



## Cisco Mini ACI ファブリック

[新機能および変更された機能 2](#)

[Cisco Mini ACI ファブリックの概要 2](#)

[Cisco Mini ACI の注意事項と制約事項 3](#)

[物理 のインストールと構成 Cisco APIC 4](#)

[仮想アプライアンス：インストールおよび構成 APIC 5](#)

[仮想 APIC のアップグレードまたはダウングレード 13](#)

[Mini ACI のアップグレード 13](#)

[仮想 Cisco APIC の物理への変換 16](#)

[物理 APIC の交換 18](#)

[Mini ACI ファブリックの再構築 18](#)

# 新機能および変更された機能

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

表 1: 新機能：Cisco APIC

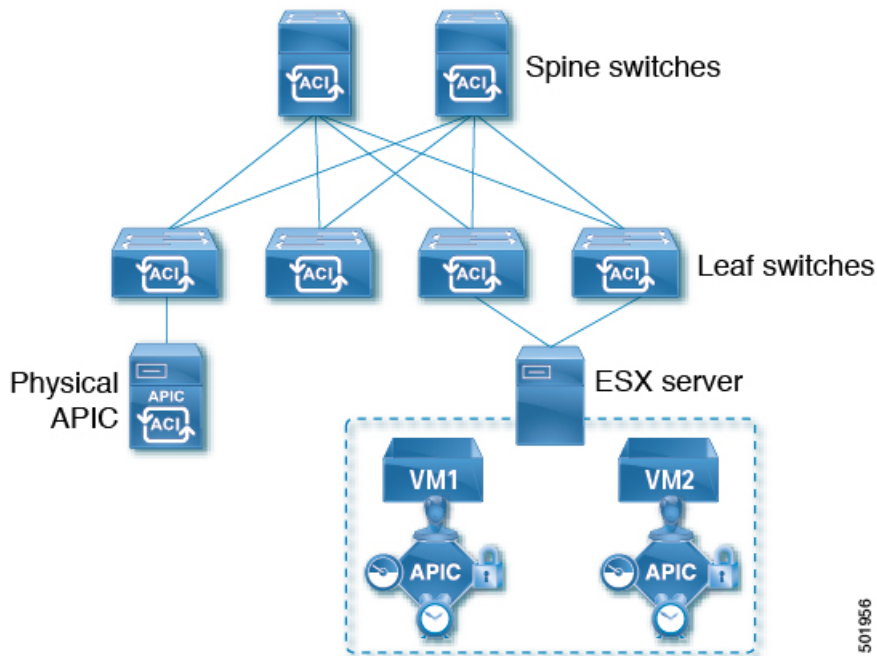
Cisco APIC リリース バージョン	特長	説明
リリース 4.1(1)	Cisco Mini ACI ファブリックおよびマルチサイト。	必要に応じて、LDAP 情報での証明書 の更新を含めるように物理 APIC セク ションを更新しました。
リリース 4.1(1)	Cisco Mini ACI ファブリックおよびマルチサイト。	Cisco Mini ACIおよび vAPIC は、Cisco ACI Multi-Site でサポートされるよう になりました。
リリース 4.0(1)	Cisco Mini ACI ファブリックおよび仮想 APIC。	このガイドは、Cisco Mini ACI および 仮想 APIC 機能のために作成されまし た。

## Cisco Mini ACI ファブリックの概要

Cisco Application Centric Infrastructure（Cisco ACI）リリース 4.0(1) では、Cisco Mini が導入されています。ACI 小規模展開向けのファブリック。Mini ACI ファブリックは Cisco Application Policy Infrastructure Controller（APIC）1つの物理と仮想マシンで実行されている APIC 2 つの仮想（vAPIC）で構成されている APIC クラスタで動作します。これにより、物理フットプリントと Cisco APIC クラスタのコストを削減し、ACI 物理的なフットプリントや初期コストの制約から大規模な導入が現実的でない、コロケーション施設や単一部屋のデータセンターなど、ACI ラック スペースや初期予算が限られたシナリオにおいてもファブリックを展開可能とします。

この図は、物理 1 つと仮想 2 つ台からなる Cisco ACI ミニファブリックの例を APIC 示しています。APIC（vAPIC）：

図 1: Cisco Mini ACI ファブリック



## Cisco Mini ACI の注意事項と制約事項

### Mini ACI ファブリック

- Cisco Mini ACI ファブリックは、Cisco ACI マルチサイトで通常のオンプレミス サイトとしてサポートされます。
- 次の機能はサポートされていません。
  - Cisco ACI マルチポッド
  - Cisco ACI 仮想ポッド
  - リモート リーフ スイッチ
- での アプリケーションのインストールと実行 Cisco Application Policy Infrastructure Controller (APIC) はサポートされていません。
- 物理 APIC および仮想をホストする ESXi サーバ APIC は、同じ NTP サーバと時刻同期されている必要があります。これにより、仮想のアップグレードまたは再起動中に同期の問題が発生しないことが保証されます。APIC として機能し、クラスタは正常に収束します。
- リリース 6.0(2) 以降の UCS ファブリック インターコネクトを含む ACI 中間 APIC スイッチを介して、Cisco Mini 仮想マシンをホストする ESXi ホストを Cisco APIC 接続することはできません。ESXi ホストを Cisco ACI リーフ スイッチに直接接続します。

- Cisco Mini ACI は、リリース 6.0(2) より前のリリースからのポリシーベースのアップグレードは Cisco APIC サポートされていません。
- 6.0(2) リリース以降では、BootX GUI から、1 つの物理 APIC のみ展開します。Cisco APIC 完全に適合した後、すべてのスイッチを追加してから仮想 APIC GUI を使用して、仮想の BootX 展開を構成 APIC 構成します。

