

01

Google Cloudとは ～Googleが提供するクラウドサービス

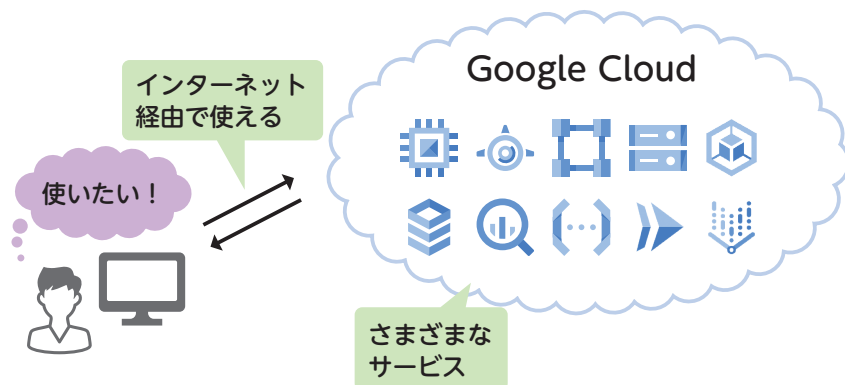
近年、クラウドサービスの利用が活発化しています。何らかのシステムを構築する際には避けては通れないほど、スタンダードな技術になっています。まずは、クラウドサービスとしてのGoogle Cloudの特徴を見ていきましょう。

Google Cloudとは

Googleは、Google検索やGmail、Googleマップ、YouTubeといった、大量のトラフィックを取り扱うグローバルなサービスを、20年以上にわたり運営しています。これらのサービスを提供するために、Googleは長年にわたり、効率的で、最適化されたインフラストラクチャ（インフラ）を構築してきました。**Google Cloud**は、その最適化されたインフラストラクチャを、ほかの企業やエンジニアが利用できるようにしたクラウドサービスです。

クラウドサービス（以下、クラウド）とは、システムを構築する際に必要となるサーバーや各種の機能を、インターネット経由で利用できるサービスのことです。基本的にWebのインターフェースから利用できるのもので、特別な環境設定は不要で、すぐに使い始めることができます。

Google Cloud



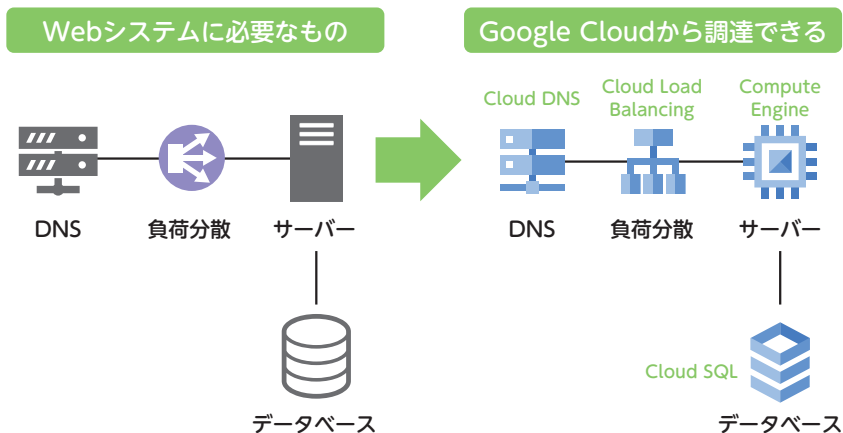
Google Cloudには、コンピューティングやストレージ、データベース、データ分析、機械学習など、実にさまざまなサービスが用意されています。これらに加えて、インフラ資源を自社で管理するオンプレミスや、ほかのクラウドを組み合わせる際にも一貫した方法を提供する、ハイブリッドクラウドやマルチクラウドの選択肢も提供しています。

システム構築に必要なものは揃っている

Google Cloudは、クラウドベンダーが運用管理する範囲が大きいサービスである、フルマネージドなサービスが多いことが特徴です。また、サーバーの存在を意識する必要がないサーバーレスなサービスが多いことも、特徴に挙げられます。このため、従来のオンプレミスのシステムで必要だった運用コストを抑えて、開発や企画などに、より多くの人的資源を割くことが可能になります。

たとえばWebシステムを構築する場合、システムに必要なサーバーやデータベースなどは、Google Cloudから調達できます。また、システムの負荷に応じてサーバーをスケール（規模や台数を拡張）できるインフラストラクチャになっています。

