

Cisco DNA アナリティクス とアシュアランス

概要

今日の IT 部門において最優先の課題になっているのが、デジタル変革です。最近の研究によれば、84 % の組織がすでにデジタル変革に取り組んでいます。これは驚くことではありません。というのも、デジタル変革によって収益や採算性が向上し、企業さらには業界全体の動向が左右される可能性のあることが、広範な研究からわかっているからです。

デジタル変革の中核には、エンタープライズ ネットワークがあります。それは、オープンでプログラム可能かつセキュアな統合ネットワークであり、それによってビジネスの俊敏性が最大限に向上し、新たなビジネス機会の追求と獲得が可能になります。これが、エンタープライズ向けintentベース ネットワーキング アーキテクチャである Cisco® Digital Network Architecture (Cisco DNA™) のビジネス価値提案です。

現在、ほとんどのネットワーキング部門は運用業務で手一杯になっており、時間の大半を、手作業によるネットワークの設定とトラブルシューティングに費やしています。これに対して、自動化およびアナリティクス プラットフォームを含むintentベースのクローズドループ アーキテクチャでは、IT 部門の時間とリソースが大幅に解放され、それを戦略的プロジェクトとデジタル変革の推進に振り向けることが可能になります。

このホワイトペーパーでは、エンタープライズ ネットワーク アーキテクチャにおけるアナリティクスとアシュアランスの役割を説明し、業界初の Cisco DNA アナリティクス プラットフォームと、それによって実現される強力なネットワーク モニタリングおよびトラブルシューティング アプリケーションである Cisco DNA アシュアランスを紹介します。

Cisco DNA アシュアランスは、エンタープライズ ネットワーク上で動作するクライアント、ネットワーク デバイス、およびアプリケーションの健全性をモニタします。また、コンテキストの関連付けを活用して根本原因を特定することでトラブルシューティング プロセスを促進し、さらには自動化プラットフォームと統合して規範的な修復を促進します。

目次

概要

ビジネス要件

ユーザ要件

最前線のエンジニア
現場担当者
エキスパート
プランナー

テクノロジー要件

計測
分散型オンデバイス分析
テレメトリ
拡張可能なストレージ
分析エンジン
機械学習
ガイド付きのトラブルシューティングと修復
自動化されたトラブルシューティングと修復

DNA Center

Cisco DNA アシュアランス

まとめ

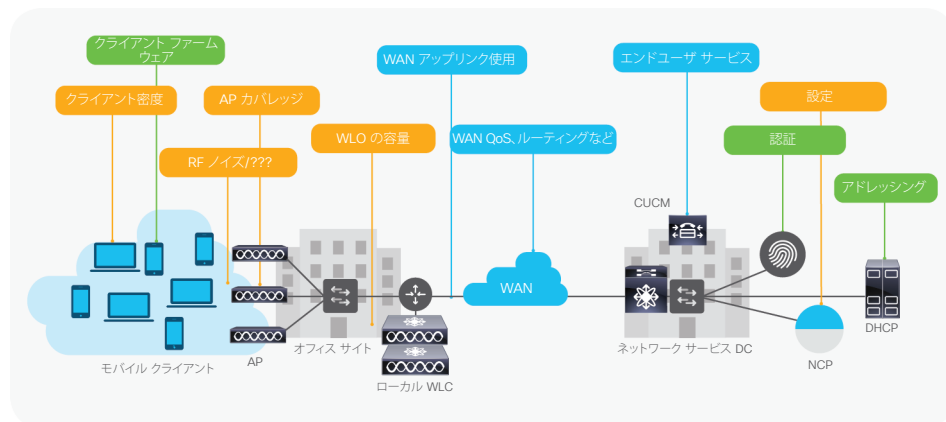
ビジネス要件

2016 年に McKinsey 社が行った調査によれば、企業は 600 億ドルを超える支出をネットワーク運用に費やしており、ネットワーク運用支出の 75 % が可視性とトラブルシューティングに費やされています。

ほとんどの企業が何千ものユーザやアプリケーションを抱え、さらには何万台ものネットワーク対応デバイスを使用していることを考えれば、こうした統計値はさほど意外ではありません。また、2016 年から 2020 年にかけて IP トラフィックが 2 倍超に増大するほか、同じ時期に 100 億台の Internet of Things (IoT) デバイスが新たにネットワーク接続されると予想されています (Cisco Visual Networking Index™ の予測による)。

IT 部門にとって、手作業によるネットワーク運用管理はますます非合理的な仕事になっており、ましてや、一貫性も互換性もないハードウェア/ソフトウェア システムとデバイスが社内に無数に存在する環境では、その困難さがさらに悪化します。そして、ネットワーク、クライアント、またはアプリケーションのトラブルシューティングは、図 1 に示すように、関係するユーザ/アプリケーション間の障害点の数が 100 を超えることも珍しくない、複雑で総体的な問題です。

図 1. ユーザ エクスペリエンスに影響する可能性のある障害点



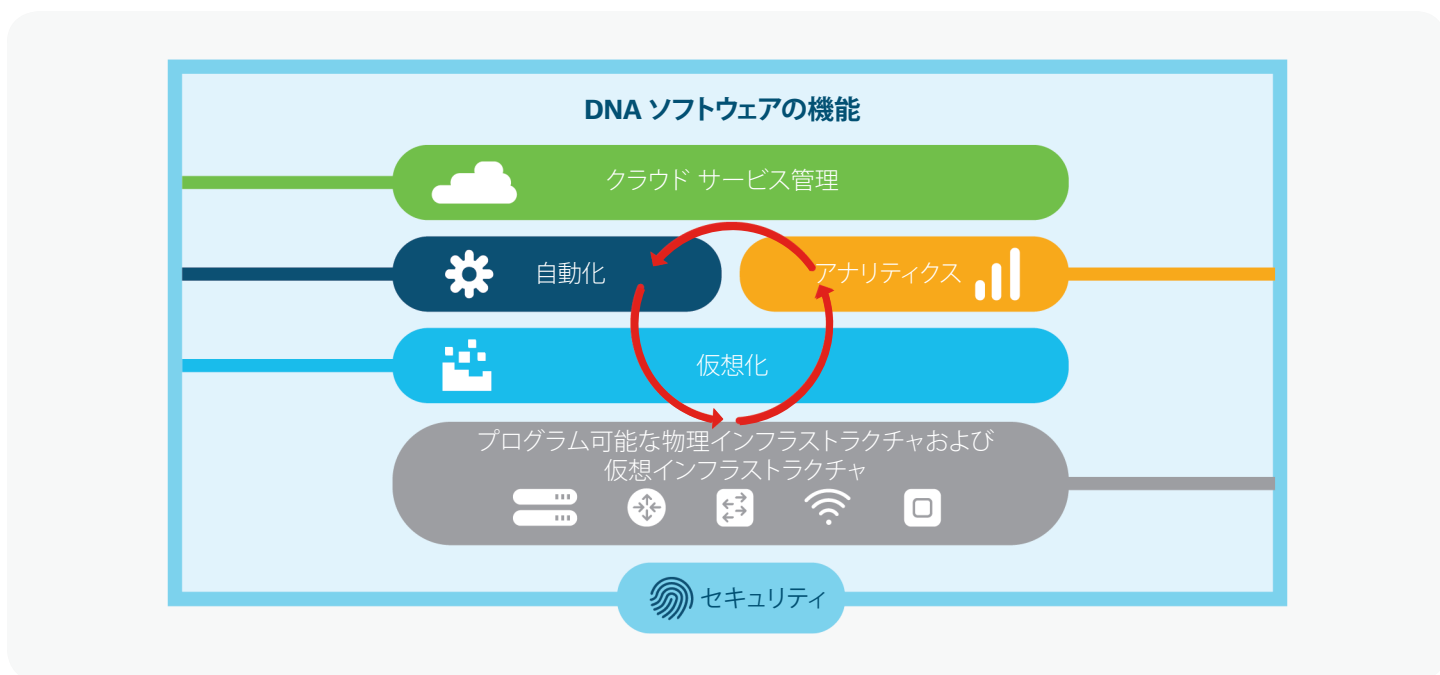
ネットワークのトラブルシューティングには、次のような課題があります。

- ・ **データ収集の課題:** ネットワーク オペレータは、データの収集にかなりの時間を費やしており、**収集**データから得た洞察結果を利用して分析とトラブルシューティングを行うのと比べて 4 倍も長い時間を割いています。
- ・ **再現の課題:** ネットワーク オペレータは、トラブルシューティングを開始した時点 (イベントが報告されてから数分後、数時間後、数日後など) で表面化していない問題を解決することはできません。つまり、オペレータが問題を検出および/または再現できない限り、それ以上の調査はまったく不可能です。
- ・ **解決までの時間:** ネットワーク品質に関する問題のほとんどは、根本原因を特定して最終的に解決するまで、何時間も (あるいはそれ以上) かかります。
- ・ **まずネットワークが疑われる:** ある問題が発生すると、原因として最初に疑われるのがネットワークである場合が多いのですが、それはたいてい誤っています。そのため、ネットワーク オペレータは、ネットワークに問題がないことを証明するだけのために、大きな労力を費やしています。

ネットワークの運用コストの急騰を制御できる企業は、高い収益性と優位性を獲得できる立場にあります。ポイントになるのは何でしょうか。それはデジタル分析です。デジタル分析によって、生産性を大幅に向上させることが可能です。たとえば McKinsey 社による 2017 年の研究によると、デジタル分析を使用して運用を合理化した企業では生産性が 20 % 向上すると予測されています。

ここで効果を発揮するのが、図 2 に示す、Cisco DNA のクローズド ループです。

図 2. Cisco DNA:クローズド ループ アーキテクチャ



Cisco DNA の自動化プラットフォームの大きな目的は、ネットワークと「話す」ことにあります。つまり、提示されたビジネス インテント (意図) を、ネットワーク デバイス上でプラットフォーム固有の最適な設定に変換することです。補足すると、アナリティクス プラットフォームの主要な役割は、ネットワークを「聞く」ことにあります。具体的に言えば、ネットワーク デバイスで生成されたすべてのネットワーク テレメトリを収集して関連付け、意味を明らかにし、そのデータを、提示されたビジネス インテントに関連付けることです。

さらに、アナリティクス プラットフォームによってネットワーク オペレータは**アシュアランス**を得られ、インテントベース ネットワーキング ポリシーに関するクローズド ループを実現できます。それには次の方法があります。

