



アカツキ流 セキュリティ監査自動化

400 個以上の Google Cloud プロジェクト監査を
自動化したノウハウを一挙公開

駒井 祐人

株式会社 アカツキゲームス


スピーカー自己紹介



駒井 祐人

アカツキゲームス

Server Engineering TechLead

 @e_koma

セールスランキング上位モバイルゲームの
バックエンドエンジニアをしています

- コンテナ ネイティブなシステム構築
- 大規模負荷対策
- クラウド セキュリティ強化

のような非機能要件充実化を得意としています



ラフロイグが好きです

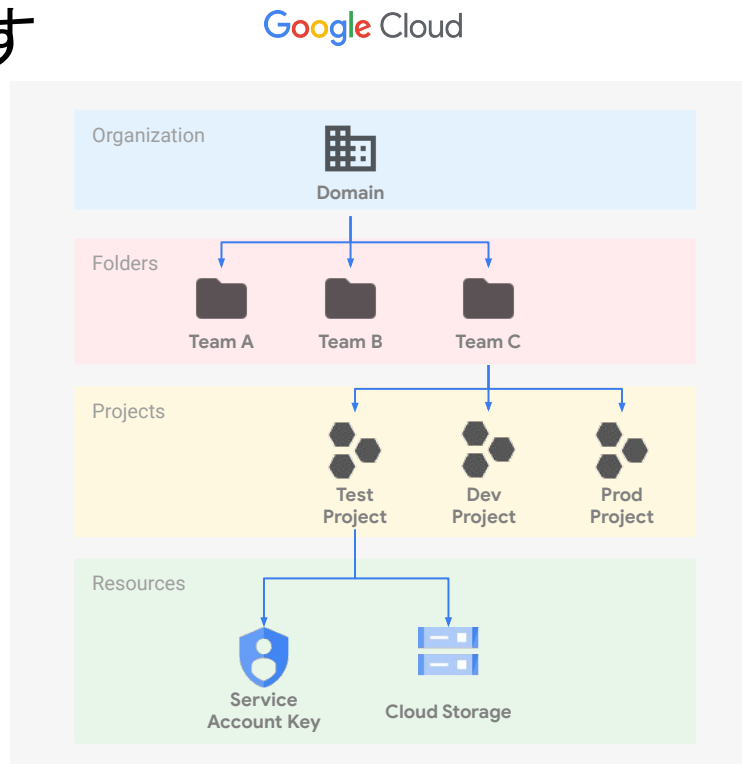


いきなりですが、質問です

組織の中に数百個の Google Cloud プロジェクトがあります

Question 1

全 Google Cloud プロジェクトの中で、
サービスアカウントキーが何個発行されていて
いつからローテーションされていないか
把握できますか？

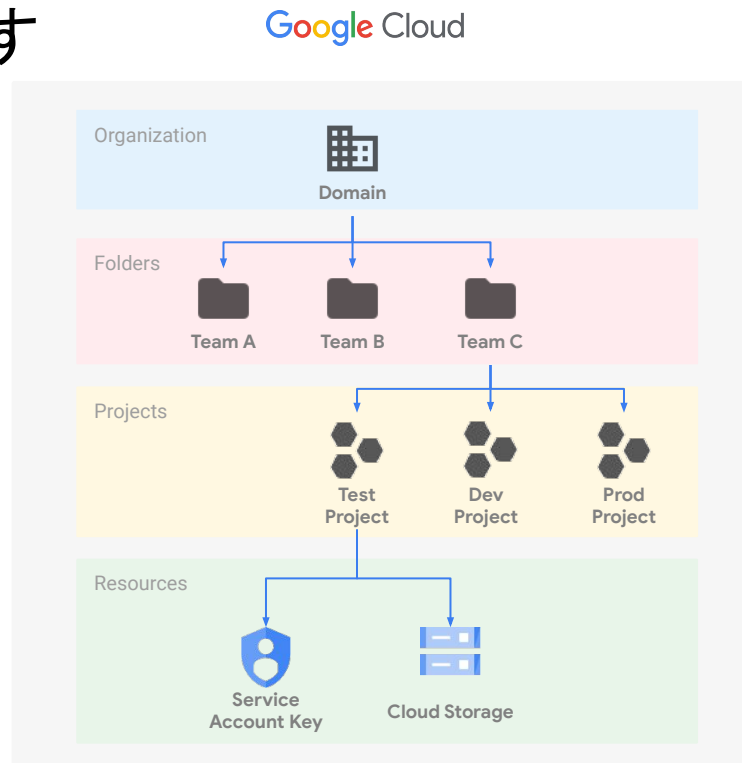


組織の中に数百個の Google Cloud プロジェクトがあります

Question 2

一般公開されてしまっている

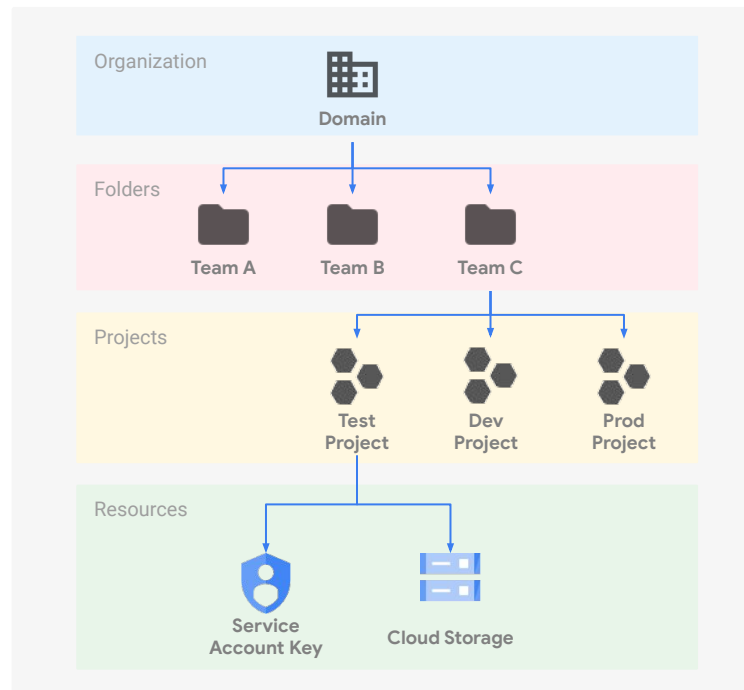
Cloud Storage バケットを検知できますか？



組織の中に数百個の Google Cloud プロジェクトがあります

Question 3

利用頻度の低いGoogle Cloud プロジェクトや
利用頻度の低いCompute Engine を
