初期構成の完了

- 外部ネットワークの構成 （1 ページ）
- テナントの作成 （5 ページ）
- BGP-EVPN を使用したサイト間接続のための VPC ピアリングの構成 （16 ページ）

外部ネットワークの構成

この手順は、外部ポリシーの作成方法を示しています。オンプレミス サイトの複数のルータに接続できる単一の外部ネットワーク、または CCR への接続に使用できる複数の VRF を持つ複数の外部ネットワークを設定できます。

始める前に

外部ネットワークを作成する前に、ハブ ネットワークを作成しておく必要があります。

ステップ 1 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）] > [外部ネットワーク（External Networks）] に移動します。**
構成された外部ネットワークが表示されます。Cisco Cloud Network Controller は 1 つのハブ ネットワークのみをサポートするため、**[ハブ ネットワーク（Hub Network）]** 列には 1 つのハブ ネットワークのみが表示されます。

ステップ 2 **[アクション（Actions）]** をクリックし、**[外部ネットワークの作成（Create External Network）]** を選択します。
[外部ネットワークの作成（Create External Network）] ウィンドウが表示されます。

（注） ハブネットワークがまだ設定されていない場合は、外部ネットワークを作成する前にハブ ネットワークを作成する必要があることを示す警告がページの上部に表示されます。メッセージ内の青い **[Cisco Cloud Network Controller 設定（Cisco Cloud Network Controller Setup）]** リンクをクリックし、ハブネットワークを作成して、ここに戻ります。ハブ ネットワークの作成の詳細については、セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成 を参照してください。

ステップ 3 次の *[外部ネットワークの作成ダイアログボックスのフィールド（Create External Network Dialog Box Fields）]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *1 : [*外部ネットワークの作成（*Create External Network*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	外部ネットワーク名を入力します。
VRF	この 外部VRF は、オンプレミス CCR との外部接続に使用されます。この目的で複数の 外部VRF を作成できます。 この VRF は、VRF が次の 3 つの特性をすべて備えている場合に 外部VRF として識別されます。 • インフラ テナントの下で構成された • 外部ネットワークに関連付けられている • クラウド コンテキスト プロファイルに関連付けられていない 外部ネットワークに関連付けられているVRFはすべて 外部VRF になります。この時点では、外部VRF はインフラ テナント以外のテナントで作成することはできず、外部VRF はクラウド コンテキスト プロファイルまたはサブネットに関連付けることはできません。 外部VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 [+ VRF の作成（+ Create VRF）] オプションを使用してVRFを作成することもできます。 3. **[選択（Select）]**をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。
ハブ ネットワーク	ハブ ネットワークは、初回セットアップで設定した後に自動的に表示されます。 （注） ハブ ネットワークがまだ設定されていない場合は、外部ネットワークを作成する前にハブネットワークを作成する必要があります。ハブ ネットワークの作成に関する詳細は、Cisco Cloud Network Controller for Google Cloud インストール ガイド、リリース 25.0(x) 以降の、「セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成」の章を参照してください。
VPN ルータ	このフィールドは編集できません。デフォルトの VPN ルータが自動的に選択されます。
[設定（Settings）]	

[プロパティ（Properties）]	説明
地域	リージョンを選択するには: 1. **[地域の追加（Add Region）]** をクリックします。 **[地域の選択（Select Regions）]** ダイアログボックスが表示されます。 • 初回セットアップの一部として選択した地域がここに表示されます。 • 複数の地域を選択して、複数の地域でクラウド ルータを起動できます。 2. **[地域の選択（Select Regions）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
VPN ネットワーク	VPNネットワークエントリは、内部接続に使用されます。設定されたすべてのVPNネットワークが、選択したすべてのリージョンに適用されます。 VPN ネットワークを追加するには、次の手順を実行します。 **1.** **[VPNネットワークの追加（Add VPN Network）]** をタップします。 **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスが表示されます。 **2.** **[名前（Name）]** フィールドに VPN ネットワークの名前を入力します。 **3.** **[+ IPSec ピアの追加（+ Add IPSec Peer）]** をクリックします。 IPSec ピア エントリごとに 2 つのトンネルが作成されます。 **4.** 追加する IPSec ピアの次のフィールドに値を入力します。 • **IPSec トンネル ピアの パブリック IP** • **事前共有キー** • **IKE Version**：IPSec トンネル接続用に **ikev1** または **ikev2** を選択します。 • **BGP ピア ASN** • **Subnet Pool Name**：**[サブネット プール名の選択（Select Subnet Pool Name）]** をクリックします。 **[サブネット プール名の選択（Select Subnet Pool Name）]** ダイアログボックスが表示されます。リストされている使用可能なサブネット プールのいずれかを選択し、**[選択（Select）]** をクリックします。 **5.** この IPSec トンネルを追加するには、チェックマークをクリックします。 別の IPSec トンネルを追加する場合は、**[+ IPSec トンネルの追加（+ Add IPSec Tunnel）]** をクリックします。 **6.** **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスで **[追加（Add）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

