



## アクセスの制限

- [ドメイン別にアクセスを制限する](#) (1 ページ)
- [RBAC ルール](#) (2 ページ)
- [RBACルール](#) (7 ページ)
- [制限付きドメインのガイドラインと制限事項](#) (7 ページ)
- [Cisco Cloud APIC GUI を使用した RBAC ルールの作成](#) (8 ページ)

### ドメイン別にアクセスを制限する

制限付きセキュリティ ドメインを使用すると、テナント A などのファブリック管理者は、両方のグループのユーザーに同じ特権が割り当てられている場合、あるユーザーグループがテナント B などの別のセキュリティ ドメインのユーザーグループによって作成されたオブジェクトを表示または変更できないようにすることができます。たとえば、テナント A の制限付きセキュリティ ドメインのテナント管理者は、テナント B のセキュリティ ドメインで設定されたポリシー、プロファイル、またはユーザーを表示できません。テナント B のセキュリティ ドメインも制限されていない限り、テナント B は、テナント A で設定されたポリシー、プロファイル、またはユーザーを表示できます。ユーザーが適切な権限を持つシステム作成の設定に対して、ユーザーは常に読み取り専用で閲覧可能であることに注意してください。

たとえば、制限付きセキュリティ ドメインのユーザがテナント A に関連付けられているとします。テナント A には、ユーザが作成したアプリケーション プロファイル 1 と管理者が作成したアプリケーション プロファイル 2 の 2 つのアプリケーション プロファイルが含まれています。アプリケーション プロファイル 2 も同じテナントのもですが、ユーザはアプリケーション プロファイル 1 しか表示できません。ユーザが制限付きセキュリティ ドメインにいる場合、管理者によって作成されたプロファイルも表示されません。

上記の例では、アプリケーション プロファイル 2 は別のユーザ（管理者）によって作成されていますが、制限のないユーザ（制限付きのセキュリティ ドメインに属していないユーザ）は、アプリケーション プロファイル 1 とアプリケーション プロファイル 2 の両方を表示できます。

## RBAC ルール

Cloud Application Policy Infrastructure Controller (cAPIC) では、ロールベース アクセス コントロール (RBAC) を介してユーザーロールに従ってアクセスが提供されます。ファブリックユーザーは以下に関連付けられています。

- ロールのセット
- ロールごとの権限タイプ：アクセスなし、読み取り専用、または読み取り/書き込み
- ユーザーがアクセスできる管理情報ツリー (MIT) の一部を識別する 1 つ以上のセキュリティドメイン タグ

Cloud APIC は、管理対象オブジェクト (MO) レベルでアクセス権限を管理します。権限は、システム内の特定の機能に対するアクセスを許可または制限する MO です。たとえば、ファブリック機器は権限ビットです。このビットは、物理ファブリックの機器に対応するすべてのオブジェクト上で cAPIC によって設定されます。

ロールは権限ビットの集合です。たとえば、「管理者」ロールが「ファブリック機器」と「テナントセキュリティ」に対する権限ビットに設定されていると、「管理者」ロールにはファブリックの機器とテナントセキュリティに対応するすべてのオブジェクトへのアクセス権があります。

セキュリティドメインは、cAPIC オブジェクト階層の特定のサブツリーに関連付けられたタグです。たとえば、デフォルトのテナント「common」にはドメインタグ `common` が付いています。同様に、特殊なドメインタグ `all` の場合、MIT オブジェクトツリー全体が含まれます。管理者は、MIT オブジェクト階層にカスタムドメインタグを割り当てることができます。

ユーザーを作成してロールを割り当てても、アクセス権は有効になりません。1 つ以上のセキュリティドメインにそのユーザーを割り当てることも必要です。デフォルトでは、cAPIC ファブリックには事前作成された次の 2 つの特殊なドメインが含まれています。

- All : MIT 全体へのアクセスを許可
- インフラ : ファブリック アクセス ポリシーなどの、ファブリック インフラストラクチャのオブジェクトおよびサブツリーへのアクセスを許可

Cisco Cloud APIC は、次の AAA ロールと権限をサポートしています。

特権	説明
ロール : 管理	
admin	すべてのファブリックの機能へのフルアクセスを提供します。管理者権限は、その他のすべての権限を組み合わせたものとみなされます。
ロール : aaa	

特権	説明
aaa	ポリシーの認証、許可、アカウントिंग、インポート/エクスポートの設定に使用されます。
<b>Role: access-admin</b>	
access-connectivity	インフラでのレイヤ 1～3 の構成、テナントの L3Out での静的ルート構成、管理インフラポリシー、テナント ERSPAN ポリシーに使用されます。
access-equipment	アクセス ポート設定に使用されます。
access-protocol	インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタ ポリシーやファームウェア ポリシーなどの操作関連のアクセスポリシーでレイヤ 1～3 のプロトコル構成に使用されます。
access-qos	CoPP および QoS に関連するポリシーの変更に使用されます。
<b>ロール : fabric-admin</b>	
fabric-connectivity	ファブリック、ファームウェア、および導入ポリシーのレイヤ 1～3 の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。
fabric-equipment	リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーに使用されます。
fabric-protocol	ファブリックでのレイヤ 1～3 のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN および正常性スコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイントトラッキングポリシーに使用されます。
<b>ロール : nw-svc-admin</b>	

