



# Cisco Cloud Network Controller のインストールの準備

- [Cisco ACI ファブリックをパブリッククラウドに拡張するための要件](#) (1 ページ)
- [Cisco Cloud Network Controller の通信ポート](#) (6 ページ)
- [Cisco Cloud Network Controller のインストールワークフロー](#) (6 ページ)

## Cisco ACI ファブリックをパブリッククラウドに拡張するための要件

Cisco Application Centric Infrastructure (ACI) をパブリッククラウドに拡張するには、その前に、Cisco ACI オンプレミスのデータセンターと AMAZON Web Services (AWS) の展開要件を満たす必要があります。

### オンプレミス データセンターの要件

このセクションでは、(ACI) ファブリックをパブリッククラウドに拡張するためのオンプレミスデータセンター要件を示します。Cisco Application Centric Infrastructure

- ファブリックに次のコンポーネントが取り付けられていることを確認します。Cisco ACI
  - Cisco Nexus 9000シリーズACIモードスイッチソフトウェアリリース14.1以降を実行している、少なくとも2つのCisco Nexus EXまたはFXスパインスイッチ、またはNexus 9332Cおよび9364Cスパインスイッチ。
  - Cisco Nexus 9000シリーズACIモードスイッチソフトウェアリリース14.1以降を実行している少なくとも2台のCisco Nexus pre-EX、EX、またはFXリーフスイッチ。



(注) Cisco Nexus pre-EX リーフ スイッチはサポートされていますが、「[Cisco Nexus 9372PX および 9372TX スイッチの販売終了およびサポート終了のお知らせ](#)」で説明されているように、これらの古い pre-EX リーフ スイッチのサポート終了が発表されているため、EX または FX リーフ スイッチなどの新しい世代のリーフ スイッチを使用することをお勧めします。

- リリース 4.1 以降および Cisco Nexus Dashboard Orchestrator (NDO) リリース 2.2(x) 以降を実行している少なくとも1つのオンプレミス Cisco Application Policy Infrastructure Controller (APIC)。
- Cisco Nexus Dashboard Orchestrator 2.2(x) は基本設定で展開されています。
- インターネット プロトコル セキュリティ (IPsec) を終端できるルータ。
- オンプレミスとクラウドサイト間のテナントトラフィックに十分な帯域幅があることを確認する必要があります。
- オンプレミスサイトのすべてのリーフスイッチに適切な Cisco ACI ライセンスがあることを確認します。
  - Cisco ACI オンプレミス サイトが単一サイトの場合、オンプレミス リーフスイッチには Essentials ライセンス階層 (またはそれ以上) を使用します。
  - Cisco ACI オンプレミス サイトがマルチサイトの場合、オンプレミス リーフスイッチには Advantage ライセンス階層 (またはそれ以上) を使用します。



(注) オンプレミスデータセンターのこれらのライセンス要件は、パブリック クラウドに展開された Cisco Cloud Network Controller の数とは無関係です。Cisco Cloud Network Controller のライセンス要件については、[Cisco Cloud Network Controller およびオンプレミス ACI ライセンスの概要](#) を参照してください。

- ファブリックに接続されているワークロード。Cisco ACI
- ファブリック (スパイン) と IPセキュリティ (IPsec) 終端デバイス間で設定されるサイト間ネットワーク (ISN)。Cisco ACI
 

ISN の作成については、『Cisco APIC Layer 3 Networking Configuration Guide』の「Multipod」の章を参照してください。<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>
- オンプレミス展開と AWS 展開の間にファイアウォールを展開する場合は、特定のファイアウォール ポートを許可する必要があります。これには、Cisco Cloud Network Controller

の HTTPS アクセス、各 AWS CCR の IPsec ポート、AWS CCR リモート管理の SSH 接続が含まれます。

これらのファイアウォールポートについては、このガイドで詳しく説明します。[Cisco Cloud Network Controller の通信ポート \(6 ページ\)](#)

## AWS パブリック クラウドの要件

このセクションでは、パブリック クラウドに (ACI) ファブリックを拡張するための Amazon Web Services (AWS) の要件を示します。Cisco Application Centric Infrastructure

### AWS アカウント

インフラテナント用に1つのAWSアカウントが必要であり、ユーザーテナントごとに1つのAWSアカウントが必要です。



(注) インフラアカウントで実行できる Cloud Network Controller は1つだけです。同じインフラアカウントで複数の Cloud Network Controller を実行することはサポートされていません。

たとえば、2つのユーザーテナントを作成する場合は、3つのAWSアカウントが必要です。各ユーザーテナントに1つのアカウントと、インフラテナントに1つのアカウントが必要です。ユーザーテナントは、信頼できる場合と信頼できない場合があります。詳細は、このガイドの[ユーザーテナントのAWSアカウントのセットアップ](#)を参照してください。