検知できますか？



本セッションで話すこと

400

個以上の Google Cloud プロジェクトのセキュリティ監査を自動化した事例

具体的には

- 組織の中のサービスアカウント キーのローテーション状況を全て把握し
- 公開バケットが存在しないか自動監査し
- 利用頻度の低い Google Cloud プロジェクトを検知

これらを実現した仕組みをご紹介します

COVID-19 のクラウド セキュリティへの影響

188 %

コロナ禍でクラウドは加速したが、
セキュリティ インシデントも加速した

30 %

クラウド上の機密データを
公開したままにしている組織

出典:Unit 42 クラウド脅威レポート2021年1H

クラウドは簡単に脆弱になる

サービスアカウント キーが流出すると...

Google Cloud の不正操作が可能になる

- ・個人情報流出リスク
- ・システム停止 / 破壊リスク

公開バケットが存在すると...

Cloud Storage に置かれたデータの読み書きが可能になる

- ・データが、マルウェアを仕込まれた状態で上書きされ
ダウンロードした PC がマルウェア感染するリスク

金銭損失・顧客損失・業務停滞・従業員への影響

アカツキゲームスのクラウド セキュリティ全体像



予防

- [Security Command Center](#)
- [Forseti Security](#)
- [Recommender](#)



検出

- [CrowdStrike Falcon](#)
- [Verizon NDR](#)
- [Future Vuls](#)

