Google Cloud

# 数百のプロジェクトに跨がった
# 請求システムをセキュアに運用する方法


松原 優

株式会社 grasys

Cloud infrastructure Division

Ops Team Leader

草間 一人

HashiCorp Japan 株式会社

Senior Solutions Engineer

# スピーカー自己紹介

松原 優
株式会社grasys
Cloud infrastructure Division
Ops Team Leader

2020年5月に grasys へ入社。現在はプレイヤーとしてインフラ構築・運用をしつつメンバーのサポートを行っている。

grasys 入社以前はゲーム業界でフロントエンドやバックエンドの開発に関わる。

# 会社紹介


grasys

gracias + system

「もっと強固なインフラに」

| | |
|---|---|
| 社名 | 株式会社 grasys |
| 創業日 | 2014 / 11 / 13 |
| 代表 | 長谷川 祐介 |
| 資本金 | 1,000 万円 |
| 社員数 | 40 名 |
| 所在地 | 恵比寿 |

# 事業規模

| | |
|---|---|
| エンドユーザー数 | 累計 3 億超ユーザー |
| クラウド プロジェクト数 | 200 プロジェクト |
| VM インスタンス運用実績 | 4,500 台／月 |
| 最大稼働インスタンス数 | 2,200 インスタンス／システム |
| 1 秒間のリクエスト回 | 200 万回／秒 |
| ビッグデータの分析基盤 | 120 兆レコード／日 |
| データ ストリーミング分析 | 2,000 ノード |
| 分散データベース | 280 ノード |

