

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

Proprietary

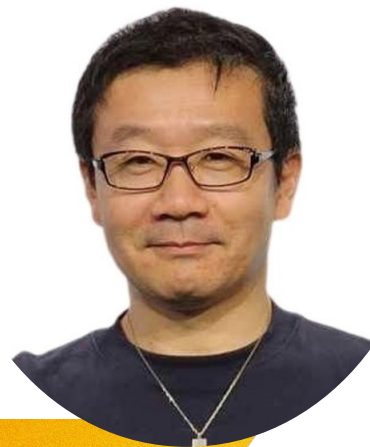


Naoki Tochizawa | 栃沢 直樹

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



Azoo 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、場当たりの対応が優先

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

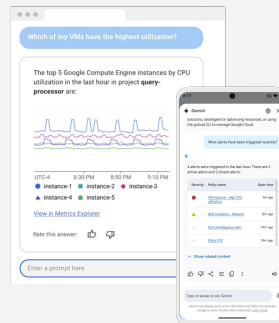


Gemini

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

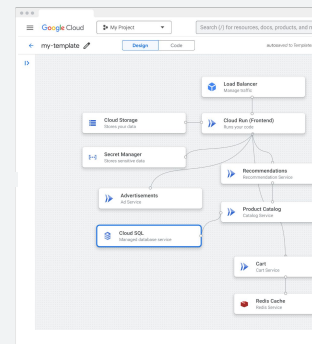
Experiencing issues? Investigate

questions about Google Cloud products and best practices, and retrieve information about your cloud resources.

Learn more about how to configure and use Gemini

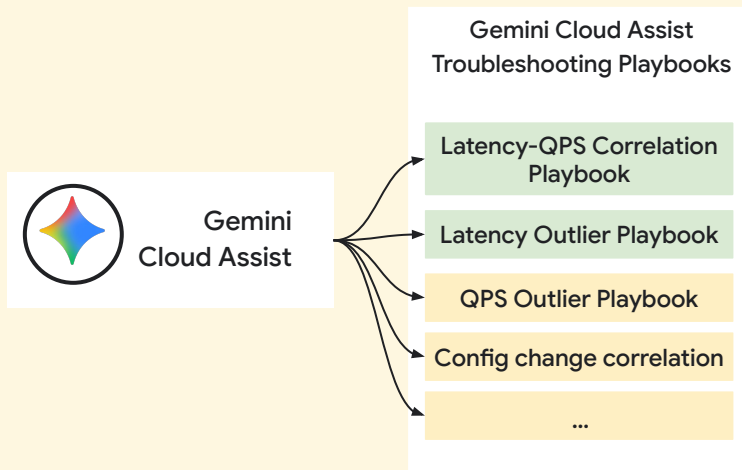
AI による調査支援

デザイン
統合



Google Cloud Assist

Gemini Cloud Assist Operations



Gemini is an AI-powered collaborator to help you get more done faster. Get answers to your questions about how to get started with a Cloud solution, strategies for optimizing resources, or using the gcloud CLI to manage Google Cloud.

In addition to general knowledge about Google Cloud, it also has some awareness of your context, like your project and console page.

How does Bigtable handle conflicting write requests?

How does GKE scale my clusters?

What is the difference between SSD and HDD?

Enter a prompt here



For best results use a detailed prompt. [Prompt guide](#)

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ください。」
- 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)

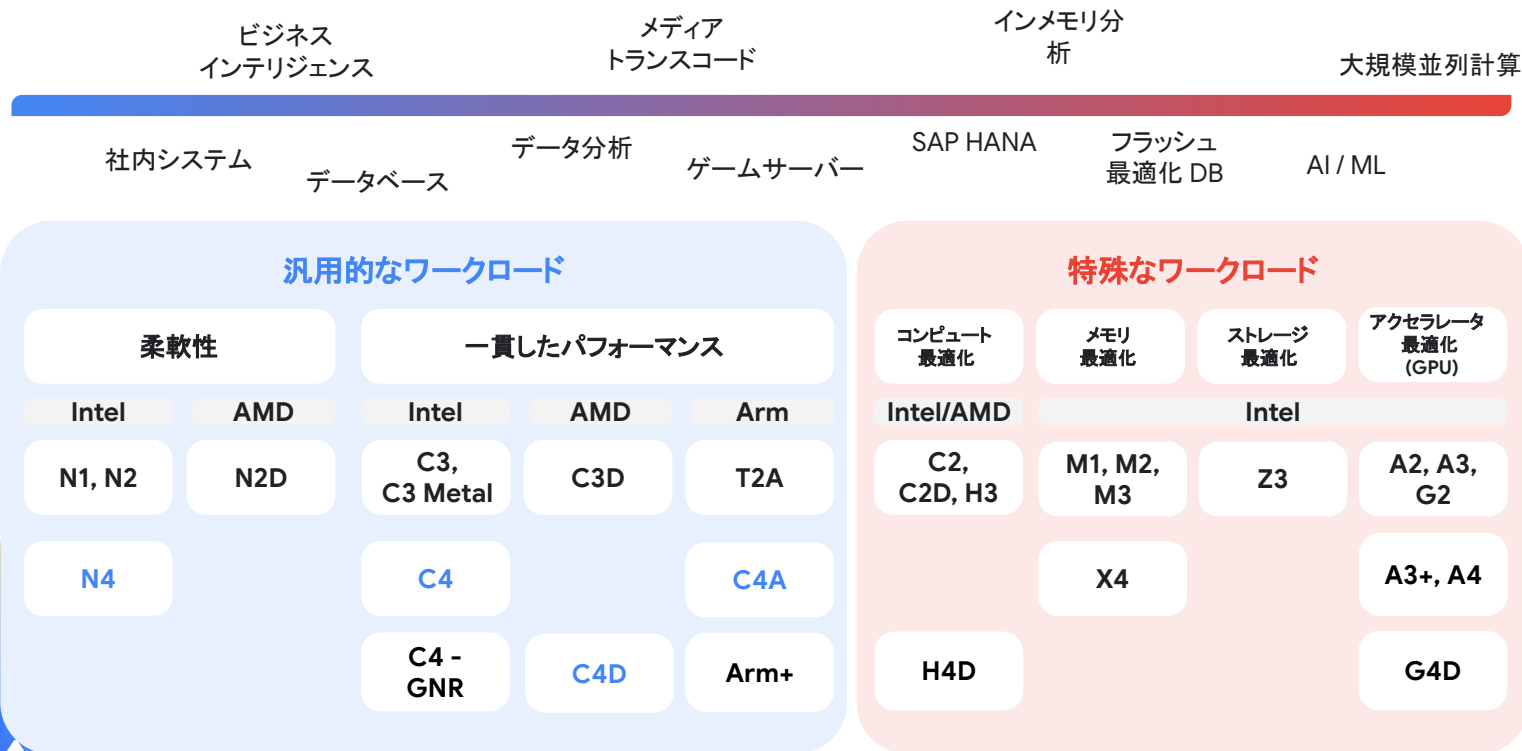
- IPU 搭載のマシンを使用して、ストレージやネットワーク処理をデータセンター側にオフロード
- ホストのコンピューティングリソースとメモリリソースを解放し、リアルタイムワークロードの CPU 応答性を最大 80% 向上させます



