Cisco Evolved Programmable Network Manager 6.0.2 ユーザーおよび管理者ガイド

初版：2022 年 4 月 22 日

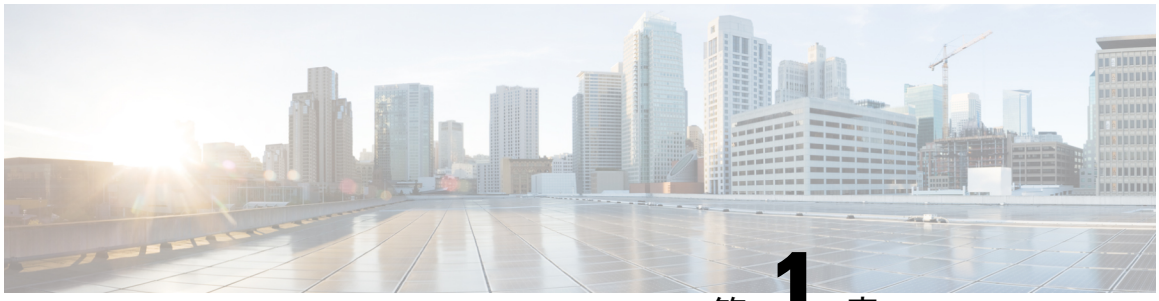
シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 I 部

Cisco EPN Manager スタートアップ ガイド



第 1 章

Cisco EPN Manager スタートアップ ガイド

（注） Cisco EPN Manager を初期使用のためにセットアップする必要がある管理者の場合は、サーバーのセットアップ タスク （873 ページ）を参照してください。

Web クライアントの要件

次に、Cisco EPN Manager Web GUI のクライアントとブラウザの要件を示します。

- ハードウェア：以下のテスト済みサポート対象ブラウザのいずれかに対応している Mac または Windows のラップトップかデスクトップ。
- ブラウザ：

（注） 1 つのブラウザセッションで Cisco EPN Manager のタブを同時に 3 つまで開くことができます。

- Google Chrome バージョン 74 ～ 84
- Mozilla Firefox ESR 60
- Mozilla Firefox バージョン 67 ～ 79
- Microsoft Internet Explorer (IE) 11.0

（注） Internet Explorer のユーザは、他のブラウザと比べて動作が遅いと報告しています。一部の GUI ページは IE でロードするのに時間がかかるためです。

- 推奨される表示解像度：1600 X 900 ピクセル以上（最小：1366 X 768）

ロード時間を短縮し、ネットワーク帯域幅の使用量を削減するために、Cisco EPN Manager は同じバージョンの Cisco EPN Manager（Firefox および IE ブラウザ）のブラウザに静的ファイル（js、css）をキャッシュします。

（注） Google Chrome では、自己署名証明書に関する既知の制限により、すべてのキャッシングディレクティブが無視され、ページコンテンツがリロードされます。

ログインおよびログアウト

GUI にログインするには、Web ブラウザのアドレス フィールドに次のように入力します。*server-ip* は Cisco EPN Manager サーバーの IP アドレスです。

https://*server-ip*

（注） Cisco EPN Manager にログインするときに、ブラウザにユーザー名とパスワードを自動入力したり保存したりしないでください。

ネットワーク設定に応じて、ブラウザを初めて Cisco EPN Manager Web サーバーに接続するときは、クライアントブラウザを更新してサーバーのセキュリティ証明書を信頼する必要があります。ユーザー固有のクライアント証明書を生成してブラウザにインポートすることもできます。これにより、ユーザーは Cisco EPN Manager にログインできます。これらの生成されたクライアント証明書を使用すると、ユーザー名とパスワードを指定せずにログインできます。これらの生成されたクライアント証明書をブラウザに更新する場合は、パスコードが必要です。これにより、クライアントと Cisco EPN Manager Web サーバー間の接続のセキュリティが保証されます。

ログアウトするには、Cisco EPN Manager ウィンドウの右上にある ⚙ をクリックし、[ログアウト（**Log Out**）] を選択します。

Cisco EPN Manager ユーザーとそのユーザーが実行できる操作については、次を参照してください。

- Cisco EPN Manager で CLI ユーザー インターフェイスを切り替える方法 （998 ページ）：Cisco EPN Manager でサポートされているすべてのユーザークラス（さまざまな CLI ユーザーアカウントを含む）について説明します。
- ユーザー グループのタイプ （999 ページ）：Web GUI ユーザーが毎日実行できる機能を制御できるユーザー グループ メカニズムについて説明します。ユーザー インターフェイスで表示できるものと操作できるものは、ユーザーアカウント権限によって制御されます。このトピックでは、デバイスのロールベース アクセス コントロール（RBAC）を管理する仮想ドメイン メカニズムについても説明します。

を使用する前に完了する必要のあるタスクのセットアップ Cisco EPN Manager

Cisco EPN Manager 機能を使用するには、管理者が次のタスクを完了する必要があります。

表 *1:* セットアップ タスクと参照

Cisco EPN Managerを使用する前に完了する必要のあるタスク	**詳細については、次を参照してください。**
Cisco EPN Manager サーバーのセットアップと設定を行います。	サーバーのセットアップ タスク （873 ページ）
デバイスとネットワークの管理を簡素化するために、デバイスを Cisco EPN Manager に追加してデバイス グループを作成します。	デバイスの追加と整理 （43 ページ）
ネットワークで使用されるインターフェイスとテクノロジーのモニターリングを有効にします。	デバイスおよびネットワークの健全性とパフォーマンスのモニター （281 ページ）
展開に合わせアラームとイベントの動作（アラームやイベントの更新頻度、電子メール、トラップ レシーバなど）をカスタマイズします。	アラームとイベント管理の設定 （312 ページ）

パスワードの変更

パスワードは、Cisco EPN Manager ウィンドウの右上にある ⚙ をクリックし、[パスワードの変更（**Change Password**）] を選択することによって、いつでも変更できます。? ([ヘルプ（help）]) アイコンをクリックして、パスワードポリシーを確認します。

（オプション）[新しいパスワードを生成（Generate New Password）] ボタンをクリックして、システムによって生成されるセキュアなパスワードを設定します。このボタンをクリックすると、新しいパスワードが隣のテキストボックスに表示されます。[新しいパスワード（New password）] および [パスワードの確認（Confirm password）] テキストボックスにも同じものが表示されます。目のアイコンをクリックするとパスワードの表示/非表示が切り替わります。[コピー（Copy）] ボタンをクリックして、パスワードをクリップボードにコピーすることもできます。

ダイアログボックス内の値をクリアするには、[リセット（Reset）] ボタンをクリックします。

メイン ウィンドウ コントロールの使用

Cisco EPN Manager タイトル バーの左上には、次のコントロールがあります。

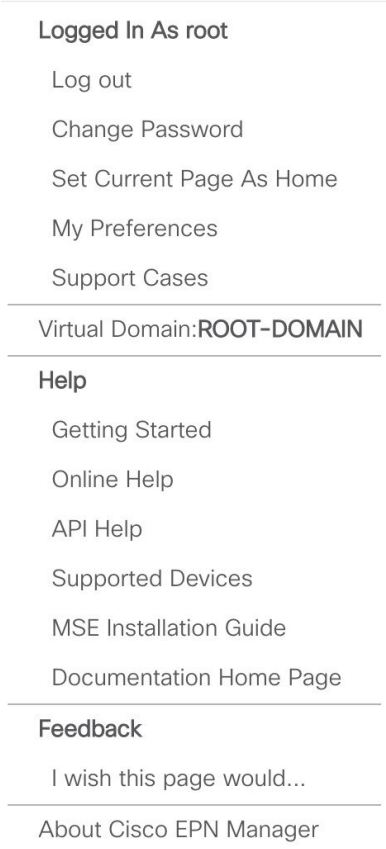
	[メニュー（Menu）] ボタン：左側のメインの Cisco EPN Manager ナビゲーション メニューを切り替えます（左側のサイドバー メニューとも呼ばれます）
	[ホーム（Home）] ボタン：ホームページ（通常は [概要（Overview）] ダッシュボード）に戻ります。

タイトル バーの右側には、使用しているユーザー名と仮想ドメインが表示されます。仮想ドメインは、デバイスの論理的なグループです。仮想ドメインは、ネットワークのデバイスや領域にアクセスする人物を制御するために使用されます。割り当てられている仮想ドメインを切り替えるには、別の仮想ドメインで作業する （32 ページ） を参照してください。

	Web GUI のグローバル設定ボタン：ログアウト、パスワードの変更、Cisco.com のアカウント プロファイルの表示、GUI 設定の調整、Cisco.com のサポート事例の確認、オンライン ヘルプの起動

タイトル バーの右側の ⚙ をクリックすると、ウィンドウ設定メニューが開きます。

図 *1* : ウィンドウ設定

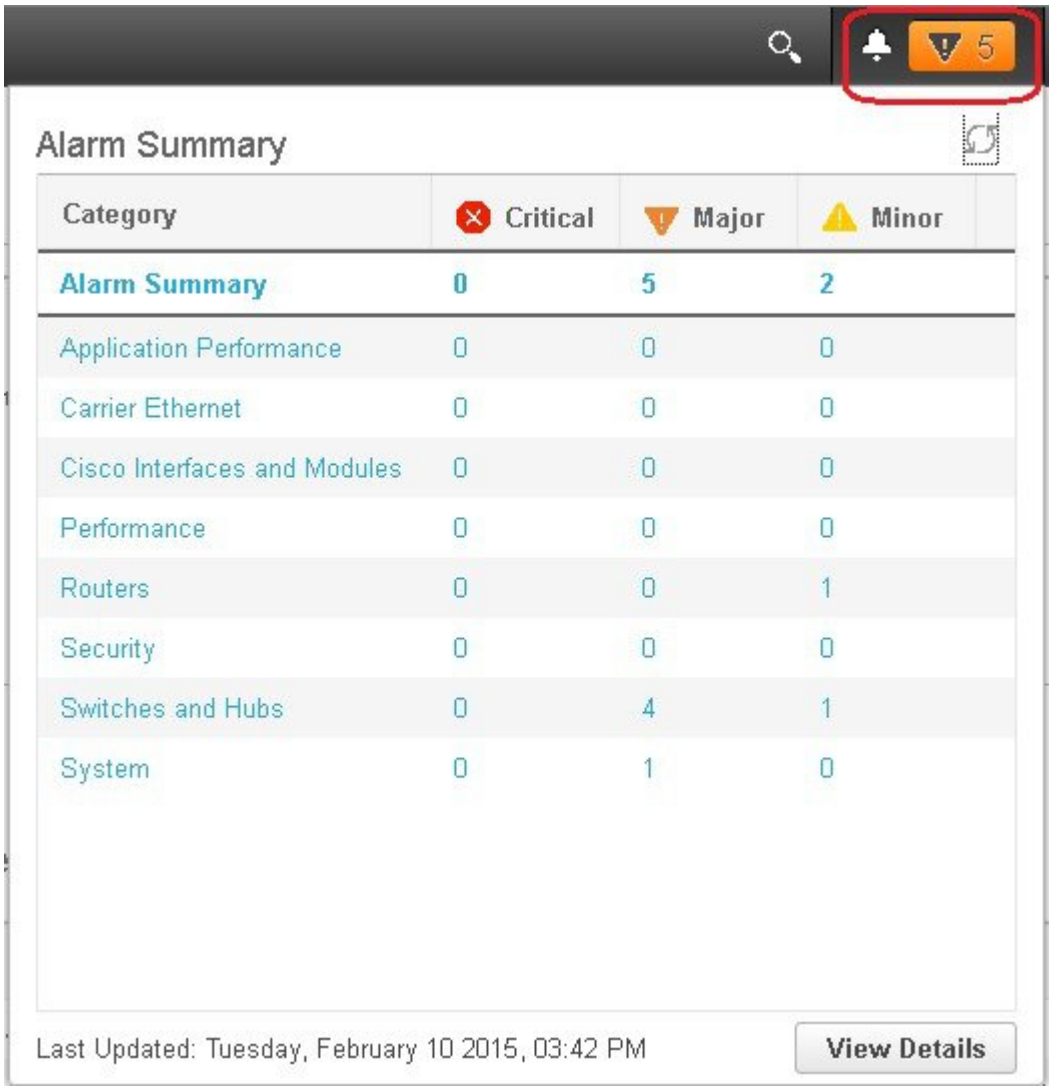


[アラームのまとめ（Alarm Summary）] には、ネットワーク内のアラーム数が視覚的に示されます。色は最も重大度の高いアラームを示します。

	[アラームのまとめ（Alarm Summary）] : 指定したカテゴリのアラーム数が視覚的に表示されます。この領域をクリックすると、[アラームのまとめ（Alarm Summary）] ポップアップ ウィンドウが開きます。

[アラームのまとめ（Alarm Summary）] ボタンをクリックすると、Cisco EPN Manager で [アラームのまとめ（Alarm Summary）] ポップアップウィンドウが開きます。ボタンとポップアップウィンドウの両方で表示されるデータをカスタマイズすることができます。

この例では、ボタンではスイッチとハブおよびシステム アラームの数が表示され、[アラームのまとめ（Alarm Summary）] ポップアップでは次の図にリストされているすべてのアラームカテゴリが表示されます。



デフォルトのホーム ページの変更

次のタスクを実行したときに、どのページが表示されるようにするかを指定できます。

- Web GUI タイトル バーの左側にある をクリックしたとき
- Cisco EPN Manager Web GUI にログインするとき

この設定はユーザー単位で保存されます。この設定は、他のユーザーに影響を与えることなく、いつでも変更できます。

ステップ 1 希望のページが表示されている状態で、Cisco EPN Manager Web GUI の右上にある をクリックします。

ステップ 2 [現在のページをホームとして設定（Set Current Page as Home）] を選択します。

ダッシュボードのセットアップと使用

ダッシュボードには、ネットワークにおける最重要データの概要が表示されます。これらは、ステータス、アラート、モニターリング、パフォーマンス、レポートの情報を提供します。ユーザーにとって重要な情報のみが表示されるように、これらのダッシュボードをカスタマイズできます。デフォルトのホームページとして [ネットワーク概要（Network Summary）] ダッシュボードを設定することをお勧めします。そうすれば、ログイン後にこのダッシュボードが表示され、何かを実行する前に、ネットワーク全体の健全性をすばやく確認できます。デフォルトのホームページとしてダッシュボードを設定するには、デフォルトのホームページの変更（6 ページ）を参照してください。

以下のダッシュボードを使用して、ネットワークをモニターしたり、管理したりします。

（注） ダッシュボードにデータを表示するには、関連するモニターリングポリシーを有効にする必要があります。デフォルトでは、デバイスのヘルスモニターリング（デバイス ヘルス モニターリング ポリシー）のみが有効になっています。詳細については、デバイスのヘルスとパフォーマンスのモニター方法：モニターリング ポリシー （281 ページ）を参照してください。

- [ネットワーク概要（Network Summary）] ダッシュボード：ネットワーク全体の健全性を確認します。「[ネットワーク サマリー（Network Summary）] ダッシュボードの概要」を参照してください。
- [サービス パフォーマンス（Service Performance）] ダッシュボード：キャリア イーサネットおよびオプティカルサービスのパフォーマンスをモニターします。「[サービス パフォーマンス（Service Performance）] ダッシュボードの概要」を参照してください。
- [パフォーマンス（Performance）] ダッシュボード：インターフェイス、QoS ポリシー、ITU-T Y.1731 プローブなどのネットワーク コンポーネントのパフォーマンス測定指標の概要を示します。「[パフォーマンス（Performance）] ダッシュボードの概要」を参照してください。
- [デバイス トレンド（Device Trends）] ダッシュボード：特定のデバイス、アプリケーション、サービスのパフォーマンスに関する情報を表示します。「[デバイス トレンド（Device Trends）] ダッシュボードの概要」を参照してください。
- [DWDM/OTNパフォーマンス（DWDM/OTN Performance）] ダッシュボード：ネットワーク内の高密度波長分割多重（DWDM）インターフェイスおよび光トランスポート ネットワーク（OTN）インターフェイスのパフォーマンスに関する情報を表示します。「[DWDM/OTNパフォーマンス（DWDM/OTN Performance）] ダッシュボードの概要」を参照してください。

管理者権限を持つユーザーは、次のダッシュボードも使用できます。

- [ライセンス（Licensing）] ダッシュボード：を参照してください。ライセンス ダッシュボードの表示
- [ジョブ（Jobs）] ダッシュボード：ジョブ ダッシュボードを使用したジョブの管理 （32 ページ）を参照してください。
- [システム モニターリング（System Monitoring）] ダッシュボード：システム監視ダッシュボードを使用して、Cisco EPN Manager サーバーのヘルス、ジョブ、パフォーマンス、および API 統計をチェックする （976 ページ）を参照してください。

次の点に注意してください。

- ダッシュボード ウィンドウの各部分の説明およびダッシュボード フィルタの使用方法については、ダッシュボードの使用方法 （24 ページ）を参照してください。
- ダッシュボード データの問題をトラブルシューティングするには、「ダッシュボードのデータが不足している理由の特定」を参照してください。

ダッシュボードのタイプ

以下のトピックでは、Cisco EPN Manager で使用可能なダッシュボードについて説明します。

[サービス パフォーマンス（Service Performance）] ダッシュボードの概要

[サービス パフォーマンス（Service Performance）] ダッシュボードから、指定した時間内の特定の回線、VC、サービスに関するパフォーマンス統計を表示できます。このダッシュボードを開くには、**[ダッシュボード（Dashboard）] > [サービス パフォーマンス（Service Performance）] >** の順に選択し、以下の表に示されているいずれかのタブを選択します。

ダッシュボード タブ	提供される情報
[CEM]	選択した回線エミュレーション（CEM）回線について： • 名前、タイプ、作成日などの詳細 • 統計情報（回線のエンドポイントの統計情報を切り替えることができます） • 伝送中に失われたパケットの数 • 宛先に到着するまでに、ジッター バッファで順序変更されたパケットの数 • ジッター バッファのオーバーランとアンダーランの数 • 順序が正しくないパケット、および後続がドロップされたパケットの数 • 不正なパケットの数 • エラー、重大なエラー、または利用不可であった秒数 • 失敗したイベント • 生成および受信された明示的なポインタ調整リレー カウンタ（L ビットと P ビットなど）の数をグラフ化するダッシュレット （注） これらのダッシュレットを表示するには、CEM と疑似回線エミュレーション（エッジ間）の両方のモニターリング ポリシーを有効にする必要があります。モニターリング ポリシー リファレンス（1199 ページ）を参照してください。
[TE トンネル（TE Tunnel）]	選択したトラフィック エンジニアリング（TE）トンネル回線について： • 名前、サービスを行える状態か、関連付けられたエンドポイントなどの詳細 • サービス統計情報 • 発信トラフィック、帯域幅使用率、および予約帯域幅 • サービスの可用性

ダッシュボード タブ	提供される情報
[SRポリシー（SR Policy）]	選択したセグメントルーティング（SR）ポリシーの場合： • 名前、サービスを行える状態か、関連付けられたエンドポイントなどの詳細 • サービス統計情報 • 発信トラフィック、帯域幅使用率、および予約帯域幅 • サービスの可用性
[CE/L3VPN]	選択した回線または VC について： • 名前、検出の状態、最終変更時刻などの詳細 • 次のパラメータの値が最も高い回線および VC を一覧表示します。 • エンドポイント間の平均のトラフィック • QoS クラス トラフィックおよびドロップ （注） インバウンド データとアウトバウンド データを切り替えることができます。[上位NのサービスQoSクラストラフィック（Top N Service QoS Class Traffic）] ダッシュレットで、ポリシー前データとポリシー後データを切り替えることもできます。 • 着信および発信 QoS ドロップ • サービス トラフィックおよび可用性 • 双方向遅延、一方向ジッター、およびサービス損失 • EVC 用の IPSLA ダッシュボードまたは L3VPN サービス用の Y.1731 ダッシュボードをクロス起動できるサービス プローブのエンドツーエンド パフォーマンス統計。
[上位CE/L3VPN（Top CE/L3VPN）]	次のパラメータの値が最も高い回線および VC を一覧表示します。 • 遅延 • ジッタ • サービス損失 • トラフィック（インバウンドとアウトバウンドの両方） CE と L3VPN サービスの情報を切り替えることができます。

（注） ダッシュボード タブのコンテンツとレイアウトをカスタマイズする方法については、「ダッシュボード タブのカスタマイズ」を参照してください。

[パフォーマンス（Performance）] ダッシュボードの概要

[パフォーマンス（Performance）] ダッシュボードでは、インターフェイス、QoS ポリシー、ITU-T Y.1731 プローブなどのネットワーク コンポーネントに関するパフォーマンス測定指標の概要を確認できます。このダッシュボードを開くには、次の表で説明するタブの **[ダッシュボード（Dashboard）]** > **[パフォーマンス（Performance）]** > を選択します。

ダッシュボード タブ	提供される情報
[インターフェイス（Interfaces）]	選択したインターフェイスについて、次の情報が表示されます。 • 名前、配置されたデバイスの IP アドレス、設定速度などの詳細 • 次のパフォーマンス メトリックの平均値、最小値、最大値（インバウンド データとアウトバウンド データについて収集されたメトリック間を切り替えることができます）。 • トラフィック • 使用率 • エラー • 破棄 • 巡回冗長検査（CRC）エラー （注） CRC エラー データはデフォルトではポーリングされません。このデータの収集を有効にするには、インターフェイス ヘルス モニターリング ポリシーの CRC パラメータのポーリング頻度を選択します（「モニターリング ポリシーのポーリングの変更」を参照してください）。 • [インターフェイスの統計情報（Interface Statistics）] ダッシュレットにリストされているパフォーマンス メトリックをグラフ化する個々のグラフ • インターフェイスの可用性 • 上位 N 個の QoS クラス マップ ポリシーのグラフ（インバウンドおよびアウトバウンドのポリシー前レート、ポリシー後レート、およびドロップ率） • QoS クラス マップ ポリシー統計（インバウンドとアウトバウンド）

ダッシュボード タブ	提供される情報
[QoS]	選択したQoSポリシーについて、次の情報が表示されます。 • 要約情報 • ポリシー前、ポリシー後、および破棄されたクラスマップ トラフィックに関する統計とグラフ • 適合クラス マップ トラフィック、超過クラス マップ トラフィック、および違反クラス マップ トラフィックに関する統計とグラフ
[Y1731]	選択したプローブ上のレイヤ 2 サービスについて、次の情報が表示されます。 • 要約情報 • ITU-T Y.1731 の統計 • エンドポイント間の遅延、ジッター、フレーム損失、CCM フレーム損失 • ジッター統計情報 • 遅延統計情報 • エンドポイントの可用性 （注） ビン統計データはデフォルトではポーリングされません。このデータの収集を有効にするには、IP SLA Y.1731 モニターリングポリシーのビン統計パラメータのポーリング頻度を選択します（「モニターリング ポリシーのポーリングの変更」を参照してください）。
[IP SLA]	選択したプローブ上のレイヤ 3 サービスについて、次の情報が表示されます。 • 要約情報 • IP サービス レベル契約（SLA）の統計 • エンドポイント間の遅延、ジッター、およびフレーム損失 • エンドポイントの可用性

ダッシュボード タブ	提供される情報
[BNG の統計（BNG Statistics）]	選択したデバイスに関する次のブロードバンド ネットワーク ゲートウェイ（BNG）情報が表示されます。 • 名前、IPアドレス、製品タイプ、ソフトウェアバージョンなどの詳細 • 設定された IP プールの名前と、各プールで使用されるアドレスの数と割合 • 選択された IP プールの使用済みアドレスまたは空きアドレスの数をグラフ化したチャート • ライン カードとセッション タイプ別の認証済みサブスクライバとアップ サブスクライバのセッション数をグラフ化したチャート 次の点に注意してください。 • チャートの下のチェックボックスを使用して、情報を表示する項目を選択します • グラフ上の任意のポイントにカーソルを移動すると、その特定の時刻の選択した項目の値が表示されます

ダッシュボード タブ	提供される情報
[ME1200 QoS]	Cisco ME 1200 デバイス上で選択したサービスに関する次の Quality of Service（QoS）情報が表示されます。 • デバイスの名前などの詳細、このデバイスと関連付けられている顧客、そのユーザー ネットワーク インターフェイス（UNI）ポート。 • 緑色（適合）トラフィック、黄色（超過）トラフィック、赤色（違反）トラフィック、および廃棄トラフィックの平均ビット レートと平均フレーム レート。インバウンド トラフィック データとアウトバウンド トラフィック データを切り替えることができます。 • [ME1200 QoSの統計情報（ME1200 QoS Statistics）] ダッシュレットに表示されたトラフィックタイプで測定されるトラフィックをグラフ化したグラフ。 次の点に注意してください。 • 5 つのトラフィック グラフが提供されます。トラフィック タイプごとに 1 つのグラフと 1 つの統合グラフ。 • フレーム レート（1 秒あたりのフレーム数）またはビット レート（1 秒あたりのキロビット数）でデータ表示を切り替えることができます。 • このチャートの下にある適切なチェックボックスを選択すると、グラフに表示される要素を指定できます。統合されたトラフィック ダッシュレットでは、トラフィック タイプを指定できます。個々のトラフィック ダッシュレットでは、サービスに関連付けられた 1 つまたは複数の EVC 制御エントリ（ECE）を指定できます。

ダッシュボード タブ	提供される情報
[光 SFP（Optical SFPs）]	選択された Small Form-Factor Pluggable（SFP）トランシーバ モジュール インターフェイスの場合： • 名前、インターフェイスが配置されているデバイスの名前と IP アドレス、設定速度などの詳細 • デバイスの次の操作メトリックの平均値、最小値、最大値。 • 光入出力電力 • 動作温度 • トランシーバ供給電圧 • レーザー バイアス電流 選択された Quad Small Form-Factor Pluggable（QSFP）トランシーバ モジュール インターフェイスの場合： 次の個々のレーンの平均値、最小値、および最大値。 • 温度 • Voltage • 現在（Current） • Tx 電力 • Rx 電力 • [SFPの統計情報（SFP Statistics）] ダッシュレットにリストされている操作メトリックをグラフ化する個々のグラフ

ダッシュボード タブ	提供される情報
[SONET/TDMインターフェイス（SONET/TDM Interfaces）]	選択したSONETまたは時分割多重（TDM）インターフェイス用。 • その名前、設定速度、格納先のデバイスのIPアドレスなどの詳細 • 次のパフォーマンス メトリックの平均値、最小値、最大値。 • エラー秒数 • 重大エラー秒数 • C ビットの重大エラー秒数 • P ビットの重大エラー秒数 • 使用不可秒数 インターフェイスの近端（受信側）と遠端（送信側）の両方の値が提供されます • [SONET/TDMの統計情報（SONET/TDM Statistics）] ダッシュレットにリストされているパフォーマンス メトリックをグラフ化する個々のグラフ
[デバイス センサー（Device Sensors）]	選択したデバイスのセンサーの場合： • 名前 • 説明 • 測定のタイプ • 現在の値 現在の値で [i] アイコンをクリックすると、過去 6 時間のトレンドが表示されます。
[MPLSリンクの遅延（MPLS Links Latency）]	選択したリンクに関する次の詳細を取得できます。 • リンク名、エンドポイントデバイス、インターフェイスなどのリンクの詳細。 • リンク遅延（一方向および双方向）。 （注） [上位N個のMPLSリンク（Top N MPLS Links）] テーブルの [リンク名（Link Name）] をクリックして、選択したリンクのMPLSリンクダッシュボードを起動できます。

次の点に注意してください。

- インターフェイスモニターリングは、デフォルトで有効になりません。このチェック方法については、Cisco EPN Managerによるモニターリング対象のチェック （287ページ）を参照してください。
- ダッシュボードタブのコンテンツとレイアウトをカスタマイズする方法については、「ダッシュボード タブのカスタマイズ」を参照してください。

[ネットワーク サマリー（Network Summary）] ダッシュボードの概要

[ネットワーク サマリー（Network Summary）] ダッシュボードは、ネットワークに現在影響を与えている最も重要な問題を警告します。また、さまざまなソースからメトリックを収集して、重要業績評価指標（KPI）のセットを表示します。このダッシュボードを開くには、次の表で説明するタブの **[ダッシュボード（Dashboard）]** > **[ネットワーク サマリー（Network Summary）]** > を選択します。

ダッシュボード タブ	提供される情報
[ネットワーク デバイス（Network Devices）]	• ステータス（ICMP到達可能性、SNMP到達可能性、デバイス管理性）、システム ヘルス、およびアラームの概要メトリック ダッシュレット 次の点に注意してください。 • メトリック ダッシュレットによって提供される情報を説明しているポップアップ ウィンドウを開くには、その名前の上にカーソルを移動してから、[?] アイコンをクリックします。 • 特定のメトリックに対応するアラームやデバイスを一覧表示するページを開くには、ダッシュレット値をクリックします。たとえば、[SNMP到達可能性ステータス（SNMP Reachability Status）] ダッシュレットが現在 50 デバイスは SNMP 経由で到達可能であることを示す場合、[50] をクリックして [ネットワークデバイス（Network Devices）] ページを開き、これらのデバイスのリストを表示します。 • CPU 使用率、メモリ使用率、および環境温度別の上位 N 個のデバイス [トップNの環境温度（Top N Environmental Temperature）] ダッシュレットの場合、次に注意してください。 • 各デバイスについて、最高記録内部温度（[取り入れ口最高温度（Max Inlet Temp）] 列に表示）と最高記録周囲温度（[その他の最高温度（Max Other Temp）] に表示）の 2 つの温度値が表示されます。デフォルトでは、デバイスはその内部の温度で並べ替えられます。 • 特定の温度値を記録するセンサーを識別するには、その *[i]*（[情報（information）]）アイコンにカーソルを合わせます。 • ネットワーク トポロジ

ダッシュボード タブ	提供される情報
[インシデント（Incidents）]	• システム ヘルス ダッシュレットとアラーム概要メトリック ダッシュレット 次の点に注意してください。 • メトリック ダッシュレットによって提供される情報を説明しているポップアップ ウィンドウを開くには、その名前の上にカーソルを移動してから、[?] アイコンをクリックします。 • 特定のメトリックに対応するアラームを一覧表示するページを開くには、ダッシュレット値をクリックします。たとえば、[アラーム概要（Alarm Summary）] ダッシュレットがネットワークで 12 の重要なアラームが発生したことを示す場合、[12] をクリックして [アラーム（Alarms）] ページを開き、これらのアラームのリストを表示します。 • ネットワーク全体と Cisco EPN Manager サーバーのアラーム カウント • 上位 N 個のアラーム タイプ • Syslog の概要 • 上位 N 個のイベント タイプとそれらのカウント • 送信された syslog の数別の上位 N 個のデバイス • 対応するデバイス、重大度、メッセージ テキストなどの syslog の詳細 • 発生したアラームの数別の上位 N 個のデバイス

ダッシュボード タブ	提供される情報
[上位 N 個のインターフェイス（Top N Interfaces）]	選択されたポート グループについて、次の情報が表示されます。 • インターフェイスの可用性と使用率の概要 • インターフェイス トラフィック、エラーと破棄、巡回冗長検査（CRC）エラー、および利用率による上位 N 個のデバイス （注） CRC エラー データはデフォルトではポーリングされません。このデータの収集を有効にするには、インターフェイス ヘルス モニターリング ポリシーの CRC パラメータのポーリング頻度を選択します（「モニターリング ポリシーのポーリングの変更」を参照してください）。 • インターフェイス可用性別の下位 N 個のデバイス またこのタブのダッシュレット（概要ダッシュレットを除く）では、その *[i]*（[情報（information）]） アイコンをクリックすることで、デバイスの隣接するデバイスまたはインターフェイスの 360 度ビューを開くできることに留意してください。
[上位 N 個の QoS（Top N QoS）]	選択されたポート グループについて、次の情報が表示されます。 • QoS ポリシー前、ポリシー後、およびドロップ レート別の上位 N 個のデバイス • 適合トラフィック レート、超過トラフィック レート、および違反トラフィック レート別の上位 N 個のデバイス インバウンド トラフィック データとアウトバウンド トラフィック データを切り替えることができます。
[上位 N 個の Y1731（Top N Y1731）]	次のパラメータの値が最も高いエンドポイントが表示されます。 • 遅延（一方向および双方向） • ジッター（一方向） • フレーム損失
上位 N 個の MPLS リンク遅延（Top N MPLS Links Latency）	• 遅延（一方向および双方向） （注） [上位N個のMPLSリンク（Top N MPLS Links）] テーブルの [リンク名（Link Name）] をクリックして、選択したリンクの MPLS リンク ダッシュボードを起動できます。

ダッシュボード タブ	提供される情報
PTP/SyncE	• 時間の経過に伴う PTP クロッククラス（PTP Clock Class over time） • 時間の経過に伴うサーボ状態（Servo State over time） • 時間の経過に伴う SyncE 品質レベル（SyncE Quality Level over time） （注） Cisco EPN Manager は、[PTP/SycE システム設定（PTP/SyncE System Settings）] ページで設定した値を使用して、ダッシュボードにデータを表示します。詳細については、「PTP/SyncE ダッシュボードの設定 （22 ページ）」を参照してください。

ダッシュレットの列を追加または削除して特定のデータを表示することができます。[上位N個のインターフェイス（Top N Interfaces）]、[上位N個のQoS（Top N QoS）]、および [上位N個のY1731（Top N Y1731）] タブでは、[並べ替え（Sort by）] オプションを使用して、列に表示されるデータをソートすることもできます。

[上位N個のインターフェイス（Top N Interfaces）] と [上位N個のQoS（Top N QoS）] タブで次のことができます。

- 特定のデバイス グループおよび/またはポート グループを選択し、これらのデバイス/ポートの情報のみを表示します。
  - ポート/デバイス グループに基づいてすべてのダッシュレットのデータをフィルタ処理するには、ダッシュボードの上部の [ポートグループ（Port Groups）] フィルタを使用します。
  - 特定のダッシュレットのデータのみをフィルタ処理するには、ダッシュレットの [編集（Edit）] アイコンをクリックして、[ポートグループ（Port Groups）] または [デバイスグループ（Device Groups）] ドロップダウンリストからデバイスまたはポートのグループを選択します。
- クラスマップでダッシュレットのデータをフィルタ処理します（デフォルトのクラスを除外することができます）。
- インターフェイスの名前リンクをクリックして、そのインターフェイスのパフォーマンスに関する情報を [パフォーマンス（Performance）] ダッシュボードに表示します。[上位 N 個のインターフェイス（Top N Interfaces）] タブでリンクをクリックすると、[インターフェイス（Interfaces）] タブが開きます。[上位 N 個の QoS（Top N QoS）] タブでリンクをクリックすると、[QoS] タブが開きます。
- インターフェイスモニターリングは、デフォルトで有効になりません。このチェック方法については、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- ダッシュボードタブのコンテンツとレイアウトをカスタマイズする方法については、「ダッシュボード タブのカスタマイズ」を参照してください。

PTP/SyncE ダッシュボードの設定

PTP/SyncE ダッシュボードにデータを表示するために Cisco EPN Manger で使用するメトリックを設定するには、**[管理者（Administrator）]**>**[システム設定（System Settings）]**>**[パフォーマンス（Performance）]** > **[PTP/SyncE]** に移動します。必須項目としてメトリックを設定して [保存（Save）] をクリックします。

セクション	説明	操作
PTP クロッククラス	[OK] または [低下（Degraded）]、あるいは [エラー（Failure）] で報告される [PTP クロッククラス（PTP Clock Class）] の値の範囲を定義できます	0 ～ 255 の範囲全体から値を入力します。3 つのカテゴリ間の値に重複がないことを確認します。
PTP サーボ状態	考えられる 5 つの PTP サーボ状態それぞれを Cisco EPN Manager が報告する方法を定義できます。	このセクションの 5 つの状態それぞれを[OK] または [低下（Degraded）] あるいは [エラー（Failure）] に設定します。
SynC の品質レベル	Cisco EPN Manager が [OK] として報告する SyncE の品質レベルを定義できます。デフォルトでは、Cisco EPN Manager で [OK] として 2 つの値を定義できます。必要に応じて 3 番目の値を追加するには、グレー表示のフィールドの横にあるチェックボックスをオンにします。[OK] として定義したものとは別の SyncE QL 値は、[低下（Degraded）] として報告されます。	ドロップダウンリストから値を選択します。
UTC Offset	システムに正しい UTC オフセットを定義できます。Cisco EPN Manager は、UTC オフセットに一致している値で設定されているデバイスを [正しい UTC オフセット（Correct UTC offset）]、この値に一致していないオフセットで設定されているデバイスを [不正な UTC オフセット（Incorrect UTC Offset）] と報告します。	0 ～ 65535 の範囲で値を入力します。

[デバイス トレンド（Device Trends）] ダッシュボードの概要

[デバイス トレンド（Device Trends）] ダッシュボードでは、特定のデバイス、アプリケーション、またはサービスのパフォーマンス情報を表示できます。このダッシュボードを開くには、次の表で説明するタブの **[ダッシュボード（Dashboard）]** > **[デバイス トレンド（Device Trends）]** > を選択します。

ダッシュボード タブ	提供される情報
[デバイス（Device）]	デバイスを選択した場合： • CPU 使用率とメモリ使用率 • ヘルス情報 • ポート サマリー
[アプリケーション（Application）]	アプリケーションまたはサービスを選択した場合： • トラフィック レートとボリューム • トラフィック レートとボリューム別の上位N個のクライアント、サーバー、およびアプリケーション （注） この機能はサポートされておらず、Cisco EPN Manager 6.1 以降では削除されます。

次の点に注意してください。

- インターフェイス モニターリングは、デフォルトで有効になりません。このチェック方法については、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- ダッシュボードタブのコンテンツとレイアウトをカスタマイズする方法については、「ダッシュボード タブのカスタマイズ」を参照してください。

[DWDM/OTNパフォーマンス（DWDM/OTN Performance）] ダッシュボードの概要

[DWDM/OTNパフォーマンス（DWDM/OTN Performance）] ダッシュボードには、特定の回線を通じて横断的に使用される DWDM インターフェイスおよび OTN インターフェイスのパフォーマンスに関する情報が表示されます。これには、物理、ODU、OTU、イーサネット、SONET、SDH のインターフェイスが含まれます。パフォーマンス情報は、インターフェイス タイプごとに異なるタブに表示されます。

このダッシュボードを開くには、次のいずれかの操作を実行します。

- **[ダッシュボード（Dashboard）]** > **[DWDM/OTNパフォーマンス（DWDM/OTN Performance）]** > **[回線（Circuit）]** を選択します。[インターフェイス（Interfaces）] ダッ

シュレットでインターフェイス名をクリックします。インターフェイスのタイプに関連するタブが開きます。たとえば、OTU インターフェイスをクリックすると [OTU] タブが開きます。

- インターフェイスの 360 ビューで、**[ビュー（VIew）]>[パフォーマンス（Performance）]** を選択します。

（注） IOS-XR デバイスの場合、ダッシュボードには、収集された OTN 15 分インターフェイスまたは選択された特定の OTN 15 分パラメータのパフォーマンス情報が表示されます。各種パラメータは次のとおりです。

- OTU FEnd
- OTU NEnd
- ODU FEnd
- ODU NEnd
- OTN GFP
- OTN FEC

次の点に注意してください。

- インターフェイスモニターリングは、デフォルトで有効になりません。このチェック方法については、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- ダッシュボードタブのコンテンツとレイアウトをカスタマイズする方法については、「ダッシュボード タブのカスタマイズ」を参照してください。

ダッシュボードの使用方法

次の図に、ダッシュボードウィンドウの主要な部分とそれらの調整に使用可能なコントロールを示します。

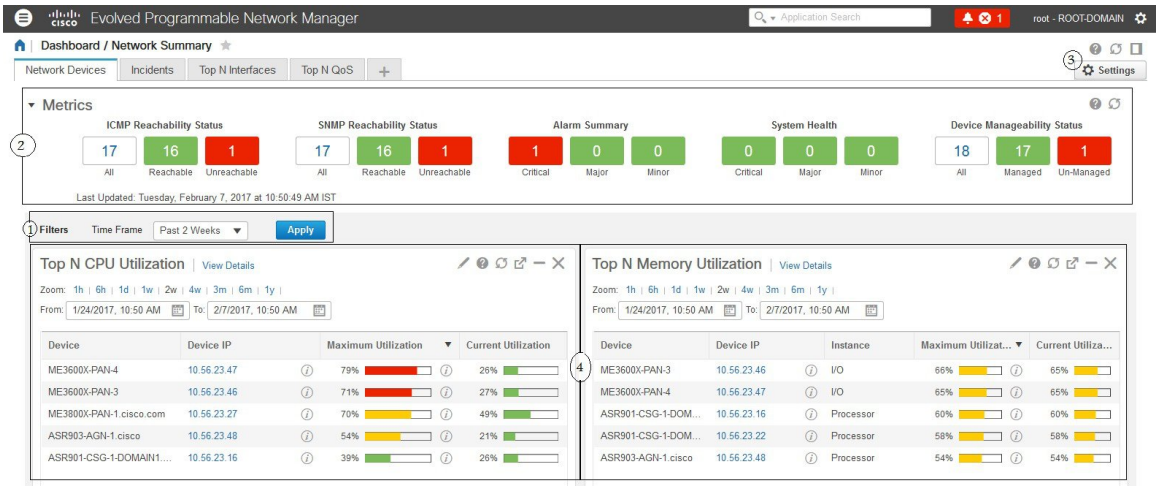
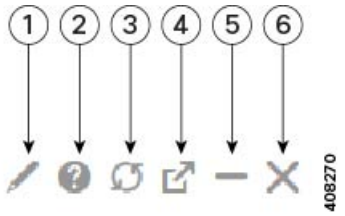


表 *2:* ダッシュボード要素

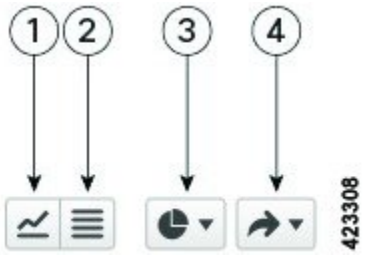
1	ダッシュボード フィルタ：選択に基づいてダッシュボード内のすべてのダッシュレットをフィルタ処理します。この例では、時間ベースのフィルタが使用されています。表示されるフィルタは、ダッシュボード タイプによって異なります。たとえば、パフォーマンス ダッシュボードでは、特定のインターフェイス、デバイス、回線、または VC を選択する必要があります。
2	メトリック ダッシュレット：アラームや使用可能なデバイスなどのクイック メトリックを提供します。
3	ダッシュボードの設定とコントロール： • ダッシュボードアイコン：オンライン ヘルプを起動したり、ダッシュボード全体を更新したり、[ドッキング（Dock）] ウィンドウを開いたりできます。 • [ダッシュボード設定（Dashboard Settings）] メニュー：ダッシュボード タブを追加または名前変更したり、新しいダッシュレット（標準とメトリックの両方）を追加したり、ダッシュボードのレイアウトを調整したり、すべてのダッシュボードをデフォルト設定にリセットしたり、選択したダッシュレットからデータをエクスポートしたりできます。 （注） 新しく追加されたダッシュボードタブまたは名前を変更されたダッシュボードタブは、[タブ（Tab）] ビューにのみ表示できます。この変更は[ダッシュボード（Dashboard）] メニューには反映されません。
4	標準ダッシュレット：ダッシュボードに関連する概要データを示します。

各ダッシュレットの右上に、そのダッシュレットが使用されたときにアクティブになるアイコンがあります。ダッシュレット タイプによって、使用可能なアイコンが決定されます。最も一般的なアイコンを次の図に示します。



1	[編集（Edit）]アイコン：クリックしてタイトル、更新間隔、表示されるデバイス数などのダッシュレットのプロパティを変更します（上位N件および下位N件のダッシュレットにのみ適用）。
2	[ヘルプ（Help）] アイコン：ダッシュレットの説明が記載されたポップアップ ウィンドウ、ダッシュレットでデータを収集するためにアクティブにする必要のあるモニターリングポリシーを示すポップアップ ウィンドウ、およびダッシュレットに適用可能なフィルタが一覧表示されたポップアップ ウィンドウを開く場合にクリックします。
3	[更新] アイコン：ダッシュレットに表示された情報を更新する場合にクリックします。
4	[切り離し（Detach）] アイコン：ダッシュレットをダッシュボード内の別の場所に移動する場合にクリックします。
5	[折りたたみ/展開（Collapse/Expand）] アイコン：最大化されたダッシュレットと最小化されたダッシュレットを切り替える場合にクリックします。
6	[閉じる（Close）]アイコン：ダッシュボードからダッシュレットを削除する場合にクリックします。

チャートを提供するダッシュレットの右下隅に、次の図で強調表示されているボタンがあります。使用可能なボタンはダッシュレット間で異なります。



1	[チャートビュー（Chart View）]ボタン：クリックすると、ダッシュレットの情報がチャートとして表示されます。
2	[テーブルビュー（Table View）]ボタン：クリックすると、ダッシュレットの情報がテーブルとして表示されます。
3	[チャートタイプ（Chart Type）]ボタン：クリックして、ダッシュレットが表示するチャートのタイプ（バー、円グラフなど）と設定する任意のオプション（各要素に固有の塗りつぶしのパターンを表示するなど）を選択します。

4	[アクション（Actions）] ボタン：クリックして、ダッシュレットが提供する情報を印刷するか、.csv または .pdf 形式のファイルに情報をエクスポートします。

ダッシュボードの追加情報については、次のトピックを参照してください。

- ダッシュボードのタイプ （8 ページ）
- ダッシュボードへのダッシュレットの追加 （28 ページ）
- 新しいダッシュボードの追加 （27 ページ）
- ダッシュボードのデータが不足している理由の特定

新しいダッシュボードの追加

新しいダッシュボードを作成するには、次の手順を実行します。新しいダッシュボードは、ダッシュボードのタイプ （8 ページ）にリストされているダッシュボードの 1 つに、新しいタブとして表示されます。

ステップ 1 関連する既存のダッシュボードを開きます。

たとえば、[パフォーマンス（Performance）] ダッシュボードに新しいタブを作成するには、**[ダッシュボード（Dashboard）] > [パフォーマンス（Performance）]** にあるいずれかのタブをクリックします。

ステップ 2 [+]（[新しいダッシュボードの追加（Add New Dashboard）]）タブをクリックします。

[設定（Settings）] メニューが開きます。

ステップ 3 新しいダッシュボードの名前を入力し、[**Apply**] をクリックします。

ステップ 4 新しいダッシュボード タブをクリックし、事前定義のダッシュレットをダッシュボードに追加する （28 ページ）の説明に従ってダッシュレットを追加します。

ダッシュボード タブのカスタマイズ

Cisco EPN Manager に表示されるダッシュボードのタブをカスタマイズするには、次の手順に従います。

ステップ 1 [ダッシュボード（Dashboard）] > を選択し、カスタマイズするダッシュボード タブを選択します。

たとえば、[パフォーマンス（Performance）] ダッシュボードの [BNG] タブをカスタマイズする場合は、**[ダッシュボード（Dashboard）] > [パフォーマンス（Performance）] > [BNG]** を選択します。

ステップ 2 必要に応じて、ダッシュボードのタブを調整します。

次のように調整できます。

- ダッシュレットをダッシュボード上の別の場所にドラッグします。

- タブの [設定（Settings）] メニューから該当する項目を選択し、タブの名前の変更、新規ダッシュレットの追加（「ダッシュボードへのダッシュレットの追加」を参照）、タブのレイアウトの変更を行います。

  新しく追加されたダッシュボードタブまたは名前が変更されたダッシュボードタブは、[タブ（Tab）] ビューにのみ表示できます。この変更は [ダッシュボード（Dashboard）] メニューには反映されません。

  （注） 追加しようと考えているダッシュレットの概要を説明するポップアップウィンドウを開くには、[ダッシュレットの追加（Add Dashlets）] ドロップダウンリストを展開し、目的のダッシュレットを見つけて、その名前の上にカーソルを置きます。

- フィルタを使用して表示する情報と適切な時間枠を指定してから、[適用（Apply）] をクリックします。

ステップ 3 タブにデータが表示されない場合は、トラブルシューティングを行います。

詳細については、「ダッシュボードのデータが不足している理由の特定」を参照してください。

ダッシュボードへのダッシュレットの追加

ダッシュボードには、2 つのタイプのダッシュレットを追加できます。

- Cisco EPN Manager で提供される事前パッケージ ダッシュレット：ダッシュレットの一部はデフォルトでダッシュボードに表示されます。他のダッシュレットは、[設定（Settings）] メニューにリストされ、必要に応じて追加できます。これらのダッシュレットにより、モニターする可能性の高い情報が提供されます（たとえば、デバイスの CPU 使用率、インターフェイスのエラーと破棄、トラフィック統計情報）。事前定義のダッシュレットをダッシュボードに追加する （28 ページ）を参照してください。
- デバイスのパフォーマンスをモニターするために作成するカスタム ダッシュレット：これらのダッシュレット タイプは、[デバイス トレンド（Device Trends）] ダッシュボードにのみ追加できます。「[デバイス トレンド（Device Trends）] ダッシュボードへのカスタマイズ済みダッシュレットの追加」を参照してください。

事前定義のダッシュレットをダッシュボードに追加する

Cisco EPN Manager は、一般的に必要なネットワーク データを提供する、事前定義のダッシュレットのセットを提供します。デフォルトで、これらのダッシュレットのサブセットがすでにダッシュボードに含まれているため、すぐに使い始めることができます。これらの事前定義のダッシュレットとは別のダッシュレットをダッシュボードに追加するには、次の手順を実行します。

（注） ダッシュレットを編集または削除するには、その右上にある該当するアイコンをクリックします（「ダッシュボードの使用方法」を参照）。

ステップ 1 サイドバー メニューで、[ダッシュボード（Dashboard）] を選択してから、ダッシュレットを追加するダッシュボードを選択します。

たとえば、[デバイス メモリ使用率（Device Memory Utilization）] ダッシュレットを [デバイス トレンド（Device Trends）] ダッシュボードに追加するには、**[ダッシュボード（Dashboard）] > [デバイス トレンド（Device Trends）] > [デバイス（Device）]** を選択します。

ステップ 2 追加するダッシュレットを特定して追加します。

a) ダッシュボードの右上で、[設定（Settings）] をクリックしてから [ダッシュレットの追加（Add Dashlets）] をクリックします。Cisco EPN Manager にそのダッシュボードに追加可能なダッシュレットが一覧表示されます。

b) 特定のダッシュレットの概要を示すポップアップウィンドウを開くには、そのダッシュレットの名前の上にカーソルを置きます。ポップアップウィンドウには、ダッシュレットが提供するデータのソースと、ダッシュレットに適用可能なフィルタも表示されます。

c) [追加（Add）] をクリックして、選択したダッシュレットをダッシュボードに追加します。

ステップ 3 ダッシュレットにデータが入力されていることを確認します。

そうでない場合は、必要なモニターリング ポリシーが有効になっているかどうかをチェックします（デバイス ヘルス モニターリング ポリシーだけがデフォルトで有効になります。これは、デバイス可用性、CPU とメモリ プールの使用率、および環境温度をチェックします）。

a) ダッシュレットの右上で、その [?]（[ヘルプ（Help）]）アイコンをクリックして、ダッシュレットのポップアップ ウィンドウを開きます。

b) [データ ソース（Data Sources）] 領域に表示された情報をチェックします。モニターリング ポリシーが表示された場合は、そのポリシーがアクティブになっているかどうかをチェックします。Cisco EPN Manager によるモニターリング対象のチェック （287 ページ） を参照してください。

[デバイス トレンド（Device Trends）] ダッシュボードへのカスタマイズ済みダッシュレットの追加

[デバイス トレンド（Device Trends）] ダッシュボード内に、必要なデバイス パフォーマンス情報を提供するダッシュレットがない場合、カスタマイズしたテンプレートを使用するダッシュレットを追加して、デバイスに対して SNMP MIB 属性をポーリングすることができます。このようなダッシュレットをダッシュボードに追加するには、次の手順に従います。

始める前に

使用可能なモニターリング ポリシーを調べて、必要な情報を収集するポリシーを判断します。ダッシュレットの作成時にポリシーを指定する必要があります。ニーズを満たすポリシーがない場合は、新しいパラメータをポーリングするポリシーを作成できます。サポートされないパラメータとサードパーティ デバイスを対象としたモニターリング ポリシーの作成 （293 ページ）を参照してください。

ステップ 1 **[ダッシュボード（Dashboard）] > [デバイス トレンド（Device Trends）] > [デバイス（Device）]** の順に選択します。

ステップ 2 ダッシュボードの右上隅にある [設定（Settings）] をクリックして、[ダッシュレットの追加（Add Dashlets）] を選択します。

ステップ 3 [デバイス ダッシュレット（Device Dashlets）] リストを展開します。

ステップ 4 [汎用ダッシュレット（Generic Dashlet）] を見つけて、**[Add]** をクリックします。

Cisco EPN Manager により、空白の汎用ダッシュレットが [デバイス トレンド（Device Trends）] ダッシュボードに追加されます。

ステップ 5 必要に応じて新しいダッシュレットを設定します。

少なくとも、次の設定を行う必要があります。

- [ダッシュレット タイトル（Dashlet Title）] フィールドに、わかりやすいタイトルを入力します。
- ダッシュボード内のすべてのダッシュレットに時間フィルタを適用しない場合は、[ダッシュボードの時間フィルタをオーバーライドする（Override Dashboard Time Filter）] チェックボックスをオンにします。
- [タイプ（Type）] ドロップダウン リストで、ダッシュレットのデータを表または線グラフのどちらで表示するかを選択します。（どちらを選択するかに関わらず、Cisco EPN Manager では、ダッシュレットの下部に、表示形式を変更するためのトグルが表示されます）。
- [ポリシー名（Policy Name）] ドロップダウン リストから、このダッシュレットのデータを収集するモニターリング ポリシーを選択します。使用可能なモニターリング ポリシーについては、モニターリング ポリシー リファレンス （1199 ページ）を参照してください。

ステップ 6 [保存して閉じる（Save and Close）] をクリックします。

データがダッシュレットに表示されない場合は、「ダッシュボードのデータが不足している理由の特定」を参照してください。

[ドック（Dock）] ウィンドウのカスタマイズ

[ドック（Dock）] ウィンドウを使用すると、頻繁に使用する Web GUI ページやポップアップ ウィンドウ（特定のデバイスの 360 度ビューなど）に素早く移動できます。このウィンドウでは、最近アクセスした 15 のページへのリンクと Cisco EPN Manager トレーニング資料へのリンクにもアクセスできます。このウィンドウを開くには、（ページの右上の領域にある）[ドック（Dock）] アイコンをクリックします。

[ドック（Dock）] ウィンドウに表示されるリンクを更新するには、次の手順に従います。

ステップ 1 Web GUI ページのリンクを [お気に入り（Favorites）] タブ（[ドック（Dock）] アイコン > **[アクセスしたリンク（Links Visited）]** > **[お気に入り（Favorites）]**）に追加する場合：

a) 追加する Web GUI ページを開きます。

b) ページの左上の領域にある星の形をした（[お気に入り（Favorites）]）アイコンをクリックします。

ステップ 2 ポップアップ ウィンドウのリンクを [ドッキング アイテム（Docked Items）] 領域（[ドック（Dock）] アイコン > [ドッキング アイテム（Docked Items）]）に追加する場合：

a) 追加するポップアップ ウィンドウを開き、その 360 度ビューを開きます。
b) ポップアップ ウィンドウの右上隅にある [ドックに追加（Add to Dock）] アイコンをクリックします。

ダッシュボードのデータが不足している理由の特定

ダッシュボードまたはダッシュレットからデータが欠落している場合、Cisco EPN Manager は次のような考えられる理由をダッシュレットにエラーメッセージで表示します。

- モニターリングポリシーが有効になっていません（Monitoring policy not enabled）
- システム内のデバイスが管理対象外か、または到達できません（Unmanaged or unreachable devices in the system）
- デバイスでテクノロジーがサポートされていません（Technology isn't supported on the device）
- サーバー時間が正確でないか、またはサーバー時間がデバイスと同期していません（Inaccurate server time or server time not synced with the device）

次の手順を実行して、原因を特定します。

ステップ 1 ダッシュレットのデータがフィルタ処理されていないかを確認します。

ダッシュレット名の隣に [編集済み（Edited）] と表示されている場合は、次の手順を実行します。

a) [編集（Edit）] アイコンをクリックし、現在のフィルタ設定を調整します。
b) [保存して閉じる（Save and Close）] をクリックします。

ステップ 2 デバイスに問題があるかどうかをチェックします。

基本デバイス情報を取得する：[デバイス 360（Device 360）] ビュー （106 ページ）を参照してください。

ステップ 3 デバイス インベントリが正しく収集されているかを確認します。

インベントリ収集またはディスカバリの問題があるデバイスの検索 （88 ページ）を参照してください。

ステップ 4 Cisco EPN Manager が使用しているモニターリング ポリシーを確認して、必要なデータが収集されているかどうかを確認します。

a) ダッシュレットの [ヘルプ（Help）] アイコンをクリックして、ダッシュレットの概要ポップアップ ウィンドウを開きます。
b) [データ ソース（Data Sources）] の下に示されるモニターリング ポリシーを確認します。

モニターリング ポリシーについては、モニターリング ポリシー リファレンス （1199 ページ）で説明しています。

c) [モニターリング ポリシー（Monitoring Policies）] ページにこのポリシーがリストされ、アクティブであることを確認します。

このページを開くには、**[モニターリング（Monitor）]**>**[モニターリング ツール（Monitoring Tools）]**>**[モニターリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] を選択します。

- ポリシーがリストされていない場合は、ステップ 4d に進みます。
- ポリシーがリストされ、ステータスが [アクティブ（Active）] である場合には、[詳細（Details）] をクリックして [収集データ（Collection Data）] ポップアップ ウィンドウを開き、デバイスがポリシーによってモニターリングされていることを確認します。そうでない場合は、ポリシーでモニターするデバイス セットの変更 （295 ページ）の説明に従ってポリシーを調整する必要があります。デバイスがポリシーに含まれている場合は、ステップ 5 に進みます。
- ポリシーがリストされ、ステータスが [非アクティブ（Inactive）] である場合には、ポリシーを選択して [アクティブ化（Activate）] をクリックします。

d) 新しいモニターリング ポリシーを作成してアクティブ化します。

モニター対象を調整する （291 ページ）を参照してください。

ステップ 5 関連するデータがシステムから消去されていないかを確認します。

データ保持設定が Web GUI データに及ぼす影響 （988 ページ） を参照してください。

別の仮想ドメインで作業する

仮想ドメインは、デバイスの論理的なグループであり、特定のサイトやデバイスへのアクセスを制御するために使用されます。仮想ドメインは、物理サイト、デバイス タイプ、ユーザー コミュニティ、または管理者が選択するあらゆる指定項目に基づいて設定できます。すべてのデバイスは ROOT-DOMAIN に属します。ROOT-DOMAIN はすべての新しい仮想ドメインの親ドメインです。仮想ドメインの詳細については、デバイスへのユーザー アクセスを制御するための仮想ドメインの作成 （1030 ページ）を参照してください。

複数の仮想ドメインへのアクセスが許可されている場合は、次の手順に従って別のドメインに切り替えることができます。

ステップ 1 タイトル バーの右側にある ⚙ をクリックします。

ステップ 2 [**Virtual Domain:** *current-domain*] を選択します。

ステップ 3 [仮想ドメイン（Virtual Domain）] ドロップダウン リストで別のドメインを選択します。

Cisco EPN Manager によって作業ドメインがただちに変更されます。

ジョブ ダッシュボードを使用したジョブの管理

適切なユーザー アカウント権限が付与されている場合は、ジョブ ダッシュボードを使用して Cisco EPN Manager ジョブを管理できます。ジョブ ダッシュボードを表示するには、**[管理**

（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] の順に選択します。ここでは、ジョブが正常に完了したか、部分的に成功したか、または失敗したかを確認できます。

実行中のジョブの数が多すぎると、Cisco EPN Manager ではリソースが使用可能になるまで他のジョブがキューに入れられます。これが原因で、スケジュールされているジョブがその通常の開始時刻を超えて遅延されると、そのジョブは実行されません。このジョブは手動で実行する必要があります。

一部のジョブでは承認が必要です。この場合は、Cisco EPN Manager から、管理者権限が付与されているユーザーに対し、ジョブがスケジュールされており承認が必要であることを通知する電子メールが送信されます。ジョブの承認後にジョブが実行されます。ジョブ承認者を設定してジョブを承認する （1027 ページ）を参照してください。

ジョブテーブルが自動更新される時間間隔を設定できます。ページの上部隅にある [設定（Settings）] をクリックし、[自動更新間隔の設定（Set Auto Refresh Rate）] フィールドのドロップダウンリストから値を選択し、[保存（Save）] をクリックします。

（注） ジョブテーブルの自動更新を無効にするには、ドロップダウンリストから [オフ（OFF）] を選択します。

次の表に、ジョブ ダッシュボードに表示されるボタンの説明を示します。

表 *3:* ジョブ ダッシュボードのボタン

ボタン	説明
[ジョブの削除（Delete Job）]	ジョブ ダッシュボードからジョブを削除します。
[ジョブの編集（Edit Job）]	選択したジョブの設定を編集します。
[スケジュールの編集（Edit Schedule）]	シリーズのスケジュールを表示し、編集できるようにします（開始時刻、間隔、終了時刻）。 （注） スケジュール済みのジョブのスケジュールを編集すると、そのジョブのステータスが [承認待ち（Pending for Approval）] に変更されます。これは、ジョブを作成したユーザーからの承認が編集のたびに必要になるためです。
[実行（Run）]	選択したジョブの新しいインスタンスを実行します。このボタンは、部分的に成功したジョブまたは失敗したジョブを再実行する場合に使用します。ジョブは、失敗したコンポーネントまたは部分的に成功したコンポーネントに対してのみ実行されます。

ボタン	説明
[中断（Abort）]	現在実行中のジョブを停止します。ただしこのジョブは後で再実行できます。すべてのジョブを中断することはできません。これに該当する場合、Cisco EPN Manager がそのこのことを示します。
[シリーズをキャンセル（Cancel Series）]	現在実行中のジョブを停止し、このジョブを再実行できないようにします。ジョブがシリーズの一部の場合、今後の実行には影響しません。
[シリーズの一時停止（Pause Series）]	スケジュールされているジョブ シリーズを一時停止します。シリーズを一時停止にすると、（[実行（Run）]を使用して）そのシリーズのインスタンスを実行することはできません。
[シリーズの再開（Resume Series）]	一時停止になっていたスケジュール済みジョブ シリーズを再開します。

（注） [ジョブの削除（Delete Job）]、[中断（Abort）]、および[シリーズをキャンセル（Cancel Series）]ボタンは、システム ジョブとポーラー ジョブの場合は使用できません。

（注） ルートユーザーとしてログインしている場合は、[ジョブダッシュボード（Job Dashboard）]ですべてのジョブを表示できます。非ルートユーザーとしてログインしている場合は、自分が実行したジョブのみを表示できます。

ジョブの詳細を表示するには、次の手順に従います。

ステップ 1 **[管理（Administration）]>[ダッシュボード（Dashboards）]>[ジョブ ダッシュボード（Job Dashboard）]**の順に選択します。

ステップ 2 [ジョブ（Jobs）]ペインで、基本的な情報（ジョブ タイプ、ステータス、ジョブ期間、次回開始時刻など）を取得するジョブ シリーズを選択します。

ステップ 3 ジョブ間隔を表示するには、ジョブ インスタンスのハイパーリンクをクリックします。

ジョブ ページ上部の[繰り返し（Recurrence）]フィールドに、ジョブの繰り返し頻度が表示されます。ジョブ間隔の詳細は、トリガーするすべてのジョブで追加されます。 ジョブの詳細ページは、ジョブが完了するまで 5 秒ごとに更新されます。

ステップ 4 失敗したジョブまたは部分的に成功したジョブに関する詳細を確認するには、ジョブ インスタンスのハイパーリンクをクリックし、結果ページに表示されるエントリを展開します。

これは特に、インベントリ関連のジョブで便利です。たとえば、ユーザーがCSVファイルを使用してデバイスをインポートした場合（一括インポート）、ジョブは [ジョブ（Jobs）] サイドバー メニューの **[ユー**

ザー ジョブ（User Jobs）] > [デバイスの一括インポート（Device Bulk Import）] に表示されます。ジョブの詳細には、正常に追加されたデバイスと、追加されなかったデバイスのリストが表示されます。

例

失敗したソフトウェア イメージ インポート ジョブのトラブルシューティングを行うには、次の手順に従います。

1. [ジョブ（Jobs）] サイドバー メニューから、**[ユーザー ジョブ（User Jobs）] > [ソフトウェア イメージのインポート（Software Image Import）]** を選択します。
2. テーブルにある失敗したジョブを見つけ、そのハイパーリンクをクリックします。
3. ジョブの詳細がまだ展開されていない場合には展開し、このジョブに関連付けられているデバイスのリストと、各デバイスのイメージ インポートのステータスを表示します。
4. 特定デバイスのインポートの詳細情報を表示するには、[ステータス（Status）] 列でそのデバイスの [i]（**情報**）アイコンをクリックします。こうすると、[イメージ管理ジョブの結果（Image Management Job Results）] ポップアップ ウィンドウが開きます。
5. 各ステップとステータスを確認します。たとえば、[プロトコル SFTP を使用したイメージの収集（Collecting image with Protocol: SFTP）] 列に、そのデバイスで SFTP がサポートされていないことが示されることがあります。

ユーザー設定の変更

ユーザー設定を変更するには、画面の右上隅にある ⚙ アイコンをクリックし、**[自分の環境設定（My Preferences）] > [全般（General）]** を選択します。

カテゴリ	ユーザー プリファレンス設定	説明
リストページ（**List pages**）	ページあたりのリストの項目数（**Items Per Page List**）	この設定を使用して、AP、コントローラ、サイトマップ、[Roles, & AAA）] > [Active Sessions] の [Monitoring] ページに表示されるエントリの数を定義します。 デフォルトでは、50 のエントリが表示されます。 （注） この設定は、ネットワーク デバイス、アラームおよびイベント、設定アーカイブ、ソフトウェア イメージの管理、設定には適用されません。
ネットワークトポロジ（**Network Topology**）	デバイスグループの選択を自動的に切り替えて、参加デバイスをすべて表示する（**Automatically switch device group selection to show all participating devices**）	この設定を使用すると、デバイスグループの選択が自動的に切り替わり、トポロジービューにすべての参加デバイスが表示されます。デフォルトでは、この設定は無効になっています。
	自動更新の間隔（マップ、テーブル）	この設定を使用して、ネットワークトポロジビューのマップとテーブルが更新される時間間隔を定義します。設定できる更新間隔は、30 秒、1 分、2 分、または 5 分です。マップとテーブルを更新しない場合は、[自動更新なし（No auto-refresh）] を選択します。 デフォルトでは、更新間隔は 1 分です。

カテゴリ	ユーザー プリファレンス設定	説明
サービスプロビジョニング	デフォルトテクノロジー	この設定を使用して、サービス プロビジョニング ページに移動して新しいサービスを作成するときにデフォルトで選択されるテクノロジーを定義します。 （注） このユーザー設定が設定されていない場合、キャリアイーサネットがデフォルト値として設定されます。
	デフォルトのサービスタイプ	この設定を使用して、サービス プロビジョニング ページに移動して新しいサービスを作成するときにデフォルトで選択されるサービスタイプを定義します。 （注） このユーザー設定が設定されていない場合、アクセス EPL がデフォルト値として設定されます。
シャーシビューの設定（**Chassis View Configuration**）	**UI** 更新間隔（**UI refresh interval**）	この設定を使用して、UI 内のデータがシャーシ ビューで更新される頻度を定義します。 デフォルトでは、UI の更新間隔は 1 分です。
	表示するシャーシラック（**Chassis racks to display**）	この設定を使用して、Cisco EPN Manager が表示するシャーシラックの数を定義します。 デフォルトでは、この値は 2 です。

カテゴリ	ユーザー プリファレンス設定	説明
デバイス インベントリ リスト ビュー（**Device Inventory List View**）	デバイスリストテーブルの更新間隔（**Device List Table Refresh Interval**）	この設定を使用して、[ネットワークデバイス（Network Devices）]ページのテーブルが更新される時間間隔を定義します。設定できる更新間隔は、1 分、2 分、5 分、10 分、15 分または 30 分です。テーブルを更新しない場合は、[更新しない（Do not refresh）] を選択します。 この設定のデフォルト値は[更新しない（Do not refresh）] です。
モビリティサービスエンジン（**Mobility Services Engine**）	**MSE 管理ビューを使用（Use MSE Admin view**）	デフォルトで、この設定は有効になっています。

カテゴリ	ユーザー プリファレンス設定	説明
ユーザーアイドルタイムアウト（User Idle Timeout）	アイドル状態のユーザーをログアウト（Logout idle user）	この設定を使用して、アイドル状態のユーザーを自動的にログアウトするかどうかを定義します。デフォルトで、このオプションは有効になっています。 （注） この設定を無効にするには、最初に [システム設定（System Settings）] で [グローバルアイドルユーザー（Global idle user）] がオフになっていることを確認します。
	指定時間後にアイドル状態のユーザーをログアウトする（Logout idle user after）	この設定では、自動ログアウトのアイドル時間も設定できます。デフォルトの値は 10 分です。 （注） この値は [システム設定（System Settings）] の [グローバルアイドルタイムアウト（Global Idle timeout）] の値を超えることはできません。

必要な変更を加えたら、[保存（Save）] をクリックして変更した設定を適用します。

ページレベルのカスタマイズおよび設定をクリアするには、EPNM ウィンドウの右上隅にある [GUI の状態設定のクリア（Clear GUI State Settings）] をクリックします。これにより、[ネットワーク概要（Network Summary）] ダッシュボード、[パフォーマンスグラフ（Performance Graphs）]、[ネットワークデバイス（Network Devices）] などのページに行われたカスタム設定が削除され、アプリケーションがデフォルト値に更新されます。

[アラームおよびイベント（Alarms and Events）] のユーザー設定の詳細については、アラームとイベントの表示設定のセットアップ （313 ページ）を参照してください。

Cisco EPN Manager 機能の拡張

上級ユーザーは、次のツールを使用して Cisco EPN Manager を拡張できます。

- Cisco Evolved Programmable Network Manager MTOSI API：Cisco EPN Manager を運用サポートシステム（OSS）と統合します。
- Cisco Evolved Programmable Network Manager REST API：その他の管理操作を管理します。

これらのツールに関する情報を確認するには、タイトル バーの右側にある ⚙ をクリックし、**[ヘルプ（Help）]** > **[APIヘルプ（API Help）]** を選択します。Cisco.com から、次のドキュメントをダウンロードすることもできます。

- Cisco Evolved Programmable Network Manager MTOSI API ガイド（OSS 統合）
- Cisco Evolved Programmable Network Manager RESTCONF NBI ガイド

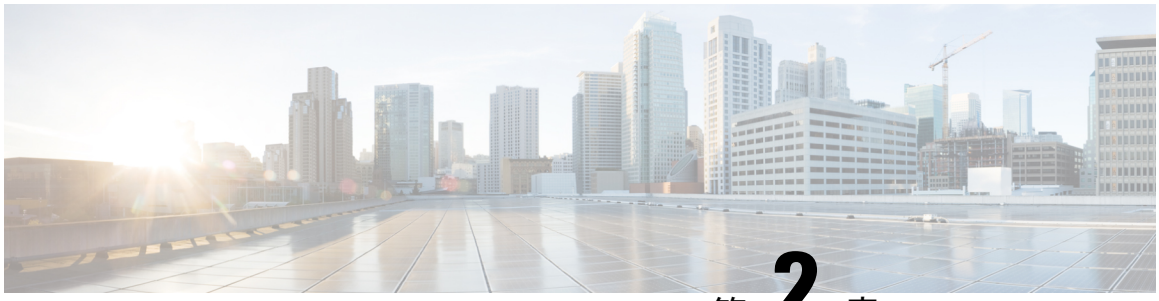
最新のインベントリに存在をチェック Cisco EPN Manager マニュアル

Cisco EPN Manager で提供されているすべてのドキュメントに関する情報およびリンクについては、『Cisco Evolved Programmable Network Manager ドキュメントの概要』を参照してください。

（注） マニュアルの発行後に、マニュアルをアップデートすることがあります。マニュアルのアップデートについては、Cisco.com で確認してください。

第 II 部

インベントリの管理



第 2 章

デバイスの追加と整理

どのデバイス ソフトウェア バージョンが Cisco EPN Manager によってサポートされているか。

すべてのデバイスは、認定されたデバイス ソフトウェア バージョンを実行している必要があります。ただし、特定のデバイスは最小のデバイス ソフトウェア バージョンを実行している必要があります。デバイス ソフトウェア バージョンを確認する方法については、次の表の手順に従ってください。

この情報を見つけるには、次の手順を実行します。	手順
認定されたすべてのデバイス ソフトウェア バージョンの一覧	『Cisco Evolved Programmable Network Manager のサポート対象デバイス』を参照してください。
	[ヘルプ（Help）] > **[サポートされるデバイス（Supported Devices）]** を選択し、[ソフトウェアバージョン（Software Version）] 列の [i] にカーソルを合わせるとポップアップが表示されます。
最小デバイス ソフトウェア バージョンが必須なデバイス	**[ヘルプ（Help）]** > **[サポートされるデバイス（Supported Devices）]** を選択し、[ソフトウェアバージョン（Software Version）] 列で **>=x.x** のようなテキストを確認します（たとえば **>=12.2** は、デバイスが少なくともデバイス ソフトウェア バージョン 12.2 を実行する必要があることを意味します）。

汎用デバイスのサポート

Cisco EPN Managerでは、公式に（機能が）サポートされていない、インベントリ機能と障害機能が制限された汎用のシスコ デバイスとサードパーティ製デバイスを管理できます。

表 *4 :* 汎用デバイスのサポート

汎用デバイスのタイプ	サポートされる機能	サポートされている **MIB**	サポートされる障害
シスコ デバイス	[システム（System）] - [概要（Summary）] システム：環境 [システム（System）] - [シビックロケーション（Civic Location）] [システム（System）] - [モジュール（Modules）] [システム（System）] - [物理ポート（Physical Ports）] [システム（System）] - [センサー（Sensor）] [インターフェイス（Interfaces）] - [すべてのインターフェイス（All Interfaces）] [インターフェイス（Interfaces）] - [イーサネットインターフェイス（Ethernet Interfaces）] [物理リンク（Physical Links）]	SNMPv2 ENTITY-MIB IF-MIB LLDP-MIB CISCO-ENTITY-FRU-CONTROL-MIB	リンクアップ/リンクダウン（IF-MIB） ウォームスタート（SNMPv2-MIB） コールドスタート（SNMPv2-MIB） 認証エラー（SNMPv2-MIB） BDI インターフェイスのダウン/アップ（BDI にローカライズされるリンクダウン/アップ）（IF-MIB） entSensorThresholdNotification（CISCO-ENTITY-SENSOR-MIB）

汎用デバイスのタイプ	サポートされる機能	サポートされている MIB	サポートされる障害
シスコ以外のデバイス	[システム（System）] - [概要（Summary）] [システム（System）] - [モジュール（Modules）] [システム（System）] - [物理ポート（Physical Ports）] [インターフェイス（Interfaces）] - [すべてのインターフェイス（All Interfaces）] [物理リンク（Physical Links）]	SNMPv2 ENTITY-MIB IF-MIB LLDP-MIB	リンクアップ/リンクダウン（IF-MIB） ウォームスタート（SNMPv2-MIB） コールドスタート（SNMPv2-MIB） 認証エラー（SNMPv2-MIB）

インベントリ検出プロセス

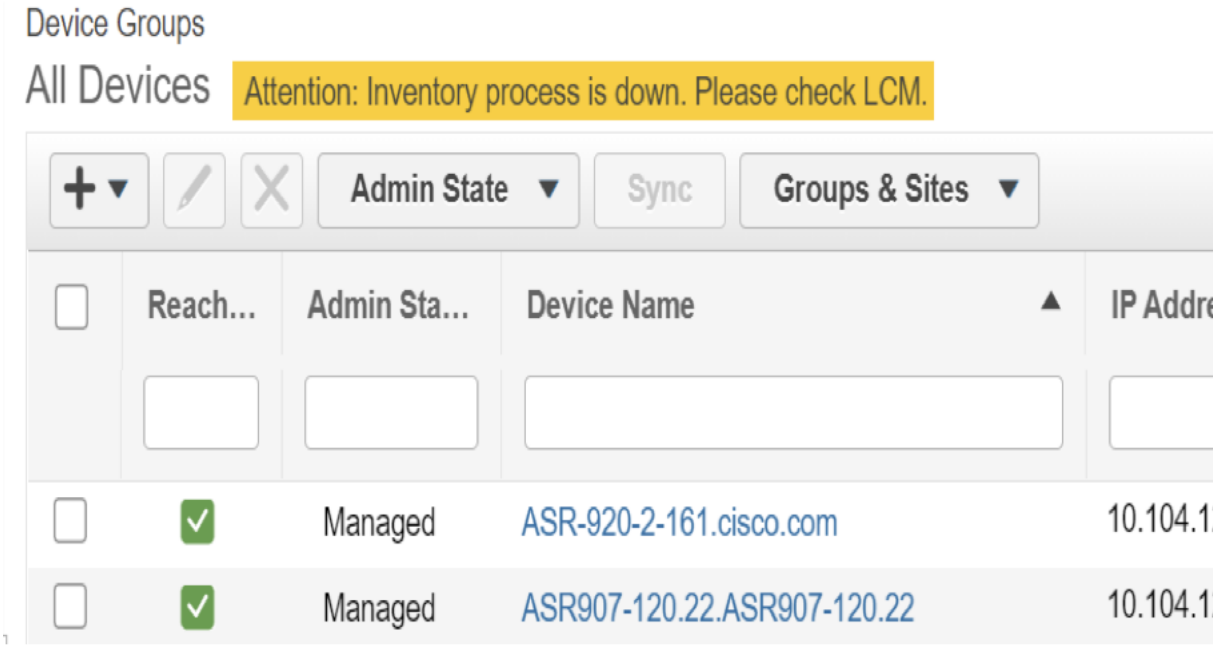
Cisco EPN Manager でデバイスのスケーリングを有効にするには、EPNM プロセスのインベントリ検出コンポーネントを別のプロセス（inventory-discovery-process）として実行します。インベントリ収集に関連するすべての機能（デバイスの追加またはインポート、手動同期、詳細同期および事後同期、障害が発生した機能の同期、インベントリの切り替え、およびユーザー定義のインベントリ検出を含む）は、nventory-discovery-process によって実行されます。

（注） IOS-XR デバイスのオープン設定インターフェイスを介して行われた設定は、EPNM では検出されません。

inventory-discovery-process がダウンした場合の動作

Cisco EPN Manager は、インベントリ検出プロセスがダウンすると、[ネットワークデバイス（Network Devices）] ページにエラーメッセージを表示します。

（注） inventory-discovery-process がダウンしている場合は、インベントリ操作を実行できません。プロセスが起動するまで待ってから、インベントリ操作を再開してください。



inventory-discovery-process に関連するログは、`/opt/CSCOlumos/logs/inventory-discovery-process` に保存されます。詳細については、インベントリ検出プロセスのログ （1102ページ）を参照してください。

inventory-discovery-process のステータス（started、stopped、stopped、unreachable、および restarting）は **[モニター（Monitor）]** > **[アラームおよびイベント（Alarms and Events）]** ページにシステム生成イベントとして表示されます。

たとえば、「Process inventory-discovery-process is unreachable and will try to restart」というイベントは、inventory-discovery-process に到達できず、自動的に再起動されることを示します。

重要 「Process inventory-discovery-process reached auto-restart limit」というイベントは、inventory-discovery-process が複数回再試行したにもかかわらず自動的に再起動できなかったことを示します。この場合、Cisco Technical Assistance Center（TAC）でサポートケースを開くことをお勧めします。シスコ サポート ケースの登録 （1090 ページ） を参照してください。

Cisco EPN Manager へのデバイスの追加

Cisco Evolved Programmable Network Manager は、デバイス、ロケーション、およびポートグループを使用してネットワーク内の要素を構成します。デバイスをテーブルまたはマップ（ネットワーク トポロジ）で表示すると、デバイスは属しているグループを単位として整理されます。デバイスが Cisco EPN Manager に追加されると、**Unassigned Group**という名前のグループ

に割り当てられます。その後、簡単な管理と設定のためのデバイス グループの作成 （92 ページ） で説明されているように、デバイスを目的のグループに移動できます。

（注）

- Cisco WLC を Cisco EPN Manager に追加するには、サポートされていないアクセス ポイント（AP）がないことを確認してください。そのようにしないと、 Cisco EPN Manager はその WLC から AP を検出しません。
- Cisco EPN Manager は、同じ IP アドレスを共有する複数の独立したネットワークをサポートしていません。追加するネットワーク要素に競合する IP アドレスが含まれていないことを確認してください。

表 *5:* デバイスの追加方法

サポートされているデバイスの追加方法	参照先：
以下を使用してシード デバイスのネイバーを検出して複数のデバイスを追加する	ディスカバリを使用したデバイスの追加（49 ページ）。
• Ping スイープと SNMP ポーリング（クイック ディスカバリ）	• クイック ディスカバリの実行 （51 ページ）
• カスタマイズされたプロトコル、クレデンシャル、およびフィルタ設定（ディスカバリ ジョブを繰り返す場合に便利）	• カスタマイズされたディスカバリ設定でのディスカバリの実行 （52 ページ）
CSV ファイルで指定された設定を使用して複数のデバイスを追加する	CSV ファイルを使用したデバイスのインポート （55 ページ）。
単一のデバイスを追加する（たとえば、新しいデバイス タイプの場合）	手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） （56 ページ）

次のトピックでは、キャリアイーサネットと光デバイスを Cisco EPN Manager に追加する方法の例を示します。

- 例：単一の Cisco NCS 2000 または NCS 4000 シリーズ デバイスの追加 （58 ページ）
- 例：プロキシ設定を使用した ENE としてのネットワーク要素の追加 （59 ページ）

Cisco EPN Manager での Cisco ME1200 デバイスの追加

Cisco EPN Manager で Cisco ME1200 デバイスを追加する際は、次の設定に従ってください。

- SNMP：他のデバイスと同じ SNMP 設定を使用します。

- CLI：プロトコル設定が [SSH2] に設定されていることを確認します。ポートを使用して telnet 経由でデバイスにアクセスできますが、SSH プロトコルを使用することを推奨します。telnet が使用されている場合は、使用されるカスタム telnet ポートは 2323 でなければなりません。
- Cisco ME1200 デバイスの設定変更は Cisco EPN Manager によって自動的に検出されないことに留意してください。変更後、デバイスを手動で同期する必要があります。これを行うには、[ネットワークデバイス（Network Devices）] テーブルで必要なデバイスを選択し、[同期（Sync）] をクリックします。

ディスカバリを使用したデバイスの追加

Cisco EPN Manager は、次の 2 つのディスカバリ方式をサポートしています。

- シードデバイスからの ping スイープ（クイック ディスカバリ）。デバイス名、SNMP コミュニティ、シード IP アドレス、およびサブネット マスクが必要です。この方法は、光デバイスのディスカバリには使用できません。クイック ディスカバリの実行 （51 ページ）を参照してください
- カスタマイズされたディスカバリ方法（ディスカバリ設定）の使用：設定を行い、今後ディスカバリを再実行する場合は、この方法をお勧めします。光デバイスを検出する場合は、この方法を使用します。カスタマイズされたディスカバリ設定でのディスカバリの実行 （52 ページ）を参照してください。

（注）

- ディスカバリ ジョブが既存のデバイスを再検出し、デバイスの最後のインベントリ収集ステータスが [完了済み（Completed）] である場合、Cisco EPN Manager は、既存のクレデンシャルを、ディスカバリ設定で指定されたクレデンシャルで上書きしません。他のすべてのステータス（既存のデバイス上）の場合、Cisco EPN Manager は、デバイスのクレデンシャルを、ディスカバリ設定で指定されたクレデンシャルで上書きします。
- データベースのメンテナンス期間中に多数のデバイスが追加された場合、サービス検出に通常より時間がかかることがあります。したがって、夜間や週末には大規模な作業を回避することをお勧めします。
- 自律 AP がディスカバリ プロセスから除外され、検出時間が最適化されます。[デバイスのインポート（Import Devices）] または [クレデンシャルプロファイル（Credential Profile）] を使用して、自律 AP を手動で追加する必要があります。

デバイスのディスカバリ プロセスは、次に示す順序で実行されます。Cisco EPN Manager はディスカバリの実行時に、デバイスの到達可能性状態（[到達可能（Reachable）]、[ping 到達可能（Ping Reachable）]、または [到達不能（Unreachable）]）を設定します。状態の詳細については、「デバイスの到達可能性状態と管理状態 （84 ページ）」を参照してください。

1. Cisco EPN Manager は、ICMP ping を使用して、デバイスに到達可能であるかどうかを判別します。デバイスに到達できない場合、到達可能状態は[到達不能（Unreachable）]に設定されます。
2. サーバーは、SNMP 通信が可能かどうかをチェックします。
   - ICMP がデバイスに到達可能で、SNMP 通信が不可能な場合、その到達可能性状態は [ping 到達可能（Ping Reachable）] に設定されます。
   - ICMP と SNMP の両方がデバイスに到達できる場合、その到達可能性状態は [到達可能（Reachable）] です。
3. デバイスの Telnet および SSH クレデンシャルが確認されます。クレデンシャルに障害が起きた場合は、障害に関する詳細が [ネットワークデバイス（Network Devices）] テーブルの [最後のインベントリ収集ステータス（Last Inventory Collection Status）] 列に表示されます（たとえば、「**Wrong CLI Credentials**」など）。到達可能性の状態は変更されません。
4. Cisco EPN Manager が SNMP を使用して必要な通知を受信できるように、デバイス設定が変更されて、トラップの受信者が追加されます。
5. インベントリ収集プロセスが開始され、すべてのデバイス情報が収集されます。
6. Web GUI にすべての情報（ディスカバリが完全に成功したか、部分的に成功したかなど）が表示されます。

（注） Cisco EPN Manager がデバイスの SNMP 読み取り/書き込みクレデンシャルを検証すると、デバイス ログが更新され、Cisco EPN Manager（IP アドレスで識別される）によって構成が変更されたことが示されます。

SNMP 通信の確認

デバイスの到達可能性の状態が [ping到達可能（Ping Reachable）] に設定されている場合は、次の手順を実行します。

（注） Cisco NCS 2000 デバイスの場合は、SNMP のクレデンシャルに加えて（または代わりに）TL1 のクレデンシャルを確認します。

ステップ 1 Cisco EPN Manager によってデバイスの検証に使用されるクレデンシャルが正しいことを確認します。

ステップ 2 デバイス上で SNMP が有効になっており、デバイスに設定されている SNMP 資格情報が、Cisco EPN Manager で設定されている資格情報と一致することを確認します。

ステップ 3 管理対象デバイスと Cisco EPN Manager サーバー間での SNMP パケットの転送に関与するすべてのネットワーク デバイスのセキュリティ設定（デフォルト動作）により、SNMP パケットがドロップされているかどうかを確認します。

検出されたデバイスの管理 IP アドレス タイプ（IPv4/IPv6）の指定

検出されたデュアルホーム（IPv4/IPv6）デバイスでは、Cisco EPN Manager が管理 IP アドレスとして IPv4 アドレスまたは IPv6 アドレスを使用するかどうかを指定します。

（注） デバイスインベントリでは、DNS 名の IPv6 サポートが制限されています。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）]** > **[検出（Discovery）]** を選択します。

ステップ 2 [管理アドレスに対する IPv4/IPv6 設定（IPv4/IPv6 Preference for Management Address）] ドロップダウンリストから [v4] または [v6] のいずれかを選択します。

（注） 選択する管理 IP アドレスで IPv4 アドレスと IPv6 アドレスが混在していないことを確認してください。

ステップ 3 [保存（Save）] をクリックします。

クイック ディスカバリの実行

単一のシードデバイスを使用して ping スイープを実行する場合には、この方法を使用します。デバイス名、SNMP コミュニティ、シードの IP アドレスおよびサブネット マスクのみが必要です。構成管理機能の使用を計画している場合は、プロトコル、ユーザー名、パスワード、およびイネーブル パスワードを入力する必要があります。

始める前に

デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニターできるように設定する （69 ページ）を参照してください。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ディスカバリ（Discovery）]** の順に選択して、ウィンドウ右上の [クイック ディスカバリ（Quick Discovery）] リンクをクリックします。

ステップ 2 少なくとも、名前、SNMP コミュニティ、シードの IP アドレス、およびサブネット マスクを入力します。

ステップ 3 [今すぐ実行（Run Now）] をクリックします。

次のタスク

結果を表示するには、[ディスカバリ ジョブ インスタンス（Discovery Job Instances）] 領域の、[ジョブ（Job）] ハイパーリンクをクリックします。

カスタマイズされたディスカバリ設定でのディスカバリの実行

Cisco EPN Manager は、ディスカバリ プロファイルを使用してネットワーク デバイスを検出できます。ディスカバリ プロファイルには、ネットワーク要素を検索し、それらに接続してインベントリを収集する方法を Cisco EPN Manager に指示する設定のコレクションが含まれています。たとえば、Cisco EPN Manager に CDP、LLDP、OSPF を使用してデバイスを検出することや、単純な ping スイープの実行を指示できます（ping スイープの結果の例は「ping スイープのサンプルの IPv4 IP アドレス （53 ページ）」に記載されています）。フィルタを作成して、コレクションの微調整、クレデンシャルセットの指定、およびその他のディスカバリ設定を行うこともできます。プロファイルは必要な数だけ作成できます。

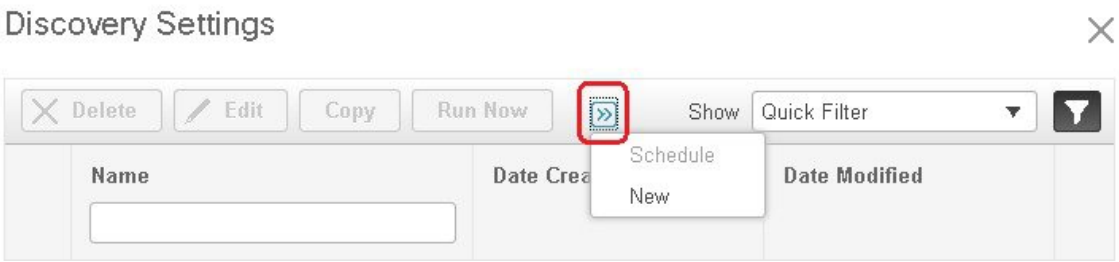
プロファイルの作成後、プロファイルを使用するディスカバリ ジョブを作成し、実行します。ディスカバリジョブの結果は [ディスカバリ（Discovery）] ページで確認できます。ジョブをスケジュールして、定期的に実行を繰り返すこともできます。

始める前に

Cisco EPN Manager がデバイスを検出できるように、デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニターできるように設定する （69 ページ）を参照してください。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）] を選択して、ウィンドウ右上の [ディスカバリ設定（Discovery Settings）] リンクをクリックします。（[ディスカバリ設定（Discovery Settings）] リンクが表示されない場合は、[クイック ディスカバリ（Quick Discovery）] リンクの隣の矢印アイコンをクリックします）。

ステップ 2 [検出設定（Discovery Settings）] ポップアップで、[新規（New）] をクリックします。



ステップ 3 [ディスカバリ設定（Discovery Settings）] ウィンドウに設定を入力します。その設定に関する情報を取得するには、設定の隣にある [?] をクリックします。たとえば、[SNMPv2 クレデンシャル（SNMPv2 Credentials）] の横にある [?] をクリックすると、ヘルプのポップアップにプロトコルと必須の属性がすべて表示されます。

ステップ 4 [今すぐ実行（Run Now）] をクリックしてジョブをすぐに実行するか、[保存（Save）] をクリックして設定を保存し、後で実行するようにディスカバリをスケジュールします。

ping スイープのサンプルの IPv4 IP アドレス

次の表に、ping スイープ結果の例を記載します。

サブネット範囲	ビット数	IP アドレスの数	サンプルのシード IP アドレス	開始 IP アドレス	終了 IP アドレス
255.255.240.0	20	4094	205.169.62.11	205.169.48.1	205.169.63.254
255.255.248.0	21	2046	205.169.62.11	205.169.56.1	205.169.63.254
255.255.252.0	22	1022	205.169.62.11	205.169.60.1	205.169.63.254
255.255.254.0	23	510	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.0	24	254	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.128	25	126	205.169.62.11	205.169.62.1	205.169.63.127
255.255.255.192	26	62	205.169.62.11	205.169.62.1	205.169.63.62
255.255.255.224	27	30	205.169.62.11	205.169.62.1	205.169.63.30
255.255.255.240	36	18	205.169.62.11	205.169.62.1	205.169.63.14
255.255.255.248	29	6	205.169.62.11	205.169.62.9	205.169.63.14
255.255.255.252	30	2	205.169.62.11	205.169.62.9	205.169.63.10
255.255.255.254	31	0	205.169.62.11		
255.255.255.255	32	1	205.169.62.11	205.169.62.11	205.169.62.11

例：ディスカバリを使用した光デバイスの追加

次の例に、シードデバイスと OTS プロトコルを使用して Cisco NCS 2000 デバイスを検出する方法を示します。

始める前に

デバイスをモデル化してモニターできるように設定する （69 ページ）を参照して、光デバイスが正しく設定されていることを確認します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [検出（Discovery）]** を選択して、ウィンドウ右上の [ディスカバリ設定（Discovery Settings）] リンクをクリックします。

ステップ 2 [ディスカバリ設定（Discovery Settings）] ウィンドウで、[新規（New）] をクリックして新しい検出プロファイルを作成します。

a) ディスカバリ プロファイル名（**NCS2k_3_OTS** など）を入力します。

b) OTS プロトコルのシード デバイスとホップ カウントの情報を入力します。

1. [詳細プロトコル（Advanced Protocols）] の横にある矢印をクリックして検出プロトコルリストを開きます。
2. [OTS トポロジ（OTS Topology）] の横にある矢印をクリックして OTS プロトコルウィンドウを開きます。
3. [OTSを有効にする（Enable OTS）] チェックボックスをオンにします。
4. [行の追加（Add Row）]（[+]）アイコンをクリックします。
5. シード デバイスの IP アドレスとホップ カウント（例：**209.165.200.224** と **3**）を入力し、[保存（Save）] をクリックしてシード デバイス情報を追加します。
6. OTS プロトコル ウィンドウで [保存（Save）] をクリックしてウィンドウを閉じます。必要に応じて、OTS プロトコル ウィンドウの外側をクリックしてウィンドウを閉じます。

c) Cisco NCS 2000 シード デバイスの TL1 デバイス クレデンシャルを入力します。

1. [クレデンシャル設定（Credential Settings）] 領域で、[TL1 クレデンシャル（TL1 Credential）] の横にある矢印をクリックして TL1 クレデンシャルウィンドウを開きます。
2. [行の追加（Add Row）]（[+]）アイコンをクリックします。
3. シードデバイスの IP アドレス、ユーザー名、パスワード、および、必要に応じて、プロキシ IP アドレスを入力します。
4. セキュア TL1 アクセスの場合は [SSH] ドロップダウンリストから [有効化（Enabled）] を選択します。非セキュア TL1 の場合は、[無効化（Disabled）] を選択します。
5. [保存（Save）] をクリックしてクレデンシャル情報を追加します。
6. TL1 クレデンシャル ウィンドウで [保存（Save] をクリックしてウィンドウを閉じます。必要に応じて、TL1 クレデンシャル ウィンドウの外側をクリックしてウィンドウを閉じます。

ステップ 3 [保存（Save）] をクリックして新しいディスカバリ プロファイルを保存します。新しい **NCS2k_3_OTS** プロファイルが [ディスカバリ設定（Discovery Settings）] ウィンドウに追加されます。

（注） エラー メッセージが表示された場合は、プロトコルが有効になっていることを確認してください（これは一般的なエラーです）。

ステップ 4 [NCS2k_3_OTS] を選択し、[今すぐ起動（Run Now）] をクリックしてディスカバリ ジョブを開始します。

ステップ 5 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）]** を選択して、ジョブの結果を確認します。

CSV ファイルを使用したデバイスのインポート

デバイスをインポートする既存の管理システムがある場合、またはスプレッドシートに異なる値を指定する場合は、CSV ファイルを使用してデバイスを追加します。

CSV ファイルの作成

次の手順に従って、CSV ファイルを作成します。

ステップ 1 [一括インポート（Bulk Import）]ダイアログボックスで使用可能なテンプレートを使用して、一括インポート CSV ファイルを作成します。ダイアログボックスを開くには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択し、[ネットワークデバイス（Network Devices）]テーブルの上にある＋アイコンをクリックし、[一括インポート（Bulk Import）]を選択します。[一括デバイス追加サンプル テンプレート（bulk device add sample template）] を使用します。

ステップ 2 各種フィールドの意味と必要なフィールドを確認するには、Web GUI にある情報を使用します。この情報は、1 つのデバイスを追加する場合でも、デバイスを一括して追加する場合でも同じです。この情報を取得するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択し、[ネットワークデバイス（Network Devices）] テーブルの上にある＋アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。必須フィールドはアスタリスクで示されます。説明が必要なフィールドの横には [?] アイコンが表示されます（[?] アイコンにカーソルを置くと、フィールドの詳細が表示されます）。

ステップ 3 作業が完了したら、変更を保存し、ファイルの場所を書き留めておきます。これにより、「CSV ファイルのインポート （55 ページ）」の説明に従ってインポートすることができます。

CSV ファイルのインポート

CSV ファイルを使用してデバイスのインポートと追加を行うには、次の手順に従います。

始める前に

デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニターできるように設定する （69 ページ）を参照してください。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）]テーブルの上にある＋アイコンをクリックし、[一括インポート（Bulk Import）] を選択します。

ステップ 3 [一括インポート（Bulk Import）] ダイアログで、次の手順を実行します。

a) [操作（Operation）] ドロップダウンリストで [デバイス（Device）] が選択されていることを確認します。
b) [参照（Browse）] をクリックしてCSVファイルに移動し、[インポート（Import）] をクリックします。

（注） 一括デバイス追加サンプル テンプレートのダウンロードの一環としてすでにエクスポート済みの CSV ファイルを選択します。csv ファイルは手動で編集しないでください。

ステップ 4 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択して、インポートのステータスを確認します。

ステップ 5 矢印をクリックして、ジョブの詳細を展開し、インポート ジョブの詳細と履歴を表示します。問題が発生した場合は、追加されたデバイスの検証と問題のトラブルシューティング （87 ページ）を参照してください。

インポート中のグループの動作

インポート中のデバイスグループに関する次の点に注意してください。

- デバイスを追加する前に、CSV ファイルに記載されているすべてのデバイスグループが Cisco EPN Manager に存在するかどうかを確認します。
- デバイスに関連付けられたグループが存在しない場合、Cisco EPN Manager はそのデバイスをグループにマッピングせずに追加します。
- Cisco EPN Manager は、インポート前の既存のグループマッピングを保持します。
- CSV ファイルにデバイスの既存のグループマッピングと新しいグループマッピングの両方が含まれている場合、Cisco EPN Manager は既存のグループに加えて、新しいグループにデバイスを関連付けます。
- 関連付けられたデバイスグループにダイナミックルールがある場合でも、Cisco EPN Manager には、**[一括インポート（Bulk Import）]** オプションで追加されたデバイスが **[デバイスを手動で追加（Add Device Manually）]** 領域に一覧表示されます。
- デバイスグループマッピングを完了するには、インポートの完了後に同期を実行します。**[ネットワークデバイス（Network Devices）]** テーブルでデバイスを選択し、**[同期（Sync）]** をクリックします。

手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ）

新しいデバイスタイプを追加して、それらの設定をデバイスのグループに適用する前にテストするには、次の手順に従います。

始める前に

デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニターできるように設定する （69 ページ）を参照してください。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [デバイスの追加（Add Device）] ダイアログボックスで、必須フィールドに値を入力します。フィールドの横にある [?] をクリックすると、そのフィールドの説明が表示されます。

（注） （ほとんどの Cisco NCS デバイスなどの）デバイスには、Telnet/SSH 情報が必須です。Telnet/SSH（60 秒）と SNMP（10 秒）のデフォルト タイムアウトがネットワーク遅延に基づいてデバイスにより異なる場合でも、デバイスを構成できます。

[管理（Administration）] > [設定（Settings ）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] ページで [SSH の厳格なホスト チェック キー（Strict host check key for SSH）] チェック ボックスを選択して、追加したデバイスの SSH キーの検証を強制することができます。これにより、Telnet/SSH のパラメータの下でアルゴリズムおよび SSH キーを指定することができます。

デバイスを追加するときにアルゴリズムと SSH キーを手動で指定しない場合は、[管理（Administration）] > [設定（Settings ）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] ページで [最初の使用で SSH キーを信頼する（Trust SSH key on first use）] チェック ボックスを選択します。その最初の通信中にデバイスから送信された SSH キーは、信頼されデバイスのクレデンシャルに追加されます。この保存されたキーは、その後デバイスが追加されたときに自動入力され、検証に使用されます。

ステップ 4 （任意）デバイスを追加する前にクレデンシャルを確認するには、[クレデンシャルの確認（Verify Credentials）] をクリックします。

ステップ 5 [追加（Add）] をクリックして、指定した設定でデバイスを追加します。

（注） NCS 2000 デバイスの場合は、TL1 ユーザーにスーパーユーザー プロファイルを提供します。提供しないとデバイスが [警告付き完了（Completed with Warning）] ステータスになり、[シャーシ ビュー（Chassis View）] で [設定（Configuration）] > [セキュリティ（Security）] タブを利用できなくなります。

（注） Telnet/SSH クレデンシャルを指定しないと、一部のインベントリデータのみが収集される場合があります。

（注） NCS 2000 デバイスの場合、[シングルセッション TL1 を有効にする（Enable Single Session TL1）] の設定はリリース 11.0 以降を実行しているデバイスに対してのみ有効です。

（注） Cisco EPN Manager は、デフォルトでは UCS を自己署名証明書で承認しません。ユーザーがこれを手動で有効にするには、*/opt/CSCOlumos/xmp_inventory/xde-home/inventoryDefaults/ncsCIMC.def* ファイルに次の行を追加します。

```
<default attribute="HTTPS_TRUST_CONDITION">always</default>

<default attribute="HTTPS_HOSTNAME_VERIFICATION_STRATEGY">allow_all</default>
```

（注） 各デバイスには、一意の SNMP エンジン ID が必要です。同じエンジン ID が 2 つのデバイスで使用されている場合、競合するデバイスの詳細でアラームが発生します。SNMP v3 ログイン情報でデバイスを管理する場合にのみ、SNMP エンジン ID の一意のチェックが行われます。

例：単一の Cisco NCS 2000 または NCS 4000 シリーズ デバイスの追加

Cisco NCS 2000 シリーズは TL1 ベースのデバイスであり、Cisco EPN Manager は TL1 プロトコルを使用してこれらのデバイスと通信します。NCS2K デバイスの推奨 TL1 アクティブセッションの数は 15 以下です。アクティブセッションの数が 15 を超えると、Cisco EPN Manager では詳細または事後対応型のインベントリ操作でデバイスから TL1 イベントを受信できなくなる場合があります。一方、Cisco NCS 4000 シリーズのデバイスは Cisco IOS XR デバイスであり、Cisco EPN Manager は SNMP および Telnet/SSH プロトコルを使用してこれらのデバイスと通信します。

始める前に

Cisco NCS デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニターできるように設定する （69 ページ）を確認してください。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [デバイスの追加（Add Device）] ダイアログボックスで、必須フィールドに値を入力します。フィールドの横にある [?] をクリックすると、そのフィールドの説明が表示されます。

- Cisco NCS 2000 シリーズおよび Cisco ONS 15454：TL1 パラメータを入力します
- Cisco NCS 4000 シリーズ：SNMP および Telnet/SSH のパラメータを入力します。

ステップ 4 [クレデンシャルの確認（Verify Credentials）] をクリックして Cisco EPN Manager がデバイスに到達できることを検証します。

ステップ 5 [追加（Add）] をクリックして、デバイスを Cisco EPN Manager に追加します。

例：プロキシ設定を使用した ENE としてのネットワーク要素の追加

特定のネットワーク要素に送信したメッセージは、ネットワーク内の他の NE を通過する必要があります。メッセージを渡すには、1 つ以上のノードがゲートウェイ ネットワーク要素（GNE）となり、ネットワーク内の他の NE に接続することができます。TL1 セッションを確立して別のノードに送信する必要があるコマンドを入力すると、ノードは GNE になります。別のノードから処理のために TL1 メッセージを受け取るノードがエンドポイント ネットワーク要素（ENE）です。ENE からのメッセージは、GNE を通じてネットワーク内の別の NE に送信されます。

始める前に

デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニターできるように設定する （69 ページ）を確認してください。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある＋アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [デバイスの追加（Add Device）] ダイアログ ボックスで、追加する ENE の IP アドレスまたは DNS 名を [一般パラメータ（General Parameters）] の下に入力します。そのフィールドの説明を確認するには、フォールドの横にある [?] をクリックします。

ステップ 4 **[TL1パラメータ（TL1 Parameters）]** に、ENE として使用するノードのプライマリおよびセカンダリ プロキシ IP アドレスを入力します。

（注） セカンダリ プロキシ IP アドレスは任意であり、プライマリ プロキシに障害が発生した場合にのみアクティブ化されます。

ステップ 5 [クレデンシャルの確認（Verify Credentials）] をクリックして Cisco EPN Manager がデバイスに接続できないことを検証します。

ステップ 6 [追加（Add）] をクリックして、デバイスを Cisco EPN Manager に追加します。

例：Cisco NCS 2000 シリーズ デバイスでシングル セッションを有効にする

Cisco NCS 2000 シリーズのデバイスは TL1-ベースのデバイスであり、Cisco EPN Manager は TL1 プロトコルを使用してこれらのデバイスと通信します。新しく追加されたデバイスを編集するか、既存の NCS 2000 デバイスを設定して、シングル セッションでマシン（EMS）アカウントを制限できます。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 デバイスを選択して [編集（Edit）] アイコンをクリックします。[デバイスの編集（Edit Device）] ウィンドウが表示されます。

ステップ 3 新しいデバイスまたは既存のデバイスでシングルセッションを編集するには、次のパラメータを設定します。

a) [TL1 パラメータ（TL1 Parameters）] の下にある [シングルセッション TL1 を有効にする（Enable Single Session TL1）] チェックボックスをオンにします。

b) 必須パラメータを入力します。

c) 次のいずれかを実行します。

- データベース上のシングル セッション設定のみを更新する場合は、[更新（Update）] をクリックします。
- データベースとデバイスの両方でシングルセッション設定を更新する場合は、[更新と同期（Update & Sync）] をクリックします。

ステップ 4 （オプション）一括インポート操作および一括編集操作でシングル セッションを編集することもできます。

（注） デフォルトにより、一括編集ではシングルセッションが無効になっています。[シングルセッションTL1を有効にする（Enable Single Session TL1）] チェック ボックスをオンにして、インポート先のすべてのデバイスに対して有効にする必要があります。[一括インポート（Bulk Import）] オプションを選択すると、シングル セッション フラグが影響を受ける可能性があります。

次のタスク

次の手順で有効なシングル セッションを確認します。

1. Cisco Transport Controller を起動し、シングル セッションが有効になっているデバイスを選択します。
2. **[プロビジョニング（Provisioning）] > [セキュリティ（Security）] > [アクティブログイン（Active Logins）]** を選択して、シングルセッションを含むアクティブデバイスをすべて表示します。シングル セッションが無効になっているデバイスは表示されません。

（注） クレデンシャルの確認は、シングル セッション タスク実行中の唯一の例外です。

デバイス通信用の強力な SSH の確立

より安全な SSH 接続でデバイスに接続するには、次の手順を実行します。

ステップ 1 SSH を使用してサーバーに接続し、管理者ユーザーとしてログインします。詳細については、「Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）」を参照してください。

ステップ 2 `/opt/CSCOlumos/xmp_inventory/xde-home/conf/` ディレクトリに移動します。

ステップ 3 `sampleTransportProperties.xml` ファイルの名前を同じディレクトリ内で `transportProperties.xml` に変更します。これにより、デバイスへの接続時に Cisco EPN Manager はより強力な暗号を使用できます。

次のタスク

Cisco EPN Manager の再起動Cisco EPN Manager の停止と再起動 （973 ページ）を参照してください。

（注） 以前の接続に戻すには、`transportProperties.xml` ファイルの名前を `sampleTransportProperties.xml` に変更し、Cisco EPN Manager を再起動します。

SVO デバイスの追加

SVO は、マルチシャーシ動作をサポートするソリューションです。SVO デバイスは、1 つの NCS2k ROADM および 50 の NCS2k OLA インスタンスをサポートできます。SVO デバイスでは、Cisco EPN Manager は管理対象プレーンのプロビジョニングに移行します。12.0.1 以降、Cisco EPN Manager は Netconf を使用して SVO インスタンスと通信します。

始める前に

Cisco NCS デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニターできるように設定する （69 ページ）を確認してください。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]**の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [デバイスの追加（Add Device）] ダイアログボックスで、必須フィールドに値を入力します。

a) [一般（General）] セクションの [IPアドレス（IP Address）] に入力します。
b) [Telnet/SSH] セクションの [プロトコル（Protocol）] ドロップダウンリストから [Netconf Over SSH2] を選択します。
c) [ユーザー名（Username）]、[パスワード（Password）]、および[パスワードの確認（Confirm Password）] を入力します。
d) [クレデンシャルの確認（Verify Credentials）] をクリックして Cisco EPN Manager がデバイスに到達できることを検証します。

ステップ 4 [追加（Add）] をクリックして、デバイスを Cisco EPN Manager に追加します。

このデバイスの **[デバイス名（Device Name）]** ハイパーリンクをクリックすると、 SSO が設定されている場合は、このデバイスの詳細を表示および管理するための SVO ノードクラフト Web UI が開きます。SSO が設定されていない場合は、SVO ノードクラフト Web UI でログイン情報を入力する必要があります。Cisco

EPN Manager から SVO ノードクラフト Web UI への SSO を有効にするには、Cisco EPN Manager から SVO UI へのシングルサインオン（SSO）を有効にする （66 ページ）を参照してください。

デバイスの一括インポートを実行することもできます。

次のタスク

- OCHCC および OCH-Trail 回線を作成してプロビジョニングするには、OCH 回線の作成とプロビジョング （668 ページ）を参照してください。
- 基盤となる NCS2K ノードから PM データをポーリングして収集するには、SVO デバイスでパフォーマンス収集を有効にする必要があります。これは、1 つ以上のデバイスの CLI テンプレートを使用して有効または無効にできます。

[デバイス360（Device 360）] ビュー - SVO

SVO デバイスの [デバイス360（Device 360）] ビューが提供する情報は次のとおりです。

[デバイス 360（Device 360）] ビューで提供される情報	説明

一般情報とツール	デバイス タイプ、その OS タイプとバージョン、その最新の設定変更、およびその最新のインベントリ収集。アイコンは、デバイスのステータスを示しています。 ポップアップウィンドウのメニューを使用して、次のタスクを実行できます。 • [自動更新（Auto-Refresh）] : デバイスのステータスとトラブルシューティングをリアルタイムで更新する場合は、[更新（Refresh）] アイコンをクリックしてオンデマンド更新を有効にします。または、ドロップダウンリストから、自動更新の間隔を 30 秒、1 分、2 分、または 5 分に設定することもできます。デフォルトでは、自動更新はオフになっています。 （注） 自動更新設定は、現在開いている [360° ビュー（360° View）] ポップアップウィンドウにのみ適用されます。このビューを閉じてからもう一度開いた場合または別のビューを開いた場合は、デフォルトでは自動更新がオフになります。 • [デバイスの詳細（Order Details）] ページを開いてソフトウェアイメージと構成ファイルの管理に関する詳細を表示します（**[表示（View）] > [詳細（Details）]**）。 • SVO Nodal クラフト UI で [デバイス設定（Device Configuration）] ページを開き、**[ビュー（View）] > [シャーシビュー（Chassis View）]**を選択して、デバイスの設定変更を実行します。 • 発生したアラームや回線、インターフェイス、およびモジュールの現在のステータスなどの情報に基づいて別のデバイスと対照比較するためのデバイスを選択します（[アクション（Actions）] メニュー）。デバイスの情報とステータスを比較する （111 ページ） を参照してください • トラブルシュート : ping またはトレースルートを実行して、アラーム ブラウザを起動し、シスコ サポート ケースを開くか、シスコ サポート コミュニティから情報を取得します（[アクション（Actions）] メニュー）。 • トポロジ : ネットワーク トポロジとデバイスのローカル トポロジを最大 3 ホップまで表示します（[アクション（Actions）] メニュー）。 • [今すぐ同期（Sync Now）]、[同期と再ビルド（Sync and Rebuild）] を使用して、デバイスのインベントリを収集し、データベースに保存します（[アクション（Actions）] メニュー）。

[アラーム（Alarms）] タブ	重大度、ステータス、および収集時刻を含む、デバイスの現在のアラーム。
[モジュール（Modules）] タブ	名前、タイプ、状態、ポート、および場所を含む、デバイス上で設定されたモジュール。
[インターフェイス（Interfaces）] タブ	ステータス情報を含む、デバイス上で設定されたインターフェイス。また、特定のインターフェイス用の [インターフェイス 360（Interface 360）] ビューを起動することもできます。
[ネイバー（Neighbors）] タブ	Cisco Discovery Protocol（CDP）経由でこのデバイスに接続している NE。選択されたデバイスで CDP がサポートされていない場合は、このタブには何も表示されません。表示される情報には、デバイス タイプ、デバイス名、ローカル ポート、およびデバイス ポートが含まれます。ポップアップトポロジマップにネイバーを表示するには、[デバイス 360° ビュー（Device 360 View）] の右上で [アクション（Actions）]>[Nホップトポロジ（N Hop Topology）] を選択します（デバイス 360 ビューからデバイスのローカル トポロジを表示する （112 ページ）を参照）。
[回路/VC（Circuit/VCs）] タブ	デバイス上でプロビジョニングされた各回線の回線/VC 名、タイプ、顧客、ステータス、および作成日。また、特定の回線/VC 用の [回線/VC 360（Circuit/VC 360）] ビューを起動することもできます。
シビック ロケーション	デバイスの位置に関する地理的情報。
最近の変更	デバイス上で行われた最新の 5 つの変更。インベントリ、設定（設定アーカイブ）、または SWIM（ソフトウェアイメージ）に分類されます（これらは、**[インベントリ（Inventory）]>[ネットワーク監査（Network Audit）]** を選択したときに表示されるものと同じタイプの変更です）。 （注） ルートユーザーとしてログインしている場合は、[最近の変更（Recent Changes）] タブですべてのアクティビティを表示できます。非ルートユーザーとしてログインしている場合は、自分が実行したアクティビティのみを表示できます。

また、**[アクション（Actions）]>[ネットワークトポロジ（Network Topology）]**（[デバイス360（Device 360）] ビューの右上にある）を選択することにより、トポロジマップに特定のデバイスを表示することもできます。

SVO UI の概要

SVO のさまざまなセクションとそれぞれのタブの詳細を次に示します。

表 *6 : SVO UI* の詳細

セクション	詳細
SVO トポロジ	このセクションには、デバイスのトポロジビューが表示されます。
障害モニターリング	このセクションには、アラーム、条件、履歴、およびプロファイルが表示されます。アラーム、条件、および履歴の詳細をエクスポートできます。アラームプロファイルのロード、アラームの関連付け、およびアラームリソースの管理もできます。
デバイス設定	このセクションでは、認証グループ、デバイス、および診断を管理できます。IPv4 設定を構成し、デバイス設定を適用することもできます。
ノード設定	このセクションの各タブで実行できるアクションの詳細を次に示します。 • 光設定：内部パッチコード、接続検証、光度、ファイバ属性、OSC 終端、GCC 終端、光度パワーモニターリング、APC を管理し、スパン損失データを測定およびエクスポートできます。 • ANS パラメータ：増幅器、インターフェイス、ラマン増幅器、およびラマンインターフェイスの詳細のエクスポートを表示できます。 • 光クロス接続：光クロス接続データを表示およびエクスポートできます。 • OTDR：OTDR プロビジョニングとトレースを管理できます。 • XML 設定：XML 設定ファイルを選択し、そこから設定をロードできます。
SVO の設定	このセクションでは、SVO の日時を設定できます。SVO およびシステムログを取得してダウンロードすることもできます。
データベース	このセクションには、データベースの詳細が表示されます。
ソフトウェア マネージャ	このセクションでは、SVOおよびデバイス ソフトウェア パッケージをダウンロードして管理できます。
インベントリ	このセクションでは、インベントリデータを表示およびエクスポートできます。

セクション	詳細
ユーザーの設定	このセクションは、ユーザーの管理、SSO 設定とユーザーの管理、および RADIUS 設定の管理に役立ちます。

必要に応じて、SVO デバイスの [デバイス名（Device Name）] ハイパーリンクをクリックすると、SVO ウィンドウにデバイスの詳細が表示されます。[シャーシ（Chassis）] ビューでは、カードを選択して、[カードを開く（Open Card）]、[削除（Delete）]、[ソフトリセット（Soft Reset）]、[ハードリセット（Hard Reset）]、[OBFL]、および [管理状態の変更（Change Admin State）] アクションを実行できます。選択したカードについて、[カードを開く（Open Card）] を選択し、それぞれのタブで [アラーム（Alarms）]、[条件（Conditions）]、[履歴（History）]、[保守（Maintenance）]、および [パフォーマンスの詳細（Performance Details）] を表示できます。[プロビジョニング（Provisioning）] タブをクリックして、選択したカードのプラグイン可能なポートモジュール、カードモード、プラグ可能なポート、トレイル トレース モニターリング、ODU インターフェイス、OTU インターフェイス、イーサネット インターフェイス、光チャネル、光しきい値、G709 しきい値、FEC しきい値、UDC、および RMON しきい値を追加できます。完了すると、EPNM の [デバイス360（Device 360）] および [インターフェイス360（Interface 360）] ビューにそれぞれの変更が表示されます。

Cisco EPN Manager から SVO UI へのシングルサインオン（SSO）を有効にする

Cisco EPN Manager から SVO UI へのシングルサインオン（SSO）を有効にするには、次の手順を実行します。

ステップ 1 SVO UI にログインします。

ステップ 2 **[メニュー（Menu）]** から **[アクセス設定（Access Configuration）]** に移動し、**[SSO]** タブをクリックします。

ステップ 3 [SSO設定（SSO Configuration）] エリアで、[SSOを有効にする（Enable SSO）] チェックボックスをオンにします。

ステップ 4 SVO UI を相互起動する Cisco EPN Manager サーバーの **IP アドレス**と**ポート**の詳細を入力し、**[適用（Apply）]** をクリックします。

ステップ 5 [SSO] で、**[+]** をクリックしてユーザー名を追加します。適切なロールをユーザーに割り当て、[適用（Apply）] をクリックします。

既存の NCS2K ベースのネットワークの移行

[光回線/VC移行（Optical Circuits / VCs Migrator）] ウィンドウを使用して、既存の NCS2K ベースのネットワークを移行できます。

一度に最大 20 回線を移行できます。

（注）
- OCH-Trail の移行では、OTU3、OTU2、OTU2E、OTU4、OTU4C2 がサポートされます。
- OCH-CC の移行では、100G、10G、40G がサポートされます。

既存の NCS2K ベースのネットワークを移行するには、次の手順を実行します。

始める前に

- NCS2K ノードを 12.3 にアップグレードし、SVO カードを装備する必要があります。
- NCS2K ノードと SVO ノードの両方を EPNM でモデル化し、異なるユーザー定義済みグループに追加する必要があります。
- NCS2K ノードと SVO ノードは同期している必要があります。
- EPNM サーバーで NCS2K ノードと SVO ノードの両方を同期します。
- EPNM で NCS2K デバイスと SVO デバイスをメンテナンス状態に移行します。
- EPNM からの移行用に設定された回線を変更しないでください。

ステップ 1 [インベントリ（Inventory）]>[その他（Other）] に移動し、[光回線/VC移行（Optical Circuits / VCs Migrator）] を選択します。

[光回線/VC移行（Optical Circuits / VCs Migrator）] ページが表示され、移行可能な回線名のリストが表示されます。

ステップ 2 移行する回線名を選択します。

回線の移行ステータスは、[移行なし（Not Migrationd）] と表示されます。

ステップ 3 [回線の移行（Migrate Circuits）] をクリックします。

移行が完了すると、回線の移行ステータスが [成功（Success）] に変わります。このページが更新されると、移行された回線名が削除されます。

次のタスク

[ネットワークトポロジ（Network Topology）] ページを確認します。移行された回線の名前が 2 回表示されます。両方の回線の [回線/VC 360（Circuit/VC 360）] ビューで回線の詳細を確認します。移行された回線には、すべての詳細（アラーム、エンドポイント、履歴、および関連する回線/VC）が含まれます。もう一方の回線は、レガシーという単語で置き換えられた回線タイプを示し、関連する詳細はありません。これらのデバイスは、[ネットワークデバイス（Network Devices）] ページから削除できます。移行した回線は、必要に応じて変更および削除できます。2つのユーザー定義グループでモデル化すると、回路をフィルタリングしてチェックすることができます。重複する回路は表示されません。

インベントリはどのように収集されていますか。

デバイスが追加されて検出されると、Cisco EPN Manager は物理的および論理的なインベントリ情報を収集し、データベースに保存します。次の表に、インベントリ収集がどのようにトリガーされるかについて示します。

インベントリ収集のトリガー	説明
着信イベントに応答して	Cisco EPN Manager は、NE の変更を通知する着信 NE SNMP トラップ、syslog、または TL1 メッセージを受信します。着信イベントには、次のようなものがあります。 • デバイス設定の変更を通知する設定変更イベント。これらのイベントは通常、syslog またはトラップです。 • その他のインベントリ イベント（トンネルのアップ/ダウン、リンクのアップ/ダウン、モジュールの入出力など）。 Cisco EPN Manager は、NE のインベントリと状態情報を収集して、データベース内の情報が NE の情報に準拠していることを確認することによって、これらの着信イベントに反応します。ほとんどのイベントは、詳細なインベントリ収集をトリガーします。Cisco EPN Manager は、変更イベントに関連するデータのみを収集します。その他のイベントは、NE の物理および論理インベントリの完全な収集（同期）をトリガーします。Cisco EPN Manager が収集するデータは、Cisco EPN Manager で定義されているメタデータとともに、着信イベントの情報によって決まります。Cisco EPN Manager のメタデータは、収集される情報を細かく調整するために、迅速なイベント、反応的なインベントリ、詳細なポーリングといったメカニズムを組み合わせて使用します。 たとえば、Cisco EPN Manager が GMPLS トンネル状態変更イベントを受信した場合は、ODU トンネル インベントリ情報を収集して、トンネルのミッドポイントと Z エンドポイントを検出します。
オン デマンド	ユーザーは、次の場所から即時にインベントリ収集（[同期（Sync）] と呼ばれる）を実行できます。 • [ネットワーク デバイス（Network Devices）] ページ：（チェックボックスをオンにして）1 つ以上のデバイスを選択し、[同期（Sync）] をクリックします。 • [デバイス 360（Device 360）] ビュー：**[アクション（Actions）]** > **[今すぐ同期（Sync Now）]** を選択します。 デバイスのインベントリの即時収集（同期） （570 ページ）を参照してください。

インベントリ収集のトリガー	説明
スケジュール（日単位）	通常のインベントリ収集は一晩中実行されます。十分な権限を持つユーザーは、**[管理（Administration）]>[ダッシュボード（Dashboards）]>[ジョブダッシュボード（Job Dashboard）]** を選択し、[システム ジョブ（System Jobs）]>[インベントリおよびディスカバリ ジョブ（Inventory and Discovery Jobs）] を選択して、インベントリが収集された日時と収集ジョブの状況を確認できます。

デバイスをモデル化してモニターできるように設定する

（注） 異なるデバイス ファミリのサポート対象の構成については、『Cisco Evolved Programmable Network Manager のサポート対象デバイス』を参照してください。

デバイスが Cisco EPN Manager で完全なユーザー権限（特権 EXEC モード）で管理されていることを確認します。

にイベントを転送するようにデバイスを設定する Cisco EPN Manager

Cisco EPN Manager がデバイスに問い合わせてイベントと通知を受信できるようにするには、イベントを Cisco EPN Manager サーバーに転送するようにデバイスを設定する必要があります。ほとんどのデバイスにとって、これは SNMP トラップと syslog を転送するように設定する必要があることを意味します。

それ以外のデバイス（一部の光デバイスなど）の場合は、TL1 メッセージを転送するようにデバイスを設定する必要があることを意味します。

ハイ アベイラビリティ展開を使用している場合は、イベントをプライマリ サーバーとセカンダリ サーバーの両方に転送するようにデバイスを設定する必要があります（仮想 IP アドレスを使用していない場合。HA での仮想 IP アドレッシングの使用 （1117 ページ）を参照）。

ほとんどの場合、この設定を行うには **snmp-server host** コマンドを使用する必要があります。さまざまなデバイスのオペレーティングシステムの前提条件が一覧表示された本書内のトピックを参照してください。

（注） デバイスで詳細なインベントリを有効にするために必要な設定については、Cisco Evolved Programmable Network Manager のサポート対象 Syslogを参照してください

必要な設定：Cisco IOS および IOS-XE デバイス オペレーティング システム

```
snmp-server host
snmp-server community public-cmty RO
snmp-server community private-cmty RW
snmp-server ifindex persist

logging server_IP
logging on
logging buffered 64000 informational

logging source-interface interface_name
logging trap informational
logging event link-status default
```

Telnet/SSH コマンド応答の遅延を回避するために、ドメイン ルックアップを無効にします。

```
no ip domain-lookup
```

SSH の有効化

```
crypto key generate rsa
ip ssh rsa keypair-name keypair-name
crypto key generate rsa usage-keys label key-label modulus modulus-size
ip ssh version [1 | 2]
```

VTY オプションを設定します。

```
line vty <number of vty>
exec-timeout
session-timeout
transport input ssh (requird only if ssh is used)
transport output ssh (required only if ssh isused)
```

CFM モデリングを有効にします。

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

SNMPv2 の場合のみ、コミュニティ ストリングを設定します。

```
snmp-server community ReadonlyCommunityName RO
```

SNMPv3 の場合のみ、次の設定を行います。

```
snmp-server user User Group v3 auth sha Password priv des Password
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group

snmp-server group Group v3 priv read v1default write v1default notify v1default
snmp-server group Group v3 priv
snmp-server group Group v3 priv notify epnm read epnm
```

（注）
- デバイスが Cisco EPN Manager でシームレスに動作するには、デバイスで生成/設定された SNMP EngineID がネットワーク内で一意である必要があります。
- クレデンシャルが機能するように、SNMP EngineID をデバイスで再設定する場合は SNMP ユーザーを再作成する必要があります。

SNMPインターフェイスの応答時間を改善するために、次の設定を使用してグローバル レベルでキャッシュを設定します。

```
snmp-server cache
```

syslog は、アラームおよびイベント管理のために Cisco EPN Manager によって使用されます。NTP 設定により、Cisco EPN Managerはイベントの正しいタイムスタンプを確実に受信します。デバイスで syslog を設定するには、次の設定を追加します。

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging Server_IP vrf default severity info [port default]
```

必須の設定：Cisco IOS XR デバイスのオペレーティング システム

```
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist

logging server_IP
logging on
logging buffered <307200-125000000>

logging source-interface interface_name

logging trap informational
logging events level informational
logging events link-status
logging events link-status software-interfaces

no cli whitespace completion
domain ipv4 host server_name server_IP
```

VTY オプションを設定します。

```
line default
exec-timeout 10 0
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

Telnet と SSH の設定は次のとおりです。

```
telnet ipv4 server max-servers no-limit
telnet vrf default ipv4 server max-servers 100
ssh server v2
ssh server rate-limit 60
cinetd rate-limit 60
```

Netconf エージェントと XML エージェントを設定します。

```
xml agent tty
netconf agent tty
```

仮想 IP アドレスを持つデバイスをモニターします。

```
ipv4 virtual address use-as-src-addr
ipv4 virtual address Virtual_IP_Address/Subnet_Mask
```

CFM モデリングを有効にします。

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

SNMPv2 の場合のみ、コミュニティ ストリングを設定します。

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

SNMPv3 の場合のみ、次の設定を行います。

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group
snmp-server group Group v3 priv read v1default write v1default notify v1default
```

（注） または、**[設定（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** に移動できます。左側の [テンプレート（Templates）] タブで **[CLIテンプレート（CLI Templates）]** > **[システムテンプレート - CLI（System Templates - CLI）]** を選択し、Default_Manageability_Config-IOS-XR テンプレートを展開して Cisco EPN Manager のディスカバリに必要な IOS-XR デバイス設定を行います。

（注）

- デバイスが Cisco EPN Manager でシームレスに動作するには、デバイスで生成/設定された SNMP EngineID がネットワーク内で一意である必要があります。
- クレデンシャルが機能するように、SNMP EngineID をデバイスで再設定する場合は SNMP ユーザーを再作成する必要があります。

次の設定を行って、SNMP インターフェイス統計情報の応答時間を改善します。

```
snmp-server ifmib stats cache
```

リンクダウン シナリオが確実にキャプチャされるように、仮想インターフェイスの SNMP トラップを設定します。

```
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression TwoHun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression FourHun*
notification linkupdown
```

SNMP のエンティティ現場交換可能ユニット（FRU）制御トラップを有効にします。

```
snmp-server traps fru-ctrl
```

syslog は、アラームおよびイベント管理のために Cisco EPN Manager によって使用されます。NTP の設定によって、Cisco EPN Manager がイベントの正しいタイムスタンプを確実に受信します。デバイスで syslog を設定するには、次の設定を追加します。

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging server_IP vrf name
```

すべての光データ ユニット（ODU）コントローラでパフォーマンス管理を有効にします。

```
controller oduX R/S/I/P
per-mon enable
```

タンデム接続モニターリング（TCM）のパフォーマンス管理を有効にします。

```
tcm id {1-6}
perf-mon enable
```

Cisco EPN Manager から Cisco Transport Controller（CTC）を開くには、HTTP/HTTPS サーバーを有効化します。

```
http server ssl
```

[設定アーカイブ（Configuration Archive）] の使用を予定している場合は、デバイスをセキュアデバイスとして設定する必要があります。CTC からデバイスを設定する手順は次のとおりです。

1. **[プロビジョニング（Provisioning）]** > **[セキュリティ（Security）]** > **[アクセス（Access）]** を選択します。
2. [EMSアクセス（EMS Access）] を [セキュア（secure）] に設定します。

（注）

- MPLS パッケージと K9 パッケージの両方がデバイスにインストールされていることを確認してください。
- Cisco IOS XR Manageability Package（MGBL）をインストールしてください。
- または、CLI テンプレートを使用して上記の前提条件をすべて適用することもできます。**[設定（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** に移動します。左ペインの [テンプレート（Templates）] タブで、**[CLIテンプレート（CLI Templates）]** > **[システムテンプレート - CLI（System Templates - CLI）]** を選択し、**Default_Manageability_Config** テンプレートを展開します。
- 詳細については、『Supported Traps』と『Supported Syslogs』を参照してください。.

必須設定：Cisco NCS シリーズ デバイス

SR ポリシーについて、選択したデバイスで次の構成時の設定を適用します。

- ポリシーステータスのロギングのイベントを有効にする構成：

```
segment-routing
traffic-eng
logging policy status
```

- 必須設定：Cisco NCS 4000 シリーズ デバイス （74 ページ）
- 必須設定：Cisco NCS 4200 シリーズ デバイス （77 ページ）

必須設定：Cisco NCS 4000 シリーズ デバイス

注目 次の手順を実行する前に、MPLS パッケージと K9 パッケージの両方がデバイスにインストールされていることを確認してください。

- Cisco EPN Manager は SSH を使用して、Cisco NCS 4000 シリーズ デバイスとの通信を保護します。SSH を有効にするには、デバイスで次の構成時の設定を適用します。

```
ssh server v2
ssh server rate-limit 600
```

- MPLS トラフィック エンジニアリング設定モードで、イベント ロギングを有効化します。

```
mpls traffic-eng logging events all
```

- VTY オプションを設定します。

```
line default
exec-timeout 10 0
session-limit 10
```

```
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

- LMP リンクを設定します。

```
router-id ipv4 unicast local IP address
```

local IP address はデバイスの IP アドレスです。

- Netconf エージェントと XML エージェントを設定します。

```
xml agent tty
netconf agent tty
```

- デバイスで SNMP を設定します。

```
snmp-server host server_IP
snmp-server community public RO SystemOwner
snmp-server community private RW SystemOwner
snmp-server ifindex persist
```

SNMPv2 または SNMPv3 を使用できます。

- SNMPv2 の場合のみ、コミュニティ ストリングを設定します。

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

- SNMPv3 の場合のみ、次の設定を行います。

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
 Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server group Group v3 priv notify Group read Group
```

ポーリングおよび設定ビューを設定するには、次のいずれかの設定オプションを選択します。

- SNMPv3 のデフォルト設定（SNMPv3 のポーリングとデフォルト設定の表示に使用）：

```
snmp-server group Group v3 priv read v1default write v1default notify
v1default
```

- SNMPv3 固有の設定：
  - SNMPv3 ポーリングの場合のみ：

```
snmp-server group Group v3 priv
```

  - SNMPv3 セット、ポーリング、およびトラップ/通知の設定を表示する場合：

```
snmp-server group Group v3 priv notify epnm read epnm write epnm
```

  - SNMPv3：LLDP MIB OID 設定を表示する場合：

```
snmp-server view Group 1.0.8802.1.1.2 included
```

LAG リンクを表示するには、デバイスに次の設定を追加します。

```
snmp-server view all 1.0.8802 included
```

（注） 最初の行の *User* と *Group* は、値を入力する必要がある 2 つの異なる変数です。

- 設定 `Snmp-server ifmib stats cache` を使用して、SNMP インターフェイスの統計情報の応答時間を改善するように stats コマンドを設定します。
- リンクダウン シナリオが確実にキャプチャされるように、仮想インターフェイスの SNMP トラップを設定します。

```
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
```

- syslog は、アラームおよびイベント管理のために Cisco EPN Manager によって使用されます。NTP の設定によって、Cisco EPN Manager がイベントの正しいタイムスタンプを確実に受信します。デバイスで syslog を設定するには、次の設定を追加します。

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging server_IP vrf name
```

次の点に注意してください。

  - タイムゾーンを指定するときには、タイムゾーンの略語と協定世界時（UTC）との時間差（時間単位）を入力します。たとえば、ロサンゼルスにあるデバイスのタイムゾーンを指定するには、`clock timezone PDT -7` と入力します。
  - *server_IP* を、Cisco EPN Manager がインストールされているホストの IP アドレスに置き換えます。

- 仮想 IP アドレスを設定します。

```
ipv4 virtual address NCS4K_Virtual_IP_Address/Subnet_Mask
ipv4 virtual address use-as-src-addr
```

（注） *NCS4K_Virtual_IP_Address* と *Subnet_Mask* は、スラッシュで区切られた 2 つの異なる変数です。必ず両方の変数値を入力してください。

- すべての光データ ユニット（ODU）コントローラでパフォーマンス管理を有効にします。

```
controller oduX R/S/I/P
per-mon enable
```

- Cisco IOS リリース 6.1.42 以降を実行している Cisco NCS4000 デバイスの光学コントローラのリンク ステータス メッセージのイベント ロギングを有効にします。

```
controller Optics <x/y/z/w>
logging events link-status
```

- タンデム接続モニターリング（TCM）のパフォーマンス管理を有効にします。

```
tcm id {1-6}
perf-mon enable
```

- サービス要求を受け入れるための Telnet または SSH レート制限を設定します。
  - Telnet の場合、1 秒あたりに受け付ける要求の数（1 ～ 100、デフォルトは 1）を設定します。

    ```
    cinetd rate-limit 100
    ```

  - SSH の場合、1 分あたりに受け付ける要求の数（1 ～ 600、デフォルトは 60）を設定します。

    ```
    ssh server rate-limit 600
    ```

- Cisco EPN Manager（[デバイス 360（Device 360）] ビュー）から Cisco Transport Controller（CTC）を開くには、HTTP/HTTPS サーバーを有効化します。

```
http server ssl
```

- [設定アーカイブ（Configuration Archive）] 機能を使用する予定の場合は、デバイスを [保護済み（secured）] として設定する必要があります。これを CTC から行うには、次のようにします。
  1. **[プロビジョニング（Provisioning）] > [セキュリティ（Security）] > [アクセス（Access）]** を選択します。
  2. EMS アクセスを [セキュア（secure）] に設定します。

- 複数の Cisco NCS 4000 シリーズ デバイスが同時に情報を送信していることが原因でパフォーマンス上の問題が発生した場合は、*1* 秒あたりの Telnet セッション数を増やします。

```
cinetd rate-limit 100
```

必須設定：Cisco NCS 4200 シリーズ デバイス

- Cisco EPN Manager は SSH を使用して、Cisco NCS 4200 シリーズ デバイスとの通信を保護します。SSH を有効にするには、デバイスで次の構成時の設定を適用します。
  - ```
    enable
    configure terminal
    hostname name
    ip domain-name name
    crypto key generate rsa
    ```
  - ```
    enable
    configure terminal
    ip ssh rsa keypair-name keypair-name
    ```

```
crypto key generate rsa usage-keys label key-label modulus modulus-size
ip ssh version [1 | 2]
```

- VTY オプションを設定します。

```
line vty <#>
exec-timeout
session-timeout
transport input ssh
transport output ssh
```

- デバイスで SNMP を設定します。

```
snmp-server host server_IP
snmp-server community public RO
snmp-server community private RW
```

SNMPv2 または SNMPv3 を使用できます。

- SNMPv2 の場合のみ、コミュニティ ストリングを設定します。

```
snmp-server community ReadonlyCommunityName RO
```

- SNMPv3 の場合のみ、次の設定を行います。

```
snmp-server user User Group v3 auth sha Password priv des  Password
snmp-server view Group 1.3.6 included
snmp-server group Group v3 priv notify Group
```

ポーリングおよび設定ビューを設定するには、次のいずれかの設定オプションを選択します。

- SNMPv3 のデフォルト設定（SNMPv3 のポーリングとデフォルト設定の表示に使用）：

```
snmp-server group Group v3 priv read v1default write v1default notify
v1default
```

- SNMPv3 固有の設定：
  - SNMPv3 ポーリングの場合のみ：

```
snmp-server group Group v3 priv
```

  - SNMPv3 セット、ポーリング、およびトラップ/通知の設定を表示する場合：

```
snmp-server group Group v3 priv notify epnm read epnm
```

  - SNMPv3：LLDP MIB OID 設定を表示する場合：

```
snmp-server view Group 1.0.8802.1.1.2 included
```

（注） 最初の行の *User* と *Group* は、値を入力する必要がある 2 つの異なる変数です。

- 構成 `Snmp-server cache` を使用して SNMP インターフェイスの応答時間を改善するためにグローバル レベルでキャッシュを設定します。

- syslog は、アラームおよびイベント管理のために Cisco EPN Manager によって使用されます。NTP の設定によって、Cisco EPN Manager がイベントの正しいタイムスタンプを確実に受信します。デバイスで syslog を設定するには、次の設定を追加します。

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging server_IP vrf default severity info [port default]
mpls traffic-eng logging lsp setups
mpls traffic-eng logging lsp teardowns
```

次の点に注意してください。

- タイムゾーンを指定するときには、タイムゾーンの略語と協定世界時（UTC）との時間差（時間単位）を入力します。たとえば、ロサンゼルスにあるデバイスのタイムゾーンを指定するには、`clock timezone PDT -7` と入力します。
- *server_IP* を、Cisco EPN Manager がインストールされているホストの IP アドレスに置き換えます。

必須設定：Cisco ASR シリーズ デバイス

SR ポリシーについて、選択したデバイスで次の構成時の設定を適用します。

- ポリシーステータスのロギングのイベントを有効にする構成：

```
segment-routing
traffic-eng
logging policy status
```

必要とされる設定の自動プッシュ

新しいデバイス（IOS、IOS-XE、および IOS-XR）がインベントリに追加されたときに、必須のデバイス管理性設定を自動的に適用できます。これにより、Cisco EPN Manager がデバイスを自動的に管理できるようになり、収集の一部が失敗するというインシデントの割合が減少し、デバイスに手動で設定を適用する必要がなくなります。Cisco EPN Manager デバイスの管理性の必須設定は、事前設定されたテンプレートにまとめられています。このテンプレートはデバイス管理性テンプレートとも呼ばれます。

（注） デバイス管理性テンプレートは、既存の設定が存在する場合にそれを上書きします。

テンプレートをデバイスに自動的に展開するには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[インベントリ（Inventory）]** > **[インベントリ（Inventory）]** を選択し、[デバイス管理性を有効にする（Enable Device Manageability）] チェックボックスをオンにします。デフォルトで、このオプションは有効になっています。こ

のオプションを有効にすると、追加されたデバイスのタイプに基づいて、デバイスの追加時に次のテンプレートのいずれかが展開されます（たとえば、XR デバイスを追加した場合は *AutoDeploy_Manageability_Config-IOS-XR* テンプレートが展開されます）。

- AutoDeploy_Manageability_Config-IOS
- AutoDeploy_Manageability_Config-IOS-XE
- AutoDeploy_Manageability_Config-IOS-XR

これらのテンプレートは **[設定（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** > **[CLIテンプレート（CLI Templates）]** > **[システムテンプレート - CLI（System Templates-CLI）]** にあります。

（注） システム定義テンプレートが適切でない場合は、これらのシステムテンプレートに基づいてユーザー定義テンプレートを作成できます。各デバイスタイプの「/opt/CSCOlumos/conf/ifm/ifm_inventory」プロパティファイルの下の新しいテンプレート名を更新します。この変更は 5 分後に有効になります。サーバーの再起動は必要ありません。

ifm_inventory.properties のエントリを終了します。

```
ifm.inventory.managebility.prerequisite.ios=AutoDeploy_Manageability_Config-IOS
ifm.inventory.managebility.prerequisite.iosxr=AutoDeploy_Manageability_Config-IOS-XR
ifm.inventory.managebility.prerequisite.iosxe=AutoDeploy_Manageability_Config-IOS-XE
```

上記のエントリを更新して、新しいテンプレート名を指定できます。たとえば、ユーザーが IOS-XR デバイス用のテンプレート `Updated_AutoDeploy_Manageability_Config-IOS-XR` を追加する場合は、ファイル内のエントリを次のように更新する必要があります。

```
ifm.inventory.managebility.prerequisite.iosxr=Updated_AutoDeploy_Manageability_Config-IOS-XR
```

「変更監査ダッシュボード」（**[モニター（Monitor）]**>**[ツール（Tools）]**>**[変更監査ダッシュボード（Change Audit Dashboard）]** を選択）には、各デバイスの追加とそれに対応するテンプレートの展開の監査ログが表示されます。

制限事項：

SNMP/CLI のタイムアウトを更新すると、デバイスの同期が完了していない状態でもテンプレートがデプロイされます。

必要な設定：Cisco ONS デバイス オペレーティング システム

設定アーカイブ機能を使用することを予定している場合、デバイスをセキュアデバイスとして設定する必要があります。それには、CTC で次の操作を行います。

1. CTC で、**[プロビジョニング（Provisioning）]** > **[セキュリティ（Security）]** > **[アクセス（Access）]** の順に選択します。
2. EMS アクセスをセキュアとして設定します。

必須設定：Cisco NCS2K シリーズ デバイス

NCS2K デバイスで設定アーカイブ機能を使用する場合は、HTTP/HTTPS サーバーを有効にします。

（注） シングルセッションが有効になっていない、または適用できないデバイスの場合は、次の手順を実行して EPNM で使用する接続数を制限します。

1. $XMP_HOME/xmp_inventory/xde-home/inventoryDefaults/onsTL1.def を開きます。
2. 次のように新しい属性タグを追加します。</test> タグの後の ConnectionCount は実際の番号（5 など）に置き換える必要があります。

   <default attribute="DEVICE_THROTTLING">ConnectionCount</default>

IPv6 デバイスに必要な設定

IPv6 アドレスを使用するデバイスにアクセスするには、次の手順を実行することによって、Cisco EPN Manager サーバー（仮想マシン）で IPv6 アドレスとスタティック ルートを設定します。

1. インターフェイスから ipv6 address autoconfig を削除します。
2. Cisco EPN Manager サーバーで IPv6 アドレスを設定します。
3. スタティック ルートを Cisco EPN Manager サーバーに追加します。

デバイス上のアーカイブ ロギングの有効化

デバイス上でアーカイブ ロギングを有効にするには、次の手順を実行して、Cisco EPN Manager 上のデバイスに対して詳細なインベントリを有効にします。

Cisco IOS-XR デバイスの場合：

```
logging  <epnm server ip>  vrf default severity alerts
logging  <epnm server ip>  vrf default severity critical
logging  <epnm server ip>  vrf default severity error
logging  <epnm server ip>  vrf default severity warning
logging  <epnm server ip>  vrf default severity notifications
logging  <epnm server ip>  vrf default severity info
snmp-server host <epnm server ip>  traps version 2c public
```

Cisco IOS および IOS-XE デバイスの場合：

```
logging host <epnm server ip>  transport udp port 514
logging host <epnm server ip>  vrf Mgmt-intf transport udp port 514
snmp-server host <epnm server ip>  traps version 2c public
```

クレデンシャルプロファイルを使用したデバイスクレデンシャルの一貫した適用

資格情報のプロファイルは、TL1、HTTP、Telnet/SSH SNMP デバイスの認証情報のコレクションです。デバイスを追加するときは、デバイスを使用する必要があります資格情報のプロファイルを指定できます。これにより、デバイス間で一貫して資格情報の設定を適用できます。

資格情報の変更、デバイスのパスワードの変更などを行う必要がある場合は、設定がプロファイルを使用するすべてのデバイスにわたって更新されるプロファイルを編集できます。

既存のプロファイルを表示するには、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）] を選択します。

新しいクレデンシャル プロファイルの作成

この手順を使用して、新しいクレデンシャルプロファイルを作成します。次に、そのプロファイルを使用し、製品全体か、または新しいデバイスの追加時に、クレデンシャルを一貫して適用できます。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択します。

ステップ 2 既存のクレデンシャルプロファイルに必要な設定のほとんどがある場合は、それを選択し、[コピー（Copy）] をクリックします。それ以外の場合は、[追加（Add）] をクリックします。

ステップ 3 プロファイル名と説明を入力します。名前と説明が [クレデンシャルプロファイル（Credential Profiles）] ページに表示されるため、クレデンシャルプロファイルが多くなる場合は可能な限り識別しやすい名前と説明にします。

ステップ 4 プロファイルのクレデンシャルを入力します。このプロファイルを使用してデバイスを追加または更新すると、ここで指定した内容がそのデバイスに適用されます。

SNMP 読み取りコミュニティ ストリングは必須です。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

既存のデバイスへの新規または変更されたプロファイルの適用

次の手順を使用して、デバイスを一括編集し、そのデバイスが関連付けられているクレデンシャル プロファイルを変更します。この操作は、デバイスとクレデンシャル プロファイル間の既存の関連付けを上書きします。また、この操作を使用して、デバイス設定を新しい設定と同期させることもできます。

（注） この手順を実行して [**Update and Sync**] を選択する前に、プロファイルのクレデンシャル設定が正しいことを確認してください。この操作によって、デバイスは新しいプロファイルと同期します。

ステップ 1 次のいずれかの方法を使用して、クレデンシャル プロファイルを設定します。

- 新しいクレデンシャル プロファイルを作成するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[クレデンシャル プロファイル（Credential Profiles）]** を選択し、[追加（Add）] をクリックします。
- 既存のプロファイルを編集するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[クレデンシャル プロファイル（Credential Profiles）]** を選択し、プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 2 プロファイルに納得できたら、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 3 変更するすべてのデバイスをフィルタリングして選択します（一括編集）。

ステップ 4 [編集（Edit）] をクリックし、[クレデンシャル プロファイル（Credential Profile）] ドロップダウン リストから新しいクレデンシャル プロファイルを選択します。

ステップ 5 次のように変更を保存します。

- [更新（Update）] は、変更を Cisco EPN Manager データベースに保存します。
- [更新して同期（Update and Sync）] は、変更を Cisco EPN Manager データベースに保存し、デバイスの物理インベントリと論理インベントリを収集して、インベントリのすべての変更を Cisco EPN Manager データベースに保存します。

クレデンシャル プロファイルの削除

この手順で、クレデンシャル プロファイルを Cisco EPN Manager から削除します。現在、プロファイルがデバイスに関連付けられている場合は、デバイスの関連付けをそのプロファイルから解除する必要があります。

ステップ 1 何らかのデバイスがプロファイルを使用しているかどうかを確認します。

a) **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[クレデンシャル プロファイル（Credential Profiles）]** に移動します。
b) 削除するクレデンシャル プロファイルを選択します。
c) [編集（Edit）] をクリックし、[デバイス リスト（Device List）] ページにデバイスが一覧表示されているかどうかを確認します。デバイスが一覧表示されている場合は、それらをメモします。

ステップ 2 必要に応じて、プロファイルからデバイスの関連付けを解除します。

a) **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** に移動します。

b) 変更するすべてのデバイスをフィルタリングして選択します（一括編集）。

c) [編集（Edit）] をクリックし、[クレデンシャル プロファイル（Credential Profile）] ドロップダウン リストから [--選択--（--Select--）] を選択します。

d) 警告ダイアログボックスで [OK] をクリックし、古いプロファイルからデバイスの関連付けを解除します。

ステップ 3 クレデンシャル プロファイルを削除するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[クレデンシャル プロファイル（Credential Profiles）]** を選択し、プロファイルを選択し、[削除（Delete）] をクリックします。

デバイスの到達可能性の状態および管理ステータスの確認

次の手順を実行して、Cisco EPN Manager がデバイスと通信できるか（到達可能性の状態）や、そのホストを管理しているか（管理ステータス）を判断します。また、管理ステータスでは、デバイスが Cisco EPN Manager によって正常に管理されているかどうかの情報も提供されます。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルでデバイスを確認します。

a) [表示（Show）] ドロップダウン リスト（テーブルの右上）から [クイック フィルタ（Quick Filter）] を選択します。

b) [デバイス名（Device Name）] 列の下にあるテキスト ボックスにデバイスの名前（またはその一部）を入力します。

ステップ 3 [到達可能性（Reachability）] 列と [管理ステータス（Admin Status）] 列の情報を確認します。これらの状態の説明については、デバイスの到達可能性状態と管理状態 （84 ページ）を参照してください。

デバイスの到達可能性状態と管理状態

デバイスの到達可能性状態：Cisco EPN Manager が設定されたすべてのプロトコルを使用してデバイスと通信できるかどうかを表します。

表 *7*: デバイスの到達可能性状態

アイコン	デバイスの到達可能性状態	説明	トラブルシューティング
	到達可能	Cisco EPN Manager は、SNMP を使用してデバイスに、または ICMP を使用して NCS 2K デバイスにアクセスすることができます。	—
	ping 到達可能	Cisco EPN Manager は、ping を使用してデバイスに到達できますが、SNMP 経由では到達できません。	ICMP ping は成功しますが、SNMP 通信が失敗する原因すべてをチェックします。デバイス SNMP クレデンシャルがデバイスと Cisco EPN Manager の両方で同じであること、SNMP がデバイス上で有効になっているかどうか、またはトランスポートネットワークが設定ミスなどの理由で SNMP パケットをドロップしていないかどうかをチェックします。基本的なデバイスプロパティの変更 （398 ページ）を参照してください。
	到達不能	Cisco EPN Manager は、ping を使用してデバイスに到達できません。	物理デバイスが動作中でネットワークに接続されていることを確認します。
	不明	Cisco EPN Manager は、デバイスに接続できません。	デバイスをチェックします。

デバイスの管理状態：デバイスの設定状態を表します（たとえば、デバイスが ping によって到達できないためにダウンしている場合や、管理者が手動でデバイスをシャットダウンした場合などです）。

表 *8*: デバイスの管理状態

デバイスの管理状態	説明	トラブルシューティング
管理対象	Cisco EPN Manager は、デバイスを積極的にモニターしています。	該当なし。

メンテナンス	Cisco EPN Manager は、デバイスの到達可能性をチェックしていますが、トラップ、syslog、または TL1 メッセージを処理していません。	デバイスを管理対象状態に移行するには、デバイスのメンテナンス状態の切り替え （86 ページ）を参照してください。
管理対象外	Cisco EPN Manager は、デバイスをモニターしていません。	[ネットワーク デバイス（Network Devices）] テーブルで、デバイスを特定し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列でデータの横にある [i] アイコンをクリックします。ポップアップ ウィンドウに、詳細とトラブルシューティングのヒントが表示されます。収集問題の一般的な原因は次のとおりです。 • デバイス SNMP クレデンシャルが間違っている。 • Cisco EPN Manager 展開がライセンスで許可されているデバイスの数を上回っている。 • デバイスがスイッチ パス トレース専用になっている。 デバイス タイプがサポートされていない場合は、その [デバイス タイプ（Device Type）] が [不明（Unknown）] になります。そのデバイス タイプのサポートが Cisco.com で提供されているかをチェックするには、**[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [ソフトウェアアップデート（Software Update）]** を選択してから、[更新の確認（Check for Updates）] をクリックします。
不明	Cisco EPN Manager は、デバイスに接続できません。	デバイスをチェックします。

デバイスのメンテナンス状態の切り替え

デバイスの管理ステータスが [メンテナンス（Maintenance）] に変更されると、Cisco EPN Manager はデバイスのインベントリ変更用のポーリング操作も、デバイスで生成されたトラップまたは Syslog の処理も行わなくなります。ただし、Cisco EPN Manager は引き続き既存のリンクを維持し、デバイスの到達可能性をチェックします。

すべての管理状態および対応するアイコンのリストについては、デバイスの到達可能性状態と管理状態 （84 ページ）を参照してください。

ステップ 1 [ネットワーク デバイス（Network Devices）] テーブルで、**[管理状態（Admin State）]** > **[メンテナンス ステートに設定（Set to Maintenance State）]** の順に選択します。

ステップ 2 デバイスを完全な管理状態に戻すには、**[管理状態（Admin State）]** > **[管理対象状態に設定（Set to Managed State）]** の順に選択します。

（注） [メンテナンス状態をスケジュール（Schedule Maintenance State）] および [管理状態をスケジュール（Schedule Managed State）] オプションを使用して、特定の日時にメンテナンスを行い、特定の日時に管理状態に戻すようにデバイスをスケジュールすることもできます。

追加されたデバイスの検証と問題のトラブルシューティング

ディスカバリ プロセスをモニターするには、次の手順を実行します。

ステップ 1 ディスカバリ プロセスを確認するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ディスカバリ（Discovery）]** を選択します。

ステップ 2 ジョブ インスタンスを展開して詳細を表示し、次の各タブをクリックして、そのデバイスのディスカバリに関する詳細を表示します。

- [到達可能（Reachable）]：ICMP を使用して到達したデバイス。デバイスは到達可能ですが、モデル化されていない可能性があります。これは、ディスカバリを使用したデバイスの追加 （49 ページ）で示されているように、さまざまな理由で発生する可能性があります。このタブの情報から問題がないか確認してください。
- [フィルタ済み（Filtered）]：カスタマイズされたディスカバリ設定に従ってフィルタ処理されたデバイス。
- [ping で到達可能（Ping Reachable）]：ICMP ping で到達可能だったものの、SNMP を使用して通信できなかったデバイス。これには、複数の理由（無効な SNMP クレデンシャル、SNMP がデバイスで有効になっていない、ネットワークで SNMP パケットが廃棄されたなど）が原因が考えられます。
- [到達不能（Unreachable）]：障害により ICMP ping に応答しなかったデバイス。
- [不明（Unknown）]：Cisco EPN Manager は、ICMP または SNMP によってデバイスに接続できません。

（注） TL1 プロトコルを使用するデバイスの場合は、ノード名にスペースが含まれないようにしてください。そうでない場合、接続障害が発生します。

ステップ 3 デバイスが正常に Cisco EPN Manager に追加されたことを確認するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。次のアクションを実行します。

- 追加したデバイスがリストに表示されていることを確認します。Cisco EPN Manager がデバイスから収集したデバイス設定とソフトウェア イメージを表示するには、デバイス名をクリックします。
- [インベントリ収集ステータス（Inventory Collection Status）] フィールドの上にマウス カーソルを合わせ、表示されるアイコンをクリックすると、デバイスから収集された情報の詳細が表示されます。
- デバイスの到達可能性ステータスの列と管理者ステータスの列を確認します。デバイスの到達可能性状態と管理状態 （84 ページ）を参照してください。

デバイス情報を編集する必要がある場合は、基本的なデバイス プロパティの変更 （398 ページ）を参照してください。

Cisco EPN Manager がデバイスをサポートしていることを確認するには、Cisco Evolved Programmable Network Manager のサポート対象デバイスを参照してください。

Cisco EPN Manager がデバイスをサポートしていることを確認するには、[設定（Settings）] アイコン（⚙）をクリックし、[サポートされているデバイス（Supported Devices）] を選択します。

インベントリ収集またはディスカバリの問題があるデバイスの検索

クイック フィルタを使用して、ディスカバリまたは収集の問題があるデバイスを特定します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択して [ネットワークデバイス（Network Devices）] ページを開きます。

ステップ 2 テーブルの左上にある [表示（Show）] ドロップダウンに [クイック フィルタ（Quick Filter）] がリストされていることを確認します。

ステップ 3 [最終インベントリ収集ステータス（Last Inventory Collection Status）] の下にあるクイックフィルタフィールドにカーソルを置き、表示されるドロップダウンリストからステータスを選択します。選択したステータスに応じてデバイスがフィルタリングされます。トラブルシューティング手順については、追加されたデバイスの検証と問題のトラブルシューティング （87 ページ）を参照してください。

デバイス モデリングの再試行ジョブ

デバイスの検出中に特定の一時的な状態により、デバイスの [最終インベントリ収集ステータス（Last Inventory Collection Status）] 値が [警告付き完了（Completed with Warning）] と表示される場合があります。この場合、これらのデバイスの障害が発生した機能は、[障害が発生した機能の同期（Failed Feature Sync）] を使用して自動的に回復します。

（注） [警告付き完了（Completed with Warning）] 状態は、デバイスが [完了（Completed）] 状態に移行して Cisco EPN Manager から使用できるようになっても、障害が発生しているために特定の機能が使用できない場合に示されます。障害が発生した機能は一覧表示され、ユーザーが推奨処置を実行することで回復できます。

（注）

- [障害が発生した機能の同期（Failed Feature Sync）] ジョブは、[警告付き完了（Completed with Warning）] 状態のデバイスのみを対象に、特定の回復可能な障害（タイムアウト エラーなど）に対して使用されます。永続的なエラーまたはシステムベースのエラー（ユーザー認証エラーや不明なエラーなど）は自動回復できません。エラーシナリオの詳細については、管理チームにお問い合わせください。
- [障害が発生した機能の同期（Failed Feature Sync）] ジョブは、Cisco EPN Manager 3.0 以降のバージョンでのみ機能します。以前のバージョンの Cisco EPN Manager ですでに [警告付き完了（Completed with Warning）] 状態になっていたデバイスを 3.0 以降のバージョンにアップグレードした場合、ユーザーは [障害が発生した機能の同期（Failed Feature Sync）] ジョブを有効にする前に、デバイスの再同期を手動で実行する必要があります。ユーザーは手動で再同期する代わりに、日次同期ジョブで再同期が自動的に行われるのを待機することもできます。詳細については、システム ジョブについて （985 ページ）の [スイッチ インベントリ（Switch Inventory）] ジョブを参照してください。

[障害が発生した機能の同期（Failed Feature Sync）] ジョブ（**[管理（Administration）]** > **[ダッシュボード（Dashboard）]** > **[ジョブダッシュボード（Job Dashboard）]**に移動し、左側のサイドバーで、**[システムジョブ（System Jobs）]** > **[インベントリおよびディスカバリジョブ（Inventory And Discovery Jobs）]**を選択します）は、デフォルトで有効になっています。デフォルトのジョブ間隔（1 時間）は **[スケジュールの編集（Edit Schedule）]** オプションを使用して編集できますが、緊急時を除き、短縮した間隔でジョブを実行することはお勧めしません。

（注） [警告付き完了（Completed with Warning）] 状態のデバイスの数が多い場合は、[障害が発生した機能の同期（Failed Feature Sync）] ジョブをできるだけ低い頻度で実行することをお勧めします。

また、Cisco EPN Manager には、[警告付き完了（Completed with Warning）] 状態のデバイスに対して、エラーを解決してデバイスを [完了（Completed）] 状態に移行するためにユーザーが実行できる追加手順が用意されています。[ネットワークデバイス（Network Devices）] テーブルでデバイスを特定し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列でデータの横にある [i] アイコンをクリックします。ポップアップウィンドウに、詳細とトラブルシューティングのヒント（[障害（Failure）]、[影響（Impact）]、[考えられる原因（Possible Causes）]、および [推奨アクション（Recommended Actions）]）が表示されます。ユーザーが推奨アクションを実行した後、デバイスを手動同期（「誤ったCLIクレデンシャル（Wrong CLI

credentials）」などのエラーに適用可能）によって [完了（Completed）] 状態に移行させることも、次回の [障害が発生した機能の同期（Failed Feature Sync）] ジョブで自動的に回復させることもできます。

[警告付き完了（Completed with Warning）] のシナリオと対応する推奨アクションの一部を次に示します。

表 *9 : [*警告付き完了（*Completed with Warning***）*]* 状態のシナリオ**

考えられる原因	推奨処置
デバイスへの接続に失敗した	デバイスが着信 CLI/SNMP 接続を受け入れることを確認し、再試行します。
デバイスへの接続が切断される	デバイスが着信 CLI/SNMP 接続を受け入れることを確認し、再試行します。
データ制限を超えた	収集エラー：インベントリ ログを使用して管理者に問い合わせてください。
TL1 プロトコルの予期しない状態	デバイスが着信 TL1 接続を受け入れることを確認し、再試行します。
HTTP プロトコルの一般的な予期しない状態	デバイスが着信 HTTP 接続を受け入れることを確認し、再試行します。
NETCONF/XML からの取得中にエラーが発生した	NETCONF/XML が設定されていることを確認し、再試行します。
NETCONF によって RPC エラーが報告された	収集エラー：インベントリ ログを使用して管理者に問い合わせてください。
CLI_SESSION_SCRIPT ドキュメントでエラーが発生した	デバイスが新しい CLI セッションを受け入れることを確認し、再試行します。
セッションのセットアップ時または切断時のエラーを示すパターンに一致した	デバイスが新しい CLI セッションを受け入れることを確認し、再試行します。
デバイスに到達できない	インベントリ ログを管理者に問い合わせてください。
デバイスとの通信の試行中にフェールセーフタイムアウトが発生した	デバイスの応答性と負荷を確認します。
デバイスとの通信の試行中にタイムアウトが発生した	デバイスに設定されたタイムアウトによって CLI 接続が停止されないことを確認し、再試行します。また、デバイスに設定されているアクティブな SSH 接続の最大数を確認します。

考えられる原因	推奨処置
SNMP GET 要求に対する応答がない	デバイスが着信 SNMP 要求を受け入れることを確認し、再試行します。
SNMP Get 要求の実行に失敗した	デバイスが着信 SNMP 要求を受け入れることを確認し、再試行します。
SNMP Get 要求の応答エラー	デバイスが着信 SNMP 要求を受け入れることを確認し、再試行します。

CSV ファイルへのデバイス情報のエクスポート

デバイス リストをファイルにエクスポートすると、すべてのデバイス情報が CSV ファイルにエクスポートされます。次に、選択したパスワードを使用してファイルが圧縮され、暗号化されます。エクスポートしたファイルには、デバイスの SNMP クレデンシャル、CLI 設定、デバイスグループ、および地理的座標に関する情報が含まれています。エクスポートされたファイルにはデバイスのクレデンシャルが含まれていますが、クレデンシャルのプロファイルは含まれていません。

⚠

注意 CSV ファイルにはエクスポートしたデバイスのすべてのクレデンシャルのリストが含まれるため、十分に注意して使用してください。デバイスのエクスポートは特殊な権限を持つユーザーのみが実行できるようにする必要があります。

Cisco EPN Manager は、オペレーティングシステムのデフォルトの zip ユーティリティを使用して、エクスポートされたファイルを開くための ZipCrypto 暗号化方式をサポートしています。ZipCrypto 暗号化方式を有効にするには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[インベントリ（Inventory）]** > **[インベントリ（Inventory）]** を選択し、[「エクスポートデバイス」用の ZipCrypto 暗号化の有効化（Enable ZipCrypto encryption for 'Export Device'）] チェックボックスをオンにします。デフォルトでは、このオプションは無効になっています。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 エクスポートするデバイスを選択し、[デバイスのエクスポート（Export Device）] を選択します（または、 をクリックして [デバイスのエクスポート（Export Device）] を選択します）。

ステップ 3 [デバイスのエクスポート（Export Device）] ダイアログボックスで、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを追加して確認します。ユーザーはエクスポートされたファイルを開くのにこのパスワードを指定する必要があります。必要に応じて、エクスポートファイル名を入力します。ブラウザの設定によっては、圧縮したファイルを開いたり保存したりできます。

ステップ 4 [エクスポート（Export）] をクリックします。

（注）　ファイルを開くことができるのは、ZipCrypto 暗号化が有効になっている場合のみです。

簡単な管理と設定のためのデバイス グループの作成

デバイスを論理グループに編成すると、デバイスの管理、モニターリング、設定が簡素化されます。グループに操作を適用できるため、グループ化によって時間が節約され、ネットワーク全体で設定が一貫して適用されます。すべてのデバイスを同じ設定で構成できる小規模の構成では、ただ1つの一般的なデバイス グループを作成するだけで済みます。グループ化メカニズムは、サブグループもサポートしています。これらのグループは、多くの Cisco EPN Manager GUI ウィンドウに表示されます。

デバイスが Cisco EPN Manager に追加されると、[未定義（Unassigned）] という名前のロケーション グループに割り当てられます。多数のデバイスを管理している場合は、デバイスを他のグループに移動して、[未定義（Unassigned）] のグループ メンバーシップが大きくなりすぎないようにしてください。

グループの仕組み

グループは、デバイスやポートなどのネットワーク要素の論理コンテナです。たとえば、デバイスの種類や場所など、展開に固有のグループを作成できます。新しいデバイスが条件に一致する場合に自動的に追加されるようにグループを設定することも、手動でデバイスを追加することもできます。

特定のタイプのグループについては、関連項目 ネットワーク デバイス グループ （93 ページ） および ポート グループ （95 ページ） を参照してください。

グループに要素を追加する方法については、グループに要素を追加する方法：動的、手動、および混在グループ （96 ページ） を参照してください。

ネットワーク デバイス グループ

次の表に、サポートされているネットワーク デバイス グループのタイプを示します。デバイス グループにはインベントリからアクセスできます。

ネットワーク デバイス グループの種類	メンバーシップの条件	ユーザーが作成または編集できるか
デバイス タイプ（Device Type）	デバイスはファミリごとにグループ化されます（たとえば、オプティカル ネットワーキング、ルータ、スイッチおよびハブなど）。各デバイス ファミリの下で、デバイスはさらにシリーズごとにグループ化されます。新しいデバイスは、適切なファミリおよびシリーズ グループに自動的に割り当てられます。たとえば、Cisco ASR 9006 は、ルータ（ファミリ）および Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ（シリーズ）に属します。 次の点に注意してください。 • デバイス タイプ グループを作成することはできません。これらはシステム定義の動的グループです。代わりに、デバイス基準を使用してユーザー定義のグループを作成し、適切なデバイス名を付けます。 • デバイス タイプ グループはネットワーク トポロジ マップには表示されません。 • [Cisco EPN Manager] で検出されたサポート対象外のデバイスには [サポート対象外のシスコデバイス（Unsupported Cisco Device）] デバイスタイプが自動的に割り当てられ、**[デバイスタイプ（Device Type）] > [サポート対象外のシスコデバイスファミリ（Unsupported Cisco Device Family）]** に表示されます。	いいえ

ロケーション（Location）	ロケーション グループを使用して、ロケーションごとにデバイスをグループ化できます。デバイスを手動で追加するか、またはデバイスを動的に追加して、ロケーション グループの階層（シアター、国、地域、キャンパス、ビルディング、フロアなど）を作成できます。 デバイスは 1 つのロケーション グループのみに表示されるはずですが、上位レベルの「親」グループにもそのデバイスが含まれています。たとえば、ビルディングのロケーション グループに属するデバイスは、親のキャンパス グループにも間接的に属している場合があります。 デフォルトでは、階層の上位のロケーションが [すべてのロケーション（All Locations）] グループとなります。ロケーションに割り当てられていないデバイスはすべて、[すべてのロケーション（All Locations）] の下の [未割り当て（Unassigned）] グループに表示されます。	はい
ユーザー定義（User Defined）	デバイスは、デバイスおよびロケーション条件のカスタマイズ可能な組み合わせによってグループ化されます。グループ名をカスタマイズして、必要なデバイスおよびロケーション基準を使用できます。	対応

ロケーショングループのインポート

[ネットワークデバイスグループ（Network Device Groups）] ページで、CSV ファイルを使用してロケーショングループをインポートできます。Cisco EPN Manager に追加するグループのすべての属性のリストが示される CSV ファイルを使用してロケーション グループをインポートするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 [グループのインポート（Import Groups）] ボタンをクリックします。[グループのインポート（Import Groups）] ダイアログが開きます。

ステップ 3 表示されたダイアログの下部にある [こちら（here）] をクリックしてサンプルテンプレートをダウンロードします。CSV ファイルを作成し、テンプレート内の形式と情報をガイドとして使用して、グループの名前、親階層、場所の設定、物理アドレス、緯度および経度の詳細を入力します。CSV ファイルを保存します。

ステップ 4 [グループのインポート（Import Groups）] ダイアログで [参照（Browse）] をクリックし、インポートするグループが含まれている CSV ファイルを選択します。

ステップ 5 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** を選択し、[グループのインポート（Import Groups）] をクリックしてジョブのステータスを表示します。

ロケーショングループのエクスポート（Export Location Groups）

ロケーショングループの情報を CSV ファイルとしてエクスポートするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 [グループのエクスポート（Export Groups）] ボタンをクリックします。[グループのエクスポート（Export Groups）] ダイアログが開きます。

ステップ 3 目的の場所にCSVファイルを保存します。CSVファイルには、グループ名、親階層、場所の設定、物理アドレス、緯度、経度などの詳細が示されます。

ポート グループ

次の表に、サポートされているポート グループのタイプを示します。

ポート グループの種類	メンバーシップの条件	ユーザーが作成または編集できるか
ポート タイプ（Port Type）	ポートの種類、速度、名前、または説明ごとにグループ化されます。新しいデバイスのポートは、適切なポート グループに自動的に割り当てられます。 ポート タイプのグループは作成できません。代わりに、デバイス基準を使用してユーザー定義グループを作成し、ユーザー定義グループの下にサブグループを作成します。	いいえ。代わりに、ユーザー定義グループを作成します。

システム定義（System Defined）	ポートの使用状況または状態別にグループ化されます。新しいデバイスのポートは、適切なポート グループに自動的に割り当てられます。 [リンクポート（Link Ports）]：別のシスコ デバイスまたは他のネットワーク デバイスに接続され、「VLAN」モードで動作し、VLAN に割り当てられるポート。 [トランクポート（Trunk Ports）]：シスコ デバイスまたは他のネットワーク デバイス（スイッチ、ルータ、ファイアウォール、サードパーティ デバイス）に接続され、すべてのVLANのトラフィックを伝送する「トランク」モードで動作しているポート。 ポートのステータスがダウンすると、そのポートは[未接続ポート（Unconnected Port）] グループに自動的に追加されます。このグループ内のポートを削除することはできません。また、このグループを他のグループのサブ グループとして再作成することはできません。 ワイヤレス デバイスおよびデータセンター デバイスは、AVC 設定済みインターフェイス、UCS インターフェイス、UCS アップリンク インターフェイス、WAN インターフェイスなど、その他のシステム定義のポート グループを使用します。 システム定義のポート グループは作成できません。代わりに、デバイス基準を使用してユーザー定義グループを作成し、ユーザー定義グループの下にサブグループを作成します。 （注） [WAN インターフェイス（WAN Interfaces）] はスタティック グループであるため、自動ポートの追加は適用されません。したがって、手動でグループにポートを追加する必要があります。	いいえ。代わりに、ユーザー定義グループを作成します。
ユーザー定義（User Defined）	ポート基準のカスタマイズ可能な組み合わせによってグループ化され、グループに名前を付けることができます。グループが動的でポートが条件に一致する場合は、そのグループに追加されます。	対応

グループに要素を追加する方法：動的、手動、および混在グループ

グループに要素を追加する方法は、グループが動的か、手動か、混在かによって異なります。

デバイスの追加方法	説明

動的	要素がグループ基準を満たしている場合、Cisco EPN Manager はグループに新しい要素を自動的に追加します。指定できるルールの数に制限はありませんが、ルールを追加するにしたがい更新のパフォーマンスに影響が及ぶ場合があります。
手動	グループの作成時またはグループの編集時に、ユーザーは手動で要素を追加します。
混合	要素は、動的ルールと手動追加の組み合わせによって追加されます。

親/子のユーザー定義グループおよびロケーション グループにおけるデバイスの継承は次のとおりです。

- ユーザー定義グループ：子グループを作成する場合：
  - 親グループと子グループの両方がダイナミックの場合、子グループは親グループ内のデバイスにのみアクセスできます。
  - 親グループが静的で、子グループが動的である場合、子グループは親グループ外のデバイスにアクセスできます。
  - 親グループと子グループが動的かつ静的である場合、子グループは親のデバイス グループからデバイスを「継承」します。
- ロケーション グループ：親グループは子のグループ デバイスを継承します。

グループおよび仮想ドメイン

グループは要素の論理コンテナですが、要素へのアクセスは仮想ドメインによって制御されます。次の例は、グループと仮想ドメインの関係を示しています。

- **SanJoseDevices** という名前のグループに 100 台のデバイスが含まれています。
- **NorthernCalifornia** という名前の仮想ドメインに 400 台のデバイスが含まれています。これらのデバイスはさまざまなグループに属しており、**SanJoseDevices** グループのデバイスが 20 台含まれています。

NorthernCalifornia 仮想ドメインにアクセスできるユーザーは、**SanJoseDevices** グループの 20 台のデバイスにアクセスできますが、このグループ内の他の 80 台のデバイスにはアクセスできません。詳細については、デバイスへのユーザーアクセスを制御するための仮想ドメインの作成 （1030 ページ）を参照してください。

ユーザー定義のデバイス グループの作成

新しいデバイス タイプ グループを作成するには、ユーザー定義グループのメカニズムを使用します。デバイスタイプグループは Cisco EPN Manager 全体で使用される特殊なカテゴリであるため、このメカニズムを使用する必要があります。作成するグループが [ユーザー定義（User Defined）] カテゴリに表示されます。

（注） Cisco ASR サテライトは、ロケーション グループにのみ所属できます。詳細については、Cisco EPN Manager でのサテライトの考慮事項 （343 ページ）を参照してください。

新しいグループを作成するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] ペインで [+]（**追加**）アイコンをクリックし、[ユーザー定義グループの作成（Create User Defined Group）] を選択します。

ステップ 3 グループの名前と説明を入力します。他のユーザー定義デバイスタイプグループが存在する場合、[親グループ（Parent Group）] ドロップダウンリストからグループを選択することで、そのグループを親グループとして設定できます。親グループを選択しなかった場合は、新しいグループが [ユーザー定義（User-Defined）] フォルダに配置されます（デフォルト）。

ステップ 4 次のように、デバイスを新しい グループに追加します。

条件を満たすデバイスを自動的に追加する場合は、[デバイスを動的に追加（Add Devices Dynamically）] 領域に条件を入力します。IP アドレスの特定の範囲内に入るデバイスをグループ化するには、角カッコ内にその範囲を入力します。たとえば、次を指定できます。

- IPv4-10.[101-155].[1-255].[1-255] および 10.126.170.[1-180]
- IPv6-2014::5217:[0000-ffff]:fe22:[1e40-1f41]

（注） ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えるとグループの更新パフォーマンスが低下する可能性があります。

デバイスを手動で追加する場合は、次の手順を実行します。

1. [デバイスを手動で追加（Add Devices Manually）] 領域を展開し、[追加（Add）] をクリックします。
2. [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスのチェックボックスをオンにして、[追加（Add）] をクリックします。

ステップ 5 [プレビュー（Preview）] タブをクリックしてグループのメンバーを表示します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 3 で選択したフォルダに新しいデバイスグループが表示されます。

（注） 動的に追加されたデバイスグループは、作成後に削除できません。デバイスを手動で追加および定義する場合は、動的に作成されたデバイスグループを削除し、新しいデバイスグループを作成する必要があります。

（注） **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[設定アーカイブ（Configuration Archive）]** > **[アーカイブ（Archives）]** > **[グループの作成（Create Group）]** に移動して、デバイスグループを作成することもできます。

ロケーション グループの作成

（注） Cisco ASR サテライトは、ロケーション グループにのみ属することができます。詳細については、Cisco EPN Manager でのサテライトの考慮事項 （343 ページ）を参照してください。

ロケーション グループを作成するには、次の手順を実行します。

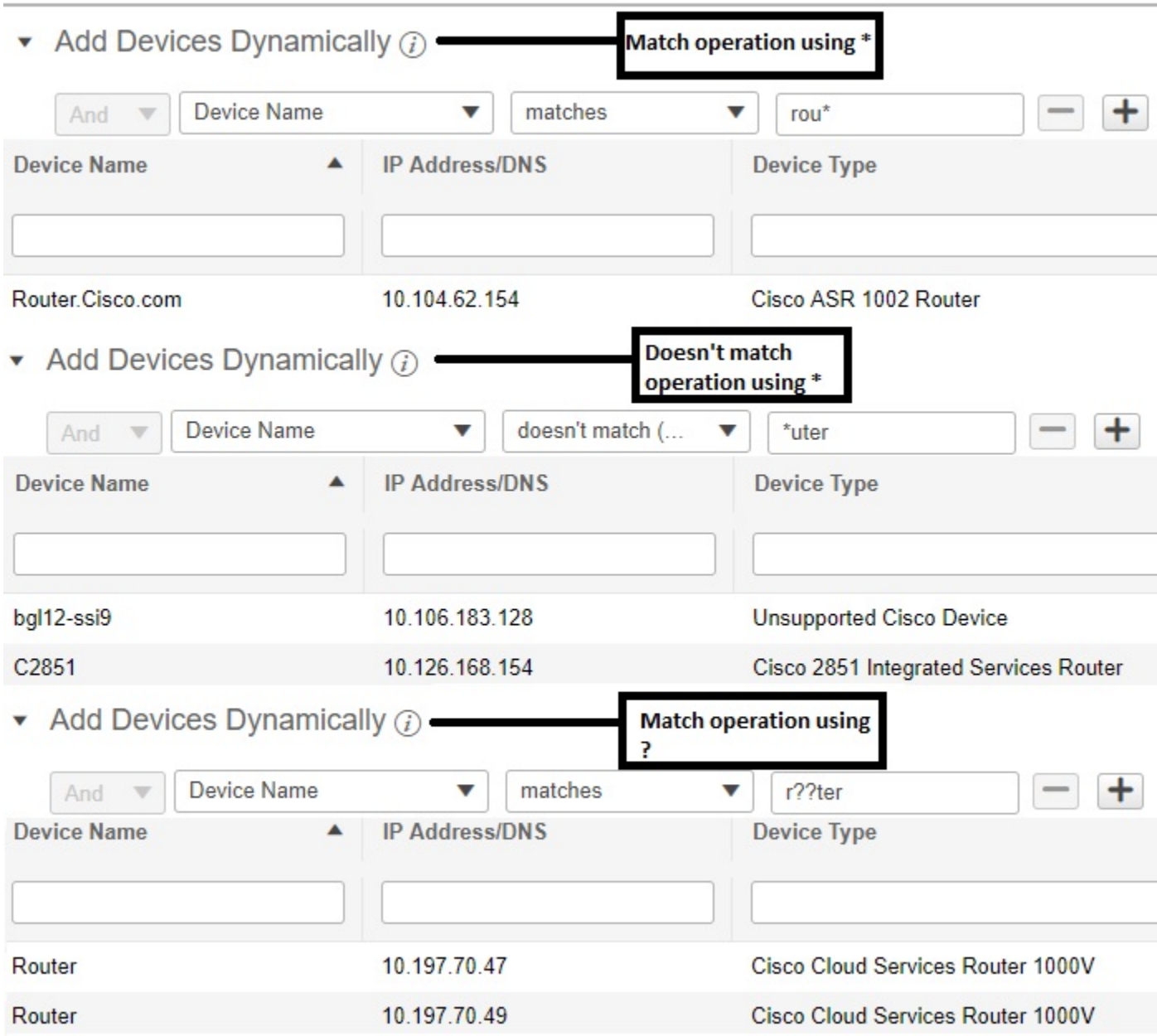
ステップ 1 **[インベントリ（Inventory）]** > **[グループ管理（Group Management）]** > **[ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインで、[追加（Add）] アイコンをクリックし、[ロケーション グループの作成（Create Location Group）] を選択します。

ステップ 3 名前と説明を入力し、[親グループ（Parent Group）] ドロップダウンリストからグループを選択します。デフォルトでは、[すべてのロケーション（All Locations）] のサブグループになります（つまり、[すべてのロケーション（All Locations）] フォルダに表示されます）。

ステップ 4 たとえば、特定の住所のビルディングにあるすべてのデバイスなど、地理的なロケーションに基づいてデバイス グループを作成する場合は、[地理的なロケーション（Geographical Location）] チェックボックスをオンにしてグループの GPS 座標を指定するか、または [マップの表示（View Map）] リンクをクリックし、マップ内の必要な場所をクリックします。この場合は、GPS 座標が自動的に入力されます。地理的なロケーションで定義されたロケーション グループは、Geo マップのグループ アイコンで表されます。グループに追加するデバイスは、そのグループの GPS 座標を継承します。詳細については、Geo マップのデバイス グループ （258 ページ） を参照してください。地理的なロケーションが一連のデバイスをグループ化する主たる理由の場合は、グループに追加するデバイスに、そのグループとは異なる独自の GPS 座標を持たせないことを推奨します。

ステップ 5 特定の基準を満たしている場合にデバイスが自動的に追加されるようにするには、[デバイスを動的に追加（Add Devices Dynamically）] 領域に基準を入力します。それ以外の場合は、この領域を空欄のままにします。



ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

ステップ 6 デバイスを手動で追加する場合は、次の手順を実行します。

a) [デバイスを手動で追加（Add Devices Manually）] で、[追加（Add）] をクリックします。

b) [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスを見つけて、[追加（Add）] をクリックします。

ステップ 7 [プレビュー（Preview）] タブをクリックして、グループ メンバーを確認します。

ステップ 8 [保存（Save）] をクリックすると、ステップ 3 で選択したフォルダ（デフォルトでは [すべてのロケーション（All Locations）]）の下に新しいロケーション グループが表示されます。

Maps GUI を起動して建物をクリックします。

ロケーショングループを編集する場合は、次の条件を満たしている場合にグループタイプを変更できます。

- グループ タイプがデフォルト。
- グループにサブグループがない。

ポート グループの作成

ポート グループを作成するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ポート グループ（Port Groups）]** を選択します。

ステップ 2 **[ポートグループ（Port Groups）] > [ユーザー定義（User Defined）]** から、[ユーザー定義（User Defined）] の横にある [i] アイコンの上にカーソルを置き、ポップアップウィンドウの [サブグループの追加（Add SubGroup）] をクリックします。

ステップ 3 名前と説明を入力し、[親グループ（Parent Group）] ドロップダウンリストからグループを選択します。デフォルトでは、ポート グループは [ユーザー定義（User Defined）] フォルダに配置されます。

ステップ 4 グループに追加するためにポートが属している必要があるデバイスを選択します。[デバイスの選択（Device Selection）] ドロップダウンリストから、次を選択できます。

- [デバイス（Device）] : すべてのデバイスのフラット リストからデバイスを選択します。
- [デバイス グループ（Device Group）] : デバイス グループを選択します（[デバイス タイプ（Device Type）]、[ロケーション（Location）]、および [ユーザー定義（User Defined）] グループのリストが表示されます）。

ステップ 5 条件を満たしている場合にポートが自動的に追加されるようにするには、[ポートを動的に追加（Add Ports Dynamically）] 領域にその条件を入力します。それ以外の場合は、この領域を空欄のままにします。

ダイナミックグループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

ステップ 6 デバイスを手動で追加する場合は、次の手順を実行します。

a) [ポートを手動で追加（Add Port Manually）] で、[追加（Add）] をクリックします。
b) [ポートの追加（Add Devices）] ダイアログボックスで、追加するデバイスを見つけて、[追加（Add）] をクリックします。

ステップ 7 [プレビュー（Preview）] タブをクリックして、グループ メンバーを確認します。

ステップ 8 [保存（Save）] をクリックすると、ステップ 3 で選択したフォルダ（デフォルトでは [ユーザー定義（User Defined）]）の下に新しいポート グループが表示されます。

グループのコピーの作成

グループの複製を作成すると、Cisco EPN Manager はデフォルトでそのグループに **CopyOf***group-name* という名前を付けます。名前は必要に応じて変更できます。

グループを複製するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインから、グループを選択します。

ステップ 3 コピーするデバイス グループを見つけ、その横にある [i] をクリックするとポップアップ ウィンドウが開きます。

ステップ 4 [グループの複製（Duplicate Group）] をクリックし（この時点では変更を加えないでください）、[保存（Save）] をクリックします。Cisco EPN Manager は **CopyOf***group-name* という名前の新しいグループを作成します。

ステップ 5 ユーザー定義のデバイス グループの作成 （97 ページ）とロケーション グループの作成 （99 ページ）の説明に従ってグループを設定します。

ステップ 6 [プレビュー（Preview）] タブをクリックし、グループメンバーを調査して、グループの設定を確認します。

ステップ 7 [保存（Save）] をクリックして、グループを保存します。

メンバーがいないグループの非表示

デフォルトでは、グループにメンバーが存在しなくても、Cisco EPN Manager は Web GUI にグループを表示します。管理者権限を持つユーザーが、この設定を変更して空のグループが非表示になる、つまり Web GUI に表示されないようにすることができます。（非表示グループは Cisco EPN Manager から削除されません）。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [グループ化（Grouping）]** を選択します。

ステップ 2 [メンバーが存在しないグループの表示（Display groups with no members）] をオフにし、[保存（Save）] をクリックします。

グループやデバイスが多数ある場合は、[メンバーが存在しないグループの表示（Display groups with no members）]チェックボックスをオンのままにすることをお勧めします。これをオフにすると、システムのパフォーマンス速度が低下します。

グループの削除

削除するグループにメンバーが含まれていないことを確認します。メンバーが含まれている場合、Cisco EPN Manager で操作を続行することはできません。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 削除するデバイス グループを左側の [デバイス グループ（Device Groups）] ペインで見つけ、その横にある [i] をクリックするとポップアップ ウィンドウが開きます。

ステップ 3 [グループの削除（Delete Group）] をクリックし、[OK] をクリックします。

デバイスの削除

デバイスを削除すると、Cisco EPN Manager でそのデバイスのモデリングおよびモニターリングは行われなくなります。

始める前に

デバイスに Cisco EPN Manager を使用してプロビジョニングされたサービスがある場合は、デバイスを削除する前にそれらのサービスを削除する必要があります。ただし、デバイス自体で検出またはプロビジョニングしたサービス（つまり、Cisco EPN Manager によって作成されていないサービス）があっても、デバイスの削除は可能です。デバイス上のサービスを検索するには、[デバイス360（Device 360）] ビューを使用します（特定のデバイスの回線/VC の表示（813 ページ）を参照）。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択して [ネットワークデバイス（Network Devices）] ページを開きます。

ステップ 2 削除するデバイスを見つけます。たとえば、[デバイスグループ（Device Groups）] リスト内を移動したり、[クイックフィルタ（Quick Filter）] ボックスにテキストを入力したりできます。

ステップ 3 デバイスを選択し、[デバイスの削除（Delete device）] アイコンをクリックします。

既存のネットワーク装置（NE）の置換

既存のネットワーク装置（NE）を、古いデバイスとまったく同じ新しいネットワーク装置に置き換えるには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] を選択し、[完了（Completed）] 状態になったときに置換する必要があるデバイスの設定バックアップを取得します。

ステップ 2 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択し、置換する必要があるデバイスのデバイスの状態を [メンテナンス（Maintenance）] に変更します。

ステップ 3 古いハードウェアと同じスロットにインストールされた RP およびラインカードを含めて、ネットワーク装置（NE）を同じハードウェアに置き換えます。

ステップ 4 古いハードウェアを接続したのと同じ方法で、新しいハードウェアを管理ポートに再接続します。

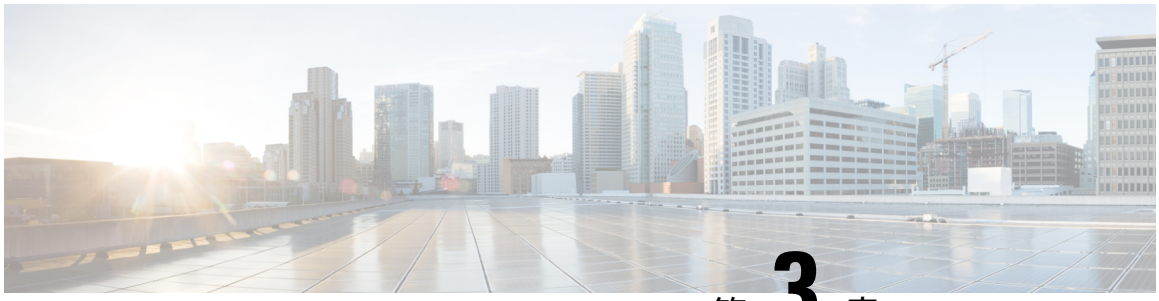
ステップ 5 新しいデバイスの基本管理設定を、古いデバイスと同じように設定します。たとえば、[管理IP（Management IP）]、[サブネット（Subnet）]、[ホスト名（Hostname）] などです。

ステップ 6 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] を選択し、新しいデバイス上の古いデバイスから設定バックアップを [ロールバック（Roll Back）] します。

ステップ 7 [ネットワークデバイス（Network Devices）] ページで、デバイスの状態を [管理対象（Managed）] に変更し、ステータスが [完了（Completed）] に変わるまで待機します。