## 物理 APIC

クラスタ内の 3 つのうち 2 つが Cisco APIC クラスタは仮想マシンとして ESXi ホスト上で動作する APIC 仮想マシンとして構成可能になりました。まず、物理のインストールと構成が APIC が必要です。物理 APIC では、ファブリック内のスパインおよびリーフスイッチを検出し、インストール中に APIC 仮想を検出し構成し、クラスタのアップグレードを Cisco APIC 促進します。

仮想 APIC では、環境を完全に管理することができますが、Cisco ACI 物理では APIC ファブリック検出を制御します。物理 APIC が使用不可能になる場合、物理的なファブリック変更（スイッチの追加や削除など）は、物理的な復旧が完了するまで APIC 行えません。

## 仮想 APIC

- 仮想の初回起動時 APIC、ブートストラッププロセスの一環として、APIC インフラストラクチャ Cisco ACI VLAN を介して物理デバイスを検出し接続します。仮想 APIC は `pass-phrase`（物理によって生成）を使用し、APIC 物理書によって署名された証明書を取得します APIC。証明書が生成された後、物理および仮想 APIC は検出メッセージを交換し、クラスタを形成します。仮想 APIC は、物理が完了しているとのデータ層の同期後に完全に適合します。APIC します。
- 仮想インバンド管理でインバンド管理を使用する場合 APIC、ノード管理 IP アドレスサブネットとアプリケーション EPG IP アドレス サブネットを同じにすることはできません。

## QoS スケーラビリティの限界

Cisco Mini の場合 ACI ファブリックと仮想 APIC スケーラビリティの制限については、この場所のお使いのリリースの検証済み拡張性ガイドを Cisco APIC 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#Verified\\_Scalability\\_Guides](https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html#Verified_Scalability_Guides)

# 物理 のインストールと構成 Cisco APIC

この手順では、物理 Cisco APIC サーバをインストールおよび構成します。

## 手順

**ステップ 1** 次の **インストールまたは Cisco APIC イメージの回復** の手順に従い、物理サーバを Cisco APIC インストールします。

通常通りに明治されているように、物理 APIC サーバをインストールおよび構成します。ただし、小型のフットプリントの場合、Cisco ACI 物理 APIC サーバをクラスタで最初として選択 Cisco APIC します。

**ステップ2** 物理サーバを構成した APIC 後、以下で説明されているように、クラスタを完了するため APIC 仮想マシンを作成し仮想をインストールします [仮想アプライアンス：インストールおよび構成 APIC（5 ページ）](#)。

---

## 仮想アプライアンス：インストールおよび構成 APIC

仮想アプライアンス：インストールおよび構成 APIC クラスタ内の（vAPIC）は、4 つの手順で構成されています。

- で説明されているインフラ VLAN トランッキング用の ACI リーフ スイッチ ポートの構成 [仮想 APIC インストールの前提条件（5 ページ）](#)。
- で説明されている VMware 標準規格 vSwitch または DVS および ESXi ホストの構成 [仮想 APIC インストールの前提条件（5 ページ）](#)。
- で説明されているように、APIC 物理で生成したパスフレーズの入手 [物理マシンからパスフレーズを取得する APIC（8 ページ）](#)。
- で説明されている各仮想サーバの APIC インストールと構成 [仮想の展開 APIC OVA の使用（9 ページ）](#)。

Cisco では、VMware vCenter を使用して vAPIC 仮想マシンを簡単に展開できるように OVA イメージを提供しています。ただし、物理 APIC と同じ ISO ファイルを使用して、vAPIC を ESXi ホストに直接インストールすることもできます。

### 仮想 APIC インストールの前提条件

#### Cisco ACI ファブリックおよび物理 APIC の展開

リモート対応 APIC 構成の前に、物理 APIC で ACI ファブリックを展開して実行する必要があります。物理 APIC は、ファブリックの検出と、リモート対応 APIC の検出と登録を制御します。

vAPIC の検出と同期は、物理 APIC からの制限された期間のパスフレーズに依存しているため、vAPIC をインストールする前に NTP サーバで物理 APIC を構成して、物理 APIC とリモート対応 APIC 間の潜在的な時間不一致および証明書同期の問題を回避することを推奨します。APIC での NTP の構成については、[コア ACI ファブリック サービスのプロビジョニング Cisco APIC 基本構成ガイド、リリース 4.x](#)）を参照してください。vAPIC 展開の物理 APIC から現在のパスフレーズを取得します。

#### リーフ スイッチ ポートとインフラ VLAN トランッキング

物理およびリモート対応 APIC は、インフラ VLAN Cisco ACI を介してお互いに検出および通信します。リーフ スイッチは、vAPIC リモート対応マシンの ESXi ホストに接続されたポートでインフラ VLAN を有効にする必要があります。これを実現するには、リーフ ポートのアタッチ可能なアクセス エンティティ プロファイル（AEP）でインフラ VLAN を有効にします。

以下で説明されているように、物理 APIC GUI からこれらの変更を行います [使用した vAPIC のリーフ スイッチ ポートの構成 Cisco APIC GUI（7 ページ）](#)。

