ESG ラボによる検証

シスコ アプリケーション セントリック インフラストラクチャ（ACI）

デジタル トランスフォーメーションを可能にする、スケーラビリティ、自動化、セキュリティ、およびオープン性を備えたソフトウェア定義型ネットワーキング（SDN）

Tony Palmer および Kerry Dolan（シニア IT 検証アナリスト）著

2017 年 10 月

この ESG Lab レポートはシスコによって委託され、
ESG の許可を得て配布されています。

目次

ESG Lab レポート

ESG Lab レポートの目的は、あらゆる種類や規模の企業向けの IT 製品に関する情報を IT プロフェッショナルに提供することです。ESG Lab レポートは、購入に関する決定を行う前に実施すべき評価プロセスに代わるものではなく、新しいテクノロジーに関する有益な情報を提供するために作成されています。ESG Lab 社の目標は、より価値のある製品の機能のいくつかを調査し、お客様が抱える問題を解決したり、改善が必要な領域を特定したりするにあたって、それらの機能をどのように活用できるかを示すことです。同社のエキスパートが示す第三者の立場からの意見は、同社独自の実践的なテストと、実稼働環境で製品を使用するお客様へのインタビューに基づいています。

はじめに

ESG Lab 社では、シスコのアプリケーション セントリック インフラストラクチャ（Cisco ACI）に対して、パフォーマンス、可用性、セキュリティ、運用性に焦点を当てて徹底的かつ実践的なテストを実施しました。比較のために、ソフトウェアのみで実現するソフトウェア定義型ネットワーキング（SDN）ソリューションに対しても同様のテストが実施されました。

エグゼクティブ サマリー

今日の組織は、移り変わる顧客の要求や、終わりなき競合他社との競争に対処する必要があります。それらに対応するには、俊敏性を大幅に高め、優れたカスタマー エクスペリエンスの提供に重点を置く必要があります。そのためには細かな調整が必要であり、多くの場合、プロセス、文化、テクノロジーの刷新が求められます。これを一般に「デジタル トランスフォーメーション」と呼んでいます。ここで重要になるのが、迅速な展開、最適な実行、高可用性の維持、およびセキュリティがすべてのアプリケーションにおいて確保されていることです。デジタル トランスフォーメーションを実現するには、運用性や自動化を複雑にすることなくソフトウェア定義の利点を発揮できるようなテクノロジーが必要です。シスコでは、デジタル トランスフォーメーションを可能にする技術として ACI を開発しています。

ESG Lab 社による検証結果

Cisco ACI に対して ESG Lab 社が実施した VM～ベア メタル サーバ間のテストでは、遅延が最大 80 %、スループットが最大 600 %、VM～ベア メタル サーバ間の大容量ファイル転送では最大 40 % の改善が確認されました。

全体的に見て、Cisco ACI のパフォーマンスは全テストにおいて一貫しており予測可能であるという結論が得られました。現実的なシナリオ、すなわち仮想化および非仮想化アプリケーションやシステムが混在し、環境全体のトラフィック フローが動的に変化して予測不可能な環境においても、Cisco ACI は一貫して低遅延と優れたスループットを維持し、ミッションクリティカルなアプリケーションで必要とされる予測可能なパフォーマンスを実証しました。

Cisco ACI は、すべてのネットワーク パスに高可用性を提供するアクティブ-アクティブ アーキテクチャを活用し、障害時でも 1 秒未満のコンバージェンスを実現します。ESG Lab 社によると、競合ソリューションでは、この種の可用性は等コスト マルチパス ルーティング（ECMP）の使用時に限られています。ECMP はルーティングにこそ有効ですが、セキュリティや NAT といった、他の重要なネットワーク サービスには可用性を提供できません。つまりアクティブ-アクティブ アーキテクチャによる可用性の確保は、現代のミッション・ビジネスクリティカルなアプリケーションでは最適とは言えないのです。テストした 2 つのソリューションの動作要素を調べると、Cisco ACI の障害発生要因は競合ソリューションと比較して 50 % 少ないことが判明しました。Cisco ACI のフェイルオーバー コンバージェンス時間はゼロないし 1 秒未満であることも、同社によるすべての可用性テストで確認されました。同社は Cisco ACI について、ミッションクリティカルおよびビジネスクリティカルなアプリケーションにとって優れた選択肢であると考えています。

データセンターのセキュリティ侵害の多くは、データセンター内部から発生します。Cisco ACI はホワイトリスト方式のセキュリティ モデルにより、ユビキタスなマイクロセグメンテーション ソリューションを提供します。ネットワーク レベルにセキュリティ ルールやポリシーを適用する作業は複雑です。データセンター内の各ネットワーク要素が、あらゆる種類のネットワーク トラフィックに対するルールやポリシーを一貫して適用しているかを IT 担当者が確認しなければならないからです。今回実施された Cisco ACI の能力テストでは、WAN 経由で接続されたデータセンター全体における複数のハイパーバイザ、ベア メタル エンドポイント、およびコンテナのワークロードに対し、一貫したマイクロセグメンテーションをサポートできるか検証されました。その結果、VMware vCenter のオブジェクトを使用して定義されたポリシーにより、両データセンター間できめ細かいエンドポイント セキュリティを適用できることが確認されました。ソフトウェアのみで実現する SDN ソリューションでも同様にテストしたところ、異なる vCenter サーバが稼働するデータセンター間で同じワークロードに対して同じファイアウォール ポリシーを適用しようとしても、ポリシーは適用されませんでした。

Cisco ACI で提供される Ansible プレイブック（作業手順書）を使用するとマルチ階層アプリケーションの展開が非常に簡単になりますが、ESG Lab 社はその点で特に感心しています。また、ESG Lab 社がテストしたソフトウェアのみで実現する SDN ソリューションと比べ、Cisco ACI の統合オーバーレイ ネットワーク仮想化モデルは、リソース消費を抑えつつ、はるかに高速な自動化を提供しました。Cisco ACI で Ansible を使用してプライベート クラウド環境のプロビジョニングを自動化したところ、ソフトウェアのみで実現する SDN の場合よりも 40 倍以上速い結果が得られました。また、ルーティングおよびゲートウェイ サービスを実行するのに VM を追加する必要がないため、コンピューティングおよびストレージ容量を大幅に削減できることも判明しました。

Cisco ACI テクノロジーは、どのような仮想化やアプリケーションが稼働しているかに関係なく、どの環境においてもシームレスに機能しました。顧客環境の多くでは複数のハイパーバイザが混在していますが、Cisco ACI のテスト環境には Hyper-V、KVM や Kubernetes コンテナなどを簡単に組み込むことができ、たとえ異なるハイパーバイザ上の VM 間であっても、運用面や機能面で同じテスト結果を達成しました。ソフトウェアのみで実現する SDN ソリューションではこのような機能がサポートされていないため、ソリューション比較としての公平性を期すため、それらのテストは行われていません。

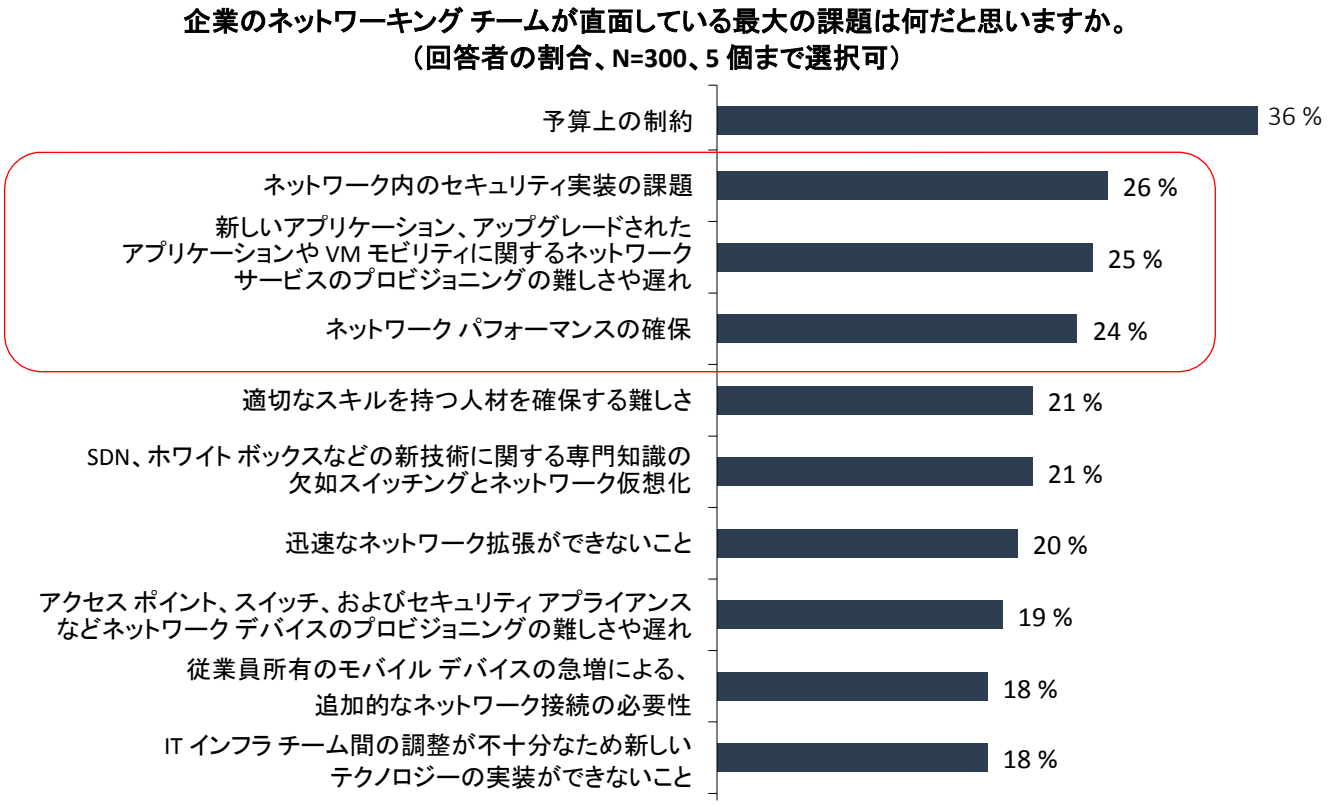
いずれにせよ今回のテストでは、ミッションクリティカルなワークロードに適したシンプルかつスケーラブルで可用性の高いネットワークを Cisco ACI により提供できることが判明しました。ESG Lab 社では、複数のハイブリッド データセンターにわたるネットワークの自動化、俊敏性、セキュリティ、および可用性の改善に関心がある場合に Cisco ACI を検討するよう勧めています。

