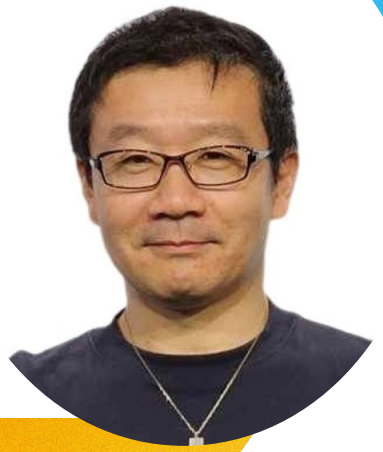
2025 年版
モダンインフラの最前線
- 開発・運用を加速するベストプラクティス

Google Cloud Next Tokyo

Naoki Tochizawa | 栃沢 直樹

Google Cloud



主なミッション

- Partner Engineer - Infrastructure Modernization
  - お客様向けの提案、ワークショップによる技術支援
  - パートナー様とのインフラ領域でのビジネス協業
- 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

Azuu Donowaki | 堂ノ脇 梓

Google Cloud

主なミッション

- Customer Engineer - Manufacturing &Industries
- 前職はコンサル会社にてインフラ移行の
  アセスメントから移行計画の作成を支援
- 現在は製造業界を中心にインフラ含めた
  クラウドの活用を推進

