Cisco Live !

Cisco Security Summit 2026 Tokyo:

AI エージェント時代のネットワーク戦略：
LAN・SASE を融合したゼロトラスト環境で実現する次世代ネットワークセキュリティ

次藤 則兼　(njito@cisco.com)

シスコシステムズ合同会社

ネットワーキング事業

July 2026

Opening

AIエージェントがネットワークを介して自律的に活動し、
高度なAIモデルが新たな脅威となる時代において、
ネットワークとセキュリティの分断は
致命的なリスクです。

本セッションでは、
AI時代にSASEやLANへ求められる要件を紐解きます。

AIの一般化は、Innovative(革新的)なのか、
それともParadigm shift(構造的な転換)なのか？

Geminiの回答

2026年現在の視点から見ると、ChatGPTやGemini、ClaudeなどのAIが一般化した
今の状況は、単なる革新（Innovative）というレベルを超えて、
完全に「パラダイムシフト（Paradigm shift）」の段階に達していると言える。

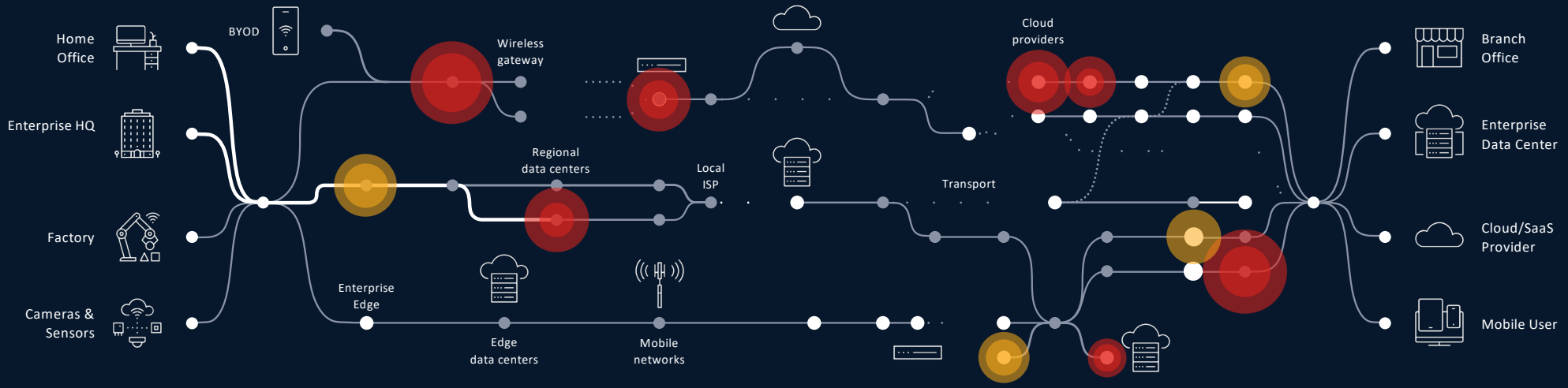
IT業界の歴史において、PCの普及、インターネットの誕生、
スマートフォンの登場に匹敵する、
あるいはそれら以上の構造転換が起きている。


本セッションのポイント
AI時代にSASEやLANに
求められる要件
ネットワークと
セキュリティの統合により
複雑化しがちな管理を
シンプルにする
Cisco Public

AI時代にSASEやLANに求められる要件

複雑さはリスクを生む

サイバー脅威、ダウンタイム、そして低いユーザー体験を改善するために、
可視性と実用的なインサイト：洞察力＝本質を見抜く力の必要性はかつてないほど高まっています。



3つの主要な課題：複雑さ、制御、可視性

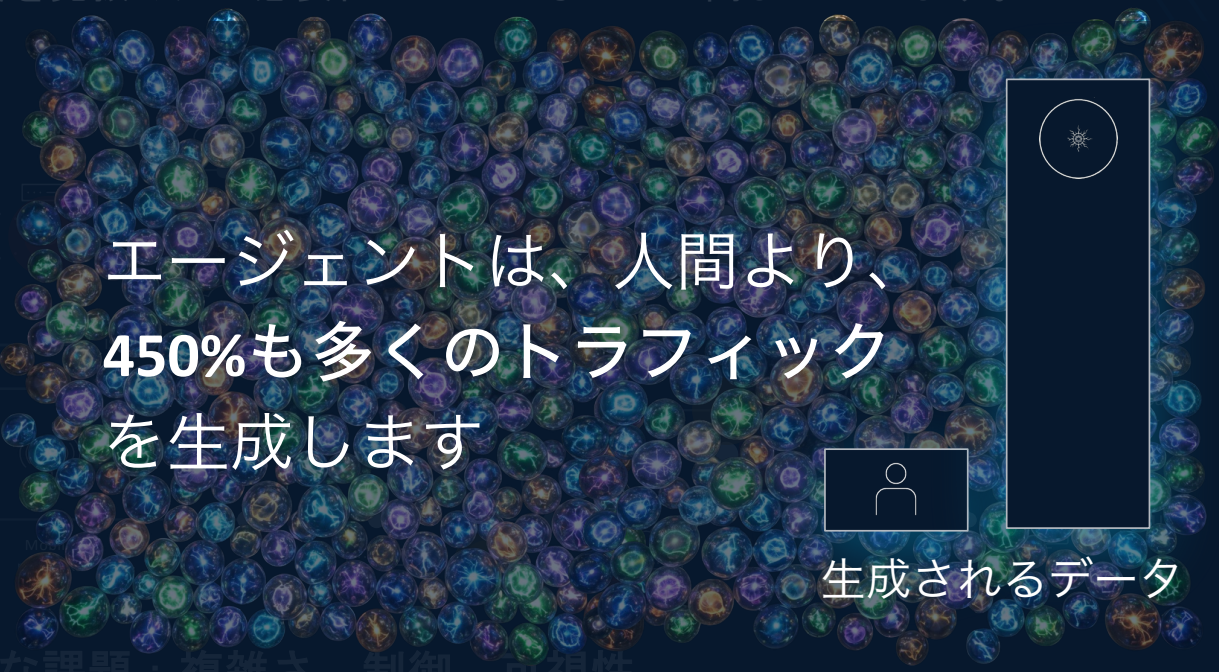
**Global 2000企業では、セキュリティとITの問題によるダウンタイムは、
直接的な費用と収益損失だけで年間4,000億ドル（およそ60兆円)の損失をもたらしています。**

複雑さはリスクを生む

サイバー脅威、ダウンタイム、そして質の低いユーザー体験から身を守るために、
可視性と実用的なインサイト：洞察力＝本質を見抜く力の必要性はかつてないほど高まっています。