背景

データセンター コンピューティングには、高性能を維持できる俊敏なネットワークが不可欠です。複数の場所から多様なデバイスで従業員がデータやアプリケーションにアクセスしている現在、ビジネスのあらゆる側面が（そして生活の大部分が）ネットワークの健全性と機能性に依存しています。しかし、こうした理由でネットワークが拡大するにつれ、ネットワークはさらに複雑化しています。そのため管理も難しくなり、パフォーマンスや稼働時間などでユーザの不満が生じます。絶え間ないセキュリティ脅威により、情報の流出、コンプライアンス違反、評判の失墜などの回復不能な損害がもたらされる可能性もあります。ネットワーク セキュリティは IT プロフェッショナルにとって常に最優先課題となっています。

ESG Lab 社の最近の調査は、こうした現実を浮き彫りにしています。同社の調査でネットワークの最大の課題について尋ねたところ、ネットワーク セキュリティの実装、アプリケーションおよびモバイル仮想マシン（VM）のネットワーク サービスのプロビジョニング、およびパフォーマンスなどが主な課題として挙げられましたが、最多の回答は予算上の制約でした（図 1 を参照）。[1]

図 1. ネットワーキングの課題トップ 10



出典：Enterprise Strategy Group、2017 年

[1] 出典：ESG Survey、『*Network Modernization Trends（ネットワークの近代化の動向）*』、2017 年 7 月。

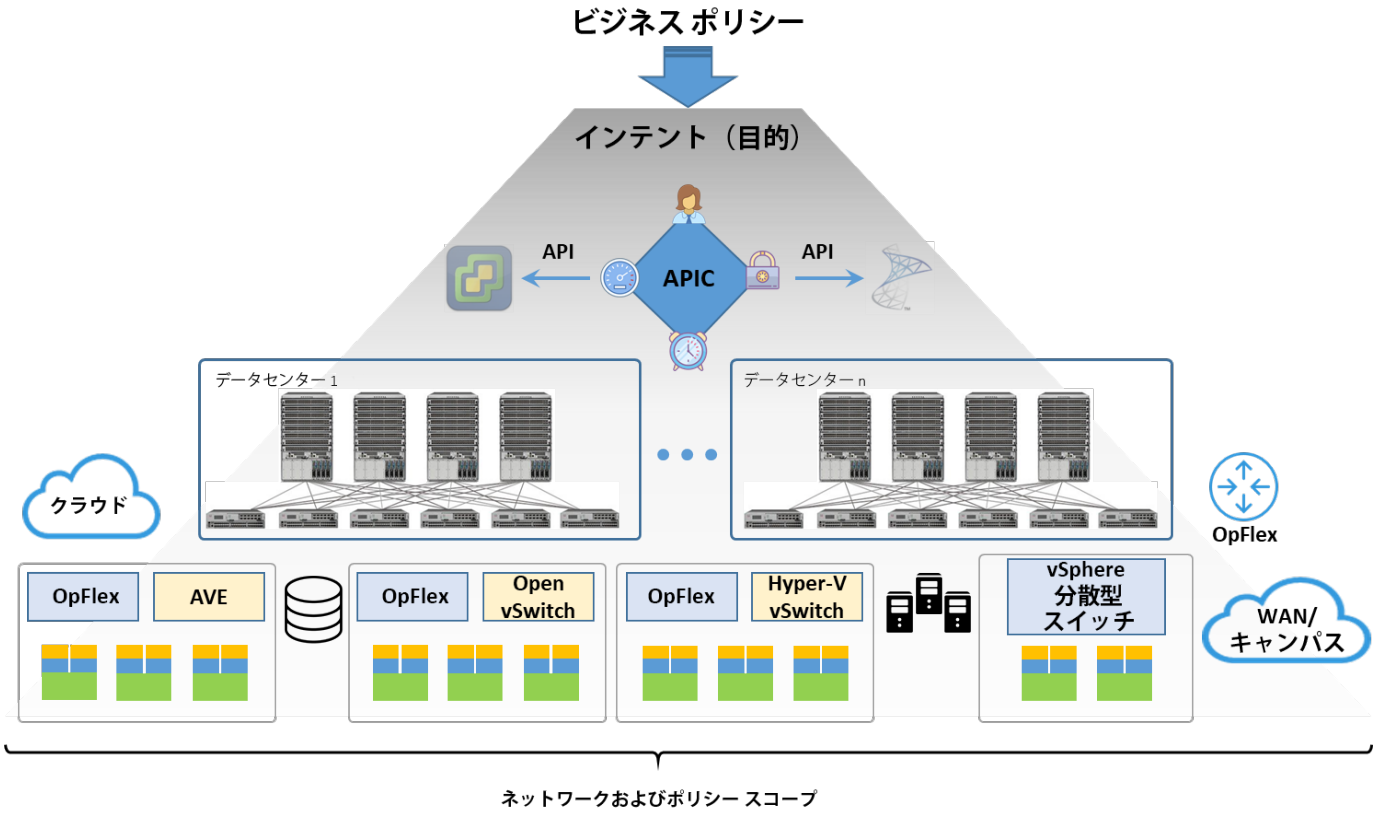
SDN では、基盤となるハードウェアからコントロール プレーンおよびデータ プレーンを抽象化することで、ネットワークの制御や運用を簡素化できます。SDN は、高品質な物理ネットワークの上に動的でプログラマブルな論理ネットワーク コンポーネントを作成することで、設計、管理、トラブルシューティングをより迅速かつ容易に行える、信頼性の高いネットワーク サービスを提供します。

Cisco ACI

Cisco ACI は、アプリケーションを中心としたネットワーク サービスを提供しながら、ネットワークの運用と管理の簡素化を保持し、物理要素と仮想要素が混在した環境を可能にする、ソフトウェア定義型ネットワーキング（SDN）のためのソリューションです。Cisco ACI は最大 400 個のスイッチと 180,000 個のエンドポイントまで拡張できます。Cisco ACI の統合オーバーレイ モデルを活用すれば、一般的なネットワーク タスクを自動化して作業を簡素化できると同時に、アプリケーションベースのポリシー主導ネットワーク サービスへと進化できます。物理、仮想、およびクラウド環境向けの共通プラットフォームを備えており、一元的な可視化と制御により、環境全体のネットワーク サービスの管理およびトラブルシューティングを可能にします。Cisco ACI は、あらゆるワークロードにマイクロセグメンテーションを提供します。仮想化環境において、Cisco ACI のマイクロセグメンテーションは、VM 属性に基づいてハイパーバイザ間およびデータセンター間でシームレスに拡張されます。さらに、ネットワークの導入や拡張のプロセスを簡素化し、セキュリティを向上させます。Cisco ACI アーキテクチャは、ソフトウェアのみで実現する SDN ソリューションに比べて障害となる要因が少なく、障害発生率を低減できる上、一般的なネットワーク障害（リンクまたはネットワーク ノード障害）から迅速に復旧することもできます。トラフィック フローの把握に役立つようハードウェアを可視化できるため、障害をより詳しく把握して修復できるようにもなります。

