



クラウド経験者に送る Google Cloud ネットワーキングの 必修ポイント

有賀 征爾

グーグル・クラウド・ジャパン合同会社

カスタマーエンジニア

スピーカー自己紹介



有賀 征爾

グーグル・クラウド・ジャパン合同会社
カスタマーエンジニア

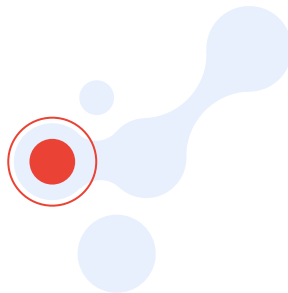
Google Cloud でネットワーキングを専門にプリセールスエンジニアをしています。ネットワーキングはクラウドサービスを使う場合の基本になる部分であり非常に面白い分野です！



本セッションの目的

本セッションの目的

- Google Cloud におけるネットワーキングの基礎を紹介
 - 設計や考え方からの理解
- Google Cloud らしい特徴の紹介



Virtual Private Cloud

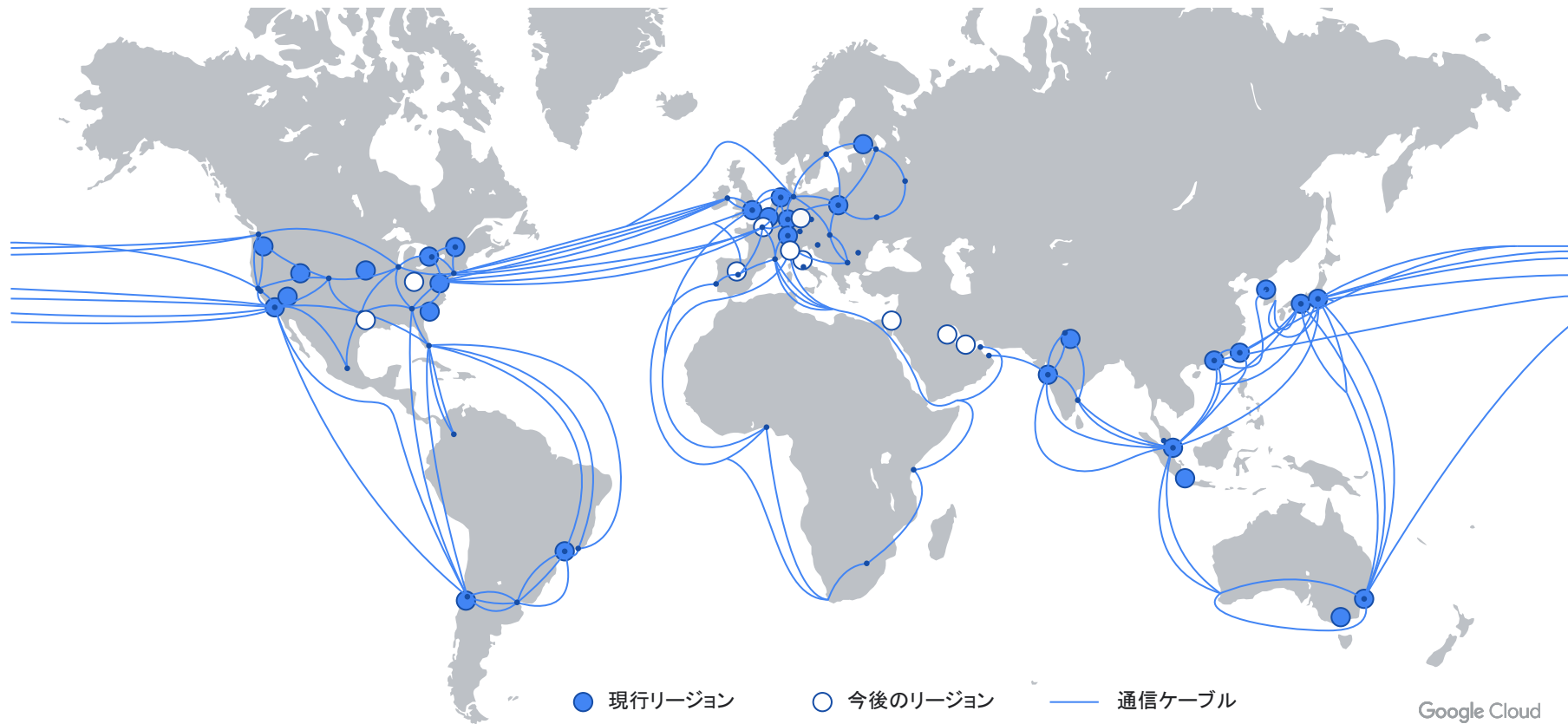


Cloud Interconnect

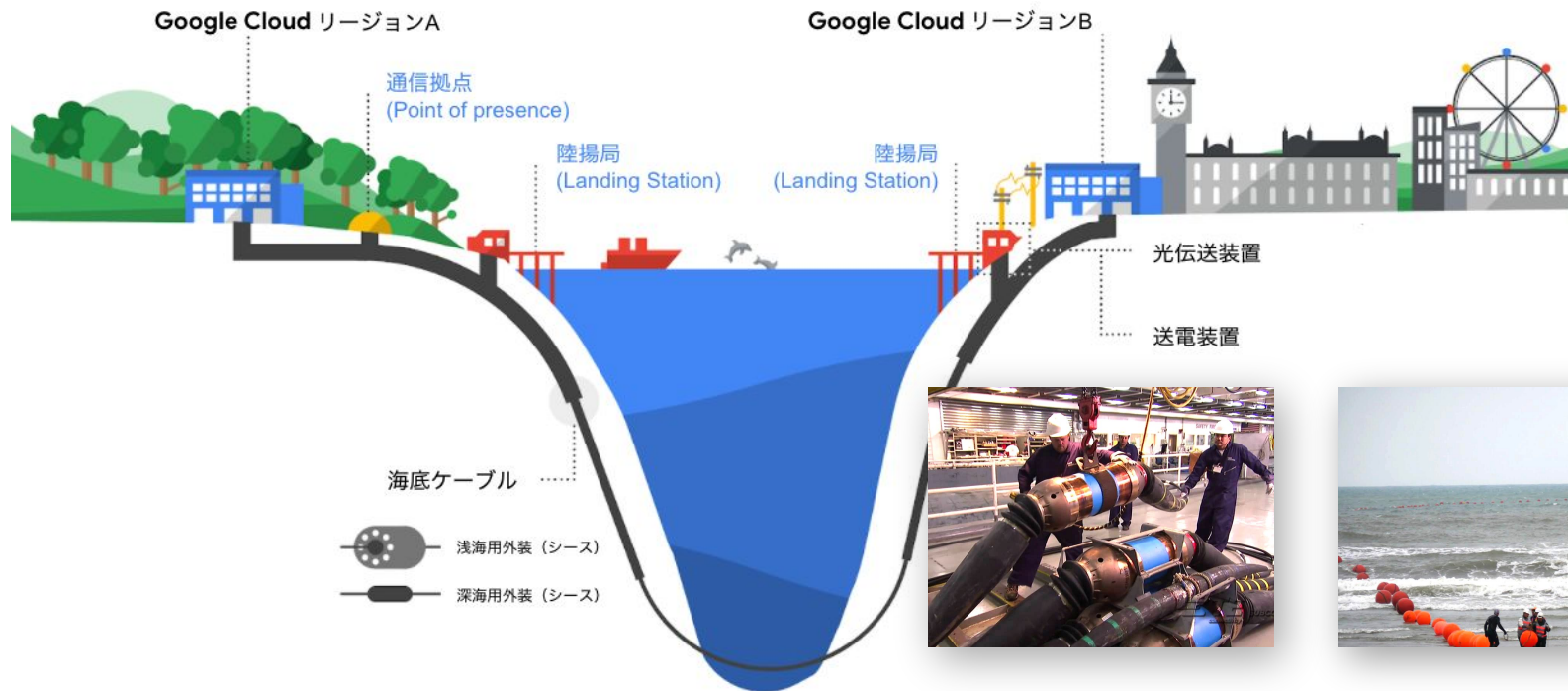


ネットワークの基礎

物理のネットワーク

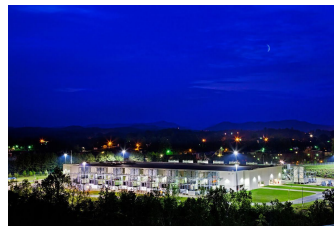


物理のネットワーク



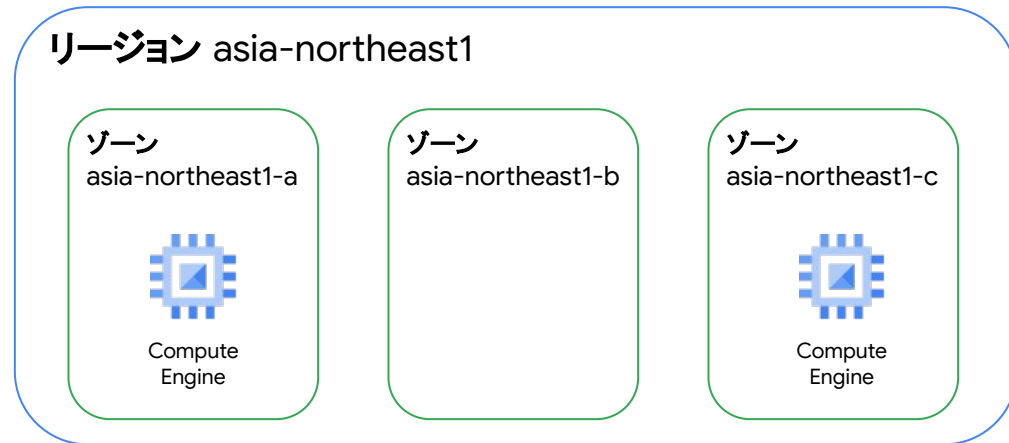
リージョン

- 複数のデータセンターで構成