Hyperdisk による 性能の向上

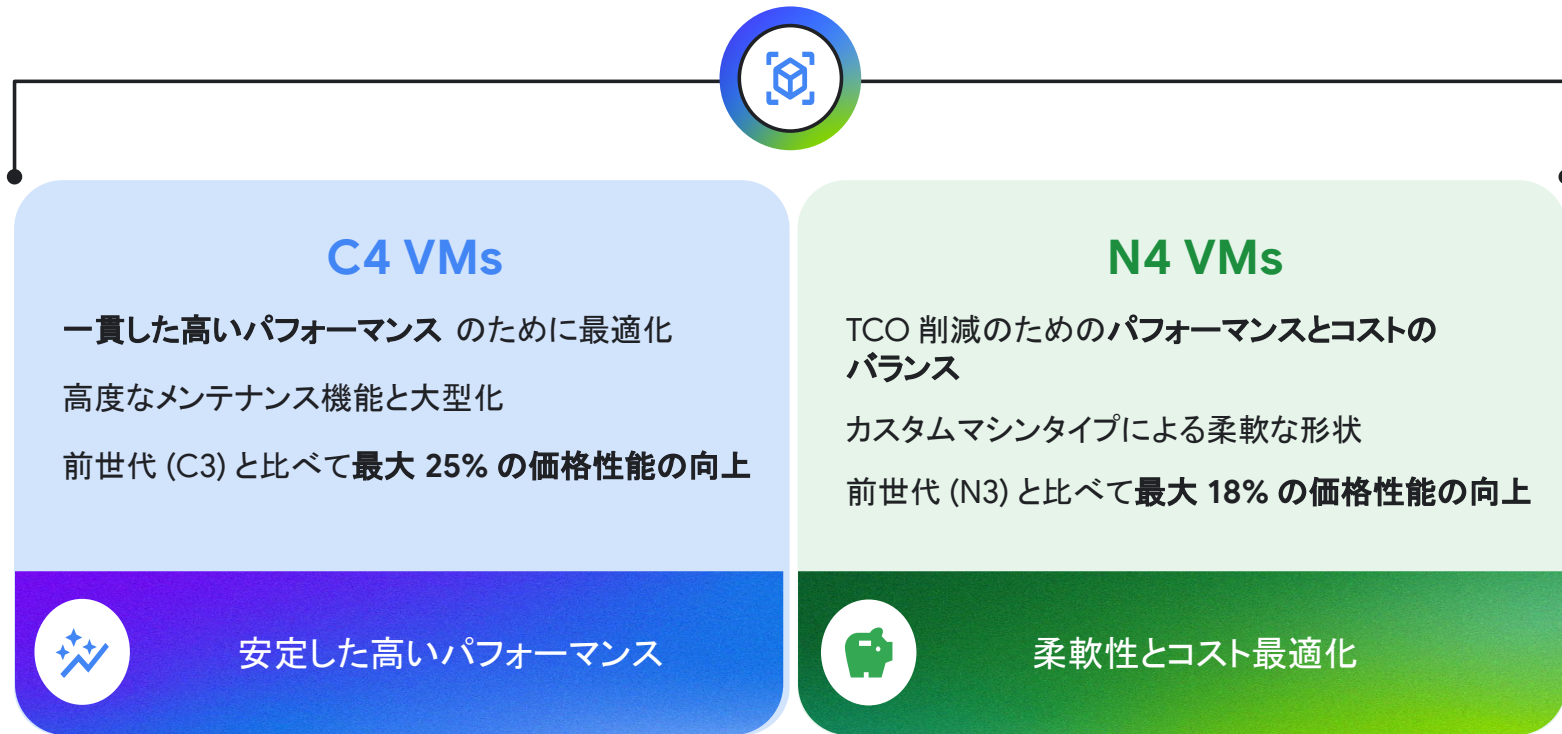
- IPU アーキテクチャを最大限活用し、Compute Engine のサイズと切り離してパフォーマンスを得ることが可能
- ワークロードに合わせてストレージ容量を簡単かつ動的に調整可能

Compute Engine ファミリー



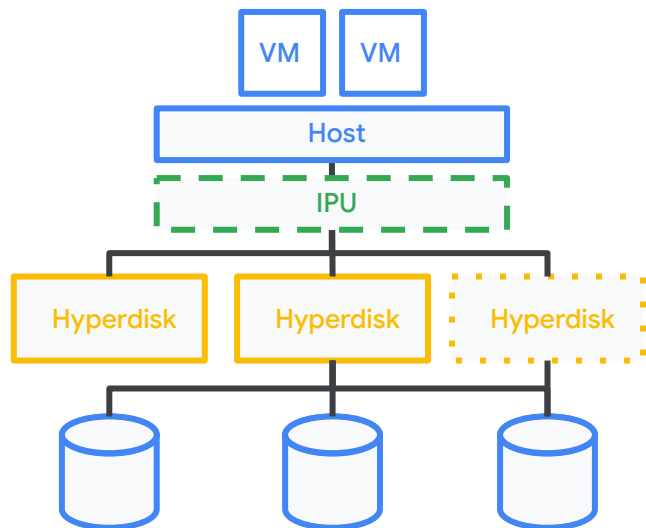
Intel ベースの C4 と N4 マシンの使い分け

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

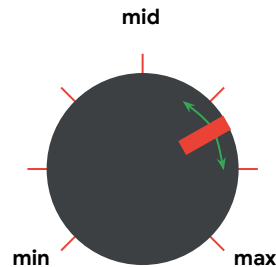


Hyperdisk によるパフォーマンスの最適化

Infrastructure 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



パフォーマンス



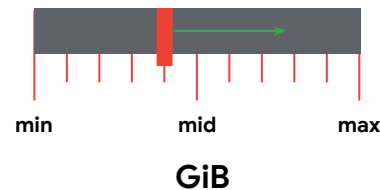
IOPs

\$0.xx per IOP/s

Throughput

\$0.xx per MiB/s

キャパシティ
(ストレージ容量)