### AWS リソース

AWS 展開の一部として次のリソースが必要です。

- Cisco APIC 5.0 Amazon マシン イメージ (AMI) にアクセスします。



(注) AMI にアクセスするには、Amazon マーケットプレイスで Cisco Cloud Network Controller に登録する必要があります。

- クラウドで実行されるアプリケーションの仮想マシン (VM) として機能する Elastic Cloud Computer (EC2) の2つのインスタンス。
- バーチャルプライベートクラウド (VPC)、サブネット、バーチャルプライベートゲートウェイ (VGW)、インターネットゲートウェイ (IGW)、セキュリティグループ、および実行予定のタスクに基づくリソース。

### CCR

使用可能なライセンスモデルには次の2種類があります。

- BYOL (Bring your own license、独自ライセンス使用)

- PAYG (Pay as You Go、従量制)

## BYOL

AWS マーケット プレイスから CCR Bring Your Own License (BYOL) に登録します。詳細については、[Cisco Cloud Network Controller のライセンスング](#)を参照してください。

Cisco Cloud Network Controller のセットアップ時に定義した帯域幅要件に応じて、適切なサイズで CCR を展開します。

ルータのスループットの値によって、展開する CCR インスタンスのサイズが決まります。スループットの値を大きくすると、より大きな VM が展開されます。CCR ライセンスは、Cisco Cloud Network Controller のセットアッププロセスの一部として設定したスループット構成に基づきます。コンプライアンスのために、Smartアカウントに同等以上のライセンスとAXフィーチャセットが必要です。

AWS アカウントに、インスタンスを展開するための許可された制限があることを確認します。AWS 管理コンソールのアカウント インスタンスの制限は、[サービス (Services)] > [EC2] > Limits から確認できます。

Cisco Catalyst 8000V は、ティアベース (T0/T1/T2/T3) のスループット オプションをサポートしています。次の表に、Cisco Catalyst 8000V 向けのさまざまなルータ スループット設定に使用される AWS EC2 インスタンスを示します。

CCR スループット	AWS EC2 インスタンス
T0 (最大 15M のスループット)	c5.xlarge
T1 (最大 100M のスループット)	c5.xlarge
T2 (最大 1G のスループット)	c5.xlarge
T3 (最大 10G のスループット)	c5.9xlarge

Tier2 (T2) は、Cisco Cloud Network Controller でサポートされるデフォルトのスループットです。

## PAYG

Cisco Cloud Network Controller は Cisco Catalyst 8000V 仮想ルータを使用し、クラウド ネットワーキングのニーズに合わせて一定範囲の AWS EC2 コンピュート インスタンスをサポートします。以下の表は、AWS 上の Cisco Cloud Network Controller でサポートされているクラウド インスタンス タイプを示しています。

AWS EC2 インスタンス	CCR スループット	vCPU の数	メモリ
c5.xlarge	最大 5 ギガビット スループット	4	8 GiB
c5.2xlarge	最大 10 ギガビット スループット	8	16 GiB

AWS EC2 インスタンス	CCR スループット	vCPU の数	メモリ
c5.4xlarge	最大 10 ギガビット スループット	16	32 GiB
c5.9xlarge	最大 10 ギガビット スループット	36	72 GiB
c5n.xlarge	最大 25 ギガビット スループット	4	10.5 GiB
c5n.2xlarge	最大 25 ギガビット スループット	8	21 GiB
c5n.4xlarge	最大 25 ギガビット スループット	16	42 GiB
c5n.9xlarge	最大 50 ギガビット スループット	36	96 GiB

初回セットアップ時に、**[VM タイプ (VM Type)]** フィールドの値を変更すると、上の表にリストされている CCR の他の要素が変更されます。VM サイズの値を大きくすると、スループットが高くなります。

### Elastic IP アドレス

インフラ VPC が展開されているリージョンに少なくとも 9 つの Elastic IP アドレスがあることを確認します。

Cisco Cloud Network Controller には 1 つの Elastic IP アドレスが必要で、CCR ごとに 4 つ必要です。導入地域のアカウントに 9 つ以上の Elastic IP アドレスが許可されていることを確認します。そうでない場合は、AWS のケースを上げて Elastic IP アドレスの数を増やします。10 以上を推奨します。



- (注) アドレスは、関連付け解除された Elastic IP アドレスであってはなりません。9 つの新しい Elastic IP アドレスに十分なリソースが必要です。未使用の Elastic IP アドレスがある場合は、それらを解放できます。

### Cisco Cloud Network Controller

Cisco Cloud Network Controller は、m5.2xlarge AWS インスタンスを使用して展開されます。

アカウントに、このインスタンスを展開できる制限があることを確認します。AWS Management Console : Services EC2 Limits で制限を確認できます。