ステップ 4 外部ネットワークの作成が完了したら、**[保存（Save）]** をクリックします。
[外部ネットワークの作成（Create External Network）] ウィンドウで **[保存（Save）]** をクリックすると、クラウド ルータが Google Cloud で構成されます。

Google Cloud でクラウドルータがで構成されていることを確認するには、インフラ VPC の Google Cloud アカウントで、**[ハイブリッド接続（Hybrid Connectivity）]** > **[クラウドルータ（Cloud Routers）]** に移動します。さまざまなリージョン用に作成されたクラウドルータが表示されます（新しく設定されたクラウドルータを表示するには、[更新（Refresh）]をクリックする必要があります）。

IPSec セッションを表示するには、**[Hybrid Connectivity]** > **[VPN]** > **[Cloud VPN Tunnels]** に移動します。

テナントの作成

次のセクションでは、マネージド テナントまたはアンマネージド テナントを作成する方法。

Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する

Google Cloud は、ファイル システムに似た方法でリソースを編成します。

- 最上位の組織は複数のフォルダを持つことができます。
- すべてのフォルダには、他のフォルダを含めることも、すべてのプロジェクトに一意の ID があるプロジェクトを含めることもできます。
- クラウド リソース（VM、VPC、サブネットなど）はプロジェクトに含まれます。

Google Cloud の観点から理解するのに有用な領域は、組織とフォルダのレベルですが、Cisco Cloud Network Controller の観点から最も関連性があるのは、プロジェクトのレベルです。

各 Cisco Cloud Network Controller テナントは、Google Cloud プロジェクトに 1 対 1 でマッピングされます。

- Cisco Cloud Network Controller テナントは、複数の Google Cloud プロジェクトにまたがることはできません。
- Google Cloud プロジェクト内に複数の Cisco Cloud Network Controller テナントを存在させることはできません。

Cisco Cloud Network Controller では、Google Cloud は **サービス アカウント**を使用してプロジェクトにアクセスできます。これらのアカウントは、Google Cloud サービスにアクセスする必要があるアプリケーション用です。これらを使用して、Cisco Cloud Network Controller と他のテナントのポリシーを実行、展開し、またプッシュすることができます。Google Cloud 内部で実行されるアプリケーションで使用されるサービスアカウントにはクレデンシャルは必要ありませんが、事前に生成された秘密キーを必要とする Google Cloud の外部で実行されるアプリケーションにはクレデンシャルが必要です。サービス アカウントは1つの Google Cloud プロジェクトに存在しますが、他のプロジェクト（Cisco Cloud Network Controller の場合、他のテナント用）のポリシーを管理するためのアクセス権も付与されます。

次の項では、Google Cloud を使用して Cisco Cloud Network Controller テナントを構成するさまざまな方法について詳しく説明します。

- 管理対象クレデンシャルを持つユーザ テナント （6 ページ）
- 管理対象外クレデンシャルを持つユーザ テナント （6 ページ）

管理対象クレデンシャルを持つユーザ テナント

このタイプのユーザ テナントには、次の特性があります。

- このテナント アカウントは、Cisco Cloud Network Controller によって管理されます。
- このタイプのユーザーテナントのテナント構成プロセスの一環として、最初にCisco Cloud Network Controller GUIで **[マネージド ID（Managed Identity）]** を選択します。
- Cisco Cloud Network Controller で必要なパラメータを構成したら、Google Cloud でこのテナントに必要な権限を設定する必要があります。Cisco Cloud Network Controller によって作成されたサービスアカウントを、次のルールを使用してIAMユーザーとして追加します。
  - クラウド機能サービス エージェント
  - コンピューティング インスタンス管理（v1）
  - コンピューティング ネットワーク管理者
  - コンピューティング セキュリティ管理者
  - 管理者のログイン
  - パブ/サブ管理者
  - ストレージ管理者

