調査レポート



エージェント型 AI がネットワーク運用に与える影響

シスコと Omdia 社による 2026 年の調査レポート

©2026 Cisco and/or its affiliates. All rights reserved.

目次

01 エグゼクティブサマリー

02 IT 部門はもはや人材採用だけでは問題を解決できない

03 ネットワークには想像以上に多くの死角がある

04 自律運用への移行はすでに共通認識となっている

05 信頼の条件

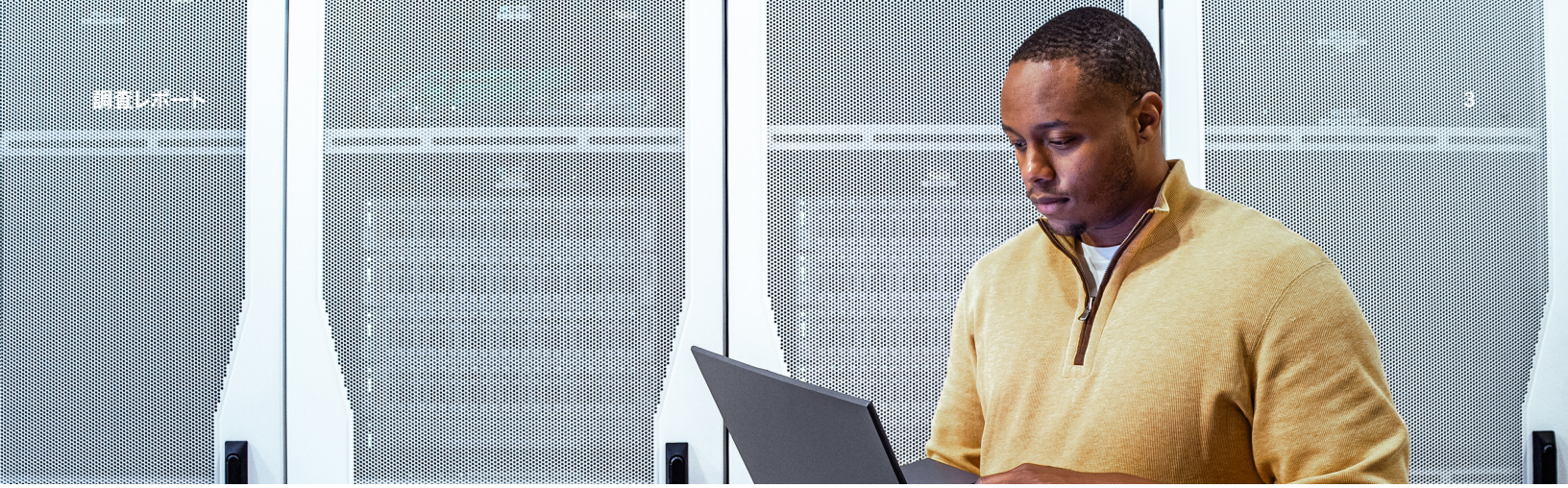
06 導入を遅らせかねない組織内の認識のギャップ

07 初期の調査結果が示す効果

08 今後を左右する 12 か月

09 この調査について

©2026 Cisco and/or its affiliates. All rights reserved.



01 エグゼクティブサマリー

AI がネットワーク運用を支援すべきかどうかという議論は、事実上終結

ネットワーク運用におけるエージェント型 AI を話題にすると、論点はほぼ必ず「信頼性」という 1 点に帰結します。企業は本当に運用管理を AI に委ねるのでしょうか？ Omdia 社が実施した独立調査は、この問い自体がすでに時代遅れになっていることを示唆しています。さらに、集約したネットワーク テレメトリ データをシスコ主導で分析した結果も、この調査を裏付けています。

1,000 人の IT およびネットワーク運用のリーダーによると、AI への移行はすでに着実に進んでいます。組織の 4 分の 3 は、すでにネットワーク運用に AI を導入しています。半数の組織は、アドバイスを提供するだけでなく実際に処理を実行するエージェント型 AI システムを、今や本番環境で稼働させています。組織の 84% は、従来の AIOps から、「AgenticOps」とも呼ばれるエージェント主導の運用へ移行し、12 か月以内には AI 主導の運用モデルに切り替わると見込んでいます。

AI を利用している組織のうち …

75%
ネットワーク運用に AI をすでに導入している割合

51%
現在、本番環境で、アドバイスを得るだけでなく実際にエージェント型 AI に処理を任せている割合

84%
12 か月以内に AI 主導の運用モデルに切り替わると見込んでいる割合

出典 : Omdia

©2026 Cisco and/or its affiliates. All rights reserved.

