

veeam

データとAIの信頼性
成熟度モデル

安全なAIの 大規模展開への 道のり



安全なAIの大規模展開 への道のり

本レポートは、金融サービス、ヘルスケア、政府、製造業、テクノロジー分野の300人のテクノロジーおよびビジネスリーダーを対象とした独立調査研究に基づいています。回答者には、データ、セキュリティ、リスク、テクノロジー戦略について直接責任を負う上級意思決定者が含まれています。調査結果は、AIの安全な拡大/停止を左右する重要な意思決定に最も近い存在である、さまざまな業界の経営陣からの回答を反映しています。



AIを導入することと、その導入に伴う要求に十分に備えることとの間には、重大なギャップがあります。世界の企業は、AI導入に向けた準備状況や、それに伴って求められるさまざまな対応力において、大きな差があります。

Veeamの「データとAIの信頼性成熟度モデル」調査レポートでは、各組織を導入、展開、準備の状況に基づいて5つのレベルに分けてランク付けを行いました。調査によれば、組織の**95%**が自社の環境内にAIを導入しています。しかし、AIを安全かつ効果的に導入することは、信頼あるAIを大規模展開するうえで必要な運用基盤の構築にはテクノロジーの導入よりも時間がかかるため、より困難であることが明らかになっています。



AIの急速な拡大に伴い、 トラブルも増加

これらの回答者の組織では、AIの導入が着実に進展しています。10人中7人近くが、AIはすでに複数の業務機能に組み込まれているか、業務や競争戦略の中心になっていると回答しています。しかし同時に、回答者たちはその程度の成熟度では調和が困難な一連の問題を報告しています。

回答者の約**52%**が、過去18か月間に少なくとも1つのAIイニシアチブの範囲が縮小されたと回答しています。10人中4人が、イニシアチブが当初のスケジュールより遅れたと報告しています。4人に1人以上（**28%**）がイニシアチブを完全に中止したと報告しており、約3人に1人はイニシアチブが計画通りに進行したと答えています。

これらの障害は、AIがすでに本番環境にある組織で発生しており、初期段階の導入よりも、導入が拡大した際に求められる対応に関係していることを意味します。

スピードがギャップを 露呈させる

リーダーが指摘した障壁は、その理由を明らかにしています。最も頻繁に挙げられる制約は、AI・機械学習分野の人材不足（**43%**）であり、次いでAIを既存のワークフローやシステムに統合することの難しさ（**33%**）が続きます。規制の不確実性（**25%**）、データ品質の限界（**20%**）、説明可能性に関する懸念（**19%**）がさらなるプレッシャーとなっています。

これらの課題はそれぞれが独立しているわけではありません。AIの導入を急いで、ガバナンス、説明責任の構造、データインフラストラクチャを通じたAIのサポート体制確立が後回しになってしまっている組織では、むしろこれらの課題が複雑に絡み合い、深刻化しています。その意味で、一連の阻害要因は個別の問題の集合体というよりも、スピードが優先された結果、置き去りにされがちな課題を示しています。

注目すべきは、テクノロジー自体を制限要因として挙げる経営陣はほとんどおらず、AIの成熟度がイノベーションの速度よりも運用の準備状況によって制約されていることを裏付けている点です。

AIが直面する限界： スキル、システム、標準

経営陣の自信は、表面的にはより楽観的なストーリーを語っています。経営幹部の約**80%**が、今後2年間でAIを安全かつ責任を持って拡張できる自信があると回答しています。しかし、調査結果は重要な違いを明らかにしています。回答者のほぼ半数は、その自信が外部関係者に容易に示せる証拠よりも、直感に基づくものであることを認めています。明確な計画に基づく自信を持つ経営陣の間では、次の3つの要素がほぼ同じく重要視されています。



55%

正式な管理
フレームワーク

55%

リーダーシップの
明確なコミットメント

53%

AIリスク
専用の機能

しかし、外部検証となるとその割合は低下します。AIに関する規制審査や監査に合格したと回答したのは**31%**のみで、同業他社とのベンチマークについて言及したのは**20%**に過ぎません。多くの組織にとって、自信は外部で検証されるものではなく、内部で生み出されるものです。これは、リーダーが設計したフレームワーク、構築したチーム、設定した優先事項を反映しており、これらすべてが緊急事態に耐えられることを証明するために外部で検証される必要があります。

この区別は、AI管理への期待が進化するにつれて重要になります。規制当局や取締役会は、管理が原則的に存在するかどうかも、それが必要に応じて実証できるかどうかにもますます関心を移しつつあります。

経営幹部の10人中9人近くが、正式なAI管理ポリシーが何らかの形で存在すると報告しています。しかし、約3分の1だけが、求められれば包括的な監査証拠を即座に提出できると答えています。多くの経営幹部は証拠が存在することを認めています、それを取りまとめるには多大な労力が必要だとしています。文書化されたポリシーと監査可能なガバナンスは別の機能であり、その間にあるギャップが重大なリスク要因となります。

