アリスタ・ホワイトペーパー

EOSとsFlowの活用でネットワークの高度な可視化を実現

現在、データセンターのアーキテクチャは、共通インフラ、共有サービス、クラウド型の2階層ネットワークへと統合が進んでいます。こうした中、システム使用率、ネットワーク使用率、合計容量は上昇を続けており、現行の世代の監視用ツールやアプリケーションでは、そのペースに追いつくことができません。

以前は、戦略的にネットワークの輻輳ポイントで専用のハードウェア・プラットフォームをいくつか使用して、アプリケーション・レベルのフローの可視化を実現するという方法も可能でした。しかし、アプリケーションの動作が変わり、インフラの共有の度合いが高まり、マルチパス・ネットワークが広く展開されている現在では、既存のツールでは、可視化を実現したり、次世代環境で求められる規模とコストを実現したりといった目標を達成できません。

アリスタのデータ分析ツールなどの手段により、テレメトリー・ネットワークの統合やオーバーレイを通じて、完全なパケット・キャプチャを利用することも可能です。しかし、データの量が多すぎてリアルタイムで効果的に処理するのが難しいケースもよくあり、データ・マイニングやストレージに課題をもたらしています。

こうした課題を克服するためには、モニタリングに2階層型の手法を取り入れる必要があります。まずは、ネットワーク全体の活動の概略を把握して、異常な動作を基本的なレベルでつかんだうえで、特定のホットスポットやフローに着目し、詳細なキャプチャと分析を行うという方法です。

ARISTA

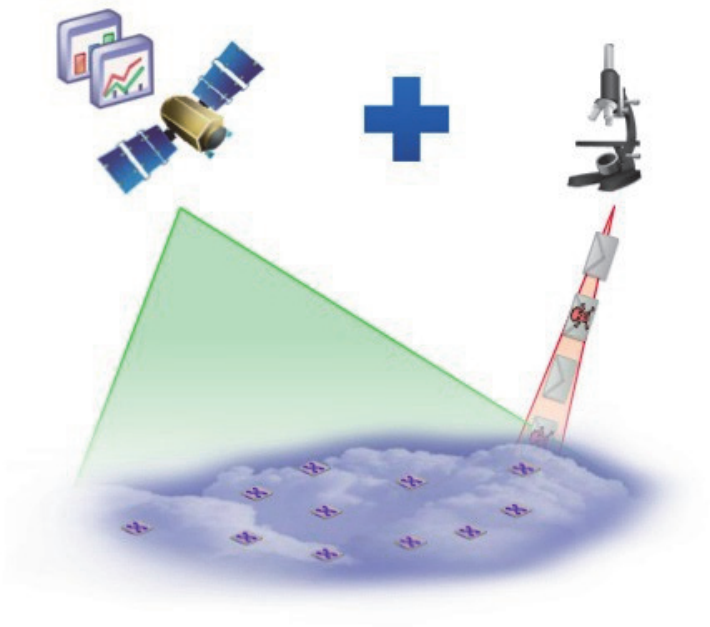

図1：概略の分析と詳細な分析を組み合わせることで最大限の可視化を実現

フロー分析

フロー分析の考え方は新しいものではなく、ハイエンドのルーターやイーサネット・スイッチの多くがその機能を提供しています。しかし、システムの合計回線容量が10～40Tbpsへと劇的に増加し、インターフェイス速度が1GbEから100GbEにまで移行したことから、ネットワークのスループットが伸びるペースは、ネットワーク・デバイスのコントロール・プレーンが搭載している汎用的なCPUの処理能力が向上するペースを大きく上回っています。したがって、リアルタイムの監視やサンプリング・フローのモニタリングの規模を拡大するには、かなりの考慮が必要です。

従来は、フローの可視化はデバイス中心という面が大きく、各ネットワーク・デバイスが専用の処理能力とメモリ・リソースを利用して、自デバイスを通過するIPフローを追跡していました。各デバイスのフロー・テーブルは、まずローカルで処理してから、一元的な場所に送信し、集約と分析を行っていました。

