



これからはじめる Azure Red Hat OpenShift (ARO)

Red Hat K.K. Technical Sales
Hirofumi Kojima
2022.10

Agenda

- コンテナはなぜ使われるのか？
- コンテナ利用に必要なもの
- コンテナはどのように使われるのか？
- なぜKubernetesが必要なのか？
- Red Hat OpenShiftの主な機能
- Managed OpenShift Service (OpenShift クラウドサービス)
- Azure Red Hat OpenShift (ARO) の概要
- Azure Red Hat OpenShift (ARO) のサービス仕様

コンテナはなぜ使われるのか？

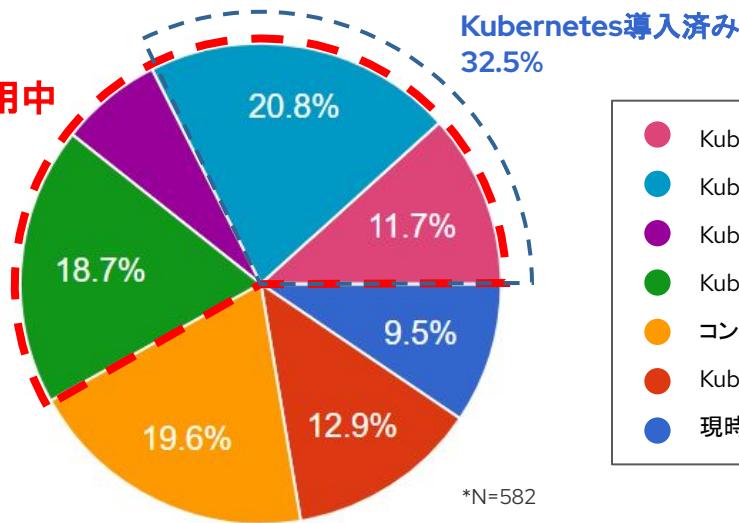
多くの企業で利用が進むコンテナ

半数を超える企業でコンテナが使用され、
約1/3はKubernetes(コンテナ基盤ソフトウェア)を使用しています。

あなたの企業(もしくは支援先企業)ではKubernetesを利用していますか?

※Kubernetesのプロダクトは問いません。

コンテナ使用中
58.0%



- Kubernetesの本番利用を行っている
- Kubernetesの検証、導入構築を行っている
- Kubernetesの利用を計画/検討している
- Kubernetesに関する情報収集は行っている
- コンテナ(Dockerなど)は使用/検討中だがKubernetesはこれから
- Kubernetes/コンテナに関してはよく知らない
- 現時点では使うことは考えていない

なぜコンテナを使うのか

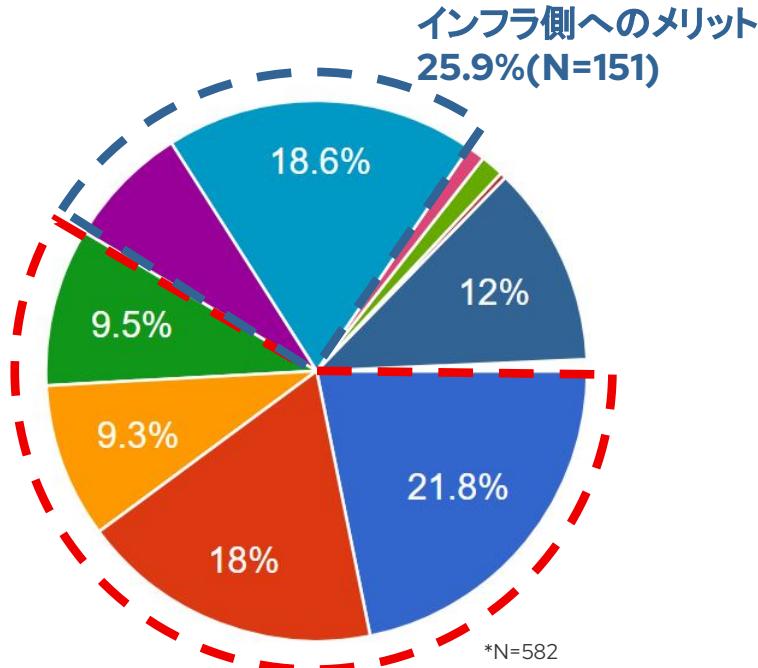
コンテナをうまく使うことで、**ビジネスメリット**を得られるから

コンテナ導入の期待値

既存システムと比べ、コンテナ(Kubernetes)導入に期待する一番のビジネスメリットはなんですか？

アプリ側へのメリット
58.5%(N=341)

- 開発生産性の向上
- 運用の効率化
- ...

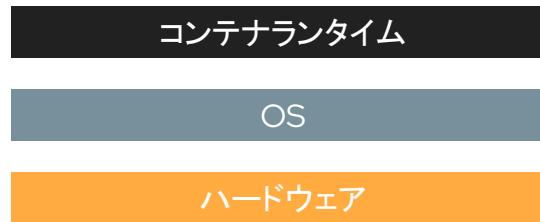
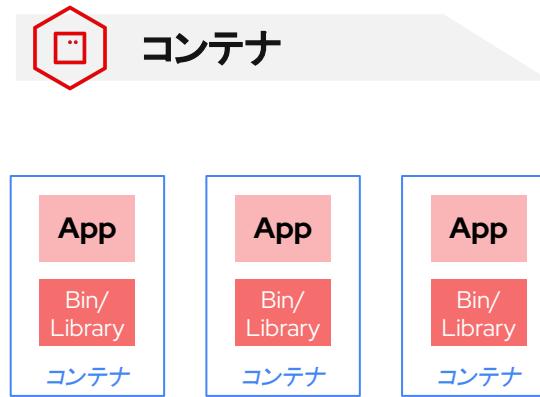
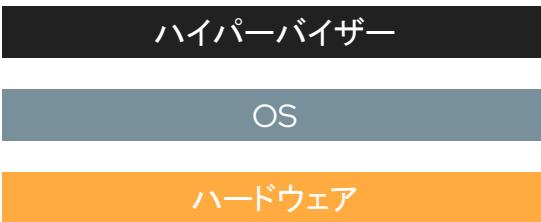


- アプリケーション開発の生産性向上、アジリティ向上
- アプリケーション運用の効率化、コスト削減
- アプリケーションリリースサイクルのスピード向上
- アプリケーションのポータビリティ(可搬性)
- インフラリソースの集約率向上、コスト削減
- インフラリソース管理の運用自動化、プロセス改善
- SoE(IoTやAI、機械学習など)の促進
- SoRのアプリケーションモダナイゼーション
- SoRのデータ利活用/マイグレーション
- まだよくわからない

コンテナとは一言で言えば何か？

アプリケーション本体と、
アプリケーションの実行に必要なライブラリ・依存関係など、
必要最小限の要素をひとつにパッケージした姿

コンテナと仮想マシンの違い



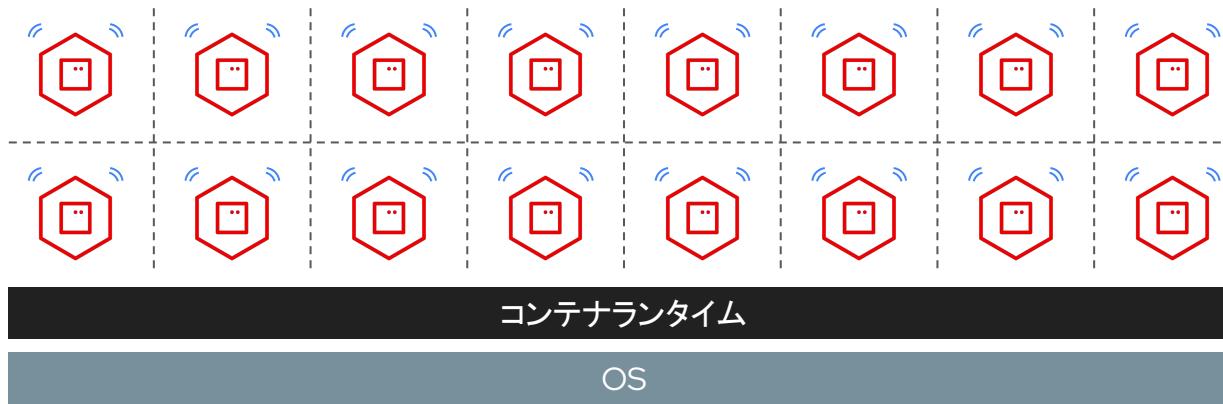
コンテナの特徴

▶ OS上で稼働

- カーネルが持つ機能を利用する。
- 1つのホストの上で複数のコンテナを同時に稼働できる。

▶ 隔離性

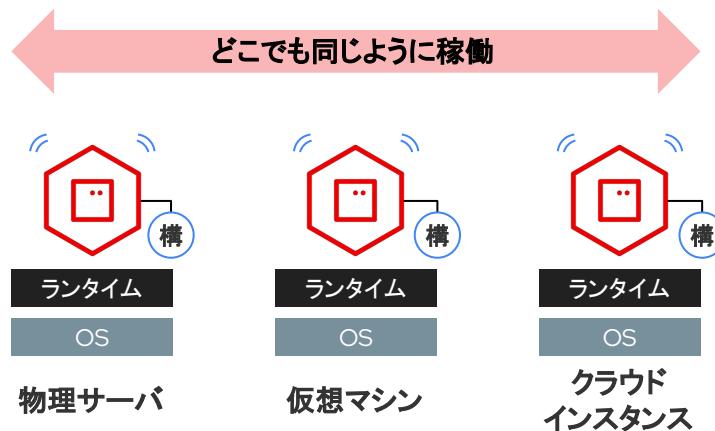
- ホストのカーネルを共有するが、コンテナ同士は隔離され互いに競合しない。
 - コンテナ同士で通信可能にはできる。



コンテナの特徴

▶ 可搬性 (Portable)

- どの環境でも同じように稼働する。
 - 環境に依存する構成情報はコンテナとは別で持つ。



▶ 軽量

- OSが無く、必要最小限の要素のみ持つ。

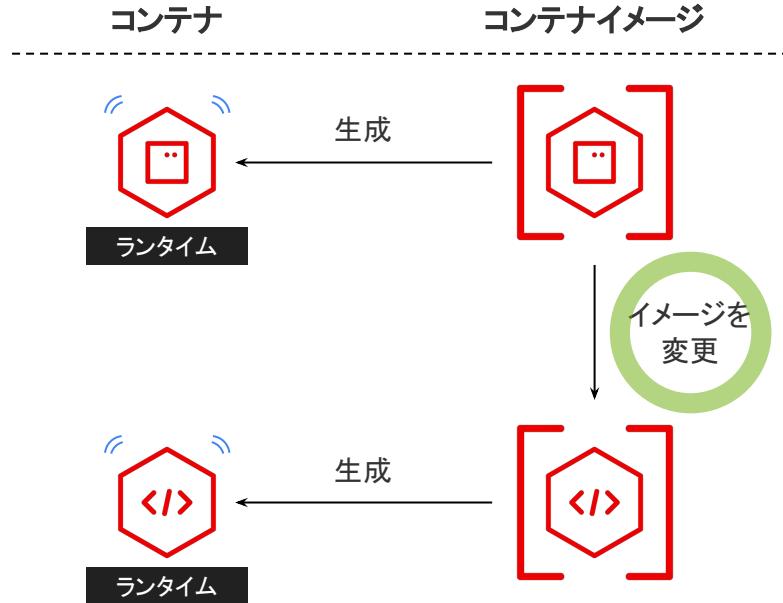
▶ 起動が高速

- OS起動時間を省略できる。

| | 仮想マシン | コンテナ |
|------|------------|---------------|
| 容量 | 1桁 ~ 2桁 GB | 2桁 MB ~ 1桁 GB |
| 起動時間 | 数分 | 数秒 |