- Compute Engine のインスタンスなどが物理的に稼働する場所



ゾーン

- リージョンを分割
 - 相互に障害の影響が及ばないように
 - 多くは 1 リージョンに 3 つのゾーン



Virtual Private Cloud

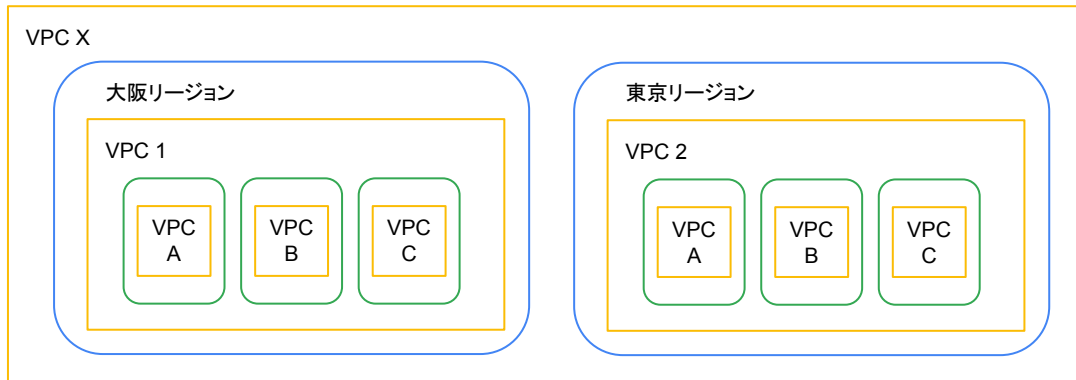


Virtual Private Cloud

- ネットワークの一番基本的な単位
 - 論理的なリソース

問題

- VPC の範囲？
 1. グローバル - VPC X
 2. リージョン - VPC1, 2
 3. ゾーン - VPC A, B, C



Virtual Private Cloud



- ネットワークの一番基本的な単位
 - 論理的なリソース

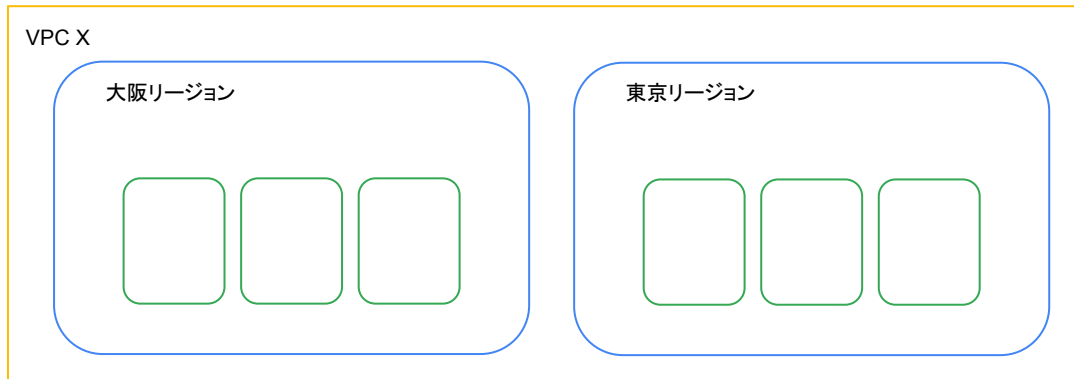
- VPC の範囲

1. グローバル - VPC X

→ 簡単にグローバル構成

2. ~~リジョン~~ → VPC1,2

3. ~~ゾーン~~ → VPC A, B, C



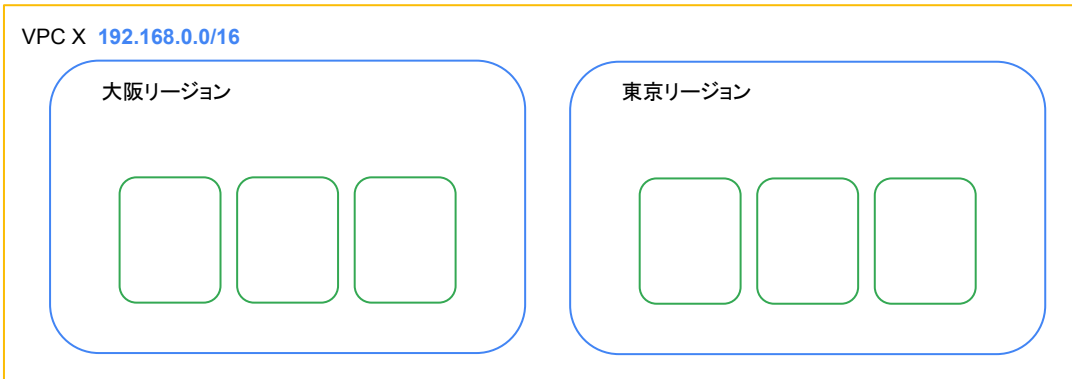
Virtual Private Cloud



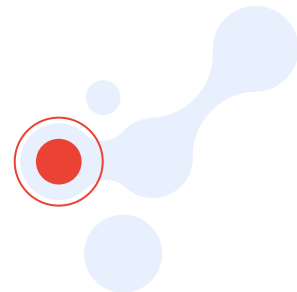
- ネットワークの一番基本的な単位
 - 論理的なリソース
 - **IP アドレスの設定**