特権	説明
nw-svc-policy	レイヤ4～レイヤ7ネットワークサービスオーケストレーションの管理に使用されます。
<b>ロール : nw-svc-params</b>	
nw-svc-params	レイヤ4～レイヤ7のサービスポリシーの管理に使用されます。
<b>Role: ops</b>	
ops	設定されているポリシーの表示に使用されま す（ポリシーのトラブルシューティングな ど）。
<b>ロール : port-mgmt</b>	
port-mgmt	ノードをセキュリティドメインに割り当てる ために使用されます。また、ノードルールを 持つセキュリティドメインのユーザーは、 port-mgmt のロールを持つドメイン all に割り 当てる必要があります。
<b>Role: tenant-admin</b>	
aaa	ポリシーの認証、許可、アカウントिंग、 インポート/エクスポートの設定に使用されま す。
access-connectivity	インフラでのレイヤ1～3の構成、テナント の L3Out での静的ルート構成、管理インフラ ポリシー、テナント ERSPAN ポリシーに使用 されます。
access-equipment	アクセスポート設定に使用されます。
access-protocol	インフラストラクチャ、NTP、SNMP、DNS、 およびイメージ管理用のファブリック全体の ポリシー、およびクラスタポリシーやファーム ウェアポリシーなどの操作関連のアクセス ポリシーでレイヤ1～3のプロトコル構成に 使用されます。
access-qos	CoPP および QoS に関連するポリシーの変更 に使用されます。

特権	説明
fabric-connectivity	ファブリック、ファームウェア、および導入ポリシーのレイヤ1～3の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。
fabric-equipment	リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーに使用されます。
fabric-protocol	ファブリックでのレイヤ1～3のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN および正常性スコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイントトラッキングポリシーに使用されます。
nw-svc-policy	レイヤ4～レイヤ7ネットワークサービスオーケストレーションの管理に使用されます。
tenant-network-profile	ネットワークプロファイルの削除および作成、エンドポイントグループの削除および作成など、テナント設定の管理に使用されます。
tenant-protocol	テナント下のレイヤ1～3プロトコルの構成、テナントトレースルートポリシー、およびファームウェアポリシーの書き込みアクセスに使用されます。
tenant-qos	テナントのQoSに関連する設定に使用されます。
tenant-security	テナントのコントラクトに関連する設定に使用されます。
<b>Role: tenant-ext-admin</b>	

特権	説明
tenant-connectivity	ブリッジドメイン、サブネット、および VRF などの レイヤ 1～3 の接続変更で使用されます。これには、リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシー、テナントのインバンドおよびアウトオブバンド管理接続構成。アトミックカウンタや正常性スコアなどのデバッグ/モニタリングポリシーなどがあります。
tenant-epg	エンドポイントグループ、VRF、ブリッジドメインの削除/作成など、テナント設定の管理に使用されます。
tenant-ext-connectivity	書き込みアクセスファームウェアポリシーに使用されます。テナント L2Out および L3Out 設定の管理。デバッグ/モニタリング/オブザーバポリシー。
tenant-ext-protocol	BGP、OSPF、PIM、IGMP などのテナント外部レイヤ 1～3 プロトコルの管理、およびトレースルート、ping、oam、eptrk などのデバッグ/モニタリング/オブザーバポリシーに使用されます。通常、ファームウェアポリシーの書き込みアクセスにのみ使用します。
tenant-network-profile	ネットワークプロファイルの削除および作成、エンドポイントグループの削除および作成など、テナント設定の管理に使用されます。
tenant-protocol	テナント下のレイヤ 1～3 プロトコルの構成、テナント トレースルート ポリシー、およびファームウェアポリシーの書き込みアクセスに使用されます。
tenant-qos	テナントの QoS に関連する設定で使用されます。
tenant-security	テナントのコントラクトに関連する設定で使用されます。

カスタム権限は、任意の MO クラスに割り当てることができます。22 個のカスタム権限が Cisco Cloud APIC GUI に表示されます。これらのカスタム権限のいずれかがクラスに割り当てられている場合、その MO のアクセスには、新しく追加されたカスタム権限が含まれます。1 つのカスタム権限を 1 つ以上の MO クラスに関連付けることができます。



