Google Cloud

とあるクラウドと Google Cloud のプロが語る

マルチクラウドの未来

株式会社G-gen
クラウドソリューション部
部長

杉村 勇馬

スピーカー自己紹介

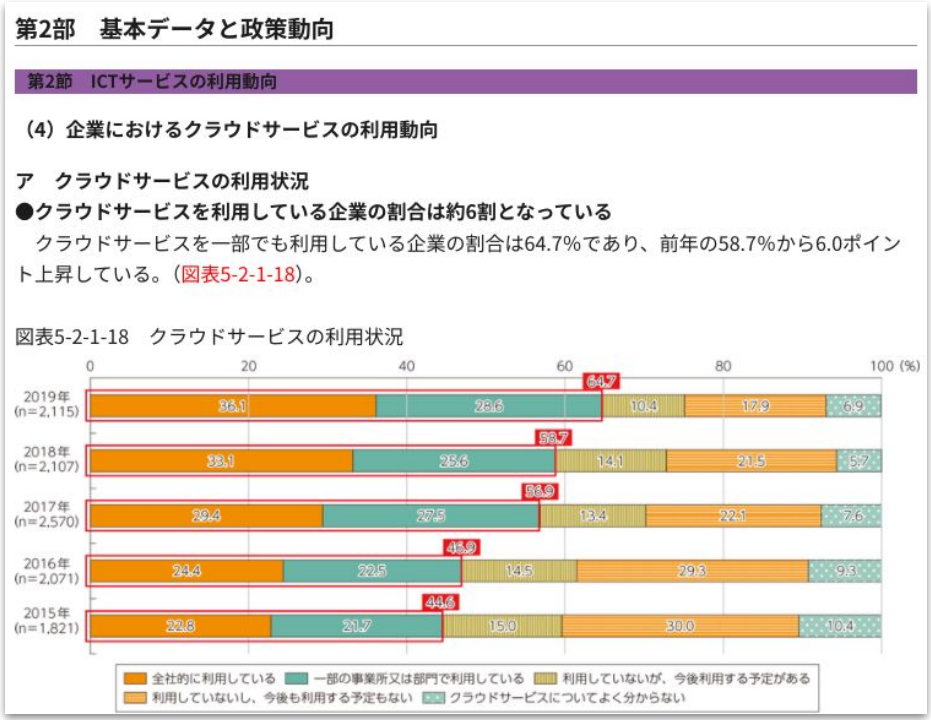
≈

株式会社G-gen
クラウドソリューション部
部長

- 元・埼玉県警 警察官
- 2017/04～: 株式会社サーバーワークス クラウドインテグレーション部
- 2019/04～: クラウドインテグレーション部 技術課 課長
- 2021/09～: 現職

今日のトピック

はじめに



第2部　基本データと政策動向

第2節　ICTサービスの利用動向

（4）企業におけるクラウドサービスの利用動向

ア　クラウドサービスの利用状況

●クラウドサービスを利用している企業の割合は約6割となっている

クラウドサービスを一部でも利用している企業の割合は64.7%であり、前年の58.7%から6.0ポイント上昇している。（図表5-2-1-18）。

図表5-2-1-18　クラウドサービスの利用状況

総務省 HP: **企業におけるクラウドサービスの利用動向**より引用
(https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd252140.html)

- パブリッククラウドの活用が当たり前になってかなり時間が経った
- 次の段階として、マルチクラウドの利用もあたりまえになりつつある
- なぜか？

今日のトピック

本日は AWS プレミアコンサルティングパートナーである
サーバーワークスの子会社であり、
Google Cloud のプレミアパートナーである G-gen社が、

- **今の日本**のマルチクラウドの状況はどうなっているのか？
- **どのように**利用するべきか？ **避けるべきこと**は何か？
- 着目すべき**課題**は何か？

といったことについて、ご紹介します。

マルチクラウドの状況

日本の傾向

社内システムの IT 基盤として

オンプレミス と
AWS or/and **Azure** を利用

オンプレミス
(データセンター)

