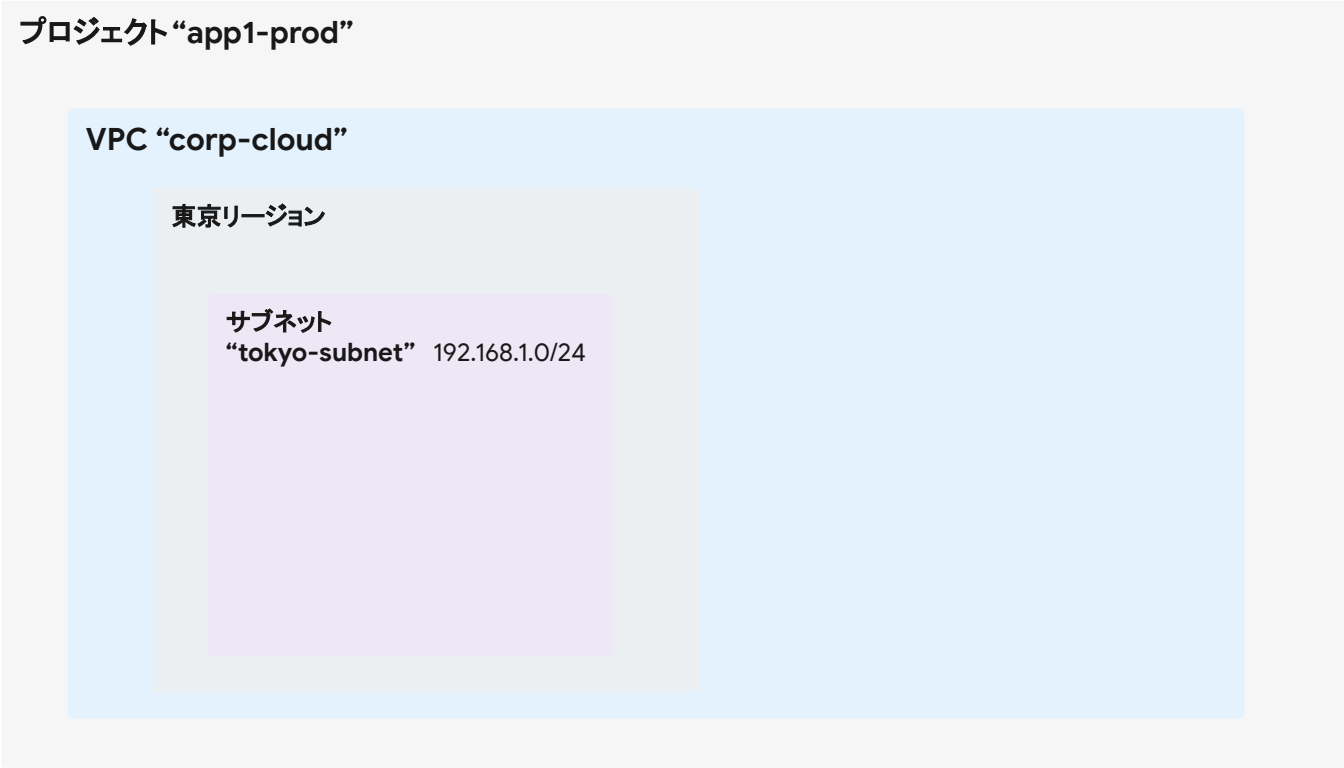
Google Cloud

Google Cloud でセキュアな エンタープライズネットワークを構築

2021 年 7 月

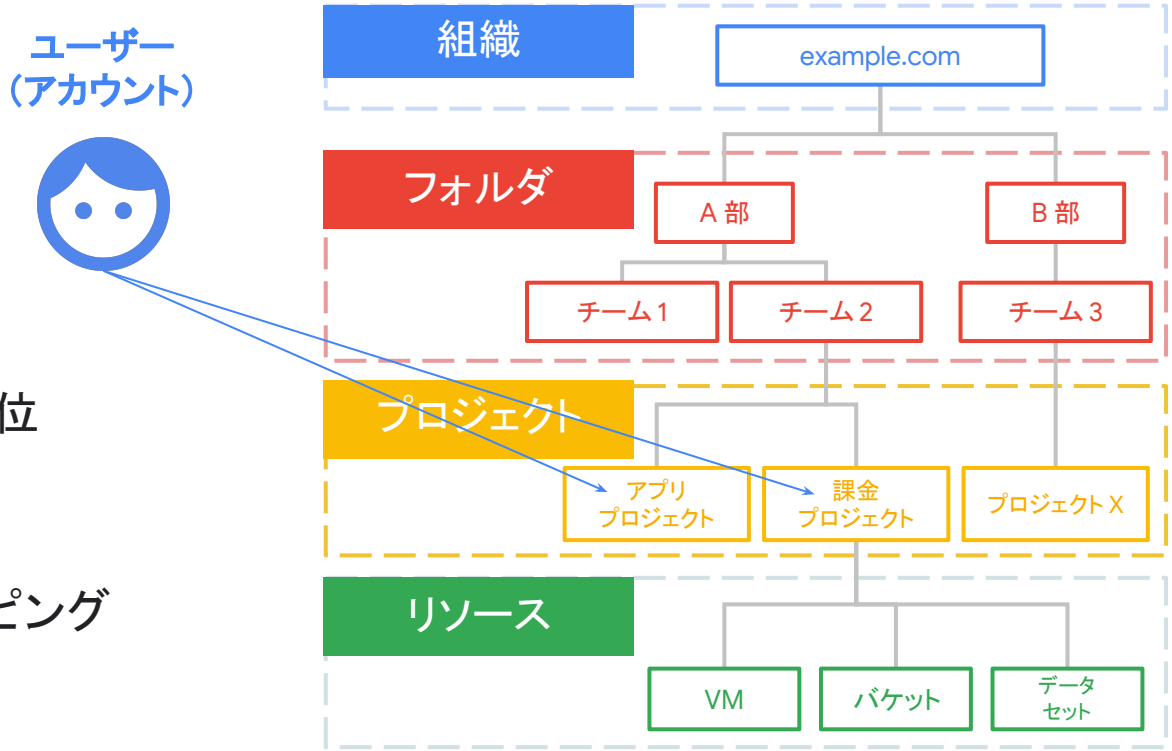
有賀 征爾 (Seiji Ariga)
カスタマーエンジニア

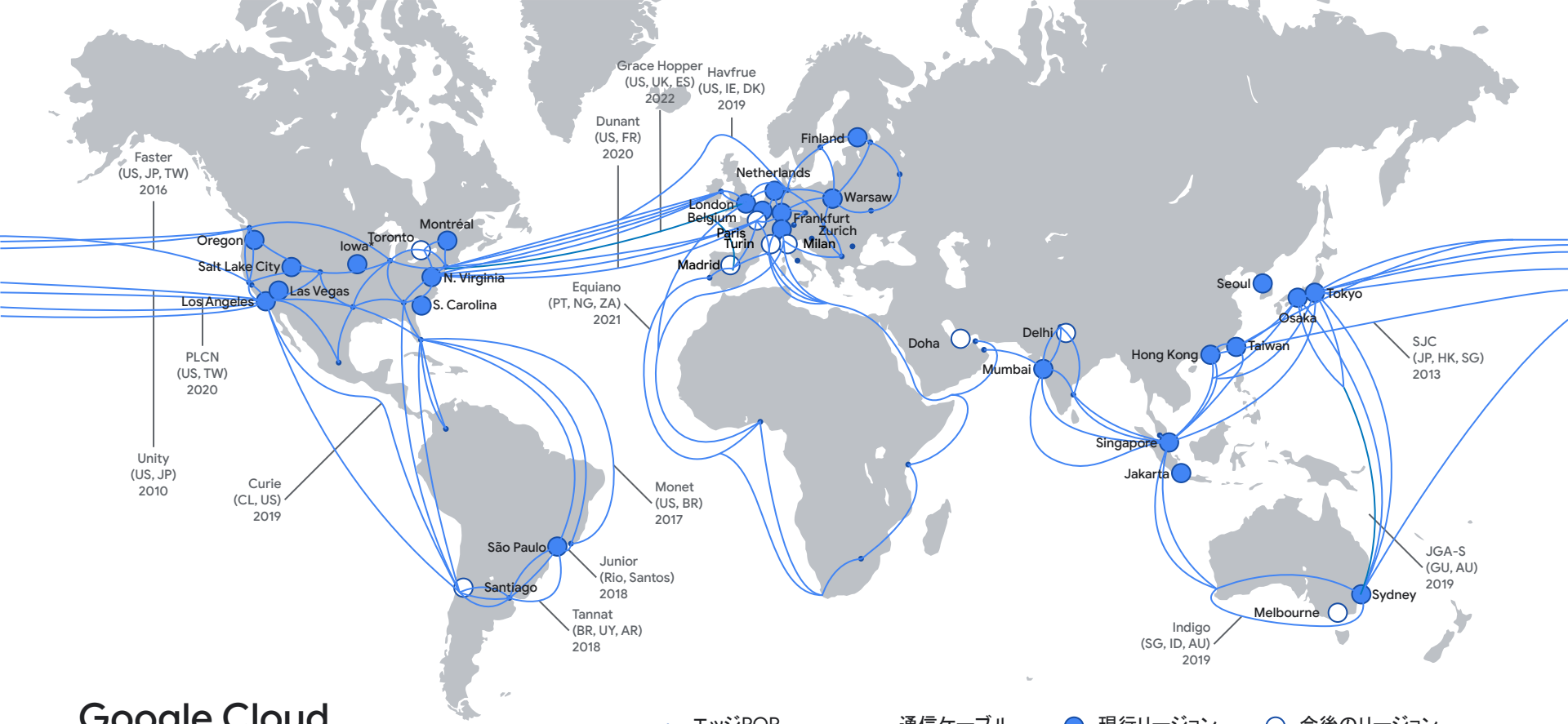
VPC とサブネットの作成



リソース階層

- **組織**