- ・ インテントの遂行を**証明**する定量的データを提供する
- ・ インテント遂行のためには修復が必要であることをコントローラに**通知**する

この 2 番目の手順は、ガイド付きトラブルシューティングや自動化されたトラブルシューティングでさらに補完することができ、それによって修復プロセスが促進されます。

次に、エンタープライズ ネットワークでのアナリティクスとアシュアランスに関するユーザ要件を見てみましょう。

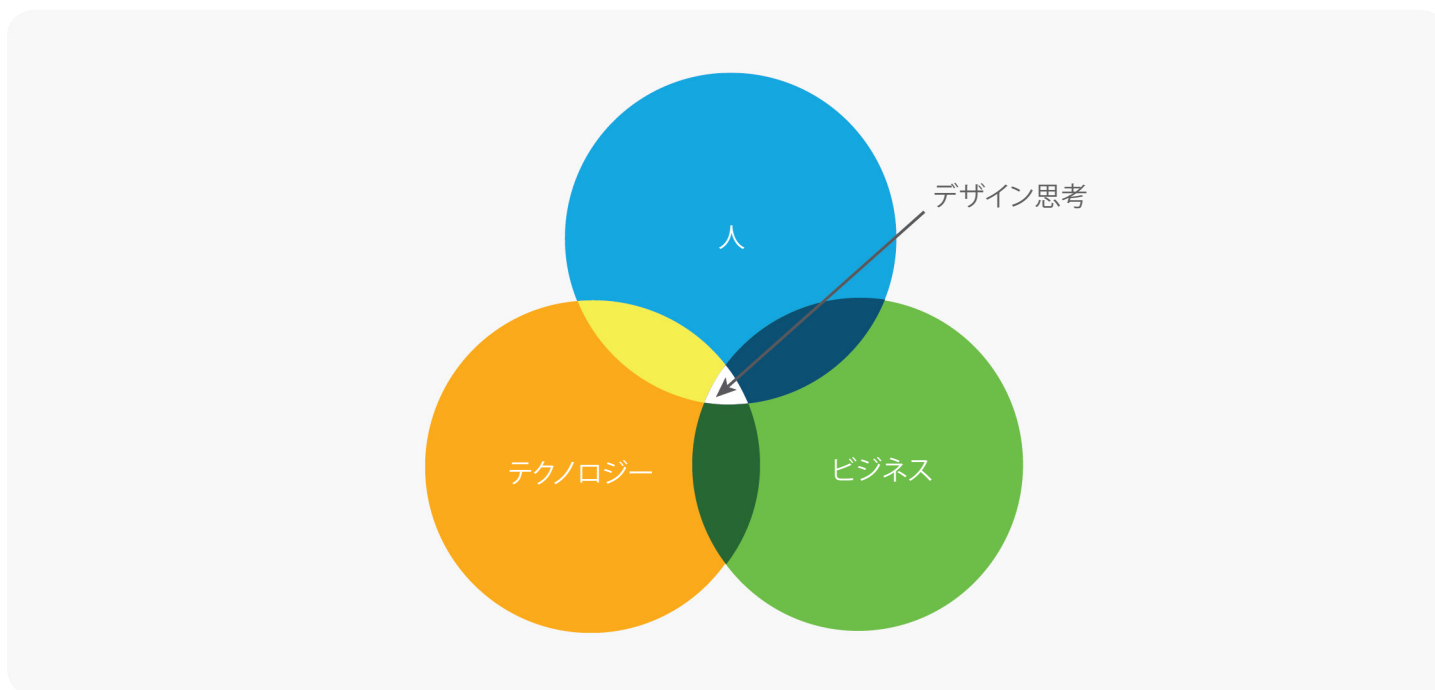
ユーザ要件

Cisco DNA は、デザイン思考の原則に基づいて構築されています。デザイン思考は、「創造的アクションの手法」として 1980 年代初頭にスタンフォード大学で提唱された、イノベーションに対する人間中心のアプローチです。後に、デザインコンサルティング企業の IDEO 社が、これをビジネス用途に応用しました。デザイン思考は、一般の人々の現実的問題を解決するための製品構築に役立つ枠組みとして機能します。具体的には、ユーザに「驚きと喜びを与える」という全体的目標のもと、人々の実際のニーズを探り出し、それらのニーズに対応するソリューションを作り出すことを意味します。

デザイン思考で重視される主義として、テクノロジーよりもユーザ エクスペリエンスが重要というものがあります。その根拠となるのは、テクノロジー、ソリューション、そしてデータは時間の経過とともに変化するが、人間の本質的なニーズは変わらないという事実です。つまり人は、デザインの数式の中で最も変化が少ない変数ということになります。デザインが優れている場合、ユーザは必ずしもそれに気づきません。形態と機能が合致していれば、特に意識せずに日常が過ぎていくことが多いからです。しかしデザインに何らかの不具合がある場合は気づきます。混乱や不満が生じ、行動の妨げや遅れになるからです。

そのためデザイン思考では、ユーザに共感してニーズを先取りすることを重視し、ユーザに喜んで使用されるような、有益かつ実用的な製品を開発しようとしています。デザイン思考の中心には、問題を効率的・効果的・エレガントに解決するという考え方があります。理想的なデザイン思考とは、図 3 に示すように、人間のニーズ、ビジネス要件、そしてテクノロジー ソリューションが交わる部分にあります。

図 3. デザイン思考の「スイートスポット」



したがってシスコでは、デザイン思考のプロセスの出発点として、ユーザの要求をより良く理解するために、エキスパートとさまざまな分野のお客様、パートナーおよび、場合によっては競合他社との綿密な面談を、何度も実施しました。面談のプロセスにおいて中立性を最大限に高めてバイアスを最小限に抑えるために、面談の多くは、面談の実施者を知らせない「ブラインド」状態で行いました。つまり、シスコの代表者が直接面談を行うのではなく、中立的な第三者に質問をしてもらいました。

このフェーズでは、下記業界の有力企業を代表するお客様やパートナーと、60 回を超える綿密な面談を実施しました。



銀行サービスと
金融サービス



製造業



IT 企業



大学と
研究センター



サービス プロバイダー



小売業者



製薬会社

こうした面談に加えて、シスコは定期的に、Enterprise Technical Advisory Board (ETAB) や Mobility Technical Advisory Board (MTAB) を含む、お客様の諮問委員会との会議を行っています。これらの委員会は、多様な業界におけるシスコの大手のお客様を代表するものであり、発展するビジネス要件に適応した製品とテクノロジーを実現するための継続的なフィードバックと指導をシスコに提供しています。

また、シスコのチームがお客様のサイトに出向き、ネットワークの設計・構築・運用の方法とそれに伴う課題を継続的に観察しました。

オンサイトでの観察に加えて、広範なデータ分析も行いました。たとえば Cisco DNA チームは Cisco IT と連携して、6 カ月の間にオープンされた 11,500 件のインシデント チケットと 1,455 件を超える更管理要求の分析および関連付けを行いました。

シスコは、ユーザをより良く理解し、満たされていないニーズや問題点を把握するために、どんな労も惜しみませんでした。こうした実践を通じて、ネットワーク上のパーソナリティに関するいくつかの典型が明らかになってきました。それは次のようなものです。

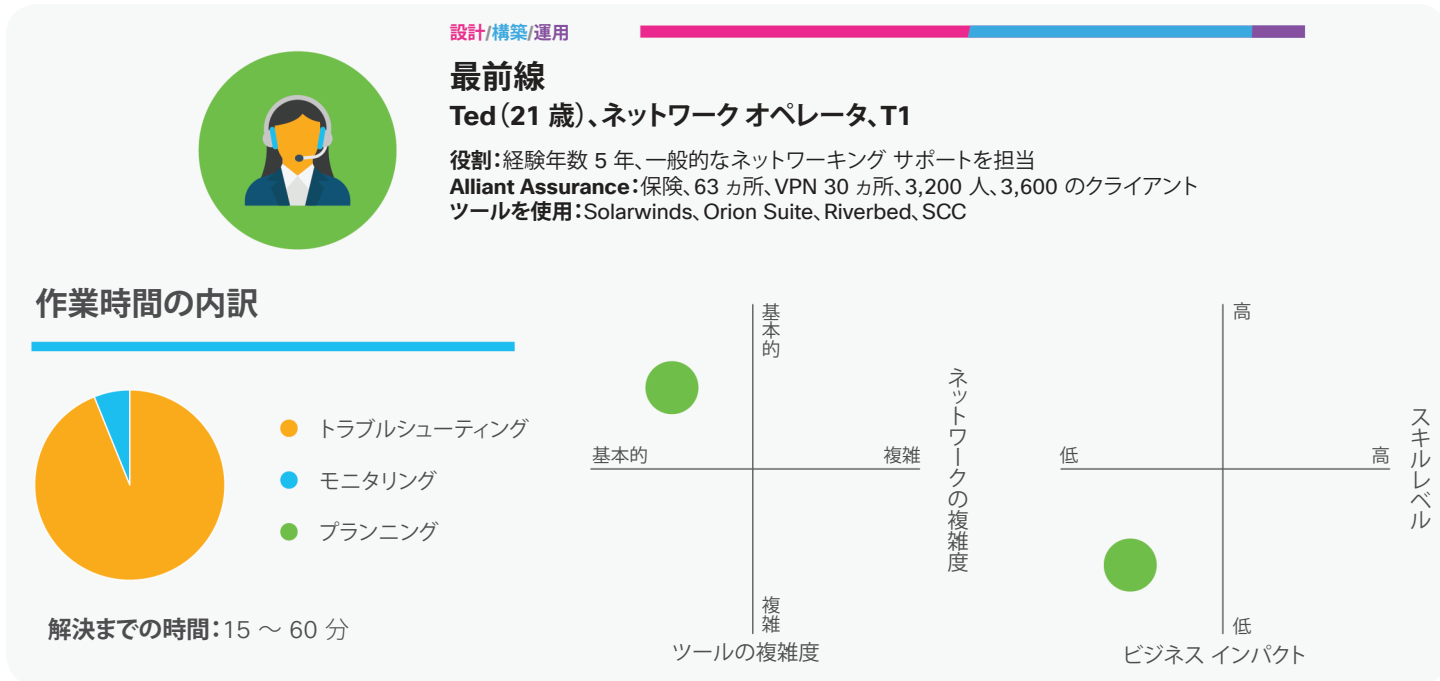
- ・ 最前線 (階層 1) のネットワーク エンジニア
- ・ 現場担当 (階層 1 および 2) のネットワーク エンジニア
- ・ エキスパート (階層 3 および 4) ネットワーク アーキテクト
- ・ プランナー (階層 3 および 4) ネットワーク エンジニアリング マネージャ

この取り組みのポイントは、ネットワーク部門内のさまざまな役割を類別するだけでなく、お客様からの直接的な声に基づいてネットワーク エンジニアの各役割の責任、ニーズ、動機付け要因、問題点を定義することにあります。その概要を、次のセクションで説明します。

最前線のエンジニア

最前線のエンジニアは、通常最初にトラブル チケットを処理する人員であり、経験や権限が最も少ないのが一般的です。概してこのレベルのエンジニアは自身の役割に関するトレーニングをほとんど受けていないのですが、その一方で、役割の実行に際して大きなプレッシャーを受けています。このエントリ レベル階層で解決される問題が増えるのは、明らかに好ましいことです。この段階で解決される問題の割合は 10 ~ 75 % と報告されており、最前線をサポートするトレーニング、ツール、リソースに比較的大きな投資を行っている企業にはそれに応じたメリットがあるということが表れています。階層 1 の最前線エンジニアに該当するユーザの典型例を、図 4 に示します。

図 4. 階層 1 の最前線ネットワーク エンジニアの典型例




概要	<ul style="list-style-type: none"> ・ エントリ レベル <ul style="list-style-type: none"> - 最小限の賃金 - スキルが比較的低い ・ アウトソーシング (場合による) ・ 遠隔地 (たいていの場合)
責任	<ul style="list-style-type: none"> ・ エントリ レベルのサポート ・ IT ジェネラリストまたはネットワーク ジェネラリスト ・ 遠隔地作業員としてのパワー ユーザ (オンサイト) ・ 通常、アウトソーシングによるサポート ・ スクリプトに厳格に従う ・ トラブル チケットをオープンして他のチームに転送する
ニーズと 動機付け要因	<ul style="list-style-type: none"> ・ 問題またはアラートを転送するための、よりスマートなチケット生成システム ・ 報告された問題を解釈し、正確な内容とコンテキストで記録する ・ 問題をより良く理解するために、検証または再現する ・ シンプルな解決方法を提示する、信頼性の高いナレッジ ベース ・ 試行錯誤によって問題を排除するための、基本的なトラブルシューティング手法 ・ ビジネス インパクトの重大度、スケールのインパクト、問題のトピックに基づく、適切なエスカレーション パス ・ ツールから送信されたアラートに結び付けられるナレッジ ベース ・ 問題の通知を可能な限り迅速に解決する能力

問題点	<ul style="list-style-type: none"> ・ サポート チケットに正確な内容または十分なコンテキストを含めないとペナルティが課される ・ 症状を見逃したり根本原因にまったくたどり着けなかったりするとペナルティが課される ・ 適切なツールを使用しないとペナルティが課される(全員がその使用方法を知っているわけではない) ・ 情報の誤りまたはトリアージの限界によって適切なエキスパートにエスカレーションしなかった場合にペナルティが課される ・ タイムリーにエスカレーションしないとペナルティが課される
コメント	<ul style="list-style-type: none"> ・ 「ネットワーク オペレーション センターによってノイズがフィルタリングされる」 ・ NOC は「たいていの場合、訓練された猿が赤信号を探すようなもの」 ・ ユーザは必ずネットワークに問題があると苦情を言うが、「問題の 60 % はアプリケーションやユーザの問題に帰着する」 ・ 2 社のお客様が、階層 1 で解決される問題は 10 % と報告(範囲内の最低の数値) ・ 3 社のお客様が、階層 1 で解決される問題は 75 % と報告(範囲内の最高の数値)
まとめ	<p>ユーザは常にネットワークに問題があると苦情を言いますが「問題の 60 % はアプリケーションやユーザの問題に帰着する」ため、最前線のエンジニアは、試行錯誤によって問題を排除するための基本的なトラブルシューティング手法を必要としています。現状では、最前線のエンジニアはトラブルシューティング ツールの使用方法についてトレーニングを受けておらず、適切なツールを使用しない場合や、症状を見逃した場合、または根本原因にたどり着けなかった場合には、ペナルティが課されます。</p>