A
N
D

AWS

Azure

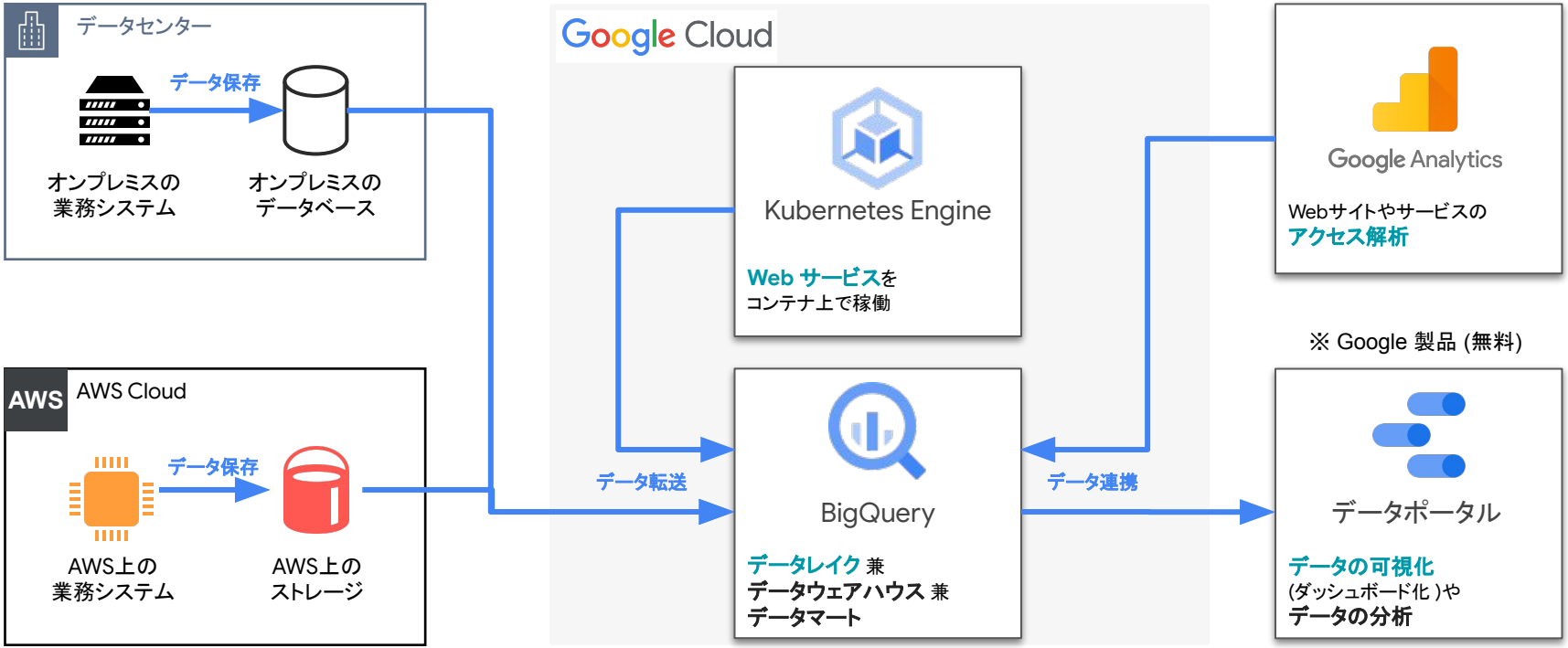
+

特定用途のために

Google Cloud を利用

Google Cloud

- **コンテナ** ベースの
  Web アプリケーション
- **データ分析** (BigQuery)
- AI/ML


データセンター
データ保存
オンプレミスの
業務システム
オンプレミスの
データベース
AWS
AWS Cloud
データ保存
AWS上の
業務システム
AWS上の
ストレージ
Google Cloud
Kubernetes Engine
Web サービスを
コンテナ上で稼働
データ転送
BigQuery
データレイク 兼
データウェアハウス 兼
データマート
データ連携
Google Analytics
Webサイトやサービスの
アクセス解析
※ Google 製品 (無料)
データポータル
データの可視化
(ダッシュボード化)や
データの分析

