Session 3

スペシャリストが語る！
Google Cloud のメリットを活かすネットワーク、セキュリティのあり方とは？

栃沢 直樹

Google Cloud
パートナー エンジニア
（Infrastructure Modernization）

有賀 征爾

Google Cloud
カスタマー エンジニア

工藤 佑介 氏

株式会社NTTデータグループ
技術革新統括本部 課長代理

鈴木 勝史 氏

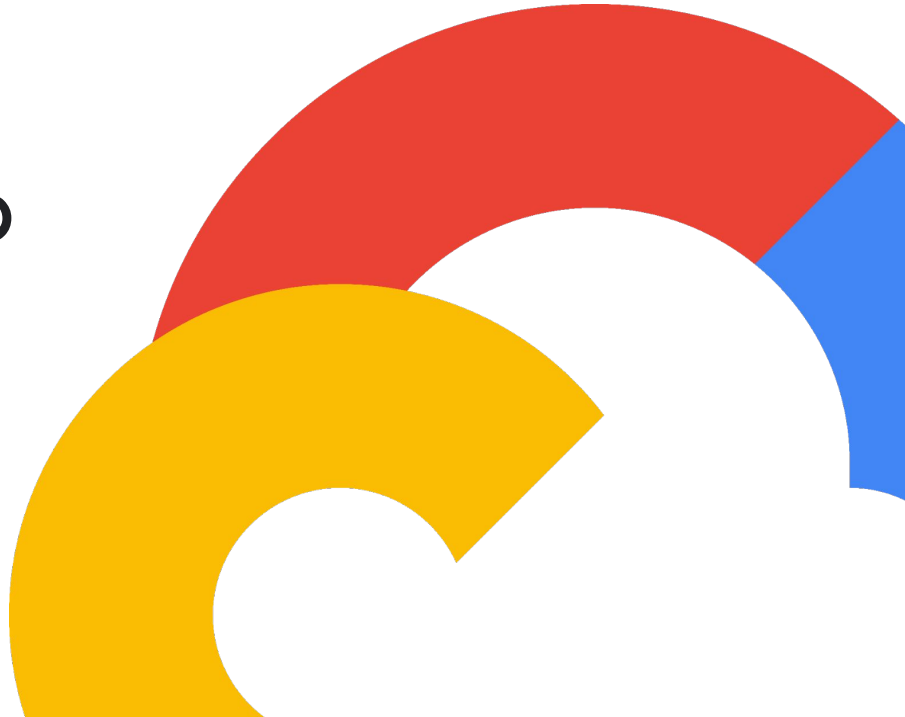
株式会社スリーシェイク
Sreake事業部 SRE

檜垣 慶太 氏

アイレット株式会社
カスタマー支援事業部 TAM
グループリーダー

パネル ディスカッション

スペシャリストが語る！
Google Cloud のメリットを
活かすネットワーク、セキュリティの
あり方とは？



Google Cloud

01

モデレーター紹介

MC

Naoki Tochizawa（栃沢直樹）

グーグル・クラウド・ジャパン

主なミッション：

- Partner Engineer - Infrastructure Modernization
  - お客様向けの提案、ワークショップ
  - 以前はセキュリティ ベンダーにて ソリューション アーキテクトシステム インテグレータにて エンジニア（Network / Security / 運用設計 etc...）

- 日本ネットワークセキュリティ協会 デジタルアイデンティティ WG サブスクライバ

MC

Seiji Ariga（有賀 征爾）

グーグル・クラウド・ジャパン

主なミッション：

- Customer Engineer - Networking
  - 以前は通信事業者にてバックボーンネットワークの設計・構築をしていました

好きな Google Cloud サービス：

- Network Connectivity Center（ネットワークの重要なピース）

アピールポイントなど：

- Google Cloud のネットワークサービスやインフラにはちょっと詳しいです

02

パネリスト紹介

Nice to meet you!