現場担当者

現場担当者は、第 1 レベルのエスカレーションを担当します。最前線のエンジニアが問題を解決できなかった場合に次のレベルのエンジニアとして問題を取り扱うのが、現場担当者です。現場担当者は一般的に、最前線のエンジニアよりも高度なトレーニングを受けており経験が豊富ですが、対応している多くの問題について、本来なら第 1 階層で解決されるべきだったという不満をしばしば述べています。

図 5. 現場担当(階層 1 および 2)のネットワーク エンジニアの典型例




設計/構築/運用

典型的な現場担当者

Charles (27 歳)、ネットワーク エンジニア、T1-T2

役割: 経験年数 8 年、クラウド エンタープライズ システム担当、ネットワーク システムを構築
HP: テクノロジー、ブランチ 4 か所、ネットワーク機器 2,300 台、ネットワーク チーム数 15
使用ツール: HP 機器、F5 ロード バランシング、Checkpoint、Brocade、Juniper、NMMI、Redfish

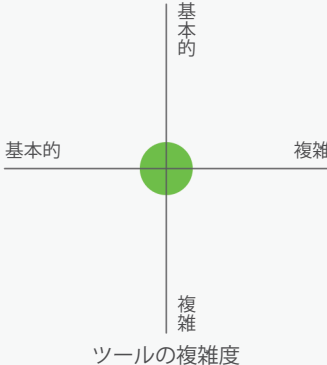
作業時間の内訳



- トラブルシューティング
- モニタリング
- プランニング

解決までの時間: 12 ~ 24 時間

基本的



基本的

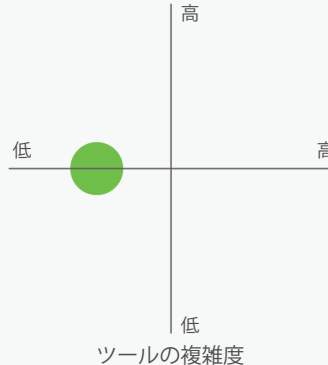
複雑

複雑

基本的

ツールの複雑度

高



高

低

低

高

低

ツールの複雑度

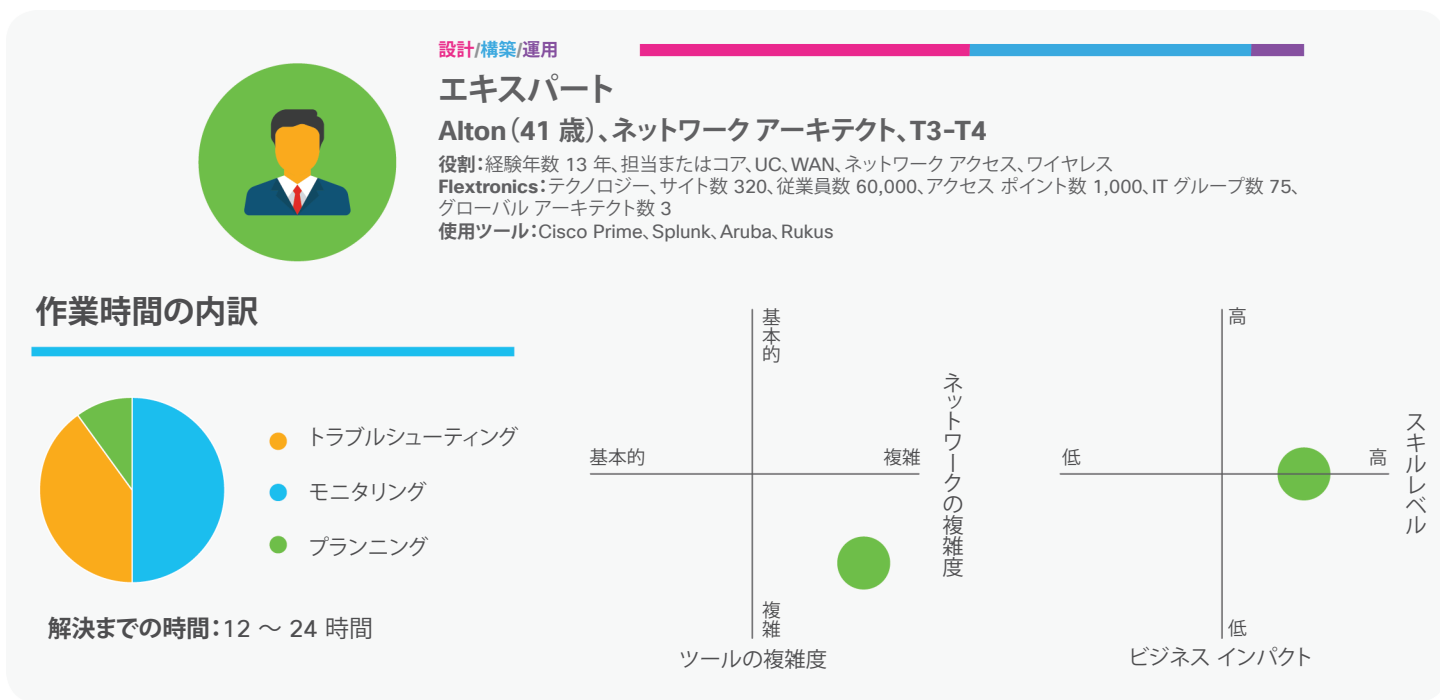
スキルレベル

概要	<ul style="list-style-type: none">・ 比較的経験が豊富<ul style="list-style-type: none">- トレーニング- 比較的報酬が多い・ 社内(たいていの場合)・ 比較的責任が大きく、アクセスが増えている
責任	<ul style="list-style-type: none">・ シンプルな階層 1 および 2 の問題の解決の初期担当者・ 基本的なモニタリングとトラブルシューティング・ ツール・ Network Operations Center (NOC) 外 (ほとんどの場合)・ ほとんどの問題がこのレベルで解決される
ニーズと動機 付け要因	<ul style="list-style-type: none">・ 問題あるいはアラートが適切なコンテキストとともに転送されてくるような、よりスマートなチケット生成システム・ さほど多くのカスタマイズを必要とせずそのまま使えるツール・ 適切なエキスパートにエスカレーションできるよう問題の重大度、スケール、インパクトを評価する能力・ 重大度 1 および 2 の問題に関する、適切なエキスパートとの迅速な連絡と効果的な連携・ 解決に必要なレベルまで問題を掘り下げられるツール・ ドキュメント (誤っている可能性あり) を補完する、正確なトポロジ図を示すツール・ サーバ、ルータ、ヘルプ デスクのサマリーなど、カスタマイズ可能なサマリー ビューを表示できるツール・ リアルタイムのステータスとイベント
問題点	<ul style="list-style-type: none">・ 重大度フィルタが不正確で信頼性が低い・ ツールが断片化され相関ロジックがない・ raw データが多すぎて、十分な洞察結果が得られない・ 階層 1 で修正されるべきであった問題に対処することが、あまりにも多い
コメント	<ul style="list-style-type: none">・ 「データ サイエンティストになるつもりはない。私はネットワーク アナリストだ」・ 「ドキュメントが常に正しいとは限らない。信頼性の高い検出によって正しいネットワークビューを提供してくれるツールが必要」・ 「マルチベンダーのツールでない限り、ツールが多すぎて、すべてを処理しきれない」・ 「イベントが正常かどうか教えてほしい」・ 2 社のお客様が、階層 2 で解決される問題は 15 % と報告 (範囲内の最低の数値)・ 2 社のお客様が、階層 2 で解決される問題は 70 % と報告 (範囲内の最高の数値)
まとめ	<p>ネットワーク ドキュメントは必ずしも正確で信頼できるとは限らないため、現場担当者は、解決に必要なレベルまで問題を掘り下げられるよう、正確・タイムリー・詳細な情報が得られるツールを必要としています。現状では、現場担当者は、関連付けロジックのない断片化したツールを使用しなければならず、それでは raw データが多すぎて十分な洞察結果が得られません。</p>

エキスパート

一般に、その次にエスカレーションされるレベルが、エキスパートになります。これらのアーキテクトは、最も多くのトレーニングを受け、認定や経験を最も多く持っていますが、将来を考慮したプランニングにも取り組んでいるため、エスカレーションによって頻繁に割り込みが入ることを快く思わない場合がほとんどです。もう1つの問題は、エキスパート知識の多くが「仲間内の知識」であるということです。これは、もっと低いサポート階層に広まれば役立つであろうと思われるかもしれませんが、大部分は文書化されていないため、広めるのは困難または不可能な場合がほとんどです。

図 6. エキスパート (階層 3 および 4) ネットワーク アーキテクトの典型例



概要	<ul style="list-style-type: none"> ・ 最も豊富な経験 <ul style="list-style-type: none"> - 認定 - トレーニング/教育 ・ 社内 (常時) ・ 最高の責任: ネットワークの設計とプランニング
責任	<ul style="list-style-type: none"> ・ 高レベルのアラートとビジネス インパクト ・ 高度なツールと仲間内の知識 ・ 複雑な問題のシナリオ プランニング ・ 全体像とリアルタイムのモニタリング ・ 大規模な修正の調整 ・ マルチベンダーによる解決 ・ エンドツーエンドの可視性 ・ 最終責任者

ニーズと動機 付け要因	<ul style="list-style-type: none">・ 問題が適切に送られてこないことが多いため、本当にネットワークが原因かどうかを最初に確認する必要がある・ 実際のデータ ポイントで問題をシミュレートして問題の重大度、スケール、インパクトを評価する必要がある・ 表面的な症状や問題を解釈して根本原因を突き止める必要がある・ 重大度 1 および 2 の問題について、適切なエキスパートに迅速に連絡して効果的に連携する必要がある・ 喫緊のニーズに対して迅速な修正または永続的な回避策で対処する必要がある・ 複数のデバイスにわたるオーケストレーション ツールが必要・ キャパシティ プランニング、可視性、予測の向上が必要
問題点	<ul style="list-style-type: none">・ 階層 1 で修正されるべきだった問題が送られてくることが、あまりにも多い・ トラブルシューティングのためプロジェクト作業を中断させられることが、頻繁にある・ ネットワークの問題ではないことを証明するために時間を取られる
コメント	<ul style="list-style-type: none">・ 「経験をソフトウェアに投入してくれるとありがたい」・ 「今の仕事は仲間内の知識に依存しており、持続可能性に欠ける」・ 「問題を解決するには、仲間内の知識とともに、ツールに対するエキスパートの目も依然必要」・ 「プロアクティブに物事を進めるには、コストをかけてトレンドを把握する必要がある」・ 「ネットワークの問題ではないことを証明するために 50 % 以上の時間が取られている」・ お客様の報告を平均すると、階層 3 で解決される問題の割合は 15 %
まとめ	<p>エキスパートは、ネットワークの問題ではないことを証明するために時間を取られているので、実際のデータ ポイントを使用して問題をシミュレートし、問題、重大度、スケール、インパクトを評価する必要があります。現状では、エキスパートは問題のトラブルシューティングに必要以上に時間を割いています（結果的にネットワークとは無関係と判明した問題に、約半分の時間が費やされている）。エキスパートの「仲間内の知識」が、低い階層のエンジニアに伝われば、プロセスの早期に根本原因を特定または潜在的問題を排除するのに役立つでしょう。</p>

プランナー

ここで考察する最後の役割は、主に将来的なネットワーク展開の計画を担当する、ネットワーク エンジニアリング マネージャです。この役割では、ネットワークのトラブルシューティングに費やす時間が大幅に減り、指針、過去のトレンド、分析、キャパシティ プランニングへの関与が多くなります。

図 7. プランナー (階層 3 および 4) ネットワーク エンジニアリング マネージャの典型例



責任	<ul style="list-style-type: none"> 主なキャパシティ プランニング ネットワークの設計およびアーキテクチャ プロシージャの作成 全階層のトレーニングの作成 毎日の健全性レポート 過去のトレンドと分析 ツールとプロセスの改善 市場動向調査
ニーズと動機 付け要因	<ul style="list-style-type: none"> 問題に対して単なる受動的対応ではないプロアクティブな対応を行うために、ネットワーク パフォーマンス、可用性、およびユーザに関する優れた可視性と分析が必要 何が適用可能か評価するために、市場をリードする製品とケース スタディを先取りする必要がある 企業のネットワーク ニーズを向上させるため、より堅牢で相関性のあるツールにアップグレードする必要がある 導入された製品がインテントに合致しているか監査するツールが必要 予測も行う優れたキャパシティ プランニング ツールが必要
問題点	<ul style="list-style-type: none"> 他のグループの作業が完了するまで待つ必要がある
まとめ	<p>プランナーは、問題を (受動的にではなく) プロアクティブに解決するために、ネットワーク パフォーマンスに対する可視性と分析を必要とします。現状では、他のグループには必要な情報を自身で収集し分析するツールとアクセス権限がないため、プランナーは、他のグループの作業が終了するまで待つことを余儀なくされています。</p>