マルチクラウドの Do と Don’t

やってはいけない

1. **一つのシステムを複数クラウドで冗長化**

   異なる運用ノウハウや手順が必要になるため **保守コストが増大**

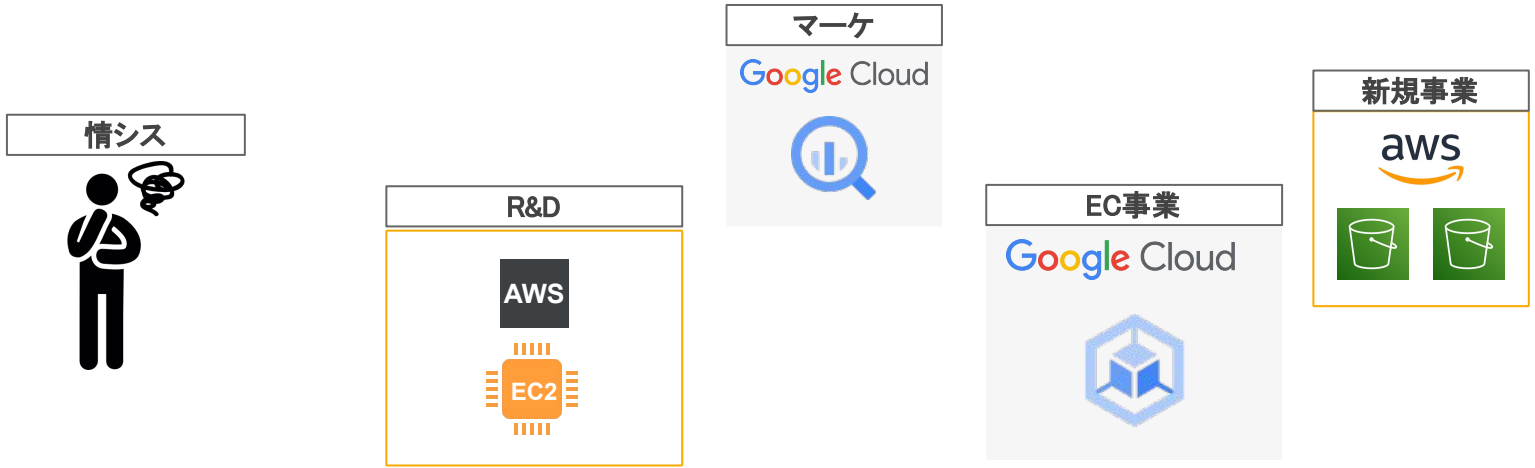
   可用性の確保は、**一つのクラウドの中で適切な設計**（ゾーン冗長化・リージョン冗長化)をすることで図るべき

やってはいけない

2. シャドー IT

別々の事業部門が、別々のパブリッククラウドを、何の監督もなしに利用している状態
セキュリティ基準もバラバラ
適切にガバナンスを効かせられれば、**セキュリティ向上** や**コストメリット**が得られる