数兆個のエージェント

エージェントは、人間より、
450%も多くのトラフィック
を生成します



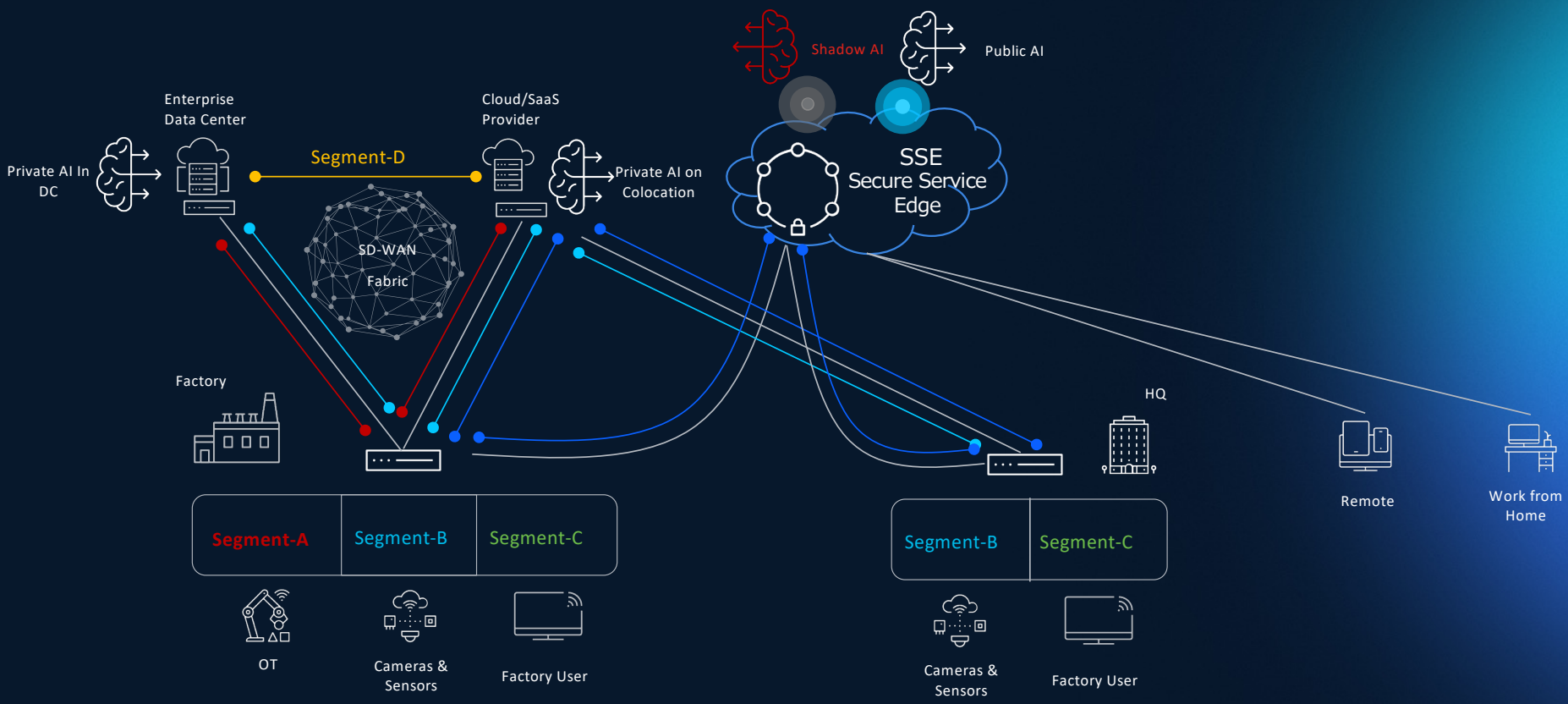
3つの主要な課題：複雑さ、制御、可視性

Global 2000企業では、セキュリティとITの問題によるダウンタイムは、
直接的な費用と収益損失だけで年間4,000億ドル（およそ60兆円)の損失をもたらしています。


AI for Network
AI-Aware Network

AI-Aware Network

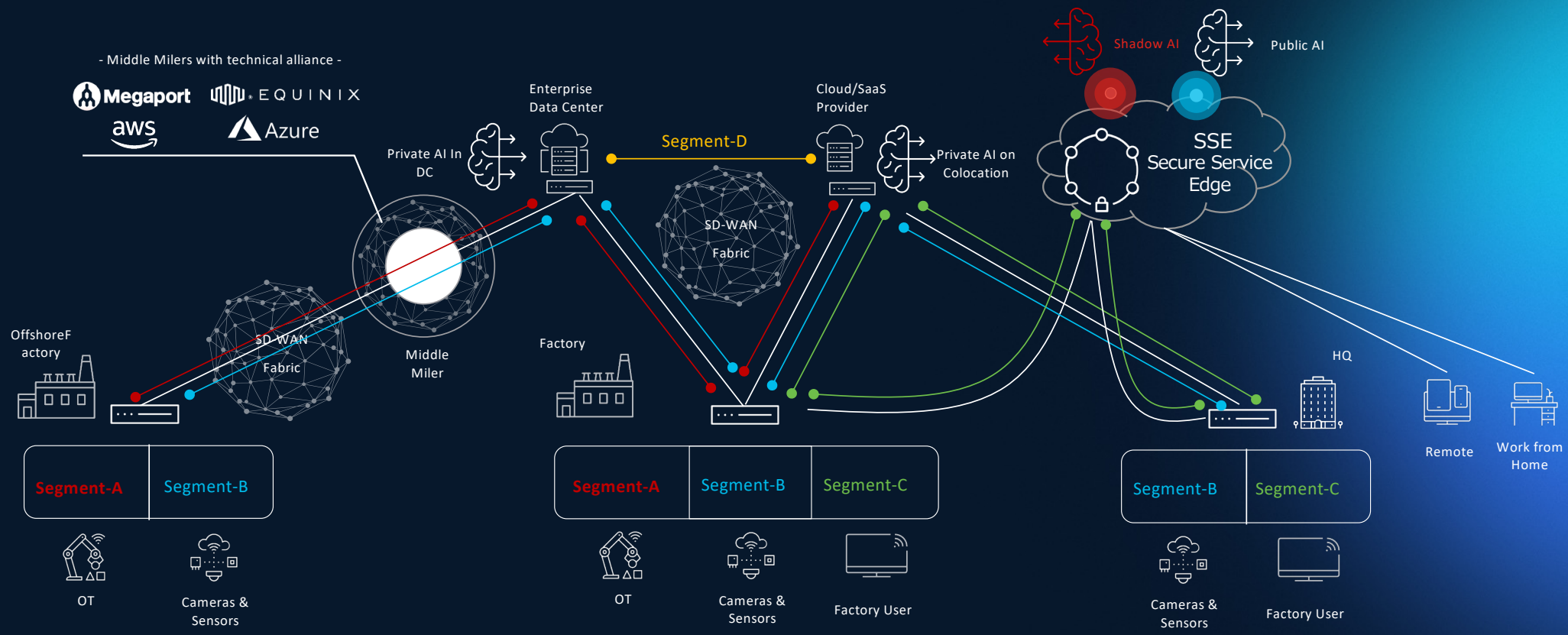
- AIを意識したネットワーク構成例#1
- リモートワーク・在宅勤務を考慮したネットワーク構成



