

セキュアなハイブリッド クラウド ネットワーク 設計パターンの最新版



Tokyo

Proprietary

守屋 裕樹

Google Cloud
クラウド コンサルタント



有賀 征爾

Google Cloud
カスタマー エンジニア



アジェンダ

- 01 ハイブリッド接続
- 02 ネットワークセキュリティ
- 03 まとめ

01. ハイブリッド接続

パターン別ハイブリッド接続環境の構成

- 接続アーキテクチャ
- 名前解決

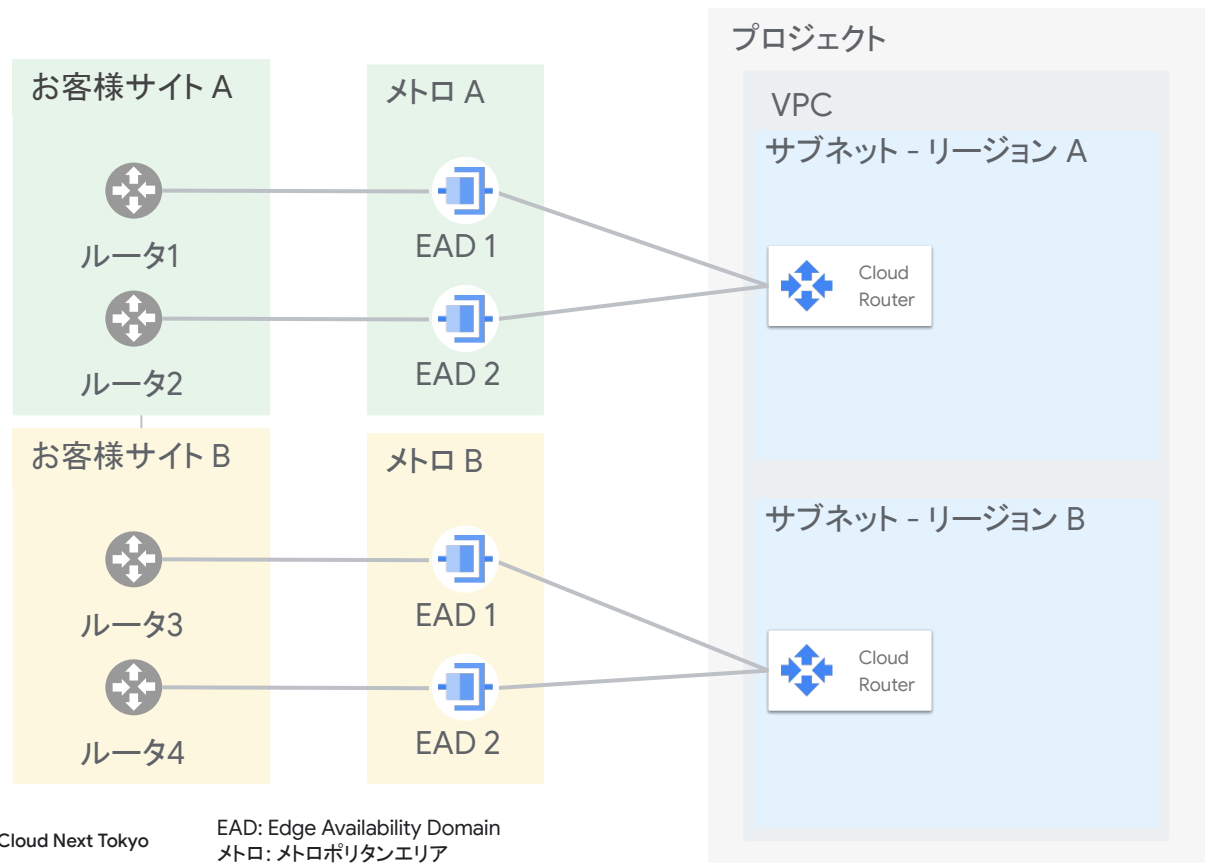
ハイブリッド接続パターン

- シングル VPC 接続
- マルチ VPC 接続
- フルメッシュ接続
- スタートポロジ接続

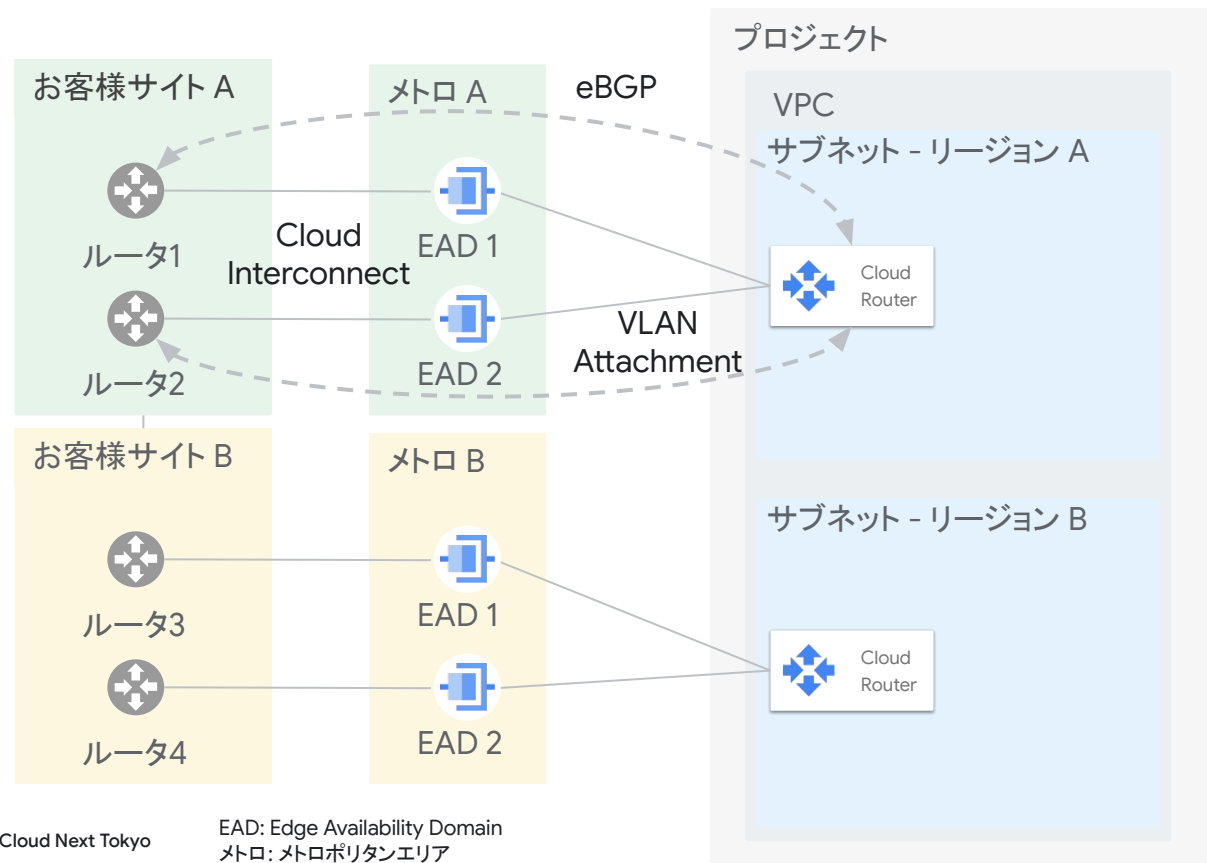
シングル VPC 接続 - ユースケース例

- オンプレミスと単一の VPC を接続したい
- 接続した VPC を複数のプロジェクトで使いたい

