

## 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？



柄沢 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



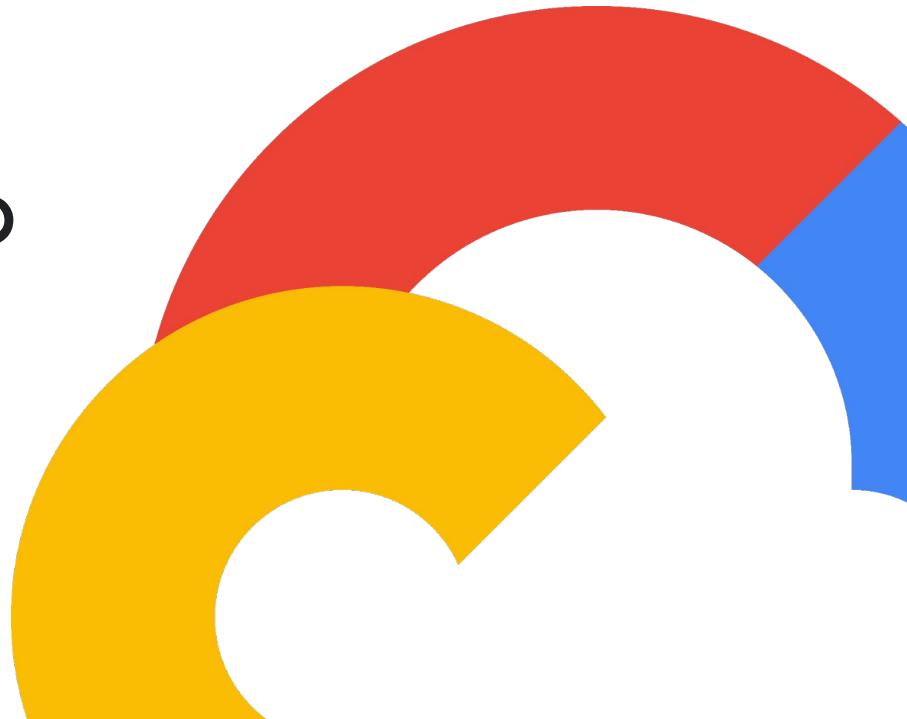
檜垣 慶太 氏

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

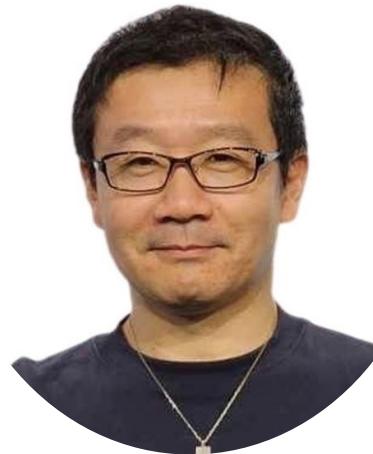
# MC

## Naoki Tochizawa (柄沢直樹)

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 サブスクリーバ



# 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 Google 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

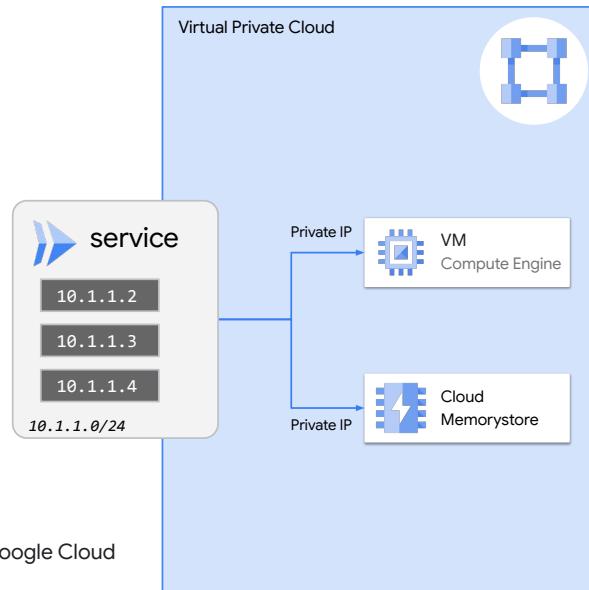
# Question 3 :