Yusuke Kudo（工藤 佑介）

株式会社NTTデータグループ

主なミッション:

- クラウド / CloudNative技術支援
  - CCoE / SRE / Platform Engineeringなど

好きな Google Cloud サービス:

- CloudRun/Firebase(すぐ使える&運用も楽)
- GKE(Autopilotのpod起動が早くなってうれしい)

アピールポイントなど:

- 様々な業界の大規模・ミッションクリティカル領域の案件リードしてます！

Nice to meet you!

Masashi Suzuki（鈴木 勝史）

株式会社スリーシェイク

主なミッション：

- お客様のクラウドインフラ（Google Cloud AWS）の
  - 設計、運用、構築支援（チーム外）
  - モダナイズ、内製化支援（チーム内）

好きな Google Cloud サービス：

- Cloud Run

アピールポイントなど：

- Google CloudおよびAWSの様々な規模の環境の支援をしています

Nice to meet you!

Keita Higaki（檜垣 慶太）

アイレット株式会社

主なミッション：

- AWS 及び Goolge Cloud を主戦場にマルチクラウド環境において、日々顧客課題の解決を目指し活動中
- SRE 特命グループも設立し、現在は DevSecOps に注力中

好きな Google Cloud サービス：

- Cloud Run / BigQuery などのサーバレスプロダクト

アピールポイントなど：

- 日々お客様の DX 支援、PM 支援、コスト最適化サポートに注力しています！

ディスカッション スタート！

Question 1 :

現在のハイブリッドクラウド構成時のトレンドとお客様が気にされるポイント

Question 2 :

