ホワイト ペーパー

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）の原理

概要

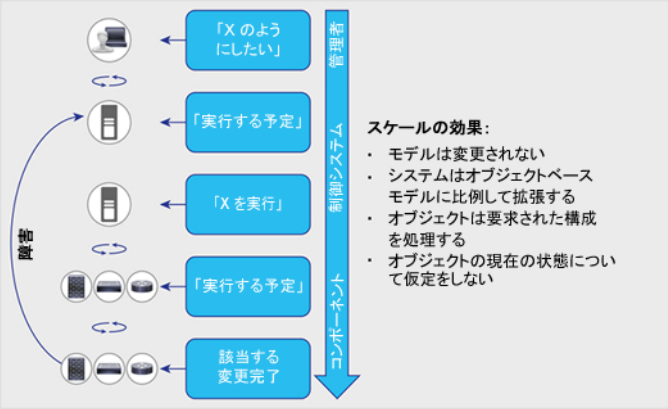
アプリケーション セントリック インフラストラクチャ（ACI）の画期的な特長のひとつとして、アプリケーション コンポーネントの接続性を表現するために高度に抽象化されたインターフェイスの導入が挙げられます。この接続性は高度に抽象化されたポリシーで制御されています。このモデルは、アプリケーション開発者が簡単に使用できると同時に、オートメーションとセキュリティが向上するように設計されています。

ACI ポリシー理論

ACI ポリシー モデルは、約束理論（Promise Theory）に基づいたオブジェクト指向モデルです。約束理論は、インテリジェント オブジェクトのスケーラブルな管理に基づいており、トップダウンの管理システムのような従来の命令型モデルとは異なります。この従来のシステムでは、セントラル マネージャが基盤オブジェクトの構成コマンドと、これらのオブジェクトの現在の状態の、両方を把握する必要があります。

これに対して約束理論では、制御システム自体が引き起こした構成のステート変更を「必要なステート変更」として、基盤オブジェクトに実行させます。オブジェクトは例外またはエラーを管理システムに送信する役割も担っています。このアプローチによって、制御システムの負荷と複雑性が軽減され、拡張性が向上します。このシステムをさらに拡張して、基盤のオブジェクトのメソッドによって、オブジェクト相互に、また下位レベルのオブジェクトからステート変更を要求できます（図 1）。

図 1.　　大規模システム制御に対する約束理論アプローチ



この理論的モデルでは、ACI は、アプリケーションを重視してアプリケーション導入のためのオブジェクト モデルを構築します。これまでアプリケーションは、ネットワークの許容範囲と、ポリシー実装構造の誤用を防ぐための要件によって、制限を受けていました。アドレッシング、VLAN、セキュリティなどの概念が互いに組み合わされ、アプリケーションの拡張性とモビリティが限定されていました。アプリケーションをモビリティや Web スケールのために再設計するとき、この従来型アプローチでは一貫性のある導入を迅速に行うことは困難です。

ACI ポリシー モデルでは、基盤のネットワーク構造については何も規定していません。ただし、約束理論で規定されるように、各種デバイスとの接続を管理するために iLeaf と呼ばれるエッジ要素が必要となります。

オブジェクト モデル

最上位レベルでは、ACI オブジェクト モデルは 1 つ以上のテナントのグループ上に構築され、ネットワーク インフラストラクチャ管理とデータ フローを分離することができます。組織の必要性に応じて、顧客、事業部門、またはグループにテナントを使用できます。たとえば、企業の場合は 1 つのテナントを組織全体に使用し、クラウド プロバイダーの場合は複数の顧客がそれぞれ 1 つ以上のテナントを各自の組織に使用することができます。

テナントはさらにコンテキストに分割できます。コンテキストは、仮想ルーティングおよび転送（VRF）インスタンス、つまり個別の IP 空間に直接関連付けられます。各テナントは、そのテナントのビジネス ニーズに応じて、1 つ以上のコンテキストを指定することができます。コンテキストを使用して、該当するテナントの組織的要件および転送要件をさらに細分化できます。コンテキストでは個別の転送インスタンスを使用するため、IP アドレッシングがマルチテナントの別のコンテキストで重複することがあります。

オブジェクト モデルは、コンテキスト内でアプリケーションを定義する一連のオブジェクトを提供します。これらのオブジェクトとは、エンドポイント（EP）とエンドポイント グループ（EPG）、およびその関係を定義するポリシーのことです（図 2）。この場合のポリシーは、単なるアクセス コントロール リスト（ACL）のセットではなく、インバウンドおよびアウトバウンド フィルタ、トラフィック品質設定、マーキング ルール、リダイレクション ルールの集合を含むことに注意してください。

