

JANOG46 Meeting Lightning Talk

GitOpsを適用したクラウドネイティブな ネットワークアーキクチャ

2020年8月28日
株式会社KDDI総合研究所
アーキテクチャグループ
関川 柊 (sh-sekigawa@kddi-research.jp)

関川 柁 (Shu Sekigawa)

■株式会社KDDI総合研究所

- 2019年 KDDI入社 運用システム開発
災害対応システム, 運用ダッシュボード etc...
- 2020年 4月より研究所へ異動, 6月より現部署
クラウドネイティブネットワークに関する研究

■JANOG Meeting初参加

- 5G時代に向けてネットワーク機能仮想化の利用が加速
- MECやスライス実現に向け、従来の仮想マシンによる仮想化に代わりコンテナ仮想化を用いた**クラウドネイティブな仮想ネットワーク機能(VNF)**がvRAN・5GCを中心として検討

※一般にCNFと呼ばれるが本スライドではVNF表記に統一

一方で...

MEC: Multi-access Edge Computing
VNF: Virtualized Network Functions
CNF: Cloud-Native Network Functions
CI/CD: Continuous Integration / Continuous Delivery

クラウドネイティブの特徴である回復性、管理力、可観測性の実現にはVNFのコンテナ化だけでは不十分

e.g. 手動でのKubernetes(K8s)クラスタ操作, 複雑な手順書による復旧

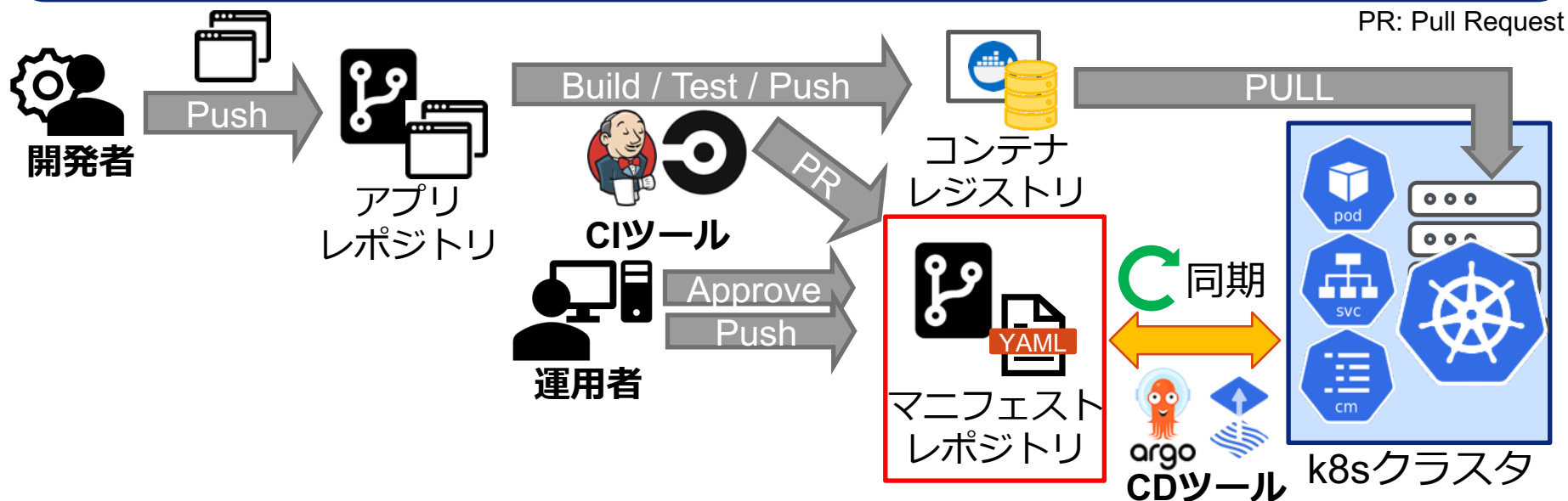
 クラウドネイティブな運用実現に向けた検討が必要

- クラウドネイティブな運用手法の一つとして**GitOps**に注目
- GitOpsを用いたCI/CDアーキテクチャを構築
仮想ネットワークの運用に対するGitOps適用を検討

GitOps

1: Guide To GitOps
(<https://www.weave.works/technologies/gitops/>)

