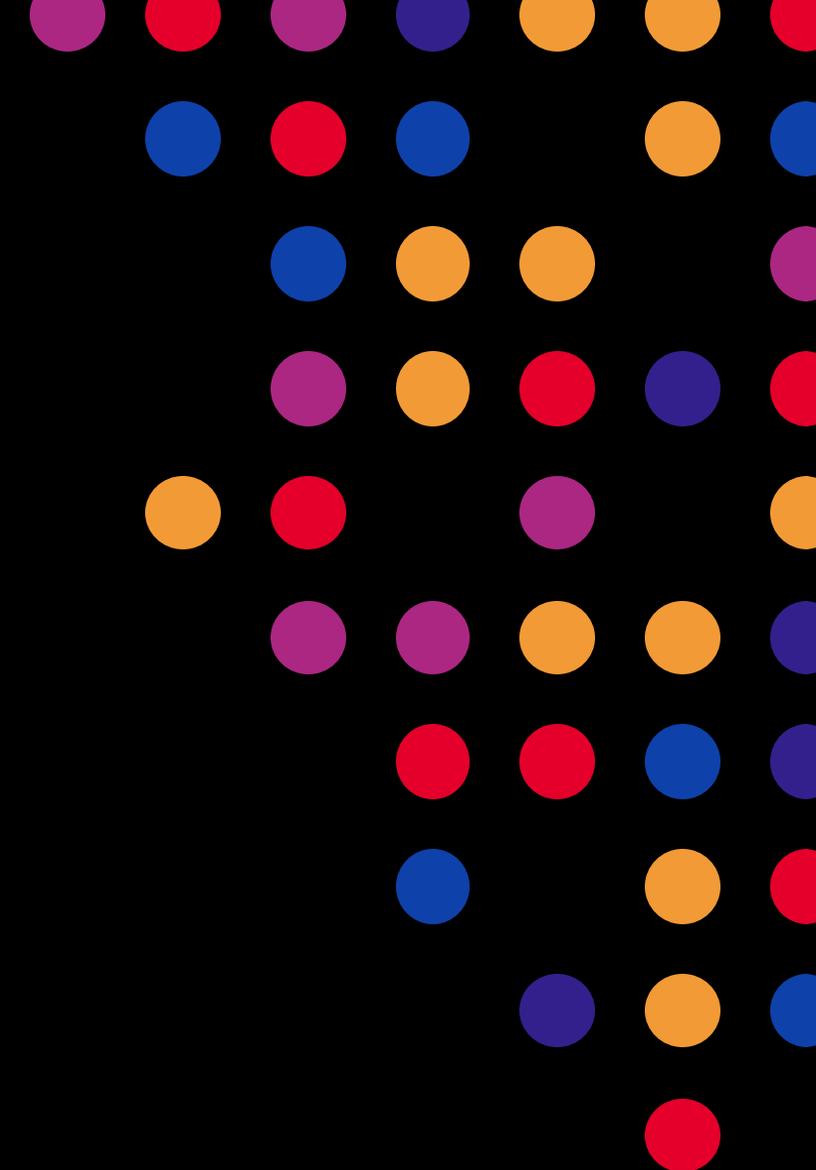




KVM最前線！ OpenShift Virtualizationと F5XCで実現するフレキシブルな 仮想化プラットフォーム

山川 達也

ソリューション営業部 セールススペシャリスト
レッドハット株式会社



レッドハット - 会社概要

米国本社

名称 : Red Hat, Inc.
本社所在地 : 米国ノースカロライナ州 ローリー
創業 : 1993年
従業員数 : 約19,000人 (2022年1月現在)
事業所数 : 35ヶ国、世界95オフィス
社長/CEO : マット・ヒックス

日本本社

名称 : レッドハット株式会社
本社所在地 : 東京都渋谷区恵比寿
営業所 : 大阪営業所 (大阪市北区)
: 中部営業所 (名古屋市中村区)
: 九州・中国営業所 (福岡市博多)
設立 : 1999年9月
代表者 : 三浦 美穂
事業内容 : Red Hat 製品の販売、サポート
教育、コンサルティングサービスの提供

Fortune 500の**90%+**のお客様がレッドハットの製品を利用

19,000+人の従業員

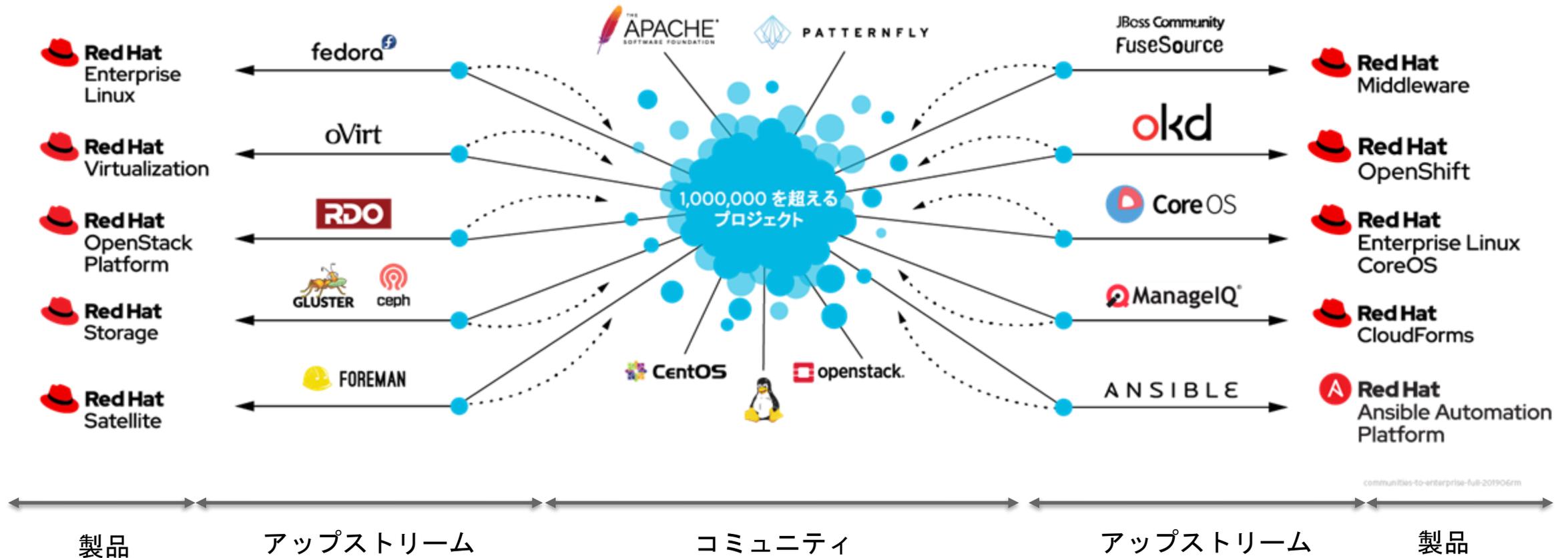
95+の地域、**35+**カ国でビジネスを展開

1993年	創業
1999年	NASDAQ上場 (NASDAQ: RHAT)
2002年	Enterprise Linux提供開始
2006年	NYSE上場 (NYSE: RHT)、JBoss Inc. 買収
2009年	S&P 500に入る
2012年	OpenShift Enterprise提供開始
2013年	Red Hat OpenStack Platform提供開始
2015年	Ansible (IT自動化)買収
2016年	3scale買収 (API管理)
2019年	IBMによる買収が完了
2021年	StackRox買収(コンテナセキュリティ製品)
2022年	主要パブリッククラウド上でのマネージドサービスの提供



レッドハットとオープンソース・コミュニティ

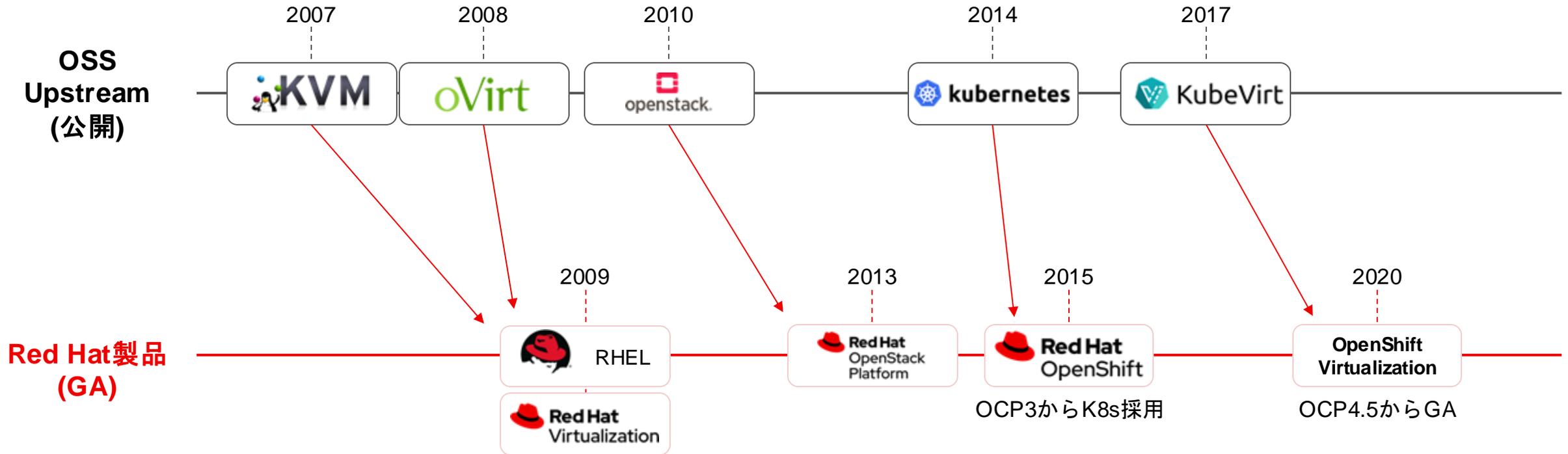
オープンソースコミュニティに参加し、開発されたソフトをエンタープライズ版にして販売



communities-to-enterprise-fall-201906rm

仮想化関連のOSSプロジェクトとRed Hat製品の関係

これまでRed Hatは、OSSのUpstreamにあるProjectを取り込んだITインフラ仮想化製品を継続的に市場に投入してきました。



OpenShift Virtualization 概要

OpenShift Virtualization

次世代の仮想化を担うアプリケーション・プラットフォーム

1. OpenShift が提供するサーバー仮想化機能

- a. Linux の仮想化機能に基づくサーバー仮想化
- b. OpenShift に標準で含まれる機能で、追加費用は不要

2. Linux と Windows の両方の仮想マシンをサポート

- a. 代表的な Linux ディストリビューションと Windows Server のテンプレートを標準装備
- b. Red Hat Enterprise Linux の仮想マシンは無償・無制限で使用可能

