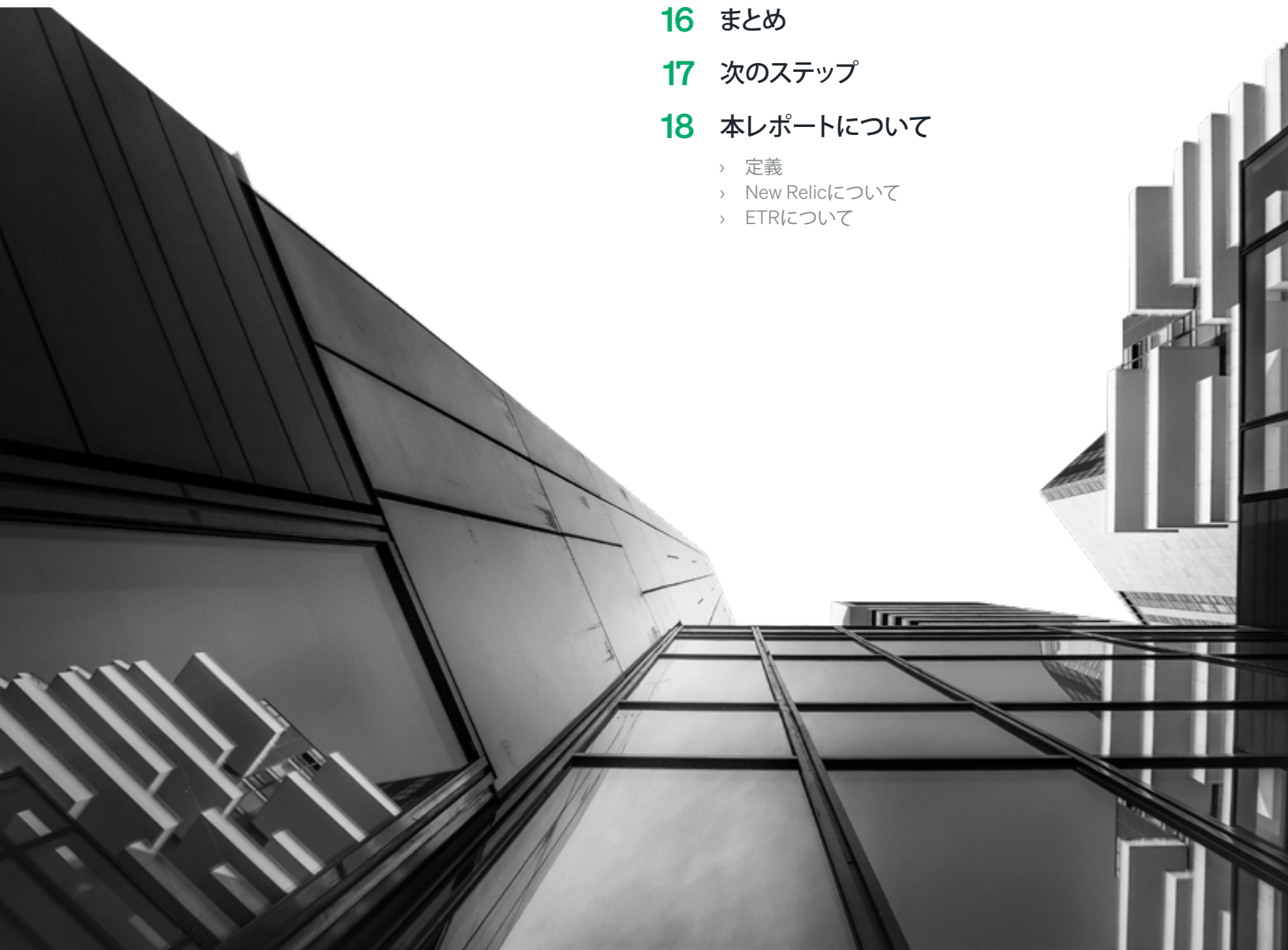


# 金融サービスと保険業界における オブザーバビリティの現状

オブザーバビリティの導入、およびビジネス価値に関する考察と分析

# 目次

- 03 概要
- 04 オブザーバビリティの導入を促進するトレンド
- 06 導入済みのオブザーバビリティ機能
- 08 金融業界における監視ツール数  
および優先順位
- 10 システム停止頻度、ダウンタイムとシステム停止  
にかかるコスト
- 12 金融業界におけるオブザーバビリティの支出
- 13 オブザーバビリティのビジネス価値
- 15 金融サービスと保険業界におけるオブザーバ  
ビリティの未来
- 16 まとめ
- 17 次のステップ
- 18 本レポートについて
  - › 定義
  - › New Relicについて
  - › ETRについて





# 概要

金融業界は、顧客からのより高い期待—高度なデジタルインタラクションやサービスへのアクセス、物理的なサービス離れなど—を通し、驚くべき変革に直面しています。金融機関離れが進むなか、Apple Pay、Revolut、ネット銀行などの国内および世界的な金融サービス業界 (FSI) のプレーヤーは、モバイルデバイスなどのオンラインで取引を完了したいという利用者のニーズに応えています。これには、銀行残高の確認、モバイルでの入金、見積りりの取得、予算の追跡、請求書の支払い、購入、送金などがあります。

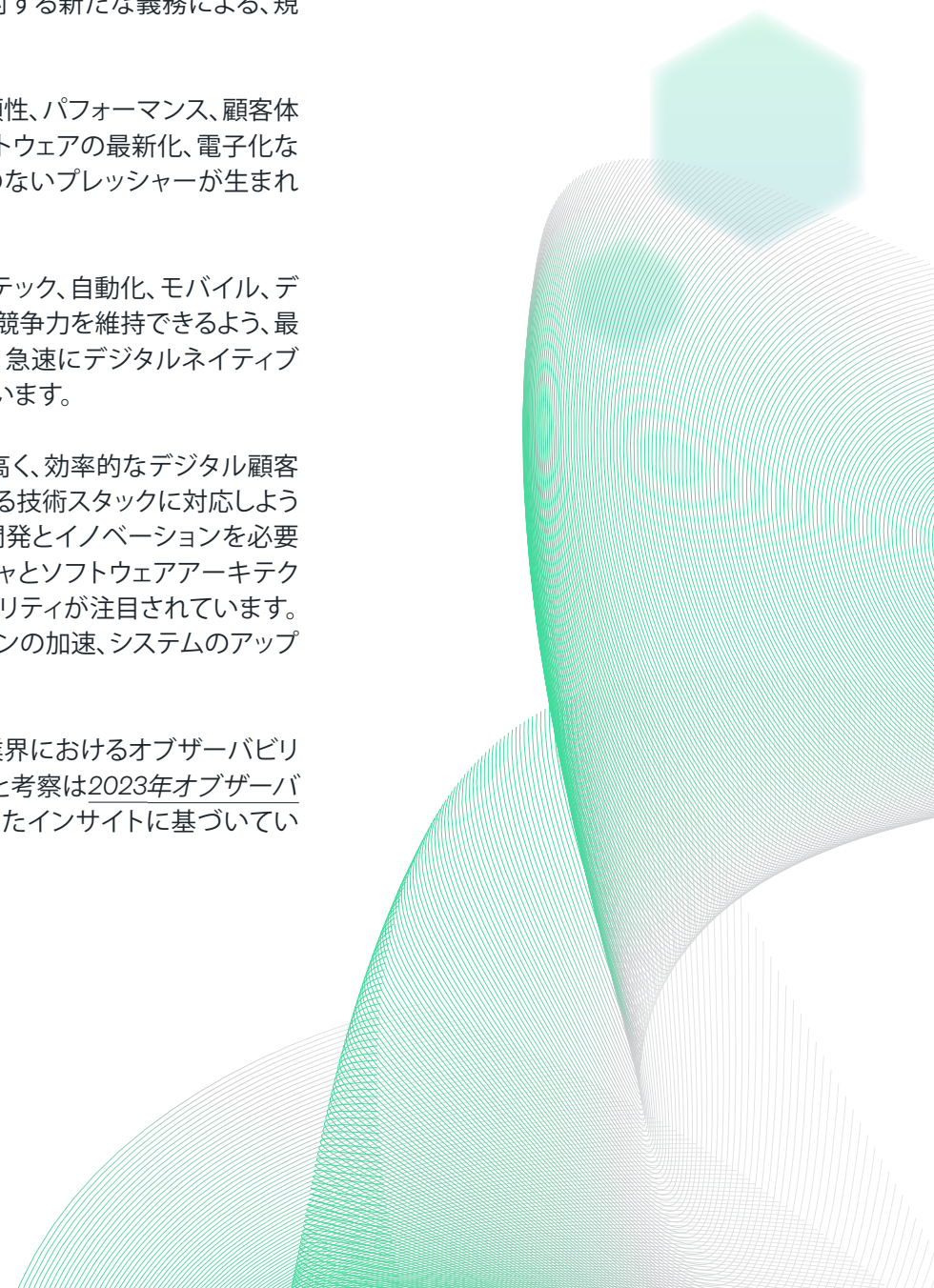
同時に、金融サービス (FSI) 組織は、デジタルオペレーショナルレジリエンス法 (DORA) などの IT およびサイバーリスク管理に対する新たな義務による、規制の強化に直面しています。