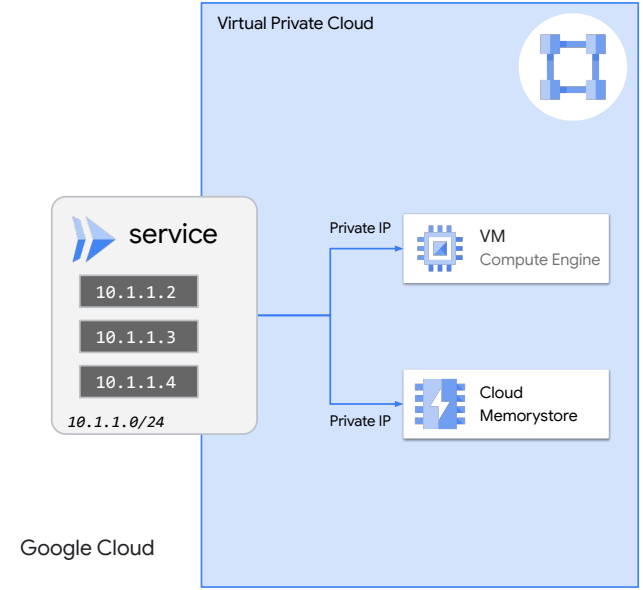
クラウドのネットワーク設計、セキュリティ実装において押さえておくべきポイント

Question 3 :
ネットワーク、セキュリティの課題とアプローチ

Cloud Run から VPC リソースへアクセスする方法 = VPC 外からのアクセスを許可する方法

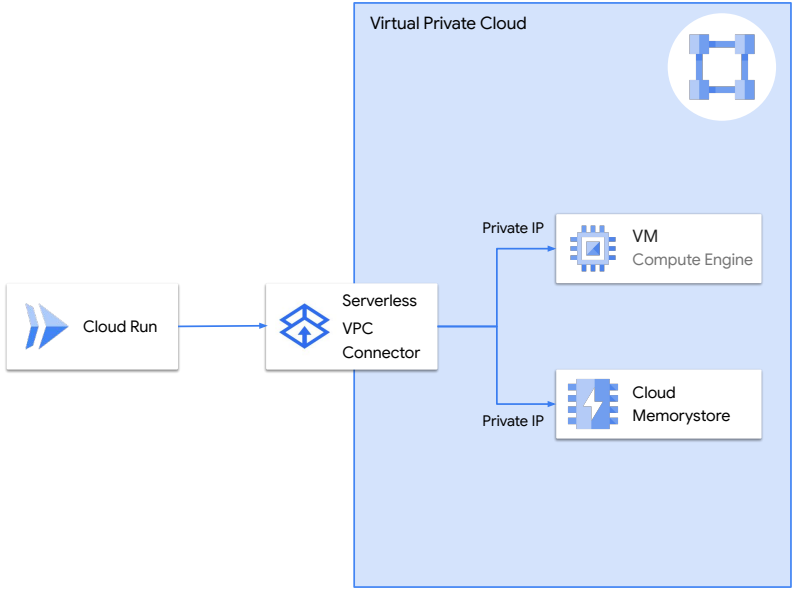
Direct VPC Egress

・Cloud Run を VPC サブネットに直結
・コンテナ インスタンスごとに IP アドレスを付与



Serverless VPC Access Connector

・中継用のコネクタ インスタンス
・コネクタの自動スケーリング（スケールインは行わない）

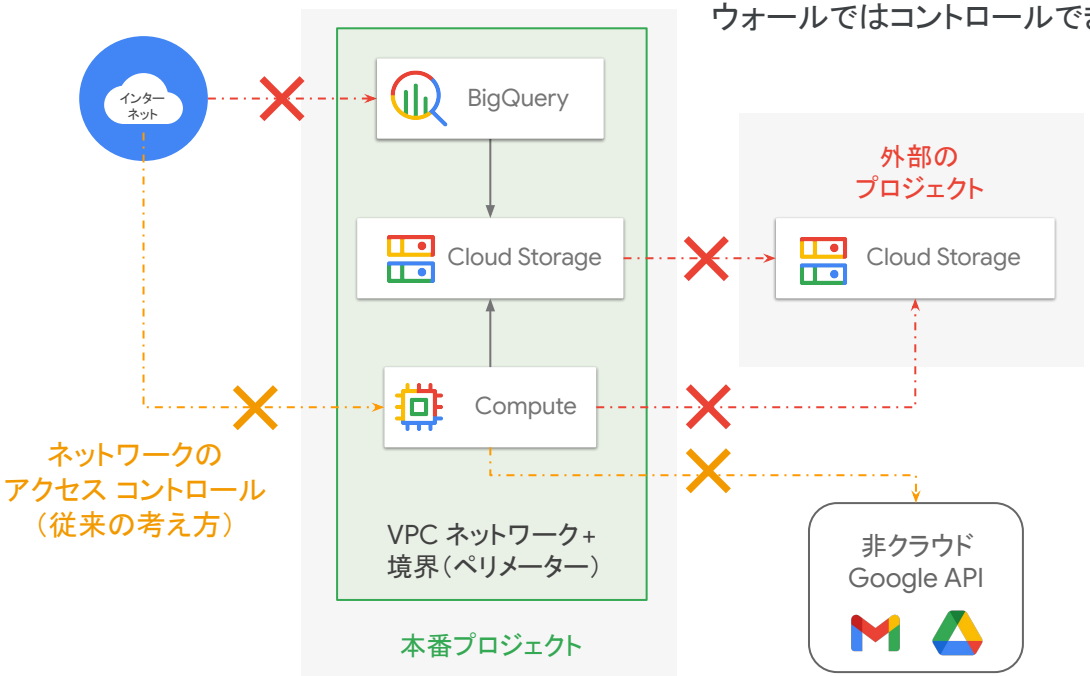


Question 4 :