## ESXi ホストおよび仮想マシン

これらは、vAPIC のESXiホスト、 vCenter、およびリモート対応マシンの要件です。

- ESXiホストは、VMware ESXiバージョン 7.0 以降を実行している必要があります。
- ESXiホストとリモート対応マシンがvCenterによって管理されている場合は、vCenterがバージョン 7.0 以降を実行している必要があります。
- vAPIC は、インフラ VLAN を介して物理 APIC と通信する必要があります。次のいずれかに該当する必要があります。
  - ESXi ホストは Cisco ACI リーフスイッチまたはリーフ スwitchの vPC ペアに直接接続されます。
  - ESXi ホストには正しい UTC 時刻が構成されている必要があります。
  - vAPIC は、最初に起動して物理 APIC に接続したときに、ホストの時間を使用します。重大な時刻の不一致は、証明書の同期の問題の原因となります。
- ESXiホストには、vAPIC リモート対応マシンをホストするために十分なリソースが必要です。各 VM には以下が必要です。
  - **メモリ** : 96 GB
  - **CPU** : 16
  - **HDD 1** : 300<sup>1</sup> GB  
標準規格の HDD を仮想イメージインストールで APIC 使用できます。
  - **HDD 2** : 100<sup>1</sup> GB SSD  
仮想データストアには、高性能の 2 番目のストレージデバイスが APIC 必要です。
  - **NIC 1 (VMXNET 3)** : アウトオブバンド
  - **NIC 2 (VMXNET 3)** : ACI インフラ VLAN トランッキング
- VMware vCenter GUIの[分散スイッチ (Distributed Switch)]設定で、検出プロトコルの[無効 (**Disabled**)]オプションを選択します。これにより、リーフ スwitchは LLDP パケットを APIC から直接受信できます。LLDP は、ゼロタッチ ファブリック検出に使用されます。
- VMware vCenter GUIの Distributed Port Group 設定で、インフラ VLAN で VLAN -0 を許可します。これにより、DVS が LLDPパケットを転送できるようになります。

<sup>1</sup> vAPIC を展開する場合、ESXi ホストには少なくとも 600 GB のストレージの合計（スワップ領域を含む）が必要です。初期展開後、リストされているストレージサイズで十分です。



---

(注) 現在のリリースは、vAPIC リモート対応マシンの vMotion をサポートしていません。

---



## 仮想スイッチの構成

仮想 APIC は、VMware DVS および標準規格の vSwitch をサポートします。リーフ スイッチ ポートと ESXiホストの構成に加えて、仮想スイッチと ESXi ホストの構成も行います。

- 新しい仮想スイッチを作成するか、既存の仮想スイッチを使用します。仮想スイッチは、標準規格のvSwitch または DVS のいずれかです。
- VMMドメイン統合の場合、DVS は APICによって vCenter に作成されています。vAPIC はこの DVS を使用できません。
- 他のデータ VLANに加えて、ACI インフラ VLAN の VLAN トランッキング用に仮想スイッチアップリンクを構成します。
- ACI リーフ スイッチに接続されている ESXi ホスト vmNIC をアップリンクに追加します
- ポート グループを作成し、ACI インフラ VLAN の VLAN トランッキングに構成します。
- 分散型スイッチでは、「設定の編編集」ユーザーは、接続された LEAF が APIC から LLDP パケットを直接受信できるように、[検出プロトコル (Discovery Protocol)] を無効にする必要があります。

VMMドメイン統合の場合、上記のポートグループは VMM 統合によって作成できます。APIC GUI で、[仮想ネットワーク (Virtual Networking)] > [VMware VMMdomain] > [ポリシー (Policy)] > [全般 (General)] に移動し、[インフラ ポートグループの構成 (Configure Infra Port Groups)] ボックスをチェックします。これにより、次のような名前のポートグループ `Infra` が vCenter の VMM ドメイン DVS で自動的に作成されます。。ただし、このポートグループは、VLAN タイプで作成され、vSphereクライアントを使用し手動で VLAN トランッキング ポート グループの設定で変更する必要があります。

ACIと VMM 統合のないvCenterの場合は、vCenter UI の左側のパネルで、[ネットワーク (Networking)] > [VDS] に移動します。次に、右側のパネルの[ネットワーク (Networks)] > [分散型ポートグループ (Distributed Port Groups)] で[新しい管理分散ポートグループ (New Distributed Port Group)] をクリックします。最後に、ポップアップ ウィンドウで、手順に従って、[VLAN トランッキング (VLAN trunking)] を指定するポートグループを [VLAN タイプ (VLAN type)] に作成し、[VLAN トランク範囲 (VLAN trunk range)] にインフラ VLAN ID を作成します。

vCenterを使用せずにESXi サーバに vAPIC を直接インストールする場合は、代わりに ESXiでVMware Standard vSwitch を構成します。vSphere Client の左側のナビゲーションバーで、[構成 (Configuration)] タブを選択します。次に、[ネットワーク (Networking)] を選択します。最後に、vSwitch[VLANID (オプション) (VLANID(Optional))] プロパティで、[すべて (All)] (<VLAN-ID>) を選択し、<VLAN-ID> ファブリック `Infra` VLAN と置き換えます。

DVS スイッチがLLDPパケットを転送できるように、両側でVLAN -0 を許可します。

## を使用した vAPIC のリーフ スイッチ ポートの構成 Cisco APIC GUI

GUI を使用して Cisco APIC vAPIC が接続されているリーフ スイッチポートの必要な `Infra` を構成します。



- (注) vAPIC が接続されているスイッチポートがファブリックですでに使用されている場合は、アクセスエンティティ プロファイルのこれらのポートでインフラVLANを有効にします。[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] > [ポリシー (Policies)] > [グローバル (Global)] > [接続<AEP-name>可能アクセス エンティティ プロファイル (Attachable Access Entity Profiles)] チェックボックスを使用します。

## 手順

---

**ステップ 1** 物理 APIC GUI にログインします。

**ステップ 2** メニュー バーから **[システム (System)]** > **[コントローラ (Controllers)]** に移動します。

**ステップ 3** 左側のナビゲーション パネルを使用して、**クイック スタートの > 仮想 APIC の追加** に移動します。

**ステップ 4** **[仮想 APIC の追加 (Add Virtual APIC)]** をクリックします。

**ステップ 5** vAPIC の接続先であるリーフ スイッチを指定します。

設定する項目は次のとおりです。

- APIC と CSSM 間の後続の通信では、**[リーフ スイッチ – リーフ 1 (Leaf Switches – Leaf 1)]** ノードとポートで、vAPIC が接続されているリーフ スイッチとポートを指定します。
- (任意) **[リーフ スイッチ : leaf2 (Leaf Switches – Leaf 2)]** ノードとポートで、vAPIC が接続されている 2 つのリーフ スイッチとポートを指定します。