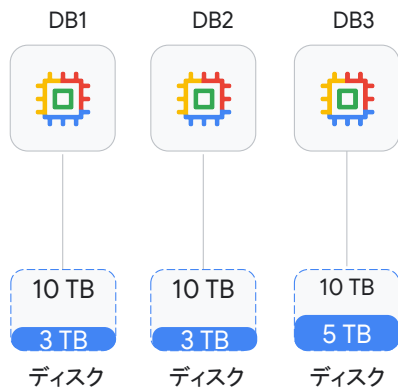


Capacity

\$0.xx per GiB

Storage Pool による最適化

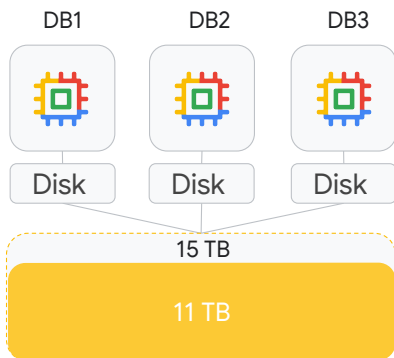
現在 (Persistent Disk)



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

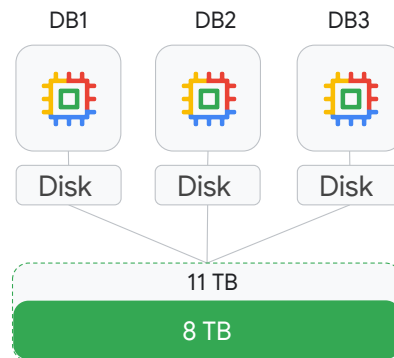


Storage Pool

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



Storage Pool

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



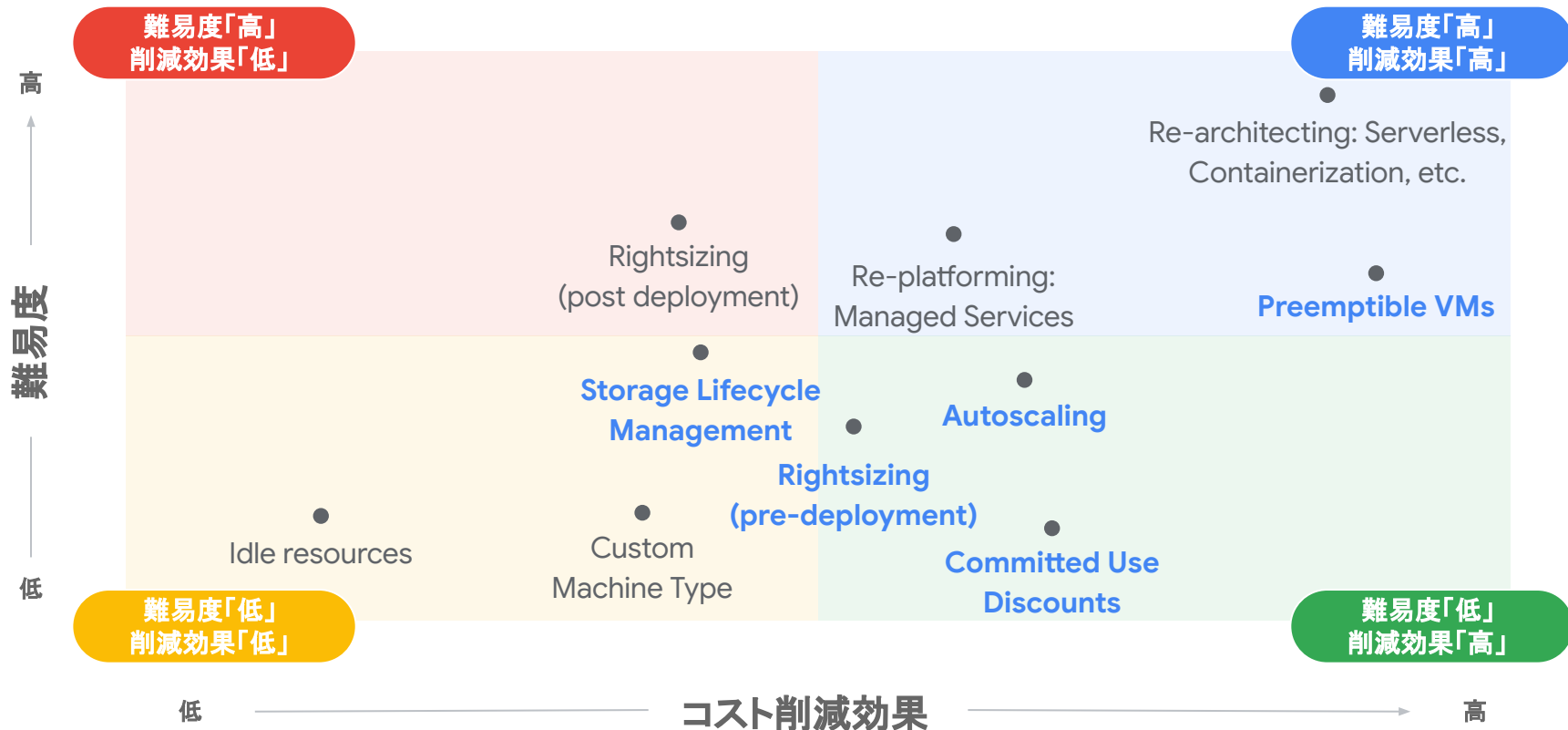
- Flexible MIG による Zone や Instance Type の柔軟性
- Capacity Planner による将来の需要を分析および予測
- Quota 管理によるリソース枯渇や制限の確認

運用最適化



- MIG による自動修復、自動スケールリング、マルチゾーン稼働
- Batchによるワークロードのスケジューリング、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



Gemini is an AI-powered collaborator to help you get more done faster. Get answers to your questions about how to get started with a Cloud solution, strategies for optimizing resources, or using the gcloud CLI to manage Google Cloud.

In addition to general knowledge about Google Cloud, it also has some awareness of your context, like your project and console page.

What is the difference between SSD and HDD?

What is Secret Manager?

What can I use Eventarc for?