問題

- IP アドレスの設定対象？
 1. 各サブネット
 2. VPC と各サブネット



Virtual Private Cloud



- ネットワークの一番基本的な単位

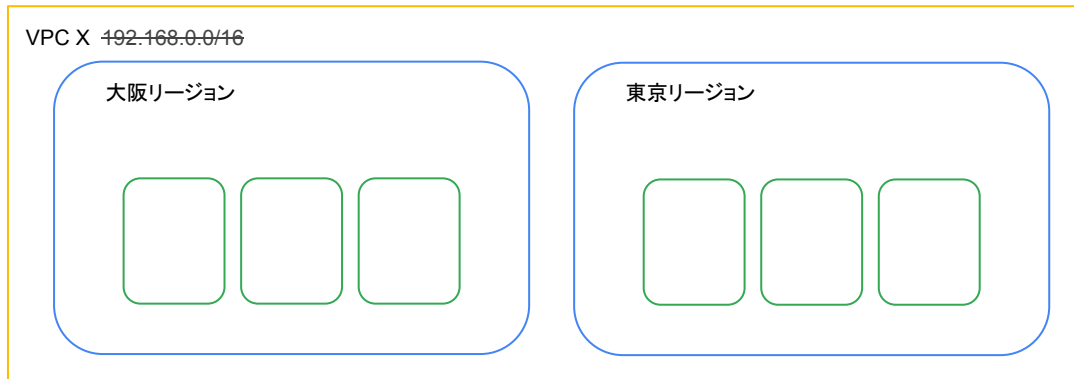
- 論理的なリソース
- IP アドレスの設定

- IP アドレスの設定対象

1. 各サブネット

→ 自由なアドレス設計

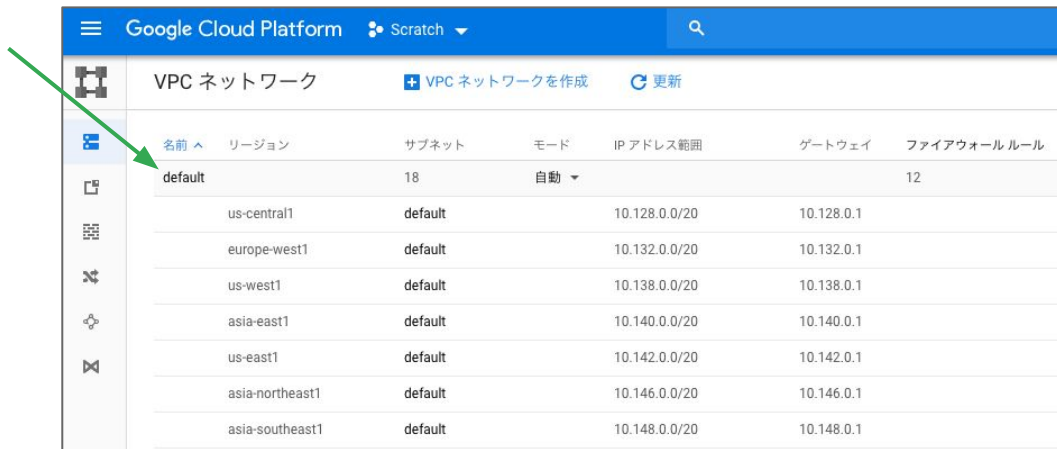
2. ~~VPC と各サブネット~~



Virtual Private Cloud



- “default” という名前の VPC は削除しても問題ありません
 - テスト以外での利用は推奨しません

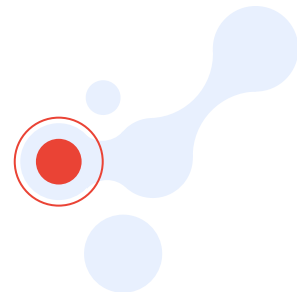


Google Cloud Platform Scratch

VPC ネットワーク + VPC ネットワークを作成 更新

名前	リージョン	サブネット	モード	IP アドレス範囲	ゲートウェイ	ファイアウォール ルール
default		18	自動			12
	us-central1	default		10.128.0.0/20	10.128.0.1	
	europa-west1	default		10.132.0.0/20	10.132.0.1	
	us-west1	default		10.138.0.0/20	10.138.0.1	
	asia-east1	default		10.140.0.0/20	10.140.0.1	
	us-east1	default		10.142.0.0/20	10.142.0.1	
	asia-northeast1	default		10.146.0.0/20	10.146.0.1	
	asia-southeast1	default		10.148.0.0/20	10.148.0.1	