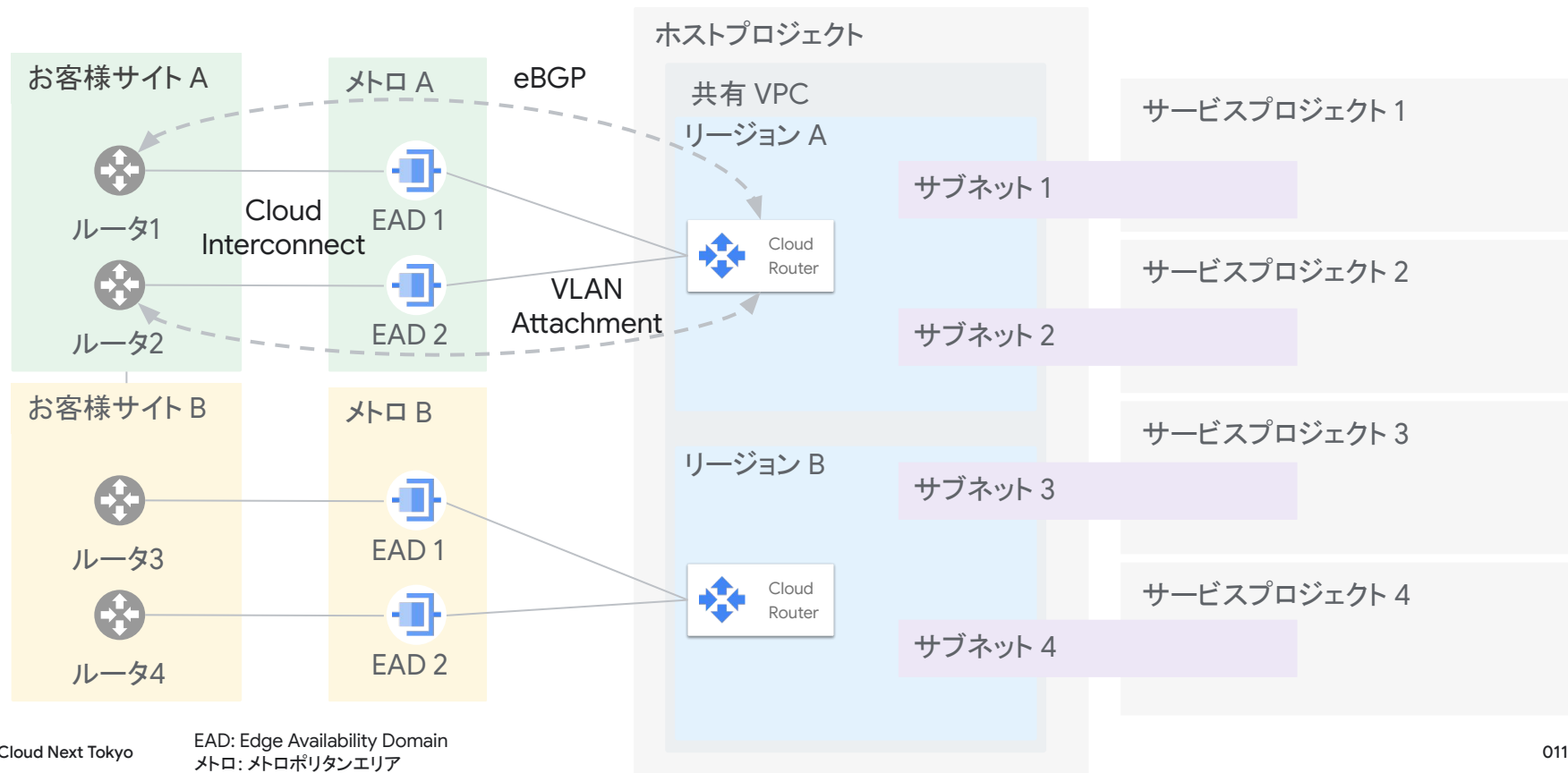
シングル VPC 接続 - アーキテクチャ



シングル VPC 接続 - アーキテクチャ

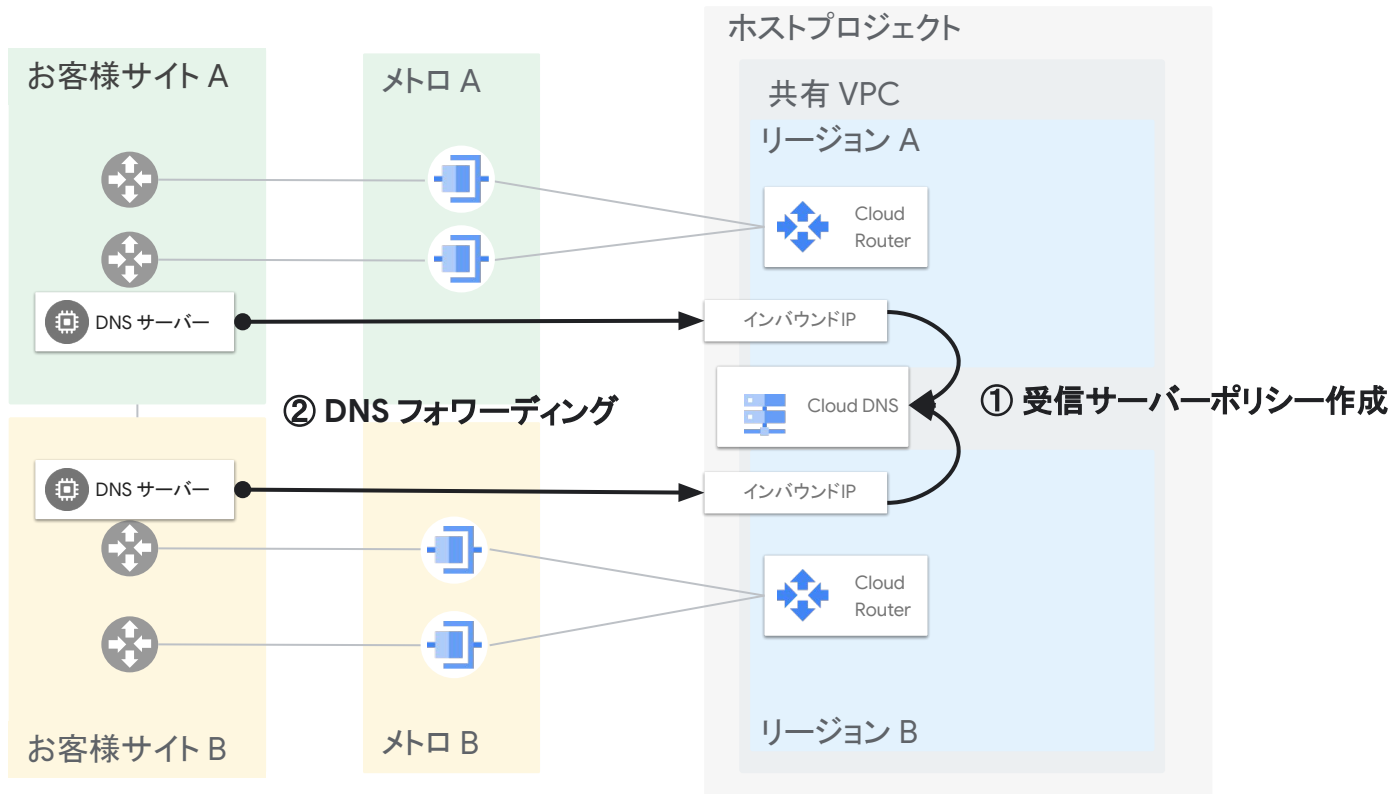


シングル VPC 接続 - アーキテクチャ



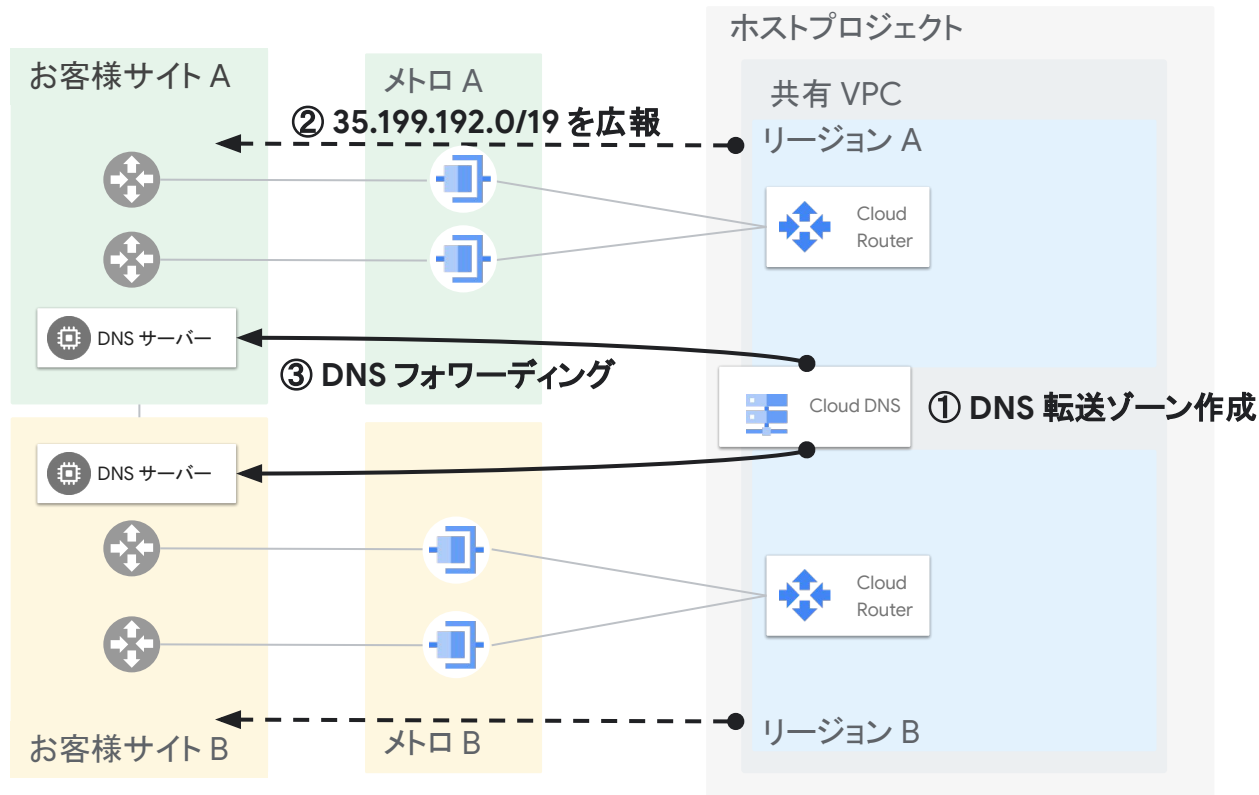
シングル VPC 接続 - ハイブリッド名前解決

オンプレミス DNS サーバーから Cloud DNS



シングル VPC 接続 - ハイブリッド名前解決

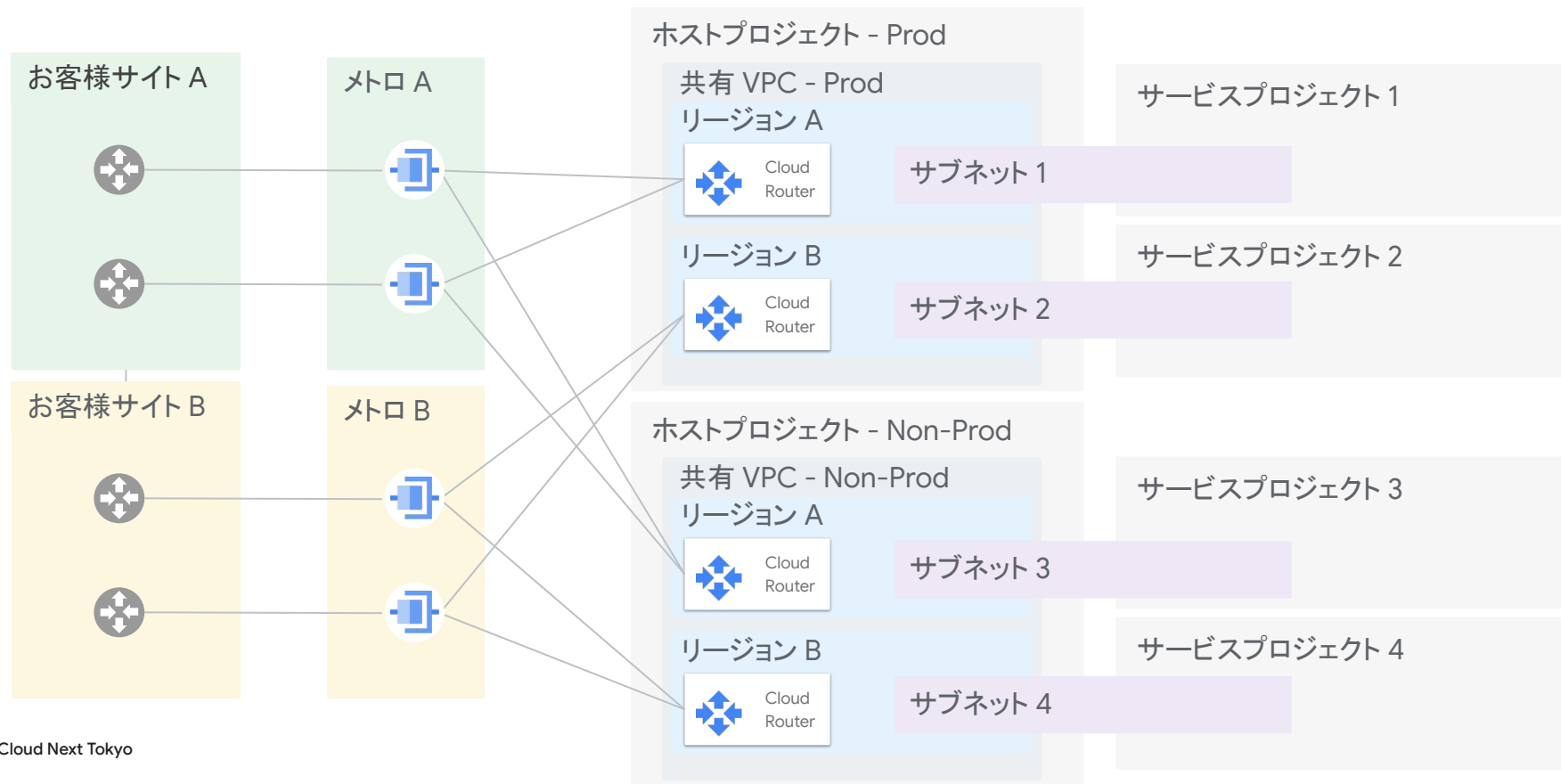
Cloud DNS からオンプレミス DNS サーバー



マルチ VPC 接続 - ユースケース例

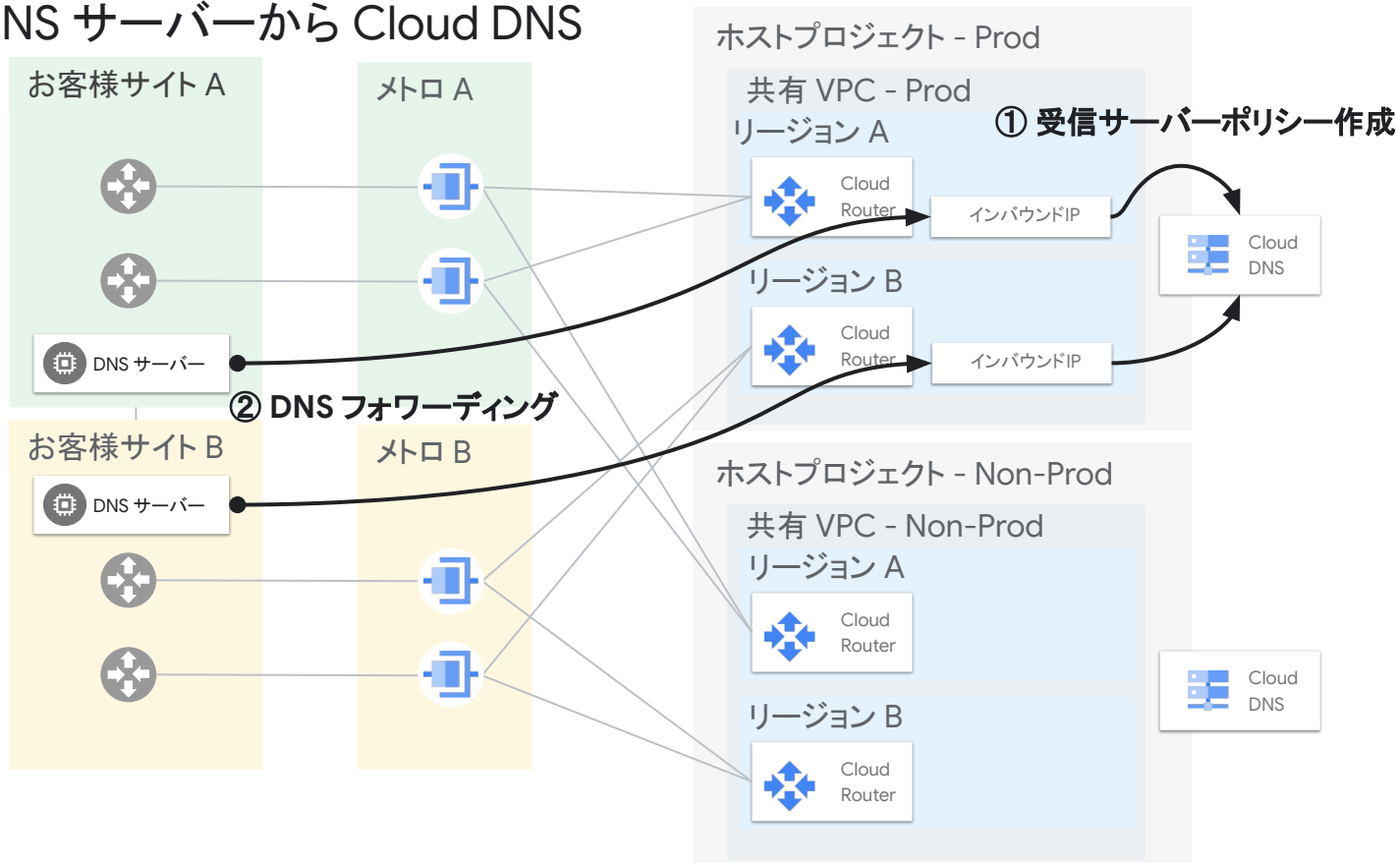
- オンプレミスと複数の VPC 環境を接続させたい
 - 本番環境と開発環境 VPC など
- 単一の接続を複数の VPC で共有したい

