次世代マルチクラウドネットワーキング

F5 Distributed Cloud のマルチクラウドネットワーキングソリューションは、パブリッククラウドやプライベートクラウドのための革新的なネットワーキングとセキュリティのサービスを提供します。また、NetOps や DevOps チームが取り組んでいる複数サービスの管理という複雑な作業を簡素化し、エンドツーエンドのポリシーと可観測性を提供します。

主な利点

より高速な導入
どのクラウドプロバイダでも同じ API、ネットワーキングおよびセキュリティ機能が提供される統合サービスを使用することで、クラウドへの移行や新しいクラウドプロバイダの採用を高速化します。

生産性の向上
自動化された Infrastructure as Code、SaaS 運用、ライフサイクル管理、および DevOps のセルフサービス運用と NetOps/SecOps の組織制御を強化するインテントドリブンなポリシーにより、クラウドネットワーキングから摩擦を取り除きます。

インフラストラクチャ運用の合理化
仮想プライベートクラウド（VPC）にクラウドネイティブの F5 Distributed Cloud Mesh ノードを導入し、オプションの F5 Global Network を使用することで、複雑なネットワーク運用に悩まされることなく、安全なマルチクラウドネットワークを提供します。

機能性の強化
NetOps チームは、サービス VPC に Distributed Cloud Mesh を導入してネットワーキングとセキュリティを設定し、DevOps チームは、DNS、ロードバランシング、API ゲートウェイを設定できます。

オプションのマネージドサービス
F5 のマネージドサービスエンジニアリングチームが、NetOps および DevOps チームを支援し、クラウド、複数のクラウド、またはハイブリッドクラウド内で最適かつセキュアなネットワークを設計、実装、テストできるようにします。

組織は、クラウドによるシンプルさと自動化の効率性を求め、**パブリッククラウドへの移行を加速させています。**一部の企業は、パブリッククラウド採用の初期段階にあり、単純なアプリケーションの移行から始めています。しかし、これより多くの企業は、クラウドへの移行をさらに進め、ミッションクリティカルなアプリをクラウドに移行しています。重要なアプリの移行には、企業の IT 要件が無数にあることから、独自の課題が伴います。

さらに、より高度な段階にある組織では、合併や買収によって複数になったパブリッククラウド環境の管理や、さまざまな機能を利用するために特定のクラウドを使用したいという事業部門への対応が強いられています。Gartner 社が 2020 年に実施した世界的調査では、81% の組織が、すでに 2 社以上のクラウドプロバイダを利用していると答えています。

これらのどの状況でも、インフラストラクチャおよび運用チームは、パブリッククラウドのネットワーキングとセキュリティに関して、非常に複雑な運用課題に直面しています。

インフラストラクチャおよび運用チームには、組織の規模により異なりますが、ネットワーク運用（NetOps）、セキュリティ運用（SecOps）、開発運用（DevOps）といった、複数のペルソナが含まれる可能性があります。

NetOps は通常、サイト管理者であり、ネットワーキング関連の運用を監督します。SecOps は、組織全体のインフラストラクチャとアプリケーションのセキュリティ運用を管理します。DevOps は、アプリケーション関連のネットワーキングとセキュリティ運用を扱います。インフラストラクチャおよび運用チームが大規模であれば、この 3 つのペルソナがすべて揃っているかもしれませんし、小規模であれば、個人がこれらすべての役割を担当しているかもしれません。

NetOps チームは、以下のような弱点があると感じています。

- **仮想エディションのアプライアンスがクラウドネイティブではない：**多くの企業は、リフトアンドシフト方式を採用して、オンプレミスのネットワーキングおよびセキュリティアプライアンスの仮想エディション（VE）をクラウドで使用しています。しかし、仮想エディションのバージョンがクラウドネイティブではなく、クラウド導入に期待される自動化やコスト効率は得られないことにすぐ気づきます。
- **クラウドネットワーキングのスキルギャップ：**次に、パブリッククラウドプロバイダの製品を直接採用しますが、クラウドネットワーキング技術におけるスキルギャップの問題に直面します。インフラストラクチャおよび運用チームは、オンプレミスでは、ネットワーキングとセキュリティを完全に制御しながらアプライアンスを管理できます。しかし、パブリッククラウドでは、スキルギャップがあるため、トランジットゲートウェイ、VNet ピアリング、アベイラビリティゾーンなど、クラウドプロバイダの構造への対応が必要になります。クラウドプロバイダのネットワーキングとセキュリティの構造は、NetOps チームがオンプレミスで慣れ親しんでいるものとはかなり異なることが多いため、クラウドプロバイダの構造の自動化とオーケストレーションが必要です。

