一元管理型ポリシー

（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一元管理型ポリシー、一元管理型ポリシーのコンポーネント、Cisco SD-WAN Manager および CLI を使用した一元管理型ポリシーの設定方法に関する概要を提供します。

一元管理型ポリシーの概要

一元管理型ポリシーとは、Cisco SD-WAN コントローラ 上でプロビジョニングされるポリシーのことであり、Cisco Catalyst SD-WAN オーバーレイネットワーク内の一元管理型コントローラです。

一元管理型ポリシーのタイプ

一元管理型制御ポリシー

一元管理型制御ポリシーは、Cisco Catalyst SD-WAN コントローラ のルートテーブルに保存され、Cisco IOS XE Catalyst SD-WAN デバイス にアドバタイズされる情報に影響を与えることによって、トラフィックのネットワーク全体のルーティングに適用されます。一元管理型制御ポリシーの効果は、Cisco IOS XE Catalyst SD-WAN デバイス がオーバーレイネットワークのデータトラフィックを宛先に送信する方法に見られます。

（注） 一元管理型制御ポリシーの設定自体は Cisco Catalyst SD-WAN コントローラ に残り、ローカルデバイスにプッシュされることはありません。

一元管理型データポリシー

一元管理型データポリシーは、オーバーレイネットワーク内の VPN 全体のデータトラフィックのフローに適用されます。これらのポリシーは、6タプルの一致（送信元と宛先のIPアドレスとポート、DSCPフィールド、プロトコル）またはVPNメンバーシップのいずれかに基づいてアクセスを許可および制限できます。これらのポリシーは、選択した Cisco IOS XE Catalyst SD-WAN デバイス にプッシュされます。

パケットヘッダーフィールドに基づく一元管理型データポリシー

データトラフィックに影響を与えるポリシーの決定は、パケットヘッダーフィールド、具体的には送信元と宛先のIPプレフィックス、送信元と宛先のIPポート、プロトコル、およびDSCPに基づいて行うことができます。

このタイプのポリシーは、ネットワーク内のトラフィックフローを変更するためによく使用されます。次に、一元管理型データポリシーで実行できる制御のタイプの例をいくつか示します。

- ローカルサイト外の任意の宛先にトラフィックを送信できる送信元のセット。たとえば、このようなデータポリシーによって拒否されたローカル送信元は、ローカルネットワーク上のホストとのみ通信できます。
- ローカルサイト外の特定の宛先セットにトラフィックを送信できる送信元のセット。たとえば、このタイプのデータポリシーに一致するローカル送信元は、あるパスを介して音声トラフィックを送信し、別のパスを介してデータトラフィックを送信できます。
- ローカルサイト外の任意の宛先、または特定の宛先の特定のポートにトラフィックを送信できる送信元アドレスと送信元ポート。

Cisco SD-WAN Manager を使用した一元管理型ポリシーの設定

一元管理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。このウィザードは、ポリシーコンポーネントの作成および編集プロセスをガイドする次の操作で構成されています。

- [対象グループの作成（Create Groups of Interest）]：関連する項目をグループ化し、ポリシーの照合やアクションコンポーネントで呼び出すリストを作成します。
- [トポロジとVPNメンバーシップの設定（Configure Topology and VPN Membership）]：ポリシーによって適用されるネットワーク構造を作成します。
- [トラフィックルールの設定（Configure Traffic Rules）]：ポリシーのマッチ条件とアクション条件を作成します。
- [サイトとVPNにポリシーを適用（Apply Policies to Sites and VPNs）]：ポリシーをオーバーレイネットワークのサイトと VPN に関連付けます。
- 一元管理型ポリシーをアクティブ化します。

  一元管理型ポリシーを有効にするには、ポリシーをアクティブ化する必要があります。

Cisco SD-WAN Manager を使用して一元管理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]** を選択します。
2. [Centralized Policy] をクリックします。
3. [Add Policy] をクリックします。

   ポリシー構成ウィザードが表示され、[対象グループの作成（Create Groups of Interest）] ウィンドウが表示されます。

一元管理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、次のセクションの説明に従って、一元管理型ポリシーで使用するリストタイプの新しいグループを作成します。

アプリケーションの構成

1. 対象グループのリストで、[アプリケーション（Application）] をクリックします。

2. [新しいアプリケーションリスト（New Application List）] をクリックします。
3. リストの名前を入力します。
4. [アプリケーション（Application）] または [アプリケーションファミリ（Application Family）] を選択します。

   アプリケーションには、**サードパーティのコントローラ**、**ABC News**、**Mircosoft Teams** など、1 つ以上のアプリケーションの名前を指定できます。Cisco IOS XE Catalyst SD-WAN デバイス では、約 2300 の異なるアプリケーションをサポートしています。サポートされているアプリケーションを一覧表示するには、CLI で **?** と入力します。

   アプリケーションファミリは、次のうちの 1 つ以上となります：**antivirus**、**application-service**、**audio_video**、**authentication**、 **behavioral**、**compression**、**database**、**encrypted**、**erp**、**file-server**、**file-transfer**、**forum**、**game**、**instant-messaging**、**mail**、**microsoft-office**、**middleware**、**network-management**、**network-service**、**peer-to-peer**、**printer**、**routing**、**security-service**、**standard**、**telephony**、**terminal**、**thin-client**、**tunneling**、**wap**、**web**、および **webmail**。
5. [選択（Select）] ドロップダウンの [検索（Search）] フィルタで、必要なアプリケーションまたはアプリケーションファミリを選択します。
6. [Add]をクリックします。

いくつかのアプリケーションリストは事前設定済みです。これらのリストを編集または削除することはできません。

Microsoft_Apps：Excel、Skype、Xbox などの Microsoft アプリケーションが含まれます。Microsoft アプリケーションの完全なリストを表示するには、[エントリ（Entries）] 列のリストをクリックします。

Google_Apps：Gmail、Google マップ、YouTube などの Google アプリケーションが含まれます。Google アプリケーションの完全なリストを表示するには、[エントリ（Entries）] 列のリストをクリックします。

カラーの設定

1. 対象グループのリストで、[色（Color）] をクリックします。
2. [新しいカラーリスト（New Color List）] をクリックします。
3. リストの名前を入力します。
4. [色の選択（Select Color）] ドロップダウンの [検索（Search）] フィルタで、必要な色を選択します。

   色は 3g、biz-internet、blue、bronze、custom1 ～ custom3、default、gold、green、lte、metro-ethernet、mpls、private1 ～ private6、public-internet、red、silver から選択できます。
5. [Add]をクリックします。

1 つのリストで複数の色を構成するには、ドロップダウンから複数の色を選択します。

コミュニティの設定

表 *1*：機能の履歴

機能名	リリース情報	説明
コミュニティの照合および設定機能	Cisco SD-WAN リリース 20.5.1 Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能では、制御ポリシーを使用してコミュニティを照合および設定できます。制御ポリシーは Cisco IOS XE Catalyst SD-WAN デバイス デバイス上で定義および適用され、コミュニティを操作します。 この機能を使用すると、操作可能なルーティングポリシーを基に単一または複数の BGP コミュニティタグをプレフィックスと照合し、割り当てることができます。

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. [標準（Standard）] または [拡張（Expanded）] を選択します。
   - 標準コミュニティリストは、コミュニティやコミュニティ番号の指定に使用されます。
   - 拡張コミュニティ リストは正規表現によるフィルタ コミュニティに使用されます。正規表現は、コミュニティ属性にマッチするパターンを指定するために使用されます。
5. [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。

6. [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（Groups 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. **[IPv4]** または **[IPv6]** を選択します。

5. [データプレフィックスの追加（Add Data Prefix）] フィールドに、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。

6. [Add]をクリックします。

ポリサーの構成

1. 対象グループリストで、[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. ポリシングパラメータを定義します。

   1. [バースト（Burst）] フィールドに、最大トラフィックバーストサイズ（15,000 ～ 10,000,000 バイト）を入力します。

   2. [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）] を選択した場合、パケット損失の優先順位（PLP）が**低く**設定されます。

   [リマーク（remark）] を選択した場合、パケット損失の優先順位（PLP）が**高く**設定されます。

   3. [レート（Rate）] フィールドに、最大トラフィックレートを 0～2^{64}–1 ビット/秒（bps）の値で入力します。

5. [Add]をクリックします。

プレフィックスの構成

1. 対象グループのリストで、[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. [プレフィックスの追加（Data Prefix）] フィールドに、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。
5. [Add]をクリックします。

サイトの設定

1. 対象グループのリストで、[サイト（Site）] をクリックします。
2. [新しいサイトリスト（New Site List）] をクリックします。
3. リストの名前を入力します。
4. [サイトの追加（Add Site）] フィールドに、1 つ以上のサイト ID をコンマで区切って入力します。

   たとえば、100 または 200 をコンマで区切るか、1 から 4294967295 の範囲で指定します。
5. [Add]をクリックします。

アプリプローブクラスの設定

1. 対象グループのリストで、[アプリケーションプローブクラス（App Probe Class）] をクリックします。
2. [新しいアプリケーションプローブクラス（New App Probe Class）] をクリックします。
3. [プローブクラス名（Prob Class Name）] フィールドにプローブクラス名を入力します。
4. [転送クラス（Forwarding Class）] ドロップダウンリストから必要な転送クラスを選択します。
5. [エントリ（Entries）] ペインで、[色（Color）] ドロップダウンリストから適切な色を選択し、**DSCP** 値を入力します。

   必要に応じて、**[+]** 記号をクリックしてエントリを追加できます。
6. [Save] をクリックします。

SLA クラスの構成

1. 対象グループのリストで、[SLAクラス（SLA Class）] をクリックします。
2. [新しいSLAクラスのリスト（New SLA Class List）] をクリックします。
3. リストの名前を入力します。

4. SLA クラスのパラメータを定義します。
    1. [損失（Loss）] フィールドに、接続の最大パケット損失を 0 ～ 100% の値で入力します。
    2. [遅延（Latency）] フィールドに、接続の最大パケット遅延を 0 ～ 1,000 ミリ秒の値で入力します。
    3. [ジッター（Jitter）] フィールドに、接続の最大ジッターを 1 ～ 1,000 ミリ秒の値で入力します。
    4. [アプリケーションプローブクラス（App Probe Class）] ドロップダウンリストから、必要なアプリケーション プローブ クラスを選択します。
5. （オプション）[フォールバックのベストトンネル（Fallback Best Tunnel）] チェックボックスをオンにして、最適なトンネル基準を有効にします。

    このオプションフィールドは Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a から利用できるので、SLA が満たされていない場合に、使用可能なカラーからベストパスまたは色を選択できます。このオプションを選択すると、ドロップダウンから必要な基準を選択できます。基準には、損失、遅延、およびジッターの値を 1 つ以上組み合わせます。
6. ドロップダウンリストから [基準（Criteria）] を選択します。使用可能な基準は次のとおりです。
    - 遅延
    - 損失
    - Jitter
    - 遅延、損失
    - 遅延、ジッター
    - 損失、遅延
    - 損失、ジッター
    - ジッター、遅延
    - ジッター、損失
    - 遅延、損失、ジッター
    - 遅延、ジッター、損失
    - 損失、遅延、ジッター
    - 損失、ジッター、遅延
    - ジッター、遅延、損失
    - ジッター、損失、遅延

7. 選択した基準の**損失バリアンス（%）**、**遅延バリアンス（ミリ秒）**、および**ジッターバリアンス（ミリ秒）**を入力します。
8. [Add]をクリックします。

TLOC の設定

1. 対象グループのリストで、**[TLOC]** をクリックします。
2. [新しいTLOCリスト（New TLOC List）] をクリックします。[TLOCリスト（TLOC 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. **[TLOC IP]** フィールドに、TLOC のシステム IP アドレスを入力します。
5. [色（Color）] フィールドで、TLOC の色を選択します。
6. [カプセル化（Encap）]フィールドで、カプセル化のタイプを選択します。
7. [プリファレンス（Preference）] フィールドで、必要に応じて、TLOC に関連付けるプリファレンスを選択します。

   指定できる範囲は 0 ～ 4294967295 です。
8. [TLOC の追加（Add TLOC）] をクリックして、別の TLOC をリストに追加します。
9. [Save] をクリックします。

（注） `set tloc` および `set tloc-list` コマンドを使用するには、set-vpn コマンドを使用する必要があります。

TLOC ごとに、アドレス、色、カプセル化を指定します。必要に応じて、TLOC アドレスに関連付けるプリファレンス値（0 ～ 232 - 1）を設定します。アクションの受け入れ条件で TLOC リストを適用する場合、複数の TLOC が使用可能でマッチ条件を満たす場合、最も高いプリファレンス値を持つ TLOC が使用されます。2 つ以上の TLOC が最も高いプリファレンス値である場合、トラフィックは ECMP 方式によってそれらの間で送信されます。

VPN の設定

1. 対象グループのリストで、**[VPN]** をクリックします。
2. [新しいVPNリスト（New VPN List）] をクリックします。
3. リストの名前を入力します。
4. [VPNの追加（Add VPN）] フィールドに、1 つ以上の VPN ID をコンマで区切って入力します。