次のタスク

すべての基本的なデバイス設定、サービス、パフォーマンス、および障害データがそのまま維持されて、新しい設定が正しいことを確認します。



第 3 章

デバイスの詳細の表示

次のトピックでは、ネットワーク デバイスに関する詳細情報を取得する方法について説明します。また、ハードウェアとソフトウェアの詳細、CPU とメモリの使用率、一般的なデバイス ヘルスなどを示すさまざまなデバイス レポートを生成することもできます。レポートの詳細については、デバイス レポート （376ページ）を参照してください。インベントリ収集の詳細については、インベントリはどのように収集されていますか。 （68 ページ）を参照してください。

デバイスの検索

デバイスを見つける最も簡単な方法は、[ネットワークデバイス（Networks Devices）] テーブル（[インベントリ （Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]）の上部に表示されるクイック検索テキスト ボックスを使用することです。デバイス名、IP アドレス、またはソフトウェアバージョンの文字列の一部を入力するか、到達可能性、管理ステータス、およびインベントリ収集の値から選択できます。ユーザー定義フィールドが作成されている場合は、ユーザー定義フィールドの値で検索することもでき

ます。また、デバイスはデバイス グループに編成されており、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択し、[デバイスグループ（Device Group）] リストからデバイス タイプを選択して表示できます。

基本デバイス情報を取得する：[デバイス 360（Device 360）] ビュー

[デバイス 360（Device 360）] ビューは、デバイス、そのインベントリ、およびそのステータスに関するクイック情報を提供するポップアップ ウィンドウです。これには、デバイスのアラーム、モジュール、インターフェイス、ネイバー、およびシャーシが含まれます。

[デバイス 360（Device 360）] ビューを起動するには、次の手順を実行します。

- ほとんどすべてのデバイステーブルの IP アドレスの横にある [i] アイコンをクリックします。
- ネットワーク トポロジで、拡張グループ内のデバイスをクリックしてから、[表示（View）] をクリックします。

[デバイス 360（Device 360）] ビューで、ビューの上部にデバイスとパフォーマンスに関する一般情報が示されます。また、ビューの下部にあるタブには、より詳細なインターフェイス情報が表示されます。[デバイス 360（Device 360）] ビューに表示される情報は、デバイスのタイプと設定によって異なります。[デバイス 360（Device 360）] ビューが提供する情報は次のとおりです。

SVO デバイスについては、[デバイス360（Device 360）] ビュー - SVO （62 ページ） を参照してください。

[デバイス 360（Device 360）] ビューで提供される情報	説明

一般情報とツール	

	デバイス タイプ、その OS タイプとバージョン、その最新の設定変更、およびその最新のインベントリ収集。アイコンは、デバイスのステータスを示しています。 （注） • セキュア ドメイン ルータ（SDR）を収容する Cisco NCS 6000 デバイスの [デバイス360（Device 360）] ビューを開いている場合は、SDR の名前も表示されます。 • Cisco Catalyst 6500 シリーズ デバイス用に [デバイス360（Device 360）] ビューをデュアルおよびクワッドスーパバイザ仮想スイッチング システム（VSS）で開いた場合、デバイスの冗長性状態、スイッチ モード、および運用の冗長性モードも表示されます。 ポップアップウィンドウにあるメニューを使用して、次のタスクを実行することもできます。 • [自動更新（Auto-Refresh）] : デバイスのステータスとトラブルシューティングをリアルタイムで更新する場合は、[更新（Refresh）] アイコンをクリックしてオンデマンド更新を有効にします。または、ドロップダウンリストから、自動更新の間隔を 30 秒、1 分、2 分、または 5 分に設定することもできます。デフォルトでは、自動更新はオフになっています。 （注） 自動更新設定は、現在開いている [360° ビュー（360° View）] ポップアップウィンドウにのみ適用されます。このビューを閉じてからもう一度開いた場合または別のビューを開いた場合は、デフォルトでは自動更新がオフになります。 • トラブルシュート：ping またはトレースルートを実行して、アラームブラウザを起動し、シスコ サポートケースを開くか、シスコサポートコミュニティから情報を取得します（**[アクション（Actions）]** メニュー）。 • パフォーマンス：デバイスの CPU とメモリをチェックします（**[表示（View）]** > **[パフォーマンスグラフ（Performance Graphs）]**）。 • トポロジ：ネットワーク トポロジとデバイスのローカル トポロジを最大 3 ホップまで表示します（[アクション（Actions）] メニュー）。 • デバイスのルーティング テーブルを確認します（[アクション（Actions）] メニュー）。 • [デバイスコンソール（Device Console）] を開き、デバイス上

	で実行するコマンドを入力します（[アクション（Actions）] メニュー）。 （注） Cisco EPN Manager では、各ユーザーがデバイスコンソールに入力したコマンドの監査情報を保持しています。この監査情報を確認するには、[管理（Administration）] > [設定（Settings）] > [システム監査（System Audit）] > > の順に選択します。 • [今すぐ同期（Sync Now）] を使用して、デバイスのインベントリを収集し、データベースに保存します（[アクション（Actions）] メニュー）。 • デバイスとの HTTP、HTTPS、SSH または Telnet セッションを開きます（[アクション（Actions）] メニュー）。 • 光デバイス用の Cisco Transport Controller を起動します（[アクション（Actions）] メニュー）。 • 20 秒ごとのビューの自動更新を有効にします（[アクション（Actions）] メニュー）。 • **[再同期条件（Resync Conditions）]（[アクション（Actions）]** メニュー）を使用して、選択した NCS2k デバイスのうち重要度が NA/NR のデバイスについて、状態を再同期できます。 • [デバイスの詳細（Order Details）] ページを開いてソフトウェア イメージとコンフィギュレーション ファイルの管理に関する詳細を表示し、デバイスのシャーシ ビューを使用します（デバイス IP アドレス ハイパーリンクをクリックするか、**[表示（View）] > [詳細（Details）]** を選択する）。 • **[表示（View）] > [設定（Configuration）]**を選択して [デバイス360（Device 360）] ページから移動せずに、デバイスの設定変更を実行するには、[設定（Configuration）] ページを直接開きます。 （注） このオプションは、設定変更を実行できるデバイスで使用できます。たとえば、NCS 2K デバイスなどです。 • 発生したアラームや回線、インターフェイス、およびモジュールの現在のステータスなどの情報に基づいて別のデバイスと対照比較するためのデバイスを選択します（[アクション（Actions）] メニュー）。「デバイスの情報とステータスを比較する」を参照してください。

	• **[アクション（Actions）]** メニューで **[デバイス（Device OAM）]** をクリックして、2 つのデバイス間で ping テストまたはトレースルートを実行します。**[デバイスOAMコマンド（Device OAM Commands）]** ウィンドウで、**[宛先IP（Destination IP）]** を入力します。**[送信元IP（Source IP）]** の指定はオプションです。**[アクション（Actions）]** ドロップダウンリストから、pingテストを実行するか、トレースルートを実行するかを選択できます。
パフォーマンス データ	デバイスのパフォーマンスのさまざまな側面を反映したチャート。デバイスに複数のメモリプールが存在する場合は、[デバイス 360（Device 360）] ビューにすべてのメモリプールの平均使用率が表示されます。個々のメモリ プールに関する情報を表示するには、ネットワーク サマリー ダッシュボードでメモリ使用率ダッシュレットを使用します。「[ネットワーク サマリー（Network Summary）] ダッシュボードの概要」を参照してください。
[アラーム（Alarms）] タブ	重大度、ステータス、および収集時刻を含む、デバイスの現在のアラーム。アラーム ソースによっては、このタブから他の 360 ビューを起動することもできます。
[モジュール（Modules）] タブ	名前、タイプ、状態、ポート、および場所を含む、デバイス上で設定されたモジュール。
[インターフェイス（Interfaces）] タブ	ステータス情報を含む、デバイス上で設定されたインターフェイス。また、特定のインターフェイス用の [インターフェイス 360（Interface 360）] ビューを起動することもできます。
[ネイバー（Neighbors）] タブ	Cisco Discovery Protocol（CDP）経由でこのデバイスに接続している NE。選択されたデバイスで CDP がサポートされていない場合は、このタブには何も表示されません。表示される情報には、デバイス タイプ、デバイス名、ローカル ポート、およびデバイス ポートが含まれます。ポップアップトポロジマップにネイバーを表示するには、[デバイス 360° ビュー（Device 360 View）] の右上で [アクション（Actions）]>[Nホップトポロジ（N Hop Topology）] を選択します（デバイス 360 ビューからデバイスのローカル トポロジを表示する （112 ページ）を参照）。
[回路/VC（Circuit/VCs）] タブ	デバイス上でプロビジョニングされた各回線の回線/VC 名、タイプ、顧客、ステータス、および作成日。また、特定の回線/VC 用の [回線/VC 360（Circuit/VC 360）] ビューを起動することもできます。
[衛星（Satellites）] タブ	クラスタ構成内の Cisco ASR 9000 デバイスの場合は、衛星の名前、タイプ、説明、ステータス、IP アドレス、および MAC アドレスが一覧表示されます。特定のサテライトの [サテライト360（Satellite 360）] ビューを起動することもできます。

シビック ロケーション	デバイスの位置に関する地理的情報。
最近の変更	デバイス上で行われた最新の 5 つの変更。インベントリ、設定（設定アーカイブ）、またはSWIM（ソフトウェアイメージ）に分類されます （注） ルートユーザーとしてログインしている場合は、[最近の変更（Recent Changes）] タブですべてのアクティビティを表示できます。非ルートユーザーとしてログインしている場合は、自分が実行したアクティビティのみを表示できます。
SRRGs	デバイスに割り当てられた共有リスクリソースグループ（SRRG）が一覧表示されます。このタブの [?]（[ヘルプ（help）]）アイコンをクリックしてその凡例を表示します。SRRG に関する詳細については、「Geo マップでの共有リスク リソース グループ（SRRG）の管理」を参照してください。

また、**[アクション（Actions）] > [ネットワーク トポロジ（Network Topology）]**（[デバイス 360（Device 360）] ビューの右上にある）を選択することにより、トポロジ マップに特定のデバイスを表示することもできます。

デバイスの情報とステータスを比較する

[比較ビュー（Comparison View）]ページでは、複数のデバイスの対照比較を実行できます。このビューには、発生したアラーム、デバイス上のモジュール、インターフェイス、および回線のステータス、最近実行された変更の概要などの情報が表示されます。デバイスを比較するには、次の手順を実行します。

ステップ 1 次のいずれかを選択して、[ネットワーク デバイス（Network Devices）] ページを開きます。

- **[モニター（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）]**
- **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワークデバイス（Network Devices）]**

ステップ 2 比較するデバイスごとに、次の手順を実行します。

a) [IPアドレス（IP Address）] 列で [i]（情報）アイコンをクリックして、[デバイス 360（Device 360）] ビューを開きます。

b) **[アクション（Actions）] > [追加して比較（Add to Compare）]** を選択します。

選択したデバイスがページの下部に表示されます。最大 4 つのデバイスを選択できます。

ステップ 3 [比較（Compare）] をクリックします。

[比較ビュー（Comparison View）] ページが開きます。

ステップ 4 ビューの上部にあるドロップダウン リストで、利用可能なすべての情報をビューに表示するか、デバイスごとに一意の情報だけを表示するかを指定します。

ステップ 5 [ビューのカスタマイズ（Customize View）] をクリックして、ビューに表示するカテゴリのチェックボックスをオンにしてから、[保存（Save）] をクリックします。

デフォルトでは、すべてのカテゴリが選択されています。

ステップ 6 選択したカテゴリごとに提供される情報が表示されるようにページをスクロール ダウンします。

次の点に注意してください。

- **比較ビュー**には、一度に 2 つのデバイスに関する情報しか表示されません。3 つ以上を選択した場合は、現在表示されていないデバイスに切り替える必要があります。
- 選択したデバイスの順序を変更するには、ページの右上にある [並べ替え（Rearrange）] をクリックします。
- 各デバイスの [表示（View）] メニューと [アクション（Actions）] メニューは、[デバイス 360（Device 360）] ビューで提供されるものと同じです。オプションを選択すると、対応するページが開きます。
- 必要に応じて、表示されるカテゴリを最小化または最大化できます。
- [比較ビュー（Comparison View）] は、回線および VC、インターフェイス、およびリンクでも利用できます。それぞれの 360 ビューからこれらの要素のいずれかを比較用に選択すると、対応するタブにその要素が表示されます。これにより、必要に応じて要素のタイプを切り替えることができます。
- デバイスの比較を終了する場合は、ページの右上にある [戻る（Back）] をクリックしてから、ページの下部にある [すべての項目をクリア（Clear All Items）] をクリックします。他の要素タイプのタブが表示されている場合は、それらのタブもクリアする必要があります。

デバイス 360 ビューからデバイスのローカル トポロジを表示する

デバイス周辺のネットワーク トポロジを最大 3 つのホップまで表示するデバイス 360 ビューから小規模なトポロジのウィンドウを起動できます。

ステップ 1 興味のあるデバイスのデバイス 360 ビューを開きます。

- ほとんどすべてのデバイス テーブルの IP アドレスの横にある [i] アイコンをクリックします。
- ネットワーク トポロジで、拡張グループ内のデバイスをクリックしてから、[表示（View）] をクリックします。

ステップ 2 [アクション（Action）] ドロップダウン メニュー（デバイス 360 ビューの右上にある）から [N ホップ トポロジ（N-Hop Topology）] を選択します。

ステップ 3 必要な情報が表示されるようにポップアップ ウィンドウを調整します。

- 編集アイコンをクリックします。
- [ホップ（Hop）] ドロップダウン リストから、ホップ カウント（1 ～ 3）を選択します。
- [レイアウト（Layout）] ドロップダウン リストから、トポロジ マップのレイアウトを選択します。

ステップ 4 変更を保存し、パン ツールとズーム ツールを使用して結果を表示します。

ネットワークのハードウェア インベントリの表示

次の手順を使用して、ネットワーク内のすべてのデバイスに関する基本的なハードウェア情報（製品名、物理ロケーション、シリアル番号、製造日など）を表示します。

ステップ 1 デバイス レベルの情報を表示する手順は次のとおりです。

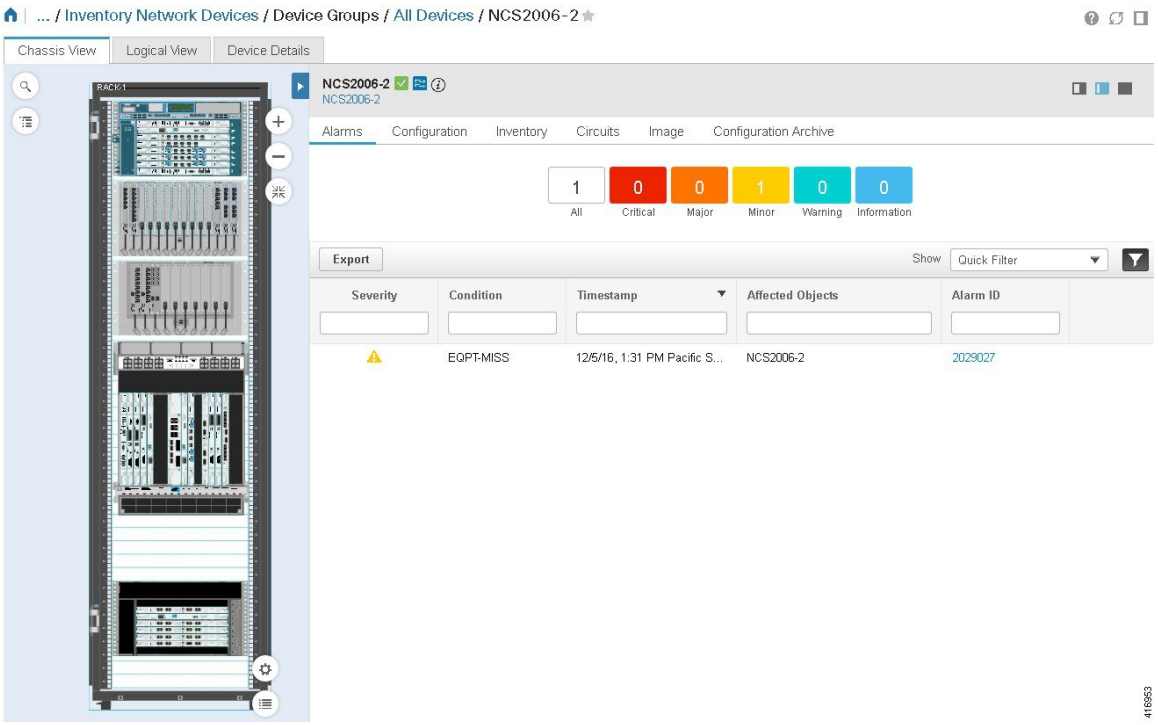
1. **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークインベントリ（Network Inventory）]** を選択します。
2. [クイックフィルタ（Quick Filter）] を使用して、特定のデバイスを検索します。たとえば、すべての ASR デバイスのハードウェア情報を一覧表示するには、[製品名（Product Name）] フィールドに ***ASR*** と入力します。

ステップ 2 要素レベルの情報を表示するには、次のいずれかの方法を使用します。

- [デバイスの詳細（Device Details）] ページから情報を取得します。完全なデバイス情報の取得：[デバイスの詳細（Device Details）] ページ （113 ページ）を参照してください。
- [シャーシビュー（Chassis View）] から情報を取得します。シャーシ ビューを開く （117 ページ）を参照してください。
- ハードウェア レポートを実行します。デバイス レポート （376 ページ） を参照してください。

完全なデバイス情報の取得：[デバイスの詳細（Device Details）] ページ

デバイスに関する最も包括的な情報については、[デバイスの詳細（Device Details）] ページを参照してください。詳細なインベントリ情報と設定オプションが表示されます。



[デバイスの詳細（Device Details）] ページを起動するには、次の手順を実行します。

- [デバイス360（Device 360）] ビューから：IP アドレスのハイパーリンクをクリックするか、または **[表示（View）]** > **[詳細（Details）]** を選択します。
- ネットワーク デバイス テーブルから：デバイス テーブルのデバイス名のハイパーリンクをクリックします。

ここに表示されるタブは、[シャーシビュー（Chassis View）] での選択によって異なります。次の表でタブについて説明します。

タブ名	説明
シャーシビュー（Chassis View）	選択された要素の状況に当てはまるインベントリ、サービス、およびアラーム情報を提供します。また、設定、イメージ管理、および設定アーカイブ機能の起動ポイントとしても機能します（論理要素を設定するには、[論理ビュー（Logical View）] タブをクリックします）。 シャーシ ビュー機能の使用方法については、[シャーシビュー（Chassis View）] ウィンドウの概要 （119 ページ）を参照してください。
論理ビュー（Logical View）	論理インベントリ情報を提供します。また、論理要素用の設定オプションも提供します。

タブ名	説明
デバイスの詳細（Device Details）	システム情報（環境、モジュール ポート、インターフェイス、およびその他の設定）を提供します。[概要（Summary）] ページには、デバイスのすべての CPU の平均使用率と、すべてのメモリ コンポーネントの平均使用率を示すグラフが表示されます。
アラーム（Alarms）	デバイス、カード、またはポートで発生したアラームに関する情報を取得します。アラームの詳細を表示する （327 ページ）を参照してください。
設定（Configuration）	デバイス、カード、またはポートを設定します。要素は、物理的な場所でグループ分けされます（論理機能に基づいてグループ分けされた要素を設定するには、[論理ビュー（Logical View）] タブをクリックします）。Cisco Evolved Programmable Network Manager を使用してデバイスを設定する方法 （396 ページ）を参照してください。
インベントリ（Inventory）	デバイスまたはカードのシリアル番号や製造年月日などの詳細なハードウェア情報を表示します。
インターフェイス（Interfaces）	デバイス、カード、またはポート上で設定されたインターフェイスのステータスを表示します。ここでは、特定のインターフェイスの [インターフェイス 360（Interface 360）] ビューを開くこともできます。Cisco EPN Manager でインターフェイス情報を表示する他の方法に関するトピックへのリンクについては、「デバイス インターフェイスの表示」を参照してください。

タブ名	説明
パフォーマンス（Performance）	概要情報とパフォーマンス測定指標の概略を表示します。次の点に注意してください。 • Cisco cBR-8（コンバージド ブロードバンド ルータ 8）ルータ以外のデバイスのシャーシ ビューを表示している場合は、選択したインターフェイスのカードまたはポートに関する情報が表示されます。[インターフェイスの詳細情報（Interface Details）] ダッシュレットのほかに表示されるダッシュレットは、選択されたインターフェイス タイプによって異なります。[インターフェイス（Interface）] ドロップダウン リストでインターフェイスを選択したら、必ず、[適用（Apply）] をクリックして表示された情報を更新します。 • Cisco cBR-8 ルータのシャーシ ビューを表示している場合は、デバイス全体の情報も表示されます。発信された音声通話の数やアップストリーム/ダウンストリーム使用率などの情報を提供するダッシュレットを表示できます。ネットワーク内の Cisco cBR-8 ルータの情報を収集してレポートするには、[ケーブルポリシー（Cable Policies）] が [モニターリングポリシー（Monitoring Policies）] ページ（**[モニター（Monitor）] > [モニターリングツール（Monitoring Tools）] > [モニターリングポリシー（Monitoring Policies）] > [ポリシー（Policies）]** ペイン）に表示され、現在アクティブであり、そのパラメータのポーリング間隔が設定されていることを確認します。 （注） [パフォーマンス（Performance）] タブには、特定の時点のダッシュレットを最大 10 個表示できます。これらのダッシュレットは、ペインの右上隅にある [設定（Settings）] アイコンをクリックし、[ダッシュレットの追加（Add Dashlet(s)）] オプションを使用して選択します。
回線（Circuits）	デバイス、カード、またはポートが参加している回線を表示します。Cisco EPN Manager で回線情報を表示する他の方法に関するトピックへのリンクについては、「回線/VC の表示」を参照してください。
イメージ（Image）	デバイス上で動作しているソフトウェア イメージを管理します。「イメージ リポジトリに保存されたイメージを表示する」を参照してください。 （注） このタブは、最上位シャーシが選択されている場合にのみ使用できます。
設定アーカイブ（Configuration Archive）	デバイス上で動作しているデバイス コンフィギュレーション ファイルを管理します。「すべてのアーカイブされたファイルを表示する」を参照してください。 （注） このタブは、最上位シャーシが選択されている場合にのみ使用できます。

[シャーシビュー（Chassis View）] を使用したデバイスの表示と管理

[シャーシビュー（Chassis View）] には、デバイス シャーシとそのハードウェア要素のインタラクティブ モデルが表示されます。[シャーシビュー（Chassis View）] では次の操作が可能です。

- シャーシの内容を表示する。
- シャーシ要素の状態を確認し、問題を迅速に特定する。
- アラームが発生した要素を表示し、アラームの詳細を提供するビューを起動する。
- [デバイスの詳細（Device Details）] ページを開く起動ポイントを使用してインターフェイスを設定する。

[シャーシビュー（Chassis View）] に表示される要素は、デバイス タイプと、デバイスに設定されている要素によって異なります。

デフォルトでは、管理ユーザーにシャーシ ビューへの読み取り/書き込みアクセス権がないことに注意してください。このユーザー グループのアクセスを有効にするには、[ユーザー、ロール、およびAAA（Users, Roles & AAA）] ページを開いて [ユーザーグループ（User Groups）] を選択し、[タスク権限（Tasks Permissions）] タブの [ネットワークモニターリング（Network Monitoring）] にある [シャーシビューの読み取りと書き込み（Chassis View Read and Write）] チェック ボックスをオンにします。

「グループで実行できるタスクを表示および変更する」を参照してください。

[シャーシビュー（Chassis View）] の起動および使用方法については、次のトピックを参照してください。

シャーシ ビューを開く

次の表で、シャーシビューを開く際に使用できる、さまざまな方法を説明します。デバイスがこれらの起動ポイントを提供していない場合、それはデバイスがシャーシ ビューをサポートしていないことを意味します。シャーシ ビューをサポートするデバイスの一覧については、https://www.cisco.com/c/en/us/support/cloud-systems-management/evolved-programmable-network-epn-manager/products-device-support-tables-list.htmlを参照してください。

シャーシビューを開くための場所	次の手順を実行します。	シャーシ ビューの表示場所
[ネットワークデバイス（Network Devices）] テーブル	デバイスの IP アドレスの横にある をクリックします。	ポップアップ ウィンドウ
	デバイス名のハイパーリンクをクリックします。	フルページ ビュー
[デバイス360度（Device 360）] ビュー	[デバイス 360 度（Device 360）] ビューの右上で、**[表示（View）] > [シャーシ ビュー（Chassis View）]** の順に選択します。	ポップアップ ウィンドウ
	[デバイス360（Device 360）] ビューの右上から、**[表示（View）] > [詳細（Details）]** の順に選択します。	フルページ ビュー
[デバイスの詳細（Device Details）] ページ	[シャーシ ビュー（Chassis View）] タブをクリックします。	フルページ ビュー

[シャーシビュー（Chassis View）] ポップアップ ウィンドウからフルページの [シャーシビュー（Chassis View）] を開くには、ウィンドウの右上隅にある [起動設定（Launch Configuration）] リンクをクリックします。

[シャーシビュー（ChassisView）]を使用したデバイスの表示および設定に必要な権限

次の表で、Cisco EPN Manager ユーザー グループのメンバーに付与される [シャーシビュー（Chassis View）] の権限について説明します。これらの権限は編集できません。ユーザー グループの詳細については、を参照してください。 ユーザーが実行できるタスク Web インターフェイスの制御 （999 ページ）

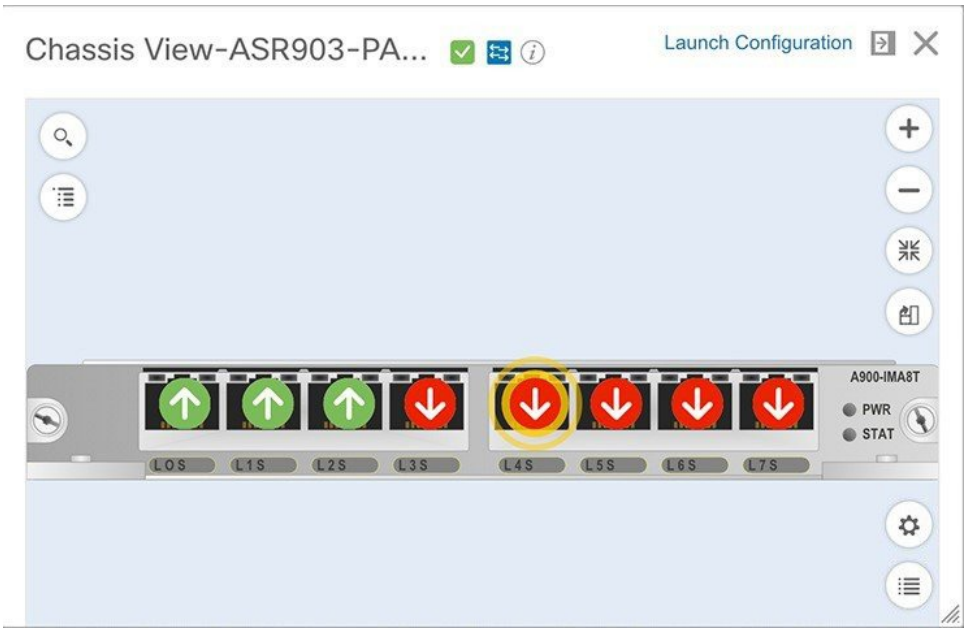
- フル アクセス（読み取りと書き込み）：このグループのユーザーは、[シャーシビュー（Chassis View）] を使用してデバイスを表示および設定できます。
- 読み取り専用アクセス：このグループのユーザーは、[シャーシビュー（Chassis View）] を使用してデバイスを表示することはできますが、設定することはできません。
- 書き込み専用アクセス：このグループのユーザーは、[シャーシビュー（Chassis View）] を使用してデバイスを設定することはできますが、表示することはできません（NBI Write グループにのみ適用されます）。
- アクセスなし：このグループのユーザーは [シャーシビュー（Chassis View）] にアクセスすることも、ビューを使用することもできません。

グループ タイプ		読み取り	書き込み
Web UI	Root	X	X
	スーパーユーザー	X	X
	管理者	—	—
	Config Managers	X	X
	System Monitoring	X	—
	User-Defined 1 ～ 4	X	—
	Monitor Lite	X	—
NBI	NBI Read	X	—
	NBI Write	—	X
	North Bound API	X	X

[シャーシビュー（Chassis View）] ウィンドウの概要

次の図は、Cisco ASR 903 ルータの [シャーシビュー（Chassis View）] を示しています。

この例では、ユーザーは、現在ダウンしているポートをクリックしました。



[シャーシビュー（Chassis View）] が更新され、ポートが常駐しているライン カード モジュールだけが表示され、そのモジュールが拡大表示されます。[シャーシビュー（Chassis View）] でポートが脈動するので、ユーザーはそのポートを見つけやすくなります。このモジュールのポートに表示されているバッジは、それらのポートのプライマリステータスを示します（ポートまたはインターフェイスの状態（123 ページ）を参照）。一部の要素は、状態（アウトオブサービス、プロビジョニングされる前など）を示す色付きの線で囲まれている場合があります。バッジやその他のインジケータの意味を説明するキーを開くには、[シャーシビュー（Chassis View）] の右下にある をクリックします。

デバイスに複数のシャーシまたはシェルフがある場合は、各シャーシまたはシェルフが同じ [シャーシビュー（Chassis View）] に表示されます（例については [シャーシビュー（Chassis View）] での混在シャーシ、マルチシャーシ、およびマルチシェルフ デバイスの表示（125 ページ）を参照）。カード イメージを取得できない場合、[シャーシビュー（Chassis View）] のカード名のそばに疑問符が表示されます。

シャーシビューに表示されるラックの数を制御する GUI の表示設定をカスタマイズできます。手順は次のとおりです。

1. Cisco EPN Manager ウィンドウの右上をクリックし、[マイプリファランス（My Preferences）] を選択します。
2. [シャーシビューの設定（Chassis View Configuration）] で、[表示するシャーシラック（Chassis racks to display）] ドロップダウンリストから値を選択します。指定した数によって、シャーシビューに表示されるラックの数が決まります。デフォルト値は 2 です。

ロード時間を短縮するため、ラック情報はデフォルトでは表示されません。関連するラック情報を表示するには、ダウンロードボタン（ラックに表示）をクリックする必要があります。

次の点に注意してください。

- [シャーシビュー（Chassis View）] には Cisco EPN Manager でパッケージ化された汎用イメージが表示されるため、[シャーシビュー（Chassis View）] に表示される色は物理デバイスと一致しない場合があります。
- セキュア ドメイン ルータ（SDR）を収容する Cisco NCS 6000 デバイスの [シャーシビュー（Chassis View）] を開いている場合、デバイス タイプと SDR の名前の両方が [シャーシビュー（Chassis View）] の上部に表示されます。クラスタまたはユーザー定義グループに属するデバイスの SDR ラベルが表示されない（自動クラスタリングがデバイスのプロキシミティに基づいて適用されるため）ことがある点に注意してください。

次の表に、[シャーシ ビュー（Chassis View）] のコンポーネントとその機能を示します。

[シャーシビュー（Chassis View）] のコンポーネント	**説明**
	デバイス上の特定のラック、シェルフ、モジュール、またはインターフェイスを検索するために使用できるフィールドを開きます。
	[シャーシ エクスプローラ（Chassis Explorer）] を開きます。
	デバイスの到達可能性状態を示します（「デバイスの到達可能性状態と管理状態（84 ページ）」を参照）。この例は、デバイスが到達可能であることを示しています。
	デバイスの管理ステータスを示します（「デバイスの到達可能性状態と管理状態（84 ページ）」を参照）。この例は、デバイスが管理されていることを示しています。
	デバイスの [デバイス 360（Device 360）] ビューを開きます。「基本デバイス情報を取得する：[デバイス 360（Device 360）] ビュー」を参照してください。
[起動設定（Launch Configuration）] リンク	デバイスの [デバイスの詳細（Device Details）] ページを開きます。このページに表示されるタブは、デバイス、モジュール、またはポートが [シャーシビュー（Chassis View）] で現在選択されているかどうかによって異なります。「完全なデバイス情報の取得：[デバイスの詳細（Device Details）] ページ」を参照してください。
	[ドック（Dock）] ウィンドウに、デバイスの [シャーシ ビュー（Chassis View）] へのショートカットを追加します。「[ドック（Dock）] ウィンドウのカスタマイズ」を参照してください。
	[シャーシ ビュー（Chassis View）] を閉じます。
	イメージをズーム インします。

[シャーシビュー（Chassis View）] のコンポーネント	説明
	イメージをズーム アウトします。
	[シャーシ ビュー（Chassis View）] 内でイメージ全体を見ることができるようにイメージのサイズを変更します。
	この機能をサポートするデバイスの前面と背面の [シャーシビュー（Chassis View）] を切り替えます。このアイコンの上にカーソルを置いたときに表示される吹き出しは、開いているビューを示します。 この機能は、次の Cisco デバイスでサポートされています。 • ASR 901S • cBR-8 • NCS 1001、1002、5001、5002、および 5008
	現在表示されているモジュールのイメージを回転します。このアイコンは、デバイス全体が表示されている場合は使用できません。
	クリックすると、[アラームの点滅を有効化（Enable Alarm Blinking）] チェックボックスにアクセスできます。このチェックボックスをオンにすると、注意を引きつけて見つけやすくするために、モジュールまたはポートに表示されているアラームバッジが点滅します。
	[シャーシビュー（Chassis View）] に表示されるバッジと色付きの線の重要性を説明するキーを開きます。

[シャーシビュー（ChassisView）]でのネットワーク要素の状態に関する情報の表示

バッジ、線、および色は、デバイスの動作状態、要素、およびコンポーネントに関する情報を提供します。[シャーシビュー（Chassis View）] の右下にある [凡例（Legends）] アイコンをクリックすると、バッジ、線、色の意味を一覧表示するキーが表示されます。

詳細については、次のトピックを参照してください。

- 機器の動作状態（シャーシ ビュー） （123 ページ）
- ポートまたはインターフェイスの状態 （123 ページ）

（注） A9K-400G-DWDM-TR ライン カードの CFP ポートはまだサポートされていないため、ポートの状態情報は表示されません。

機器の動作状態（シャーシ ビュー）

機器の動作状態はネットワーク要素の実行状態を表しています。

機器の動作状態	アイコン	説明
サービス中（In Service）	（なし）	機器が正常に動作しています。
事前プロビジョニング済み		（Cisco NCS 2000 および Cisco ONS デバイスのみ）機器は設定されていますが、シャーシには物理的に存在していません。
失敗/無効/ダウン/休止中/メンテナンス中のため休止中		機器は正常に動作していません。
不明		機器の動作状態は不明です。デバイスからの応答はありません（または不十分な応答）。

ポートまたはインターフェイスの状態

ポートまたはインターフェイスのプライマリ状態：管理者と運用状態を組み合わせることでポートまたはインターフェイスの最も重要な状態情報を伝えます。[多層トレース（Multilayer Trace）]には、ポートのプライマリ状態またはアラーム状態が表示されます。[シャーシビュー（Chassis View）]の場合は、要素が状態変化を示す色の変化をサポートしていない場合でも、生成されたアラームから状態変更情報を取得できます。

（注） ポート/インターフェイスにアラームが関連付けられている場合、アラーム アイコンが表示され、ポートアイコンは表示されません。このアラームは、ポートがテスト中または管理ダウン状態でない場合にのみ表示されます。

ポートまたはインターフェイスのプライマリ状態	アイコン	管理ステータス	動作状態
不明		不明	不明
ダウン		アップ	ダウン
テスト		テスト	—

管理上ダウン		管理上ダウン	—
アップ		アップ	アップ
自動アップ		アップ	自動アップ

ポートまたはインターフェイスの管理状態：ポートまたはインターフェイスの設定状態を表します（たとえば、管理者が手動でポートをシャットダウンした場合など）。

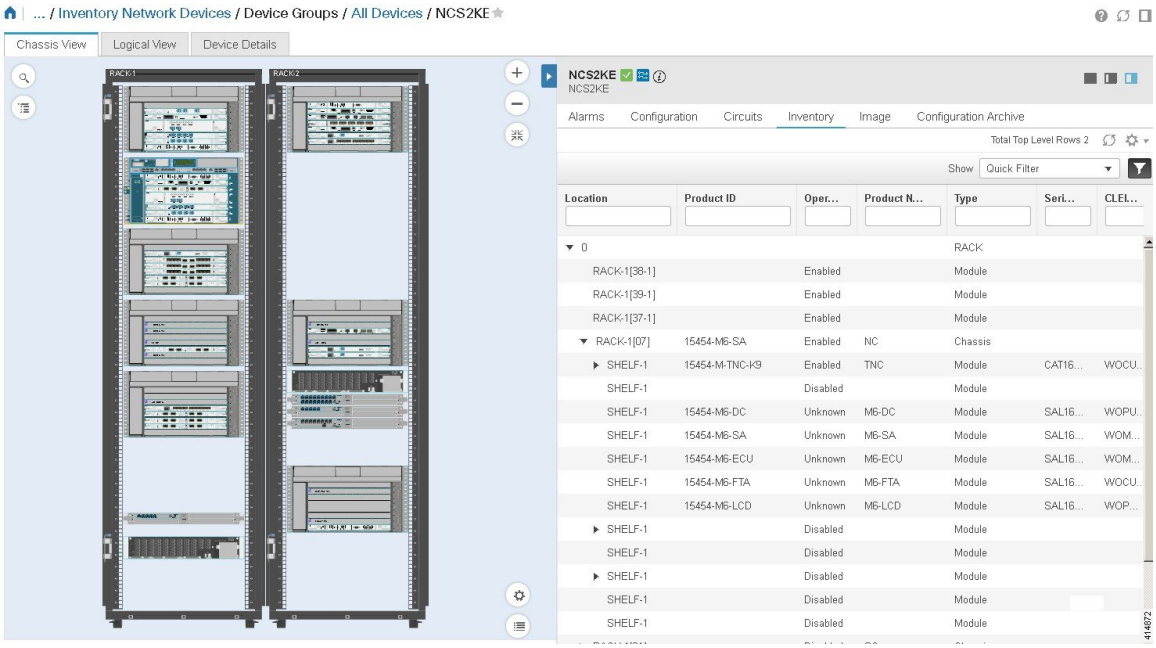
ポートまたはインターフェイスの管理状態	アイコン	説明
不明		ポートまたはインターフェイスの管理状態は不明です。デバイスからの応答（または不十分な応答）はありません。
管理上ダウン		ポートまたはインターフェイスは管理者によって手動でシャットダウンされました。
アップ		ポートまたはインターフェイスは管理者によって有効にされています。
テスト		ポートまたはインターフェイスは管理者によってテストされています。

ポートまたはインターフェイスの動作状態：ポートまたはインターフェイスの実行状態と、それが適切に動作しているかどうかを伝えます。

ポートまたはインターフェイスの動作状態	アイコン	説明
不明		ポートまたはインターフェイスの動作状態は不明です。デバイスからの応答（または不十分な応答）はありません。
ダウン		ポートまたはインターフェイスは正しく動作していません。
アップ		ポートまたはインターフェイスがデータを送受信しています。
自動アップ		ポートまたはインターフェイスがデータを送受信しています（特定のデバイスのみがこの状態をサポートしています。他のデバイスは [アップ（Up）] を使用します）。

[シャーシビュー（Chassis View）] での混在シャーシ、マルチシャーシ、およびマルチシェルフ デバイスの表示

次の例に、Cisco NCS 2000 シャーシと Cisco ONS 15454 シャーシの両方を備えた混合 [シャーシビュー（Chassis View）] を示します。シャーシのタイプが異なるため、シェルフ番号は連続していません。



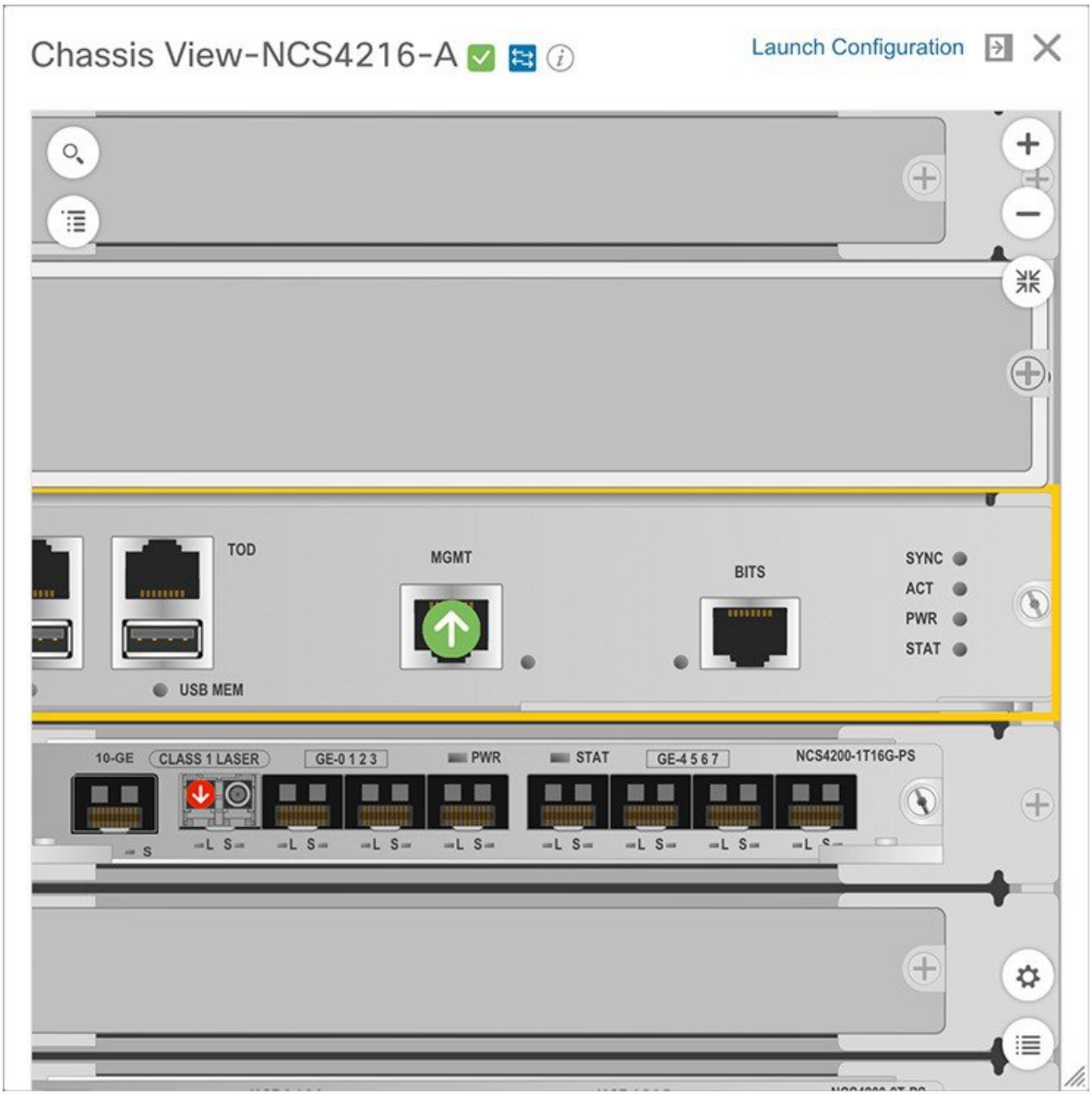
混合シャーシ、マルチシャーシ、およびマルチシェルフ デバイスの場合は、シャーシ ビューでのアラームの表示 （125 ページ） で説明しているとおり、Cisco EPN Manager はシャーシまたはシェルフにアラームを集約します。

クラスタ内のマルチシャーシ デバイスの場合、[デバイス360（Device 360）] ビューの [シャーシ（Chassis）] タブでは、どのシャーシがプライマリで、どのシャーシがバックアップであるかが識別されます。

（注） マルチシェルフ デバイス用に開いた [シャーシビュー（Chassis View）] には、最初の 4 台のラックのみが表示されます。関連するラック情報を表示するには、ユーザーがダウンロードボタン（ラック番号 5 以上に表示）をクリックする必要があります。

シャーシ ビューでのアラームの表示

[シャーシ ビュー（Chassis View）] のアラーム バッジは、機器にローカライズされた 1 つ以上のアラームを表します。複数のアラームを持つ要素に、バッジアイコンは最も重大な警告を伝えます



（注意をひくため）アラーム アイコンが点滅するようにシャーシ ビューをカスタマイズするには、ビューの右下の をクリックしてから、[アラームの点滅を有効にする（Enable Alarm Blinking）] チェック ボックスをオンにします。

（注） ポート/インターフェイスにアラームが関連付けられている場合、アラーム アイコンが表示され、ポート アイコンは表示されません。このアラームは、ポートがテスト中または管理ダウン状態でない場合にのみ表示されます。

デバイスに固有のアラームを表示するには、次の手順を実行します。

ステップ 1 デバイスのシャーシ ビューを開いて、[設定の起動（Launch Configuration）] リンクをクリックします。

[デバイスの詳細（Device Details）] ページが開きます。

ステップ 2 選択していない場合は、[アラーム（Alarms）] タブをクリックします。

そのデバイスに関して発生しているすべてのアラームがここに表示されます。

ステップ 3 （ラインカードやポートなど）特定のデバイス コンポーネントのアラームを表示するには、次のいずれかを実行します。

- シャーシ ビューのコンポーネントをダブルクリックします。
-  をクリックして [シャーシエクスプローラ（Chassis Explorer）] を開き、そのエントリをクリックします。

[シャーシビュー（Chassis View）] での回線ルートの表示

回線に参加しているデバイスの [シャーシビュー（Chassis View）] を使用して、回線のエンドツーエンドの物理ルートを表示できます。また、回線の電力レベルとスパン損失を表示することもできます。

（注） この機能は OCH WSON 光回線タイプにのみ使用できます。

ステップ 1 左側のサイドバーで、**[インベントリ（Inventory）]**>**[デバイス管理（Device Management）]**>**[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 [ネットワークデバイス（Networks Devices）] テーブルで、目的のデバイス名のハイパーリンクをクリックし、[シャーシビュー（Chassis View）] のフルページ ビューを開きます。

ステップ 3 [シャーシビューエクスプローラ（Chassis View Explorer）] を展開してシェルフを選択します。

ステップ 4 右ペインの [回線（Circuits）] サブタブをクリックし、物理ルートを表示する回線を選択します。

[シャーシビュー（Chassis View）] に回線の物理ルートが表示されます。同じカードのポート間の内部接続は、点線で表示されます。

ステップ 5 左ペインで[シャーシビュー（Chassis View）]の横にある目のアイコンをクリックして、物理ルート、電力レベル、およびスパン損失を表示または非表示にします。

デバイス ポートの表示

デバイスの物理ポートに関する詳細情報は、[デバイスの詳細（Device Details）] ページから取得できます。また、さまざまな 360 ビューで基本的なポート情報を確認できます。

モジュールとポートを備えたデバイス シャーシを表示するには、[シャーシビュー（Chassis View）] を使用します。シャーシ ビューを開く （117 ページ）を参照してください。

情報を表示する対象ポート	次の手順を実行します。
デバイス上のすべての物理ポート（ポート エイリアスと常駐モジュールを含む）	1. [デバイスの詳細（Device Details）] ページを開きます。 • [デバイス360（Device 360）] ビューの右上で、**[表示（View）] > [詳細（Details）]** の順に選択します。 • デバイス テーブルにあるデバイス名のハイパーリンクをクリックします。 2. [デバイスの詳細（Device Details）] タブで、**[システム（System）] > [物理ポート（Physical Ports）] >** を選択します。.
インターフェイスのポート	360 ビューの [インターフェイス（Interface）] タブを確認します。
モジュールに接続されたポート	[デバイス360（Device 360）] ビューの [モジュール（Modules）] タブを確認します。
ネイバーに接続されたポート	[デバイス360（Device 360）] ビューの [ネイバー（Neighbors）] タブを確認します。

ポートの状態とアイコンのマトリックスについては、ポートまたはインターフェイスの状態（123 ページ）を参照してください。

デバイス インターフェイスの表示

Cisco EPN Manager は、デバイス インターフェイスを表示するための次の方法を提供しています。

インターフェイスを表示する方法	詳細については、以下を参照してください。
特定のインターフェイスに関する詳細の表示	デバイス インターフェイスの概要：[インターフェイス360（Interface 360）] ビュー （129 ページ）

特定のデバイスのインターフェイスの表示	• 特定のデバイスのインターフェイスを表示する：[デバイス 360（Device 360）] ビュー （129 ページ） • [デバイスの詳細（Device Details）] ページを使用した、デバイスのインターフェイスに関する包括的情報の取得 （134 ページ）

特定のデバイスのインターフェイスを表示する：[デバイス360（Device 360）] ビュー

[デバイス 360（Device 360）] ビューを使用すると、デバイスのインターフェイスのステータスをすばやく確認できます。

ステップ 1 [デバイス360（Device 360）] ビューを開きます。

- ほぼすべてのデバイス テーブルの IP アドレスの横にある [i] アイコンをクリックします。
- ネットワーク トポロジで、展開されたグループ内のデバイスをクリックし、[表示（View）] をクリックします。

ステップ 2 [インターフェイス（Interfaces）] タブをクリックします。

デバイス インターフェイスの概要：[インターフェイス360（Interface 360）] ビュー

[インターフェイス360（Interface 360）] ビューには、一般的なインターフェイスの詳細、インターフェイス ステータス、インターフェイスのアラーム、インターフェイスを通過する回線/VC、パフォーマンス情報など、特定のインターフェイスの概要情報が表示されます。[インターフェイス360（Interface 360）] ビューの [アクション（Actions）] メニューから、インターフェイスの有効化および無効化などの基本的なタスクを実行できます。[トポロジで表示（Show in Topology）] オプションでトポロジ マップを起動すると、マップのコンテキストにインターフェイスを表示できます。

アラーム テーブル、リンク テーブル、デバイス 360 ビューなどで、インターフェイス名の横に [i] アイコンが表示されていれば、[インターフェイス360（Interface 360）] ビューを起動できます。

[インターフェイス360（Interface 360）] ビューでは、ビュー上部にインターフェイスの一般的な情報が表示され、ビュー下部の各タブに詳細なインターフェイス情報が表示されます。[インターフェイス 360（Interface 360）] ビューに表示される情報は、インターフェイス設定に応じて異なります。

表示されるタブは、このビューを起動したインターフェイスのタイプによって異なります。たとえば光インターフェイスの場合は、光インターフェイスのタイプに応じて、[光物理（Optical Physical）] タブまたは [ODU] タブが表示されます。

（注） [インターフェイス360（Interface 360）] では、IPv6 のサポートが制限されています。

ポップアップウィンドウメニューを使用して、次のタスクを実行することもできます。

- [自動更新（Auto-Refresh）]：ステータスとトラブルシューティングをリアルタイムで更新する場合は、[更新（Refresh）] アイコンをクリックしてオンデマンド更新を有効にします。または、ドロップダウンリストから、自動更新の間隔を 30 秒、1 分、2 分、または 5 分に設定することもできます。デフォルトでは、自動更新はオフになっています。

（注） 自動更新設定は、現在開いている [360° ビュー（360° View）] ポップアップウィンドウにのみ適用されます。このビューを閉じてからもう一度開いた場合または別のビューを開いた場合は、デフォルトでは自動更新がオフになります。

- インターフェイスが関連付けられているポートまたはライン カードを強調表示するシャーシ ビューを開きます（[表示（View）] メニュー）。この機能は、現場の技術者に問題の原因となっている箇所を説明する必要がある場合に便利です。
- 発生したアラームや関連付けられている回線および VC の現在のステータスなどの情報に基づいて、別のインターフェイスと対照比較するインターフェイスを選択します（[アクション（Actions）] メニュー）。インターフェイスの情報とステータスを比較する （133 ページ）を参照してください。
- [表示（View）] > [パフォーマンス（Performance）] を選択して、特定のインターフェイスタイプの関連するパフォーマンス ダッシュボードにパフォーマンス情報を表示します。
- [アクション（Actions）] メニューからインターフェイスを有効または無効にします。
- [アクション（Actions）] メニューから MPLS インターフェイスのロックアウトを有効または無効にします。インターフェイスが属している MPLS TE トンネルリンクの保守作業を行う前に、MPLS インターフェイスをロックアウトします。[インターフェイス360（Interface 360）] ビューをいったん閉じて再度開き、更新された詳細を確認します。

（注） MPLS ロックアウトは、トンネルインターフェイスには適用されません。

MPLS ロックアウトは、EPNM で有効な検出済み MPLS リンクがあるインターフェイスにのみ適用されます。

- インターフェイスが配置されているデバイスをトポロジ マップで表示します（[アクション（Actions）] メニュー）。
- **[アクション（Actions）]** メニューからインターフェイスを有効または無効にします。
- **[アクション（Actions）]** メニューから AINS で有効にします。
- **[アクション（Actions）]** > **[ポートの移行（Migrate Port）]** を使用して、ポート間でポート設定をコピーしてアクティブ化します。この操作は XR デバイスでのみサポートされています。この操作の実行中は、空の宛先ポートのみを選択できます（ポートには設定は存在しません）。**show running-config interface** <宛先ポート> コマンドを使用して、宛先ポートが空であることを確認します。操作が成功すると、送信元ポートがシャットダウンされます。
  - 送信元ポートと宛て先ポートの両方を同じにすることはできません。
  - 送信元ポートと宛先ポートは異なるカードのものにすることができますが、同じタイプである必要があります（たとえば、送信元ポートがギガビットイーサネットの場合は宛先ポートもギガビットイーサネットである必要があります）。
  - ポートの移行操作は、イーサネット物理ポートにのみ適用されます。

  ポートの移行操作を実行する前に、デバイスをメンテナンスモードに移すことを推奨します。この操作は、XR プラットフォームによって提供される機能に基づいています。デバイスは **replace** CLI コマンドをサポートしている必要があります。

警告 サービスエンドポイントが設定されているポート設定を移行すると、意図した目的と検出されるサービスとの間にギャップが生じます。サービスエンドポイントの変更を調整することはできないため、サービスの調整によってこの問題に対処することはできません。

- 移行されたポートのアラームをクリアするために、次の API を使用できます。

```
https://<Server
IP>/webacs/alarm-rest/ClearAlarmsByPort?portName=<Port_Name>&deviceIp=<Device IP>
```

  それぞれの説明は次のとおりです。
  - **<Server IP>** は、サーバーの IP アドレスです。
  - **<Port_Name>** は、デバイスが設定されているポートの名前です。
  - **<Device IP>** は、デバイスの IP アドレスです。

- トラブルシューティングの目的で、光インターフェイス（光物理インターフェイスを除く）のパフォーマンスデータのベースラインを設定します。詳細については、「光パフォーマンス データのベースラインの設定 （134 ページ）」を参照してください。

- 動作中インターフェイスからデバイス上のプロテクションインターフェイスへのパターン切り替えを設定するには、[アクション（Actions）] メニューにある [UPSR/SNCPプロテクション（UPSR/SNCP Protection）] オプションを使用します。このオプションは、動作中インターフェイスとプロテクションインターフェイスが設定されているデバイスの場合にのみ、GUI で使用できます。Cisco EPN Manager はユーザー設定に基づいて、インベントリデータベースとデバイスインターフェイスとの定期的な同期を実行します。インターフェイスを切り替える操作は次の順序で進みます。
  - [ロックアウト（Lockout）]：動作中インターフェイスがプロテクションインターフェイスに切り替わるのを防ぎます。
  - [保護を強制（Force Protect）]：保護インターフェイスに切り替えます。
  - [ワーキングを強制（Force Working）]：ワーキングインターフェイスに切り替えます。
  - [手動で保護（Manual Protect）]：手動で保護インターフェイスに切り替えます。
  - [手動で動作中（Manual Working）]：手動で動作中インターフェイスに切り替えます。
  - [クリア（Clear）]：以前に設定された外部コマンドをクリアします。

[インターフェイス360（Interface 360）] ビューに表示される情報	説明
一般情報	インターフェイス名、ステータス、説明、タイプ、デバイス名、IPアドレス、MAC アドレスなど。
パフォーマンスデータ	[表示（View）]>[パフォーマンス（Performance）] から関連するパフォーマンス ダッシュボードへの起動ポイント。
アラーム	インターフェイスの現在のアラーム、アラームの重大度、ステータス、および生成時刻。また、アラーム ブラウザの起動ポイントも示されます。
インターフェイス	関連付けられている各インターフェイスの名前、インターフェイスタイプ、動作および管理ステータス。また、[インターフェイス360（Interface 360）] ビューの起動ポイントも示されます。
回線/VC	（回線に参加しているインターフェイスの場合）回線/VC の名前、タイプ、顧客、ステータス、および作成日。また、[回線/VC 360（Circuit/VC 360）] ビューの起動ポイントも示されます。
EFP	インターフェイスに関連付けられているすべてのEFP（該当する場合）。また、動作ステータス、管理ステータス、およびEFPタイプも示されます。

特定のインターフェイス タイプに関連する詳細情報	光物理、ODU、FECなど、インターフェイスのタイプに関連するタブの追加のインターフェイス情報とパフォーマンス データ。
光物理	インターフェイスのリアルタイム パフォーマンス モニターリング データ。このデータは10秒ごとに収集され、直近12回分のポーリング結果がここに表示されます。表示できるカウンタの一覧については、「光モニターリング ポリシーのパフォーマンス カウンタ」を参照してください。

インターフェイスの情報とステータスを比較する

[比較ビュー（Comparison View）]ページでは、複数のインターフェイスの対照比較を実行し、IP アドレスと MAC アドレス、発生したアラーム、関連する回線と VC などの情報を表示できます。インターフェイスを比較するには、次の手順を実行します。

ステップ 1 比較するインターフェイスごとに、次の手順を実行します。

a) デバイスインターフェイスの概要：[インターフェイス360（Interface 360）] ビュー（129ページ）の説明に従って、[インターフェイス360（Interface 360）] ビューを開きます。

b) **[アクション（Actions）]** > **[追加して比較（Add to Compare）]** を選択します。

選択したインターフェイスがページの下部に表示されます。最大 4 つのインターフェイスを選択できます。

ステップ 2 [比較（Compare）] をクリックします。

[比較ビュー（Comparison View）] ページが開きます。

ステップ 3 ビュー上部にあるドロップダウンリストで、利用可能なすべての情報を表示するか、インターフェイスごとに一意の情報だけを表示するかを指定します。

ステップ 4 [ビューのカスタマイズ（Customize View）]をクリックして、ビューに表示するカテゴリのチェックボックスをオンにしてから、[保存（Save）] をクリックします。

デフォルトでは、すべてのカテゴリが選択されています。

ステップ 5 選択したカテゴリごとに提供される情報が表示されるようにページをスクロール ダウンします。

次の点に注意してください。

- [比較ビュー（Comparison View）] には、一度に 2 つのインターフェイスに関する情報しか表示されません。3 つ以上を選択した場合は、現在表示されていないインターフェイスに切り替える必要があります。
- 選択したインターフェイスの順序を変更するには、[再整理（Rearrange）] をクリックします。
- 各インターフェイスの [表示（View）] メニューと [アクション（Actions）] メニューは、[インターフェイス360（Interface 360）] ビューで提供されるものと同じです。オプションを選択すると、対応するページが開きます。

- 必要に応じて、表示されるカテゴリを最小化または最大化できます。
- [比較ビュー（Comparison View）] は、回線および VC、デバイス、およびリンクでも利用できます。それぞれの 360 ビューからこれらの要素のいずれかを比較用に選択すると、対応するタブにその要素が表示されます。これにより、必要に応じて要素のタイプを切り替えることができます。
- インターフェイスの比較を終了する場合は、ページの上部にある [戻る（Back）] をクリックしてから、ページの下部にある [すべての項目をクリア（Clear All Items）] をクリックします。他の要素タイプのタブが表示されている場合は、それらのタブもクリアする必要があります。

[デバイスの詳細（Device Details）] ページを使用した、デバイスのインターフェイスに関する包括的情報の取得

デバイス上に設定されているすべてのインターフェイスに関する幅広い情報を取得するには、[デバイスの詳細（Device Details）] ページを使用します。簡単にナビゲーションできるよう、インターフェイスはタイプ別にグループ化されています。

ステップ 1 [デバイスの詳細（Device Details）] ページを開きます。

- テーブル内のデバイスの多くに表示される、デバイス名のハイパーリンクをクリックします。
- デバイスの 360 度ビューの右上で、**[表示（View）]** > **[詳細（Details）]** の順に選択します。

ステップ 2 [デバイスの詳細（Device Details）] タブで [インターフェイス（Interfaces）] をダブルクリックし、デバイスに設定されている（全タイプの）すべてのインターフェイスのリストを表示します。

ステップ 3 同じタイプのすべてのインターフェイスを表示するには、タイプ（[イーサネットインターフェイス（Ethernet Interfaces）] など）をクリックします。

ステップ 4 特定のインターフェイスについての詳細を表示するには、インターフェイス名のハイパーリンクをクリックします。

光パフォーマンス データのベースラインの設定

光インターフェイス パフォーマンス データのベースラインを設定すると、リアルタイム ネットワーク パフォーマンスと固定のパフォーマンス統計セットの比較が可能になります。この方法で、通常のベースライン ネットワーク パフォーマンスと異常なネットワーク動作を比較できます。

ベースラインを設定すると、ベースライン値に基づいて新着のパフォーマンス統計がすべて再計算され、ベースライン値と現在のリアルタイム値の差（具体的には現在の値からベースライン値を引いた値）が表示されます。

この機能をサポートする光インターフェイスは、[インターフェイス360（Interface 360）] ビューの関連タブに [ベースラインの設定（Set Baseline）] ボタンがあります。

光インターフェイスのパフォーマンス統計のベースラインを設定する手順は次のとおりです。

ステップ 1 関連インターフェイスの [インターフェイス360（Interface 360）] ビューを開きます。

ステップ 2 インターフェイス タイプ（FEC、OTU など）に固有のタブを開きます。

ステップ 3 [ベースラインの設定（Set Baseline）] ボタンをクリックします。

テーブル内の行がクリアされます。新しい各行には、ベースライン値と現在のリアルタイム値の差を反映した値が表示されます。

ステップ 4 リアルタイム値に戻る（ベースラインを実質的に削除する）には、[インターフェイス360（Interface 360）] ビューを閉じてから再度開きます。

デバイス モジュールの表示

デバイス モジュール情報を表示するには、[インベントリ（Inventory）]>[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択し、必要な情報量に応じて [デバイス360（Device 360）] または [デバイスの詳細（Device Details）] ページを起動します。

取得する情報	必要な操作
基本的なモジュール情報：ステータス、タイプ、ポート	[デバイス360（Device 360）] ビューで、[モジュール（Modules）] タブをクリックします。[デバイス360（Device 360）] ビューを開く方法は次のとおりです。 • ほぼすべてのデバイステーブルで IP アドレスの横にある [i] アイコンをクリックします。 • ネットワークトポロジで、展開されたビュー内のデバイスをクリックしてから、[表示（View）] をクリックします。

モジュールの機器タイプと電源の情報	[デバイスの詳細（Device Details）] ページにある [デバイスの詳細（Device Details）] タブで [システム（System）] > [モジュール（Modules）] を選択します。 [デバイスの詳細（Device Details）] ページを開く方法は次のとおりです。 • ほぼすべてのデバイステーブルに表示される、デバイス名のハイパーリンクをクリックします。 • [デバイス360（Device 360）] ビューの右上で、[表示（View）] > [詳細（Details）] の順に選択します。 （注） モジュール関連情報の取得が制限されているため、このページでは Cisco CAT6500 デバイスの SFP トランシーバが「未指定（Unspecified）」製品として表示されます。

環境情報の表示（電源装置、ファン）

電源装置やファンの詳細といった環境関連の情報は、デバイスの [デバイスの詳細（Device Details）] ページに表示されます。この情報にアクセスする手順は次のとおりです。

ステップ 1 次のいずれかを実行します。

- ほぼすべてのデバイステーブルに表示されるデバイス名のハイパーリンクをクリックし、[デバイスの詳細（Device Details）] タブをクリックします（選択されていない場合）。
- [デバイス 360（Device 360）] ビューの右上で [表示（View）] > [詳細（Details）] を選択し、[デバイスの詳細（Device Details）] タブをクリックします（選択されていない場合）。

ステップ 2 左側にある **[機能（Features）]**ペインで、**[システム（System）]** > **[環境（Environment）]** を選択します。

デバイス ネイバーの表示

ネイバー名、ポート番号、インデックス、デュプレックス設定などのデバイス ネイバー情報は、デバイスの [デバイス360（Device 360）] ビューに表示されます。

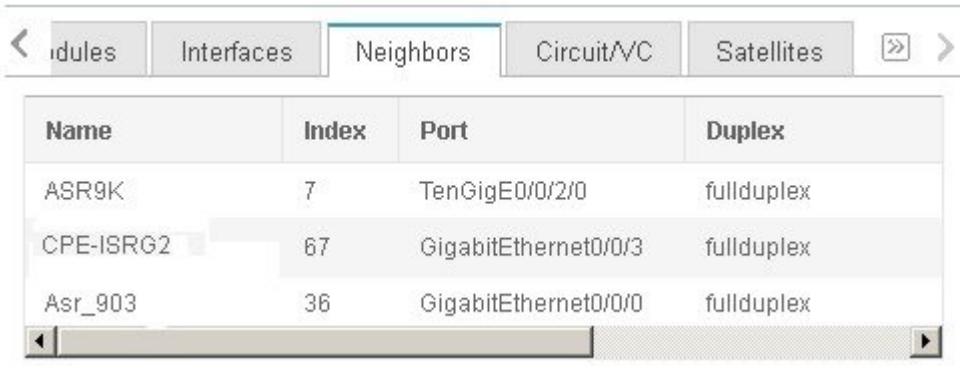
ステップ 1 [デバイス360（Device 360）] ビューを開きます。

- ほぼすべてのデバイステーブルで IP アドレスの横にある [i]（**情報**）アイコンをクリックします。
- ネットワークトポロジで、展開されたグループ内のデバイスをクリックし、[表示（View）] をクリックします。

ステップ 2 [ネイバー（Neighbors）] タブをクリックします。

例

次に例を示します。



リンクの詳細情報の取得

Cisco EPN Manager には、リンクを表示し、それらの詳細を取得するさまざまな方法が用意されています。

次のリンク情報を表示するには：	以下の手順を参照：
特定のリンク	特定のリンクの概要：[リンク 360（Link 360）] ビュー （235 ページ）
トポロジ マップ内の特定のリンク	トポロジ マップでの特定のリンクの表示 （239 ページ）
トポロジ マップ内のグループ	ネットワーク トポロジ マップでのデバイス グループのリンクの表示 （239 ページ）
Cisco EPN Manager のすべて	リンク テーブルの表示 （240 ページ）

回線/VC の表示

Cisco EPN Manager は、回線/VC を表示するためのさまざまな方法を提供します。

以下の回線/VC 情報を表示するには：	以下の手順を参照：

トポロジ マップ、回線/VC 360 ビュー、または回線/VC 詳細ページにおける特定の回線/VC	• 回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ） • 回線/VC に関する総合情報の取得：[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウ （810 ページ）
デバイス	特定のデバイスの回線/VC の表示 （813 ページ）
トポロジ マップまたは拡張テーブルのデバイス グループ	デバイス グループの回線/VC を表示する （813 ページ）
Cisco EPN Manager のすべて	Cisco EPN Manager ですべての回線/VC を表示 （815 ページ）

サテライトの表示

Cisco EPN Manager では、次の方法でホスト/サテライト構成のサテライト情報を表示できます。

サテライトを表示する方法	参照先
トポロジ マップを使用してロケーション グループ内のすべてのサテライトを表示する	トポロジ マップでの Cisco ASR 9000 ホスト/サテライト トポロジの表示 （344 ページ）
[デバイス360（Device 360）] ビューで特定のデバイスのサテライトを表示する	• Cisco ASR 9000 ホストに接続されているサテライトの特定 （346 ページ） • 基本デバイス情報を取得する：[デバイス 360（Device 360）] ビュー （106 ページ）
[サテライト360（Satellite 360）] ビューを使用して、特定のサテライトの詳細（接続先のホストなど）を表示する	サテライトに接続されているホストの特定 （347 ページ）

カスタム値用のユーザー定義フィールドの作成

デバイスまたは回線/VCにカスタム属性を割り当てる場合は、テーブルに表示する独自のフィールドを作成し、それらのフィールドでカスタム値を定義できます。たとえば、特定のデバイスに顧客名のラベルを付けることもできます。ユーザー定義フィールドを作成して値を割り当てたら、テーブルでこれらの値を使用して検索できます。

ユーザー定義フィールドを作成する手順は次のとおりです。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [全般（General）] > [ユーザー定義フィールド（User Defined Fields）]** を選択します。

ステップ 2 [+]アイコンをクリックします。ドロップダウンリストからユーザー定義フィールドのタイプ（UDF）を選択し、ラベルと説明を入力します。

ステップ 3 次のように、特定のデバイス/回線/VC に対して新しく作成したユーザー定義フィールドに値を割り当てます。

a) デバイス テーブルまたは回線/VC のテーブルに移動します。

b) テーブルの右上にある設定アイコンをクリックし、[列（Columns）] を選択してからユーザー定義フィールドを選択して、テーブルの列としてユーザー定義フィールドを表示します。

c) テーブル内の目的のデバイスまたは回線/VC に移動し、ユーザー定義の列に値を入力して [保存（Save）] をクリックします。

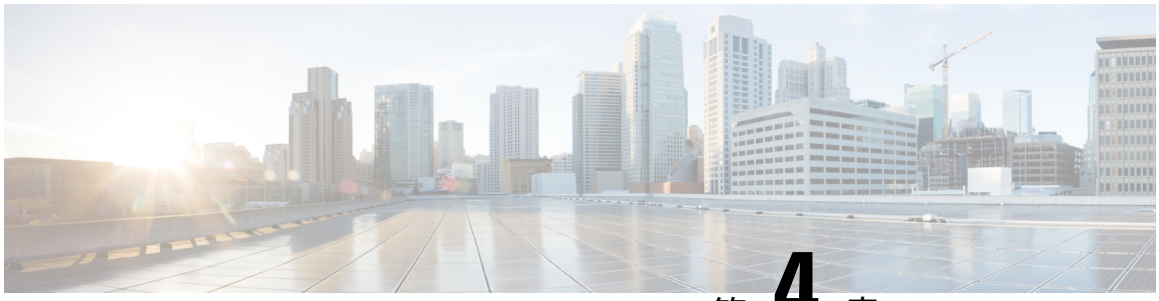
ユーザー定義フィールドの削除

ユーザー定義フィールドを削除するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [全般（General）] > [ユーザー定義フィールド（User Defined Fields）]** を選択します。

ステップ 2 削除するユーザー定義フィールドを選択し、[削除（Delete）] アイコンをクリックします。

これにより、選択したユーザー定義フィールドが削除されます。



第 4 章

デバイス コンフィギュレーション ファイルの管理

デバイス コンフィギュレーション ファイル管理のセットアップ

- 設定アーカイブ操作のタイムアウトの制御 （144 ページ）
- データベースからデバイス コンフィギュレーション ファイルを消去するタイミングの制御 （145 ページ）

デバイスが正しく構成されていることを確認する

構成のアーカイブ機能を使用する前にデバイスの設定を確認してください で設定によると デバイスをモデル化してモニターできるように設定する （69 ページ） 。

アーカイブのトリガー方法の制御

デフォルトでは、Cisco EPN Manager は次のタイミングでデバイス コンフィギュレーション ファイルをアーカイブに保存します。

- 新しいデバイスが Cisco EPN Manager に追加された場合
- デバイスの変更通知を受信した場合
- 完全同期または詳細同期の場合にアーカイブ収集が実行されない

（注） イベントが発生すると、設定された保留タイマーの期間後にアーカイブデータが収集されます。

管理者権限を持つユーザーはこれらの設定を変更できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択します。

ステップ 2 次の条件に従って、アーカイブ設定を調整します。

このチェックボックスをオンした場合：	ファイルをアーカイブする条件：
すぐに使える設定をアーカイブしますか?（Archive configuration out-of-box?）	新しいデバイスが追加された場合（デフォルトで有効にされます）
「受信設定変更イベントの設定をアーカイブしますか?（Archive configuration on receiving configuration change events?）」	設定の変更通知が送信された場合（デフォルトで有効にされます）。次を参照：イベント トリガー アーカイブをセットアップする （143 ページ）

ステップ 3 デバイスのグループ（または単一のデバイス）に対して定期的なアーカイブをスケジュールするには、次の手順に従います。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [アーカイブ収集の設定（Configuration Archive Collection）]** の順に選択します。

b) [デバイス（Devices）] タブで、定期的にアーカイブする複数のデバイスまたはデバイスグループを選択します。
c) **[アーカイブのスケジュール設定（Schedule Archive）]** をクリックし、[繰り返し（Recurrence）] 領域でスケジュール設定を実行します。多数のデバイスに対してこの操作が行われるようにする場合、実稼働に影響を与える可能性が最も少ない時間にアーカイブをスケジュールしてください。
d) [リポジトリへのバックアップ（Backup to Repository）] ボタンをクリックして、定期的にデバイス設定を外部リポジトリに転送します。リポジトリの設定や作成は CLI コマンドで行うことができます。サポートされているリポジトリは FTP、SSH FTP（SFTP）、ネットワーク ファイル システム（NFS）です。GnuPG を使用して、エクスポートされたファイルを暗号化することもできます。GnuPG を使用して暗号化する場合は、暗号化パスワードを入力する必要があります。

イベント トリガー アーカイブをセットアップする

デフォルトで、Cisco EPN Manager は、変更通知イベントを受信するたびに、デバイスのコンフィギュレーションファイルをバックアップします。この機能は、デバイスが適切に設定されている場合にのみ機能します。インベントリはどのように収集されていますか。（68 ページ）を参照してください。たとえば、Cisco IOS XR と Cisco IOS XE を実行しているデバイスの場合は、次の設定を行う必要があります。

```
logging server-IP
```

Cisco EPN Manager は設定変更イベントを受信すると、さらに設定変更イベントを受信した場合に備えて 10 分間（デフォルト）待機してからアーカイブを実行します。これにより、複数の収集プロセスの同時実行が回避されます。この設定を確認または変更するには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択してから、**[インベントリ（Inventory）]** > **[設定アーカイブ（Configuration Archive）]** を選択し、[ホールドオフタイマー（Hold Off Timer）] を調整します。

（注） 優先イベントと呼ばれる特定のイベントの場合は、[ホールドオフタイマー（Hold Off Timer）] をより短い期間に設定できます。詳細については、完全優先ベントの動作の変更（1084 ページ）を参照してください。

イベント トリガー アーカイブをオフにするには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択してから、**[インベントリ（Inventory）]** > **[設定アーカイブ（Configuration Archive）]** を選択し、**[受信設定変更イベントの設定をアーカイブしますか?（Archive configuration on receiving configuration change events?）]** チェックボックスをオフにします。

設定ファイルの変更を確認する場合に除外する項目の指定

Cisco EPN Manager は、バージョンの異なるデバイス コンフィギュレーション ファイルを比較して違いを特定する際に、ファイルの一部の行を除外する必要があります。Cisco EPN Manager

はデフォルトでルータやスイッチのクロック設定など、一部の行を除外します。管理者権限がある場合は、除外される行を確認した上で、除外する行を追加できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択します。

ステップ 2 [詳細（Advanced）] タブをクリックします。

ステップ 3 [製品ファミリ（Product Family）] リストで、コマンドの除外を適用するデバイスまたはグループを選択します。

ステップ 4 [コマンド除外リスト（Command Exclude List）] に、その選択で除外するカンマ区切りのコンフィギュレーション コマンドのリストを入力します。これらは、コンフィギュレーションの変更についてデバイスを確認する際に Cisco EPN Manager が無視するパラメータです。

ステップ 5 [保存（Save）] をクリックします。

設定アーカイブ操作のタイムアウトの制御

設定アーカイブタスクでは、フェッチアクティビティごとにデバイスのCLIタイムアウト値が使用されます。1 つの設定アーカイブタスクには 1 ～ 5 個のファイルが伴います。その結果、全体的なジョブタイムアウト値は次のロジックを使用して決定されます。**全体的なジョブタイムアウト = ファイルの数 * デバイスの CLI タイムアウト**。

CLI タイムアウト値を設定するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択し、デバイス編集アイコンをクリックし、[Telnet/SSH] オプションを選択し、[タイムアウト（Timeout）] フィールドに値を入力します。

（注） CLI のタイムアウトにより設定アーカイブタスクが失敗した場合は、デバイスの CLI タイムアウト値を増やす必要があります。

アラームをトリガーする頻度の制御

デフォルトでは、Cisco EPN Manager は設定に基づいてデバイス コンフィギュレーション ファイルをアーカイブに保存します。ただし、これらのジョブが失敗した場合は、アラーム通知を生成するように選択できます。

設定アーカイブ ジョブが失敗すると、Cisco EPN Manager は 7 日間または 5 つ以上のコンフィギュレーションファイルを待機してからアラームをトリガーします。アラームには、アラームのトリガー原因に関する情報と、設定アーカイブに関連付けられたその他の関連情報が含まれています。アラームの生成頻度に関するデフォルト設定を変更するには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから **[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択し、コンフィギュレーションファイルの最大数（超過するとアラームが生成される）およびアラームがトリ

ガーされるまで待機する日数の[アラームしきい値（Alarm Threshold）]パラメータを調整します。

データベースからデバイス コンフィギュレーション ファイルを消去するタイミングの制御

デバイスのコンフィギュレーションファイルをデータベースから自動的に削除することはできません（ファイルは手動で削除できます）。ファイルは、ユーザーの設定に基づき、Cisco EPN Managerによって定期的に消去することができます。管理者権限を持つユーザーは、コンフィギュレーション ファイルが消去されるタイミングを次のように調整できます。コンフィギュレーションファイルを一切消去しない場合は、次の手順に従う際、両方のフィールドを空にしてください。

（注） コンフィギュレーションファイルを手動で削除する方法の詳細については、「アーカイブ済みデバイス設定ファイルの削除」を参照してください。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）]** > **[設定アーカイブ（Configuration Archive）]** を選択します。

ステップ 2 次の条件に従って、アーカイブ設定を調整します。

使用するフィールド	ファイルを消去する条件
[設定アーカイブの最大数（Max. configuration archives）]	デバイスのコンフィギュレーション ファイルの数がこの設定（デフォルトは 5）を超えた場合。
[最大保持日数（Max. days retained）]	コンフィギュレーションファイルの存続期間がこの設定（デフォルトは 7）を超えた場合。

ファイルが最後にアーカイブされた時刻を確認する方法

ステップ 1 デバイスの実行コンフィギュレーション ファイルがアーカイブにバックアップされた最終日を特定するには、[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[設定アーカイブ（Configuration Archive）]を選択し、[デバイス（Devices）]タブをクリックします。[最新のアーカイブ（Latest Archive）]列に、最新のアーカイブが最初に示された各デバイスのアーカイブ タイム スタンプのリストが表示されます。[作成者（Created By）]列には、アーカイブのトリガー（たとえば、syslog）が表示されます。

ステップ 2 デバイスの最新のアーカイブ済み実行コンフィギュレーションファイルの内容を表示するには、タイムスタンプのハイパーリンクをクリックします。[実行コンフィギュレーション（Running Configuration）] ウィンドウにファイルの内容が表示されます。

ステップ 3 デバイスのアーカイブ間で加えられた変更を表示するには、デバイスのコンフィギュレーション ファイルの比較または削除 （153 ページ）を参照してください。

デバイス コンフィギュレーション ファイルのアーカイブへのバックアップ

データベースにバックアップされる内容

設定アーカイブは、デバイス コンフィギュレーション ファイルのコピーを保持し、それらをデータベースに保存します。ほとんどのコンフィギュレーションファイルは、デバイスから受信したものとして読み取り可能な形式に保存され、以前のバージョンと比較できます。デバイス設定は、アーカイブに保存されているファイルを使用して、前の状態に復元できます。

デバイス上の実行コンフィギュレーションとスタートアップ コンフィギュレーションが同じ場合、Cisco EPN Manager は実行コンフィギュレーションのみをデータベースにコピーします。そのため、イメージリポジトリを表示するときに、実行コンフィギュレーションのアーカイブのみが表示されることがあります。

コンフィギュレーションファイルが最後のバックアップから変更されていない場合、Cisco EPN Manager はファイルをアーカイブしません。Cisco EPN Manager はジョブが成功したことを報告し、ジョブの結果には **Already Exists** と表示されます。

Cisco EPN Manager は、次のデバイス コンフィギュレーション ファイルを収集およびアーカイブします。

デバイス/デバイス OS	バックアップ内容
Cisco IOS および Cisco IOS XE	最新のスタートアップ コンフィギュレーション、実行コンフィギュレーション、および VLAN 設定。

デバイス/デバイス OS	バックアップ内容
Cisco IOS XR	• 最新の実行コンフィギュレーション。アクティブなパッケージが含まれます。デバイスは、システムユーザーが管理する必要があります。これは、システム ユーザー以外のユーザーはコマンドライン インターフェイス（CLI）で copy コマンドを使用できないためです。 • データベース設定（バイナリ ファイル） （注） Cisco NCS 4000 デバイスの場合、データベースは、ローカルマシン上のファイル システムに .tgz ファイルとしてバックアップされます。
Cisco NCS	データベース設定（バイナリ ファイル） （注） Cisco NCS 2000 デバイスの場合、データベースは、バイナリ ファイルとしてバックアップされます。これはテキスト ファイルではないため、バージョンを比較できませんが、設定アーカイブのファイル タイム スタンプで確認できます。

コンフィギュレーションファイルをバックアップ（アーカイブ）する

コンフィギュレーション ファイルをバックアップすると、Cisco EPN Manager がデバイスからコンフィギュレーションファイルのコピーを取得して、設定アーカイブ（データベース）にコピー（バックアップ）します。コピーをアーカイブに保存する前に、Cisco EPN Manager は取得したファイルとアーカイブ内の同じタイプの最新バージョン（実行と実行、スタートアップとスタートアップ）を比較します。Cisco EPN Manager は、2 つのファイルが異なる場合にのみファイルをアーカイブします。アーカイブ済みのバージョンの数が最大値（デフォルトは 5）を超えると、最も古いアーカイブが消去されます。

実行コンフィギュレーションとスタートアップ コンフィギュレーションの両方をサポートするデバイスの場合は、Cisco EPN Manager がスタートアップ コンフィギュレーションの最新バージョンと実行コンフィギュレーション ファイルの最新バージョンを比較することによって、バックアッププロセス中に「同期外れ」（不同期）のデバイスを特定します。同期外れのデバイスの詳細については、実行デバイス コンフィギュレーションとスタートアップ デバイス コンフィギュレーションの同期 （151 ページ）を参照してください。

次の表に、サポートされているバックアップ方式とそれらのトリガー方法の説明を示します。デフォルト設定をチェックまたは調整するには、アーカイブのトリガー方法の制御 （142 ページ）を参照してください。

Cisco NCS 2000 データベースをアーカイブしたときに、データベースまたはフラッシュがビジーであることを伝えるエラーメッセージが表示された場合は、次のいずれかが原因の可能性があります。

- アーカイブ操作を他の設定アーカイブまたはイメージ管理操作と並行して実行している。短い時間間隔で操作を再試行する必要があります。
- 複数のユーザーが同時に同じ操作を実行している。短い時間間隔で操作を再試行する必要があります。
- デバイスのソフトウェア ダウンロード アラームが解消されていない。アラームを解消する必要があります。

表 *10* : バックアップ方式

バックアップ方式	説明	注記
オンデマンド手動バックアップ	[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] を選択して、デバイスを選択し、**[アーカイブ収集のスケジュール設定（Schedule Archive Collection）]** をクリックします（ジョブをすぐに実行するか後で実行します）。	該当なし
定期的にスケジュールされたバックアップ	[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] を選択して、デバイスを選択し、**[アーカイブ収集のスケジュール設定（Schedule Archive Collection）]]** をクリックします。スケジューラで、**[Recurrence]** を指定します。	該当なし
新しいデバイスのバックアップ	Cisco EPN Manager は、自動的に新しいデバイスのバックアップを実行します。	デフォルトで有効
イベント トリガー バックアップ（デバイス変更通知）	Cisco EPN Manager は、管理対象デバイスから syslog を受信したときに自動的にバックアップを実行します。	デフォルトで有効

アーカイブに保存されているデバイス コンフィギュレーション ファイルの表示

すべてのアーカイブされたファイルを表示する

データベースに保存されたコンフィギュレーション ファイルを表示するには、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration

Archive）] を選択します。開始する場所に応じて、[アーカイブ（Archives）] タブまたは [デバイス（Devices）] タブをクリックします。

- **Archives** タブ：アーカイブされたコンフィギュレーション ファイルのリスト。最新のアーカイブが先頭に表示されます。[アウト オブ バンド（Out of Band）] 列は、Cisco EPN Manager 以外のアプリケーションによって変更が行われたかどうかを示します。左側の [グループ（Groups）] リストを使用して、アーカイブをデバイス タイプ別とファミリ別で表示します。グローバル設定に関して実行できることは次のとおりです。
  - アーカイブされたバージョンへのデバイス設定のロールバック （156 ページ）
  - 実行コンフィギュレーションによるスタートアップ コンフィギュレーションの上書き（155 ページ）
  - タグを使用した重要なコンフィギュレーション ファイルのラベル付け （150 ページ）
- **Devices** タブ：アーカイブされた設定を含むデバイスのフラットなリスト。ここから、次の操作を実行できます。
  - アーカイブへのバックアップをスケジュールします（デバイス コンフィギュレーション ファイルのアーカイブへのバックアップ （146 ページ）を参照）。
  - デバイス名のハイパーリンクをクリックして、特定のデバイスのアーカイブされたファイルを表示します（特定のデバイスのアーカイブされたファイルを表示する （149 ページ）を参照）。

デフォルトで、Cisco EPN Manager は、ファイルの最大 5 つのバージョンを保存し、7 日前より古いファイルをすべて削除します。デバイス コンフィギュレーション ファイルは、データベースから手動で削除することはできません（現在の消去設定をチェックするには、データベースからデバイス コンフィギュレーション ファイルを消去するタイミングの制御 （145 ページ）を参照してください）。

特定のデバイスのアーカイブされたファイルを表示する

（注） 実行コンフィギュレーション ファイルだけが表示され、スタートアップ ファイルが表示されないのは、この 2 つのファイルが同じものだからです。Cisco EPN Manager は、実行コンフィギュレーションと異なっている場合にしか、スタートアップ コンフィギュレーションをバックアップしません。

ステップ 1 [**Inventory**] > [**Device Management**] > [**Configuration Archive**] を選択して、[**Devices**] タブをクリックします。

ステップ 2 デバイス名のハイパーリンクをクリックします。Cisco EPN Manager に、タイムスタンプに基づいてアーカイブされたファイルが一覧表示されます。

アーカイブされた設定ファイルの raw コンテンツの表示

この手順を使用して、設定アーカイブに保存されているスタートアップ コンフィギュレーション ファイル、実行コンフィギュレーション ファイル、VLAN（サポートされている場合）コンフィギュレーション ファイル、データベース コンフィギュレーション ファイルおよび管理コンフィギュレーション ファイルを表示します。タイムスタンプに応じてバージョンを選択し、それらを別のバージョンと比較できます。

（注） Cisco NCS 2000 および Cisco NCS 4000 のデバイスの場合、データベースはバイナリ ファイルとしてバックアップされます。これはテキスト ファイルではないため、表示したり他のバージョンと比較できませんが、ファイルを直接エクスポートすることができます。

設定アーカイブに保存されている実行コンフィギュレーション ファイルの内容を表示するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）]** を選択し、[デバイス（Devices）] タブをクリックします。

ステップ 2 デバイス名のハイパーリンクをクリックします。Cisco EPN Manager に、タイムスタンプに基づいてアーカイブされたファイルが一覧表示されます。

ステップ 3 タイム スタンプを展開して、その時点でアーカイブされたファイルを表示します。実行コンフィギュレーション、スタートアップ コンフィギュレーション、管理コンフィギュレーション、VLAN コンフィギュレーション、およびデータベース コンフィギュレーションの詳細が表示されます。これらのカテゴリの下にある [詳細（Details）] ハイパーリンクをクリックし、詳細を表示します。

（注） 実行コンフィギュレーションファイルのみが表示されてスタートアップ ファイルが表示されない場合、2 つのファイルは同じです。Cisco EPN Manager は実行コンフィギュレーションと異なる場合にのみスタートアップ コンフィギュレーションをバックアップします。

ステップ 4 [設定タイプ（Configuration Type）] の下にあるファイルをクリックし、その raw データを表示します。[Raw コンフィギュレーション（Raw Configuration）] タブの上から下へとファイルの内容が一覧表示されます。

ステップ 5 別のファイルの内容と比較するには、[比較対象（Compare With）] 列の下にある任意のハイパーリンクをクリックします。選択肢は、アーカイブにバックアップされたデバイスのタイプと設定ファイルの数によって異なります。カラー コードは、更新、削除、または追加されたものを示します。

タグを使用した重要なコンフィギュレーションファイルのラベル付け

コンフィギュレーションファイルにタグを割り当てることは、重要な設定を識別し、必要な情報を伝えるためのわかりやすい方法です。タグは、[設定アーカイブ（Configuration Archive）]

ページでファイルの一覧とともに表示されます。また、次の手順を使用して、タグを編集および削除することもできます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

ステップ 2 [アーカイブ（Archives）] タブで、ラベル付けするコンフィギュレーション ファイルを見つけて [タグの編集（Edit Tags）] をクリックします。

ステップ 3 [タグの編集（Edit Tag）] ダイアログボックスに内容を入力するか、既存のタグを編集または削除して、[保存（**Save**）] をクリックします。

実行デバイス コンフィギュレーションとスタートアップ デバイス コンフィギュレーションの同期

スタートアップ コンフィギュレーション ファイルと実行コンフィギュレーション ファイルを持つデバイスは、同期が取れていない（非同期）場合があります。スタートアップ ファイル（デバイスの再起動時に読み込まれる）が実行コンフィギュレーションと異なる場合、デバイスは同期が取れていないと判断されます。変更された実行コンフィギュレーションはスタートアップ コンフィギュレーションとしても保存しない限り、デバイスを再起動すると、実行コンフィギュレーションの変更が失われます。上書き操作は、現在の実行コンフィギュレーションでデバイスのスタートアップ コンフィギュレーションを上書きして、ファイルを同期します。

（注） このデバイス構成ファイルの同期操作は、デバイスの即時インベントリ収集を実行する同期操作とは異なります。この同期動作については、デバイスのインベントリの即時収集（同期）（570 ページ）で説明されています。

ステップ 1 同期が取れていないデバイスの特定。

a) [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

b) [デバイス（Devices）] タブで、**[Startup/Runningの不一致（Startup/Running Mismatch）]**フィールドフィールドを確認します。

c) いずれかのデバイスのリストに [**Yes**] と表示されている場合は、それらのデバイスをメモします。

ステップ 2 デバイスを同期するには。

a) [デバイス（Devices）] タブで同期されていないデバイスを選択し、[上書き（Overwrite）]**[アーカイブの上書きのスケジュール（Schedule Archive Overwrite）]** をクリックします。（上書き操作の詳細については、実行コンフィギュレーションによるスタートアップ コンフィギュレーションの上書き （155 ページ）を参照してください）。

ステップ 3 ジョブの詳細を確認するには、**[管理（Administration）] > [ジョブダッシュボード（Job Dashboard）]** の順に選択して、上書きジョブの詳細を表示します。

コンフィギュレーション ファイルのダウンロード

同時に最大 1000 台までのデバイスの起動および実行コンフィギュレーション ファイルをローカル システムにダウンロードできます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

ステップ 2 [最新のアーカイブのエクスポート（Export Latest Archives）] ドロップダウンリストから次のいずれかのオプションを選択して、構成ファイルをダウンロードします。

1. [サニタイズ（Sanitized）] : デバイスのクレデンシャル パスワードがダウンロードしたファイル内でマスクされます。
2. [非サニタイズ（Unsanitized）] : デバイスのクレデンシャル パスワードがダウンロードしたファイル内に表示されます。

[非サニタイズ（Unsanitized）] オプションは、ロールベース アクセス コントロール（RBAC）で設定されているユーザー権限に基づいて表示されます。

このオプションは、デバイスのサポートされているすべての設定を csv ファイルとしてダウンロードします。デバイスのスタートアップ コンフィギュレーションまたは実行コンフィギュレーションのみをダウンロードするには、次の代替ステップを使用します。

- [インベントリ（Inventory）]>[デバイス管理（Device Management）]>[設定アーカイブ（Configuration Archive）]ページで、設定ファイルをダウンロードするデバイスをクリックするか、または[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]ページで設定ファイルをダウンロードするデバイスをクリックし、[設定アーカイブ（Configuration Archive）] タブをクリックします。
- [展開（Expand）] アイコンを使用して、アーカイブの必要な設定の詳細を表示します。
- [詳細（Details）] をクリックします。
- [エクスポート（Export）] ドロップダウンリストで [サニタイズ（Sanitized）] または [非サニタイズ（Unsanitized）] を選択します。

メモ このコンフィギュレーション ファイルを WLC にアップロードする前に、各行の先頭にキーワード **config** を追加する必要があります。

デバイスのコンフィギュレーションファイルの比較または削除

比較機能は、2つのコンフィギュレーションファイルを並べて表示し、追加、削除、および除外された値を異なる色で示します。この機能を使用して、同期されていないデバイスの起動時と実行時のコンフィギュレーションファイル間の違いを表示するか、または同様なデバイスの設定が異なっているかどうかを検出します。これで、設定アーカイブをデータベースから削除できるようになります。

Cisco EPN Manager は、NTP クロック レート（管理対象のネットワーク要素上で絶えず変化していても、設定変更とは見なされない）のような、小型のコマンドセットをデフォルトで除外します。設定ファイルの変更を確認する場合に除外する項目の指定（143 ページ）で説明するように、除外されたコマンドのリストは変更できます。

（注） ファイルがバイナリ形式で保存されるため、Cisco NCS 2000 デバイス上ではファイルの比較はサポートされていません。テキスト ベースのファイルのみが比較できます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

ステップ 2 デバイスの設定アーカイブを削除するには、[デバイス]タブで設定を削除するデバイスを見つけ、[X]（削除）ボタンをクリックします。

ステップ 3 デバイスの設定アーカイブを比較するには、次の操作を実行します。

a) [デバイス（Devices）] タブで、比較する設定を持つデバイスを見つけ、そのデバイス名のハイパーリンクをクリックします。

b) タイム スタンプを展開して、その時点でアーカイブされたファイルを表示します。

c) [比較対象（Compare With）]列の下にあるハイパーリンクのいずれかをクリックして比較ウィンドウを起動します。選択肢は、アーカイブにバックアップされたデバイスのタイプと設定ファイルの数によって異なります。カラー コードは、更新、削除、または追加されたものを示します。

[設定の比較（Configuration Comparison）] ウィンドウでは、raw ファイルに注目するか、またはファイルの特定の部分（configlet）に注目することで、設定を調べることができます。下部のウィンドウの色分けを使用して、何が更新、削除、または追加されたかを確認します。

デバイスへの外部コンフィギュレーションファイルの展開

展開のスケジュール操作は、外部ファイルを使用してデバイスの設定を更新します。ロールバックと定期展開の違いは、ロールバックではアーカイブから既存のファイルを使用するのに対して、定期展開では外部ファイルを使用することです。

デバイスのタイプによっては、展開ジョブに次の設定を指定できます。

- 現在のスタートアップ コンフィギュレーションを新しいバージョンで書き換え、必要に応じて展開後にデバイスを再起動します。
- 新しいファイルと現在実行中の設定をマージし、必要に応じてファイルを新しいスタートアップ コンフィギュレーションとしてアーカイブします。
- データベース コンフィギュレーション ファイルの展開を .tgz 形式でスケジュール設定します。

（注） 構成アーカイブの展開がEPNMから実行されたら、デバイスを手動で同期する必要があります。

ローカル マシンにファイルを作成する場所があることを確認します。

ステップ 1 デバイスの [デバイスの詳細（Device Details）] ページを開き、そのページから展開操作を実行します。

a) [インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）] を選択します。

b) デバイス名のハイパーリンクをクリックし、[デバイスの詳細（Device Details）] ページを開きます。

ステップ 2 [設定アーカイブ（Configuration Archive）] タブをクリックしてデバイスの [設定アーカイブ（Configuration Archive）] ページを開きます。

Cisco NCS 2000 と Cisco ONS のデバイスの場合、この選択肢は [シャーシビュー（Chassis View）] タブをクリックすると、右側に表示されます。

ステップ 3 **[展開のスケジュール設定（Schedule Deploy）]** をクリックして、展開ジョブ ダイアログ ボックスを開きます。

ステップ 4 [参照（Browse）] をクリックし、ファイルの場所まで移動してファイルを選択し、展開するファイルを選択します。

（注） Cisco for NCS 4000 デバイスにデータベース コンフィギュレーションを展開するには、ファイルを .tgz 形式でアップロードする必要があります。

ステップ 5 展開するファイルのタイプに応じて、次のようにジョブ パラメータを設定します。

- [スタートアップ コンフィギュレーション（Startup configuration）] : [スタートアップ コンフィギュレーションの上書き（Overwrite Startup Configuration）] を選択します。展開操作の後にデバイスを再起動する場合は、[再起動（Reboot）] チェックボックスをオンにします。
- 実行コンフィギュレーション：[**Merge with Running Configuration**] を選択します。また、スタートアップ コンフィギュレーションとしてデバイスにファイルを保存するには、[**Save to Startup**] チェック ボックスをオンにします。
- データベース コンフィギュレーション：[**Deploy Database Configuration**] を選択し、データベース ファイルを選択します（Cisco NCS 4000 デバイスの場合は .tgz 形式、Cisco NCS2000 デバイスの場合は .cfg 形式）。
- [管理設定（Aadmin Configuration）] : **Merge with Admin Configuration** を選択し、[デバイス VM の管理者パスワード（Device VM Admin Password）] を入力します。

ステップ 6 展開ジョブをすぐに実行するか、後で実行するようにスケジュールを設定し、[送信（Submit）] をクリックします。

ステップ 7 **[管理（Administration）] > [ジョブダッシュボード（Job Dashboard）]** の順に選択して、イメージアクティブ化ジョブの詳細を表示します。

実行コンフィギュレーションによるスタートアップ コンフィギュレーションの上書き

上書き操作により、デバイスの実行コンフィギュレーションがデバイスのスタートアップ コンフィギュレーションにコピーされます。実行コンフィギュレーションに変更を加えた後、デバイスのスタートアップ コンフィギュレーションを上書きしなければ、デバイスを再起動するとその変更内容が失われます。

（注） （**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）]** を選択すると表示される）[デバイス（Devices）] タブの [アーカイブ上書きのスケジュール（Schedule Archive Overwrite）] ボタンで選択できるのはデバイスだけで、構成ファイルを選択することはできないため、このボタンは使用しないでください。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして [デバイスの詳細（Order Details）] ページを開き、[設定アーカイブ（Configuration Archive）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスの場合、この選択肢は [シャーシビュー（Chassis View）] タブをクリックすると、右側に表示されます。

ステップ 3 [上書きのスケジュール（Schedule Overwrite）] [アーカイブ上書きのスケジュール（Schedule Archive Overwrite）] をクリックし、ジョブを即時に実行するか、後で実行するかを設定してから、[送信（Submit）] をクリックします。

ステップ 4 **[管理（Administration）] > [ジョブダッシュボード（Job Dashboard）]** を選択して、イメージ アクティブ化ジョブの詳細を表示します。

アーカイブされたバージョンへのデバイス設定のロールバック

ロールバック操作により、アーカイブのファイルがデバイスにコピーされ、新しいファイルが現在の設定になります。実行コンフィギュレーション、スタートアップ コンフィギュレーション、VLAN設定をロールバックできます。デフォルトでは、この操作はファイルをマージして実行されます。実行コンフィギュレーションをロールバックする場合、ファイルをマージするのではなく、上書きするオプションを選択できます。コンフィギュレーションファイルを前のバージョンにロールバックするには、次の手順に従います。

ステップ 1 **Inventory** > **Device Management** > **Configuration Archive** を選択します。

ステップ 2 [**Archives**] タブをクリックし、コンフィギュレーション ファイルをロールバックするデバイスを選択してから [アーカイブロールバックのスケジュール（Schedule Archive Rollback）] をクリックします。

ステップ 3 ロールバックするファイルのタイプを選択します。[設定ロールバックのスケジュール（Schedule Configuration Rollback）] ダイアログボックスで次の操作を行います。

a) [ロールバックのオプション（Rollback Options）] 領域を展開します。

b) [**Files to Rollback**] ドロップダウンリストからファイル タイプを選択します。[**All**] を選択すると、この操作がスタートアップ コンフィギュレーションファイル、実行コンフィギュレーションファイル、および VLAN コンフィギュレーション ファイルに適用されます。

（注） Cisco IOS XR 64 ビットデバイスでは、[管理設定（Admin Configuration）] を選択した場合は、[デバイスの VM 管理者パスワード（Device VM Admin Password）] を入力します。

ステップ 4 ロールバック先の特定のコンフィギュレーション ファイルのバージョンをクリックします。

ステップ 5 [アーカイブロールバックのスケジュール（Schedule Archive Rollback）] をクリックし、次の設定を行います。

表 *11* : デバイス設定のロールバック

領域	オプション	説明
ロールバック（Rollback）	[ロールバックするファイル（Files to rollback）]	[データベース設定（Database Configuration）]、[実行コンフィギュレーション（Running Configuration）]、[管理者設定（Admin Configuration）] のいずれかを選択します。
	[再起動（Reboot）]	（起動のみ）起動コンフィギュレーションをロールバックした後、デバイスを再起動すると、起動コンフィギュレーションが実行コンフィギュレーションになります。
	[スタートアップに保存（Save to startup）]	（実行のみ）実行コンフィギュレーションをロールバックした後、その実行コンフィギュレーションを起動コンフィギュレーションに保存します。
	[ロールバック前のアーカイブ（Archive before rollback）]	ロールバック操作を開始する前に、選択されたファイルをバックアップします。
	[設定の上書き（Overwrite configurations）]	古い実行コンフィギュレーションを（マージするのではなく）新しい実行コンフィギュレーションで上書きします。
	[アーカイブの失敗時ロールバックを続行（Continue rollback on archive failure）]	（[ロールバック前のアーカイブ（Archive before rollback）] が選択されている場合）選択されたファイルが正常にデータベースに保存されなくてもロールバックを続行します。
	[VRF名（VRF Name）]	ドロップダウンリストから適切な VRF 名を選択します。VRF 名は送信時に検証されます。
ロールバック（Rollback）	[データベース設定のロールバック（Rollback Database Configuration）]	データベース設定ファイルのロールバック操作を開始します。
スケジュール（Schedule）	（Web GUI を参照）	ロールバックを即時に実行するか、後でスケジュールした時間に実行するかを指定します。

ステップ 6 **Submit** をクリックします。

ローカル ファイル システムへのコンフィギュレーション ファイルのエクスポート

実行コンフィギュレーション ファイルおよびスタートアップ コンフィギュレーション ファイルをエクスポートできます。

（注） Cisco NCS 2000 デバイスの場合は、データベース コンフィギュレーションをバイナリ ファイルとしてローカル マシンのファイル システムにエクスポートできます。Cisco NCS 4000 デバイスの場合は、データベース コンフィギュレーションを .tgz ファイルとしてエクスポートできます。エクスポートすると、ブラウザにプロンプトが表示されファイルを保存するか開くように促されます。

ステップ 1 **Inventory** > **Device Management** > **Configuration Archive** を選択します。

ステップ 2 [デバイス（Devices）] タブで、エクスポートするアーカイブがあるデバイスを見つけ、そのデバイス名のハイパーリンクをクリックします。

ステップ 3 エクスポートするコンフィギュレーションのバージョンを見つけ、それを展開します。

ステップ 4 [設定タイプ（Configuration Type）] 列で、エクスポートするファイル（[実行コンフィギュレーション（Running Configuration）]、あるいは、サポートされている場合は [スタートアップ コンフィギュレーション（Startup Configuration）]、または [データベース コンフィギュレーション（Database Configuration）]）のハイパーリンクをクリックします。

ステップ 5 ファイル ビューア ページで、[**Export**] をクリックしてローカル マシンにファイルを保存します。

アーカイブ済みデバイス設定ファイルの削除

デバイス設定のロールバック特権を持つユーザーの場合、次のいずれかの手順を実行すると、データベースからアーカイブ済みデバイス設定ファイルを手動で削除できます。

（方法 1）

1. **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）]** の順に選択します。

   [設定アーカイブ（Configuration Archive）] ページの [デバイス（Devices）] タブが選択された状態で開きます。

2. [名前（Name）] 列から、削除する設定ファイルのデバイスのリンクをクリックします。

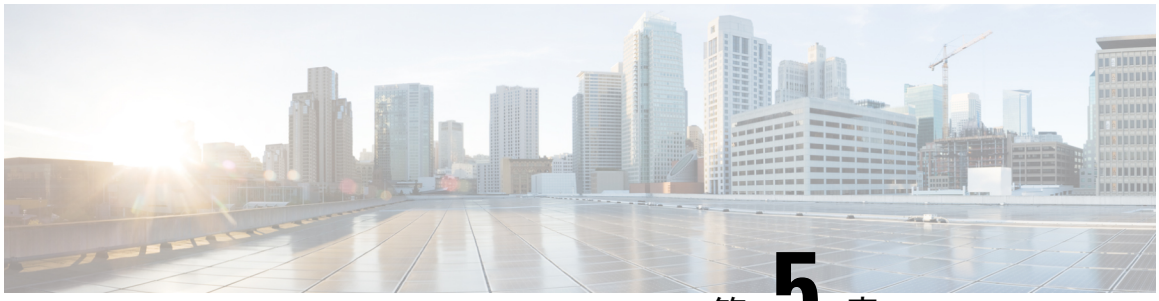
   その [アーカイブの詳細（Archive Details）] ページが開きます。

3. 削除する設定ファイルのラジオ ボタンをクリックしてから、[X]（[削除（Delete）]）アイコンをクリックします。
4. [はい（Yes）] をクリックして、設定ファイルの削除を確認します。

（方法 2）

1. **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[設定アーカイブ（Configuration Archive）]** の順に選択します。

   [設定アーカイブ（Configuration Archive）] ページの [デバイス（Devices）] タブが選択された状態で開きます。
2. [アーカイブ（Archives）] タブをクリックします。
3. 削除する設定ファイルのチェックボックスをクリックしてから、[X]（[削除（Delete）]）アイコンをクリックします。
4. [はい（Yes）] をクリックして、設定ファイルの削除を確認します。



第 5 章

デバイス ソフトウェア イメージの管理

ソフトウェア イメージ管理のセットアップ

（注） IPv6 のサポートは利用できません。

- インベントリ収集中にイメージ リポジトリに保存されたイメージの制御方法 （163 ページ）
- イメージの転送および配布設定の調整 （163 ページ）

デバイスが正しく構成されていることを確認する

Cisco EPN Manager場合、SNMP 読み取り/書き込みコミュニティをあなたのデバイスで構成されている文字列に一致にデバイスが追加されたときに指定された文字列にのみデバイスからファイルを転送できます Cisco EPN Manager 。さらに、デバイスはインベントリはどのように収集されていますか。 （68 ページ）の設定に従って設定されている必要があります。

（注） セキュリティを強化するために、Cisco EPN Manager では、旧バージョンの Cisco IOS-XE と IOS-XR で使用される SSH CBC（暗号ブロック連鎖）暗号方式の一部を使用しなくなりました。それらは脆弱であると見なされたためです。Cisco IOS-XE を実行するデバイスの場合は、16.5.x 以降のバージョンにアップグレードしていることを確認します。Cisco IOS-XR を実行するデバイスの場合は、6.1.2 以降のバージョンにアップグレードします。それ以外の場合は、ソフトウェア イメージ管理の複数の操作が失敗します。

これはお勧めしませんが（セキュリティが低下するため）、Cisco EPN Manager での使用が停止された CBC 暗号方式を SSHD サービス設定ファイルに戻すためのオプションもあります。このためには、最初に **/etc/ssh/sshd_config** ディレクトリに格納されたファイルの暗号方式の行に CBC 暗号方式を設定し（下の例を参照）、次に **service sshd stop/start** コマンドを使用して SSHD サービスを再起動します。

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,
arcfour256,arcfour128,aes128-cbc,3des-cbc,
cast128-cbc,aes192-cbc,aes256-cbc
```

（注） ソフトウェア イメージの管理は、NAT 環境ではサポートされていません。つまりそのイメージ管理機能など、イメージのインポート、アップグレード、配布、およびアクティブ化、NAT 環境で機能しません。

Cisco EPN Manager サーバーでの FTP/TFTP/SFTP/SCP 設定の確認

FTP、TFTP、SFTP、または SCP を使用する場合は、それが有効で適切に設定されていることを確認してください。サーバーでの FTP/TFTP/SFTP サービスの有効化（970 ページ）を参照してください。

インベントリ収集中にイメージリポジトリに保存されたイメージの制御方法

ソフトウェアイメージの収集はデータ収集プロセスを遅くする可能性があるため、デフォルトでは、Cisco EPN Manager は、インベントリ収集の実行時には、イメージ リポジトリでのデバイス ソフトウェア イメージの収集および保存を実行しません。次に説明する手順を使用して設定を変更できるのは、管理権限を持つユーザーです。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、次に **[インベントリ（Inventory）] > [イメージ管理（Image Management）]** を選択します。

ステップ 2 Cisco EPN Manager によるインベントリ収集の実行時にデバイス イメージを取得してイメージ リポジトリに保存するには、[インベントリ収集と同時にイメージを収集（Collect images along with inventory collection）] チェック ボックスをオンにします。

ステップ 3 [保存（Save）] をクリックします。

イメージの転送および配布設定の調整

Cisco EPN Manager がイメージをソフトウェア イメージ管理サーバーからデバイスに転送する際にデフォルトで使用するプロトコルを指定するには、この手順を使用します。また、Cisco EPN Manager がイメージの転送と配布に関連するさまざまなタスクをデフォルトで実行するように設定することもできます。たとえば、アップグレードの前に現在のイメージをバックアップする、アップグレード後にデバイスを再起動する、シリアルアップグレードが失敗した場合に次のデバイスをアップグレードするなどのタスクを実行するように設定できます。次に説明する手順を使用して設定を変更できるのは、管理権限を持つユーザーです。

この手順では、デフォルトのみを設定します。これらのデフォルトは、実際の配布操作を実行する際にオーバーライドできます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、次に **[インベントリ（Inventory）] > [ソフトウェアイメージ管理（Software Image Management）]** を選択します。

ステップ 2 [基本（Basic）] タブで、Cisco EPN Manager がイメージを配布する際に実行するタスクを指定します。

設定	説明	デフォルト
ジョブの設定		
失敗した場合に配信を続けます（Continue distribution on failure）	複数のデバイスにイメージを配布する場合、あるデバイスへの配布が失敗しても、他のデバイスへの配布を続行します。	有効

設定	説明	デフォルト
TFTP フォールバック（TFTP fallback）	TFTP フォールバック コマンドを実行中のイメージに挿入し、イメージの配布が失敗した場合にイメージをリロードできるようにします。 TFTP フォールバック コマンドを実行中のイメージに挿入し、イメージの配布が失敗した場合にイメージをリロードできるようにします。	無効
実行中のイメージのバックアップ（Backup running image）	イメージを配布する前に、実行中のイメージを TFTP サーバーにバックアップします。	無効
起動コマンドを挿入する（Insert boot command）	イメージを配布した後、起動コマンドを実行中のイメージに挿入します。	無効
[配布前にスマート フラッシュ削除（Smart Flash Delete Before Distribution）]	配布の前に、フラッシュから不要なファイルを削除してメモリスペースを解放します	無効
その他の設定		
インベントリのコレクションと一緒に画像を収集する	インベントリ収集中にソフトウェアイメージをデバイスから収集し、イメージリポジトリに保存するには、このオプションを選択します。	無効
使用可能なメジャーリリースの最新イメージを表示する	最新のメンテナンスリリースを表示する場合は、このオプションを選択します。	無効
同じ機能をサポートするイメージを表示する	実行中のイメージでサポートされているのと同じ機能を持つ使用可能なイメージを表示するには、このオプションを選択します。	無効
使用可能なより上位のイメージバージョンを表示する	実行中のイメージで使用可能なより上位のイメージバージョンを表示するには、このオプションを選択します。	無効
配信ジョブ中にソフトウェアをアクティブにするオプションを削除する	配布ジョブ中にソフトウェアをアクティブ化するオプションを削除するには、このオプションを選択します。	無効
EPN Manager サーバーによって開始されるコピー操作	EPN Manager サーバーによってコピー操作を開始する場合は、このオプションを選択します。	無効

ステップ 3 [イメージ転送プロトコルの順序（Image Transfer Protocol Order）] で、Cisco EPN Manager がイメージを転送する際にデフォルトで使用するプロトコルを指定します。優先順位でプロトコルを並べ替えます。最初にリストされているプロトコルが失敗した場合、Cisco EPN Manager は次にリストされているプロトコルを使用します。

（注） デバイスへのイメージの配布には、デバイスでサポートされている最もセキュアなプロトコル（TFTP ではなく SCP など）を使用します。非常に大きなファイルを転送する場合、またはサーバーとクライアントが地理的に離れている場合には、TFTP はタイムアウトになる傾向があります。イメージの配布に SCP を選択する場合は、デバイスがフル ユーザー権限（特権 EXEC モード）を使用して Cisco EPN Manager で管理されていることを確認してください。フル ユーザー権限を使用しないと、配布はコピー権限エラー（「SCP：プロトコルエラー：権限拒否（SCP: protocol error: Privilege denied）」）が原因で失敗します。

ステップ 4 [保存（Save）] をクリックします。

デバイス グループを管理するソフトウェア イメージ管理サーバーの追加

イメージをデバイスのグループに配布するには、ソフトウェア イメージ管理サーバーを追加し、イメージ配布に使用するプロトコルを指定します。最大 3 つのサーバーを追加できます。

ステップ 1 サーバーを追加します。

a) **[管理（Administration）] > [サーバー（Servers）] > [ソフトウェアイメージ管理サーバー（Software Image Management Servers）]** の順に選択します。

b) [行の追加（Add Row）] アイコンをクリックし、サーバーがサポートするサーバー名、IP アドレス、およびデバイス グループを入力します。

c) [保存（Save）] をクリックします。

ステップ 2 サーバー プロトコル設定を構成します。

a) サーバー名の横にあるチェックボックスをオンにし、[プロトコルの管理（Manage Protocols）] をクリックします。

b) [行の追加（Add Row）] アイコンをクリックし、ソフトウェア イメージ管理プロトコルの詳細（ユーザー名、パスワードなど）を入力します。

c) [保存（Save）] をクリックします。

デバイスからイメージ リポジトリへのソフトウェア イメージのコピー（ベースラインの作成）

システムの設定によっては、Cisco EPN Managerがインベントリ収集時にデバイスのソフトウェアイメージをイメージリポジトリにコピーすることがあります（インベントリ収集中にイメージリポジトリに保存されたイメージの制御方法（163ページ）を参照）。この操作を手動で実行する必要がある場合は、ソフトウェア イメージをデバイスからイメージ リポジトリへ次直接インポートする次の手順を実行します。

開始する前に、イメージが（リモートにロードされているのではなく）デバイス上に物理的に存在することを確認します。

（注） 多数のイメージをインポートする場合は、生産に影響を与える可能性が最も低い時間にこの操作を実行します。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ソフトウェア イメージ（Software Images）]** の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログボックスで、次の情報を入力します。

a) [ソース（Source）] 領域では、デバイスを選択します（一度に 1 つのデバイス グループを選択することもできます）。

b) [収集オプション（Collection Options）] 領域では、ファイルをすぐにインポートするか、または後でインポートするためのスケジュールを設定するかを指定します。

ステップ 4 **[送信（Submit）]** をクリックします。

ネットワーク デバイスでどのイメージが使用されているかを調べる方法

ネットワークデバイスで使用されるイメージのリストを表示するには、**[レポート（Reports）]** > **[レポート起動パッド（Reports Launch Pad）]** > **[デバイス（Device）]** > **[ソフトウェアの詳細情報（Detailed Software）]** を選択します。

ネットワーク デバイスで使用される上位 10 個のイメージ（およびそれらのイメージを使用しているデバイスの数）を一覧表示するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ソフトウェアイメージ（Software Images）]** を選択します。[便利なリンク（Useful Links）] の下にある [ソフトウェアイメージリポジトリ（Software Image

Repository）] をクリックし、ページの右上隅にある [イメージダッシュボード（Image Dashboard）] アイコンをクリックします。

デバイスに最新のイメージがあることを確認する方法

デバイス タイプがイメージの推奨事項に対応している場合、次の手順を使用して、デバイスが Cisco.com からの最新のイメージが設定されているかどうかを確認できます。それ以外の場合は、Cisco.com の製品サポート ページを使用して、この情報を取得します。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]** を選択し、デバイス名のハイパーリンクをクリックして [デバイスの詳細（Device Details）] ページを開きます。

ステップ 2 [ソフトウェアイメージ（Software Image）] タブをクリックし、[推奨されるイメージ（Recommended Images）] 領域までスクロールします。Cisco EPN Manager には、デバイスに対して推奨される Cisco.com のすべてのイメージが一覧表示されます。

Cisco NCS 2000 と Cisco ONS のデバイスの場合、この選択肢は [シャーシビュー（Chassis View）] タブをクリックすると、右側に表示されます。

（注） 推奨事項のリストは情報提供のみを目的としています。推奨されるイメージのいずれかを使用するには、Cisco.com から取得し、イメージ リポジトリに追加する必要があります。ソフトウェア イメージをリポジトリに追加（インポート）する （169 ページ） を参照してください。

イメージ リポジトリに保存されたイメージを表示する

この手順は、イメージ リポジトリに保存されたすべてのソフトウェア イメージを一覧表示する場合に使用します。イメージはイメージタイプ別に分類され、対応するソフトウェアイメージのグループ フォルダに保存されます。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェアイメージ（Software Images）]** を選択します。Cisco EPN Manager の [ソフトウェアイメージの概要（Software Image Summary）] パネルに、イメージ リポジトリに保存されたイメージが一覧表示されます。

グローバル設定に関して実行できることは次のとおりです。

- ネットワーク デバイス（クライアント マシン上のファイル システム、IPv4 または IPv6 サーバー（URL）、FTP サーバー、および Cisco.com）からイメージ リポジトリに新しいイメージをインポートする。Web GUI を使用して、Cisco.com から入手可能なイメージを見つけることができますが、イメージは手動でダウンロードしてから、インポートする必要があります。ソフトウェア イメージをリポジトリに追加（インポート）する （169 ページ）を参照してください。

- デバイスがこのイメージにアップグレードするために満たす必要のある要件を調整する。ソフトウェア イメージをアップグレードするためのデバイス要件の変更 （173 ページ）を参照してください。
- アップグレード分析を実行する。デバイスがイメージ要件を満たしていることの確認（アップグレード分析） （174 ページ）を参照してください。
- 新しいソフトウェア イメージをデバイスにコピーする。 デバイスへの新しいソフトウェア イメージの配布 （174 ページ）を参照してください。
- イメージをアクティブにして、新しいイメージをデバイスの実行イメージにする。デバイスで新しいソフトウェア イメージをアクティブにする （182 ページ）を参照してください。
- Cisco IOS XR イメージをコミットすることにより、デバイスのリロード後もイメージを保持し、ロールバック ポイントを作成する。デバイスのリロード間での Cisco ISO XR イメージのコミット （188 ページ）を参照してください。
- イメージ リポジトリからイメージを削除する（イメージの削除は手動プロセスでのみ行えます）。イメージ リポジトリからのソフトウェア イメージ ファイルの削除 （189 ページ）を参照してください。

ステップ 2 ソフトウェア イメージ リポジトリに移動し、ソフトウェア イメージのハイパーリンクをクリックして、ファイル名、イメージ名、ファミリ、バージョン、ファイル サイズなどが一覧表示された [イメージ情報（Image Information）] ページを開きます。

グローバル設定に関して実行できることは次のとおりです。

- ページの下部にある [デバイスの詳細（Device Details）] 領域をチェックして、どのデバイスがこのイメージを使用しているかを確認します。
- デバイスがこのイメージにアップグレードするために満たす必要のある要件を調整する。（ソフトウェア イメージをアップグレードするためのデバイス要件の変更 （173 ページ） を参照。）

イメージを使用しているデバイスの確認

ステップ 1 [インベントリ （Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [ソフトウェア イメージの概要（Software Image Summary）] パネルで、ナビゲーション領域のイメージ カテゴリを展開するか、または [クイック フィルタ（Quick Filter）] フィールドのいずれかにテキストの一部を入力して、対象のイメージを見つけます。たとえば、[バージョン（Version）] フィールドに **3.1** と入力すると、3.12.02S、3.13.01S などのバージョンが一覧表示されます。

ステップ 3 イメージのハイパーリンクをクリックして、[ソフトウェアイメージの概要（Software Image Summary）] ページを開きます。そのイメージを使用するすべてのデバイスが Cisco EPN Manager の [デバイスの詳細（Device Details）] 領域に一覧表示されます。

Cisco.comからソフトウェアをダウンロードする権限があるかどうかを調べる方法

Cisco EPN Manager には、指定したデバイス タイプに推奨される最新のソフトウェア イメージが表示され、Cisco.com からソフトウェア イメージを直接ダウンロードできます。Cisco.com から EULA または K9 ソフトウェア イメージをダウンロードするには、EULA 契約または K9 契約を定期的に承認または更新する必要があります。

Cisco EPN Manager には延期されたソフトウェア イメージは表示されません。詳細については、『Cisco EPN Manager 2.1 Supported Devices』リストを参照してください。

ソフトウェア イメージをリポジトリに追加（インポート）する

Cisco EPN Manager では、指定したデバイス タイプに推奨される最新のソフトウェア イメージが表示され、Cisco.com からソフトウェア イメージを直接ダウンロードできます。Cisco EPN Manager には、提供が停止されたソフトウェア イメージは表示されません。詳細については、「Cisco EPN Manager 3.1 のサポート対象デバイス」のリストを参照してください。

（注） Cisco.com から K9 ソフトウェア イメージをダウンロードするには、定期的に https://software.cisco.com/download/eula.html K9 契約を確認して同意する必要があります。

次のトピックでは、ソフトウェア イメージをイメージ リポジトリに追加するさまざまな方法について説明します。失敗したインポートのトラブルシューティング方法の例については、ジョブ ダッシュボードを使用したジョブの管理 （32 ページ）を参照してください。

- 管理対象デバイスで実行されているソフトウェア イメージの追加 （170 ページ）
- IPv4 サーバー（URL）からのソフトウェアイメージの追加 （171 ページ）
- FTP プロトコル サーバーのソフトウェア イメージの追加（プロトコル） （171 ページ）
- クライアント マシンのファイル システムからのソフトウェア イメージの追加 （172 ページ）

（注） Cisco NCS デバイスと Cisco ONS デバイスの場合、ソフトウェア イメージをインポートするには、クライアント マシンのファイル システムからのソフトウェア イメージの追加 （172 ページ）に記載された手順を使用する必要があります。

管理対象デバイスで実行されているソフトウェア イメージの追加

この方法では、管理対象デバイスからソフトウェア イメージを取得し、イメージ リポジトリにそのイメージを保存します。

（注） デバイスへのイメージの配布には、デバイスでサポートされている最もセキュアなプロトコル（TFTP ではなく SCP など）を使用します。非常に大きなファイルを転送する場合、またはサーバーとクライアントが地理的に離れている場合には、TFTP はタイムアウトになる傾向があります。イメージの配布に SCP を選択する場合は、デバイスがフル ユーザー権限（特権 EXEC モード）を使用して Cisco EPN Manager で管理されていることを確認してください。フル ユーザー権限を使用しないと、配布はコピー権限エラー（「SCP：プロトコル エラー：権限拒否（SCP: protocol error: Privilege denied）」）が原因で失敗します。

デバイスからサーバーにイメージをコピーする場合のみ（その逆ではない）、TFTP がサポートされることに注意してください。

制限事項

- Cisco IOS XR デバイスの場合、デバイスからのイメージの直接インポートは、Cisco EPN Managerによってサポートされていません。SMU と PIE のインポートも、これらのデバイスではサポートされていません。
- Cisco IOS-XE デバイスについては、デバイスが「packages.conf」ファイルを使用してロードされている場合、そのデバイスからイメージを直接インポートすることはできません。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ソフトウェア イメージ（Software Images）]** の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、

a) [デバイス（Device）] をクリックし、[コレクション オプション（Collection Options）] の下で 1 つ以上のデバイスを選択します。

b) VRF 経由での収集を有効にする場合は、[VRF 名（VRF Name）] チェックボックスをオンにして VRF 名を指定します。

c) [スケジュール（Schedule）]エリアで、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

d) [送信（Submit）] をクリックします。

ステップ 4 ジョブのステータスを表示するには、ポップアップ メッセージ内のジョブ リンクをクリックするか、**Administration > Job Dashboard** を選択します。

ステップ 5 イメージが [ソフトウェア イメージ（Software Images）] ページ（**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ソフトウェア イメージ（Software Images）]**）に表示されていることを確認します。

IPv4 サーバー（URL）からのソフトウェアイメージの追加

ネットワークアクセス可能なIPv4サーバーからソフトウェアイメージをインポートできます。次のファイル形式がサポートされます。.bin、.tar、.aes、.pie、.mini、.vm、.gz、.ova、および .ros。

インポートするファイルは、推奨されるファイルの命名規則に従う必要があります。たとえば、.tar ファイルの命名規則は *image family*-*****-*image version*.**tar** です。image family は大文字で入力する必要があります。命名規則に基づいた NCS540.tar ファイルの名前は、**NCS540-iosxr-k9-6.0.2.tar** です。

Cisco EPN Manager は、シスコ以外の標準イメージのインポートをサポートしています。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、次の手順を実行します。

a) **URL** をクリックします。

b) [イメージを収集する URL（URL To Collect Image）] フィールドに、URL を次の形式で入力します（ユーザー クレデンシャルが必要ない HTTP URL を使用することもできます）。

http://*username***:***password***@***server-ip/filename*

c) [スケジュール（Schedule）]エリアで、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

d) **Submit** をクリックします。

ステップ 4 ジョブのステータスを表示するには、ポップアップ メッセージ内のジョブ リンクをクリックするか、**Administration > Job Dashboard** を選択します。

ステップ 5 イメージが [ソフトウェア イメージ（Software Images）] ページ（**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）]**）に表示されていることを確認します。

FTP プロトコル サーバーのソフトウェア イメージの追加（プロトコル）

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、次の手順を実行します。

a) **Protocol** をクリックします。

b) [プロトコル（Protocol）] フィールドに FTP と入力してから、FTP ユーザー名、パスワード、サーバー名または IP アドレス、およびファイル名を入力します。ファイル名の例は次のとおりです。

/*ftpfolder*/asr901-universalk9-mz.154-3.S4.bin

c) [スケジュール（Schedule）] エリアで、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

d) **Submit** をクリックします。

ステップ 4 ジョブのステータスを表示するには、ポップアップ メッセージ内のジョブ リンクをクリックするか、**Administration > Job Dashboard** を選択します。

ステップ 5 [ソフトウェア イメージ（Software Images）] ページ（[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）]）に、イメージがリストされていることを確認します。

クライアント マシンのファイル システムからのソフトウェア イメージの追加

始める前に

ソフトウェア イメージ ファイルをインポートすると、ブラウザ セッションが一時的にブロックされます。アップロード処理がブラウザ セッションのアイドル タイムアウトの制限値を超えると、Cisco EPN Manager からログアウトされて、ファイルのインポート操作が異常終了します。したがって、インポート操作を開始する前に、アイドル タイムアウトの制限値を増やすことを推奨します。アイドル タイムアウト値を増やすには、アイドル ユーザー用のグローバル タイムアウトを設定する （1028 ページ）を参照してください。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、次の手順を実行します。

a) **File** をクリックします。

b) **[Browse]** ボタンをクリックし、ソフトウェア イメージ ファイルに移動します。

c) [スケジュール（Schedule）] 領域で、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

d) **Submit** をクリックします。

（注） [ファイル（File）] オプションを使用したインポートは推奨されないため、より大きなサイズ（200 MB より大きい場合など）のファイルをインポートするには URL または [プロトコル（Protocol）] オプションを使用する必要があります。

ステップ 4 ジョブのステータスを表示するには、ポップアップ メッセージ内のジョブ リンクをクリックするか、**Administration > Job Dashboard** を選択します。

ステップ 5 [ソフトウェアイメージ（Software Images）]ページ（[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）]）に、イメージがリストされていることを確認します。

ソフトウェアイメージをアップグレードするためのデバイス要件の変更

以下の手順を使用して、ソフトウェアイメージをデバイスに配布するためにデバイスが満たす必要のある RAM、フラッシュ、およびブート ROM の要件を変更します。アップグレード分析を行う場合、これらの値を確認します（デバイスがイメージ要件を満たしていることの確認（アップグレード分析） （174 ページ）を参照）。

（注） この操作は、Cisco NCS 2000 と Cisco ONS ファミリのデバイスでのみサポートされます。

ステップ 1 [インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [ソフトウェア イメージ サマリー（Software Image Summary）] パネルで、関連付けられたハイパーリンクをクリックすることによって、ソフトウェア イメージを検索および選択します。

ステップ 3 ソフトウェア イメージ名のハイパーリンクをクリックして、イメージ情報を開きます。

ステップ 4 以下のように、デバイス要件を調整します。

- 最小 RAM（1 ～ 999999999999999）
- 最小 FLASH（1 ～ 999999999999999）
- ブート ROM の最小バージョン

ステップ 5 **Save** をクリックします。

ステップ 6 以前の要件を維持するには、[デフォルトに戻す（Restore Defaults）] をクリックします。

デバイスがイメージ要件を満たしていることの確認（アップグレード分析）

アップグレード分析では、デバイスのRAMまたはFLASH（デバイスのタイプによって異なります）容量は十分であるか、イメージはデバイスファミリと適合するか、およびソフトウェアのバージョンはデバイス上で実行中のイメージのバージョンと適合するかを確認できます。分析の後、デバイスごとの結果を提供するレポートがCisco EPN Managerで表示されます。レポートデータは以下から収集されます。

- ソフトウェアイメージリポジトリ。これには、イメージヘッダー内の最小RAM、最小フラッシュなどの情報が含まれます。
- Cisco EPN Managerインベントリ。これには、デバイス上のアクティブイメージに関する情報と、フラッシュメモリ、モジュール、プロセッサの詳細が含まれます。

（注） アップグレード分析は、Cisco ASR 9000デバイスを除くすべてのCisco IOS-XRデバイス（Cisco NCS 1000、Cisco NCS 4000、Cisco NCS 5000、Cisco NCS 5500、およびCisco NCS 6000）でサポートされています。

イメージのデバイス要件を調節する場合は、ソフトウェアイメージをアップグレードするためのデバイス要件の変更 （173 ページ）を参照してください。

ステップ1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ2 [便利なリンク（Useful Links）] で、**[アップグレード分析（Upgrade Analysis）][ソフトウェアイメージアップグレード分析（Software Image Upgrade Analysis）]** をクリックします。（[ソフトウェアイメージ（Software Images）] ページから画像を選択しないでください）。

ステップ3 [アップグレード分析（Upgrade Analysis）] ダイアログで以下を行います。

a) ソフトウェア イメージのソース（イメージ リポジトリまたは Cisco.com）を選択します。
b) 分析するデバイスを選択します。
c) デバイスを分析するソフトウェア イメージを選択します。
d) [レポートの実行（Run Report）] をクリックします。

レポートでは、デバイスが IP アドレスでグループ化されます。

デバイスへの新しいソフトウェア イメージの配布

イメージ配布操作では、新しいソフトウェアイメージがデバイス上の指定場所にコピーされます。類似デバイスのイメージは、1 回の展開で配布できます。この場合、デバイスごとに選択

内容を調整します。ジョブを作成するときに、ジョブを即時に実行するか、スケジュールした時点で実行するかを決定します。

（注） Cisco EPN Manager では、TFTP によりサーバーからデバイスにイメージを配布する操作はサポートされていません。

配布するイメージを選択すると、Cisco EPN Manager では、そのイメージに適切なデバイスだけが表示されます。配布ジョブを作成するときに、Cisco EPN Manager が次のいずれを実行するかを指定します。

- 同じジョブでイメージをアクティブにするか、またはアクティブ化をスキップする。アクティブ化を遅らせることで、イメージをアクティブにする前に次の作業を実行できます。
  - メモリ不足が発生していないか確認し、イメージまたはパッケージの配布のためにディスク スペースを空ける。
  - アップグレード分析を実行し、選択したイメージに対してデバイスが適切であるかどうかを確認する。
- （Cisco IOS XR のみ）同じジョブでイメージをコミットするか、またはコミットをスキップする。

制限事項：

- Cisco IOS-XR デバイス（Cisco ASR 9000 デバイスを除く）にイメージを配布すると、インストール パッケージがアクティブ化およびコミットされる前に、イメージがデバイスのストレージにコピーされます。ただし Cisco ASR 9000 デバイスでは、イメージが Cisco EPN Managerからデバイスに直接インストールおよび追加され、デバイス ストレージにコピーされません。これにより、デバイス上のイメージによって消費される領域が減少します。イメージをデバイス ストレージにコピーせずに、イメージを非アクティブ状態にするには、次のコマンドを使用します。

  ```
  install add protocol://image path/image name
  ```

- Cisco ASR 9000 デバイスの場合、同時にアクティブ化できるデバイス/パッケージ ペアは最大 16 個です。また、.tarイメージをアクティブ化するには、同じ最大数のパッケージが含まれている必要があります。
- 配布プロセスでは、配布に使用されているプロトコルがデバイスでサポートされていない場合、配布に失敗する可能性があります。たとえば SCP プロトコルを使用してイメージを Cisco ASR 9000 デバイスに配布すると、これらのデバイスのコマンド ラインではデバイス ストレージへのイメージのコピーがサポートされていないため、配布に失敗します。
- EPNM は、並行して最大 5 のアクティブな配布操作をサポートします。これらの配布操作にはアクティブ化操作は含まれません。

イメージはデバイス上の任意のファイル システム（ルート ディレクトリにあるフォルダを含む）に配布できます。これは、NCS 42XX、NCS520（IOS-XE）、および ASR907 デバイスで

のみサポートされています。スタンバイ フラッシュがあるファイル システムを選択すると、イメージはアクティブ フラッシュとスタンバイ フラッシュの両方に配布されます。つまり、イメージをアクティブ フラッシュに配布する場合、スタンバイ フラッシュにイメージを再配布する必要はありません。

（注） デバイス フォルダにイメージを直接配布するオプションは、Cisco ASR907 デバイスと Cisco NCS42xx デバイスでのみサポートされています。

処理の進行に伴い、Cisco EPN Manager にフィードバックとステータスが表示されます。イメージを多数のデバイスに配布する場合は、アップグレード期間中にサイトのサービスが完全に停止することがないように、各リブートをずらすことができます。イメージ配布を効率的に実行するには、配布の実行元となるデバイスおよびサーバーが、地理的に同じ場所や建物内にある必要があります。ネットワークの速度低下や元々速度が遅いために配布に時間がかかる場合、配布ジョブはエラーを返します。

（注） デバイスへのイメージの配布には、デバイスでサポートされている最もセキュアなプロトコル（TFTP ではなく SCP など）を使用します。非常に大きなファイルを転送する場合、またはサーバーとクライアントが地理的に離れている場合には、TFTP はタイムアウトになる傾向があります。イメージの配布に SCP プロトコルを選択する場合は、デバイスがフル ユーザー権限（特権 EXEC モード）を使用して Cisco EPN Manager で管理されていることを確認してください。フル ユーザー権限を使用しないと、配布はコピー権限エラー（「SCP：プロトコル エラー：権限拒否（SCP: protocol error: Privilege denied）」）が原因で失敗します。

はじめる前に

- デバイスへのイメージの配布には、デバイスでサポートされている最もセキュアなプロトコル（TFTP ではなく SCP など）を使用します。非常に大きなファイルを転送する場合、またはサーバーとクライアントが地理的に離れている場合には、TFTP はタイムアウトになる傾向があります。イメージの配布に SCP プロトコルを選択する場合は、デバイスがフル ユーザー権限（特権 EXEC モード）を使用して Cisco EPN Manager で管理されていることを確認してください。フル ユーザー権限を使用しないと、配布はコピー権限エラー（「SCP：プロトコル エラー：権限拒否（SCP: protocol error: Privilege denied）」）が原因で失敗します。
- イメージを Cisco ME 1200 デバイスに配布するときには、配布直後にデバイスでイメージをアクティブにする必要があります。デバイスでイメージのアクティブ化を実行できる状態であることを確認します。

ステップ 1 [インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 ソフトウェアイメージ管理ライフサイクル ウィジェットの青い [**Distribute**] アイコンをクリックします。Cisco EPN Manager に、イメージに適切なデバイスが表示されます。イメージ設定は、配布ジョブの作成時にデバイスごとに変更できます。

（注） 必要なデバイスがリストにない場合は、ファイルに関連付けられているイメージ ファミリが、選択されているデバイスのファミリと同一であることを確認してください。

デバイス ファミリ、タイプ、バージョン、サイズを確認するには、[デバイスの詳細（Device Details）] ページの [イメージ（Image）] タブを使用します。

ステップ 3 [イメージの選択（Image Selection）] タブから、デバイスに配布するイメージを選択します。

（注） 選択したイメージのイメージ ファミリ、タイプ、バージョン、およびサイズの詳細を確認します。

ステップ 4 [デバイスの選択（Device Selection）] タブから、イメージを配布するデバイスを選択します。デバイスごとに配布設定を詳細に調整できます。

ステップ 5 [イメージ詳細の検証（Image Details Verification）] タブの [配布場所（Distribute Location）] ドロップダウン メニューを使用して、イメージを配布する必要があるデバイス上のファイル システムを選択します。このフィールドには、デバイス上で使用可能なフォルダが表示されます。新しいフォルダにイメージを配布するには、デバイスでフォルダを手動で作成してから、このステップに戻ります。あるいは、配布プロセス中に自動的に新しいフォルダを作成することもできます。このためには、「/opt/CSCOlumos/swim」内の「swim_configuration.xml」ファイルを選択し、新しいフォルダの名前を指定します。このディレクトリの下にフォルダが自動的に作成されます。[検証状態（Verification State）] フィールドに、選択したソフトウェアのステータスが表示されます。ステータス（[成功（Success）] または [失敗（Failure）]）に基づいて、選択したデバイスの互換性の状態を判断できます。たとえば、状態が成功の場合はイメージの配布を続行するのに十分なスペースがあります。

a) Cisco EPN Manager の [イメージの詳細の検証（Image Details Verification）] タブには、デバイスとイメージごとに 1 つの行が表示されます。
b) 各デバイスのイメージのコピー先の場所を確認します。Cisco EPN Manager では、メモリの計算に基づいて場所が選択されます。

（注） Cisco NCS 2000 ファミリおよび Cisco ONS ファミリのデバイスでは、場所が指定されません。

場所を変更するには、[イメージの配布（Distribute Image）] フィールドで場所の値をダブルクリックし、ドロップダウンリストから別の場所を選択します。

[**Save**] をクリックすると、Cisco EPN Manager により、その場所にイメージを格納できるだけの十分なスペースがあるかどうかが判別されます。十分なスペースがある場合は、[**Save**] のクリック後に Cisco EPN Manager に緑のチェックマークが表示されます。それ以外の場合は、別の場所を選択するか、またはステップ 5 で [配布前にスマート フラッシュ削除（Smart Flash Delete Before Distribution）] オプションを選択する必要があります。実行中のイメージはデバイスから削除されないことに注意してください。

ステップ 6 配布設定を行います。

[イメージ展開（Image Deployment）] タブ領域で、配布ジョブの動作（一括配布ジョブで配布がデバイスで失敗した場合に続行するかどうかなど）を設定します（この設定は、管理者が設定したデフォルトに

基づいて読み込まれます。詳細については、イメージの転送および配布設定の調整（163 ページ）を参照してください）。

SVO デバイスの場合：

- [デバイスの選択（Device Selection）] で ROADM インスタンスを選択した場合、使用可能な [分散（Distribute）] オプションは [SVO]、[NCS2K]、および [両方（Both）] です。
- [デバイスの選択（Device Selection）] で OLA インスタンスを選択した場合、使用可能な [分散（Distribute）] オプションは [NCS2K] です

イメージ展開オプション

- [配布前にスマートフラッシュ削除（Smart Flash Delete Before Distribution）]：デバイスのメモリが不足している場合に備えて、（実行中のイメージを除く）すべてのファイルを削除し、ディスク スペースを空けます（選択したフラッシュに十分な空きスペースができるまで、他のイメージ ファイルも削除されます）。
- [失敗時に配布を続行（Continue on Failure）]：デバイスで配布が失敗しても、配布を続行します。
- [TFTPフォールバック（TFTP Fallback）]：TFTP フォールバック コマンドを実行イメージに挿入して、配布の失敗時にイメージをリロードします。
- [ブートコマンドの挿入（Insert Boot Command）]：イメージの配布後に、実行イメージにブート コマンドを挿入します。
- [ISSU]：In-Service Software Upgrade（ISSU）をアクティブ化して、最小限のサービス中断でデバイスのソフトウェアを更新します。
- [FPDイメージのアップグレード（Upgrade FPD image）]：Field Programmable Device（FPD）とは、個別のソフトウェア アップグレードをサポートする、ルータ カードに実装されたハードウェア デバイスのことです。このオプションを選択すると、イメージの配布とアクティブ化のプロセスで、アップグレードのために FPD イメージ パッケージが自動的に選択されます。その他の機能には次のものがあります。
  - [配布前にスマート フラッシュ削除（Smart Flash Delete Before Distribution）]
  - [同時配布（Parallel Distribution）]
  - [失敗時に配布を続行（Continue distribution on failure）]
- [インターフェイスモジュールの遅延（Interface Module Delay）]：各インターフェイス モジュール（IM）の活性挿抜（OIR）間の遅延を調整します。
- [実行中のイメージの消去（Erase Running Image）]：デバイスの実行中のイメージを消去します。
- **[VRF による配布（Distribute via VRF）]**：VRF を使用してイメージを配布するには、[VRF による配布を追加する（Add Distribute via VRF）] チェックボックスをオンにします。
  - [VRF名（VRF Nam）]：イメージの配布およびファイル転送に使用する適切な VRF（VPN ルーティングおよび転送）名を入力します。

（注） このフィールドは、[VRFによる配布（Distribute via VRF）]チェックボックスがオンになっている場合にのみ使用できます。

複数のデバイスが選択されている場合は、[VRF名（VRF Name）]フィールドに共通のVRF 名のみが表示されます。

表 *12:* イメージ展開オプションのサポート

デバイス	[配布前にスマートフラッシュ削除（Smart Flash Delete Before Distribution）]	[失敗時に配布を続行（Continue distribution on Failure）]	[TFTPフォールバック（TFTP Fallback）]	[ブートコマンドの挿入（Insert Boot Command）]
Cisco IOS（ASR 901）	対応	対応	対応	対応
Cisco IOS-XE（ASR 903/920）	対応	対応	対応	対応
Cisco IOS XE（NCS 4200/ASR 907）	対応	対応	-	対応
Cisco Nexus	対応	対応	対応	対応
Cisco IOS（ME36X/ME38X）	対応	対応	対応	対応
Cisco IOS-XR	対応（Cisco ASR 9000デバイスの場合、実行中のイメージより前のバージョンの .tar イメージは削除されます）	対応	-	-
Cisco NCS 2000 と Cisco ONS 15454	-	対応	-	-
Cisco NCS 4000	対応	対応	-	-
Cisco NCS 1000	対応	対応	-	-
Cisco NCS 6000	-	-	-	-
SVO	-	対応	-	-

表 *13* : イメージ展開オプションのサポート

デバイス	ISSU	[FPDイメージのアップグレード（Upgrade FPD image）]	[インターフェイスモジュールの遅延（Interface Module Delay）]	[実行中のイメージの消去（Erase Running Image）]	[VRFによる配布（Distribute via VRF）]
Cisco IOS（ASR 901）	-	-	-	-	対応
Cisco IOS-XE（ASR 920）	-	-	-	-	対応
Cisco IOS XE（NCS 4200/ASR 903/907）	対応（デバイスが「インストール」モードの場合のみ）	-	対応（ISSUが使用可能な場合のみ）	-	対応
Cisco Nexus	-	-	-	-	-
Cisco IOS（ME36X/ME38X）	-	-	-	対応	-
Cisco IOS-XR	Y（NCS4K、ASR9K 32ビット、およびNCS560のみ）	-	-	-	-
Cisco NCS 2000 と Cisco ONS 15454	-	-	-	-	-
Cisco NCS 4000	対応	対応	-	-	-
Cisco NCS 1000	-	対応	-	-	-
Cisco NCS 6000	-	-	-	-	-

ステップ 7 必要に応じて [ジョブオプションのアクティブ化（Activate Job Options）] ウィンドウで、必要な設定を選択します。

- [アクティブ化オプション（Activate Options）] : [順次（Sequential）] または [並行（Parallel）]
- [失敗後に続行（Continue on Failure）] : デバイスで配布が失敗した場合でも、配布を続行します。
- [コミット（Commit）] : 配布後にデバイスでイメージをコミットします。
- [FPD アップグレード（FPDs Upgrade）] : Field-Programmable Device（FPD）とは、ルータ カードに実装し、個別のソフトウェア アップグレードをサポートするハードウェア デバイスのことです。このオプションを有効にすると、アップグレードに FPD イメージ パッケージが使用されます。

ステップ 8 イメージ アクティブ化の設定を行います。

デバイスの OS	設定
Cisco IOS および Cisco IOS XE	デバイスのリロード時にイメージをアクティブ化する場合は、[**Insert Boot Command**] をオンにして、以下の操作を行います。 • 処理の完了時にデバイスをリロードする（およびイメージをアクティブ化する）場合は、ドロップダウンリストから [**Sequential**] または [**Parallel**] を選択します。このオプションは Cisco IOS XE デバイスでは使用できません。 • 処理の完了時にデバイスをリロードしない場合は、ドロップダウンリストから [**OFF**] を選択します。 [ブートコマンドの挿入（Insert Boot Command）] をオンにせずにイメージをアクティブ化する場合は、[**Sequential**] または [**Parallel**] を選択します。
Cisco IOS XR、Cisco NCS 2000、Cisco ONS	• イメージをアクティブ化またはリロードする場合は、ドロップダウンリストから [**Sequential**] または [**Parallel**] を選択します。 • イメージをアクティブ化しない場合は、ドロップダウンリストから [**OFF**] を選択します。 （注） ISSU アップグレードを実行する場合は、ドロップダウンリストから [オフ（OFF）] を選択します。このオプションは、一部の Cisco IOS XR デバイス（NCS4K、ASR9K 32 ビット、NCS560 など）のみに適用されます。 （注） ドロップダウンリストから [オフ（OFF）] を選択すると、[イメージのダウングレードのみ（Only image downgrade）] オプションが無効になります。このオプションはすべての Cisco NCS 2000 デバイスに適用されます。

Admin 設定で、配布プロセスでイメージをアクティブにする機能が無効に設定されているために、アクティブ化オプションが表示されないことがあります。イメージをアクティブにするには、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] に戻り、[アクティブ化] アイコンをクリックします。

ステップ 9 （Cisco IOS XR デバイス）イメージ コミット設定を行います。このジョブでイメージをコミットするには、[**Commit**] をオンにします。イメージを後でコミットする場合は、[**Commit**] をオンにせずに、デバイスのリロード間での Cisco ISO XR イメージのコミット （188 ページ）の手順に従います。

ステップ 10 [配布スケジュール（Schedule Distribution）] エリアでは、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュール設定します。

ステップ 11 **Submit** をクリックします。

ステップ 12 **Administration > Job Dashboard** を選択し、イメージ配布ジョブに関する詳細を確認します。

（注） コピー タスクにかかる時間が 2 時間を超える場合は、Cisco EPN Manager から選択したデバイスまでの接続速度を確認します。

次のタスク

次に示すイメージ配布エラーが発生した場合は、示されているコマンドを使用してデバイスを設定し、もう一度試してください。

問題：[この端末からの ssh 接続は許可されていません（ssh connections not permitted from this terminal'）] というエラーが発生する。

原因：デバイスの設定が誤っています。

解決策：次のコマンドを使用してデバイスを設定します。