  - ≒ドメイン
- **プロジェクト**
  - リソースをまとめる単位
- **フォルダ**
  - プロジェクトをグルーピング



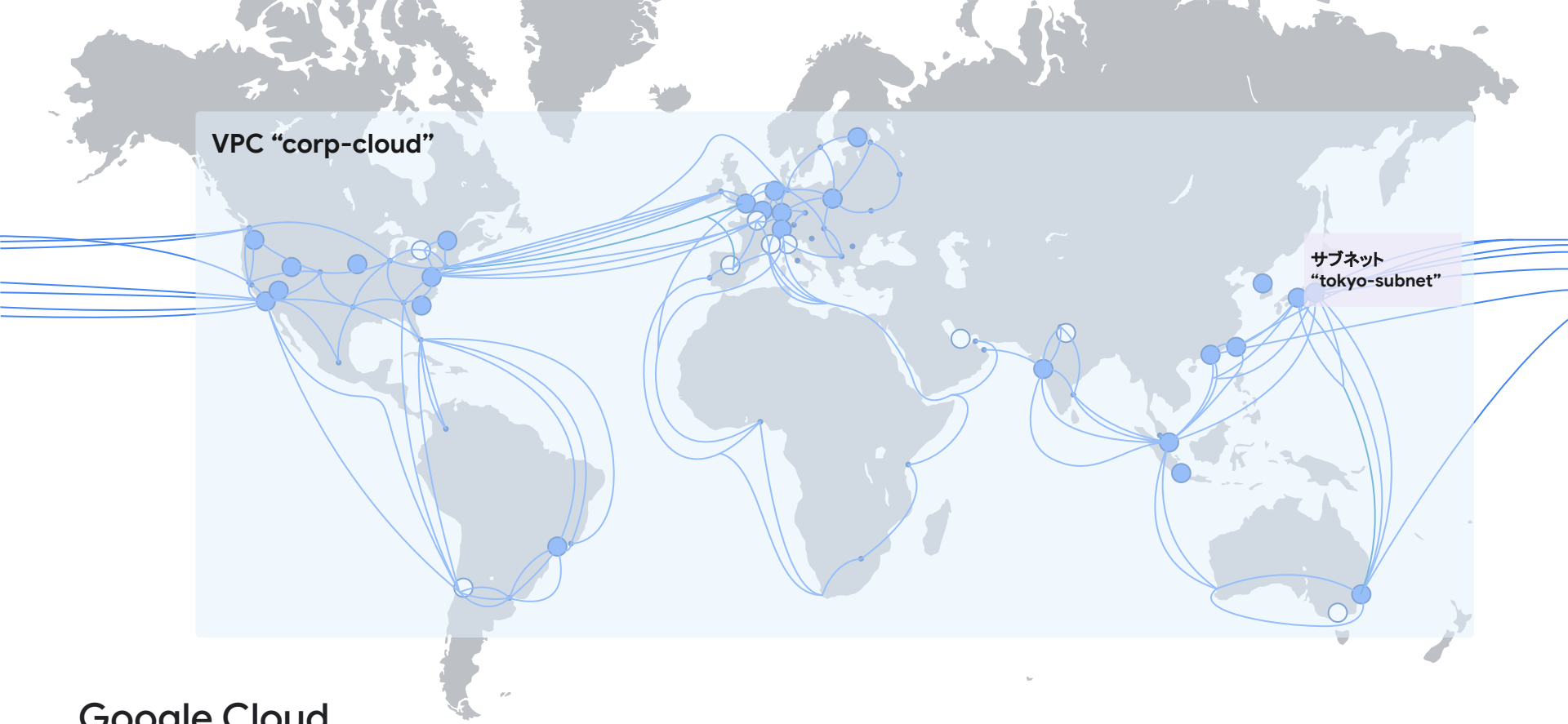


Google Cloud

エッジPOP　通信ケーブル　現行リージョン　今後のリージョン

全世界に展開するネットワークとリージョン

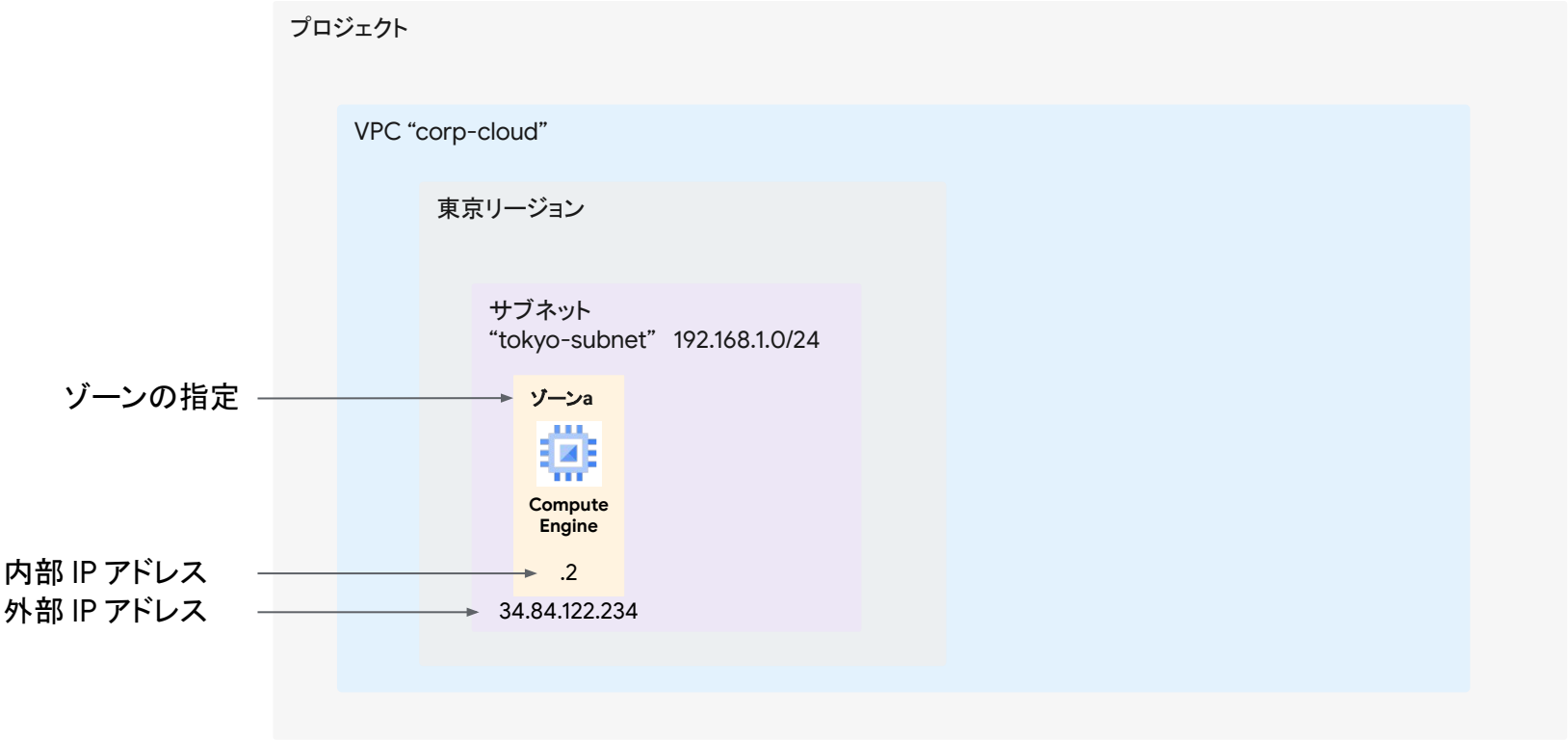
*Exception: region has 4 zones.