コンテナの特徴

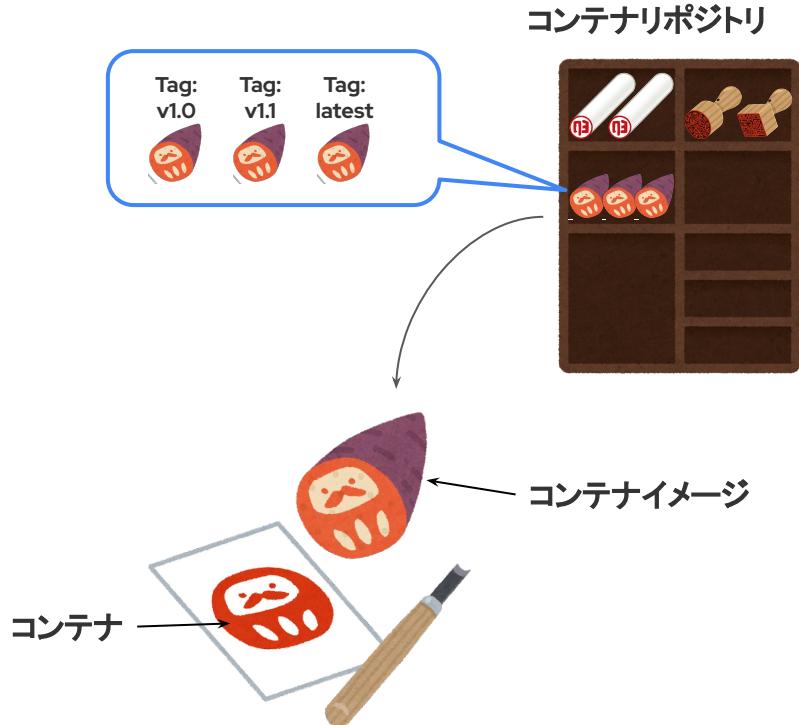
- ▶ **イメージから生成**
 - コンテナイメージから複製して作られる。
- ▶ **不变性 (Immutable)**
 - 同じコンテナイメージから起動したコンテナは、毎回必ず同じものとなる。
- ▶ **揮発性 (Ephemeral)**
 - コンテナに加えた変更は、コンテナが停止すると失われる。
 - コンテナ自身に永続性は無い。
 - コンテナに変更を加えたい場合は、コンテナイメージを変更して新しくコンテナを起動する。
 - 古いコンテナは破棄する。



コンテナを使うために 必要なもの

コンテナイメージ

- ▶ **コンテナの素**
 - あらゆるコンテナはイメージから作られる。
- ▶ **コンテナリポジトリで管理**
 - 同じイメージは系列立てて管理される。
 - それぞれのイメージはタグで区別される。
- ▶ **利用できるイメージ**
 - パブリックなイメージ
 - Web上で公開されている。
 - プライベートなイメージ
 - ユーザーが独自に作る。
- ▶ **イメージの作り方(イメージのビルト)**
 - 既存イメージに追加変更を加えてビルトする。
- ▶ **セキュリティには要注意**
 - 特にパブリックなイメージは「信頼できる提供元のイメージか」「脆弱性は無いか」など注意すること。



コンテナレジストリ

▶ コンテナイメージの保管場所

- コンテナイメージはレジストリで保管され、共有される。
 - コンテナレジストリからイメージをダウンロードすることを “Pull” と呼ぶ。
 - コンテナレジストリにイメージをアップロードすることを “Push” と呼ぶ。

▶ 使用できるコンテナレジストリ

- パブリックなレジストリ
 - [Docker Hub](#) や [Quay.io](#) など、Web上で公開されたレジストリ。
- プライベートなレジストリ
 - イメージを非公開にするため、独自に構築したり、クラウドのサービスを使うなどして準備する。

コンテナレジストリ



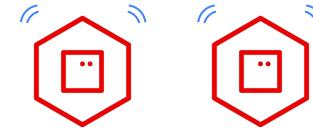
コンテナランタイム

- ▶ **コンテナが稼働するために必要なソフトウェア**
 - コンテナの作成・実行・停止・削除などのライフサイクルの管理をする。
 - ランタイムがなければコンテナは動かない。

▶ 有名なランタイム

- ローカル環境で使うとき
 - [Docker](#) (RHEL7で採用)
 - [Podman](#) (RHEL8, 9で採用)
- コンテナ基盤(Kubernetesなど)で使うとき
 - [cri-o](#) (Red Hat OpenShiftで採用)
 - [containerd](#)

※ ランタイムの役割や機能はおおむね同じだが、思想・内部アーキテクチャは変わるため微妙な違いはある。



ランタイム

ランタイムの役割

- コンテナのライフサイクル管理
 - ハードウェアリソースの分離
 - モニタリング・ロギング
 - コンテナイメージのPull・管理
 - コンテナイメージのビルド・Push
- ...etc

コンテナは
どのように使われるのか？

アプリケーション開発現場でのコンテナのうまい使いかた

▶ アプリケーション本番稼働の問題

○ 環境への依存

- 微妙な環境の違いによって、開発環境とステージング・本番環境で挙動が違うなどの問題が起こりえる。

○ システム基盤への依存

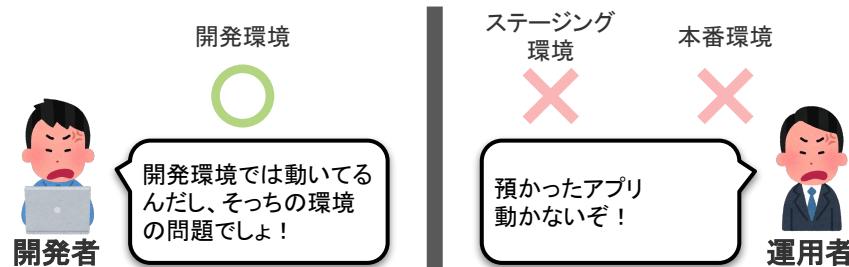
- 別の基盤(例えばオンプレミスからクラウド)へのアプリケーション移行が難しい。

▶ コンテナを使うことによる解決

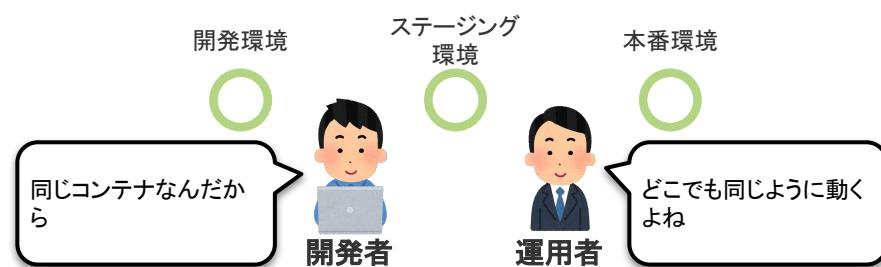
○ 環境やシステム基盤への依存を極小化

- コンテナは基盤への依存性が低いため、環境ごとに挙動が違うことを防ぐことができる。
- 基盤ごとの違いはコンテナ自体とは別で吸収できるため、アプリケーションの移行が比較的容易である。

コンテナ化されていないアプリケーション



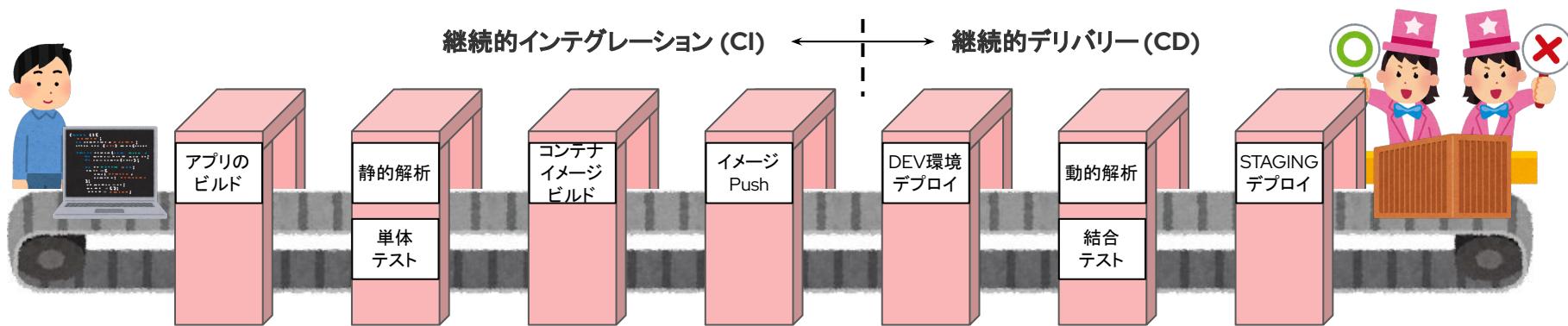
コンテナ化されたアプリケーション



開発～デリバリーまでのコンテナのうまい使いかた

▶ 継続的インテグレーションと継続的デリバリー(CI/CD)

- アプリケーションのビルドからコンテナのビルド、デプロイまでを自動的に行うようとする。
 - 途中で行うコードの解析やテストなども自動化する。
 - CI/CD用のソフトウェアを利用して、“パイプライン”を構成する
- 人の作業を「アプリケーションのソースコードの投入」と「デプロイの承認」など最小限にして極力自動化することで、アプリケーションデリバリーまでの作業品質を均一化する。



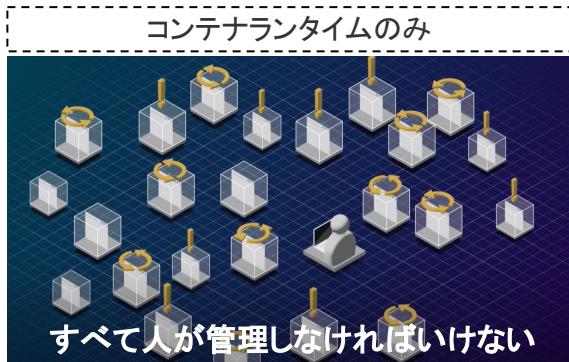
なぜKubernetesが必要なのか？

実稼働するシステムでコンテナを使うために

コンテナオーケストレータ = Kubernetes を使う

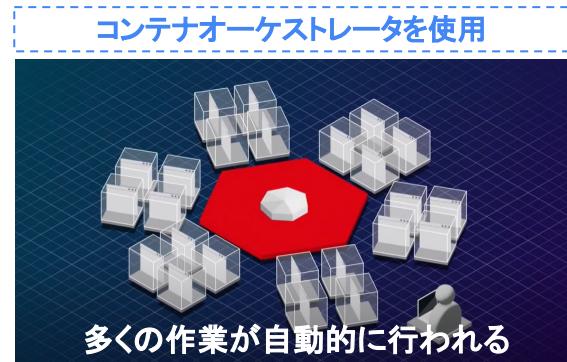
コンテナオーケストレータはコンテナの管理・運用を自動化し、ランタイムだけでは足りないシステムの可用性や運用性を提供します。