- Weaveworks 社の提唱¹するクラウドネイティブな**CI/CDストラテジー**
- ソースコードに加え, 構成・設定を記述したマニフェストを**Git**で管理
- マニフェストに**同期**してK8sにアプリケーションを配置

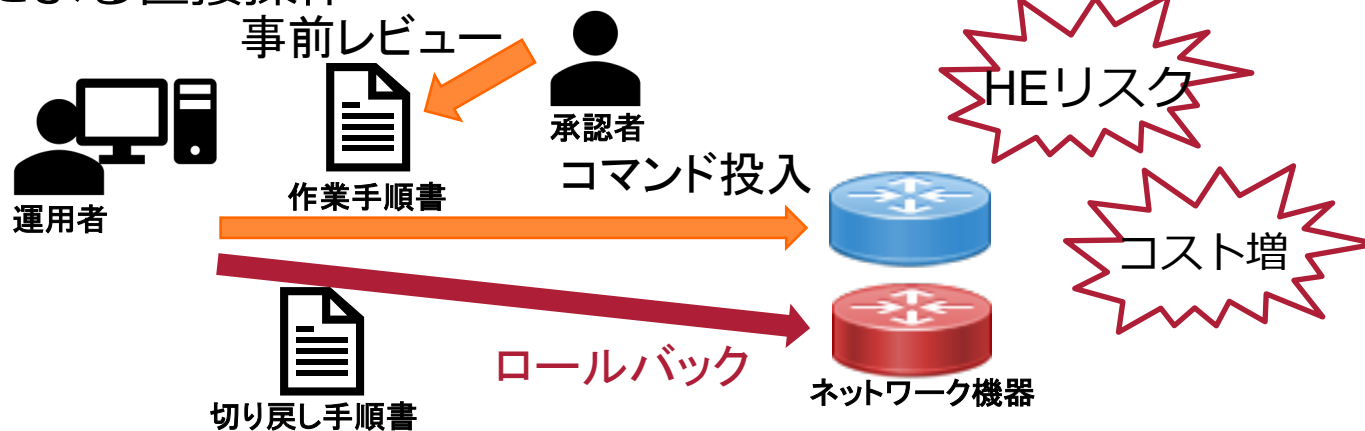


- マニフェストレポジトリでK8sクラスタの**あるべき状態**を管理
理想状態の世代管理が可能, 運用操作の属人化を防止
- マニフェストレポジトリを分解点とした**CIとCDの分離**
CIツールへの権限集中を回避, セキュリティ向上

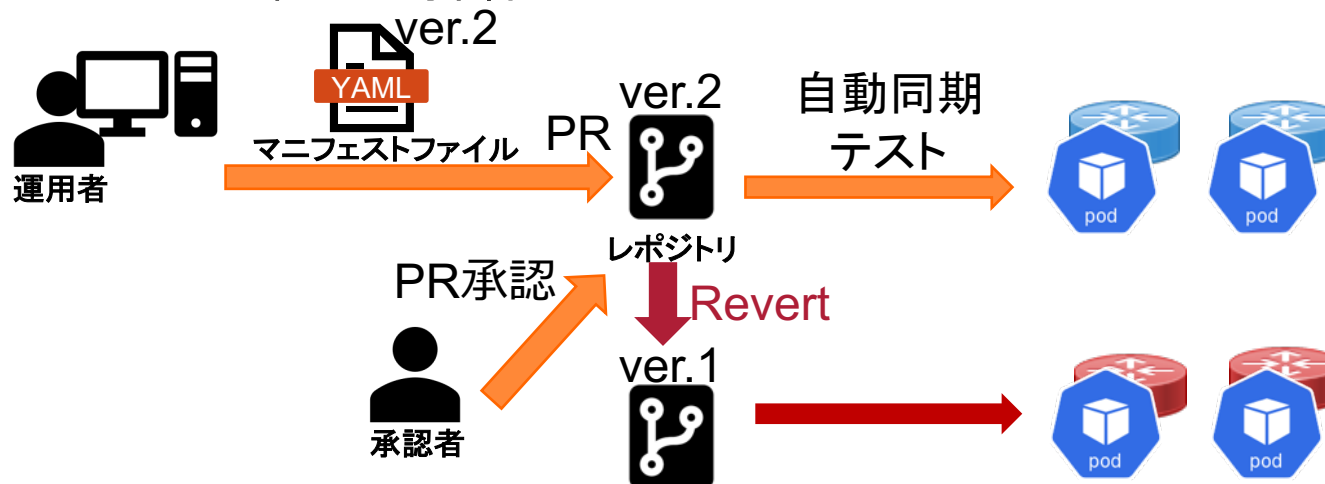
VNFに対するGitOps適用の効果 (1/2)