全体最適の観点で、権限の集約と分譲のバランスを探ることが望ましい （≠ 中央集権化）



おすすめ

望ましいマルチクラウドは、

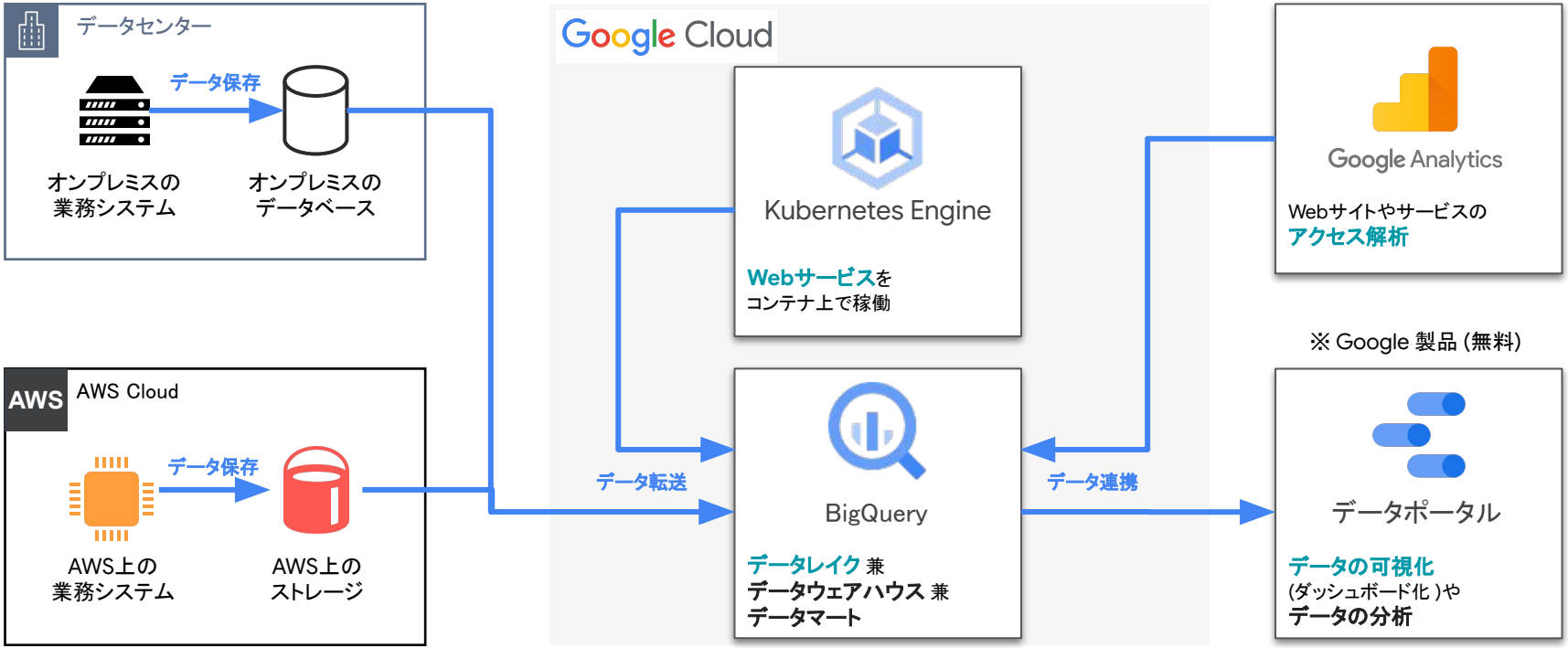
IT インフラは一つのクラウドに軸をおきつつ、
各クラウドサービスの得意分野を使い分ける

というもの

前述した

- **社内システムの IT 基盤として** オンプレミス + AWS or/and Azure を利用
- 一部の **特定用途のために** Google Cloud を利用

といったケースは、これに合致している


データセンター
データ保存
オンプレミスの
業務システム
オンプレミスの
データベース
AWS
AWS Cloud
データ保存
AWS上の
業務システム
AWS上の
ストレージ
Google Cloud
Kubernetes Engine
Webサービスを
コンテナ上で稼働
データ転送
BigQuery
データレイク 兼
データウェアハウス 兼
データマート
データ連携
Google Analytics
Webサイトやサービスの
アクセス解析
※ Google 製品 (無料)
データポータル
データの可視化
(ダッシュボード化)や
データの分析

マルチクラウドの未来

マルチクラウドの未来

日本企業では今後、以下のような方向性が想像される

- DX を背景に **IT 内製化**が進む
  - 差別化に繋がりにくい SoR は**アウトソース寄り**
  - 差別化に繋がりビジネス密結合・スピードが求められる SoE や SoI は**内製寄り**
  - いずれも**クラウド・バイ・デフォルト**
- この背景から **最適なプラットフォーム**(サービス) **を選択するために**
  ユーザー企業主導で **能動的に**マルチクラウド戦略が取られる