※ Google Cloud が提供している脅威検出サービスもあります

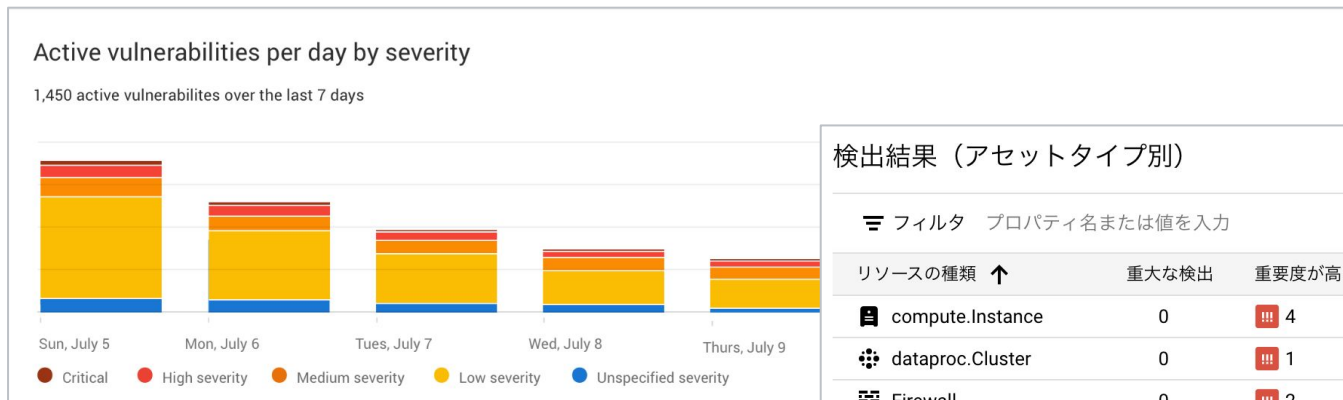


Security Command Center

Security Command Center(SCC) とは？

Google Cloud のセキュリティ管理サービス

脅威の予防 / 検出を組織一元管理



検出結果 (アセットタイプ別)

フィルタ プロパティ名または値を入力

リソースの種類 ↑	重大な検出	重要度が高い検出	重要度が中程度の検出
compute.Instance	0	4	0
dataproc.Cluster	0	1	0
Firewall	0	2	0
Folder	0	0	1
resourcemanager.Project	0	4	4
sql.Instance	0	2	0

Security Command Center(SCC) とは？

Google Cloud のセキュリティ管理サービス

脅威の予防 / 検出を組織一元管理

	Premium	Standard
アセット管理	○	○
脅威予防	○	△ (+ Forseti)
脅威検出	○	× (+ 3rd party)
費用	有料 (※)	無料

※ Google Cloud 利用料金の5% または \$25,000 の大きい方



Forseti Security

Forseti Security とは？

Google Cloud のセキュリティ監査用 OSS

- SCC Standard tier では足りない監査を補える
- 独自のカスタムルールを実装可能
- Security Command Center と統合可能

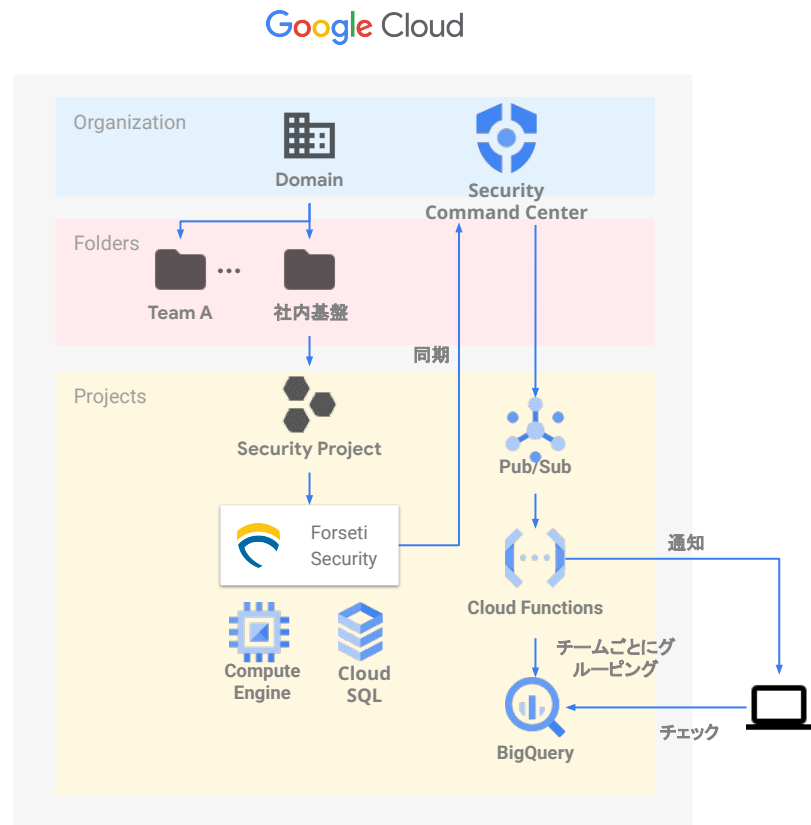


<https://forsetisecurity.org/>

Forseti Security の運用

監査サーバを運用する

- 違反結果を SCC に統合し、**一元管理**
- 1日1回通知 / 月1回の**レポート**
チームごとのビューを用意
- 実行時以外サーバ停止し、**コスト最適化**