アジェンダ

01 企業が抱えるインフラ環境の課題

02 パフォーマンスとコストの両立

03 既存資産を活かすシームレスな移行とネットワークの可視化

04 脅威からシステムを保護するための可視化とセキュリティ管理の効率化

05 まとめ

01. 企業が抱えるインフラ環境の課題

2025 年 企業のインフラが直面する「現実」

悲鳴 1.
無限に増大する「性能要求」

「AI/ML の導入で既存インフラに限界が…」

- 少しの遅延も許されないユーザー体験
- 性能不足がビジネスの足かせとなる

悲鳴 2.
終わりのない「コスト圧力」

「性能は上げろ、でも予算は削れ、という矛盾…」

- 常に厳しく問われる投資対効果（ROI）
- リソースのサイジングミスが許されない

悲鳴 3.
制御不能な「複雑性」

「管理すべき対象が、もはや把握できない…」

- システムは増殖し、全体像の把握が困難に
- 色んな環境を使用しており、IP アドレスの管理が困難に

悲鳴 4.
日々巧妙化する「セキュリティ脅威」

「攻撃の入口は増える、守る人材は足りない…」

- AI をも活用し進化する攻撃手法
- 拡大し続けるアタックサーフェス

パラダイム シフト: 人手による運用から「AI アシスト運用」へ

Before
人手による「事後対応」運用

- アラートの洪水による障害検知
- 障害の原因特定は、熟練者の「経験と勘」頼み
- 根本解決よりも、場当たり的な対処が優先

エンジニアは疲弊し、イノベーションに時間が割けない。。

After
AI による「事前対応」運用

- AI が異常の予兆を検知し、人に知らせる
- AI が膨大なデータを分析し、原因と解決策を提案
- 人は最終的な意思決定と創造的な作業に集中

システムは安定し、未来のための戦略業務に注力できる

Google Cloud の Gemini Portfolio

ソフトウェア開発

ソフトウェアのデリバリーを**加速する**

Gemini Code Assist

アプリケーションライフサイクル

クラウド アプリケーションを効率的に管理する

Gemini Cloud Assist

セキュリティ

セキュリティの専門知識を**向上させる**

Gemini in Security

データ分析

高速なデータ分析

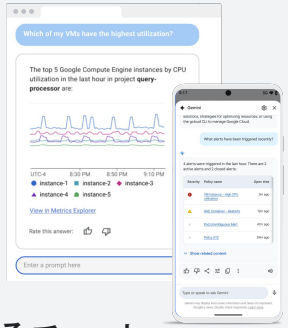
Gemini in BigQuery

ビジネスインテリジェンス

データインサイトの**自動化**

Gemini in Looker

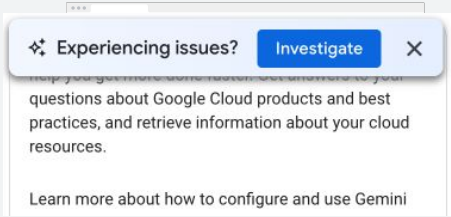
Gemini による生成AI 支援の活用を簡単に



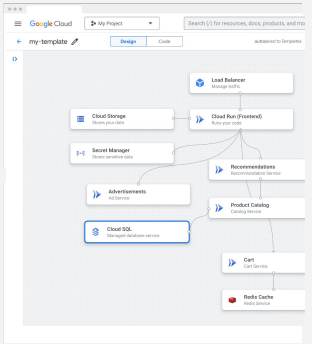
自然言語によるチャット

Compose a query

コンソールに対する
スマートアクション

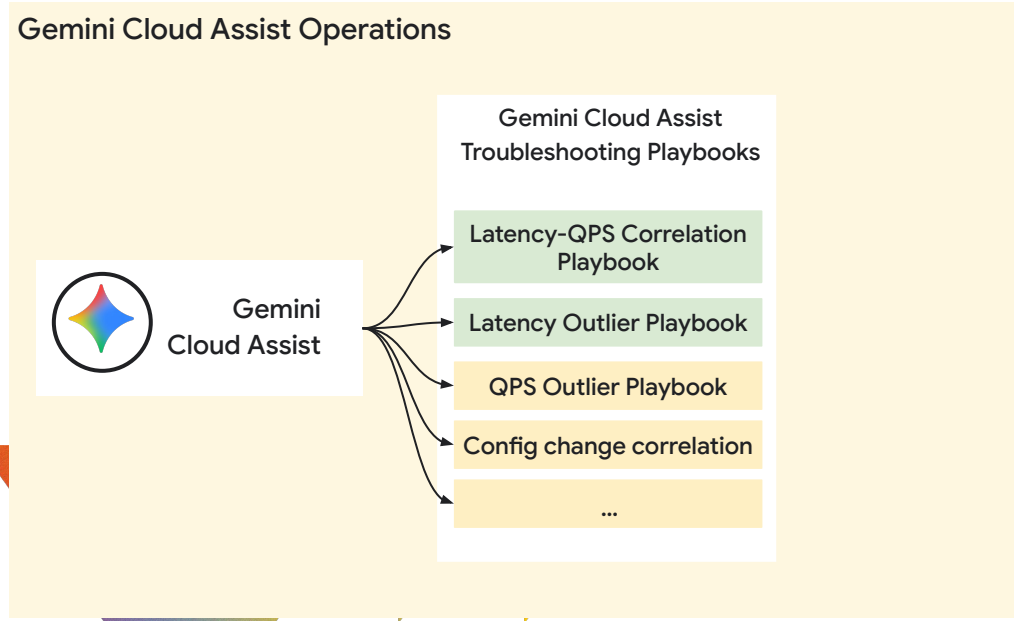


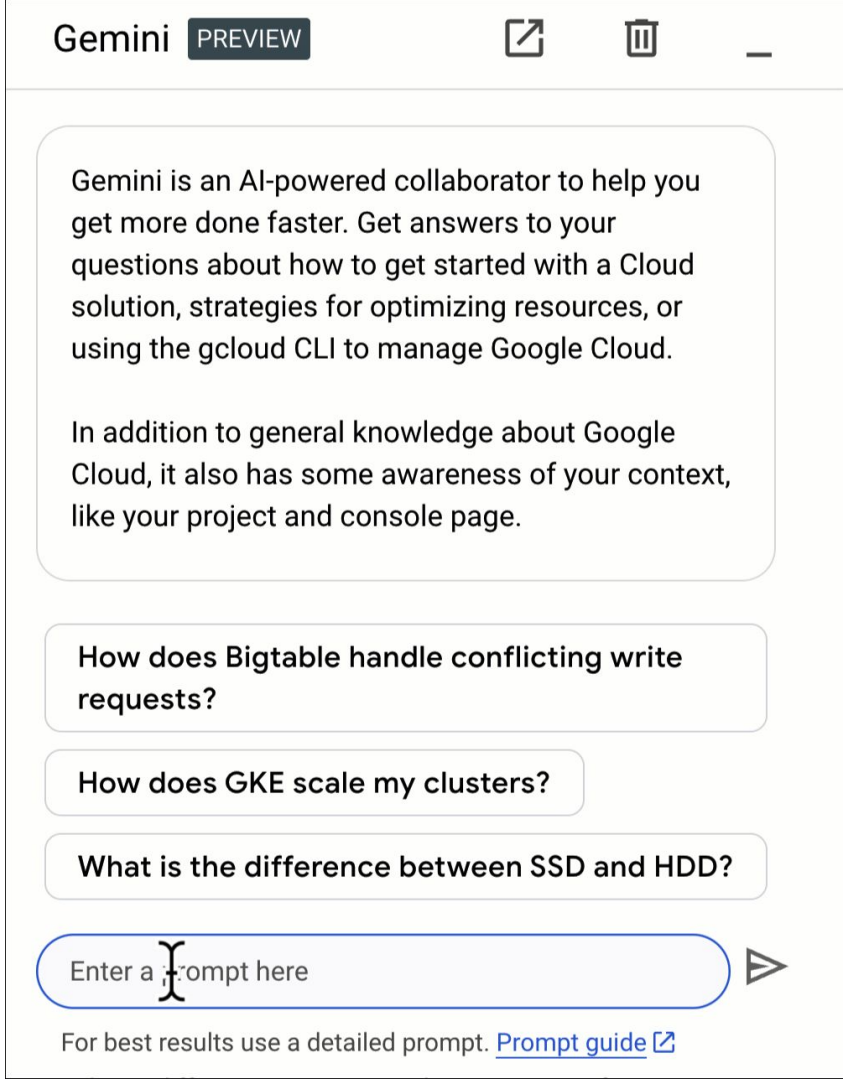
AI による調査支援



デザイン
統合

Google Cloud Assist





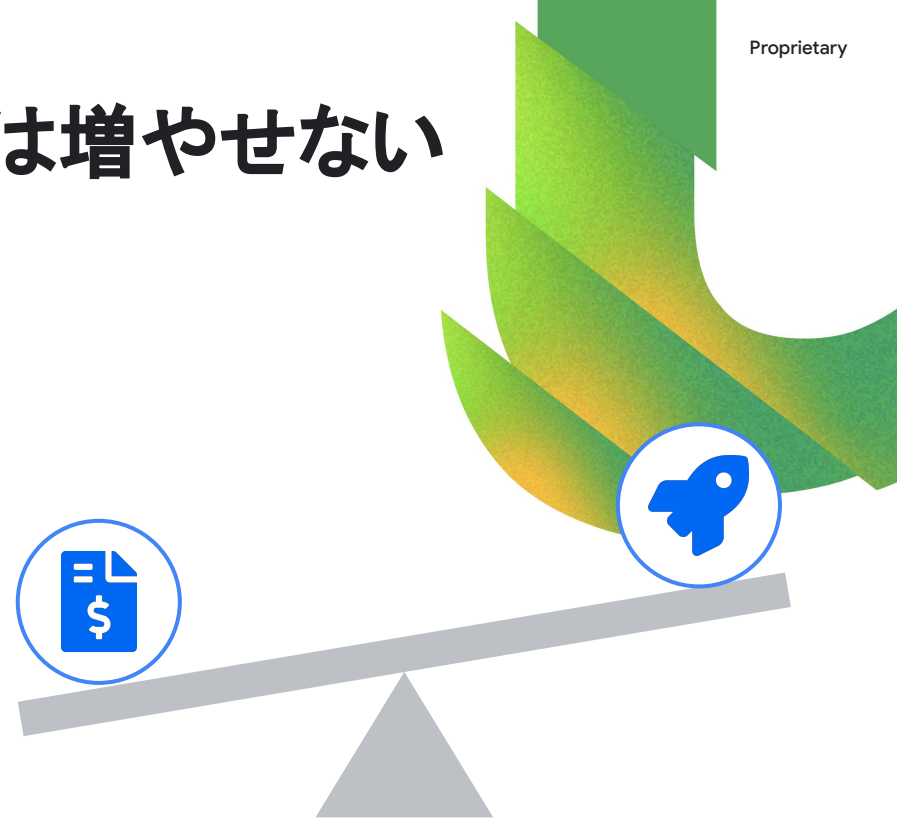
02. パフォーマンスとコストの両立

性能は上げたい、でも予算は増やせない

インフラ担当者の悩み

- ユーザー部門より
  「**Web サイトが遅すぎる！機会損失になってます。**」
- アプリ運用チームより
  「**夜間バッチが終わらない！もっと早いマシンにして下さい。**」
- 経営部門より
  「**これ以上のコスト増は認められない。コスト削減を意識してください。**」

多くのインフラ担当者はたくさんのジレンマを抱えています。



解決策1:
インフラの性能を限界まで引き出す

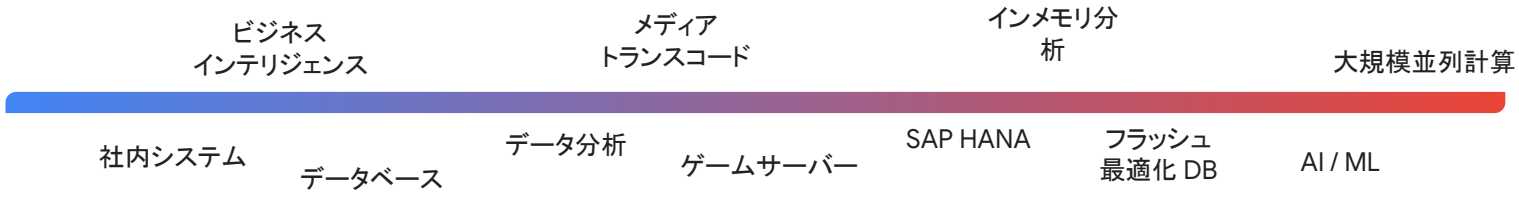
Next-Gen VM の活用 (N4 / C4 / C4A / C4D)

- **IPU 搭載のマシンを使用して**、ストレージやネットワーク**処理をデータセンター側にオフロード**
- ホストのコンピューティングリソースとメモリリソースを解放し、リアルタイムワークロードの **CPU 応答性を最大 80% 向上**させます

Hyperdisk による 性能の向上

- IPU アーキテクチャを最大限活用し、**Compute Engine のサイズと切り離してパフォーマンスを得ることが可能**
- ワークロードに合わせて**ストレージ容量を簡単かつ動的に調整可能**

Compute Engine ファミリー



汎用的なワークロード

柔軟性		一貫したパフォーマンス		
Intel	AMD	Intel	AMD	Arm
N1, N2	N2D	C3, C3 Metal	C3D	T2A
N4		C4		C4A
		C4 - GNR	C4D	Arm+

特殊なワークロード

コンピュート 最適化	メモリ 最適化	ストレージ 最適化	アクセラレータ 最適化 (GPU)
Intel/AMD	Intel		
C2, C2D, H3	M1, M2, M3	Z3	A2, A3, G2
	X4		A3+, A4
H4D			G4D

Intel ベースの C4 と N4 マシンの使い分け

Titanium と Intel の最新 5 世代目 Emerald Rapidsプロセッサを搭載

C4 VMs

一貫した高いパフォーマンス のために最適化

高度なメンテナンス機能と大型化

前世代 (C3) と比べて**最大 25% の価格性能の向上**

安定した高いパフォーマンス

N4 VMs

TCO 削減のための**パフォーマンスとコストのバランス**

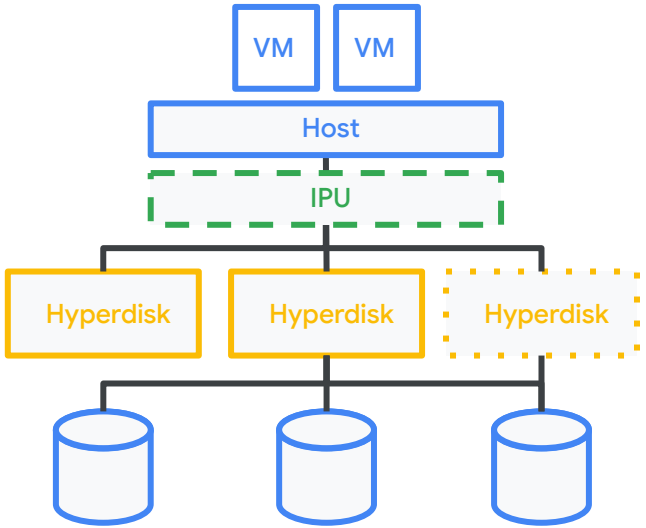
カスタムマシンタイプによる柔軟な形状

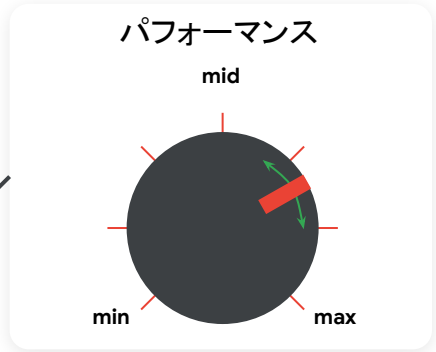
前世代 (N3) と比べて**最大 18% の価格性能の向上**

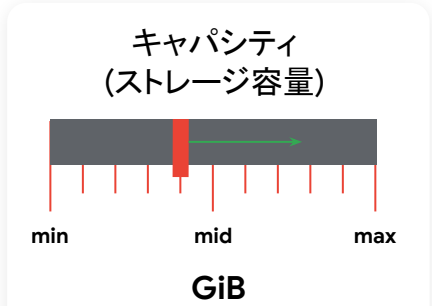
柔軟性とコスト最適化

Hyperdisk によるパフォーマンスの最適化

Infrastrcture Processing Unit（IPU）がパフォーマンス向上とサイジング（＝コスト）の最適化を実現







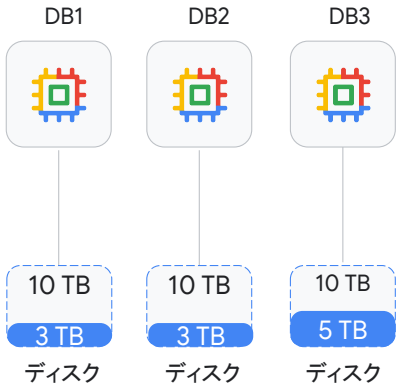
IOPs
$0.xx per IOP/s

Throughput
$0.xx per MiB/s

Capacity
$0.xx per GiB

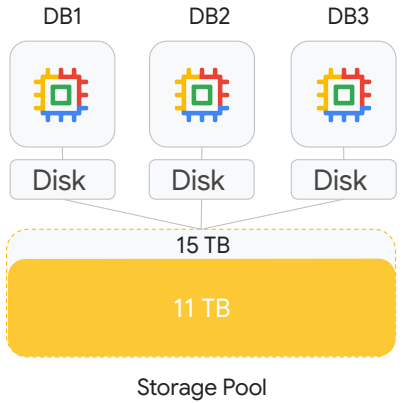
Storage Pool による最適化

現在 (Persistent Disk)



