ローカライズ型ポリシー

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

このセクションのトピックでは、さまざまなタイプのローカライズ型ポリシー、ローカライズ型ポリシーのコンポーネント、および Cisco SD-WAN Manager または CLI を使用してローカライズ型ポリシーを設定する方法に関する概要情報を提供します。

ローカライズ型ポリシーの概要

ローカライズ型ポリシーとは、Cisco IOS XE Catalyst SD-WAN デバイス の CLI または Cisco SD-WAN Managerデバイステンプレートを介してローカルにプロビジョニングされたポリシーを指します。

ローカライズ型ポリシーのタイプ

ローカライズ型制御ポリシー

制御ポリシーは、Cisco IOS XE Catalyst SD-WAN オーバーレイネットワークのコントロール プレーントラフィックに作用し、オーバーレイネットワークを通過するルーティングパスの決定に影響を及ぼします。ローカライズ型制御ポリシーは、Cisco IOS XE Catalyst SD-WAN デバイスで設定されるポリシーであり（したがって、ローカル）、デバイスが属するサイトローカルネットワークに対する BGP および OSPF ルーティングの決定に影響を及ぼします。

オーバーレイネットワークに参加するだけでなく、Cisco IOS XE Catalyst SD-WAN デバイス はローカルサイトでネットワークに参加したりするため、他のネットワークデバイスからは通常のルータに見えます。そのため、ローカルサイトのルータとルート情報を交換できるように、Cisco IOS XE Catalyst SD-WAN デバイス で BGP や OSPF などのルーティングプロトコルをプロビジョニングできます。ローカルネットワークでルーティング動作を制御および変更するには、デバイスでルートポリシーと呼ばれる制御タイプのポリシーを設定します。ルートポリシーは、ローカルブランチで実行されるルーティングにのみ適用され、ローカルデバイスのルートテーブルのルートテーブルエントリにのみ影響します。

デバイスで 設定するローカライズ型制御ポリシーを使用すると、デバイスが配置されているローカルサイトのネットワークのルーティングポリシーに影響を与えることができます。このタイプの制御ポリシーは、ルートポリシーと呼ばれています。このポリシーは、通常のドライバで設定するルーティングポリシーに似ており、サイトとローカル間ネットワークでの BGP および OSPF ルーティング動作を変更できるようにします。一元管理型制御ポリシーはオーバーレイネットワーク全体のルーティング動作に影響しますが、ルートポリシーはローカルブランチのルーティングにのみ適用されます。

ローカライズ型データポリシー

データポリシーは、Cisco IOS XE Catalyst SD-WAN オーバーレイネットワークのデータプレーンに作用し、ネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス 間におけるデータトラフィックの送信の仕方に影響を及ぼします。Cisco Catalyst SD-WAN アーキテクチャでは、2 つのタイプのデータポリシーを定義します。一元管理型データポリシーという、データパケットの IP ヘッダーフィールドとネットワーク セグメンテーションに基づいてデータトラフィックのフローを制御するタイプと、ローカライズ型データポリシーという、インターフェイス間を行き来するデータトラフィックのフローと Cisco IOS XE Catalyst SD-WAN デバイス でのインターフェイスキューを制御するタイプです。

ローカライズ型データポリシーは、ローカルの Cisco IOS XE Catalyst SD-WAN デバイス にプロビジョニングされるのでこう呼ばれていますが、ある決まったルータインターフェイスに適用されるポリシーで、そうしたインターフェイスによって送受信されるデータトラフィックの処理の仕方に影響を及ぼします。ローカライズ型データポリシーは、アクセスリスト（ACL）とも呼ばれます。アクセスリストを使用すると、サービスクラス（CoS）のプロビジョニングや、データパケットの分類、さまざまなクラスの伝送プロパティの優先順位付けを行うことができます。ポリシングを設定して、パケットミラーリングのプロビジョニングもできます。

IPv4 の場合は、QoS アクションの設定が可能です。

ルータ上の任意の VPN に IPv4 アクセスリストを適用できるほか、ユニキャストおよびマルチキャストトラフィックに作用するアクセスリストの作成もできます。IPv6 アクセスリストの場合は、適用できるのがトランスポート VPN（VPN 0）のトンネルインターフェイスのみとなります。

アクセスリストの適用は、インターフェイスのアウトバウンドまたはインバウンド方向のいずれかとなります。アウトバウンド方向に IPv4 ACL を適用すると、ローカルサービス側ネットワークから IPsec トンネルを通過してリモートサービス側ネットワークに向かうデータパケットに影響を及ぼします。インバウンド方向に IPv4 ACL を適用すると、IPsec トンネルから出てローカル Cisco IOS XE Catalyst SD-WAN デバイス で受信されるデータパケットに影響を及ぼします。IPv6 の場合は、アウトバウンド ACL がルータによって送信されるトラフィックに適用され、インバウンド ACL は受信トラフィックに適用されます。

明示的なアクセスリストと暗示的なアクセスリスト

ローカライズ型データポリシーを使用して設定するアクセスリストは、明示的な ACL と呼ばれます。明示的な ACL は、ルータ上の任意の VPN に適用できます。

ルータ トンネル インターフェイスには、サービスとも呼ばれる暗黙的な *ACL* もあります。これらの一部はデフォルトでトンネルインターフェイスに存在し、無効にしない限り有効です。設定によって、その他の暗黙的な ACL を有効にすることもできます。Cisco IOS XE Catalyst SD-WAN デバイス では、DHCP（DHCPv4 および DHCPv6 の場合）、DNS、および ICMP の各サービスがデフォルトで有効になっています。BGP、Netconf、NTP、OSPF、SSHD、および STUN のサービスを有効にすることもできます。

QoS アクションの実行

アクセスリストを使用すると、Quality of Service（QoS）をプロビジョニングできます。これにより、データトラフィックを重要度で分類して、複数のインターフェイスキューに分散させ、さまざまなクラスのトラフィックの送信レートを制御できるようになります。「転送と QoS の概要」を参照してください。

データパケットのミラーリング

パケットが分類されたら、アクセスリストを設定して、Cisco vEdge デバイス で検出されたデータパケットの複製を別のネットワークデバイス上の指定された宛先に送信できます。Cisco IOS XE Catalyst SD-WAN デバイス でサポートしているミラーリングは 1 対 1 です。つまり、すべてのパケットの複製は代わりの宛先に送信されます。

Cisco SD-WAN Manager を使用したローカライズ型ポリシーの設定

ローカライズ型ポリシーを設定するには、Cisco SD-WAN Manager のポリシー構成ウィザードを使用します。ウィザードは、次のローカライズ型ポリシーコンポーネントを構成および変更するための 5 つのウィンドウで構成される UI ポリシービルダーです。

- 対象グループ（リストとも呼ばれます）
- QoS に使用する転送クラス
- アクセス制御リスト（ACL）
- ルートポリシー
- ポリシー設定

作成する特定のポリシーに応じて、これらのコンポーネントの一部またはすべてを構成します。コンポーネントをスキップするには、ウィンドウの下部にある [次へ（Next）] をクリックします。コンポーネントに戻るには、ウィンドウの下部の [戻る（Back）] をクリックします。

Cisco SD-WAN Manager を使用してローカライズ型ポリシーを設定するには、このセクションに続く手順で示すステップを実行します。

ポリシー構成ウィザードの開始

ポリシー構成ウィザードを開始するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [ローカライズ側ポリシー（Localized Policy）] を選択します。
3. [Add Policy] をクリックします。