この動きは、現実を無視した願望ではなく、構造的な問題に対する合理的な対応です。現代のネットワークは、人間の運用能力では対応しきれない規模に拡大しているからです。アラートの量、変更の頻度、複数のドメインにまたがる複雑さは、どれだけ人員を増やしても対処できないレベルに達しています。企業はこうした状況を数字で把握し、自律運用を、管理すべきリスクではなく、設計によって実現すべき不可欠な仕組みと結論付けています。

本調査から得られた主な知見は以下のとおりです。

- **IT 部門はもはや人材採用だけでは問題を解決できません。**ネットワーク需要が過去最高水準に達する一方で、回答者の 95% は、既存の非エージェント型ツール（AIOps）が 1 つ以上の領域で需要の増大に対応できていないと回答しています。AgenticOps を利用していない組織が処理待ちのネットワークアラートを手作業で解消するには、約 100 人の専門家からなるチームが必要です。

- **ネットワークには想像以上に多くの死角があります。**回答者の 92% は、問題が複数のドメインにまたがることが多いと回答しています。また、チームは可視性の確保に 10 種類以上の個別ツールを利用しています。このような情報とツールの分断は、構造的な弱点となっています。

- **自律運用への移行はすでに共通認識となっています。**人員では対応しきれない業務量と、手作業では関連付けられない分断された情報に直面し、組織の 51% はすでにエージェント型 AI を本番環境で運用しています。また、84% は 12 か月以内に運用を全面的に AI が主導するモデルを実現すると見込んでいます。

- **信頼を得るための条件は明確です。**企業が求めているのは、自動化の抑制ではなく、信頼できるエージェントを中心とした自動化です。ただし透明性は必須条件です。組織の 69% が、エージェント型 AI のアクションに至る因果関係を詳しく追跡できることを求めています。また 86% は、個別ツールを追加するのではなく、単一の統合プラットフォームを導入することが、最も効果的な解決策だと回答しています。

- **最大の障壁は技術ではなく、組織としての準備状況かもしれません。**AgenticOps への移行を認識している割合は、NetOps の実務担当者では事業部門の幹部のほぼ 2 倍です。こうした現場と経営層の認識のギャップは、AI の導入や運用変革を遅らせる可能性があります。

- **AI 活用で先行する組織は、すでに差を広げています。**NetOps における AI 導入レベルが最も高い組織は、成熟度の低い同業組織と比べて、従業員 1 人あたりの生産性が 30% 近く高く、エンドツーエンドの完全な可視性を実現している割合は 3.2 倍です。この結果は、AI の成熟度が単なる運用改善にとどまらず、競争優位性を生み出しつつあることを示唆しています。

©2026 Cisco and/or its affiliates. All rights reserved.



02 対応能力

IT 部門はもはや人材採用だけでは問題を解決できない

過去 20 年間、運用の複雑化には、人員、ツール、プロセスを増やすことで対応してきました。しかし、AIOps ベースの運用では対応しきれず、このモデルは限界に達しています。

アラートを人手で処理するという計算は、もはや成り立たない

現在、平均的な組織では 1 日あたり約 4,100 件の監視アラートとイベントが発生しており、その半数強（51%）がネットワーク関連です。一般的な担当者が 1 日に確認、調査、解決できるネットワークアラートは約 21 件です。日々の処理待ちアラートを手作業で解消するには、約 100 人の専門家からなるチームが必要です。しかし、ほとんどのネットワーク運用チームには、それをはるかに下回る人員しかいません。

アラート解消に必要な人員の計算

4,100	51%	21	約 100
1 日のアラート・イベントの発生数（1 組織あたり）	ネットワーク関連（1 日あたり約 2,100 件）	1 人の担当者が 1 日に 処理できるアラート数	処理待ちのネットワークアラートを手作業で解消するために必要な専門家の数

出典 : Omdia

©2026 Cisco and/or its affiliates. All rights reserved.

その結果として生じるのは、予測可能でありながら、運用を徐々にむしばむ次のような問題です。

46% のネットワークアラートが、人員不足、繰り返し発生するノイズ、誤検知を理由に、調査されないままクローズされています。

45% の調査時間が、誤検知の追跡に費やされています。この作業は問題の解決にも価値の創出にもつながりません。

65% のリーダーが、「アラート疲れ」を従業員の不満の大きな原因としています。また、67% は、大量のアラートによってチームが他の重要な業務に取り組めなくなっていると回答しています。

出典 : Omdia

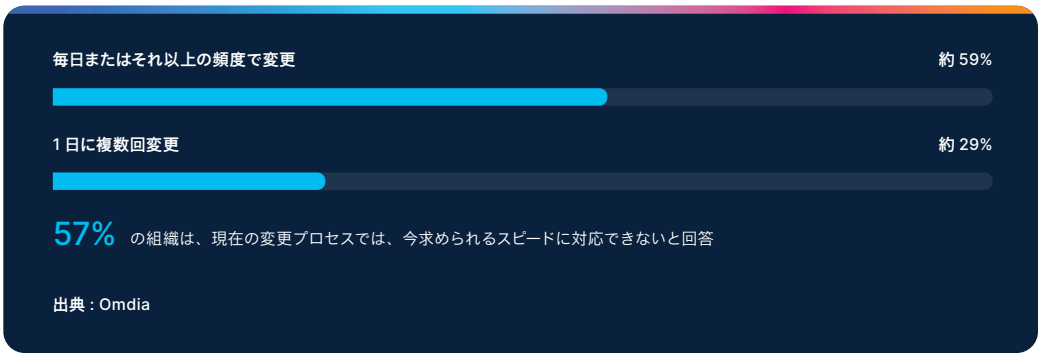
これはもはや、採用活動を改善すれば解決できる人員の問題ではありません。ネットワーク環境が生み出す情報量と、人間の情報処理能力との間にある構造的な不均衡なのです。

絶え間なく発生する変更

現在、組織の 5 分の 3 近くが、本番ネットワーク環境に毎日、またはそれ以上の頻度で変更を加えています。その半数は 1 日に複数回変更を加えており、1 時間に複数回変更する組織も少なくありません。しかし 57% は、現在の変更プロセスでは、今求められる更新のスピードに対応できないと回答しています。ネットワークはもはや、時折変更を加えるだけの安定したシステムではありません。絶えず変化するシステムであり、運用モデルもその変化に対応する必要があります。

本番ネットワークの変更頻度

変更はもはや時折発生するものではありません。ほとんどのチームで毎日、多くの場合は時間単位で発生しています。



©2026 Cisco and/or its affiliates. All rights reserved.