   たとえば、100 または 200 をコンマで区切るか、1 から 65530 の範囲で指定します。

5. [Add]をクリックします。

リージョンの設定

最小リリース：Cisco vManage リリース 20.7.1

マルチリージョンファブリック（以前の階層型SD-WAN）のリージョンのリストを設定するには、**[管理（Administration）] > [設定（Settings）]** でマルチリージョンファブリックが有効になっていること）を確認します。

1. 対象グループのリストで、[リージョン（Region）] をクリックします。
2. [New Region List] をクリックします。
3. [リージョンリスト名（Region List Name）] フィールドに、リーションのリスト名を入力します。
4. [リージョンの追加（Add Region）] フィールドに、1 つ以上のリージョンをコンマで区切って入力するか、範囲を入力します。

   たとえば、リージョン 1、3 をコンマで指定するか、範囲 1 から 4 を指定します。
5. [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 [トポロジと VPN メンバーシップの設定（Configure Topology and VPN Membership）] に移動します。

優先カラーグループの設定

表 *2:* 機能の履歴

機能名	リリース情報	説明
優先するデータプレーントンネルの優先グループを選択します。	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、アプリケーション認識型ルーティング（AAR）の優先カラーとバックアップ優先カラーのランク付けのサポートが追加されます。Cisco IOS XE Catalyst SD-WAN デバイス の色またはパスの設定に基づいて、最大 3 段階の優先順位を設定できます。

トランスポート設定の順序を設定して、転送トラフィックの優先順位を選択できます。

1. 対象グループのリストで、[優先カラーグループ（Preferred Color Group）] をクリックします。
2. [New Preferred Color Group] をクリックします。
3. [優先カラーグループ名（Preferred Color Group Name）] フィールドに、優先カラーグループの名前を入力します。
4. [プライマリカラー（Primary Colors）] ペインで、次の手順を実行します。

1. [カラーの設定（Color Preference）] ドロップダウンリストでカラーの設定を選択します。
2. [パスの設定（Path Preference）] ドロップダウンリストでパスの設定を選択します。

フィールド	説明
Preferred Color Group Name	優先カラーグループの名前を入力します。
Color Preference	ドロップダウンリストでカラーの設定を選択します。次のオプションがあります。 • デフォルト • 3g • biz-internet • ブルー • bronze • custom1 • custom2 など 複数の色を選択できます。
Path Preference	ドロップダウンリストでパスの設定を選択します。次のオプションがあります。 • [Direct Path]：送信先デバイスと宛先デバイス間のダイレクトパスのみを使用します。 • [マルチホップパス（Multi Hop Path）]： マルチリージョンファブリックネットワークでは、ダイレクトパスが使用可能な場合でも、コアリージョンを含むマルチホップパスを送信先デバイスと宛先デバイス間で使用します。 • [All Paths]：送信先デバイスと宛先デバイス間の任意のパスを使用します。 （注） このオプションは、パス設定をまったく構成しないことと同じです。ポリシーを マルチリージョン ファブリック ネットワーク以外に適用する場合は、このオプションを使用します。

5. [セカンダリカラー（Secondary Colors）] ペインで、次の手順を実行します。
   1. [カラーの設定（Color Preference）] ドロップダウンリストでカラーの設定を選択します。

2. [パスの設定（Path Preference）] ドロップダウンリストでパスの設定を選択します。

6. [ターシャリカラー（Tertiary Colors）] ペインで、次の手順を実行します。
   1. [カラーの設定（Color Preference）] ドロップダウンリストでカラーの設定を選択します。
   2. [パスの設定（Path Preference）] ドロップダウンリストでパスの設定を選択します。
7. [Add]をクリックします。

色のランク付けを設定する場合は、次のガイドラインが役立ちます。

- プライマリ設定は必須であり、各優先順位レベルで少なくとも 1 つの優先パスまたはカラーを設定する必要があります。両方を設定することもできます。
- 複数のカラーを設定できます。
- パスの設定がされていない場合、すべてのパスは使用可能な優先色によって制約されます。
- パスの設定の制約内でカラーが設定されていない場合は、すべての色を使用できます。
- 設定は優先順位の高い順に適用され、トラフィックを転送するパスまたはカラーを決定します。

プライマリカラー、セカンダリカラー、およびターシャリカラーがダウンしている場合、パケットはドロップされません。トラフィックは通常のルーティング設定にフォールバックし、他の色がアップしているかどうかを選択します。

WAN Insights（WANI）の Cisco SD-WAN Manager への統合

表 *3:* 機能の履歴

機能名	リリース情報	説明
WAN Insights ポリシーの自動化	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	この機能を使用すると、Cisco SD-WAN Analytics で使用可能な推奨事項を Cisco SD-WAN Manager AAR ポリシーに適用し、適用された推奨事項を Cisco SD-WAN Manager で表示させることができます。

Cisco SD-WAN Analytics は、Cisco Catalyst SD-WAN 向けのクラウドベースの分析サービスであり、アプリケーションとネットワークのパフォーマンスについて包括的なインサイトを提供するものです。分析サービスは、Cisco DNA Advantage と Cisco DNA Premier ソフトウェアをサブスクリプションすると利用できます。Cisco SD-WAN Analytics では、トラフィックフローに関するメタデータを収集してクラウドストレージに保存し、収集したデータに基づいて分析を生

成します。予測パス分析によって生成されるパスの推奨事項は、長期に渡るインサイトに基づいています。これらの推奨事項は、Cisco SD-WAN Manager で手動で作成するポリシーに変換し、ネットワークに適用する必要があります。

予測パス推奨事項は、アクティブな推奨事項を実用的な一元管理型AARポリシーに適用して、Cisco Catalyst SD-WAN ネットワーク内の転送に関する決定に影響を与えられる機能です。推奨事項はAARポリシーの一部として適用されてから、Cisco SD-WAN コントローラ にプッシュされます。予測パス推奨事項のSD-WAN ネットワークへの適用にあたっては、AAR ポリシーの TLOC 設定として適用されます。

予測パス推奨事項の使用に関する詳細は、「予測パスの推奨事項」を参照してください。

予測パス推奨事項の適用

Cisco SD-WAN Analytics に予測パスの推奨事項がある場合は、次の手順を実行して、推奨事項をアプリケーション認識型ルーティングポリシーに適用します。

1. Cisco SD-WAN Manager メニューで、右上隅にあるベルのアイコンをクリックします。[通知（Notifications）] ペインにアクティブなアラームが表示されます。
2. [通知（Notifications）] ペインに [アクティブな推奨事項（Active Recommendations）] がある場合は、サイトをクリックして推奨事項を確認します。または、Cisco SD-WAN Manager メニューから **[分析（Analytics）]** > **[予測ネットワーク（Predictive Networks）]** の順にクリックして確認することもできます。
3. [アクティブな推奨事項（Active Recommendations）] をクリックし、[適用（Apply）] をクリックします。
4. [予測パス推奨事項の適用（Apply Predictive Path Recommendations）] ウィンドウで、[適用に進む（Proceed to Apply）] をクリックして新しい推奨事項を適用します。

   適用された推奨事項は、Cisco SD-WAN Manager によって生成された設定で確認し、 Cisco SD-WAN コントローラ にプッシュできます。

考慮すべき点

- Cisco SD-WAN Manager は、ログイン時に推奨事項をプルします。推奨事項を更新する場合は、ページを更新するか、ログインし直します。
- Cisco SD-WAN Manager は、一部の AAR ポリシーにのみ関連付けられているアプリケーションリストの推奨事項をサポートします。特定のアプリケーションリストに AAR ポリシーが存在しない場合、推奨事項は無効であり、ポリシー処理は実行されません。
- WAN Insights は、AAR ポリシーが定義されていない場合でも、標準アプリケーショングループ の推奨事項を生成します。ただし、AAR ポリシーが定義されていないため、ポリシーの自動化は実行されません。
- 同じサイトとアプリケーションリストに対し、WANIによって、適用される推奨事項の終端が生成され、なおかつ別の推奨事項も生成される場合、推奨事項は設定に基づいて適用されます。

- Cloud OnRamp for SaaS に対する WANI 推奨事項の適用はサポートされていません。

予測パス推奨事項

WAN Insights (WANI) を使用すれば、現在のネットワーク設定のパフォーマンスを追跡し、ポリシーとパスを調整して最高のユーザー体験を実現できます。 予測パスの推奨事項は、AAR ポリシーの TLOC 設定に影響を及ぼします。

WAN Insights は、アプリケーショントラフィックの最適なパスを見つけるために、統計モデルを使用して Cisco Catalyst SD-WAN の履歴データを調査する予測ネットワーク最適化ツールです。WANI では、アプリケーション トラフィック フロー中にエクスポートされたテレメトリデータを分析し、SLA 違反（低品質のパフォーマンスなど）の発生する可能性を減らすパスについて、長期的な推奨事項を生成します。

予測ネットワークは、アプリケーションの SLA 違反を検出するために、AAR ポリシーで定義されている各アプリケーションリストに SLA を関連付けます。これは、特定のサイトおよび TLOC で SLA 違反の可能性を計算し、推奨事項を生成するために使用されます。

データポリシーに関する対象グループの構成の詳細については、「一元管理型ポリシーの対象グループの構成」を参照してください。

トポロジと VPN メンバーシップの設定

[トポロジとVPNメンバーシップの設定（Configure Topology and VPN Membership）] ウィンドウを初めて開くと、デフォルトで [トポロジ（Topology）] ウィンドウが表示されます。

トポロジと VPN メンバーシップを設定するには、次の手順を実行します。

ハブアンドスポーク

1. [トポロジの追加（Add Topology）] ドロップダウンで、[ハブアンドスポーク（Hub-and-Spoke）] を選択します。
2. ハブアンドスポークポリシーの名前を入力します。
3. ポリシーの説明を入力します。
4. [VPN リスト（VPN Lists）] フィールドで、ポリシーの VPN リストを選択します。
5. 左側のペインで、[ハブアンドスポークの追加（Add Hub-and-Spoke）] をクリックします。テキスト文字列 [マイハブアンドスポーク（My Hub-and-Spoke）] を含むハブアンドスポーク ポリシー コンポーネントが左側のペインに追加されます。
6. [マイハブアンドスポーク（My Hub-and-Spoke）]のテキスト文字列をダブルクリックし、ポリシーコンポーネントの名前を入力します。
7. 右側のペインで、次のようにネットワークトポロジにハブサイトを追加します。
   1. [ハブサイトの追加（Add Hub Sites）] をクリックします。
   2. [サイトリスト（Site List）] フィールドで、ポリシーコンポーネントのサイトリストを選択します。

3. [Add]をクリックします。
4. ポリシーコンポーネントにさらにハブサイトを追加するには、これらの手順を繰り返します。

8. 右側のペインで、ネットワークトポロジにスポークサイトを追加します。
   1. [スポークサイトの追加（Add Spoke Sites）] をクリックします。
   2. [サイトリストフィールド（Site List Field）] で、ポリシーコンポーネントのサイトリストを選択します。
   3. [Add]をクリックします。
   4. ポリシーコンポーネントにさらにスポークサイトを追加するには、これらの手順を繰り返します。
9. 必要に応じて手順を繰り返して、ハブアンドスポークポリシーにコンポーネントを追加します。
10. [ハブアンドスポークポリシーの保存（Save Hub-and-Spoke Policy）] をクリックします。

[メッシュ（Mesh）]

1. [トポロジの追加（Add Topology）] ドロップダウンで、[メッシュ（Mesh）] を選択します。
2. メッシュ リージョン ポリシー コンポーネントの名前を入力します。
3. メッシュ リージョン ポリシー コンポーネントの説明を入力します。
4. [VPN リスト（VPN Lists）] フィールドで、ポリシーの VPN リストを選択します。
5. [新しいメッシュリージョン（New Mesh Region）] をクリックします。
6. [メッシュリージョン名（Mesh Region Name）] フィールドに、個々のメッシュリージョンの名前を入力します。
7. [サイトリスト（Site List）] フィールドで、メッシュ領域に含める 1 つ以上のサイトを選択します。
8. [Add]をクリックします。
9. メッシュリージョンをさらにポリシーに追加するには、これらの手順を繰り返します。
10. [メッシュトポロジの保存（Save Mesh Topology）] をクリックします。

カスタム制御（ルートおよびTLOC）：一元管理型ルート制御ポリシー（OMP ルートの照合用）

1. [トポロジの追加（Add Topology）] ドロップダウンで、[カスタム制御（ルートおよび TLOC）（Custom Control (Route & TLOC））] を選択します。
2. 制御ポリシーの名前を入力します。

