



IPv6 ACL

- [IPv6 ACL の制限 \(1 ページ\)](#)
- [IPv6 ACL の概要 \(2 ページ\)](#)
- [IPv6 ACL の設定方法 \(5 ページ\)](#)
- [IPv6 ACL のモニタリング \(12 ページ\)](#)
- [IPv6 ACL の設定例 \(13 ページ\)](#)
- [IPv6 ACL の機能履歴 \(14 ページ\)](#)

IPv6 ACL の制限

IPv6 がサポートするのは名前付き ACL だけです。IPv4 ACL では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再起 ACL (**reflect** キーワード) をサポートしません。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制約事項はありません。ハードウェア転送が必要なインターフェイス (物理ポートまたは SVI) に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。ACL がインターフェイスでサポートされていない場合、ACL は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ (ACE) を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されるのを許可しません。

IPv6 ACL の概要

ここでは、IPv6 ACL について説明します。

IPv6 ACL の概要

アクセスコントロールリスト (ACL) とは、特定のインターフェイスへのアクセスを制限するために使用されるルールセットのことです。ACL はデバイスに設定され、管理インターフェイスおよび任意の動的インターフェイスに適用されます。

Web 認証用に事前認証 ACL を作成することもできます。このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。IPv4 と MAC どちらのアクセスリストタイプのどの方向に対してでも、レイヤ 2 インターフェイスにポート ACL を適用できます。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向 (インバウンドまたはアウトバウンド) に適用されます。

ACL のタイプ

次のセクションでは ACL のタイプについて説明します。

ユーザ単位 IPv6 ACL

ユーザあたりの ACL の場合、テキスト文字列としての完全なアクセス コントロール エントリ (ACE) が Cisco Secure Access Control Server (Cisco Secure ACS) で設定されます。

フィルタ ID IPv6 ACL

filter-id ACL の場合、完全な ACE および `acl name (filter-id)` がデバイスで設定され、`filter-id` のみが次に設定されます。Cisco Secure ACS で設定されます。

ダウンロード可能 IPv6 ACL

ダウンロード可能 ACL (dACL) の場合、完全な ACE および dacl 名は Cisco Secure ACS のみで設定されます。

Cisco Secure ACS はその ACCESS-Accept 属性で dacl 名をデバイスに送信します。デバイスは dacl 名を取得し、ACE のために dACL 名を ACCESS-request 属性を使用して Cisco Secure ACS に送り返します。

スイッチ スタックおよび IPv6 ACL

アクティブ スイッチは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバに配信します。

スタンバイ スイッチがアクティブ スイッチを引き継ぐと、ACL 設定がすべてのスタック メンバに配信されます。メンバスイッチは、新しいアクティブスイッチによって配信された設定を同期し、不要なエントリを消去します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、アクティブ スイッチは変更内容をすべてのスタック メンバに配信します。

ACL 優先順位

、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、ポート ACL です。

次の例で、簡単な使用例を説明します。

- スイッチ仮想インターフェイス (SVI) に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。

VLAN マップ

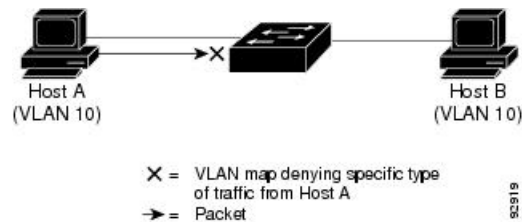
VLAN ACL または VLAN マップは、VLAN 内のネットワークトラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリング および特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向 (入力または出力) で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセスコントロールされます（IP トラフィックは、MAC VLAN マップではアクセス制御されません）。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用できません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

図 1: VLAN マップによるトラフィックの制御

次の図に、VLAN マップを適用して、特定のトラフィックタイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用で



きます。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージプロトコル (ICMP) キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジドフレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラーメッセージが表示されます。

IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラーメッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェアメモリに空きがない場合、パケットはインターフェイスでドロップされ、アンロードのエラーメッセージが記録されます。

ハードウェアメモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

IPv6 ACL の設定方法

ここでは、IPv6 ACL の設定方法に関する情報を示します。

IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Device# show access-lists preauth_ipv6_acl

IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 access-list {list-name log-update threshold role-based list-name} 例： Device(config)# ipv6 access-list example_acl_list	IPv6 ACL 名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	{deny permit} protocol {source-ipv6-prefix/ prefix-length any threshold host source-ipv6-address} [IPv6 ACL の許可条件または拒否条件を指定します。