この方法は、トラフィックのパターンが垂直型（North/South）中心でインターフェイスの数（および合計スループット）が比較的少なかった頃には効果的に機能していました。しかしその後、演算処理への負担がアンバランスに大きくなりました。ポート密度とインターフェイス速度の向上のペースが、CPUのパフォーマンス向上のペースを上回っていたからです。この結果、多くのネットワーキング製品では、システムの回線容量全体のごくわずかな割合のみにまでサポートが縮小されました。

垂直方向の輻輳ポイントでのみトラフィックをモニタリングするというのは、現在のアプリケーションのフローや全体的な規模の傾向とは相反するものです。現在では、水平型（East/West）のトラフィック・パターンが増え、フローも膨大であることから、多くのネットワークの接触点で正確に監視する方が望まれます。

一部のテクノロジー企業が提示している解決策の1つとしては、フロー・テーブルの生成を専用の外部デバイスにオフロードし、このデバイスがネットワーク・タップやミラー・ポートを通じてトラフィックの一部のみを収集するというものがあります。しかしこの方法では、可視化はいっそう損なわれ、コストもかさみます。これは次のような理由からです。

- 複数のデバイスで並列的に処理していたフロー監視を統合して特定のデバイスに一元化した場合、そのデバイスの拡張性が、一元化する前の各デバイス全体の拡張性を上回っていなくてはならない。

- 個別のモジュール型デバイスは、密度とスループットの面で拡張性に限りがある。したがって、インフラの全体的なモニタリング能力は、物理インターフェイスや総体的なパフォーマンスに左右される。こうしたシステムを拡張するには、ハードウェアのアップグレードやリプレースしか方法がない。

- こうしたテクノロジーは、ベンダー独自のアーキテクチャを利用している可能性が非常に高い。したがって、購入、ライセンス、サポートのコストがかさみ、拡張がますます困難になる。

コスト的に現実味のあるスケーラブルなインフラを実現し、広範な可視化を可能にするためには、分散型のオープンなアーキテクチャが鍵になるとアリスタは考えています。同じ原則はモニタリングにも当てはまります。

