オブザーバビリティのニーズを促進する戦略と傾向は、セキュリティ、ガバナンス、リスク、コンプライアンスへのさらなる注力、カスタマーエクスペリエンスの管理、マルチクラウド環境への統合、クラウドネイティブなアプリケーションアーキテクチャーの開発、より速いソフトウェアリリースサイクルの優先と回答しました。

大多数（85%）が、来年に 5 つ以上の追加的な性能をデプロイ予定で、42% が自社のオブザーバビリティ計画の支援のため来年の予算増額を予定していました。

今後 3 年間で、IoT（41%）、AI（40%）、5G（32%）、ブロックチェーン（27%）などの新興テクノロジー向けのオブザーバビリティがもっとも必要であると予測しています。

**31%**

**が、オブザーバビリティは開発者／エンジニアの業務を楽にすると回答**

# ヨーロッパ

## アイルランドとイギリス

アイルランドとイギリスの調査対象者の大多数（84%）が、5 つ以上のオブザーバビリティ性能をデプロイ済みでした。回答者の半数が、オブザーバビリティは、ソフトウェアスタックに関する判断におけるチーム間の連携強化をもたらすと回答し、42% が開発者／エンジニアの生産性の向上、35% が運用効率の改善を挙げました。

これらの有力な利点にもかかわらず、本レポートの定義によるフルスタックオブザーバビリティを実現しているのは 27% のみで、すでに優先／実現していると回答したのはわずか 2% でした。ただし、彼らは 2025 年までに 17 の性能のほとんどを獲得すると予測していました。

**ツールとデータの分断**

49% が単一の、連結プラットフォームを好むと回答したにもかかわらず、オブザーバビリティのニーズに対して単一のツールを使用しているのは、アイルランドとイギリスの回答者のわずか 2% でした。いっぽうで 3 分の 2 が、5 つ以上のツールを使用していると回答しました。加えて、38% が自社組織のデータのサイロ化を指摘し、そのうち 12% は完全にサイロ化している、17% はサイロ化と統合が約半々であると回答しました。また 29% が、そのテレメトリデータの可視化／ダッシュボード構築は多種化していると回答しました。

ほぼ 3 分の 1（30%）が JT ツールの統合をオブザーバビリティの主な利点として挙げたいっぽう、22% が多種からなる技術スタック、20% が監視ツールが多すぎてデータがサイロ化していることをフルスタックオブザーバビリティの優先／実現の主な課題に挙げました。

**サービスレベルのメトリクスの改善の余地**

使用ツール数の多さからすれば、アイルランドとイギリスの回答者の 60% が、ソフトウェアとシステムの中断を複数のツールで最初に検知すると回答し、対して単一のオブザーバビリティプラットフォームを通じて中断を最初に検知するのは 15% のみだったのも、当然のことと言えます。残りの 25% は、手動でのシステムチェック／検査や苦情、インシデントチケットを通じて最初に中断を検知すると回答しました。

稼働停止はかなり頻繁に発生しており、最大 69% が稼働停止は週 1 回以上発生すると回答しました。いっぽう、これらの稼働停止の検知はかなり速く（最大 61% が 30 分未満で稼働停止を検知と回答）、解決にはより長い時間がかかっていました（最大 62% が稼働停止の解決に 30 分超と回答）。これらの結果にもかかわらず、29% が自社の IT パフォーマンスは十分であると考えていました。

**支持は高いものの、コストが高く予算不足**

アイルランドとイギリスの回答者は、価格の透明性（42%）、予算に見合う価格（37%）が、オブザーバビリティツールの価格特性としてもっとも重要であると回答しました。また 39% が、予測可能な支出が、もっとも重要な請求特性であると回答しました。3 分の 1 は、フルスタックオブザーバビリティの実現の最大の障壁は予算不足であるとし、25% が価格が高すぎると回答しました。実際、63% が、IT 予算のオブザーバビリティツールへの配分は 10% 未満であると回答しています。ただし、44% が、来年の予算増額を予定していると回答しました。

これらの予算計画は、技術に特化した最高幹部の 77% と、技術に特化していない最高幹部の 70% の支持を含め、アイルランドとイギリスの全グループのオブザーバビリティへの強い支持と、71% がオブザーバビリティを中核的な事業目標の達成要因とみなしているという事実を受けてのものと思われます。