従来：人手による直接操作

HE: Human Error



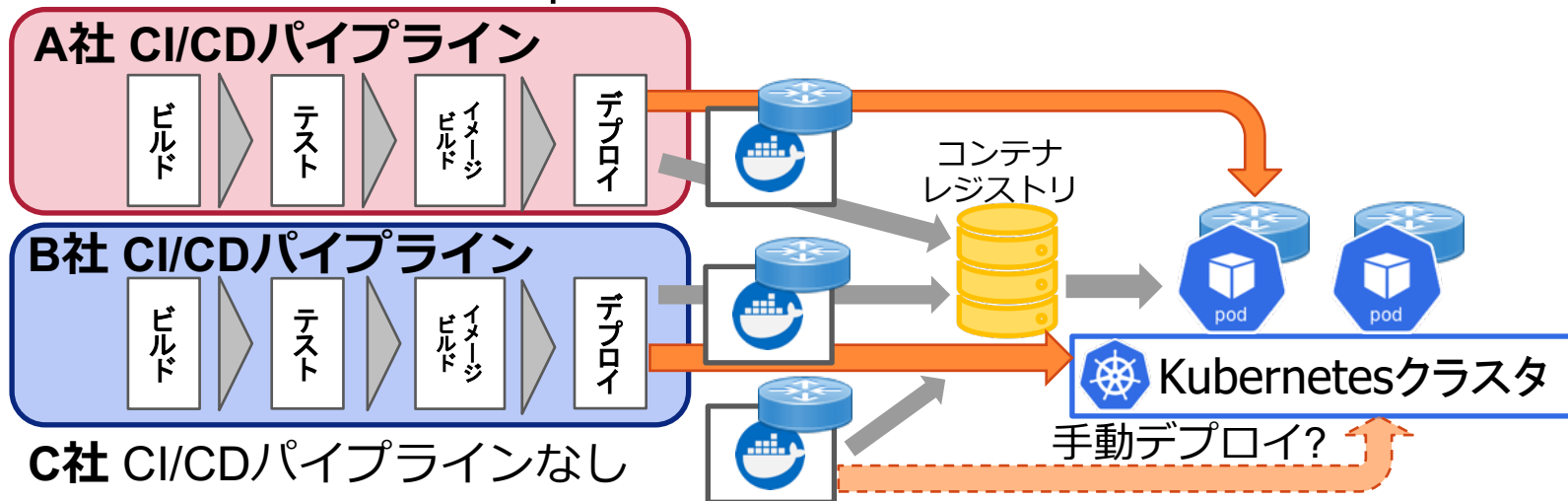
GitOps：レポジトリ経由で操作



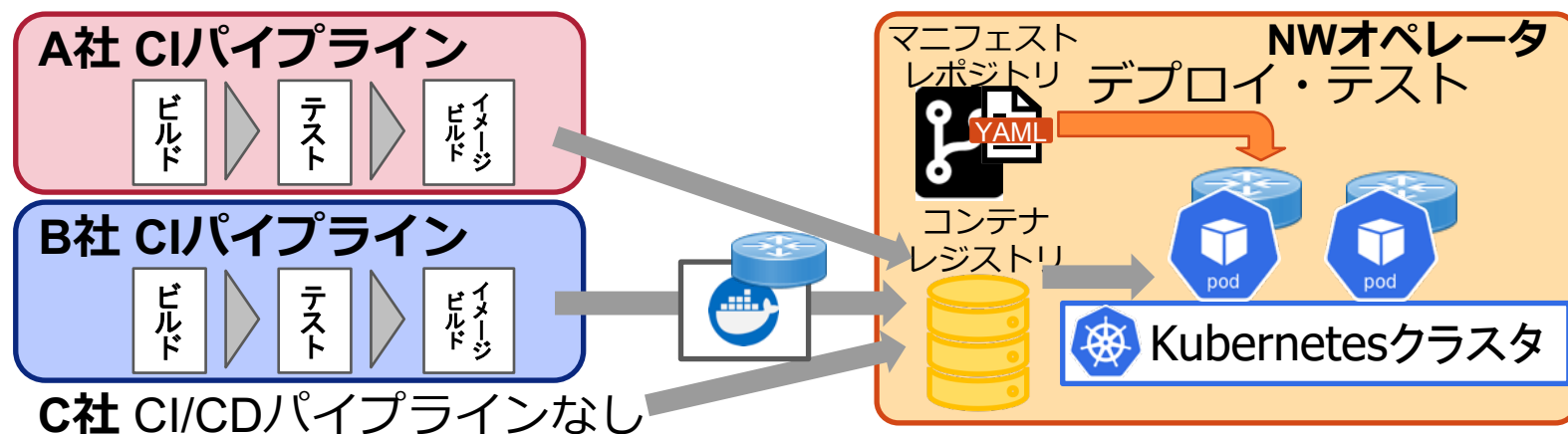
- HEの防止, Pull Requestベースの運用による承認フローの組み込み
- 前バージョンの状態へGit操作によって容易にロールバック