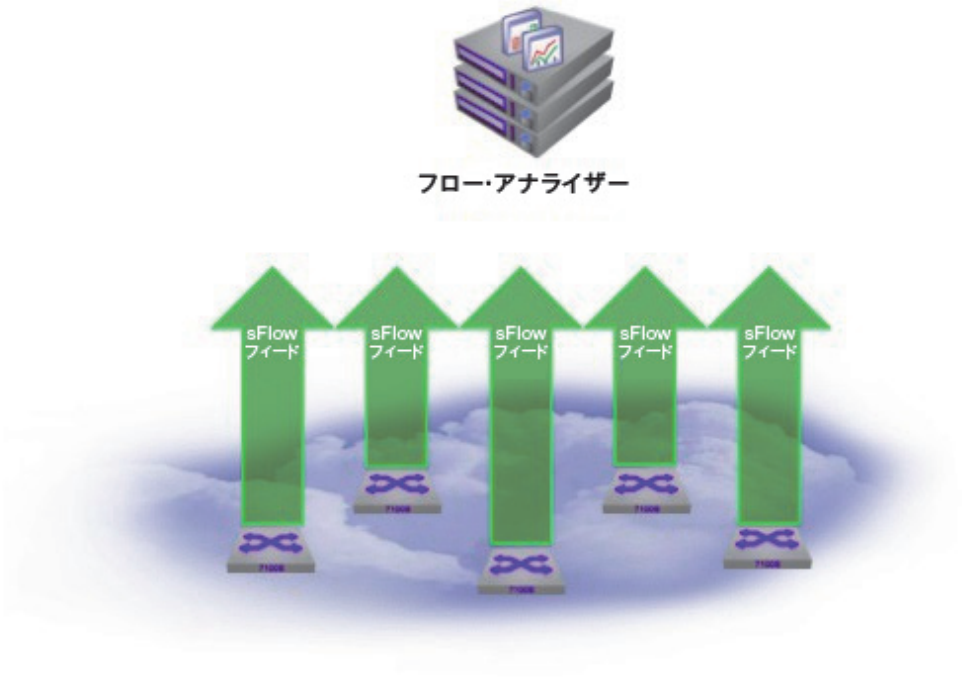

図2: 並列型のモニタリングは拡張性で一元的なデバイスを圧倒

アリスタは、リーフ、スパイン、スプライン、テレメトリーを問わず、ネットワークのすべてのレイヤのすべての製品にsFlow(RFC 3176)を搭載しました。包括的で一貫性のある分散型のフロー情報のストリームを、ネットワーク・インフラ全体に対して単独で提供しています。

sFlow(RFC 3176)の概要

sFlowは、広く利用されているオープン・スタンダードで、ここまで述べてきた拡張性の問題に対処することを目的としています。広く実装されている技術であることから、フローのモニタリング製品でありがちな、デバイスの種類ごとに可視化に壁ができるという状況を回避できます。特に重要なのは、新しいデバイスを導入するごとに、その規模に比例してネットワークをモニタリングできることです。

次のような特徴から、sFlowは現代のネットワーク・デザインには理想的です。

- **演算処理の費用対効果が高い** – sFlowは、ネットワークの中でさまざまな価格帯や規模の幅広い製品にハードウェアで実装できることから、ネットワークのスパイン/コアとリーフ/エッジの間で可視化のギャップが生じることはありません。

- **インターフェイス速度に応じてパフォーマンスが向上** – Flowは、10Gb、40Gb、100Gbイーサネットやそれ以上をサポートしています。

- **内蔵のハードウェアを利用した統計的なサンプリング** – パケットをリアルタイムで処理する必要がないことから、デバイスやモニタリング・ツールにかかるデータの負荷を抑制し、データ整合性を維持できます。これにより、正確で偏りのないテレメトリーを実現できます。

- **自然な分散** – ネットワーク・トポロジに新しいデバイスを追加するごとに、sFlowの処理の規模が拡大します。一元的なボトルネックがなく、水平型と垂直型のどちらのネットワークの可視化にも標準で対応できます。

- **データ収集用のアプリケーションはハードウェアに非依存** – sFlowの分析ツールは、標準的なサーバー上のオープンなオペレーティング・システムで動作します。

- **生データをリアルタイムでエクスポート** – sFlowでは、各デバイスでの事前の相関付けや処理は不要で、フロー・データの要約も行いません。コレクターは、ペイロード・データを含むトラフィックの情報を包括的に収集できます。

- **ローカルでの相関付けが不要** – ローカル・デバイスのCPUのパフォーマンスに関係なく、正確なフロー・データを提供できます。

sFlowは非常に広範囲な活用が可能 – sFlowのデータは、複数のアプリケーションが並行して定期的に使用します。たとえば次のようなアプリケーションです。

- アプリケーションのパフォーマンス管理
- トラブルシューティング
- キャパシティ・プランニング
- 輻輳管理
- 精算、請求、返金
- 異常や攻撃の検出と監査
- 経路の調査

テレメトリー・オーバーレイでのsFlow

アリスタのすべての製品がsFlowをサポートしていることから、データセンター全体で分散してフロー情報を生成できます。しかし、多くのネットワーク・インフラには、レガシー・デバイスや移行期のリンクが多少は残っています。こうしたものに対しては、別途モニタリングを行う方が適切です。

DANZを装備したタップ・アグリゲーター（パケット・ブローカー）を導入すると、ネットワーク・タップや、ポート・ミラーリングのトラフィックから、sFlowのデータグラムを生成できます。