図 2 からわかるように、Cisco Application Policy Infrastructure Controller（APIC）は、サードパーティ オプションおよびオープン ソース オプションも含めた物理および仮想スイッチング層と統合されます。これによりネットワークとセキュリティ サービスをアプリケーションに合わせて調整し、ビジネス ポリシーとの整合性を確保する、ポリシーモデルの基盤を構築します。

図 2. シスコ アプリケーション セントリック インフラストラクチャ



出典：Enterprise Strategy Group、2017 年

Application Policy Infrastructure Controller（APIC）

Cisco APIC[2] は、スケーリングおよびパフォーマンスのためにアプリケーション ライフサイクルを最適化することを目的として、すべてのファブリック情報およびマネージド仮想スイッチへのアクセスと制御を一元化します。そのため APIC は、物理および仮想リソースにわたる柔軟なネットワークおよびポリシー プロビジョニングをサポートしています。APIC は Cisco ACI ファブリックとコネクテッド仮想スイッチを管理・運用する、最小 3 ノードのコントローラ クラスタで構成されています。APIC クラスタは、複数の仮想マシン管理（VMM）および物理ドメイン間において、エンドポイント ネットワーク状態のシームレスな同期と管理を実現します。Cisco ACI ファブリック ソフトウェアは、OpFlex プロトコルを使用して基礎コンポーネントを管理できるオブジェクトベースのスイッチ OS（オープン REST API を介してプログラム可能）を提供し、アプリケーション認識型ネットワークおよびポリシー自動化を可能にするオープン フレームワークを形成します。

Cisco Nexus 9000 シリーズ スイッチ

Nexus 9000 シリーズ [3] は、1/10/25/40/50/100G イーサネットを備えた多様なフォーム ファクタで、高性能、高密度、低遅延、電力効率を実現するように設計されています。同シリーズのスイッチはシスコのクラウド スケール ASIC テクノロジーを搭載しており、Cisco NX-OS ソフトウェアまたはアプリケーション セントリック インフラストラクチャ（ACI）モードで動作します。これらは、従来型のデータセンター展開や完全自動のデータセンター展開の両方に適しています。

Cisco Application Virtual Switch（AVS）/Application Virtual Edge（AVE）

Cisco AVS および AVS（近日発売予定の次世代 AVS）は、Cisco ACI フレームワークのソフトウェア コンポーネントです。これらは、Cisco ACI の管理およびオーケストレーション プラットフォームと統合されて仮想ネットワークのプロビジョニングを自動化する、専用の分散仮想スイッチで構成されています。AVS/AVE は、さまざまな転送オプションやカプセル化オプション、アプリケーション サービスへのトラフィック ステアリング、ステートフル インスペクションを、数多くの VMware vCenter 仮想化ホストおよびデータセンターにわたって提供できるよう設計されています。Cisco AVS と Cisco AVE は仮想リーフとして Cisco ACI アーキテクチャと統合され、Cisco APIC によって管理されます。Cisco AVS は、コントロール プレーンと APIC の通信に OpFlex プロトコルを実装しています。

シスコは最近、パブリック クラウド環境内で Cisco ACI を利用できるようにすることを発表しました。この新製品は「Cisco ACI Anywhere」という名称であり、次世代の Cisco AVS である Cisco AVE を利用します。Cisco ACI Anywhere の目的は、プライベート クラウドに加え、顧客が選択したパブリック クラウドでアプリケーションを実行できる柔軟性を提供しつつ、マルチクラウド ドメイン全体で一貫したネットワーク ポリシーを維持することです。

OpFlex とサードパーティ製の仮想スイッチング

Cisco ACI では、インテリジェント オブジェクトのスケーラブルな制御に基づいた宣言型制御モデルを使用します。宣言型制御とは、「各オブジェクトには目的の状態に達するように要求され、そのための方法を正確に伝達されなくても、当該状態に達することを約束する」と定めるものです。従来の命令型モデルでは、目的の状態に到達するのに要素をすべて細部まで指定する必要がありましたが、宣言型制御はその必要がありません。Cisco ACI では宣言型制御を利用して、アプリケーション、運用およびインフラの要件を分離し、それぞれを個別に指定できるようにします。OpFlex プロトコルは、宣言型制御を実装するために Cisco ACI によって使用されるメカニズムです。宣言型制御により、抽象ポリシーをレンダリングできる一連のスマート デバイスに、ネットワーク ポリシー コントローラから抽象ポリシーが転送されます。

Cisco ACI は、シスコの AVS および AVE に加え、OpFlex プロトコルを使用して Open vSwitch（OVS）および Microsoft Hyper-V 仮想スイッチと連携します。APIC はまた、VMware VDS などの他のサードパーティ製 vSwitch とのインターフェイスを提供するノースバンド API を使用しています。OpFlex は、Nexus 7000、ASR 1000、および ASR 9000 などの特定のシスコ ルータおよびスイッチとのやり取りにも使用されます。

[2] APIC の詳細については、次の URL を参照してください。
https://www.cisco.com/c/ja_jp/products/cloud-systems-management/application-policy-infrastructure-controller-apic/index.html

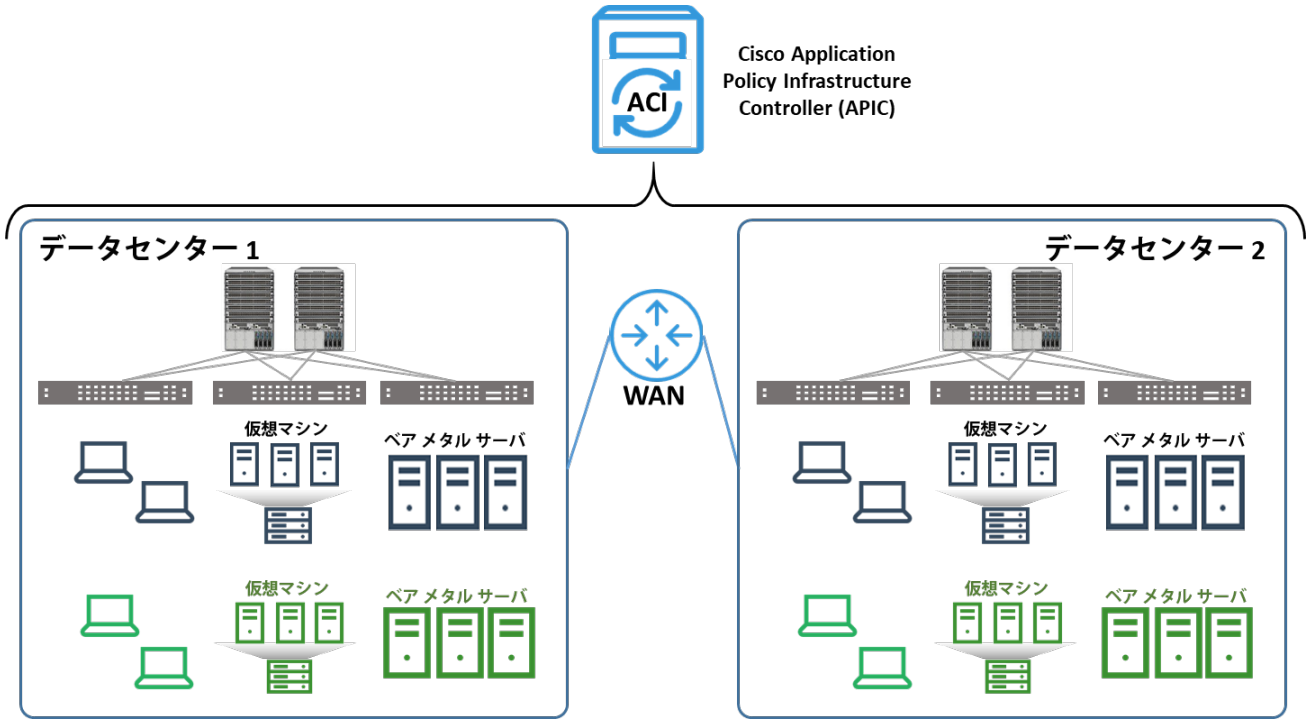
[3] Nexus 9000 シリーズの詳細については、次の URL を参照してください。
https://www.cisco.com/c/ja_jp/products/switches/nexus-9000-series-switches/index.html?stickynav=1

ESG ラボによる検証

ESG Lab 社は Cisco ACI の実践的な評価とテストを行い、結果をソフトウェアのみで実現するの SDN ソリューションと比較しました。テストでは、複数のデータセンターにわたる物理サーバと仮想サーバを備えた最新の分散型エンタープライズ環境において、Cisco ACI が提供するパフォーマンス、可用性、セキュリティ、および自動化を実証します。