```
line vty 0 <number available in the device>
               transport input ssh
               transport output ssh
```

<number available in the device>：デバイスで実行されている IOS バージョンに応じた固有識別子（15 ～ 100 以上）を表します。

（注） これらのコマンドは、Cisco IOS-XR デバイスではサポートされていません。

デバイスで新しいソフトウェアイメージをアクティブにする

（注） Cisco IOS XR イメージをアクティブにするには、以下の手順、またはCisco IOS XR イメージのアクティブ化、非アクティブ化、およびデバイスからの削除（186ページ）の手順（単一デバイスで非アクティブ化操作を実行します）を実行できます。

新しいイメージがデバイスでアクティブになっている場合、それがディスクで実行されているイメージになります。新しいイメージをアクティブにしても、非アクティブにされたイメージは削除されません。デバイスからイメージを手動で削除する必要があります。

同じジョブで、イメージの配布とアクティブ化を実行する場合、デバイスへの新しいソフトウェア イメージの配布 （174 ページ）を参照してください。

新しいイメージをデバイスに配布せずに、イメージをアクティブにするには（たとえば、デバイスにアクティブにしたいイメージが存在する）、次の手順を実行します。アクティブ化は配布操作を使用しますが、新しいイメージを配布しません。

（注） EPNM は、並行して最大 20 のアクティブなアクティブ化操作をサポートします。これらのアクティブ化操作には、配布操作は含まれません。

始める前に

- Cisco NCS 2000 デバイスでイメージをアクティブにする、または復元する前に、デバイスで抑制されているすべてのアラームが無効にされていることを確認してください。
- **ISSU** オプションを選択してバンドル モードでイメージをアクティブにする場合は、**show version | in image** コマンドを実行してイメージが「.bin」形式であるかどうかをチェックし、デバイスが現在バンドル モードであるかどうかを確認できます。また、[デバイスの詳細（Device Details）] ビューの [イメージ（Images）] タブで、イメージのファイル名を確かめることによって、イメージの形式を確認することができます。
- ISSU オプションを使用してアクティブにする際、デバイスがサブパッケージ モードである場合（たとえば、イメージが「bootflash:ISSU/packages.conf」という形式である場合）、必ず同じフォルダを使用してイメージをアクティブにします。

ステップ 1 [インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 ソフトウェア イメージ管理ライフサイクル ウィジェットの [有効化（Activate）] アイコンをクリックします。

ステップ 3 （注） スタンバイ バージョンがアクティブ バージョンよりも古い場合、アクティブ化の操作は実行できません。

[有効化ソース（Activation Source）] タブで、必要に応じて [ライブラリから有効化（Activate from Library）]、[完了した配布ジョブから有効化（Activate from Completed Distribution Jobs）]、または [スタンバイ/代替イメージから有効化（Activate from Standby/Alternate Images）] を選択します。

ステップ 4 [完了した配布ジョブから有効化（Activate from Completed Distribution Jobs）] を選択する場合は、ジョブ選択タブに移動して、配布に成功または一部成功したジョブを選択します。次に、[プレビューの有効化（Activate Preview）] タブに移動し、イメージ名とフラッシュの詳細が表示されたデバイスリストを選択します。[ジョブオプションの有効化（Activate Job Options）] タブをクリックします。

ステップ 5 [ジョブ オプションの有効化（Activate Job Options）] ウィンドウで、必要な設定を選択し、ステップ 10 に移動します。

- [失敗後に続行（Continue on Failure）]：デバイスで配布が失敗した場合でも、アクティブ化を続行します。
- [コミット（Commit）]：配布後にデバイスでイメージをコミットします。
- [ブートコマンドの挿入（Insert Boot Command）]：イメージの配布後に、実行イメージにブート コマンドを挿入します。これは、ISSUオプションを指定したデバイスをアクティブ化する際の前提条件です。
- [オプションのアクティブ化（Activate Options）]：[オフ（Off）]、[順次（Sequential）]、または [並行（Parallel）]
- [失敗後に続行（Continue on Failure）]：デバイスで配布が失敗した場合でも、配布を続行します。
- [コミット（Commit）]：配布後にデバイスでイメージをコミットします。

- [FPD アップグレード（FPDs Upgrade）]：Field-Programmable Device（FPD）とは、ルータ カードに実装し、個別のソフトウェア アップグレードをサポートするハードウェア デバイスのことです。このオプションを有効にすると、アップグレードに FPD イメージ パッケージが使用されます。
- ISSU オプション：
  - [デバイスアップグレードモード（Device Upgrade Mode）]：オプションは次のとおりです。
    - [バンドルモード（Bundle Mode）]：**ISSU** オプションを選択してイメージをアクティブにするには、[バンドルモード（Bundle Mode）] を選択し、モノリシック Cisco IOS イメージを使用して起動します。これにより、.bin ファイルをポイントしているデバイスのブート変数がバンドルモードで稼働しているデバイスを取得します。このオプションを選択するには、アクティブ化後にデバイスをリロードする必要があります。デバイスがバンドル モードであるかどうかを確認するには、コマンド **show version | in image** を実行して、イメージが「.bin」形式であるかどうかを確認します。また、[デバイスの詳細（Device Details）] ビューの [イメージ（Images）] タブで、イメージのファイル名を確かめることによって、イメージの形式を確認することができます。
    - [インストールモード（Install Mode）]：ISSU オプションを使用してアクティブにするとき、デバイスがサブパッケージモードである場合（たとえば、イメージが「bootflash:/ISSU/packages.conf」形式である場合）に、このオプションを使用します。デバイスはインストールモードで実行されます。イメージをアクティブにするために、同じフォルダを使用します。フォルダの場所を変更すると、アクティブ化の操作が失敗します。イメージモードですでに実行しているデバイスのインストール モードを選択した場合、デバイスは（ISSU の）リロードをしなくてもアクティブになり、ブート イメージは packages.conf ファイルをポイントし続けます。他のすべてのシナリオでは、デバイスがリロードされます。

      （注） 重複するブート変数を回避するため、デバイスの現在のブート変数が「bootflash:/ISSU/packages.conf」であることを確認します。

    - [すでに存在（Currently Exists）]：現在動作しているモード（インストールまたはバンドル）と同じモードでデバイスをアクティブにする場合、このオプションを選択して同じモードでイメージをアクティブにします。
  - [インターフェイスモジュールの遅延（Interface Module Delay）]：このオプションで指定した時間（秒単位）により、各インターフェイス モジュール（IM）の活性挿抜（OIR）間の遅延が調整されます。このオプションは、ブート コマンドの挿入と ISSU オプションが有効である場合のみ、サポート対象デバイスが選択されている場合に有効です。アップグレードに十分な時間を確保するために、遅延の値を 1200 秒以上に設定することをお勧めします。

ステップ 6 [有効化ソース（Activation Source）] タブの [ライブラリから有効化（Activate from Library）] を選択する場合は、[イメージ選択（Image Selection）] タブをクリックします。

ステップ 7 [スタンバイ イメージからアクティブ化（Activate from Standby Image）] を選択する場合、ステップ 9 に進みます。

ステップ 8 [イメージ選択（Image Selection）] タブで、配布するソフトウェア イメージを選択します。

ステップ 9 [デバイスの選択（Device Selection）] タブをクリックし、イメージをアクティブ化するデバイスを選択します。

a) [デバイスの選択方法（Select devices by）] トグル ボタンをクリックして、[グループ（Group）] または [デバイス（Device）] オプションからデバイスを選択できます。

b) [グループ（Group）] オプションを選択した場合は、デバイス グループを選択し、[デバイスの選択（Choose Devices）] ペインに一覧表示されるデバイスを選択します。選択したデバイスは、[選択されたデバイス（Selected Devices）] ペインに表示されます。

デフォルトで、選択したイメージを適用できるデバイスが表示されます。たとえば、ステップ 3 で [スタンバイ/代替イメージからアクティブ化（Activate from Standby/Alternate Images）] オプションを選択した場合、[デバイスの選択（Device Selection）] タブには、スタンバイ/代替イメージのアクティブ化をサポートする Cisco NCS 2000、Cisco ONS 15454、Cisco ME1200 などのデバイスだけが表示されます。

ステップ 10 [イメージの有効化（Activate Image）] タブをクリックし、選択したデバイスおよびソフトウェア イメージを有効化するために正しくマッピングしているかどうかを確認します。アクティブ化にスタンバイ イメージを使用する場合は、[イメージ選択の確認（Verify Image Selection）] タブをクリックします。

（注） スタンバイ/代替イメージをアクティブにする際に、スタンバイ/代替イメージのバージョンがデバイスで実行されているイメージよりも古いバージョンである場合、[確認ステータス メッセージ（Verification Status Message）] 列に、赤色で古いバージョンにダウングレードしようとしていることが示されます。

ステップ 11 [ジョブ オプションの有効化（Activate Job Options）] タブをクリックし、必要なジョブの有効化オプションを選択します。

[有効化（Activate）] ドロップダウン リストから [ISSU] オプションを選択した場合、デバイスの再起動は不要で、デバイスのソフトウェアイメージがアップグレードされます。

ISO XR デバイスの場合、[ISSU] チェックボックスをオンにすると、デバイスでステートフルスイッチオーバーが設定されます。

スタンバイイメージでアクティブ化する際に、選択したデバイスがダウングレードをサポートする場合、[イメージのダウングレードのみ（Only image downgrade）] チェックボックスが表示されます。このチェックボックスをオンにすると、デバイスがダウングレード操作をサポートしている場合のみ（たとえば、Cisco NCS 2000 デバイスの場合など）、ダウングレードされます。また、指定されたアップグレード操作はすべて失敗します。

SVO デバイスの場合は、[適用先（Apply to）] ドロップダウンリスト（[アクティブ化オプション（Activation Options）] の下）から [NCS2K] または [SVO] または [両方（Both）] を選択して、イメージをアクティブ化するデバイスを選択します。

ステップ 12 [スケジュールのアクティブ化（Schedule Activation）] タブに移動し、[今すぐ（Now）] または [日付（Date）] を選択して、[送信（Submit）] をクリックし、選択したデバイスのソフトウェア イメージをアクティブにします。

シスコ デバイスに関する情報、およびそれらがイメージ配布でサポートするプロトコルについては、以下の表を参照してください。

表 *14 :* シスコ デバイスとサポートされるイメージ配布プロトコル

シスコ デバイス	TFTP	[FTP]	SCP	SFTP	HTTPS
Cisco ASR 1000	対応	対応	×	対応	×
Cisco ASR9000	対応	×	×	対応	×
Cisco IOS XR（Cisco ASR9000 デバイスを除く）	対応	対応	対応	対応	×
Cisco NCS42xx、Cisco ASR9XX、または Cisco ASR 1000	対応	対応	対応	×	×
Cisco ME1200	対応	対応	×	対応	×
Cisco NCS2000 および Cisco ONS デバイス	×	対応	×	×	対応

Cisco IOS XR イメージのアクティブ化、非アクティブ化、およびデバイスからの削除

[シャーシビュー（Chassis View）] ページページから特定のデバイスでのアクティブ化、非アクティブ化、および削除操作を実行できます。このビューには、ディスク上のすべての実行イメージがリストされます。

始める前に

Cisco NCS 2000 デバイスでイメージをアクティブにする、または復元する前に、デバイスで抑制されているすべてのアラームが無効にされていることを確認してください。

ステップ 1 **[シャーシビュー（Chassis View）]** ページ ページを開き、[イメージ（Image）] タブをクリックします。

ステップ 2 [適用済みイメージ（Applied Images）] エリアを展開し、デバイスにインストールされたイメージをすべて表示します。

- アクティブ：デバイスがアクティブに使用しているイメージ。
- 非アクティブ：ブート デバイスに追加されているものの、アクティブ化されていないイメージ。

- 使用可能：物理的にデバイス上に存在するものの、ブート デバイスに追加されていないイメージ。

ステップ 3 [表示（Show）] ドロップダウンリストを使用してデバイスのイメージのリストをフィルタします。管理したいイメージを特定し、その[ステータス（Status）]フィールドをダブルクリックします。フィールドが編集可能な行に変わります。

ステップ 4 [ステータス（Status）] ドロップダウン リストから実行する操作を選択し、[保存（Save）] をクリックします。選択できるオプションは、次のとおりです。

- Active
- 非アクティブ化
- 削除（Remove）
- 追加（Add）
- 追加して有効化
- Available

ステップ 5 イメージ テーブルの上で [適用（Apply）] をクリックします。

ステップ 6 **[管理（Administration）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択し、イメージ アクティブ化ジョブの詳細を表示します。

FPD イメージの表示およびアップグレード

Field Programmable Device（FPD）とは、個別のソフトウェア アップグレードをサポートする、ルータ カードに実装されたハードウェア デバイスのことです。イメージの配布とアクティブ化のプロセスで、アップグレードのために FPD イメージ パッケージが自動的に選択されるように設定できます。アップグレードの実行前には、FPD の詳細（デバイス名、カードの種類、ハードウェアのバージョンなど）を表示できます。

手順は次のとおりです。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 FPD イメージを含むデバイスを探して選択します。

ステップ 3 [イメージ（Images）] タブをクリックします。

FPDデバイス名、ロケーション、使用可能なカードの種類とハードウェア バージョン、ATR 値、イメージのステータス、および実行中のプログラムされた値を表示できるようになりました。

ステップ 4 FPDイメージの詳細を確認したら、[FPDイメージのアップグレード（Upgrade FPD image）]ボタンをクリックしてアップグレード設定を行います。

ステップ 5 アップグレードをすぐに実行する、将来の特定の日時に実行する、または定期的に実行するようにスケジュールします。

ステップ 6 **[送信（Submit）]** をクリックします。

デバイスのリロード間での Cisco ISO XR イメージのコミット

（注） Cisco IOS XR デバイスの場合、デバイスがその設定で一定期間稼働し、パッケージの変更が適切であると確信できるまでは、パッケージ変更をコミットしないことが推奨されます。

デバイスに Cisco IOS XR パッケージをコミットすると、パッケージの設定はデバイスのリロード後にも維持されます。また、コミット操作では、ロールバック操作に使用できるロールバック ポイントがデバイスに作成されます。

イメージの配布、アクティブ化、コミットを同一ジョブで行う場合は、「デバイスへの新しいソフトウェア イメージの配布 （174 ページ）」で説明する手順を使用します。

アクティブ化したイメージをコミットするには、次の手順に従います。

（注） 単一デバイスだけを使用している場合は、[デバイスの詳細（Device Details）] ページからコミット操作を実行します（**[Image]** タブをクリックしてイメージを選択し、**[Commit]** をクリックします）。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 ソフトウェア イメージ管理ライフサイクル ウィジェットの [コミット（Commit）] アイコンをクリックします。

ステップ 3 コミットするイメージのあるデバイスを選択して、[送信（Submit）] をクリックします。（アクティブ化されているイメージだけがコミット可能です。）

ステップ 4 アクティブ化するソフトウェア イメージを選択し、[送信（**Submit**）] をクリックします。

ステップ 5 [配布スケジュール（Schedule Distribution）] エリアで、コミット ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 **Administration > Job Dashboard** を選択し、イメージ アクティブ化ジョブに関する詳細を確認します。

Cisco IOS XR イメージのロールバック

Cisco IOS XR イメージをロールバックすると、デバイス イメージが以前のインストール状態（具体的にはインストール ロールバック ポイント）に戻ります。イメージがデバイスから削除された場合、パッケージに関連付けられているロールバック ポイントもすべて削除され、そのポイントにはロールバックできなくなります。

ロールバック ジョブは、一度に1台のデバイスでのみ実行できます。同じジョブで複数のデバイスに対してロールバックを実行することはできません。

（注） ロールバック機能は、Cisco ASR 9000 デバイスなどの Cisco IOS-XR デバイスでのみサポートされます。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択し、イメージをロールバックするデバイスの名前のハイパーリンクをクリックします。

ステップ 2 [イメージ（Image）] タブをクリックし、[ロールバック情報（Rollback Info）] 領域を展開します。

ステップ 3 ロールバックするソフトウェア イメージのコミット ID を選択し、[ロールバック（Rollback）] をクリックします。ロールバック スケジューラが開きます。

ステップ 4 ロールバック操作が完了した後にイメージをコミットする場合は、[ロールバック後にコミットする（Commit After Rollback）] をオンにします。

ステップ 5 [ロールバックのスケジュール（Schedule Rollback）] 領域で、ロールバック ジョブをすぐに実行するか後で実行するようにスケジュールし、[送信（Submit）] をクリックします。

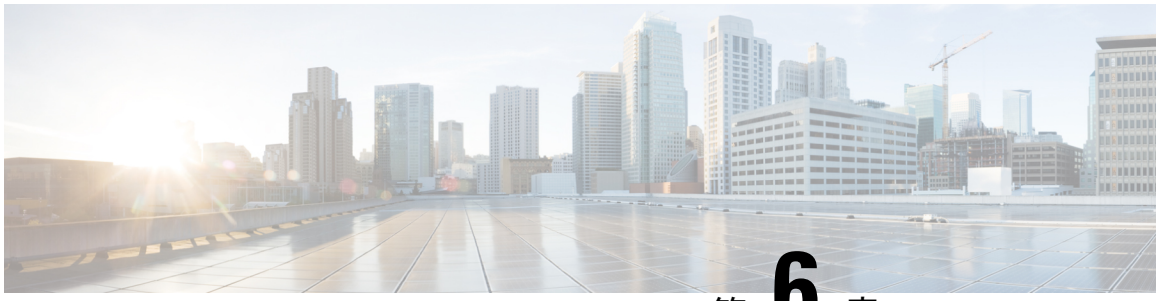
イメージ リポジトリからのソフトウェア イメージ ファイルの削除

ソフトウェア イメージは手動でのみイメージ リポジトリから削除できます。Cisco EPN Manager がイメージ リポジトリの自動消去を行うことはありません。十分な権限がある場合、次の手順に従って、イメージ リポジトリからソフトウェア イメージ ファイルを削除することができます。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ソフトウェア イメージ（Software Images）]** の順に選択します。

ステップ 2 左側の [ソフトウェア イメージ サマリー（Software Images Summary）] パネルで、削除するイメージを選択します。

ステップ 3 [削除（Delete）] をクリックします。



第 6 章

コンプライアンスを使用した設定の監査の実行

コンプライアンス監査の実行方法

次の表に、コンプライアンス機能を使用するための基本的な手順を示します。

	説明	参照先：
1	名前と他の説明テキストを含むコンプライアンス ポリシーを作成します。	新しいコンプライアンス ポリシーの作成 （193 ページ）
2	コンプライアンス ポリシーにルールを追加します。ルールは違反を構成するものを指定します。	コンプライアンス ポリシー ルールの作成 （193 ページ）

3	（ネットワーク デバイスで監査を実行するために使用する）コンプライアンス プロファイルを作成し、次の手順を実行します。 • コンプライアンス ポリシーをそのプロファイルに追加します。 • 監査に含めるポリシー ルールを選択します。 同じプロファイルに複数のカスタム ポリシーや定義済みのシステム ポリシーを追加できます。	ポリシーとルールが含まれているコンプライアンス プロファイルの作成 （200 ページ）
4	プロファイルを選択し、監査ジョブをスケジューリングして、コンプライアンス監査を実行します。	コンプライアンス監査の実行 （202 ページ）
5	コンプライアンス監査の結果を表示し、必要に応じて違反を修正します。	コンプライアンス監査の結果の表示 （203 ページ）

コンプライアンス監査の有効化および無効化

コンプライアンス機能は、デバイス設定ベースラインと監査ポリシーを使用して、ネットワーク デバイスの設定の逸脱を検出して訂正します。一部のコンプライアンス レポートはシステムパフォーマンスに影響する可能性があるため、デフォルトではこれは無効になっています。コンプライアンス機能を有効にするには、次の手順を実行します。

（注） コンプライアンス機能を使用するには、システムが『Cisco Evolved Programmable Network Manager Installation Guide』で指定されているプロフェッショナル サイジング要件を満たす必要があります。

（注） Cisco EPN Manager で、コンプライアンス監査を無効にすると、GUI からのコンプライアンスが無効になり、バックグラウンドでのコンプライアンスデータの収集が停止します。コンプライアンス設定を機能させるには、ユーザーが Cisco EPN Manager サーバーを再起動してデバイスを再同期する必要があります。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[一般（General）]** > **[サーバー（Server）]** を選択します。

ステップ 2 [コンプライアンス サービス（Compliance Services）] の横の [有効化（Enable）] をクリックし、次に [保存（Save）] をクリックします。

ステップ 3 アプリケーションを再起動します。

ステップ 4 デバイス インベントリを再同期します。手順としては、[インベントリ（Inventory）] > [ネットワークデバイス（Network Devices）] の順に選択し、すべてのデバイスを選択した後、[同期（Sync）] をクリックします。

（注） バージョン 3.0 にアップグレードする前に Cisco EPN Manager でコンプライアンスが有効になっていた場合、アップグレード後は [システム設定（System Settings）] でコンプライアンスが無効になります。ユーザーは、この項で説明する手順に従って手動でコンプライアンスを有効にする必要があります。この場合は、Cisco EPN Manager サーバーの再起動とデバイスの再同期は必要ありません。

新しいコンプライアンス ポリシーの作成

空のポリシー テンプレートから新しいコンプライアンス ポリシーを作成できます。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択します。

ステップ 2 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域にある [コンプライアンス ポリシーの作成（Create Compliance Policy）]（+）アイコンをクリックします。

ステップ 3 ダイアログボックスに名前と任意の説明を入力し、[作成（Create）] をクリックします。ポリシーが左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域に追加されます。

ポリシーを複製するには、ポリシーオプションボタンを選択し、[複製（Duplicate）] をクリックします。

コンプライアンス ポリシー ルールの作成

コンプライアンス ポリシー ルールはプラットフォーム固有であり、デバイスの違反と見なされるものを定義します。また、違反を修正する CLI コマンドをルールに含めることもできます。コンプライアンス監査ジョブを設定する際に監査に含めるルールを選択できます（コンプライアンス監査の実行 （202 ページ）を参照）。

Cisco EPN Manger は、AireOS ワイヤレス LAN コントローラ プラットフォームの監査をサポートします。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択して、左側のナビゲーション領域からポリシーを選択します。

ステップ 2 作業領域ペインから [新規（New）] をクリックし、新しいルールを追加します。

類似するルールがある場合は、[複製（Duplicate）] をクリックし、ルールを編集して新しい名前で保存することができます。

ステップ 3 ルールの基準を入力して新しいルールを設定します。

（注） Cisco EPN Manager は、すべての Java ベースの正規表現をサポートしています。http://www.rexegg.com/regex-quickstart.htmlを参照してください。

a) タイトル、説明、およびその他の情報を [ルール情報（Rule Information）] テキスト フィールドに入力します。この情報は、フリー テキストであり、ルールの設定には影響しません。

b) このルールの対象デバイスを [プラットフォームの選択（Platform Selection）] 領域に指定します。

c) （任意）[ルールの入力（Rule Inputs）] 領域で、[新規（New）] をクリックし、このルールを含んでいるポリシーの実行時にユーザーに表示する入力フィールドを指定します。たとえば、IP アドレスの入力を求めるプロンプトを表示できます。

（注） [複数の値の承認（Accept Multiple Values）] チェックボックスをオンにした場合は、すべてのルール入力が条件に一致している場合にのみ監査に合格します。

d) [条件とアクション（Conditions and Actions）] 領域で、[新規（New）] をクリックし、確認する基準を指定します。これにより、ルールの合否の条件が決定します。例：ルールの条件とアクション （194 ページ）の例を参考にしてください。

ステップ 4 [作成（Create）] をクリックします。ルールがコンプライアンス ポリシーに追加されます。

必要な数だけルールを作成できます。監査ジョブを実行する場合は、検証するルールを選択できることを覚えておいてください。

（注） 新しいコンプライアンス ポリシー ルールを作成したとき、正規表現を使用してルールまたはコマンドを検証するには、Java 正規表現を使用して式をテストすることをお勧めします。

次のタスク

コンプライアンス ポリシーとそのルールを含むプロファイルを作成し、そのプロファイルを使用して監査を実行します。ポリシーとルールが含まれているコンプライアンス プロファイルの作成 （200 ページ） を参照してください。

例：ルールの条件とアクション

条件およびアクションの例：デバイスに設定された DNS サーバー

このコンプライアンス ポリシーは、**IP name-server 1.2.3.4** または **IP name-server2.3.4.5** がデバイスに設定されているかどうかを確認します。設定されている場合、ポリシーは「DNSサー

バーを1.2.3.4または2.3.4.5として設定する必要があります（DNS server must be configured as either 1.2.3.4 or 2.3.4.5）」というメッセージで違反を発生させます。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	ip name-server {1.2.3.4|2.3.4.5}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	違反は発生しません
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させる
		違反メッセージタイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	DNS サーバーを 1.2.3.4 または 2.3.4.5 として設定する必要があります

例：ブロック オプション

このコンプライアンス ポリシーでは、ある特定のブロック内に定義されている不正または未承認の SNMP コミュニティ文字列があるかどうかを確認します。ブロック内で検出された場合、ポリシーは「承認されていないコミュニティ文字列<1.1>を検出しました（Detected unauthorized community string <1.1>）」というメッセージで違反を報告し、すべての非準拠 SNMP 文字列をブロックから削除します。

タブ	タブ領域	フィールド	値
ルール情報（Rule Information）		ルール タイトル（Rule Title）	snmp-server community having non-standard entries
プラットフォームの選択（Platform Selection）			Cisco IOS デバイス、Cisco IOS-XE デバイス
Condition 1			

[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	snmp-server community (.*)
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させません（Does Not Raise a Violation）
Condition 2			

[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	以前に一致したブロック（Previously Matched Blocks）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	snmp-server community ((public RO)|(private RW))
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させます。
		違反メッセージ タイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	承認されていないコミュニティ文字列 <1.1> を検出しました。（Detected unauthorized community string <1.1>.）

（注） 上記の例では、最初の条件での一致基準は 1.1、1.2 などと呼びます。2 番目の条件での一致基準は 2.1、2.2 などと呼びます。

条件およびアクションの例：コミュニティ文字列

このコンプライアンス ポリシーは、**snmp-server community public** または **snmp-server community private** が（望ましくない）デバイスに設定されているかを確認します。設定されている場合、ポリシーは「コミュニティストリングxxxxxが設定されています（Community string *xxxxx* configured）」というメッセージで違反を発生させます。ここで、*xxx* は最初に見つかった違反です。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	snmp-server community {public|private}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	違反を発生させる
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	続行（Continue）
		違反メッセージ タイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	コミュニティ ストリング *xxxxx* が設定されています。

条件およびアクションの例：IOS ソフトウェア バージョン

このコンプライアンス ポリシーは、Cisco IOS ソフトウェアのバージョン **15.0(2)SE7** がデバイスにインストールされているかどうかを確認します。インストールされていない場合、ポリシーは「show versionの出力に文字列xxxxxが含まれています（Output of show version contains the string *xxxxx*）」というメッセージで違反を発生させます。ここで *xxxx* は 15.0(2)SE7 と一致しない Cisco IOS ソフトウェア バージョンです。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	デバイス コマンド出力
		show コマンド（Show Commands）	show version
	条件一致基準（Condition Match Criteria）	演算子	文字列を含む
		値	15.0(2)SE7

アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させます。
		違反メッセージ タイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	show version の出力に文字列 *xxxxx* が含まれています。

条件およびアクションの例：NTP サーバーの冗長性

このコンプライアンス ポリシーは、デバイスでコマンド **ntp server** が少なくとも 2 回表示されるかどうかを確認します。表示されない場合、ポリシーは、「少なくとも2つのNTPサーバーを構成する必要があります（At least two NTP servers must be configured）」というメッセージで違反を発生させます。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	条件一致基準（Condition Match Criteria）	演算子	式と一致させます。
		値	(ntp server.*\n){2,}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させる
		違反メッセージ タイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	NTP サーバーを 2 つ以上設定する必要があります。

ポリシーとルールが含まれているコンプライアンス プロファイルの作成

コンプライアンス プロファイルには、1 つ以上のコンプライアンス ポリシーが含まれています。コンプライアンスポリシーをプロファイルに追加すると、すべてのポリシールールがプロファイルに適用されます。含めるポリシールールを選択すること（および、その他を無視すること）で、プロファイルをカスタマイズできます。複数のポリシーをプロファイルにグループ化すると、ルールをポリシーごとに選択したり、選択を解除することができます。

ルートユーザー、管理者ユーザー、またはスーパーユーザーとしてログインする場合は、次の操作を行えます。

- プロファイルの作成、編集、削除。
- [ポリシー（Policies）] ページで作成したルールの選択。

（注） 「その他」のユーザーが関連アクションを実行するには、次のタスク権限を有効にする必要があります。

- [コンプライアンス監査プロファイルアクセス（Compliance Audit Profile Access）] : プロファイルを実行および更新し、プロファイル内のポリシーを参照する。
- [コンプライアンス監査プロファイル編集アクセス（Compliance Audit Profile Edit Access）] : コンプライアンス監査プロファイルを作成および編集する。

タスク権限は、**[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** > **[ユーザーグループ（User Groups）]** ページで確認できます。

[コンプライアンス監査プロファイルへのアクセス（Compliance Audit Profile Access）] タスク権限を選択していないと、[コンプライアンス監査プロファイルの編集アクセス（Compliance Audit Profile Edit Access）] タスク権限を選択していても、[プロファイル（Profile）] ページを表示できません。

ステップ 1 **[設定（Configuration）]** > **[コンプライアンス（Compliance）]** > **[プロファイル（Profiles）]** を選択します。

ステップ 2 [コンプライアンス プロファイル（Compliance Profiles）] ナビゲーション領域にある [ポリシー プロファイルの作成（Create Policy Profile）]（+）アイコンをクリックします。この操作によって [コンプライアンス ポリシーの追加（Add Compliance Policies）] ダイアログボックスが開きます。

ステップ 3 プロファイルに含めるポリシーを選択します。ユーザー定義のポリシーが、[ユーザー定義（User Defined）] カテゴリで使用できるようになります。

a) [コンプライアンス ポリシーの追加（Add Compliance Policies）] ダイアログ ボックスで、追加するポリシーを選択します。

b) [OK] をクリックします。ポリシーが [コンプライアンス ポリシー セレクタ（Compliance Policy Selector）] 領域に追加されます。

ステップ 4 ポリシーに含めるルールを選択します。

a) [コンプライアンス ポリシー セレクタ（Compliance Policy Selector）] 領域でポリシーを選択します。ポリシーのルールは、右側の領域に表示されます。

b) 特定のルールを選択するか、または選択を解除して、[保存（Save）] をクリックします。

（注） ここで選択したルールのみが、このプロファイルのポリシー インスタンスに適用されます。この選択によって、コンプライアンス ポリシーの元のバージョンが変更されることはありません。

次のタスク

コンプライアンス監査の実行（202 ページ）の説明に従って、コンプライアンス監査ジョブをスケジュールします。

コンプライアンス監査プロファイルのインポートおよびエクスポート

コンプライアンス プロファイルは XML ファイルとして保存されます。個々のコンプライアンス プロファイルをインポートおよびエクスポートできます。ファイルは、XML 形式でのみインポートできます。

コンプライアンス監査プロファイルのインポート

コンプライアンス監査プロファイルをインポートする前に、プロファイルに関連付けられているすべてのユーザー定義ポリシーが Cisco EPN Manager で使用可能であることを確認します。コンプライアンス プロファイルをインポートするには、次の手順を実行します。

1. **[設定（Configuration）]** > **[コンプライアンス（Compliance）]** > **[プロファイル（Profiles）]** に移動します。
2. 左側の **[コンプライアンス プロファイル（Compliance Profiles）]** 領域にある [プロファイルのインポート（Import Profiles）] アイコンをクリックします。
3. **[プロファイルのインポート（Import Profiles）]** ダイアログボックスで、**[プロファイルの選択（Choose Profiles）]** をクリックします。
4. プロファイル XML ファイルを参照して選択します。
5. （オプション）複数のプロファイルをインポートするには、**[追加ファイルの選択（Choose more files）]** をクリックし、プロファイル XML ファイルをアップロードします。
6. [Import] をクリックします。

Cisco EPN Managerは、無効なプロファイルXMLファイルがアップロードされた場合にエラーメッセージを表示します。インポートに失敗したプロファイルのログを確認するには、**[プロファイルのインポート（Import Profiles）]**ダイアログの警告アイコンをクリックします。

コンプライアンス監査プロファイルのエクスポート

コンプライアンス プロファイルをエクスポートするには、次の手順を実行します。

1. 左側の**[コンプライアンスプロファイル（Compliance Profiles）]**ナビゲーション領域のプロファイルの横にある [i] アイコンの上にマウスを合わせます。
2. **[ポリシープロファイル（Policy Profile）]**ポップアップウィンドウで、**[XMLとしてプロファイルをエクスポート（Export Profile as XML）]**ハイパーリンクをクリックし、ファイルを保存します。

コンプライアンス監査の実行

コンプライアンス監査を実行するには、プロファイルを選択し、監査するデバイスを選択し（プロファイル内のポリシーとルールを使用）、監査ジョブのスケジュールを設定します。

ステップ 1 **[設定（Configuration）]**>**[コンプライアンス（Compliance）]**>**[プロファイル（Profiles）]**を選択します。

ステップ 2 左側の[コンプライアンスプロファイル（Compliance Profiles）]ナビゲーション領域でプロファイルを選択します。

ステップ 3 [コンプライアンス プロファイル（Compliance Profiles）] ナビゲーション領域で [コンプライアンス監査の実行（Run Compliance Audit）] アイコンをクリックします。

ステップ 4 [デバイスおよび設定（Devices and Configuration）] 領域で、目的のデバイスと監査するコンフィギュレーション ファイルを選択します。

a) デバイス（またはデバイス グループ）を選択します。

b) 監査するコンフィギュレーション ファイルを指定します。

- [最新のアーカイブ済みの設定を使用（Use Latest Archived Configuration）]：アーカイブから最新のバックアップ ファイルを監査します。使用可能なバックアップ ファイルがない場合、Cisco EPN Managerはデバイスの監査を実行しません。
- [現在のデバイス設定を使用（Use Current Device Configuration）]：デバイスの実行コンフィギュレーションをポーリングし、監査します（たとえば、showコマンド出力はデバイスの実行コンフィギュレーションから生成されます）。

  このオプションを選択すると、Cisco EPN Managerは最初にデバイスからコンフィギュレーションのバックアップを取得してから監査を実行します。これは、定期的またはイベントがトリガーしたコンフィギュレーションバックアップが有効になっていない場合に役に立ち、また、Cisco EPN Managerにアーカイブ済みのコンフィギュレーションがデバイスとの同期が取れていないことが頻繁にあるため、便利です。

c) [次へ（Next）] をクリックします。

ステップ 5 [アイドル時間制限の設定（分）（Configure Idle Time Limit (min)）] フィールドに値を入力します。デフォルトでは、制限時間は 5 分に設定されます。ユーザーが制限時間を変更する場合は、5 ～ 30 の数字を入力できます。設定された制限時間の間アイドル状態が続くと、監査ジョブは中止されます。

ステップ 6 すぐに監査ジョブをスケジュール設定する場合は [今すぐ（Now）] を選択し、後でスケジュール設定する場合は [日付（Date）] を選択して日時を入力します。

監査ジョブを定期的に繰り返すには、[定期（Recurrence）] オプションを使用します。

ステップ 7 [終了（Finish）] をクリックします。監査ジョブがスケジュール設定されます。監査ジョブがスケジュールされると、通知ポップアップが表示されます。監査ジョブのステータスを表示するには、[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

次のタスク

コンプライアンス監査の結果の表示（203 ページ）の説明に従って、監査結果を確認します。

コンプライアンス監査の結果の表示

この手順を使用して、監査ジョブの結果を確認します。結果から、監査したデバイス、スキップしたデバイス、違反があったデバイスなどがわかります。単一のデバイスでさまざまなコンプライアンス ポリシーが実行されている場合があります。

ジョブを作成したら、そのジョブに関して次の設定を行えます。

- [シリーズを一時停止（Pause Series）]：後日に実行するようにスケジュール設定されているジョブのみに適用できます。実行中のジョブを一時停止することはできません。
- [シリーズを再開（Resume Series）]：一時停止されているジョブのみに適用できます。
- [スケジュールを編集（Edit Schedule）]：スケジュール済みのジョブを別の時間に再度スケジュール設定します。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

ステップ 2 [監査ジョブ（Audit Jobs）] タブをクリックしてジョブを見つけ、[前回の実行（Last Run）] 列の情報を確認します。

最後の実行結果の値	説明
[失敗（Failure）]	監査した 1 つ以上のデバイスが、プロファイルで指定されたポリシーに違反しています。
[一部成功（Partial Success）]	コンプライアンス ジョブに、監査済みおよび監査なしのデバイスが両方含まれ、監査済みデバイスのコンプライアンス ステータスは成功です。

[成功 (Success)]	監査したすべてのデバイスは、プロファイルで指定されたポリシーに準拠しています。

コンプライアンス監査ジョブの場合、サポートされる違反の数は Cisco EPN Manager の標準設定で 20,000 件、Pro 以上の設定では 80,000 件です。

ステップ 3 監査の確認が失敗した場合は、次の手順を実行します。

- 失敗したデバイスを確認するには、[失敗（Failure）] ハイパーリンクの横にある [i] アイコンにカーソルを合わせて詳細のポップアップを表示します。
- ジョブを選択し、[ジョブの詳細を表示（View Job Details）] をクリックし、ポップアップのデバイスの横にある [i] アイコンをクリックして [デバイス 360（Device 360）] ビューを起動します。

ステップ 4 最も詳細な情報を確認するには、[失敗（Failure）] ハイパーリンクをクリックして [コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを開きます。

（注） [コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを行き来するには、[次へ（Next）] および [前へ（Previous）] ボタンを使用します。

次のタスク

違反を修正するには、デバイスのコンプライアンス違反の修正（206ページ）を参照してください。

違反ジョブの詳細の表示

次の表に、[違反の詳細（Violation Details）] ページから表示できる詳細を示します。

表示内容	選択方法
スケジュール済み修正可能違反ジョブのステータス。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[実行中（Running）] を選択します。
修正済み違反ジョブの詳細。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[修正済み（Fixed）] を選択します。 **3.** [修正済み（Fixed）] リンクをクリックします。

修正失敗違反ジョブの詳細。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[修正失敗（Fix Failed）] を選択します。 **3.** [修正失敗（Fix Failed）] リンクをクリックします。

監査の失敗および違反のサマリー詳細の表示

詳細な違反情報を表示し、このデータをエクスポートし、コンプライアンス ジョブの詳細を表示できます。特定のジョブの詳細データをエクスポートしたり、複数のジョブのサマリーデータをエクスポートすることができます。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

ステップ 2 特定の監査ジョブの詳細を表示するには、次の手順を実行します。

a) [監査ジョブ（Audit Jobs）] タブをクリックして、ジョブを見つけます。

b) [失敗（Failure）] ハイパーリンクをクリックし、[コンプライアンス監査の詳細（Compliance Audit Details）] ウィンドウを表示します。

ポリシー名、設定したルール、そのコンプライアンス状態、合計違反数、ジョブのインスタンス カウント、その中で最も重大度の高い値、および無視したカウント値に関する情報を表示できます。

c) これらの詳細をエクスポートするには、次のいずれかのオプションを使用します。

- 違反の詳細は Microsoft Excel スプレッドシートに XLS でエクスポートするには、[XLS としてエクスポート（Export as XLS）] をクリックします。
- 違反の詳細を Microsoft Excel スプレッドシートにカンマ区切りのテキストでエクスポートするには、[CSV としてエクスポート（Export as CSV）] をクリックします。
- 違反の詳細を HTML ファイルにエクスポートするには、[HTML としてエクスポート（Export as HTML）] をクリックします。

d) [ファイルの保存（Save File）] をクリックします。

ステップ 3 すべての監査ジョブの総合的なサマリーを表示するには、次の手順を実行します。

a) [違反サマリー（Violation Summary）] タブをクリックします。

違反が発生したすべてのデバイス、その関連のポリシーとプロファイル名、監査ジョブ ID、関連ルールとルールの重大度値、違反の修正が可能かどうかの詳細、またはすでに修正されているかどうか、違反に関連付けられたメッセージについて総合的なレポートを表示できます。

b) この詳細なサマリー レポートをエクスポートするには、ドロップダウン メニューから次のいずれかのオプションを選択します。

- サマリーを Microsoft Excel spreadsheet にカンマ区切りのテキストでエクスポートするには、[違反レポート CSV（Violation Report CSV）] をクリックします。
- サマリーを PDF ファイルをエクスポートするには、[違反レポート PDF（Violation Report PDF）] をクリックします。

c) [ファイルの保存（Save File）] をクリックします。

次のタスク

違反を修正するには、デバイスのコンプライアンス違反の修正（206 ページ）を参照してください。

デバイスのコンプライアンス違反の修正

この手順を使用して、失敗したコンプライアンス監査のコンプライアンス違反を修正します。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

ステップ 2 [監査ジョブ（Audit Jobs）] をクリックしてジョブを見つけ、[前回の実行結果（Last Run Result）] 列の情報を確認します。

ステップ 3 [失敗（Failure）] ハイパーリンクをクリックし、[コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを開きます。

（注） [コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを行き来するには、[次へ（Next）] および [前へ（Previous）] ボタンを使用します。

ステップ 4 [ジョブの詳細と違反（Job Details and Violations）] 領域で [次へ（Next）] をクリックします。

ステップ 5 [デバイス別の違反（Violations by Device）] 領域でデバイスと違反を選択し、[次へ（Next）] をクリックします。

ステップ 6 [修正ルールの入力（Fix Rule Inputs）] 領域で、以前にポリシーで定義した修正コマンドをプレビューし、[次へ（Next）] をクリックします。

条件に対するアクションとして修正 CLI の ^<Rule input ID>^ を使用してカスタム ポリシーを作成した場合は、[修正ルールの入力（Fix Rule Inputs）] タブが表示されます。必須の修正ルールの値を入力して [次へ（Next）] をクリックします。

ステップ 7 [修正コマンドのプレビュー（Preview Fix Commands）] ポップアップに表示された設定を確認します。

ステップ 8 生成された設定がデバイスに展開できるように修正ジョブのスケジュールを設定し、[修正ジョブのスケジュール設定（Schedule the Fix Job）] をクリックします。

（注） ユーザーは、デバイスのスタートアップ コンフィギュレーションにコンプライアンス修正 CLI を追加できます。これにより、デバイスの再起動時にも修正 CLI が保持されます。

次のタスク

違反ジョブの詳細を表示するには、監査の失敗および違反のサマリー詳細の表示 （205 ページ）を参照してください。

監査の失敗および違反のサマリー詳細の表示

詳細な違反情報を表示し、このデータをエクスポートし、コンプライアンス ジョブの詳細を表示できます。特定のジョブの詳細データをエクスポートしたり、複数のジョブのサマリーデータをエクスポートすることができます。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザージョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）] を選択します。

ステップ 2 特定の監査ジョブの詳細を表示するには、次の手順を実行します。

a) [監査ジョブ（Audit Jobs）] タブをクリックして、ジョブを見つけます。

b) [失敗（Failure）] ハイパーリンクをクリックし、[コンプライアンス監査の詳細（Compliance Audit Details）] ウィンドウを表示します。

ポリシー名、設定したルール、そのコンプライアンス状態、合計違反数、ジョブのインスタンス カウント、その中で最も重大度の高い値、および無視したカウント値に関する情報を表示できます。

c) これらの詳細をエクスポートするには、次のいずれかのオプションを使用します。

- 違反の詳細は Microsoft Excel スプレッドシートに XLS でエクスポートするには、[XLS としてエクスポート（Export as XLS）] をクリックします。
- 違反の詳細を Microsoft Excel スプレッドシートにカンマ区切りのテキストでエクスポートするには、[CSV としてエクスポート（Export as CSV）] をクリックします。
- 違反の詳細を HTML ファイルにエクスポートするには、[HTML としてエクスポート（Export as HTML）] をクリックします。

d) [ファイルの保存（Save File）] をクリックします。

ステップ 3 すべての監査ジョブの総合的なサマリーを表示するには、次の手順を実行します。

a) [違反サマリー（Violation Summary）] タブをクリックします。

違反が発生したすべてのデバイス、その関連のポリシーとプロファイル名、監査ジョブ ID、関連ルールとルールの重大度値、違反の修正が可能かどうかの詳細、またはすでに修正されているかどうか、違反に関連付けられたメッセージについて総合的なレポートを表示できます。

b) この詳細なサマリー レポートをエクスポートするには、ドロップダウン メニューから次のいずれかのオプションを選択します。

- サマリーを Microsoft Excel spreadsheet にカンマ区切りのテキストでエクスポートするには、[違反レポート CSV（Violation Report CSV）] をクリックします。
- サマリーを PDF ファイルをエクスポートするには、[違反レポート PDF（Violation Report PDF）] をクリックします。

c) [ファイルの保存（Save File）] をクリックします。

次のタスク

違反を修正するには、デバイスのコンプライアンス違反の修正（206ページ）を参照してください。

コンプライアンス ポリシーのインポートおよびエクスポート

コンプライアンス ポリシーはXMLファイルとして保存されます。個別のコンプライアンス ポリシーをエクスポートし、必要に応じて、それらのポリシーを別のサーバーにインポートすることができます。ファイルは、XML 形式でのみインポートできます。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択します。

ステップ 2 コンプライアンス ポリシーをエクスポートするには、次の手順を実行します。

a) 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域のポリシーの横にある [i] アイコンの上にマウスを合わせます。

b) ポップアップ ウィンドウで、[XML としてポリシーをエクスポート（Export Policy as XML）] ハイパーリンクをクリックし、ファイルを保存します。

ステップ 3 コンプライアンス ポリシーをインポートするには、次の手順を実行します。

a) 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域の上にある [ポリシーのインポート（Import Policies）] アイコンをクリックします。

b) [ポリシーのインポート（Import Policies）] ダイアログボックスで、[ポリシーの選択（Choose Policies）] をクリックします。

c) XML ファイルを参照して選択します。

d) [インポート（Import）] をクリックします。

コンプライアンスポリシーXMLファイルのコンテンツの表示

コンプライアンス ポリシーは XML ファイルとして保存されます。ポリシーの XML ファイルの内容を表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択します。

ステップ 2 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域でポリシーを見つけ、そのポリシーの横にある [i] アイコンの上にマウスを合わせます。

ステップ 3 ポップアップ ウィンドウで、[XML としてポリシーを表示（View Policy as XML）] ハイパーリンクをクリックします。Cisco EPN Manager は内容を XML 形式で表示します。

PSIRT および EOX 情報の表示

（注） [PSIRT と EOX（PSIRT and EOX）] ページには、PAS および RBML バンドルの生成日が表示されます。PAS レポートには、バンドルの生成日以前に公開された PSIRT および EoX レコードが保持されます。バンドルの生成後に公開された PSIRT レコードは表示されません。

デバイスのセキュリティ脆弱性の表示

レポートを実行して、Cisco Product Security Incident Response Team（PSIRT）によって定義されているセキュリティの脆弱性が、ネットワーク内のデバイスにあるかどうかを判断できます。レポートには、[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報が含まれます。また、特定の脆弱性に関するマニュアルを参照できます。このマニュアルでは、脆弱性の影響と環境を保護するために必要と考えられる手順が説明されています。

（注） PSIRT および EOX レポートを特定のデバイスに対して実行することはできません。PSIRT および EOX ジョブのスケジュールを設定すると、管理対象で完了状態にあるすべてのデバイスに対してレポートが生成されます（[インベントリ（Inventory）]>[設定（Configuration）]>[ネットワークデバイス（Network Devices）] ページ）。

始める前に

ジョブのスケジュールを設定する前にデバイスを同期します。**[設定（Configuration）]**>**[ネットワーク デバイス（Network Devices）]** を選択し、デバイスを選択して [同期（Sync）] をクリックします。

ステップ 1 **[レポート（Reports）]** > **[PSIRT と EOX（PSIRT and EoX）]** を選択します。

ステップ 2 ジョブのスケジュールを設定して実行します。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。作成する必要のないジョブはそれぞれのタブで区別します。

ステップ 3 PSIRT レポートの現在のステータスを表示するには、[ジョブの詳細を表示（View Job Details）] をクリックします。

ステップ 4 レポートが完了したら、[デバイス PSIRT（Device PSIRT）] タブをクリックして PSIRT 情報を表示します。

ステップ 5 [PSIRT タイトル（PSIRT Title）] 列のハイパーリンクをクリックすると、セキュリティの脆弱性の詳しい説明が表示されます。

ステップ 6 （任意）デバイスの PSIRT の詳細はデバイスごと、またはすべてのデバイスをまとめて PDF 形式および CSV 形式でエクスポートできます。

デバイスのハードウェアとソフトウェアのサポート終了レポートの表示

レポートを実行して、ネットワーク内のシスコ デバイス ハードウェアまたはソフトウェアがサポート終了（EOX）に到達しているかどうかを判断できます。これは、製品のアップグレードや代替オプションを決定する際に役立ちます。

ステップ 1 [レポート（Reports）] > [PSIRTとEOX（PSIRT and EOX）] を選択します。

ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 ジョブの完了後に、次のEOXタブのいずれかをクリックすると、そのタブ固有のレポート情報が表示されます。

- **デバイス ハードウェア EOX（Device Hardware EOX）**
- **デバイス ソフトウェア EOX（Device Software EOX）**
- **モジュールハードウェア EOX（Module Hardware EOX）**

ステップ 4 （任意）これらの EOX の詳細は、デバイスごとまたはすべてのデバイスをまとめて PDF 形式および CSV 形式でエクスポートできます。

モジュール ハードウェアのサポート終了レポートの表示

レポートを実行して、ネットワーク内のシスコモジュールハードウェアがサポート終了（EOX）に到達しているかどうかを判断できます。これは、製品のアップグレードや代替オプションを決定する際に役立ちます。

ステップ 1 [レポート（Reports）] > [PSIRTとEOX（PSIRT and EOX）] を選択します。

ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 [モジュールハードウェアEOX（Module Hardware EOX）] タブをクリックして、モジュール ハードウェアの情報を表示します。

ステップ 4 （任意）これらの EOX の詳細は、モジュールごとに PDF 形式および CSV 形式でエクスポートできます。

デバイスのフィールド通知の表示

レポートを実行して、完全なインベントリ収集が完了している管理対象シスコデバイスにField Noticeがあるかどうかを判断できます。Field Noticeとは、セキュリティ脆弱性の問題以外でシ

スコ製品に直接関係する重要な問題に関する通知です。通常、アップグレード、回避策、またはその他の対策が必要となります。

ステップ 1 [レポート（Reports）] > [PSIRTとEOX（PSIRT and EOX）] を選択します。

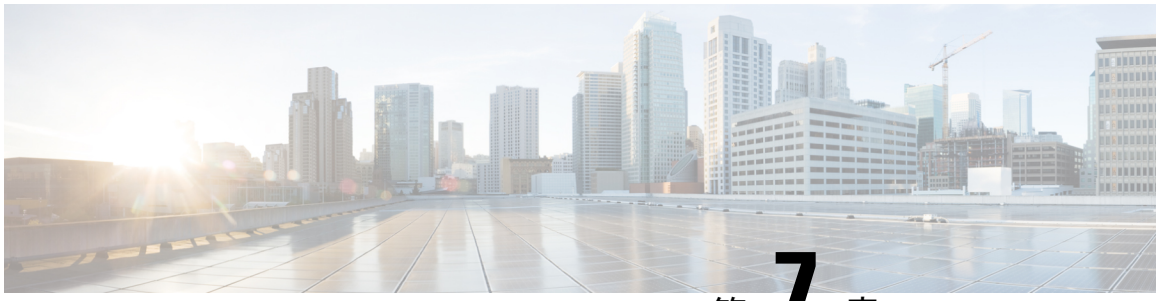
ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 [フィールド通知（Field Notice）] タブをクリックすると、フィールド通知の情報が表示されます。

ステップ 4 [脆弱（Vulnerable）] 列の [i] アイコンをクリックして、[フィールド通知URL（Field Notice URL）] および [警告の詳細（Caveat Details）] ダイアログボックスを開きます。cisco.com で詳細を確認するには、[フィールド通知URL（Field Notice URL）] をクリックします。

ステップ 5 （任意）デバイスのフィールド通知の詳細はデバイスごと、またはすべてのデバイスをまとめてPDF形式およびCSV形式でエクスポートできます。



第 7 章

ユーザー定義のインベントリ検出ジョブ

ユーザー定義のインベントリ検出ジョブ

インベントリの切り替えジョブは、ネットワーク上のデバイスの物理インベントリと論理インベントリの情報を収集するために毎日実行されるシステムジョブです。デフォルトでは、このジョブはネットワーク上のすべてのデバイスに対して実行されます。選択したデバイスセットまたはデバイスグループのインベントリのみを収集するようにこのジョブをカスタマイズすることはできません。また、このジョブの長時間実行中のインスタンスを簡単に中止することはできません。

ユーザー定義のインベントリ検出ジョブを作成できます。この場合、次を実行することができます。

- 選択したデバイスセットまたはデバイスグループのインベントリのみを収集する。
- 繰り返しをカスタマイズする。
- ジョブを実行する回数を選択する。
- 予想よりも長い時間実行されているジョブを自動的に中止する。
- 以前に中止されたジョブの実行からスキップされたデバイスでのインベントリ収集の優先順位を選択する。

デフォルトのインベントリの切り替えジョブまたはユーザー定義のインベントリ検出ジョブを実行できます。ユーザー定義のインベントリ検出ジョブを実行する前に、デフォルトのインベントリの切り替えジョブを無効にする必要があります。手順は次のとおりです。

1. **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）]** に移動します。
2. [インベントリ（Inventory）] で、[インベントリ切り替えジョブの無効化（Disable Switch Inventory Job）] チェックボックスをオンにして、[保存（Save）] をクリックします。この設定を有効にすると、デフォルトのインベントリ切り替えジョブが無効になり、ユーザー定義のインベントリ検出ジョブが有効になります。

デフォルトのインベントリ切り替えジョブに戻すには、[インベントリ切り替えジョブの無効化（Disable Switch Inventory Job）] チェックボックスをオフにします。これにより、スケジュールされたユーザー定義のインベントリ検出ジョブが無効になり、一時停止されます。

（注） インベントリ検出ジョブとインベントリ切り替えジョブを切り替えると（たとえば、インベントリ検出ジョブからインベントリ切り替えジョブに）、切り替えたジョブは有効になりますが、自動的には実行されません。ジョブダッシュボード（**[管理（Administration）]**>**[ダッシュボード（Dashboards）]**> **[ジョブ（Jobs）]** ダッシュボード）からジョブを選択し、[シリーズの再開（Resume）] をクリックして、ジョブの実行を手動で再開する必要があります。

ユーザー定義のインベントリ検出ジョブの作成

ユーザー定義のインベントリの切り替えジョブを作成するには、次の手順を実行します。

始める前に

デフォルトのインベントリ切り替えジョブを無効にします。**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[インベントリ（Inventory）]** に移動します。[インベントリ（Inventory）] で、[インベントリ切り替えジョブの無効化（Disable Switch Inventory Job）] チェックボックスをオンにして、[保存（Save）] をクリックします。

（注） デフォルトのインベントリの切り替えジョブを無効にしていない場合でも、ユーザー定義のインベントリ検出ジョブを作成できます。これらの新しく作成されたジョブは中断されたままになります。デフォルトのインベントリ切り替えジョブを無効にした後に、これらのジョブが実行できるようになります。

ステップ 1 **[管理（Administration）]**>**[ダッシュボード（Dashboards）]**>**[ジョブダッシュボード（Job Dashboard）]**> **[ユーザージョブ（User Jobs）]** に移動し、[+] をクリックします。

ステップ 2 ジョブ名を指定します。アルファベット、数字、アンダースコア、ハイフン、スペースを使用できます。特殊文字は使用できません。

ステップ 3 [選択（Select）] トグルボタンをクリックして、[デバイス別（By Device）] または [グループ別（By Group）] を選択します。

- [デバイス別（By Device）]：システム内のすべてのデバイスのリストを表示します。選択できるデバイスの数に制限はありません。
- [グループ別（By Group）]：システムおよびユーザー定義のすべてのグループのリストを表示します。一度に選択できるデバイスグループは 1 つのみです。

必要に応じてデバイスまたはデバイスグループを選択し、[次へ（Next）] をクリックします。

ステップ 4 次の設定を行って、ジョブをスケジュールします。

設定のスケジュール

- [開始時刻（Start time）]：開始日時を指定します。
- [繰り返し（Recurrence）]：[毎時（Hourly）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）]、[毎年（Yearly）] のいずれかを選択します。スケジュール可能な最小の繰り返し時間は 6 時間ごとです。これは、デフォルトの繰り返し時間でもあります。
- [終了時刻（End time）]：ジョブの終了時刻を指定するオプションのいずれかを選択します。
  - [終了日時なし（No End Date / Time）]：終了時刻を指定せず、ジョブを無期限に実行する場合。
  - [この回数を実行後（After）]：指定した回数を実行した後にジョブを終了します。このオプションは、[繰り返し（Recurrence）] を [毎時（Hourly）] または [毎日（Daily）] を選択した場合にのみ使用できます。
  - [終了時刻（End at）]：特定の日時にジョブを終了します。

設定の中止

- [長時間実行ジョブを中止する（Abort Long running Job）]：このチェックボックスをオンにして、カットオフ時刻を時間と分で指定します。ここで指定した時間を超えて実行されているジョブは、自動的に中止されます。指定できる最小時間は 2 時間です。
- [次回の実行で最初に中止デバイスを収集する（Collect Abort Devices First in Next Run）]：中止されたデバイスの同期を次回の実行で優先するには、このチェックボックスをオンにします。

ステップ 5 **[終了（Finish）]** をクリックします。

新しく作成されたジョブは、[ジョブ（Jobs）] ダッシュボード（**[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ（Jobs）] ダッシュボード** > **[ユーザージョブ（User jobs）]** > **[インベントリ検出ジョブ（Inventory Discovery Jobs）]**）に表示できます。ジョブをすぐに実行する場合は、ジョブを選択して [実行（Run）] をクリックします。詳細については、ジョブ ダッシュボードを使用したジョブの管理 （32 ページ）を参照してください。

ユーザー定義のインベントリ検出ジョブの編集

ステップ 1 [ジョブ（Jobs）] ダッシュボードからインベントリ検出ジョブを選択します。

ステップ 2 [スケジュール（Schedule）] をクリックして、スケジュール設定を変更します。

（注） スケジュールの編集または設定の中止のみを実行できます。ジョブの作成時に選択したデバイスまたはデバイスグループは変更できません。

ジョブダッシュボードへの結果の表示

[ジョブ（Job）] ダッシュボードで実行したジョブの結果を表示できます。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブダッシュボード（Jobs Dashboard）]** > **[ユーザージョブ（User jobs）]** > **[インベントリ検出ジョブ（Inventory Discovery Jobs）]** に移動します。

ステップ 2 ジョブのハイパーリンクをクリックします。

ジョブの [ジョブ結果（Job Results）] ページに、次の詳細が表示されます。

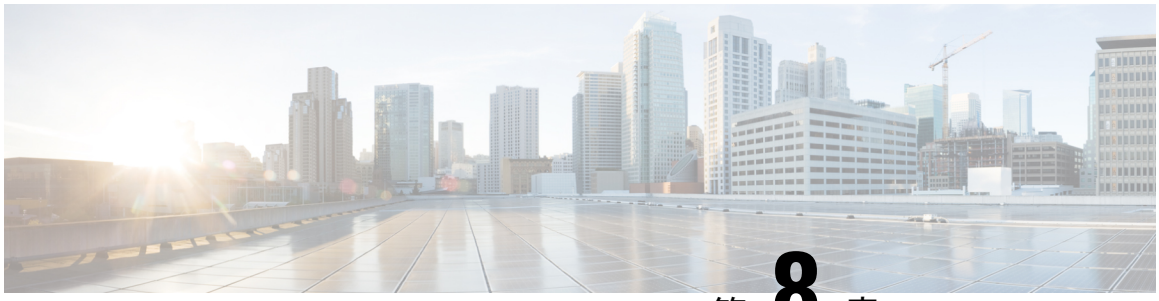
- 個々のデバイスの収集サマリー：デバイス名、IP アドレス、開始時刻、終了時刻、結果
- 次を示すデバイス固有の結果：
  - [成功（Success）]：デバイスのインベントリ収集ステータスが [完了（Completed）] の場合。
  - [失敗（Failed）]：デバイスのインベントリ収集ステータスが [警告（Warning）]、[収集の失敗（Collection Failure）]、またはクレデンシャルの障害で完了した場合。
  - [キャンセル済み（Canceled）]：ジョブが中止された場合。

（注） [管理対象：完了（Managed-Complete）] の状態でないデバイスは、ジョブの実行中にスキップされます。参加しているデバイスのいずれかがすでに同期されている場合は、それらのデバイスはインベントリ検出ジョブの実行中にスキップされ、[キャンセル済み（Cancelled）] としてマークされます。

- 全体的なジョブ収集ステータス：
  - [成功（Success）]：インベントリ収集がすべてのデバイスで成功した場合。
  - [失敗（Failure）]：インベントリ収集がすべてのデバイスで失敗した場合。
  - [一部成功（Partial Success）]：一部のデバイスでインベントリ収集が失敗した場合。
  - [キャンセル済み（Canceled）]：ジョブが中止された場合。

第 III 部

ネットワークの視覚化



第 8 章

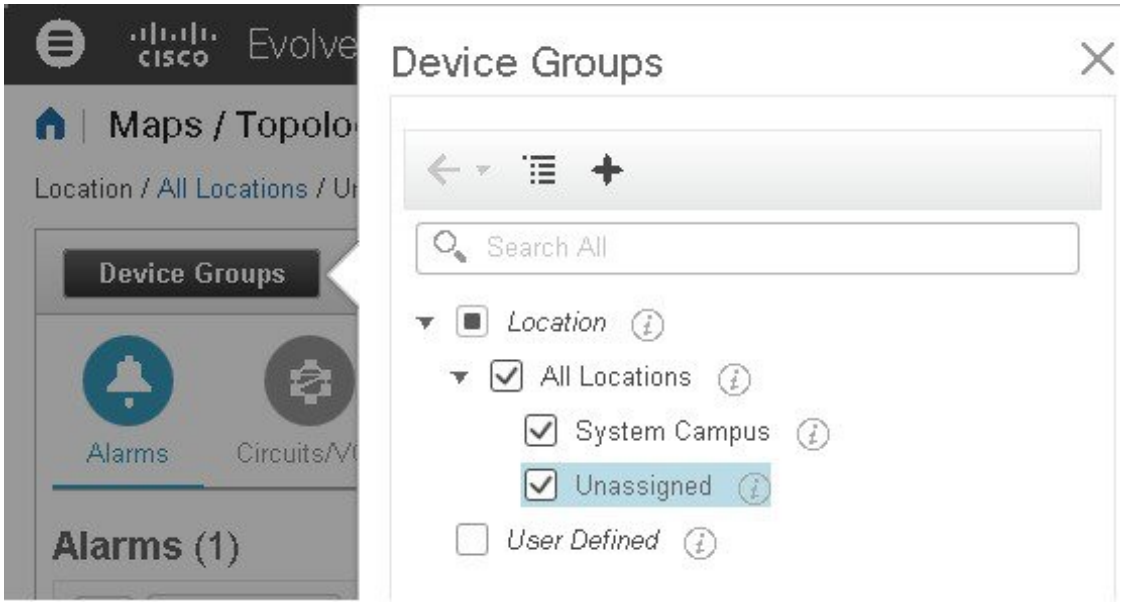
ネットワーク トポロジの視覚化

この章では、次のトピックについて説明します。

ネットワーク トポロジの概要

[ネットワークトポロジ（Network Topology）] ウィンドウには、デバイスのグラフ形式のトポロジ マップ ビュー、それらの間のリンク、およびマップ内の要素のアクティブなアラームが表示されます。また、表示されたトポロジマップ内で回線/VC を可視化することもできます。また、[ネットワークトポロジ（Network Topology）] ウィンドウでは、マップ要素のツールと機能にアクセスでき、ドリルダウンしてマップ要素の詳細情報を取得できます。

[ネットワークトポロジ（Network Topology）] ウィンドウは、左側のサイドバーからアクセスします（**[マップ（Maps）] > [トポロジ（Topology）] > [ネットワークトポロジ（Network Topology）]**）。[ネットワークトポロジ（Network Topology）] ウィンドウの内容は、選択したデバイス グループによって決まります。デバイス グループを選択するには、ツールバーの [デバイスグループ（Device Groups）] ボタンをクリックし、[デバイスグループ（Device Groups）] パネルで 1 つ以上のグループを選択します。[デバイスグループ（Device Groups）] パネルから、中央のデバイス グループ化機能にアクセスして、新しいグループを作成したり、グループにデバイスを追加したりできます。詳細については、簡単な管理と設定のためのデバイス グループの作成 （92 ページ）を参照してください。



各ネットワーク トポロジマップは、アラーム/回線/VC/リンク情報を表示する左ペインと、マップ自体を表示する右ペインに分かれています。左ペインのツールバーを使用して、両方のペインのスペースを制御します。たとえば、100% を選択するとマップのみが表示されます。50% を選択すると、マップと左ペインが画面に均等に表示されます。左ペインが展開されると、タブ内のテーブルに追加の列が追加されることがあります。

- [アラーム（Alarms）]、[回線/VC（Circuits/VCs）]、および [リンク（Links）]（左ペイン）：マップに表示されているデバイスおよびトポロジに関連する情報が提供されます。
  - [アラーム（Alarms）] タブ：選択したグループの現在のアラームとその重大度がリストされたテーブルを表示します。アラームを選択し、クリアや確認などの基本アクションを実行できます。アラームの詳細については、[アラーム（Alarms）] タブの下部にある [アラームテーブル（Alarms Table）] リンクをクリックします。
  - [回線/VC（Circuits/VCs）] タブ：選択したグループ内のデバイスに関連する回線/VC を一覧表示し、各回線/VC のプライマリ状態を示します。プライマリ状態は、プロビジョニング、有用性、ディスカバリ、およびアラーム状態に基づいて回線の現在の最も重大な状態を反映します。回線または VC の状態 （790 ページ）を参照してください。デフォルトで、回線/VC はプライマリ状態別に重大度の高い順に並べ替えられます。次の点に注意してください。

- リストで回線/VC を選択すると、トポロジマップに回線/VC が視覚的に表示されます。
- タブの下部にある [回線/VC（Circuits/VCs）] リンクをクリックすると、個別のウィンドウが起動されてテーブルに各回線/VC の詳細が表示されます。
- タブの下部にある [ネットワークインターフェイス（Network Interfaces）] リンクをクリックすると、UNI や ENNI などの回線/VC への参加が設定されたインターフェイスが一覧表示されます。
- 該当するツールバーアイコンをクリックして、新しい回線の作成や、選択した回線での ITU-T Y.1564 テストなどのアクションを実行できます。

- [リンク（Links）] タブ：選択したデバイス グループに関連するリンクが一覧表示され、リンク上で最も重大度の高いアラームが表示されます。テーブル内のリンクを選択すると、トポロジ マップ内のリンクが強調表示されます。タブの下部にある [リンクテーブル（Links Table）] リンクをクリックすると、別のウィンドウが開き、リンクのテーブルが表示されます。

- [トポロジマップ（Topology map）]（右ペイン）：選択したデバイス グループのトポロジがグラフ形式で表示されます。グループのデバイスとサブグループ（存在する場合）と、それらの間のリンク（物理、イーサネット、およびテクノロジー固有のリンク）が表示されます。さらに、デバイスまたはリンクのアクティブアラームも表示されるため、ネットワークの問題を簡単に特定できます。問題をトラブルシューティングするには、トポロジマップからデバイスやリンクの詳細情報にドリルダウンできます。トポロジマップは、カスタマイズ、フィルタリング、および必要な情報を正確に表示するための操作が可能です。

  マップの右上隅にあるトグル ボタンを使用して、ネットワーク トポロジ マップと地理的マップを切り替えることができます。

  このペインの右上隅にある **[自動更新（Auto-Refresh）]** ドロップダウンリストを使用して、トポロジマップビューのアラーム、回路/VC、およびリンクテーブルを更新する更新時間間隔を選択します。更新間隔は、**[ユーザーごとの設定（Per user preference）]**（詳細については「ユーザー設定の変更」を参照）、**[10秒ごと（Every 10 seconds）]**、**[30秒ごと（Every 30 seconds）]**、または **[自動更新なし（No auto-refresh）]** に設定できます。

（注） [10秒ごと（Every 10 seconds）] を選択すると、意図的にトポロジマップの [アラーム（Alarms）]テーブルに[アクション（Actions）] オプションが表示されなくなります。

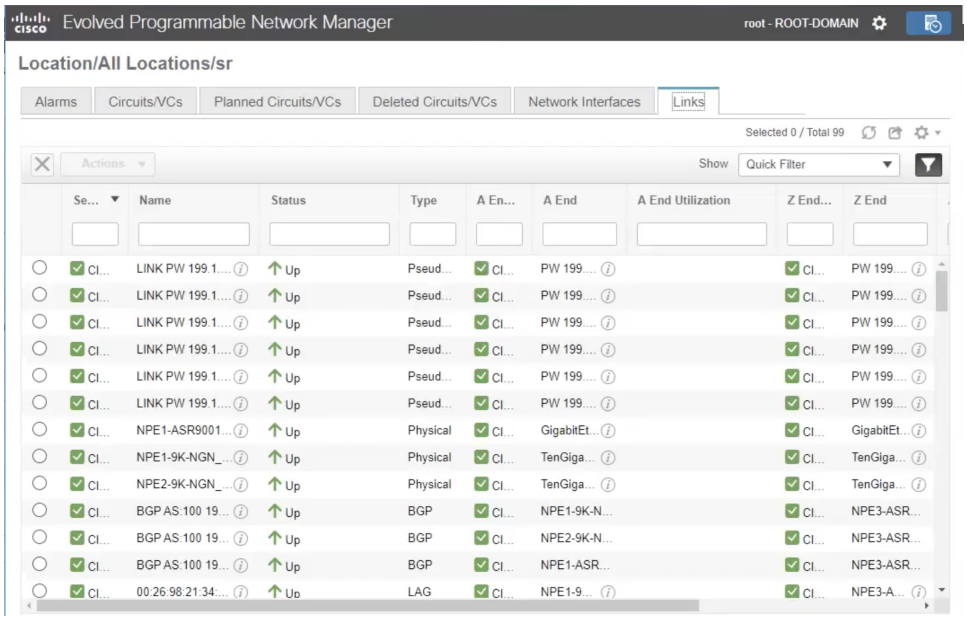
ネットワーク トポロジ マップからのアラーム、ネットワーク インターフェイス、回線/VC、およびリンクの詳細テーブルの表示

[ネットワークトポロジ（Network Topology）] ウィンドウから拡張テーブルにアクセスして、選択したデバイス グループのアラーム、ネットワーク インターフェイス、回線/VC、およびリンクの詳細を一覧表示できます。これらの拡張テーブルは、別個のブラウザ ウィンドウで開きます。

[ネットワークトポロジ（Network Topology）] ウィンドウからアクセスするテーブルには、選択したデバイス グループの情報のみが表示されます。システム内のすべてのアラーム/回線/計画された回線/削除された回線/ネットワーク インターフェイス/リンクの完全なリストにアクセスするには、**[インベントリ（Inventory）]** > **[その他（Other）]** を選択してから目的のテーブル（リンク、ネットワーク インターフェイスなど）を選択します。

拡張詳細テーブルを開くには、タブの右上隅にある [切断（Detach）] アイコンをクリックするか、特定のタブの下部にあるハイパーリンクをクリックします（たとえば、[アラーム（Alarms）] タブの下部にある [アラームテーブル（Alarms Table）] リンクをクリックします）。

拡張テーブルを表示するウィンドウには、[アラーム（Alarms）]、[回線/VC（Circuits/VCs）]、[計画された回線/VC（Planned Circuits/VCs）]、[削除された回線/VC（Deleted Circuits/VCs）]、[ネットワークインターフェイス（Network Interfaces）]、[リンク（Links）] の各タブがあります。



拡張テーブルを使用する場合は、次の点に注意してください。

- 拡張テーブル ウィンドウを開くと、[ネットワークトポロジ（Network Topology）] ウィンドウの左ペインが無効になります。拡張テーブル ウィンドウを閉じると、[ネットワークトポロジ（Network Topology）] ウィンドウの左ペインにあるタブが再び有効になります。
- 拡張テーブルと [ネットワークトポロジ（Network Topology）] ウィンドウ内の対応するタブ間には同期が確立されています。たとえば、回線/VC の拡張テーブルで回線/VC を選択すると、[ネットワークトポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] タブでもその回線が選択され、回線/VC オーバーレイがトポロジマップに表示されます。逆に、[ネットワークトポロジ（Network Topology）] ウィンドウで回線/VC を選択してから拡張テーブルを開くと、同じ回線/VC が拡張テーブルで選択されています。
- ネットワークトポロジビューのすべてのテーブルは、ページの右上隅にある **[自動更新（Auto-Refresh）]** ドロップダウンリストで選択した設定に基づいて更新されます。更新間隔は、**[ユーザーごとの設定（Per user preference）]**（詳細については「ユーザー設定の変更」を参照）、**[10秒ごと（Every 10 seconds）]**、**[30秒ごと（Every 30 seconds）]**、または **[自動更新なし（No auto-refresh）]** に設定できます。デフォルトの更新間隔は、[ユーザーごとの設定（Per user preference）] です。

（注） [10秒ごと（Every 10 seconds）] を選択した場合、意図的にポロジビューのテーブルには [アクション（Actions）] オプションがありません。

- テーブルの右上にある [エクスポート（Export）] アイコンをクリックすると、テーブルのデータがファイルにエクスポートされます。

（注） 回線/VC およびネットワーク インターフェイス テーブルでは、CSV 形式のみがサポートされています。これら 2 つのテーブルのデータは、フィルタまたは UI ページに関係なくエクスポートされます。それ以外のテーブルの場合、[エクスポート（Export）] ではCSV 形式と PDF 形式の両方がサポートされ、適用されたフィルタと現在の UI ページに基づいてデータがエクスポートされます。

- [回線/VC（Circuits/VCs）] および [削除済み回線/VC（Deleted Circuits/VCs）] タブの [プロビジョニング（Provisioning）] 列の横にある [i] アイコンをクリックすると、回線/VC に参加している各デバイスの設定、設定エラー、ロールバック設定、およびロールバック設定エラーの詳細が表示されます。[i] アイコンは、[なし（None）] を除くすべてのプロビジョニング状態で使用できます。

詳細テーブルでのデータのフィルタ処理

[表示（Show）] ドロップダウン リストからクイック フィルタまたは高度なフィルタを使用して、特定のアラーム、回線/VC、ネットワーク インターフェイス、またはリンクを見つけるためにデータをフィルタ処理することもできます。クイック フィルタでは、列の上部に入力したテキストに従って、列に表示されるコンテンツが絞り込まれます。高度なフィルタを使用すると、「次を含まない（Does not contain）」、「等しくない（Does not equal）」、「次で終わる（Ends with）」、「が空である（Is empty）」などの複数の演算子を使用してフィルタを適用し、テーブル内のデータを絞り込むことができます。また、ユーザー定義フィルタを作成することもできます。これを保存すると、[表示（Show）] ドロップダウン メニューに追加されます。

ユーザー定義フィルタを作成して保存するには、次の手順を実行します。

ステップ 1 アラーム、回線/VC、ネットワーク インターフェイス、およびリンクの拡張テーブルの上にある [表示（Show）] ドロップダウン リストから、[高度なフィルタ（Advanced Filter）] を選択します。

ステップ 2 [高度なフィルタ（Advanced Filter）] データ ポップアップ ウィンドウで、高度なフィルタ条件を入力し、[名前を付けて保存（Save As）] をクリックします。

ステップ 3 [フィルタの保存（Save Filter）] ダイアログボックスで、フィルタの名前を入力して [保存（Save）] をクリックします。

ユーザー定義フィルタを編集または削除するには、[表示（Show）] ドロップダウン リストから [ユーザー定義フィルタの管理（Manage User Defined Filters）] を選択します。

マップでのデバイスの検索

トポロジ マップと Geo マップで、次の条件でデバイスを検索できます。

- デバイス名
- デバイス ファミリ
- IP アドレス
- ユーザー定義フィールドの値

マップで特定のデバイスを検索するには、次の手順を実行します。

ステップ 1 ツールバーの [検索（Search）] アイコンをクリックします。

ステップ 2 デバイス名、IPアドレス、デバイスファミリ、ユーザー定義フィールドの値の全部または一部を検索テキスト ボックスに入力し、Enter を押します。トポロジ マップに、検索条件に一致するデバイスの一覧が表示されます。Geo マップの [検索結果（Search Results）] パネルには、検索に一致するデバイスが一覧表示され、それらのデバイスがマッピングされているかどうかが示されます。[i] アイコンをクリックして、デ

バイスに関する詳細情報が含まれている [デバイス 360（Device 360）] を表示します。デバイスをクリックして、マップ内でハイライト表示します。

トポロジ マップの表示内容の決定

ネットワーク トポロジ マップに表示するデバイス グループの選択

トポロジマップを使用すると、1 つまたは複数のデバイス グループのトポロジを視覚化できます。選択されたグループでは、特定のネットワーク セグメント、顧客ネットワーク、またはその他のネットワーク要素の組み合わせがカバーされている場合があります。デバイスのグループ化は、階層的に行われます。他の複数のサブグループを含む最上位の親グループが 2 つあります。それらは、ロケーション グループとユーザー定義グループです。同一の最上位の親グループ内に複数のグループを表示することができます。たとえば、ロケーション グループを複数表示することはできますが、1 つのロケーション グループと 1 つのユーザー定義グループを表示することはできません。

トポロジマップに表示するデバイス グループを決定するには、左側のペインにある [デバイス グループ（Device Groups）] ボタンをクリックし、1 つまたは複数のデバイス グループを選択します。

トポロジマップでグループごとに表示できるデバイスの最大数は 1,500 です。トポロジマップをロードすると、Cisco EPN Manager は 2 つのしきい値で次の警告メッセージを表示します。

- 1,000 デバイス：低速である可能性を示すポップアップメッセージでマップを表示します。
- 1,500 デバイス：空のマップにポップアップメッセージが表示され、非常に多いデバイスの場合はマップを表示できないことが示されます。

（注） しきい値の制限は、デバイス間のリンク数ではなく、デバイス数に基づいています。

必要なグループをトポロジマップに表示させた後、任意のデバイスまたはリンクに関する追加情報にアクセスできます。「デバイスの詳細情報の取得」および「リンクの詳細情報の取得（137 ページ）」を参照してください。

トポロジマップには、ユーザーに割り当てられている仮想ドメインに基づき、ログインしているユーザーがアクセス特権を持つデバイスのみが表示されます。

（注） トポロジ コンポーネントが適切に描画されない、あるいはコンポーネント データがマップに表示されないなど、トポロジに関する問題が発生した場合は、ブラウザ キャッシュをクリアして再試行することをお勧めします。

トポロジ マップにネットワーク要素を表示するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 左側のペインにある [デバイス グループ（Device Groups）] ボタンをクリックし、[デバイス グループ（Device Groups）] パネルを開きます。

ステップ 3 トポロジマップに表示するデバイス グループをクリックし、[ロード（Load）] をクリックします。デバイス グループの選択は、トポロジ マップの上に表示されます。

ステップ 4 必要に応じて特定のデバイス/リンク タイプを表示し、手動リンクを追加するなどを行って、トポロジマップをカスタマイズします。詳細については、次のトピックを参照してください。

- ネットワーク トポロジ マップに表示するリンクとデバイス タイプの変更 （230 ページ）
- トポロジ マップへのリンクの手動による追加 （228 ページ）
- ネットワーク トポロジ マップのレイアウトの変更 （244 ページ）

トポロジ マップにサブグループのコンテンツを表示する

サブグループを展開すると現在のコンテキストでそのコンテンツを表示できます。またはドリルダウンすると、現在のマップ コンテキストとは別にサブグループのコンテンツを表示できます。

（注） あるデバイスが複数のグループに属している場合、サブグループを展開すると、展開されたグループの 1 つにのみ、そのデバイスが表示されることに注意してください。デバイスは、属しているすべてのグループに表示されるわけではありません。複数のグループに属するデバイスが設定に含まれる場合は、この方法ではなく、[デバイス グループ（Device Groups）] ペインでそれらのグループを選択して、トポロジマップで個々にグループを表示してください。これにより、特定のグループに属するすべてのデバイスが常に表示されます。

サブグループの内容を表示するには、次の手順を実行します。

ステップ 1 トポロジ マップのサブグループをクリックします。

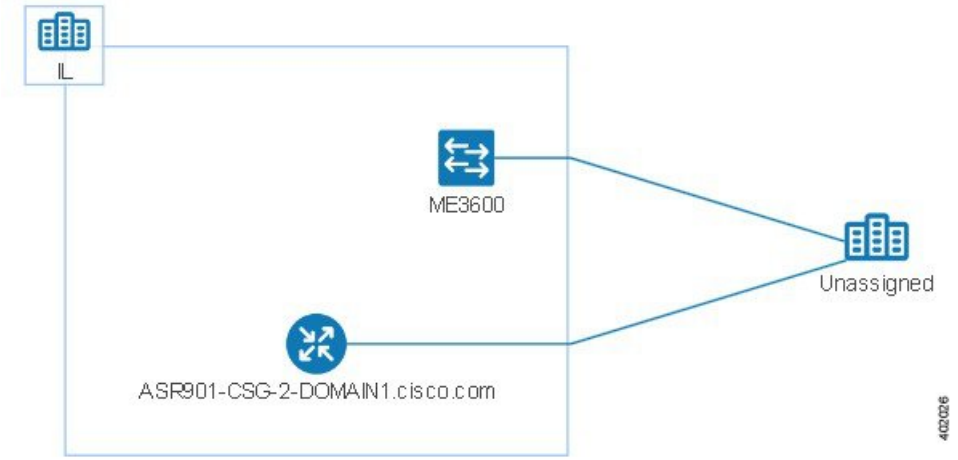
ステップ 2 表示されたポップアップで、次のいずれかをクリックします。

- [グループのドリルダウン（Drill down group）]：トポロジ マップにサブグループがそのまま表示されます。つまり、現在表示されているグループが、選択したサブグループに置き換えられます。サブグループ名が [デバイス グループ（Device Groups）] ペインで選択されることに注意してください。

  （注） サブグループをダブルクリックすると、グループへのドリル ダウンをすばやく実行できます。

- [グループの展開（Expand group）]：現在のトポロジマップ表示にサブグループのコンテンツが追加されます。

下の図では、IL グループが展開されています。



トポロジ マップへのデバイスとネットワークの手動による追加

システムで管理されていないデバイスやネットワークは、それらを手動で追加することでトポロジ マップや Geo マップに表示できます。

ステップ 1 トポロジ ツールバーで、[作成（Create）] > [管理対象外デバイスの作成（Create Unmanaged Device）] か、または [作成（Create）] > [管理対象外ネットワークの作成（Create Unmanaged Network）] を選択します。

ステップ 2 マップをクリックし、デバイスまたはネットワークをマップに追加します。

ステップ 3 マップに新たに追加したデバイスまたはネットワークをクリックします。表示されたパネルから、デバイスまたはネットワークをグループに追加する、デバイスまたはネットワークの名前を変更する、あるいはデバイスまたはネットワークを削除することができます。

デバイスまたはネットワークをトポロジ マップに追加した後は、Geo マップでも使用できるようになります。管理対象外デバイスがマップされていないデバイスのリストに表示され、その位置を設定することができます。Geo マップへのマップされていないデバイスの配置 （260 ページ）を参照してください。

トポロジ マップへのリンクの手動による追加

2 台のデバイスが接続されていることがわかっているものの、Cisco EPN Manager がリンクを検出できず、それをマップに表示している場合は、そのリンクを手動で追加できます。このリンクを追加した後は、関連するグループがマップに表示される場合は常にデフォルトで表示されます。

手動リンクを使用できる最も一般的なシナリオを次に示します。

- IOS-XR（NCS 4000、9000、5000、1000）を実行している Cisco NCS デバイス上のトランク ポートの光/DWDM コントローラと NCS 2000 デバイスのアド/ドロップ ポート ペア間。
- IOS-XR（NCS 4000、9000、5000、1000）を実行している Cisco NCS デバイス上のクライアント ポートの光/DWDM コントローラと NCS 2000 トランスポンダ クライアント ポート間（10GE/100GE ポートの接続を表す）。
- IOS-XR（NCS 4000、9000、5000、1000）を実行している Cisco NCS デバイス上のポートの 10GE/100GE コントローラと NCS 2000 トランスポンダ クライアント ポート間（10GE/100GE ポートの接続を表す）。
- 400-G-XP ラインカードを搭載した Cisco NCS 2000 シリーズ デバイス上の 2 つのトランク ポート間。このリンクは、管理対象 OTU リンクとして作成する必要があります。
- 400-G-XP ラインカードを搭載した Cisco NCS 2000 シリーズ デバイスと、4H-OPW-QC2 ラインカードを搭載した Cisco NCS 4000 シリーズ デバイス間。このリンクは、管理対象 OTU リンクとして作成する必要があります。

手動リンクは、管理対象または管理対象外にすることができます。

- 管理対象外のリンク：視覚化する場合に限ります。2 台のデバイスが接続されているものの、それらのデバイス間のリンクを完全に管理する必要がない場合は、管理対象外の手動リンクをマップに追加できます。このリンクは、グレーの破線で表示されます。
- 管理対象リンク：管理対象の手動リンクを追加すると、そのリンクはデータベースに保存されてすべてのリンク テーブルに組み込まれます。他のすべての管理対象リンクと同様にマップ上に実線で表示されます。Cisco EPN Manager は、接続先の管理対象デバイス インターフェイスからリンク ステータスを取得します。手動で追加した管理対象リンクの検出ステータスは [事前プロビジョニング済み（Pre-provisioned）] になります。これは、システムで検出されなかったことを示します。

（注） 1 つのデバイスを誤って削除した場合は、管理型リンクのもう一方の端も削除してから、管理型リンクを再作成してください。

2 台のデバイス間にリンクを手動で追加するには、次の手順を実行します。

ステップ 1 トポロジ ツールバーで、**[作成（Create）]** > **[管理対処外リンクの作成（Create Unmanaged Link）]**、または **[作成（Create）]** > **[管理対象リンクの作成（Create Managed Link）]** を選択します。

ステップ 2 トポロジ マップ内で最初のデバイスをクリックし、マウス ボタンを押したまま 2 番目のデバイスまでドラッグします。

ステップ 3 [インターフェイスの詳細（Interface Details）] ダイアログで、使用可能なインターフェイスのドロップダウン リストから最初のデバイスの送信元インターフェイスと、2 番目のデバイスのターゲット インターフェイスを選択し、[OK] をクリックします。

（注） エンドポイントが別のリンクの一部ではないことを確認します。IOS-XR デバイスから SVO アド/ドロップポートの場合、2 つの管理型リンクを作成して集約リンクを形成する必要があります。

選択した 2 台のデバイス間のリンクがマップに表示されます。

手動で追加したリンクの削除

マップに手動で追加したリンクは、システムから削除できます。

- 手動で追加した管理対象リンクは、以下の手順に従って [リンク（Links）] テーブルから削除します。
- 手動で追加した管理対象外リンクを削除するには、マップ内のリンクをクリックし、[リンク（Link）] パネルの [削除（Delete）] をクリックします。
- エンドポイントを削除する前に、必ず管理型リンクを削除してください。
- SVO ノードでは、管理型リンクを削除する前に相互接続を削除しないでください。

手動で追加した管理対象リンクを削除する手順は次のとおりです。

ステップ 1 左側のサイドバーで、**[インベントリ（Inventory）]** > **[その他（Other）]** > **[リンク（Links）]** を選択します。

ステップ 2 [リンク（Links）] テーブルの [ステータス（Status）] 列をフィルタ処理して、事前プロビジョニングされたリンクを表示し、目的のリンクを選択します。

ステップ 3 [削除（Delete）] アイコンをクリックしてリンクを削除します。[削除（Delete）] アイコンは、手動で追加したリンクに対してのみ有効になります。

ステップ 4 または、手動で作成したリンクを削除するには、削除するリンクの情報アイコン（I）をクリックします。

[リンクの詳細（Link Details）] ウィンドウに、[タイプ（Type）] が [手動（Manual）] の単一リンクが表示されます。

ステップ 5 エントリを選択し、削除アイコン（X）をクリックしてリンクを削除します。

手動で追加した管理対象外リンクを削除する手順は次のとおりです。

1. [リンク（Links）]テーブルの[ステータス（Status）]列をフィルタ処理して、事前プロビジョニングされたリンクを表示し、目的のリンクを選択します。
2. 手動で作成した管理対象外リンクを削除するには、削除するリンクの情報アイコン（I）をクリックします。[リンクの詳細（Link Details）] ウィンドウに、[タイプ（Type）] が [手動（Manual）] の単一リンクが表示されます。
3. エントリを選択し、削除アイコン（X）をクリックしてリンクを削除します。

リンク名の変更

デフォルトで、リンク名は A エンドおよび Z エンドのインターフェイス名に基づいてシステムによって自動的に生成されます。リンク名は変更できます。この場合、すべてのリンク テーブル、[リンク360（Link 360）] ビュー、およびマップ上に新しい名前が表示されます。

リンクの名前を変更する手順は次のとおりです。

ステップ 1 いずれかのリンク テーブルに移動します。

ステップ 2 名前を変更するリンクを選択します。

ステップ 3 [アクション（Actions）] > [名前の変更（Rename）] を選択します。

ステップ 4 リンクの一意の名前を入力し、[名前の変更（Rename）] をクリックします。

ネットワーク トポロジ マップに表示するリンクとデバイス タイプの変更

特定タイプのリンクやデバイスのみを選択してネットワーク トポロジ マップに表示することができます。[表示（Show）] ボタンをクリックして [リンク（Links）] または [デバイス ファミリ（Device Families）] を選択し、リンクとデバイス タイプの完全なリストを表示し、表示するものを選択します。

（注） マップ上に表示する特定の回路/VC を選択すると、リンク/デバイス タイプのフィルタは無効になります。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 トポロジツールバーで [表示（Show）] をクリックし、[リンク（Links）] または [デバイス ファミリ（Device Families）] を選択します。

ステップ 4 [リンク（Links）] ダイアログで、次の手順を実行します。

- トポロジマップに表示するリンクのタイプ（たとえば、物理層リンク、イーサネット層リンクなど）を選択します。[リンク（Links）] ダイアログには、ネットワーク内に存在するリンク タイプのみが表示されます。ネットワーク内にリンク タイプが存在していても、選択したデバイス グループにない場合、そのリンク タイプは無効になります。
- 単一のリンクから集約リンクを差別化する場合は、チェックボックスとして [集約リンクの表示（Display Aggregated Links）] を選択します。
- この機能をサポートするリンク上の帯域幅利用の仮想化を有効にできます。詳細については、リンクでの帯域幅使用率をマップに表示 （242 ページ） を参照してください。
- [OK] をクリックします。トポロジ マップに選択内容が反映されます。選択したリンク タイプのみが表示されます。

ステップ 5 [デバイス（Devices）] ダイアログで次の手順を実行します。

- トポロジマップに表示するデバイス タイプ（たとえば、ルータ、スイッチおよびハブ、オプティカル ネットワーキングなど）を選択します。[デバイス（Device）] ダイアログには、ネットワーク内に存在するデバイス タイプのみが表示されます。ネットワーク内にデバイス タイプが存在していても、選択したデバイス グループにない場合、そのデバイス タイプは無効になります。
- [OK] をクリックします。トポロジ マップに選択内容が反映されます。選択したデバイス タイプのみが表示されます。

（注） マップ上にオプティカル ネットワークを表示する場合、デフォルトでは、光回線増幅器として機能するデバイスがある場合は、それらが表示されます。これらの光回線増幅器デバイスをマップに表示しない場合は、[デバイス機能（Device Functions）] の下にある [光回線増幅器の表示（Display Optical Line Amplifier）] チェックボックスをオフにします。[デバイスの機能（Device Functions）] の下にある [光回線増幅器の表示（Display Optical Line Amplifier）] チェックボックスは、回線増幅器の機能をサポートする光デバイスがセットアップに存在する場合にのみ表示されます。

トポロジマップでのラベルの表示/非表示

デバイス名ラベルを非表示にすることもできます。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 トポロジ ツールバーの [表示（Show）] ボタンをクリックします。

ステップ 3 **[ラベル（Labels）]** チェックボックスをオンにします。

ステップ 4 [表示（Show）] ダイアログを閉じます。選択内容がトポロジ マップに適用されます。

アラームによるデバイスとリンクのフィルタ処理

アラームが含まれているデバイスまたはリンクのみを表示し、残りのデバイスを抑制するには、次の手順を実行します。

ステップ 1 左側のサイドバーで、**[マップ（Maps）] > [トポロジマップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 トポロジ ツールバーの [表示（Show）] クリックし、[アラーム（Alarms）] を選択します。

ステップ 3 チェックボックスを選択してすべてのアラームを表示するか、またはスライダを使用して特定の重大度以上のアラームを表示します。

ステップ 4 アラームを含んでいるデバイスとリンクのみを表示するには、[選択されたアラームを含む要素のみを表示（Show only elements with the selected alarms）] を選択します。

ステップ 5 [表示（Show）] ダイアログを保存して閉じるには、[OK] をクリックします。

マップ表示のグローバル設定の保存

マップツールバーの [表示（Show）] ボタンを使用すると、デバイス名（ラベル）、デバイスタイプ、リンクタイプ、アラームの重大度など、マップ表示に表示する項目を選択できます。

スーパーユーザーまたは管理ユーザーは、すべての新しいユーザーに自動的に適用され、すべてのユーザーがオンデマンドで読み込めるグローバル設定として選択肢を保存できます。グローバル設定を削除することもできます。

（注） ネットワークトポロジの編集権限を持つユーザーは、グローバル設定を保存および削除できます。トポロジマップにアクセスするには、ネットワークトポロジの権限も必要です。

次の項目がグローバル設定として保存されます。

- ラベルのオン/オフ
- デバイス ファミリ
- リンク タイプ

- アラーム重大度
- 帯域幅使用率

マップ表示のグローバル設定を保存する手順は次のとおりです。

ステップ 1 左側のサイドバーから、[マップ（Maps）] > [トポロジマップ（Topology Maps）] >[ネットワークトポロジ（Network Topology）] の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 トポロジ ツールバーの [表示（Show）] をクリックし、マップに表示する項目を選択します。

ステップ 4 [グローバル設定（Global Preferences）] > [保存（Save）] を選択します。

保存したグローバル設定は、必要に応じて [削除（Delete）] をクリックして削除できます。

マップ表示のグローバル設定の読み込み

マップ ツールバーの [表示（Show）] ボタンを使用すると、デバイス名（ラベル）、デバイス タイプ、リンク タイプ、アラームの重大度など、マップ表示に表示する項目を選択できます。

マップ表示のグローバル設定が定義されている場合は、読み込むことができます。読み込んだマップ表示に必要に応じて独自の変更を加えることができます。

次の項目がグローバル設定として保存されます。

- ラベルのオン/オフ
- デバイス ファミリ
- リンク タイプ
- 障害の重大度
- 帯域幅使用率

マップ表示のグローバル設定を読み込む手順は次のとおりです。

ステップ 1 左側のサイドバーから、[マップ（Maps）] > [トポロジマップ（Topology Maps）] >[ネットワークトポロジ（Network Topology）] の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 [グローバル設定（Global Preferences）] > [ロード（Load）] を選択します。グローバル設定が定義されていない場合、このオプションは無効になります。

大規模なトポロジ マップの特定のセクションを隔離する

トポロジマップに何千ものデバイスが表示される場合は、特定のデバイスまたはデバイスセットのみを重点的に扱うことができます。[概要（Overview）]ペインにはトポロジマップ全体が縮小サイズで表示されるので、そこから大きなトポロジマップ内の表示させたい領域を選択できます。また、トポロジ マップ内の要素のアラーム ステータスも見やすく表示されます。

ステップ 1 トポロジ ツールバーで [概要（Overview）] アイコンをクリックします。トポロジ マップの右下に [概要（Overview）] ペインが表示され、次の項目が表示されます。

- ドット：ネットワークの任意の要素を示します。ドットの色は、ネットワーク要素に関連するアラームの重大度を示します。
- 実線：リンクを示します。線の色は、関連するアラームの重大度を示します。
- 青い四角：選択された領域を表します。四角内の領域がマップ ペインに表示されます。四隅のハンドルを使用して、選択領域のサイズを変更できます。
- パン モード カーソル：選択領域内に表示されるカーソル。このカーソルを使って選択領域を移動すると、マップ ペインのさまざまな要素を参照できます。
- ズーム モード カーソル：選択領域の外に表示されます。このカーソルを使用して、新しい選択領域を定義したり、既存の選択領域を拡大します。

ステップ 2 トポロジ マップに表示させたい領域上でマウスをドラッグし、四角形を描きます。

ステップ 3 右上隅にある [x] をクリックして [概要（Overview）] ペインを閉じます。

デバイスの詳細情報の取得

トポロジ マップでドリルダウンすると、デバイスに関する詳細を得ることができます。

ステップ 1 トポロジ マップで該当するデバイスをクリックします。ポップアップが開き、デバイスの基本情報とアラーム情報が表示されます。

ステップ 2 [360 度表示（View 360）] をクリックすると、[デバイス 360（Device 360）] ビューにアクセスしてデバイスの詳細情報を表示できます。

詳細については、基本デバイス情報を取得する：[デバイス 360（Device 360）] ビュー （106 ページ） を参照してください。

リンクの詳細情報の取得

Cisco EPN Manager には、リンクを表示し、それらの詳細を取得するさまざまな方法が用意されています。

次のリンク情報を表示するには：	以下の手順を参照：
特定のリンク	特定のリンクの概要：[リンク 360（Link 360）] ビュー （235 ページ）
トポロジ マップ内の特定のリンク	トポロジ マップでの特定のリンクの表示 （239 ページ）
トポロジ マップ内のグループ	ネットワーク トポロジ マップでのデバイス グループのリンクの表示 （239 ページ）
Cisco EPN Manager のすべて	リンク テーブルの表示 （240 ページ）

特定のリンクの概要：[リンク 360（Link 360）] ビュー

[リンク 360（Link 360）] ビューでは、デバイスのリンクの設定とステータスをすばやく確認できます。[リンク 360（Link 360）] ビューそれぞれには、リンクの A 側と Z 側に関する情報（タイプ、方向、容量など）が表示されます。また、リンクとデバイス タイプによっては、電力レベル、スパン損失、ビット エラーなどのさまざまなメトリックも表示されます。

[リンク 360（Link 360）] ビューを起動するには、リンク テーブルのリンク名の横にある [i] アイコンをクリックします。これには、トポロジ マップで [リンク テーブル（Links Table）] をクリックするか、または**[インベントリ（Inventory）]>[その他（Other）]>[リンク（Links）]** を選択すると開くテーブルが含まれています。

[リンク 360（Link 360）] ビューでは、ビューの上部にリンクとパフォーマンスに関する一般情報が示され、ビューの下部にあるタブにはより詳細なリンク情報が示されます。

[リンク 360（Link 360）] ビューで提供される情報	説明

一般情報	リンク名、サービサビリティ ステータス、最高重大度アラーム、タイプ、方向、容量、および使用率。リンク サービサビリティの状態の定義については、リンクの有用性状態 （237 ページ）を参照してください。 表示されているリンクがOTS リンクまたはOTU リンクの場合は、[使用率（Utilization）] フィールドの [i]（**情報**）アイコンをクリックして [使用波長（Used Wavelengths）] ポップアップ ウィンドウを開くことができます。このウィンドウには、リンク上に設定されている光チャネルと、現在これらのチャネルを使用している回線が一覧表示されます。 [自動更新（Auto-Refresh）]：ステータスとトラブルシューティングをリアルタイムで更新する場合は、[更新（Refresh）] アイコンをクリックしてオンデマンド更新を有効にします。または、ドロップダウンリストから、自動更新の間隔を 30 秒、1 分、2 分、または 5 分に設定することもできます。デフォルトでは、自動更新はオフになっています。 （注） 自動更新設定は、現在開いている [360° ビュー（360° View）] ポップアップウィンドウにのみ適用されます。このビューを閉じてからもう一度開いた場合または別のビューを開いた場合は、デフォルトでは自動更新がオフになります。
パフォーマンス データ	リンク パフォーマンスをさまざまな側面から示すグラフまたはチャート。
スパンロス	チャネルのスパンロスデータが、最小および最大のしきい値と解像度とともに表示されます。スパンロスデータが範囲外の場合は、赤色で表示されます。
アラーム	重大度、ステータス、生成された時刻、アラームの発生源、アラームの ID を含む、リンクに関する現在のアラーム。また、アラーム ブラウザの起動ポイントも示されます。
Links	（LAGのみ）リンク集約グループのA側とZ側のポートのステータス、名前、およびIP アドレス。
エンドポイント	リンクのエンドポイントとして機能するデバイスおよびインターフェイス。[インターフェイス360（Interface 360）] ビューの起動ポイントが示されます。光デバイスの場合、このタブには、送信および受信された信号について記録された最新の電力値も表示されます。 （注） 電力値は通常、手動リンクの場合は表示されません。ただし、Cisco NCS 1000 デバイスと Cisco NCS 2000 デバイスの間の手動の LMP リンクまたはOTS リンクについて [リンク360（Link 360）] ビューを開くと、両方のエンドポイントの電力値がビューに表示されます。

回線/VC	（リンクを横断する回線/VCの場合）回線/VC名、タイプ、顧客、ステータス、作成日。また、[回線/VC 360（Circuit/VC 360）] ビューの起動ポイントも示されます。
SRRG（SRRGs）	リンクまたはリンクのエンドポイントデバイスに割り当てられている共有リスク リソース グループ（SRRG）のリスト。一覧表示されている各SRRGについては、それがリンク/デバイスのデフォルトのSRRGか、またはリンク/デバイスに割り当てられたものかを確認できます。SRRGに関する詳細については、「Geoマップでの共有リスク リソース グループ（SRRG）の管理」を参照してください。
APC	リンクのサイド、管理ステータス、APCステータス、および進捗ステータスを一覧表示します。

リンクの有用性状態

サービスアビリティ状態	アイコン	説明
管理上ダウン		リンクは意図的に管理者によってシャットダウンされました。
ダウン		リンクがダウンしています（ただしダウンは不適切な状態）。
アップ		リンクはアップの状態で、トラフィックがリンクを通過しています。
自動アップ		信号が検出されたためリンクはアップ状態です（この状態は光デバイスでのみサポートされています）。
取得不可		リンクがまだ検出されていないか、またはそのステータスが取得できません。
一部		リンクの要求、リソース、またはリソース状態に不一致があります。例： • リンクが、一部のサービス リソースをアクティブ化し、他のサービス リソースを非アクティブにする要求を処理している。 • リンクにいくつかのアクティブ リソースといくつかの非アクティブ リソースがある。 • アップしているリンク リソースとダウンしているリンク リソースがある。 • リンクのリソースのいずれかの状態が不明である。

リンクの情報とステータスの比較

[比較ビュー（Comparison View）] では、複数のリンクの対照比較を実行し、発生したアラームや、関連するエンドポイント、回線、および VC のステータスなどの情報を表示できます。リンクを比較するには、次の手順を実施します。

ステップ 1 比較するリンクごとに次の手順を行います。

a) 「特定のリンクの概要：[リンク 360（Link 360）] ビュー」の説明に従って、[リンク360（Link 360）] ビューを開きます。

b) **[アクション（Actions）] > [追加して比較（Add to Compare）]** を選択します。

選択したリンクがページの下部に表示されます。最大 4 つのリンクを選択できます。

ステップ 2 [比較（Compare）] をクリックします。

比較ビューが開きます。

ステップ 3 ビューの上部にあるドロップダウンリストで、利用可能なすべての情報をビューに表示するか、リンクごとに一意の情報だけを表示するかを指定します。

ステップ 4 [比較ビュー（Comparison View）] をクリックして、ビューに表示するカテゴリのチェックボックスをオンにしてから、[保存（Save）] をクリックします。

デフォルトで、すべてのカテゴリがすでに選択されています。

ステップ 5 選択したカテゴリごとに提供される情報が表示されるようにページをスクロール ダウンします。

次の点に注意してください。

- [比較ビュー（Comparison View）] には、一度に 2 つのリンクに関する情報しか表示されません。3 つ以上を選択した場合は、現在表示されていないリンクに切り替える必要があります。
- 選択したリンクの順序を変更するには、[並べ替え（Rearrange）] をクリックします。
- 各リンクの [アクション（Actions）] メニューは、[リンク360（Link 360）] ビューで提供されるメニューと同じです。オプションを選択すると、対応するページが開きます。
- 必要に応じて、表示されるカテゴリを最小化または最大化できます。
- [比較ビュー（Comparison View）] は、回線と VC、デバイス、およびインターフェイスでも利用できます。それぞれの 360 ビューからこれらの要素のいずれかを比較用に選択すると、対応するタブにその要素が表示されます。これにより、必要に応じて要素のタイプを切り替えることができます。
- リンクの比較を終了する場合は、ビューの上部にある [戻る（Back）] をクリックしてから、ページの下部にある [すべてクリア（Clear All）] をクリックします。他の要素タイプのタブが表示されている場合は、それらのタブもクリアする必要があります。

トポロジ マップでの特定のリンクの表示

次のページから特定のリンクを選択し、そのリンクをトポロジ マップに表示します。

- リンク 360 ビューを起動し、**[アクション（Actions）] > [トポロジに表示（Show in Topology）]** を選択します。リンク 360 ビューを表示する方法については、特定のリンクの概要：[リンク 360（Link 360）] ビュー （235 ページ）を参照してください。
- リンク テーブルから特定のリンクを選択し、**[アクション（Actions）] > [トポロジに表示（Show in Topology）]** を選択します。リンク テーブルにアクセスするには、トポロジ マップの [リンク（Links）] タブで [リンク テーブル（Links Table）] ハイパーリンクをクリックするか、または **[インベントリ（Inventory）] > [その他（Other）] > [リンク（Links）]** を選択します。

ネットワーク トポロジ マップでのデバイス グループのリンクの表示

Cisco EPN Manager は、次の規則を使用して、トポロジ マップにリンクを表示します。

- 実線は、トポロジ マップ内の 2 つの要素間で検出されたリンク タイプを表します。
- 点線は、トポロジで手動で描画された管理対象外リンクを表します。
- （**[表示（Show）] > [リンク（Links）]** メニューで有効にした場合）鎖線は、集約リンクを表します。
- 重要なアラームがあるリンクは赤色で表示され、リンク上にアラーム アイコンが表示されます。
- ダウンしており、重要なアラームがない既存のリンクはグレーで表示され、リンク上に [?]アイコンが表示されます。そのリンクは、6時間経過すると自動的にマップから削除されますが、必要に応じ、[リンク（Links）] テーブルから、または [リンクの詳細（Link Details）] ビューから時間の経過前に手動で削除することができます。

アラーム重大度バッジがリンクに表示されている場合は、リンクに影響を与えている最も重大なアラームを表します。集約リンクについては、集約内のいずれかのリンクに影響する最も重大なアラームを表します。

トポロジ マップ内のリンクの詳細を取得するには、次の手順を実行します。

- マウスを使用してリンク上にカーソルを移動し、最も重大なアラームまたはリンクの帯域幅使用率の情報など、そのリンクに関する有用な情報を（もしあれば）「概要表示」するパネルを表示します。リンク上にアラームがなく、帯域幅使用率の情報もない場合は、このパネルは表示されません。リンク上にアラームがある場合は、アラームの重大度アイコンの横にある数字をクリックすると、それらのアラームだけを一覧表示するテーブルが表示されます。
- リンクをクリックすると、リンクのタイプ、リンクの A 側および Z 側のデバイスとインターフェイス、リンクの使用状況などのリンク情報を表示するポップアップ ウィンドウが表示されます。集約リンクの場合は、基盤となっているすべてのリンクのリストがポップ

アップウィンドウに表示されます。リンクの数が1行で200リンクを超えると、Cisco EPN Managerはリンクパネルに警告メッセージを表示し、200 リンクのみを表示します。

リンク テーブルの表示

Cisco EPN Managerは、管理しているすべてのリンクを一覧表示したリストを提供します。これによって、特定のタイプ、または共通の文字列を共有する名前を持ったすべてのリンクを簡単に見つけることができます。また、重大なアラームがあるリンクを特定し、インターフェイス 360 ビューを起動して影響を受ける側を表示することができます。

このテーブルでは、リンク使用率や容量もすばやく確認できます。

さらに、トポロジマップに表示されている現在のグループのリンクを示すテーブルを開くこともできます。このテーブルは、システム内のすべてのリンクを示すテーブルと同じ情報およびアクションを提供します。

ステップ 1 リンク テーブルを表示するには、次の手順を実行します。

- すべてのリンクの場合：左側のサイドバーで、**[インベントリ（Inventory）]**>**[その他（Other）]**>**[リンク（Links）]** の順に選択します。
- 選択したデバイス グループのリンクの場合：トポロジ マップ ウィンドウの左側のペインで [リンク（Link）] タブを選択し、タブの右上隅にある [解除（Detach）] アイコンをクリックするか、タブの下部にある [リンクテーブル（Links Table）] ハイパーリンクをクリックします。[リンク（Links）] テーブルが新しいウィンドウで開きます。

ステップ 2 ここでは、次の操作を実行できます。

- 特定タイプのリンクの検索：たとえば、物理的、疑似ワイヤ、LAG、ODUなどです。[タイプ（Type）] フィールドにマウスのカーソルを置き、ドロップダウン リストからリンク タイプを選択します。また、この方法で手動リンクを検索することもできます。
- [リンク名（Link Name）]テキストボックスにテキストを入力し、名前でリンクを検索します。また、部分的な文字列（たとえば、「**3.3.3.3_**」）を入力することもできます。
- 重大アラームが設定されたリンクを検索するには、[重大度（Severity）]テキストボックスをクリックして重大度ドロップダウン リストを表示し、重大度を選択します。A 側またはZ 側からもこの同じ手順を実行できます。テーブルには、リンクのどちらの側により重大なアラームがあるかが示されます。また、インターフェイス 360 ビューを両側に起動できます。
- [ステータス（Status）]列のリンクの動作および検出ステータスを参照してください。リンクの動作ステータスは [アップ（Up）] または [ダウン（Down）] です。検出ステータスは次のいずれかになります。
  - [事前プロビジョニング済み（Pre-provisioned）] : ユーザーが手動で作成したものの、システムで検出されなかった管理対象リンク。これらのリンクは、システムやマップから削除できます。リンクを選択し、[削除（Delete）] アイコンをクリックします。

- [事前プロビジョニング済み - 未完了（Pre-provisioned-Incomplete）]：完全に検出できなかった手動で作成されたリンク。
- [検出済み - 未完了（Discovered-Incomplete）]：完全に検出できなかったリンク。一部検出されたこれらのリンクはトポロジ マップに表示されません。
- [不明（Unknown）]：ダウンしているため、検出できなくなっている既存のリンク。これらのリンクは、トポロジ マップ上に 6 時間残りますが、色がグレーになっており、リンク上に表示される [?] アイコンで識別されます。ステータスが [不明（Unknown）] のリンクは、テーブル上で当該のリンクを選択し、[削除（Delete）] をクリックすると削除できます。

- 光リンク（OTS、OTN、ODU）とパケットリンク（物理、LAG）での帯域幅使用率を確認します。リンクの各側の [使用率（Utilization）] 列には、実際の使用状況データ（たとえば、OTS リンクのチャネルの数）、使用されている総容量のパーセンテージ、およびデフォルトの使用率計算期間（1 時間）が表示されます。[容量（Capacity）] 列には、リンクの総帯域幅容量が表示されます。

  （注） パケット リンクおよびケーブル リンクでの使用率を表示するには、インターフェイス ヘルスのモニターリング ポリシーを作成し、関連するデバイスで有効にする必要があります。詳細については、基本的なインターフェイス モニターリングの設定 （283 ページ） を参照してください。

Type	A End ...	A End	A End Utilization	Z End ...	Z End	Z End Utilization	Capacity
Physical	Critical	GigabitEth...	0% (1.2800899e-7 Gbps) 1h	Clea...	GigabitEth...	0% (3.8312794e-7 Gbp	1 Gbps
Physical	Clea...	GigabitEth...	0% (1.574779e-7 Gbps) 1h	Clea...	GigabitEth...	0% (4.6376692e-7 Gbp	1 Gbps
Physical	Clea...	TenGigabi...	0% (0.000044290136 Gbps) 1	Clea...	TenGigabi...	0% (0.00003339692 Gb	10 Gbps
Physical	Clea...	TenGigabi...	0% (0.000071106515 Gbps) 1	Clea...	TenGigabi...	0% (0.00007004112 Gb	10 Gbps
Physical	Clea...	GigabitEth...	0% (3.2127232e-8 Gbps) 1h	Clea...	GigabitEth...	0% (0.0000010210271	1 Gbps
Physical	Clea...	GigabitEth...	0% (6.619419e-8 Gbps) 1h	Clea...	GigabitEth...	0% (1.9693468e-7 Gbp	1 Gbps
Physical	Clea...	TenGigabi...	0.03% (0.002898862 Gbps) 1h	Clea...	TenGigabi...	0.03% (0.0028905713 (	10 Gbps
Physical	Clea...	GigabitEth...	0.05% (0.00047108906 Gbps)	Clea...	GigabitEth...	8.01% (0.08006172 Gbp	1 Gbps
Physical	Clea...	GigabitEth...	0% (8.722009e-8 Gbps) 1h	Clea...	GigabitEth...	0% (6.596751e-8 Gbps)	1 Gbps
Physical	Clea...	GigabitEth...	0% (8.718443e-8 Gbps) 1h	Clea...	GigabitEth...	0% (6.419498e-8 Gbps)	1 Gbps
Physical	Clea...	TenGigabi...	1.25% (0.12529424 Gbps) 1h	Clea...	TenGigabi...	1.09% (0.109484255 Gl	10 Gbps
Physical	Clea...	GigabitEth...	0.03% (0.00029982472 Gbps)	Clea...	GigabitEth...	26.69% (0.2668724 Gbp	1 Gbps
Physical	Clea...	TenGigabi...	0.03% (0.0028978328 Gbps)	Clea...	TenGigabi...	0.03% (0.0028960628 (	10 Gbps
LAG	Clea...	ASR-9K-...	17.35% (0.34694874 Gbps) 1h	Clea...	ASR920_...	0.04% (0.00077091146	2 Gbps
Physical	Clea...	TenGigabi...	1.1% (0.109563656 Gbps) 1h	Clea...	TenGigabi...	1.24% (0.1243847 Gbps	10 Gbps

- リンク タイプによっては、リンクをクリックし、[アクション（Actions）] ドロップダウン メニューから選択することでアクションを実行します（たとえば、OTS リンクの場合は、[OTDR スキャン（OTDR Scan）] を実行できます）。
- トポロジ マップに特定のリンクを表示するには、**[アクション（Actions）] > [ネットワーク トポロジ（Network Topology）]** をクリックします。

リンクに関する問題のトラブルシューティング

ここでは、リンクを使用する際に発生する可能性がある問題の解決策を紹介します。

リンクの問題	考えられる原因	ソリューション
以前に存在していたリンクがトポロジ マップに表示されなくなった。	エンドポイント デバイスの 1 つでホスト名が変更された可能性があります。	1. ホスト名が変更されたデバイスをシステムから削除して、もう一度追加します。 2. デバイスとそれに接続されているすべてのデバイスを同期して、すべての情報が更新されていることを確認します。

リンクでの帯域幅使用率をマップに表示

トポロジ マップおよび Geo マップでは、回線のプロビジョニングに使用されている光リンク（OTS、OTN、ODU）、パケット リンク（物理、LAG）、およびケーブル リンク（L2TP）での帯域幅使用率の可視化を有効にできます。このようにすると、リンクが過剰使用状態になっていたり、過剰使用状態に近くなっていることを簡単に特定できます。

帯域幅使用率を有効にするには、トポロジ マップまたは Geo マップの右上隅にある [帯域幅使用率（Bandwidth Utilization）] アイコンの横にある矢印をクリックし、[使用率（Utilization）] チェック ボックスをオンにします。物理リンクと LAG リンクの場合は、[使用率（Utilization）] チェック ボックスの横にある矢印をクリックして、リンクの使用率を表示する期間を選択できます。WAE が統合されていない場合、MPLS リンク 360 ビューの MPLS リンク帯域幅使用率の値は使用できません。

帯域幅使用率を有効にすると、太いリンクがマップに表示され、帯域幅使用率のしきい値に基づいて色分けされます。サポートされているリンク タイプでの帯域幅使用率の色分けを確認するには、マップの右上にある [使用率（Utilization）] パネルで [?] アイコンをクリックします。帯域幅使用率の色分けのしきい値は、[管理（Administration）] > [設定（Settings）] > [システム（System）] [設定（Settings）] > [マップ（Maps）] > [帯域幅使用率（Bandwidth Utilization）] で設定できます。リンク帯域幅使用率の色分けしきい値の定義（243 ページ）を参照してください。

帯域幅使用率のデータは、帯域幅使用率の可視化が無効になっている場合も、リンク関連のすべてのビュー（リンクをクリックすると表示される [リンク（Link）] パネルや、[リンク（Links）] テーブル、[リンク 360（Link 360）] など）に表示されます。

帯域幅使用率は、次のように計算されます。

- NCS 2000 デバイス間の OTS リンクの場合、リンク容量は、デバイスで設定可能な光ファイバ属性パラメータから計算されます。OTS リンクが SSON 回線（チャネル番号が「Nyquist」に設定されています）を許可するように設定されている場合は、容量は96チャネルと見なされます。帯域幅使用率は、容量に関連して使用されている 50 GHz ITU チャネルの数という観点から計算されます。SSON 回線の場合、各キャリア NC またはキャリア トレールが実際のサイズに関係なく 1 つの使用中のチャネルとしてカウントされるため、結果は概算です。

  [使用率（Utilization）] 列の [i] アイコンをクリックし、使用されているチャネルと、それらのチャネルを使用している回線の詳細を表示するダイアログを表示します。

（注） ダイアログは 50 GHz ITU の波長/周波数のみを表示するため、SSON キャリア回線は表示されない場合もあります。

- OTN リンクと ODU リンクの場合、帯域幅使用率は予約済みの ODU0 タイムスロットの数に基づいて計算され、1 秒あたりのギガビット数で表示されます。
- 物理リンクおよび LAG リンクの場合、帯域幅使用率はリンク インターフェイスの入力と出力のデータ レートから計算されます。これらのリンク タイプについては、平均使用率またはピーク使用率を表示するかどうかを定義できます。使用率データを表示する期間を 15 分、1 時間、6 時間、または 1 日に指定することもできます。
- ケーブル L2TP リンクの場合、L2TP 使用率は、使用可能な L2TP トンネルについて計算されます。L2TP トンネルが存在する場合、L2TP リンクの使用率は、関連付けられているダウンストリーム コントローラの OFDM チャネル使用率を取得することにより、RPD ごとに計算されます。

（注） パケット リンクおよびケーブル リンクでの使用率を表示するには、インターフェイス ヘルスのモニターリング ポリシーを作成し、関連するデバイスで有効にする必要があります。詳細については、基本的なインターフェイス モニターリングの設定（283 ページ）を参照してください。

リンク帯域幅使用率の色分けしきい値の定義

帯域幅使用率の視覚化を有効にすると、マップ内のリンクはリンク上で現在使用されている総帯域幅のパーセンテージに基づいて色分けされます。リンクでの帯域幅使用率をマップに表示（242 ページ）を参照してください。デフォルトのしきい値はシステムによって定義されますが、独自のしきい値を定義して帯域幅使用率がどのようにリンクに反映されるかを決定することができます。

色分けしきい値を定義するには、次の手順を実行します。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [マップ（Maps）] > [帯域幅使用率（Bandwidth Utilization）]。

ステップ 2 しきい値を定義するリンクのタイプを選択します。

ステップ 3 [リンクの色分けしきい値（Link Coloring Thresholds）] 領域で、リンクを色分けする基準を定義します。各行で、色とその色が表す帯域幅のパーセンテージ範囲を定義します。デフォルトのしきい値は、緑色が 0 ～ 25 %、黄色が 26 ～ 50 %、オレンジ色が 51 ～ 75 %、赤色が 76 ～ 100 % です。

次の点に注意してください。

- 最大 4 個のしきい値を定義できます。
- 最初のしきい値はゼロから始まり、最後のしきい値は 100 で終わる必要があります。
- しきい値は連続している必要があります。つまり、各行の範囲は前の行の範囲の次から始める必要があります。たとえば、行 1 の範囲が 0 ～ 25 % であれば、行 2 の範囲は 26 % で始まる必要があります。

ステップ 4 [保存（Save）] をクリックします。

マップで帯域幅使用率の視覚化を有効にした場合は、これらのしきい値に従ってリンクが色分けされます。

デバイスおよびリンクの障害情報の表示

デバイスまたはリンクにアラームが関連付けられいる場合は、トポロジ マップのデバイス アイコンまたはリンクにアラーム バッジが表示されます。アラーム バッジの色はアラームの重大度に対応してマイナー（黄色）、メジャー（オレンジ）、クリティカル（赤）で表示され、[アラームブラウザ（Alarm Browser）] に表示されるアラームと一致しています。

グループの場合、アラーム バッジは、グループ メンバーに関する現在アクティブな最も重大度の高いアラームを表します。

リンク ダウンなどのリンク関連のアラームは、トポロジマップの関連リンク上にアラームバッジを生成させます。リンク アップ アラームが受信されると、リンク アラームおよび対応するバッジがクリアされます。

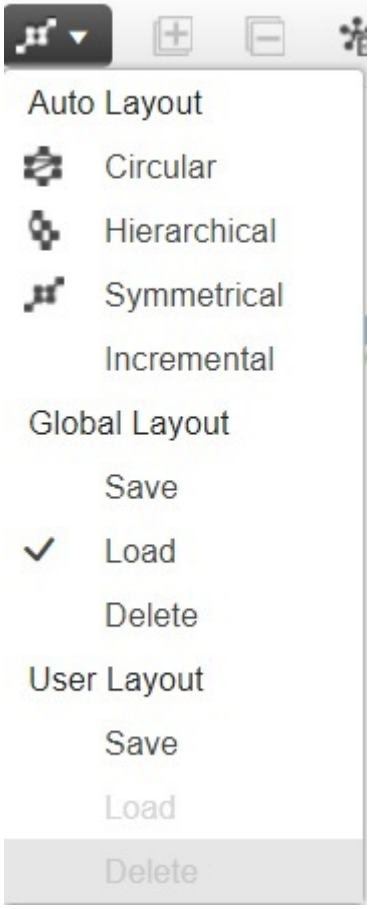
詳細については、アラーム重大度アイコン （318 ページ）を参照してください。

ネットワーク トポロジ マップのレイアウトの変更

トポロジ マップは、初めて開いたときは、デフォルトのグローバル レイアウトに従って表示されます。グローバル レイアウトは、ネットワーク トポロジの「編集」権限を持つユーザーによって変更できます。マップに加えた変更は、現在のブラウザセッションでのみ維持されます。つまり、次にマップを開いたときは、グローバル レイアウトが適用されます。自分のマッ

プ レイアウトを将来のセッションでも維持する場合は、レイアウトを保存できます。保存したレイアウトは、グローバル レイアウトをオーバーライドします。

トポロジ ツールバーの [レイアウト（Layout）] アイコンをクリックし、レイアウト オプションにアクセスします。



- チェックマークは、現在使用されているのはどのレイアウトであるかを示します。たとえば、[グローバルレイアウト（Global Layout）] で [ロード（Load）] の隣にチェックマークがある場合、現在使用されているのはグローバル レイアウトです。

- マップ内でデバイスを移動し、その新しいレイアウトをすべてのユーザーに向けたグローバル レイアウトとして保存する場合は、[グローバルレイアウト（Global Layout）] で [保存（Save）] をクリックします。このオプションは、ネットワーク トポロジの「編集」権限を持つユーザーのみが使用できます。

- マップ内でデバイスを移動し、その自分のレイアウトを次回のブラウザセッションのために保存する場合は、[ユーザーレイアウト（User Layout）] で [保存（Save）] をクリックします。

- グローバル レイアウトが使用されているときに自分の保存したレイアウトを使用する場合は、[ユーザーレイアウト（User Layout）] で [ロード（Load）] をクリックします。

トポロジマップ内にデバイスおよびその他のネットワーク要素（ラベル、ノード、それらの間の接続など）を配置する方法を指定することができます。そうするには、それらをマップ内の必要な位置にドラッグするか、次の事前定義のオプションのいずれかを選択します。

- [対称（Symmetrical）]（デフォルト）：トポロジ固有の対称性を維持します。これによって隣接ノードがさらに接近するので、ノードが重なるのを防ぐことができます。
- [円形（Circular）]：ネットワーク要素を円形に配置し、ネットワーク トポロジ固有のクラスタを強調表示します。
- [階層（Hierarchical）]：依存関係および要素間のフローが維持されるようにします。
- [増分（Incremental）]：特定要素の相対的な位置を維持し、新たに追加された要素の位置を調整します。ノード/リンクを再描画して重なりを解消するには、このレイアウトを使用します。

ネットワーク トポロジへの背景イメージの追加

背景画像は、選択したグループのトポロジマップに適用できます。これは、地理的な場所に応じてネットワークをグループ化する場合などに便利です。サブグループには、親グループとは異なる画像を含めることができます。たとえば、1 つのグループに国マップを適用し、そのサブグループに州マップを適用できます。背景画像は、グループおよびユーザーごとに保存されます。

背景画像が適用されると、ズーム機能を使用できるようになり、ズームインやズームアウトに応じて画像上のデバイスの位置が維持されます。

このシステムでは、背景画像として選択できる事前定義済みの画像がいくつか用意されています。または、独自のカスタム背景画像を使用することができます。

始める前に

カスタム背景画像を追加するときは、次のガイドラインに従います。

- 背景画像ファイルは、高可用性（HA）の対象となるディレクトリ内のサーバーに存在する必要があります。つまり、プライマリ サーバーに障害が発生した場合はセカンダリ サーバーに移動されます。
- 画像は .png 形式または .jpg 形式である必要があります（.png を推奨）。
- マップをレンダリングするのに要する時間は画像のサイズに比例するため、ファイル サイズはできるだけ小さくする必要があります。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [ネットワークトポロジ（Network Topology）] ウィンドウで、トポロジツールバーの [背景画像の追加（**Add Background Image** ）] アイコンをクリックします。[グループ背景画像の管理（Manage Group Background Image）] ダイアログが開きます。

ステップ 3 [グループの選択（Select Group）] ドロップダウンリストから必要なグループを選択します。

ステップ 4 [背景画像（Background Image）] ドロップダウンリストから、[事前定義（**Predefined** ）] または [カスタム画像（**Custom Image** ）] を選択します。

ステップ 5 カスタム画像の場合は、[画像の選択（**Select Image** ）] をクリックし、イメージ ファイルに移動してダブルクリックします。定義済み画像の場合は、表示される画像の 1 つを選択します。

ステップ 6 **Apply** をクリックします。

ステップ 7 トポロジマップで、必要に応じてデバイスを配置します（デバイスはマップ上にランダムに配置されています）。

ステップ 8 **[レイアウト（Layout）]** > **[現在のレイアウトを保存（Save Current Layout）]** を選択して新しいレイアウトを保存します。

回線/VC の可視化とトレース

回線/VC を使用する場合は、既存のネットワーク トポロジ内で回線/VC がどのように展開されているかを確認することが非常に役立ちます。Cisco EPN Manager は、既存のトポロジ マップ上に回線/VC をオーバーレイして、回線/VC のエンドポイントとミッドポイント、エンドポイントのロール（該当する場合）、および回線/VC に関連する障害情報をわかりやすく示します。

トポロジマップのオーバーレイ機能に関する注意事項は次のとおりです。

- トポロジマップで回線をオーバーレイするには、左側の [回線/VC（Circuits/VCs）] タブで回線/VC を選択します。
- 選択したグループに回線/VC に参加しているすべてのデバイスが含まれていない場合は、グループを切り替えてフル オーバーレイを表示するかどうかを確認するポップアップが表示されます。
- 選択した回線/VC に参加しているデバイス以外のすべてのデバイスをマップから削除するには、[参加デバイスのみを表示する（Show Participating Devices Only）] チェックボックスをオンにします。

（注） このオプションは、回線オーバーレイ中にデバイスの上限である 1,500 を超えると強制的にチェックされます。

[参加デバイスのみ表示（Show Participating Only）] オプションを選択し、復元パスに制約リンク/ノードがある場合、マップのネットワークトポロジには、作業パスの一部ではないリンクとノードが表示されます。

- デバイスグループを変更または展開するときに、コンテキストを失うことなく、論理マップ上にデバイスグループをオーバーレイできます。

詳細については、検出/プロビジョニングされた回線/VCの表示と管理（789ページ）を参照してください。

回線のルートの表示

光回線およびCEM回線、MPLS-TE、およびSR-TEサービスの場合は、特定の回線に関連付けられたルートを表示できます。

表示するには、トポロジ ツールバーの [ルート（Routes）] ドロップダウン メニューを使用します。[ルート（Routes）] メニューでは、サービス内のリンクからのルートが計算されます。また、回線ルートに関するその他のデータを確認することもできます。たとえば、リンク上の作業パスは「W」ラベルで表され、保護されたパスには「P」ラベルが付いています。回線に関連付けられているルートの表示 （818 ページ）を参照してください。

光チャネル（OCH）回線の場合は、参加デバイスの [シャーシビュー（Chassis View）] を起動して回線のエンドツーエンドの物理ルートを表示できます。この場合は、物理ルートを表示するOCH回線を選択します。マップで、参加デバイスのいずれかをクリックして[シャーシビュー（Chassis View）] を起動します。

[シャーシビュー（Chassis View）] に回線の物理ルートが表示されます。同じカードのポート間の内部接続は、点線で表示されます。[シャーシビュー（Chassis View）] の目のアイコンを使用して、物理ルート、電力レベル、およびスパン損失を表示または非表示にします。

（注） OCH回線の場合のみ、参加しているデバイスのシャーシビューを起動できます。この機能は、他のタイプの回線またはサービスではサポートされていません。

回線のすべてのルートのトレースと視覚化

[ネットワーク トポロジ（Network Topology）] ウィンドウから回線の完全なマルチレイヤ トレースを実行できます。詳細については、回線/VCの完全なルートをトレースおよび可視化する （860 ページ）を参照してください。

ネットワーク トポロジ マップでのクロック同期ネットワークの表示

同期イーサネット（Sync-E）または Precision Time Protocol（PTP）によるクロック同期がネットワーク内のデバイスに設定されている場合、クロック同期ネットワークをトポロジマップ上に表示できます。

- Sync-E オーバーレイには、プライマリ クロックと、各デバイスのプライマリおよびセカンダリ クロック入力を含め、Sync-E ネットワークのトポロジと階層が表示されます。これにより、任意の Sync-E 対応デバイスからプライマリ クロックまでのクロック信号またはプライマリ クロックから Sync-E 対応デバイスまでのクロック信号をトレースできます。
- PTP オーバーレイには、クロック同期ツリートポロジ、PTP 階層、ツリー上の各デバイスのクロックロール（プライマリ、境界、従属、またはトランスペアレント）が表示されます。

ステップ 1 左側のサイドバーから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 トポロジ ルーツバーで [表示（Show）] をクリックし、[テクノロジー（Technology）] を選択します。各テクノロジーでマップに表示される内容についての説明を表示するには、疑問符アイコンをクリックします。

（注） [テクノロジー（Technology）] を選択する前に、[帯域幅使用率（Bandwidth Utilization）] オプションを無効にする必要があります。

ステップ 4 対象のテクノロジーを選択し、[OK] をクリックします。

クロック同期ネットワークが、マップ内の既存のネットワークの上にオーバーレイとして表示されます。右下の凡例に、選択したテクノロジーのマップで使用されている表記が説明されます。

（注） 別のデバイス グループを選択すると、テクノロジー オーバーレイが削除されます。

トポロジ マップでのルーティング ネットワークの表示

ネットワークで使用されるルーティング プロトコルを、トポロジ マップでオーバーレイとしてグラフィック表示できます。次のルーティング プロトコルのオーバーレイがサポートされています。

- OSPF：
  - OSPF オーバーレイには、ネットワーク内のさまざまな OSPF ドメインと、それらのドメイン間のリンクが表示されます。リンクにはエリア間 OSPF リンクのラベルが付いています。オーバーレイには、各リンクが属する OSPF エリア ID と各ルータのロール（エリア境界ルータ（ABR）や代表ルータ（DR）など）が表示されます。
  - OSPF オーバーレイは、IOS-XE を実行しているデバイス（ASR 90x、ASR 920、および NCS 42xx デバイス）および IOS-XR を実行しているデバイス（ASR 9000、NCS 4000 デバイス）でサポートされます。OSPF オーバーレイは、XR-XE クロスプラットフォーム デバイスでもサポートされています。

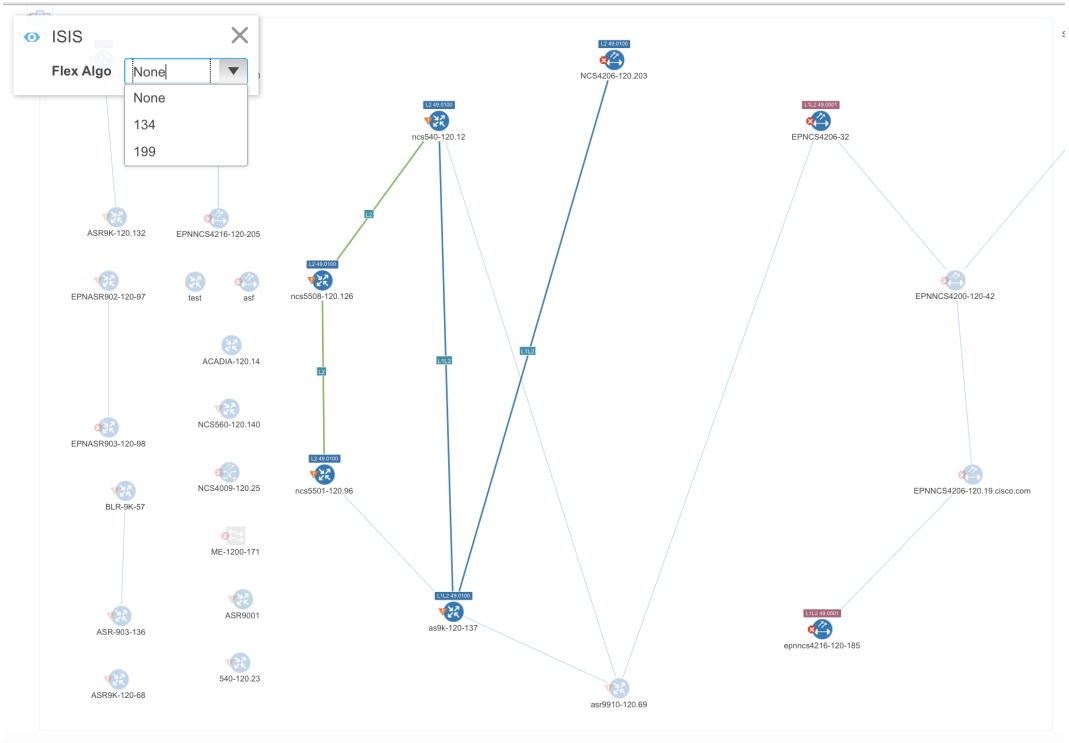
- BGP：
  - BGP オーバーレイは、各デバイスが属する自律システムの ID をデバイスにラベル付けし、自律システム内および自律システム間のリンクを表示します。
  - 接続された 2 台のルータが同じ自律システムに属している場合、リンクは内部 BGP リンクです。異なる自律システムに属している場合は外部リンクとしてマークされます。
  - 一意の自律システムはそれぞれ異なる色で示されるため、同じ AS に属するデバイスを簡単に識別できます。
  - オーバーレイでは、ルート リフレクタまたはルート クライアントとして機能するデバイスもマークされます。
  - BGP オーバーレイは、ASR 920、ASR 901、ASR 901_10G、NCS 42xx、および ASR 9000 デバイスでサポートされています。
- ISIS：
  - ISIS オーバーレイには、内部ゲートウェイ プロトコル（IGP）として ISIS を実行しているデバイス（中継システム - IS）が表示されます。これらのデバイスの上には、IS タイプ、さまざまな ISIS ドメインを識別するエリア ID、およびデバイスが指定中継システム（DIS）かどうかを示す表記が表示されます。表記では、NET アドレスの最初の 6 バイトが示されます。表記にカーソルを合わせると、完全な NET アドレスとプロセス ID を含むツールチップが表示されます。
  - IS タイプは、エリア内ルーティングの場合は L1、エリア間ルーティングの場合は L2、エリア内ルーティングとエリア間ルーティングの両方の場合は L1L2 です。
  - 各 ISIS ドメインは異なる色で表されます。
  - ISIS ネットワーク内のリンク上の表記は、ISIS 隣接関係を示します。複数の隣接関係タイプが存在する集約リンクの場合、複数の隣接関係タイプの表記がリンクに表示されます。
  - [Flex Algo] ドロップダウンリストから値を選択します。値を選択すると、Cisco EPN Manager はオーバーレイを更新し、指定済みの Flex Algo 値で設定されたデバイスのみを反映します。その他のサポートされていないデバイス（Cisco IOS-XE デバイス）および一致しない IOS-XR ノードはグレー表示されます。

（注） デフォルトの ISIS オーバーレイに戻すには、[なし（None）] を選択します。

  - ISIS オーバーレイは、IOS-XE を実行しているデバイス（ASR 903、ASR 907、および NCS 42xx デバイス）および IOS-XR を実行しているデバイス（ASR 9000、NCS 4000 デバイス）でサポートされます。Flex Algo の ISIS オーバーレイは、IOS-XR（ASR 9000、NCS 540、NCS 560、NCS 5500）デバイスでサポートされています。

（注） DIS 表示は、特定の IS レベルのコンテキストではなく、デバイス レベルで表示されます。

マップ内の ISIS オーバーレイの例を次に示します。



マップにテクノロジー オーバーレイを表示する手順は次のとおりです。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 トポロジ ツールバーで [表示（Show）] をクリックし、[リンク（Links）] を選択します。ISIS リンク、BGP リンク、OMS リンクなど、関連するタイプのリンクがマップに表示されていることを確認します。また、帯域幅使用率が有効になっている場合は、無効にします。

ステップ 4 トポロジ ルーツバーで [表示（Show）] をクリックし、[テクノロジー（Technology）] を選択します。各テクノロジーでマップに表示される内容についての説明を表示するには、疑問符アイコンをクリックします。

ステップ 5 必要なルーティング プロトコルを選択し、[OK] をクリックします。

ルーティング ネットワークが、マップ内の既存のネットワーク上にオーバーレイとして表示されます。右下の凡例に、選択したテクノロジーのマップで使用されている表記が説明されます。

（注）　別のデバイス グループを選択すると、テクノロジー オーバーレイが削除されます。

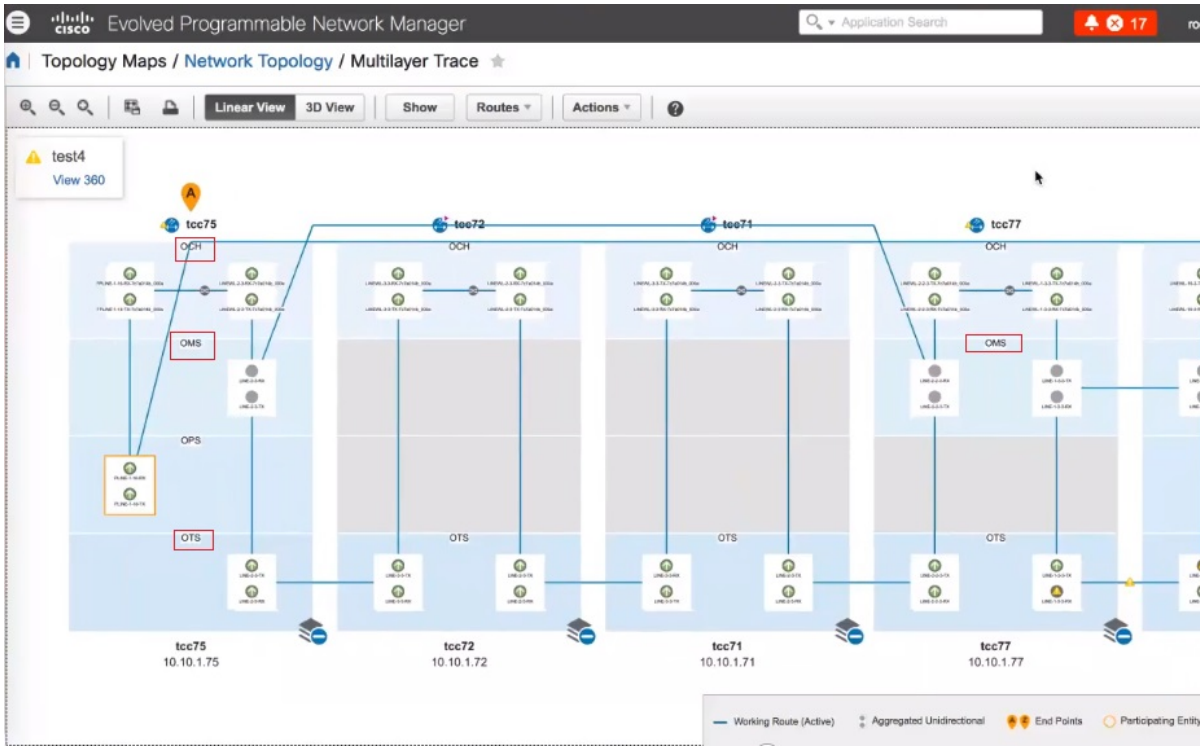
OMS リンクの表示

EPNM で、OTS リンクのシーケンスによって接続されている ROADM デバイスの自動検出 OMS リンクを表示します。OMS リンクのマルチトレース ビュー、[回線/VC 360*（Circuit/VCs 360*）] ビュー、OMS の OMS リンクおよびアラーム リンク層の特性を表示できます。

OMS リンクのマルチトレース ビューを表示する手順は次のとおりです。

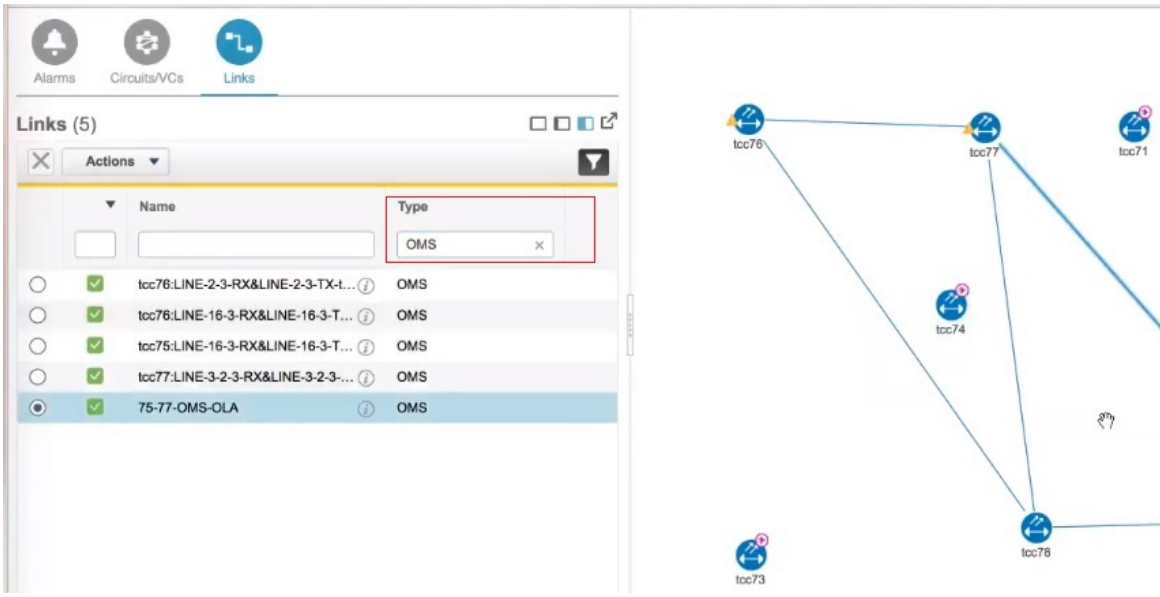
- **[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。
- [回線/VC（Circuits/VCs）] をクリックしてデバイスを選択し、[マルチレイヤトレース（Multilayer Trace）] リンクをクリックして接続されたリンクを表示します。たとえば、次の図には OCH および OPS リンク層だけでなく、OMS リンクのマルチトレース ビューが示されています。

図 *2 : [マルチレイヤトレース（Multilayer Trace）] ビュー*



[タイプ（Type）] フィルタを使用して、OMS リンクとそのネットワークのみを選択して表示します。

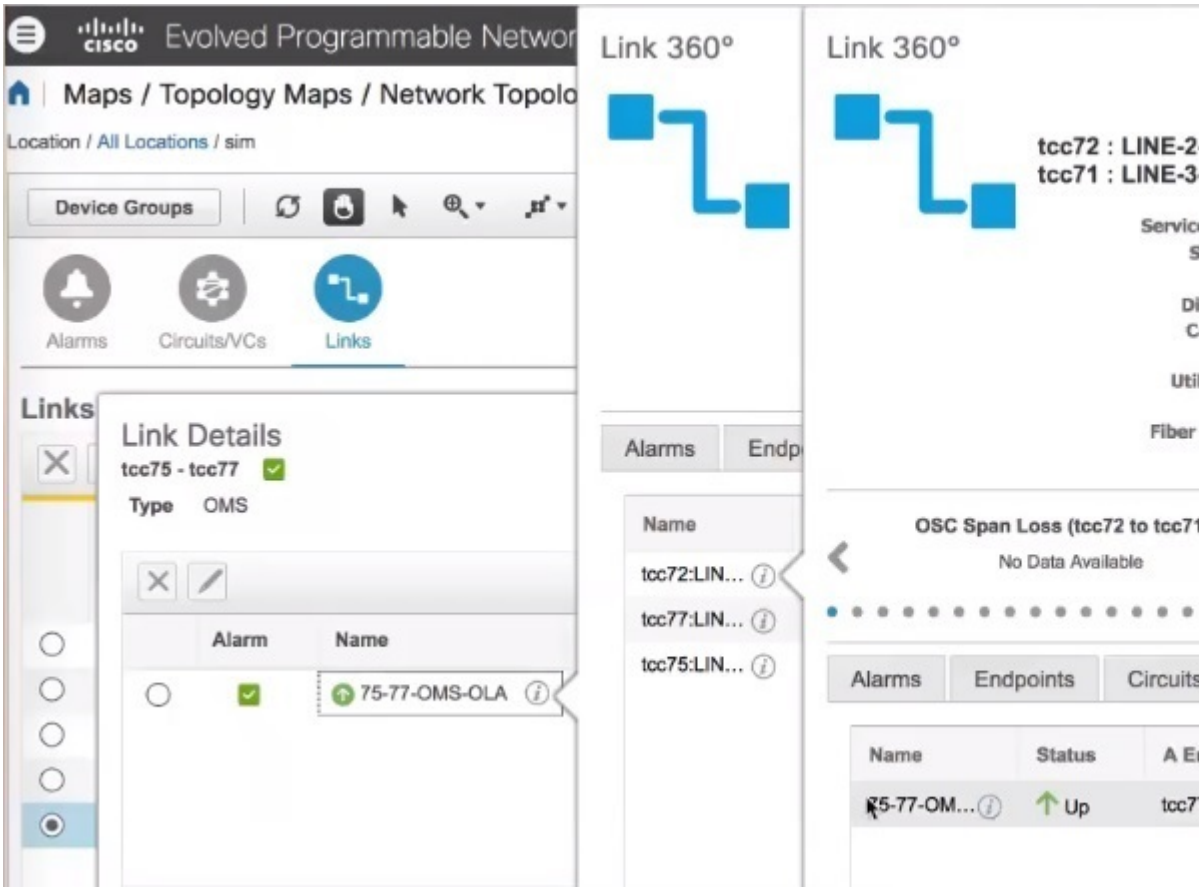
図 *3 : [タイプ（Type）] フィルタで [OMS] を選択する*



OMS リンクの特性を表示する手順は次のとおりです。

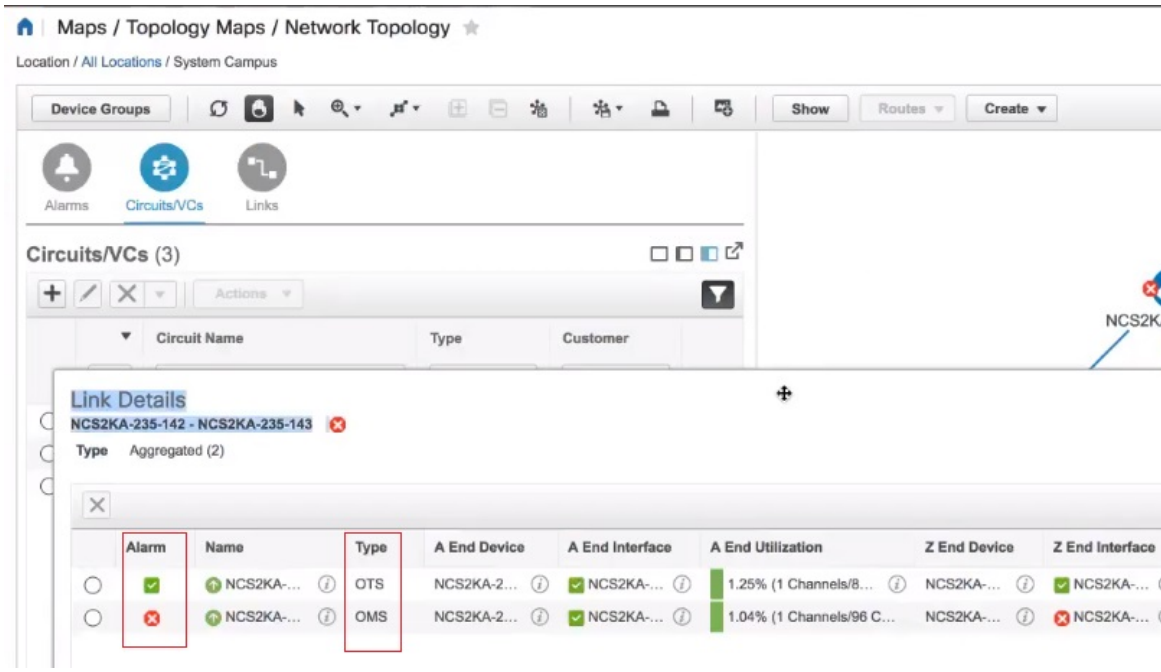
- [表示（Show）] ボタンをクリックし、[リンクの詳細（Link Details）] ダイアログ ボックスに OMS リンクが使用されている場所を表示します。OMS リンク タイプを選択した場合は、エンドポイント、計画されている回線 VC（存在する場合）、および OTS リンクのシーケンスの詳細が表示されます。

図 *4 : [*リンクの詳細（***Link Details***）*]* と *[*リンク *360**（***Link 360****）*]* ビュー



- OTS リンク名の横にある [i] アイコンをクリックして、OMS リンク タイプの [リンク360*（Link 360*）] ビューを表示します。
- OMS リンクのアラーム リンク層を表示します。

図 *5:* アラームを使用した *[*リンクの詳細（***Link Details***）*]*



トポロジマップでのデバイス間の SR パスの特定

トポロジマップで SR がサポートしているデバイス間のアクティブな SR パスを検索するには、次の手順を実行します。

ステップ 1 SR パスを検索する SR サポート対象デバイスをクリックします。ポップアップが開き、デバイスの基本情報とアラーム情報が表示されます。

ステップ 2 **Show SR Path** をクリックします。[SR パスの表示（Show SR Path）] ダイアログが開きます。

ステップ 3 エンドポイントを選択するには、SR パスを検出する SR サポート対象デバイスをクリックします。[エンドポイント（Endpoint）] フィールドに、選択したデバイスの詳細が入力されます。

（注） 選択したデバイスがセグメント化されたルーティングをサポートしていない場合は、エラーメッセージが表示されます。

また、フィールドにデバイス名を入力するか、またはドロップダウンリストから選択することによっても、デバイスを選択できます。

ステップ 4 **OK** をクリックします。選択したデバイスのトポロジマップで SR パスが強調表示されます。

イメージ ファイルとしてトポロジ マップを保存する

トポロジ マップ全体、またはトポロジ マップから選択したオブジェクトをイメージ ファイルとして保存できます。これにより、特定の状態にあるトポロジマップのコピーを保存できるので、将来、トポロジに対して複数の変更を行う際にそれを基準として使用できます。

イメージ ファイルとしてトポロジ マップを保存するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 必要に応じて、トポロジ マップの内容やレイアウトを変更します。

ステップ 4 トポロジ ツールバーの [イメージの保存（Save Image）] アイコンをクリックします。

ステップ 5 [イメージの保存（Save Image）] ドロップダウンリストから、保存するイメージのファイルタイプを選択します。

ローカルの Temp フォルダにイメージが保存されます。

地理的マップ（Geo マップ）でのネットワークの表示

Geo マップの概要

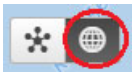
Geoマップを使用すると、ネットワークデバイスを世界地図上に配置し、それらの地理的コンテキスト内でモニターすることができます。世界地図は、インターネットを介してマッププロバイダにアクセスしてインポートするか（オンラインモード）、またはローカルにインストールされているマップ リソースから（オフライン モード）表示されます。

（注） オンライン モードで Geo マップを使用して作業する場合は、各クライアントからか、または Cisco EPN Manager サーバーがプロキシとして使用されている場合はそのサーバーからインターネットへの接続が必要です。

Geoマップにはトポロジマップを介してアクセスします。Geoマップを開くには、次の手順を実行します。

ステップ 1 左側のサイドバーで、**[マップ（Maps）] > [トポロジマップ（Topology Maps）] > [ネットワークトポロジ（Network Topology）]** を選択します。

ステップ 2 マップの右上にある [地理的マップ（Geographical Map）] トグル ボタンをクリックします。



Geo マップの概要：

- マップの右上の隅にあるトグル ボタンを使用して、トポロジ マップと Geo マップを相互に切り替えることができます。
- Geoマップには、GPS座標が定義されているデバイスが表示されます。GPS座標を持たないデバイスはGeoマップに表示されず、また、「マップされていないデバイス」と呼ばれます。Geo マップへのマップされていないデバイスの配置 （260 ページ）を参照してください。
- Geoマップ内のデバイスをクリックすると、アラーム、基本情報、ロケーション座標、シビック ロケーション（デバイスに定義されている場合）を確認できます。
- GPS ロケーション設定をサポートする光デバイス（NCS 2000 デバイス）の場合、Geo マップのデバイスのロケーションに加える変更はデバイスと同期され、デバイスに加えられた変更はGeoマップのデバイスのロケーションと同期されます（デバイス自体に加えられたロケーションの変更が Geo マップに反映されます）。
- GPS 座標は DMM 形式（度数と 10 進数の分数）で表示されますが、ユーザーは DMM、DD（10 進数の度数）、または DMS（度数、分数、秒数）の形式で GPS 座標を定義できます。
- Geoマップ上にデバイスが存在しない場合は、世界地図全体が表示されます。特定の領域にデバイスが存在する場合は、世界のその領域のみが表示されます。Geoマップには、世界地図のうちデバイスが含まれている部分のみが表示されます。

- トポロジ マップの場合と同様に、Geo マップには、選択したデバイス グループのデバイスが表示されます。デバイス グループの選択は、あるマップでの選択を変更すると別のマップも変更されるように、トポロジ マップと Geo マップ間で同期されます。
- 選択したデバイス グループ内の定義された地理的位置を持つデバイス グループがある場合、そのグループはデバイス グループ アイコンで Geo マップに表示されます。デバイス グループに地理的位置がない場合、そのグループに含まれているデバイスはGeoマップに個別に表示されます。詳細については、Geoマップのデバイス グループ （258ページ） を参照してください。
- Geoマップは、クラスタ内で相互に地理的に近接するグループをグループ化し、クラスタ内のデバイス数を表す数が示されたクラスタ アイコンで表示されます。個々のデバイスを表示するには、拡大します。クラスタのメンバーの特定 （263ページ） を参照してください。
- トポロジ マップと同様に、Geo マップに回線/VC を表示できます。ただし、回線/VC の作成や、回線/VC の変更のようなプロビジョニング アクションを開始すると、ビューはトポロジ マップに切り替わります。

Geo マップのデバイス グループ

Geoマップには、個々のデバイスに加えて、特定の住所にある建物内のデバイスなど、定義された場所を持つデバイス グループが表示されます。

Geo マップでグループを表示するときは、次の点を考慮してください。

- Geoマップに表示できるのは、ロケーションタイプのデバイス グループだけで、定義された地理的位置がある場合にのみ表示されます。ロケーションは、デバイス グループのプロパティで定義されます。ロケーション デバイス グループを作成または編集し、グループの地理的位置を定義するには、[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）] に移動します。詳細については、ロケーション グループの作成 （99ページ） を参照してください。
- グループ メンバーはグループのロケーションを継承します。
- グループのロケーションが他のデバイスまたはグループと同じ場合、そのロケーションはクラスタに含まれます。クラスタ アイコンに表示される数字は、クラスタ内のデバイスの合計数（グループに含まれるデバイスを含む）を表します。
- グループ内のいずれかのデバイスにアラームがある場合、最も重大度の高いアラーム アイコンがデバイス グループ アイコンに表示されます。
- ロケーション グループ アイコンをクリックすると、グループに関する情報（名前、GPS 座標、アラーム情報など）を含むパネルが表示されます。グループのシビック ロケーション情報を定義すると、このパネルにも表示されます。パネルの [メンバーを表示（Show Members）] リンクをクリックすると、そのグループに属するデバイスとサブグループのリストが表示されます。または、ロケーション グループ アイコンをダブルクリックすると、同じ結果を得られます。
- グループ メンバー デバイスに地理的な位置が指定されている場合、そのデバイスは Geo マップ上に個々のデバイスとして表示され、アラームはグループではなくデバイス自体に

表示されます。グループのロケーションの重要性を保持するために、地理的位置グループ内のすべてのデバイスが、そのグループの GPS 座標を継承することが推奨されます。

Geoマップの設定

このシステムは、クライアントからの直接インターネット接続を介して、またはプロキシとして機能する EPN Manager サーバー経由で、マップ タイルを特定の Mapbox URL から取得するようにデフォルトで設定されています。必要に応じて、特定の URL を指定して別のマップ タイル プロバイダを使用できます。どちらのオプションもインターネット接続が必要です。インターネットに接続していない場合は、マップ リソースをローカルにインストールし、システムがローカル マップ リソースを使用するよう指定することで、オフライン モードで効果的に作業できます。

Geo マップの設定は、[システム設定（System Settings）] で管理できます。左側のナビゲーション ウィンドウで、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[マップ（Maps）]** > **[ネットワークトポロジ（Network Topology）]** を選択します。

[ネットワークトポロジ（Network Topology）] ページでは、次の操作を実行できます。

- Geo マップの有効化または無効化。デフォルトでは、Geo マップが有効になっています。つまり、すべてのクライアントに Geo マップ機能があります。[**Enable geo map**] チェックボックスをオフにして、機能を無効にできます。
- マップ タイルのソースの特定（インターネット接続を使用）。デフォルトのマップ タイル プロバイダは Mapbox です。別のマップ タイル プロバイダを使用している場合は、マップ タイル アクセスの URL を指定する必要があります。この URL の正確な形式は、マップ タイル プロバイダからリクエストしてください。[マッププロバイダ（Map Provider）] ドロップダウンリストで [カスタム（Custom）] を選択し、URL を入力します。Geo マップ機能は、Mapbox 以外のプロバイダからのマップ タイルではテストされていないことに注意してください。
- Cisco EPN Manager サーバーをインターネットにアクセスしてマップ タイルを取得するためのプロキシにする。セキュリティ上の理由から、各クライアントから直接インターネットにアクセスしたくない場合があります。[**Via management application proxy**] チェックボックスを有効にすると、マップ プロバイダの URL へのインターネット アクセスは、クライアント経由で直接行うのではなく、Cisco EPN Manager サーバー経由で行われます。
- インターネットに接続する必要のないインストールされたマップ リソースを使用して、Geo マップを表示するように指定する。[マッププロバイダ（Map Provider）] ドロップダウンリストで [インストール済みマップリソース（Installed Map Resources）] を選択します。マップ リソースをインストールする方法については、『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください。

Geo マップに表示されないデバイス（マップされていないデバイス）の特定

任意の選択したデバイス グループ地理地図 GPS 座標で定義されているデバイスのみに自動的に表示されます。地質地図、または別のデバイス グループを選択するときに切り替えた、ポップアップ メッセージが表示され、そこにどのように多くのマップされていないデバイスは、どのように多くのデバイス座標を持っていない、したがって、マップには表示されませんを意味表示されます。

Geo マップに表示されていないデバイスを特定するには、マップ上にある [**Unmapped Devices**] ボタンをクリックします。

Geo マップへのマップされていないデバイスの配置

マップされていないデバイスを Geo マップ上の目的の位置にドラッグ アンド ドロップするか、または GPS 座標を指定して Geo マップ上でのデバイスの位置を定義できます。

GPS 座標は、次のいずれかの形式で指定できます。

- 度と 10 進数の分（DMM）：41 24.2028、2 10.4418
- 10 進数の度（DD）：41.40338、2.17403
- 度、分、および秒（DMS）：41°24'12.2""N 2°10'26.5""E

（注） DMS 形式を使用する場合は、二重引用符（""）を使用して秒を示してください。

マップされていないデバイスを Geo マップ上に配置するには、次の手順を実行します。

ステップ 1 左側のサイドバーで、**[マップ（Maps）]** > **[トポロジマップ（Topology Maps）]** > **[ネットワークトポロジ（Network Topology）]** を選択します。

ステップ 2 マップの右上にある [地理的マップ（Geographical Map）] トグル ボタンをクリックします。

ステップ 3 マップの上にある [マップされていないデバイス（Unmapped Devices）] ボタンをクリックします。

ステップ 4 右側の [マップされていないデバイス（Unmapped Devices）] パネルで、次のいずれかを実行します。

a) マップ上にデバイスをドラッグ アンド ドロップするか、または複数のデバイスを選択してマップ上にドラッグ アンド ドロップします。

b) マップ上に配置するデバイスを選択し、**Set Location** をクリックします。表示されたダイアログで、GPS 座標を指定します（例：緯度 59.623325、経度 103.535156）。**Place Device** をクリックします。

（注） 複数のデバイスを選択すると、それらのデバイスは 1 つのクラスタに統合されてマップ上の同じ位置に配置されます。クラスタ アイコンにはクラスタに含まれているデバイスの数が表示されます。

Geo マップでのデバイスのロケーションの変更

Geo マップ上の別のロケーションにデバイスを異動するには、[ロケーションの編集（Edit Location）] ダイアログを開き、マップ上の必要なロケーションにデバイスをドラッグするか、または座標を手動で設定する必要があります。デバイスがクラスタ内にある場合は、クラスタを開いてデバイスを表示してから、そのデバイスのロケーションを変更する必要があります。

GPS 座標は、次のいずれかの形式で指定できます。

- 度と 10 進数の分（DMM）：41 24.2028、2 10.4418
- 10 進数の度（DD）：41.40338、2.17403
- 度、分、および秒（DMS）：41°24'12.2""N 2°10'26.5""E

（注） DMS 形式を使用する場合は、二重引用符（""）を使用して秒を示してください。

デバイスのロケーションを変更するには、次の手順を実行します。

ステップ 1 Geo マップ上のデバイスをクリックします。ポップアップが開き、デバイスの基本情報とアラーム情報が表示されます。

ステップ 2 **Actions** ドロップダウンリストから **Edit Location** を選択します。[ロケーションの編集（Edit Location）] が開きます。

ステップ 3 必要なロケーションにデバイスをドラッグするか、必要に応じて GPS 座標を変更します。

ステップ 4 **Save** をクリックします。

クラスタでのデバイスのロケーションの変更

互いに近接するデバイスは Geo マップのクラスタ内にグループ化されます。クラスタ内の 1 つ以上のデバイスのロケーションを変更できます。デバイスはクラスタから削除され、個別のデバイスとして Geo マップに表示されます。

クラスタ内のデバイスのロケーションを変更するには、次の手順を実行します。

ステップ 1 Geo マップのクラスタをクリックします。クラスタの基本情報が示されたポップアップが表示されます。

ステップ 2 [デバイスの表示（Show Devices）] をクリックします。マップの右側にパネルが表示され、クラスタ内のすべてのデバイスのリストが表示されます。

ステップ 3 右側のパネルで、次のいずれかを実行します。

a) マップ上にデバイスをドラッグ アンド ドロップするか、または複数のデバイスを選択してマップ上にドラッグ アンド ドロップします。

b) マップ上に配置するデバイスを選択し、**Set Location** をクリックします。表示されたダイアログで、GPS 座標を指定します（例：緯度 59.623325、経度 103.535156）。**Place Device** をクリックします。

デバイスがクラスタから削除され、マップ上の指定されたロケーションに配置されます。

Geo マップからのデバイスの削除

Geoマップにデバイスを表示する必要がなくなった場合は、そのデバイスを削除できます。削除したデバイスは [マップされていないデバイス（Unmapped Devices）] リストに表示されます。

Geo マップからのデバイスを削除するには、次の手順を実行します。

ステップ 1 Geo マップ上のデバイスをクリックします。ポップアップが開き、デバイスの基本情報とアラーム情報が表示されます。

ステップ 2 **Actions** ドロップダウンリストから **Edit Location** を選択します。[ロケーションの編集（Edit Location）] が開きます。

ステップ 3 [ロケーションの編集（Edit Location）] ダイアログで、[**Remove Location**] をクリックします。

Geo マップからのクラスタ デバイスの削除

クラスタ内のデバイスを Geo マップから削除できます。個々のクラスタ デバイスを削除することも、同じクラスタ内の複数のデバイスを一度に削除することも可能です。削除したデバイスは [マップされていないデバイス（Unmapped Devices）] リストに表示されます。

Geo マップからクラスタ デバイスを削除する手順は次のとおりです。

ステップ 1 削除するデバイスを含むクラスタをクリックします。ポップアップが開き、デバイスの基本情報とアラーム情報が表示されます。

ステップ 2 **Show Devices** をクリックします。クラスタに含まれるデバイスの一覧が表示されます。

ステップ 3 削除するデバイスを選択します。

ステップ 4 **Set Location** をクリックします。

ステップ 5 表示されるダイアログ ボックスで [**Remove Location**] をクリックします

ステップ 6 デバイスが [マップされていないデバイス（Unmapped Devices）] リストに移動されることを知らせる警告メッセージが表示されたら、[はい（Yes）] をクリックします。

クラスタのメンバーの特定

クラスタは、マップ上で2つ以上のデバイス グループが相互に近接している場合に形成されます。クラスタはGeoマップ上に円で示され、中心部分にはそのクラスタ内に存在するデバイスの数（個々のデバイスもグループ内のデバイスも含む）を示す数字が表示されます。拡大すると、マップ上に個々のクラスタ メンバーが表示されます。

（注） クラスタ メンバーが相互に近接している（約8メートル以内の距離にある）場合、拡大しても個々のデバイスおよびグループは表示されません。クラスタ内の個々のメンバーを表示するには、次の手順を実行してください。

クラスタ内のデバイスおよびグループの一覧を表示する手順は次のとおりです。

ステップ 1 クラスタ アイコンをクリックします。

ステップ 2 表示されたポップアップで、[**Show Members**] をクリックします。クラスタに含まれているデバイスまたはデバイス グループがマップ右側のパネルに表示されます。クラスタにグループが含まれている場合は、ドリルダウンしてグループ内のデバイスを表示できます。前のリストに戻るには、ダイアログの上部にあるナビゲーション リンクを使用します。

ステップ 3 デバイスのロケーションを変更するには、そのデバイスをリストからマップ上にドラッグするか、[**Set Manually**] をクリックして新しい座標を指定します。

Geo マップでの特定のロケーションの検索

Geoマップで特定のロケーション（都道府県、国、市区町村、特定の住所など）を検索できます。検索ボックスにキーワードを入力すると、そのキーワードを含むすべてのロケーションが番地レベルで結果に表示されます。検索結果で目的のロケーションを選択して、マップ内で特定できます。

（注） このロケーション検索を実行するには、インターネット接続が必要です。

Geo マップで特定のロケーションを検索する手順は次のとおりです。

ステップ 1 ツールバーの [検索（Search）] アイコンをクリックします。

ステップ 2 検索キーワードの全部または一部を検索テキスト ボックスに入力し、Enter を押します。

検索結果パネルの [住所（Address）] タブに、検索に一致するロケーションが一覧表示されます。

ステップ 3 検索結果でロケーションを選択します。
指定したロケーションがマップによってパンおよびズームされ、マップ上のマーカーが正確な位置を示します。

Geo マップのロケーション フィルタ

Geo マップのロケーション フィルタを使用する手順は次のとおりです。

ステップ 1 **[マップ（Map）] > [トポロジマップ（Topology Maps）] > [ネットワークトポロジ（Network Topology）]** に移動し、[表示（Show）] ボタンをクリックして [ロケーション（Location）] を選択します。

ステップ 2 [ロケーション（Location）] ポップアップ ウィンドウで、[フィルタを有効にする（Enable Filter）] オプションをオンにします。次のいずれかのフィールドの値を指定します。

- [シビックロケーション（Civic Location）]：任意のシビック ロケーション（デバイスのロケーションとは関係ない）
- [緯度/経度（Latitude/Longitude）]：ロケーション座標（マップをクリックして値を自動的に入力することもできます）
- [デバイス名によるロケーション（Location by Device name）]：デバイスの名前（Geo マップに現在表示されているデバイスの一覧から）

ステップ 3 [半径（radius）] の値を指定すると、指定した検索領域内のすべてのデバイスが表示されます。

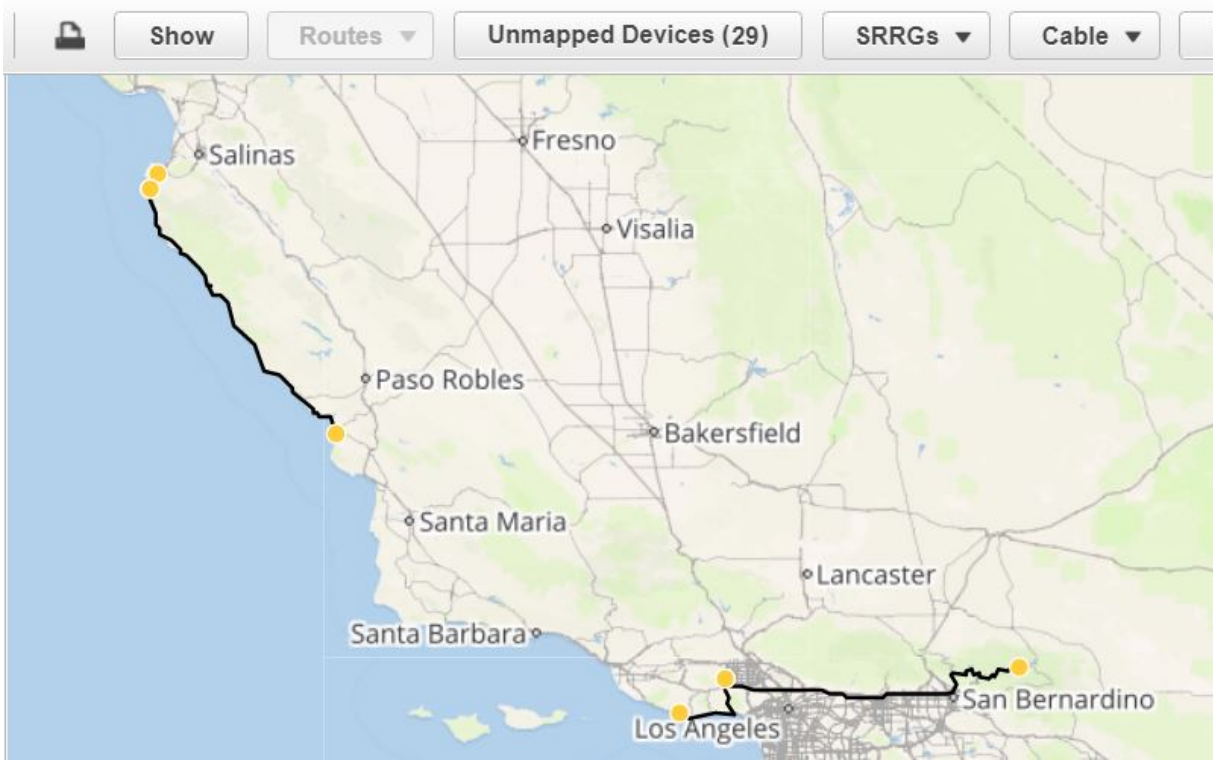
ステップ 4 完了したら、[保存（Save）] をクリックします。

Geo マップでの光ファイバ パスの表示と管理

Geo マップで光ファイバを表示するには、光ファイバのロケーション データを含む KML ファイルを作成して Cisco EPN Manager にインポートする必要があります。光ファイバのロケーション データのインポートについては、KML ファイルからのロケーション データのインポート（268 ページ）を参照してください。

光ファイバのロケーション データを含む KML ファイルをインポートすると、Geo マップに光ファイバが表示されます。マップ上に表示されないようにする場合は、**[表示（Show）] > [リンク（Links）]** に移動し、物理層リンクで [ファイバ（Fiber）] をオフにします。

光ファイバは、Geo マップで次のように表示されます。



光ファイバを編集/削除する方法と光ファイバをリンクに関連付ける方法については、光ファイバ パスの管理（265 ページ）および光ファイバへのリンクの関連付け（266 ページ）を参照してください。

光ファイバ パスの管理

Geo マップに表示される光ファイバ パスは、[ファイバ管理（Fiber Management）] ダイアログ ボックスで編集、削除したり、リンクに関連付けたりすることができます。Geo マップ ツールバーの [ファイバ（Fibers）] ボタンをクリックすると、[ファイバ管理（Fiber Management）] ダイアログ ボックスが開きます。

次の点に注意してください。

- [ファイバ管理（Fiber Management）] ダイアログには、マップに現在表示されている光ファイバのみが一覧表示されます。Geo マップに表示できない光ファイバは、[ファイバ管理（Fiber Management）] ダイアログに表示されません。管理する光ファイバが表示されるように Geo マップを設定してください。
- [ファイバ管理（Fiber Management）] ダイアログで光ファイバを選択すると、選択した光ファイバが Geo マップで紫色でハイライト表示されます。光ファイバがリンクに関連付けられている場合、リンクもマップで紫色でハイライト表示されます。Geo マップで光ファイバをクリックすると、その光ファイバが [ファイバ管理（Fiber Management）] ダイアログで選択されます。
- 特定の光ファイバに関する追加の詳細情報を表示するには、光ファイバ名の横にある矢印をクリックして光ファイバの説明を表示します。

- 光ファイバ名、長さ（km 単位）、および説明を編集できます。光ファイバを編集するには、光ファイバを選択して [編集（Edit）] ボタンをクリックします。編集が完了したら、[保存（Save）] をクリックします。
- 光ファイバを削除するには、目的の光ファイバを選択して [削除（Delete）] ボタンをクリックします。
- [関連付けられたリンク（Associated Link）] 列には、光ファイバが関連付けられているリンクが表示されます（存在する場合）。光ファイバを選択し、テーブル上にある [ファイバとリンクの関連付けを削除] アイコンをクリックすれば、必要に応じてリンクの関連付けを解除できます。詳細については、光ファイバへのリンクの関連付け （266 ページ） を参照してください。

光ファイバへのリンクの関連付け

光ファイバを OTN または OTS リンクに関連付けて、光ファイバと関連リンクの両方をマップ上で可視化できます。光ファイバをリンクに関連付けるには、必要な情報を KML ファイルに入力してシステムにインポートする必要があります。

光ファイバとリンクの関連付けを指定する形式を説明した KML テンプレートをダウンロードして、必要な情報を追加してからインポートできます。

リンクを光ファイバに関連付ける手順は次のとおりです。

ステップ 1 正しい KML 形式および光ファイバとリンクの関連付け手順を含む KML テンプレートをダウンロードします。

- Geo マップ ツールバーの [インポート（Import）] アイコンをクリックし、[KML] を選択します。
- 表示されたダイアログの下部にあるリンクをクリックして、KML テンプレートをダウンロードします。
- KML ファイルで、「リンクの関連付け情報（Links association info）」というフォルダを見つけます。このフォルダには、光ファイバとリンクの関連付けを作成するための形式と手順が含まれています。

ステップ 2 KML ファイルに必要な情報を入力して保存し、システムにインポートします。KML ファイルからのロケーション データのインポート （268 ページ） を参照してください。

ステップ 3 Geo マップに光ファイバが表示されていることを確認し、ツールバーの [ファイバ（Fibers）] をクリックします。[ファイバ管理（Fiber Management）] ダイアログの [関連付けられたリンク（Associated Link）] 列にリンクが表示されます。光ファイバを選択し、テーブル上にある [ファイバとリンクの関連付けを削除] アイコンをクリックすれば、リンクの関連付けを削除できます。

Geo マップでの回路/VC の可視化

Geo マップの回線/VC オーバーレイ機能は、トポロジマップのオーバーレイと非常によく似ています。ただし、マップの機能にいくつかの違いがあるため、Geo マップのオーバーレイ機能に関するいくつかの項目には注意が必要です。

- Geo マップで回線をオーバーレイするには、トポロジ マップの場合と同様に、左側の [回線/VC（Circuits/VCs）] タブで回線/VC を選択します。
- 選択した回線/VC に参加しているデバイス以外のすべてのデバイスをマップから削除するには、[参加デバイスのみを表示する（Show Participating Devices Only）] チェック ボックスをオンにします。
- [参加デバイス（Participating Devices）] リンクをクリックすると、回線/VC に参加しているすべてのデバイスの一覧が表示されます。この一覧にはデバイスのロール（A 側や Z 側など）が表示され、デバイスのロケーションを変更したり、マップからデバイスを削除したりできます。
- 参加デバイスが Geo マップ上のクラスタ内にある場合、デバイスのロールを示すバッジがクラスタ アイコンに表示されます。個々のデバイスを拡大表示すれば、ロール バッジが指しているデバイスを正確に確認できます。または、[参加デバイス（Participating Devices）] リンクをクリックして、回線/VC 内のすべてのデバイスとそのロールを確認してください。
- 一部の参加デバイスがマップに現在表示されていない場合は、メッセージが表示され、マッピングされていないデバイスの一覧を開くことができます。マップ上にデバイスを配置するには、デバイスをドラッグ アンド ドロップするか、[ロケーションの設定（Set Location）] をクリックして GPS 座標を入力します。

Geo マップでのデバイス間の SR パスの特定

Geo マップ上のデバイス間のアクティブな SR パスを検索するには、次の手順を実行します。

ステップ 1 SR パスを検索する SR サポート対象デバイスをクリックします。ポップアップが開き、デバイスの基本情報とアラーム情報が表示されます。

ステップ 2 **Actions** ドロップダウンリストから **Show SR Path** を選択します。[SR パスの表示（Show SR Path）] ダイアログが開きます。

ステップ 3 エンドポイントを選択するには、SR パスを検出する SR サポート対象デバイスをクリックします。[エンドポイント（Endpoint）] フィールドに、選択したデバイスの詳細が入力されます。

（注） 選択したデバイスがセグメント化されたルーティングをサポートしていない場合は、エラーメッセージが表示されます。

また、フィールドにデバイス名を入力するか、またはドロップダウンリストから選択することによっても、デバイスを選択できます。

ステップ 4 **OK** をクリックします。選択したデバイスの Geo マップで SR パスが強調表示されます。

ロケーション データのインポート

Geo マップにデバイスを手動で配置する以外にも、デバイスまたは光ファイバの座標を外部ファイルで指定してインポートすることもできます。システムはファイルから座標を読み取り、デバイス/光ファイバをマップ上に配置します。これは、マップ上にアイテムを一括で配置したり、別のシステムからロケーションデータを転送したりする場合に便利です。Geoマップから既存のロケーションをエクスポートし、変更を加えたデータをシステムにインポートし直すこともできます。

デバイスおよび光ファイバパスのロケーション、KML ファイルから手動で作成した管理対象リンクをインポートできます。

KMLファイル形式の場合は、システムが読み取れる形式で情報を入力するテンプレートをGUIからダウンロードできます。テンプレートをダウンロードするには、ジオマップ上の [ロケーションのインポート（Import Locations）] アイコンをクリックし、テンプレートリンクをクリックします。

詳細については、KML ファイルからのロケーション データのインポート （268 ページ）を参照してください。

KML ファイルからのロケーション データのインポート

KML（Keyhole Markup Language）は、2 次元もしくは 3 次元のマップ、または Google Earth のような Earth ブラウザで地理データの表示に使用されるファイル形式です。KML は XML 標準に基づいており、要素と属性が入れ子になったタグベースの構造を使用します。デバイスと光ファイバパスのロケーション データを含むKML ファイルを作成してインポートし、Geo マップにデバイスと光ファイバを配置できます。KML ファイルには、次のロケーション データを含めることができます。

- デバイスのロケーション データ
- 光ファイバのロケーション データ
- 光ファイバとリンクの関連付け
- 手動で作成した管理対象リンク。インポートした管理対象リンクは、トポロジ マップとGeoマップに表示されます（管理対象リンクの両方のエンドポイントがGeoマップに「マッピング」されている場合）。

KMLファイル内に情報を入力する際に必要な形式を示したテンプレートが用意されています。

（注） 座標は 10 進数（DD）形式（例：41.40338、2.17403）で入力する必要があります。

次にデバイス ロケーションの KML 形式の例を示します。

```
<Placemark>
 <name>454A-234-157</name>
 <Point>
  <coordinates> -121.930938,37.411522</coordinates>
 </Point>
```

```
 <ExtendedData>
  <Data namename="nodeIpAddress">
   <value>10.56.23.47</value>
  </Data>
 </ExtendedData>
</Placemark>
```

次に光ファイバ パスの KML 形式の例を示します。

```
<Placemark>
 <name>Fiber-1</name>
 <description>Fiber-1 long description</description>
 <LineString>
  <coordinates> -121.930938,37.411522,0.0 -121.931405,37.413011,0.0
-121.929364,37.413588,0.0 -121.930973,37.414602,0.0
  </coordinates>
 <LineString>
</Placemark>
```

次の例に示す光ファイバとリンクの関連付けの KML 形式では、以下の必須事項に注意してください。

- 各フォルダに「linkAssociation」という名前でリンクの関連付けを 1 つ定義する。
- 関連付けるリンクの A から Z へのパスに続くシーケンス内に光ファイバのセグメントを指定する。
- 関連付けるリンクの A 側と Z 側の IP アドレスを指定する。

```
<Folder>
 <name>Links association info</name>
  <Folder>
   <name>linksAssociation</name>
   <description>OTS link-1</description>
   <ExtendedData>
    <Data> name="segments">
     <value>Fiber-1,Fiber-1-to-2-segment,Fiber-2</value>
    </Data>
    <Data> name="nodeAIpAddress">
     <value>10.56.23.47</value>
    </Data>
    <Data> name="nodeZIpAddress">
     <value>2001:cdba:0000:0000:0000:0000:3257:9652</value>
    </Data>
    <Data> name="nodeAInterfaceName">
     <value>LINE-2-17-3-TX</value>
    </Data>
    <Data> name="nodeZInterfaceName">
     <value>LINE-1-1-3-TX</value>
    </Data>
    <Data> name="linktype">
     <value>OTS</value>
    </Data>
   </ExtendedData>
  </Folder>
</Folder>
```

次の例に示す光ファイバとリンクの関連付けの KML 形式では、以下の必須事項に注意してください。

- 各フォルダに「linkAssociation」という名前でリンクの関連付けを 1 つ定義する。
- 関連付けるリンクの A から Z へのパスに続くシーケンス内に光ファイバのセグメントを指定する。
- 関連付けるリンクの A 側と Z 側の IP アドレスを指定する。