テクノロジー要件

インテントベース ネットワーキングの戦略的ビジョンは、自己学習、自己防御、自己修復するネットワークを構築することにあります。

ネットワークが自らを修復するという考え方は、現実というより SF のように感じられるかもしれませんが、アーキテクチャの観点から見れば、最初の印象よりは若干現実的に思えてくるのではないのでしょうか。

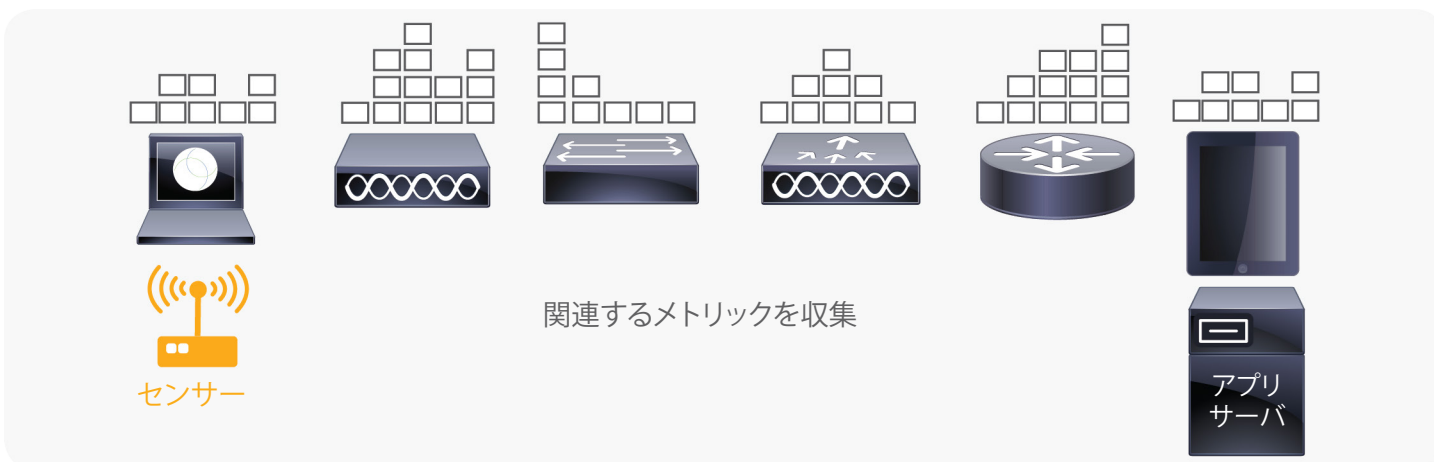
Cisco DNA Center™ はエンタープライズ ネットワークに自動化と分析を導入するプラットフォームですが、自己修復型ネットワークを究極の目標とするのであれば、アーキテクチャ全体でインテントベース ネットワーキングを提供する必要があります。

このセクションでは、こうしたテクノロジー アーキテクチャ要件の概要を説明します。

計測

未測定のをモニタリング、レポート、分析、関連付け、学習することはできません。そのため自己修復型ネットワークでは、図 8 に示すように、計測が第 1 のアーキテクチャ要件になります。

図 8. アーキテクチャ要件 1: 計測



この目的のために、シスコでは、Cisco Unified Access™ Data Plane (UADP) 2.0 Application-Specific Integrated Circuit (ASIC) を基盤にした Cisco Catalyst® 9000 スイッチング ファミリーなどの Cisco DNA 対応ネットワーク デバイスに、定期的な計測を導入しました。各 UADP 2.0 ASIC が 384,000 の柔軟なカウンタをサポートしており、それを使用してチップ内の事実上あらゆるイベントを計測することができます。また、各 ASIC では、テーブル内に 128,000 の NetFlow レコードを保存できます。

一方、計測を必要とするのはネットワークだけではないことも指摘しておくべきです。たとえば、ユーザの Quality of Experience (QoE) を正確にキャプチャするには、ネットワークの Quality-of-Service (QoS) メトリック (損失、遅延、ジッターなど) を計測するだけでなく、フローに影響するあらゆる要素 (クライアント エンドポイント、センサー、アプリケーション サーバなど、ネットワークの外部で動作するハードウェアおよびソフトウェア要素を含む) から、関連するパフォーマンス メトリックを収集することが不可欠です。

クライアントの計測も可能です。分析を目的としたクライアント計測の有効な例としては、Apple と Cisco iOS による分析が挙げられます。この分析では、Apple デバイスが (信号レベルと雑音比も含めて) 観察したアクセス ポイントなどのネットワーク ビューを Cisco DNA アシュアランスと共有するのに加え、それらのデバイスとネットワークの関連付けが解除された原因 (デバイスがアイドルになったことなど) も、分析エンジンと共有します。

クライアント計測のもう 1 つの有益な例として、適応型アプリケーション動作の観察があります。たとえば、多くのマルチメディア アプリケーションで、レート適応型のビデオ コーデックが使用されています。これらのコーデックにより、ネットワークの状況に応

じて解像度とフレーム レートを上下させることができます。たとえば、適応型のビデオ コーデックによってネットワーク輻輳が検出され、その補償としてビデオ解像度が Full HD (1080p、1920x1080 ピクセル) から VGA (640x480 ピクセル) に低下し、ビデオ フレーム レートが 24 フレーム/秒 (fps) から 5 fps に低下した例を考えてみましょう。この場合、ビデオ品質が 97 % 低下します。そのような調整を行うと、損失と遅延に関するネットワーク サービス レベル属性が、いずれも最高レベルになる可能性があります。ただし、これらのネットワーク メトリックだけでユーザ エクスペリエンスの大幅な低下が判断されるわけではありません。そのため、エンド ユーザのエクスペリエンスを正確に反映するには、クライアントやアプリケーション サーバなどネットワーク外部の関連 KPI (主要パフォーマンス評価指標) を計測する、より全体的なアプローチが必要になります。

ネットワーク外部のメトリックを計測するもう 1 つの方法が、センサーによる計測です。たとえば、ワイヤレス センサーを全社に導入して、オンボーディング エクスペリエンスや、ネットワーク サービスの可用性とパフォーマンス (認証、認可、アカウントティング (AAA)、Dynamic Host Configuration Protocol (DHCP)、DNS など)、さらには特定のアプリケーションなどについて、プロアクティブかつ継続的にテストして報告することができます。

分散型オンデバイス分析

ネットワーク デバイスやその他のデバイスで計測できるデータが増えてくると、それぞれの場合に適切なアクションを実行できるようにするには、最もクリティカルな KPI はどれか判別しなければならないという課題が生じます。たとえば、各 UADP 2.0 ASIC 上にある 384,000 のフレキシブル カウンタすべてが同等に重要であり、それぞれ特定のアクションを必要としている場合、それらすべてに対応すると、すぐに CPU やネットワーク リソースのフラッドが発生します。

そうした状態を補正するために、オンデバイス分析が推奨されます。それによって、重要なメトリックを特定してただちに処理することが可能になります。一方、クリティカルでない他のメトリックは、情報目的または高度なトラブルシューティング シナリオ用として保持されます。それについては後述します。オンデバイス分析は、(分析と処理を分散することにより) アーキテクチャの効率性を向上させるだけでなく、(外部の分析エンジンにテレメトリを送信して応答を待つことなく、デバイスが問題を自己分析し、ただちに修復できるため) 応答性を改善するのにも役立ちます。オンデバイス分析を表したイラストを、図 9 に示します。

図 9. アーキテクチャ要件 2: オンデバイス分析

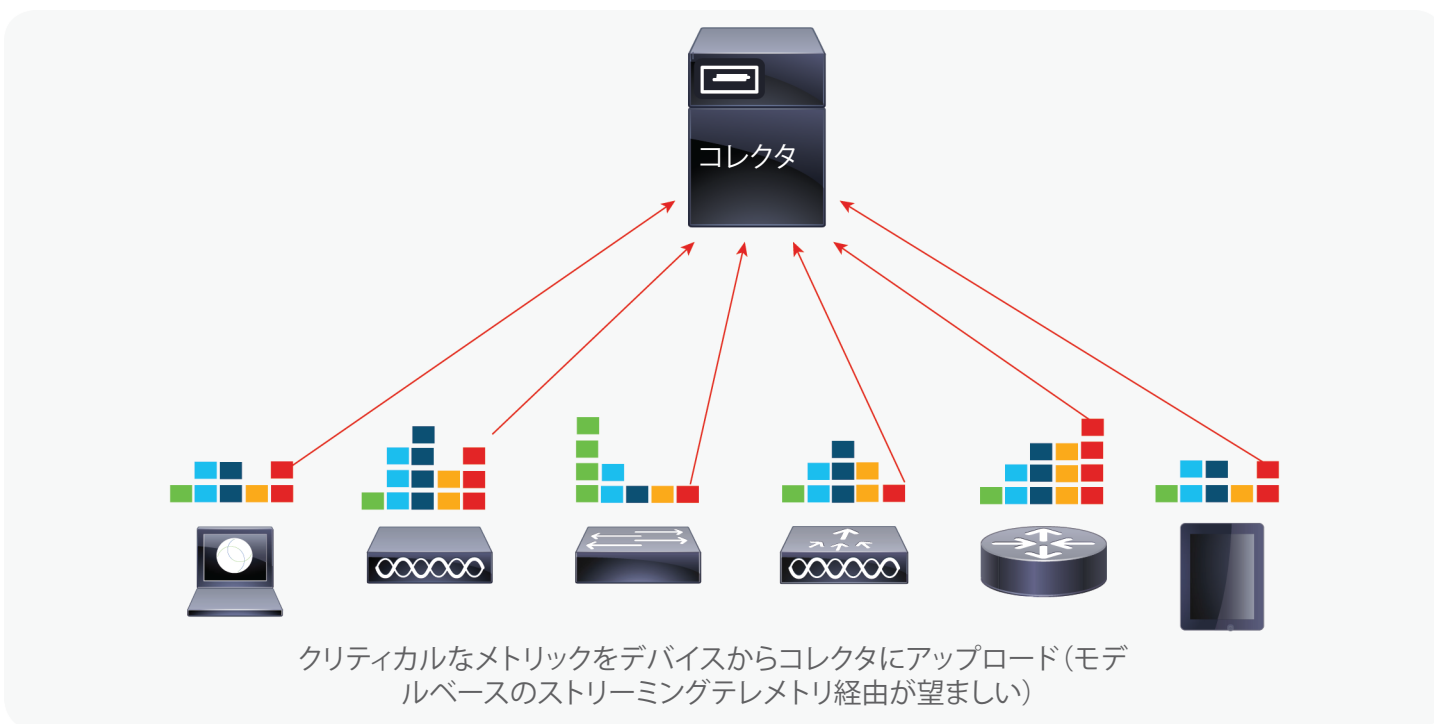


テレメトリ

次の課題となるのが、デバイスからのデータの取り出しです。それにはテレメトリが必要になります。テレメトリは、Simple Network Management Protocol (SNMP)、syslog、NetFlow などのレガシー プロトコルを含め、長年にわたってさまざまな形式で存在してきました。しかし SNMP をはじめとする一部のプロトコルは、デジタル ネットワーク アーキテクチャで使用するには重大な欠点があります。たとえば SNMP はポーリングベースであるため、クリティカルな KPI がデバイス上で測定されても、コレクタは次のポーリングまでそれを認識することができません。さらに、必要なデータ ポイントがたとえ 1 つだけの場合でも、MIB 全体をコレクタに読み込む必要があります。また、複数のレシーバがこの情報を必要とする場合には、SNMP 情報を各レシーバにユニキャストしなければなりません。こうした制限があるため、SNMP は、プログラム可能なインフラストラクチャにとっては低速で非効率なプロトコルになっています。

これに対して、モデルベースのストリーミング テレメトリは、デバイスからのデータ取り出しに大幅な改善をもたらします。まず、データをデバイスから(特定のポーリング間隔で「プル」するのではなく)いつでも「プッシュ」することができます。さらに、MIB 全体ではなく個々のメトリックのストリーミングが可能です。たとえば、特定のアプリケーションがルータでドロップされたかどうか知りたい場合には、「show policy-map interface」コマンドで表示されるすべての統計値とカウンタを含む) CISCO-CBQOS-MIB 全体をプルして関連キューを検索してからそのキュー内のドロップを検索するのではなく、その特定のアプリケーションについてドロップがカウントされたときには必ずルータからアラートがプッシュされるよう設定することができます。さらに、情報をメッセージ バスでストリーミングすることができるので、データに関心を持つすべての関係者が、ただちに効率よくデータを受け取ることができます。図 10 に、ストリーミング テレメトリを通じてクリティカルなメトリックがデバイスからコレクタにプッシュされる様子を示します。

