

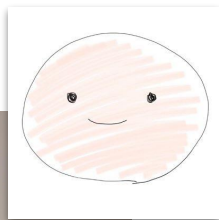
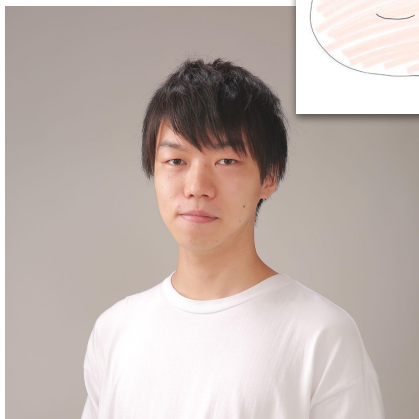
【速報】日本経済新聞社 Anthos の本番導入に成功

岩月海人

日本経済新聞社 デジタル事業ソフトウェアエンジニア



自己紹介



- 名前: 岩月 海人 (Kaito Iwatsuki)
- 所属:
 - 2019-2020: エムスリー株式会社
 - 2020-: 日本経済新聞社
- やっていること:
 - バックエンド開発・インフラ構築
 - SRE (Kubernetes 基盤運用 etc.)

本日は話すこと

- 日経電子版での Anthos 導入前の GKE 運用における状況と課題
- なぜ Anthos を選んだか
- Anthos を採用してどうだったか
 - Multi Cluster Ingress (メイン)
 - Anthos Service Mesh
 - Config Connector

本日は話さないこと

- GKE (Kubernetes) などの技術選定
 - 以前の登壇資料¹があるのでそちらを参照ください
- Anthos x マルチクラウドの話
- Anthos x オンプレの話

¹「GKE + Istio + GitOps で作る 日経電子版の新 Microservice 基盤」

https://inthecloud.withgoogle.com/anthos-day-2001/Google_Cloud_Anthos_Day_200130_Session10.pdf

日経電子版とは

- 日経の記事を Web で配信
- 有料ユーザ 80 万人以上
- 無料ユーザ 450 万人以上





Anthos 導入の背景

Anthos 導入前の GKE 運用の状況

- 日経電子版の一部のマイクロサービスは、GKE + Istio + GitOps を利用した基盤上で稼働しています。

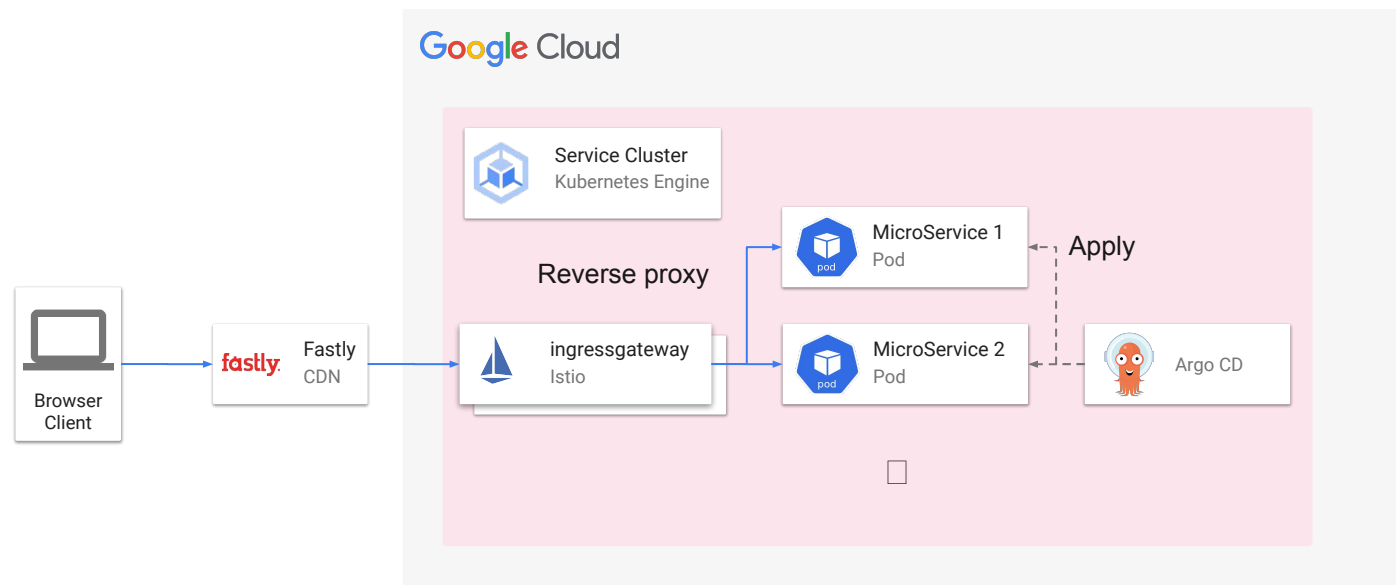


1「GKE + Istio + GitOps で作る 日経電子版の新 Microservice 基盤」

https://inthecloud.withgoogle.com/anthos-day-2001/Google_Cloud_Anthos_Day_200130_Session10.pdf

Anthos 導入前の GKE 運用の状況

Anthos 導入前のアーキテクチャ



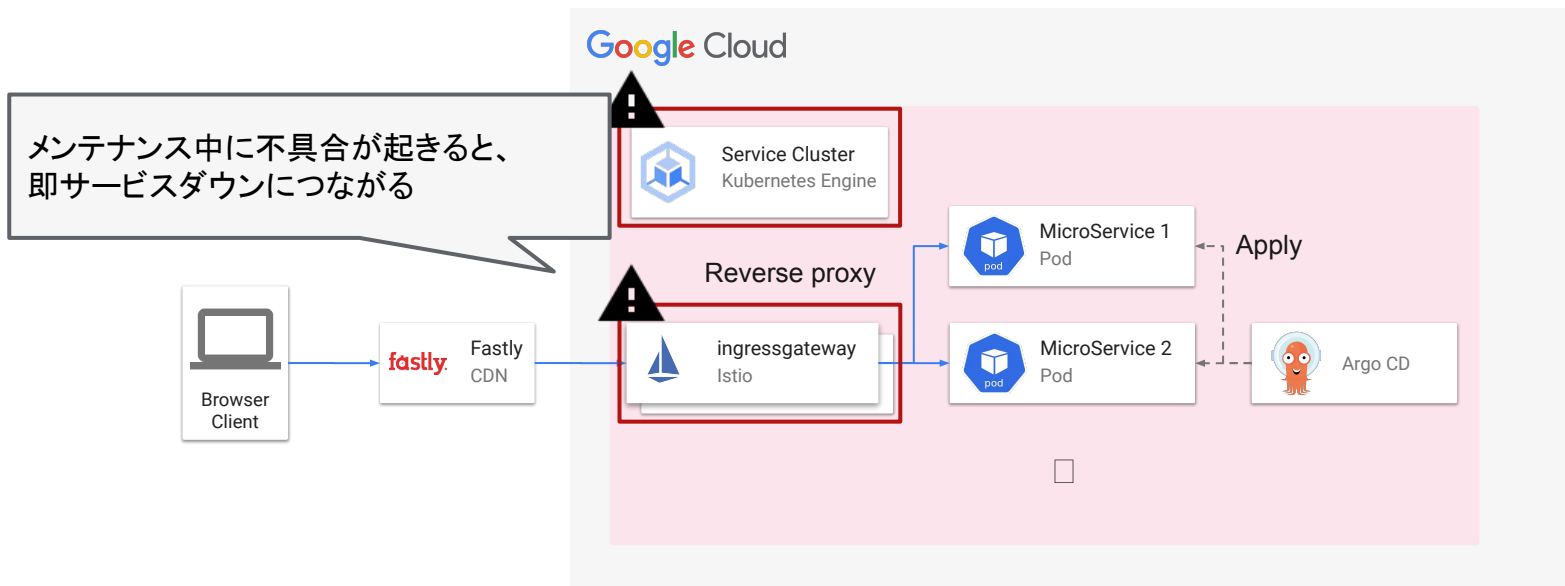
Anthos 導入前の GKE 運用の課題

GKE(とそのエコシステム)を運用していく中で以下のような課題が...