図 2. 論理オブジェクト モデル

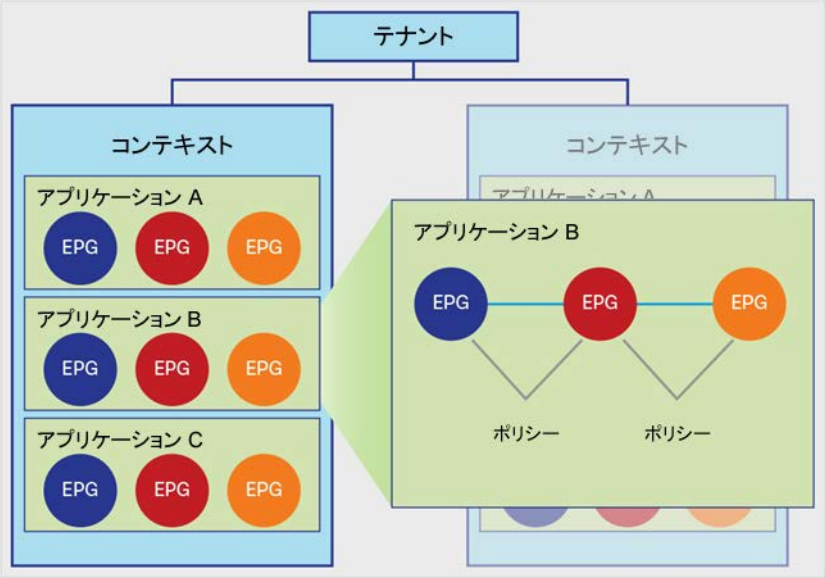


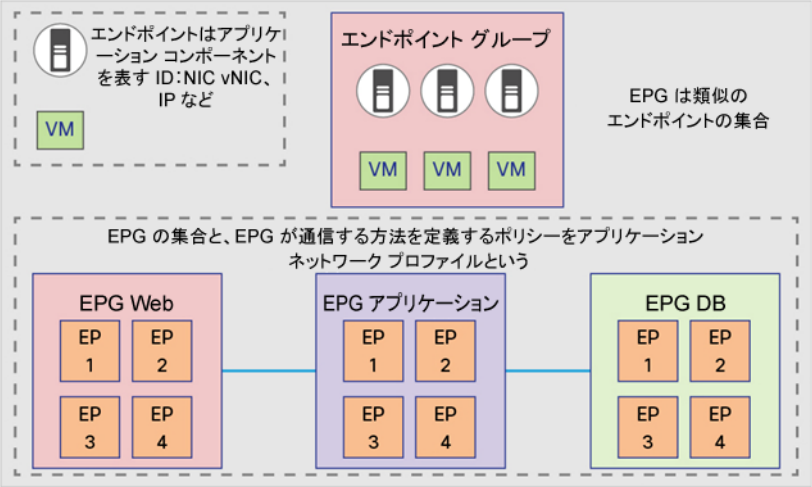
図 2 に、2 つのコンテキストを持つテナントと、そのコンテキストで構成されるアプリケーションを示します。図示された EPG はエンドポイントのグループで、アプリケーション層またはその他の論理的なアプリケーション グループを構成します。たとえば、図の右側の拡大表示したアプリケーション B は、Web 層（青）、アプリケーション層（赤）、データベース層（オレンジ）で構成されます。EPG とその相互作用を定義するポリシーの組み合わせが、ACI モデルのアプリケーション ネットワーク プロファイルとなります。

エンドポイント グループ

EPG は、アプリケーション層または一連のサービスを表す、類似するエンドポイントの集合です。類似のポリシーを必要とするオブジェクトを、論理的にグループ化したものです。たとえば、アプリケーションの Web 層を構成するコンポーネントのグループを EPG にすることができます。エンドポイントは、ネットワーク インターフェイス カード（NIC）、仮想 NIC（vNIC）、IP アドレス、またはドメイン ネーム システム（DNS）名を使用して定義され、将来的にアプリケーション コンポーネントを識別するメソッドをサポートするよう拡張できます。

EPG は、外部ネットワーク、ネットワーク サービス、セキュリティ デバイス、ネットワーク ストレージなどのエンティティの表現にも使用されます。EPG は類似した機能を提供する 1 つ以上のエンドポイントの集合です。論理的にグループ化されたもので、使用されているアプリケーション導入モデルに応じて、さまざまな使用オプションがあります（図 3）。

図 3. エンドポイント グループの関係



EPG は柔軟性を主な特徴として設計されているため、ユーザが選ぶ 1 つまたは複数の導入モデルに合わせてカスタマイズした使い方ができます。EPG を使用してポリシーが適用される要素を定義することもできます。ネットワーク ファブリック内で、ポリシーが EPG 間に適用され、EPG が互いに通信する方法が定義されます。このアプローチは、EPG 内のポリシー適用に今後拡張できるように設計されています。