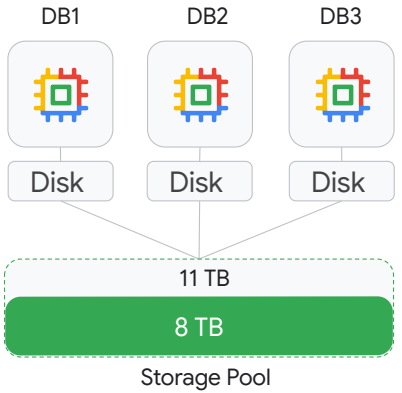
計 11 TB を使用中
払い出し済み 30 TB の容量に対して課金

Storage Pool を利用した場合



計 11 TB を使用中
払い出し済み 15 TB の容量に対して課金

Storage Pool の重複削除をした場合



計 8 TB を使用中
払い出し済み 11 TB の容量に対して課金

ストレージ TCO を最大 40% 削減することが可能

解決策 2:
無駄をなくし、全体コストを最適化する

Compute コスト最適化

- 確定利用割引(CUD)の柔軟な消費モデル
- FinOps Hub の活用による効率的なコスト最適化
- ベストプラクティスやサイジングの推奨事項

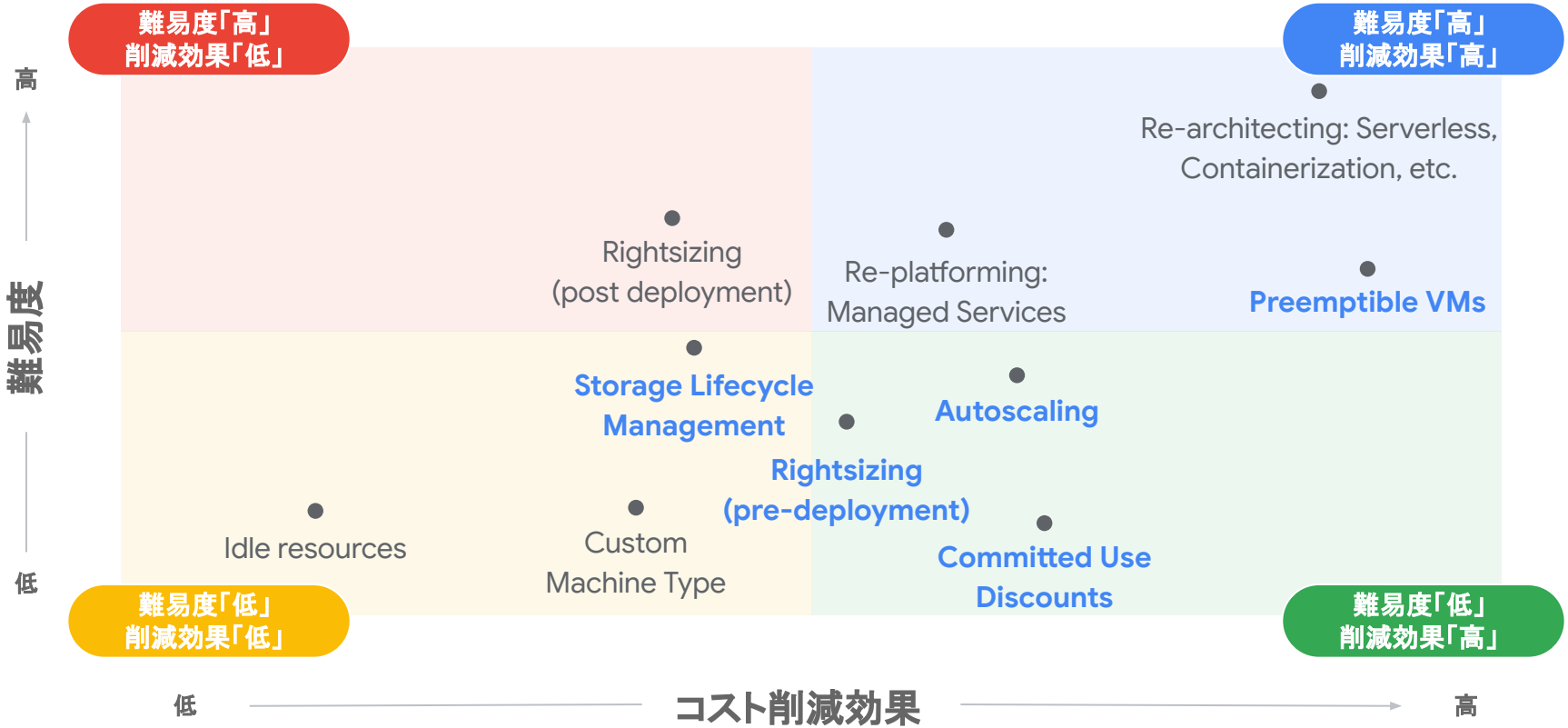
キャパシティ最適化

- Flexible MIG による Zone や Instance Type の柔軟性
- Capacity Planner による将来の需要を分析および予測
- Quota 管理によるリソース枯渇や制限の確認

運用最適化

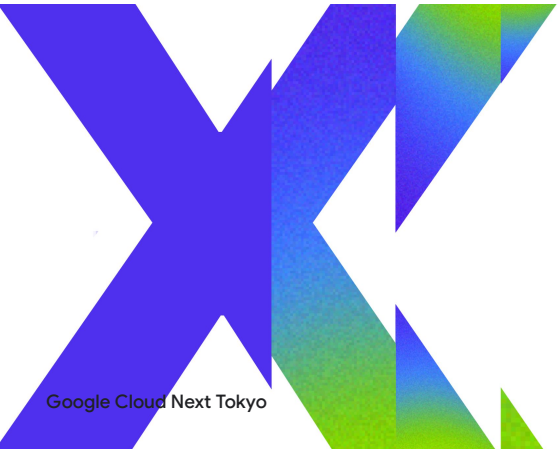
- MIG による自動修復、自動スケーリング、マルチゾーン稼働
- Batchによるワークロードのスケジュール、キューイング、実行
- Equivalent Code Component を使用してコードを自動生成

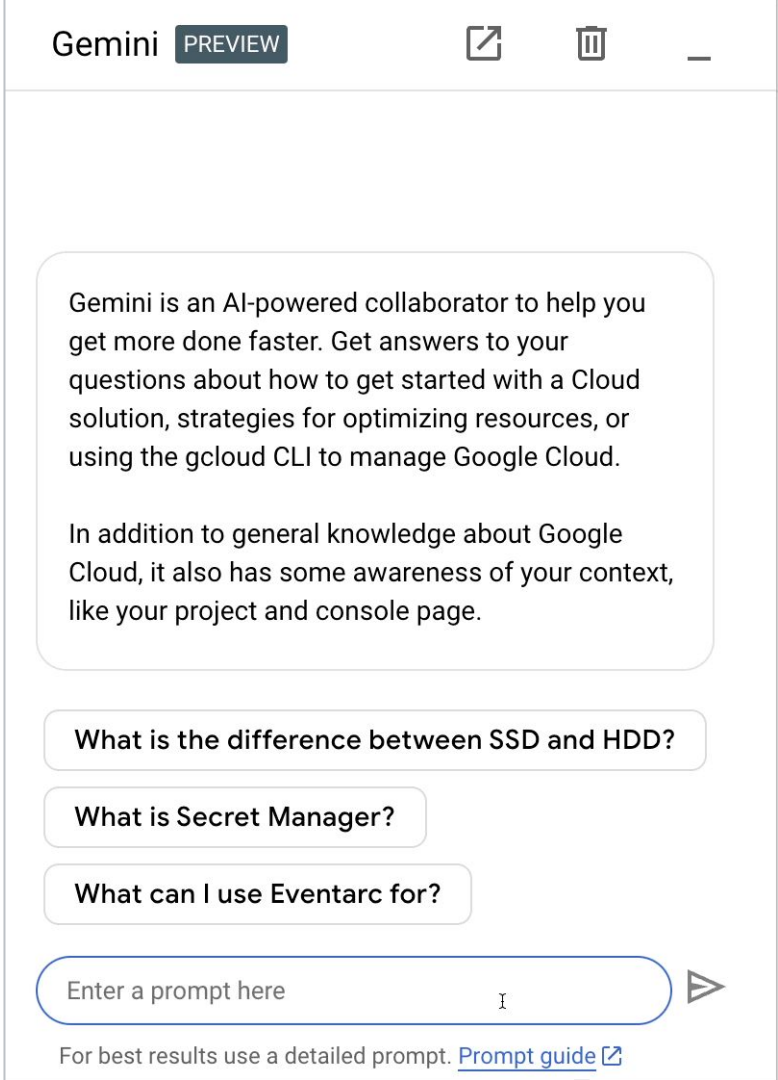
コスト最適化を行う方法



Gemini にコスト最適化方法を聞いてみよう

Gemini
Cloud Assist





03. 既存資産を活かすシームレスな移行とネットワークの可視化

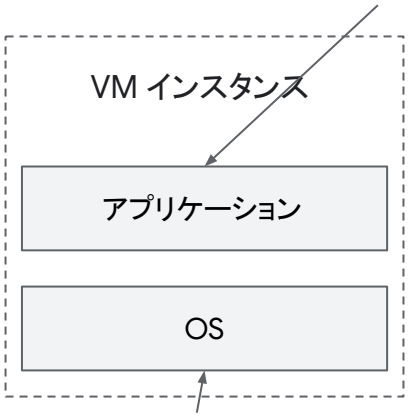
オンプレミスは無くならない。
どうやってクラウドと共存させる？

クラウド移行を実現したお客様が抱える
ネットワークの課題

- IP アドレスを変えられないレガシー VM が移行できない
- ネットワーク構成が複雑となり、運用が煩雑となっている

IP アドレスが変えられないレガシーなサーバ

- **DNS を利用した ホスト名 による管理**を利用したアプリケーション連携を見据えた仕組みへの移行がベストプラクティス
  - アプリケーションのモビリティが向上する
  - サーバレスサービスやAPI サービスへのアクセスを考慮する上でも必要
- **一方で実際にアプリケーションの改修、連携する外部システムとの調整が難しい**