**今後のオブザーバビリティ計画**

ヨーロッパの他の国やその他地域と同様に、アイルランドとイギリスでのオブザーバビリティの最大の促進要因は、セキュリティ、ガバナンス、リスク、コンプライアンスへのさらなる注力です。実際、アイルランドとイギリスの回答者の 60% は、すでにセキュリティ監視をデプロイしており、大多数（96%）が 2025 年までにデプロイ予定であると回答しています。

来年には、ディストリビューティッド（分散）トレーシング（42%）、AIOps（40%）、ML モデルパフォーマンス監視（37%）をはじめ、62% が 5 つ以上の追加的なオブザーバビリティ性能をデプロイ予定であると回答しました。

今後 3 年間で、AI（45%）、IoT（44%）、5G（30%）などの新興テクノロジー向けのオブザーバビリティがもっとも必要であると予測しています。

**50%** が、オブザーバビリティによりソフトウェアスタックに関する判断におけるチーム間の協力体制が強化されたと回答

# 北米

成長と安定性は、多くのビジネスリーダーにとって最重要事項です。北米地域のカナダと米国では76%がオブザーバビリティを中核的な事業目標の達成要因とみなし、これを達成する媒体として、オブザーバビリティのデプロイメントの最大の利点はアップタイムと信頼性の向上であると考えていました。またこれが、全グループからの高いレベルの支持と、北米の回答者が来年のオブザーバビリティ予算を増額する理由でもあると思われます。

**デプロイメントと予算計画**

約4分の3（76%）が、1～10のオブザーバビリティ性能をデプロイしていると回答しました。来年には、70%が5つ以上の追加的な性能のデプロイを予定していました。他の地域と比べ、彼らは来年の予算増額の予定がもっとも多い傾向にありました（63%、また25%を超える増額予定が18%）。

**フルスタックオブザーバビリティの実現**

北米の回答者は、SDLCのデプロイ（74%）および運用（81%）段階での拡張的または完全なオブザーバビリティの使用がもっとも多い傾向にありました。しかし、本レポートの定義によるフルスタックオブザーバビリティを実現しているのは31%にとどまり、すでにフルスタックオブザーバビリティを優先／実現していると回答したのはわずか3%でした。ほぼ4分1（24%）が、フルスタックオブザーバビリティの優先／実現の主な課題として、監視ツールが多すぎることを挙げました。実際、大多数が複数ツールを使用すると回答し、そのうち73%が5つ以上のツール使用を回答しました。43%が単一の連結プラットフォームを好むと回答したものの、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3%でした。統合されたテレメトリデータを持つ傾向がもっとも多く（56%）、そのテレメトリデータは単一のダッシュボードソリューションに可視化されていました（74%）。

**サービスレベルのメトリクスの改善**

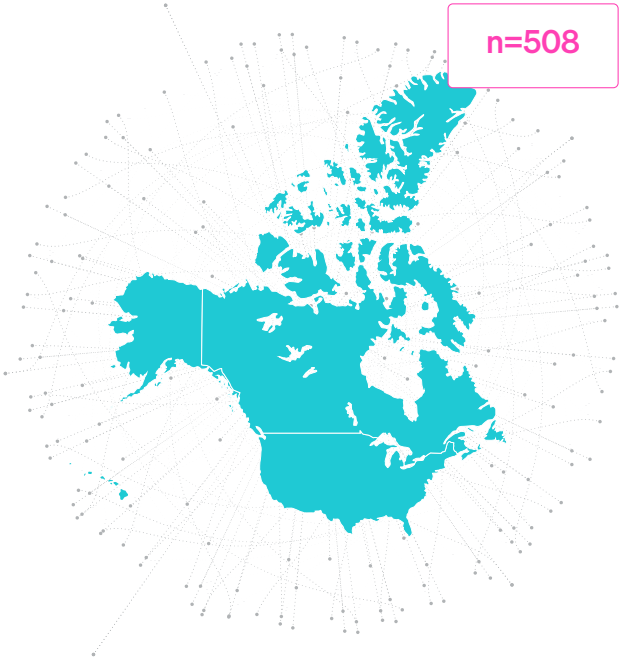
4分の1が、自社のITチームは、単一のオブザーバビリティプラットフォームを通じてソフトウェアやシステムの中断を最初に検知すると回答しました。これは他の地域と比べて最多でした。これは、彼らの稼働停止の頻度がもっとも少なく、稼働停止の30分未満での検知がもっとも多いとの報告に寄与している可能性があります。ただし、40%がビジネスインパクトの大きい稼働停止が週1回以上発生し、その稼働停止の30%近くが解決に60分超かかると回答しました。にもかかわらず、31%が自社のITパフォーマンスは十分であると回答しています。5分の2が、オブザーバビリティツールに関するスタッフのトレーニングが自社組織のMTTR短縮にもっとも役立つと回答し、これは他の地域に比べて最多でした。