コマンドまたはアクション	目的
<pre>operator [port-number] { destination-ipv6-prefix/ prefix-length any host destination-ipv6-address} [operator [port-number]][dscp value] [fragments] [log] [log-input][sequence value] [time-range name]</pre> <p>例 :</p> <pre>Device(config-ipv6-acl)# permit tcp 2001:DB8:0300:0201::/32 eq telnet any</pre>	<ul style="list-style-type: none"> • protocolには、IPの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udpまたはIPv6プロトコル番号を表す0～255の整数を使用できます。 • <i>source-ipv6-prefix/prefix-length</i> または <i>destination-ipv6-prefix/prefix-length</i> は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーククラスで、コロン区切りの16ビット値を使用した16進形式で指定します (RFC 2373 を参照)。 • IPv6 プレフィックス <i>::/0</i> の短縮形として、any を入力します。 • host <i>source-ipv6-address</i> または <i>destination-ipv6-address</i> には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホストアドレスを入力します。アドレスはコロン区切りの16ビット値を使用した16進形式で指定します。 • (任意) operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、lt (より小さい)、gt (より大きい)、eq (等しい)、neq (等しくない)、および range (包含範囲) があります。 <i>source-ipv6-prefix/prefix-length</i> 引数のあとの operator は、送信元ポートに一致する必要があります。 <i>destination-ipv6-prefix/prefix-length</i> 引数のあとの operator は、宛先ポートに一致する必要があります。 • (任意) port-number は、0～65535の10進数またはTCPあるいはUDPポートの名前です。TCPポート名を使用できるのは、TCPのフィル

	コマンドまたはアクション	目的
		<p>タリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。</p> <ul style="list-style-type: none"> • (任意) dscp value を入力して、各 IPv6 パケットヘッダーの Traffic Class フィールド内のトラフィッククラス値と DiffServ コードポイント値を照合します。指定できる範囲は 0～63 です。 • (任意) fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • (任意) log を指定すると、エントリと一致するパケットに関するログメッセージがコンソールに送信されます。log-input を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 • (任意) sequence value を入力して、アクセスリストステートメントのシーケンス番号を指定します。指定できる範囲は 1～4,294,967,295 です。 • (任意) time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 5	<pre>{deny permit} tcp {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6- prefix/prefix-length any host destination-ipv6-address} [operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port protocol}] [psh] [range {port protocol}] [rst] [sequence value] [syn] [time-range name] [urg]</pre>	<p>IPv6 ACL の許可条件または拒否条件を指定します。</p> <p>TCP の場合は tcp を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。</p> <ul style="list-style-type: none"> • ack : 確認応答 (ACK) ビットセット。

	コマンドまたはアクション	目的
	例： Device(config-ipv6-acl)# deny tcp host 2001:DB8:1::1 any log-input	<ul style="list-style-type: none"> • established : 確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin : 終了ビットセット。送信者からのデータはそれ以上ありません。 • neq {port protocol} : 所定のポート番号上にはないパケットだけを照合します。 • psh : プッシュ機能ビットセット • range {port protocol} : ポート番号の範囲内のパケットだけを照合します。 • rst : リセットビットセット • syn : 同期ビットセット • urg : 緊急ポインタビットセット
ステップ 6	end 例： Device(config-ipv6-acl)# end	IPv6 アクセス リスト コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 7	show ipv6 access-list 例： Device# show ipv6 access-list	IPv6 ACL が正しく設定されていることを確認します。

インターフェイスへの IPv6 ACL の付加

レイヤ 3 インターフェイスで発信または着信トラフィックに ACL を、あるいはレイヤ 2 インターフェイスで着信トラフィックに を適用できます。レイヤ 3 インターフェイスで着信トラフィックにだけ ACL を適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	アクセスリストを適用するレイヤ2インターフェイス（ポート ACL 用）またはレイヤ3インターフェイス（ルータ ACL 用）を指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	no switchport 例： Device(config-if)# no switchport	インターフェイスをルーテッドインターフェイスの状態に戻して、レイヤ2の詳細設定をすべて削除します。
ステップ 5	ipv6 address ipv6-address 例： Device(config-if)# ipv6 address 2001:DB8::1	レイヤ3インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。
ステップ 6	ipv6 traffic-filter access-list-name {in out} 例： Device(config-if)# ipv6 traffic-filter acl1 in	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。
ステップ 7	end 例： Device(config-ipv6-acl)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VLAN マップの設定