図 10. アーキテクチャ要件 3: テレメトリ



リアルタイムで判断を行う必要性を含め、デジタル ネットワークには動的な性質があるため、回避可能なネットワーク停止の低減(または撲滅)や、緊急事態の検出と即時の対応の自動化などの、ネットワークのモニタリングとトラブルシューティングに関する課題を解決するには、ストリーミング テレメトリが重要になります。

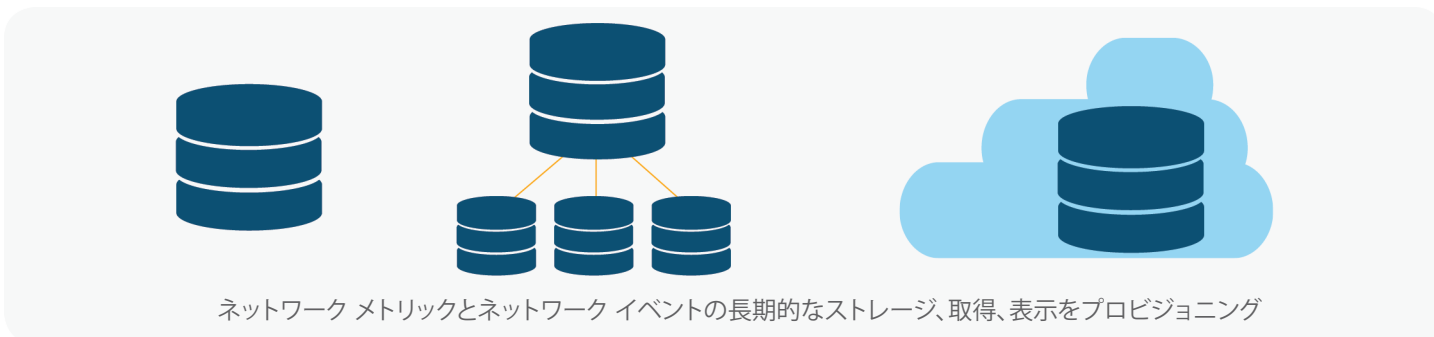
拡張可能なストレージ

ネットワークでは莫大なデータ量(一般には 1 日約 1 TB)が生成される可能性があるため、拡張可能なストレージを適切にプロビジョニングすることが必要になります。拡張可能なストレージには次のような形態があります。

- ・ 一元化されたコレクタ: 導入は簡単ですが、3 つのオプションのうち拡張性は最も低くなります。
- ・ 分散したコレクタ: 拡張性が向上しますが、複雑性も増大します。
- ・ クラウドベースのコレクタ: 拡張性が最大で、運用も容易ですが、一般的にクラウド サービス プロバイダーへの継続的な出費が必要になります。

これらのストレージ オプションを図 11 に示します。

図 11. アーキテクチャ要件 4: 拡張可能なストレージ



どのオプションを選択しても、ネットワーク アーキテクトはいずれ、どのぐらいの量のデータをどの程度の期間保存する必要があるかという問題に直面することになります。これらの拡張可能なストレージ ソリューションはどれも、(少なくとも大きなコストなしでは) 継続的な容量を無限に提供するわけではありません。そのため通常は、定義された時間間隔で raw データの集約が行われます。たとえば、30 日後に(すべての raw データ ポイントではなく) 平均値と最小/最大の外れ値を保存するなどの定義を行うことが可能です。粒度の細かいデータを粗いレベルへと加工する時間間隔は、企業のポリシー、規制要件、容量のトレンドと計画要件などによって変わってきます。

分析エンジン

ネットワークから収集されたデータが一元化ストレージ システムまたは分散ストレージ システムまたはクラウドベースのストレージ システムに保存されると、分析が可能になります。最初に行われる分析操作の 1 つに、基準の確立、つまり「正常」な状態(または少なくとも特定のエンタープライズ ネットワークにおける正常な状態)の定義があります。基準が確立されると、図 12 に示すように、異常(基準からの大幅な逸脱)を特定し、さらなるアクションを始動させることができます。

図 12. アーキテクチャ要件 5: 分析エンジン

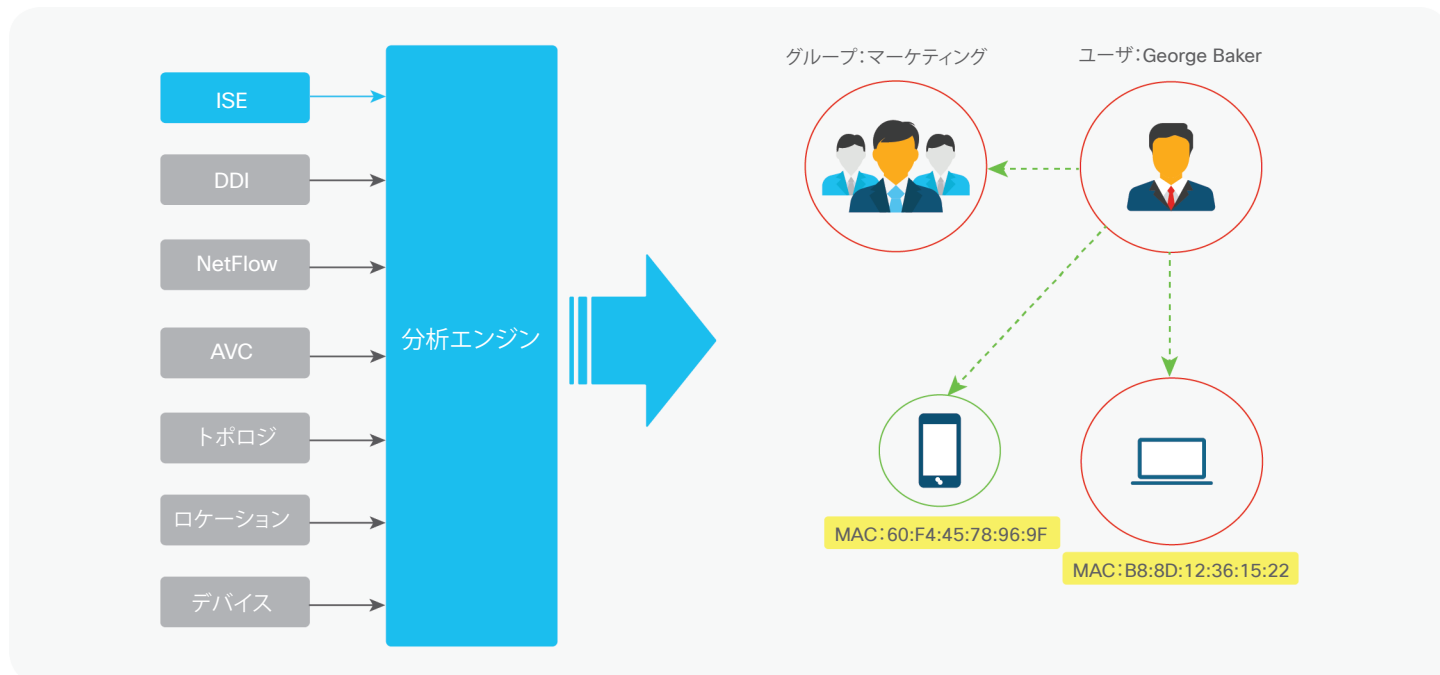


分析エンジンの主な役割は、コンテキストを提供することです。ネットワーキングでは、状況を理解する上でコンテキストが不可欠な役割を担っています。それによって正確な洞察結果が得られ、問題を修復するための適切なアクションを実施できます。理想的には、対象のオブジェクトまたはイベントについて複数のデータ ソース(つまり複数の視点)を関連付けることで、正確なコンテキストが得られます。次のネットワーキングの例について考えてみましょう。

この例では、あるユーザが IT ヘルプ デスクに問い合わせ、Cisco Webex® のアプリケーション パフォーマンスが低いと訴えています。問い合わせを受けたアナリストには、ネットワークとアプリケーションのどちらが問題なのかわからず、根本原因がどこにあるのかもわかりません。しかし複数の情報源を関連付ければ、根本原因を効率的かつ効果的に絞り込める可能性があります。図 13 ~ 19 に、そのような問題のトラブルシューティングを行うネットワーク アナリストが、分析エンジンによって複数のデータ ソースを関連付けることで、コンテキストと洞察結果を徐々に得ていく様子を示します。

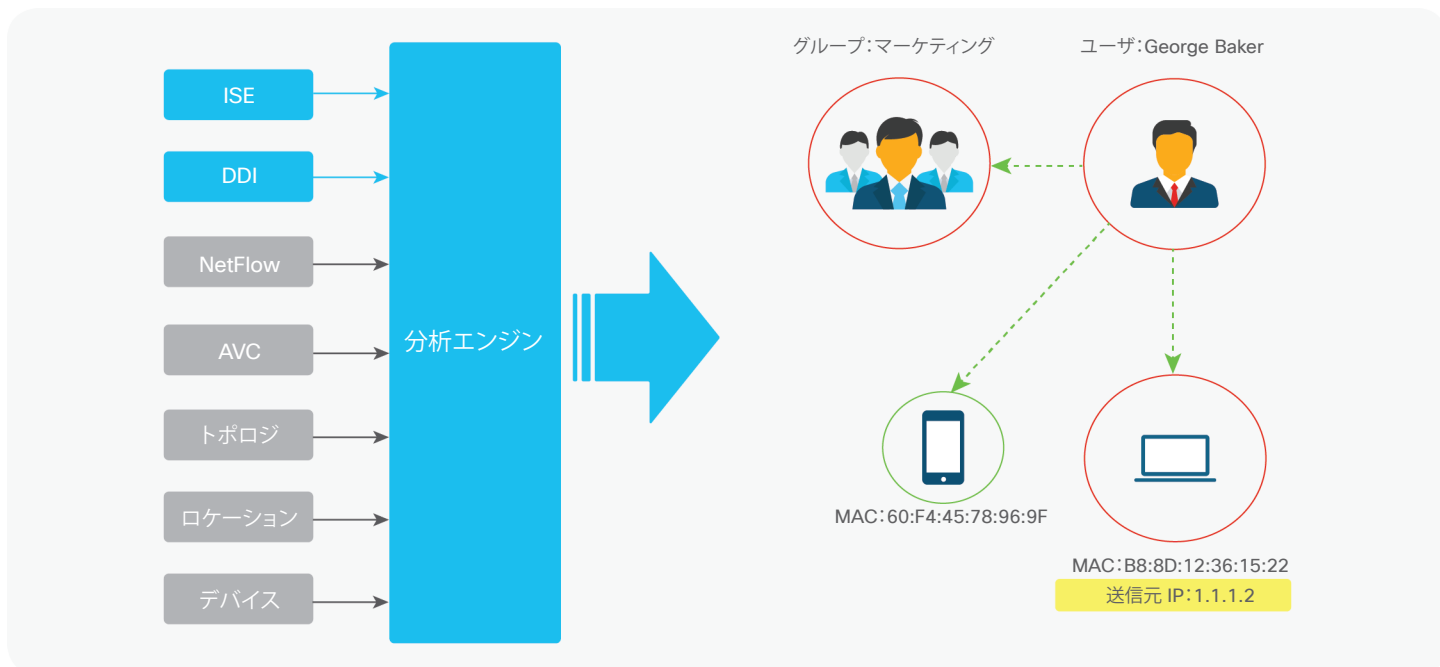
ユーザのアイデンティティが明らかなので、分析エンジンは最初に、図 13 に示すようにポリシー エンジン (具体的には Cisco Identity Services Engine (ISE)) にユーザと使用デバイスの詳細を問い合わせることができます。