3. ポリシーの説明を入力します。
4. 左側のペインで、[シーケンスタイプ（Sequence Type）] をクリックします。[カスタム制御ポリシーの追加（Add Custom Control Policy）] ポップアップウィンドウが表示されます。
5. [ルート（Route）] を選択します。テキスト文字列 [ルート（Route）] を含むポリシーコンポーネントが左側のペインに追加されます。
6. [ルート（Route）] のテキスト文字列をダブルクリックし、ポリシーコンポーネント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（Sequence Rule）] をクリックします。[マッチ/アクション（Match/Actions）] ボックスが開き、デフォルトで [マッチ（Match）] が選択されています。
8. [マッチ（Match）] ボックスの下に表示されるボックスから、目的のポリシー照合タイプを選択します。次に、そのマッチ条件の値を選択または入力します。必要に応じて、シーケンスルールの追加のマッチ条件を設定します。
9. [Actions] をクリックします。デフォルトでは、[拒否（Reject）] オプションが選択されています。受け入れられたパケットで実行するアクションを設定するには、[受け入れ（Accept）] オプションをクリックします。次に、アクションを選択するか、アクションの値を入力します。
10. [Save Match and Actions] をクリックします。
11. 必要に応じて、[シーケンスルール（Sequence Rule）] をクリックして、シーケンスルールをさらに設定します。並べ替えるには、ドラッグアンドドロップします。
12. 必要に応じて、[シーケンスタイプ（Sequence Type）] をクリックして、シーケンスをさらに設定します。並べ替えるには、ドラッグアンドドロップします。
13. [制御ポリシーの保存（Save Control Policy）] をクリックします。

カスタム制御（ルートおよび TLOC）：一元管理型 TLOC 制御ポリシー（TLOC ルートの照合用）

1. [トポロジの追加（Add Topology）] ドロップダウンで、[カスタム制御（ルートおよび TLOC）（Custom Control (Route & TLOC））] を選択します。
2. 制御ポリシーの名前を入力します。
3. ポリシーの説明を入力します。
4. 左側のペインで、[シーケンスタイプ（Sequence Type）] をクリックします。[カスタム制御ポリシーの追加（Add Custom Control Policy）] ポップアップウィンドウが表示されます。
5. **[TLOC]** を選択します。テキスト文字列 **[TLOC]** を含むポリシーコンポーネントが左側のペインに追加されます。

6. **[TLOC]** のテキスト文字列をダブルクリックし、ポリシーコンポーネント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（Sequence Rule）] をクリックします。[マッチ/アクション（Match/Actions）] ボックスが開き、デフォルトで [マッチ（Match）] が選択されています。
8. [マッチ（Match）] ボックスの下に表示されるボックスから、目的のポリシー照合タイプを選択します。次に、そのマッチ条件の値を選択または入力します。必要に応じて、シーケンスルールの追加のマッチ条件を設定します。
9. [Actions] をクリックします。デフォルトでは、[拒否（Reject）] オプションが選択されています。受け入れられたパケットで実行するアクションを設定するには、[受け入れ（Accept）] オプションをクリックします。次に、アクションを選択するか、アクションの値を入力します。
10. [Save Match and Actions] をクリックします。
11. 必要に応じて、[シーケンスルール（Sequence Rule）] をクリックして、シーケンスルールをさらに設定します。並べ替えるには、ドラッグアンドドロップします。
12. 必要に応じて、[シーケンスタイプ（Sequence Type）] をクリックして、シーケンスをさらに設定します。並べ替えるには、ドラッグアンドドロップします。
13. [制御ポリシーの保存（Save Control Policy）] をクリックします。

一元管理型制御ポリシーは、マッチとアクションがペアになったシーケンスで構成されています。シーケンスには番号が付けられ、ポリシー内のマッチとアクションのペアごとにルートや TLOC の分析順序が設定されます。

（注） シーケンスには、ポリシー用に **match app-list** または **dns-app-list** を設定させられますが、両方を設定することはできません。ポリシーに対して **match app-list** と **dns-app-list** の両方を設定することはできない仕組みになっています。

一元管理型制御ポリシーの各シーケンスには、1 つのマッチ条件（ルートまたは TLOC 用）と 1つのアクション条件を含めることができます。

Default Action

選択されたルートやTLOCが、一元管理型制御ポリシーのマッチ条件のいずれにもマッチしない場合、デフォルトアクションが適用されます。デフォルトでは、ルートまたはTLOCが拒否されるようになっています。

選択されたデータパケットが、データポリシーのマッチ条件のいずれにもマッチしない場合、デフォルトのアクションがパケットに適用されます。デフォルトでは、データパケットがドロップされるようになっています。

既存のトポロジのインポート

1. [トポロジの追加（Add Topology）] ドロップダウンで、[既存のトポロジのインポート（Import Existing Topology）] をクリックします。[既存のトポロジのインポート（Import Existing Topology）] ポップアップが表示されます。
2. トポロジのタイプを選択します。
3. [ポリシータイプ（Policy Type）] で、インポートするトポロジの名前を選択します。
4. [ポリシー（Policy）] ドロップダウンで、インポートするポリシーを選択します。

（注） ポリシー構成ウィザードでは、他の一元管理型ポリシー（データ、制御、またはアプリケーション認識型ルーティング）のインスタンスのように、設定済みのポリシーをインポートすることはできません。ポリシー全体を設定する必要があります。

5. [Import] をクリックします。

[次へ（Next）] をクリックして、ウィザードの [トラフィックルールの設定（Configure Traffic Rules）] に移動します。

VPN メンバーシップポリシーの作成

1. [ネットワークトポロジの指定（Specify your network topology）] エリアで、[VPNメンバーシップ（VPN Membership）] をクリックします。
2. [VPNメンバーシップポリシーの追加（Add VPN Membership Policy）] をクリックします。

（注） 一度に追加できる VPN メンバーシップは 1 つだけなので、すべてのサイトリストと VPN リストを1つのポリシーに含める必要があります。

[VPNメンバーシップポリシーの追加（Add VPN Membership Policy）] ポップアップが表示されます。

3. VPN メンバーシップポリシーの名前と説明を入力します。
4. [サイトリスト（Site List）] フィールドで、サイトリストを選択します。
5. [VPN リスト（VPN Lists）] フィールドで、VPN リストを選択します。
6. [リストの追加（Add List）] をクリックして、VPNメンバーシップに別のVPNを追加します。
7. [Save] をクリックします。

8. [次へ（Next）] をクリックして、ウィザードの [トラフィックルールの設定（Configure Traffic Rules）] に移動します。

トラフィックルールの設定

表 4 : 機能の履歴

機能名	リリース情報	説明
ICMP メッセージとのポリシー照合	Cisco IOS XE リリース 17.4.1 Cisco vManage リリース 20.4.1	これは、一元管理型データポリシー、ローカライズ型データポリシー、およびアプリケーション認識型ルーティングポリシー向けに ICMP メッセージのリストを指定する場合に使用可能な新しいマッチ条件に対応できるようにする機能です。

[トラフィックルールの設定（Configure Traffic Rules）] ウィンドウを初めて開くと、デフォルトで、[アプリケーション認識型ルーティング（Application-Aware Routin）] が選択されています。

作成済みの AAR ルーティングポリシーについては、このページで確認することもできます。このページには、ポリシーの名前、タイプ、モード、説明、更新者、最終更新の詳細など、ポリシーに関連するさまざまな情報が記載されています。

（注） [モード（Mode）] 列を参照すると、ポリシーのセキュリティステータスが確認できます。ステータスは、ポリシーが統合セキュリティで使用されているかどうかを見分けるのに役立ちます。モードステータスは、セキュリティポリシーにのみ適用され、一元管理型またはローカライズ型ポリシーには関係ありません。

Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローのトラフィックルールの設定の詳細については、「Cisco Catalyst SD-WANアプリケーションインテリジェンスエンジン」を参照してください。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

一元管理型データポリシーのトラフィックルールを設定するには、次の手順を実行します。

1. [トラフィックデータ（Traffic Data）] をクリックします。
2. [ポリシーの追加（Add Policy）] ドロップダウンをクリックします。
3. [Create New] をクリックします。[データポリシーの追加（Add Data Policy）] ウィンドウが表示されます。

4. データポリシーの名前と説明を入力します。
5. 右側のペインで、[シーケンスタイプ（Sequence Type）] をクリックします。[データポリシーの追加（Add Data Policy）] ポップアップウィンドウが開きます。
6. 作成するデータポリシーのタイプを [アプリケーションファイアウォール（Application Firewall）]、[QoS]、[トラフィックエンジニアリング（Traffic Engineering）]、[カスタム（Custom）] から選択します。

（注） 同じマッチ条件に対して複数のデータポリシーのタイプを設定する場合は、カスタムポリシーを設定する必要があります。

7. **アプリケーション**、**ファイアウォール**、**QoS**、**トラフィック エンジニアリング**、または**カスタム**のテキスト文字列を含むポリシーシーケンスが左側のペインに追加されます。
8. 該当するテキスト文字列をダブルクリックして、ポリシーシーケンスの名前を入力します。入力した名前は、左側のペインと右側のペインの両方にある [シーケンスタイプ（Sequence Type）] リストに表示されます。
9. 右側のペインで、[シーケンスルール（Sequence Rule）] をクリックします。[マッチ/アクション（Match/Action）] ボックスが開き、デフォルトで [マッチ（Match）] が選択されています。使用可能なポリシーのマッチ条件は、ダイアログボックスの下に一覧表示されます。

一致条件	手順
なし（すべてのパケットに一致）	マッチ条件を指定しないでください。

一致条件	手順
アプリケーション/アプリケーション ファミリー リスト	1. [マッチ（Match）] 条件で、[アプリケーション/アプリケーションファミリリスト（Applications/Application Family List）] をクリックします。 2. ドロップダウンで、アプリケーションファミリを選択します。 3. アプリケーションリストを作成するには、次の手順を実行します。 1. [新しいアプリケーションリスト（New Application List）] をクリックします。 2. リストの名前を入力します。 3. [アプリケーション（Application）] をクリックして、個々のアプリケーションのリストを作成します。[アプリケーションファミリ（Application Family）] をクリックして、関連するアプリケーションのリストを作成します。 4. [アプリケーションの選択（Select Application）] ドロップダウンで、目的のアプリケーションまたはアプリケーションファミリを選択します。 5. [Save] をクリックします。 このマッチ条件は、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 の IPv6 トラフィックに使用できます。
Destination Data Prefix	1. [マッチ（Match）] 条件で、[接続先データプレフィックス（Destination Data Prefix）] をクリックします。 2. 接続先プレフィックスのリストと照合するには、ドロップダウンから該当するリストを選択します。 3. 個々の宛先プレフィックスと照合するには、[宛先：IPプレフィックス（Destination: IP Prefix）] フィールドにプレフィックスを入力します。
宛先ポート	1. [マッチ（Match）] 条件で、[接続先ポート（Destination Port）] をクリックします。 2. [宛先ポート（Destination Port）] フィールドにポート番号を入力します。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。
DNS アプリケーションリスト（DNS Application List）	スプリット DNS を有効にするには、アプリケーションリストを追加します。 1. [マッチ（Match）] 条件で、[DNS アプリケーションリスト（DNS Application List）] をクリックします。 2. ドロップダウンで、アプリケーションファミリを選択します。 このマッチ条件は、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 の IPv6 トラフィックに使用できます。

一致条件	手順
DNS	アプリケーションリストを追加して、スプリットDNS要求を処理します。 **1.** [マッチ（Match）] 条件で、[DNS] をクリックします。 **2.** DNS アプリケーションの DNS 要求を処理するには、ドロップダウンで [要求（Request）] を選択し、アプリケーションの DNS 応答を処理するには [応答（Response）] を選択します。
[DSCP]	**1.** [マッチ（Match）] 条件で、[DSCP] をクリックします。 **2.** **[DSCP]** フィールドに、DSCP 値を 0 ～ 63 の数値で入力します。
パケット長（Packet Length）	**1.** [マッチ（Match）] 条件で、[パケット長（Packet Length）] をクリックします。 **2.** [パケット長（Packet Length）] フィールドに、パケット長を 0 ～ 65535 の値で入力します。
PLP	**1.** [マッチ（Match）] 条件で、[PLP] をクリックして、[パケット損失の優先順位（Packet Loss Priority）] を設定します。 **2.** [PLP] ドロップダウンで、[低（Low）] または [高（High）] を選択します。PLP を [高（High）] に設定するには、[注釈超過（exceed remark）] オプションのあるポリサーを適用します。
Protocol	**1.** [マッチ（Match）] 条件で、[プロトコル（Protocol）] をクリックします。 **2.** [プロトコル（Protocol）] フィールドに、インターネットプロトコル番号を 0 ～ 255 の数字で入力します。
ICMP Message	ICMP メッセージと照合するには、[プロトコル（Protocol）] フィールドで、インターネットプロトコル番号を 1、58、またはその両方に設定します。 （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。
Source Data Prefix	**1.** [マッチ（Match）] 条件で、[送信元データプレフィックス（Source Data Prefix）] をクリックします。 **2.** 送信元プレフィックスのリストと照合するには、ドロップダウンから該当するリストを選択します。 **3.** 個々の送信元プレフィックスと照合するには、[送信元（Source）] フィールドにプレフィックスを入力します。