AI 自体が運用の負担を増大させている

本調査で明らかになった皮肉な状況の 1 つは、運用負担を軽減するはずのテクノロジーが、同時に新たな負担を生み出していることです。回答者の 3 分の 2（67%）は、生成 AI ブームによってネットワークが大幅に複雑化したと回答しています。さらに 70% は、AI の導入によって NetOps の業務負荷が減るどころか増えたと回答しています。注目すべき点は、組織の 95% が、既存の非エージェント型ツール(AIOps) に大きな課題があると回答していることです。主な理由は、人間による解釈に頼りすぎていることと、ドメインを横断した可視性が不足していることです。

AI がもたらす変化は、ツールや業務負荷にとどまりません。ネットワークの利用方法や仕事の進め方も根本から変えています。AI との直接通信で生じるネットワークトラフィックをシスコが分析したところ、1 日あたりの平均 AI トラフィックは 6 か月ごとに倍増するペースで増えていることがわかりました。この予測は、同じ分析で確認された具体的な数値に基づいています。クライアントあたりの AI との直接通信トラフィックは 54% 増加しました。この増加を加速させているのは、AI タスクの複雑化と考えられます。複雑なタスクには、単純なクエリよりも多くのデータ交換が必要です。

重要なのは、このデータが AI トラフィックの実態の一部しか捉えていないことです。Copilot や Search などのプラットフォームに組み込まれた AI が生成するトラフィックは含まれていません。また、エージェントが継続的に生成するマシン間トラフィックの、今後避けられない急増も含まれていません。実際、シスコの調査では、AI エージェントがネットワークの「パワーユーザー」として、人間ではなくソフトウェアの速度で動作することがわかっています。実証テストでは、エージェントがタスクを実行すると、タスクあたりの総トラフィック量が最大 450% 増加することが示されています。

ネットワークトラフィックに占める AI の割合

6 か月ごと

AI トラフィックは倍増し、さらに倍増し、また倍増する



出典：シスコ

AI が大きな変革をもたらす理由は、(少なくとも現時点では) その規模の大きさではありません。その理由は、AI が増加に増加を重ね、既存のネットワークや運用が想定していなかった挙動を示すことにあります。

見えてくるのは、従来の AIOps 運用モデルがあらゆる面で同時に圧迫されている状況です。アラートや変更が増えるだけでなく、AI トラフィックの大幅な増加も迫っています。

©2026 Cisco and/or its affiliates. All rights reserved.



03 分断

ネットワークには想像以上に多くの死角がある

対応すべき量の多さが第 1 の構造的な問題だとすれば、分断は第 2 の問題です。

現代のネットワーク障害は、組織の境界を越えて発生します。組織の 92% は、パフォーマンスの問題がクラウド、セキュリティ、アプリケーション、エンドポイントなど、複数のドメインにまたがることが多いと報告しています。問題の震源地が、最初に症状が現れた場所と同じであることはめったにありません。レイテンシに関する苦情の原因がクラウドネットワークの設定ミスにあり、それがアプリケーションの速度低下として現れると同時に、セキュリティツールで検出されることもあります。

しかし、こうした問題の診断に使うツールは、依然としてサイロ化したままです。組織は、ネットワーク全体のエンドツーエンドの可視性を確保するために、平均で 10 種類近くの個別ツールに依存しています。各ツールが示すのは全体像のごく一部にすぎず、全体を把握できるツールはありません。その結果、チームは全体像を把握できないまま問題を診断し、ログやイベントを手作業で関連付け、部門をまたいでインシデントの対応を引き継いでいます。

分断された可視性とツール

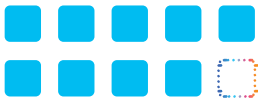
92%

のパフォーマンス問題が、複数のドメインに同時にまたがる。問題の震源地が、最初に症状が現れた場所と同じであることはめったにない

クラウド | セキュリティ | アプリケーション | エンドポイント | サードパーティ API | WAN

約 10

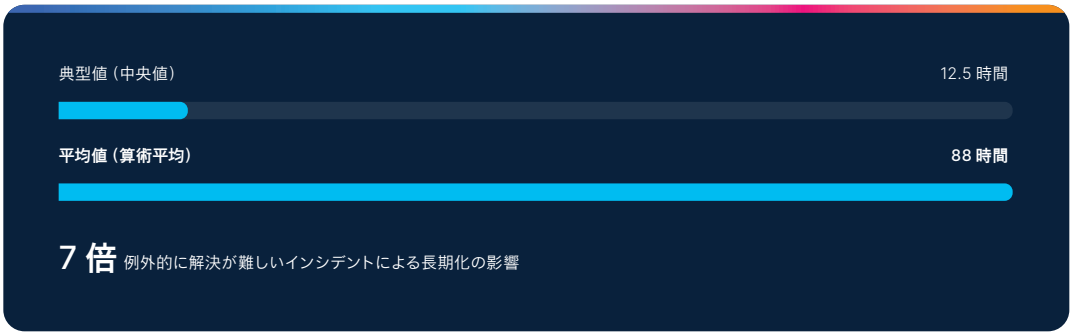
種類のツールにより、エンドツーエンドの可視性を確保している。各ツールが示すのは全体像の一部にすぎず、全体を把握できるものはない



出典 : Omdia

©2026 Cisco and/or its affiliates. All rights reserved.