AI-Aware Network

AIを意識したネットワーク構成例#2

グローバル・ミドルマイルを考慮したグローバルでのAIの活用

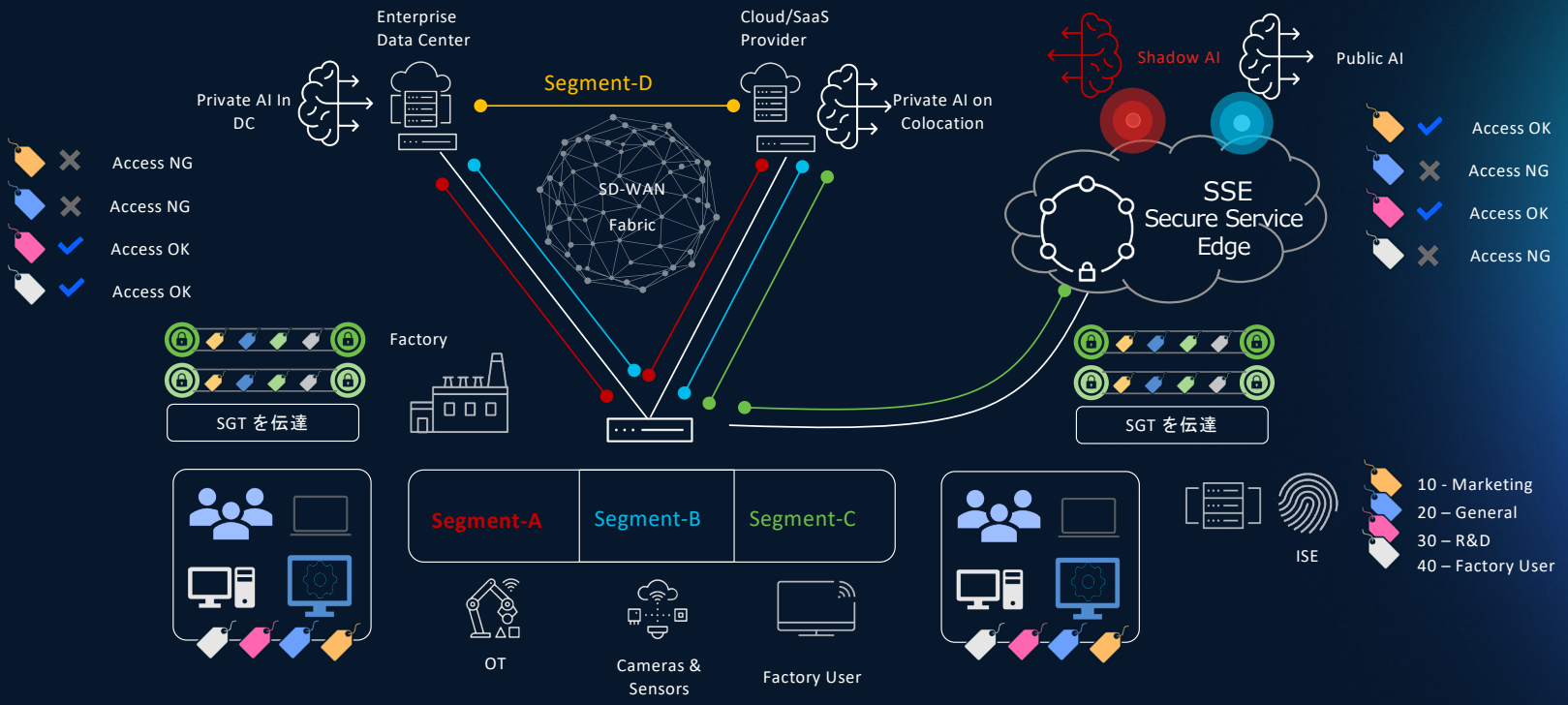


AI-Aware Network

AIを意識したネットワーク構成例#3

Common Policy(Micro Segmentation)でのアクセスコントロール

マクロセグメンテーションの中で、TAG付けを行い、
さらに小さなセクションに分割。
それぞれのセクションに独自のセキュリティポリシーを設定してアクセスできるようにする手法。



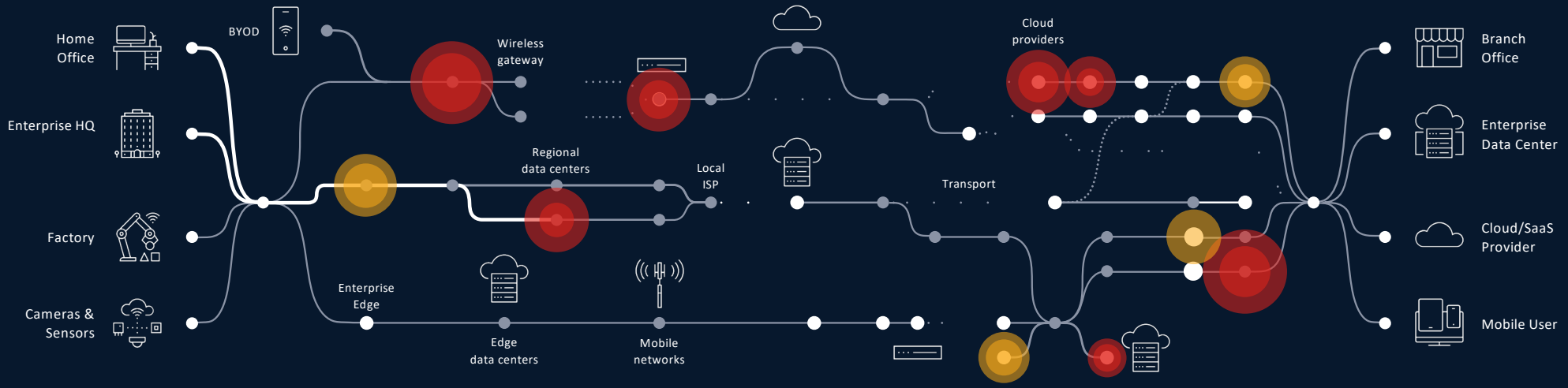
従来のACLベースでは実現できない、
属性やビヘイビアに応じたダイナミックかつ詳細なセグメンテーションとセキュリティ設定が可能。