一致条件	手順
送信元ポート	**1.** [マッチ（Match）] 条件で、[送信元ポート（Source Port）] をクリックします。 **2.** [送信元（Source）] フィールドに、ポート番号を入力します。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。
[TCP]	**1.** [マッチ（Match）] 条件で、[TCP] をクリックします。 **2.** **[TCP]** フィールドで指定できるオプションは **[SYN]** だけです。

10. QoS およびトラフィック エンジニアリングのデータポリシーの場合：[プロトコル（Protocol）] ドロップダウンリストから [IPv4] を選択すると、ポリシーは IPv4 アドレスファミリのみに適用されます。[IPv6] を選択すると、ポリシーは IPv6 アドレスファミリのみに適用されます。ポリシーを IPv4 と IPv6 のアドレスファミリに適用するには、[両方（Both）] を選択します。

11. 1 つ以上の**マッチ**条件を選択するには、ボックスをクリックし、説明に従って値を設定します。

（注） すべてのポリシーシーケンスタイプですべてのマッチ条件を使用できるわけではありません。

12. マッチするデータトラフィックに対して実行するアクションを選択するには、[アクション（Actions）] ボックスをクリックします。

13. マッチするトラフィックをドロップするには、[ドロップ（Drop）] をクリックします。使用可能なポリシーアクションが右側に表示されます。

14. マッチするトラフィックを受け入れるには、[受け入れ（Accept）] をクリックします。使用可能なポリシーアクションが右側に表示されます。

15. 説明に従ってポリシーアクションを設定します。

（注） すべての一致条件ですべてのアクションを使用できるわけではありません。

アクション条件	説明	手順
カウンタ	条件にマッチするデータパケットをカウントします。	**1.** [アクション（Action）] 条件で、[カウンタ（Counter）] をクリックします。 **2.** [カウンタ名（Counter Name）] フィールドに、パケットカウンタを保存するファイルの名前を入力します。

アクション条件	説明	手順
[DSCP]	条件がマッチするデータパケットに DSCP 値を割り当てます。	1. [アクション（Action）] 条件で、[DSCP] をクリックします。 2. **[DSCP]** フィールドに、DSCP 値を 0 ～ 63 の数値で入力します。
Forwarding Class	条件がマッチするデータパケットに転送クラスを割り当てます。	1. [マッチ（Match）] 条件で、[転送クラス（Forwarding Class）] をクリックします。 2. [転送クラス（Forwarding Class）] フィールドで、クラス値を 32 文字以内で入力します。
Log	サポートされる最小リリース：Cisco vManage リリース 20.11.1 および Cisco IOS XE リリース 17.11.1a ロギングを有効にするには、[ログ（Log）] をクリックします。 （DP、AAR、または ACL）データポリシーパケットにログアクションが設定されている場合、ログが生成され、syslog に記録されます。グローバルな **log-rate-limit** により、すべてのログがログに記録されるわけではありません。パケットヘッダーが最初にログに記録される際、syslog メッセージが生成され、その後もフローがアクティブである限り、5 分ごとに syslog メッセージが生成されます。	1. [アクション（Action）] 条件で、[ログ（Log）] をクリックしてロギングを有効にします。
Policer	条件がマッチするデータパケットにポリサーを適用します。	1. [マッチ（Match）] 条件で、[ポリサー（Policer）] をクリックします。 2. [ポリサー（Policer）] ドロップダウンフィールドで、ポリサーの名前を選択します。

アクション条件	説明	手順
損失の修正	条件がマッチするデータパケットに損失の修正を適用します。 前方誤り訂正（FEC）では、冗長データの送信によってリンク上で失われたパケットが回復されるため、受信者はデータの再送信を要求することなくエラーを訂正できます。 FECはIPSecトンネルでのみサポートされ、GREトンネルではサポートされません。 • [FEC 適応（FEC Adaptive）]：対応するパケットは、通過するトンネルが測定された損失に基づいて信頼できないと見なされた場合にのみ、FEC の対象となります。 [FEC適応（FEC Adaptive）] を選択すると、追加の [損失しきい値] フィールドが表示され、FEC を自動的に有効にするためのパケット損失のしきい値を指定できます。 適応FECは、パケット損失が2%になると機能し始めます。この値は設定可能です。 1～5%の損失しきい値を指定できます。デフォルトのパケット損失しきい値は 2% です。 • [FEC 常時（FEC Always）]： 対応するパケットは常に FEC の対象となります。 • [パケット複製（Packet Duplication）]： 単一のトンネルを経由して重複パケットを送信します。複数のトンネルが使用可能な場合、重複パケットは、最適なパラメータを使用してトンネル経由で送信されます。	1. [マッチ（Match）] 条件で、[損失の修正（Loss Correction）] をクリックします。 2. [損失の修正（Loss Correction）] フィールドで、[FEC適応（FEC Adaptive）]、[FEC 常時（FEC Always）]、または [パケット複製（Packet Duplication）] を選択します。
[Save Match and Actions] をクリックします。		

16. 必要に応じて、追加のシーケンスルールを作成します。ルールをドラッグアンドドロップして再配置します。
17. [データポリシーの保存（Save Data Policy）] をクリックします。
18. [次へ（Next）] をクリックして、ウィザードの [サイトとVPNにポリシーを適用（Apply Policies to Sites and VPNs）] に移動します。

マッチパラメータ：制御ポリシー

OMP および TLOC ルートの場合、次の属性を一致させることができます。

一致条件	説明
カラーリスト	1 つ以上の色。使用できる色は、3g、biz-internet、blue、bronze、custom1、custom2、custom3、default、gold、green、lte、metro-ethernet、mpls、private1～private6、public-internet、red、silver です。
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）] フィールドでは、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。
種類	コミュニティタイプを指定します。[標準（Standard）] を選択してコミュニティとコミュニティ番号を指定するか、[拡張（Expanded）] を選択して正規表現を使用してコミュニティをフィルタリングします。正規表現は、コミュニティ属性にマッチするパターンを指定するために使用されます。

一致条件	説明
OR 条件	コミュニティリストの各正規表現文字列をルートのコミュニティ文字列と比較します。 OR条件は複数のコミュニティリストに適用され、すべてのデバイスで有効です。 Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、コミュニティの [タイプ（Types）] フィールドと [条件（Criteria）] フィールドを使用できます。
OMP タグ	デバイスのルーティングデータベース内のルートまたはプレフィックスに関連付けられたタグ値。 範囲は 0 ～ 4294967295 です。
Origin	ルートが学習されたプロトコル。
発信元（Originator）	ルートが学習された IP アドレス。
パスタイプ	Cisco 階層型 SD-WAN アーキテクチャでは、パスタイプに応じてルートが照合されます。パスタイプは以下のとおりです。 • **階層パス**：アクセスリージョンから境界ルータへのホップを含むルート。リージョン0を経由して別の境界ルータへと進み、別のアクセスリージョン内のエッジルータへと続きます。 • **ダイレクトパス**：あるエッジルータから別のエッジルータへのダイレクトパスルート。 • **トランスポート ゲートウェイ パス**：トランスポートゲートウェイ機能が有効になっているルータによって再発信されるルート。 （注） このオプションは、Cisco vManage リリース 20.8.1 以降で使用できます。

一致条件	説明
優先順位	プレフィックスの優先度。これは、ルートまたはプレフィックスがローカルサイト（デバイスのルーティングデータベース）に持つプレファレンス値です。プリファレンス値が大きいほど優先されます。指定できる範囲は 0 ～ 255 です。
プレフィックス リスト	1 つ以上のプレフィックス。プレフィックス リストの名前を指定します。
Cisco SD-WAN Manager では使用できません。	個々のサイト識別子。 範囲は 0 ～ 4294967295 です。
サイト	1 つ以上のオーバーレイネットワークのサイト識別子。
[地域（Region）]	Cisco 階層型 SD-WAN 用に定義されたリージョン。 指定できる範囲は 1 ～ 63 です。 （注） このオプションは、Cisco vManage リリース 20.7.1 以降で使用できます。
ロール（Role）	Cisco 階層型 SD-WAN アーキテクチャでは、デバイスタイプ（**境界ルータ**または**エッジルータ**）に応じて照合が実行されます。 （注） このオプションは、Cisco vManage リリース 20.8.1 以降で使用できます。
TLOC	個々の TLOC アドレス。 （注） `set tloc` および `set tloc-list` コマンドを使用するには、set-vpn コマンドを使用する必要があります。
VPN	個々の VPN 識別子。範囲は 0～65535です。
キャリア	制御トラフィックのキャリア。値は、デフォルト、carrier1 ～ carrier 8 です。

一致条件	説明
ドメイン ID	TLOC に関連付けられたドメイン識別子。 範囲は 0 ～ 4294967295 です。
OMP タグ	デバイスのルートテーブル内の TLOC ルートに関連付けられているタグ値。 範囲は 0 ～ 4294967295 です。
サイト	個々のサイトのコントリビュータまたは複数のオーバーレイ ネットワーク サイトの識別子。 範囲は 0 ～ 4294967295 です。

CLI では、**policy control-policy sequence match route** コマンドで一致するように OMP ルート属性を設定し、**policy control-policy sequence match tloc** コマンドで一致するように TLOC 属性を設定します。

マッチパラメータ：データポリシー

一元管理型データポリシーは、IP ヘッダー内の IP プレフィックスとフィールド、およびアプリケーションを照合できます。スプリット DNS を有効にすることもできます。

ポリシー内の各シーケンスには、1 つ以上のマッチ条件を含めることができます。

表 *5*:

一致条件	説明
省略	すべてのパケットに一致。
アプリケーション/アプリケーション ファミリ リスト（Application/Application Family List）	アプリケーションまたはアプリケーションファミリ。 このマッチ条件は、Cisco IOS XE リリース17.9.1a および Cisco vManage リリース20.9.1 以降の IPv6 トラフィックで使用できます。
Destination Data Prefix	宛先プレフィックス、IP プレフィックス、およびプレフィックス長のグループ。範囲は0から65535です。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。

一致条件	説明
Destination Region（宛先リージョン）	次のいずれかを選択します。 • [Primary]：宛先デバイスが送信元と同じプライマリリージョン（アクセスリージョンとも呼ばれる）にある場合、トラフィックに一致します。このトラフィックは、コアリージョンを通過するマルチホップパスを使用して宛先に到達します。 • [Secondary]：宛先デバイスが送信元と同じプライマリリージョンにないが、送信元と同じセカンダリリージョンにある場合、トラフィックに一致します。このトラフィックは、セカンダリリージョンで説明されているように、ダイレクトトンネルを使用して宛先に到達できます。 • [Other]：宛先デバイスが送信元と同じプライマリリージョンまたはセカンダリリージョンにない場合、トラフィックに一致します。このトラフィックには、送信元から宛先へのマルチホップパスが必要です。 （注） 最小リリース：Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a
DNSアプリケーションリスト（DNS Application List）	スプリットDNSを有効にして、アプリケーションごとにDNS要求と応答を解決および処理します。**app-list** リストの名前。このリストは、DNS要求が処理されるアプリケーションを指定します。 このマッチ条件は、Cisco IOS XE リリース17.9.1a および Cisco vManage リリース20.9.1 以降の IPv6 トラフィックで使用できます。
DNS	DNSパケットを処理する方向を指定します。アプリケーションによって送信されたDNS要求（アウトバウンド DNS クエリ用）を処理するには、**dns request** を指定します。DNSサーバーからアプリケーションに返されるDNS応答を処理するには、**dns response** を指定します。
[DSCP]	DSCP 値を指定します。
パケット長	パケット長を指定します。範囲は 0 から 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。
パケット損失優先順位（PLP）（Packet Loss Priority (PLP)）	パケット損失の優先順位を指定します。デフォルトでは、パケットの PLP 値は **low** です。PLP 値を [**high**] に設定するには、[**exceed remark**] オプションのあるポリサーを適用します。
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。

一致条件	説明
ICMP メッセージ（ICMP Message）	プロトコル（IPv4）の場合、プロトコル値を1と入力すると、[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。同様に、プロトコル値に 58 を入力すると、プロトコル IPv6 の [ICMP メッセージ（ICMP Message）] フィールドが表示されます。 [プロトコル（Protocol）] で [両方（Both）] を選択すると場合、[ICMPメッセージ（ICMP Message）] または [ICMPv6メッセージ（ICMPv6 Message）] フィールドが表示されます。 （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。
Source Data Prefix	送信元プレフィックスのグループまたは個々の送信元プレフィックスを指定します。
送信元ポート	送信元ポート番号を指定します。範囲は0から65535です。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。
TCP フラグ	TCP フラグの syn を指定します。
トラフィック転送先（Traffic To）	マルチリージョン ファブリック アーキテクチャでは、境界ルータがサービスを提供しているアクセスリージョン、コアリージョン、またはサービス VPN に流れる境界ルータトラフィックを照合します。 （注） 最小リリース：Cisco vManage リリース 20.8.1