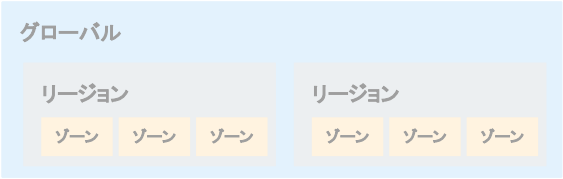
Google Cloud

全世界に展開するネットワークとリージョン

Compute Engine VM の作成



グローバル、リージョン、ゾーン



- **グローバル**
  - 例：VPC、外部HTTP(S)ロードバランサー、ファイアウォールルール
- **リージョン**
  - 地理的なロケーション
  - 例：Cloud Storage バケット、リージョン永続ディスク（Regional PD）
- **ゾーン**
  - インフラストラクチャの分離
  - 例：ゾーンクラスタ（GKE）、ゾーン永続ディスク（Zonal PD）

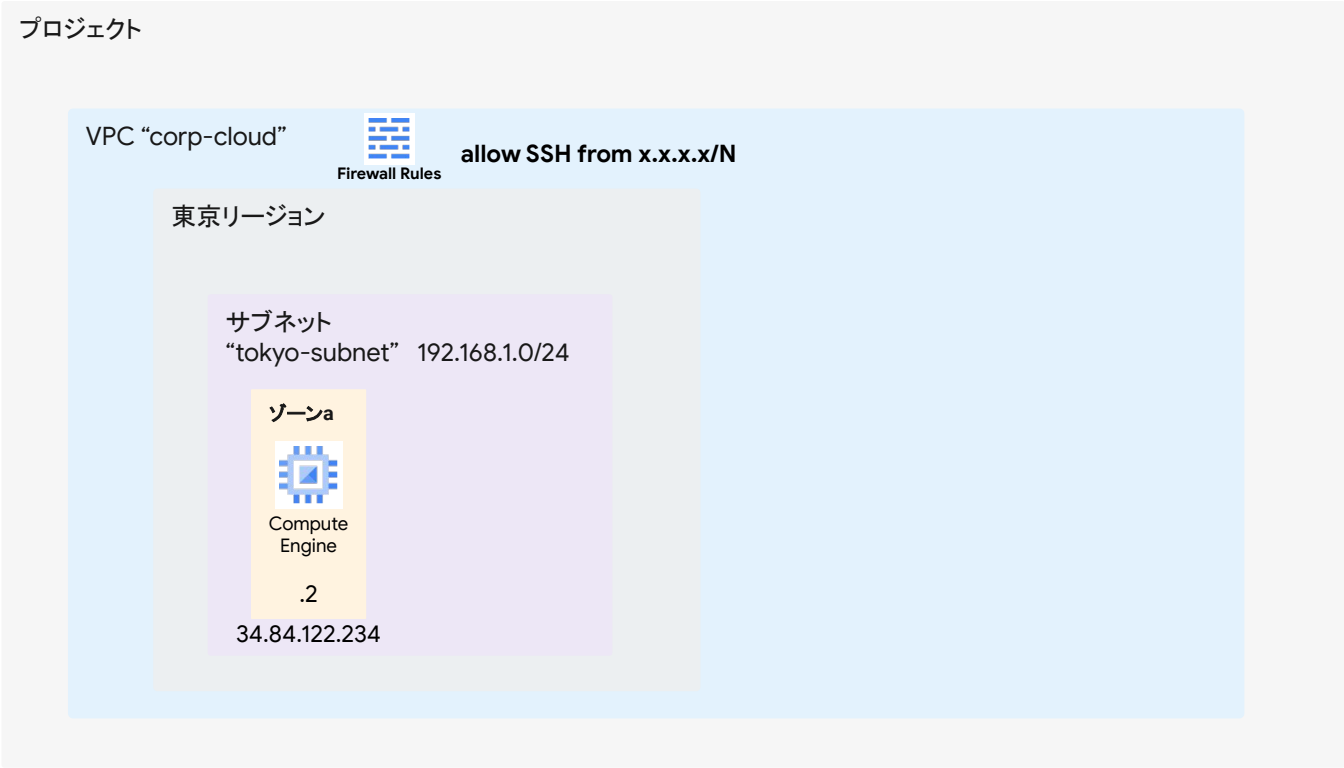
外部 IP アドレス、内部 IP アドレス

- **外部 IP アドレス**
  - インターネットとの通信に利用
  - お客さま所有 IP アドレスを持ち込むことも可能（BYOIP: Bring Your Own IP）

- **内部 IP アドレス**
  - VPC ネットワーク内（とオンプレミス）の通信に利用
  - RFC 1918 (例 10.1.2.0/24)や、パブリック IP アドレスも使用できます

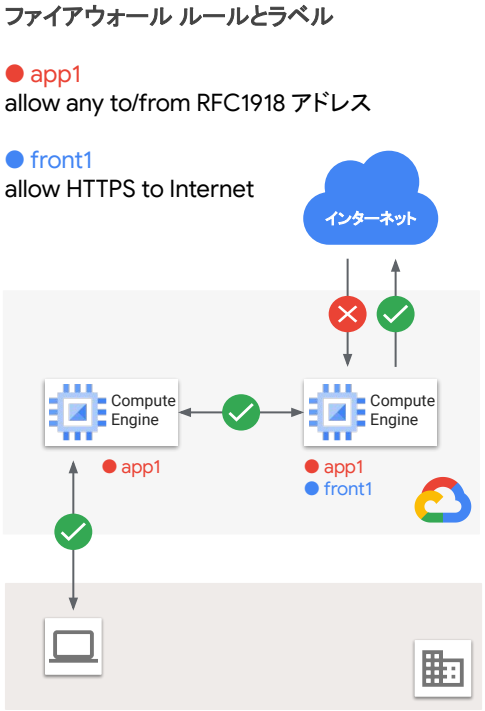
- 種別
  - リージョン、グローバル
  - エフェメラル（動的、一時的）、静的