Google Cloud のネットワーク・セキュリティ領域でのおすすめのサービス・機能

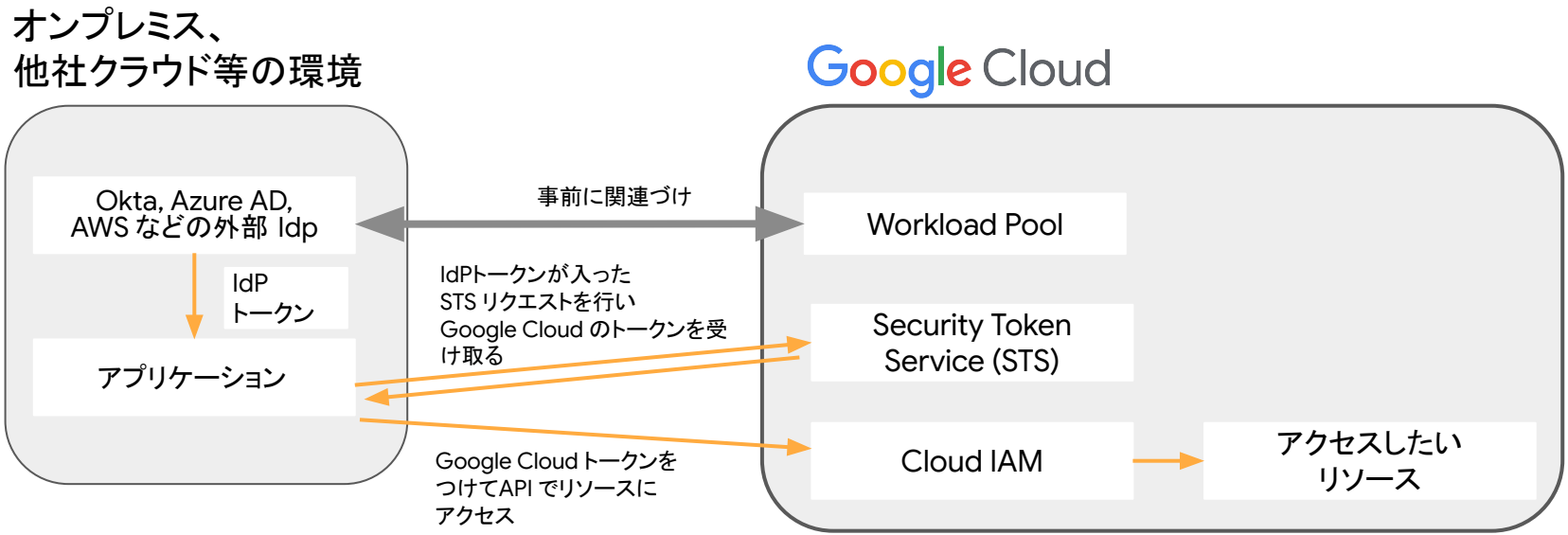
VPC Service Controls（VPC-SC）

IP アドレスが共用されている API への アクセスは、IP アドレスベースのファイア ウォールではコントロールできない

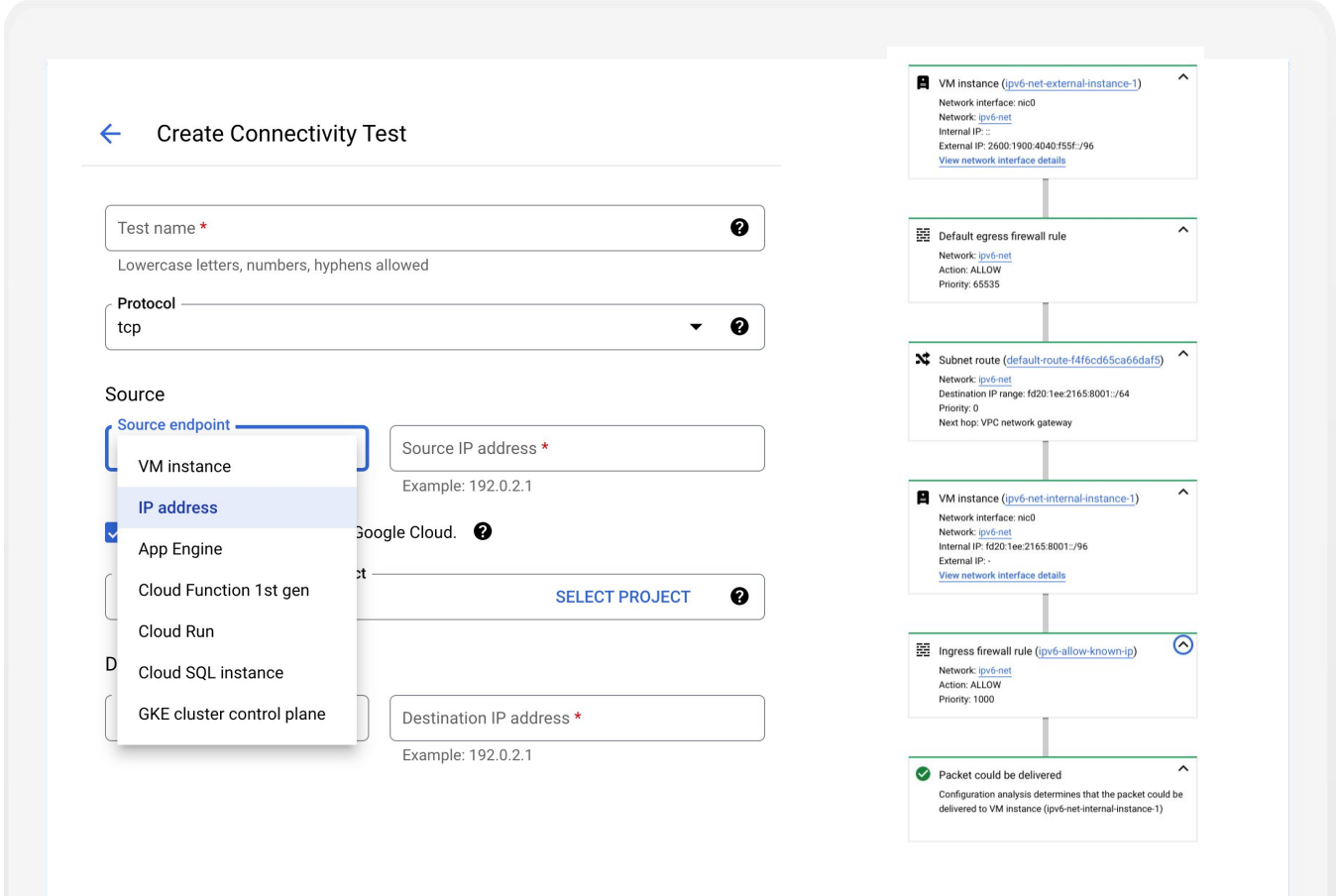


Workload Identity Federation