# パートナー

grasys

Google Cloud

HashiCorp

PF 統合管理

elastic

検索・監視・セキュリティ

fastly

超高機能・高速 CDN

paloalto NETWORKS

セキュリティ PF

Looker

データ分析 PF

# grasys の取り組み

grasys

## 攻めのインフラ

オーケストレーションを母体とし

運用を意識したシステム設計・構築

作業効率の向上



# 請求システムについて

# なぜ請求システムが必要だったのか

- Google Cloud プレミア Service パートナーとして 200 を超えるプロジェクトを管理
- プロジェクト毎の使用リソースを元に運用費計算

自動システム化

# なぜ請求システムが必要だったのか

- インフラの会社だからこそ社内のインフラは運用したくない
- 運用コストを下げたい

Google Kubernetes Engine

# なぜ請求システムが必要だったのか

- 顧客情報を含むデータの通信
- dynamic に認証情報を生成したい

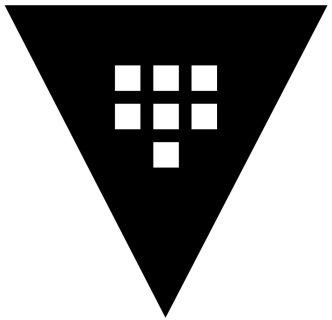
HashiCorp Vault を利用した

セキュアなシステム

# HashiCorp Vault とは

ざっくりと

API の暗号化キー、パスワード、証明書データベース
クレデンシャル といった情報を安全に管理できます。

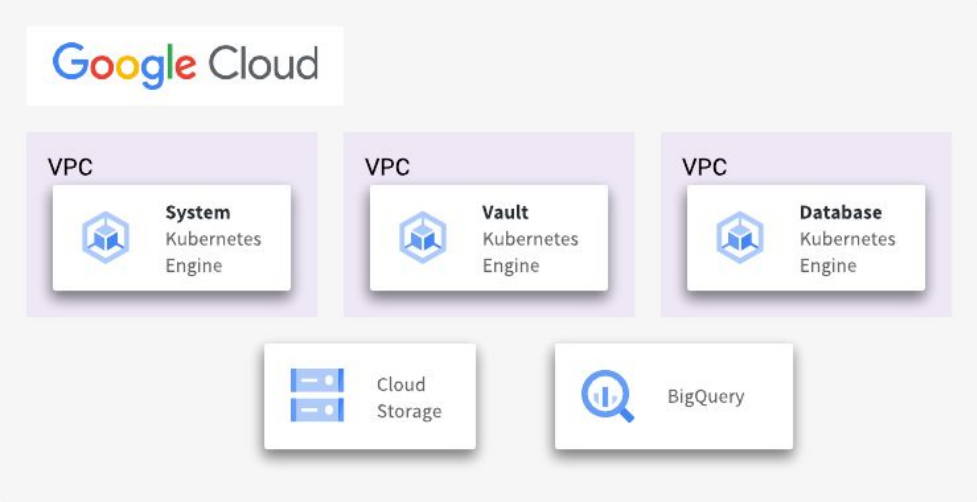


HashiCorp
Vault

# 請求システムの構成と HashiCorp Vault の利用事例

# 請求システムの全体構成

1. 請求システム用 / Vault 用 / Database 用の3つの Kubernetes Engine
2. Cloud Storage
3. BigQuery
4. クラスターは互いに VPC Peering によって接続