ファイアウォール ルールの追加

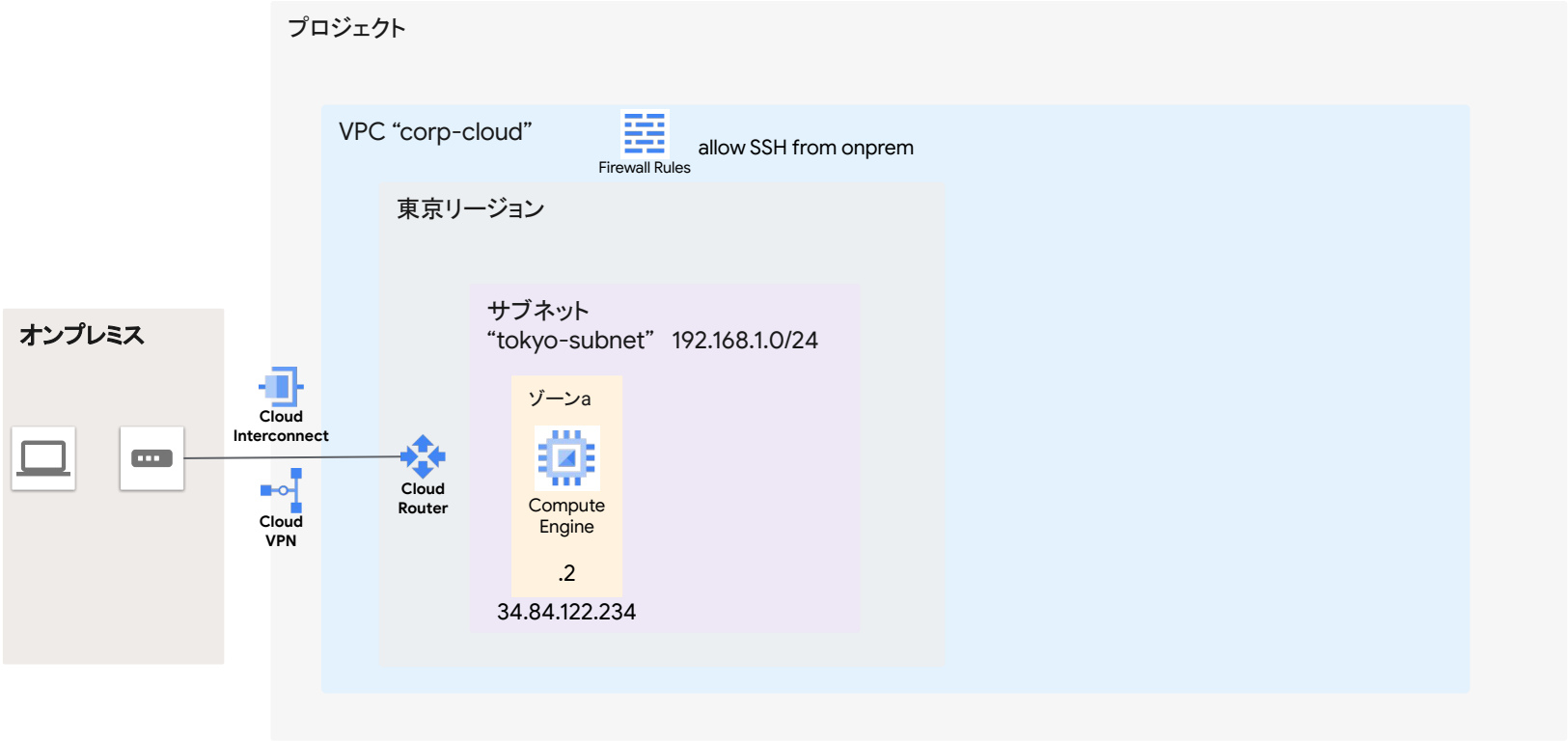


VPC ファイアウォール ルール

- 外向き・内向きのルール
- ステートフル
  （コネクショントラッキング）
- ホストベースの分散実装
  （単一のボトルネック無し）
- ラベルによる適用
  - ネットワークタグ
  - サービスアカウント

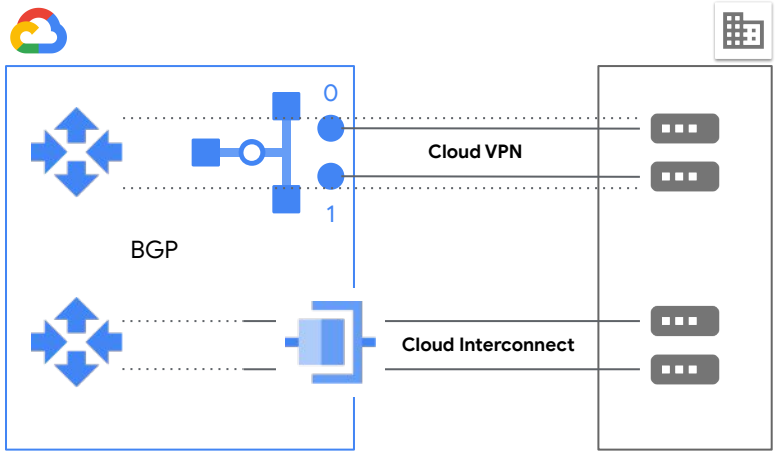


オンプレミスとの閉域接続



ハイブリッドネットワーキング

- **Cloud VPN**
  - サイト間 IPsec VPN
  - HA 構成（SLA 99.99%）
- **Cloud Interconnect**
  - 専用線接続（10 Gbps、100 Gbps）
  - 直接（Dedicated Interconnect）
  - パートナー経由（Partner Interconnect）
- **Cloud Router**
  - BGP で経路交換を行うソフトウェアタスク