システム構築に必要なものは揃っている



11

ハイブリッドクラウドと
マルチクラウド

～オンプレミスやほかクラウドを利用した構成

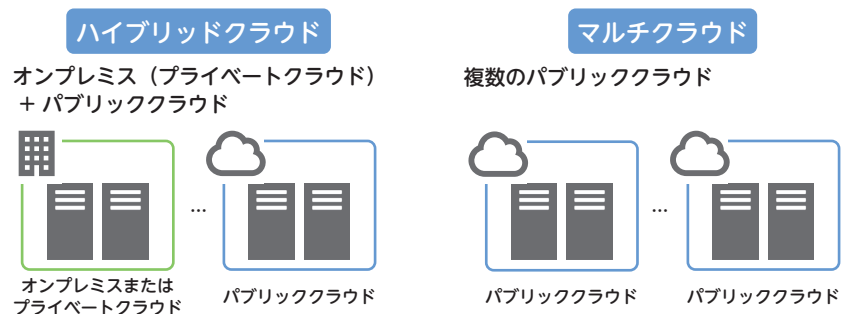
近ごろのクラウド利用では、1つのパブリッククラウドだけを使うのではなく、オンプレミスや複数のクラウドを組み合わせた構成にすることがスタンダードになってきました。これらの構成について学んでおきましょう。

○ ハイブリッド／マルチクラウドとは

パブリッククラウドがあらゆる業界／規模の組織で利用されるようになってきたとはいえ、既存のシステムをすべてパブリッククラウドに置き換えるのをためらう人もいるでしょう。それに対する手段の1つとして、**ハイブリッドクラウド**があります。ハイブリッドクラウドとは、**既存のオンプレミスとパブリッククラウドを組み合わせた構成**のことです。ハイブリッドクラウドにすると、データ分析や機械学習といった一部のワークロードではパブリッククラウドを活用し、ほかはオンプレミスにするといったことができます。

一方、パブリッククラウドだけを使いたい企業でも、それぞれのパブリッククラウドの特性を活かした形で複数のパブリッククラウドを活用するケースもあります。そうした構成を**マルチクラウド**といいます。ハイブリッドクラウドやマルチクラウドにすると、特定ベンダーに依存することにより発生するリスクを下げて、より柔軟なシステム構成が選択できます。

■ ハイブリッドクラウドとマルチクラウドの違い

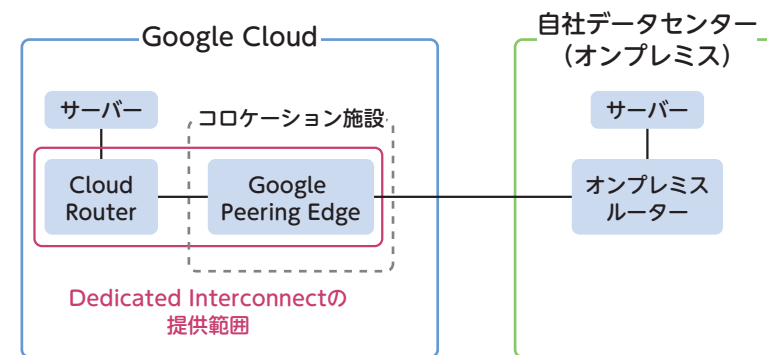


○ ハイブリッドクラウドを実現するサービス

ハイブリッドクラウドの構成において、オンプレミスとパブリッククラウドの間で安全に安定した通信ができるよう、パブリックなインターネットを介さずにオンプレミスとクラウドを接続するネットワークサービスが提供されるようになりました。Google Cloudでは**Cloud Interconnect**というサービスが提供されています。このサービスを活用すると、オンプレミスとGoogle Cloudをダイレクトに接続できます。Cloud Interconnectには、**Dedicated Interconnect**と**Partner Interconnect**という2つの提供形態があります。Dedicated InterconnectとPartner Interconnectの違いは第5章でも解説しますが、この2つの形態には、自社のデータセンターをGoogleのデータセンターと直接閉域で接続するか、あるいは、パートナーのネットワークを経由して接続するか、という違いがあります。

一方、マルチクラウドについてはどうでしょうか。Google Cloudは、マルチクラウドを実現するためのネットワーキングサービスを直接提供していませんが、パブリッククラウド間を接続できるようなサービスを提供しているサービスプロバイダもあります。また、IPsec-VPN (IPsecというネットワークの暗号化技術を使ったVPN) によるサイト間接続ができるCloud VPNというサービスも提供されています。Cloud VPNを使うとIPsecの設定をするだけで、暗号化された通信路でオンプレミスやほかのクラウドと安全に接続できます。

■ Dedicated Interconnect



Googleのデータセンターと利用者のデータセンターを閉域接続する構成

15

リソース階層 ～複数のリソースを管理するしくみ

Google Cloudを実際に使う際は、1つのプロジェクトではなく、複数のプロジェクトが必要になることがほとんどです。Google Cloudには、複数のプロジェクトやサービスを管理するリソース階層というしくみがあります。