これらすべての要因により、最適な稼働時間、信頼性、パフォーマンス、顧客体験、イノベーションを実現しながら、核となるソフトウェアの最新化、電子化など、デジタルインフラストラクチャに対する前例のないプレッシャーが生まれています。

これまでの金融機関は、フィンテック、インシュアテック、自動化、モバイル、デジタルネイティブなどのトレンドが押し寄せる中、競争力を維持できるよう、最新化を目指して競っています。多くの金融機関は、急速にデジタルネイティブやデジタルファーストモデルへの移行を加速しています。

金融サービスと保険機関は、流動的で信頼性が高く、効率的なデジタル顧客体験 (DCX) の提供を目指して、ますます複雑化する技術スタックに対応しようとしています。結果として、顧客に焦点を当てた開発とイノベーションを必要な速度で確実に進めるため、インフラストラクチャとソフトウェアアーキテクチャーをリアルタイムで可視化するオブザーバビリティが注目されています。これにより、迅速で正確な意思決定、イノベーションの加速、システムのアップタイムと信頼性を向上しようとしています。

本レポートでは、金融サービス業界 (FSI) と保険業界におけるオブザーバビリティの導入とビジネス価値に着目しました。データと考察は 2023年オブザーバビリティ予測調査 より、176件の回答者から得られたインサイトに基づいています。



# オブザーバビリティ導入を促進するトレンド

クラウドへの移行とデジタルネイティブの子会社の設立は、金融機関がシステムを最新化するための最も迅速な方法と考えられています。このアプローチにより、アジャイルで革新的なサービスを迅速に市場に投入することが可能になり、核となるシステムがモダン化されることにより、その可能性を最大限に発揮することができます。

金融サービス／保険業界の組織において、オブザーバビリティの必要性を促進する主要なテクノロジー戦略とトレンドは、セキュリティ、ガバナンス、リスク、コンプライアンス重視の高まり(54%)、マルチクラウド環境への移行(43%)、GPTなどの人工知能(AI)技術の導入(40%)、クラウドネイティブのアプリケーションアーキテクチャーの開発(38%)、顧客体験マネジメント重視の強化(35%)という結果でした。業界の複雑な規制要件を考慮すると、セキュリティ、ガバナンス、リスク、コンプライアンス重視の高まり(54%)が最大の推進要因であることは自明です。

## 43%

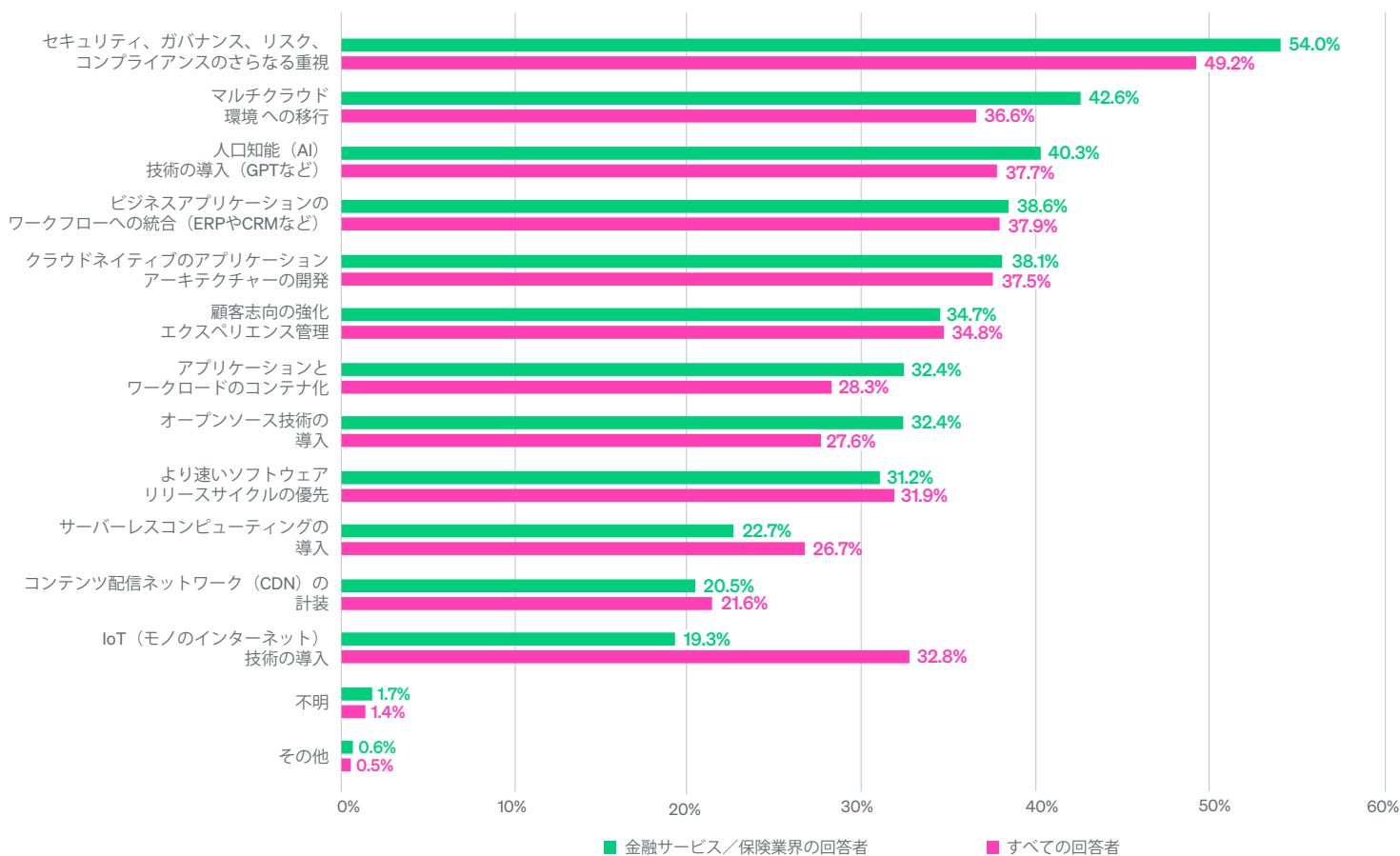
マルチクラウド環境への移行がオブザーバビリティの最大の推進要因であると回答



オブザーバビリティの導入を促進する要因の上位3項目

また、ERP やCRMなどのビジネスアプリケーションのワークフローへの統合が進んでいること(全回答者38%に対し、金融サービス/保険業界の割合は39%)や、アプリケーションとワークロードのコンテナ化(全回答者の28%に比べて金融サービスでは32%)、オープンソーステクノロジーの導入(全回答者の28%に比べて金融サービスでは32%)などの要因も明らかになっています。