ネットワークとセキュリティの統合により
複雑化しがちな管理をシンプルにする

AI for Network

複雑さはリスクを生む

サイバー脅威、ダウンタイム、そして低いユーザー体験を改善するために、
可視性と実用的なインサイト：洞察力＝本質を見抜く力の必要性はかつてないほど高まっています。



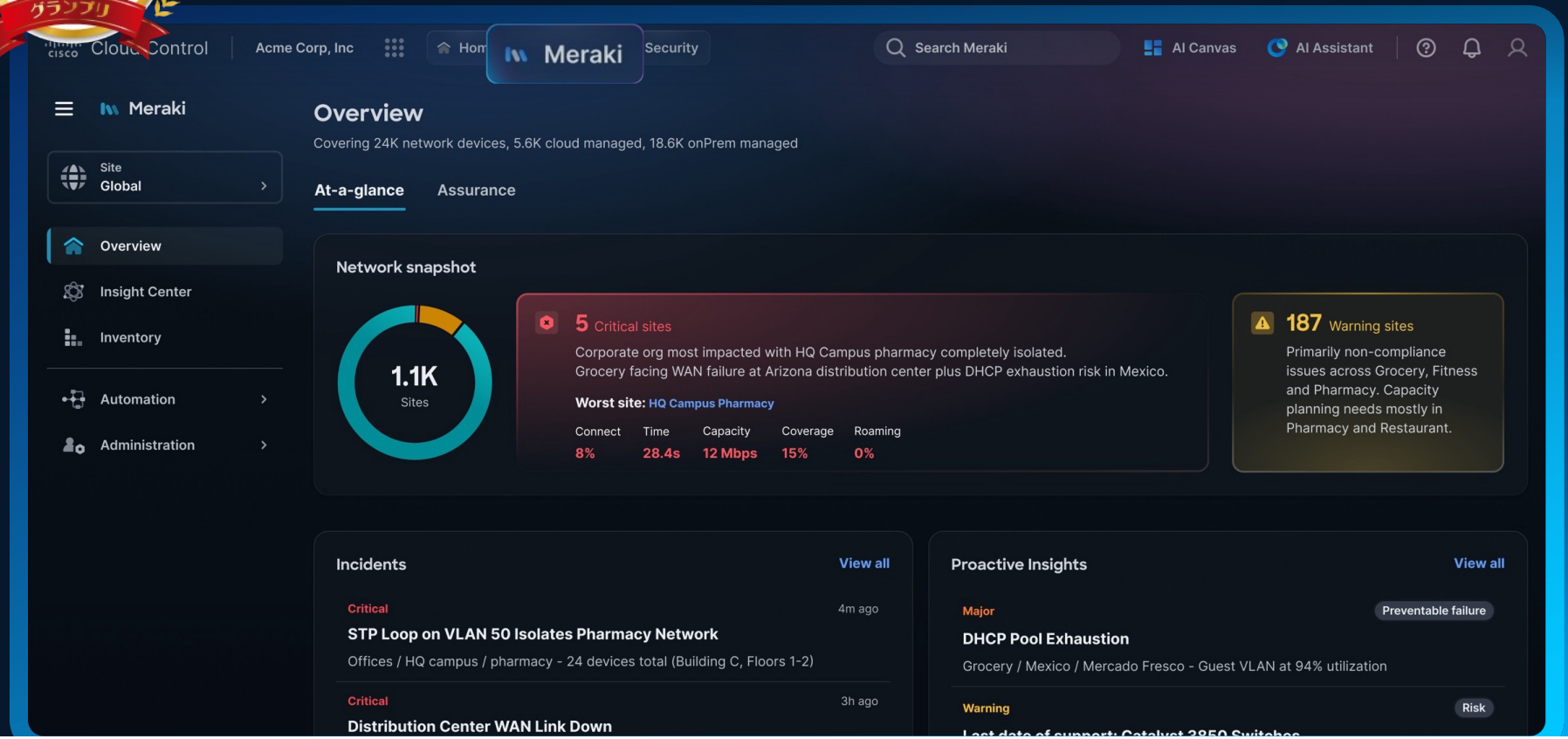
3つの主要な課題：複雑さ、制御、可視性

**Global 2000企業では、セキュリティとITの問題によるダウンタイムは、
直接的な費用と収益損失だけで年間4,000億ドル（およそ60兆円)の損失をもたらしています。**

Controlled Availability - June 2026

Cisco Cloud Control

クロスドメイン統合プラットフォーム



クロスドメイン統合プラットフォーム

The foundation everything is built on.

Cisco Cloud Control

Cisco products

- Meraki
- Intersight
- Splunk
- ThousandEyes
- Catalyst SD-WAN
- IQ
- Catalyst Center
- Nexus Dashboard
- Security
- Nexus Hyperfabric
- Collaboration Control Hub

AgenticOps

AI Canvas
Collaborative agentic workspace

AI Assistant
Conversational entry point

Platform services

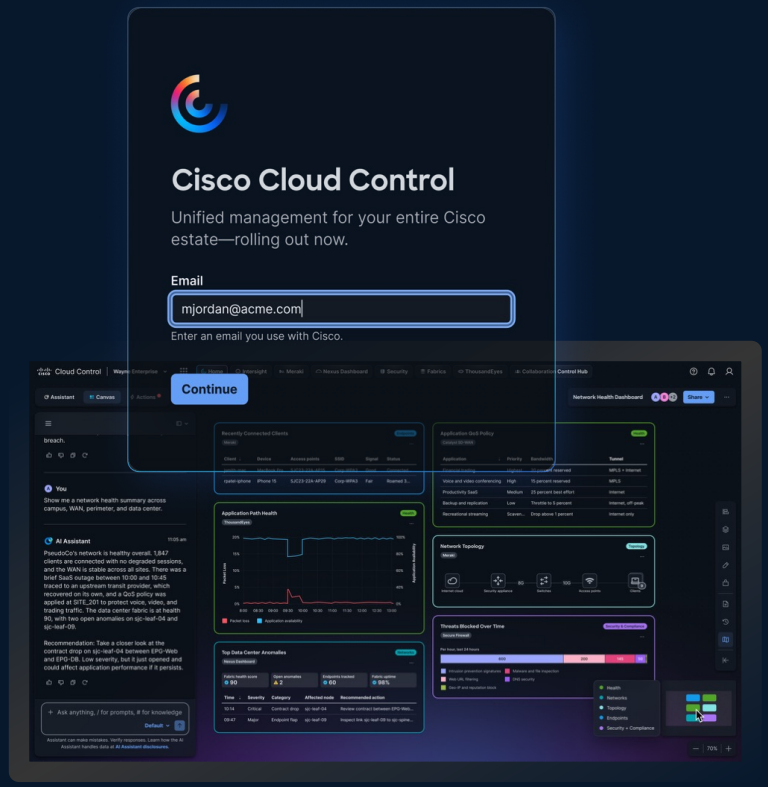
- Identity
- Inventory
- Topology
- Alerts & Notifications
- Licensing

Customize & extend

Marketplace | Agent Builder | App Builder

CCC: Cisco Cloud Control

https://www.cisco.com/site/jp/ja/solutions/artificial-intelligence/agentic-ops/cisco-cloud-control/index.html
https://cisco.service-now.com/helpzone?id=kb_article&sysparm_article=KB0071849



御客様の多くはネットワーク、セキュリティ、可観測性、コラボレーション、コンピューティング、クラウドなど、複雑化する環境を管理しています。多くの場合、運用チームは、インベントリの把握、イベントの相関分析、インシデントのトラブルシューティング、ポリシーの適用、コンプライアンスの証明を行うために、複数のコンソールを行き来せざるを得ません。

Cisco Cloud Controlは、シスコの製品ポートフォリオ全体にわたるチームの運用方法を変革するように設計されています。

企業オペレーターが必要とする基盤レイヤーを統合し、一貫したアクセスを実現する共有IDとテナントモデル、製品全体にわたる標準化されたインベントリとトポロジーモデル、ドメイン間でアラートとコンテキストを接続する相関レイヤー、そして共有された運用コンテキストに基づいて推論を行うAIレイヤーといったプラットフォームサービスを提供します。

AI Canvas

https://www.cisco.com/site/jp/ja/solutions/artificial-intelligence/agentic-ops/ai-canvas/index.html

「人間のオペレーター（運用担当者）とAIエージェントがリアルタイムで共闘する、マルチプレイヤー型の生成AIワークスペース（生成UI）」

単なる一問一答のチャットボットではなく、ネットワーキング、セキュリティ、オブザーバビリティなど、ドメインをまたぐ複雑なITインフラのトラブルシューティングを、人とAIが同じライブデータや証跡を見ながら一緒に進められる共同作業空間（デジタル作戦指令室のようなもの）