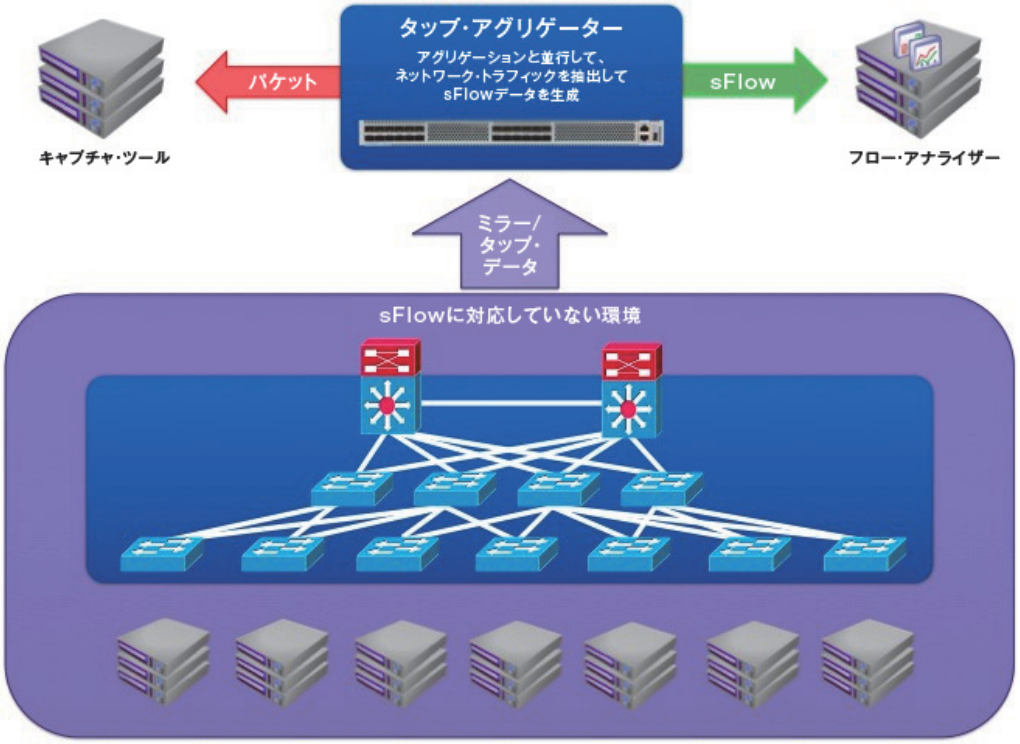

図3:タップ・アグリゲーション・レイヤからのsFlowの生成

すべてのデバイスを一貫した枠組みでモニタリングでき、共通のツールを使用できることは明らかなメリットですが、実はメリットはもう1つあります。多くのデバイスでは従来型のフロー・モニタリングをCPUやデータ・プレーンのハードウェアに実装していることから、この処理の負担がなくなると、ネットワークのパフォーマンスや拡張性も向上するという点です。

軽量で最適な拡張性を備えたsFlowへの対応によって、Arista 7500Eシリーズのモジュール型プラットフォームは、最大1152個の10GbEポート、288個の40GbEポート、96個の100GbEポートを実現し、高帯域幅のリンクや広範囲のリンクをはじめ、多種多様な用途に確実に適合しています。

EOSとsFlowのパワーを活用して情報処理の負担を克服

適切な軽量のテクノロジーを選択することによって、インフラ全体の高度な可視化を実現でき、デバイスや分析ツールに過大な負荷がかかることもない、というのがここまでの話でした。しかし、話はそれで終わりではありません。

フロー分析で検知した異常を、完全なパケット・キャプチャに基づく詳細な調査へとつなげるためには、データ収集のアプリケーションには、インフラまたはテレメトリー・ハードウェアからキャプチャを開始するためのチャネルが必要となります。