主要パブリッククラウドの強み

AWS / Azure / Google Cloud サービス対照表

得意・不得意はあれど、本気で **やろうと思えば、できることはほぼ同じ**。

サービス	Google Cloud	Amazon Web Services (AWS)	Microsoft Azure
仮想サーバ	Google Compute Engine (GCE)	Amazon EC2	Azure Virtual Machines
仮想ネットワーク	Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC)	Azure Virtual Network
マネージドDB	Cloud SQL	Amazon RDS	Azure Database
データウェアハウス	BigQuery	Amazon Redshift	Azure Synapse Analytics
オブジェクト ストレージ	Cloud Storage	Amazon S3	Azure Blob
可視化 (BI) ツール	Data Portal / Looker	Amazon QuickSight	Power BI
ID・権限管理	Cloud Identity / Cloud IAM	AWS IAM	Azure Active Directory / Azure RBAC
コンテナオーケストレーション	Google Kubernetes Engine (GKE)	Amazon ECS / Amazon EKS	Container Instances / Azure Kubernetes Service
DNS	Cloud DNS	Amazon Route 53	Azure DNS
FaaS	Cloud Functions	AWS Lambda	Azure Functions

強み

3 大パブリッククラウドの強み

Amazon Web Services

- IaaS 機能は 3 クラウドで最も充実しており、実現できることが多い
- **技術者が多い・情報が手に入りやすい**

IaaS

Google Cloud

- **データ分析基盤** (特に BigQuery)
- **Web アプリケーション用プラットフォーム**
  (Google Kubernetes Engine (GKE) や App Engine (GAE) など)

Data

Microsoft Azure

- **Active Directory**
- Microsoft 製品との連携や**ライセンスのコストメリット**
  (Windows Server, Active Directory, MS SQL Server...)

ID (Microsoft)

IaaS としての Google Cloud

インフラを移行する先としての Google Cloud もオススメしています。

1

データ分析に強い

BigQueryなどのデータ分析サービスの存在に加えて Google Analytics 等のマーケ系サービスとの親和性も高い。
社内システムを Google Cloud に移行することで今後の**データ活用をスムーズに実現**できる

2

CPU / Memory あたりの料金が安い

仮想サーバの CPU / Memory あたりの料金が AWS を始めとする**他のパブリッククラウドよりも安価**に利用できる

3

権限管理がシンプル

Google Workspace (旧 G Suite) もしくは Cloud Identity (無償から) と連携した ID 管理に加えプロジェクト (テナント) 分割が容易に行えるなど**権限管理・分譲がシンプル**

課題とその対処法

セキュリティ・統制

セキュリティ・統制

課題

担当者が複数クラウドを扱うことによって学習コストがかかり
意識すべきセキュリティ要件が意識できない状態になる可能性があります。

→ 誤設定・ガードレイルの設置不足等によるセキュリティ・インシデントのリスクが増えます。

例:

1. AWS にも Google Cloud にも “**IAM**” という言葉が出てくるがその **内部構造は大きく異なる**。
   同じものと理解してしまうと誤設定が生じる。

2. AWS Security Hub や Security Command Center (Google Cloud) など CSPM 的な検知機能を
   ON にしても、その **検知結果の意味・優先度・対処法が分からない**状態になり
   リスク低減等のアクションが取れない。

プラットフォームセキュリティ（AWS）

証跡管理	「いつ、だれが、何を、どのように」 実行したか記録する	AWS Config →変更記録 AWS CloudTrail →API履歴記録 Amazon CloudWatch Logs →ログ管理
予防的対策	オペレーションミスや悪意ある行動により、 システムに不利益がもたらされることを防止する	AWS Organizations (SCP) AWS Identity and Access Management (IAM)
発見的対策	システムに不利益がもたらされたことを検知する	AWS Security Hub Amazon GuardDuty Amazon EventBridge (旧CloudWatch Events)

プラットフォームセキュリティ (Google Cloud)