主な特徴

アプリと API を中心とした接続
ネットワークを公開することなく、アプリや API をクラウド上で配信できます。

L3-L7 ネットワーキングおよびセキュリティスタックの統合
L3-L7 ネットワーキングとセキュリティを統合し、クラウドポリシーを統一できます。

ライフサイクル管理のための SaaS ベースのコントロールプレーンおよび運用
SaaS ベースのコントローラと分析サービスにより、エンドツーエンドのライフサイクル管理を実現します。

グローバルなパフォーマンスと大容量のクロスクラウドバックボーン
グローバルバックボーンにより、クラウド全体で決定論的なパフォーマンスを提供します。

豊富な可観測性と分析
一元的な可観測性により、クラウド、サイト、レイヤー全体でデータとアウトプットを効率的に監視できます。

拡張可能な外部セキュリティサービス挿入
F5 BIG-IP およびサードパーティ製ファイアウォールのオプションのサービス挿入により、ソリューションを拡張できます。

クラウドネットワーキングの運用は、クラウドのスキルギャップ、クラウド構造間の違い、複数のポイント製品によりまとまらない運用、および可視化の分断を原因として、インフラストラクチャおよび運用チームにとって扱いが複雑なものになっています。

- **高度なネットワーキングおよびセキュリティ制御の欠如：**一方で、取り組みをさらに進め、ミッションクリティカルなアプリをクラウドに移行しようとしている企業は、別の問題に直面しています。クラウドには、企業がオンプレミスで使い慣れているのと同レベルの高度なネットワーキングとセキュリティ制御がありません。たとえば、きめ細かい VPC 間トラフィックのセグメンテーションポリシーの実現は困難です。

- **複数のポイント製品を利用することでポリシーや設定がまとまらず複雑化する運用：**高度なネットワークとセキュリティを実現するために、NetOps は、ネットワーキング / ルーティングやファイアウォールのための複数のポイント製品を利用して、パブリッククラウド製品を強化しています。しかし、これらのポイント製品のアプライアンスは、ポリシーや設定の運用モデルが異なるため、より複雑になり、ポリシーが一貫していません。

SecOps の課題は以下のとおりです。

- **外部のセキュリティサービスとの複雑な統合：**SecOps は、パブリッククラウド上でも、オンプレミスで使っているのと同じセキュリティ製品（ネットワークファイアウォールやアプリケーションファイアウォールなど）を使いたいと考えています。しかし、パブリッククラウドのネットワーキングに関する専門知識が不足しているため、パブリッククラウド上での製品の導入と運用に苦労しています。具体的には以下のことに苦労しています。
  - パブリッククラウドのトラフィックフローにセキュリティサービスを挿入する
  - きめ細かいポリシーにより、トラフィックをセキュリティサービスに誘導して検査する

以下は、DevOps チームが抱える問題です。

- **サイロ化した運用モデル：**アプリケーションのアーキテクチャ自体がモノリシックからマイクロサービスに変化しています。DevOps チームは、バックエンドのロードバランサ、API ゲートウェイおよびサービスメッシュ技術によるクラスタ運用を必要としています。
- **早めの準備で後に備える：**DevOps は、チームごと、マイクロサービスごと、アプリごとにクラスタを運用する必要があり、多くのロードバランサとクラスタを管理しなければならなくなります。複数のイテレーションにまたがることで、マイクロサービスへの移行による利点であるサービスの高速化が生かされないため、DevOps は、NetOps によりクラスタがプロビジョニングおよび接続されるまで待つことができません。
- **別々のセルフサービスが必要：**NetOps と DevOps に必要なことは、NetOps チームが組織全体のポリシー（たとえば、「dev」環境のアプリは「prod」環境のアプリと通信できないなど）の設定のみを担当し、DevOps チームにはアプリ固有のポリシーを独自に設定する能力を提供するセルフサービス機能が提供されることです。