しかし、金融サービス/保険業界の回答者は、モノのインターネット (IoT) の導入についてはあまり重視しておらず、回答者全体が33%で7位にランクしているのに対し、12位(19%)という結果でした。電子化が進む銀行業界ではIoTは通常関連性がないと考えられているため、この結果は理にかなっています。



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

# 導入済みの オブザーバビリティ機能

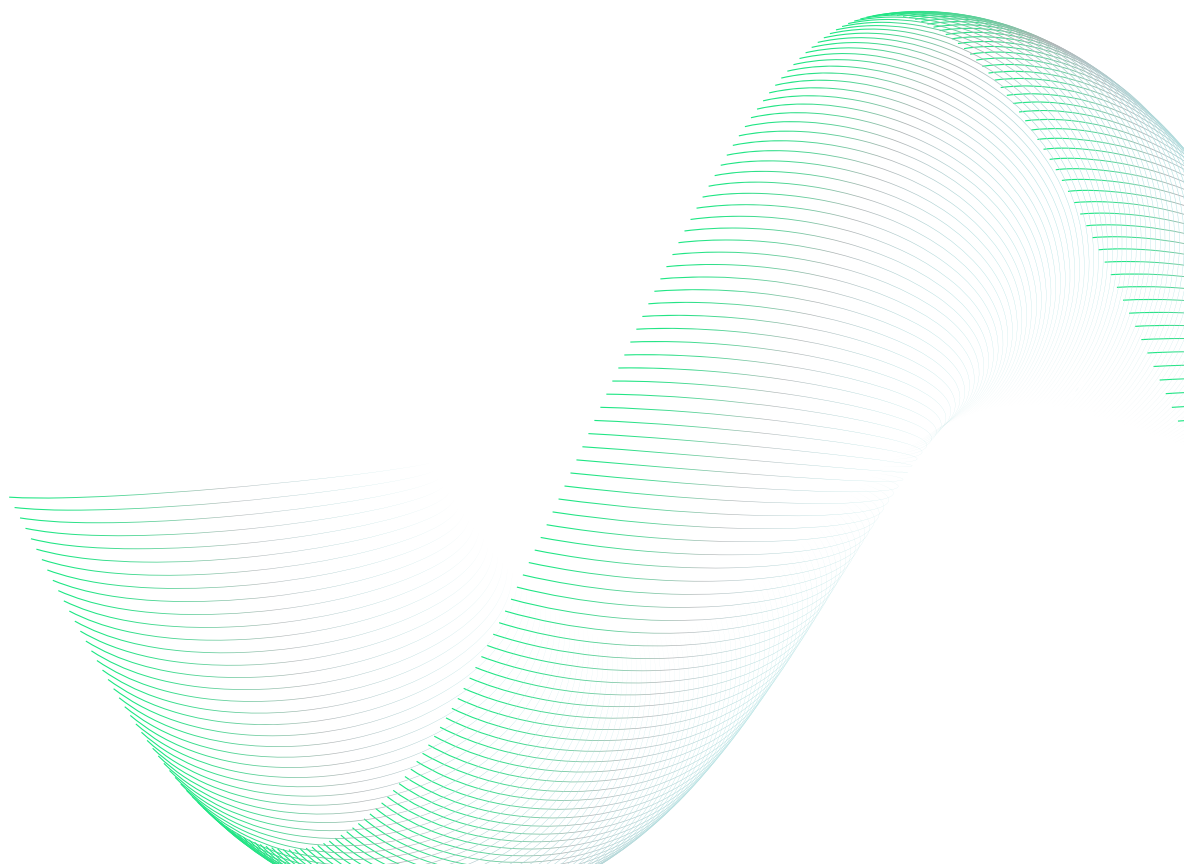
複雑な金融および保険サービスには、フルスタックのオブザーバビリティと、ミドルウェア、サービスとしてのクラウドプラットフォーム (PaaS)、および主軸となるプラットフォームとの幅広い統合が必要です。全体の33%がフルスタックのオブザーバビリティを実現しているのに対し、金融サービス／保険業界の組織では、38%がフルスタックのオブザーバビリティを実現しています。実際、金融サービス／保険業界の組織は、調査対象の17の機能のうち12機能を、全回答者よりも高い割合で導入していました。

金融サービス／保険業界の組織は、バックエンドとコアバンキングシステムの運用に不可欠な機能を、より広範囲に導入しています。たとえば、インフラストラクチャ監視 (全体の57%に比べて75%)、アプリケーションパフォーマンスの監視またはAPM (全体の50%に比べて63%)、Kubernetes (K8s) の監視 (全体の25%に比べて35%) などが挙げられます。

顧客中心のサービスと最適なDCXを作成することは、消費者との信頼とロイヤルティを構築し維持しようとする金融機関や保険機関にとって不可欠です。プロバイダの選択、アカウントの迅速な開設、または対面で完了する手続きをオンラインで開始するなど、あらゆるサービスの日常業務において、全デバイスにわたる簡単に信頼性の高い接続が期待されます。