Enter a prompt here



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？

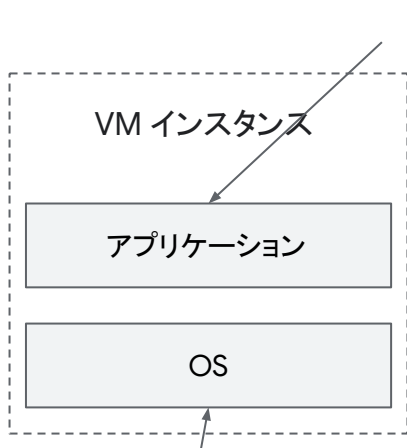


クラウド移行を実現したお客様が抱える ネットワークの課題

- 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



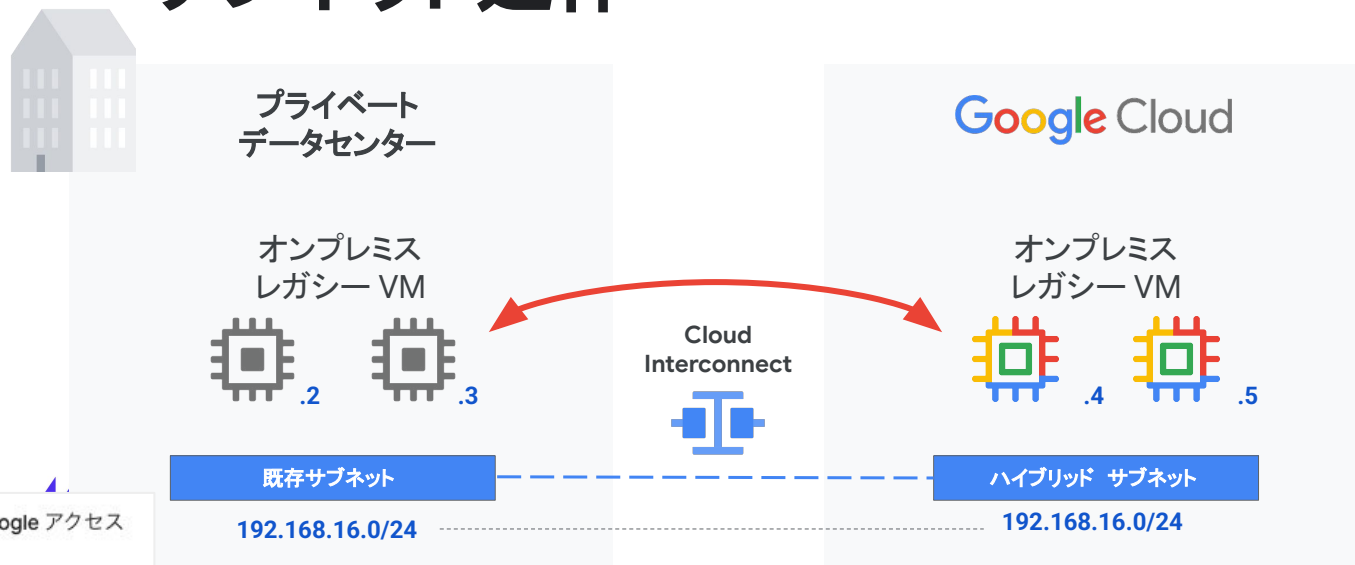
IP を変更しない限り、ハイブリッド クラウド構成を
前提として移行することは困難

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



プライベート Google アクセス

- オン
 オフ

ハイブリッドサブネット ?

- オン
 オフ

保存

キャンセル

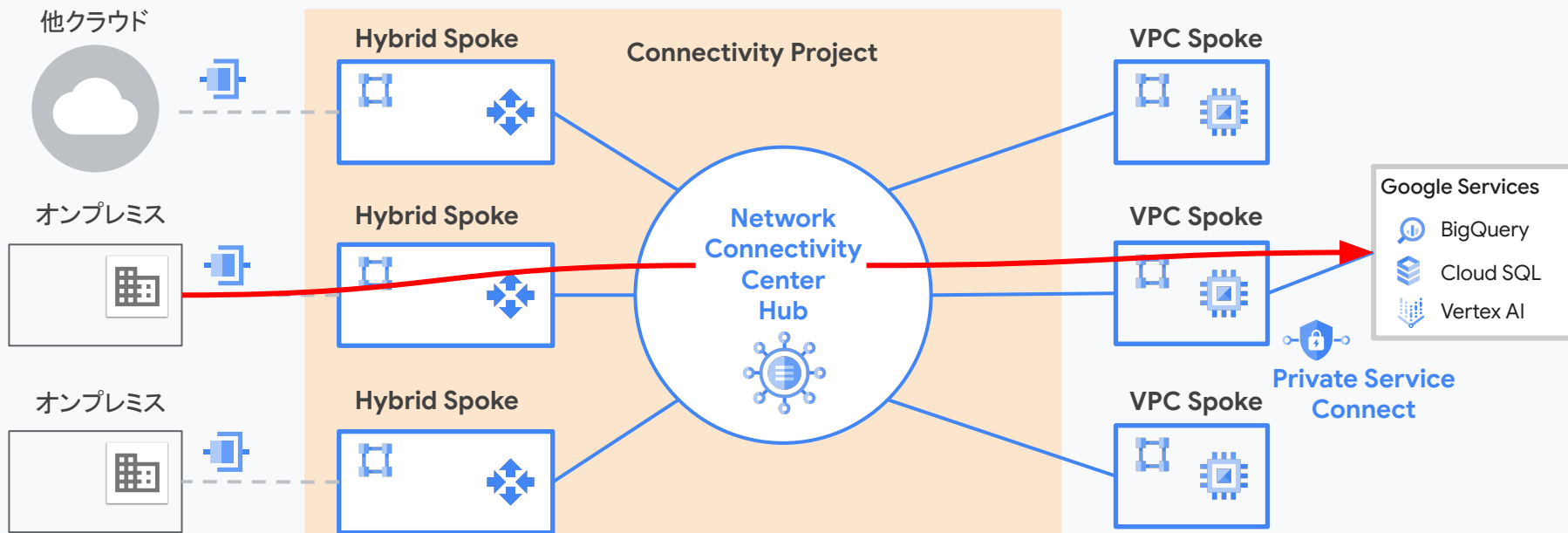
- 設定は VPC のサブネットで [ハイブリッド サブネット] を “ON” にするだけ
 - オンプレミスルータでは Proxy ARP が有効になっていれば OK
- IP アドレスを変えられないレガシー VM の移行にも対応
- Migrate to Virtual Machine (M2VM) による移行にも対応

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	
	共有 VPC	Network Connectivity Center (NCC)	サービス公開型
			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

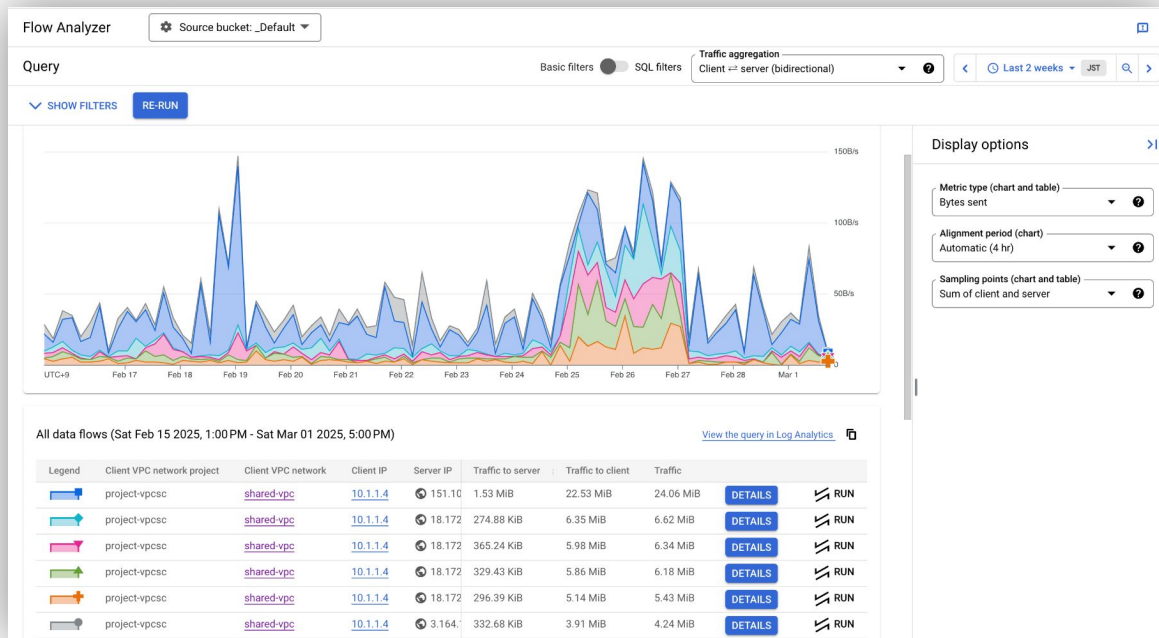
Network Connectivity Center を利用したシンプルなハイブリッド接続