Forseti Security で検知している一例

- IAM
 - 100 日以内に **ローテーションされていないサービスアカウント キーを検知**
 - 組織ドメイン外のユーザが IAM 権限を持っている Google Cloud プロジェクト / Google Group を検知
- Cloud Storage
 - Bucket ACL の **公開設定 (AllUsers) を検知**
- BigQuery
 - 公開データセット / gmail.com ユーザへの権限付与を検知
- Compute Engine
 - 公開イメージを検知
- Firewall
 - IP 制限なし / 全 port 許可ルールを検知

SCC Standard + Forseti Security で実現できたこと

- 400 個以上の Google Cloud プロジェクトに対して
社内セキュリティポリシーに沿った監査を自動化することができた
- Forseti のサーバ費は 月 4 万円 程度

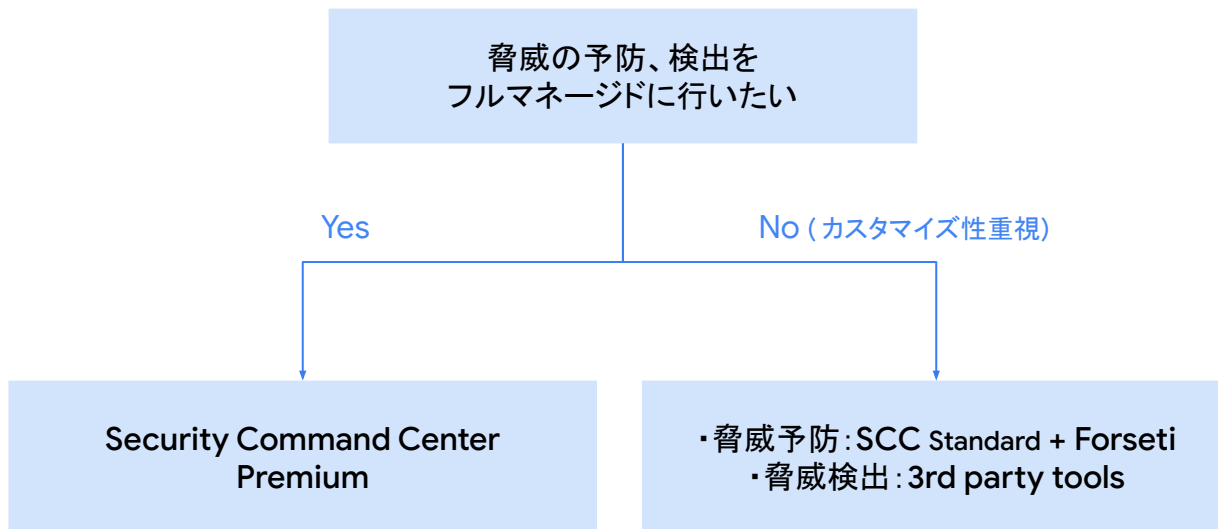
Forseti を利用する際の注意

 メンテナンスが怪しい箇所が多々あります

 OSS に細かい修正を加えた Terraform module を公開しています

- <https://registry.terraform.io/modules/e-koma/forseti/google/latest>
- ※ Upstream には何度か修正提案してます

どのサービスを利用すればよいか？





Recommender

Recommender とは？

いわゆる、推奨事項

- 地味にダッシュボードの横にあります
- 利用頻度が低い
Google Cloud プロジェクトは
検知しようがないので組織一括で検知する



The screenshot shows the Google Cloud Platform interface with the '推奨事項' (Recommendations) tab selected. A notification states that IAM permissions are required to view recommendations. A recommendation card for '未使用の Compute Engine リソース' (Unused Compute Engine resources) is displayed, indicating a cost saving of \$1.05/month. The card includes a link to delete disks and a 'すべて表示' (Show all) button.