MTTR（平均復旧時間）の劇的な短縮: AIエージェントがドメインを横断して原因特定から解決策の提示までを先回りして行うため、インシデント対応のスピードが圧倒的に上がる。

運用のシンプル化と属人化の解消: 専門知識が少ない担当者でも、AIのガイドや自然言語での対話を通じて、高度なトラブルシューティングやインシデント対応が可能になる。

SASE: Cisco Catalyst SD-WAN & Cisco Secure Access

https://www.cisco.com/site/jp/ja/solutions/secure-access-service-edge-sase/index.html

Cisco Catalyst SD-WANは、既存のルータ機器をそのまま活かして移行できるルータベースのSD-WANソリューションです。

最大の特徴は、BGPやOSPFなどの高度なルーティングプロトコルをフルサポートしており、既存のネットワーク環境とスムーズに統合できる点です。また、VRFを用いた柔軟なネットワークの論理分割やPoE対応といったルータならではの強みを持ちつつ、アプリ毎の動的な経路選択や強力な統合セキュリティ機能により、安全で効率的なWAN環境を実現します。

Cisco Secure Accessは、ゼロトラストを基盤にあらゆる場所からの安全なアクセスを実現するクラウド型SSEソリューションです。世界最大級の脅威インテリジェンス「Talos」を統合し、第三者機関の評価でもIDベースの攻撃に対し高い防御率（最高評価AAA）を達成する高いセキュリティ精度を誇ります。

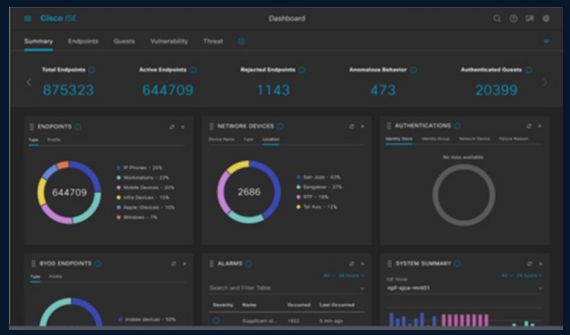
さらに、最新の「AI Guardrails」機能を備え、生成AIに対するプロンプトの入力内容を意味（セマンティック）レベルで解析します。これにより、機密情報の漏洩やプロンプトインジェクション攻撃を動的に防ぎ、組織の安全なAI活用を強力に支援します

セグメンテーション：Catalyst Center & Cisco ISE

https://www.cisco.com/site/jp/ja/solutions/artificial-intelligence/agentic-ops/cisco-cloud-control/index.html
https://www.cisco.com/site/jp/ja/products/security/identity-services-engine/index.html

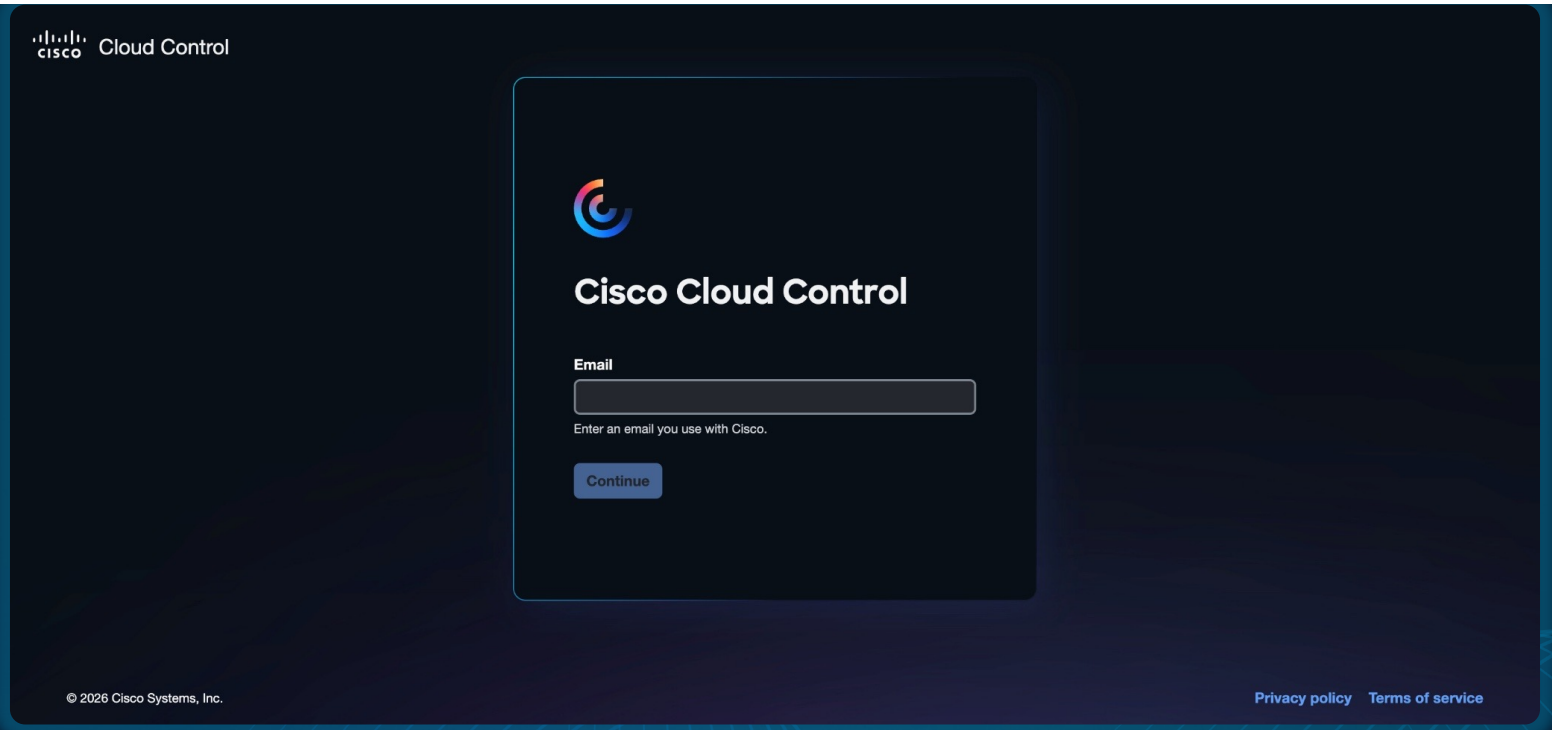
Cisco Catalyst Centerは、高度なAIモデルを悪用した脅威に対し、Cisco Catalyst Centerはマクロおよびマイクロセグメンテーション（SDA）を統合管理し、強固なゼロトラストを実現します。

組織や業務単位でネットワークを大きく分ける「マクロ」と、同一セグメント内でもAI端末やユーザーごとに通信を制限する「マイクロ」を組み合わせることで、万が一AIの脆弱性を突いた攻撃を受けても、脅威の横展開（ラテラルムーブ）を自動かつ即座に遮断します。