[対象グループの作成（Create Groups of Interest）] ページが表示されます。

ローカライズ型ポリシーの対象グループの構成

[対象グループの作成（Create Groups of Interest）] で、ローカライズ型ポリシーで使用するグループのリストを作成します。

[対象グループの作成（Create Groups of Interest）] で、次のセクションの説明に従って、リストタイプの新しいグループを作成し、ローカライズ型ポリシーで使用します。

AS パスの構成

1. [対象グループ（Group of Interest）] リストで、[AS パス（AS Path）] をクリックします。

2. [新しい AS パスリスト（New AS Path List）] をクリックします。
3. リストの名前を入力します。
4. AS パスは、AS 番号をコンマで区切って入力します。
5. [Add]をクリックします。

   [AS パス（AS Path）] リストには、1 つ以上の BGP AS パスを指定します。各 AS は、単一の数値または正規表現として記述できます。1 つのパスに複数の AS を指定するには、コンマで区切ってリストに含めます。1 つのリストに複数の AS パスを構成するには、複数の **as-path** オプションを含め、各オプションに 1 つの AS パスを指定します。

コミュニティの設定

コミュニティリストは、ルートマップの match 句で使用するコミュニティのグループ作成に使用されるリストです。コミュニティリストは、ルートの受け入れ、優先、配布、またはアドバタイズの制御に使用できます。また、コミュニティリストは、ルートのコミュニティの設定、追加または変更にも使用できます。

1. [対象グループ（Group of Interest）] リストで、[コミュニティ（Community）] をクリックします。
2. [新しいコミュニティリスト（New Community List）] をクリックします。
3. コミュニティリストの名前を入力します。
4. [コミュニティの追加（Add Community）] フィールドに、次のいずれかの形式で、1 つ以上のデータプレフィックスをコンマで区切って入力します。
   - *aa*:*nn*：自律システム（AS）番号とネットワーク番号。各番号は、1 ～ 65535 の範囲の 2 バイト値です。
   - **internet**：このコミュニティのルートはインターネットコミュニティにアドバタイズされます。このコミュニティは、すべての BGP 対応ネットワーキングデバイスで構成されます。
   - **local-as**：このコミュニティのルートはローカル AS 番号の外にはアドバタイズされません。
   - **no-advertise**：NO_ADVERTISE コミュニティをルートにアタッチします。このコミュニティのルートは他の BGP ピアにはアドバタイズされません。
   - **no-export**：NO_EXPORT コミュニティをルートにアタッチします。このコミュニティのルートは、ローカル AS や BGP コンフェデレーション境界の外にアドバタイズされません。1 つのリストに複数の BGP コミュニティを設定するには、複数の **community** オプションを含め、各オプションに 1 つのコミュニティを指定します。
5. [Add]をクリックします。

データプレフィックスの設定

1. [対象グループ（Group of Interest）] リストで、[データプレフィックス（Data Prefix）] をクリックします。
2. [新しいデータプレフィックスリスト（New Data Prefix List）] をクリックします。
3. リストの名前を入力します。
4. 1つ以上の IP プレフィックスを入力します。
5. [Add]をクリックします。

   データプレフィックスリストには、1 つ以上の IP プレフィックスを指定します。ユニキャストアドレスとマルチキャストアドレスの両方を指定できます。1 つのリストに複数のプレフィックスを構成するには、複数の **ip-prefix** オプションを含め、各オプションに 1 つのプレフィックスを指定します。

拡張コミュニティの構成

1. [対象グループ（Group of Interest）] リストで、[拡張コミュニティ（Extended Community）] をクリックします。
2. [新しい拡張コミュニティリスト（New Extended Community List）] をクリックします。
3. リストの名前を入力します。
4. 次の形式で BGP 拡張コミュニティを入力します。
   - [rt]（aa:nn | ip-address）：ルート ターゲット コミュニティ。BGP によって運ばれる一連のルートを受信できる 1 つ以上のルータです。AS 番号とネットワーク番号を 1 ～ 65535 の 2 バイトの数値、または IP アドレスで指定します。
   - [soo]（aa:nn | ip-address）：ルートオリジンコミュニティ。一連のルートを BGP に挿入できる 1 つ以上のルータです。AS 番号とネットワーク番号を 1 ～ 65535 の 2 バイトの数値、または IP アドレスで指定します。1 つのリストに複数の拡張 BGP コミュニティを設定するには、複数の [community] オプションを含め、各オプションに 1 つのコミュニティを指定します。
5. [Add]をクリックします。

クラスマップの設定

1. [対象グループ（Group of Interest）] リストで、[クラスマップ（Class Map）] をクリックします。
2. [新しいクラスリスト（New Class List）] をクリックします。
3. クラスの名前を入力します。
4. [キュー（Queue）] ドロップダウンリストから必要なキューを選択します。

5. [Save] をクリックします。

ミラーの設定

1. [対象グループ（Group of Interest）] リストで、[ミラー（Mirror）] をクリックします。
2. [新しいミラーリスト（New Mirror List）] をクリックします。[ミラーリスト（Mirror List）] ポップアップが表示されます。
3. リストの名前を入力します。
4. [Remote Destination IP] フィールドには、パケットをミラーリングする宛先の IP アドレスを入力します。
5. [Source IP] フィールドには、ミラーリングするパケットの送信元 IP アドレスを入力します。
6. [Add]をクリックします。

   ミラーリングパラメータを設定するには、パケットのミラーリング先のリモート接続先を定義し、パケットの送信元を定義します。ミラーリングはユニキャストトラフィックにのみ適用されます。マルチキャストトラフィックには適用されません。

ポリサーの構成

1. [対象グループ（Group of Interest）] リストで、[ポリサー（Policer）] をクリックします。
2. [新しいポリサーリスト（New Policer List）] をクリックします。
3. リストの名前を入力します。
4. [バースト(bps)（Burst (bps)）] フィールドに、最大トラフィックバーストサイズを入力します。15,000 ～ 10,000,000 バイトの値を指定できます。
5. [超過（Exceed）] フィールドで、バーストサイズまたはトラフィックレートを超えたときに実行するアクションを選択します。[ドロップ（Drop）]（デフォルト）を選択して、[パケット損失の優先順位（PLP）（Packet Loss Priority (PLP)）] を [低（Low）] に設定します。[注釈（Remark）] を選択して、PLP を [高（High）] に設定します。
6. [レート(bps)（Rate (bps)）] フィールドに、最大トラフィックレートを入力します。8 ～ 2^{64} bps（8 ～ 100,000,000,000）の値にすることができます。
7. [Add]をクリックします。

プレフィックスの構成

1. [対象グループ（group of interest）] リストで、[プレフィックス（Prefix）] をクリックします。
2. [新しいプレフィックスリスト（New Prefix List）] をクリックします。
3. リストの名前を入力します。

4. [インターネットプロトコル（Internet Protocol）] フィールドで、[IPv4] または [IPv6] をクリックします。
5. [Add Prefix] で、リストのプレフィックスを入力します。（例を表示します。）必要に応じて、右側にある緑色の [インポート（Import）] リンクをクリックして、プレフィックスリストをインポートします。
6. [Add]をクリックします。

[次へ（Next）] をクリックして、ウィザードの [転送クラス/QoSの設定（Configure Forwarding Classes/QoS）] に移動します。