○ リソース階層とは

リソース階層とは、プロジェクトやサービスを管理するための階層構造のことです。企業など、組織でGoogle Cloudを利用する際は、リソース階層を定義します。リソース階層を利用すると、パソコンに保存したファイルをフォルダに分けて整理するかのよう、さまざまなチームが利用するプロジェクトを、フォルダで階層的に管理できます。フォルダ単位で管理ポリシーを設定することにより、企業のそれぞれの部署やチームの利用状況にあわせて、プロジェクトやリソースに対するアクセス制限や権限設定を適切に実施できます。

リソース階層の最上位ノードは**組織**リソースで、組織(企業など)を表します。「組織」リソースは、階層の下にあるすべてのリソースを一元管理します。**ノード**とは、木構造のリソース階層において、枝分かれしている部分のことです。そして「組織」やフォルダ、プロジェクト、プロジェクトの中で実際に使われるサービス(Compute EngineやGoogle Kubernetes Engineなど)といった、Google Cloudを構成する要素のことを**リソース**と呼びます。

○ リソース階層を構成する3つの要素

リソース階層を構成する要素は、3つあります。

組織

「組織」はルートノード、つまりリソース階層の頂点にあたる「リソース」です。組織は、ドメイン(たとえば、example.com)と1対1で紐付きます。ここでい

う「組織」はあくまで設定上の概念なので、現実の1つの組織(企業)が複数のドメインを用意して、本部ごとといった単位で「組織」リソースを作成することもできます。たとえば、ドメインが「ec-example.com」の組織は流通本部向け、ドメインが「fsi-example.com」の組織は金融本部向けといった構成も可能です。この場合は「組織」ごとに独立したリソース階層が用意されるので、流通本部と金融本部は、個別にリソース管理を行うことになります。

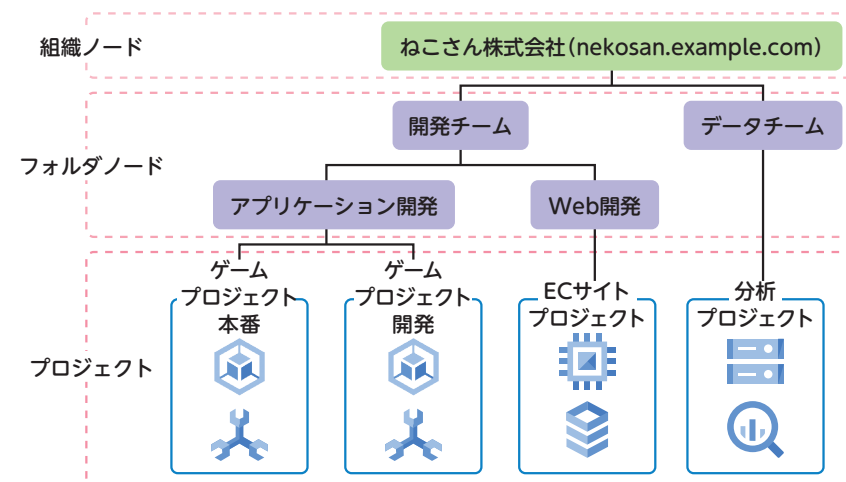
フォルダ

フォルダを使用すると、組織配下の部署やチームのさまざまな要件を分離できます。また、本番環境と開発環境のリソースを分けることもできます。フォルダは部署といった組織別に分けるケースもあれば、あるプロジェクトの本番環境フォルダ、開発環境フォルダといった環境別に分けるケースもあります。なお、フォルダの中にフォルダを作成するといった構成も可能です。

プロジェクト

階層の一番下にあるのが、プロジェクトです。プロジェクトごとに、アプリケーションを構成するコンピューティングやストレージ、ネットワークといった、実際にシステムで使うサービスを用意します。

■ リソース階層



20

Compute Engineを
使う流れ

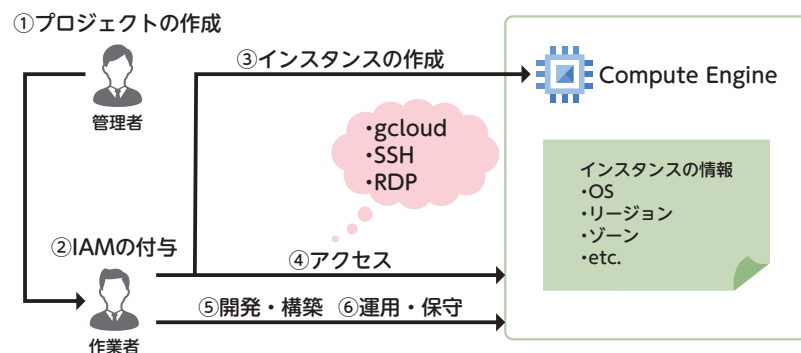
～仮想マシンを使うまで

Compute Engineを使う際は、インスタンスを作成する必要があります。インスタンスの作成時にはさまざまな情報を入力する必要がありますので、どのような情報が必要になるのか、全体像を押さえておきましょう。