## 38%

金融サービス／保険業界の組織はフルスタックオブザーバビリティを実現していると回答

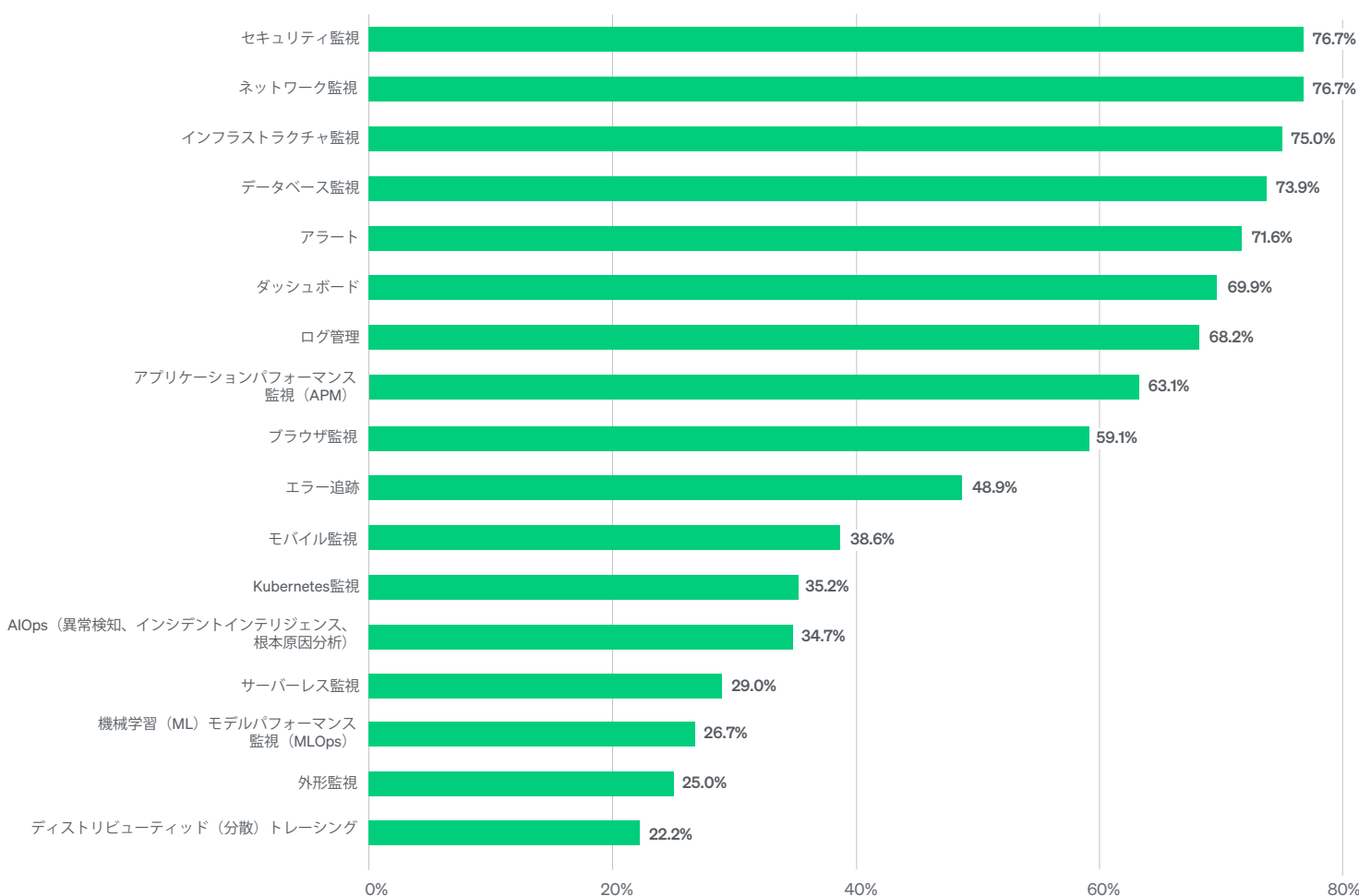


デジタルエクスペリエンス監視 (DEM) には、完璧なDCXを提供するためのパフォーマンスと信頼性の追跡および最適化が含まれます。DEMは、ブラウザ監視とモバイル監視を含むリアルユーザー監視 (RUM) と、外形監視を組み合わせたものです。

金融サービス／保険業界の組織では、ブラウザ監視 (全体の51%に比べて59%) と外形監視 (全体の24%に比べて25%) の導入率が高いことが明らかになっています。また、モバイル監視の導入率がわずかに低いこともわかりました (全体43%に比べて39%)。これは、ビジネスバンキング、プライベートバンキング、コアバンキング、トレーディング、クレジットとローン、支

払処理、企業保険、再保険、その他多くのFSI業界が、関連するモバイルアプリケーションを保有していないことが多いためと考えられます。

さらに、金融サービス／保険業界の組織の4分の3以上が、セキュリティ監視 (77%)、ネットワーク監視 (77%)、インフラストラクチャ監視 (75%) を導入していることがわかりました。データベース監視 (74%)、アラート (72%)、ダッシュボード (70%)、ログ管理 (68%) も広く導入されています。これらの各機能は、一般的に他の全業界と比較して金融サービス／保険業界の組織で多く導入されている結果となりました。



金融サービス／保険業界における、導入済みのオブザーバビリティ機能



# 金融業における監視ツール数 および優先順位

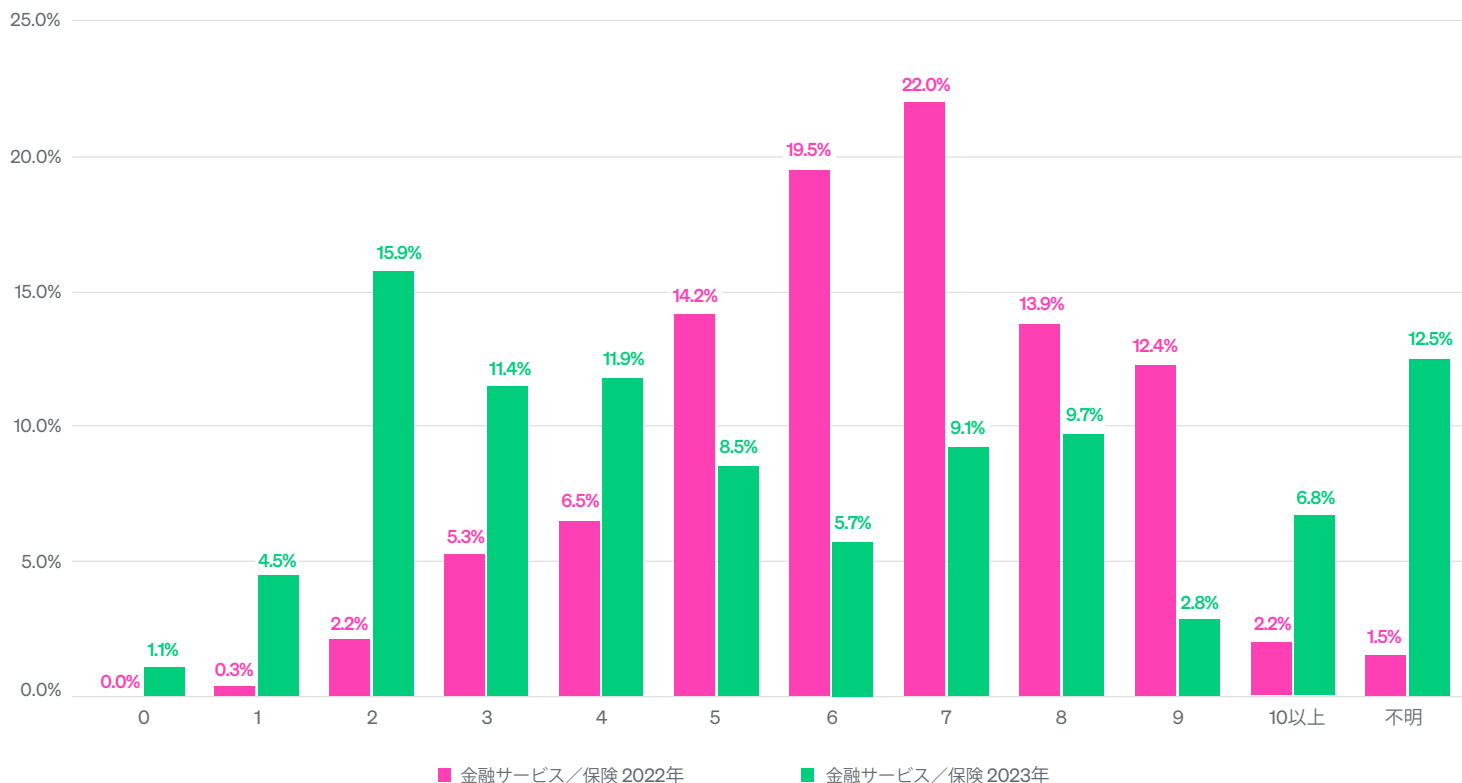
調査から、金融サービス／保険業界の組織が、本調査に含まれる17のオブザーバビリティ機能について、平均よりも少ない数の監視ツールを使用する傾向があることが明らかになっています。たとえば、平均の28%と比較して、金融サービス／保険業界では、32%が4未満のオブザーバビリティツールを使用していました。