転送クラス/QoSの設定

[転送クラス/QoS（Forwarding Classes/QoS）] ページを初めて開くと、デフォルトで[QoSマップ（QoS Map）]が選択されています。

QoS マップ（QoS Map）

新しい QoS マッピングを作成するには、次の手順を実行します。

1. [QoS] で、[QoSマップの追加（Add QoS Map）] ドロップダウンリストをクリックします。
2. [新規作成（Create New）] を選択します。
3. QoS マッピングの名前と説明を入力します。
4. [キューの追加（Add Queue）] をクリックします。[キューの追加（Add Queue）] ポップアップが表示されます。
5. [キュー（Queue）] ドロップダウンリストからキュー番号を選択します。
6. 最大帯域幅とバッファの割合、およびスケジューリングとドロップタイプを選択します。
7. [転送クラス（Forwarding Class）] を入力します。
8. [キューを保存（Save Queue）] をクリックします。

既存の QoS マッピングをインポートするには、次の手順を実行します。

1. [QoS] で、[QoSマップの追加（Add QoS Map）] ドロップダウンリストをクリックします。
2. [既存をインポート（Import Existing）] を選択します。[既存のアプリケーションQoSマップポリシーのインポート（Import Existing Application QoS Map Policy）] ポップアップが表示されます。
3. [QoSマップ（QoS Map）] ポリシーを選択します。
4. [Import] をクリックします。

QoSマッピングを表示またはコピーするか、ローカライズ型ポリシーからマッピングを削除するには、**[...]** をクリックして、目的のアクションを選択します。

ハードウェアの場合、各インターフェイスには 0 ～ 7 の番号が付けられた 8 つのキューがあります。キュー 0 は低遅延キューイング（LLQ）用に予約されているため、キュー 0 にマップされるクラスはすべて LLQ を使用するように構成する必要があります。すべてのデフォルトのスケジューリング方式は、加重ラウンドロビン（WRR）です。

Cisco IOS XE Catalyst SD-WAN デバイス の場合、各インターフェイスには 0 ～ 7 の番号が付けられた 8 つのキューがあります。キュー 0 は制御トラフィック用に予約されており、キュー 1、2、3、4、5、6、7 はデータトラフィック用に使用できます。8 つのキューすべてのスケジューリング方式は WRR です。LLQ はサポートされていません。

Cisco IOS XE Catalyst SD-WAN デバイス で QoS パラメータを設定するには、QoS スケジューリングとシェーピングを有効にする必要があります。Cisco IOS XE Catalyst SD-WAN デバイスがトランスポート側インターフェイスから受信するトラフィックの QoS パラメータを有効にするには、次の手順を実行します。

Cisco IOS XE Catalyst SD-WAN デバイス がサービス側インターフェイスから受信するトラフィックの QoS パラメータを有効にするには、次の手順を実行します。

ポリシーの書き換え

QoS マッピングのポリシー書き換えルールを構成するには、次の手順を実行します。

1. [ポリシーの書き換え（Policy Rewrite）] で、[書き換えポリシーの追加（Add Rewrite Policy）] ドロップダウンリストをクリックします。
2. [新規作成（Create New）] を選択します。
3. 書き換えルールの名前と説明を入力します。
4. [書き換えルールの追加（Add Rewrite Rule）] をクリックします。[ルールの追加（Add Rule）] ポップアップが表示されます。
5. [クラス（Class）] ドロップダウンからクラスを選択します。
6. [優先順位（Priority）] ドロップダウンから優先順位（[低（Low）] または [高（High）]）を選択します。

   [低（Low）] の優先順位は Cisco IOS XE Catalyst SD-WAN デバイス でのみサポートされます。
7. **[DSCP]** フィールドに DSCP 値（0 ～ 63）を入力します。
8. [レイヤ2サービスクラス（Layer 2 Class of Service）] フィールドに、サービスクラス（CoS）の値（0 ～ 7）を入力します。
9. [Save Rule] をクリックします。

既存の書き換えルールをインポートするには、次の手順を実行します。

1. [QoS] で、[書き換えポリシーの追加（Add Rewrite Policy）] ドロップダウンをクリックします。

2. [既存をインポート（Import Existing）] を選択します。[既存のポリシー書き換えのインポート（Import Existing Policy Rewrite）] ポップアップが表示されます。
3. 書き換えルールポリシーを選択します。
4. [Import] をクリックします。

[次へ（Next）] をクリックして、[アクセスリストの設定（Configure Access Lists）] ページに移動します。

ACL の設定

1. [アクセス制御リストの設定（Configure Access Control Lists）] ページで、ACL を設定します。
2. 新しいアクセス制御リスト（ACL）を作成するには、[アクセス制御リストポリシーの追加（Add Access Control List Policy）] ドロップダウンリストをクリックします。次のオプションのいずれかを選択します。
   - **IPv4 ACL ポリシーの追加（Add IPv4 ACL Policy）**：IPv4 ACL ポリシーを設定します。
   - **IPv6 ACL ポリシーの追加（Add IPv6 ACL Policy）**：IPv6 ACL ポリシーを設定します。
   - **既存のインポート（Import Existing）**：既存の ACL ポリシーをインポートします。
3. [IPv4 ACLポリシーの追加（Add IPv4 ACL Policy）] をクリックすると、[IPv4 ACLポリシーの追加（Add IPv4 ACL Policy）] ページが表示されます。

   または

   [IPv6 ACLポリシーの追加（Add IPv6 ACL Policy）] をクリックすると、[IPv6 ACLポリシーの追加（Add IPv6 ACL Policy）] ページが表示されます。
4. [ACLポリシー（ACL Policy）] ページで、ACL の名前と説明を入力します。
5. 左側のペインで、[ALCシーケンスの追加（Add ACL Sequence）] をクリックします。左側のペインに [アクセス制御リスト（Access Control List）] ボックスが表示されます。
6. [アクセス制御リスト（Access Control List）] ボックスをダブルクリックし、ACL の名前を入力します。
7. 右側のペインで、[シーケンスルールの追加（Add Sequence Rule）] をクリックして、ACL に単一のシーケンスを作成します。デフォルトでは [マッチ（Match）] が選択されています。
8. マッチ条件をクリックします。
9. 左側に、マッチ条件の値を入力します。
   1. 右側に、ポリシーが一致した場合に実行するアクションを入力します。

10. ステップ 6 ～ 8 を繰り返して、ACL にマッチ/アクションペアを追加します。
11. ACL のマッチ/アクションペアを並び替えるには、右側のペインでそれらを目的の位置にドラッグします。
12. ACL からマッチ/アクションペアを削除するには、条件の右上にある **[X]** をクリックします。
13. [マッチとアクションの保存（Save Match and Actions）] をクリックして、シーケンスルールを保存します。
14. ACL のシーケンスルールを並び替えるには、左側のペインでルールを目的の位置にドラッグします。
15. ACL のシーケンスルールをコピー、削除、または名前変更するには、左側のペインで、ルール名の横にある **[...]** をクリックし、目的のオプションを選択します。

Default Action

評価されるパケットがアクセスリストのマッチ条件のいずれにも一致しない場合、デフォルトアクションがこのパケットに適用されます。デフォルトでは、パケットはドロップされます。デフォルトのアクションを変更するには、次の手順を実行します。

1. 左側のペインで [Default Action] をクリックします。
2. [鉛筆（Pencil）] アイコンをクリックします。
3. デフォルトのアクションを [Accept] に変更します。
4. [Save Match and Actions] をクリックします。
5. [アクセス制御リストポリシーの保存（Save Access Control List Policy）] をクリックします。