表 *6 : ICMP* メッセージのタイプ/コードと対応する列挙値

Type	コード	列挙型
0	0	echo-reply

3		unreachable
	0	net-unreachable
	1	host-unreachable
	2	protocol-unreachable
	3	port-unreachable
	4	packet-too-big
	5	source-route-failed
	6	network-unknown
	7	host-unknown
	8	host-isolated
	9	dod-net-prohibited
	10	dod-host-prohibited
	11	net-tos-unreachable
	12	host-tos-unreachable
	13	administratively-prohibited
	14	host-precedence-unreachable
	15	precedence-unreachable
5		redirect
	0	net-redirect
	1	host-redirect
	2	net-tos-redirect
	3	host-tos-redirect
8	0	echo
9	0	router-advertisement
10	0	router-solicitation
11		time-exceeded
	0	ttl-exceeded
	1	reassembly-timeout
12		parameter-problem
	0	general-parameter-problem
	1	option-missing
	2	no-room-for-option
13	0	timestamp-request

14	0	timestamp-reply
40	0	photuris
54	0	extended-echo
43		extended-echo-reply
	0	echo-reply-no-error
	1	malformed-query
	2	interface-error
	3	table-entry-error
	4	multiple-interface-match

表 *7 : ICMPv6* メッセージのタイプ/コードと対応する列挙値

Type	コード（**Code**）	列挙型
1		unreachable
	0	no-route
	1	no-admin
	2	beyond-scope
	3	destination-unreachable
	4	port-unreachable
	5	source-policy
	6	reject-route
	7	source-route-header
2	0	packet-too-big
3		time-exceeded
	0	hop-limit
	1	reassembly-timeout
4		parameter-problem
	0	Header
	1	next-header
	2	parameter-option
128	0	echo-request
129	0	echo-reply
130	0	mld-query

131	0	mld-report
132	0	mld-reduction
133	0	router-solicitation
134	0	router-advertisement
135	0	nd-ns
136	0	nd-na
137	0	redirect
138		router-renumbering
	0	renum-command
	1	renum-result
	255	renum-seq-number
139		ni-query
	0	ni-query-v6-address
	1	ni-query-name
	2	ni-query-v4-address
140		ni-response
	0	ni-response-success
	1	ni-response-refuse
	2	ni-response-qtype-unknown
141	0	ind-solicitation
142	0	ind-advertisement
143		mldv2-report
144	0	dhaad-request
145	0	dhaad-reply
146	0	mpd-solicitation
147	0	mpd-advertisement
148	0	cp-solicitation
149	0	cp-advertisement
151	0	mr-advertisement
152	0	mr-solicitation
153	0	mr-termination
155	0	rpl-control

アクションパラメータ：制御ポリシー

マッチ条件ごとに、ルートまたはTLOCが制御ポリシーに一致した場合に実行する対応するアクションを設定します。

CLI では、**policy control-policy action** コマンドでアクションを設定します。

一元管理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。

アクションでは、まず、一致するルートまたは TLOC を受け入れるか拒否するかを指定します。

表 *8*：

説明	Cisco SD-WAN Manager
ルートを受け入れます。受け入れられたルートは、ポリシー設定の**アクション**部分で設定された追加パラメータによって変更できます。	[承認（Accept）] をクリック
パケットを廃棄します。	[**Reject**] をクリックします。

次に、受け入れられるルートまたは TLOC に対して、以下のアクションを設定できます。

アクション条件	説明
エクスポート先	指定した VPN または VPN のリストにルートをエクスポートします（**一致ルート**マッチ条件の場合のみ）。 範囲は 0 ～ 65535 またはリスト名です。
OMP タグ	ルート、プレフィックス、または TLOC のタグ文字列を変更します。 範囲は 0 ～ 4294967295 です。
優先順位	ルート、プレフィックス、またはTLOCのプリファレンス値を指定された値に変更します。プリファレンス値が高いほど優先されます。範囲は 0 ～ 255 です。
Service	トラフィックを宛先に配信する前にトラフィックをリダイレクトするサービスを指定します。 TLOC アドレスまたは TLOC のリストは、サービスに到達するためにトラフィックをリダイレクトする必要がある TLOC を識別します。TLOC が複数ある場合、トラフィックは TLOC 間でロードバランシングされます。 VPN 識別子は、サービスが配置されている場所です。 標準サービス：**FW**、**IDS**、**IDP** カスタムサービス：**netsvc1**、**netsvc2**、**netsvc3**、**netsvc4** **vpn service** 設定コマンドを使用して、サービスデバイスと同じ場所に配置されている Cisco IOS XE Catalyst SD-WAN デバイスでサービス自体を設定します。

アクション条件	説明
TLOC	TLOC アドレス、色、およびカプセル化を指定されたアドレスと色に変更します。 TLOC ごとに、アドレス、色、およびカプセル化を指定します。*address* はシステム IP アドレスです。*color* には次のいずれかの色を指定します：**3g**、**biz-internet**、**blue**、**bronze**、**custom1**、**custom2**、**custom3**、**default**、**gold**、**green**、**lte**、**metro-ethernet**、**mpls**、**private1** ～ **private6**、**public-internet**、**red**、**silver**。*encapsulation* は **gre** または **ipsec** です。必要に応じて、TLOC アドレスに関連付けるプリファレンス値（0 ～ 232 - 1）を設定します。**アクションの受け入れ**条件で TLOC リストを適用する場合、複数の TLOC が使用可能でマッチ条件を満たす場合、最も高いプリファレンス値を持つ TLOC が使用されます。2 つ以上の TLOC が最も高いプリファレンス値である場合、トラフィックは ECMP 方式によってそれらの間で送信されます。
TLOC アクション	アクションで指定されたメカニズムを使用して、一致するルートまたは TLOC を直接指定し、最終的な宛先が到達可能かどうかのエンドツーエンドのトラッキングを有効にします。 TLOC アクションオプションを設定すると、Cisco Catalyst SD-WAN コントローラ が最終的な宛先デバイスへのパスをエンドツーエンドでトラッキングできるようになります。

（注） **preferences** コマンドは、インバウンドとアウトバウンドのトラフィックをトンネルに向けるためのプリファレンスを制御します。設定は 0 ～ 4294967295（232 – 1）の値で、デフォルト値は 0 です。高い値が低い値に優先します。

Cisco vEdge device に 2 つ以上のトンネルがあるとき、すべての TLOC のプリファレンスが同じで、トラフィックフローに影響を与えるポリシーが適用されていない場合、すべての TLOC が OMP にアドバタイズされます。ルータがトラフィックを送受信するときは、ECMP を使用して、トラフィックフローをトンネル間で均等に分散します。

アクションパラメータ：データポリシー

表 *9:* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイス のパス設定のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	Cisco IOS XE Catalyst SD-WAN デバイス に拡張され、ポリシーアクションに対して 1 つ以上のローカル トランスポート ロケータ（TLOC）を選択することをサポートします。
データポリシーを使用した SIG へのトラフィックリダイレクト	Cisco IOS XE リリース 17.4.1 Cisco vManage リリース 20.4.1	この機能を使用すると、データポリシーの作成時に、アプリケーションリストを他の一致基準とともに定義し、アプリケーション トラフィックをセキュア インターネット ゲートウェイ（SIG）にリダイレクトできます。

機能名	リリース情報	説明
データポリシーにおけるネクストホップアクションの拡張	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能は、Cisco IOS XE Catalyst SD-WAN デバイスで設定された機能との同等になるよう、一元管理型データポリシーの一致アクション条件を強化します。next-hop-loose アクションを設定している場合、この機能はネクストホップアドレスを使用できない際に、アプリケーション トラフィックを使用可能なルートにリダイレクトするのに役立ちます。
データポリシーを使用したSIGへのトラフィック リダイレクション：ルーティングへのフォールバック	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能を使用すると、すべての SIG トンネルがダウンしている場合に、フォールバックメカニズムとして、インターネットに向かうトラフィックが Cisco Catalyst SD-WAN オーバーレイを介してルーティングされるように設定できます。
ローカライズ型データポリシーと一元管理型データポリシーの両方のログアクション	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	この機能では、Cisco IOS XE Catalyst SD-WAN デバイスでデータポリシーを設定する際に、データポリシー、アプリケーション ルート ポリシー、およびローカライズ型ポリシーのログアクションパラメータを設定できます。 log パラメータを使用すると、パケットがログに記録され、syslog メッセージを生成できます。フローがアクティブな場合、ログは 5 分ごとに外部の syslog サーバーにエクスポートされます。**policy log-rate-limit** コマンドを使用して、設定されたレートに従ってポリシーログを制御できます。

データトラフィックが一元管理型データポリシーの一致部分の条件に一致した場合、パケットを受け入れるか、ドロップできます。その後、受け入れられたパケットにパラメータを関連付けることができます。

CLI では、**policy data-policy vpn-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。

一元管理型データ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。

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（Accept）] をクリック	パケットを受け入れます。受け入れられたパケットは、ポリシー設定のアクション部分で設定された追加パラメータで変更できます。
Cflowd	cflowd トラフィックモニタリングを有効にします。

アクション条件	説明
カウンタ	受け入れられたパケットまたはドロップされたパケットをカウントします。カウンタの名前を指定します。Cisco IOS XE Catalyst SD-WAN デバイス 上で **show policy access-lists counters** コマンドを使用します。
[ドロップ（Drop）] をクリック	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。
ログ	最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a および Cisco vManage リリース 20.11.1 ロギングを有効にするには、[ログ（Log）] をクリックします。 （DP、AAR、または ACL）データポリシーパケットにログアクションが設定されている場合、ログが生成され、syslog に記録されます。グローバルな **log-rate-limit** により、すべてのログがログに記録されるわけではありません。パケットヘッダーが最初にログに記録される際、syslog メッセージが生成され、その後もフローがアクティブである限り、 5 分ごとに syslog メッセージが生成されます。 **policy log-rate-limit** の CLI に関する詳細については、「 **policy log-rate-limit** command in the Cisco Catalyst SD-WAN Qualified Command Reference」ガイドを参照してください。
リダイレクト DNS	DNS 要求を特定の DNS サーバーにリダイレクトします。DNS 要求のリダイレクトはオプションですが、リダイレクトする場合は両方のアクションを指定する必要があります。 インバウンドポリシーの場合、**redirect-dns host** によって、DNS 応答が要求元のサービス VPN に正しく転送されるようになります。 アウトバウンドポリシーの場合は、DNS サーバーの IP アドレスを指定してください。 （注） Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以降のリリースにアップグレードする場合は、**nat use-vpn 0** を介してリダイレクト DNS を設定して、DNS をダイレクト インターネット インターフェイス（DIA）にリダイレクトする必要があります。 （注） 同じシーケンスのアクションとして redirect-dns でローカル TLOC プリファレンスのみを設定できますが、リモート TLOC は設定できません。 （注） リダイレクト DNS と SIG を同時に設定することはできません。

アクション条件	説明
TCP 最適化	TCPを微調整してラウンドトリップ遅延を減らし、TCPトラフィックのマッチング全体を向上させます。
セキュア インターネット ゲートウェイ	アプリケーション トラフィックを SIG にリダイレクト （注） アプリケーション トラフィックを SIG にリダイレクトするデータポリシーを適用する前に、SIG トンネルを設定しておく必要があります。 自動 SIG トンネルの設定の詳細については、「Automatic Tunnels」を参照してください。手動 SIG トンネルの設定の詳細については、「Manual Tunnels」を参照してください。 [ルーティングにフォールバック（Fallback to Routing）] チェックボックスをオンにして、すべての SIG トンネルがダウンしている場合に、インターネットに向かうトラフィックを Cisco SD-WAN オーバーレイ経由でルーティングします。このオプションは、Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 で導入されました。

（注） Cisco IOS XE Catalyst SD-WAN デバイス では、TCP 最適化が削除されると、最適化が進行中のすべてのフローがドロップされます。

次に、受け入れられるパケットに対して以下のパラメータを設定できます。

アクション条件	説明
Cflowd	cflowd トラフィックモニタリングを有効にします。
NAT プールまたは **NAT VPN**	NAT機能を有効にして、トラフィックをインターネットやその他の外部接続先に直接リダイレクトできるようにします。
[DSCP]	DSCP 値。範囲は 0 ～ 63 です。
Forwarding Class	転送クラスの名前。

アクション条件	説明
ローカル TLOC	色およびカプセル化に一致する TLOC の 1 つにパケットを送信できるようにします。使用できる色は、3g、biz-internet、blue、bronze、custom1、custom2、custom3、default、gold、green、lte、metro-ethernet、mpls、private1～private6、public-internet、red、silver です。 カプセル化オプションは、**ipsec** および **gre** です。 デフォルトでは、TLOC が使用できない場合、トラフィックは代替 TLOC を使用して転送されます。TLOC が使用できない場合にトラフィックをドロップするには、**restrict** オプションを含めます。 デフォルトでは、カプセル化は **ipsec** です。
Next Hop	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 IOS XE Catalyst SD-WAN リリース 17.5.1a および Cisco vManage リリース 20.5.1 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。このオプションは、シーケンスタイプが [トラフィックエンジニアリング（Traffic Engineering）] または [カスタム（Custom）] で、プロトコルが **IPv4** または **IPv6** のいずれかの場合にのみ使用でき、両方では使用できません。
Policer	ポリサーを適用します。**policy policer** コマンドで設定されたポリサーの名前を指定します。