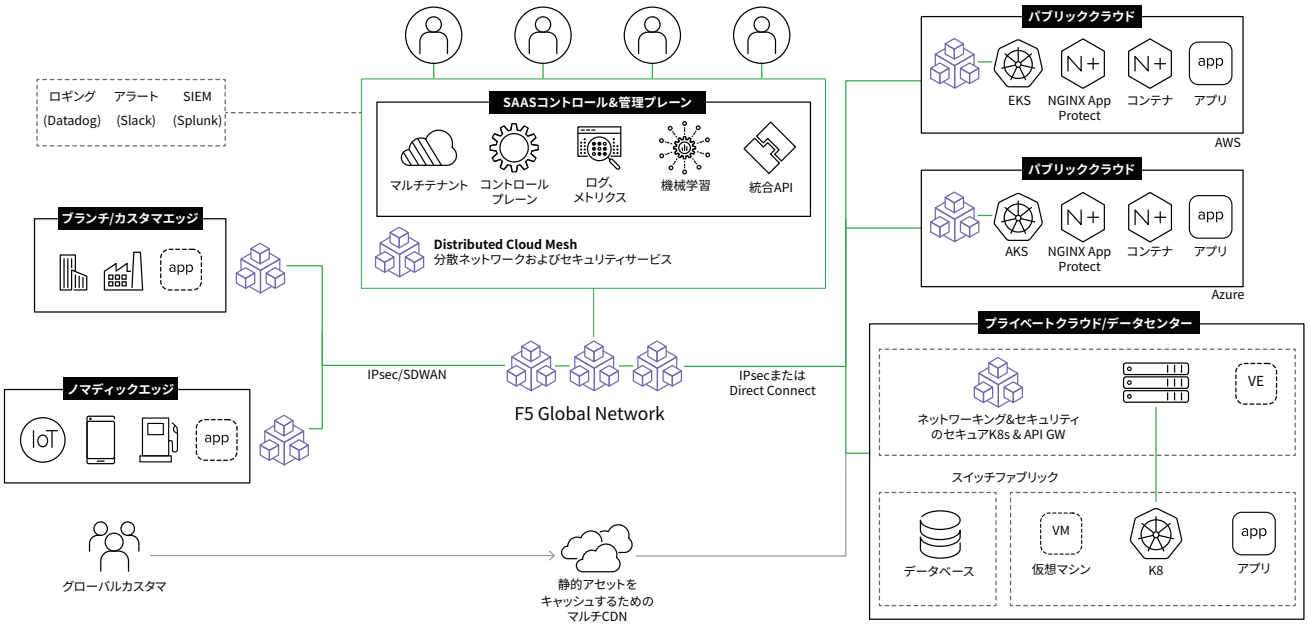
F5 Distributed Cloud Services：クラウド全体でのシームレスでセキュアなアプリ間接続を実現

F5® Distributed Cloud Servicesは、1つまたは複数のクラウドで複数のネットワーキングとセキュリティサービスを管理する NetOps、SecOps、DevOps チームの複雑な運用を簡素化する、革新的で新しいマルチクラウドネットワーキングサービスを提供します。この簡素化を実現する上で重要になるのが、統一されたエンドツーエンドのポリシーときめ細かい可観測性です。

F5 Distributed Cloud マルチクラウドネットワーキングソリューションは以下のとおりです。

- **F5® Distributed Cloud Mesh：**F5 のレイヤー 3 からレイヤー 7 のネットワーキングとセキュリティサービスを統合したスタックには、仮想ルーター、ネットワークファイアウォール、分散ロードバランサ、アプリケーションファイアウォール、API ゲートウェイ、API セキュリティが含まれます。Distributed Cloud Mesh は、顧客のプライベートまたはパブリッククラウド、エッジロケーション（支店や小売店、製造施設など）、および F5 Global Network に導入できます。
- **F5® Distributed Cloud Console：**Distributed Cloud Console は、スタックの複数のレイヤー（L3-L7）間と複数の異種クラウド間に、一元化された可観測性を提供します。
- **F5 Global Network：**高性能なグローバルネットワークは、10 Tbps 以上の容量を提供し、23 以上の POP（Point of Presence）で構成されていて、新しい POP も継続的に追加されています。数 Tbps のプライベートバックボーンは、クラウドや SaaS プロバイダへのプライベートピアリングを提供します。