インシデント解決までの時間



46%

インシデントの解決には通常 1 日を超える時間がかかると回答した組織の割合

10 組織に 1 組織

インシデントの解決には通常 1 週間を超える時間がかかると回答した組織の割合

出典：Omdia

この分断による悪影響が最も顕著に表れるのは、問題の解決時間です。ネットワークインシデントの平均解決時間は 88 時間です。これは、中央値の 12.5 時間の 7 倍にあたります。この差は、多くの組織が問題に比較的うまく対処する一方で、複雑なインシデントの解決に日常的に苦慮している組織も少なくないことを示しています。こうしたインシデントへの対応は、数日から数週間に及ぶこともあります。回答者のほぼ半数（46%）は、インシデントの解決に通常 1 日を超える時間がかかると回答し、10 人に 1 人は 1 週間を超えると回答しています。ごく少数の例外的に解決が難しいインシデントが、組織の運用を大きく妨げています。こうした深刻で解決が困難なインシデントに遭遇すると、運用チームの対応は長期化します。それが足かせとなり、NetOps はビジネスが求めるスピードで対応できなくなっています。

©2026 Cisco and/or its affiliates. All rights reserved.



04 自律性

自律運用への移行はすでに共通認識となっている

人員では対応しきれない業務量と、手作業では関連付けられない分断された情報に直面した企業は、ある明確な共通認識に達しています。それは、必要なのは人員やダッシュボードの追加ではなく、エージェント主導の自律運用だ、というものです。

調査結果は、この結論を極めて明確に裏付けている：

75%	ネットワーク運用に AI テクノロジー（AIOps から AgenticOps まで）を導入している組織の割合
51%	現在、本番環境で、実際にエージェント型 AI に処理を任せている組織の割合
80%	AI に高度な自律性、または完全な自律性を持たせることに抵抗がない組織の割合（56% は人間がアクションを承認する場合、24% は人間による監督がまったくない場合）。
82%	少なくとも一部のアクションについて、AI が人間の事前承認なしに本番環境を変更することに抵抗がない組織の割合

出典：Omdia

©2026 Cisco and/or its affiliates. All rights reserved.

自律性の段階

AI に高度な自律性、または完全な自律性を持たせることに抵抗がない 80% の内訳

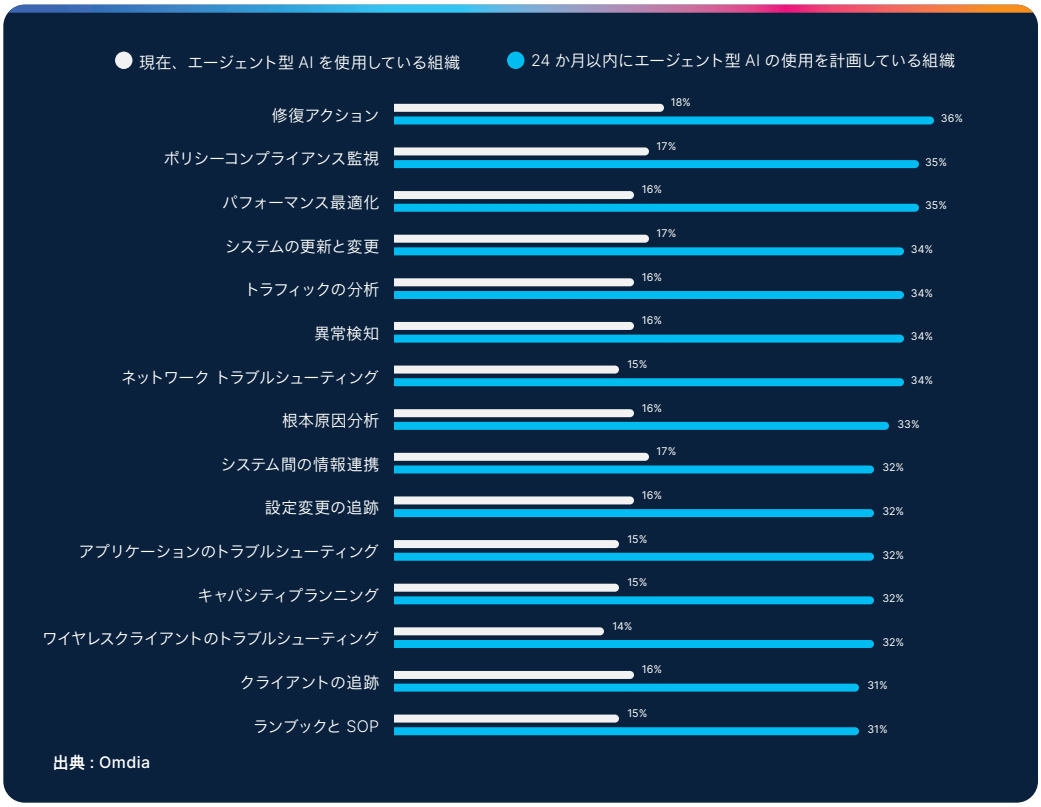


組織の大多数（85%）は、AI エージェントが 5 年以内に大半の運用タスクを自律的に管理するようになると考えています。実際、80% は、今の段階においても、NetOps で AI に高度な自律性、または完全な自律性を持たせることに抵抗がないと回答しています。82% は、少なくとも一部のアクションについて、AI が人間の事前承認なしに本番ネットワークを変更することに抵抗がありません。これには、トラフィックの経路変更、ワイヤレスパラメータの調整、不審なエンドポイントの隔離、インシデントへの対応から解決までの一連の処理などが含まれます。