マルチ VPC 接続 - アーキテクチャ



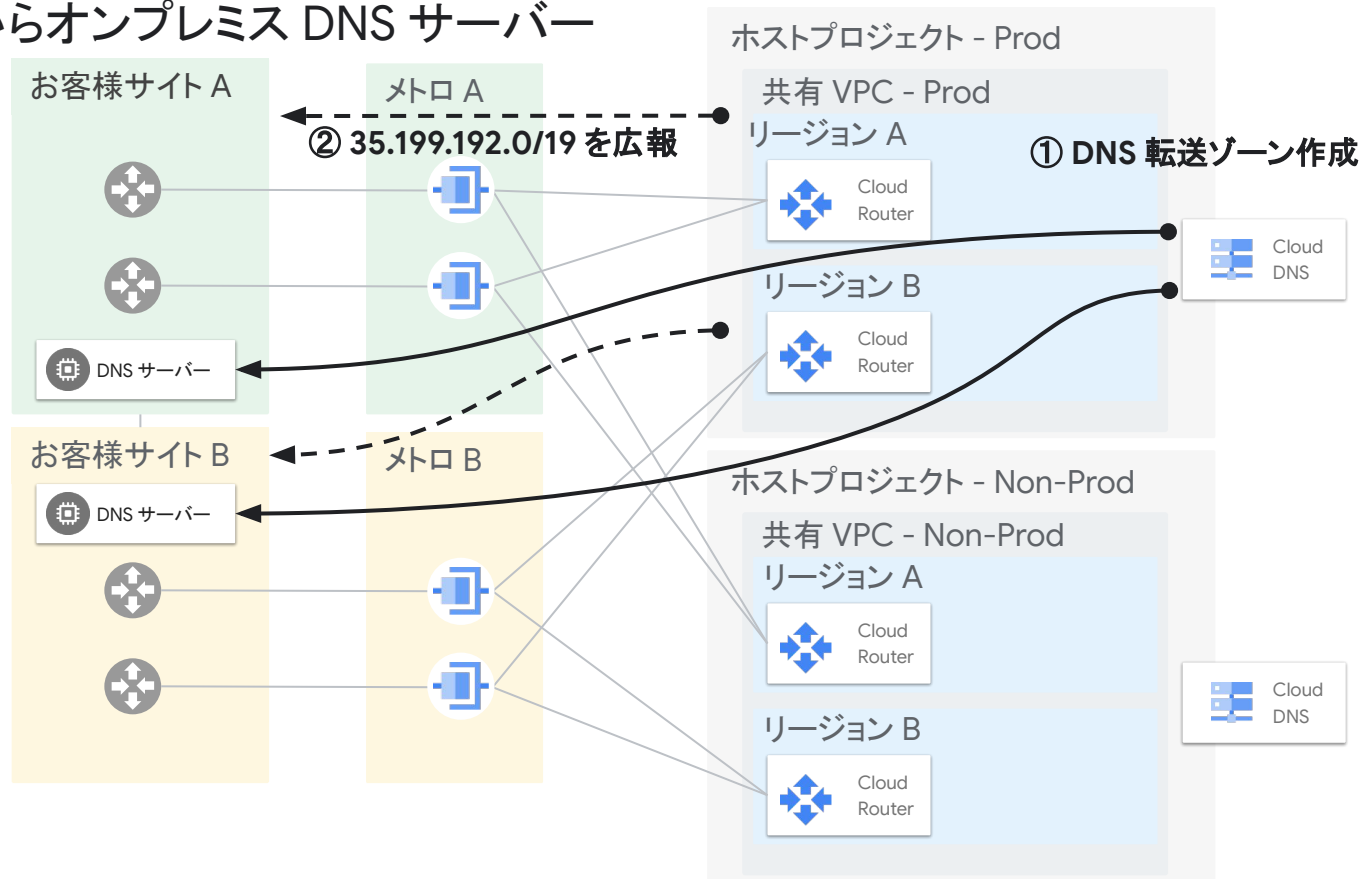
マルチ VPC 接続 - ハイブリッド名前解決

オンプレミス DNS サーバーから Cloud DNS



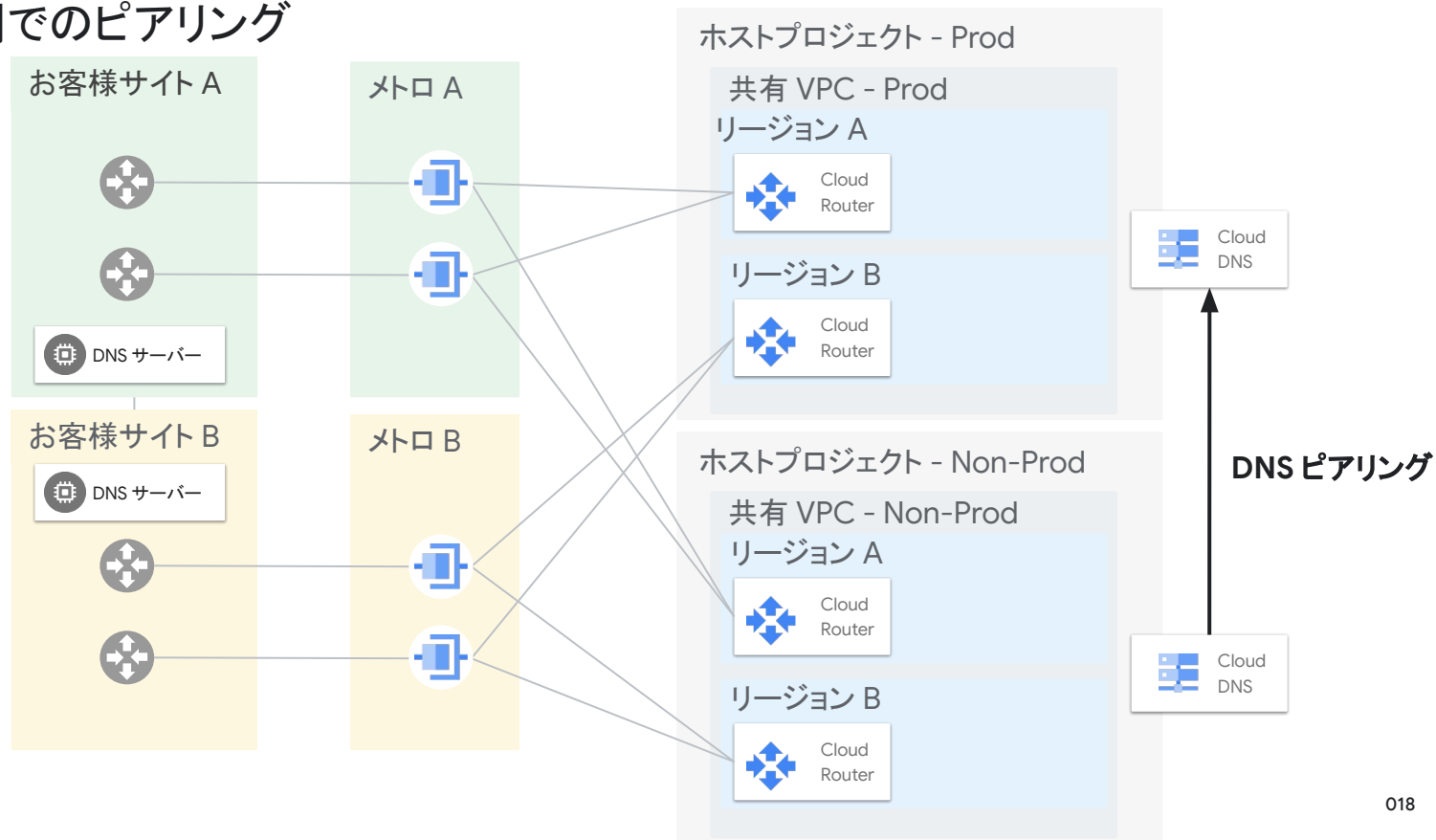
マルチ VPC 接続 - ハイブリッド名前解決

Cloud DNS からオンプレミス DNS サーバー