**ステップ 6** 追加する vAPIC の vCenter 情報を指定します。

追加する vAPIC が VMware vCenter を使用してインストールされている場合は、ここに情報を入力します。

- **[VMM ドメイン (VMM Domain)]** **f r**、既存の VMM ドメインを選択するか、一意の名前を指定して新しい VMM ドメインを作成します。
- **[ユーザー名 (Username)]**、**[パスワード (Password)]**、および **[パスワードの確認 (Confirm Password)]** では、vCenter ログイン情報を指定します。
- **[ホスト名 (または IP アドレス) (Host Name (or IP Address))]** の場合、vCenter のホスト名または IP アドレスを指定します。
- **[データセンター (Data center)]** の場合、vAPIC が配置されている vCenter のデータセンターを指定します。

**ステップ 7** **[送信 (Submit)]** をクリックして変更を保存します。

---

## 物理マシンからパスフレーズを取得する APIC

このセクションでは、仮想マシンがクラスタに参加するために必要な自動生成されたパスフレーズの取得方法について APIC 説明します。

## 手順

---

**ステップ 1** 物理にログインします APIC。

**ステップ 2** **[システム (System)]** > **[システム設定 (System Settings)]** に移動します。

**ステップ 3** 左側のサイドサイドバーで、**[APIC パスフレーズ (APIC Passphrase)]** を選択します。



次の [現在のセキュアなパスフレーズ (Current Passphrase) ] の文字列は、仮想インストール中に入力する必要がある現在アクティブな APIC パスフレーズです。

(注)

このパスフレーズは、物理的に自動的に生成され、APIC 60 分後に期限切れになります。仮想 APIC 展開が 60 分以上遅延すると、パスフレーズが期限切れになり、無効になります。この場合は、新しいパスフレーズを入手します。上記の手順に活用。

---

## 仮想の展開 APIC OVA の使用

手順に従って、仮想マシン内で Cisco APIC インストールします。

### 始める前に

の説明に従って、ESX ホストとリモート対応マシンを [仮想 APIC インストールの前提条件 \(5 ページ\)](#) 構成します。

### 手順

---

**ステップ 1** 仮想 OVA イメージを Cisco APIC ダウンロードします。

a) ソフトウェア ダウンロード ページ リンクを参照します：

<https://software.cisco.com/download/home/285968390/type>

b) 登録手続きを開始するには、[APIC ソフトウェア (APIC Software) ] をクリックします。

c) リリース バージョンを選択し、仮想 Cisco APIC VMware vCenter サーバからアクセス可能な場所に OVA イメージを転送します。

**ステップ 2** VMware vCenter にログインします。

**ステップ 3** 仮想が展開されている ESXi ホストを Cisco APIC 右クリックし、[OVF テンプレートの展開 (Deploy OVF Template) ] を選択します

**ステップ 4** 仮想 Cisco APIC OVA ファイルを選択して、[次へ (Next) ] をクリックします

**ステップ 5** イメージをインストールするデータセンターまたはフォルダを選択し、[次へ (Next) ] をクリックします。

**ステップ 6** 詳細を確認し、[次へ (Next) ] をクリックして続行します。

**ステップ 7** 仮想データストアのストレージデバイスを Cisco APIC 指定します。

a) OVF テンプレートの展開の [ストレージの選択 (Select Storage) ] ステップで、ウィンドウの右下隅にある [詳細 (Advanced)] をクリックします。

b) 次の [ストレージ (Storage) ] デバイス ([SSD ストレージ (SSD Storage) ] ディスク グループ) を選択します。

次の SSD ストレージデータストアに、100 GB 以上の空き容量がある高性能ストレージデバイス (SSD) を選択します。

- c) 次の [ストレージ (Storage) ] デバイス ( [他のすべてのディスク (All other disks) ] ディスク グループ) を選択します。

仮想メイン イメージに対して少なくとも 300 GB の使用可能なストレージデバイスを Cisco APIC 選択します。

- d) [次へ (Next) ] をクリックして続行します。

**ステップ 8** 環境に応じてアウトオブバンド (OOB) ネットワークとインフラ ネットワークを指定します。

OVF テンプレートの展開の [ネットワークの選択 (Select networks) ] OVF テンプレートの展開のステップで、。必要なネットワークを選択してから、[次へ (Next) ] をクリックして続行します。

**ステップ 9** 「ファブリックの詳細」を参照してください。

OVF テンプレート展開の [テンプレートのカスタマイズ (Customize template) ] ステップで、次の詳細情報を入力します。

- [コントローラ ID (Controller ID) ] : 構成するコントローラの ID。コントローラ ID は 2 または 3 であり、これは構成する 2 番目または 3 番目のコントローラのどちらであるかによって異なります。次の 1 のコントローラ ID 値は、前のセクションの説明に従って Cisco APIC 物理的に予約されます。
- [TEP プール (TEP Pool) ] : TEP アドレスのプール。
- [TEP ネットマスク (TEP Netmask) ] : TEP アドレスのネットマスク。
- [VLAN id] : インフラ ネットワークに使用される VLAN ID。
- [IPv4 OOB IP アドレス (IPv4 OOB IP Address) ] : このコントローラのアウトオブバンド管理用の IP アドレス。
- [IPv4 ネットワーク マスク (IPv4 OOB network mask) ] : これは、アウトオブバンド管理ネットワーク上で行われます。
- [IPv4 ゲートウェイ (IPv4 gateway) ] : アウトオブバンド ネットワークのゲートウェイ アドレス。
- [パスフレーズ (Passphrase) ] : 次の [物理マシンからパスフレーズを取得する APIC \(8 ページ\)](#) 取得したパスフレーズ

(注)