○ Compute Engineを使う流れ

Compute Engineを使うには、まずはGoogle Cloudでプロジェクトを作成する必要があります。そして、管理者よりCompute Engineのリソースを操作する権限を付与してもらうことで、インスタンスを作成できるようになります。インスタンスを作成したあとは、Cloud ShellやSSH接続を用いてインスタンスにアクセスして、ソフトウェアのインストールといった構築作業を行います。

■ Compute Engineを使う流れ



○ インスタンスの設定項目

Compute Engineの仮想マシン（インスタンス）は、必要な項目を入力して、作成ボタンをクリックするだけで作成できます。インスタンスの作成は、Google Cloud コンソールから行えます。

■ インスタンス作成画面

← インスタンスの作成

VM インスタンスを作成するには、次のいずれかのオプションを選択します。

- 新規 VM インスタンス**
最初から単一の VM インスタンスを作成します
- テンプレートから VM インスタンスを新規作成**
既存のテンプレートから単一の VM インスタンスを作成します
- マシンイメージからの新しい VM インスタンス**
既存のマシンイメージから単一の VM インスタンスを作成します
- Marketplace**
VM インスタンスにすぐに使えるソリューションをデプロイします

名前 ^②
名前を変更できません
instance-1

ラベル ^③ (省略可)
+ ラベルを追加

リージョン ^④
リージョンは変更できません
us-central1 (アイオワ)

ゾーン ^⑤
ゾーンは変更できません
us-central1-a

マシンの構成

マシン ファミリー
汎用 コンピューティング最適化 メモリ最適化 GPU
費用と柔軟性を考慮して最適化された、一般的なワークロード向けのマシンタイプ

シリーズ
E2

可用性に基づく CPU プラットフォーム選択

マシンタイプ
e2-medium (2 vCPU, 4 GB メモリ)

vCPU
1 個の共有コア

メモリ
4 GB

GPU
-

インスタンス作成画面では、次の情報を入力します。なお、インスタンスの名前は、1つのプロジェクト内で一意の名前にする必要があります。リージョンが異なる場合でも一意にする必要があるため、注意が必要です。

■ インスタンスの設定項目

設定項目	説明
名前	インスタンスの名前 (Linux インスタンスであればホスト名)
リージョン	リソースを実行できる特定の地理的なロケーション
ゾーン	リージョン内の分離された場所
マシンタイプファミリー	マシンタイプをグループ化したもの。汎用、メモリ最適化、コンピューティング最適化、GPU から選択可能
シリーズ	CPU プラットフォームの世代
マシンタイプ	インスタンスのサイズ (vCPU 数、メモリ)
ブートディスク	利用 OS とディスクサイズ
サービスアカウント	インスタンス内で使う Google Cloud のサービスアカウント
アクセススコープ	API アクセス権のタイプとレベル

27

VPC

～仮想ネットワークサービス

VPCは数ある Google Cloudのサービスの中でも、非常に重要なサービスです。さまざまなサービスと関わりが深いので、機能や特徴についてしっかり押さえておきましょう。

○ VPCとは

Virtual Private Cloud (以下、VPC) は、Google Cloud内に論理的に構成された仮想ネットワークを提供するサービスです。VPCは、クラウド上のリソースやサービスに、グローバルなネットワーキングを提供します。また拡張性と柔軟性に優れており、セキュアなネットワークの設定がかんたんに行えます。

ここでは、VPCに用意されている機能を紹介します。クラウドに限らず、インフラの運用経験がある人には、お馴染みの機能もあるでしょう。

■ VPCの機能一覧

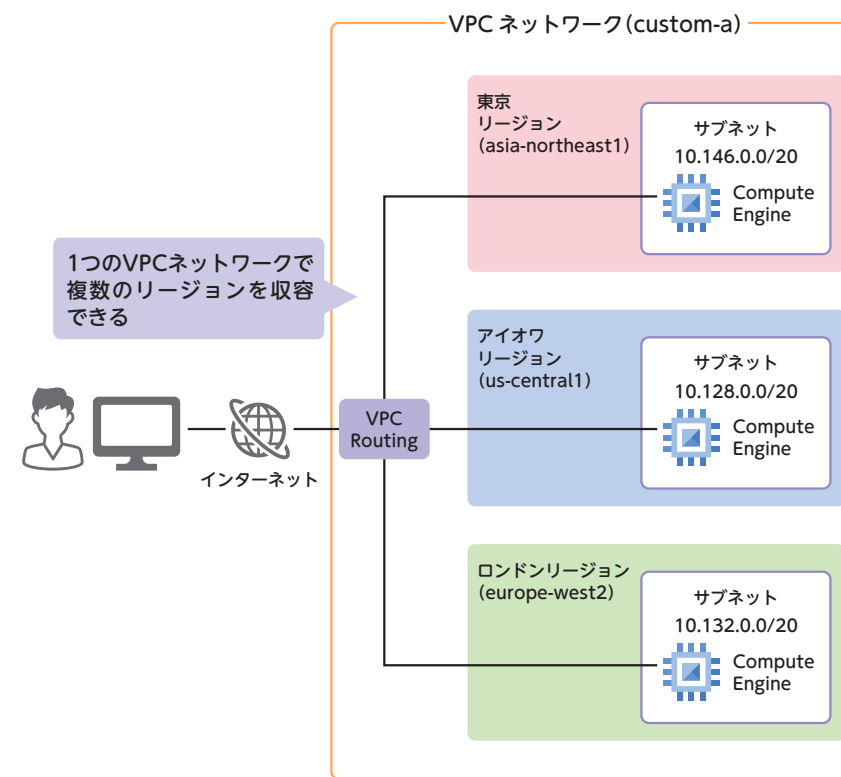
サービス名	概要
VPCネットワーク	Google Cloud内に構成される仮想ネットワーク
外部IPアドレス	主にインターネットへのアクセスに使うIPアドレス（外部IPアドレス）
ファイアウォール	接続の許可または拒否を行う
ルート	ルーティングの設定
VPCネットワークピアリング	VPCネットワーク同士の接続
共有VPC	異なるプロジェクトでVPCを共有
サーバーレスVPCアクセス	サーバーレスなGoogle CloudサービスからVPCへの接続
パケットのミラーリング	検査用にトラフィックのクローンを作成

