HyperFRAME RESEARCH

調査概要

Cisco AgenticOps :

自律型ネットワーキングとクロスドメイン インテリジェンスによるグローバルレジリエンスの再構築

2026 年 3 月

執筆者 :
Ron Westefall
インフラストラクチャおよびネットワーキング担当 VP 兼プラクティスリーダー

エグゼクティブサマリー

組織のネットワーク運用（NetOps）は、単なるデバイス管理から、AI が駆動する分散型の機能群全体を管理・監督する役割へと進化しています。静的環境と線形的成長を前提とした既存の運用フレームワークは、機能不全に陥っているのです。今日の NetOps は急激に複雑化しています。運用対象は数百万もの一時的なクラウドエンティティと数十億台に及ぶ OT/IT エッジデバイスに広がっており、生成されるテレメトリの量は人間が処理できる範囲をはるかに超えています。エンジニアが手作業でログを調査する運用体制では、問題の特定や修正、サービス停止の防止に時間がかかりすぎます。ネットワークの安定性の維持、トラフィックルーティング、および脅威の軽減には、マシンスピードでの判断と制御が求められています。この変化に対応するには、受動的な監視から、人間が介入する前に状況を理解し、自律的に修正できるシステムへと移行する必要があります。それがシスコの AgenticOps です。

シスコの AgenticOps は、さまざまなレベルの自律性を持つ AI エージェントを企業全体で管理・拡張するためのフレームワークであり、IT 環境内で自律型 AI エージェントを展開、管理、監視、統制するための運用規律を提供します。このフレームワークにより、エージェントはインフラストラクチャを監視し、問題について推論し、人間の介入を最小限に抑えながら是正措置を講じることができます。AgenticOps は、エージェントのライフサイクル全体を対象に、信頼性、安全性、説明責任を維持するための基盤を提供します。また、ガバナンス、透明性、制御機能を備えており、運用中のエージェントの自律的な動作や実行状況を監督できます。

シスコの AgenticOps は、IT 運用（AIOps）のさらなる進化形です。エージェントファーストの設計思想のもと、目的特化型の自律的なアクションと監督機能を融合することで、人間とエージェントが協調して動作するマルチプレーヤー環境を実現します。AgenticOps は、AIOps を上回る次のような重要な特長を備えています。

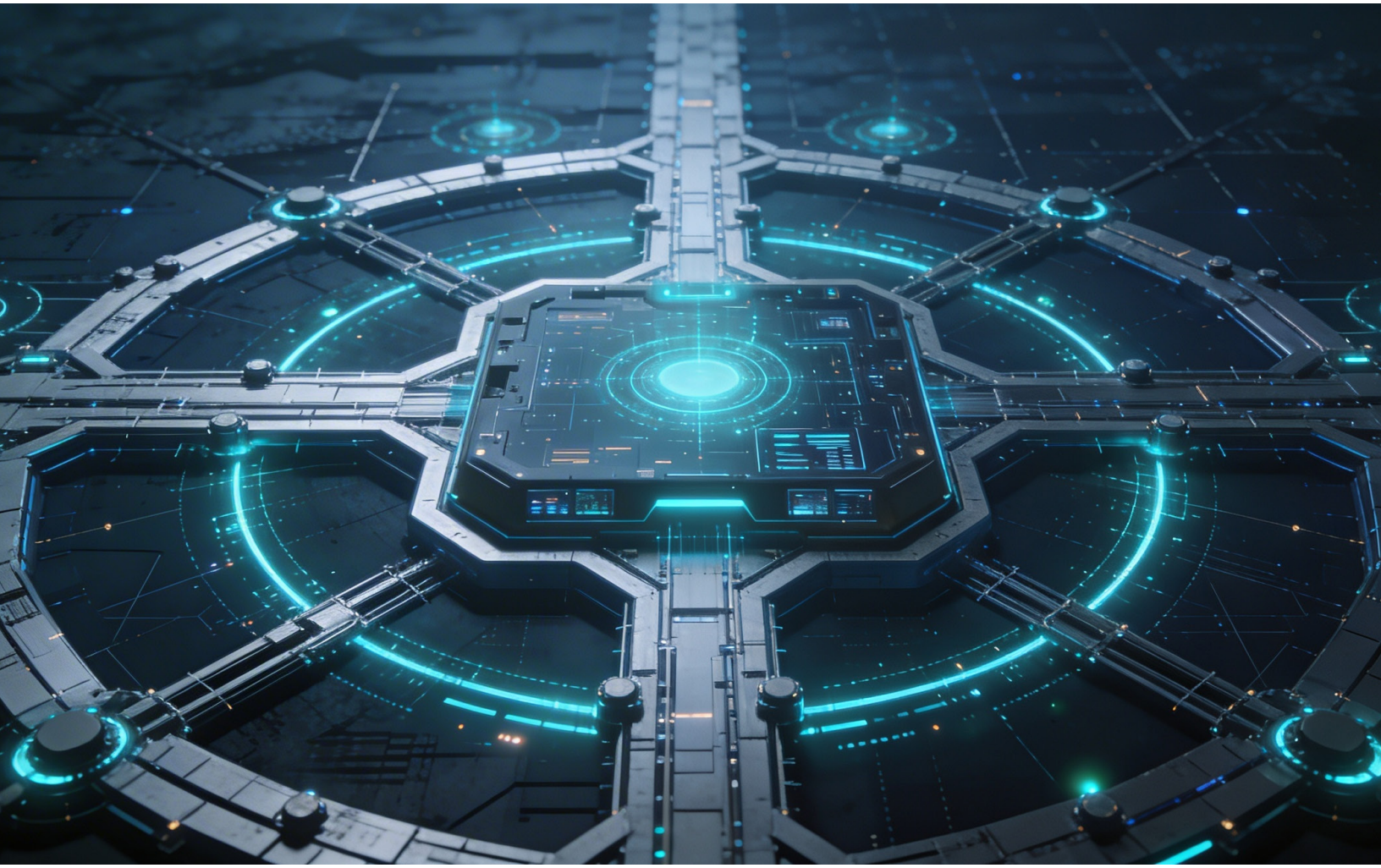
- AIOps は、生成 AI と機械学習を活用して異常を検出し、関連するイベントの相関分析を行います。推奨事項の解釈、自動化スクリプトの作成、修正の承認・実行は人間のオペレータが行う必要があります。
- AgenticOps はさらに一歩進み、企業が AI エージェントを安全かつ確実に展開できるようにします。これらの AI エージェントは、問題を自律的に推論し、さまざまなソフトウェアおよびハードウェアプラットフォームにまたがる複雑なマルチステップタスクを、マシンスピードで完了できます。AgenticOps は IT 運用に自律性をもたらし、人間の能力とスキルを強化します。推論、シミュレーション、クローズドループ実行を組み合わせることで、ネットワークをリアクティブ（事後対応型）なシステムから、プロアクティブ（事前対応型）で自己最適化するシステムへと変革します。