単一のツールのみを使用している、と回答した金融サービス／保険業界の回答者の割合は、昨年から15倍に増え、0.3%から4.5%に増加しました。ただし、平均ツール数は1つ分減り、2022年の平均6ツールから2023年には5ツールとなりました。

調査から、FSIと保険業界の組織は、他の業界と比較して、技術スタックを単一の統合ビューで把握するために使用するオブザーバビリティツールの数を削減する方向にあります。

15倍 ↑

昨年以來、単一のツールを使用する金融サービス／保険業界の回答者の割合が増加



金融サービス／保険業界の組織で使用されたオブザーバビリティ機能ツール数の2022年と2023年の比較



「組織のテレメトリーデータ（メトリクス、イベント、ログ、トレース）がどのように統合されているか」の質問には、32%がより統合されている、43%がよりサイロ化されている、22%が統合とサイロ化がおおよそ半々であると回答しました。

さらに、金融サービス／保険業界の組織のITチームは、1つ以上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ことがもっとも多く（69%）、28%がシステム停止を手動によるチェック／検査や苦情、インシデントチケットによって検知していると回答しました。

しかしながら、金融サービス／保険業界では、単一の統合型プラットフォームを希望する、と答えた回答者が多数でした（52%）。また42%が、オブザーバビリティから最大の価値を得るために、今後1年間でツールを統合する予定であると回答しています。

**これまでのいくつかの役割で、私が直面した最大のミスの1つは、インフラストラクチャを監視するアプリケーション、ログを監視するアプリケーション、そしてAPM用のアプリケーションを1つずつ使用していたことでした。インシデントを調査し、複数のツールにわたる異常の原因を検出するのは煩わしく、時間の無駄でした。Pomeloを立ち上げたとき、ツールを1つにして開発者チーム全員がその特定のツールを使いこなせるようにすると決めました。」**



Juan Jose Behrand氏

Pomelo社エンジニアリングディレクター

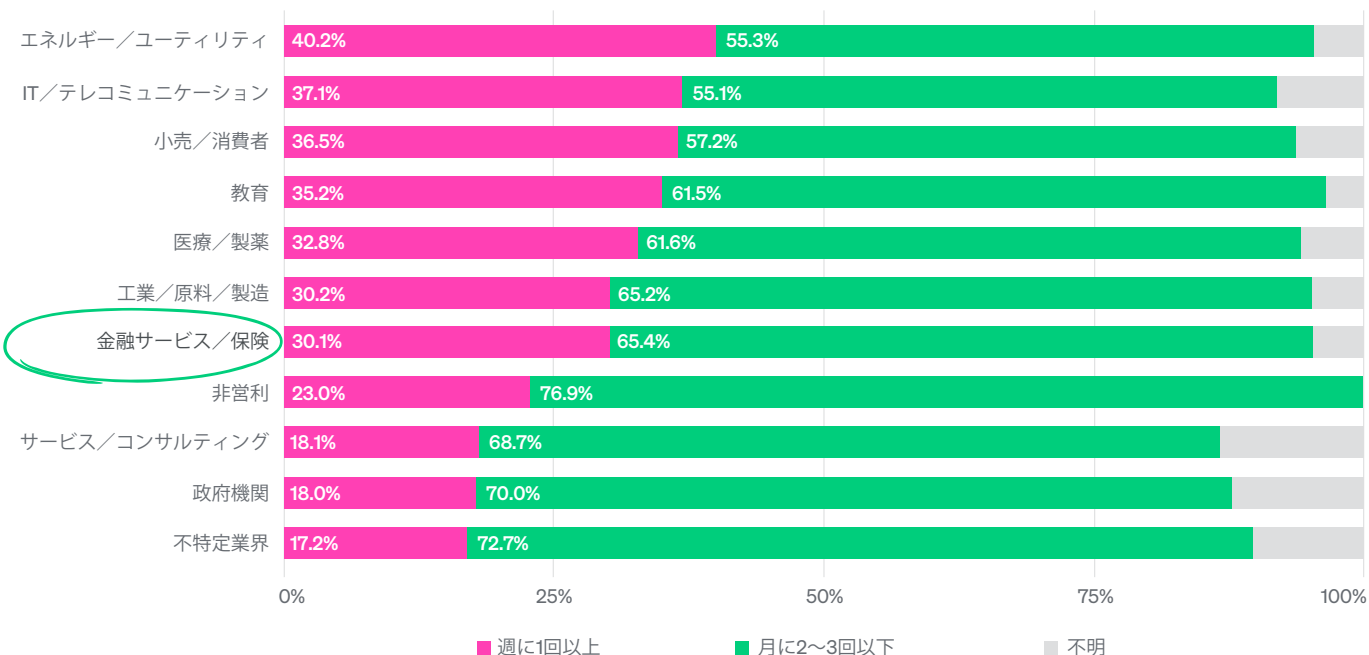
# 43%

テレメトリーデータがある程度、ほとんど、あるいは完全にサイロ化されていると回答

# システム停止の頻度、 ダウンタイムとコスト

金融サービス／保険業界の組織は、他の多くの業界に比べてビジネスインパクトの大きいシステム停止の経験が少なく、全体平均の32%に対し、30%が週1回以上発生しているという結果が出ています。

これは、金融サービス／保険業界の組織は、全業界で5番目にシステム停止の頻度が低いことを意味します。



業界別、ビジネスに影響を与えるシステムの停止頻度

ダウンタイムの合計は、システム停止の平均検出時間 (MTTD) と平均復旧時間 (MTTR) を足して算出されます。5分の2 (40%) の金融サービス／保険業界の回答者が、ビジネスインパクトの大きいシステム停止を検知するのに30分以上要すると回答し (これは平均の44%よりも低い)、66%が問題の解決に30分以上要すると回答しています。また、21%がビジネスインパクトの大きいシステム停止を検知するのに60分以上かかると回答し、36%が問題の解決に60分以上要すると回答しました。

66%

ビジネスに影響を与えるシステム停止の解決に、30分以上を要すると回答

銀行は伝統的にシステムの耐障害性が高く、基幹システムの変更やソフトウェア開発のペースは比較的遅いものでした。そのため、ビジネスインパクトの大きいシステム停止が発生すると、その障害はより複雑になる傾向があり、ビジネスへの影響が大きくなり、解決までに時間がかかります。

これはほとんどの業界で同じ状況が見られています。組織が成熟したオブザーバビリティを実践して多数のインシデントをプロアクティブに解決し、排除できるようになると、たとえ早期に検出して迅速に把握できたとしても、次には解決に時間がかかる、より複雑で予測不可能なインシデントが残されます。

ただし、MTTRが比較的高いにもかかわらず、64%の回答者は、オブザーバビリティソリューションを導入してからMTTRがある程度改善したと答えています。

特に、フルスタックオブザーバビリティを実現している金融サービス／保険業界の組織は、実現していない組織よりも、ビジネスインパクトの大きいシステム停止に対してより迅速なMTTDを報告できている傾向が強く見られています。ビジネスインパクトの大きいシステム停止について、MTTDが30分以下である、と回答した組織の半数以上（51%）、およびMTTDが5分以下である、と回答した組織の58%がフルスタックオブザーバビリティを導入している結果となりました。

金融サービス／保険業界の回答者の3分の1以上（35%）が、重要なビジネスアプリケーションのシステム停止にかかるコストはダウンタイム1時間あたり50万ドル以上と試算しています。これは平均よりも高く、他の業界と比べて全体で3番目に高く、22%が自社組織におけるそのコストは1時間あたり100万ドル以上と推定しています。