- より安全な GKE アップグレードの仕組みが必要
 - GKE の公式アップグレードフローであるIn Place Upgrade は、どれだけ検証しても実施時にサービスダウンのリスクがある
 - Istio などのコンポーネントのアップグレードも同様
 - 一度アップグレードをしてしまうと切り戻しが難しい
 - 日経電子版はニュースメディアであるという性質からBCP (事業継続計画) を見据えた柔軟な構成が要求されていた

Anthos 導入前の GKE 運用の課題

Anthos 導入前のアーキテクチャ



Anthos 導入前の GKE 運用の課題

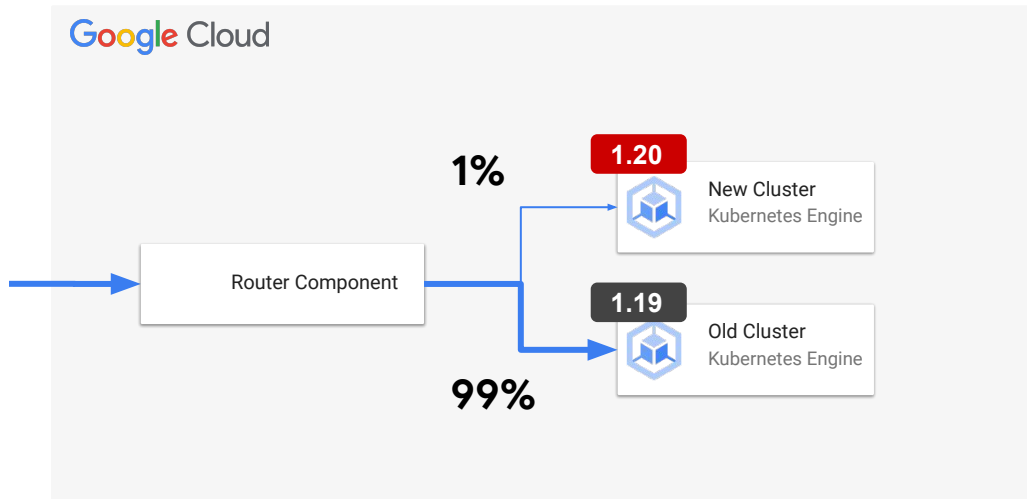


より安全な GKE アップグレードの仕組みが必要

- In Place Upgrade を避ける仕組みが必要
- クラスタの Canary Upgrade を行いたい

Canary Upgrade

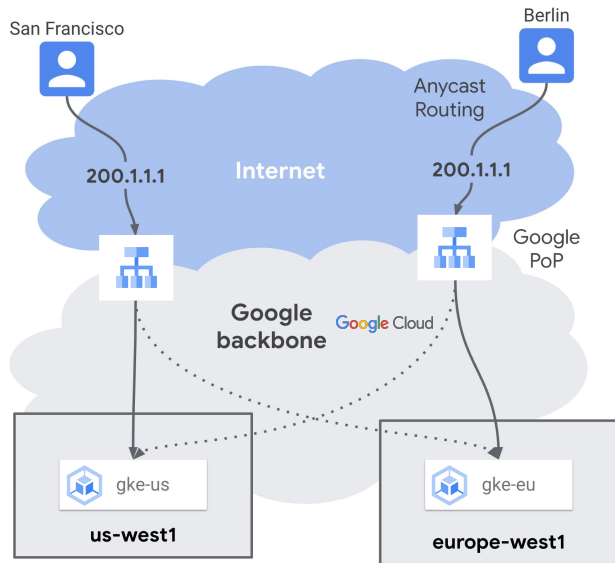
一部のトラフィックをアップグレードしたクラスタに流し徐々に展開





Multi Cluster Ingress

Multi Cluster Ingress | Solution



Multi Cluster Ingress は、GKE クラスタ用のクラウドホスト型マルチクラスタ Ingress コントローラです。

出典 : <https://cloud.google.com/kubernetes-engine/docs/concepts/ingress-for-anthos?hl=ja>

これを使えば Canary Upgrade ができそう? 🤔

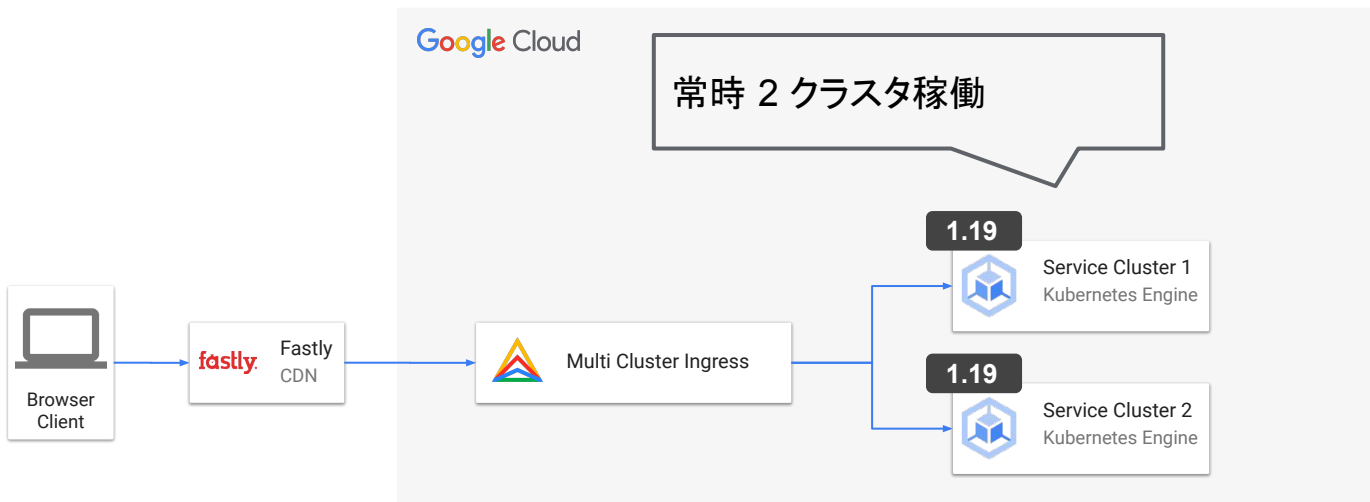
Multi Cluster Ingress | Solution



- 現状は Canary Upgrade を実現できず...
 - 現状の Multi Cluster Ingress はシンプルなラウンドロビンのみ
- マルチクラスタ化 x Rolling Upgrade で擬似的に要求を満たせる
 - 詳しいメンテナンスのフローは後述