```
<Folder>
 <name>Links association info</name>
  <Folder>
   <name>linksAssociation</name>
   <description>OTS link-1</description>
   <ExtendedData>
    <Data> name="segments">
     <value>Fiber-1,Fiber-1-to-2-segment,Fiber-2</value>
    </Data>
    <Data> name="nodeAIpAddress">
     <value>10.56.23.47</value>
    </Data>
    <Data> name="nodeZIpAddress">
     <value>2001:cdba:0000:0000:0000:0000:3257:9652</value>
    </Data>
    <Data> name="nodeAInterfaceName">
     <value>LINE-2-17-3-TX</value>
    </Data>
    <Data> name="nodeZInterfaceName">
     <value>LINE-1-1-3-TX</value>
    </Data>
    <Data> name="linktype">
     <value>OTS</value>
    </Data>
   </ExtendedData>
  </Folder>
</Folder>
```

KML ファイルからロケーション データをインポートする手順は次のとおりです。

ステップ 1 Geo マップ ツールバーの [インポート（Import）] アイコンをクリックし、[KML] を選択します。

ステップ 2 必要に応じて、表示されたダイアログの下部にあるリンクをクリックして、KML テンプレートをダウンロードします。

ステップ 3 KML ファイルを作成し、テンプレートの形式と情報をガイドとして使用してデバイス/光ファイバ/リンクデータを入力します。KML ファイルを保存します。

ステップ 4 [KMLのインポート（Import KML）] ダイアログで、保存した KML ファイルを参照して [インポート（Import）] をクリックします。デバイスと光ファイバが Geo マップ上の指定したロケーションに配置されます。管理対象リンクはトポロジマップに表示されます。インポートした管理対象リンクを Geo マップに表示するには、リンクの両側にあるデバイスが Geo マップにマッピングされている必要があります。

Geo マップからのロケーション データのエクスポート

デバイス、光ファイバ、光ファイバとリンクの関連付け、および手動で作成した管理対象リンクのロケーションデータをGeoマップからKMLファイルにエクスポートできます。KMLファイルにデータをエクスポートしたら、必要に応じてデータを編集し、Geoマップにインポートし直すことができます。

（注） 光ファイバのロケーション データを他のロケーション データと一緒にエクスポートすることはできません。個別にエクスポートする必要があります。

ステップ 1 Geo マップ ツールバーの [KMLのエクスポート（Export KML）] アイコンをクリックします。

ステップ 2 [エクスポートオプション（KML）（Export Options (KML)）] ダイアログで、エクスポートするロケーション データを選択します。

（注） [デバイスの地理的場所（Device Geo Location）]、[管理型リンク（Managed Links）]、[管理対象外のリンク（Unmanaged Links）]、[管理対象外のデバイス（Unmanaged Devices）]、[管理対象外のネットワーク（Unmanaged Networks）]、[関連付けられている光ファイバ（Associated Fibers）]、および [関連付けられていない光ファイバ（Unassociated Fibers）] を選択できます。[関連付けられていない光ファイバ（Unassociated Fibers）] を選択した場合、他のオプションは無効になります。これらの光ファイバは他のロケーションデータとは別にエクスポートする必要があるためです。

ステップ 3 [エクスポート（Export）] をクリックします。選択したロケーションデータを含むKMLファイルが作成されます。

オフラインデバイスの同期

オフライン時間のしきい値に基づき、オフラインデバイスまたはデバイスグループを同期するよう設定できます。オフラインデバイスの同期はデフォルトで無効になっています。オフラインデバイスを同期すると、到達可能性障害が回復後の自動的なデバイス同期が有効になります。すべての子グループを除いて親グループのデバイスのみを選択することはできません。子グループのいずれかを選択すると、親グループは選択されたと見なされません。このシナリオに対処するために、親グループのデバイスを含むことができる新しい子グループを作成できます。オフラインデバイスで同期が行われるタイミングを設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）]** に移動し、**[オフラインデバイスの同期（Sync Offline Devices）]** を選択します。

ステップ 2 **[選択（Select）]** ボタンを使用して、[グループごと（By Group）] または [デバイスごと（By Device）] を選択します。

ステップ 3 同期用に設定するデバイスグループまたはデバイスを選択します。

ステップ 4 時間と分のドロップダウンリストから **[オフラインのしきい値時間（Offline Threshold Time）]** を設定します。

ステップ 5 [保存（Save）] をクリックします。

Geo マップでの共有リスク リソース グループ（SRRG）の管理

（注） この機能がサポートされるのは、光デバイスとリンク上のみです（とくに NCS 2000 および NCS 4000 デバイス、OTS、OTU、および OCH リンク）。

共有リスク リソース グループ（SRRG）は、共通のリソースを共有し、障害が発生すると、グループ内のデバイスとリンクおよびそれらが参加している回線のすべてに影響するデバイスとリンクのセットです。グループ内のデバイスとリンクが、同じ障害のリスクを共有しているため、同じSRRGに属していると見なされます。たとえば、光ファイバの障害がグループ内のすべてのリンクの障害につながる可能性があるため、共通の光ファイバを共有しているリンクは同じ SRRG に属していると見なされます。

各 SRRG には 32 ビットの数値識別子があります。デバイスでは、SRRG がグローバル デバイス レベルで設定されます。リンクでは、同じ SRRG が A 側インターフェイスと Z 側インターフェイスで設定されます。

Geo マップ上の [共有リスク（SRRG）（Shared Risks (SRRGs)）] ボタンから次の SRRG 機能を使用できます。

- SRRG が設定されたデバイスとリンクを可視化する。
- SRRG に数値識別子よりも識別しやすいユーザー定義の名前を付ける。
- SRRG リソース プールに割り当てることができる新しい SRRG を作成する。
- SRRGプールとプールタイプを作成および管理できるシステム設定ウィンドウをクロス起動する。

SRRG を管理している場合は、SRRG をサポートしているデバイスだけを表示するようにマップがフィルタ処理されます。

詳細については、以下を参照してください。

- SRRG プールと SRRG ID について （273 ページ）
- 割り当て済みの SRRG と未割り当ての SRRG を表示する （274 ページ）
- SRRG 割り当てを管理する （275 ページ）
- SRRG プール タイプとリソース プールの作成および管理 （276 ページ）

SRRG プールと SRRG ID について

SRRG プール タイプとリソース プールを使用して、識別および ID の割り当てを目的として SRRG をカテゴリにグループ化できます。各プール タイプに SRRG ID の範囲を指定します。特定のプール タイプの SRRG リソース プール（プール タイプに対して定義された範囲内の一連の SRRG ID を持つ）を複数作成できます。デバイスまたはリンク用に新しい SRRG を作成する際に、特定の SRRG プール タイプおよびリソース プールに割り当てることができます。新しい SRRG の ID は、選択したリソース プールの ID 範囲から作成されます。

（注） SRRG プール タイプおよびプールの管理には、コンフィグレット アクセス権限が必要です。

詳細については、「SRRG プール タイプとリソース プールの作成および管理 （276 ページ）」を参照してください。

プール タイプ

SRRG リソース プールを作成する前に、プール タイプを作成する必要があります。プール タイプを使用すると、ネットワークに応じて SRRG のカテゴリを作成できます。

使用可能なプール タイプが 15 個、予約済みのプール タイプが 1 個あります。各プール タイプに ID の範囲が指定されています。次の表は、SRRG プール タイプの定義例を示しています。

プール タイプ ID	2 進数	プール タイプ名	範囲の開始	範囲の終了
0	0000	セントラル オフィス	0	1048575
1	0001	ROADM ノード	1048576	2097151
2	0010	ROADM 度	2097152	3145727
3	0011	ROADM アド/ドロップ	3145728	4194303
4	0100	スイッチ ノード	4194304	5242879
5	0101	リンク	5242880	6291455
6	0110	カード	6291456	7340031
7	0111	将来的にサポート	7340032	8388607
8	1000	光ファイバ ダクト/コンジット	8388608	9437183
9	1001	将来的にサポート	9437184	10485759
10	1010	将来的にサポート	10485760	11534335

プール タイプ ID	2 進数	プール タイプ名	範囲の開始	範囲の終了
11	1011	将来的にサポート	11534336	12582911
12	1100	将来的にサポート	12582912	13631487
13	1101	将来的にサポート	13631488	14680063
14	1110	将来的にサポート	14680064	15728639
15	1111	EPNM保存済みグローバル	15728640	16777215

SRRG リソース プール

プール タイプを作成した後は、特定のタイプのリソース プールを作成できます。各リソース プールには、プール タイプの範囲内で一連の ID を割り当てることができます。プールの範囲を重複させることはできません。

特定のリソース プールに新しい SRRG を割り当てることができます。SRRG の ID は、リソース プールに定義された範囲から取得されます。

SRRG プールの ID は、以下で構成される 32 ビット数値です。

- **ビット 0 ～ 1**：予約済み。00 に設定されます。
- **ビット 2**：SRRG が Cisco EPN Manager を使用して設定されていることを示します。1 に設定されます。
- **ビット 3 ～ 7**：リソース プールに対して選択されたグループ/リージョン。
- **ビット 8 ～ 11**：プール タイプ ID。
- **ビット 12 ～ 31**：プール ID の範囲。

割り当て済みの SRRG と未割り当ての SRRG を表示する

管理対象デバイス上で設定されたSRRGのグローバル リストを表示できます。これらのSRRGは特定のデバイスまたはリンク上で定義されたシステムまたはユーザーによって検出されたため、そのすべてが「割り当て済みの」SRRGになります。また、未割り当てのSRRGを表示することもできます。未割り当ての SRRG は、システムからしか削除できません。

（注） デバイスの SRRG の割り当て解除または SRRG の削除は、Cisco EPN Manager からのみ行ってください。デバイスから削除しても、Cisco EPN Manager の ENE から SRRG が割り当て解除または削除されることはありません。

各 SRRG には変更できない数値 ID が割り当てられますが、SRRG にラベルを割り当てて、より識別しやすい名前を付けることができます。

SRRG を選択すると、Geo マップに割り当てられたデバイス/リンクを表示できます。

SRRG を表示してラベルを付けるには、次の手順を実行します。

ステップ 1 左側のサイドバーで、[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）] を選択します。

ステップ 2 マップの右上にある [地理的マップ（Geographical Map）] トグル ボタンをクリックします。

ステップ 3 マップの上にある [共有リスク（SRRG）（Shared Risks (SRRGs)）] ボタンをクリックして、[表示と命名（View and Name）] を選択します。[共有リスク リソース グループ（Shared Risk Resource Groups）] ダイアログが表示されます。これには、割り当て済みの SRRG と未割り当ての SRRG を示す 2 つのタブが表示されます。SRRG の割り当てを表示すると、デバイス グループの選択がデフォルトのすべてのロケーション グループに変更されることに注意してください。

ステップ 4 Geo マップに表示する SRRG を選択します。SRRG が定義されたデバイスとリンクがマップ内で強調表示されます。

ステップ 5 SRRG の名前を変更するには、関連する SRRG ID の横にある [SRRG ラベル（SRRG Label）] 列をクリックして、必要な一意の名前を入力し、[保存（Save）] をクリックします。

（注） 割り当てられた SRRG の [SRRGラベル（SRRG Label）] 列のみ編集できます。

SRRG 割り当てを管理する

単純なウィザードを使用して、特定のデバイスとリンクを選択し、それらに割り当てられた SRRG を表示して、必要に応じて、割り当てを変更することができます。

SRRG 割り当てを管理するには、次の手順を実行します。

ステップ 1 左側のサイドバーで、[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）] を選択します。

ステップ 2 マップの右上にある [地理的マップ（Geographical Map）] トグル ボタンをクリックします。

ステップ 3 マップの上にある [共有リスク（SRRG）（Shared Risks (SRRGs)）] ボタンをクリックして、[割り当ての管理（Manage Assignments）] を選択します。SRRG 割り当ての管理ウィザードが開きます。

ステップ 4 SRRG割り当てを管理するデバイス/リンクを選択します。マップ内の必要なデバイス/リンクをクリックすることも、ウィザードのステップ 1 でボックスをクリックし、リストからデバイスを選択することもできます。

ステップ 5 [次へ（Next）] をクリックします。上記のステップで選択したすべてのデバイス/リンクに共通するすべての SRRG のリストが表示されます。SRRG が選択されたデバイスのいずれかにだけ割り当てられている場合は、リストに表示されません。SRRG は、デバイス上のデフォルトか、割り当て済みか、未割り当てかに基づいて色分けされます。疑問符アイコンをクリックすると、凡例が表示されます。

ステップ 6 プラス アイコンをクリックして、選択したデバイス/リンク用の追加の SRRG を選択するか、SRRG 名を入力することにより、その場で新しい SRRG を作成します。名前が一意の場合は、[新規作成（Create New）] リンクが表示されます。リンクをクリックして SRRG を作成します。

ステップ 7 前のステップで新しい SRRG を作成した場合は、選択したタイプのプール タイプと SRRG リソース プールを選択できるようになっています。SRRG の ID は、選択した SRRG プールに対して定義された範囲から取得されます。SRRG ID には、範囲内の数値に加えて、リージョンとタイプのビットが含まれます。

ステップ 8 [次へ（Next）] をクリックして、選択肢と SRRG 割り当ての概要を表示します。

ステップ 9 [終了（Finish）] をクリックします。SRRG の変更が成功した場合に、その旨が通知されます。失敗した場合は、エラー ダイアログに失敗の詳細が表示されます。

SRRG プール タイプとリソース プールの作成および管理

SRRG プール タイプとリソース プールを使用して、識別および ID の割り当てを目的として SRRG をカテゴリにグループ化できます。各プール タイプに SRRG ID の範囲を指定します。特定のプール タイプの SRRG リソース プール（プール タイプに対して定義された範囲内の一連の SRRG ID を持つ）を複数作成できます。デバイスまたはリンク用に新しい SRRG を作成する際に、特定の SRRG プール タイプおよびリソース プールに割り当てることができます。新しい SRRG の ID は、選択したリソース プールの ID 範囲から作成されます。

（注） SRRG プール タイプおよびプールの管理には、コンフィグレット アクセス権限が必要です。

SRRG プール タイプおよびリソース プールを作成するには、[管理（Administration）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [プールタイプ（Pool Types）] に移動するか、Geo マップの [SRRG] メニューから [プール設定（Pool Settings）] を選択します。

新しい SRRG プールを作成する手順は次のとおりです。

ステップ 1 [管理（Administration）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [プールタイプ（Pool Types）] に移動し、新しい SRRG プールに関連するプール タイプの既存のプール タイプを確認します。存在しない場合は、次のように新しいプール タイプを作成します。

a) [SRRGプールタイプ（SRRG Pool Types）] ウィンドウで、プラス アイコンをクリックしてテーブルに行を追加します。

b) [名前（Name）] フィールドに、SRRG 用に作成するグループ化を表すプール タイプの一意の名前を入力します。たとえば、「NCS 2000 デバイス」などです。

c) [タイプID（Type ID）] フィールドに、0 ～ 14 の範囲内の ID を入力します。プール タイプ ID ごとの使用可能な ID の範囲に関する説明は、SRRG プールと SRRG ID について（273 ページ）のプール タイプ定義の表を参照してください。

d) このプール タイプの ID 範囲の開始値と終了値を入力します。使用可能な範囲のすべてまたは一部を使用できます。[範囲の開始（Start Range）] または [範囲の終了（End Range）] フィールドのツールチップには、プール タイプで使用可能な範囲が表示されます。

e) **[保存（Save）]** をクリックします。

ステップ 2 次の手順に従って SRRG プールを作成します。

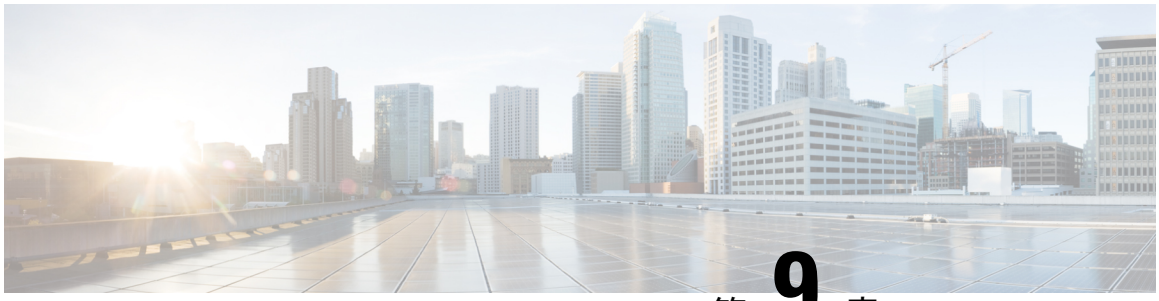
a) [管理（Administration）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [SRRG プール（SRRG Pool）] に移動します。

b) [SRRGプール（SRRG Pool）] ウィンドウで、プラス アイコンをクリックしてテーブルに行を追加します。
c) [SRRGプールの詳細（SRRG Pool Details）] 領域で、[タイプ（Type）] ドロップダウン メニューから必要なプール タイプを選択します。
d) SRRG プールの一意の名前を入力し、オプションで説明を入力します。
e) [グループ（Group）] ドロップダウン メニューから、この SRRG プールのデバイス グループを選択します。
f) このプールの SRRG ID 範囲の開始と終了を入力します。範囲は、選択したプール タイプの範囲内である必要があります。
g) **[保存（Save）]** をクリックします。

新しい SRRG プールが SRRG プール テーブルに追加されます。選択したデバイスまたはリンクの SRRG ID を作成するときにも選択できます。

第 IV 部

ネットワークの監視



第 9 章

デバイスおよびネットワークの健全性とパフォーマンスのモニター

デバイスのヘルスとパフォーマンスのモニター方法：モニターリング ポリシー

モニターリング ポリシーは、Cisco EPN Manager が以下を制御することによってどのようにネットワークをモニターするかを制御します。

- モニター対象：Cisco EPN Manager がモニターするネットワークとデバイスの属性。
- モニター頻度：パラメータをポーリングするレート。
- 問題を指摘するタイミング：ポーリングする属性の受け入れ可能な値。

- 問題の指摘方法：しきい値を超えた場合に Cisco EPN Manager がアラームを生成するかどうかとアラームの重大度。

モニターリング ポリシーは、モニター対象の制御は別として、レポート、ダッシュボード、および Cisco EPN Manager のその他の領域に表示可能なデータを決定する点で重要です。モニターリング ポリシーは、デバイス上の変更を行いません。

デフォルトで、デバイス ヘルス モニターリング（つまり、デバイス ヘルス モニターリング ポリシー）のみが有効になります。インターフェイス ヘルス モニターリングは、大規模な展開でシステム パフォーマンスを保護するためにデフォルトでは有効になりません。デバイス ヘルス モニターリング ポリシーは、デバイスの Cisco NCS 2000 ファミリと Cisco ONS ファミリに適用されないことに注意してください。これらのデバイス タイプをモニターするには、モニターリング ポリシー リファレンス（1199 ページ）に記載された光モニターリング ポリシーを使用します。

次の手順は、モニターリング ポリシーの設定方法を要約したものです。

1. モニターリング ポリシー用のテンプレートとしてモニターリング **ポリシー タイプ**を使用し、ポリシーにわかりやすい名前を付けます。ポリシー タイプは、Cisco EPN Manager に同梱されており、Quality of Service、光 SFP、TDM/SONET などのさまざまなテクノロジーとサービスのモニターリングを簡単に開始できるようにします。完全なリストは、モニターリング ポリシー リファレンス（1199 ページ）に記載されています。
2. ポリシーのポーリング頻度を調整するか、特定のパラメータのポーリングをすべて無効にします。
3. パラメータのしきい値を超えたときに Cisco EPN Manager が生成する Threshold Crossing Alarm（TCA）を指定します。一部の TCA はデフォルトで設定されます。これらを調整または無効にしたり、新しい TCA を設定したりできます。
4. ポリシーでモニターするデバイスを指定します。デバイスは、ポリシータイプに基づいてフィルタ処理されます。
5. ポリシーをアクティブにします。ポーリングされたデータが Web GUI のダッシュボード、レポート、[アラームおよびイベント（Alarms and Events）] テーブルなどの領域に表示されます。

モニターリングポリシーは、一定のポーリング間隔でネットワークとデバイス属性をポーリングすることでデータを収集します。次の理由により、ポリシーがポーリング間隔を超えて実行される場合があります。

1. 毎日のバックアップや毎日のインベントリ収集などのプロセスへのサーバーの負荷
2. デバイスへの接続またはネットワーク遅延の問題
3. デバイスからのデータ収集には、設定されているポーリング間隔よりも時間がかかります。

ポーリング中のデバイスがある場合や、または以前のポリシーの実行によりキュー内にデバイスがある場合、ポリシーは現在のポーリング間隔でのこれらのデバイスのポーリングをスキッ

プします。この動作により、特定のデバイスのモニター対象データが最大 10% 失われる可能性があります。

モニターリング ポリシーを表示して管理するには、**[モニター（Monitor）]** > **[モニターリング ツール（Monitoring Tools）]** > **[モニターリング ポリシー（Monitoring Policies）]** を選択します。

ナビゲーション	説明
自動監視（Automonitoring）	Cisco EPN Manager でデフォルトで有効になるポリシーが一覧表示されます。デバイス ヘルス モニターリング ポリシーだけがデフォルトで有効になります。このポリシーの設定を調整できます。
マイ ポリシー（My Policies）	自分が作成したポリシーがここに表示されます。[マイ ポリシー（My Policies）] からポリシーを選択すると、そのポリシーの詳細を表示できます。

基本的なデバイス ヘルス モニターリングのセットアップ

デバイス ヘルス モニターリング ポリシーは、デフォルトで有効になっています。シスコ デバイスとサード パーティ デバイスの両方をモニターします。シスコ デバイスの場合、デバイス ヘルス モニターリングは管理対象デバイスで CPU 使用率、メモリ プールの使用率、環境温度、デバイスの可用性をチェックします。サード パーティ デバイスの場合、デバイス ヘルス モニターリングは管理対象デバイスの可用性のみをチェックします。このポリシーに、使用率や温度のしきい値を指定します。もしこのしきい値を超えた場合、GUI クライアントに表示されるアラームをトリガーします。

このポリシーの現在の設定を表示するには、**[モニター（Monitor）]** > **[モニターリング ツール（Monitoring Tools）]** > **[モニターリングポリシー（Monitoring Policies）]** の順に選択し、左側のリストから [自動モニター（Automonitoring）] を選択します。また、ポーリング頻度やさまざまなパラメータのしきい値を調整できます。ポーリング頻度やしきい値を調整するには、GUI クライアントに表示されるドロップダウン リストを使用します。

また、特定のデバイス（たとえば、特定のタイプのデバイスや特定の地理的場所に位置するデバイスなど）をモニターするデバイス ヘルス モニターリング ポリシーを作成することもできます。その実行方法については、モニター対象を調整する（291ページ）を参照してください。

基本的なインターフェイス モニターリングの設定

デフォルトでは、インターフェイスはモニターされません。これにより、多数のインターフェイスがあるネットワークのシステムパフォーマンスが保護されます。

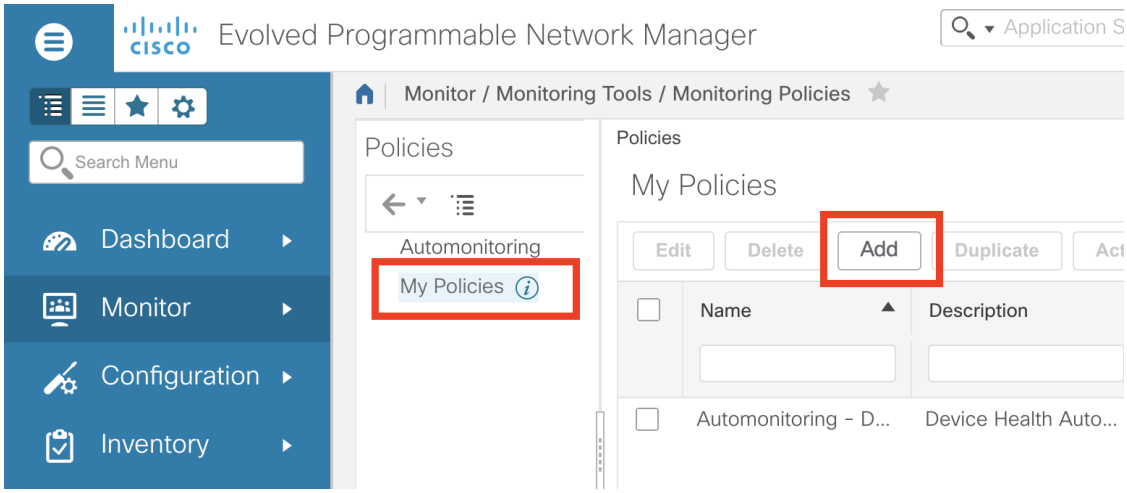
基本的なインターフェイス モニターリングを設定するには、次の手順を使用します。

インターフェイス モニターリングを設定して有効するには、次の手順に従います。

ステップ 1 **[モニター（Monitor）]>[モニタリングツール（Monitoring Tools）]>[モニタリングポリシー（Monitoring Policies）]** の順に選択し、左側のリストから [マイポリシー（My Policies）] を選択します。

ステップ 2 [追加（Add）] をクリックして、新しいポリシーを作成します。

図 *6:* モニターリング ポリシーの追加



ステップ 3 汎用インターフェイス モニターリングの場合は [インターフェイス ヘルス（Interface Health）] を選択します。光デバイスをモニターリングする場合は、[光15分（Optical 15 Mins）] またはその他の光ポリシー（モニターリング ポリシー リファレンス （1199 ページ）を参照）を選択します。

ポリシーを選択すると、Cisco EPN Manager によりこのウィンドウにポリシー設定が読み込まれます。

ステップ 4 名前と説明を入力します。

ステップ 5 [デバイスの選択（Device Selection）] ドロップダウンリストから適切なオプションボタンをクリックし、モニターするデバイスまたはデバイスグループを選択します。インターフェイスヘルスのモニタリングポリシーの場合、ポートグループも選択できます。

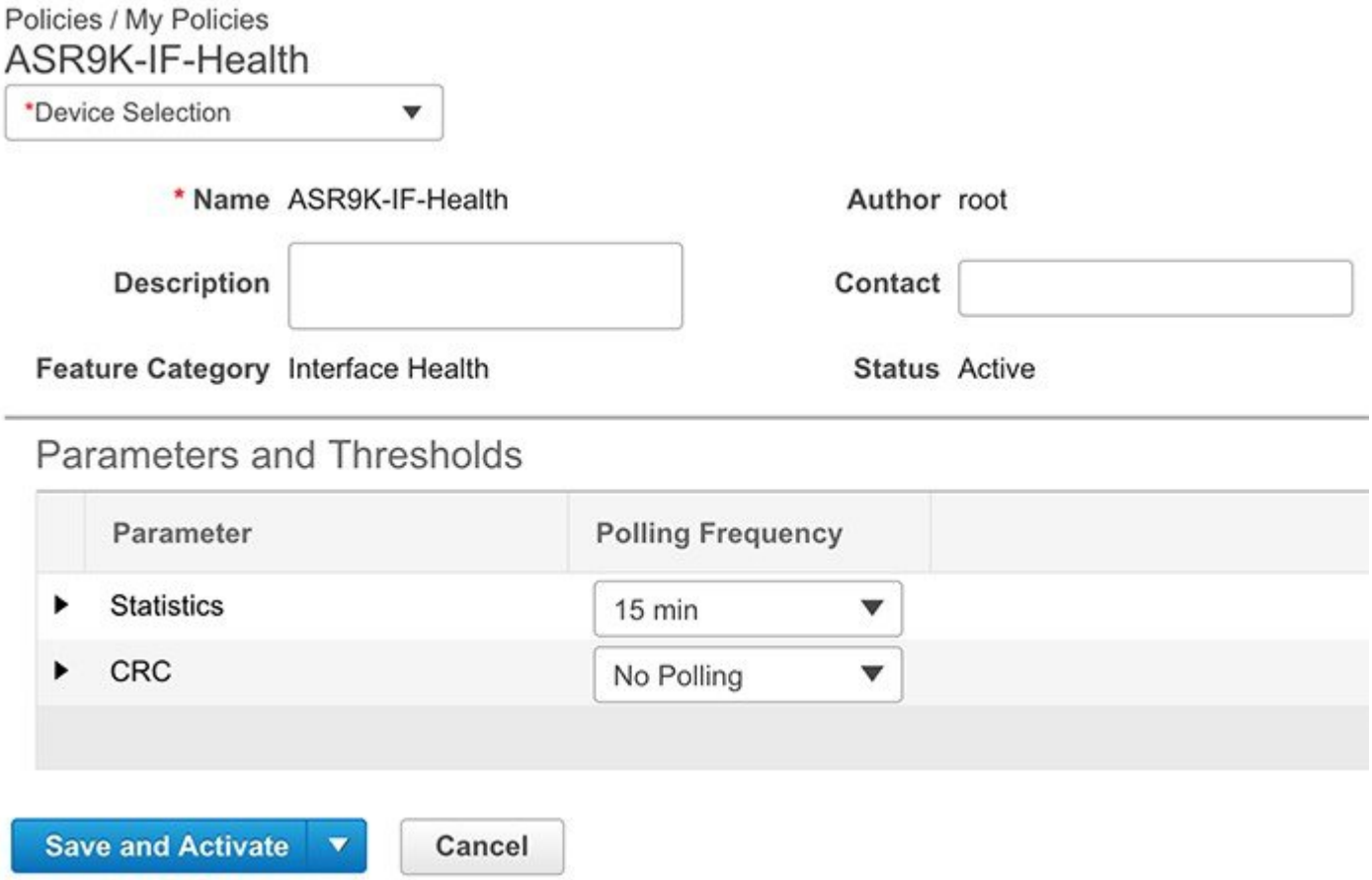
Cisco EPN Manager では、ステップ 3 で選択したポリシーに該当するデバイスまたはポートのみが一覧表示されます。

次の点に注意してください。

- ポーリングとしきい値にデフォルト設定を使用するには、ステップ 8 に進みます。
- 現在のリリースの制約により Cisco EPN Manager では、インターフェイスヘルスのモニタリングポリシーは、巡回冗長検査（CRC）エラーデータについて、選択したポートグループに関連付けられているインターフェイスだけでなく、ネットワーク内のすべてのインターフェイスをポーリングします。CRC エラーのデータを確認するときは、常にこのことに注意してください。

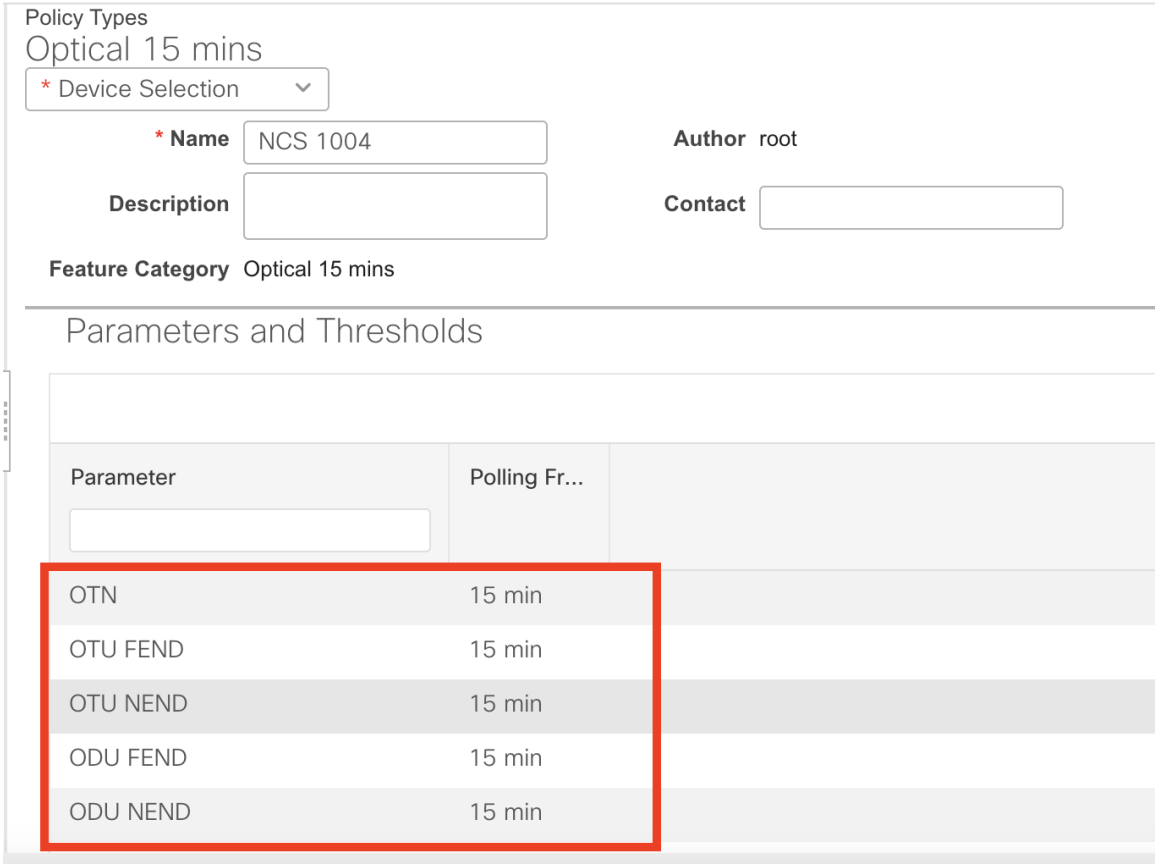
ステップ 6 インターフェイスのポーリング頻度を調整するには、[ポーリング頻度（Polling Frequency）] ドロップダウンリストから値を選択します。異なるパラメータのポーリング頻度を設定できるポリシーと、すべてのパラメータに 1 つのポーリング頻度だけが適用されるポリシーがあります。

Cisco ASR 9000 インターフェイスをモニターするポリシーの例を次に示します。このポリシーには [インターフェイスヘルス（Interface Health）] ポリシー タイプが使用されており、すべてのパラメータが同一間隔でポーリングされます。



また、Cisco NCS 1004 インターフェイスをモニターするポリシーの例を次に示します。

このポリシーでは [光15分（Optical 15 mins）] ポリシー タイプが使用され、インターフェイス タイプごとに固有のポーリング間隔が設定されています。間隔を編集するには、その間隔をダブルクリックします。



ステップ 7 ポリシーで TCA カスタマイズがサポートされている場合は、しきい値を調整できます。モニターリングポリシーのしきい値およびアラーム動作の変更 （296 ページ）を参照してください。

ステップ 8 次をクリックします。

- モニタリングを今すぐ開始する場合は [保存してアクティブにする（Save and Activate）]。
- ポリシーを保存して後でアクティブ化する場合は [保存して閉じる（Save and Close）]。

ダッシュボードを使用したネットワークとデバイスの状態の確認

Cisco EPN Manager は、デバイスとネットワークをモニターするためのさまざまなダッシュボードを提供します。ダッシュボードが提供できる内容の例を次に示します。

- ネットワーク全体のリアルタイムのステータス情報（到達不能なデバイス、ダウンしているインターフェイス、最新のアラームなど）。

- 履歴情報の要約（最も頻繁に発生するアラーム、メモリと CPU の使用率が最も高いデバイスとインターフェイスなど）。
- デバイス固有の情報（デバイスの可用性履歴、使用率、インターフェイス統計情報、アラームなど）。
- テクノロジー固有の情報（キャリア イーサネット サービスなど）。

ダッシュボードの詳細については、ダッシュボードのセットアップと使用 （7 ページ） を参照してください。

Cisco EPN Managerによるモニターリング対象のチェック

このトピックでは、次の情報を取得する方法について説明します。

- 有効化されているポリシー、そのステータス、およびその履歴。
- Cisco EPN Manager がポーリングしている特定のパラメータ、ポーリング頻度、およびそのしきい値超過アラーム（TCA）の設定。
- ポリシーの作成者、およびポリシーのベースとして使用されたポリシー タイプ。

ポリシーによるポーリング対象、ポリシーの前回の実行時間、およびポリシーが現在アクティブかどうかを確認するには、**[モニタ（Monitor）]**>**[モニタリング ツール（Monitoring Tools）]**>**[モニタリングポリシー（Monitoring Policies）]** を選択してから、[ポリシー（My Policies）] を選択します。Cisco EPN Manager により、作成した、またはアクセス権のあるモニタリング ポリシーが、次の情報とともに一覧表示されます。

ポリシーのフィールド	説明
名前	ポリシー名（ポリシーの作成者が指定します）。ポリシーの作成者を確認するには、この表の後にある手順を参照してください。
[説明（Description）]	ポリシーの説明（ポリシーの作成者が指定します）。
[タイプ（Type）]	このポリシーを作成するときに使用されたテンプレート（ポリシータイプ）。ポリシータイプの詳細については、デバイスのヘルスとパフォーマンスのモニター方法：モニターリング ポリシー （281 ページ）を参照してください。
[ステータス（Status）]	[アクティブ（Active）] または [非アクティブ（Inactive）]

ポリシーのフィールド	説明
[しきい値（Threshold）]	ポリシーがパラメータしきい値をモニターし、TCA を生成するかどうか。「はい（Yes）」が表示される場合、この表の後にある手順を使用して TCA 設定を確認できます。
[有効化履歴（Activation History）]	アクティブなモニターリング ポリシー：ポリシーが有効化された回数を表示し、次の情報が含まれる [有効化履歴（Activation History）] ポップアップ ウィンドウへのハイパーリンクを提供します。 • ポリシーが有効化された時間。 • 各ポリシー実行でポーリングされたデバイス。非常に長い一覧の場合は、マウス カーソルを一覧の [有効化対象（Activated for）] 列にホバーし、ポップアップ ウィンドウを起動します。 非アクティブなモニターリングポリシー：[使用できません（Not Available）] が表示されます。
[収集ステータス（Collection Status）]	アクティブなモニターリング ポリシー：次の情報が含まれる [収集ステータス（Collection Status）] ポップアップ ウィンドウへのハイパーリンクを提供します。 • ポリシーによってポーリングされた各デバイスのデバイス名、IP アドレス、および可用性状態。 • 各ポリシー実行でポーリングされたパラメータ。非常に長い一覧の場合は、マウス カーソルを一覧の [パラメータ（Parameters）] 列にホバーし、ポップアップ ウィンドウを起動します。 非アクティブなモニターリングポリシー：[使用できません（Not Available）] が表示されます。

ポーリング頻度と TCA の詳細を表示するには、[ポリシー（My Policies）] で、左側の一覧からポリシーを選択します。ポリシー タイプに応じて次の情報が表示されます。

（注） [オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、および[オプティカル30秒（Optical 30 secs）]のパラメータを表示するには、モニターリング ポリシー リファレンス （1199 ページ）を参照してください。

ポリシーのフィールド	説明
全般情報（General Information）	名前、説明、作成者、ステータス、ポリシー タイプ（機能カテゴリ）。ポリシー タイプの詳細については、デバイスのヘルスとパフォーマンスのモニター方法：モニターリング ポリシー （281 ページ）を参照してください。
[デバイスの選択（Device Selection）]	ポリシーがモニターするデバイス。
[ポーリング頻度（Polling Frequency）]	Cisco EPN Manager がデバイス パラメータをポーリングする頻度。
[パラメータとしきい値（Parameters and Thresholds）]	ポーリングされたパラメータとその TCA 設定（ある場合）。TCA 設定を表示するには、パラメータ名の横にある矢印をクリックします。さまざまなポリシー タイプによってポーリングされるパラメータを表示する方法については、モニターリング ポリシーによりポーリングされるパラメータとカウンタの確認 （289 ページ）を参照してください。

モニターリングポリシーによりポーリングされるパラメータとカウンタの確認

Cisco EPN Manager によるモニターリング対象のチェック （287 ページ） 現在アクティブなモニターリング ポリシーを確認する方法を説明します。ポリシーでポーリングされるパラメータを確認するには、次の手順に従います。

（注） [オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、および[オプティカル30秒（Optical 30 secs）]のパラメータを表示するには、モニターリング ポリシー リファレンス （1199 ページ）を参照してください。

この手順では、次のパラメータを確認できます。

- 既存のポリシーにより（ポリシーがアクティブ/非アクティブであるかどうかに関係なく）ポーリングされるパラメータ。

- 1 つのポリシー タイプで使用されるパラメータ。ポリシーの作成前に、新しいポリシーでポーリングされる内容を確認する場合に便利です。

ステップ 1 **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [モニターリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] を選択します。Web GUI に、既存のアクティブなモニターリング ポリシーと非アクティブなモニターリング ポリシーのリストが表示されます。

ステップ 2 **既存のポリシーで使用されるパラメータを確認するには**：

- 最後にポーリングされたパラメータを確認するには、右側のウィンドウでポリシーを見つけ、[収集ステータス（Collection Status）] 列の [詳細（Details）] をクリックします。[収集データ（Collection Data）] ダイアログボックスの [パラメータ（Parameter）] 列のテキストにマウス カーソルを合わせます。ポーリングされたパラメータのリストが表示されます。
- パラメータとそのポーリング設定を確認するには、左側のナビゲーション エリアで [マイ ポリシー（My Policies）] を展開し、確認するポリシーを選択します。右側のウィンドウに、パラメータとそのポーリング設定が表示されます。

ステップ 3 **特定のポリシー タイプで使用されるパラメータを確認するには**：

a) [編集（Edit）] をクリックします。左側のナビゲーション エリアに、サポートされるポリシー タイプのリストが表示されます。

b) ポリシータイプを選択します。右側のウィンドウに、そのポリシーでポーリングされるパラメータと、デフォルトのポーリング設定およびTCA設定が表示されます。（モニターリング ポリシーの作成時にこれらの設定をカスタマイズできます。）

[ポリシー（Policies）] ペインのポップアップ ウィンドウ

[モニターリングポリシー（Monitoring Policies）] ページの [ポリシー（Policies）] ペインで、対応するポリシーまたはポリシーフォルダの概要情報とアクションリンクを提供するポップアップ ウィンドウを開くことができます。ポップアップ ウィンドウを開くには、該当する [i]（**情報**）アイコン上にカーソルを移動します。

- ポリシーのポップアップ ウィンドウを開くと、そのポリシーのタイプ、ステータス、最終更新時のタイムスタンプなどの情報が表示されます。[アクション（Actions）] 領域のリンクをクリックして、ポリシーを編集、削除、または複製できます。
- ポリシー フォルダのポップアップ ウィンドウを開くと、フォルダの名前とそこに含まれるポリシーの数が表示されます。[アクション（Actions）] 領域のリンクをクリックして、フォルダを削除したり、新しいサブフォルダを追加したりできます。フォルダを追加および削除できるのは、[マイポリシー（My Policies）] 内のみです。また、ユーザーが作成したフォルダが配置されている場合は、新しいポリシーの作成時に必ず宛先フォルダを指定する必要があります。

モニターリングポリシーのデバイス、ポーリング、しきい値、およびアラーム設定の確認

モニターリングポリシーのしきい値とアラーム設定を確認するには、次の手順を実行します。

ステップ 1 **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [モニターリング ポリシー（Monitoring Policies）]** を選択してから、[マイ ポリシー（My Policies）] を選択します。

ステップ 2 モニターリング ポリシーを選択し、[編集（Edit）] をクリックしてポリシーの詳細を開きます。

ステップ 3 ポリシーで監視するデバイスを確認するには、[デバイスの選択（Device Selection）] ドロップダウン リストをクリックします。監視されているデバイスは、チェック マークで示されます。デバイスを追加または削除するには、ポリシーでモニターするデバイス セットの変更 （295 ページ）を参照してください。

ステップ 4 ポリシーで使用されているポーリング間隔を確認するには、[ポーリング間隔（Polling Interval）] の設定をクリックします。パラメータごとのポーリングについては、個別のパラメータを展開して設定を確認します。ポーリングの設定を調整するには、モニターリング ポリシーのポーリングの変更 （295 ページ）を参照してください。

光ポリシー ポーリング周波数は変更できません。無効にすることのみが可能です。

ステップ 5 ポリシーで使用されているしきい値とアラームの設定を確認するには、[ポーリングとしきい値（Polling and Thresholds）] 領域のパラメータを展開します。しきい値とアラームの設定を変更するには、モニターリング ポリシーのしきい値およびアラーム動作の変更 （296 ページ）を参照してください。

光ポリシーのしきい値はカスタマイズできません。

モニター対象を調整する

Cisco EPN Manager のモニター対象を調整するには、次の表のガイダンスに従って、必要な最良の方法を見つけてください。

条件：		参照先：
Cisco EPN Manager が必要なデータを収集している	ポーリング頻度を変更する必要がある	モニターリング ポリシーのポーリングの変更 （295 ページ）
	アラーム動作を調整する必要がある	モニターリング ポリシーのしきい値およびアラーム動作の変更 （296 ページ）
	モニターするデバイスを調整する必要がある	ポリシーでモニターするデバイス セットの変更 （295 ページ）

条件：		参照先：
Cisco EPN Manager が必要なデータを収集してない	同様のモニターリング ポリシーがすでに存在する	既存のポリシーベースの新規モニターリング ポリシーの作成 （292 ページ）
	同様のモニターリング ポリシーは存在しないが、ポリシー タイプの 1 つにモニターするパラメータが含まれている	事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成 （293 ページ）
	同様のモニターリング ポリシーは存在せず、どのポリシー タイプにもモニターするパラメータが含まれていない	サポートされないパラメータとサードパーティ デバイスを対象としたモニターリング ポリシーの作成 （293 ページ）
	サポートされていないデバイスまたはサードパーティ デバイスをモニターする必要がある	

既存のポリシー ベースの新規モニターリング ポリシーの作成

ステップ 1 現在のモニター対象を調べて、新しいポリシーを作成する必要があるかどうかを確認します。Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。

ステップ 2 既存のポリシーの複製を作成します。

a) **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [モニターリング ポリシー（Monitoring Policies）]** の順に選択し、左側にあるリストで [マイ ポリシー（My Policies）] をクリックします。

b) 複製するポリシーを見つけます。

c) ポリシーを選択し、[複製（Duplicate）] をクリックします。

d) [複製ポリシーの作成（Duplicate Policy Creation）] ダイアログで、親フォルダを選択し、ポリシーの名前と説明を入力して [OK] をクリックします。

ステップ 3 複製したポリシーに変更を加えます。

a) [マイ ポリシー（My Policies）] でポリシーを見つけます。

b) ポリシーを選択して、[編集（Edit）] をクリックします。

c) 必要に応じて、設定を変更します。参照先：

- ポリシーでモニターするデバイス セットの変更 （295 ページ）
- モニターリング ポリシーのポーリングの変更 （295 ページ）
- モニターリング ポリシーのしきい値およびアラーム動作の変更 （296 ページ）

ステップ 4 次をクリックします。

- ポリシーを保存し、選択したデバイスで即座にアクティブ化する場合には、[保存してアクティブにする（Save and Activate）]。

- ポリシーを保存して後でアクティブ化する場合は [保存して閉じる（Save and Close）]。

事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成

ステップ 1 現在モニターされている対象を確認します。Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。

ステップ 2 **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [モニターリング ポリシー（Monitoring Policies）]** を選択し、[追加（Add）] をクリックします。

ステップ 3 [ポリシー タイプ（Policy Types）] メニューから、使用するポリシー タイプ テンプレートを選択します。

ステップ 4 新しいポリシーを設定します。

a) [デバイスの選択（Device Selection）] ドロップダウン リストから、デバイス、デバイス グループ、またはポート グループを選択します。（すべてのモニターリング タイプをポート グループに適用できるわけではありません。）

b) 名前と連絡先を入力し、説明を編集します。

c) [パラメータとしきい値（Parameters and Thresholds）] で、ポーリング設定、パラメータ値、およびアラームの条件を設定します。モニターリング ポリシーのポーリングの変更 （295 ページ）およびモニターリング ポリシーのしきい値およびアラーム動作の変更 （296 ページ）を参照してください。

ステップ 5 次をクリックします。

- ポリシーを保存し、選択したデバイスで即座にアクティブ化する場合には、[保存してアクティブにする（Save and Activate）]。
- ポリシーを保存して後でアクティブ化する場合は [保存して閉じる（Save and Close）]。

サポートされないパラメータとサードパーティデバイスを対象としたモニターリング ポリシーの作成

サードパーティまたはシスコのデバイスおよびデバイス グループをモニターするためのカスタム MIB ポーリング ポリシーを設計できます。また、Cisco EPN Manager がデフォルト ポリシーを提供していないデバイスの機能をモニターするためのカスタム MIB ポリシーを作成することもできます。この機能を使用して、以下の操作を実行することができます。

- デバイス タイプの SNMP MIB をアップロードし、ポーリングするデバイスと属性およびポーリング頻度を選択する。
- 単一の MIB 定義ファイルまたは依存関係がある MIB のグループを ZIP ファイルとしてアップロードする。

• 折れ線グラフまたは表として結果を表示する。

この機能により、同じデバイスおよび属性に対するポーリングを容易に繰り返すことができ、SNMP を使用してシスコ デバイスをポーリングする方法をカスタマイズできます。

最大 25 のカスタム MIB ポーリング ポリシーを作成できます。

カスタム MIB ポーリング ポリシーを作成するには、次の手順を実行します。

ステップ 1 **[モニター（Monitor）]** > **[モニターリング ツール（Monitoring Tools）]** > **[モニターリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] を選択し、[追加（Add）] をクリックします。

ステップ 2 [ポリシー タイプ（Policy Types）] メニューから、[カスタム MIB ポーリング（Custom MIB Polling）] を選択します。

ステップ 3 ポリシーの名前を入力します。

ステップ 4 [MIB の選択（MIB Selection）] タブで、ポーリング頻度を指定し、MIB 情報を入力します。

- Cisco EPN Manager でモニターする MIB が [MIB（MIBs）] ドロップダウンリストに表示されない場合は、URL http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2 からモニターする MIB をダウンロードします。
- MIB をアップロードするには、ZIP ファイルをアップロードする場合にのみファイル名の拡張子を指定します。
- ZIP ファイルをアップロードする場合は、すべての依存 MIB ファイルが ZIP に含まれているか、またはすでにシステムに存在することを確認してください。
- ファイルをアップロードし、MIB 定義に同じ名前が付いていることを確認します。ZIP ファイルをアップロードする場合、そのファイル名を好きなように指定できますが、その中に含まれている MIB ファイルも同じ規則に従う必要があります（例：MyMibs.zip は、ZIP 内のすべての MIB ファイルがその MIB 名に一致していれば許容可能です）。

ステップ 5 デバイスで作成したポリシーをアクティブ化する前にテストするには、[テスト（Test）] タブをクリックして、新しいポリシーをテストするデバイスを選択します。

ステップ 6 指定したデバイスでポリシーを即座にアクティブ化するには、[保存してアクティブにする（Save and Activate）] をクリックします。

ステップ 7 MIB ポーリング データを表示するには、作成したポリシーの名前を使用して [パフォーマンス（Performance）] ダッシュボードの汎用ダッシュレットを作成します。

（注） Cisco ASR デバイスの SNMP ポーリングの日付を表示するには、CPU 使用率の場合は show platform hardware qfp active datapath utilization | inc Processing コマンドを、メモリ使用率の場合は show platform hardware qfp active infrastructure exmem statistics | sec DRAM コマンドを使用する必要があります。

過去のモニターリング ポリシー データ収集のステータスの確認

モニターリング ポリシーの過去のデータ収集を確認するには、次の手順を実行します。

ステップ 1 **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [モニターリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] をクリックします。

ステップ 2 ポリシーを見つけ、[収集ステータス（Collection Status）] の下にある [詳細（Details）] をクリックして [収集データ（Collection Data）] ダイアログを開きます。デバイスに対してポーリングを行ったパラメータを確認するには、[パラメータ（Parameter）] 列のテキストの上にマウスを重ねます。

ポリシーでモニターするデバイス セットの変更

モニターリング情報の収集頻度（ポーリング間隔）をカスタマイズできます。すべてのポリシーにこれらの設定がすべて含まれているわけではありません。たとえば、統計情報だけを収集するポリシーには、しきい値やアラームが関連付けられていない可能性があります。

ステップ 1 **Monitor > Monitoring Policies > My Policies** を選択してから、編集するポリシーを選択します。

ステップ 2 編集するポリシーを確認して [**Edit**] をクリックします。

ステップ 3 [デバイスの選択（Device Selection）] ドロップダウン リストをクリックします。

ステップ 4 必要に応じてデバイスを選択および選択解除します。

ステップ 5 [**Save and Activate**] をクリックしてポリシーを保存し、選択したデバイスですぐにアクティブ化します。

モニターリング ポリシーのポーリングの変更

モニターリング情報の収集頻度（ポーリング間隔）をカスタマイズできます。すべてのポリシーにこれらの設定がすべて含まれているわけではありません。たとえば、統計情報だけを収集するポリシーには、しきい値やアラームが関連付けられていない可能性があります。

ステップ 1 **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [モニターリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] をクリックします。

ステップ 2 編集するポリシーを選択して、[編集（Edit）] をクリックします。

ステップ 3 ポーリング頻度を調整します。ポーリングの調整方法は、モニターリング ポリシーのタイプに応じて異なります。

- すべての属性に 1 つのポーリング頻度を適用するポリシー：ポーリング頻度を調整するには、[ポーリング頻度（Polling Frequency）] ドロップダウンリストから新しい間隔を選択します。ポーリングを無効にするには、ページ下部にある [保存して非アクティブ化（Save and Deactivate）] をクリックしてポリシーを非アクティブ化します。
- 属性ごとにポーリング頻度を設定するポリシー：特定の属性のポーリング設定を変更するには、属性の行をダブルクリックして設定を変更します。[ポーリングなし（No Polling）] を選択すると、その属性のポーリングだけが無効になります。

ポリシーですべての属性のポーリングを無効にするには、ページ下部にある [保存して非アクティブにする（Save and Deactivate）] をクリックしてポリシーを非アクティブにします。次の手順に進まないでください。

ステップ 4 ポリシーを保存して選択したデバイスで即座にアクティブ化する場合は [保存してアクティブにする（Save and Activate）] をクリックします。

モニターリング ポリシーのしきい値およびアラーム動作の変更

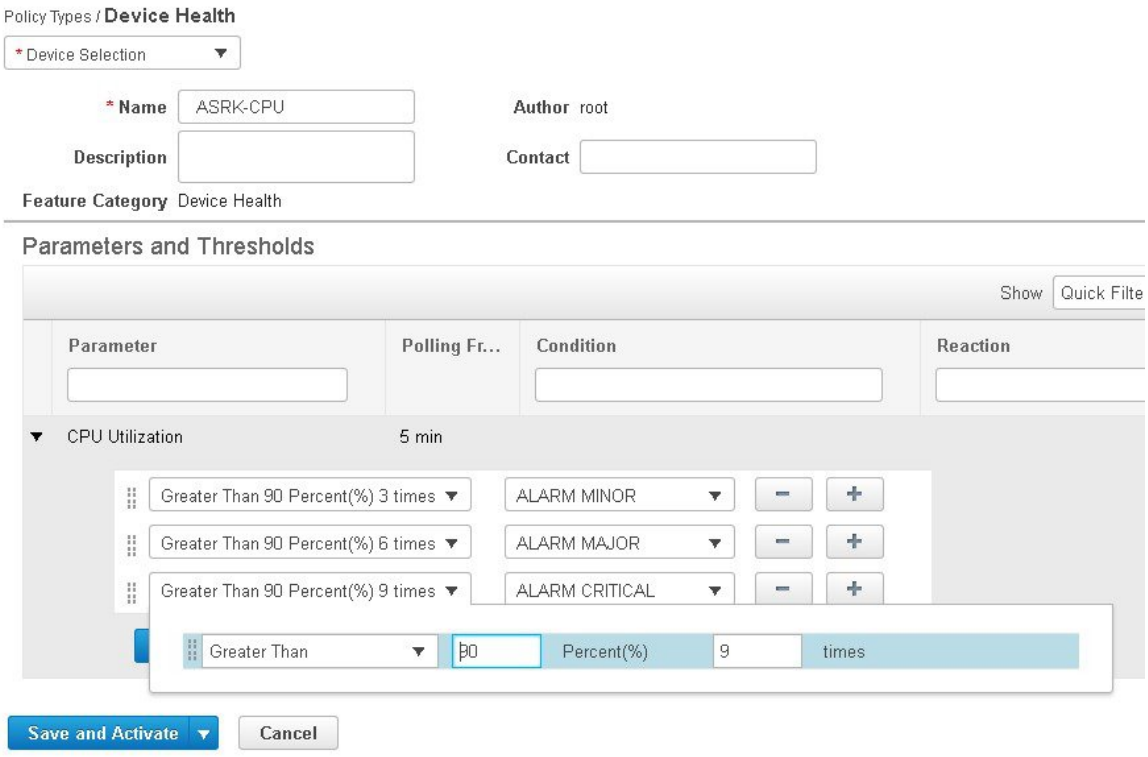
問題を示すしきい値と、問題が検出された場合に Cisco EPN Manager で情報イベントまたは（任意の重大度の）アラームを生成するかどうかをカスタマイズできます。すべてのポリシーにこれらの設定がすべて含まれているわけではありません。たとえば、統計情報だけを収集するポリシーには、しきい値やアラームが関連付けられていない可能性があります。

ステップ 1 **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [モニターリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] を選択します。

ステップ 2 編集するポリシーを選択して、[編集（Edit）] をクリックします。

ステップ 3 変更するパラメータを検索します。パラメータを検索するには、[パラメータ（Parameters）]テキストボックスに文字列を入力します。

ステップ 4 パラメータを展開します。既存の条件を変更するか、新しい条件を追加することができます。次の図では、Cisco ASR 9000 デバイスの CPU 使用率のしきい値とアラームが指定されています。



（注） 次の表に示すように、各メトリックに対して設定できるしきい値は合計 50 個までです。

ステップ 5 操作が完了したら、[保存してアクティブにする（Save and Activate）] をクリックして、選択したデバイスにポリシーを保存して即座にアクティブにします。

パフォーマンス テストの実行

パフォーマンス テストを実行すると、Cisco EPN Manager がリアルタイムでネットワーク デバイスに接続して情報を取得します。一方、レポートにはデータベースに保存された履歴データが使用されます。詳細については、実行するテストの種類に応じて次のトピックを参照してください。

- EVC の Y.1564 に基づくパフォーマンス テスト （848 ページ）
- EVC の Y1731 に基づくパフォーマンス テスト （852 ページ）
- 光回線のパフォーマンス テスト （853 ページ）
- 回線エミュレーション サービスのパフォーマンス テスト （856 ページ）

Cisco EPN Manager は、OTS 光リンクでの OTDR パフォーマンス テストの実行もサポートしています。詳細については、OTS リンクでの OTDR パフォーマンス テストの実行 （298 ページ）を参照してください。

OTS リンクでの OTDR パフォーマンス テストの実行

光タイム ドメイン反射率計（OTDR）テストは、光ファイバの長さに応じた減衰のグラフィカルなシグネチャであり、リンク コンポーネント（ケーブル、コネクタ、スプライス）の性能に関する分析情報を提供します。OTS リンク関連の問題（デバイスやスプライスの劣化、ケーブルの曲げなど）のリモート診断が可能です。

OTDR テストは、TNC カードの OTDR ポートに接続されている OTS リンクでのみ開始できます。

（注） NCS1001 デバイスの場合、デフォルトの xml 設定がデバイス設定によって異なる場合は、/opt/CSCOlumos/conf/ncs1k-otdr-ports.xml にデバイス固有の設定を含む .xml ファイルを追加する必要があります。そうすることで、EDFA 回線ポートに関連付けられた OTS リンクと OTDR ポート間のアソシエーション/接続が提供されます。

次の表に示すように、OTDR 機能の一部は特定のユーザーグループに制限されています。

ユーザー グループ		OTDR スキャン結果の表示	OTDR スキャンの実行と分析	OTDR スキャンの設定	ベースラインの設定
Web GUI	Root	対応	対応	対応	対応
	スーパーユーザー	対応	対応	対応	対応
	Admin	対応	対応	対応	対応
	Config Managers	対応	対応	対応	対応
	System Monitoring	対応	対応	×	対応

OTDR スキャンには、リンク テーブルの [アクション（Actions）] メニューまたは [インターフェイス360（Interface 360）] ビューからアクセスできます。[OTDRスキャン（OTDR Scan）] メニュー オプションは、OTDR がサポートされているリンクまたはインターフェイスでのみ使用できます。

OTDR スキャンを実行する手順は次のとおりです。

ステップ 1 次のいずれかの方法で OTDR スキャン ウィンドウにアクセスします。

- **[インベントリ（Inventory）]** > **[その他（Other）]** > **[リンク（Links）]** を選択します。目的の OTS リンクを選択し、[アクション（Actions）] > [OTDRスキャン（OTDR Scan）] を選択します。

- テストするリンクのどちらかの側の [インターフェイス360（Interface 360）] ビューを開き、[アクション（Actions）] > [OTDRスキャン（OTDR Scan）] を選択します。

[OTDRスキャン（OTDR Scan）] ウィンドウが開いて、このリンクの最後のスキャン結果が表示されます。

ステップ 2 [設定（Configure）] タブで、リンクの両側のOTDR設定を確認し、必要に応じて変更します。OTDR ポート値の設定 （301 ページ）を参照してください。

ステップ 3 [スキャン（Scans）] タブで、**[スキャン方向の変更（Change Scan Direction）]** の横にある矢印をクリックして、方向設定を表示します。**[スキャン方向（Scan Direction）]** 領域に、選択した OTS リンクの A 側と Z 側が表示され、テストを実行する方向を選択できます。

ステップ 4 **[スキャン方向（Scan Direction）]** で、関連する矢印をクリックしてテストの方向を選択します。各方向矢印の上には、その方向の最後のスキャンが実行された時期か、またはダウンロードする新しいスキャンがあるかどうかを示す情報が表示されます。

テーブルには、選択した方向のすべてのシステム、ベースライン、およびインポートされたスキャンが表示されます。次の操作を実行できます。

- 可能な場合は、*[i]* アイコンをクリックして、1 つまたは複数のスキャンを表示します。
- マグアイコンをクリックして、スキャンをダウンロードします。

  （注） デバイスから Cisco EPN Manager にスキャン結果を表示/ダウンロードするには、TFTP を有効にする必要があります。

- 1 つまたは複数のスキャンを選択し、丸い矢印をクリックしてこれらのスキャンをダウンロードします。
- 列のデータをフィルタリングおよびソートします。

ステップ 5 次のいずれかの方法で新しいスキャンを開始します。

- テーブルから特定のスキャンを選択し、[スキャンの開始（Start Scan）] ボタンをクリックします。
- テーブルから特定のスキャンを選択せずにスキャンを開始するには、**[スキャンの開始（Start Scan）]** をクリックします。[新規スキャンの開始（Start New Scan）] ダイアログが表示されます。必要に応じて **[距離プロファイル（Distance Profile）]** および **[スキャンモード（Scan mode）]** を選択し、**[続行（Continue）]** をクリックしてスキャンを開始します。

[スキャン方向の変更（Change Scan Direction）] ウィンドウでスキャンの進行状況を確認できます。進行中のスキャンを停止するには、スキャンを実行する方向矢印の上にある **[キャンセル（Cancel）]** リンクをクリックします。

ステップ 6 スキャンが完了すると、次のようになります。

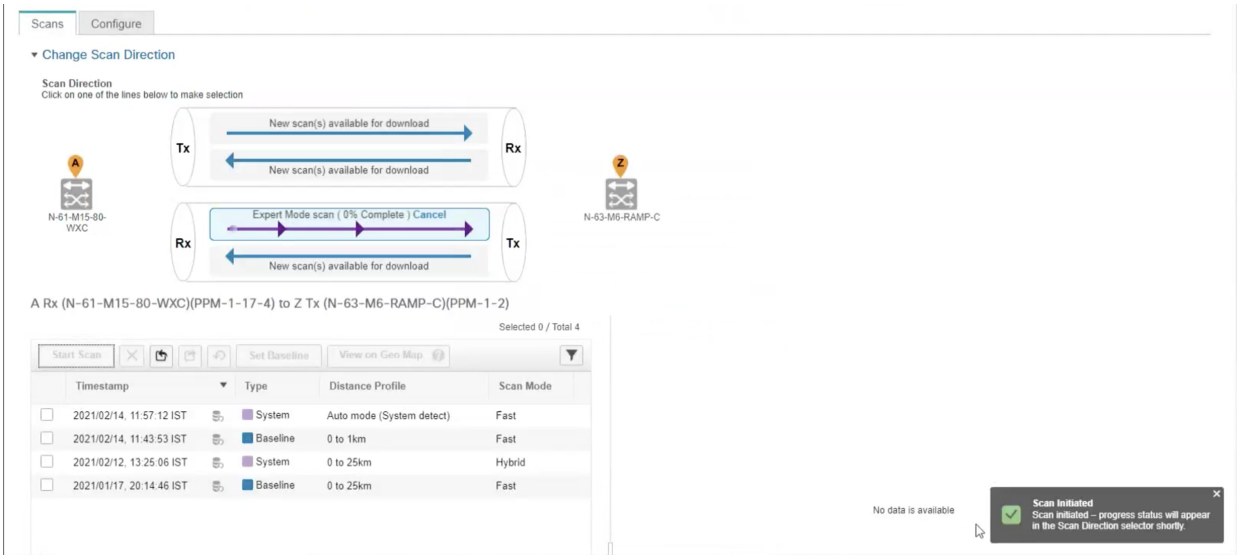
- スキャン結果が、指定した距離プロファイル（km）上の電力測定値（dB）とともにグラフィカル表示されます。ベースライン グラフを表示して、最後のスキャン読み取り値と比較することもできます。
- [i] アイコンをクリックすると、[Events] タブに、距離（km）、ベースライン読み取り値（dB）、および以前のスキャン読み取り値（dB）を含むテーブルが表示されます。ベースラインとスキャン結

果の比較である相対/絶対しきい値が表示されます。[タイプ（Type）] フィールドを使用して、イベントの詳細の [反射（Reflection）]、[挿入損失（Insertion Loss）]、または [反射と損失（Reflection with Loss）] をフィルタリングします。イベントを分析するには、テーブルでイベントを選択して [イベントの分析（Analyze Event）] をクリックします。これにより、イベントの特定の場所でスキャンが再実行されます。

（注）
- しきい値がデバイスに設定された値を超えると、アラームが発生します。[Reflection]、[Insertion Loss]、および [Reflection with Loss] の情報は、[Type] フィールドのアイコンを使用すると再表示されます。
- 繰り返しおよびしきい値は、NCS1001 デバイスではサポートされません。
- NCS2K デバイスの場合、新しいスキャンを開始するときに、[高速（Fast）] スキャンと [ハイブリッド（Hybrid）] スキャンのいずれかを選択できます。このオプションは、NCS1001 デバイスでは使用できません。

- Geo マップのコンテキスト内にスキャン結果を表示するには、[Geoマップで表示（View on Geo Map）] をクリックします。Geo マップでの OTDR スキャン結果の表示 （304 ページ）を参照してください

図 7: [スキャンイベントの詳細（*Scan Event Details*）] の表示



ステップ 7 （任意）[ベースラインの設定（Set Baseline）] をクリックして、OTDR テストのベースラインを設定します。ベースラインを設定すると、最後のスキャン結果と比較できます。

[ベースラインの設定（Set Baseline）] は NCS1001 デバイスではサポートされていません。

ステップ 8 スキャン結果をエクスポートするには、OTDR スキャン結果のエクスポート （303 ページ）を参照してください。

ステップ 9 スキャンをインポートするには、OTDR スキャンのインポート （303 ページ）を参照してください。

ステップ 10 定義した一定の間隔で OTDR スキャンを実行するようにスケジュールするには、OTDR スキャンの繰り返しのプロビジョニング （302 ページ）を参照してください。

OTDR ポート値の設定

OTDR スキャンでは、各セクターの TNCS カードのデフォルト設定を使用するか、必要に応じて設定を変更できます。

ステップ 1 「OTS リンクでの OTDR パフォーマンス テストの実行」トピックの説明に従って、OTDR スキャン ページにアクセスします。

ステップ 2 [設定（Configure）] タブの [デバイス（Device）] ドロップダウンリストからデバイスを選択します。次の列にデフォルト値を持つすべてのセクターがテーブルに一覧表示されます。

- スキャンステータス（Scan Status）：スキャンの累積ステータス
- 損失感度（dB）（Loss Sensitivity (dB)）
- 反射感度（dB）（Reflection Sensitivity (dB)）
- 始点（km）（Start Point (km)）
- 終点（km）（End Point (km)）
- パルス幅（マイクロ秒）（Pulse Width (microseconds)）
- 解像度（m）（Resolution (m)）
- 測定時間（s）（Measure Time (s)）
- ベースライン（Baseline）：デフォルトでは設定されていない
- しきい値損失（dB）（Threshold Loss (dB)）
- しきい値反射（dB）（Threshold Reflection (dB)）
- 繰り返し（Recurrence）：デフォルトでは設定されていない

OTDR の測定範囲は、各セクターに定義された光ファイバ スパンに基づいて分類されます。OTDR 測定セクターは以下のとおりです。

- **ゾーン #1**：距離 0 ～ 1 km
- **ゾーン #2**：距離 0 ～ 25 km
- **ゾーン #3**：距離 0 ～ 80 km
- **ゾーン #4**：全距離
- **エキスパート モード**：カスタム距離設定の場合は、始点パラメータと終点パラメータを編集できます。
- **自動モード（システム検出）**：終点パラメータが自動的に定義されます。

（注） NCS1K デバイスの場合、[Expert Mode] と [Auto Mode (System Detect)] のみがサポートされます。

[設定（Configure）] タブに表示されている距離プロファイルのパラメータは、30 秒ごとに更新されます。

[OTDR設定（OTDR settings）] ページで **[絶対しきい値を有効化（Enable Absolute Threshold）]** を有効にすると、OTDR アルゴリズムのベースラインが無効になり、OTDR 設定で設定した値（絶対イベント損失しきい値（dB）および絶対イベント反射しきい値（dB））が考慮されます。各セクターで設定される実際の値を設定できます。

[絶対しきい値を有効化（Enable Absolute Threshold）] を無効にすると、ベースラインアルゴリズムがアクティブになり、絶対しきい値ではなく特定のセクター（ゾーン #1、ゾーン #2 など）の正しいアラームしきい値を取得できます。

ステップ 3 デバイスの OTDR 設定を変更するには、[デバイスのOTDR設定（Device OTDR Settings）] ハイパーリンクをクリックします。OTDR 設定の詳細については、光インターフェイスのプロビジョニング （457ページ）の「OTDR 自動スキャンの設定」を参照してください。

ステップ 4 セクターのパラメータを編集するには、テーブルで目的の距離プロファイルを選択して [編集（Edit）] をクリックします。ポップアップ ウィンドウが表示されます。

ステップ 5 ポップアップ ウィンドウで、以下を実行できます。

- **ゾーン #1 ～ゾーン #4** の場合は、[損失感度（dB）（Loss Sensitivity (dB)）]、[反射感度（dB）（Reflection Sensitivity (dB)）]、[しきい値損失（dB）（Threshold Loss (dB)）]、[しきい値反射（dB）（Threshold Reflection (dB)）]、および [繰り返し（Recurrence）] の値を編集できます。スキャンの繰り返しの設定については、OTDR スキャンの繰り返しのプロビジョニング （302 ページ）を参照してください。
- **エキスパート モード**の場合は、スキャン ステータスとベースラインを除き、テーブル内のすべての列を編集できます。
- **自動モード**の場合は、[損失感度（dB）（Loss Sensitivity (dB)）]、[反射感度（dB）（Reflection Sensitivity (dB)）]、[しきい値損失（dB）（Threshold Loss (dB)）]、[しきい値反射（dB）（Threshold Reflection (dB)）]、および [繰り返し（Recurrence）] の値を編集できます。[終点（End Point）] の値（OTDR スキャンの光ファイバ スパンの長さ）は自動的に定義されます。スキャンの他の値（[パルス幅（Pulse Width）]、[測定時間（Measure Time）]、[解像度（Resolution）]）は、検出された光ファイバ スパンの長さに基づいて設定されます。

絶対しきい値を有効にするには、[OTDR設定（OTDR Settings）] ページで [絶対光ファイバパスの不合格基準（Absolute Fiber Pass Fail Criteria）] チェックボックスをオンにする必要があります。

ステップ 6 [保存（Save）] をクリックします。

OTDR スキャンの繰り返しのプロビジョニング

選択したポートで OTDR スキャンの繰り返しを設定するには、次の手順を実行します。

ステップ 1 [OTDRスキャン（OTDR Scan）] ページの [設定（Configure）] タブで、[デバイス（Device）] ドロップダウンリストから、定期的なスキャンをプロビジョニングするポートを選択します。

ステップ 2 該当する距離プロファイルを選択し、[編集（Edit）] をクリックします。ポップアップ ウィンドウが表示されます。

ステップ 3 [繰り返し（Recurrence）] 領域で、次のいずれかを選択してスキャン頻度を設定します。

- [なし（None）]：繰り返しは設定されない（デフォルト）。
- [毎週（Weekly）]：毎週繰り返すスキャンをスケジュールするには、ステップ 4（303 ページ） に進みます。
- [間隔（Intervals）]：詳細に指定した定期的なスキャンをスケジュールするには、ステップ 5（303 ページ） に進みます。

ステップ 4 [曜日（on）] ドロップダウンリストから希望する曜日を選択し、時間と分を入力します。

ステップ 5 0 ～ 365 の範囲で目的の日数を選択し、時間と分を入力します。

ステップ 6 [保存（Save）] をクリックします。

OTDR スキャン結果のエクスポート

スキャン結果をローカル マシンにエクスポートできます。

ステップ 1 エクスポートファイルを作成するスキャンを選択します。

ステップ 2 [Export Scans] アイコンをクリックします。

エクスポートしたファイル（.sor 形式）がローカル マシンにダウンロードされます。

OTDR スキャンのインポート

スキャン結果をローカルからインポートできます。

ステップ 1 [Import Scans] アイコンをクリックします。

[Import Scan (.sor)] ウィンドウが表示されます。

ステップ 2 [Browse] をクリックし、インポートする必要がある .sor ファイルを選択します。

ステップ 3 ドロップダウンリストから [Distance Profile] を選択します。

ステップ 4 方向を示す目的の線をクリックして、[Scan Direction] を選択します。

ステップ 5 [インポート（Import）] をクリックします。

Geo マップでの OTDR スキャン結果の表示

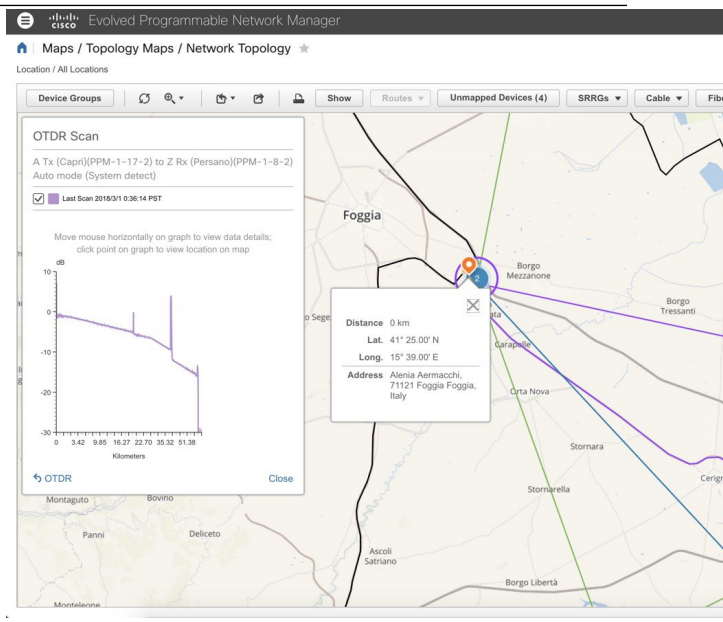
OTDR スキャン結果を Geo マップのコンテキストに表示して、問題が発生している光ファイバのロケーションを特定できます。たとえば、OTDR テストでリンク エンドポイントから 20 km の集中損失が報告された場合、その地理的な位置をマップ上で可視化できます。

前提条件：

- 光ファイバを Geo マップ上に表示するには、光ファイバ データと座標を含む KML ファイルをインポートする必要があります。を参照してくださいKML ファイルからのロケーション データのインポート （268 ページ）。
- OTDR スキャンを実行する OTS リンクが光ファイバに関連付けられている必要があります。光ファイバへのリンクの関連付け （266 ページ）を参照してください。
- A 側デバイスと Z 側デバイスが Geo マップにマッピングされている必要があります。Geo マップへのマップされていないデバイスの配置 （260 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	OTDR スキャンを起動します。	
ステップ 2	スキャンパラメータを定義してスキャンを実行します。	
ステップ 3	[Geoマップで表示（View on Geo Map）] をクリックします。	Geo マップが開きます。OTDR スキャン結果のグラフが左側に表示されます。Geoマップがズームされ、関連するデバイス、リンク、および光ファイバ（紫色で強調表示）が表示されます。
ステップ 4	OTDR スキャン結果のグラフ内のポイントをクリックします。	Geoマップの光ファイバ上の正確な位置にロケーション アイコンが表示され、光ファイバに沿った距離（km）、正確な座標、住所など、ロケーションに関する情報がポップアップ パネルに表示されます。 （注） 正確なロケーションを計算できない場合、ロケーション アイコンは、正確なロケーションの特定の半径内に収まるおおよその位置を示します。ポップアップ パネルに半径（km）が表示され、マップ内のロケーションアイコンを囲む円が、正確なロケーションの半径内に収まるおおよその位置を示します。

	コマンドまたはアクション	目的
		
ステップ 5	必要に応じて OTDR スキャン ページに戻るには、OTDR スキャン結果のグラフの下にある [OTDR] リンクをクリックします。	

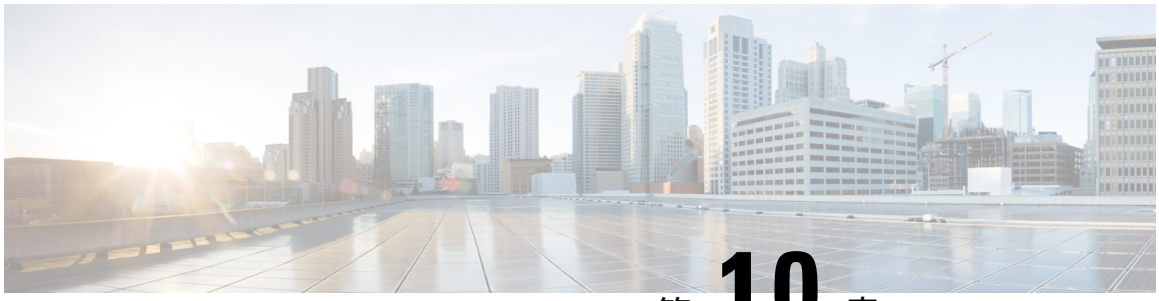
レポートを使用したネットワーク パフォーマンスのモニター

Cisco EPN Manager は、ネットワークのパフォーマンスをモニターするのに役立つさまざまなレポートを提供します。次に例を示します。

- 環境温度、CPU とメモリの使用率
- インターフェイス エラーと破棄
- キャリア イーサネット デバイスの場合：IPSLA イーサネット OAM、PWE3、QoS、およびその他の CE レポート
- 光デバイスの場合：イーサネット、OTN、SDH/SONET、およびその他の光レポート

パフォーマンス レポートを実行すると、データベースに保存されている履歴データが取得されます。レポートには、Cisco EPN Manager が収集するように設定されているデータ、つまりモニターリングポリシーを使用して収集およびモニターされるデータのみが表示されます。（イベントおよびアラーム関連のレポートではモニターリング ポリシーを有効にする必要はありません。そのデータは自動的に収集されます。）さまざまなレポートに対してどのモニターリング ポリシーを有効にする必要があるかについては、使用可能なレポート（356ページ）を参照してください。

（注） レポートの生成中に、最後のサンプルが省略されることがあります。これは、レポート生成時間の後にサンプルが DB に挿入されたためです。これを回避するには、**/opt/CSCOlumos/conf/ReportExportSettings.properties** ファイルを編集して、任意のレポートのオフセットを定義します。



第 10 章

アラームとイベントのモニターリング

アラームおよびイベントとは

イベントとは、特定の時点で発生する個別のインシデントです（ポートステータスの変更、デバイスが到達不能になるなど）。イベントは、ネットワーク内のエラー、障害、または例外的な状況を示す場合があります。また、イベントは、それらのエラー、障害、または状況のクリアを示す場合もあります。イベントには重大度が関連付けられています（これは、アラーム重大度レベルの変更 （1079 ページ）の説明に従って調整できます）。

アラーム は、1 つ以上の関連イベントへの Cisco EPN Manager 応答です。特定のイベントだけがアラームを生成します。アラームには、状態（クリア済みまたはクリアされていない）と重大度（クリティカル、メジャー、マイナーなど）があります。アラームは、最新のイベントの重大度を継承します。クリアイベントが生成されるまで（またはアラームが手動でクリアされるまで）、アラームは開いたままです。

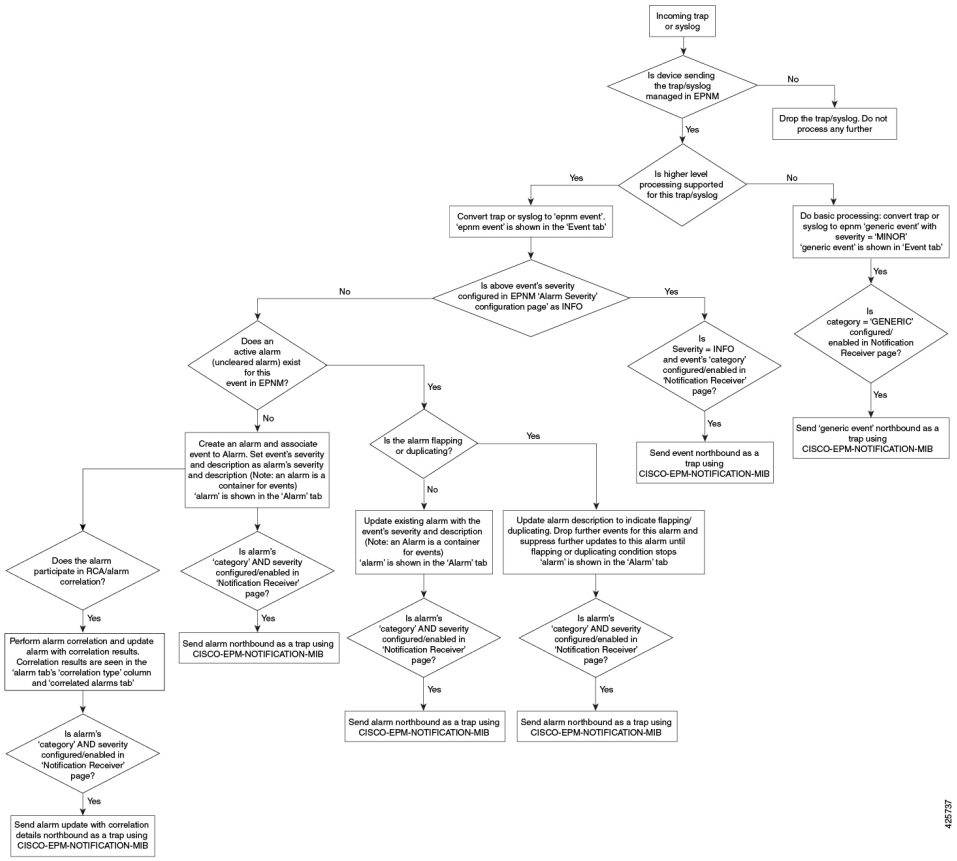
関連トピック

アラームおよびイベントはどのように作成および更新しますか。 （308 ページ）
アラームの確認とクリア （330 ページ）
イベントとアラームのバッジと色の解釈 （318 ページ）

アラームおよびイベントはどのように作成および更新しますか。

Cisco EPN Manager は、IPv4 と IPv6 の両方のデバイスの SNMP トラップ、syslog、および TL1 メッセージを処理します。これは、これらのイベントに対する応答方法を決定するイベントカタログを維持します。以下のフローチャートは、これらのアラームやイベントの処理方法を表します。

図 *8 :* アラーム処理フローチャート



Cisco EPN Manager は、イベントを処理するときに次の一般的手順を実行します。

1. 受信した SNMP トラップ、syslog、または TL1 メッセージについて、イベント カタログを確認して、（一般的な処理ではなく）上位レベルの処理が必要かどうかを確認します（raw イベントを調べ、事前定義済みのパターンがないかを確認することにより）。
   - raw イベントをカタログに一致させることができない場合、イベントは、汎用イベントと見なされ、一般的な処理が行われます。汎用イベントはGUIに表示され、通知で転送できます。（汎用イベント処理は無効にできます。汎用トラップおよびSyslogの処理の無効化および有効化（1088ページ）を参照）。これにより、Cisco EPN Manager が受信したトラップおよび syslog が破棄されないようになります。つまり、一般的な処理が行われて汎用イベントが作成されるか、上位レベルの処理が行われてアラームや処理済みイベントが作成されるかのいずれかになります。
   - raw イベントをカタログに一致させることができる場合、raw イベントは上位レベルの処理の対象と見なされ、Cisco EPN Managerによって、処理済みイベントが重大度および（場合によっては）アラームとともに作成されます。
2. イベントの原因となっているデバイスおよびデバイス コンポーネントを特定します（イベントの場所を特定します）。

3. サポートされているイベントによってインベントリ収集がトリガーされるかどうかをチェックします。

   一部のイベントには、収集が必要な情報を Cisco EPN Manager に指示する特定のルールがあります。詳細については、次を参照してください。インベントリはどのように収集されていますか。（68 ページ）

4. イベントの重大度が [情報（INFO）] または [クリア済み（CLEARED）] かどうかを確認します。

   - [情報（INFO）] または [クリア済み（CLEARED）] の場合、Cisco EPN Manager はイベントを保存し、GUI に表示します。
   - 他の重大度の場合、Cisco EPN Manager は新しいアラームを作成する必要があるかどうかを評価します（次のステップ）。

5. アラームがすでに存在するか、新しいアラームを作成する必要があるかどうかを確認します。

   - アラームが存在する場合、Cisco EPN Manager は、イベントを既存のアラームに関連付けます。アラームの重大度が、新しいイベントの重大度に対応するように変更され、アラームのタイム スタンプが更新されます。これがクリア イベント（リンク アップ イベントなど）の場合、アラームが作成されます。

   （注） 場合によっては、デバイスがクリアアラームを生成しないことがあります。管理者は、アラームの自動クリア間隔の変更（1081 ページ）の手順に従って、アラームの自動クリア間隔を設定する必要があります。

   - アラームが存在しない場合、Cisco EPN Manager は新しいアラームを作成し、これにイベントと同じ重大度を割り当てます。

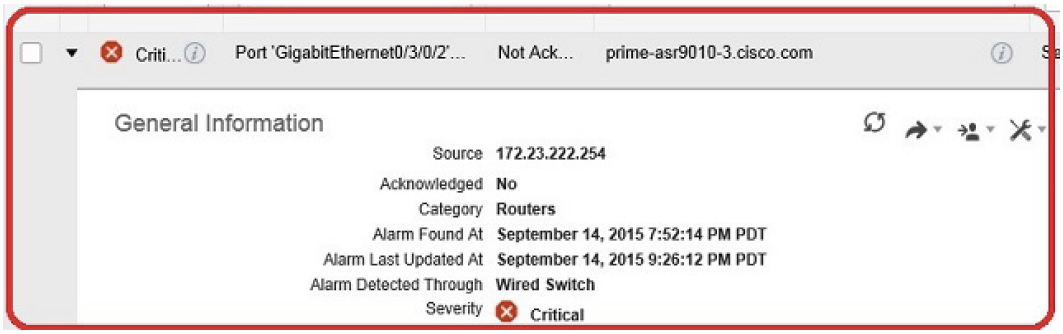
6. 新規または既存のアラームを他のアラームに関連付けることができるかどうかを確認します。（アラームは、イベントではなく、他のアラームに関連付けられていることに注意してください）関連付けることができる場合、Cisco EPN Manager によって次のことが実行されます。

   - 原因となっているアラームを**根本原因アラーム**として特定します。
   - 結果として生じたアラームを**症状アラーム**として特定します。

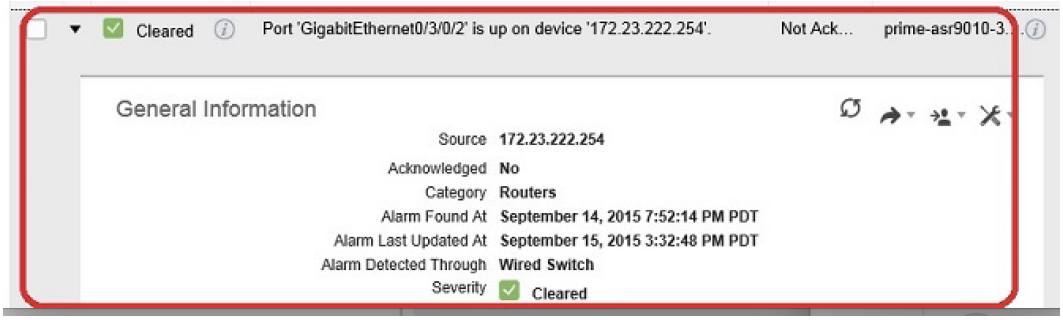
   関連付けられたアラームでクリアされていないものを特定するには、[アラームおよびイベント（Alarms and Events）] テーブルの [関連付けられたアラーム（Correlated Alarms）] タブを確認します。これらの種類のアラームの詳細については、根本原因と相関アラームを表示する（326 ページ）を参照してください。

例：リンク ダウン アラーム

この例では、Cisco EPN Manager はデバイスからリンク ダウン トラップを受信してリンク ダウン イベントを生成します。ポートが動作していないため、Cisco EPN Manager はリンク ダウン アラームも生成します。



Cisco EPN Manager はデバイスからリンク アップ トラップを受信すると、リンク アップ イベントを生成してアラームをクリアします。



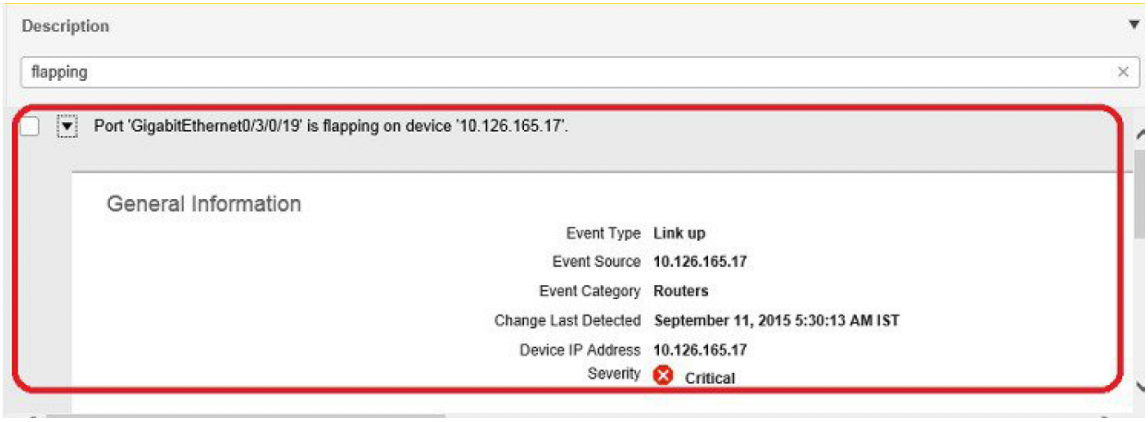
ポートがメンテナンスのためにダウンしているか、またはネットワーク管理者によって無効にされている場合、Cisco EPN Manager は重大度が MINOR のリンクダウンアラームを生成します。このアラームの重大度を変更するには、**[システム設定（System Settings）] > [アラーム設定（Alarm Settings）] > [アラームの重大度と自動消去（Alarm Severity and Auto Clear）]**で [リンクダウン（管理者ダウン）（Link down(admin down)）] フラグを変更します。詳細については、「アラーム重大度レベルの変更 （1079 ページ）」を参照してください。

フラッピング イベントとフロー制御

フラッピングとは、同じアラームに関連するイベント通知が連続して大量に発生することです。障害によってイベント通知が繰り返された場合に起きる可能性があります（コネクタの取り付けが緩いケーブルなど）。同じタイプの複数のイベントが同じソースに関連付けられており、短期間に繰り返されている場合、フラッピングイベントとして識別されます。Cisco EPN Manager によってフラッピングイベントのアラームが生成されます。このアラームは、300 秒以内に同じイベントが 5 回発生した場合に生成されます。インターフェイス ダウン、インターフェイス アップ、インターフェイス ダウン、インターフェイス アップ、インターフェイス ダウンなどの順番の 5 つのオカレンスが考えられます。

フラッピングイベントのアラームが生成されると、デバイスは継続的な同期状態になります。これにより、デバイスでサービスプロビジョニングやOAMなどのデバイス設定を展開できなくなります。ところがCisco EPN Managerの場合、モニター対象デバイスでフラッピング アラームが発生すると、Cisco EPN Managerによってこのアラームが検出され、デバイスのフラッピング状態がクリアされるまでアラームの更新が停止されます。

フラッピングイベントとして検出されたアラームは、終了条件（300秒以内に同じイベントが発生しなかった場合にアラームがクリアされる）に基づいてクリアされます。これにより、イベントのフローを制御してデバイス同期の不要なトリガーを回避できます。



サポートされるイベント

Cisco EPN Managerでサポートされているイベントの詳細については、次のドキュメントを参照してください。

- Cisco Evolved Programmable Network Managerのサポート対象トラップ
- Cisco Evolved Programmable Network Managerのサポート対象Syslog
- Cisco Evolved Programmable Network Managerのサポート対象TL1メッセージ

サポートされていないイベントの処理方法については、イベントの表示（汎用イベントを含む）（334ページ）を参照してください。

アラームとイベント管理の設定

- アラームとイベントの表示設定のセットアップ（313ページ）
- アラーム サマリーのカスタマイズ（316ページ）

（注） アドバンス ユーザーは、Cisco EPN Manager の Representational State Transfer（REST）API を使用して、デバイスの障害情報にアクセスすることもできます。API の詳細については、Cisco EPN Manager ウィンドウの右上にある ⚙ をクリックし、**[ヘルプ（Help）]** > **[APIヘルプ（API Help）]** を選択します。

アラームとイベントの表示設定のセットアップ

Cisco EPN Manager の [アラーム（Alarms）] および [イベント（Events）] テーブルには、デフォルトで最後の 4000 個のアラームまたはイベントが表示されます。Cisco EPN Manager は、キャッシュ内で使用可能な情報のみを表示できます（4000 未満の場合もあります）。4,000 を超えるアラームまたはイベントを表示する場合は、テーブルの上にある [アラーム履歴の表示（Show Alarm History）] をクリックします。

（注） 4,000 のアラームとイベントの一覧には、表示されないクリアされたアラームも含まれています。開いているすべてのアラームを表示するには、**[アラーム履歴の表示（Show Alarm History）]** をクリックします。

Cisco EPN Manager ウィンドウの右上にある ⚙ をクリックし、[マイプリファレンス（My Preferences）] を選択すると、次のアラームおよびイベントの表示をカスタマイズできます。変更を加えたら、[保存（Save）] をクリックして新しい設定を適用します。確認済み、クリア済み、割り当て済みアラームを表示するかどうかなどのその他の設定は、管理者によってグローバルに制御されます。（確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する （1076 ページ） を参照）。

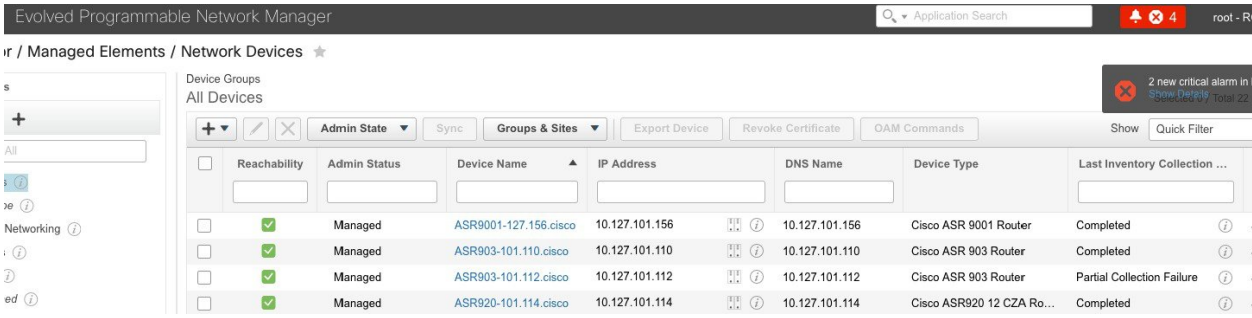
ユーザー プリファレンス設定	説明
[アラームおよびイベント（Alarms & Events）] ページの自動更新	[アラームおよびイベント（Alarms and Events）] ページの自動更新を有効または無効にします。有効にすると、**[アラームのまとめ（Alarm Summary）] のアラーム数を更新**の設定に従ってページが更新されます。
[アラームのまとめ]のアラームカウントを___分/秒ごとに更新（Refresh Alarm count in the Alarm Summary every ___ minutes/seconds）	[アラームのまとめ（Alarm Summary）] のアラーム カウントの更新間隔を設定します（デフォルトは 1 分です）。（アラーム サマリーのカスタマイズ （316 ページ） を参照）。

ユーザー プリファレンス設定	説明
[アラームおよびイベント（Alarms & Events）] ページの [アラームバッジング（Alarm Badging）] の有効化	ユーザーが [アラームバッジング（Alarm Badging）] を有効にすると、**[モニター（Monitor）] > [モニターリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms & Events）]** ページでデバイス グループの横にアラーム重大度のアイコンが表示されます。
[アラーム（Alarm）]の有効化 [確認（Acknowledge）] [警告メッセージ（Warning Message）]	（注） この設定は、[確認済みのアラームを非表示（Hide Acknowledged Alarms）] も有効になっている場合にのみ設定できます。その設定はデフォルトで無効になっています（前の表を参照）。 ユーザーがアラームを選択して **[ステータスの変更（Change Status）] > [確認（Acknowledge）]** を選択したときに、次のメッセージが表示されないようにします。 **「警告：今このアラームを確認すると、7日以内に元のイベントが再び発生した場合は、このアラームは生成されません。（Warning: This alarm will not be generated, if the original event recurs again, within next 7 days, as it is acknowledged now.）」「確認せずにアラームをクリアすると、イベントが再び発生した場合にアラームが生成されます。（Clearing the alarm instead of acknowledging will cause the alarm to be generated if the event recurs again.）」「アラーム確認を続行しますか。（Proceed with alarm acknowledgment?）」**
「この状態のすべてをクリア」に対する確認プロンプトの無効化	ユーザーがアラームを選択して **[ステータスの変更（Change Status）] > [この状態のすべてをクリア（Clear all of this condition）]** を選択したときに、次のメッセージが表示されないようにします。 **「この状態のすべてのアラームをクリアしてよろしいですか。（Are you sure you want to clear all alarms of this condition?）」** （デフォルトでは無効）

ユーザー プリファレンス設定	説明
「この状態のすべてをクリア」に対する「重大度を [情報（Information）] に設定」プロンプトの無効化	ユーザーがアラームを選択して **[ステータスの変更（Change Status）] > [この状態のすべてをクリア（Clear all of this condition）]** を選択したときに表示される次のメッセージを無効化します。 **「選択したアラームの状態の重大度を[情報（Information）]に設定しますか。（Do you want to set the severity for the selected alarm's condition to Information?）」** **「警告：これはシステム全体の変更で、この状態に関する今後のアラームが作成されなくなります。（WARNING: This is a system-wide change that will prevent creation of future alarms of this condition.）」「この変更は、[システム設定（System Settings）]の[重要度設定（Severity Configuration）]ページで元に戻すことができます。（You can undo this change on the Severity Configuration page under System Settings.）」** （デフォルトでは無効） （注） 十分な権限を持つユーザーは、確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する（1076ページ）の手順を使用して重大度を元の値にリセットできます。
[アラームのまとめ（Alarm Summary）] ツールバーのアラーム カテゴリの選択	[アラームのまとめ（Alarm Summary）] に表示される内容を管理します（アラーム サマリーのカスタマイズ （316 ページ） を参照）。
特定の状態のアラームをすべてクリアする場合、状態の重大度を常に [情報（Information）] に設定する	ユーザーがアラームを選択し、**[ステータスの変更（Change Status）] > [この状態のすべてをクリア（Clear all of this condition）]** を選択した場合。（デフォルトでは無効）
新規の重大なアラームカウントの通知の有効化	重大なアラームのカウントを表示する通知ポップアップを有効にします。このカウントは、[アラームのまとめ（Alarm Summary）] の [アラーム カウントの更新（Refresh Alarm count）] に設定されている間隔（アラーム サマリーのカスタマイズ（316ページ）を参照）に応じてアラーム間隔が更新されると更新されます。未処理の重大なアラームのみが表示されます。

重大なアラーム通知の表示

ネットワーク内の重大なアラームのカウントは、すべてのページに通知ポップアップとして表示されます。カウントの更新は 1 分ごと、または [マイ設定（My Preferences）] ページの設定に応じて一定の間隔で行われます。



[詳細の表示（Show Details）] ハイパーリンクをクリックすると、**[モニター（Monitor）] > [モニターリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] > [アラーム（Alarms）]** ページに重大なアラームの一覧が表示されます。

（注） 未処理の重大なアラームのみがカウントおよび表示されます。

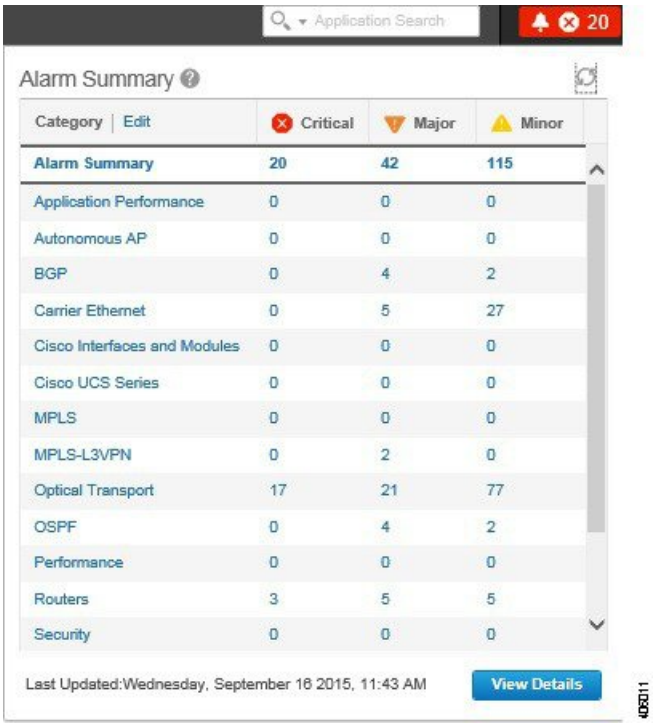
通知はデフォルトでは有効になっていないため、[自分の環境設定（My Preferences）] ページから有効にする必要があります。重大なアラーム カウントの通知を有効にする詳しい方法については、アラームとイベントの表示設定のセットアップ （313 ページ）を参照してください。

アラーム サマリーのカスタマイズ

表示するアラーム カテゴリを指定できます。

- Cisco EPN Manager [Cisco Prime Infrastructure] タイトル バーのアラーム カウント（ベル）では、関心のあるアラーム カウントを視覚的に容易に確認できます。
- アラーム カウントをクリックしたときに起動する [アラームのまとめ（Alarm Summary）] ポップアップ ウィンドウでは、次の図に示すように、アラーム カウントを重大度ともに視覚的に容易に確認できます。

（注） EPNM を使用している Web ブラウザでポップアップブロッカーが無効になっていることを確認します。



この情報をカスタマイズするには、次の手順を実行します。

ステップ 1 [アラームのまとめ（Alarm Summary）] ポップアップ ウィンドウの左上にある [編集（Edit）] をクリックします。これにより、[マイ プリファレンス（My Preferences）] が開きます。また、Web の GUI ウィンドウの右上にある ⚙ をクリックし、[マイ プリファレンス（My Preferences）] を選択しても、このページを開くことができます。

ステップ 2 [アラームおよびイベント（Alarms & Events）] タブをクリックします。

ステップ 3 [アラームのまとめ（Alarm Summary）] の更新間隔を変更するには、[[アラームおよびイベント]ページと[アラームのまとめ]のアラームカウントを次の間隔で更新（Refresh Alarms & Events page and Alarm count in the Alarm Summary every）] ドロップダウンリストから数値を選択します。

ステップ 4 [アラームのまとめ（Alarm Summary）] に表示する情報を指定するには、[アラームカテゴリ（Alarm Categories）] 領域に移動します。**[表示するデフォルトカテゴリ（Default category to display）]** ドロップダウンリストから **[アラームのまとめ（Alarm Summary）]** を選択します。対応するチェックボックスを選択または選択解除して、必要なアラーム カテゴリを有効または無効にします。

ステップ 5 [保存（Save）] をクリックして、[自分の環境設定（My Preferences）] ウィンドウで行った変更を確定します。

イベントとアラームのバッジと色の解釈

ネットワークに問題がある場合、Cisco EPN Manager は問題が発生している要素にアラームまたはイベントのアイコンを表示して、問題をフラグします。アラーム重大度アイコン（318ページ）にアイコンとその色を示します。

アラーム重大度アイコン

次の表に、Web GUI のさまざまな部分に表示されるアイコンのアラームの色とその重大度を示します。

重大度アイコン	説明	カラー
	クリティカル アラーム	赤
	メジャーアラーム	オレンジ
	マイナーアラーム	黄
	警告アラーム	ライト ブルー
	アラームはクリア済み。正常、OK	緑
	情報アラーム	青
	不確定アラーム	暗い青色

アラームの検索および表示

アラームを表示するには、**[モニター（Monitor）]** > **[モニターリングツール（Monitoring Tools）]** > **[アラームおよびイベント（Alarms and Events）]** に移動します。[アラーム（Alarms）] タブでは、アラームがそれぞれのサブタブの下のテーブルに一覧表示されます。これらの各テーブルには、デフォルトの列のセットが表示されます。デフォルトで表示されない列を有効にするには、テーブルの右上隅の⚙をクリックして、列を選択します。

（注） [アラーム（Alarms）] タブのすべてのタブを正しく表示するには、Internet Explorer 11 ではなく Microsoft Edge ブラウザを使用することをお勧めします。Dojo ウィジェットには Internet Explorer 11 の既知の制限があるためです。Microsoft Internet Explorer (IE) 11.0 は廃止されます。

次の表で説明するように、表示されるアラームテーブルから特定のアラームを検索することができます。表の下に、カスタマイズ（プリセット）したフィルタを作成して保存する方法を説明します。アラームの詳細については、アラームの詳細を表示する （327ページ）を参照してください。

（注） デフォルトでは、認知済みアラームとクリア済みアラームは検索対象となりません。この動作は、システム管理者が制御します。参照先 確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する （1076 ページ）

検索対象のアラーム	**[モニター（Monitor）]>[モニターリング ツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]の順に選択した後の操作**
特定のデバイスによって生成されたアラーム	アクティブなアラームを確認する場合、デバイス名の横にある「i」アイコンをクリックしてデバイスの 360 度ビューを表示し、[アラーム（Alarms）]タブをクリックします。クリアされたアラームを確認する場合は、表「アラームおよびイベント」を参照してください。 （注） • NCS 2000 デバイスの場合、一時的な状態はアラームとして処理され、[アラーム（Alarms）]テーブルに表示されます。***[i]*** をクリックして、[インターフェイス360（Interface 360）] ビューで関連するポートに移動します。この機能は、**[アラームのその他の設定（Alarm Other Settings）]** ページで **[一時的な状態アラームの有効化（Enable Transient Condition Alarms）]** チェックボックスをオンにした場合にのみ有効になります。詳細については、「アラームクリーンアップ、表示、および電子メールオプションの指定（1071 ページ）」を参照してください。 • SVO デバイスの場合、デバイス名のハイパーリンクをクリックすると、SVO UI が相互起動します。SVO デバイスのハイパーリンクは、**[その他の設定（Alarm Settings）]** ページで **[SVO へのアラームの相互起動を有効にする（Enable Alarms Cross Launch to SVO）]** チェックボックスをオンにした場合にのみ有効になります。詳細については、アラームクリーンアップ、表示、および電子メールオプションの指定（1071 ページ）を参照してください。 クリアされたアラームまたは相関付けられたアラームを確認する場合、該当するタブをクリックし、[場所（Location）]列にデバイス名またはコンポーネントを入力します。ワイルドカードを使用できます。 特定のデバイスについて、シャーシ ビューを使用してデバイスのアラームを確認することもできます。シャーシ ビューでのアラームの表示 （125 ページ）を参照してください。

検索対象のアラーム	**[モニター（Monitor）]>[モニターリング ツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]の順に選択した後の操作**
特定の回線/VCによって生成されたアラーム	**1.** デバイス名の横にある [i] アイコンをクリックして [デバイス360（Device 360）] ビューを表示し、[回線/VC（Circuit/VC）] タブをクリックします。 **2.** 回線/VC 名の横にある [i] アイコンをクリックして [回線/VC 360（Circuit/VC 360）] ビューを表示し、[アラーム（Alarms] タブをクリックします。 回線/VC のアラーム情報を取得する別の方法については、回線/VC のエラーのチェック （839 ページ）を参照してください。
ネットワーク内のすべてのアラーム	[アラーム履歴の表示（Show Alarm History）] リンクをクリックします。
自分に割り当てられているアラーム	[表示（Show）] ドロップダウン フィルタ リストをクリックし、[自分への割り当て（Assigned to me）] を選択します。このフィルタは、[クリア済みアラーム（Cleared alarms）]および[相関アラーム（Correlated alarms）] タブでも使用できます。
未割り当てのアラーム	[表示（Show）] ドロップダウン フィルタ リストをクリックし、[未割り当てのアラーム（Unassigned Alarms）] を選択します。このフィルタは、[クリア済みアラーム（Cleared alarms）] および [相関アラーム（Correlated alarms）] タブでも使用できます。
クリア済みアラーム	[表示（Show）] ドロップダウン フィルタ リストをクリックし、[クリア済みアラーム（Cleared Alarms）] を選択します。このフィルタは、[クリア済みアラーム（Cleared alarms）] および [相関アラーム（Correlated alarms）] タブでも使用できます。
ネットワークアラーム	**[アラーム（Alarms）]** タブの下の **[ネットワークアラーム（Network Alarms）]** タブをクリックして、ネットワークに影響するすべてのアラームを表示します。 このタブは、**[アラームのその他の設定（Alarm Other Settings）]** ページで **[ネットワークアラームビューの有効化（Enable Network Alarms View）]** チェックボックスをオンにした場合にのみ有効になります。詳細については、「アラームクリーンアップ、表示、および電子メールオプションの指定 （1071 ページ）」を参照してください。

検索対象のアラーム	[モニター（Monitor）]>[モニターリング ツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]の順に選択した後の操作
Cisco EPN Manager タイムスタンプに基づく最新のアラーム	アクティブなアラームを確認する場合：: • 過去 30 分間に発生したアラーム：[表示（Show）] ドロップダウン フィルタをクリックし、過去 5 分、15 分、または 30 分を選択します（**CEPNM タイムスタンプ**）。 • 過去 24 時間に発生したアラーム：[表示（Show）] ドロップダウン フィルタをクリックし、過去 1 時間、8 時間、または 24 時間を選択します（**CEPNM タイムスタンプ**）。 • 過去 7 日間に発生したアラーム：[表示（Show）] ドロップダウン フィルタをクリックし、過去 7 日間（**CEPNM タイムスタンプ**）を選択します。 これらのフィルタは、クリアされたアラームと相関付けられたアラームにも使用できます。クリア済みアラームと相関アラームではデバイス タイムスタンプによるフィルタリングがサポートされていないため、フィルタに（**CEONM タイムスタンプ**）サフィックスはありません。（**CEPNM タイムスタンプ**）と（**デバイス タイムスタンプ**）の詳細については、デバイス タイムスタンプと CEPNM タイムスタンプ（324 ページ）を参照してください。
デバイスのタイムスタンプに基づく最新のアラーム	前の行と同じ手順ですが、（**CEONM タイムスタンプ**）サフィックスが付いたフィルタを選択します。このフィルタは、クリア済みアラームまたは相関アラームを検索する場合はサポートされません。
デバイスのグループ、シリーズ、またはタイプによって生成されたすべてのアラーム	左側のナビゲーション ペインで、グループを選択します。このフィルタは、クリアされたアラームと相関付けられたアラームにも使用できます。
カスタマイズされたフィルタを使用したアラーム	高度なフィルタを作成して保存します（この表の後に続く手順を参照）。

[**Show**] ドロップダウンリストのクイック フィルタまたは高度なフィルタを使用してデータをフィルタリングし、特定のアラームを検索することもできます。

アラームテーブルのデータのフィルタリング

特定のアラームを検索するには、[表示（Show）] ドロップダウンリストのクイックフィルタまたは高度なフィルタを使用してデータをフィルタリングできます。クイック フィルタでは、列

の上部に入力したテキストに従って、列に表示されるコンテンツが絞り込まれます。高度なフィルタを使用すると、「次を含まない（Does not contain）」、「等しくない（Does not equal）」、「次で終わる（Ends with）」、「が空である（Is empty）」などの複数の演算子を使用してフィルタを適用し、テーブル内のデータを絞り込むことができます。また、ユーザー定義フィルタを作成することもできます。これを保存すると、[表示（Show）] ドロップダウンメニューに追加されます。

EPNM でローカルに作成されたルートユーザーと管理者ユーザーには、他のユーザーと共有できるパブリックフィルタを作成するオプションがあります。また、（どちらかによって作成された）パブリックフィルタを編集および削除することもできます。パブリックフィルタを作成するオプションは、ルートユーザーと管理者ユーザーのみが使用できます。他のユーザーにはこのオプションがなく、デフォルトではプライベートユーザー定義フィルタのみを作成できます。

ユーザー定義フィルタを作成するには、次の手順を実行します。

ステップ 1 アラームの拡張テーブルの上にある [表示（Show）] をクリックし、[高度なフィルタ（Advanced Filter）] を選択します。

ステップ 2 [高度なフィルタ（Advanced Filter）] データ ポップアップ ウィンドウで、高度なフィルタ条件を入力し、[名前を付けて保存（Save As）] をクリックします。

ステップ 3 [フィルタの保存（Save Filter）] ダイアログボックスで、フィルタの名前を入力して [保存（Save）] をクリックします。

a) **ルートユーザーと管理者ユーザーのみ**：表示されるダイアログボックスで、次のいずれかのオプションを選択します。

- フィルタを他のユーザーと共有する場合は、[パブリック（Public）] を選択します。新しく作成されたフィルタは、[高度なフィルタ（Advanced Filters）] の下の [表示（Show）] ドロップダウンリストに追加され、他のユーザーが使用できます。
- フィルタを他のユーザーと共有しない場合は、[プライベート（Private）] を選択します。新しく作成されたフィルタは、[高度なフィルタ（Advanced Filters）] の下の [表示（Show）] ドロップダウンリストに追加されますが、他のユーザーには表示されません。

（**ルートユーザーおよび管理者ユーザーのみ**）：ユーザー定義フィルタを編集または削除するには、**[表示（Show）] > [ユーザー定義フィルタの管理（Show Manage User Defined Filters）]** をクリックし、ユーザー定義フィルタを選択して [編集（Edit）] または [削除（Remove）] をクリックします。

[アラーム（Alarms）] テーブルでのカスタム値用のユーザー定義フィールド（UDF）の作成

独自のフィールドを作成し、これらのフィールドにカスタム値を定義して、[アラーム（Alarms）] テーブルに表示できます。たとえば、特定のアラームに顧客名のラベルを設定します。ユー

ザー定義フィールドを作成し、値を割り当てると、[アラーム（Alarms）] テーブルでこれらの値を使用してアラームを検索できます。

（注） 設計上、高度なフィルタはユーザー定義フィールド（UDF）ではサポートされていません。

アラーム用にユーザー定義フィールドを作成するには、次の手順を実行します。

始める前に

ユーザー定義フィールドを有効にするには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [アラームおよびイベント（Alarms and Events）] > [その他の設定のアラーム（Alarm Other Settings）]**に移動し、[アラームのユーザー定義フィールド機能を有効にする（Enable User Defined Field feature for alarms）] チェックボックスをオンにします。

デバイス UDF の通知を有効にするには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [アラームおよびイベント（Alarms and Events）] > [その他の設定のアラーム（Alarm Other Settings）]**に移動し、[通知で送信されるデバイス UDF の有効化（Enable Device UDF to be sent in notifications）] チェックボックスをオンにします。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [全般（General）] > [ユーザー定義フィールド（User Defined Fields）]** に移動します

ステップ 2 [+] アイコンをクリックします。ドロップダウンリストから [アラーム（Alarms）] を選択し、ラベルと説明を入力します。

アラームのユーザー定義フィールドの値を編集するには、次の手順を実行します。

1. **[モニター（Monitor）] > [モニターリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] > [アラーム（Alarms）]** に移動します。
2. テーブルの右上にある設定アイコンをクリックし、[列（Columns）] を選択してからユーザー定義フィールドを選択し、列として表示するユーザー定義フィールドをリストから選択します。
3. 対応するアラームのチェックボックスをオンにし、[UDF の編集（Edit UDF）] をクリックします。
4. ユーザー定義フィールドに必要な値を入力し、[保存（Save）] をクリックします。

デバイス タイムスタンプと CEPNM タイムスタンプ

デバイス タイムスタンプは syslogs メッセージ内に埋め込まれた情報であり、一方 **CEPNM タイムスタンプ**はデバイスからのメッセージが Cisco EPN Manager エンドで受信されるときの時間です。

デバイスでは次の構成が推奨されます。

service timestamps log datetime show-timezone msec year

これらはデバイス タイムスタンプの場合にサポートされている既定のフォーマットであることに注意してください。

- yyyy MMM dd HH:mm:ss.SSS z
- yyyy MMM dd HH:mm:ss z
- MMM dd HH:mm:ss z
- yyyy MMM dd HH:mm:ss.SSS
- yyyy MMM dd HH:mm:ss
- MMM dd HH:mm:ss

フォーマット内の **z** はタイム ゾーンを意味します。

（注） 3 文字のタイム ゾーンのみサポートされており、時間/分オフセットでのタイム ゾーンはサポートされていません。

アラームの追跡とモニターリング

アラームを追跡およびモニターするには、[更新（Refresh）] ドロップダウンリストでアラームの自動更新間隔を 10 秒に設定します。アラームのリストが更新され、最新の 4000 アラームと対応する [アラームID（Alarm ID）] が表示されます。

トポロジ マップでの特定のアラームの表示

[アラーム（Alarms）]テーブルで特定のアラームを選択し、トポロジマップを起動して、マップ上にアラームを表示できます。

ステップ 1 [アラーム（Alarms）]テーブルを表示するには、**[モニター（Monitor）]**>**[モニターリングツール（Monitoring Tools）]** > **[アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 2 [アラーム（Alarms）] タブで目的のアラームを見つけて選択します。

ステップ 3 **[トラブルシュート（Troubleshoot）]** > **[ネットワークトポロジ（Network Topology）]** を選択します。

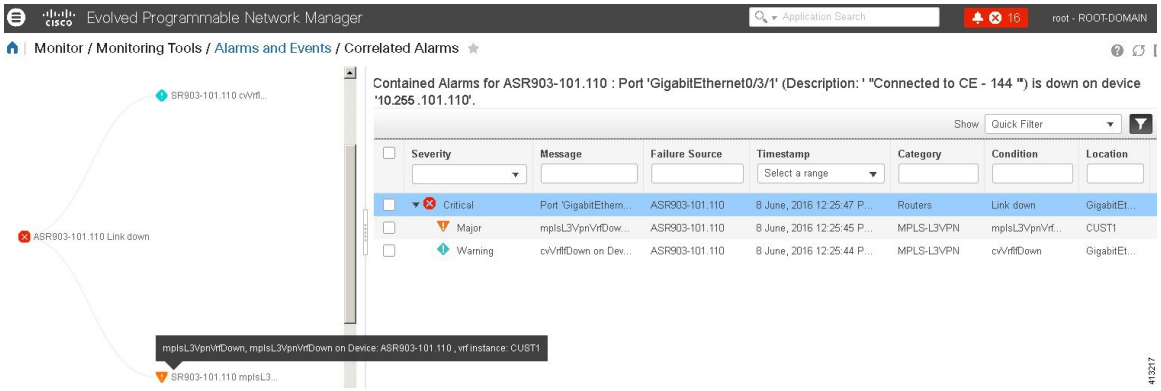
ビューがトポロジ マップに切り替わり、アラーム付きのデバイスがマップでハイライト表示されます。

根本原因と相関アラームを表示する

アラームとアラーム シーケンスの因果関係は、Cisco EPN Manager の相関プロセスによって決まります。相関プロセスをサポートするアラームは、次のとおりです。

- 根本原因アラーム：他のアラームを引き起こすアラーム（「相関」アラーム）。
- 症状アラーム：別のアラームの結果として引き起こされるアラーム（「相関対象」アラーム）。

根本原因アラームと症状アラームは階層状に表示されるため、影響を受けたネットワーク要素を簡単に識別できます。次の図は、未クリアのリンク ダウン アラームが他の 2 つのリンク ダウン症状アラームの根本原因となっている例です。階層でアラームのツールチップを表示するには、アラームにマウスを合わせます。



このビューは、アラーム シーケンスに複数の階層がある場合に特に役立ちます。階層の数に関係なく、すべてのアラーム シーケンスには根本原因アラームが 1 つしかありません。

未クリアの相関アラームを表示する手順は次のとおりです。

ステップ 1 **[モニター（Monitor）] > [アラームとイベント（Alarms and Events）]** を選択します。

ステップ 2 [相関アラーム（Correlated Alarms）] タブをクリックします。

ステップ 3 [相関タイプ（Correlation Type）] 列の をクリックして、アラームに関する詳細情報を新しいビューで表示します。

未クリアの相関アラームは、メインの [アラームおよびイベント（Alarms and Events）] テーブルで確認することもできます。[相関タイプ（Correlation Type）] 列の をクリックして、アラームに関する詳細情報を新しいビューで表示します。

このビューでは、次の操作を実行できます。

1. アラームの確認やクリアなどのアクションを実行する。詳細については、アラームの確認とクリア（330 ページ）を参照してください。
2. 重大度、ステータス、タイム スタンプに基づいてリストをフィルタリングする。

3. テーブルの右上隅にある ⚙ をクリックして、表示する列の一覧を選択する。

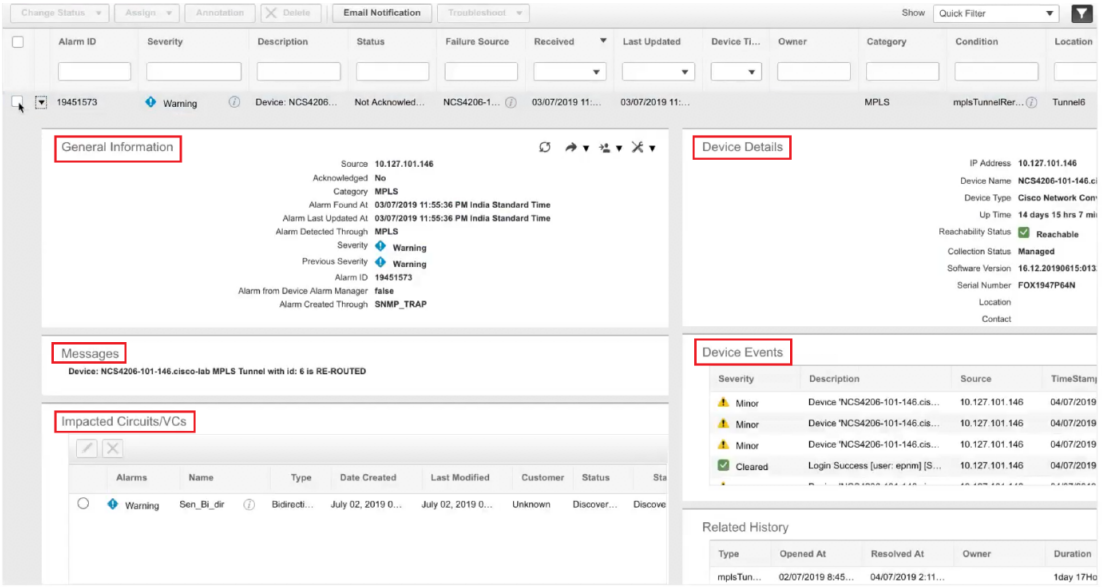
[クリア済み（Cleared）] の相関アラームは、[クリア済みアラーム（Cleared Alarms）] タブに表示されます。未クリアのアラームと同様に、[相関タイプ（Correlation Type）] 列には、そのクリア済みアラームが根本原因アラームまたは症状アラームとして示されます。

トラブルシューティングと詳細なアラーム情報の取得

アラームの詳細を表示する

アラームの詳細を取得するには、それを展開します。[アラーム（Alarms）] リストからこれを行うことができます（**[モニター（Monitor）]**>**[モニターリング ツール（Monitoring Tools）]**>**[アラームおよびイベント（Alarms and Events）]** を選択するか、[アラームのまとめ（Alarm Summary）] ポップアップで [詳細（Details）] をクリックします）。アラームを展開すると、テーブルの自動更新が一時停止されます。丸で囲まれた領域については、この図の下の表で説明します。

図 *9:* アラームの詳細を表示する



General Information：アラームの検出日と最終更新日、現在の重大度と最新の重大度、アラーム ID、およびアラームの検出方法	**Device Details**：管理対象デバイスの名前、アドレス、稼働時間、到達可能性ステータス、収集ステータスなど
Messages：トラップ、syslog、または TL1 メッセージ	**Device Events**：過去 1 時間の最近のデバイス イベント（任意のタイプ、時系列順）
Impacted Circuits/VCs：アラームの影響を受けるキャリア イーサネットまたは光回線/VC	

アクティブ アラームのトラブルシューティング情報の検索

この手順を使用して、アクティブなアラームの発生原因の説明や、そのアラームに対して推奨される対応を把握します。

（注） すべてのアラームにこの情報があるとは限りません。十分な権限を持つユーザーが、ポップアップ ウィンドウに表示される情報を追加または変更できます。アラームのトラブルシューティング テキストのカスタマイズ （1080 ページ）を参照してください。

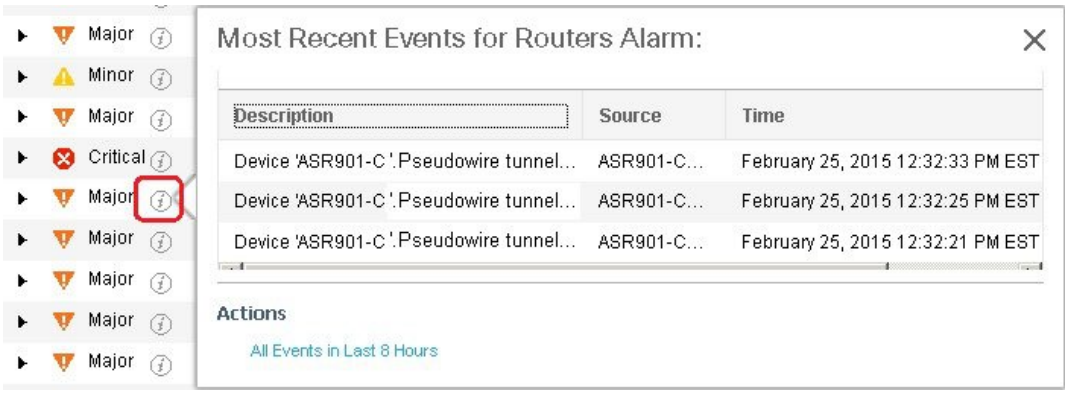
ステップ 1 **[モニター（Monitor）]>[モニターリング ツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]** を選択し、[アラーム（Alarms）] タブをクリックします（インターフェイス アラームの場合は、[アラーム（Alarms）] タブの下の [インターフェイス 360（Interface 360）] ビューからこの情報を取得することもできます）。

ステップ 2 アラームを見つけて [重大度（Severity）] 列の [i] アイコンをクリックし、アラームの説明とトラブルシューティングの推奨アクションが表示されたポップアップ ウィンドウを開きます。

何らかのアクションを取る場合は、そのアクションを文書化することをお勧めします。アラームを選択し、[注釈（Annotation）] をクリックします。

アラームに関連付けられているイベントの検索

アラームに関連付けられているイベントを表示するには、[アラーム（Alarms）] テーブルから [重要度（Severity）] の横にある [i] アイコンをクリックします。



アラームが他のサービスまたはネットワーク要素に影響を及ぼすかどうかを調べる

[アラーム（Alarms）]テーブルには、アラームがネットワークの他の部分に影響するかどうかを示す [影響するサービス（Service Affecting）] 列が含まれています。

（注） サービスに影響を与える情報は、光デバイスのみに表示されます。

- **SA** サービスに影響を与えるアラームであることを意味します
- **NSA** サービスに影響を与えるアラームではないことを意味します

サービスに影響を与える可能性があるすべてのアラームを識別するには、[表示（Show）] ドロップダウンリストから **[Quick Filter]** を選択し、[サービスの影響（Service Affecting）] 列の上にあるフィールドに **SA** と入力します。

どのサービスが影響を受けるを見つける、アラームを展開し、アラームの詳細の影響を受ける回路/VCs 領域で詳細を確認します。

または、[アラームとイベント（Alarms and Events）]ページの [影響を与えるサービス（Service Affecting）] タブから、アラームに影響を与えるすべてのサービスのリストを表示することもできます。このリストには、Cisco EPN Manager によって管理されるすべてのデバイスについて、影響を与えるサービスの情報が含まれています。**[影響を与えるサービス（Service Affecting）]** タブに移動するには、**[モニター（Monitor）]**>**[モニターリングツール（Monitoring Tools）]** > **[アラームとイベント（Alarms and Events）]** を選択し、**[影響を与えるサービス（Service Affecting）]** タブをクリックします。

（注） このタブには、[アクティブなアラームを表示（Showing Active Alarms）] オプションはありません。デフォルトでは、アラームのリスト全体が表示されます。

[アラーム（Alarms）]テーブルには、アラームが他のアラーム（根本原因アラーム）を引き起こしているか、またはアラームが別のアラームの症状（症状アラーム）であるかを示す [相関タイプ（Correlation Type）] 列も含まれています。詳細については、根本原因と相関アラームを表示する （326 ページ）を参照してください。

アラームの確認とクリア

アラームの有効なステータスは、[未確認（Not Acknowledged）]、[確認済み（Acknowledged）]、または [クリア済み（Cleared）] です。

未確認

[未確認（Not Acknowledged）] は、問題が対応されていないことを表します。ネットワーク内の新しい障害状態、または再発したクリア済みの障害状態を示す場合があります。[未確認（Not Acknowledged）] アラームは、確認応答またはクリアされるまで、[アラームおよびイベント（Alarms and Events）] テーブルから削除されません。

確認済み

[確認済み（Acknowledged）] とは、障害状態が認識されて対応されているか、または無視できることを表します。アラームを確認済みステータスに移行することは手動操作であり、その際にアラームのステータスが [確認済み（Acknowledged）] に変わります。確認されたイベントは引き続き未解決とみなされる（つまり、クリアされていない）ので、関連するイベントが再発すると、イベントがアラームに追加されます。

デフォルトでは、確認済みのアラームは [アラーム（Alarms）] リストから削除されません。この動作は、管理者によって制御される [**Hide Acknowledge Alarms**] 設定によって異なります。

確認されたアラームは、[未確認（Not Acknowledged）] ステータスに戻すことができます（たとえば、誤ったアラームを確認した場合など）。

クリア済み

クリア済みとは、障害状態が現在は存在しないことを意味します。アラームがクリアされていても、関連するイベントが繰り返される場合、Cisco EPN Manager は新しいアラームを表示します。アラームはユーザーまたは Cisco EPN Manager システムによってクリアされる場合があります。クリア済みのアラームは [アラーム（Alarms）] リストから削除されます（ただし、[クリア済みのアラーム（Cleared Alarms）] タブにはそれらを表示できます）。

デフォルトでは、クリア済みのアラームは [アラームおよびイベント（Alarms and Events）] ページに表示されません。クリア済みのアラームを [アラームおよびイベント（Alarms and Events）] ページの [アラーム履歴（Alarms History）] テーブルに表示するには、次の手順を実行します。

（注） FRU アラームの生成時にインベントリにロケーション パラメータがない場合、生成されたアラームにはロケーション パラメータがありません。この FRU アラームがクリアされると、アラームにはインベントリ ロケーション パラメータがない可能性があります。

- **[管理（Administration）] > [設定（Settings）] > [システム設定（System settings）]** を選択し、[アラームおよびイベント（Alarms and Events）] を選択します。
- [アラームの表示オプション（Alarm Display Options）] の下にある [クリア済みのアラームを非表示（Hide cleared Alarms）] チェックボックスをオフにします。

[**Clear all of this Condition**] を選択してアラームをクリアすることもできます。この場合は、同じ問題のアラームがすべてクリアされます。その条件を持つすべてのアラームを情報の重大度に変更するように求めるプロンプトが表示されることがあります。これは、関連するイベントが繰り返される場合に新しいアラームが表示されないことを意味します。この設定は慎重に使用する必要があります。

アラームのステータスを変更するには、次の手順を実行します。

ステップ 1 **Monitor > Monitoring Tools > Alarms & Events**を選択します。

ステップ 2 アラームを選択し、[**Change Status**] と該当するステータス（[確認（Acknowledge）]、[未確認（Unacknowledge）]、[クリア（Clear）]、[この条件のすべてをクリア（Clear all of this Condition）]）を選択します。

（注） [**Clear all of this Condition**] により、選択したアラームと同じ条件のすべてのアラームに対してイベントのクリアがトリガーされます。このステータスを選択すると、Cisco EPN Manager は選択したアラーム条件の重大度を [情報（Information）] に変更するかどうかを確認するダイアログを表示します。これにより、Cisco EPN Manager では指定した条件のアラームが作成されなくなります。条件の重大度を後でリセットするには、**Administration > System Settings > Severity Configuration** を選択して重大度を変更します。詳細については、アラーム重大度レベルの変更 （1079 ページ）を参照してください。

ステップ 3 [**Yes**] をクリックして、指定した条件のすべてのアラームをクリアすることを確認します。

サポートされているアラーム クリア メカニズムについて

イベントがクリアされているかどうかにかかわらず、使用可能なアラームが多く存在する状況に直面する場合があります。このような問題が発生した場合に、Cisco EPN Manager でサポートされている解決策の一部を紹介します。

- アラームのデフォルトのクリア：障害がデバイスで解決され、同じデバイスでイベントがトリガーされます。たとえば、デバイス到達可能イベントは、デバイス到達不能イベントをクリアします。次に、これによって、デバイス到達不能アラームがクリアされます。
- アラームの自動クリア：場合によっては、デバイスがクリアアラームを生成しないことがあります。この場合、Cisco EPN Manager は 24 時間（デフォルトの間隔）待機してから、

アラームを自動クリアします。自動クリアの間隔を変更するには管理者権限が必要です。間隔を設定する方法については、アラームの自動クリア間隔の変更（1081 ページ）を参照してください。

- ポートのインベントリ ステータスに基づいたアラームのクリア：デバイスが再起動したり、カードがリロードされたり、RSP フェールオーバーが発生したりすると、そのデバイスのインベントリ収集がトリガーされます。このインベントリ同期中に、Cisco EPN Manager はデバイスの特定のポートの動作状態に基づいて、その特定のポートにある複数のタイプのアラームをクリアします。たとえば、Cisco EPN Manager はデバイスからリンク ダウン トラップを受信すると、動作がダウンしている特定のポートでリンク ダウン アラームを生成します。デバイスの再起動後、ポートの動作状態がアップに変わると、Cisco EPN Manager によってリンク ダウン アラームが自動的にクリアされます。
- デバイスを同期してアラームをクリアする：クリアする未処理のアクティブアラームと存在しないイベントのリストを Cisco EPN Manager が取得するように、デバイスが同期されます。これは、イベント ベースのアラーム/イベント レポート（トラップ/syslog による）とは異なるメカニズムです。同期が完了すると、[アラーム（Alarms）] テーブルが更新されて未処理のアクティブ アラームのみが表示されます。

（注） この機能は、特定のデバイスまたは特定のデバイス機能でのみサポートされます。たとえば、光デバイス、または NCS 4K、NCS 1K などのデバイスの光部分でこの機能がサポートされています。

（注） この機能は、NCS 42xx などの特定のパケット デバイスでもサポートされます。NCS 42xx デバイスでサポートされている syslog の一覧については、『Cisco Evolved Programmable Network Manager Supported Syslogs』スプレッドシートを参照してください。NCS 42xx デバイスの場合、デバイスで設定されているアラーム重大度は、Cisco EPN Manager で設定されているアラーム重大度（**[管理（Administration）] > [システム設定（System Settings）] > [アラームおよびイベント（Alarms and Events）] > [アラーム重大度と自動クリア（Alarm Severity and Auto Clear）]**）を上書きします。この機能は、ASR 9K や 9xx などの他のパケット デバイスではサポートされていません。

- アラームの手動クリア：クリアイベントが欠落している場合、特定のアラームを選択してステータスを [クリア（Clear）] に変更することで、アラームを手動でクリアできます。詳細については、アラームの確認とクリア（330 ページ）の「**クリア済み**」を参照してください。

アラームへの注釈の追加

注釈機能では、自由形式のテキストをアラームに追加できます。テキストはアラーム詳細の[メッセージ（Messages）]領域に表示されます。アラームにテキストを追加するには、[アラームおよびイベント（Alarms and Events）] テーブルでアラームを選択し、[注釈（Annotate）] をクリックしてテキストを入力します。確認応答と同様に、アラームに注釈を付けると、Cisco EPN Managerはユーザー名と注釈のタイムスタンプをアラーム詳細の[メッセージ（Messages）]領域に追加します。

アラームがトリガーされる方法の管理（アラームしきい値）

情報の収集頻度（ポーリング間隔）、問題を示すしきい値、および問題が検出された場合にCisco EPN Manager で情報イベントまたは（ある重大度の）アラームを生成するかどうかをカスタマイズできます。すべてのポリシーにこれらの設定がすべて含まれているわけではありません。たとえば、統計情報だけを収集するポリシーには、しきい値やアラームが関連付けられていない可能性があります。

ステップ 1 **Monitor > Monitoring Tools > Monitoring Policies > My Policies** を選択してから、編集するポリシーを選択します。

ステップ 2 変更するパラメータを検索します。パラメータを検索するには、[パラメータ（Parameters）]テキストボックスに文字列を入力します。

ステップ 3 ポーリング間隔を調整するには、[ポーリング頻度（Polling Frequency）] ドロップダウンリストから新しい間隔を選択します。ポーリングを無効にするには、[**No Polling**] を選択します。パラメータのグループに適用されるポーリング頻度があることに注意してください。グループ間隔を変更すると、そのグループのすべての設定のポーリングが変更されます。ポリシーに、関連付けられたしきい値またはイベントがない場合、Cisco EPN Manager は変更を保存するように求めるプロンプトを表示します。

ステップ 4 しきい値を変更するには、パラメータを展開し、パラメータのドロップダウン リストから値を選択します。

ステップ 5 しきい値を超過した場合に Cisco EPN Manager が何を実行するかを指定するには、パラメータのドロップダウンリストからアラーム値を選択します。指定した重要度のアラームを生成する、情報イベントを生成する、または何もしない（何の対応も指定しない場合）ように Cisco EPN Manager を設定できます。

ステップ 6 次をクリックします。

- **Save and Activate** ポリシーを保存し、選択したデバイスですぐに有効化します。
- **Save and Close** ポリシーを保存し、後で有効にします。

イベントの表示（汎用イベントを含む）

[イベント（Events）]タブには、サポートされているイベントと汎用（サポートされていない）イベントが表示されます。サポートされるイベントは、ネットワークに関する情報に基づいてCisco EPN Managerが生成するイベントです。このネットワーク情報は、デバイスによって生成されたSyslogとトラップ、またはポーリングとインベントリ収集を通じて受信されます。このプロセスについては、アラームおよびイベントはどのように作成および更新しますか。（308ページ）で説明します。汎用イベントは、Cisco EPN Managerが認識しないイベントです。Cisco EPN Managerは、イベントをドロップするのではなく、イベントをマイナー重大度に割り当てます（この重大度はすべての汎用イベントに適用されます。変更するには、アラーム重大度レベルの変更（1079ページ）を参照してください）。必要に応じて、汎用イベントで表示される情報をカスタマイズできます（Web GUIに表示される汎用イベントのカスタマイズ（1088ページ）を参照）。サポートされるイベントについては、サポートされるイベント（312ページ）を参照してください。

汎用イベントの処理は、デフォルトでは無効になっています。管理者権限を持つユーザーは、無効にしたり、再度有効にすることができます。

[イベント（Events）]タブにはさまざまなフィルタが用意されており、それを使用して探している情報を見つけることができます。アラームの検索および表示（318ページ）で説明されている同じ手順を使用して、カスタマイズ（プリセット）したフィルタを作成して保存することもできます。次の表に、イベントをフィルタリングする方法の一部を示します。

検索するイベント	**[モニター（Monitor）]>[モニターリングツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]を選択し、[イベント（Events）]タブをクリックして、次の手順を実行します。**
ネットワーク内のすべてのイベント	[イベント履歴の表示（Show Event History）]ハイパーリンクをクリックします。
最新の4,000のイベント	[アクティブなイベントの表示（Showing Active Events）]ハイパーリンクをクリックします。
デバイス グループ、シリーズ、タイプ、ロケーション グループ、またはユーザー定義グループによって生成されたすべてのイベント	左側のサイドバー メニューからグループを選択します。
最後の *x* 分、時間、または日のイベント	[表示（Show）]ドロップダウン フィルタ リストをクリックし、適切なフィルタを選択します。
直前の1時間に生成された非情報イベント	[表示（Show）]ドロップダウン フィルタ リストから、[過去1時間の非情報イベント（Non-info events in last hour）]を選択します。

検索するイベント	**[モニター（Monitor）]>[モニターリングツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]** を選択し、**[イベント（Events）]** タブをクリックして、次の手順を実行します。
カスタマイズされたフィルタを使用したイベント	高度なフィルタを作成して保存します（アラームの検索および表示 （318 ページ） を参照）。

イベントまたは Syslog をアラームとして設定

アラームを生成するイベントを設定できます。イベントは、トラップまたはsyslogにすることができます。

イベントまたは syslog をアラームとして設定するには、次の手順を実行します。

ステップ 1 <XMP_HOME/conf/fault/event/eventTypes 下の構成ファイル **PKT_INFRA-FM_EvenTypes.xml** を開きます。

ステップ 2 「_」と「-」以外の特殊文字やスペースを含まない一意の英数字を使用して Bean ID を作成します。

ステップ 3 必要に応じて、名前、メッセージ、および説明を設定します。

ステップ 4 次の値を以下のように設定します。

- defaultCategory = オプティカル伝送
- defaultSeverity = 設定する syslog の重大度
- clearBy = イベント

ステップ 5 コンフィギュレーションファイルを保存します。イベントのアラームは、[アラームおよびイベント（Alarms and Events）] の [アラーム（Alarms）] タブに反映されます。Cisco EPN Manager を再起動する必要はありません。

ログファイル **decap.core.java.log** をチェックして、シンタックスエラーを確認できます。

（注） イベントまたはsyslogをアラームとして設定すると、Cisco EPN Managerの GUI を使用してアラームをクリアすることができません。アラームは、対応するイベントがクリアされると自動的にクリアされます。

CSV ファイルまたは PDF ファイルへのアラーム、イベント、または syslog のエクスポート

この手順を使用して、アラーム、イベント、または syslog を CSV ファイルまたは PDF ファイルとして保存します。

ステップ 1 エクスポートするデータに移動します。

- アラーム：**[モニター（Monitor）]** > **[モニターリング ツール（Monitoring Tools）]** > **[アラームおよびイベント（Alarms and Events）]** を選択し、[アラーム（Alarms）] タブ、または [クリア済みのアラーム（Cleared Alarms）] または [関連付けられているアラーム（Correlated Alarms）] タブをクリックします。
- イベント：**[モニター（Monitor）]** > **[モニターリングツール（Monitoring Tools）]** > **[アラームおよびイベント（Alarms and Events）]** を選択し、[イベント（Events）] タブをクリックします。
- syslogs：**[モニター（Monitor）]** > **[モニターリング ツール（Monitoring Tools）]** > **[アラームとイベント（Alarms and Events）]** を選択し、**[syslog（Syslogs）]** タブをクリックします。

ステップ 2 データが大量にある場合はフィルタを適用します。フィルタを適用しないと、エクスポートの処理に時間がかかることがあります。

ステップ 3 テーブルの右上にある をクリックし、[エクスポート（Export）] ダイアログボックスを開きます。

ステップ 4 [CSV] または [PDF] を選択して [OK] をクリックし、ファイルを保存します。

特定のアラームのイベントをエクスポートするには、[アラーム（Alarms）] タブで、その特定のアラームの横にある [i] アイコンの上にマウスを合わせます。ポップアップ ウィンドウが開いたら、そのウィンドウの右上隅にある をクリックし、エクスポート操作を実行します。

アラーム ポリシーとは

アラームポリシーはフィルタリングの方法で、これを使用することでネットワークの状況に関するアラームを制御し、システムのノイズを削減することができます。アラームポリシーを使用すると、指定した条件に基づいてネットワークで生成されるアラームを制御できます。アラームポリシーのリストを表示するには、**[モニター（Monitor）]** > **[モニターリングツール（Monitoring Tools）]** > **[アラームポリシー（Alarm Policies）]** に移動します。アラームポリシーを作成、編集、削除、およびランク付けすることができます。

アラームポリシーには、1つ以上の条件とアクションが含まれます。Cisco EPN Managerは、指定したすべての条件を満たすイベントまたはアラームにアクションを適用します。

（注） 新しく作成したアラームポリシーがポリシー作成前に生成されたアラームに遡及的に適用されることはありません。

次の操作を実行するアラーム ポリシーを作成できます。

- アラームの抑制：選択したイベントのアラームを生成しません。ただし、イベントは通常通り作成され、保存されます。

- イベントおよびアラームの抑制：イベントおよびアラームを作成しません。

（注） entsensor アラームの場合は、**[アラームの抑制（Suppress Alarms）]** オプションを使用してアラームを抑制するアラームポリシー機能を使用する必要があります。**[アラームとイベントの抑制（Suppress Alarms and Events）]** オプションは使用しないでください。

アラーム ポリシーのランク

Cisco EPN Manager は、ランクに基づいてアラームポリシーの優先順位または実行順序を決定します。複数のポリシーが同じアラームまたはイベントに適用される場合、Cisco EPN Manager はより高いランクのアラームポリシーを実行します。デフォルトでは、Cisco EPN Manager は作成された順序でアラームポリシーをランク付けします。

アラームポリシーをランク付けする際の注意点は次のとおりです。

- アラームポリシーは昇順でランク付けされます。したがって、番号が小さいポリシーほど優先順位が高くなります。

  たとえば、ランク 1 のアラームポリシーは、ランク 10 のアラームポリシーよりも優先されます。

- 優先順位が最も高いポリシーが最初に適用され、以降は優先順位が次に高いポリシーから順に適用されていきます。

- ランクが高いポリシーがランクが低いポリシーの動作に影響を与えたり、ランクが低いポリシーを完全にオーバーライドすることもあります。

- Cisco EPN Manager は、ランクが高いアラーム抑制ポリシーがすでにイベントに適用されている場合は、次のインスタンス内のアラームを抑制しません。

アラームポリシーのランクを変更するには、次の手順を実行します。

ステップ 1 **[モニター（Monitor）]**>**[モニターリングツール（Monitoring Tools）]**>**[アラームポリシー（Alarm Policies）]** に移動します。

Cisco EPN Manager には、作成された順序でアラームポリシーのリストが表示されます。

ステップ 2 ランクを変更するアラームポリシーを選択します。

ステップ 3 [移動先（Move To）] アイコンをクリックし、[行（Row）] フィールドにランクを入力するか、[上へ移動（Move up）] アイコンまたは [下へ移動（Move down）] アイコンをクリックしてランクを変更します。

アラーム ポリシーの表示

ステップ 1 [モニター（Monitor）]>[モニターリングツール（Monitoring Tools）]>[アラームポリシー（Alarm Policies）] を選択します。

すべてのアラームポリシーのリストがこのページに表示されます。

ステップ 2 ポリシーを表示するには、展開アイコンをクリックします。

新しいアラーム ポリシーの作成

新しいアラームポリシーを作成するには、次の手順を実行します。

ステップ 1 **[モニター（Monitor）]>[モニターリングツール（Monitoring Tools）]>[アラームポリシー（Alarm Policies）]** を選択します。

ステップ 2 [追加（Add）] アイコンをクリックし、[ポリシー タイプの選択（Select A Policy Type）] ウィンドウからポリシー タイプを選択します。

[新しいアラーム ポリシーの作成（Create a New Alarm Policy）] ウィザードが表示されます。

ステップ 3 [ポリシーの属性（Policy Attributes）] ページで [名前（Name）]、[説明（Description）]（任意）に入力し、実行するアクションのタイプを選択します。

ステップ 4 [アクションオプション（Action Options）] タブにある次のオプションのうち、いずれか 1 つを選択します。

- [完全に抑制（Suppress Permanently）]。
- [この期間に条件が改善されない場合に表示（分）（Display if the condition persists for this duration (minutes)）]：タイム スライダを使用して期間を選択します。

（注） このタブは、ステップ 3 で [アラームの抑制（Suppress Alarms）] を選択した場合にのみ有効になります。

ステップ 5 デバイス グループを選択します。

どのデバイスも選択しなかった場合は、ポリシーがすべてのデバイスに適用されます。

ステップ 6 [ポリシーの属性（Policy Attributes）] ページで選択したアクションに基づいて抑制するアラームまたはイベントを選択します。

ステップ 7 [概要（Summary）] をクリックして、ポリシーの詳細を表示します。設定を変更する場合は、それぞれのページに移動して必要な変更を行います。

ステップ 8 [終了（Finish）] をクリックします。

既存のアラーム ポリシーの編集

アラームポリシーを編集するには、次の手順を実行します。

手順

ステップ 1 [モニター（Monitor）]>[モニターリングツール（Monitoring Tools）]>[アラームポリシー（Alarm Policies）] を選択します。

ステップ 2 ポリシーを選択し、[編集（Edit）] アイコンをクリックします。

このアイコンをクリックすると、[アラームポリシーの編集（Edit Alarm Policy）] ウィザードが起動します。

ステップ 3 [ポリシーの属性（Policy Attributes）] ページで、必要に応じて [説明（Description）] を確認し、変更します。

（注） ポリシー作成中は、選択したポリシー名およびアクションを編集できません。

ステップ 4 [アラーム ポリシーの編集（Edit Alarm Policy）] ウィザードでの残りのステップは、[新しいアラーム ポリシーの作成（Create a New Alarm Policy）] ウィザードの手順と同じです。新しいアラーム ポリシーの作成（338 ページ）を参照してください。

ステップ 5 [終了（Finish）] をクリックして、変更を保存するか、または [キャンセル（Cancel）] をクリックして、変更を廃棄します。

アラーム ポリシーの削除

アラームポリシーを削除するには、次の手順を実行します。

手順

ステップ 1 [モニター（Monitor）]>[モニターリングツール（Monitoring Tools）]>[アラームポリシー（Alarm Policies）] を選択します。

ステップ 2 削除するアラームポリシーを選択し、[削除（Delete）] アイコンをクリックします。

ステップ 3 [Delete Confirmation] ダイアログボックスで [Yes] をクリックして削除するか、または [No] をクリックしてキャンセルします。

アラームおよびイベントの通知ポリシー

特定のデバイス グループから特定の受信者グループに生成された特定の対象アラームに関する通知を送信するためのポリシーを作成できます。

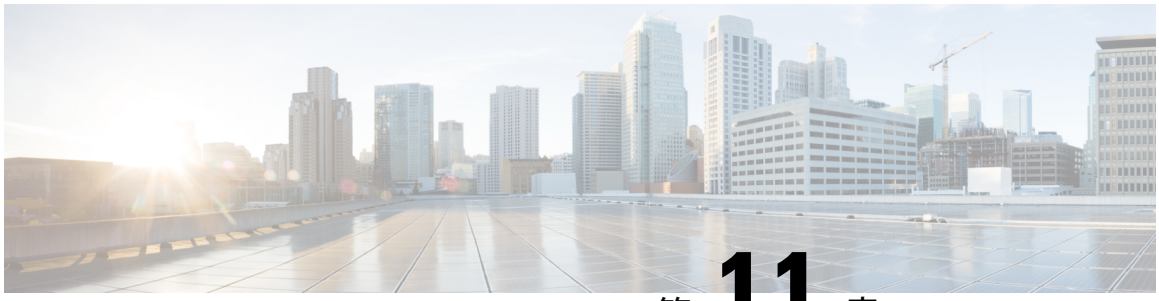
詳細については、「障害管理タスク」の「イベントの受信、転送、および通知（1059ページ）」の項を参照してください。.

シスコからサポートを受ける

Monitor > Monitoring Tools > Alarms and Events でアラームを受信し、シスコ サポート コミュニティ（アラームをクリックして **Troubleshoot > Support Forum** を選択）で解決策が見つからない場合は、Cisco EPN Manager を使用してサポート要求を開きます（アラームをクリックして **Troubleshoot > Support Case** を選択）。

Cisco EPN Manager 内の問題への対応

Cisco EPN Manager は、サーバーの CPU とディスクの使用率、ファンと電源装置の障害、高可用性（HA）状態の変化など、独自の機能を監視するための内部 SNMP トラップを生成します。これらのタイプのイベントの詳細については、サーバー内部 SNMP トラップをトラブルシュートする （982 ページ）を参照してください。



第 11 章

Cisco ASR 9000 ネットワーク仮想化（nV）サテライトおよびクラスタ サービスのモニターリング

Cisco ASR 9000 nV サテライトのモニターリング

Cisco ASR 9000 nV サテライト機能セットを使用すると、1 つ以上の小規模なサテライト スイッチを Cisco ASR9000 デバイスと相互接続し、単一の結合アクセス、アグリゲーション、エッジ システムを形成できます。

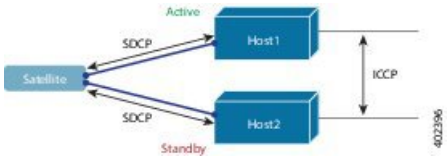
Cisco EPN Manager Cisco ASR 9000v、Cisco ASR 901、Cisco ASR 901S、Cisco ASR 903、および Cisco NCS 5001/2 デバイスをサテライトとしてサポートします。Cisco ASR 9000v は、Cisco ASR 9000 デバイスと共に nV サテライト モードでのみ使用できる専用サテライト スイッチです。Cisco ASR 901 および Cisco ASR 903 スイッチは「デュアル モード」スイッチです。つまり、両方ともスタンドアロンスイッチとして、または Cisco ASR 9000 デバイスを搭載した nV システム内のサテライトスイッチとして動作できます（その場合は、プライマリ Cisco ASR 9000 で完全に管理、制御できます）。

サテライト機能を使用すると、サテライトスイッチとプライマリ Cisco ASR 9000 間での冗長相互接続および非冗長相互接続の両方が可能になります。サテライトスイッチのアクセス側イーサネットポートは、ローカルに接続されたイーサネットポートと同様に、ホストプライマリ Cisco ASR 9000 のコントロールパネル内と管理パネル内に表示されます。ホスト Cisco ASR 9000 で設定できる機能はすべて、サテライトがあるポートでも同じように設定および実行でき

ます。サテライト スイッチは事実上、ホスト Cisco ASR 9000 の仮想ライン カードです。サテライト上のハードウェア センサのソフトウェア アップグレード、インベントリ、および環境モニターリング（電圧、温度など）のようなサテライトのシャーシ管理機能も、ホスト Cisco ASR 9000 シャーシの他のライン カードと同様に、ホスト Cisco ASR 9000 の同じ機能にシームレスに統合されます。

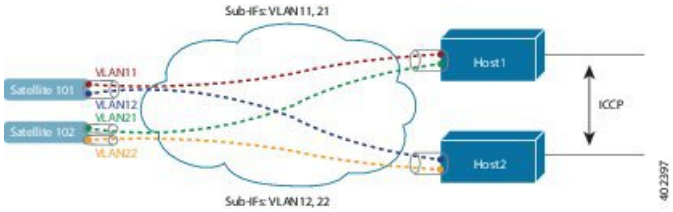
Cisco EPN Manager は、次のタイプの nV サテライト設定をサポートしています。

- デュアル ホーム ハブとスポーク（インベントリ サポートのみ）



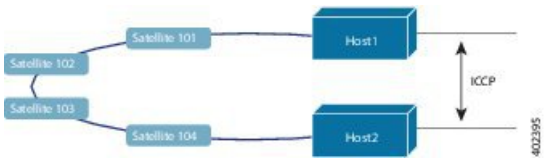
  - 同じサテライトは、アクティブとスタンバイの 2 つの個別の Cisco ASR 9000 ホストのデュアル ホームとなります。
  - 各ホストには、サテライトを持つ独立した制御チャネルがあります。
  - サテライトには、どちらのホストがアクティブで、どちらがスタンバイかが通知されます。
  - サテライトがアクティブなホストまたはリンクを失うと、スタンバイ ホストへのフェールオーバーが発生します。

- L2 ファブリック ハブとスポーク



  - L2 ファブリックは、イーサネットレイヤ 2 ドメイン間のサテライト接続をサポートします。
  - サテライト ファブリック リンクの冗長性：2 つの VLAN/EVC を持つ単一の物理リンク、またはそれぞれ 1 つの VLAN/EVC を持つ 2 つの物理リンク。
  - 各ホスト L2 サブインターフェイスは、1 つのサテライト ファブリック ポートにマップされます。

- シンプル リング



  - リング内の各サテライトは、2 つのホストを個別に SDCP で実行します。

- 各サテライトは、物理リング トポロジ上の論理的なハブ アンドスポーク トポロジを維持します。
- サテライト間での直接ローカル スイッチングは必要ありません。すべてパケットがホストを通過します。

Cisco EPN Manager でのサテライトの考慮事項

Cisco EPN Manager は [ネットワーク検出（Network Discovery）] ページからのサテライト デバイス管理操作をサポートしていないため、サテライトは[ネットワーク検出（Network Discovery）] ページ（**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]**）には表示されません。

通常、サテライトはネットワーク ノードとしてロケーションに従って管理されるため、ロケーション グループにのみ属すことができます。さらに、ホスト デバイスをグループに追加すると、そのグループが次のガイドラインを満たさない限り、そのサテライトは自動的にグループに追加されません。

- [デバイスを手動で追加する（Add Devices Manually）] を使用する場合：グループの作成（または編集）ページから、[追加（Add）] をクリックし、[フィルタ基準（Filter by）] ドロップダウンリストから [すべてのロケーション（All Locations）] を選択します。基準に一致する場合、サテライトがリストされます。
- [デバイスを動的に追加する（Add Devices Dynamically）] を使用する場合：ロケーション グループを作成していることを確認してください。グループの作成（または編集）ページで、ページ上部の [親グループ（Parent Group）] から [すべてのロケーション（All Locations）] を選択します。

Cisco ASR 9000 nV サテライトのデバイスと OS の最小要件

nV サテライト機能セットのデバイスおよびデバイス オペレーティング システムの最小要件を次に示します。

- ハードウェア：シャーシ間リンクの場所としての Cisco ASR 9000 Enhanced Ethernet ライン カードを搭載した Cisco ASR 9000 シリーズ アグリゲーション サービス ルータと、サテライト デバイスとしての Cisco ASR9000v、Cisco ASR 901、Cisco ASR 903、Cisco NCS 5001、または Cisco NCS 5002 ルータ。

（注） サテライトが ASR 9000 デバイスでない場合、その詳細はホスト デバイスのシャーシ ビューでは確認できません。

- ソフトウェア：Cisco IOS XR 5.2.0

追加サポートが利用できる場合があります。詳細については、Cisco Evolved Programmable Network Manager のサポート対象デバイスを参照してください。

特定のサテライトに関するクイック情報の表示：サテライト360ビュー

[サテライト360（Satellite 360）] ビューは、サテライト デバイス、そのインベントリ、およびステータスに関するクイック情報を表示するポップアップ ウィンドウです。これには、デバイス アラーム、モジュール、インターフェイス、およびホストが含まれます。

サテライト 360 ビューを起動するには、次の手順を実行します。

- ほぼすべてのデバイス テーブルにあるデバイス名の横の [i] アイコンをクリックします。
- ネットワーク トポロジで、展開されたグループ内のデバイスをクリックし、[表示（View）] をクリックします。
-

[サテライト360（Satellite 360）] ビューで、ビューの上部にサテライト デバイスに関する一般情報が示され、ビューの下部にあるタブにはより詳細なインターフェイス情報が示されます。

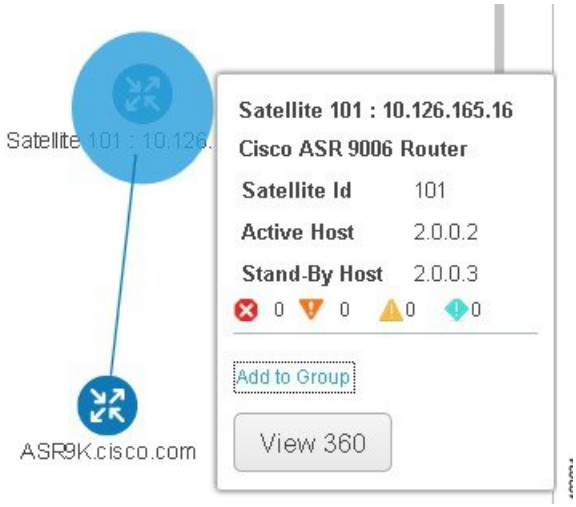
[サテライト360（Satellite 360）] ビューに表示される情報	**説明**
一般情報	サテライトデバイスのタイプと名前、ステータス、最後の設定変更、および最後のインベントリ 収集、
モジュール	名前、タイプ、状態、ポート、および場所を含む、サテライトデバイス上で設定されたモジュール。
インターフェイス	関連付けられているサテライトデバイスそれぞれの名前、動作および管理者ステータス。また、[インターフェイス 360（Interface 360）] ビューの起動ポイントも示されます。
ホスト（Hosts）	サテライトに接続されているホストデバイスの名前、IPアドレス、およびロール（アクティブまたはスタンバイ）。

トポロジ マップでの Cisco ASR 9000 ホスト/サテライト トポロジの表示

Cisco ASR 9000 ホスト/サテライト トポロジを視覚化し、ホストまたはサテライトにアクティブなアラームがあるかどうかを一目で確認できます。トポロジ マップからドリル ダウンすると、ホスト デバイスとサテライト デバイスに関する詳細な情報を得ることができます。

Cisco ASR 9000 ホストのサテライト ID と IP アドレスを含むラベルで、マップ内のサテライトを簡単に識別できます。

（注） サテライト トポロジ内のデバイス間のリンクを表示するには、リンク タイプ フィルタ（マップの右上隅）でシャーシ間制御リンクとICCPリンクを有効にする必要があります。ICCPプロトコルは、リンクをホストするためにホストに使用されます。



Cisco ASR 9000 ホスト/サテライトのトポロジをマップで表示するには、次の手順を実行します。

ステップ 1 左側のナビゲーション ペインで **Maps > Network Topology** を選択します。

ステップ 2 左側の [グループ（Groups）] ウィンドウから、Cisco ASR 9000 ホストとサテライトを含むグループを選択します。トポロジ マップには選択したグループのすべてのデバイスが表示されます。

ステップ 3 マップ内でホストまたはサテライトの 1 つを見つけます。

ステップ 4 ホストとサテライト間のリンクを表示するには、次のサイトを使用します。

- トポロジ ツールバーの [フィルタ（Filter）] アイコンをクリックし、**Link Types** を選択します。
- コントロール プレーン、シャーシ間制御、および ICCP チェックボックスをオンにしてから、**OK** をクリックします。

ステップ 5 サテライトをクリックしてポップアップを起動し、サテライト ID とともにアクティブ ホストとスタンバイ ホストの ID も表示します。

ステップ 6 Cisco ASR 9000 ホストに接続されているサテライトの特定 （346 ページ）の説明に従って、ポップアップの [ビュー 360（View 360）] をクリックして [サテライト 360（Satellite 360）] ビューのサテライトとそのホストに関する詳細情報を表示します。

Cisco ASR 9000 ホストに接続されているサテライトの特定

選択した Cisco ASR 9000 ホストのデバイス 360 ビューには、デバイス自体とホストに接続されているサテライトに関する情報が含まれています。

Cisco ASR 9000 ホストに接続されているサテライトを特定するには、次の手順を実行します。

ステップ 1 左側のナビゲーション ペインで **Inventory > Network Devices** を選択します。

ステップ 2 左側の [デバイス グループ（Device Group）] ペインから、Cisco ASR 9000 ホストを含むグループを選択します。

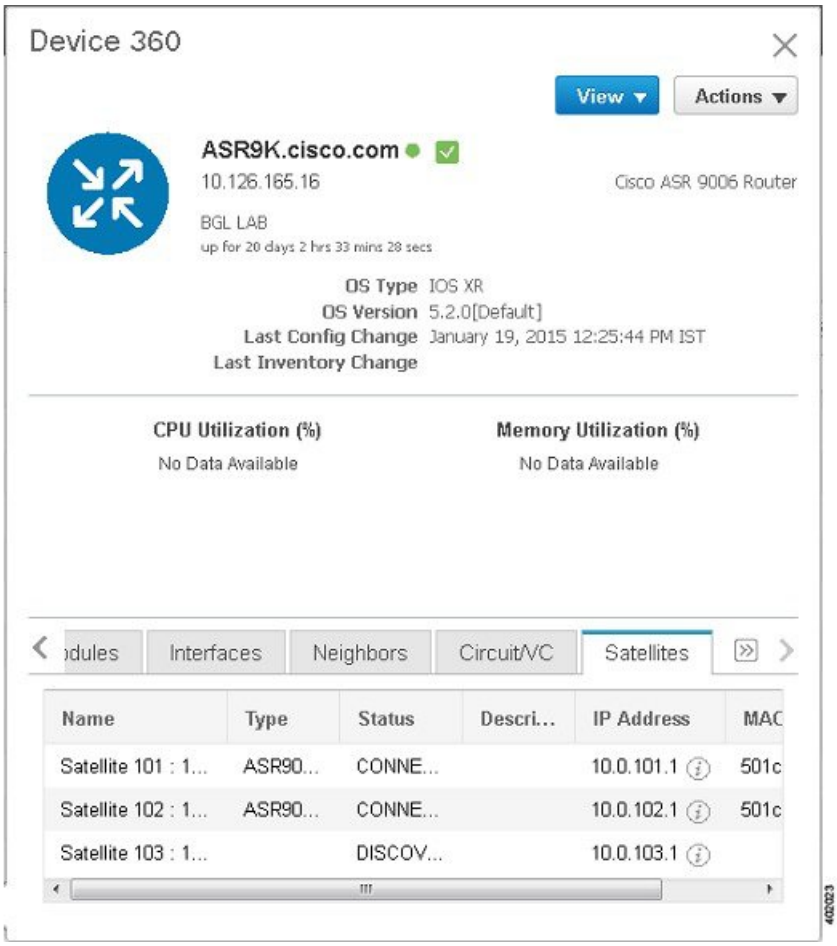
ステップ 3 右側のデバイス リストでホストを見つけます。

ステップ 4 デバイス IP アドレス/DNS の横にある [i] アイコンをクリックして、ホストのデバイス 360 ビューを開きます。

（注） また、デバイスをクリックし、表示されたポップアップで **View 360** をクリックすると、マップからデバイス 360 ビューにアクセスすることもできます。

[サテライト（Satellites）] タブには、ホストに関連付けられているサテライトのリストが表示され、タイプ、説明、IP アドレス、MAC アドレスなど、各サテライトに関する基本的な情報が表示されます。また、サテライトが現在ホストに接続されているか、ホストから切断されているかも示されます。[サテライト（Satellites）] タブは、Cisco ASR 9000 ホストとサテライトのデバイスのデバイス 360 ビューにのみ表示されます。

ステップ 5 [サテライト（Satellites）] タブの IP アドレスの横にある [i] アイコンをクリックして、サテライトのデバイス 360 ビューを開きます。[ホスト（Hosts）] タブには、そのサテライトに関連付けられているアクティブなホストとスタンバイ ホストのリストが表示されます。



サテライトに接続されているホストの特定

通常、マップ内のリンクは、ホストと接続されているサテライトを含めてサテライトトポロジを明確に表示します。何らかの理由で、サテライトがリンクなしに表示される場合、サテライトが関連付けられているホストは簡単に特定できます。

サテライトに接続されているホストを特定するには、次の手順を実行します。

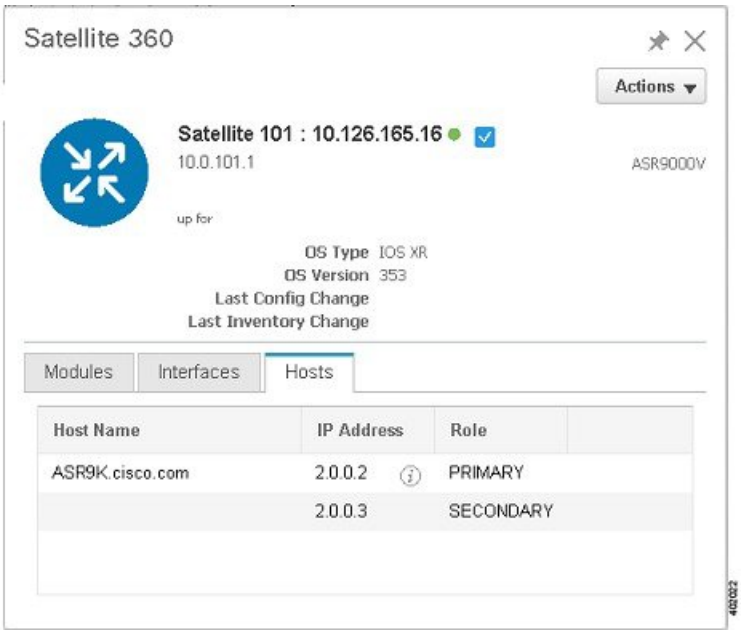
ステップ 1 左側のナビゲーション ペインで **Maps > Network Topology** を選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインから、Cisco ASR 9000 ホストとサテライトを含むグループを選択します。マップには選択したグループのすべてのデバイスが表示されます。

ステップ 3 **Satellite ID** で始まるラベルで識別されているサテライト デバイスをクリックします。

ステップ 4 表示されたポップアップで、**View 360** をクリックし、サテライト 360 ビューをクリックして起動します。

サテライト 360 ビューの [ホスト（Hosts）] タブには、サテライトが接続されているホスト デバイスとそれらのローフ（アクティブかスタンバイか）のリストが表示されます。



Cisco ASR 9000 nV サテライトの障害のモニターリング

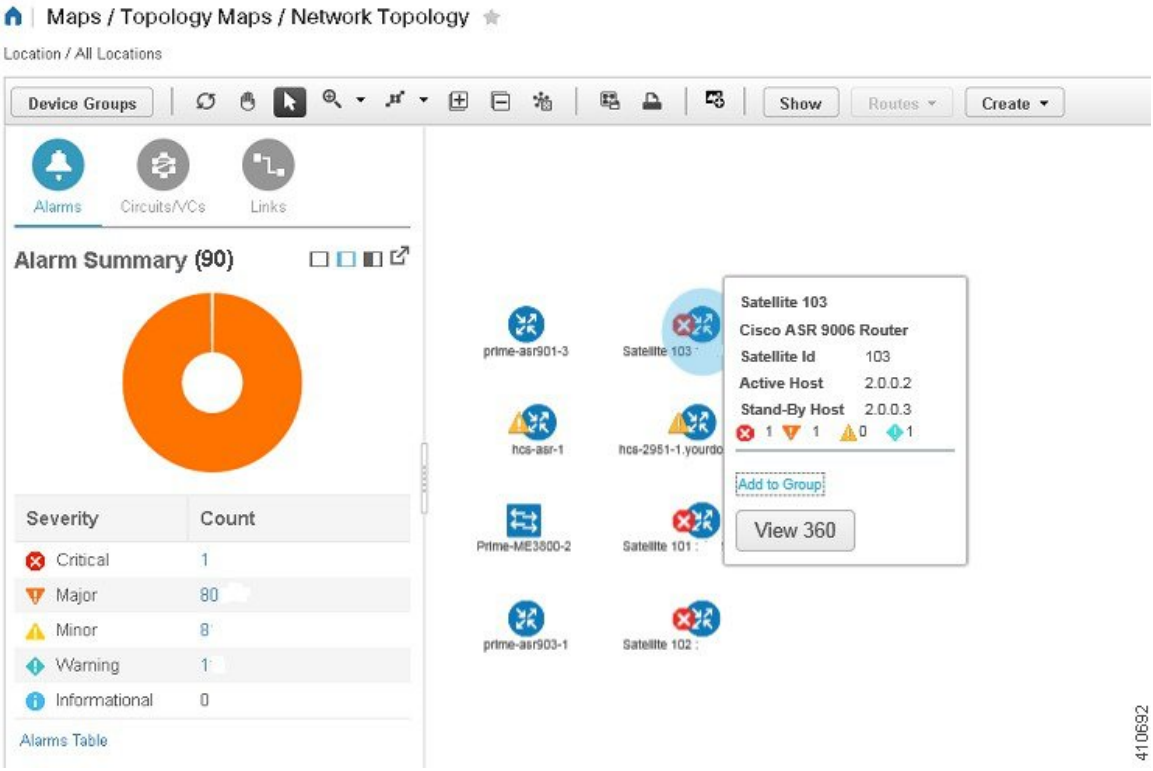
サテライトで障害が発生すると、障害のタイプに応じて、Cisco EPN Manager はホスト デバイスまたはサテライト デバイスのいずれかに障害を関連付けます（ローカライズ）。

- ポート、ファン、モジュールなどの物理エンティティで障害が発生した場合は、Cisco EPN Manager はサテライト デバイスを障害の場所として識別します。
- サブインターフェイスなどの論理構成体で障害が発生した場合は、サブインターフェイスがホスト上に設定されているため、Cisco EPN Manager はホストデバイスを障害の場所として識別します。

デュアルホームのサテライトでアラームが発生すると、そのアラームはアクティブ ホスト上の 1 つのアラームとスタンバイ ホスト上の別のアラームで複製されます。

トポロジ マップでのサテライト障害の表示

トポロジマップには、アラーム ソース（サテライト デバイス、ホスト デバイス、またはサテライトデバイスとホストデバイス間のリンク）にアラームバッジがオーバーレイされて表示されます。

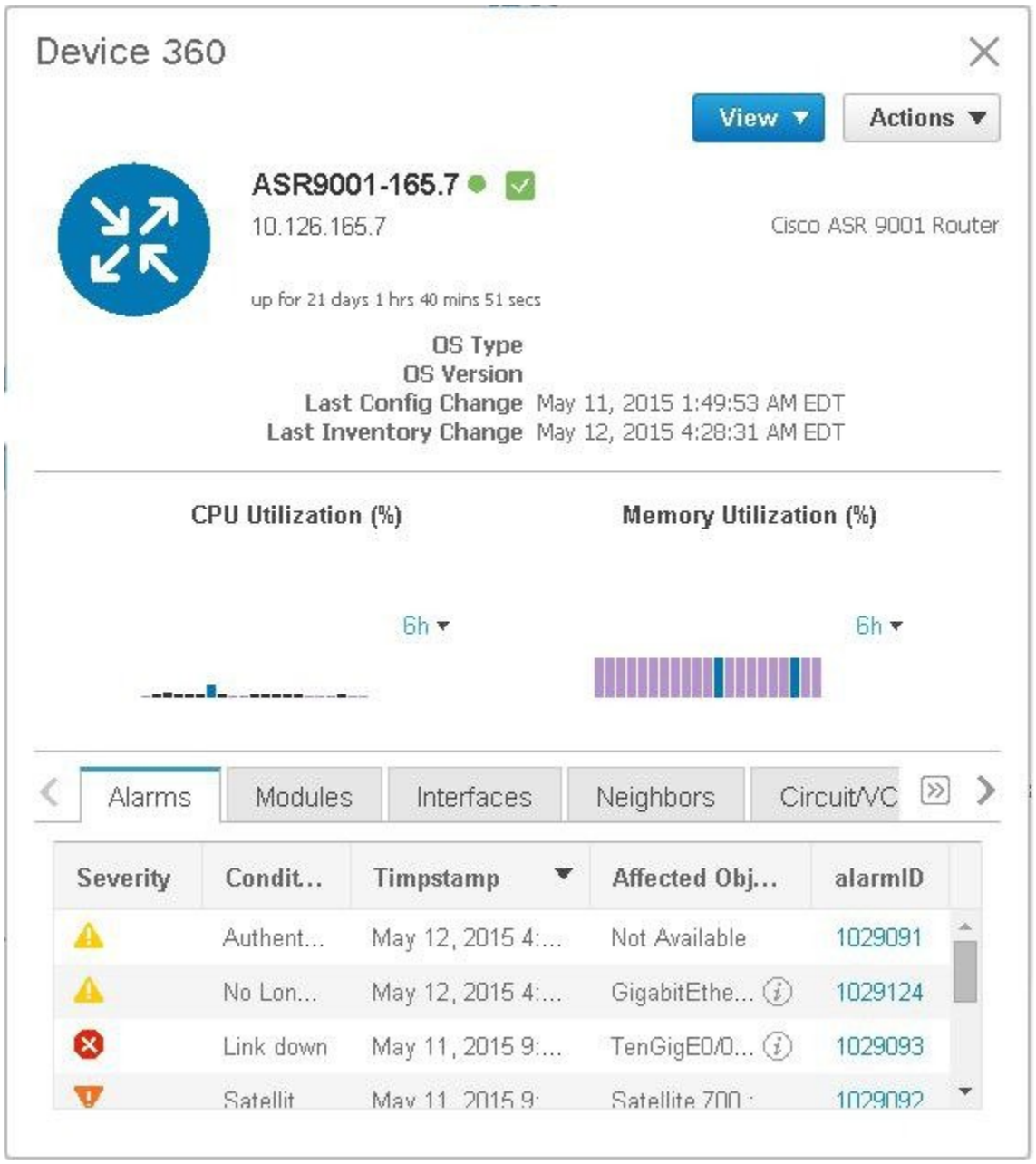


同じエンティティに複数のアラームがある場合、アラームバッジの重大度は最も重大なアラームの重大度を表します。

アラームが発生したエンティティを右クリックすると、エンティティに関連するすべてのアクティブ アラームのカウントを示すポップアップが表示されます。リンク ダウンなどのリンク関連のアラームは、トポロジ マップの関連リンク上にアラーム バッジを生成させます。

デバイス 360 ビューを使用したサテライト障害の表示

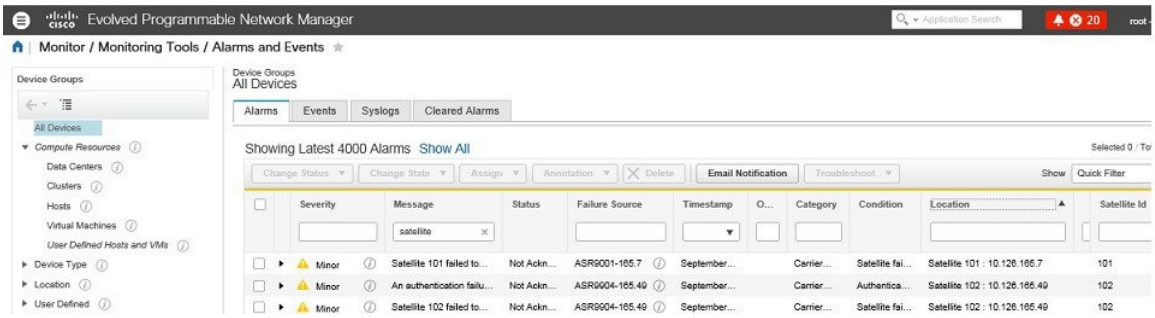
デバイス アラームの影響を受けるオブジェクトを確認するには、ポップアップ メニューから [ビュー 360（View 360）] をクリックし、[影響を受けるオブジェクト（Affected Objects）] 列を確認します。特定のアラームの詳細を表示する場合は、[alarmID] ハイパーリンクをクリックします。



[アラームおよびイベント（Alarms and Events）] テーブルでのサテライト障害の表示

[アラーム（Alarm）] テーブルからサテライト アラーム情報を取得するには、**[モニター（Monitor）]>[モニターリングツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]** を選択し、[アラーム（Alarms）] タブをクリックします。

Cisco EPN Manager は、障害ソースとしてホスト デバイスを一覧表示します。[サテライト ID（Satellite ID）] フィールドと [場所（Location）] フィールドで、サテライト ソースを識別します。



406012

Cisco ASR 9000 nV エッジ クラスタのモニターリング

nV エッジの機能は、2 台以上の Cisco ASR 9000 シリーズ ルータのシャーシが結合され、単一の論理スイッチングまたはルーティングエンティティを形成します。これにより、2 台の Cisco ASR 9000 シリーズ ルータ プラットフォームを単一の仮想 Cisco ASR 9000 シリーズ システムとして運用することができます。実質的に、2 台の物理シャーシが共有コントロールプレーンで論理的にリンクされるので、2 台のルート スイッチ プロセッサ（RSP）が単一のシャーシに収容されているのと同じことになります。

nV エッジ トポロジには、次の 2 つのタイプのリンクがあります。

- 制御トラフィックに使用される制御リンク。
- シャーシ間のデータ生成と転送に使用されるラック間リンク。

nV エッジのデバイスと OS の最小要件

nV エッジのデバイスとデバイス オペレーティング システムの最小要件を次に示します。

- Cisco IOS XR 5.2.0 を実行している 2 台の Cisco ASR 9000 デバイス
- 4 10G SFP（IRL の場合）
- 4 1G SFP（クラスタ/制御リンクの場合）
- シャーシごとに 2 つの RSP ノード（クラスタ設定をサポートする単一 RSP システムである Cisco ASR 9001 を除く）

追加サポートが利用できる場合があります。Cisco Evolved Programmable Network Manager のサポート対象デバイスを参照してください。

トポロジ マップでの nV エッジ クラスタの表示

nV エッジ クラスタは、トポロジ マップ内で、2 つのリンクされたシャーシ（1 つのプライマリと 1 つのバックアップ）で構成される単一のオブジェクトとして示されます。

Cisco ASR 9000 nV エッジ トポロジをマップに表示するには、次の手順を実行します。

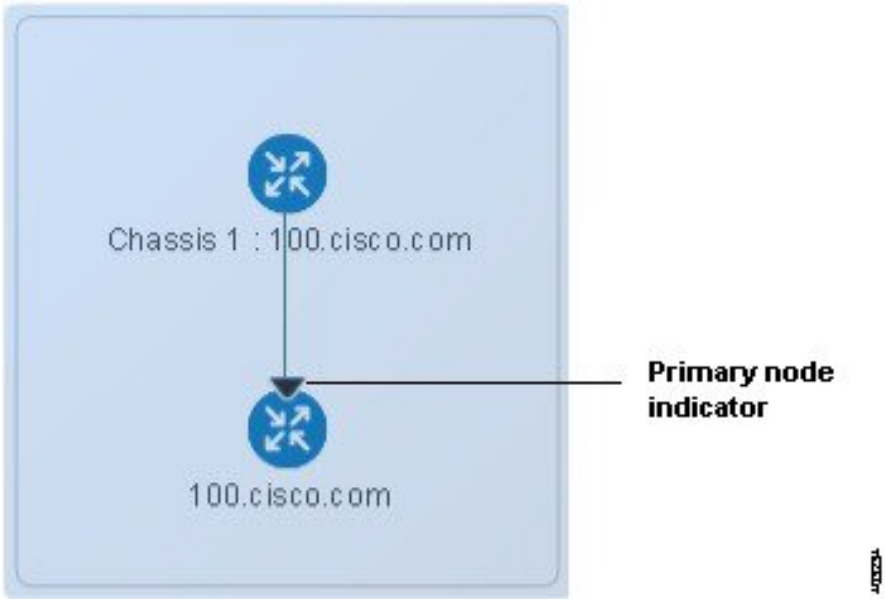
ステップ 1 左側のナビゲーション ペインで **Maps > Network Topology** を選択します。

ステップ 2 左側の [グループ（Groups）] ペインから、Cisco ASR 9000 クラスタを含むグループを選択します。トポロジ マップには選択したグループのすべてのデバイスが表示されます。

ステップ 3 プライマリ シャーシまたはバックアップ シャーシをクリックします。両方のシャーシが選択され、2 つのシャーシを一緒に表示するポップアップが開きます。各シャーシに個別にアクセスすることはできません。

ステップ 4 クラスタ トポロジにリンクを表示するには、次の手順を実行します。

- トポロジ ツールバーのフィルタ アイコンをクリックし、**Link Types** を選択します。
- コントロールプレーンとシャーシ間制御チェックボックスをオンにしてから、**OK** をクリックします。



クラスタでのプライマリ デバイスとバックアップ デバイスの識別

トポロジ マップには、プライマリのシャーシとバックアップのシャーシが明確に表示されます。シャーシに関する詳細は、デバイス 360 ビューに表示されます。

プライマリ デバイスとバックアップ デバイスを識別し、詳細情報を表示するには、次の手順を実行します。

ステップ 1 左側のナビゲーション ペインで **Maps > Network Topology** を選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインから、Cisco ASR 9000 クラスタのセットアップを含むグループを選択します。マップには選択したグループのすべてのデバイスが表示されます。

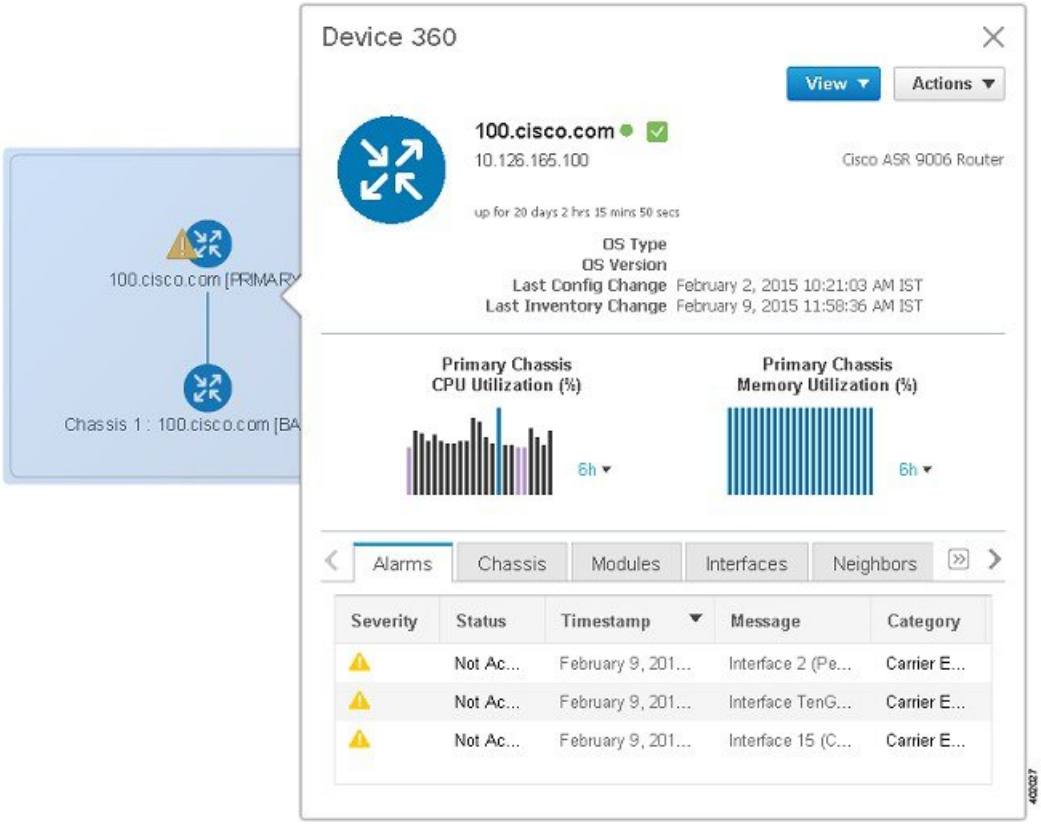
ステップ 3 クラスタの表示をクリックします。

ステップ 4 表示されたポップアップで、**[View 360]** をクリックします。

[デバイス 360（Device 360）] ビューの [シャーシ（Chassis）] タブには、クラスタ内のシャーシのリストが表示され、識別されて、それらのステータスとロール（プライマリかバックアップか）の情報も表示されます。

Cisco ASR 9000 nV エッジ クラスタ サービスのモニターリングとトラブルシューティング

Cisco EPN Manager は、クラスタにアラーム インジケーターを表示し、Device 360 ビューのプライマリ シャーシの CPU とメモリ使用率を示すグラフが表示されます。



第 12 章

レポートの管理

レポートの概要

Cisco EPN Manager レポートでは、システムおよびネットワークの健全性に関する情報と障害情報が提供されます。定期的にレポートが実行されるようにカスタマイズしてスケジュールすることができます。レポートは、表形式またはグラフィック形式（またはこれらの形式の混合）でデータを表示できます。レポートは CSV または PDF 形式で保存することもできます。CSV または PDF ファイルは、後でダウンロードするために Cisco EPN Manager サーバーに保存するか、または電子メール アドレスに送信できます。

Cisco EPN Manager では、次のタイプのデータが提供されます。

- 現在：時間に依存しないデータのスナップショットを提供します。
- 履歴：デバイスから定期的にデータを取得し、そのデータを Cisco EPN Manager データベースに保存します。
- 傾向：最小値、最大値、および平均値として集計された集約データを使用してレポートを生成します。

Cisco EPN Manager では、特定の基準に基づいてこれらのレポートをフィルタリングできます。たとえば、IPSLA Y.1731 レポートをプローブに基づいてフィルタリングし、PWE3 レポートを仮想接続識別子（VCID）に基づいてフィルタリングできます。また、レポートをエクスポー

トしたり、レポートを論理グループにソートしたり、長期間保存するためにレポートをアーカイブすることもできます。

レポートファイルの圧縮

特定のファイルサイズ制限を超えるレポートを圧縮することもできます。デフォルトでは、5 MB を超えるレポートは zip 形式で圧縮されます。ファイルサイズの制限を変更するには、`ReportResources.properties` ファイル内の変数 `minSizeToCompressFile` を更新します。

ステップ 1 CLI 管理者ユーザーとして Cisco EPN Manager にログインします（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 2 `ReportResources.properties` ファイルを開きます。

ファイルパス：`/opt/CSCOlumos/conf/rfm/classes/com/cisco/server/resources/ReportResources.properties`

ステップ 3 `minSizeToCompressFile` を必要な値（バイト単位）で更新します。

たとえば、7 MBを超えるファイルを圧縮する場合は、変数を次のように更新します。

```
minSizeToCompressFile=7340032
```

ステップ 4 ファイルを保存します。

この変更を有効にするには、Cisco EPN Manager を再起動する必要があります。

使用可能なレポート

[レポート起動パッド（Reports Launch Pad）] では、次の Cisco EPN Manager レポートにアクセスできます。

- キャリア イーサネット パフォーマンス レポート （356 ページ）
- 光パフォーマンス レポート （367 ページ）
- パフォーマンス レポート （374 ページ）
- Network Summary レポート （375 ページ）
- デバイス レポート （376 ページ）

キャリア イーサネット パフォーマンス レポート

この項では、Cisco EPN Manager でサポートされるキャリア イーサネット（CE）パフォーマンス レポートを示します。適切なレポート データを収集できるように有効化する必要があるモニターリング ポリシーも含まれます。モニターリング ポリシーの詳細については、デバイスのヘルスとパフォーマンスのモニター方法：モニターリング ポリシー （281 ページ）を参照してください。

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
IPSLA グラフ	平均遅延後方、平均遅延前方、平均遅延双方向、ジッター前方、ジッター後方、平均後方パケット損失率、平均前方パケット損失率、可用性のグラフィカル表示。	*IPSLA* IPSLA モニターリング ポリシーの詳細については、IP SLA モニターリング ポリシー（1204ページ）を参照してください。	応答時間の平均、応答時間の最大、応答時間の最小、ジッター Neg DS 平均、ジッター Neg SD 平均、ジッター Pos DS 平均、ジッター Pos SD 平均、パケット損失の全体的な Util の平均、パケット損失 DS Util 平均、パケット損失 SD Util 平均、遅延一方向 SD 平均、遅延一方向 SD 最大、遅延一方向 SD 最小、遅延一方向 DS 平均、遅延一方向 DS 最大、遅延一方向 DS 最小
IPSLA 統計情報	プローブ インデックス、IPSLA プローブ タイプ、TOS、ターゲット IP、VRF 名、平均遅延双方向、平均遅延前方、平均遅延後方、パケット損失率前方、パケット損失率後方、平均ジッター前方、平均ジッター後方、平均後方パケット損失率、平均前方パケット損失率、可用性の表形式表示。	*IPSLA* IPSLA モニターリング ポリシーの詳細については、IP SLA モニターリング ポリシー（1204ページ）を参照してください。	ジッター Neg DS 平均、ジッター Neg SD 平均、ジッター Pos DS 平均、ジッター Pos SD 平均、パケット損失の全体的な Util の平均、パケット損失 DS Util 平均、パケット損失 SD Util 平均、遅延一方向 SD 平均、遅延一方向 SD 最大、遅延一方向 SD 最小、遅延一方向 DS 平均、遅延一方向 DS 最大、遅延一方向 DS 最小

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
IPSLA 上位 N	プローブ インデックス、IPSLA プローブ タイプ、TOS、ターゲット IP、VRF 名、平均遅延双方向、最大遅延双方向、最小遅延双方向、平均遅延前方、最大遅延前方、最小遅延前方、平均遅延後方、最大遅延後方、最小遅延後方、平均前方パケット損失率、平均後方パケット損失率、ジッター前方、ジッター後方、可用性の表形式表示。	*IPSLA* IPSLA モニターリング ポリシーの詳細については、IP SLA モニターリング ポリシー（1204ページ）を参照してください。	応答時間の平均、応答時間の最大、応答時間の最小、ジッター Neg DS 平均、ジッター Neg SD 平均、ジッター Pos DS 平均、ジッター Pos SD 平均、パケット損失の全体的な Util の平均、パケット損失 DS Util 平均、パケット損失 SD Util 平均、遅延一方向 SD 平均、遅延一方向 SD 最大、遅延一方向 SD 最小、遅延一方向 DS 平均、遅延一方向 DS 最大、遅延一方向 DS 最小
IPSLA Y.1731 グラフ	Y.1731 プローブの平均遅延後方、平均遅延前方、ジッター双方向、ジッター前方、ジッター後方、平均後方フレーム損失率、平均前方フレーム損失率、可用性のグラフィカル表示。 （注） [プローブ（Probe Index）] 列の値が -1 の場合は、デバイスにプローブインデックスが設定されていないことを示します。	*IPSLA Y.1731* IPSLA Y.1731 モニターリング ポリシーの詳細については、IP SLA Y.1731 モニターリングポリシー（1201ページ）を参照してください。	平均遅延双方向、平均遅延前方、平均遅延後方、平均正ジッター前方、平均負ジッター前方、平均正ジッター後方、平均負ジッター後方、平均前方フレーム損失率、平均後方フレーム損失率

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
IPSLA Y.1731 統計情報	Y.1731 プローブの操作タイプ、CFM ドメイン、送信元、宛先、フレーム タイプ、平均遅延双方向、平均遅延前方、平均遅延後方、平均ジッター、前方フレーム損失率、後方フレーム損失率、平均前方ジッター、平均後方ジッター、可用性の表形式表示。	*IPSLA Y.1731* IPSLA Y.1731 モニターリング ポリシーの詳細については、IPSLA Y.1731 モニターリングポリシー（1201 ページ）を参照してください。	平均遅延双方向、平均遅延前方、平均遅延後方、平均前方フレーム損失率、平均後方フレーム損失率、平均ジッター
IPSLA Y.1731 上位 N	Y.1731 テクノロジーを使用して設定されたデバイスの操作タイプ、CFM ドメイン、送信元、宛先、フレーム タイプ、平均遅延双方向、最大遅延双方向、最小遅延双方向、平均遅延前方、最大遅延前方、最小遅延前方、平均遅延後方、最大遅延後方、最小遅延後方、平均前方フレーム損失率、最大前方フレーム損失率、最小前方フレーム損失率、平均後方フレーム損失率、最大後方フレーム損失率、最小後方フレーム損失率、ジッター前方、ジッター後方、可用性の表形式表示。	*IPSLA Y.1731* IPSLA Y.1731 モニターリング ポリシーの詳細については、IPSLA Y.1731 モニターリングポリシー（1201 ページ）を参照してください。	平均遅延双方向、平均遅延前方、平均遅延後方、平均正ジッター前方、平均負ジッター前方、平均正ジッター後方、平均負ジッター後方、平均前方フレーム損失率、平均後方フレーム損失率

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
インターフェイスのアベイラビリティ	ネットワーク内のデバイスに関するインターフェイスの詳細の表示	インターフェイス ヘルス インターフェイス ヘルス モニターリング ポリシーの詳細については、インターフェイスのヘルス モニターリング ポリシー（1200ページ）を参照してください。	統計情報（Statistics）
インターフェイスのグラフ	一定期間のインターフェイス トラフィック統計情報：受信トラフィック、発信トラフィック、受信使用率、発信使用率。	インターフェイス ヘルス インターフェイス ヘルス モニターリング ポリシーの詳細については、インターフェイスのヘルス モニターリング ポリシー（1200ページ）を参照してください。	統計情報（Statistics）
インターフェイス上位 N	インターフェイス トラフィック統計情報の上位 N レポートの表形式表示：最大受信トラフィック、平均受信トラフィック、最大発信トラフィック、平均発信トラフィック、最大受信使用率、最大発信使用率と現在の受信使用率、現在の発信使用率、受信エラー、発信エラー、受信破棄、発信破棄、インターフェイスの可用性。	インターフェイス ヘルス インターフェイス ヘルス モニターリング ポリシーの詳細については、インターフェイスのヘルス モニターリング ポリシー（1200ページ）を参照してください。	統計情報（Statistics）

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
インターフェイス トラフィック（Interface Traffic）	インターフェイス トラフィック統計情報の表形式表示：受信トラフィックレート、発信トラフィックレート、受信使用率、発信使用率、受信エラー、発信エラー、受信破棄、発信破棄、受信パケットレート、発信パケットレート（L3 パケット含む）、CRC エラーと割合。	インターフェイス ヘルス インターフェイス ヘルス モニターリング ポリシーの詳細については、インターフェイスのヘルス モニターリング ポリシー（1200ページ）を参照してください。	統計情報と CRC
光リンク SFP 電力レベル	A エンド デバイス、A エンド インターフェイス、Z エンド デバイス、Z エンド インターフェイス、Tx と Rx の電力レベルの表形式表示。 （注） このレポートの前提条件は、ネットワークで CDP/LLDP 対応リンクを使用することです。	光 *SFP* 光 SFP モニターリング ポリシーの詳細については、光 SFP モニターリング ポリシー（1207ページ）を参照してください。	光 Tx Power、光 Rx Power

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
リンク使用率	A エンド デバイス、A エンド インターフェイス、A メンバー、A エンド受信使用率、A エンド発信使用率、Z エンド デバイス、Z エンド インターフェイス、Z メンバー、イベント時間、属するリンク集約グループを含む、リンクに参加しているインターフェイスのインターフェイス使用率。 （注） このレポートの前提条件は、ネットワークで CDP/LLDP 対応リンクを使用することです。	インターフェイス ヘルス インターフェイス ヘルス モニターリング ポリシーの詳細については、インターフェイスのヘルス モニターリング ポリシー（1200ページ）を参照してください。	統計情報（Statistics）
MPLS リンクの統計情報	MPLS セグメント ルーティングにおけるリンク遅延とジッタの表現。	*MPLS* リンクのパフォーマンス MPLS モニターリング ポリシーの詳細については、MPLS リンク パフォーマンス モニターリング ポリシー（1205ページ）を参照してください。	平均遅延、最小遅延、最大遅延、RX パケット、TX パケット

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
光 SFP インターフェイス	インターフェイスのデバイスの送信/受信電力レベルの表形式表示。デバイス名、インターフェイス名、RxPower、TxPower、EVENTTIME が含まれます。	光 *SFP* 光 SFP モニターリング ポリシーの詳細については、光 SFP モニターリング ポリシー（1207ページ）を参照してください。	光 Tx Power、光 Rx Power
PWE3 統計情報	デバイス名を含む PWE3 トラフィックと可用性の統計情報、IP アドレス、VC ID、ピア アドレス、VC タイプ、現在の受信ビット レート、現在の発信ビット レート、現在の受信バイト レート、現在の発信バイト レート、現在の受信パケット レート、現在の発信パケット レート、グローバル可用性、受信可用性と発信可用性の表形式表示。	疑似回線エミュレーション（エッジ間） 疑似回線エミュレーション（エッジ間）のモニターリング ポリシーの詳細については、疑似回線エミュレーション（エッジ間）モニターリング ポリシー（1202ページ）を参照してください。	PW VC パフォーマンス合計受信 HC パケット レート、PW VC パフォーマンス合計受信 HC バイト レート、PW VC パフォーマンス合計発信 HC パケット レート、PW VC パフォーマンス合計発信 HC バイト レート、PW VC 操作ステータス アップ、PW VC 受信操作ステータス アップ、PW VC 発信操作ステータス アップ、PW VC 操作ステータス ダウン、PW VC パフォーマンス合計受信 HC パケット、PW VC パフォーマンス合計受信 HC バイト、PW VC パフォーマンス合計発信 HC パケット、PW VC パフォーマンス合計発信 HC バイト、PW VC 受信操作ステータス ダウン、PW VC 発信操作ステータス ダウン

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
PWE3 上位 N	デバイス名、IP アドレス、VC ID、ピア アドレス、VC タイプ、平均受信バイト レート、平均発信バイト レート、最大受信バイト レート、最大発信バイト レート、平均受信ビット レート、平均発信ビット レート、最大受信ビット レート、最大発信ビット レート、平均受信パケット レート、平均発信パケット レート、最大受信パケット レート、最大発信パケット レート、グローバル受信可用性とグローバル発信可用性を含む、PWE3 統計情報の上位 N レポートの表形式表示。	疑似回線エミュレーション（エッジ間） 疑似回線エミュレーション（エッジ間）のモニターリング ポリシーの詳細については、疑似回線エミュレーション（エッジ間）モニターリング ポリシー（1202ページ）を参照してください。	PW VC パフォーマンス合計受信 HC パケット レート、PW VC パフォーマンス合計受信 HC バイト レート、PW VC パフォーマンス合計発信 HC パケット レート、PW VC パフォーマンス合計発信 HC バイト レート、PW VC 操作スタータス アップ、PW VC 受信操作ステータス アップ、PW VC 発信操作ステータス アップ、PW VC 操作ステータス ダウン、PW VC パフォーマンス合計受信 HC パケット、PW VC パフォーマンス合計受信 HC バイト、PW VC パフォーマンス合計発信 HC パケット、PW VC パフォーマンス合計発信 HC バイト、PW VC 受信操作ステータス ダウン、PW VC 発信操作ステータス ダウン

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
PWE3 トラフィック グラフ	平均受信ビット レート、平均発信ビット レート、平均受信バイト レート、平均発信バイト レート、平均受信パケット レート、平均発信パケット レート、グローバル可用性、受信可用性と発信可用性を含む、PWE3 トラフィックのグラフィカル表示。	疑似回線エミュレーション（エッジ間） 疑似回線エミュレーション（エッジ間）のモニターリング ポリシーの詳細については、疑似回線エミュレーション（エッジ間）モニターリング ポリシー（1202ページ）を参照してください。	PW VC パフォーマンス合計受信 HC パケット レート、PW VC パフォーマンス合計受信 HC バイト レート、PW VC パフォーマンス合計発信 HC パケット レート、PW VC パフォーマンス合計発信 HC バイト レート、PW VC 操作スタータス アップ、PW VC 受信操作ステータス アップ、PW VC 発信操作ステータス アップ、PW VC 操作ステータス ダウン、PW VC パフォーマンス合計受信 HC パケット、PW VC パフォーマンス合計受信 HC バイト、PW VC パフォーマンス合計発信 HC パケット、PW VC パフォーマンス合計発信 HC バイト、PW VC 受信操作ステータス ダウン、PW VC 発信操作ステータス ダウン

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
QoS ポリシング	ポリシー マップ ClassMap の詳細の表形式表示。詳細には、ポリシー マップの方向、平均超過バイト レート、最大超過バイト レート、最大超過日付、平均違反バイト レート、最大違反バイト レート、最大違反日付、平均適合バイト レート、最大適合バイト レート、最大適合日付、CIR 現在のレートと PIR 現在のレートが含まれます。また、超過、違反、適合のバイト レートのグラフィカル表示も含まれます。	*Quality of Service* サービス品質モニターリング ポリシーの詳細については、QoS サービス モニターリング ポリシー（1203ページ）を参照してください。	適合バイト レート、超過バイト レート、違反バイト レート、超過パケット、違反バイト、CIR、適合バイト、超過バイト、PIR

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
QoS ポリシー（QoS Policy）	ポリシー マップ ClassMap の詳細のグラフィカル表示と表形式表示。詳細には、ポリシー マップの方向、平均事前ポリシー バイト レート、最大事前ポリシー バイト レート、平均事後ポリシー バイト レート、最大事後ポリシー バイト レート、最大事前ポリシー日、最大事後ポリシー日、平均ドロップ率、最大ドロップ率、最大ドロップ日、CIR の平均事前ポリシー、平均インターフェイス速度率、CIR の最大事前ポリシー、最大インターフェイス速度率、CIR の平均事前ポリシー、CIR の最大事前ポリシー、インターフェイス速度日が含まれます。また、事前ポリシー、事後ポリシー、ドロップ ビット レート、ドロップ率のグラフィカル表示も含まれます。	*Quality of Service* サービス品質モニターリング ポリシーの詳細については、QoS サービス モニターリング ポリシー（1203ページ）を参照してください。	ドロップ バイト レート、ドロップ率、事後ポリシー バイト レート、事前ポリシー バイト レート、CIR の事前ポリシー率、CIR の事後ポリシー率、CIR、事後ポリシー レート（バイト/秒）、事前ポリシー バイト

光パフォーマンス レポート

表 15 : 光パフォーマンス レポートに、Cisco EPN Manager でサポートされる光パフォーマンス レポートを示します。すべてのグラフィカルレポートについては、レポートのスケジュールまたは実行時に、最大4つのインターフェイスを選択していることを確認してください。すべて

の表形式レポートについては、レポートのスケジュールまたは実行時に、[表示（Show）]フィールドを使用してページに表示するレコード数を指定してください。

生成されるレポートに表示されるパフォーマンスデータは、モニタリングポリシーを有効にするときに有効化したモニタリング ポリシー パラメータによって異なります。モニターリング タイプおよび関連するパフォーマンス カウンタの詳細な一覧については、モニターリング ポリシー リファレンス（1199ページ）を参照してください。モニターリング ポリシーの詳細については、デバイスおよびネットワークの健全性とパフォーマンスのモニター（281ページ）を参照してください。レポート結果を理解する方法については、レポート出力の例：Web GUI出力と CSV ファイル出力（388 ページ）を参照してください。

（注） これらのレポートのデータを入力するには、[オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、または [オプティカル30秒（Optical 30 secs）] モニターリングポリシーを有効にします。

表 *15* : 光パフォーマンス レポート

レポート	レポート タイプ	内容	有効化する必要があるモニターリング ポリシー パラメータ	ポーリングする必要があるパラメータ
Ethernet	イーサネットレポート：IOS-XR および SVO デバイス	上位層プロトコルから送信が要求されて、宛先がこの副層のマルチキャストまたはブロードキャストアドレスではなかったパケットの総数（廃棄または未送信のものも含む）を示すグラフィカルおよび表形式のレポート。詳細には、エラーなしで送信されたマルチキャストフレームの総数、上位層プロトコルから要求されたパケットの総数、送信されたオクテットの総数、インターフェイスで受信されたオクテットの総数、エラーのために破棄されたパケットの数も含まれます。 新しいレポートのレポート出力をカスタマイズするには、**[レポート（Reports）] > [レポート起動パッド（Report Launch Pad）] > [光パフォーマンス（Optical Performance）] > [イーサネット（Ethernet）]** を選択し、[新規（New）] をクリックして、[設定（Settings）] 領域の [カスタマイズ（Customize）] をクリックします。 既存のレポートのレポート出力をカスタマイズするには、**[レポート（Reports）] > [レポート起動パッド（Report Launch Pad）] > [光パフォーマンス（Optical Performance）] > [イーサネット（Ethernet）]** を選択し、必要なレポートリンクをクリックして、[設定（Settings）] 領域の [カスタマイズ（Customize）] をクリックします。	[オプティカル1日（Optical 1 day）]、 [オプティカル15分（Optical 15 mins）]、 または[オプティカル30秒（Optical 30 secs）] 光モニターリング ポリシーによって収集される情報については、モニターリング ポリシー リファレンス（1199ページ）を参照してください。 レポート結果を理解する方法については、レポート出力の例：Web GUI 出力と CSV ファイル出力（388ページ）を参照してください。	Ethernet

レポート	レポート タイプ	内容	有効化する必要があるモニターリング ポリシー パラメータ	ポーリングする必要があるパラメータ
OTN	セクションモニターリング近端および遠端レポート：NCS1K、NCS2K、NCS4K（Section Monitoring NEnd & FEnd Reports-NCS1K, NCS2K and NCS4K）	OTN回線タイプのデバイスとインターフェイスのOTN セクション モニターリング詳細を示すグラフィカルおよび表形式のレポート。詳細には、バックグラウンドブロック エラーの数とその比率、エラー秒数とその比率、重大エラー秒数とその比率、使用不可秒数、および障害カウントの数が含まれます。	[オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、または[オプティカル30秒（Optical 30 secs）] 光モニターリング ポリシーによって収集される情報については、モニターリング ポリシー リファレンス（1199ページ）を参照してください。 レポート結果を理解する方法については、レポート出力の例：Web GUI 出力とCSV ファイル出力（388ページ）を参照してください。	OTN DWDM インフラストラクチャ[1]
	パス モニターリング近端および遠端レポート（Path Monitoring NEnd & FEnd Reports）	OTN回線タイプのデバイスとインターフェイスのOTN パス モニターリング詳細を示すグラフィカルおよび表形式のレポート。バックグラウンドブロック エラーの数とその比率、エラー秒数とその比率、重大エラー秒数とその比率、使用不可秒数、障害カウントの数などの詳細が提供されます。		
	前方誤り訂正レポート：NCS1K、NCS2K、NCS4K（Forward Error Correction Reports-NCS1K, NCS2K and NCS4K）	OTN回線タイプのデバイスとインターフェイスのOTN前方誤り訂正詳細を示すグラフィカルおよび表形式のレポート。詳細には、ECW、UCW、ビットエラー訂正の数、訂正不可能なワードの数、およびパフォーマンスモニタリングの時間間隔中に検出された事前前方誤り訂正ベースのビットエラーカウントが含まれます。		
	タンデム接続モニターリング近端および遠端レポート（Tandem Connection Monitoring NEnd & FEnd Reports）	OTN回線タイプのデバイスとインターフェイスのタンデム接続モニターリング詳細を提供するグラフィカルおよび表形式のレポート。詳細には、バックグラウンドブロック エラーの数とその比率、エラー秒数とその比率、重大エラー秒数とその比率、使用不可秒数、および障害カウントの数が含まれます。		OTN
	GFP 統計レポート：NCS2K および NCS4K（GFP Statistics Reports–NCS2K and NCS4K）			OTN DWDM インフラストラクチャ[1]

レポート	レポート タイプ	内容	有効化する必要があるモニターリング ポリシー パラメータ	ポーリングする必要があるパラメータ
		OTN回線タイプのデバイスのジェネリック フレーミング プロシージャ（GFP）統計を提供するグラフィカルおよび表形式のレポート。GFP 統計には、送受信したGFPフレームとバイトの数、受信したシングル ビット エラーとマルチ ビット エラーの数、CRC エラー/無効な GFP タイプ/無効な CID で受信したパケットの数、送受信したCMFフレームの数、および cHEC と tHEC のマルチ ビット エラーの数が含まれます。		

レポート	レポート タイプ	内容	有効化する必要があるモニターリング ポリシー パラメータ	ポーリングする必要があるパラメータ
Physical	光パワーレポート：NCS1K、NCS2K、SVO、および NCS4K	物理回線タイプのデバイスで送受信した信号の光入出力パワーの平均、最小、および最大パーセンテージを提供するグラフィックおよび表形式のレポート。 （注） グラフィックレポートは、SVO デバイスではサポートされていません。	[オプティカル1日（Optical 1 day）]、 [オプティカル15分（Optical 15 mins）]、 または[オプティカル30秒（Optical 30 secs）] 光モニターリング ポリシーによって収集される情報については、モニターリング ポリシー リファレンス（1199ページ）を参照してください。 レポート結果を理解する方法については、レポート出力の例：Web GUI 出力と CSV ファイル出力（388ページ）を参照してください。 （注） *[オプティカル 30 秒（Optical 30 secs）]* SVO デバイスには適用されません。	Physical DWDM インフラストラクチャ[1]
	レーザーバイアス電流レポート：NCS1K、NCS2K、SVO、および NCS4K	レーザーバイアス電流の平均、最小、および最大パーセンテージを提供するグラフィックおよび表形式のレポート。レーザーバイアス電流は、整数のパーセンテージで表現される正規化された値です。 （注） グラフィックレポートは、SVO デバイスではサポートされていません。		
	光物理レポート：CS1K、NCS2K、SVO、および NCS4K	単方向ポート上の光パワーの平均、最小、および最大値を提供するグラフィックおよび表形式のレポート。詳細には、光サービスチャネルの平均、最小、および最大電力レベル、光信号対雑音比の平均、最小、最大、光パワーの警告、波長分散、2次偏波モード分散、偏波依存損失、微分群遅延、偏波変化率、および位相ノイズが含まれます。 （注） グラフィックレポートは、SVO デバイスではサポートされていません。		

レポート	レポート タイプ	内容	有効化する必要があるモニターリング ポリシー パラメータ	ポーリングする必要があるパラメータ
SDH または SONET	SDH リジェネレータ セクション レポート（SDH Regenerator Section Report）	ネットワーク内のデバイスのSDHリジェネレータセクション層のパフォーマンスモニターリング詳細を提供するグラフィカルおよび表形式のレポート。詳細には、バックグラウンドブロックエラーの数とその比率、エラー秒数とその比率、重大エラー秒数とその比率、使用不可秒数、エラーブロックの数、およびフレーム同期外れ秒数が含まれます。	[オプティカル1日（Optical 1 day）] または *[光 15 分（Optical 15 mins）]* 光モニターリング ポリシーによって収集される情報については、モニターリング ポリシー リファレンス（1199ページ）を参照してください。 レポート結果を理解する方法については、レポート出力の例：Web GUI 出力と CSV ファイル出力（388ページ）を参照してください。	SDH/SONET DWDM インフラストラクチャ[1]
	SDH 多重化セクション近端および遠端レポート：NCS2K（SDH Multiplex Section NEnd & FEnd Reports - NCS4K）	ネットワーク内のデバイスのSDH多重化セクション層のパフォーマンスモニターリング詳細を提供するグラフィカルおよび表形式のレポート。詳細には、バックグラウンドブロックエラーの数とその比率、エラー秒数とその比率、重大エラー秒数とその比率、使用不可秒数、エラーブロックの数、障害カウントの数、保護スイッチング（スイッチングカウント）、リングカウント、スパンカウント、作業カウント、時間、着信転送までの時間、スパン時間、および作業時間が含まれます。		
	SDH 多重化セクション近端および遠端レポート：NCS4K（SDH Multiplex Section NEnd & FEnd Reports - NCS4K）	ネットワーク内のデバイスのSDH多重化セクション層のパフォーマンスモニターリング詳細を提供するグラフィカルおよび表形式のレポート。詳細には、バックグラウンドブロックエラーの数とその比率、エラー秒数とその比率、重大エラー秒数とその比率、使用不可秒数、およびエラーブロックの数が含まれます。		
	SONET セクション レポート（SONET Section Report）	ネットワーク内のデバイスの SONET セクション層のパフォーマンスモニターリング詳細を提供するグラフィカルおよび表形式のレポート。詳細には、符号違反の数、エラー秒数、重大エラー秒数、および重大エラー フレーム秒数が含まれます。		
	SONET 回線近端および遠端レポート：NCS2K（SONET Line NEnd & FEnd Reports - NCS2K）			

レポート	レポート タイプ	内容	有効化する必要があるモニターリング ポリシー パラメータ	ポーリングする必要があるパラメータ
		ネットワーク内のデバイスの SONET 回線層のパフォーマンス モニターリング詳細を提供するグラフィカルおよび表形式のレポート。詳細には、符号違反の数、エラー秒数、重大エラー秒数、使用不可秒数、障害カウントの数、保護スイッチング（スイッチングカウント）、リングカウント、スパンカウント、作業カウント、時間、着信転送までの時間、スパン時間、および作業時間が含まれます。		
	SONET 回線近端および遠端レポート：NCS4K（SONET Line NEnd & FEnd Reports - NCS4K）	ネットワーク内のデバイスの SONET 回線層のパフォーマンス モニターリング詳細を提供するグラフィカルおよび表形式のレポート。詳細には、符号違反の数、エラー秒数、重大エラー秒数、使用不可秒数、および障害カウントの数が含まれます。		

1. すべての Cisco Optical Networking Services（ONS）および Cisco Network Convergence System（NCS）2000 シリーズのデバイスに対してこのパラメータを有効化する必要があります。

パフォーマンス レポート

この項では、Cisco EPN Manager でサポートされる基本的なパフォーマンス レポートを一覧表示します。また、各レポート タイプで有効にする必要があるモニターリング ポリシーとパラメータもリストされます。これらのレポートは、光およびキャリア イーサネット技術の両方に適用されます。

（注） アスタリスク（*）が付いたレポートタイプは、SVO および Cisco NCS 2000 シリーズ デバイスに適用されます。

モニターリング ポリシーの詳細については、デバイスおよびネットワークの健全性とパフォーマンスのモニター （281 ページ）を参照してください。

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
環境温度（Environmental Temperature）*	ネットワークデバイスのデバイス IP アドレス、名前、センサー名、センサータイプ、最大インレット温度、その他の最大温度、およびイベントタイムを表形式で表示します。	*Device Health* デバイス ヘルス モニターリングポリシーの詳細については、デバイスのヘルスモニターリングポリシー（1199 ページ）を参照してください。	環境温度（Environment Temperature）
Threshold Violations	表にネットワークのしきい値違反アラームデータ（送信元、イベント タイプ、カテゴリ、説明）が一覧表示されます。	インターフェイスヘルス デバイス ヘルス モニターリングポリシーの詳細については、デバイスのヘルスモニターリングポリシー（1199 ページ）を参照してください。	管理ステータスのアップ/ダウン（Admin Status Up/Down） 動作ステータスのアップ/ダウン（Operational Status Up/Down） 管理ステータスのアップおよび動作ステータスのダウンの割合（Admin Status Up and Operational Status Down Percentage）

Network Summary レポート

この項では、Cisco EPN Manager でサポートされる Network Summary レポートを一覧表示します。次のレポートでは、ネットワークのヘルスの情報について説明します。

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	ポーリングする必要があるパラメータ
リンク フラップ レポート（Link Flap Report）	A エンドデバイス、A エンドインターフェイス、Z エンド デバイス、Z エンドインターフェイス、リンク名、フラップ数の表形式表示。	NA	NA

デバイス レポート

この項では、Cisco EPN Managerでサポートされるデバイス レポートを一覧表示します。また、各レポート タイプで有効にする必要があるモニターリング ポリシーとパラメータもリストされます。これらのレポートは、光およびキャリア イーサネット技術の両方に適用されます。

（注） アスタリスク（*）が付いたレポートタイプは、SVOおよびCisco NCS 2000シリーズデバイスに適用されます。

モニターリング ポリシーの詳細については、デバイスおよびネットワークの健全性とパフォーマンスのモニター （281 ページ）を参照してください。

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
[アラームレポート（Alarm Report）]	ネットワーク内のデバイスのアラームのリスト。重大度、メッセージ、ステータス、障害原因、タイムスタンプ、作成時刻、デバイス タイムスタンプ、所有者、カテゴリ、条件、場所、サービスの影響、サテライトIDが含まれます。	NA	NA
[CPU使用率（CPU Utilization）]	すべてのデバイスと指定した期間の平均CPU使用率を一覧表示するテーブル。	*Device Health* デバイス ヘルス モニターリング ポリシーの詳細については、デバイスのヘルス モニターリング ポリシー （1199 ページ） を参照してください。	CPU使用率
ハードウェアの詳細情報 *	インベントリまたはデバイス タイプ全体のハードウェア情報（スイッチおよびハブ、ルータ、および光トランスポートなど）。	NA	NA
ソフトウェアの詳細情報 *	インベントリまたはデバイス タイプ全体のソフトウェア情報（スイッチおよびハブ、ルータ、および光トランスポートなど）。	NA	NA
[デバイス アベイラビリティ（Device Availability）]	ネットワーク内で利用可能なすべてのデバイスとその到達可能性の割合を一覧表示するテーブル。	NA	NA

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
デバイス クレデンシャルの検証	ネットワーク内のデバイスのクレデンシャル ステータス。各デバイスのログイン、到達可能性、およびプロトコル ステータスが含まれます。また、デバイスの最終変更日時が含まれます。	NA	NA
Device Health	指定された期間のネットワーク デバイスの CPU 使用率、メモリ使用率、および応答可能性情報。デバイス上のすべての CPU モジュールおよびメモリ プールの最小、最大、および平均が含まれます。	*Device Health* デバイス ヘルス モニターリング ポリシーの詳細については、デバイスのヘルス モニターリング ポリシー（1199 ページ） を参照してください。	CPU 使用率
デバイスのシリアル番号	ネットワークに存在するデバイスのシリアル番号を一覧表示します。	NA	NA
[イベントレポート（Event Report）]	ネットワーク内のデバイスのイベントのリスト。説明、障害原因、タイム スタンプ、デバイス タイムスタンプ、重大度、カテゴリ、条件が含まれます。	NA	NA
Identity Capability	ネットワーク内のスイッチのアイデンティティ機能の概要情報。	NA	NA
[物理インターフェイス（Physical Interface）]（以前の [インターフェイスの詳細（Interface Detail）]）	ネットワーク内のデバイスのインターフェイスの詳細。デバイス名、ポート名、ポートの説明、MAC アドレス、管理ステータス、動作ステータスが含まれます。	NA	NA
IP インターフェイス	ネットワーク内のデバイスの論理ポートデータ。デバイス名、ポート名、ポート IP アドレス、ポートの説明、管理ステータス、動作ステータスが含まれます。	NA	NA

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
インベントリ *	ネットワーク内のデバイスの基本的なインベントリ データ。モデル別のコントローラの数、ソフトウェア バージョン別のコントローラの数、コントローラ インベントリ、モデル別の AP の数、ソフトウェア バージョン別の AP の数、AP インベントリ、関連付け解除 AP、自律 AP インベントリ、メンテナンス モード AP、バージョン別の MSE の数、MSE、モデル別のスイッチの数、バージョン別のスイッチの数、スイッチ インベントリ、スイッチ デバイス ソフトウェア イメージ、モデル別のルータの数、バージョン別のルータの数、ルータ インベントリ、ルータ デバイス ソフトウェア イメージ、モデル別の Cisco インターフェイスおよびモジュール デバイスの数、ソフトウェア バージョン別の Cisco インターフェイスおよびモジュール デバイスの数、Cisco インターフェイスおよびモジュールのデバイス インベントリ、Cisco インターフェイスおよびモジュール - ソフトウェア イメージ、モデル別のストレージ ネットワーキング デバイスの数、ソフトウェア バージョン別のストレージ ネットワーキング デバイスの数、ストレージ ネットワーキング デバイス インベントリ、ストレージ ネットワーキング デバイス - ソフトウェア イメージ、モデル別のセキュリティおよび VPN の数、ソフトウェア バージョン別のセキュリティおよび VPN の数、セキュリティおよび VPN インベントリが含まれます。	NA	NA
リンク レポート	ネットワーク内の OTU、OTS、ODU、OMS 対応リンクのリンク使用率。	*Device Health* デバイス ヘルス モニターリング ポリシーの詳細については、デバイスのヘルス モニターリング ポリシー（1199 ページ） を参照してください。	NA

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
メモリ使用率（Memory Utilization）	指定された期間のメモリ使用率情報。すべてのメモリプール/モジュールに関する情報が含まれます。	*Device Health* デバイス ヘルス モニターリング ポリシーの詳細については、デバイスのヘルス モニターリング ポリシー（1199ページ） を参照してください。	[メモリ プール使用率（Memory Pool Utilization）]
ネットワークインベントリの詳細	ネットワークのネットワークインベントリ情報には、デバイス名、機器タイプ、動作ステータス、実際の機器タイプ、物理的な場所、CLEI コード、ハードウェア部品番号、製造日、シリアル番号、製品 ID、バージョン ID、および UDF（[設定（Settings）] タブの列リストから選択された場合） が含まれます。	*Device Health* デバイス ヘルス モニターリング ポリシーの詳細については、デバイスのヘルス モニターリング ポリシー（1199ページ） を参照してください。	NA
ポート キャパシティ	ネットワーク内のデバイスのインターフェイス使用率（%）。	NA	NA
SFP ポートとモジュールの詳細	ネットワーク上の Small Form-factor Pluggable およびモジュールの詳細を一覧表示します。	NA	NA
サードパーティデバイスの詳細	ネットワーク上のサードパーティデバイスの詳細を一覧表示します。	NA	NA
PTP の状態	PTP クロッククラス、PTP サーボ、ポートインデックス、PTP 境界クロックデータ。	PTP/SyncE モニターリングポリシー PTP/SyncE モニターリングポリシーの詳細については、PTP/SyncE モニターリングポリシー（1203ページ）を参照してください。	NA

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
PWIDインベントリ	ローカルデバイスとピアデバイスの PWID を表示し、エクスポートします。ドメインごと、およびルータごとにすべてのサービスのすべての PWID を一覧表示します。	*Device Health* デバイス ヘルス モニターリング ポリシーの詳細については、デバイスのヘルス モニターリング ポリシー（1199 ページ） を参照してください。	NA
VLAN	ネットワーク内のスイッチの VLAN 情報。	NA	NA
VLAN 詳細（VLAN Detailed）	ネットワーク内のスイッチの詳細なVLAN情報。VLAN ID、VLAN 名、VTP ドメイン名、管理ステータス、デバイスIPアドレス、デバイス名、インターフェイスIPアドレス、動作 VLAN モード、および動作ステータスが含まれます。	NA	NA
有線デバイスインベントリの詳細情報 *	ネットワーク内の有線デバイスの詳細なインベントリデータ。システム情報、シャーシ情報、モジュール情報、モジュール ポート インターフェイス、VLANインターフェイス、ソフトウェア イメージ情報、メモリ プール情報、フラッシュ デバイス、フラッシュ パーティション、フラッシュ ファイルが含まれます。 （注） レポートを保存せずにすぐに実行する場合は、最大 5 台のデバイスを選択できます。6 台以上のデバイスを含めるには、レポートを保存またはスケジュール設定します。	NA	NA
有線デバイスの可用性 *	ネットワークで最高の可用性の有線デバイスのリスト。デバイス名、平均可用性（%）が含まれます。 （注） このレポートは SVO デバイスには適用されません。	NA	NA
有線モジュールの詳細 *	デバイス名、デバイス IP、機器名、ポート数、動作ステータス、ベンダー機器タイプ、製造元、シリアル番号、UDI など、ネットワーク内の有線デバイスの詳細なモジュール情報を示すテーブル。	NA	NA

レポート タイプ	内容	有効にする必要があるモニターリング ポリシー	有効化する必要があるパラメータ
有線ポートの属性	管理ステータス、動作ステータス、MACアドレスなどのポート属性情報。VLAN ID、アクセスモードVLAN、デバイスIPアドレス、インターフェイスIPアドレス、説明、MACアドレス、管理ステータス、動作ステータス、タイプ、MTU、速度、デュプレックス、IsTrunk、トランクカプセル化が含まれます。	*Device Health* デバイス ヘルス モニターリング ポリシーの詳細については、デバイスのヘルス モニターリング ポリシー（1199ページ）を参照してください。	NA
有線ポートプラガブル属性	プラガブルモデル情報、プラガブルの説明、プラガブルタイプ、ポート名、デバイスIPアドレス、インターフェイスip_address、MACアドレス、動作ステータス、MTU、速度などのポートプラガブル属性情報。	*Device Health* デバイス ヘルス モニターリング ポリシーの詳細については、デバイスのヘルス モニターリング ポリシー（1199ページ）を参照してください。	NA

SFTP リポジトリの設定

レポートをエクスポートできる外部 SFTP リポジトリ（ローカルまたはリモート）を設定できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [全般（General）] > [レポート（General）]** に移動します。

ステップ 2 [外部サーバー設定（External Server Settings）] 領域の下に表示されるフィールドに SFTP サーバーの詳細を入力します。

ステップ 3 [保存（Save）] をクリックします。

新しいレポートの作成、スケジュール設定、実行

[レポート起動パッド（Report Launch Pad）] では、1 つのページからすべての Cisco EPN Manager レポートにアクセスできます。このページでは、すべてのレポート操作（作成、保存、表示、スケジュール設定、カスタマイズ）を実行できます。

レポートの詳細を表示するには、レポートの種類の横にあるツールチップにカーソルを移動します。

新しいレポートを作成してスケジュール設定し、実行するには、次の手順に従います。

始める前に

外部 SFTP リポジトリへのレポートのエクスポートを予定している場合は、外部サーバーが設定されていることを確認します。詳細については、SFTP リポジトリの設定（381 ページ）を参照してください。

ステップ 1 左側のサイドバーから、**[レポート（Reports）]** > **[レポート起動パッド（Report Launch Pad）]** を選択します。

ステップ 2 起動するレポートを見つけ、[新規作成（New）] をクリックします。

[レポート期間（Report Period）] フィールドの一部として新しいテキストボックスの [過去（Last）] が追加され、ユーザーは過去 24 時間のレポートを生成できるようになりました。

（注） 1 ～ 24 の範囲（過去 24 時間）で値を入力します。

ステップ 3 [レポートの詳細（Report Details）] ページで、レポートのタイトルを入力します。

[レポート タイトル（Report Title）] フィールドを編集できます。

ステップ 4 ドロップダウンリストから適切な [レポート作成者（Report By）] カテゴリを選択します。

ステップ 5 [レポート基準（Report Criteria）] フィールドでは、前の [レポート作成者（Report By）] で行った選択に応じて結果を分類できます。

（注） 上部の仮想ドメイン チェックボックスを選択した場合、レポート条件フィルタに 1 つ以上の値が存在する場合は、編集ボタンが有効になります。

ステップ 6 [編集（Edit）]をクリックしてデバイス選択ウィザードを開き、必要なデバイスを選択します。[プレビュー（Preview）] タブをクリックして、選択したデバイスを確認し、[OK] をクリックします。選択したデバイスを削除することもできます。

[レポートの詳細（Report Details）] ページに表示されるパラメータは、選択するレポートのタイプによって異なります。一部のレポートでは、レポートの結果をカスタマイズする必要があります。レポート結果のカスタマイズ方法の詳細については、レポート結果のカスタマイズ（384 ページ）を参照してください。

ステップ 7 このレポートを後で実行するか、または繰り返しのレポートとして実行する場合は、[スケジューリング（Scheduling）] を選択し、必要なスケジュールパラメータを入力します。スケジューリングを有効にすると、[保存（Save）] を除くすべてのオプションが非表示になります。

ステップ 8 レポートを実行するには、次のいずれかのオプションを選択します。

- [実行（Run）]：レポート設定を保存せずにレポートを実行します。
- [保存（Save）]：レポートをすぐに実行せずにこのレポート設定を保存します。スケジュールパラメータが入力済みの場合は、スケジュールされた日時にレポートが自動的に実行されます。
- [実行して保存（Run and Save）]：レポートの設定を保存し、ただちにレポートを実行します。

- [保存してエクスポート（Save and Export）]：レポートを保存して実行し、結果をファイルにエクスポートします。レポートのエクスポートオプションと電子メールオプションを選択するように求められます。 使用可能なエクスポートオプションは次のとおりです。
  - [エクスポート形式（Export Format）]：CSV または PDF 形式を選択します。CSV ファイルは、最大 100 万件のレコードを持つことができる single.csv ファイルです。レコード数が 100 万を超えた場合、Cisco EPN Manager は別の CSV ファイルを生成して残りのレコードを収容します。両方の CSV ファイルが zip 形式でエクスポートされます。

    （注） この条件は、[レポート（Reports）] 起動パッドの下に表示されるレポートに適用され、シンプルなレポートとも呼ばれます。カスタムレポートには、この条件チェックはありません。

  - [エクスポートデリミタ（Export Delimiter）]：このフィールドは、レポートをエクスポートするために CSV 形式を選択した場合にのみ使用できます。次の文字のいずれかを入力します。**＊＃@％^＆|,!$**を使用すると、エクスポートされたデータが区切り記号で区切られた状態で表示されます。
  - [ファイルにエクスポート（Export to File）]：オンデマンドリポジトリ/localdisk/ftp/reportsOnDemand/ にレポートをエクスポートするには、このオプションを選択します。
  - [SFTP にエクスポート（Export to SFTP）]：レポートを SFTP リポジトリにエクスポートするには、このオプションを選択します。

    （注） このオプションを選択する前に、SFTP リポジトリが設定されていることを確認します。

  - [電子メール（Email）]：Cisco EPN Manager がレポートを生成した後に電子メールを送信するには、このオプションを選択します。宛先の電子メールアドレス、件名行の内容、およびエクスポートしたファイルを添付ファイルとして含めるかどうかを入力します。

  操作が終了したら、[OK] をクリックします。

- [保存して電子メール送信（Save and Email）]：レポートを保存して実行し、結果をファイルにエクスポートして電子メールで送信します。以下を要求するプロンプトが表示されます。
  - エクスポートするレポートのファイル形式を選択します。
  - 宛先メール アドレスと電子メールの件名を入力します。

    （注） Cisco EPN Manager では、CSV として [エクスポート形式（Export Format）] を選択して [保存および電子メール（Save and Email）] オプションをクリックすると、15,000 個を超えるレコードがファイルにある場合は、CSV ファイルが zip 形式で送信されます。レコードが 15,000 個未満のファイルはプレーンな CSV ファイルとして送信されます。

  操作が終了したら、[OK] をクリックします。

- [キャンセル（Cancel）]：このレポートを実行も保存もせずに前のページに戻ります。

レポート結果のカスタマイズ

多くのレポートでは、結果をカスタマイズして各種の情報を含めたり、除外したりすることができます。この機能をサポートしているレポートには、[カスタマイズ（Customize）]ボタンが表示されます。このボタンをクリックして[カスタム レポートの作成（Create Custom Report）]ページにアクセスし、レポートの結果をカスタマイズできます。

レポート結果をカスタマイズするには、次の手順に従います。

ステップ 1 カスタマイズするレポートを選択します。

a) 新しいレポートを作成します。**[レポート（Reports）]** > **[レポート起動パッド（Report Launch Pad）]** をクリックします。

b) 定期レポートをカスタマイズします。**[レポート（Reports）]**>**[保存済みレポートのテンプレート（Saved Report Templates）]** をクリックし、レポート名のハイパーリンクをクリックします。

ステップ 2 [レポートの詳細（Report Details）] ページで [カスタマイズ（Customize）] をクリックします。

ステップ 3 [カスタム レポートの作成（Create Custom Report）] ページで、必要な情報を入力し、[適用（Apply）] をクリックして変更を確定します。

ステップ 4 [レポートの詳細（Report Details）] ページで [保存（Save）] をクリックします。

ユーザー定義フィールドを使用したレポート データのフィルタ処理とカスタマイズ

カスタム属性を作成し、それらに値を割り当てることができます。ユーザー定義フィールド（UDF）の作成方法については、カスタム値用のユーザー定義フィールドの作成（138ページ）を参照してください。その後、UDF を使用して、レポート結果をフィルタ処理したり、カスタマイズすることができます。

Cisco EPN Manager は、2 分ごとに作成される UDF の値をスキャンし、メタデータが保存される UDF.json ファイルを生成します。このファイルには、`/opt/CSCOlumos/conf/rfm/classes/com/cisco/server/reports/conf/UDF.json` からアクセスできます。

次に、UDF.json ファイルに UDF のメタデータを表示する例を示します。

```
[
  {
    "label": "internal",
    "hidden": true,
    "displayName": "Internal",
    "fixedColumn": false
  },
  {
    "label": "location",
```

```
    "hidden": true,
    "displayName": "Location",
    "fixedColumn": false
  },
  {
    "label": "quality",
    "hidden": true,
    "displayName": "Quality",
    "fixedColumn": false
  },
```

この例では、次のようになります。

- 属性の *label* は、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [全般（General）] > [ユーザー定義フィールド（User Defined Fields）]**ページで作成されたユーザー定義フィールドです。
- 属性の hidden はデフォルトで False に設定されています。この属性が True に設定されている場合、UDF は [レポート（Report）] ページで非表示になります。レポート結果をカスタマイズするときに UDF を選択できるように、この属性を False に設定する必要があります。
- 属性の *displayName* は、レポート結果に表示される UDF 名を変更するために使用されます。
- 属性の *fixedColumn* は、hidden 属性が False に設定されている場合にのみ適用されます。

UDF.json ファイルで必要な変更を行った後に、レポートの結果をカスタマイズできます。レポート結果のカスタマイズ （384 ページ） を参照してください。

次のレポートについては、UDF に基づいてレポートをフィルタリングおよびカスタマイズできます。

レポートカテゴリ	レポート名	レポートタイプ
CE パフォーマンス	インターフェイスのグラフ	インターフェイス入力使用率グラフ（Interface In Utilization Graph）
		インターフェイス着信トラフィック グラフ
		インターフェイス出力使用率グラフ（Interface Out Utilization Graph）
		インターフェイス発信トラフィック グラフ（Interface Out Traffic Graph）
	インターフェイス上位 N	インターフェイス上位 N 入力使用率
		トラフィック上位 N 着信トラフィック
		インターフェイス上位 N 出力使用率
		トラフィック上位 N 発信トラフィック
		インターフェイス下位 N 可用性（Interface Bottom N Availability）
	インターフェイス トラフィック（Interface Traffic）	Interface Errors and Discards
		インターフェイス トラフィック レポート（Interface Traffic Report）
		インターフェイス CRC エラー レポート
パフォーマンス	Environmental Temperature	要約された環境温度
		現在の環境温度

レポートカテゴリ	レポート名	レポートタイプ
デバイス	CPU 使用率	CPU 使用率
		上位 CPU 使用率
		下位 CPU 使用率
	メモリ使用率（Memory Utilization）	メモリ使用率
		上位メモリ使用率
		下位メモリ使用率
	有線モジュールの詳細	有線モジュール詳細レポートの詳細
	有線デバイスの詳細なインベントリ	有線デバイスの詳細なインベントリレポートの詳細

UDF.json ファイル内の UDF のフィルタ タイプを変更することもできます。デフォルトのフィルタ タイプは String です。

次に、フィルタ タイプとその定義の例を示します。