Hosts ファイルでの管理

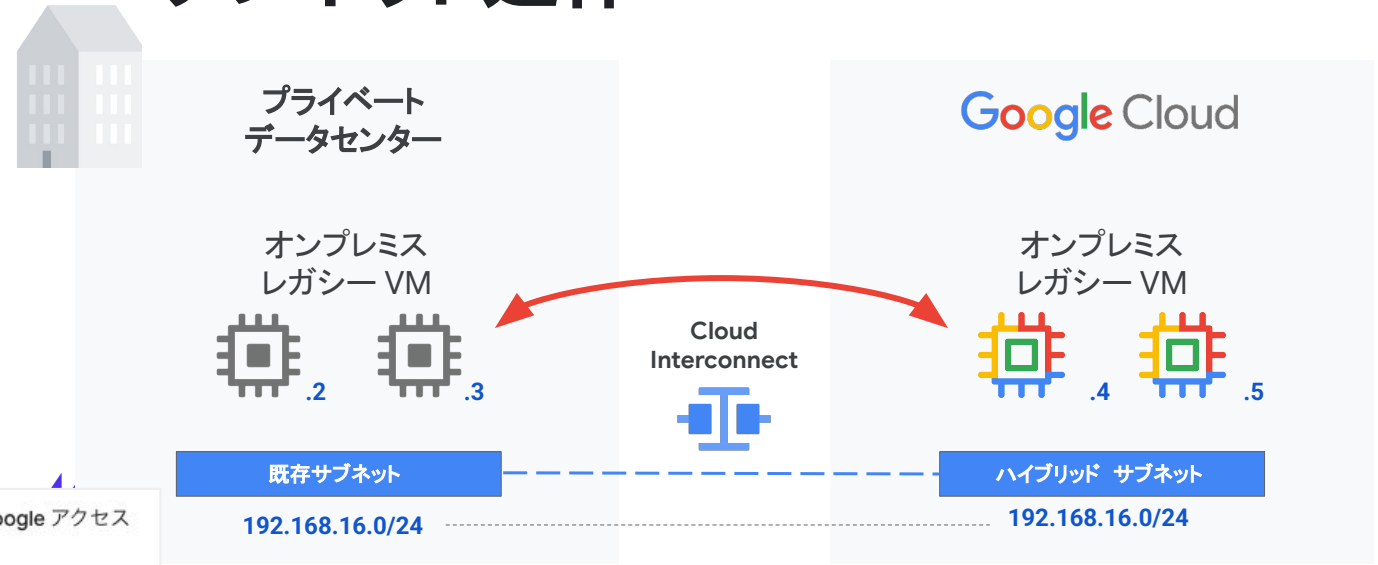
アプリへ 連携する ターゲットの
IP アドレスをハード コーディング

IP を変更しない限り、ハイブリッド クラウド構成を
前提として移行することは困難

クラウドの API サービスとの連携も難しくなる

クラウドサービス

解決策 1: ハイブリッド サブネットによるサブネット延伸



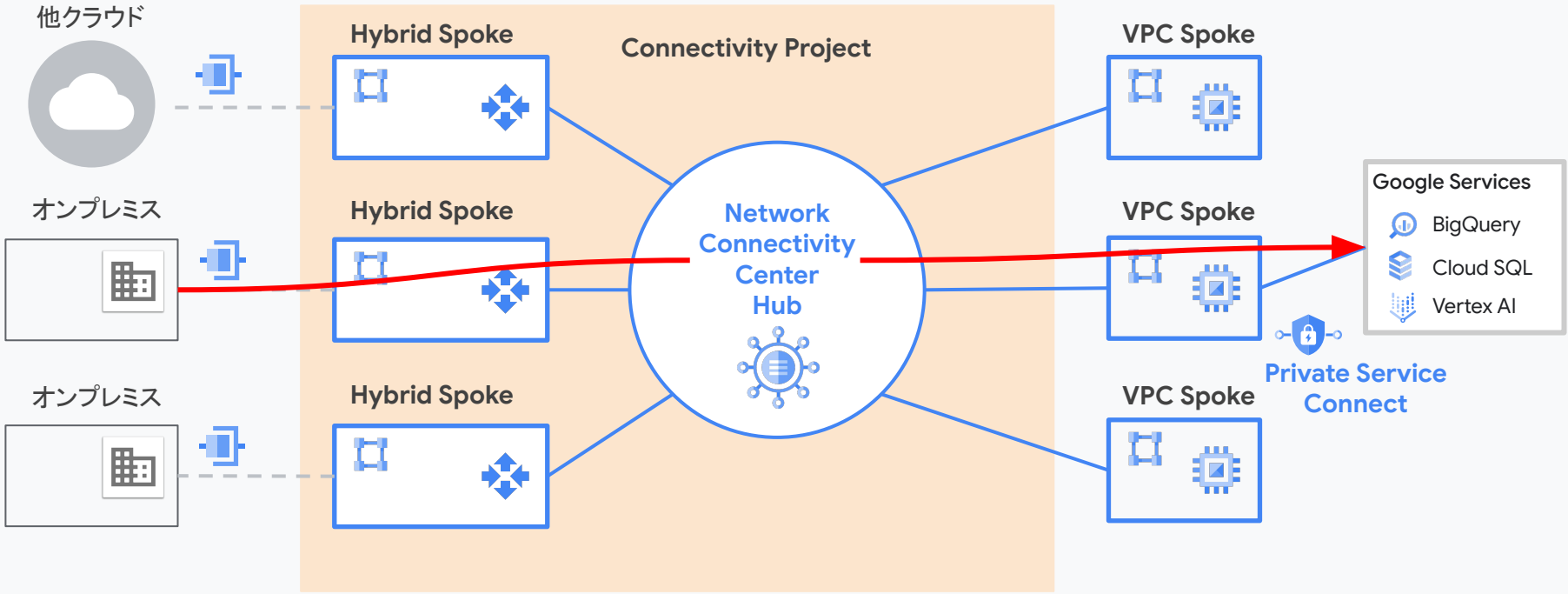
- 設定は VPC のサブネットで **[ハイブリッド サブネット]** を “ON” にするだけ
  - オンプレミスルータでは Proxy ARP が有効になっていれば OK
- IP アドレスを変えられないレガシー VM の移行にも対応
- Migrate to Virtual Machine（M2VM）による移行にも対応

解決策 2:ネットワーク管理のあり方を理解する

	集中管理	分散管理	
			サービス公開型
	共有 VPC	Network Connectivity Center（NCC）	Private Service Connect
VPC 管理	ネットワーク管理者	利用部門	利用部門
サブネット管理	ネットワーク管理者	利用部門 * 他ネットワークとのアドレス重複は考慮が必要	利用部門
ネットワーク相互接続	ホストプロジェクトでルーティング管理	NCC Hub との VPC Peering	サービス単位でエンドポイントを公開

- 組み合わせて利用することも可能
- マイクロ サービス化を行う上でサービス公開型を採用することでサービス間の　IP アドレス管理の負担は軽減される

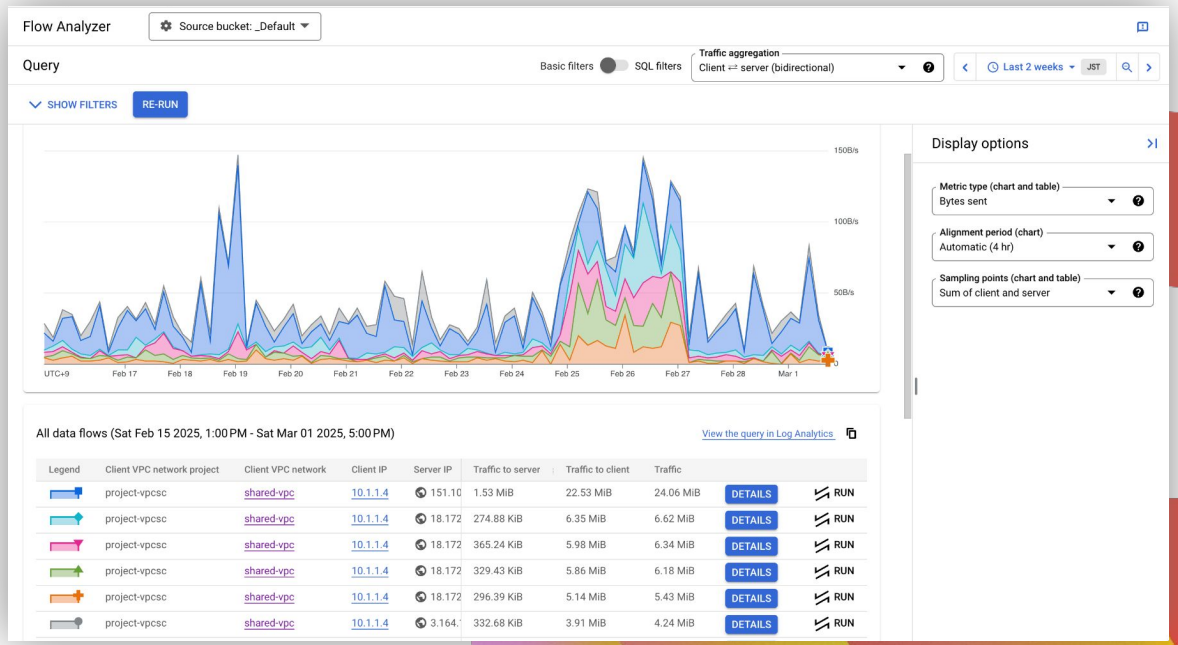
Network Connectivity Center を利用したシンプルなハイブリッド接続