これは仮定の話ではありません。すでに進む方向は定まっています。組織の 84% は、今後 12 か月以内に運用を全面的に AI が主導するモデルに切り替える見込みです。また、個々の NetOps プロセスにおけるエージェント型 AI の導入は、その期間にほぼ倍増する見込みです。

NetOps プロセス別に見るエージェントの導入見通し

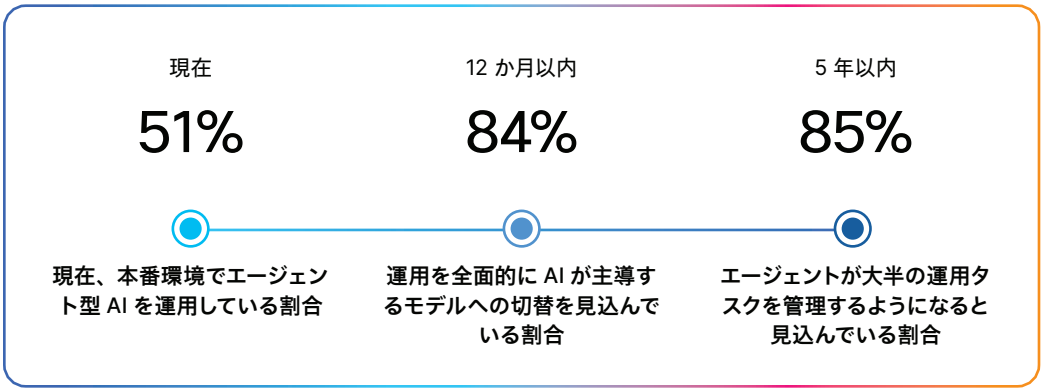
今後 24 か月以内のエージェント型 AI の導入計画をプロセス別に見ると、すべてのプロセスで現在の約 2 倍になる見通しです。



©2026 Cisco and/or its affiliates. All rights reserved.

導入の見通し

別々の質問から得られた 3 つの調査結果は、いずれも同じ方向を示しています。

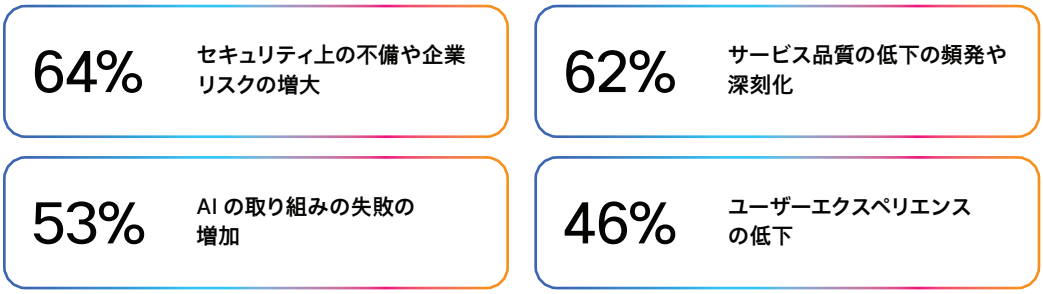


出典 : Omdia

導入の動機は、理念よりも実用性にあります。NetOps にエージェント主導の AI を導入する主な目的は、セキュリティと脅威検出の強化、ネットワークの複雑さへの対処、エンドユーザーエクスペリエンスの向上です。企業が AgenticOps を導入するのは、流行しているからではありません。自動化しないという選択肢が、容認できない結果を招くと考えているからです。64% はセキュリティ上の不備や企業リスクの増大、62% はサービス品質の低下の頻発や深刻化、53% は AI の取り組みの失敗の増加、46% はユーザーエクスペリエンスの低下を予想しています。

自動化しないことのコスト

リーダーは、何もしないことを無害な選択とは考えていません。大多数は、複数の面で代償を払うことになると予想しています。



出典 : Omdia

AI がネットワークを運用するかどうかという議論には、業界ではすでに終止符が打たれています。今は、どのように運用するかを決める段階に入っています。

©2026 Cisco and/or its affiliates. All rights reserved.



05 信頼

信頼の条件

企業は、AI に無条件で運用管理を委ねているわけではありません。AgenticOps を受け入れるリーダーは、権限を委ねる条件も明確にしています。しかも、その条件には驚くほど共通点があります。

透明性は必須条件

AgenticOps への期待は大きいものの、信頼を得るには、推論の過程を可視化し、透明性を確保する必要があります。組織の 69% は、エージェントのアクションについて詳細に説明できることを求めています。また、回答の中で最も多かった 36% は、完全なオブザーバビリティ（詳細な追跡、要約された判断根拠、アクション後の監査）が最低限必要だと回答しています。

調査結果が伝えるメッセージは明確です。透明性がなければ信頼は得られません。

求められるのは統合アーキテクチャ

見えないものを信頼することはできません。ツールが分断されていると、得られる情報も個別のツールに散在し、その間に生じる死角で信頼が失われます。企業はこのことを理解しています。86% は、コンピューティング、セキュリティ、アプリケーション、ネットワーキングを網羅する単一の統合プラットフォームが解決策だと回答しています。個別ツールをさらに追加することではありません。

今後の道筋

86% **最も効果的な解決策は、コンピューティング、ストレージ、アプリケーション、ネットワーキングを網羅する単一の統合プラットフォームだと回答**

出典：Omdia

©2026 Cisco and/or its affiliates. All rights reserved.