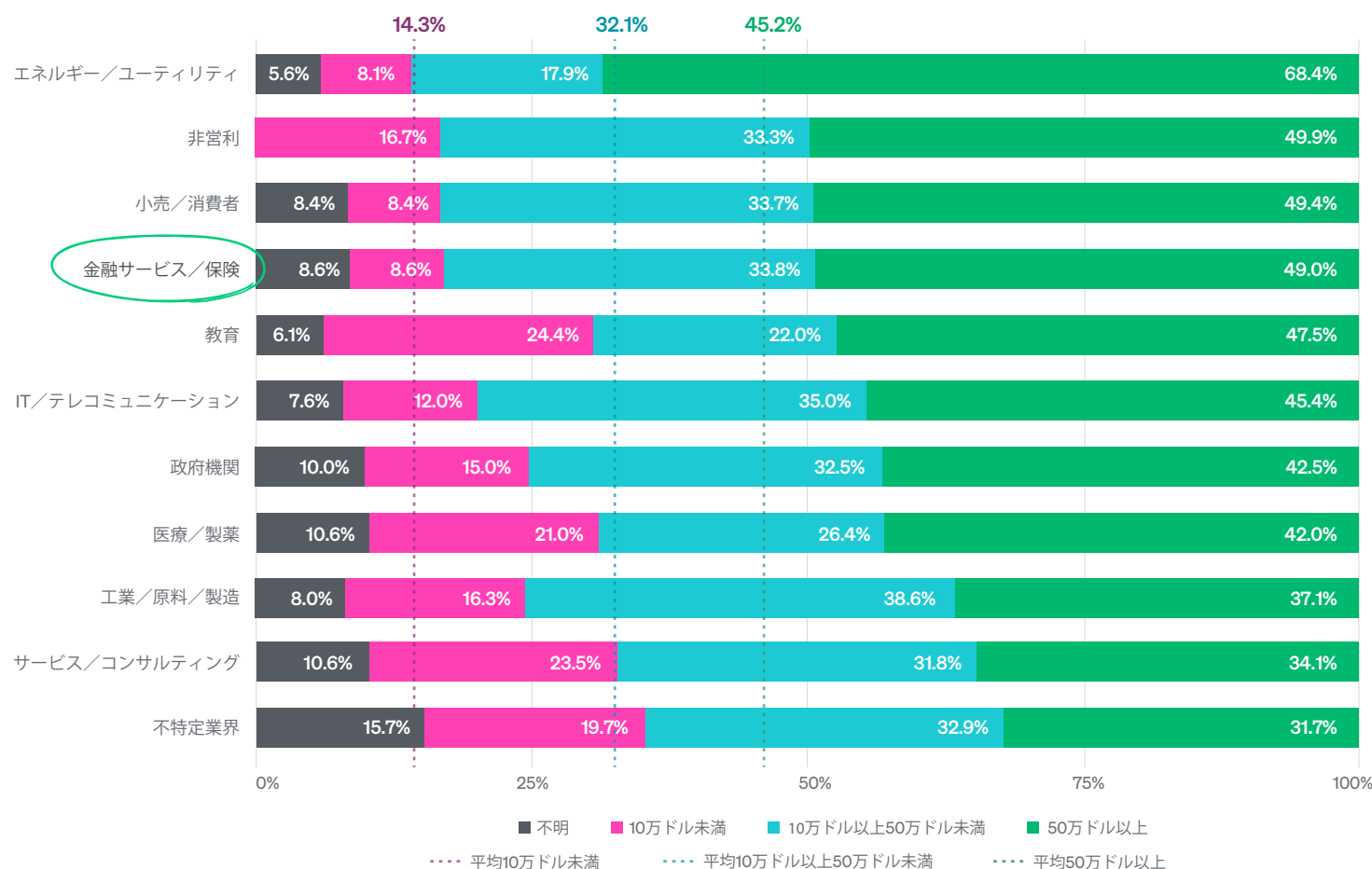
したがって、金融サービス／保険業界の組織のシステム停止頻度とMTTDは平均よりも低いにもかかわらず、MTTRと1時間あたりのシステム停止にかかるコストは平均より高く、年間のシステム停止に伴うコストの中央値は1,044万ドルとなっています。年間停止コストは全業界の年間のシステム停止に伴うコスト775万ドルより約35%高く、全体で4番目に高くなっています。

FSIは高リスクを含むビジネスであり、金融業界の一部の分野（世界的な企業の電信送金や資金移動、トレーディングなど）では取引あたりの平均コストが大きくなる可能性があるため、この業界ではインシデントのコストが高額になるのは不合理なことではありません。



# 金融業向けオブザーバビリティの支出

金融サービス／保険業界の組織は、他の業種よりもオブザーバビリティへの支出が多い傾向にあり、ほぼ半数(49%)が年間50万ドル以上を、31%が100万ドル以上をオブザーバビリティに費やすと回答しています。年間のオブザーバビリティ支出が10万ドル以下との回答はわずか9%でした。