▶ コンテナの管理・運用を自動化



【人が行う作業】

- 属人的な障害復旧オペレーション
- 手動によるコンテナ変更作業
- アプリケーションごとの設定管理
- 定期的な監視作業



【人が行う作業】

- ビジネス変化に応じた適切なリソース調整

様々なクラウドでのコンテナアプリの実行

クラウドプロバイダごとに異なる実装やサービスの詳細を知る必要がなく、
コンテナアプリの実行状態を記述して、宣言的に実行できます。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment # デプロイの名前
spec:
  replicas: 3 # レプリカ数 (Podの数)
  template: # 作成される Pod のテンプレート
    metadata:
      labels: # Pod 管理に利用されるラベル
        app: nginx
    spec:
      containers:
        - name: nginx
          image: nginx:1.14.2
          ports: # 利用するポート番号
            - containerPort: 80
```

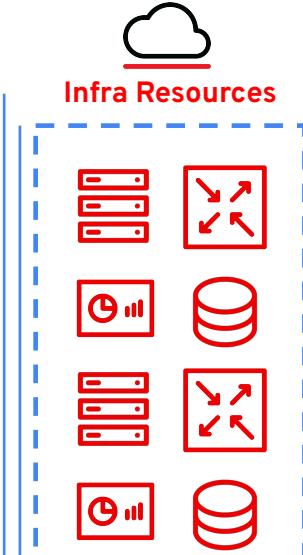
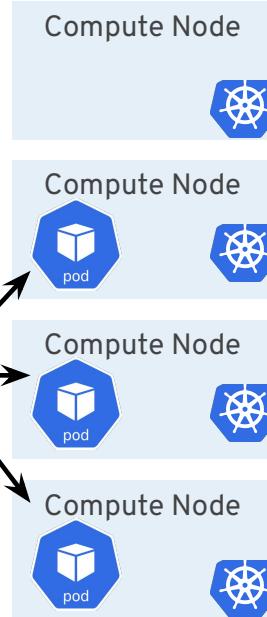
※ Pod: Kubernetes 上でのコンテナアプリの実行単位。

コンテナや、コンテナが利用する外部ストレージの設定などをまとめたもの。
基本的には、1 Pod = 1 コンテナアプリ、を想定。



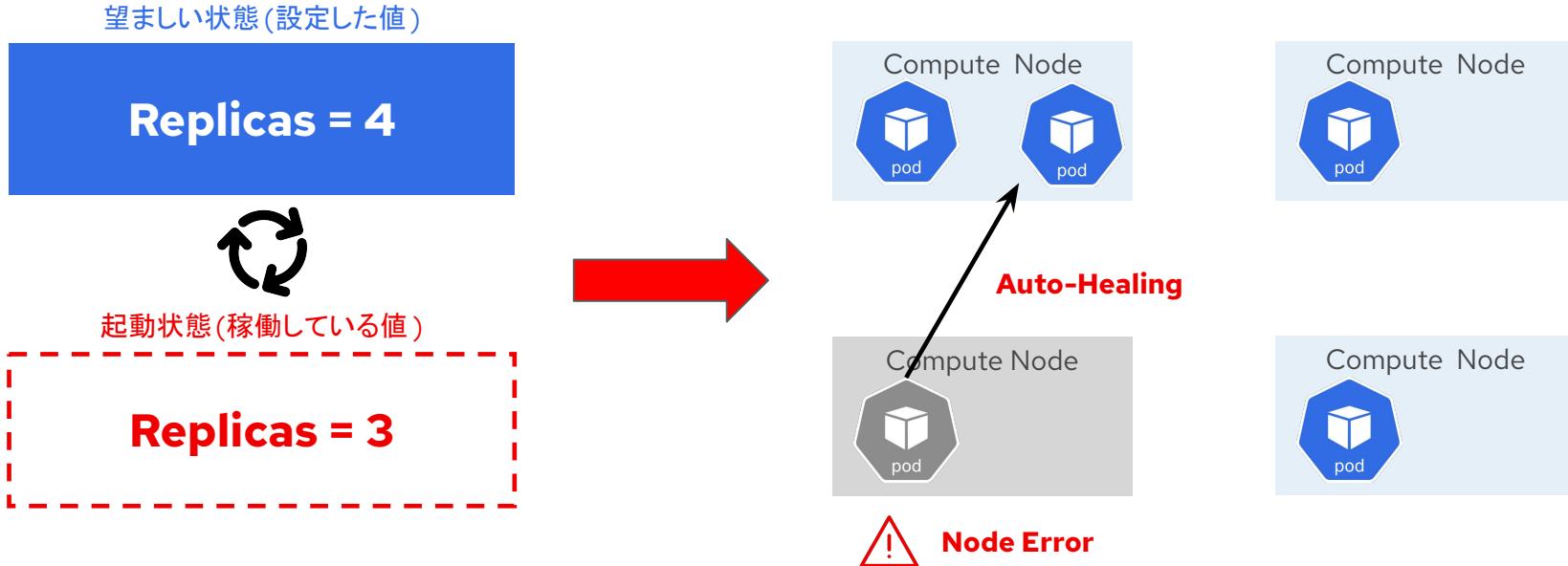
kubernetes

Deploy



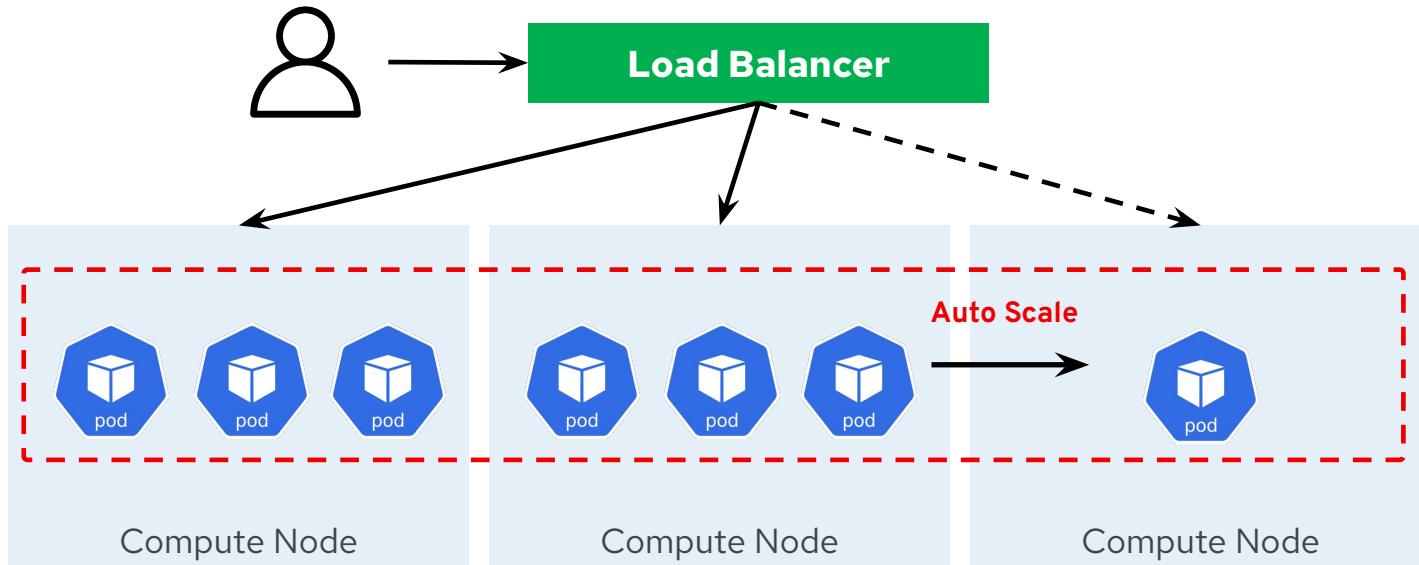
コンテナアプリの冗長性の担保 (セルフヒーリング)

Kubernetesは、現在のアプリケーションが望ましい状態に一致するように動作します。



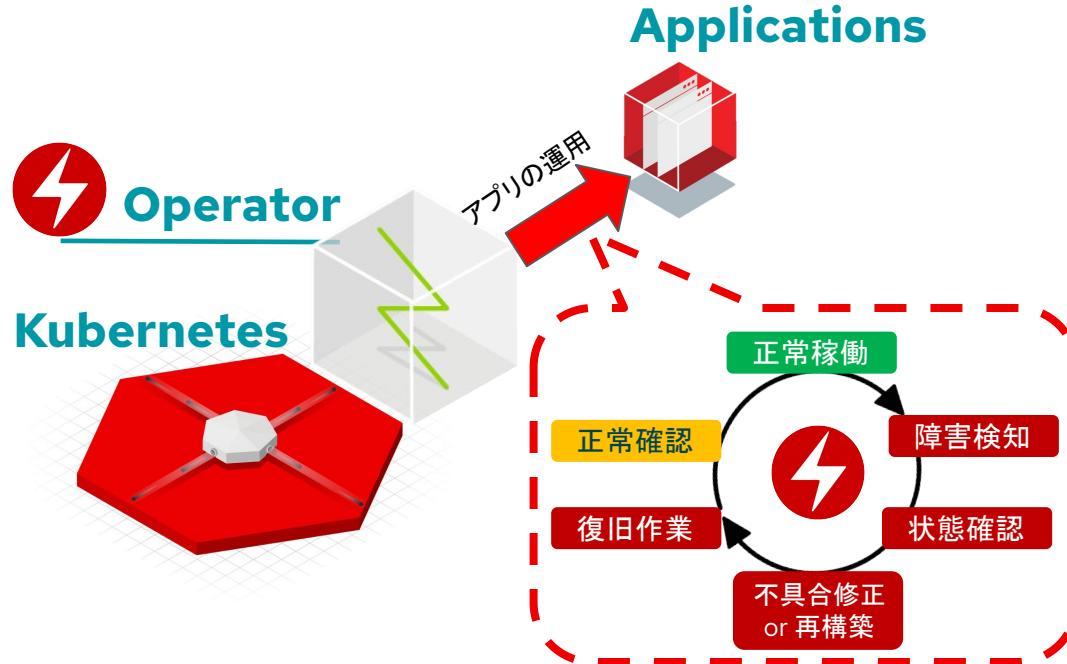
負荷状況に応じた動的なスケールアウト(オートスケーリング)

負荷状況に応じたスケールアウトや、不要なリソースの縮退を、動的に実行できます。



Operator(運用専用コンテナ)で、コンテナアプリの運用自動化

運用の知見やマニュアルをコード化し、ステートフルアプリケーションの運用を自動化



- アプリ運用のマニュアルをコード化及びパッケージングして、アプリの **運用専用コンテナ** として実行
- アプリ運用に必要となる、下記のような作業を自動的に実行
 - インストール
 - コンフィグデプロイ
 - アップデート
 - リソーススケーリング
 - バックアップ、リカバリー
 - モニタリング
 - ロギング
- アプリを利用したシステム構築や、障害復旧などの自動化を支援
- Operatorの開発フレームワークも提供

Kubernetesだけではできないこと

Kubernetesはコンテナの管理、運用に役立つ機能を提供しますが、それ単体だけではできないこともあります。コンテナのビルドやミドルウェアの管理には、Kubernetes以外のツールの連携が必要です。

Kubernetesでは提供されない機能

コンテナの動的
ビルド/デプロイ

ミドルウェア
の管理

クラスタの
ロギングや監視

コンテナの
セキュリティ

クラスタ
アップグレード



kubernetes



Bare metal



Virtual



Private cloud



Public cloud



Edge

Red Hat OpenShift

エンタープライズに求められる機能を Kubernetes に付随し、サポートすることで、ビジネス価値に直結する機能を提供しています。**アプリケーション開発の効率化に重きを置く点** が、インフラ運用の効率化に取り組むことを目的とした Kubernetes 単体利用と大きく異なる点です。



コンテナの動的
ビルド/デプロイ

ミドルウェア
の管理

クラスタの
ロギングや監視

コンテナの
セキュリティ

クラスタ
アップグレード



kubernetes



Bare metal



Virtual



Private cloud



Public cloud



Edge

Red Hat OpenShift の主な機能

OpenShiftで提供されるセルフ開発の利用例

Gitリポジトリのソースコードを利用して、OpenShift環境にNode.jsアプリをデプロイ

1

コンテナの動的
ビルド/デプロイ

Import from git

Git

Git Repo URL *

<https://github.com/jankleinert/concession-kiosk-backend>

› Show Advanced Git Options

Builder

Builder Image *



Builder Image Version *

IST 10

開発者は自身がアプリ開発に利用している
GitリポジトリのURLを指定

Node.jsのバージョンを選択

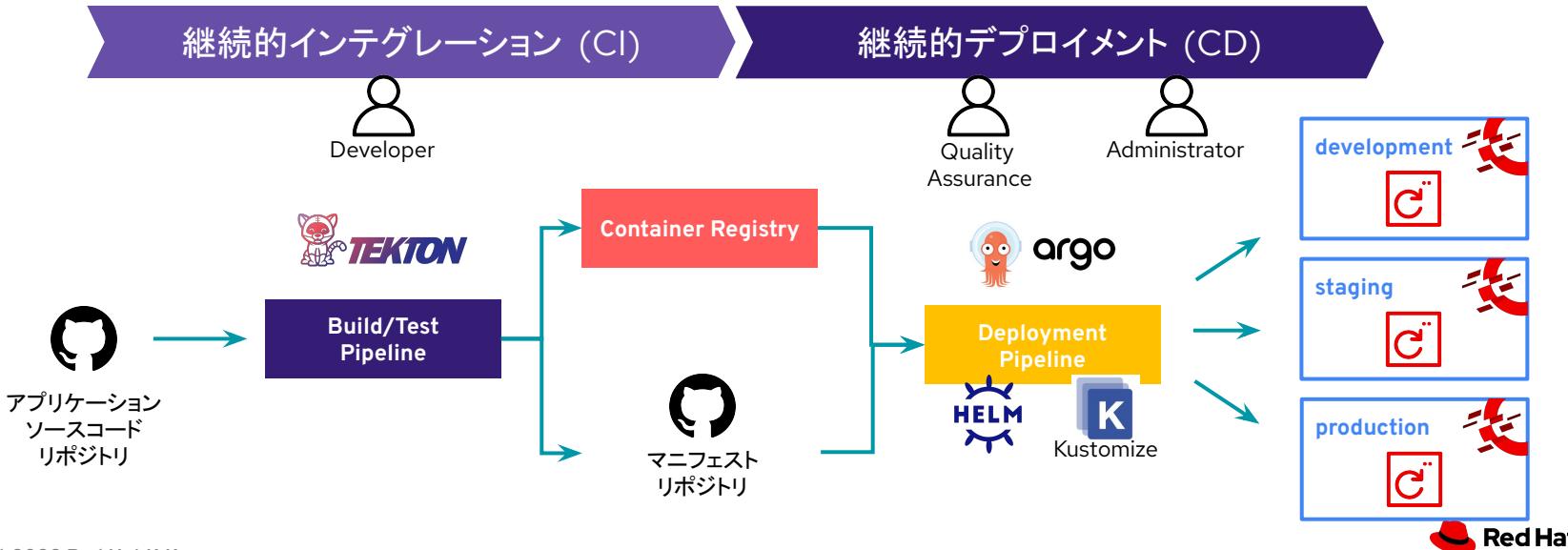
OpenShift上にデプロイするコンテナアプリ用
のビルダーイメージを選択 (この例では
Node.jsアプリをビルト・デプロイするために予
めOpenShiftで用意されている、専用のコンテ
ナイイメージを選択)

コンテナアプリのビルト/テスト/デプロイ の完全自動化

1

コンテナの動的
ビルト/デプロイ

- OpenShiftに統合されたPipelines ([Tekton](#)) を利用可能
 - ソースコードの静的解析/ビルト、単体/インテグレーションテストを実施 (CI部分を担当)
 - サーバレスなアーキテクチャ
- OpenShiftに統合されたGitOps ([Argo CD](#)) を利用可能
 - GitリポジトリをSingle Source of Truthとし、デプロイ先の状態変化を自動検知して、定義された状態を維持
- TektonとArgo CDは、Operatorによって運用を自動化



WebブラウザベースのIDEを提供

1

コンテナの動的
ビルド/デプロイ

様々な開発環境のテンプレートを利用可能 (OpenShift Dev Spaces)

The screenshot shows the Red Hat CodeReady Workspaces interface. On the left, there's a sidebar with navigation links like 'Get Started Page', 'Workspaces', 'RECENT WORKSPACES', and '+ Create Workspace'. The main area is titled 'Getting Started with CodeReady Workspaces' and has a sub-section 'Select a Sample' with a 'Filter by' dropdown. Below this, there's a grid of 15 workspace templates:

- JBoss**: Java with JBoss EAP XP 2.0 Bootable Jar
- JBoss**: Java with JBoss EAP XP 2.0 Microprofile
- JBoss**: Java stack with OpenJDK 8, Maven 3.6.3 and JBoss EAP 7.3
- Red Hat Fuse**: Red Hat Fuse stack with OpenJDK 8 and Maven 3.6.3
- Tooling for Apache Camel K**: Tooling to develop Integration projects with Apache Camel K