```
[
  {
    "label": "internal",
    "displayName": "Internal",
    "hidden": false,
    "fixedColumn": false,
    "filterMetadata": {
      "sqlDataType": "Boolean",
      "attr": "internal",
      "label": "UDF: Internal Used",
      "filterType": "boolean"
    }
  },
  {
    "label": "location",
    "displayName": "Location",
    "hidden": false,
    "fixedColumn": false
  },
  {
    "label": "quality",
    "displayName": "Quality",
    "hidden": false,
    "fixedColumn": false,
    "filterMetadata": {
      "sqlDataType": "Number",
      "selectItems": {
        "1": "High Quality",
        "2": "Mid Quality",
        "3": "Low Quality"
      },
      "attr": "quality",
      "label": "UDF: Quality",
      "filterType": "enumeration"
```

```
    }
  },
  {
    "label": "sapid",
    "displayName": "SAP ID",
    "hidden": false,
    "fixedColumn": true,
    "filterMetadata": {
      "sqlDataType": "Number",
      "attr": "sapid",
      "label": "UDF: SAP ID",
      "filterType": "numeric"
    }
  },
  {
    "label": "startTime",
    "displayName": "Start Time",
    "hidden": false,
    "fixedColumn": false,
    "filterMetadata": {
      "sqlDataType": "Timestamp",
      "attr": "startTime",
      "label": "UDF: Start Time",
      "filterType": "datetime"
    }
  },
  {
    "label": "vendor",
    "displayName": "Vendor",
    "hidden": false,
    "fixedColumn": true,
    "filterMetadata": {
      "sqlDataType": "String",
      "selectItems": {
        "huawei": "Hua Wei",
        "alu": "Alcatel Lucent",
        "cisco": "Cisco"
      },
      "attr": "vendor",
      "label": "UDF: Vendor",
      "filterType": "enumeration"
    }
  }
]
```

UDF.json ファイルで必要な変更を行った後、[Report Details] ページの [Advanced Filter] オプションを使用してレポートデータをフィルタ処理します。

レポート出力の例：Web GUI 出力と CSV ファイル出力

この例では、ネットワークの近端で使用可能な Cisco NCS 2000 シリーズ デバイスのセクションモニターリング レポートが生成されます。[レポートの詳細（Report Details）]ページの下部に結果を表示するか、結果を CSV または PDF ファイルにエクスポートするかを選択できます。レポートを作成して実行する方法の詳細については、「新しいレポートの作成、スケジュール設定、実行 （381 ページ）」を参照してください。

次の図は、[レポートの詳細（Report Details）] ページの下部に結果がどのように表示されるかを示しています。

SectionMonitoringNearEndNCS2K
Generated: 2015-Apr-02, 17:52:03 IST
Cisco EPN Manager
Report By: Interfaces By Device
Devices: M6-235-140;nmtgte-m6-159;M6-235-139
Report Interval: 15 minutes
Reporting Period: Last 6 hours
Show: All records
Section Monitoring NEnd Report

Device Name	Device IP Address	Interface	DateTime	BBE-SM	BBER-SM	ES-SM	ESR-SM	SES-SM	SESR-SM	UAS-SM	FC-SM
M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:00:00 IST	0	0.00000	0	0.00000	0	0.00000	0	0
M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:15:00 IST	0	0.00000	0	0.00000	0	0.00000	0	0
M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:30:00 IST	0	0.00000	0	0.00000	0	0.00000	0	0
M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 13:00:00 IST	0	0.00000	0	0.00000	0	0.00000	0	0

403223

スケジューリングが有効になっており、結果をCSVファイルにエクスポートした場合、レポートは/localdisk/ftp/reportsというリポジトリに保存されます。レポートリポジトリの場所は調整できます。詳細については、レポートの消去 （993 ページ）を参照してください。

（注） スケジューリングが無効になっており、結果をCSVファイルにエクスポートした場合、レポートは /localdisk/ftp/reportsOnDemand というリポジトリに保存されます。

CSV ファイルのファイル命名規則は *ReportTitle_yyyymmdd_hhmmss*.csv です。*yyyymmdd* はレポート結果をエクスポートした年月日、*hhmmss* は時、分、秒です。

次の図は、結果が CSV ファイルでどのように表示されるかを示しています。

	A	B	C	D	E	F	G	H	I	J	K	L
1	Section Monitoring Report for Cisco NCS 2000 Series Devices											
2	Generated: 20 17:52:03 IST											
3	Report By: Interfaces By Device											
4	Devices: M6-235-140;nmtgte-m6-159;M6-235-139											
5	Report Interval: 15 minutes											
6	Reporting Period: Last 6 hours											
7	Show: All records											
8												
9	Section Monitoring NEnd Report											
10	Device Name	Device IP Address	Interface	DateTime	BBE-SM	BBER-SM	ES-SM	ESR-SM	SES-SM	SESR-SM	UAS-SM	FC-SM
11	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:00:00 IST	0	0	0	0	0	0	0	0
12	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:15:00 IST	0	0	0	0	0	0	0	0
13	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:30:00 IST	0	0	0	0	0	0	0	0
14	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 13:00:00 IST	0	0	0	0	0	0	0	0

403224

次の表に、セクション モニターリング レポートの結果を解釈する方法の説明を示します。

列名	説明
デバイス名（Device Name）	ネットワークの近端にあるデバイスの名前。
Device IP Address（デバイス IP アドレス）	デバイスの IP アドレス
インターフェイス（Interface）	デバイスのインターフェイス名。

列名	説明
日時（DateTime）	デバイスのセクションモニターリングデータが収集された日時。この列の値は、レポートの作成時に選択したレポート間隔によって異なります。レポート間隔は 15 分または 24 時間です。
BBE-SM	デバイスのバックグランドブロック エラーの数。
BBER-SM	デバイスのバックグランド ブロック エラー率。
ES-SM	デバイスのエラー秒数。
ESR-SM	デバイスのエラー秒比率。
SES-SM	デバイスの重大エラー秒数。
SESR-SM	デバイスの重大エラー秒比率。
UAS-SM	デバイスの使用不可秒数。
FC-SM	デバイスの障害カウント（AIS/RFI 検出）の数。

他の光パフォーマンス レポートの結果に表示されるパフォーマンス カウンタの詳細については、「光モニターリング ポリシーのパフォーマンス カウンタ（1210ページ）」を参照してください。

空のレポートのトラブルシューティングのヒント

レポートが正常に実行されたものの、エクスポートできる出力ファイルがない場合は、次のいずれかのトラブルシューティングのヒントを試すことができます。

確認事項	次に例を示します。
...正しい監視ポリシーを有効にしました。有効にする必要がある監視ポリシーの詳細については、モニターリング ポリシー リファレンス（1199 ページ）を参照してください。	QoS レポートの場合、QoS 監視ポリシーを有効にする必要があります。

確認事項	次に例を示します。
...定期的な収集を有効にしました。	システム監視定期レポート（CPU/ディスク/メモリ）の場合は、定期的な収集を有効にする必要があります。有効にした後は、出力を確認するために12時間後にレポートを生成する必要があります。 （注） 定期的な収集を有効にするには、**`https://<Server IP>/webacs/ncsDiag.do`** にある [システム監視設定（System Monitoring Setting）] で [定期的な収集を有効化（Periodic Collection Enable）] ボタンをクリックします。
...特定のレポートに正しいデバイス タイプを選択しました。	CE パフォーマンス レポートの生成に NCS デバイスを選択しないでください。これらはオプティカル デバイスです。
...レポートの生成中に正しい期間を選択しました。	2日前にポリシーを有効にした場合は、2週間の期間を選択できません。
... デバイスを正しく設定しました。詳細については、デバイスをモデル化してモニターできるように設定する（69ページ）を参照してください。	QoS レポートの場合、デバイスで QoS を設定するか、または有効にする必要があります。
... デバイスインベントリの収集が成功しました。詳細については、インベントリ収集またはディスカバリの問題があるデバイスの検索（88 ページ）を参照してください。	レポートにデータを含めるには、インベントリ収集ステータスが [完了（Complete）] である必要があります。

第 V 部

デバイスの設定

第 13 章

デバイスの設定

この章では、次のトピックについて説明します。

Cisco Evolved Programmable Network Manager を使用してデバイスを設定する方法

Cisco EPN Manager には、ネットワークの物理デバイスを変更する方法として次の 2 つが用意されています。実行できるアクションは、ユーザーアカウント権限とネットワーク内のデバイスのタイプによって異なります。

デバイスを設定するための出発点	この方法の使用目的：
左側のナビゲーション メニューの [設定（Configuration）] メニュー	デバイス名をクリックし、[設定（Configuration）] タブをクリックします。 選択したデバイスでデバイス機能を設定できます。また、デバイスに展開された適用済みおよびスケジュール済みの機能テンプレートのリストを表示できます。
設定テンプレートの作成と展開	システムテンプレートを使用して *1* つ以上のデバイスに対して一般的なネットワーク管理タスクを実行します。たとえば、ホスト名の追加やルーティング プロトコルの設定などです。導入のニーズに合わせて独自のテンプレートを作成することもできます。これらは複数のデバイスに適用できるため、通常、テンプレートは特定のデバイス オペレーティング システムやデバイス タイプに適用されます。構成テンプレートを使用すると、Cisco EPN Manager は、テンプレート基準を満たすデバイスのみを表示します。

（注） また、デバイスを選択し、[編集（Edit）] をクリックして、[ネットワーク デバイス（Network Devices）] 表（**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]**）からデバイスのプロパティを編集することもできます。これにより、デバイスの編集ウィザードが起動されます。ただし、ウィザードを使用して行う変更は、デバイス クレデンシャルに限定されており、行った変更は物理デバイスに影響しません。データベースに保存されているデバイス情報を更新するのみです。

光デバイスの場合は、Cisco EPN Manager から起動できる Cisco Transport Controller を使用してデバイスを設定することもできます。Cisco NCS および Cisco ONS デバイスを管理するための Cisco Transport Controller の起動 （572 ページ）を参照してください

変更を行った後、データベースに変更を保存し、必要に応じてデバイスの物理および論理インベントリを収集します。詳細については、デバイスのインベントリの即時収集（同期） （570 ページ）を参照してください。

どのデバイスが設定操作をサポートしているか。

次の場合、デバイスで設定操作がサポートされています。

- Cisco EPN Manager では、デバイス モデルがサポートされています。
- Cisco EPN Manager では、デバイスのオペレーティング システムがサポートされています。
- Cisco EPN Manager では適用可能なテクノロジーまたはサービスがサポートされており、それらはデバイスで有効になっています。

何がサポートされているかについては、Cisco Evolved Programmable Network Manager のサポート対象デバイスを参照してください。

CLI 設定テンプレートで使用されているコマンドの特定

この手順を使用して、[CLI テンプレート（CLI Templates）] ドロワから起動するコマンドで使用されるコマンドそのものを表示します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features and Technologies）]**を選択し、**[CLI テンプレート（CLI Templates）]** を選択します。次に例を示します。

- 設定済みのテンプレートは、[システム テンプレート（System Template）] の [CLI] の下にあります。
- カスタマイズされたテンプレートは、[マイ テンプレート（My Templates）] の下にあります。

ステップ 2 左側のサイドバーにある [テンプレート（Templates] メニューのテンプレートをダブルクリックします。

ステップ 3 [テンプレートの詳細（Template Detail）] 領域で、[CLI コンテンツ（CLI Content）] タブを選択します。コマンドがそのタブに表示されます。

デバイスのクレデンシャルとプロトコル設定の変更

デバイスのクレデンシャルとプロトコル設定を更新するには、次の手順に従います。設定をデータベースに保存するときにインベントリの収集を実行し、毎日インベントリの収集を待機するのではなく、すべての物理デバイスと論理デバイスの変更を収集して、それらの変更をデータベースに保存することもできます。

ステップ 1 **[インベントリ（Inventory）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 編集するデバイスを選択して、[編集（Edit）]をクリックします。複数のデバイスを選択して、一括で変更することもできます。

ステップ 3 変更するパラメータをダブルクリックします。デバイス タイプに応じて、次を編集できます。

- デバイスで使用されているクレデンシャル プロファイル
- デバイスが属するグループ
- SNMP ポート、再試行、タイムアウト、クレデンシャル、および SNMPv3 認証情報
- Telnet/SSH2 のクレデンシャルとタイムアウト
- HTTP/HTTPS のクレデンシャル、ポート、タイムアウト
- TL1 のクレデンシャルとプロキシ IP アドレス（GNE/ENE の場合）
- シビック ロケーション（Civic Location）

ステップ 4 [クレデンシャルの確認（Verify Credentials）] をクリックして、新しいクレデンシャルが物理デバイス上のクレデンシャルと同じであることを確認します。

ステップ 5 次のように変更を保存します。

- [更新（Update）] は、変更をデータベースに保存します。
- [更新して同期（Update and Sync）] は、変更をデータベースに保存し、デバイスの物理インベントリと論理インベントリも収集して、すべての変更をデータベースに保存します。

基本的なデバイス プロパティの変更

Cisco EPN Manager は、物理デバイスで基本的なプロパティを変更するために使用できるコマンド テンプレートを提供します。これらのテンプレートを使用するには、**[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択し、左側の [テンプレート（Templates）] ペインから **[CLI テンプレート（CLI Templates）] > [システム テンプレート - CLI（System Templates - CLI）]** を選択します。

（注） ここで実行する操作は、[編集（Edit）] ウィザード（ネットワーク デバイス テーブルから起動できる）で実行する操作とは異なります。[編集（Edit）] ウィザードでは、データベースに保存されたデバイス情報のプロパティを変更します。この操作では、物理デバイスのプロパティは変更されません。

CLI 設定テンプレート名	次の場合に使用します。	必要な入力値
Add-Host-Name-IOS および -IOS-XR	クライアントホスト名を設定します	ホスト名
Remove-Host-Name-IOS および -IOS-XR		
Syslog-Host-Logging-IOS および -IOS-XR	特定のレベルのメッセージを記録するホストを指定します	ホスト名
Add-Tacacs-Server-IOS および -IOS-XR	認証に使用する TACACS または TACACS+ サーバーを設定します	ホスト アドレス、キー値、認証リスト名、グループ名
Remove-Tacacs-Server-IOS および -IOS-XR		
Add-Tacacs-Plus-Server-IOS および -IOS-XR		
Remove-Tacacs-Plus-Server-IOS および -IOS-XR		
Add-SNMP-Configuration-IOS および -IOS-XR	SNMP バージョン、パスワード、パスワードの暗号化、サーバーおよびグループ設定、UDP ポートなどを設定します	ホスト名、コミュニティ名、システム所有者
Remove-SNMP-Configuration-IOS および -IOS-XR		
Enable-Traps-ASR903	Cisco ASR 903 でトラップの有効/無効を切り替えます	トラップ名（リストが提供されます）
Disable-Traps-ASR903		
Enable-Traps-IOS および -IOS-XR	Cisco IOS および Cisco IOS XR のデバイスでトラップの有効/無効を切り替えます	
Disable-Traps-IOS および -IOS-XR		
Enable-Traps-ME3600 および -ME3800	Cisco ME3600 および ME3800 でトラップの有効/無効を切り替えます	
Disable-Traps-ME3600 および -ME3800		
Enable-Trap-Host-IOS および IOS-XR	SNMP トラップのターゲットホストを設定します	ホスト IP アドレス、コミュニティ ストリング
Show-Users-on-Device-IOS および -IOS-XR	Cisco IOS および Cisco IOS XR のデバイスのユーザーセッション情報を表示します	（選択したデバイスから実行されます。必要な入力はありません）

インターフェイスの有効化と無効化

インターフェイス360ビューを使用して、インターフェイスをすばやく有効または無効にします。[デバイスの詳細（Device Details）] ページからこれらと同じアクションを実行できますが、インターフェイス360ビューを使用するほうがより効率的な場合があります（アラームに応答する場合など）。インターフェイス360ビューの右上には、有効化と無効化のオプションが表示された [アクション（Actions）] メニューがあります。

インターフェイス 360 ビューを起動するには、デバイス インターフェイスの概要：[インターフェイス360（Interface 360）] ビュー （129 ページ）を参照してください。

デバイスの [デバイスの詳細（Device Details）] ページからインターフェイスを有効または無効にするには、インターフェイスの設定のトピック（イーサネット、ループバック、シリアル、トンネルなど）を参照してください。

デバイス インターフェイスの物理属性の設定

Cisco EPN Manager を使用すると、デバイスのインターフェイスの物理属性を設定できます。カードの操作モード、スロットごとの帯域幅割り当て、スロット接続可能タイプ（VCoPなど）の属性とAINS 設定は設定可能です。

インターフェイスの物理属性を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 インターフェイスを設定するには、次の表に示すパスに移動します。

ステップ 5 変更を加えるには、コントローラ/カード名のハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。変更を加えて、[保存（Save）] をクリックします。

表 *16* : インターフェイスの物理属性の設定

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
5G または 10G としてカードタイプの設定。	**[物理（Physical）] > [カード モード（Card Mode）]**	設定を 10G から 5G に変更することはできますが、5G から 10G への変更はサポートされていません。選択したデバイスによって、デフォルトのカードモードは 5G または 10G に設定されます。サポートされるカード モードの詳細については、Cisco EPN Manager でサポートされるデバイスを参照してください。 （注） アクティブ回線の一部となっているスロットでカードモードを設定することはできません。	デバイスのスロットとサポートされているカード モードのタイプの詳細については、次の表（「デバイスのスロットとサポートされるカード モードのタイプ」）を参照してください。
T1 または E1 としてのカードモードの設定。	**[物理（Physical）] > [カード モード（Card Mode）]**	選択するデバイスとカードに応じて、設定を T1 から E1 に変更することも、その逆に変更することもできます。 T1 モードと E1 モードは、カードで使用されるチャネル モードのタイプを表します。 （注） アクティブ回線の一部となっているスロットでカードモードを設定することはできません。	-
OC3 または OC12 としてのカードモードの設定。	**[物理（Physical）] > [カード モード（Card Mode）]**	（Cisco ASR 903 ルータの）A900-IMA4OS カードのカードモードを OC3 または OC12 として設定できます。 OC3 モードと OC12 モードは、異なる光伝送回線のデータ伝送速度を表します。	-

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
カード保護の設定	**[物理（Physical）] > [カード保護（Card Protection）]**	カードをプライマリ メンバーまたはバックアップ メンバー（インターフェイス）として機能するように設定します。プライマリ インターフェイスとそのバックアップ インターフェイスは、保護グループを構成します（一意の整数で示されます）。カードをバックアップ メンバーに関連付けると、プライマリ インターフェイスに障害が発生した場合、保護インターフェイスはプライマリ インターフェイスからのトラフィック負荷を迅速に想定できるようになります。アクティブ メンバーとして表示されるカードは、サービスの保護メンバーとして機能するカードです。 プライマリ メンバーとバックアップ メンバーが同じタイプであることを確認します。たとえば、プライマリ メンバーとして T1 インターフェイスを選択した場合、バックアップ メンバーも T1 インターフェイスである必要があります。 ホールドオフタイマーは、1 + 1 カードプロテクション（IOS XE バージョン 16.10.1 以降を搭載した NCS 42XX デバイス）で使用できます。これは、ネットワークの不整合が発生した場合に連続してスイッチングが行われないようにするために使用されます。有効な範囲は 0 ～ 10 秒です。デフォルト値は 5 です。 保護グループの管理モードは、[ロックアウト（Lockout）] > [強制切り替え（Force Switch）] > [手動スイッチ（Manual Switch）] > [なし（None）] の順序で設定されます。これらのモードと元に戻すタイマーの詳細については、APS または MSP および UPSR または SNCP 保護グループの設定（414 ページ）の説明を参照してください。	-
NCS42xx デバイス上に NCS4200-1T16G-PS カードを設定します。	**[物理（Physical）] > [カード モード（Card Mode）]**	スロット番号に関係なく、NCS4200-1T16G-PS カードのすべてのカード モードを表示できます。 （注） NCS42xx デバイスの一部のスロットで NCS4200-1T16G-PS カードを設定すると、それらのスロットの設定はデフォルト値にリセットされます。	-

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
ASR9xx デバイス上で A900-IMA8CT1Z-M カードと A900-IMA8CS1Z-M カードを設定します。	**[物理（Physical）] > [カード モード（Card Mode）]**	A900-IMA8CT1Z-M カードと A900-IMA8CS1Z-M カードのカード モードを表示および設定できます。	-

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
自動インサービス（AINS）のインターフェイスモジュールのタイプを設定します。	**[物理（Physical）] > [自動インサービス（AINS）（Automatic In-Service (AINS)]**	[カード（Cards）] タブを使用して、AINS に適切なコントローラタイプを設定します。カードを手動で挿入および取り出す場合、AINS 値は 20 分遅れて取り込まれます。 [ポート/コントローラ（Ports/Controllers）] タブには、AINS 対応のすべてのポートとコントローラのリストが表示されます。サポートされているポートとコントローラは、Ethernet、E1、E3、T1、T3、および SONET と SDH です。[編集（Edit）] アイコンを使用して、[セカンダリ管理状態（Secondary Admin State）] の値と [Soak タイマー（Soak Timer）] の値（時間単位または分単位）を設定できます。 **注**：ポートまたはコントローラでの AINS の有効化は、デバイス上で手動で実行する操作です。 次に、設定可能な[セカンダリ管理状態（Secondary Admin State）] の値を示します。 • [IS_AINS]：デバイスが [自動インサービス（Automatic In-Service）] 状態であることを示します。 • [IS]：デバイスが [インサービス（In-Service）] 状態であることを示します。 • [OOS_MT]：デバイスが [インメンテナンス（In-Maintenance）] 状態であることを示します。 Soak タイマーを時間単位で設定するには、[Soak タイマー（時間）（Soak Timer Hours）] フィールドを使用します。有効な範囲は 0 ～ 48 時間です。Soak タイマーを分単位で設定するには、[Soak タイマー（分）（Soak Timer Minutes）] ドロップダウンリストを使用します。使用可能な値は、15 分、30 分、および 45 分です。デフォルト値は 15 分です。	-

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
選択したデバイス スロット用に予約する必要がある帯域幅を設定します。	**[物理（Physical）] > [帯域幅（Bandwidth）]**	指定した帯域幅は、選択したスロット用に予約され、スロットが動作しているかどうかにかかわらず、スロットで使用できるようになります。選択したスロット/カードがダウンし、しばらくしてからオンラインに戻った場合は、このフィールドで指定された値に基づいて設定された帯域幅が使用できるようになります。	NCS4200-1T16G-PS カードでは、事前設定された帯域幅値 80 Gbps または 100 Gbps を NCS4216 デバイスで予約できます。
Virtual Container over Packet（VCoP）のインターフェイス プラガブル タイプを設定します。	**[物理（Physical）] > [接続可能（Pluggable）]**	このメニューを使用して、VCoP 対応インターフェイスに適切なポート タイプを選択します。たとえば、ポート タイプは OC3、OC12、DS3 のいずれかに設定できます。 （注） VCoP スマート SFP は、パケット ネットワーク全体で透過的に SONET 信号を転送する機能を提供します。VCoP スマート SFP は特殊なタイプの光トランシーバであり、STS1、STS-3c、または STS-12c レベルで SONET ビット ストリームをパケット形式にカプセル化します。	-

条件と制限事項：次に、Cisco ASR 920、Cisco NCS4202、および Cisco NCS 4206 のデバイスでサポートされてる Cisco ASR 900 シリーズ ルート スイッチ プロセッサ 2（RSP2A）モジュール（A900-RSP2A-128）でコントローラ モードを設定するための条件と制限を示します。

- 設定できる最大帯域幅は OC-48 です。モジュール上には最大 20 個のポートを設定できます。
  - ポート 0 ～ 11 は T1 ポートです。
  - ポート 12 ～ 15 は T3/E3 ポートです。
  - ポート 16 ～ 19 は OC3/OC12 ポートです。

    （注） 特定のポートが OC48 として設定されている場合、設定可能な最大帯域幅が OC48 であるため、設定できるのはそれらの特定のポートの 1 つのみです。

- Cisco A900-RSP2A-128 モジュールの設定制限：
  - SDH/E3/E1/DS0 コントローラ モードは設定できません。
  - イーサネットはコントローラ モードとして設定できません。
  - 保護タイプ UPSR は設定できません。
  - コントローラ モード設定をデバイスに展開すると、Cisco EPN Manager を使用して設定を元に戻すことはできません。

表 *17 :* デバイスのスロットとサポートされるカード モードのタイプ

Cisco NCS 4206 デバイス	Cisco NCS 4216 デバイス	Cisco ASR903 デバイス	Cisco ASR907 デバイス
• スロット 0、1：非サポート • スロット 2、3、4、5：デフォルト モード 10G	• スロット 0、1：非サポート • スロット 3、4、7、8、11、12：デフォルト モード 10G • スロット 2、5、6、9、10、13、14、15：デフォルト モード 5G	• スロット 0、1：非サポート • スロット 2、3、4、5：デフォルト モード 10G	• スロット 0、1：非サポート • スロット 3、4、7、8、11、12：デフォルト モード 10G • スロット 2、5、6、9、10、13、14、15：デフォルト モード 5G

表 *18 :* コントローラ モードおよびサポートされるポート タイプ

SONET（0 ～ 3）	SONET（4 ～ 7）
• 最大 2.5G • OC48/OC12/OC3 をサポートできますが、合計 2.5G に制限されます。 • たとえば、ポート 0 に OC48 が設定されている場合、ポート 1/2/3 は使用できません。	• 最大 2.5G • ポート グループに OC12/OC3/1G が設定されている場合、OC48 は許可されません。

回線エミュレーションの設定

Cisco EPN Manager は、従来の TDM ネットワークとパケット スイッチド ネットワーク（PSN）間にブリッジを提供する回線エミュレーション（CEM）のプロビジョニングをサポートします。CEM は、パケット スイッチド ネットワーク上で TDM（または PDH）回線を伝送する方法です。回線エミュレーション（CEM）は物理接続の模倣です。この機能によって、既存の IP ネットワークを使用して専用回線エミュレーション サービスを提供できるようになります。また、他のマルチサービス プラットフォーム インターフェイスの形式の要件を満たさないデータ ストリームやプロトコルを伝送できるようになります。

Cisco EPN Manager は次の CEM モードをサポートしています。

- Structure-Agnostic time-division multiplexing（TDM）over Packet（SAToP）：これは、着信 TDM データが任意のビット ストリームと見なされる非構造化モードです。ビット ストリームに適用される可能性がある構造は無視されます。SAToP では、TDM ビット ストリームが PSN 経由の疑似回線（PW）としてカプセル化されます。

- Circuit Emulation over Packet（CEP）：このモードは、MPLS プロバイダを介して同期光ネットワーク/同期デジタル階層（SONET/SDH）回線とサービスをエミュレートするために使用されます。パケット指向ネットワークで SONET/SDH 回線を伝送するために、同期ペイロード エンベロープ（SPE）またはバーチャル トリビュタリ（VT）はフラグメントに分割されます。CEP ヘッダーと必要に応じて RTP ヘッダーが各フラグメントの前に付加されます。

Cisco EPN Manager での CEP の詳細については、サポートされる回線エミュレーション サービス （621 ページ）を参照してください。

回線がチャネル化される場合、回線は論理的に、高順位のパス（HOP）と低順位のパス（LOP）と呼ばれる小さい帯域幅チャネルに分割されます。これらのパスが SONET ペイロードを伝送します。回線がチャネル化されない場合、回線の全帯域幅がブロードバンドサービスを伝送する単一のチャネル専用となります。Cisco EPN Manager では、T3 または E3 チャネルを T1 にチャネル化し、T1 をさらに DS0 タイム スロットにチャネル化できます。Cisco EPN Manager を使用して CEM サービスをプロビジョニングする前に、まず、CEM インターフェイスを設定して、HOP および LOP のパラメータを設定する必要があります。

チャネライズド SONET インターフェイスは、複数の STS ストリームを複合したものであり、固有のペイロードポインタを持つ独立したフレームとして維持されます。フレームは、転送される前に多重化されます。SONET では同期転送信号（STS）フレーミングが使用され、SDH では同期トランスポート モード（STM）フレーミングが使用されます。STS はオプティカル キャリア 1（OC-1）の電気的等価であり、STM-1 は 3 オプティカル キャリア 1（OC-1）の電気的等価です。

ここでは、Cisco EPN Manager を使用して最初に CEM のインターフェイスを設定する方法について説明します。次に、適切なコントローラ モードと保護グループが設定されたこれらのインターフェイスを使用して、CEM サービスをプロビジョニングすることができます。

CEM サービスを設定するための前提条件

CEM サービスのプロビジョニング（回線エミュレーション サービスのプロビジョニング （727 ページ）を参照）の前に、次の前提条件が満たされていることを確認します。

- デバイスの CEM に必要なループバックを設定します。ループバック インターフェイスの設定 （445 ページ）を参照してください。
- SONET、SDH、PDH、HOP、および HOP コントローラに必要な CEM パラメータを設定します。CEM のインターフェイスの設定 （409 ページ）を参照してください。
- APS 保護を提供するように、現用インターフェイス グループとバックアップ用インターフェイス グループを構成します。APS または MSP および UPSR または SNCP 保護グループの設定 （414 ページ）を参照してください。.

SONET モードの設定例

次に、STS-1 モードを設定する設定コマンドと例を示します。

STS-1 モードの設定

STS-1 モードを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode vt-15
end
```

（注） デフォルトのモードはありません。modes vt-15、mode ct3、mode t3、mode unframed、mode vt-2 がサポートされています。システムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

STS-1 の DS1/T1 CT3 モードの設定：

STS-1 の DS1/T1 CT3 モードを設定するには、次の手順を使用して T1 リンクを設定します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode ct3
t1 1 clock source internal
t1 1 framing unframed
end
```

（注） システムをデフォルトの状態に戻すには、このコマンドの no 形式を使用します。

STS-Nc の設定：連続連結

STS-Nc の連続連結を設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1-3 mode sts-3c
end
```

（注） システムをデフォルトの状態に戻すには、このコマンドの**no**形式を使用します。また、STS-3c または STS-12c を設定するには、それぞれ 3 または 12 の倍数の数値を使用します。

CESoPSNでの SONET モード VT1.5-T1 のCEMグループの設定

CESoPSN の STS-1 の VT 1.5 モードで CEM グループを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 2
mode vt-15
vtg 1 t1 1 cem-group 56 timeslots 1 - 8
end
```

CESoPSN における SONET モード CT3-T1 の CEM グループの設定

CESoPSN の STS-1 の CT3 モードで CEM グループを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode ct3
t1 3 cem-group 28 timeslots 1 - 7
end
```

CEM のインターフェイスの設定

Cisco EPN Manager を使用して、回線エミュレーション（CEM）にインターフェイスを設定できます。これを行うには、適切なコントローラ モードをインターフェイスに設定してから、CEM の PDH（E1、T1、E3、T3）、SONET、および SDH コントローラを設定します。CEM で設定したインターフェイスは、CEM サービスをプロビジョニングする際に使用できます。回線エミュレーション サービスのプロビジョニング （727 ページ）を参照してください。

CEM のインターフェイスを設定するには、次の手順に従います。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 CEM のパラメータを設定するには、次の表で説明する設定オプションに移動します。

ステップ 5 変更を加えるには、コントローラ/カード名のハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。変更を加えて、[保存（Save）] をクリックします。

例

表 *19 : CEM* インターフェイスの設定オプション

CEM インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
SONET、SDH、イーサネット、T3、あるいはE1、E3、またはSTS1Eとしてコントローラモードを設定します。	**[回線エミュレーション（Circuit Emulation）] > [コントローラモード（Controller Mode）]**	選択のために表示されるコントローラモードオプションは、選択したメディアタイプに基づいています。詳細については、「コントローラモードおよびサポートされるポートタイプ」を参照してください。	–
PDH（E1、T1、E3 および T3）コントローラを設定します。	**[回線エミュレーション（Circuit Emulation）] > [PDH]**	各種の PDH パラメータについては、次を参照してください。CEM インターフェイス（PDH、SONET、および SDH）のフィールドの説明（419 ページ）	-

CEMインターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
CEM の SONET および SDH コントローラを設定します。	**[回線エミュレーション（Circuit Emulation）] > [SONET および SDH（SONET and SDH）]**	各種の SONET および SDH パラメータについては、次を参照してください。CEM インターフェイス（PDH、SONET、および SDH）のフィールドの説明（419 ページ）	デバイスのポートとサポートされているコントローラのタイプの詳細については、次の表（「コントローラモードおよびサポートされるポートタイプ」）を参照してください。
CEM プロビジョニングの現用メンバーインターフェイスと保護メンバーインターフェイスを設定します。	**[回線エミュレーション（Circuit Emulation）] > [保護グループ（Protection Group）]**	APS または MSP および UPSR または SNCP 保護グループの設定（414 ページ）を参照してください	-

コントローラ モードおよびサポートされるポート タイプ

- EOWYN IM にはペア ワイズ制限があります。有効なペアは（0,1）（2,3）（4,5）（6,7）です。

（注） ペアごとに 最大 2.5 Gbps（OC48）の帯域幅（両方のポートを組み合わせて）を設定できます。

- レート OC3/OC12/OC48 はポート 0 ～ 7 についてのみ設定でき、ポート 8 では OC192 レートのみを設定できます。

表 *20 :* 異なるレート *OCN -> n * 51.84 Mbit/s* で使用される帯域幅

レート設定	帯域幅
OC1	51.84 Mb/s
OC3	155.52 Mb/s
OC12	622.08 Mb/s
OC48	2488.32 Mb/s ～ = 2.5 Gb/s
OC192	9953.28 Mb/s ～ = 10 Gb/s

MediaType コントローラの設定

MediaType コントローラを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
end
```

SONET ポートの設定

SONET ポートを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
rate OC12
end
```

上記の例には、OC-12 モードで SONET ポートを設定する方法が示されています。

STS1E ポートの設定

STS1E ポートを設定するには、次のコマンドを使用します。

```
NCS4200-120.33#sh run | sec 0/4/0
controller MediaType 0/4/0
 mode sts1e
controller STS1E 0/4/0
 no snmp trap link-status
 no ais-shut
 alarm-report all
 secondary-admin-state auto-in-service
 clock source internal
 cablelength short
 overhead j0 tx length 64-byte
 overhead j0 expected length 64-byte
 !
 sts-1 1
```

CEM インターフェイスの設定例：

- 次の例は、CEM フレーミングのタイプが「unframed」、モードが「c-11」、クロックソースのタイプが「internet」、保護グループに関連付けられた ACR 値が「acr

255」に設定されたデバイスに挿入する CEM インターフェイス設定を示しています。

```
NCS4206-120.32#show running-config | section 0/4/0
controller MediaType 0/4/0
 mode sonet
controller SONET 0/4/0
 rate OC3
 no ais-shut
 framing sonet
 clock source line
 loopback network
 !
 sts-1 1
  clock source internal
  mode unframed
  cem-group 1 cep
 !
 sts-1 2
  clock source internal
  loopback network
  mode unframed
  cem-group 2 cep
 !
 sts-1 3
  clock source internal
  mode vt-15
  vtg 1 vt 1 protection-group 15 working
  vtg 1 vt 3 protection-group 16 working
  vtg 1 vt 4 protection-group 17 working
 !
 aps group acr 255
 aps protect 1 6.6.6.6 / aps working 1
!
interface CEM0/4/0
 no ip address
 cem 1
 !
 cem 2
 !
connect sam CEM0/4/0 1 CEM0/4/0 2
 !
NCS4206-120.32#
```

- 次に、STS1E を使用した CEM インターフェイスの設定例を示します。

```
controller STS1E 0/4/1
  sts-1 1
    mode vt-15
    vtg 1 t1 1 cem-group 0 cep
interface CEM0/4/1
 no ip address
 cem 0
 !



controller STS1E 0/4/0
 sts-1 1
  clock source internal
  mode unframed
  cem-group 0 cep
```

```
interface CEM0/4/0
 no ip address
 cem 0
 !
```

APS または MSP および UPSR または SNCP 保護グループの設定

CEM の保護グループを表示すると、デバイスに対して有効な自動保護スイッチング（APS）、単方向パス スイッチング リング（UPSR）、多重サービス保護（MSP）、サブネットワーク接続保護（SNCP）インターフェイスを理解するのに役立ちます。APS と UPSR は、SONET ネットワーク内の保護インターフェイスを動作中インターフェイスのバックアップとして使用するメカニズムです。インターフェイスを APS または UPSR の保護グループに関連付けると、動作中インターフェイスで障害が発生した場合に、保護インターフェイスにそのトラフィック負荷が迅速に引き継がれます。現用インターフェイスとその保護インターフェイスが保護グループを構成します。SONET 保護グループは、SONET 回線層でファイバ（外部）障害または機器（インターフェイスおよび内部）障害からの回復機能を提供します。Cisco EPN Manager を使用すると、CEM 回線のメイン動作コントローラとして機能する SONET コントローラの現用メンバーを表示できます。保護メンバーは、メインの現用コントローラのバックアップとして機能します。これらの詳細を表示するには、CEM のインターフェイスの設定（409 ページ）の説明に従ってインターフェイスが必要なコントローラ モードに設定されていることを確認してください。

MSP と SNCP とは、SDH ネットワーク内の保護インターフェイスを動作中インターフェイスのバックアップとして使用するメカニズムです。インターフェイスを MSP または SNCP の保護グループに関連付けると、動作中インターフェイスで障害が発生した場合に、そのトラフィック負荷が保護インターフェイスに迅速に引き継がれます。動作中インターフェイスとそれらの保護インターフェイスとで保護グループを構成します。

MSP は、1+1 保護メカニズムを提供するポート レベル保護のための SDH の保護メカニズムです。ネットワーク トポロジ マップでは、復帰モード、単方向モード、双方向モード、および acr/dcr モードなど、すべてのモードがサポートされています。SDH の MSP は SONET の APS に似ています。たとえば、NCS 4206 デバイスには動作モードと保護モードの両方があります。

SDH-MSP 機能は、インターフェイス モジュール（IM）全体の SDH コントローラのポート レベルの冗長性を提供します。異なる IM のポートは、動作モードの 1 つのポートと保護モードの他のポートを設定できます。

SNCP は SDH ネットワークの保護メカニズムで、回線障害が発生したときに SDH 接続を別の SDH 回線に切り替えることができます。保護インターフェイスは、現用インターフェイスのバックアップインターフェイスとして機能します。動作中インターフェイスに障害が発生すると、保護インターフェイスはそのトラフィック負荷を迅速に引き継ぎます。保護パスへの切り替えは、非リバーティブモードで行われます。トランスミッション障害が原因で保護が保護パスに切り替えられた場合、障害が修正されると、元のパスへの自動スイッチバックは行われません。SONET での SNCP と同等な機能は UPSR と呼ばれています。プロビジョニング ウィザードまたは CLI を使用して、CEM サービスと SNCP をプロビジョニングできます。サポートされているモードは、VC4_16C、VC4_4C、VC4、AU4_VC12、AU4-VC11、AU3-VC12、AU3-VC11 です。

（注） ミックスモードのサポートは利用できません。

次に制限事項の一部を示します。

- SNCP を使用して SDH でサポートされているモードは STM64 ポートではサポートされていません。
- ループバックおよびビット エラー レート テスト（BERT）は、物理メンバー コントローラでのみ設定できます。
- サポートされている拡張性は 336 回路に制限されています

保護グループを変更する前に、コントローラ/インターフェイスを保護に必ず追加してください。

APS/MSP 保護グループを設定し、UPSR/SNCP インターフェイスを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 保護グループで設定されたデバイスを選択するため、そのデバイス名のハイパーリンクをクリックします。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **[回線エミュレーション（Circuit Emulation）] > [保護グループ（Protection Group）]** を選択します。

ステップ 5 APS/MSP パラメータを設定するには、[APS/MSP] タブをクリックし、変更するグループの [保護グループ（Protection ）] ハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。

ステップ 6 表示および設定できるフィールドは次のとおりです。

- [動作中メンバー（Working Member）] には、回線のメインの動作コントローラとして機能する SONET/SDH コントローラが表示されます。
- [保護メンバー（Protecting Member）] には、回線の動作中メンバーへのバックアップとして機能する SONET/SDH コントローラが表示されます。
- [保護ステータス（Protection Status）] には、グループが回線のアクティブメンバーか非アクティブ メンバーかが示されます。
- [Hello 時間（Hello Time）] フィールドと [保留時間（Hold Time）] フィールドは、保護メンバーと現用メンバーの時間範囲を表示します。hello タイマーは、hello パケット間の時間を定義します。保留タイマーは、保護インターフェイス プロセスが現用インターフェイスのルータのダウンを宣言するまでの時間を設定します。デフォルトでは、保留時間は hello 時間の 3 倍以上となります。
- [ループバック IP（Loopback IP）] は、現用インターフェイスを持つルータの IP アドレス（通常はループバック アドレス）を含む保護インターフェイスの設定を決定します。

- [復帰時間（Revertive Time）]（分単位）は、動作中インターフェイスが利用可能になった後に、設定されている時間に基づいて保護インターフェイスから動作中インターフェイスへの自動スイッチオーバーを有効にできます。リバーティブ時間がゼロの場合、保護は非リバーティブになります。
- [方向（Directional）] ドロップダウン メニューには、バックアップ保護を有効にする必要がある方向が表示されます。
  - 双方向モードでは、動作中メンバーの障害によって動作中メンバーから保護メンバーへの APS/MSP スイッチオーバーがトリガーされます。この場合、受信チャネルと送信チャネルはペアとして切り替わります。
  - 単方向モードでは、動作中メンバーの障害によって障害が発生したメンバーから保護インターフェイスの対応する回線のみへの APS/MSP スイッチオーバーがトリガーされます。
- [ADM] チェックボックスが有効になっている場合は、アド/ドロップマルチプレクサ（ADM）と保護メンバーが関連付けられます。
- [APS 要求（APS Request）] ドロップダウン メニューを使用すると次の値を設定できます。値は [ロックアウト（Lockout）] > [強制切り替え（Force Switch）] > [手動切り替え（Manual Switch）] > [モードなし（No Mode）] の順序に設定できます。たとえば、[強制切り替え（Force Switch）] がデバイスに現在設定されている場合は、[手動スイッチ（Manual Switch）] または [モードなし（No Mode）] の値のみを設定できます。[強制切り替え（Force Switch）] の設定時にロックアウトは設定できません。
  - [ロックアウト（Lockout）]：動作中インターフェイスが保護インターフェイスに切り替わるのを防ぎます。たとえば、保護インターフェイスが回線 1 として設定されている場合、ロックアウトオプションを使用すると、保護インターフェイスがアクティブになるのを防ぎます。
  - [手動切り替え（Manual Switch）]：同等かより高いプライオリティを持つ要求が実行されている場合を除いて、回線を保護インターフェイスに手動で切り替えます。
  - [強制切り替え（Force Switch）]：同等かより高いプライオリティを持つ要求が実行されている場合を除いて、回線を保護インターフェイスに手動で切り替えます。たとえば、保護インターフェイスが特定の回線として設定されている場合、force コマンドは保護インターフェイスをアクティブに設定します。
  - [モードなし（No Mode）]：デバイスの保護グループから現在の APS/MSP 要求設定を削除します。

（注） SONET または SDH の保護グループをクリアするには、SONET または SDH いずれかの保護グループ ID を選択し、[削除（Delete）]（X）アイコンをクリックします。

ステップ 7 UPSR/SNCP インターフェイスに関連付けられている類似パラメータを表示するには、[UPSR/SNCP] タブをクリックします。

保護グループ番号、デバイスで構成されている現用メンバーと保護メンバー、グループのアクティブ パス、現在の保護ステータスなどの情報を表示できます。この情報は変更できません。

（注） 設定された SDH を超える UPSR/SNCP を持つ IM のシャットダウンまたは削除中に、UI の変更を検証し、各インターフェイス モジュールの活性挿抜（OIR）を確認できます。**show protection-group** コマンドを使用します。

- 次のステータスの変更を表示するには、次の手順を実行します。
  - [手動（Manual）]：SNCP 保護グループを手動で設定すると、ステータスが表示されます。
  - [クリア（Clear）]：以前に設定された外部コマンドをクリアします。
  - [自動（Auto）]：SNCP 保護グループを最初に設定したときにステータスが表示されます。
  - [強制（Force）]：手動で切り替えるときにステータスが表示されます。
  - [Fail（失敗）]：保護された現用パスがダウンしているときにステータスが表示されます。
  - [信号障害（Signal Failure）]：リンク障害が発生しているときにステータスが SF に送信されます。
  - [信号の劣化（Signal Degrade）]：現用パスがダウンしているときにステータスが表示されます。
  - [ロックアウト（Lockout）]：動作中インターフェイスが保護インターフェイスに切り替わるのを防ぎます。

ステップ 8 **[回線エミュレーション（Circuit Emulation）]** > **[SONET および SDH（SONET and SDH）]** を選択します。

ステップ 9 ACR コントローラ、上位パス、下位パスのパラメータを表示または設定するには、関連するタブをクリックします。変更する SONET または SDH ハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。SDH の設定の詳細については、EPNM での SDH のモード設定 （427 ページ）、SDH パラメータの設定 （425 ページ）、および SDH 回線およびセクション パラメータの設定 （428 ページ） SAToP の SDH VC 設定パラメータ （430 ページ） SDH T1/E1 設定パラメータ （429 ページ） SDH T3/E3 設定パラメータ （429 ページ）を参照してください。

[ACR コントローラ] タブを使用して、SONET/SDH 保護グループの仮想 SONET アクセス回線冗長性（ACR）/SDH アクセス回線冗長性（ACR）の詳細を表示します。

CEM のクロッキングの設定

クロッキング モードは、CEM 回線の送信側と受信側で同じクロックを達成するための複数の方法を定義します。Cisco EPN Manager でのクロックの回復と配信には、次の方法があります。

- 同期クロッキング：同期クロッキングによって、送信元と宛先の PDH（TDM）回線が同じクロックに合わせて同期化されます。このクロックは、何らかの物理的クロック配信手段で配信されたものです（SONET、SDH など）。特定の TDM 回線のクロックは、次のものから渡すことができます。

- 回線：送信クロックは、同じ物理回線の受信者からのものです。
- 内部：コントローラは、内部クロックを使用して送信データをクロッキングします。
- フリー ランニング：送信クロックはライン カードから取得され、内部のフリー ランニング オシレータから導出できます。
- 回復：送信クロックは、CEM インターフェイスでインバンド擬似回線ベースのアクティブクロック回復から導出されます。

Cisco EPN Manager でこれらのクロッキング値を設定するには、「CEM インターフェイスの設定」を参照してください。

- 適応クロッキング：適応クロッキングは、ルータに共通クロック ソースがない場合に使用されます。クロックは、デジッタ バッファ占有レベルに基づくパケット到達率に基づいて、導出されます。Cisco EPN Manager では、CEM サービスのプロビジョニングの際に、デジッタ バッファのサイズ（1 ～ 32）を設定できます。デジッタ バッファのサイズにより、回線がどれほどネットワーク ジッターを許容できる決定します。
- 差分クロッキング：差分クロッキングが使用されるのは、セルサイトと集約ルータに共通のクロック ソースがあるが、TDM 回線のクロッキングに別のソースが使用されている場合です。TDM のクロックは、共通のクロックを基準とする、パケットの RTP ヘッダーの差分情報から導出されます。差分クロック回復の基になるのは、RTP ヘッダーで受信したタイムスタンプです。

CEM のクロック復元を設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] タブをクリックし、左側の [論理ビュー（Logical View）] タブをクリックします。

ステップ 2 **[クロック（Clock）] > [復元クロック（Recovered Clock）]** を選択します。

ステップ 3 クロック ソースの導出元の新しいインターフェイスを追加するには、追加アイコン（[+]）をクリックします。

ステップ 4 既存の復元クロック設定を編集するには、[復元インターフェイス（Recovering Interface）] ハイパーリンクをクリックし、ページ右上にある [編集（Edit）] アイコンをクリックします。

ステップ 5 次の復元クロック値を指定します。

1. 復元されたクロック設定を容易に識別できるように、[復元されたクロック ID（Recovered Clock ID）] に固有の数値を入力します。この ID を使用して、CEM インターフェイスをこの復元クロック設定に直接関連付けることができます。
2. [復元モード（Recover Mode）] ドロップダウンリストから、次のいずれかを選択します。
   - [適応（Adaptive）] : デバイス間に共通のクロック ソースがない場合、関連付けられている保護グループの保護メンバーとして選択されたコントローラでのパケット到着率から、復元クロックが導出されます。
   - [差分（Differential）] : エッジデバイス間に共通のクロック ソースがある場合、パケットのタイミング情報と、共通クロックの関連する差分から、復元クロックが導出されます。

3. **CEM グループ番号**を容易に識別できるように、固有の数値を入力します。これにより、クロックに関連付けられている CEM が識別されます。
4. [復元インターフェイス（Recovering Interface）] ドロップダウンリストから、必要なコントローラを選択します。クロックに関連付けられているこのコントローラは仮想 CEM インターフェイスであり、バックアップ クロック ソースが必要な場合にはこのインターフェイスからクロックが導出されます。

ステップ 6 **[保存（Save）]** をクリックします。

変更が保存され、デバイスに展開されます。

CEM インターフェイス（PDH、SONET、および SDH）のフィールドの説明

次の表に示された CEM パラメータを設定するには、次の手順を実行します。

ステップ 1 SONET、PDH、HOP、およびHOPコントローラで必須のCEMパラメータを設定します。CEMのインターフェイスの設定 （409 ページ）を参照してください。

ステップ 2 CEM のクロックのディストリビューションとリカバリを設定します。CEM のクロッキングの設定 （417 ページ）を参照してください。

表 *21 : CEM* インターフェイス（*SONET*、*SDH*、および *PDH*）フィールドの説明

フィールド	説明	値	説明	適切なコントローラモード
利率	データが転送されるレートを識別します。SFP（Small Form-factor Pluggable）によって異なります。	LR_DSR_OC1_STM0	STM レベル 0 のチャネライズド OC-1 回線でサポートされるレイヤレートを示します。OC-1 は、転送データ レートが最大 51.84 Mbit/s の光キャリアネットワーク回線です。	STS1E
		LR_DSR_OC3_STM1	STM レベル 1 のチャネライズド OC-3 回線でサポートされるレイヤ レートを示します。OC-3 は、転送データ レートが最大 155.52 Mbit/s のオプティカル キャリア ネットワーク回線です。	SONET/SDH
		LR_DSR_OC12_STM4	STM レベル 4 のチャネライズド OC-12 回線でサポートされるレイヤ レートを示します。 OC-12 は、転送データ レートが最大 622.08 Mbit/s のオプティカル キャリア ネットワーク回線です。	SONET/SDH
		LR_DSR_OC48_STM16	STM レベル 16 のチャネライズド OC-48 回線でサポートされるレイヤ レートを示します。OC-48 は、転送データ レートが最大 2.4Gbps のオプティカル キャリア ネットワーク回線です。	SONET/SDH
		LR_DSR_OC192_STM64	STM レベル 64 のチャネライズド OC-192 回線でサポートされるレイヤ レートを示します。 STM レベル 64 のチャネライズド OC-192 回線。OC-192 は、転送データ レートが最大 9.6Gbps のオプティカル キャリア ネットワーク回線です。	SONET/SDH

フィールド	説明	値	説明	適切なコントローラモード
[モード（Mode）]	高次および低次パスのチャネル化のタイプ（レベル n の同期転送信号（STS-n）など）を示します。	高次パス値： STS3C、STS12C、STS48C、STS192C、T3、UNFRAMED、VT15、VT2、および CT3。 下位パス値： VT15、T1、および E1。 （注） STS1E でサポートされているモード： 上位パス値：T3 と UNFRAMED 下位パス値：CT3 と VT15	• STS-n：レベル n の同期転送信号（STS）のチャネル化を伴うモード。 • T1、E1、T3、および E3：コントローラで使用されるチャネル化モードを示します。T1 または E1 回路の伝送データ レートは最大 1.544 Mbps です。T3 または E3 回路の伝送データ レートは最大 44.736 Mbit/s です。 • VT 1.5：コントローラが最大 1.728 Mbit/s の転送データ レートのバーチャル トリビュタリ ネットワーク回線であることを示します。 • VT 2：コントローラが最大 2.304 Mbit/s の転送データ レートのバーチャル トリビュタリ ネットワーク回線であることを示します。 • Unframed：1 つの CEM チャネルがすべての T1/E1 タイムスロットに使用されることを示します。	HOP と LOP
		VC4_16C、VC4_4C、VC4、AU4_VC12、AU4-VC11、AU3-VC12、AU3-VC11、T3、E3、VC1X、TUG3	サポートされている SDH モード	HOP と LOP

フィールド	説明	値	説明	適切なコントローラモード
クロック送信元（Clock Source）	SONET ポートまたは SDH ポートで送信されたクロック信号の送信元を特定します。	回線（Line）	コントローラは、回線の受信データストリームから回復されたクロックを使用して送信データのログを記録します。	すべて（All）
		内線	送信クロックはラインカードから取得され、内部の物理回線から派生させることができます。	すべて（All）
		回復	送信クロックを駆動するために使用される CEM インターフェイス上のインバウンド疑似回線ベースのアクティブクロック回復。	SONET、SDH、HOP、および LOP。
フレーミング（Framing）	CEM チャネルに使用するフレーミングモード。	CRC と NO_CRC。	CRC：巡回冗長検査でフレーミングタイプを表します。	SONET/SDH
		Unframed、DSX1_ESF、DSX1_SF、Auto Detect、C_BIT、および M13。	• Unframed：1 つの CEM チャネルがすべてのタイムスロットに使用されることを示します。 • DSX1_SF：インターフェイスの DS1 タイプがスーパーフレームとしてフレーミングタイプを持つことを示します。SF は、インバウンドシグナリング抽出に 1 つのスーパーフレームあたり 12 のフレームを使用します。 • DSX1_ESF：DS1 タイプのインターフェイスが拡張スーパーフレームとしてフレーミングタイプを持つことを示します。ESF は 1 つの ESF あたり 24 のフレームを使用します。	PDH、HOP、LOP、および STS1E。

フィールド	説明	値	説明	適切なコントローラモード
ループバック	CEM インターフェイスに関連付けられたループバック値を指定します。	ローカル、ネットワーク回線、リモート、リモート回線、ネットワーク ペイロード、および不明。	様々なループバック値に関する詳細な説明については、最新の IOS コマンド リファレンスを参照してください。	すべて（All）
		Diag、ローカル ペイロード、リモート ESF ペイロード、リモート ESF 回線、リモート ESF 回線 CSU、リモート ESF 回線 NIU、リモート Iboc、リモート Iboc CSU、リモート Iboc FAC1、リモート Iboc、および FAC2。	—	PDH
保護権限	復元クロックを取得する優先順位を指定します。	現用（WORKING!!）	復元クロックは、優先順位の最も高いクロックから取得されます。	SONET/SDH
		保護（PROTECT）	復元クロックはプライマリ クロックより優先順位の低いクロックから取得されます。	SONET/SDH
ケーブル長（Cable Length）	ケーブルの長さに応じて伝送減衰を設定します。たとえば、短い 115 を選択した場合、ケーブル長は 0 ～ 115 フィートです。ケーブル長さが 110 ～ 220 フィートなどの場合は、[ショート 220（Short 220）] を選択します。値は [ショート 110（Short 110）] から [ショート 550（Short 550）]、[ショート LT 225（Short LT 225）]、[ロング GT 225（Long GT 225）] の間になります。			PDH
回線コーディング（Line Coding）	コントローラの回線エンコーディング方式は次のとおりです。 • E1 の場合、オプションは交互マーク反転（AMI）です。 • T1 の場合、選択可能なオプションは AMI と Bipolar with 8 Zero Substitution（B8ZS）です。			PDH
チャネル化モード（Channelization Mode）	コントローラで使用する必要があるチャネル化モードを示します。T1 または E1 の回線の伝送データ レートは最大 1.544 Mbps です。値は [T1]、[E1]、および [非チャネル化（Unchannelized）] です。 （注） T3 コントローラの場合はチャネル化された T1/E1 プロパティを表示または変更し、E3 コントローラの場合はチャネル化された T1/E1 プロパティを表示または変更します。			PDH

フィールド	説明	値	説明	適切なコントローラモード
保護グループ番号（Protection Group Number）	保護番号または ACR グループを識別します。			SONET/SDH
保護ループバック名（Protection Loopback Name）	デバイス上のループバック インターフェイスの名前を識別します。			SONET/SDH
保護ループバック IP（Protection Loopback IP）	デバイス上のループバック インターフェイスの IP アドレスを識別します。			SONET/SDH
保護復帰時間（Protection Revertive Time） 保護非復帰時間（Protection Non-Revertive Time）	現用回線で障害が発生した場合、ソフトウェアは保護回線に切り替え、現用回線が回復した場合は復帰タイマーに基づいて待機し、現用回線をアクティブ リンクに戻します。 信号に障害が発生した場合、ソフトウェアは保護回線に切り替えますが、現用回線への自動復帰は行いません。これがデフォルトのオプションです。			SONET/SDH
動作ステータス	CEM インターフェイスの動作ステータス。このフィールドは編集できません。	Up、Down、および Not-Applicable。	• Down：インターフェイスがダウンしています。 • Not-Applicable：インターフェイスの動作ステータスが不明です。 • Up：インターフェイスが機能しています。	SONET、SDH、HOP、LOP、および STS1E。

フィールド	説明	値	説明	適切なコントローラ モード
管理ステータス	CEM インターフェイスの管理ステータス。	Up、Down、および Not-Applicable。	• Up：CEM インターフェイスは機能しています。 • Down：CEM インターフェイスはダウンしています。 • Not-Applicable：管理ステータスは不明です。	SONET、SDH、HOP、LOP、および STS1E。
復元クロック ID	CEM インターフェイスに関連付けられたクロック設定の一意の識別子。復元クロック ID を設定するには、CEM のクロック設定を参照してください。			PDH、ホップ、および LOP。
AUG タイプ（AUG Type）	管理ユニット グループ（AUG）は、STM レベルにおいて定義された位置を占めている 1 台以上の管理ユニットから構成されます。AUG-3 グループ化と AUG-4 グループ化はサポートされている AUG タイプです。			SDH

SDH パラメータの設定

SDH CEM チャネル化モードを設定するには、次の表を参照してください。

表 *22:* コントローラ モードおよびサポートされるポート タイプ

SDH モード	CEM	ポート	適切なコントローラ モード
VC4_16c	CEP	STM16	HOP
VC4_4c	CEP	STM4、STM16	HOP
VC4	CEP	OC3/STM1、OC12/STM4、OC48/STM16	HOP
VC1X	CEP	OC3/STM1、OC12/STM4、OC48/STM16	HOP
TUG3-E3	SATop	OC3/STM1、OC12/STM4、OC48/STM16	HOP

SDH モード	CEM	ポート	適切なコントローラ モード
TUG-3-T3	SATop	OC3/STM1、OC12/STM4、OC48/STM16	HOP
VC11_T1	SATop	OC3/STM1、OC12/STM4、OC48/STM16	LOP
VC12_E1	SATop	STM1、STM4、STM16	LOP
VC11	CEP	OC3/STM1、OC12/STM4、OC48/STM16	LOP
VC12	CEP	OC3/STM1、OC12/STM4、OC48/STM16	LOP

メディアタイプ コントローラの設定

各 SFP ポート（16 ～ 19）は、STM1、STM4、STM16 として設定できます。設定するメディアタイプ コントローラを選択し、コントローラ設定モードを開始する必要があります。コントローラを SDH ポートとして設定する必要があります。

```
To configure MediaType Controller:
enable
configure terminal controller
MediaType 0/0/16
mode sdh
end
```

SDH ポートでのレートの設定

```
To configure rate on SDH ports:
 enable
configure terminal
controller MediaType 0/0/16
mode sdh
end
```

（注） コマンドの no 形式の設定はサポートされていません。デフォルトの状態に戻すには、そのポートの下にあるすべての設定を削除した後、メディアタイプ コントローラの下で no mode sdh コマンドを使用します。

EPNM での SDH のモード設定

同期転送モジュール（STM）信号は、SONET の STS の同期デジタル階層（SDH）版に相当します。このドキュメントでは、STM という用語はパス幅と光回線レートの両方を表します。STM 信号内のパスは、管理ユニット（AU）と呼ばれます。AU は、より上位のパス層と多重化セクション層間の適合を可能にする情報構造です。AU は、情報ペイロード（より上位の VC）と AU ポインタで構成されます。AU ポインタは、ペイロードフレームの開始のオフセットを多重化セクション フレームの開始と相対的に示します。AU-3 ポインタは 3 バイトで構成され、AU-4 ポインタは 9 バイトで構成されます。STM-1 フレームのペイロードは、1つの AU-4 ユニットまたは3つの AU-3 ユニットで構成されています。管理ユニット グループ（AUG）の拡張マッピングは、STM ペイロードにおいて固定の定義された位置を占める 1 つまたは複数の管理ユニットで構成されます。拡張マッピングは STM1 レベルでサポートされています。

次のタイプの拡張マッピングがサポートされています。

- 拡張マッピング AU-4

（注） これはデフォルトの拡張マッピングモードです

- 拡張マッピング AU-3

SDH では次のモードがサポートされています。

- AU-4_16c（VC4-16c）
- AU-4_4c（VC4-4c）
- AU-4（VC4）
- AU-4 — TUG-3 — DS3
- AU-4 — TUG-3 — T3
- AU-4 — TUG-3 — E3
- AU-4 — TUG-3 — TUG-2 — VC-11 — T1
- AU-4 — TUG-3 — TUG-2 — VC-12 — E1
- AU-4 — TUG-3 — TUG-2 — VC-11
- AU-4 — TUG-3 — TUG-2 — VC-12
- AU-3: T3
- AU-3 — TUG-2 — VC-11—T1
- AU-3 — TUG-2 — VC-12—E1
- AU-3 — TUG-2 — VC-11
- AU-3 — TUG-2 — VC-12
- AU-3 — E3

管理ユニット グループ（AUG） マッピングを構成するには、たとえば、AU-3 または AU-4 マッピングの設定に次の設定コマンドを使用します。

```
configure terminal
 aug mapping [au-3 | au-4]
end
```

（注） **aug mapping** コマンドは、SDH フレーミングが設定されているときにのみ使用できます。AUG モードはデフォルトでは AUG-4 であり、STM-1 レベルでサポートされています。

SDH 回線およびセクション パラメータの設定

次のパラメータは、回線レベルとセクション レベルでの SDH 設定に影響します。

ループバック（Loopback）

SDH ポートをテストするループバックを設定します。

- local：Tx から Rx パスに信号をループします。アラーム表示信号（AIS）をネットワークに送信します。
- network：Rx から Tx パスに信号をループします。

回線ループバックの設定

```
 To configure loopback:
enable
configure terminal
controller sdh 0/0/16
loopback [local | network]
end
```

（注） システムをデフォルトの状態に戻すには、このコマンドの no 形式を使用します。

クロック送信元（Clock Source）

次の場合にクロック ソースを指定します。

- line：リンクは回線から回復したクロックを使用します。
- internal：リンクは内部クロック ソースを使用します。これがデフォルトの設定です。

```
To configure clock, use the following commands:
enable
configure terminal
controller sdh 0/0/16
clock source [line | internal]
end
```

（注） デフォルトは internal です。システムをデフォルトの状態に戻すには、このコマンドの no 形式を使用します。

ネットワーククロック SDH の設定

```
To configure network-clock SDH, use the following commands:
enable
configure terminal
controller sdh 0/0/16
clock source line
end
enable
configure terminal
network-clock input-source 1 controller sdh 0/0/16
end
```

SDH T1/E1 設定パラメータ

次のパラメータは、SDH T1/E1 の設定に影響します。

- クロック：T1 インターフェイスまたは E1 インターフェイスのクロック ソースを指定します。
- 説明：コントローラの説明を指定します。
- ループバック：ループバック モードでの T1 インターフェイスまたは E1 インターフェイスを設定します。

SDH T1/E1 パラメータの設定

```
To configure T1/E1 parameters:
enable
configure terminal
controller sdh 0/0/16
rate stm4
au-3 1
mode vc1x
tug-2 1 payload vc11
t1 1 loopback [local | network line]
t1 1 clock source [line | internal | recovered]
end
```

SDH T3/E3 設定パラメータ

次のパラメータは、SDH T3/E3 の設定に影響します。

- クロック：T3 リンクまたは E3 リンクのクロック ソースを指定します。
- ループバック：ループバック モードでの T3 リンクまたは E3 リンクを設定します。

SDH T3/E3 パラメータの設定

```
To configure SDH T3/E3 parameters configuration:
enable
```

```
configure terminal
controller sdh 0/0/16
rate stm4
au-4 1
mode tug 3
tug-3 1
mode e3
e3 1 clock source [line | internal | recovered]
e3 framing [m13 | c-bit ] (applicable to for mode e3)
e3 1 loopback [local | network line]
e3 bert pattern 0s interval 2
tug-3 2
mode t3
t3 1 clock source [line | internal | recovered]
t3 framing [m13 | c-bit ] (applicable to for mode t3)
t3 1 loopback [local | network line]
end
```

（注） これは、AUG マッピング AU-4 モード T3 および AU-3 モード T3 に適用されます。

SAToP の SDH VC 設定パラメータ

次のパラメータは、SDH VC 設定に影響します。

- クロック：VC のクロック ソースを指定します。
- ループバック：ループバック モードでの VC を設定します。

VC パラメータの設定

```
To configure VC parameters:
enable
configure terminal
controller sdh 0/0/16
rate stm4
au-3 1
mode vc1x
tug-2 1 payload vc11
vc 1 loopback [local | network]
vc 1 clock source internal
end
```

Sync-E、BITS、および PTP を使用したクロックの同期

同期イーサネット（Sync-E）：

Cisco EPN Manager を使用すると、周波数同期を有効にして、イーサネット インターフェイス上で高品質のビットクロック同期を実現できます。同期イーサネット（Sync-E）により、必要な同期が物理レベルで実現します。

これには、ルータがネットワーク内のクロックを最優先で識別できるように Sync-E を設定する必要があります。このクロックは「プライマリクロック」とも呼ばれます。ネットワーク上の他のデバイス（メンバー）は、すべてプライマリクロックの設定に基づいてクロックをリ

セットします。プライマリクロックとそのメンバー間で常にメッセージが交換され、ネットワーク内のすべてのクロックが効率的かつ継続的に同期されます。Cisco EPN Manager を使用すると、このプライマリクロックを指定でき、また、Sync-Eパラメータをグローバルレベルとインターフェイスレベルで設定できます。Sync-E プロパティを設定すると、ネットワーク トポロジ オーバーレイ上のデバイス間の論理階層とトポロジを表示できます。

（注） Sync-E 構成は、イーサネット インターフェイスでのみサポートされています。

Building Integrated Timing Supply（BITS）：

BITS では、Building Integrated Timing Supply（BITS）ポート クロックによってクロッキング情報が提供されます。Sync-E を使用するイーサネット リンクは、SONET/SDH と同じ方法で、つまり高品質なストラタム 1 追跡可能クロック信号とビット クロックのタイミングを取ることで同期されます。SSM や ESMC などの処理メッセージは、Sync-E リンクを維持し、ノードが最も信頼性に優れた送信元から常にタイミングを得られるようにします。

Precision Time Protocol（PTP）：

TDM を使用するネットワークでデータ ストリームを正確にリアセンブルするには、受信デバイスが正しいチャネルを認識できるように、デバイス クロックを定期的に同期する必要があります。Precision Time Protocol（PTP）標準：

- この同期を可能にするクロック同期プロトコルを指定します。
- ネットワーク経由で通信する 1 つ以上のノードから構成される分散システムに適用されます。

PTP は、プライマリと従属のデバイスの概念を使用して、正確なクロック同期を実現します。Cisco EPN Manager を使用することで、PTP により、従属デバイスと定期的にメッセージを交換するプライマリデバイスを設定できます。各従属デバイスは、メッセージの送受信時刻を通知した後、そのシステム時刻とプライマリデバイスのシステム時刻の差を計算します。従属デバイスは、プライマリデバイスと同期されるようにクロックを調整します。プライマリデバイスが次のメッセージ交換を開始すると、従属デバイスは再び時刻の差を計算し、クロックを調整します。このように同期が繰り返されることによって、デバイス クロックが調整され、データ ストリームが正確にリアセンブルされます。個々のインターフェイス上の PTP を変更するには、PTP クロック ポート コマンドを使用します。PTP プロパティを設定すると、ネットワーク トポロジ オーバーレイ上のデバイス間の論理階層とトポロジを表示できます。

（注） デバイスには制限があるため、インターフェイス モジュールには最大 4 つ（インターフェイス モジュールごとに最大 2 つ）のクロック ソースを設定できます。この制限は、Sync-E と TDM の両方のインターフェイスに適用されます。

Sync-E、BITS、および PTP を設定するには：

ステップ 1 **[設定（Configuration）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。

ステップ 3 グローバル Sync-E プロパティを設定します。

a) [論理ビュー（Logical View）] タブをクリックします。

b) [クロック（Clock）] > [Sync-E] をクリックします。利用可能なすべての Sync-E グローバル設定が一覧表示されます。

c) 新しいグローバル Sync-E プロパティのセットを作成するには、[+] アイコンをクリックします。Sync-E グローバル パラメータのセットは、1 つのみ作成できます。

d) Sync-E のグローバル パラメータを指定します。これらのパラメータの詳しい説明については、次の表を参照してください。

e) **[保存（Save）] をクリックします。**
変更が保存され、グローバル Sync-E の構成がデバイスに展開されます。これで、この構成に関連付けるインターフェイスを指定できます。

ステップ 4 関連付けられたインターフェイスと、インターフェイス固有の Sync-E パラメータを指定します。

a) [クロック（Clock）] > [Sync-E] をクリックし、上記の手順で作成した Sync-E グローバル構成を選択します。

b) [インターフェイス入力ソース（Interface Input Source）] タブをクリックします。

c) [+] をクリックして、必要なインターフェイスを指定します。

同期タイプごとに 1 つのインターフェイスのみを設定できます。

d) [インターフェイス名（Interface Name）] ドロップダウン メニューを使用して、必要なインターフェイスを選択します。

e) インターフェイス レベルの Sync-E パラメータを指定します。これらのパラメータの詳細については、下記の表を参照してください。

f) **[保存（Save）] をクリックします。**

ステップ 5 BITS の周波数設定を指定します（XE デバイス場合）。

a) [論理ビュー（Logical View）] タブをクリックします。

b) [クロック（Clock）] > [BITS 周波数（BITS-Frequency）] をクリックします。

c) 次の BITS の値を指定します。

- [送信元スロット（Source Slot）] : 値は RO と R1 です。
- [プライオリティ（Priority）] : 1 ～ 250 の範囲の数値。
- [クロックタイプ（Clock Type）] : 値は 2.048 MHz および 10 MHz です。

d) **[保存（Save）]** をクリックします。

ステップ 6 BITS のインターフェイスを設定します。

a) [論理ビュー（Logical View）] タブをクリックします。

b) [クロック（Clock）] > [BITS インターフェイス（BITS-Interface）] をクリックします。

c) 次の BITS の値を指定します。

XE デバイスの場合：

- [送信元スロット（Source Slot）]：オプションは RO と R1 です。
- [プライオリティ（Priority）]：1 ～ 250 の範囲の数値。
- [クロックタイプ（Clock Type）]：オプションは E1 と T1 です。

（注） BITS インターフェイスを T1 として設定するには、SSM オプションは OPTION2_GEN1 または OPTION2_GEN2 である必要があります。

XR デバイスの場合：

- [クロックインターフェイス（Clock Interface）]：オプションは BITS0_IN、BITS0_OUT、BITS1_IN、および BITS1_OUT です。
- [クロックタイプ（Clock Type）]：オプションは E1、T1、J1、_2M、および _64K です。

d) **[保存（Save）]** をクリックします。

e) インターフェイスの BITS クロックを設定します。

1. [クロック（Clock）] > [BITS インターフェイス（BITS-Interface）] に移動し、上記のステップで作成した BITS インターフェイス設定の送信元スロットをクリックします。
2. [BITS クロックの設定（Bits Clock Settings）] タブをクリックし、下記の表の説明に従ってクロックを設定します。
3. **[保存（Save）]** をクリックします。

ステップ 7 PTP クロックを設定します。

a) [論理ビュー（Logical View）] タブをクリックします。

b) [クロック（Clock）] > [PTP] をクリックします。

c) [+] をクリックして、新しい PTP 値のセットを指定するか、[クロック モード（Clock Mode）] ハイパーリンクをクリックし、ページの右上にある [編集（Edit）] アイコンをクリックします。

d) 次の共通の PTP パラメータを指定し、[保存（Save）] をクリックします。

- [クロック モード（Clock Mode）]：PTP 操作のモードを選択します。オプションは [通常（Ordinary）]、[境界（Boundary）]、および [E2E トランスペアレント（E2E Transparent）] です。E2E は、エンドツーエンド トランスペアレント クロック モードを表します。
- [ドメイン番号（Domain No）]：PTP トラフィックに使用されるドメインの番号を入力します。1 つのネットワークに複数のドメインを含めることができます。範囲は 1 ～ 127 です。
- [ハイブリッド クロック（Hybrid Clock）]：ハイブリッド クラウドを有効または無効にします。

e) [クロック モード（Clock Mode）] ハイパーリンクをクリックし、[ポート（Port）] タブをクリックして、共通のプロパティに関連付ける必要があるポートの詳細を指定します。

f) 次のポートの詳細を指定し、[保存（Save）] をクリックします。

- [ポート名（Port Name）]：PTP ポート クロックの名前を入力します。

- [ポートモード（Port Mode）]：プライマリまたは従属のクロックの PTP 権限を選択します。
- [ループバック インターフェイス番号（Loopback Interface Number）]：デバイス インターフェイスから取得したクロック識別子を入力します。
- [アナウンス タイムアウト（Announce Timeout）]：セッションがタイムアウトするまでの PTP アナウンス間隔の数を入力します。範囲は 1 ～ 10 です。
- [遅延要求間隔（Delay Request Interval）]：インターフェイスを PTP プライマリモードで動作させる時間を選択します。選択した間隔は、遅延要求メッセージのメンバーデバイスに適用されます。間隔には、基数 2 の値が使用されます。
- [同期間隔（Sync Interval）]：PTP 同期メッセージを送信する時間間隔を選択します。
- [アナウンス間隔（Announce Interval）]：PTP アナウンス パケットを送信する時間間隔を選択します。

g) [ポート名（Port Name）] ハイパーリンクをクリックし、[クロック ソース（Clock Source）] タブをクリックします。

h) [+] をクリックして新しいインターフェイスを追加するか、発信元アドレスのハイパーリンクをクリックし、ページの右上にある [編集（Edit）] をクリックします。

i) クロックの [発信元アドレス（Source Address）] と [プライオリティ（Priority）] を指定します。

- [プライオリティなし（No Priority）]：優先順位値として 0 を割り当てます。
- [プライオリティ 1（Priority 1）]：クロック選択の最初の値を確認します。優先順位が最も低いクロックが優先され、値 1 が割り当てられます。
- [プライオリティ 2（Priority 2）]：[プライオリティ 1（Priority 1）] フィールドで複数のクロックの値が同じである場合、このフィールドの値がクロック選択に使用されます。これにより、優先順位値として 2 が割り当てられます。

j) [保存（Save）] をクリックして、変更内容をデバイスに展開します。

すべての Sync-E グローバルおよびインターフェイス レベルのパラメータの詳細については、次の表を参照してください。

フィールド	説明
[クロック（Clock）] > [Sync-E 共通プロパティ（Sync-E Common Properties）]（グローバル レベル）	
自動選択プロセス	クロックの同期に使用されるメソッドのタイプを示します。値は [自動（Automatic）]、[強制（Forced）]、[手動（Manual）]、および [Cisco] です。 注：各同期タイプでは、1 つのインターフェイスのみを設定できます。

フィールド	説明
[クロック タイプ（Clock Type）]	使用されるイーサネット機器クロック（EEC）オプションを示します。 [オプション 1（Option 1）]：欧州のタイム ゾーンの EEC オプション I を表します。 [オプション 2（Option 2）]：北米のタイム ゾーンの EEC オプション II を表します。
[QL モードの有効化（QL Mode Enabled）]	クロックを品質レベル（QL）機能で使用するかどうかを示します。値は [有効（Enabled）] または [無効（Disabled）] です。
[ESMC の有効化（ESMC Enabled）]	イーサネット同期メッセージング チャネル（ESMC）のステータスを示します。値は [有効（Enabled）] または [無効（Disabled）] です。
[SSM オプション（SSM Option）]	同期ステータス メッセージ（SSM）オプションが使用されていることを示します。 [オプション 1（Option 1）]：ITU-T オプション I を表します。 [オプション 2- GEN1（Option 2-GEN1）]：ITU-T オプション II 第 1 世代を表します。 [オプション 2- GEN2（Option 2-GEN2）]：ITU-T オプション II 第 2 世代を表します。
[ホールド オフ時間（Hold Off Time）]（グローバル レベル）	障害イベントに対して保護応答を発行するまでデバイスが待機する時間の長さ（ミリ秒単位）を示します。 有効範囲は 300 ～ 1800 ミリ秒です。
[復元待ち時間（Wait To Restore Time）]（グローバル レベル）	障害が修正された後、スパンが元の状態に戻るまで待機する時間の長さ（秒単位）を示します。 有効な範囲は 0 ～ 86400 秒です。
[復帰の有効化（Revert Enabled）]	ネットワーク クロックがリバーティブ モードを使用するかどうかを指定します。値は [有効（Enabled）] または [無効（Disabled）] です。
[Sync-E] > [インターフェイス入力ソース（インターフェイス レベル）プロパティ（Interface Input Source (Interface Level) Properties）]	
[インターフェイス名（Interface Name）]	Sync-E に関連付けられたギガビットまたは 10 ギガビット インターフェイスの名前とハイパーリンク。
[アクティブ クロック（Active Clock）]	インターフェイスがアクティブ クロックとして現在選択されているかどうかを示します。このインターフェイスはプライマリインターフェイスにもセカンダリインターフェイスにもなりますが、Sync-E に現在有効になっているインターフェイスはアクティブなインターフェイスと見なされます。

フィールド	説明
[プライオリティ（Priority）]	複数のインターフェイスが設定されている場合、クロッキング用のSync-Eインターフェイスを選択するために使用される値を示します。値は 1 ～ 250 で、優先順位が最も高いのは 1 です。 優先順位が最も高いクロックは、プライマリクロックです。
[ホールド オフ時間（Hold Off Time）]（インターフェイス レベル）	クロック ソースがダウンした後、ソースを削除するまでに待機する時間の長さ（ミリ秒単位）を示します。 有効な値の範囲は 300 ～ 1800 ミリ秒です。
[復元待ち時間（Wait To Restore Time）]（インターフェイス レベル）	障害が修正された後、インターフェイスが元の状態に戻るまで待機する時間の長さ（秒単位）を示します。 有効な値の範囲は 0 ～ 86400 秒です。
[Rx Exact/QL Use]	クロックを使用する必要がある QL 受信機能を示します。
[Tx Exact/QL Send]	クロックを使用する必要がある QL 送信機能を示します。
[クロック（Clock）] > [BITS 周波数と BITS インターフェイスのプロパティ（BITS-Frequency and BITS-Interface Properties）]	
[送信元スロット（Source Slot）]	クロックソースが R0 か R1 かを示します（XE デバイスの場合）。
クロックインターフェイス	クロックソースが BITS0_IN、BITS0_OUT、BITS1_IN、または BITS1_OUT かどうかを示します（XR デバイスの場合）。
[プライオリティ（Priority）]	複数のインターフェイスが設定されている場合、クロッキング用のBITSインターフェイスを選択するために使用される値を示します。値は 1 ～ 250 で、優先順位が最も高いのは 1 です。 優先順位が最も高いクロックは、プライマリクロックです。

フィールド	説明
[クロック タイプ（Clock Type）]	使用する必要のあるクロックタイプが E1 回線と T1 回線のどちらであるかを示します（XE デバイスの場合）。XR デバイスの場合、回線は E1、T1、J1、2M、または 64K のいずれかです。 BITS インターフェイスのパラメータの場合、[クロックタイプ（Clock Type）] は、クロックに関連付ける必要のある周波数の値を示します。 XE デバイスでサポートされているクロックタイプは次のとおりです。 • [BITS 周波数（BITS Frequency）]：サポートされているオプションは 2.048_MHz と10_MHz です。 • [BITS インターフェイス（BITS Interface）]：サポートされているオプションは T1 と E1 です。 XR デバイスでサポートされているクロックタイプは次のとおりです。 • [BITS インターフェイス（BITS Interface）]：サポートされているオプションは T1、E1、J1、2M、および 64K です。
[BITS フレーミング（Bits Framing）]	BITS 構成に関連付ける必要のあるフレーミング値（CAS など）。 • XE デバイスのサポートされているビットフレーミング値：E1_CAS_CRC4、E1_CAS、E1_CRC4、E1_FAS、T1_D4、T1_ESF、および T1_SF • XR デバイスのサポートされているビットフレーミング値：E1_CRC4、E1_FAS、J1_D4、J1_ESF、T1_D4、および T1_ESF
[インピーダンス（Impedance）]	OHMS 形式のクロックに関連付けられているインピーダンス値。サポートされているインピーダンス値は 75 オームおよび 120 オームです。
[BITS サブフレーミング（Bits Sub Framing）]	E1 クロックタイプの XR デバイスでサポートされているビットサブフレーミング値は、SA4、SA5、SA6、SA7、および SA8 です。

フィールド	説明
Line Code	BITS インターフェイスに関連付ける必要がある回線コードの値。 XE デバイスでサポートされている回線コードの値は次のとおりです。 • E1 インターフェイスの場合：値は AMI と HDB3 です。 • T1 インターフェイスの場合：値は AMI と B8ZS です。 XR デバイスでサポートされている回線コードの値は次のとおりです。 • E1 インターフェイスの場合：値は AMI と HDB3 です。 • J1 インターフェイスの場合：値は AMI と B8ZS です。 • T1 インターフェイスの場合：値は AMI と B8ZS です。
Line Build Out（LBO）	BITS インターフェイスに関連付ける必要がある Line Build Out の値。このフィールドは、T1 インターフェイスでのみサポートされています。 XE デバイスでサポートされている Line Build Out の値は次のとおりです。 • T1 インターフェイスの場合：値は 0 ～ 133ft、133 ～ 266ft、266 ～ 399ft、399 ～ 533ft、および 533 ～ 655ft です。 XR デバイスのサポートされている Line Build Out の値は次のとおりです。 • T1 BITS0_OUT インターフェイスの場合：値は 0、1、2、3、および 4 です。 • T1 BITS1_OUT インターフェイスの場合：値は0、1、2、3、および 4 です。

次のタスク

（オプション）ネットワーク トポロジ オーバーレイでは、Sync-E および PTP デバイスのプロパティを表示できます。「ネットワーク トポロジ マップでのクロック同期ネットワークの表示 （248 ページ）」を参照してください。

• [Sync-E オーバーレイ（Sync-E overlay）]：Sync-E ネットワークのトポロジと階層が表示されます。各デバイスのプライマリおよびセカンダリ クロック入力が表示されます。

- [PTPオーバーレイ（PTP overlay）]：クロック同期ツリートポロジ、Precision Time Protocol の階層、およびツリー内の各デバイスのクロックロール（プライマリ、境界、従属、またはトランスペアレント）が表示されます。

IP SLA の設定（TWAMP レスポンダ/TWAMP ライトレスポンダ）

IETF Two-Way Active Measurement Protocol（TWAMP）は、TWAMP をサポートする 2 台のデバイス間でのラウンドトリップ IP パフォーマンスの測定に関する規格を定めたものです。TWAMP 制御プロトコルは、パフォーマンス測定プローブを送受信することで、パフォーマンス測定セッションを設定するために使用されます。セッションが作成されると、TWAMP テストパケットが送信され、パケット損失、遅延などのパフォーマンス統計情報の計算を支援します。TWAMP ライトは、テストセッションの確立に使用される制御プロトコルをシンプル化するという点で標準の TWAMP とは異なります。

TWAMP レスポンダは、Cisco IOS XE（NCS 42xx）と Cisco IOS XR（ASR 9000、NCS 540、NCS 560、NCS 5500）デバイスの両方でサポートされています。TWAMP ライトレスポンダは、Cisco IOS XR（ASR 9000、NCS 540、NCS 560、NCS 5500）デバイスのみでサポートされています。TWAMP ライトは IPv4 アドレスと IPv6 アドレスをサポートしていますが、標準 TWAMP は IPv4 アドレスのみをサポートしています。

TWAMP インターフェイスの設定の詳細については、次を参照してください。

- TWAMP レスポンダの設定 （439 ページ）
- TWAMP ライト レスポンダの設定 （440 ページ）

TWAMP レスポンダの設定

Cisco EPN Manager を使用して TWAMP を設定すると、選択したデバイスは TWAMP サーバーとして設定されます。TWAMP サーバーは、指定されたポートで接続要求と制御要求をリッスンします。指定した非アクティビティ値は、TWAMP 制御セッションの非アクティビティタイマー（秒単位）として構成されます。

TWAMP のエントリを追加または編集するには、次の手順を使用します。

ステップ 1 移行方法 **Configuration > Network Devices.**

ステップ 2 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 TWAMP レスポンダ設定を追加または編集するには、[IP SLA] > [TWAMP レスポンダ（TWAMP Responder）] を選択します。

ステップ 5 選択したデバイスにTWAMPパラメータを追加するには、[+]アイコンをクリックします。既存のパラメータを編集するには、[ポート名（Port Name）] ハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。デバイスごとに追加できる TWAMP パラメータのセットは 1 つだけです。

ステップ 6 必要に応じて、次のパラメータを編集します。すべてのパラメータは必須です。

- [ポート（Port）] : 1 ～ 65535 の数値を使用して、接続要求と制御要求をリッスンするように TWAMP サーバーに設定する必要があるポートを指定します。デフォルト値は 862 です。
- [非アクティビティ タイムアウト（Inactivity Timeout）] : 1 ～ 604800 の数値を使用して、TWAMP レスポンダテストセッションの非アクティビティ時間（秒単位）として設定する必要がある時間を指定します。デフォルト値は 900 秒です。
- [サーバー アイドル時間タイムアウト（Server Inactivity Timeout）] : 1 ～ 6000 の数値を使用して、TWAMP 制御セッションの TWAMP サーバー アイドル時間時間（秒単位）として設定する必要がある時間を指定します。デフォルト値は 900 秒です。

ステップ 7 [保存（Save）] をクリックして、デバイスに変更を展開します。

TWAMP ライト レスポンダの設定

TWAMP ライトレスポンダのインターフェイスを管理するには、次の手順を使用します。

- TWAMP ライトレスポンダの追加 （440 ページ）
- TWAMP ライトレスポンダの設定の編集 （441 ページ）
- TWAMP ライトレスポンダ設定の削除 （441 ページ）
- TWAMP ライトセッションの詳細を表示するコマンド （442 ページ）

TWAMP ライトレスポンダの追加

TWAMP ライトレスポンダのエントリを追加するには、次の手順を使用します。

ステップ 1 [Configuration] > [Network Devices] を選択します。

ステップ 2 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 左側のタブで、[Logical View] をクリックします。

ステップ 4 [IP SLA] > [Twamp Light Responder] を選択します。

ステップ 5 [TWAMP Light Responder] ページで [+] アイコンをクリックします。

ステップ 6 表示されたフィールドに適切な値を入力します。特定のフィールドの横にあるツールチップにマウスを合わせると、許容値の範囲に関する情報が表示されます。

a) Session ID：セッション ID を指定します。最大 65535 個のテストセッションを設定できます。

b) Timeout：（任意）TWAMP ライトレスポンダのテストセッションの非アクティブ時間を 60 ～ 86400（秒単位）の範囲で指定します。デフォルトは、タイムアウトなしです。
c) Local IP address：IPv4 アドレスまたは IPv6 アドレスを指定します。
d) Local Port：1 ～ 65535 の範囲の数値を使用して、セッション用に設定するポートを指定します。
e) Remote IP address：IPv4 アドレスまたは IPv6 アドレスを指定します。

（注） 指定された [Local IP address] が IPv4 アドレスである場合、[Remote IP address] は IPv4 アドレスである必要があります。同様に、指定された [Local IP address] が IPv6 アドレスである場合、[Remote IP address] も IPv6 アドレスである必要があります。

f) Remote Port：1 ～ 65535 の範囲の数値を使用して、セッション用に設定するポートを指定します。
g) VRF Name：ドロップダウンリストから任意の VRF 名を選択します。

ステップ 7 [保存（Save）] をクリックして、デバイスに変更を展開します。

TWAMP ライトレスポンダの設定の編集

既存の TWAMP ライトレスポンダ設定を編集するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network Devices] を選択します。
ステップ 2 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細（Device Details）] ページを起動します。
ステップ 3 左側のタブで、[Logical View] をクリックします。
ステップ 4 [IP SLA] > [Twamp Light Responder] を選択します。
ステップ 5 [Session ID] をクリックして、選択したセッションのパラメータを編集します。

（注） [Timeout] のみを変更できます。

ステップ 6 [保存（Save）] をクリックして、デバイスに変更を展開します。

TWAMP ライトレスポンダ設定の削除

既存の TWAMP ライトレスポンダ設定を削除するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network Devices] を選択します。
ステップ 2 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細（Device Details）] ページを起動します。
ステップ 3 左側のタブで、[Logical View] をクリックします。
ステップ 4 [IP SLA] > [Twamp Light Responder] を選択します。
ステップ 5 削除する [Session ID] の隣にあるチェックボックスをオンにします。

ステップ 6 [X] をクリックし、続いて [Delete] をクリックして、選択した設定の削除を確認してから削除します。

TWAMP ライトセッションの詳細を表示するコマンド

デバイスでのセッションの詳細を表示するには、次のコマンドを使用します。

コマンド	使用法
`show ipsla twamp session`	有効になっているすべての TWAMP ライトセッションを一覧表示します。
`show running-config ipsla responder twamp-light test-session <test session ID>`	特定の TWAMP ライトセッションの詳細を表示します。

インターフェイスの設定

Cisco EPN Manager を使用すると、次の設定オプションを使用して CE インターフェイスおよび光インターフェイスを設定できます。

インターフェイスを設定する前に、デバイスのインベントリ収集ステータスが [完了（Completed）] であることを確認します。

イーサネット インターフェイスとサブインターフェイスの設定

[デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、これらのインターフェイスを作成、編集、削除、有効化、無効化できます。

ステップ 1 選択項目 **Configuration > Network Devices.**

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **Interfaces > Ethernet** を選択します。

ステップ 5 イーサネット サブインターフェイスを追加するには、次の手順を実行します。

a) イーサネット インターフェイスを選択し、**Add Subinterface** をクリックします。

（注） このボタンは、選択するデバイスに応じて有効になります。たとえばCisco ASR903 デバイスの場合、このボタンは無効です。

a) [基本設定（Basic Configuration）] エリアでは、少なくとも [インターフェイス番号（Interface Number）] に番号を入力し（事前に番号が入力されていない場合）、オプションでサブインターフェイスの説明を入力します。

b) [VLAN 番号（VLAN Number）] フィールドに、このサブインターフェイスの VLAN ID を表すのに使用できる数値を入力します。802.1Q タイプのカプセル化だけがサポートされている点に注意してください。

c) ネイティブ VLAN ID と同じ VLAN 番号を使用するには、[ネイティブ VLAN（Native VLAN）] チェックボックスをオンにします。

d) [データプレーン ループバック（Dataplane Loopback）] ドロップダウン メニューで、ループバック値として設定する必要がある値を選択します。オプションは、[空白（Blank）]（設定を変更しない）、[なし（None）]（インターフェイスからイーサネットループバックを削除する）、[内部（Internal）]、および [外部（External）] です。デバイスですでに設定されている値は、太字で強調表示されます。

e) IPv4 サブインターフェイスを作成する場合は、[IPv4 インターフェイス（IPv4 Interface）] エリアで [IP タイプ（IP Type）] を選択します。選択できるオプションは、次のとおりです。

- なし
- [スタティック IP（Static IP）]：IP アドレスおよびサブネット マスクを入力します。
- [DHCP IP]：プール名を入力します。
- [DHCP ネゴシエーション（DHCP Negotiated）]：ホスト名およびクライアント ID を入力します（[なし（None）]、[インターフェイス（Interface）]、[ポート チャネル（Port Channel）]）。

また、セカンダリ IP アドレスとマスクを入力できます。

f) [IPv6 アドレス（IPv6 Address）] エリアで IPv6 サブインターフェイスを追加するには、[追加（Add）] ドロップダウンリストからタイプを選択します。オプションは [グローバル（Global）]、[アンナンバード（Unnumbered）]、[リンク ローカル（Link Local）]、[自動設定（Auto Configuration）]、[DHCP] です。

- [グローバル（Global）]：IP アドレスとサブネットマスク、およびタイプ（[一般（General）]、[EUI-64]、[エニーキャスト（Anycast）]、[CGA]）を入力します。
- [アンナンバード（Unnumbered）]：[アナンバード インターフェイス（Interface Unnumbered To）] テキスボックスにテキストを入力します。
- [リンク ローカル（Link Local）]：自動設定または手動設定（IPv6 アドレスが必要です）。
- [自動設定（Autoconfiguration）]。
- [DHCP]：アドレスの割り当てのための 2 メッセージ交換を有効にするオプション。

既存のインターフェイスまたはサブインターフェイスを編集する場合は、[インターフェイス番号（Interface Number）] の値以外のすべての値を変更できます。

（注） 異常な動作を避けるため、[説明（Description）] フィールドに § 文字を使用しないでください。

g) **[保存（Save）]** をクリックして、デバイスの選択したインターフェイスにサブインターフェイスを追加します。

ステップ 6 インターフェイスとサブインターフェイスを有効、無効、または削除するには、インターフェイスを選択して該当するボタンをクリックします。

[サブインターフェイスの削除（Delete Subinterface）] ボタンは、サポートされている一部のデバイス（Cisco ASR903 デバイスなど）でのみ有効になります。

ステップ 7 [保存（Save）] をクリックして、デバイスに変更を展開します。

ループバック インターフェイスの設定

インターフェイスのループバック状態を変更して、光ネットワークのパフォーマンスをテストできます。ループバック設定を変更する前に、デバイスが管理状態であるか、または理想的には完了状態であることを確認してください。

インターフェイスのループバック設定を変更するには、次の手順を実行します。

ステップ 1 移行方法 **Configuration > Network Devices.**

ステップ 2 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **Interfaces > Loopback** を選択します。

ステップ 5 新しいループバック インターフェイスを指定するには、 **Add** をクリックします。

a) [基本設定（Basic Configuration）] タブで、[ループバック インターフェイス番号（Loopback Interface Number）] を指定します（事前に入力されていない場合）。

b) IPv4 ループバック インターフェイスを作成する場合は、[IP タイプ（IP Type）] を指定します。

- なし。
- [静的（Static）]：静的 IP アドレスと静的 IP アドレスのサブネット マスクを入力します。
- [DHCP IP]：DHCP プール名を入力します。

また、バックアップ ループバック インターフェイスとして使用できるように、マスクを使用してセカンダリ IP アドレスを入力することもできます。

c) IPv6 ループバック インターフェイスを追加する場合は、[IPv6 アドレス（IPv6 Address）] 領域で [追加（Add）] ドロップダウン リストからタイプを選択します。選択できるオプションは、次のとおりです。

- [グローバル（Global）]：IP アドレス、サブネット マスク、およびタイプ（[一般（General）]、[EUI-64]、[エニーキャスト（Anycast）]、[CGA]）を指定する必要があります。
- [アンナンバード（Unnumbered）]：[アンナンバードインターフェイスの宛先（Interface Unnumbered To）] テキストボックスにテキストを入力する必要があります。
- [リンク ローカル（Link Local）]：自動設定または手動設定のいずれかであり、IPv6 アドレスが必要です。
- Autoconfiguration
- [DHCP]：アドレスの自動割り当てのための 2 メッセージ交換を有効にするオプションも設定できます。

ステップ 6 既存のループバック インターフェイスを編集するには、インターフェイスを選択し、[編集（Edit）] ボタンをクリックして、速度、デュプレックス、およびその他の設定のみを変更します。インターフェイス番号は編集できません。

ステップ 7 インターフェイスで上記のループバック設定を有効にするには、必要なループバック プロセスを選択し、[有効にする] をクリックします。

ステップ 8 **Save** をクリックし、これらの変更をデバイス上に展開します。

IOT インターフェイスの有効化または無効化

[デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、IOT インターフェイスを有効または無効にすることができます。これは、EM、C3794、X.21、およびシリアルインターフェイス（RS232、RS485、および RS422）に適用されます。インターフェイスを有効または無効にすると、上記技術に対応するすべてのコントローラのリストが表示されます。

（注） インターフェイスが存在しない場合は、インターフェイスの有効化または/無効化のコマンドはデバイスに送信されません。

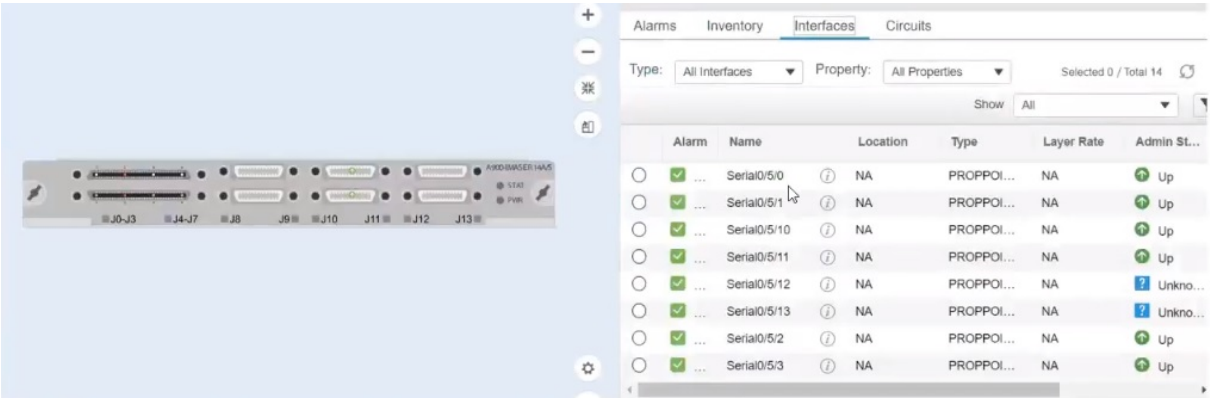
（注） すべての IOT サービスに対する QoS サポートはありません。

ステップ 1 選択項目 **Configuration > Network Devices.**

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

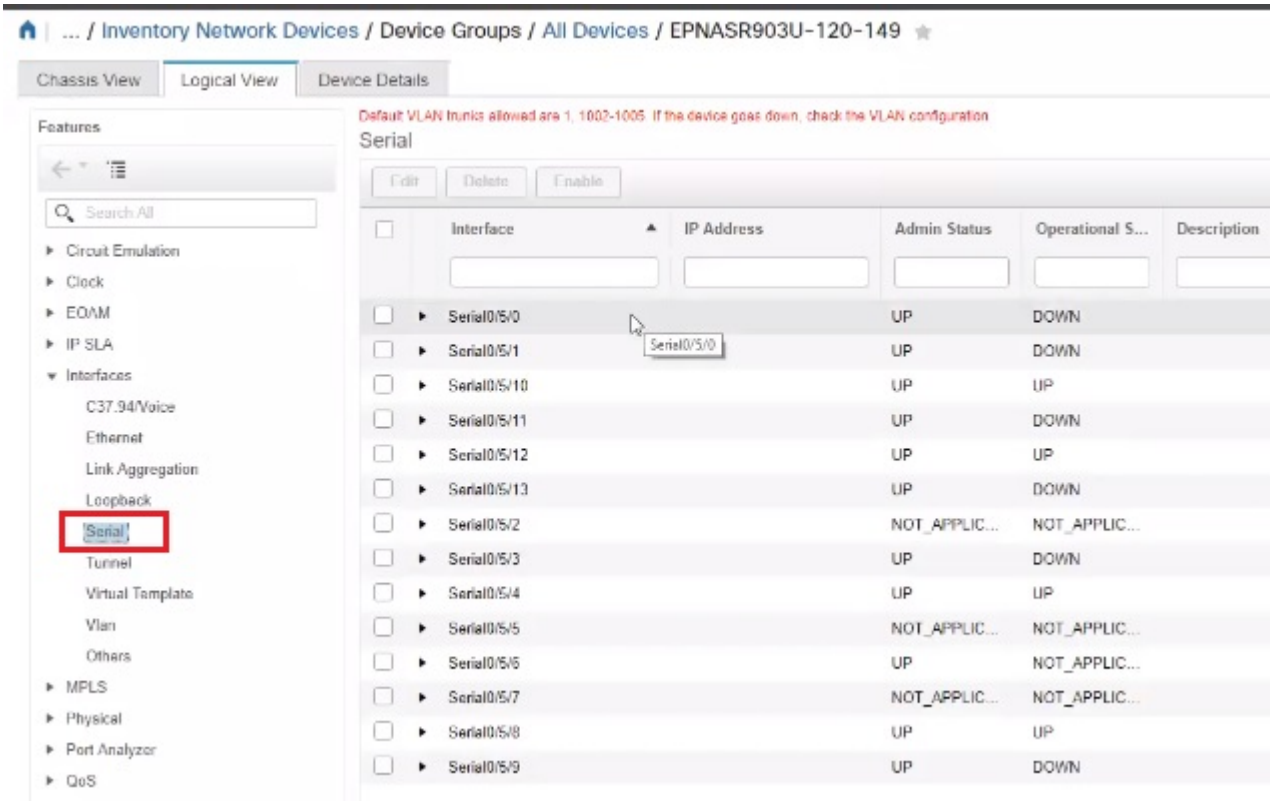
ステップ 3 [シャーシビュー（Chassis View）] タブで、設定されている CEM またはチャネルグループにリストされているすべてのシリアルコントローラを表示します。

図 *10 :* シャーシ ビュー（*Chassis View*）



ステップ 4 [論理ビュー（Logical View）] タブで、すべてのシリアルインターフェイスと、さらに X.21 インターフェイスも表示するか、あるいは有効または無効にします。

図 *11* : シリアル



ステップ 5 **Interfaces > Serial**を選択します。

ステップ 6 右側のペインで、EPNM でサポートされているシリアルコントローラのすべてのリストを表示し、一度に 1 つのコントローラを確認して有効にするか、または無効にします。

ステップ 7 **Save** をクリックします。

トンネル インターフェイスの有効化または無効化

[デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、これらのインターフェイスを有効または無効にすることができます。

ステップ 1 選択項目 **Configuration > Network Devices.**

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックし、左側のメニューから **Interfaces > Tunnel** を選択します。

ステップ 4 トンネル インターフェイスを有効または無効にするには、インターフェイスを選択し、[有効にする（Enable）] または [無効にする（Disable）] ボタンをクリックします。

（注） MPLS TE トンネルインターフェイスは、ここで有効または無効にすることができます。MPLS TE トンネルの作成または編集については、MPLS TE トンネルの作成とプロビジョニング （751 ページ）を参照してください。

スイッチ ポート インターフェイスの設定

[デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、これらのインターフェイスを編集、削除、有効化、無効化できます。

ステップ 1 選択項目 **Configuration > Network Devices.**

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

（注） [Configuration] タブは、サポートされるデバイスに対してのみ表示されます。

ステップ 4 **Interfaces > Switch Port** を選択します。

ステップ 5 インターフェイスを編集するには、インターフェイスを選択し、**Edit** をクリックします。

- 管理モードの選択：[静的（Static）]、[トンネル 802.1Q]、または [ルーテッド（Routed）]
- ポートの高速設定を有効または無効にし、必要に応じて速度とデュプレックスを調整します。

ステップ 6 **Save** をクリックします。

イーサネット インターフェイスの設定

[デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、イーサネット インターフェイスを編集、削除、有効化、無効化できます。

制限事項

- NCS 4202 および ASR 901 では、メディアタイプ RJ45 ギガビットイーサネットで速度とデュプレックスがサポートされます。
- メディアタイプが設定されていない場合、速度とデュプレックスのドロップダウンは無効になります。
- 他の IOS/XE デバイスタイプの場合、ドロップダウンは無効になり、EPNM から速度とデュプレックスの値を設定することはできません。

- NCS 4202 では、速度が 1 Gig に設定されている場合は全二重オプションのみがサポートされ、10 および 100 Mbps の場合は半二重と全二重の両方がサポートされます。
- ASR 901 では、10、100、1000 Mbps のすべての速度で、半二重および全二重がサポートされます。
- 速度ドロップダウンで [自動（Auto）] オプションを選択すると、速度とデュプレックスの両方のドロップダウンに [自動（Auto）] が反映され、この場合、ユーザーはネゴシエーションモードを [自動（Auto）] に設定できます。
- ドロップダウンから速度とデュプレックスを手動で選択すると、「no negotiation auto」コマンドが適切な速度とデュプレックスの値でデバイスに送信されます。

ステップ 1 選択項目 **Configuration > Network Devices.**

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

（注） [Configuration] タブは、サポートされるデバイスに対してのみ表示されます。

ステップ 4 **Interfaces > Ethernet** を選択します。

ステップ 5 インターフェイスを編集するには、インターフェイスを選択し、**Edit** をクリックします。

これで、必要な詳細を変更できます。

ステップ 6 **Save** をクリックします。

仮想テンプレートのインターフェイスの表示

[デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。このページからは、仮想テンプレートのインターフェイスのみを表示できます。インターフェイスを追加、編集、有効化、または無効化することはできません。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **[インターフェイス（Interfaces）] > [仮想テンプレート（Virtual Template）]** を選択します。

VLAN のインターフェイスの表示

[デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。このページからは、VLAN のインターフェイスのみを表示できます。インターフェイスを追加、編集、有効化、または無効化することはできません。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **[インターフェイス（Interfaces）]** > **[VLAN]** を選択します。

光インターフェイスの設定

EPN Manager を使用すると、光インターフェイスを設定して、管理設定を変更し、標準的な FEC モードをインターフェイス上で有効にし、ペイロード設定を変更し、ループバック設定を変更できます。これを行うには、デバイスの現在のインターフェイス設定のリストを表示する [デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブを使用します。デバイス設定とユーザーアカウントの権限に応じて、これらのインターフェイスを作成、編集、削除、有効化、無効化できます。

光インターフェイスは、次の方法で設定できます。

• スケルチ モードの設定 （475 ページ）
• NCS 1004 インターフェイスのスケルチモードとホールドオフタイマーの設定 （476 ページ）
• 例：Cisco NCS 2006 インターフェイスの管理ステータスの変更 （476 ページ）

光インターフェイスでのループバック設定の変更

インターフェイスのループバック状態を変更して、光ネットワークのパフォーマンスをテストできます。ループバック設定を変更する前に、デバイスが管理状態であるか、または理想的には完了状態であることを確認してください。変更するインターフェイスは、メンテナンス（OOS、MT）管理状態である必要があります。EPN マネージャでは、SONET、SDH、イーサネット、FC/FICON、および OTN インターフェイス タイプでのみループバック設定を編集できます。

インターフェイスのループバック設定を変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 **[光インターフェイス（Optical Interfaces）] > [メンテナンス（Maintenance）] > [ループバック（Loopback）]** を選択します。

選択したデバイスのインターフェイスがループバック設定と共に表示されます。サポートされていないインターフェイス（データ ストレージ、OTS、ビデオなど）は表示されません。

ステップ 5 ループバック設定を編集するには、インターフェイス名（ハイパーリンク）を選択し、[編集（Edit）] をクリックして変更を加えます。デバイスが [管理対象（Managed）] または [完全（Complete）] の状態で、インターフェイスが [メンテナンス（OOS、MT）（ Maintenance（OOS, MT）] 管理状態であることを確認します。

a) [内部（Internal）]：これは、ターミナル ループバックで適用されるのと同じ設定を適用します。
b) [回線（Line）]：これは、ファシリティ ループバックで適用されるのと同じ設定を適用します。
c) [ループバックなし（No_Loopback）]：このオプションを選択すると、ループバックの値がインターフェイスに設定されません。

ループバック状態を変更する前に、まずドロップダウン メニューから [ループバックなし（No_loopback）] オプションを使用して現在のループバック設定をクリアしてから、選択した設定を再適用してください。

ステップ 6 [保存（Save）] をクリックして編集内容を保存します。

ポップアップ通知によって変更のステータスが通知されます。

（注） 編集タスクが失敗した場合は、デバイスが [管理（Managed）] または [完了（Completed）] の状態にあることを確認し、Cisco EPN Manager がデバイス設定と同期していることを確認します。そうでない場合は、デバイスを Cisco EPN Manager と再同期します。デバイスのインベントリの即時収集（同期） （570 ページ）を参照してください。.

接続ステータスの継続的な確認

接続確認機能を使用すると、光インターフェイスの電力レベルを表示し、インターフェイスでの接続と挿入損失を確認できます。接続の確認ではケーブルが接続状態にあるかどうかが示され、挿入損失の確認ではケーブル損失が予想値内にあるかどうかが示されます。挿入損失のパラメータは、発生する可能性がある障害を予測するために、ネットワーク要素内の考えられるすべての光パスで収集されます。

Cisco EPN Manager を使用すると、接続確認パラメータを表示することができ、インターフェイスでの接続確認を有効または無効にすることができます。関連付けられているアラームの応答確認の値を設定することもできます。

光インターフェイスの接続ステータスを確認するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 接続確認機能を有効または無効にし、共通しきい値を設定するには、[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [接続確認（Connection Verification）] をクリックします。

ステップ 5 ページの右上隅にある [編集（Edit）] アイコンをクリックし、共通のパラメータを編集します。

ステップ 6 選択したデバイスの次のしきい値パラメータを入力し、[保存（Save）] をクリックします。

- [接続確認の有効化（Connection Verification Enabled）] : [はい（True）] または [いいえ（False）] に設定し、選択したデバイス上でこの機能を有効または無効にします。
- [失敗 IL しきい値（dB） （Fail IL Threshold (dB)）] : 0 ～ 20 の範囲の数値を入力します。このしきい値を超えると、アラームが生成されます。
- [等級の IL しきい値（db） （Degree IL Threshold (dB)）] : 失敗した IL しきい値より小さい値を入力します。

ステップ 7 [光インターフェイス（Optical Interfaces）] > [メンテナンス（Maintenance）] > [接続確認エントリ（Connection Verification Entry）] をクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 8 [A 側（A Side）] ハイパーリンクをクリックすると、接続の次の値が表示されます。

- [A 側（A Side）]：接続確認の開始スロットを表示します。
- [Z 側（Z Side）]：接続確認の宛先スロットを表示します。
- [最終更新（Last Refresh）]：接続確認と挿入損失の確認が前回実行された日時を表示します。
- [最後の接続変更（Connectivity Last Change）]：接続情報が前回変更された日時を表示します。
- [接続確認（Connectivity Verification）]：接続のステータスを表示します。
  - [接続済み（Connected）]：ケーブルまたはパッチ コードが接続されています。
  - [切断済み（Disconnected）]：ケーブルまたはパッチ コードは切断されています。
  - [無効（無効）]：ケーブルまたはパッチ コードは接続確認から除外されています。
  - [未測定（Not Measurable）]：電源を検出できません。接続確認でケーブルまたはパッチ コードをテストできません。
  - [未確認（Not Verified）]：接続確認でケーブルまたはパッチ コードがテストされていません。
- [過剰な挿入損失（dB）（Excess Insertion Loss (dB)）]：設定しきい値を超える過剰な挿入損失を表示します。
- [挿入損失の最終変更（Insertion Loss Last Change）]：挿入損失の確認情報が前回変更された日時を表示します。
- [表示名：A と Z 側、A と Z 側モジュール（Display names for- A and Z side、A and Z Side Modules）]：A と Z 側、および A と Z 側モジュールの接続の識別名。
- [Insertion Loss Verification]：次のいずれかの挿入損失の確認ステータスを表示します。
  - [Not Verified]：ケーブルまたはパッチコードに対して挿入損失の確認がテストされていません（これは最初のブート時のデフォルトステータスです）。
  - [Not Measurable]：電源を検出できません。ケーブルまたはパッチコードに対して挿入損失をテストできません。
  - [Loss OK]：ケーブルまたはパッチコードの挿入損失は予測値の範囲内です。
  - [Degrade]：ケーブルまたはパッチコードの挿入損失が劣化しています。

    挿入損失が挿入損失の劣化しきい値を超え、挿入損失の障害しきい値よりも小さい場合、パッチコードの挿入損失の確認は [Degrade] になります。[Connection Verification] ペインのパッチコードの対応する行が黄色で強調表示されます。
  - [Fail]：ケーブルまたはパッチコードの挿入損失が不合格しきい値を超えました。この状態が発生すると、GUI でパッチコードが強調表示され、障害状態を示します。

挿入損失が挿入損失の障害しきい値を超えた場合、パッチコードの挿入損失の確認は [Fail] になります。[Connection Verification] ペインのパッチコードの対応する行がオレンジ色で強調表示されます。

- [Disabled]：ケーブルまたはパッチコードは接続確認から除外されています。

- [Acknowledgement]：関連付けられたアラームの設定値が表示されます。値は True または False に設定できます。

ステップ 9 [接続確認アクション（Connection Verification Action）] ドロップダウン メニューで、設定したしきい値に到達したときに実行する必要があるアクションを選択し、[保存（Save）]をクリックします。オプションは、[損失と接続の確認（Verify loss and connectivity）]、[確認を無効にする（Disable verification）]、および [損失アラームへの確認応答（Acknowledge loss alarm）] です。

ステップ 10 （オプション）接続確認パラメータについてアラームの生成方法を指定するには、次のいずれかの値を選択します。

- [損失アラームへの確認応答（Acknowledge Loss Alarm）] : アラームを発生させずに、インターフェイスが [失敗 IL しきい値（Fail IL Threshold）] のしきい値を超えて動作できるようにします。失敗 IL しきい値がさらに増加する場合は、アラームが再発生します。

- [確認応答のクリア（Clear Acknowledge）] : [失敗 IL しきい値（Fail IL Threshold）] のしきい値がデフォルトに設定され、アラームが再評価されていることを示します。しきい値を超えると、アラームが発生します。

ODU コントローラ上の PRBS の設定

疑似ランダム バイナリ シーケンス（PRBS）は、選択したオーバーヘッド バイトを使用してヘッダーとトレーラ データを安全に転送できることを確認するためのテストメカニズムです。送信側ノードと受信側ノードの両方が、PRBS テストが行われていることを認識する必要があります。それには Cisco EPN Manager を使用して、これらのノード上で適切な PRBS モードを有効にします。Cisco EPN Manager を使用して PRBS を設定できるのは、光デバイスの非チャネライズド ODU コントローラのみです。

PRBS は PRBS_31 パターンを生成し、PRBS_11、PRBS_23、および PRBS_31 パターンを検出するために、トランク ポートも有効にします。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブに移動します。

- NCS 1004 デバイスの場合、このオプションは**[シャーシビュー（Chassis View）]** > **[設定（Configuration）]** > **[PRBSの設定（PRBS Configuration）]**で使用できます。ステップ 5 に進みます。

- NCS 4000 デバイスの場合、このオプションは [デバイスの詳細（Device Details）] ページの左上にある [論理ビュー（Logical View）] タブにあります

ステップ 4 [光インターフェイス（Optical Interfaces）] > [メンテナンス（Maintenance）] > [PRBS の設定（PRBS Configuration）] の順に選択します。すべての ODU コントローラとそれらのコントローラの現在の PRBS パラメータが表示されます。コントローラがリストされない場合は、上述の前提条件が満たされていることを確認してください。

ステップ 5 PRBS を設定するには、コントローラ名のハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。

ステップ 6 次のパラメータに変更を加えます。

a) [管理状態（Admin State）] ドロップダウン リストから、ODU コントローラの有効な管理状態を選択します。[00S-MT]（メンテナンス）、[OOS-DSBLD]（無効）、および [IS]（インサービス）の中から選択できます。

PRBS パラメータを編集できるのは、[管理状態（Admin State）] を [00S-MT]（メンテナンス）状態に設定した場合のみです。

コントローラの管理状態だけを編集する場合は、PRBS モードを [無効（Disabled）] に設定し、目的の管理状態を選択します。

b) [PRBS テスト（PRBS Test）] の値として [有効（Enabled）] または [無効（Disabled）] を選択します。

c) コントローラの PRBS モードを選択します。表の 1 列目の値（以下を参照）を最初のコントローラに設定したら、2 列目で示されている対応する値を 2 番目のコントローラ（ノード 2）に設定します。

コントローラ 1 のモード（ノード 1）	コントローラ 2 のモード（ノード 2）
ソース（Source）	シンク
シンク	ソース（Source）
送信元シンク	Loopback
Loopback	送信元シンク

d) [パターン（Pattern）] ドロップダウン リストから、次のいずれかの PRBS パターンを選択します。選択したパターンがライン カードで生成または検出されます。

- NONE
- PN11
- PN23
- PN31
- INVERTEDPN11
- INVERTEDPN31

ステップ 7 [保存（Save）] をクリックして、更新後の設定をデバイスに展開します。

ステップ 8 （オプション）設定を確認するには、選択したコントローラの [設定（Configuration）] タブで [光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [PRBS] を選択して更新後の PRBS パラメータを表示します。ODU UNI 回線に対して PRBS テストを実行するには、回線（ODU UNI）での PRBS テストの実行 （854 ページ）を参照してください。

OSC の有効化および無効化

Cisco EPN Manager を使用して、光デバイスのインターフェイス上で光サービス チャネル（OSC）の終端を有効または無効にします。OSC は OC3 回線と、次のカードの FastEthernet（FSTE）インターフェイスおよび GigabitEthernet（GigE）インターフェイス上で設定できます。

- 伝送ネットワーク制御システム（TNCS）
- 転送ノード コントローラ：拡張（TNCE）
- 転送ノード コントローラ（TNC）

ONS15454 NE の場合、サポートされているインターフェイスは次のカードの OC3 インターフェイスです。

- 光サービス チャネル モデム（OSCM）
- 光サービス チャネルおよびコンバイナ/セパレータ モジュール（OSC-CSM）

光デバイスで OSC を設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 [光インターフェイス（Optical Interfaces）] > [通信チャネル（Comm Channel）] を選択します。

選択したデバイスの設定可能なすべての G709 対応インターフェイスが表示されます。

ステップ 5 [OSC] タブをクリックします。

ステップ 6 通信チャネルの名前のハイパーリンクをクリックして、設定する通信チャネルを選択します。

通信チャネル名と現在の OSC 設定が表示されます。

ステップ 7 ページの右上にある [編集（Edit）] アイコンをクリックします。

ステップ 8 [OSC] チェックボックスを使用して、選択した通信チャネルで [OSC] を有効または無効にします。

ステップ 9 **[保存（Save）]** をクリックします。

変更が保存され、更新された設定がデバイスに展開されます。確認するには、[光インターフェイス（Optical Interfaces）]>[プロビジョニング（Provisioning）]>[通信チャネル（Comm Channel）] の下に選択した通信チャネルの OSC 設定を表示します。

未確認アラームの表示および確認応答

デバイスで生成されたアラームに基づいて、未確認ステータスのアラームの詳細を表示し、デバイス上で未読アラーム通知として表示されなくなるように [確認応答済み（Acknowledged）] としてマークできます。手順は次のとおりです。

ステップ 1 [設定（Configuration）]>[ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 **[光インターフェイス（Optical Interfaces）]>[メンテナンス（Maintenance）]>[未確認アラーム（Unverified Alarms）]** を選択して、[未確認（Unverified）] ステータスのアラームを表示します。

ステップ 5 アラームを確認し、必要なアクションを実行したら、アラームを選択し、[確認応答済み（Acknowledged）] ボタンをクリックして、これらのアラームを直接デバイス上で [確認済み（Verified）] とマークします。

光インターフェイスのプロビジョニング

Cisco EPN Manager を使用して次の設定オプションを光デバイスで有効にすることができます。

（注） 選択したデバイスに応じて、次の設定オプションが有効または無効になります。デバイスがこれらのオプションをサポートしているかどうかを確認するには、「Cisco EPN マネージャ用のサポートされているデバイス」を参照してください。

- **イーサネット MTU**

  Cisco EPN Manager を使用すると、光デバイスのイーサネット インターフェイス上に MTU 値を設定できます。MTU はインターフェイスを通過するパケットの最大伝送サイズ（バイト単位）です。Cisco EPN Manager を使用して、TNC モジュールと ECU モジュールのギガビット イーサネット インターフェイスと高速イーサネット インターフェイスを除くすべてのイーサネット インターフェイスの MTU 値を変更できます。

  新しいイーサネット MTU 値がデバイスに設定されていることを確認するには、デバイスの [デバイスの詳細（Device Details）] ページに移動し、[イーサネット インターフェイス（Ethernet Interface）] タブをクリックします。

- **GMPLS**

  Generalized Multi-Protocol Label Switching（GMPLS）を使用すると、GMPLS 回線の作成時に使用される光ファイバと異種波長パラメータを定義および表示できます。これは、MPLS プロトコル上のパケットベースのデータを網羅し、ネットワーク間でのチャネルの作成と保守を可能にします。非パケット スイッチング デバイスがサポートされています。つまり、GMPLS はパケット ベースの MPLS プロトコルを拡張して、非パケット スイッチング デバイスで構成されるネットワーク間でトンネルの作成と保守を可能にします。GMPLS トンネルは、時分割多重（TDM）インターフェイスとスイッチング タイプを横断できます。

  GMPLS を設定するには、Cisco EPN Manager の [設定（Configuration）] タブを使用します。このタブでは、すべての LMP 対応光コントローラで GMPLS を設定できます。GMPLS 設定の前提条件である LMP の有効化も同じ [設定（Configuration）] タブを使用して実行できます。

  （注） アクティブな光回線の一部である LMP 対応コントローラでは、GMPL を無効にすることはできません。

- **パケット終端**

  Cisco EPN Manager を使用すると、光デバイスの ODU コントローラでパケット終端を設定できます。これを行うには、イーサネット パケットのデバイスでパケット終端が事前に設定されていることを確認します。その後に、デバイスで既に作成され、Cisco EPN Manager によって検出された設定を編集できます。

  パケット終端を設定するには、[終端モード（Termination Mode）] と [マッピング モード（Mapping Mode）] の両方の値を指定する必要があります。

- **LMP**

  リンク管理プロトコル（LMP）は、ルーティング、シグナリング、およびリンク管理を行うために、ノード間で必要なチャネルとリンクを管理するのに役立ちます。また、LMP は、トラフィック エンジニアリング（TE）リンクの管理にも使用されます。これにより、ノードのペア間で実行する単一のトラフィック エンジニアリング（TE）リンクに複数のデータ リンクを使用できます。

  Cisco EPN Manager を使用して LMP ネイバーを作成するには、ネイバーの名前、リンク ID、ルータ ID、およびインターフェイス ID と、共通リンクおよびインターフェイス ID を指定する必要があります。光デバイスにコントローラごとに追加できる LMP リンクは 1 つだけです。

  LMP が効果的に動作できるように Cisco EPN Manager を使用して単一のデバイスに LMP 設定を正常に展開できますが、リンクに参加している両方のデバイス セットで LMP を設定する必要があります。これにより、LMP リンクがアクティブになります。

  制限事項：

- LMP リンクの作成後は [番号（Numbering）] の値を編集することはできません。[番号（Numbering）] の値を編集するには、LMP リンクを削除してから、新しい [番号（Numbering）] の値で再作成します。
- 2 つの LMP ネイバー間でネイバー ルータの ID を重複させることはできません。
- LMP リンクを追加する場合は、コントローラが別の LMP リンクにまだ関連付けられていないことを確認します。関連付けられていると、展開が失敗する原因となります。

- **OTN トポロジ**

  [設定（Configuration）] タブを使用して、光 OTN コントローラに関連付けられているトポロジ インスタンスとエリア ID を追加または変更できます。コントローラに事前に構成されたトポロジ インスタンスとエリア ID がない場合、Cisco EPN Manager はトポロジ インスタンスを OTN に、エリア ID を 0 に設定します。

  Cisco EPN Manager では、他のコントローラで事前に設定されているのと同じトポロジ インスタンスとエリア ID を使用できません。デバイスに事前に設定されているトポロジ インスタンスとエリア ID を知るには、[マップ（Maps）]>[ネットワーク トポロジ（Network Topology）] をクリックします。

- **NNI**

  光インターフェイスは、ネットワーク ノード インターフェイス（NNI）として機能するように設定できます。NNI は、インターフェイスが他のネットワーク ノードに接続していることを示します。Cisco EPN Manager では、光デバイスの OTU コントローラで NNI を設定できます。これらのインターフェイスはさらに、送信元ポートと宛先ポートとして機能するように設定できます。

  デバイスがトポロジに含まれていない場合、その NNI コントローラを設定すると、エリア ID 0 を持つそのコントローラの OTN トポロジ インスタンスが作成されます。

  デバイスに存在するすべてのコントローラに対して、コントローラごとに作成できる NNI 設定は 1 つのみです。

  注：トポロジインスタンスで事前に設定されている NNI コントローラは削除できません。

- **ブレークアウト（Breakout）**

  光デバイスでのブレークアウトを有効にすると、光ファイバとケーブルのマルチレーン アーキテクチャを使用して、単一の高密度ポートを複数の低密度ポートに分割できます。たとえば、100G ポートは 10 個の異なる 10G ポートとして動作するように設定できます。また、単一の 40G ポートは 4 つの異なる 10G ポートとして機能します。Cisco EPN Manager を使用してブレークアウトを設定するには、次の表を参照してください。

  前提条件：

  インターフェイスの [ポート モード（Port Mode）] の値を [ブレークアウト（Breakout）] に変更して、インターフェイスにブレークアウトを事前に設定してください。ポートモード/ペイロード設定とブレークアウト設定の変更（472 ページ）を参照してください。これにより、そのインターフェイスの他のすべてのポート モードパラメータが [なし（None）]

に変更されてポート上でのブレークアウトが可能になり、レーンを設定できるようになります。インターフェイスごとに最大 10 個のレーンを追加できます。

制限事項：

- 特定のインターフェイスに属するすべてのレーンは、同じマッピング タイプである必要があります。
- OTU2 コントローラと OTU2e コントローラは、パケット終端モードの場合にのみサポートされます。
- Cisco NCS 5.2.4x デバイスでは、ブレークアウト レーンはポート モードがイーサネット タイプの場合にのみ作成できます。
- OPU2e フレーミング タイプにマップされている 10G クライアントはサポートされていません。
- SONET コントローラと SDH コントローラでは、ブレークアウトは設定できません。

設定例：

コントローラ オプティクス 0/0/0/0 を選択し、マッピング モードとして GFPF でブレークアウトを有効にし、フレーム値が OPU2 の場合、デバイスにプッシュされる設定は次のようになります。

```
controller optics 0/0/0/0 breakout-mode 1 ethernet framing opu2 mapping gFpF
```

- **パフォーマンス モニターリング**

  パフォーマンスのモニターリング（PM） は、システムの保守とトラブルシューティングのためのパフォーマンス カウンタを収集するのに役立ちます。現在の PM カウンタと履歴 PM カウンタの両方を定期的に取得できます。光デバイスの OTU コントローラと ODU コントローラでパフォーマンスのモニターリングを有効または無効にできます。

  TCM コントローラ レベルでパフォーマンスのモニターリングを設定するには、OTN インターフェイスとそれらに関連する TCM パフォーマンス カウンタを設定する必要があります。

  - 参考：OTN-FEC インターフェイス用のパフォーマンス カウンタ （1213 ページ）
  - 参考：OTN-ODU インターフェイスのパフォーマンス カウンタ （1214 ページ）
  - 参考：OTN-OTU インターフェイスのパフォーマンス カウンタ （1215 ページ）

- **ODU（LO）コントローラのチャネル化**：

  ODU コントローラを複数の下位 ODU サブコントローラに関連付け、それらの ODU サブコントローラの支流ポート番号（TPN）と支流スロット（TS）を設定します。TPN の有効な範囲は 1 ～ 80 です。コロン（:）を使用して TS 文字列が区切られている場合、これは個々の支流スロットであることを示します。TS 文字列が半角ダッシュ（-）を使用して区切られている場合、これは支流スロットの範囲を示します。

  サブコントローラの ODU レベルを選択する場合は、サブコントローラの ODU レベルが、関連付けるメイン コントローラの ODU レベルよりも低くなるようにしてください。たと

えば、サブコントローラを ODU3 レベルの ODU コントローラと関連付ける場合は、サブコントローラ キャブはレベル ODU2、ODU1、または ODU1 になります。

- **OTDR の設定**：

  この機能を使用すると、修復されたファイバスパンまたはOSCチャネルの起動時にOTDRスキャンを自動的に開始するように設定できます。これを行うには、[LOS上の自動スキャン（Auto Scan on LOS）]パラメータが有効になっていることを確認します。ファイバ上のLOSがクリアされ、次の基準に基づいてアラームが発生すると、ファイバは修復するものと見なされます。

  - [絶対しきい値を有効にする（Enable Absolute Threshold）] チェックボックスをオンにすると、OTDR スキャンで測定された挿入損失が設定されている [絶対イベント損失しきい値（db）（Absolute Event Loss Threshold (dB)）] の値より大きい場合は「OTDR-LOSS-THR-EXCEEDED」 アラームが発生します。
  - OTDR スキャンの合計背面反射が指定した [合計背面反射（db）（Total Back Reflection (dB)）] の値より小さい場合。
  - [絶対合否基準（Absolute Pass Fail Criteria）] が無効になっている場合は、前回のリリースの基準からの [損失（Loss）] と [背面反射（Back Reflection）] の値がしきい値と見なされます。このシナリオでは、OTDR-LOSS-THR-EXCEEDED アラームが発生します。

  自動スキャンをトリガーする方法に応じて、次のパラメータを設定できます。

  - [スパン損失増加時の自動スキャン（Auto Scan on Span Loss Increase）]：ファイバ上で測定されたスパン損失が設定されたしきい値より大きい場合、ファイバ上でOTDRスキャンが自動的に開始されます。デフォルトのしきい値は 2 です。
  - [Rx 方向での OLR 連続測定を有効にする（Enable OLR continuous measurement on RX direction）]：設定されたしきい値に応じてカードのLINE-RXポート（入力）のスパン損失を測定します。
  - [WSON プロビジョニングから WDM 側を有効にする（Enable WDM Side from WSON Provisioning）]：OTDR スキャン中に [損失（Loss）] と [背面反射（Back Reflection）] のしきい値が交差すると、回線の作成が阻止されます。

  ファイバの合計スパン損失が許可されている範囲内に[イベント損失しきい値（Event Loss Threshold）] の値を設定できます。ファイバ上で測定されたスパン損失がイベント損失しきい値より大きい場合、OTDR スキャンはファイバ上でトリガーされます。

- **自動レーザー遮断（ALS）の設定**

  自動レーザー遮断（ALS）は、ファイバの切断などの問題が発生した場合にトランスミッタの出力電力を自動的にシャットダウンするために使用される技術です。ALSがファイバペアの両端にプロビジョニングされていれば、破損したファイバから危険なレベルのレーザー光が漏れるのを防ぐ安全機能になります。インターフェイスがシャットダウンされたら、ALSモードを次のように設定し、インターフェイスを再起動するために実行する必要があるアクションを設定できます。

- [無効モード（Disabled mode）]：モードが無効になっている場合は、ALS が無効になります。信号消失（LOS）はレーザーのシャットダウンを引き起こしません。
- [手動再起動モード（Manual restart mode）]：ALS エージェントが 500 ミリ秒にわたる LOS を検出するとレーザーがオフになります。ALS を連動させると、手動コマンドが発行されてパルス幅の期間はレーザーがオンになります。LOS が 100 ms 間解除されていた場合、レーザーがオンになります。
- [自動再起動モード（Automatic restart mode）]：ALS エージェントが 500 ミリ秒にわたる LOS を検出すると、レーザーはパルス間隔の間はシャットダウンされます。その後、選択したパルス幅の期間はレーザーが自動的にオンになります。LOS が依然として存在する場合、レーザーは再びシャットダウンされます。LOS が 100 ms 間解除されるまでこのパターンは継続し、100 ms 間解除されると、レーザーがオンのままになります。

Cisco EPN Manager を使用すると、ALS モード、ALS リカバリ間隔（秒単位）、およびリカバリ パルス幅（秒単位）を設定できます。インターフェイスの ALS モードが [手動再起動（Manual Restart）] に設定されている場合は、インターフェイスを手動で再起動する必要があります。これを行うには、デバイスの [デバイスの詳細（Device Details）] ページに移動し、[光（Optical）] > [自動レーザー シャットダウン（Automatic Laser Shutdown）] を選択し、[手動再起動 ALS モード（Manual Restart ALS mode）] に設定されたインターフェイスを見つけて、[再起動（Restart）] ボタンをクリックします。

- **SNTP サーバーを使用した日付と時刻の設定**：

  シンプル ネットワーク タイム プロトコル（SNTP）は、コンピュータのクロックを基準時刻に同期するために使用されるインターネット プロトコルです。SNTP サーバーを使用すると、すべての NE で同じ日付と時刻の基準が使用されます。サーバーにより、停電やソフトウェアのアップグレード後にノードの時刻が同期されます。

  SNTP サーバーを使用して日付と時刻を設定するには、まず現在の時刻とタイム ゾーン値を指定してから、日付と時刻の基準ポイントとして使用できるプライマリ サーバーとバックアップ サーバーを設定する必要があります。タイムゾーン値を設定する前に、SNTP サーバー値が設定されていないことを確認してください。SNTP サーバーを削除する場合は、最初に必ずバックアップ サーバーを削除した後でプライマリ サーバーを削除してます。プライマリ サーバーのみを削除することはできません。

- **波長の設定**：

  Cisco EPN Manager を使用すると、光学コントローラの波長周波数をプロビジョニングできます。光学コントローラで設定された現在の波長を表示した後、選択したカードのタイプに応じて波長周波数を変更できます。

  波長は、DWDM 光学ポートとして設定されている場合にのみ、光学コントローラで設定できます。波長を変更するときは、光ポートを [In Service] 状態にすることはできません。

表：光インターフェイスのプロビジョニング

上記の機能を使用して光デバイスを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 次の表に示すように、必要な設定メニューに移動し、必要な値を指定します。

表 *23 :* 表 : 光インターフェイスの設定

タスク	サポートされているインターフェイス/コントローラ	ナビゲーション	注記
イーサネット MTU の設定	TNC モジュールと ECU モジュール上のギガビット/高速イーサネットインターフェイスを除くすべてのイーサネット インターフェイス。	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [イーサネット MTU（Ethernet MTU）]	-
GMPLS の設定	LMP 対応の光コントローラ。	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [GMPLS]	-
パケット終端の設定	パケット終端で事前に設定された ODU コントローラ。	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [OTN] > [パケット終端（Packet Termination）]	イーサネット パケットにのみ適用されます。
LMP ネイバーの設定	すべての光コントローラ。	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [LMP]	ネイバー ルータ ID をネイバー間で重複させることはできません
OTN トポロジの設定	すべての光 OTN コントローラ。	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [OTN] > [トポロジ（Topology）]	-

NNI の設定	すべての OTU コントローラ。	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [OTN] > [NNI]	-
ブレークアウトの設定	ポート モードの値を持つすべての光コントローラが「ブレークアウト」に設定されています。	光インターフェイス > プロビジョニング > ポート モード > ブレークアウト タブ	-
パフォーマンス モニターリングの設定	すべての OTU および ODU コントローラ。	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [パフォーマンス モニターリング（Performance Monitoring）]	-
ODU（LO）コントローラのチャネル化	すべての ODU コントローラ。	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [ODU チャネル化（ODU Channelization）] > [サブ コントローラ（Sub-Controllers）] タブ	-
OTDR の設定	-	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [OTDR 設定（OTDR Settings）]	-
ALS の設定	すべての ALS サポート対象インターフェイス	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [自動レーザー シャットダウン（Automatic Laser Shutdown）]	-

SNTP を使用した日付と時刻の設定	-	• SNTP のプライマリサーバーとバックアップ サーバーを指定するには、次の手順を実行します。 [光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [NTP 設定（NTP Settings）] を選択します。 • SNTP で使用できる現在の時刻とタイムゾーンを指定するには、次の手順を実行します。 [光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [タイム ゾーン設定（Time Zone Settings）] を選択します。	-
波長の設定	すべての光学コントローラ	[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [波長（Wavelength）]	-
TCM と TTI の設定	-	TCM パラメータと TTI パラメータの設定（469ページ）を参照してください	-
保護プロファイルの設定	-	保護プロファイルの設定（468ページ）を参照してください	-
ペイロードとブレークアウトの設定	-	ポートモード/ペイロード設定とブレークアウト設定の変更 （472 ページ）を参照してください	-

管理ステータスの設定	-	光インターフェイスの管理ステータスの変更（466ページ）を参照してください	-
FEC モードの設定	-	OTN インターフェイスの設定 （473 ページ）を参照してください	-
GCC の有効化と無効化	-	参照 GCC 接続の有効化および無効化（474ページ）	-
スケルチ モードの設定	-	参照 スケルチ モードの設定 （475 ページ）	-

光インターフェイスの管理ステータスの変更

Cisco EPN Manager を使用すると、インターフェイスの管理状態を変更して、光ネットワークのパフォーマンステスト能力を向上させることができます。インターフェイスの管理ステータスは、インターフェイスが Cisco EPN Manager によって管理されているか、ダウンしているか、またはメンテナンスモードになっているかを定義します。インターフェイスの管理ステータスがダウンの場合は、そのインターフェイスが到達不能状態であるか、またはデバイスが Cisco EPN Manager でサポートされていないことを示します。管理ステータスを [動作中（Up）] に変更すると、Cisco EPN Manager でインターフェイスを管理できるため、より優れた監視機能が提供されます。インターフェイスの管理状態を変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 **[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [管理ステータス（Admin Status）]** を選択します。

選択したデバイスのインターフェイスが、管理状態の設定と共に表示されます。管理状態を変更できないインターフェイス（PCHAN インターフェイスや PLINE インターフェイスなど）は表示されません。

ステップ 5 [光コントローラ（Optical Controllers）] タブまたは [イーサネット コントローラ（Ethernet Controllers）] タブをクリックして、必要なコントローラを編集します。

ステップ 6 管理ステータスを編集するには、インターフェイスの名前ハイパーリンクをクリックしてインターフェイスを選択し、ページの右上隅にある [編集（Edit）] アイコンをクリックします。デバイスのインベントリ収集ステータスが [管理（Managed）] か [完了（Completed）] であることを確認します。

次の値のいずれかを選択します。

a) [ダウン（DOWN）]：インターフェイスが管理上はダウンすることを意味します。
b) [動作中（UP）]：インターフェイスが管理上は動作していることを意味します。
c) [テスト中（TESTING）]：インターフェイスはメンテナンス状態であり、管理者がインターフェイスを使用してテストを実行していることを意味します。

ステップ 7 [保存（Save）] をクリックして保存して、変更をデバイスに展開します。

ポップアップ通知によって変更のステータスが通知されます。Cisco NCS2K デバイス上で変更される管理ステータスの例を確認するには、例：Cisco NCS 2006 インターフェイスの管理ステータスの変更（476 ページ）を参照してください。

（注） 編集タスクが失敗した場合は、デバイスが [管理（Managed）] または [完了（Completed）] の状態にあることを確認し、Cisco EPN Manager がデバイス設定と同期していることを確認します。そうでない場合は、デバイスのインベントリの即時収集（同期）（570 ページ）の説明に従って、デバイスを Cisco EPN Manager と再同期します。

シャーシビューでの光インターフェイスの管理ステータスの変更

Cisco EPN Manager を使用すると、インターフェイスの管理状態を変更して、光ネットワークのパフォーマンステスト能力を向上させることができます。インターフェイスの管理ステータスは、インターフェイスが Cisco EPN Manager によって管理されているか、ダウンしているか、またはメンテナンスモードになっているかを定義します。インターフェイスの管理ステータスがダウンの場合は、そのインターフェイスが到達不能状態であるか、またはデバイスが Cisco EPN Manager でサポートされていないことを示します。管理ステータスを [動作中（Up）] に変更すると、Cisco EPN Manager でインターフェイスを管理できるため、より優れた監視機能が提供されます。インターフェイスの管理状態を変更するには、次の手順を実行します。

始める前に

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [シャーシビュー（Chassis View）] ウィンドウで、[設定（Configuration）] タブをクリックし、[回線（Line）] をクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 管理ステータスを編集するには、インターフェイスの名前ハイパーリンクをクリックしてインターフェイスを選択し、ページの右上隅にある [編集（Edit）] アイコンをクリックします。デバイスのインベントリ収集ステータスが [管理（Managed）] か [完了（Completed）] であることを確認します。

次の値のいずれかを選択します。

a) [ダウン（DOWN）]：インターフェイスが管理上はダウンすることを意味します。

b) [動作中（UP）]：インターフェイスが管理上は動作していることを意味します。
c) [テスト中（TESTING）]：インターフェイスはメンテナンス状態であり、管理者がインターフェイスを使用してテストを実行していることを意味します。
d) [動作および使用中（UP AINS）]：インターフェイスが管理上は動作し、使用中であることを意味します。

（注） [動作および使用中（UP AINS）] ステータスは、シャーシビューにのみ表示されます。

ステップ 5 [保存（Save）] をクリックして保存して、変更をデバイスに展開します。

ポップアップ通知によって変更のステータスが通知されます。

（注） 編集タスクが失敗した場合は、デバイスが [管理（Managed）] または [完了（Completed）] の状態にあることを確認し、Cisco EPN Manager がデバイス設定と同期していることを確認します。そうでない場合は、デバイスのインベントリの即時収集（同期） （570 ページ）の説明に従って、デバイスを Cisco EPN Manager と再同期します。

保護プロファイルの設定

Cisco EPN Manager を使用すると、光デバイスに異なる保護プロファイル（またはグループ）をプロビジョニングできます。これにより、これらのデバイスの可用性が確保され、信頼性が向上します。保護プロファイルは、カードで自動保護スイッチング（APS）を有効にする必要があるかどうかを定義し、また、障害発生時のトラフィック フローの方向も設定します。デバイス上のカードは、設定の単方向の再生成をサポートするように設定することも、送信チャネルと受信チャネルのいずれかに障害が発生した場合に、両方のチャネルが切り替わるように設定することもできます。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。
ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。
ステップ 3 [デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブをクリックします。
ステップ 4 **[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [保護プロファイル（Protection Profile）]** を選択します。
ステップ 5 保護プロファイルを追加するには、[+] 記号をクリックします。
ステップ 6 保護プロファイルに一意の名前を指定します。この名前は必須フィールドであり、最大 32 文字で、スペースを含めることはできません。
ステップ 7 保護プロファイルに必要なタイプを選択します。選択できるオプションは、次のとおりです。

- [1 + 1 BDIR APS（One plus one BDIR APS）]：1 + 1 の自動保護切り替え（APS）を有効にし、カードを双方向に設定します。
- [1 + 1 UNIDIR APS（One plus one UNIDIR APS）]：1 + 1 の自動保護切り替え（APS）を有効にし、カードを単方向に設定します。

- [1 + 1 UNIDIR NO APS（One plus one UNIDIR NO APS）]：APS なしに 1 + 1 を有効にし、カードを単方向に設定します。
- [1 + 1 PLUS R BDIR APS（One plus one PLUS R BIDIR APS）]：1 + 1 + R の APS を有効にし、カードを双方向に設定します。

（注）
- BDIR（双方向）は、送信チャネルと受信チャネルのどちらかに障害が発生した場合に、その両方が切り替わることを意味します。
- UNIDIR（単方向）は、カードが単方向の設定の再生成をサポートしていることを意味します。したがって、ポートが送信ポートである場合はリンクの送信元として、受信ポートである場合はリンクの宛先としてのみポートを使用できます。

ステップ 8 プロファイルの保護モードを**[元に戻す]**または**[非リバーティブ]**として選択します。リバース モードは、[復元の待機時間（Wait to Restore Time）] として指定した（ステップ 9）時間が経過した後、障害状態をポストした現用ポートに対してノードがトラフィックを戻すようにします。

ステップ 9 サブネットワークの接続モードを [SNC_N]（デフォルト）、[SNC_I]、または [SNC_S] として選択します。

ステップ 10 サブネットワークの接続モードを [SNC_S] として選択すると、TCM ドロップダウン リストから TCM-ID 値を選択できます。デフォルトでは、サブネットワーク接続モードとして [SNC_S] を選択すると、TCM-4 が選択されます。[TCM-ID] 列値は、SNC_S の場合、[TCM4] から [TCM1] ～ [TCM6] に変更できます。

（注） [SNC_I] と [SNC_N] の場合、[TCM-ID] 値を変更することはできません。[なし（None）] に設定する必要があります。

ステップ 11 0 ～ 720 の数値を使用して、[復元の待機時間（Wait to Restore Time）] を秒単位で入力します。0 より大きい値の場合、値は 300 より大きく、30 秒間隔で指定してください。復元の待機時間は、回線が復元されるまで待機する必要がある時間を定義します。保護モードに [元に戻す（Revertive）] を選択した場合、デフォルトの復元の待機時間は 300 で、それ以外は 0 です。

ステップ 12 [保留時間（Hold Off Time）] の値をミリ秒単位で入力します。この値は、システムが代替パスに切り替えるまで待機する時間を定義します。有効な範囲は 100 ～ 10000 秒です。デフォルト値は 0 です。

ステップ 13 [保存（Save）] をクリックして、更新後の変更内容をデバイスに展開します。

ステップ 14 （オプション）設定を確認するには、選択したコントローラの [設定（Configuration）] タブで [光インターフェイス（Optical Interfaces）]>[プロビジョニング（Provisioning）]>[保護プロファイル（Protection Profile）] を選択して更新後の保護プロファイル パラメータを表示します。

（注） 上記の手順は、NCS2K デバイスには適用されません。

TCM パラメータと TTI パラメータの設定

Cisco EPN Manager を使用すると、ODU トンネル 回線の ODU コントローラでタンデム接続モニターリング（TCM）とトレイルトレース識別子（TTI）を設定できます。これにより、これらのコントローラでのパフォーマンス監視機能を有効または無効にすることができます。

これらのODUコントローラのTCM接続に信号障害と信号劣化のしきい値を設定することで、デバイスの機能をさらに監視できます。また、送信元および宛先のアクセスポイント識別子を変更することもできます。これを行うには、次の前提条件が満たされていることを確認してください。

始める前に

- デバイスのインベントリ収集ステータスが[完了（Completed）]であることを確認します。
- コントローラがループバック用に設定されていることを確認します。そうでない場合は、**[光インターフェイス（Optical Interfaces）]** > **[メンテナンス（Maintenance）]** > **[ループバック（Loopback）]**でコントローラのループバック設定を変更します。ループバックインターフェイスの設定 （445 ページ）を参照してください。

（注） ODU UNI 回線のエンドポイントでは、TCM は OTUx-ODUx コントローラでのみサポートされています。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 TCM/TTI パラメータを設定するには、**[光インターフェイス（Optical Interfaces）]** > **[プロビジョニング（Provisioning）]** > **[TCM の設定（TCM Configuration）]**を選択します。

または、デバイスの[シャーシビュー（Chassis View）]タブに移動し、シャーシエクスプローラからカードを選択して[設定（Configuration）]タブをクリックし、[OTN]>[トレース識別子（Trail Trace Identifier）]を選択します。

（注） NCS2K デバイスの TCM パラメータを設定するには、デバイスの [シャーシビュー（Chassis View）] タブに移動し、シャーシエクスプローラからカードを選択して [設定（Configuration）] タブをクリックし、[OTN] > [トレールトレース識別子（Trail Trace Identifier）] を選択します。

ステップ 5 リストに表示されているコントローラのいずれかのTCMパラメータを表示または編集するには、そのコントローラの [TCM ID] ハイパーリンクをクリックします。

ステップ 6 これらのパラメータを編集するには、ページの右上隅にある [編集（Edit）]アイコンをクリックします。

ステップ 7 次の TCM パラメータに変更を加えます。

編集可能な TCM パラメータ	説明
状態（State）	デバイス上の TCM プロパティの状態を有効または無効に設定します。

編集可能な TCM パラメータ	説明
信号障害のしきい値（Signal Failure Threshold）	ODUk コントローラの信号障害のしきい値を設定します。値は E6、E7、E8、および E9 です。
送信済み API（Sent API）	TTI の送信元アクセス ポイント識別子を設定します。 最大 14 バイト長の値を入力します。
送信済み DAPI（Sent DAPI）	TTI の宛先アクセス ポイント識別子を設定します。最大 14 バイト長の値を入力します。
送信済み演算子固有文字列型（Sent Operator Specific String Type）	TTI の演算子固有文字列の型を 16 進数または ASCII 型として設定します。
送信済み演算子固有文字列（Sent Operator Specific String）	TTI の演算子固有文字列を設定します。 最大 32 文字の長さの値を入力します。
パフォーマンス モニター（Performance Monitor）	ODUk コントローラのパフォーマンス監視を有効または無効にします。
信号劣化のしきい値	信号劣化のしきい値を設定します。 値は E6、E7、E8、および E9 です。
予測 SAPI（Expected SAPI）	TTI の現在の送信元アクセス ポイント識別子を設定します。最大 14 バイト長の値を入力します。
予測 DAPI（Expected DAPI）	TTI の現在の宛先アクセス ポイント識別子を設定します。最大 14 バイト長の値を入力します。
予測演算子固有文字列型（Expected Operator Specific String Type）	TTI の演算子固有文字列の型を 16 進数または ASCII 型として設定します。
予測演算子固有文字列（Expected Operator Specific String）	TTI の演算子固有文字列を設定します。 最大 32 文字の長さの値を入力します。

ステップ 8 [保存（Save）] をクリックして、更新後の設定をデバイスに展開します。

ステップ 9 （オプション）設定を確認するには、[設定（Configuration）] タブで [光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] > [TCMの設定（TCM Configuration）] を選択し、選択したデバイスの TCM パラメータを表示します。

ステップ 10 （オプション）これらの更新後の TCM パラメータと TTI パラメータは、選択したデバイスの [デバイスの詳細（Device Details）] とポート 360 ビューで表示できます。デバイスの詳細の表示 （105 ページ）および特定のデバイスのインターフェイスを表示する：[デバイス 360（Device 360）] ビュー （129 ページ）を参照してください。

ステップ 11 （オプション）TCM パラメータは、ネットワーク トポロジ オーバーレイにも表されます。これらのパラメータを表示するには、[マップ（Map）]>[ネットワーク トポロジ]に移動し、関連付けられたこれらの TCM パラメータを持つ光回線を選択します。

ポートモード/ペイロード設定とブレークアウト設定の変更

[デバイスの設定（Device Configuration）] タブを使用すると、SONET インターフェイスと SDH インターフェイス上のパケットのペイロードのタイプを表示および変更して、それらのブレークアウトを有効にすることができます。ペイロード設定を変更する前に、デバイスが Cisco EPN Manager と同期していることを確認します。光デバイスでのブレークアウトを有効にすると、光ファイバとケーブルのマルチレーンアーキテクチャを使用して、単一の高密度ポートを複数の高密度ポートに分割できます。たとえば、100G ポートは 10 個の異なる 10G ポートとして動作するように設定できます。また、単一の 40G ポートは 4 つの異なる 10G ポートとして機能します。

インターフェイス上のペイロードとブレーククアウト設定を変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **[光インターフェイス（Optical Interfaces）]** > **[プロビジョニング（Provisioning）]** を選択します。

ステップ 5 選択したデバイスのタイプに応じて、**[ペイロードタイプ（Payload Type）]** または **[ポートモード（Port Mode）]** を選択します。

ステップ 6 変更するインターフェイスの名前（ハイパーリンク）をクリックします。

名前やそのペイロード タイプなどのインターフェイスの共通プロパティが表示されます。

ステップ 7 変更する OTN インターフェイスの名前（ハイパーリンク）をクリックし、[編集（Edit）] アイコンをクリックします。

ステップ 8 [ポート モード（Port Mode）]、[フレーミング（Framing）]、[マッピング タイプ（Mapping Type）]、[レート（Rate）]、および [ビット レート（Bit Rate）] の値を変更します。これらの値がカードの帯域幅制限を超えないようにしてください。

ステップ 9 このインターフェイス上のイーサネット パケットと OTN パケットのブレークアウト レーンを関連付けるには、[ブレークアウト（Breakout）] タブをクリックします。このタブは、デバイスにブレークアウトが事前に設定されている場合にのみ表示されます。

a) [+] アイコンをクリックして新しいレーンを追加します。コントローラあたり最大 10 レーンを追加できます。既存のレーンを変更するには、[レーン（Lane）] ハイパーリンクをクリックします。
b) ブレークアウト レーンのレーン番号、ポート モード、マッピング タイプ、所有ポート番号、フレーミング値などのブレークアウト パラメータを指定します。

ステップ 10 [保存（Save）] をクリックして、変更内容をデバイスに展開します。

ポップアップ通知によって変更のステータスが通知されます。

（注） 編集タスクが失敗した場合は、インターフェイスが [管理（Managed）] であることを確認し、Cisco EPN Manager がデバイス設定と同期していることを確認します。そうでない場合は、デバイスを Cisco EPN Manager と再同期します。デバイスの変更内容の保存 （570 ページ）を参照してください。また、ペイロードがカードの帯域幅制限を超えていないことを確認します。

（注） 手順 6 ー 10 は、NCS2K デバイスには適用されません。

OTN インターフェイスの設定

FEC モードは、OTN 回線の転送エラー修正（FEC）メカニズムを定義します。転送エラー修正（FEC）メカニズいむはマージンの改善と光リーチの拡張のためにパフォーマンスを向上させます。FEC モード設定を [標準（Standard）] に変更するには、[デバイスの設定（Device Configuration）] タブを使用する必要があります。

FEC モード設定を変更する前に、変更しようとしているインターフェイスの管理状態が [ダウン（故障中）（Down (out of service)）] で、G709 の設定が有効になっていることを確認してください。G709 の設定を有効にするには、シャーシ ビューで OTN 回線の設定を使用します。

インターフェイスの FEC モードを変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 **[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）]** を選択します。

ステップ 5 FEC を [ダウン（Down）] に変更する必要がある OTN インターフェイスの管理状態を変更します。光インターフェイスの管理ステータスの変更 （466 ページ）を参照してください。

ステップ 6 デバイス タイプに応じて次のいずれかを選択し、変更するインターフェイスを選択します。

- **[OTN 回線（OTN Lines）] > [OTNFEC]**
- **[OTN] > [FEC]**

選択したデバイスの設定可能なすべての G709 対応インターフェイスが表示されます。

または、デバイスの [シャーシ ビュー（Chassis View）] タブに移動し、シャーシエクスプローラからカードを選択して [設定（Configuration）] タブをクリックし、[OTN] > [OTN 回線（OTN Lines）] を選択します。このオプションを使用すると、同期メッセージの有効化、管理者 SSM の選択、同期提供パラメータの有効化、G709 値の true または false への設定など、追加パラメータを設定できます。

ステップ 7 編集するインターフェイスを選択し、ウィンドウの右上にある [編集（Edit）] アイコンをクリックします。

ステップ 8 必要な FEC モードを選択します。デフォルトは [なし（None）] です。

ステップ 9 （Cisco NCS 2000 デバイスのみ）必要な **SDBER** 値を選択します。信号劣化ビットエラー レート（SDBER）の条件は、設定したしきい値に基づき、回線劣化に対して信号劣化アラームが発生することを示します。

ステップ 10 [保存（Save）] をクリックして変更を保存します。

ポップアップ通知によって変更のステータスが通知されます。

（注） 編集タスクが失敗した場合は、インターフェイスが [管理（Managed）] または [完了（Completed）] であることを確認し、Cisco EPN Manager がデバイス設定と同期していることを確認します。また、デバイスで G709 の設定が有効になっていることを確認する必要もあります。インターフェイスの管理状態を変更するには、光インターフェイスの管理ステータスの変更（466 ページ）を参照してください。

GCC 接続の有効化および無効化

Cisco EPN Manager は、光デバイスのインターフェイス上での汎用通信チャネル（GCC）接続のプロビジョニングをサポートしています。GCC は、TXP カードまたは MXP カードのトランク ポートと OTN、OTU、および ODU コントローラで設定できます。GCC の設定は、インターフェイスで設定された FEC モードと管理ステータスに関係なく変更できます。

光デバイスで GCC を設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] の順に選択します。すべての Cisco EPN Manager デバイスが表示されます。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定する光デバイスを選択します。

ステップ 3 [設定（Configuration）] タブをクリックし、[光インターフェイス（Optical Interfaces）] > [プロビジョニング（Provisioning）] を選択します。

ステップ 4 デバイス タイプに応じて次のいずれかを選択します。

- **[通信チャネル（Comm Channels）] > [GCC]**
- **[OTN] > [GCC]**

選択したデバイスの設定可能なすべての G709 対応インターフェイスが表示されます。

ステップ 5 編集するコントローラのタイプに基づいて、[OTU コントローラ（OTU Controllers）] タブまたは [ODU コントローラ（ODU Controllers）] タブをクリックします。

ステップ 6 リストに表示されているコントローラのいずれかの GCC の設定を編集するには、コントローラの名前ハイパーリンクをクリックします。

ステップ 7 ページの右上にある [編集（Edit）] アイコンをクリックします。

ステップ 8 [GCC] チェックボックスを使用し、選択したコントローラの GCC を有効または無効にします。ODU コントローラで設定される値は GCC1 で、OTU コントローラで設定される値は GCC0 です。

ステップ 9 **[保存（Save）]** をクリックします。変更が保存され、更新された設定がデバイスに展開されます。

設定を確認するには、[光インターフェイス（Optical Interfaces）]>[プロビジョニング（Provisioning）] で、選択したコントローラの GCC パラメータを表示します。

400G-XC トランク ポートを搭載した Cisco NCS デバイス上で GCC を有効にすると、Cisco EPN Manager はトランク ポート間の OUT リンクを検出します。

スケルチ モードの設定

Cisco EPN Manager を使用すると、光デバイスのインターフェイス上に異なるスケルチ モードを設定できます。スケルチモードは特定の障害に応答して遠端レーザーをシャットダウンするのに役立ちます。スケルチ モードは、OCH、OTN、SONET または SDH、FC または FICON、イーサネット、ビデオ、および光デバイスのデータ ストレージ インターフェイスで設定できます。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [設定（Configuration）] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細（Device Details）] ページの上部にある [論理ビュー（Logical View）] タブの下にあります。

ステップ 4 **[光インターフェイス（Optical Interfaces）]** > **[プロビジョニング（Provisioning）]** > **[スケルチ モード（Squelch Mode）]** を選択します。

ステップ 5 インターフェイスの名前ハイパーリンクをクリックして、設定するインターフェイスを選択します。

インターフェイスの名前と現在のスケルチ モード設定が表示されます。

ステップ 6 ページの右上隅にある [編集（Edit）] アイコンをクリックします。

ステップ 7 インターフェイスに必要なスケルチ モードを選択します。選択できるオプションは、次のとおりです。

- [無効（DISABLE）]：スケルチが無効になっています。
- [AIS]：アラーム表示信号（AIS）が有効になっています。
- [なし（NONE）]：透過モードが有効になっています。
- [スケルチ（SQUELCH）]：スケルチが有効になっています。
- **[ODU_AIS]**
- [G_AIS]：Generis AIS が有効になっています。
- [NOS]：FC ペイロードでスケルチが無効になっています。
- **[LF]**

ステップ 8 **[保存（Save）]** をクリックします。

変更が保存され、更新された設定がデバイスに展開されます。確認するには、**[光インターフェイス] > [スケルチ**モード] の下に、選択したインターフェイスのスケルチ モード パラメータを表示します。

NCS 1004 インターフェイスのスケルチモードとホールドオフタイマーの設定

スケルチモードは特定の障害に応答して遠端レーザーをシャットダウンするのに役立ちます。NCS 1004 インターフェイスのスケルチモードとホールドオフタイマーを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [Configuration] タブをクリックして [Ethernet] タブを選択します。

ステップ 4 編集するインターフェイスを選択して編集アイコンをクリックします。

[Edit Ethernet Controller] ウィンドウが表示されます。

ステップ 5 ドロップダウンリストから [Squelch Mode] を選択します。

ステップ 6 [Hold Off Timer] に値を入力します。

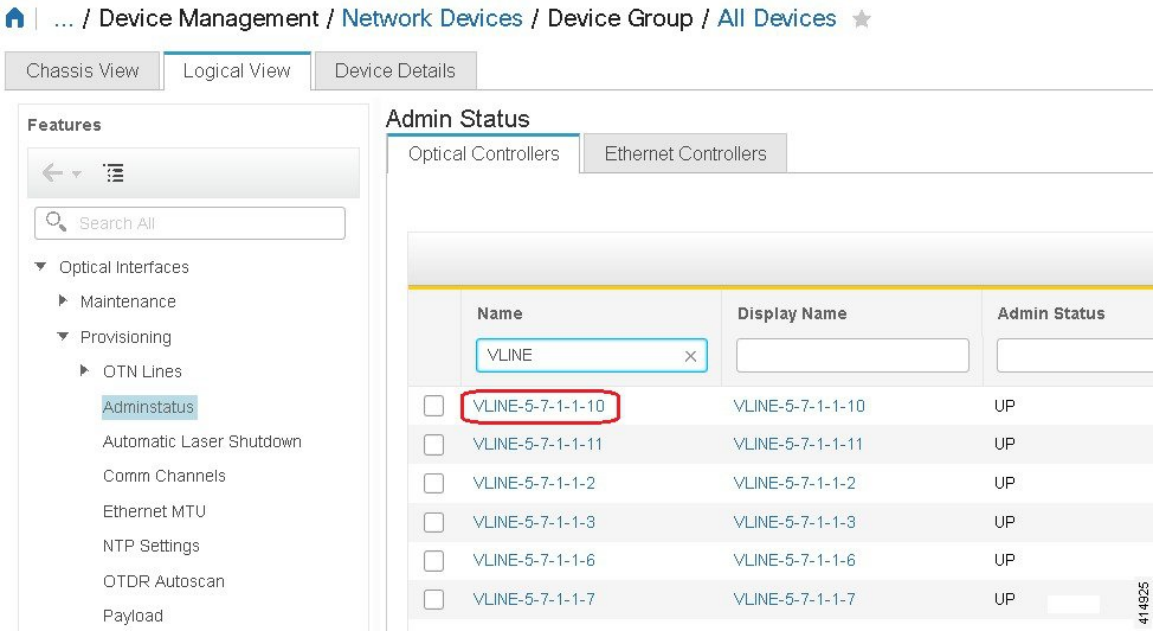
ホールドオフ時間の範囲は、0 ～ 3000 ミリ秒です。

ステップ 7 [Apply] をクリックします。

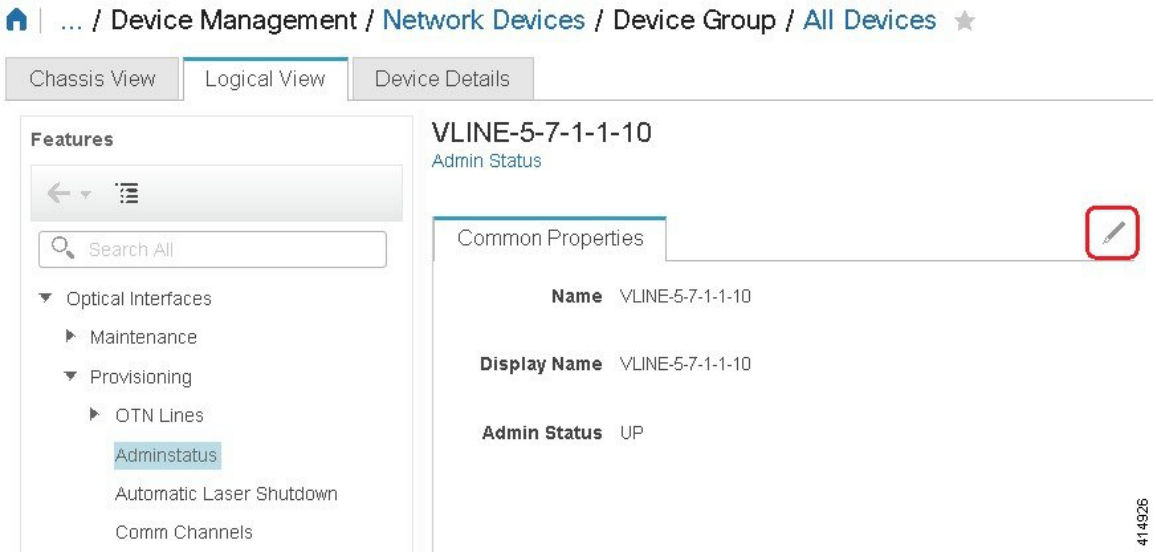
例：Cisco NCS 2006 インターフェイスの管理ステータスの変更

この例では、Cisco NCS 2006 VLINE インターフェイスの管理ステータスを変更する方法を示します。この例では、設定の変更は [デバイスの詳細（Device Details）] ページから開始されますが、[論理ビュー（Logical View）] タブの下にあります（その他のデバイスでは、[設定（Configuration）] タブで設定の変更が実行されます）。

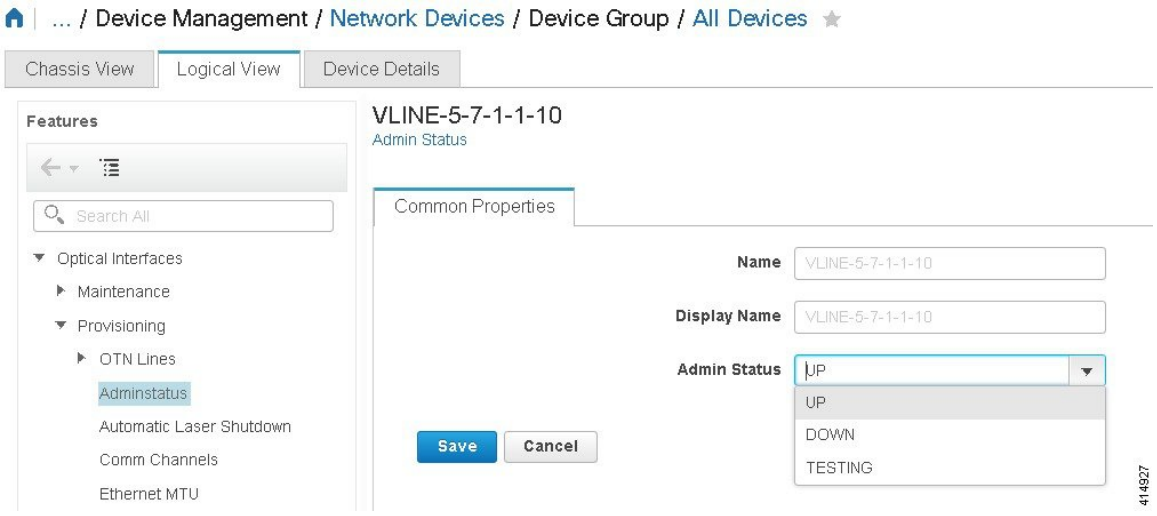
ステップ 1 [論理ビュー（Logical View）] タブの [デバイスの詳細（Device Details）] ページで、編集するインターフェイスのハイパーリンクをクリックします。



ステップ 2 インターフェイスの [共通プロパティ（Common Properties）] ウィンドウで、ウィンドウの右上隅にある [編集（Edit）] アイコンをクリックします。



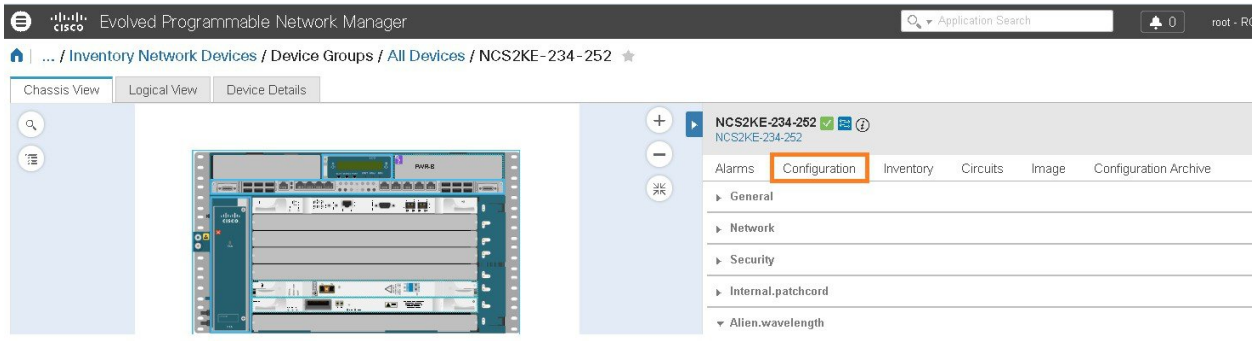
ステップ 3 [管理ステータス（Admin Status）] ドロップダウン リストから新しい設定を選択し、[保存（Save）] をクリックします。



シャーシ ビューを使用したデバイスの設定

デバイスのシャーシ ビューからデバイスとカードを設定できます。これは、シャーシ ビューの [設定（Configuration）] サブタブからのみ実行できます。サブタブは、[ネットワーク デバイス（Network Devices）] ページで選択したデバイスのタイプに応じて表示されます。

（注） この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみ使用できます。



ステップ 1 左側のサイドバーから、**[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシ ビュー（Chassis View）] タブが表示されます。

ステップ 3 右側のペインで、[設定（Configuration）] サブタブをクリックします。

ステップ 4 [全般（General）] 領域を展開した後、ノード名、ノード エイリアスなどのデバイスの詳細を入力し、デバイスをプロビジョニングする場所を選択します。

ステップ 5 デバイスが関連付けられているコントローラと同期するためのデバイスの同期時間を設定します。NTP/SNTP サーバーの時刻を使用するか、または同期用に手動の日付と時刻を設定できます。

ステップ 6 デバイスの冷却プロファイルを手動で変更するには、[手動冷却を有効にする（Enable Manual Cooling）] チェック ボックスをオンにします。冷却プロファイルを使用すると、デバイスのシェルフのファンの速度を制御できます。

ステップ 7 [適用（Apply）] をクリックします。設定の変更が更新されます。

ステップ 8 [ネットワーク（Network）] を展開し、変更するネットワーク設定を選択し、[ネットワーク（Network）] 領域の左上にある [編集（Edit）] アイコンをクリックします。[ネットワークの全般設定の編集（Edit Network General Settings] ウィンドウが表示されます。

ステップ 9 必要な設定を変更し、[適用（Apply）] をクリックします。

（注） デバイスのノード アドレス、ネット/サブネットマスクの長さ、マスク、および MAC アドレスは変更できません。

ステップ 10 デバイスのセキュリティを設定します。デバイスのユーザーおよびユーザー ログインの作成と管理（479 ページ）を参照してください。

ステップ 11 デバイスの送信側（TX）と受信側（RX）のパッチコードを設定します。デバイスのパッチコードの設定（480 ページ）を参照してください。

ステップ 12 デバイスの異種波長を設定します。GMPLS および WSON のプロパティの構成 （493 ページ） を参照してください。

デバイスのユーザーおよびユーザー ログインの作成と管理

この手順を使用してユーザーを作成し、デバイスを管理するロールを割り当てます。また、一度にデバイスにアクセスしているユーザーのリストを表示することもできます。

ステップ 1 左側のサイドバーから、**[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシ ビュー（Chassis View）] タブが表示されます。

ステップ 3 右側のペインで、[設定（Configuration）] サブタブをクリックし、[セキュリティ（Security）] 領域を展開します。

ステップ 4 [ユーザー（User）] タブで、[+] アイコンをクリックしてユーザーを追加します。

ステップ 5 ユーザー名を入力します。

ステップ 6 [セキュリティ レベル（Security Level）] ドロップダウン リストから、次のオプションのいずれかを選択します。

- [レトリーバ（Retriever）]：このセキュリティ レベルのユーザーは、デバイスから情報を表示および取得できますが、設定を変更することはできません。

- [メンテナンス（Maintenance）]：このセキュリティ レベルを持つユーザーはデバイスから情報を取得して、カードのリセット、相互接続または保護グループ内での手動/強制/ロックアウト、BLSR メンテナンスなどの限られた保守操作を実行できます。
- [プロビジョニング（Provisioning）]：このセキュリティ レベルを持つユーザーは、スーパー ユーザーに制限されている操作を除き、すべての保守操作およびプロビジョニング アクションを実行できます。
- [スーパーユーザー（Super User）]：このセキュリティ レベルを持つユーザーは、すべてのプロビジョニング ユーザーのアクションに加え、ユーザー セキュリティ プロファイルの作成と削除、時刻、日付、ノード名、IP アドレスなどの基本的なシステム パラメータの設定、ならびにデータベースのバックアップと復元を実行できます。

ステップ 7 パスワードを入力し、[保存（Save）] をクリックします。ユーザーが [ユーザー（Users）] テーブルに追加されます。

ユーザーを編集または削除するユーザーを選択できます。ただし、ユーザー名は編集できません。また、Cisco EPN Manager にデバイスを追加したユーザーを削除することはできません。

[セキュリティ（Security）] 領域で [ActiveLogins] タブをクリックし、CTC、TL1 セッション、または Cisco EPN Manager を使用してデバイスにログインしたユーザーのリストを表示します。デバイスの最大ログインセッション数に到達すると、1 人のユーザーまたは複数のユーザーをログアウトさせることができます。

デバイスのパッチコードの設定

クライアント カード トランク ポートと DWDM フィルタ ポートは、異なるノードまたは同じ単一シェルフ ノードまたはマルチシェルフ ノードに配置できます。クライアント カード トランク ポートと DWDM フィルタ ポートの間には、仮想リンクが必要です。内部パッチコードは、単一シェルフ ノードまたはマルチシェルフ ノードのいずれかで、DWDM シェルフの 2 つの側面の間に仮想リンクを提供します。ただし、パッチコードには双方向性があり、それぞれの方向が別々のパッチコードとして管理されます。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

この手順では、WDM（波長分割多重化）に ANS（自動ノード設定）を使用して、シャーシ ビューで内部パッチコードを設定する方法を説明します。シャーシ ビューを使用して、これらの内部パッチコードを作成および削除できます。デバイスの送信側（TX）と受信側（RX）のパッチコードを設定するには、次の手順を実行します。

ステップ 1 左側のサイドバーから、**[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシ ビュー（Chassis View）] タブが表示されます。

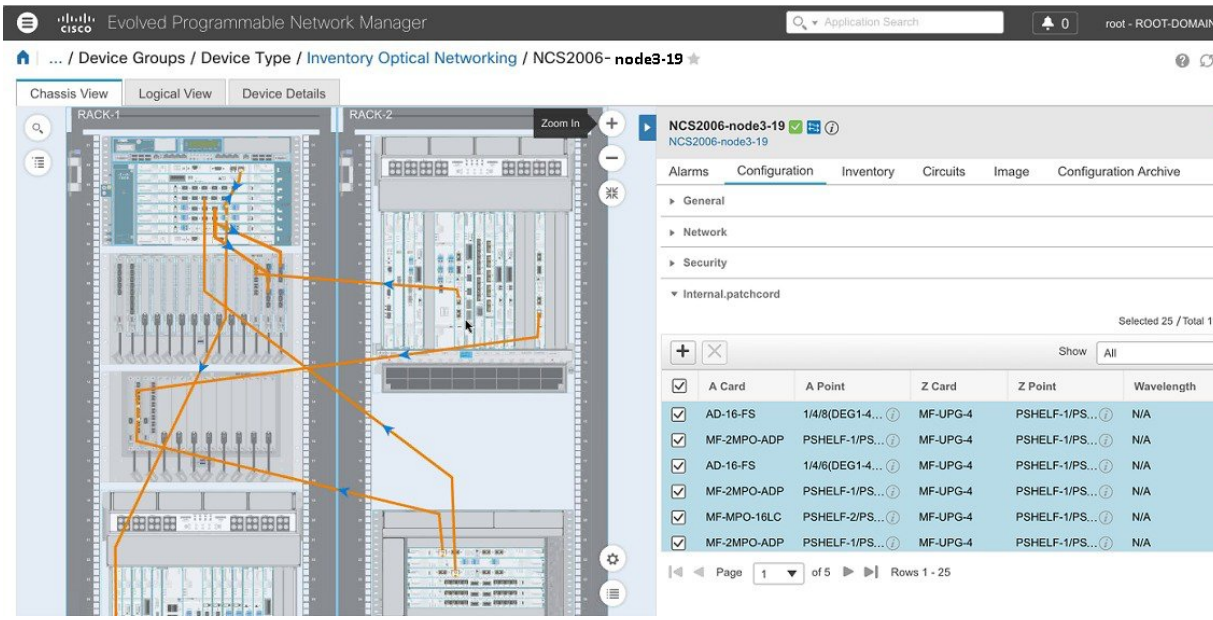
ステップ 3 右側のペインで、[設定（Configuration）] サブタブをクリックし、[Internal.patchcord] 領域を展開します。

ステップ 4 [+] アイコンをクリックした後、デバイスに必要な送信側（TX）と受信側（RX）のパッチコードを選択します。

ステップ 5 [終了（Finish）] をクリックします。パッチコードが [内部パッチコード（Internal Patchcords）] テーブルに追加されます。

（注） パッチコードはいったん作成したら、変更することはできません。ただし、削除できます。

[内部パッチコード（Internal Patchcords）] テーブルで 1 つのパッチ コードまたは複数のパッチコードを選択し、左側のペインに表示されるデバイスのシャーシ ビューにパッチコードの方向を表示できます（下図参照）。



外部パッチコード

OCH フィルタポートを備えていないデバイスにトランスポンダまたは ITU-T ラインカードを取り付ける場合は、外部パッチコードが必要です。外部パッチコードは、NCS 2000 Cisco Transport Controller のみを使用して設定できます。これらのパッチコードは、EPN Manager に OTS リンクとして表示されます。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

次の手順では、シャーシビューを使用して外部パッチコードを表示する方法について説明します。

ステップ 1 左側のサイドバーから、**[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシ ビュー（Chassis View）] タブが表示されます。

ステップ 3 右側のペインで、[設定（Configuration）] サブタブをクリックし、[メンテナンス（Maintenance）] 領域を展開します。

ステップ 4 [外部パッチコード（External Patchcords）] サブタブをクリックします。

デバイス内のシェルフに対する保護グループの設定

デバイス内のシェルフの保護グループを作成するには、次の手順を実行します。

（注） ラックの保護グループは設定できません。

始める前に

次に、シェルフの保護グループを作成するときの前提条件を示します。

- Y ケーブル保護グループを作成するには、クライアントポートで設定されている同じタイプの 2 枚のカードが同じシェルフに接続されていることを確認します。
- スプリッタ保護グループを作成するには、トランク ポート 3-1 とトランク 4-1 で構成されている少なくとも 1 枚の OTU2XP カードがシェルフに接続されていることを確認します。

ステップ 1 左側のサイドバーから、**[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシ ビュー（Chassis View）] タブが表示されます。

ステップ 3 シャーシ ビュー エクスプローラを展開した後、保護グループを設定するシェルフを選択します。

ステップ 4 右側のペインで、[設定（Configuration）] サブタブをクリックした後、[保護（Protection）] 領域を展開します。

ステップ 5 [+] アイコンをクリックして、[保護グループの作成（Create Protection Group）] ウィンドウを開きます。

ステップ 6 [タイプ（Type）] ドロップダウン リストから、次のいずれかの保護タイプを選択します。

- [スプリッタ（Splitter）]：この保護タイプは、MXPP/TXPP カードを使用する場合にのみ適用されます。これらのカードは、スプリッタ（回線レベル）の保護（通常は TXPP または MXPP トランスポンダ カード上のトランク保護）を提供します。
- [Y ケーブル（Y Cable）]：この保護タイプは、クライアント ポートで構成されている 2 つのトランスポンダまたは 2 つのマックスポンダ カードがデバイス内の同じシェルフに接続されている場合にのみ適用されます。

ステップ 7 シェルフの保護ポートと現用ポートを選択します。

（注） これらのポートは、この手順の冒頭に記載されている前提条件を満たしている場合にのみ選択できます。

ステップ 8 保護タイプに単方向か、双方向かのいずれかを選択します。双方向モードでは、アクティブインターフェイスで障害が発生すると、アクティブ インターフェイスから保護/バックアップ インターフェイスへのトラフィックの切り替えがトリガーされます。

ステップ 9 [元に戻す（Revertive）] トグル オプション ボタンをクリックして、障害が修正された後にシェルフを保護ポートから元のポートに戻します。

ステップ 10 保留時間をミリ秒単位で選択します。保留時間は、障害が修正された後に元のポートに切り替えられるまで、保護ポートのシェルフが待機する必要がある時間です。保留時間が経過すると、シェルフは元のポートに戻ることができます。保留時間の最小値は 0.5 である必要があります。

ステップ 11 [適用（Apply）] をクリックします。保護グループが [保護（Protection）] テーブルに追加されます。

ラインカードの動作モードの設定

NCS 1004 デバイスの NCS1K4-OTN-XP カードの動作モードを設定し、ラインカードをアクティブまたは非アクティブにするには、次の手順を実行します。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、**シャーシ ビュー**を起動します。

ステップ 2 右側に表示されるウィンドウで [設定（Configuration）] タブをクリックします。

ステップ 3 **[ラインカードの動作モード（Line Card Operating Mode）]** サブタブを展開します。

ステップ 4 ラインカードの動作モードを編集するには、カードの動作モードを選択して **[編集（Edit）]** をクリックします。

ステップ 5 ドロップダウンリストから **[カード動作モード（Card Operating Mode）]** を選択し、**[アクション（Action）]** ドロップダウンリストから目的のアクションを割り当てます。

ステップ 6 **[適用（Apply）]** をクリックして変更内容を展開します。

スライスの設定

Cisco EPN Manager を使用すると、クライアント ポートとトランク ポートのビットレートを制御し、各スライスの FEC と暗号化のタイプを設定することでスライスを設定できます。

スライスの 5 つのクライアント ポートを同じビットレートで設定する必要があります。また、トランク ポートは両方とも常に同じ FEC モードに設定してください。

（注） スライスの設定は現在、Cisco NCS 1002 および NCS 1004 デバイスでのみサポートされています。

NCS 1002 デバイスのスライスの設定

Cisco NCS 1002 デバイスのスライスを設定するには、次の手順を実行します。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、**シャーシ ビュー**を起動します。

ステップ 2 右側に表示されるウィンドウで [設定（Configuration）] タブをクリックします。

ステップ 3 [スライスの設定（Slice Configuration）] サブタブを展開します。

ステップ 4 新しいスライスの設定を追加するには、[+]（追加）ボタンをクリックし、次の詳細を指定します。

スライス設定パラメータ	説明
スライス番号	スライス ID を表す数値。スライスごとに作成できる設定セットは 1 つのみです。
クライアント ビットレート	スライスのクライアントポートで設定するビット/秒（ギガビット/秒単位）の合計数。
トランク ビットレート	スライスのトランク ポートで設定するビット/秒（ギガビット/秒単位）の合計数。
FEC	トランク ポートに設定する FEC 値。 FEC モード設定を変更する前に、変更しようとしているインターフェイスの管理状態が [ダウン（故障中）（Down (out of service)）] で、G709 の設定が有効になっていることを確認してください。
暗号化（Encryption）	暗号化されたトラフィックまたは暗号化されていないトラフィックで機能するようにスライスを設定します。

ステップ 5 [適用（Apply）] をクリックして、変更をすぐにデバイスに展開します。

スライスごとに追加できるパラメータのセットは 1 つだけで、一度保存するとすべてのパラメータが編集できなくなります。パラメータを編集するには、スライスの設定を削除してからもう一度追加します。

（注） 管理状態が [動作中（UP）] の場合、スライス設定は削除できません。

NCS 1004 デバイスのスライスの設定

NCS1004 デバイスのスライスを設定するには、次の手順を実行します。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、**シャーシ ビュー**を起動します。

ステップ 2 [シャーシエクスプローラ（Chassis Explorer）] から、設定するスロットを選択します。

ステップ 3 右側に表示されるウィンドウで [設定（Configuration）] タブをクリックします。

ステップ 4 [スライスの設定（Slice Configuration）] サブタブを展開します。

ステップ 5 [カードモード（Card Mode）] ドロップダウンリストから、適切なオプションを選択します。

使用可能なオプションは、[Slice Mode]、[Muxponder Mode]、および [Regen Mode] です。

ステップ 6 新しいスライスの設定を追加するには、[+]（追加）ボタンをクリックし、次の詳細を指定します。

スライス設定パラメータ	説明
スライス番号	スライス ID を表す数値。この値は、NCS 1004 デバイスでは変更できません。
クライアント ビットレート	スライスのクライアントポートで設定するビット/秒（ギガビット/秒単位）の合計数。選択可能なオプションは、[100GE] および [OTU4] です。[100GE] は、[スライスモード（Slice Mode）] と [マックスポンダモード（Muxponder Mode）] の両方に適用されます。[OTU4] は [マックスポンダモード（Muxponder Mode）] にのみ適用されます。
トランク ビットレート	スライスのトランク ポートで設定するビット/秒（ギガビット/秒単位）の合計数。 （注） [Regen Mode] の場合、[Trunk Bitrate] は設定にのみ適用されます。
MAC アドレススヌーピング	有効にすると、隣接する MAC アドレスが表示されます。

ステップ 7 [適用（Apply）] をクリックして、変更をすぐにデバイスに展開します。

スライスごとに追加できるパラメータのセットは 1 つだけで、一度保存するとすべてのパラメータが編集できなくなります。パラメータを編集するには、スライスの設定を削除してからもう一度追加します。

（注） 管理状態が [動作中（UP）] の場合、スライス設定は削除できません。

[デバイスの詳細（Device Details）] ページからのインターフェイスの設定

[デバイスの詳細（Device Details）] ページからインターフェイスを設定するには、次の手順を実行します。

ステップ 1 デバイスのシャーシ ビューを開いて、[設定の起動（Launch Configuration）] リンクをクリックします。

[デバイスの詳細（Device Details）] ページが開きます。

ステップ 2 [論理ビュー（Logical View）] タブをクリックします。

ステップ 3 [機能（Features）] ウィンドウで、[インターフェイス（Interfaces）] > 設定するインターフェイスのタイプを選択します。

ステップ 4 選択したインターフェイス タイプに固有の手順を実行してインターフェイスを追加または編集します（インターフェイスの設定 （442 ページ）を参照）。

Cisco NCS 1000 インターフェイス設定の更新

Cisco NCS 1000 シリーズ デバイスに設定されてインターフェイスの [管理ステータス（Admin Status）]、[波長（nm）（Wavelength (nm)）]、および [ループバック（Loopback）] の設定は [デバイスの詳細（Device Details）] ページからすばやく更新できます。これを行うには、次の手順を実行します。

ステップ 1 完全なデバイス情報の取得：[デバイスの詳細（Device Details）] ページ （113 ページ）の説明に従って、Cisco NCS 1000 シリーズ デバイスの [デバイスの詳細（Device Details）] ページを開きます。

ステップ 2 [設定（Configuration）] タブをクリックします。

ページが更新され、3 つのサブタブ（[光学（Optics）]、[イーサネット（Ethernet）]、および[コヒーレント DSP（Coherent DSP）] が表示されます。

ステップ 3 更新するインターフェイスのタイプのサブタブをクリックします。

ステップ 4 必要な変更を加えます。

方法 1

1. [インターフェイス（Interfaces）] テーブルで、更新するインターフェイスを見つけます。
2. 変更するパラメータをクリックして、ドロップダウン リストを開きます。
3. 設定する値を選択し、[保存（Save）]をクリックします。

方法 2

1. 更新するインターフェイスのオプション ボタンをクリックし、鉛筆 （[編集（Edit）]）アイコンをクリックします。

   [インターフェイス タイプの編集（Edit Interface Type）] ダイアログボックスが開きます。
2. 使用可能なドロップダウン リストから設定する値を選択し、[適用（Apply）] をクリックします。
3. [OK] をクリックして、変更内容を確定します。

次の点に注意してください。

- 光学インターフェイスの場合：
  - [管理ステータス（Admin Status）] と [波長（nm）（Wavelength (nm)）] パラメータを更新できます。
  - 新しい波長値を設定できるのは、[光学タイプ（Optics Type）] パラメータが [DWDM] に設定されている場合のみです。
- コヒーレント DSP およびイーサネット インターフェイスの場合：
  - [管理ステータス（Admin Status）] と [ループバック（Loopback）] パラメータを更新できます。
  - 新しいループバック値を設定できるのは、[管理者ステータス（Admin Status）] パラメータが [テスト中（Testing）] に設定されている場合のみです。

- [ループバック（Loopback）] パラメータを [回線（Line）] に設定すると、Cisco EPN Manager はファシリティループバックに適用されるのと同じ設定を適用します。ファシリティループバックは、カードの回線インターフェイスユニット（LIU）、電気インターフェイスアセンブリ（EIA）、および関連するケーブル配線をテストします。
- [ループバック（Loopback）] パラメータを [内部（Internal）] に設定した場合、Cisco EPN Manager は端末ループバックに適用されるのと同じ設定を適用します。

コントローラ（光学、OTS、OCH、DSP、および DWDM）の設定

Cisco EPN Manager を使用すると、波長、FEC、SD、SF BER のレポートとしきい値などの光デバイスコントローラのパラメータを、OTS、OTS OCH、DWDM などのタイプのコントローラに設定できます。

光トランスポート セクション（OTS）コントローラは、OTS 光インターフェイスのすべての光パラメータを保持します。光インターフェイスは、VOA や増幅器などのハードウェア コンポーネントに応じて異なる機能を備えています。したがって、OTS コントローラで有効または無効にするパラメータは、特定の光インターフェイスの実際のハードウェア機能によって異なります。OTS コントローラの増幅器のゲイン範囲、増幅器チルト、光安全性リモートインターロック（OSRI）などのパラメータを設定できます。

光トランスポート セクション OCH（OTS OCH）コントローラは、OTS 光インターフェイスで使用可能な OCM デバイスを表します。このコントローラは、OTS インターフェイス上のチャネルの粒度を持ちます。OTS OCH コントローラには波長情報が含まれています。OTS OCH コントローラの管理ステータスのみを設定できます。

コントローラを設定する前にスライス設定の完了を確認するには、NCS 1002 デバイスのスライスの設定 （484 ページ）を参照してください。

光コントローラのパラメータを設定するには、次の手順を実行します。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、**シャーシ ビュー**を起動します。

ステップ 2 右側に表示されるウィンドウで [設定（Configuration）] タブをクリックします。

ステップ 3 [コントローラ（Controllers）] サブタブを展開します。デバイスの選択に応じて、サポートされているタブが表示されます。

ステップ 4 光コントローラの設定を編集するには、[光学（Optics）] をクリックし、必要な設定を選択して [変更（Modify）] アイコンをクリックし、変更を加えます。