## 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

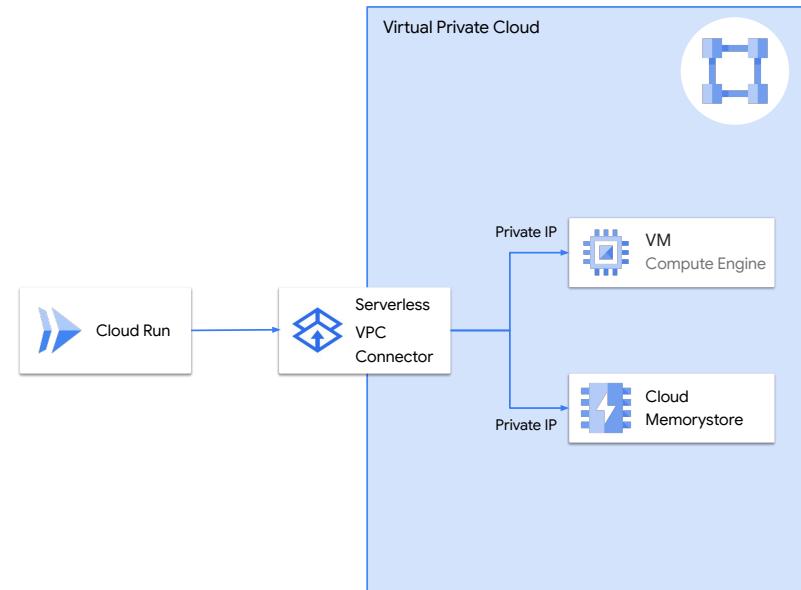
## Direct VPC Egress

- 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

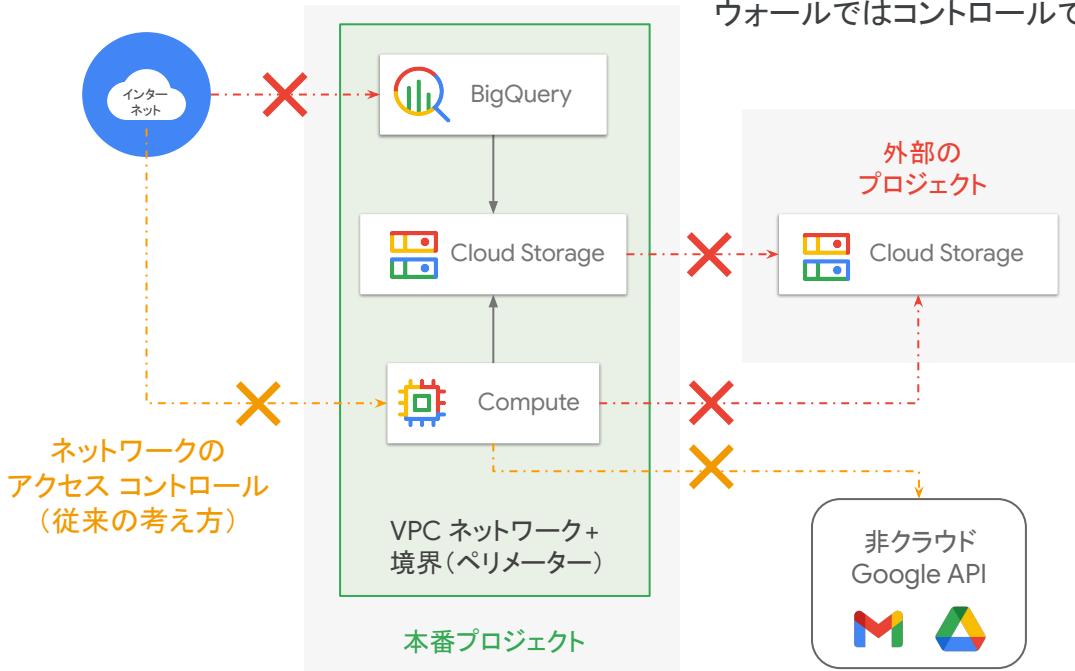
- 中継用のコネクタ インスタンス
- コネクタの自動スケーリング(スケールインは行わない)