デバイスアクセスポリシーを設定するには、「デバイスアクセスポリシー」を参照してください。

[次へ（Next）] をクリックして、[ルートポリシーの設定（Route Policy page）] ページに移動します。

明示的なアクセスリストと暗示的なアクセスリスト

ローカライズ型データポリシーを介して **policy access-list** コマンドを使用して設定するアクセスリストは、明示的な ACL と呼ばれます。明示的な ACL は、デバイス上の任意の VPN の、どのインターフェイスにも適用できます。

VPN 0 のデバイスのトンネルインターフェイスには、サービスとも呼ばれる暗黙的な *ACL* もあります。一部のサービスはトンネルインターフェイスでデフォルトで有効化されており、無効にしない限り有効のままです。設定で、他のサービスを有効にすることもできます。**allow-service** コマンドで、暗黙的な ACL を設定および変更します。

```
Device(config)# vpn 0
Device(config-vpn)# interface interface-name
Device(config-interface)# tunnel-interface
```

```
Device(config-tunnel-interface)# allow-service service-name
Device(config-tunnel-interface)# no allow-service service-name
```

Cisco IOS XE Catalyst SD-WAN デバイス では、DHCP（DHCPv4 および DHCPv6 の場合）、DNS、および ICMP の各サービスがデフォルトで有効になっています。これら 3 つのサービスにより、トンネルインターフェイスは DHCP、DNS、および ICMP パケットを受け入れることができます。BGP、Netconf、NTP、OSPF、SSHD、および STUN のサービスを有効にすることもできます。

（注） 接続がデバイスから開始され、デバイスで NAT が有効になっている場合（たとえば、ダイレクト インターネット アクセス（DIA）が設定されている場合）、暗黙的な ACL が **no allow-service** として設定されていても、リターントラフィックは NAT エントリによって許可されます。この場合も、明示的な ACL でこのトラフィックをブロックできます。

明示的な ACL と Cisco IOS XE ACL を混同しないようにしてください。Cisco IOS XE ACL は、Cisco Catalyst SD-WAN の明示的および暗黙的 ACL と双方向でやり取りせず、暗黙的 ACL または明示的 ACL を上書きできません。Cisco IOS XE ACL は、トラフィック処理操作の順序において、後で実行されます。

データトラフィックが明示的 ACL と暗黙的 ACL の両方に一致する場合、パケットの処理方法は ACL の設定によって異なります。具体的には、以下に応じて決定されます。

- 暗黙的 ACL が許可（**allow-service** *service-name*）または拒否（**no allow-service** *service-name*）として設定されているかどうか。暗黙的 ACL でサービスを許可することは、明示的 ACL で**許可**アクションを指定することと同じであり、暗黙的 ACL でサービスを許可しないことは、明示的 ACL で**ドロップ**アクションを指定することと同じです。
- 明示的 ACL で、**許可**アクションまたは**拒否**アクションがポリシーシーケンスで設定されているか、デフォルトアクションで設定されているか。

次の表に、暗黙的 ACL と明示的 ACL の両方に一致するトラフィックの処理方法を示します。

表 1:

暗黙的 ACL	**明示的 ACL**：**シーケンス**	**明示的 ACL**：**デフォルト**	**結果**
許可（承認）	拒否（ドロップ）	—	拒否（ドロップ）
許可（承認）	—	拒否（ドロップ）	許可（承認）
拒否（ドロップ）	許可（承認）	—	許可（承認）
拒否（ドロップ）	—	許可（承認）	拒否（ドロップ）

ルートポリシーの設定

[ルートポリシーの設定（Configure Route Policies）] で、ルーティングポリシーを設定します。

1. [ルートポリシーの追加（Add Route Policy）] で、[新規作成（Create New）] を選択します。
2. ルートポリシーの名前と説明を入力します。
3. 左側のペインで、[シーケンスタイプの追加（Add Sequence Type）] をクリックします。左側のペインに [ルート（Route）] ボックスが表示されます。
4. [ルート（Route）] ボックスをダブルクリックし、ルートポリシーの名前を入力します。
5. 右側のペインで、[シーケンスルールの追加（Add Sequence Rule）] をクリックして、ポリシーに単一のシーケンスを作成します。デフォルトでは [マッチ（Match）] が選択されています。
6. [Protocol] ドロップダウンリストから目的のプロトコルを選択します。オプションは、[IPv4]、[IPv6]、またはその両方です。
7. マッチ条件をクリックします。
8. 左側に、マッチ条件の値を入力します。
9. 右側に、ポリシーが一致した場合に実行するアクションを入力します。
10. ステップ 6 ～ 8 を繰り返して、ルートポリシーにマッチ/アクションのペアを追加します。
11. ルートポリシーのマッチ/アクションのペアを並び替えるには、右側のペインでペアを目的の位置にドラッグします。
12. ルートポリシーからマッチ/アクションのペアを削除するには、条件の右上にある [X] をクリックします。
13. [マッチとアクションの保存（Save Match and Actions）] をクリックして、シーケンスルールを保存します。
14. ルートポリシーのシーケンスルールを並び替えるには、左側のペインでルールを目的の位置にドラッグします。
15. ルート ポリシー シーケンス ルールをコピー、削除、または名前変更するには、左側のペインでルール名の横にある **[...]** をクリックし、目的のオプションを選択します。
16. どのルート ポリシー シーケンス ルールにも一致するパケットがない場合、デフォルトのアクションはパケットをドロップすることです。デフォルトのアクションを変更するには、次の手順を実行します。
    1. 左側のペインで [Default Action] をクリックします。
    2. 鉛筆アイコンをクリックします。
    3. デフォルトのアクションを [Accept] に変更します。

4. [Save Match and Actions] をクリックします。

17. [Save Route Policy] をクリックします。

18. [次へ（Next）] をクリックして、[ポリシーの概要（Policy Overview）] ページに移動します。

match パラメータ

アクセスリストパラメータ

アクセスリストがあれば、IPヘッダーのIPプレフィックスおよびフィールドを照合できます。

CLI では、**policy access-list sequence match** コマンドを使用してマッチパラメータを設定します。

access-list の各シーケンスには、マッチ条件が 1 つ含まれている必要があります。

ACLのマッチクラスはサポートされません。書き換えポリシーを使用すればDSCP値を設定できます。

アクセスリストの場合、次のパラメータを照合できます。

一致条件	説明
Class	**policy class-map** コマンドで定義されたクラスの名前。
Destination Data Prefix	data-prefix-list リストの名前。
宛先ポート	単一のポート番号、ポート番号のリスト（スペースで区切られた番号）、またはポート番号の範囲（ハイフン[-]で区切られた2つの番号）を指定します。範囲は0～65535です。
[DSCP]	DSCP 値を指定します。範囲は 0 ～ 63 です。
Protocol	インターネットプロトコル番号を指定します。範囲は 0 ～ 255 です。
ICMP Message	[プロトコル（Protocol）] 値を 1 にすると、[ICMP メッセージ（ICMP Message）] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。 [次ヘッダー（Next Header）]の値を58にすると、[ICMP メッセージ（ICMP Message）] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。 （注） このフィールドは、Cisco IOS XEリリース17.4.1、、Cisco vManageリリース20.4.1 以降で使用できます。 **icmp-msg** および **icmp6-msg** メッセージタイプについては、一元管理型の章にある「ICMP メッセージタイプ/コードと対応する列挙値」の表を参照してください。