3. 仮想マシンの専用移行ツールを用意

- a. 既存のサーバー仮想化環境から OpenShift Virtualization へ仮想マシンを移行するツールを無償で使用可能



Virtual Machine



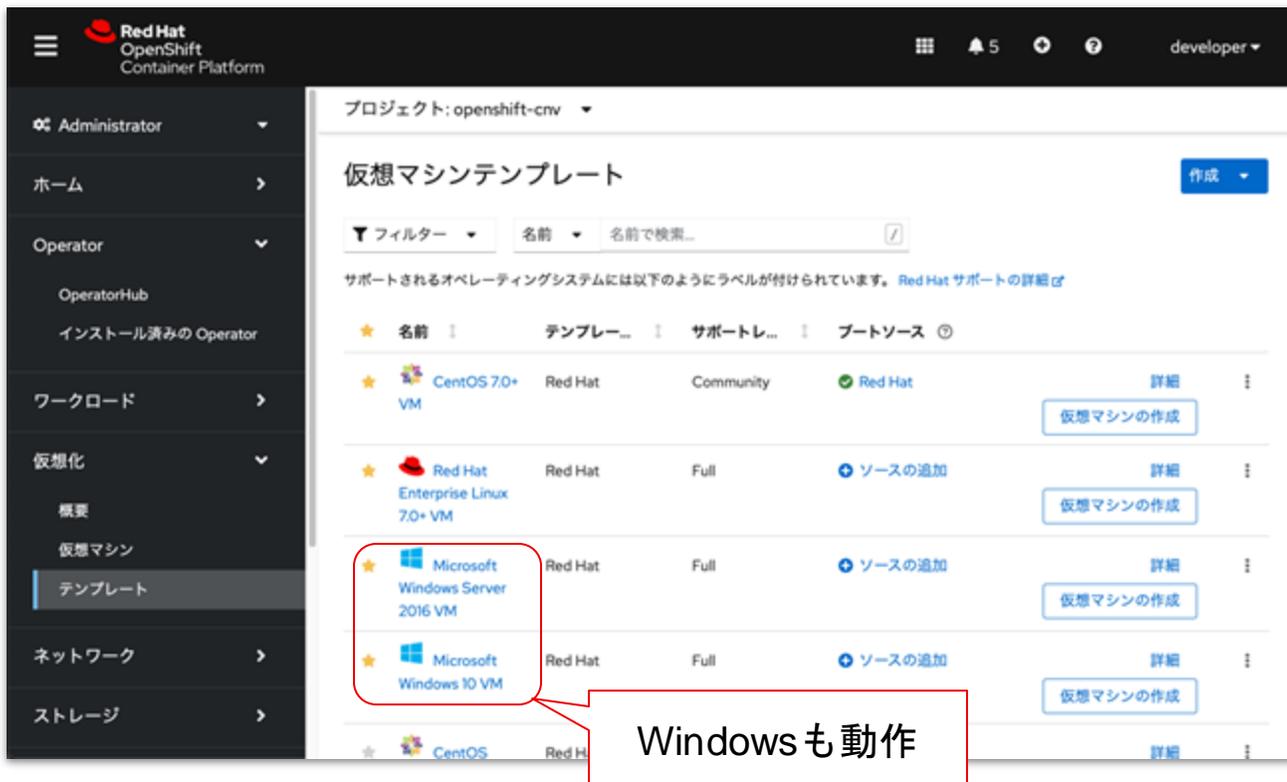
OpenShift Virtualization

Red Hat OpenShift



OpenShift で仮想マシンを起動・管理できる標準機能

これからはOpenShiftでコンテナのみならず仮想マシンも起動・管理できます。OpenShiftの標準機能として、全てのEdition*1に含まれています。コンテナ・VMが混在するシステムを統一したインターフェースで運用できます。

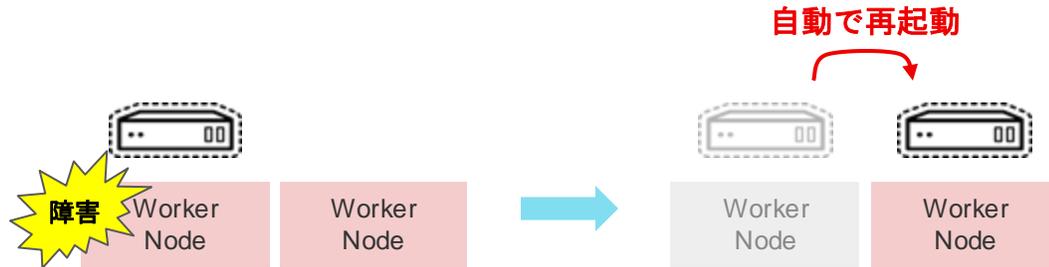


- OpenShift (Bare Metal Node) で動作し、LinuxのKVM機能を応用してVMを扱うことができます
- UpstreamのOSS「KubeVirt」は2023年7月に1.0版をリリースし、技術としても一定の成熟を果たしています
- OpenShift Virtualizationの機能はOperatorHubから簡単に無料でインストール可能です

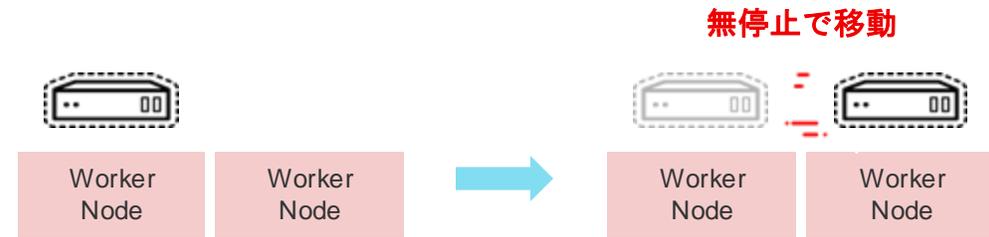
OpenShift Virtualization が提供するサーバー仮想化機能

OpenShift Virtualization は、仮想化基盤を支える様々な機能を用意しています。

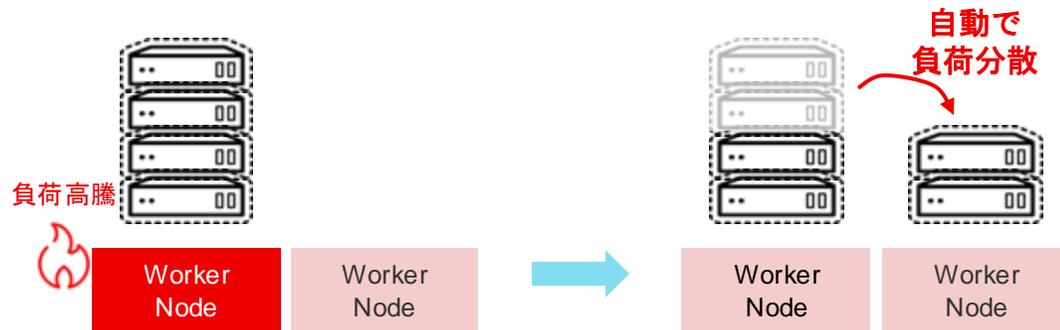
高可用性 (HA)