ステップ 5 OTS コントローラの設定を編集するには、[OTS] をクリックし、必要な設定を選択して [変更（Modify）] アイコンをクリックし、変更を加えます。

ステップ 6 OTS-OCH コントローラの設定を編集するには、[OTS-OCH] をクリックし、必要な設定を選択して [変更（Modify）] アイコンをクリックし、変更を加えます。

ステップ 7 コヒーレント DSP の設定を編集するには、[コヒーレント DSP（Coherent DSP）] をクリックし、必要な設定を選択して [変更（Modify）] アイコンをクリックし、変更を加えます。

（注）　トランスポート管理ステータスが IS に設定されている場合はパラメータを編集できません。

ステップ 8　DWDM コントローラの設定を編集するには、[DWDM] をクリックし、必要な設定を選択して [変更（Modify）] アイコンをクリックし、変更を加えます。

カテゴリ	パラメータ	説明
一般的な光学、OTS-OCH、DSP、および DWDM のコントローラパラメータ	• 名前（Name） • 管理ステータス（Admin Status） • 動作ステータス（Operational Status） • トランスポート管理ステータス（Transport Admin Status）	[名前（Name）]：（表示のみ）ポート番号を表示します。 [管理ステータス（Admin Status）]：インターフェイスが管理対象（動作中）かダウンか、またはメンテナンスモードかを定義します。インターフェイスのステータスが [動作中（Up）] の場合、コントローラのプロパティは変更できません。 [動作ステータス（Operational Status）]：インターフェイスが動作可能で、プロビジョニング済みとして実行されているかどうかを定義します。 [トランスポート管理ステータス（Transport Admin Status）]：コントローラのトランスポート管理状態を定義します。
一般的な光学および DWDM のパラメータ	実波長（nm）（Actual Wavelength (nm)）	チャネルで使用する実際の波長を表示します。
-	波長（nm）（Wavelength (nm)）	チャネルで設定された波長値を表示します。デバイスインベントリ収集ステータスが [完了（Completed）] になると、[実波長（Actual Wavelength）] と [波長（Wavelength）] の値が一致します。
-	FEC モード（FEC Mode）	コントローラで設定する FEC 値。 FEC モード設定を変更する前に、変更しようとしているインターフェイスの管理状態が [ダウン（故障中）（Down (out of service)）] で、G709 の設定が有効になっていることを確認してください。
光パラメータ	速度（Speed）	コントローラが動作する必要がある速度値（ギガビット/秒）を設定します。
-	DAC レート	ドロップダウンリストから DAC レートを選択します。
-	最小波長分散	最小波長分散値を入力します。
-	最大波長分散	最大波長分散値を入力します。
-	設定される送信電力	送信電力を入力します。
-	変調タイプ	ドロップダウンリストから変調タイプを設定します。

カテゴリ	パラメータ	説明
-	差分変調（Differential Modulation）	設定された速度値に基づいて、差分エンコーディング（DE）を有効または無効にします。
-	ループバック（Loopback）	ループバックを次のように設定します。 • [内部（Internal）]：すべてのパケットがルータの内部でループバックされてから外部インターフェイスに到達します。内部 Rx から Tx へのパスをテストし、物理ポートから出力するトラフィックを停止します。 • [回線（Line）]：着信ネットワーク パケットが外部インターフェイスを通じてループバックされます。
-	SD BER	信号劣化ビット エラー レートを設定します。オプションは、E-5、E-6、E-7、E-8、または E-9 です。
-	SF BER	信号障害ビット エラー レートを設定します。オプションは E-3、E-4、または E-5 です。
DWDM パラメータ	ループバック（Loopback）	ループバックを次のように設定します。 • [内部（Internal）]：すべてのパケットがルータの内部でループバックされてから外部インターフェイスに到達します。内部 Rx から Tx へのパスをテストし、物理ポートから出力するトラフィックを停止します。 • [回線（Line）]：着信ネットワーク パケットが外部インターフェイスを通じてループバックされます。
-	• OTU-SD • OTU-SF • ODU-SD • ODU-SF	SF（信号障害）と SD（信号劣化）の BER レポートとしきい値の設定 アラームが OTU アラームか ODU アラームかに応じて、アラームは SM BER が SD BER しきい値または SF BER しきい値に基づいて超過していることを表します。
OTS パラメータ	ポート ロール（Port Role）	ポートの現在の動作状態。 保護スイッチの場合、通信の作業ロールが表示されますが、増幅器モジュールの場合は [通信回線/OSC（Com Line/Osc）] ロールまたは [通信確認（Com Check）] ロールが表示されます。
-	Rx/Tx 下限しきい値（dBm）（Rx/Tx Low Threshold (dBm)）	受信者/トランスポンダの下限受信電力しきい値を設定します。有効な範囲は -500 ～ 300 です。

カテゴリ	パラメータ	説明
-	増幅器チャネル電力（dBm）（Ampli Channel Power (dBm)）	チャネル電力設定ポイントごとに増幅器を設定します。有効な範囲は -500 ～ 300 です。デフォルト値は 0.0 です。
-	チャネル電力最大デルタ（dBm）（Channel Power Max Delta (dBm)）	測定されたすべてのチャネル電力間の最大差異を設定します。有効値は 0 ～ 200 です。
-	増幅器ゲインと増幅器ゲインの範囲（Ampli Gain and Ampli Gain Range）	増幅器ゲイン設定ポイントを設定します。この範囲の有効モードは [通常（Normal）] または [拡張（Extended）] です。 （注） 増幅器ゲインの範囲は、コントローラがシャットダウン状態にある場合にのみ設定できます。
-	増幅器安全性コントローラ モード（Ampli Safety Controller Mode）	安全制御モードを [自動（Auto）] または [無効（Disabled）] に設定します。
-	OSRI	光安全性リモート インターロックを [オン（On）] または [オフ（Off）] に設定します。
-	増幅器チルト（Ampli Tilt）	-50 ～ +50 の数値を使用して増幅器チルトを設定します。

（注） IOS-XR（RON）光コントローラの編集画面に表示される値は、デバイスの実行コンフィギュレーションです。

光コントローラの [DAC レート（DAC Rate）]、[FEC]、および [変調方式（Modulation Type）] 属性に対して [設定しない（Not Set）] が選択されている場合、EPNM はデバイスから既存の構成を削除し、GI が完了するとそれらの属性の動作値をユーザーインターフェイスに表示します。

ステップ 9 [適用（Apply）] をクリックして、変更内容をデバイスにすぐに展開します。

ステップ 10 （オプション）DWDM グリッド値の単位を波長または周波数に変更するには、[管理者（Administrator）] > [設定（Settings）] > [システム設定（System Settings）] > [回線/VC 表示（Circuits/VCs Display）] に移動し、[DWDM グリッド単位（DWDM Grid Unit）] 領域で [波長（ナノメートル（nm））（Wavelength (Nanometer (nm)）] または [周波数（テラヘルツ派（THz））（Frequency (Tatrahertx (THz))）] のいずれかを選択します。

パッシブ ユニットの設定

パッシブ ユニットは、光デバイス用に Cisco EPN Manager を使用してプロビジョニングされたパッシブカードです。Cisco EPN Manager はこれらのパッシブ ユニットをデータベースに保持し、デバイスには展開しません。設定が完了したら、これらのパッシブ ユニットを [デバイスの詳細（Device Details）] ページと [インベントリ（Inventory）] ページで表示し、それらを使用してネットワーク トポロジで管理対象リンクを作成できます。

（注） パッシブ ユニットの設定は現在、Cisco NCS 1001 デバイスでのみサポートされています。

パッシブ ユニットを追加または削除するには、次の手順を実行します。

始める前に

このタスクを実行する前に、「管理者」または「設定マネージャ」のユーザー権限があることを確認します。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、**シャーシ ビュー**を起動します。

ステップ 2 右側に表示されるウィンドウで [設定（Configuration）] タブをクリックします。

ステップ 3 [パッシブ ユニット（Passive Units）] サブタブを展開します。

ステップ 4 パッシブユニットを追加するには、[追加（Add）]（+）アイコンをクリックし、次の詳細を指定します。

- 機器 ID：パッシブ ユニットの一意の識別子を選択します。デバイスごとに最大 9 つのパッシブ ユニットを追加できます。
- 機器のタイプ：スロットが 48 チャネル マックスポンダ/でマックスポンダとしてプロビジョニングされるか、ODD/EVEN ユニットとしてプロビジョニングされるかを決定する機器のタイプを選択します。オプションは[CME]、[ODDE]、および [EVENE] です。
- （オプション）シリアル番号：各パッシブユニットに固有のシリアル番号。Cisco EPN Managerは、この構成をデバイスに展開せず、データベースにのみ保持します。

ステップ 5 [適用（Apply）] をクリックして変更内容をデバイスに展開します。

ステップ 6 （オプション）パッシブ ユニットが正常に作成されたことを確認するには、[インターフェイス（Interfaces）] タブまたは [デバイスの詳細（Device Details）] タブに移動し、[インターフェイス名（Interface Name）] フィルタを使用してパッシブ ユニットを見つけます。

パッシブ ユニットに使用される命名規則は次のとおりです。

PUnit<number of the card> <equipment ID of the passive unit>

たとえば、*PUnit/1/16* などです。

ステップ 7 パッシブ ユニットの設定を編集するには、それらの設定を削除し、同じ機器 ID を使用して詳細を再度設定します。

ステップ 8 パッシブユニットを削除するには、必要なパッシブユニットを選択し、[削除（Delete）]（X）アイコンをクリックします。リンクに関連付けられているパッシブ ユニットも削除できます。これにより、リンクが [部分的（Partial）] 状態に切り替わします。

ステップ 9 （オプション）同じ値を持つ複数のパッシブユニットを照合するには、必要なパッシブユニットを選択し、[照合（Match）]をクリックします。ドロップダウンリストからシミュレートされたパッシブユニット番号を選択し、[適用（Apply）] をクリックします。

ステップ 10 （オプション）これらのパッシブポートを使用して手動リンクを設定するには、ネットワークトポロジに移動し、トポロジ マップへのリンクの手動による追加 （228 ページ）従って、リンクを作成します。

光ケーブルでの増幅器モジュール設定の編集

グリッドモード、ノードタイプ、およびUDC VLANの設定を変更することで、デバイスの光スロットに挿入されている増幅器モジュールの設定を変更できます。

増幅器モジュール設定を編集するには、次の手順を実行します。

始める前に

このタスクを実行する前に、「管理者」または「設定マネージャ」のユーザー権限があることを確認します。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、**シャーシ ビュー**を起動します。

ステップ 2 右側に表示されるウィンドウで [設定（Configuration）] タブをクリックします。

ステップ 3 [増幅器モジュール設定（Amplifier Module Settings）] サブタブを展開します。

ステップ 4 編集する設定を選択し、[編集（Edit）] アイコンをクリックして次のパラメータを指定します。

- [グリッドモード（Grid Mode）]：増幅器モジュールのインターフェイス上の光スペクトルを定義します。
- [ノードタイプ（Node Type）]：増幅器が動作するように設定するノードのタイプを定義します。オプションは、[端末（Terminal）]、[回線（Line）]、および [設定なし（Not Set）] です。
- [UDC VLAN]：選択したスロットとその UDC ポートに関連付けられている VLAN を定義します。

（注） 指定したUDC VLANがデバイス上で一意であることを確認します。重複する値はサポートされていません。

ステップ 5 [適用（Apply）] をクリックして変更内容をデバイスに展開します。

ステップ 6 （オプション）イーサネットコントローラを設定するには、[イーサネット（Ethernet）]サブタブを展開します。編集するコントローラを選択し、[編集（Edit）] アイコンをクリックし、必要な変更を加えます。[適用（Apply）] をクリックして、変更内容をデバイスに保存します。

GMPLS および WSON のプロパティの構成

GMPLS UNI：

Generalized Multiprotocol Label Switching（GMPLS）ユーザー ネットワーク インターフェイス（UNI）は、光ネットワーク内の 2 台のクライアント（UNI-C）間の回線接続を作成します。この接続は、UNI-C ノードがルータノードであり、UNI-N ノードが光ノードである、UNI クライアント（UNI-C）と UNI ネットワーク（UNI-N）ノード間の信号交換によって実行されます。

GMPLS UNI は、Cisco NCS 1002 ノードの 100G および 200G トランク ポートでのみサポートされています。OCH トレイル回路の前提条件は、NCS 2000 シリーズ ノードの光チャネル アド/ドロップ NCS 2000 シリーズインターフェイスと NCS 1002 ノードの NCS 1002 インターフェイス間にリンク管理プロトコル（LMP）リンクを作成することです。

UNI はクライアント（UNI-C）とネットワーク（UNI-N）のロールに分割されます。UNI-C ネットワーク要素は、回線プロビジョニング情報を要求して受け入れます。UNI-N ネットワーク要素は、UNI-C ノードに隣接するノードであり、コアネットワーク全体の回線プロビジョニング情報を受け入れ、転送します。

UNI 回線プロビジョニングの場合、ネットワークは次の要件を満たしている必要があります。

- NE は UNI-C として設定され、UNI-N NE に接続されている必要があります。
- NE は UNI-N として設定され、UNI-C NE に接続されている必要があります。

静的 UNI：

リンク管理プロトコル（LMP）は、トンネルの送信元ノードと宛先ノードのトランク光コントローラ上に作成される論理リンクです。2 つの異なるデバイスのポート間に静的 LMP リンク（静的 UNI）を作成できます。たとえば、Cisco NCS 2000 シリーズ ノードと Cisco NCS 1002 ノードの間などです。これは、GMPLS UNI トンネルの LMP ネイバーの設定に役立ちます。

Cisco EPN Manager を使用して静的 UNI を設定し、RX ポートと TX ポートを選択して、UNI に参加するカード、シェルフ、またはスロットを識別します。RX ポートは UNI の送信元を表し、TX ポートは宛先を表します。

[リモート デバイス（Remote Device）] フィールドを使用して、選択したノードの管理 IP アドレスを指定します。[リモート クライアント インターフェイス（Remote Client Interface）] フィールドを使用して、光学コントローラの LMP リンク IP アドレスを選択します。

異種波長：

[異種波長（Alien Wavelength）] タブを使用して、異種波長のポートと波長パラメータを表示および設定します。また、必要な異種波長のタイプ、トランクモード、および前方誤り訂正（FEC）モードを指定することもできます。

光ファイバ属性：

GMPLS UNI の作成時に使用するパラメータを光ファイバのタイプ（分散シフト（DS）、True-Wave Classic（TWC）、またはその他の値を選択）などの値を設定することで設定できま

す。また、光ファイバの長さを指定し、偏光モード分散ファイバ係数を指定することもできます。

[減衰器入力（Attenuator In）] の値は、ノード出力ポート（LINE-TX ポートなど）と光ファイバの入力パラメータ間での入力光減衰（dB 単位）を識別します。同様に、[減衰器出力（Attenuator Out）] の値は、ノード入力ポート（LINE-RX ポートなど）と光ファイバの出力パラメータ間での入力光減衰（dB 単位）を識別します。

光グリッド内の2つの隣接チャネル間の最小周波数間隔を設定するチャネル間隔値を選択できます。スパンで予測される最大チャネル数を指定するには、[チャネル番号（Channel Number）] フィールドを使用し、チャネル番号とチャネル間隔の値が一致していることを確認します。たとえば、100 GHz 間隔を持つ 80 個のチャンネルは存在できません。

仮想トランク：

[仮想トランク（Virtual Trunk）] タブを使用して、デバイスの [ドロップポート（Drop Port）]、[説明設定（Description Configuration）]、[TXP制御モード（TXP Control Mode）]、および [異種波長タイプ（Alien Wavelength Type）] を指定できます。

LMP の終了：

[LMP の終了（LMP Termination）] タブを使用して、デバイスの [仮想トランク（Virtual Trunk）]、[LMP タイプ（LMP Type）]、[リモートデバイス（Remote Device）]、[リモートインターフェイス（Remote Interface）]、および [ピアリング（Peering）] を指定できます。また、[LMP の終了（LMP Termination）] タブで既存の LMP の終了を編集することもできます。

GMPLS/WSON パラメータを設定するには、次の手順を実行します。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、**シャーシ ビュー**を起動します。

ステップ 2 右側に表示されるウィンドウで [設定（Configuration）] タブをクリックします。

ステップ 3 これらのパラメータを設定するには、次の表に示すパスに移動します。

タスク	ナビゲーション	説明
ファイバ属性の設定	[GMPLS/WSON] サブタブ > [ファイバ属性（Fiber Attributes）]	ファイバ側、タイプ、長さ、検証、チャネル間隔、チャネル番号、およびドメインの値を指定します。減衰器（入力と出力）の値を指定することもできます（オプション）。
静的 UNI の作成と編集	[GMPLS/WSON] サブタブ > [静的 UNI（Static UNI）]	• UNI に参加する必要がある RX ポートと TX ポートのリモートコントローラを追加します。 • [リモートデバイス（Remote Device）] フィールドは、ノードの管理 IP アドレスを指定します。 • [リモート クライアント インターフェイス（Remote Client Interface）] フィールドは、コントローラのリンク IP アドレスを指定します。 （注） 上記の設定を使用して、リモート TXP ノードを設定できます。

タスク	ナビゲーション	説明
GMPLS UNI の作成と編集	[GMPLS/WSON] サブタブ > [GMPLS UNI（GMPLS UNIs）]	• GMPLS UNI の入力ポートと出力ポートを指定し、UNI が番号付けされているタイプか、番号なしタイプかを選択します。UNI が UNI-C タイプか UNI-N タイプかを必ず指定してください。 • トランク値は、GMPLS UNI の設定に応じて、それぞれの異種波長値に自動的に設定されます。設定された異種波長が両方のトランク ポートでサポートされている場合は、トランク ポートの 1 つに設定すると、両方のトランク ポート上に同じ異種波長が自動的に設定されます。 • Cisco NCS 2000 デバイスの場合、GMPLS UNI トランク値はデフォルトに設定できます。 • ローカルおよびリモート システムの IP と、リモート システムの IP およびコントローラを指定します。これらの値を指定すると、UNI のリモート システム接続が有効になります。 （注） Cisco EPN Manager で管理されるデバイスのリモート システム IP のみを指定できます。
異種波長パラメータの設定：	[GMPLS/WSON] サブタブ > [異種波長（Alien Wavelength）]	必要な異種波長のタイプ、トランクモード、およびFECモードを指定します。
仮想トランクの設定および編集	[GMPLS/WSON] サブタブ > [仮想トランク（Virtual Trunk）]	[ドロップポート（Drop Port）]、[説明設定（Description Configuration）]、[TXP制御モード（Txp Control Mode）]（LOCAL および NONE）、および [異種波長タイプ（Alien Wavelength Type）] を指定します。 （注） 説明のみを編集でき、他の属性は編集できません。
LMP の終了の設定と編集	[GMPLS/WSON] サブタブ > [LMP の終了（LMP Termination）]	[仮想トランク（Virtual Trunk）]、[LMP タイプ（LMP Type）]、[リモートデバイス（Remote Device）]、[リモートインターフェイス（Remote Interface）]、および [ピアリング（Peering）] を指定します。 （注） NCS2K デバイスの [LMPタイプ（LMP Type）] が [NoSignal] で、[TXPCONTROLMODE] が [GMPLS] の場合、EPNM UI では、（NCS2K から NCS1004 LMP または NCS2K から NCS4K LMP の場合に）LMP タイプ（検出された LMP）が [信号送信済み（NCS1004）（Signaled (NCS1004)）] と表示されます。

（注） 信号未送信 LMP の場合、コマンドはローカルデバイスにのみプッシュされます。手動で、または設定テンプレートを使用して、リモートデバイスに設定をプッシュする必要があります。

ステップ 4 変更を加えて、[保存（Save）] をクリックします。

ステップ 5 設定後に値を編集するには、値を選択し、ツールバーの [編集（Edit）] アイコンをクリックします。変更を加えて、[保存（Save）] をクリックします。

LMP リンクの作成については、光チャネル（OCH）トレールのユーザー/ネットワーク間インターフェイス（UNI） （616 ページ）を参照してください。

OTS ポートでの光安全性リモートインターロック（OSRI）の有効化または無効化

OTS インターフェイスで設定されたポートの光安全性リモートインターロック（OSRI）ステータスを変更できます。

OSRI を有効または無効にするには、次の手順を実行します。

始める前に

このタスクを実行する前に、「管理者」または「設定マネージャ」のユーザー権限があることを確認します。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、**シャーシ ビュー**を起動します。

ステップ 2 右側に表示されるウィンドウで [設定（Configuration）] タブをクリックします。

ステップ 3 [メンテナンス（Maintenance）] タブを展開し、[OSRI] サブタブをクリックします。

ステップ 4 OSRI を有効または無効にするポートを選択します。

ステップ 5 ドロップダウンリストから、[有効（Enable）] または [無効（Disable）] を選択して OSRI を有効または無効にします。

光カードの設定

- 着脱可能ポート モジュールおよびカード モード設定の編集と削除 （508 ページ）
- Cisco NCS 2000 デバイス用のカードとサポートされる設定 （509 ページ）

シャーシ ビューからカードを設定する

この手順では、シャーシ ビューを使用して、Cisco EPN Manager にカードを追加します。カードを追加したら、そのカードタイプの関連トピック内の手順に従って、それを設定できます。通常は、カードを物理的にスロットに挿入する前に行います。

始める前に

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

ステップ 1 シャーシ ビューを開く （117 ページ）の説明に従って、シャーシ ビューを起動します。

ステップ 2 次のいずれかの操作を実行して、カードを追加するスロットを選択します。

- 物理シャーシ ビューで空のスロットを選択してから、スロット ポップアップ ウィンドウで [カードの追加（Add Card）] リンクをクリックします。
- シャーシ ビュー エクスプローラを使用して空のスロットに移動し、そのスロットの横にある [i] アイコンの上にマウス カーソルを移動してから、情報ポップアップ ウィンドウで [カードの追加（Add Card）] ハイパーリンクをクリックします。

Cisco EPN Manager では、物理シャーシ ビューでスロット強調表示され（それが事前にプロビジョニングされていることを示す）、そのデバイス タイプでサポートされているすべてのカードの一覧が表示されます。

（注） 選択したカードが物理スロット タイプに適切であることを確認します。

ステップ 3 追加するカードを見つけて、[追加（Add）] をクリックします。カードを追加すると、Cisco EPN Manager にステータス メッセージが表示されます。

ステップ 4 カードをすぐに設定するには、ステータス ポップアップ メッセージ内の [今すぐ設定（Configure Now）] をクリックします。そうでない場合は、[無視（Ignore）] をクリックします。

カードの削除

カードを削除すると、Cisco EPN Manager はカードに関連付けられている動作モードの設定を含め、カードに関するすべての情報を削除します。削除したカードを後になって再び追加する際に、この情報は復元されません。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

カードを Cisco EPN Manager から削除するには、次の手順に従います。

始める前に

カードを削除する前に、以下の点を確認してください。

- 関連付けられているペイロード値とカードの動作モードが削除されていること。
- カード上で実行されるアクティブな設定がないこと（カードを再び追加する際に、設定を復元することはできません）。

ステップ 1 「シャーシ ビューを開く （117 ページ）」の説明に従って、シャーシ ビューを起動します。

ステップ 2 次のいずれかの方法で、削除するカードのスロットを選択します。

- 物理シャーシ ビューでスロット内のカードを選択し、表示されるポップアップ ウィンドウ内で [カードの削除（Delete Card）] リンクをクリックします。
- シャーシ ビュー エクスプローラを使用してカードに移動し、カードの横にある「i」アイコンの上にマウスのカーソルを重ね、表示されるポップアップ ウィンドウで [カードの削除（Delete Card）] ハイパーリンクをクリックします。

Cisco EPN Manager の物理シャーシ ビューでは、スロットが強調表示され（プロビジョニング済みであることを意味する）、スロット内のすべてのカードを削除すると、そのスロットはシャーシ ビューで空の状態になります。

カードを削除した後、Cisco EPN Manager によってノードのインベントリ収集が行われます。

カードのリセット

カードをリセットすると、同期操作を実行した場合と同様に、シャーシ内のカード位置が再設定されます。Cisco EPN Manager では設定変更は修正されず、代わりに設定の保存とインベントリ収集のトリガーがされます。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

設定済みのカードをリセットするには：

ステップ 1 「シャーシ ビューを開く （117 ページ）」の説明に従って、シャーシ ビューを起動します。

ステップ 2 次のいずれかの方法で、削除するカードのスロットを選択します。

- スロット内のカードを物理シャーシ ビューから選択し、ポップアップ ウィンドウの [カードのリセット（Reset Card）] リンクをクリックします。
- シャーシ ビュー エクスプローラを使用してカードに移動し、マウス カーソルをカードの横の [i] アイコンの上に置き、ポップアップ ウィンドウの [カードのリセット（Reset Card）] ハイパーリンクをクリックします。

Cisco EPN Manager では、物理シャーシ ビューでスロットが強調表示されます（プロビジョニング済みであることを示します）。カードをリセットすると、同期が実行され、インベントリ収集がトリガーされます。

次のタスク

「カードの設定：400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC （501 ページ）」の説明に従って、カードのプロパティを設定します。

カードの設定：OTU2-XP、MR-MXP、WSE、AR-XPE、AR-XP、AR-MXP、40E-MXP-C、および 40ME-MXP-C

カードの動作モードと接続可能ポート モジュール（PPM）を設定するには、次の手順を実行します。

始める前に

OTU2-XP カードと 40E-MXP-Cカードは、カード動作モードを設定することなく、PPMで直接設定できます。ただし、他のカードのカード動作モードを設定する場合は、シスコ トランスポート コントローラを介して直接この設定を実行できます。

- デバイス同期が完了しており、デバイスのインベントリ収集ステータスが「管理（Managed）」または「完了（Completed）」であることを確認してください。
- PPM を追加または削除するたびに、事後対応型インベントリ収集がトリガーされ、デバイスは同期プロセスを開始します。デバイスにさらに設定変更を展開する前に、事後対応型インベントリの収集が完了するまで待機してください。デバイスの同期が進行中である場合は、PPM 設定変更のデバイスへの展開が失敗します。
- カードの動作モードが設定されたら、デバイスの同期が完了していることを確認します。慰安両していない場合は、Cisco EPN Manager は選択したカードの適切なペイロード値を表示できません。
- カードで設定変更を行う前に、すべてのカードできめ細かなインベントリが使用可能であることを確認してください。
- 40E-MXP-C、40ME-MXP-C、および OTU2-XP カードを除くすべてのサポート対象カードでは、まずシスコ トランスポート コントローラを使用してカードの動作モードを設定してから Cisco EPN Manager に戻り、次の手順に進む必要があります。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 設定するデバイス名のハイパーリンクをクリックしてデバイスを選択し、そのデバイスの [シャーシ（Chassis）] ビューを起動します。この機能は、Cisco NCS 2000 デバイスのみでサポートされています。

ステップ 3 [シャーシ エクスプローラ（Chassis Explorer）] を使用して、設定するカードを選択します。

ステップ 4 右側に表示されるウィンドウで [設定（Configuration）] サブタブをクリックします。

ステップ 5 CTC ツールに移動し、カードの動作モードを設定します。カードモードの設定は、OTU2-XP、MR-MXP、WSE、AR-XPE、AR-XP、および AR-MXP カードではサポートされていません。Cisco NCS 2000 デバイス上の他のすべてのカードについては、カードの設定：400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC （501 ページ）の説明に従って、カードの動作モードを設定します。

ステップ 6 [接続可能ポート モジュール（Pluggable Port Modules）] セクションを展開し、ポート モジュールとそれぞれの適切なペイロード値を設定します。

ステップ 7 [ポート モジュール（Port Modules）] セクションの [+]（追加）アイコンをクリックし、ポート モジュール（PPM）を作成します。

ステップ 8 **PPM 番号**を選択し、[保存（Save）] をクリックします。[PPM ポート（PPM Port）] はデフォルトで [PPM（1 ポート）（PPM (1 port)）] に設定されており、変更できません。

（注） 選択されているカードの最大数の PPM が作成されている場合、[+]（追加）アイコンは無効になります。次の手順に進むには、使用可能なすべてのポートを作成する必要があります。

ステップ 9 [接続可能ポート モジュール（Pluggable Port Modules）] セクションの [+]（追加）アイコンをクリックします。

（注） 一部の PPM では、該当するペイロード値が有効ではないことがあります。有効にするには、上記のステップ 5 で説明したカード モードの設定を行い、ペイロード値をもう一度設定してみます。

ステップ 10 選択した PPM に関連付ける必要がある**ポート番号**、**ポート タイプ**、および**レーン数**を選択します。[ポート タイプ（ペイロード）（Port Type (payload)）] には、以下の表 2 で説明するサポートされているクライアント信号のいずれかを設定できます。

（注） 指定されたポート タイプ（ペイロード）が、選択されているカードの動作モードまたは PPM でサポートされていない場合は、デバイスへの変更の展開が失敗します。指定するペイロード値が、選択したカードでサポートされていることを確認します。参考までに、次の表 2 を参照してください。

ステップ 11 [終了（Finish）] をクリックして、デバイスに変更を展開します。

ステップ 12 （オプション）Cisco EPN Manager で変更が表示されない場合、これは複数のユーザーが同じカード モード設定を操作しているために、変更が動的に反映されていないことが原因で発生している可能性があります。最新の変更を表示するには、各セクションの [更新（Refresh）] アイコンをクリックします。

展開が失敗する場合は、エラー ログ フォルダ（**/opt/CSCOlumos/logs/config.log**）に移動して、エラーの原因の詳細を確認してください。

カードの設定：400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC

カード動作モードと PPM を設定するには、次の手順に従います。

始める前に

- デバイス同期が完了しており、デバイスのインベントリ収集ステータスが「完了（Completed）」であることを確認してください。デバイス同期が実行中の場合、PPM 設定変更の展開が失敗します。
- カードモードの設定は、OTU2-XP、MR-MXP、WSE、AR-XPE、AR-XP、および AR-MXP カードではサポートされていません。これらのカードのカード動作モードを設定するには、Cisco Transport Controller ツールを使用します。
- デバイス同期が完了しており、デバイスのインベントリ収集ステータスが「管理（Managed）」または「完了（Completed）」であることを確認してください。
- カードで設定変更を行う前に、すべてのカードできめ細かなインベントリが使用可能であることを確認してください。
- デフォルトでは、デバイススロットリングは無効です。デバイススロットリングを有効にするには、**cd /opt/CSCOlumos/xmp_inventory/xde-home/inventoryDefaults** に移動し、**vi onsTL1.def** を実行して次の xml タグを追加します。

  <default attribute="DEVICE_THROTTLING">noOfconnections</default>

  ここで、**noOfconnections** は EPNM への最大 TL1 セッションの番号です。

  次に例を示します。**<default attribute="DEVICE_THROTTLING">6</default>**

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 設定するデバイス名のハイパーリンクをクリックしてデバイスを選択し、そのデバイスの [シャーシ（Chassis）] ビューを起動します。

ステップ 3 [シャーシ エクスプローラ（Chassis Explorer）] を使用して、設定するカードを選択します。

ステップ 4 右側に表示されるウィンドウで [設定（Configuration）] サブタブをクリックします。

ステップ 5 [接続可能ポート モジュール（Pluggable Port Modules）] セクションを展開し、ポート モジュールとそれぞれの適切なペイロード値を設定します。

ステップ 6 [ポート モジュール（Port Modules）] セクションの [+]（追加）アイコンをクリックし、ポート モジュール（PPM）を作成します。PPM 番号を選択し、[保存（Save）] をクリックします。[PPM ポート（PPM Port）] の値はデフォルトで [PPM（1 ポート）（PPM (1 port)）] に設定されており、変更できません。

（注）
- 選択されているカードに適用可能な最大数の PPM が作成されている場合、[+]（追加）アイコンは無効になります。次のステップに進む前に、選択されたカードに必要な数の PPM を作成する必要があります。100G-CK-C カードの場合、次の手順に進む前に、少なくとも 1 つの PPM を作成する必要があります。
- 400G-XP-LC カードでは、次のステップで説明するカード動作モードの設定の前に、PPM 11 と 12 が作成されていることを確認してください（ただし、カード モードはいずれかのトランク ポートで作成されます）。PPM 11 と 12 がない場合、デバイスに展開される設定変更は失敗します。
- このステップは、100G-LC-C、100G-ME-C、100G-CK-C、100ME-CK-C、200G-CK-LC、および 100GS-CK-C カードではオプションです。

ステップ 7 [カード動作モード（Card Operating Modes）] セクションを展開し、選択したカードの動作モードを設定します。

ステップ 8 [+]（追加）アイコンをクリックしてサポートされているカード動作モードのリストを表示するか、または編集アイコンをクリックして既存のカード動作モードを変更します。10x10G-LC カードの場合、最大 5 つのカード動作モード（クライアントまたはトランク ポートのセットとして動作可能な 10 ポート）を追加できますが、その他のすべてのカードでは、設定できるカード動作モードは 1 つだけです。カード動作モードを設定すると、「+」（追加）アイコンは無効になります。

ステップ 9 左側のパネルから動作モードを選択してパラメータを変更します。

（注）
- カードのピア構成に基づいて、一部のカード動作モードが無効になります。動作モードの横にある [i] アイコンをクリックして、動作モードを有効にする方法を確認します。動作モードを有効にするために必要なピア カード構成については、以下の「表 1」を参照してください。
- MXP カードの場合、トランク カード、ピア カード、およびピア スキップ カード構成が、以下に説明する順序になっていることを確認してください。

カード動作モード	トランク カード	ピア カード	ピア スキップ カード
MXP_200G	スロット 2	スロット 3	スロット 4
ONS 15454 M6 デバイスの MXP_200G	スロット 2 または 7 の 100GS-CK-LC または 200G-CK-LC カード。	スロット 3、4 または 5、6。	スロット 3、4 または 5、6。
Cisco NCS 2015 デバイスの MXP_200G	スロット 2、7、8、13 または 14 の 100GS-CK-LC または 200G-CK-LC カード。	隣接スロットの MR-MXP カード。	隣接スロットの MR-MXP カード。
MXP_10x10G_100G	スロット 7	スロット 6	スロット 5
ONS 15454 M6 デバイスの MXP_10x10G_100G	スロット 2 または 7 の 100GS-CK-LC または 200G-CK-LC カード	隣接スロット 3、4 または 5、6 の MR-MXP カード。	隣接スロット 3、4 または 5、6 の MR-MXP カード。
Cisco NCS 2015 デバイスの MXP_10x10G_100G	スロット 2、7、8、13 または 14 の 100GS-CK-LC または 200G-CK-LC カード。	隣接スロットの MR-MXP カード。	隣接スロットの MR-MXP カード。
ONS 15454 M6 デバイスの MXP_CK_100G	100GS-CK-LC または 200G-CK-LC カードとピア MR-MXP カードを隣接スロット 2-3、4-5、6-7 に装着する必要がある。		
Cisco NCS 2015 デバイスの MXP_CK_100G	100GS-CK-LC または 200G-CK-LC カードとピア MR-MXP カードを隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要がある。		

400G-XP-LC カードの場合は、M-100G/M-200G のトランク動作モードで OTNXC カードの動作モードを設定できます。トランク動作モードに基づいてサポートされるスライス設定（それぞれ「スライス 1 とスライス 4 」またはスライス 1、2、3、4）は OPM-100G と OPM-10x10Gです。

トランク 11 で設定されているトランク動作モードは、トランク 12 に自動的に反映されます。たとえば、トランク 11 で M-200G を設定すると、トランク 12 のトランク動作モードはグレー表示されます。ただし、M-200G はトランク 12 に自動的に設定されます。OPM_100G スライスと OPM_10x10G スライスを混在させることができ、スライスそれぞれは互いの影響を受けません。

ステップ 10 [保存（Save）] をクリックして、デバイスに変更を展開します。

ステップ 11 [接続可能ポート モジュール（Pluggable Port Modules）] セクションを展開して、各 PPM のペイロード値を設定します。

ステップ 12 [接続可能ポート モジュール（Pluggable Port Modules）] セクションの [+]（追加）アイコンをクリックします。

（注） 一部の PPM では、該当するペイロード値が有効ではないことがあります。有効にするには、上記のステップ 9 で説明したカード モードの設定を行い、ペイロード値をもう一度設定してみます。

ステップ 13 選択した PPM に関連付ける必要がある**ポート番号**、**ポート タイプ**、および**レーン数**を選択します。[ポート タイプ（ペイロード）（Port Type (payload)）] には、以下の「表 1」で説明するサポートされているクライアント信号のいずれかを設定できます。

（注）
- 指定されたポート タイプ（ペイロード）が、選択されているカード モードまたは PPM でサポートされていない場合は、デバイスへの変更の展開が失敗します。指定するペイロード値が、選択したカードでサポートされていることを確認します。参考のために「表 1」を参照してください。
- レーン数は、ペイロード値の分割が可能なカードでのみ設定できます。その他のすべてのカードでは、[レーン数（Number of Lanes）] フィールドは無効になっています。

ステップ 14 [終了（Finish）] をクリックして、デバイスに変更を展開します。

ステップ 15 （オプション）Cisco EPN Manager で変更が表示されない場合、これは複数のユーザーが同じカード モード設定を操作しているために、変更が動的に反映されていないことが原因で発生している可能性があります。最新の変更を表示するには、各セクションの [更新（Refresh）] アイコンをクリックします。

展開が失敗する場合は、エラー ログ フォルダ（**/opt/CSCOlumos/logs/config.log**）に移動して、エラーの原因の詳細を確認してください。

SONET および Flex の回線カードの設定

この手順では、Cisco EPN Manager を使用して10X10G-LC SONET カードと 400G-XP、200G-CK-LC、および 100GS-CK-LC Flex カードの回線カードの設定を変更する方法について説明します。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

SONET または Flex 回線カードを設定するには、次の手順を実行します。

始める前に

- SONET 回線カードを設定するには、動作モード MXP10X10G および OC192 のペイロード値を持つカードを選択してください。
- SONET または Flex の回線カード設定を削除するには、選択したカードに関連付けられているペイロード値を削除する必要があるだけです。これにより、SONET または Flex の設定がデバイスから自動的に削除されます。ペイロード値を削除するには、[設定（Configuration）] サブタブの下にある [接続可能なポート モード（Pluggable Port Mode）] 領域を使用します。
- SONET または Flex の回線カードの設定中に、回線カードのタイプを SONET から SDH に変更する場合、またはその他の同様の変更を行う場合は、まずデバイスの管理状態が [OOS 無効（OOS-Disabled）] に設定されていることを確認する必要があります。デバイスの状態が [OOS 無効（OOS-Disabled）] でない場合、デバイスに展開された回線設定の変更は失敗します。
- Flex 回線カードを設定するには、カードのカード動作モードが以前に設定済みであることを確認します。カードの設定：400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC（501 ページ）を参照してください。

ステップ 1 シャーシ ビューを開く（117 ページ）の説明に従って、シャーシ ビューを起動します。

ステップ 2 次のいずれかの方法で、設定するカードのスロットを選択します。

- ズームインとズームアウトのオプションを使用して、物理 [シャーシビュー（Chassis View）] からスロット内のカードを選択します。
- [シャーシエクスプローラ（Chassis Explorer）] ビューを使用し、カードに移動して選択します。

ステップ 3 右側に表示されるウィンドウで [設定（Configuration）] サブタブをクリックします。

ステップ 4 [ライン（Line）] セクションを展開し、[SONET] または [Flex] サブタブを選択します。

SONET の設定でサポートされているカードは 10x10G-LC カードのみです。Flex カードの場合は、400G-XP、200G-CK-LC、および 100GS-CK-LC カードです。

ステップ 5 設定を編集するには、次のいずれかの方法を選択します。

- 編集する設定の [SONET] タブまたは [Flex] タブを選択し、[編集] アイコンをクリックします。
- 編集するインライン パラメータを、テーブルの行内で 1 つずつクリックします。

ステップ 6 次の表に示すパラメータに必要な変更を加え、[保存（Save）] をクリックしてデバイスに変更を展開します。

SONET パラメータの設定時：

- [タイプ（Type）] を [SDH] に設定すると、[メッセージの同期（Sync Messages）] チェックボックスが自動的に無効になり、設定できません。
- [メッセージの同期（Sync Messages）] チェックボックスを有効にすると、[管理者 SSM（Admin SSM）] オプションが無効になり、null に設定されます。

Flex パラメータの設定時：

- 400G-XP-LC カードの場合、Flex ライン カードはトランク ポート 11/12 に対してのみ設定できます。
- 100GS-CK-LC カードの場合、Flex ライン カードはトランク ポート 2 に対してのみ設定できます。

表 *24 : SONET* および *Flex* ラインの設定パラメータと説明

ライン カードのタイプ	ラインカードの設定パラメータ	説明
SONET	ポート番号（Port Number）	設定する SONET インターフェイスのポート番号。
	ポート名（Port Name）	SONET 光ポートの名前を追加できます。
	SD BER	信号劣化ビット エラー レートを設定します。
	SF BER	信号障害ビット エラー レートを設定します。
	タイプ（Type）	ポートを SONET または SDH として定義します。
	同期を提供（Provides Sync）	オンにすると、カードは NE のタイミング基準としてプロビジョニングされます。
	メッセージングの同期（Sync Messaging）	同期ステータス メッセージ（S1 バイト）をイネーブルにします。これにより、ノードで最適なタイミング ソースを選択できるようになります。
	管理 SSM 入力（Admin SSM In）	ノードが SSM 信号を受信しない場合、デフォルトで STU（Synchronization Traceability Unknown）になります。管理者 SSM を使用すると、STU 値を次のいずれかでオーバーライドできます。 • PRS：プライマリ基準ソース（Stratum 1） • STS2：Stratum 2 • TNC - トランジット ノード クロック • STS3E：Stratum 3E • STS3：Stratum 3 • SMC：SONET 最小クロック • ST4：Stratum 4

ライン カードのタイプ	ラインカードの設定パラメータ	説明
Flex	ポート（Port）	設定する Flex インターフェイスのポート番号。
	グリッドレス（Gridless）	選択したカードのグリッドレス調整機能を有効または無効にします。この機能を有効にすると、カードの周波数値を設定できます。選択できるオプションは、次のとおりです。 • 有効：選択すると、Flex の周波数パラメータを編集できます。 • 無効：選択すると、Flex の周波数パラメータが無効になります。
	周波数（Frequency）	400G-XP、200G-CK-LC、および 100GS-CK-LC カードのポートの周波数を、191350 ～ 196100 の範囲で指定します。

着脱可能ポート モジュールおよびカード モード設定の編集と削除

始める前に

PPM を削除するための前提条件：

- PPM がアクティブ回線またはプロビジョニング回線の一部となっていないことを確認します。
- PPM とそのそれぞれのペイロード値を、以下の手順で説明している順序でのみ削除する必要があります。先にクライアント ポート 1 ～ 10 を手動で削除してから、関連付けられた PPM を削除します。
- デバイス同期が完了しており、デバイスのインベントリ収集ステータスが「完了（Completed）」または「管理（Managed）」であることを確認します。

カード動作モードを削除するための前提条件：

- カードがアクティブ回線またはプロビジョニング回線の一部となっていないことを確認します。
- 400G-XP カードの場合、PPM 11 および 12 は削除できません。これらの PPM は、関連付けられたカード動作モードが削除されると自動的に削除されます。
- ピア カードまたはスキップ カードがアクティブ状態でない必要があります。CTC を使用してピア カードまたはスキップ カードの関連付けを削除してから、Cisco EPN Manager を使用して再びカード動作モードの削除を試すことができます。Cisco EPN Manager から直接、カードの削除を試みることもできます。詳細については、カードの削除（497ページ）を参照してください。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 設定するデバイス名のハイパーリンクをクリックしてデバイスを選択し、そのデバイスの [シャーシ（Chassis）] ビューを起動します。

ステップ 3 [シャーシエクスプローラ（Chassis Explorer）] を使用して、設定を削除するカードを選択します。

ステップ 4 右側に表示されるウィンドウで [設定（Configuration）] サブタブをクリックします。

ステップ 5 着脱式ポート モジュール（PPM）を削除するには、[着脱式ポートモジュール（Pluggable Port Modules）] セクションを展開します。

a) [着脱式ポートモジュール（Pluggable Port Modules）] サブセクションで、削除対象の関連付けられたペイロード値を選択し、[X]（削除）アイコンをクリックします。

b) [OK] をクリックして確定します。変更がデバイスに展開されます。

c) [ポートモジュール（Port Modules）] サブセクションで、削除する PPM を選択し、[X]（削除）アイコンをクリックします。

d) [OK] をクリックして確定します。変更がデバイスに展開されます。

（注） PPM を削除する前に、対象の PPM に関連付けられているすべてのペイロード値を削除する必要があります。

ステップ 6 [カード動作モード（Card Operating Modes）] セクションを展開し、カードの設定を削除します。

a) カード モードの設定を編集するには、必ず 400G-XP カードのみを選択し、編集アイコンをクリックして変更を加えます。他のカードの設定を編集する場合はすべて、カードモードの設定を削除してから、新しい値で再作成する必要があります。

b) カード モードの設定を削除するには、削除が必要なカード モードの設定を選択し、[X]（削除）アイコンをクリックします。

c) [OK] をクリックして確定します。変更がデバイスに展開されます。

Cisco NCS 2000 デバイス用のカードとサポートされる設定

表 *25 : 100GS-CK-LC* および *200G-CK-LC* カード：サポートされる構成

カード動作モード	トランク カード	ピア カード	ピア スキップ カード	サポートされるペイロード タイプ

MXP_200G	スロット 2、7、8、13 または 14 の 100GS-CK-LC または 200G-CK-LC カード。	スロット 3、6、9、12、または 15 の MR-MXP カード。	スロット 4、5、10、11 または 16 の MR-MXP カード。	100GE と OTU4 OTU4 は 200G-CK-LC カードでのみサポートされています。 任意の 100 G 構成の再生成 10GE 10GE 100GE
MXP_10x10G_100G	スロット 2、7、8、13 または 14 の 100GS-CK-LC または 200G-CK-LC カード。	スロット 3、6、9、12、または 15 の 10x10G-LC カード。	スロット 4、5、10、11 または 16 の MR-MXP カード。	100GE と OTU4 OTU4 は 200G-CK-LC カードでのみサポートされています。 任意の 100 G 構成の再生成 10GE 10GE 100GE
MXP_CK_100G	100GS-CK-LC または 200G-CK-LC カードとピア MR-MXP カードを隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要がある。	該当なし	該当なし	100GE と OTU4 OTU4 は 200G-CK-LC カードでのみサポートされています。 任意の 100 G 構成の再生成 10GE 10GE 100GE
RGN-100G	100GS-CK-LC または 200G-CK-LC カードとピア カード 100GS-CK-LC または 200G-CK-LC を隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要がある。	該当なし	該当なし	100GE と OTU4 OTU4 は 200G-CK-LC カードでのみサポートされています。 任意の 100 G 構成の再生成 10GE 10GE 100GE

TXP-100G	100GS-CK-LC または200G-CK-LC	該当なし	該当なし	該当なし

表 ***26 : 100G-CK-C*** および ***100ME-CKC*** カード：サポートされる構成

カード動作モード	トランク カード	ピア カード	スキップ カード	サポートされるペイロード タイプ
TXP-100G	100G-CK-C/ 100ME-CKC	該当なし	該当なし	100GE、OTU4 ：任意の 100 G 構成の再生成 40GE
RGN-100G	100G-CK-C/ 100ME-CKC カードとピア カード 100G-LC-C/ 100G-ME-C/ 100G-CK-C/ 100ME-CKC を隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要がある。		該当なし	100GE、OTU4 ：任意の 100 G 構成の再生成 40GE
MXP-2x40G	100G-CK-C/ 100ME-CKC	該当なし	該当なし	100GE、OTU4 ：任意の 100 G 構成の再生成 40GE

表 ***27 : 100G-LC-C*** および ***100G-ME-C*** カード：サポートされる構成

カード動作モード	トランク カード	ピア カード	スキップ カード	サポートされるペイロード タイプ
TXP-100G	100G-LC-C/ 100G-ME-C	該当なし	該当なし	100GE、OTU4 ：任意の 100 G 構成の再生成 40GE
RGN-100G	100G-LC-C/ 100G-ME-C カードとピア カード 100G-LC-C/ 100G-ME-C/ 100G-CK-C/ 100ME-CKC を隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要がある。		該当なし	100GE、OTU4 ：任意の 100 G 構成の再生成 40GE

表 *28 : 10X10G-LC* カード：サポートされる構成

カード動作モード	トランク カード	ピア カード	スキップ カード	サポートされるペイロード タイプ
TXPP-10G	10x10G-LC	該当なし	該当なし	OC192/STM-64、10GE-LAN Phy、10GE-WAN Phy（OC192を使用）、OTU2、OTU2e、8G FC、10G FC、FICON 10x10G-LC カードを 100GS-CK-LC カードに接続すると、OC192/STM64 および 10GE のみがサポートされます。 10x10G-LC カードを 200G-CK-LC カードに接続すると、OC192/STM64、10GE、および OTU2 のみがサポートされます。 10GE-LAN Phy、OTU2 10GE-LAN Phy、OTU2e、OTU2、OC192/STM-64、8G FC、10G FC、IB_5G 10GE、10G FC 10GE 10GE、OTU2e
TXP-10G	10x10G-LC	該当なし	該当なし	OC192/STM-64、10GE-LAN Phy、10GE-WAN Phy（OC192を使用）、OTU2、OTU2e、8G FC、10G FC、FICON 10x10G-LC カードを 100GS-CK-LC カードに接続すると、OC192/STM64 および 10GE のみがサポートされます。 10x10G-LC カードを 200G-CK-LC カードに接続すると、OC192/STM64、10GE、および OTU2 のみがサポートされます。 10GE-LAN Phy、OTU2 10GE-LAN Phy、OTU2e、OTU2、OC192/STM-64、8G FC、10G FC、IB_5G 10GE、10G FC 10GE 10GE、OTU2e

MXP-10x10G	10x10G-L カードとピア 100G-LC-C、100G-ME-C、100G-CK-C、100ME-CKC、100GS-CK-LC または 200G-CK-LC カードを隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要がある。	該当なし	該当なし	OC192/STM-64、10GE-LAN Phy、10GE-WAN Phy（OC192を使用）、OTU2、OTU2e、8G FC、10G FC、FICON 10x10G-LC カードを 100GS-CK-LC カードに接続すると、OC192/STM64 および 10GE のみがサポートされます。 10x10G-LC カードを 200G-CK-LC カードに接続すると、OC192/STM64、10GE、および OTU2 のみがサポートされます。 10GE-LAN Phy、OTU2 10GE-LAN Phy、OTU2e、OTU2、OC192/STM-64、8G FC、10G FC、IB_5G 10GE、10G FC 10GE 10GE、OTU2e
RGN-10G	10x10G-LC	該当なし	該当なし	OC192/STM-64、10GE-LAN Phy、10GE-WAN Phy（OC192を使用）、OTU2、OTU2e、8G FC、10G FC、FICON 10x10G-LC カードを 100GS-CK-LC カードに接続すると、OC192/STM64 および 10GE のみがサポートされます。 10x10G-LC カードを 200G-CK-LC カードに接続すると、OC192/STM64、10GE、および OTU2 のみがサポートされます。 10GE-LAN Phy、OTU2 10GE-LAN Phy、OTU2e、OTU2、OC192/STM-64、8G FC、10G FC、IB_5G 10GE、10G FC 10GE 10GE、OTU2e
低遅延	10x10G-LC	該当なし	該当なし	該当なし

ファンアウト - 10X10G	10x10G-LC	該当なし	該当なし	OC192/STM-64、10GE-LAN Phy、10GE-WAN Phy（OC192を使用）、OTU2、OTU2e、8G FC、10G FC、FICON 10x10G-LC カードを 100GS-CK-LC カードに接続すると、OC192/STM64 および 10GE のみがサポートされます。 10x10G-LC カードを 200G-CK-LC カードに接続すると、OC192/STM64、10GE、および OTU2 のみがサポートされます。 10GE-LAN Phy、OTU2 10GE-LAN Phy、OTU2e、OTU2、OC192/STM-64、8G FC、10G FC、IB_5G 10GE、10G FC 10GE 10GE、OTU2e

Cisco NCS 2000 デバイスの 400G-XP-LC カードおよび MR-MXP カードは、次のカード動作モードとペイロード値で設定できます。

- ペイロード タイプ OTU2/OC192 は MR-MXP カードでサポートされます。
- ペイロード タイプ 16G-FC/OTU2 は 400G-XP-LC カードでサポートされます。
- スライス動作モード OPM_6x16G_LC は 400G-XP-LC カードでサポートされます。

MPLS LDP および MPLS-TE リンクの検出と設定

Cisco EPN Manager を使用して、MPLS ネットワークでラベル配布プロトコル（LDP）および MPLS-TE リンクを設定できます。

MPLS LDP

LDP は、基になる IGP ルーティング プロトコルによって選択されたルートにラベルを割り当てることにより、MPLS ネットワークにおけるホップバイホップ（つまりダイナミック ラベル）配布の標準の方式を提供します。ラベルスイッチパス（LSP）と呼ばれるラベル付きの結果のパスによって、ラベル付きトラフィックが MPLS バックボーン全体に転送されます。Cisco EPN Manager を使用すると、潜在的ピアを設定し、これらのピアとの LDP セッションを確立して情報を交換できます。

Cisco EPN Manager を使用して LDP を設定するには、LDP リンクの設定を必要とするデバイスのネットワーク アドレスとインターフェイス、および設定する IP アドレスのサブネット マスクを知る必要があります。

（注） MPLS LDP を設定する前に、LDP ID がデバイスで事前に設定されていることを確認してください。

MPLS-TE

Cisco EPN Manager は、MPLS トラフィック エンジニアリング（MPLS-TE）サービスのプロビジョニングをサポートしています。MPLS-TE により、MPLS バックボーンにおいてレイヤ 2 の TE 機能をレイヤ 3 経由でレプリケートして拡張できます。MPLS TE は、バックボーン全体でラベルスイッチド パス（LSP）を確立および維持するために、Resource Reservation Protocol（RSVP）を使用します。詳細については、サポートされている MPLS トラフィック エンジニアリング サービス （623 ページ） を参照してください。

LDP パラメータと MPLS-TE パラメータを設定する手順は次のとおりです。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

（注） デバイスに提供されている EPNM サポートのレベルに応じて、[Logical View] タブが表示される場合があります。

ステップ 4 LDP リンクを設定する手順は次のとおりです。

a) [MPLS] > [LDP] を選択し、[共通プロパティ（Common Properties）] タブをクリックし、[+] をクリックして新しい LDP パラメータを指定します。既存のパラメータを編集するには、[LDP アドレス（LDP Address）] ハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。

（注） デバイスごとに 1 セットの LDP 設定のみ追加できます。

b) [共通プロパティ（Common Properties）] タブで、次の表に示す LDP パラメータを指定します。

MPLS LDP のフィールド	フィールドの説明
LDP インターフェイス（LDP Interface）	デバイス上の LDP セッションのソース ループバック インターフェイスとなる LDP インターフェイスを選択します。
LDP アドレス（LDP Address）	LDP インターフェイスの IP アドレスを指定します。いったん設定した LDP アドレスは編集できません。LDP アドレスを変更するには、LDP セッションを削除し、新しい LDP アドレスを使用して新しいセッションを作成します。
セッション保留時間（Session Hold Time）	（任意）保留タイマーが期限切れになった後に hello を受信しなかった場合に LDP セッションがダウンする時間（秒単位）を入力します。範囲は 15 ～ 65535 です。

MPLS LDP のフィールド	フィールドの説明
NSR の有効化（NSR Enabled）	true または false を選択して、LDP ノンストップ ルーティング（NSR）を有効または無効にします。NSR を有効にすると、ラベル配布プロトコル（LDP）がピア セッションを失うことなく動作を継続できます。
検出保留時間（Discovery Hold time）と検出ターゲット保留時間（Discovery Target Hold time）	（任意）LDP ソースと検出された LDP ネイバーから LDP hello メッセージを受信しなくてもそのネイバーを記憶しておく時間（秒単位）を入力します。範囲は 1 ～ 65535 です。
検出保留間隔（Discovery Hold Interval）と検出ターゲット保留間隔（Discovery Target Hold Interval）	（任意）LDP ソースと検出された LDP ネイバーを記憶しておく時間間隔（秒単位）を入力します。範囲は 1 ～ 65535 です。
ダウンストリーム最小ラベル（DownStream Min Label）とダウンストリーム最大ラベル（DownStream Max Label）	（任意）LSP で許可され、ダウンストリーム オン デマンド方式のラベル配布により確立される最小および最大ホップ数を入力します。ISO XE の場合は 16 ～ 32767、ISO XR デバイスの場合は 16000 ～ 1048575 の範囲で指定します。
ダウンストリーム最大ホップ数（DownStream Max Hop Count）	（任意）LSP で許可され、ダウンストリーム オン デマンド方式のラベル配布により確立されるホップ数を入力します。範囲は 1 ～ 255 です。
IGP ホールド ダウン時間（IGP Hold Down Time）	（任意）リンク アップ時のセッション確立後に LDP 同期ステートの宣言が遅延される時間（秒単位）を入力して指定します。ISO XE の場合は 1 ～ 2147483647 ミリ秒、ISO XR デバイスの場合は 5 ～ 300 ミリ秒の範囲で指定します。
エントロピーの有効化（Entropy Enabled）	true または false を選択して、MPLS LDP エントロピー ラベル サポート機能を有効または無効にします。この機能は、エントロピー ラベルを使用して MPLS ネットワーク間の負荷分散を改善するのに役立ちます。
明示的ヌルの有効化（Explicit Null Enabled）	（任意）直接接続されたルートの明示的 null ラベルをアドバタイズするには、この値を有効にします。値は Yes（有効）または No（無効）です。
初期バックオフ（Initial Back Off）と最大バックオフ（Max Back Off）	（任意）初期バックオフ遅延値と最大バックオフ遅延値（秒単位）を入力します。範囲は 5 ～ 2147483 です。

c) [保存（Save）] をクリックして、変更内容をデバイスに展開します。
d) [インターフェイス（Interfaces）] をクリックし、[+] をクリックしてインターフェイス パラメータを指定します。

MPLS LDP のフィールド	フィールドの説明
インターフェイス名（Interface Name）	LDP セッションに参加するインターフェイスの名前を指定します。
ラベル配布方法（Label Distribution Method）	ラベル配布方法として 「LDP」を指定します。
Hello 間隔（Hello Interval）	（任意）helloメッセージが送信される時間間隔（秒単位）を入力します。範囲は 1 ～ 65535 です。

e) [保存（Save）] をクリックして、変更内容をデバイスに展開します。同じプロパティがピア デバイスで構成されます。ネイバー デバイスが形成されると、[ネイバー（Neighbors）] タブに詳細が設定されます。

ステップ 5 MPLS-TE リンクを設定する手順は次のとおりです。

a) [MPLS] > [MPLS-TE] を選択します。.

b) [MPLS-TE FRR] 領域で、[MPLS TE Tunnel Enabled] チェックボックスをオンにします。MPLS-TE パラメータのデフォルト値は、次の表に示すように表示されます。

MPLS TE トンネルのフィールド	フィールドの説明
MPLS TE トンネルの有効化（MPLS TE Tunnel Enabled）	自動帯域幅対応トンネルのリストの表示を有効にし、トンネルの現在の信号送信帯域幅が、自動帯域幅によって適用される帯域幅と同じかどうかを示します。
自動帯域幅タイマー周波数（秒）（Auto Bandwidth Timer Frequency (Sec)）	トンネル インターフェイスの自動帯域幅がトリガーされる間隔（秒単位）を設定します。
タイマー周波数の再最適化（秒）（Reoptimize Timer Frequency (Sec)）	すべての TE トンネルの再最適化間隔をトリガーする値（秒単位）を設定します。
自動バックアップトンネルの有効化（Auto Backup Tunnel Enabled）	自動的に構築される MPLS-TE バックアップ トンネルに関する情報を表示します。
バックアップ トンネル最小範囲（Backup Tunnel Min. Range）とバックアップ トンネル最大範囲（Backup Tunnel Max. Range）	指定した最小値と最大値の間でバックアップ自動トンネル番号の範囲を設定します。バックアップ トンネルの最小範囲は最大範囲よりも小さくしてください。
SRLG を除く（SRLG Exclude）	除外の目的で SRLG 値を取得する IP アドレスを指定します。必要に応じて、次のいずれかのオプションを選択します。 • 優先（Preferred） • 強制（Forced） • なし（None） （注） [SRLG を除く（SRLG Exclude）] オプションは IOS-XE でのみ使用できます。

MPLS TE トンネルのフィールド	フィールドの説明
番号付けされていないインターフェイス（Un-numbered Interface）	明示的なアドレスを使用せずに、指定したインターフェイスでの IP 処理を有効にします。

ステップ 6 [保存（Save）] をクリックして、変更内容をデバイスに展開します。

次のタスク

ネットワーク トポロジ上で LDP リンクを監視します。

1. 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。
2. [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。
3. トポロジ ツールバーで [表示（Show）] をクリックし、[リンク（Links）] を選択します。
4. [コントロールプレーン（Control Plane）] の [LDP] チェックボックスをオンにすると、マップ上に LDP リンクが表示されます。
5. LDP リンクをクリックすると、リンクの詳細が表示されます。

MPLS-TE サービスをプロビジョニングする方法については、MPLS トラフィック エンジニアリング サービスのプロビジョニング （740 ページ）を参照してください。

SPAN と RSPAN を使用したポートの分析

Cisco EPN Manager を使用すると、SPAN または RSPAN を使用して、スイッチ上の別のポートまたはモニター デバイスにトラフィックのコピーを送信することで、ポートまたは VLAN を通過するネットワーク トラフィックを解析できます。SPAN では、送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックが宛先ポートにコピー（ミラーリング）されて解析されます。送信元ポートに出入りするトラフィックや、送信元 VLAN に出入りするトラフィックが監視されます。

着信トラフィックを監視するように SPAN を設定した場合、別の VLAN から送信元 VLAN にルーティングされるトラフィックは監視できません。ただし、送信元 VLAN で受信され、別の VLAN にルーティングされるトラフィックは監視できます。

Cisco EPN Manager では、デバイスごとに 1 つのローカル SPAN セッションのみを設定できます。ローカル SPAN セッションでは、1 つ以上の送信元ポートからのトラフィックが宛先ポートにコピーされて解析されます。

リモート SPAN を使用すると、異なるスイッチ上の送信元ポート、送信元 VLAN、および宛先ポートを設定でき、ネットワーク上にある複数のスイッチのリモートモニターリングが可能になります。各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN 上で

伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN を監視する宛先セッションに転送されます。

（注） ポートを監視するには、ポートを 1 つ以上の VLAN（送信元または宛先）に関連付ける必要があります。

ポートの監視（またはミラーリング）を有効にする手順は次のとおりです。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 RSPAN セッションを設定します。

a) [ポートアナライザ（Port Analyzer）] > [RSPAN] > [宛先ノード（Destination Node）] の順に選択し、RSPAN の宛先ノードを設定します。

b) [+] をクリックして RSPAN セッション ID を指定します。既存の設定を編集するには、セッション ID のハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。

最大 14 個の RSPAN セッションと SPAN セッションを追加できます。

c) セッション ID を選択し、[保存（Save）] をクリックします。

セッションタイプのリモート宛先（リモート RSPAN）はデフォルトで設定されており、編集できません。

d) セッション ID のハイパーリンクをクリックし、宛先ノードの送信元設定と宛先設定を指定します。

e) [送信元設定（Source Settings）] タブをクリックし、有効な VLAN ID（選択したデバイスで設定された VLAN に基づいて自動設定）を選択して、[保存（Save）] をクリックします。

宛先ノードの送信元として追加できる VLAN は 1 つだけです。VLAN を設定していない場合は、設定してからこの手順に戻る必要があります。VLAN のインターフェイスの表示（450 ページ）を参照してください。

f) [宛先設定（Destination Settings）] タブをクリックし、RSPAN の宛先ノードとして機能させるインターフェイスを選択して、[保存（Save）] をクリックします。

a) 機能パネルから、[ポートアナライザ（Port Analyzer）] > [RSPAN] > [送信元ノード（Source Node）] の順に選択し、RSPAN の送信元ノードを設定します。

b) [+] をクリックし、共通の RSPAN 送信元ノード設定を指定します。既存の設定を編集するには、セッション ID のハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。

c) セッション ID を選択し、[保存（Save）] をクリックします。

セッション タイプ [リモート送信元（リモート RSPAN）] はデフォルトで設定されており、編集できません。

d) セッション ID のハイパーリンクをクリックし、送信元ノードの送信元設定と宛先設定を指定します。
e) [送信元設定（Source Settings）] タブをクリックし、次の値を指定して、[保存（Save）] をクリックします。

i）[インターフェイス（Interface）] ドロップダウン メニューで、RSPAN 送信元ノードの送信元インターフェイスとして機能するインターフェイスを選択します。

RSPAN の送信元ノードとして指定したインターフェイスは、SPAN の送信元/宛先ノードとしても使用できます。

ii）[方向（Direction）] ドロップダウン メニューで、インターフェイスを RSPAN 送信元ノードに適用する際の必要な方向を選択します。選択できるオプションは、次のとおりです。

- [送信（Transmit）] : スイッチによる変更および処理がすべて完了した後に、送信元インターフェイスが送信したすべてのパケットをモニターします。送信元が送信した各パケットのコピーが、そのセッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。
- [受信（Receive）] : スイッチが変更または処理を行う前に、送信元インターフェイスまたはVLANが受信したすべてのパケットをモニターします。送信元が受信した各パケットのコピーが、そのセッションに対応する宛先ポートに送られます。
- [両方（Both）] : （デフォルト値）受信パケットと送信パケットの両方についてポートまたはVLANをモニターします。

RSPANの送信元ノードに複数のインターフェイスを追加し、それらのインターフェイスに単一のVLAN ID を関連付けることができます。

f) [宛先設定（Destination Settings）] タブをクリックし、有効な VLAN ID（選択したデバイスで設定された VLAN に基づいて自動設定）を選択して、[保存（Save）] をクリックします。

ステップ 5 SPAN セッションを設定します。

a) [ポートアナライザ（Port Analyzer）] > [SPAN] をクリックします。
b) [+] をクリックし、共通の SPAN 送信元ノード設定を指定します。既存の設定を編集するには、セッション ID のハイパーリンクをクリックし、ページの右上隅にある [編集（Edit）] アイコンをクリックします。

RSPAN の送信元ノードおよび宛先ノードとして設定したインターフェイスは、SPAN 用には使用できません。

c) セッション ID を選択し、[保存（Save）] をクリックします。
セッションタイプ[ローカル（ローカルRSPAN）]はデフォルトで設定されており、編集できません。
d) セッション ID のハイパーリンクをクリックし、SPAN の送信元設定と宛先設定を指定します。
e) [送信元設定（Source Settings）] タブをクリックし、インターフェイスと、インターフェイスを SPAN に適用する際の必要な方向を選択し、[保存（Save）]をクリックします。詳細については、ステップ4を参照してください。

RSPAN の送信元ノードとして指定したインターフェイスは、SPAN の送信元/宛先ノードとしても使用できます。

f) [宛先設定（Destination Settings）] タブをクリックし、有効な VLAN ID（選択したデバイスで設定された VLAN に基づいて自動設定）を選択して、[保存（Save）] をクリックします。

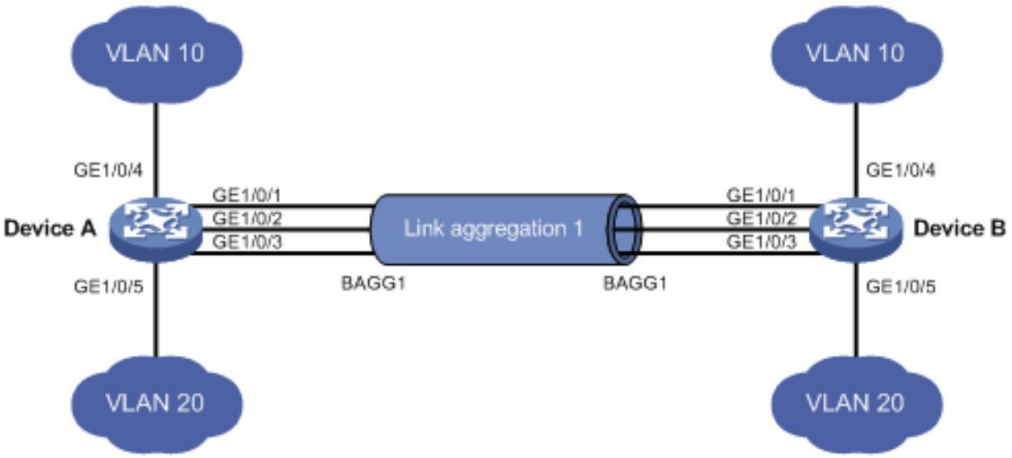
g) （任意）変更が正しく構成されたことを確認するには、デバイス CLI で次のコマンドを使用します。

```
show monitor session all
```

イーサネット Link Aggregation Group の設定と表示

イーサネット Link Aggregation Group（LAG）は、1 つ以上のポートを集約したグループで、単一のリンクとして扱われます。各バンドルには、1 つの MAC、1 つの IP アドレス、1 つの設定セット（ACL など）があります。LAG により、複数のスイッチ ポートを 1 つのスイッチ ポートとして扱うことができます。ポート グループは、2 つのネットワーク要素間で高帯域接続を行う単一の論理ポートとして動作します。単一の LAGl により、トラフィックの負荷がチャネルのリンク全体にわたって分散します。LAG は、2 つのリンクを使用してサービスをプロビジョニングするのに役立ちます。リンクの一方で障害が発生すると、トラフィックが他方のリンクに移動します。

次の図は、デバイス A とデバイス B の 2 つのデバイス間で作成された LAG を示しています。



405431

Cisco EPN Manager では次の方法で LAG を表示および管理できます。

- 複数のインターフェイスを使用した Link Aggregation Group（LAG）の作成 （522 ページ）
- イーサネット LAG プロパティの表示 （523 ページ）

複数のインターフェイスを使用した Link Aggregation Group（LAG）の作成

Cisco EPN Manager を使用すると、複数の物理スイッチ ポートを単一の論理スイッチ ポートとして扱う機能を提供する LAG を作成できます。

始める前に

- まだ既存の LAG の一部となっていないインターフェイスのみを選択できます。1 つのインターフェイスを複数の LAG の一部にすることはできません。
- 選択したインターフェイスのグループはすべて同じ帯域幅タイプで構成されている必要があります。
- LAG に参加するデバイスのインベントリ収集ステータスは「完了（Completed）」となっている必要があります。

LAG を作成する手順は次のとおりです。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 [インターフェイス（Interfaces）] > [リンクの集約（Link Aggregation）] を選択します。

ステップ 5 使用する制御方法の種類に応じて [PAgP] タブまたは [LACP] タブをクリックします。

ステップ 6 追加（+）記号をクリックして新しい LAG を作成します。

ステップ 7 LAG の一意の名前を入力します。指定するチャネル グループ ID が LAG 名の一部となるようにします。たとえば、チャネル グループ ID が 10 の場合、LAG 名は次のようになります。

- 「Bundle-Ether10」（Cisco IOS-XR デバイスの場合）。
- 「Port-channel10」（Cisco IOS、Cisco ME3600、および Cisco ME3800 デバイスの場合）。

ステップ 8 チャネル グループ ID を指定するには、1 ～ 16 の数値を入力します。各種デバイスのチャネル グループ ID の範囲は、Cisco ASR 90X デバイスでは 1 ～ 8、Cisco ASR 920X デバイスでは 1 ～ 64、Cisco ME3x00 デバイスでは 1 ～ 26、Cisco NCS42xx デバイスでは 1 ～ 48、Cisco ASR9000 デバイスでは 1 ～ 65535 です。

ステップ 9 [メンバーポート設定（Member Port Settings）] タブをクリックし、メンバー ポートの値を指定します。

- LACP モード（LACP Modes）：LACP は次のモードに設定できます。
  - アクティブ（Active）：このモードでは、ポートから LACP パケットが定期的にパートナー ポートに送信されます。
  - パッシブ（Passive）：このモードでは、パートナー ポートから LACP パケットが送信されるまで、ポートから LACP パケットが送信されません。パートナー ポートから LACP パケットを受信した後で、ポートは LACP パケットをパートナー ポートに送信します。

- PAgP モード（PAgP Modes）：PAgP モードは、AUTO、DESIRABLE、または ON に設定できます。ASR9K デバイスでは、ON の PAgP モードのみ有効です。ON は、モードが PAgP - 手動に設定されたことを意味します。

ステップ 10 [保存（Save）] をクリックします。

変更内容が保存され、作成された LAG にインターフェイスを追加できるようになりました。

ステップ 11 作成された LAG にインターフェイスを追加するには、[リンク集約（Link Aggregation）] テーブルから必要なチャネル グループを選択し、[編集] アイコンをクリックします。

ステップ 12 LAG の作成に使用するインターフェイスを選択します。

ステップ 13 [保存（Save）] をクリックします。

選択したインターフェイスを使用して LAG が作成されます。

イーサネット LAG プロパティの表示

イーサネット LAG のプロパティは次の方法で表示できます。

- デバイスの [設定（Configuration）] タブを使用する：
  1. **[ネットワークデバイス（Network Devices）] > [デバイスのプロパティ（Device Properties）] > [設定（Configuration）]** タブに移動します。
  2. デバイス名のハイパーリンクをクリックして、LAG を設定するデバイスを選択します。
  3. [論理ビュー（Logical View）] タブをクリックします。
  4. [機能（Features）] パネルで、[インターフェイス（Interfaces）] > [リンク集約（Link Aggregation）] をクリックします。

- [デバイスの詳細（Device Details）] タブを使用する：
  1. **[ネットワークデバイス（Network Devices）] > [デバイスのプロパティ（Device Properties）]** に移動します。
  2. デバイス名のハイパーリンクをクリックして、LAG を設定するデバイスを選択します。
  3. [デバイスの詳細（Device Details）] タブをクリックします。
  4. [機能（Features）] パネルで、[インターフェイス（Interfaces）] > [イーサネットチャネル（Ether Channel）] をクリックします。

ルーティング プロトコルとセキュリティの設定

Cisco EPN Manager を使用して、CE および光デバイス用に次のルーティング プロトコルを設定できます。ACL を使用してデバイスのセキュリティを設定することもできます。

ルーティング プロトコルや ACL を設定する場合は、事前にデバイスのインベントリ収集ステータスが [完了（Completed）] であることを確認してください。

デバイスのルーティング テーブルを表示するには、[デバイス 360（Device 360）] ビューを開き、**[操作（Actions）] > [ルーティングテーブル情報（Routing Table Info）] > [すべて（All）]** を選択します。

BGP の設定

ボーダー ゲートウェイ プロトコル（BGP）は、ネットワーク内の自律システム（AS）間でルーティング情報と到達可能性情報を交換することを目的とした、標準化された外部ゲートウェイ プロトコルです。BGP を設定することにより、デバイスでは、ネットワーク管理者が設定したパス、ネットワーク ポリシー、またはルールセットに基づいてルーティングを決定できます。

Cisco EPN Manager を使用すると、AS 番号とルータ ID を指定して、BGP ルーティングを設定し、BGP ルーティング プロセスを確立できます。そして、BGP ネイバーを作成できます。これにより、ルータが BGP ルーティングのためにネイバー コンフィギュレーション モードになり、ネイバーの IP アドレスが BGP ピアとして設定されます。BGP ネイバーを設定するには、ネイバーの IPv4 アドレスとそのピア AS 番号を指定する必要があります。BGP ネイバーは BGP ルーティングの一部として設定してください。BGP ルーティングを有効にするには、1 つ以上のネイバーと 1 つ以上のアドレス ファミリを事前に設定しておく必要があります。

デバイスの BGP と BGP ネイバー ルーティング テーブルを表示するには、[デバイス 360（Device 360）] ビューを開き、[操作（Actions）] > [ルーティングテーブル情報（Routing Table Info）] を選択します。

デバイスで BGP ルーティング プロトコルを設定する手順は次のとおりです。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、必要なデバイスを選択します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 [ルーティング（Routing）] > [BGP] を選択します。

（注） クアッドスーパーバイザ仮想スイッチング システム（VSS）を備えた Cisco Catalyst 6500 シリーズ デバイスの設定変更は、このページには動的に反映されません。これらの変更を表示するには、24 時間の定期的なデバイス同期が完了していることを確認してください。または、Cisco EPN Manager でこれらのデバイスを手動で同期することもできます。

ステップ 5 BGP ルーティング プロセスを設定するには、[+] アイコンをクリックします。または、BGP が既に設定されている場合は、AS 番号のハイパーリンクをクリックし、[編集（Edit）] アイコンをクリックして、次の表に示す BGP プロセスの詳細を入力します。

ステップ 6 [保存（Save）] をクリックしてデバイスに変更を展開し、[BGP アドレスファミリ（BGP Address Family）] タブと [BGP ネイバー（BGP Neighbor）] タブを有効にします。

ステップ 7 BGP アドレス ファミリの詳細を設定するには、[BGP アドレスファミリ（BGP Address Family）] タブをクリックし、次の表に示すアドレス ファミリの詳細を選択して、[保存（Save）] をクリックします。

ステップ 8 BGP ネイバーを設定するには、[BGP ネイバー（BGP Neighbor）]タブをクリックし、リストからデバイスの IP アドレスを選択してネイバー デバイスを選択します。

ステップ 9 新しい BGP ネイバーを作成するには、[追加（Add）] アイコン（[+]）をクリックし、次の表に示す詳細を指定します。

ステップ 10 [保存（Save）] をクリックします。更新された BGP ルーティング プロセス値が保存され、選択したデバイスに展開されます。

変更内容が保存されたことを確認するには、[設定（Configuration）] > [ネットワークデバイス（Network Devices）] に移動し、[デバイスの詳細（Device Details）] ページを起動し、[論理ビュー（Logical View）] タブをクリックします。[ルーティング（Routing）] > [BGP] を選択します。ネイバー アドレス（Neighbor Address）、リモート AS（Remote AS）、アドレス ファミリ タイプ（Address Family Type）とモディファイヤ（Modifier）、アドバタイズ間隔時間（Advertise Interval Time）など、デバイスで設定されている BGP 設定の詳細を表示できます。

フィールド	サブフィールド	説明
共通の BGP プロセス フィールド	AS 番号（AS Number）	1 から 4294967295 までの数値を使用して AS 番号を入力します。
	ルータ ID（Router ID）	• ルータ ID を入力します。値には、IPv4 アドレスを次の形式で指定できます。 • A.B.C.D（IPv4 アドレスの場合）。A、B、C、および D は 0～ 255 の整数です。
	ネイバーの変更を記録（Log Neighbor Changes）	ネイバー ルータの変更を追跡する場合に選択します。

フィールド	サブフィールド	説明
BGP アドレス ファミリ フィールド	BGP グローバル AF（BGP Global AF）	• アドレス ファミリ（Address Family）：ルーティング プロセスの BGP アドレス ファミリ プレフィックスを入力します。IPv4 と IPv6（ユニキャスト、マルチキャスト、およびMVPNの場合）、VPNv4 と VPNv6（ユニキャストの場合）、IPv4（MDT の場合）、および L2VPN_EVPN_AF（EVPNベースのサービスの場合）を選択できます。 • ラベルの割り当て（Allocate Label）：ラベル付きユニキャスト アドレス プレフィックスを選択します。 • ラベルの割り当てのカスタム ポリシー名（Allocate Label Custom Policy Name）：ルーティング プロセスに関連付けるカスタム ポリシーを選択します。 （注） [Allocate Label] および [Allocate Label Custom Policy Name] フィールドは、IOS デバイスタイプにのみ適用されます。
	BGP の追加パス（BGP Additional Paths）	パスの詳細を指定します。これらのパスにより、暗黙的に以前のパスから新しいパスに代わることなく、同じピアセッションを介して同じプレフィックスのマルチパスをアドバタイズできます。 • 追加パス（Additional Paths）：デバイスが追加パスを送信、受信、または送受信する必要があるかどうかを選択します。これらはアドレス ファミリ レベルまたはネイバー レベルで行われます。セッションの確立中に、指定した BGP ネイバーが追加パス機能（送信または受信のどちら（あるいは両方）を実行できるか）についてネゴシエートします。 （注） Cisco CAT65000 デバイスの設定時には、追加パスの値として [インストール（Install）] のみ設定できます。 • 最適値（Best Value）：このフィールドは、選択した [追加パス（Additional Paths）] の値が [最適値（Best Value）] フィールドの設定をサポートしている場合にのみ有効になります。
	BGP ネイバー AF（BGP Neighbor AF）	指定した BGP ネイバーが属するアドレス ファミリの詳細を指定します。 • ネイバー アドレス（Neighbor Address）：隣接ルータのルータ ID を選択します。これらの値は [ネイバー（Neighbor）] タブで作成した BGP ネイバーに基づいて設定されます。値には、IPv4 または IPv6 のアドレスを次の形式で指定できます。 • A.B.C.D（IPv4 アドレスの場合）。A、B、C、および D は 0～ 255 の整数です。 • xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx（IPv6 アドレスの場合）。x は 16 進数の値であり、アドレスではコロン（:）で区切られた 4

フィールド	サブフィールド	説明
		つの 16 進数アドレスの 8 セット（セットごとに 16 ビット）を使用します。 • ラベルの送信（Send Label）：ネイバーに関連付ける必要があるラベルのタイプを選択します。 • リフレクタ クライアントのルーティング（Route Reflector Client）：このフィールドでは、ルータを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定できます。 • AIGP：Accumulated Interior Gateway Protocol（AIGP）のパス属性を有効にする場合に選択します。 • コミュニティの送信（Send Community）：コミュニティ属性を外部ボーダー ゲートウェイ プロトコル（eBGP）ネイバーに送信する際に従う送信方法を選択します。 • ネクスト ホップ セルフ（Next Hop Self）：ピアリング セッションを通じてアドバタイズされるルートの BGP ネクスト ホップ属性を、セッションのローカル発信元アドレスに設定する場合に選択します。 • 着信および発信ルート マップ名（Incoming and Outgoing Route Map Name）：ルート ポリシーをネイバーからの着信更新または送信更新に適用する必要があるかどうかを指定する場合に選択します。
	BGP ネットワーク マスク（BGP Network Mask）	• ネットワーク アドレス（Network Address）とネットワーク マスク（Network Mask）：指定した IP アドレスのネットワーク IP アドレスとネットワーク マスクを指定します。 • バック ドア ルート（Back Door Route）：外部ボーダー ゲートウェイ プロトコル（eBGP）のアドミニストレーティブ ディスタンスに、ローカル発信元の BGP ルートのアドミニストレーティブ ディスタンスを設定し、Interior Gateway Protocol（IGP）ルートよりも推奨度を低くすることができます。 • ネットワーク ルート ポリシー名（Network Route Policy Name）：ラベル割り当てのプレフィックスの選択に使用するルート ポリシーを選択します。これにより、BGP において、すべてのグローバル ルート セットまたはフィルター処理されたグローバル ルート セットにラベルを割り当てることができます（ルート ポリシーにより指定）。
[BGP ネイバー（BGP Neighbor）]	-	次の値を指定します。 • ピア AS 番号（Peer AS Number）：1 ～ 4294967295 の整数を使用して自律システム番号の値を入力します。

フィールド	サブフィールド	説明
タブのフィールド		• ネイバー アドレス（Neighbor Address）：設定する BGP ネイバーの IP アドレスを入力します。値には、IPv4 または IPv6 のアドレスを次の形式で指定できます。 • A.B.C.D（IPv4 アドレスの場合）。A、B、C、および D は 0～ 255 の整数です。 • xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx（IPv6 アドレスの場合）。x は 16 進数の値であり、アドレスではコロン（:）で区切られた 4 つの 16 進数アドレスの 8 セット（セットごとに 16 ビット）を使用します。 • ローカル AS 番号（Local AS Number）とアクション（Action）：AS_PATH 属性の先頭に付ける自律システム番号を指定します。値の範囲は、1 ～ 65535 の有効な自律システム番号です。 • 更新元（Update Source）：このオプションを使用して、ピア ルータに最も近いインターフェイスを使用する代わりにループバック インターフェイスを使用してピアの関係（TCP 接続）を確立します。 • フォールオーバー（Fall-over）：値を選択すると、BGP 高速ピアリング セッションの無効化が有効になり、指定した BGP ネイバーの隣接の変更についてコンバージェンスと応答時間が向上します。 • パスワードの暗号化（Password Encryption）とパスワード（Password）：パスワードの暗号化を有効にするかどうかを指定し、有効にした場合はパスワードの値を指定します。 • （表示のみ）ネイバー状態（Neighbor State）：BGP ルーティング プロセスに参加しているネイバーデバイスの接続ステータスを表示します。ステータスは、アイドル（Idle）、接続（Connect）、アクティブ（Active）、オープン送信（Opensent）、オープン確認（Openconfirm）、および確立済み（Established）です。 ネイバーデバイスは、接続ステータスが確立済み（Established）の場合にのみイベントを生成します。デバイスからの更新が生じている場合は、接続状態を頻繁に確認してください。 （注） インベントリが詳細に同期されている間は、ネイバー状態の値は更新されません。更新値を表示するには、同期が正常に終了するまで待ってください。

IS-IS の設定

Intermediate System-to-Intermediate System（IS-IS）プロトコルは、2 レベルの階層を使用して大規模なルーティング ドメイン（管理の目的でエリアに分割される）をサポートする、ドメイン内 OSI 動的ルーティング プロトコルです。1 つのエリア内のルーティングのことと、レベル 1 ルーティングと呼びます。エリア間のルーティングのことを、レベル2ルーティングと呼びます。シスコ ルータで IP の IS-IS を有効にし、他の IS-IS 対応ルータとルーティング情報を交換するには、次のタスクを実行する必要があります。

- デバイスで IS-IS ルーティング プロセスを有効にし、エリアを割り当てます。
- 必要なインターフェイスで IS-IS IP ルーティングを有効にします。

有効な IP アドレスを持つインターフェイスは、レベル 1（エリア内）ルータ、レベル 1_2（レベル 1 ルータとレベル 2 の両方）ルータ、または特定の IS-IS インスタンスのレベル 2（エリア間のみ）ルーティング インターフェイスとして機能するように指定できます。指定したインターフェイス間のルータ間で IS-IS ルーティングの動作が開始されると、IS-IS ネイバーフッドが自動的に生成されます。

（注） IS-IS ルーティングを有効にするには、デフォルトで少なくとも 1 つのアドレス ファミリを設定する必要があります。このリリースでは、Cisco EPN Manager を使用したアドレス ファミリの設定はできません。

デバイスで IS-IS プロセスを設定する手順は次のとおりです。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、IS-IS ルーティング プロトコルを設定するデバイスを選択します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **[ルーティング（Routing）] > [IS-IS]** を選択します。

ステップ 5 新しい IS-IS プロセスを設定するには、[+] アイコンをクリックし、次のパラメータを入力します。

- 英数字のみを使用して [IS-IS プロセス ID（S-IS Process ID）] を指定します。スペースや特殊文字は使用できません。
- [NET ID] を NSAP 形式で指定します。たとえば、49.0001.0000.0001.0010.00 などと指定できます。
  - 49：AFI（権限および形式インジケータ）を表すエリア ID の 1 番目の部分を表します。
  - 0001：エリア ID の 2 番目の部分を表します。
  - 0000.0001.0010：システム ID を表します。
  - 00：N セレクタを表します。常に 0 です。

- [IS-IS タイプ（IS-IS Type）] フィールドで IS-IS ルーティング プロトコルのタイプを指定します。[レベル 1（Level 1）]、[レベル 2（Level 2）]、[レベル 1_2（Level 1_2）] を選択できます。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 選択したデバイスのインターフェイスでこのルーティング プロセスを設定する手順は次のとおりです。

a) **[ルーティング（Routing）] > [IS-IS]** のリストから、上記の手順で作成した IS-IS プロトコル プロセスを選択します。

b) IS-IS プロセス ID のハイパーリンクをクリックします。

c) [IS-IS インターフェイス（IS-IS Interfaces）] タブを使用して、選択した IS-IS 設定を適用するデバイスのインターフェイスを指定します。

- [+] アイコンをクリックして、インターフェイスの詳細を入力します。
- [回路タイプ（Circuit Type）] ドロップダウン メニューから、この設定を適用する回路のタイプを選択します。[レベル 1（Level 1）]、[レベル 2（Level 2）]、[レベル 1_2（Level 1_2）] を選択できます。
- [インターフェイス（Interface）] ドロップダウン メニューで、必要なインターフェイスを選択します。
- （任意）レベル 1 とレベル 2 のメトリックと優先度の値を指定します。[優先度（Priority）] フィールドでは、1 ～ 127 の値を入力します。[メトリック（Metric）] では、1 ～ 16777214 の値を入力します。
- ポイントツーポイント接続を有効にする場合は、[ポイントツーポイント（Point-to-Point）] チェックボックスをオンにします。
- [保存（Save）] をクリックして、選択したインターフェイスに設定を展開します。

ステップ 8 [保存（Save）] をクリックします。選択した IS-IS プロセスが、デバイス上の指定したインターフェイスで設定されます。

ステップ 9 （任意）選択したデバイスに関連付けられている IS-IS ネイバーを表示するには、IS-IS のハイパーリンクをクリックし、[IS-IS ネイバー（IS-IS Neighbors）] タブをクリックします。設定されたネイバーのホスト名、IP アドレス、システム ID、IS-IS タイプ、接続状態、設定済みのホールドダウン時間値、およびローカル インターフェイス名を表示できます。

（注） IS-IS ネイバーのホスト名が 15 の一意の文字を超える場合は、ホスト名が Cisco EPN Manager に表示されません。ホスト名は必ず一意の 15 文字以下にしてください。

ステップ 10 （任意）Cisco EPN Manager を使用して設定した IS-IS ルーティング プロセスを削除する手順は次のとおりです。

a) [設定（Configuration）] > [ネットワークデバイス（Network Devices）] に移動し、[デバイスの詳細（Device Details）] ページを起動し、[ルーティング（Routing）] > [IS-IS] を選択します。

b) リストから必要な IS-IS プロセスを選択します。

c) 削除のための [x] アイコンをクリックし、[OK] をクリックして削除操作を確定します。

OSPF の設定

Open Shortest Path First（OSPF）は各種の標準規格に準拠したルーティング プロトコルであり、最短パス優先（SPF）アルゴリズムを使用して宛先への最適なルートを決定します。OSPF は、同じ設定済みエリア内のすべてのルータにリンク ステート アドバタイズメント（LSA）を送信します。OSPF は、ルーティング テーブル内の変更に関するルーティング アップデートだけを送信します。ルーティング テーブル全体を定期的に送信することはしません。

Cisco EPN Manager を使用して、IPv4 および IPv6 アドレスの OSPF を設定できます。そのためには、ルータ ID、ルータで設定するアドミニストレーティブ ディスタンス、および設定する最大パス値がわかっていることが必要です。

OSPF ルーティング プロセスを設定する手順は次のとおりです。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、OSPF を有効にするデバイスを選択します。IOS-XR デバイスのみを選択します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 [ルーティング（Routing）] > [OSPF] を選択します。

（注） クアッド スーパーバイザ仮想スイッチング システム（VSS）を備えた Cisco Catalyst 6500 シリーズ デバイスの設定変更は、このページには動的に反映されません。これらの変更を表示するには、24 時間の定期的なデバイス同期が完了していることを確認してください。または、Cisco EPN Manager でこれらのデバイスを手動で同期することもできます。

ステップ 5 新しい OSPF プロセスを追加するには、[+] 記号をクリックします。既存の OSPF プロセスを変更するには、プロセス ID のハイパーリンクをクリックして必要なプロセスを選択し、ページの右上隅にある [編集（Edit）] アイコンをクリックします。

ステップ 6 次の表に示すように、共通の OSPF パラメータを指定します。

ステップ 7 [保存（Save）] をクリックします。設定の変更が保存されます。確認するには、[設定（Configuration）] タブをクリックし、**[ルーティング（Routing）] > [OSPF]**を選択して、表示される詳細を確認します。

ステップ 8 [OSPF インターフェイス（OSPF Interfaces）] の設定を指定します。

基本的なプロパティで OSPF プロセスを設定したら、その設定をネットワーク全体または OSPF エリアに直接展開できます。それには、OSPF エリア ID、デバイスのインターフェイスの詳細、ネットワーク タイプなどを指定する必要があります。OSPF インターフェイスの設定を変更する手順は次のとおりです。

a) **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。
b) デバイス名のハイパーリンクをクリックして、設定を変更するデバイスを選択します。
c) [設定（Configuration）] タブをクリックし、[ルーティング（Routing）] > [OSPF] を選択します。
d) プロセス ID のハイパーリンクをクリックして、必要なプロセスを選択します。
e) [OSPF インターフェイス（OSPF Interfaces）] タブをクリックします。
f) [追加（Add）]アイコン（[+]）をクリックして、選択したデバイスの OSPF プロセスに関連付けられたインターフェイスに新しい設定を追加します。既存の値を編集するには、インターフェイス名のハイパーリンクをクリックし、ページの右上にある [編集（Edit）] アイコンをクリックします。

g) 次の表に示すように、パラメータを指定します。
h) [保存（Save）] をクリックして、変更内容をデバイスに展開します。

オプション	説明
OSPF の共通のプロパティ	**説明**
プロセス ID（Process ID）	選択した OSPF プロセスを識別する 1 ～ 65535 の一意の数値。
ルータ ID（Router ID）	エリア 0 ルータのルータ ID。
コスト（Cost）	ネットワーク全体のパケット送信コストを設定します。この値は、OSPF ルータによる最短パスの計算に使用されます。これは Cisco IOS-XE デバイスでは有効になりません。 1 ～ 65535 の数値を入力します。
トポロジの優先順位（Topology Priority）	サブネット用に指定されたルータを表示します。1 ～ 255 の数値を入力します。
ルートあたりの最大パス数（Maximum number of paths per route）	ルータがルートごとの負荷分散に使用できるパスの最大数を定義します。デフォルト値は 4 です。1 ～ 64 の数値を設定できます。
アドミニストレーティブ ディスタンス（Administrative Distance）	パスの選択に設定する距離を指定します。デフォルト値は 110 で、使用可能な値は 1 ～ 255 です。
外部エリア ディスタンス（External Area Distance）	外部タイプ 5 およびタイプ 7 のルートの距離を指定します。1 ～ 255 の数値を選択できます。
エリア間ディスタンス（Inter Area Distance）	1 ～ 255 の値を使用して、エリア間ルートのエリア間距離を指定します。
エリア内ディスタンス（Intra Area Distance）	1 ～ 255 の値を使用して、エリア内ルートのエリア内距離を指定します。
ルーティング（Routing）> OSPF > OSPF インターフェイス（OSPF Interface）/PEP プロパティ（PEP Properties）	**説明**
エリア ID（Area ID）	0 ～ 4294967295 の整数を使用して、NE の OSPF エリア ID を指定します。 ID を 0.0.0.0 にすることはできません。
インターフェイス名（Interface Name）	指定した OSPF インターフェイス/PEP 設定を関連付ける必要があるデバイスのインターフェイス。
インターフェイス コスト（Interface cost）	ネットワーク全体のパケット送信のコスト。このコストは、OSPF ルータによる最短パスの計算に使用されます。
インターフェイス プライオリティ（Interface Priority）	サブネット用に指定されたルータ。

オプション	説明
ネットワーク タイプ（Network Type）	OSPFプロセスに関連付けられたネットワークのタイプ。ブロードキャスト（Broadcast）、NBMA、ポイントツーポイント（Point to Point）、およびポイントツーマルチポイント（Point to Multipoint）を選択できます。
dead 間隔（Dead Interval）	OSPF ルータのパケットが表示されなくなってから、ネイバールータがそのルータのダウンを宣言するまでの秒数。シスコのデフォルトは 40 秒です。
Hello 間隔（Hello Interval）	OSPF ルータが送信する OSPF hello パケット アドバタイズメントの間隔の秒数。シスコのデフォルトは 10 秒です。
再送信間隔（Retransmit Interval）	パケットが再送信される前に経過する時間。シスコのデフォルトは 5 秒です。
送信遅延（Transmit Delay）	サービス速度。シスコのデフォルトは 1 秒です。

スタティック ルーティングの設定

スタティック ルーティングは最も単純な形式のルーティングで、ネットワーク管理者が手動でルーティング テーブルにルートを入力します。ルートは、ネットワーク管理者が変更しない限り変わりません。スタティック ルーティングは通常、設定するデバイスが非常に少なく、ルートが変わらないことを管理者が確信している場合に使用します。スタティック ルーティングの主な欠点は、接続が切断されるたびに、手動で設定したルートを更新して修正する必要があるため、ネットワーク トポロジの変更または外部ネットワークの障害に対処できないことです。

ステップ 1 選択項目 **Configuration > Network Devices.**

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **Routing > Static** を選択します。

ステップ 5 スタティック ルーティングを設定するには、**Add** をクリックします。

a) IPv4 スタティックルートを追加する場合は、[IPv4 スタティックルート（IPv4 Static route）] 領域で、[追加（+）（Add（+））] アイコンをクリックします。次のフィールドに必要な詳細情報を入力します。

[宛先ネットワーク（Destination Network）]、[ネットワークマスク（Network Mask）]、[ネクストホップ IP（Next Hop IP）]、[発信インターフェイス（Outgoing Interface）]、[永続的ルート（Permanent Route）]、または [アドミニストレーティブ ディスタンス（Administrative Distance）]。

b) IPv6 スタティックルートを追加する場合は、[IPv6 スタティックルート（IPv6 Static route）] 領域で、[追加（+）（Add（+））] アイコンをクリックします。次のフィールドに必要な詳細情報を入力します。

[宛先 IPv6 プレフィックス（Destination IPv6 Prefix）]、[プレフィックス長（Prefix Length）]、[ネクストホップ IPv6 アドレス（Next Hop IPv6 Address）]、[発信インターフェイス（Outgoing interface）]、[アドミニストレーティブ ディスタンス（Administrative Distance）]、[キャストタイプ（Cast Type）]、または [タグ値（Tag Value）]。

ステップ 6 **Save** をクリックします。

ACL の設定

[デバイスの詳細（Device Details）] ページの [設定（Configuration）] タブには、デバイスでの現在の CFM 設定のリストが表示されます。デバイス設定とユーザー アカウントの権限に応じて、デバイスで ACL を設定できます。

ACL を設定する手順は次のとおりです。

ステップ 1 選択項目 **Configuration > Network Devices.**

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細（Device Details）] ページを起動します。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **Security > ACL** を選択します。

ステップ 5 ACL に次のパラメータを指定します。

a) 名前（Name）/番号（Number）：ACL の一意の識別子を指定します。英数字、ハイフン、および下線を使用できます。

b) タイプ（Type）：ACL のタイプが標準か拡張かを指定します。選択したデバイスのタイプによってはこのドロップダウン メニューが非表示になります。たとえば、Cisco IOS-XR デバイスではこのドロップダウン メニューは非表示になります。

c) （任意）説明（Description）：ACL に関する参照用の説明を入力します。

ステップ 6 **Save** をクリックして値を Cisco EPN Manager に保存します。この操作ではデバイスに変更が展開されません。

ステップ 7 上記の手順で作成した ACL の横にあるドロップダウン アイコンをクリックし、次の ACE 値を指定します。

a) [行の追加（Add Row）] をクリックして新しい ACE を追加します。または、既存の ACE を選択し、[編集（Edit）] をクリックして、[アクション]（[許可（Permit）] または [拒否（Deny）]）、[ソース IP（Source IP）]、[宛先 IP（Destination IP）] を指定し、必要に応じて、ACE に関連付ける必要があるワイルド カード ソース、ポート情報、および説明を指定します。

b) [保存（Save）] をクリックして、ACE に関連付けられた値を保存します。

c) 上下矢印（ボタン）を使用して、選択した ACL についてデバイスに ACE を適用する順序を指定します。

ステップ 8 上記の手順で作成した ACL を選択し、[インターフェイスに適用（Apply to Interface）] をクリックして、この ACL を適用する必要があるインターフェイスを指定します。

ステップ 9 [OK] をクリックして、デバイスの選択したインターフェイスに、指定した ACL 値を展開します。

セグメント ルーティングの設定

セグメントルーティング（SR）では、送信元ルーティングの概念を使用します。送信元ルーティングでは、送信元が明示的パスまたは内部ゲートウェイプロトコル（IGP）最短パスのいずれかを選択し、パケットヘッダー内のパスをセグメントの順序付きリストとしてエンコードします。セグメントは、ネットワークの宛先への完全なルートを形成するためにルータが組み合わせることができるサブパスです。各セグメントは、新しい IGP 拡張機能を使用してネットワーク全体に配布されるセグメント識別子（SID）で識別されます。

Cisco EPN Manager GUI では、次のセグメント ルーティング サブメニュー オプションを使用して、デバイスのセグメント ルーティング パラメータを設定できます。また、CLI から設定されたセグメントルーティング設定を表示または編集することもできます。

- セグメント設定の構成
- ルーティングプロセスの設定
- PCE サーバーの設定
- パス計算クライアント（PCC）の設定
- アフィニティの設定
- オンデマンドポリシーの設定

次の表に、UI からセグメントルーティングパラメータを設定できるデバイス、およびサポートされているソフトウェアバージョンを示します。

デバイスシリーズおよびタイプ	ソフトウェア バージョン
NCS 540	6.5.3、6.6.1、7.0.1、7.1.1
NCS 560	6.5.3、6.6.1、7.0.1、7.1.1
NCS 5500	6.5.3、6.6.1、7.0.1、7.1.1
ASR 9000	6.5.3、6.6.1、7.0.1、7.1.1

セグメント設定の構成

選択したデバイスのセグメントルーティングのグローバル設定を構成するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、セグメントルーティングを設定するデバイスを選択します。

ステップ 3 左側のタブで、[Logical View] をクリックします。

ステップ 4 **[Segment Routing] > [Segment Settings]** を選択します。

ステップ 5 [General] タブで、[+] アイコンをクリックして必要な値を入力し、[Save] をクリックします。既存の設定を編集するには、対応するハイパーリンクをクリックします。

属性	説明
Global Block Min	セグメント ルーティング グローバル ブロック（SRGB）は、ラベルスイッチデータベースでセグメントルーティング用に保存されているラベル値の範囲です。SRGB ラベル値は SR 対応ノードにプレフィックスセグメント識別子（SID）として割り当てられ、ドメイン全体で有効です。 16000 ～ 1048575 の範囲で値を入力します。
Global Block Max	
Local Block Min	セグメント ルーティング ローカル ブロック（SRLB）は、隣接関係セグメント識別子（adj-SID）の手動割り当てのために保存されているラベル値の範囲です。これらのラベルはローカルで重要であり、ラベルを割り当てるノードでのみ有効です。 15000 ～ 1048575 の範囲で値を入力します。
Local Block Max	
Binding SID	ドロップダウン リストから値を選択します。
最大 SID 深度	ノードまたはノード上のリンクによってサポートされている SID の数。1 ～ 255 の範囲で値を入力します。

（注） 次のコマンドを実行して、SRGB または SRLB の変更が有効になるように、ラベルの不一致をクリアします。

```
#clear segment-routing local-block discrepancy all
```

ステップ 6 [Mapping Server] タブで、[+] をクリックして必要な値を入力し、[Save] をクリックします。[OK] をクリックして、変更をデバイスにプッシュすることを確認します。既存の設定を削除するには、対応するチェックボックスをオンにして [X] をクリックします。

属性	説明
IP Address Prefix	IPv4 アドレスを入力します。
Mask	サブネットマスクの詳細を入力します
アドレス ファミリ（Address Family）	アドレスファミリを IPv4 として選択します。
Start of SID Range	0 ～ 1048575 の範囲で値を入力します。
Number of Allocated SIDs	0 ～ 1048575 の範囲で値を入力します。デフォルト値は 1 です。

ステップ 7 [Adjacency SID Mapping] タブで、[+] をクリックして必要な値を入力し、[Save] をクリックします。[OK] をクリックして、変更をデバイスにプッシュすることを確認します。既存の設定を削除するには、対応するチェックボックスをオンにして [X] をクリックします。

属性	説明
インターフェイス（Interface）	ループバック インターフェイスをドロップダウンリストから選択します。
アドレス ファミリ（Address Family）	アドレスファミリを IPv4 として選択します。
ネクスト ホップ アドレス	ネクストホップの IPv4 アドレスを入力します。
SID Mapping Type	マッピングタイプとして、[Absolute] または [Index] のいずれかを選択します。
SID Value	SID 値の有効範囲は SID マッピングタイプによって異なります。 • [Index] タイプの場合：0 ～ 1048575 • [Absolute] タイプの場合：15000 ～ 1048575

ルーティングプロセスの設定

選択したデバイスのセグメントルーティングのルーティング プロセス パラメータを設定するには、次の手順を実行します。

始める前に

ルーティング プロセス パラメータを設定する前に、**[論理的ビュー（Logical View）]** > **[ルーティング（Routing）]** ページで、デバイスに対して OSPF および ISIS ルーティングプロセスを設定したことを確認します。詳細については、「ルーティングプロトコルとセキュリティの設定 （524 ページ）」を参照してください。

（注） Cisco EPN Manager は、セグメントルーティングで OSPFV3 プロトコルをサポートしていません。

ステップ 1 **[設定（Configuration）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。

ステップ 3 左側のタブで、[Logical View] をクリックします。

ステップ 4 **[Segment Routing] > [Routing Process]** をクリックします。

ステップ 5 対応するハイパーリンクをクリックし、[Save] をクリックして、各タブで必要に応じて属性の値を入力します。

タブ	属性	説明
プロパティ（Properties）	プロセス ID（Process ID）	このフィールドには、デバイスに対して設定されているプロセス ID が自動的に入力されます。
	Process Type	このフィールドは、デバイスの設定に基づいて ISIS または OSPF として自動的に入力されます。
	Global Block Min	デフォルトの SRGB の範囲は 16000 ～ 23999 です。ここで入力した値は、[Segment Settings] で設定されたグローバル値を上書きします。
	Global Block Max	
	Advertise Local Prefix SID Mapping	このフィールドは、デフォルトで有効になっています。
	Override LDP Labels	LDP ラベルを上書きするには、このチェックボックスをオンにします。
	Receive Remote Prefix SID Mapping	リモートプレフィックス SID マッピングを受信するには、このチェックボックスをオンにします
	Avoid Microloop	マイクロループを回避するには、このチェックボックスをオンにします。

タブ	属性	説明
Connected Prefix SID Mapping	Ip Address Prefix	IPv4 アドレスを入力します
	Mask	サブネットマスクの詳細を入力します
	SID Mapping Type	ドロップダウンリストから、[Absolute] または [Index] マッピングタイプのいずれかを選択します。
	SID Value	SID 値の有効範囲は SID マッピングタイプによって異なります。 • [Index] タイプの場合：0 ～ 1048575 • [Absolute] タイプの場合：16000 ～ 1048575
	Flex Algorithm	128 ～ 255 の範囲の Flex アルゴリズム値を入力します。[Strict SPF] が有効になっている場合、このフィールドはグレー表示されます。
	Strict SPF	必要に応じてチェックボックスをオンにします。
	Replace Prefix SID with Explicit Null	必要に応じてチェックボックスをオンにします。

タブ	属性	説明
Interface Prefix SID Mapping	SID Mapping Type	ドロップダウンリストから、[Absolute] または [Index] マッピングタイプのいずれかを選択します。
	SID Value	SID 値の有効範囲は SID マッピングタイプによって異なります。 • [Index] タイプの場合：0 ～ 1048575 • [Absolute] タイプの場合：16000 ～ 1048575
	Strict SPF	必要に応じてチェックボックスをオンにします。
	Replace Prefix SID with Explicit Null	必要に応じてチェックボックスをオンにします。

（注）
- ISIS ルーティングプロセスの場合は、接続されたプレフィックスまたはローカルプレフィックスのいずれかを設定できます。OSPFルーティングプロセスの場合は、ローカルプレフィックス SID 設定のみがサポートされます。
- ローカルプレフィックス SID を設定する場合、IP が設定されているループ バック インターフェイスのみが [ルーティングプロセス（Routing Process）] でモデル化されます。
- ローカルプレフィックス SID の場合、デバイスは次の設定をサポートしています。
  - prefix-sid index/absolute 100 explicit-null（algorithm/strict-spf がない prefix-sid）
  - prefix-sid algorithm 128 index /absolute 16000（algorithm がある prefix-sid）
  - prefix-sid strict-spf index/absolute 200 explicit-null（strict-spf がある prefix-sid）

パス計算クライアント（PCC）の設定

選択したデバイスの PCC クライアントパラメータを設定するには、次の手順を実行します。

始める前に

- PCC は、EPNM で表示および変更するために事前に検出する必要があるワンタイム設定です。

  設定例

```
segment-routing
traffic-eng
pcc
```

- PCC ピアイベントを受信するには、segment-routing traffic-eng logging の下で、pcep peer-status logging を使用してデバイスを有効にする必要があります。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。

ステップ 3 左側のタブで、[Logical View] をクリックします。

ステップ 4 **[Segment Routing]** > **[PCC]** をクリックします。

ステップ 5 対応するハイパーリンクをクリックし、[Save] をクリックして、各タブで必要に応じて属性の値を入力します。[Ok] をクリックして、変更をデバイスにプッシュすることを確認します。

タブ	属性	説明
PCC	Source Address	IPv4 アドレスを入力します。
	Report All	この値を True に設定するには、このチェックボックスをオンにします。
	PCC Centric Model	この値を True に設定するには、このチェックボックスをオンにします。
	Session Dead time	単位は秒です。 0 ～ 255 の範囲の値を入力します。
	Session Keepalive Time	単位は秒です。 0 ～ 255 の範囲の値を入力します。このパラメータを無効にする場合は、0 を入力します。
	Delegated Policy Up Time	単位は秒です。 0 ～ 3600 の値を入力します。このパラメータを無効にする場合は、0 を入力します。
	PCE Initiated Orphan State Time	15 ～ 14400 の範囲の値を入力します。
	PCE Initiated Policy Delegation Time	10 ～ 180 秒の範囲の値を入力します。

タブ	属性	説明
PCC's Peer Database	PCE Address	IPv4 アドレスを入力します。
	Precedence	0 ～ 255 の範囲の値を入力して優先度を設定します。0 が最も優先度が高く、255 が最も優先度が低くなります。
	[Password]	クライアント/サーバー認証のパスワード（クリアテキストパスワード）とキーチェーンの詳細を入力します。
	Keychain	

PCE サーバーの設定

選択したデバイスを PCE サーバーとして設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。

ステップ 3 左側のタブで、[Logical View] をクリックします。

ステップ 4 **[Segment Routing]** > **[PCE Server]** をクリックします。

ステップ 5 [+] をクリックして必要な値を入力し、[Save] をクリックします。[Ok] をクリックして、変更をデバイスにプッシュすることを確認します。

タブ	属性	説明
PCE Sever	IPアドレス	IPv4 アドレスを入力します。
	State Sync Address	複数の IPv4 アドレスをカンマで区切って入力します。
	Keepalive Time	単位は秒です。 0～255 の範囲の値を入力します。デフォルト値は 30 です。このパラメータを無効にするには 0 を入力します。
	[Password]	クライアント/サーバーの詳細を認証するためのパスワード（クリアテキスト）を入力します。
	Minimum Peer Keepalive Interval	単位は秒です。 0 ～ 255 の範囲の数値を入力します。デフォルト値は 20 です。このパラメータを無効にするには 0 を入力します。
	Strict SIDs Only	このオプションを有効にするには、チェックボックスをオンにします。このオプションは、デフォルトで無効になっています。
	Topology Reoptimization Interval	単位は秒です。 600 ～ 86400 の範囲の値を入力します。デフォルト値は 1800 です。

（注） デバイスとネットワークの制限により、一度設定した PCE サーバーは削除できません。

アフィニティの設定

選択したデバイスのセグメントルーティングのアフィニティパラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。

ステップ 3 左側のタブで、[Logical View] をクリックします。

ステップ 4 **[Segment Routing]** > **[Affinity]** を選択します。

ステップ 5 [+]アイコンをクリックして必要な値を入力し、[Save] をクリックします。[OK] をクリックして、変更をデバイスにプッシュすることを確認します。編集するには、対応するハイパーリンクをクリックします。既存の設定を削除するには、対応するチェックボックスをオンにして [X] をクリックします。

タブ	属性	説明
アフィニティ	Affinity Name	アフィニティ属性の名前を入力します。
	ビット位置	0～255 の範囲の値を入力します。
Affinity Mapping	Interface Name	ドロップダウンリストからループバックインターフェイスを選択して、インターフェイスをアフィニティに関連付けます。少なくとも 1つのアフィニティをインターフェイスに関連付ける必要があります。
	Affinity Name	インターフェイスに関連付けるアフィニティをドロップダウンリストから選択します。 1 つのインターフェイスに複数のアフィニティを関連付けることができます。
	Metric value	0 ～ 2147485647 の範囲の値を入力します

オンデマンドポリシーの設定

選択したデバイスのセグメントルーティングのオンデマンド ポリシー パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。

ステップ 3 左側のタブで、[Logical View] をクリックします。

ステップ 4 **[Segment Routing]** > **[On-Demand Policy]** をクリックします。

ステップ 5 [+]アイコンをクリックして必要な値を入力し、[Save] をクリックします。[OK] をクリックして、変更をデバイスにプッシュすることを確認します。編集するには、対応するハイパーリンクをクリックします。既存の設定を削除するには、対応するチェックボックスをオンにして [X] をクリックします。

タブ	属性	説明
オンデマンドポリシーテンプレート	カラー	1 ～ 4294901295 の範囲で値を入力します。
	Bandwidth	1 ～ 4294967295（kbps）の範囲で値を入力します。
	Path type	ドロップダウンリストから値を選択します。
	SID の上限（Max SID Limit）	1 ～ 255 の範囲で値を入力します。
	Metric Margin Mode	ドロップダウンリストから値を選択します。
	メトリック タイプ	ドロップダウンリストからメトリックタイプを選択します。
	メトリックマージン値（Metric Margin Value）	0 ～ 2147483647 の範囲の値を入力します。
Flex Algorithm	カラー	このフィールドには、[On-Demand Policy Template] タブに入力した値が自動的に入力されます。
	Flex Algorithm	128 ～ 255 の範囲でプレフィックス SID アルゴリズム値を入力します。
Disjoint Path	カラー	このフィールドには、[On-Demand Policy Template] タブに入力した値が自動的に入力されます。
	Group Id	1 ～ 65535 の値を入力します。
	Disjointness Type	ドロップダウンリストを使用して値を選択します。
	Sub Group Id	1 ～ 65535 の値を入力します。

セグメント ルーティング ポリシーを設定するには、「セグメント ルーティング ポリシーの作成とプロビジョニング （658 ページ）」を参照してください。

EOAM の障害とパフォーマンスのモニターリングを設定する

Cisco EPN Manager を使用すれば、キャリア イーサネット サービスのモニターリングとトラブルシューティングに EOAM（Ethernet Operations, Administration and Management）プロトコルを使用するようにネットワーク内のデバイスを設定することができます。また、Cisco EPN Manager 内の事前定義のテンプレートとして使用可能な CLI コマンドのセットを使用して、イーサネットサービスに対して接続テストとパフォーマンステストを実行するできます。

CFM の設定

CFM 設定では、EOAM プロトコルを使用してキャリア イーサネット サービスのモニターリングとトラブルシューティングを行うためのステージを設定します。新規キャリアイーサネット EVC の作成およびプロビジョニング（641 ページ）で説明しているように、EVC を作成およびプロビジョニングするときに CFM を EVC レベルで設定することもできます。

CFM を設定すると、個々のデバイスについて CFM の設定をすばやく簡単に表示できるようになります。

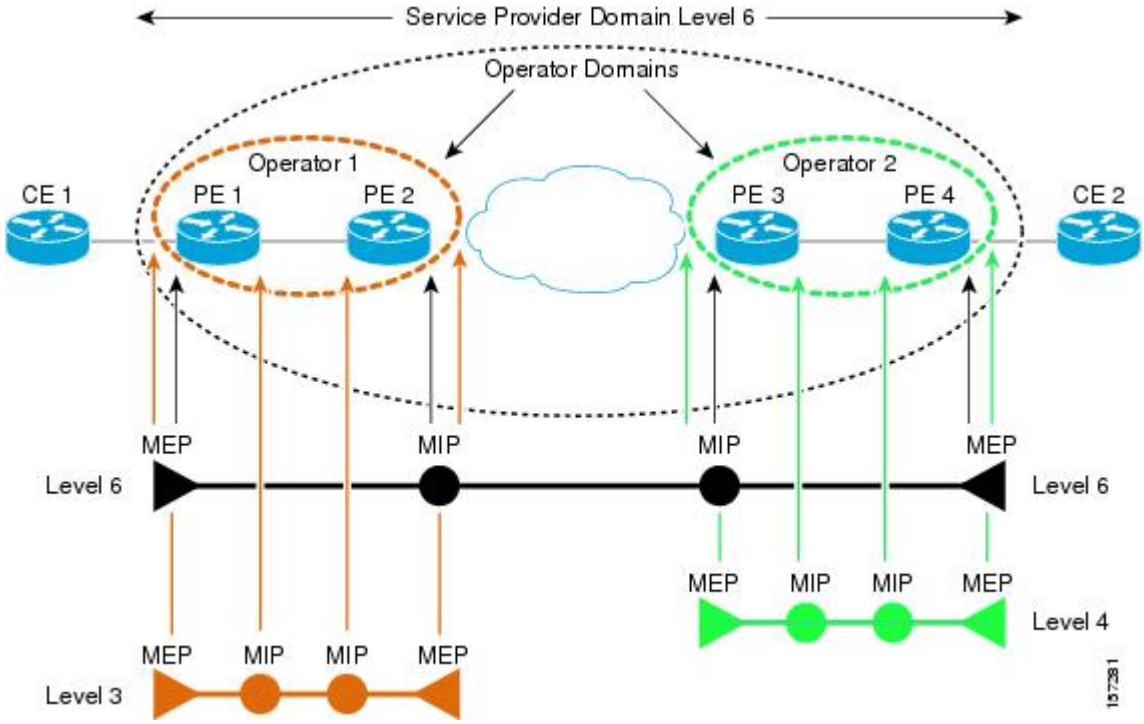
CFM の概要

IEEE 接続障害管理（CFM）は、サービスごとのエンドツーエンド イーサネット レイヤの運用、管理、保守（OAM）プロトコルです。CFM には、大規模イーサネット メトロポリタンエリア ネットワーク（MAN）および WAN の予防的な接続モニターリング、障害検証、および障害分離の機能が含まれています。

CFM は、サービス VLAN 単位（または EVC 単位）で動作します。EVC に障害が発生したかどうかを知ることができ、発生した障害を迅速に切り分けるツールが用意されています。

CFM 対応ネットワークは、以下で説明するように、メンテナンス ドメイン、CFM サービス、およびメンテナンス ポイントで構成されます。

図 *12 : CFM* メンテナンス ドメイン



メンテナンス ドメイン

イーサネット CFM は、任意のサービス プロバイダ ネットワーク内にあり、階層型メンテナンス ドメインで構成される機能モデルに依存しています。メンテナンス ドメインは、シングル エンティティにより所有および運用が行われ、一連の内部境界ポートにより定義される、ネットワーク上の管理空間です。ドメインは一意のメンテナンス レベルに割り当てられ、これによりドメインの階層関係が定義されます。複数のメンテナンス ドメインのネストまたは接触は許されますが、交差はできません。2 つのドメインがネストする場合、外側のドメインはそれに含まれるドメインより上位のメンテナンス レベルでなければなりません。1 台のデバイスが複数のメンテナンス ドメインに参加する場合もあります。

CFM サービス

CFM サービス（メンテナンスの関連付け）により、ネットワーク内の接続に応じて CFM メンテナンス ドメインを分割することが可能になります。たとえば、ネットワークがいくつかの仮想 LAN（VLAN）に分割されている場合、CFM サービスはそれぞれに作成されます。CFM は、各サービスに個別に実行できます。CFM サービスは、常にメンテナンス ドメインに関連付けられ、そのメンテナンス ドメイン内で動作するため、そのドメインのメンテナンス レベルに関連付けられます。サービス関連の CFM フレームはすべて、関連付けられたメンテナンス ドメインのメンテナンス レベルを伝送します。ドメイン内には多数の CFM サービスが存在する可能性があります。MEP を設定するには、あらかじめ CFM サービスをドメインで設定しておく必要があります。

メンテナンス ポイント

メンテナンス ポイントは、CFM メンテナンス ドメインに参加するインターフェイスの境界を定めるものです。メンテナンス ポイントは、特定のインターフェイス上の特定の CFM サービスのインスタンスになります。CFM は、インターフェイスに CFM メンテナンス ポイントが存在する場合にのみ、そのインターフェイス上で動作します。メンテナンス ポイントは、特定の CFM サービスに常に関連付けられるため、特定のレベルの特定のメンテナンス ドメインに関連付けられます。メンテナンス ポイントは、関連するメンテナンス ドメインと同じレベルの CFM フレームを一般的に処理するだけです。下位メンテナンス レベルのフレームは通常ドロップされますが、上位のメンテナンス レベルのフレームは常に透過的に転送されます。これはメンテナンス ドメイン階層の適用に役立ち、特定のドメインの CFM フレームがドメインの境界を越えてリークできないようになります。メンテナンス ポイントには次の 2 種類があります。

- メンテナンス エンド ポイント（MEP）：ドメインのエッジに作成されます。CFM メッセージをドメイン内に制限する役割があります。メンテナンス エンド ポイント（MEP）は、ドメイン内の特定のサービスのメンバで、CFM フレームを送信および受信する役割があります。これらは定期的に連続性チェック メッセージを送信し、ドメイン内の他の MEP から同様のメッセージを受信します。また、管理者の要求に応じて traceroute メッセージやループバック メッセージも送信します。
- メンテナンス中間ポイント（MIP）：ドメイン内部のポイントです。MIP は CFM パケットを転送しますが、MEP は CFM パケットをドメイン内に保持する必要があるため、CFM パケットを転送しません。MEP とは異なり、MIP はインターフェイスごとに明示的に設定されません。MIP は、CFM 802.1ag 規格で指定されたアルゴリズムに従って自動的に作成されます。

CFM メンテナンスドメインとメンテナンスの関連付け（サービス）の表示

デバイスの CFM 設定を表示するには、次の手順を実行します。

ステップ 1 左側のサイドバーから **Inventory > Network Devices** を選択します。

ステップ 2 デバイスのリストで必要なデバイスを見つけ、デバイス名のハイパーリンクをクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 **EOAM > CFM** を選択します。

EOAM の接続チェックとパフォーマンス チェックの実行

Cisco EPN Manager では、EOAM 関連の定義済みの設定テンプレートが提供されています。これらを使用して、キャリア イーサネット ネットワーク内の仮想接続（VC）について接続とパフォーマンスをモニターリングできます。

これらのテンプレートを使用するには、左側のサイドバーから **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選

択し、**[CLI テンプレート（CLI Templates）]**> **[システム テンプレート - CLI（System Templates - CLI）]** を選択します。

次の表に、使用可能な EOAM 設定テンプレートと、その目的、および指定する必要がある必須入力パラメータを示します。

（注） テンプレートの展開の結果や出力を確認するには、変更の展開時に表示されるジョブの詳細を確認します。

表 *29 : EOAM* テンプレート

テンプレート名	用途	必須入力値	その他の情報
EOAM-CCDB-Content-IOS	CFM の動作を確認するため、またはネットワークでの EOAM の設定状況を確認するために、メンテナンス中間ポイント（MIP）の連続性チェックデータベース（CCDB）の内容を表示します。	どのフィールドも必須ではありません。 **Domain ID:** メンテナンス ドメインを識別する方法を選択し、対応するフィールドに値を入力します。 **Service:** ICC MEG 識別子、VLAN ID、または VPN ID に基づいて、ドメイン内のメンテナンス アソシエーションを指定します。	
EOAM-CCDB-Content-IOS-XR	CFM の動作を確認するため、またはネットワークでの EOAM の設定状況を確認するために、メンテナンス中間ポイント（MIP）の連続性チェックデータベース（CCDB）の内容を表示します。	どのフィールドも必須ではありません。 **Node ID:** ラック/スロット/モジュールの表記に入力された、指定されたノードの CFM CCM 学習データベース。	
EOAM-CFM-Ping-IOS および EOAM-CFM-Ping-IOS-XR	CFM ループバック メッセージを使用して、宛先 MIP または MEP への接続を確認します。	**Ping Destination Type:** 宛先 MEP を MAC アドレスまたは MEP ID で識別します。宛先 MEP が複数ある場合は、[マルチキャスト（Multicast）] を選択します。 宛先 MEP のメンテナンス ドメイン名（Maintenance domain name for destination MEP）：宛先 MEP が存在するドメインの名前。	

テンプレート名	用途	必須入力値	その他の情報
EOAM-CFM-Traceroute-IOS	IOS デバイス（IOS devices）：宛先 MEP までルートをトレースし、ホップの数とホップ間の接続を確認します。	**Destination Type:** MAC アドレス、MEP ID、または explore のオプションで宛先 MEP を識別します。 **Maintenance domain name for destination MEP:** 宛先 MEP が存在するドメインの名前。 **Service Type:** ドメイン内のメンテナンス アソシエーション（MA）を名前、ITU キャリア コード（ICC）、MA 番号、VLAN ID、または VPN ID のいずれかで識別します。	
EOAM-CFM-Traceroute-IOS-XR	IOS-XR デバイス（IOS-XR devices）：宛先 MEP までルートをトレースし、ホップの数とホップ間の接続を確認します。	**Maintenance domain name for destination MEP:** 宛先 MEP が存在するドメインの名前。 **Service Name:**指定されたメンテナンス ドメイン内のメンテナンスアソシエーション（MA）によってモニターリングされるサービス インスタンスの名前。 **Destination Type:** MAC アドレス、MEP ID、または explore のオプションのいずれかで宛先 MEP を識別します。 **Source MEP ID:** ドメイン内のメンテナンス アソシエーション（MA）を名前、ITU キャリア コード（ICC）、MA 番号、VLAN ID、または VPN ID のいずれかで識別します。 **Source Interface Type:** ローカルに定義された CFM MEP のソースインターフェイス タイプ。 **Interface Path ID:** 物理または仮想インターフェイス名。	

テンプレート名	用途	必須入力値	その他の情報
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Loopback-IOS-XR	CFM ループバックのオンデマンド イーサネット SLA 動作を設定します。デフォルトでは、双方向の遅延とジッタを測定します。	**Probe Domain:** プローブを有効にする場合にチェックボックスをオンにします。 **Domain Name:** ローカルに定義された CFM MEP のメンテナンス ドメインの名前。 **Domain Interface Type:** ローカルに定義された CFM MEP のソース インターフェイス タイプ。 **Domain Interface Path ID:** 物理または仮想インターフェイス名。 **Domain MAC Address or MEP-ID:** ドメインを MAC アドレスで識別するか MEP ID で識別するかを選択し、以下の関連するフィールドに必要な情報を入力します。MEP ID の場合は、1 から 8191 までの ID を入力します。	必要に応じて、測定する統計のタイプ、集計タイプにビンを使用するかどうか、プローブの頻度と期間の値などを指定できます。指定した値によってデフォルトのアクションがオーバーライドされます。
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Synthetic-Loss-Measurement-IOS-XR	CFM の合成損失測定のオンデマンド イーサネット SLA 動作を設定します。デフォルトでは、両方の方向について一方向フレーム損失率（FLR）を測定します。	**Probe Domain:** プローブを有効にする場合にチェックボックスをオンにします。 **Domain Name:** ローカルに定義された CFM MEP のメンテナンス ドメインの名前。 **Domain Interface Type:** ローカルに定義された CFM MEP のソース インターフェイス タイプ。 **Domain Interface Path ID:** 物理または仮想インターフェイス名。 **Domain MAC Address or MEP-ID:** ドメインを MAC アドレスで識別するか MEP ID で識別するかを選択し、以下の関連するフィールドに必要な情報を入力します。MEP ID の場合は、1 から 8191 までの ID を入力します。	必要に応じて、測定する統計のタイプ、集計タイプにビンを使用するかどうか、プローブの頻度と期間の値などを指定できます。指定した値によってデフォルトのアクションがオーバーライドされます。

テンプレート名	用途	必須入力値	その他の情報
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Delay-Measurement-IOS-XR	CFM の遅延測定のオンデマンドイーサネット SLA 動作を設定します。デフォルトでは、両方の方向について一方向の遅延とジッタ、および双方向の遅延とジッタを測定します。	**Probe Domain:** プローブを有効にする場合にチェックボックスをオンにします。 **Domain Name:** ローカルに定義された CFM MEP のメンテナンス ドメインの名前。 **Domain Interface Type:** ローカルに定義された CFM MEP のソースインターフェイスタイプ。 **Domain Interface Path ID:** 物理または仮想インターフェイス名。 **Domain MAC Address or MEP-ID:** ドメインを MAC アドレスで識別するか MEP ID で識別するかを選択し、以下の関連するフィールドに必要な情報を入力します。MEP ID の場合は、1 から 8191 までの ID を入力します。	必要に応じて、測定する統計のタイプ、集計タイプにビンを使用するかどうか、プローブの頻度と期間の値などを指定できます。指定した値によってデフォルトのアクションがオーバーライドされます。

テンプレート名	用途	必須入力値	その他の情報
EOAM-Configure-Y-1731-PM-Direct-On-Demand-IOS	イーサネット サービスのリアルタイム トラブルシューティングをダイレクト モードで実行します。ダイレクト モードでは、動作が作成されて直ちに実行されます。	フレーム タイプ（Frame Type）：DMMv1（フレーム遅延）または SLM（フレーム損失）のいずれかのフレーム タイプ。 ドメイン名（Domain Name）：ローカルに定義された CFM MEP のメンテナンス ドメインの名前。 EVC または VLAN：テストを実行する EVC または VLAN を識別します。VLAN ID には 1 ～ 4096 を指定できます。 ターゲット MPID（Target MPID）または MAC アドレス（MAC Address）：宛先の MEP を、MPID（1 ～ 8191）または MAC アドレスのいずれかで識別します。 CoS 値（CoS Value）：指定した MEP の CFM メッセージに適用されるサービス クラス レベル（0 ～ 7）。 ローカル MPID（Local MPID）または MAC アドレス（MAC Address）：ソースの MEP を、MPID（1 ～ 8191）または MAC アドレスのいずれかで識別します。 バースト（Burst）または連続（Continuous）：オンデマンド動作中にフレームの連続ストリームを送信するかフレームのバーストを送信するかを指定します。 集計期間（Aggregation Period）：パフォーマンス測定が実行される時間の長さを秒単位で指定します（1 ～ 900）。この時間の経過後に統計が生成されます。	
EOAM-Configure-Y-1731-PM-Referenced-On-Demand-IOS	イーサネット サービスのリアルタイム トラブルシューティングを参照モードで実行します。参照モードでは、以前に設定した動作が開始され実行されます。	フレーム タイプ（Frame Type）：プローブのタイプ（DMMv1 または SLM）。 動作番号（Operation Number）：参照される動作の番号。	
Remove-CFM-MEP- IOS	デバイスから MEP 設定を削除します。	インターフェイス名（Interface Name）、サービス インスタンス番号（Service Instance Number）、EVC 名（EVC Name）。	

テンプレート名	用途	必須入力値	その他の情報
Remove-CFM-MEP-IOSXR	デバイスから MEP 設定を削除します。	インターフェイス名（Interface Name）、ドメイン名（Domain Name）。	
Remove-CFM-Service-IOS	CFM サービスを削除します。	インターフェイス名（Interface Name）、サービス インスタンス番号（Service Instance Number）、EVC 名（EVC Name）、ドメイン名（Domain Name）、レベル（Level）、サービス名（Service Name）。	

Quality of Service（QoS）の設定

Quality of Service（QoS）は、ネットワークトラフィックの差別化サービスを配信できるようにするための機能のセットです。QoS機能は、次の機能によって、より優れた予測可能性の高いネットワーク サービスを提供します。

- さまざまなネットワーク トラフィック クラスへの優先的な処理の提供。
- 重要なユーザーおよびアプリケーションの専用帯域幅のサポート。
- ジッターおよび遅延の制御（リアルタイム トラフィックに必要）。
- ネットワークの輻輳の回避と管理。
- トラフィック フローをスムーズにするネットワーク トラフィックのシェーピング。
- ネットワーク全体でのトラフィックの優先順位の設定。

Cisco EPN Manager を使用して、キャリア イーサネット インターフェイスでの QoS を設定できます。適切な QoS アクションを適用する前に、分類プロファイル（またはクラス マップ）を作成することによって、関連するトラフィックを差別化する必要があります。デバイスに着信したパケットは、分類プロファイルの一致基準と照らし合わせて検査され、パケットがそのクラスに属しているかどうかを判定されます。一致するトラフィックは、アクションプロファイル（またはポリシー マップ）で定義されたアクションの対象となります。

（注） すべての IOT サービスに対する QoS サポートはありません。

分類プロファイルとアクションプロファイルを設定するには、左側のサイドバーで**Configuration > QoS > Profiles** を選択します。

このセクションは、次のトピックで構成されています。

- QoS 分類プロファイルの作成 （555 ページ）
- QoS アクション プロファイルの作成 （558 ページ）

- デバイスで設定されている QoS プロファイルの確認 （565 ページ）
- インターフェイスへの QoS アクション プロファイルの適用 （565 ページ）
- デバイスから検出された QoS プロファイルのインポート （566 ページ）
- 複数のインターフェイスからの QoS アクション プロファイルの関連付け解除 （568 ページ）
- デバイスからの QoS 分類およびアクション プロファイルの削除 （568 ページ）

QoS 分類プロファイルの作成

トラフィックをクラス別に分類して、各クラスの分類基準と一致するトラフィックに特定のアクションが適用されるようにするには、分類プロファイル（クラス マップ）を作成します。

分類プロファイルを作成するには、次の手順に従います。

ステップ 1 左側のサイドバーで [設定（Configuration）] > [QoS] > [プロファイル（Profiles）] の順に選択します。

ステップ 2 [グローバル QoS 分類プロファイル（Global QoS Classification Profiles）] ページの上部にある追加アイコン（[+]）をクリックします。

ステップ 3 分類プロファイルの一意の名前を入力します。プロファイルを識別しやすくするために、プロファイルで定義された分類基準を反映した名前にしてください。さらに識別しやすくするには、説明を追加できます。

ステップ 4 プロファイルでの一致基準を定義します。

- [すべてと一致（Match All）]：トラフィックがすべてのクラス分類基準と一致すると、このクラスに分類されます。
- [いずれかと一致（Match Any）]：トラフィックがいずれかのクラス分類基準と一致すると、このクラスに分類されます。

ステップ 5 分類プロファイルの分類基準を定義するために、[QoS 分類（QoS Classifications）] の下にあるプラス アイコンをクリックします。

ステップ 6 トラフィックの分類基準とするアクションを選択してから、[値（Value）] 列をクリックして関連する値を入力します。

アクション	説明	値
ACL	指定のアクセス コントロール リスト（ACL）でパケットを許可する必要があります。	ACL 名。最大 32 文字の英数字。

アクション	説明	値
MPLS：インポジション	パケットに設定されたラベル エントリの Experimental（EXP）ビットの値が、ユーザーが指定した MPLS EXP 値と一致する必要があります。MPLS インポジションまたは MPLS Topmost を一致基準として使用します。MPLS 基準のいずれかを使用すると、他の基準は使用できなくなります。	0 ～ 7 の数値。最大 8 つのカンマ区切り値を入力できます。
MPLS：Topmost	topmost ラベルの Experimental（EXP）ビットの値が、ユーザーが指定した MPLS EXP 値と一致する必要があります。	0 ～ 7 の数値。最大 8 つのカンマ区切り値を入力できます。
重ねて表示	このアクションは、クラスマップを別のクラスマップにカスケードするために使用します。既存のクラスマップと同様の分類ポリシーを使用する新しいクラスマップを作成する場合は、このアクションを使用できます。	子クラス マップを参照します。
QoS 分類：COS	パケットのレイヤ 2 サービス クラス（CoS）ビットの値が、指定された CoS 値と一致する必要があります。	0 ～ 7 の数値。最大 8 つのカンマ区切り値を入力できます。
QoS 分類：COS：内部	指定された値が、パケットのレイヤ 2 サービス クラス（CoS）マーキングの QinQ パケットの内部 CoS 値と一致する必要があります。	0 ～ 7 の数値。最大 8 つのカンマ区切り値を入力できます。
QoS 分類：DSCP	パケットの IP DiffServ コードポイント（DSCP）の値が、指定された値の 1 つ以上と一致する必要があります。	有効な値は 0 ～ 63 です。最大 8 つのカンマ区切り値を入力できます。
QoS 分類：DSCP：IPv4 のみ	IPv4 パケットの DSCP 値と照合します。	有効な値は 0 ～ 63 です。最大 8 つのカンマ区切り値を入力できます。
QoS 分類：優先順位	パケットの IP プレシデンス値が、1 つ以上のプレシデンス値と一致する必要があります。	0 ～ 7 の数値。最大 8 つのカンマ区切り値を入力できます。
QoS 分類：優先順位：IPv4 のみ	IPv4 パケットのプレシデンス値と照合します。	0 ～ 7 の数値。最大 8 つのカンマ区切り値を入力できます。
QoS 分類：DEI	Drop Eligible Indicator（DEI）を使用して、輻輳発生時にドロップする対象フレームを示します。パケットが指定された DEI 値と一致する必要があります。	0 または 1。

アクション	説明	値
QoS グループ	選択されたQoSグループに応じてパケットを許可する必要があります。	選択されたデバイスに応じて、0～55、0 ～ 99、または 0 ～ 511 の範囲内にある最大 8 つのカンマ区切り値を入力できます。入力する値がデバイスでサポートされることを確認してください。
QoS 分類：サービス インスタンス	プロバイダ エッジ（PE）ルータでのサービス プロバイダ設定には、さまざまなサービスインスタンスがあります。QoSポリシーマップは、これらのサービスインスタンスまたはサービスインスタンス グループに適用されます。 （注） この基準が適用されるのはCisco ASR 903 のみです。	1 ～ 8000 の範囲にある任意の数のカンマ区切り値、またはそれぞれ 1 ～ 8000 の範囲にある、ハイフンでつながれた値を入力できます。
QoS 分類：VLAN	仮想ローカルエリア ネットワーク（VLAN）の識別番号を基本にしてトラフィックの照合と分類を行います。 （注） [+] アイコンをクリックして、複数の QOS 分類：VLAN を追加し、値を指定します。	1 ～ 4095 の範囲にある任意の数のカンマ区切り値、またはそれぞれ 1 ～ 4095 の範囲にある、ハイフンでつながれた値を入力できます。
QoS 分類： VLAN：内部	内部仮想ローカルエリア ネットワーク（VLAN）の識別番号を基本にしてトラフィックの照合と分類を行います。 （注） [+] アイコンをクリックして、複数のQoS分類：VLAN：内部行を追加し、値を指定します。	1 ～ 4095 の範囲にある任意の数のカンマ区切り値、またはそれぞれ 1 ～ 4095 の範囲にある、ハイフンでつながれた値を入力できます。
QoS 分類：廃棄クラス	選択された破棄クラスに応じて、パケットを許可/破棄する必要があることを意味します。	0 ～ 7 の任意の数値を入力できます。
QoS 分類：トラフィック クラス	QoS 設定のトラフィック クラス。	0 ～ 7 の任意の数値を入力できます。

ステップ 7 必要に応じて、追加の QoS 分類を定義します。

ステップ 8 ウィンドウ下部で [保存（**Save**）] をクリックし、プロファイルを保存します。右下隅に、プロファイルが保存されたことを示す通知が表示され、左側のプロファイル リストにプロファイルが表示されます。

ステップ 9 リストからプロファイルを選択し、**Deploy** ボタンをクリックしてデバイスへのプロファイルの展開を開始します。

ステップ 10 既存の分類プロファイルの詳細を使用して新しいプロファイルを作成する場合は、**Clone** ボタンをクリックします。このプロファイルには、複製元の分類プロファイルの名前の末尾にサフィックス **-clone** が追加された名前が付けられます。複製したプロファイルの名前、一致基準、その他の詳細は編集できます。

ステップ 11 選択したプロファイルで、デバイス上の既存のクラスマップをオーバーライドするには、**Override existing configuration** チェックボックスをオンにします。このチェックボックスをオンにしないと、プロファイルはデバイス上の設定とマージされます。

ステップ 12 QoS 分類プロファイルを展開するデバイスを選択します。

ステップ 13 必要に応じて、展開をスケジュールします。

ステップ 14 [送信（**Submit**）] をクリックします。右下隅に、プロファイルが展開されたことを示す通知が表示されます。展開ジョブのステータスを確認するには、左側のサイドバーから **Administration > Job Dashboard** を選択します。該当するジョブを選択します。ウィンドウの下部セクションにジョブの詳細情報と履歴が表示されます。詳細については、[情報（Information）] アイコンをクリックしてください。

QoS アクション プロファイルの作成

特定のトラフィック クラスに属しているトラフィックに適用するアクションを指定するには、アクション プロファイル（ポリシー マップ）を作成します。

アクション プロファイルを作成するには、次の手順に従います。

ステップ 1 左側のサイドバーで [設定（Configuration）] > [QoS] > [プロファイル（Profiles）] を選択します。

ステップ 2 左側の [QoS プロファイル（QoS Profiles）] ペインで [ユーザー定義のグローバル QoS プロファイル（User Defined Global QoS Profiles）] > [アクション プロファイル（Action Profiles）] を選択します。

ステップ 3 [アクション プロファイルの作成（Create Action Profile）] ペイン上部にある追加（[+]）アイコンをクリックします。

ステップ 4 アクション プロファイルに一意の名前を指定し、必要に応じて説明を入力します。

ステップ 5 アクションを割り当てる分類プロファイルを選択します。[分類プロファイル（Classification Profiles）] でプラス記号のアイコンをクリックし、リストから必要なプロファイルを選択し、**OK** をクリックします。

ステップ 6 分類プロファイル（クラス マップ）を選択し、トラフィックがプロファイルに一致する場合に適用するアクションを定義します。ポリシング、マーキング、キューイング、シェーピング、および RED の各アクションと、サービス ポリシー（H-QoS）を定義できます。各アクション タイプとその説明が表示される次のようなタブがあります。

- [ポリサー アクション（Policer Action）]：トラフィック ポリシングは、トークン バケット アルゴリズムによりインターフェイスで許容されるトラフィックの最大レートを管理します。トラフィック ポリシングでは、CIR のバースト サイズ（Bc）を設定できるので、ある程度の帯域幅管理も行えます。最大情報レート（PIR）がサポートされている場合は 2 番目のトークン バケットが強制的に適用されます。この 2 レート ポリサーは 2 つの独立レート（設定情報レート（CIR）と最大情報レート（PIR））でトラフィックを計測できます。認定トークン バケットは、オーバーフローするまで最大で認定バースト（Bc）のサイズのバイト数を保持でき、パケットが CIR に準拠しているか、CIR を超えているかを判別します。ピーク トークン バケットは、オーバーフローするまで最大でピーク

バースト（Be）のサイズのバイト数を保持でき、パケットが PIR に違反しているかどうかを判別します。パケットが CIR/PIR に準拠している場合、超えている場合、違反している場合それぞれに異なるアクションを実行できます。たとえば、準拠するパケットが送信されるように設定し、超過するパケットは優先順位を低くして送信し、違反するパケットはドロップされるように設定できます。

[ポリサー アクション（Policer Action）] タブでは、次の項目を指定します。

- [設定情報レート（CIR）（Committed Information Rate (CIR)）]：長期平均転送速度。これは 1 秒あたりのビット数（bps）または使用可能/未使用帯域幅に対する割合として指定できます。このレートを下回るトラフィックは、常に適用されます。入力する CIR 値がデバイスでサポートされていることを確認し、正しい CIR 単位値（bps、kbps、mbps、gpbs、パーセント）を選択します。
- [バースト（Bc）（Burst (Bc)）]：トラフィック バーストの最大サイズ（バイト単位）。これを超えると、一部のトラフィックは CIR を超えます。
- [最大情報レート（PIR）（Peak Information Rate (PIR)）]：一部のトラフィックが CIR に関連付けられた PIR 値を超えるまでの許容トラフィック バースト量。入力する PIR 値がデバイスでサポートされていることを確認し、CIR で選択したものと同じ単位値（bps、kbps、mbps、gpbs、パーセント）を選択します。
- [超過バースト（Be）（Excess Burst (Be)）]：トラフィック バーストの最大サイズ（バイト単位）。これを超えると、トラフィックは PIR を超えます。
- [トラフィックの色分け動作（Traffic Coloring Behavior）] で、トラフィックがレート制限に準拠している場合、超えた場合、または違反した場合に実行するアクションを選択します。必要に応じて値を指定します。カラーアウェア トラフィック ポリシングを有効にするには、[適合カラー（Conform Color）] と [超過カラー（Exceed Color）] の値をそれぞれのクラス プロファイルに関連付けて指定します。カラーアウェア ポリシングでは、CIR、PIR、適合アクション、超過アクション、および違反アクションに基づいて、次のような結果になります。
  - 測定レートが CIR 以下で、指定されたクラス（適合カラー）に属するパケットは、レートに適合しているものとしてポリシングされます。これらのパケットは、指定された適合アクションに従ってもポリシングされます。この場合、パケットは送信されます。
  - 測定レートが CIR と PIR の間にあり、適合カラー クラスまたは超過カラー クラスのいずれかに属するパケットは、CIR を超えているものとしてポリシングされます。これらのパケットは、指定された超過アクションに従ってもポリシングされます。この場合、パケットの優先順位値が設定されて、パケットが送信されます。
  - 測定レートが PIR より高いパケット、または適合カラー クラスにも超過カラー クラスにも属さないパケットは、レートに違反しているものとしてポリシングされます。これらのパケットは、指定された違反アクションに従ってもポリシングされます。この場合、パケットは廃棄されます。

- [マーカー アクション（Marker Action）]：パケット マーキングを利用すれば、ネットワークを複数の優先度レベルまたはサービス クラスに分割できます。トラフィック フローのマーキングは、次により実行されます。
  - タイプ オブ サービス（ToS）バイトに IP precedence ビットまたは DSCP ビットを設定する。

- レイヤ 2 ヘッダー内の CoS ビットを設定する。
- インポーズされた、または最上位のマルチ プロトコル ラベル スイッチング（MPLS）ラベル内に EXP ビットを設定する。
- qos-group ビット、traffic-clas ビット、および discard-class ビットを設定する。

[マーカー アクション（Marker Action）] タブでは、次の項目を指定します。

- [マーキング機能とマーキング値（Marking Feature and Marking Value）]：トラフィックのマーキング方法と必須値。

- [キューイング アクション（Queueing Action）]：キューイングは、トラフィック輻輳管理に使用されます。輻輳管理では、キューを作成し、そのキューにパケットの分類に基づいてパケットを割り当て、キューにあるパケットの送信をスケジューリングする必要があります。

  [キューイング アクション（Queueing Action）] タブで、トラフィックのキューイング方法（[帯域幅（Bandwidth）] または [プライオリティ（Priority）]）を選択し、次の項目を指定します。

  - [帯域幅（Bandwidth）]：トラフィック クラスに割り当てられる帯域幅の量を、キロビット/秒または絶対保証帯域幅に対するパーセンテージのいずれかで指定します。帯域幅に基づいてキューイングすることを選択した場合は、残り帯域幅のパーセンテージとして帯域幅を割り当てることもできます。
  - [キュー制限（Queue Limit）]：このクラスに関連付けられているすべての個別キューのパケット/バイト/ミリ秒の最大数。キューのサイズがこの値を超えると、パケットがドロップされます。

  [帯域幅（Bandwidth）] を選択した場合は、次の項目を指定します。

  - [均等化キューを有効にする（Enable Fair Queue）]：重み付け均等化キューイングを有効にするには、このチェックボックスをオンにします

    。
  - [個別キュー サイズ（Individual Queue Size）]：均等化キューが有効な場合に使用します。輻輳期間に各クラス別キューで許容する最大パケット数を指定します。

  [プライオリティ（Priority）] を選択した場合は、次の項目を指定します。

  - [キュー バースト サイズ（バイト数）（Queue Burst Size (bytes)）]：バースト サイズにより、ネットワークが一時的なトラフィックのバーストに対応できるように設定されます。範囲は 18 ～ 2000000 バイトです。デフォルトは、設定された帯域幅レートで 200 ミリ秒のトラフィックです。
  - [プライオリティ レベル（Priority Level）]：ポリシー マップのクラスに、異なる優先順位（プライオリティ キュー レベル 1 ～ 3）を設定できます。これらのキューのパケットは、他のキューと比較して低遅延になります。同じポリシー マップ内の異なる 2 つのクラスに同じ優先度レベルを指定することはできません。

- [シェーピング アクション（Shaping Action）]：トラフィック シェーピングでは、指定されたレートにトラフィックをシェーピングすることでトラフィックが調整されます。

  [シェーピング アクション（Shaping Action）] タブでは、次の項目を指定します。

  - [平均またはピーク レート トラフィック シェーピングの選択（Select Average or Peak rate traffic shaping）]：平均レート シェーピングでは、転送速度が CIR に制限されます。ピーク レート シェーピングでは、CIR を超えるトラフィックを送信するようルータを設定します。ピーク レートを判別するため、ルータでは「ピーク レート＝CIR(1＋Be／Bc)」という公式が使用されます。ここで Be は超過バースト サイズ、Bc は認定バースト サイズです。
  - ピーク レート トラフィック シェーピングを選択する場合は、バースト サイズと超過バースト サイズをバイト単位で指定します。
  - 必要に応じて、FECN 適応型シェーピングを有効にします。適応型シェーピングでは、逆方向明示的輻輳通知（BECN）信号を受信すると使用可能な帯域幅が推定されます。FECN 適応型シェーピングにより、ルータは順方向明示的輻輳通知（FECN）信号を BECN 信号として反映します。
  - FECN 適応型シェーピングが有効な場合は、適応レート（トラフィック シェーピングの最小ビット レート）を指定します。

- [RED アクション（RED Action）]：重み付けランダム早期検出（WRED）は、キューがその制限に達する前に輻輳を制御する、プロアクティブなキューイング戦略を採用した輻輳回避手法です。WRED は、ランダム早期検出（RED）メカニズムと IP プレシデンス、DiffServ コード ポイント（DSCP）、および discard-class の機能を組み合わせて、優先順位が高いパケットから処理します。インターフェイスで輻輳が発生し始めると、WRED は優先順位の低いトラフィックを高い確率で破棄します。WRED は、レイヤ 3 キューの平均の深さを制御します。

  [RED アクション（RED Action）] タブで、次の項目を指定します。

  - [分類メカニズム（Classification Mechanism）]：WRED ドロップ ポリシーを定義するための基準を選択します。WRED では、次のように特定のパケット分類に基づいてドロップ ポリシーを定義します。

    [CLP]：セル損失率優先度（CLP）値に基づいて WRED のドロップ ポリシーを設定します。有効な値は、0 または 1 です。

    [CoS]：パケットに関連付けられている指定されたサービス クラス（CoS）ビットに基づいて WRED のドロップ ポリシーを設定します。有効な値は 0 ～ 7 です。

    [破棄クラス（Discard Class）]：discard-class の値に基づいて WRED のドロップ ポリシーを設定します。有効な値は 0 ～ 7 です。discard-class の値により、トラフィック ドロップの Per-Hop Behavior（PHB）が設定されます。discard-class に基づく WRED は出力機能です。

    [DSCP]：DSCP 値に基づいて WRED のドロップ ポリシーを設定します。設定されている場合、ルータは設定した WRED しきい値に従い、指定された DSCP 値を持つパケットをランダムにドロップします。

    [プレシデンス（Precedence）]：IP プレシデンス レベルに基づいて WRED のドロップ ポリシーを設定します。有効な値は 0 ～ 7 です。通常、0 はアグレッシブに管理可能な（ドロップ可能

な）優先順位が低いトラフィックを表し、7は優先順位が高いトラフィックを表します。プレシデンス レベルが低いトラフィックは通常、廃棄確率が高くなります。WRED によりパケットがドロップされると、TCP を使用している送信元ホストはこのドロップ操作を検知し、パケットの送信速度を低下させます。

[DEI]：フレーム リレー フレームのアドレス フィールドの廃棄条件（DE）ビットを使用して、輻輳が発生しているフレーム リレー ネットワークでのフレームの廃棄を優先します。フレーム リレー DE ビットは 1 ビットしかないため、設定は 2 つ（0 または 1）しかありません。フレーム リレー ネットワークで輻輳が発生した場合、DE ビットが 0 に設定されているフレームよりも前に、DE ビットが 1 に設定されているフレームが廃棄されます。

[RED デフォルト（RED Default）]：WRED プロファイルのクラスの最小しきい値、最大しきい値、およびマーク確率デノミネータ（MPD）の設定値のデフォルト セットです。

- 必要に応じて ECN を有効にします。ECN（明示的輻輳通知）は、平均キュー長が特定のしきい値を超えた場合、ECN は、それらをドロップする代わりにパケットをマーキングします。ルータとエンド ホストは、このマーキングをネットワークの輻輳とパケットの送信速度の低下を示す警告として使用します。
- 選択した分類メカニズムの有効な値ごとに、しきい値とマーク確率を定義します。たとえば、プレシデンスを使用する場合には 7 つの有効な値それぞれにしきい値を定義できます。最小しきい値は、キューで許容する最小パケット数です。平均キューの長さが最小しきい値に達すると、WRED では、指定された DSCP、IP プレシデンス、discard-class、または atm-clp の値で、「一部の」パケットがランダムにドロップされます。有効な最小しきい値は 1 ～ 16,384 です。最大しきい値は、キューで許容する最大パケット数です。平均キューの長さが最大しきい値を超えると、WRED では、指定された DSCP、IP プレシデンス、discard-class、または atm-clp の値のすべてのパケットがドロップされます。有効な最大しきい値は、最小しきい値 ～ 16,384 です。

- **[サービス ポリシー（Service Policy）]**：

  [サービス ポリシー（Service Policy）] タブでは、階層型 QoS（H-QoS）を設定できます。H-QoS により、階層の複数レベルで QoS 動作を指定できます。H-QoS を使用して、複数のキューを一括でシェーピングするため複数のポリシーマップを指定できます。すべての階層型ポリシー タイプは、最上位の親ポリシーと 1 つ以上の子ポリシーで構成されます。service-policy コマンドは、ポリシーを異なるポリシーに適用する場合、およびポリシーをインターフェイスに適用する場合に使用します。

  H-QoS を設定するには、[サービス ポリシー（Service Policy）] タブに移動し、[有効化（Enable）] チェックボックスをオンにし、[サービス ポリシー（Service Policy）] ドロップダウン メニューから子サービス ポリシーを選択します。選択した子サービス ポリシーは、このアクション プロファイルが属する親ポリシーマップに関連付けられます。子サービス ポリシーは、同じポリシーマップの親ポリシーとして機能できない点に注意してください。たとえば、子サービス ポリシー「X」が親ポリシー マップ「Y」に属している場合、子ポリシー「X」にサービス ポリシー マップ「Y」を含めることはできません。

  H-QoS の制約事項：Cisco IOS-XE デバイス（Cisco ASR903、Cisco ASR907、Cisco ASR920、Cisco NCS42XX など）には、次に示す H-QoS の制約事項が適用されます。

- 親ポリシー マップの制約事項：
  - 親ポリシー マップを作成するときには、「class-default」クラスだけを使用できます。
  - 親ポリシー マップには、EFP（サービス インスタンス）などの一致条件が設定されているクラスが含まれている必要があります。
  - 親ポリシー マップには、VLAN などの一致条件が設定されているクラスが含まれている必要があります。
- 子ポリシー マップの制約事項：
  - EFP（サービス インスタンス）と VLAN を一致タイプとして使用して子ポリシー マップを作成することはできません。

ステップ 7 ウィンドウ下部で [保存（**Save**）] をクリックし、プロファイルを保存します。右下隅に、プロファイルが保存されたことを示す通知が表示され、左側のプロファイル リストにプロファイルが表示されます。

ステップ 8 [グローバル QoS アクション プロファイル（Global QoS Action Profiles）] ペインでプロファイルを選択し、[展開（**Deploy**）] ボタンをクリックし、デバイスへのプロファイルの展開を開始します。

ステップ 9 既存のアクションプロファイルの詳細情報を使用して新しいプロファイルを作成するには、[複製（**Clone**）] ボタンをクリックします。このプロファイルの名前は、複製元のアクション プロファイルの名前にサフィックス **-clone** が付いたものになります。複製したプロファイルでは、名前やアクションなどの詳細情報を編集できます。

ステップ 10 選択したプロファイルで、デバイス上の既存のポリシーマップをオーバーライドするには、[既存の設定の上書き（**Override existing configuration**）] チェックボックスをオンにします。このチェックボックスをオンにしないと、プロファイルにデバイスの設定がマージされます。

ステップ 11 QoS アクション プロファイルを展開するデバイスを選択します。

ステップ 12 必要に応じて、展開をスケジュールします。

ステップ 13 [送信（**Submit**）] をクリックします。右下隅に、プロファイルが展開されたことを示す通知が表示されます。展開ジョブのステータスを確認するには、左側のサイドバーから **Administration > Job Dashboard** を選択します。該当するジョブを選択します。ウィンドウの下部セクションにジョブの詳細情報と履歴が表示されます。詳細については、[情報（Information）] アイコンをクリックしてください。

QoS サブアクション プロファイルの作成

アクション プロファイル（ポリシー マップ）は、特定のトラフィック クラスに属しているトラフィックに適用するアクションを指定します。これらは、トラフィックがプロファイルに一致する場合に適用するアクションを定義する、複数の分類プロファイルに関連付けられます。ポリシング、マーキング、キューイング、シェーピング、およびREDの各アクションと、サービス ポリシー（H-QoS）を定義できます。

サブアクションプロファイルは、単一の分類プロファイルにのみ関連付けられているアクション プロファイルです。回線/VC のプロビジョニング中にサブアクション プロファイルを使用

して、単一のアクションに基づくアクションプロファイルを回線/VC に関連付けることができます。

サブアクション プロファイルを作成する手順は次のとおりです。

ステップ 1 左側のサイドバーで [設定（Configuration）] > [QoS] > [プロファイル（Profiles）] を選択します。

ステップ 2 左側の [QoS プロファイル（QoS Profiles）] ペインで [ユーザー定義のグローバル QoS プロファイル（User Defined Global QoS Profiles）] > [サブアクション プロファイル（Sub-Action Profiles）] を選択します。

ステップ 3 [サブアクション プロファイルの作成（Create Sub-Action Profile）] ペイン上部にある追加（[+]）アイコンをクリックします。

ステップ 4 サブアクション プロファイルに一意の名前を指定します。説明を入力することもできます。

ステップ 5 アクションを割り当てる分類プロファイルを選択します。[分類プロファイル（Classification Profiles）] でプラス記号のアイコンをクリックし、リストから必要なプロファイルを選択し、**OK** をクリックします。

サブアクション プロファイルに追加できる分類プロファイルは 1 つだけです。複数の分類プロファイルを関連付けるには、アクション プロファイルを作成する必要があります。

ステップ 6 トラフィックが分類プロファイルで指定された条件と一致する場合に実行する必要があるアクションを指定します。各種のオプションの説明については、QoS アクション プロファイルの作成 （558 ページ）を参照してください。

QoS アクションおよびサブアクション プロファイルのインポートとエクスポート

ステップ 1 左側のサイドバーで [設定（Configuration）] > [QoS] > [プロファイル（Profiles）] を選択します。

ステップ 2 アクション プロファイルをエクスポートするには、左側のペインで [ユーザー定義のグローバル QoS プロファイル（User Defined Global QoS Profiles）] > [アクション プロファイル（Action Profiles）] を選択します。

ステップ 3 サブアクション プロファイルをエクスポートするには、左側のペインで [ユーザー定義のグローバル QoS プロファイル（User Defined Global QoS Profiles）] > [サブアクション プロファイル（Sub-Action Profiles）] を選択します。

ステップ 4 プロファイルをエクスポートするには、エクスポートするプロファイルを選択し、[エクスポート（Export）] をクリックします。指定した場所にファイルが保存されます。

ステップ 5 プロファイルをインポートするには、[インポート（Import）] をクリックし、インポートする XML ファイル（アクションまたはサブアクションプロファイルに関する情報を含む）を選択し、[OK] をクリックします。インポートされたプロファイルはそれぞれ、[アクション プロファイル（Action Profiles）] ページまたは [サブアクション プロファイル（Sub-Action Profiles）] ページに表示されます。

以下の点に注意してください。

- 1 つのインスタンスでインポートできるプロファイルの数に制限はありませんが、最適なパフォーマンスを確保するため、選択するプロファイルは 10 個までにすることをお勧めします。
- インポートするファイルのサイズは 20 MB 未満にしてください。

• XML 形式のみのファイルをインポートできます。

デバイスで設定されている QoS プロファイルの確認

特定のデバイスに展開された QoS プロファイルを確認するには、次の手順を実行します。

ステップ 1 左側のサイドバーから **Inventory > Network Devices** を選択します。

ステップ 2 必要なデバイスを見つけ、デバイス名のハイパーリンクをクリックします。デバイスの詳細が表示されます。

ステップ 3 [論理ビュー（Logical View）] タブをクリックします。

ステップ 4 左側のペインで QoS の横の矢印をクリックし、[アクション プロファイル（Action Profiles）] または [分類プロファイル（Classification Profiles）] を選択します。選択したデバイスに展開されているプロファイルを示すテーブルが表示されます。プロファイル名（青色のハイパーリンク）をクリッして、プロファイルの詳細を表示します。

インターフェイスへの QoS アクション プロファイルの適用

デバイスに導入されたアクション プロファイルを選択し、そのデバイス上の複数のインターフェイスにアクション プロファイルを適用できます。アクション プロファイルにより、特定のトラフィック クラスに属するトラフィックに適用するアクションを指定できます。既存のプロファイルをインターフェイスに適用する前に、プロファイルに変更を加えたり、そのプロファイルを使用して新しいプロファイルを作成したりできます。すでにアクションプロファイルが適用されているインターフェイスを選択すると、Cisco EPN Manager はその旨を通知し、ユーザーに既存のプロファイルをオーバーライドするオプションを提示します。インターフェイスにアクションプロファイルを適用するには、その前に、必要なプロファイルがデバイスに導入されている状態にしなければなりません。これを行うには、QoS アクション プロファイルの作成 （558 ページ）を参照してください。

アクション プロファイルをインターフェイスに適用するには、次の手順に従います。

ステップ 1 左側のサイドバーで、**[構成（Configuration）] > [QoS] > [インターフェイス（Interfaces）]** の順に選択します。

Cisco EPN Manager インターフェイスが [イーサネット CSMA/CD、IEEE8023 ADLAG（Ethernet CSMA/CD, IEEE8023 ADLAG）]、[ギガビット イーサネット（Gigabit Ethernet）]、および [L2 VLAN] カテゴリに表示されます。その他すべてのポートは、[ユーザー定義（User Defined）] カテゴリに表示されます。

ステップ 2 アクション プロファイルに関連付けるインターフェイスを選択します。

ステップ 3 [アクション プロファイルの関連付け（Associate Action Profile）] をクリックし、アクション プロファイルを選択して、そのプロファイルを適用する方向を設定します。使用可能なアクション プロファイルのリス

トと、それらのプロファイルを適用できるインターフェイスがリストされます。インターフェイスごとに、その名前、適用方向、およびそのインターフェイスにすでに存在するアクションプロファイルがリストされます。

（注） QoSスケーリングプロファイルの設定は、バンドルイーサネットインターフェイスとサブインターフェイスのアクションプロファイルを関連付けるための前提条件になります。設定例：

```
hw-module profile qos bundle <high-scale|medium-scale|low-scale> location <card>
```

ステップ 4 [アクションプロファイル（Action Profiles）] ドロップダウンリストから必要なアクションプロファイルを選択します。メニューが空の場合は、アクションプロファイルを作成してから、それらのアクションプロファイルをデバイスに関連付ける必要があります。QoS アクション プロファイルの作成 （558 ページ）を参照してください。

ステップ 5 [インターフェイス（Interfaces）] セクションで、プロファイルを適用する方向を指定します。プロファイルをサブインターフェイスに適用する場合は、メインインターフェイスの方向と逆の方向で適用するようにしてください。適用する方向を変更するには、ダイアログの左上隅にある [編集（Edit）] アイコンを使用します。

（注） キューイングアクションが含まれるポリシーマップを入力方向でインターフェイスに適用することはできません。

ステップ 6 （任意）選択したアクションプロファイルを将来の日時に適用するようにスケジュールすることもできます。それには、[スケジュール（Schedule）]セクションを展開し、プロファイルを適用する日時と頻度を指定します。必要に応じて、このタスクは [ジョブ（Jobs）] ページでさらに編集できます。

ステップ 7 [OK] をクリックしてアクションプロファイルを選択したデバイスに適用します。ダイアログの右下隅に表示される通知で、プロファイルが正常に適用されたか、またはジョブが失敗したかを確認できます。詳細情報を確認するには、[詳細の表示（Show Details）] リンクをクリックします。

アクション プロファイルとそのプロファイルが適用されるインターフェイスとの関連付けを解除するには、次を参照してください。 複数のインターフェイスからの QoS アクション プロファイルの関連付け解除 （568 ページ）

デバイスから検出された QoS プロファイルのインポート

デバイスから検出された QoS プロファイルを Cisco EPN Manager に直接インポートできます。インポートした QoS プロファイルを、Cisco EPN Manager を使って編集したり、デバイス上でさらに詳細に設定したりできます。Cisco EPN Manager にすでに存在する他のプロファイルと同じプロファイル名を持つ、デバイスから検出されたプロファイルは、グローバルプロファイルとして表されます。これは、[グローバル プロファイル（Global Profiles）] ページの [グローバル（Global）] 列に示されます。複数のグローバル プロファイルの名前が同じでも、QoS 設定が異なる場合があることに注意してください。グローバル プロファイルのインポート時には、検出されたプロファイルによって（同じ名前の）既存のプロファイルを上書きするか、それともインポート前にプロファイルの名前を変更するかを選択できます。

デバイスから検出された QoS プロファイルをインポートするには、次の手順を実行します。

始める前に

デバイスのインベントリ収集ステータスが [完了（Completed）] であることを確認します。これにより、デバイスの QoS プロファイルが Cisco EPN Manager によって検出されることを確認できます。

ステップ 1 左側のサイドバーから **[設定（Configuration）] > [QoS] > [プロファイル（Profiles）]** を選択し、すべての Cisco EPN Manager QoS プロファイルを表示します。

ステップ 2 アクションプロファイルをインポートするには、左側の [QoS プロファイル（QoS Profiles）] ペインから、**[検出されたプロファイル（Discovered Profiles）] > [アクション プロファイル（Action Profiles）]** を選択します。

ステップ 3 分類プロファイルをインポートするには、左側の [QoS プロファイル（QoS Profiles）] ペインから、**[検出されたプロファイル（Discovered Profiles）] > [分類プロファイル（Classification Profiles）]** を選択します。

ステップ 4 最初にデバイスを選択した後で、そのデバイスで検出されたプロファイルを選択するには、次の手順を実行します。

a) [設定（Configuration）] > [ネットワーク デバイス（Network Devices）] を選択し、デバイス名のハイパーリンクをクリックして、デバイスを選択します。
b) [論理ビュー（Logical View）] タブをクリックします。
c) [QoS] を展開します。
d) デバイスからインポートするプロファイルのタイプに応じて、[アクション プロファイル（Action Profiles）] または [分類プロファイル（Classification Profiles）] を選択します。
e) （オプション）プロファイルを表示した後、Cisco EPN Manager によって検出されたすべての QoS プロファイルをリストしているページからそれらのプロファイルを直接インポートするには、[グローバル プロファイル ページ（Global Profile Page）] ハイパーリンクをクリックし、ステップ 5 に進みます。
f) プロファイルを選択し、[グローバルにする（Make Global）] をクリックします。
g) ステップ 6 に進みます。

ステップ 5 インポートするプロファイルを選択して、[インポート（Import）] をクリックします。まだデバイスに存在しないプロファイルのみを確実にインポートするには、（[グローバル（Global）] 列に [いいえ（No）] とマークされている）グローバルでないプロファイルを選択します。

ステップ 6 Cisco EPN Manager に重複プロファイルがある場合は、プロファイルの名前を変更して新しい名前で同じ QoS 設定のプロファイルを作成するか、それとも既存のプロファイルを上書きするかを選択するよう求められます。必要な変更を加えます。

ステップ 7 既存の QoS プロファイルの詳細を使用して新しいプロファイルを作成するには、[複製（**Clone**）] ボタンをクリックします。このプロファイルは、複製元の QoS プロファイルの名前にサフィックス **-clone** が付いた名前になります。この複製されたプロファイルの詳細を任意に編集できます。

ステップ 8 [保存（Save）] をクリックして、選択した QoS プロファイルをインポートします。

インポートしたプロファイルを特定のデバイスのインターフェイスに適用するには、インターフェイスへの QoS アクション プロファイルの適用 （565 ページ）を参照してください。

複数のインターフェイスからのQoSアクションプロファイルの関連付け解除

アクション プロファイルにより、特定のトラフィック クラスに属するトラフィックに適用するアクションを指定できます。デバイスに導入されたアクションプロファイルを選択し、そのデバイス上の複数のインターフェイスにアクションプロファイルを適用できます。プロファイルをインターフェイスに適用した後、必要に応じてプロファイルとインターフェイスの関連付けを解除することができます。アクションプロファイルとインターフェイスの関連付けを解除するには、その前に、対象のプロファイルがデバイスに適用されていることを確認する必要があります。インターフェイスへのQoSアクションプロファイルの適用（565ページ）を参照してください。

アクション プロファイルをインターフェイスに適用するには、次の手順に従います。

ステップ1 左側のサイドバーで、**[構成（Configuration）]**>**[QoS]**>**[インターフェイス（Interfaces）]**の順に選択します。

あるいは、[構成（Configuration）]>[QoS]>[プロファイル（Profiles）]に移動してプロファイルを選択した後、そのプロファイルが適用されているインターフェイスからプロファイルの関連付けを解除することもできます。

Cisco EPN Manager インターフェイスが [イーサネット CSMA/CD、IEEE8023 ADLAG（Ethernet CSMA/CD, IEEE8023 ADLAG）]および[L2 VLAN]カテゴリの下に表示されます。その他すべてのポートは、[ユーザー定義（User Defined）] カテゴリの下に表示されます。

ステップ2 アクション プロファイルの関連付けを解除するインターフェイスを選択します。

ステップ3 **[アクションプロファイルの関連付け解除（De-associate Action Profile）]**をクリックします。

ステップ4 （任意）選択したアクションプロファイルを将来の日時に関連付け解除するようにスケジュールすることもできます。それには、[スケジュール（Schedule）]セクションを展開し、関連付けを解除する必要があるプロファイルに応じて日時と頻度を指定します。

ステップ5 [OK]をクリックして確認します。選択したインターフェイスからアクションプロファイルの関連付けが解除されます。ウィンドウの右下隅に表示される通知で、プロファイルが正常に関連付け解除されたか、またはジョブが失敗したかを確認できます。詳細情報を確認するには、[詳細の表示（Show Details）]リンクをクリックします。

デバイスからの QoS 分類およびアクション プロファイルの削除

デバイスに展開されている QoS 分類およびアクション プロファイルを削除するには、次の表に示すパスに移動します。

（注） デバイスから直接検出されたQoSアクションおよび分類プロファイルは削除できません。Cisco EPN Managerを使用して作成した（およびそれにインポートした）プロファイルのみを削除できます。

参照プロファイルの削除を避けるため、削除操作は次のシナリオではサポートされていません。

- 他の分類プロファイルに関連付けられた QoS 分類プロファイルは削除できません。たとえば、分類プロファイルで [カスケード（Cascade）] オプションを使用して選択した分類プロファイルを参照する場合、選択したプロファイルの削除操作は失敗します。
- アクション プロファイルによって参照される QoS 分類プロファイルは削除できません。
- デバイス インターフェイスに正常に適用されたアクション プロファイルは削除できません。
- アクション プロファイルは、別のアクション プロファイルによって参照されている場合は削除できません。たとえば、アクションプロファイルが参照ポリシーを使用して他のアクション プロファイルに関連付けられている場合、そのアクション プロファイルの削除操作は失敗します。

表 *30 : QoS* アクションおよび分類プロファイルを削除するためのナビゲーション パス

タスク	GUI での手順
ユーザー定義の分類プロファイルの削除	**1.** [構成（Configuration）] > [QoS] > [分類プロファイル（Classification Profiles）] を選択します。 **2.** デバイスや Cisco EPN Manager から削除する分類プロファイルを選択します。 **3.** タスク バーで [X]（削除）アイコンをクリックします。 **4.** または、デバイスのハイパーリンクをクリックして、選択した分類プロファイルを削除するデバイスを選択することもできます。 **5.** [送信（Submit）] をクリックします。[ジョブの詳細（Job Details）] ポップアップ ウィンドウをクリックして、削除操作のステータスを確認できます。

ユーザー定義のアクション プロファイルの削除	1. [構成（Configuration）] > [QoS] > [アクションプロファイル（Action Profiles）] を選択します。 2. デバイスや Cisco EPN Manager から削除するアクション プロファイルを選択します。 3. タスク バーで [X]（削除）アイコンをクリックします。 4. または、デバイスのハイパーリンクをクリックして、選択したアクション プロファイルを削除するデバイスを選択することもできます。 5. [送信（Submit）] をクリックします。[ジョブの詳細（Job Details）] ポップアップ ウィンドウをクリックして、削除操作のステータスを確認できます。

デバイスの変更内容の保存

デバイスに変更を加えた後、データベースに変更を保存し、必要に応じてデバイスの物理および論理インベントリを収集します。詳細については、次のトピックを参照してください。

- データベースへのデバイス設定変更の保存（更新） （570 ページ）
- デバイスのインベントリの即時収集（同期） （570 ページ）

データベースへのデバイス設定変更の保存（更新）

デバイスに変更を加えた後は、構成ウィンドウの [更新（Update）] をクリックして変更内容をデータベースに保存してください。[更新（Update）] ボタンが表示されていない場合は、手動による同期を実行して、変更を保存するだけでなく、デバイスの物理および論理インベントリを収集してデータベースに保存してください。参照先デバイスのインベントリの即時収集（同期） （570 ページ）

デバイスのインベントリの即時収集（同期）

同期操作は、デバイスの即時インベントリ収集を実行します。同期の実行時に、Cisco EPN Manager は選択されているデバイスの物理インベントリと論理インベントリを収集し、データベースを存在するすべての更新で同期します。デバイスの変更後に同期操作を実行しない場合は、日次インベントリ収集まで変更内容がデータベースに保存されません。

（注） 同期操作は、更新操作とは異なります。更新操作では、設定の変更内容が保存されますが、インベントリ収集は実行されません。同期の代わりに更新を使用する場合は、データベースへのデバイス設定変更の保存（更新） （570 ページ）を参照してください。

（注） この同期操作は、同期されていないデバイス コンフィギュレーション ファイルを使用した作業とは異なります。同期されていないデバイスとは、スタートアップ コンフィギュレーション ファイルが実行コンフィギュレーション ファイルと異なるデバイスです。詳細については、実行デバイス コンフィギュレーションとスタートアップ デバイス コンフィギュレーションの同期 （151 ページ）を参照してください。

手動での同期を実行するには、次のいずれかの方法を使用します。

インベントリ収集対象：	次の手順を実行します。
単一デバイス	• デバイスの [デバイス 360（Device 360）] ビューで **[アクション（Actions）] > [今すぐ同期する（Sync Now）]** を選択します。 （注） デバイスでの同期操作のステータスを表示できます。詳細については、デバイス同期状態 （571 ページ）を参照してください。 • [ネットワーク デバイス（Network Devices）] テーブルでデバイスのチェックボックスをオンにし、[同期（Sync）] をクリックします。
複数のデバイス	[ネットワーク デバイス（Network Devices）] テーブルでデバイスを選択し（デバイスのチェックボックスをオンにし）、[同期（Sync）] をクリックします。

デバイス同期状態

[デバイスの同期状態（Device Sync State）]：デバイスで実行された同期操作のステータスを示します。

表 *31* : デバイス同期状態

アイコン	デバイス同期状態	説明
↻	同期中	デバイスの同期を実行中です。
↔	完了	デバイスの同期が正常に完了しました。

	エラー/警告（Error/Warning）	以下の一覧に示すエラーまたは警告： • 追加開始（Add Initiated） • 収集の失敗（Collection Failure） • 警告付き完了（Completed with Warning） • 削除処理中（Delete In Progress） • サービス中（In Service） • サービスメンテナンス中（In Service Maintenance） • ライセンスなし • 収集一部失敗（Partial Collection Failure） • SNMP 接続失敗（SNMP Connectivity Failed） • SNMP ユーザー認証失敗（SNMP User Authentication Failed） • スイッチ ポート トレース（Switch Port Trace） • 誤った CLI クレデンシャル（Wrong CLI Credentials）

（注） サービスメンテナンスフィルタは、最後のインベントリ収集ステータスには使用できません。

Cisco NCS および Cisco ONS デバイスを管理するための Cisco Transport Controller の起動

Cisco Transport Controller（CTC）は、Cisco ONS および Cisco NCS デバイスのサブセットに使用されるソフトウェア インターフェイスです。CTC はコントロール カード上で Java アプリケーションとして実行されます。CTC を使用して、これらのデバイスをプロビジョニングおよび管理します。

CTC は Cisco EPN Manager から起動できます。選択した NE リリースに関わらず、最新の CTC リリースだけが起動されます。他の CTC リリースを使用する必要がある場合は、Web ブラウザから CTC を起動し、該当する CTC リリースを使用している NE に直接接続してください。

CTC を起動するには、次の手順に従います。

始める前に

CTC を起動するようにデバイスが正しく設定されていることを確認します。デバイスをモデル化してモニターできるように設定する （69 ページ）を参照してください。

ステップ 1 左側のサイドバーで、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択します。

ステップ 2 Cisco ONS または Cisco NCS デバイスの IP アドレスの横にある「i」アイコンをクリックし、デバイスの 360 度ビューを起動します。

ステップ 3 デバイスの 360 度ビューで、[アクション（Actions）] > [CTC の起動（Launch CTC）] の順に選択します。CTC ランチャアプリケーションがコンピュータにダウンロードされます。選択したデバイスタイプで CTC の起動がサポートされていない場合、このアクションは無効になります。

ステップ 4 [CTC ランチャ（CTC Launcher）] ウィンドウで、次のいずれかの接続モードを選択します。

- [IP を使用（Use IP）] : デバイスの IP アドレスを使用してデバイスへの接続が確立されます（デフォルト オプション）。
- [TL1 トンネルを使用（Use TL1 Tunnel）] : TL1 セッションを使用してデバイスへの接続が確立されます。TL1 セッションは、CTC から開始することも、TL1 端末を使用して開始することもできます。注 : サード パーティの OSI ベースの GNE の背後にあるデバイスには、このオプションを使用して接続してください。CTC ランチャにより、OSI ベースの GNE 経由で TCP トラフィックを転送するための TL1 トンネルが作成され、CTC でプロビジョニングが行われます。

ステップ 5 CTC のバージョンを選択し、**Launch CTC** をクリックします。

ステップ 6 CTC クレデンシャルを入力します。

第 14 章

デバイス設定の変更を自動化するテンプレートの作成

この章は次のトピックで構成されています。

新しい設定テンプレートを作成する理由

Cisco EPN Manager には、ネットワーク デバイスで変更を加えるために使用できる多数の設定済みの設定テンプレートが用意されています。これらについては、既存のテンプレートを使用した新規 CLI 設定テンプレートの作成 （578 ページ） で説明しています。

十分な権限を持っている場合は、ご使用の環境のニーズに完全に合う新しいテンプレートを作成し、そのテンプレートを他の人が使用できるようにすることもできます。複数のテンプレートをまとめて1つの複合テンプレートにグループ化するなど、テンプレートを必要に応じて単純または複雑にすることができます。最後に、設定グループを作成してテンプレートを特定のデバイスに関連付けることができます。

Cisco EPN Manager には、テンプレートで使用できる設定済みの CLI コマンドが用意されています。また、新しいCLIコマンドを作成するために使用できる空白のCLIテンプレートも用意されています。それらは単独で使用することも、複合テンプレートで他のコマンドと組み合わせて使用することもできます。

設定テンプレートをどのように使用するかは、ネットワークの大きさ、組織内の設計者の数、およびデバイス構成の変化量などの要素によって異なる場合があります。次に例を示します。

- 設計者の人数が 1 人または 2 人で、デバイス構成の数も限定的な小規模なネットワークの場合は、「良好」とわかっているCLI構成を一連のテンプレートにコピーすることから開始します。その後、それらを複合テンプレートに結合して、オペレータが利用できるようにすることができます。
- 多くの異なるデバイス構成を含む大規模ネットワークの場合は、標準化できる設定の識別を試行します。これにより、これらの標準への例外の量を制御したり、必要に応じて機能のオン/オフを切り替えることができます。

を使用して設定テンプレートを作成する方法 Cisco EPN Manager

Cisco EPN Manager では、ユーザー アカウントの特権に応じて新しい設定テンプレートを作成するためのさまざまな方法が用意されています。「CLI 設定テンプレート」には、1 つ以上の CLI 設定コマンド（デバイスの設定時に入力するコマンドと同じコマンド）が含まれています。複合設定テンプレートは、2 つ以上の CLI または複合設定テンプレートで構成されます。コマンドをデバイスに展開する順序を指定できます。

- 設定済み CLI テンプレートの 1 つを変更します。新規複合テンプレートの作成 （589 ページ）を参照してください。
- 空のCLIテンプレートを使用し、コードを手入力します。空白テンプレートを使用した新しい CLI 設定テンプレートの作成 （577 ページ）を参照してください。
- 空の CLI テンプレートを使用し、コマンド ライン コンフィギュレーション セッション、CLI スクリプト、またはその他の一連の保存済みコンフィギュレーション コマンドからコードをコピーして貼り付けます。既存のテンプレートを使用した新規 CLI 設定テンプレートの作成 （578 ページ）を参照してください。
- 既存の複数の設定済みテンプレートまたはユーザー定義テンプレートを1つのテンプレートにマージします。複合テンプレートに含まれるテンプレートが、デバイスに展開される順序を指定してください。デバイスのグループにテンプレートを展開するための設定グループの作成 （592 ページ）を参照してください。

テンプレートのセットを作成したら、それらをエクスポートおよびインポートできます。

空白テンプレートを使用した新しい CLI 設定テンプレートの作成

テンプレートを使用して、一連の再利用可能なデバイス設定コマンドを定義します。CLI テンプレートとその使用法の説明は、**[設定（Configuration）]**>**[テンプレート（Templates）]**>**[機能およびテクノロジー（Features & Technologies）]** を選択し、続いて**[CLIテンプレート（CLI Templates）]** を選択すると、Web GUI に表示されます。

Cisco EPN Manager に付属のテンプレートを編集する場合は、そのテンプレートのコピーを作成し、コピーに新しい名前を付けて編集します。既存のテンプレートを使用した新規CLI設定テンプレートの作成 （578 ページ）を参照してください。

作成したテンプレートは [マイ テンプレート（My Templates）] に保存されます。

始める前に

シスコ オプティカル ネットワーキング デバイスでは、設定テンプレートはデフォルトではサポートされていません。設定テンプレートのサポートを有効にするには、既存の定義済み CLI 設定テンプレートを選択して、その [デバイス タイプ（Device Type）] セクションで [オプティカル ネットワーキング（Optical Networking）] チェックボックスをオンにします。この CLI テンプレートを新規テンプレートとして保存します。テンプレートはユーザー定義テンプレートとして保存され、テンプレートに Cisco NCS 2000 デバイス、Cisco NCS 4000 デバイスなどのすべてのオプティカル ネットワーキング デバイスがリストされます。

ステップ 1 **[設定（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [CLI テンプレート（CLI Templates）] を展開し、[CLI] を選択します。

ステップ 3 [テンプレートの基本設定（Template Basic）] 領域で、次の操作を行います。

a) 意味のあるテンプレート名を入力します。テンプレートは、Web GUI にアルファベット順で表示されます。

b) （任意）テンプレートの用途に関する短い説明を入力します（たとえば、「IOS デバイスのトラップの有効化」など）。

c) （任意）直感的な名前でテンプレートにタグを付けます。タグについての説明を表示するには、[マイ タグ（My Tag）] を選択します。

d) テンプレートを実行するために使用できるデバイス オペレーティング システムを入力します（たとえば、12.2、15.3 など）。テンプレートを実行すると、古いデバイス OS バージョンがフィルタリングされて除外されます。このフィールドを空白のままにすると、テンプレートは指定されたデバイスのすべての OS に適用されます。

ステップ 4 [テンプレートの詳細（Template Detail）] 領域で、デバイス コンフィギュレーション コマンドを指定します。

a) [CLI コンテンツ（CLI Content）] フィールドに、コードを入力するか、またはコピーしたコードを貼り付けます。コマンドライン コンフィギュレーション セッション、CLI スクリプト、またはその他の保

存されている一連のコンフィギュレーション コマンドからコードをコピーできます。コードを入力するには、Apache VTL を使用する必要があります。

b) [変数の追加（Add Variables）] ダイアログを使用して、変数を設定します。テンプレートを実行する際に、これらの変数に値を入力するようプロンプトが出されます。

- コード内での名前を使用して変数を作成するには、コード（スペースなし）を選択し、[変数の追加（Add Variables）] 領域の右上にある [+] 記号をクリックします。これにより、[変数の追加（Add Variables）] ダイアログに、該当する名前で新しい（未設定の）変数が作成されます。
- [変数の追加（Add Variables）] 領域の右上にある [+] 記号をクリックします。これにより、[変数の追加（Add Variables）] ダイアログに空白の行が追加されます。

変数の作成については、テンプレートへの変数の入力 （579 ページ）を参照してください。

c) テンプレートを実行する際に変数がどのように表示されるかを確認するには、[フォーム ビュー（Form View）] をクリックします。

d) 変数を保存するには、[CLI に追加（Add to CLI）] をクリックします。

ステップ 5 テンプレートを保存します。[新しいテンプレートとして保存（Save as New Template）] をクリックして、[マイテンプレート（My Template）] でテンプレートを保存するフォルダを指定し、[保存（Save）] をクリックします。

（注）
1. [テンプレートの詳細（Template Detail）] 領域でのデバイス設定コマンドでは、特殊文字を使用できません。
2. [テンプレートの基本（Template Basic）] 領域の下にある [説明（Description）] フィールドに XML 固有の特殊文字を入力すると、テンプレートのエクスポートが失敗します。

既存のテンプレートを使用した新規 CLI 設定テンプレートの作成

新しい設定テンプレートを作成するのに最も簡単な方法は、同様の既存のテンプレートを見つけてコピーし、そのコピーを編集することです。作成済みのテンプレートも、この手順を使用して編集できます（編集できるテンプレートは、自分が作成したものだけです）。

ステップ 1 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [CLI テンプレート（CLI Templates）] を展開し、[システム テンプレート - CLI（System Templates - CLI）] を選択します。

ステップ 3 左側のテンプレートナビゲーション パネルで、コピーするテンプレートを見つけて、そのテンプレート名の横に表示されている [i] アイコンにマウスのカーソルを重ね、表示されるポップアップ ウィンドウで [複製（Duplicate）] をクリックします。

ステップ 4 [複製テンプレートの作成（Duplicate Template Creation）] ダイアログで、新しいテンプレートを保存するフォルダ（[マイ テンプレート（My Templates）] 内のフォルダ）を指定し、[OK] をクリックします。

たとえば、**[CLIテンプレート（CLI Templates）]** > **[システムテンプレート-CLI（System Templates - CLI）]** の下にあるテンプレートをコピーすると、そのテンプレートはデフォルトで **[マイテンプレート（My Templates）]** > **[CLIテンプレート（CLI Templates）]** > **[システムテンプレート-CLI（ユーザー定義）（System Templates - CLI (User Defined)）]** の下に保存されます。

ステップ 5 空白テンプレートを使用した新しい CLI 設定テンプレートの作成 （577 ページ） の説明に従って、検証基準と CLI コンテンツを追加します。

テンプレートへの変数の入力

次のトピックでは、テンプレートに変数を入力する場合に役立つ情報を提供します。

データ型

表 1 に、[変数の管理（Manage Variables）] ページで設定できるデータ型を示します。

データ タイプ	説明
文字列	CLIテンプレートのテキストボックスを作成できます。検証式とデフォルト値を指定するには、行を展開して[デフォルト値（Default Value）]および[検証式（Validation Expression）] フィールドを設定します。
整数（Integer）	数値のみを受け入れるテキストボックスを作成できます。整数の範囲を指定する場合は、行を展開して [範囲開始（Range From）] および [終了（To）] フィールドを設定します。検証式とデフォルト値を指定するには、行を展開して[デフォルト値（Default Value）] および[検証式（Validation Expression）] フィールドを設定します。
DB	データベースタイプを指定できます。CLIテンプレートのデータベース変数の管理 （580 ページ） を参照してください。
IPv4 アドレス（IPv4 Address）	CLI テンプレートに IPv4 アドレスのみを受け入れるテキスト ボックスを作成できます。検証式とデフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] および [検証式（Validation Expression）] フィールドを設定します。

ドロップダウン（Drop-down）	CLI テンプレートにリストを作成できます。検証式とデフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] フィールドを設定します（UI に表示される複数のリストにはコンマ区切り値を使用）。
チェックボックス（Check box）	CLI テンプレートのチェックボックスを作成できます。 検証式とデフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] フィールドを設定します。
オプション ボタン（Radio Button）	CLIテンプレートのオプションボタンを作成できます。検証式とデフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] フィールドを設定します。
テキスト領域	CLI テンプレートに複数の値を許可するテキスト領域を作成できます。検証式とデフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] および [検証式（Validation Expression）] フィールドを設定します。

CLI テンプレートのデータベース変数の管理

次のような場合は、データベース（DB）変数を使用できます。

- DB 変数が CLI テンプレートでデータ型の 1 つである場合。デバイス固有のコマンドを生成するために DB 変数を使用できます。
- DB 変数が事前定義された変数である場合。事前定義された DB 変数の一覧を表示するには、場所 folder/opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate にある CLITemplateDbVariablesQuery.properties ファイルを参照します。
- たとえば、SysObjectID、IPAddress、ProductSeries、ImageVersion は DB 変数です。デバイスが Cisco EPN Manager に追加されると、デバイスの完全な詳細が DB 変数に収集されます。つまり、デバイスの OID は SysObjectID に、製品シリーズは ProductSeries に、デバイスのイメージ バージョンは ImageVersion にというように収集されます。
- DB 変数によって収集されたデータを使用して、正確なコマンドをデバイスに生成できます。
- [タイプ（Type）] フィールドで DB 変数を選択できます（[管理対象の変数（Managed Variables）] ページを使用）。名前フィールドを展開して、使用する DB 変数のいずれかをデフォルト値のフィールドに入力します。
- デバイスが検出され、Cisco EPN Manager に追加された際に、インベントリ収集中に集められたデータベース値を使用して、CLI テンプレートを作成できます。