図 13. コンテキストの関連付けの例、パート 1: ユーザとデバイスの特定



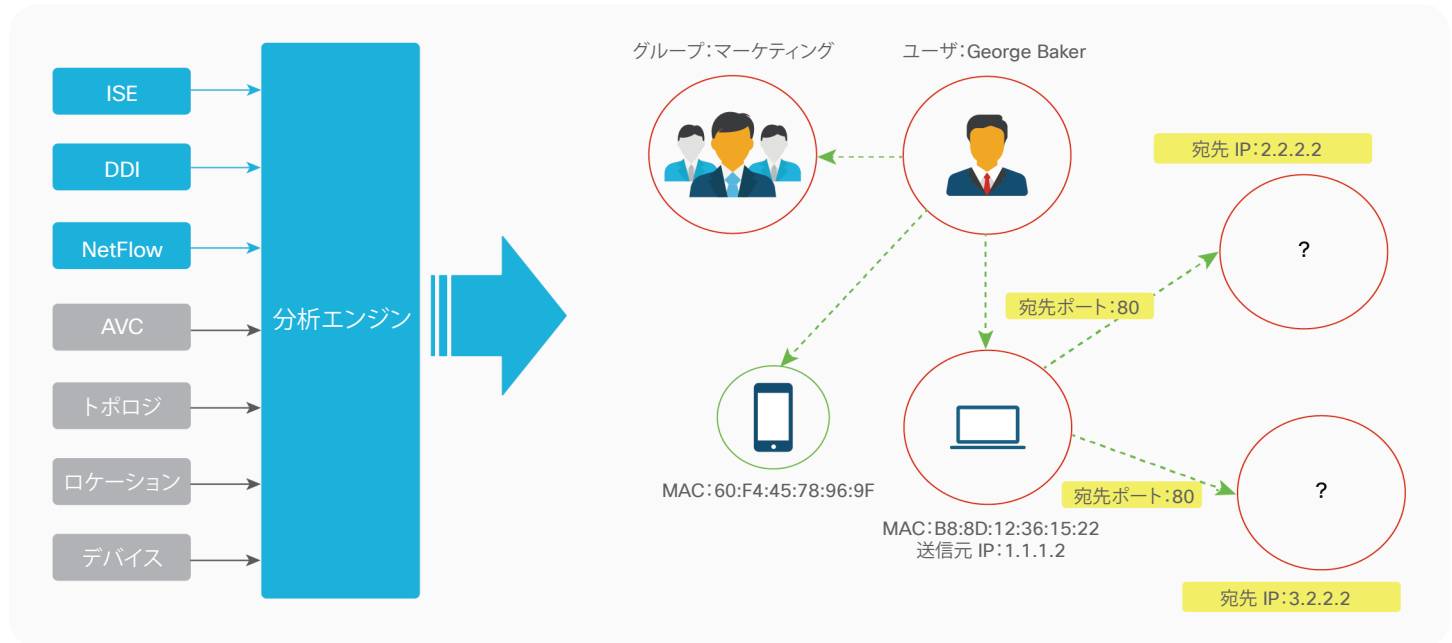
次に、図 14 に示すように、ユーザのデバイスの MAC アドレスを、DNS、DHCP、および IP アドレッシング システムから提供されたデータに関連付けて、問題が発生しているデバイスの IP アドレスを特定します。

図 14. コンテキストの関連付けの例、パート 2: クライアント IP アドレスの特定



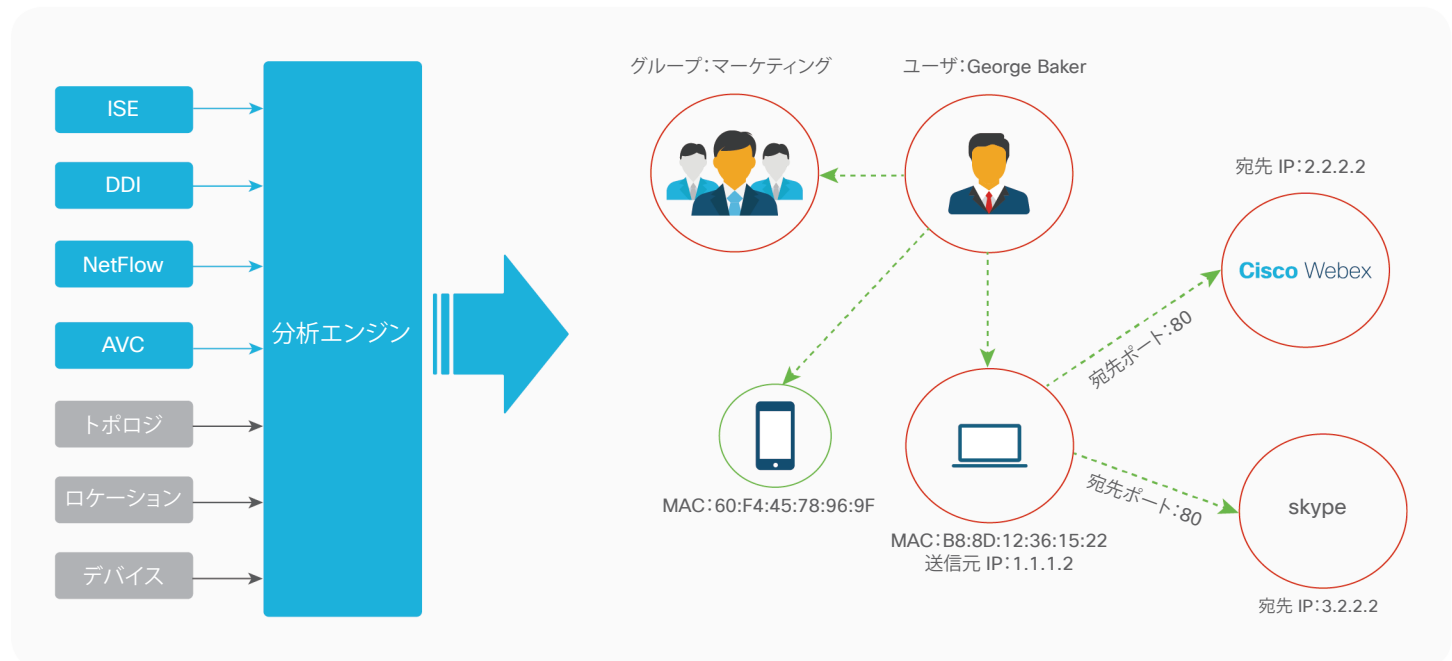
続けて、図 15 に示すように、クライアント デバイスの「送信元アドレス」フィールドに一致するレコードをフィルタリングして、デバイスの IP アドレスと NetFlow レコードを関連付けます。

図 15. コンテキストの関連付けの例、パート 3: フロー レコードの特定



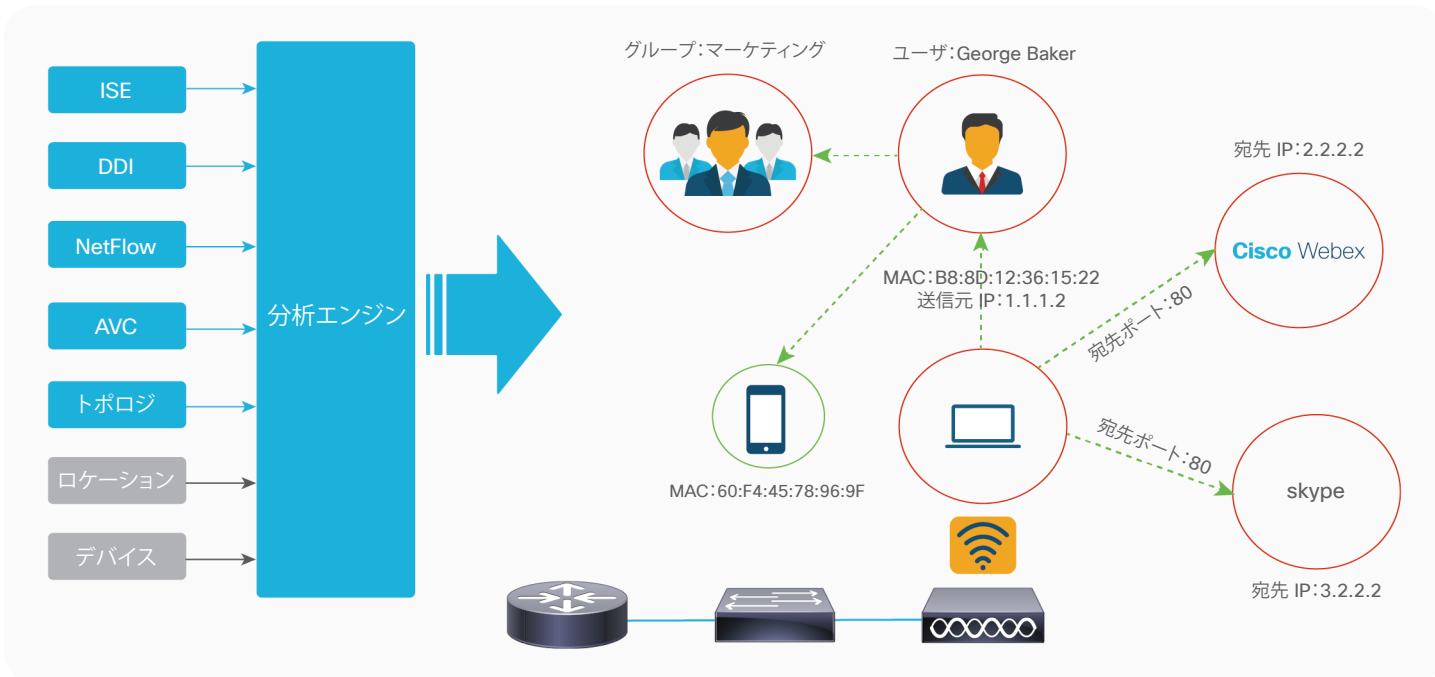
この時点で疑問となるのは、問題が発生した Webex® アプリケーションと関係していたのはどのフローだったのかということです。基本的な NetFlow レコードには、フローを生成したアプリケーションを示す詳細情報は含まれていません。しかし、Application Visibility and Control (AVC) テクノロジーを通じてこの情報が NetFlow レコードに挿入されている可能性があります。これで、図 16 に示すように、フローとそれぞれのアプリケーションが関連付けられ、Webex フローが明確に特定されました。

図 16. コンテキストの関連付けの例、パート 4: アプリケーション フローの特定



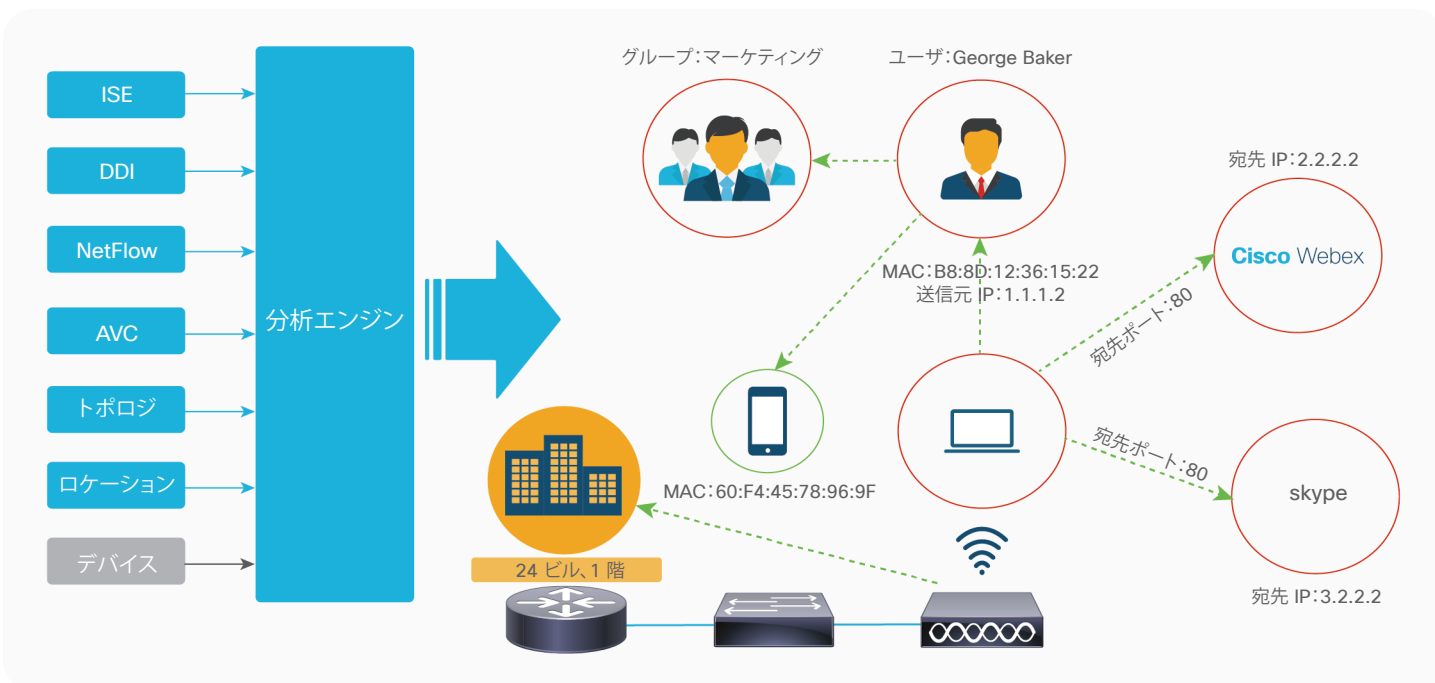
次に分析エンジンは、図 17 に示すように、クライアントのアタッチメントポイントから開始して、フローが通過したネットワークトポロジを関連付けます。