- Google Cloud の外部から Google Cloud の API を呼び出すときに、サービスアカウントの API キーではなく、短時間だけ有効なトークンを発行する
- サービス アカウントのキーの漏洩対策



Network Intelligence Center - Connectivity Test

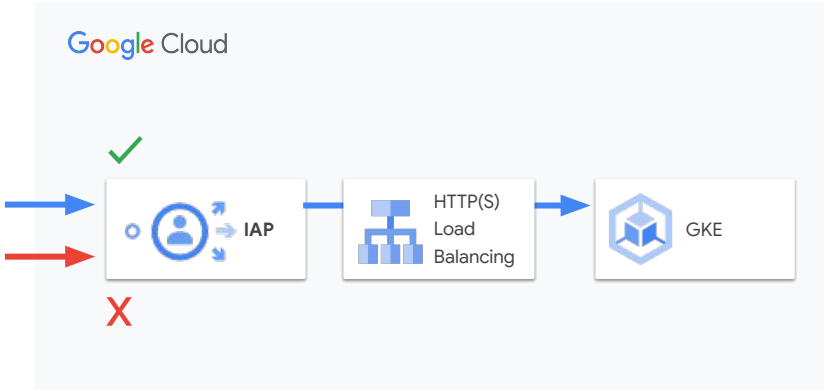


Identity Aware Proxy (IAP)