プレビュー

解決策 3:
ネットワークをより可視化する　Flow Analyzer

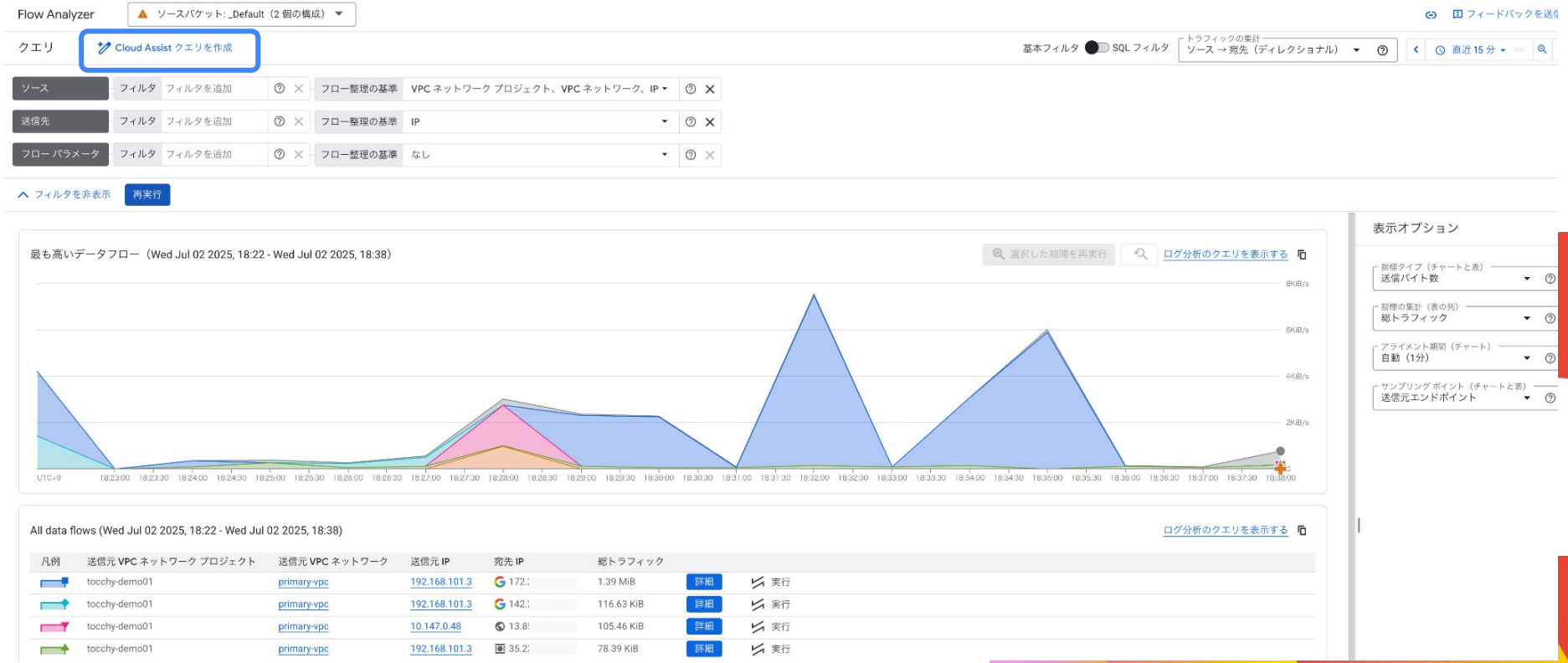
- **Network Intelligence Center に追加された新しい機能**
  - VPC Flow Logs を分析するための複雑な SQL クエリを記載することなくトラフィック フローを解析可能に



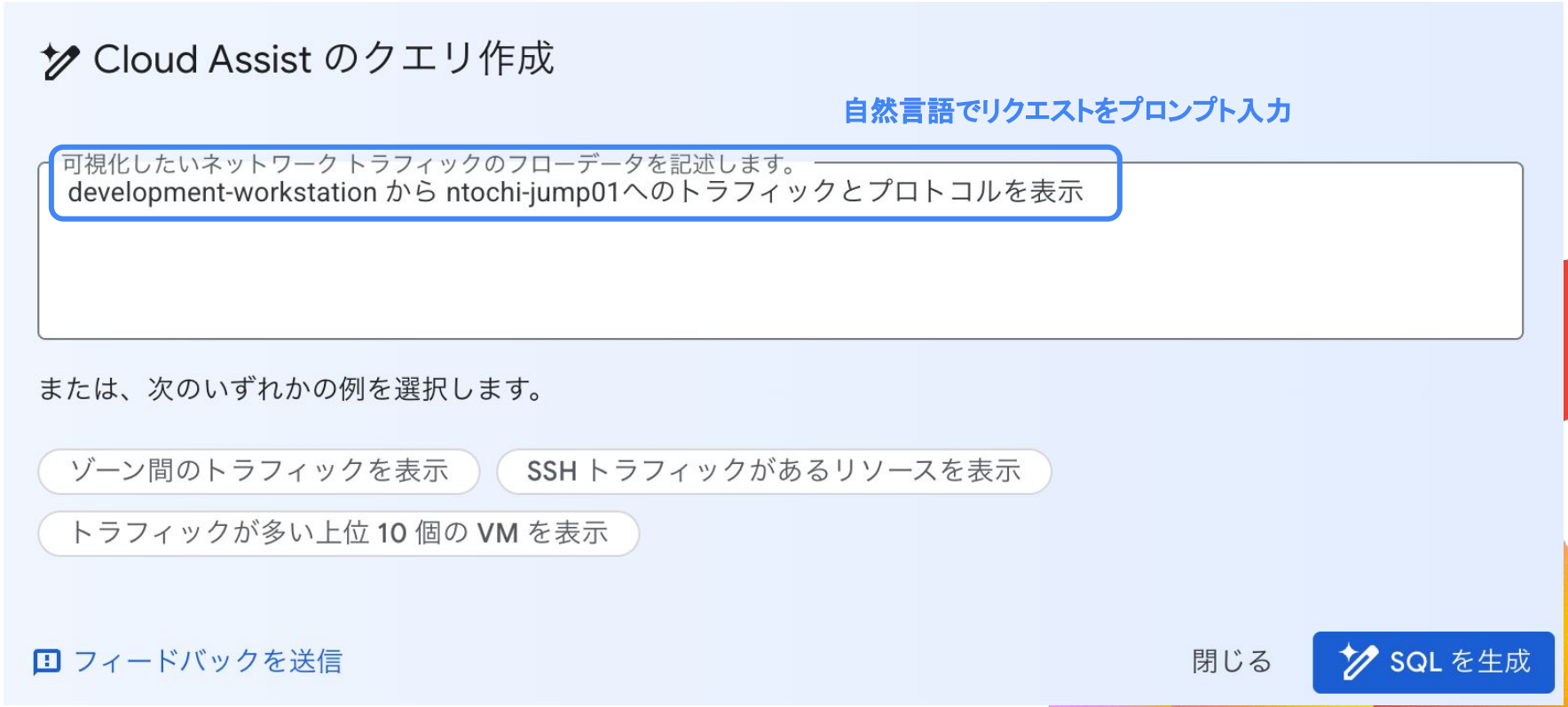
VPC Flow Logs を設定

Flow Analyzer を選択

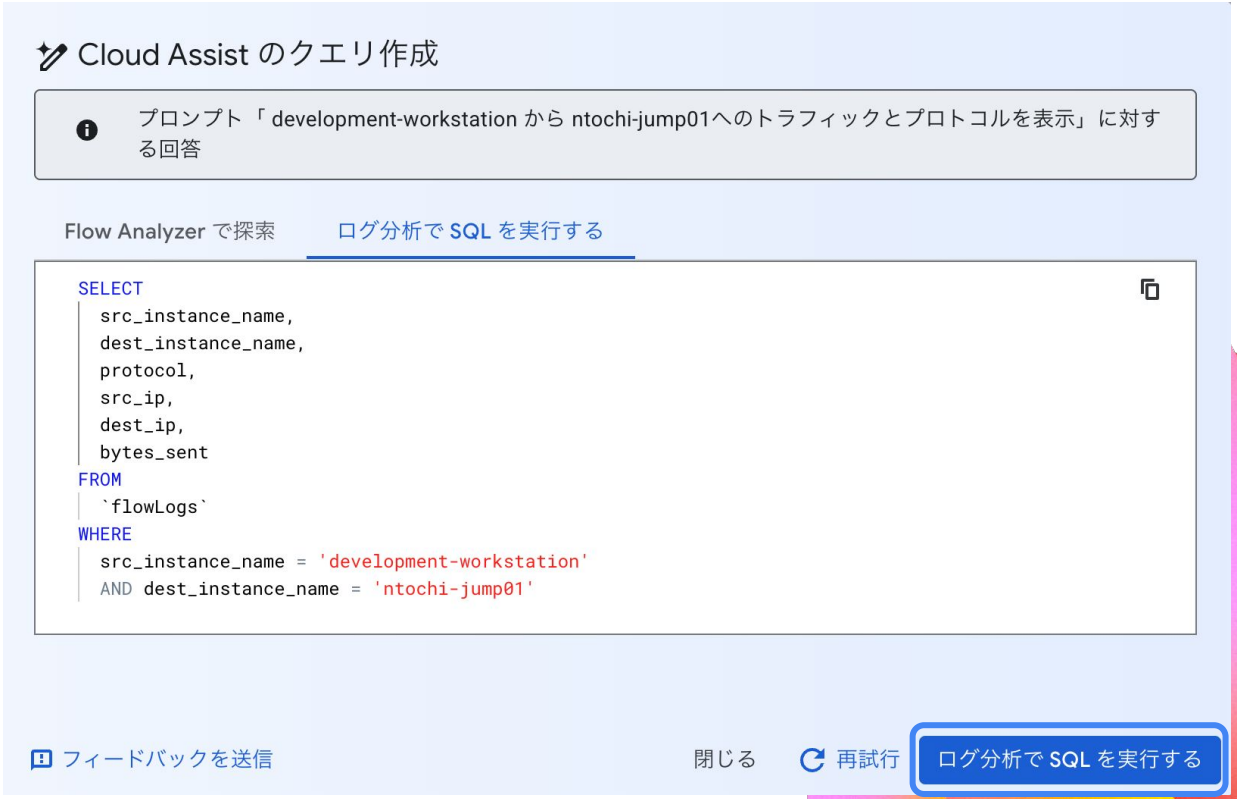
Flow Analyzer で Cloud Assist クエリを作成



Flow Analyzer で Cloud Assist クエリを作成



Cloud Assist が SQL を生成



クエリ結果がテーブル表示

ログ分析

直近 1 時間 JST

クエリ　最近 (4)　保存済み (0)