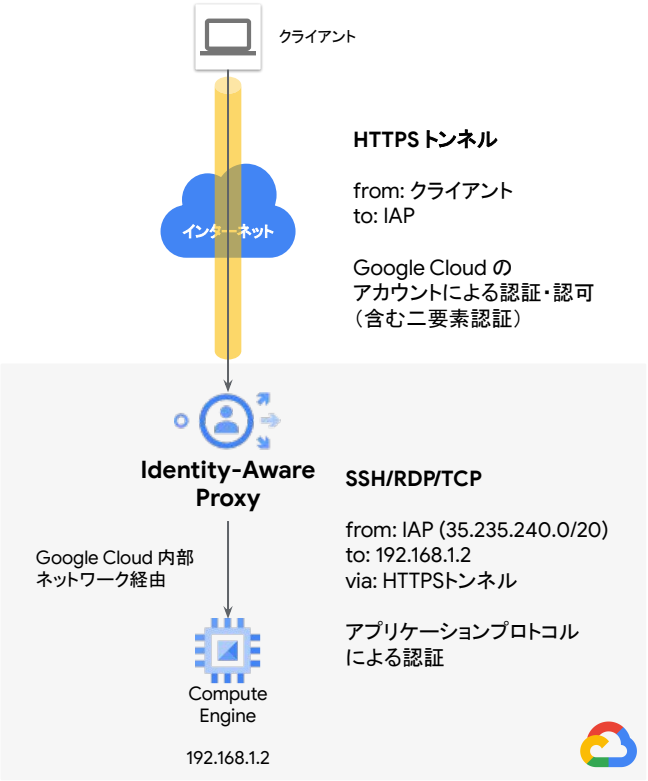


通常、冗長化された
オンプレミス ルータ
と接続

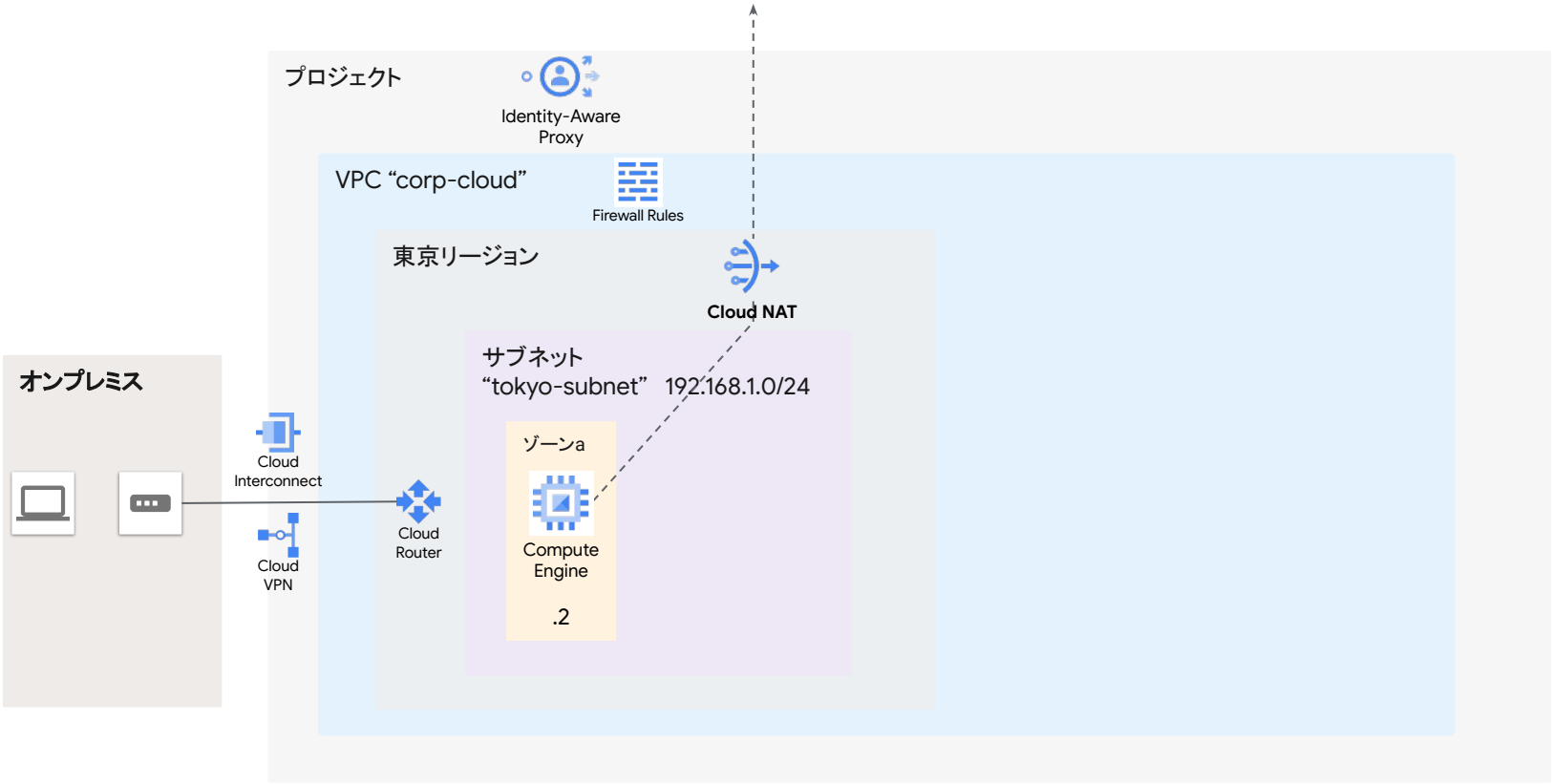
外部 IP アドレスの削除

Identity-Aware Proxy の TCP 転送による安全な接続

- **Identity-Aware Proxy**
  - HTTPS によるアクセスの一元的な承認レイヤ
  - アプリから独立したアクセス制御
- **TCP 転送**
  - IAP を経由した TCP over HTTPSトンネル
  - 接続先に外部 IP アドレスは不要
  - Google Cloud ネットワークのみを経由

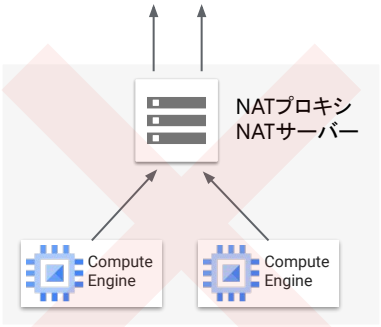


Cloud NAT による外部接続

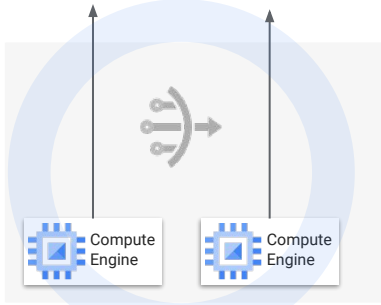


Cloud NAT

- VM に外部 IP アドレス無しで外部接続
- ホストベースの NAT
  - 単一のボトルネックなし
  - ハイパフォーマンス
- 柔軟な設定
  - スケーリング
  - タイムアウト
  - NAT 対象
  - NAT 方式