テスト ベッドは、実稼働環境と開発環境をサポートする仮想化サーバおよびベア メタル サーバが混在し、複数のデータセンターが稼働する顧客環境を再現しています（図 3 を参照）。顧客環境の多くでは複数のハイパーバイザが混在していますが、Cisco ACI のテスト環境には Hyper-V、KVM や Kubernetes コンテナなどを簡単に組み込むことができ、たとえ異なるハイパーバイザ上の VM 間であっても、運用面や機能面で同じテスト結果を達成しました。ソフトウェアのみで実現する SDN ソリューションではこのような機能がサポートされていないため、ソリューション比較としての公平性を期すため、それらのテストは行われていません。

図 3. 今回のテスト ベッド



出典：Enterprise Strategy Group、2017 年

パフォーマンス

ESG Lab 社では、組織で実際に使用される一般的なユースケースをエミュレートした複数のシナリオ（単一ホスト上のハイパーバイザでホストされている仮想マシン間で実行されるワークロード、異なるホスト上の仮想マシン間で実行されるワークロード、仮想マシンとベア メタル サーバ間で実行されるワークロード）で、Cisco ACI のパフォーマンスをソフトウェアのみで実現するソリューションと比較しました。

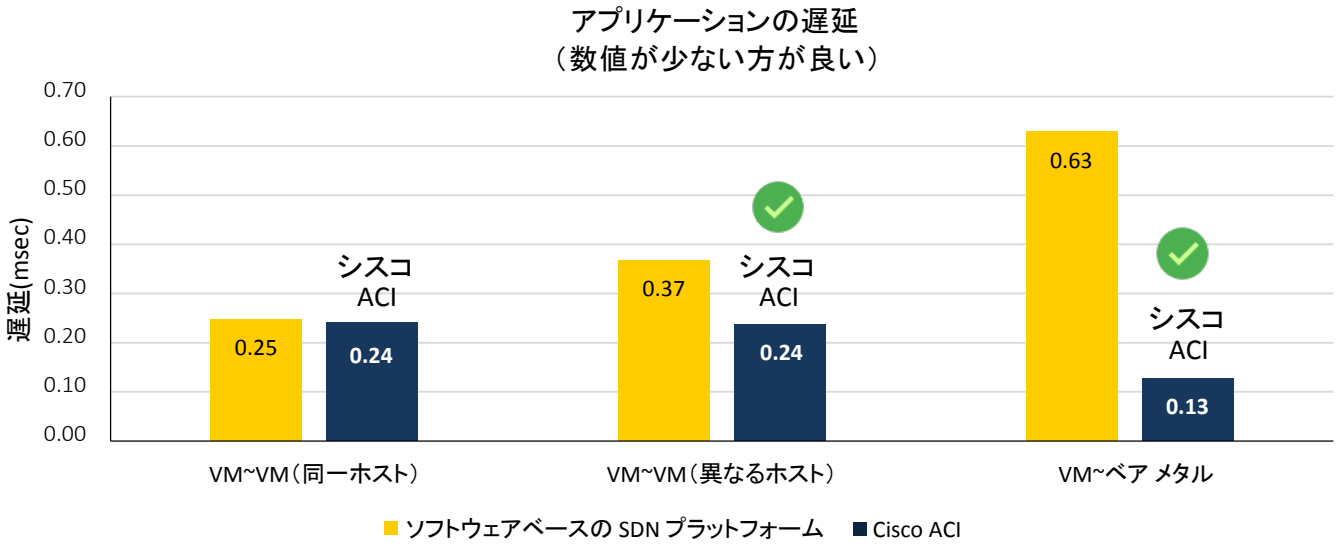
ESG Lab 社によるテスト

パフォーマンス テストはアプリケーションに依存するところが大きいものですが、いくつかの要素に着目すると結果の理解に役立ちます。ネットワーク インフラ、ストレージのスループットと遅延、アプリケーション ソフトウェア、およびハイパーバイザ スケジューラなどはすべて、パフォーマンスに何らかの影響を与える要因です。ESG Lab 社では、ソフトウェアのみで実現する SDN プラットフォームと Cisco ACI のパフォーマンスを比較するにあたり、3 つの単純なメトリックを選択しました。

アプリケーションの遅延は、Linux nmap バージョン 6.40 を用いて測定されました。ネットワーク スループットは、Linux iPerf3 を使用して、最大セグメント サイズ（MSS）を 250、500、および 1,448 バイトとしてテストされました。アプリケーションのスループットは、2 つの異なるプロトコルを使用して、7 GB ファイルのダウンロード（CentOS 上で稼働している Apache から *wget* を使用した HTTP ファイル転送）を行うことによりテストされました。すべてのテストでは、Xeon E5-2650（10 コア CPU）をデュアルで搭載した Cisco C220-M4L サーバを使用しました。VXLAN 対応 NIC を搭載したすべてのホストで、大量受信オフロード（LRO）と TCP セグメンテーション オフロード（TSO）をホスト レベルとゲスト レベルで有効にし、Receive Side Scaling（RSS）を有効にしました。テストに使用したすべての VM は、同一の vCPU、メモリ、およびネットワーク構成を持つ単一のテンプレートから作成されました。仮想化 x86 プラットフォームでのテストでは、繰り返すたびに結果がわずかに異なる可能性があるため、各テストを 10 回実行して平均値をとり、結果の正確性と一貫性を図りました。

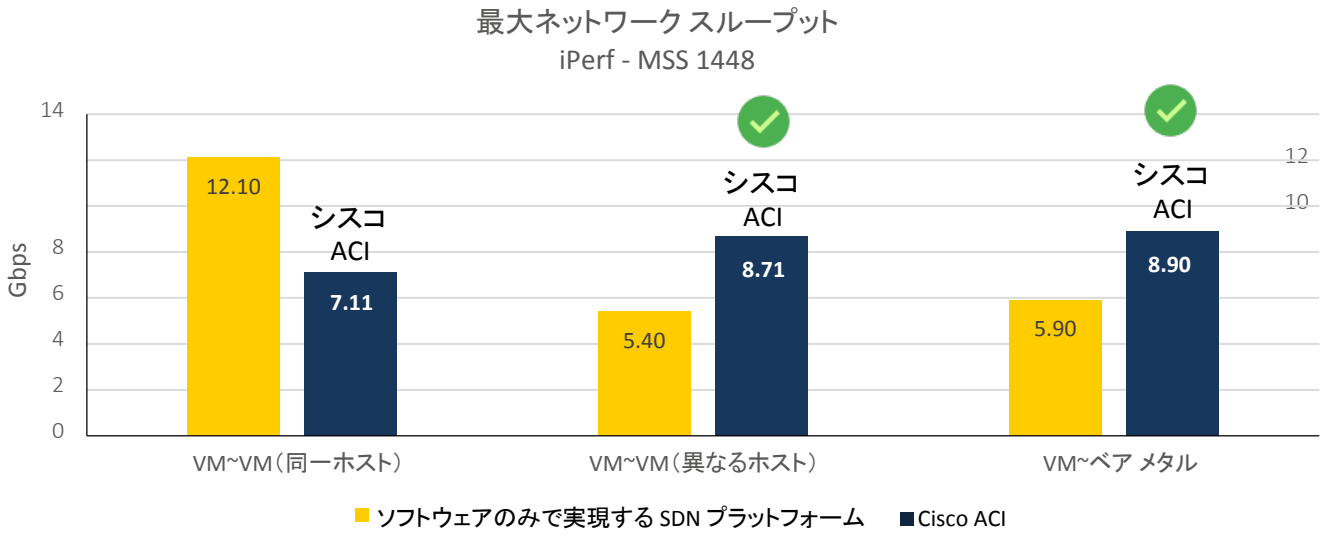
図 4 は、同じハイパーバイザの VM 間、異なるハイパーバイザの VM 間、および VM からベア メタル間での遅延を示しています。いずれの場合でも Cisco ACI が優位性を示し、仮想マシンで実行されるソフトウェアのみで実現する SDN ソリューションよりも遅延が 80 % 低い結果となりました。

図 4. アプリケーションの遅延



次に、iPerf3 を使用してネットワーク スループットのテストを実施しました。このテストでは、両 VM が同一ホスト上にある場合に限りソフトウェアのみで実現する SDN プラットフォームが優れたパフォーマンスを示しましたが、トラフィックが別のホストに流れる場合や、仮想化されていないベア メタル サーバを使用した場合は、Cisco ACI の方が優れた結果を残しました。図 5 に、MSS を 1,448 に設定した場合の結果を示しています。このテストで ACI は、VM からベア メタル サーバへのトラフィックにおいて 61 % のパフォーマンス優位性を示しました。セグメント サイズが小さくなると、より顕著な違いが認められました。MSS を 500 バイトにして同じように VM からベア メタル サーバへのテストを実施したところ、ACI のスループットは、ソフトウェアのみで実現する SDN の 3.8 倍となりました。MSS が 250 バイトの場合、VM からベア メタル サーバへの ACI のスループットは、ソフトウェアのみで実現するソリューションの 6 倍となりました。