マルチ VPC 接続 - ハイブリッド名前解決

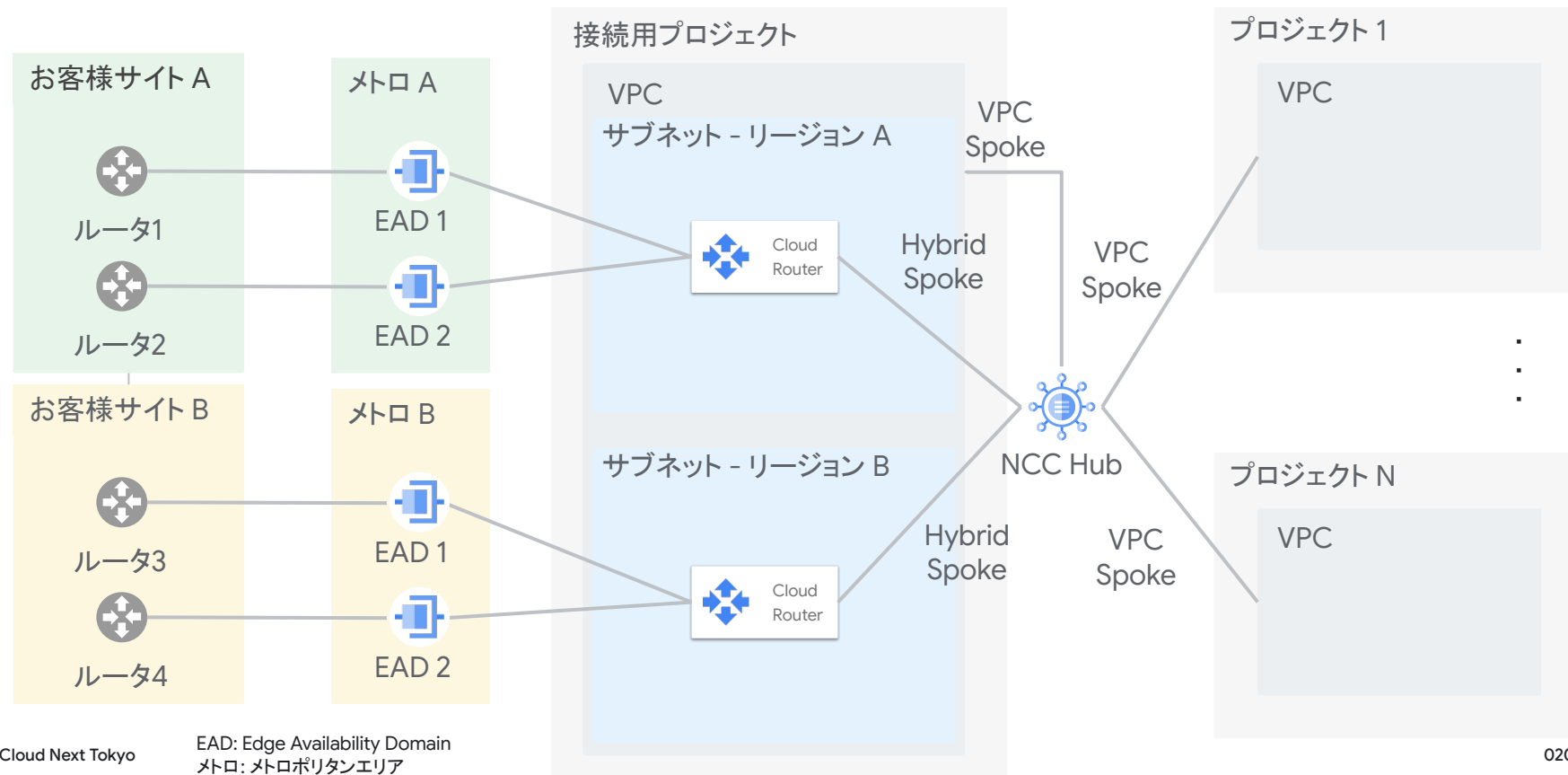
Cloud DNS 間でのピアリング



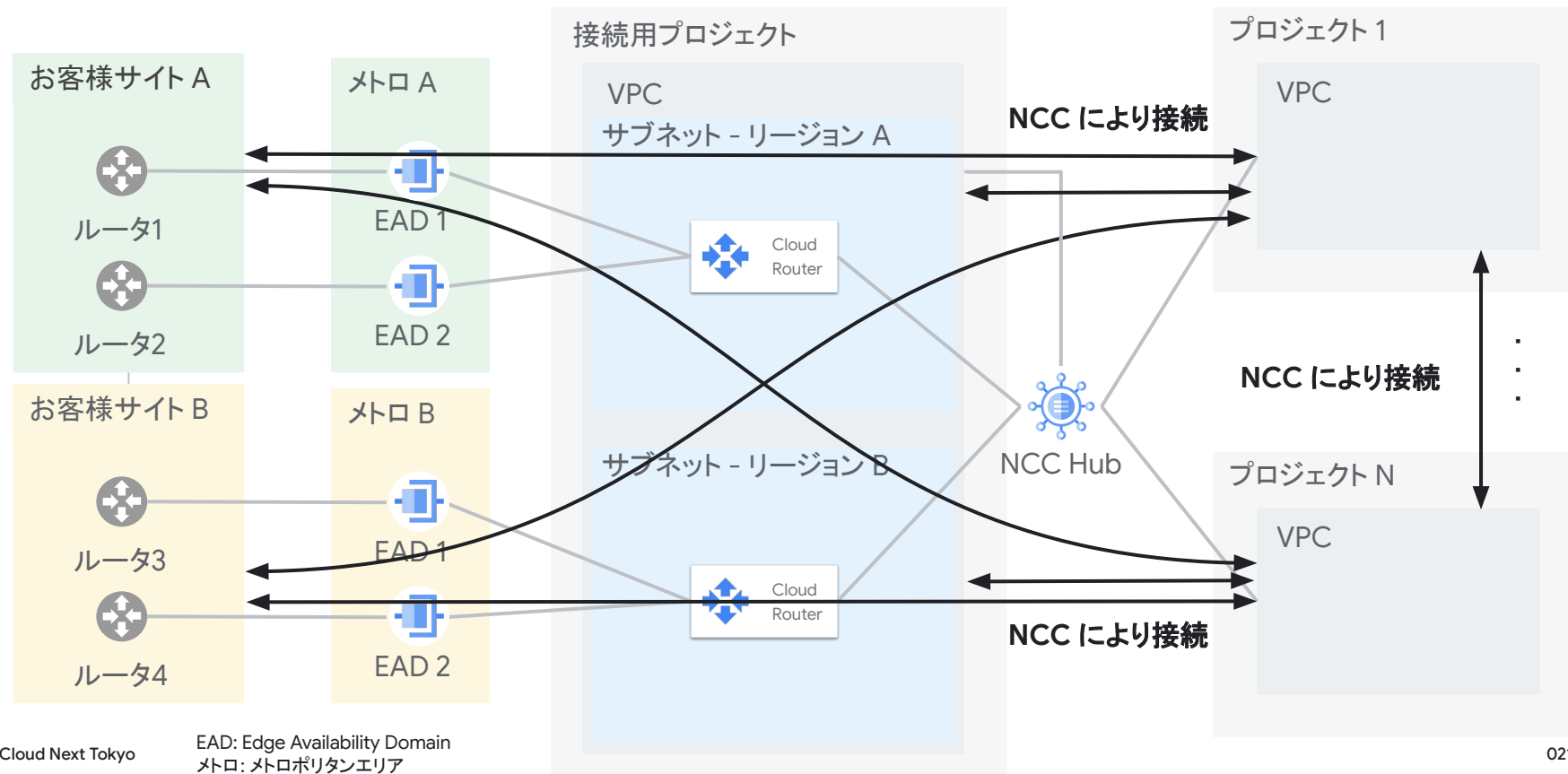
フルメッシュ接続 - ユースケースス例

- より多くの VPC をオンプレミスと接続させたい
 - 複数の独立した部署やチームが保有する VPC など
- 接続した VPC 同士もプライベート接続させたい