これは、日常業務において、終わりのないダッシュボード監視や手作業によるチケットルーティングから脱却することを意味します。AgenticOps では、エンジニアがネットワークのボトルネックに関する通知を受け取って問題を特定する前に、エージェントがあらゆる依存関係を継続的に監視し、推論を行います。ローカルデバイスからクラウドに至るまで、エージェントが問題を即座に検出し、修正を実行します。AgenticOps は、運用ドメイン間のサイロを解消し、サービス全体のエクスペリエンスを最大限に向上させます。

重要なのは、AgenticOps フレームワークが組織の既存のワークフローに根ざしていることです。自律的な運用は、一朝一夕に実現できるものではなく、またそうあるべきでもありません。人間とエージェントが協調して運用するマルチプレーヤー環境において、フレームワーク内のエージェントは、人間による承認や連携を前提とした具体的な修復ブループリントを提供します。これにより、チームはシステムへの信頼を築きながら権限を段階的に委任できるようになり、IT ライフサイクルは、絶え間ない手動介入を前提とした状態から、高い信頼のもとで自動的に監督される状態へと移行します。

この調査概要では、次の 3 つの重要なポイントを示します。

1. まず、AgenticOps が必要とされる理由です。現代のデジタル インフラストラクチャは、その複雑さが転換点に達しており、リアルタイムのテレメトリと効果的な修復との間のギャップを埋めるためには、マシンスピードでの自律的な実行が不可欠になっています。
2. 第 2 のポイントは、シスコの AgenticOps フレームワークが、トラブルシューティング、最適化、検証に特化したエージェント機能で構成されるエージェント型ワークフォースを展開することで、ネットワークをサイロのない自律的な環境へと変革する点です。これらのエージェントは、クロスドメインテレメトリと 40 年にわたって蓄積・体系化された専門知識を活用し、IT チームと協働するパートナーとして機能します。
3. 最後に、シスコが NetOps 向け AgenticOps の優れたプロバイダーである理由を考察します。その理由は、シスコが緊密に統合された独自の多層 AI アーキテクチャを備えていることにあります。このアーキテクチャが、完全なクロスドメイン実装を通じて運用を合理化し、価値実現までの時間を短縮します。結びとして、意思決定者が戦略を段階的な実行へと落とし込むための実践的なアクションプランを示します。



戦略上の必須事項：AgenticOps が必要な理由

AgenticOps：従来の AIOps では不十分

従来の AIOps ソリューションには機能的な限界があります。まず、異常を検知してアラートを生成する機械学習が登場しました。次に生成 AI が登場し、問題を説明して解決策を推奨するようになりました。続いて登場したのが AIOps プラットフォームです。AIOps プラットフォームは、ネットワーキングやセキュリティなどの個別の機能サイロ内でテレメトリを収集し、イベント間の相関分析を行い、アラート機能を改善するように設計されています。AIOps はノイズの低減には効果を発揮しますが、運用モデルを変えるものではありません。問題解決の中心は依然として人間であり、分断されたドメインやインサイトの間のギャップを人手で埋める必要があります。