安全策に求められるのは、選択ではなく組み合わせ

不可欠な安全策を尋ねると、回答者は 6 つの候補から平均 3 つを選びました。各項目の選択率に大きな差はありませんでした。

必要な安全策

99%

の組織が、これらの安全策なしには、AI を信頼してアクションを任せられないと回答しています。安全策を何も設けずに進めると回答した組織は、わずか 1% でした。

出典 : Omdia

すべての安全策が必要な項目として挙げられ、不要とされたものはありませんでした。

- 説明可能な AI アクション
- アクションに対する人間の承認
- ポリシーに基づく運用上の制限
- 緊急時のオーバーライドメカニズム
- ロールベースアクセス制御
- 改ざん不可能な監査証跡

組織はこれらを、どれか 1 つを選ぶ代替案ではなく、組み合わせて備えるべき基本要件と捉えています。

これらの調査結果を総合すると、信頼という問題の捉え方が根本的に変わります。企業は自動化を減らすことを求めているわけではありません。求めているのは、信頼できる自動化なのです。多数のツールから情報をつなぎ合わせるのではなく、単一の統合インターフェイスで状況を把握し、追跡できる自動化です。企業が求めているのは、説明可能性、承認ゲート、ポリシーに基づく制限、オーバーライドの仕組み、監査証跡によって適切に制御された、エージェント主導の自律運用です。

©2026 Cisco and/or its affiliates. All rights reserved.



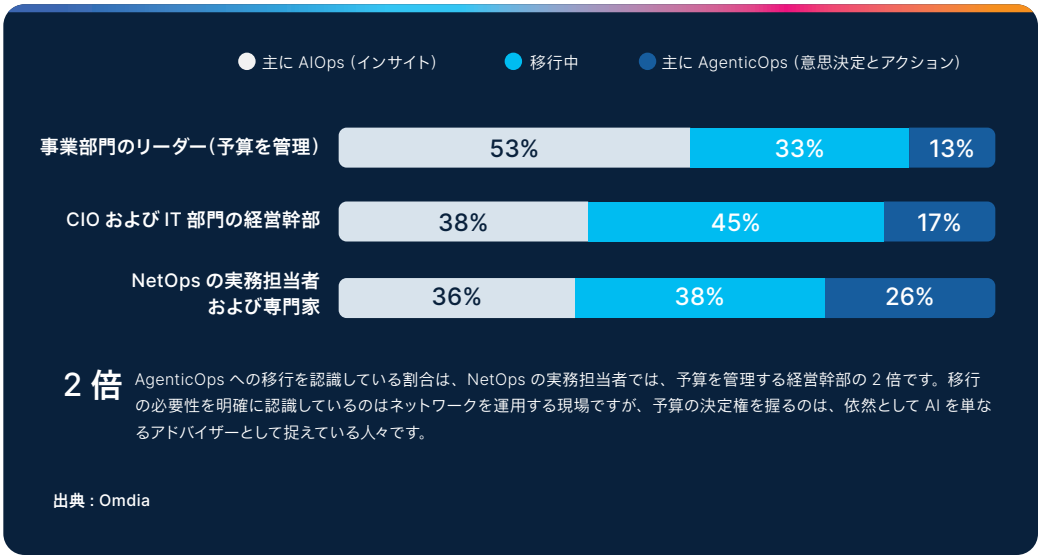
06 導入への準備

導入を遅らせかねない組織内の認識のギャップ

AgenticOps にとって最大の障害は、技術的なものではないかもしれません。組織面の問題である可能性があります。本調査では、日々の業務を担う人々と予算を管理する人々との間に、大きな認識のギャップがあることが明らかになりました。AgenticOps への移行を認識している割合は、NetOps の実務担当者では事業部門の幹部の約 2 倍です。日々運用上の負担を感じている実務担当者は、この動きを明確に認識しています。予算に影響力を持つ事業部門のリーダーは、運用における AI を、エージェントによる自律的な実行ではなく、インサイトや推奨事項を提供するものと捉える傾向がはるかに強くなっています。これは従来の「AIOps」の考え方です。

各グループが IT 運用における AI の役割をどのように捉えているか

日々の業務に近い立場にいるほど、AI の役割が助言から実行へ移っていることを認識しています。



2 倍 AgenticOps への移行を認識している割合は、NetOps の実務担当者では、予算を管理する経営幹部の 2 倍です。移行の必要性を明確に認識しているのはネットワークを運用する現場ですが、予算の決定権を握るのは、依然として AI を単なるアドバイザーとして捉えている人々です。

出典：Omdia

©2026 Cisco and/or its affiliates. All rights reserved.