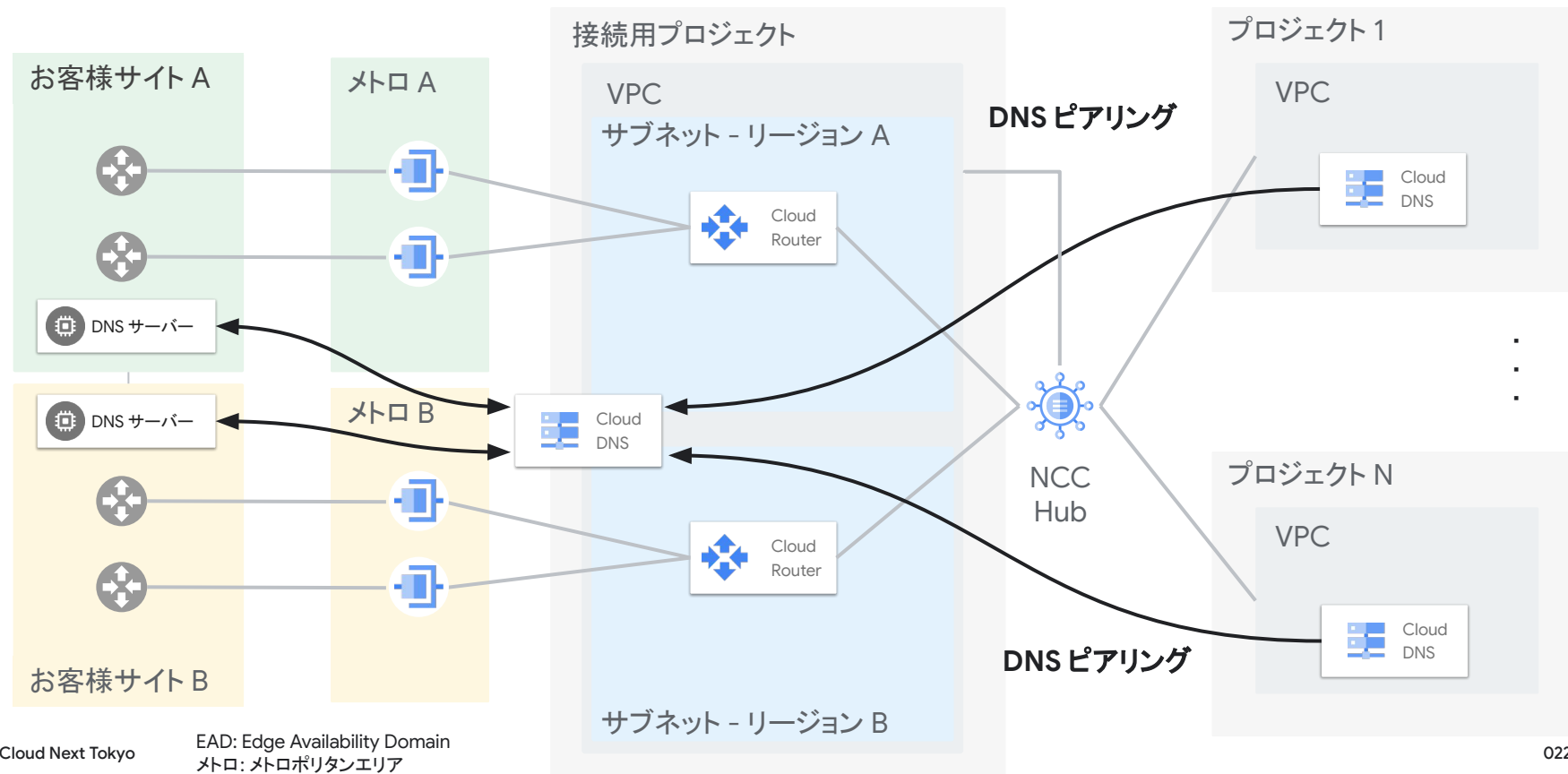
フルメッシュ接続 - アーキテクチャ



フルメッシュ接続 - アーキテクチャ



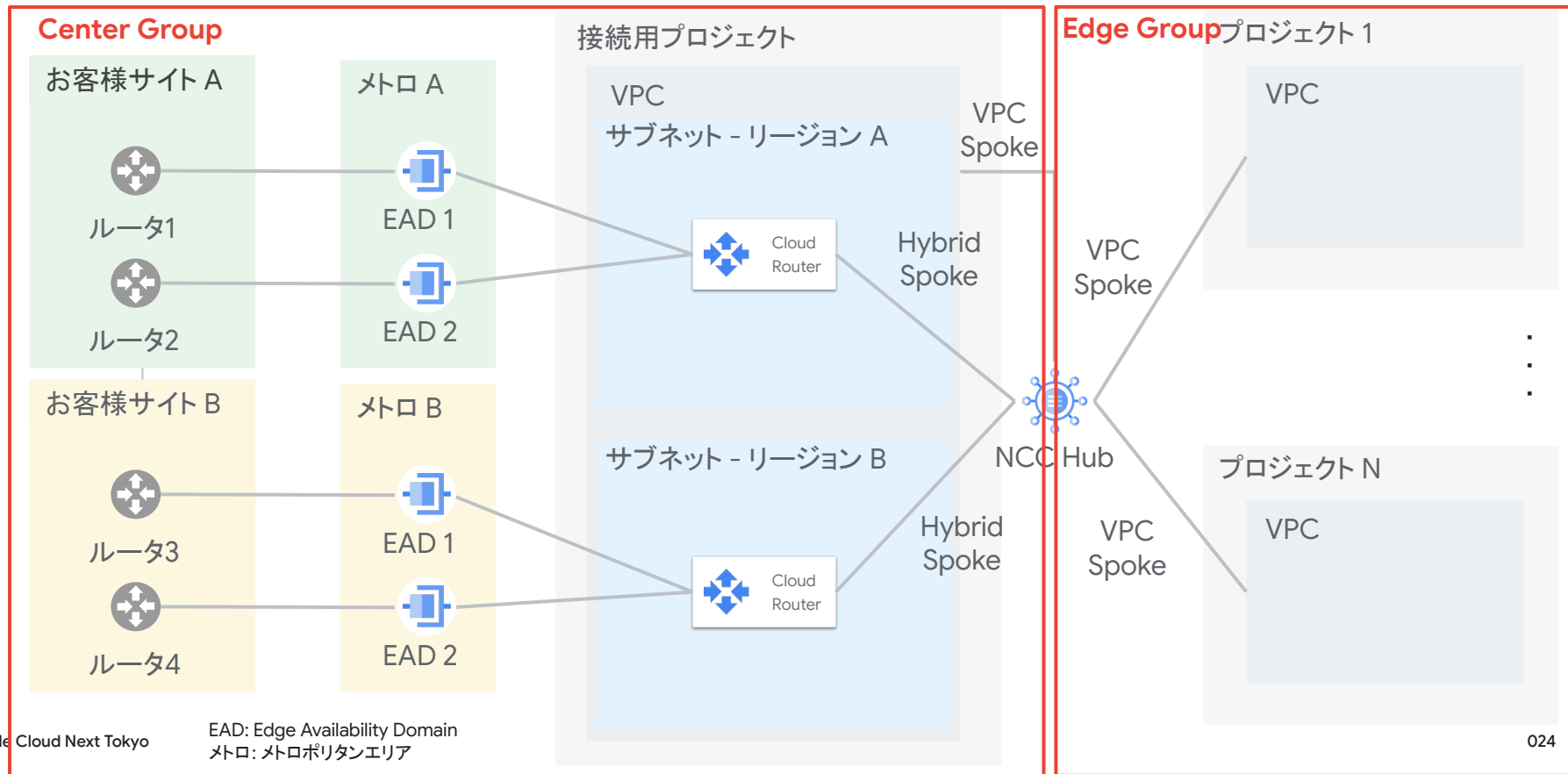
フルメッシュ接続 - ハイブリッド名前解決



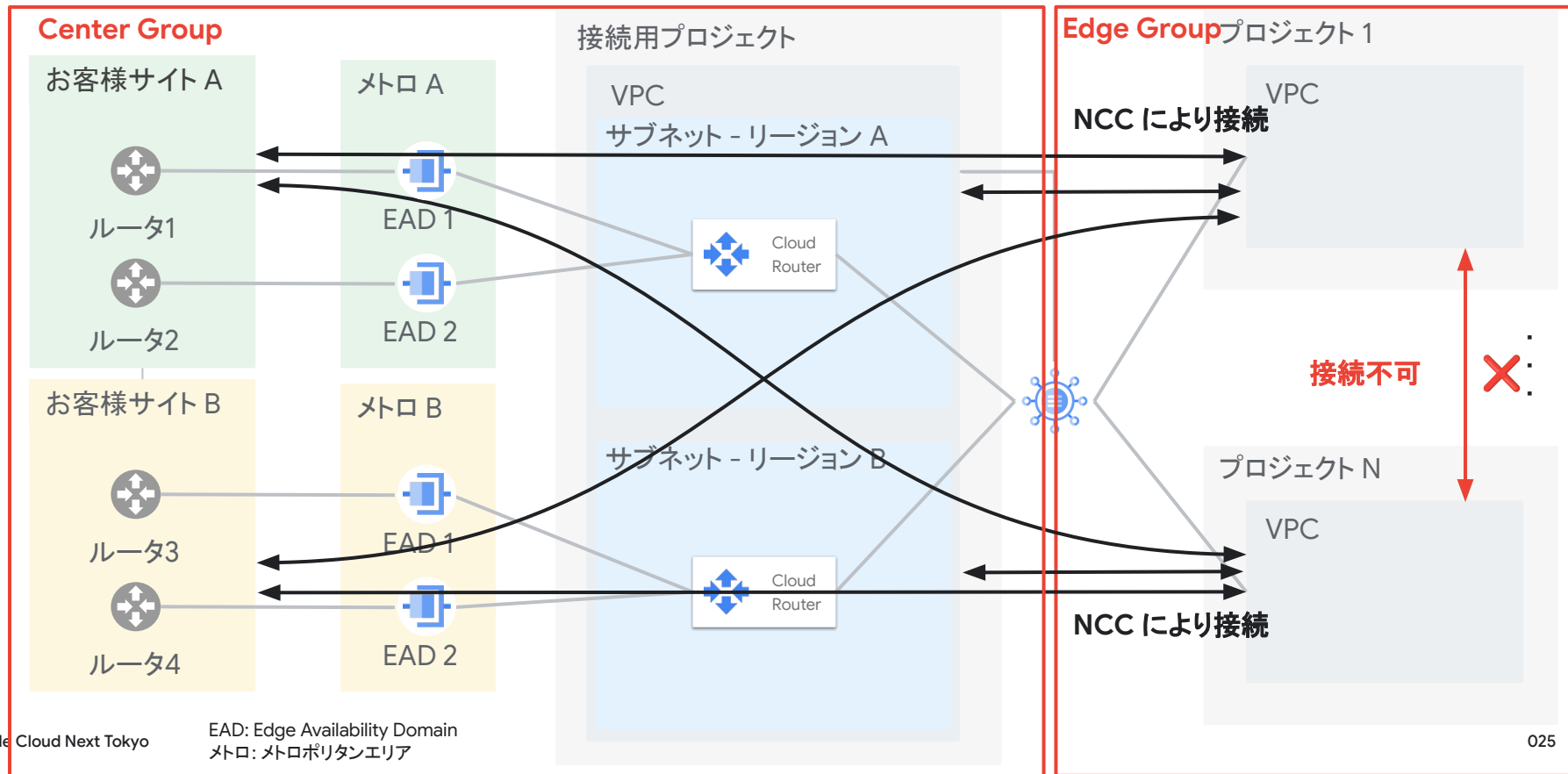
スタートポロジー接続 - ユースケース例

- より多くの VPC をオンプレミスと接続させたい
 - 複数の独立した部署やチームが保有する VPC など
- VPC 同士の接続は制限したい

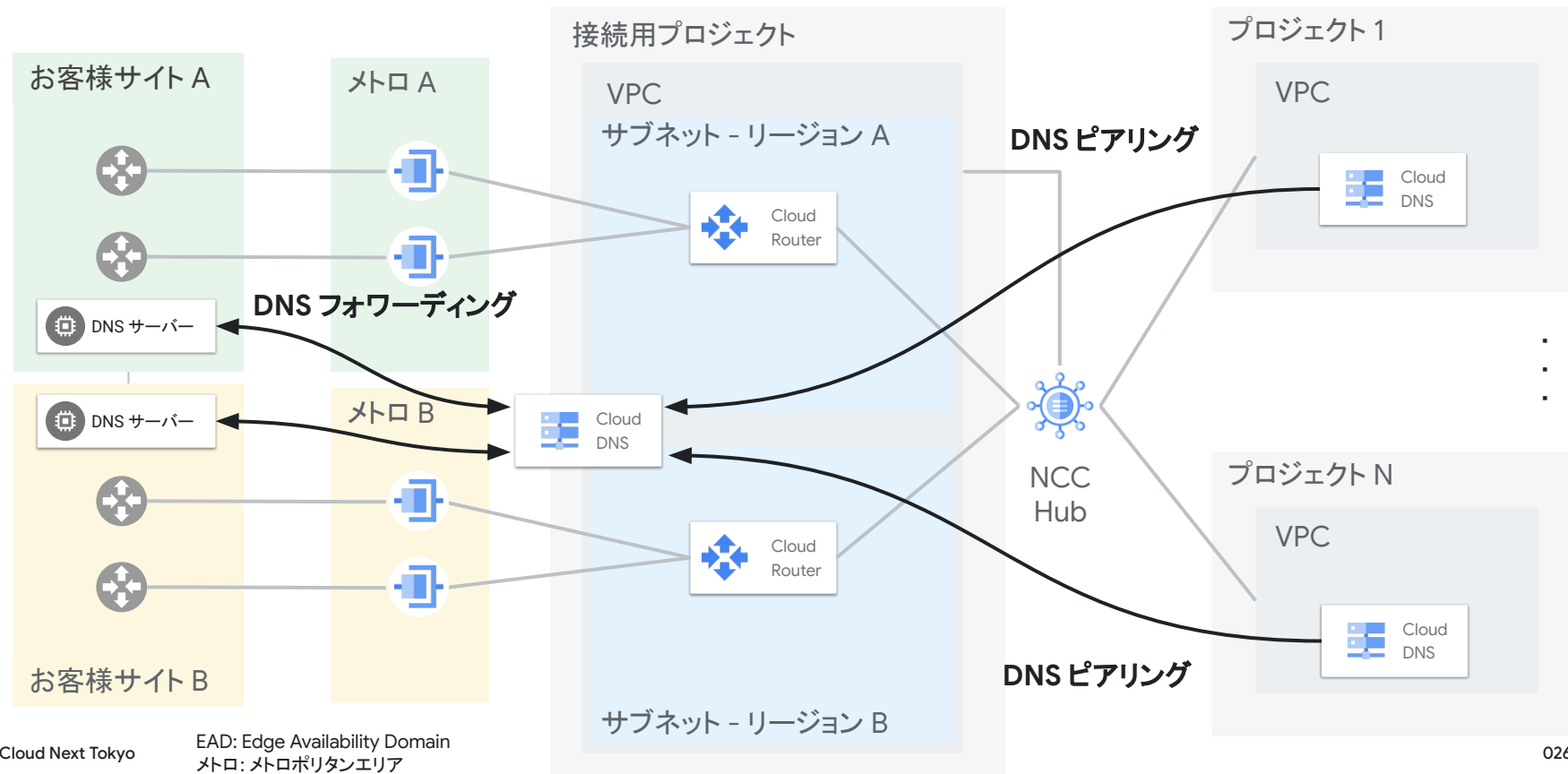