（注） Enterprise JavaBeans クエリ言語（EJB QL）を使用してカスタマイズされたクエリを作成することができますが、これを試行できるのは高度な開発者のみです。CLITemplateDbVariablesQuery.properties ファイルで定義された変数のみを使用することを推奨します。

検証式の使用

[検証式（Validation Expression）] で定義した値は、関連付けられているコンポーネント値で検証されます。たとえば、設計フローでデフォルト値と検証式の値を入力した場合、設計フロー中に検証されます。つまり、デフォルト値が検証式に入力された値と一致しない場合、設計フローで取得エラーが発生します。

（注） 検証式の値は、文字列データ型フィールドにのみ機能します。

たとえば、**[設定（Configuration）]**>**[テンプレート（Templates）]**>**[機能およびテクノロジー（Features and Technologies）]** の順に選択し、**[CLI テンプレート（CLI Templates）]** > **[CLI]** を選択します。[テンプレートの詳細（Template Detail）] 領域で、[変数の追加（Add Variable）] タブをクリックして変数のリストを表示します。[変数の追加（Add Variable）] タブで追加のプラス記号（+）をクリックし、CLI テンプレートに行を追加します。[タイプ（Type）] フィールドで [文字列（String）] を選択し、残りの値を入力して、[保存（Save）] をクリックします。変数のリストで、この新しい変数の詳細を展開し、正規表現を設定します。そのテキストボックスではスペースは許可されません。[検証式（Validation Expression）] フィールドに、次の式を入力します。

```
^[\S]+$
```

デフォルト値（オプション）：ncs

この値は、[検証式（Validation Expression）] フィールドの正規表現と一致する必要があります。

テンプレートを保存してからデバイスを選択します。テキストフィールドにスペースを入力してみてください。正規表現のエラーが発生するはずです。

マルチライン コマンドの追加

[CLI コンテンツ（CLI Content）] 領域にマルチライン コマンドを入力するには、次の構文を使用します。

```
<MLTCMD>First Line of Multiline Command
Second Line of Multiline Command
......
......
```

```
Last Line of Multiline Command</MLTCMD>
```

引数の説明

- <MLTCMD> および </MLTCMD> タグは大文字と小文字が区別され、大文字で入力する必要があります。
- マルチライン コマンドは、<MLTCMD> タグと </MLTCMD> タグで囲む必要があります。
- タグの先頭にはスペースを使用できません。
- <MLTCMD> と </MLTCMD> タグは単一行では使用できません。

例 1：

```
<MLTCMD>banner_motd Welcome to
Cisco. You are using
Multi-line commands.
</MLTCMD>
```

例 2：

```
<MLTCMD>banner motd ~ ${message}
</MLTCMD>
```

{message} はマルチライン入力変数です。

マルチライン バナー コマンドを使用する場合の制限事項

Cisco EPN Manager はマルチライン バナー コマンドをサポートしていません。次の例に示すように、*banner file xyz format* 形式を使用できます。

```
#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
(config)#parameter-map type webauth global
(config-params-parameter-map)# type webauth
(config-params-parameter-map)#banner file tftp://209.165.202.10/banner.txt
(config-params-parameter-map)#^Z
#more tftp://192.168.0.0/banner.txt
Disclaimer:
Usage of this wireless network is restricted to authorized users only.
Unauthorized access is strictly forbidden.
All accesses are logged and can be monitored.
#
```

イネーブル モード コマンドの追加

CLI テンプレートにイネーブル モード コマンドを追加する場合は、次の構文を使用します。

```
#MODE_ENABLE<<commands >>#MODE_END_ENABLE
```

インタラクティブ コマンドの追加

インタラクティブ コマンドには、コマンドの実行後に入力する必要がある入力が含まれています。

[CLI Content] 領域にインタラクティブ コマンドを入力するには、次の構文を使用します。

```
CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question
2<R>command response 2
```

<IQ> および <R> タグは大文字と小文字が区別され、大文字で入力する必要があります。

次に例を示します。

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

（注） 対話型の質問ではすべて、<IQNONEWLINE> タグを <IQNONEWLINE> タグに置き換える必要があります。これらの質問では、どのコントローラー デバイスでもコマンドでデフォルトの <return> または改行文字は必要ありません。たとえば、

```
#INTERACTIVE
transfer download start <IQNONEWLINE>y/N<R>y<IQNONEWLINE>y/N<R>y
#ENDS_INTERACTIVE
```

（注） <IQ> タグは、対話型の質問に正規表現を使用します。パターンを照合するには、有効な正規表現を使用する必要があります。

Format

```
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
```

Example for invalid content used in interactive question

```
#INTERACTIVE
save config<IQ>Are you sure you want to save? (y/n)<R>y
#ENDS_INTERACTIVE
```

間に質問マーク「?」を使用すると無効になり、パターンと一致しません。

Example for valid content used in interactive question

```
#INTERACTIVE
save config<IQ>(y/n)<R>y
#ENDS_INTERACTIVE
```

インタラクティブ イネーブル モード コマンドの組み合わせ

インタラクティブ イネーブル モード コマンドを組み合わせるには、次の構文を使用します。

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

次に例を示します。

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>XXX
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

インタラクティブ マルチライン コマンドの追加

以下は、複数行を含むインタラクティブ コマンドの例です。

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
@</MLTCMD>
#ENDS_INTERACTIVE
```

テンプレートでのグローバル変数の使用

Cisco EPN Manager では、カスタマイズした CLI 設定をデバイスに展開できます。このためには、カスタマイズした設定オプションを含む CLI テンプレートを作成します。CLI テンプレートの作成時、または既存のテンプレートの変更時に、グローバル変数またはテンプレート変数を使用してテンプレートの内容を定義できます。

- テンプレート変数：CLI テンプレートまたはサービスの作成時、変数に値を入力できます。
- グローバル変数：事前に定義され、CLIテンプレートまたはサービスにグローバル レベルで関連付けられています（デフォルト）。サービス作成時に、グローバル変数を表示することや、グローバル変数の値を入力することはできません。

すべての変数名は、グローバル変数またはテンプレート変数のいずれであるかを示す単語で始まります。グローバル変数は、CLI テンプレートや複合テンプレートなどすべての Cisco EPN Manager テンプレートで使用できます。グローバル変数は、変数に関連付けることができるタイプ オブ サービス（CE、L3VPN、CEM など）を識別します。新しいグローバル変数を作成するときには、文字「gv」で始まり、変数を容易に把握できる単語が続く名前を必ず指定してください。作成するグローバル変数は、さらに編集したり削除したりできます。Cisco EPN Manager でデフォルトで使用可能なグローバル変数は、編集または削除できません。グローバル変数はすべてのテンプレート タイプに適用されますが、CLIテンプレートの作成時に作成された変数は、そのテンプレートだけに適用されます。CLIテンプレートの作成時に作成された変数を他の CLI テンプレートに関連付けることはできません。

以下に示すCLIテンプレートの設定例では、「gv.service-ethernet-maintInterfaceName」はグローバル変数です。このテンプレートがサービスに関連付けられている場合、サービスの作成時に、グローバル変数の変更可能な部分（mainInterfaceName）が、サービスで指定されている値（CE サービスのイーサネット インターフェイス名など）に置き換えられます。ただし、サービス作成時にこのグローバル変数を表示または変更することはできません。「$descr」はテンプレート変数を示す静的な値です。このテンプレート変数により、サービス作成時に（説明フィールドの）文字列（String）型の変数を変更または指定できます。

```
interface $gv.service-ethernet-mainInterfaceName
            description $descr
          exit
```

グローバル変数を使用して CLI テンプレートを作成するには、次の手順に従います。

ステップ 1 **[設定（Configuration）]** > **[テンプレート（Templates）]** > **[グローバル変数（Global Variable）]** の順に選択し、新しいグローバル変数を作成します。

Cisco EPN Manager で各サービス タイプ（CE、L3VPN、および CEM）に事前に読み込まれている既存のグローバル変数を使用するには、ステップ 4 に移動します。

ステップ 2 追加（「+」）アイコンをクリックします。既存の変数を編集するには、グローバル変数を選択して [編集（Edit）] ボタンをクリックします。

ステップ 3 以下のパラメータを指定し、[保存（Save）] をクリックします。変更内容が Cisco EPN Manager データベースに保存されますが、デバイスに即時には展開されるわけではありません。

- [名前（Name）]：変数の一意の名前を入力します。名前は文字「gv」で始まり、その後にこのグローバル変数が関係するサービス タイプが続くものにしてください。ドット、ハイフン、アンダースコアなどの特殊文字を使用できます。
- [説明（Description）]：変数を簡単に確認できるようにする一意の説明を入力します。CLI テンプレートで使用するこの変数の目的を確認できるようにするため、この説明は非常に重要です。CLI テンプ

レートは、サービス（L2、L3 サービスなど）のプロビジョニングにも使用できます。サービス作成ページでは、変数の目的を確認できる唯一の情報が変数の説明です。

- [タイプ（Type）]：次のいずれかのオプションを使用して変数のタイプを指定します。
  - [文字列（String）]：CLI テンプレートのテキスト ボックスを作成できます。サービス プロビジョニングで使用する CLI テンプレートには、文字列タイプの変数だけが適用されます。
  - [整数（Integer）]：数値だけを受け入れるテキスト ボックスを作成できます。後で値の範囲を指定するように設定できます。
  - [IPv4 アドレス（IPv4 Address）]：CLI テンプレートの IPv4 アドレスのみを受け入れるテキスト ボックスを作成できます。
  - [ドロップダウン（Drop-down）]：CLI テンプレートのドロップダウンリストを作成できます。
  - [チェックボックス（Check box）]：CLI テンプレートのチェックボックス フィールドを作成できます。
  - [オプション ボタン（Radio Button）]：CLI テンプレートのオプション ボタンを作成できます。
  - [テキスト領域（Text Area）]：CLI テンプレートの複数行の値の入力を許可するテキスト領域を作成できます。
- [値（Value）]：前述の [タイプ（Type）] で選択した値に基づいて生成する必要がある値を指定します。

  サービスまたはCLIテンプレートの作成時に値を指定するには、プレースホルダとして[使用不可（Not Available）] を選択できます。
- [表示ラベル（Display Label）]：Cisco EPN Manager GUI での変数の表示方法を入力します。

ステップ 4 CLI テンプレートとグローバル変数を関連付けます。

a) [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] の順に移動します。

b) 新しい CLI テンプレートを最初から作成するには、空白テンプレートを使用した新しい CLI 設定テンプレートの作成 （577 ページ）を参照してください。

c) 既存のテンプレートにグローバル変数を関連付けるには、既存のテンプレートを使用した新規 CLI 設定テンプレートの作成 （578 ページ）を参照してください。

d) グローバル変数を追加するには、[テンプレートの詳細（Template Details）] セクションで [グローバル テンプレートの追加（Add Global Variable）] 検索フィールドを使用して、グローバル変数を検索します。ページの右上隅に表示される [グローバル変数（Global Variable）] ハイパーリンクを使用すると、簡単に確認できます。1 つの同じ CLI テンプレートで、CLI 変数およびテンプレート変数とともにグローバル変数を使用できます。

変数が属しているサービスを確認するには、変数名を調べます。CE サービスに適用される変数の変数名は「gv.ce-service-ethernet*」で始まります。L3VPN サービスに適用される変数の変数名は「gv.l3vpn-service-l3vpn*」で始まります。これらの変数には、新しい CLI 変数または既存の CLI 変数を関連付けることができます。

a) CLI テンプレートに必要な変更を行い、[新しいテンプレートとして保存（Save as New Template）] をクリックします。
b) CLI テンプレートが保存され、[マイ テンプレート（My Templates）] > [CLI テンプレート（ユーザー定義）（CLI Templates (User Defined)）] に表示されます。
c) （任意）デバイスへのテンプレートの展開 （591 ページ）の説明に従い、CLI テンプレートをデバイスに展開します。

ステップ 5 （オプション）（グローバル変数とテンプレート変数が関連付けられている）CLI テンプレートを使用してサービス（L2、L3VPN、CEM、Flex LSP、レイヤ 3 リンク）をプロビジョニングするには、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

例

Cisco EPN Manager で使用可能なサンプル グローバル変数：

- L3VPN サービスで使用できるサンプル グローバル変数を次に示します。

☐	gv.service-l3vpn-InterfaceDetailsMap	Interface Detail	String
☐	gv.service-l3vpn-bgpASNumber	BGP AS Number	String
☐	gv.service-l3vpn-bgpNeighborASNu...	BGP Neighbor AS Number	String
☐	gv.service-l3vpn-bgpNeighborAddres...	Neighbor Address Family	String
☐	gv.service-l3vpn-bgpNeighborsList	BGP Neighbor	String
☐	gv.service-l3vpn-bgpRouterId	BGP Router ID	String
☐	gv.service-l3vpn-bridgeDomainList	Bridge Domain ID	String
☐	gv.service-l3vpn-mainInterfaceName...	Main Interface Name	String
☐	gv.service-l3vpn-ospfArea	OSPF Area	String
☐	gv.service-l3vpn-ospfProcessId	OSPF Process ID	String
☐	gv.service-l3vpn-serviceInstanceNu...	Service Instance Number	String
☐	gv.service-l3vpn-serviceInterfaceNa...	Sub-Interface or BDI/BVI Name	String
☐	gv.service-l3vpn-vrfAddressFamilyList	VRF Routing Address Family	String
☐	gv.service-l3vpn-vrfName	VRF Name	String

- CEM サービスで使用できるサンプル グローバル変数を次に示します。

gv.service-cem-auNumber	AU (AU-3 or AU-4) number	String
gv.service-cem-cemFrameType	CEM frame type	String
gv.service-cem-cemGroupNumber	CEM group number	String
gv.service-cem-cemGroupNumberList	CEM group number list for local connects	String
gv.service-cem-cemInterfaceName	CEM interface name	String
gv.service-cem-cemInterfaceNameList	CEM interface name list for local connects	String
gv.service-cem-controllerInterfaceName	Controller name	String
gv.service-cem-e1Number	E1 number	String
gv.service-cem-l2vpnContextName	L2VPN context name	String

CLI 設定テンプレートのインポートとエクスポート

次の項目で、設定テンプレートのエクスポート方法とインポート方法を説明します。テンプレートはエクスポートでき、テンプレートには .xml ファイル名が付けられます。また、テンプレートが複数ある場合は zip ファイルとしてエクスポートされます。

- 複数の設定テンプレートをエクスポートする場合は、.xml ファイルが zip ファイルに配置され、**Exported Templates** というプレフィックス名が付与されます。
- 単一のファイルのエクスポートとインポートは .xml ファイルとして実行されます。
- 個別のファイルを選択するか、または zip ファイルをインポートすることで、複数の .xml ファイルをインポートできます。
- CLI テンプレートをインポートする場合、ファイルに含まれているユーザー定義のグローバル関数は自動的にはインポートされません。これらの変数は CLI テンプレートに手動で追加する必要があります。
- CLI コマンドを使用して CLI テンプレートをインポートする場合は、有効な構文を使用して変数名を必ず使用してください。変数名はアルファベットまたはアンダースコア（_）で始まる必要があります。サポートされている特殊文字は、アンダースコアとハイフンです。

警告 テンプレート変数はインポート時に検証されないため、適切な変数名を必ず使用してください。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]の順に選択します。>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]の順に選択します。

ステップ 2 設定テンプレートをエクスポートするには、次の手順を実行します。

a) エクスポートするテンプレートを選択し、 をクリックします。

b) 目的の場所にファイルを保存します。

（注） [説明（Description）] フィールドまたは [テンプレートの詳細（Template Detail）] フィールドに XML 固有の特殊文字がある場合は、テンプレートのエクスポートが失敗します。

ステップ 3 設定テンプレートをインポートするには、次の手順を実行します。

a) [CLI テンプレート（CLI Templates）] フォルダで、**CLI** の横にある [i] の上にマウス カーソルを合わせます。

b) [すべてのテンプレートの表示（Show All Templates）] をクリックし、[インポート（Import）] をクリックします。

c) [テンプレートのインポート（Import Templates）] ダイアログボックスで、テンプレートのインポート先の [マイ テンプレート（My Templates）] フォルダを選択し、[テンプレートの選択（Select Templates）] をクリックしてインポートするファイルまで移動します。

d) 選択したテンプレートを確認し、[OK] をクリックします。

新規複合テンプレートの作成

事前に設定したテンプレートやユーザーが作成したテンプレートのすべてを単一の複合テンプレートに追加できます。このテンプレートは、必要としている個々の機能テンプレートすべてを集約します。また、複合テンプレートを作成すると、メンバーテンプレートを実行する順序も指定できます。複合テンプレートを使用して、単一のデバイスまたはデバイスのグループに変更を加えることができます。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [複合テンプレート（Composite Templates）] フォルダを展開し、[複合テンプレート（Composite Templates）] を選択します。

ステップ 3 [テンプレートの基本設定（Template Basic）] 領域に、テンプレートの名前を入力します。

ステップ 4 [テンプレートの詳細（Template Detail）] 領域で、複合テンプレートに含めるテンプレートを選択します。矢印を使用し、デバイスに展開する順序でテンプレートを配置します。たとえば、ACL を作成し、インターフェイスに関連付けるには、まずACLテンプレートを配置し、その後にインターフェイステンプレートを続けます。

ステップ 5 [新しいテンプレートとして保存（Save as New Template）] をクリックします。テンプレートを保存した後にデバイスに適用します（「」を参照してください）。

タグを使用したテンプレートへのショートカットの作成

タグをテンプレートに適用すると、そのテンプレートは [マイ タグ（My Tags）] フォルダのリストに表示されます。設定テンプレートにタグ付けすることで、以下を行う際に役立ちます。

- 検索フィールドでタグ名を使用したテンプレートの検索
- 追加のデバイスを設定するための、参照としてのタグ付けされたテンプレートの使用

既存のテンプレートにタグ付けするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [マイ テンプレート（My Templates）] フォルダを展開し、タグを付けるテンプレートを選択します。

ステップ 3 [次のタグを使用（Tag as）] テキスト ボックスにタグ名を入力し、[保存（Save）] をクリックします。

トラブルシューティング テンプレートの作成

トラブルシューティングテンプレートを使用して、デバイス上で実行する一連の再利用可能な非設定コマンド（「show」コマンドなど）を定義します。

トラブルシューティング テンプレートを作成するには

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [CLI テンプレート（CLI Templates）] を展開し、[CLI] を選択します。

ステップ 3 [テンプレートの基本設定（Template Basic）] 領域で、次の操作を行います。

a) テンプレートの名前を入力します。

b) [Troubleshooting Template] チェックボックスをオンにします。これを行うと、テンプレートがトラブルシューティング テンプレートに変更され、トラブルシューティング テンプレートとしてタグ付けされます。

（注）
1. タイプデバイス用のトラブルシューティング テンプレートのみを作成できます。
2. [Tags] フィールドの「TroubleshootingTemplate」タグは編集しないでください。

ステップ 4 [Template Detail] 領域で、必要に応じてコマンドと変数を指定します。変数の作成については、テンプレートへの変数の入力 （579 ページ）を参照してください。

ステップ 5 テンプレートを保存します。[新しいテンプレートとして保存（Save as New Template）] をクリックして、[マイテンプレート（My Template）] でテンプレートを保存するフォルダを指定し、[保存（Save）] をクリックします。

（注） 「MODE_ENABLE」をトラブルシューティング テンプレートと一緒に使用することはできません。

次のタスク

トラブルシューティング テンプレートを展開し、失敗したテンプレートの展開を編集/再試行する手順は、CLI テンプレートの場合と同様です。次の項を参照してください。

- ウィザードを使用した CLI テンプレートの展開フロー （594 ページ）
- デプロイに失敗したテンプレートの編集と再試行 （601 ページ）

デバイスへのテンプレートの展開

ここでは、構成テンプレートを使用してデバイスにコマンド グループを展開（実行）する方法について説明します。

- デバイスのグループにテンプレートを展開するための設定グループの作成
- ウィザードを使用した設定グループの展開フロー
- ウィザードを使用した CLI テンプレートの展開フロー
- ウィザードを使用した複合テンプレートの展開フロー
- 設定グループを使用しないデバイスへのテンプレートの展開

設定導入動作の制御

管理者は、 ユーザーが新しいデバイス設定テンプレートを展開するときに、デバイス設定をバックアップするか、またはロールバックするかを選択できます。

テンプレート導入前のデバイス設定のアーカイブ

[デバイス設定のバックアップ（Backup Device Configuration）] が有効になっている場合は、新しい設定テンプレートが展開される前に、Cisco EPN Manager がすべてのデバイスの実行時の設定とスタートアップ/管理設定を自動的にバックアップします。

1. **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [設定（Configuration）]** を選択します。

2. [デバイス設定のバックアップ（Backup Device Configuration）] チェックボックスをオンにします。
3. [保存（Save）] をクリックします。

テンプレート導入失敗時のデバイス設定のロールバック

新しい設定テンプレートのデバイスへの展開に失敗した場合、 Cisco EPN Manager は、最後にアーカイブされた実行時の設定とスタートアップ/管理設定に各デバイスを自動的にロールバックします。

1. **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [設定（Configuration）]** を選択します。
2. [設定のロールバック（Rollback Configuration）] チェックボックスをオンにします。
3. [保存（Save）] をクリックします。

デバイスのグループにテンプレートを展開するための設定グループの作成

複数のデバイスに同じ設定が必要な場合、それらのデバイスとデバイスに共通して適用できるテンプレートを含む設定グループを作成できます。設定グループを作成することで、新しいテンプレートを展開するデバイスを覚えていなくても、新しいテンプレートをすぐに適用できます。

複合テンプレートではサイズの小さい複数のテンプレートを1つにグループ化できる一方、設定グループは、テンプレートとデバイスのグループとの「関係」およびコマンドの実行順を指定します。

ステップ 1 **[構成（Configuration）] > [テンプレート（Templates）] > [設定グループ（Configuration Groups）]** の順に選択します。

ステップ 2 [設定グループの基本（Configuration Group Basic）] 領域で、名前を入力します。

ステップ 3 選択可能なデバイスを表示するには、[テンプレートの選択（Template Selection）] 領域で [追加（Add）] をクリックし、テンプレートを選択して1つ以上のテンプレートを追加します。これにより、[デバイスタイプ（Device Type）] フィールドにも値が取り込まれます。

ステップ 4 さらにテンプレートを追加するには、[テンプレートの選択（Template Selection）] 領域で [追加（Add）] をクリックします。相互に排他的なテンプレート（たとえば、Add-Host-Name-IOS と Add-Host-Name-IOS-XR）を同時に選択することはできません。

ステップ 5 テンプレートを展開するデバイスを選択し、[次へ（Next）]をクリックして入力オプションを選択します。

ステップ 6 [デバイスの選択（Device Selection）] 領域で、設定グループに追加するデバイスを選択します。

ステップ 7 複数のテンプレートを使用する場合、テンプレートを選択して上矢印または下矢印をクリックすることで、テンプレートがリストされる順序を変更できます。

ステップ 8 [新しい設定グループとして保存（Save as New Configuration Group）] をクリックします。

ウィザードを使用した設定グループの展開フロー

（注） この展開フローは、コントローラ ベースのテンプレートには適用されません。

ステップ 1 設定グループを作成したら、[展開（Deploy）] をクリックします。[テンプレートの展開 - 準備とスケジュール（Template Deployment -Prepare and Schedule）] ウィザード ページが開きます。

ステップ 2 [テンプレート（Templates）] 領域で、設定グループに追加するテンプレートを表示します。

ステップ 3 [デバイスに展開（Deployed on Devices）] 領域および設定グループの作成中に、設定グループの作成時に選択したデバイスを表示します。

ステップ 4 [値の割り当て（Value Assignment）] 領域で、[テンプレートの選択（Select Template）] ドロップダウン リストから、CLIテンプレートと適切なデバイスを選択します。テンプレートを展開するデバイスの詳細や、CLI プレビューの詳細などを表示できます。[適用（Apply）] をクリックします。

ステップ 5 （任意）[スケジュール（Schedule）] 領域で展開ジョブをスケジュールします。

- わかりやすい展開ジョブ名を付けてから、ただちに実行するか、後で実行するかを指定します。
- また、時間単位、日次、週次、月次、または年次単位で定期的にジョブを実行するようにスケジュールできます。
- 次のジョブ オプションを設定できます。

  失敗ポリシー（Failure Policy）：

  - [失敗を無視して続行（Ignore failure and continue）]：これはデフォルトのオプションです。 デバイスは、テンプレートの展開にランダムに選択されます。ジョブを実行できないデバイスがあった場合、そのデバイスをスキップし、引き続き残りのデバイスでジョブを実行します。ジョブ結果には、選択したすべてのデバイスの成功/失敗情報が表示されます。
  - [失敗で停止（Stop on failure）]：ジョブがデバイスでの実行に失敗した場合、そのジョブは停止します。 ジョブ結果は、ジョブが正常に実行されたデバイスと、テンプレートの展開が行われなかった他のデバイスについてのみ更新されます。「未試行（Not Attempted）」メッセージが表示されます。展開のために選択されたデバイスの順序は、[値の割り当て（Value assignment）] ペインのデバイスの順序と同じです。
  - [実行コンフィギュレーションをスタートアップにコピー（Copy Running Config to Startup）]：テンプレートの展開ジョブが成功すると、デバイスの実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。
  - [展開後にコンフィギュレーションをアーカイブ（Archive Config after deploy）]：新しい設定アーカイブ ジョブを作成し、テンプレートを正常に展開した後で、デバイスのコンフィギュレーションをアーカイブします。

ステップ 6 [概要（Summary）] 領域で、展開の概要を表示します。

ステップ 7 [OK] をクリックしてテンプレートを展開します。

ステップ 8 ジョブのステータスを表示するには、ポップアップ ダイアログボックスで [ジョブのステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] を起動します。

ウィザードを使用した CLI テンプレートの展開フロー

ステップ 1 CLIテンプレートを作成した後、[展開（Deploy）] をクリックします。[展開（Deployment）] ウィザードページが開きます。

ステップ 2 テンプレートを展開するデバイスを選択し、[次へ（Next）] をクリックして入力オプションを選択します。

ステップ 3 [デバイスの追加（Add devices）] テーブルから、テンプレートを展開するデバイスを選択します。選択したデバイスが [展開するデバイス（Devices to deploy）] テーブルに表示されます。

ステップ 4 テンプレートを展開するモードを選択します。オプションは、[ワークフロー（Work Flow）]および[CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] です。

ステップ 5 [ワークフロー（Work Flow）] オプションをクリックし、[次へ（Next）] をクリックします。ステップ *6* を参照してください。

ステップ 6 または、[CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] オプションをクリックし、CSV のエクスポート/インポート メカニズムを使用して選択したデバイスのテンプレート プロパティをすべて更新します。

a) CSV ファイル内の設定値の入力時に省略可能フィールドをスキップする場合は、[省略可能パラメータも必要ですか（Do you want Optional Parameters）] チェックボックスをオフにします。
b) [CSV のエクスポート（Export CSV）] をクリックし、ローカル システムに CSV テンプレートをダウンロードします。
c) ダウンロードした CSV テンプレートで個々のデバイスの設定値を入力します。
d) [CSV のインポート（Import CSV）] をクリックし、更新した CSV ファイルをアップロードします。入力値は自動的に更新されます。
e) [次へ（Next）] をクリックして値を入力します。

ステップ 7 [入力値（Input Values）] タブでは、[フォーム（Form）] ビューと [CLI] ビューを切り替えることができます。[入力値（Input Values）] タブで以下を設定します。

a) 各テンプレートのすべての必須フィールドに入力してから、[適用（Apply）] をクリックします。

（注） プロファイル管理では、Fault-Profile-Definition および Fault-Profile-Apply テンプレートを使用できます。これらのテンプレートを展開するときに、[入力値（Input Values）] ウィンドウで、参照テーブルから選択した障害タイプに該当する障害タグを入力する必要があります。

検証が成功すると、選択したテンプレートの周囲の円の境界が緑色に変わります。

（注） 検証メッセージが正常に表示された場合は、変更がワークフロー内の選択したデバイスにのみ適用されたことを意味します。設定を完了するには、手順の残りのステップを実行します。

ステップ 8 必要な設定値を入力したら、[次へ（Next）]または[CLI]をクリックして、デバイスおよびテンプレートの設定値を確認します。

ステップ 9 必要に応じて、[展開のスケジュール設定（Schedule Deployment）] タブを使用して展開ジョブをスケジュール設定します。

- わかりやすい展開ジョブ名を付けてから、ただちに実行するか、後で実行するかを指定します。
- また、時間単位、日次、週次、月次、または年次単位で定期的にジョブを実行するようにスケジュールできます。
- 次のジョブ オプションを設定できます。

  失敗ポリシー（Failure Policy）：

  - [失敗を無視して続行（Ignore failure and continue）]：これはデフォルトのオプションです。 デバイスは、テンプレートの展開にランダムに選択されます。ジョブを実行できないデバイスがあった場合、そのデバイスをスキップし、引き続き残りのデバイスでジョブを実行します。ジョブ結果には、選択したすべてのデバイスの成功/失敗情報が表示されます。
  - [失敗で停止（Stop on failure）]：ジョブがデバイスでの実行に失敗した場合、そのジョブは停止します。 ジョブ結果は、ジョブが正常に実行されたデバイスと、テンプレートの展開が行われなかった他のデバイスについてのみ更新されます。「未試行（Not Attempted）」メッセージが表示されます。展開のために選択されたデバイスの順序は、[値の割り当て（Value assignment）]ペインのデバイスの順序と同じです。
  - [実行コンフィギュレーションをスタートアップにコピー（Copy Running Config to Startup）]：テンプレートの展開ジョブが成功すると、デバイスの実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。
  - [展開後にコンフィギュレーションをアーカイブ（Archive Config after deploy）]：新しい設定アーカイブ ジョブを作成し、テンプレートを正常に展開した後で、デバイスのコンフィギュレーションをアーカイブします。

ステップ 10 [次へ（Next）] をクリックしてジョブ展開サマリーを表示します。

ステップ 11 各デバイスの CLI ビューを [展開サマリー（Deployment Summary）] タブに表示できます。

ステップ 12 [終了（Finish）] をクリックしてテンプレートを展開します。

ステップ 13 ジョブのステータスを表示するには、ポップアップ ダイアログボックスで [ジョブのステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] を起動します。

（注） SG220 デバイスは設定テンプレートの展開をサポートしませんが、SG300 および SG500 デバイスは CLI テンプレート展開をサポートします。ただし、SG300 デバイスおよび SG500 デバイスはどちらも、次のシステム CLI テンプレートのみサポートします。

- APIC ブートストラップ
- バナー構成 - IOS（Banner Configuration-IOS）
- Best_Practice_Access_3k
- Best_Practice_Access_4k
- Best_Practice_Global
- 認証局 - IOS（Certificate Authority-IOS）
- SNMPv3 の設定
- VLAN の設定
- Configure_Access_Port
- クリプト マップの設定
- DNS の設定
- EEM Environmental Variables
- イネーブルパスワード - IOS（Enable Password-IOS）
- EtherChannel
- HTTP SWIM イメージ アップグレード テンプレート
- HTTP-HTTPSサーバーおよびWSMAの構成 - IOS（HTTP-HTTPS Server and WSMA Configuration-IOS）
- ローカル管理ユーザー
- プラグアンドプレイ ブートストラップ
- RADIUS_AUTH
- Radius Acct. サーバー
- Radius 設定-IOS
- リロード構成 - IOS（Reload Configuration-IOS）
- TACACS サーバー
- TACACS-POST-PNP
- トラップ受信者
- stp

（注） **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] > [デバイス/アーカイブ（Devices/Archives）] > [設定の展開（Deploy Config）]** を選択して、テンプレートベースの設定（ユーザー定義テンプレートまたはシステム定義テンプレート）をデバイスにプッシュすることもできます。

ウィザードを使用した複合テンプレートの展開フロー

ステップ 1 [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [複合テンプレート（Composite Templates）] > [複合テンプレート（Composite Templates）] の順に選択します。

ステップ 2 [テンプレートの基本設定（Template Basic）] セクションに、必要な情報を入力します。

ステップ 3 [テンプレートの詳細（Template Detail）] 領域で、複合テンプレートに含めるテンプレートを選択し、[新しいテンプレートとして保存（Save as New Template）] をクリックします。

ステップ 4 複合テンプレートを作成した後、[展開（Deploy）] をクリックします。[展開（Deployment）] ウィザードページが開きます。

ステップ 5 テンプレートを展開するデバイスを選択します。

ステップ 6 [デバイスの追加（Add devices）] テーブルから、テンプレートを展開するデバイスを選択します。選択したデバイスが [展開するデバイス（Devices to deploy）] テーブルに表示されます。

ステップ 7 テンプレートを展開するモードを選択します。オプションは、[ワークフロー（Work Flow）] および [CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] です。

ステップ 8 [ワークフロー（Work Flow）] オプションをクリックし、[次へ（Next）] をクリックします。ステップ *6* を参照してください。

ステップ 9 または、[CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] オプションをクリックし、CSV のエクスポート/インポート メカニズムを使用して選択したデバイスのテンプレート プロパティをすべて更新します。

a) CSV ファイル内の設定値の入力時に省略可能フィールドをスキップする場合は、[省略可能パラメータも必要ですか（Do you want Optional Parameters）] チェックボックスをオフにします。
b) [CSV のエクスポート（Export CSV）] をクリックし、ローカル システムに CSV テンプレートをダウンロードします。
c) ダウンロードした CSV テンプレートで個々のデバイスの設定値を入力します。
d) [CSV のインポート（Import CSV）] をクリックし、更新された CSV ファイルをアップロードします。入力値は自動的に更新されます。
e) [次へ（Next）] をクリックして値を入力します。

ステップ 10 [入力値（Input Values）] タブでは、[フォーム（Form）] ビューと [CLI] ビューを切り替えることができます。[入力値（Input Values）] タブで以下を設定します。

a) ナビゲーション ウィジェットでデバイスのテンプレートを選択します。テンプレートを選択するには、右上隅の円（T1、T2、T3、T4、T5、...）をクリックします。テンプレートが 5 個より多い場合

は、3 つのドットをクリックします。使用可能なすべてのテンプレートがあるドロップダウン リストが表示されます。

b) 各テンプレートのすべての必須フィールドに入力してから、[適用（Apply）] をクリックします。

検証が成功すると、選択したテンプレートの周りの輪郭線が緑色に変わり、ポップアップで使用可能なテンプレートとして選択されたテンプレートの隣に緑色のチェックマークが表示されます。

ステップ 11 必要な設定値を入力したら、[次へ（Next）] または [CLI] をクリックして、デバイスおよびテンプレートの設定値を確認します。

ステップ 12 必要に応じて、[展開のスケジュール設定（Schedule Deployment）] タブを使用して展開ジョブをスケジュール設定します。

- わかりやすい展開ジョブ名を付けてから、ただちに実行するか、後で実行するかを指定します。
- また、時間単位、日次、週次、月次、または年次単位で定期的にジョブを実行するようにスケジュールできます。
- 次のジョブ オプションを設定できます。

  失敗ポリシー（Failure Policy）：

  - [失敗を無視して続行（Ignore failure and continue）]：これはデフォルトのオプションです。デバイスは、テンプレートの展開にランダムに選択されます。ジョブを実行できないデバイスがあった場合、そのデバイスをスキップし、引き続き残りのデバイスでジョブを実行します。ジョブ結果には、選択したすべてのデバイスの成功/失敗情報が表示されます。
  - [失敗で停止（Stop on failure）]：ジョブがデバイスでの実行に失敗した場合、そのジョブは停止します。 ジョブ結果は、ジョブが正常に実行されたデバイスと、テンプレートの展開が行われなかった他のデバイスについてのみ更新されます。「未試行（Not Attempted）」メッセージが表示されます。展開のために選択されたデバイスの順序は、[値の割り当て（Value assignment）] ペインのデバイスの順序と同じです。
  - [実行コンフィギュレーションをスタートアップにコピー（Copy Running Config to Startup）]：テンプレートの展開ジョブが成功すると、デバイスの実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。
  - [展開後にコンフィギュレーションをアーカイブ（Archive Config after deploy）]：新しい設定アーカイブ ジョブを作成し、テンプレートを正常に展開した後で、デバイスのコンフィギュレーションをアーカイブします。

ステップ 13 [次へ（Next）] をクリックしてジョブ展開サマリーを表示します。

ステップ 14 [展開サマリー（Deployment Summary）] タブに、各デバイスの CLI ビューが表示されます。

ステップ 15 [終了（Finish）] をクリックしてテンプレートを展開します。

ステップ 16 ジョブのステータスを表示するには、ポップアップ ダイアログボックスで [ジョブのステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] を起動します。

設定グループを使用しないデバイスへのテンプレートの展開

テンプレートを保存すると、デバイスで展開（実行）できるようになります。テンプレートは、**[構成（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** ナビゲーション領域から、または **[構成（Configuration）]** > **[テンプレート（Templates）]** > **[設定グループ（Configuration Groups）]** から起動できる [設定グループ（Configuration Groups）] を使用して展開できます（デバイスのグループにテンプレートを展開するための設定グループの作成 （592 ページ） を参照）。

[機能およびテクノロジー（Features & Technologies）] ナビゲーション領域からカスタマイズされたテンプレートまたはシステム テンプレートを展開するには、次の手順を実行します。

ステップ 1 **[構成（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 展開するテンプレートが含まれているドロワーを展開します。

ステップ 3 展開するテンプレートを選択し、[展開（Deploy）] をクリックします。

ステップ 4 [テンプレートの展開（Template Deployment）] ウィンドウで、設定とスケジュールを確認し、**OK** をクリックします。

テンプレート展開のためのロールベース アクセス コントロール

Cisco EPN Manager は、テンプレート展開のロールベースの制限をサポートしています。この機能を使用すると、承認されたユーザーグループのユーザーにテンプレートの表示と展開のみを許可できます。作成、編集、削除、インポート、エクスポートなど、テンプレートに対する他のすべての操作は制限されます。

（注） この機能は、CLI テンプレートにのみ適用されます。

タスク権限とジョブ権限

管理者またはルートユーザーとしてログインし、次のタスク権限を持つユーザーグループを作成します。（タスク権限は、**[管理（Administration）]**>**[ユーザー（Users）]**>**[ユーザー、ロール、およびAAA（Users, Roles & AAA）]** > **[ユーザーグループ（User Groups）]** ウィンドウで確認できます）。

- [アクセス設定の展開（Deploy Configuring Access）] の有効化
- [設計設定テンプレートへのアクセス（Design Configuration Template Access）] の無効化

設定展開ジョブを管理するには、ユーザーグループに対して次のジョブ権限を有効にします。これらのジョブ権限がないと、ユーザーはジョブを表示、編集、実行できません。

- [ジョブの編集（Edit Job）]

- ジョブの実行（Run Job）
- ジョブの表示（Schedule Job）

テンプレート展開のロールベースアクセスの有効化

テンプレート展開のロールベースアクセスコントロールを有効にするには、[ルート（Root）]、[管理者（Admin）]、または [設定（Config）] ユーザーとしてログインし、**[テンプレートの基本（Template Basic）]** 領域（**[構成（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** > **[CLIテンプレート（CLI Templates）]** > **[CLI]**）で **[ユーザーグループ（User group）]** ドロップダウンリストからテンプレートをユーザーグループに割り当てます。**[ユーザーグループ（User group）]** ドロップダウンリストには、前述のタスク権限で設定されたユーザーグループのみが含まれます。このリストから1つ以上のユーザーグループにテンプレートを割り当てることができます。

テンプレートをユーザーグループに割り当てた後は、承認されたユーザーグループのユーザーのみがテンプレートを表示および展開できます。未承認のユーザーグループのユーザーは、テンプレートを表示できません。

複合テンプレートの場合、含まれるすべての CLI テンプレートを実行するための適切なユーザーグループ権限を持つユーザーのみがテンプレートを展開できます。

展開ユーザーは、関連付けられたユーザーグループに割り当てられたテンプレートに対してのみ、ジョブを編集または実行できます。

（注）
- どのユーザーグループにも割り当てられていないテンプレートには、すべてのユーザーがアクセスして展開できます。
- ユーザーグループに関連付けられたテンプレートをインポートする場合は、RBACテンプレートがシームレスに機能するように、展開の「ユーザーグループ」のロールが送信元システムと宛先システムで同じであることを確認します。
- 展開のユーザーグループのロールに不一致がある場合は、テンプレートをユーザーグループに再割り当てするか、テンプレートを編集して既存のすべてのユーザーグループの関連付けを削除し、テンプレートを保存することをお勧めします。

展開した設定テンプレートのステータスと結果の確認

設定テンプレートをデプロイすると、Cisco EPN Manager にハイパーリンク付きのダイアログボックスが表示され、[ジョブ（Jobs）] ウィンドウに移動できます。ここから、次の操作を実行できます。

- [履歴] タブをクリックし、ジョブインスタンスを展開して、コマンドの結果を表示する。
- 展開を繰り返すか、後でスケジュールする。
- ジョブを管理する（削除、一時停止、再開など）。

テンプレート展開失敗の Syslog

デバイスへのテンプレートの展開に失敗すると、Cisco EPN Manager は重大度が ERROR の syslog を生成し、EPNM で設定された宛先 IP に送信します。

この宛先IPを設定するには、「Syslogとしてのシステム監査ログの転送（1099ページ）」を参照してください。

syslog の生成を有効にするには、次の手順に従います。

1. **[管理（Administration）]** > **[設定（Settings）]** > **[ロギング（Logging）]** > **[SysLogロギングオプション（Syslog Logging Option）]** の順に選択します。
2. [SysLogを有効にする（Enable Syslog）] チェックボックスをオンにします。

デプロイに失敗したテンプレートの編集と再試行

デプロイ時に指定された値が正しくないか、または無効であるために、デバイスでのテンプレートのデプロイが部分的に、または完全に失敗することがあります。

編集および再試行の機能では、そうした不具合が発生したジョブについて、以前の入力を変更して再実行できるので便利です。

重要 CLIテンプレート、トラブルシューティングテンプレート、および複合テンプレートの場合、編集および再試行機能を使用して、失敗したジョブを再実行できます。

ジョブのステータスはジョブダッシュボードで確認できます。失敗した設定テンプレートジョブでは、[編集（Edit）]アイコン（  ）が有効になります。このアイコンをクリックすると[テンプレートのデプロイ - 編集および再試行（Template Deployment - Edit and Retry）] ウィンドウが開き、前に提供された入力を修正してデプロイを再試行することができます。

テンプレートのデプロイは、次のいずれかの理由で失敗することがあります。

1. 変数に提供された値が正しくないか、サポートされていない。
    1. **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。
    2. [ジョブ（Jobs）] ページで、失敗したデプロイのジョブを選択します。
    3. [編集（Edit）] アイコンをクリックします。[テンプレートのデプロイ - 編集および再試行（Template Deployment - Edit and Retry）] ウィンドウで、必要に応じて値を編集し、[OK] をクリックします。
2. 1 台以上のデバイスが到達不能か、クレデンシャルが正しくない。
    1. デバイスの到達可能性の問題を解決します。

2. **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。
3. [ジョブ（Jobs）] ページで、失敗したデプロイのジョブを選択します。
4. [ジョブ（Jobs）] ページで [実行（Run）] をクリックし、デプロイを再実行します。

3. 設定テンプレートのコマンドが正しくないか、無効である。

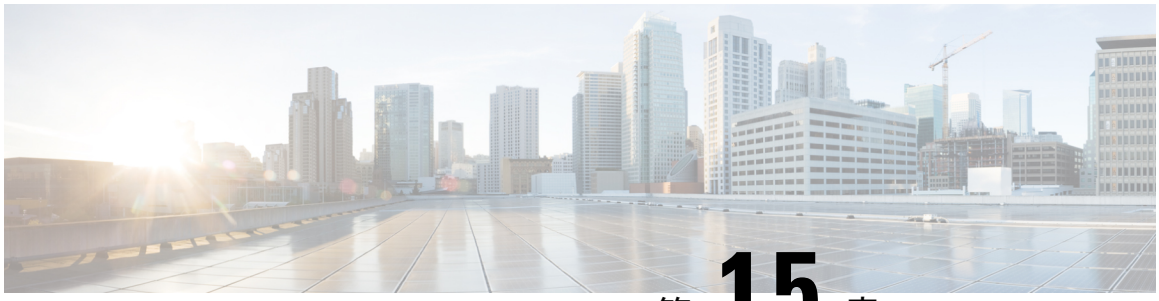
   この場合はテンプレートを修正する必要があります。この場合は、編集および再試行の機能を使用できません。

元のテンプレートを変更すると、失敗した設定テンプレートジョブの編集と再試行がブロックされます。変更したテンプレートについては、デプロイウィザードを使用してテンプレートをデプロイする必要があります。

（注）
- 設定グループ、および「ポート」タイプのテンプレートに対しては、編集および再試行の操作はサポートされません。
- Cisco EPN Manager 5.1 にアップグレードする場合は、この操作を行う前にブラウザのキャッシュをクリアする必要があります。

第 VI 部

回線の管理



第 15 章

回線/VC の検出およびプロビジョニングの概要

回線/VC のプロビジョニングの概要

Cisco EPN Manager は、キャリアイーサネット（CE）、オプティカル/DWDM、L3VPN、回線エミュレーション、セグメントルーティング、MPLS トラフィック エンジニアリングなどのさまざまな技術に対応した回線/VCのプロビジョニングをサポートしています。ほとんどの場合、回線は複数のデバイスにまたがっています。回線をプロビジョニングするには、複数のデバイス間で設定を変更する必要があります。Cisco EPN Manager には、回線に参加する複数のデバイス間で必要な設定変更を行えるプロビジョニング ウィザードが用意されています。

プロビジョニング ウィザードは、必要なすべての情報をステップ バイ ステップのアプローチで収集し、すべてのデバイスに必要な設定を生成します。ユーザーは、各デバイスについて生成された設定を確認し、サービス パラメータに変更を加えるか、設定をデバイスに展開するかを選択できます。

設定の変更は、「アトミック」トランザクションとして参加デバイスに展開されます。Cisco EPN Manager は、これらの操作をすべてまとめて実行するか、まったく実行しないかのどちらかのベストエフォートを試みます。「アトミック」トランザクションの概念を実装するため、Cisco EPN Manager は、プロビジョニング中の障害からの回復に役立つロールバック機能を備えています。

複数のデバイスを設定するときに、いずれかのデバイスで設定が失敗した場合、Cisco EPN Manager は、これまでにすべての参加デバイスで行われた設定変更をロールバックするためのベストエフォートを試みます。デバイスの設定状態は、プロビジョニング操作が試行される前と同じ状態に復元されます。

サポートされているキャリア イーサネット VC

キャリアイーサネット（CE）ネットワークでは、データは、さまざまなサービスタイプの属性と定義に従って、ポイントツーポイントおよびマルチポイントツーマルチポイントのイーサネット仮想コネクション（EVC）およびオペレータ仮想コネクション（OVC）にわたって転送されます。サービスタイプには、E-Line、E-LAN、E-Tree、E-Access、EVPN バーチャル プライベート ワイヤ サービス、およびマルチセグメント疑似回線サービスがあります。

EVC タイプにはそれぞれ、ポートベースのサービスと VLAN ベースのサービスがあります。これらは、UNI で使用されるサービス識別の方法によって区別されます。すべてを 1 つのバンドル UNI にまとめて使用する EVC（ポートベース）のことを「プライベート」と呼びます。一方、サービス多重化された UNI を使用する EVC（VLAN ベース）のことを「バーチャル プライベート」と呼びます。

E-Line、E-LAN、および E-Tree サービスでは、各 EVC は CE サービス フレームの形式で、UNI（ユーザー ネットワーク インターフェイス）から UNI にデータを運びます。この場合は UNI が、サービス プロバイダの責任とサブスクライバーの責任を分ける物理的な責任分界点になります。E-Access オペレータ仮想コネクション（OVC）では、ENNI（外部ネットワーク ネットワーク インターフェイス)におけるサービス プロバイダ間の相互接続が可能になります。この場合は ENNI が、相互接続している 2 つのサービス プロバイダの責任を分ける物理的な責任分界点になります。

各 EVC は豊富な属性セットを使用して設定できます。属性には、帯域幅プロファイル（認定情報レート - CIR、過剰情報レート - EIR、認定バースト サイズ - CBS、過剰バースト サイズ - EBS）、複数のサービス クラス、アプリケーション指向のパフォーマンス目的、トラフィック管理、転送ルールなどがあります。

Cisco EPN Manager は、次の EVC タイプの検出とプロビジョニングをサポートしています。それぞれについては以降のトピックで説明します。

- E-Line （607 ページ）：
  - MPLS（エッジへ）
  - シングルセグメントの擬似回線
  - イーサネット アクセス：ローカル、G.8032、ICCP-SM
- E-LAN （608 ページ）
  - MPLS（エッジへ）
  - シングルセグメントの擬似回線
  - 冗長擬似回線を備えた VPLS/H-VPLS

    - イーサネット アクセス：VPLS ベース
- E-Tree （609 ページ）：MPLS（エッジへ）
- E-Access （609 ページ）：MPLS（エッジへ）
- EVPN 仮想プライベート ワイヤ サービス（VPWS） （610 ページ）
- マルチセグメント疑似回線 （610 ページ）

マルチポイント EVC のコア テクノロジー

E-LAN または E-Tree EVC のコア テクノロジーは、VPLS（仮想プライベート LAN サービス）または H-VPLS（階層型 VPLS）のいずれかにできます。

- VPLS：MPLS ネットワーク経由でイーサネットベースのマルチポイント ツー マルチポイント通信を提供するレイヤ 2 VPN テクノロジー。VPLS では、疑似回線を介してサイトを接続することにより、地理的に分散したサイト間で、イーサネット ブロードキャスト ドメインを共有できます。ネットワークは、顧客の LAN セグメントを接続して単一のブリッジ型イーサネット LAN を作成することによって、LAN スイッチまたはブリッジをエミュレートします。
- H-VPLS：ネットワークを、MPLS コアを使用して相互接続される複数のエッジ ドメインに分割します。エッジ デバイスはローカル U-PE デバイスのみを認識するため、大きいルーティング テーブルのサポートは必要ありません。H-VPLS アーキテクチャでは、イーサネット マルチポイント、ポイントツーポイント レイヤ 2 VPN サービスだけでなく、レイヤ 3 VPN サービスへのイーサネット アクセスも可能にする柔軟なアーキテクチャ モデルを提供するため、サービス プロバイダは、単一の高速アーキテクチャに複数のサービスを提供できます。

E-TREE EVC では、H-VPLS は冗長性をサポートします。2 つのハブは、すべてのトラフィックが通過するコネクタとして機能します。プライマリ ハブに障害が発生すると、トラフィックはバックアップ ハブに切り替えられます。コア テクノロジーとしての H-VPLS では、E-Tree のルートとリーフ間に直接接続がありません。リーフ間通信を回避するために、H-VPLS はスプリット ホライズン機能とともに使用されます。

VPLS がコア テクノロジーとして使用される場合、冗長性はサポートされず、ルートとリーフ間に直接接続があります。ハブはルートに配置されます。これは、ルートがハブのロールを引き受けることを意味します。

E-Line

E-Line は、ポイントツーポイント EVC に基づいたイーサネット サービスを指します。2 種類の E-Line VC があります。

- 次の特性を持つイーサネット専用回線（EPL）
    - ポートベース

- 2 つの UNI 間でポイントツーポイント EVC を使用して、サービス フレーム、ヘッダー、およびほとんどのレイヤ2プロトコルが送信元と宛先の両方のUNIで同一になるように高度な透明性を提供します。
- すべてのCE-VLAN IDが1つのEVCにバンドルされている、すべて対1のバンドル。サービスの多重化はありません。

- 次の特性を持つイーサネット仮想専用回線（EVPL）
  - VLAN ベース
  - 2 つの UNI 間でポイントツーポイント EVC を使用しますが、EPL のように完全な透明性を提供しません。つまり、すべてのレイヤ2制御プロトコルがUNIで廃棄されます。
  - サービスの多重化が可能です。つまり、複数の EVC を UNI でサポートすることができます。

E-Line サービスの制限事項を次に示します。

- 昇格後の E-line サービス用 MEP グループの割り当ては、サービスの作成中に見られる状況と一致しない場合があります。
- E-line サービス用 MEP グループは、デバイス名の辞書順に基づいて割り当てられます。
- XConnect は、CFM に登録する前に 1 回起動する必要があります。これはデバイスの動作です。PW またはネイバーがすでに確立されている場合にのみ、DOWN サービスの CFM の詳細がビュー 360 に正しく表示されます。

E-LAN

E-LAN は、マルチポイントツーマルチポイント EVC に基づくイーサネット サービスを意味します。E-LAN VC には、次の 2 つのタイプがあります。

- イーサネット プライベート LAN（EP-LAN）、次のような特長がある
  - ポートベース
  - UNI でのオールツーワン バンドリング
  - 非常に透過的、CE-VLAN ID と PCP ビットの操作なし
  - EP-LAN マルチポートの透過性は EPL より複雑
- イーサネット仮想プライベート LAN（EVP-LAN）、次のような特長がある
  - VLAN ベース
  - サービスの多重化とバンドリングを許可

E-LAN サービスの制限事項を次に示します。

- XR デバイスの場合、プローブ名には一意のプローブ ID が含まれている必要があります（PM2_<probeid>_*）。
- 昇格中にサービス（ELAN/ETREE）に対して CFM が無効になっている場合でも、MEP グループを提供する必要があります。
- **localhost** と **hairpin** は、E-LAN ではサポートされていません。

E-Tree

E-Tree VC は多数の UNI を接続するルーテッド マルチポイント VC で、サイトにハブアンドスポーク マルチポイント接続を提供します。各 UNI は、ルートまたはリーフとして指定されています。ルート UNI は、すべてのリーフ UNI と通信できます。リーフ UNI は、ルート UNI とだけ通信でき、他のリーフ UNI とは通信できません。

E-Tree VC は、単一のサービス インスタンスを提供するために必要な UNI 間の分離を提供します。この場合、さまざまな顧客（それぞれリーフ UNI を持つ）が 1 つ以上の UNI を持つ JSP に接続します。複数のルート UNI があることは、ロード シェアリングと復元力のスキームにとって有用です。

E-Tree VC には 2 つのタイプがあります。

- イーサネット プライベート TREE（EP-TREE）：次の特性があります。
  - ルーテッド マルチポイント、ポートベース。
  - UNI での全対 1 バンドリング。
  - 複数の EPL を使用した一般的なハブ アンド スポーク構成よりも単純である。ハブの機能はルート UNI によって実行されます。
  - 主なレイヤ 2 制御プロトコルの CE-VLAN タグの保持とトンネリングを提供する。
  - CE-VLAN CoS 保持をサポートする。
- イーサネット仮想プライベート TREE（EVP-TREE）：次の特性があります。
  - ルーテッド マルチポイント、VLAN ベース。
  - ハブ サイトで多重化される複数の EVPL に対する代替手段を提供する。
  - サブスクライバの UNI の 1 つ以上が他のサービス（たとえば、EVPL または EVP-LAN）もサポートする場合に使用される。

E-Tree サービスの制限事項を次に示します。

- **localhost** と **hairpin** は、E-Tree ではサポートされていません。

E-Access

イーサネット アクセス サービスにより、サービス プロバイダは、いずれかのサイトがサービス プロバイダの独自のネットワークの外部にある場合に、2 つの顧客サイト間にオペレータ仮想接続（OVC）を構築できます。このような場合、サービス プロバイダは、フランチャイズ外 UNI に到達するためにローカル卸売アクセス プロバイダが提供する E-Access サービスを使

用します。サービス プロバイダが ENNI で E アクセス サービスに接続すると、トラフィックは、オペレータ仮想接続（OVC）を介して ENNI とフランチャイズ外 UNI との間で転送されます。

E-Access の定義には、外部インターフェイスに関連する属性（この場合 ENNI と UNI）と、これらの外部インターフェイスを関連付ける仮想イーサネット接続に関連する属性が含まれます。E-Access サービスでは、ポイントツーポイント OVC を使用して、ENNI での 1 つの OVC エンドポイントと、UNI での 1 つの OVC エンドポイントを関連付けます。

E-Access VC には 2 つのタイプがあります。

- アクセス EPL：次の特性があります。
  - プライベートまたはポートベース
  - UNI ごとに 1 つの OVC
  - すべての CE-VLAN ID が OVC にマッピングされる
- アクセス EVPL：次の特性があります。
  - VLAN ベース
  - UNI ごとに複数の OVC が可能
  - 複数の CE-VLAN ID（ただし、すべてではない）が 1 つの OVC にバンドルされる

EVPN 仮想プライベート ワイヤ サービス（VPWS）

EVPN-VPWS は、ポイントツーポイント サービス用の BGP コントロール プレーン ソリューションです。これにより、PE のペア間で EVPN インスタンスを確立するためのシグナリングおよびカプセル化技術が実装されます。EVPN-VPWS には、MAC ルックアップを使用せずに、あるネットワークから別のネットワークにトラフィックを転送する機能があります。VPWS 対応の EVPN により、ポイントツーポイント イーサネット サービスにおいてシングルセグメントおよびマルチセグメント PW をシグナリングする必要性がなくなります。EVPN-VPWS テクノロジーは、IP/MPLS コアで動作します。IP コアでは BGP がサポートされ、MPLS コアではエンドポイント間でのパケットのスイッチングがサポートされます。

マルチセグメント疑似回線

Cisco EPN Manager は、マルチセグメント疑似回線を使用するポイントツーポイント EPL および EVPL サービスの検出をサポートします。

マルチセグメント疑似回線ベースのサービス用のデバイスを設定するとき、Cisco EPN Manager は、設定の一部であるすべての疑似回線セグメントを 1 つのサービスとして検出します。

このサービス用のデバイスを設定すると、Cisco EPN Manager の回線 360 度ビューで [エンドポイント（Endpoint）] の下にマルチセグメント疑似回線のエッジエンドポイントを表示できます。Cisco EPN Manager の [オーバーレイ（Overlay）] タブと [マルチレイヤトレース（Multilayer Trace）] タブには、マルチセグメント疑似回線に参加しているすべての NE（ヘッド、ミッド、テールなど）が表示されます。また、これらのタブには、基盤となる SR ポリシーと、各疑似

回線セグメントによって設定および通過されるMPLSトンネルも表示されます。マルチセグメント疑似回線サービスを設定する前に、次のデバイス設定があることを確認してください。

- GI を有効にする

```
logging <Server_IP> vrf default severity info port default
logging hostnameprefix <Server_IP>
snmp-server host <Server_IP> traps vrf
snmp-server host <Server_IP> traps version 2c public
```

- GI を介してインターフェイスのアップ/ダウンをサポートする

```
snmp-server traps l2tun sessions
snmp-server traps l2tun tunnel-up
snmp-server traps l2tun tunnel-down
snmp-server traps l2tun pseudowire status
```

（注）
- マルチセグメント疑似回線は、すべての IOS XR デバイスで EVPL および EPL サービスの検出をサポートします。プロビジョニングはサポートされません。
- これはサービス検出専用であるため、マルチセグメント疑似回線設定を使用したサービスのプロモーションは無効になっています。

EVPN ELAN の可視化

EPNM は、XE プラットフォームと XR プラットフォームで構成される EVPN ELAN シングルホーミング（RFC 7432 から）ネットワーク管理をサポートします。EVPN ELAN の可視化は検出のみでサポートされており、プロビジョニングや昇格ではサポートされていません。

EVC のプロビジョニングでサポートされるネットワーク構造

Cisco EPN Manager EVC と OVC はアクセス ネットワークの組み合わせを通じてプロビジョニングできます。エンドポイントは、MPLS ルータ、イーサネット アクセス スイッチ、または Cisco ASR 9000 ルータに接続された nV サテライトで直接設定できます。EVC は、異なるイーサネット アクセス ネットワーク、同じネットワーク、または同じデバイス上に、エンドポイントを設定することができます。Cisco EPN Manager は、接続の作成に必要なだけの設定を行います。

EVC は次のネットワークを介してプロビジョニングできます。

- MPLS ドメイン：Cisco EPN Manager は、管理対象ネットワークに単一の MPLS ドメインが含まれていると仮定します。どのルータも、ターゲットの LDP セッションを介して他のルータと通信できます。または、MPLS トラフィック エンジニアリングまたはセグメント ルーティングを使用して MPLS エンドツーエンド接続を実現することもできます。

- イーサネット アクセス ネットワーク：Cisco EPN Manager は、中央の MPLS ドメインに接続されたイーサネット アクセス ネットワークを介して EVC をプロビジョニングできます。ネットワークはシステムによって検出されます。G.8032 アクセス リングまたは ICCP-SM リンクを介して EVC をプロビジョニングできます。次のものがアクセス ネットワークの候補になります。
  - G.8032 リング。これには、MPLS ドメインを横断する EvC の作成を可能にするルータが含まれている必要があります。
  - G.8032 オープン リング。これはリンクのシーケンスを意味します。
- Cisco ASR 9000 nV サテライト トポロジ：Cisco EPN Manager は、Cisco ASR 9000 ホストに接続されたシングルホーム nV サテライト デバイスで EVC を設定できます。

サービスの検出とプロビジョニングをサポートする場合、Cisco EPN Manager はアクセス ネットワークでトポロジを検出する必要があります。正常に検出するためには、次の前提条件を満たしている必要があります。

- ICCP-SM の場合、LACP を使用して LAG を設定する必要があります。
- G.8032 の場合、CDP または LLDP をリング ポートで設定する必要があります。

サポートされる光回線

ここでの回線とは、2 つ以上の接続終端ポイント（CTP）間のエンドツーエンド接続を表します。回線は、交互に出現する一連のクロス接続とリンク接続で構成されます。最も単純な形式では、回線は単一のクロス接続で構成されます（回線が同じ NE 上の 2 つの CTP 間で定義されている場合）。回線は、双方向または単方向にでき、ポイントツーポイントまたはポイントツーマルチポイントにでき、保護付きまたは保護なしにできます。

Cisco EPN Manager は、高密度波長分割多重（DWDM）光チャネル（OCH）回線タイプのプロビジョニングと、光転送ネットワーク（OTN）回線タイプのプロビジョニングをサポートします。DWDM の光技術は、既存の光ファイバ バックボーン上の帯域幅を広げるために使用されます。これは同じ光ファイバ上で異なる波長の複数の信号を同時に結合して送信します。実際には、1 つの光ファイバが複数の仮想光ファイバに変換されます。

Cisco EPN Manager は、次の光回線タイプをサポートします。

- 高密度波長分割多重（DWDM）回線 （613 ページ）
  - Optical Channel Network Connection（OCHNC）WSON （613 ページ）
  - 光チャネル クライアント接続（OCHCC）WSON （613 ページ）
  - 光チャネル（OCH）トレイル WSON （614 ページ）
  - IOS-XR プラットフォームベースのデバイスを直接接続する光チャネル（OCH）トレール （614 ページ）
  - NCS 2000 デバイス経由で IOS-XR プラットフォームベースのデバイスを接続する光チャネル（OCH）トレール （615 ページ）
  - NCS 1002、NCS 55xx、および ASR 9K デバイスを接続する光チャネル（OCH）トレール （615 ページ）

高密度波長分割多重（DWDM）回線

以降のトピックでは、さまざまな光チャネル（OCH）およびメディア チャネル（MCH）回線タイプについて説明します。

Optical Channel Network Connection（OCHNC）WSON

OCHNC WSON 回線は、指定された C バンド波長で 2 つの光ノード間の接続を確立します。この接続は、波長選択スイッチ、マルチプレクサ、デマルチプレクサ、および挿入/分岐カード上に存在するポートを介して行われます。OCHNC WSON 回線では、波長が送信元 OCH ポートから DWDM システムに入り、DWDM システムから送信先 OCH ポートに出ます。

光チャネル クライアント接続（OCHCC）WSON

OCHCC WSON 回線は、OCHNC WSON を拡張して、TXP/MXP カードの送信元クライアント ポートから宛先クライアント ポートへの光接続を作成します。OCHCC WSON 回線は、DWDM システムを通過する実際のエンドツーエンド クライアント サービスを表します。各 OCHCC WSON 回線は、トランスポンダ（TXP）、マックスポンダ（MXP）、GE_XP（レイヤ 1 DWDM モード）、10GE_XP（レイヤ 1 DWDM モード）、または ITU-T ライン カード上のクライアントまたはトランク ポートのペアに関連付けられています。OCHCC WSON 回線は、スプリッタ保護を単一の保護回線として管理できます。ただし、Y 字型ケーブル保護の場合は、2 つの OCHCC WSON 回線と 2 つの保護グループが必要です。

（注） Cisco EPN Manager は、OCHCC WSON 回線により接続されている Cisco NCS 2000 シリーズ デバイスと Cisco IOS-XR デバイスとの間の LMP リンクを検出できます。

光チャネル（OCH）トレイル WSON

OCH トレイル WSON 回線は、OCHCC WSON 回線を転送します。OCH トレイル WSON 回線は、トランスポンダ（TXP）、マックスポンダ（MXP）、GE_XP、10GE_XP、または ITU-T ライン カードの送信元トランク ポートから宛先トランク ポートへの光接続を作成します。OCH トレイル WSON は、2 つのカード間の共通接続を表し、その上にクライアント OCHCC WSON 回線、SVLAN 回線、または STS 回線がすべて搭載されています。OCHCC WSON が作成されると、対応する OCH トレイルが自動的に作成されます。2 つの TXP、MXP、GE_XP、または 10GE_XP カード間に OCHCC WSON が作成されると、CTC 内に 2 つの回線が作成されます。次のものがあります。

- 1 つの OCHCC WSON（クライアント ポート エンドポイント側）
- 1 つの OCH トレイル WSON（トランク ポート エンドポイント側）

2 つの TXPP カード間または 2 つの MXPP カード間に OCHCC WSON が作成されると、CTC 内に 3 つの回線が作成されます。次のものがあります。

- 1 つの OCHCC WSON（クライアント ポート エンドポイント側）
- 2 つの OCH トレイル WSON（トランク ポート エンドポイント側）。1 つは作業用、もう 1 つは保護トランク用です。

IOS-XR プラットフォームベースのデバイスを直接接続する光チャネル（OCH）トレール

Cisco EPN Manager は、直接接続された IOS-XR プラットフォームベースのデバイスのトランクポート間の OCH トレール回線を検出してプロビジョニングできます。

これらの回線には固定ルートがあり、サポートされているオプションの数は限られています。詳細については、IOS-XR プラットフォームベースのデバイスを直接接続する OCH トレール回線の作成とプロビジョニング （679 ページ）を参照してください。

回線のプロビジョニングを有効にするには、デバイスのトランクポート間でマネージドリンクを作成する必要があります。

OCH トレール ハイブリッド回線は、Cisco IOS-XR デバイスと Cisco NCS 2000 シリーズ デバイスを接続します。Cisco EPN Manager でこうした回線を検出できるようにするには、回線のトランク ポートを、手動リンクを介して接続するか、または Cisco NCS 2000 シリーズ デバイスのパッシブ ユニットへの LMP リンクを介して接続する必要があります。

（注） このタイプの光回線では、プロビジョニングはサポートされません。

OCH-Trail ハイブリッド回線は、Cisco SVO ネットワークを介して Cisco IOS-XR デバイスを別の Cisco IOS-XR デバイスに接続します。Cisco EPN Manager は、Cisco SVO デバイスのパッシブユニットへのいずれかの手動リンクを介して、トランクポートを接続する必要がある回線をプロビジョニングできます。EPNM でのこのような回線の検出はサポートされていません。

NCS 2000 デバイス経由で IOS-XR プラットフォームベースのデバイスを接続する光チャネル（OCH）トレール

Cisco EPN Manager は、NCS 2000 DWDM ネットワーク経由で接続された IOS-XR プラットフォームベースのデバイスのトランクポート間の OCH トレイル回線を検出できます。

これらの OCH トレイル回線は読み取り専用であり、関連するメディアチャネル NC 回線が NCS 2000 デバイスで作成または削除されると、自動的に作成および削除されます。

この回線には次の前提条件があります。

- 各 NCS 1004 のトランクポートと NCS 2000 のパッシブポートとの間に LMP リンクを作成する必要があります。詳細については、GMPLS および WSON のプロパティの構成 （493 ページ）を参照してください。

  LMP の終端のタイプは「NCS 1004 シグナリング」である必要があります。

- NCS 1004 のクライアントポートとトランクポートをアクティブにする必要があります。詳細については、光インターフェイスのプロビジョニング （457 ページ）を参照してください。

- メディアチャネル NC は、NCS 2000 デバイスのパッシブポート間を、 EPNM を使って、プロビジョニングする必要があります。この回線をプロビジョニングすると、NCS 1004 の関連するトランクポートも表示されます。中間の NCS 1004 デバイスは、この回線の再生器として使用できます。

NCS 4000 デバイスが OTU4 ペイロードを使用して NCS 1000 のクライアントポートに接続されている場合は、TE リンクが検出され、ODU トンネル回線ルーティングに使用できます。

NCS 1002、NCS 55xx、および ASR 9K デバイスを接続する光チャネル（OCH）トレール

Cisco EPN Manager 次のデバイスから OCH トレール回線を検出できます。

- NCS 1002 デバイスの送信元トランク ポートから別の NCS 1002 デバイスの宛先トランク ポートへ。
- NCS 55xx デバイスの送信元トランク ポート（NCS55-6X200-DWDM-S カード上のトランク ポート）から別の NCS 55xx デバイスの宛先トランク ポートへ。
- ASR 9K デバイスの送信元トランク ポート（ASR9K-400G-DWDM-TR 上のトランク ポート）から別の ASR 9K デバイスの宛先トランク ポートへ。

これらの各デバイスのトランク ポートは、NCS 2K デバイスのパッシブ ユニットへの手動リンクによって接続する必要があります。手動リンクが終端される場合、NCS 2K ネットワークのパッシブ ユニットのポート間の前提条件として、OCH-NC 回線が作成される必要があります。

（注） このタイプの光回線では、プロビジョニングはサポートされません。

光チャネル（OCH）トレールのユーザー/ネットワーク間インターフェイス（UNI）

OCH トレール UNI 回線は、次のデバイス間の接続を確立します。

- Cisco NCS 2000 シリーズ デバイスと Cisco NCS 4000 シリーズ デバイス。Cisco NCS 2000 シリーズのデバイスで構成され、Cisco NCS 4000 シリーズのデバイスで終端する DWDM ネットワークのエンドツーエンドの構成を提供します。OCH トレールの UNI 回線が Cisco NCS 4016 ネットワーク要素で作成されると、対応する OCHNC 回線が Cisco NCS 2006 ネットワーク要素で作成されます。

（注） OCHNC 回線を変更または削除することはできません。

- UNI-C および Cisco NCS 2000 シリーズ デバイスとして機能する Cisco NCS 1000 シリーズ デバイスは、UNI-N として機能します。OCH トレール UNI 回線は、ソース NCS 1002 ノードの NCS 1002 トランク インターフェイス（UNI-C）を起点とし、宛先 NCS 2000 シリーズ ノードの NCS 2000 シリーズ インターフェイス（UNI-N）を終端として、光接続を作成します。OCH トレール UNI 回線の前提条件として、NCS 2000 シリーズ ノードの光チャネル アド/ドロップ NCS 2000 シリーズ インターフェイスと、NCS 1002 ノードの NCS 1002 インターフェイスとの間に、リンク管理プロトコル（LMP）リンクを作成する必要があります。GMPLS および WSON のプロパティの構成 （493 ページ）を参照してください。

（注） Cisco EPN Manager は、ソフトウェア バージョン 6.3.2 で実行されている NCS 1002 デバイスを起点とする OCH トレール UNI 回線を検出します。

LMP リンクは、番号付きリンクまたは番号なしリンクのいずれかです。番号なしリンクには IP アドレスがありません。

- 番号なしリンクの場合、Cisco EPN Manager によって、必要な明示的パス オブジェクトが、ソース デバイスである NCS 1000 シリーズ デバイスに作成されます。このデバイスには 2 つの制約が含まれます。1 つはソースのピア NCS 2000 シリーズ デバイスに対するもので、もう 1 つは宛先デバイスに対するものです。必要に応じて、さらに制約を追加できます。

- 番号付きリンクの場合、デフォルトの明示的パス オブジェクトは必要ありません。制約を追加する場合は、最初に明示的パス内でソースの NCS 2000 シリーズ ノードを指定する必要があります。これはノードが OCH トレール UNI 回線のソース エンドポイントとして選択されている場合でも同様です。ソースの NCS 2000 シリーズ ノードを最初の制約として追加しないと、NCS 2000 シリーズ ノード上に対応する OCHNC 回線が作成されません。

（注） 同じ OCH トレール UNI 回線で番号付きリンクと番号なしリンクの両方を使用することはできません。

Spectrum Switched Optical Network（SSON）回線

SSON 回線を使用すると、スパン内で 96 を超えるチャネルを提供できます。SSON 機能を使用すると、回線をメディア チャネル グループ内に作成した場合に、回線が互いに近くに配置されます。回線間の最小間隔は 50 GHz です。

SSON 回線を作成できるのは、ソース ノードと宛先ノードに SSON パッケージがインストールされている場合のみです。

（注） 既存の OCHNC、OCHCC、および OCH トレール回線は SSON 回線にアップグレードできません。

Cisco EPN Manager は、次の SSON 回線をサポートしています。

- メディア チャネル回線：メディア チャネル（MCH）は、使用可能な任意の周波数（フレキシブル周波数）で動作し、2 つの光ノード間の接続を確立します。スペクトルの連続するセクションがソース ノードと宛先ノードの間に割り当てられます。MCH には、割り当てられた光帯域幅に関する情報が含まれています。メディア チャネルには次の 3 つのモードがあります。
  - メディア チャネル トレール：MCH トレール SSON 回線は、MCHCC SSON 回線を転送します。これらの回線は、（キャリア トレールに基づいて）同じ場所にある TXP のトランク ポート間に光接続を作成します。
  - メディア チャネル ネットワーク接続（MCHNC）：MCHNC SSON 回線は、（キャリアに基づいて）フィルタ ポート間に光接続を作成します。
  - メディア チャネル クライアント接続（MCHCC）：MCHCC 回線は、同じ場所にある TXP のクライアント ポート間に光接続を作成します。
- メディア チャネル グループ（MCHG）：MCHG は、1 つ以上のメディア チャネルを含めることができるコンテナです。メディア チャネルをまとめてグループ化するとスペクトル効率が高まります。OCH 回線と比べて、より近い間隔で回線を作成できます。MCHG が C バンド全体をカバーしている場合は、メディア チャネルの最大数を単一のファイバで達成できます。

管理対象プレーン回線

SVO デバイスでは、Cisco EPNM は管理対象プレーンのプロビジョニングをサポートします。SVO デバイスについては、SVO デバイスの追加 （61 ページ） を参照してください。SVO デバイスで OCH-Trail と OCH-CC をプロビジョニングできます。OCHCC および OCH-Trail 回線

を作成してプロビジョニングするには、OCH回線の作成とプロビジョング （668ページ）を参照してください。

光トランスポート ネットワーク（OTN）回線

OTN は、ネイティブ プロトコルに関係なく、データの既存のフレームをカプセル化する方法であるデジタルラッパーを指定し、SDH/SONET で使用されるものと同様の光データ ユニット（ODU）を作成します。OTN は、SDH/SONET のネットワーク管理機能を波長ベースで提供します。ただし、デジタル ラッパーは、フレーム サイズの面で柔軟性があり、データの複数の既存のフレームを、多波長システムのオーバーヘッドを低く抑えて効率的に管理できる単一のエンティティにラッピングできます。

OTN の指定には、フレーミング規則、非侵入パフォーマンス モニターリング、エラー訂正（FEC）、レート適応、多重化メカニズム、リング保護、および波長ベースで動作するネットワーク復元メカニズムが含まれます。

デジタルラッパーのキー要素は、マージンの改善と光リーチの拡張のためにパフォーマンスを向上させる前方誤り訂正（FEC）メカニズムです。

OTN アーキテクチャは、ITU-T G.872 に準拠しています。OTN 回線は、Resource Reservation Protocol（RSVP）シグナリングを使用して、イングレスとイーグレスのノード間に静的または動的に確立できます。OTN 回線は、トランジット LSR を介してスイッチされるイングレスとイーグレスのラベル スイッチ ルータ（LSR）間のラベル スイッチド パス（LSP）として確立および保守されます。リクエストがユーザー インターフェイスから送られて来た場合、LSP はソフト常時接続（SPC）として確立される場合があります。

以下に OTN 回線のタイプを示します。

- 光チャネル データ ユニットのユーザー/ネットワーク間インターフェイス（ODU UNI）（618 ページ）
- 光チャネル データ ユニット（ODU）トンネル （619 ページ）
- Optical Channel Payload Unit（OPU）Over Optical Channel Data Unit（ODU） （619 ページ）
- 光チャネル データ ユニットのユーザー/ネットワーク間インターフェイス（ODU UNI）ヘアピン （620 ページ）
- 光チャネル データ ユニット（ODU） （620 ページ）

光チャネル データ ユニットのユーザー/ネットワーク間インターフェイス（ODU UNI）

ODU は、ネットワーク入力から出力にクライアント信号を伝送するために定義されたトランスポート コンテナです。ODU は、クライアント データのペイロード エリア、およびパフォーマンスのモニターリングと障害管理を提供します。ODU のペイロード エリアには、クライアントとして単一の非 OTN 信号または複数の低速 ODU を含めることができます。ODU UNI 回線は、OTN アーキテクチャを通過する実際のエンドツーエンドのクライアント サービスを表します。

オープン エンドの ODU UNI

オープンエンドの ODU UNI 回線では、一方または両方のエンドポイントを、クライアント ペイロード コントローラではなく ODU サブコントローラに接続することができます。

Cisco EPN Manager は次の 3 種類のオープンエンド ODU UNI をサポートしています。

- 送信元インターフェイスのみが ODU サブコントローラである
- 宛先インターフェイスのみが ODU サブコントローラである
- 送信元インターフェイスと宛先インターフェイスの両方が ODU サブコントローラである

オープンエンドの ODU UNI 回線を作成するには、デバイスを Cisco EPN Manager に追加する前に、デバイスに ODU サブコントローラを設定する必要があります。デバイス上の ODU サブコントローラを設定するには、**controller oduk** コマンドを使用します。

例：Cisco NCS 4000 デバイスで ODU サブコントローラを設定する

この例では、2 つの ODU0 サブコントローラが ODU1 コントローラに設定されています。

```
RP/0/RP0:router#conf
RP/0/RP0:router(config)# controller ODU10/1/0/1
RP/0/RP0:router(config-odu1)# tsg 1.25G
RP/0/RP0:router(config-odu1)# ODU0 tpn 1 ts 1
RP/0/RP0:router(config-odu1)#  ODU0 tpn 2 ts 2
RP/0/RP0:router(config-odu1)#commit
```

ODU サブコントローラがデバイス上で正しく設定されていることを確認するには、次のようにします。

```
RP/0/RP0:router#sh controllers ODU0 ?
  0/1/0/0     ODU0 Interface Instance
  0/1/0/1/10  ODU0 Interface Instance
  0/1/0/1/20  ODU0 Interface Instance
  R/S/I/P     Forward interface in Rack/Slot/Instance/Port format
```

デバイス上で ODU サブコントローラを設定したら、デバイスを Cisco EPN Manager に追加する必要があります。これで、ODU0 0/1/0/1/10 および ODU0 0/1/0/1/20 サブコントローラがインベントリで使用可能であることを確認できます。

光チャネル データ ユニット（ODU）トンネル

ODU トンネル回線は、ODU UNI を転送します。ODU トンネルは、トラフィック エンジニアリング（TE）リンクに接続されている 2 台の Cisco NCS 4000 シリーズ デバイス間の共通接続を表します。ODU UNI 回線が作成されると、対応する ODU トンネルが自動的に作成されます。

Optical Channel Payload Unit（OPU）Over Optical Channel Data Unit（ODU）

OPU over ODU 回線は、2 つの顧客指定施設間の高帯域幅ポイントツーポイント接続を提供します。クライアント信号は、GCC0 経由のインバンド管理を使用して OTN フレーミング構造にマップされます。このような回線では、ODU UNI 回線を使用して、クライアント信号がネットワーク経由で伝送されます。OPU over ODU 回線を作成してプロビジョニングするには、次のタスクを実行する必要があります。

- Cisco EPN Manager を使用して、ODU UNI 回線を作成します。ODU UNI 回線の作成方法については、OTN 回線の作成とプロビジョング （689 ページ）を参照してください。
- Cisco Transport Controller（CTC）を使用して、LMP リンクを作成し、OPU over ODU 回線で使用するデバイス上のリンクを有効にします。LMP の作成方法については、『OTN and DWDM Configuration Guide for Cisco NCS 4000 Series』の「DLP-K27 Create an LMP Using CTC」の項を参照してください。
- Cisco EPN Manager を使用して、LMP リンク対応デバイスとの OPU over ODU 回線を作成します。OPU over ODU 回線の作成方法については、OTN 回線の作成とプロビジョング（689 ページ）を参照してください。

光チャネルデータユニットのユーザー/ネットワーク間インターフェイス（ODUUNI）ヘアピン

ODU UNI ヘアピン回線は ODU UNI 回線に似ていますが、管理プレーンで作成され、ソースと宛先は同じデバイスですが、インターフェイスが異なるイントラ ノード回線です。このタイプの回線では、2 台のクライアントまたは 2 台の ODU サブコントローラ間で接続が確立されます。

Cisco EPN Manager は、次のタイプの ODU UNI ヘアピン回線をサポートしています。

- オープンエンドのクロス接続のない回線：このタイプの回線では、送信元と宛先の両方のインターフェイスが OTU インターフェイスではありません。
- 片側にオープンエンドのクロス接続を持つ回線：このタイプの回線では、送信元または宛先のいずれかのインターフェイスが OTU インターフェイスになります。
- 両側にオープンエンドのクロス接続を持つ回線：このタイプの回線では、送信元または宛先の両方のインターフェイスが OTU インターフェイスになります。

光チャネル データ ユニット（ODU）

光チャネルデータユニット（ODU）回線は、トラフィックエンジニアリング（TE）リンクに接続されている 2 台の Cisco NCS 2000 シリーズ デバイス間の共通接続を表します。ODU は OTU コントローラのサブコントローラとして作成されます。ODU には、光チャネルをサポートするメンテナンス機能と操作機能の情報が含まれています。ODU のオーバーヘッド（OH）情報が ODU ペイロードに追加され、完全な ODUk が作成されます。ODUk の OH は、エンドツーエンドの ODUk パスと 6 つのレベルのタンデム接続モニターリング専用の部分で構成されます。ODUk パスの OH は、ODUk が組み立ておよび分解される場所で終了します。TCM の OH が追加され、送信元で終端されて、対応するタンデム接続にシンクします。

ODU クロス接続は、OTN ネットワーク内の 2 つの OTN ポートまたはクライアント ポート間のエンド ツー エンド チャネルです。Cisco EPN Manager は双方向 SNC-N 保護を使用した ODU のクロス接続をサポートしています。

サポートされる回線エミュレーション サービス

回線エミュレーション（CEM）は、IP ネットワークを介したプロトコルを選ばない伝送を提供します。これにより、独自のアプリケーションまたはレガシーアプリケーションは、専用回線のように接続先に透過的に伝送できます。従来の TDM ネットワークでは、地理的に分散した場所間で多数の物理回線を保持して、TDM トランスポートを提供します。CEM を使用すると、TDM エンドポイントを IP/MPLS コア上で接続できます。CEM では、エンドポイントは TDM 回線に接続されますが、回線は使用可能な IP/MPLS 接続がある各ローカル ルータで終端します。ルータは、IP/MPLS コア上の TDM フレームを回線エミュレーション（CEM）の疑似回線（PW）経由で使用可能な IP/MPLS 接続があるリモート エンドポイントに転送します。したがって、TDM エンドポイントは物理回線で直接接続されているかのように通信できます。Cisco EPN Manager では、次の CEM モードがサポートされています。

- Structure-Agnostic time-division multiplexing（TDM）over Packet（SAToP）：これは、着信 TDM データが任意のビット ストリームと見なされる非構造化モードです。ビット ストリームに適用される可能性がある構造は無視されます。SAToP では、TDM ビット ストリームが PSN 経由の疑似回線（PW）としてカプセル化されます。
- Circuit Emulation over Packet（CEP）：このモードは、MPLS プロバイダを介して同期光ネットワーク/同期デジタル階層（SONET/SDH）回線とサービスをエミュレートするために使用されます。パケット指向ネットワークで SONET/SDH 回線を伝送するために、同期ペイロード エンベロープ（SPE）またはバーチャル トリビュタリ（VT）はフラグメントに分割されます。CEP ヘッダーと必要に応じて RTP ヘッダーが各フラグメントの前に付加されます。
- Circuit Emulation Service over Packet Switched Network（CESoPSN）：これは、構造化された TDM 信号が PW としてカプセル化され、PSN 上で送信される構造化モードです。有効なタイムスロットのみを選択し、伝送のアイドル タイムスロットを無視します。したがって、CESoPSN は、利用された帯域幅を保存できます。

Cisco EPN Manager は、回線がデータを送信できるレートに応じて次の CEM サービス タイプをサポートします。

- DS0：最大 64 Kbps の伝送データ レートの基本的なデジタル信号。
- T1 および E1：デジタル信号（DS）は、北米、韓国、および日本では T キャリア、その他の国では E キャリアと呼ばれます。T1 回線の最大伝送データ レートは 1.544 Mbps です。E1 回線の最大伝送データ レートは、フレーム化モードでは 1.984 Mbps、非フレーム化モードでは 2.048 Mbps です。
- T3 および E3：T3 回線の最大伝送データ レートは 44.736 Mbps です。E3 回線の最大伝送データ レートは 34.368 Mbps です。T3 または E3 回線は、ペイロードで 672 の DS0 レベル チャネルと 28 の DS1 レベル チャネルを伝送できます。
- VT 1.5：最大 1.728 Mbps の伝送データ レートのバーチャル トリビュタリ ネットワーク回線。
- STS-1：最大 51.84 Mbps の伝送データ レートの同期転送信号。

- STS-3c：最大 155.52 Mbps の伝送データレートの同期転送信号。
- STS-12c：最大 622.08 Mbps の伝送データレートの同期転送信号。
- STS-48c：最大 2488.32 Mbps の伝送データレートの同期転送信号。
- VC4：最大 155.52 Mbps の伝送データレートを持つ同期転送モジュール
- VC4-4c：最大 622.08 Mbps の伝送データレートを持つ同期転送モジュール
- VC4-16c：最大 2488.32 Mbps の伝送データレートを持つ同期転送モジュール。
- VC11：最大 1.7 Mbps の伝送データ レートを持つ仮想コンテナ回線。
- VC12：最大 2.2 Mbps の伝送データ レートを持つ仮想コンテナ回線。

（注） IOS-XE デバイスでは、ポイントツーポイント サービスで **l2vpn xconnect** コマンドを使用します。

サポートされている L3VPN サービス

MPLS レイヤ 3 VPN はプライベート IP ネットワークを形成します。顧客はプロバイダ エッジ（PE）ルータの IP ピアとして機能するカスタマーエッジ（CE）ルータを介してネットワークに接続します。

仮想ルーティングおよび転送（VRF）

PE では、仮想ルーティングおよび転送（VRF）インスタンスが L3VPN サービスのトラフィック転送専用の仮想 IP ルータとして機能します。VRF は、マルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）を介して相互にルートを学習し、MPLS を使用してトラフィックを転送します。

VPN は少なくとも 1 つ、通常は複数の VRF で構成されます。Cisco EPN Manager は VPN ID を使用して、単一の VPN を一緒に形成する VRF を検出します。VPN ID がプロビジョニングされていない既存のネットワークを Cisco EPN Manager が検出すると、同じ名前のすべての VRF を取得し、それらを 1 つの VPN に関連付けます。バージョン番号プレフィックスと異なるサフィックスによる命名規則を使用する Cisco PRIME プロビジョニングを使用して作成された VPN の場合、Cisco EPN Manager は異なる VRF を 1 つの VPN に属しているものとして認識します。

一般に、さまざまな命名規則を受け入れるように設定できる正規表現があります。

ルート ターゲット（RT）

VRF 間の接続は VRF によってインポートおよびエクスポートされるルートターゲット（RT）を使用して定義されます。Cisco EPN Manager は、フルメッシュ接続のセットアップを容易にし、使用するルートターゲットを自動的に割り当てます。ルート ターゲットは、AS 番号または IPv4 アドレスのいずれかのプレフィックス（フル メッシュ プレフィックス、100 [681682]

など）で構成されます。プレフィックスは、ネットワーク内の既存のBGP自律システム（AS）番号から選択することも、手動で入力することもできます。プレフィックスに続く2番目の番号はCisco EPN Managerによって自動的に割り当てられます。

あるいは、ルート ターゲットを手動で選択することもでき、また、フル メッシュに加えてこれを行うこともできます。VPNの作成時にVPN内で使用するルート ターゲットを入力する初期画面が表示され、VRF ごとにインポートおよびエクスポートするルート ターゲットを選択できます。また、ルート ターゲットを使用するアドレス ファミリ（IPv4またはIPv6）も指定します。これは、他のVPNで使用されるルート ターゲットをインポートすることによって、エクストラネットを設定する場合などに使用できます。

ルートの再配布

PEとCEの間で交換されるルートは、リモート エンドポイントが各VRFで到達できるプレフィックスがわかるようにMP-BGPルーティング プロトコルに再配布する必要があります。ルートの再配布を制御するため、Cisco EPN Managerでは必要なプロトコル（OSPF、静的、接続済み、またはRIP）、プロトコルのメトリック値、および必要に応じて適用可能なルートポリシーを定義できます。

エンドポイント

Cisco EPN Managerは、イーサネット サブインターフェイス上のIPエンドポイントの作成をサポートします。タグなしカプセル化の選択、あるいは802.1qまたは802.1adのカプセル化を使用した、外部VLANと、必要に応じて内部VLANの指定をサポートします。エンドポイント上のIPv4アドレスとIPv6アドレスの両方を指定できます。また、BGPおよびOSPFネイバーの詳細を指定して、CEとPEの間でBGPおよびOSPFネイバーをプロビジョニングすることもできます。

Cisco EPN Managerを使用してL3VPNサービスをプロビジョニングする方法については、L3VPN サービスのプロビジョニング （700 ページ）を参照してください。

サポートされているセグメント ルーティング サービス

Cisco EPN Manageは、セグメント ルーティング トラフィック エンジニアリング（SR-TE）ポリシーを使用して、EPLのプロビジョニング、EVPL、アクセスEPL、アクセスEVPLキャリアイーサネットのポイントツーポイント サービスをサポートしています。CEサービスの変更時にSR-TEポリシーを変更できます。回線/VC 360*の[関連回線/VC（Related Circuits/VC）]タブを使用して、このサービスに関連付けられたSRポリシーを表示できます。

サポートされている MPLS トラフィック エンジニアリング サービス

従来のIPネットワークでは、パケットはホップ単位で転送され、送信元から宛先までの各ルータでルートルックアップが実行されます。宛先ベースの転送メカニズムでは、ネットワーク内のルータのペア間で使用可能な帯域幅は最適に使用されません。ほとんどの場合、最適でない

パスの IP ネットワークでの利用率は低くなります。使用可能な帯域幅の非効率的な使用によるパケット ドロップを回避し、より優れたパフォーマンスを得るために、トラフィック エンジニアリング（TE）が実装されています。TE は最適なトラフィックに従うように定義されたトラフィックを次善のパスに送信するため、ルータのペア間での帯域幅の使用率が向上します。

マルチプロトコル ラベル スイッチング（MPLS）には、レイヤ 2 テクノロジーとレイヤ 3 テクノロジーが統合されています。MPLS ドメインでは、一意のラベルがデータ パケットに割り当てられ、パケットはこれらのラベルに基づいて転送されます。これにより、ルーティング テーブルの複雑なルックアップが回避されます。MPLS は VC スイッチング機能を作成し、フレーム リレーや非同期転送モード（ATM）などの従来のネットワークを介して提供される場合と比べても IP ベースのネットワーク サービスで同様のパフォーマンスを実現します。

従来のレイヤ 2 機能をレイヤ 3 で使用可能にすることで、MPLS はトラフィック エンジニアリングを可能にしています。MPLS TE を使用すると、MPLS バックボーンはレイヤ 2 の TE 機能をレイヤ 3 上に復元し、拡張できます。

MPLS TE は、バックボーン全体でラベルスイッチド パス（LSP）を確立および維持するために、Resource Reservation Protocol（RSVP）を使用します。LSP で使用されるパスは、LSP リソース要件と、帯域幅や属性などのネットワーク リソースに基づいています。使用可能なリソースは、リンク状態ベースの内部ゲートウェイ プロトコル（IGP）への拡張機能によってフラッディングされます。Cisco EPN Manager は、使用可能な帯域幅をフラッディングし、ネットワーク全体にステータス情報をリンクする IGP として OSPF をサポートします。この情報に基づいて、入力（ヘッドエンド）ルータは、ネットワーク内の使用可能なすべてのリソースに関する情報をトポロジとともに収集し、一連の MPLS 対応ルータ間のネットワークを通じてトンネルを定義します。これは、制約ベースのルーティングと呼ばれています。最も短いパスが過度に利用されると、IGP はトラフィックをこれらの LSP に自動的にルーティングします。また、MPLS TE トンネルの明示的パスを作成およびプロビジョニングすることもできます。

Cisco EPN Manager は、パス、リンク、およびノードの障害に対する MPLS TE トンネルの完全なパス保護メカニズムを提供します。セカンダリ LSP を確立することで、トンネルの TE トラフィックを伝送する保護 LSP を障害から保護します。保護された LSP に障害がある場合、送信元ルータは、トンネルのトラフィックを一時的に伝送するセカンダリ LSP をすぐにイネーブルにします。セカンダリ LSP で障害が発生した場合は、セカンダリ パスの障害がクリアされるまでトンネルのパス保護は機能しなくなります。

Cisco EPN Manager は、次の MPLS TE サービス タイプをサポートします。

- 単方向 TE トンネル（Unidirectional TE Tunnel） （624 ページ）
- 双方向 TE トンネル（Bidirectional TE Tunnel） （625 ページ）
- MPLS TE 3 リンク （625 ページ）

単方向 TE トンネル（Unidirectional TE Tunnel）

MPLS TE トンネルは、LSR ペアを接続する単方向トンネルです。単方向トンネルが作成されると、MPLS ネットワーク内の特定のパスに対応するトンネルにラベルが割り当てられます。トラフィックはトンネルを通じてルーティングされます。リターン トラフィックをルーティングするには、同じルータ間に別の単方向トンネルを作成する必要があります。たとえば、ルー

タ A はトンネル 1 のヘッドエンド、ルータ B はテール エンドであり、これは単方向トンネルです。別の単方向トンネルを作成する必要があります。たとえば、ルータ B をヘッド エンドとし、ルータ A をテール エンドとするトンネル 2 です。

双方向 TE トンネル（Bidirectional TE Tunnel）

相互接続されている LSR ペアの間に確立された 2 つの単方向 TE トンネルを互いにバインドして、双方向で相互にルーティングされた TE トンネルを形成することができます。単方向トンネルのバインドは、トンネルの送信元アドレスと宛先アドレス、グローバル ID、関連付け ID、および関連付けアドレスに基づきます。たとえば、2 つの単方向トンネル（トンネル C とトンネル D）によって接続されたルータ A とルータ B をバインドして、次の条件が満足された場合にのみ、双方向 TE トンネルを形成できます。

- トンネル C の送信元アドレスがトンネル D の宛先アドレスであり、トンネル D の送信元アドレスがトンネル C の宛先アドレスである。
- トンネル C およびトンネル D のグローバル ID、関連付け ID、および関連付けアドレスが同じである。トンネルの関連付け ID と関連付けアドレスはシステムで定義されており、トンネル用のグローバル ID を割り当てる必要があります。

双方向 TE トンネルは、RSVP-TE のセキュリティ機能を継承します。

MPLS TE 3 リンク

2 つのデバイス間のトラフィック エンジニアリング リンクを有効にするには、デバイスの両端で次のインターフェイスなどを設定する必要があります。

- ループバック インターフェイス
- イーサネット インターフェイス
- BDI インターフェイス
- OSPF、RSVP、および MPLS
- IS-IS および BGP

これらの設定は、Cisco EPN Manager の MPLS TE 3 リンクプロビジョニング機能を使用して実行できます。

サポートされているシリアル サービス

シリアル通信では、シリアル ポートは一度に 1 ビットずつ数バイトの情報を送受信します。シリアル通信は、より長い距離で使用できます。デバイス間のケーブル配線は、最大 1200 メートルまで延長できます。シリアル通信は ASCII データの送信に使用されます。通信は、地上、送信、および受信の 3 つの伝送回線を使用して実行されます。シリアルは非同期であるため、ポートは 1 つの回線でデータを送信しながら別の回線でデータを受信できます。その他の回線はハンドシェイクに使用できますが、必須ではありません。

Cisco EPN Manager は、次のシリアル サービス タイプをサポートしています。

- RS232：ネットワーク内のデバイスをリンクしてシリアルデータの交換を可能にする標準的な通信プロトコルです。デバイス間のデータ交換に使用されるパスの電圧を定義します。一般的な電圧、信号レベル、共通のピン ワイヤ設定、および最小限の制御信号を指定します。RS232インターフェイスは、短距離および低速要件に適しています。RS232-RS422 ポイントツーポイント サービスは、RS232 サービスと RS422 サービスの設定時に対応するメディアタイプを選択することで設定できます。
- RS485：複数のデバイスの単純なネットワークを形成するために使用される通信バスを定義する EIA/TIA 標準規格です。RS485 インターフェイスは、シングルペア ケーブルを使用してシンプレックスモードまたは半二重モードで使用できます。全二重または同時送受信操作は、2ペア ケーブルで実装できます。このインターフェイスは、長距離にわたって高速であることが求められる場合に使用されます。
- RS422：RS232 よりも長い距離と高速のボー レートを実現するように設計された EIA/TIA 標準規格です。シリアルデータ回線を介した高速でのデータ伝送を可能にするため、RS422 は最大100 kbps のデータレートと最大 4000 フィートまでの距離に対応しています。RS422 は差動トランスミッタと受信機を使用して伝送技術のバランスをとっています。差動ドライバを使用できるようにするため、RS422 は 4 本の導体ケーブルを使用します。さらに、1 本のケーブルに最大 10 台の受信機を設置でき、マルチポイント ネットワークまたはバスを提供できます。
- raw ソケット：IP ネットワークを通じてシリアル データを転送するための方法です。raw ソケットは、リモート端末ユニット（RTU）から遠隔監視制御・情報取得（SCADA）データを転送します。raw ソケットは、ポイントツーポイント接続とポイントツーマルチポイント接続をサポートします。raw ソケットは、非同期シリアル回線を介したポイントツーマルチポイント接続をサポートし、組み込み自動 TCP 接続再試行メカニズムを備えています。同期 RS232、RS422 P2MP オプションを選択し、[同期（Synch）] オプションとメディアタイプオプションを選択して raw ソケットを設定できます。

回線/VC 検出の概要

Cisco EPN Manager は、サービス検出機能を使用して、ネットワーク内に存在する回線/VC を自動的に検出します。**[管理（Administration）] > [システム設定（System Settings）]** でサービス検出機能が有効になっていることを確認します。サービス検出の有効化および無効化 （790 ページ）を参照してください。

回線/VC 検出は、デバイス レベルのインベントリ検出に依存し、次の 2 つの部分で構成されています。

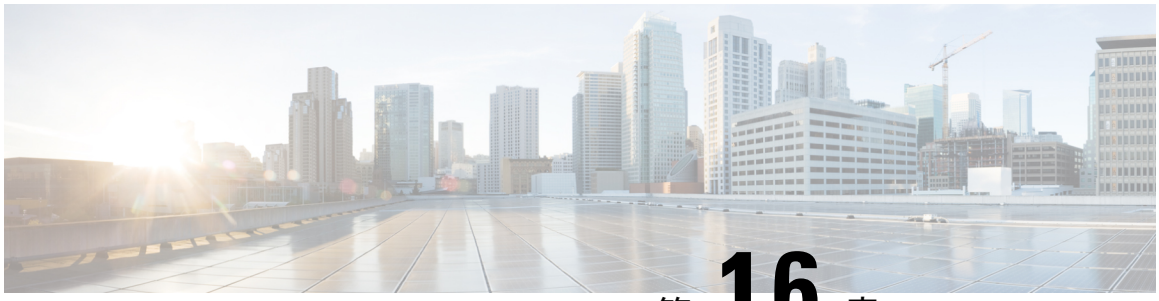
- リソースに対するサービス（RFS）の検出：RFS は、異なるデバイス上のリソース間の関係を表します。RFS 検出時に、デバイス レベルのオブジェクトとネットワーク レベルのオブジェクトが作成されます。デバイス レベルの RFS オブジェクトは、デバイス レベル設定の回線/VC 設定部分を表します。ネットワーク レベルの RFS オブジェクトは、デバ

イスまたはその他のネットワーク レベルのオブジェクトを集約して、ネットワーク レベルのエンティティを表します。

- 顧客向けサービス（CFS）マッチング ：CFS は、回線/VC の顧客向けデータを表します。CFS は検出された RFS から派生し、ネットワーク内の回線/VC のエンドポイントを表します。CFS 検出時に、検出された RFS オブジェクトに対して CFS オブジェクトが作成されます。

検出は、Cisco EPN Manager で進行中のプロセスです。Cisco EPN Manager の使用を開始したときに、ネットワークに存在する回線/VC が検出されます。後で、プロビジョニング ウィザードを使用して回線/VC のプロビジョニングを開始すると、Cisco EPN Manager はプロビジョニングされた回線/VC を検出し、回線/VC で使用されるリソースとネットワークから検出されたリソースとの間の一致を検索します。検出された回線/VC とプロビジョニングされた回線/VC の間に一致が見つかった場合、検出された CFS にプロビジョニングされた CFS からの情報がコピーされます。

Cisco EPN Manager では、プロビジョニングされたバージョンと検出されたバージョンを比較して、デバイス設定で行われた可能性のある変更を識別し、必要に応じて調整を行うことができます。回線/VCのプロビジョニングされたバージョンと検出されたバージョンの比較と調整（826 ページ）を参照してください



第 16 章

回線/VC のプロビジョニング

での回線/VC のプロビジョニング Cisco EPN Manager

回線/VCの作成とプロビジョニングのプロセスは、サポートされているすべてのテクノロジーで類似しており、次の手順が含まれています。

- 回線/VC のエンドポイントの指定。
- 回線/VC の設定パラメータの定義。

Cisco EPN Manager でのプロビジョニング サポートの詳しい概要については、回線/VC のプロビジョニング （629 ページ）参照してください。

新しい回線/VC を作成してプロビジョニングするには、次の手順を実行します。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] タブをクリックします。

ステップ 5 [+] アイコンをクリックします。マップ右側の新しいペインにプロビジョニング ウィザードが表示されます。

（注） または、**[設定（Configuration）] > [ネットワーク（Network）] > [サービス プロビジョニング（Service Provisioning）]** を選択してプロビジョニング ウィザードを表示します。

ステップ 6 [テクノロジー（Technology）] ドロップダウン リストから必要なテクノロジーを選択します。たとえば、光/DWDM ネットワークの回線を作成する場合は、[光（Optical）] を選択します。

ステップ 7 [サービス タイプ（Service Type）] 領域で、作成する回線/VC のタイプを選択します。たとえば、光/DWDM ネットワーク用の回線/VC を作成する場合は、OCHNC WSON、OCHCC WSON、OCH-Trail WSON、OCH-Trail UNI、ODU UNI、ODU トンネル、OPU over ODU など、さまざまな回線タイプがあります。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [カスタマー サービスの詳細情報（Customer Service Details）] ページに移動します。

ステップ 10 （オプション）回線/VC の作成対象顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customers）]** に移動し、プロビジョニング ウィザードに移動して回線/VC のプロビジョニングを開始します。

ステップ 11 サービス名と説明を入力します。

ステップ 12 [展開アクション（Deployment Action）] ドロップダウンリストから、回線/VC の属性を定義した後に実行するアクションを選択します。次のオプションがあります。

- [プレビュー（Preview）]：各デバイスで生成された CLI を表示します。CLI を確認して、属性を編集するか、展開を進めるかを決定できます。
- [展開（Deploy）]：プロビジョニング ウィザードの最後のページで [送信（Submit）] をクリックした直後に関連するデバイスに設定を展開します。

  次のいずれかの展開オプションをクリックします。

  - [今すぐ展開（Deploy Now）]：プロビジョニング順序を直接展開します。
  - [後で展開（Deploy Later）]：作成されたプロビジョニング順序を保存します。同じ順序は、後で展開できます。プロビジョニング順序を再展開するには、左側のペインの下部にある回線/VC のリンクをクリックします。

- [展開のスケジュール（Schedule Deployment）]：指定した時間に、今後の展開の順序を保存します。プロビジョニング順序をスケジュールし、スケジュールした時刻に展開するジョブの順序を作成します。必要に応じて、[ジョブ スケジューラ（Job Scheduler）] ダイアログボックスで順序をプロビジョニングする日付と時刻を指定できます。

  この [展開のスケジュール（Schedule Deployment）] オプション ボタンをクリックした場合は、次を指定します。

  - [スケジュール時刻の展開（Deploy Schedule Time）]：プロビジョニング順序の展開のスケジュール時刻を指定します。
  - [サーバー時刻（Server Time）]：現在のサーバー時刻を表示します。

プロビジョニング順序をスケジュールし、保存する方法の詳細については、次を参照してください。プロビジョニング順序の保存とスケジュール （736 ページ）

ステップ 13 [次へ（Next）] をクリックしてエンドポイントを選択し、選択したテクノロジーに基づいて属性を定義します。

ステップ 14 [送信（Submit）] をクリックします。選択した展開アクションに応じて、関連するアクションが実行されます。つまり、設定のプレビューを選択した場合は、設定を表示できるプレビューページが表示され、その後に [展開（Deploy）] をクリックします。展開を選択した場合、設定は関連するデバイスに直接展開されます。

ステップ 15 （オプション）[このビューのままにする（Leave this View）] ボタンをクリックして Cisco EPN Manager を引き続き使用し、サービスの展開をバックグラウンドで続行できるようにします。

（注） デバイスがビジー状態の場合、サービスを展開する Cisco EPN Manager からの要求は、その要求がタイム アウトする事前に設定された時間まで待機します。この設定を変更するには、サービス展開のタイムアウト値の設定 （632 ページ）を参照してください。

回線/VC が、[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに追加されているはずです。プロビジョニング状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

さまざまなテクノロジーに対して回線/VCを作成し、プロビジョニングする方法については、次を参照してください。

- キャリア イーサネット ネットワークの EVC のプロビジョニング （639 ページ）
- 光/DWDM ネットワークの回線のプロビジョニング （665 ページ）
- L3VPN サービスのプロビジョニング （700 ページ）
- 回線エミュレーション サービスのプロビジョニング （727 ページ）
- MPLS トラフィック エンジニアリング サービスのプロビジョニング （740 ページ）

保存されたプロビジョニング順序は、**[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** > **[プロビジョニング（Provisioning）]** から [計画済み回線/VC（Planned Circuits/VCs）] タブに表示できます。

[最後の実行の統計（Last run stat）] フィールドの [I] アイコンをクリックし、設定とデバイスの詳細を表示します。

サービス展開のタイムアウト値の設定

デバイスにサービスを展開すると、デバイスが事前に占有されているか、またはビジー状態の場合は、作成されたサービス要求は事前に設定された時間まで待機して、サービスを展開するための「デバイス ロック」を取得します。デフォルトでは、タイムアウト値は 60 分に設定されます。

デフォルトのタイムアウト値を変更するには、次の手順を実行します。

ステップ 1 左側のサイドバーから **Administration > Settings > System Settings** を選択します。

ステップ 2 [回線/VC（Circuits/VCs）] セクションを展開し、[展開設定（Deployment Settings）] をクリックします。

ステップ 3 必要なタイムアウト値を分単位で設定します。

Cisco EPN Manager は、サービスを展開するためのデバイス ロックを取得するために指定された時間まで待機します。この時間以内にロックが取得されなかった場合、サービス展開操作は失敗します。

回線アクティベーション待機タイムアウト値の設定

回線アクティベーション待機タイムアウトまでプロビジョニングシステムが待機する最大時間間隔を設定できます。

ステップ 1 左側のサイドバーから **Administration > Settings > System Settings** を選択します。

ステップ 2 [回線/VC（Circuits/VCs）] セクションを展開し、[展開設定（Deployment Settings）] をクリックします。

ステップ 3 [回線アクティベーション待機タイムアウト（Circuit Activation Wait Timeout）] フィールドで、必要なタイムアウト値を分単位で設定します。

デフォルトのタイムアウト値は 5 分です。

WSON/SSON 回線を自動削除するための設定

EPNM が管理する NCS2K TL1 ベースの WSON/SSON 回線を自動削除するオプションを有効にできます。回線が他のデバイスまたは CTC から削除されると、EPNM からも削除されます。WSON/SSON 回線の自動削除を設定するには、次の手順を実行します。

ステップ 1 左側のサイドバーから **Administration > Settings > System Settings** を選択します。

ステップ 2 [回線/VC（Circuits/VCs）] セクションを展開し、[展開設定（Deployment Settings）] をクリックします。

ステップ 3 **[WSON/SSON 回線の自動検出（Auto detect WSON/SSON circuits）]** チェックボックスをオンにします。

展開が失敗した場合の動作

回線/VC を展開すると、Cisco EPN Manager は回線/VC のタイプに基づいて、参加しているデバイスでの設定変更を実行します。設定変更がデバイスに正常に展開された場合にのみ、回線/VCは正常にプロビジョニングされたと見なされます。参加しているデバイスのいずれかで設定変更の展開が失敗した場合は、Cisco EPN Manager がこれまでにデバイスで行われたすべての設定変更をロールバックします。

参加しているデバイスのいずれかで設定変更の展開が失敗した場合は、プロビジョニングウィザードで**[再展開（Redeploy）]**をクリックできます。再展開アクションは、同じ設定で展開を再試行します。

（注） [再展開（Redeploy）] ボタンは、OCHNC WSON、OCHCC WSON、OCHCC、OCH-Trail WSON、OCH-Trail、Media Channel NC SSON、Media Channel Trail SSON、Media Channel CC SSON 光回線でサポートされています。

展開アクションでは、次のシナリオのいずれかが発生する可能性があります。

- 参加しているすべてのデバイスで展開が成功し、ロールバックは開始されない：このシナリオでは、すべてのデバイスが正常に設定され、回線のプロビジョニングが成功します。
- 展開が失敗して、ロールバックが開始され、成功する：このシナリオでは、複数のデバイスを設定したときに、デバイスのいずれかで設定が失敗します。障害は、たとえば、デバイスが設定を拒否したなど、さまざまな理由が原因となる可能性があります。Cisco EPN Manager は障害を識別し、すべてのデバイスで行われたすべての設定変更を正常にロールバックします。このシナリオでは、すべてのデバイス設定が展開前の状態に復元されます。

  順番に回線をプロビジョニングするように設定された3つのデバイス（A、B、およびC）を使用した例を以下に示します。デバイスAでは設定変更が正常に展開されますが、デバイス B では展開が失敗します。Cisco EPN Manager は、失敗を検出して、デバイス B およびCの以降の設定を中止します。また、プロビジョニングの逆順で設定をロールバックします。つまり、最初にデバイス B をロールバックしてからデバイス A をロールバックします。3 つのデバイスで順に実行されるアクションを以下に示します。

  - デバイスC：まだ変更がデバイスに展開されていないため、デバイスCに対するロールバックは必要ありません。これは、設定変更がデバイスCに送信される前に、デバイス B で設定の失敗が検出されたことを意味します。
  - デバイス B：Cisco EPN Manager は、展開が失敗する前にこのデバイスで行われた設定変更があるかどうかをチェックします。変更がある場合は、このデバイスの部分的な設定が削除され、デバイスが以前の設定にロールバックされます。

- デバイス A：Cisco EPN Manager は、デバイス A で完全なロールバックを実行します。正常に展開されたすべての設定変更が削除され、デバイスは以前の設定にロールバックされます。

- 展開が失敗して、ロールバックが開始されたが、失敗した：このシナリオでは、参加しているデバイスのいずれかで設定の展開が失敗すると、Cisco EPN Manager がロールバックを実行しますが、1 つ以上のデバイス上のロールバックが失敗します。この場合、ロールバックが失敗したデバイスには部分的な設定が残ります。

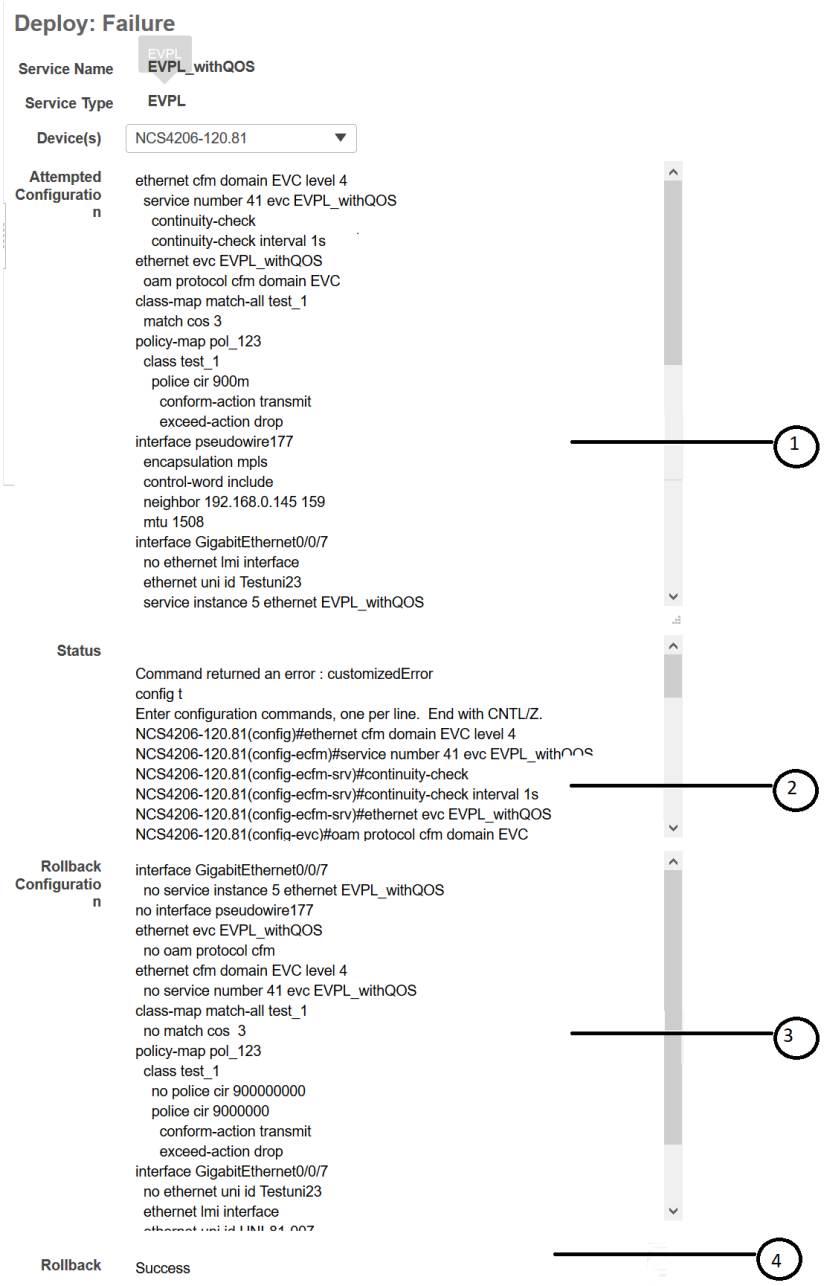
  たとえば、デバイス A および B で設定変更が正常に展開され、デバイス C で展開が失敗した場合です。Cisco EPN Manager は、失敗を特定して、プロビジョニングの逆順でロールバックを開始します。つまり、デバイス C、デバイス B、デバイス A の順にロールバックします。3 つのデバイスで順に実行されるアクションを以下に示します。

  - デバイス C：Cisco EPN Manager はデバイス C で正常にロールバックを実行します。
  - デバイス B：デバイス B でロールバックを試みると、デバイス接続が失われ、デバイス上に部分的な設定が残される可能性があります。
  - デバイス A：Cisco EPN Manager は、デバイス B でロールバックが失敗しても、デバイス A のロールバックを実行します。

（注） ロールバックは、他のさまざまな理由で失敗することがあります。

プロビジョニング ウィザードで、設定をプレビューしてから、[展開（Deploy）] をクリックします。展開が失敗すると、参加している各デバイスのロールバック設定とステータスが表示されます。[デバイス（Device(s)）] ドロップダウン リストで、ロールバック設定とステータスを表示するデバイスを選択します。

次の図に、各デバイスのロールバック設定とロールバック ステータスを示します。



1	[試みた設定（Attempted Configuration）]：[デバイス（Device(s)）] ドロップダウン リストで選択されたデバイスに展開された設定を表示します。
2	[展開ステータス（Deployment Status）]：選択されたデバイスの展開ステータスを表示します。展開が成功すると、[成功（Success）] というステータスが表示されます。展開が失敗すると、失敗に関する情報が提供されます。

3	[ロールバック設定（Roll back Configuration）]：ロールバックが自動的に試みられる設定を表示します。
4	[ロールバック ステータス（Roll back Status）]：選択されたデバイスのロールバックステータスを表示します。ロールバックが成功すると、[成功（Success）] というステータスが表示されます。ロールバックが失敗すると、失敗に関する情報が提供されます。この情報を使用して、デバイスの部分的な設定を手動でクリーンアップすることができます。

[削除（Delete）] をクリックして、失敗した展開をこのウィンドウから削除することもできます。

また、拡張テーブル内の [回線/VC（Circuits/VCs）] タブと [削除済み回線/VC（Deleted Circuits/VCs）] タブの [プロビジョニング（Provisioning）] 列の横にある [i] アイコンをクリックして回線/VC に参加している各デバイスの設定、設定エラー、ロールバック設定、およびロールバック設定エラーの詳細を表示することもできます。[i] アイコンは、[なし（None）] を除くすべてのプロビジョニング状態で使用できます。拡張テーブルへのアクセス方法については、ネットワーク トポロジ マップからのアラーム、ネットワーク インターフェイス、回線/VC、およびリンクの詳細テーブルの表示 （222 ページ）を参照してください。

展開とロールバックの失敗をトラブルシュートする方法については、構成導入の失敗およびロールバックの失敗のトラブルシューティング （636 ページ）を参照してください。

構成導入の失敗およびロールバックの失敗のトラブルシューティング

以下に、導入またはロールバックの失敗をトラブルシューティングするためのヒントを示します。

- 導入は失敗するが、ロールバックは成功する場合：構成導入が失敗しても、ロールバックは自動的に開始され、結果が結果ページに表示されます。各デバイスの結果ページに表示される試行された設定とエラー メッセージを分析し、展開の失敗の根本原因を特定します。

  導入の失敗の原因として、次の問題が考えられますが、これらに限定されません。

  - プロビジョニング ウィザードでサービス パラメータに無効な値が入力されました。たとえば、サービス ID はすでに存在しているか、生成された CLI にセマンティック エラーがある可能性があります。
  - デバイスに到達できない、デバイスパスワードが変更された、などのデバイスの問題があります。

  この場合は、導入に失敗した回線を（作成時に指定した名前で）特定し、その回線を編集してプロビジョニングを再試行する必要があります。値を変更するサービスパラメータが編集できない場合は、回線を削除して新しい回線を作成します。

（注） 回線を削除する前に、使用されていないことを確認します。

- 導入とロールバックの両方が失敗する場合：この場合は、次の手順を実行します。
  1. デバイスに到達可能であることを確認し、デバイスの再同期を実行します。
  2. 前の導入で報告されたデバイスの問題があれば、問題を修正します。
  3. 回線を編集し、必要に応じて属性を更新して、回線の導入を再試行します。
  4. 導入が失敗すると、Cisco EPN Manager はロールバックを開始します。
  5. ロールが再び失敗した場合は、ロールバックの失敗の原因を特定します。
  6. 失敗の原因を特定するには、構成とロールバック トランザクションの詳細、サービス導入の試行の履歴、および回線/VC 360 度ビューに表示されるロールバック試行を使用できます。回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ）を参照してください。
  7. 手動でデバイスに保存されている部分構成を削除します。

また、シスコ担当者に問い合わせて、設定の展開の失敗とロールバックの失敗の根本原因を分析し、特定することもできます。

WAN 自動化エンジンの統合

Cisco WAN Automation Engine と Cisco EPN Manager の統合

Cisco WAN Automation Engine（WAE）のプラットフォームは、ソフトウェア モジュールを相互接続し、ネットワークと通信し、外部アプリケーションとインターフェイスする API を提供するオープンでプログラマブルなフレームワークです。

Cisco WAE は、ネットワークの継続的なモニターリングと分析およびネットワーク上のトラフィック需要に基づく現在のネットワークのモデルを作成および維持するためのツールを提供します。このネットワーク モデルには、トポロジ、設定、トラフィック情報など、特定の時点でのネットワークに関するすべての関連情報が含まれています。この情報は、トラフィック要求、パス、ノードとリンクの障害、ネットワークの最適化、またはその他の変更によるネットワークへの影響を分析するための基礎として使用できます。

（注） 詳細については、『*Cisco WAN Automation Engine (WAE) Installation Guide*』と『*Cisco WAN Automation Engine (WAE) User Guide*』を参照してください。

Cisco EPN Manager では、明示的なパスを持つ単方向トンネルまたは双方向トンネルを作成すると、WAN Automation Engine（WAE）との統合により、Cisco EPN Manager から自動的に REST コールを使用して明示的なパスが提供されます。そのため、明示的なパスを手動で入力する必

要がなくなります。WAE は、可能なネットワーク パスのリストを表示し、適切なパスを選択できるようにします。

WAE パラメータの設定

WAE パスの詳細を指定するには、次の手順を実行します。

始める前に

WAE パラメータを設定することを確認します。

1. **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。
2. 回線 VC を展開し、[WAE サーバー設定（WAE Server Settings）] を選択します。
3. 関連する WAE の詳細（バージョン 7.1.3 以降）とフィールドの詳細（[WAE サーバー IP（WAE Server IP）]、[WAE ポートアドレス（WAE Port Address）]、[WAE サーバーユーザー名（WAE Server User Name）]、[WAE サーバーパスワード（WAE Server Password）] など）を入力します。
4. [保存（Save）] をクリックして WAE サーバーの設定を保存するか、または [デフォルトにリセット（Reset to Defaults）] をクリックしてすべての入力をクリアします。

ステップ 1 必要なパラメータを持つ単方向トンネルまたは双方向トンネルを作成します。詳細については、MPLS TE トンネルの作成とプロビジョニング （751 ページ）を参照してください。

ステップ 2 [パスの制約の詳細（Path Constraints Details）] 領域で、パスのタイプを [動作中（Working）] または [保護済み（Protected）] のいずれかとして選択します。フィールドと属性の説明については、パスの制約の詳細に関するフィールド参照：MPLS TE トンネル （762 ページ）を参照してください。

ステップ 3 必要に応じて [新しいパス（New Path）] チェックボックスをオンにして、[WAEサーバーからパスを選択（Choose Path from WAE server）] チェックボックスをオンにします。

ステップ 4 [WAE サーバーからパスを選択（Choose Path from WAE server）] チェックボックスをオンにします。EPNM マネージャは、WAE ネットワークを取得するために REST 要求を WAE に送信します。
WAE は可能なネットワークのリストを返します。

ステップ 5 [WAE ネットワークの選択（Select WAE Network）] ドロップダウン リストから、ネットワークを選択します。
EPNM マネージャは、送信元、宛先、ネットワークなどの必要なすべてのパラメータを持つ REST 設定要求を WAE に送信します。返される最大パスのデフォルト値は 2 です。最大パス値は WAE を介して設定されます。WAE は、要求を満たす可能性のあるパスのリストを表示します。

ステップ 6 [WAE パスの選択（Select WAE Path）] ドロップダウン リストから、返された適切なパスを選択します。
EPNM は、マップ上に選択したパス オーバーレイを表示します。

ステップ 7 [パス名（Path Name）] フィールドにパスの名前を入力します。
最後に選択したパスを明示的なパスとして使用して、順序のプロビジョニングを続行できます。

キャリアイーサネットネットワークのEVCのプロビジョニング

Cisco EPN Manager キャリア イーサネット プロビジョニング サポートの概要

このトピックでは、Cisco EPN Manager におけるキャリア イーサネット サービス プロビジョニング サポートの概要を示します。さまざまなタイプの EVC とサポートされる基盤ネットワークの詳細については、回線/VC の検出およびプロビジョニングの概要 （605 ページ）を参照してください。

Cisco EPN Manager は、次のタイプのポートベースおよび VLAN ベースの VC のプロビジョニングをサポートします。

- E-line：イーサネット専用回線（EPL）とイーサネット仮想専用回線（EVPL）。E-Line （607 ページ）を参照してください。
- E-LAN：EP-LAN と EVP-LAN。E-LAN （608 ページ）を参照してください。
- E-Access：Access EPL と Access EVPL。E-Access （609 ページ）を参照してください。
- E-TREE：EP-TREE と EVP-TREE。E-Tree （609 ページ）を参照してください。
- EVPN 仮想プライベートワイヤサービス（VPWS）。EVPN 仮想プライベート ワイヤ サービス（VPWS） （610 ページ）を参照してください。

Cisco EPN Manager は、EVC の作成時に使用可能な次の補足プロビジョニング機能をサポートします。

- UNI のプロビジョニング：EVC ごとに、参加する UNI の属性を定義する必要があります。EVC の作成中にこれを行うか、または EVC の作成プロセスとは無関係に UNI をプロビジョニングできます。UNI としてのデバイスおよびインターフェイスの設定 （656 ページ）を参照してください。
- ENNI のプロビジョニング：E-Access 回線の場合、ENNI の属性を定義する必要があります。EVC の作成中にこれを行うか、または EVC の作成プロセスとは無関係に ENNI をプロビジョニングできます。デバイスとインターフェイスを ENNI として設定する （657 ページ）を参照してください。
- QoS プロファイル：QoS プロファイルを作成して VC に適用できます。

- EVC 属性のプロファイル：EVC のすべての必須属性を含むプロファイルを作成できます。これらのプロファイルを EVC の作成中に選択して、EVC の属性を定義できます。各 EVC の属性を個別に定義する必要はありません。回線/VC プロファイル （776 ページ） を参照してください。

EVC プロビジョニングの前提条件

EVC をプロビジョニングする前に、次の前提条件を満たしている必要があります。

1. EVC をプロビジョニングする前にデバイスの間の通信をセットアップする必要があります。
   - MPLS エンドツーエンド ネットワークでは、ラベル配布プロトコル（LDP）をネットワーク全体でセットアップし、各デバイスに LDP ID を指定する必要があります。これにより、MPLS ネットワークのピアのラベル スイッチ ルータ（LSR）は、ホップバイホップ転送をサポートするためにラベル バインド情報を交換できます。または、MPLS トラフィック エンジニアリングまたはセグメントルーティングを使用して MPLS エンドツーエンド接続を実現できます。具体的には、単方向または双方向の TE トンネルを介した EVC（P2P タイプのみ）プロビジョニングがサポートされます。TE トンネルを介した CEm プロビジョニングと SR ポリシーを介したプロビジョニングもサポートされています。
   - イーサネット アクセスがある場合、つまり、すべてのデバイスが MPLS に対応しているわけではない場合は、イーサネット アクセス スイッチを MPLS スイッチに接続するように G.8032 リングまたは ICCP-SM を設定する必要があります。
   - CDP または LLDP は、イーサネット リンク検出を有効にするように、G.8032 リング内のリンク上に設定する必要があります。
2. ICCP-SM と G.8032 ネットワーク上に EVC をプロビジョニングするには、すべての VLAN（1 から 4095 まで）をプライマリまたはセカンダリ VLAN として設定する必要があります。
3. EVC をプロビジョニングするデバイスのインベントリ収集の状態は [完了（Completed）] である必要があります。これを確認するには **Inventory > Network Devices** に移動し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列のステータスを確認します。
4. システムに顧客を作成して、回線/VC の作成およびプロビジョニング プロセス中に顧客に回線/VC を関連付けられるようにすることができます。左側のサイドバーで **Inventory > Other > Customers** を選択し、顧客を作成および管理します。
5. EVC でインターフェイスを使用する場合は、インターフェイスのデフォルト設定をリセットすることをお勧めします。グローバル コンフィギュレーション モードでは、各インターフェイスで次のコマンドを設定します。

   ```
   default interface 'interface-name'
   ```

6. ME3600 と ME3800 デバイスでは、サービス インスタンスは、VLAN が許可されていないトランク ポートでのみ設定できます。インターフェイスで次のコマンドを設定し、Cisco EPN Manager でデバイスを再同期します。

```
interface GigabitEthernetXX/XX
switchport trunk allowed vlan none
switchport mode trunk
```

7. EVPN の使用時に EPL および EVPN サービスをプロビジョニングするには、デバイス設定の [BGP] セクションで次のコマンドを定義します。このコマンドを設定しない場合、EVPN サービスのプロビジョニング時にデバイスは表示されません。