## 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)

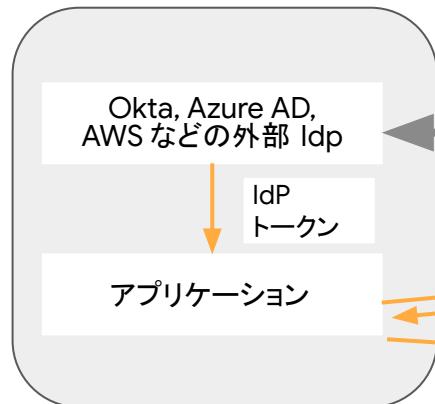


IP アドレスが共用されている API への  
アクセスは、IP アドレスベースのファイア  
ウォールではコントロールできない

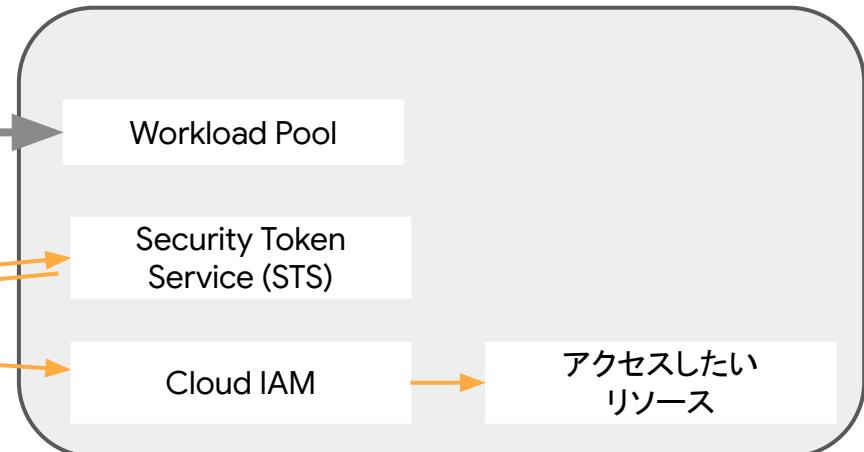
# Workload Identity Federation

- 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

オンプレミス、  
他社クラウド等の環境



Google Cloud



# Network Intelligence Center - Connectivity Test

## Create Connectivity Test

Test name \*

Lowercase letters, numbers, hyphens allowed

Protocol —  
tcp

Source

Source endpoint —  
VM instance

IP address

App Engine

Cloud Function 1st gen

Cloud Run

Cloud SQL instance

GKE cluster control plane

Source IP address \*

Example: 192.0.2.1

SELECT PROJECT

Destination IP address \*

Example: 192.0.2.1

VM instance (ipv6-net-external-instance-1)

Network interface: nic0

Network: ipv6-net

Internal IP: ::

External IP: 2600:1900:4040:f55f::96

[View network interface details](#)

Default egress firewall rule

Network: ipv6-net

Action: ALLOW

Priority: 65535

Subnet route (default-route-f4f6cd65ca66dafs)

Network: ipv6-net

Destination IP range: fd20:1ee:2165:8001::/64

Priority: 0

Next hop: VPC network gateway

VM instance (ipv6-net-internal-instance-1)

Network interface: nic0

Network: ipv6-net

Internal IP: fd20:1ee:2165:8001::/96

External IP: ::

[View network interface details](#)

Ingress firewall rule (ipv6-allow-known-ip)

