Google Cloud

# Professional Cloud Network Engineer

## 認定試験ガイド

Professional Cloud Network Engineer は、Google Cloud でネットワーク アーキテクチャを実装、管理します。クラウド インフラストラクチャを設計するアーキテクトと一緒にネットワーキング チームやクラウドチームで働くこともあります。Cloud Network Engineer は、Google Cloud Console やコマンドライン インターフェースを使用し、ネットワーク サービス、アプリケーションとコンテナのネットワーキング、ハイブリッドおよびマルチクラウド接続、VPC の実装、確立されたネットワーク アーキテクチャのセキュリティに関する経験を活用して、クラウドの実装を成功させます。

### セクション **1: Google Cloud** ネットワークの設計、計画、プロトタイピング（試験内容の約 **26%**）

1.1 全体的なネットワーク アーキテクチャを設計する。以下のような点を考慮します。

- 高可用性、フェイルオーバー、障害復旧の戦略
- DNS 戦略（例: オンプレミス、Cloud DNS、GSLB）
- セキュリティとデータの引き出しの要件
- 負荷分散
- プロジェクトごとおよび VPC ごとの割り当ての適用
- ハイブリッド接続（例: 限定公開の Google アクセスを使用したハイブリッド接続）
- コンテナ ネットワーキング
- IAM ロール
- SaaS、PaaS、IaaS サービス
- セキュリティ目的でのマイクロセグメンテーション（例: メタデータ、タグ、サービス アカウントの使用）

1.2 Virtual Private Cloud（VPC）インスタンスを設計する。以下のような点を考慮します。

- IP アドレスの管理とお客様所有 IP アドレスの使用（BYOIP）
- スタンドアロン VPC と共有 VPC
- 複数と単一
- リージョンとマルチリージョンの比較
- VPC ネットワーク ピアリング
- ファイアウォール（サービス アカウント ベース、タグベースなど）
- カスタムルート
- マネージド サービス（Cloud SQL、Memorystore など）の使用

- マルチ NIC と内部ロードバランサをネクストホップまたは等価コスト マルチパス（ECMP）ルートとして使用する VPC へのサードパーティ デバイス挿入（NGFW）

1.3 ハイブリッド クラウドとマルチクラウドのネットワークを設計する。以下のような点を考慮します。

- Dedicated Interconnect と Partner Interconnect
- マルチクラウド接続
- ダイレクト ピアリング
- IPsec VPN
- フェイルオーバーと障害復旧戦略
- リージョン ルーティング モードとグローバル VPC ルーティング モード
- オンプレミスのロケーションから複数の VPC へのアクセス（例: 共有 VPC、マルチ VPC ピアリング トポロジなど）
- ハイブリッド接続ソリューションにより提供される帯域幅と制約
- オンプレミス ロケーションから Google のサービスまたは API へのプライベート アクセス
- オンプレミス ロケーションとクラウド間の IP アドレス管理
- DNS ピアリングと転送

1.4 Google Kubernetes Engine の IP アドレス指定プランを設計する。以下のような点を考慮します。

- 一般公開クラスタノードと限定公開クラスタノード
- コントロール プレーンのパブリック エンドポイントとプライベート エンドポイント
- サブネットとエイリアス IP
- RFC 1918、RFC 1918 以外、プライベートで使用されるパブリック IP（PUPI）アドレス オプション

## セクション **2: Virtual Private Cloud**（**VPC**）インスタンスの実装（試験内容の約 **21%**）

2.1 VPC を構成する。以下のような点を考察します。

- Google Cloud VPC のリソース（例: ネットワーク、サブネット、ファイアウォール ルールなど）
- VPC ネットワーク ピアリング
- 共有 VPC ネットワークの作成と他のプロジェクトとのサブネットの共有
- Google サービスへの API アクセス（例: 限定公開の Google アクセス、公開インターフェースなど）
- 作成後の VPC サブネット範囲の拡大

2.2 ルーティングを構成する。以下のような点を考慮します。

- 静的ルーティングと動的ルーティング

- グローバルとリージョン範囲での動的ルーティング
- タグと優先度を使用したルーティング ポリシー
- ネクストホップとしての内部ロードバランサ
- VPC ネットワーク ピアリングを介したカスタムルートのインポートとエクスポート

2.3 Google Kubernetes Engine クラスタの構成と保守を行う。以下のような点を考慮します。

- エイリアス IP を使用した VPC ネイティブ クラスタ
- 共有 VPC を使用したクラスタ
- Kubernetes ネットワーク ポリシーの作成
- 限定公開クラスタとコントロール プレーンのプライベート エンドポイント
- クラスタ コントロール プレーン エンドポイント用の承認済みネットワークの追加

2.4 ファイアウォール ルールを構成、管理する。以下のような点を考慮します。

- ターゲット ネットワーク タグとサービス アカウント
- ルールの優先度
- ネットワーク プロトコル
- 上り / 下りルール
- ファイアウォール ルールのロギング
- ファイアウォール インサイト
- 階層型ファイアウォール