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

VPC ネットワーク / VPC ネットワーク

VPC ネットワーク [+ VPC ネットワークを作成](#) [更新](#)

現在のプロジェクトのネットワーク 現在のプロジェクトのサブネット

i このプロジェクトでは SMTP ポート 25 が許可されていません。 [詳細](#)

VPC ネットワーク [Manage flow logs](#) [プレビュー](#)

フィルタ [primary-vpc](#) プロバティ名または値を入力

<input type="checkbox"/>	名前 ↑	サブネット	MTU ?	モード	IPv6 ULA 範囲	ゲートウェイ	フローログ構成 ?
<input type="checkbox"/>	primary-vpc	6	1500	カスタム			+ 1

VPC Flow Logs を構成する [×](#)

構成 - 組織 [プレビュー](#)

[構成を追加](#)

構成 - VPC ネットワーク [プレビュー](#)

新しい構成 [✕](#)

名前 * -primary-vpc [?](#)
小文字、数字、ハイフンのみ使用できます

説明

集計間隔
サンプリングされたパケットの情報がこの間隔で集計され、フローログ レコードが生成されます。詳細については、次をご覧ください。 [ログの収集](#)

5秒 30秒 1分 5分 15分

↑ 詳細設定

フィルタに一致するログのみ保持
詳細については、 [ログのフィルタリング](#) をご覧ください。

メタデータ アノテーション
フローログ レコードに含めることができる追加情報。利用可能なメタデータ アノテーションのリストについては、 [レコードの形式](#) をご覧ください

すべて選択
 カスタム

セカンダリ サンプリング レート * % [?](#)

完了

Flow Analyzer を選択

VPC Flow Logs

VPC Flow Logs は、ネットワーク トラフィックをサンプリングしてフローログを生成します。VPC Flow Logs は、組織、VPC ネットワーク、または個々のリソース（サブネット、Cloud Interconnect の VLAN アタッチメント、Cloud VPN トンネルなど）に対して構成できます。VPC Flow Logs を使用すると、ネットワーク トラフィック パターンの分析情報を取得して、費用を最適化したり、ネットワーク セキュリティを強化したりできます。 [詳細](#)

VPC Flow Logs の構成を追加

組織レベルの構成 [プレビュー](#) [Flow Analyzer で表示](#)

≡ フィルタ プロパティ名または値を入力

<input type="checkbox"/>	設定名 ↑	構成の詳細	ステータス	操作
--------------------------	-------	-------	-------	----

表示できる組織レベルのフローログの構成はありません

プロジェクト レベルの構成 [Flow Analyzer で表示する](#)

[VPC ネットワーク](#) [プレビュー](#) [サブネット](#) [プレビュー](#) [VLAN アタッチメント](#) [Cloud VPN トンネル](#)

≡ フィルタ プロパティ名または値を入力

<input type="checkbox"/>	設定名	VPC ネットワークの名前 ↑	構成の詳細	ステータス	操作
--------------------------	-----	-----------------	-------	-------	----

<input type="checkbox"/>	demo-flow-primary-vpc	primary-vpc	集計: 5 秒 metadata: すべて	オン	Flow Analyzer で表示 ⋮
--------------------------	-----------------------	-------------	-------------------------	----	-------------------------------------

Flow Analyzer で Cloud Assist クエリを作成

Flow Analyzer

▲ ソースバケット: _Default (2 個の構成) ▼

🔄 📄 フィードバックを送信

クエリ

🔗 Cloud Assist クエリを作成
基本フィルタ SQL フィルタ

トラフィックの集計

ソース → 宛先 (ディレクショナル)

🔍

◀

🕒

直近 15 分

▶

🔍

ソース	フィルタ	フィルタを追加	🔍	✕	フロー整理の基準	VPC ネットワーク プロジェクト、VPC ネットワーク、IP	🔍	✕
送信先	フィルタ	フィルタを追加	🔍	✕	フロー整理の基準	IP	▼	🔍
フロー パラメータ	フィルタ	フィルタを追加	🔍	✕	フロー整理の基準	なし	▼	🔍

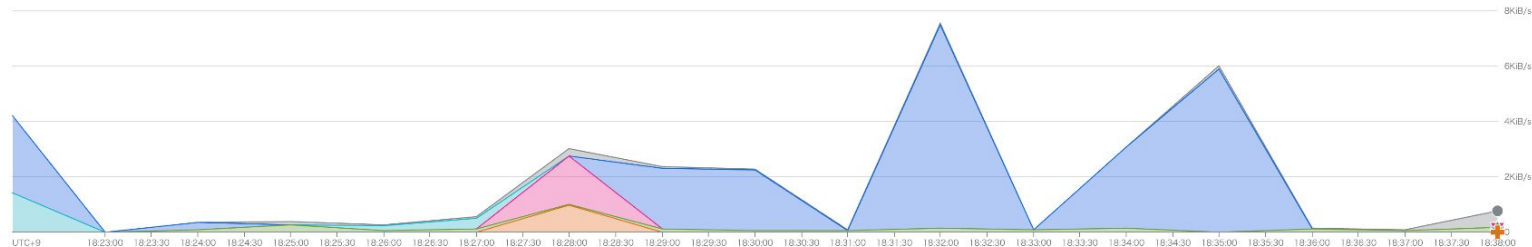
⏪ フィルタを非表示

再実行

最も高いデータフロー (Wed Jul 02 2025, 18:22 - Wed Jul 02 2025, 18:38)

🔍 選択した期間を再実行

🔍

[ログ分析のクエリを表示する](#)
📄


表示オプション

- 指標タイプ (チャートと表)
 - 送信バイト数
- 指標の集計 (表の列)
 - 総トラフィック
- アラメント期間 (チャート)
 - 自動 (1分)
- サンプリング ポイント (チャートと表)
 - 送信元エンドポイント