アクション条件	説明
Service	トラフィックを宛先に配信する前にリダイレクトするサービスを指定します。 TLOC アドレスまたは TLOC のリストは、サービスに到達するためにトラフィックをリダイレクトする必要があるリモート TLOC を識別します。TLOC が複数ある場合、トラフィックは TLOC 間でロードバランシングされます。 VPN 識別子は、サービスが配置されている場所です。 標準サービス：**FW**、**IDS**、**IDP** カスタムサービス：**netsvc1**、**netsvc2**、**netsvc3**、**netsvc4** TLOC リストは、**policy lists tloc-list** リストで設定されます。 **vpn service** コマンドを使用して、サービスデバイスと併置された Cisco IOS XE Catalyst SD-WAN デバイス でサービス自体を設定します。
TLOC	リスト内のいずれかの TLOC の IP アドレス、色、およびカプセル化に一致するリモート TLOC にトラフィックを転送します。一致する TLOC にプリファレンス値が設定されている場合、その値がトラフィックに割り当てられます。
[承認（Accept）] をクリックし、[VPN] アクションを実行	パケットが属する VPN を設定します。範囲は 0 ～ 65530です。

（注） データポリシーは、マッチ条件が「一般（generic）」の場合、ルーティングプロトコルパケットを含むローカルで生成されたパケットに適用されます。

設定例：

```
sequence 21
   match
    source-ip 10.0.0.0/8
   action accept
```

このような状況では、ルーティングプロトコルパケットをエスケープするシーケンスを、データポリシーに追加する必要がある場合があります。たとえば、OSPF をスキップするには、次の設定を使用します。

```
sequence 20
   match
    source-ip 10.0.0.0/8
    protocol  89
   action accept
sequence 21
   match
    source-ip 10.0.0.0/8
   action accept
```

次の表では、IPv4 および IPv6 のアクションについて説明します。

表 *10*：

IPv4 アクション	IPv6 アクション
drop、dscp、next-hop（from-service のみ）/vpn、count、転送クラス、ポリサー（インターフェイス ACL のみ）、App-route SLA（のみ）	該当なし
app-route preferred color、app-route sla strict、cflowd、nat、redirect-dns	該当なし
該当なし	drop、dscp、next-hop/vpn、count、転送クラス、ポリサー（インターフェイス ACL のみ） App-route SLA（のみ）、App-route preferred color、app-route sla strict
ポリサー（DataPolicy）、tcp-optimization、fec-always、	ポリサー（DataPolicy）
tloc、tloc-list（set tloc、set tloc-list）	tloc、tloc-list（set tloc、set tloc-list）
App-Route backup-preferred color、local-tloc、local-tloc-list	App-Route backup-preferred color、local-tloc、local-tloc-list

サイトと VPN へのポリシーの適用

[サイトと VPN にポリシーを適用（Apply Policies to Sites and VPNs）] ページで、サイトと VPN にポリシーを適用します。

1. [ポリシー名（Policy Name）] フィールドに、ポリシー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。
2. [ポリシーの説明（Policy Description）] フィールドに、ポリシーの説明を入力します。最大 2048 文字を使用できます。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。
3. ポリシーを VPN とサイトに関連付けます。VPN とサイトの選択肢は、ポリシーブロックのタイプによって異なります。
    1. [トポロジ（Topology）] ポリシーブロックの場合は、[新しいサイトリスト（New Site List）]、[インバウンドサイトリスト（Inbound Site List）]、[アウトバウンドサイトリスト（Outbound Site List）]、または [VPNリスト（VPN List）] をクリックします。トポロジブロックによっては[追加（Add）]ボタンがない場合があります。1つ以上のサイトリストを選択し、1つ以上のVPNリストを選択します。[Add]をクリックします。

2. [アプリケーション認識型ルーティング（Application-Aware Routing）] ポリシーブロックの場合は、[新しいサイトリスト（New Site List）] と [VPNリスト（VPN list）] をクリックします。1つ以上のサイトリストを選択し、1つ以上の VPN リストを選択します。[Add]をクリックします。
3. [トラフィックデータ（Traffic Data）] ポリシーブロックの場合は、[新しいサイトリストとVPNリスト（New Site List and VPN List）] をクリックします。ポリシーを適用する方向（[サービスから（From Service）]、[トンネルから（From Tunnel）]、[すべて（All）]）を選択し、1 つ以上のサイトリストおよび 1 つ以上の VPN リストを選択します。[Add]をクリックします。
4. cflowd ポリシーブロックの場合は、[新しいサイトリスト（New Site List）] をクリックします。1 つ以上のサイトリストを選択し、[追加（Add）] をクリックします。

4. [プレビュー（Preview）] をクリックして、設定されたポリシーを表示します。ポリシーはCLI形式で表示されます。
5. [Save Policy] をクリックします。**[設定（Configuration）]** > **[ポリシー（Policies）]** を選択すると、ポリシーテーブルに新しく作成されたポリシーが表示されます。

Cisco IOS XE Catalyst SD-WAN デバイス での NAT フォールバック

	リリース情報	
Cisco IOS XE Catalyst SD-WAN デバイス での NAT フォールバック	Cisco IOS XE リリース 17.3.2 Cisco vManage リリース 20.3.2	Cisco IOS XE Catalyst SD-WAN デバイスでは、ダイレクトインターネットアクセス（DIA）の NAT フォールバック機能をサポートしています。NAT フォールバック機能は、DIA ルートに送信されるすべてのトラフィックが必要に応じて代替ルートを使用できるよう、ルーティングベースのメカニズムを提供します。このリリースでは、サービス側とトンネル側でフォールバックがサポートされます。

（注） Cisco SD-WAN Manager を使用して NAT DIA フォールバックを設定するには、Cisco SD-WAN Manager によって Cisco Catalyst SD-WAN コントローラ が管理される必要があります。

Cisco SD-WAN Manager を使用して NAT フォールバックを有効にするには、次の手順を実行してデータポリシーを作成および設定します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [カスタムオプション（Custom Options）] ドロップダウンの [一元管理型ポリシー（Centralized Policy）] で [トラフィックポリシー（Traffic Policy）] を選択します。
3. [トラフィックデータ（Traffic Data）] をクリックします。
4. [ポリシーの追加（Add Policy）] ドロップダウンから、[新規作成（Create New）] を選択します。
5. [シーケンスタイプ（Sequence Type）] をクリックし、[カスタム（Custom）] を選択します。
6. [(+)シーケンスルール（Sequence Rule）] をクリックして、新規のシーケンスルールを作成します。
7. マッチ条件を追加したら、[アクション（Actions）]、[承認（Accept）] の順にクリックします。
8. [NAT VPN] をクリックし、[フォールバック（Fallback）] チェックボックスをオンにします。
9. [アクションの保存と照合（Save and Match Actions）] をクリックします。
10. [データポリシーの保存（Save Data Policy）] をクリックします。

既存の一元管理型ポリシーを編集し、ポリシーをインポートします。

1. [一元管理型ポリシー（Centralized Policy）] をクリックし、必要な一元管理型ポリシーの [...] をクリックして [編集（Edit）] を選択します。
2. [トラフィックルール（Traffic Rules）] をクリックし、[トラフィックデータ（Traffic Data）] を選択します。
3. [ポリシーの追加（Add Policy）] ドロップダウンから、[既存のインポート（Import Existing）] を選択します。
4. [ポリシー（Policy）] ドロップダウンから、作成した NAT ポリシーを選択します。
5. [ポリシー適用（Policy Application）] をクリックし、[トラフィックデータ（Traffic Data）] を選択します。
6. [+新しいサイトリストとVPNリスト（+ New Site List and VPN List）] をクリックします。
7. 必要に応じて、方向、VPN、およびサイトを選択します。
8. [Add]をクリックします。
9. [ポリシーの変更の保存（Save Policy Changes）] をクリックします。
10. **[VPN]** をクリックして、ドロップダウンから **[Site]** を選択します。

（注） 次の NAT フォールバックアクション/コマンドがサポートされるようになりました。

- アクション：`nat fallback`
- ポリシーを適用する場合：`direction from-tunnel`

一元管理型ポリシーのアクティブ化

一元管理型ポリシーをアクティブにすると、接続されているすべての Cisco SD-WAN コントローラにそのポリシーが送信されます。一元管理型ポリシーを有効にするには、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。[一元管理型ポリシー（Centralized Policy）] がデフォルトで選択され、表示されます。
2. 必要なポリシーについて、[...] をクリックし、[アクティブ化（Activate）] を選択します。[ポリシーのアクティブ化（Activate Policy）] ポップアップが表示されます。ポリシーが適用される到達可能な Cisco SD-WAN コントローラ の IP アドレスが一覧表示されます。
3. [Activate] をクリックします。

一元管理型ポリシーの表示

一元管理型ポリシーを表示するには、次の手順を実行します。

1. [一元管理型ポリシー（Centralized Policy）] から、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. [一元管理型ポリシー（Centralized Policy）] から、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）] ドロップダウンで、[CLIポリシー（CLI Policy）] をクリックします。
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. [一元管理型ポリシー（Centralized Policy）] から、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、一元管理型ポリシーの設定

CLI を使用して一元管理型制御ポリシーを設定するには、次の手順を実行します。

1. 次のように、一元管理型制御ポリシーを適用するオーバーレイ ネットワーク サイトのリストを作成します（**apply-policy** コマンドを使用）。

```
vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```

リストには、必要な数のサイト ID を含めることができます。サイト ID ごとに 1 つの **site-id** コマンドを含めます。連続するサイト ID の場合は、番号をダッシュ（-）で区切って範囲指定できます。必要に応じて、さらにサイトリストを作成します。

2. 必要に応じて、次のように IP プレフィックスと TLOC、VPN のリストを作成します。

```
vSmart(config)# policy lists
vSmart(config-lists)# prefix-list list-name
vSmart(config-lists-list-name)# ip-prefix prefix/length
vSmart(config)# policy lists
vSmart(config-lists)# tloc-list list-name
vSmart(config-lists-list-name)# tloc address
color color
encap encapsulation
[preference value]
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id
```

```
vsmart(config)# policy lists data-ipv6-prefix-list dest_ip_prefix_list
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# ipv6-prefix 2001:DB8::/32
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# commit
Commit complete.
```

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match destination-data-ipv6-prefix-list
dest_ip_prefix_list
vsmart (config-match)# commit
vsmart(config-match)# exit
vsmart(config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vm9(config-match)# commit
Commit complete.
vm9(config-match)# end
```

```
vsmart(config)# policy
vsmart(config-policy)#  data-policy data_policy_1
vsmart(config-data-policy-data_policy_1)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8::/32
vsmart(config-match)# exit
vsmart(config-sequence-101)# match destination-ipv6 2001:DB8::/32
vsmart(config-match)#
```

3. 次のように制御ポリシーインスタンスを作成します。

```
vSmart(config)# policy control-policy policy-name
vSmart(config-control-policy-policy-name)#
```

4. 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。

```
vSmart(config-control-policy-policy-name)# sequence
number
vSmart(config-sequence-number)#
```

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。

5. ルートおよびTLOCのマッチパラメータを次のように定義します。

```
vSmart(config-sequence-number)# match route route-parameter
vSmart(config-sequence-number)# match tloc tloc-parameter
```

6. 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。

```
vSmart(config-sequence-number)# action reject
vSmart(config-sequence-number)# action accept export-to (vpn
vpn-id | vpn-list list-name)
vSmart(config-sequence-number)# action accept set omp-tag
number

vSmart(config-sequence-number)# action accept set
preference value

vSmart(config-sequence-number)# action accept set
service service-name
(tloc ip-address |
tloc-list list-name)
[vpn vpn-id]

vSmart(config-sequence-number)# action accept set tloc
ip-address
color color
[encap encapsulation]
vSmart(config-sequence-number)# action accept set tloc-action
action

vSmart(config-sequence-number)# action accept set tloc-list list-name
```

7. 必要に応じて、制御ポリシー内にマッチ/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。

8. ルートがいずれかのシーケンス条件のどれにもマッチしない場合、そのルートはデフォルトで拒否されています。マッチしないルートを受け入れる場合は、ポリシーのデフォルトアクションを設定します。

```
vSmart(config-policy-name)# default-action accept
```

9. Cisco Catalyst SD-WAN オーバーレイネットワーク内の 1 つ以上のサイトにポリシーを適用します。

```
vSmart(config)# apply-policy site-list
list-name
control-policy
policy-name (in | out)
```