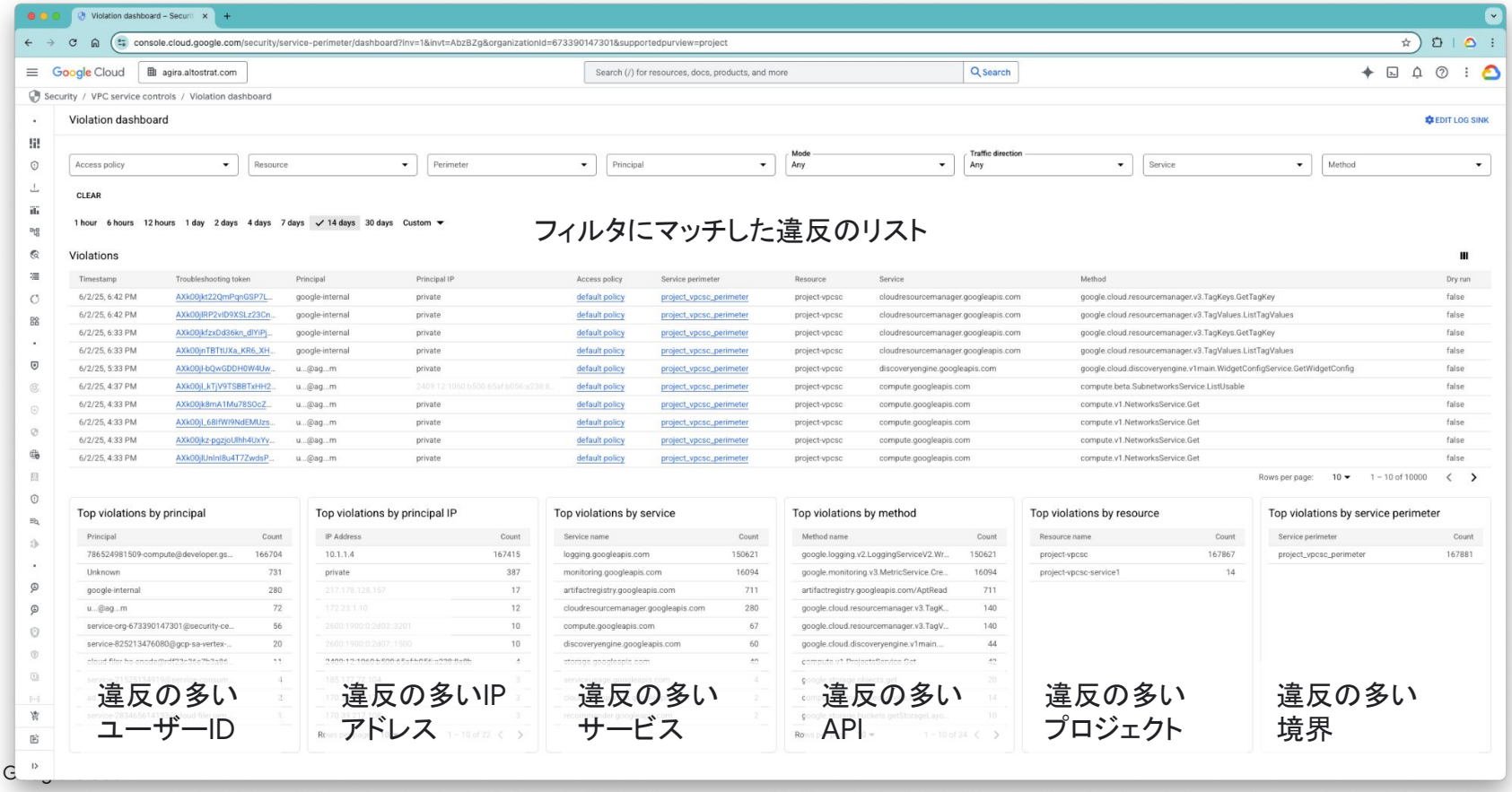
Google の **BeyondCorp セキュリティ モデルを元に**
設計され、ゼロトラスト ネットワークを実現