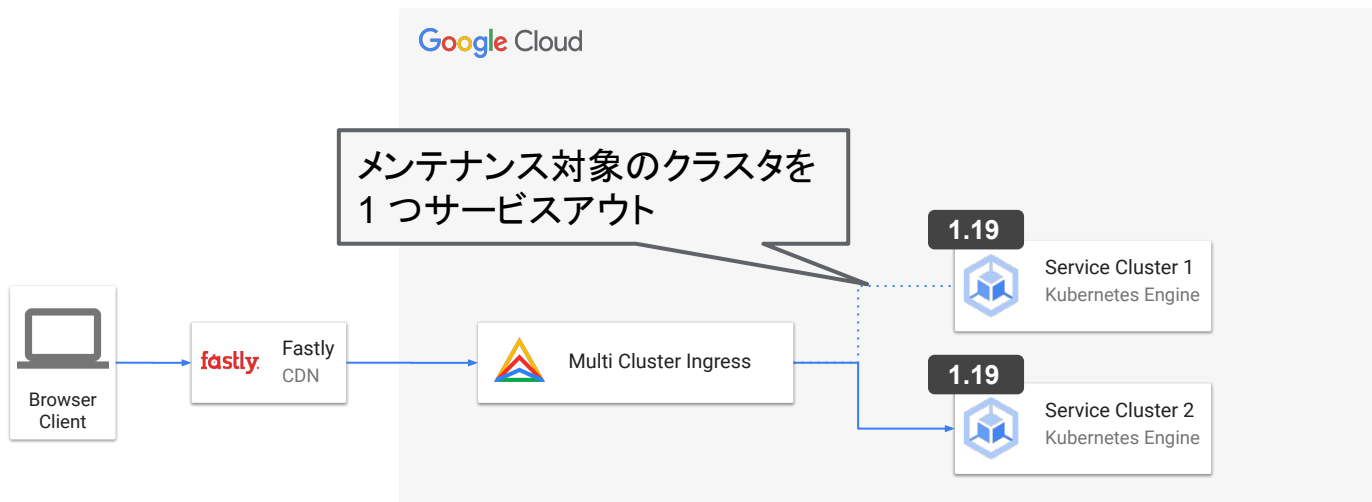
Multi Cluster Ingress | Solution

Rolling Upgrade Flow



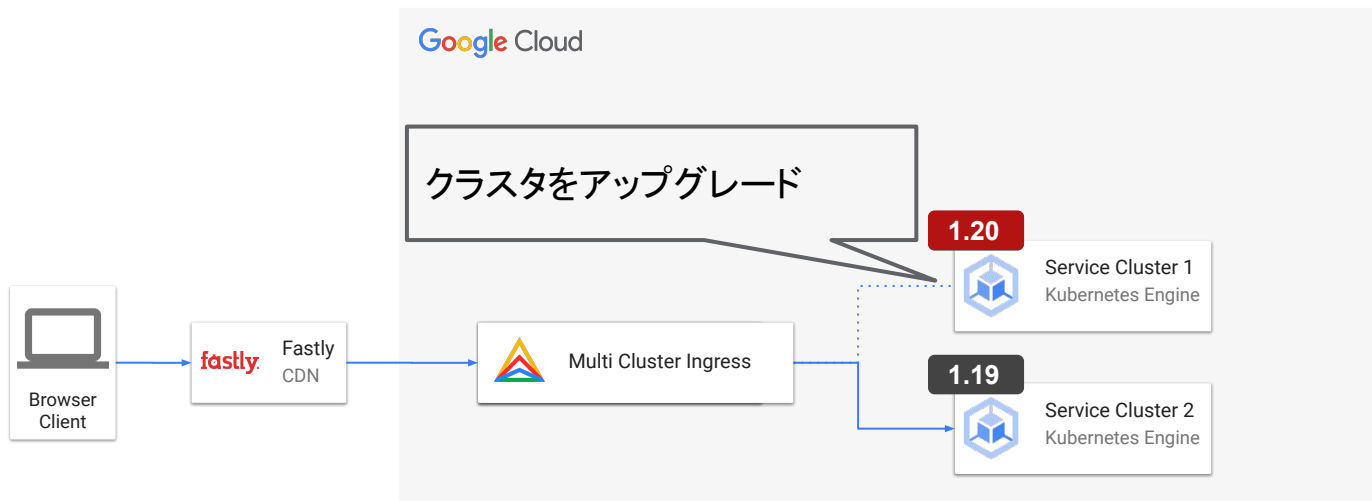
Multi Cluster Ingress | Solution

Rolling Upgrade Flow



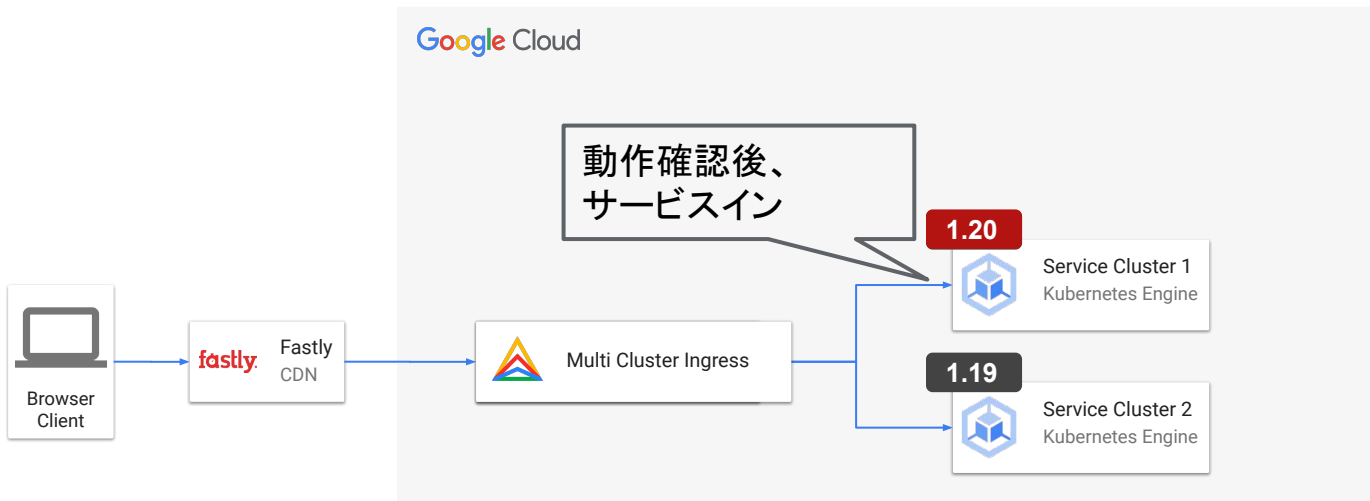
Multi Cluster Ingress | Solution

Rolling Upgrade Flow



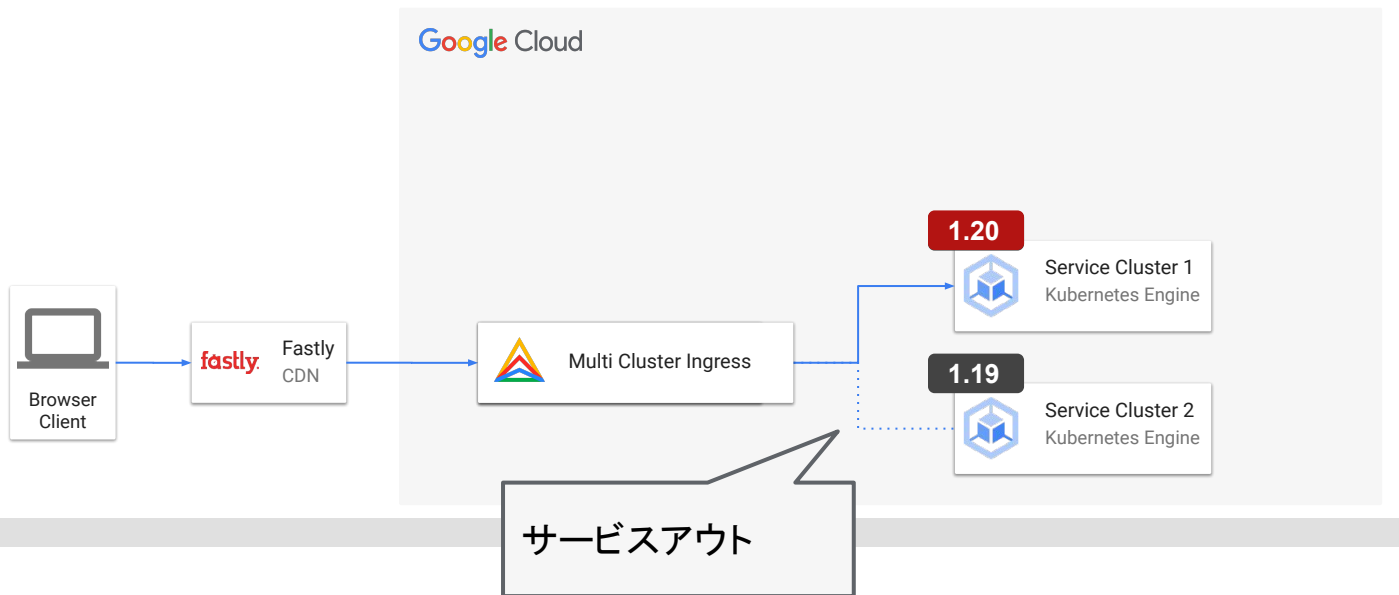
Multi Cluster Ingress | Solution

Rolling Upgrade Flow



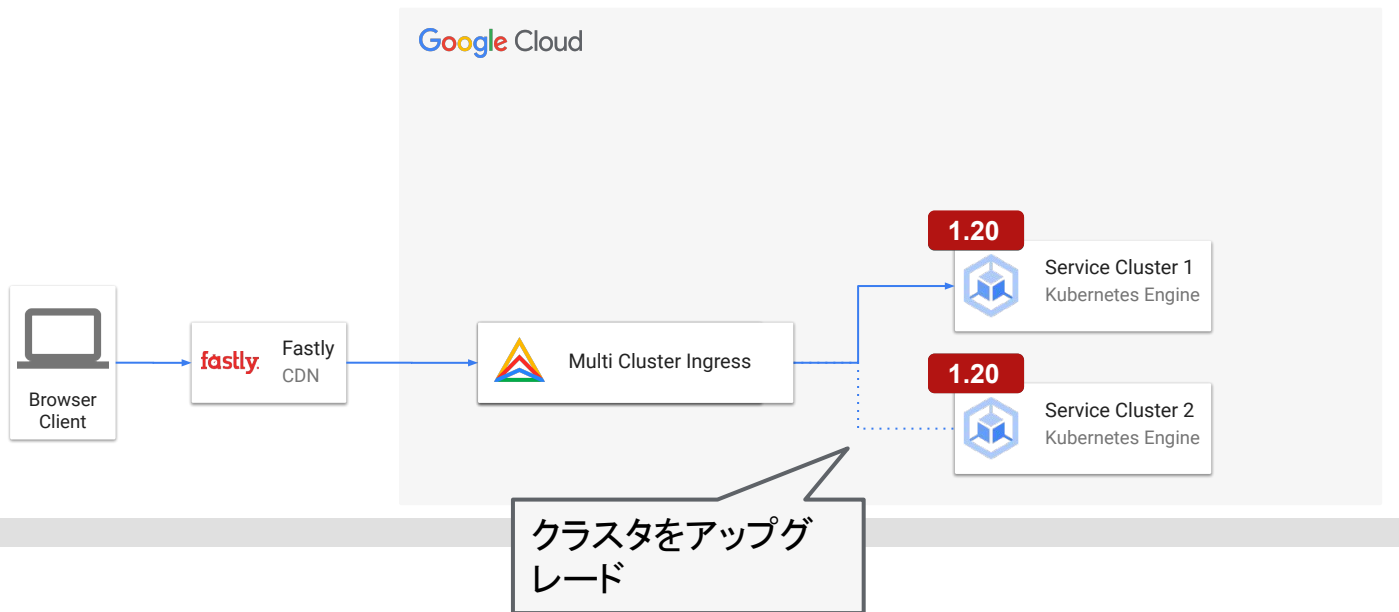
Multi Cluster Ingress | Solution

Rolling Upgrade Flow