一致条件	説明
パケット長（Packet Length）	パケットの長さを指定します。指定できる範囲は 0 ～ 65535 です。単一の長さ、長さのリスト（スペースで区切られた番号）、または長さの範囲（ハイフン [-] で区切られた2つの番号）を指定します。
Source Data Prefix	**data-prefix-list** リストの名前を指定します。
PLP	パケット損失プライオリティ（PLP）（[高（high）]	[低（low）]）を指定します。デフォルトでは、パケットの PLP 値は [低（low）] です。PLP 値を [高（high）] に設定するには、**注釈超過**オプションのあるポリサーを適用します。
送信元ポート	単一のポート番号、ポート番号のリスト（スペースで区切られた番号）、またはポート番号の範囲（ハイフン [-] で区切られた2つの番号）を指定します。範囲は0～65535です。
[TCP]	**syn**

ルートポリシーパラメータ

ルートポリシーの場合、次のパラメータを照合できます。

一致条件	説明
Address	**Prefix-List** リストの名前を指定します。
AS パスリスト	1 つ以上の BGP AS パスリストを指定します。各 AS は、単一の数値または正規表現として記述できます。1 つのパスに複数の AS 番号を指定するには、引用符（" "）でくくってリストに含めます。1 つのリストに複数の AS パスを設定するには、複数の **AS パス**オプションを含め、オプションごとに 1 つの AS パスを指定します。

一致条件	説明
コミュニティ リスト	1 つ以上の BGP コミュニティのリスト。[コミュニティリスト（Community List）] では、次の項目を指定できます。 • *aa*:*nn*：AS 番号とネットワーク番号。各番号は、1 ～ 65535 の範囲の 2 バイト値です。 • **internet**：このコミュニティのルートはインターネットコミュニティにアドバタイズされます。このコミュニティは、すべての BGP 対応ネットワーキングデバイスで構成されます。 • **local-as**：このコミュニティのルートは、ローカル AS 番号以外ではアドバタイズされません。 • **no-advertise**：NO_ADVERTISE コミュニティをルートにアタッチします。このコミュニティのルートは他の BGP ピアにはアドバタイズされません。 • **no-export**：NO_EXPORT コミュニティをルートにアタッチします。このコミュニティのルートは、ローカル AS や BGP コンフェデレーション境界の外にアドバタイズされません。1 つのリストに複数の BGP コミュニティを設定するには、複数の **community** オプションを含め、各オプションに 1 つのコミュニティを指定します。
拡張コミュニティ リスト	1 つ以上の BGP 拡張コミュニティのリストを指定します。[コミュニティ（community）] では、次の項目を指定できます。 • **[rt]**（*aa*:*nn* | *ip-address*）：ルート ターゲット コミュニティ。BGP によって運ばれる一連のルートを受信できる 1 つ以上のルータです。AS 番号とネットワーク番号を 1 ～ 65535 の 2 バイトの数値、または IP アドレスで指定します。 • **[soo]**（*aa*:*nn* | *ip-address*）：ルートオリジンコミュニティ。一連のルートを BGP に挿入できる 1 つ以上のルータです。AS 番号とネットワーク番号を 1 ～ 65535 の 2 バイトの数値、または IP アドレスで指定します。1 つのリストに複数の拡張 BGP コミュニティを設定するには、複数の [community] オプションを含め、各オプションに 1 つのコミュニティを指定します。
BGP ローカル プリファレンス	BGP ローカルプリファレンス番号を指定します。範囲は 0 ～ 4294967295 です。
[メトリック（Metric）]	ルートメトリック値を指定します。範囲は 0 ～ 4294967295 です。
Next Hop	IP プレフィックスリストの名前を指定します。
OMP タグ	OMP タグ番号を指定します。範囲は 0 ～ 4294967295 です。
Origin	BGP 送信元コードを指定します。オプションは、EGP（デフォルト）、IGP、Incomplete です。
OSPF タグ	OSPF タグ番号を指定します。範囲は 0 ～ 4294967295 です。
Peer	ピア IP アドレスを指定します。

アクションパラメータ

アクセスリストパラメータ

パケットがアクセスリストの一致部分の条件に一致すると、そのパケットを受け入れ、ドロップ、またはカウントできます。その後、受け入れられたパケットを分類、ミラーリング、またはポリシングできます。

CLI では、**policy access-list sequence action** コマンドによってアクションパラメータを設定します。

アクセスリストの各シーケンスには、1 つのアクション条件を含めることができます。

アクションでは、最初に一致するデータパケットを受け入れるかドロップするか、およびそれをカウントするかどうかを指定します。

アクション条件	説明
承認	パケットを受け入れます。受け入れられたパケットは、アクセスリストの**アクション**部分に設定された追加パラメータによって変更できます。
カウンタ	カウンタの名前。カウンタ情報を表示するには、Cisco IOS XE Catalyst SD-WAN デバイスで **show policy access-lists counters** コマンドを使用します。
削除（Drop）	パケットを廃棄します。これがデフォルトのアクションになります。

受け入れられたパケットに対して、次のアクションを設定できます。

説明	値または範囲
Class	QoS クラスの名前を指定します。**policy class-map** コマンドを使用して定義することもできます。
Mirror List	ミラーの名前を指定します。これは **policy mirror** コマンドで定義されます。
Policer	**policy policer** コマンドで定義されたポリサーの名前を指定します。
[DSCP]	パケットの DSCP 値を指定します。範囲は 0 ～ 63 です。
Next Hop	IPv4 アドレスを指定します。パケットの転送先となるネクストホップ IP アドレスを設定します。 （注） Cisco vManage リリース 20.5.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、[ネクストホップが使用できない場合にデフォルトルートを使用（Use Default Route when Next Hop is not available）] フィールドが [ネクストホップアクション（Next Hop action）] パラメータの横に表示されます。

ルートポリシーパラメータ

ローカライズ型制御ポリシーの各シーケンスには、1 つのアクション条件を含めることができます。

ルートがルートポリシーの一致部分の条件に一致する場合、そのルートは許可または拒否されます。

受け入れられたパケットに対して、次のアクションを設定できます。

説明	値または範囲
アグリゲータ	BGP ルートアグリゲータが配置されている AS 番号とルートアグリゲータの IP アドレスを設定します。指定できる範囲は 1 ～ 65535 です。
AS パス	AS パスから除外する、または AS パスの先頭に付加する、AS 番号または一連の AS 番号を設定します。指定できる範囲は 1 ～ 65535 です。
アトミック集約	BGP アトミック集約属性を設定します。
Community	BGP コミュニティ値を設定します。 Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、[追加コミュニティ（Community Additive）] オプションフィールドを使用できます。追加オプションは、ルートの既存のコミュニティにコミュニティを追加します。
ローカルプリファレンス	BGP ローカルプリファレンスを設定します。範囲は 0 ～ 4294967295 です。
[メトリック（Metric）]	メトリック値を設定します。範囲は 0 ～ 4294967295 です。
Metric Type	メトリック タイプを設定します。オプションは、type1 または type2 です。
Next Hop	IPv4 アドレスを設定します。パケットの転送先となるネクストホップ IP アドレスを設定します。 （注） Cisco vManage リリース 20.5.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、[ネクストホップが使用できない場合にデフォルトルートを使用（Use Default Route when Next Hop is not available）] フィールドが [ネクストホップアクション（Next Hop action）] パラメータの横に表示されます。
OMP タグ	使用する OSPF の OMP タグを設定します。範囲は 0 ～ 4294967295 です。
Origin	BGP 送信元コードを設定します。オプションは、EGP（デフォルト）、IGP、Incomplete です。
発信元（Originator）	ルートが学習された IP アドレスを設定します。
OSPF タグ	OSPF タグ値を設定します。範囲は 0 ～ 4294967295 です。
重量	BGP の重量を設定します。範囲は 0 ～ 4294967295 です。