10. 設定するアクションがサービスの場合は、次のように、Cisco IOS XE Catalyst SD-WAN デバイスで必要なサービスを設定して、Cisco Catalyst SD-WAN コントローラがサービスに到達する方法を認識できるようにします。

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
vsmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8::/32
vsmart(config-set)#
```

サービスが配置されている VPN と、サービス側デバイスに到達するための 1 ～ 4 つの IP アドレスを指定します。複数のデバイスが同じサービスを提供する場合、デバイスはそれらの間でトラフィックをロードバランシングします。Cisco IOS XE Catalyst SD-WAN デバイスはサービスを追跡し、アドレス（またはアドレスの 1 つ）がローカルで、つまりデバイスのローカルサイトで解決でき、OMP を介して学習されない場合にのみ、サービスを Cisco Catalyst SD-WAN コントローラ にアドバタイズします。以前にアドバタイズされたサービスが使用できなくなった場合、Cisco IOS XE Catalyst SD-WAN デバイスはサービスアドバタイズメントを撤回します。

次に、VPN メンバーシップ データ ポリシーを設定するための手順について概要を示します。

1. 次のように、VPN メンバーシップポリシーを適用するオーバーレイ ネットワーク サイトのリストを作成します（**apply-policy** コマンドを使用）。

```
vSmart(config)# policy
vSmart (config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```

リストには、必要な数のサイト ID を含めることができます。サイト ID ごとに 1 つの **site-id** コマンドを含めます。連続するサイト ID の場合は、番号をダッシュ（-）で区切って範囲指定できます。必要に応じて、さらにサイトリストを作成します。

2. 必要に応じて、IP プレフィックスと VPN のリストを作成します。

```
vSmart(config)# policy lists
vSmart(config-lists)# data-prefix-list list-name
vSmart(config-lists-list-name)# ip-prefix prefix/length
```

```
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id
```

```
vsmart(config)# policy lists data-ipv6-prefix-list dest_ip_prefix_list
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# ipv6-prefix 2001:DB8:19::1
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# commit
Commit complete.
```

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match destination-data-ipv6-prefix-list
dest_ip_prefix_list
vsmart (config-match)# commit
vsmart(config-match)# exit
vsmart(config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vm9(config-match)# commit
Commit complete.
vm9(config-match)# end
```

```
vsmart(config)# policy
vsmart(config-policy)# data-policy data_policy_1
vsmart(config-data-policy-data_policy_1)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8:19::1
vsmart(config-match)# exit
vsmart(config-sequence-101)# match destination-ipv6 2001:DB8:19::1
vsmart(config-match)#
```

3. 必要に応じて、TLOC のリストを作成します。

```
vSmart(config)# policy
vSmart(config-policy)# lists tloc-list list-name
vSmart(config-lists-list-name)# tloc ip-address color color encap encapsulation
[preference number}
```

4. 必要に応じて、ポリシングパラメータを定義します。

```
vSmart(config-policy)# policer policer-name
vSmart(config-policer)# rate bandwidth
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

5. 次のように、データポリシーのインスタンスを作成し、それをVPNのリストに関連付けます。

```
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy-policy-name)# vpn-list list-name
```

6. 一連のマッチ/ペア シーケンスを次のように作成します。

```
vSmart(config-vpn-list)# sequence number
vSmart(config-sequence-number)#
```

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。

7. 次のように、パケットのマッチパラメータを定義します。

```
vSmart(config-sequence-number)# match parameters
```

8. 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。

```
vSmart(config-sequence-number)# action (accept | drop) [count counter-name] [log]
 [tcp-optimization]
vSmart(config-sequence-number)# action acccept nat [pool number] [use-vpn 0]
vSmart(config-sequence-number)# action accept redirect-dns (host | ip-address)
vSmart(config-sequence-number)# action accept set parameters

vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
vsmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8:19::1
vsmart(config-set)#
```

9. 必要に応じて、データポリシー内にマッチ/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。

10. ルートがいずれかのシーケンス条件のどれにもマッチしない場合、そのルートはデフォルトで拒否されています。マッチしないプレフィックス付きルートを受け入れる場合は、ポリシーのデフォルトアクションを設定します。

```
vSmart(config-policy-name)# default-action accept
```

11. オーバーレイネットワーク内の 1 つ以上のサイトにポリシーを適用します。

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all
|from-service | from-tunnel)
```

一元管理型ポリシーの設定例

このトピックでは、Cisco IOS XE 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たり、Cisco IOS XE Catalyst SD-WAN デバイスをインターネット出口ポイントとして設定できる一元管理型データポリシーの設定例をいくつか紹介します。

一般的な一元管理型ポリシーの例

このセクションでは、Cisco Catalyst SD-WAN コントローラ で一元管理型データポリシーを設定してその設定をコミットした後、ポリシーそのものによって、必要な Cisco IOS XE Catalyst SD-WANデバイスにプッシュされることを示す一元管理型データポリシーの一般的な例を紹介します。

ここでは、Cisco Catalyst SD-WAN コントローラ vm9 で次のような単純なデータポリシーを設定するとします。

```
vm9# show running-config policy
policy
 data-policy test-data-policy
  vpn-list test-vpn-list
   sequence 10
    match
     destination-ip 209.165.201.0/27
    !
    action drop
     count test-counter
    !
   !
   default-action drop
  !
 !
 lists
  vpn-list test-vpn-list
   vpn 1
  !
  site-list test-site-list
   site-id 500
  !
 !
!
```

次に、**test-site-list** という、サイト 500 を含むサイトリストに、このポリシーを以下のように適用します。

```
vm9# show sdwan running-config apply-policy
apply-policy
 site-list test-site-list
  data-policy test-data-policy
 !
!
```

Cisco Catalyst SD-WAN コントローラ は設定がアクティブ化されるとすぐに、サイト 500 の Cisco IOS XE Catalyst SD-WAN デバイス にポリシー設定をプッシュします。こうしたデバイスの 1 つである vm5 について、ポリシーが受信されたことが以下から確認できます。

```
vm5# show sdwan policy from-vsmart
policy-from-vsmart
```

```
 data-policy test-data-policy
  vpn-list test-vpn-list
   sequence 10
    match
     destination-ip 209.165.201.0/27
    !
    action drop
     count test-counter
    !
   !
   default-action drop
  !
 !
 lists
  vpn-list test-vpn-list
   vpn 1
  !
 !
!
```

アクセス制御

次は、データポリシーによって、送信元から特定の宛先に送信できるパケットタイプを制限する例を示しています。ここでは、サイト 100 の送信元アドレス 192.0.2.1 のホストと VPN 100 は、203.0.113.1 の宛先ホストに TCP トラフィックのみを送信できるようになっています。このポリシーでは、192.0.2.1 によって送信される TCP トラフィックのネクストホップも指定して、TLOC 209.165.200.225、カラーをゴールドに設定しています。他のトラフィックは、**default-action** ステートメントの結果として、すべて受け入れられます。

```
policy
  lists
     site-list north
       site-id 100
     vpn-list vpn-north
       vpn 100
  !
  data-policy tcp-only
     vpn-list vpn-north
       sequence 10
         match
           source-ip 192.0.2.1/32
           destination-ip 198.51.100.1/32
           protocol tcp
         action accept
           set tloc 203.0.113.1 gold
       !
       default-action accept
   !
!
apply-policy
   site north data-policy tcp-only
```

トラフィック制限

次の例は、特定のタイプのデータトラフィックが VPN 間で送信されないようにする方法を示しています。このポリシーは、SMTP メールトラフィックを伝送するポート 25 で、209.165.201.0/27 を発信元とするデータトラフィックをドロップします。ただし、このポリシーは、209.165.201.0/27 からの非 SMTP トラフィックを含む、他のすべてのデータトラフィックを受け入れます。

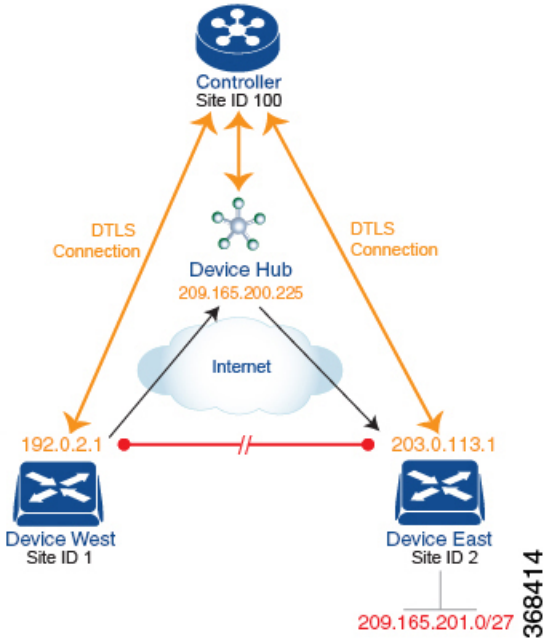
```
policy
  lists
    data-prefix-list north-ones
      ip-prefix 209.165.201.0/27
      port 25
    vpn-list all-vpns
      vpn 1
      vpn 2
    site-list north
      site-id 100
  !
  data-policy no-mail
   vpn-list all-vpns
     sequence 10
       match
         source-data-prefix-list north-ones
       action drop
     !
     default-action accept
  !
!
apply-policy
  site north data-policy no-mail
```

トラフィック エンジニアリング

次は、すべてのトラフィックを直接ではなく、デバイスハブを介して Cisco IOS XE Catalyst SD-WAN デバイスに流入させるようにするトラフィック エンジニアリングの例です。

Cisco IOS XE Catalyst SD-WAN オーバーレイネットワークでドメインを設計する一般的な方法の 1 つに、ある Cisco IOS XE Catalyst SD-WAN デバイスから別のデバイスにトラフィックを直接送信するのではなく、データセンターに通常配置されているハブルータを介して、ブランチ宛てのすべてのトラフィックをルーティングするというのがあります。これは、1 つのデバイスがハブとして機能し、別のデバイスがスポークであるハブアンドスポーク設計と考えることができます。このような設計では、ローカルブランチ間のトラフィックは、デバイスの起動時にスポークルータとハブルータの間に確立される IPsec 接続を介して移動します。確立された接続を使用すると、デバイスは、互いに IPsec 接続を確立するための時間と CPU サイクルを費やす必要がなくなります。これが多数のデバイスを含む大規模なネットワークだった場合、ルータの各ペア間でフルメッシュの接続を確立すると、ルータの CPU が大量に必要になります。この設計のもう 1 つの特性として、管理という観点から見た場合、ハブルータには、調整したトラフィックフローポリシーを設定した方が簡単なはずです。なぜならオーバーレイネットワーク内のハブルータは数が少ない上に、一元管理型データセンターに配置されているからです。

すべてのデバイス スポーク ルータ トラフィックを Cisco ハブルータに転送するには、1 つの方法として、ローカルネットワーク内のルートに関連付けられた TLOC を変更するポリシーを作成するというのがあります。次の図のトポロジについて考えてみましょう。



このトポロジには、異なるブランチに 2 つのデバイスがあります。

- サイト ID 1 のデバイス西。このデバイスの TLOC は、IP アドレス（192.0.2.1）、カラー（ゴールド）、およびカプセル化（ここでは IPsec）によって定義されます。TLOC の全アドレスを記述するなら、{192.0.2.1, gold, ipsec} となります。カラーは、単にトラフィックのフローを識別し、他のフローと区別するための方法です。
- サイト ID 2 のデバイス東の TLOC アドレスは、{203.0.113.1, gold, ipsec} です。

デバイス西とデバイス東は、Cisco Catalyst SD-WAN コントローラ によって配布された OMP ルートから互いの TLOC アドレスを学習します。この例では、デバイス東が、プレフィックス 209.165.201.0/27 を TLOC {203.0.113.1, gold, } で到達可能なものとしてアドバタイズします。ポリシーが何もなければ、デバイス西は 209.165.201.0/27 宛てのトラフィックを TLOC {203.0.113.1, gold, ipsec} にルーティングできるでしょう。つまり、トラフィックは、デバイス西からデバイス東に直接送信されることになるはずということです。

ただし、この設計では、デバイス西からデバイス東へのすべてのトラフィックは、デバイス東に移動する前に、TLOC アドレスが {209.165.200.225, gold, ipsec} であるハブルータを介してルーティングされる必要があります。このトラフィックフローを有効にするには、ルートの TLOC を変更するポリシーを定義します。そこで、プレフィックス 209.165.201.0/27 に関して、プレフィックス 209.165.201.0/27 に関連付けられている TLOC を、デバイス東の TLOC アドレスである {203.0.113.1, gold, ipsec} から、ハブルータの TLOC アドレスである {209.165.200.225, gold, ipsec} に変更するポリシーを作成します。こうしてできるのが、Cisco Catalyst SD-WAN コントローラ によってデバイス西にアドバタイズされ、デバイス東の TLOC アドレスではなく、ハブルータの TLOC アドレスを含むプレフィックス 209.165.201.0/27 の OMP ルートです。トラフィックフローの観点から見ると、デバイス西は 209.165.201.0/27 宛てのすべてのトラフィックをハブルータに送信します。

また、デバイスは、Cisco Catalyst SD-WAN コントローラ によってアドバタイズされた OMP ルートからデバイス西およびデバイス東の TLOC アドレスを学習します。デバイスはこれら 2 つの TLOC アドレスを使用する必要があるため、ハブによるデバイスへのトラフィックの転送方法を制御するためのポリシーは必要ありません。

デバイス西（およびネットワークドメイン内の他のデバイス）に対し、プレフィックス 209.165.201.0/27 宛てのトラフィックをデバイスである TLOC 209.165.200.225（ゴールド）に送信するよう指示する場合の、 Cisco Catalyst SD-WAN コントローラ でのポリシー設定は次のようになります。