**国別のハイライト**

調査対象の北米各国の、オブザーバビリティの重要ポイントのまとめは以下の通りです。

**カナダ** 🇨🇦は、オブザーバビリティを開発者／エンジニアの生産性向上と連携強化の促進要因とみなし、大多数が来年に最大12の追加的性能のデプロイを予定

**米国** 🇺🇸は、明白なビジネスオペレーションの利点を感じ、来年のオブザーバビリティの予算増額を予定



# 北米

## カナダ

カナダでは、オブザーバビリティは開発者／エンジニアの生産性向上とイノベーションに明らかな効果があり、すべてのロールでの支持がありました。しかし、組織的な課題、ツールの分散、予算不足により、フルスタックオブザーバビリティの優先／実現が阻まれていました。実際、フルスタックオブザーバビリティが優先／実現されていると回答したのは 7% のみ、本レポートでの定義による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 29% にとどまりました。

カナダの回答者は、オブザーバビリティを今後のテクノロジーの促進要因とみなし、今後 3 年間で大多数の性能をデプロイする予定でした。これらの予定を支援すべく、76% が、来年のオブザーバビリティ予算の増額または現状維持を予定しています。

**強い支持と予算増額の目標**

カナダの大多数（85%）の回答者は、自社組織の技術に特化した最高幹部がオブザーバビリティを支持していると回答しました。加えて、76% が開発者の支持も挙げました。

これらの高いレベルの支持が、来年のオブザーバビリティ予算がある程度、または大幅に増額予定であるとの 54% の回答に寄与していると思われます。

**組織とツールの分散化の課題**

フルスタックオブザーバビリティの多くの利点にもかかわらず、カナダの回答者はその優先／実現の課題として、戦略（31%）、専門的人材（27%）、スキル（20%）の欠如を指摘しました。

また、4 分の 1 は監視ツールが多すぎることを課題として挙げました。ほぼ 4 分の 3（74%）が 5 つ以上、46% は 7 つ以上の自社組織でのツール使用を回答しました。興味深いことに、41% が単一の、連結プラットフォームを好むとしたにもかかわらず、単一ツールを使用しているとの回答はありませんでした。

**開発者／エンジニアの生産性向上、連携強化、イノベーション**

カナダの半数以上（51%）の回答者が、オブザーバビリティは開発者の時間をリアクティブな作業からプロアクティブな業務へ移行するのに役立つと回答し、いっぽうで 46% は、ソフトウェアスタックに関する判断におけるチーム間の連携強化を挙げました。

半数近く（46%）が、オブザーバビリティによりアップタイムと信頼性が改善する、また 40% が運用効率が改善し、カスタマーエクスペリエンスが向上すると回答しました。

また、オブザーバビリティはチーム間の連携を可能にし（40%）、イノベーションを促進する（36%）ことで、開発者とエンジニアの生活向上に寄与すると回答しました。

**今後のオブザーバビリティ計画**

カナダの回答者の半数以上（56%）が、自社組織におけるオブザーバビリティのニーズの促進要因は、セキュリティ、ガバナンス、リスク、コンプライアンスへのさらなる注力であると回答しました。また、クラウドネイティブなアプリケーションアーキテクチャーの開発（48%）、マルチクラウド環境への統合（46%）も挙げています。

今後については、大多数が来年に 1 ～ 12 の追加的な性能のデプロイを予定し、予定していないのは 9% のみでした。今後 3 年間で IoT（48%）、AI（47%）、ブロックチェーン（36%）、5G（28%）などの新興テクノロジー向けのオブザーバビリティがもっとも必要であると予測しています。

**76%**

**が、来年のオブザーバビリティ予算の増額または現状維持を予定**

# 北米

## 🇺🇸 米国

米国では、その他の地域とほぼ同様に、オブザーバビリティのツールと実践が分断されており、4 分の 3 近くが 5 つ以上のオブザーバビリティツールを使用していました。この分断が、彼らのサービスレベルのメトリクスに悪影響を与えているように思われます。