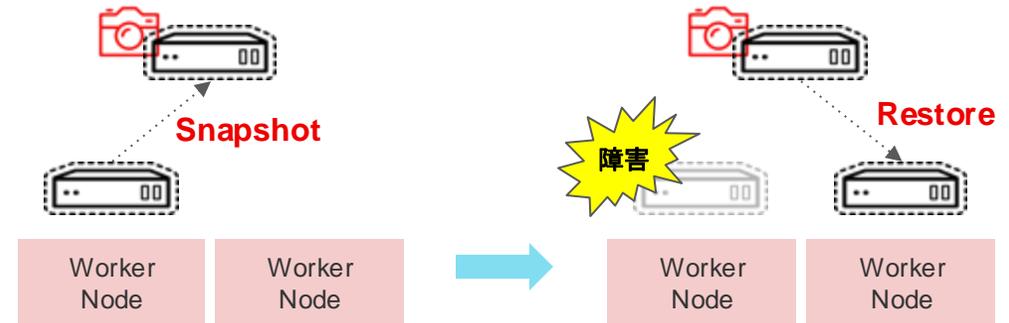
ライブマイグレーション



負荷分散



VM スナップショット / リストア



OpenShift には RHEL VM の費用が含まれています

OpenShiftにEntitlementされるSubs

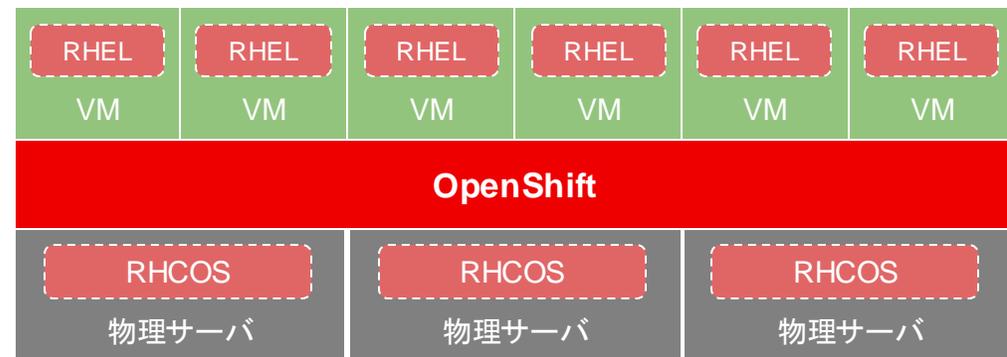
個別に利用料がかかるSubs

OpenShift 上の RHEL 仮想マシンの Subscription は OpenShift Virtualization 機能自体に含まれており、別途 Subscription 購入は不要です。また RHEL 仮想マシンの台数制限もありません。他社製ハイパーバイザ上の RHEL コストの大幅削減が目指せます。

RHEL Subsを別途購入する必要あり



コスト増減：
- 他社製ハイパーバイザ費用
- RHEL Subs費用
+ OpenShift Subs費用



今こそCentOS to RHELのチャンスです

ハイパーバイザをOpenShift Virtualizationに変える事は、お持ちのCentOS仮想マシンを一気にRHELにマイグレーションするチャンスです。これを機会にエンタープライズグレードのOSの1つであるRHELの利点を手にしてください。

CentOSの位置づけの変更



CentOS Linux7が**2024年6月**で終了し、以後、Communityの体制はCentOS Streamのリリースモデルに移行します



高頻度でUpdateされ、RHELの将来のマイナーリリースのベースとして、開発者の方々がいち早く触れる事ができるようになります。この変更は回り回ってエンドユーザー様にも好循環をもたらします

RHEL≠CentOSの有料版、長期サポートだけじゃない魅力



分散するIT環境・ハイブリッドクラウドにおけるRHELのコンテンツ配信、パッチ、プロビジョニングを含め全てを一元管理

Red Hat Satellite でインフラストラクチャを管理



Red Hatの知見の提供とプロアクティブかつ具体的な推奨行動の喚起、最新の脅威・脆弱性への対応方針の展開等、RHELを徹底的に使いこなす為のツールで、OpenShift / RHELに含まれるサービスです

Red Hat Insights データを調べる。問題を特定する。対応策を講じる。

OpenShift Virtualizationなら、新たな費用増無しでRHELにマイグレーションできます

CentOS Linuxを含むRPM系Linuxは、Convert2RHEL*1を利用して簡単にRHELへ移行できます



ユーザー事例

Ally Bank

新しい環境はあらゆる側面を強化し近代化する機会をもたらす。既存の仮想環境上で長年にわたって学んだ教訓を取り入れながら、約13,000VMを対象に移行計画を進めており、現時点で約5,000VMの移行が完了している



なぜOpenShift Virtualizationという道を選んだのか、そしてそのアーキテクチャーやPOC、移行プロセスを通して得られた教訓について深く掘り下げたセッションとなった

Why OpenShift Virtualization?

1つのプラットフォームでコンテナと仮想マシンを、RHELだけでなくWindowsも混在して実行・管理することができる

- OpenShiftエコシステムをコンテナ管理と同様に活用できる
- 仮想マシンとコンテナを同じクラスターで管理することにより、サービスにスケーラビリティを持たせられている

移行プロジェクトのポイント

- 2018年からOpenShiftを利用し始め、ボーダーを設けずにモノリス Appsをマイクロサービス化推進している
- 1年半前からOCPVを検討開始し、移行しやすいワークロードから移行している (CMDDBやCOTSに苦労している)
- OCPVクラスターは最小構成で構築し、それ以降は移行で空いた仮想環境のリソースを再利用している
- いわゆるSORの健全性を再評価するに至っている
- Migration ToolkitやAnsibleを活用し、移行を完全に自動化している (週に数百VMの移行が可能な状態になっている)

OpenShift Virtualization 技術要素

OpenShift クラスターの構成



Control Plane Node (3 nodes)

- クラスター全体にわたってリソース*1を管理する役割を持つノード
- OS は Red Hat Enterprise Linux CoreOS*2 (RHCOS)

API Server: リソースのライフサイクル制御に使うインターフェース

Controllers: リソースの状態を常に監視し好ましい状態になるよう制御

Schedulers: リソースの配置するノードを決定

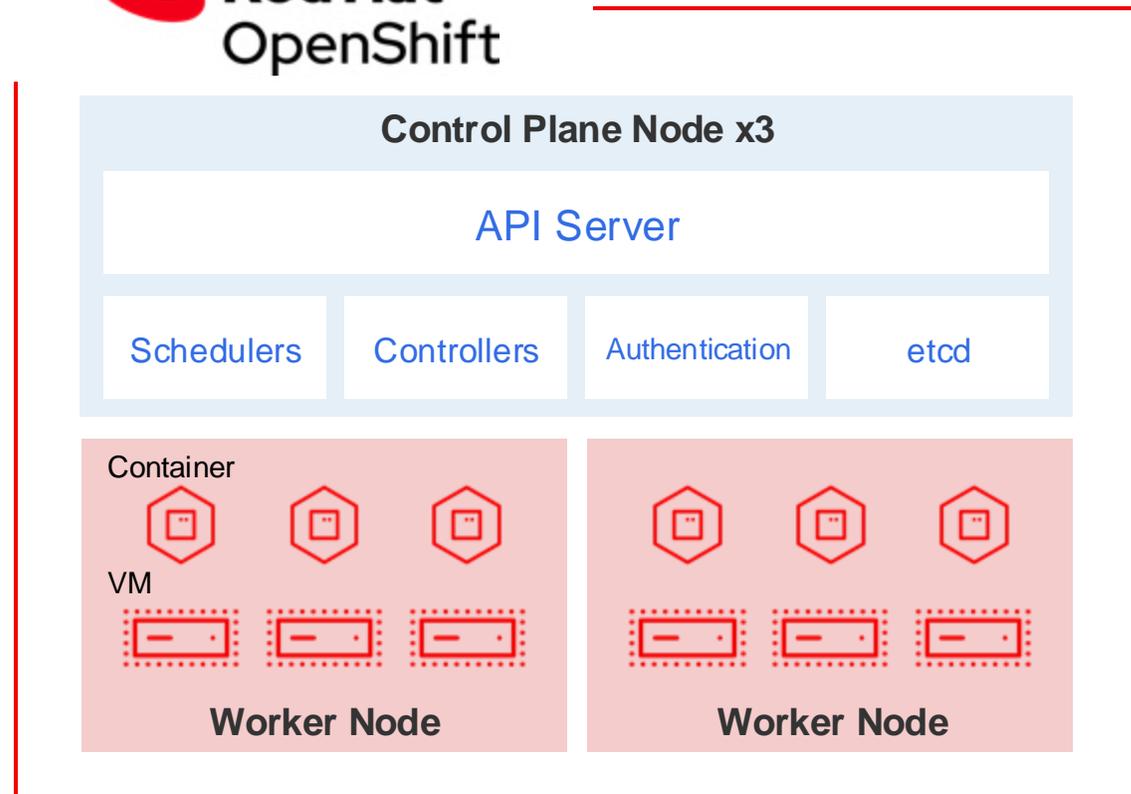
Authentication: ユーザー認証サービスを提供

etcd: クラスターの状態や構成を管理するデータベース



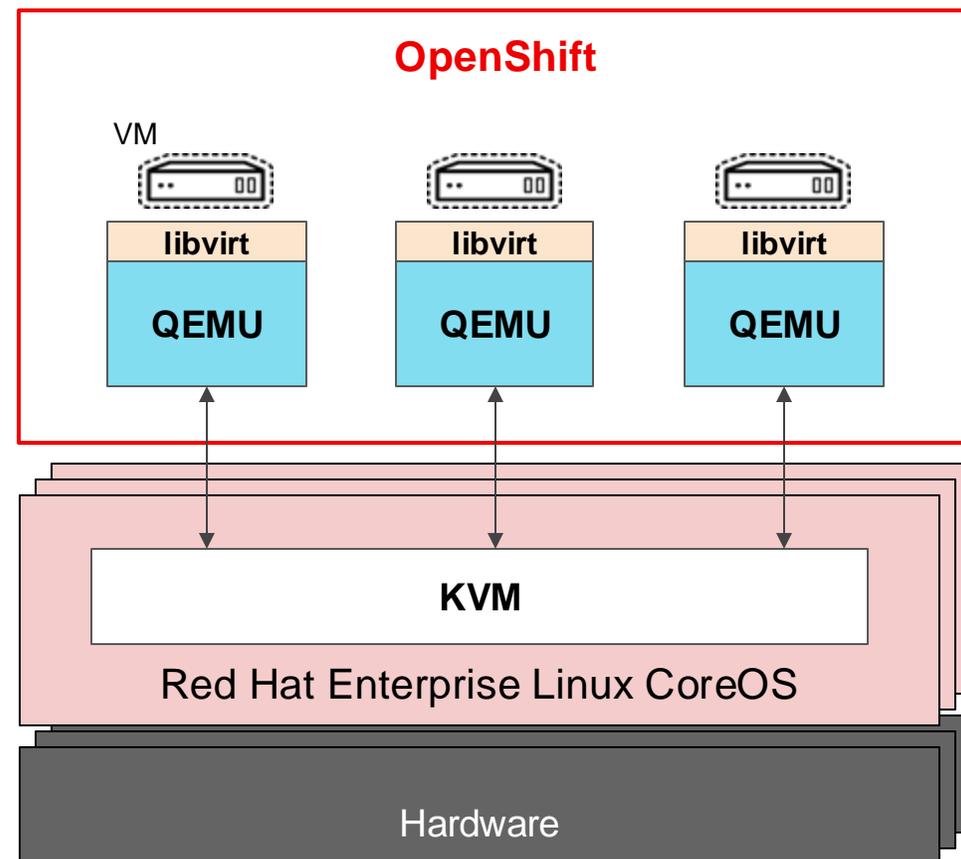
Worker Node (2~N nodes)