All data flows (Wed Jul 02 2025, 18:22 - Wed Jul 02 2025, 18:38)

[ログ分析のクエリを表示する](#)
📄

凡例	送信元 VPC ネットワーク プロジェクト	送信元 VPC ネットワーク	送信元 IP	宛先 IP	総トラフィック		
	tocchy-demo01	primary-vpc	192.168.101.3	172.:	1.39 MiB	詳細	🚫 実行
	tocchy-demo01	primary-vpc	192.168.101.3	142.:	116.63 KiB	詳細	🚫 実行
	tocchy-demo01	primary-vpc	10.147.0.48	13.8:	105.46 KiB	詳細	🚫 実行
	tocchy-demo01	primary-vpc	192.168.101.3	35.2:	78.39 KiB	詳細	🚫 実行

Flow Analyzer で Cloud Assist クエリを作成

✎ Cloud Assist のクエリ作成

自然言語でリクエストをプロンプト入力

可視化したいネットワークトラフィックのフローデータを記述します。 —
development-workstation から ntochi-jump01へのトラフィックとプロトコルを表示

または、次のいずれかの例を選択します。

ゾーン間のトラフィックを表示

SSH トラフィックがあるリソースを表示

トラフィックが多い上位 10 個の VM を表示

📧 フィードバックを送信

閉じる

✎ SQL を生成

Cloud Assist が SQL を生成

✍️ Cloud Assist のクエリ作成

- ❶ プロンプト「development-workstation から ntochi-jump01へのトラフィックとプロトコルを表示」に対する回答

Flow Analyzer で探索

ログ分析で SQL を実行する

```
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'
```

🗨️ フィードバックを送信

閉じる

🔄 再試行

ログ分析で SQL を実行する

クエリ結果がテーブル表示

ログ分析

クエリ 最近 (4) 保存済み (0)

形式 消去 SQLリファレンス

実行可能

```

1  --
2  -- 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。
3  --
4  WITH
5  flowLogs AS (
6  SELECT
7    JSON_VALUE(json_payload.connection.src_ip) AS src_ip,
8    JSON_VALUE(json_payload.connection.dest_ip) AS dest_ip,
9    JSON_VALUE(json_payload.src_instance.vm_name) AS src_instance_name,
10   JSON_VALUE(json_payload.dest_instance.vm_name) AS dest_instance_name,
11   CAST(JSON_VALUE(json_payload.connection.protocol) AS INT64) AS protocol,
12   CAST(JSON_VALUE(json_payload.bytes_sent) AS INT64) AS bytes_sent,
13   timestamp,
14   PARSE_TIMESTAMP("%Y-%m-%dT%H:%M:%E+SZ", JSON_VALUE(json_payload.start_time)) AS start_time,
15   PARSE_TIMESTAMP("%Y-%m-%dT%H:%M:%E+SZ", JSON_VALUE(json_payload.end_time)) AS end_time,
16 FROM
17   | 'tocchy-demo01.global._Default'
18 WHERE
19   | log_id IN ('compute.googleapis.com/vpc_flows',
20   | 'networkmanagement.googleapis.com/vpc_flows')
21 --
22 -- Gemini により生成されたクエリの開始
23 --
24 SELECT
25   src_instance_name,
26   dest_instance_name,
27   protocol,
28   src_ip,
29   dest_ip,
30   bytes_sent
31 FROM
32   'flowLogs'
33 WHERE
34   src_instance_name = 'development-workstation'
35   AND dest_instance_name = 'ntochi-jump01'

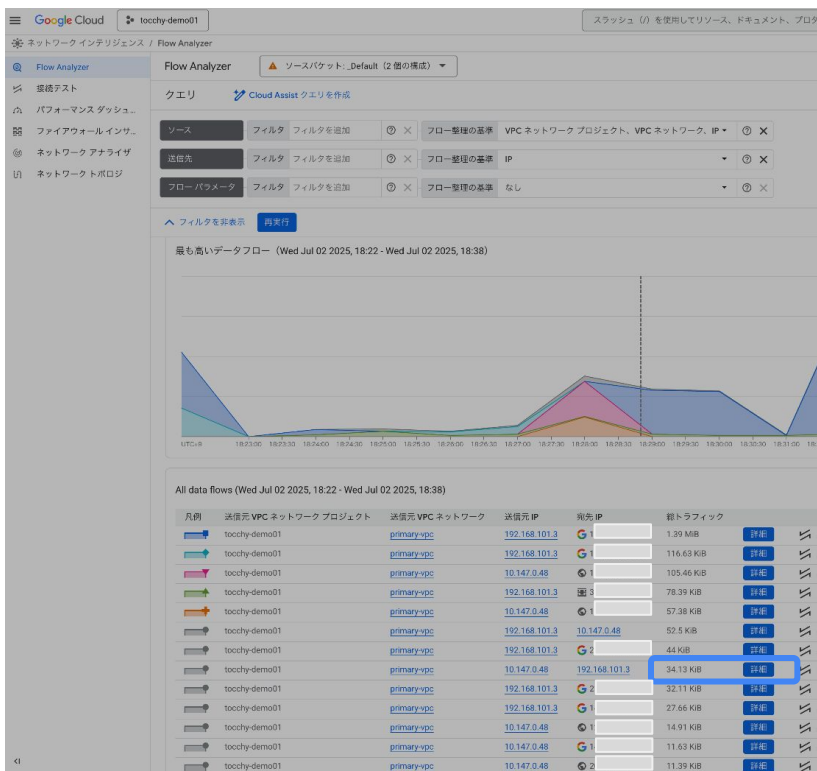
```

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



フローの詳細 (Wed Jul 02 2025, 18:24 - Wed Jul 02 2025, 18:40)

development-workstation (GCE インスタンス) → ntochi-jump01 (GCE インスタンス)

接続テストを実行

送信元

GCE インスタンス development-workstation
 IP 192.168.101.3
 VPC ネットワーク primary-vpc
 GCP ソーン asia-northeast1-a
 VPC ネットワーク プロジェクト tochy-demo01
 GCE インスタンス プロジェクト tochy-demo01
 VPC サブネットワーク hybrid-subnet01
 GCP リージョン asia-northeast1

送信先

GCE インスタンス ntochi-jump01
 IP 10.147.0.48
 GCP ソーン asia-northeast1-b
 GCE インスタンス プロジェクト tochy-demo01
 VPC ネットワーク primary-vpc
 VPC サブネットワーク primary01-subnet
 GCP リージョン asia-northeast1
 VPC ネットワーク プロジェクト tochy-demo01