2.5 VPC Service Controls を実装する。以下のような点を考慮します。

- アクセスレベルとサービス境界の作成および構成
- VPC のアクセス可能なサービス
- 境界ブリッジ
- 監査ロギング
- ドライラン モード

## セクション **3:** ネットワーク サービスの構成（試験内容の約 **23%**）

3.1 ロード バランシングを構成する。以下のような点を考慮します。

- バックエンド サービスとネットワーク エンドポイント グループ（NEG）
- バックエンド サービスへのトラフィックとヘルスチェックを許可するファイアウォール ルール
- バックエンド サービスとターゲット インスタンス グループのヘルスチェック

- 分散方式を使用したバックエンドおよびバックエンド サービスの構成（例: RPS、CPU、カスタムなど）、セッション アフィニティ、容量スケーリング/スケーラー
- TCP および SSL プロキシ ロードバランサ
- ロードバランサ（例: 外部 TCP/UDP ネットワーク負荷分散、内部 TCP/UDP 負荷分散、外部 HTTP(S) 負荷分散、内部 HTTP(S) 負荷分散など）
- プロトコル転送
- ワークロードの増加への対応（自動スケーリングと手動スケーリングそれぞれを使用した場合）

3.2 Google Cloud Armor ポリシーを構成する。以下のような点を考慮します。

- セキュリティ ポリシー
- ウェブ アプリケーション ファイアウォール（WAF）ルール（例: SQL インジェクション、クロスサイト スクリプティング、リモート ファイル インクルードなど）
- ロードバランサ バックエンドへのセキュリティ ポリシーの接続

3.3 Cloud CDN の構成。以下のような点を考慮します。

- 有効化と無効化
- Cloud CDN
- キャッシュキー無効化キャッシュ オブジェクト
- 署名付き URL
- カスタム送信元

3.4 Cloud DNS の構成と保守を行う。以下のような点を考察します。

- ゾーンとレコードの管理
- Cloud DNS への移行
- DNS Security Extensions（DNSSEC）
- 転送と DNS サーバー ポリシー
- オンプレミス DNS と Google Cloud の統合
- スプリット ホライズン DNS
- DNS ピアリング
- 限定公開 DNS のロギング

3.5 Cloud NAT を構成する。以下のような点を考察します。

- アドレス指定
- ポートの割り振り
- タイムアウトのカスタマイズ
- ロギングとモニタリング

- 組織のポリシーの制約ごとの制限

3.6 ネットワーク パケット インスペクションを構成する。以下のような点を考察します。

- 単一 VPC トポロジとマルチ VPC トポロジでの Packet Mirroring
- Packet Mirroring のソースとトラフィックのフィルタを使用した関連トラフィックのキャプチャ
- マルチ NIC VM（次世代のファイアウォール アプライアンスなど）を使用した VPC 間トラフィックのルーティングと検査
- 高可用性マルチ NIC VM ルーティングのネクストホップとしての内部ロードバランサの構成

## セクション **4:** ハイブリッド相互接続の実装（試験内容の約 **14%**）

4.1 Cloud Interconnect を構成する。以下のような点を考慮します。

- Dedicated Interconnect 接続と VLAN アタッチメント
- Partner Interconnect 接続と VLAN アタッチメント

4.2 サイト間 IPsec VPN を構成する。以下のような点を考慮します。

- 高可用性 VPN（動的ルーティング）
- Classic VPN（ルートベースのルーティング、ポリシーベースのルーティングなど）

4.3 Cloud Router を構成する。以下のような点を考慮します。

- Border Gateway Protocol（BGP）属性（例:ASN、ルート優先度/MED、リンクローカル アドレスなど）
- BGP によるカスタム ルート アドバタイズ
- 信頼性が高く冗長な Cloud Router のデプロイ

## セクション **5:** ネットワーク オペレーションの管理、モニタリング、最適化（試験内容の約 **16%**）

5.1 Google Cloud のオペレーション スイートを使用してロギングとモニタリングを行う。以下のような点を考慮します。

- ネットワーク コンポーネントのログの確認（例: VPN、Cloud Router、VPC Service Controls など）
- ネットワーキング コンポーネント（例: VPN、Cloud Interconnect 接続と相互接続のアタッチメント、Cloud Router、ロードバランサ、Google Cloud Armor、Cloud NAT など）

5.2 セキュリティを管理、維持する。以下のような点を考慮します。

- ファイアウォール（例: クラウドベース、プライベート）
- IAM の問題の診断と解決（例: 共有 VPC、セキュリティ/ネットワーク管理者など）

5.3 接続性の維持管理とトラブルシューティングを行う。以下のような点を考慮します。

- HTTP(S) ロード バランシングによるトラフィック フローのドレインとリダイレクト
- フローログを使用した、上りトラフィックと下りトラフィックのモニタリング
- ファイアウォール ログとファイアウォール インサイトのモニタリング
- VPN の管理とトラブルシューティング
- Cloud Router の BGP ピアリング問題のトラブルシューティング

5.4 レイテンシとトラフィック フローのモニタリング、管理、トラブルシューティングを行う。以下のような点を考慮します。

- ネットワークのスループットとレイテンシのテスト
- ルーティングの問題の診断
- Network Intelligence Center を使用したトポロジの可視化、接続のテスト、パフォーマンスのモニタリング