ポリシー設定の構成

[ポリシーの概要（Policy Overview）] で、ポリシーを設定します。

1. [ローカライズ型マスターポリシーの名前と説明の入力（Enter name and description for your localized master policy）] ペインで、ポリシーの名前と説明を入力します。
2. [ポリシー設定（Policy Settings）] ペインで、設定するポリシーの適用チェックボックスをオンにします。次のオプションがあります。
   - **[Netflow]**：IPv4 トラフィックのトラフィック フロー モニリングを実行します。
   - **[Netflow IPv6]**：IPv6 トラフィックのトラフィック フローモニタリングを実行します。
   - [アプリケーション（Application）]：IPv4 アプリケーションを追跡して監視します。
   - [アプリケーション IPv6（Application IPv6）]：IPv6 アプリケーションを追跡して監視します。
   - [クラウド QoS（Cloud QoS）]：QoS スケジューリングを有効にします。
   - [クラウド QoS サービス側（Cloud QoS Service Side）]：サービス側で QoS スケジューリングを有効にします。
   - [暗黙的な ACL ロギング（Implicit ACL Logging）]：トラフィック フロー モニタリングを実行するサービスとマッチしないためにドロップされたすべてのパケットのヘッダーをログに記録します。
3. パケットフローのログ記録の頻度を設定するには、[ログ頻度（Log Frequency）] をクリックします。

   パケットフローとは、アクセスリスト（ACL）、cflowd フロー、またはアプリケーション認識型ルーティングフローにマッチするもののことです。
4. [プレビュー（Preview）] をクリックして、CLI 形式でポリシー全体を表示します。
5. [Save Policy] をクリックします。

デバイステンプレートへのローカライズ型データポリシーの適用

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. 新しいデバイステンプレートを作成する場合、次の手順を実行します。
   1. [Device Template] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート（Device Templates）] は [デバイス（Device）] と呼ばれています。

2. [テンプレートの作成（Create Template）] ドロップダウンから、[機能テンプレートから（From Feature Template）] を選択します。
3. [デバイスモデル（Device Model）] ドロップダウンから、Cisco IOS XE Catalyst SD-WAN デバイス の 1 つを選択します。
4. [Template Name] フィールドに、デバイステンプレートの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（–）、下線（_）のみです。スペースやその他の文字を含めることはできません。
5. [Description] フィールドにデバイステンプレートの説明を入力します。このフィールドは必須であり、任意の文字とスペースを含めることができます。
6. ステップ 4 に進みます。

3. 既存のデバイステンプレートを編集する場合は、次の手順を実行します。
   1. [デバイステンプレート（Device Templates）] をクリックし、目的のテンプレートを見つけたら、[...] をクリックして [編集（Edit）] を選択します。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート（Device Templates）] は [デバイス（Device）] と呼ばれています。

   2. [Additional Templates] をクリックします。画面をスクロールして、[追加のテンプレート（Additional Templates）] セクションまで行きます。
   3. [ポリシー（Policy）] ドロップダウンから、設定したポリシーの名前を選択します。
4. [説明（Description）] フィールドのすぐ下にある [追加テンプレート（Additional Templates）] をクリックします。画面をスクロールして、[追加のテンプレート（Additional Templates）] セクションまで行きます。
5. [ポリシー（Policy）] ドロップダウンから、設定したポリシーの名前を選択します。
6. [作成（Create）]（新しいテンプレートの場合）または [更新（Update）]（既存のテンプレートの場合）をクリックします。

ローカライズ型ポリシーのアクティブ化

1. [ローカライズ型ポリシー（Localized Policy）] をクリックして、ポリシーを選択します。
2. 目的のポリシーについて、[...] をクリックし、[アクティブ化（Activate）] を選択します。
3. [ポリシーのアクティブ化（Activate Policy）] ポップアップで、[アクティブ化（Activate）] をクリックして、ネットワーク内の到達可能なすべての Cisco SD-WAN コントローラ にポリシーをプッシュします。

4. **[OK]** をクリックして、すべての Cisco SD-WAN コントローラ でポリシーのアクティブ化を確認します。
5. ローカライズ型ポリシーを非アクティブにするには、**[=]** を選択し、ポリシーを選択します。
6. 目的のポリシーについて、[...] をクリックし、[非アクティブ化（Deactivate）] を選択します。
7. [ポリシーの非アクティブ化（Deactivate Policy）] ポップアップで、[非アクティブ化（Deactivate）] をクリックして、到達可能なすべての Cisco SD-WAN コントローラ からポリシーを削除することを確認します。

ローカライズ型ポリシーの表示

ローカライズ型ポリシーを表示するには、次の手順を実行します。

1. [ローカライズ型ポリシー（Localized Policy）] をクリックして、ポリシーを選択します。
2. UI ポリシービルダーまたは CLI を使用して作成されたポリシーの場合は、[...] をクリックし、[表示（View）] を選択します。UI ポリシー ビルダーを使用して作成されたポリシーはグラフィカル形式で表示され、CLI メソッドを使用して作成されたポリシーはテキスト形式で表示されます。
3. Cisco SD-WAN Manager ポリシー構成ウィザードを使用して作成されたポリシーの場合は、[...] をクリックし、[プレビュー（Preview）] を選択します。このポリシーはテキスト形式で表示されます。

ポリシーのコピー、編集、削除

ポリシーをコピーするには、次の手順を実行します。

1. [ローカライズ型ポリシー（Localized Policy）] をクリックして、ポリシーを選択します。
2. 目的のポリシーについて、[...] をクリックし、[コピー（Copy）] を選択します。
3. [ポリシーのコピー（Policy Copy）] ポップアップウィンドウで、ポリシー名とポリシーの説明を入力します。

（注） Cisco IOS XE リリース 17.2 以降では、次のポリシータイプのポリシー名に 127 文字がサポートされています。

- 中央ルートポリシー
- ローカルルートポリシー
- ローカルアクセス制御リスト（ACL）
- ローカル IPv6 ACL
- 中央データポリシー
- 中央アプリケーション ルート ポリシー
- QoS マップ
- 書き換えルール

他のすべてのポリシー名は 32 文字をサポートします。

4. [コピー（Copy）] をクリックします。

Cisco SD-WAN Manager ポリシー構成ウィザードで作成したポリシーを編集するには、次の手順を実行します。

1. 目的のポリシーについて、[...] をクリックし、[編集（Edit）] を選択します。
2. 必要に応じて、ポリシーを編集します。
3. [ポリシーの変更の保存（Save Policy Changes）] をクリックします。

CLI 方式で作成されたポリシーを編集するには、次の手順を実行します。

1. [カスタムオプション（Custom Options）] ドロップダウンの [ローカライズ型ポリシー（Localized Policy）] で [CLIポリシー（CLI Policy）] を選択します。
2. 目的のポリシーについて、[...] をクリックし、[編集（Edit）] を選択します。
3. 必要に応じて、ポリシーを編集します。
4. [Update] をクリックします。

ポリシーを削除するには、次の手順を実行します。

1. [ローカライズ型ポリシー（Localized Policy）] をクリックして、ポリシーを選択します。
2. 目的のポリシーについて、[...] をクリックし、[削除（Delete）] を選択します。
3. **[OK]** をクリックして、ポリシーの削除を確認します。