説明責任の枠組みがこのパターンを強化しています。ほとんどの経営幹部は、AI管理の主な責任をCTOまたはCDOに委ねていますが、かなりの割合が部門横断的な委員会に依存して監督を調整しています。**7%**は専任のAI管理リーダーが存在しています。

これらのモデルはそれぞれ効果的ですが、明確に定義された所有権と説明責任に依存しており、AIが組織の各機能に拡大するにつれて、この2つの条件を維持することが難しくなります。明確な役割やエスカレーション経路がなければ、特に大規模な問題が発生した場合、ポリシーの対象範囲を運用制御に確実に結び付けることはできません。

研究では、AIの導入が広く普及し、リーダー層の楽観的な見方が強い環境が示唆されています。しかし、導入とその熱意を維持するために必要な運用基盤は、ほとんどの組織では依然として形成段階にあります。この移行を最も効果的に進めている企業には、証拠に裏付けられた自信という共通する特徴があります。特に、本レポートの上位レベル（レベル4および5）にランキングされている組織には、単に設計されただけでなく、精査の下で導入およびテストされた実践的な管理プログラムが存在する傾向にあります。



大規模なAIでは スピードよりも準備が重要

データとAIの信頼性成熟度モデルでは、リーダーに対して認識と現実のギャップを埋めるための構造化されたベンチマーク手法を提供します。組織がエンタープライズ全体でデータとAIをどの程度一貫して管理、保護、復元、活用しているかを評価し、意図の表明ではなく実際の運用状況を測定します。調査と先進的な慣行に基づいて構築されたこのモデルでは、成熟度レベルを「アドホック」から「業界リーダー」までの5段階で測定し、備えを仮定から測定可能な機能へと転換します。

自信が証拠に先行しているのではないかと疑うリーダー向けに、本レポートでは、多くの組織がそれを欠いていると示唆する外部の参照物も提供しています。

大規模なAIを維持できるのは、必ずしもAIを早期に導入した組織であるとは限りません。持続的にAIを拡張できる組織とは、管理、責任体制、データ基盤への早期投資を行い、AIの管理能力を超えるリスクを生じさせることなくAIを拡張できるようにしている組織です。

本エグゼクティブサマリは米国地域のデータに焦点を当てています。さらに、データとAIの信頼性成熟度モデルは、より多くのリージョンと業界における調査結果にも拡大し、ガバナンス、回復力、AIへの準備に対するリーダー陣の取り組みについて詳しく検証しています。本レポートでは、リーダー陣がそうした標準に対する自らの立ち位置を評価するための方法を提供するとともに、それを満たすための明確な道筋について示しています。



方法および範囲

本エグゼクティブサマリは、金融サービス、ヘルスケア、政府、製造業、テクノロジー分野の**1300人のテクノロジーおよびビジネスリーダー**を対象に実施された、Veeamが委託した調査に基づいています。回答者には、データ、セキュリティ、リスク、テクノロジー戦略を担当する上級意思決定者が含まれています。本レポートで参照されている調査結果は、より広範な調査集団内の経営陣の回答者に焦点を当てています。

本調査では、組織が実際にAIをどのように導入、管理、拡張しているかを調査し、運用上の準備状況、ガバナンス構造、そしてリーダー陣の信頼を形成する条件に焦点を当てました。調査結果は、将来の意図の表明ではなく、報告された行動、成果、および意思決定の条件を反映しています。ベンチマーク結果は全体調査を通じて得られたものであり、参加したリーダーの実際の回答を反映しており、AIが初期導入からより広範な事業運営へと移行する中で、組織全体に共通するパターンを明らかにするために活用されています。



Veeam Software について

VeeamはデータとAIを託す信頼のパートナー。組織が自社のデータとAIを完全に理解し、保護し、回復力を確保することで、安全なAIの大規模な活用を加速できるよう支援しています。データの回復力とデータセキュリティ態勢管理の両方における市場リーダーとして、Veeamはアイデンティティ、データ、セキュリティ、AIリスクを収束させることを念頭に設計されています。

Veeamは、あらゆるデータ資産、アイデンティティ、AIモデルにわたって、詳細でコンテキストに応じたインテリジェンスを提供します。人間とAIエージェントの両方に対するアクセスを管理し、プライバシー、コンプライアンス、修復プロセスを自動化するとともに、ランサムウェア、災害、AIの誤作動などの最新の脅威から組織を保護・復元し、クリーンで信頼できるデータのリストアを実現しています。Veeamは、組織が単にデータを保護するだけでなく、その価値を活かし、最大限に発揮できるよう支援します。

米国シアトルに本社を置き、30か国以上に事業拠点を構えるVeeamは、全世界で55万社を超えるお客様を保護しています。この中にはFortune 500の82%の企業が含まれ、ビジネスを止めないVeeamに信頼をお寄せいただいています。

詳細については、www.veeam.com/jpをご覧ください。また、LinkedIn (@veeam-software) およびX (@veeam_japan) にてVeeamをフォローしてください。