現在のインフラストラクチャの現実として、障害やパフォーマンスの低下が単一のレイヤのみに起因することはほとんどありません。むしろ、ネットワーク、クラウド、セキュリティプロトコル、アプリケーションスタックの間で生じる複雑な相互作用から発生するのが一般的です。従来の AIOps は依然として大部分がサイロ化され、監視中心の仕組みであるため、クロスドメインの問題が発生すると、チームは手作業による相関分析や対策チームの設置を余儀なくされます。AIOps はシステムの異常を検出しますが、その後の推論は人間に委ねられています。このような人間主導の障害対応への依存は、アラート疲れを招き、平均修復時間 (MTTR) の長期化につながります。

たとえば AIOps は、トラフィックの急増を一般的な「CPU 使用率が高い」という通知で知らせるような、構造化データやしきい値ベースのアラートへの対応に限定されています。一方、AgenticOps は、LLM を活用したツール強化型プランニングにより、人間のような推論を用いて運用スタック全体を横断的に分析します。自律型エージェントは、エンジニアにアラートを通知するだけでなく、マーケティングワークフローの可視化情報を照会して販売状況を確認し、社内のドキュメントリポジトリから特定のプロモーション向けスケーリングランブックを取得し、必要なスクリプトを実行してリソースを拡張したうえで、最終的にチームのメッセージングチャネルで対応内容全体を要約することで、根本原因を調査できます。こうした変化により、システムは過去のパターンを受動的に観察する存在から、クロスプラットフォームの調査やエンドツーエンドのタスク実行を行える能動的な参加者に変わります。つまり、AIOps は今日のデジタル NetOps が求める要件に対応できるだけの拡張性を備えていないモデルなのです。

AIOps と AgenticOps : 運用上の影響における主な違い

NetOps アクティビティ	従来の AIOps	AgenticOps
監視と監督	エンジニアが手動でダッシュボードを監視し、アラートに対応します。	エージェントがシステムを継続的に監視し、人間は監督的な役割に移行します。
変更管理	システム変更には手動での実施と人間による監視が必要です。	エージェントが、安全なパラメータの範囲内で、自律的に変更の計画、シミュレーション、実行を行います。
トラブルシューティング	人間主導の調査。エンジニアがログを詳しく調べ、根本原因を特定します。	エージェント主導の診断。エージェントが問題を特定し、解決策を推論したうえで、人間による検証を経て、または検証なしでアクションを実行します。

出典 : HyperFRAME Research 社

AgenticOps は、インテリジェントなアクションを優先することで、AIOps とは明確に一線を画します。AgenticOps は、自己修復環境という概念を実際の運用で実現するものであり、エージェント AI を使用して障害を予測し、パフォーマンスの低下やさらに深刻な事態がネットワーク全体へ波及する前に是正措置を講じます。受動的な監視からマシンスピードの実行へ移行することで、組織はインフラストラクチャ負債の解消を優先できるようになると同時に、人間主導の対策チームではデジタルディスラプションや障害の発生ペースに対応しきれないことによって生じる業務停止時間の削減・解消も可能になります。

AgenticOps を企業レベルで導入できる体制を整えるには、まず以下の点に取り組む必要があります。

1. 自律型エージェントに関する明確な説明責任、監査可能性、およびヒューマンインザループのガードレールを定義したガバナンスフレームワークを確立します。

2. モジュール式のデータ主導型アーキテクチャを優先し、段階的アプローチ（Crawl - Walk - Run）を採用することで、既存のワークフローやシステム全体にわたって、高品質なデータファブリックと低遅延の統合を実現します。

3. ドメイン固有のインテリジェンスと、クロスドメインの統合テレメトリ、ヒューマンインザループのガバナンスを組み合わせたエンドツーエンドの AgenticOps フレームワークを採用することで、準備態勢を整え、スキル不足に対応し、導入を容易にします。

ツールからチームメイトへ：シスコのエージェント型ワークフォースの台頭

AgenticOps は、AI を自律的なデジタルピアからなる高度なワークフォースへと進化させます。シスコは、このプラットフォームに目的特化型の CCIE レベルのロジックを組み込むことで、基本的な自動化の枠を超え、積極的なコラボレーションを実現する常時稼働の機能を提供します。そのエージェント機能は、高度な運用インテリジェンスを活用してネットワークをプロアクティブに管理し、人間が開始する調査から、ディープシンキングによる継続的な環境評価まで、柔軟なレベルの自律性を提供します。こうした変化は、AI を人間のオペレータと一緒にネットワークを運用する協働パートナーへと位置付ける大きな転換を意味し、AI と人間の専門知識が融合してネットワークをオーケストレーションするエージェント型パートナーシップを形成します。

シスコはこのほど、運用の簡素化と AI 主導のソリューションを優先し、自律的でサイロのないネットワークへの移行を推進する AgenticOps フレームワークの次世代版を発表しました。この進化の中心となるのが、最小限の手動介入でネットワーク環境を運用できるよう設計された、トラブルシューティング、最適化、検証のための拡張エージェント機能の導入です。これらのエージェント機能は、AI 機能強化とともに、Cisco AI Assistant、Cisco Agentic Workflow、Cisco Cloud Control プラットフォーム、AI Canvas（近日提供予定）などの一般的な IT インターフェイス、およびサードパーティ製アプリケーションに統合されています。