○ VPCネットワーク

VPCネットワークとは、Google Cloud内に構成される、仮想ネットワークのことです。VPCの中心となる機能で、VPCネットワークのことを指してVPCと呼ぶ場合もあります。

VPCネットワークは、Andromedaと呼ばれるGoogle独自の技術を活用したネットワークです。VPCネットワークを使用すると、複数のサブネットをルーターで接続した、物理ネットワークと同等のグローバルネットワークが構成可能です。なお、1つのVPCネットワークには複数のリージョンを収容できます。

■ VPCネットワーク



37

Cloud Storage

～安全で信頼性が高いストレージサービス

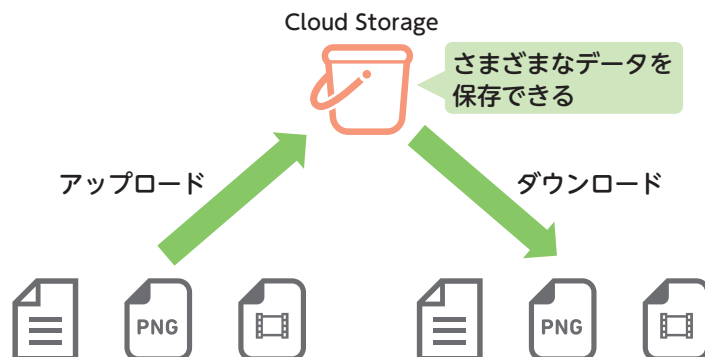
Cloud Storageは耐久性が高いストレージサービスです。実際にシステムを構築する際、Google Cloudのほかのサービスと組み合わせてよく使われるので、概要や特徴を押さえておきましょう。

○ Cloud Storageとは

Cloud Storageは、データ容量が無制限で、耐久性が高いストレージサービスです。Google Cloudの数あるサービスの中でも、10年以上の歴史があるサービスです。Cloud Storageは、もともとはGoogleが公開しているGoogle Codelabsというサービス内で、2010年5月にGoogle Storage for Developersという名称で一般公開されたものでした。その後、2011年10月に「Google Cloud Storage（現在はCloud Storage）」という名称で、正式なサービスとして提供が開始されました。

Cloud Storageは、各種データのバックアップやアーカイブ、Compute Engineの複数のインスタンスからアクセスするための共有ストレージとしてなど、幅広い用途で利用可能です。またデータ分析（P.240参照）でも、分析用の未加工のデータを蓄積する場所として、よく使われます。

■ Cloud Storage



○ Cloud Storageはオブジェクトストレージサービス

Cloud Storageは安全で信頼性の高い**オブジェクトストレージ**サービスです。オブジェクトストレージとは、データを「オブジェクト」と呼ばれる単位で管理するストレージのことです。ここでいうオブジェクトは、一般的なファイルと考えて差し支えないでしょう。オブジェクトは「バケット」と呼ばれる入れ物に格納されます。

■ オブジェクトストレージサービス



○ Cloud Storageの特徴

Cloud Storageには、次のような特徴があります。

データ容量が無制限

データ容量が無制限です。アップロードするデータサイズの下限もありません（0byteのオブジェクトを作成することが可能）。また、バケットに格納するオブジェクト数にも制限がありません。ミニマムでスタートでき、容量を気にせずに保存できます。ただし、1つのオブジェクトのサイズは最大5TBになります。