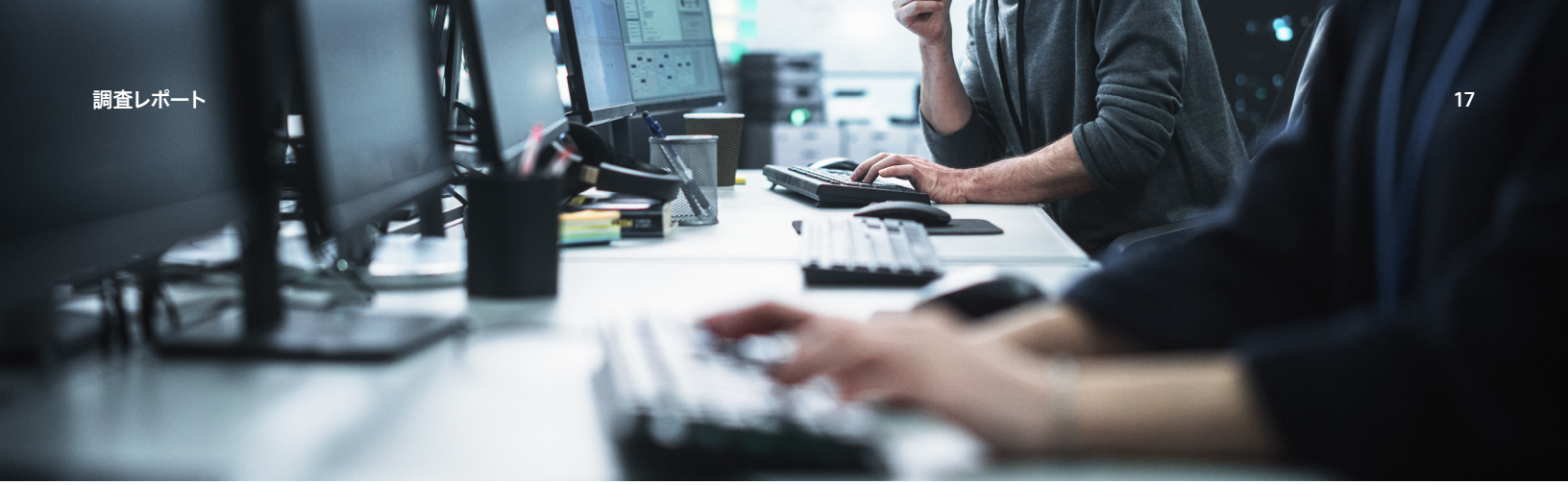
このギャップが重要なのは、必要性を最もよく理解している人が、必ずしも投資を判断する立場にいないからです。そのため、技術部門のリーダーには、AgenticOps が単なる段階的な改善ではなく、根本的な変革をもたらすものであることを、財務部門や事業部門の関係者に伝える役割が求められます。

他にも障壁はありますが、その深刻さは予想を下回っています。主な懸念事項は、データセキュリティとプライバシー（38%）、AI の導入と統合の複雑さ（34%）、リスクとコンプライアンス（30%）です。一方、最も少なかった回答は「目標が不明確」と「経営層の支援不足」でした。これは、組織に意欲や方向性が欠けているわけではないことを示しています。障壁となっているのは意欲ではなく、実行と信頼の問題です。

NetOps における AI 活用の最大の障壁



©2026 Cisco and/or its affiliates. All rights reserved.



07 結果

初期の調査結果が示す効果

投資は成果を上げているのでしょうか？初期の調査結果は、期待の持てるものです。

AgenticOps の導入を含め、ネットワーク運用への AI 活用に最も積極的に投資してきた組織は、成熟度の低い同業組織と比べて、重要な指標で明らかに優れた成果を上げています。

NetOps における AI 成熟度がもたらす効果

約 30%

担当者 1 人あたりの生産性向上率。AI 活用の成熟度が最も高い組織は、担当者 1 人が 1 日に解決するアラートの数が多い。

3.2 倍

AI 活用の成熟度が最も低い同業組織と比べた場合に、エッジインフラストラクチャのボトルネックを完全に可視化している確率。

出典 : Omdia

©2026 Cisco and/or its affiliates. All rights reserved.

生産性

個人の生産性の向上。 AgenticOps を利用し、AI 活用の成熟度が最も高い組織の担当者は、成熟度が最も低い組織の担当者と比べて、生産性が 30% 近くも高くなっています。担当者 1 人が 1 日に調査、解決するアラートの数も大幅に多くなっています。他の条件が同じなら、この生産性の向上によって、同じ量の処理待ちアラートに対応するために必要な専門家を数十人減らせます。その分、限られた人材をより価値の高い業務に振り向けられます。

可視性

可視性の向上。 エージェントを活用する最も成熟した組織は、エッジインフラストラクチャのボトルネックをエンドツーエンドで完全に可視化している確率が 3.2 倍も高くなります。また、パフォーマンス問題が複数のドメインにまたがることを認識している割合も、はるかに高くなっています。この認識は、問題を解決するための前提条件です。

対応能力

自信と対応能力の向上。 成熟した組織では、チームが業務量になんとか対応している、あるいは対応が追いついていないという報告よりも、十分に対応できているという報告が目立ちます。

©2026 Cisco and/or its affiliates. All rights reserved.