(注) カスタム権限はCisco Cloud APIC GUIで表示されますが、現在サポートされていません。

事前に定義された一連の管理対象オブジェクト クラスをドメインに関連付けることができます。これらのクラスがオーバーラップすることはできません。ドメインの関連付けをサポートするクラスの例：

- レイヤ 2 およびレイヤ 3 のネットワークで管理されたオブジェクト
- ネットワーク プロファイル (物理、レイヤ 2、レイヤ 3、管理など)
- Quality of Service (QoS) ポリシー

ドメインに関連付けることができるオブジェクトが作成されると、ユーザは、ユーザのアクセス権の範囲内でオブジェクトにドメインを割り当てる必要があります。ドメインの割り当てはいつでも変更できます。

## RBACルール

RBACルールは、リソース（アプリケーションプロファイル、EPG、コントラクトなど）を、別のセキュリティドメインにいるためにアクセスできないユーザに選択的に公開します。RBACルールは、アクセスされるオブジェクトを特定する識別名（DN）と、オブジェクトにアクセスするユーザを含むセキュリティドメインの名前の2つの部分で構成されます。

RBACルールには2つのタイプがあります。

- 暗黙的：ユーザは、RBAC階層に基づいてルールまたは権限を継承します
- 明示的：ルールは特定のポリシーに基づいてユーザに直接割り当てられます

制限付きおよび制限なしの両方のセキュリティドメインがサポートされています。



(注) 管理情報ツリー内の異なる部分に存在するユーザに対し、RBAC規則によりオブジェクトを公開することは可能ですが、CLIの使用によってツリーの構造を横断することでそのようなオブジェクトに移動することはできません。ただし、RBAC規則に含まれるオブジェクトのDNをユーザが把握していれば、ユーザはMO検索コマンドにより、CLIを使用してそれを見つけることができます。

## 制限付きドメインのガイドラインと制限事項

制限付きドメインのユーザに対するガイドラインと制限は次のとおりです。

- あるセキュリティドメインのユーザに別のセキュリティドメインが割り当てられている場合、そのユーザは新しいドメインに関連付けられた構成にアクセスできます。

- ユーザは、「制限付き」とマークされた1つ以上のセキュリティドメインの一部になることができます。
- 制限付きドメイン ユーザは、システムで作成された構成への読み取り専用アクセス権を持っています。
- 複数のセキュリティドメインを持つユーザの場合、すべてのセキュリティドメインを合わせた長さが 1024 文字を超えることはできません。長さが 1024 を超えると、ユーザはポリシーの作成に問題が発生します。
- Cloud APIC の制限付きドメインは、クラウドリソースではサポートされていません。つまり、ある制限付きドメインのユーザは、別の制限付きドメインのユーザによって作成されたクラウドリソースを表示できます。

## Cisco Cloud APIC GUI を使用した RBAC ルールの作成

このセクションでは、GUI を使用して RBAC ルールを作成する方法について説明します。



- (注) RBAC ルールを構成できますが、Cloud APIC GUI は構成をサポートしていません。この手順（手順 4）を使用して構成された DN は、API を使用して照会できます。

### 始める前に

セキュリティドメインの作成詳細なタスクについては、「[セキュリティドメインの作成](#)」を参照してください。

- ステップ 1** インテントアイコンをクリックします。[**インテント (Intent)**]メニューが表示されます。
- ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。  
[**インテント (Intent)**]メニューに**管理オプション**のリストが表示されます。
- ステップ 3** [**インテント (Intent)**]メニューの[**管理 (Administrative)**]リストから、[**セキュリティ (Security)**] > [**RBAC ルール (RBAC Rules)**] > [**RBAC ルールの作成 (Create RBAC Rule)**] をクリックします。[**RBAC ルールの作成 (Create RBAC Rule)**] ダイアログボックスが表示されます。
- ステップ 4** **DN** フィールドに、ルールの DN を入力します。  
明示的な RBAC ルールを作成するには、ObjectStore でアプリケーションの DN を見つけます。ここでその DN 値を使用します。
- ステップ 5** セキュリティドメインを選択します。
  - a) [**セキュリティドメインの選択 (Select 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 Domain)**] ダイアログボックスが表示されます。



- b) **[セキュリティドメインの選択 (Select Security Domain)]** ダイアログで、左側の列のセキュリティドメインをクリックして選択し、**[選択 (Select)]** をクリックします。**[RBAC ルールの作成]** ダイアログボックスに戻ります。

**ステップ 6** **[書き込みを許可]** フィールドで、**[はい]** をクリックして書き込みを許可するか、**[いいえ]** をクリックして書き込みを許可しません。

**ステップ 7** 設定が終わったら **[保存 (Save)]** をクリックします。

(注) 明示的な RBAC ルールを作成した後、セキュリティドメインに割り当てられたユーザは、以前に (ObjectStore から) 定義されたアプリケーションとその子のみを表示できます。

---



## 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。