図 17. コンテキストの関連付けの例、パート 5: ネットワークアタッチメントポイントとネットワークトポロジの特定



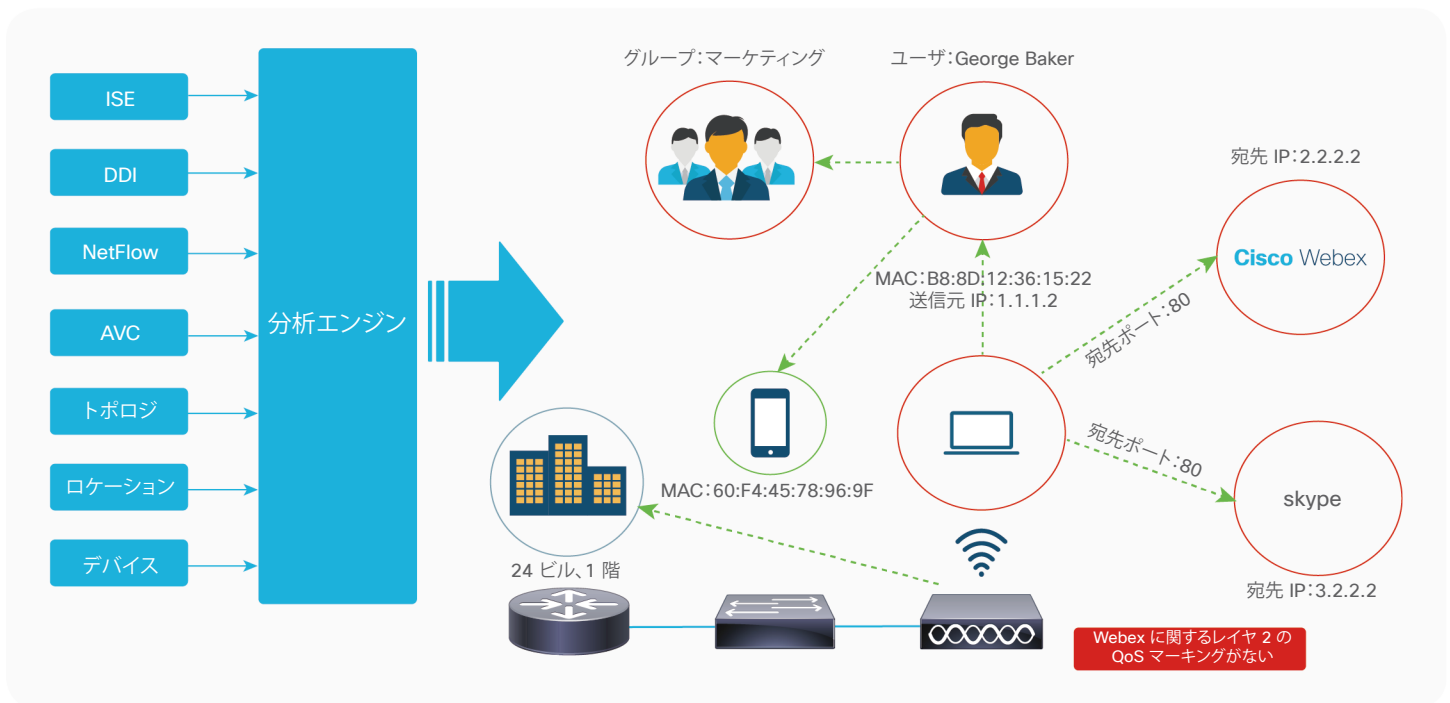
場合によっては問題が特定の建物やサイトに限定されていることがあるため、図 18 に示すように、地理的な位置が関連付けられることもあります。

図 18. コンテキストの関連付けの例、パート 6: ロケーション情報の関連付け



続いて、図 19 に示すように、KPI、ポリシー メトリック、設定の詳細、syslog などを含むデバイス情報をすべて関連付けに含めることで、ネットワークの問題の根本原因を特定できます。

図 19. コンテキストの関連付けの例、パート 7: ネットワーク デバイス データの関連付け



この例では、コンテキストを包括的に関連付けることで、アプリケーションのパフォーマンス低下の根本原因がワイヤレス LAN での QoS マーキングおよび処理の欠落にあったことが、正確に特定されました。

ただし、根本原因が判明するだけでは不十分です。実施可能な修復措置が必要です。この例の場合、George Baker の iPhone で iOS 機能の Fast Lane を有効にしたり Webex をアプリケーションのホワイトリストに含めてこの優先処理の対象にしたりするなどの修復方法を、この時点でオペレータに示すことができます。そして、推奨されたこの修復操作は、アナリストによって 1 回のクリックで実施することができます。今後、最終的にはこの作業は自動化されます。

機械学習

前述のように、分析エンジンは、特定のデータ ポイントを他のデータ ポイントと比較するようにプログラミングする必要があります。しかし、エンタープライズ ネットワークのデータ ポイントの順列・組み合わせの数は膨大であるため、どんなプログラマーであっても、それを特定するのは非常に困難であり、ましてやプログラミングするなどほぼ不可能です。そこで、これまで不明であった関連付けや因果関係を検索および特定するために、機械学習アルゴリズムで従来型の分析エンジンを補います。

機械学習は、ガイド付きまたはガイドなし(「監視あり」または「監視なし」とも呼ばれます)で実行できます。ガイド付きの方法では、機械学習によって観察結果が人間のオペレータに提示され、オペレータはその観察結果に関心があるかどうかを入力します。関心があるとされた場合は、人工知能(AI)が学習パターンを調整し、類似する関係を探します。Cisco DNA アシュアランスでは、機械学習アルゴリズムがガイド付きで動作します。オペレータは、「(親指を立てる) 受理」アイコンをクリックして観察結果を「関心あり」としてタグ付けするか、「(親指を下げる) 却下」アイコンをクリックして「関心なし」とすることができます。

図 20. アーキテクチャ要件 6: 機械学習



認知分析および予測分析のために、すべてのデータ ポイントと順序・組み合わせを分析

前述のように、エンタープライズ ネットワーキングでは、ユーザとアプリケーション間の障害点が 100 を超える可能性があります。そのため、あり得るすべてのデータ ポイント関連付けの順序・組み合わせを特定して理解し、最終的には分析エンジンにプログラミングする作業は、人間の能力をすぐに超えてしまいます。たとえば 100 の障害点がある場合、その障害の原因になった可能性のある組み合わせの数は、 $4,950 [(n * (n-1) / 2)]$ になります。

そこで、機械学習を導入します。機械学習は人工知能の応用であり、明示的にプログラミングされていなくても自動的に経験から学習して改善を行う能力を、システムに提供します。主な目的は、人の介入を最小限に抑えて（または、まったく無しで）システムが自動的に学習できるようにすることです（図 20）。

機械学習のプロセスは、データの監視と、関連付け・推論・予測を改善するためのデータ内/パターンの探索から始まります。たとえば次のような状況が考えられます。

- ・ データ ポイント間のパターンがない
- ・ データ ポイント間のパターンが、まったくの偶然に起因している可能性がある
- ・ データ ポイント間のパターンが相関関係を示している
- ・ データ ポイント間のパターンが、因果関係に基づく結果である

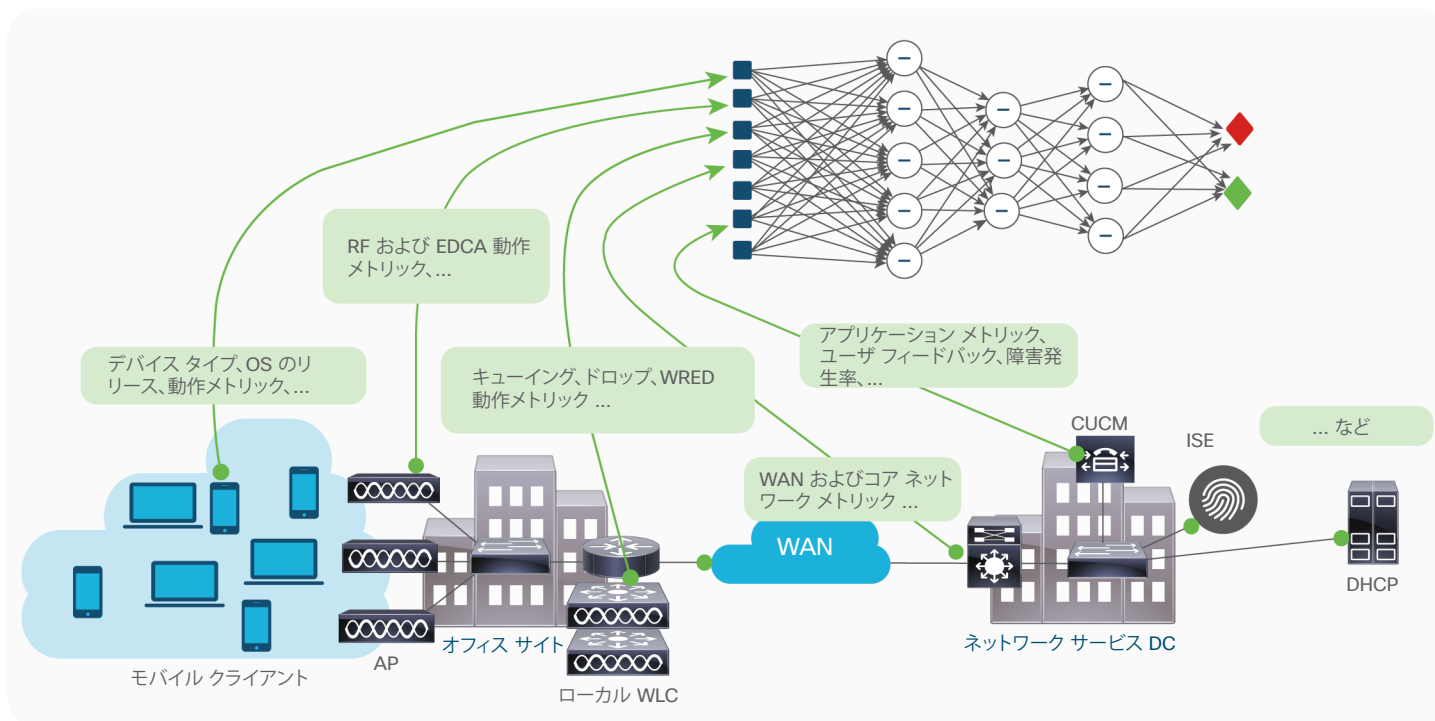
相関関係を示すパターンが特定された場合、AI は、類似するパターンを検索して根本原因を特定できます。たとえば、特定のクライアント オペレーティング システムと、ワイヤレス ローミング レートの高い複数のインスタンス間で相関関係が特定された場合、AI は、このパターンと比較して、そのオペレーティング システムが動作するすべてのクライアントを調査できます。それにより、クライアント OS でのローミングのパフォーマンス低下の根本原因を特定できる可能性があります。ただし、実際には根本原因が別にある可能性もあるため、この相関関係が必ずしも因果関係に基づく結果であるとは限りません。たとえば、クライアントの OS バージョンとたまたま同時期にリリースされたハードウェア ドライバが実際の根本原因であったことが判明する場合もあり得ます。

このような問題の根本原因を特定するのが、**認知分析**の機能です。ただし、いったんこれらの根本原因が特定されると、認知分析が**予測分析**の領域まで発展することがあります。言い換えると、目前の問題を、実際の発生に先立って予測します。その目標は、そもそもそうした問題が発生しないようにするデータ主導型のアクションを実施することにあります。

たとえば、デバイスのメモリ消費とデバイスのクラッシュの間に因果関係があると特定された場合を考えてみましょう。この因果関係を特定し、デバイス ファミリのメモリ消費を慎重にモニタリングすることで、プロセスをリダイレクトまたはプルーニングしてシステム クラッシュを未然に防止することが可能になります。

エンタープライズ ネットワーキングに機械学習を適用する様子を図 21 に示します。

図 21. エンタープライズ ネットワーキングに適用された機械学習アルゴリズム



ガイド付きトラブルシューティングと修復

分析と機械学習は問題または潜在的な問題の特定に役立ちますが、多くの場合、根本原因を分析するには別のトラブルシューティング手順が必要になります。

一般的にこれらの手順は、疑わしいデバイスから追加情報を取得することから始まります。これは、Cisco Technical Assistance Center (TAC) でケースをオープンすることと似ています。TAC では、報告された問題のトラブルシューティングを行う最初の手順として、一般的に、デバイスの「show tech」レポートが TAC エンジニアに提供されます。このレポートには、事実上すべての、モニタリングされたメトリックが含まれています。

その後、通常は、分割統治法的アプローチによって問題領域を隔離し、それを徐々に狭めていって最終的に根本原因を明確にすることが必要になります。この手順には、1 つのテストの結果によって次のテストの内容が決まる、トラブルシューティングテストが含まれる場合があります。

ただし、根本原因を絞り込むことでトラブルシューティングが終了するわけではありません。現在の問題の原因をオペレータに通知するだけでは不十分です。それよりも、具体的な修復方法を提示することが必要です。オペレータは、推奨されるアクションをネットワーク デバイスにプッシュする自動化プラットフォームを通じて、推奨されるアクションをすばやく有効にすることができます。図 22 に、ガイド付きのトラブルシューティングと修復を表したイラストを示します。

図 22. アーキテクチャ要件 7: ガイド付きトラブルシューティングと修復

分析エンジン

Failed to reach from Fabric Edge node to Fabric Border node in the underlay.