このようなテナントの作成手順については、Cisco Cloud Network Controller GUI を使用した管理対象テナントの作成 （9 ページ） を参照してください。

管理対象外クレデンシャルを持つユーザ テナント

このタイプのユーザ テナントには、次の特性があります。

- このテナント アカウントは、Cisco Cloud Network Controller によって管理されていません。
- このタイプのテナントの Cisco Cloud Network Controller に必要なパラメータを構成する前に、まず、このテナントに関連付けられたサービス アカウントの Google Cloud から必要な秘密キー情報を含むJSONファイルをダウンロードする必要があります。
- このタイプのユーザーテナントのテナント構成プロセスの一環として、Cisco Cloud Network Controller GUIで **[アンマネージド ID（Unmanaged Identity）]** を選択します。Cisco Cloud Network Controller でこのタイプのテナントの構成プロセスの一環として、ダウンロードした JSON ファイルから次の情報を提供します。
  - キーID
  - RSA プライベート キー
  - クライアントID
  - E メール

このようなテナントの作成手順については、Cisco Cloud Network Controller GUI を使用したアンマネージド テナントの作成 （13 ページ） を参照してください。

ユーザー テナントの Google Cloud プロジェクトのセットアップ

このセクションの手順を実行して、ユーザー テナントの Google Cloud プロジェクトをセットアップします。そのユーザー テナントは、管理対象または管理対象外のテナントです。

ステップ 1 必要に応じて、ユーザー テナントの Google Cloud プロジェクトを作成します。

各ユーザー テナントは Google Cloud プロジェクトに 1 対 1 でマッピングされます。ユーザー テナント用の Google Cloud プロジェクトがまだ作成されていない場合は、次の手順に従って Google Cloud プロジェクトを作成します。

a) Google アカウントにログインします。
b) **[IAM & Admin]** > **[Manage resources]** に移動します。
c) ページの上部にある **[組織の選択（Select Organization）]** ドロップダウン リストを使用して、プロジェクトを作成する組織を選択します。
d) **[+プロジェクトの作成（+ CREATE PROJECT）]** をクリックします。
e) 表示される **[新規プロジェクト（New Project）]** ウィンドウで、プロジェクト名を入力し、必要に応じて課金アカウントを選択します。

プロジェクト名には、文字、数字、一重引用符、ハイフン、スペース、または感嘆符のみを含めることができ、4ー30 文字にする必要があります。

f) **[場所（Location）]** フィールドに親組織またはフォルダを入力します。

そのリソースは、新しいプロジェクトの階層的な親になります。

g) [作成（CREATE）] をクリックします。

ステップ 2 Google Cloud で、この管理対象テナントに関連付けられたサービス アカウントで適切なサービス API を有効にします。

a) Google Cloud GUIで、このユーザー テナントに関連付けられている Google Cloud プロジェクトにログインします。
プロジェクトの **ダッシュボード** が表示されます。
b) **ダッシュボード** の上部にある検索バーで、**「API & Services」** を検索し、その検索結果をクリックして **「API & Services」** ウィンドウにアクセスします。
c) **「API & Services」** ウィンドウで、**[+ ENABLE APIS AND SERVICES]** タブをクリックします。

[API ライブラリ（API Library）] ウィンドウが表示されます。

d) **[Search for APIs & Services]**フィールドで、必要なサービスを検索して有効にします。

次のリストの各サービスについて、

1. **[API とサービスの検索（Search for APIs & Services）]** フィールドで API またはサービスを検索します。

2. 検索結果をクリックすると、その API またはサービスのページが表示されます。
3. その API またはサービス ページで **[ENABLE]** ボタンをクリックします。

次に、検索して有効にする必要がある API とサービスを示します。

- コンピューティング エンジン
- Cloud Deployment Manager V2 API
- Cloud Pub / Sub API
- クラウド リソース マネージャ API
- Service Usage API
- Cloud Logging API

各 API またはサービスを有効にするには数分かかります。各APIまたはサービスを有効にした後、**[API とサービス（APIs & Services）]** ウィンドウに戻る必要があります。

上記のすべての API とサービスを有効にすると、次の追加の API とサービスが自動的に有効になります。

- Identity and Access Management（IAM）API
- IAM サービス アカウントの資格情報
- クラウド OS ログイン API
- クラウド DNS API
- レコメンダAPI