- スケジュールされたコンテナや VM が稼働するノード
- ワークロードの量によってノード数を決める。途中で追加することも可能
- OS は Red Hat Enterprise Linux CoreOS (RHCOS)



OpenShift Virtualization における仮想環境の実現

- **KVM = Kernel-based Virtual Machine**
 - Linux ホストをハイパーバイザーとして使えるようにする Linux カーネルモジュール
 - VM 内部の処理をホストの CPU で実行（仮想 CPU）
 - ホスト上の VM 全てで共有
- **実績豊富な KVM + QEMU + libvirt *スタック**
 - Red Hat がリリースした複数のプロダクトで実装 & 本番利用
 - Red Hat Enterprise Linux
 - Red Hat Virtualization (販売終了)
 - Red Hat OpenStack Platform
 - Red Hat OpenShift Virtualization

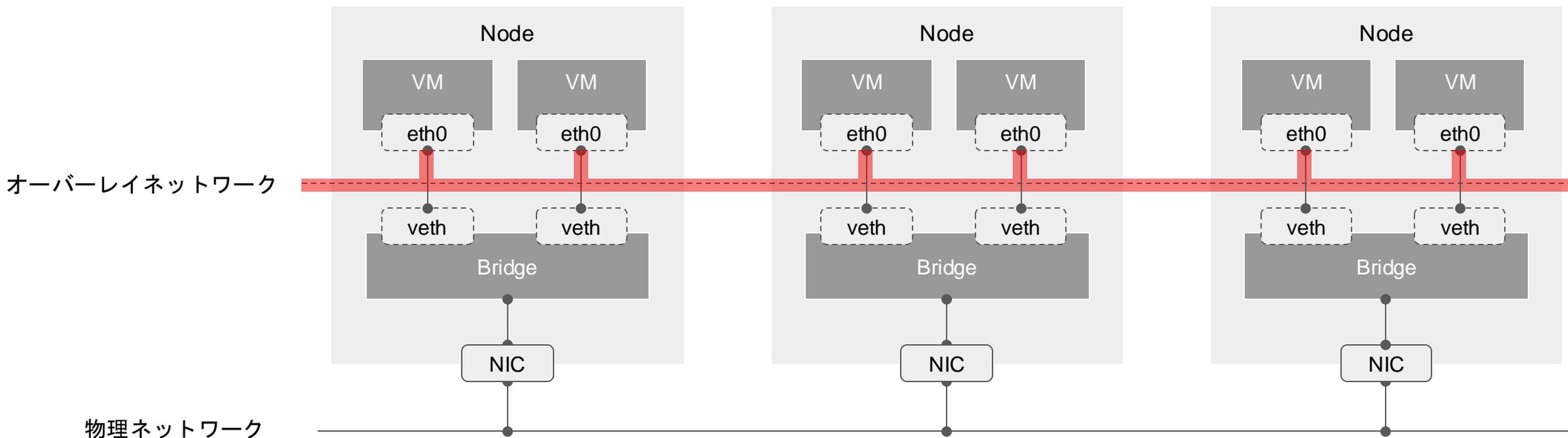


OpenShift の仮想ネットワークの仕組み

OpenShiftはLinuxの仮想ネットワークの仕組み等を応用してオーバーレイネットワークを実現しています。

また、インスタンスに複数のネットワーク・インタフェース (NIC) を持たせ複数NWに接続させる事も可能です。

オーバーレイネットワークを利用することで、ネットワークの設定や管理を効率化することが可能です。



Node内通信はL2通信

Node跨ぎはL2 over L3のトンネリングを経てVM同士の内部IPで通信

OpenShiftと従来の 企業ネットワークの課題と F5ソリューションによる解決策

Enterprise 企業が抱えるITインフラの課題

システムの増加に伴い、Enterprise企業では数多くのITインフラの課題に悩まされています。
ニーズに合わせて、柔軟なITインフラの構築が求められます。

スケーラビリティ

企業の成長や新しい拠点の追加に対応するため、ネットワークが柔軟にスケーリングできることが求められます。
従来のネットワーク構成ではスケーリングが困難になることが多いため、クラウドベースのネットワークソリューションの活用が求められます。

ネットワーク管理と監視

大規模な企業ネットワークでは、ネットワーク全体を一元的に管理・監視することが課題です。
ネットワークトラフィックの可視化、パフォーマンスの監視、異常検知が必要で、これには高度なネットワーク管理ツールや自動化が不可欠です。

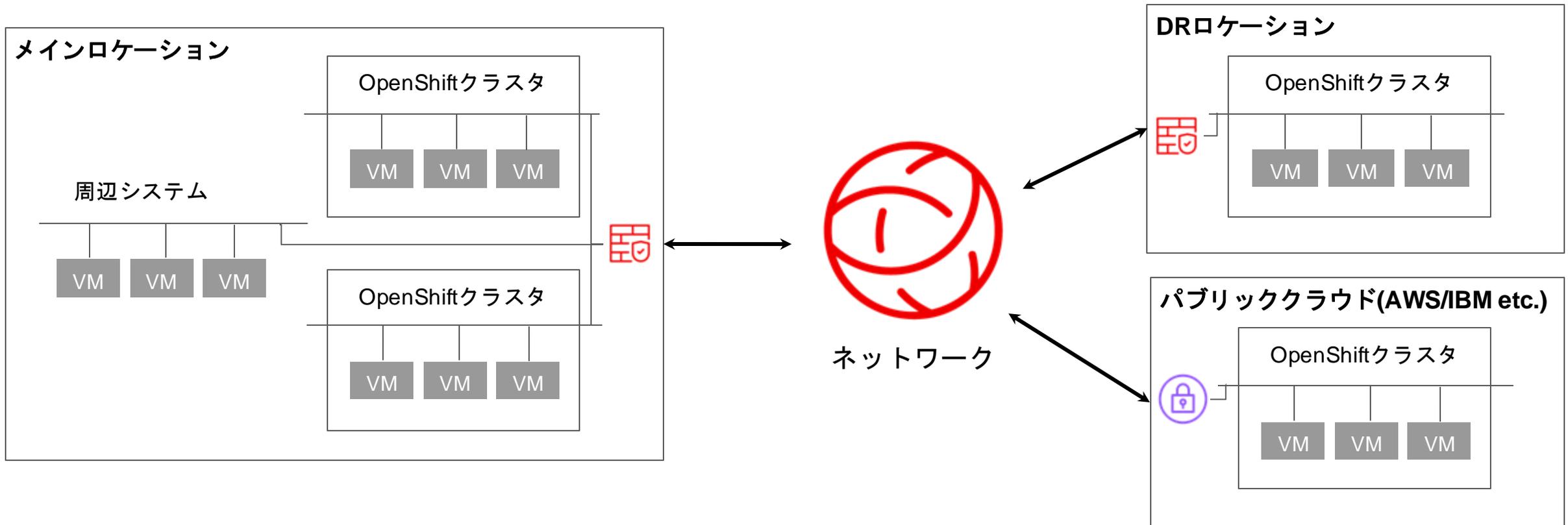
セキュリティ

サイバー攻撃の増加に伴い、企業ネットワークは常に攻撃のリスクにさらされています。
ランサムウェア、フィッシング、DDoS攻撃などからネットワークを保護するためには、強力なファイアウォール、侵入検知システム、エンドポイントセキュリティなどの対策が必要です。

OpenShift導入企業様においては、複数クラスタ、複数サイト、クラウドの活用によりITインフラ基盤の拡張とともに管理の方法についてご検討されるケースが増えています