- Java Gradle**: Java stack with OpenJDK 8, Maven 3.6.3, and Gradle 6.1
- Quarkus**: Java Quarkus
- Java Vert.x**: Java stack with OpenJDK 11, Maven 3.6.3 and Vert.x booster
- Java Maven**: Java stack with OpenJDK 11, Maven 3.6.3 and Vert.x demo application
- Java Spring Boot**: Java stack with OpenJDK 8, Maven 3.6.3 and Spring Boot Petclinic demo application
- NodeJS ConfigMap Express**: NodeJS stack with NPM 6.14.6, NodeJS 12.18.4 and ConfigMap Web Application
- NodeJS MongoDB**: NodeJS stack with NPM 6.14.6, NodeJS 12.18.4 and MongoDB
- C++**: C and C++ Developer Tools stack with GCC 8.3.1, cmake 3.11.4 and make 4.2.1
- .NET**: .NET Core SDK 3.1.003, Runtime, C# Language Support and Debugger
- Go**: Stack with Go 1.12.2
- PHP CakePHP**: PHP Stack with PHP 7.3.5, Apache Web Server 2.4.37, Composer 1.8.4 and a quickstart CakePHP application for OpenShift
- PHP-DI**: PHP Stack with PHP 7.3.5, Apache Web Server 2.4.37 and Composer 1.8.4
- Python**: Python Stack with Python 3.9.0

On the right side, there's a large terminal window showing the output of a 'start native' command for a Quarkus application. The terminal output includes logs for Dockerfile builds, Java compilation, and a successful build. It also shows a browser preview of the application at <http://localhost:8080/index.html>.

OperatorHub.io

<https://operatorhub.io/>

KubernetesのOperatorのカタログを掲載するポータルサイトです。Red HatとMicrosoft、Google、Amazon Web Servicesと共に2019年にローンチしました。



Red Hat Ecosystem Catalog

<https://catalog.redhat.com/software>

Red Hat製品が稼働するハードウェア・ソフトウェアの認定製品を検索できるポータルサイトです。ソフトウェア認定では、サードパーティのOperator認定とコンテナの認定があり、既に多くのソフトウェアが登録されています。



Red Hat Marketplace

<https://marketplace.redhat.com/>

Red Hat認定のOperatorを検索し、購入・デプロイ・管理を容易にするオープンクラウドマーケットプレイスです。Red Hat OpenShift環境で利用できます。

Red Hat Marketplace

2

ミドルウェアの管理

- Red Hat製品だけでなく、様々なパートナーのOperator(数百以上)を掲載
- OpenShiftではOperatorHubという形式で統合されており、Red Hat MarketplaceにあるOperatorを簡単にデプロイすることが可能

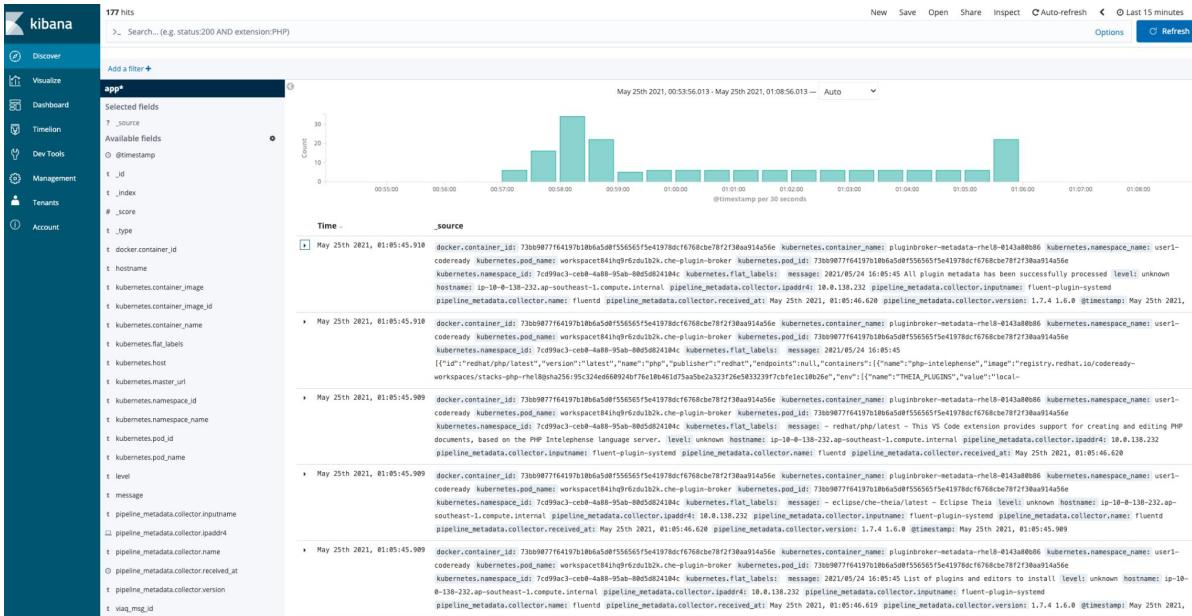
The screenshot shows the Red Hat Marketplace website interface. At the top, there's a navigation bar with links for Solutions, Sell with us, Blog, Docs, Support, a search bar, and buttons for Log in and Create account. Below the navigation is a sidebar with 'Product categories' like Featured products, AI/machine learning, Application runtime, Big data, Database, Datasets, Developer tools, Integration & delivery, Logging & tracing, Monitoring, Networking, Platform, Security, Storage, and Streaming & messaging. It also includes sections for 'Delivery methods' (Download, Operator, SaaS) and 'Certifications' (Enterprise ready). The main content area is titled 'All products' and shows 'Viewing 214 products'. A dropdown menu allows sorting by relevance. The page displays a grid of 20 product cards, each with a logo, name, developer, description, and rating. Some products shown include E.D.D.I., Anchore Enterprise, FP-PREDICT+, Ivory Service Architect, Modeling Tool, Densify, Red Hat Single Sign-On, Red Hat JBoss Enterprise Application Platform, Joget DX, Dynatrace, Lightbend Akka Platform Operator, Anaconda Team Edition, GigaSpaces InsightEdge, Hazelcast Jet, and Couchbase Server Enterprise Edition.

OpenShiftに統合されたロギング

3

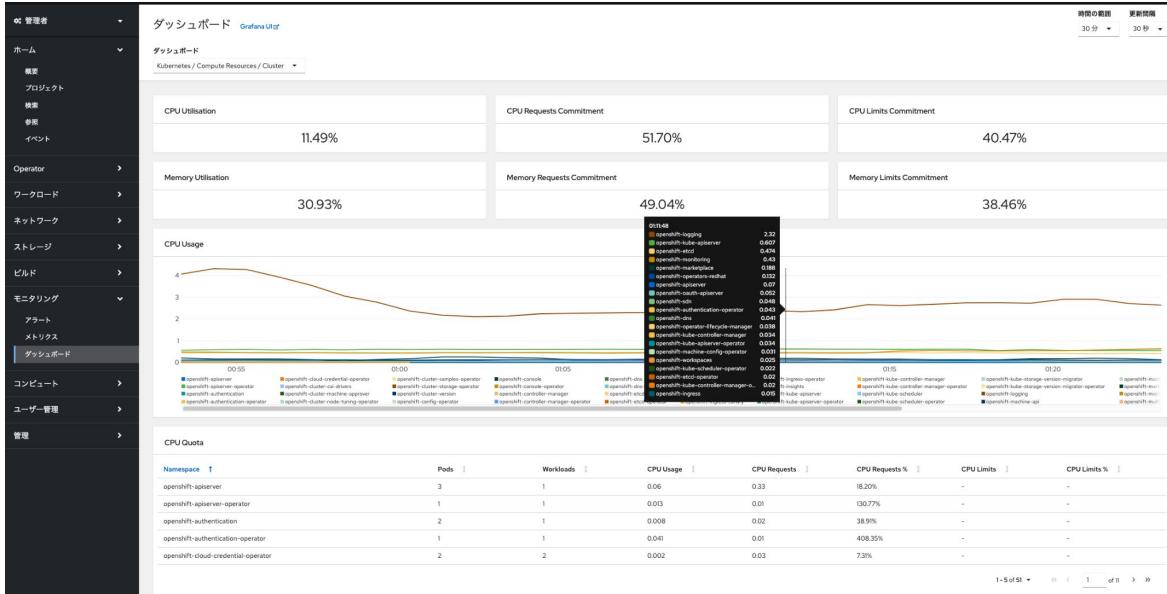
クラスタの ロギングや監視

- ロギングには、Elasticsearch/Fluentd/Kibana (EFKスタック) を利用
 - ユーザは自分が利用するプロジェクト上のアプリログ、管理者は全てのシステムログを参照可能
 - ログは外部システムへの転送が可能
 - Elasticsearch、Fluentd/rsyslogを利用するログ集積システム、Apache Kafkaのブローカ



OpenShiftに統合されたモニタリング

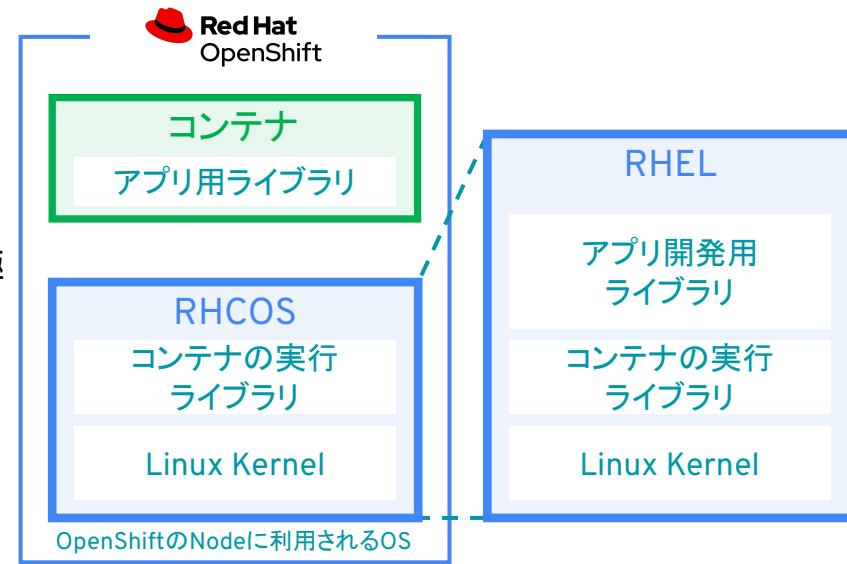
- モニタリングには、Prometheusを利用
- 管理者はOpenShift環境全体のリソース利用量や、API呼び出しのパフォーマンスなどを参照可能
- モニタリングによるアラートは、PagerDuty/Webhook/Email/Slackを利用した通知設定が可能