図 1：F5 のマルチクラウドネットワーキングソリューションのリファレンスアーキテクチャ



F5 DISTRIBUTED CLOUD SERVICES は、NETOPS、SECOPS および DEVOPS チームの複雑な運用を簡素化する、革新的で新しいマルチクラウドネットワーキングサービスを提供します。

- **SaaS-based F5 Distributed Cloud Platform：**F5 Distributed Cloud Platform は、SaaS 型で、エンドツーエンドのライフサイクル管理、AI/ML を活用した分析、API を通じたエコシステムとの豊富な統合機能により、分散コントロールおよび管理プレーンを提供します。

F5 Distributed Cloud マルチクラウドネットワーキングソリューションが、NetOps、SecOps、DevOps チームが直面する課題にどのように対処しているかを説明します。

- **クラウド全体で統一されたポリシーを使用した運用の簡素化：**Distributed Cloud Mesh は、スタックの複数のレイヤー全体で統一された運用モデルを提供します。ルーティングレイヤー、ロードバランサレイヤー、ネットワークファイアウォール、アプリファイアウォールなど、スタックのどのレイヤーでも構成モデルは同じです。Distributed Cloud Mesh は、どのクラウドにも導入でき、クラウド全体で統一されたアプリネットワーキングとセキュリティポリシーを提供します。この分散コントロールプレーンにより、ポリシーと設定は、一度定義されれば、複数のクラウドに導入されたすべてのノードに配布されます。Distributed Cloud Console は、すべてのスタックレイヤーとすべてのクラウド全体にきめ細かい可観測性を提供し、運用チームの完全な可視化を確保します。
- **Infrastructure as Code による自動化とオーケストレーションによる導入の高速化：**Distributed Cloud Mesh は、Infrastructure as Code を提供することで、クラウドプロバイダのネットワーキング構造（AWS トランジットゲートウェイ、VPC アタッチメント、VNet ピアリングなど）の設定の自動化とオーケストレーションを行い、クラウドにおけるネットワーキングとセキュリティの設定および管理の複雑さを軽減します。自動化とオーケストレーションにより、クラウドネットワーキングのスキルギャップの問題を解決し、より迅速な導入を実現します。Distributed Cloud Mesh は、アベイラビリティゾーン、セキュリティグループ、トランジットゲートウェイ、VPC アタッチメントなど、クラウドプロバイダの構造を活用し、クラウドネイティブな手法で一から構築されています。Mesh は、ユーザーが各クラウドの利点を最大限に活用できるようにするとともに、クラウド構造を自動化およびオーケストレーションし、運用を簡素化して、導入を高速化します。
- **きめ細かいネットワーキングとセキュリティ制御：**Distributed Cloud Mesh は、VPC 間トラフィックのセグメンテーション、およびクラウド全体で統一された誘導ポリシーのためのきめ細かいネットワーキングおよびセキュリティ制御を提供します。VPC 間トラフィックは、VPC レベルだけでなく、サブネット、IP アドレス、ポートレベルでセグメンテーションできます。Distributed Cloud Mesh は、柔軟なタグ付けメカニズム（dev、staging、prod など）やビジネスグループ（マーケティング、財務、開発）を提供するので、運用チームは、ビジネスの必要性（たとえば、開発環境のアプリが prod 環境のアプリと通信できないようにする）を表すポリシーを作成できます。

高性能かつ大容量で、プライベートのクロスクラウドバックボーンに支えられる、統一ポリシー、運用簡素化および豊富な可観測性により、クラウド全体でのアプリ間中心の通信による恩恵を受けることができます。