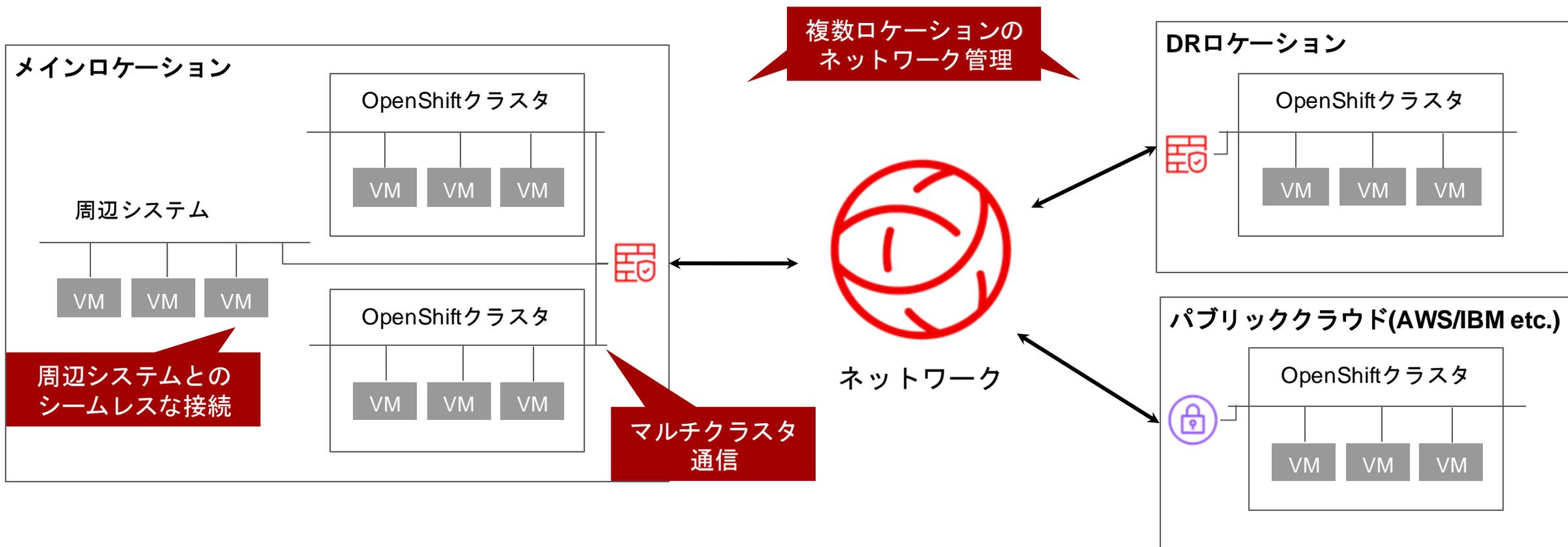
Enterprise 企業におけるオープンハイブリッドな OpenShift 環境

OpenShiftは、企業の様々なIT要件に合わせて柔軟な拡張が可能です。同一サイト内でのOpenShiftクラスタ間や周辺システムとの通信やパブリッククラウド含む複数サイト間での通信をどう効率的に自動構築・管理するかが拡張性の高い基盤を構築する上でのキーとなります。



Enterprise 企業におけるオープンハイブリッドな OpenShift 環境

OpenShiftは、企業の様々なIT要件に合わせて柔軟な拡張が可能です。同一サイト内でのOpenShiftクラスタ間や周辺システムとの通信やパブリッククラウド含む複数サイト間での通信をどう効率的に自動構築・管理するかがポイントです。



Red Hat と F5 連携ソリューション

Red HatはF5のソリューションとの連携により柔軟なネットワーク環境の設計・構築・運用が可能です。
コアデータセンターからエッジまで、様々なローケーションに存在するRed Hat環境を、F5のソリューションを利用して安全に公開することができます。

F5 BIG-IP

F5 Cloud Services

F5 Silverline

SHAPE Security

Volterra

LiLAC

wib

Heyhack

NGINX



F5 BIG-IP

ミッションクリティカルな環境におけるハードウェアおよび仮想アプライアンス

ADC/LB

Remote Access

FW

SSL可視化

WAF

DNS



F5 Distributed Cloud (XC) Services

F5のテクノロジーを統合し、包括的にF5の価値を提供するSaaS型クラウドサービス

WAF(WAAP)

Routed DDoS

API security

Bot defense

MCN

Managed k8s



F5 NGINX

Webアプリケーションのモダナイゼーションを下支えするクラウドネイティブソフトウェア

Microservice

Ingress Controller

API GW

ADC

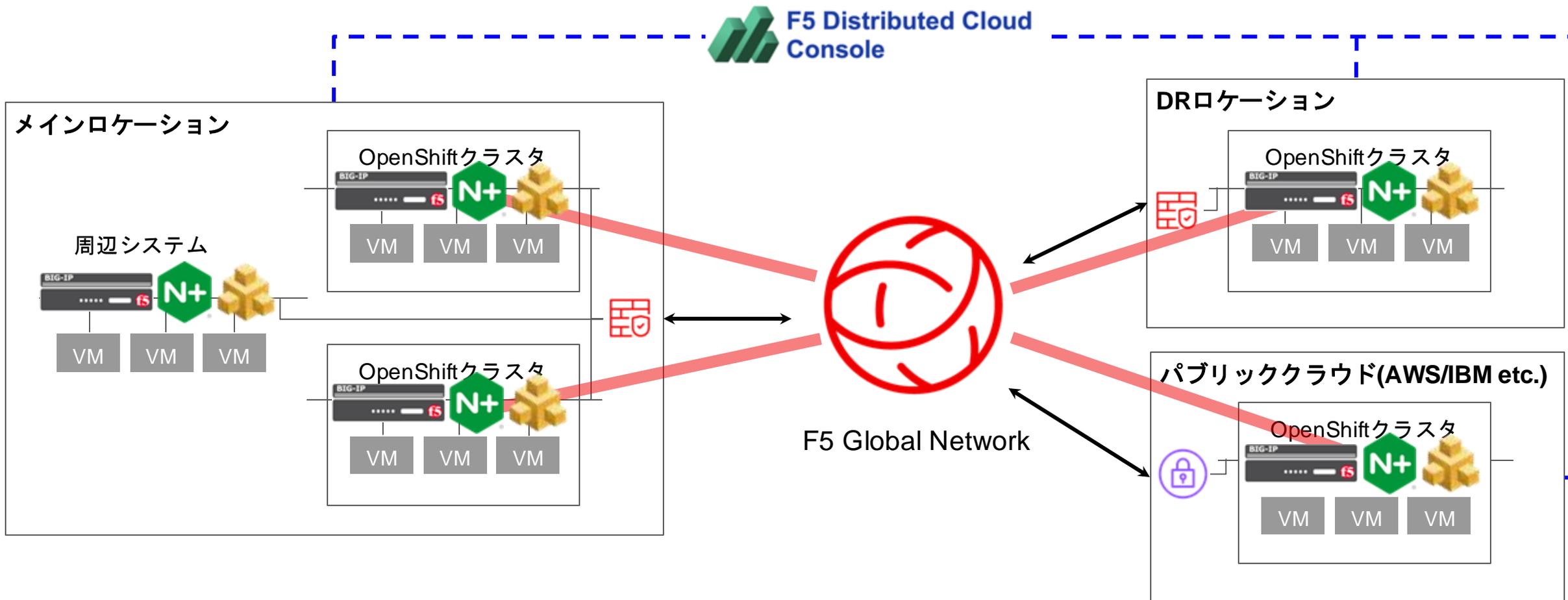
Service Mesh

Web Server



OpenShift はすべてのF5製品との連携

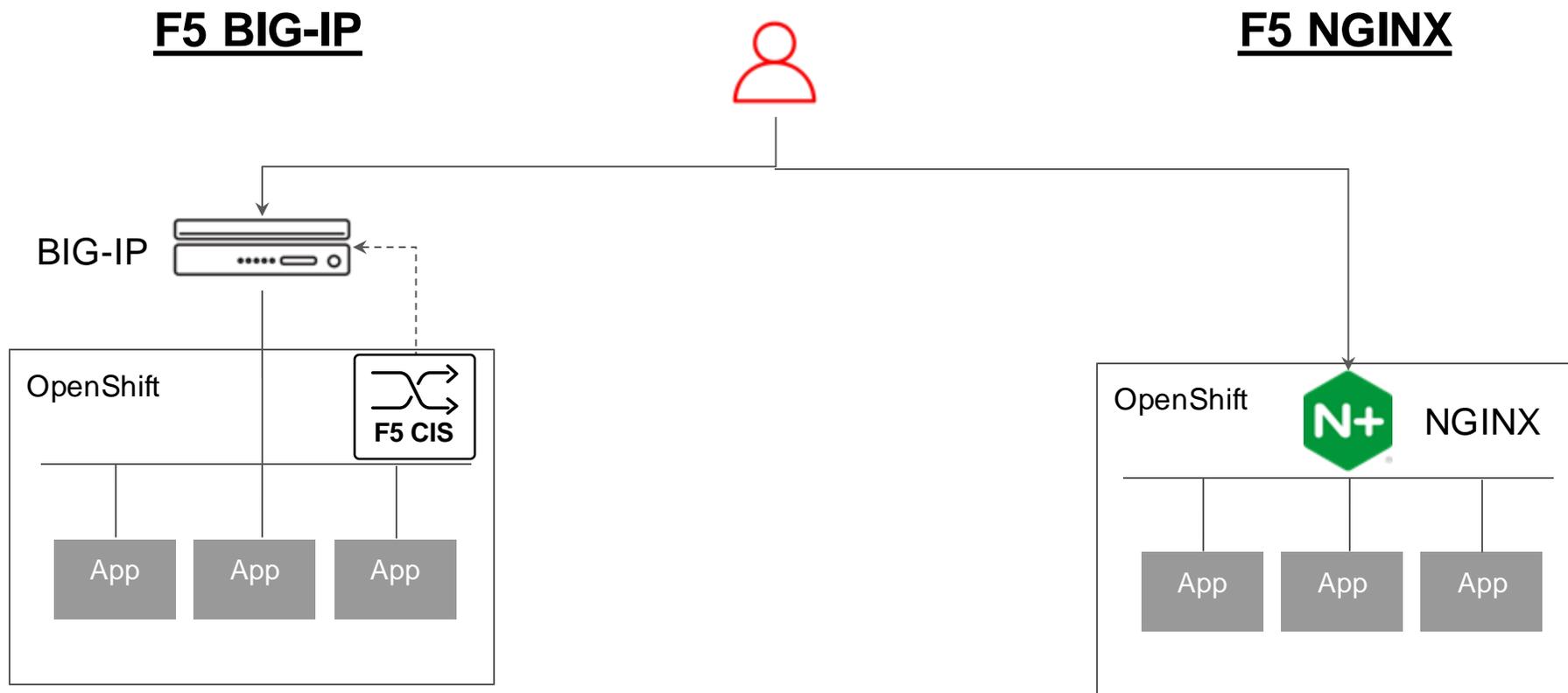
OpenShiftは、F5XC Meshだけではなく、BIG-IPやNGINXを含めたすべてのF5製品との連携を実現し お客様の要望に柔軟に対応することが可能です。