アプリケーションの前段に配置する
リバース プロキシ（Identity-Aware Proxy）

- コンテキスト ベースのアクセス ポリシー
- ユーザー・アプリ間の暗号化を強制
- SSH や RDP 等のプロトコルにも対応

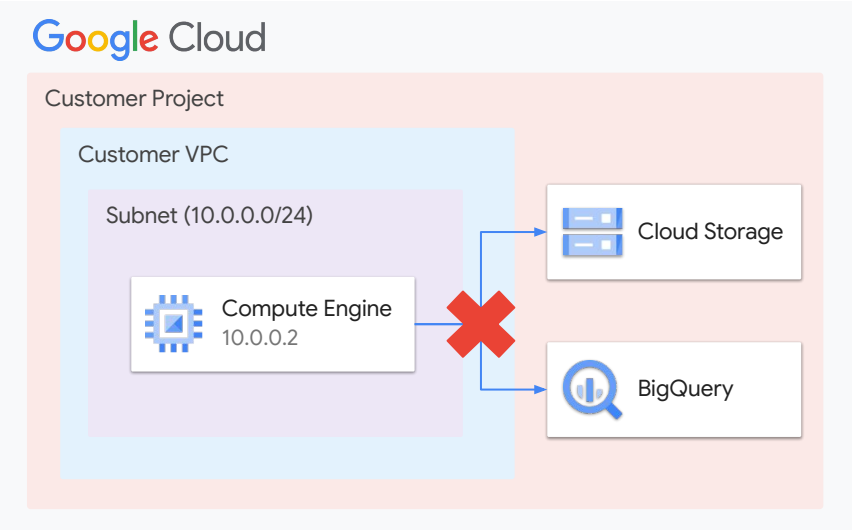


VPC Service Controls（VPC-SC）- 違反ダッシュボード

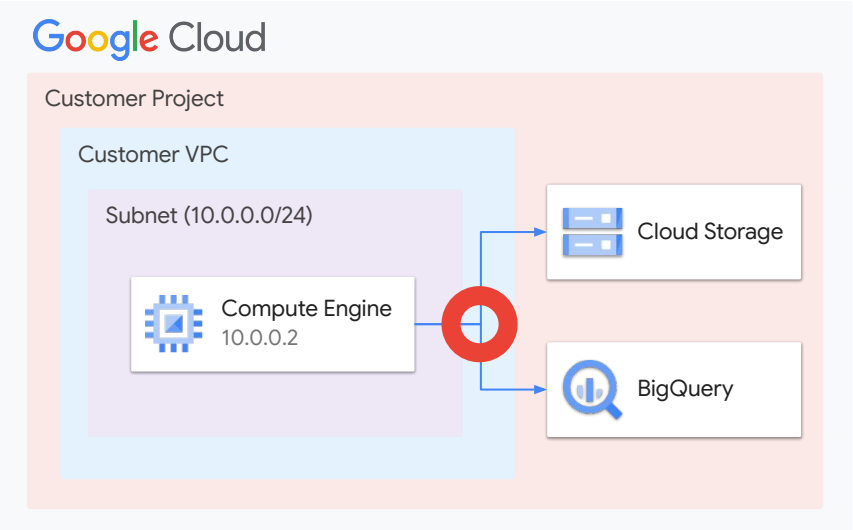


限定公開の Google アクセス

- 外部 IP アドレスを持たないリソースからGoogle API サービスにアクセスさせる機能
  - 外部IP を持たない VM でも デフォルト ルート(0.0.0.0/0)を利用して Google APIs にアクセスが可能となる
- Private Service Connect を使う場合にも、オンにすることが前提となるサービス