ここで EPG の使用例を挙げます。

- 従来のネットワーク VLAN で定義された EPG：すべてのエンドポイントが EPG に配置された所定の VLAN に接続されている
- Virtual Extensible LAN（VXLAN）で定義された EPG：VXLAN を使用する以外は、VLAN と同じ
- VMware ポート グループにマッピングされた EPG
- IP またはサブネットで定義された EPG：172.168.10.10 または 172.168.10 など
- DNS 名または DNS 範囲で定義された EPG：example.foo.com または *.web.foo.com など

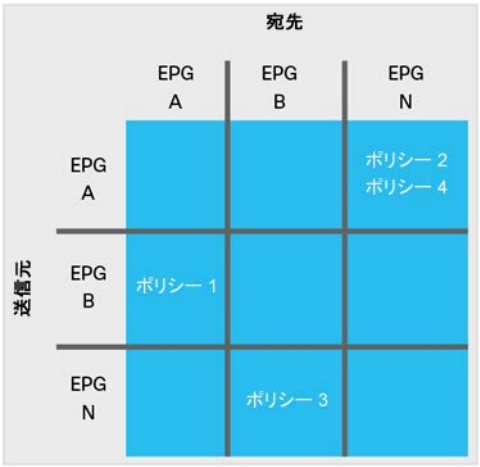
EPG は柔軟に使用でき、拡張性もあります。このモデルの目的は、実環境の導入モデルに対応するアプリケーション ネットワーク モデルを構築するためのツールを提供することです。エンドポイントの定義も拡張でき、今後の製品拡張や業界要件に対応させることができます。

EPG モデルには、管理面で多数のメリットがあります。一貫したポリシーを高レベルのオートメーションとオーケストレーション ツールに適用できる単独のオブジェクトを作成することができます。ポリシーを変更するために、個々のエンドポイントでツールを操作する必要はありません。また、ネットワーク内の配置場所にかかわらず、同じグループ内のエンドポイント全体で一貫性を維持できます。

ポリシーの実施

EPG とポリシーとの関係は、ソース EPG（sEPG）を表す 1 つの軸と、宛先 EPG（dEPG）を表すもう 1 つの軸を持つマトリクスとして考えられます。該当する sEPG と dEPG が交差する場所に 1 つ以上のポリシーが配置されます。ほとんどの場合、マトリクスは空白の部分が多くなります。これは多くの EPG は互いに通信する必要がないためです（図 4）。

図 4. ポリシー実施のマトリクス



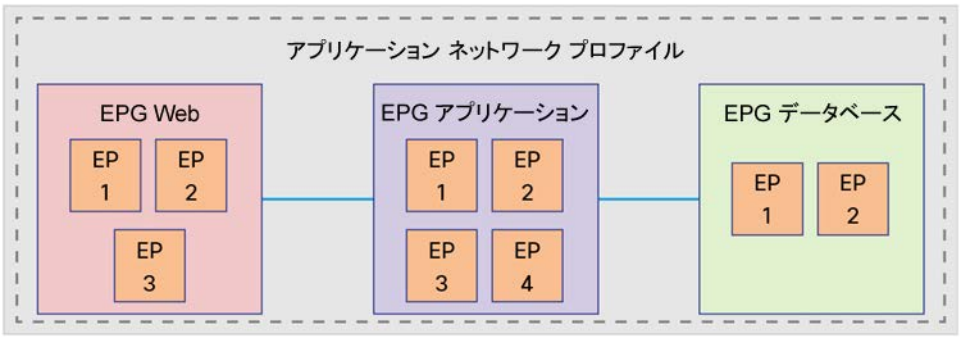
ポリシーは、サービス品質（QoS）、アクセス コントロール、サービス導入などのフィルタごとに分割されます。フィルタは、2 つの EPG の間のポリシーに関する固有のルールです。フィルタには、インバウンド ルールとアウトバウンド ルールとして、許可、拒否、リダイレクト、ログ、コピー、マークがあります。

アプリケーション ネットワーク プロファイル

アプリケーション ネットワーク プロファイルは、EPG とその接続、およびこれらの接続を定義するポリシーの集合です。ネットワーク ファブリック内のアプリケーションと、その相互依存関係を論理的に説明します。

アプリケーションの設計と導入の方法に合う論理的手法でモデル化するように設計されています。ポリシーと接続性の構成および施行は、管理者が手作業で行うのではなく、システムが行います。図 5 は、アクセス プロファイルの例です。