Virtual Private Cloud - サブネット



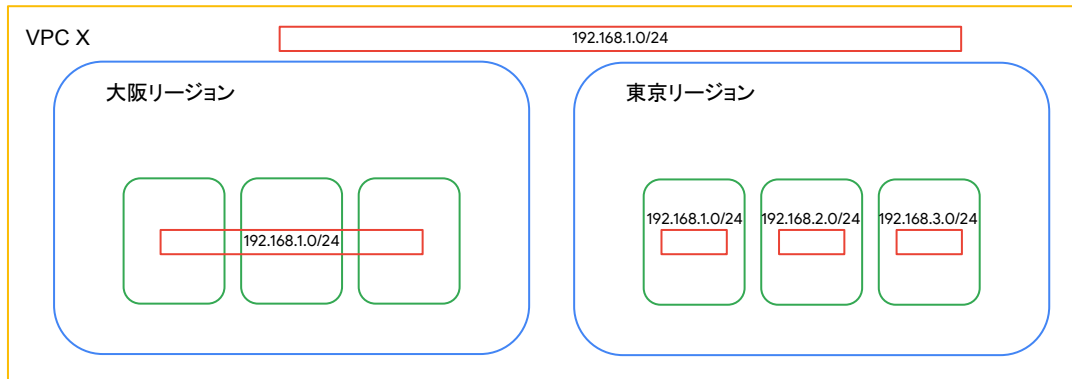
- ネットワークの一番基本的な単位

- 論理的なリソース
- IP アドレスの設定

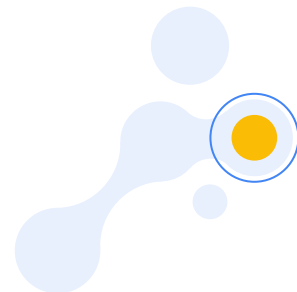
- IP アドレスの設定対象

問題 サブネット？

1. グローバル
2. リージョン
3. ゾーン



Virtual Private Cloud - サブネット



- ネットワークの一番基本的な単位

- 論理的なリソース
- IP アドレスの設定

- IP アドレスの設定対象

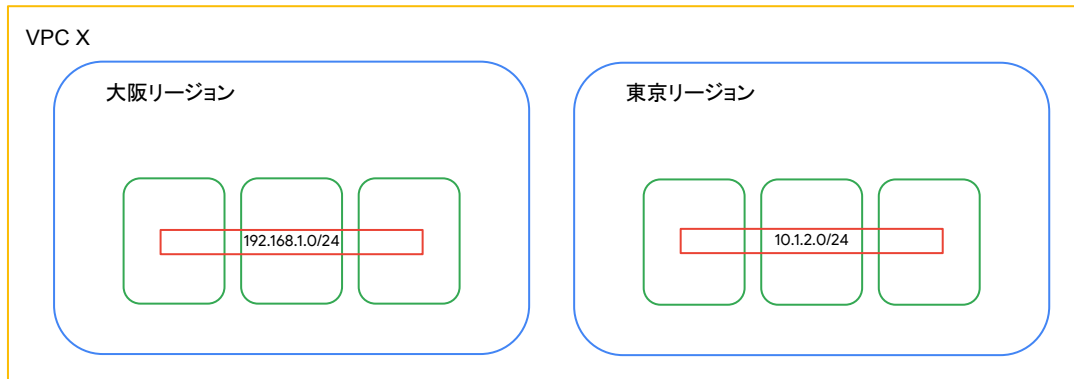
- サブネット

1. ~~グローバル~~

2. リージョン

→ 冗長をシンプルに

3. ~~ゾーン~~



Virtual Private Cloud - サブネット



- ネットワークの一番基本的な単位

- 論理的なリソース
- IP アドレスの設定

- IP アドレスの設定対象

- サブネット

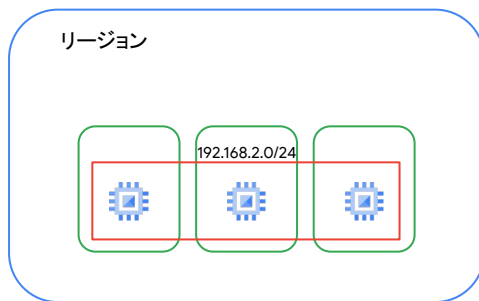
- リージョン

→ 冗長をシンプルに

Google Cloud

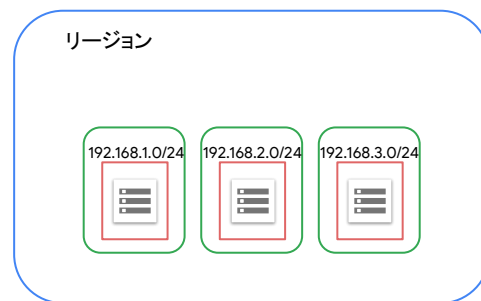
リージョン単位のサブネットの場合

サブネット1つ



ゾーン単位のサブネットの場合の例

サブネット3つ



Virtual Private Cloud - サブネット

- VM のサブネットマスク
 - 常に /32
 - ARP が発生しない
 - 一致させることも可
 - MULTI_IP_SUBNET
 - VM のイメージ作成時に指定

サブネットの設定によらず常に /32



```
$ ip addr show dev ens4
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 42:01:0a:92:00:07 brd ff:ff:ff:ff:ff:ff
    inet 10.146.0.7/32 brd 10.146.0.7 scope global dynamic ens4
        valid_lft 2207sec preferred_lft 2207sec
```

サブネットの設定と同じマスク長となる例

```
$ ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP
group default qlen 1000
    link/ether 0e:7e:b9:fd:f9:75 brd ff:ff:ff:ff:ff:ff
    inet 172.31.27.249/24 brd 172.31.31.255 scope global dynamic eth0
        valid_lft 3483sec preferred_lft 3483sec
```