自動的に有効になっていない場合は、手動で有効にします。

ステップ 3 Google Cloud のこの管理対象テナントに必要な権限を設定します。

a) Google Cloud GUIで、このユーザー テナントに関連付けられている Google Cloud プロジェクトにログインします。
プロジェクトの **ダッシュボード** が表示されます。

b) 左側のナビゲーション バーで、**[IAM & Admin]** をクリックし、**[IAM]** を選択します。

[IAM] ウィンドウが表示され、いくつかのサービス アカウントが表示されます。

c) 適切なサービス アカウントを見つけます。

d) このサービス アカウントの権限を設定します。

1. このサービス アカウントの行にある鉛筆アイコンをクリックします。

[権限の編集（Edit Permissions）] ウィンドウが表示されます。

2. **[+別のロールの追加（+ ADD ANOTHER ROLE）]** をクリックし、ロールとして **[エディタ（Editor)]** を選択します。

サービス アカウントが表示された **[IAM]** ウィンドウに戻ります。

3. **[+別のロールの追加（+ ADD ANOTHER ROLE）]** を再度クリックし、このサービス アカウントに必要な残りのロールを追加します。

   以下は、このプロセスの最初のステップで追加したクラウド機能サービス エージェントを含む、このサービス アカウントに割り当てる必要があるロールの完全なリストです。

   - エディタ（Editor）
   - ロール管理者
   - プロジェクト IAM 管理者

4. 必要なすべてのロールを追加した後で、**[保存（Save）]** をクリックします。

   IAM ウィンドウに戻り、サービス アカウントが表示され、必要なロールがこのサービス アカウントに割り当てられます。

管理対象テナントの作成

次のセクションでは、管理対象テナントを作成するために必要な情報を提供します。

- Cisco Cloud Network Controller で管理対象テナントを作成する
- Google Cloud の管理対象テナントに必要な権限を設定します。

Cisco Cloud Network Controller GUI を使用した管理対象テナントの作成

このセクションでは、GUI を使用して Cisco Cloud Network Controller で管理するテナントを作成する方法について説明します。

ステップ 1 ユーザーテナントの Google Cloud プロジェクトをセットアップします。

これらの手順については、ユーザー テナントの Google Cloud プロジェクトのセットアップ （7 ページ）を参照してください。

ステップ 2 Cisco Cloud Network Controller GUI で、**[アプリケーション管理（Application Management）]** > **[VRF]**に移動します。

すでに設定されているテナントのテーブルが表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[テナントの作成（Create Tenant）]**を選択します。

[テナントの作成（Create Tenant）] ダイアログ ボックスが表示されます。

ステップ 4 次の *[テナント ダイアログボックス フィールドの作成（Create Tenant Dialog Box Field）]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *2:* テナント ダイアログボックス フィールドの作成

[プロパティ（Properties）]	**説明**
名前（Name）	テナント名を入力します。正規表現の一致: `[az]（[-a-z0-9] * [a-z0-9]）？` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。
説明	テナントの説明を入力します。
[設定（Settings）]	
セキュリティドメインの追加（Add Security Domain）	テナントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。
Google Cloud Project	
Google Cloud Project ID	この Cisco Cloud Network Controller テナントに関連付けられる Google Cloud プロジェクト ID を入力します。
アクセスタイプ	Cisco Cloud Network Controller で管理する予定のテナントの場合は、アクセス タイプとして **[管理対象 ID（Managed Identity）]** を選択します。 詳細については、Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する （5 ページ）を参照してください。

[プロパティ（Properties）]	説明
Google Cloud Project のセキュリティ ドメインを追加	（注） テナントの作成時の Google Cloud のセキュリティ ドメインの追加はオプションです。 アカウントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[Google Cloud Project のセキュリティ ドメインの追加（Add Security Domain for Google Cloud Project）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。

ステップ 5 設定が終わったら [Save] をクリックします。

次のタスク

Google Cloud で管理対象テナントに必要な構成を完了します。これらの手順については、マネージド テナント用に Google Cloud で必要な権限を設定する （11 ページ） にアクセスしてください。