図 5. iPerf3 使用時のネットワーク スループット



注目すべきなのは、同じホスト内の VM から VM へのテストでは、VM 間のトラフィックがリーフ スイッチを通過するため、10 Gbps のネットワーク アップリンクが ACI のボトルネックとなったことです。25 Gbps のアップリンクであれば Cisco ACI が同等のスループットを達成できたであろうと考えられます。

最後に、*wget* を使用して HTTP 経由で 7 GB のファイルを転送する場合について調べました。

図 6. wget による 7 GB ファイルの転送

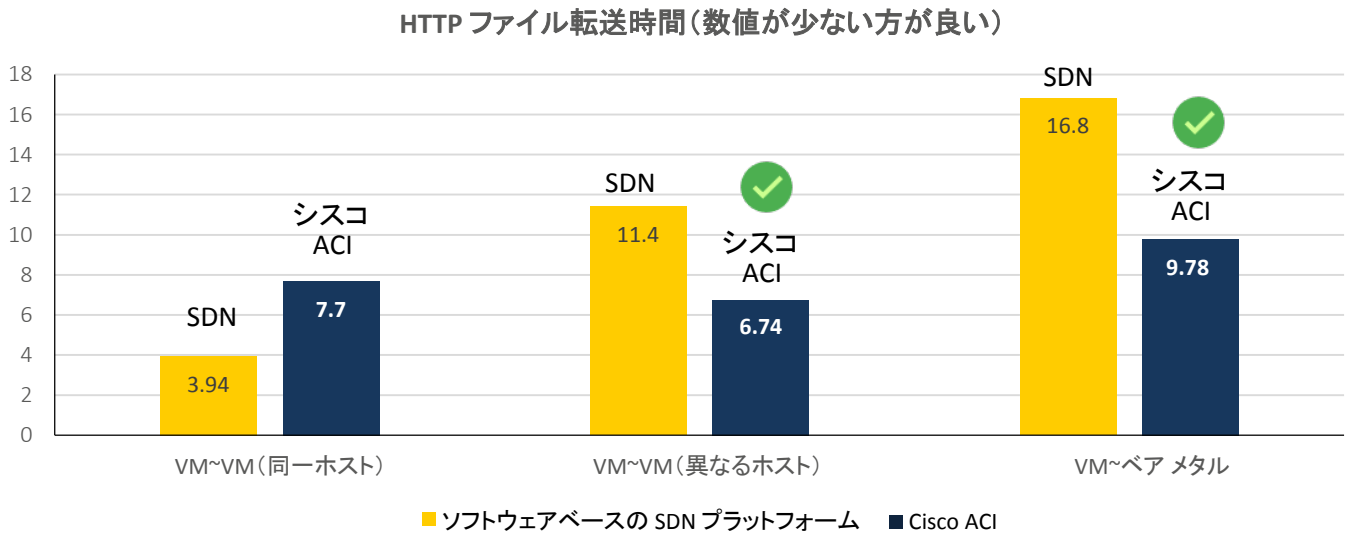


図 6 に示すように、同一ホスト内 VM 間ファイル転送ではソフトウェアのみで実現するソリューションの方が速く、ハイパーバイザ間またはベア メタル サーバへの転送では Cisco ACI のパフォーマンスが上回りました。

Cisco ACI が優れている理由

現代のエンタープライズ コンピューティングには、高パフォーマンスを維持するネットワークが不可欠です。複数の場所から多様なデバイスで従業員がデータやアプリケーションにアクセスしている現在、ビジネスのあらゆる側面がネットワークの健全性と機能性に依存しています。今日直面している最大の課題についてネットワーキング チームに尋ねたところ、約 4 人に 1 人がネットワーク パフォーマンスの提供であると回答しました。企業のビジネス成長に最も大きな影響を及ぼす可能性がある要素として、回答者の 23 % はアプリケーション パフォーマンスの最大化を挙げています。[4]

ESG Lab 社による実践的なテストで、仮想マシンにオーバーレイ ルーティングおよびゲートウェイ機能が提供されている場合には、ソフトウェアのみで実現する SDN よりも Cisco ACI の方が一貫して優れたパフォーマンスを示すことを確認しました。Cisco ACI では、異なる ESXi ホスト上の VM 間のテストで 40 ～ 50 %、VM とベア メタル サーバ間では最大 80 %、遅延が低減しました。

同じホスト内の VM 間ではソフトウェアのみで実現するソリューションの方が高いスループットを示しましたが、実際の用途では、異なるホスト上の VM 間のトラフィック、または VM からベア メタル サーバへのトラフィックがほとんどです。シスコでは、25 GbE NIC を使用することでボトルネックが解消され、同じホスト上での VM 間通信のパフォーマンスが同等になると考えています。異なる ESXi ホスト上の VM 間のワークロードであれば、Cisco ACI は同等のスループットを示し、VM とベア メタル サーバ間では ACI が 33 % 上回る結果となりました。

ファイル転送では、同じハイパーバイザ内の VM 間の場合にはアプリケーションの種類によって結果が左右されましたが、トラフィックがハイパーバイザを移動する場合、またはベア メタル サーバに流れる場合、Cisco ACI では一貫して転送時間が短縮されました。

実環境におけるトラフィック フローはダイナミックで予測不可能であることが多く、仮想化/非仮想化のアプリケーションおよびシステムの両方によって結果が左右されますが、それをシミュレートしたテストにおいて Cisco ACI は、ミッションクリティカルなアプリケーションに適した予測可能なパフォーマンス、そして一貫した低遅延と優れたスループットを示しました。

ネットワークの可用性

昨今の「Always-On」ビジネスにとって、ダウンタイムの代償の大きさを考えると、ディザスタ リカバリ計画とビジネス継続性計画が非常に重要になっていると言えます。今回のテストでは、Cisco ACI アーキテクチャの可用性を調べ、仮想マシンで稼働しているソフトウェアのみで実現する SDN と比較しました。

テストでは ACI のアクティブ-アクティブ特性を調べ、アーキテクチャおよびアプローチの異なる各障害発生要因と比較して予測されるコンバージェンス時間を調べました。Cisco ACI アーキテクチャの調査で明らかになった基本的な障害発生要因は、わずか 6 つです。ESG Lab 社はこれらの障害発生要因をテストし、障害およびリカバリ時の影響について表 1 にまとめました。

[4] **出典**：ESG Survey、『*Network Modernization Trends（ネットワークの近代化の動向）*』、2017 年 7 月。

表 1. Cisco ACI の障害発生要因

障害発生要因	冗長モード	障害時の影響	リカバリ時の影響
APIC ノード障害	スケールアウト クラスタ	なし	なし
APIC クラスタ障害	ホット スタンバイ ノード	管理プレーンへのアクセス不能	なし（構成のバックアップあり）
スパイン ノード障害	ECMP	1 秒未満	なし
リーフ ノード障害	ECMP、vPC	1 秒未満	なし
リーフ/スパイン リンク障害	ECMP、vPC	1 秒未満	なし
サーバ リンク障害	vPC	1 秒未満（サーバ スタックに依存）	サーバ スタックに依存

APIC ノード、さらにはクラスタ全体に障害が発生しても、パフォーマンス、マイクロセグメンテーション、または SDN ルーティングには何の影響もありませんでした。その他の障害でも、影響はすべて 1 秒未満に留まっていました。ソフトウェアのみで実現する SDN プラットフォームのアーキテクチャも検証した結果、オーバーレイ ルータおよびゲートウェイとしての仮想マシンの構成に起因する障害発生要因が増えていることが判明しました。

表 2. ソフトウェアのみで実現する SDN ソリューションにおける障害発生要因

障害発生要因	冗長モード	障害時の影響	リカバリ時の影響
管理 VM	なし（ハイパーバイザ HA に依存）	管理プレーン、ファイアウォール	なし（構成のバックアップあり）
コントローラ VM 障害	スケールアウト クラスタ	なし	なし
コントローラ クラスタ障害	vSphere HA、SRM	管理プレーンへのアクセス不能、ARP 抑制不能	なし（構成のバックアップあり）
オーバーレイ ルータ制御 VM の単一障害	HA（ハートビート）	30 ～ 32 秒のダウンタイム	なし
オーバーレイ ルータ制御 VM の二重障害	なし（vSphere HA）	全面停止	なし
ゲートウェイ アクティブ/スタンバイ モード	ESG HA（ハートビート）	24 秒のダウンタイム	なし
ゲートウェイ アクティブ/アクティブ モード	ECMP	24 秒のダウンタイム	最大で 12 秒
アンダーレイ スパイン ノード障害	ECMP	1 秒未満（アンダーレイに依存）	なし
アンダーレイ リーフ ノード障害	ECMP、vPC	1 秒未満（アンダーレイに依存）	なし
アンダーレイ リーフ/スパイン リンク障害	ECMP、vPC	1 秒未満（アンダーレイに依存）	なし
サーバ リンク障害	vPC	1 秒未満（サーバ スタックに依存）	サーバ スタックに依存