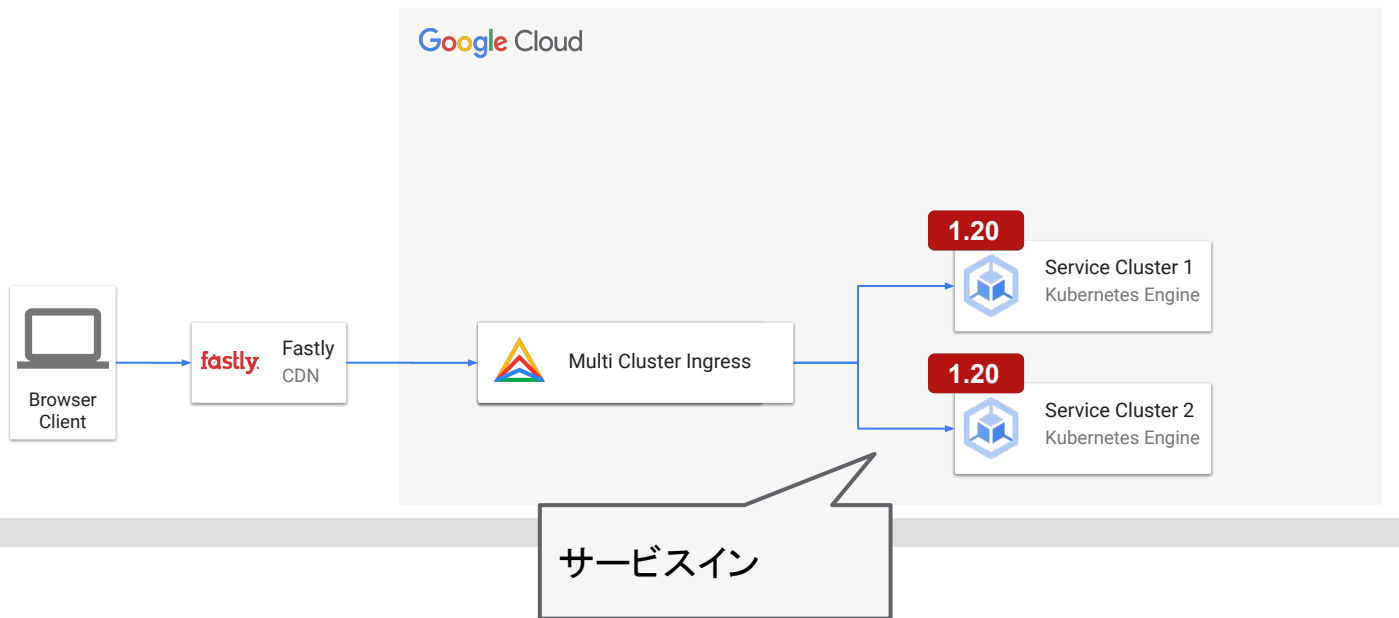
Multi Cluster Ingress | Solution

Rolling Upgrade Flow



Multi Cluster Ingress | Solution

Rolling Upgrade Flow

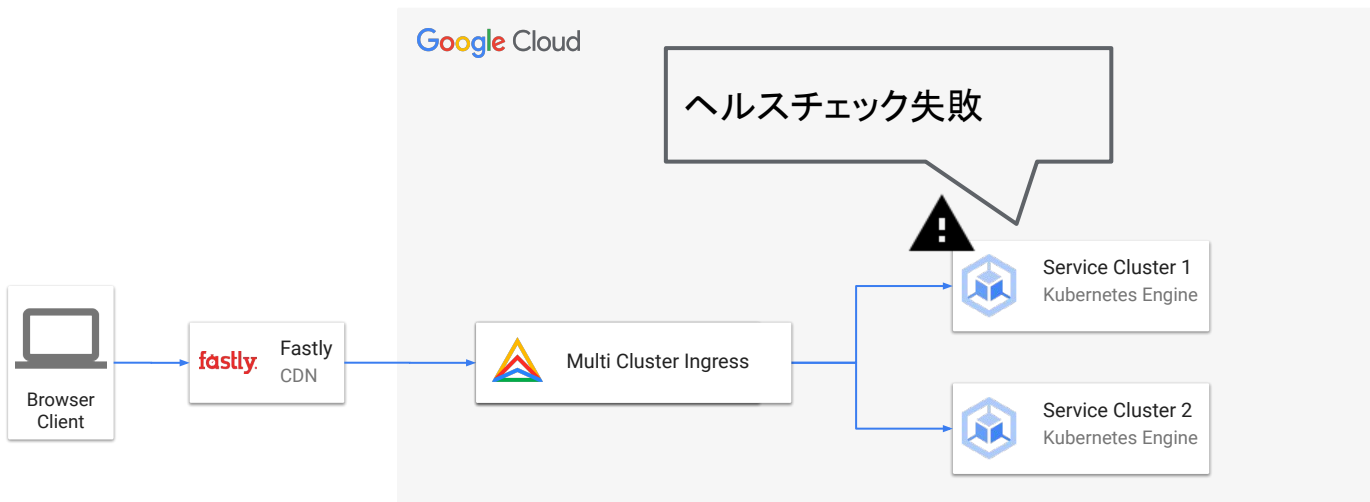


Multi Cluster Ingress | Result

- クラスタを Rolling Upgrade できるようになった
 - メンテナンス時に対象クラスタの切り離しが可能
 - GKE のアップグレードはある程度 In Place Upgrade で実施できるが、Istio などの主要コンポーネントの更新作業も Rolling で実施でき、安全性が高まった
- DNS 切り替えなどでは実現できない Failover の機能も実現
 - Load Balancer のヘルスチェックが失敗するとルーティングから外される
 - マルチリージョンでクラスタを展開することで耐障害性が向上