保存　クエリを実行

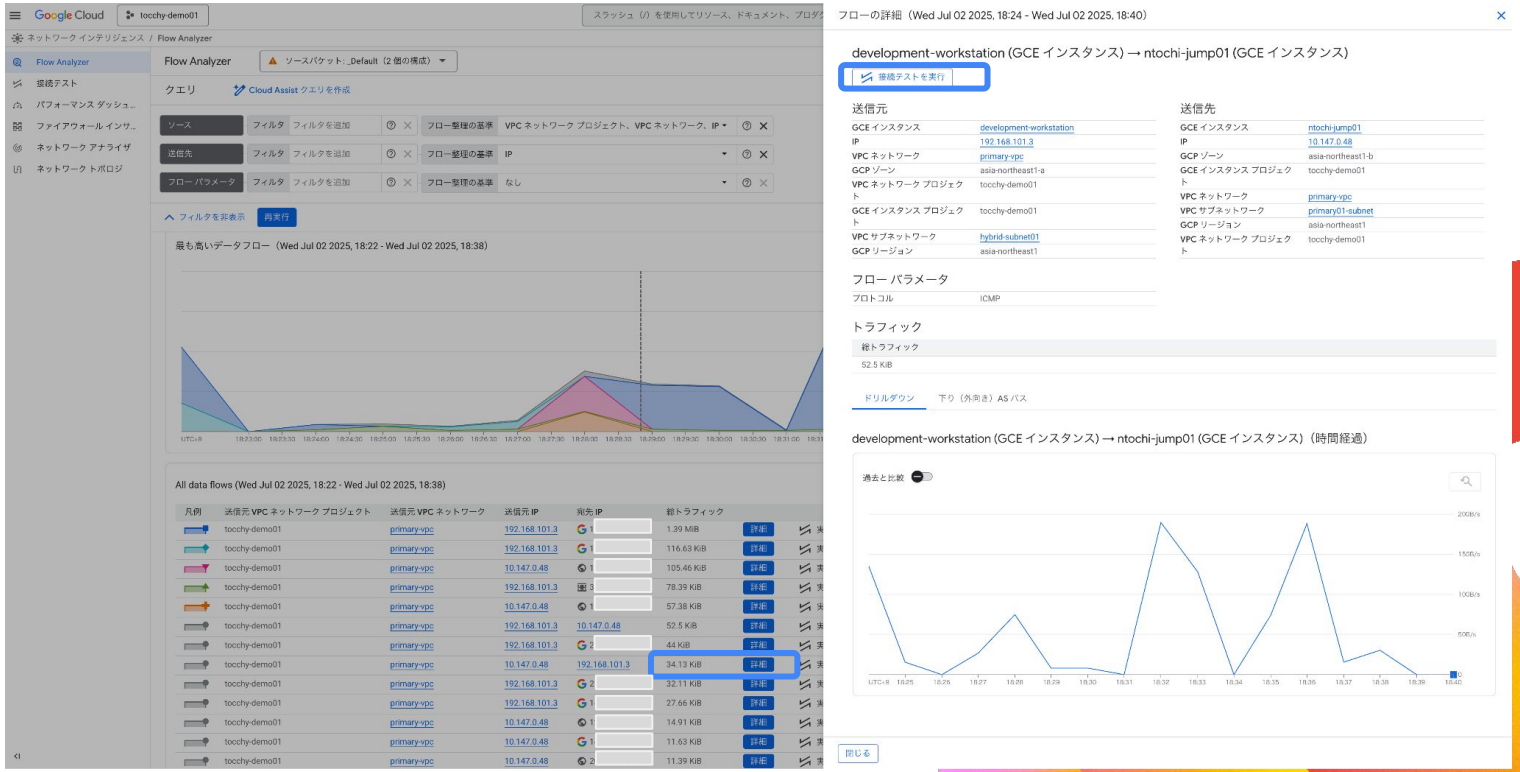
形式　消去　SQL リファレンス　実行可能

```
--
-- この WITH ステートメントは、Gemini により生成されたクエリで VPC Flow Logs からの必要なデータキャストを提供するものです。生成されたクエリは以下のとおりです。
--
WITH
  flowLogs AS (
  SELECT
    JSON_VALUE(json_payload.connection.src_ip) AS src_ip,
    JSON_VALUE(json_payload.connection.dest_ip) AS dest_ip,
    JSON_VALUE(json_payload.src_instance.vm_name) AS src_instance_name,
    JSON_VALUE(json_payload.dest_instance.vm_name) AS dest_instance_name,
    CAST(JSON_VALUE(json_payload.connection.protocol) AS INT64) AS protocol,
    CAST(JSON_VALUE(json_payload.bytes_sent) AS INT64) AS bytes_sent,
    timestamp,
    PARSE_TIMESTAMP("%Y-%m-%dT%H:%M:%E*SZ", JSON_VALUE(json_payload.start_time)) AS start_time,
    PARSE_TIMESTAMP("%Y-%m-%dT%H:%M:%E*SZ", JSON_VALUE(json_payload.end_time)) AS end_time,
  FROM
    `tocchy-demo01.global._Default._Default`
  WHERE
    log_id IN ('compute.googleapis.com/vpc_flows',
      'networkmanagement.googleapis.com/vpc_flows') )
  --
  -- Gemini により生成されたクエリの開始
  --
SELECT
  src_instance_name,
  dest_instance_name,
  protocol,
  src_ip,
  dest_ip,
  bytes_sent
FROM
  `flowLogs`
WHERE
  src_instance_name = 'development-workstation'
  AND dest_instance_name = 'ntochi-jump01'
```

結果 (335)　テーブル　平均読み込み時間のチャート　両方　ダウンロード　アラートを作成　ダッシュボードに保存

行	src_instance_name STRING	dest_instance_name STRING	protocol INTEGER	src_ip STRING	dest_ip STRING	bytes_sent INTEGER
1	development-workstation	ntochi-jump01	1	192.168.101.3	10.147.0.48	16128
2	development-workstation	ntochi-jump01	1	192.168.101.3	10.147.0.48	896
3	development-workstation	ntochi-jump01	1	192.168.101.3	10.147.0.48	896
4	development-workstation	ntochi-jump01	1	192.168.101.3	10.147.0.48	224

Flow Analyzer から接続テストの実行も可能



Flow Analyzer から接続テストの実行も可能

04. 脅威からシステムを保護するための可視化とセキュリティ管理の効率化

攻撃対象は増える一方、セキュリティ人材は足りない

攻撃は賢く、より広範囲に

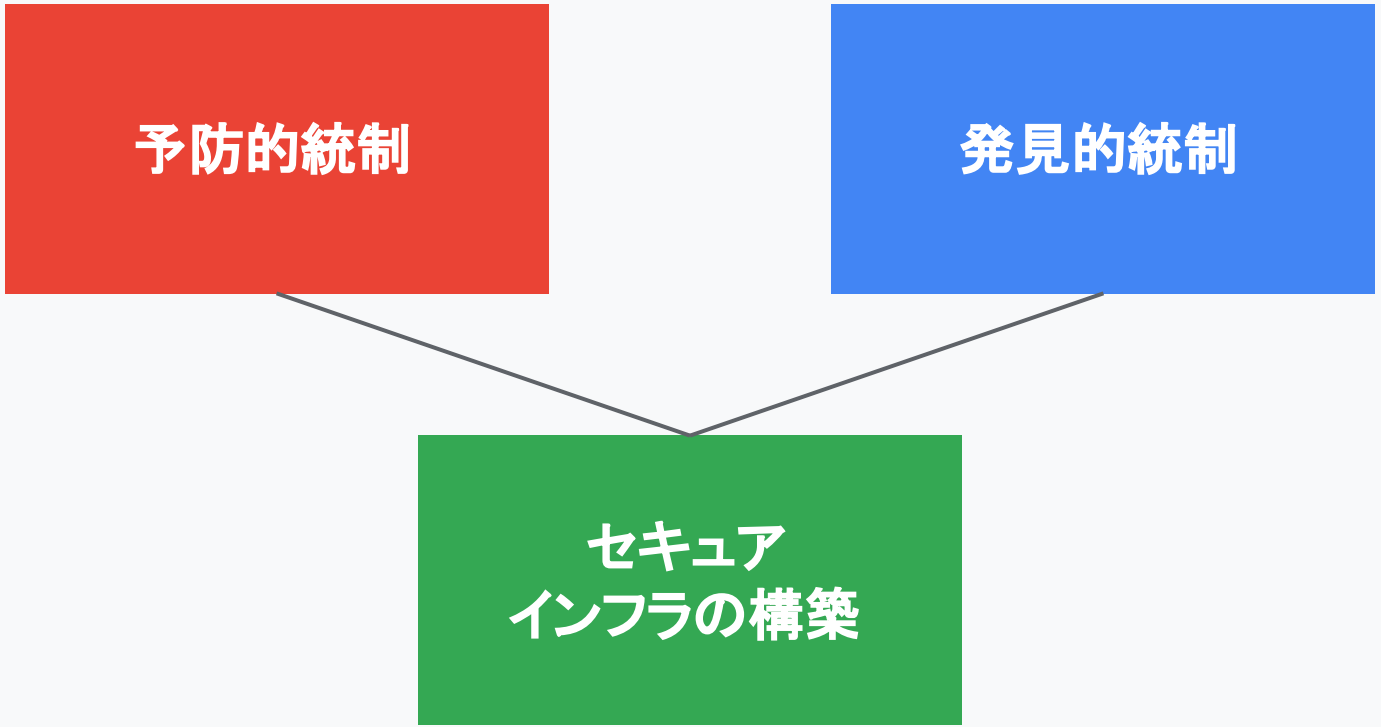
- **攻撃手法の高度化**
  AIを活用した自動攻撃、ゼロデイ脆弱性の悪用が当たり前に
- **攻撃対象領域の爆発的拡大**：
  クラウド、API、コンテナ、サプライチェーン... ビジネスの成長そのものが新たな「入口」を生み出す。