フローパラメータ

プロトコル ICMP

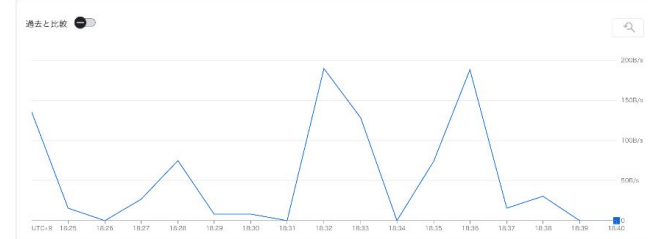
トラフィック

総トラフィック

52.5 KiB

ドリルダウン 下り (外向き) AS パス

development-workstation (GCE インスタンス) → ntochi-jump01 (GCE インスタンス) (時間経過)



閉じる

Flow Analyzer から接続テストの実行も可能

フローの詳細 (Wed Jul 02 2025, 18:25 - Wed Jul 02 2025, 18:41)

development-workstation (GCE インスタンス) → ntochi-jump

[接続テストを実行](#)

送信元

GCE インスタンス	development-workstation
IP	192.168.101.3
VPC ネットワーク	primary-vpc
GCP ゾーン	asia-northeast1-a
VPC ネットワーク プロジェクト	tochyi-demo01
GCE インスタンス プロジェクト	tochyi-demo01
VPC サブネットワーク	hybrid-subnet01
GCP リージョン	asia-northeast1

送信先

GCE イン	
IP	
GCP ゾ	
GCE イン	
ト	
VPC ネット	
VPC サブ	
GCP リ	
VPC ネット	
ト	

フロー パラメータ

プロトコル: ICMP

トラフィック

総トラフィック: 52.5 KIB

[ドリルダウン](#) 下り (外向き) AS パス

development-workstation (GCE インスタンス) → ntochi-jump01 (GCE インスタンス)

過去と比較

接続テストの結果

前回のテストの時間
2025-07-02 (18:40:56)

全体的な構成分析の結果
→ 到達可能

構成分析トレースの選択
→ trace0

選択したトレースの分析結果
✔ パケットは配信可能です

構成分析トレースのパス

- VM インスタンス (development-workstation)
 - ネットワーク インターフェース: nic0
 - ネットワーク: primary-vpc
 - 内部 IP: 192.168.101.3
 - 外部 IP: -
 - [ネットワーク インターフェースの詳細を表示](#)
- 下り (外向き) 階層型ファイアウォール ポリシールール
 - アクション: 許可
 - 優先度: 1500
- サブネット ルート
 - 名称: default-route-86dd4d18af49e41b
 - ネットワーク: primary-vpc
 - 送信先 IP 範囲: 10.147.0.0/24
 - ネクストホップ: VPC ネットワーク ゲートウェイ
- VM インスタンス (ntochi-jump01)
 - ネットワーク インターフェース: nic0
 - ネットワーク: primary-vpc
 - 内部 IP: 10.147.0.48
 - 外部 IP: -
 - [ネットワーク インターフェースの詳細を表示](#)

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
- **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。

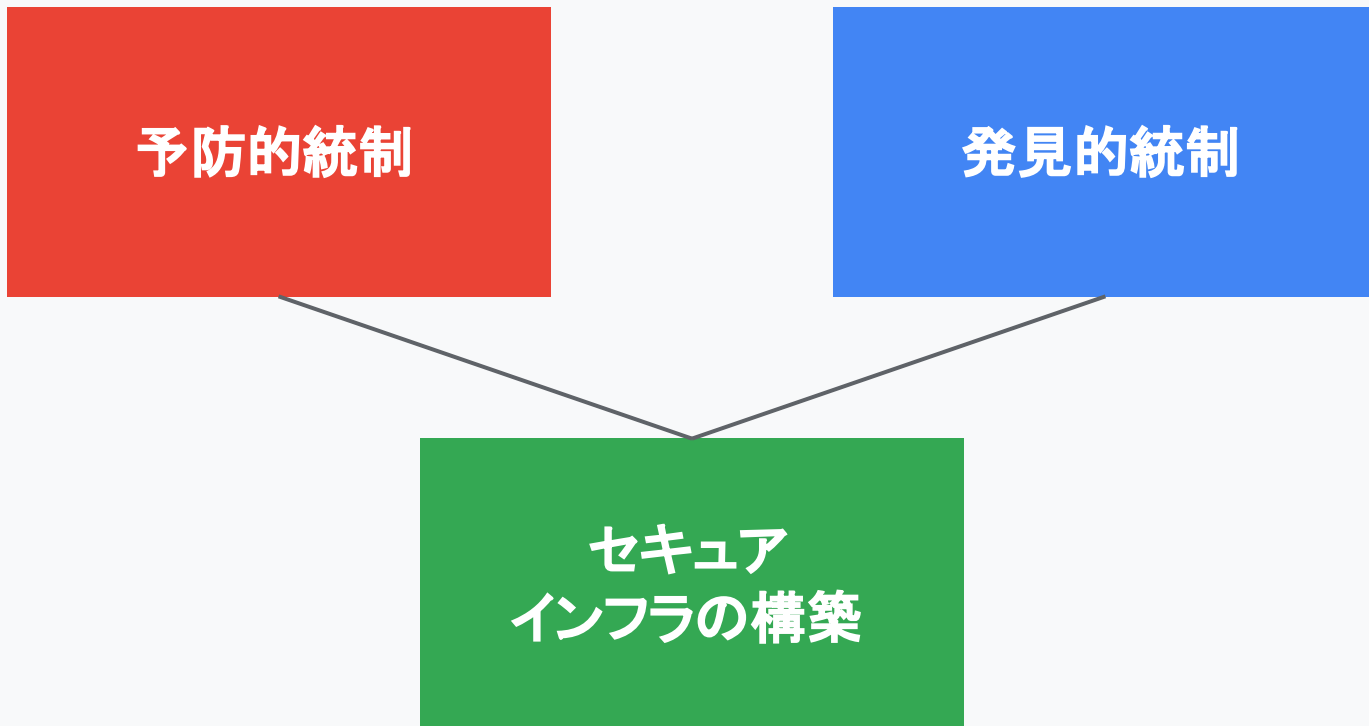


人手と時間には
限りがある

- **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 を通じ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
行っただ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