Description: There is a connectivity failure from Fabric Edge node <NAME> to Fabric Border node <NAME>. This can prevent many of the Fabric services from functioning correctly.

Impact: Location: San Jose, 6 Switches, 7 Routers

Suggested Actions (4):

1. Verify running configuration compliant with provisioned configuration.
2. Verify routing table on Border node and Edge node.
3. Verify IGP adjacencies are up with the upstream device(s).

コンテキストによってデータを関連付けることで、問題の根本原因を特定

自動化されたトラブルシューティングと修復

ガイド付きトラブルシューティング システムは、自己の有効性をモニタリングする必要があります。実際には、推奨されたアクションによって根本原因が修復されない場合もあります。その場合には、ガイド付きトラブルシューティングのアルゴリズムも、トラブルシューティング手法を学習して適応する必要があります。場合によっては、たとえば「93 % の確率でアクション X がこの問題を解決した」などのように、システムが自己測定した有効性をオペレータに提示することさえあり得ます。

時間の経過とともに有効性スコアが向上してくると、ネットワーク オペレータは、プロセスにおける手作業（つまり、ボタンを明示的にクリックして推奨されるアクションを実行すること）を担当する役割から離れ、同じ問題の発生時にはシステムが「推奨されたアクションを常に実行する」よう設定できるようになります（図 23 参照）。この時点で、自己修復型ネットワークが実現したことになります。

図 23. アーキテクチャ要件 8: 自動化されたトラブルシューティングと修復

ネットワークコントローラ

分析エンジン

推奨されたアクションを実行しますか。

はい 常 いいえ

実用的な洞察結果をオペレータに提示する
根本原因を修復するための入力を求める
自己修復オプションを提示する

自己修復ワークフローによってあらゆる問題に対応できる可能性は低いですが、一般的で反復的な問題には確かに対応可能です。さらに、手動によるプログラミングと機械学習の両方を通じて、対応可能な問題の数は時間の経過とともに増加します。

ここで重要なのは、この最後のアーキテクチャ要件には、技術的な課題(自己学習型トラブルシューティング アルゴリズム)だけでなく、信頼性に関する課題も含まれているということです。

この信頼性の問題を説明するために、自動運転車にたとえて考えてみます。一部の自動車メーカー(Tesla Motors など)では、自動運転機能を搭載した車両が生産されています。しかし、このような機能が技術的に存在しても、多くのドライバーはそれを利用しようとは思いません。それは、機能に対する十分な信頼性が確立されていないためです。

この状況はネットワーキングでも同様です。ネットワーク管理者はネットワークの状態について責任を負っています。管理者は、自動化システムの機能を十分に信頼できるようになって初めて、マシンにマシンの修復を任せることができます。そのため、基盤となるプロセスを、高度なネットワーク管理者に最大限に開示することが重要になります。それによって管理者は、システムを謎めいたブラック ボックスとしてではなく、予測可能な確定的システムとして捉え、徐々に信頼性を高めることができます。

自動運転車の例に戻ると、レーダー、レーザー、冗長システムなどに加えて、何十機ものカメラが車の全周囲を常時モニタリングしていることをドライバーが理解すれば、自車の自律機能への信頼感の形成に大きく寄与し、それによって自動機能が使用される可能性が高まります。

注:以前のセクションで、自己修復型インテントベース ネットワークを実現するための 8 つのアーキテクチャ要件を説明しました。このホワイトペーパーの執筆時点(2018 年 4 月)では、これら 8 つのうち 5 つの要件がすでに達成され、今後数ヵ月以内に 6 つ目の要件が達成される予定です。というわけで、自己修復ネットワークは壮大な目標に見えるかもしれませんが、実際にはそれほど遠いものではありません。

DNA Center

前述のように、DNA Center は、ネットワークの設計とプロビジョニング、ネットワーク ポリシーの管理、ネットワークのアシユアランスを行う一元化ソリューションです。

そのために DNA Center アプライアンスには、Cisco DNA と連動する、次のような重要なソフトウェア コンポーネントが搭載されています。

- Network Controller Platform (NCP) : Cisco DNA の自動化コンポーネント
- Network Data Platform (NDP) : Cisco DNA の分析コンポーネント

さらに、ほとんどのプラットフォームと同様、DNA Center にはいくつかの組み込みアプリケーションが含まれています。そうしたアプリケーションの 1 つが Cisco DNA アシユアランスです。これについて、このホワイトペーパーで詳細に説明します。図 24 に、DNA Center 内での NCP、NDP、Cisco DNA アシユアランスの関係を示します。

図 24. DNA Center: NCP、NDP、Cisco DNA アシユアランス



Cisco DNA アシユアランス

シスコでは、ユーザ要件に適應するために、Cisco DNA アシユアランスの設計に、次のようなトップダウン アプローチを採用しました。

- ・ 受動的ではなくプロアクティブ
- ・ すべてのクライアント、ネットワーク デバイス、およびアプリケーションの全体的な健全性を正確に提示
- ・ あらゆるクライアント、ネットワーク デバイス、またはアプリケーションに対して、広い(エンドツーエンドの)可視性と深い(360度の)可視性の両方を発揮
- ・ 機械学習機能によってネットワークを認識
- ・ コンテキストの関連付けによって実用的な洞察結果を提供
- ・ 柔軟かつプログラム可能
- ・ 俊敏なストリーミング テレメトリによってマイクロサービスを提供
- ・ オープン インターフェイスと充実したパートナー エコシステムをサポート
- ・ ハイパー分散型でマルチテナント型のクラウド対応アーキテクチャをサポート
- ・ 修復プロセスを完全に自動化する長期的目標を視野に、ガイド付き修復を提供

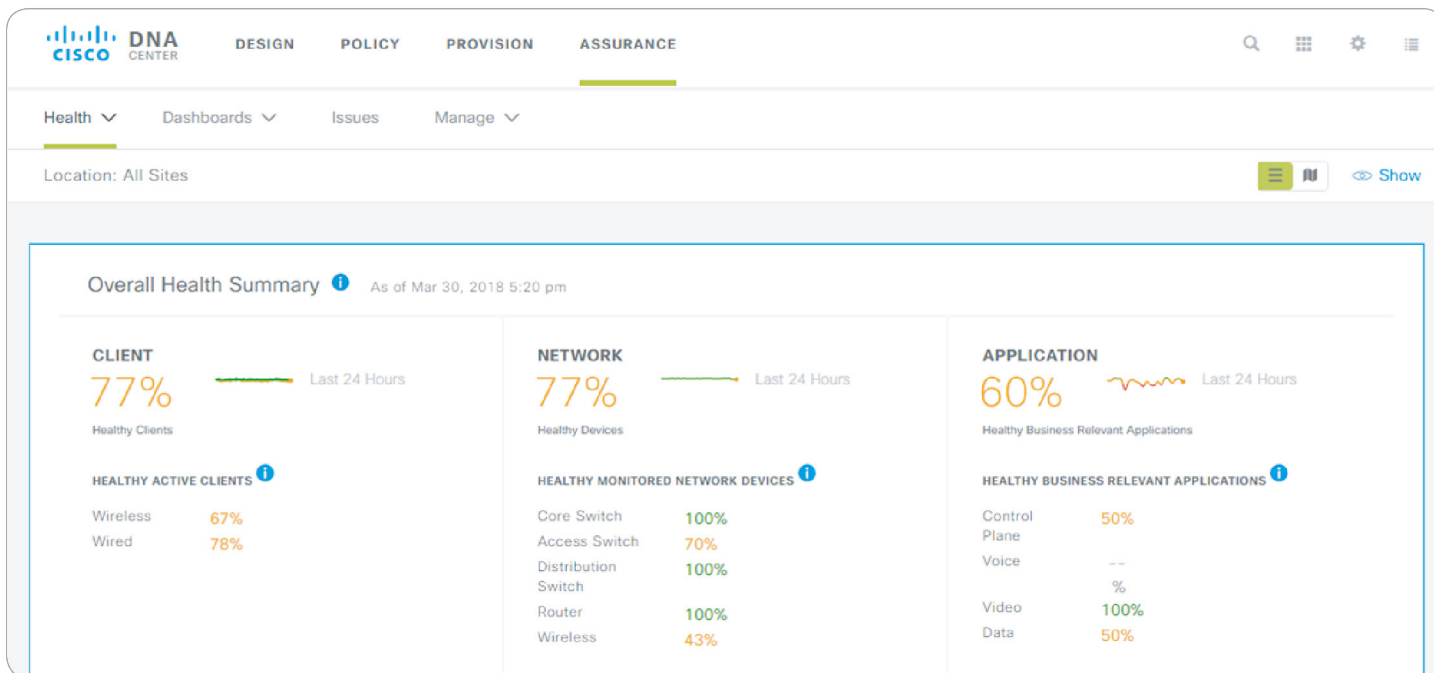
こうして、Cisco DNA アシユアランスには次のような主要機能が含まれました。

- ・ ネットワーク デバイスと、ネットワークに接続しているクライアントから常時学習することで実現される、エンドツーエンドのネットワーク可視性
- ・ ユーザから苦情が出る前にプロアクティブにイベントを特定して対応できる、実用的な洞察結果
- ・ 100 を超える洞察結果に対するガイド付き修復アクション
- ・ 時間を遡って過去のネットワーク問題をトラブルシューティングする機能
- ・ 数秒以内でのリアルタイム アプリケーショントラフィック フロー可視化による、ネットワーク可視性の向上と問題解決時間の短縮
- ・ 事前に問題の根本原因を詳細に特定する、プロアクティブなトラブルシューティング機能

ランディング ページ (図 25) からわかるように、Cisco DNA アシユアランスは、3 つの側面から見た健全性に基づいて企業をモニタリングします。

- ・ ネットワークの健全性
- ・ クライアントの健全性
- ・ アプリケーションの健全性

図 25. Cisco DNA アシユアランス:ランディング ページ



まとめ

このホワイトペーパーでは、Cisco DNA アナリティクスとアシユアランスについて説明しました。まず、インテントベース ネットワーキング アーキテクチャにおける、分析とアシユアランスに関するビジネス要件とユーザ要件の概要を示しました。

次に、自己修復型ネットワークにおけるテクノロジー アーキテクチャ要件の概要を示しました。その要件とは次のとおりです。

- ・ 計測
- ・ 分散型オンボード分析
- ・ テレメトリ
- ・ 拡張可能なストレージ
- ・ 分析エンジン
- ・ 機械学習
- ・ ガイド付きおよび自動化されたトラブルシューティング

これらの要件のほとんどが、すでに Cisco DNA で提供されており、追加のコンポーネントも着々と加えられています。

最後に、これらすべてのテクノロジーを活用してネットワーク/クライアント/アプリケーション アシユアランスを社内に提供する DNA Center 内アプリケーションとして、Cisco DNA アシユアランスを紹介しました。