人手と時間には限りがある

- **終わらないアラート対応**
  大量のアラートに追われ、本当に危険な兆候を見抜けない「アラート疲れ」
- **深刻な専門家不足**
  高度な脅威を分析・対応できる人材が不足し、一人の担当者への負荷は増すばかり

「事後対応（リアクティブ）運用」には限界がある

プラットフォーム セキュリティ検討の指針



解決策 1:
セキュリティ対策の全体像を見据える

予防的統制

サービス アカウントの利用
IAM を通した最小権限の原則の徹底

組織ポリシーの活用

セキュア インフラの構築

Private Service Connect
API アクセス制御

Cloud NGFW（Firewall、IPS）
Cloud Armor（WAF、DDoS対策）

VPC
Service Controls

予防的統制 、セキュア インフラの構築 を
行ったうえでカバーできない
データの移動をペリメーター
（境界）で制御

発見的統制

Security Command Center
Cloud Operations

解決策 2：
セキュリティ事故を未然に防ぐ、発見できる準備

- 組み込みの脅威検出機能、Google Cloud セキュリティサービス、サードパーティ セキュリティサービスなどの情報を収集・分析設定
- ミスや脅威、脆弱性などのリスクをダッシュボードとして可視化する
- 検知・可視化したリスクへ対応するために、他の Google Cloud サービスや SIEM/SOAR と連携する

Security Command Center

リスクの検知 → リスクの可視化 → リスクへの対応

Security Command Center

- Container Threat Detection
- Event Thread Detection
- Security Health Analytics
- Virtual Machine Threat Detection
- Web Security Scanner
- Cloud Run Threat Detection プレビュー

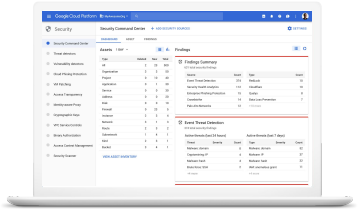
統合された Google Cloud セキュリティサービス

- Anomaly Detection
- Cloud Armor
- Sensitive Data Protection
- Asset Inventory
- VM Manager

サードパーティ セキュリティサービス

- Acalvio
- Prisma
- Chef
- McAfee

- アセットダッシュボード
- 脅威ダッシュボード
- 脆弱性ダッシュボード
- コンプライアンスダッシュボード
- 検出結果ダッシュボード
- ソースダッシュボード



その他Googleサービスとの連携

Cloud Pub/Sub → Cloud Run Functions

BigQuery への検出結果のエクスポート

BigQuery

サードパーティサービスとの連携

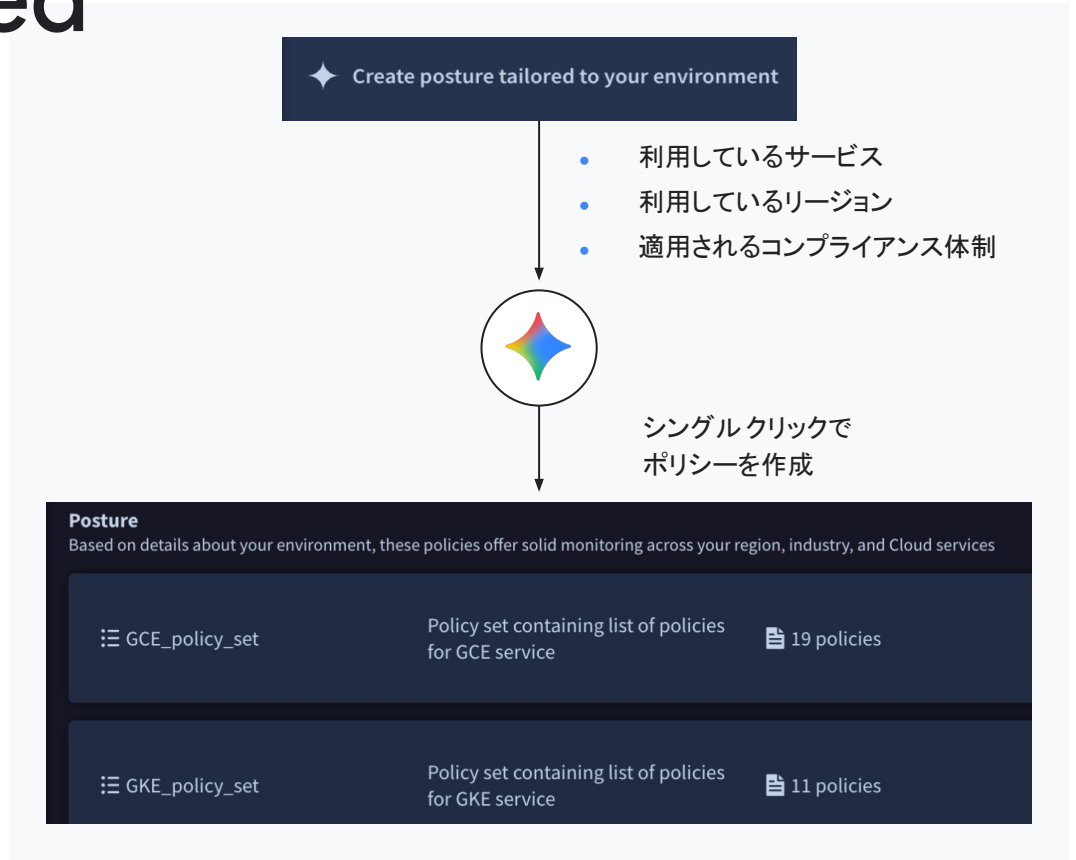
- Elastic Stack
- ServiceNow
- Splunk
- QRadar