シスコのエージェント型ワークフォース：エージェント機能

エージェント機能	主な役割	主な機能	高度なツール
自律的トラブルシューティング	インシデント対応（検出から解決まで）	テレメトリを基に根本原因を推論し、複数の仮説を同時に検証するとともに、CCIE レベルの精度で確実な修復を実行します。	AI パケットキャプチャ（数千のシグナルをリアルタイムで相関分析）
継続的な最適化	継続的な改善（パフォーマンスと効率）	エンドツーエンドのネットワーク状態をリアルタイムで把握し、RF、QoS、通信経路、コントロールプレーンを自律的に調整することで、ユーザー体験を継続的に維持します。	AI 設定推奨事項（予測可能な運用を実現するためのプロアクティブな調整）
信頼検証	変更の安全性（意図から結果まで）	リスクを考慮したエージェント型評価により、ライブトポロジ、設定、テレメトリに基づいてネットワーク変更を検証し、その影響や影響範囲を特定します。	影響モデリング（変更がシステム全体にどのような影響を及ぼすかを推論）

出典：HyperFRAME Research 社

このエージェント型ワークフォースの第 1 弾は、自律型トラブルシューティングです。インシデントの検出から解決までを責任を持って担うことが主な役割です。これらの機能は、ネットワーキング、セキュリティ、インターネットの各レイヤからのテレメトリをリアルタイムで相関分析し、ドメイン横断的に問題を調査、推論、解決します。仮説に依存するのではなく、シグナルを大規模に分析して根本原因を特定し、修復手順を推奨または実行します。この機能は、AI パケットキャプチャなどの新しいツールによって強化されており、エージェントは数千のシグナルを同時に処理し、信頼性の高い証拠と説明を数分で提供できるようになります。

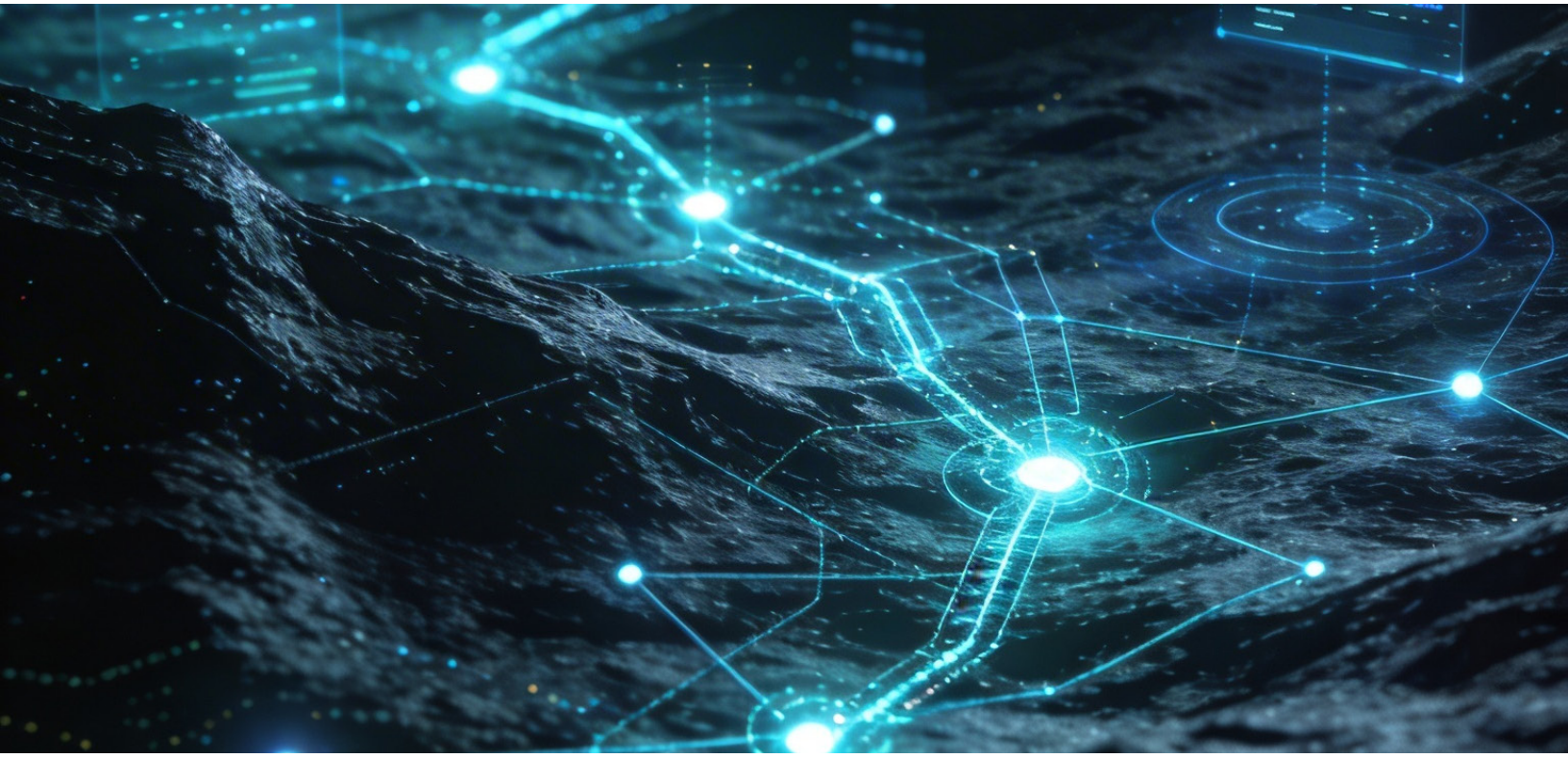
ネットワークの正常性を支えるのが、継続的最適化エージェント機能です。これは、パフォーマンスと効率の継続的な改善に重点を置くデジタルオペレータです。これらのエージェント機能はプロアクティブに動作し、ワイヤレス、スイッチング、WAN 環境全体における設定のばらつきを検出するとともに、ユーザーに影響が及ぶ前にパフォーマンス低下を予測します。また、サポートチケットを待つのではなく、新たなリスクパターンを認識し、定義されたガードレールの範囲内で環境を調整します。現在、予測可能なネットワークパフォーマンスをプロアクティブに確保するよう設計された AI 設定推奨事項など、スキルの拡張が行われています。

