# 「HashiCorp」製品で加速する クラウドとオンプレの運用一元化と高度な自動連携

## ハイブリッドクラウド運用に適したIaCソリューション

クラウドが多くの企業の IT インフラとして一般的になる一方で、 既存のオンプレミス環境を使い続ける例も少なくありません。IT 部門に負担の大きいハイブリッド運用を効率化する手段として期待されるのが、 Infrastructure as Code （IaC） を用いた IT インフラの自動化です。 今回はハイブリッドクラウド環境にてインフラ運用の自動化が求められる背景を踏まえた上で、 実際の例として、 クラウド上に構築した仮想アプライアンスのロードバランサの動的な設定変更を、 HashiCorp 製品を用いて実現する例を紹介します。

## クラウドの先進機能は魅力である一方、既存環境との併存運用が課題

企業のITインフラとして、クラウドプラットフォームは多くの魅力を備えています。ハードウェアのセットアップ・運用管理が基本的に不要であり、優れた可用性を得ることができる上に、ソフトウェアベースでさまざまな機能を実装できるため、短期間でシステムを構築できるようになっています。しかも、メガクラウドとも呼ばれる世界的クラウド事業者を中心に、数々の最先端テクノロジーを容易に使えるようになっている点も魅力といえるでしょう。

クラウドインフラでは、そのさまざまな機能をソフトウェアによる定義で設定できます。設定を動的に変化させられるため、高い柔軟性や拡張性が得られ、また自動化を駆使して運用管理の負担軽減も可能です。オートスケールは、その中でも代表的かつ分かりやすい例といえるでしょう。システムに対する負荷が増大した際、仮想マシンやコンテナを自動的に増やして拡張することで、管理者が手間をかける必要なく、パフォーマンス低下などの問題を避けることができます。

クラウドを生かせば人的リソースを運用から開発などへ振り向けられるようになるという期待感から、既存のオンプレミス環境にあるシステムのクラウド移行（クラウドリフト）や、クラウドネイティブな機能の積極的な活用（クラウドシフト）に取り組む企業も多く見られます。しかし、そこには課題もあります。

完全に移行するまでは両方の環境を並行して運用することになるため、管理の複雑さを伴うことがあります。しかも、社内の全てのサーバーをクラウド移行するには時間がかかり、場合によっては完全にクラウドへ移行せずオンプレミス環境も一部に残すという判断もあるでしょう。

異なる複数のITインフラを並行稼働させることは、運用負荷の増大につながります。例えば新たなサービスをリリースする際、いちいち複数の画面を開いて、それぞれに対して相互に関連し合う設定を、間違いないよう行う必要があります。会社として規定されているセキュリティポリシーなどを適用させる際も、それぞれの環境ごとに管理コンソールや運用ツールを用いて、別々に行うことになるはずです。二度手間になるだけでなく、設定ミスなどのリスクも増大してしまいます。

## クラウド時代の運用を変えるIaC、オンプレミス対応のツールも

混在環境の課題はオンプレミス環境の時代からありました。その運用を支えるため、これまでにもさまざまな運用管理ツールが登場し、使われています。そして近年では、クラウド環境を中心とした「Infrastructure as Code」（以下、IaC）ツールが普及してきました。

IaCはITインフラをコードベースで管理・制御する仕組みです。メガクラウドを中心に、クラウド上で使われるものというイメー

ジを持つ方もいるかもしれませんが、必ずしもそうとは限りません。ツールによっては、複数のパブリッククラウドやプライベートクラウド、さらには主にオンプレミスで使われるITインフラ機器まで含めて一元的に扱えるものがあります。こうしたIaCツールを活用すれば1つのツールで操作できるようになり、運用に統一感を持たせることが可能です。

もう少し具体的に説明していきましょう。クラウドとオンプレミスの混在環境でよくある例として、クラウド上のサーバーへのアクセスをオンプレミスのファイアウォールなどで制御しているようなケースが考えられます。近年の高機能なファイアウォールやUTM（統合脅威管理）製品は、WAF（Webアプリケーションファイアウォール）やサーバー側のロードバランサ、リモートワークなどに伴い増加した社外からのVPNアクセスなど、多くの企業が複数の機能を活用していることもあって、容易には移行や移動ができません。機能面もさることながら、長年の実績に裏付けられた信頼性や、IT部門にとって使い慣れたものであることも含め、捨てがたい存在です。こうした理由から、クラウドへの移行過程でも、こうしたオンプレミスのファイアウォールを経由して、クラウド上のサービスにアクセスさせる形態になる場面は多いと考えられます。