図 5. アプリケーション ネットワーク プロファイル



次は、アプリケーション ネットワーク プロファイルの作成に必要となる一般的な手順です。

1. EPG を作成します（前述のとおり）。
2. 以下のルールで接続性を定義するポリシーを作成します。
   - 許可
   - 拒否
   - ログ

- マーク
- リダイレクト
- コピー

3. コントラクトと呼ばれるポリシー構造を使用して、EPG 間の接続ポイントを作成します。

コントラクト

コントラクトは、インバウンドおよびアウトバウンドの許可、拒否、および QoS のルール、およびリダイレクトなどのポリシーを定義します。コントラクトによって、環境の要件に応じて、EPG が他の EPG と通信する方法をシンプルにも複雑にも定義できます。コントラクトは EPG 間で適用されますが、プロバイダー/コンシューマの関係を使用して EPG に接続されます。基本的に、1 つの EPG がコントラクトを提供し、その他の EPG はそのコントラクトを使用します。

プロバイダー/コンシューマのモデルは、さまざまな目的で役立ちます。アプリケーション層に自然な方法で「シールド」または「膜」を付加して、層がアプリケーションのその他の要素と連携する方法を規定できます。たとえば、Web サーバは通常 HTTP や HTTPS を提供できます。こうしたサービスのみを許可するコントラクトで Web サーバを覆うことができます。また、コントラクトのプロバイダー/コンシューマ モデルでは、コントラクトにある複数の接続ではなく、1 つのポリシー オブジェクトだけにポリシーの更新を適用すればよいことから、シンプルで一貫した処理が可能になり、セキュリティが強化されます。コントラクトを利用することにより、ポリシーを 1 度定義すれば何回も再利用できるため、管理が一層シンプルになります（図 6）。

図 6. コントラクト

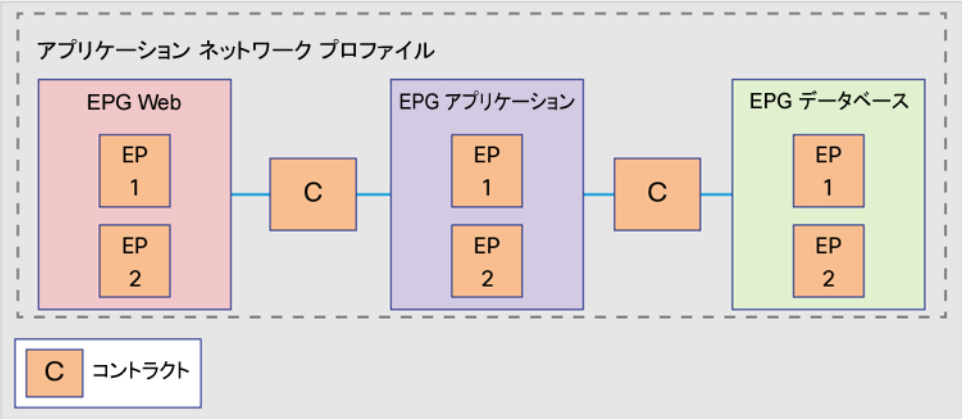
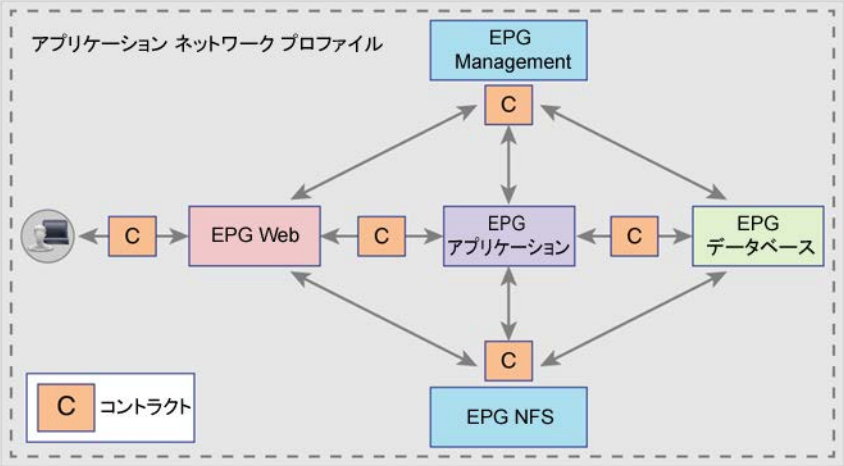


図 7 は、EPG 接続性によって定義された Web アプリケーションの 3 つの層と、その通信を定義するコントラクトとの関係を示しています。こうした要素の集まりが、アプリケーション ネットワーク プロファイルを構成します。コントラクトによって、通常は複数の EPG と通信するサービスの再利用性とポリシーの整合性も実現できます。

図 7. アプリケーション ネットワーク プロファイルの全体図



まとめ

本文書では、ACI の内容、ポリシー モデルの使用方法など、ACI ポリシー モデルの紹介説明に限られています。このモデルには、ここでは取り上げられていない、その他の構造やオブジェクトが多数あります。

詳細情報

http://www.cisco.com/jp/go/aci を参照してください。