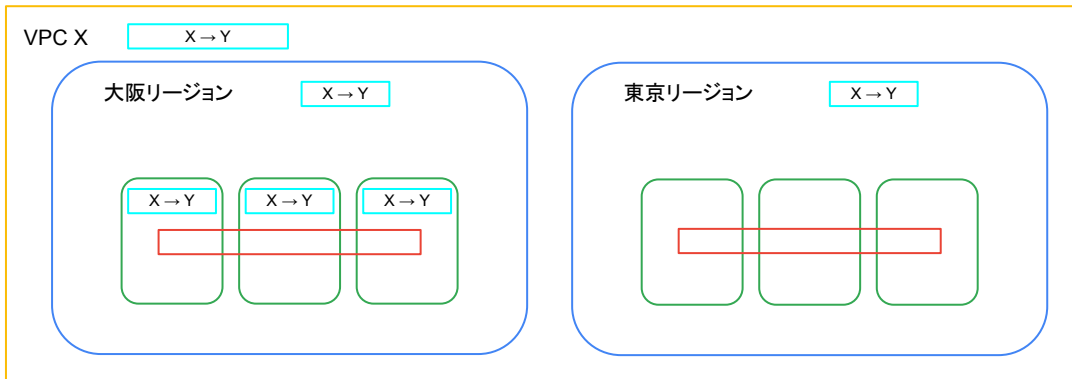
Virtual Private Cloud - ルート



- ネットワークの一番基本的な単位
 - 論理的なリソース
 - IP アドレスの設定
 - ルート

問題

- ルートの範囲？
 - グローバル
 - リージョン
 - ゾーン



Virtual Private Cloud - ルート



- ネットワークの一番基本的な単位

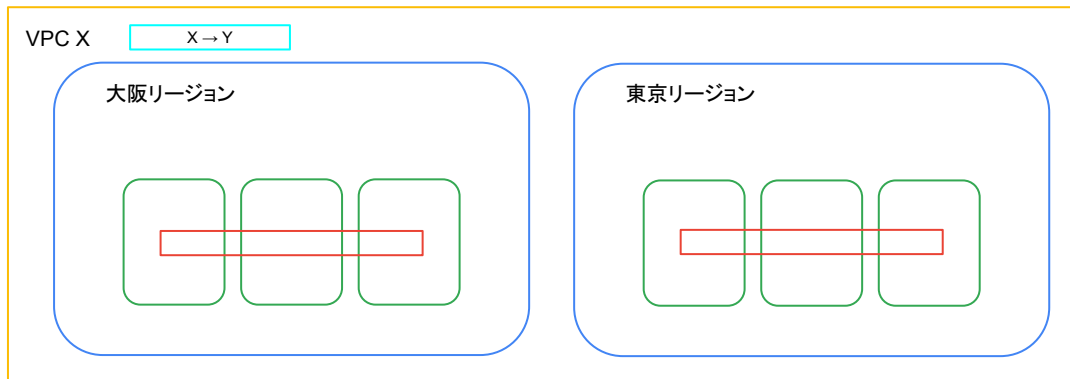
- 論理的なリソース
- IP アドレスの設定
- ルート

- ルートの範囲

- **グローバル**
 - ルーティングが簡単
 - 細かい調整には一手間

○ ~~リージョン~~

○ ~~ゾーン~~



Virtual Private Cloud - ルート

- ネットワークの一番基本的な単位

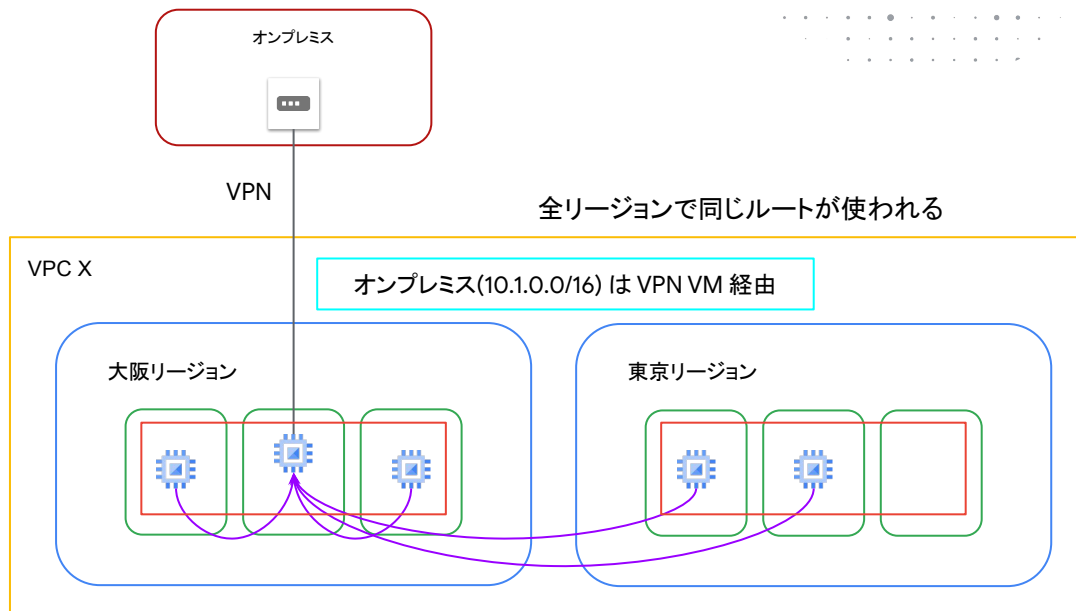
- 論理的なリソース
- IP アドレスの設定
- ルート

- ルートの範囲

- **グローバル**

→ ルーティングが簡単

→ 細かい調整には一手間



Virtual Private Cloud - ルート

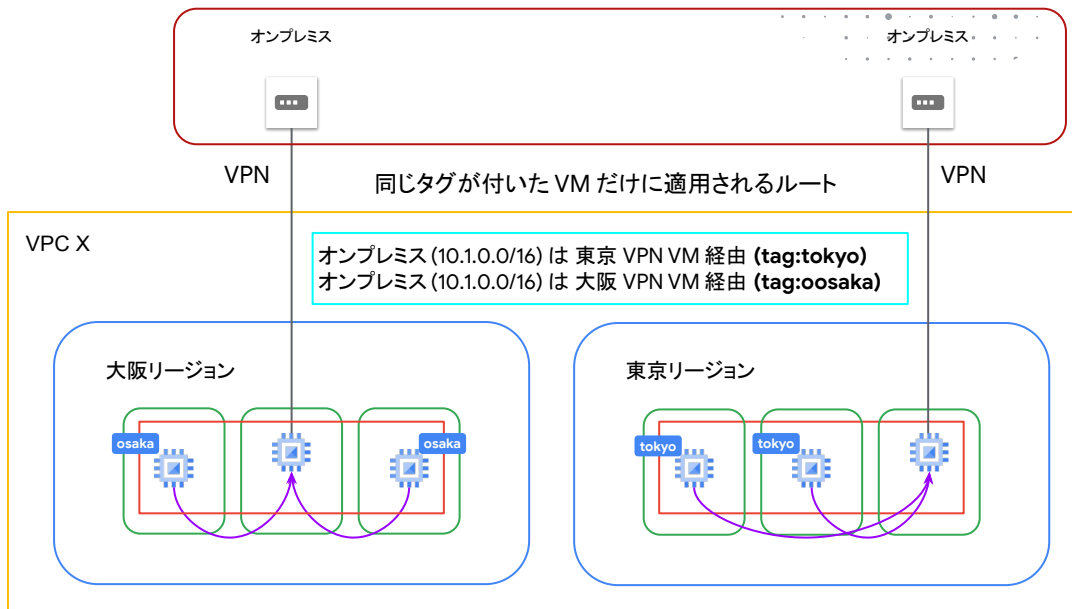
- ネットワークの一番基本的な単位

- 論理的なリソース
- IP アドレスの設定
- ルート

- ルートの範囲

- グローバル

- ルーティングが簡単
- 細かい調整には一手間
- タグを使った調整



静的ルーティング

- グローバルなリソース
- ネットワークタグで適用対象をグルーピング



← ルートの作成

名前 *
default-to-internet

小文字、数字、ハイフンのみ使用できます

Description

ネットワーク *
default

送信先 IP 範囲 *
0.0.0.0/0

例: 10.0.0.0/16

優先度 *
1000

優先度は正の整数にする必要があります (値が小さいほど優先順位が高くなります)