60 分後に自動的に期限切れになります。VM の構成と OVA の展開に時間がかかる場合は、物理 Cisco APIC から新しいパスフレーズを取得します。VM のプロパティの [vApp のオプション (vApp Options) ] タブで、VM を構成した後、パスフレーズを更新します。この場合、上記の手順を使用して現在のパスフレーズを取得し、そのパスフレーズをリモート対応 Cisco APIC VM に対する admin (Windows の場合) または sudo (Linux の場合) 特権を持っている必要があります。パスリモート対応を再適用する前に、Cisco APIC この手順を使用する VM :

- a) 「rescue-user」アカウントを使用する 仮想 Cisco APIC VM のコンソールにログインします。
- b) 次の **acidiag touch clean** コマンドの後に **acidiag touch setup** コマンドを使用します。
- c) VM の電源をオフにします。
- d) 仮想 Cisco APIC VM で、[設定の編集 (Edit Settings) ] を右クリックして選択します。

- e) 次の**VM オプション**>**vApp** プロパティを使用して、次から取得した更新されたパスフレーズを入力します Cisco APIC。
- f) 仮想 Cisco APIC VM を電源オンにします。

**ステップ 10** 展開の詳細を確認し、**終了 (Finish)** をクリックし、仮想を展開します Cisco APIC。

**ステップ 11** OVA の展開プロセスが完了したら、仮想 Cisco APIC VM を開始します。

VM が起動すると、仮想 APIC は、物理と通信し、Cisco APIC クラスタに参加します。

(注)

初期仮想 Cisco APIC 起動と同期が完了するまでに数分かかる場合があります。

---

インストールが完了したら、仮想 Cisco APIC は、トポロジ図の特別なアイコンで識別されます。

### 次のタスク

仮想 Cisco APIC がインストールされ、クラスタに追加され、*Cisco APIC* 開始ガイドおよび *Cisco APIC* 基本構成ガイドの説明に従って残りの環境をセットアップします。

## 仮想の展開 APIC ESXi で直接アクセス

次の手順に従って、vAPIC をESXiホスト内に直接インストールします。この vAPIC インストールでは、物理 APIC インストールと同じ ISO ファイルを使用します。

### 始める前に

の説明に従って、ESX ホストとスイッチを [仮想 APIC インストールの前提条件 \(5 ページ\)](#) 構成します。

### 手順

---

**ステップ 1** ISO イメージをダウンロードします。

- a) ソフトウェア ダウンロード ページ リンクを参照します：  
<https://software.cisco.com/download/home/285968390/type>
- b) **[APIC ソフトウェア (APIC Software)]** をクリックします。
- c) リリースバージョンを選択し、APIC イメージ (iso) をダウンロードし、ESXi サーバからアクセス可能な場所に配置します。

**ステップ 2** APIC ISO イメージを ESXi ホストにコピーします。

**ステップ 3** vSphere クライアントを使用して VMware ESXi ホストにログインします。

**ステップ 4** vAPIC をインストールする仮想マシン (VM) を作成します。

VM のハードウェア要件は [仮想 APIC インストールの前提条件 \(5 ページ\)](#) のとおりです。

**ステップ 5** vAPIC をインストールする VM のブート イメージとしてダウンロードした APIC ISO イメージを指定し、VM の電源をオンにします。

インストールは、物理 APIC の場合と同様に進みます。インストールが完了すると、VM はシャットダウンされます。

**ステップ 6** VM の電源を投入します。

**ステップ 7** vAPIC の初期ブート中にファブリック情報を提供します。

vAPIC VM の初回起動時に、設定を完了するために次のファブリック情報が要求されます。

- ファブリック名
- ファブリック ID
- アクティブなコントローラの数
- ポッド ID

次の **1** という回答は、1 つの POD のみが現在ミニACIファブリックでサポートされているためです。

- スタンバイコントローラかどうか

次の **NO** という回答は、アクティブなコントローラを構成しているためです。

- APIC であるかどうか -X

次の **NO** という回答は、vAPIC は APIC-X ではないためです。

- コントローラ ID

構成するコントローラの ID。コントローラ ID は 2 または 3 であり、これは構成する 2 番目または 3 番目のコントローラのどちらであるかによって異なります。次の 1 のコントローラ ID 値は、前のセクションで APIC インストールされている物理に予約されます。

- コントローラ名

vAPIC のホスト名。

- TEP アドレスのプール
- インフラ ネットワークの VLAN ID
- アウトオブバンド管理情報
- 物理 APIC からのパスフレーズ

取得したパスフレーズ [物理マシンからパスフレーズを取得する APIC \(8 ページ\)](#)

(注)

60 分後に自動的に期限切れになります。vAPIC 展開のこの段階で、物理 APIC の現在のパスフレーズを取得することを推奨します。

(注)

Cisco APCI リリース 6.0(2)以降、ブートストラップとクラスタの起動には、クラスタのブリングアップ GUI を使用するか、API を使用します。次の GUI を使用した APIC クラスタの呼び出し 手順に関する詳細は、APIC スタートアップガイドを参照してください。API を使用したクラスターの立ち上げの詳細については、CISCO DCNM API リファレンス ガイドを参照してください。

**ステップ 8** 入力した詳細が正しいことを確認し、展開を続行します。

展開プロセスが完了すると、仮想 APIC は、物理と通信し、APIC クラスタに参加します。

(注)

最初の vAPIC の起動と同期は、完了するまでに数分かかることがあります。

---

インストールが完了したら、仮想 Cisco APIC は、トポロジ図の特別なアイコンで識別されます。

### 次のタスク

仮想 Cisco APIC がインストールされ、クラスタに追加され、『*Cisco APIC Getting Started Guide*』および『*Cisco APIC Basic Configuration Guide*』。

## 仮想 APIC のアップグレードまたはダウングレード

仮想サーバを直接アップグレード APIC しません。物理は通常通り APIC アップグレードし、その後物理マシンが APIC アップグレードイメージを復号化して仮想マシンに送信し、APIC アップグレードを実行します。