エージェント型ワークフォースの次の構成要素は、ネットワーク変更をより安全かつ予測可能にする役割を担う信頼検証エージェント機能です。この機能は、変更が発生する前にその潜在的影響と影響範囲をモデル化し、隠れた依存関係や下流のリスクを明らかにします。変更が実装されると、エージェントはその結果を自動的に検証するとともに、その結果から学習し、今後のアクションを改善します。これらの機能は、変更がシステム内でどのように伝播するかを推論することで、すべての更新が意図しない影響を伴うことなく、ネットワークを本来意図した状態へと近づけることを保証します。

シスコのエージェント機能は、必要な自律性レベルに応じてさまざまなモードで動作できる柔軟性を備えています。

1. オンデマンド機能は、人間によってトリガーされ、顧客の特定の問題の解決など、明確な目標に焦点を当てています。
2. アンビエントエージェント機能は常時稼働し、Wi-Fi の最適化やポリシーのばらつきの修正といった継続的な目標を追求します。
3. ディープシンキングモードは、環境全体の検証や大規模な計画策定など、長期にわたる複雑な目標を処理します。

長期的には、シスコのエコシステムにおけるすべてのエージェント機能がこれら 3 つのモードすべてに対応し、IT チームのための包括的かつ適応性のあるサポートシステムになることが予想されます。



テレメトリから信頼へ：Cisco AgenticOps の基盤アーキテクチャ

シスコのエージェントフレームワークは、クロスドメインテレメトリをはじめとする、戦略的アーキテクチャの 4 本の柱に基づいて構築されています。シスコのエージェントテクノロジーは、キャンパス、ブランチ、WAN、データセンター環境に加え、セキュリティレイヤおよびアプリケーションパスを網羅する、業界でも最も広範なテレメトリセットの 1 つを活用していることが分かっています。この包括的なエンドツーエンドの監視ポイントにより、エージェントはシステム全体にわたって推論とアクションの実行が可能となり、個別のデータポイントではなくネットワーク全体の範囲に基づいたインサイトが得られるようになります。

第 2 の柱の焦点は、アンサンブルモデルとシスコの体系化された専門知識であり、これらにより汎用 AI を専門的な運用インテリジェンスへと変換します。フロンティアモデルと基盤モデルを Deep Network Model などの目的特化型モデルと組み合わせることで、シスコのエージェント機能は Cisco Certified Internetwork Expert（CCIE）のナレッジパックおよび人間が厳選したランブックに基づいたものとなります。このようなさまざまなモデルの組み合わせにより、迅速な対応、きめ細かなトラブルシューティング、複雑なアーキテクチャ課題の解決のいずれが求められる状況であっても、タスクに応じてシステムが適切なツールを選択できるようになります。

これらのアクションが安全に実行されるよう、第 3 の柱ではツール、ガードレール、信頼を設計段階から統合しています。シスコのエージェント機能はやみくもに動作するわけではなく、MCP と API を使用してデータを収集しつつ、明示的なガードレールと顧客が定義した承認モデルの範囲内で動作します。透明性を維持するため、すべてのアクションには明確な論拠、証拠、および完全な監査証跡が付随します。シスコでは、信頼は単なる機能ではなくシステムの基本特性として扱われており、IT チームが自動化された実行を常に制御できるようにしています。