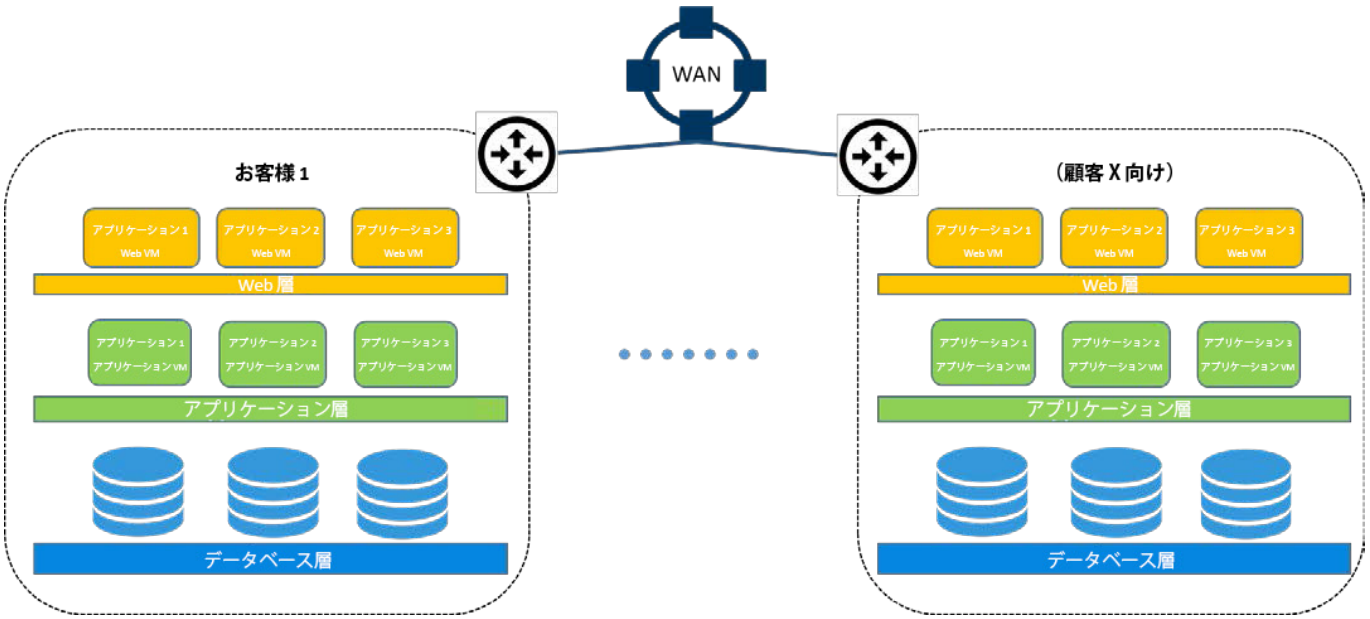
テストでは、24 秒の停止（1 つのゲートウェイ ノードが障害を起こした場合）から SDN オーバーレイ ネットワークの完全停止（複数のオーバーレイ ルータ VM が障害を起こした場合）までの影響が確認されました。テスト結果の詳細を表 2 に示します。Cisco ACI に同等の障害発生要因がないものは、赤字で表示しています。これらのシナリオの一部は定期保守にも関係することに注目してください。ESG Lab 社の結論は、ソフトウェアのみで実現するソリューションと比べて Cisco ACI の障害発生要因は少なく、これらの障害発生要因が環境に与える影響ははるかに小さいというものでした。

ネットワーク自動化

ESG Lab 社では、Cisco ACI の自動化オプションについても調査しました。ネットワーク自動化は、SDN テクノロジーの価値を引き出す上で重要な役割を果たします。自動化により、コストを削減しながら、ネットワークベースのサービスを迅速に提供できるためです。ネットワーク自動化は、物理インフラストラクチャからネットワーク サービスの構成情報を抽象化します。これにより、自動化ソフトウェア オーケストレーション ツールを使用してサービスをセットアップできます。

Cisco ACI は、Cisco UCS-D、Cisco Cloud Center、VMware vRealize Automation/Orchestrator、Microsoft Windows Azure Pack、OpenStack Neutron（複数のディストリビューション）、Ansible、Python SDK、および ACI ツールキットなど、さまざまな自動化/オーケストレーション ツールをサポートしています。ESG Lab 社では、Ansible[5] を使用して、任意の数のアプリケーションまたはテナントに対応する Cisco ACI とソフトウェアのみで実現する SDN の両環境で、インターネット/WAN アクセスを持つ 3 層トポロジの作成を自動化しました（図 7 を参照）。この構成では、各顧客がルーティング可能な独自のサブネットを取得します。また、顧客が互いに隔離されていること、Web 層サブネットが WAN デバイスに自動的に通知されること、ベア メタル サブネットへの接続が自動であること、およびネットワーク制御とデータ プレーンが冗長構成であることが必須となります。

図 7. インターネットおよび WAN アクセスを持つ 3 層トポロジの作成



出典：Enterprise Strategy Group、2017 年

このシナリオをソフトウェアのみで実現する SDN で実装するには、複数の課題があります。たとえば、自動化できない分野もいくつか存在します。また、テナント ゲートウェイから OSPF に静的ルートを設定する作業は複雑であり、DevOps エンジニアが実施するにはルーティングを十分理解するという 1 段階余分な手順も必要となります。ソフトウェアのみで実現する SDN に 10 個のトポロジを導入する作業には、約 60 分の時間がかかりました。さらに、VM ベースのルータとゲートウェイには、40 個の vCPU、30 GB の RAM、および 60 GB のストレージが必要でした。Cisco ACI の導入の場合、ルーティングの専門知識は不要です。すべてのアクティビティが自動化され、コード行は 20 % 少なくて済み、トポロジの導入はわずか 1 分半で完了しました。Cisco ACI の導入では新しいリソースも必要ありませんでした。

[5] Cisco ACI Ansible モジュールについては、http://docs.ansible.com/ansible/devel/list_of_network_modules.html#aci [英語] で確認できます。

Cisco ACI が優れている理由

リソースやワークフォースが高度に分散化されている今日、ネットワークの可用性は、ビジネスクリティカルでありミッションクリティカルでもあります。ネットワークに障害が発生すると、すべてに影響が波及します。しかし、こうした理由でネットワークが拡大するにつれ、ネットワークはさらに複雑化しています。そのため管理も難しくなり、パフォーマンスや稼働時間などでユーザの不満が生じます。これは顧客離れにもつながります。

SDN の当初の目的は、基盤となるハードウェアからコントロールおよびデータ プレーンを抽象化することで、ネットワーク制御および運用を簡素化することです。SDN は、高品質な物理ネットワークをベースにして動的でプログラマブルな論理ネットワーク コンポーネントを作成することで、設計、管理、トラブルシューティングを容易に行える、信頼性の高いネットワーク サービスを提供できます。

しかし、SDN ソリューションはすべて同じではありません。音声、ビデオ、または金融サービスのような 1 秒未満のコンバージェンスを必要とするミッションクリティカルなアプリケーションのサポートという点では、ルーティング機能およびゲートウェイ機能を VM で実行するソフトウェアのみで実現する SDN ソリューションでは問題があると言えます。

また、Cisco ACI がミッションクリティカルおよびビジネスクリティカルなアプリケーションに適した高可用性のアクティブ-アクティブ SDN を提供できることも確認されました。Cisco ACI のアーキテクチャには障害発生要因が少なく、ESG でテストしたすべてのネットワーク障害イベントにおいて、トラフィックへの影響はゼロまたは 1 秒未満でした。ソフトウェアのみで実現する SDN の場合、アーキテクチャがアクティブ-パッシブ方式であるため、複雑さと障害発生要因の数が増加して、単一の障害イベントで最大 32 秒のダウンタイムが発生しました。

Ansible を使用して Cisco ACI でプライベート クラウド環境のプロビジョニングを自動化したところ、ソフトウェアのみで実現する SDN の場合よりも 40 倍以上速いことが確認されました。また、ルーティングおよびゲートウェイ サービスを実行するのに VM を追加する必要がないため、コンピューティングおよびストレージ容量を大幅に削減できることも判明しました。