また、AWS Management Console : Services EC2 NETWORK & SECURITY Elastic IPs で使用されている Elastic IP アドレスの数も確認できます。

## Cisco Cloud Network Controller の通信ポート

Cisco Cloud Network Controller 環境を設定する際は、下記のポートがネットワーク通信に必要であることを注意してください。

- Cisco Nexus Dashboard Orchestrator と Cisco Cloud Network Controller の間の通信用：HTTPS (TCP ポート 443 インバウンド/アウトバウンド)

Cisco Cloud Network Controller には、[セットアップ ウィザード](#)を使用した [Cisco Cloud Network Controller の構成](#) の最初に Cisco Cloud Network Controller にログインするために使用したのと同じ Cisco Cloud Network Controller 管理 IP アドレスを使用します。

- AWS の Cisco Cloud Network Controller で導入されたオンプレミス IPsec デバイスと CCR 間の通信：標準 IPsec ポート (UDP ポート 500 および許可 IP プロトコル番号 50 および 51 のインバウンド/アウトバウンド)

2つの Amazon Web Services CCR の場合、[CCR およびテナント情報の検索](#) で説明されているように、または [サイト間インフラストラクチャの設定](#) の手順に従って ISN デバイス構成ファイルをダウンロードした場合に提供されているように、パブリック IPsec ピアリング IP は 3 番目のネットワーク インターフェイスの Elastic IP アドレスを使用します。

- AWS で Cisco Cloud Network Controller によって導入された CCR を接続して管理する場合は、各 CCR のパブリック IP アドレスへのポート TCP 22 インバウンド/アウトバウンドを許可します。
- ライセンス登録の場合 ([tools.cisco.com](https://tools.cisco.com) へ)：ポート 443 (アウトバウンド) が必要です。
- DNS の場合：UDP ポート 53 アウトバウンド
- NTP の場合：UDP ポート 123 アウトバウンド
- リモート認証 (LDAP、Radius、TACACS+、SAML) を使用する場合は、適切なポートを開きます。
- 認証局を使用する場合は、適切なポートを開きます。

## Cisco Cloud Network Controller のインストールワークフ

### □一

このセクションでは、Cisco Cloud Network Controller をインストールして展開するために必要なタスクの概要について説明します。インストール タスクは、AWS マネジメント コンソール、AWS クラウド形成テンプレート、Cisco Cloud Network Controller セットアップ ウィザード、および Nexus Dashboard Orchestrator を使用して実行します。

1. オンプレミスデータセンターとパブリッククラウドのタスクを含む、すべての前提条件を満たします。

セクション「[Cisco ACI ファブリックをパブリッククラウドに拡張するための要件 \(1 ページ\)](#)」を参照してください。

2. AWS クラウド形成テンプレートを使用して Cisco Cloud Network Controller を展開します。

このタスクには、スタックの作成、テンプレートのアップロード（またはAWSテンプレートURLの提供）、テンプレートパラメータの設定、およびテンプレートの送信が含まれます。それから、Cisco Cloud Network Controller の IP アドレスをキャプチャします。

また、Amazon EC2 SSH キーペアを作成し、AWS Marketplace で Cisco Cloud Network Controller にサブスクライブする必要もあります。

セクション「[AWS での Cisco Cloud Network Controller の展開](#)」を参照してください。

3. セットアップウィザードを使用して Cisco Cloud Network Controller を構成します。

このタスクには、Cisco Cloud Network Controller へのログインと、パブリッククラウドに接続するため Cisco Cloud Network Controller により管理されるファブリックの構成が含まれます。AWS リージョンの選択も追加します。サイト間ネットワーク (ISN) ピアリング用のボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) と OSPF エリア ID を指定し、外部サブネットを追加します。次に、IPsec ピアアドレスを追加します。

セクション「[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。

4. Nexus Dashboard Orchestrator を使用して Cisco Cloud Network Controller を構成します。

このタスクには、Nexus Dashboard Orchestrator GUI へのログイン、オンプレミスとクラウドサイトの追加、インフラストラクチャファブリック接続の構成、およびオンプレミスサイトのプロパティの構成が含まれます。次に、Cisco ACI スパイン、BGP ピアリングを構成し、オンプレミスサイトと AWS Cisco Cloud Network Controller サイト間の接続を有効にします。

セクション「[マルチサイトを介した Cisco Cloud Network Controller の管理](#)」を参照してください。

5. Cisco ACI ポリシーを AWS パブリッククラウドに拡張するため、Cisco Cloud Network Controller を使用します。

「[Cisco Cloud Network Controller GUI のナビゲート](#)」および「[Cisco Cloud Network Controller コンポーネントの構成](#)」の項を参照してください。



## 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。