- **高度なセキュリティ制御を実現する、シンプルで柔軟なセキュリティサービスの挿入：** Distributed Cloud Mesh は、クラウド全体における外部セキュリティサービスの導入をオーケストレーションするので、SecOps および NetOps チームは、必要なセキュリティサービスをクラウドで使用できます。Distributed Cloud Mesh は、IP アドレス / ポートレベルのきめ細かい誘導ポリシーを提供し、どのトラフィックをセキュリティサービスで検査する必要があるかを決定します。トラフィック誘導ポリシーは、柔軟なタグ付けメカニズムを使って定義でき、ビジネスの必要性を表すポリシーをクラウド間で統一し、一貫性を確保できます。Distributed Cloud Console は、Distributed Cloud Mesh と外部セキュリティサービスの両方に対して豊富な可観測性を提供し、NetOps および SecOps チームの可視化を強化できます。
- **グローバルなマルチクラウドバックボーンを備えたアプリ中心のアーキテクチャにより、DevOps チームを高速化：** Distributed Cloud Mesh のプロキシベースのアーキテクチャにより、DevOps は、基礎となるネットワーキングおよびルーティングインフラストラクチャを気にすることなく、クラウド全体でアプリをアドバタイズできます。アプリ間中心のグローバルバックボーンにより、DevOps は、クラウド間でアプリを簡単に通信させることができます。NetOps や DevOps がクロスクラウド接続プロバイダに対応する必要はありません。F5 の大容量パブリックネットワークにより、DevOps は、ネットワークとネットワーク上のアプリのセキュリティを完全に保護しながら、ワンクリックで簡単にアプリケーションをパブリックにアドバタイズできます。さらに、F5 Global Network は、クラウドおよび SaaS プロバイダ間のプライベート接続を提供するので、規制対象企業は、アプリ、クラウドおよび SaaS プロバイダのエンドツーエンドのプライベート接続を確保できます。
- **マルチテナンシーとネットワーク分離：** F5 Distributed Cloud Platform は、マルチテナント対応なので、NetOps は、各 DevOps チームのワークスペースを作成できます。そのため、DevOps は、NetOps のサポートを必要とせず、セルフサービス方式で各クラスタに Distributed Cloud Mesh を導入できます。さらに、NetOps チームが組織全体のポリシーを適用するための完全な可視化と制御を維持しながら、DevOps チームは、独自のワークスペースでアプリケーション固有のポリシーを管理できます。Distributed Cloud Mesh は、ワークスペース間でネットワークを完全に分離するため、DevOps チームのアプリケーションは互いに分離されますが、ワークスペース間の通信にポリシーを適用できます。

要約すると、F5 Distributed Cloud のマルチクラウドネットワーキングソリューションは、以下のような差別化要因を提供します。

- ネットワークを公開することなく、アプリや API をクラウド上で配信できる
- L3-L7 ネットワーキングとセキュリティを統合し、クラウドポリシーを統一できる
- ライフサイクル管理のための SaaS ベースのコントローラと分析サービスを利用できる
- クラウド間で決定論的なパフォーマンスを提供するグローバルバックボーンが搭載されている
- F5 BIG-IP およびサードパーティ製ファイアウォールのサービス挿入により拡張できる

高性能かつ大容量で、プライベートのクロスクラウドバックボーンに支えられる、統一ポリシー、運用簡素化および豊富な可観測性により、クラウド全体でのアプリ間中心の通信による恩恵を受けることができます。

図 2：F5 Distributed Cloud Platform と競合ソリューションのマルチクラウドネットワーキング機能の比較

機能	その他のソリューション	Distributed Cloud Mesh
統合 L3-L7+ ネットワーキング＋セキュリティサービス	X	✓
NetOps と DevOps のためのマルチテナンシー＋セルフサービス	X	✓
マルチレイヤーのセキュリティ	X	✓
基礎となるネットワークを公開しないアプリ間接続	X	✓
グローバルな物理ネットワーク	X	✓
セキュリティサービス挿入	✓	✓
NetOps のための自動化支援	✓	✓
可観測性と分析	外部	✓
ライフサイクル管理	コントローラ	SaaS

使用事例

F5 Distributed Cloud Services によるマルチクラウドネットワーキングの 4 つの重要な使用事例：

1. マルチクラウドトランジット

Distributed Cloud Mesh は、マルチクラウドトランジット機能により、あらゆるクラウドにシームレスでセキュアなネットワーキングを提供します。インターネット経由、自社のプライベートバックボーン、または F5 Global Network のいずれかの物理トランジットを介して複数のクラウドを安全に接続します。このソリューションのコントロールプレーンである F5 Distributed Cloud Console は、SaaS ベースの運用および可観測性ポータルであり、パブリックおよびプライベートクラウドやエッジサイト全体のインフラストラクチャおよびアプリを管理できます。
F5 Distributed Cloud Platform は、以下を提供します。