セキュリティ

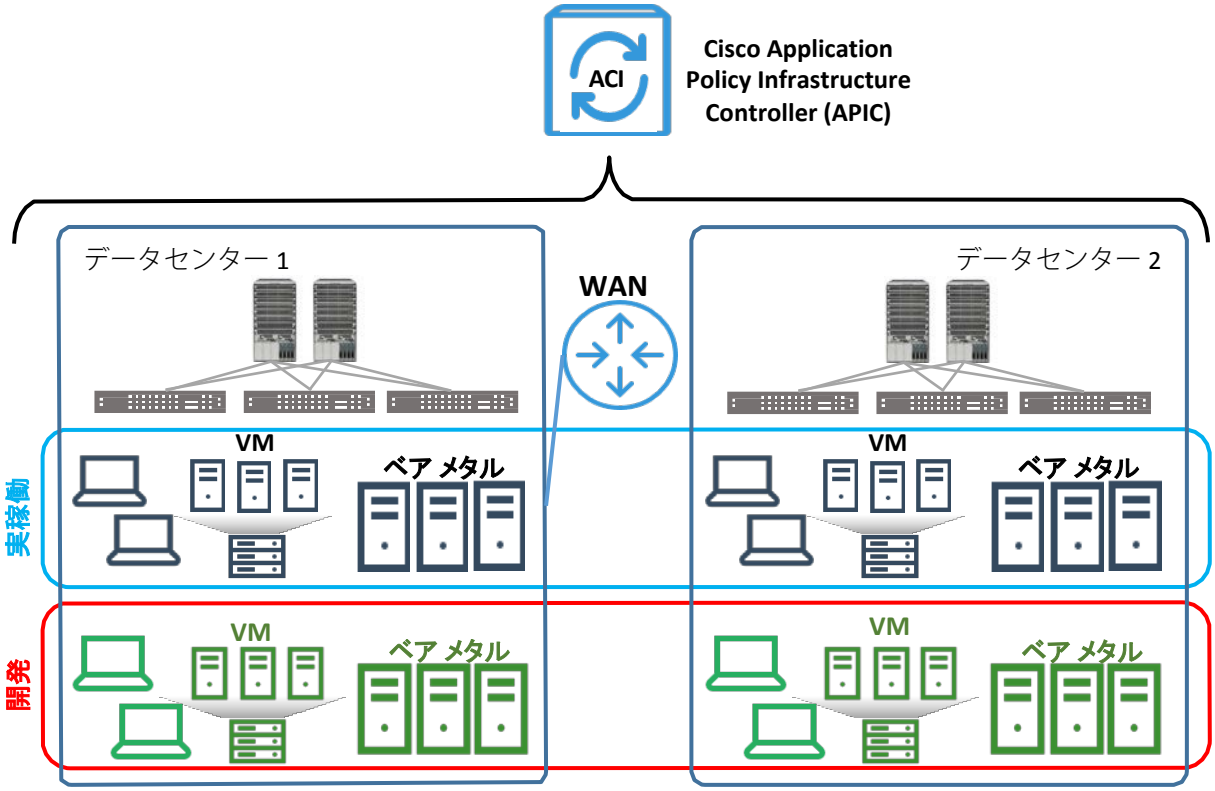
Cisco ACI は、複数のハイパーバイザ、ベア メタル エンドポイント、およびコンテナに対して、一貫したマイクロセグメンテーション サポートを提供するように設計されているため、エンドポイント セキュリティをきめ細かく適用できます。マイクロセグメンテーションは、ファイアウォールなどのネットワーク要素に依存せずワークロード レベルでセキュリティ ポリシーを適用できるので、エンドツーエンドのネットワーク セキュリティをネットワーク トラフィック レベルのみで提供できます。Cisco ACI は、セキュリティ ポリシーを定義するために、ワークロードの種類ごとに特化したコントラクトを作成します。コントラクトは、ワークロードがアクセスできるデータおよびエンドポイントを指定します。この指定は、データセンター内のワークロードの位置に依存しません。データセンター内またはデータセンター間でワークロードを移動しても、Cisco ACI はそのコントラクトを維持します。Cisco ACI コントラクトではレイヤ 4 までのセキュリティ ルールが定義されます。また、QoS などのパラメータも定義できます。

ESG Lab 社によるテスト

テストでは最初に、2 つのデータセンターに置かれた、異なる vCenter 下にあるワークロードについて、Cisco ACI がどのようにして一貫したセキュリティ ルールを適用するのか調査しました。データセンターは IP ルーティング WAN によって相互に接続しています。図 8 はテスト トポロジを示しています。1 つのデータセンター内にそれぞれ独立した WordPress 実稼働サイトおよび開発サイトを設け、2 つのクライアントを設定しました。次に、Cisco ACI によりマイクロセグメンテーションを両データセンターにまたがって実装し、以下のファイアウォール ルールを適用しました。

- WAN 内の実稼働クライアントが両データセンターの WordPress 実稼働サイトと通信できるようにする一方で、開発サイトとの通信は防止する。
- WAN 内の開発クライアントが両データセンターの開発サイトと通信できるようにする一方で、実稼働サイトとの通信は防止する。

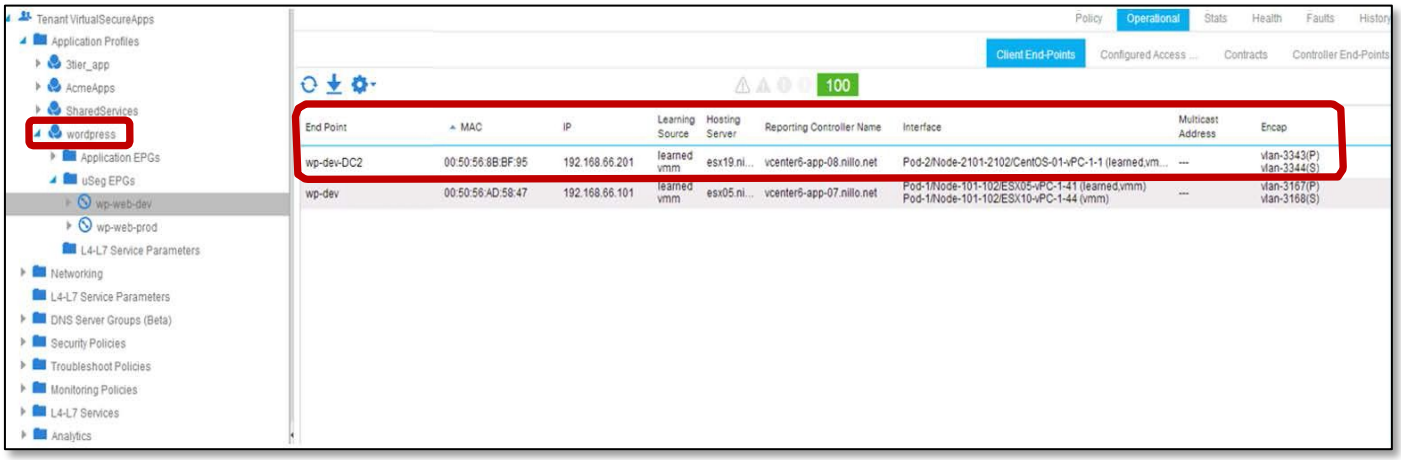
図 8. ラボ トポロジー：データセンター間でのマイクロセグメンテーション



出典：Enterprise Strategy Group、2017 年

VM は、vCenter オブジェクト（具体的には vSphere タグの組み合わせ）を使用して、正しいセキュリティ ポリシーに分類されました。これは非常に重要な点です。その後、各クライアントがサイトと通信する際に、個々のコントラクトに定義されたファイアウォール ルールが守られていたことが確認されました。さらに重要なのは、たとえ VM が vMotion を使用して異なる vCenter に移動された場合であっても、Cisco ACI が両データセンターの実稼働サイトおよび開発サイトのどちらにも同じファイアウォール ルールを適用していたことです。テストでは、両データセンターにわたるマイクロセグメンテーションにある個々の VM の詳細も確認されました。ワークロードの詳細には、IP アドレス、MAC アドレス、およびサーバ ホストが含まれています。図 9 は、両データセンターの開発 VM の詳細を示しています。VM の詳細に加えてコントラクトの詳細も表示されていますが、Cisco ACI が正しいポリシーを適用していることを確認できます。

図 9. ACI GUI における個々のワークロードの詳細



出典：Enterprise Strategy Group、2017 年

テストでは同様のトポロジを使用して、ソフトウェアのみで実現する SDN ソリューションでも同じ内容を調査しました。ソフトウェアのみで実現する SDN ソリューションでは、Cisco ACI とは異なり、VM が別の vCenter に移動したときに、2 つのデータセンターにまたがってファイアウォール ポリシーを維持することはできませんでした。データセンター間で一貫したルールを適用しようとしても、ポリシーが機能しないことが判明しました。

Cisco ACI が優れている理由

最近の ESG Lab 社による調査で、企業のビジネス拡大に最も大きな影響を与え得るネットワーク機能を挙げてもらったところ、ネットワーク セキュリティの確保と回答した回答者が圧倒的多数の 46 % を占めました。[6]