業界別のオブザーバビリティの年間支出



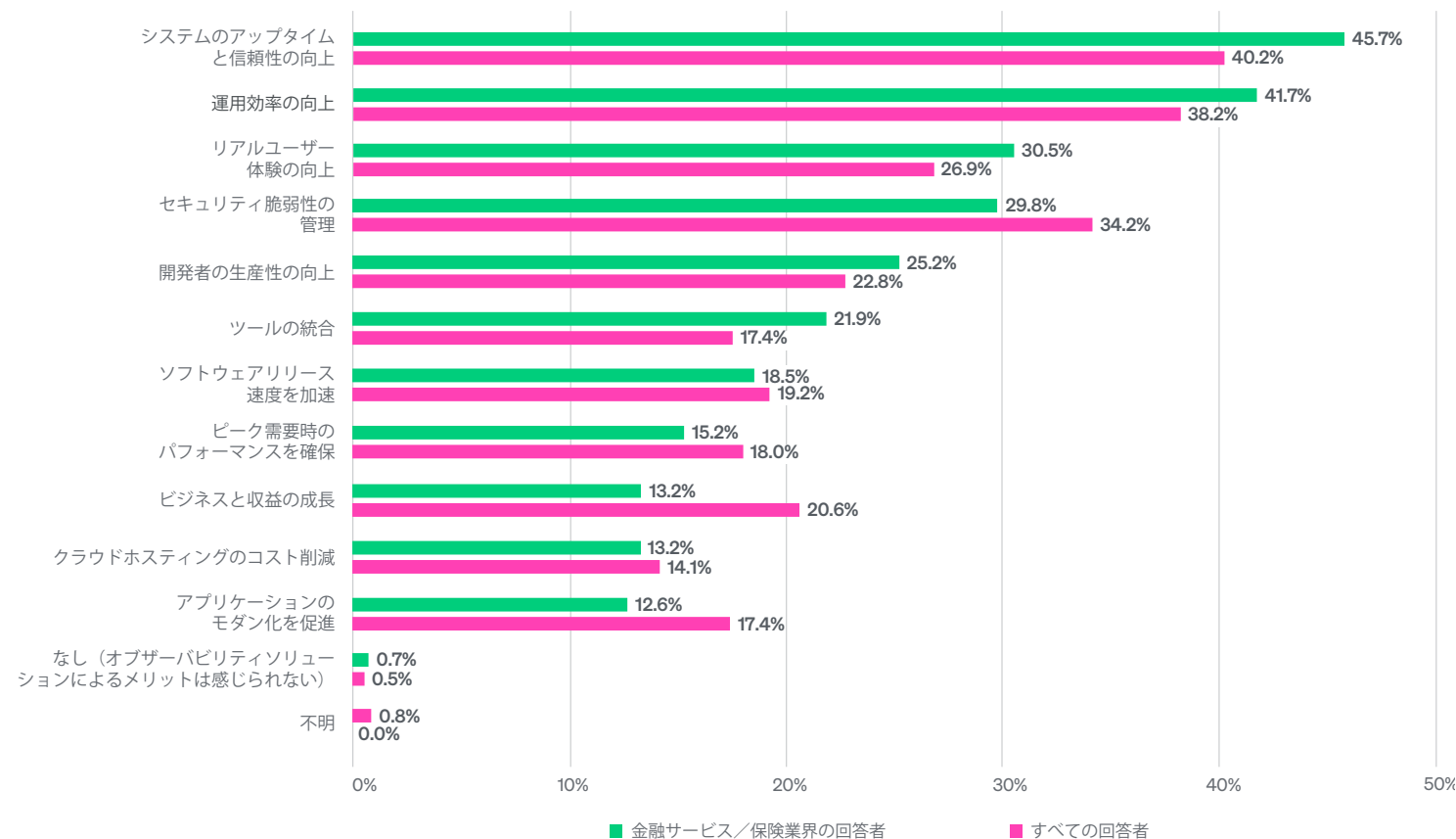
# オブザーバビリティの ビジネス価値

オブザーバビリティはどのような点で業務改善にもっとも役立つかについて尋ねたところ、IT意思決定者 (ITDM) の上位2件の回答は、ビジネスの主要パフォーマンス指標 (KPI) (47%)と技術KPI (43%)の達成でした。実務担当者の上位2つの回答は、生産性を向上させて問題をより迅速に解決する(45%)と、業務が容易になる(36%)でした。

オブザーバビリティによって実現されるビジネス成果に関しては、金融サービス／保険業界の回答者の40%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しています。また、全体の34%と比較して、ほぼ5分の2(39%)が、オブザーバビリティにより顧客の行動への理解が深まり、収益維持率が向上するようになった、と回答しています。

金融サービス／保険業界の回答者は、オブザーバビリティによってもたらされる主なメリットとして、システムの稼働時間と信頼性の向上(46%)、運用効率の向上(42%)、リアルユーザー体験の向上(31%)、セキュリティ脆弱性の管理(30%)が挙げられると回答しました。



オブザーバビリティの主な利点

自社組織がオブザーバビリティへの年間投資から得られる価値の額を尋ねたところ、52%が50万ドル以上、41%が年間で100万ドル以上と回答しました。5分の1(22%)が、年間500万ドル以上の価値が得られていると推定しています。金融サービス／保険業界の組織がオブザーバビリティから得る価値は、平均よりもやや高い結果となっています。

年間支出と年間で得られる価値の見積もりに基づくと、金融サービス／保険業界の組織は年間投資収益率 (ROI) の中央値として投資の2倍の価値を得ていることになります。

ROIにさらにポジティブなインパクトを与える要因はいくつかあります。以下は、そのような組織に見られる特徴です。

- ・ フルスタックオブザーバビリティを実現している組織の回答者は、実現していない回答者(100%)に比べて年間ROIの中央値が高い(114%)
- ・ 成熟したオブザーバビリティを実践している組織の回答者は、成熟度の低い実践を行う回答者(100%)に比べて年間ROIの中央値が高い(250%)
- ・ 現在5つ以上の機能を導入している組織の回答者は、1〜4つの機能を導入している組織(0%)に比べて年間ROIの中央値が高い(114%)
- ・ 現在5つ以上のオブザーバビリティの実践の特性を備えている組織の回答者は、1〜4つを備えている組織(100%)に比べて年間ROIの中央値が高い(114%)

これらの結果は、金融サービス／保険業界の組織が少なくとも2倍のROIを得ており、より多くの技術スタックを監視している組織や、より成熟したオブザーバビリティを実践している組織では、ROIはさらに高くなることを強く示唆しています。



# 41%

自社組織はオブザーバビリティへの投資から年間100万ドル以上の総価値を得ていると回答

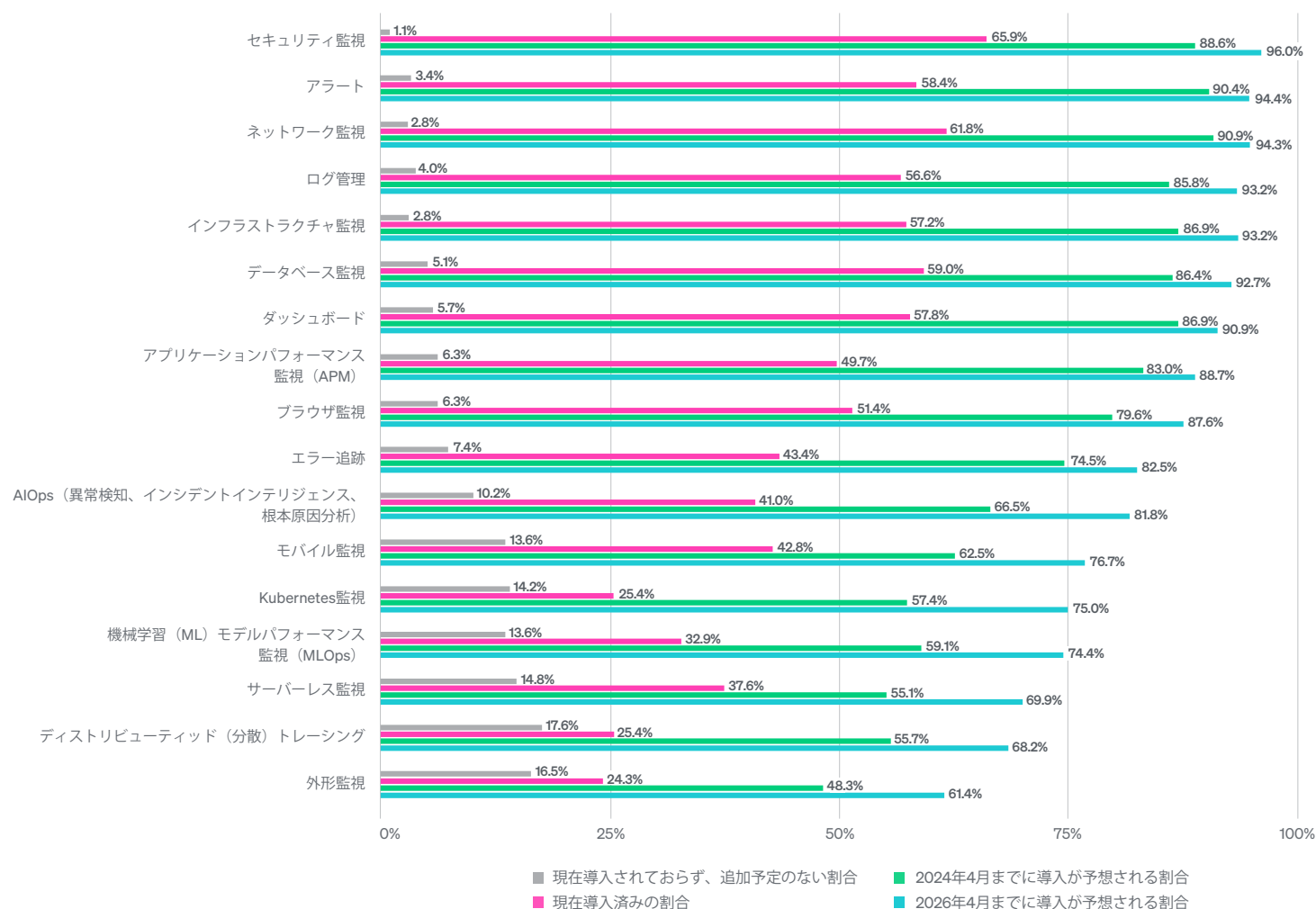
# 金融サービスと保険業界におけるオブザーバビリティの未来

金融サービス／保険業界の組織は、今後1～3年間に積極的なオブザーバビリティ導入計画を立てています。2026年半ばまでに、大多数がセキュリティ監視(96%)を、次いでアラートとネットワーク監視(それぞれ94%)を導入する予定と回答しています。