Arista EOSは、汎用的なJSON/RPC APIにネイティブに対応しています。したがって、ネットワーク内のモニタリングとパケット・キャプチャのポリシーや、テレメトリー・レイヤ内のタップ・アグリゲーション・ポリシーに関して、どのパートナー・アプリケーションからでも作成や変更を行うことができます。

注目に値する挙動の検出時に、シンプルなJSON/RPCで取得元と通信

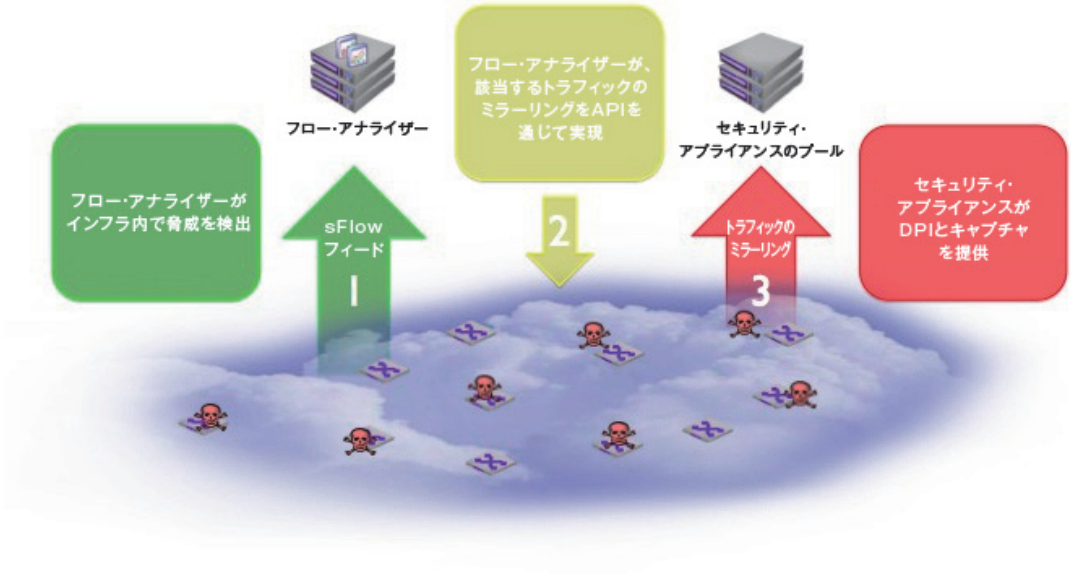

図4：検出と詳細なキャプチャをオープンなAPIで自動化

検出からキャプチャまでのプロセスを自動化することによって、検出、キャプチャ、運用担当者への警告を迅速に行うことのできるシステムを構築し、インフラやツールにかかるコストを最小限に抑えられます。

自律的動作で最大限の拡張性を実現

自動化やクローズド・ループのアーキテクチャをさらに拡張するのは、堅牢でオープンなアリスタのLinux/x86アーキテクチャです。ローカル・インテリジェンスから挙動分析まで、アプリケーションの可能性が広がります。

アリスタの各デバイスは、小規模なサーバーに相当する処理をローカルで行い、標準的なLinux OSのプロセスとメモリ管理を備えています。さらに、EOSでは、データ・プレーンの統計情報とモニタリングにオープンにアクセスできます。各デバイスは、重要なテレメトリー・データをローカルで解析し、分析とキャプチャに関する判断を初めて下すことができます。

ローカル・アプリケーションでsFlowデータをリアルタイムでモニタリングするシンプルなケースを考えてみましょう。広範囲なネットワーク・サンプリングという背景がなくても、ローカルで見られる傾向は、パフォーマンス、容量、セキュリティに関する差し迫った問題を示す重要な早期警報となります。たとえば、過度の接続率、トラフィックの種類、インターフェイスの輻輳、高レイテンシー、パケット損失などは、分析用のキャプチャリングを必要とする事態の徴候である可能性がありますが、それだけではありません。アップストリームのオーケストレーション・ツールが新しいワークロードの配置や負荷分散について判断するうえでの重要な材料にもなり得ます。