証跡管理	「いつ、だれが、何を、どのように」 実行したか記録する	 Cloud Audit Logs  Cloud Logging
予防的対策	オペレーションミスや悪意ある行動により、 システムに不利益がもたらされることを防止する	 Cloud Resource Manager  Cloud IAM
発見的対策	システムに不利益がもたらされたことを検知する	 Cloud Monitoring  Cloud Logging  Security Command Center

セキュリティ・統制

対処法

以下のような対処法が考えられます。

1. **担当者のスキルアップ**

   公式トレーニング受講、資格試験の取得、新規採用

2. **パートナーの活用**

   クラウドに関する高度な知見を持ち、**かつエンタープライズ IT に慣れている**ベンダーを選定する必要がある。こういったベンダーにセキュリティ アセスメントと対処を行ってもらう。

3. サードパーティ **CSPM・NDR 製品等の活用**

   クラウドを横断で検知・管理できる CSPM (Cloud Security Posture Management) 製品等を活用する。

   参考記事: クラウドセキュリティに「NDR」と「CSPM」が欠かせない理由とは。G-gen主催ウェビナーをレポート (TECH+, マイナビ)

アカウント管理

アカウント管理

課題

利用対象のクラウドが増えてくると、アカウント管理が大変になってきます。

例:

1. **クラウドの管理コンソールのアカウント**
   - AWS => IAM User
   - Google Cloud => Google アカウント ...
2. **仮想サーバのアカウント**
   - Linux の OS ユーザー
   - Windows の OS アカウント ...
3. **マネージドサービスのアカウント**
   - Amazon QuickSight や Amazon Connect など、
   - 利用法によっては IAM User と紐付かないアカウント等