マネージド テナント用に Google Cloud で必要な権限を設定する

マネージドテナントを作成している場合は、Google Cloud で必要なアクセス許可を設定する必要があります。

（注） アンマネージド テナントを作成している場合は、この手順に従う必要はありません。

ステップ 1 Google Cloud GUI で、このマネージド テナントに関連付けられる Google Cloud プロジェクトにログインします。

プロジェクトの **ダッシュボード** が表示されます。

ステップ 2 左側のナビゲーション バーで、**[IAM & Admin]** をクリックし、**[IAM]** を選択します。

[IAM] ウィンドウが表示され、いくつかのサービス アカウントが表示されます。

ステップ 3 インフラアカウントに関連付けられているプロジェクトで作成されたサービス アカウントを見つけます。

ステップ 4 サービス アカウント名をコピーします。

ステップ 5 このサービス アカウント名を、ユーザー テナント プロジェクトの IAM ユーザーとして追加します。

ステップ 6 このサービス アカウントの権限を設定します。

a) このサービス アカウントの行にある鉛筆アイコンをクリックします。

[権限の編集（Edit Permissions）] ウィンドウが表示されます。

b) **[+別のロールの追加（+ ADD ANOTHER ROLE）]** をクリックし、ロールとして **[クラウド機能サービス エージェント（Cloud Functions Service Agent）]**を選択します。

サービス アカウントが表示された **[IAM]** ウィンドウに戻ります。

c) **[+別のロールの追加（+ ADD ANOTHER ROLE）]** を再度クリックし、このサービス アカウントに必要な残りのロールを追加します。

以下は、このプロセスの最初のステップで追加したクラウド機能サービス エージェントを含む、このサービス アカウントに割り当てる必要があるロールの完全なリストです。

- クラウド機能サービス エージェント
- コンピューティング インスタンス管理（v1）
- コンピューティング ネットワーク管理者
- コンピューティング セキュリティ管理者
- 管理者のログイン
- パブ/サブ管理者
- ストレージ管理者

d) 必要なすべてのロールを追加した後で、**[保存（Save）]** をクリックします。

IAM ウィンドウに戻り、サービスアカウントが表示され、必要なロールがこのサービスアカウントに割り当てられます。

アンマネージド テナントの作成

次のセクションでは、アンマネージド テナントを作成するために必要な情報を提供します。

- Google Cloud からアンマネージドテナントに必要な秘密鍵情報を生成してダウンロードします
- Cisco Cloud Network Controller にアンマネージド テナントを作成する

アンマネージド テナントの Google Cloud からの秘密キー情報の生成とダウンロード

アンマネージド テナントを作成する場合は、最初に Google Cloud から必要な秘密キー情報を生成してダウンロードする必要があります。

（注） マネージド テナントを作成している場合は、この手順の手順に従う必要はありません。

ステップ 1 Google Cloud で、まだ選択されていない場合、アンマネージド テナントに関連付けられる Google Cloud プロジェクトを選択します。

ステップ 2 左側のナビゲーション バーで、**[IAM & Admin]** をクリックし、**サービス アカウント** を選択します。

この Google Cloud プロジェクトのサービス アカウントが表示されます。

ステップ 3 既存のサービス アカウントを選択するか、**[+サービス アカウントの作成（+ CREATE SERVICE ACCOUNT）]** をクリックして新しいアカウントを作成します。

このサービス アカウントの情報が表示され、**[詳細（Details）]** タブがデフォルトで選択されています。

ステップ 4 **[キー（KEYS）]** タブをクリックします。

ステップ 5 **[ADD KEY（キーの作成）]** > **[新しいキーの作成（Create New Key）]**をクリックします。

このサービス アカウントの秘密キーを作成するためのオプションを提供するウィンドウが表示されます。

ステップ 6 **JSON** キータイプを選択したまま、**[作成（Create）]** をクリックします。

秘密キーがコンピュータに保存されたことを示すウィンドウが表示されます。

ステップ 7 コンピュータにダウンロードしたJSONファイルを見つけて、コンピュータ上の安全な場所に移動します。

この JSON ファイルには、管理対象外テナントのフィールドに入力する必要があるキー情報が含まれています。

Cisco Cloud Network Controller GUI を使用したアンマネージド テナントの作成

このセクションでは、GUI を使用して Cisco Cloud Network Controller GUI で管理対象外のテナントを作成する方法について説明します。

始める前に

このセクションの手順を使って続行する前に、アンマネージド テナントの Google Cloud からの秘密キー情報の生成とダウンロード （12 ページ） で説明されている手順を完了します。