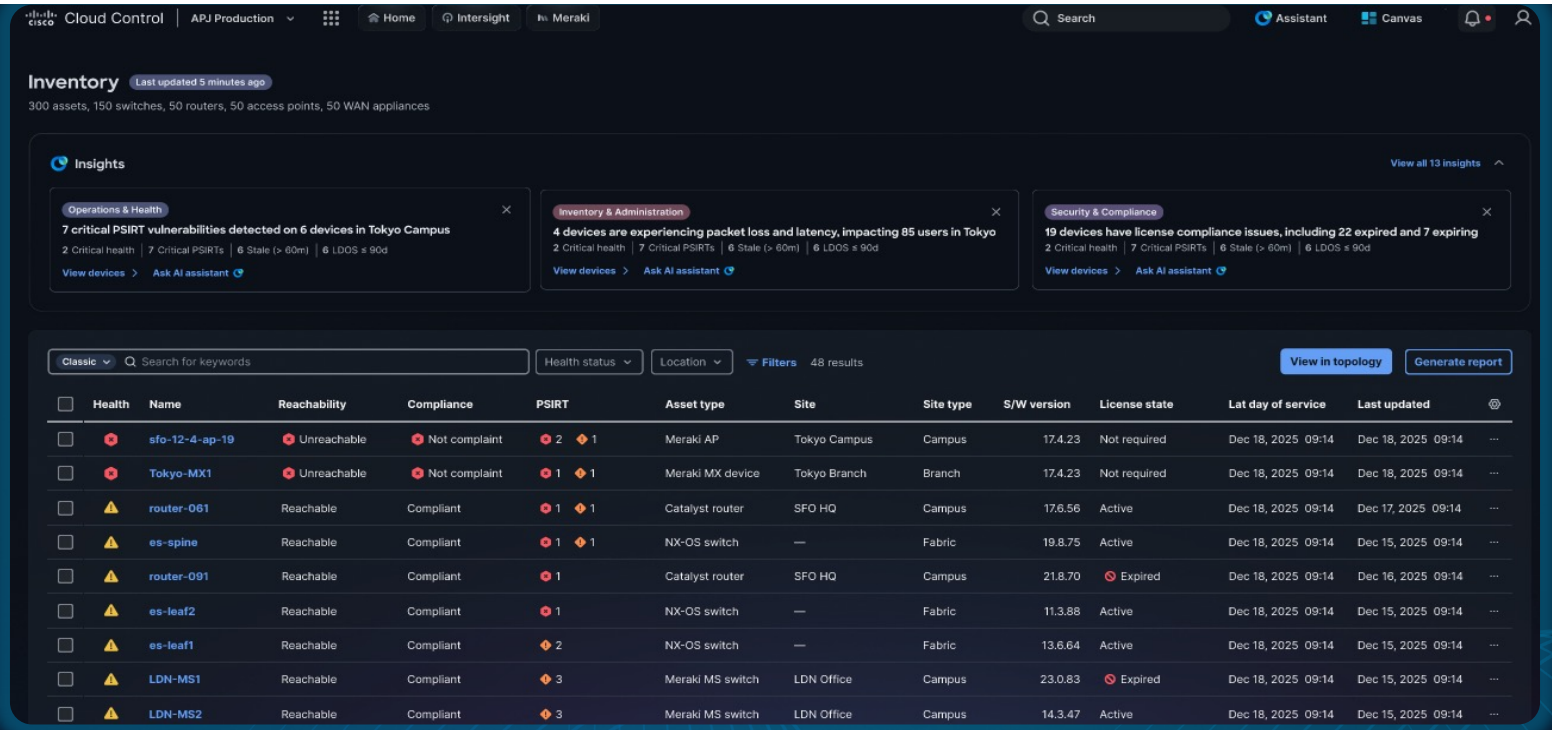


Cisco ISEは、高度なAIを悪用した攻撃に対し、Cisco ISEは「誰が・何が」接続しているかを厳格に識別し、動的なセグメンテーションを実現します。

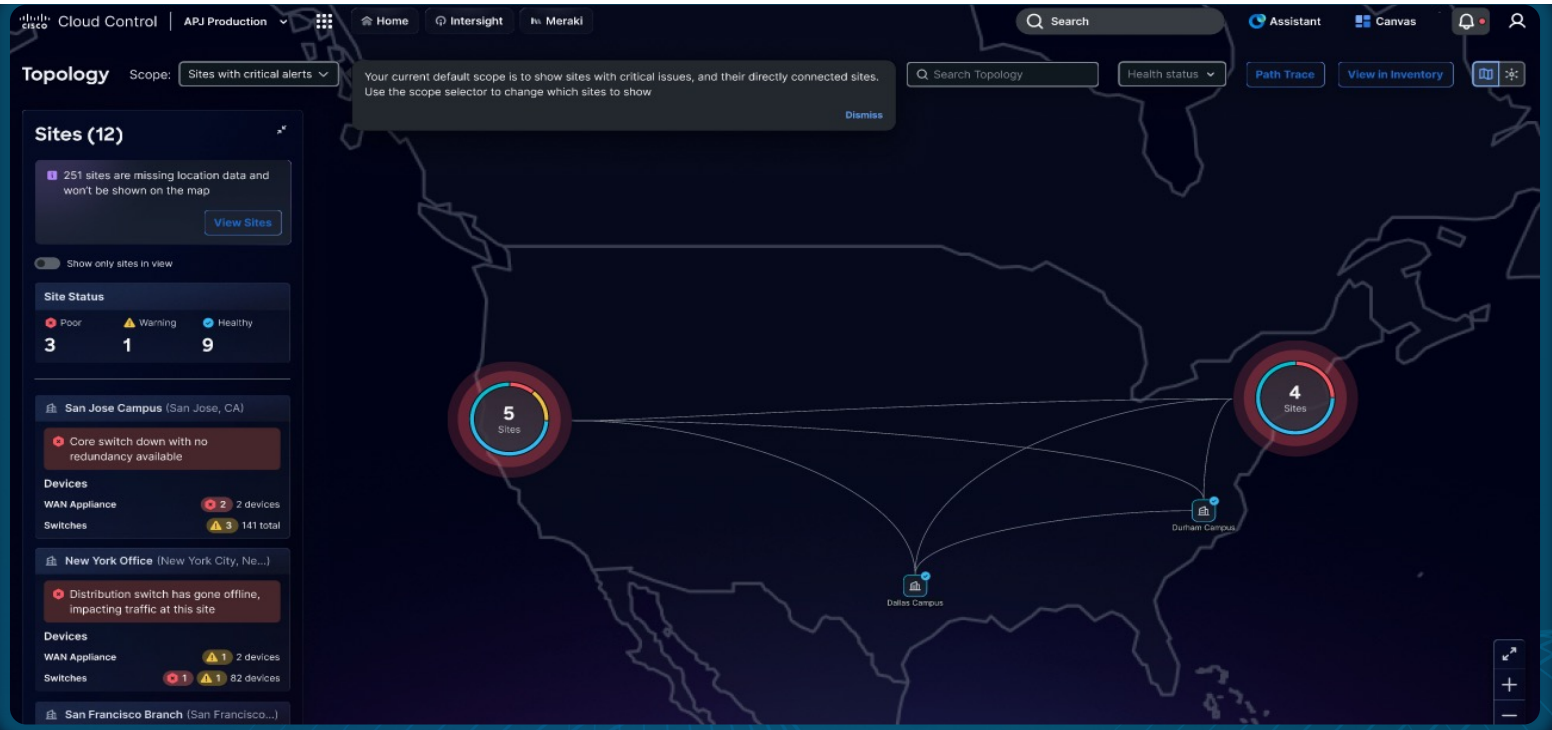
事業部ごとにネットワークを分ける「マクロ」と、同じ環境内でもAI端末やユーザーごとに通信を絞る「マイクロ」の制御を、SGT（セキュリティグループタグ）を用いて一元管理。AIモデルの乗っ取りや未知の脅威を検知した際は、対象端末のアクセス権限を自動で即座に剥奪し、被害の拡大を防ぎます。