アカウント管理

対処法

以下のような対処法が考えられます。

1. **ID Federation**

   Active Directory を IDaaS として AWS や Google Cloud と ID 連携。

   自動プロビジョニングなどの仕組みを構築する。

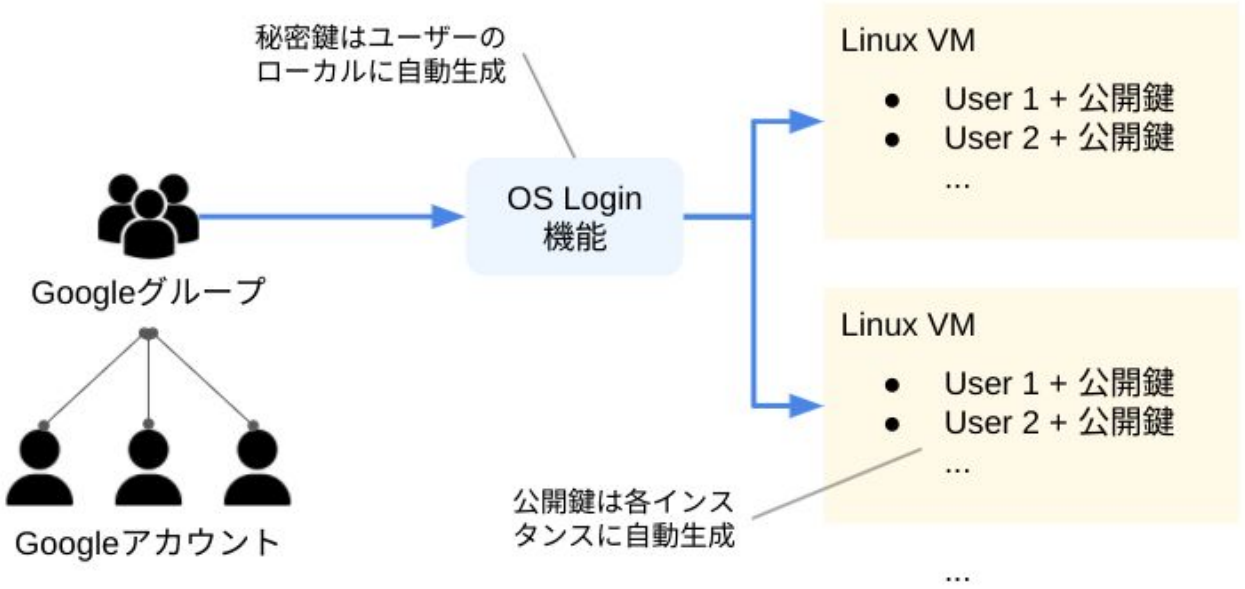
2. 仮想サーバの OS アカウントを**クラウドアカウントと連携**

   AWS => AWS Systems Manager Session Manager 機能

   Google Cloud => OS Login 機能

参考記事: Google Compute EngineのOS Login機能でSSHユーザを楽に管理しよう

OS Login 機能 (Google Cloud)




```
$ gcloud compute ssh --project=${PROJECT_ID} --zone=${ZONE} ${VM_NAME}
```

CLI コマンドで簡単にログインできる

リソース管理

リソース管理・請求管理

課題

利用対象のクラウドが増えてくると、リソース管理が大変になってきます。

例:

1. **テナント (AWS アカウント/ Google Cloud プロジェクト)**
   どの部署が**どこ**で**何を**しているのか
2. **仮想サーバやマネージドサービスのリソース**
   どの部署が**何**を**どのくらい**使っているのか
3. **請求管理**
   請求はどうなっているか
   適切なコスト削減ができているか

リソース管理・請求管理

対処法

以下のような対処法が考えられます。

1. アカウント**特権管理**と**管理監督**の体制を構築

   クラウドリソースを専任で管理監督する体制（**CCoE** と呼べるかもしれない）を構築。

   各部門の利用するクラウド環境を横断して閲覧できるようにしておく。

2. サードパーティ**管理製品の活用**

   リソースを横断的に視覚化する製品などを活用する

3. **パートナーの活用**

   クラウドに関する高度な知見を持ち、**かつエンタープライズ IT に慣れている**ベンダーを選定する必要がある。こういったベンダーに管理を一部、代行してもらう。

ネットワーク

ネットワーク

課題

利用対象のクラウドが増えてくると、ネットワーク管理が大変になってきます。

例:

1. **専用線 (閉域網) やインターネット VPN**
   敷設、監視、月額回線費用 ...
2. **クラウド VPC の管理運用**
   利用部門は適切に VPC 設定をしているか？
   IT 部門なり CCoE が VPC を中央管理すべきなのか？

ネットワーク

対処法

以下のような対処法が考えられます。

1. **専用線（閉域網）神話を捨てる**

   専用線が安全だという神話を捨てるときかもしれません。パブリッククラウドはインターネット経由での利用が前提です。**暗号化**・**認証/認可**・**利用者属性に基づく認証**などを適切に行えばインターネット経由でも安全です。