- マルチクラウドネットワーキングを簡素化する SaaS ベースのコントロールプレーン
- 高度に自動化された、高速かつ冗長で、セキュアなサイト間接続

- L3-L7 ネットワーキングおよびセキュリティの統合
- 各クラウドプロバイダのネットワーキングとセキュリティの構造のオーケストレーションおよび自動化
- すべてのクラウドにおいて、ネットワーク、セキュリティ、およびアプリケーションの健全性とパフォーマンスを示す単一の信頼できる情報源
- F5 グローバルネットワークのファイババックボーン、顧客提供のネットワーク、または完全に自動化されたサイト間 IPsec/SSL 仮想プライベートネットワークなど、グリーンフィールドまたは既存環境向けのさまざまな接続オプション

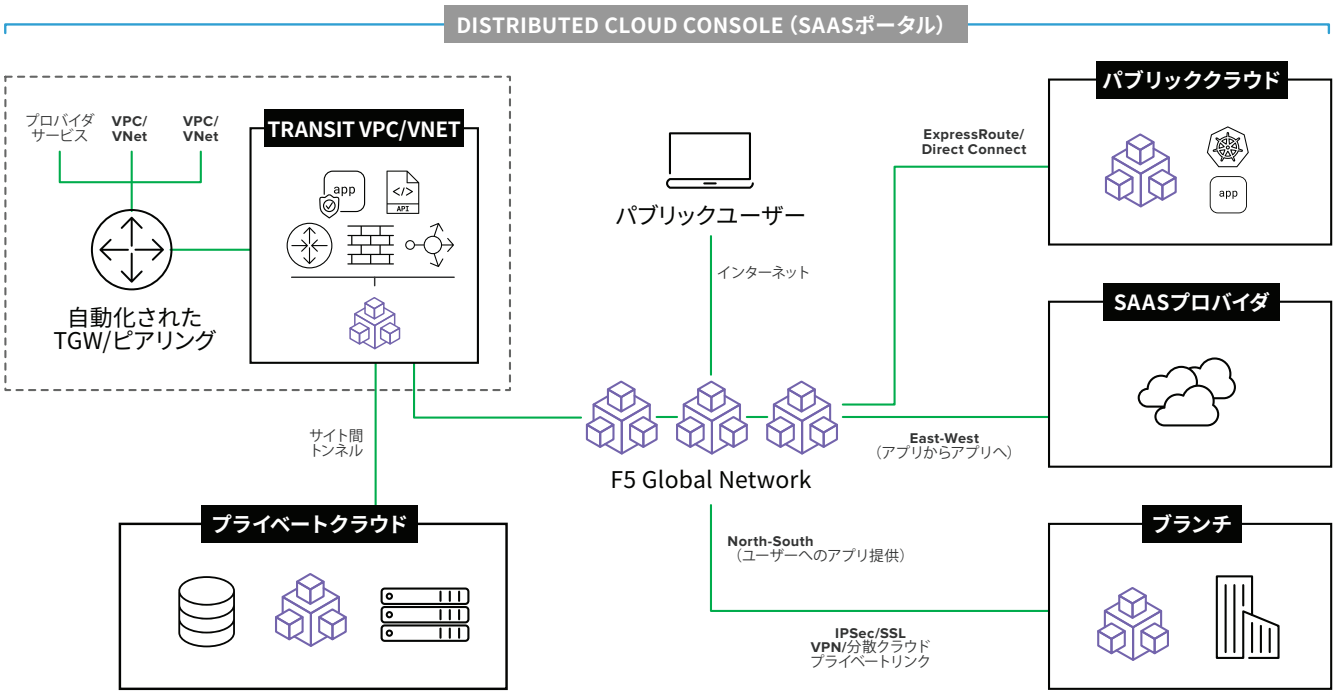


図 3：Distributed Cloud Mesh 内部でのマルチクラウドトランジットがどのように機能するかを視覚的に示した図

2. セキュリティサービス挿入

Distributed Cloud Mesh と Distributed Cloud Console により、F5® BIG-IP 製品やその他のサードパーティ製セキュリティサービスを挿入できます。そのため、SecOps チームは、既存のスキルセットとポリシーへの投資を保護しながら、すべてのプライベートクラウドとパブリッククラウドにセキュリティサービスの制御を拡張できます。