VLAN マップを作成して、1つまたは複数の VLAN に適用するには、次のステップを実行します。

始める前に

VLAN に適用する IPv6 ACL を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	vlan access-map name [number] 例： Device(config)# vlan access-map map_1 20	<p>VLAN マップを作成して、VLAN アクセスマップ コマンド モードを開始します。</p> <p>VLAN マップには、名前または（オプションで）番号を指定できます。番号は、マップ内のエントリのシーケンス番号です。</p> <p>同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。</p> <p>VLAN マップでは、特定の permit または deny キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。</p>
ステップ 4	match {ip ipv6 mac} address {name number} [name number] 例： Device(config-access-map)# match ipv6 address ip_net	<p>パケットを1つまたは複数のアクセスリストと照合します。パケットの照合は、対応するプロトコルタイプのアクセスリストに対してだけ行われます。IP パケットは、IP アクセスリストに対して照合されます。非 IP パケットは、名前付き MAC アクセスリストに対してだけ照合されます。</p>

	コマンドまたはアクション	目的
		(注) パケットタイプ (IP または MAC) に対する <code>match</code> 句が VLAN マップに設定されている場合で、そのマップアクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。 <code>match</code> 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。
ステップ 5	<p>IP パケットまたは非 IP パケットを (既知の 1 MAC アドレスのみを使って) 指定し、1 つ以上の ACL とそのパケットを照合するには、次のコマンドのいずれかを入力します。</p> <ul style="list-style-type: none"> • action { forward } Device(config-access-map)# action forward • action { drop } Device(config-access-map)# action drop 	マップ エントリに対するアクションを設定します。
ステップ 6	<p>vlan filter mapname vlan-list list</p> <p>例 :</p> <pre>Device(config)# vlan filter map 1 vlan-list 20-22</pre>	<p>VLAN マップを 1 つまたは複数の VLAN に適用します。</p> <p><code>list</code> には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12, 22, 30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。</p>
ステップ 7	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VLAN への VLAN マップの適用

VLAN マップを 1 つまたは複数の VLAN に適用するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	vlan filter mapname vlan-list list 例： Device(config)# vlan filter map 1 vlan-list 20-22	VLAN マップを1つまたは複数の VLAN に適用します。 list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12, 22, 30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。
ステップ 4	end 例： Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv6 ACL のモニタリング

次の表に示された1つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセスリスト、すべての IPv6 アクセスリスト、または特定のアクセスリストに関する情報を表示できます。

表 1: **show ACL** コマンド

コマンド	目的
show access-lists	スイッチに設定されたすべてのアクセスリストを表示します。
show ipv6 access-list [<i>access-list-name</i>]	設定済みのすべての IPv6 アクセスリストまたは名前指定されたアクセスリストを表示します。
show vlan access-map [<i>map-name</i>]	VLAN アクセス マップ設定を表示します。
show vlan filter [<i>access-map access-map</i> <i>vlan vlan-id</i>]	VACL と VLAN 間のマッピングを表示します。

IPv6 ACL の設定例

ここでは、IPv6 ACL の設定例を示します。

例 : IPv6 ACL の作成

この例では、IPv6-ACL という名前の IPv6 アクセスリストを設定します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番目の拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番目の拒否エントリは、すべて的一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番目の許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセスリストの末尾にあるため、2 番目の許可エントリは必要です。



(注) ログギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
Device> enable
Device(config)# ipv6 access-list IPv6_ACL
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(config-ipv6-acl)# permit any any
Device(config-ipv6-acl)# end
```

例 : IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。スイッチに設定されているすべてのアクセス リストが表示されます。

```
Device# show access-lists

Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。スイッチに設定されている IPv6 アクセス リストだけが表示されます。

```
Device# show ipv6 access-list

IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30
IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

例：VLAN アクセスマップ設定の表示

次に、`show vlan access-map` 特権 EXEC コマンドの出力例を示します。

```
Device# show vlan access-map
```

```
Vlan access-map "m1" 10
  Match clauses:
    ipv6 address: ip2
  Action: drop
```

次に、`show ipv6 access-lists` 特権 EXEC コマンドの出力例を示します。スイッチに設定されている IPv6 アクセス リストだけが表示されます。

```
Device# show ipv6 access-list
```

```
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30
IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

IPv6 ACL の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IPv6 ACL	IPv6 ACL を作成して、インターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IPv4 の名前付き ACL を作成し、適用する方法と類似しています。レイヤ 3 管理トラフィックをフィルタリングするため、入ルータ ACL を作成し、適用することもできます。
Cisco IOS XE Gibraltar 16.11.1	IPv6 ダウンロード可能 ALC	IPv6 dACL がサポートされます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。