# 請求システムの処理の流れ

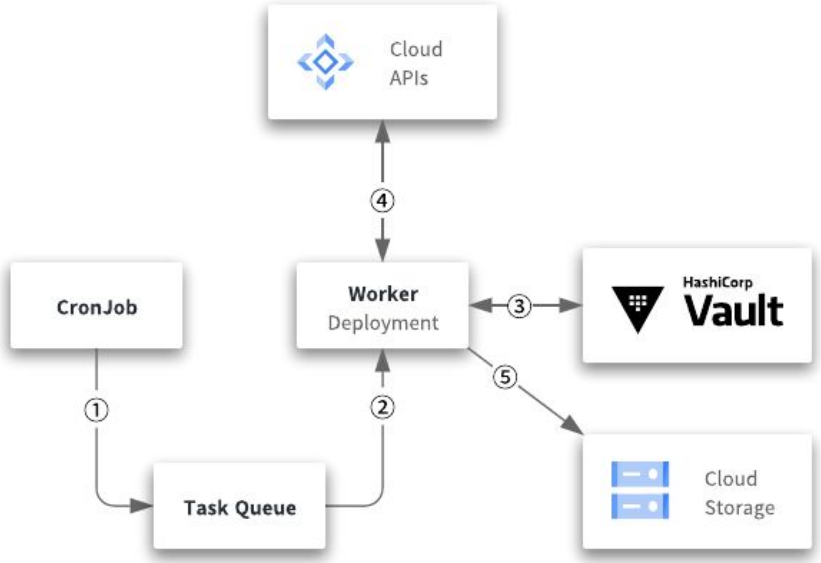
01 | プロジェクトのリソース情報の取得

02 | プロジェクトのリソース情報を CRM へ

03 | CRM から帳票管理サービスへ

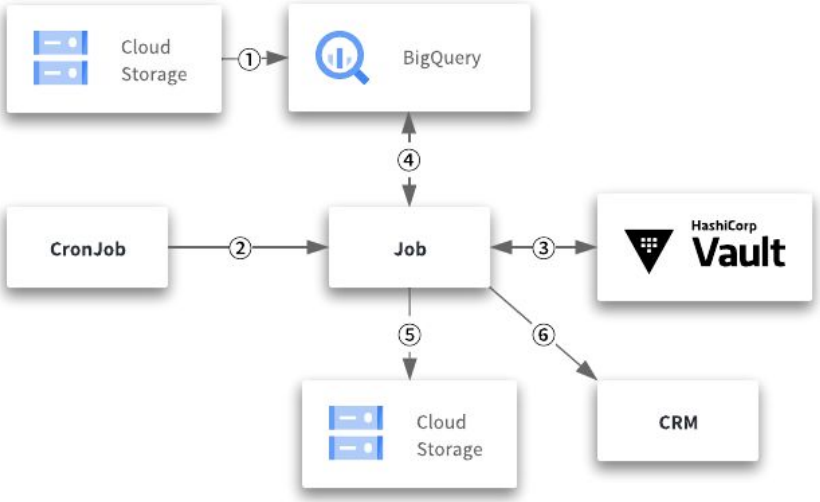
# プロジェクトのリソース情報の取得

1. CronJob による定期実行
2. Task Queue から Job 取得
3. Vault で Google Cloud サービスアカウントのトークン取得
    a. Google Cloud Secrets Engine
4. Cloud APIs へ問い合わせ
5. Cloud Storage にアップロード



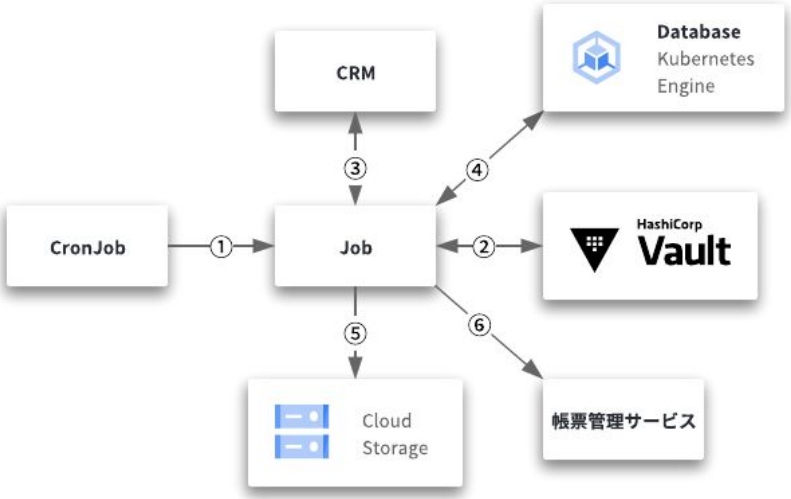
# プロジェクトのリソース情報を CRM へ

1. Cloud Storage から BigQuery にデータをロード
2. CronJob による定期実行
3. Vaultでトークン発行
    a. KV Secrets Engine
4. BigQuery から集計データ取得
5. Cloud Storage にアップロード
6. CRM REST API



# CRM から帳票管理サービスへ

1. CronJob による定期実行
2. Vault でトークン発行 / クレデンシャル生成
    a. KV Secrets Engine
    b. Database Secrets Engine
3. CRM REST API
4. DataBase からマスターデータの取得
5. Cloud Storage にアップロード
6. 帳票管理サービス REST API



# Google Kubernetes Engine と

# HashiCorp Vault を使って

# セキュアな請求自動システムを運用

# 運用してみて

- 先日トラブルが発生、それまではメンテなしで運用できていた
- 運用コストを下げることに成功

# よりコストダウンするための方法

- プリエンプティブル VM
- Spot VM ( pre-GA )
- Google Kubernetes Engine Autopilot
  - Spot Pod