インスタンスタグ
public

ネクストホップ
デフォルト インターネット ゲートウェイ

作成 キャンセル

← 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

ネットワーキング

ホスト名とネットワーク インターフェース

ネットワーク タグ
public

ホスト名

このインスタンスのカスタムホスト名を設定するか、デフォルトのままにします。設定は後から変更することはできません

IP 転送

☐ 有効にする

ネットワーク パフォーマンスの構成

ネットワーク インターフェース カード
-

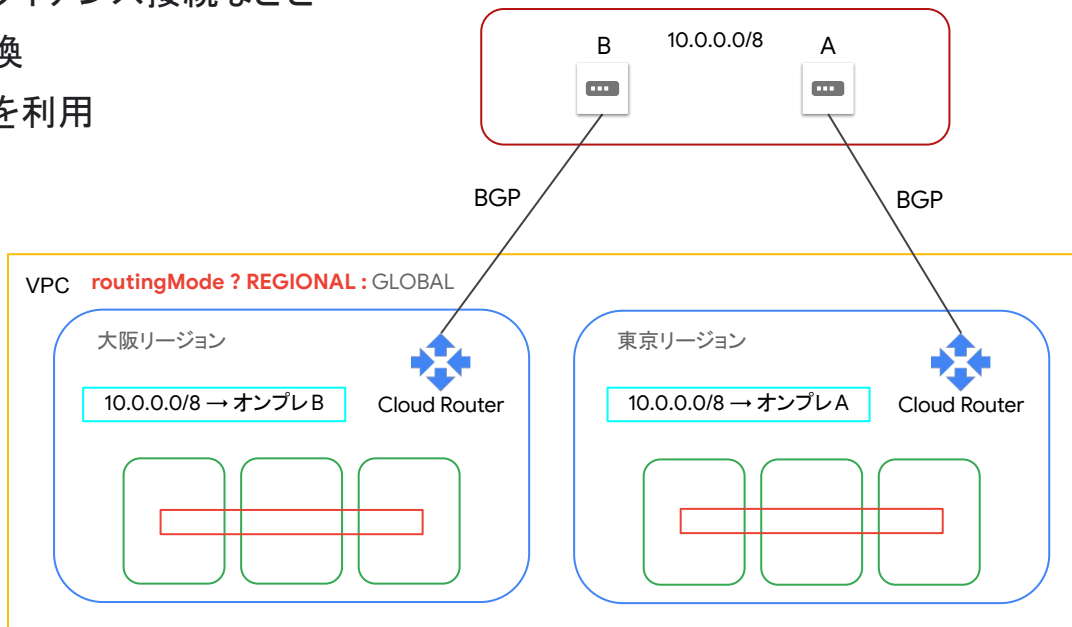
ネットワーク帯域幅

☐ 合計下り (外向き) 帯域幅を増やす
送信ネットワークの最大帯域幅: 2 Gbps

動的ルーティング

Cloud VPN Cloud Interconnect

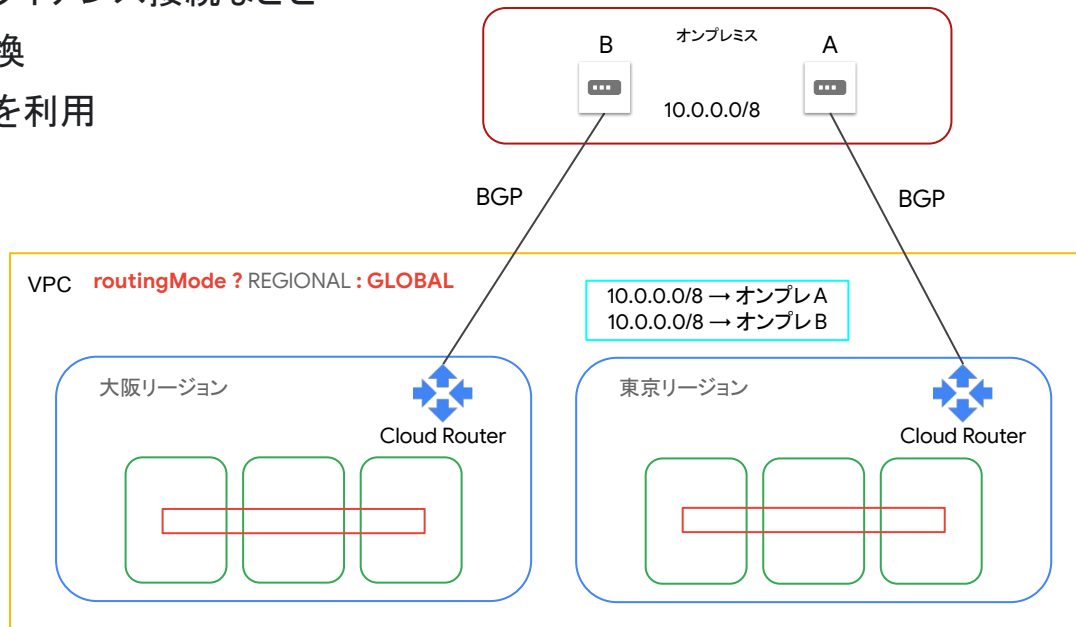
- VPN 接続、専用線接続、仮想アプライアンス接続などと動的ルーティング (BGP) で経路交換
 - Cloud Router (仮想ルータ) を利用
- VPC のルーティングモード
 - リージョナル
 - グローバル



動的ルーティング

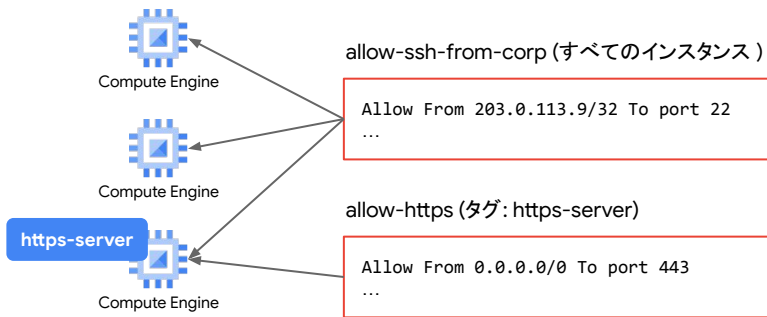
Cloud VPN Cloud Interconnect

- VPN 接続、専用線接続、仮想アプライアンス接続などと動的ルーティング (BGP) で経路交換
 - Cloud Router (仮想ルータ) を利用
- VPC のルーティングモード
 - リージョナル
 - **グローバル**
- ブログ記事 (Medium.com)

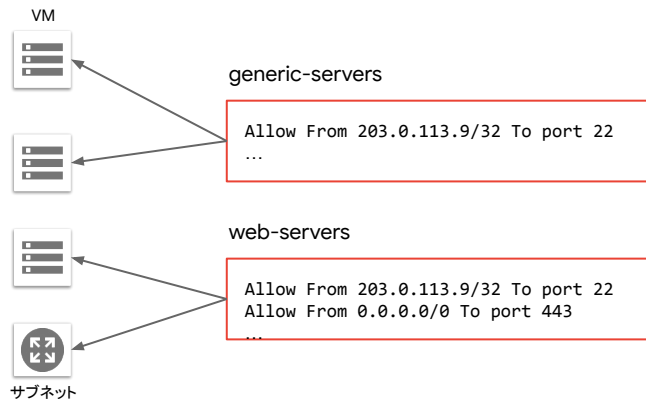


Virtual Private Cloud - ファイアウォール

- グローバル に設定 (ルートと同じ)
- ファイアウォール ルールの実現方法の例
 - Google Cloud では複数のルールを組み合わせで設定
 - VM ベースのファイアウォールのみ