非常に高い耐久性

99.999999999%（イレブンナイン）の耐久性（年間0.000000001%の確率でしかデータが損失しない）があります。また構成によって異なりますが、99.0%～99.95%の可用性がSLAとして提示されています。なお可用性とは、サービスが障害やエラーなどなく稼働できる度合いのことです。

48

GKE／K8sを使うメリット ～GKEとCompute Engineの比較

GKE／K8sにはほかにも、ローリングアップデートやロールバックといった、さまざまな機能があります。同じことをCompute Engineで行う場合と比較しながら、GKEを選ぶメリットを明確にしていきたいと思います。

ローリングアップデート

前節で紹介したデプロイメントがどのようにしてローリングアップデートを実現しているのか、Compute Engineでローリングアップデートを実現した場合と比較して考えてみましょう。Compute Engineでローリングアップデートを実現する場合は、新しいバージョンのアプリケーションをインストールしたインスタンスを新規作成して、ロードバランサの向き先を切り替えるという手順を自分で行う必要があります。しかし、GKEの場合は、デプロイメントの設定ファイルに書かれたポッドの情報を書き換えるだけで「Compute Engineの場合」に示した手順が、すべて自動で行われます。

ローリングアップデートの手順を比較

Compute Engineの場合

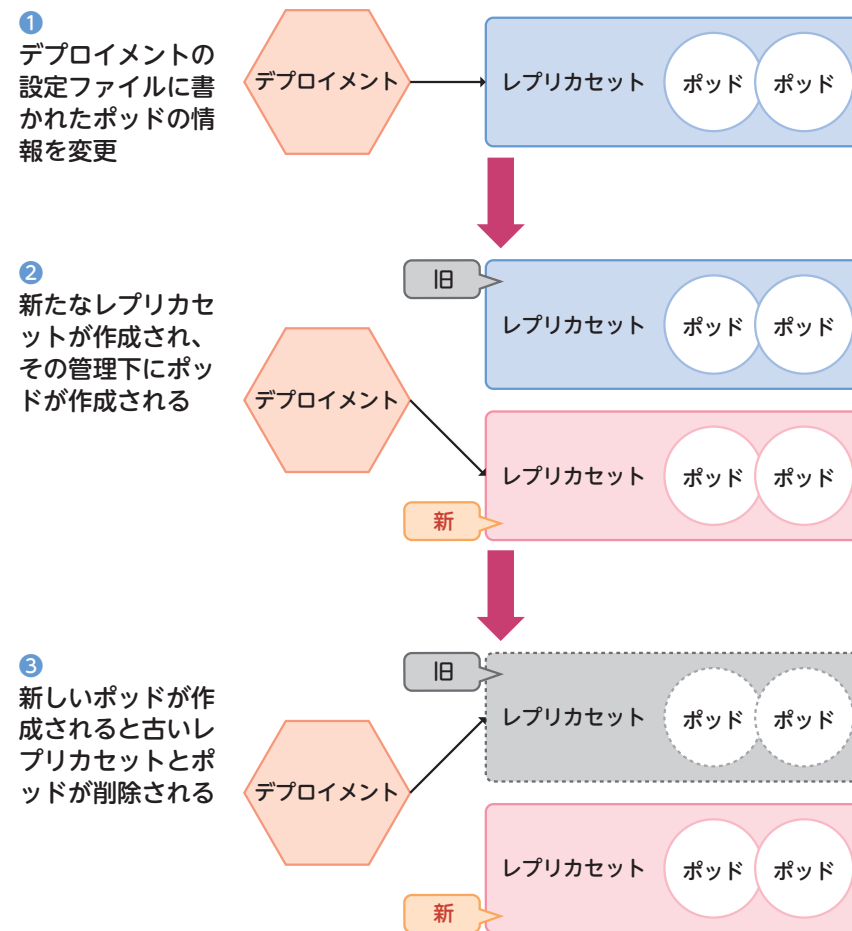
- ① 新規インスタンスの作成
- ↓
- ② 各種ミドルウェアのインストール
- ↓
- ③ アプリケーションのデプロイ
- ↓
- ④ ロードバランサの向き先の切り替え
- ↓
- ⑤ 古いインスタンスの削除

GKEの場合

- ① デプロイメントの設定ファイルに書かれたポッドの情報を変更

GKEでローリングアップデートを行う際、内部的には、デプロイメントがレプリカセットをうまく使って新旧のバージョンを入れ替えています。コンテナは「起動が速い」というメリットもあるため、ローリングアップデートにおける入れ替えや巻き戻しにかかる時間も、仮想マシンを用いた運用に比べて圧倒的に速くなります。もう少しイメージしやすいように、K8sの内部的なローリングアップデートのフローを図で紹介します（厳密にはもう少し細かい処理を行っています）。