スタートポロジ接続 - アーキテクチャ



スタートポロジ接続 - アーキテクチャ



スタートポロジ接続 - ハイブリッド名前解決



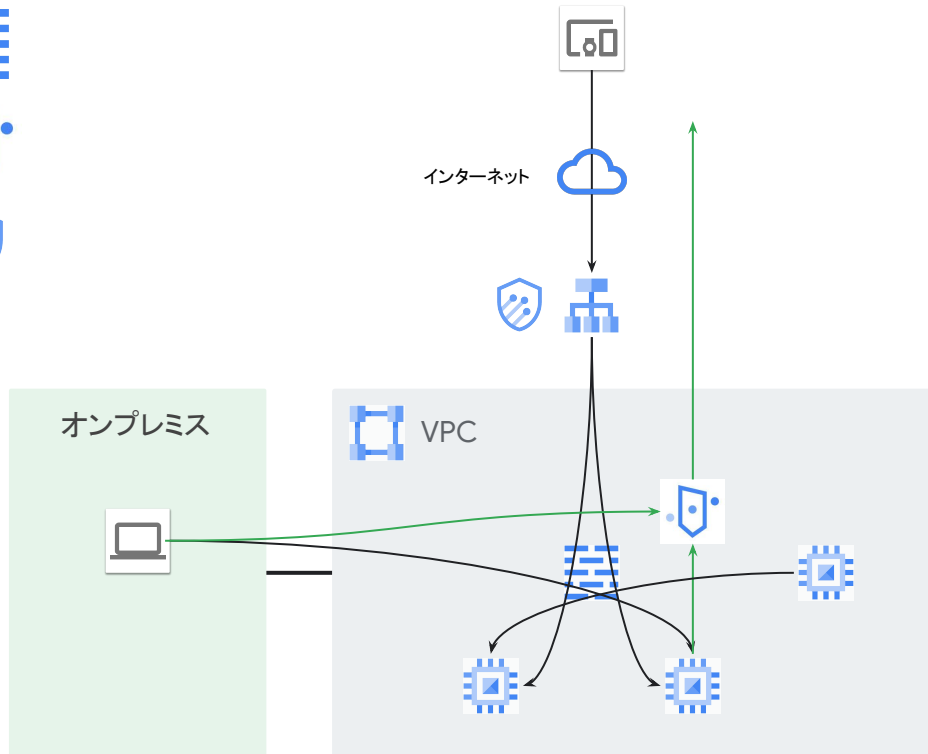
02. ネットワーク・セキュリティ

Google Cloud でのネットワークセキュリティ

- Cloud NGFW
- Secure Web Proxy
- Cloud Armor

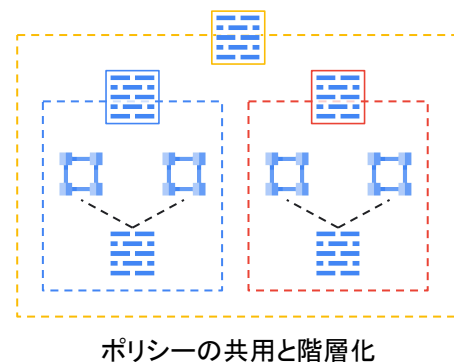
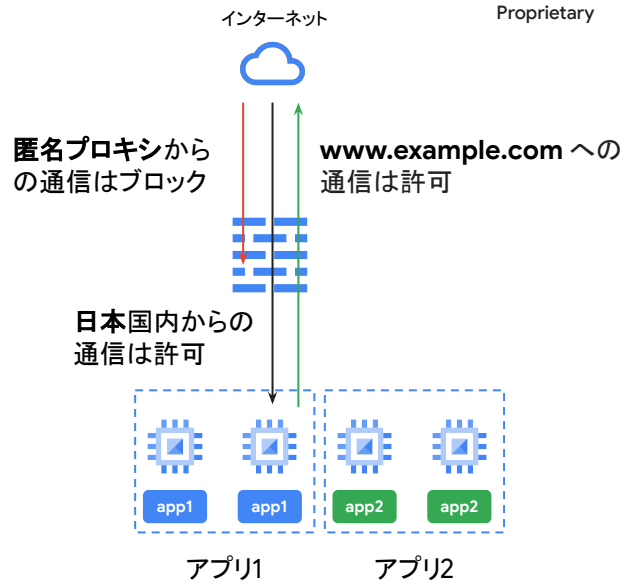