Google Cloud Platform

ダッシュボード アクティビティ **推奨事項**

関連する IAM 権限がない場合、このプロジェクトに利用できるすべての推奨事項が表

\$ 未使用の **Compute Engine** リソース コストの節約

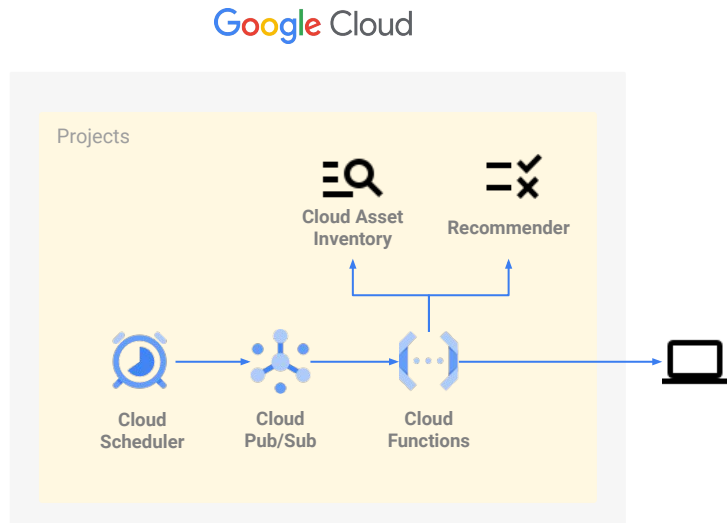
未使用のリソースをバックアップしてから削除して、費用を削減します。 **\$1.05/月**
見積もり

[ディスクを削除してコストを削減 \(削減額: \\$0.72/月\)](#)
他 3 件

→ [すべて表示](#)

Recommender の運用

- Cloud Asset Inventory を利用し
組織全体のアセットを一括取得
- アセットに推奨事項が存在するかチェック



Recommender で実現できたこと

Security Command Center では検知できない

放置されたリソース(= セキュリティホールリスク)を検知する仕組みが作れた

検知例

- 利用頻度が低い Google Cloud プロジェクト
- アイドル状態の Compute Engine
- アイドル状態の Cloud SQL

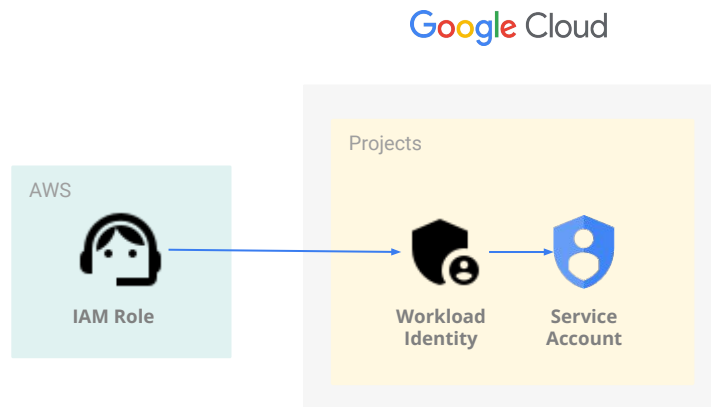


Workload Identity

Workload Identity とは？


サービスアカウント キーを使わずに、
AWS 等の外部プロバイダから
Google Cloud へアクセスを可能とする
認証

- サービスアカウント キーを不要にできます
- GKE の話ではありません



Workload Identity を利用するための Tips

 利用できる: Cloud SDK / gcloud CLI

 利用できない: bq / gsutil

bq コマンドで Workload Identity を利用可能にするパッチをブログに書いてます

- Akatsuki Hackers Lab id:NeoCat さん
「Google Cloud のサービスアカウントキーなしで gcloud や bq コマンドを AWS から利用してみた」
<https://hackerslab.aktsk.jp/2021/12/09/000429>

全体まとめ

1. Security Command Center + Forseti Security を利用することで
400 個以上存在するGoogle Cloud プロジェクトの監査を自動化した
2. Recommender を利用することで
使われていないリソースを組織一括で検知することができた
3. Workload Identity を利用することで
キーを発行せず、他社プロバイダからアクセス可能にすることができる



さいごに



株式会社アカツキゲームス

<https://game.aktsk.jp>



ゲームを軸とした
IPプロデュースカンパニーとして
世界に突き抜ける



開発 / 運用メンバー募集中！！

楽しい開発ができます！！

- Google Cloud / AWS
- Elixir / Ruby / Go
- <https://aktsk.jp/recruit/career/#engineer>

Thank you.