このアーキテクチャの最後の柱はマルチモーダル インタラクションです。これは、IT チームが AI との関わり方に柔軟性を必要としているという認識に基づいています。シスコは単一のインターフェイスを強制するのではなく、既存の GA ダッシュボードや AI Assistant、AI Canvas などの新しいプラットフォーム、メッセージングシステム、ServiceNow などのサードパーティ製ツールといったさまざまなタッチポイントを通じてエージェント機能を提供しています。イベント駆動型アラートやサードパーティのインターフェイスと統合することで、このシステムは現代の IT 組織における既存のワークフローに適応し、チームが最も生産性を発揮できる環境で機能を提供できるようになっています。

シスコのエージェントフレームワーク（NetOps 向け）：4 本の戦略的柱

柱	主要目標	主な機能	重要な理由
クロスドメインテレメトリ	可視性とコンテキスト	キャンパス、ブランチ、WAN、データセンター、セキュリティ、アプリケーションパス全体を網羅します。	エージェントがシステム全体で推論できるようにすることで、サイロ化を解消します。
アンサンブルモデルと専門知識	運用インテリジェンス	フロンティアモデルに、専用の Deep Network Model と CCIE ナレッジパックを組み合わせます。	汎用 AI を超え、専門的かつエキスパートレベルのトラブルシューティング ロジックを実現します。
ツール、ガードレール、信頼	安全な実行	明示的なガードレールの範囲内で MCP/API を使用し、推論と監査証跡を提供します。	AI が「やみくもに動作」することを防ぎ、人間のオペレータが主導権を維持できるようにします。
マルチモーダル インタラクション	ワークフローの統合	ダッシュボード、AI Assistant、AI Canvas、メッセージングからアクセスできます。	単一のインターフェイスを強制するのではなく、IT チームの業務の進め方に適応します。

出典：HyperFRAME Research 社

Cisco Edge : AgenticOps による自律型ネットワーキングの未来の保護

シスコの AgenticOps フレームワークは、顧客の多様なニーズに合わせてインテリジェンスを最適化することで際立っており、以下を特徴とします。

1. **Deep Network Model :** 40 年以上にわたるシスコの知的財産でトレーニングされた専用の大規模言語モデル (LLM) が、ネットワーク運用の基盤となるロジックを解釈し、ライブテレメトリと直接統合することでリアルタイムのインサイトを提供します。
2. **クロスドメインスコープ :** ネットワーク、セキュリティ、コラボレーションにまたがるシスコのすべてのワークロードを統合的に可視化します。
3. **データ基盤 :** Splunk (セキュリティとログ)、ThousandEyes (インターネットおよび SaaS の可視化)、Meraki (クラウドネットワーキング) の機能を活用して構築された大規模なデータレイクです。
4. **コネクテッド エージェント インテリジェンス:**シスコのプラットフォームおよびソリューション全体でネットワーク、セキュリティ、コラボレーションの各テクノロジーを統合し、連携させることにより、エージェントとツールが情報をシームレスに共有し、リアルタイムで連携できるようにします。

シスコの Deep Network Model により、エージェントは広範な運用インテリジェンスに基づいて動作できます。競合他社がワイヤレス診断やデータセンター自動化というサイロ内で運用することが多いのに対して、シスコのエージェント機能は、Splunk、ThousandEyes、Meraki の機能を活用して構築された大規模なデータレイクを活用します。その結果、AgenticOps フレームワークは単純なパターン認識のレベルを超え、CCIE レベルのロジックを使用して、ユーザーのデバイスからクラウドアプリケーションに至るまで、エンタープライズスタック全体にわたって複雑な自律的アクションを実行できるようになります。このモデルは、3,000 を超える推論トレースによってさらに高度化されています。推論トレースとは、専門家が導き出したロジックパスであり、AI が統計的な推測に依存するのではなく、専門家による診断手順を模倣できるようにするものです。

シスコの AgenticOps フレームワークを HPE Juniper 社や Arista 社のソリューションと差別化しているのは、Splunk プラットフォームによるデータ基盤です。シスコのエージェントは、パケットライフサイクル全体にわたるクロスドメインのコンテキストで動作します。シスコは、Meraki、ThousandEyes、Splunk の広範なセキュリティおよびログデータファブリックから得られるリアルタイムテレメトリを統合し、一元的な AI Canvas を実現しています。これにより、エージェントは、ホーム Wi-Fi 接続からパブリックインターネット、さらにクラウドネイティブ アプリケーションのバックエンドに至るまで、ユーザー体験を追跡できるだけの可視性を得ることができます。

このテレメトリにより、シスコは競合他社によく見られる、サイロ化された単一ドメインの診断を超えた対応が可能になります。シスコ環境下の自律型エージェントは、アプリケーション パフォーマンスの低下を特定のセキュリティアップデートや地域の ISP の障害と関連付けることができるため、内部ネットワークのみに焦点を当てているベンダーでは把握できない根本原因を特定できます。この包括的なデータ基盤により、シスコのエージェントは、トラフィックの再ルーティングやセキュリティポリシーの調整などのアクションを実行する際に、ビジネスへの影響を総合的に把握したうえで判断できます。その結果、Arista 社や HPE Juniper 社には実現が難しいレベルのフルスタック運用インテリジェンスを提供できます。