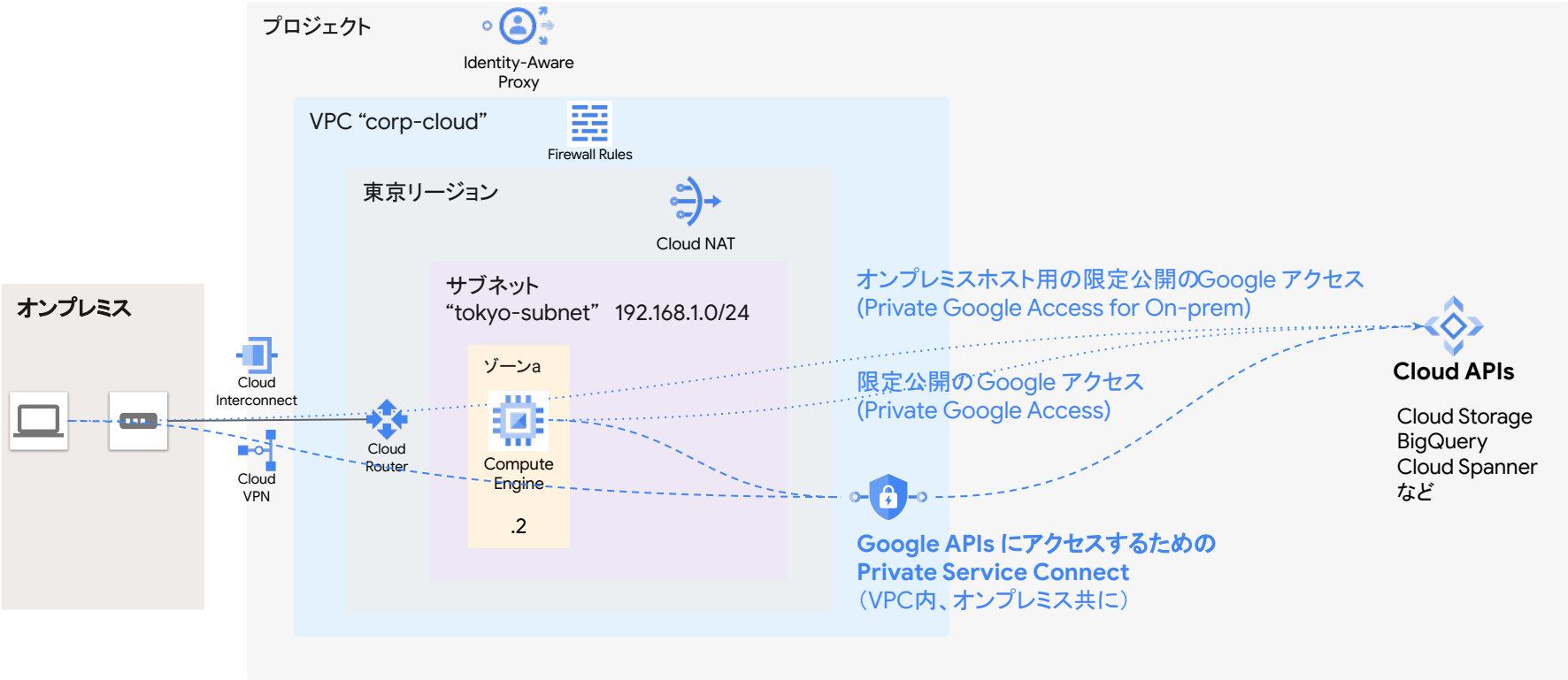


NATプロキシ/サーバーで
NATを実施



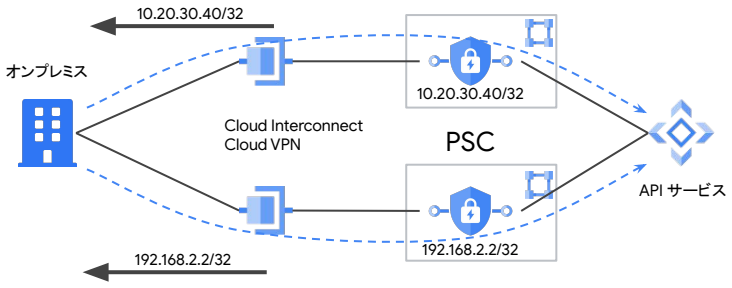
インスタンスのある
各ホストでNATを実施

Google Cloud APIs への閉域網でのアクセス

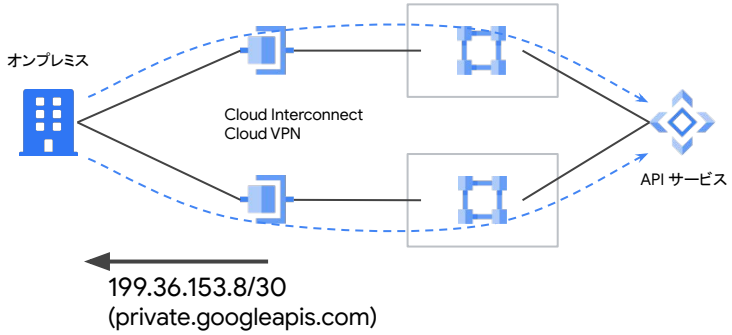


Cloud APIs に閉域網でアクセスする 2 つの方法

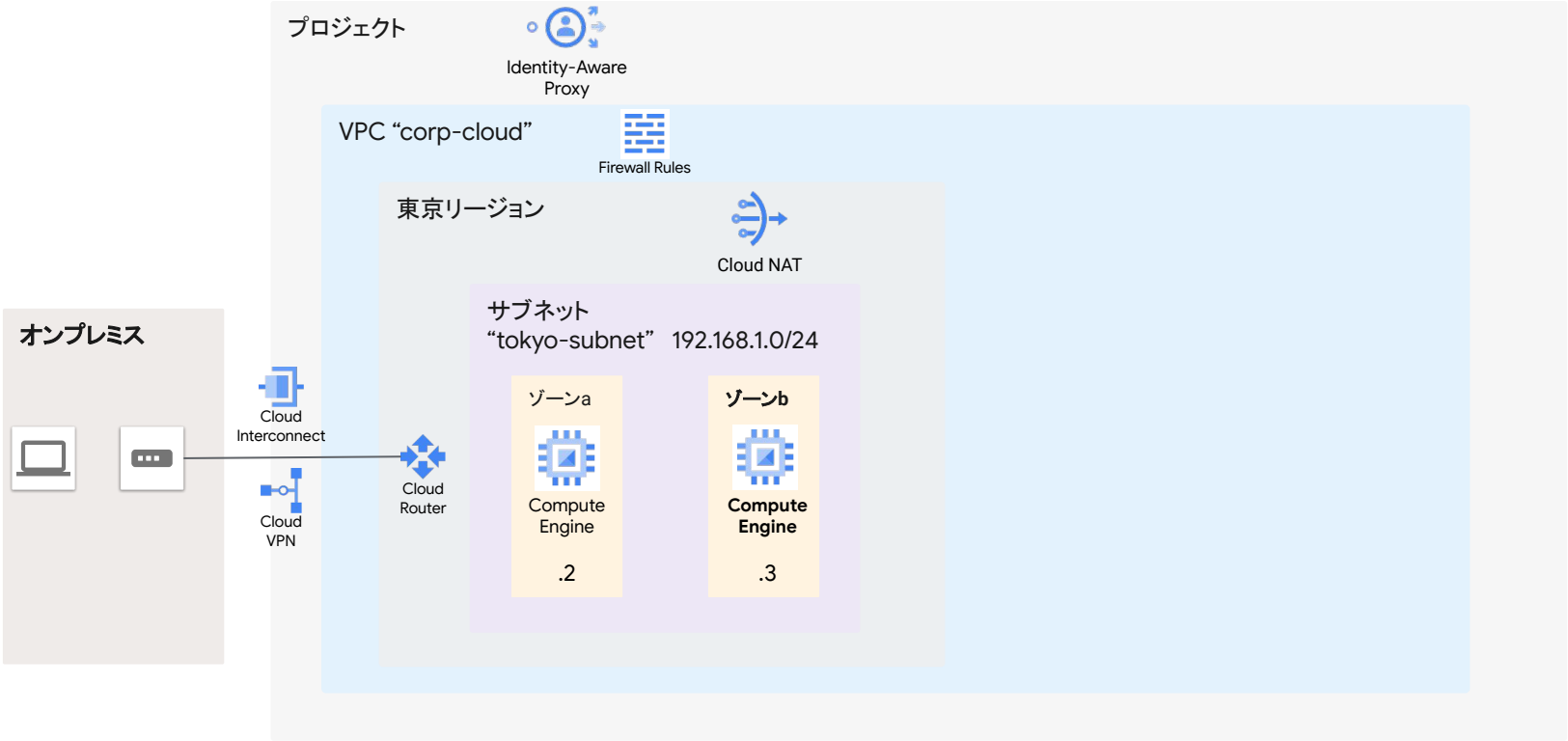
- Private Service Connect NEW
  - VPC 内に作成したエンドポイント経由でアクセス



- （オンプレミスホスト用の）限定公開の Google アクセス OLD
  - 既定のエンドポイント経由でアクセス



複数ゾーンの利用による冗長化



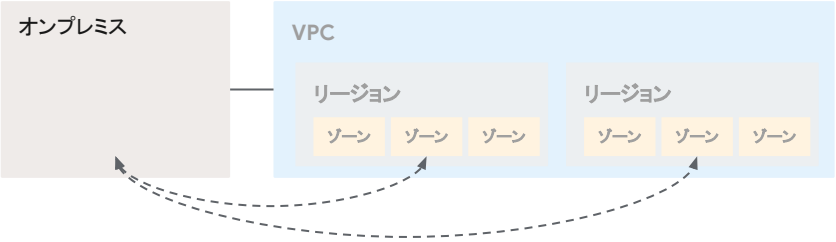
ゾーン冗長

- ゾーン間は低遅延（地理的に近距離）
- サブネットはリージョンリソース
  - 同一のサブネットをゾーン間で利用可能
- 経路情報（ルート）もゾーン間で共用
  - オンプレミスとの通信に追加の設定は不要
- ファイアウォール ルールや Cloud NAT も共用

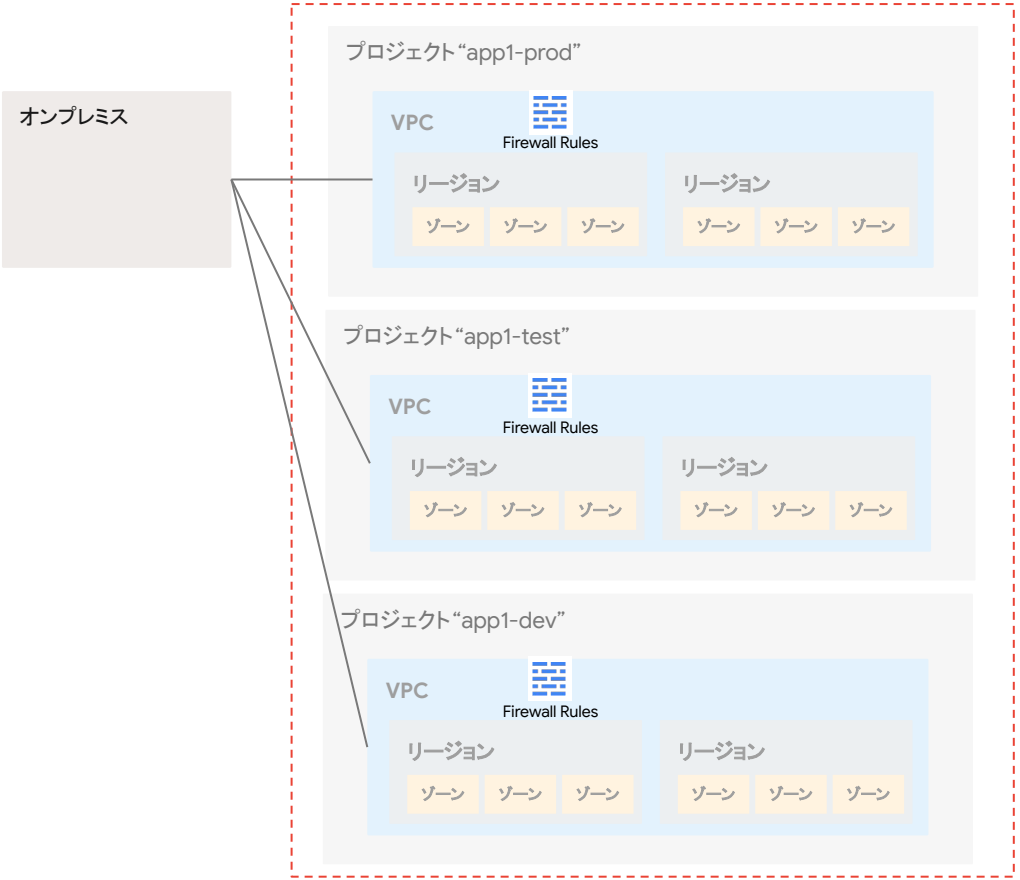
複数リージョンの利用による冗長化

リージョン冗長

- リージョンは地理的に分散
  - 距離なりの遅延は発生（具体的な値は google cloud "inter-region latency" で検索）
- サブネットのアドレスは自由に設定可能
  - 「同一 CIDR 内」といった制限は無し
- 経路情報はリージョン間で伝播可能
  - VPC のルーティングモードを「グローバル」に設定
  - オンプレミスとの通信も簡単にマルチリージョンで実現