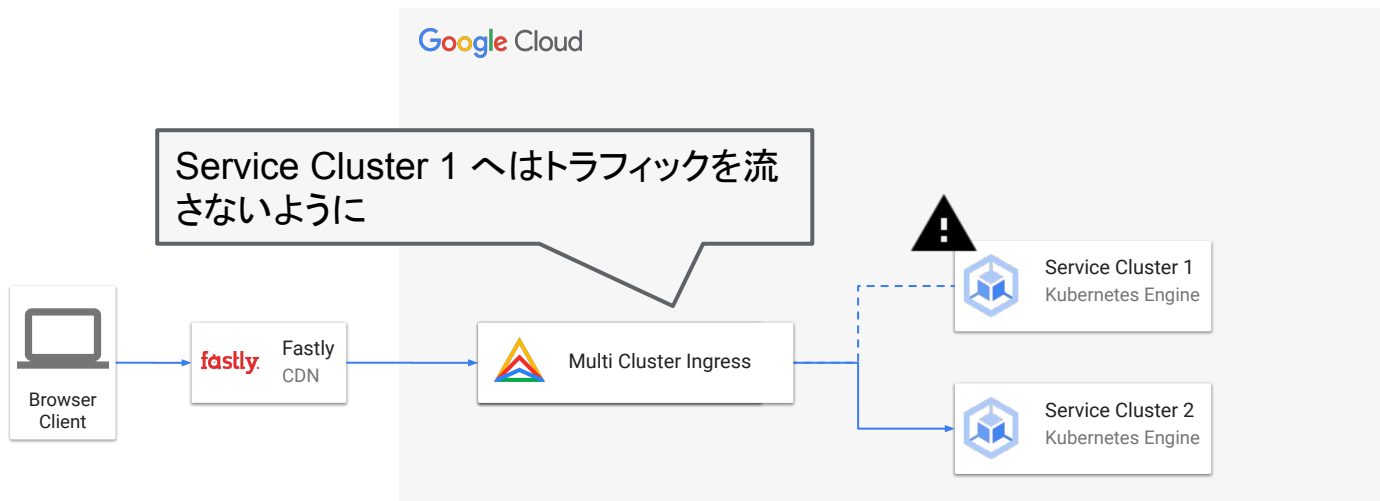
Multi Cluster Ingress | Failover

Failover



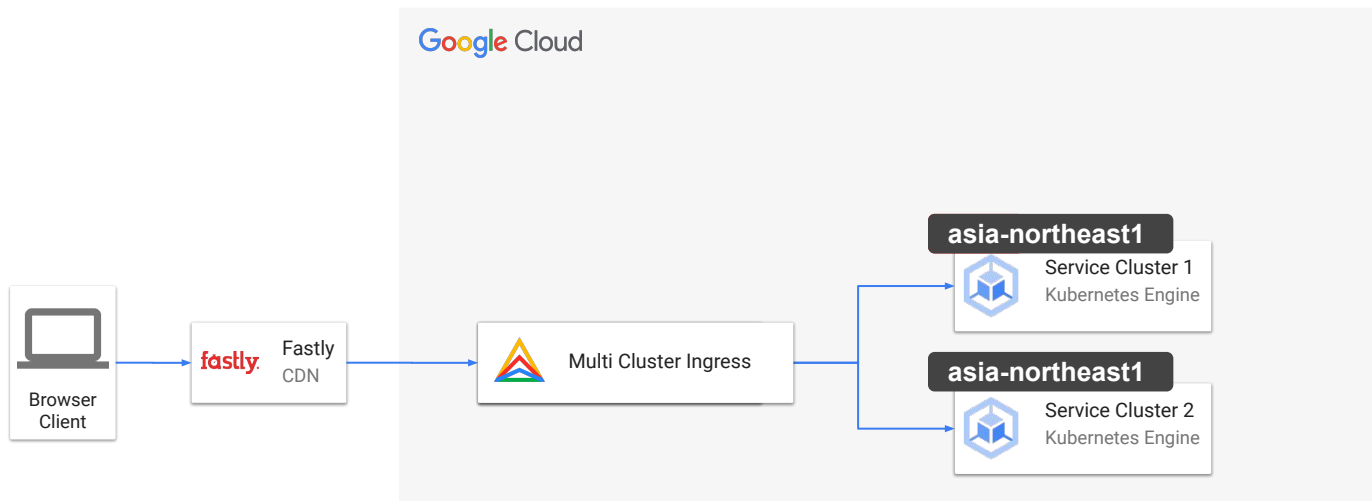
Multi Cluster Ingress | Failover

Failover



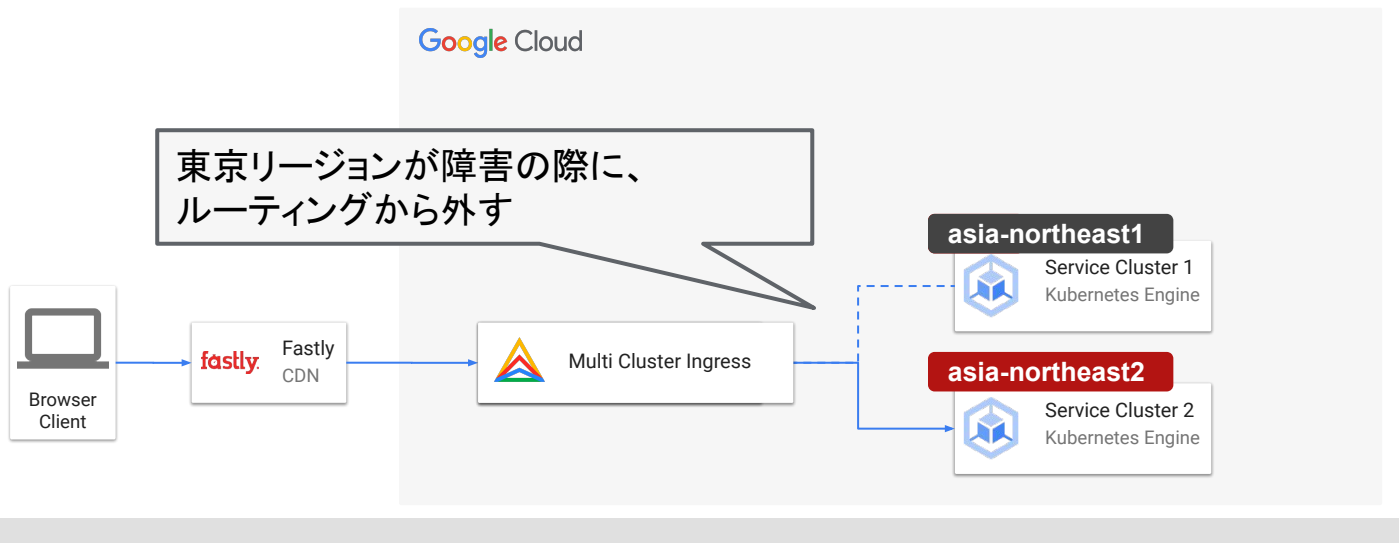
Multi Cluster Ingress | Failover

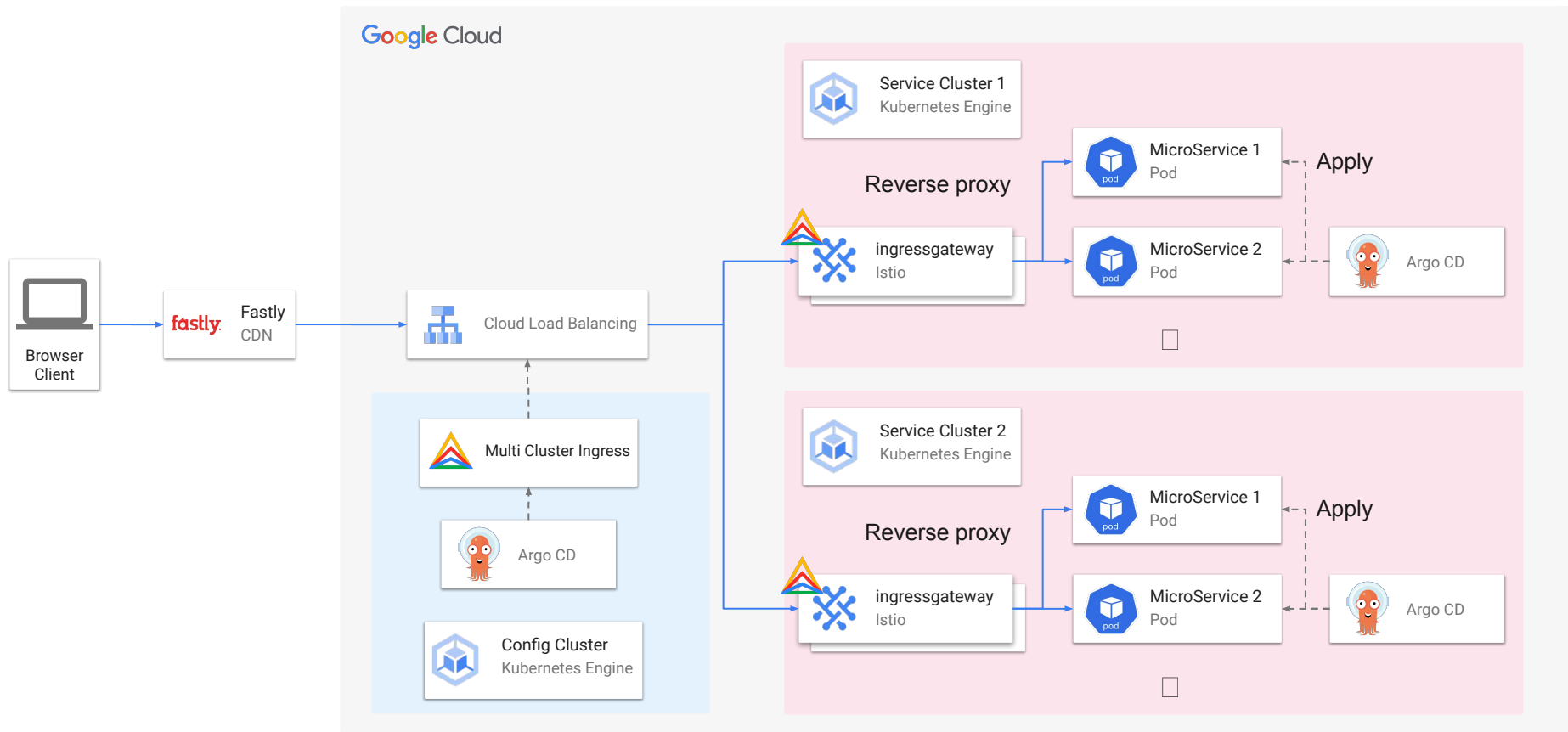
Failover

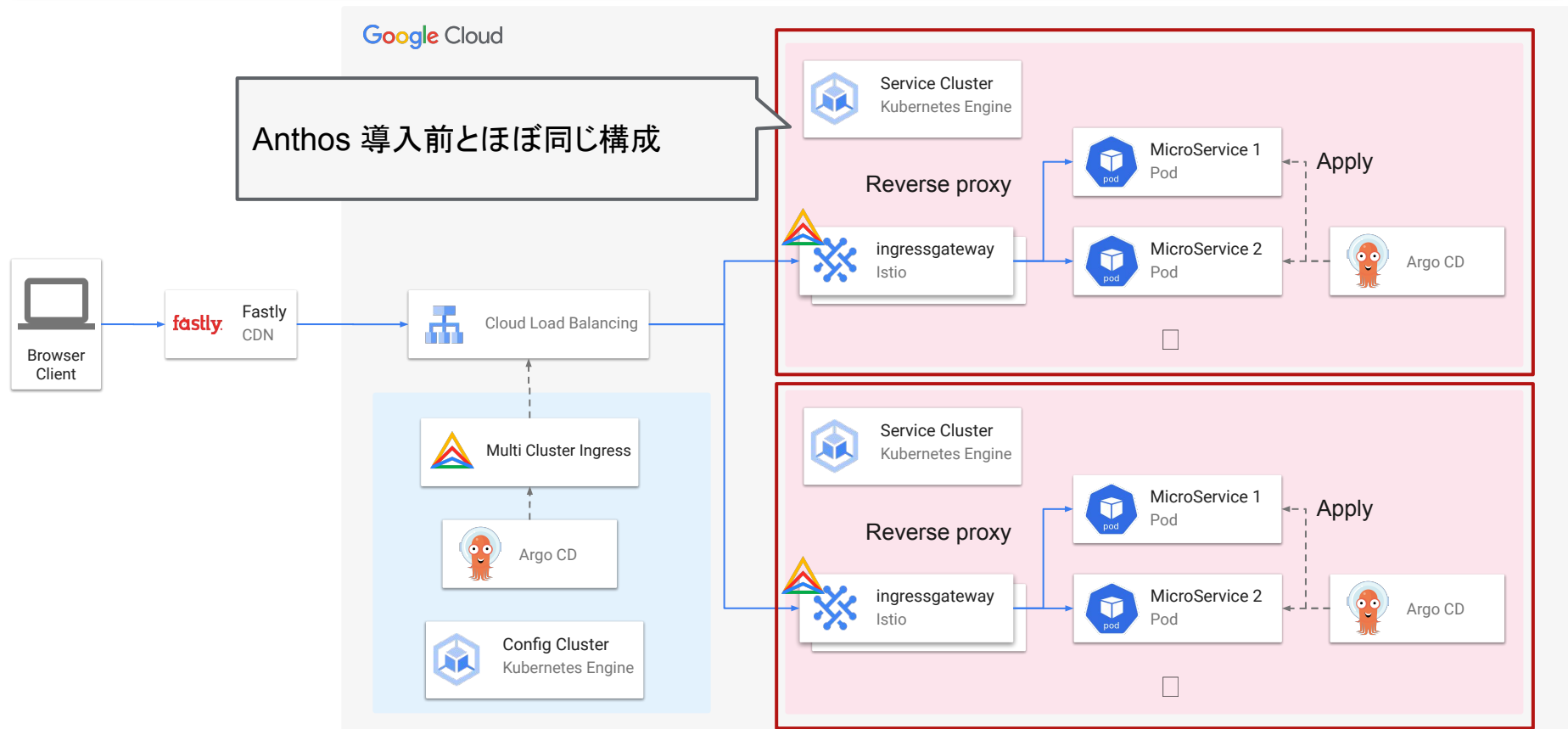


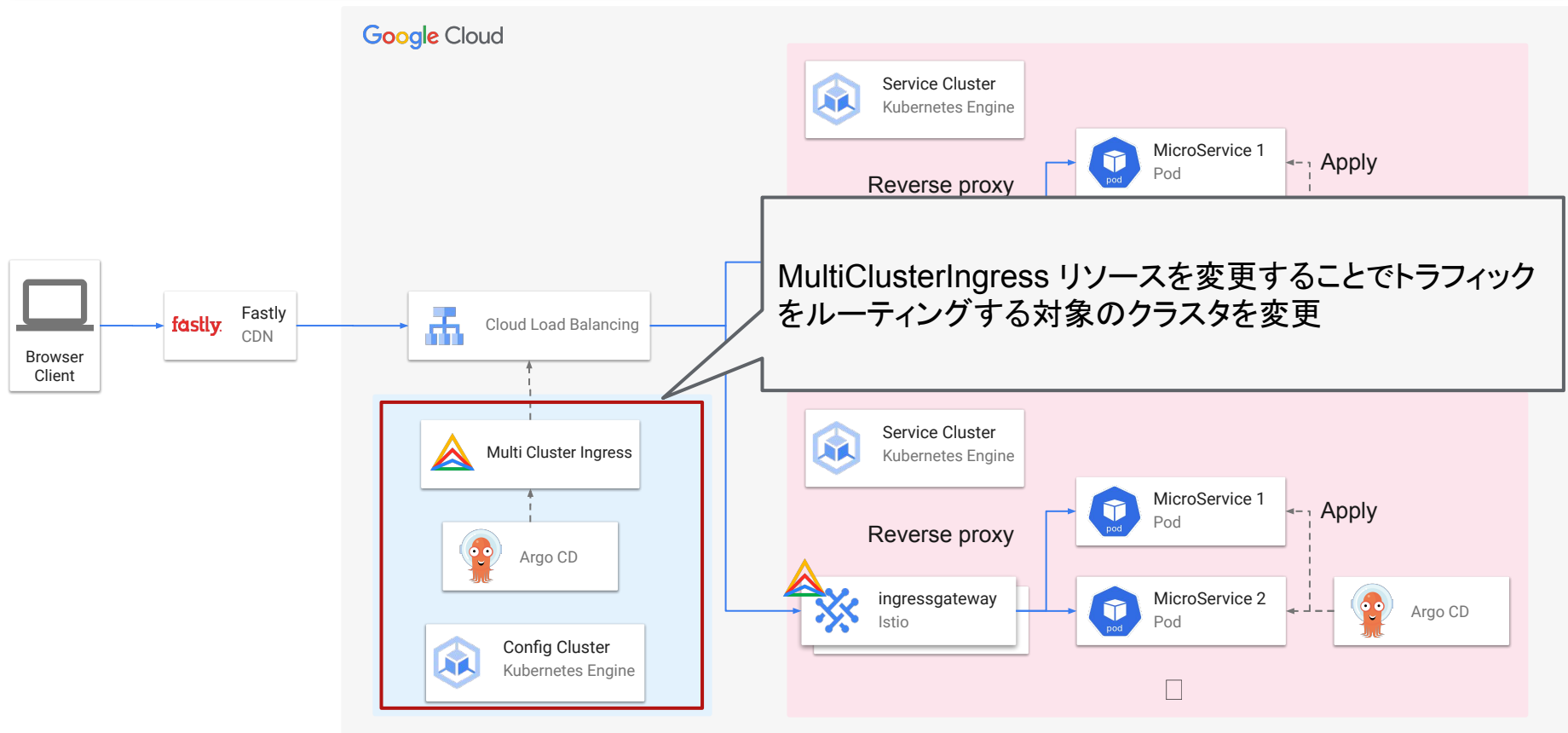
Multi Cluster Ingress | Failover

Failover









Multi Cluster Ingress | Future tasks

- HTTP Host ベースのトラフィックルーティングしかできない
 - HTTP ヘッダベースでルーティングができると柔軟性が向上して嬉しい
 - e.g. クラスタ名をヘッダで指定してルーティング
- YAML apply から実際のルーティング (LB) への反映に数分かかる
- シンプルなラウンドロビンのみ対応
 - Weighted Routing ができれば本当の Canary Upgrade が可能に
- Config Cluster が落ちるとルーティングの制御ができなくなってしまう