アプリケーション仮想化が進むにつれ、データセンターのネットワーク セキュリティを適用する作業は、ますます複雑化しています。特に、データセンター内およびデータセンター間で VM を異なるホストに移動できるようになったことで、その傾向がいっそう高まっています。ネットワーク レベルにセキュリティ ルールやポリシーを適用する作業は複雑です。データセンター内の各ネットワーク要素が、あらゆる種類のネットワーク トラフィックに対するルールやポリシーを一貫して適用しているかを IT 担当者が確認しなければならないからです。ポリシーの適用に一貫性がないと、データの損失、ネットワークの脆弱性、および計画外の停止を招き、そのすべてがブランドの失墜や収益の損失につながる可能性があります。

ESG Lab 社による Cisco ACI の能力テストでは、WAN 経由で接続されたデータセンター全体における複数のハイパーバイザ、ベア メタル エンドポイント、およびコンテナのワークロードに対し、一貫したマイクロセグメンテーションをサポートできるか検証しました。実稼働ワークロードと開発ワークロードにコントラクトを適用したことにより、2 つのデータセンター全体できめ細かいエンドポイント セキュリティが適用され、どちらのワークロードについても、コントラクトで定義されたサイトとのみ通信できることが確認されました。ソフトウェアのみで実現する SDN ソリューションで同じテストを実施したところ、データセンター間で同じワークロードに同じファイアウォール ポリシーを適用しようとしてもポリシーが機能しないことが判明しました。

[6] 出典：ESG Survey、『*Network Modernization Trends（ネットワークの近代化の動向）*』、2017 年 7 月。

顧客インタビュー

ESG Lab 社では、NTT America 社の製品エンジニアリング/オペレーションズ部門の責任者 Indranil Sengupta 氏に、同社のクラウド データセンターにおける Cisco ACI の使用についてインタビューしました。NTT America 社は、世界的な Fortune 500 企業である NTT コミュニケーションズ社の子会社として、北米、南米、中米に事業を展開しています。同社の製品エンジニアリング/オペレーションズ部門は、複雑な要件を持つグローバル顧客に管理型インフラ サービスを提供しています。

同社はテスト開発ニーズおよび実稼動ニーズの両方に対し、インフラ プラットフォームと継続的な管理を提供しています。競争の激しい業界で成功するためには、一貫性、セキュリティ、拡張性を合わせ持つサービスを提供しながら、常に効率向上に取り組む必要があります。NTT America 社では Cisco ACI の SDN を活用することで、ネットワーク サービスの導入と継続的な管理を自動化しています。これにより管理の労力やコストを削減しながら、顧客のニーズの変化や拡大に合わせて迅速かつ容易にサービスを調整できています。

マネージド サービス プラットフォームのコスト効率を維持するにはマルチテナントが不可欠ですが、同社の顧客要件は複雑であるため、各テナントのインフラストラクチャが異なっています。一般的なハイパースケールの Web サービスは、すべてのサービスを本質的に同じとみなす類型的なアプローチでマルチテナントをサポートします。ただしこれでは、同社の顧客の複雑な要件には対応できません。Cisco ACI を活用すれば、マルチテナントの効率性を活かしながら、各顧客に合わせたネットワークを提供できます。Cisco ACI がなければ、同社のエンジニアは各テナント環境を個別に作成する必要がありますが、顧客は混乱し、同社にとってもコスト増を招くでしょう。

同社が Cisco ACI を活用することで、コストを削減しながらサービス提供をより簡単に拡張できています。Cisco ACI はまた、サービス提供の迅速化も可能にしました。Sengupta 氏は、「当社は金融顧客向けのソリューションを導入しましたが、それは複雑で、コンプライアンスやセキュリティ面で厳しい制限も伴っていました。しかし Cisco ACI を活用することで、予想の半分の時間で導入することができ、お客様に喜んでいただけました」と述べています。

NTT America 社では、より多くの顧客へ Cisco ACI を導入し、それによる効率性と柔軟性の向上を提供し続ける予定です。Sengupta 氏はまた、「非常に競争の激しい業界なので、四半期単位で努力やコストを削減するために漸進的な改善が必要です。Cisco ACI を活用することで、より優れた多くのサービスを値上げせずに顧客に提供できています」とも述べています。

結論

IT 部門にとって、今日のビジネスのスピードや規模と歩調を合わせるには多大な労力が必要です。要件の異なる多数のアプリケーションを処理し、無数のエンドポイントが存在する複数拠点に対応するため IT 管理者が限界まで働くことも多くあります。さらに IT のコンシューマ化により、ユーザの期待が高まるだけでなく、ユーザの立場も強くなっています。このような状況において、洗練された SDN ソリューションは「あると良い」を通り越し、ビジネスの成功と収益性に不可欠なものとなっています。ただし、一貫性のある高パフォーマンスを発揮できなければ、運用の簡素化や自動化などは無意味です。シームレスで優れたカスタマー エクスペリエンスを実現するには、スループットおよび遅延の影響を受けやすいビデオ、音声、金融サービスなどのミッションクリティカルなアプリケーションをサポートする、現代のアプリケーションに適した高可用性「Always-On」エコシステムが必要です。SDN ソリューションは、必要なセキュリティ モデルを実現できるよう、複数のデータセンター間のアプリケーションを水平方向にも垂直方向にもバインドし、保護できる必要があります。

ハイブリッド クラウドの動向を受け入れ、オンプレミスおよびマルチクラウド ドメイン全体までアプリケーションの実行を拡大しようとする組織が増えています。このため、インフラ重視の管理からアプリケーション中心の管理に移行し、コンテナやマイクロサービスなどのパブリック クラウド サービスとテクノロジーといった最新の IT システムを活用する必要があります。インフラ管理はもはや重要ではないというわけではありませんが、ハイブリッド クラウドの焦点が、基盤となるインフラの抽象化を通じたアプリケーションのサポートにあることは明かです。IT 変革をサポートする新しいテクノロジーを活用する上で、ハイブリッド クラウドは中心的な技術となります。ハイブリッド クラウド戦略を成功させるには、これらのダイナミック アプリケーションをサポートする堅固な SDN 戦略が不可欠となるのです。

Cisco ACI は、そのようなソリューションを提供し、効率性、シンプルさ、セキュリティ、高パフォーマンス、および高可用性を実現するための、アプリケーション重視のネットワーキング サービスを提供するエコシステムを構築します。これには物理、仮想、そしてクラウドの各要素が含まれており、組織環境の成長に合わせて容易に拡張できます。Cisco ACI は、コントローラ クラスタおよび Nexus 9000 シリーズ スイッチが提供するソフトウェア定義型ネットワーキングを利用して、複数のハイパーバイザおよびデータセンターにわたるネットワーク ファブリックを検出・管理し、そのオープン フレームワークによって、ネットワーク管理およびオーケストレーション ベンダーによるソリューションとの統合を容易にします。

仮想化/非仮想化両方のアプリケーションやシステムが含まれる実環境では、トラフィック フローの多くが動的で予測不可能ですが、Cisco ACI はそうした環境にもうまく適合して一貫した高パフォーマンスを提供できることが確認されました。今回のテストで、Cisco ACI は、ミッションクリティカルなアプリケーションに適した予測可能なパフォーマンスを提供し、一貫して低遅延と良好なスループットを維持しました。また、Cisco ACI がミッションクリティカルおよびビジネスクリティカルなアプリケーションに適した高可用性 SDN を提供できることも確認されました。テストしたすべてのネットワーク障害イベントにおいて、トラフィックへの影響（フェールオーバー コンバージェンス時間）はゼロないし 1 秒未満でした。

Cisco ACI で Ansible を使用してプライベート クラウド環境のプロビジョニングを自動化したところ、ソフトウェアのみで実現する SDN の場合よりも 40 倍以上速い結果が得られました。また、ルーティングおよびゲートウェイ サービスを実行するのに VM を追加する必要がないため、コンピューティングおよびストレージ容量を大幅に削減できることも判明しました。さらに、Cisco ACI ではマイクロセグメンテーション ポリシーとセキュリティ ポリシーをデータセンター内およびデータセンター間で一貫して適用できることも確認されました。

高度に仮想化されたデータセンター、パブリック クラウド、プライベート クラウドのビジネス ニーズに対応できるネットワークを、仮想化インフラと物理インフラを組み合わせて構築することは、ますます困難になっています。いずれにせよ今回のテストでは、ミッションクリティカルなワークロードに適したシンプルかつスケーラブルで可用性の高いネットワークを Cisco ACI により提供できることが判明しました。ESG Lab 社では、複数のハイブリッド データセンターにわたるネットワークの自動化、俊敏性、セキュリティ、および可用性の改善に関心がある場合に Cisco ACI を検討するよう勧めています。

Enterprise Strategy Group は、IT アナリスト、調査、検証、および戦略会社であり、
市場のインテリジェンスや実用的な考察をグローバル IT コミュニティに提供しています。

www.esg-global.com contact@esg-global.com P. 508.482.0188