08 展望

今後を左右する 12 か月

本レポートの調査結果は、すでに訪れた転換点を示しています。企業は、人手による運用では対応しきれないほど、ネットワークの規模が大きく、変化が速く、情報やツールが分断されているという構造的な問題に直面しました。そして、エージェント主導の自律運用が解決策だと結論付けました。企業はすでに本番環境への導入を開始し、信頼を置くための条件を明確にしています。また、1 年以内に AI 主導のモデルに切り替えると見込んでいます。

残された問いは、もはや方向性ではありません。問われているのは実行です。組織は、エージェント主導の自律性を信頼できるものにするための安全策を導入するのでしょうか？分断されたツール群を、自ら必要だと述べている統合プラットフォームへと集約するのでしょうか？そして、技術部門のリーダーは、事業部門の関係者の理解と協力を得られるのでしょうか？

今後 12 か月で、AgenticOps が企業ネットワークを運用するかどうかが決まるわけではありません。本調査の対象企業は、その点についてはすでに決断しています。今後 12 か月で決まるのは、AgenticOps がどれほど効果的にネットワークを運用できるか、そして今後 10 年間のネットワーク運用を支えるモデルを確立し、どの組織が先行するかです。

混乱した運用から、効率的な自律運用へ

運用が混乱する「現状」から、AgenticOps によるエージェント中心の効率的な運用という「将来像」へ移行するには、経営層が明確な方針のもとで戦略的に行動する必要があります。

©2026 Cisco and/or its affiliates. All rights reserved.

01

「採用」から「設計」へと転換する

処理量と対応能力の不均衡を、人員数だけで解決しようとするのはやめましょう。1日に 4,100 件発生するアラートを処理できるだけの人員を採用することはできません。仮にできても、持続可能なビジネスモデルにはなりません。重点と予算を「人員の追加」から「自律運用の設計」へ移しましょう。誤検知を手作業で追跡する「チケット処理担当者」ではなく、エージェントを管理する「エージェント オーケストレータ」へと役割を変えられるよう、チームのリスキリングを進めましょう。目標は、優秀な人材を、大量のアラートや絶え間ないシステム変更への対応から解放し、戦略的なネットワーク設計という価値の高い業務に振り向けることです。

02

「経営層と実務担当者」の隔たりを埋める

ネットワークを運用する人々と予算を提供する人々との間には、危険な認識の隔たりがあります。NetOps チームは、人手に依存した現在のモデルが限界に達していることを理解しています。しかし、事業部門の経営幹部は、エージェント主導の自動化を事業存続のための戦略ではなく、「あれば望ましいもの」と捉えているかもしれません。リーダーの役割は、1 日 4,100 件のアラートや長期化する解決時間といった技術面の実態を、ビジネス上のリスクとして伝えることです。AgenticOps への移行を、単なる IT のアップグレードではなく、サービス停止やセキュリティ侵害からビジネスを守るリスク軽減戦略として位置付けましょう。

03

「信頼第一」のガバナンス フレームワークを構築する

危機が起きる前に、AI とエージェントの安全策を定めましょう。エージェントのアクションと自律性の価値は、それらにどれだけ信頼を置けるかで決まります。利用規模を拡大する前に、エージェントのセキュリティ、透明性、監査可能性、人間が関与する監督を確保できるソリューションを導入してください。AI に許可するアクションを明確に定め、判断の記録と説明を徹底するガバナンスによって、ツールを支えてください。こうした対応を経て初めて、未知への不安を取り除けます。自社環境に導入するすべてのベンダーとシステムに対して、「説明可能な AI」を必須要件にしてください。

©2026 Cisco and/or its affiliates. All rights reserved.

09 付録

この調査について

ネットワーク運用における AI の成熟に伴い、共通の用語体系が形成されつつあります。以下の定義は、IT 運用と NetOps に適用される AI の種類について、業界で区別が明確になりつつある状況を反映しています。

人工知能（AI）とは、言語の理解、パターンの認識、問題解決、新たな情報からの学習など、通常は人間の知能を必要とするタスクを機械が実行するための幅広い能力です。人工知能は、以下のすべてを包含する総称です。

生成 AI は、プロンプトに応じてテキスト、コード、画像、要約などの新しいコンテンツを生成する AI の一種です。分類や予測だけでなく、新たな出力を生成することで、チャットアシスタントやコーディング支援ツールなどの機能を支えています。

AIOps は機械学習と分析から発展し、現在は生成 AI によって機能が拡張されています。問題を検出し、システム間のイベントを関連付け、修正策を提案します。ただし、通常は人間が結果を解釈し、対応する必要があります。

エージェント型 AI は、定められた安全策の範囲内で自律的にアクションを実行することで、さらに一歩進んだ役割を担います。目標の達成に向けて意思決定し、アクションを実行し、状況の変化に適応します。人間は各ステップを実行するのではなく、エージェントを指揮して目標を設定します。人間が目的を設計し、エージェントが実行を担います。

Agentic Operations（**AgenticOps** と呼ばれることが増えています）は、エージェント型 AI から発展しつつある運用手法です。人間が指揮するエージェントが、ドメインを横断して状況を把握し、推論し、アクションを実行します。運用担当者が方針と安全策を設定し、エージェントが、従来は手作業で行っていたタスクを実行します。

本レポートのすべての情報は、Omdia 社が 2026 年に実施した独立調査に基づいています。北米、西ヨーロッパ、アジア太平洋地域の従業員 500 人以上の組織に所属する、IT およびネットワーク運用のリーダー 1,000 人を対象にアンケートを実施しました。また、2025 年 10 月から 2026 年 4 月までの AI との直接通信によるネットワークトラフィックを追跡した、集約テレメトリデータのシスコによる分析結果も含まれています。

©2026 Cisco and/or its affiliates. All rights reserved.