```
policy
  lists
    prefix-list east-prefixes
      ip-prefix 209.165.201.0/27
    site-list west-sites
      site-id 1
  control-policy change-tloc
    sequence 10
      match route
        prefix-list east-prefixes
        site-id 2
      action accept
        set tloc 209.165.200.225 color gold encap ipsec
apply-policy
  site west-sites control-policy change-tloc out
```

このポリシーの大まかな英語訳は次のとおりです。

```
Create a list named “east-prefixes” that contains the IP prefix “209.165.201.0/27”
  Create a list named “west-sites” that contains the site-id “1”
  Define a control policy named “change-tloc”
    Create a policy sequence element that:
      Matches a prefix from list “east-prefixes”, that is, matches “209.165.201.0/27”
      AND matches a route from site-id “2”
    If a match occurs:
      Accept the route
      AND change the route’s TLOC to “209.165.200.225” with a color of "gold" and an
encapsulation of "ipsec"
  Apply the control policy “change-tloc” to OMP routes sent by the vSmart
    controller to “west-sites”, that is, to site ID 1
```

この制御ポリシーは、apply-policy site コマンドの **out** オプションで示されるように、アウトバウンドポリシーとして Cisco Catalyst SD-WAN コントローラ で設定されます。このオプションでは、Cisco Catalyst SD-WAN コントローラ はルートテーブルからルートを配布した後に、OMP ルートに TLOC 変更を適用することになります。Cisco Catalyst SD-WAN コントローラ がデバイス西に配布するプレフィックス 209.165.201.0/27 の OMP ルートは、209.165.201.0/27 を TLOC 209.165.200.225（ゴールド）に関連付けます。これが、デバイス西のルートテーブルにインストールされる OMP ルートです。最終的に、デバイス西が 209.165.201.0/27 にトラフィックを送信すると、トラフィックはハブに送信されます。また、デバイス西とデバイス東との間で DTLS トンネルが直接確立されることはありません。

ネットワークの西側に 1 つではなく多数のサイトがあり、その各サイトに独自のデバイスがある場合も、容易にこの同じポリシーをすべてのサイトに適用できます。これを行うには、ただ **site-list west-sites** リストに、すべてのサイトのサイト ID を追加するだけです。ポリシーにたったこれだけの変更を行うだけで、すべての西側サイトから、デバイスを介してプレフィックス

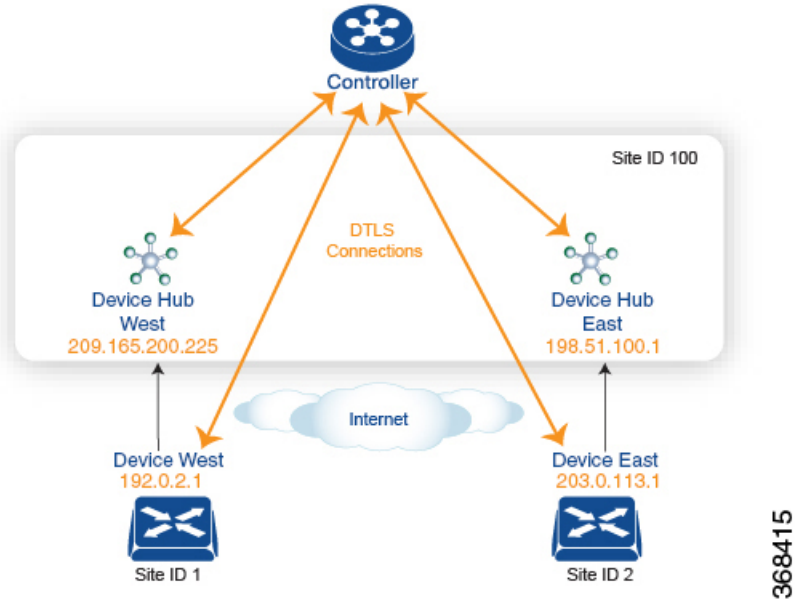
209.165.201.0/27 にバインドさせたトラフィックを送信させることができます。次に例を示します。

```
policy
  lists
    prefix-list east-prefixes
      ip-prefix 209.165.201.0/27
    site-list west-sites
      site-id 1
      site-id 11
      site-id 12
      site-id 13
  control-policy change-tloc
    sequence 10
      match route
        prefix-list east-prefixes
        site-id 2
      action accept
        set tloc 209.165.200.225 color gold encap ipsec
apply-policy
  site west-sites control-policy change-tloc out
```

任意のトポロジの作成

前の例で説明したハブアンドスポークスタイルのトポロジに冗長性を持たせる場合、Cisco ハブをもう 1 つ追加してデュアルホームハブサイトを作成することができます。次の図は、サイト ID 100 に 2 つのデバイスハブがあることを示しています。すべてのブランチ間トラフィックは、今まで通り、デバイスハブを介してルーティングする必要があります。ただし、今はデュアルホーム接続されたハブがあるため、データトラフィックは2つのハブルータ間で共有する必要があります。

- デバイスハブ西（TLOC 209.165.200.225、ゴールド）。オーバーレイネットワークの西側にあるブランチからのすべてのデータトラフィックは通過させて、このデバイスで処理する必要があります。
- デバイスハブ東（TLOC 198.51.100.1、ゴールド）。同様に、東側のすべてのデータトラフィックはデバイスハブ東を通過させます。



西側のデータトラフィックはデバイスハブ西を介して送信し、東西のトラフィックはデバイスハブ東を介して送信されるようにする場合の、Cisco Catalyst SD-WAN コントローラ のポリシー設定は次のようになります。

```
policy
  lists
    site-list west-sites
      site-id 1
    site-list east-sites
      site-id 2
    tloc-list west-hub-tlocs
      tloc-id 209.165.200.225 gold
    tloc-list east-hub-tlocs
      tloc-id 198.51.100.1 gold
  control-policy prefer-west-hub
    sequence 10
      match tloc
        tloc-list west-hub-tlocs
      action accept
        set preference 50
  control-policy prefer-east-hub
    sequence 10
      match tloc
        tloc-list east-hub-tlocs
      action accept
        set preference 50
apply-policy
  site west-sites control-policy prefer-west-hub out
  site east-sites control-policy prefer-east-hub out
```

このポリシー設定に関する説明は次の通りです。

apply-policy 構成コマンドに必要なサイトリストの作成。

- **site-list west-sites** は、オーバーレイネットワークの西側にある、すべてのデバイスの全サイト ID を一覧表示するものです。

- **site-list east-sites** は、ネットワークの東側にあるデバイスのサイト ID を一覧表示するものです。

制御ポリシーのマッチ条件に必要な TLOC リストの作成。

- **west-hub-tlocs** は、西側デバイスからのトラフィックを処理するのに必要なデバイスハブ西の TLOC を一覧表示するものです。
- **east-hub-tlocs** は、東側デバイスからのトラフィックを処理するために、デバイスハブ東の TLOC を一覧表示するものです。

2 つの制御ポリシーの定義。

- **prefer-west-hub** は、デバイス西ハブルータの TLOC アドレスである TLOC 209.165.200.225（ゴールド）を宛先とする OMP ルートに影響を与えるものです。このポリシーによって、OMP ルートのプリファレンス値が 50 に変更されます。この値は十分大きいので、大きなプリファレンス値を持つ OMP ルートは他にないはずです。したがって、プリファレンス値を高く設定することで、サイト 100 宛てのトラフィックがデバイス西ハブルータに転送されます。
- 同様に、**prefer-east-hub** は、デバイス東ハブルータの TLOC アドレスである TLOC 198.51.100.1（ゴールド） を宛先とする OMP ルートのプリファレンス値を 50 に設定するものなので、サイト 100 宛てのトラフィックを デバイス東ハブルータである 198.51.100.1 に転送します。

制御ポリシーの適用。

- **apply-policy** 構成の最初の行によって、Cisco Catalyst SD-WAN コントローラ は、**prefer-west-hub** 制御ポリシーを、**west-sites** リストに掲載されているサイト（ここではサイト ID 1 のみ）に適用させられます。そのため、TLOC 209.165.200.225 宛ての OMP ルートのプリファレンス値は 50 に変更され、デバイス西からハブサイトに送信されるトラフィックはデバイス西ハブルータを通過することになります。
- Cisco Catalyst SD-WAN コントローラ は、**east-sites** リスト内のデバイスにアドバタイズする OMP ルートに **prefer-east-hub** 制御ポリシーを適用します。これにより、TLOC 198.51.100.1 宛ての OMP ルートのプリファレンス値が 50 に変更されるので、デバイス東のトラフィックはデバイス東ハブルータに接続することになります。

コミュニティの例

これは、コミュニティリストへの一元管理型制御ポリシーの設定例です。

```
policy
  lists
   expanded-community-list test
    community 0:110* 100:[7-9]+
    community 0:110* 11:*

   community-list test-com
    community 0:1
    community 0:2
```

```
control-policy test
  sequence 10
   match route
    expanded-community-list test

   action accept
    set
     community 100:2 100:3
     additive
```

これは、標準コミュニティリストの設定例です。

```
Standard Community list

route : 0:1234 0:11 0:12

community-list
   community 0:100
   community 0:1234
   community 0:101
*MATCH*

route : 0:1234 0:11 0:12
community-list
  community 0:100
  community 0:5678
  community 0:101
*NO MATCH*
```

これは、拡張コミュニティリストの設定例です。OR マッチで、コミュニティリストの各正規表現文字列をルートのコミュニティストリングと比較します。

```
Expanded Community list
route - 0:1234  0:5678
expanded-community-list:
  community 0:110* 11:
  community 0:110* 100:[7-9]+
  community 0:12[3-7]+
*MATCH*

route - 0:1234  0:5678
expanded-community-list:
   community 0:111*
   community 0:110* 11:*
*NO MATCH*
```

EXACT マッチの入力文字列は、コミュニティがソート順になっている必要があります。バイト値でソートし、文字列の先頭と末尾にメタ文字を追加します。

```
route - 0:1234 0:5678
expanded-community-list:
community ^0:1234 0:5678$
*MATCH*
```

AND マッチの入力文字列は、コミュニティがソート順になっている必要があります。ソートされたコミュニティ間でブラインドマッチを行うには、「.+」を追加します。

```
route - 0:0 0:1234  0:5678  0:9789 0:9800 0:9900 0:9999 1:10
expanded-community-list:
   community 0:1234 .+ 0:9900 .+
*MATCH*
```

SIG データポリシーのフォールバック

Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 から、**sig-action fallback-to-routing** コマンドを使用して、すべての SIG トンネルがダウンした場合に、インターネットに向かうトラフィックを Cisco Catalyst SD-WAN オーバーレイを介してルーティングさせるように設定することができます。以下は、このフォールバックメカニズムの設定を示した例です。

```
data-policy _VPN10_SIG_Fall_Back
  vpn-list VPN10
    sequence 1
     match
      app-list Google_Apps
      source-ip 0.0.0.0/0
     !
     action accept
      sig
      sig-action fallback-to-routing
     !
    !
  default-action drop
```

ランク付けカラーの優先順位の例

```
policy lists
  preferred-color-group GROUP1_COLORS
   primary-preference
    color-preference biz-internet
    path-preference direct-tunnel
   !
   secondary-preference
    color-preference mpls
    path-preference multi-hop-path
   !
   tertiary-preference
    color-preference lte
   !
  !
  preferred-color-group GROUP2_COLORS
   primary-preference
    color-preference mpls
   !
   secondary-preference
    color-preference biz-internet
   !
  !
  preferred-color-group GROUP3_COLORS
   primary-preference
    color-preference mpls biz-internet lte
   !
```

IPv6 アプリケーションに対するデータポリシーの例

```
policy
 data-policy _VPN1_Data-Policy-For-Ipv6-Traffic
  vpn-list VPN1
    sequence 1
     match
      app-list Msft-0365
      source-ipv6 0::0/0
```

```
      !
     action accept
     !
    !
  default-action drop
 !
 lists
  app-list Msft-0365
   app ms-office-web-apps
  !
  site-list SITE-100
   site-id 100
  !
  vpn-list VPN1
   vpn 1
  !
 !
!
apply-policy
 site-list SITE-100
  data-policy _VPN1_Data-Policy-For-Ipv6-Traffic all
 !
!
```

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。