しかし一方で、既存ファイアウォール製品は基本的にクラウドライクな動的な対応を想定した作りではありません。クラウド側の変化に合わせた対応をさせるには、外部から動的に設定を変更する仕組みが求められます。そこで役立つのが、IaCツールの中でも、オンプレミスの多彩な機器にも対応した製品、というわけです。

## 東京エレクトロンデバイスのノウハウを生かし、IaCツールのオンプレミス適用を加速

上記の課題に対応し、マルチクラウドからオンプレミスのITインフラ機器まで幅広くカバーするIaCソリューションの1つがHashiCorpの開発する「Terraform」です。東京エレクトロンデバイスでは、Terraformをはじめ、HashiCorpの製品の代理店として、以下の製品を取り扱っています。

**●クラウドインフラの自動化「Terraform」**

IaCを活用してインフラを自動化する製品です。クラウドはもちろん、オンプレミス環境のネットワーク機器やサーバー、ストレージなどのインフラについて、コードでの構成定義やプロビジョニングの自動化、変更管理やバージョン管理を実現します。エンタープライズ向けの「Terraform Enterprise」では、組織としてのセキュリティ運用やガバナンスに役立つ機能、Terraform自体の可用性やパフォーマンスを向上する機能も備えています。本製品を活用することで、オペレーション自動化の促進、作業にかかわる人的ミスや工数の削減、ITインフラの容易な変更管理、インフラ構成の再利用性向上を実現できます。

**●クラウドセキュリティの自動化「Vault」**

トークン、パスワード、証明書、暗号化キーなどの機密データをセキュアに一元管理し、それらへのアクセスを厳密に制御する製品です。対象となるクラウドサービスや機器、アプリケーションやデータベースなどの認証情報をセキュアに一元管理して必要時のみ発行する動的シークレット管理機能、データベースに入力する個人情報や機密性の高い情報を暗号化するEncryption as a Service機能により、生産性とセキュリティの向上に役立ちます。

**●クラウドネットワークの自動化「Consul」**

一元的な共有レジストリにより、クラウドネットワークを自動化する製品です。動的なIPアドレスなどで構成されるクラウドネイティブインフラのネットワーク構成において、自動管理、ポリシー制御を可能にします。あらゆるアプリケーションやサービスを動的に検出するサービスディスカバリ機能、動的に変化するIPアドレスでなくサービス名に基づく共有レジストリ機能、そしてサービスごとに定義された通信ポリシーに従って通信制御を行うサービスメッシュ機能により、作業工数やミスの削減に効果を発揮します。

**●クラウドアプリケーションの自動化「Nomad」**

あらゆるアプリケーションに使える、シンプルで柔軟なワークロード用のスケジューラー・オーケストレーター製品です。デプロイ前の空きリソース検証、検証結果に基づくワークロードに最適なデプロイ、ワークロードの稼働状況の管理と維持を自動実行するスケジューリング機能を備え、またTerraform、Vault、Consulと統合して使えるようになっており、これらを組み合わせて一元化

されたインフラプラットフォームを実現でき、作業の工数やミス削減に役立ちます。

東京エレクトロンデバイスでは、これらHashiCorp製品と、長年培ってきたオンプレミス環境の製品に関する自社のノウハウとを組み合わせ、ハイブリッド・マルチベンダー環境の自動化ソリューションを構築していきます。

