Engineer

# Google Cloud

Googleが提供するクラウド基盤

## どのようなものか

Google Cloudは、自社データセンターの計算資源を貸し出すGoogleの事業です。Compute Engineの仮想マシン、Cloud Storageのオブジェクトストレージ、Cloud SQLのマネージドデータベース、GKEのKubernetesクラスター、BigQueryのデータウェアハウスなど、多くのサービスを従量制で提供します。旧称のGoogle Cloud Platform、略してGCPも、Google自身の文書の一部を含め、今も広く使われています。

Google Cloudが顧客のために動かすものは、すべてプロジェクトの中にあります。プロジェクトは、リソース、そのために有効にしたAPI、リソースが消費する割り当て、支払いをする請求先アカウントとの関連付けをまとめる入れ物です。変更できる表示名と、Google Cloud全体で一意で、プロジェクトの作成後は変わらないプロジェクトIDを持ちます。プロジェクトはフォルダーへまとめられ、フォルダーに別のフォルダーも入り、階層構造全体は企業のGoogle WorkspaceまたはCloud Identityアカウントに属する組織リソースにつながります。組織やフォルダーで設定したロールと組織ポリシーは、配下のすべてのプロジェクトへ継承されます。適切に構成した階層なら管理しやすく、構成が不適切だと、後で整理し直すのが難しくなります。

ネットワークの範囲は、ほかの大手クラウドと異なります。Google CloudのVPCネットワークは、経路やファイアウォール規則も含め、どのリージョンにも属さないグローバルなリソースで、リージョンごとなのはサブネットだけです。そのため、ベルギーとアイオワの仮想マシンが一つのプライベートネットワークを共有し、リージョン間のVPNやピアリングなしに、内部アドレスで通信できます。対してAWSでは、各VPCは一つのリージョンにあります。

認証に使う主体は二種類あります。人はGoogleアカウントでログインし、プロジェクト、フォルダー、組織全体のいずれかでIAMロールを受けます。プログラムはサービスアカウントを使います。一つのプロジェクトに属する主体で、仮想

マシン、コンテナー、ビルドジョブが、その主体として動けます。Compute Engineインスタンスへサービスアカウントを付ければ、そこで動くコードは、ディスクへパスワードや鍵ファイルを置かずに、そのアカウントのロールでGoogle APIを呼べます。

概念を判断に生かす

「Google Cloudとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 実際の使用量に合わせてサーバーを構成し、月額費用を事前に把握したうえで、クラウドへの移行もクラウドからの移転も進めます。

**サービスを見る** お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Google Cloud・AWSでDockerアプリ20個を運用 — 20 デプロイし監視したコンテナアプリケーション

**Google Cloud・AWSでDockerアプリ20個を運用** お問い合わせ →

## なぜ重要なのか

多くのチームがGoogle Cloudを選ぶ理由は、データです。BigQueryは、サーバーの規模を決める必要のないウェアハウスです。テーブルはプロジェクト内のデータセットに置き、クエリは標準SQLで書きます。オンデマンド方式では各クエリの読み取りバイト数で、容量ベースの方式では、スロットで測る予約済みの処理能力に対して課金します。列単位で保存するため、課金対象は行全体ではなく、クエリが触れた列の分です。隣のCloud Storageが取り込み前の置き場になり、バケットからファイルを読み込むのが標準的な入口です。ほかならウェアハウスのクラスターを用意し、調整するチームも、バケット、データセット、クエリから始められます。

二つ目の理由は、多くのものが結び付く、プロジェクトという境界です。請求、割り当て、有効なAPI、IAMが集まるため、アプリケーションと環境の組み合わせごとに一つ作ると、本番とテストの権限も請求明細も明確に分かれます。プロジェクトを停止すれば、請求も中の全リソースも一度に止まります。所有者は30日間、復元できますが、Cloud Storageなど、一部のサービスはデータをもっと早く消す場合があります。上位では、フォルダーに組織ポリシーを一度設定すると、既定ネットワークや、ダウンロード可能なサービスアカウントの鍵など、危険な設定の種類全体を、配下の全プロジェクトで禁止できます。小さいチームが十二個のプロジェクトを、一つずつ手で調べずにそろえる方法です。

## 実際の活用例

三つの事例が、ウェアハウスへの取り込み先、バックアップの外部保存先、プライベートネットワークの一端としてのGoogle Cloudを示します。

データの仕事では、IPsec VPNの先のウェアハウスから、六つのETL/ELTパイプラインでBigQueryへ投入しました。整理したデータセットとテーブルをエクスポートし、gzipで圧縮してGoogle Cloud Storageのバケットへ転送しました。BigQueryへのアップロードとスキーマの対応付けは、bq CLIとPythonの取り込みスクリプトで自動化しました。Cloud Storageを経由する転送とBigQueryへの読み込みが自動で動くようになると、手作業で3時間以上だった全工程は20分未満になり、BigQueryの更新は週次から日次へ変わり、読み出すPython APIの性能は30%向上しました。