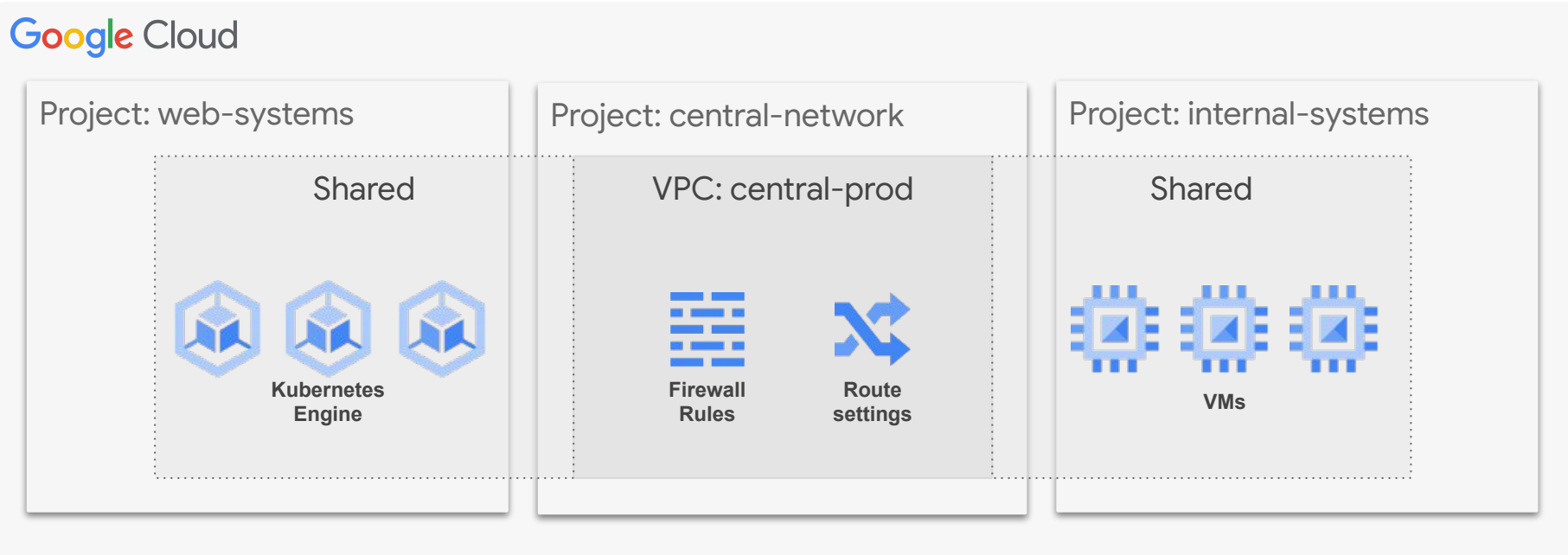
2. **Shared VPC の活用**

   VPC を中央管理し、それを利用部門にシェアして利用してもらう Shared VPC 機能を活用。セキュアなネットワーク設定を維持する。

   AWS : Share VPCs with AWS RAM

   Google Cloud : Shared VPC overview

Shared VPC の活用



- VPC の中央管理を情シス等が行う（不用意なネットワーク設定がされないよう）
- 業務部門は、VPC を “間借り” して使用し、自分たちのリソースを配置する。
  ※リソースの請求はリソースが存在するプロジェクトに対して行われる。

まとめ

避けるべき / 望ましいマルチクラウド

以下のようなマルチクラウド導入は、避けるべき

1. **一つのシステムを複数クラウドで冗長化**
2. **シャドー IT**

反対に、望ましいマルチクラウドは、以下

IT インフラは一つのクラウドに軸をおきつつ、
各クラウドサービスの得意分野を使い分ける

マルチクラウドの未来

日本企業では今後、以下のような方向性が想像される

- DX を背景に **IT 内製化**が進む
  - 差別化に繋がりにくい SoR は**アウトソース寄り**
  - 差別化に繋がりビジネス密結合・スピードが求められる SoE や SoI は**内製寄り**
  - いずれも**クラウド・バイ・デフォルト**
- この背景から **最適なプラットフォーム**(サービス) **を選択するために**
  ユーザー企業主導で **能動的に**マルチクラウド戦略が取られる

G-gen のスタンス

お客様のクラウドジャーニーを伴走支援

G-gen は Google Cloud を専業とするクラウドネイティブな会社ではありますが、
AWS や **オンプレミス IT** に対する深い知見を持つ営業・エンジニアが在籍しています。

- クラウド導入が **初めて**
- クラウドの知見を持つ人が **社内にいない**
- AWS や Azure は触ったことがあるが **Google Cloud のことは分からない**

上記のようなお客様に対して G-gen は **伴走** しながらサービスを提供します。
「作って終わり」ではなく **今後の運用** やお客様による **内製化** を視野に入れ、
営業とエンジニアが一体となってプロジェクトを進めます。

G-gen Tech Blog

G-gen Tech Blog では、

Google Cloud の日本語情報を提供することで

日本にクラウド技術を普及させることを

目的として、日々情報を追加しています。

G-gen ブログ　検索

G-gen のメリット

G-gen の請求代行サービス では、

Google Cloud を 5 % オフで利用可能です。

G-gen 請求代行

検索

Thank you.

Google Cloud