階層型ファイアウォールポリシーによる組織単位のアクセス管理

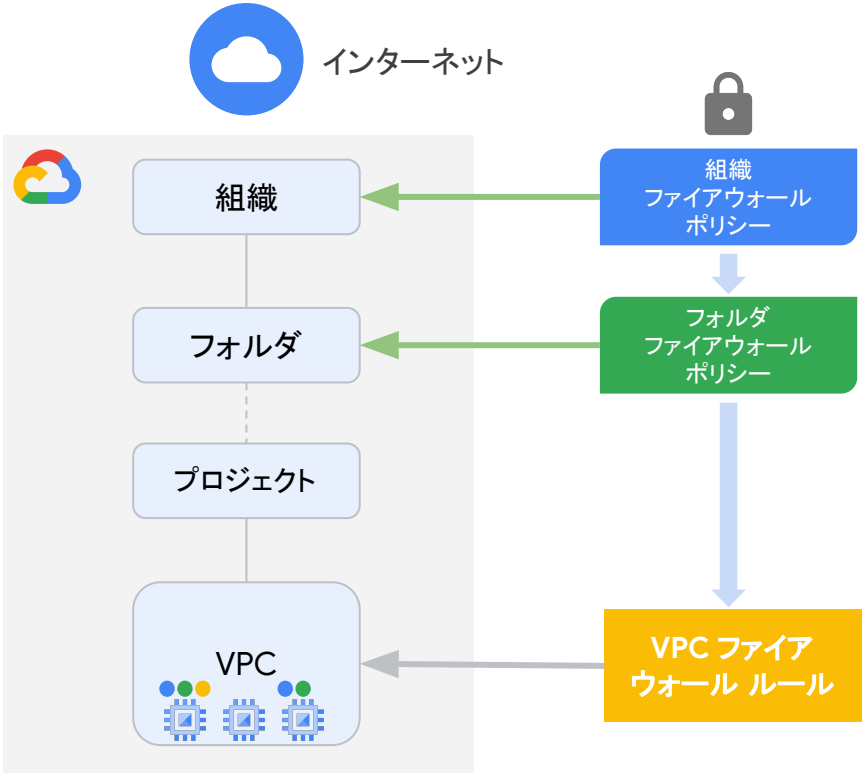


階層型
ファイアウォールポリシー

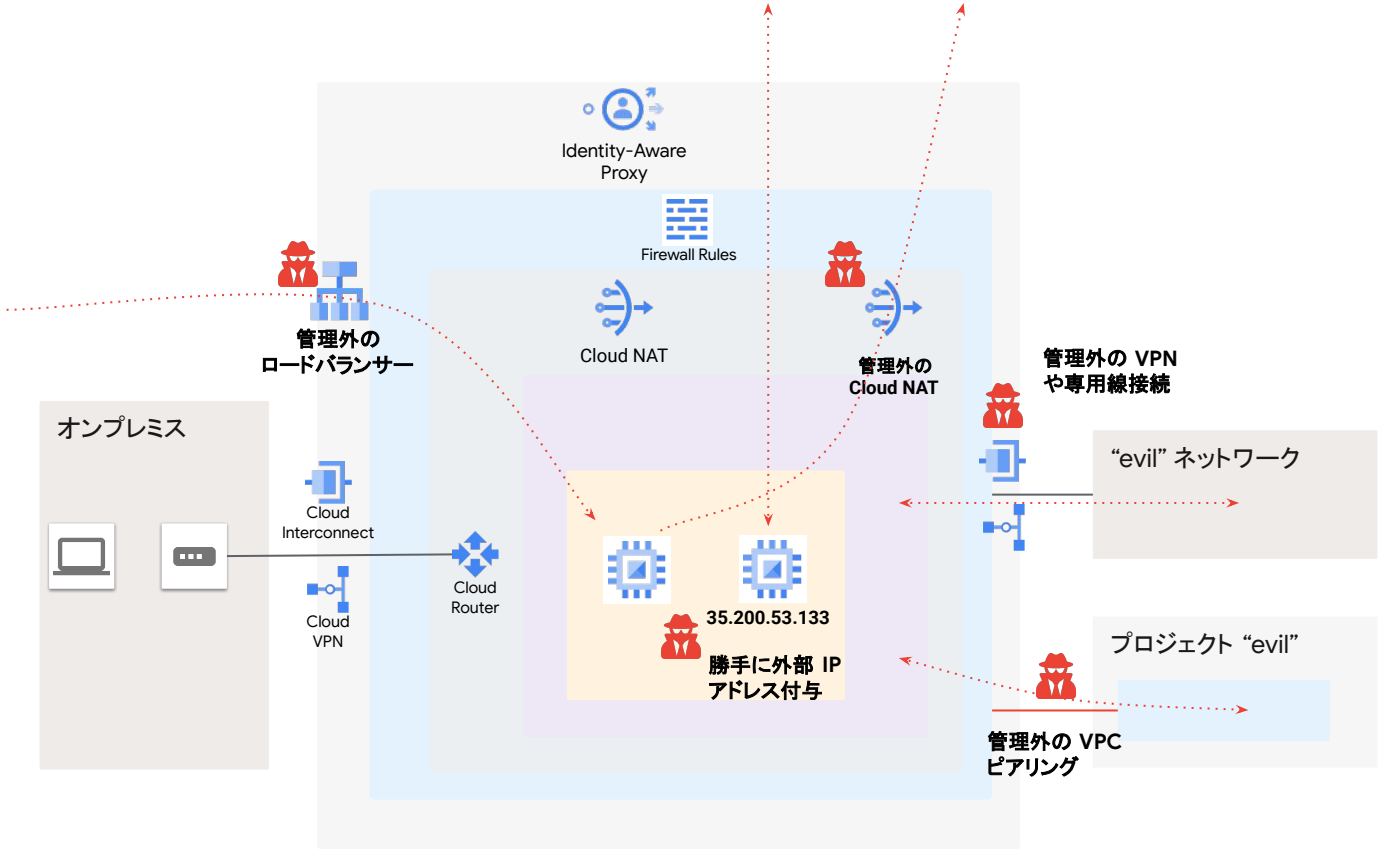
SSH from x.x.x.x/N allow
any from オンプレミス goto_next
MySQL from any deny

階層型ファイアウォール ポリシー

- 複数のファイアウォール ポリシーを組織、フォルダ単位で管理
- 新規プロジェクト、ネットワークにも自動的な防御を提供
- 権限の移譲による柔軟な構成をサポート
  - 詳細な設定はプロジェクトで