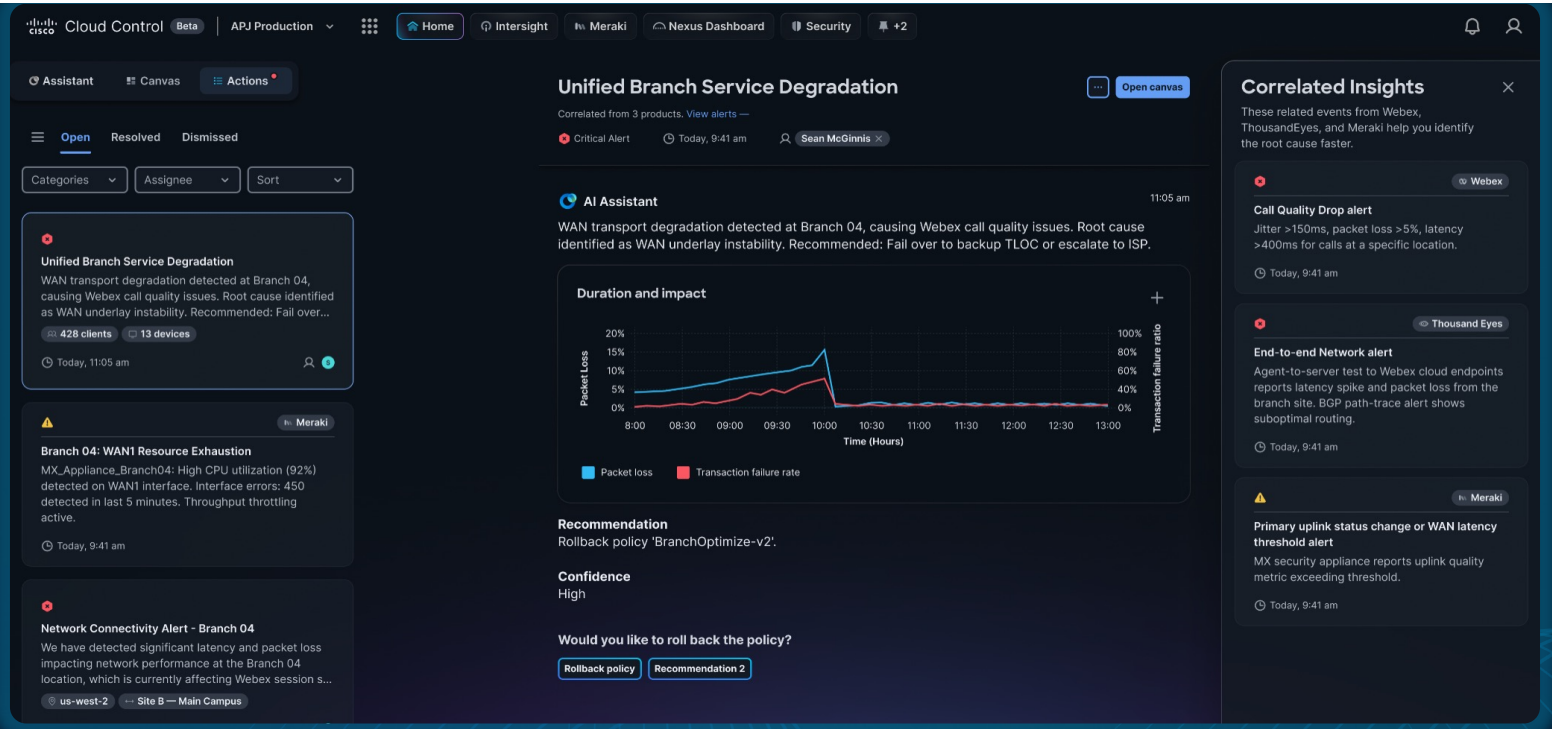
一度だけのシングルサインオン



すべての資産を一つの場所で管理



トポロジー情報を一つの画面に統合



「可視化」から「実行」へ

Cisco AI Canvas

Cisco Cloud Control のワークスペース

Cisco Cloud Control ユースケース

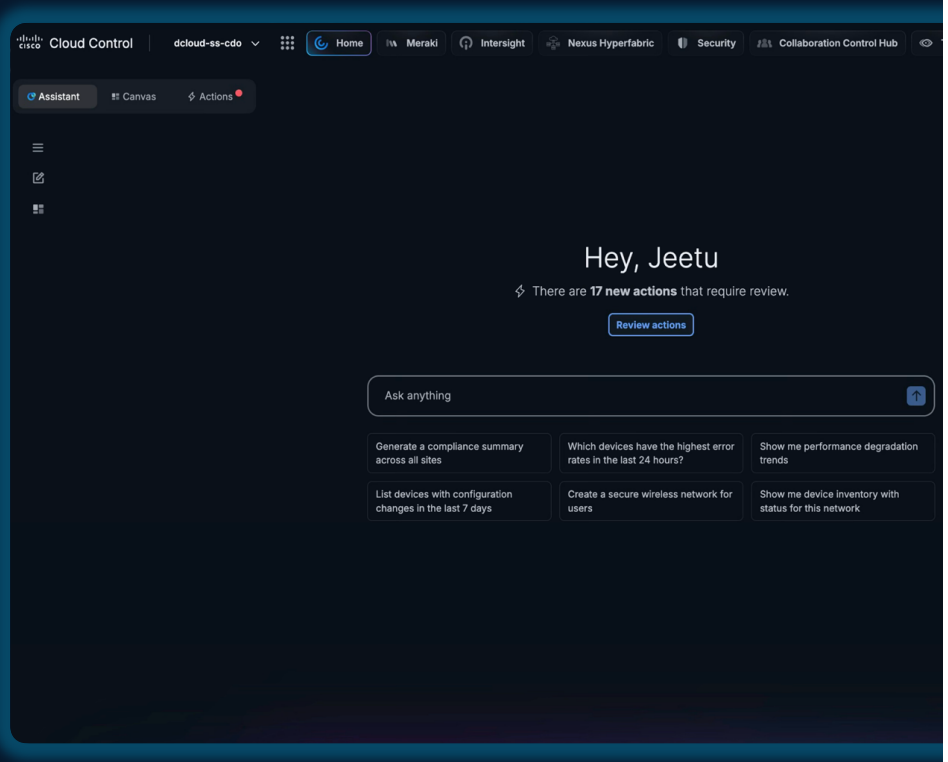
01 マネジメントの統合

02 ドメインをまたぐトラブルシューティング

03 データセンタとキャンパスのファブリック接続

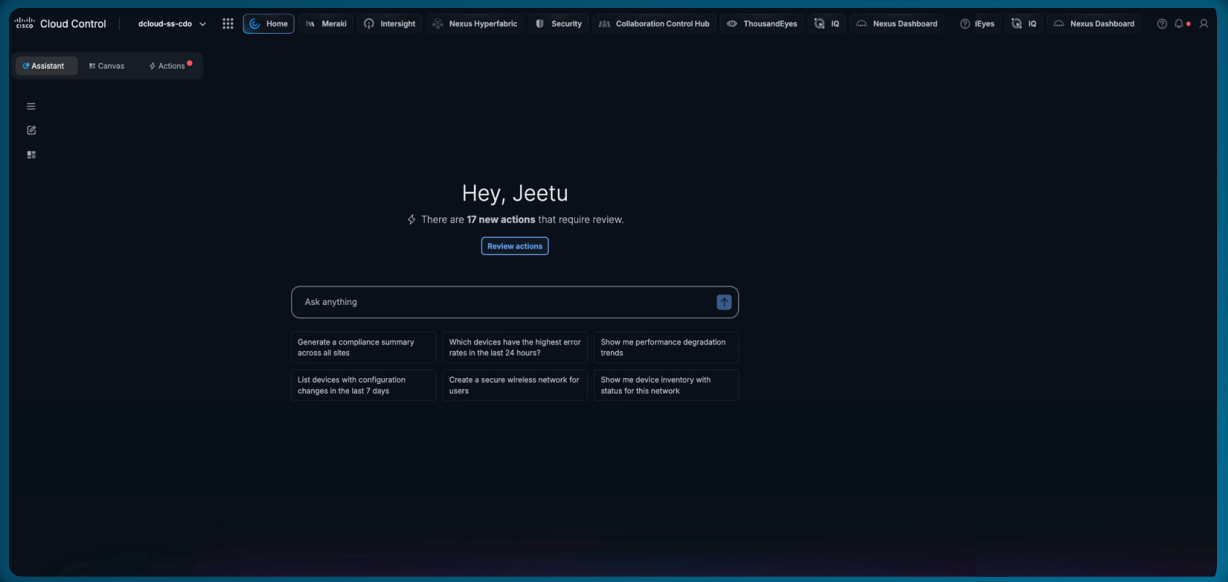
04 企業・組織内のエージェントの保護

05 トークンの利用状況を監視・最適化 (Tokenomics)



Cisco Public

Cisco Cloud Control
ユースケース



複数の拠点から、いくつかのSaaSアプリケーションが遅いというクレームがあります。

特にWeb会議などの断続的な音声の切断があります。
LAN側とWAN側、Internet側を含めて、どこに問題点があるのかを調査してください。

Cisco Cloud Control ユースケース

注意！

デモ環境につき、実際のトラブルとは異なります。

音声切断・SaaS遅延 — 総合調査レポート

LAN・WAN・Internet の3層を横断して調査しました。**問題は複数レイヤーで同時発生しており、拠点ごとに主因が異なります。**

重大度別 問題サマリー

重大度	拠点/対象	問題	レイヤ
Critical	**Buenos Aires**	VPN スコア **33/100**（大幅劣化）	VPN/W
Critical	**Site 101 (San Jose Branch)**	WAN 稼働率 **0%**（回線 oper-up なのにデータプレーン不通）	WAN
High	**Site 102 (London Branch)**	トンネル異常率 **47.6%**、レイテンシ 183–196ms	WAN
High	**Buenos Aires**	有線クライアント スコア **53/100**、スイッチポート断片化	LAN
High	**Mexico City**	クライアントスコア Fair 91、AP接続不可・スイッチアクセス制御アラート多発	LAN
Warning	**Microsoft O365 (Internet)**		Interne
Warning	**Mexico City エージェント×2台**	NTP 時刻ずれ **+6分**（ThousandEyes 計測精度に影響）	LAN

Cisco Cloud Control ユースケース

注意！

デモ環境につき、実際のトラブルとは異なります。

🌐 レイヤー別 詳細分析

1 LAN 側

項目	状況
Buenos Aires スイッチ (MS130) ポート13	パケット断片化（MTU不一致の疑い）→ 音声RTPパケット分割が断続切断を誘発
Buenos Aires 有線クライアント	スコア 53/100。アクセスポリシーによるトラフィックブロック、STP ルートガード発動が複