Network: ipv6-net

Action: ALLOW

Priority: 1000

Packet could be delivered

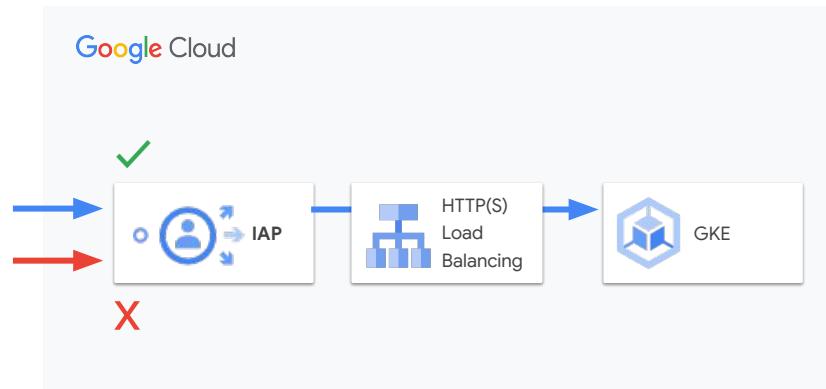
Configuration analysis determines that the packet could be delivered to VM instance (ipv6-net-internal-instance-1)

# 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

Violation dashboard - Security

console.cloud.google.com/security/service-perimeter/dashboard?inv=1&inv=AbzBZg&organizationId=673390147301&supportedpurview=project

Google Cloud agira.altostrat.com

Security / VPC service controls / Violation dashboard

Violation dashboard

Access policy Resource Perimeter Principal Mode Any Traffic direction Any Service Method

CLEAR

1 hour 6 hours 12 hours 1 day 2 days 4 days 7 days  14 days 30 days Custom

### フィルタにマッチした違反のリスト

Timestamp	Troubleshooting token	Principal	Principal IP	Access policy	Service perimeter	Resource	Service	Method	Dry run
6/2/25, 6:42 PM	AXx00jkt22QmPqGSP7L	google-internal	private	default policy	project_vpcsc_perimeter	project-vpcsc	cloudresourcemanager.googleapis.com	google.cloud.resourcemanager.v3.TagKeys.GetTagKey	false
6/2/25, 6:42 PM	AXx00jRP2vD9Xkz23Cn	google-internal	private	default policy	project_vpcsc_perimeter	project-vpcsc	cloudresourcemanager.googleapis.com	google.cloud.resourcemanager.v3.TagValues.ListTagValues	false
6/2/25, 6:33 PM	AXx00jkfzD05kn_dyYp	google-internal	private	default policy	project_vpcsc_perimeter	project-vpcsc	cloudresourcemanager.googleapis.com	google.cloud.resourcemanager.v3.TagKeys.GetTagKey	false
6/2/25, 6:33 PM	AXx00jTBTHXa_KR6_XH	google-internal	private	default policy	project_vpcsc_perimeter	project-vpcsc	cloudresourcemanager.googleapis.com	google.cloud.resourcemanager.v3.TagValues.ListTagValues	false
6/2/25, 5:33 PM	AXx00jbqwGDDH0W4UW	u...@ag...m	private	default policy	project_vpcsc_perimeter	project-vpcsc	discoveryengine.googleapis.com	google.cloud.discoveryengine.v1main.WidgetConfigService.GetWidgetConfig	false
6/2/25, 4:37 PM	AXx00j_kTV9TSBtHH2	u...@ag...m	2409.12.1060.6500.65af6056.a238.8	default policy	project_vpcsc_perimeter	project-vpcsc	compute.googleapis.com	compute.beta.SubnetworksService.ListUsable	false
6/2/25, 4:33 PM	AXx00j8AmA1Mu7850CZ	u...@ag...m	private	default policy	project_vpcsc_perimeter	project-vpcsc	compute.googleapis.com	compute.v1.NetworksService.Get	false
6/2/25, 4:33 PM	AXx00j_68IW9N9EMUzr	u...@ag...m	private	default policy	project_vpcsc_perimeter	project-vpcsc	compute.googleapis.com	compute.v1.NetworksService.Get	false
6/2/25, 4:33 PM	AXx00jkz_pgzgjUlh4txYv	u...@ag...m	private	default policy	project_vpcsc_perimeter	project-vpcsc	compute.googleapis.com	compute.v1.NetworksService.Get	false
6/2/25, 4:33 PM	AXx00jUlnl0u4T7ZwdsP	u...@ag...m	private	default policy	project_vpcsc_perimeter	project-vpcsc	compute.googleapis.com	compute.v1.NetworksService.Get	false