Enterprise / Premium Tier　プライベート プレビュー

Gemini-generated Postures for Google Cloud

自分でカスタムの Security Posture Policy を 作成するのは難しく、時間もかかる

Gemini と Security Command Center に自社のクラウド環境に合った Posture Policy を作成してもらう

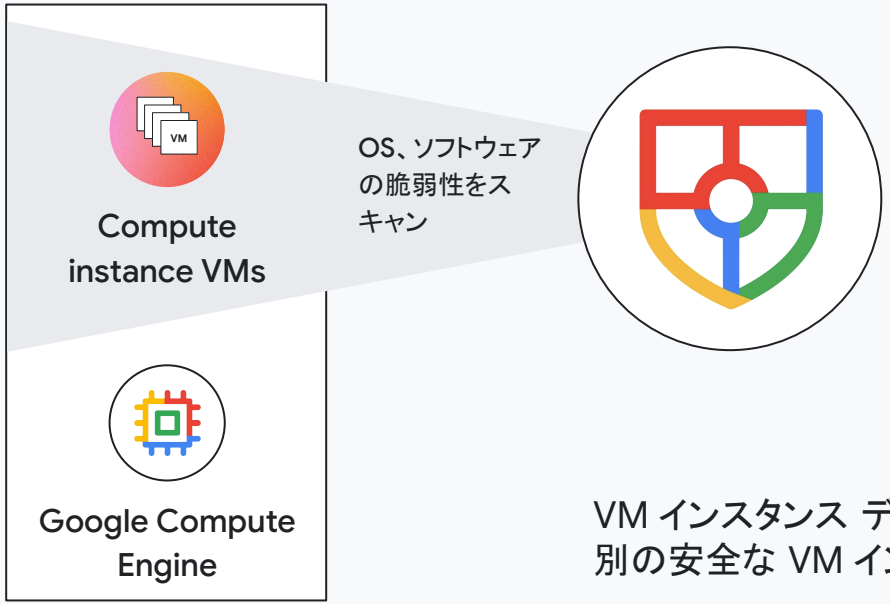


Gemini を利用して自社にあったセキュリティ要件を定義してポリシーとして設定

Enterprise / Premium Tier　プレビュー

エージェントレス脆弱性管理

Vulnerability Assessment for Google Cloud



- 導入や管理が必要なエージェントは不要
- お客様のクラウドリソースは消費されない
- 追加のライセンスコストは不要

VM インスタンス ディスクのクローンを定期的に作成して別の安全な VM インスタンスでチェックを実施

従来の VM Manager による エージェント ベースの脆弱性管理も利用可能

Premium Tier　プレビュー

バックアップ データに対する脅威を検出する

Event Threat Detection Rule

Backup and DR のバックアッププランや
バックアップデータの削除に対応

Ransomware

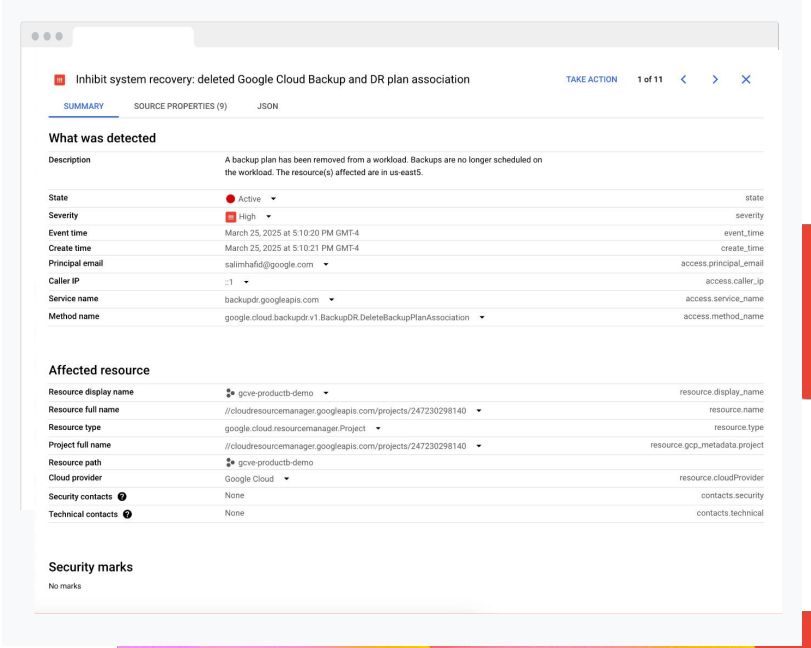
- ランサムウェアの
  主な脅威は
  データ損失
- 攻撃者は
  バックアップの
  侵害を目指す

破壊的行為の検出

バックアップおよびBackup Vault の
削除の試行

**リカバリーに影響がある
イベントを検出**

バックアップ プラン および バックアップ
インフラの削除



Enterprise / Premium Tier

プレビュー

Cloud Run の脅威検出

ハイリスクなインシデントの検出

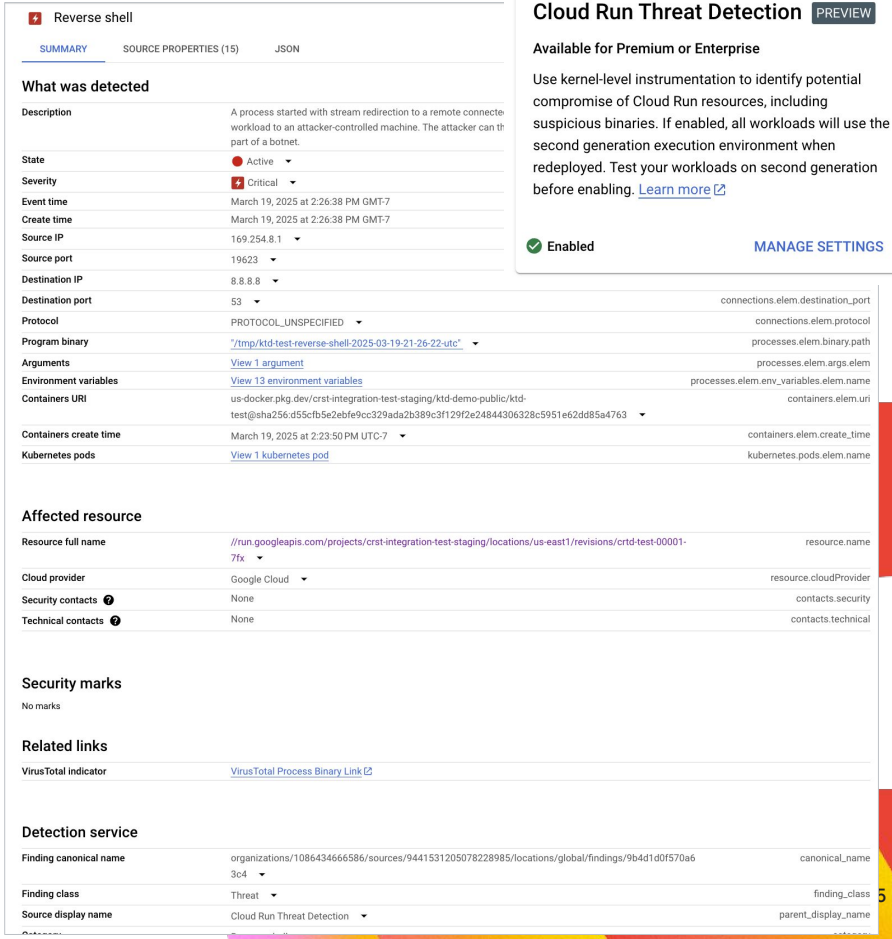
Cloud Run で動くアプリに対して異常なビヘイビア、
未知のアクセス試行、脆弱性および脅威などを継続的に
モニタリング

検知と調査

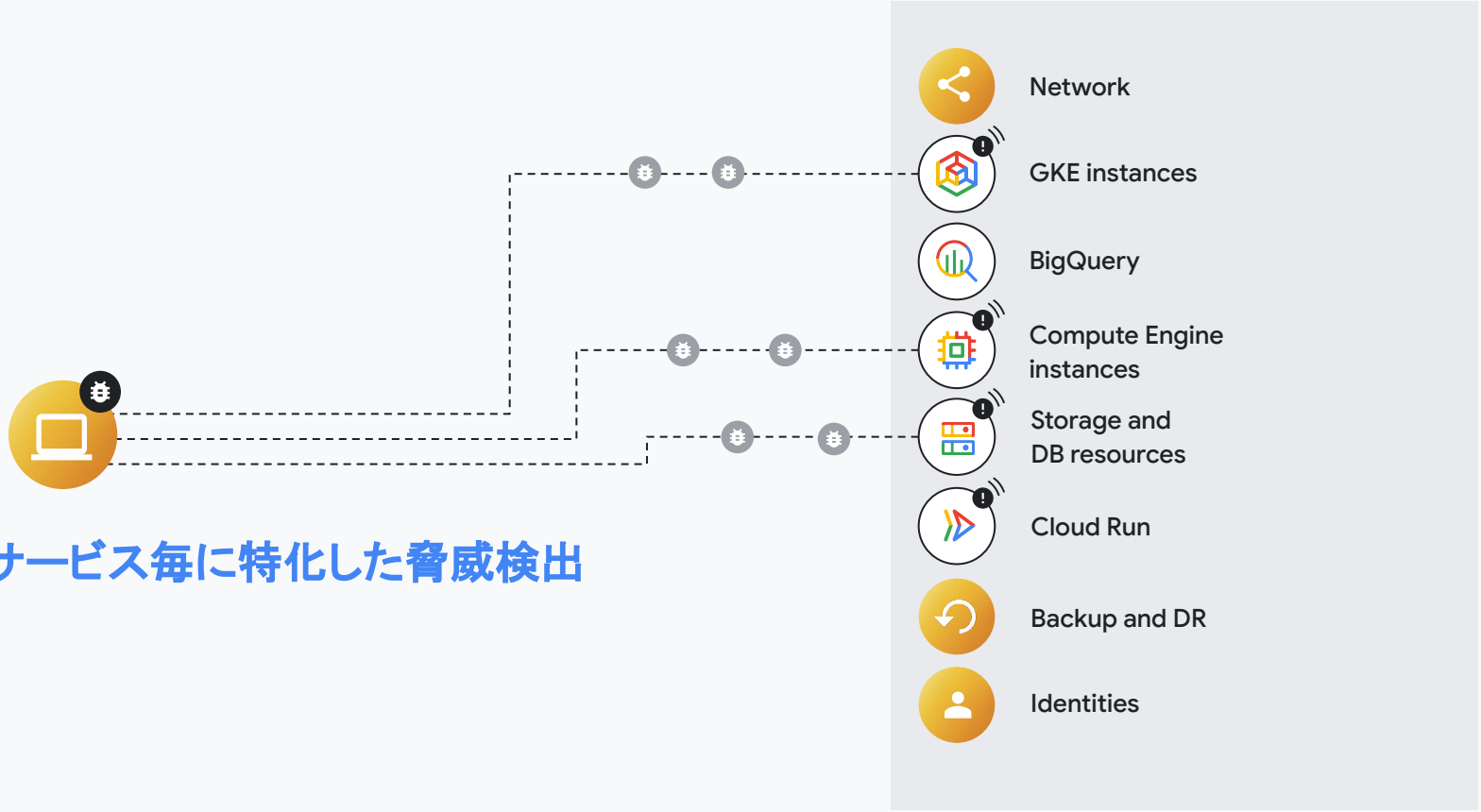
ニアリアルタイムにランタイムに対する攻撃を検出して
最新の脅威インテリジェンスを利用して調査

Shift-left security

セキュリティインサイト、アラート、および組み込みの
修復機能で、セキュリティの問題が発生を抑制



アクティブに脅威を検出する



サービス毎に特化した脅威検出

05. まとめ

2025 年のモダンインフラの姿

- Compute Engine や Hyperdisk などの**最新技術と AI の活用で性能向上とコスト最適化は** トレードオフではなく**同時に実現することが可能**
- クラウド **ネットワークの特性を理解** して、**AI** や クラウドが提供する**マネージドサービスの利点を最大限に活用** してネットワークの運用を楽にする
- **セキュリティ対策のポートフォリオを俯瞰** した上したうえで、セキュリティ事故の**予兆を発見** できる組みを少しずつ導入していく