オブザーバビリティへの強い支持にもかかわらず、すでにフルスタックオブザーバビリティを優先／実現していると回答した米国の回答者は 4% に過ぎず、いっぽうで本レポートの定義による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 31% でした。しかし、今後 3 年間で、米国の回答者は AI、IoT、5G などの新興テクノロジーを支援するオブザーバビリティに注目していくと回答しています。

**データとツールの分散**

米国の回答者のほぼ 4 分の 3（73%）が、5 つ以上のオブザーバビリティツールを使用していると回答しました。43% が単一の、連結プラットフォームを好むと回答したにもかかわらず、単一のツールを使用しているのは 3% のみでした。当然のことながら、24% が、監視ツールが多すぎることが自社組織のフルスタックオブザーバビリティの優先／実現を阻んでいると回答しました。

自社組織のテレメトリデータが完全に統合されていると答えたのは 8% のみで、すべてのテレメトリデータが単一のダッシュボードソリューションに可視化されているとの回答は 14% のみでした。

**頻繁な稼働停止と遅い MTTD ／ MTTR**

米国のほぼ半数（48%）の回答者が、カスタマーやエンドユーザーに影響するビジネスインパクトの大きい稼働停止を週 1 回以上経験していました。さらに、55% がこれらの稼働停止の検知に 30 分を越える時間がかかり、63% がその解決に 30 分超の時間がかかると回答しました。これらの結果にもかかわらず、31% が自社の IT パフォーマンスは十分であると考えていました。

また 43% が、IT チームはソフトウェアとシステムの中断の検知のため、主に複数のツールを使用すると回答しました。さらに 32% が、IT チームは主に手動のチェック／検査やインシデントチケット、苦情に頼っていると回答しました。

**明白なビジネスオペレーションの利点と支持**

米国の 4 分の 3 以上の回答者が、最高幹部がオブザーバビリティを支持していると回答しました（技術に特化した最高幹部の 79%、特化していない幹部の 77%）。

オブザーバビリティがどのような点で開発者／エンジニアの生活向上にもっとも役立つかとの問いには、35% が生産性の向上とチーム間の連携強化、30% がイノベーションの促進、26% が開発者／エンジニアの業務を楽にすると回答しました。

約半数（49%）が、オブザーバビリティを中核的な事業目標の達成要因とみなしていました。そのため、65% が来年にオブザーバビリティツールの予算増額を予定しているのは、当然のことと言えます。

**今後のオブザーバビリティ計画**

自社組織においてオブザーバビリティのニーズを促進する戦略とトレンドが何かについては、米国の回答者の半数以上が、セキュリティ、ガバナンス、リスク、コンプライアンスへのさらなる注力、またカスタマーエクスペリエンス管理への注力、クラウドネイティブなアプリケーションアーキテクチャーの開発を挙げました。

大多数が来年に 1～14 の追加的な性能のデプロイを予定しており、予定していないのは 8% のみでした。

新興テクノロジーについては、半数以上（53%）が、今後 3 年間で AI 向けのオブザーバビリティがもっとも必要になるとし、次いで IoT（44%）、5G（35%）、ブロックチェーン（34%）、Web3（18%）と回答しました。

**35%**

**が、オブザーバビリティは生産性を向上し、チーム間の連携を強化すると回答**

# 会社概要

New Relic は、オブザーバビリティのリーダーとして、優れたソフトウェアの計画、構築、デプロイ、運用に対するデータ駆動型のアプローチによりエンジニアを支援しています。New Relic は、メトリクス、イベント、ログ、トレースからなる全テレメトリが集約された唯一の統合データプラットフォームを、強力なフルスタック分析ツールと組み合わせて提供し、意見ではなくデータにもとづくエンジニアのベストパフォーマンスを可能にします。

直感的かつ予測可能な、業界初の従量課金制の価格設定にもとづき提供される New Relic は、計画サイクルタイム、変更失敗率、リリース頻度、MTTR の改善を促し、エンジニアにさらなる費用対効果をもたらします。これにより、世界をリードする大企業や成長著しいスタートアップ企業のアップタイムと信頼性、運用効率の向上を助け、イノベーションと成長を加速させる優れたカスタマーエクスペリエンスの創出を支援します。

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、年間の IT 支出が 1 兆ドル以上であり、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包括的な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 のプラットフォームについて知る