Red Hat と F5 BIG-IP / NGINX の連携

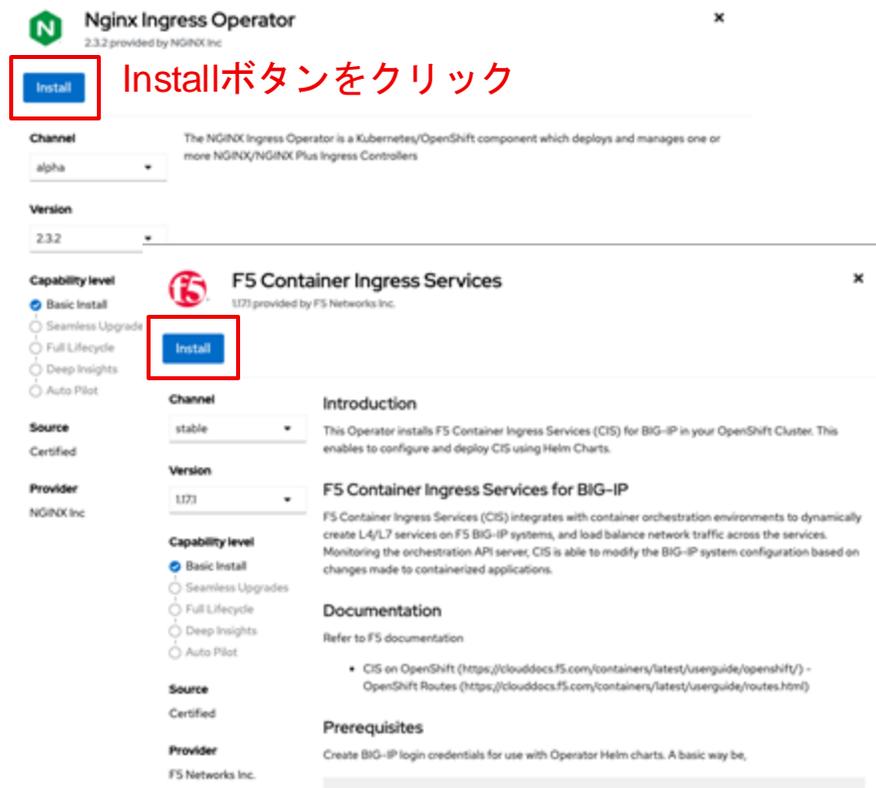
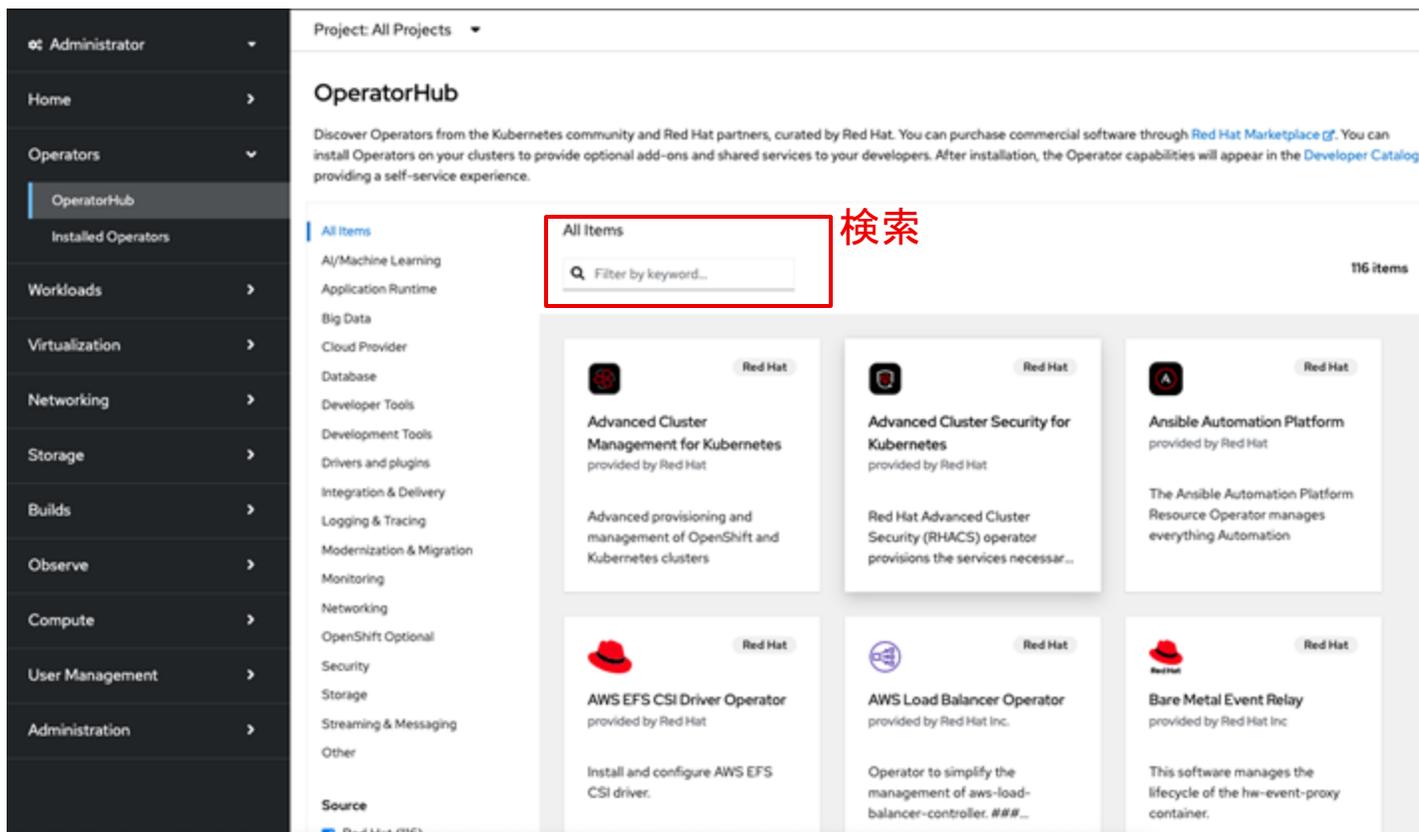
F5 BIG-IPとNGINXは、それぞれ構築や運用をサポートするOpenShift Operatorによる機能が提供されています。

F5からの提供OperatorであるF5 Container Ingress Service (CIS) やNGINX Ingress Controllerを導入すると、OpenShift上で動作するアプリケーションの拡張に合わせて動的に連携し、各種設定の効率化が可能です。

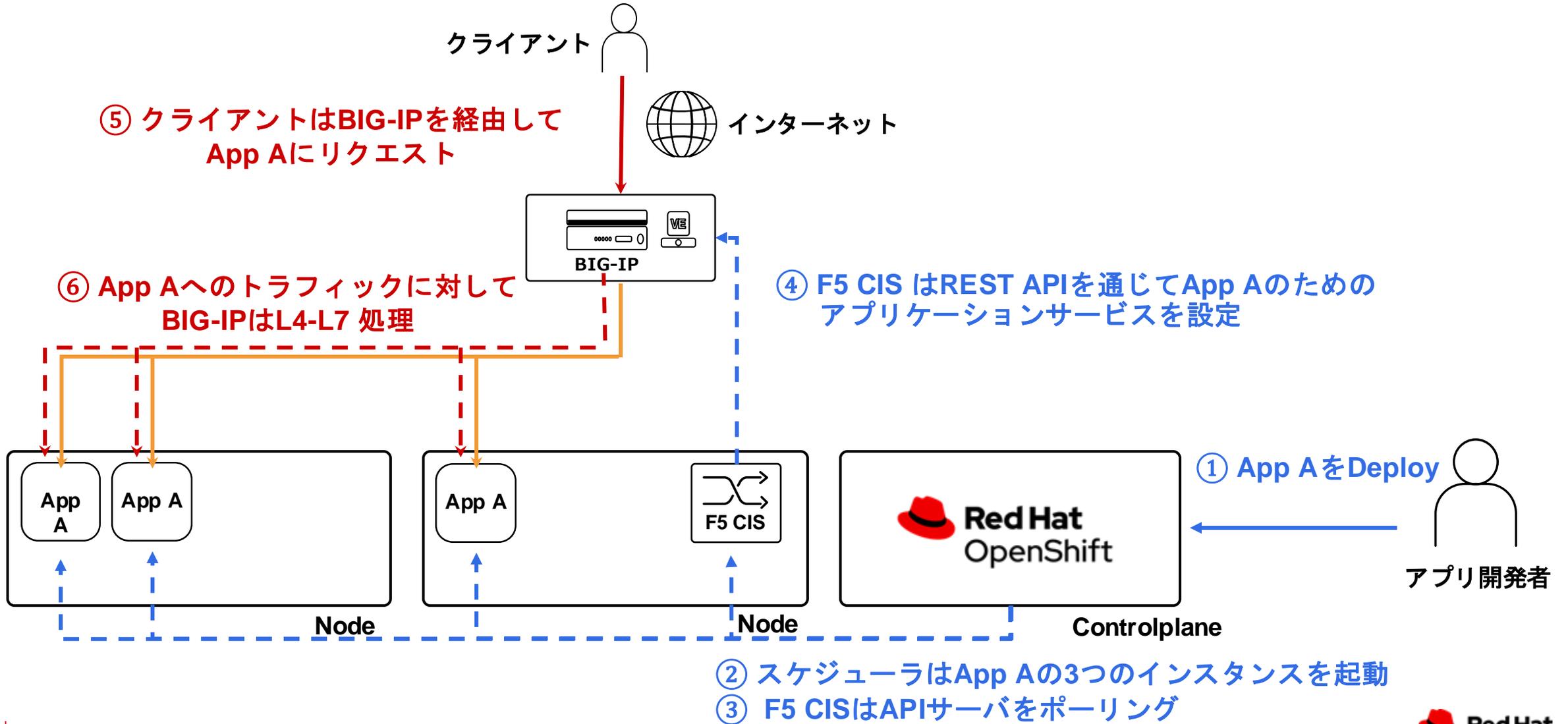


F5 ソリューションの OpenShift Operator インストール

OpenShiftはOperatorを利用することによって、各ミドルウェアのインストール、設定、監視、アップグレードなどの運用操作を自動化できます。OpenShiftクラスタ上にあるOperatorHubから、F5社のOperatorを簡単にインストール可能です。