最後に、シスコはクロスドメインのコネクテッド エージェント インテリジェンスを活用することで、エージェントがネットワーキング、セキュリティ、Webex などのコラボレーションツールの領域をまたいで連携し、手動によるハンドオフなしに問題を解決できるようにしています。このレベルの統合は、より限定的なポートフォリオに注力している HPE Juniper 社や Arista 社などの競合他社には実現できません。この水平統合により、エンドユーザーに影響が及ぶ前に、さまざまな部門やテクノロジースタックにまたがるパフォーマンス問題を軽減できます。たとえば遅延を特定したネットワークエージェントは、Webex エージェントと自動的に連携して通話品質を改善したり、セキュリティエージェントをトリガーして侵害されたデバイスを隔離したりできます。これらはすべて、IT 部門間での手動による介入やハンドオフなしに行われます。

シスコは、堅牢な説明可能性と組み込みの安全対策を提供することで、AI の安全性と信頼性を重視する姿勢を示しています。信頼性を確保するため、システムはすべてのエージェントのアクションについて透明性の高い推論を提供し、次のことを可能にしています。

- **AI によるハルシネーションの軽減 :** すべての自律的なアクションには、結論に至るまでに使用された具体的なデータとロジックを説明する推論経路「Chain of Thought (思考の連鎖)」が伴います。
- **ロールバックの自動化 :** 意図しない影響からネットワークを保護します。このフレームワークには、AI による変更によってパフォーマンスの低下が発生した場合に設定を直ちに元に戻す自動ロールバックメカニズムが組み込まれており、自動最適化中でも高い可用性を確保できます。

以上から、シスコはネットワーキング、セキュリティ、アプリケーションの各プラットフォーム間のギャップを埋めることができる唯一のベンダーとして、独自の競争優位性を確立していると言えます。

競合他社との比較：シスコ vs. 競合他社

機能	Cisco AgenticOps	HPE Juniper 社 / Arista 社
インテリジェンスエンジン	**Deep Network Model :** 40 年以上にわたるシスコの知的財産と CCIE の知見に基づいてトレーニングされています。	汎用モデルまたはサイロ化された AIOps でパターンマッチングを行います。
データの範囲	**クロスドメイン :** ネットワーキング、セキュリティ、コラボレーション（Webex）を統合しています。	主に、内部ネットワークまたはワイヤレスのサイロに焦点を当てています。
データ基盤	**Splunk + Meraki + ThousandEyes :** 自社所有ネットワークと外部ネットワークにまたがる大規模な「データ基盤」です。	独自のハードウェアテレメトリまたは特定のクラウドツールに限定されます。
エージェント間同期	**水平統合 :** あるドメインのエージェントが他のドメインのエージェントと連携し、手動によるハンドオフなしで問題を解決します。	垂直的なサイロ：複数の IT 部門間で手動によるハンドオフが必要です。

出典：HyperFRAME Research 社

シスコのポートフォリオの優位性: AgenticOps による自律型エンタープライズの開拓

シスコの主な強みは、ネットワーク管理を手作業中心の運用から自動化された統合デジタルシステムへと移行する革新的な AgenticOps フレームワークにあると考えられます。この進化を主導するのは、トラブルシューティング、最適化、検証を担う AI エージェント機能からなる専門チームです。このチームは、デジタル CCIE として、インシデントの解決から変更の安全性確保まで、あらゆる業務を担います。エンドツーエンドのアーキテクチャは、AgenticOps の基盤となるシスコの 4 本の主要な柱によって支えられています。

1. 広範なクロスドメインテレメトリ
2. エキスパートの知見に基づいたモデルのアンサンブル
3. 厳格な信頼のガードレール
4. シスコの AI Assistant や AI Canvas などの柔軟なマルチモーダル インターフェイス

シスコは AgenticOps の導入戦略の成功に欠かせない信頼できるパートナーとして確固たる地位を確立していると考えられます。シスコは、診断精度を確保する Deep Network Model と、Splunk の大規模データファブリック、さらに Meraki と ThousandEyes のテレメトリを組み合わせることで、競合他社では容易に実現できないネットワーク全体の一元的な可視化を実現しています。シスコのエージェント機能は非常に汎用性が高く、オンデマンド、アンビエント、ディープシンキングの各モードで動作し、各組織のさまざまな運用ニーズと自律性レベルに対応します。

企業の 68% が毎年基盤モデルの刷新を計画する中で [1]、Cisco AgenticOps は競合他社に対して大きな優位性を発揮します。コアビジネスロジックに影響を与えたり、技術的負債を蓄積したりすることなく、AI エンジンをシームレスに切り替えられるためです。さらにシスコの AgenticOps は、追跡可能でエージェントから呼び出し可能な API と、自律的アクションの統制と信頼性を確保する安全ガードレールを提供することで、調査回答者の 90% が抱くハルシネーションやセキュリティに関する懸念 [1] に直接対処します。