内向きの通信
外向きの通信

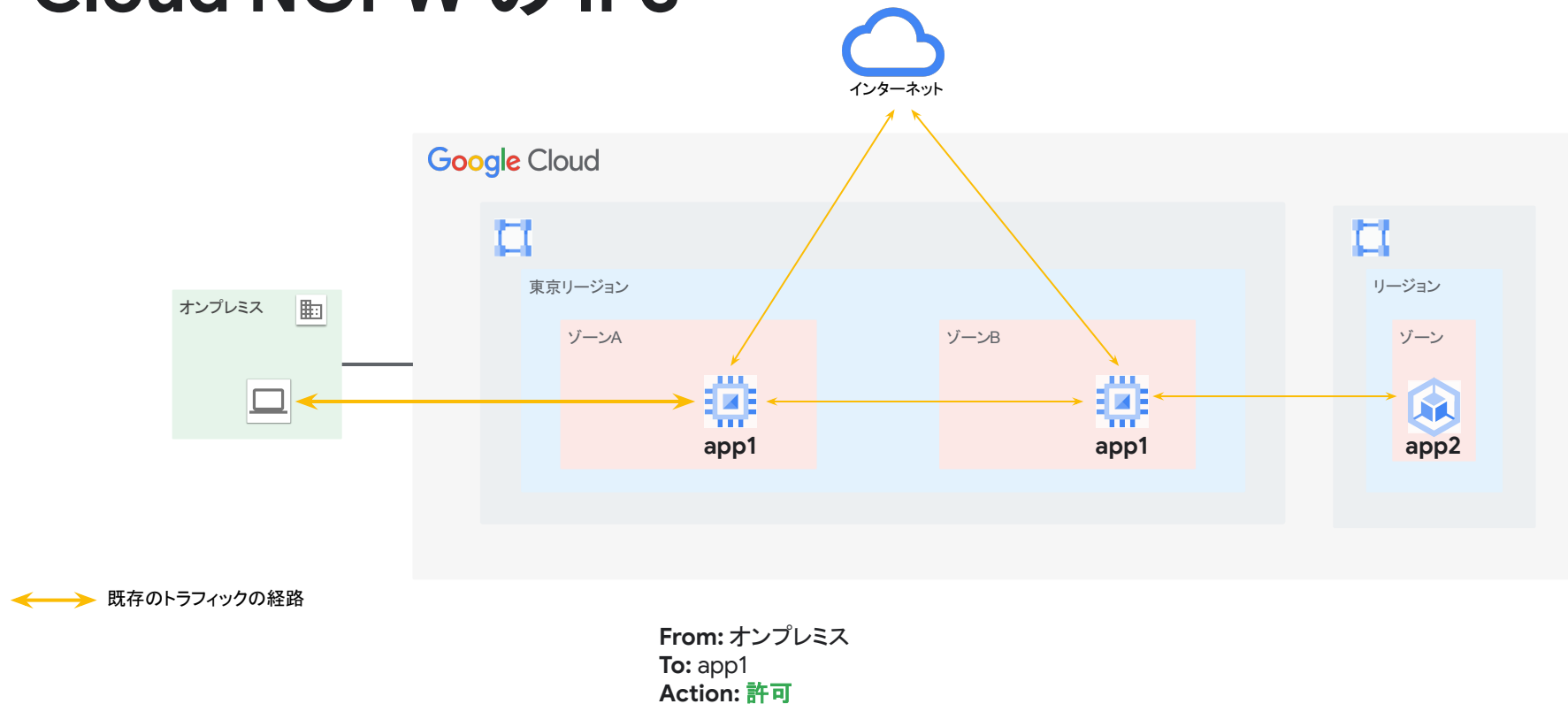


Cloud NGFW

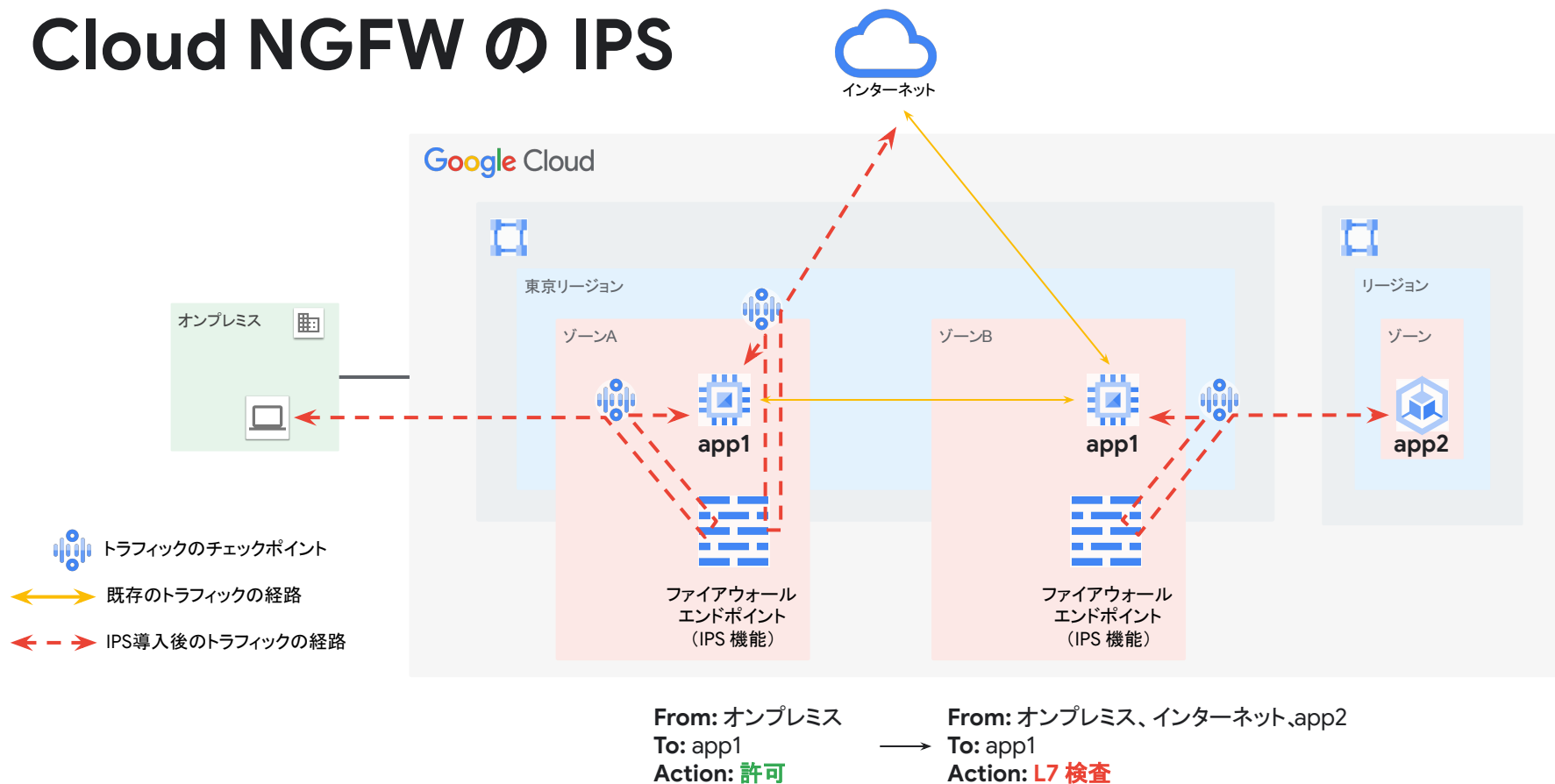
- Google Compute Engine 用のファイアウォール
 - 効率的なフィルタリングを実現
 - タグ、ホスト名(FQDN)、IPアドレス属性
 - ポリシーの共用、階層化
 - IPS 機能 (Intrusion Prevention System)
 - Palo Alto Networks 社のエンジンを利用
 - ネットワークの構成を変えずに導入可



Cloud NGFW の IPS

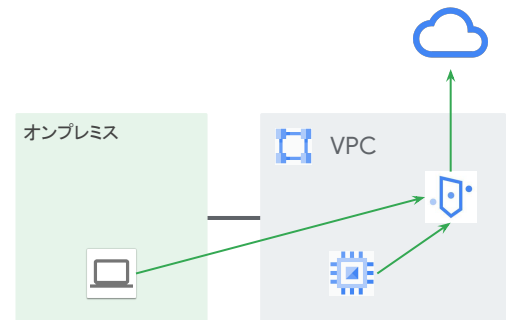


Cloud NGFW の IPS

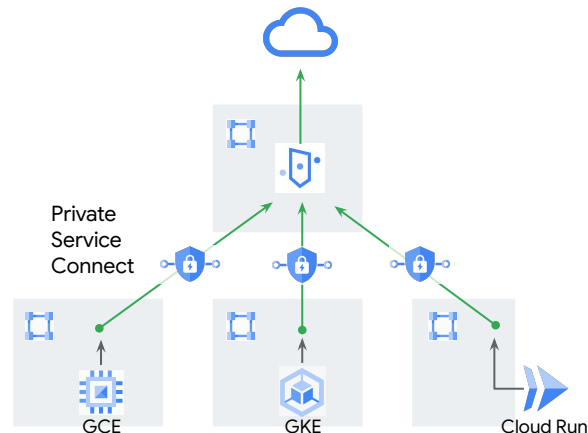


Secure Web Proxy

- マネージド プロキシ (フォワードプロキシ)
 - 明示型プロキシ、透過型プロキシとして利用
 - HTTP/HTTPS、TCP プロキシをサポート
 - クラウド内 & オンプレミスから接続
 - 細かいアクセスコントロールも可能
 - IP アドレス、HTTP ヘッダ、URL など
 - TLS インспекション



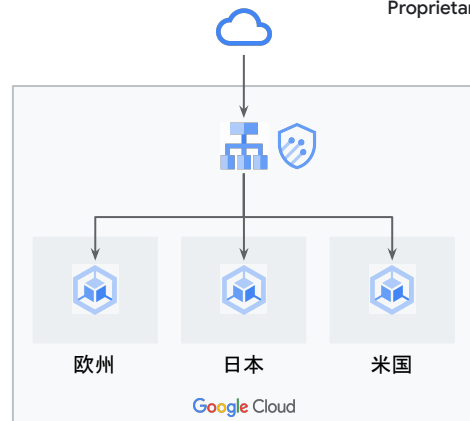
クラウド内からはもとより
オンプレミスからも利用可能



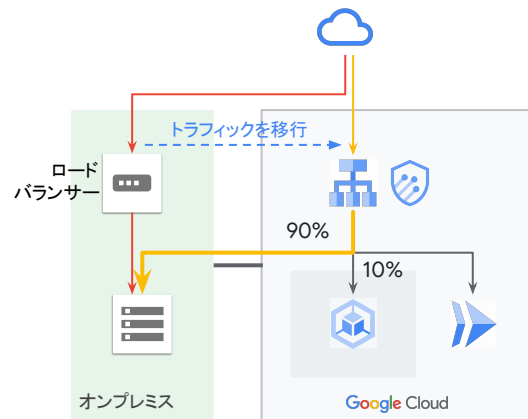
Private Service Connect によって
複数の VPC からサービスとして利用

Cloud Armor

- フルマネージドの **WAF & DDoS 対策** サービス
 - 細かなアクセスコントロール
 - アプリケーションレイヤ攻撃からの防御
 - マネージドなシグネチャ
 - ボットの検知とブロック
 - 機械学習ベースの DDoS 検知と防御
 - 非ウェブトラフィックへの DDoS 防御