Rows per page: 10 1 – 10 of 10000

#### Top violations by principal

Principal	Count
786524981509-compute@developer-gs...	166704
Unknown	731
google-internal	280
u...@ag...m	72
service-org-673390147301@security-ce...	56
service-825213476080@gcp-sa-vertex...	20
...	...

#### Top violations by principal IP

IP Address	Count
10.1.1.4	167415
private	387
217.178.128.167	17
172.23.12.10	12
2600:1900:0:2403:3201	10
2600:1900:0:2407:1500	10
...	...

#### Top violations by service

Service name	Count
logging.googleapis.com	150621
monitoring.googleapis.com	16094
artifactregistry.googleapis.com	711
cloudresourcemanager.googleapis.com	280
compute.googleapis.com	67
discoveryengine.googleapis.com	60
storage.googleapis.com	49
...	...

#### Top violations by method

Method name	Count
google.logging.v2.LoggingServiceV2.Wr...	150621
google.monitoring.v3.MetricService.Cre...	16094
artifactregistry.googleapis.com/ApiRead	711
google.cloud.resourcemanager.v3.TagKe...	140
google.cloud.resourcemanager.v3.TagVa...	140
google.cloud.discoveryengine.v1main...	44
compute.v1.ProjectsServices.Get	20
service.v1.Services.Get	14
compute.v1.Networks.Get	10
...	...

#### Top violations by resource

Resource name	Count
project-vpcsc	167867
project-vpcsc-service1	14
...	...

#### Top violations by service perimeter

Service perimeter	Count
project_vpcsc_perimeter	167861
...	...

#### 違反の多いユーザーID

違反の多いIPアドレス

違反の多いサービス

違反の多いAPI

違反の多いプロジェクト

違反の多い境界

# 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

## Google Cloud

Customer Project

Customer VPC

Subnet (10.0.0.0/24)



Compute Engine  
10.0.0.2

Cloud Storage



BigQuery



## Google Cloud

Customer Project

Customer VPC

Subnet (10.0.0.0/24)



Compute Engine  
10.0.0.2

Cloud Storage



BigQuery

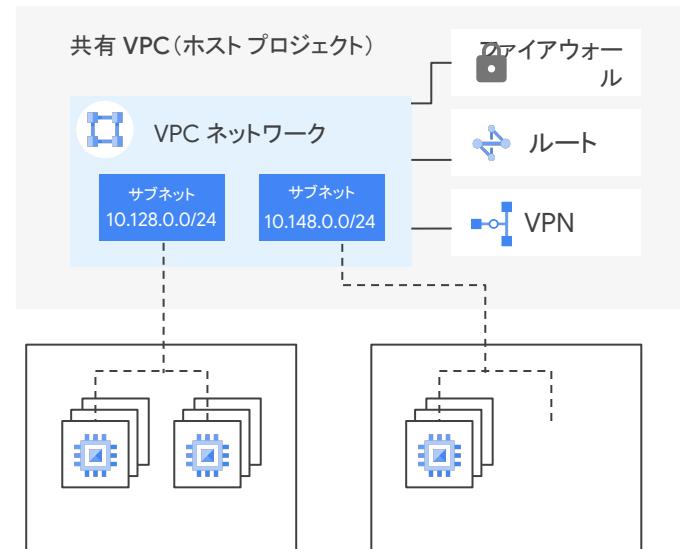


Private Google Access 無効の場合はアクセス不可

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