CLIを使用した、IPv4に対するローカライズ型ポリシーの設定

Cisco IOS XE Catalyst SD-WAN デバイス で CLI を使用してアクセスリストを設定する手順の概要を次に示します。

1. 必要に応じて、IP プレフィックスのリストを作成します。

```
デバイス(config)# policy lists data-prefix-list ipv4_prefix_list
デバイス(config-data-prefix-list-ipv4_prefix_list)
# ip-prefix 192.168.0.3/24
```

2. QoS の場合は、**class-map ios** を設定します。

```
デバイス(config)# class-map match-any class1
デバイス(config)#  match qos-group 1
class-map match-any class6
match qos-group 6
class-map match-any class7
match qos-group 7
class-map match-any class4
match qos-group 4
class-map match-any class5
match qos-group 5
class-map match-any class2
match qos-group 2
class-map match-any class3
match qos-group 3
class-map match-any class1
match qos-group 1
end
```

（注） ここでは **class-default** を使用しているため、queue2 はオプションです。

3. QoS の場合は、必要に応じて、パケットの外部 IP ヘッダーの DSCP フィールドを上書きする書き換えルールを定義します。

```
デバイス(config)# policy rewrite-rule rule1
デバイス(config-rewrite-rule-rule1)# class class1 low dscp 3
デバイス(config-rewrite-rule-rule1)# class class2 high dscp 4
Will be a table to map class-id → QoS-Group, QID, DSCP, Discard-Class
```

4. QoS の場合、各転送クラスを出力キューにマッピングし、各転送クラスの QoS スケジューラを設定して、QoS スケジューラを QoS マップにグループ化します。

```
デバイス(config)# policy class-map class class1 queue 1
<0..7>[1]
```

5. QoS マップ設定の場合、シェーピングが設定されている場合は、インターフェイス シェーピング設定とマージします。

シェーピングが設定されていない場合は、**qos-map** に対して生成された **policy-map** を適用できます。

```
デバイス(config)# policy-map qos_map_for_data_policy
<name:string
デバイス(config-pmap)# class class1 name:string
デバイス(config-pmap-c)# bandwidth percentage
デバイス(config-pmap-c)# random-detect
```

6. シェーピング設定なしで WAN インターフェイスを設定します。

```
デバイス(config)# policy-map qos_map_for_data_policy name:string
デバイス(config-pmap)# class class1 name:string
デバイス(config-pmap-c)# bandwidth percentage
デバイス(config-pmap-c)# random-detect
```

7. シェーピング設定を使用して WAN インターフェイスを設定します。

```
デバイス(config)# policy-map shaping_interface
デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# shape average 100000000(rate-in-bps)
デバイス(config-pmap-c)# service-policy qos_map_for_data_policy
```

8. **service-policy** を Cisco IOS XE Catalyst SD-WAN デバイス に関連付けます。

```
デバイス(config)# sdwan interface GigabitEthernet 1
デバイス(config-if)# rewrite-rule rule1
デバイス(config-if)# service-policy output qos_map_for_data_policy
```

9. ポリシングパラメータを次のように定義します。

```
デバイス(config)# policy policer policer_On_gige
デバイス(config-policer-policer_On_gige)# rate ?
Description: Bandwidth for 1g interfaces: <8..1000000000>bps; for 10g interfaces:

<8..10000000000>bps
Possible completions:<0..2^64-1>
デバイス(config-policer-policer_On_gige)# burst
Description: Burst rate, in bytes
Possible completions:<15000..10000000>
デバイス(config-policer-policer_On_gige)# exceed drop
```

10. アクセスリストセットをポリサーに関連付けます。

```
デバイス(config)# policy access-list ipv4_acl
デバイス(config-access-list-ipv4_acl)# sequence 100
デバイス(config-sequence-100)# match dscp 10
デバイス(config-match)# exit
デバイス(config-sequence-100)# action accept
デバイス(config-sequence-100)# action count dscp_10_count
デバイス(config-sequence-100)# policer policer_On_gige
デバイス(config-sequence-100)# action drop
vm5(config-action)#
```

11. アクセスリストを LAN または WAN インターフェイスに関連付けます。

```
デバイス(config)# sdwan interface GigabitEthernet5
デバイス(config-interface-GigabitEthernet5)# access-list ipv4_acl
デバイス(config-interface-GigabitEthernet5)# commit
```

CLIを使用した、IPv6に対するローカライズ型ポリシーの設定

以下は、CLI を使用した、アクセスリストを設定する手順の概略です。

1. ポリシングパラメータを次のように定義します。

   ```
   デバイス(config)# policy policer policer_On_gige
   デバイス (config-policer-policer_On_gige)# rate ?
   Description: Bandwidth for 1g interfaces: <8..1000000000>bps;for 10g interfaces:
   <8..10000000000>bps Possible completions: <0..2^64-1>
   デバイス(config-policer-policer_On_gige)# burst
   Description: Burst rate, in bytes Possible completions:<15000..10000000>
   デバイス(config-policer-policer_On_gige)# exceed drop
   ```

2. アクセスリストインスタンスを次のように作成します。

   ```
   デバイス (config)# policy ipv6 access-list ipv6_access_list
   ```

3. 一連のマッチ/アクションペアのシーケンスを次のように作成します。

   ```
   デバイス(config-access-list-ipv6_access_list)# sequence 100
   ```

   マッチ/アクションペアは、最も小さい番号のペアから始まり、ルートがペアのいずれかの条件にマッチしたときに終了するシーケンス番号の順に評価されます。または、マッチが見つからない場合は、デフォルトのアクション（ルートを拒否するか、そのまま受け入れる）が実行されます。

4. 次のように、パケットのマッチパラメータを定義します。

   ```
   デバイス(config-sequence-100)# match traffic-class 10
   デバイス(config-match)# exit
   ```

5. 次のように、マッチしたときに実行するアクションを定義します。

   ```
   デバイス(config-sequence-100)# action accept count traffic_class10_count
   デバイス(config-sequence-100)# action drop
   デバイス(config-sequence-100)# action accept class class1
   デバイス(config-sequence-100)# action accept policer policer_On_gige
   ```

6. 必要に応じて、アクセスリスト内にマッチ/アクションペアの追加の番号付きシーケンスを作成します。

7. パケットがいずれかのシーケンスの条件のどれにもマッチしない場合、そのパケットはデフォルトで拒否されています。マッチしないパケットを受け入れる場合は、アクセスリストのデフォルトアクションを設定します。

8. アクセスリストをインターフェイスに適用します。

```
デバイス(config)# sdwan interface GigabitEthernet5
デバイス(config-interface-GigabitEthernet5)
# ipv6 access-list ipv6_access_list in
デバイス(config-interface-GigabitEthernet5)
# commit
```

インバウンド方向（**in**）にアクセスリストを適用すると、インターフェイスで受信されるパケットに影響が出ます。アウトバウンド方向（**out**）に適用すると、インターフェイスで送信されるパケットに影響が出ます。

ローカライズ型データポリシーの設定例

このトピックでは、ローカライズ型データポリシーを設定する簡単な例をいくつか紹介します。これはポリシーを使用して Cisco Catalyst SD-WAN ドメイン全体のトラフィックフローに影響を与える方法を理解するのに役立ちます。ローカライズされたデータポリシー（アクセスリストとも呼ばれる）は、ローカルの Cisco vEdge デバイス で直接設定されます。

QoS

Quality of Service（QoS）を設定して、 データパケットを分類し、トラフィックが Cisco vEdge デバイスのインターフェイスやインターフェイスキューでどのように出入りするかを制御できます。QoS ポリシーの設定方法の例については、「転送および QoS の設定例」を参照してください。