ここまでのまとめ

- GKE 基盤の運用における課題
 - 安全なクラスタメンテナンスの仕組みが必要
- Multi Cluster Ingress の導入
 - クラスタの Rolling Upgrade が可能に

他にも Anthos のプロダクトを導入

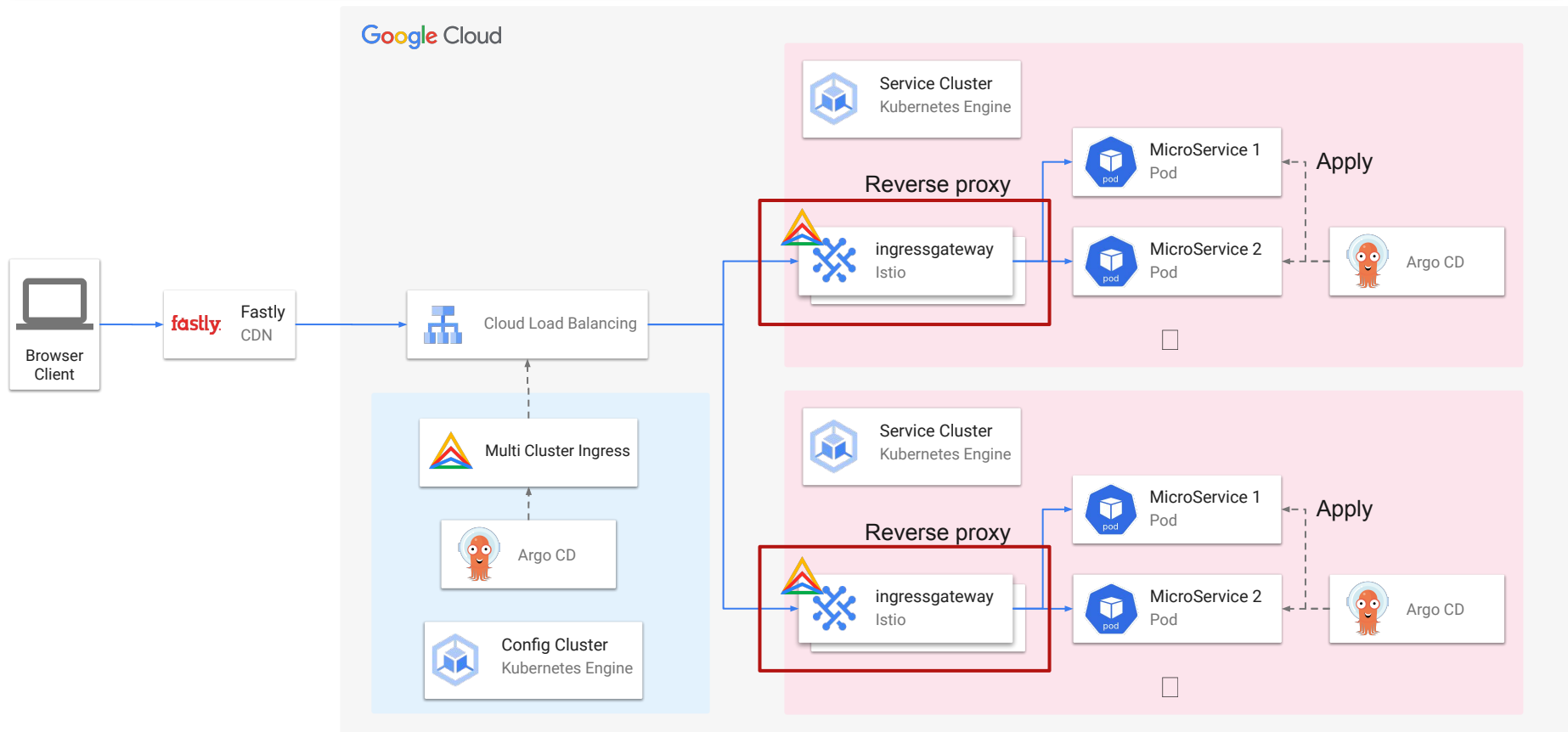
Anthos ライセンスをサブスクライブすると、他の Anthos Product も利用でき、運用改善のために導入したものを2つ紹介します。

- Anthos Service Mesh
- Config Connector

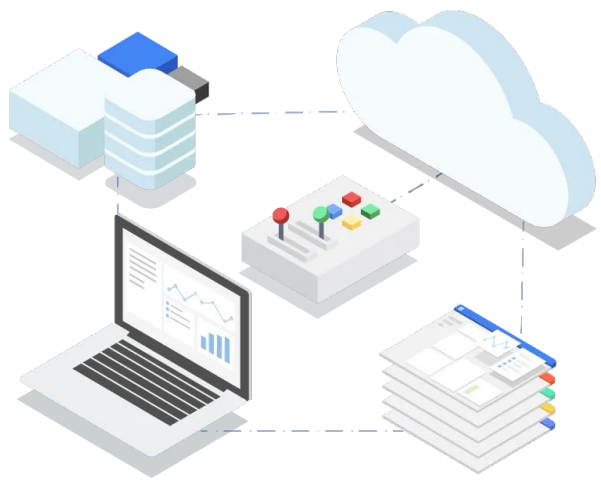




Anthos Service Mesh



Anthos Service Mesh



Anthos Service Mesh は、オンプレミスまたは Google Cloud で信頼性の高いサービス メッシュをモニタリングし、管理するのに便利な一連のツールです。

出典 : <https://cloud.google.com/anthos/service-mesh>

Anthos Service Mesh

- もともと Istio を利用していたので、運用コストを下げるために Managed Istio という位置づけで導入
 - 当時はサービスメッシュ内の証明書管理を移譲できたり、Cloud Monitoring/Logging との統合が主なメリット
 - 加えて導入時 Google-managed Control Plane が Beta だったりと、今後の機能拡充に期待して導入

Anthos Service Mesh | Result

- Istio 運用のコストが減った
 - Google-managed Control Plane にするとアップグレードも自動化可能になる
 - サービスメッシュに関してGoogle Cloud の サポートを受けられる(かなり重要)

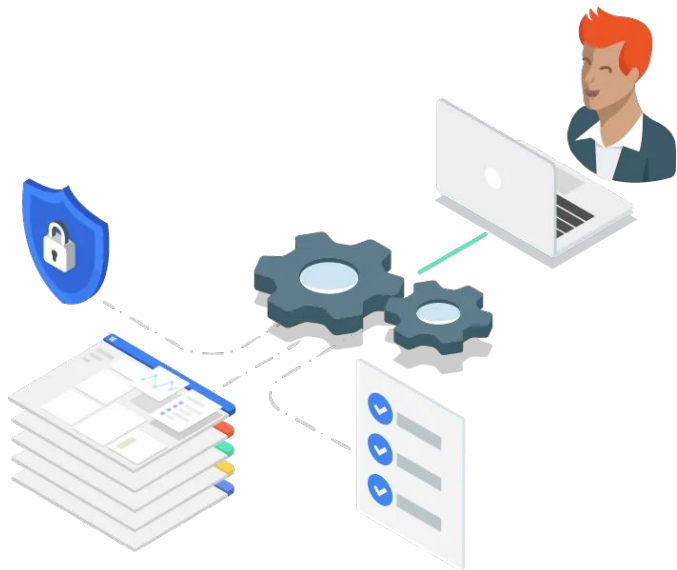
Anthos Service Mesh | Future tasks

- 本家 istio では修正されているような不具合を踏んでしまうことも...
- Setup が Script である
 - YAML を Git レポジトリで格納するのが難しい
 - GitOps との親和性が高いとは言えない
- 「HTTP ヘッダをログに含める」などの細かいカスタムはできない
 - マネージドの制約なので仕方ない
 - 必要な Pod には Nginx を Sidecar として組み込んで対応している