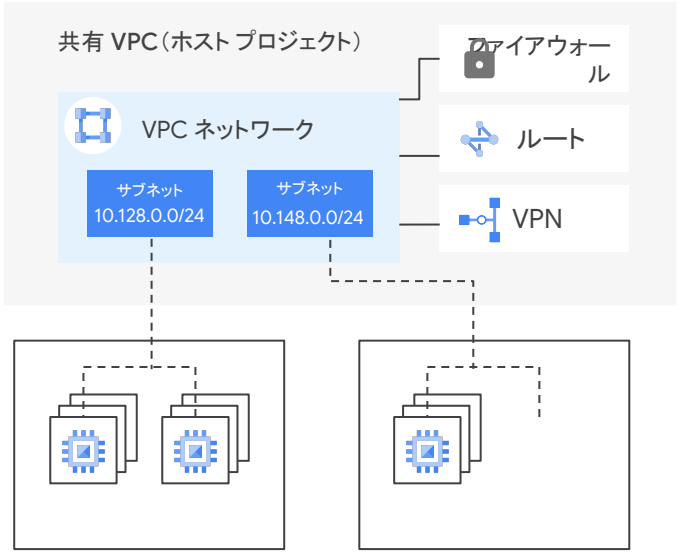
Private Google Access 無効の場合はアクセス不可



Private Google Access 有効の場合はアクセス可

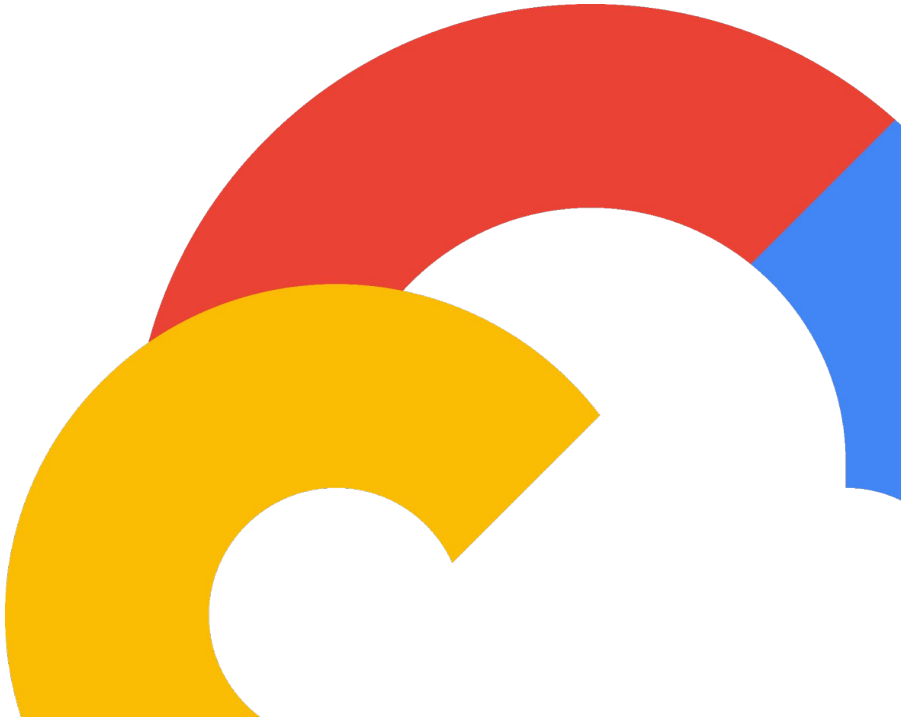
共有 VPC

- 外部プロジェクトに自リソース（サブネット）の利用許可を与える仕組み
  - 権限委譲の仕組み
  - VPC 自体は通常の VPC
- 一つのシステム複数のチームで開発
  - VPC 分割による責任分界
  - 共有 VPC による責任分界



Question 5 :
おすすめのクラウドのネットワーク、セキュリティのベストプラクティスのキャッチアップ方法

Thank you



Google Cloud