ICMP Message の例

この例では、ICMP メッセージのローカライズ型データポリシーの設定を表示します。

```
policy
access-list acl_1
 sequence 100
  match
   protocol 1
   icmp-msg administratively-prohibited
  !
  action accept
   count administratively-prohibited
  !
  !
```

ルータ生成 Cisco SD-WAN Manager トラフィックの QoS

表 *2 :* 機能の履歴

機能名	リリース情報	説明
ルータ生成 Cisco SD-WAN Manager トラフィックの QoS	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a	これは、特定の要件に基づいてルータ生成 Cisco SD-WAN Manager トラフィックに優先順位を付けたり、キューイングしたりするのに役立つ機能です。QoS ポリシーとクラスマップを使用して、選択したキューを介して Cisco SD-WAN Manager トラフィックをルーティングします。

ルータ生成 Cisco SD-WAN Manager トラフィックの QoS について

Quality of Service（QoS）は、特定のタイプのトラフィックが他のトラフィックよりも優先されるように、ネットワークトラフィックを管理および優先順位付けするために使用される技術です。QoS は、ネットワークデバイスの管理とモニタリングに使用されるルータ生成 Cisco SD-WAN Manager トラフィックにとって特に重要です。詳細については、「転送と QoS」を参照してください。

ルータ生成トラフィックは、特定の要件に基づいて優先順位を付けたり、キューイングしたりできます。優先順位付けは、QoS ポリシーとクラスマップを使用して実現できます。

ルータ生成トラフィックを選択したキューに入れるには、次の手順を用いてください。

1. CLI テンプレートを使用してクラスマップを定義する：優先するトラフィックのタイプを指定します。この場合、クラスマップを作成して、キューに入れるルータ生成トラフィックを識別します。
2. CLI テンプレートを使用してポリシーマップを定義する：クラスマップで識別されたトラフィックに対して実行するアクションを定義します。優先順位を割り当てる、またはルータ生成トラフィックを特定のキューに配置するポリシーマップを作成します。

ルータ生成 Cisco SD-WAN Manager トラフィックにとっての QoS 上の利点

- ネットワークパフォーマンスの向上：ルータ生成された重要なトラフィックを重要度の低いトラフィックよりも優先することで、ネットワーク管理機能をスムーズに動作させ、ネットワークデバイスを効果的にモニターして制御します。
- ユーザーエクスペリエンスの向上：ルータ生成されたトラフィックをキューイングすることで、ネットワークの輻輳が防止されるので、ユーザー生成されたトラフィックによりネットワーク管理機能に悪い影響が出ません。キューイングにより、ユーザーエクスペリエンスが向上することになります。
- ネットワークの可用性の向上：ネットワーク管理の問題によって引き起こされるネットワークのダウンタイムのリスクを軽減します。これにより、ネットワークの可用性を向上させ、ネットワークの問題による事業運営への影響を軽減します。
- ネットワーク管理の簡素化：ネットワーク管理を簡素化し、手動による介入の必要性を軽減します。簡素化することで、時間の節約になるほか、人的エラーによるリスクの軽減もできるようになります。
- ネットワークリソースの効率的な使用：QoS ポリシーとクラスマップを使用すると、ネットワークリソースの効率的な割り当てができます。これにより、ルータで生成された重要なトラフィックが効率的にフローでき、他のネットワークトラフィックへの影響も最小限に抑えることができます。

ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の制約事項

- ルータ生成 Cisco SD-WAN Manager トラフィックに対して QoS 機能サポートしているのは、Cisco IOS XE Catalyst SD-WAN デバイス のみです。
- ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の設定は、CLI テンプレートを使用する場合にのみ可能です。
- この機能を使用すると、Cisco SD-WAN Manager 用にデバイスが生成するトラフィックに対してのみ、キューを使用して優先順位を付けることができます。他のデータおよび管理プレーントラフィックでは、引き続きデフォルトでキュー 0 を使用します。

CLI テンプレートを使用した、ルータで生成された Cisco SD-WAN Manager トラフィックの QoS の設定

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

クラスマップの定義とキュー番号へのマッピング

1. ローカライズ型ポリシーを使用してクラスマップを定義し、キュー番号にマッピングします。

   policy class-map class *Queue_1* **queue** *2*
2. 変更を確定します。

クラス マップを定義し、キュー番号にマッピングするための設定例の全容を次に示します。

```
config-t
policy class-map class Queue_1 queue 2
!
```

ルータで生成された Cisco SD-WAN Manager トラフィックの QoS の有効化

ここでは、ルータで生成された Cisco SD-WAN Manager トラフィックの QoS を有効にする CLI 設定例を示します。

1. config-policy モードを開始します。

   policy
2. 転送クラスを使用し、優先順位を付けるキューにマッピングしたクラスマップを使用します。

   vmanage-forwarding-class *queue_name*
3. 変更を確定します。

   ルータで生成された Cisco SD-WAN Manager トラフィックの QoS が有効になっています。

ルータで生成された Cisco SD-WAN Manager トラフィックの QoS を有効にする設定例の全容を次に示します。

```
config-t
policy
vmanage-forwarding-class Queue_1
!
```

CLI を使用した、ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の確認

以下は、**show policy-map interface** コマンドで **GigabitEthernet 1** キーワードを指定した場合のサンプル出力例です。

```
Device# show policy-map interface GigabitEthernet 1
```

```
Service-policy output: shape_GigabitEthernet1

  Class-map: class-default (match-any)
    8619 packets, 5056404 bytes
    5 minute offered rate 113000 bps, drop rate 0000 bps
    Match: any
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 8619/5056404
    shape (average) cir 4200000, bc 16800, be 16800
    target shape rate 4200000

    Service-policy : qosmap

      queue stats for all priority classes:
        Queueing
        priority level 1
        queue limit 512 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 565/95064

      Class-map: Queue0 (match-any)
        565 packets, 95064 bytes
        5 minute offered rate 4000 bps, drop rate 0000 bps
        Match: qos-group 0
        police:
            rate 30 %
            rate 1260000 bps, burst 39375 bytes
          conformed 565 packets, 95064 bytes; actions:
            transmit
          exceeded 0 packets, 0 bytes; actions:
            drop
          conformed 4000 bps, exceeded 0000 bps
        Priority: Strict, b/w exceed drops: 0

        Priority Level: 1

      Class-map: Queue_1 (match-any)
        8050 packets, 4961100 bytes                                  ------------------->
        5 minute offered rate 111000 bps, drop rate 0000 bps
        Match: qos-group 1
        Queueing
        queue limit 64 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 8050/4961100
        bandwidth remaining ratio 10

      Class-map: Queue_2 (match-any)
        4 packets, 240 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: qos-group 2
        Queueing
        queue limit 64 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 4/240
        bandwidth remaining ratio 10
```

この例では、それぞれのキューの **Class-map** に、ルータから宛先へのパケット転送の数、サイズ、およびレートが表示されています。Queue_1 に変更があるのを確認でき、パケット転送の追跡ができます。

ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS のトラブルシューティング

問題

CLI を使用して変更をコミットできない

Possible Causes

変更のコミット中に、入力されたキュー名に入力ミスや誤りがあった可能性があります。たとえば、queue 2 ではなく queuee 2 と入力すると、次のエラーが表示されます。「中止：「policy vmanage-traffic-forwarding-class」の不正な参照（Aborted: illegal reference 'policy vmanage-traffic-forwarding-class'）」

ソリューション

ルータからの Cisco SD-WAN Manager トラフィックが通過する正しいキュー名を入力します。

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。