バックアップでは、重要データのバックアップ100件を自動化しました。PostgreSQL側をBarmanが担い、外部のコピーをGoogle Cloudへ置きました。BashとPythonで手順全体を制御、検証し、保持ポリシーでコピーを最新に保ち、整合性検査で、単に存在するだけでなく正常であることを確かめました。その後、バックアップは自動実行され、すべてのデータベースで検証できるようになりました。

ネットワークでは、Google CloudとオンプレミスのLinuxシステムを結ぶ、WireGuardとIPsecのトンネル八本を、一組として管理し、障害を調べました。設定を標準化し、健全性を監視し、繰り返す経路や鍵交換の問題を、再起動でしのがず根本から直しました。その後は八本とも、安全かつ安定して動くようになりました。

## 問題が起きるところ

Google Cloudで特に気を付けたいのは、便利さの裏側です。使い始めた日の午後の作業を楽にした設定が、一年後、選んだことを誰も覚えていなくなっても、そのまま残ります。

**既定ネットワークが開いたままです。** 組織ポリシーで防がない限り、新しいプロジェクトには、全リージョンにサブネットを持ち、四つのファイアウォール規則があらかじめ入った既定ネットワークが付きます。三つは、インターネット全体を表す0.0.0.0/0から、tcp:22のSSH、tcp:3389のリモートデスクトップ、ICMPを受け入れます。四つ目は、ネットワーク内の10.128.0.0/9から、すべてのTCP、UDP、ICMPを許します。そのネットワークで外部アドレスを与えた仮想マシンは、インターネット上のどこからでもSSH接続を試みられる状態になります。`compute.skipDefaultNetworkCreation` 制約で新規プロジェクトへの作成を防ぎ、通信元を明記した規則を持つカスタムネットワークに置き換えます。

**サービスアカウントの鍵がリポジトリーに入ります。** 利用者が管理する鍵は、それを持つ人がサービスアカウントとして動けるJSONファイルです。既定では、鍵が削除されるまで有効です。CIの機密情報、コンテナーイメージ、そして誤ってリポジトリーへと、容易に広がります。Googleは、より安全な代替手段があれば、そちらを選ぶよう勧めます。Google Cloud上のワークロードは、実行先リソースに付けたサービスアカウントを使います。CIシステムや別のクラウドなど、外部のものはWorkload Identity Federationを使い、外部システム自体の認証情報を、有効期間の短いGoogleトークンと交換します。2024年5月3日以降に作った組織では、組織ポリシーの制約によって、鍵の作成とアップロードが既定で無効です。以前からある組織も、同じ制約を設定できます。

**小さいクエリが大きいテーブルを読みます。** オンデマンド方式のBigQueryは、クエリが読むバイト数で課金します。クラスタリングしていないテーブルでは、`LIMIT` 句は、その量を変えません。`SELECT * ... LIMIT 10` は十行を返しても、全列の全バイトに課金します。必要な列だけを選び、大きいテーブルは日付で分割して、その日付を絞るクエリが古いパーティションを飛ばせるようにします。新しいクエリは実行前にドライランの見積もりを確認し、課金対象の最大バイト数を設定します。見積もりが上限を超えるクエリは、実行前に失敗し、料金はかかりません。

**低頻度アクセス用のストレージに、頻繁に使うデータを置きます。** Cloud StorageのNearline、Coldline、Archiveは、Standardより保存一ギガバイト当たりの料金が低い代わりに、取り出し料金と、30日、90日、365日の最低保存期間があります。最低保存期間より前に削除、置換、移動したオブジェクトには、全期間置いたものとして課金します。そのため、日々入れ替えるバックアップや、パイプラインが書いて一時間以内に消す一時ファイルは、StandardよりArchiveの方が高くなる場合があります。低頻度用のクラスは、一度書いてめったに読まないデータ向きです。ライフサイクル規則で、古くなるにつれて移せます。

## 参考資料

- Google Cloudのドキュメント — 全製品のガイド、参照文書、チュートリアルをまとめたGoogleの索引です。
- リソース階層について — 組織、フォルダー、プロジェクトの入れ子と、ロールやポリシーの継承方法です。
- VPCファイアウォール規則 — 既定ネットワークに最初からある規則も含め、ファイアウォール規則を評価する方法です。
- サービスアカウントの鍵の管理に関するベストプラクティス — 鍵が流出する経路、制限する方法、代わりに使うものです。
- 費用の見積もりと管理 — ドライラン、課金対象の最大バイト数、`LIMIT` による節約が小さい理由についてのBigQueryの説明です。

- ストレージクラス — 最低保存期間、取り出し料金、可用性を含む、各クラスの比較です。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

## 用語を実務に結び付ける

「Google Cloudとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/google-cloud/