K8sのローリングアップデート



55

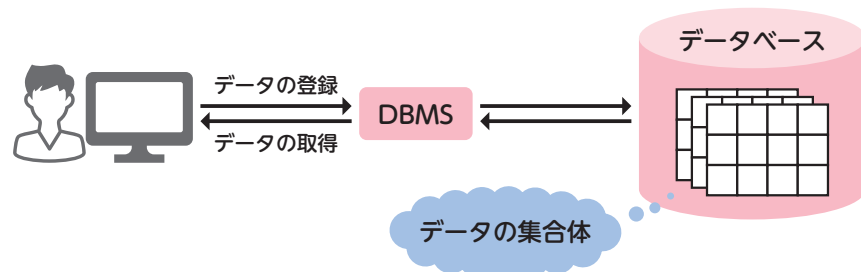
データベースとは
～整理されたデータの集合体

システムを構築する際、データベースは欠かせない存在です。Google Cloudではさまざまなデータベースサービスが提供されていますが、サービスを紹介する前に、まずはデータベースとは何かを解説しましょう。

○ データベースとは

データベースとは、検索や蓄積が容易にできるように整理された、データの集合体のことです。システムでは、さまざまなデータを扱います。通販サイトやSNSなどを考えてみると、ユーザー情報や購買履歴、ブログ記事、画像など、実にさまざまなデータを扱っていることが容易に想像できるでしょう。これらのデータを保存するのに使うのが、データベースです。システムやアプリケーションを構築するのに、必須のしくみといえるでしょう。また、これらのデータベースを管理するシステムのことを、**データベースマネジメントシステム (DBMS)** といいます。代表的なDBMSには、MySQLやPostgreSQL、Oracle Databaseなどがあります。DBMSがあることによって、データベースにデータを登録したり、データベースからデータを取得したりすることが、かんたんに行えます。

■ データベースとは



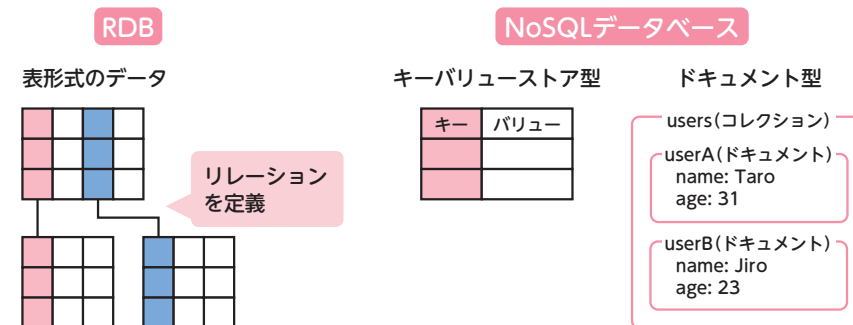
○ リレーショナルデータベースとNoSQLデータベース

データベースには、大きく分けて**リレーショナルデータベース (RDB)**と**NoSQLデータベース**があります。

RDBは、データを表形式として管理するデータベースです。表と表の関係(リレーション)を定義できるので、データの複雑な関連性を扱えます。また、データベースに対する操作には**SQL**と呼ばれる言語を使用します。

NoSQLデータベースは、RDBの対義語として使われている言葉です。NoSQLデータベースの中にはさまざまな方式があり、**特定のデータベースのしくみを指すものではありません**。いずれもデータへのアクセスにSQLを使用しないので、総称として「NoSQLデータベース」と呼ばれています。一般的に、NoSQLは単純なデータ構造で保存するため、高速にアクセスできます。データを保存するしくみとして代表的なものに、キーバリューストア型やドキュメント型があります。

■ RDBとNoSQLデータベース



まとめ

- ▶ データベースとは、検索や蓄積が容易にできるように整理されたデータの集合体のこと
- ▶ データベースには、RDBとNoSQLデータベースがある

62

BigQuery
～代表的なデータ分析サービス

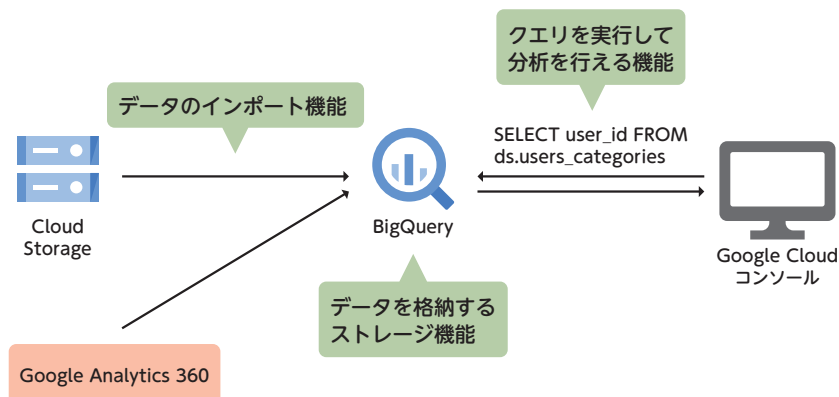
Google Cloudのデータ分析サービスの代表であるBigQueryについて、その特徴や基本的なしくみ、料金体系を紹介します。また、RDBとの技術的な違いについても説明しましょう。