Distributed Cloud Mesh は、クラウドに依存しないトラフィック誘導ルールにより、セキュリティサービスを適用する場所と方法を簡素化します。誘導ルールにより、ネットワークトラフィックは、仮想クラウドネットワークからセキュリティサービスを経由し、宛先に再ルーティングされます。異なるパブリックおよびプライベートクラウドでも同じ誘導ルールが使用されます。F5® Distributed Cloud Console を使用することで、IT 専門家は、クラウドおよびネットワークにおけるトラフィックのきめ細かい可視化と一元管理を行うことができます。

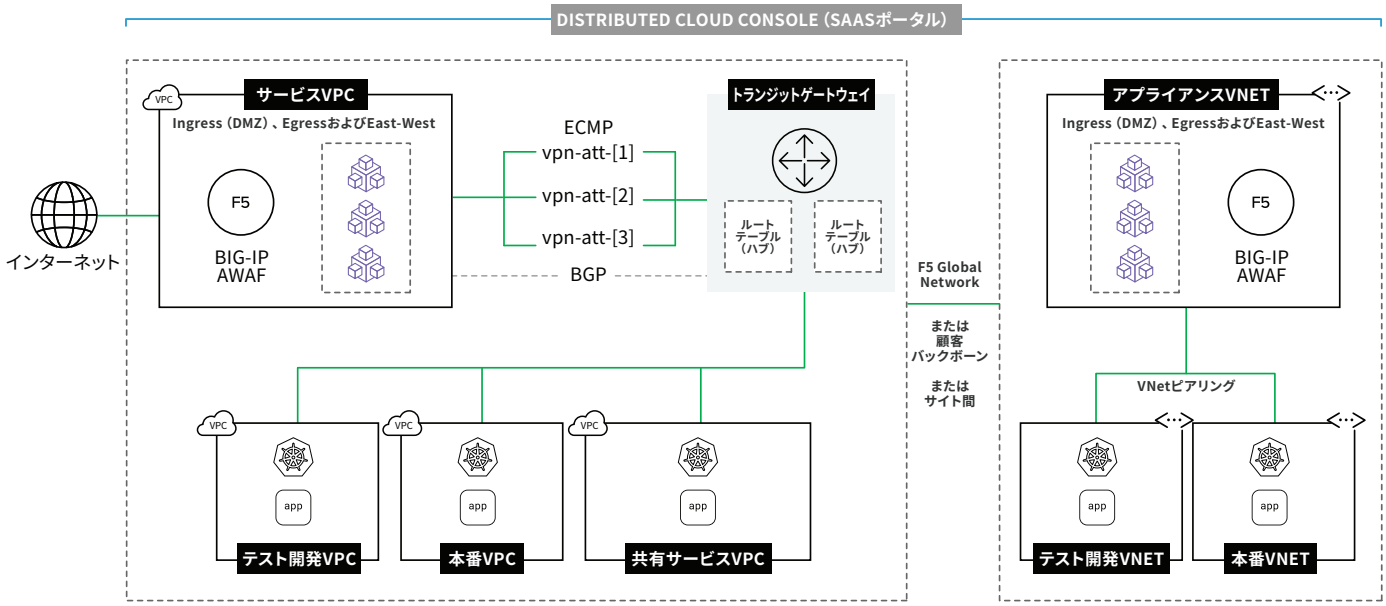


図 4：セキュリティサービス挿入の使用事例を視覚的に示した図

3. マルチクラスタアプリメッシュ

マルチクラスタアプリメッシュは、きめ細かく制御せず、基礎となるネットワーキングとルーティングを気にせずに、顧客のパブリックまたはプライベートクラウドと F5 Global Network 全体でアプリケーションと API をアドバタイズできます。あるクラスタでホストされているアプリケーションサービスは、クラウド間で他のローカルクラスタやリモートクラスタにエクスポートおよびアドバタイズでき、分散アプリを透過的に相互接続させることができます。Distributed Cloud Mesh は、サービスを提供するだけでなく、サービスを監視し、フルスタックの高度なセキュリティを適用して、あらゆるセキュリティホールを排除します。

この使用事例は、Kubernetes にも、従来の仮想マシンやコンテナ環境にも適用されます。Distributed Cloud Mesh は、Kubernetes にネイティブに接続してサービスを検出、特定のサービスをクラウド間のリモートクラスタにアドバタイズ、およびクラウド間でセキュリティポリシーを配布してアドバタイズされたサービスを保護できます。