ステップ 1 ユーザーテナントの Google Cloud プロジェクトをセットアップします。

これらの手順については、ユーザー テナントの Google Cloud プロジェクトのセットアップ （7 ページ）を参照してください。

ステップ 2 Cisco Cloud Network Controller GUI で、**[アプリケーション管理（Application Management）]** > **[VRF]**に移動します。

すでに設定されているテナントのテーブルが表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[テナントの作成（Create Tenant）]**を選択します。

[テナントの作成（Create Tenant）] ダイアログ ボックスが表示されます。

ステップ 4 次の *[*テナント ダイアログボックス フィールドの作成（*Create Tenant Dialog Box Field*）*]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *3:* テナント ダイアログボックス フィールドの作成

[プロパティ（Properties）]	**説明**
名前（Name）	テナント名を入力します。正規表現の一致: `[az]([-a-z0-9]*[a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。
説明	テナントの説明を入力します。
[設定（Settings）]	
セキュリティ ドメインの追加（Add Security Domain）	テナントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]**をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]**をクリックして、セキュリティ ドメインをテナントに追加します。
Google Cloud Project	

[プロパティ（**Properties**）]	説明
Google Cloud Project ID	この Cisco Cloud Network Controller テナントに関連付けられる Google Cloud プロジェクト ID を入力します。
アクセスタイプ	Cisco Cloud Network Controller で管理されていないテナントの場合は、アクセスタイプとして**[アンマネージド ID（Unmanaged Identity）]** を選択します。 詳細については、Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する （5 ページ）を参照してください。
キーID	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード （12 ページ） でダウンロードした JSON ファイルの `private_key_id` フィールドの情報を入力します。
RSA プライベート キー	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード （12 ページ） でダウンロードした JSON ファイルの `private_key` フィールドの情報を入力します。
クライアントID	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード （12 ページ） でダウンロードした JSON ファイルの `client_id` フィールドの情報を入力します。
電子メール	Google Cloud プロジェクトに関連付けられている E メール アドレスを入力します。

[プロパティ（Properties）]	説明
Google Cloud Project のセキュリティ ドメインを追加	（注） テナントの作成時の Google Cloud のセキュリティ ドメインの追加はオプションです。 アカウントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[Google Cloud Project のセキュリティ ドメインの追加（Add Security Domain for Google Cloud Project）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。

ステップ 5 設定が終わったら [Save] をクリックします。

BGP-EVPN を使用したサイト間接続のための VPC ピアリングの構成

Cisco Catalyst 8000V ルーターを使用してサイト間接続用に BGP-EVPN 接続を構成した場合は、これらの手順に従って、Google Cloud サイト内のユーザー VPC が他のクラウド サイトまたは ACI オンプレミス サイトの VPC と通信できるようにします。詳細については、*Cisco Cloud Network Controller for Google Cloud ユーザー ガイド*の「BGP-EVPN を使用したサイト間接続」セクションの「VPC ピアリング」を参照してください。

通常、VRF を作成してから、その VRF の**ハブ ピアリング**を確認する Nexus ダッシュボード オーケストレータを介して BGP-EVPN を使用して、サイト間接続用に VPC ピアリングを構成します。これらの手順については、該当する Nexus Dashboard Orchestrator のドキュメントを参照してください。

Cisco Cloud Network Controller 側でこの構成を変更するには、次の手順を実行します。

ステップ 1 Cisco Cloud Network Controller GUI で、**[アプリケーション管理（Application Management）]** > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]** に移動します。

ステップ 2 **[名前（Name）]** 列で、オーバーレイ 1 VPC とピアリングする VPC に関連付けられているクラウド コンテキスト プロファイルの名前をダブルクリックします。

このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。

ステップ 3 **[アクション（Actions）]** > **[編集（Edit）]**をクリックします。

ステップ 4 **[VPC ハブ ピアリング（VPC Hub Peering）]** 領域で、**[有効化（Enable）]** の横にあるボックスをクリックして、この VPC の VPC ピアリングを有効にし、**[保存（Save）]** をクリックします。

ステップ 5 Google Cloud で、**[VPC ネットワーク（VPC network）]** > **[VPC ネットワーク ピアリング（VPC network peering）]**に移動します。

ステップ 6 Google Cloud サイトのユーザー VPC がオーバーレイ 1 VPC とピアリングしていることを確認します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。