○ BigQueryとは

BigQueryはフルマネージドのデータウェアハウスサービスです。データウェアハウスと名のつくサービスはさまざまな企業から多数提供されており、実装されている機能もサービスごとに異なります。

BigQueryは、マニュアル・バッチ・ストリーミングでのデータインポートやデータを格納するストレージとしての機能、そしてクエリを実行して分析を行う機能など、多くのパワフルな機能を備えています。クラウドサービスなので、それらを少ない準備で利用できます。またBigQueryは、Google AnalyticsやCloud Storageのデータを読み込めたり、前述のようにGoogle Cloudのサービスで一連のデータ分析基盤を構築できたりします。ほかのGoogle Cloudサービスと親和性が高く、用途に応じてさまざまな使い方が可能です。

■ BigQuery



○ BigQueryの特徴

BigQueryには、ここまで紹介したもの以外にも、さまざまな特徴があります。

高い処理能力

ペタバイト規模の大規模なデータに対しても高速にクエリを実行できるなど、非常に高い処理能力を誇ります。

スケーラビリティ

ストレージ容量が無制限かつ自動でスケールアウトするため、大規模なデータであっても特別な準備は必要ありません。サーバーノードやストレージの追加といったインフラ作業は不要です。

可用性

SLAで1カ月あたり99.99%の稼働時間が保証されています。

低コスト

非常に低いコストで大規模なデータを処理できます。

セキュリティ

インフラとして必要なセキュリティ対策が施され、アクセス制御を含む、ユーザーがデータ保護を実現するために必要な機能が提供されています。

ほかのGoogle Cloud サービスとの連携

ほかのGoogle Cloudサービスとの親和性が高く、ビジネスのニーズにあわせて柔軟にデータ分析基盤を構築できます。

67

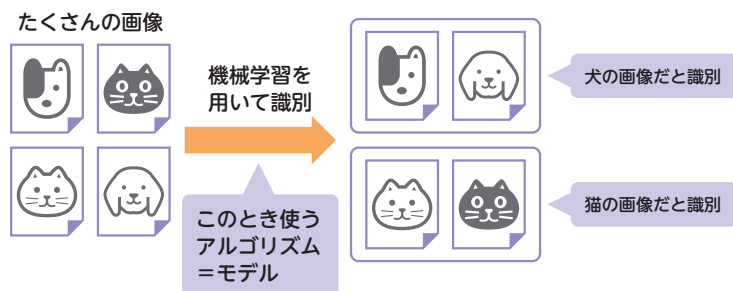
Google Cloudの AI・機械学習関連サービス ～かんたんに機械学習できる

Google Cloudでは、かんたんにAI・機械学習を扱える、AI building blocksというサービスが提供されています。さまざまな種類のものが用意されているので、特徴を理解しておきましょう。

○ 機械学習 (Machine Learning) とは

機械学習 (Machine Learning) とは、「経験を通して改善されるコンピュータアルゴリズムの研究」のことです。機械学習を使うと、大量のデータから天候を予測したり、画像をある特徴で分類したりできます。たとえば、たくさんの画像から犬と猫を識別したいとしましょう。この識別するときに用いるアルゴリズムの研究が機械学習であり、このアルゴリズムのことを**モデル**と呼びます。

■ 機械学習とは



○ Google Cloudの機械学習サービス

Google Cloudからは、アプリケーションやほかのGoogle Cloudのサービスからかんたんに機械学習を活用できる**AI building blocks**と、モデル開発を効率的に行える**Vertex AI**という2種類の機械学習サービスが主に提供されています。Vertex AIは、2021年5月にリリースされました。本書では、すぐに扱

うことができるAI building Blocksに焦点をあてて解説します。

AI building blocksは、Google Cloudで提供されているAI・機械学習系のサービスの総称です。Google Cloudコンソールのみで操作することも可能で、専門知識がなくてもAI・機械学習を使用した分析が可能です。

たとえば、ユーザーが画像や動画を自由にアップロードできるアプリケーションがあった場合に、著作権違反の画像や不適切な動画を検知したいとします。その要件を満たすには、バックエンドのアップロード処理に、AI building blocksのVision AIやVideo AIを使用します。これらを使うと、画像や動画に含まれるコンテンツをチェックできます。なお、サービスによっては、Googleの学習済みモデルを使用できます。

○ 機械学習の専門知識が不要

専門知識がなくても機械学習ができるのは、**専門知識が必要な工程をすべてサービスが行うため**です。一例として、一般的な機械学習の工程とAI building blocksのAutoML Tablesの工程を比較してみましょう。AutoML Tablesの場合、データをインポートするだけで予測が可能です。

■ 一般的な機械学習とAutoML Tablesの工程比較