Config Connector

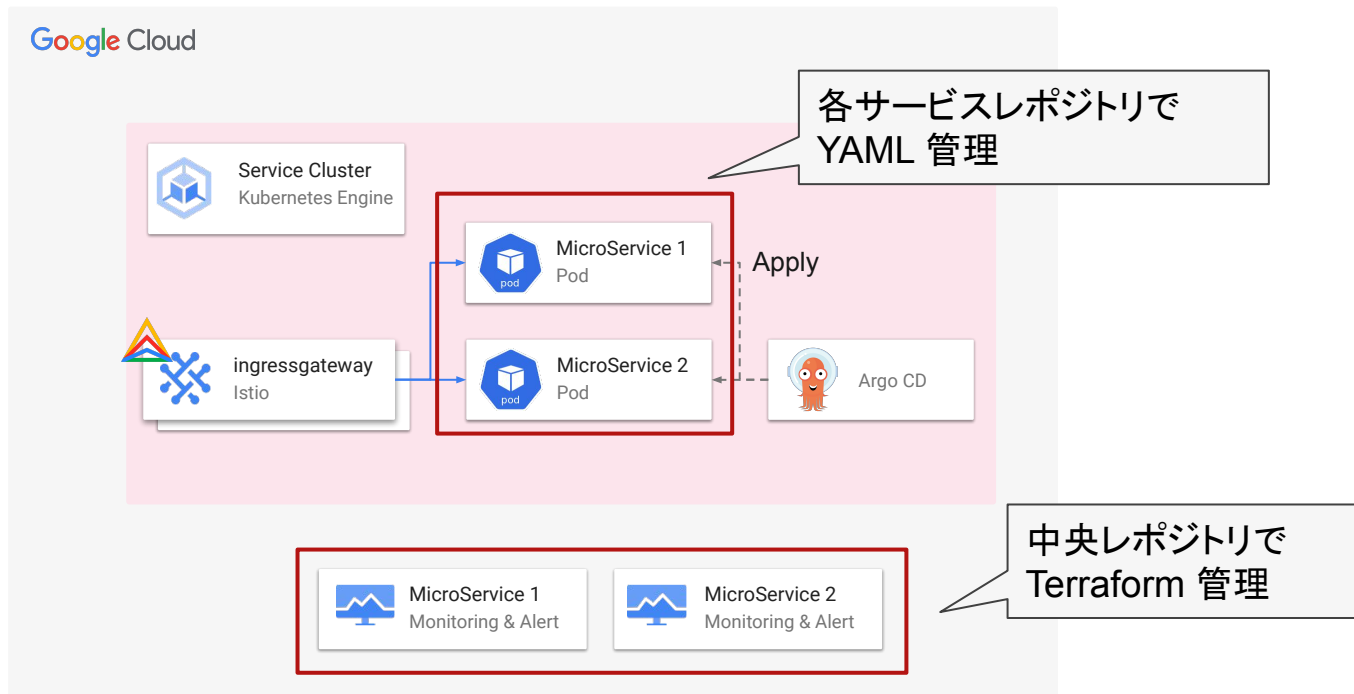
Config Connector



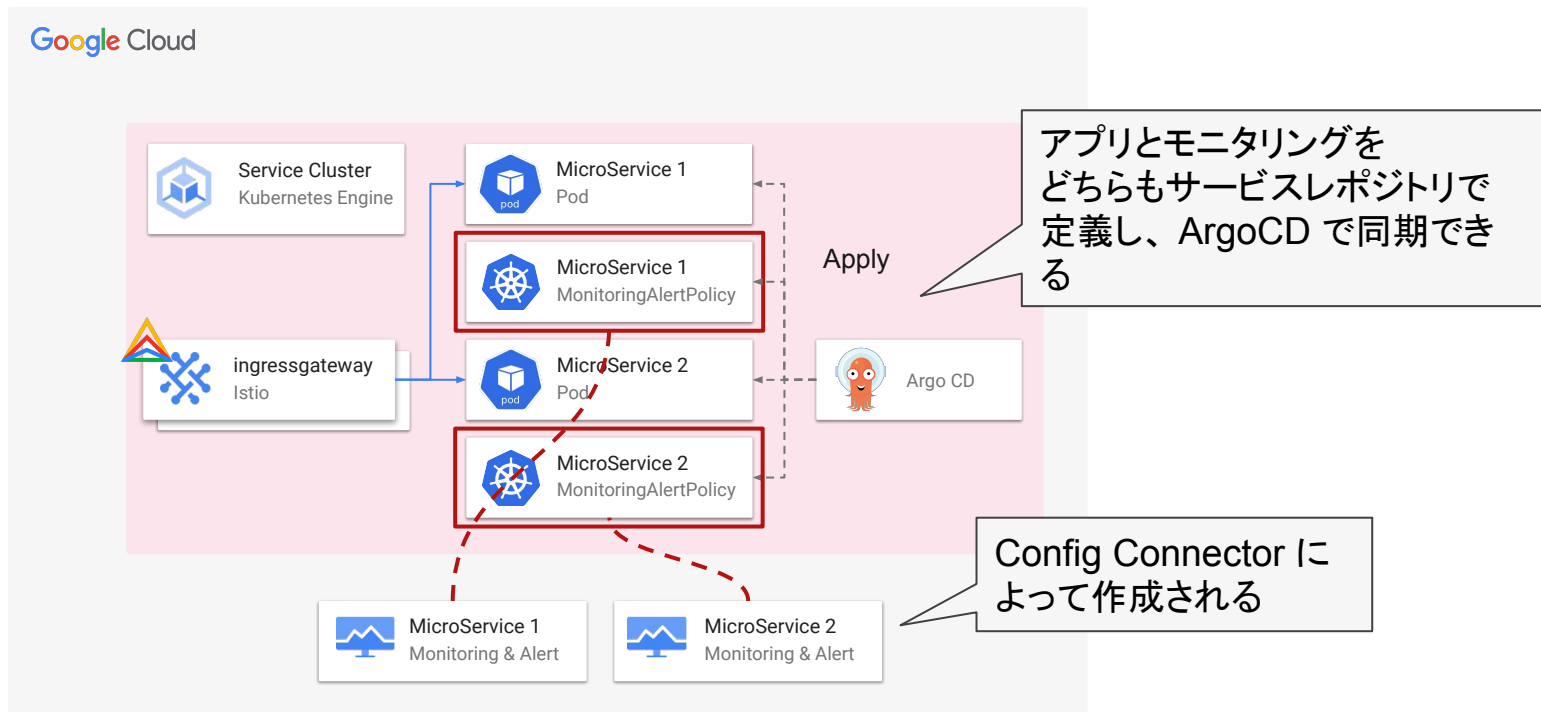
Config Connector は、Kubernetes を介して
Google Cloud リソースを管理できる
Kubernetes アドオンです。

出典 : <https://cloud.google.com/config-connector/docs/overview>

Config Connector | 導入前のリソース管理



Config Connector | 導入後のリソース管理



Config Connector | Results



- アプリケーションレポジトリに YAML 定義を追加すると GitOps 的に監視を追加できる
 - アプリケーションリソースと同じレイヤで管理できて把握がしやすい

Config Connector | Future tasks



- よりコアなクラウドリソースに Config Connector を利用できないか検討する
 - IAM・DB など



まとめ

まとめ

- GKE 基盤の運用における課題
 - 安全なクラスタメンテナンスの仕組みが必要
- Multi Cluster Ingress の導入
 - クラスターの Rolling Upgrade が可能に
- 運用改善のために Anthos プロダクトを導入
 - Anthos Service Mesh
 - Istio の運用負荷が軽減
 - Config Connector
 - クラウドリソースを GitOps 的に管理できるように

We're Hiring!

- SRE チームメンバー募集中
- 興味がある方は、
 - Twitter (@nikkeideveloper) に DM
 - 技術ブログ・採用サイト: <https://hack.nikkei.com/>
- カジュアル面談大歓迎
 - <https://herp.careers/v1/nikkei>

一緒に日経電子版の基盤をより良いものにしていきましょう!!



Thank you.