F5 Container Ingress Service 概要



OpenShift と F5 Distributed Cloud Service の連携

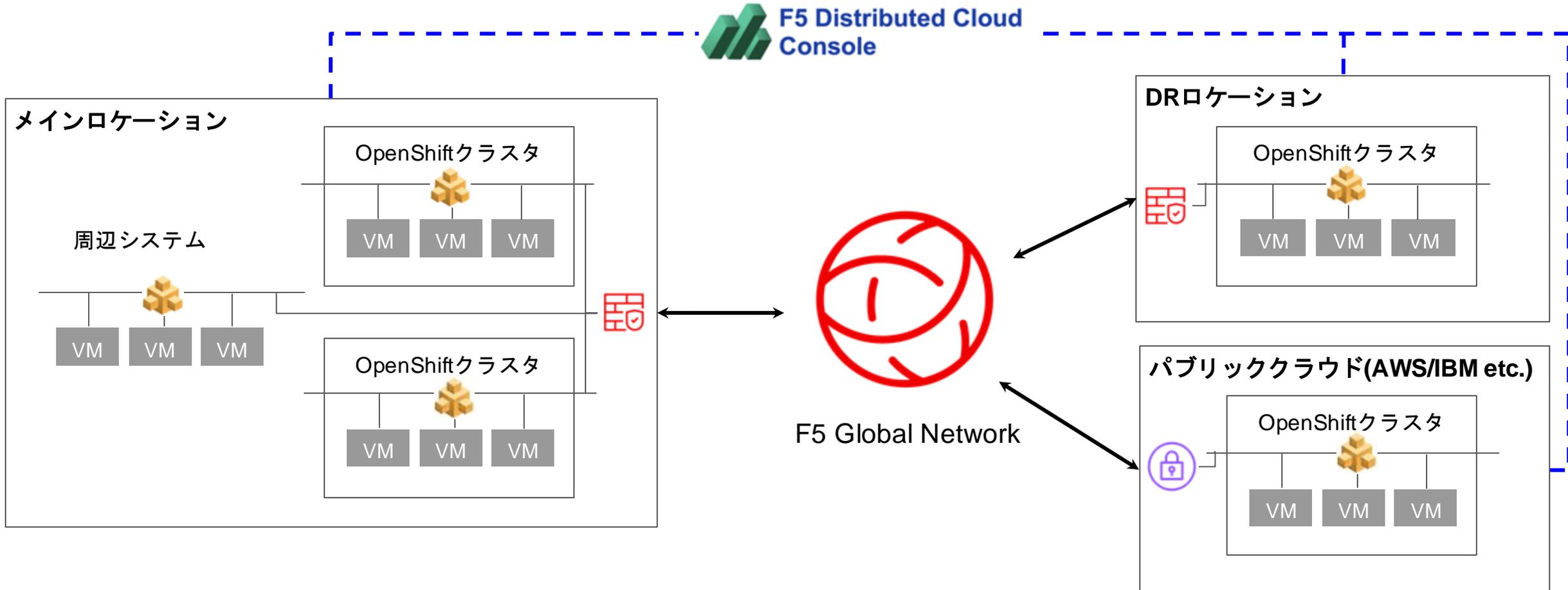
OpenShiftのとF5 Distributed Cloud (XC) Service のソリューションを組み合わせると、ネットワーク環境の効率的な運用を実現することが可能です。

メリット

- 複数ロケーションに存在するF5XC MeshのCE (Customer Edge) の一元管理やネットワーク可視化
- OpenShiftとF5 XC Meshによるネットワークセグメンテーションの効率化
周辺システムのVLANネットワークとの接続
- 複数ロケーションにおける OpenShift マルチクラスタ間通信の一元管理と可視化
- インターネット公開エンドポイントの一元化と API を含むセキュリティ機能の実装

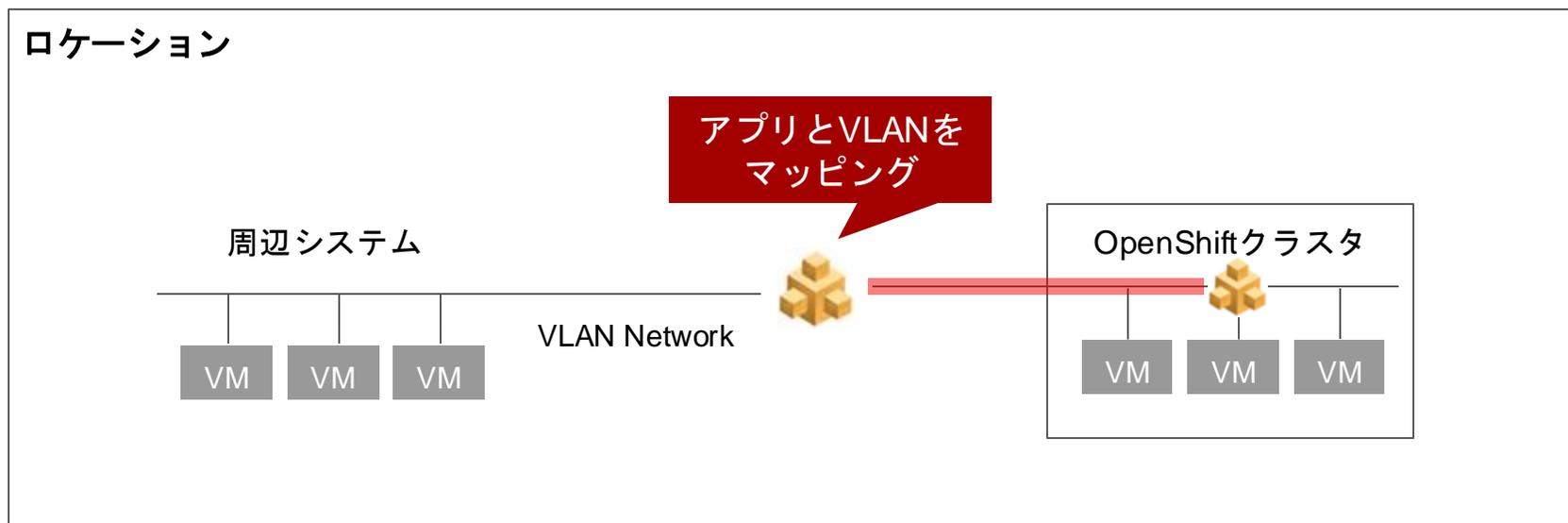
OpenShift と F5 XC Mesh による設定の一元管理やネットワーク可視化

複数ロケーションに構築されているOpenShiftにF5 XC MeshのCustomer Edgeを展開し、クラウドコンソール側で管理することが可能です。F5 XC Meshは、ロードバランサーとしても活用することが可能です。



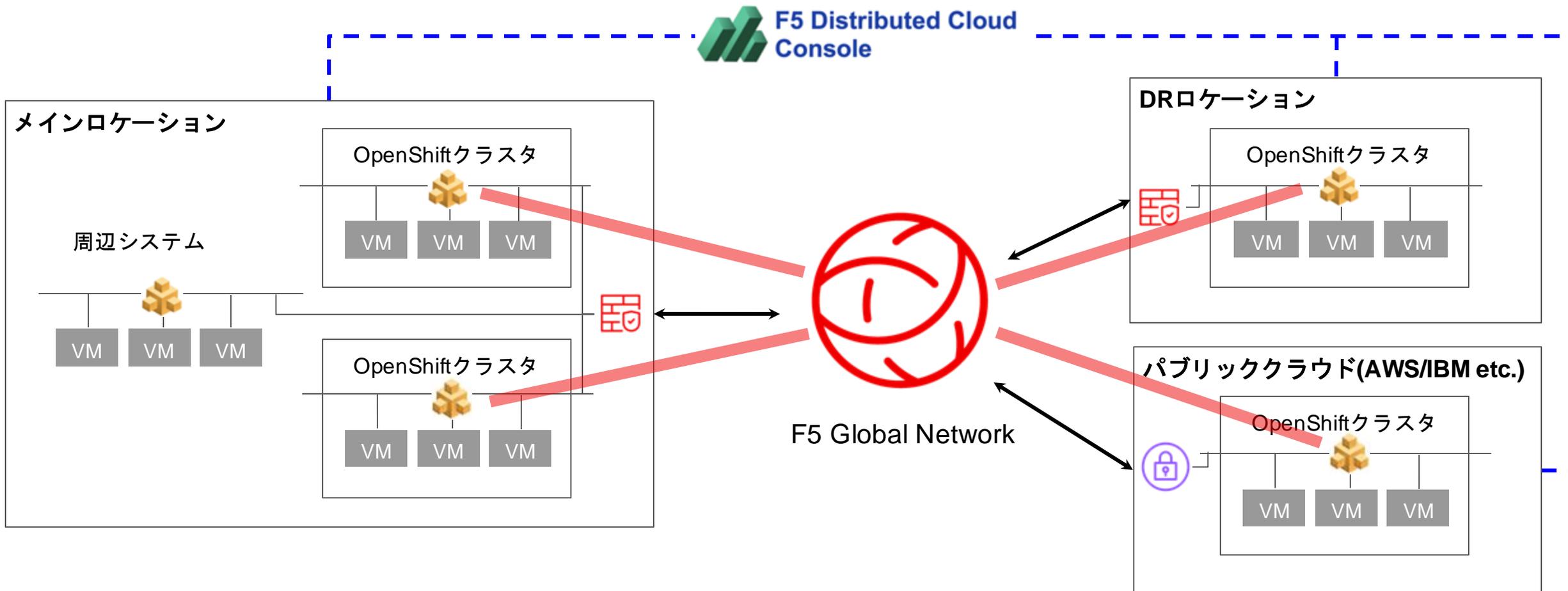
OpenShift と F5 XC Mesh によるネットワークセグメンテーションの効率化