また、ほとんどの企業が、インフラストラクチャ監視(93%)、APM(89%)、K8s監視(75%)などのバックエンドおよびコアバンキングシステムの運用に不可欠な機能や、ブラウザ監視

(88%)、モバイル監視(77%)、外形監視(61%)などのDEM機能を導入する予定と予想しています。

次年度にオブザーバビリティ支出から最大の価値を得るため、47%が既存のオブザーバビリティツールを最大限活用する方法についてのトレーニングを計画し、42%がツール統合を計画していると回答しています。



# まとめ

金融サービス／保険業界の組織は、新商品やサービスの提供に注力しながら、新たな規制を乗り越え、顧客の獲得を目指して競争するなど、市場の大きな変革を経験しています。これらすべてのバランスを保つために、オブザーバビリティを利用して稼働時間、信頼性、パフォーマンス、効率、シームレスな顧客体験、最先端のイノベーションを実現しています。

金融サービスおよび保険のオブザーバビリティの現状レポートからの洞察では、業界の組織がオブザーバビリティのビジネス価値を理解しており、オブザーバビリティへの投資を増やしていることが明らかになりました。組織の安全性を維持しながら、急速な最新化と革新を行うために、エンジニアは、複雑な技術スタック全体にわたるエンドツーエンドの可視性を実現するために、オブザーバビリティに大きく頼っています。

また、調査より、金融サービス／保険業界の組織が監視ツールの統合を始めていることも示唆されています。今後数年間でより多くの機能を導入することへの強い関心も見られ、これらの組織では、ポイントソリューションからエンドツーエンドの可視性を利用するよりも、堅牢なプラットフォームへ移行する兆しが見られます。





# 次のステップ

New Relicは、FSIと保険業界の組織がDCXを改善し、デジタルトランスフォーメーションの取り組みを通して、フルスタックのオブザーバビリティを実現できるよう支援し、独自のポジションを築いています。

データソース（モバイルバンキングアプリ、ウェブベースのプラットフォーム、ATMネットワーク、決済ゲートウェイ、サードパーティAPIなど）を計装し、オールインワンのNew Relicオブザーバビリティプラットフォームを使用することで、重要なビジネス指標を監視できます。それには、取引の成功率と失敗率、資金移動の速度、融資処理時間、顧客エンゲージメント時間、ATM稼働時間、サードパーティサービスの可用性、ネットプロモータースコア（NPS）、顧客解約率、収益漏洩率などが含まれます。

金融サービス／保険業界の組織は、インフラストラクチャ監視、APM、K8s監視など、バックエンドおよびコアバンキングシステムの運用に不可欠なNew Relic機能を使用できます。

これらのチームは、New Relicのコアウェブバイタル（Core Web Vitals）のクイックスタート（ダッシュボードとアラート機能に含まれる、ビルド済みのオープンソースインテグレーション）を使用すれば、New Relicのブラウザ監視エージェントデータでサイトのCore Web Vitalsを監視し、スコアを改善できます。

New Relicのオブザーバビリティプラットフォーム監視ツールを活用することで、FSIおよび保険業界の組織は、自社の技術スタックと顧客体験のあらゆるステージを可視化できます。また、顧客、製品、サービスパスを単一のビジネスジャーニーに統合し、ビジネスメトリクスに対する財務的なインパクトを定量化できる業界唯一のビジネスオブザーバビリティアプリケーションである、New RelicのPathpointも使用できます。例えば、ウェブサイトが停止すると、Pathpointは稼働停止が発生したことを示すだけでなく、そのダウンタイム1分ごとに失われる潜在的収益も示します。

サービスレベル管理やDEM（ブラウザ監視、モバイル監視、外形監視）などのNew Relicの機能により、FSIと保険機関のITチームは、消費者に影響を与える前に問題をプロアクティブに検知、解決し、最終的に最適化されたユーザーエクスペリエンスを提供します。

潜在的なビジネス成果には、カスタマージャーニー全体の可視化、パターンと問題点の特定、顧客行動の予測、パーソナライズされたサービスの実現、法規制の遵守の徹底などが含まれます。



**Core Web Vitals**は、サイト全般のユーザーエクスペリエンスを測定するためのGoogleが提唱している指標で、サイトのSEO（検索エンジン最適化）ランキングに影響し、そのビジネスに関するユーザーの認知について貴重なインサイトを提供します。Core Web Vitalsを理解することのメリットには、ユーザーエクスペリエンスの向上、SEOの強化、パフォーマンス最適化、インサイトと分析の強化、ビジネス価値の向上などがあります。

カスタマイズされた詳細なデモをご覧になり、お客様の困難な技術的課題に対する解決策と、魅力的な価格設定に関する情報を入手してください。

デモをリクエストする

# 本レポートについて

本レポート内のすべてのデータは、2023年3月から4月に2023年オブザーバビリティ予測レポートのために実施された調査より得られたものです。これは同種の研究において唯一の、生データをオープンソースとした調査です。[2023年オブザーバビリティ予測の調査結果をご覧ください。](#)

金融サービス／保険業界の回答者は、2023年オブザーバビリティ予測調査の調査対象者の10%にあたる176名です。

ETRIは、関連する専門性に基づき調査対象者を選定しました。ETRIは、回答者のサンプルサイズを獲得するのに、彼らが拠点とする国と組織でのロールタイプ（実務担当者およびITDM）にもとづき、割当法と呼ばれる非確率サンプリングタイプを実施しました。地理的分配の割当には、15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表記は米国ドル（USD）です。

## 定義

本レポートで使用されている[定義](#)をご覧ください。

「New Relicから収集したデータは、混乱を理解し、同時にリアルタイムのパフォーマンスの把握も可能にします。継続的リリースに注力するハイペースな環境では、これらのリアルタイムのメトリクスが、システム全体を理解するための、そして改善の必要なサービスやAPIを特定するためのレンズとなります。いつでも迅速にリリースの状況を確認でき、顧客体験に影響を与えうるあらゆる問題を事前に解決できます。」

Sonal Samal氏

10x Banking社、リリースマネージャー



## New Relicについて

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、導入、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ー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について

Enterprise Technology Research (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ーサーチャーファームです。2010年以来、ETRは1つの目標に向かって着実に実績を重ねています。すなわち、企業リサーチにおいて、不完全でバイアスのかかった、統計的に有意ではないデータから形成されることの多い意見の必要性を排除することです。

ETRの扱うITDMコミュニティは、業界で最高クラスの顧客／評価者の視点を提供できる独自のポジションを占めています。このコミュニティから得た専有データとインサイトは、機関投資家やテクノロジー企業、ITDMが、拡張する市場における複雑な企業テクノロジーの展望を概観する上で、大きな役割を果たしています。