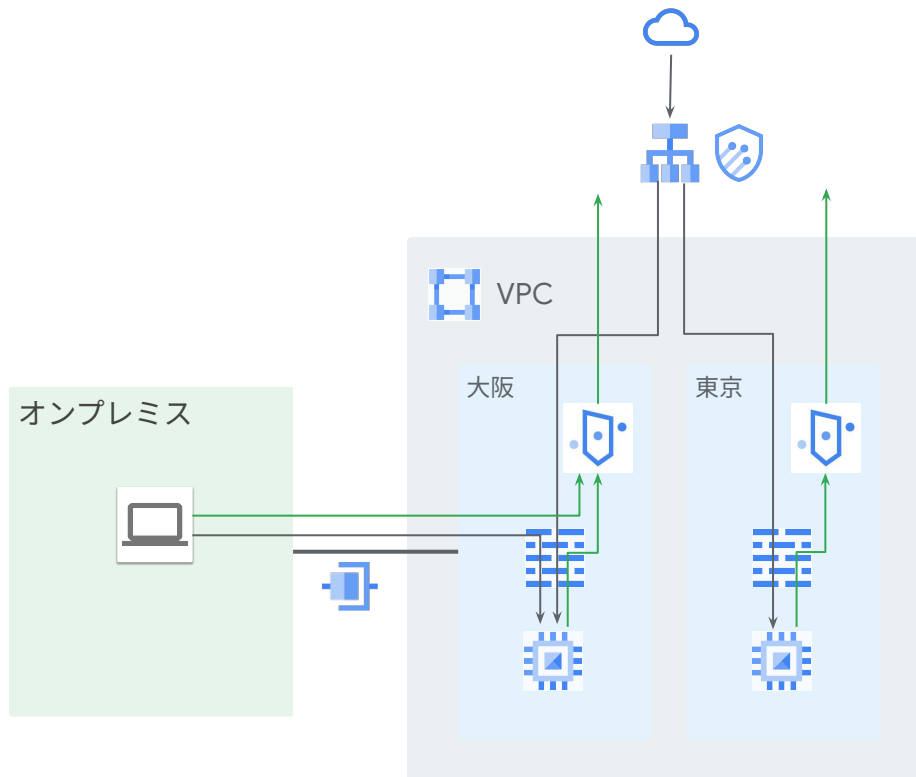


Google Cloud 上のグローバルなシステム



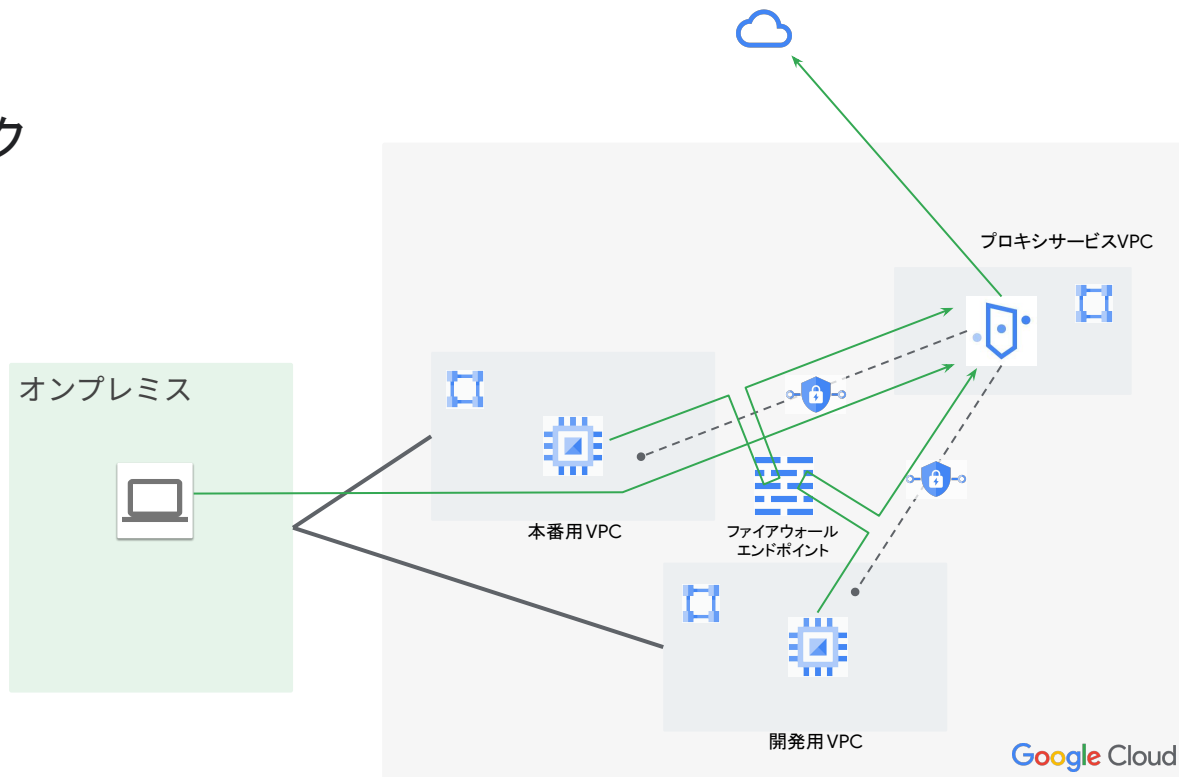
オンプレミスとのハイブリッドなシステム

シングル VPC 構成



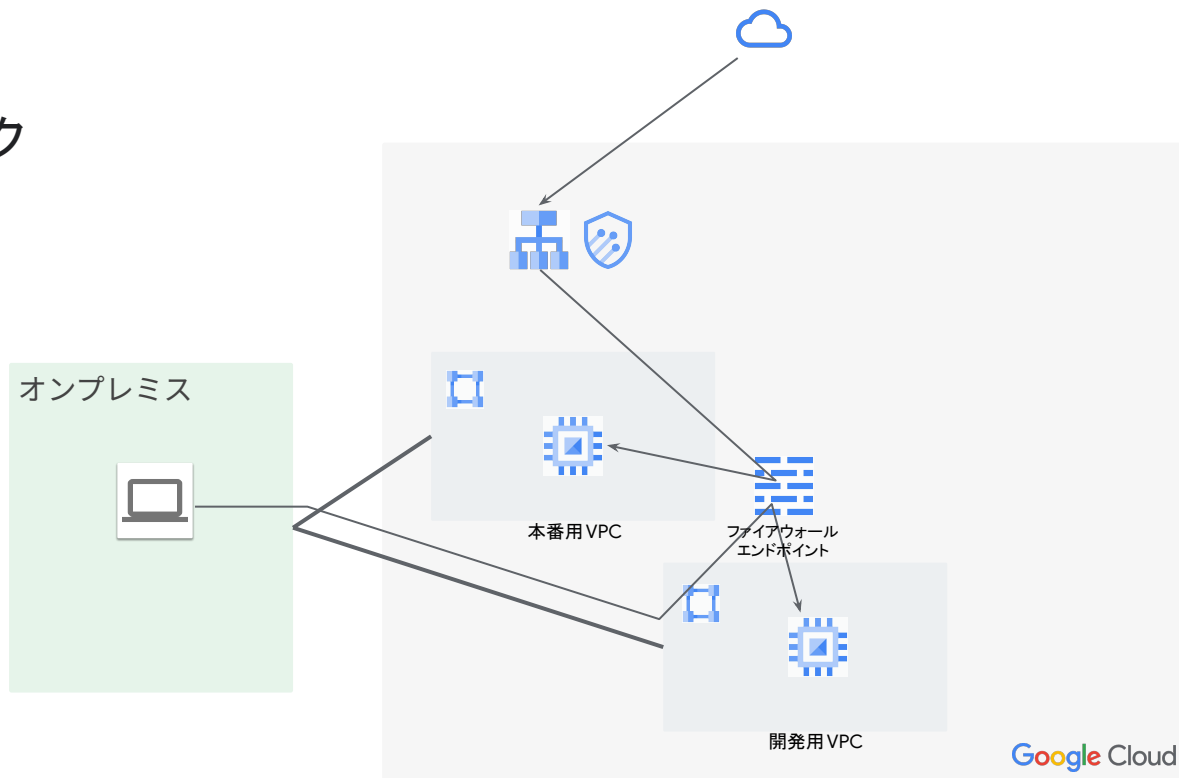
マルチ VPC 構成

外向きのトラフィック

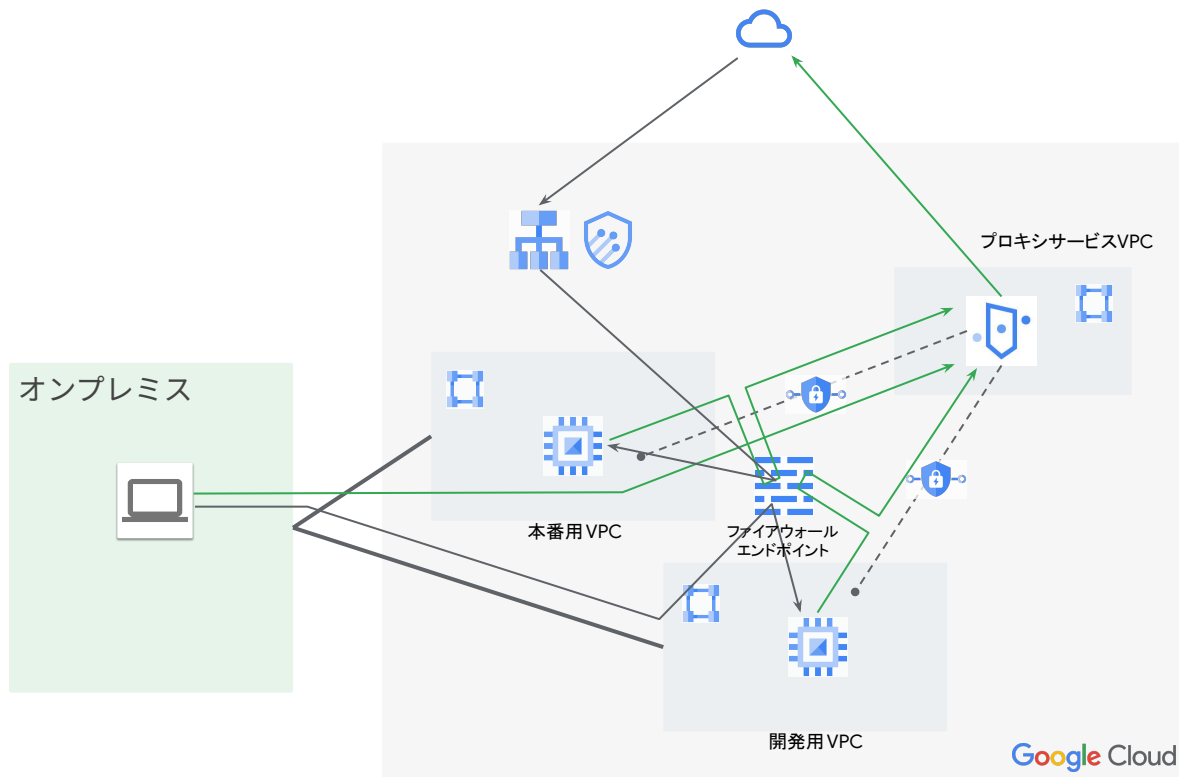


マルチ VPC 構成

内向きのトラフィック



マルチ VPC 構成



03. まとめ

まとめ

- **ハイブリッド接続**

- ユースケースに応じた適切なハイブリッド接続の選択
- Cloud DNS の機能を活用した効率的な名前解決の実現

- **ネットワークセキュリティ**

- トラフィックの経路、トラフィックの向きに応じたソリューションの選択
- 柔軟な導入方法 → 容易に導入可能