物理サーバのみのクラスタの Cisco ACI アップグレードまたはダウングレードに使用するのと同じ ISO イメージを使用して、APIC 物理サーバのみのクラスタをアップグレードまたは APIC ダウングレードします ([Cisco APIC およびスイッチ ソフトウェアのアップグレードとダウングレード](#) を参照)。



---

(注) 4.0(1) より前のバージョンにダウングレードすることは Cisco APIC サポートされていません。

---

## Mini ACI のアップグレード

次の手順を使用し、Mini ACI を Cisco Application Centric Infrastructure (ACI) リリース 6.0(1) 以前からリリース 6.0(2) 以降へアップグレードします。

### 制限事項

- 次の Cisco Application Policy Infrastructure Controller (APIC) リリース 6.0(2) にアップグレードする場合、リリース 6.0(2) より前のリリースへのダウングレードはサポートされていません。
- 物理ホスト 1 つと APIC 仮想ホスト 2 つのみをサポート APIC (ESXi ホスト上)。
- リリース 6.0(2) 以前のリリースから ACI ポリシーベースのアップグレードは Mini で Cisco APIC サポートされていません。
- VMM ドメインが仮想 VLAN で有効になっている DVS で APIC インスタンスが展開されていない場合、その DVS ドメインの 6.0.2 へのアップグレード後は、CDP 隣接関係のみがサポートされます。

## 始める前に

詳細については、[前提条件](#) セクションを参照してください。

## 手順

---

- ステップ 1** [Mini] になっていることを確認します。ACI クラスタは正常です。
- acidiag avread**、**show version**、**show controller** コマンドを使用して確認します。
- ステップ 2** 次の Cisco APIC GUI で、クラスタ サイズを 3 から 1 に減らします。コマンドを使用して **acidiag avread** 確認します。
- ステップ 3** 仮想クラスタの APIC ノード 3 をデコミッションします。デコミッションが完了するまで数分待ちます。
- 詳細については、*Cisco APIC* クラスタの管理（スタートアップ ガイド）の章を参照してください。  
[GUI 手順を使用して、クラスタ内の Cisco APIC コントローラの デコミッション](#)
- ステップ 4** 仮想クラスタのノード 2 を APIC デコミッションします。デコミッションが完了するまで数分待ちます。
- 詳細については、*Cisco APIC* クラスタの管理（スタートアップ ガイド）の章を参照してください。  
[GUI 手順を使用して、クラスタ内の Cisco APIC コントローラの手順](#)を参照してください。
- ステップ 5** VMware vCenter GUI を使用して、リモート対応の以前のインスタンス（ノード 2、3）を削除します。APIC（Cisco Umbrella Enforcement API を実行している Cisco APIC 6.0(2) より前のソフトウェア リリース）。
- ステップ 6** 拒否して削除します Cisco APIC（必要な場合）。
- Cisco APIC GUI で、[システム (System)] > [コントローラ (Controllers)] に移動します。[ナビゲーション (Navigation)] ペインで、[コントローラ (Controllers)] > *apic\_controller\_name* > [ノードで表示されるクラスタ (Cluster as Seen by Node)] を展開します。存在する場合 Cisco APIC は、[未承認のコントローラ (Unauthorized Controllers)] 承認済み状態になっており、そのコントローラに対して拒否および削除アクションを実行します。
- ステップ 7** 次の **acidiag avread** および **show controller** コマンドを実行して、クラスタ サイズが 1 であることを確認します。これらのコマンドは、単一の物理を持つ ACI Mini の正常性も示します APIC。
- ステップ 8** 物理 APIC を リリース 6.0(2) にアップグレードします。これには数分かかる場合があります。
- 注意**  
アップグレードが完了したことを確認してから次のステップに進みます。
- acidiag avread**、**show version**、**show controller** コマンドを使用して確認します。
- ステップ 9** ファブリック ノード（リーフおよびスパイン スイッチ）をリリース 6.0(2) にアップグレードします。
- acidiag avread**、**show version**、**show controller** コマンドを使用して確認します。
- (注)  
すべてのファブリック ノードと APIC 1（物理 APIC）は、他のを展開する前に 6.0(2) にアップグレードされます Cisco APIC。



## ステップ 10 ノード 2 および 3 の仮想 APICVirtual を展開します。

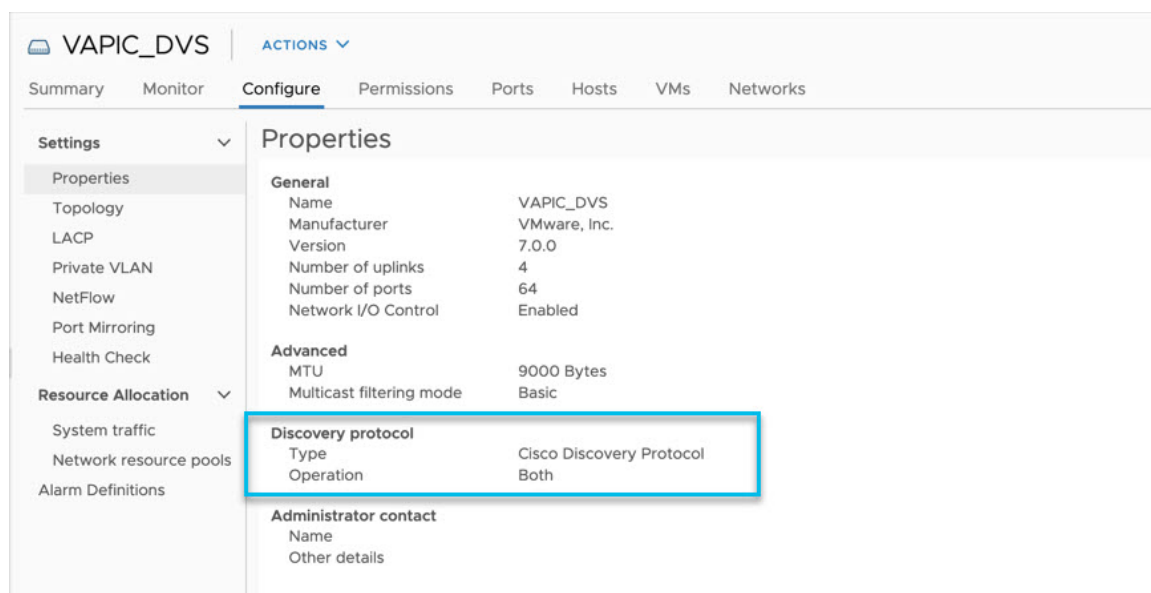
詳細な手順については、[VMware vCenter を使用した仮想 APIC の展開](#) を参照してください。