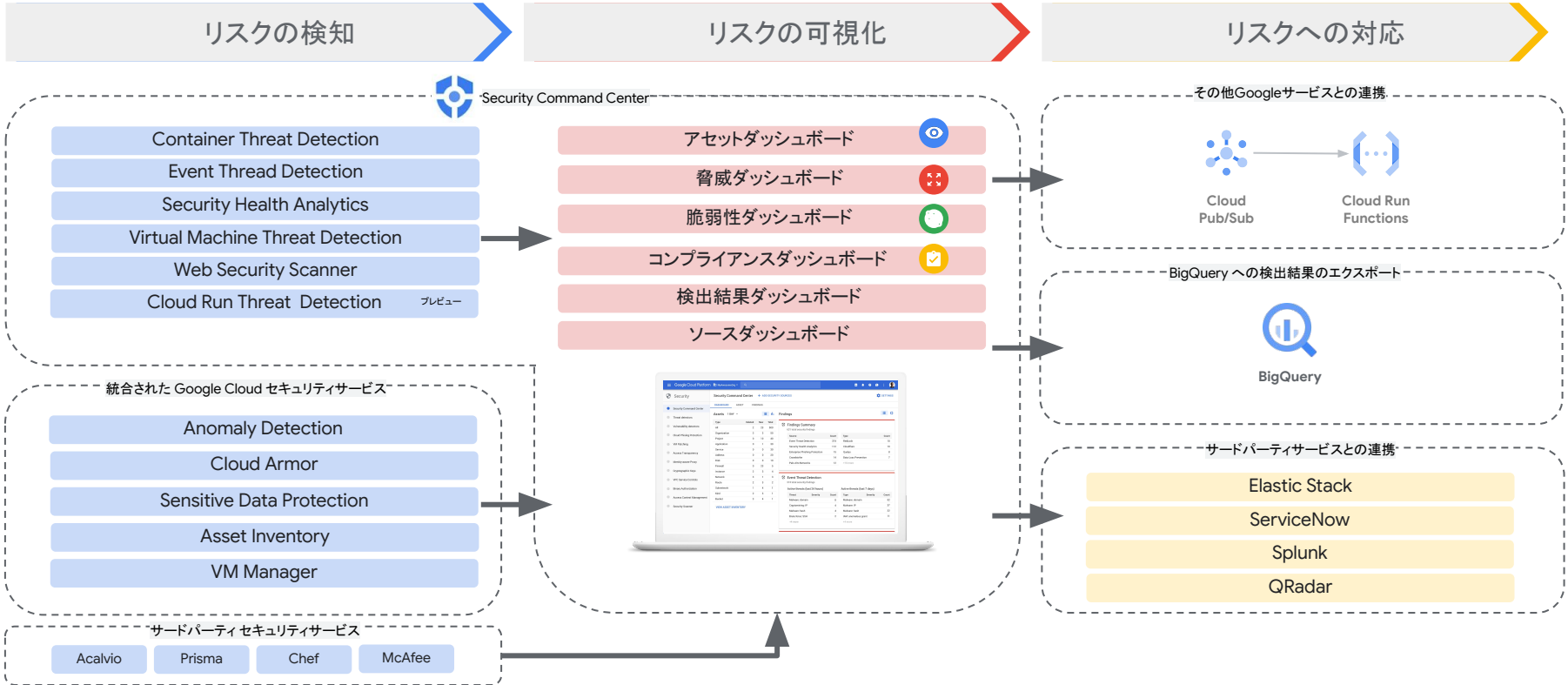
Security Command Center
Cloud Operations

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



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

✦ Create posture tailored to your environment

- 利用しているサービス
- 利用しているリージョン
- 適用されるコンプライアンス体制



シングルクリックでポリシーを作成

Posture

Based on details about your environment, these policies offer solid monitoring across your region, industry, and Cloud services

☰ GCE_policy_set

Policy set containing list of policies for GCE service 19 policies

☰ GKE_policy_set

Policy set containing list of policies for GKE service 11 policies

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

エージェントレス脆弱性管理

Vulnerability Assessment for Google Cloud



Compute
instance VMs



Google Compute
Engine

OS、ソフトウェア
の脆弱性をス
キャン



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

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

Inhibit system recovery: deleted Google Cloud Backup and DR plan association TAKE ACTION 1 of 11 < > X

SUMMARY SOURCE PROPERTIES (9) JSON

What was detected

Description A backup plan has been removed from a workload. Backups are no longer scheduled on the workload. The resource(s) affected are in us-east5.

State	Active	state
Severity	High	severity
Event time	March 25, 2025 at 5:10:20 PM GMT-4	event_time
Create time	March 25, 2025 at 5:10:21 PM GMT-4	create_time
Principal email	salimhafid@google.com	access.principal_email
Caller IP	11	access.caller_ip
Service name	backupdr.googleapis.com	access.service_name
Method name	google.cloud.backup.v1.BackupDR.DeleteBackupPlanAssociation	access.method_name

Affected resource

Resource display name	gcve-productb-demo	resource.display_name
Resource full name	//cloudresourcemanager.googleapis.com/projects/247230298140	resource.name
Resource type	google.cloud.resourcemanager.Project	resource.type
Project full name	//cloudresourcemanager.googleapis.com/projects/247230298140	resource.gcp_metadata.project
Resource path	//gcve-productb-demo	resource.cloudProvider
Cloud provider	Google Cloud	resource.cloudProvider
Security contacts	None	contacts.security
Technical contacts	None	contacts.technical

Security marks

No marks

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

Reverse shell

PREVIEW

SUMMARY
SOURCE PROPERTIES (15)
JSON

What was detected

Description	A process started with stream redirection to a remote connecto workload to an attacker-controlled machine. The attacker can th part of a botnet.
State	● Active
Severity	🔴 Critical
Event time	March 19, 2025 at 2:26:38 PM GMT-7
Create time	March 19, 2025 at 2:26:38 PM GMT-7
Source IP	169.254.8.1
Source port	19623
Destination IP	8.8.8.8
Destination port	53
Protocol	PROTOCOL_UNSPECIFIED
Program binary	"/tmp/ktd-test-reverse-shell-2025-03-19-21-26-22-utc"
Arguments	View 1 argument
Environment variables	View 13 environment variables
Containers URI	us-docker.pkg.dev/crst-integration-test-staging/ktd-demo-public/ktd-test@sha256:d55c5fb5e2bfe9cc329ada2b389c3f129f2e24844306328c5951e62dd85a4763
Containers create time	March 19, 2025 at 2:23:50 PM UTC-7
Kubernetes pods	View 1 kubernetes pod

Affected resource

Resource full name	"/run.googleapis.com/projects/crst-integration-test-staging/locations/us-east1/revisions/crtd-test-00001-7fx"
Cloud provider	Google Cloud
Security contacts	None
Technical contacts	None

Security marks

No marks

Related links

VirusTotal indicator	VirusTotal Process Binary Link
----------------------	--

Detection service

Finding canonical name	organizations/1086434666586/sources/9441531205078228985/locations/global/findings/9b4d1d0f570a63c4
Finding class	Threat
Source display name	Cloud Run Threat Detection

Cloud Run Threat Detection

Available for Premium or Enterprise

Use kernel-level instrumentation to identify potential compromise of Cloud Run resources, including suspicious binaries. If enabled, all workloads will use the second generation execution environment when redeployed. Test your workloads on second generation before enabling. [Learn more](#)

✔ Enabled
[MANAGE SETTINGS](#)

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



Network



GKE instances



BigQuery



Compute Engine instances



Storage and DB resources



Cloud Run



Backup and DR



Identities

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