VNFに対するGitOps適用の効果 (2/2)

従来：CIツール中心のVender-specificなパイプラインによるデプロイ



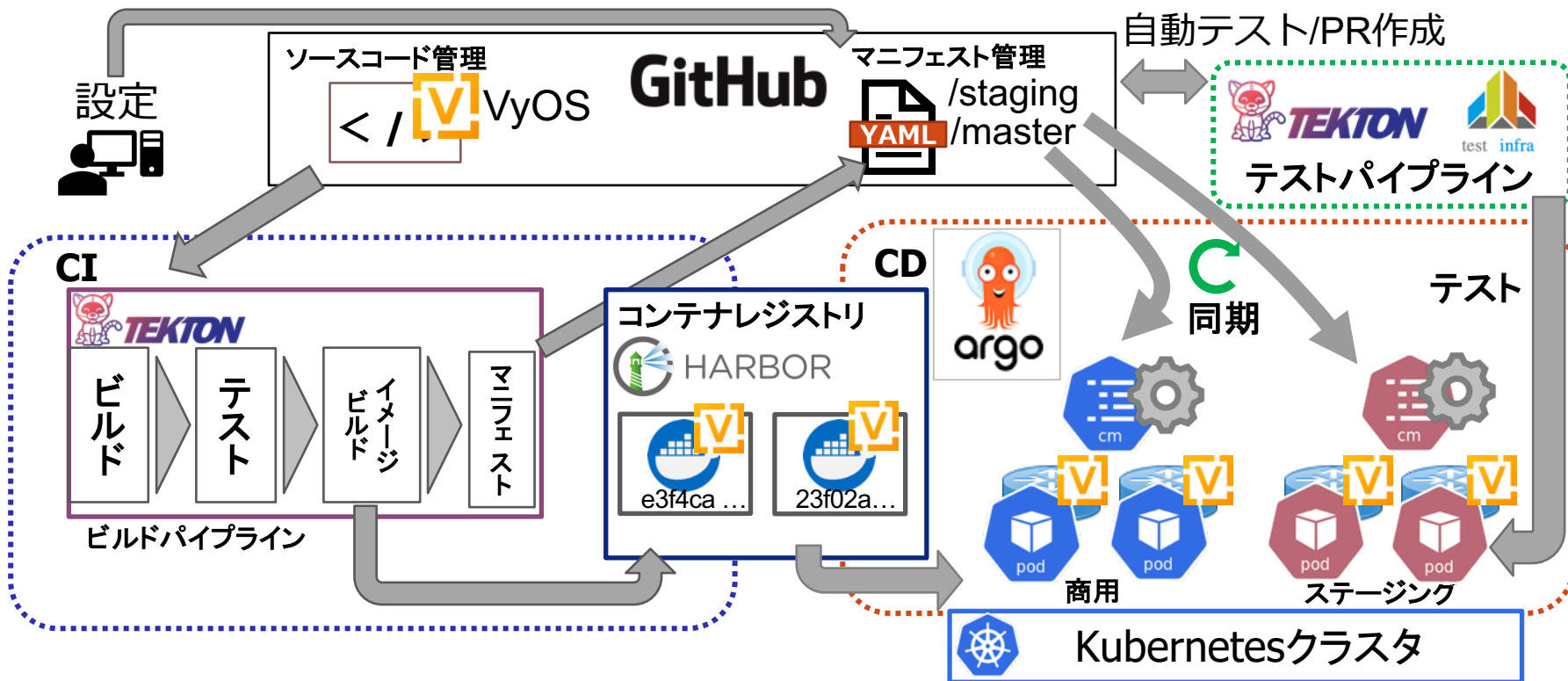
GitOps：CI/CDの分離によってCDはNWオペレータ内で完結



マルチベンダVNFをNWオペレータのポリシーに従ってデプロイ可能
e.g. 複数ベンダの製品を組み合わせたデプロイルール

VNFへのGitOpsの適用について既存OSSで対応可能か検証を実施

- CI: **Tekton Pipelines** CD: **Argo CD**を利用し、GitOps検証環境を構築
- VNFとしてコンテナ化した**VyOS**を使用