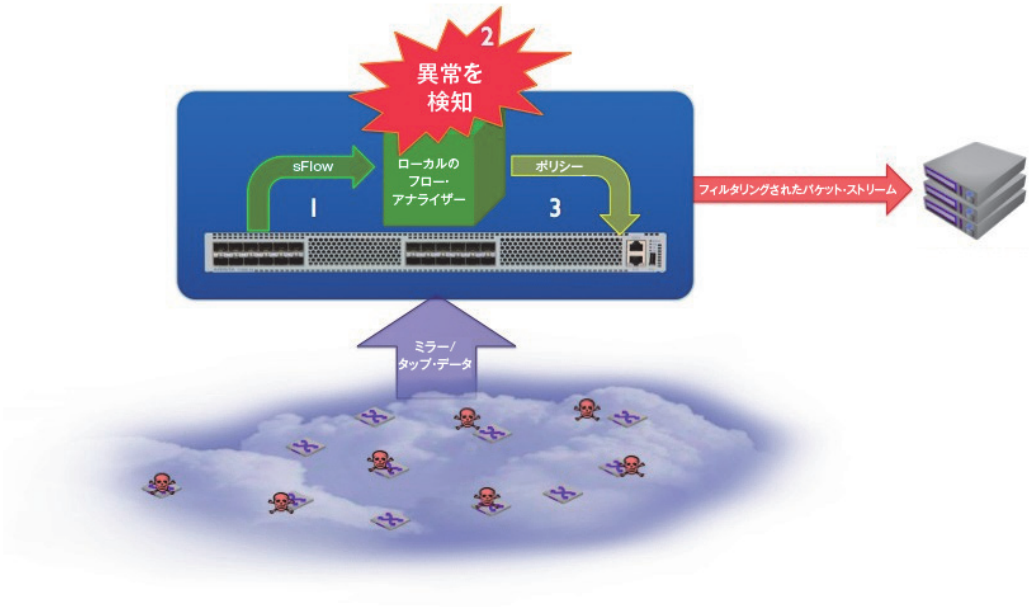

図5:ローカルの自動化によって異常な状況にもインテリジェントな対応が可能

純粋なLinux環境をそのまま利用したEOSと、sFlow、LANZ、データ・プレーンから得られる多種多様なテレメトリー・データによって、インテリジェントなネットワーク制御とキャプチャリングに対する可能性が広がります。これらは、インフラの拡張に比例する形で規模を拡大できます。

まとめ

データセンターの規模とクラウドの経済性でテレメトリーに対応するためには、一元的に管理したメインフレーム的なアプローチによる従来型のモニタリングを見直す必要があります。リニアなスケーラビリティを達成するためには、インテリジェンスを分散し、インフラ全体を一貫性のある形で可視化しなくてはなりません。

これは、データ生成の手段を別のものに置き換えるというだけの問題ではありません。高度な自動化が求められる中で、規模を飛躍的に拡大しながら、運用のオーバーヘッドを抑えるという部分が問題です。

アリスタの製品ラインナップは、シンプルかつオープンなアプローチでこうした要件を満たすことができます。運用担当者は、まず可視性を高めたうえで、自動化したワークフローを構築し、レスポンス・タイムとアプリケーション・インテリジェンスを強化できます。ネットワーク内の機能とテレメトリーとの間の障壁をなくすことによって、スケーラブルなソリューションを最小限のコストで構築できます。

アリスタネットワークスジャパン合同会社

〒170-6045　東京都豊島区東池袋3-3-1　サンシャイン60　45F
Tel:03-5979-2012　　Fax:03-5979-2013
お問い合わせ先
Japan-sales@arista.com

www.arista.com/jp

2014年7月