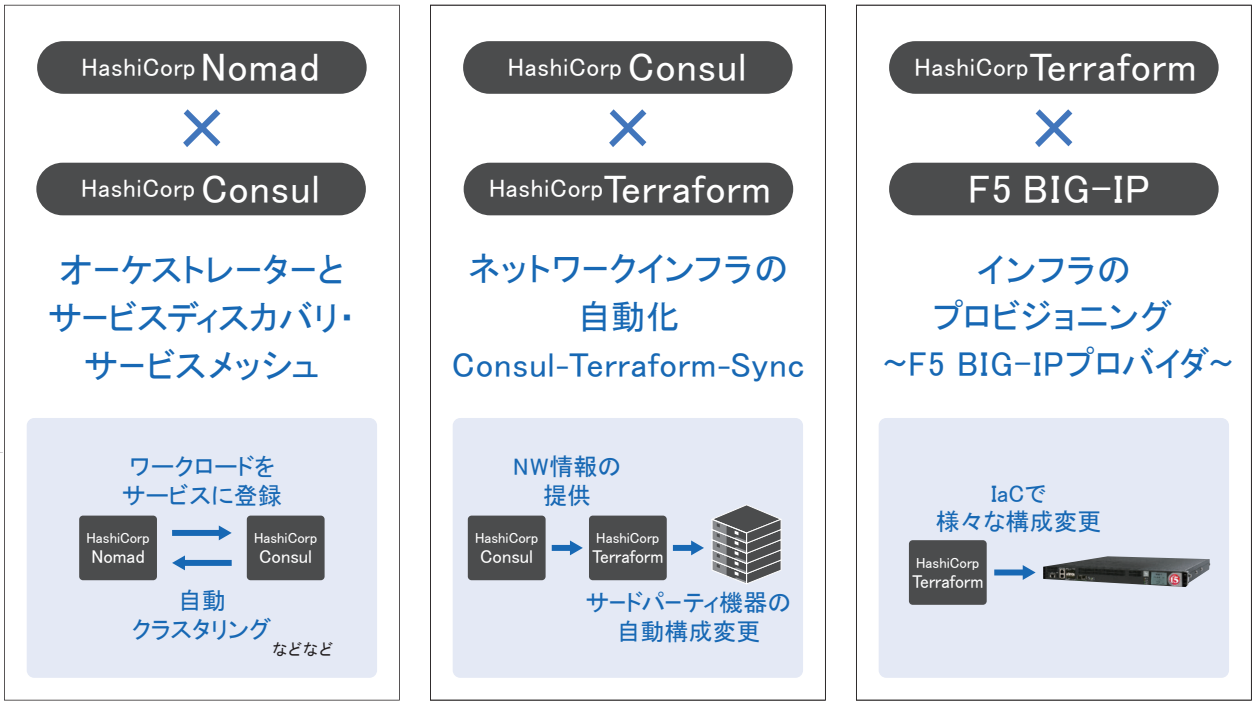
## コンテナデプロイに応じた負荷分散の設定自動化を実証

ハイブリッド・マルチベンダー環境の自動化について、東京エレクトロンデバイスでは、さまざまなベンダーの製品と実際に連携させる実証にも取り組んでいます。その実例の1つとして今回紹介したいのが、ロードバランサとの連携自動化です。ロードバランサ製品には、当社が販売代理店として長年扱っているF5 BIP-IPを用いています。

**●システム構成**

・コンテナ環境：Docker
・ロードバランサ：F5 BIG-IP(今回は仮想アプライアンスを使用)
・オーケストレーター： HashiCorp Nomad
・サービスディスカバリ／サービスレジストリ：HashiCorp Consul
・IaC：HashiCorp Terraform

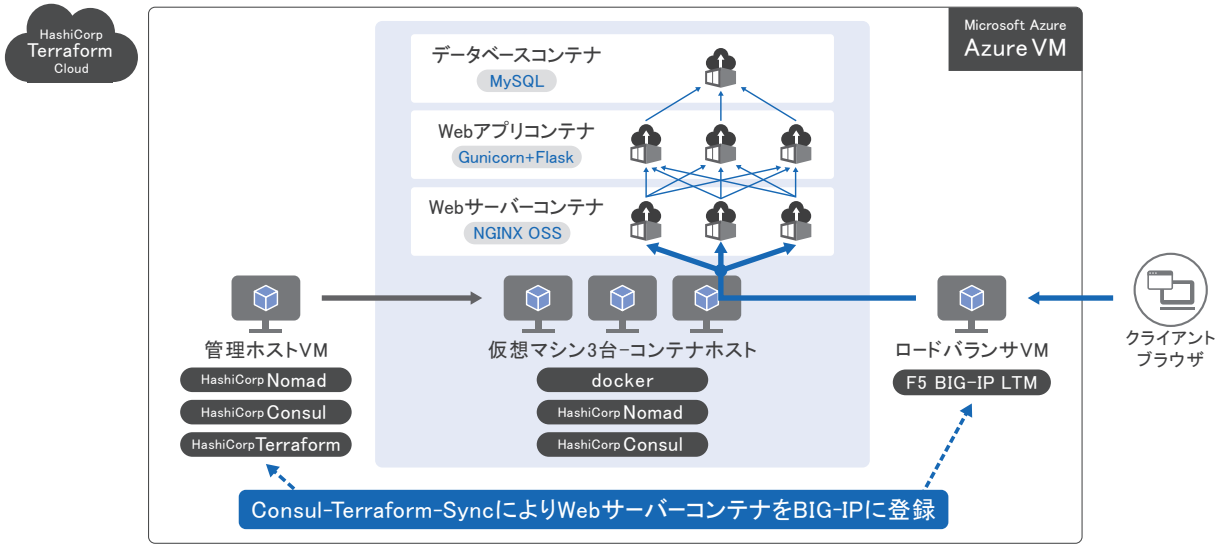
HashiCorp製品がF5 BIG-IPの設定変更を自動的に実行するために、下図のような連携を行います。