Mexico City	AP到達不可・スイッチポートのアクセス制御アラートが多発、DNS 設定ミスあり
Mexico City エージェント	NTP 同期ずれ（6分）→ TLS/認証タイムアウトがTeams接続に影響する可能性

2 WAN 側

項目	状況
Site 101 (San Jose Branch)	両エッジとも WAN 稼働率 0% — 即時対応必要
Site 102 (London Branch)	異常率 47.6%（7トンネル）、パケットロス 0.39–0.41%
Buenos Aires WAN	スコア 75/100、VPN スコア 33/100 — 拠点間・SaaS への経路が不安定
Webex Meeting @ Site 11	vQoE 4.87（Poor）、レイテンシ 201–226ms、ジッター最大 6ms

3 Internet 側（ThousandEyes）

項目	状況
Microsoft Office 365	07/08 04:50 UTC [redacted]
Microsoft Corporation ネットワーク	[redacted] (Chicago/Dallas/London)
MS Teams の vQoE データ	SD-WAN側でアプリ分類が未設定のため計測値なし
ISP レベル	[redacted] 複数 ISP でネットワーク障害検知

Cisco Cloud Control ユースケース

注意！

デモ環境につき、実際のトラブルとは異なります。

🎯 根本原因の分析

```
音声切断の主因（重みつき）：
  1. Internet/                                → 直接的な切断要因
  2. Buenos Aires VPN劣化(33/100) + LAN断片化 → 音声RTPの連続性を破壊
  3. SD-WAN Site101/102 のトンネル不安定 → WAN経路冗長が機能していない
  4. SaaS遅延全般 → WAN回線レイテンシ（183–226ms）がリアルタイム音声の閾値超過
```

✅ 推奨アクション（優先順）

優先度	対象	アクション
🔴 即時	**Site 101 WAN**	TLOC ヘルスとトンネル状態を確認、データプレーンの状態不一致を解消
🔴 即時	**Buenos Aires VPN**	VPN トンネルの再確立、IKEフェーズ確認、回線品質確認
🟠 当日中	**Buenos Aires スイッチ ポート13**	MTU を 1500→1400 に調整（または Jumbo Frame 設定確認）、接続機器の確認
🟠 当日中	**Mexico City NTP**	MexicoCity-Campus-Edge1/2 の NTP 設定を修正
🟠 当日中	**Site 102 London**	トンネル異常ログを確認、ISP回線の品質レポートを取得
🟡 今週中	**MS Teams QoE 監視**	SD-WAN でアプリケーション分類を設定し vQoE 計測を有効化
🟡 今週中	**Mexico City LAN**	AP 接続不可 / DNS 設定ミスを解消、アクセスポリシー見直し

cisco Live !

Thank you