実際に動くところ、
見てみたいですよね？

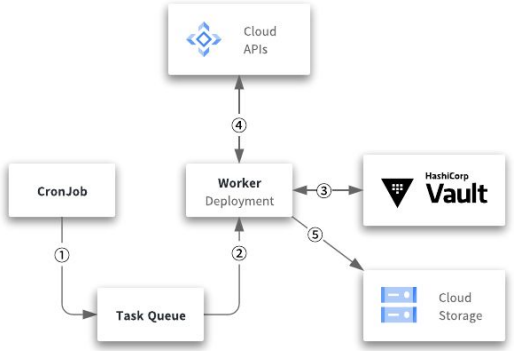
# ここからは、わたしがお話します

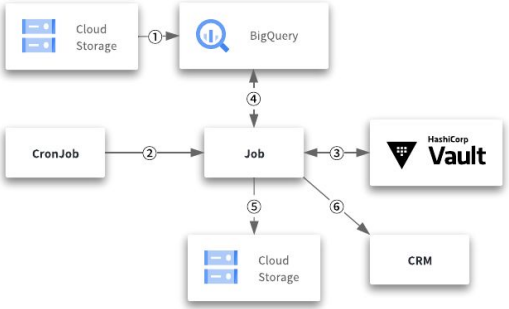

草間 一人
HashiCorp Japan 株式会社
Senior Solutions Engineer

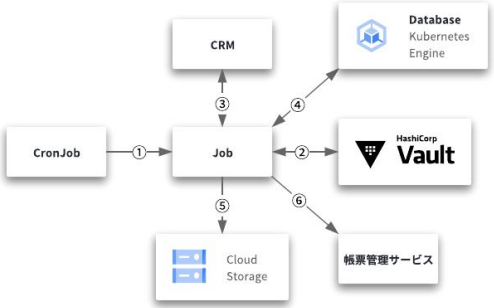
HashiCorp の Senior Solutions Engineer として、Terraformや Vault、Consul などのプリセールスに携わるエンジニア。

プライベートの活動として、日本最大のクラウドネイティブ技術の カンファレンス CloudNative Days の Co-Chair も務めています。

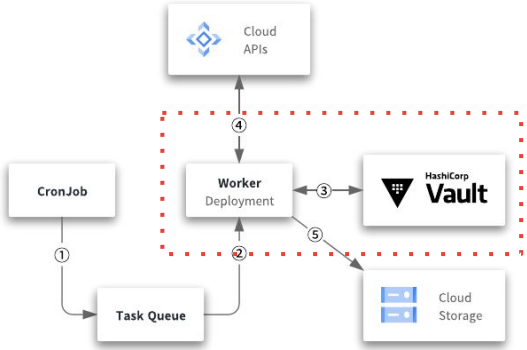
# 再掲

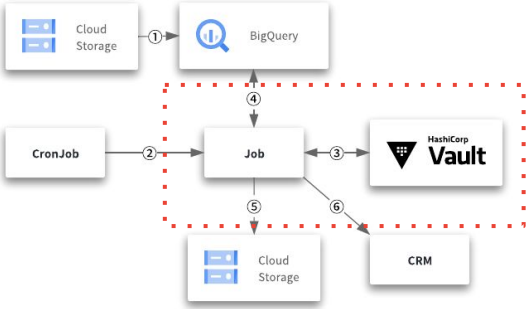

Cloud APIs
CronJob
Worker Deployment
HashiCorp Vault
Task Queue
Cloud Storage
①
②
③
④
⑤

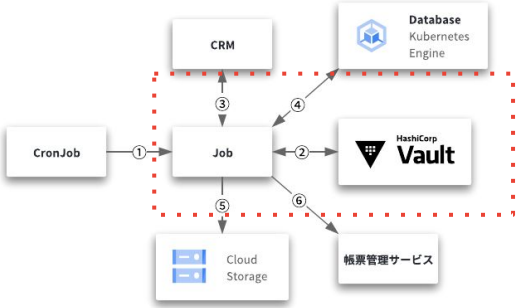

Cloud Storage
BigQuery
CronJob
Job
HashiCorp Vault
Cloud Storage
CRM
①
②
③
④
⑤
⑥


CRM
Database Kubernetes Engine
CronJob
Job
HashiCorp Vault
Cloud Storage
帳票管理サービス
①
②
③
④
⑤
⑥

# 再掲


Cloud APIs
CronJob
Worker Deployment
HashiCorp Vault
Task Queue
Cloud Storage


Cloud Storage
BigQuery
CronJob
Job
HashiCorp Vault
Cloud Storage
CRM


CRM
Database Kubernetes Engine
CronJob
Job
HashiCorp Vault
Cloud Storage
帳票管理サービス

動画あり：視聴ページをご覧ください

# Thank you.

Google Cloud