コンテナ利用に最適化された RHCOS(Red Hat Enterprise Linux CoreOS)を利用することによって、より安全かつ安定したコンテナ環境を提供します。

RHCOSは、RHELのKernelを利用しコンテナ実行に必要なライブラリだけを載せたコンテナ専用軽量OSです。
従来のRHELと同等の利用でサポートされます。

- OpenShiftと連携し、動的なUpgradeをOne-Clickで実現
- ライブラリが少ないため、セキュリティホールを生む可能性が極めて低い
 - そのため、多くのプログラムをOSの中で動かすことができない



ベースイメージの提供

4

コンテナの
セキュリティ

- コンテナベースイメージ(アプリケーションランタイム / SDK)をRed Hat Ecosystem Catalogにて提供
- セキュリティ脆弱性診断にも対応しており、**安心してコンテナイメージを利用可能**

The screenshot shows the Red Hat Ecosystem Catalog interface. On the left, there's a search bar with 'python' and a 'Search' button. Below it are filters for 'Provider' (Couchbase, IBM, New Relic, Red Hat, Inc.) and 'Category' (Application Delivery). The main area displays three container images for Python:

- Red Hat rhel8/python-27 Python 2.7** by Red Hat, Inc. (Platform for building and running Python 2.7 applications, updated 20 days ago)
- Red Hat ubi8/python-27 Python 2.7** by Red Hat, Inc. (Platform for building and running Python 2.7 applications, updated 21 days ago)
- Red Hat rhe8/python Python 3.8** by Red Hat, Inc. (Platform for building and running Python 3.8 applications, updated a month ago)

An orange arrow points from the search results to the detailed view of the Python 3.8 image. The detailed view shows a 'latest' tag, a 'Health index' (A), and a green checkmark indicating no unapplied security advisories. It also mentions the Container Health Index analysis is based on RPM packages signed and created by Red Hat.

OpenShiftのサブスクリプションに 含まれるベースイメージ

4

コンテナの
セキュリティ

「Software Collections(for RHEL7)」および「Application Streams (for RHEL8, RHEL9)」の
コンテナイメージのサポートが OpenShift のサブスクリプションに含まれています。

よく利用されることが多い、開発系の言語やデータベースなどのソフトウェアのバージョンの
サポート提供期間を短くする代わりに、バージョン更新頻度を高くしています。

Red Hat Enterprise Linux 7 Software Collections Product Life Cycle

Note

<https://access.redhat.com/ja/node/4654951>

Red Hat Enterprise Linux 8/9 Application Streams

Note

<https://access.redhat.com/support/policy/updates/rhel-app-streams-life-cycle>

Application Streamsの一部抜粋

| Application Stream | Release Date | Retirement Date |
|--------------------|--------------|-----------------|
| mariadb 10.5 | May 2021 | May 2026 |
| postgresql 13 | May 2021 | May 2026 |
| python 3.9 | May 2021 | May 2024 |
| redis 6 | May 2021 | May 2024 |
| dotnet 5.0 | Dec 2020 | Jan 2022 |
| nginx 1.18 | Nov 2020 | Nov 2022 |
| perl 5.30 | Nov 2020 | Nov 2023 |
| php 7.4 | Nov 2020 | May 2029 |

Over The Air (OTA) アップデート

5

クラスタアップグレード

- Cluster Version Operator (CVO) によるOpenShift 環境のアップデートの自動化
- CVOがネットワーク経由で、OpenShiftの有効なアップデート情報をチェックし、管理者に提示
- Web Consoleから簡単にアップデートを実行可能
 - 全てのコントローラ、コンピュートノードを、順番にアップデート (Self-ManagedのOpenShiftでは、一部のコンピュートノードをアップデート対象から外すことが可能)
 - コンピュートノードで Podが起動している場合、Podの停止→コンピュートノードのアップデートと再起動→Podの起動、を順番に実施
- 下記がアップデート対象
 - ホストOS (RHCOS)
 - OpenShiftのクラスタ管理サービス (Kubernetes, Monitoring, Networkなどを各種 Cluster Operatorによって管理)

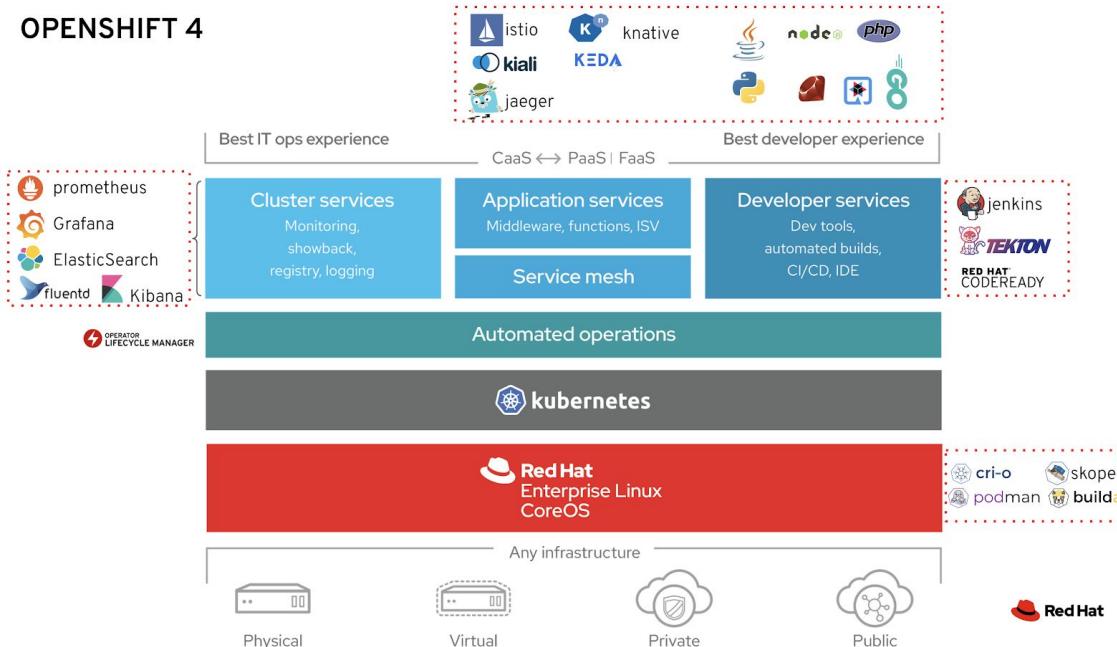
クラスター設定

詳細 ClusterOperators グローバル設定



Red Hat OpenShiftを構成するコンポーネント

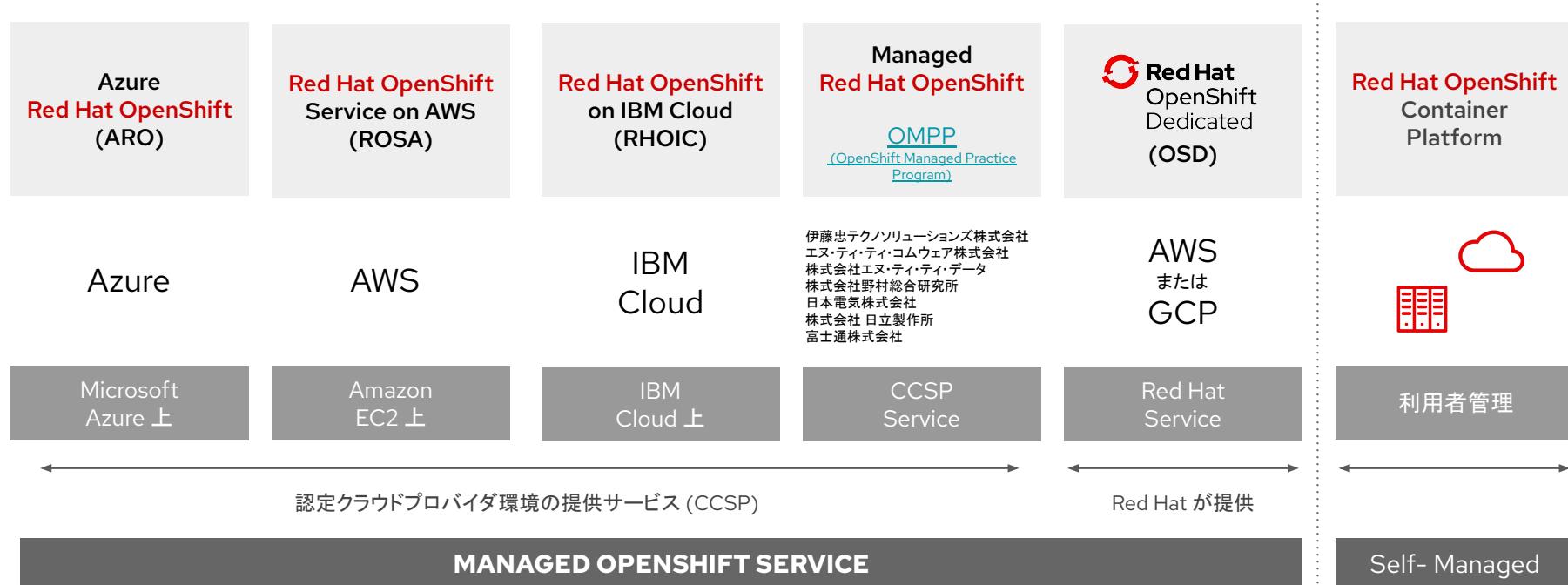
- 全てオープンソースソフトウェアであり、いくつかの主要なCloud Native Computing Foundation (CNCF) オープンソースプロジェクトで構成



Source: What's Inside OpenShift 4 <https://cloud.redhat.com/blog/whats-inside-openshift-4>

Red Hat OpenShift Everywhere

OpenShiftは、Azure上でも、AWS上でも、Google Cloud上でも、Red Hat OpenStack上でも、VMware上でも、オンプレのベアメタルサーバ上でも、[テス^ト済み](#)なので、場所を選ばずにどこでも同じ知識で運用を回す事ができるというのが大きな特徴です



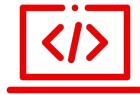
ここまでまとめ

- コンテナは、アプリケーション側に、より大きなビジネスメリットを提供
- コンテナは仮想マシンと同じように見えるが、様々な異なる特徴がある
- コンテナをうまく使うことで、アプリケーションの開発や運用を効率化可能
- 実稼働するシステムでは可用性や運用性が必要となるため、Kubernetesといった、コンテナオーケストレータを使うことが求められる