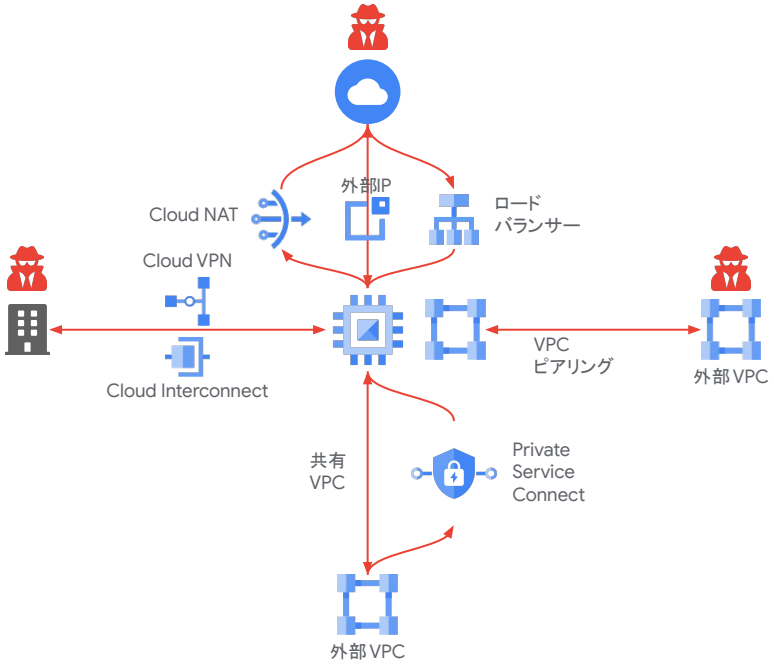


外部接続の厳密な管理

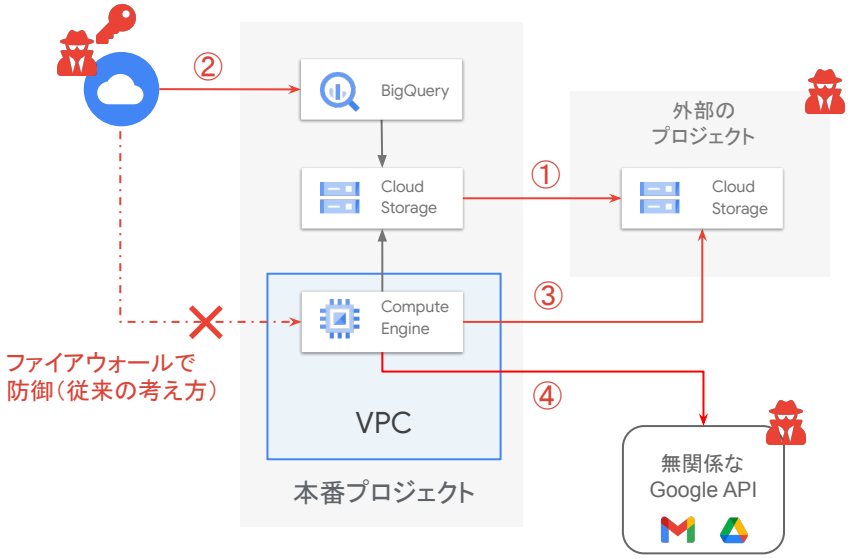

Identity-Aware Proxy
Firewall Rules
管理外の ロードバランサー
Cloud NAT
管理外の Cloud NAT
管理外の VPN や専用線接続
オンプレミス
Cloud Interconnect
Cloud VPN
Cloud Router
35.200.53.133
勝手に外部 IP アドレス付与
“evil” ネットワーク
プロジェクト “evil”
管理外の VPC ピアリング

組織ポリシーの制約

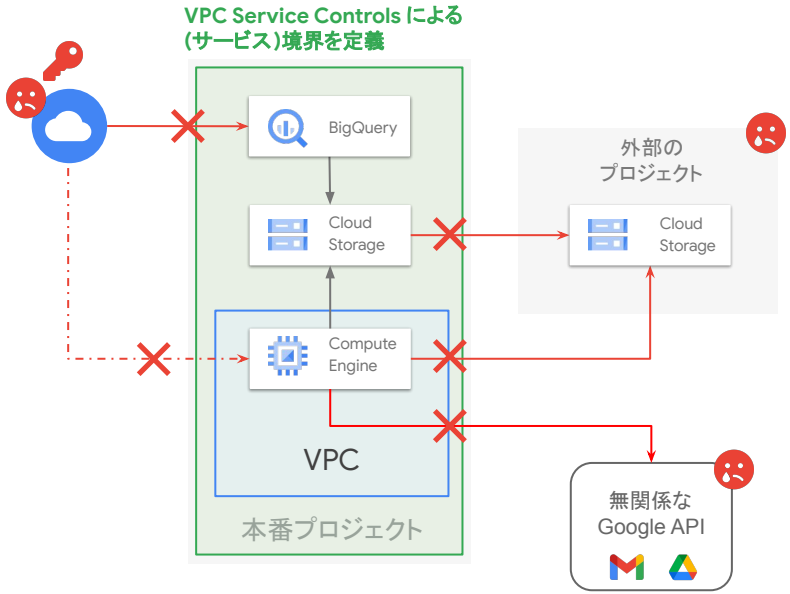
- リソースに対する組織、フォルダ、プロジェクト単位の制約
- リストとブール値による制約
  - 許可値、拒否値のリスト
  - 特定の動作の可否（ブール）
- ネットワークリソースに対する制約
  - 外部 IP アドレスの利用制限
  - Cloud Interconnect / Cloud VPN の接続先の制限
  - 共有 VPC の接続先の制限
  - IP 転送の利用制限
  - Cloud NAT の利用制限
  - Cloud Load Balancing の利用制限
  - Protocol Forwarding の利用制限
  - VPC ピアリングの接続相手制限
  - Private Service Connect の利用制限



VPC Service Controls による API サービスの保護



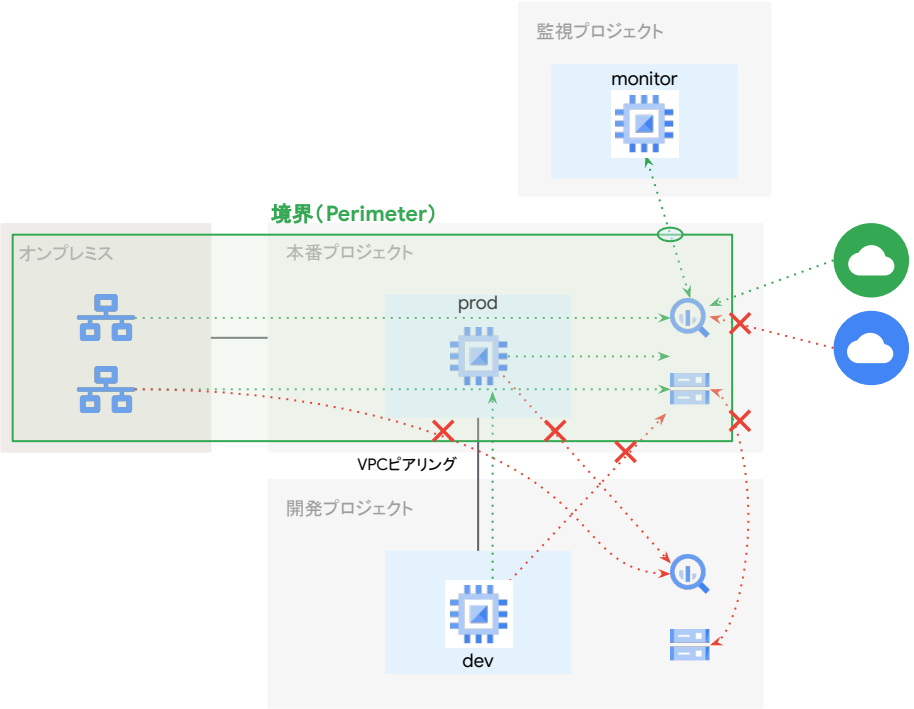
1. バケットポリシーの誤設定で公開・共有
2. 盗まれた認証情報でインターネットからアクセス
3. 内部犯やバグで外部リソースへデータをコピー
4. 内部犯やバグで他のGoogle API 群へデータをコピー



- 「境界」(Perimeter)を定義
- 境界内で管理するAPI を指定
- 境界をまたぐアクセスをコントロール
- 組織単位で管理

VPC Service Controls

- 境界をまたぐ API アクセスを管理
  - API アクセス以外は従来通り
    ファイアウォールで管理
- 閉域接続されたオンプレミスも境界内として扱われる
  - オンプレミスの一部だけ、
    といった区別は不可
- 特定の IP アドレスからのアクセスだけ許可することも可能
- 特定のプロジェクト(から|へ)の
  アクセスを一部許可することも可能



本日のまとめ

セキュアなネットワークを段階的に構築

01 | **外部との接続を適切に管理する**

02 | **組織、フォルダを活用し、一元的なアクセス管理を実現**

03 | **API サービス(へ|から)のアクセスも忘れずに**

Thank you.