F5 XC Meshを利用することで、OpenShiftのオーバーレイネットワーク上のアプリケーションと周辺システムが存在するVLANで区切られたネットワークをマッピングし、ネットワークセグメンテーションを効率的に実装することが可能です。



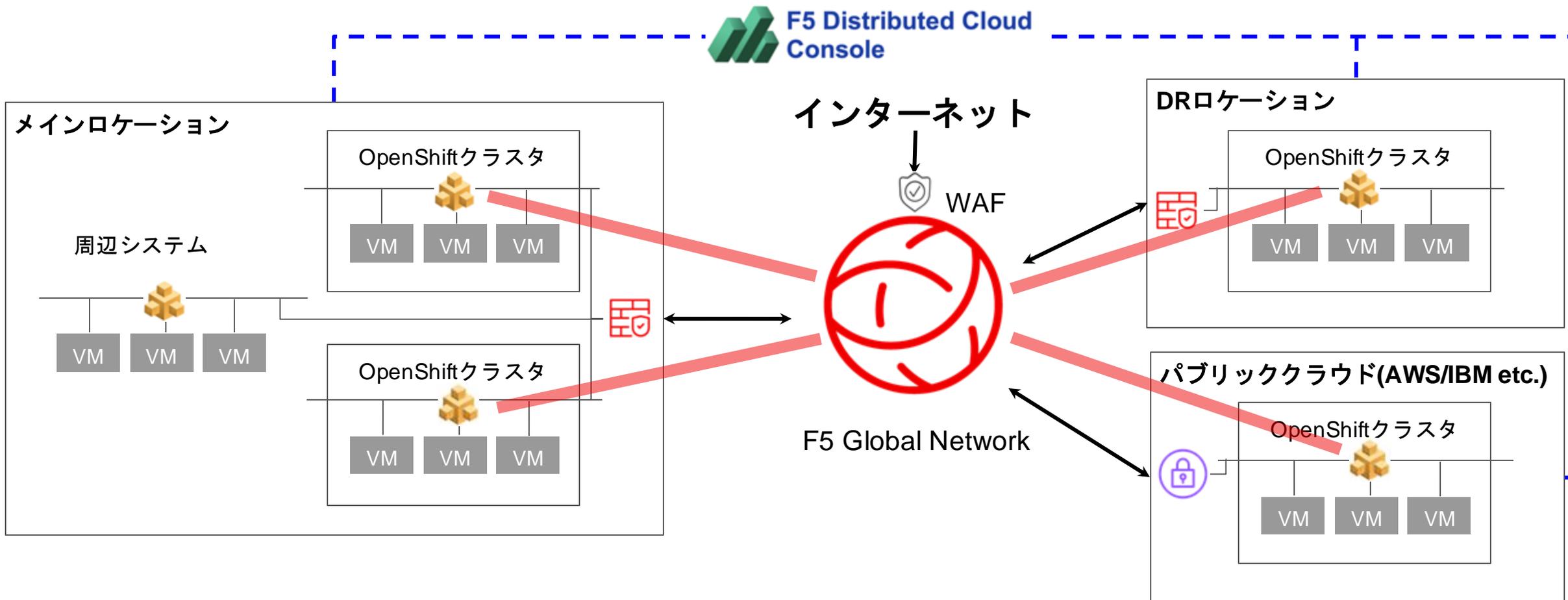
複数ロケーションにおける OpenShift マルチクラスター間通信の一元管理と可視化

複数ロケーションに構築されているOpenShiftにF5 XC MeshのCustomer Edgeを展開することで、IPアドレスの重複を気にすることなく複数ロケーション間で暗号化ネットワークを確立することが可能です。



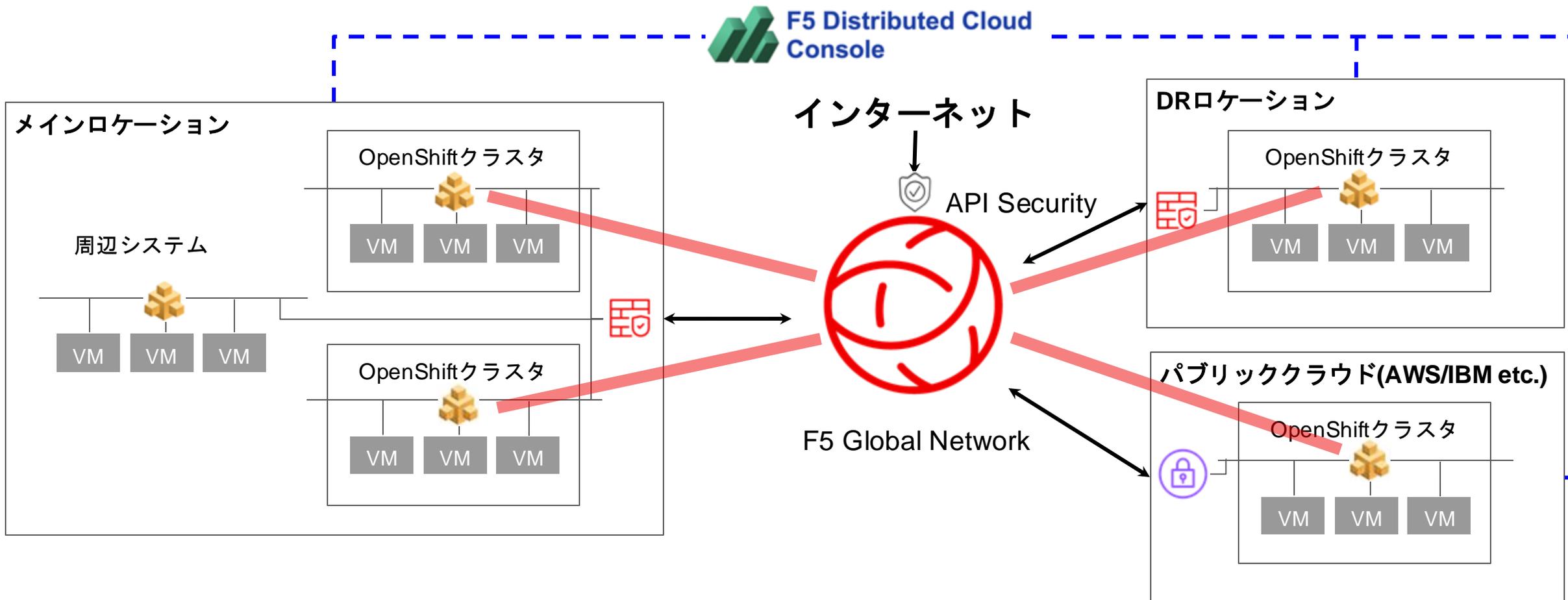
OpenShift サービスのインターネットへの公開

OpenShift上で構築されたアプリケーションをF5 Global Networkを介してインターネットに公開できます。インターネットからの通信を集約し、WAF/DDoS/Bot対策などセキュリティ関連の取り組みを一元化できます。



OpenShift 上のアプリケーションの API セキュリティ

OpenShiftは、Red Hatが提供するOpenAPI互換のAPIマネジメント製品やNGINXと組み合わせてAPIエンドポイントが提供されるケースが増えています。F5 XC API Securityにより、APIエンドポイントの可視化と保護の一元化が可能です。



まとめ

- **OpenShift Virtualization 概要**

- OpenShiftに標準機能として提供されている仮想マシンを起動・管理できる機能。仮想化基盤に必要な機能が搭載
- OpenShiftの利用料の中にRHEL VMの費用が含まれており、ハードのスペックが許す限りRHELを自由に増やすことが可能

- **OpenShift Virtualization 技術要素**

- OpenShift Virtualization における仮想環境の実現には、多数の実績があるKVMが活用
- OpenShiftの機能で、ネットワーク設定や管理が容易なオーバーレイネットワークを実現

- **OpenShiftと従来の企業ネットワークの課題とF5ソリューションによる解決策**

- BIG-IP / NGINXとOpenShift Operatorで提供されるソリューションの連携
- F5 XCによる複数ロケーションのF5 CE (Customer Edge) の一元管理やネットワーク可視化
- F5 Global Networkを活用したインターネットへのエンドポイントの公開とセキュリティ対策