- Red Hat OpenShiftは、アプリケーション開発を効率化する様々な機能を提供
 - コンテナの動的ビルド/デプロイ
 - ミドルウェアの管理
 - クラスタのロギングや監視
 - コンテナのセキュリティ
 - クラスタアップグレード
- Red Hat OpenShiftは、様々なオンプレ/クラウド環境で実行可能

Managed OpenShift Service (OpenShift クラウドサービス)

Red HatがOpenShiftのManaged Serviceを推奨する理由

運用の複雑さを軽減し、開発者がアプリケーションの構築と運用に集中



素早い価値の提供

- ・管理されたクラスタを数十分で提供
- ・開発者の生産性を90%向上
- ・ビジネス付加価値の高いアプリケーションにフォーカスした開発を支援



運用効率の向上

- ・インフラリソースの管理から日常業務までFully Managed
 - 監視、ロギング、ネットワークなどを含む
 - ・柔軟な消費ベースの価格設定



24x365のサポート

- ・SLA 99.95% (ARO)
- ・業界をリードするSREチームによる24時間365日のフルスタック管理とサポート
- ・完全監視、管理、更新



クラウドの選択肢

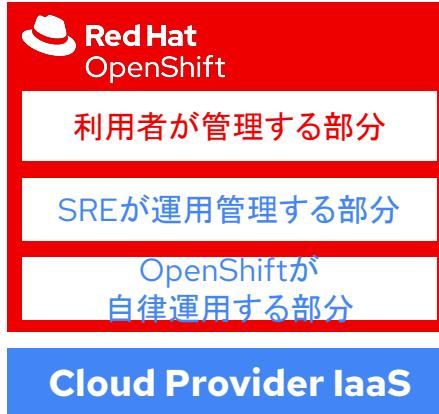
- ・すべての主要なパブリッククラウド上でManaged Kubernetesを提供する唯一の企業
- ・クラウドを超えた一貫したOpenShiftの経験

OpenShift運用管理の基本的な分類

SREが運用管理する部分

Red Hatやマネージドサービス
プロバイダのSREが行う作業

- Cluster Logging / Monitoring
- クラスタアップグレード
- クラスタ障害対応
- キャパシティ管理 など



利用者は、RHEL+Kubernetesの上で実行するアプリの設計・開発・運用、将来の成長性を見込んだスケールアウト・ダウン、共同開発グループを作成するためのユーザー管理、に集中できます。

言い換えると、これら以外の項目の変更や管理をしたい場合、マネージドでない、通常のOpenShiftのご利用を推奨します。

利用者が管理する部分

サービス利用に伴う作業

- テナント(Project)設計
- アプリ開発・運用、アプリのデータ管理
- クラウドのストレージ、
ネットワークを利用するための設定
 - ストレージプール設定
 - プライベートネットワーク設定など
- Compute Node の追加・削除・
ラベル付加、の実行指示
- ユーザー管理 (RBAC含)
- プラットフォーム監査ログ要求 など

OpenShiftが自律運用する部分

Cluster Operatorによって
動的に管理されるもの

- クラスタ作成 (API経由で作成)
- Controller / Compute Nodeの保守
- IaaSの制御
 - クラウドのストレージ、
ネットワークの払い出しなど

Azure Red Hat OpenShift (ARO) の概要

Azure Red Hat OpenShift (ARO) の概要

AzureにおけるフルマネージドのRed Hat OpenShiftサービス
マイクロソフトとRed Hatの両社で統合されたサポートエクスペリエンスと
共同設計、運用、サポート体制



エンタープライズグレードのオペレーション、 セキュリティ、コンプライアンス

業界をリードする SLA 99.95% の可用性を確保し、
ビジネス クリティカルなアプリを確実に展開



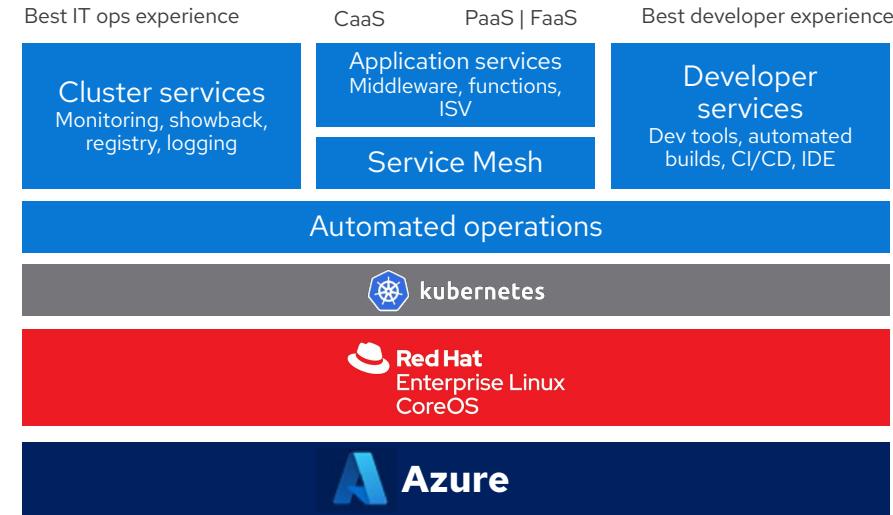
革新的な開発者支援

組み込みの CI/CD パイプラインを使用して、
開発者の生産性を向上し、MySQL, PostgreSQL,
Redis, Cosmos DB などの各種 Azure サービスに、
アプリケーションを簡単に接続可能



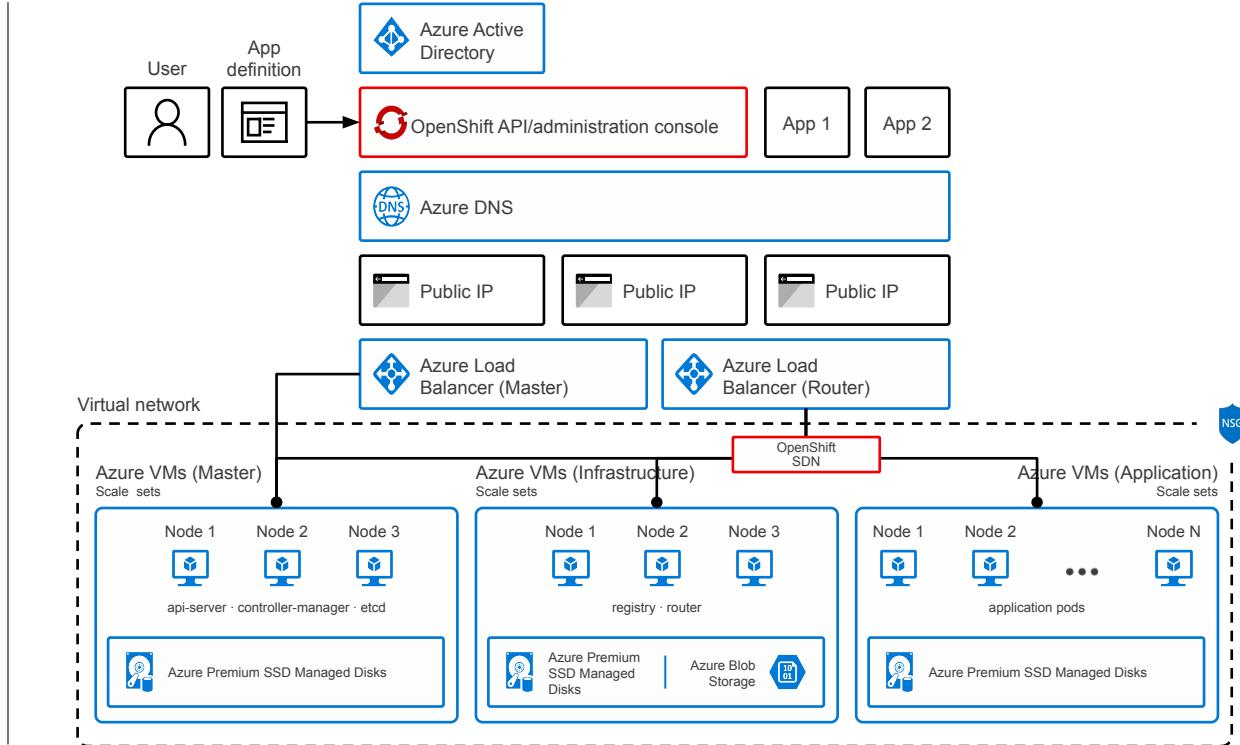
柔軟なスケーラビリティ

複数のアプリケーション ノードを持つ
高可用性クラスターを迅速に構築でき、
アプリケーション要求の変化に応じてスケーリング
さらに、標準、ハイメモリ、または、
高CPUのアプリケーション ノードを選択可能



IaaS に OpenShift を構築する場合

| 責任範囲 | |
|------------------------|-----------------------|
| ユーザ管理 | お客様 |
| プロジェクトとクオータの管理 | お客様 |
| アプリケーションライフサイクル | お客様 |
| クラスタの作成 | お客様 |
| クラスタの管理 | お客様 |
| モニタリングとロギング | お客様 |
| ネットワークの設定 | お客様 |
| ソフトウェアおよびセキュリティ更新プログラム | お客様 |
| プラットフォームのサポート | Microsoft and Red Hat |



Azure Red Hat OpenShift (ARO) の場合

| 責任範囲 | |
|------------------------|-----------------------|
| ユーザ管理 | お客様 |
| プロジェクトとクオータの管理 | お客様 |
| アプリケーションライフサイクル | お客様 |
| クラスタの作成 | Microsoft and Red Hat |
| クラスタの管理 | Microsoft and Red Hat |
| モニタリングとロギング | Microsoft and Red Hat |
| ネットワークの設定 | Microsoft and Red Hat |
| ソフトウェアおよびセキュリティ更新プログラム | Microsoft and Red Hat |
| プラットフォームのサポート | Microsoft and Red Hat |



マイクロソフトと Red Hat におまかせください

クラスターの管理

VMの監視と運用

ノードのセキュリティ保護

パッチの管理

Azure Red Hat OpenShift の特徴

- フルマネージド
- セルフサービスデプロイ
- スケーラビリティと信頼性
- ハイブリッドかつセキュアな環境
- シングルサインオン
- 統合サポート

フルマネージドの OpenShift サービス



ファーストパーティの
OpenShift サービス



Azure にデプロイされ、
お客様のサブスクリプションに
ご請求
Red Hat との個別契約不要



マイクロソフトと Red Hat が
共同でエンジニアリング、
運用、統合サポートを実施

Azure で OpenShift をすぐに利用開始

- Azure CLI/Portalで OpenShift のクラスターを Azure 上に作成可能
- 開発用、テスト用などの環境を柔軟に追加
- 従量課金で必要な時に必要なリソースを利用

ホーム > Azure Red Hat OpenShift >
Azure Red Hat OpenShift の作成 ...

基本 Authentication Networking Tags 確認および作成

プロジェクトの詳細

デプロイしているリソースとコストを管理するサブスクリプションを選択します。フォルダーのようなリソース グループを使用して、すべてのリソースを整理し、管理します。

| | |
|---------------|--------------------------|
| サブスクリプション * ① | Visual Studio Enterprise |
| リソース グループ * ① | aero-hands-on-rg01 |
| | 新規作成 |

インスタンスの詳細

リージョン * ① Japan East

OpenShift cluster name * ① testmyaro01

Domain name * ① testmydomain01

Master VM size * 3 x Standard D8s v3
8 vcpu 数、32 GB のメモリ
サイズを変更します