続行する前に展開のステータスを確認します。vCenter GUIで、 の下のステータスをチェックして、展開が成功したことを確認します。[モニタ (Monitor) ] タブに表示されるフィールドとアイコンについて説明します。

- Cisco APIC GUI、インターフェイス ポリシー グループで CDP を有効にします。次の [ファブリック (Fabric) ] > [アクセス ポリシー (Access Policies) ] > [インターフェイス (Interfaces) ] > [VPC インターフェイス (VPC Interface) ] に移動し、 の仮想ポートチャネルを [リンク集約タイプ (Link Aggregation Type) ] フィールドに選択します。 [CDP ポリシー (CDP Policy) ] フィールドで、 `system-cdp-enabled` オプションを選択します。
- CDP を有効にし、LLDP を無効にするには、VMM ドメインに基づいて、次のいずれかのオプションを使用します。

- VMM ドメインが構成されていません。VMware vCenter GUI を使用して、CDP を有効にし LLDP を無効にします。

ポート グループとして、VLAN 0 を追加して LLDP パケットを許可します。



- VMM ドメインが次のように構成されています。Cisco APIC GUI で、VMM ドメインが仮想 ESXi ホストに接続されたインターフェイスで構成されている場合に、VMM ドメインの vSwitch ポリシーを変更して CDP を有効にし、APIC LLDP を無効にします。詳細は次のとおりです。

- vSwitch ポリシーで CDP を有効にします。次の [仮想ネットワーク (Virtual Networking) ] > [VMware] > [VMM ドメイン (VMM Domain) ] > [vSwitch ポリシー (vSwitch Policy) ] に移動します。
- LLDP ポリシーを Rx のみに変更します。次の場所に移動します。[ナビゲーション (Navigation) ] ペインで、[ファブリック (Fabric) ] > [アクセス ポリシー (Access Policies) ] > [ポリシー (Policies) ] > [インターフェイス (Interface) ] > [LLDP インターフェイス (LLDP Interface) ]

> > > の順に選択します。 [有効 (Enabled)] オプション ([受信状態 (Received State)] および [無効 (Disabled)] オプション [送信状態 (Transmit State)] を選択します。

3. CDP 隣接関係が学習されたことを確認します。

```
sw1-leaf1# show cdp nei interf eth1/37
```

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater,  
V - VoIP-Phone, D - Remotely-Managed-Device,  
s - Supports-STP-Dispute
```

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
sw1-esx4	Eth1/37	147	S	VMware ESX	vmnic2

4. LLDP を使用した vSwitch ポリシーを [無効化 (Disabled)] を変更します。
5. VMware vCenter GUI を活用、LLDP パケットを許可するポート グループに VLAN 0 を追加します。

**ステップ 11** 仮想 APIC インスタンス 2 および 3 の電源をオンにします。表示される IP アドレスは展開中に使用される仮想 APIC インスタンス IP アドレスです APIC。展開が正常に完了したことを確認するには、次のメッセージが表示されます。