本実証における HashiCorp の各製品の連携

**●実証における各製品の連携の流れ**

あらかじめ、Dockerのホストとして、Microsoft Azure上の仮想マシンを用意してあります。今回の実証では、このDocker上にデータベースとWebアプリケーション、Webサーバーの3階層に分かれたコンテナをデプロイし、デプロイが完了したコンテナに対しサービスメッシュを構成、F5 BIG-IPのロードバランサで負荷分散設定を行うまでの連携を試してみました。




本トライアルにおけるシステム全体構成図

改めて各製品の役割を説明しましょう。Nomadは宣言型のコードでワークロードをデプロイできる製品です。どのアプリをどのクラウドに、どれだけのリソースで何インスタンス立ち上げるかなど、これから実現しようとする形態をコードとして宣言しておき、デプロイを自動実行するものです。

ConsulはNomadとの連携を通じて、新たにデプロイされたワークロードを自動検出し、ネットワーク情報などをサービスレジストリに登録します。こうして動的に変更・生成されたネットワーク情報がTerraformに連携されることで、BIG-IPの構成変更が自動実行できるという仕組みです。

F5社ではTerraform用のBIG-IPプロバイダを提供しており、Terraformはこれを介してBIG-IPの設定変更を行います。Nomadでジョブを実行するだけで、ここまでの一連の変更が自動的に連続して行われ、全て完了した時点で、完全な形でサービスが開始されるのです。

今回の実証では、3種類のコンテナを各1個ずつデプロイした状態から、WebアプリとWebサーバーのコンテナをスケールアウトすると、Consulがこれを検知してサービスメッシュを再構成し、続いてTerraformがBIG-IPのサーバープールに追加登録を行い、負荷分散が開始されることを検証しました。また、逆にコンテナ数を減少させた場合も、同様に一連の設定変更が自動で行われます。

## さまざまなサードパーティ連携、ユースケースの検証を計画

TerrafromとBIG-IPの連携は、今回トライアルしたロードバランサ以外にも、ファイアウォールのルール管理やDNSレコード管理などにも適用できると考えられます。またF5製品に限らず、さまざまなサードパーティ製品との連携が可能になることでしょう。東京エレクトロンデバイスでは、今後も引き続き、オンプレミス機器を中心としてさまざまな連携を検証し、また検証が求められる各種ユースケースを発掘していく方針です。ご興味、ご関心のある方は、ぜひ東京エレクトロンデバイスにご相談ください。



東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp

新宿：〒163-1034 東京都新宿区西新宿 3-7-1 新宿パークタワー S34 階
Tel.03-5908-1990 Fax.03-5908-1991

大阪：〒540-6033 大阪府大阪市中央区城見 1-2-27 クリスタルタワー 33 階
Tel.06-4792-1908 Fax.06-6945-8581

名古屋：〒451-0045 愛知県名古屋市西区名駅 2-27-8 名古屋プライムセントラルタワー 8 階
Tel.052-562-0826 Fax.052-561-5382

つくば：〒305-0033 茨城県つくば市東新井 15-4 関友つくばビル 7 階
Tel.029-848-6030 Fax.029-848-6035

お問い合わせは、Web サイトの下記フォームよりお願いします。
https://cn.teldevice.co.jp/product/hashicorp/form.html