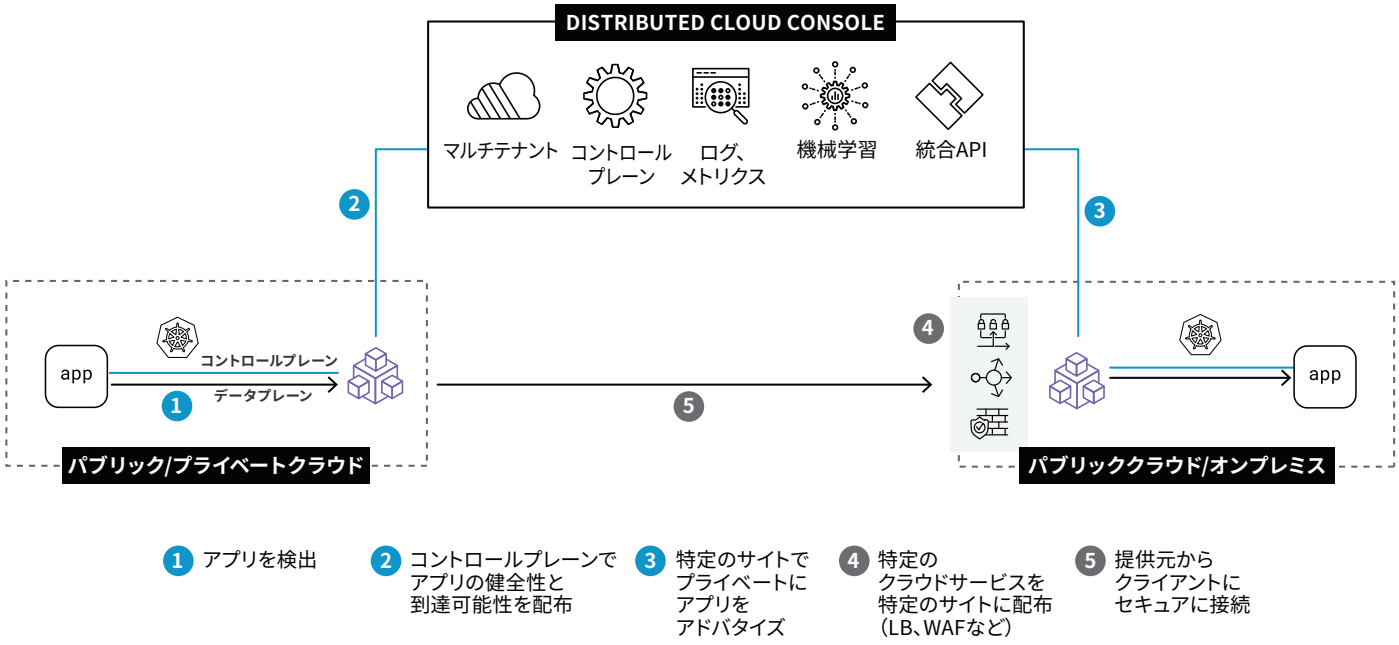


図 5：Distributed Cloud Mesh で提供されるマルチクラスタアプリメッシュを視覚的に示した図

4. IP アドレスの重複

Distributed Cloud Mesh は、そのプロキシベースのアーキテクチャにより、IP の重複に対するクリーンなソリューションを提供します。重複が問題になるのは、基礎となるネットワーク上の接続が公開されている場合のみです。Distributed Cloud Mesh は、基盤となるレイヤー 3 ネットワークが公開されているかどうかに関係なく、クラスタ間のレイヤー 7 でサービスをアドバタイズできます。そのため、レイヤー 3 ネットワークに重複する IP があっても、サービスはクラスタ間でアドバタイズできます。

Distributed Cloud Mesh を使用することで、リモートサービスの実際の IP アドレスが何であっても、リモートサービスをローカル IP アドレスでローカルサブネットに配信できます。そのため、ネットワークの変更は一切必要ありません。ネットワークアドレス変換（NAT）、ファイアウォールのピンホール、ルーティング変更もありません。Distributed Cloud Mesh は、最もクリーンな IP 重複ソリューションとして、ネットワークを遮断することなく完全な制御と完全な可視化を提供します。

マルチクラウドネットワーキングソリューションを無料でお試しする、または他のオプションを確認できます。詳しくは、F5.com のマルチクラウドネットワーキングのウェブページを参照してください。