```
System pre-configured successfully.  
Use: https://<VAPIC INSTANCE IP ADDRESS> to complete the bootstrapping.
```

**ステップ 12** 仮想 APIC をクラスタに追加します。

物理の GUI Cisco APIC で APIC 次の [システム (System)] > [コントローラ (Controller)] に移動します。次の [コントローラ (Controllers)] > [apic\_name] > [ノードで表示されるクラスタ (Cluster as Seen by Node)] を展開し選択します。詳細な [ノードの追加 (Add Node)] ノード 2 と 3 を追加する手順については、Cisco APIC クラスタの管理 (スタートアップ ガイド) の章を [ノード追加オプションを使用した APIC クラスタの拡大](#) の手順でインストールします。

両方のノードを追加したら、しばらく待ってからクラスタが [完全に適合 (Fully Fit)] するか確認します。

**ステップ 13** Mini ACI クラスタが正常であることを確認します。

**acdiag avread**、**show version**、**show controller** コマンドを使用して確認します。

---

## 仮想 Cisco APIC の物理への変換

### 6.0(1) 以前のリリースで仮想 APIC を物理に変換する

クラスタ内の仮想 Cisco Application Policy Infrastructure Controller (APIC) サーバを 1 台ずつ Cisco APIC 物理サーバに変換します。

変換中に、クラスタが2つの物理ノードと1つの仮想ノードを含む APIC 短い期間が生じます APIC。このような組み合わせはこれらのリリースではサポートされていませんが、Mini ACI を物理フォーム ファクタのクラスタで構成される APIC 通常の ACI ファブリックに変換する目的でのみ許可されます。

## 手順

---

**ステップ 1** クラスタから Cisco APIC 仮想 3 をデコミッションします。 [GUI を使用したクラスタでの Cisco APIC のデコミッション](#) 章（Cisco APIC 開始ガイド）を参照してください。

**ステップ 2** 新しい物理 Cisco APIC を APIC クラスタに 3 として追加します。これは、 [GUI を使用したクラスタでの Cisco APIC のデコミッション](#) 章（Cisco APIC 開始ガイド）で説明されています。

**ステップ 3** 2 についても同じことを APIC 繰り返します。

---

## 6.0(2) リリース以降で仮想APIC を物理に変換

最初にクラスタの仮想 Cisco Application Policy Infrastructure Controller (APIC) サーバを最初に削除し、次に 2 つの物理 Cisco APIC サーバを一度に削除します。

6.0(2) リリース以降、APIC すべて仮想サーバを持つクラスタ APIC がサポートされています。ただし、これらのリリースでは、Mini ACIを除き、同じクラスタ内の仮想と物理の混合はサポートされていません（1 つの物理、2 つの仮想は制限されています）。これにより、6.0(2) リリース以降のすべての物理 APIC で Mini ACI を通常の ACI ファブリックに変換する手順が変更されました。

Mini ACI を通常の ACI ファブリックに直接変換し、APIC 物理 1 をすべての仮想 s で置き換える操作は、APIC これらのリリースで認定されておらず、以下の手順の範囲ではありません。

## 手順

---

**ステップ 1** 以下の説明に従い、クラスタから仮想 APIC Cisco 2 および 3 の両方を削除します。 [ノード削除オプションを使用した APIC クラスタの縮小](#)（Cisco APIC 開始ガイド）。

[ノードの削除 (Delete Node)] 操作で APIC 両方のノードを選択して、2 および APIC 3 の両方を **削除する必要があります**。これは、3 クラスタの 1 つのノードのみを APIC 削除することができないためです。 [ノード削除オプションを使用した APIC クラスタの縮小](#)（Cisco APIC 開始ガイド）で説明されています。

**ステップ 2** クラスタに物理的な APIC Cisco スイッチを APIC 2 および APIC と 3 として追加します。これは、 [ノード追加オプションを使用した APIC クラスタの拡大](#)（Cisco APIC 開始ガイド）で説明されています。

ステップ 1 の削除操作と同様に、APIC 2 および APIC 3 を同時に追加する必要があります。

---

## 物理 APIC の交換

6.0(1) 以前のリリースでは、この物理の手順を使用して、Cisco Application Policy Infrastructure Controller (APIC) を置き換えます。

Cisco APIC 6.0(2) 以降のリリースで、**vapicjoin** コマンドはサポートされていません。ただし、この手順を使用する必要はありません。BootX が物理的な証明書を Cisco APIC 自動的に更新するためです。

### 手順

---

**ステップ 1** 通常通りに新しい物理 Cisco APIC をインストールします。

物理 のインストーと構成 Cisco APIC Mini ACI ファブリックの については、[物理 のインストールと構成 Cisco APIC \(4 ページ\)](#) で説明されています

**ステップ 2** 新しい物理の証明書を更新 Cisco APIC します。

いずれかの仮想から証明書を取得すると、Cisco APIC 新しい物理 Cisco APIC で通信できます。

このコマンドでは、次のように置き換えます。

- `<vapic-ip>` いずれかの vAPIC の IP アドレスを使用します。
- `<vapic-password>` IP を指定した vAPIC の管理者パスワードを使用します。
- `admin` は `apic local admin` です。LDAP または他の認証方式を使用している場合は、`acidiag vapicjoin` コマンドを実行する前に、AAA レルムを LDAP からローカルに変更します。

例 :

```
# acidiag vapicjoin -n <vapic-ip> -u admin -p <vapic-password>
```

---

## Mini ACI ファブリックの再構築

この手順により、ミニ ACI ファブリックを再構築（再初期化）できます。これは、次のいずれかの理由で必要になる場合があります。

- TEP IP を変更するには
- インフラ VLAN を変更するには
- ファブリック名を変更するには
- TAC トラブルシューティング タスクを実行するには

この手順により、Cisco APIC で構成を消去します。完全なファブリックの再構築を実行する場合は、すべてのファブリックの APIC 手順を実行します。あるいは、これらの手順を使用して仮想環境のみを APIC 転送されます。再構成す

ることもできます。仮想構成の再構築は、APIC 例えば初期構成に問題があり仮想 APIC がクラスタに参加できない場合などにのみ選択できます。

## 始める前に

次の点を確認してください。

- 定期的にスケジュールされた構成のバックアップ
- 物理用に構成された到達可能な CIMC Cisco APIC コンソール アクセス
- 仮想の仮想コンソール アクセス Cisco APIC

## 手順

---

**ステップ 1** (オプション) 既存の構成をバックアップします。

現在の構成を保持したい場合は、[構成ファイルのインポートとエクスポート](#)で説明されているように構成のエクスポートを実行します。

**ステップ 2** 構成の消去 Cisco APICの構成を消去します。

構成は消去するが、ファブリック情報は保持する場合：

例：

```
# acidiag touch clean
```

構成を消去してファブリック情報を変更するには、次の手順を実行します。

例：

```
# acidiag touch setup
```

**ステップ 3** vAPIC をシャットダウンします。

**ステップ 4** を再構成します。APIC物理を再構成します。

次の touch setup または touch clean 操作を仮想 Cisco APIC でのみ実行するには、このステップをスキップしてください。

a) 物理 APIC をリブートします。

例：

```
# acidiag reboot
```

b) 次のセットアップ スクリプトを実行します。

例：

```
# setup-clean-config.sh
```

c) 物理 APIC をリロードします。

例：

```
# reload
```

**ステップ 5** vAPIC VM を再構成して再起動します。

- a) 仮想構成を APIC 更新します。

仮想の VM プロパティで、APIC構成情報を再入力します。 **ステップ 9** ([仮想の展開 APIC OVA の使用 \(9 ページ\)](#)) を参照してください。

- b) vAPIC 仮想マシンを再起動します。
-



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>. Cisco product warranty information is available at <https://www.cisco.com/c/en/us/products/warranty-listing.html>. US Federal Communications Commission Notices are found here <https://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2024 Cisco Systems, Inc. All rights reserved.

【注意】シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



#### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

## 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。