目的ベースのルールを複数適用
ルール側で適用対象を設定



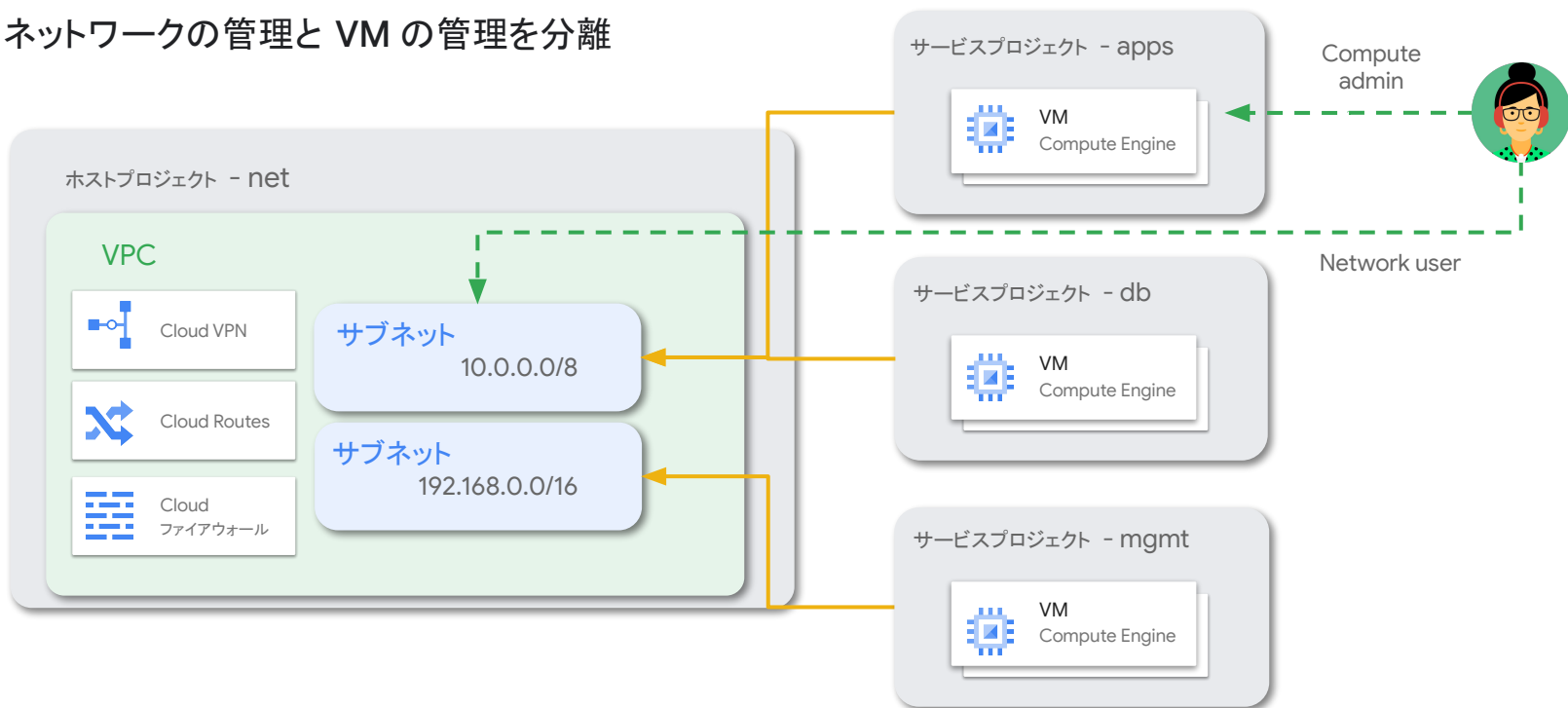
役割ベースのルールを一つ適用
VM 側で(も)適用対象を設定



特徴的な機能

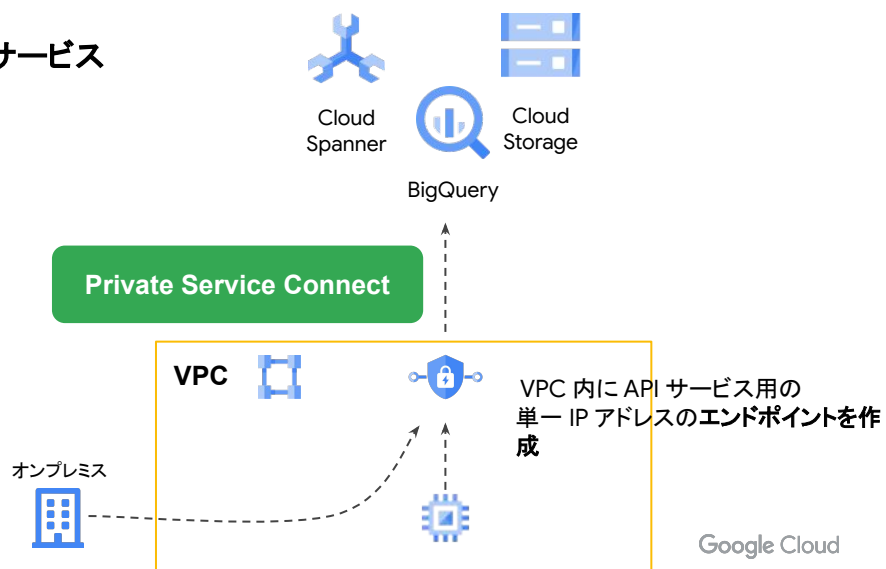
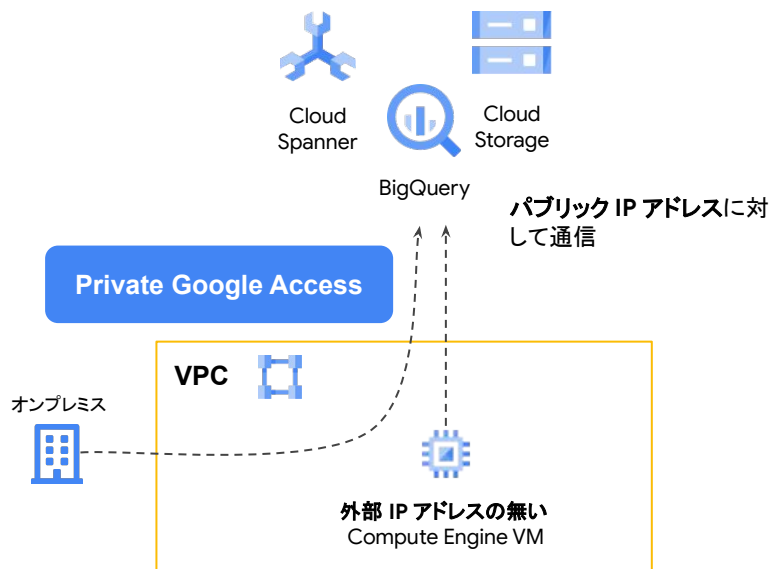
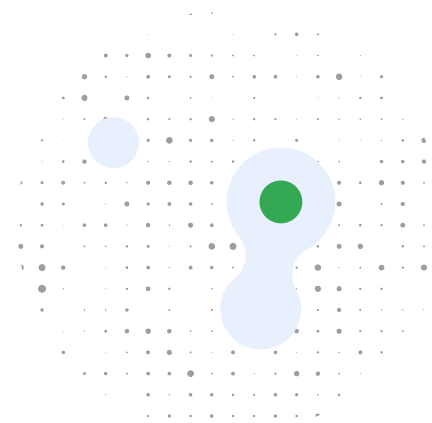
共有 VPC

- 一つの VPC を複数のプロジェクトで共有
- ネットワークの管理と VM の管理を分離



Google API (サービス)への閉域接続

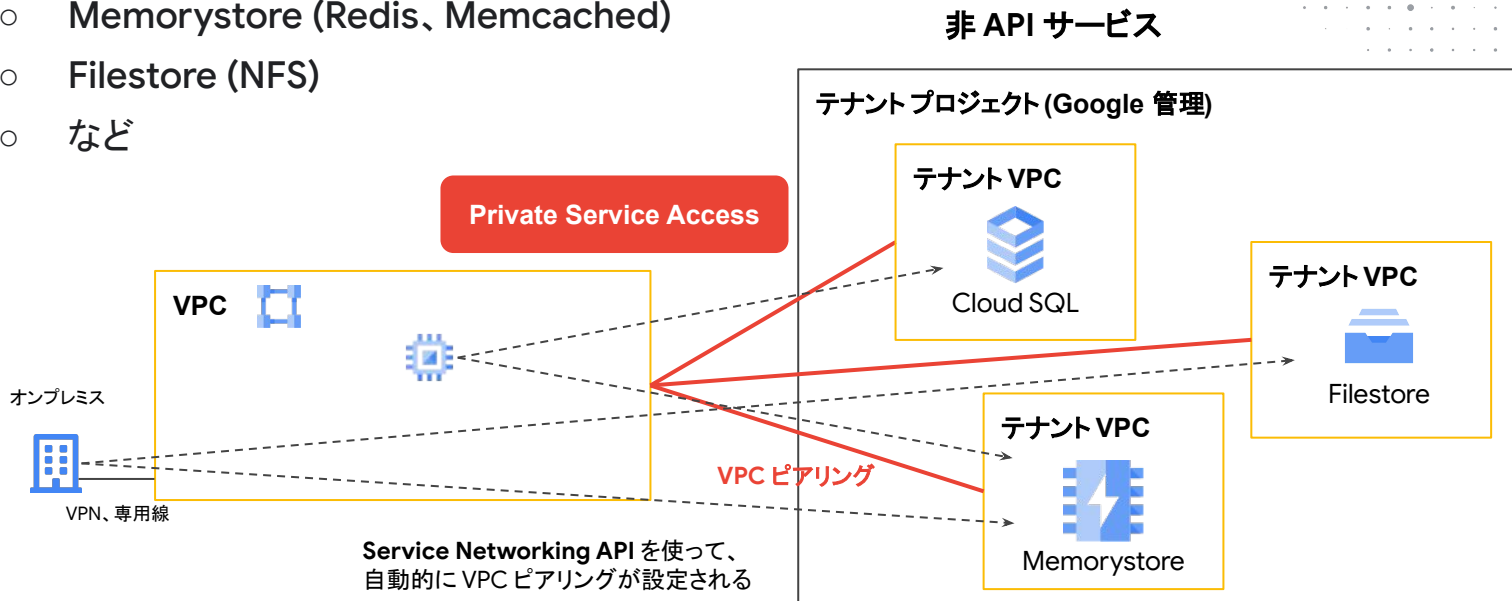
- Private Google Access
- Private Service Connect
- オンプレミスからも接続可