総括すると、自律的なネットワーク運用への移行は段階的に進めることをお勧めします。AgenticOps は、ほとんどの企業で段階的アプローチ（Crawl - Walk - Run）によって導入されると予想されます。まず、エージェント支援による診断と人間の承認を伴う修復から始まり、次に、明確なロールバックパスを備えた、十分に理解された低リスクのアクションに対するクローズドループ実行へと拡張します。そして、システムへの信頼が高まるにつれて、より自律的なエージェント主導の運用へと移行していきます。やがて、AgenticOps のガバナンス制御、監査可能性、影響範囲の封じ込めは、AI そのものと同じくらい重要になると考えられます。

1 (HyperFRAME Research Lens: 1Q 2026)

AgenticOps への移行と評価に関する推奨事項

- **AgenticOps を活用した戦略的変革の推進：**CTO、CIO、インフラストラクチャ / 運用担当 VP、ネットワーク運用（NetOps）担当 VP、セキュリティ運用（SecOps）担当 VP、クラウド /IT 戦略担当ディレクタ、チーフアーキテクトなどの主要な意思決定者は、シスコの AgenticOps フレームワークの評価を優先する必要があります。なぜならこのフレームワークは、AI を単なる生産性向上ツールから、複雑な環境を大規模に、自律的にトラブルシューティング、最適化、検証できる専門エージェントで構成されたエージェント型ワークフォースへと変革するからです。40 年にわたって体系化されたネットワーキングの専門知識と、NetOps、SecOps、クラウド領域にわたる統合テレメトリを活用することで、このフレームワークは運用上のリスクを大幅に軽減し、解決までの時間を短縮すると同時に、透明性の高い信頼ベースのガードレールによって人間による監督を維持します。
- **包括的な自律型 NetOps の重視：**組織は、Cisco AgenticOps フレームワークの採用を検討する必要があります。なぜならこのフレームワークは、複雑なネットワーク環境全体で、自律的なトラブルシューティング、プロアクティブなパフォーマンス最適化、リスクを考慮した変更検証を実行できる包括的なエージェント型ワークフォースを提供し、チームの能力向上に直接貢献するからです。エージェントは、オンデマンド支援からディープシンキングによる計画立案まで、さまざまな実行モードで動作し、リアルタイムテレメトリを活用してインシデントを解決するとともに、ユーザーに影響が及ぶ前に問題を未然に防ぎます。
- **信頼を重視したエージェントフレームワークの採用を優先：**AgenticOps における信頼できるアドバイザーとして、シスコを検討すべきです。なぜならシスコのフレームワークは、40 年に及ぶ専門知識とクロスドメインテレメトリを活用しており、人間が厳選した専門的な運用インテリジェンスに基づいて自律的なアクションが実行されるようになっているからです。また、シスコの AgenticOps フレームワークは、明確なガードレールとマルチモーダル インターフェイスを採用することで、透明性と制御性を重視しています。そのため、すべてのエージェントのアクションが監査可能であり、確立された IT ワークフローに沿っていることが保証されます。

HYPERFRAME RESEARCH について:

HyperFRAME Research は、ハイパースケールのパブリッククラウドからメインフレーム、その間のあらゆるテクノロジー領域に至るまで、テクノロジーの世界市場に関する詳細な調査と洞察を提供しています。戦略アドバイザリサービス、カスタム調査レポート、個別のコンサルティングサービス、デジタルイベント、市場参入計画の策定、メッセージテスト、リード創出プログラムなど、サービス内容は多岐にわたります。

当社の業界アナリストは、あらゆる業界のテクノロジーソリューション、ビジネス課題、市場動向、エンドユーザーニーズに関する、厳密な定性的・定量的評価を専門としています。HyperFRAME Research は、アナリスト対応、製品、マーケティングといったお客様の各チームと緊密に連携し、お客様のソートリーダーシップの構築と強化を支援するとともに、お客様の専門性を効果的に訴求することで、ブランドおよび製品の認知度向上に貢献します。読者、視聴者、リスナーの心をつかむコンテンツを通じて、お客様のメッセージがあらゆるチャネルで効果的に伝わるよう支援します。

お問い合わせ先:

Steven Dickens
HyperFRAME Research | CEO 兼主席アナリスト
電子メールアドレス:
steven.dickens@hyperframeresearch.com
電話番号:
+1 845 505 1678
X: @StevenDickens3
LinkedIn: Steven Dickens
BlueSky: Steven Dickens

寄稿者:

Ron Westefall
インフラストラクチャおよびネットワーキング担当 VP 兼プラクティスリーダー

お問い合わせ先

本レポートに関するお問い合わせは、HyperFRAME Research までご連絡ください。速やかに対応いたします。

引用

本書は、認定された報道機関およびアナリストによる引用が可能ですが、引用する際は、著者名、著者の役職、および「HyperFRAME Research」を明記し、文脈に沿って引用してください。報道機関またはアナリストではない場合、引用するには、事前に書面による HyperFRAME Research の許可を得る必要があります。

使用許諾

開示情報

HyperFRAME Research は、本書で言及されている企業をはじめとする多数のハイテク企業に調査、分析、アドバイス、およびコンサルティングを提供しています。同社の従業員は、本書で言及されているいずれの企業の株式も保有していません。


HyperFRAME
RESEARCH