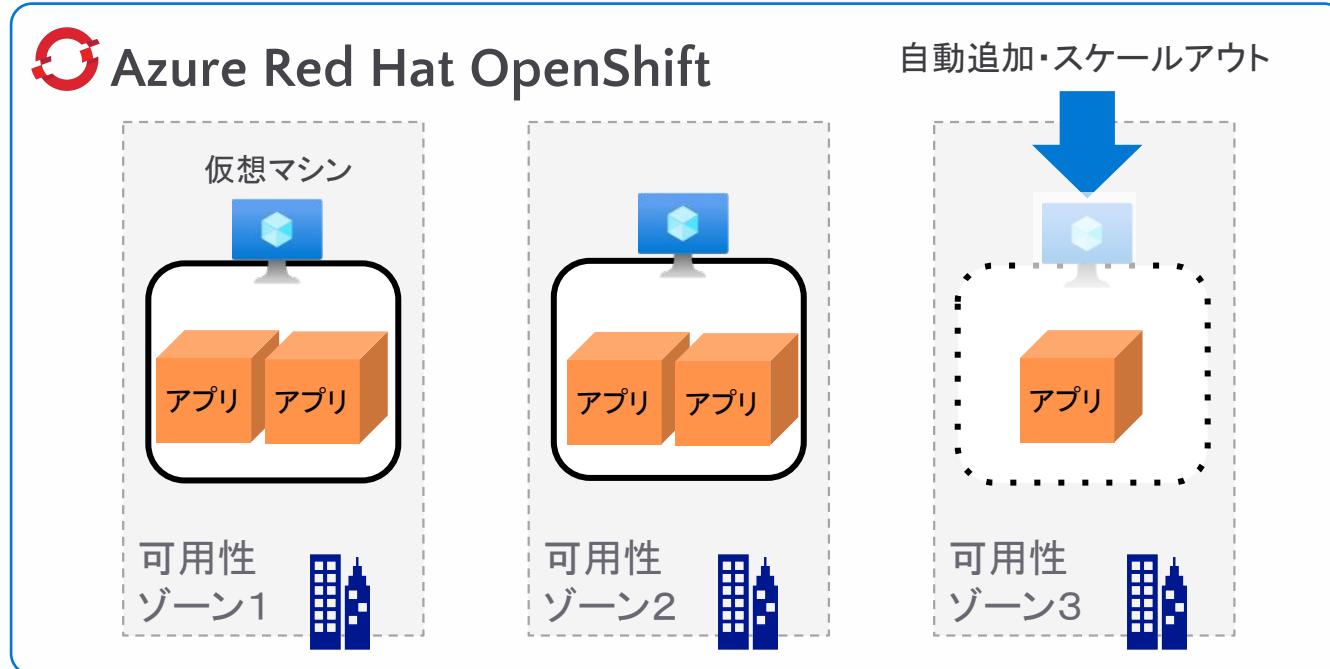
Worker VM size * 3 x Standard D4s v3
4 vcpu 数、16 GB のメモリ
サイズを変更します

Worker node count * ① 3

[確認および作成](#) < 前へ 次: Authentication >

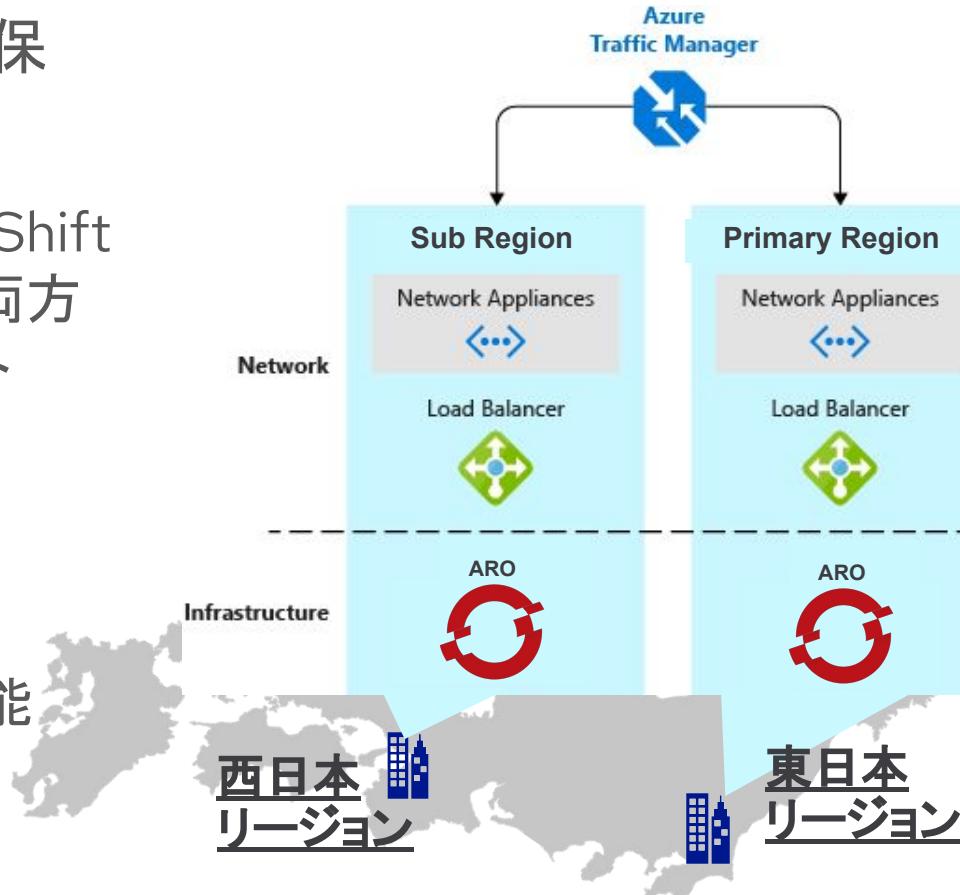
高いスケーラビリティと信頼性

- ・ クラウドの特徴を生かし、負荷変動にも柔軟にスケールして対応可能
- ・ マルチ可用性ゾーンをサポートし、高信頼な OpenShift 環境を提供



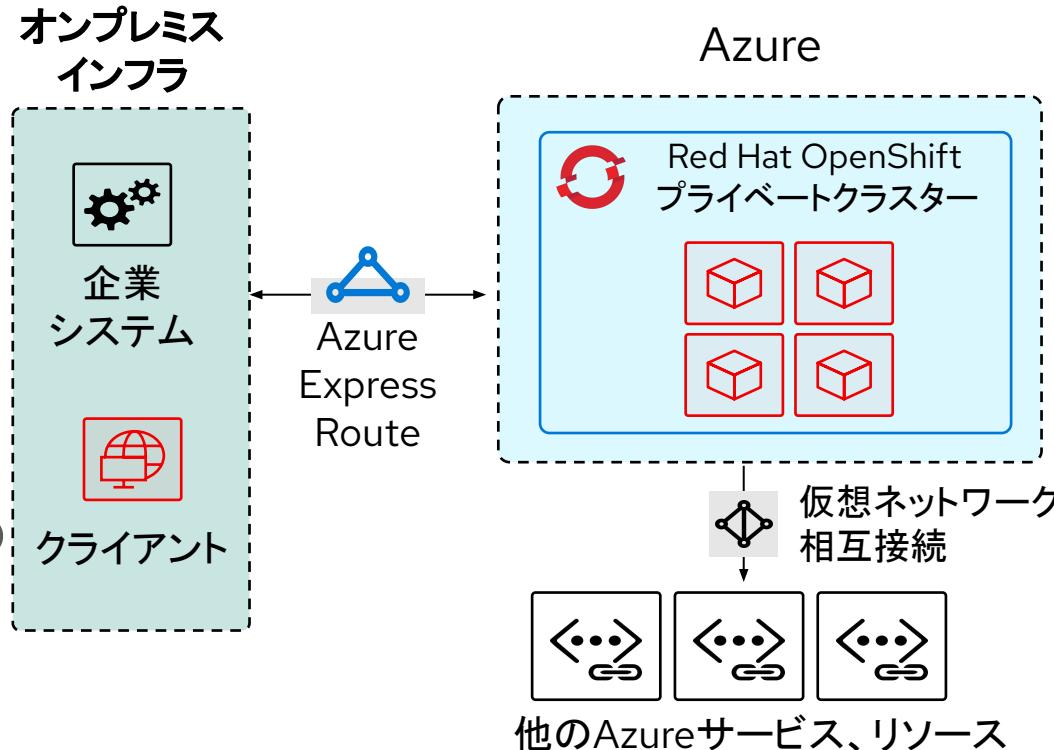
ビジネス継続性の確保

- Azure Red Hat OpenShift
は東日本と西日本の両方
のリージョンをサポート
- 大災害への備えや、
広域負荷分散など、
国内複数リージョンを
組み合わせて活用可能



ハイブリッドかつセキュアな OpenShift 環境

- お客様のオンプレミス ネットワークとAzure 上の OpenShift クラスターとの 相互接続により、 オンプレミスの環境を拡張
- プライベートなネットワークで、 セキュアにオンプレミスや他の Azure サービスと接続



シングルサインオンによる統合された認証

- Azure Red Hat OpenShift の管理者やアプリ開発者の認証に、Azure Active Directoryとの統合によるシングルサインオンをサポート
- OpenShift でサポートされている様々な認証サービス連携
(HTPasswd/LDAP/GitHubなど) を利用可能

Dashboard > App registrations > Register an application

Register an application

* Name
The user-facing display name for this application (this can be changed later).

aro-azuread-auth

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Microsoft only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

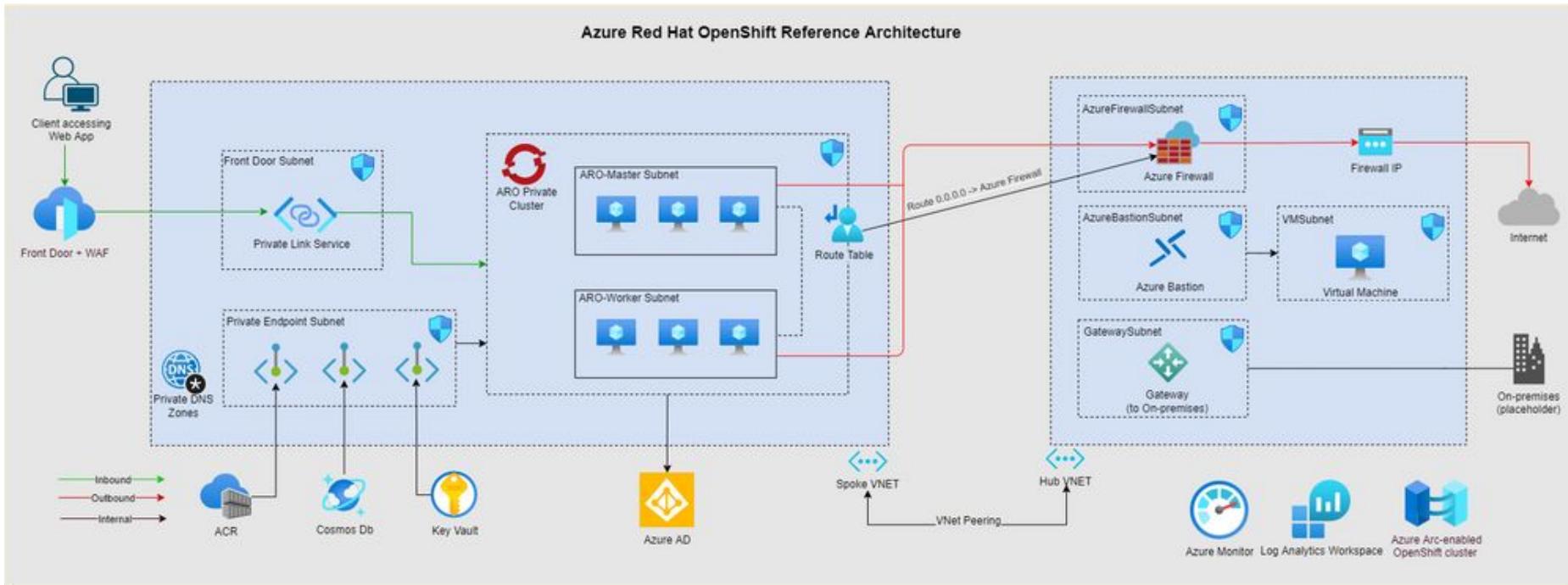
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

By proceeding, you agree to the Microsoft Platform Policies [↗](#)

[Register](#)

AROのリファレンスアーキテクチャ



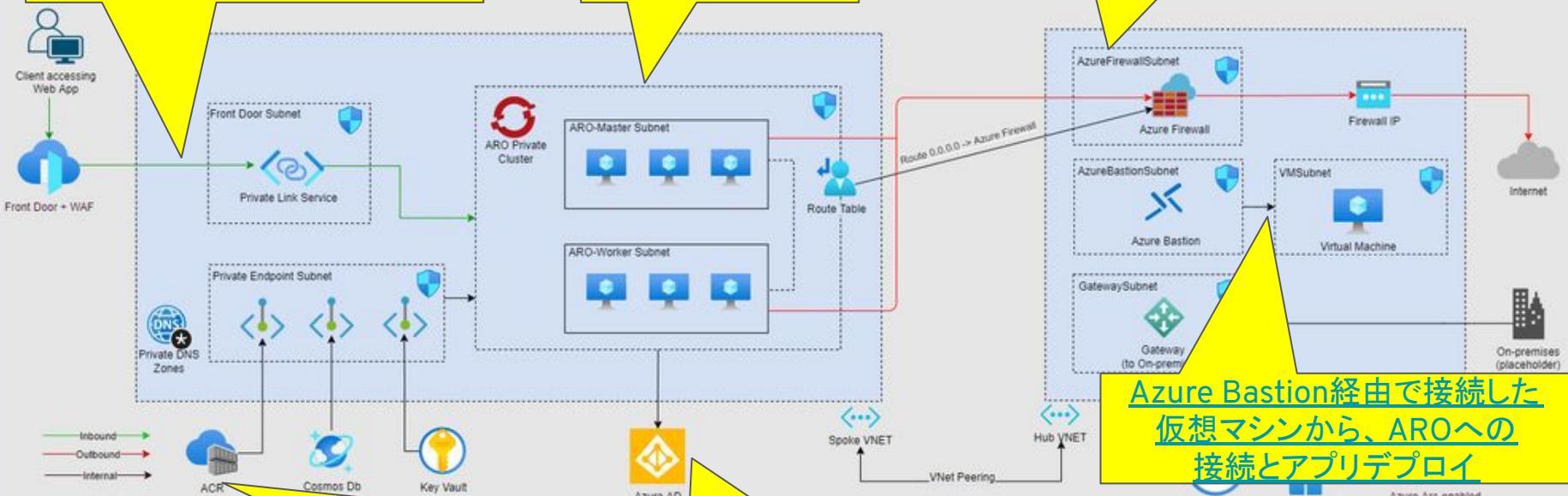
引用元: [Azure Red Hat OpenShift Reference Architecture & Reference Implementation](#)
[Announcing landing zone accelerator for Azure Red Hat OpenShift \(ARO\)](#)

AROのリファレンスアーキテクチャ

Azure Front Doorを利用した
AROへのセキュアな接続

プライベートな
AROクラスター

Azure Firewallによる
送信トラフィックの制御



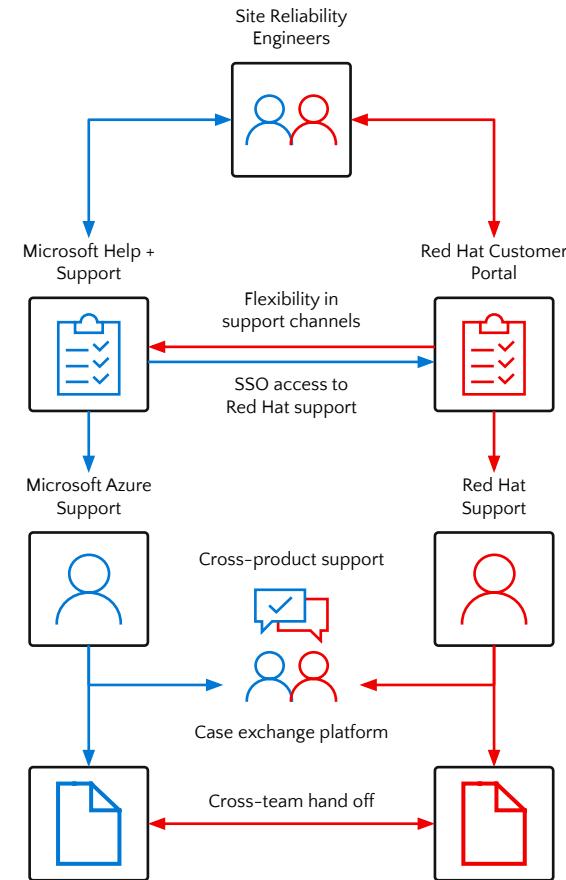
Azure Container Registry
(ACR)とのプライベート接続

Azure ADとの連携

引用元: [Azure Red Hat OpenShift Reference Architecture & Reference Implementation](#)
[Announcing landing zone accelerator for Azure Red Hat OpenShift \(ARO\)](#)

共同サポートと運用体制

- ・ Azure ポータル内の統合サポートは 24 時間 365 日利用可能
- ・ ISO 27001 準拠 B2B 通信チャネル
- ・ Red Hat オンサイトチームとの共同サポート
- ・ 統合チケットシステム



Azure Red Hat OpenShift (ARO) のサービス仕様

契約形態

- 契約条件や請求元は、マイクロソフト
- 管理作業やサポートは、マイクロソフトとRed Hatが連携して実施

| ARO | |
|----------------------------|---------------------|
| 処理主体 (Transacted) | Microsoft |
| 請求元 (Billed by) ※1 | Microsoft |
| 契約条件 (Contract terms) | Microsoft |
| マネージド管理主体 (Managed by) ※2 | Microsoft + Red Hat |
| サポート作業主体 (Supported by) ※3 | Microsoft + Red Hat |

※1: 請求元が発行する請求書には、OpenShiftサービスの利用料金や、仮想マシンやストレージなどのクラウドサービスの利用料金が記載されます。

※2: ロギング、モニタリング、プラットフォームのアップグレード、セキュリティ、などを担当する主体者。

※3: インストール、利用方法、設定、問題診断、バグ解決などに関して、チャット、電話、メールなどでの問い合わせ対応を実施する主体者。

AROの主なサービス仕様

Specification

ARO

デフォルトのアーキテクチャ

([マルチAZに自動デプロイ](#))

また、[Infra Nodeは現時点では使用不可](#))

Controller Node: Standard_D8s_v3 (8 vCPU, 32GiB Memory) x3 ([3台未満はサポート外](#))

Compute Node: Standard_D4s_v3 (4 vCPU, 16GiB Memory) x3 ([3台未満はサポート外](#))

Max Compute Nodes

[60](#)

対応リージョン

東日本, 西日本リージョン、[他リージョン](#)

プライベートクラスター

[対応](#)

IDプロバイダー (認証)

[Azure Active Directory](#)、
[OpenShiftでサポートされている認証プロバイダ \(LDAPなど\)](#)

Azureサービスとの連携

Azure Disk/Files(標準のストレージ機能), Azure Container Insights (ロギング/モニタリング)
[Azure Service Operator](#)を利用した、Azureサービスデプロイが可能。

アップグレード作業

基本的に、お客様が新マイナーバージョン (4.8や4.9など)や、新パッチバージョン (4.8.15など)への
[アップグレードを実施](#)。ただし、ARO SREチームが、[緊急性の高い新パッチバージョンへのアップグレードを、予告なく実施](#)することもあります。

SLA

99.95%

ARO overview of responsibility assignment matrix

- マイクロソフトとRed Hatは、AzureのIaaS基盤とOpenShiftを管理
- お客様は、AROにデプロイしたアプリ、アプリの {データ、ロギング、ネットワークポリシー }、VNet間接続、VPN接続やプライベートエンドポイントなどのオプション設定や保守、を管理
- 詳細: <https://docs.microsoft.com/ja-jp/azure/openshift/responsibility-matrix>

| Resource | Incident and operations management | Change management | Identity and access management | Security and regulation compliance | | |