K8s上でVyOSをコンテナ化・デプロイ・テストを実施
マニフェストに同期する形で自動的にネットワークを構成

■ GitOpsなコンフィグの投入

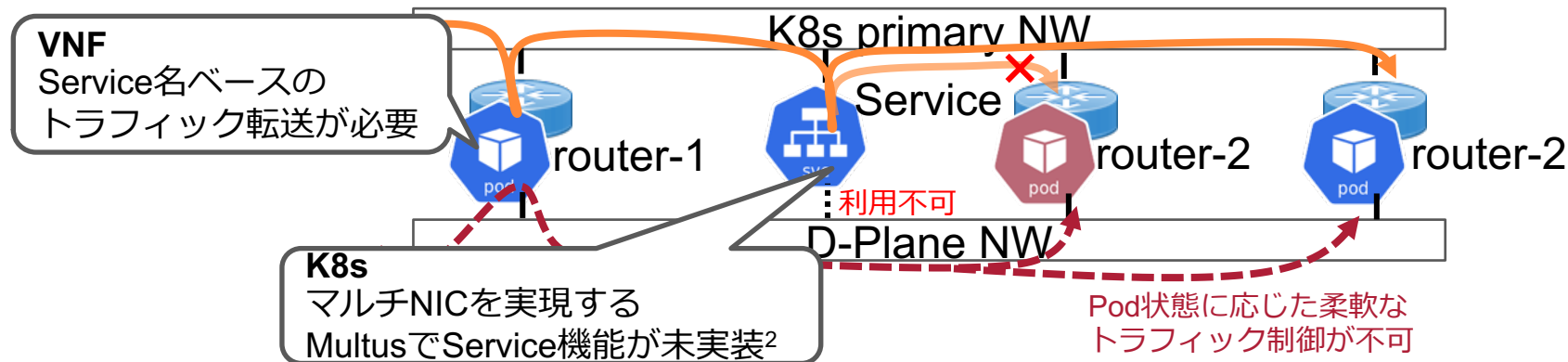
- VyOSは本来はCLIで操作、GitOpsではマニフェストによる管理が必要
- Kustomizeの**configMapGenerator機能**を利用
スタートアップコンフィグとして設定内容を投入
➡ マニフェストの変更でPodが再作成され、設定が更新
- CLIから一時的な設定変更は可能、マニフェストとズレ

■ 今後の課題：サービスディスカバリ

- K8sでは**Service**機能によってPodへのアクセスを柔軟に制御

Router1->2の転送

Serviceにより動作中のPodへ
トラフィックを自動的に振り分け



➡ コンフィグ変更時にPod再作成によるサービス断が発生

この問題に対応するOSSとしてNSMやDANMが開発
特にNSMについてソフトウェアの動作・機能を検証中

■背景

- 5G時代に向けコンテナ仮想化を利用したクラウドネイティブなネットワーク機能仮想化が検討
- ネットワーク運用のクラウドネイティブ化に向けてGitOps手法のネットワーク機能への適用を検証

■GitOps

- Gitレポジトリで構成、設定内容などをマニフェストとして管理
- マニフェストに同期してK8sにアプリケーションをデプロイ

■VNFへのGitOps適用

- GitOpsの適用によりネットワークの運用においてHEの防止・運用コスト削減・マルチベンダVNFへの対応を実現
- Tekton Pipelines・Argo CDでGitOpsなCI/CDパイプラインを構築
仮想ネットワークをマニフェストに従って自動構成

■今後の課題

- ネットワーク運用のクラウドネイティブ化の実現にはサービスディスカバリによる柔軟なトラフィック転送機能などVNF、K8sインフラ双方の対応が必要
- NSM, DANMなどネットワークのクラウドネイティブ化に向けたOSSプロジェクトの開発動向が鍵