非 Google API (サービス)への閉域接続

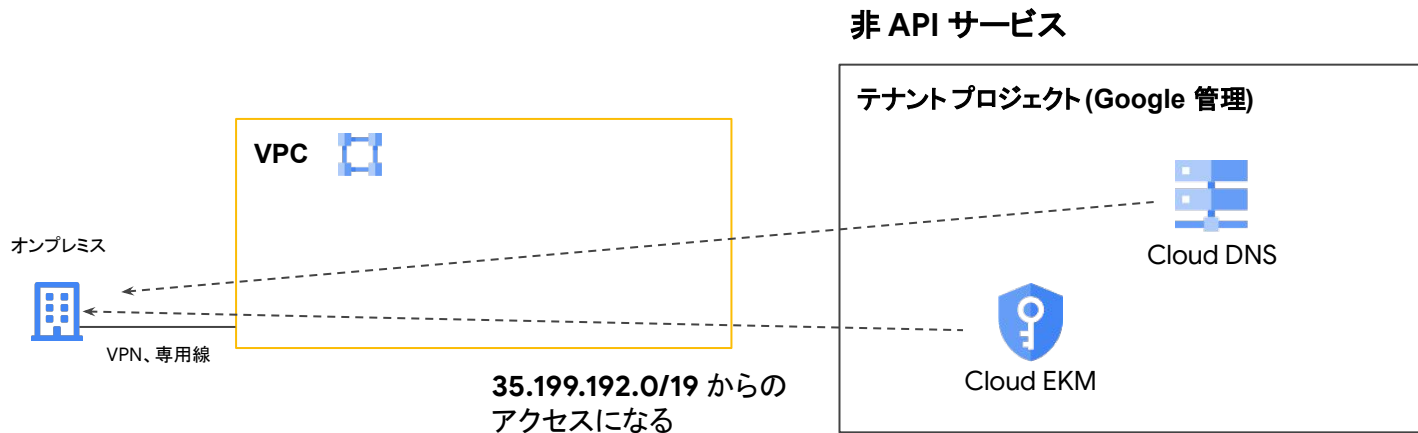
- Private Service Access

- Cloud SQL (MySQL、PostgreSQL、SQL Server)
- Memorystore (Redis、Memcached)
- Filestore (NFS)
- など



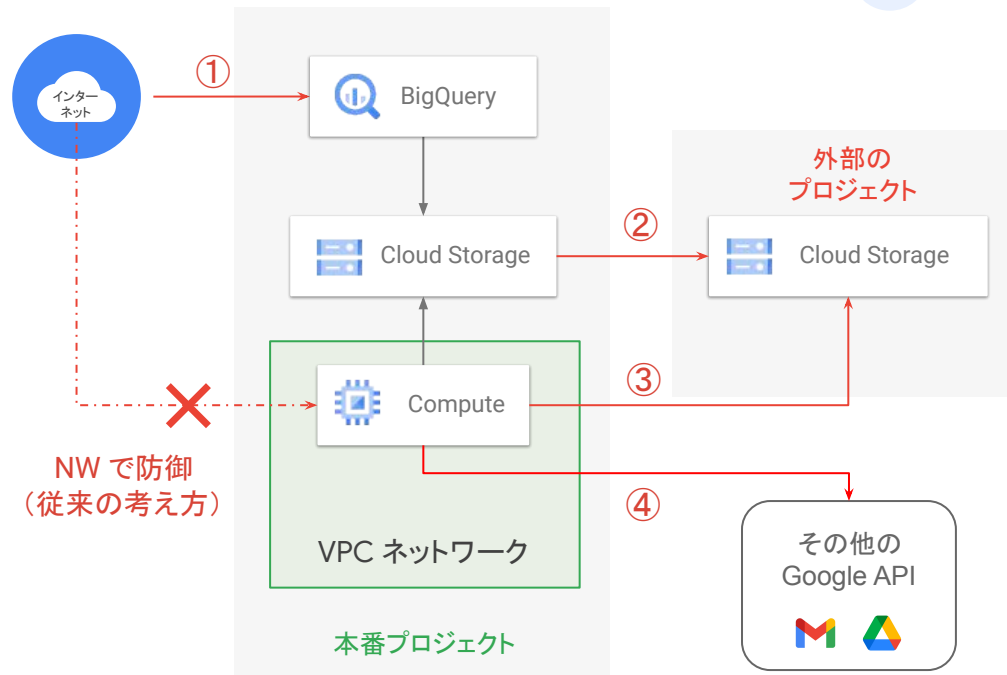
非 Google API (サービス)からの閉域接続

- マネージドサービスからオンプレミスへのアクセス
 - Cloud DNS (の DNS 転送)
 - Cloud EKM (External Key Manager)

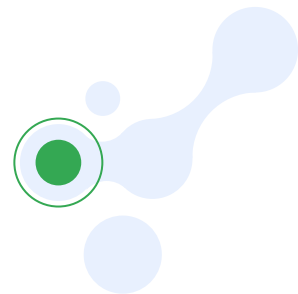


API サービスへのアクセス制限の必要性

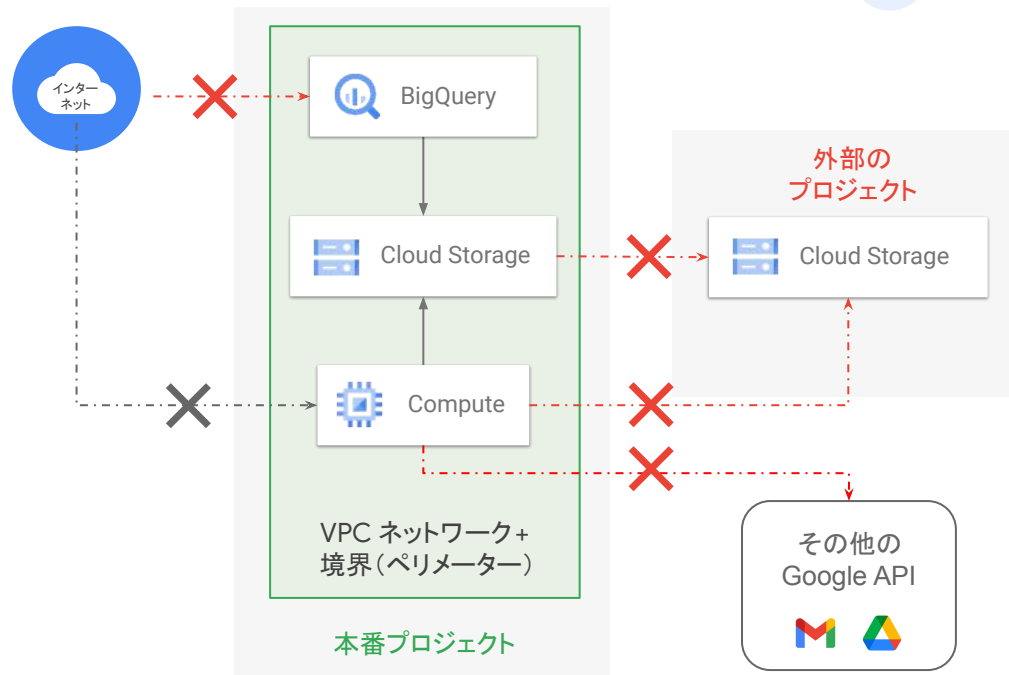
1. 窃取された認証情報による機密データへのアクセス
2. IAM ポリシーの設定誤りによる想定外の共有
3. 内部犯や、危険なコードで不正なクラウド リソースへデータコピー
4. 他の Google API 群へデータ転送



VPC Service Controls による API の保護



- セキュリティ境界を設定
- 境界を越えるデータの移動をブロック
- 境界を越えられる例外の定義も可
- プロジェクトオーナーにも変更不可 (組織レベルでの防御)





まとめ

本日のまとめ



ネットワーキングの基礎

- グローバルな VPC
- リージョナルなサブネット
- グローバルな ルート と ファイアウォール
- 静的ルーティング と 動的ルーティング



特徴的な機能

- 共有 VPC
- サービスと閉域アクセス
- VPC Service Controls



Thank you.