|--------------------------------------|------------------------------------|-------------------|--------------------------------|------------------------------------|--|--|
| Customer Data | Customer | | | | | |
| Customer applications | Customer | | | | | |
| Developer services | Customer | | | | | |
| Platform monitoring | Microsoft + Red Hat | | | | | |
| Logging | Microsoft + Red Hat | Shared | | | | |
| Application networking | Shared | | Microsoft + Red Hat | | | |
| Cluster networking | Microsoft + Red Hat | Shared | | Microsoft + Red Hat | | |
| Virtual networking | Shared | | | | | |
| Controller nodes | Microsoft + Red Hat | | | | | |
| Compute nodes | Microsoft + Red Hat | | | | | |
| Cluster version | Microsoft + Red Hat | Shared | Microsoft + Red Hat | | | |
| Capacity management | Microsoft + Red Hat | Shared | Microsoft + Red Hat | | | |
| Virtual storage | Microsoft + Red Hat | | | | | |
| Physical infrastructure and security | Microsoft + Red Hat | | | | | |

AROのバックアップポリシー

- AROにデプロイしたアプリケーションのバックアップとリストアについては、お客様の責任で実施いただきます。
 - Veleroを利用した、永続ボリューム(外部ストレージの利用設定)を含んだアプリケーションのバックアップとリストア手順を、AROの公式ドキュメントで紹介
 - <https://docs.microsoft.com/ja-jp/azure/openshift/howto-create-a-backup>
 - <https://docs.microsoft.com/ja-jp/azure/openshift/howto-create-a-restore>
- AROのOpenShift環境、etcdデータなどのバックアップポリシーは、現時点では公開していません。

AROのライフサイクル (2022年9月時点)

- AROでは、OpenShiftの2つのマイナーバージョンをサポート (最新と1つ前)
- AROの新しいマイナーバージョンがリリースされると、2つ前以上のAROのマイナーバージョンを使っている場合、サポート終了日(お客様にメールを事前送信)から、30日以内にアップグレードする必要があります
 - 参考情報: リリース情報を含んだ、AROのロードマップ <https://github.com/Azure/OpenShift/projects/1>
- マイナーバージョンの延長サポートを提供する、Extended Update Support (EUS)は無し
- 詳細: <https://docs.microsoft.com/ja-jp/azure/openshift/support-lifecycle>

| OpenShift バージョン | OpenShift リリース | AROの一般提供 | AROのEnd of Life (サポート終了日) |
|-----------------|----------------|------------|--------------------------------|
| 4.7 | 2021年2月24日 | 2021年7月15日 | ARO 4.9 一般提供日 (2022年2月1日) |
| 4.8 | 2021年7月27日 | 2021年9月15日 | ARO 4.10 一般提供日 (2022年6月21日) |
| 4.9 | 2021年10月18日 | 2022年2月1日 | ARO 4.11 一般提供日 |
| 4.10 | 2022年3月10日 | 2022年6月21日 | ARO 4.12 一般提供日 |
| 4.11 | 2022年8月10日 | 未提供 | 未定 |

参考: ARO 利用料金モデル (2022年9月時点, 税抜き)

- Controller Node x3 / Compute Node x3 (AROのデフォルトアーキテクチャを想定)
- 東日本リージョンで、1年間利用を想定 (1年間契約)
- 参考情報: <https://azure.microsoft.com/ja-jp/pricing/details/openshift/>

| ARO pricing model | |
|---|---|
| Controller Nodes x3 | \$2,856 /y (\$238 /m) x3 = \$8.568 /y (1 Year Commitment) |
| Compute Nodes x3 (OpenShiftのサブスクリプション料金を含む) | \$2,436 /y (\$203 /m) x3 = \$7,308 /y (1 Year Commitment) |
| Other Services | <p style="text-align: center;">計算対象外</p> <p>* 計算を簡単にするために、他のコンピューティング、ネットワーキング、ストレージリソースなどは計算対象外としています。</p> |
| Total | \$8,568 + \$7,308 = \$15,876 /y |

参考情報

- マイクロソフトのWebsite: Azure Red Hat OpenShift
 - <https://azure.microsoft.com/ja-jp/services/openshift/#overview>
- レッドハットのWebsite: Microsoft Azure Red Hat OpenShift
 - <https://www.redhat.com/ja/technologies/cloud-computing/openshift/azure>
- Azure Red Hat OpenShiftのドキュメント
 - 操作ガイド/サポートポリシー/ライフサイクル/FAQ...などを記載
 - <https://docs.microsoft.com/ja-jp/azure/openshift/>
- Azure Red Hat OpenShift Reference Architecture & Reference Implementation
 - <https://techcommunity.microsoft.com/t5/fasttrack-for-azure/azure-red-hat-openshift-reference-architecture-and-reference/ba-p/3470115>
 - <https://techcommunity.microsoft.com/t5/azure-developer-community-blog/announcing-landing-zone-accelerator-for-azure-red-hat-openshift/ba-p/3614057>



Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



twitter.com/RedHat