```
address-family l2vpn evpn
```

新規キャリア イーサネット EVC の作成およびプロビジョニング

EVC はトポロジ マップのコンテキストで作成します。トポロジ マップとプロビジョニング ウィザードにアクセスするには、左側のサイドバーから **[構成（Configuration）]** > **[ネットワーク（Network）]** > **[サービス プロビジョニング（Service Provisioning）]** の順に選択します。または、次の手順での説明に従ってトポロジ マップからプロビジョニング ウィザードを開くこともできます。

EVC を作成してプロビジョニングするプロセスは、サポートされているすべての EVC タイプで同様であり、次の作業が含まれます。

- EVC のエンドポイント（UNI および ENNI）を指定します。
- 回線/VC の設定パラメータを定義します。

サービスがプロビジョニングされた後は、サービスを編集し、A エンド ポイントまたは Z エンド ポイントを更新または変更できます。

エンドポイントの変更は、EPL や EVPL などの E 回線サービスでサポートされています。変更できるのは管理対象エンドポイントと、フル サービスまたは部分的サービスのみです。

サービスの変更中に、既存の UNI に異なるデバイスか、または異なるポートを持つ同じデバイスがある場合は、既存の他の UNI に変更できます。

これには次のような制約があります。

- 1 回のサービス変更で、両端のエンドポイントを変更することはできません。
- スタンドアロン UNI ウィザードを使用して UNI を作成し、EPL サービスまたは EVPL サービスの変更に使用します。
- サービスの変更中に新しい UNI を作成することはできません。

始める前に

EVC をプロビジョニングする前に満たす必要がある前提条件については、EVC プロビジョニングの前提条件 （640 ページ）を参照してください。

新しい EVC を作成するには、次の手順に従います。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 ツールバーで [デバイス グループ（Device Group）] ボタンをクリックし、マップに表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、[+] アイコンをクリックします。これにより、マップの右側に新しいペインが開き、[プロビジョニング ウィザード（Provisioning Wizard）] が表示されます。

ステップ 4 [テクノロジー（Technology）] ドロップダウンリストで **Carrier Ethernet** を選択します。Cisco EPN Manager の [サービス タイプ（Service Type）] 領域に、関連する回線/VC タイプのリストが表示されます。たとえば、キャリア イーサネット サービス タイプには EPL、EVPL、EP-LAN などが含まれます。

ステップ 5 [サービス タイプ（Service Type）] リストから、作成する回線/VC のタイプを選択します。

ステップ 6 さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 7 **Next** をクリックして [サービスの詳細（Service Details）] ページに移動します。

ステップ 8 （オプション）EVC の作成対象顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。

ステップ 9 サービスの詳細を入力します。フィールドと属性の説明については、サービス詳細の参考資料 （650 ページ）を参照してください。

ステップ 10 E-Line EVC、E-Tree EVC、E-LAN EVC の場合：必要に応じて、EVC で障害およびパフォーマンス モニターリングを可能にするサービス OAM を設定します。E-Line EVC の場合：[サービス OAM（Service OAM）] オプションを有効にするには、[CFM の有効化（Enable CFM）] チェックボックスをオンにします。その後、新しい CFM ドメインを作成するか、または E 回線 EVC の既存のドメインを選択することができます。サービス OAM （655 ページ）を参照してください。プラス アイコンをクリックして [サービス OAM（Service OAM）] テーブルに行を追加し、該当する列に値を入力します。E-Tree EVC の場合、方向（リーフからルート、ルートからリーフ、またはルートからルート）を指定する必要があります。

たとえば EVPL/EPL サービスの場合、ポイントツーポイント サービスまたはマルチポイントサービスを昇格させ、調整する場合は、[CFM ドメイン名（CFM Domain name）]、[CFM ドメインレベル（CFM Domain level）]、および [メンテナンス（Maint）] などの CFM パラメータを有効にします。関連付けられた[名前のタイプ（Name Type）] フィールド、[ITU キャリアコード（ITU Carrier Code）] フィールド、[ITU MEG ID コード（ITU MEG ID Code）] フィールド、[継続性チェック間隔（Continuity check interval）] フィールド。CFM パラメータは、サービス昇格時に検出されたバージョンから読み取られます。検出されたバージョンか、またはプロビジョニングされたバージョンとの調整を実行できます。

（注） デフォルトでは、[メンテナンス関連名（Maint Assoc Name）] として IEEE が選択されています。[メンテナンス（Maint）] で [ITU] が選択されている場合。関連付けられた[名前のタイプ（Name Type）] ドロップダウンリスト、[ITU キャリアコード（ITU Carrier Code）]、および [ITU MEG ID コード（ITU MEG ID code）] が表示されます。

ステップ 11 [展開アクション（Deployment Action）] フィールドに、ECV の作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 12 **Next** をクリックして UNI を定義するページに移動します。E-Access の場合、ENNI を定義するページもあります。

ステップ 13 UNI として機能するデバイスとインターフェイスを識別します。

（注） エンドポイントのいずれかが、Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、[管理対象外（Unmanaged）] チェックボックスをオンにして、その管理対象外デバイスの情報を入力します。アンマネージド エンドポイントを使用した回線/VC のプロビジョニング （778 ページ）を参照してください。

- デバイス上で必要なインターフェイスを既に設定している場合は、**Create New UNI** チェックボックスをオフにして、関連する UNI 名をリストから選択します。

  （注） リスト内の UNI 名は、UNI の作成時に選択したサービスとオプションによって異なります。

  - EPL、Access EPL、EP LAN、および EP Tree サービスの場合は、作成時に [すべてを1つにバンドリング（All To One Bundling）] オプションが選択された UNI のみが表示されます。
  - EVPL、Access EVPL、および EVP Tree サービスの場合、[多重化（Multiplexing）] オプションまたは [バンドリング（Bundling）] オプション、またはその両方が作成時に選択された UNI のみがリストされます。

- 新しい UNI を作成するには、次の手順を実行します。
  - **Create New UNI** チェックボックスがオンになっていることを確認します。
  - [UNI 名（UNI Name）] フィールドに、UNI を簡単に識別できるような UNI 名を入力します。
  - [デバイス（Device）] フィールドのリストからデバイスを選択するか、マップ内のデバイスをクリックして選択し、[デバイス（Device）] フィールドに取り込みます。選択したデバイスのポートのリストが表示されます。
  - [ポート（Port）] テーブルから必要なポートを選択します。ポートを UNI に使用できない場合は、[ポート（Port）] テーブルの UNI 名の横にアラート アイコンが表示され、ポートが選択できない理由が示されます。

  （注） UNI の作成時に選択したデバイスは、マップ内でオレンジ色の丸で囲われます。オレンジの円の上に UNI 名が表示されます。ポイントツーポイント EVC の場合、オレンジの円に、これが A 側または Z 側のどちらのエンドポイントであるかを示すラベルが付けられます。

ステップ 14 新しい UNI を作成している場合は、新しい UNI の詳細を入力します。フィールドと属性の説明については、新規 UNI の詳細リファレンス （651 ページ）を参照してください。

ステップ 15 UNI サービスの詳細を入力します。フィールドと属性の説明については、UNI サービス詳細の参照 （652 ページ）を参照してください。

ステップ 16 H-VPLS をコア テクノロジーとして使用する E-LAN EVC および E-TREE EVC の場合、プライマリ ハブとセカンダリ ハブとして機能するデバイスをそれぞれ選択します。

ステップ 17 E 回線 EVC の場合：[疑似回線設定（Pseudowire Settings）] ページで、次のようにして EVC が経由する TE トンネルを選択できます。

1. [静的優先パス（Static Preferred Path）] チェックボックスをオンにして、サービスの静的ルートを割り当てます。
2. [優先パス タイプ（Preferred Path Type）] に [双方向（Bidirectional）] または [単方向（Unidirectional）]、あるいは [SR ポリシー（SR Policy）] を選択します。
3. [優先パス（Preferred Path）] ドロップダウン リストから、必要な双方向 TE トンネルを選択します。このリストには、EVC のエンドポイント間にすでに存在する双方向 TE トンネルのすべてが示されます。

   （注） このフィールドが有効になるのは、[優先パス タイプ（Preferred Path Type）] として [双方向（Bidirectional）] を選択した場合のみです。

4. [優先パス（A-Z）（Preferred Path (A-Z)）] および [優先パス（Z-A）（Preferred Path (Z-A)）] ドロップダウン リストのそれぞれから、必要な単方向 TE トンネルを選択します。

   （注） これらのフィールドは、[優先パス タイプ（Preferred Path Type）] に [単方向（Unidirectional）] を選択したときにのみ使用できます。

5. 優先パスが使用できない場合にデフォルト パスが使用されるようにするには、[LDP へのフォールバックを許可（Allow Fallback to LDP）] チェックボックスをオンにします。

   （注） エンドポイント間にトンネルが存在しない場合、[優先パス（Preferred Path）] および [LDP へのフォールバックを許可（Allow Fallback to LDP）] オプションは無効になります。

6. 接続の両側で疑似回線ペイロードを識別するためにコントロール ワードが使用されるようにするには、[送信コントロール ワード（Send Control Word）] チェックボックスをオンにします。
7. イーサネット、VLAN、または IP のいずれかを使用する相互接続サイトが必要な場合は、[相互接続オプション（Interworking Option）] を選択します。EVC のいずれかのエンドポイントが管理対象外デバイスである場合は、このオプションを有効にする必要があります。
8. 疑似回線に必要な帯域幅を入力します。
9. [PW ID] フィールドには、ポイントツーポイント サービスの疑似回線の設定に表示する識別子を入力します。

   （注） 疑似回線（PW）の ID は、PW ID のリソース プールから自動的に割り当てられます。PW ID 値は、サービスの作成時にのみ変更できます。EVC サービスの変更時にこの値を編集することはできません。入力された PW ID が既にサービスに割り当てられている場合は、エラー メッセージが表示されます。

ステップ 18 （オプション）サービスに参加するデバイス上に設定する追加の CLI コマンドをテンプレートに追加する場合は、[サービス テンプレート（Service Template）] ページを使用します。詳細については、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

ステップ 19 回線/VC に必要な情報をすべて入力したら、**Submit** をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集（Edit

Attributes）]をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

ステップ 20 回線/VC が、[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] タブのリストに追加されているはずです。

設定の展開が失敗した場合は、展開が失敗した場合の動作（633ページ）を参照してください。

EVPN VPWS 技術を使用した新しいキャリアイーサネット EVC の作成とプロビジョニング

EVPN を使用してキャリアイーサネット EVC を作成してプロビジョニングするには、次の手順を実行します。

始める前に

EVC をプロビジョニングする前に満たす必要がある前提条件については、EVC プロビジョニングの前提条件 （640 ページ）を参照してください。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 ツールバーで [デバイス グループ（Device Group）] ボタンをクリックし、マップに表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、[+] アイコンをクリックします。これにより、マップの右側に新しいペインが開き、[プロビジョニング ウィザード（Provisioning Wizard）] が表示されます。

ステップ 4 [テクノロジー（Technology）] ドロップダウン リストで **Carrier Ethernet** を選択すると、Cisco EPN Manager は [サービス タイプ（Service Type）] 領域に関連する回線/VC タイプのリストを表示します。EVPN は、キャリアイーサネットのサービスタイプ EPL および EVPL でサポートされています。

ステップ 5 [サービス タイプ（Service Type）] リストから、作成する回線/VC のタイプを選択します。

ステップ 6 さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 7 **Next** をクリックして [サービスの詳細（Service Details）] ページに移動します。

ステップ 8 （オプション）EVC の作成対象顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。

ステップ 9 サービスの詳細を入力します。フィールドと属性の説明については、サービス詳細の参考資料（650ページ）を参照してください。

ステップ 10 [EVPN を使用（Use EVPN）] チェックボックスをオンにします。

ステップ 11 E-Line EVC の場合：必要に応じて、EVC で障害およびパフォーマンスのモニターリングを可能にするサービス OAM を設定します。[CFM の有効化（Enable CFM）] チェックボックスをオンにしてサービス OAM オプションを有効にします。その後、新しい CFM ドメインを作成するか、または E 回線 EVC の既存のドメインを選択することができます。サービス OAM （655 ページ）を参照してください。プラス

アイコンをクリックして [サービス OAM（Service OAM）] テーブルに行を追加し、該当する列に値を入力します。

（注） ICC ベースの CFM は、EVPN ではサポートされていません。

ステップ 12 [展開アクション（Deployment Action）] フィールドに、ECV の作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 13 UNI として機能するデバイスとインターフェイスを識別します。

（注） EVPN は、管理対象外デバイスをサポートしていません。

[サービスの詳細（Service Detail）] ページの [EVPN を使用（Use EVPN）] チェックボックスをオンにすると、EVPN をサポートするデバイスのみが [UNI A] ページと [UNI Z] ページに表示されます。

- デバイス上で必要なインターフェイスを既に設定している場合は、**Create New UNI** チェックボックスをオフにして、関連する UNI 名をリストから選択します。

  （注） リスト内の UNI 名は、UNI の作成時に選択したサービスとオプションによって異なります。

  - EPL、Access EPL、EPE LAN、および EP Tree サービスの場合は、作成時に [すべてを1つにバンドリング（All To One Bundling）] オプションが選択された UNI のみが表示されます。
  - EVPL、Access EVPL、および EVP Tree サービスの場合、[多重化（Multiplexing）] オプションまたは [バンドリング（Bundling）] オプション、またはその両方が作成時に選択された UNI のみがリストされます。

- 新しい UNI を作成するには、次の手順を実行します。
  - **Create New UNI** チェックボックスがオンになっていることを確認します。
  - [UNI 名（UNI Name）] フィールドに、UNI を簡単に識別できるような UNI 名を入力します。
  - [デバイス（Device）] フィールドのリストからデバイスを選択するか、マップ内のデバイスをクリックして選択し、[デバイス（Device）] フィールドに取り込みます。選択したデバイスのポートのリストが表示されます。
  - [ポート（Port）] テーブルから必要なポートを選択します。ポートを UNI に使用できない場合は、[ポート（Port）] テーブルの UNI 名の横にアラート アイコンが表示され、ポートが選択できない理由が示されます。

  （注） UNI の作成時に選択したデバイスは、マップ内でオレンジ色の丸で囲われます。オレンジの円の上に UNI 名が表示されます。ポイントツーポイント EVC の場合、オレンジの円に、これが A 側または Z 側のどちらのエンドポイントであるかを示すラベルが付けられます。

ステップ 14 新しい UNI を作成している場合は、新しい UNI の詳細を入力します。フィールドと属性の説明については、新規 UNI の詳細リファレンス （651 ページ）を参照してください。

ステップ 15 UNI サービスの詳細を入力します。フィールドと属性の説明については、UNI サービス詳細の参照（652 ページ）を参照してください。

ステップ 16 E-Line EVC の場合：[EVPNの設定（EVPN Settings）] ページで、次の手順を実行します。

1. [EVPN インスタンス（EVI）ID（EVPN Instance (EVI ID)] は事前に入力されています。この値は必要に応じて変更できます。
2. [RD 値（RD Value）] を指定するには、[自動 RD（Auto RD）] チェックボックスをオフにします。
3. [RT のインポート（Import RT）] および [RT のエクスポート（Export RT）] の値を指定するには、[自動 RT（Auto RT）] チェックボックスをオフにします。

   （注） [RT のインポート（Import RT）]、[RT のエクスポート（Export RT）]、[RD]、および [コントロールワード（Control Word）] は、使用した EVI ID が他のそのサービスにも関連付けられていない場合にのみ編集できます。

4. 接続の両側でペイロートを識別するためにコントロールワードを使用するには、[コントロールワード（Control Word）] チェックボックスをオンにします。
5. Z エンド AC 識別子と A エンド AC 識別子は事前に入力されています。これらの値は必要に応じて変更できます。
6. [静的優先パス（Static Preferred Path）] チェックボックスを選択して A ～ Z または Z ～ A の優先パスを指定し、SR ポリシーを指定できます。
7. 優先パスが使用できない場合にデフォルト パスが使用されるようにするには、[LDP へのフォールバックを許可（Allow Fallback to LDP）] チェックボックスをオンにします。

   （注） エンドポイント間にトンネルが存在しない場合、[優先パス（Preferred Path）] および [LDP へのフォールバックを許可（Allow Fallback to LDP）] オプションは無効になります。

ステップ 17 （オプション）サービスに参加するデバイス上に設定する追加の CLI コマンドをテンプレートに追加する場合は、[サービス テンプレート（Service Template）] ページを使用します。詳細については、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

ステップ 18 回線/VC に必要な情報をすべて入力したら、**Submit** をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集（Edit Attributes）] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

ステップ 19 回線/VC が、[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] タブのリストに追加されているはずです。

複数の UNI を使用した EVC の作成およびプロビジョニング

Cisco EPN Manager では、マルチポイント EVC（E-LAN および E-Tree）を作成してプロビジョニングするプロセスで、複数の UNI の作成/選択がサポートされています。

（注） VPLS をコア テクノロジーとして使用する EVC の場合、同じデバイス上に複数の UNI を設定できますが、H-VPLS ベースの EVC の場合はその限りではありません。

始める前に

EVC をプロビジョニングする前に満たす必要がある前提条件については、EVC プロビジョニングの前提条件 （640 ページ）を参照してください。

新しい EVC を作成するには、次の手順に従います。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

ステップ 2 ツールバーで [デバイス グループ（Device Groups）] をクリックし、マップ上に表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブをクリックします。

ステップ 4 [回線/VC（Circuits/VCs）] ペインのツールバーで、[+]（作成）アイコンをクリックします。

マップの右側に新しいペインが開き、[プロビジョニング ウィザード（Provisioning Wizard）] が表示されます。

ステップ 5 [テクノロジーの選択（Select Technology）] ドロップダウン リストで **Carrier Ethernet** を選択します。

ステップ 6 [サービス タイプ（Service Type）] リストから、マルチポイント EVC タイプを選択します。

ステップ 7 さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 8 **Next** をクリックして [サービスの詳細（Service Details）] ページに移動します。

ステップ 9 EVC を作成する対象の顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。

ステップ 10 サービスの詳細を入力します。フィールドと属性の説明については、サービス詳細の参考資料 （650 ページ）を参照してください。

ステップ 11 [展開アクション（Deployment Action）] フィールドに、ECV の作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 12 [次へ（Next）] をクリックして UNI を定義するページに進みます。

ステップ 13 [マルチ UNI（Multi UNI）] 領域でプラス アイコンをクリックし、最初の UNI をテーブルに追加します。UNI にはデフォルトの名前が付けられて、自動的にテーブル内で選択された状態になります。プラス アイコンをクリックするたびに、新しい UNI がテーブルに追加されます。

または、マップ内のデバイスをクリックして新しい UNI をテーブルに追加することもできます。この場合、新規 UNI の詳細の [デバイス（Device）] フィールドに、そのデバイスの名前が取り込まれます。

ステップ 14 テーブルから、属性を定義または編集する UNI を選択します。

ステップ 15 UNI として機能するデバイスとインターフェイスを識別します。

- 既存の UNI を使用する場合、[新規 UNI の作成（Create New UNI）] チェックボックスをオフにして、リストから該当する UNI 名を選択します。

  （注） リスト内の UNI 名は、UNI の作成時に選択したサービスとオプションによって異なります。

  - EPL、Access EPL、EP LAN、および EP Tree サービスの場合は、作成時に [すべてを1つにバンドリング（All To One Bundling）] オプションが選択された UNI のみが表示されます。
  - EVPL、Access EVPL、および EVP Tree サービスの場合、[多重化（Multiplexing）] オプションまたは [バンドリング（Bundling）] オプション、またはその両方が作成時に選択された UNI のみがリストされます。

- 新しい UNI を定義するには、次の手順に従います。
  - [新規 UNI の作成（Create New UNI）] チェックボックスがオフにされていることを確認します。
  - [UNI 名（UNI Name）] フィールドに、UNI を簡単に識別できるような UNI 名を入力します。
  - [デバイス（Device）] フィールドで、リストからデバイスを選択します。選択したデバイスのポートのリストが表示されます。
  - [ポート（Port）] テーブルから必要なポートを選択します。ポートを UNI に使用できない場合は、[ポート（Port）] テーブルの UNI 名の横にアラート アイコンが表示され、ポートが選択できない理由が示されます。

ステップ 16 新しい UNI を作成している場合は、新しい UNI の詳細を入力します。新規 UNI の詳細は、[マルチ UNI（Multi UNI）] テーブルで現在選択されている UNI に関するものです。フィールドと属性の説明については、新規 UNI の詳細リファレンス （651 ページ）を参照してください。

ステップ 17 UNI サービスの詳細を入力します。フィールドと属性の説明については、UNI サービス詳細の参照 （652 ページ）を参照してください。[次へ（Next）] をクリックします。

ステップ 18 エンドポイントのいずれかが Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、[管理対象外（Unmanaged）] ページでその管理対象外デバイスの情報を入力します。アンマネージドエンドポイントを使用した回線/VC のプロビジョニング （778 ページ）を参照してください。

ステップ 19 これはオプションです。テンプレートに、サービスに参加するデバイス上に設定する追加の CLI コマンドを付加する場合は、[サービス テンプレート（Service Template）] ページを使用します。詳細については、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

ステップ 20 回線/VC に必要な情報をすべて入力したら、[送信（Submit）] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集（Edit Attributes）] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

ステップ 21 回線/VC が、[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに追加されているはずです。

サービス詳細の参考資料

次の表に、サービス レベルの EVC を定義する属性を示し、それらについて説明します。すべての属性がすべての EVC タイプに関連するわけではないことに注意してください。

表 *32*：サービスの詳細

属性	説明
サービス名（Service Name）	回線/VC を特定する一意の名前。
サービスの説明（Service Description）	VC を識別するのに役立つ VC の説明。
サービス タイプ（Service Type）	作成するサービスのタイプに基づいて事前に入力されています（EPL、EVPL、EP-LAN など）。
EVPN を使用（Use EVPN）	EVPN ベースのコネクションを作成できます。
サービス MTU	VC を通過するフレームの最大サイズ（バイト単位）。値は 64 ～ 65535 です。サービス MTU は、サービスのすべての UNI で定義された MTU 以下である必要があります。
コアテクノロジー	VPLS または H-VPLS。マルチポイント EVC のコア テクノロジー （607 ページ）を参照してください。 （注） VPLS または H-VPLS の場合は、プロビジョニング ウィザードを使用して最大 20 台のデバイスをプロビジョニングできます。
VPN ID	マルチポイント EVC に関連します（VPLS と H-VPLS の両方）。このフィールドには、次の使用可能な擬似回線の ID が自動的に入力されます。この ID は、EVC の作成プロセス中に変更できます（有効な値の範囲：1 ～ 4294967295）。EVC の変更時には、ID は編集できません。 （注） VPN ID はネットワーク全体で一意に使用されます。つまり、2 つのサービスで同じ VPN ID が使用されることはありません。また、擬似回線の競合を回避するため、ネットワークですでに設定されている擬似回線 ID を VPN ID に使用することはできません。VPN ID 値が [PW ID] フィールドに表示されます。サービスの作成および変更時にマルチポイント サービスの PW ID 値を変更することはできません。

属性	説明
PW ID	マルチポイント EVC およびポイントツーポイント EVC に関連します。このフィールドには、次の使用可能な擬似回線の ID が自動的に入力されます。この ID を編集し、EVC 作成プロセス時にポイントツーポイント EVC の場合にのみ値（有効値範囲：1 ～ 4294967295）を割り当てることができます。EVC の変更時には、ID は編集できません。 （注） PW ID はネットワーク全体で一意に使用されます。つまり、2 つのサービスで同じ PW ID が使用されることはありません。
バンドリング	この VC で複数の VLAN を有効にします。複数の CE-VLAN ID は、1 つの EVC にバンドルされます。
CE-VLAN ID の保持	出力サービス フレームの CE-VLAN ID が対応する入力サービス フレームの CE-VLAN ID と同じ値であることを確認します。バンドリングが有効な場合、これを有効にする必要があります。
CE-VLAN ID CoS の保持	出力サービス フレームの CE-VLAN CoS が対応する入力サービス フレームの CE-VLAN CoS と同じ値であることを確認します。CoS マーキングは変更できません。

新規 UNI の詳細リファレンス

次の表に、UNI として指定されているポートに関連する属性とその説明をリストします。すべての属性がすべての EVC タイプに関連するわけではないことに注意してください。

表 *33 :* 新規 *UNI* の詳細（*New UNI Details*）

属性	説明
[MTU]	インターフェイスを通過するパケットの最大伝送サイズ（バイト単位）。UNI の MTU は、サービス レベルで定義された MTU 以上でなければなりません。
自動ネゴシエーション（Auto Negotiation）	速度とデュプレックス モードを自動的にネゴシエートするには、このチェックボックスをオンにします。
速度	ポートの速度。ポートでサポートされている場合は、速度を下げることができます。 （注） [自動ネゴシエーション（Auto Negotiation）] チェックボックスをオンにすると、このフィールドは使用できません。

属性	説明
デュプレックス モード（Duplex Mode）	• [全二重（Full Duplex）]：UNI と顧客のアクセス スイッチ間で、どちらの側も全二重をサポートしていると仮定して、双方向の同時通信を使用します。一方の側が全二重をサポートしていない場合、ポートはダウンします。 • [自動ネゴシエーション（Auto-Negotiation）]：サポートされている内容に応じて、2つのデバイス間で合意されたモードを使用します。全二重が試行されますが、一方のデバイスがそれをサポートしていない場合、半二重が使用されます。 （注） [自動ネゴシエーション（Auto Negotiation）]チェックボックスをオンにすると、このフィールドは使用できません。
[サービス多重化（Service Multiplexing）]	UNI が複数の EVC インスタンスに参加できるようにします。
[UNI 許可バンドリング（UNI Allows Bundling）]	バンドルを有効にして、UNI が VC に参加できるようにします。バンドルについては、以下を参照してください： サービス詳細の参考資料 （650 ページ）
[タグなし CE-VLAN ID（Untagged CE-VLAN ID）]	タグなしトラフィックに割り当てられた CE-VLAN の ID。
[入力/出力 QoS プロファイル（Ingress/Egress QoS Profile）]	UNI の入力または出力トラフィックに必須の QoS プロファイルを選択します。プロファイルの一覧には、デバイスで設定され、システムによって検出されるポリシーマップおよびユーザー定義の QoS プロファイルが含まれます。
[UNI QoS プロファイル（UNI QoS Profile）]	UNI 自体の QoS プロファイルを適用して、UNI の帯域幅プロファイルおよびその他の QoS 属性を定義します。UNI レベルで QoS プロファイルを適用する場合は、サービス レベルで QoS プロファイルを適用しないでください。
[リンク OAM の有効化（Enable Link OAM）]	IEEE 803.1ah リンクの操作とメンテナンスを有効にします。リンク OAM が有効になっている場合は、この UNI と顧客のアクセス スイッチ間のリンクの状態に関連するイベントが表示されます。
[リンク管理の有効化（Enable Link Management）]	顧客アクセス スイッチがこの UNI、VLAN ID、UNI 上のサービスなどに関する情報を取得できるようにします。

UNI サービス詳細の参照

次の表に、UNI に関連する EVC の属性（EVC がこの UNI でどのように動作するか、など）の一覧と説明を示します。すべての属性がすべての EVC タイプに関連しているとは限りません。

（注） QinQ 属性については、選択したデバイスでサポートされている属性のみがウィザードに表示されます。

表 *34 : UNI* サービス詳細

属性	説明	その他の情報
入力/出力サービス QoS プロファイル（Ingress/Egress Service QoS Profile）	UNI の入力または出力トラフィックに必須の QoS プロファイルを選択します。プロファイルの一覧には、デバイスで設定され、システムによって検出されるポリシーマップおよびユーザー定義の QoS プロファイルが含まれます。 （注） リリース 4.0.0 以降では、独立した列（[Sub-Policy]）は、値 **True** を表示することによって、特定のポリシーがサブポリシーであるかどうかを示します。サブポリシーではないポリシーの場合は、関連付けられている [Sub-Policy] 列に値 **NA** が表示されます。	
レイヤ 2 制御プロトコル プロファイル（Layer 2 Control Protocol Profile）	さまざまな通信プロトコルの処理方法を決定するプロファイル。さまざまなプロトコルを使用するフレームは、トンネル化、ドロップ、またはピアリングされます。詳細については、MEF 6.1 を参照してください。	
指定	E-Tree の場合：VC の UNI のロール（リーフまたはルート）を選択します。	
ルートを指定したポイントツーポイント接続の使用（Use point to point connection with Root）	E-Tree の場合：UNI がリーフとして指定された場合、このチェックボックスを選択して、ルートとリーフ間のアクティブな疑似回線を作成できます。このチェックボックスは、単一デバイスに複数のエンドポイントが存在する場合またはサービスに複数のルートが存在する場合は表示されません。	
一致（Match）	UNI を入力するためにトラフィックに必要なタギングのタイプを選択します。 • Dot1q：サービス インスタンスへのインターフェイスの 802.1q フレーム入力のマッピング。 • Dot1ad：サービスインスタンスへのインターフェイスの 802.1ad フレーム入力のマッピング。 • デフォルト（Default）：このポートの他のどの VC にも割り当てられないトラフィック。 • タグなし（Untagged）：VLAN タグがないフレーム	Dot1AD は、15.3(3) ソフトウェア バージョンを実行している ME3600 デバイスではサポートされません。
VLAN の自動割り当て	UNI に VLAN ID を自動的に割り当てるには、このチェックボックスをオンにします。	

属性	説明	その他の情報
VLAN	VLAN ID。1 ～ 4094 の整数。ハイフンまたはカンマで区切られた一連の VLAN ID を使用して VLAN ID の範囲を入力できます。	[VLAN の自動割り当て（Auto Allocate VLAN）] チェックボックスをオンにした場合、このフィールドは使用できません。
内部 VLAN（Inner VLAN(s)）	VLAN タギングの第 2 レベルの VLAN ID。1 ～ 4094 の整数。ハイフンまたはカンマで区切られた一連の VLAN ID を使用して VLAN ID の範囲を入力できます。	
タグなしバンドル（Untagged Bundled）	VLAN タグのないトラフィックを VLAN タグ付きのフレームとともにバンドルできます。	
優先順位タグ付きバンドル（Priority Tagged Bundled）	優先順位タグ付きトラフィックを VLAN タグ付きフレームとともにバンドルできます。	
完全一致（Exact）	サービスによる伝送対象として一致していない追加の VLAN タグが付けられたトラフィックのアドミタンスを防止します。	IOS-XR デバイスにのみ適用されます。
外部 VLAN CoS（Outer VLAN CoS）	フレームに関連付ける必要がある外部 VLAN サービス クラス ID。CoS ID は、0 ～ 7 の範囲の整数です。	IOS デバイスにのみ適用されます。
内部 VLAN CoS（Inner VLAN CoS）	フレームに関連付ける必要がある内部 VLAN サービス クラス ID。CoS ID は、0 ～ 7 の範囲の整数です。	IOS デバイスにのみ適用されます。
E-Type	サービスを指定された EtherType のフレームのみ伝送するように制限します。 • IPv4 • IPv6 • PPPoE-All • PPPoE-Discovery • PPPoE-Session	IOS デバイスにのみ適用されます。

属性	説明	その他の情報
定義書き換えアクション（Rewrite Definition Action）	フレームが UNI に入ったときに実行するカプセル化調整。 • なし • ポップ（Pop）：入力のフレームから 1 個または 2 個の VLAN タグを削除し、出力で追加します。 • プッシュ（Push）：入力のフレームから 1 個または 2 個の VLAN タグ（Dot1q または Dot1ad タグ）を追加し、出力で削除します。 • 変換（Translate）：VLAN タグを新しい VLAN タグ（Dot1q または Dot1ad タグ）で置き換えます。変換は、1:1、1:2、2:1、または 2:2 です。	変換アクションは、IOS-XR デバイスにのみに適用されます。

サービス OAM

サービス レベルで、EVC のモニターリングとトラブルシューティングを可能にする EOAM（Ethernet Operations, Administration and Management）パラメータを定義できます。実際には、EVC のエンドポイント上の接続障害管理（CFM）コンポーネントを設定することになります。

ポイントツーポイント EVC では、一方向（UNI A から UNI Z へなど）または双方向で OAM パラメータを定義できます。マルチポイント EVC では、送信元と送信先の MEP グループを定義してから、EVC エンドポイントを特定の MEP グループに関連付けることができます。

CFM の詳細とデバイス レベルの CFM 設定については、EOAM の障害とパフォーマンスのモニターリングを設定する （546 ページ）を参照してください。

次のように、プロビジョニング ウィザードの [カスタマー サービスの詳細（Customer Service Details）] ページの [サービス OAM（Service OAM）] セクションを使用して、モニターするサービス フレームの仕様を定義し、そのフレームに適用する OAM プロファイルを定義します。

- [送信元（From）]：EVC を経由するトラフィック フローの送信元。
- [送信先（To）]：EVC を経由するトラフィック フローの送信先。
- [方向（Direction）]（E ツリーのみ）：リーフとルート間またはルートからルートへのトラフィック フローの方向。

（注） [送信元（From）] フィールドと [送信先（To）] フィールドに入力すると、MEP グループ、つまり、順序付けされた UNI のセットが作成されます。ウィザードの次のページで、UNI をこれらの MEP グループの 1 つに関連付けます。

- [CoS]：フレームに関連付ける必要のあるサービス クラス識別子。
- [OAM プロファイル（OAM Profile）]：パフォーマンス モニターリングを有効にするためにフレームに適用する必要のある OAM 属性のセット。次の OAM プロファイルを選択に使用できます。

- パフォーマンス モニターリング 1：コミュニティ チェックと合成損失測定を有効にします。このプロファイルは、ポイントツーポイントとマルチポイントの両方の EVC をサポートします。
- [パフォーマンス モニターリング 2（Performance Monitoring 2）]：コミュニティ チェック、合成損失測定、およびシングルエンド遅延測定を有効にします。このプロファイルは、ポイントツーポイントとマルチポイントの両方の EVC をサポートします。
- [パフォーマンス モニターリング 3（Performance Monitoring 3）]：コミュニティ チェック、合成損失測定、およびデュアルエンド遅延測定を有効にします。このプロファイルは、ポイントツーポイントとマルチポイントの両方の EVC をサポートします。
- [パフォーマンス モニターリング 3（Performance Monitoring 3）]：コミュニティ チェック、合成損失測定、およびデュアルエンド遅延測定を有効にします。このプロファイルは、フレーム サイズ 64（損失および遅延）、履歴間隔 2（遅延）および 5（損失）、集約間隔 60 をサポートします。
- [パフォーマンス モニターリング 4（Performance Monitoring 4）]：コミュニティ チェック、合成損失測定、およびデュアルエンド遅延測定を有効にします。このプロファイルは、フレーム サイズ 152（損失および遅延）、履歴間隔 10、集約間隔 300（5 分間のサンプル）をサポートします。

- [コミュニティ チェック間隔（Continuity Check Interval）]：コミュニティ チェック メッセージの間隔。

UNI としてのデバイスおよびインターフェイスの設定

ユーザー ネットワーク インターフェイス（UNI）は、サブスクライバ（カスタマー エッジ（CE））の責任とサービス プロバイダ（プロバイダ エッジ（PE））の責任とを分ける、物理的な責任分界点です。

UNI は EVC のエンドポイントの境界を定めるため、デバイスのインターフェイスを UNI として設定することは、VC プロビジョニングで不可欠の部分となります。UNI は、VC の作成時に設定できます。あるいは、VC の作成とは別の UNI を設定することもできます。設定した UNI は、VC の作成時に使用可能になります。

UNI を設定するには、次の手順に従います。

ステップ 1 新規キャリア イーサネット EVC の作成およびプロビジョニング （641 ページ）の説明に従って、プロビジョニング ウィザードにアクセスします。

ステップ 2 [テクノロジーの選択（Select Technology）] ドロップダウン リストから **Carrier Ethernet** を選択します。

ステップ 3 [サービス タイプ（Service Types）] リストから **UNI** を選択します。

ステップ 4 **Next** をクリックして [カスタマー サービスの詳細（Customer Service Details）] ページに移動します。

ステップ 5 UNI の一意の名前と説明を入力し、必要に応じて顧客を関連付けます。

ステップ 6 UNI のサービス属性を次のように定義します。

- [すべてを 1 つにバンドル（All to One Bundling）]：UNI を VC 専用にするポートベースの VC の場合。有効にすると、すべての CE-VLAN ID が 1 つの VC にバンドルされます。[すべてを 1 つにバン

ドル（All to One Bundling）] を選択すると、[多重化（Multiplexing）] と [バンドリング（Bundling）] は選択できなくなります。

- [サービス多重化（Service Multiplexing）]：UNI を複数の VC で共有する VLAN ベースの VC の場合。有効にすると、UNI を複数の EVC インスタンスに参加させることができます。
- [バンドリング（Bundling）]：UNI に複数の VLAN を使用することができます。複数 CE-VLAN ID が 1 つの EVC にバンドルされます。

ステップ 7 [展開（Deploy）] で、完了時にただちに UNI を展開するか、デバイスに展開する前に CLI のプレビューを表示するかを選択します。

ステップ 8 **Next** をクリックして [UNI の詳細（UNI Details）] 定義ページに移動します。

ステップ 9 UNI として設定するデバイスとポートを選択します。

ステップ 10 新規 UNI の詳細リファレンス （651 ページ）の説明に従って、UNI の属性を設定します。

ステップ 11 **Submit** をクリックします。完了時に回線を展開するように選択していた場合は、ジョブが作成され、必要な CLI がデバイスに展開されます。実際にデバイスに展開する前に CLI のプレビューを表示することを選択した場合、この時点でプレビューが表示されます。CLI を確認します。属性のいずれかを変更する場合は、[属性の編集（Edit Attributes）] をクリックします。それ以外の場合は、**Deploy** をクリックします。

デバイスとインターフェイスを ENNI として設定する

External Network to Network Interface（ENNI）は、各オペレータ ネットワークが別々の管理認証局の制御下にある 2 つの Metro Ethernet Network（MEN）間のインターフェイスである参照ポイントを指定します。ENNI は、サービスの特性を維持しながら、複数のオペレータ MEN 全体でのイーサネット サービスの拡張をサポートするように設計されています。

E アクセス VC をプロビジョニングする場合は、隣接するネットワーク経由でトラフィックを伝送する ENNI を定義する必要があります。ENNI の設定は VC 作成プロセスで行うことができます。または、VC 作成とは無関係に ENNI を設定できます。このような ENNI は VC 作成中に選択できます。

ENNI を設定するには、次の手順を実行します。

ステップ 1 新規キャリア イーサネット EVC の作成およびプロビジョニング （641 ページ）の説明に従って、プロビジョニング ウィザードにアクセスします。

ステップ 2 [テクノロジーの選択（Select Technology）] ドロップダウン リストから **Carrier Ethernet** を選択します。

ステップ 3 [サービス タイプ（Service Types）] リストから **ENNI** を選択します。

ステップ 4 **Next** をクリックして [カスタマー サービスの詳細（Customer Service Details）] ページに移動します。

ステップ 5 ENNI の一意の名前と説明を入力し、必要に応じて、顧客/オペレータに関連付けます。

ステップ 6 [展開（Deploy）] で、ENNI を完了時にすぐに展開するか、最初にデバイスに展開する CLI のプレビューを表示するかを選択します。

ステップ 7 **Next** をクリックして、[ENNI の詳細（ENNI Details）] 定義ページに移動します。

ステップ 8 ENNI として設定するデバイスとポートを選択します。

ステップ 9 ENNI に関する次のパラメータを定義します。

- MTU：インターフェイスを通過するパケットのバイト単位の最大伝送サイズ。ENNI の MTU は 1526 より大きくする必要があります。
- 速度：これがサポートされていれば、必要に応じて、ポートの速度を抑えることができます。

ステップ 10 **Submit** をクリックします。完了時に回線を展開するように選択していた場合は、ジョブが作成され、必要な CLI がデバイスに展開されます。実際にデバイスに展開する前に、CLI のプレビューを表示するように選択していた場合は、ここでプレビューが表示されます。CLI を確認します。属性のいずれかを変更する場合は、[属性の編集（Edit Attributes）] をクリックします。それ以外の場合は、**Deploy** をクリックします。

セグメント ルーティング

セグメント ルーティングの設定

セグメント ルーティング（SR）は、送信元ルーティングを実行するための柔軟でスケーラブルな方法です。送信元ルータは、明示的パスまたは内部ゲートウェイ プロトコル（IGP）最短パスのいずれかを選択し、パケット ヘッダー内のパスをセグメントの順序付きリストとしてエンコードします。セグメントは、ネットワークの宛先への完全なルートを形成するためにルータを組み合わせることができるサブパスを表しています。各セグメントは、新しい IGP 拡張機能を使用してネットワーク全体に配布されるセグメント識別子（SID）で識別されます。

各ルータ（ノード）と各リンク（隣接関係）には関連付けられた SID があります。ノード セグメント識別子はグローバルに一意であり、IGP で決定されたルータへの最短パスを表します。ネットワーク管理者は各ルータに予約されたブロックからノード ID を割り当てます。一方、隣接関係セグメント ID はローカルで有効なものであり、出力インターフェイスなどの隣接ルータに固有の隣接関係を表します。ルータは、ノード ID の予約済みブロック外の隣接関係識別子を自動的に生成します。MPLS ネットワークでは、セグメント識別子は MPLS ラベル スタック エントリとしてエンコードされます。セグメント ID は指定したパスに沿ってデータを移動します。ノード セグメントはマルチホップ パスを使用できますが、隣接関係セグメントはワンホップ パスです。

（注） SR ポリシー可視化オーバーレイは、サブインターフェイスではサポートされていません。

セグメント ルーティング ポリシーの作成とプロビジョニング

SR ポリシーを作成し、プロビジョニングするには、次の手順を実行します。

始める前に

SR ポリシーのプロビジョニングの前に、次の前提条件が満たされていることを確認します。

- デバイス上とルータプロトコルレベル（ISIS / OSPF）で MPLS TE が有効になっている。
- SR-TE は、traffic-eng の優先オプションとして設定されていなければならない。
- ブロックレベルとループバックインターフェイスのラベル割り当て

ステップ 1 左側のプレーンで、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 ツールバーで [デバイスグループ（Device Group）] ボタンをクリックし、マップに表示されるデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、[+] アイコンをクリックします。これにより、マップの右側に新しいペインが開き、[プロビジョニング ウィザード（Provisioning Wizard）] が表示されます。

ステップ 4 [テクノロジー（Technology）] ドロップダウン リストで **Segment Routing** を選択すると、Cisco EPN Manager は [サービス タイプ（Service Type）] 領域に関連する回線/VC タイプのリストを表示します。

ステップ 5 [サービスタイプ（Service Type）] リストで、[SR ポリシー（SR Policy）] を選択します。

ステップ 6 さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 7 **Next** をクリックして [サービスの詳細（Service Details）] ページに移動します。

ステップ 8 （オプション）ポリシーの作成対象の顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。

ステップ 9 サービスの詳細を入力します。

サービスの詳細は、[Activate] チェックボックス、[Name]、および [Description] で構成されます。[Activate] チェックボックスを使用して、ポリシーの動作ステータスを [Up] または [Down] に設定します。

ステップ 10 ポリシーの詳細を入力します。詳細については、[ポリシーの詳細（Policy Details）] のフィールドリファレンス：SR ポリシー （660 ページ）を参照してください。

ステップ 11 [自動ルートの設定（Autoroute Settings）] の詳細を入力します。詳細については、[自動ルート設定の詳細（Autoroute Settings Details）] のフィールドリファレンス：SR ポリシー （660 ページ）を参照してください。

ステップ 12 [デプロイアクション（Deployment Action）] フィールドに、ポリシー作成プロセス終了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。詳細については、プロビジョニング順序の保存とスケジュール （736 ページ）を参照してください。

ステップ 13 **Next** をクリックして、[パスおよび制約の詳細（Path and Constraint Details）] ページに移動します。

ステップ 14 [候補パス（Candidate Paths）]、[パスの詳細（Path Details）]、および [パスの制約の詳細（Path Constraint Details）] を指定します。詳細については、パスおよび制約の詳細のフィールド参照：SR ポリシー （661 ページ）を参照してください。

ステップ 15 **Next** をクリックし、[テンプレートの詳細（Template Details）] ページに移動します。テンプレートの詳細については、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

ステップ 16 [送信（Submit）] をクリックします。選択した展開アクションに応じて、関連するアクションが実行されます。つまり、設定のプレビューを選択した場合は、設定を表示できるプレビューページが表示され、その後に [展開（Deploy）] をクリックします。展開を選択した場合、設定は関連するデバイスに直接展開されます。

[ポリシーの詳細（Policy Details）] のフィールドリファレンス：SR ポリシー

次の表に、セグメント ルーティング ポリシーを作成するためのポリシーの詳細を定義する属性のリストを示し、説明します。

表 *35 : [*ポリシーの詳細（*Policy Details***）*]* セクションの参照：*SR* ポリシー**

属性	説明
ポリシー名	ポリシー名を入力します。
ヘッドエンド（Head End）	ドロップダウンリストからヘッドエンドを選択します。
カラー	カラー値の範囲は 1 ～ 4294967295 です。
エンドポイント（End Point）	ドロップダウンリストからエンドポイントを選択します。
明示的なバインド SID	明示的なバインド SID（Explicit Binding SID）の範囲は 16 ～ 1048575 です。
帯域幅（Bandwidth）	帯域幅の値の範囲は [帯域幅の単位（Bandwidth Unit）] フィールドで選択した値によって異なります。
帯域幅の単位（Bandwidth Unit）	ドロップダウンリストから値を選択します。使用可能なオプションは、[Kbps]、[Mbps]、および [Gbps] です。

（注） [帯域幅（Bandwidth）] フィールドと [帯域幅の単位（Bandwidth Unit）] フィールドは [ダイナミックとPCE（Dynamic With PCE）] パスタイプにのみ適用されます。

[自動ルート設定の詳細（Autoroute Settings Details）] のフィールドリファレンス：SR ポリシー

次の表に、セグメント ルーティング ポリシーを作成するための自動ルート設定の詳細を定義する属性のリストを示し、説明します。

表 *36 : [*自動ルート設定の詳細（***Autoroute Settings Details***）*]* セクションの参照：***SR*** ポリシー

属性	説明
自動メトリックモード（Auto Metric Mode）	ドロップダウンリストから値を選択します。使用可能なオプションは [一定（Constant）] および [相対（Relative）] です。
自動メトリック値（Auto Metric Value）	[自動メトリックモード（Auto Metric Mode）] フィールドで選択した値に応じて、自動メトリック値（Auto Metric Value）の範囲が変わります。[一定（Constant）] の場合、範囲は 1 ～ 2147483647 です。[相対（Relative）] の場合、範囲は -10 ～ 10です。
すべてのプレフィックスを許可（Allow All Prefixes）	すべての IP プレフィックスを許可する場合は、このチェックボックスをオンにします。
許可プレフィックス（Allowed Prefixes）	このフィールドは [すべてのプレフィックスを許可（Allow All Prefixes）] チェックボックスをオンにしていない場合にのみ表示されます。必要なプレフィックスをテーブルに追加します。

パスおよび制約の詳細のフィールド参照：SR ポリシー

次の表に、セグメント ルーティング ポリシーを作成するためのパス制約の詳細を定義する属性のリストを示し、説明します。

表 *37 : [*パス制約の詳細（***Path Constraint Details***）*]* セクションの参照：***SR*** ポリシー

属性	説明
候補パス（Candidate Paths）	
Path Type	SR ポリシーに必要なパスを選択します。値は、[ダイナミック（Dynamic）]、[明示的（Explicit）]、および [ダイナミックとPCE（Dynamic With PCE）] です。
設定	候補パスの設定値の範囲は 1 ～ 65535 です。
[ダイナミック（Dynamic）] および [ダイナミックとPCE（Dynamic With PCE）] パスタイプのパスの詳細：	
メトリック タイプ	必要な [メトリックタイプ（Metric Type）] を選択します。値は、[IGP]、[遅延（Latency）]、[TE]、および [ホップ数（HopCount）] です。
メトリックマージンタイプ（Metric Margin Type）	必要な [メトリックマージンタイプ（Metric Margin Type）] を選択します。値は [絶対（Absolute）] および [相対（Relative）] です。
メトリックマージン値（Metric Margin Value）	[メトリックマージン値（Metric Margin Value）] の範囲は 0 ～ 2147483647 です。

属性	説明
SID の上限（Max SID Limit）	[SIDの上限（Max SID Limit）] は 1 ～ 255 です。
[明示的（Explicit）] パスタイプのパスの詳細：	
新しいセグメントリスト（New Segment List）	新しいセグメントリストを作成する場合は、このチェックボックスをオンにします。
セグメントリスト名（Segment List Name）	このフィールドは [新しいセグメントリスト（New Segment List）] チェックボックスがオンになっている場合に表示されます。
既存のセグメントリスト（Existing Segment List）	このフィールドは [New Segment List] チェックボックスがオフになっている場合に表示されます。ドロップダウンリストからセグメントリストを選択します。
Weight	重みの範囲は 1 ～ 4294967295 です。
（注） パスの詳細を入力する場合は、[+] アイコンをクリックし、[セグメントリスト名（Segment List Name）] と [重み（Weight）] を入力して、セグメントリストに詳細を追加する必要があります。 [新しいセグメントリスト（New Segment List）] チェックボックスがオンになっている場合は、セグメントテーブルがアクティブになり編集できます。 • [+] をクリックしてセグメントを追加できます。[インデックス（Index）] の値を入力し、[デバイス（Device）]、[セグメントタイプ（Segment Type）]、および [インターフェイス（Interface）] をそれぞれのドロップダウンリストから選択します。 • セグメントを複数追加した場合は、セグメントウィンドウで上矢印または下矢印を使用して目的のキューに配置できます。 • セグメントを作成中の場合にのみ、セグメントウィンドウでセグメントを編集または削除することもできます。作成したセグメントリストは、その後変更できません。 • また、ラベルが割り当てられていないインターフェイスにラベルを割り当てることもできます。	
パスの制約の詳細（Path Constraint Details）	
アフィニティ操作（Affinity Operation）	適切なアフィニティ操作を個別に選択し、関連する詳細を指定します。値は、[いずれかを除外する（Exclude-Any）]、[いずれかを含める（Include-Any）]、および [すべて含める（Include-All）] です。

属性	説明
いずれかのアフィニティ名を除外する（Exclude Any Affinity Names）	ドロップダウンリストから名前を選択します。
いずれかのアフィニティ名を含める（Include Any Affinity Names）	このフィールドは[いずれかを含める（Include-Any）]が選択されている場合に表示されます。ドロップダウンリストから、追加するアフィニティ名を選択します。
すべてのアフィニティ名を含める（Include All Affinity Names）	このフィールドは[すべて含める（Include-All）]が選択されている場合に表示されます。ドロップダウンリストから、追加するアフィニティ名を選択します。
SID アルゴリズム（SID Algorithm）	[SIDアルゴリズム（SID Algorithm）] の範囲は 128 ～ 255 です。
ディスジョイントグループのタイプ（Disjoint Group Type）	ドロップダウンリストから値を選択します。値は、[リンク（Link）]、[ノード（Node）]、[Srlg]、および [Srlg-Node]です。
ディスジョイントグループ ID（Disjoint Group Id）	[グループIDの分離（Disjoint Group Id）] の範囲は 1 ～ 65535 です。
ディスジョイントサブグループ ID（Disjoint Sub Group Id）	[ディスジョイントサブグループID（Disjoint Sub Group Id）] の範囲は 1 ～ 65535 です。

セグメント ルーティング ポリシーを使用したキャリア イーサネット サービスの作成とプロビジョニング

Cisco EPN Manager は、セグメント ルーティング トラフィック エンジニアリング（SR-TE）ポリシーを使用して、EPL のプロビジョニング、EVPL、アクセス EPL、アクセス EVPL キャリア イーサネットのポイントツーポイント サービスをサポートしています。CE サービスの変更時に SR-TE ポリシーを変更できます。回線/VC 360* の [関連回線/VC（Related Circuits/VC）] タブを使用して、このサービスに関連付けられた SR ポリシーを表示できます。SR ポリシーの場合、バックアップパスの可視化はオーバーレイで使用できます。[バックアップパスの表示（Show Backup Path）] を展開し、除外するノードまたはリンクを選択できます。[適用（Apply）] をクリックすると、新しいバックアップパスが表示されます。

SR ポリシーを使用して EVPL サービスを作成およびプロビジョニングするには、次の手順を実行します。

ステップ 1 左側のプレーンで、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 ツールバーで [デバイス グループ（Device Group）] ボタンをクリックし、マップに表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、[+] アイコンをクリックします。これにより、マップの右側に新しいペインが開き、[プロビジョニング ウィザード（Provisioning Wizard）] が表示されます。

ステップ 4 [テクノロジー（Technology）] ドロップダウン リストで **Carrier Ethernet** を選択すると、Cisco EPN Manager は [サービス タイプ（Service Type）] 領域に関連する回線/VC タイプのリストを表示します。たとえば、キャリア イーサネット サービス タイプには EPL、EVPL、EP-LAN などが含まれます。

ステップ 5 [サービス タイプ（Service Type）] リストから、作成する回線/VC のタイプを選択します。たとえば、EVPL などです。

ステップ 6 さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 7 **Next** をクリックして [サービスの詳細（Service Details）] ページに移動します。

ステップ 8 （オプション）EVPL の作成対象顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。

ステップ 9 サービスの詳細を入力します。フィールドと属性の説明については、サービス詳細の参考資料 （650 ページ）を参照してください。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [展開アクション（Deployment Action）] フィールドに、EVPL 作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。詳細については、プロビジョニング順序の保存とスケジュール （736 ページ）を参照してください。

ステップ 12 **Next** をクリックして UNI を定義するページに移動します。E-Access の場合、ENNI を定義するページもあります。

ステップ 13 UNI として機能するデバイスとインターフェイスを識別します。

（注） エンドポイントのいずれかが、Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、[管理対象外（Unmanaged）] チェックボックスをオンにして、その管理対象外デバイスの情報を入力します。アンマネージド エンドポイントを使用した回線/VC のプロビジョニング （778 ページ）を参照してください。

ステップ 14 新しい UNI を作成している場合は、新しい UNI の詳細を入力します。フィールドと属性の説明については、新規 UNI の詳細リファレンス （651 ページ）を参照してください。

ステップ 15 UNI サービスの詳細を入力します。フィールドと属性の説明については、UNI サービス詳細の参照 （652 ページ）を参照してください。

ステップ 16 エンドポイントのいずれかが、Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、[管理対象外（Unmanaged）] チェックボックスをオンにして、その管理対象外デバイスの情報を入力します。詳細については、アンマネージド エンドポイントを使用した回線/VC のプロビジョニング （778 ページ）を参照してください。

ステップ 17 H-VPLS をコア テクノロジーとして使用する E-LAN EVC および E-TREE EVC の場合、プライマリ ハブとセカンダリ ハブとして機能するデバイスをそれぞれ選択します。

ステップ 18 E 回線 EVC、E アクセス EVC の場合：[疑似回線の設定（Pseudowire Settings）] ページで、次のようにして EVC が経由するセグメント ルーティングの SR-TE ポリシーを選択できます。

1. [静的優先パス（Static Preferred Path）] チェックボックスをオンにして、サービスの静的ルートを割り当てます。

   （注） E アクセスの場合、このチェックボックスは表示されません。

2. [SR ポリシー（SR Policy）] オプション ボタンをクリックします。
3. [優先パス（A-Z）（Preferred Path (A-Z)）] および [優先パス（Z-A）（Preferred Path (Z-A)）] ドロップダウン リストのそれぞれから SR-TE ポリシーを選択します。

   （注） [優先パス（A ～ Z）（Preferred Path (A-Z)）] と [優先パス（Z ～ A）（Preferred Path (Z-A)）] はどちらもオプションのフィールドです。

4. 新規キャリア イーサネット EVC の作成およびプロビジョニング （641 ページ） でステップ 5 ～ 8 を繰り返します。

ステップ 19 新規キャリア イーサネット EVC の作成およびプロビジョニング （641 ページ） でステップ 20 ～ 22 を繰り返します。

光/DWDM ネットワークの回線のプロビジョニング

Cisco EPN Manager 光/DWDM ネットワーク プロビジョニング サポートの概要

Cisco EPN Manager は、高密度波長分割多重（DWDM）光チャネル（OCH）の回線タイプのプロビジョニングをサポートします。DWDM の光技術は、既存の光ファイバ バックボーン上の帯域幅を広げるために使用されます。これは同じ光ファイバ上で異なる波長の複数の信号を同時に結合して送信します。実際には、1 つの光ファイバが複数の仮想光ファイバに変換されます。

Cisco EPN Manager は、次の光回線をサポートします。

- 高密度波長分割多重（DWDM）光チャネルの（OCH）回線：以下は、光チャネルのさまざまな回線タイプです。
  - 光チャネル ネットワーク接続（OCHNC）WSON：OCHNC WSON 回線は、指定された C バンド波長で 2 つの光ノード間の接続を確立します。詳細については、Optical Channel Network Connection（OCHNC）WSON （613 ページ）を参照してください。
  - 光チャネル クライアント接続（OCHCC）WSON：OCHCC WSON 回線は、OCHNC WSON を拡張して、送信元クライアント ポートから TXP/MXP カードの接続先クライアント ポートへの光接続を作成します。詳細については、光チャネル クライアント接続（OCHCC）WSON （613 ページ）を参照してください。
  - 光チャネル（OCH）トレール WSON：OCH トレール WSON 回線は、OCHCC WSON 回線を伝送します。詳細については、光チャネル（OCH）トレイル WSON（614 ページ）を参照してください。
  - NCS 1002、NCS 55xx、および ASR 9K デバイスを接続する光チャネル（OCH）トレール：この OCH トレール回線は、NCS 1002、NCS 55xx、または ASR 9K デバイスの送信元トランク ポートから別の同様なデバイスの宛先トランク ポートへの光接続を作成します。詳細については、NCS 1002、NCS 55xx、および ASR 9K デバイスを接続する光チャネル（OCH）トレール （615 ページ）を参照してください。
  - 光チャネル（OCH）トレールのユーザー/ネットワーク間インターフェイス（UNI）：OCH トレールの UNI 回線は、Cisco NCS 2000 シリーズのデバイスと Cisco NCS 4000 シリーズのデバイス間の接続を確立します。詳細については、光チャネル（OCH）トレールのユーザー/ネットワーク間インターフェイス（UNI） （616ページ）を参照してください。
  - スペクトラム スイッチド光ネットワーク（SSON）：SSON 回線を使用すると、スパン内のより多くのチャンネルを表示できます。SSON 機能を使用すると、回線をメディア チャネル グループ内に作成した場合に、回線が互いに近くに配置されます。詳細については、Spectrum Switched Optical Network（SSON）回線 （617ページ）を参照してください。
- 光トランスポート ネットワーク（OTN）：OTN 回線は、Resource Reservation Protocol（RSVP）シグナリングを使用して、イングレスとイーグレスのノード間に静的または動

的に確立できます。詳細については、光トランスポート ネットワーク（OTN）回線（618 ページ）を参照してください。

- 光チャネルデータユニットユーザー/ネットワーク間インターフェイス（ODU UNI）：ODU UNI 回線は、OTN アーキテクチャを経由する実際のエンドツーエンドのクライアント サービスを表します。詳細については、光チャネル データ ユニットのユーザー/ネットワーク間インターフェイス（ODU UNI）（618 ページ）を参照してください。
- 光チャネル データ ユニット（ODU）トンネル：ODU トンネル回線は、ODU UNI を伝送します。詳細については、光チャネル データ ユニット（ODU）トンネル（619 ページ）を参照してください。
- 光チャネル データ ユニット（ODU）を介した光チャネル ペイロード ユニット（OPU）：ODU を介した OPU 回線は、2 つの顧客指定宅内間の高帯域幅のポイントツーポイント接続を提供します。これらの回線は、ODU UNI 回線を使用して、ネットワーク経由でクライアント信号を伝送します。詳細については、Optical Channel Payload Unit（OPU）Over Optical Channel Data Unit（ODU）（619 ページ）を参照してください。
- 光チャネルデータユニットのユーザー/ネットワーク インターフェイス（ODU UNI）ヘアピン：ODU UNI ヘアピン回線は ODU UNI 回線に似ていますが、管理プレーンで作成され、送信元と宛先は同じデバイスですが、インターフェイスが異なる内部ノード回線です。詳細については、光チャネル データ ユニットのユーザー/ネットワーク間インターフェイス（ODU UNI）ヘアピン（620 ページ）を参照してください。
- 光チャネルデータユニット（ODU）：光チャネルデータユニット（ODU）は、OTU コントローラのサブコントローラとして作成されます。ODU には、光チャネルをサポートするメンテナンス機能と操作機能の情報が含まれています。詳細については、光チャネル データ ユニット（ODU）（620 ページ）を参照してください。

光回線のプロビジョニングの前提条件

以下は光回線をプロビジョニングするための前提条件です。

- Cisco EPN Manager は、Wavelength Switched Optical Network（WSON）回線と非 WSON 回線の両方をサポートします。ただし、非 WSON 回線については、Cisco EPN Manager は、回線オーバーレイ、回線 360 度ビュー、マルチレイヤ トレース ビュー、および回線の詳細が含まれる回線検出のみをサポートします。Cisco EPN Manager は、非 WSON 回線のプロビジョニング、有効化、非アクティブ化、保護スイッチ アクション、および変更をサポートしません。
- デバイス間の通信は、光回線をプロビジョニングする前にセットアップする必要があります。
- 光回線をプロビジョニングするデバイスのインベントリ収集の状態は[完了（Completed）]である必要があります。これを確認するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** に移動し、

[最後のインベントリ収集ステータス（Last Inventory Collection Status）] 列でステータスを確認します。

- DWDM グリッド ユニットは、波長または周波数に設定する必要があります。これには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [回線/VC 表示（Circuits/VCs Display）]** を選択し、、[DWDM グリッド単位（DWDM Grid Unit）] エリアで [波長（ナノメートル（nm））（Wavelength (Nanometer (nm))）] または [周波数（テラヘルツ（THz））（Frequency (Terahertz (THz))）] を選択します。
- ソフトウェア バージョン 10.7 以降で動作している NCS 2000 シリーズのデバイスを使用して OCHNC またはメディア チャネル NC 回線をプロビジョニングする前に、シスコのトランスポート コントローラ（CTC）または Cisco EPN Manager のいずれかで UNI 設定を必ず作成してください。
- 必要に応じて、システムに顧客を作成し、回線/VC の作成およびプロビジョニング プロセス中に顧客に回線/VC を関連付けられるようにする必要があります。左のサイドバーから **[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customers）]** を選択して、顧客を作成および管理します。
- NC57-18DD-SE カードの場合、次のコマンド形式を使用して、ポート 0 ー 17 および 24 ー 29 を 400G モードで再利用します。

  hw-module port-range <start port> <end port> location <loc> mode <port_mode>

  例：**hw-module port-range 8 9 location 0/1/CPU0 mode 400**

OCH 回線の作成とプロビジョニング

OCH 回線をプロビジョニングするには、次の手順を実行します。

始める前に

オプティカル回線をプロビジョニングする前の前提条件については、光回線のプロビジョニングの前提条件 （667 ページ）を参照してください。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] をクリックして、OCH 回線を作成する場所を選択します。

ステップ 3 [デバイスグループ（Device Groups）] ポップアップウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [回線/VC（Circuits/VCs）] タブをクリックし、[回線/VC（Circuits/VCs）] ペイン ツールバーで [+]（[作成（Create）]）アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。

（プロビジョニングウィザードを表示するもう 1 つの方法として、**[設定（Configuration）]**>**[ネットワーク（Network）]** > **[サービスプロビジョニング（Service Provisioning）]** の順に選択する方法があります。）

ステップ 6 [テクノロジー（Technology）] ドロップダウン リストから [光（Optical）] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ（Service Type）] 領域に表示します。たとえば、OCH 回線の [光（Optical）] サービスタイプには、[OCHNC]、[OCHCC]、[OCH-Trail]、[OCHNC WSON]、[OCHCC WSON]、[OCH-Trail WSON]、および [OCH-Trail UNI] があります。

ステップ 7 [サービス タイプ（Service Type）] エリアで、作成する OCH 回線のタイプを選択します。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [顧客セクション（Customer Section）] ページに移動します。

ステップ 10 （オプション）回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）]** > **[その他（Other）]** > **[顧客（Customers）]** の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。

ステップ 11 [顧客セクション（Customer Section）] ページに回線名とその説明を入力します。

ステップ 12 [次へ（Next）] をクリックして [回線セクション（Circuit Section）] ページに移動します。

（注） 光サービスタイプとして OCH-Trail UNI を選択すると、[エンドポイントセクション（Endpoint Section）] ページが最初に表示され、その後 [回線セクション（Circuit Section）] ページが表示されます。

ステップ 13 回線の詳細を入力します。フィールドと属性の説明については、OCH 回線タイプの [回線（Circuit）] セクション リファレンス （671 ページ） を参照してください。

ステップ 14 [次へ（Next）] をクリックして [エンドポイント セクション（Endpoint Section）] ページに移動します。

ステップ 15 [帯域幅（Bandwidth）] ドロップダウンリストから帯域幅を選択します。

ステップ 16 [エンドポイント（Endpoint）]テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名（Device Name）] 列に読み込まれます。[エンドポイント（Endpoint）] テーブルの行をクリックして、[デバイス名（Device Name）]、[終端ポイント（Termination Point）]、[ポートの追加/ドロップ（Add/Drop Port）]、[OCH トレール（OCH-Trail）]、および[サイド（Side）] の各列を編集することもできます。[サイド（Side）]列は、選択したポートに基づいて自動的に設定されます。選択した回線タイプと互換性があり、使用可能なネットワーク要素だけが表示されます。

同じ FEC モードのエンドポイントを選択します。異なる FEC モードのエンドポイントを選択すると、エラーメッセージが表示されます。

（注） [ポートの追加（Add Port）] 列と [ポートのドロップ（Drop Port）] 列は、OCHNC WSON 回線の場合にのみ使用可能です。[ポートの追加（Add Port）]列に追加する必要があるポートを選択すると、[ポートのドロップ（Drop Port）]列と [サイド（Side）]列の値が自動的に設定されます。また、[ポートのドロップ（Drop Port）] 列の値を手動で編集することもできます。

ステップ 17 OCH 回線のトレールの多様性を選択します。作成する OCH 回線と選択するトレールは異なります。

（注） 作成したトレールの多様性を変更または削除することはできません。

OCHNC 回線では、[PSMのダイバーシティ（Diversity for PSM）] チェックボックスをオンにして、ダイバーシティを追加します。

ステップ 18 [次へ（Next）] をクリックして [制約セクション（Constraints Section）] ページに進みます。

ステップ 19 マップでデバイス ノードまたはリンクをクリックし、[制約（Constraints）] テーブルに追加します。あるいは、テーブルツールバーで [+] ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名（Node/Link Name）]、[包含/除外（Include/Exclude）]、および [ルート（Route）] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。

（注） 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約（Constraints）] テーブルの列にデータを読み込むことはできません。OCHCC トレール WSON 回線には、次のルートの制約条件が適用されます。

- 変更されたルートの制約事項は、すぐには回線に適用されませんが、再ルーティングが必要になる場合があります。ただし、変更は次回のルート操作または復元時に適用されます。
- [回線オーバーレイ（Circuit Overlay）] には現在のルートに適用可能な制約事項のみが表示され、**回線の編集**ウィザードには現在設定されている制約事項が表示されます。
- **回線の編集**ウィザードには、回線オーバーレイを使用して表示される制約事項アイコンとは異なる制約事項を表示する制約事項テーブルが含まれています。
- 回線の変更中に、ドロップダウンリストから **[アクションの再ルーティング（Reroute Actions）]** を選択できます。リストから [なし（None）]、[動作パス（Working Path）]、または [保護パス（Protection path）] を選択できます。
- 関連する OTS リンクを作業パスに含めたり除外したりするには、ソース リンク ターミネーション ポイントを選択し、光学次数を制約として OTS リンク ターミネーション ポイントを選択します。たとえば、3 つのノード（A、B、および C）がすべて接続されており、回線の送信元ノードと宛先ノードがそれぞれ A と B である 3 ノードトポロジについて考えてみます。B と C を接続する作業パスリンクを含める場合は、制約を選択するときに、C に接続する光学次数とともにリストされているリンク ターミネーション ポイントを選択します。たとえば、ノード B の光学次数 1 を使用して C を接続する場合、制約として B-1 を選択します。このシナリオは、作業パスにリンクを含めるか除外する場合に適用できます。

ステップ 20 [次へ（Next）] をクリックして [異種波長セクション（Alien Wavelength Section）] ページに移動します。送信元ノードと宛先ノードのカード、トランクモード、FEC モードなどの現在の異種波長の設定が表示されます。送信元ノードと宛先ノードの異種波長に新しい設定を作成できます。

（注） [異種波長セクション（Alien Wavelength Section）] は、OCHNC WSON 回線を作成する場合にのみ使用できます。

ステップ 21 [今すぐ作成（Create Now）] をクリックして回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー（Preview）] をクリックするとプレビューが表示されます。設定をデバイスに展開するかキャンセルするかを選択できますが、 属性を編集することはできません。

（注） 「回線のアクティブ化を検証できません。タイムアウトの期限が切れました（Cannot validate the activation of the circuit. Time out expired）」というエラーメッセージを受信した場合、デバイスがコントロールプレーンの回路をアクティブにするのに時間がかかっていることを意味します。EPNM では回線が欠落した状態になります。EPNM で削除しても、ネットワーク上の回線は削除されません。回線を [動作中（UP）] として表示し、EPNM で検出する必要がある場合は、EPNM からのデバイスの完全同期を実行する必要があります。EPNM から再度作成できるように、CTC から削除する必要があります。

ステップ 22 [ネットワークトポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

（注） OCH-Trail のみが作成された場合、[回線/VC 360（Circuit/VC 360）] の [関連する回線（Related Circuits）] タブにはデータが表示されません。OCHCC が作成されると、OCH-Trail も作成されます。これらの回線の場合、[関連する回線（Related Circuits）] タブで、OCHCC-WSON には OCH-Trail WSON が含まれ、OCH-Trail WSON には OCHCC-WSON が含まれます。

OCH 回線タイプの [回線（Circuit）] セクション リファレンス

次の表に、OCH 回線タイプを定義する属性とその説明をリストします。

表 *38 : [*回線（*Circuit*）*]*セクション リファレンス：*OCH* 回線タイプ

属性	説明	有効
[回線詳細（Circuit Details）]		
ラベル（Label）	回線を識別する一意の名前。	
状態	回線の管理状態。値は次のとおりです。 • [サービス中（In Service）]：回線はサービス中で、トラフィックを伝送できます。 • [サービス停止中（Out of Service）]：回線が停止し、トラフィックを伝送できません。	すべての OCH 回線タイプ。
双方向	双方向回線を作成するには、このチェックボックスをオンにします。	OCHCC WSON および OCH Trail WSON 回線タイプ。
[アクティベーションの待機（Wait For Activation）]	回線アクティベーションの設定時間を待機するには、このチェックボックスをオンにします。	OCHCC WSON および OCH Trail WSON 回線タイプ。

属性	説明	有効
Protection	回線の保護機構。Cisco EPN Manager は、選択した回線タイプに基づいて、次の保護メカニズムをサポートします。 • [なし（None）]：保護されていない回線の場合、この値はすべての OCH 回線タイプに使用できます。 • [PSM]：保護スイッチモジュール（PSM）カードが TXP カードに接続されている場合。この値は、回線タイプが OCHNC WSON または OCHCC WSON であるときに使用できます。 • [Y 字型ケーブル（Y-Cable）]：トランスポンダまたはマックスポンダ カードが回線を保護する場合。この値は回線タイプが OCHCC WSON であるときに使用できます。 • [スプリッタ（Splitter）]：MXPP/TXPP カードが使用されている場合。回線の送信元と宛先は、MXPP_MR_2.5G カードおよび TXPP_MR_2.5G カード上にあります。これらのカードは、スプリッタ（回線レベル）の保護（通常は TXPP または MXPP トランスポンダカード上のトランク保護）を提供します。この値は回線タイプが OCHCC WSON であるときにのみ使用できます。	OCHNC WSON 回線タイプ。
[ルート プロパティ（Route Properties）]		
[トンネルと異なる（Diverse From Tunnel）]	トンネルを選択し、プロビジョニングする回線でそのトンネルが使用されないことを確認します。これにより、トンネルに障害がある場合に、同じトンネルが他の回線で使用されなくなります。	[相互ダイバーシティ（Mutual Diversity）] チェックボックスがオフの場合の OCH-Trail UNI 回線タイプ。
検証	回線の検証モード。値は次のとおりです。 • [フル（Full）]：回線の検証結果が承認しきい値以上になると回線が作成されます。 • [なし（None）]：承認しきい値を考慮せずに回線が作成されます。	すべての OCH 回線タイプ。

属性	説明	有効
[承認しきい値（Acceptance Threshold）]	OCH 保護回線に設定された保護承認しきい値。値は次のとおりです。 • [緑（Green）]：復元失敗の危険性が 0 % であることを示します。 • [黄（Yellow）]：復元失敗の危険性が 0 % ～ 16 % の間であることを示します。 • [オレンジ（Orange）]：復元失敗の危険性が 16 % ～ 50 % の間であることを示します。 • [赤（Red）]：復元失敗の危険性が 50 % を超えていることを示します。	[検証（Validation）] フィールドが [フル（Full）] に設定されている場合のすべての OCH 回線タイプ。
[保護の承認しきい値（Protect Acceptance Threshold）]	OCH 保護回線に設定された保護承認しきい値。値は次のとおりです。 • [緑（Green）]：復元失敗の危険性が 0 % であることを示します。 • [黄（Yellow）]：復元失敗の危険性が 0 % ～ 16 % の間であることを示します。 • [オレンジ（Orange）]：復元失敗の危険性が 16 % ～ 50 % の間であることを示します。 • [赤（Red）]：復元失敗の危険性が 50 % を超えていることを示します。	次の場合の OCHNC WSON 回線タイプ: • [保護（Protection）] フィールドが [PSM]、[Y 字型ケーブル（Y-Cable）]、または [スプリッタ（Splitter）] に設定されている。 • [検証（Validation）] フィールドが [フル（Full）] に設定されている。
[パス アラームを無視（Ignore Path Alarms）]	パス アラームを無視するには、このチェックボックスをオンにします。	OCHCC WSON、OCHNC WSON、および OCH-Trail WSON 回線タイプ。
[再生成を許可（Allow Regeneration）]	ネットワーク要素が信号を再生成できるようにするには、このチェックボックスをオンにします。	すべての OCH 回線タイプ。

属性	説明	有効
[ソーク時間（Soak Time）]	障害が修正された後、元のパスに切り替わるまでに、復元されたパス上の回線が待機する期間。	[元に戻す（Revert）] が [手動（Manual）] または [自動（Automatic）] に設定されている場合の OCHCC WSON、OCHNC WSON、および OCH-Trail WSON 回線タイプ。
[復元（Restoration）]	障害が発生した OCH 回線を新しいルートに復元するには、このチェックボックスをオンにします。	すべての OCH 回線タイプ。
復元頻度	[優先（Preferred）] または [必須（Required）] オプションボタンをオンにして、周波数タイプを選択します。	[復元（Restoration）] チェックボックスがオンの場合の OCH-Trail 回線タイプ。
[プライオリティ（Priority）]	障害が発生した OCH 回線の復元操作に優先順位を付けます。値は [高（High）]、[プライオリティ 1（Priority 1）]、[プライオリティ 2（Priority 2）]、[プライオリティ 3（Priority 3）]、[プライオリティ 4（Priority 4）]、[プライオリティ 5（Priority 5）]、[プライオリティ 6（Priority 6）]、および [低（Low）] です。	[復元（Restoration）] チェックボックスがオンの場合のすべての OCH 回線タイプ。
[復元の検証（Restoration Validation）]	復元操作の検証モード。値は次のとおりです。 • [なし（None）]：復元の承認しきい値を考慮せずに回線が作成されます。 • [継承（Inherited）]：復元される回線は、プライマリ回線から検証と承認のしきい値を継承します。 • [フル（Full）]：復元の検証結果が復元の承認しきい値以上になると回線が作成されます。	[復元（Restoration）] チェックボックスがオンの場合のすべての OCH 回線タイプ。

属性	説明	有効
[復元の承認しきい値（Restoration Acceptance Threshold）]	OCH 回線の復元操作に設定された承認しきい値。値は次のとおりです。 • [緑（Green）]：復元失敗の危険性が 0 % であることを示します。 • [黄（Yellow）]：復元失敗の危険性が 0 % ～ 16 % の間であることを示します。 • [オレンジ（Orange）]：復元失敗の危険性が 16 % ～ 50 % の間であることを示します。 • [赤（Red）]：復元失敗の危険性が 50 % を超えていることを示します。	次の場合のすべての OCH 回線タイプ： • [復元（Restoration）] チェックボックスがオンになっている。 • [復元検証（Restoration Validation）] フィールドが [フル（Full）] に設定されている。
[復元保護の承認しきい値（Restoration Protect Acceptance Threshold）]	OCH 回線の復元操作に設定された保護の承認しきい値。値は次のとおりです。 • [緑（Green）]：復元失敗の危険性が 0 % であることを示します。 • [黄（Yellow）]：復元失敗の危険性が 0 % ～ 16 % の間であることを示します。 • [オレンジ（Orange）]：復元失敗の危険性が 16 % ～ 50 % の間であることを示します。 • [赤（Red）]：復元失敗の危険性が 50 % を超えていることを示します。	次の場合の OCHNC WSON 回線タイプ: • [保護（Protection）] フィールドが [PSM]、[Y 字型ケーブル（Y-Cable）]、または [スプリッタ（Splitter）] に設定されている。 • [復元（Restoration）] チェックボックスがオンになっている。 • [復元検証（Restoration Validation）] フィールドが [フル（Full）] に設定されている。

属性	説明	有効
[復元ソーク時間（Restoration Soak Time）]	障害アラームの発生後、新しいパスに復元されるまでに、オプティカルパス上の回線が待機する期間。 デフォルトの復元ソーク時間は 2 分です。	[復元（Restoration）] が選択されている場合の OCH-Trail および OCH-NC。
[元に戻す（Revert）]	障害が修正された後、復元されたパスから元のパスに回線を戻します。値は [なし（None）]、[手動（Manual）]、および [自動（Automatic）] です。	[復元（Restoration）] チェックボックスがオンになっている場合の OCHCC WSON、OCHNC WSON、OCH-Trail、および OCH-Trail WSON 回線タイプ。
[元に戻すソーク時間（Revert Soak Time）]	障害が修正された後、元のパスに戻すまでに、オプティカルパス上の回線が待機する期間。 デフォルトの元に戻すソーク時間は 1 分です。	[元に戻す（Revert）] が [自動（Automatic）] に設定されている場合の OCH-Trail および OCH-NC。
[管理状態（Admin State）]	回線の管理状態として [アップ（Up）] または [ダウン（Down）] を選択します。これは、回線の動作可能性に影響を及ぼし、回線を有効化するか無効化するかが決定されます。	OCH-Trail UNI 回線タイプ。
光プロパティ（Optical Properties）		
グリッドタイプ	ドロップダウンリストから必要なグリッドタイプを選択します。**[フレックス 6.25 GHz（Flex 6.25 GHz）]**、**[固定 50 GHz（Fixed 50 GHz）]**、**[フレックス 100 MHz（Flex 100 MHz）]**、**[固定 75 GHz（Fixed 75 GHz）]** から選択できます	OCH-Trail 回線タイプ。
波長（nm）/周波数（THz）	ドロップダウンリストから波長を選択します。	OCH-Trail 回線タイプ。
主周波数	[優先（Preferred）] または [必須（Required）] オプションボタンをオンにして、周波数タイプを選択します。	OCH-Trail 回線タイプ。
[優先波長プロパティ（Preferred Wavelength Properties）]		

属性	説明	有効
[波長オプション（Wavelength Options）]	回線の波長オプション。値は [設定しない（Do Not Set）]、[デフォルトに設定（Set To Default）]、および [優先波長を設定（Set Preferred Wavelength）] です。	OCH-Trail UNI 回線タイプ。
[作業ポートのプロパティ（Work Port Properties）]		
[自動プロビジョニング（Auto Provisioning）]	自動プロビジョニング機能を有効にするには、このチェックボックスをオンにします。	すべての OCH 回線タイプ
[C バンド（C Band）]	回線をプロビジョニングするための従来の波長ウィンドウ。値は次のとおりです。 • [奇数（Odd）] : ITU グリッドの奇数位置。 • [偶数（Even）] : ITU グリッドの偶数位置。	• [自動プロビジョニング（Restoration）] チェックボックスがオンになっている場合のすべての OCHCC WSON、OCHNC WSON、および OCH-Trail WSON 回線タイプ。 • [波長オプション（Wavelength Options）] が [優先波長を設定（Set Preferred Wavelength）] に設定されている場合の OCH-Trail UNI 回線タイプ。

属性	説明	有効
[波長/周波数（Wavelength/Frequency）]	回線の波長または周波数。この値は、選択したCバンドに適用されます。 （注） DWDM グリッド単位を波長または周波数に設定する必要があります。これには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [回線/VC 表示（Circuits/VCs Display）]** を選択し、、[DWDM グリッド単位（DWDM Grid Unit）] エリアで **[波長（ナノメートル（nm））（Wavelength (Nanometer (nm))）]** または **[周波数（テラヘルツ（THz））（Frequency (Terahertz (THz))）]** を選択します。	[C バンド（C Band）] フィールドが [奇数（Odd）] または [偶数（Even）] に設定されている場合のすべての OCH 回線タイプ。
[優先/必須（Preferred/Required）]	[C バンド（C Band）] フィールドと [波長/周波数（Wavelength/Frequency）] フィールドで設定した値が、回線をプロビジョニングするときに優先される値であるか必須の値であるかを決定するために選択します。	[自動プロビジョニング（Auto Provisioning）] チェックボックスがオフの場合のすべての OCH 回線タイプ。
[保護ポートのプロパティ（Protect Port Properties）]		
[作業ポートからコピー（Copy from Work Port）]	[作業ポートのプロパティ（Work Port Properties）] セクションで設定した値をコピーするには、このチェックボックスをオンにします。	[保護（Protection）] フィールドが [PSM]、[Y 字型ケーブル（Y-Cable）]、または [スプリッタ（Splitter）] に設定されている場合のすべての OCH 回線タイプ。

（注） EPNM は、OCH-Trail の作成中に従来の回線の色を検証するために、次のパラメータをサポートしています。

- AmpliGainRange
- ChPwr
- ゲイン
- Tilt
- WkgMode - OpticalAmplificationSettings tableVoaAttenuation
- Attenuator - OpticalTransportSettings table

これらのポートパラメータがデバイスで変更された場合、リアクティブインベントリはトリガーされません。EPNM でパラメータを更新するには、同期操作をトリガーする必要があります。

IOS-XR プラットフォームベースのデバイスを直接接続する OCH トレール回線の作成とプロビジョニング

IOS-XR プラットフォームベースのデバイスを直接接続する OCH トレール回線を作成およびプロビジョニングするには、次の手順を実行します。

始める前に

光回線をプロビジョニングする前に満たす必要がある前提条件については、光回線のプロビジョニングの前提条件 （667 ページ）を参照してください。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックして、OCH 回線を作成する場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [回線/VC（Circuits/VCs）] タブをクリックし、[回線/VC（Circuits/VCs）] ペイン ツールバーで [+]（[作成（Create）]）アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。

プロビジョニング ウィザードを表示するもう 1 つの方法として、**[設定（Configuration）] > [ネットワーク（Network）] > [サービス プロビジョニング（Service Provisioning）]** の順に選択する方法があります。

ステップ 6 [テクノロジー（Technology）] ドロップダウン リストから [光（Optical）] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ（Service Type）] 領域に表示します。たとえ

ば、OCH 回線の [光（Optical）] サービス タイプには、[OCHNC WSON]、[OCHCC WSON]、[OCH-Trail WSON]、および [OCH-Trail UNI] があります。

ステップ 7 [サービス タイプ（Service Type）] エリアで、作成する OCH 回線のタイプを選択します。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [顧客セクション（Customer Section）] ページに移動します。

ステップ 10 （オプション）回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customers）]** の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。

ステップ 11 [顧客セクション（Customer Section）] ページに回線名とその説明を入力します。

ステップ 12 [次へ（Next）] をクリックして [回線セクション（Circuit Section）] ページに移動します。

（注） 光サービス タイプとして OCH-Trail UNI を選択すると、[エンドポイント セクション（Endpoint Section）] ページが最初に表示され、その後 [回線セクション（Circuit Section）] ページが表示されます。

ステップ 13 回線の詳細を入力します。フィールドと属性の説明については、OCH 回線タイプの [回線（Circuit）] セクション リファレンス （671 ページ） を参照してください。

ステップ 14 [次へ（Next）] をクリックして [エンドポイント セクション（Endpoint Section）] ページに移動します。

ステップ 15 [エンドポイント（Endpoint）]テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名（Device Name）] 列に読み込まれます。あるいは、[エンドポイント（Endpoint）]テーブルの行をクリックして、[デバイス名（Device Name）]、[終端ポイント（Termination Point）]、[ポートの追加/ドロップ（Add/Drop Port）]、[OCH トレール（OCH-Trail）]、および [サイド（Side）] の各列を編集できます。[サイド（Side）] 列は、選択したポートに基づいて自動的に設定されます。選択した回線タイプと互換性があり、使用可能なネットワーク要素だけが表示されます。

（注） [ポートの追加（Add Port）] 列と [ポートのドロップ（Drop Port）] 列は、OCHNC WSON 回線の場合にのみ使用可能です。[ポートの追加（Add Port）] 列に追加する必要があるポートを選択すると、[ポートのドロップ（Drop Port）] 列と [サイド（Side）] 列の値が自動的に設定されます。また、[ポートのドロップ（Drop Port）] 列の値を手動で編集することもできます。

ステップ 16 OCH 回線のトレールの多様性を選択します。作成する OCH 回線と選択するトレールは異なります。

（注） 作成後にトレールの多様性を変更または削除することはできません。

ステップ 17 [次へ（Next）] をクリックして [制約セクション（Constraints Section）] ページに進みます。

ステップ 18 マップでデバイス ノードまたはリンクをクリックし、[制約（Constraints）]テーブルに追加します。あるいは、テーブル ツールバーで「+」ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名（Node/Link Name）]、[包含/除外（Include/Exclude）]、および [ルート（Route）] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。

（注） 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約（Constraints）] テーブルの列にデータを読み込むことはできません。OCHCC トレール WSON 回線には、次のルートの制約条件が適用されます。

- 変更されたルートの制約事項は、すぐには回線に適用されませんが、再ルーティングが必要になる場合があります。ただし、変更は次回のルート操作または復元時に適用されます。
- [回線オーバーレイ（Circuit Overlay）] には現在のルートに適用可能な制約事項のみが表示され、**回線の編集**ウィザードには現在設定されている制約事項が表示されます。
- **回線の編集**ウィザードには、回線オーバーレイを使用して表示される制約事項アイコンとは異なる制約事項を表示する制約事項テーブルが含まれています。

ステップ 19 [次へ（Next）] をクリックして [異種波長セクション（Alien Wavelength Section）] ページに移動します。送信元ノードと宛先ノードのカード、トランク モード、Fec モードなどの現在の異種波長の設定が表示されます。送信元ノードと宛先ノードの異種波長に新しい設定を作成できます。

（注） [異種波長セクション（Alien Wavelength Section）] は、OCHNC WSON 回線を作成する場合にのみ使用できます。

ステップ 20 [今すぐ作成（Create Now）] をクリックして回線を作成します。デバイスに展開する前に TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー（Preview）] をクリックするとプレビューが表示されます。この場合、設定をデバイスに展開するかキャンセルするかを選択できますが、属性を編集することはできません。

ステップ 21 [ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

互いに異なる 2 つの OCH トレール UNI 回線の作成およびプロビジョニング

互いに異なる 2 つの OCH トレール UNI 回線を作成するには、この手順を使用します。両方の回線の始点は同じデバイスにする必要があります。プロビジョニング ウィザードを使用して、1 つのウィンドウで両方の回線を迅速に作成することができます。

始める前に

オプティカル回線をプロビジョニングする前に満たす必要がある前提条件については、光回線のプロビジョニングの前提条件 （667 ページ）を参照してください。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックして、OCH 回線を作成する場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [回線/VC（Circuits/VCs）] タブをクリックし、[回線/VC（Circuits/VCs）] ペイン ツールバーで [+]（[作成（Create）]）アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。

プロビジョニング ウィザードを表示するもう 1 つの方法として、**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[サービス プロビジョニング（Service Provisioning）]** の順に選択する方法があります。

ステップ 6 [テクノロジー（Technology）] ドロップダウン リストから、[オプティカル（Optical）] を選択します。

ステップ 7 [サービス タイプ（Service Type）] 領域で、[OCH トレール UNI（OCH-Trail UNI）] を選択します。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [顧客セクション（Customer Section）] ページに移動します。

ステップ 10 互いに異なる 2 つの OCH トレール UNI 回線を作成するには、[相互ダイバーシティ（Mutual Diversity）] チェックボックスをオンにします。

ステップ 11 [顧客セクション（Customer Section）] ページで、回線の名前と説明を入力します。

ステップ 12 [次へ（Next）] をクリックして [エンドポイント セクション（Endpoint Section）] ページに移動します。

ステップ 13 [エンドポイント（Endpoint）] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名（Device Name）] 列に読み込まれます。または、[エンドポイント（Endpoint）] テーブル内の行をクリックしてデバイス名とインターフェイスを編集することもできます。

（注） 行が編集モードになっていると、マップ内のデバイスをクリックしても、[デバイス名（Device Name）] 列に名前は取り込まれません。

ステップ 14 [次へ（Next）] をクリックして [回線セクション（Circuit Section）] ページに進みます。

ステップ 15 回線の詳細を入力します。フィールドと属性の説明については、OCH 回線タイプの [回線（Circuit）] セクション リファレンス （671 ページ） を参照してください。

ステップ 16 [次へ（Next）] をクリックして [制約セクション（Constraints Section）] ページに進みます。

ステップ 17 マップでデバイス ノードまたはリンクをクリックし、[制約（Constraints）] テーブルに追加します。あるいは、テーブル ツールバーで「+」ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名（Node/Link Name）]、[包含/除外（Include/Exclude）]、および [ルート（Route）] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。

（注） 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約（Constraints）] テーブルの列にデータを読み込むことはできません。

ステップ 18 [次へ（Next）] をクリックします。2 番目の回線の [顧客セクション（Customer Section）] ページが表示されます。

ステップ 19 ステップ 11 からステップ 17 を繰り返して 2 番目の回線を作成します。

ステップ 20 [今すぐ作成（Create Now）] をクリックして回線を作成します。デバイスに展開する前に TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー（Preview）] をクリックするとプレビューが表示されます。この場合、設定をデバイスに展開するかキャンセルするかを選択できますが、属性を編集することはできません。

ステップ 21 回線が、[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに追加されているはずです。プロビジョニングの状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックして [回線/VC 360（Circuit/VC 360）] ビューを表示します。

メディア チャネル グループ SSON 回線の作成とプロビジョニング

メディア チャネル グループの SSON 回線を作成し、プロビジョニングするには、次の手順を実行します。

始める前に

光回線をプロビジョニングする前に満たす必要がある前提条件については、光回線のプロビジョニングの前提条件 （667 ページ）を参照してください。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックして、メディア チャネル グループの SSON 回線を作成する場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [回線/VC（Circuits/VCs）] タブをクリックし、[回線/VC（Circuits/VCs）] ペイン ツールバーで [+]（[作成（Create）]）アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。

プロビジョニング ウィザードを表示するもう 1 つの方法として、**[設定（Configuration）] > [ネットワーク（Network）] > [サービス プロビジョニング（Service Provisioning）]** の順に選択する方法があります。

ステップ 6 [テクノロジー（Technology）] ドロップダウン リストから [光（Optical）] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ（Service Type）] 領域に表示します。

ステップ 7 [サービス タイプ（Service Type）] 領域で、[メディア チャネル グループの SSON（Media Channel Group SSON）] を選択します。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [顧客セクション（Customer Section）] ページに移動します。

ステップ 10 （オプション）回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customers）]** の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。

ステップ 11 [顧客セクション（Customer Section）] ページに回線名とその説明を入力します。

（注） [回線名（Circuit Name）] フィールドには最大 80 文字を使用することができます。

ステップ 12 [次へ（Next）] をクリックして [エンドポイント セクション（Endpoint Section）] ページに移動します。

ステップ 13 [エンドポイント（Endpoint）]テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名（Device Name）] 列に読み込まれます。あるいは、[エンドポイント（Endpoint）]テーブルの行をクリックして、[デバイス名（Device Name）]、[終端ポイント（Termination Point）]、[ポートの追加（Add Port）]、および [ポートのドロップ（Drop Port）] の各列を編集します。選択した回線タイプと互換性があり使用可能なネットワーク要素だけが表示されます。

（注） 行が編集モードになっていると、マップ内のデバイスをクリックしても、[デバイス名（Device Name）] 列に名前は取り込まれません。

ステップ 14 [次へ（Next）] をクリックして [回線セクション（Circuit Section）] ページに進みます。

ステップ 15 必要な回線幅を選択します。

ステップ 16 [中央波長/周波数のプロパティ（Central Wavelength/Frequency Properties）] を設定するには、次のいずれかを実行します。

- [自動プロビジョニング（Auto Provisioning）] チェックボックスをオンにします。
- 回線に必要な**波長**を選択して、[優先（Preferred）] オプションまたは [必須（Required）] オプションを選択し、[波長（Wavelength）] フィールドに設定した値が回線をプロビジョニングするために優先されるか、または必須であるかを特定します。

ステップ 17 [次へ（Next）] をクリックして [制約セクション（Constraints Section）] ページに進みます。

ステップ 18 マップでデバイス ノードまたはリンクをクリックし、[制約（Constraints）]テーブルに追加します。あるいは、テーブル ツールバーで「+」ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名（Node/Link Name）]、[包含/除外（Include/Exclude）]、および [ルート（Route）] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。

（注） 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約（Constraints）] テーブルの列にデータを読み込むことはできません。

[光プロパティ（Optical Properties）] で、[復元（Restoration）] チェックボックスがオンになっており、[元に戻す（Revert）]が [なし（None）]に設定されている場合は、[代替制約事項（Alternate Constraints）] チェックボックスを選択できます。

ステップ 19 [今すぐ作成（Create Now）] をクリックして、回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示する場合、[プレビュー（Preview）] をクリックするとプレビューが表示されます。この時点で、設定をデバイスに展開するか、またはキャンセルすることができますが、属性を編集することはできません。

[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

メディア チャネル SSON 回線の作成とプロビジョニング

メディア チャネルの SSON 回線を作成し、プロビジョニングするには、次の手順を実行します。

始める前に

- メディア チャネル SSON 回線をメディア チャネル グループに関連付けるために、メディア チャネル グループの SSON が既に作成されていることを確認します。メディア チャネル グループ SSON 回線の作成とプロビジョニング （683 ページ）を参照してください。
- 光回線をプロビジョニングする前に満たす必要がある前提条件については、光回線のプロビジョニングの前提条件 （667 ページ）を参照してください。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイスグループ（Device Groups）] をクリックして、メディアチャネルの SSON 回線を作成する場所を選択します。

ステップ 3 [デバイスグループ（Device Groups）] ポップアップウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [回線/VC（Circuits/VCs）] タブをクリックし、[回線/VC（Circuits/VCs）] ペインツールバーで [+]（[作成（Create）]）アイコンをクリックします。プロビジョニングウィザードが新しいペインで開きます。

プロビジョニングウィザードを表示するもう 1 つの方法として、**[設定（Configuration）] > [ネットワーク（Network）] > [サービスプロビジョニング（Service Provisioning）]** の順に選択する方法があります。

ステップ 6 [テクノロジー（Technology）] ドロップダウン リストから [光（Optical）] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ（Service Type）] 領域に表示します。たとえば、メディア チャネル SSON 回線の光サービス タイプには、[メディア チャネル NC SSON（Media Channel NC SSON）]、[メディア チャネル トレール SSON（Media Channel Trail SSON）]、および [メディア チャネル CC SSON（Media Channel CC SSON）] などがあります。

ステップ 7 [サービス タイプ（Service Type）] 領域で、作成するメディア チャネルの SSON 回線のタイプを選択します。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [顧客セクション（Customer Section）] ページに移動します。

ステップ 10 （オプション）回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customers）]** の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。

ステップ 11 [顧客セクション（Customer Section）] ページで、回線の名前と説明を入力します。

（注） メディアチャネル NC SSON およびメディアチャネルトレール SSON 回線の場合、[回線名（Circuit Name）] フィールドには最大 77 文字を使用できます。77 文字のうち、3 文字はキャリアサフィックス用に予約されています。

メディア チャネル CC SSON 回線の場合、[回線名（Circuit Name）] フィールドには最大 71 文字を使用できます。

ステップ 12 [次へ（Next）] をクリックして [エンドポイント セクション（Endpoint Section）] ページに移動します。

ステップ 13 [エンドポイント（Endpoint）]テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名（Device Name）] 列に読み込まれます。あるいは、[エンドポイント（Endpoint）] テーブルの行をクリックして、[デバイス名（Device Name）] 列および [終端ポイント（Termination Point）] 列を編集します。[サイド（Side）] 列は、終端ポイントに基づいて自動的に設定されます。選択した回線タイプと互換性があり、使用可能なネットワーク要素だけが表示されます。

（注） [MCH トレール名（MCH-Trail Name）] 列は、メディア チャネル CC SSON 回線を作成する場合にのみ使用できます。

ステップ 14 MCH 回線のメディア チャネルの種類を選択します。作成する MCH 回線と選択するメディア チャネルは異なります。

（注） 作成後にメディア チャネルの種類を変更または削除することはできません。

ステップ 15 [次へ（Next）] をクリックして [回線セクション（Circuit Section）] ページに移動します。

（注） メディア チャネル CC SSON 回線では、[エンドポイント（Endpoints）] テーブルに MCH トレール名を入力した場合、[回線セクション（Circuit Section）] ページは使用できません。

ステップ 16 メディアチャネル SSON 回線を関連付けるメディアチャネルグループを選択します。

ステップ 17 回線の詳細を入力します。フィールドと属性の説明については、メディア チャネル SSON 回線タイプの回線セクション リファレンス （686 ページ） を参照してください。

ステップ 18 [次へ（Next）] をクリックして [制約セクション（Constraints Section）] ページに進みます。

（注） MCHNC SSON 回線の場合、NCS1K および NCS2K デバイスを Regen モードで制約として追加できます。

ステップ 19 マップでデバイス ノードまたはリンクをクリックし、[制約（Constraints）]テーブルに追加します。あるいは、テーブルツールバーで [+] ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名（Node/Link Name）]、[包含/除外（Include/Exclude）]、および [ルート（Route）] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。

（注） 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約（Constraints）] テーブルの列にデータを読み込むことはできません。

ステップ 20 [今すぐ作成（Create Now）] をクリックして、回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー（Preview）] をクリックします。設定をデバイスに展開するかキャンセルするかを選択できますが、属性を編集することはできません。

[ネットワークトポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

メディア チャネル SSON 回線タイプの回線セクション リファレンス

次の表に、メディア チャネル SSON 回線のタイプを定義する属性のリストと説明を示します。

表 *39 : [*回線セクション（*Circuit Section*）*]* のリファレンス：メディア チャネル *SSON* 回線のタイプ

属性	説明	有効
中心波長/周波数のプロパティ		
自動プロビジョニング（Auto Provisioning）	このチェックボックスをオンにすると、回線の波長または周波数のプロパティが自動的に設定されます。	すべてのメディア チャネル SSON 回線のタイプ。
波長（nm）（Wavelength (nm)）	回線の波長または周波数。 （注） DWDM グリッド単位を波長または周波数に設定する必要があります。これには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [回線/VC 表示（Circuits/VCs Display）]** を選択し、[DWDM グリッド単位（DWDM Grid Unit）] エリアで [波長（ナノメートル（nm））（Wavelength (Nanometer (nm))）] または [周波数（テラヘルツ（THz））（Frequency (Terahertz (THz))）] を選択します。	[自動プロビジョニング（Auto Provisioning）] チェックボックスがオフの場合のすべてのメディア チャネル SSON 回線のタイプ。
優先/必須（Preferred/Required）	[波長（Wavelength）] フィールドで設定した値が、回線をプロビジョニングするときに優先される値であるか必須の値であるかを決定するために選択します。	[自動プロビジョニング（Auto Provisioning）] チェックボックスがオフの場合のすべてのメディア チャネル SSON 回線のタイプ。
光プロパティ（Optical Properties）		
検証	回線の検証モード。値は次のとおりです。 • [フル（Full）]：回線の検証結果が承認しきい値以上になると回線が作成されます。 • [なし（None）]：承認しきい値を考慮せずに回線が作成されます。	すべてのメディア チャネル SSON 回線のタイプ。

属性	説明	有効
承認しきい値（Acceptance Threshold）	回線に設定された保護承認しきい値。値は次のとおりです。 • [緑（Green）]：復元失敗の危険性が 0 % であることを示します。 • [黄（Yellow）]：復元失敗の危険性が 0 % ～ 16 % の間であることを示します。 • [オレンジ（Orange）]：復元失敗の危険性が 16 % ～ 50 % の間であることを示します。 • [赤（Red）]：復元失敗の危険性が 50 % を超えていることを示します。	[検証（Validation）] フィールドが [フル（Full）] に設定されている場合のすべてのメディア チャネル SSON 回線タイプ。
[パス アラームを無視（Ignore Path Alarms）]	パス アラームを無視するには、このチェックボックスをオンにします。	すべてのメディア チャネル SSON 回線のタイプ。
[再生成を許可（Allow Regeneration）]	ネットワーク要素が信号を再生成できるようにするには、このチェックボックスをオンにします。	すべてのメディア チャネル SSON 回線のタイプ。
復元（Restoration）	障害が発生したメディア チャネル SSON 回線を新しいルートに復元するには、このチェックボックスをオンにします。	すべてのメディア チャネル SSON 回線のタイプ。
プライオリティ（Priority）	障害が発生した回線の復元操作に優先順位を付けます。値は [高（High）]、[プライオリティ 1（Priority 1）]、[プライオリティ 2（Priority 2）]、[プライオリティ 3（Priority 3）]、[プライオリティ 4（Priority 4）]、[プライオリティ 5（Priority 5）]、[プライオリティ 6（Priority 6）]、および [低（Low）] です。	[復元（Restoration）] チェックボックスがオンの場合のすべてのメディア チャネル SSON 回線タイプ。
[復元の検証（Restoration Validation）]	復元操作の検証モード。値は次のとおりです。 • [なし（None）]：復元の承認しきい値を考慮せずに回線が作成されます。 • [継承（Inherited）]：復元された回線は、プライマリ回線から検証と承認のしきい値を継承します。 • [フル（Full）]：復元の検証結果が復元の承認しきい値以上になると回線が作成されます。	[復元（Restoration）] チェックボックスがオンの場合のすべてのメディア チャネル SSON 回線タイプ。

属性	説明	有効
[復元の承認しきい値（Restoration Acceptance Threshold）]	回線の復元操作に設定された承認しきい値。値は次のとおりです。 • [緑（Green）]：復元失敗の危険性が 0 % であることを示します。 • [黄（Yellow）]：復元失敗の危険性が 0 % ～ 16 % の間であることを示します。 • [オレンジ（Orange）]：復元失敗の危険性が 16 % ～ 50 % の間であることを示します。 • [赤（Red）]：復元失敗の危険性が 50 % を超えていることを示します。	次の場合のすべてのメディア チャネル SSON 回線タイプ。 • [復元（Restoration）] チェックボックスがオンになっている。 • [復元検証（Restoration Validation）] フィールドが [フル（Full）] に設定されている。
[元に戻す（Revert）]	障害が修正された後、復元されたパスから元のパスに回線を戻します。値は [なし（None）]、[手動（Manual）]、および [自動（Automatic）] です。	[復元（Restoration）] チェックボックスがオンの場合のすべてのメディア チャネル SSON 回線タイプ。
[ソーク時間（Soak Time）]	障害が修正された後、元のパスに切り替わるまでに、復元されたパス上の回線が待機する期間。	[元に戻す（Revert）] オプションが [手動（Manual）] または [自動（Automatic）] に設定されている場合、すべてのメディア チャネル SSON 回線タイプ。

OTN 回線の作成とプロビジョング

OTN 回線をプロビジョニングするには、次の手順に従います。

始める前に

光回線をプロビジョニングする前に満たしている必要がある前提条件については、光回線のプロビジョニングの前提条件 （667 ページ）を参照してください。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックして、OTN 回線を作成する場所を選択します。

ステップ 3 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 4 [回線/VC（Circuits/VCs）] タブをクリックし、[回線/VC（Circuits/VCs）] ペイン ツールバーで [+]（[作成（Create）]）アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。

プロビジョニング ウィザードを表示するもう 1 つの方法として、**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[サービス プロビジョニング（Service Provisioning）]** の順に選択する方法があります。

ステップ 5 [テクノロジー（Technology）] ドロップダウン リストから、[オプティカル（Optical）] を選択します。Cisco EPN Manager の [サービス タイプ（Service Type）] エリアに、関連する回線タイプのリストが表示されます。たとえば、OTN 回線のサービス タイプには、[ODU UNI]、[ODU トンネル（ODU Tunnel）]、[OPU over ODU]、および [ODU UNI ヘアピン（ODU UNI Hairpin）] があります。

ステップ 6 [サービス タイプ（Service Type）] エリアで、作成する OTN 回線のタイプを選択します。

ステップ 7 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 8 [次へ（Next）] をクリックして [顧客の詳細（Customer Details）] ページに移動します。

ステップ 9 （オプション）回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）]** > **[その他（Other）]** > **[顧客（Customers）]** の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。

ステップ 10 [顧客の詳細（Customer Details）] ページに回線名とその説明を入力します。

ステップ 11 [次へ（Next）] をクリックして [回線の詳細（Circuit Details）] ページに移動します。

ステップ 12 回線の詳細を入力します。フィールドと属性の説明については、OTN 回線タイプの回線セクション参照（691 ページ） を参照してください。

ステップ 13 [次へ（Next）] をクリックして [エンドポイント セクション（Endpoint Section）] ページに移動します。

ステップ 14 [エンドポイント（Endpoint）] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名（Device Name）] 列に読み込まれます。あるいは、[エンドポイント（Endpoint）] テーブルの行をクリックして、[デバイス名（Device Name）] および [インターフェイス/終端ポイント（Interface/Termination Point）] 列を編集します。選択した回線タイプと互換性があり使用可能なネットワーク要素だけが表示されます。

（注） 行が編集モードになっている場合は、マップのデバイスをクリックして [デバイス名（Device Name）] 列にデータを読み込むことはできません。

ステップ 15 回線の保護タイプとパス オプションを入力します。フィールドと属性の説明については、OTN回線タイプの [エンドポイント（Endpoint）] セクション リファレンス （693 ページ） を参照してください。

ステップ 16 [今すぐ作成（Createe Now）] をクリックして、回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー（Preview）] をクリックすると

プレビューが表示されます。TL1 または CLI コマンドのプレビューを確認したら、設定をデバイスに展開するか、またはプロビジョニング操作をキャンセルできます。

[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] タブのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

OTN 回線タイプの回線セクション参照

次の表に、OTN 回線タイプを定義する属性の一覧と説明を示します。

表 *40 :* 回線セクション参照：*OTN* 回線タイプ

属性	説明	有効
回線プロパティ		
Bandwidth	OTN 回線をプロビジョニングするために必要な帯域幅。 帯域幅とサービス タイプ フィールドの値のマッピングについては、表 42 : 値のマッピング：ODU UNI 回線の帯域幅とサービス タイプを参照してください。	すべての OTN 回線タイプ。
A エンド：オープンエンド（A-End Open Ended）	送信元エンドポイントがクライアントのペイロードコントローラではなく ODU サブコントローラに接続されているオープンエンド回線を作成するには、このチェックボックスをオンにします。 （注） このチェックボックスをオンにすると、Cisco NCS 4000 デバイスに ODU サブコントローラが展開されません。デバイスを Cisco EPN Manager に追加する前に Cisco NCS 4000 デバイスで ODU サブコントローラを設定する必要があります。オープンエンド ODU UNI、および Cisco NCS 4000 デバイスで ODU サブコントローラを設定する方法については、オープン エンドの ODU UNI （619 ページ）を参照してください。	帯域幅フィールドが ODU0、ODU1、ODU2、または ODU2E に設定されている場合、ODU UNI 回線タイプ。

属性	説明	有効
Z エンド：オープンエンド（Z-End Open Ended）	宛先エンド ポイントがクライアントのペイロード コントローラではなく ODU サブコントローラに接続されているオープンエンド回路を作成するには、このチェックボックスをオンにします。 （注） このチェックボックスをオンにすると、Cisco NCS 4000 デバイスに ODU サブコントローラが展開されません。デバイスを Cisco EPN Manager に追加する前に Cisco NCS 4000 デバイスで ODU サブコントローラを設定する必要があります。オープンエンド ODU UNI、および Cisco NCS 4000 デバイスで ODU サブコントローラを設定する方法については、オープン エンドの ODU UNI （619 ページ）を参照してください。	帯域幅フィールドが ODU0、ODU1、ODU2、または ODU2E に設定されている場合、ODU UNI 回線タイプ。
サービス タイプ（Service Type）	選択した帯域幅でサポートされているサービス タイプ。 帯域幅とサービス タイプ フィールドの値のマッピングについては、表 42 : 値のマッピング：ODU UNI 回線の帯域幅とサービス タイプを参照してください。	ODU UNI 回線タイプ。
ルート プロパティ（Route Properties）		
ビット レート	1 秒あたりのビット数の合計。	帯域幅フィールドが ODUFLEX に設定されている場合、すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。
フレーミング タイプ（Framing Type）	要求されたサービスの基本信号。値は次のとおりです。 • CBR：固定ビット レート。 • GFP-F 固定（GFP-F-Fixed）：固定のフレーム マップ型ジェネリック フレーミング プロシージャ。	帯域幅フィールドが ODUFLEX に設定されている場合、すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。

属性	説明	有効
ルートを記録（Record Route）	回線ルートを記録するには、このチェックボックスをオンにします。	すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。

OTN 回線タイプの [エンドポイント（Endpoint）] セクション リファレンス

次の表に、OTN 回線タイプの保護タイプおよびパス オプションを定義する属性をリストして説明します。

表 *41 : [*エンドポイント（*Endpoint***）*]* セクション リファレンス：*OTN* 回線タイプ**

属性	説明	有効
エンドポイント		
デバイス名（Device Name）	回線の A エンド デバイスと Z エンド デバイス。 （注） ODU UNI ヘアピン回線では、A エンドと Z エンドが同じデバイスになりますが、終端地点が異なります。	すべての OTN 回線タイプ。
インターフェイス（Interface）	AエンドデバイスとZエンドデバイスのインターフェイス名。	ODU UNI 回線。
終端地点	カードの終端地点。	OPU over ODU および ODU UNI ヘアピン回線。

属性	説明	有効
[保護タイプ（Protection Type）]	OTN 回線の保護タイプ。値は次のとおりです。 • [1+0]：非保護カード。現用パスで障害が検出されると、データが失われます。 • [1+1]：プライマリ パスとセカンダリ パスの両方がトラフィックをエンドツーエンドで伝送し、受信者は両方のトラフィックを受信して比較します。あるパスで出力ノードが障害を検出すると、トラフィックは影響を受けていないパスに切り替えられます。 • [1+R]：プライマリ パスで障害が発生すると、復元されたパスが計算され、トラフィックは復元されたパスに切り替えられます。プライマリ パスが復帰不可能な場合、復元されたパスは新しいプライマリ パスになります。 • [1+1+R]：プライマリ パスとセカンダリ パスの両方でトラフィックが伝送されます。あるパスで出力ノードが障害を検出すると、トラフィックは影響を受けていないパスに切り替えられます。復元されたパスが計算され、トラフィックは復元されたパスに切り替えられます。プライマリ パスまたはセカンダリ パスが復帰不可能な場合、復元されたパスは新しいプライマリ パスまたはセカンダリ パスになります。 （注） この保護タイプは、Cisco NCS 4000 シリーズ デバイスではサポートされていません。	すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。
[トンネル ID と異なる（Diverse From Tunnel ID）]	トンネルを選択し、プロビジョニングする回線でそのトンネルが使用されないことを確認します。これにより、トンネルに障害がある場合に、同じトンネルが他の回線で使用されなくなります。	すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。

[動作中のパス（Working Path）]、[保護パス（Protected Path）]、および [復元パス（Restored Path）]

[保護パス（Protected Path）] フィールド グループは、[保護タイプ（Protection Type）] フィールドが [1+1] または [1+1+R] に設定されている場合に限り、すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）で使用できます。

[復元パス（Restored Path）] フィールド グループは、[保護タイプ（Protection Type）] フィールドが [1+R] または [1+1+R] に設定されている場合に限り、すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）で使用できます。

属性	説明	有効
タイプ（Type）	回線の現用パスまたは保護パスのタイプを選択します。値は [ダイナミック（Dynamic）] および [明示的（Explicit）] です。	すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。
新規作成（New）	回線の新しい明示的な作業パスまたは保護パスを作成するには、このチェックボックスをオンにします。	[タイプ（Type）] フィールドが [明示的（Explicit）] に設定されている場合のすべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。
[既存の EP を選択（Select Existing EP）]	回線の既存の明示的な現用パスまたは保護パスを選択します。	[タイプ（Type）] フィールドが [明示的（Explicit）] に設定されており、[新規作成（New）] チェックボックスがオフになっている場合のすべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。

属性	説明	有効
新しい名前（New Name）	作成する明示的なパスの名前を入力します。[新しい名前（New Name）] フィールドの下のテーブルで、[+] ボタンをクリックしてテーブルに新しい行を追加し、デバイスを選択して、そのデバイスのインターフェイスとして明示的なパス コントローラを選択します。	[タイプ（Type）] フィールドが [明示的（Explicit）] に設定されており、[新規作成（New）] チェックボックスがオンになっている場合のすべての OTN 回線タイプ（ODU UNI ヘアピンを除く）。
[保護のプロファイル（Protection Profile）] [保護プロファイル（Protection Profile）] フィールド グループは、[保護タイプ（Protection Type）] フィールドが [1+1]、[1+R]、または [1+1+R] に設定されており、有効な A エンド デバイスが選択されている場合に限り、すべての OTN 回線タイプ（ODU UNI ヘアピンを除く）で使用できます。		
[保護のプロファイル（Protection Profile）]	回線の保護を管理するために使用されるプロファイル。この保護プロファイルは、回線の A エンド ノードで設定する必要があります。 （注） デバイスに設定されている保護プロファイルを入力できます。 保護タイプ、SNC、ホールドオフ、復元待ち、回線復帰などの保護プロファイルの詳細が表示されます。	

ODU UNI 回線の帯域幅とサービス タイプの値のマッピング

次の表に、ODU UNI 回線の帯域幅とサービス タイプ フィールドの値のマッピングを示します。

表 *42 :* 値のマッピング：*ODU UNI* 回線の帯域幅とサービス タイプ

Bandwidth	サービス タイプ（Service Type）
ODU0	• イーサネット OPU0 GMP

Bandwidth	サービス タイプ（Service Type）
ODU1	• OTN OPU1 • Sonet OPU1 BMP • SDH OPU1 BMP
ODU1E	• イーサネット OPU1e BMP • OTN OPU1e
ODU1F	• OTN OPU1f
ODU2	• イーサネット OPU2 GFP_F • イーサネット OPU2 GFP_F_EXT • イーサネット OPU2 WIS • OTN OPU2 • Sonet OPU2 AMP • Sonet OPU2 BMP • SDH OPU2 AMP • SDH OPU2 BMP
ODU2E	• イーサネット OPU2e BMP • OTN OPU2e
ODU2F	• OTN OPU2f
ODU4	• OTN OPU4 • イーサネット OPU4 GFP_F • イーサネット OPU4 GMP
ODUFLEX	• OTN OPUFlex • イーサネット OPUFlex GFP_F

ODU 回線の作成とプロビジョング

ODU 回線を作成し、プロビジョングするには、次の手順を実行します。

始める前に

- 光回線をプロビジョニングする前に満たす必要がある前提条件については、光回線のプロビジョニングの前提条件 （667 ページ）を参照してください。
- デバイス間に管理対象リンクを作成するには、トポロジマップへのリンクの手動による追加 （228 ページ）を参照してください。

ステップ 1 左側のサイドバーから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイスグループ（Device Groups）] をクリックして、ODU 回線を作成する場所を選択します。

ステップ 3 [デバイスグループ（Device Groups）] ポップアップウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [回線/VC（Circuits/VCs）] タブをクリックし、[回線/VC（Circuits/VCs）] ペイン ツールバーで [+]（[作成（Create）]）アイコンをクリックします。プロビジョニングウィザードが新しいペインで開きます。

プロビジョニングウィザードを表示するもう 1 つの方法として、**[設定（Configuration）] > [ネットワーク（Network）] > [サービスプロビジョニング（Service Provisioning）]** の順に選択する方法があります。

ステップ 6 [テクノロジー（Technology）] ドロップダウン リストから [光（Optical）] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ（Service Type）] 領域に表示します。

ステップ 7 [サービス タイプ（Service Type）] 領域で、[ODU] を選択します。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [顧客セクション（Customer Section）] ページに移動します。

ステップ 10 （オプション）回線の顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customers）]** の順に移動し、システムで顧客を作成して、プロビジョニングウィザードを再起動します。

ステップ 11 [顧客セクション（Customer Section）] ページで、回線の名前と説明を入力します。

ステップ 12 [次へ（Next）] をクリックして [回線セクション（Circuit Section）] ページに進みます。

ステップ 13 ここでは、**リモート** ODU 回線と **ローカル** ODU 回線の 2 種類の ODU 回線を作成できます。

リモート ODU 回線（2 つの異なるデバイス間の相互接続）を作成するには、次の手順を実行します。

a) [ローカルクロスコネクト（Local Cross Connect）] チェックボックスをオフにします。

b) 回線には、次のいずれかの保護タイプを選択します。

[なし（None）]：回線の保護タイプなし。

[1+1]：プライマリパスとセカンダリパスの両方でトラフィックをエンドツーエンドに伝送します。受信側はプライマリパスとセカンダリパスからトラフィックを受信し、両方のトラフィックを比較します。あるパスで出力ノードが障害を検出すると、トラフィックは影響を受けていないパスに切り替えられます。

（注） 保護タイプとして [1+1] を選択した場合、[接続モード（Connection Mode）] はデフォルトで [SNC-N] に設定されます。

c) 回線に必要な [復帰時間（Reversion Time）] と [保留タイマー（Hold off Timer）] を選択します。

（注） これらのフィールドは、保護タイプとして [1+1] を選択した場合にのみ使用できます。

d) [次へ（Next）] をクリックして [エンドポイント セクション（Endpoint Section）] ページに移動します。

e) [エンドポイント（Endpoint）] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名（Device Name）] 列に読み込まれます。あるいは、[エンドポイン

ト（Endpoint）] テーブルの行をクリックして、[デバイス名（Device Name）] 列および [終端ポイント（Termination Point）] 列を編集します。選択した回線タイプと互換性があり、使用可能なネットワーク要素だけが表示されます。

（注） 行が編集モードになっていると、マップ内のデバイスをクリックしても、[デバイス名（Device Name）] 列に名前は取り込まれません。

f) [次へ（Next）] をクリックして [制約セクション（Constraints Section）] ページに移動します。
g) マップでデバイス ノードをクリックし、[制約（Constraints）] テーブルに追加します。あるいは、テーブルツールバーで [+] ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名（Node/Link Name）]、[包含/除外（Include/Exclude）]、および [ルート（Route）] 列を編集することもできます。ODU 回線タイプと互換性があるネットワーク要素のみが表示されます。

（注） ODU 回線の制約事項としてリンクを指定することはできません。

h) （オプション）[パスの計算（Calculate Path）] をクリックして、選択したエンドポイント間に有効な動作中のパスがあるかどうかを確認します。選択したエンドポイント間に有効な動作中のパスが存在する場合、パスはトポロジ マップに「W」ラベルで表示されます。選択したエンドポイント間に有効な動作中のパスが存在しない場合は、選択したエンドポイント間に動作中のパスを確立できない理由を表示する [パスの計算結果（Path Calculation Result）] セクションが表示されます。
i) [今すぐ作成（Create Now）] をクリックして、回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示する場合、[プレビュー（Preview）] をクリックします。設定をデバイスに展開するかキャンセルするかを選択できますが、属性を編集することはできません。

ローカル ODU 回線（同じデバイス内の相互接続）を作成するには、次の手順を実行します。

a) [ローカルクロスコネクト（Local Cross Connect）] チェックボックスをオンにします。
b) [帯域幅（Bandwidth）] や [サービスタイプ（Service type）] などの回線プロパティを選択します。
c) 回線には、次のいずれかの保護タイプを選択します。

[なし（None）] : 回線の保護タイプなし。

[1+1] : プライマリパスとセカンダリパスの両方でトラフィックをエンドツーエンドに伝送します。受信側はプライマリパスとセカンダリパスからトラフィックを受信し、両方のトラフィックを比較します。あるパスで出力ノードが障害を検出すると、トラフィックは影響を受けていないパスに切り替えられます。

（注） 保護タイプとして [1+1] を選択した場合、[接続モード（Connection Mode）] はデフォルトで [SNC-N] に設定されます。

d) 回線に必要な [復帰時間（Reversion Time）] と [保留タイマー（Hold off Timer）] を選択します。

（注） これらのフィールドは、保護タイプとして [1+1] を選択した場合にのみ使用できます。

e) [次へ（Next）] をクリックして [エンドポイント セクション（Endpoint Section）] ページに移動します。
f) ODU 回線をプロビジョニングする**デバイス名**を選択します。
g) [ソース（Source）]、[セカンダリ ソース/宛先（Secondary Source/Destination）]、および [宛先（Destination）] ポートを選択します。[ODU] スライスを選択します。

（注） [セカンダリソース/宛先（Secondary Source/Destination）] は、保護タイプとして [1+1] を選択した場合にのみ使用できます。

h) [今すぐ作成（Create Now）] をクリックして回線を作成します。回線のプレビューを表示する場合は、[プレビュー（Preview）] をクリックします。設定をデバイスに展開するかキャンセルするかを選択できますが、属性を編集することはできません。

[ネットワークトポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

L3VPN サービスのプロビジョニング

サポートされている L3VPN サービス

MPLS レイヤ 3 VPN はプライベート IP ネットワークを形成します。顧客はプロバイダ エッジ（PE）ルータの IP ピアとして機能するカスタマーエッジ（CE）ルータを介してネットワークに接続します。

仮想ルーティングおよび転送（VRF）

PE では、仮想ルーティングおよび転送（VRF）インスタンスが L3VPN サービスのトラフィック転送専用の仮想 IP ルータとして機能します。VRF は、マルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）を介して相互にルートを学習し、MPLS を使用してトラフィックを転送します。

VPN は少なくとも 1 つ、通常は複数の VRF で構成されます。Cisco EPN Manager は VPN ID を使用して、単一の VPN を一緒に形成する VRF を検出します。VPN ID がプロビジョニングされていない既存のネットワークを Cisco EPN Manager が検出すると、同じ名前のすべての VRF を取得し、それらを 1 つの VPN に関連付けます。バージョン番号プレフィックスと異なるサフィックスによる命名規則を使用する Cisco PRIME プロビジョニングを使用して作成された

VPN の場合、Cisco EPN Manager は異なる VRF を 1 つの VPN に属しているものとして認識します。

一般に、さまざまな命名規則を受け入れるように設定できる正規表現があります。

ルート ターゲット（RT）

VRF 間の接続は VRF によってインポートおよびエクスポートされるルートターゲット（RT）を使用して定義されます。Cisco EPN Manager は、フルメッシュ接続のセットアップを容易にし、使用するルートターゲットを自動的に割り当てます。ルート ターゲットは、AS 番号または IPv4 アドレスのいずれかのプレフィックス（フル メッシュ プレフィックス、100 [681682] など）で構成されます。プレフィックスは、ネットワーク内の既存の BGP 自律システム（AS）番号から選択することも、手動で入力することもできます。プレフィックスに続く 2 番目の番号は Cisco EPN Manager によって自動的に割り当てられます。

あるいは、ルート ターゲットを手動で選択することもでき、また、フル メッシュに加えてこれを行うこともできます。VPN の作成時に VPN 内で使用するルート ターゲットを入力する初期画面が表示され、VRF ごとにインポートおよびエクスポートするルート ターゲットを選択できます。また、ルート ターゲットを使用するアドレス ファミリ（IPv4 または IPv6）も指定します。これは、他の VPN で使用されるルート ターゲットをインポートすることによって、エクストラネットを設定する場合などに使用できます。

ルートの再配布

PE と CE の間で交換されるルートは、リモート エンドポイントが各 VRF で到達できるプレフィックスがわかるように MP-BGP ルーティング プロトコルに再配布する必要があります。ルートの再配布を制御するため、Cisco EPN Manager では必要なプロトコル（OSPF、静的、接続済み、または RIP）、プロトコルのメトリック値、および必要に応じて適用可能なルートポリシーを定義できます。

エンドポイント

Cisco EPN Manager は、イーサネット サブインターフェイス上の IP エンドポイントの作成をサポートします。タグなしカプセル化の選択、あるいは 802.1q または 802.1ad のカプセル化を使用した、外部 VLAN と、必要に応じて内部 VLAN の指定をサポートします。エンドポイント上の IPv4 アドレスと IPv6 アドレスの両方を指定できます。また、BGP および OSPF ネイバーの詳細を指定して、CE と PE の間で BGP および OSPF ネイバーをプロビジョニングすることもできます。

Cisco EPN Manager を使用して L3VPN サービスをプロビジョニングする方法については、L3VPN サービスのプロビジョニング （700 ページ）を参照してください。

L3VPN プロビジョニングの機能と制限事項

Cisco EPN Manager は次の L3VPN 機能をサポートしています。

- VRF の作成
- ルートターゲット ID の自動割り当て。
- ルート識別子の自動割り当て

- 複数の条件（VPN ID、共通名、およびプライムプロビジョニングの命名規則）に基づいて、複数の VRF で構成された VPN の検出。
- L3VPN プロビジョニング用のデバイスは、プロビジョニングをポイント アンド クリックの手法を使用して選択できます。
- VRF に付加された IP エンドポイントの定義。VRF とのイーサネット サブインターフェイスの関連付け。
- CE と PE 間での BGP または OSPF、あるいはその両方のネイバーのプロビジョニング。
- エンドポイント インターフェイスへの QoS プロファイルのアタッチ。
- 既存の VPN への新しい VRF の追加。
- Cisco EPN Manager を使用して作成し、展開された（または検出し、昇格させた）VPN と関連する VRF の変更。
- L3VPN サービスのネットワーク トポロジのオーバーレイ。
- デバイスから直接検出された L3VPN サービスの昇格。これは、検出されたサービスの変更と削除にさらに役立ちます。
- OSPF デュアル AS ルーティングによるルート ターゲットの使用。
- BDI/BVI インターフェイス（サブインターフェイス）を使用した L3VPN サービスをプロビジョニングするための、統合ルーティングとブリッジングの使用。
- IP サービス レベル契約（SLA）および CLI テンプレートと L3VPN サービスとの関連付け。
- 接続されたルート、静的ルート、RIP ルート、または OSPF ルートを使用した PE-CE リンクと MP-BGP コア間でのルートの再配布。
- LAG インターフェイスを使用した L3VPN サービスのプロビジョニング。
- HSRP を使用している L3VPN サービスのプロビジョニング。

Cisco EPN Manager には、L3VPN に次の制限事項があります。

- VRF をサポートするデバイスのリストについては、Cisco Evolved Programmable Network Manager のサポート対象デバイスを参照してください。
- マルチキャスト VPN をプロビジョニングすることはできません。サポートされているのは、ユニキャスト VPN のみです。
- L3VPN サービスの作成時、VPN に任意の数の VRF を追加できます。ただし、5 つを超える VRF を追加することはお勧めしません。[VRFの変更（Modify VRF）] オプションと [VRFの追加（Add VRF）] オプションを使用して、後でより多くの VRF を VPN に追加できます。L3VPN サービスには、緑色のフィールドを使用してプロビジョニングされている場合、最大 15 個のエンドポイントを含めることができます。

- デバイスごとにサポートされているのは 1 つの VRF のみです。複数の VRF を作成できますが、異なるデバイス上で同じ VRF 名か、または異なる VRF 名を使用できます。
- ルート ポリシーは選択できますが、L3VPN サービス内で定義することはできません。
- PE-CE では、BGP、OSPF、および OSPFv3 ルーティング プロトコルのみがサポートされています。
- 複数の接続された PE はサポートされていないため、Site of Origin サポートもありません。
- L3VPN サービスを削除すると、サービスに関連付けられている IP SLA 操作がデバイスから削除されます。また、関連付された操作が削除されると、その操作はそれ以降は使用できなくなります。
- 統合ルーティングおよびブリッジング（IRB）は、Cisco Catalyst 6500 シリーズ スイッチではサポートされていません。
- [Modify VRF] フローによるルート識別子の変更は、IOS XR デバイスでのみサポートされています。
- 最大 15 個のエンドポイントが、完全に検出された L3VPN サービスの昇格後の変更/削除でサポートされます。L3VPN プロモーションの**[最大エンドポイント数（Maximum Number of Endpoints）]** を設定するには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]**に移動し、**[回線/VC（Circuits/VCs）]** で **[検出設定（Discovery Settings）]** を選択します。

L3VPN プロビジョニングの前提条件

L3VPN サービスのプロビジョニングを開始する前に、次の前提条件に従っていることを確認します。

L3VPN サービスをプロビジョニングするための前提条件は次のとおりです。

- BGP は、すべてのデバイス上に設定する必要があります。通常、すべてのデバイスは、ルート リフレクタのペアを介して相互に通信する必要があります。
- BGP のセットアップに必要な構成前の変更：

  次の例に示すように、BGP ルータ ID を設定します。

  ```
  router bgp 65300
      bgp router-id 10.1.1.1
  ```

  次のコマンドを使用して、Vpn4 と Vpn6 を親アドレス ファミリとして設定します。

  ```
  router bgp 100
  address-family vpnv4 unicast
  address-family vpnv6 unicast
  ```

- MPLS 到達可能性は、デバイス間で設定する必要があります。MPLS コア ネットワーク設定をセットアップする必要があります。

- L3VPN サービスがプロビジョニングされるデバイスのインベントリ収集ステータスが [完了済み（Completed）] である必要があります。デバイスのステータスを確認するには、[インベントリ（Inventory）] > [ネットワーク デバイス（Network Devices）] に移動し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列のステータスを確認します。
- XE デバイスで IPv6 アドレスファミリを使用して L3VPN サービスをプロビジョニングする前に、IPv6 ルーティングを有効にする必要があります。IPv6 ルーティングを有効にするには、次のコマンドを設定します。

  ```
  ipv6 unicast-routing
  ```

- （オプション）L3VPN サービスのプロビジョニング時に L3VPN サービスを顧客に関連付けられるように、システム内に顧客を作成する必要があります。顧客を作成し、管理するには、[インベントリ）Inventory）] > [その他（Other）] > [顧客（Customers）] を選択します。

L3VPN サービスの検出

Cisco EPN Manager は、複数の条件を使用して複数の VRF を 1 つの VPN に関連付けます。

- VRF が VPN ID で設定されている場合：VPN サービスは VPN ID を使用して検出され、同じ VPN に属している VRF を識別します。検出する必要がある VPN があり、1 つの VPN 内で異なる VRF 名が使用されている場合、Cisco EPN Manager は VRF 名によって VRF を検出します。

  デバイスごとに作成される VRF が 1 つのみの場合は、VPN 上のあらゆる場所で同じ VRF 名を使用するのが一般的です。Cisco EPN Manager が同じ名前で VPN ID のない複数の VRF を確認した場合は、それらを単一の VPN と見なし、VPN 名は VRF の名前になります。

- 最初にプライム プロビジョニングを使用してプロビジョニングされた VPN の場合：Cisco EPN Manager はプライム プロビジョニング VRF 命名規則も認識します。プライム プロビジョニングで使用される命名規則は、次の形式です。

  V<number>:<VPN name><optional suffix, one of -s -h -etc>

  同じ名前と番号を持つ VRF は、同じ VPN に属しています。たとえば、「ABC」と呼ばれる VPN に属している VRF は次のとおりです。

  V1:ABC、V2:ABC、V4:ABC-s、V22:ABC-h、V001:ABC など

- VRF に VPN ID がなく、プライム プロビジョニング規則に従って他の名前と一致しない一意の名前を持つ場合は、単独で VPN に配置されます。VPN の名前は VRF の名前になります。

プライムプロビジョニング命名規則機能は、製品に埋め込まれた正規表現によって駆動されます。VPN の設定がオプションではなく、正規表現と一致する可能性がある命名規則がある場合は、その正規表現を変更できます。正規表現を変更するには、シスコ アドバンスト サービス担当者にお問い合わせください。

新規 L3VPN サービスの作成およびプロビジョニング

ユニキャスト L3VPN の作成およびプロビジョニング プロセスには、次の作業が含まれます。

- （オプション）顧客を VPN に関連付ける。
- L3VPN を経由してエンドポイントまで伝送されるトラフィックの処理方法に影響する属性の定義。
- L3VPN のエンドポイントおよびルート再配布値の指定。
- （オプション）IPv4 または IPv6 を使用するデバイス間のエンドツーエンド応答所要時間をモニターするための IP サービス レベル契約（SLA）動作を設定する。
- （オプション）ユーザー定義の CLI テンプレートを L3VPN サービスと関連付ける。

注：このリリースではユニキャスト L3VPN サービスのみがサポートされます。

新しい L3VPN サービスを作成するには、次の手順を実行します。

ステップ 1 左側のペインから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

ステップ 2 ツールバーで [デバイス グループ（Device Groups）] をクリックし、マップ上に表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブをクリックし、[回線/VC（Circuits/VCs）] ペイン ツールバーで [+]（[作成（Create）]）アイコンをクリックします。

マップの右側の新しいペインでプロビジョニング ウィザードが開きます。あるいは、[設定（Configuration）] > [ネットワーク（Network）] > [サービスのプロビジョニング（Service Provisioning）] を選択して L3VPN プロビジョニング ウィザードにアクセスすることもできます。

ステップ 4 [テクノロジー（Technology）] ドロップダウン リストから [L3VPN] を選択します。サポートされている L3VPN サービス タイプの一覧が表示されます。

ステップ 5 [サービス タイプ（Service Type）] セクションで、[ユニキャスト（Unicast）] を選択し、[次へ（Next）] をクリックして顧客とサービスの詳細を入力します。このリリースでサポートされているサービスタイプは、ユニキャスト L3VPN のみです。

ステップ 6 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。

ステップ 7 （オプション）VPN に関連付ける顧客を選択します。ドロップダウン リストに顧客が表示されていない場合は、[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customers）] を選択して顧客を作成し、この手順に戻ります。

ステップ 8 基本的な L3VPN パラメータを次のように指定します。

a) [アクティブ化（Activate）] チェックボックスを使用して、サービスをアクティブ状態にするか（チェックボックスがオン）、それとも非アクティブにするか（チェックボックスがオフ）を指定します。アクティブ状態の場合、トラフィックが回線を通過できるようになり、関連付けられているすべて

の IP エンドポイントのサービス状態が自動的に True に設定されます。非アクティブ状態の場合は、IP エンドポイントのサービス状態を True または False に設定できます。

b) 一意のサービス名を指定し、オプションで説明を入力します。

c) サービスの一意の VPN ID を入力します。VPN ID は、OUI:VPN インデックス形式である必要があります。たとえば、36B:3 などです。ここでは、36B は組織固有識別子（OUI）であり、3 は VPN インデックスです。

d) [IP MTU] フィールドに、値を 1500（デフォルト）～ 9216 の範囲で入力します。サービス MTU は、L3VPN 経由で非フラグメント化された状態で伝送できる最大 IP パケットサイズ（バイト数）です。これにはレイヤ 2 ヘッダーは含まれません。

設定されるインターフェイス MTU は、サービス MTU にすべてのレイヤ 2 ヘッダーのサイズを追加したものです。イーサネットの場合は、これによって 14 バイトおよび VLAN ヘッダーごとに 4 バイトが追加されます。

UNI MTU の値は、サービス MTU と外部および内部の VLAN 値によって異なります。

- 外部および内部 VLAN の両方が存在する場合、UNI MTU 値はサービス MTU + 14 +（4*2）より大きくなります。
- 外部 VLAN のみが存在する場合、UNI MTU 値はサービス MTU + 14 +（4 *1）より大きくなります。
- VLAN が存在しない場合、UNI MTU 値はサービス MTU + 14 より大きくなります。

e) （オプション）このサービスのフルメッシュトポロジを作成するには、[フルメッシュの作成（Create Full Mesh）] チェックボックスをオンにし、フル メッシュ プレフィックスを [新規プレフィックス（New Prefix）] フィールドに手動で入力するか、[既存のプレフィックス（Existing Prefix）] ドロップダウン リストから値を選択します。使用可能なオプションは、選択されたデバイスで検出されたフルメッシュプレフィックス値によって異なります。

f) アドレスファミリを [フルメッシュアドレスファミリ（Full Mesh Address Family）] ドロップダウンリストで [IPv4]、[IPv6]、または [両方（Both）] として選択します。

ステップ 9 [ルート ターゲットの割り当て（Route Target Allocation）] セクションを使用して、ルート ターゲット アドレス ファミリ（[IPv4]、[IPv6]、または [両方（Both）]）および関連付けられているルート ターゲット値を手動で指定します。1 つの L3VPN サービスに複数のルート ターゲットを作成できます。次の手順でこの L3VPN サービスに接続させる任意の VRF に、これらのルート ターゲットを関連付けることができます。

（注） また、VRF に関連付けられたルート ターゲットを、VRF が属する L3VPN にも関連付ける必要があります。

（注） 設定されたルートポリシーが、ルートポリシーの [エクスポート（Export）] ドロップダウンリストに表示されます。

ステップ 10 [展開アクション（Deployment Action）] ドロップダウンリストで、サービス作成プロセスの完了時に実行する必要があるタスクを指定します。選択できるオプションは、次のとおりです。

- [プレビュー（Preview）]：デバイスに展開する前に、生成された設定を確認できます。
- [展開（Deploy）]：完了したらすぐに、該当するデバイスに設定を展開できます。

ステップ 11 [次へ（Next）] をクリックして、VRF を L3VPN サービスに関連付けます。

ステップ 12 [VRF（VRFs）] ドロップダウン リストから必要な VRF を選択するか、または以下の説明に従って新しい VRF を追加し、[次へ（Next）] をクリックします。L3VPN サービスの作成中に、最大 5 つの VRF を VPN に関連付けることができます。さらに多くの VRF を VPN に関連付けるには、L3VPN サービスへの VRF の追加およびコピー（726 ページ）を参照してください。新しい VRF を作成するには、次の手順を実行します。

1. [+] アイコンをクリックして、VRF の詳細を手動で追加します。VRF の詳細を自動入力するには、マップ上で該当するデバイスをクリックします。デバイスの詳細および VRF の新しい名前が自動的に [VRF の追加（Add VRFs）] ページに入力されます。
2. 手動で VRF の詳細を指定するには、[デバイス（Device）] ドロップダウンリストで必要なデバイスを選択します。その後、VRF 名と説明を手動で入力し、[RD 自動] チェックボックスをオンにします。

   （注） 同じデバイスに複数の VRF を作成する場合は、それらが同じ VPN に属さないようにするために、それぞれ異なる名前を付ける必要があります。同じデバイス上に同じ名前で複数の VRF を作成することはできません。

ステップ 13 IPv4 および IPv6 ルート ターゲットとルート配布詳細を次のように指定します。

1. ルートターゲット：[ルートターゲット（Route Target）] ドロップダウンリストで、この VRF のルートターゲットを選択します。このドロップダウンリストに表示されるオプションは、ステップ 7 でこのサービスに関連付けられたルートターゲットによって決まります。
2. ルートターゲットを適用する方向を選択します。選択したデバイスに応じて、[インポート（Import）]、[エクスポート（Export）]、[両方（Both）]、または [なし（None）] を選択します。

   選択したデバイスのタイプに従って方向を選択します。たとえば Cisco IOS-XR デバイスの場合は、ルート ターゲットの方向として [なし（None）] を選択できません。
3. [ルート ポリシー（Route Policy）] セクションで、ルート ターゲットのインポートおよびエクスポート ポリシーを指定します。

   （注） オペーク拡張コミュニティ（Opaque Extended Community）が接続されている [ルートポリシー（Route Policy）] は、エクスポートにのみ適用されます。

4. [ルート配布（Route Distribution）] セクションで、VRF に関連付ける必要があるプロトコル、プロトコルのメトリック値、ルーティング プロセス ID、関連するルート ポリシー、およびルート一致タイプを指定します。
   - [プロトコル（Protocol）]：ルートの再配布元となる必要がある送信元プロトコルを選択します。選択できるオプションは、[静的（Static）]、[接続（Connected）]、[RIP]、および [OSPF] です。
   - [メトリック（Metric）]：（オプション）同じルータ上のルーティング プロセス間で再配布時に使用するメトリックの数値を入力します。
   - [ルーティング プロセス ID（Routing Process ID）]：（OSPF および RIP のみに適用可能）デバイス上のルーティング プロセスのインスタンスを識別する一意の数値を指定します。

- [ルート ポリシー（Route Policy）] :（オプション）選択したデバイス上に存在するいずれかのルート ポリシーを選択します。Cisco EPN Manager を使用してルート ポリシーを作成することはできません。

  （注） オペーク拡張コミュニティ（Opaque Extended Community）が接続されている [ルートポリシー（Route Policy）] は、再配布では使用できません。

- [ルート一致タイプ（Route Match Type）]（OSPF にのみ適用可能）：選択したルートポリシーに関連付けられている一致タイプをドロップダウンリストで指定します。

ステップ 14 IP エンドポイントおよび UNI の値を、次のように手動で指定します。

- エンドポイント インターフェイスがすでに UNI として設定されている場合は、[新規 UNI（New UNI）] チェックボックスをオフにし、[UNI 名（UNI Name）] ドロップダウン リストから必要な UNI を選択します。
- 新しい UNI を作成するには、次の手順を実行します。
  1. [新規 UNI（New UNI）] チェックボックスをオンにします。
  2. [UNI 名（UNI Name）] フィールドに、UNI の一意の名前を入力します。
  3. [デバイス（Device）] ドロップダウンで、デバイス、およびデバイスに必要なインターフェイスを選択して、UNI の説明を入力します。
  4. [サービス多重化（Service Multiplexing）] チェックボックスをオンにして、複数の L3VPN またはキャリア イーサネット サービスを UNI でサポートできるようにします。
  5. UNI の IP 最大伝送ユニット（MTU）（UNI の速度とデュプレックスの設定）を指定します。
  6. [自動ネゴシエーション（Auto Negotiation）] チェックボックスをオンにして UNI の速度とデュプレックスの設定を自動的に調整するか、[自動ネゴシエーション（Auto Negotiation）] チェックボックスをオフにして速度とデュプレックスの設定を手動で指定します。
  7. UNI での入力または出力トラフィック用の UNI QoS プロファイルを選択します。プロファイルの一覧には、デバイスで設定され、システムによって検出されるポリシーマップおよびユーザー定義の QoS プロファイルが含まれます。UNI QoS プロファイルを選択した場合は、これ以降の手順でサービス エンドポイントに個別の QoS ポリシーを追加できません。エンドポイントに特定の QoS ポリシーを追加するには、[UNI 入力 QoS プロファイル（UNI Ingress QoS Profile）] および [UNI 出力 QoS プロファイル（Egress QoS Profile）] フィールドの両方を空のままにしてください。

     （注） 入力および出力方向に対し、検出された 2 つの異なる QoS プロファイルを選択できますが、ユーザー定義 QoS プロファイルの場合は両方の方向に 1 つの QoS プロファイルだけを選択できます。

  8. [リンク OAM の有効化（Enable Link OAM）] を選択して IEEE 803.1ah リンクの動作およびメンテナンスを有効にします。リンク OAM が有効な場合、この UNI と顧客のアクセス スイッチの間のリンク状態に関連するイベントが表示されます。

9. [リンク管理の有効化（Enable Link Management）] を選択すると、顧客のアクセス スイッチでこの UNI、VLAN ID、UNI 上のサービスなどの情報を取得できるようになります。

UNI テーブルのフィールドおよび属性の詳細については、新規 UNI の詳細リファレンス （651 ページ）を参照してください。

ステップ 15 次の詳細を設定することで L3VPN に関連付けるサービスエンドポイントを指定し、[次へ（Next）] をクリックします。

- [VRF 名（VRF Name）]：この VPN に関連付けることができる VRF を 1 つ選択します。
- [IPv4およびIPv6アドレス（IPv4 and IPv6 address）]：サービスエンドポイントの IP アドレスおよびネットワークマスクを入力します。単にネットワーク マスクの長さを表す整数としてマスクを入力できます（または CIDR 形式も可能です）。
- [VLAN および内部 VLAN（VLAN and Inner VLANs）]：1 ～ 4094 までの整数を使用して、内部および外部の VLAN の識別子を入力します。内部 VLAN は、VLAN タギングの第 2 レベルの識別子です。
- [QoS ポリシー（QoS Policy）]：（オプション）サービス エンドポイントに適用する必要がある QoS ポリシーを選択します。上記のステップで UNI 入力/出力 QoS プロファイルをサービスに関連付けた場合は、このフィールドが無効になります。QoS プロファイルの作成については、Quality of Service（QoS）の設定 （554 ページ）を参照してください。

  （注） 入力および出力方向に対し、検出された 2 つの異なる QoS ポリシーを選択できますが、ユーザー定義の QoS ポリシーの場合は両方の方向に 1 つの QoS ポリシーだけを選択できます。

- [サービス状態（Service State）]：関連付けられた IP エンドポイントのサービス状態を True または False のいずれに設定する必要があるかを指定します。L3VPN がアクティブ状態の場合（上記のステップ 6 で指定）、このチェックボックスは無効になり、すべてのサービス状態値が自動的に True に設定されます。
- **[統合ルーティングおよびブリッジングの使用（Use Integrated Routing & Bridging）]**：サブインターフェイスまたは BVI（仮想）インターフェイスで VRF および IP アドレスを設定する必要があるかどうかを指定します。

  （注） このチェックボックスは、統合ルーティングおよびブリッジングをサポートするデバイス（Cisco ASR 90XX デバイスなど）を選択している場合にのみ有効になります。Cisco ASR90x およびその他の IOS-XE デバイスでは、BDI インターフェイスによって設定が処理されるため、[Use Integrated Routing & Bridging] チェックボックスをオフにすることはできません。

- （オプション）HSRP の詳細を指定するには、[HSRP の有効化（Enable HSRP）] チェックボックスをオンにします。HSRP の詳細のリファレンス （713 ページ）を参照してください。

ステップ 16 [次へ（Next）] をクリックして、[PE-CE ルーティング（PE-CE Routing）] ページに移動します。

ステップ 17 [+] アイコンをクリックして、PE-CE ルーティングの詳細を追加します。PE-CE ルーティングの詳細のリファレンス （715 ページ）を参照してください。

ステップ 18 （オプション）一覧から既存の IP SLA パラメータを選択するか、以下の表で説明する IP SLA 動作パラメータを指定して、[次へ（Next）] をクリックします。

IP SLA 設定	IP SLA パラメータ	説明
動作設定	[名前（Name）]	選択した L3VPN サービスに関する IP SLA 動作を識別する一意の名前を入力します。
	タイプ（Type）	この L3VPN サービスに参加するデバイス用に生成する必要がある IP SLA 動作のタイプを選択します。選択できるオプションは、次のとおりです。 • [UDP エコー（UDP Echo）]：応答所要時間を測定し、シスコ デバイスと IPv4 または IPv6 を使用するデバイスの間のエンドツーエンド接続をテストするように、IP SLA の User Datagram Protocol（UDP）エコー動作を設定します。 • [ICMP エコー（ICMP Echo）]：シスコ デバイスと、IPv4 または IPv6 を使用するその他のデバイス（後述する送信元/宛先値）との間のエンドツーエンド ネットワーク応答所要時間を測定できるようにします。[ICMP エコー（ICMP Echo）] タイプの IP SLA 動作で、[接続損失（Connection Loss）] アクション変数を関連付けることはできません。 • [UDP ジッター（UDP Jitter）]UDP ジッター動作を設定します。これにより、IPv4 または IPv6 ネットワークで UDP トラフィックを伝送するネットワークのラウンドトリップ遅延、一方向遅延、一方向ジッター、一方向パケット損失、および接続を分析できます。
	ソース（Source）	IP SLA 設定の生成の送信元ポイントとして機能するデバイスを指定します。IP SLA 応答は、この送信元デバイスと宛先デバイスの間の接続に基づいて生成されます。この動作の VRF 値は、送信元の選択に応じて自動的に選択されます。
	送信元ポート（Source Port）	0 ～ 65535 の範囲の数値を 1 つ入力し、IP SLA 動作の設定対象となる送信元ポートの値を指定します。
	[接続先（Destination）]	IP SLA 設定の生成の宛先ポイントとして機能するデバイスを指定します。IP SLA 応答は、送信元デバイスとこの宛先デバイス間の接続に基づいて生成されます。
	[宛先ポート（Destination Port）]	0 ～ 65535 の範囲の数値を 1 つ入力し、IP SLA 動作の生成対象となる宛先ポート値を指定します。
	VRF	VRF の詳細は、IP SLA 動作の送信元として指定したデバイスに基づいて自動的に選択されます。

IP SLA 設定	IP SLA パラメータ	説明
反応設定	アクション変数（Action Variable）	IP SLA 反応をトリガーする条件となる変数を選択します。たとえば、モニターリング対象の値が指定のレベルを超えるか下回った場合、またはタイムアウトや接続損失などのモニターリング対象のイベントが発生した場合です。 • [接続損失（Connection Loss）]：接続損失が発生した場合にイベントをトリガーする必要があることを指定します。動作のタイプとして [ICPM エコー（ICPM Echo）] を選択した場合、この値は表示されません。 • [ラウンドトリップ時間（Round Trip Time）]：このアクション変数を選択した場合、[上限しきい値（Upper Threshold Value）] および [下限しきい値（Lower Threshold Value）] を入力する必要があります。これらは、モニタリング対象の値が特定の上限しきい値を超えるか下限を下回った場合に、イベントをトリガーする必要があることを示します。 • [タイム アウト（Time Out）]：指定された一連のタイムアウトが連続して発生した場合に、イベントをトリガーする必要があることを示します。 • [エラーの確認（Verify Error）]：VerifyError タイプのエラーが発生した場合に、イベントをトリガーする必要があることを示します。
	アクションタイプ	[アクション変数（Action Variable）] フィールドに設定された条件に基づいて実行する必要のあるアクションを、次の中から 1 つ選択します。 • [なし（None）]：アクションは実行されません。 • [トラップおよびトリガー（Trap and Trigger）]：違反条件に一致した場合に、以下の [トラップのみ（Trap Only）] および [トリガーのみ（Trigger Only）] オプションの定義に従って、両方の SNMP トラップをトリガーし、別の IP SLA 動作を開始します。 • [トラップのみ（Trap Only）]：モニター対象の要素で特定の違反タイプが発生した場合に、SNMP ロギング トラップを送信します。 • [トリガーのみ（Trigger Only）]：違反条件に一致した場合に、1 つ以上のターゲット動作の動作状態を [保留（pending）] から [アクティブ（active）] に変更します。ターゲット動作は、ターゲット動作のライフタイム値の設定に従い、その存続期間が満了するまで続行されます。トリガーされたターゲット動作が再びトリガーされるには、その前に存続期間が終了している必要があります。

IP SLA 設定	IP SLA パラメータ	説明
	しきい値タイプ（Threshold Type）	IP SLA イベントの生成条件とするしきい値タイプを選択します。 • [平均（Average）]：このしきい値タイプを選択する場合は、[N値（N Value）] を入力します。これは、指定された上限しきい値を超えるか下限しきい値を下回り、N プローブの合計値の平均に達した場合に、イベントをトリガーする必要があることを示します。 • [連続（Consecutive）]：このしきい値タイプを選択する場合は、反応設定の一部として [連続値（Consecutive Values）] を入力してください。このしきい値タイプは、指定回数を超えて違反が連続発生した場合にのみ、イベントをトリガーします。たとえば連続値 5 を入力して連続違反タイプを使用した場合、タイムアウトが 5 回連続して発生した場合、またはラウンドトリップ時間が上限しきい値を 5 回連続して超えた場合にアクションが実行されます。 • [即時（Immediate）]：反応タイプ（応答所要時間など）の値が上限しきい値を超えるか下限しきい値を下回った場合、またはタイムアウト、接続の切断、エラーの検証イベントが発生した場合に、即座にイベントをトリガーします。 • [しない（Never）]：イベントをトリガーしません。 • [X/Y 回（X out of Y occurrences）]：このしきい値タイプを選択した場合は、[X 値（X Values）] および [Y 値（Y Values）] を入力して、発生回数を指定します。これを選択すると、y 回のプローブ動作内に x 回の違反が発生した場合に（x 回/y 回）、イベントがトリガーされます。

IP SLA 設定	IP SLA パラメータ	説明
単純なスケジュール（Simple Schedule）	-	次の値を入力して、個別の IP SLA 動作のスケジュール パラメータを入力します。 • [頻度（Frequency）]：経過時間を秒数で入力します。この時間内に動作が繰り返されます。 • [ライフ タイム（Life Time）]：動作がアクティブ状態に保たれる時間の合計を秒数で入力します。単一の動作は、その動作のライフタイム中に、指定された頻度で繰り返し実行されます。 • [エージアウトする（Age Out）]：動作をアクティブ状態に保つ時間の長さを秒数で入力します。たとえば、エージ アウトの値を 43200 に指定すると、非アクティブ状態が 12 時間続いた後で動作がエージアウトします。 • [今すぐ開始（Start Now）] および [後で開始（Start After）]：[今すぐ開始（Start Now）] チェックボックスをオンにすると、保存後ただちに IP SLA 動作を実行するようにスケジュールされます。または [後で開始（Start After）] フィールドを使用し、分数を指定すると、その経過後に動作が実行されます。

ステップ 19 （オプション）[サービス テンプレート（Service Template）] ページを使用すると、サービスに参加するデバイスに設定される追加の CLI コマンドを含むテンプレートを付加できます。詳細については、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

ステップ 20 サービスに必要な情報をすべて入力したら、[送信（Submit）] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合、プレビューがこの時点で表示され、[属性の編集（Edit Attributes）] をクリックして L3VPN 属性を変更できます。そうでない場合は、設定が即座にデバイスに展開されます。

サービスに参加しているデバイスのうち 1 台でも展開に失敗した場合は、サービスに参加しているすべてのデバイスで設定がロールバックされます。サービスに関連付けられているエンドポイントを削除するには、L3VPN サービス エンドポイントの削除 （834 ページ）を参照してください。この L3VPN サービスにさらに VRF を追加するには、L3VPN サービスへの VRF の追加およびコピー （726 ページ）を参照してください。

HSRP の詳細のリファレンス

Hot Standby Router Protocol（HSRP）は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファースト ホップ冗長性を確保することでネットワークの可用性を高めるシスコの標準方式です。Hot Standby Router Protocol（HSRP）は、IP ネットワークに冗長性をもたらし、ユーザー トラフィックが確実に最初のホップ ルータ障害から即座かつ透過的に回復できるようにします。HSRP を使用すると、1 つの LAN 上の複数のルータが、ホ

スト上のデフォルトゲートウェイとして設定された仮想IPとMACアドレスを共有できます。HSRP グループで設定されたルータのグループには、アクティブルータとして選択された 1 台のルータと、スタンバイルータとして選択されたもう 1 台のルータがあります。アクティブルータは、仮想 IP アドレスに送信されるパケットを転送するロールを担います。アクティブルータで障害が発生すると、スタンバイ ルータが新しいアクティブ ルータのロールを引き継ぎます。Cisco EPN Manager では、IP ベースまたは IP サービスイメージを実行するスイッチでは IPv4 用の HSRP がサポートされており、IPv6 用の HSRP はユニキャストルーティングでサポートされています。HSRPは、アドレス ファミリ IPv6 の IOS-XE デバイスではサポートされていません。次の表に、HSRP 属性のリストを示し、説明します。

表 *43 : HSRP* 設定

属性	説明
グループ番号（Group Number）	IOS-XE デバイスまたは IOS-XR デバイスのスタンバイ グループ番号を入力します。推奨される値の範囲は次のとおりです。 • IOS-XE の値の範囲：0 ～ 255 • IOS-XR の値の範囲：1 ～ 4095
仮想 IP（Virtual IP）	IPv4/IPv6 アドレスを入力します。仮想 IP アドレスと SEP アドレスが同じサブネット内に入力されていることを確認します。
プライオリティ（Priority）	優先度を入力して、プライマリ ルータにするルータを決定します。 優先順位の値の範囲：0 ～ 255
Hello タイマー（Hello Timer）	hello パケット間の時間を秒単位で入力します。 （注） [Helloタイマー（Hello Timer）] と [最小遅延（Minimum Delay）] の値を指定した IOS-XR デバイスでは、[ホールドタイマー（Hold Timer）] と [リロード遅延（Reload Delay）] の値を入力する必要があります。 Hello 時間値の範囲：1 ～ 255
最小遅延（Minimum Delay）	最小遅延時間を秒単位で入力します。 遅延値の範囲：0 ～ 10000
プリエンプト最小遅延（Preempt Minimum Delay）	ルータのプリエンプト遅延を指定します。 遅延値の範囲：0 ～ 3600
認証キー（Authentication Key）	グループ番号が 1 ～ 255 の場合は、認証キーを入力します。これにより、認証メッセージを HSRP マルチキャストに含めることができます。これにより、承認されたルータのみが HSRP グループに確実に含まれます。

属性	説明
ホールド タイマー（Hold Timer）	保留時間を秒単位で入力します。 保留時間値の範囲：1 ～ 255 （注） 保留時間は、XE デバイスの hello タイマーよりも長くする必要があります。
リロード遅延（Reload Delay）	リロードの遅延時間を入力します。 遅延値の範囲：0 ～ 10000
プリエンプト リロード遅延（Preempt Reload Delay）	プリエンプト再読み込み遅延を入力します。 遅延値の範囲：0 ～ 3600 このフィールドは、IOS-XR デバイスではサポートされていません。

PE-CE ルーティングの詳細のリファレンス

次の表に、レイヤ 3 VPN サービスをプロビジョニングするための PE-CE を定義する属性のリストを示し、説明します。

表 *44 : PE-CE* ルーティングのリファレンス

属性	説明
ルーティング プロトコル設定（Routing Protocol Settings）	
PE デバイス（PE Device）	擬似回線デバイスの名前。
VRF	ウィザードの [VRF] ページで指定した VRF 名が読み込まれています。
ルーティング プロトコル タイプ（Routing Protocol Type）	**[BGP]**、**[OSPF]**、または **[OSPFv3]** をレイヤ 3 VPN サービスのルーティングプロトコルとして選択します。 （注） 選択したルーティング プロトコルに基づいて、[BGP ネイバー情報（BGP Neighbor Information）] セクションまたは [OSPF プロセス情報（OSPF Process Information）] セクションが表示されます。 XR デバイスおよび XE デバイスの場合、PE-CE 認証はルーティング プロトコル タイプと認証タイプの選択に基づきます。詳細については、「PE-CE 認証」テーブルを参照してください。
アドレス ファミリ（Address Family）	アドレス ファミリを IPv4 または IPv6 として選択します。 （注） IPv6 は OSPF ルーティング プロトコルではサポートされていません。

属性	説明
認証タイプ（Authentication Type）	認証タイプを選択します。MD5認証タイプのみがサポートされます。 （注） [認証タイプ（Authentication Type）] フィールドは、ルーティング プロトコルとして OSPF または OSPFv3 を選択した場合にのみ使用できます。
BGP ネイバー情報（BGP Neighbor information） （注） このセクションは、ルーティング プロトコルとして BGP を選択した場合にのみ使用できます。	
ネイバー アドレス（Neighbor Address）	ネイバーの IP アドレスを入力します。
ネイバーAS（Neighbor AS）	このネイバーの自律システム番号を入力します。これは、BGP ネイバーとのピアリング セッションを確立するために使用される固有識別子です。
入力ルート ポリシー（Ingress Route Policy）	このネイバーから受信した BGP ルートに適用されるルート ポリシーを入力します。
出力ルート ポリシー（Egress Route Policy）	このネイバーに送信されるルートに適用するルート ポリシーを入力します。
ローカル AS（Local AS）	BGP ネイバーとのピアリング セッションを確立するために使用される固有のローカル識別子を入力します。

属性	説明
AS アクション（AS Action）	ローカル自律システム（AS）番号に関連付ける必要があるアクション タイプを、次の中から 1 つ選択します。 • [付加（Prepend）]：このオプションを使用すると、ネイバーから受信するルートに AS 番号を付加するように BGP が設定されます。 • [付加しない（No Prepend）]：このオプションを使用すると、ネイバーから受信するルートに AS 番号を付加しないように BGP が設定されます。 • [付加しない（No Prepend）]、[AS を置換（Replace AS）]：[AS を置換（Replace AS）] を使用すると、（ip-address で設定された）ローカル AS 番号のみが AS_PATH 属性に付加されます。ローカル BGP ルーティング プロセスからの AS 番号は付加されません。 • **[付加しない（No Prepend）]、[AS を置換（Replace AS）]、[デュアル AS（Dual AS）]**：デュアル AS オプションを使用して、ピアリングセッションを確立するように eBGP ネイバーを設定します。これを行うには、AS 番号（ローカル BGP ルーティングプロセスから）または ip-address 引数で設定された AS 番号（local-as）を使用します。

OSPF プロセス情報（OSPF Process Information）

（注） このセクションは、ルーティング プロトコルとして OSPF または OSPFv3 を選択した場合にのみ使用できます。

自動生成プロセス ID	デフォルトでは、このチェックボックスがオンになっており、プロセス ID が自動生成されます。 （注） このチェックボックスは、IOS-XR デバイスにのみ適用されます。
既存プロセス ID	**[自動生成プロセス ID（Auto Generate Process ID）]** チェックボックスをオフにすると、既存のプロセス ID から選択できます。
ルータ ID（Router ID）	OSPF プロトコルの IPv4 アドレスを指定します。
エリア ID（Area ID）	OSPF プロトコルのエリアを定義します。有効範囲は 0 ～ 4294967295 です。
メトリック	OSPF プロトコルの数値を指定します。
ドメイン タイプ（Domain Type）	必要なドメイン タイプを選択します。

属性	説明
ドメイン値（Domain Value）	6 オクテットの 16 進数形式でドメイン値を入力します。たとえば、00000000000F などです。
BFD 最小間隔（BFD Min Interval）	制御パケットがネイバーに送信される最小間隔を入力します。範囲は 3 ～ 30000 ミリ秒です。
BFD Min Rx	最小 Rx 値を入力します。範囲は 3 ～ 30000 ミリ秒です。
BFD の乗数（BFD Multiplier）	この乗数は、BFDがネイバーのダウンを宣言するまでのパケットが失われる回数です。OSPF プロトコルの範囲は Cisco IOS-XR では 2 ー 50、Cisco IOS-XR デバイスでは 3 ー 50 です。
BFD 高速検出（BFD Fast Detect）	隣接する転送エンジン間のパスで障害を迅速に検出するには、このチェックボックスをオンにします。

（注） EPNM では、対象の L3VPN インスタンスの PE-CE ルーティング用に作成できる OSPF プロセスは 1 つだけです。XE プラットフォームの場合はこれで十分です。これは、単一の OSPFv3 プロセスで IPv4 と IPv6 の両方のアドレスファミリを管理できるためです。ただし、IOS-XR プラットフォームでは、OSPFv3 は IPv6 のみをサポートし、IPv4 をサポートしません。お客様が IPv4 と IPv6 の両方のアドレスファミリを使用する場合、OSPF と OSPFv3 の両方のプロセスを EPNM から作成する必要があります。

PE-CE 認証

次の表に、XE デバイスと XR デバイスの選択に基づいた PE-CE 認証のルーティング プロトコルと認証タイプの関連する組み合わせのリストを示します。

表 *45 : PE-CE* 認証のリファレンス

デバイス（**Device**）	ルーティング プロトコル（**Routing Protocol**）	認証タイプ（**Authentication Type**）	パスワード タイプ（**Password Type**）
XE	BGP	—	次のオブション ボタンのいずれかをクリックします。 • [プレーン テキスト（Plain Text）] : パスワードを入力できるようにします。 • [暗号化（Encrypted）] : パスワードとして16進数値を入力できるようにします。
	OSPF	—	—
	OSPFv3	キーチェーン認証タイプのみが使用できます。 [キーチェーン（Key Chain）] ドロップダウン リストから、デバイス上に設定されている認証キーチェーンを選択します。	—

デバイス（Device）	ルーティング プロトコル（Routing Protocol）	認証タイプ（Authentication Type）	パスワード タイプ（Password Type）
XR	BGP	—	次のオブション ボタンのいずれかをクリックします。 • [プレーン テキスト（Plain Text）]：パスワードを入力できるようにします。 • [暗号化（Encrypted）]：パスワードとして16進数値を入力できるようにします。
	OSPF	MD5 またはキーチェーンを選択します。	次のオブション ボタンのいずれかをクリックします。 • [プレーン テキスト（Plain Text）]：パスワードを入力できるようにします。 • [暗号化（Encrypted）]： パスワードとして16進数値を入力できるようにします。
	OSPFv3	認証タイプとして、[IPSec - MD5] または [IPSec-SHA1] のいずれかを選択します。	次のオブション ボタンのいずれかをクリックします。 • [プレーン テキスト（Plain Text）]：パスワードを入力できるようにします。 • [暗号化（Encrypted）]： パスワードとして16進数値を入力できるようにします。

設定例：L3VPN サービスのプロビジョニング

次に、以下のパラメータを使用して Cisco ASR 9000 デバイスに展開する設定例を示します。

- BDI（仮想）インターフェイルでの VRF アドレスと IP アドレス（IPv4 と IPv6 の両方）の作成。
- OSPF プロトコルを BGP プロトコルの再配布。

例：Cisco ASR 9000 デバイスの BVI 対応インターフェイス（サブインターフェイス）での L3VPN サービスのプロビジョニング。

```
  vrf vrfrbvibdi9k
  vpn id aaaaaa:21
  address-family ipv4 unicast
    import route-target
      6:55
  address-family ipv6 unicast
    import route-target
      6:55
    export route-target
      6:55
interface GigabitEthernet0/0/0/17
  no shutdown
  exit
interface GigabitEthernet0/0/0/17.1
  encapsulation dot1q 1198
  shutdown
interface BVI 1
  vrf   vrfrbvibdi9k
  ipv4 address 88.7.6.4 255.224.0.0
l2vpn
  bridge group BDI1
    bridge-domain 1
      routed interface BVI 1
      interface GigabitEthernet0/0/0/17.1
router bgp 140
  vrf  vrfrbvibdi9k
    rd auto
    address-family ipv6 unicast
    address-family ipv4 unicast
      exit
    exit
  exit
```

例：OSPF ルート配布を使用して L3VPN サービスをプロビジョニングするための BVI 対応インターフェイスの使用（デュアル AS を使用）。

```
vrf definition VRF2-2VRF-2UNI-BDI
  vpn id AAAAAA:2
  rd 532533:2
  address-family ipv4
    route-target import 6:5
    route-target export 6:5
  address-family ipv6
    route-target export 6:5
interface GigabitEthernet0/0/0
  duplex full
  service instance 2 ethernet
    encapsulation dot1q 761
    bridge-domain 14
    shutdown
  exit
interface BDI14
  vrf forwarding VRF2-2VRF-2UNI-BDI
  ip address 5.44.3.7 255.255.0.0
router bgp 120
  address-family ipv4 vrf VRF2-2VRF-2UNI-BDI
    neighbor 55.4.3.2 remote-as 71
    neighbor 55.4.3.2 activate
    redistribute rip metric 6
    neighbor 55.4.3.2 local-as 387
  address-family ipv6 vrf VRF2-2VRF-2UNI-BDI
```

```
  neighbor c5::98 remote-as 50
  neighbor c5::98 activate
  redistribute ospf 65 match external metric 2
  neighbor c5::98 local-as 324 no-prepend replace-as dual-as
  exit
exit
```

L3VPN サービスの詳細表示

Cisco EPN Manager を使用すると、次の方法で L3VPN サービスに関する詳細情報を表示できます。

- [回線/VC 360（Circuit/VC 360）] ビューの使用：[回線/VC 360（Circuit/VC 360）] ビューには、Cisco EPN Manager を使用して作成された特定の L3VPN に関する詳細情報が表示されます。「回線/VC の表示」を参照してください。L3VPN サービスに関連付けられているさまざまなパラメータは、[要約（Summary）]、[VRF（VRFs）]、[サイトの詳細（Site Details）]、[HSRP]、[PE-CE ルーティング（PE-CE Routing）] の 5 つのタブに表示されます。

（注） サービス検出時に HSRP のさらに詳しい説明を表示するには、[サイトの詳細（Site Details）] タブをクリックし、IP エンドポイントから行を選択します。また、選択した OSPFv3 ルーティング プロトコル タイプと IPv6 アドレス ファミリの 6VPE 認証プロパティを表示するには、[PE-CE ルーティング（PE-CE Routing）] タブをクリックします。

- [ネットワーク トポロジ（Network Topology）] と [サービスの詳細（Service Details）] ビューの使用：[ネットワーク トポロジ（Network Topology）] ウィンドウには、デバイスのグラフィカルなトポロジ マップ ビュー、デバイス間のリンク、デバイスまたはリンクのアクティブ アラームが示されます。また、表示されたトポロジ マップ内で L3VPN を視覚化することもできます。
  - L3VPN とその詳細の完全なリストを表示するには、トポロジ ウィンドウのデバイス グループの回線/VC リストの表示 （814 ページ）を参照してください。回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビューを参照してください。
  - 特定のデバイスの L3VPN サービスの詳細を表示するには、「特定のデバイスの回線/VC の表示」を参照してください。
- **アラーム テーブルの使用**：Cisco EPN Manager のアラーム テーブルには、L3VPN サービスに問題があるかどうかを一目で確認する方法がいくつかあります。「回線/VC のエラーのチェック」を参照してください。

HSRP のより詳細な説明の表示

ホット スタンバイ ルーティング プロトコル（HSRP）の詳細を使用して L3VPN サービスを作成した後、[回線 360/拡張詳細（Circuit 360/extended details）] ビューで HSRP プロパティを表示できます。

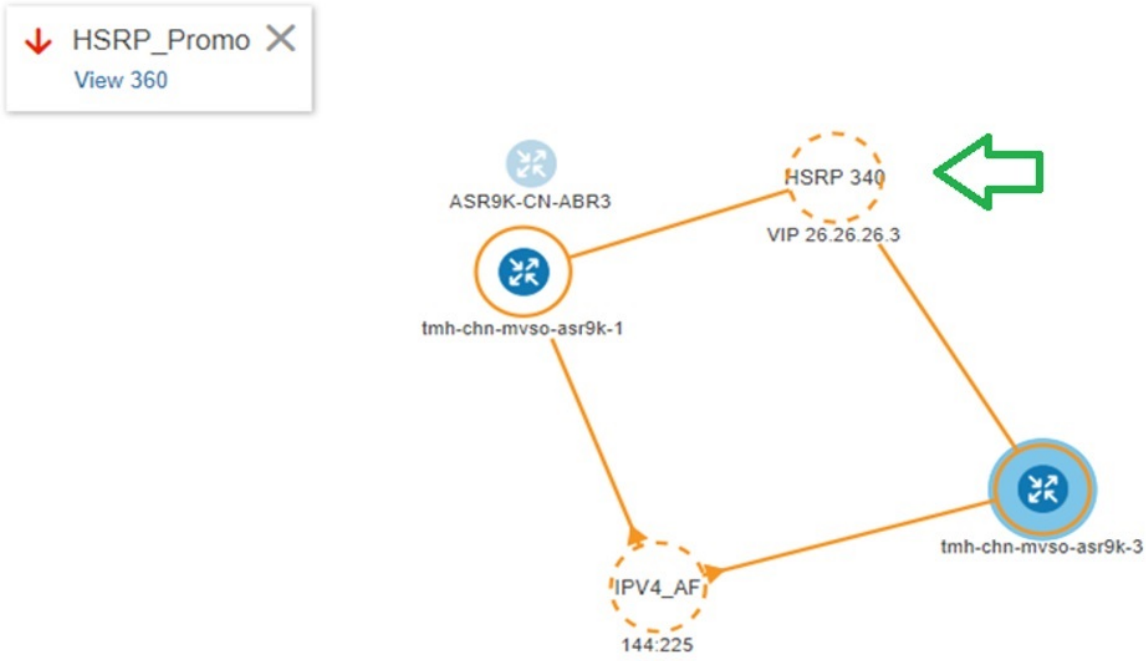
ステップ 1 左側のペインから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

ステップ 2 ツールバーから [デバイス グループ（Device Groups）] をクリックした後、L3VPNサービスをフィルタ処理して表示します。

ステップ 3 図に示すように、L3VPN サービスを選択して HSRP のオーバーレイを表示します。

図 *13 : オーバーレイ : HSRP*



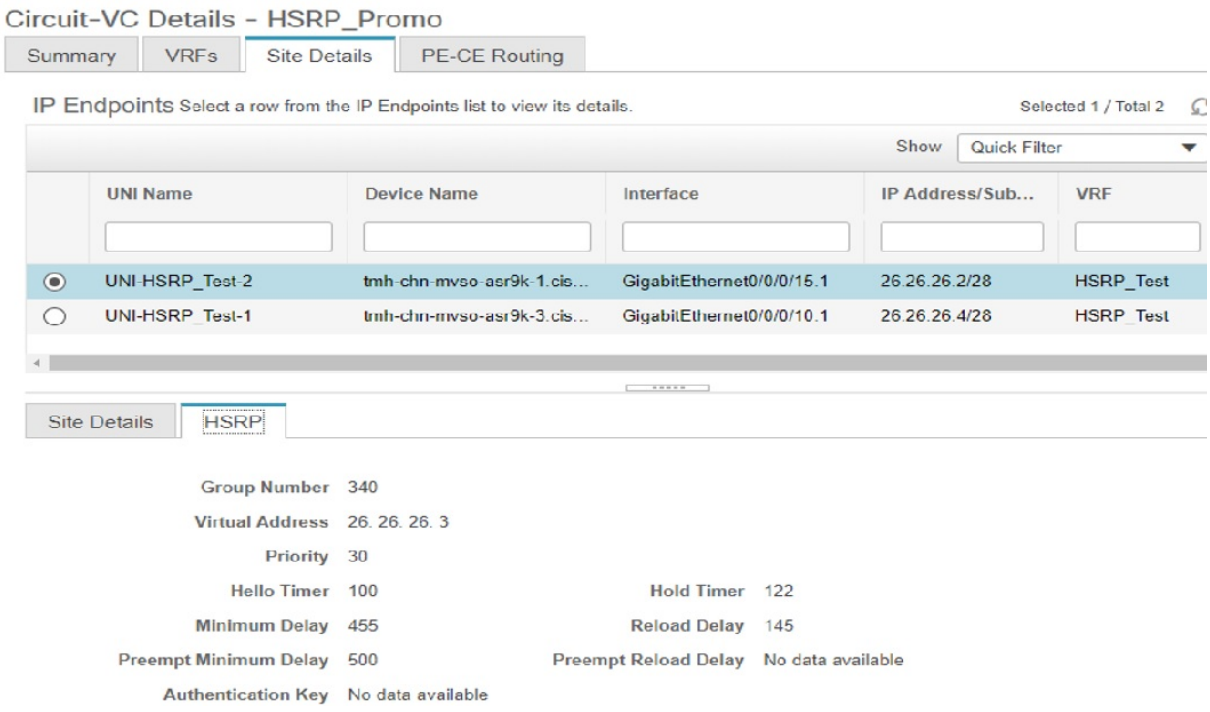
ステップ 4 HSRP ノードまたはそれに接続されているリンクをクリックし、次に示す HSRP に関連する詳細を表示します。

図 *14 : HSRP* の詳細

ステップ 5 HSRP のより詳しい説明を表示するには、次の手順を実行します。

- [360 度表示（View 360）] ハイパーリンクをクリックします。[回線/VC 360*（Circuit/VC 360*）] ページが表示されます。
- [表示（View）] > [詳細（Details）] を選択します。
- [回線/VC の詳細（Circuit-VC Details）] ウィンドウで、[サイトの詳細（Site Details）] タブをクリックします。
- IP エンドポイントを選択した後、[HSRP] タブをクリックしてプロパティを表示します。

図 *15 :* より詳細な説明（***Extended Details***）



L3VPN および VRF の変更

Cisco EPN Manager を使用して作成されて展開された L3VPN サービスには変更を加えることができます。サービスに関連付けられているフルメッシュプレフィックス、QoS プロファイル、ルートターゲット値、OSPF 設定は変更できますが、サービスに関連付けられている顧客の詳細、VPN 名、サービス MTU 値などのパラメータを変更することはできません。これらのパラメータを変更するには、サービスを削除してから新しい値を設定してサービスを再作成する必要があります。また、L3VPN サービスに関連付けられている VRF を変更することもできます。

L3VPN サービスおよび VRF を変更するには、次の手順に従います。

始める前に

Cisco EPN Manager を使用して検出されてプロモートされた L3VPN サービスに変更を加えるには、L3VPN サービスのルート識別子が **rd device_ip:number** の形式で指定されていることを確認する必要があります。次に例を示します。

```
vrf definition vdvvgfr420
  rd 10.104.120.133:420
  vpn id 36B:420
  !
address-family...
```

ルート識別子が他の形式で指定されている場合、サービスを編集することはできません。

ステップ 1 **[マップ（Maps）] > [ネットワーク トポロジ（Network Topology）]** に移動します。

ステップ 2 [回線/VC（Circuits/VCs）] タブをクリックし、変更を加える L3VPN サービスを選択します。

ステップ 3 鉛筆（変更）アイコンをクリックします。

ステップ 4 選択した L3VPN に変更を加えるには、[VPN の変更（Modify VPN）] を選択し、[次へ（Next）] をクリックします。

[プロビジョニング（Provisioning）] ウィザードに、選択した L3VPN に関連付けられている VRF、エンドポイントおよびその他の詳細が表示されます。

ステップ 5 必要に応じて、[IP MTU] の値を変更できます。

ステップ 6 選択した L3VPN に関連付けられている VRF を変更するには、[VRF の変更（Modify VRF）] を選択し、[次へ（Next）] をクリックします。

[プロビジョニング（Provisioning）] ウィザードに、選択した L3VPN に関連付けられている VRF、エンドポイントおよびその他の詳細が表示されます。既存の VRF パラメータを変更するだけでなく、新しいルート ターゲット値を VRF に関連付けることもできます。

VRF を変更する際に、UNI に関連付けられている QoS プロファイルを変更することはできませんが、サービス エンドポイントに関連付けられている QoS ポリシーは変更できます。

（注） 選択した L3VPN に関連付けられている VRF 名とデバイスを変更することはできません。

ステップ 7 必要に応じて変更した後、[送信（Submit）] をクリックしてデバイスに展開される設定をプレビューします。

（注） VPN を変更する際に、VPN に関連付けられている VRF を変更することはできません。VRF を変更する場合は、L3VPN サービスへの VRF の追加およびコピー （726 ページ）を参照してください。

ステップ 8 変更内容を確認してから [展開（Deploy）] をクリックしてデバイスに変更を展開します。

サービスに参加しているデバイスのうち 1 台でも展開に失敗した場合は、サービスに参加しているすべてのデバイスで設定がロールバックされます。

ステップ 9 変更が保存されていることを確認するには、L3VPN サービスの詳細を表示します。L3VPN サービスの詳細表示 （722 ページ） を参照してください。

L3VPN サービスへの VRF の追加およびコピー

Cisco EPN Manager を使用して、新しい VRF を作成したり、それを既存の L3VPN サービスに関連付けたりすることができます。また、L3VPN サービス用に新しい VRF を作成するため、ルート ターゲットやその他の詳細を既存の VRF からコピーすることもできます。

新しい VRF を L3VPN サービスに関連付けるには、以下の手順を実行します。

ステップ 1 **[マップ（Maps）] > [ネットワーク トポロジ（Network Topology）]** に移動します。

ステップ 2 [回線/VC（Circuits/VCs）] タブをクリックして、新しい VRF を関連付ける L3VPN サービスを選択します。

また、[設定（Configuration）] > [ネットワーク（Network）] > [サービス プロビジョニング（Service Provisioning）] の順に選択することによって、[L3VPN プロビジョニング（L3VPN Provisioning）] ウィザードにアクセスすることもできます。

ステップ 3 鉛筆（変更）アイコンをクリックします。

[L3VPN プロビジョニング（L3VPN Provisioning）] ウィザードが表示されます。

ステップ 4 [VRF の追加（Add VRF）] を選択して、[次へ（Next）] をクリックします。

ステップ 5 [+] アイコンをクリックして、新しい VRF の詳細を手動で追加します。VRF の詳細を自動入力するには、マップでデバイスをクリックし、その VRF を選択します。デバイスの詳細と VRF の新しい名前は、VRF のページに自動的に入力されます。

ステップ 6 [コピー元（Copy From）] ドロップダウン リストをクリックして必要な VRF を選択し、既存の VRF から VRF の詳細をコピーできます。

選択した L3VPN に関連付けられたそれらの VRF のみが、VRF ルート ターゲットおよびルート再配布の詳細とともに表示されます。

ステップ 7 それ以外の場合は、選択した VPN サービスに追加する VRF の詳細を手動で指定します。さまざまな VRF パラメータの詳細については、「新規 L3VPN サービスの作成およびプロビジョニング」を参照してください。

ステップ 8 エンドポイントや BGP ネイバーの詳細の追加など必要な変更を加え、[送信（Submit）] をクリックします。

ステップ 9 デバイスに導入する設定をプレビューし、必要な変更を加え、[導入（Deploy）] をクリックしてデバイスへの変更を導入します。

導入された変更を確認するには、選択した L3VPN サービスの詳細を表示します。「L3VPN サービスの詳細表示」を参照してください。

L3VPN サービスの変更や削除の詳細については、L3VPN サービス エンドポイントの削除 （834 ページ）および L3VPN および VRF の変更 （725 ページ）を参照してください。

回線エミュレーション サービスのプロビジョニング

Cisco EPN Manager CEM のプロビジョニング サポートの概要

Cisco EPN Manager は、回線エミュレーション（CEM）サービスのプロビジョニングをサポートします。CEM は、従来の TDM ネットワークとパケット スイッチド ネットワーク（PSN）の間のブリッジを提供します。これは、TDM データをパケットにカプセル化し、適切なヘッダーを付与して、それらのパケットをPSN経由で宛先ノードに送信します。詳細については、サポートされる回線エミュレーション サービス （621 ページ）を参照してください。

さらに、MPLS TE トンネルを CEM サービスに割り当て、CEM サービスがネットワークを通過できるようにすることができます。プロビジョニング ウィザードの [優先パス（Preferred Path）] ドロップダウン リストを使用して、CEM サービスに MPLS TE トンネルを割り当てます。詳細については、CEM サービスの詳細 （730 ページ）を参照してください。

（注） 優先パスで選択されたトンネルに十分な帯域幅がない場合、CEM サービスのプロビジョニングは失敗します。

CEM プロビジョニングの前提条件

CEM サービスをプロビジョニングするには、次の前提条件を満たしている必要があります。

- CEM サービスの発信側と着信側のエンドポイントで、IP/MPLS 接続を有効にする必要があります。
- ループバック インターフェイスや ACR グループなどの CEM 設定を、CEM サービスで使用されるデバイスで設定する必要があります。詳細については、回線エミュレーションの設定 （406 ページ）を参照してください。
- CEM サービスがプロビジョニングされるデバイスのインベントリ収集ステータスが、[完了済み（Completed）] である必要があります。これを確認するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、[最後のインベントリ収集ステータス（Last Inventory Collection Status）] 列でステータスを確認します。
- オプションで、顧客をシステムに作成して、サービスの作成中およびプロビジョニング プロセス中に CEM サービスを顧客に関連付けることができます。左のサイドバーから **[インベントリ（Inventory）]** > **[その他（Other）]** > **[顧客（Customers）]** を選択して、顧客を作成および管理します。

新しい CEM サービスの作成とプロビジョニング

Cisco EPN Manager で CEM サービスを作成してプロビジョニングするには、次の操作を行います。

- CEM サービスのエンドポイントの指定。
- CEM サービスとそのエンドポイントを介して配信されるトラフィックの処理方法に影響する属性の定義。

始める前に

CEM サービスをプロビジョニングする前に満たしている必要がある前提条件については、CEM プロビジョニングの前提条件 （728 ページ）を参照してください。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックして、CEM サービスを作成する場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [+]アイコンをクリックします。マップ右側の新しいペインにプロビジョニング ウィザードが表示されます。

プロビジョニング ウィザードを表示するもう 1 つの方法として、**[設定（Configuration）] > [ネットワーク（Network）] > [サービス プロビジョニング（Service Provisioning）]** の順に選択する方法があります。

ステップ 6 [テクノロジー（Technology）] ドロップダウンリストから [回線エミュレーション（Circuit Emulation）] を選択します。

ステップ 7 [サービス タイプ（Service Type）] ドロップダウンリストから、回線のデータ転送速度に基づいて必要な CEM サービス タイプを選択します。Cisco EPN Manager でサポートされている CEM サービス タイプのリストについては、サポートされる回線エミュレーション サービス （621 ページ）を参照してください。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [カスタマー サービスの詳細情報（Customer Service Details）] ページに移動します。

ステップ 10 （オプション）EVC の作成対象顧客を選択します。リストに顧客が表示されない場合は、**Inventory > Other > Customers** に移動し、システムで顧客を作成し、プロビジョニング ウィザードに移動して CEM サービスのプロビジョニングを開始します。

ステップ 11 [アクティブ化（Activate）] チェックボックスをオンにし、プロビジョニングするサービスに関連付けられているインターフェイスをアクティブにします。

ステップ 12 サービス名と説明を入力します。

ステップ 13 [展開アクション（Deployment Action）] フィールドに、CEM サービス作成プロセス完了時のアクションを指定します。実際に展開する前に関連デバイスに展開される設定のプレビューを要求するか、または完了後すぐに設定を展開することができます。

[展開（Deploy）] を選択した場合は、次の展開オプションのいずれかをクリックします。

- [今すぐ展開（Deploy Now）]：プロビジョニング順序を直接展開します。
- [後で展開（Deploy Later）]：作成されたプロビジョニング順序を保存しておき、後で同じ順序を展開します。

- [展開のスケジュール（Schedule Deployment）]：プロビジョニングの順序をスケジュールし、スケジュールされた時刻に展開します。この [展開のスケジュール（Schedule Deployment）] オプションボタンをクリックした場合は、次を指定します。
  - [スケジュール時刻の展開（Deploy Schedule Time）]：プロビジョニング順序の展開のスケジュール時刻を指定します。
  - [サーバー時刻（Server Time）]：現在のサーバー時刻を表示します。

ステップ 14 [次へ（Next）] をクリックし、[A エンド（A End）] 設定と [Z エンド（Z End）] 設定、および CEM サービスの転送設定を入力します。フィールドと属性の説明については、CEM サービスの詳細 （730 ページ）を参照してください。

ステップ 15 エンドポイントの 1 つが Cisco EPN Manager により管理されていないデバイス上のインターフェイスの場合は、[管理対象外デバイス（Unmanaged Device）] チェックボックスをオンにし、その管理対象外デバイスの情報を入力します。詳細については、アンマネージド エンドポイントを使用した回線/VC のプロビジョニング （778 ページ）を参照してください。

（注） [管理対象外デバイス（Unmanaged Device）] チェックボックスは、[Z エンド設定（Z End Configurations）] ページだけで使用できます。

ステップ 16 （オプション）サービスに参加するデバイスで設定される追加の CLI コマンドがあるテンプレートを追加するには、[テンプレートの詳細（Template Details）] ページで追加してください。詳細については、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

ステップ 17 サービスに必要な情報をすべて入力したら、[送信（Submit）] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集（Edit Attributes）]をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

CEM サービスを [ネットワークトポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに追加する必要があります。プロビジョニング状態を確認するには、回線/VC 名の横の [i] アイコンをクリックします。[回線/VC 360（Circuit/VC 360）] ビューが表示されます。Also, you can view the saved provisioning job in the Planned Circuits/VCs tab from **[インベントリ（Inventory）]** > **[その他（Other）]** > **[回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）]** > **[計画回線/VC（Planned Circuits/VCs）]** から [計画回線/VC（Planned Circuits/VCs）] タブで保存されたプロビジョニングジョブを表示することもできます。

CEM サービスの詳細

次の表では、CEM サービスのタイプを定義する属性をリストし、説明しています。

表 *46 :* 回線セクションのリファレンス - *CEM* サービス タイプ

属性	説明
[A エンド（A End）] と [Z エンドの設定（Z End Configurations）]	

属性	説明
Device	CEM サービスの送信元と宛先のデバイスの名前。
作業パスと保護パス	
ポート名またはインターフェイス名（Port Name or Interface Name）	CEMサービスにおける送信元と宛先デバイスのインターフェイス名。ポート名またはポート グループを選択できます。 [保護パス（Protecting Path）] エリアの下にあるポート名を選択すると、単方向パス スイッチ型リング（UPSR）保護メカニズムが有効になります。 [保護パス（Protecting Path）] エリアの下にあるポート グループを選択すると、自動保護スイッチング（APS）の保護メカニズムが有効になります。保護グループの設定方法の詳細については、APS または MSP および UPSR または SNCP 保護グループの設定 （414 ページ）を参照してください。
高次パス	SONET/SDH 回線がチャネライズされると、高次パス（HOP）および低次パス（LOP）と呼ばれる、より小さな帯域幅のチャネルに論理的に分割されます。HOP または同期転送信号（STS）パスは、より高い帯域幅の TDM データを伝送するために使用されます。HOP は、その中に LOP を含むこともできます。 CEM サービスで使用可能なパスとパスモードを選択します。
低次パス	LOP またはバーチャル トリビュタリ（VT）パスは、より低い帯域幅の TDM データを伝送するために使用されます。
DS0 タイムスロット（DS0 Time Slot）	DS0 グループで使用できる 1 つ以上のタイムスロットを選択します。 （注） このフィールドは、[サービス タイプ（Service Type）] フィールドの [DS0] を選択するときにのみ使用できます。
クロッキング	
ネットワーク内のノードは、クロック レートが異なる可能性があります。ノードでのタイミングの違いによって、受信ノードは、送信された情報をドロップしたり、再読み取りしたりする可能性があります。すべてのノードを同じクロック レートに同期させるには、クロッキングが必要です。クロッキングの詳細については、CEM のクロッキングの設定 （417ページ）を参照してください。	

属性	説明
Clock Source	すべてのノードを同じクロック レートで同期できるように、単一の送信元からクロックレートを回復できるようにします。値は次のとおりです。 • [内部（Internal）]：ホストから回復されるクロック レート。 • [回線（Line）]：SONET/SDH 回線から回復されるクロック レート。 • [適応クロック回復（Adaptive Clock Recovery）]：デジッタ バッファ フル レベルに基づいてクロック レートが回復されます。遅延変動により、デジッタ バッファ フル レベルは常に変動します。TDM サービス クロックは、変動をフィルタリングした後に回復されます。復元クロックの精度は遅延変動によって異なります。 • [差分クロックリカバリ（Differential Clock Recovery）]：クロック レートは Sync-E を使用してプライマリクロックから回復されます。ネットワークのプライマリクロックを設定する方法の詳細については、Sync-E、BITS、および PTP を使用したクロックの同期 （430 ページ） を参照してください。
QOS 選択可能なプロファイルのリストには、デバイスで設定され、システムによって検出されたポリシーマップ、およびユーザー定義の QoS プロファイルが含まれます。	
入力 QoS プロファイル（Ingress QoS Profile）	A エンド デバイスと Z エンド デバイスで設定されている入力 QoS ポリシーを選択します。
管理されていないデバイス詳細 （注） 次のフィールドは Z エンドの設定でのみ使用できます。	
管理対象外デバイス（Unmanaged Device）	Cisco EPN Manager で管理されていないデバイスを含めて、部分的サービスを作成する場合に、このチェックボックスをオンにします。
新規デバイス（New Device）	新しい管理対象外デバイスを作成する場合に、このチェックボックスをオンにします。
Device	ドロップダウンリストから管理対象外デバイスを選択します。 （注） このフィールドは、[新規デバイス（New Device）]チェックボックスがオフになっている場合にだけ使用できます。

属性	説明
デバイス名（Device Name）	作成する新しい管理対象外デバイスの一意の名前を入力します。 （注） このフィールドは、[新規デバイス（New Device）]チェックボックスがオンになっている場合にだけ使用できます。[新規デバイス（New Device）] チェックボックスがオフの場合、[デバイス（Device）] ドロップダウン リストで選択した管理対象外デバイスの名前がこのフィールドに入力されます。
デバイス IP（Device IP）	作成する新しい管理対象外デバイスの IP アドレスを入力します。 （注） このフィールドは、[新規デバイス（New Device）]チェックボックスがオンになっている場合にだけ使用できます。[新規デバイス（New Device）] チェックボックスがオフの場合、[デバイス（Device）] ドロップダウン リストで選択した管理対象外デバイスの IP アドレスがこのフィールドに入力されます。
LDP IP	管理対象外デバイスの有効な LDP IP を入力します。
VC ID	管理対象外デバイスの仮想回線（VC）の固有 ID を入力します。
転送設定	
フレーム タイプ（Frame Type）	このフィールドは表示専用で、CEM サービスの作成時に選択した CEM サービスタイプに基づいて自動入力されます。値は [CESoPSN]、[SAToP]、[FRAMED_SAToP]、および [CEP] です。 サービス タイプが [T1]、[T3]、[E1]、および [E3 CEM] の場合は、フレーム タイプを [SAToP] または [FRAMED_SAToP] として選択します。 E3 コントローラ上のサービスタイプ E3 のフレームタイプ CEP を選択できます。 （注） CEM サービスの展開後、 SDH を持つ SONET フレーム モードを介した T1/T3 サービスと E1/E3 サービスの CLI 変更を [デバイス プレビューの設定（Device Preview Config）] に表示します。FRAMED-SAToP フレーム タイプは、NCS42xx デバイスまたは ASR9xx デバイスでサポートされています。
ペイロード サイズ（Payload Size）	各 IP パケットに入れられるバイト数。有効な範囲は 64 ～ 1312 です。範囲は、デバイスの機能、サポート レベル、および設定されたデジッタ バッファ サイズの値に応じて異なります。

属性	説明
デジッタ バッファ サイズ（Dejitter Buffer Size）	ネットワーク ジッターを許容するエミュレートされた回路の能力を決定します。有効な範囲は 1 ～ 32 です。範囲は、デバイスの機能、サポートのレベル、および設定されたペイロードサイズの値によって異なります。
アイドル パターン（Idle pattern）	サービスがダウンしたときにデータを送信するアイドル パターン。有効範囲は 0x00 ～ 0xFF です。
ダミー モード（Dummy Mode）	損失フレームまたは破損フレームの穴埋め用ビット パターンを設定できます。値はラスト フレームとユーザー定義です。
ダミー パターン（Dummy Pattern）	損失フレームまたは破損フレームの穴埋め用ビット パターン。有効範囲は 0x00 ～ 0xFF です。デフォルトは 0xFF です。 （注） このフィールドは、ユーザー定義としてダミーモードを選択した場合にのみ有効になります。
RTP ヘッダー対応（RTP Header Enabled）	CEM サービスの Real-Time Transport Protocol (RTP) ヘッダーを有効にするには、このチェックボックスをオンにします。
RTP 圧縮対応（RTP Compression Enabled）	パケットが送信される前にパケットの IP ヘッダーを圧縮するには、このチェックボックスをオンにします。ネットワークのオーバーヘッドを削減し、RTP の伝送を高速化します。
疑似回線の設定	
優先パス タイプ（Preferred Path Type）	優先パスタイプを双方向または単方向として選択します。
優先経路（Preferred Path）	CEM サービスを通過させる MPLS 双方向 TE トンネルを選択します。 （注） このフィールドは、優先パス タイプに [双方向（Bidirectional）] を選択したときにのみ使用できます。
優先パス（A～Z）（Preferred Path (A-Z)）	A エンドポイントから Z エンドポイントまで CEM サービスを移動させるために必要な単方向トンネルを選択します。 （注） このフィールドは、優先パス タイプに [単方向（Unidirectional）] を選択したときにのみ使用できます。
優先パス（Z～A）（Preferred Path (Z-A)）	Z エンドポイントから A エンドポイントに CEM サービスを移動させるために必要な単方向トンネルを選択します。 （注） このフィールドは、優先パス タイプに [単方向（Unidirectional）] を選択したときにのみ使用できます。

属性	説明
LDP へのフォールバックを許可（Allow Fallback to LDP）	選択した優先パスがダウンした時に、CEM サービスがデフォルトの MPLS Label Distribution Protocol（LDP）にフォールバックされるようにするには、このチェックボックスをオンにします。 （注） このチェックボックスは、[優先パス（Preferred Path）] フィールドで有効な MPLS TE トンネルを選択した場合にのみ使用できます。
送信コントロールワード（Send Control Word）	接続の両側で疑似回線ペイロードを特定するためにコントロールワードを使用する場合は、このチェックボックスをオンにします。
[インターネットワーキング（Internetworking）] のオプション	EVC のエンドポイントのいずれかが管理対象外デバイスの場合、オプションを選択します。
帯域幅（kbps）（Bandwidth (kbps)）	疑似回線に必要な帯域幅を入力します。
PWID	疑似回線識別子を入力します。この ID は、ポイントツーポイントサービスの [擬似線設定（Pseudowire Settings）] に表示されます。

CEM サービスの変更

Cisco EPN Manager を使用して作成および展開された CEM サービスを変更できます。

始める前に

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジマップ（Topology Maps）] > [ネットワークトポロジ（Network Topology）]** の順に選択します。

ステップ 2 [Device Groups] をクリックして、変更する CEM サービスがある場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [Network Topology] ウィンドウで、[Circuits/VCs] タブをクリックし、変更する CEM サービスを選択します。

ステップ 5 鉛筆（変更）アイコンをクリックします。

[Modify CEM] ウィンドウが表示されます。[Z Endpoint] の詳細のみを変更できます。

ステップ 6 [Device] を変更するには、[Device] ドロップダウンリストからデバイスを選択します。

ステップ 7 [Working Path] を変更するには、ドロップダウンリストから [Interface Name] を選択します。

ステップ 8 [Higher Order Path] を変更するには、ドロップダウンリストから [Available Paths] と [Path Mode] を選択します。

ステップ 9 [Lower Order Path] を変更するには、ドロップダウンリストから [Available Paths] を選択します。

ステップ 10 必要に応じて変更したら、[送信（Submit）] をクリックしてデバイスに展開される設定をプレビューします。

ステップ 11 変更内容を確認してから [展開（Deploy）] をクリックしてデバイスに変更を展開します。

プロビジョニング順序の保存とスケジュール

回線/VC、MPLS トンネル、または L3VPN サービステクノロジーなどのプロビジョニング サービスを作成、変更、または削除すると、サービスをプレビューまたは展開できます。プロビジョニング順序を保存またはスケジュールする前に、[今すぐ展開（Deploy Now）]、[後で展開（Deploy Later）]、[展開のスケジュール（Schedule Deployment）] などの展開オプションを選択できます。

[計画回線/VC（Planned Circuits/VCs）] タブに保存されたプロビジョニング順序を表示し、必要に応じて計画サービスを変更するか、後続サービスを作成することができます。次に、制限事項の一部を示します。

- 計画バージョンが存在する場合は、ライブ回線の変更および削除操作はすべて無効になります。また、**[インベントリ（Inventory）] > [回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）]** で計画順序のサービスを修正することはできません。詳細については、「次の作業」の項を参照してください。
- [計画回線（Planned Circuits）] から順序を編集する場合、Cisco EPNM では計画に変更を加えることができます。
- [計画回線（Planned Circuits）] からの削除アクションは、最後に試行されたプロビジョニングされたバージョンに戻される計画サービスを削除します。スケジュール順序の場合、ジョブ ダッシュボードから時刻が更新されると、同じ時刻が [計画回線（Planned Circuits）] に反映されません。

展開を保存してスケジュールするには、次の手順を実行します。

ステップ 1 次のパスのいずれかを使用して計画プロビジョニングの順序を作成するには、次の手順を実行します。

[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）] を選択します。

または

[インベントリ（Inventory）] > [回線/VCs およびネットワーク インターフェイス（Circuits/VCs&Network Interfaces）] を選択します。

ステップ 2 「での回線/VC のプロビジョニング Cisco EPN Manager」というトピックのステップ 2 ～ 12 を繰り返します。

ステップ 3 展開を保存してスケジュールするには、次の手順を実行します。

a) [展開（Deploy）] 領域で、[後で展開（Deploy Later）] オプション ボタンをクリックして、プロビジョニング順序を保存します。
b) [展開（Deploy）] 領域で、[展開のスケジュール（Schedule Deployment）] オプション ボタンをクリックし、指定した時刻に今後の展開の順序を保存します。次の値を指定します。
   - [スケジュール時刻の展開（Deploy Schedule Time）]：プロビジョニング順序の展開のスケジュール時刻を指定します。
   - [サーバー時刻（Server Time）]：現在のサーバー時刻を表示します。
c) [次へ（Next）]をクリックしてエンドポイントを選択し、選択したテクノロジーに基づいて属性を定義します。
d) [送信（Submit）]をクリックします。選択した展開アクションに応じて、関連するアクションが実行されます。つまり、設定のプレビューを選択した場合は、設定を表示できるプレビュー ページが表示され、その後に [展開（Deploy）] をクリックします。展開を選択した場合、設定は関連するデバイスに直接展開されます。展開の保存/スケジュールが成功したことを示すメッセージを受け取ったら、[閉じる（Close）] をクリックします。

ステップ 4 左側のペインで、[回線/VC（Circuit/VCs）]ハイパーリンクをクリックします。[場所/すべての場所/未割り当て（Locations/All Locations/Unassigned）] 拡張ビュー ウィンドウが表示されます。

ステップ 5 [計画回線 VC（Planned Circuits VC）] タブをクリックし、新しく作成されたプロビジョニング サービスの詳細を表示します。新しく作成されたプロビジョニング サービスのステータスは、[計画済みの作成（Create Planned）] として表示されます。展開スケジュールの時刻、プロビジョニングするサービスのタイプおよび名前、顧客名、および最終変更日時を表示します。必要に応じて、サービスは再度変更することができます。計画されたサービスの場合、展開するまでは何度でも修正できます。ステータスは[計画済みの変更（Modify Planned）] として表示されます。

（注） [計画回線/VC（Planned Circuits/VCs）] タブは、**[マップ（Maps）] > [トポロジ（Topology）] > [ネットワーク トポロジ（Network Topology）]** から [回線/VC（Circuit/VCs）] をクリックした場合にのみ使用できます。[後で展開（Deploy Later）] オプションの場合は、展開スケジュール時刻が表示されません。

何度かの修正の間に最新バージョンがキャプチャされます。スケジュールされた順序があり、最新バージョンが [後で展開（Deploy Later）] に設定されている場合は、そのうちに以前にスケジュールされたすべての順序が [ジョブ（Job）] ダッシュボードから削除されます。

ステップ 6 計画順序の作成をクリックした後、**[アクション（Actions）] > [展開（Deploy）]** を選択してサービスを直接展開します。

ステップ 7 （オプション）必要に応じて他のアクションを実行できます。

a) 新しいプロビジョニング ワークフローを作成するには、[+] アイコンをクリックします。
b) 計画したサービスを削除するには、[X] アイコンをクリックします。サービスが削除されると、ウィンドウの右下隅に成功か失敗かのメッセージが表示されます。
c) [後でデプロイ（Deploy Later）] サービスは、[X] をクリックすると削除され、計画されていたデプロイ サービスに関するトレースは EPNM に保存されません。
d) デプロイされたスケジュール済みのサービスが削除されると、対応するジョブとサービスがクリアされます。

ステップ 8 スケジュールしたプロビジョニング ジョブを表示するには、**[管理（Administration）]** > **[ダッシュボード（Dashboard）]** > **[ジョブ ダッシュボード（Job Dashboard）]** を選択します。ステータスは [スケジュール済み（Scheduled）] として表示され、次回の展開の開始時刻などを表示できます。

a) （オプション）[スケジュールの編集（Edit Schedule）] をクリックして、スケジュールの順序を編集します。

- [スケジュール（Schedule）] ウィンドウで、必要に応じてスケジュール時刻やその他の詳細を変更します。
- [保存（Save）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] ウィンドウに戻ります。

b) （オプション）ジョブを削除するには、[X] アイコンをクリックします。

ジョブが正常にデプロイされると、エントリのリストがジョブ ダッシュボードに表示されます。[後で展開（Deploy Later）] オプションでは、時刻が定義されていないため、ジョブは作成されません。

次のタスク

[インベントリ（Inventory）] > **[回線/VC およびネットワーク インターフェイス（Circuits/VCs&Network インターフェイス]** を選択して計画回線/VC を表示します。新しいプロビジョニング ワークフローの作成、既存のサービスの展開、または特定のプロビジョニング順序のサービスの修正を行えます。正常に展開されると、プロビジョニング順序のエントリが [計画回線/VC（Planned Circuits）] タブからクリアされます。

（注） [回線/VC（Circuit/VCs）] タブに展開した回線/VCを、[計画回線/VC（Planned Circuits/VCs）] タブに計画回線を表示します。

回線/VCの変更または削除操作は実行できません。これは、展開したバージョンにさらに修正を加える前に、まず計画したバージョンをクリアする必要があるためです。[計画回線/VC（Planned Circuits/VCs）] をクリックして、選択した回線/VC に修正を加えるか、または計画したバージョンを展開します。

削除操作

計画したバージョンを削除すると、ウィンドウの右下隅に成功または失敗を示すメッセージが表示されます。[回線/VC（Circuits/VCs）] タブでサービスを削除すると、[計画の変更がキャンセルされました（Modify Plan Canceled）] と [計画の削除がキャンセルされました（Delete Plan Canceled）] というステータスが表示されます。

[計画回線/VC（Planned Circuit/VCs）] タブからサービスを削除すると、関連付けられた UNI も [ネットワークインターフェイス（Network Interface）] タブから削除されます。削除された UNI は再利用可能になります。

設定のプレビュー

新しいプロビジョニング回線/VC の作成時に [展開アクション（Deployment Action）] が [プレビュー（Preview）] として選択されている場合は、[展開（Deploy）] ページに [今すぐ展開

（Deploy Now）] または [後で展開（Deploy Later）] あるいは [展開のスケジュール（Schedule Deployment）] のいずれかを選択するオプションが表示されます。

ネットワーク インターフェイスの表示

[回線/VC（Circuits/VCs）] タブで [ネットワーク インターフェイス（Network Interfaces）] をクリックして、サービスをプロビジョニングするためのネットワーク インターフェイスの詳細を表示します。ウィザードを使用してインターフェイスを変更または削除できます。

EM-Voice CEM サービスのプロビジョニング

EM IM では、ポート 0 ～ 3 が 1 つのグループを形成し、ポート 4 と 5 が別のグループを形成します。これらのグループそれぞれに適用可能な EM タイプがサービス プロビジョニング時に EPNM に反映され、各ポートに適用可能なタイプのリストが表示されるようになります。

選択したサービス タイプ EM-Voice の CEM サービスをプロビジョニングするには、次の手順を実行します。

ステップ 1 左側のペインで、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイスグループ（Device Groups）] をクリックして、CEM サービスを作成する場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [+]アイコンをクリックします。マップ右側の新しいペインにプロビジョニング ウィザードが表示されます。

プロビジョニング ウィザードを表示するもう 1 つの方法として、**[設定（Configuration）] > [ネットワーク（Network）] > [サービス プロビジョニング（Service Provisioning）]** の順に選択する方法があります。

ステップ 6 [テクノロジー（Technology）] ドロップダウンリストから [回線エミュレーション（Circuit Emulation）] を選択します。

ステップ 7 [サービスタイプ（Service Type）] ドロップダウン リストから、[EM-Voice] を選択してデータを送信します。Cisco EPN Manager でサポートされている CEM サービス タイプのリストについては、サポートされる回線エミュレーション サービス （621 ページ）を参照してください。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックした後、サービス名とその説明を入力します。

ステップ 10 [次へ（Next）] をクリックした後、CEM サービスの [A エンド（A End）] 設定を入力します。フィールドと属性の説明については、CEM サービスの詳細 （730 ページ）を参照してください。

a) [ポート名（Port Name）] ドロップダウン リストからインターフェイス名を選択します。デバイスの設定に基づいて、ポートのリストが表示され、各ポートに適用可能なタイプのリストを表示できます。

b) [EM タイプ（EM Type）] ドロップダウン リストから、ポート上に設定できるタイプを選択します。

（注） [タイプ（Type）] は [ポート名（Port Name）] フィールドで選択したインターフェイス名と [該当するタイプ（Applicable Type）] に基づいて一覧表示されます。

ステップ 11 [次へ（Next）] をクリックした後、CEM サービスの [Z エンド（Z End）] 設定を入力します。

（注） EM タイプは、A エンドポイント EM タイプと同じである必要があります。

ステップ 12 [送信（Submit）] をクリックして、設定をデバイスにプッシュします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、[属性の編集（Edit Attributes）] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

MPLS トラフィック エンジニアリング サービスのプロビジョニング

Cisco EPN Manager MPLS TE のプロビジョニング サポートの概要

Cisco EPN Manager は、MPLS トラフィック エンジニアリング サービスのプロビジョニングをサポートしています。MPLS TE を使用すると、MPLS バックボーンはレイヤ 2 の TE 機能をレイヤ 3 上に復元し、拡張できます。MPLS TE は、バックボーン全体でラベルスイッチド パス（LSP）を確立および維持するために、Resource Reservation Protocol（RSVP）を使用します。詳細については、サポートされている MPLS トラフィック エンジニアリング サービス （623 ページ）を参照してください。

MPLS TE サービスのプロビジョニング機能

Cisco EPN Manager は次の MPLS TE 機能をサポートしています。

- 明示的なルーティング、制約ベースのルーティング、およびトランク アドミッション コントロールのサポート。
- リンク障害とノード障害に対するパス保護メカニズムのプロビジョニング。

- ラベル交換パス（LSP）を確立し、維持するための Resource Reservation Protocol（RSVP）の使用。
- OSPF と ISIS を使用して TE リンクをアドバタイズする機能。

Cisco EPN Manager の MPLS TE 制限事項を次に示します。

- MPLS TE トンネルは、NCS 4206、4216 デバイス、NCS4K、NCS 5500、ASR9k、および ASR9XX でのみサポートされています。ただし、インベントリ サポートは NCS 4201 と NCS 4202 に対して提供されます。
- OSPF および ISIS は、MPLS TE を実装するための IGP としてサポートされています。
- NCS5500 デバイスでは、ラップ保護、BFD、および障害 OAM はサポートされていません。
- MPLS TE 属性は、属性が Cisco EPN Manager Web インターフェイスを介してプロビジョニングされている場合にのみ使用でき、データベースに入力されます。

（注） MPLS TE トンネルのプロビジョニングをサポートするデバイスのリストについては、次を参照してください。 Cisco Evolved Programmable Network Manager のサポート対象デバイス

MPLS TE レイヤ 3 リンクの作成とプロビジョニング

MPLS TE レイヤ 3 リンクをプロビジョニングするには、次の手順を実行します。

始める前に

MPLS TE レイヤ 3 リンクをプロビジョニングする前に満たす必要がある前提条件については、「MPLS TE サービスのプロビジョニングの前提条件 （750 ページ）」を参照してください。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [Device Groups] をクリックして、MPLS TE レイヤ 3 リンクを作成する場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [+]アイコンをクリックします。マップ右側の新しいペインにプロビジョニング ウィザードが表示されます。

ステップ 6 [テクノロジー（Technology）] ドロップダウンリストから [MPLS TE] を選択します。Cisco EPN Manager は、関連するサービス タイプのリストを [サービス タイプ（Service Type）] 領域に表示します。

ステップ 7 [サービス タイプ（Service Type）] 領域で、[レイヤ 3 リンク（Layer 3 Link）] を選択します。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [リンク設定（Link Settings）] ページに移動します。

ステップ 10 レイヤ 3 リンクの名前と説明を入力します。

ステップ 11 次のいずれかの方法で、[A エンド デバイス（A End Device）]、[A エンド インターフェイス（A End Interface）]、[Z エンドデバイス（Z End Device）]、および [Z エンドインターフェイス（Z End Interface）] フィールドを選択します。

- マップ上のリンクをクリックすると、[A エンドデバイス（A End Device）]、[A エンドインターフェイス（A End Interface）]、[Z エンドデバイス（Z End Device）]、および [Z エンドインターフェイス（Z End Interface）] の各フィールドが自動的に設定されます。
- マップ上のデバイス ノードをクリックすると、[A エンド デバイス（A End Device）] フィールドが自動的に設定されます。A エンド デバイスが 1 つのデバイスのみに接続されている場合は、[Z エンド デバイス（Z End Device）] フィールドが自動的に設定されます。[A エンド デバイス（A End Device）] が複数のデバイスに接続されている場合は、[Z エンド デバイス（Z End Device）] を手動で選択する必要があります。

ステップ 12 A エンド デバイスと Z エンド デバイスの IP アドレスとマスクを入力します。

ステップ 13 次のオプションから L2 検出プロトコルを選択します。

- [なし（NONE）]：レイヤ 3 リンクに対して有効にする L2 Discovery Protocol がありません。
- [CDP]：ネットワークに接続されているシスコ デバイス間での通信を容易にするために レイヤ 3 リンクに対して有効にする Cisco Discovery Protocol。
- [LLDP]：シスコ以外のデバイスをサポートし、IEEE 802.1AB LLDP をサポートする他のデバイス間の相互運用を可能にするために、レイヤ 3 リンクに対して有効にする Link Layer Discovery Protocol。
- [ALL]：レイヤ 3 リンクに対して有効にする CDP と LLDP の両方。

ステップ 14 レイヤ 3 リンクに必要なルーティング プロトコルを選択します。値は [BGP]、[ISIS]、および [OSPF] です。ルーティング プロトコルの設定方法については、次を参照してください。ルーティング プロトコルとセキュリティの設定 （524 ページ）

ステップ 15 （オプション）レイヤ 3 リンクのリンク VLAN ID を入力します。

ステップ 16 （オプション）プロビジョニングするレイヤ 3 リンクで MPLS TE をサポートするには、[MPLS TE の有効化（Enable MPLS TE）] チェックボックスをオンにします。

（注） このチェックボックスは、ルーティング プロトコルとして OSPF または ISIS を選択した場合にのみ使用できます。

ステップ 17 [次へ（Next）] をクリックし、[A エンド（A End）] と [Z エンド（Z End）] の詳細を入力します。フィールドと属性の説明については、MPLS TE レイヤ 3 リンクの A エンドの詳細と Z エンドの詳細に関するフィールド参照 （743 ページ）を参照してください。

ステップ 18 [展開アクション（Deployment Action）] フィールドに、MPLS レイヤ 3 リンクの作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 19 [送信（Submit）] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集（Edit Attributes）] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

サービスが [ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] タブのリストに追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

MPLS TE レイヤ 3 リンクの A エンドの詳細と Z エンドの詳細に関するフィールド参照

次の表に、MPLS TE レイヤ 3 リンクを定義する属性のリストを示し、説明します。

表 *47 : MPLS TE* レイヤ *3* リンクの *A* エンドの詳細と *Z* エンドの詳細に関するフィールド参照

属性	説明	ルーティング プロトコルが次の場合に使用できます。
A エンドと同じ（Same as A End）	A エンドデバイスと Z エンドデバイスの両方に同じルーティングおよび MPLS-TE 設定を使用する場合は、このチェックボックスをオンにします。 （注） このチェックボックスは、プロビジョニング ウィザードの [Z エンドの詳細（Z End Details）] ページでのみ使用できます。	BGP、ISIS、および OSPF
BGP AS 番号（BGP AS Number）	ネットワークに割り当てられている固有の BGP 自律システム番号を選択します。	BGP
ルート ポリシー（ルート ポリシー）	BGP が格納するルートとルーティング テーブルから取得するルートを制御するには、ルーティング ポリシーを選択します。	BGP
ルート リフレクタ クライアント（Route Reflector Client）	ローカル ルートのリフレクタのルート リフレクタ クライアントとして BGP ネイバーを設定して使用可能なルートをアドバタイズするには、このチェックボックスをオンにします。	BGP

属性	説明	ルーティング プロトコルが次の場合に使用できます。
AIGP の使用（Use AIGP）	レイヤ 3 リンクに Accumulated Interior Gateway Protocol（AIGP）メトリック属性を使用するには、このチェックボックスをオンにします。AIGP は、ネットワーク内のパスの累積エンドツーエンド メトリックを伝送する BGP 属性です。	BGP
更新の送信元（Update Source）	必要な送信元インターフェイスを選択します。 （注） このフィールドは、[AIGP の使用（Use AIGP）] チェックボックスがオフになっている場合にのみ使用できます。	BGP
ISIS プロセス ID（ISIS Process ID）	A エンド デバイスと Z エンド デバイスの両方で使用できる ISIS ルーティング プロセス ID を選択します。ISIS プロセスを設定する方法については、IS-IS の設定（529 ページ）を参照してください。	ISIS
ネットワーク（Network）	選択した ISIS プロセス ID に基づいて、ネットワーク ID が自動的に設定されます。	ISIS

属性	説明	ルーティング プロトコルが次の場合に使用できます。
回線タイプ（Circuit Type）	次のオプションから、レイヤ3リンクに必要な隣接関係のタイプを選択します。 • [なし（NONE）]：隣接関係は確立されません。 • [レベル 1（Level-1）]：選択したデバイスとそのネイバー間に共通するエリア アドレスが 1 つ以上ある場合は、レベル 1 隣接関係を確立します。 • [レベル 2 のみ（Level-2-only）]：回線上にレベル 2 の隣接関係を確立します。隣接デバイスがレベル 1 のみのデバイスの場合、隣接関係は確立されません。 • [レベル 1-2（Level-1-2）]：ネイバーもレベル 1-2 デバイスとして設定されており、共通するエリアが 1 つ以上ある場合、レベル 1 と 2 の隣接関係を確立します。共通のエリアがない場合は、レベル 2 の隣接関係が確立されます。	ISIS
レベル 1 メトリック（Level 1 Metric）	レベル 1（エリア内）ルーティングの SPF 計算で使用する必要があるメトリックを入力します。 （注） このフィールドは、[回線タイプ（Circuit Type）] を [レベル 1（Level-1）] または [レベル 1-2（Level-1-2）] として選択した場合にのみ使用できます。	ISIS
レベル 2 メトリック（Level 2 Metric）	レベル 2（エリア間）ルーティングの SPF 計算で使用する必要があるメトリックを入力します。 （注） このフィールドは、[回線タイプ（Circuit Type）] を [レベル 2（Level-2）] または [レベル 1-2（Level-1-2）] として選択した場合にのみ使用できます。	ISIS

属性	説明	ルーティング プロトコルが次の場合に使用できます。
OSPF プロセス ID（OSPF Process ID）	OSPF ルーティング プロセス ID を選択します。OSPF プロセスを設定する方法については、OSPF の設定 （531 ページ）を参照してください。 （注） Z エンド デバイスの OSPF ルーティング プロセスは変更できません。	OSPF
OSPF Area	OSPF ルーティング プロセスを展開するエリアを入力します。	OSPF
メトリック（Metric）	OSPF ルーティング プロセスで使用されるルーティング メトリックを入力します。	OSPF
BFD テンプレート（BFD Template）	レイヤ 3 リンクの BFD テンプレートを選択します。BFD テンプレートは、BFD セッションで使用される設定可能パラメータのセットを定義します。これには、BFD 制御およびエコー パケットに使用される送受信タイマー、セッションが CV 関数を提供するときに使用される送信タイマー間隔、乗数値、およびエコー受信間隔が含まれます。 （注） BFD テンプレートは、IOS-XE デバイスに適用できます。	ISIS および OSPF
BFD 最小間隔（BFD Min Interval）	対応する BFD 設定範囲の BFD セッションの最小制御パケット間隔を入力します。 （注） このフィールドは、[BFD テンプレート（BFD Template）] を選択していない場合にのみ使用できます。	BGP、ISIS、および OSPF

属性	説明	ルーティング プロトコルが次の場合に使用できます。
BFD の乗数（BFD Multiplier）	BFD 乗数を入力します。この値は BFD 最小間隔とともに使用して、バンドル メンバ リンクの非同期モードでの制御パケットとエコー パケットの両方の間隔と障害検出時間を決定します。 （注） このフィールドは、[BFD テンプレート（BFD Template）] を選択していない場合にのみ使用できます。	BGP、ISIS、および OSPF
BFD 高速検出（BFD Fast Detect）	隣接する転送エンジン間のパスで障害を迅速に検出するには、このチェックボックスをオンにします。 （注） これは、Cisco IOS-XR デバイスにのみ適用されます。	BGP、ISIS、および OSPF
認証モード（Authentication Mode）	ISIS パケットの送受信に必要な認証モードを選択します。 （注） 認証フィールドは、Cisco IOS XE デバイスを選択した場合にのみ使用できます。使用可能なオプションは、[なし（NONE）]、[HMAC_MD5]、および [テキスト（TEXT）] です。デフォルトでは、[なし（NONE）] が選択されます。	ISIS
認証キー チェーン（Authentication Key Chain）	認証キー チェーンを選択します。これにより、ルーティング プロトコルの認証が有効になり、認証キーのグループを識別します。	ISIS
送信専用の認証（Authentication for Send Only）	送信される ISIS パケットに対してのみ認証を実行するには、このチェックボックスをオンにします。 （注） これは、IOS-XE デバイスにのみ適用されます。	ISIS

属性	説明	ルーティング プロトコルが次の場合に使用できます。
パスワード タイプ（Password Type）	パスワードタイプを [暗号化（Encrypted）] または [プレーン テキスト（Plain Text）] として選択します。	BGP
パスワード（Password）	目的のパスワードを入力します。2 つのピア間の接続を確立するには、パスワードが必要です。	BGP
MPLS-TE		
ループバック インターフェイス	レイヤ 3 リンクのループバック インターフェイス アドレスを選択します。ループバック インターフェイスを設定する方法については、「ループバック インターフェイスの設定」を参照してください。	ISIS および OSPF
Administrative Weight	MPLS TE トンネル メトリックを絶対モードで入力します。	ISIS および OSPF
TE 属性（TE Attributes）	パス選択時にトンネルのアフィニティ ビットと比較する MPLS TE リンク属性を入力します。	ISIS および OSPF
パーセンテージを使用（Is Percentage）	レイヤ 3 リンクの帯域幅をパーセンテージで割り当てるには、このチェックボックスをオンにします。	ISIS および OSPF
グローバル帯域幅（Global Bandwidth）	CBR のレイヤ 3 リンク用に予約される通常の TE トンネル帯域幅を入力します。 たとえば、レイヤ 3 リンクのグローバル帯域幅として 10% を割り当てる場合は、[パーセンテージを使用（Is Percentage）] チェックボックスをオンにし、[グローバル帯域幅（Global Bandwidth）] フィールドに値 10 を入力します。一方で、グローバル帯域幅として 50 Kbps を割り当てる場合は、[パーセンテージを使用（Is Percentage）] チェックボックスをオフにし、[帯域幅の単位（Bandwidth Unit）] ドロップダウン リストから [Kbps] を選択し、[グローバル帯域幅（Global Bandwidth）] フィールドに値 50 を入力します。	ISIS および OSPF

属性	説明	ルーティング プロトコルが次の場合に使用できます。
サブプール帯域幅（Subpool Bandwidth）	グローバル プール帯域幅から予約されているサブプール帯域幅を入力します。 たとえば、レイヤ 3 リンクのサブプール帯域幅として 10% を割り当てる場合は、[パーセンテージを使用（Is Percentage）] チェックボックスをオンにし、[サブプール帯域幅（Subpool Bandwidth）] フィールドに値 10 を入力します。一方で、サブプール帯域幅として 50 Kbps を割り当てる場合は、[パーセンテージを使用（Is Percentage）] チェックボックスをオフにし、[帯域幅の単位（Bandwidth Unit）] ドロップダウン リストから [Kbps] を選択し、[サブプール帯域幅（Subpool Bandwidth）] フィールドに値 50 を入力します。	ISIS および OSPF
自動トンネル バックアップ（Auto Tunnel Backup）	このチェックボックスをオンにして、ルータが MPLS TE トンネルを使用して設定されたインターフェイスでバックアップ トンネルが動的に構築できるようにします。	ISIS および OSPF
バックアップ トンネルでの SLRG の除外（Exclude SLRG for Backup Tunnel）	このチェックボックスをオンにして、特定のインターフェイスに関連付けられた自動トンネルバックアップの特定のリンク上で、SRLG 値の除外を有効にできるようにします。	ISIS および OSPF
BFD 高速検出（BFD Fast Detect）	隣接する転送エンジン間のパスで障害を迅速に検出するには、このチェックボックスをオンにします。	ISIS および OSPF
QoS		
Ingress Policy	A エンド デバイスと Z エンド デバイスで設定されている入力 QoS ポリシーを選択します。	BGP、ISIS、および OSPF
出力ポリシー（Egress Policy）	A エンド デバイスと Z エンド デバイスで設定されている出力 QoS ポリシーを選択します。	BGP、ISIS、および OSPF
追加設定（Additional Settings）		

属性	説明	ルーティング プロトコルが次の場合に使用できます。
Enable MPLS TE	プロビジョニングするレイヤ 3 リンクで MPLS をサポートするには、このチェックボックスをオンにします。	ISIS および OSPF
SyncE の有効化（Enable SyncE）	レイヤ 3 リンクのインターフェイス レベルで同期イーサネットを有効にするには、このチェックボックスをオンにします。 （注） これは、IOS-XE デバイスにのみ適用されます。	BGP、ISIS、および OSPF

MPLS TE サービスのプロビジョニングの前提条件

MPLS TE サービスをプロビジョニングするには、次の前提条件を満たす必要があります。

- OSPF または IS-IS は、MPLS TE サービスに参加するデバイスで設定する必要があります。
- MPLS TE L3 リンクをプロビジョニングする前に、LLDP/CDP を有効にする必要があります。
- MPLS TE サービス プロビジョニングに使用されるすべてのリンクは TE に対応している必要があります。
- TE に対応しているリンクは、運用上、稼働している必要があります。
- トンネルの送信元ノードと宛先ノードに到達可能である必要があります。
- WAE パラメータ REST コールは EPN Manager から自動的にセットアップできます。
- MPLS 到達可能性は、デバイス間で設定する必要があります。MPLS コア ネットワーク設定をセットアップする必要があります。
- MPLS TE サービスがプロビジョニングされるデバイスのインベントリ収集ステータスが、[完了済み（Completed）] である必要があります。これを確認するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** に移動し、[最後のインベントリ収集ステータス（Last Inventory Collection Status）] 列でステータスを確認します。
- 必要に応じて、顧客をシステムに作成して、サービスの作成中およびプロビジョニング プロセス中に MPLS TE サービスを顧客に関連付けることができます。左のサイドバーから **[インベントリ（Inventory）]** > **[その他（Other）]** > **[顧客（Customers）]** を選択して、顧客を作成および管理します。

MPLS TE トンネルの作成とプロビジョニング

MPLS TE トンネルをプロビジョニングするには、次の手順を実行します。

始める前に

MPLS TE トンネルをプロビジョニングする前に満たす必要がある前提条件については、次を参照してください。 MPLS TE サービスのプロビジョニングの前提条件 （750 ページ）

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジマップ（Topology Maps）] > [ネットワークトポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックして、MPLS TE トンネルを作成する場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [+]アイコンをクリックします。マップ右側の新しいペインにプロビジョニング ウィザードが表示されます。

ステップ 6 [テクノロジー（Technology）] ドロップダウンリストから [MPLS TE] を選択します。Cisco EPN Manager は、関連するサービス タイプのリストを [サービス タイプ（Service Type）] 領域に表示します。

ステップ 7 [サービス タイプ（Service Type）] 領域で、[単方向 TE トンネル（Unidirectional TE Tunnel）] または [双方向 TE トンネル（Bidirectional TE Tunnel）] を選択します。

ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル（776 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックして [カスタマー サービスの詳細情報（Customer Service Details）] ページに移動します。

ステップ 10 （オプション）サービスをプロビジョニングする対象としての顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customers）]** の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。

ステップ 11 サービス名とその説明を入力した後、サービスの詳細を入力します。サービスの詳細に関するフィールド参照：MPLS TE トンネル （752 ページ）を参照してください。

（注）
- サービス名を指定しない場合、Cisco EPN Manager は次の形式でサービス名を割り当てます。
  - 送信元デバイスと宛先デバイスに共通のトンネル ID がある場合、サービス名は <SourceDeviceName>_<TunnelId>_<DestinationDeviceName> 形式で割り当てられます。
  - 送信元デバイスと宛先デバイスに固有のトンネル ID がある場合、サービス名は <SourceDeviceName>_<ATunnelId>_<ZTunnelId>_<DestinationDeviceName> 形式で割り当てられます。
- トンネルのシグナル名は、システム内のデバイス間で一意である必要があります。

ステップ 12 [次へ（Next）] をクリックした後、トンネル作成パラメータを入力します。フィールドと属性の説明については、トンネルの作成に関するフィールド参照：MPLS TE トンネル （753 ページ）を参照してください。

ステップ 13 [次へ（Next）] をクリックした後、パスの制約の詳細を入力します。フィールドと属性の説明については、パスの制約の詳細に関するフィールド参照：MPLS TE トンネル（762 ページ）を参照してください。

ステップ 14 [送信（Submit）] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集（Edit Attributes）] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストにサービスが追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを表示します。

サービスの詳細に関するフィールド参照：MPLS TE トンネル

次の表に、MPLS TE トンネルを作成するためのサービスの詳細を定義する属性のリストを示し、説明します。

表 *48 : [*サービスの詳細（*Service Details***）*]* セクションのリファレンス：*MPLS TE* トンネル**

属性	説明
アクティブ化	デフォルトでは、このチェックボックスはオンになっています。展開時にトンネルをアクティブにすることができます。
FRR の有効化（Enable FRR）	このチェックボックスをオンにすると、MPLS TE トンネルのリンクとノード保護を提供する高速再ルーティング機能が有効になります。 （注） このチェックボックスは、単方向TEトンネルを作成する場合にのみ使用できます。
自動帯域幅の有効化（Enable Auto Bandwidth）	トラフィックに基づいて TE トンネルに最大帯域幅と最小帯域幅を自動的に割り当てるには、このチェックボックスをオンにします。
ラップ保護（Wrap Protection）	中間リンクの障害シナリオを検出するには、このチェックボックスをオンにします。 （注） このチェックボックスは、双方向TEトンネルを作成する場合にのみ使用できます。
障害 OAM の有効化（Enable Fault OAM）	MPLS TE トンネルのプロビジョニングとメンテナンスをサポートする障害 OAM プロトコルとメッセージを有効にするには、このチェックボックスをオンにします。 （注） このチェックボックスは、双方向TEトンネルを作成する場合にのみ使用できます。

属性	説明
自動ルートの有効化（Enable Autoroute）	トンネルの自動ルートを有効にするには、このチェックボックスをオンにします。
BFD 設定の有効化（Enable BFD Settings）	Bidirectional Forwarding Detection（BFD）プロトコルを有効にするには、このチェックボックスをオンにします。BFDは、高速転送パスの障害検出時刻と、一貫した障害検出方式を提供します。
保護タイプ（Protection Type）	TE トンネルには、次のいずれかの保護メカニズムを選択します。 • [動作中（Working）]：トンネルには動作中のパスのみが存在します。 • [動作中＋保護（Working＋Protected）]：トンネルには動作中のパスと保護されたパスがあり、動作中のパスに障害が発生した場合、トラフィック フローは、リンクがダウンすることなく、保護されたパスに自動的にルーティングされます。 • [動作中＋復元（Working＋Restore）]：トンネルには動作中のパスと復元パスがあり、動作中のパスに障害が発生するとリンクがダウンし、トラフィック フローが復元パスにルーティングされます。 • [動作中+保護+復元（Working＋Protected＋Restore）]：トンネルには動作中のパス、保護パス、および復元パスがあり、動作中のパスに障害が発生した場合、トラフィック フローは保護されたパスにルーティングされます。また、保護されたパスにも障害が発生すると、リンクがダウンし、トラフィック フローが復元パスにルーティングされます。
展開アクション（Deployment Action）	MPLS TE トンネル作成プロセスが完了したときにどのようになるかを指定するには、次のいずれかのオプションを選択します。 • [プレビュー（Preview）]：実際の展開前に、関連するデバイスに展開される設定をプレビューします。 • [展開（Deploy）]：完了直後に設定を展開します。

トンネルの作成に関するフィールド参照：MPLS TE トンネル

次の表に、MPLS TE トンネルの作成を定義する属性のリストを示し、説明します。

表 *49 : [*トンネル作成（***Tunnel Creation***）*]* セクションのリファレンス：***MPLS TE*** トンネル

属性	説明
トンネルの作成（Create Tunnel）	

属性	説明
送信元（Source）	トンネルの送信元または A エンドポイント。
送信元ルーティング プロセス（Source routing Process）	TE が有効で、選択した送信元エンドポイントで設定されている OSPF または ISIS ルーティング プロセス。OSPF または ISIS ルーティング プロセスに基づいて、送信元エンドポイントで設定されたルータ ID とループバック アドレスを決定できます。
接続先（Destination）	トンネルの宛先または Z エンドポイント。
宛先ルーティング プロセス（Destination Routing Process）	TE が有効になっており、選択した宛先エンドポイントで設定されている OSPF または ISIS ルーティング プロセス。OSPF または ISIS ルーティング プロセスに基づいて、宛先エンドポイントで設定されたルータ ID とループバック アドレスを決定できます。
トンネル設定（Tunnel Setting）	
グローバル ID（Global ID）	送信元と宛先の両方のエンドポイントに割り当てられているグローバル ID。この ID は、2 つの単方向トンネルを 1 つの双方向 TE トンネルにバインドする ID と同じである必要があります。デフォルト値は 0 です。 （注） この属性は、双方向 TE トンネルを作成する場合にのみ使用できます。EPNM は、1 ～ 2147483647 の範囲内でのみグローバル ID をサポートします。
アンフィニティ ビット（Affinity Bits）	アフィニティビットは、動的バックアップパスの設定時に双方向 TE トンネルが使用するリンク属性を決定します。
アフィニティ マスク（Affinity Mask）	アフィニティマスクは、ルータが確認する必要があるリンク属性を決定します。 アフィニティ ビットとアフィニティ マスクを使用して、動的バックアップ パスを構成するときにリンク属性を含めるか除外することができます。マスクのビットが 0 の場合、そのビットに関連付けられているリンク属性の値とは無関係です。この場合、動的バックアップ パスを設定する際に、リンク属性は除外されます。マスクのビットが 1 の場合、関連付けられているリンク属性の値は、そのビットのトンネルのアフィニティと一致する必要があります。この場合、動的バックアップ パスを設定するときに link 属性が含まれます。

属性	説明
セットアップ優先度（Setup Priority）	単方向または双方向の TE トンネルの LSP に割り当てられているセットアップ優先度。この優先度に基づいて、LSP は、ブロックする既存のトンネルか、または優先度の低い LSP を決定できます。 有効な値は 0 ー 7 です。値が小さいほど、プライオリティが高いことを示します。たとえば、セットアップ優先順位が 0 の LSP は、セットアップ優先順位が 1 ～ 7 の任意の LSP をブロックできます。 （注） セットアップ優先度を保留優先度より高くすることはできません。
保留優先度（Hold Priority）	単方向または双方向の TE トンネルの LSP に割り当てられている保留優先度この優先度に基づいて、LSP はセットアップ優先度の高い別のシグナリング LSP によってブロックする必要があるかどうかを決定できます。 有効な値は 0 ー 7 です。値が小さいほど、プライオリティが高いことを示します。たとえば、保留優先度が 0 の LSP は、別の LSP によってブロックすることはできません。
帯域幅プール タイプ（Bandwidth Pool Type）	MPLS TE の制約ベース ルーティング（CBR）の各リンクの予約可能帯域幅を管理するために使用される帯域幅プール。値は次のとおりです。 • [グローバル（Global）]：通常の TE トンネル帯域幅。 • [サブプール（Subpool）]：グローバル プールの一部。サブプール帯域幅は、使用中以外はグローバル プールから予約されません。サブプール トンネルには、グローバル プール トンネルよりも高い優先度が必要です。 （注） このフィールドは、[自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスがオフになっている場合にのみ使用できます。
帯域幅（Bandwidth）	双方向 TE トンネルの帯域幅。ドロップダウンリストから帯域幅の単位を選択できます。使用可能な単位は、[Kbps]、[Mbps]、および[Gbps] です。 たとえば、トンネルに 1000000 Kbps の帯域幅を割り当てる場合は、値を 1000 Gbps と入力します。 （注） このフィールドは、[自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスがオフになっている場合にのみ使用できます。

属性	説明
自動最大帯域幅（Auto Bandwidth Max）	Cisco EPN Managerは、トラフィックに基づいてTEトンネルの最大帯域幅を自動的に割り当てます。ただし、必要に応じて帯域幅を変更できます。ドロップダウンリストから帯域幅の単位を選択できます。使用可能な単位は、[Kbps]、[Mbps]、および [Gbps] です。 （注） このフィールドは、[顧客サービスの詳細（Customer Service Detail）] 画面の [自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスをオンにした場合にのみ使用できます。
自動最小帯域幅（Auto Bandwidth Min）	Cisco EPN Managerは、トラフィックに基づいてTEトンネルの最小帯域幅を自動的に割り当てます。ただし、必要に応じて帯域幅を変更できます。ドロップダウンリストから帯域幅の単位を選択できます。使用可能な単位は、[Kbps]、[Mbps]、および [Gbps] です。 （注） このフィールドは、[顧客サービスの詳細（Customer Service Detail）] 画面の [自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスをオンにした場合にのみ使用できます。
帯域幅変更頻度（秒）（Bandwidth Change Frequency (Sec)）	帯域幅変更頻度を秒単位で入力します。有効な範囲は 300 ー 604800 です。 （注） このフィールドは、トンネルの作成時に [顧客サービスの詳細（Customer Service Detail）] ページの [自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスをオンにした場合にのみ使用できます。
調整しきい値（Adjustment Threshold）	最大のサンプル パーセンテージが現在の帯域幅よりも大きいか、または小さい場合に、調整をトリガーする帯域幅調整しきい値をパーセンテージ単位で入力します。調整しきい値は、現在のトンネル帯域幅と絶対（最小）帯域幅のパーセンテージです。トンネルに再度シグナリングするには、自動帯域幅の両方のしきい値を満たす必要があります。トンネル帯域幅は、最大のサンプル出力レートと現在のトンネル帯域幅の差分が調整しきい値よりも大きい場合に調整されます。 Cisco IOS-XR デバイスを接続するトンネルの有効範囲は 1 ー 100 です。Cisco IOS-XE デバイスを接続するトンネルの範囲は 1 ー 99 です。 （注） このフィールドは、トンネルの作成時に [顧客サービスの詳細（Customer Service Detail）] ページの [自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスをオンにした場合にのみ使用できます。

属性	説明
オーバーフローしきい値（Overflow Threshold）	オーバーフロー検出をトリガーするには、オーバーフローしきい値をパーセンテージで入力します。これは、実際にシグナリングされたトンネル帯域幅のパーセンテージです。測定された帯域幅と実際の帯域幅の差分が、連続してN回のオーバーフローしきい値のパーセンテージよりも大きい場合 、オーバーフロー検出がトリガーされます。これは、オーバーフロー制限とも呼ばれます。 Cisco IOS-XR デバイスを接続するトンネルの有効な範囲は 1 ～ 100 で、Cisco IOS-XE デバイスを接続するトンネルの範囲は 1 ～ 99 です。 （注） このフィールドは、トンネルの作成時に [顧客サービスの詳細（Customer Service Detail）] ページの [自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスをオンにした場合にのみ使用できます。
オーバーフロー制限（Overflow Limit）	測定された帯域幅と実際のトンネルの帯域幅のちがいがトンネル用に定義されているオーバーフローしきい値を超える場合がある連続的な収集期間の数を入力します。 有効な範囲は 1 ～ 10 です。 （注） このフィールドは、トンネルの作成時に [顧客サービスの詳細（Customer Service Detail）] ページの [自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスをオンにした場合にのみ使用できます。
収集帯域幅（Collect Bandwidth）	トンネルの帯域幅情報を収集するには、このチェックボックスをオンにします。 （注） このフィールドは、トンネルの作成時に [顧客サービスの詳細（Customer Service Detail）] ページの [自動帯域幅の有効化（Enable Auto Bandwidth）] チェックボックスをオンにした場合にのみ使用できます。
BFD 設定（BFD Settings）	
新規 BFD（New BFD）	デフォルトでは、[BFD 設定の有効化（Enable BFD Settings）] チェックボックスをオンにすると、このチェックボックスはオンになります。プロビジョニング中に双方向（Flex LSP）と単方向のトンネルの両方に対して新しい BFD テンプレートを作成できます。
BFD テンプレート名（BFD Template Name）	新しい BFD テンプレートの名前を入力します。

属性	説明
BFD テンプレート（BFD Template）	デバイス名を連結して、選択したBFDテンプレート名を表示します。たとえば、AエンドデバイスやZエンドデバイスから連結します。既存のテンプレート名から既存のテンプレートを選択すると、関連する[最小間隔（Min Interval）] と [乗数（Multiplier）] の範囲値がデフォルトで表示されます。 アルファベット、数字、および特殊文字の _（アンダースコア）、-（ハイフン）、.（ドット） を使用することができ、BFD テンプレート名の長さは 32 文字未満である必要があります。 BFDテンプレート名には.（ドット）または数字または数字と.（ドット）の組み合わせは使用できません。 （注） このフィールドは、[新規 BFD（New BFD）] チェックボックスをオフにした場合にのみ使用できます。
最小間隔（Min Interval） Multiplier（乗数）	BFDは、間隔と乗数を使用して、非同期モードで制御およびエコーパケットが送信される期間を指定します。また、それらに対応する障害検出も実行します。障害検出タイマーは次の式に基づいて起動します。この場合、*I* は最小間隔を指定し、*M* は乗数（**`I x M`**）です。 （注） これらのフィールドは、[BFD 設定の有効化（Enable BFD Settings）] チェックボックスと [新規 BFD（New BFD）] チェックボックスがオンになっている場合にのみ使用できます。 [最小間隔（Min Interval）] と [乗数（Multiplier）] の値が新しいBFDと既存のBFDの両方に表示されます。既存のBFDの場合は、値を編集することはできません。

BFD テンプレートの使用に関するロジック

XE デバイスの単方向および FLEX の LSP トンネルに BFD テンプレー設定を使用します。XR デバイスの単方向およびFLEX の LSP トンネルには、インライン設定を使用します。EPNM には、新しい BFD テンプレートを作成するか、または次のロジックに基づいて既存の BFD テンプレートを再利用するオプションが用意されています。

（注） FLEX LSP トンネルは双方向トンネルと呼ばれています。

次の表に、BFD テンプレートを使用するためのロジックを示します。

表 ***50 : BFD*** テンプレートのロジック：***MPLS TE*** トンネル

単一方向（**Unidirectional**）

デバイス名の組み合わせ	設定ロジックの説明
XE-XE XE-XR	XE デバイスを送信元と宛先（または XR デバイスを宛先）として選択した場合、ロジックは BFD テンプレート設定として動作します。 新しい BFD テンプレートを作成するには、次の手順を実行します。 **1.** EPNM は、デフォルトで選択された [新規 BFD（New BFD）] チェックボックスを表示します。 **2.** BFD テンプレートの名前を入力します。 **3.** [最小間隔（Min Interval）] に 4 ～ 1000 の範囲値を入力します。 **4.** [乗数（Multiplier）] に 3 ～ 50 の範囲値を入力します。 既存の BFD テンプレートを再利用するには、次の手順を実行します。 **1.** [新規 BFD（New BFD）] チェックボックスをオフにします。 **2.** [BFD テンプレート（BFD Template）] ドロップダウン リストから、既存の BFD テンプレートを選択します。A エンド デバイスの既存の BFD テンプレート名すべてのリストが表示されます。 **3.** [最小間隔（Min Interval）] と [乗数（Multiplier）] の範囲値が表示されます。 **4.** **[送信（Submit）]** をクリックします。
XR-XR XR-XE	XR デバイスを送信元と宛先（または XE デバイスを宛先）として選択した場合、ロジックはインライン設定として動作します。EPNM は、[最小間隔（Min Interval）] フィールドと [乗数（Multiplier）] フィールドのみを表示します。
双方向	

XE-XE	XE デバイスを送信元と宛先として選択した場合、ロジックは BFD テンプレート設定として動作します。 BFD テンプレートを作成するには、次の手順を実行します。 **1.** EPNM は、デフォルトで選択された [新規 BFD（New BFD）] チェックボックスを表示します。 **2.** BFD テンプレートの名前を入力します。 **3.** [最小間隔（Min Interval）] に 4 ～ 1000 の範囲値を入力します。 **4.** [乗数（Multiplier）] に 3 ～ 50 の範囲値を入力します。 既存の BFD テンプレートを再利用するには、次の手順を実行します。 **1.** [新規 BFD（New BFD）] チェックボックスをオフにします。 **2.** [BFD テンプレート（BFD Template）] ドロップダウン リストから、既存の BFD テンプレートを選択します。**A エンド** デバイスと **Z エンド** デバイスの既存の BFD テンプレート名すべてのリストが表示されます。 **3.** [最小間隔（Min Interval）] と [乗数（Multiplier）] の範囲値が表示されます。 **4.** **[送信（Submit）]** をクリックします。

XE-XR	XE デバイスを送信元、XR デバイスを宛先として選択した場合、ロジックは BFD テンプレート設定として動作します。 新しい BFD テンプレートを作成するには、次の手順を実行します。 **1.** EPNM は、デフォルトで選択された [新規 BFD（New BFD）] チェックボックスを表示します。 **2.** BFD テンプレート名を入力します。 **3.** [最小間隔（Min Interval）] に 4 ～ 1000 の範囲値を入力します。 **4.** [乗数（Multiplier）] に 3 ～ 10 の範囲値を入力します。 既存のBFDテンプレートを再利用するには、次の手順を実行します。 **1.** [新規 BFD（New BFD）] チェックボックスをオフにします。 **2.** [BFD テンプレート（BFD Template）] ドロップダウン リストから、既存のBFDテンプレートを選択します。これにより、A エンド デバイスの既存のすべての BFD テンプレート名のリストが表示されます。 **3.** [最小間隔（Min Interval）] と [乗数（Multiplier）] の範囲値が表示されます。 **4.** **[送信（Submit）]** をクリックします。
XR-XR	XR デバイスを送信元と宛先として選択した場合、ロジックはインライン設定として動作します。EPNM は、[最小間隔（Min Interval）] フィールドと [乗数（Multiplier）] フィールドのみを表示します。

XR-XE	XR デバイスを送信元、XE デバイスを宛先として選択した場合、ロジックは BFD テンプレート設定として動作します。 新しい BFD テンプレートを作成するには、次の手順を実行します。 1. EPNM は、デフォルトで選択された [新規 BFD（New BFD）] チェックボックスを表示します。 2. BFD テンプレートの名前を入力します。 3. [最小間隔（Min Interval）] に 4 ～ 1000 の範囲値を入力します。 4. [乗数（Multiplier）] に 3 ～ 10 の範囲値を入力します。 既存のテンプレートを再利用するには、次の手順を実行します。 1. [新規 BFD（New BFD）] チェックボックスをオフにします。 2. [BFD テンプレート（BFD Template）] ドロップダウン リストから、既存の BFD テンプレートを選択します。**Z エンド** デバイスの既存の BFD テンプレート名がすべて一覧表示されます。 3. [最小間隔（Min Interval）] と [乗数（Multiplier）] の範囲値が表示されます。 4. **[送信（Submit）]** をクリックします。

パスの制約の詳細に関するフィールド参照：MPLS TE トンネル

次の表に、MPLS TE トンネルを作成するためのパスの制約の詳細を定義する属性のリストを示し、説明します。

表 *51 :* パスの制約の詳細に関するセクションのリファレンス：*MPLS TE* トンネル

属性	説明
Path Type	TE トンネルに必要なパスを選択します。値は、[動作中（Working）]、[保護（Protected）]、および[復元（Restore）] です。[パスタイプ（Path Type）] フィールドで選択した値に基づいて、[ワーキングパス（Working Path）]、[プロテクションパス（Protection Path）]、および [リストアパス（Restore Path）] フィールドグループを使用できます。
ロックダウンの有効化（Enable Lock Down）	動作中の LSP を再最適化しない場合は、このチェックボックスをオンにします。
Enable SRLG	SRLG を有効にする場合は、このチェックボックスをオンにします。 （注）　これは、保護パスでのみ設定できます。

属性	説明
スティッキの有効化（Enable Sticky）	トンネルパスが変更された場合に新しい LSP に切り替えないようにするには、このチェックボックスをオンにします。 （注） ロックダウンが有効になっている場合にのみ、ワーキングパス用に設定できます。
非リバーティブの有効化（Enable Non-Revertive）	動作中のパスが復元された場合でも、プロテクションパスから最初のワーキングパスに戻さない場合は、このチェックボックスをオンにします。 （注） これは、保護パスでのみ設定できます。
タイプ（Type）	トンネルに動作中のパスまたは保護パスのタイプを選択します。値は [動的（Dynamic）] および [明示的（Explicit）] です。
新規パス（New Path）	トンネルに新たに動作中のパス、保護パス、または復元パスを作成する場合にこのチェックボックスをオンにします。 （注） 以下のすべてのフィールドは、[タイプ（Type）] フィールドで [明示的（Explicit）] を選択した場合にのみ使用できます。
既存のパスの選択（Select Existing Path）	トンネルに既存の明示的な動作中のパス、保護パス、または復元パスを選択します。 （注） このフィールドは、[新規パス（New Path）] チェックボックスをオフにした場合にのみ使用できます。
WAE サーバーからのパスの選択（Choose path from WAE server）	WAE ネットワークとパスを指定するには、このチェックボックスをオンにします。 （注） このフィールドは、[新規パス（New Path）] チェックボックスをオンにした場合にのみ使用できます。 [動的（Dynamic）] タイプと [パス（Path）] タイプを [動作中（Working）] に選択した場合は、このチェックボックスをオンまたはオフにすることができます。明示的なパスを WAE サーバーから直接読み取り、手動で設定しない場合は、このチェックボックスをオンにすることを推奨します。
WAE ネットワークの選択（Select WAE Network）	下向き矢印をクリックして、ダイアログボックスから WAE ネットワークを選択します。 （注） このフィールドは、[WAE サーバーからのパスの選択（Choose path from WAE server）] チェックボックスをオンにした場合にのみ使用できます。

属性	説明
WAE パスの選択（Select the WAE Path）	下向きの矢印をクリックして、明示的なパスを選択します。 （注） このフィールドは、[WAE サーバーからのパスの選択（Choose path from WAE server）] チェックボックスをオンにした場合にのみ使用できます。
パス名（Path Name）	作成する明示的なパスの名前を入力します。[動作中のパス（Working Path）] テーブル、[保護パス（Protection Path）] テーブル、または [復元パス（Restore Path）] テーブルで、[+] ボタンをクリックしてテーブルに新しい行を追加した後、MPLS 対応デバイス、デバイスのインターフェイスとして明示的なパス コントローラ、およびパスの制約タイプを選択します。 パステーブルでは、送信元デバイスと宛先デバイスを除く MPLS 対応デバイスを選択できます。Cisco EPN Manager は厳密なパス制約タイプのみをサポートしています。 （注） このフィールドは、[新規（New）] チェックボックスをオンにした場合にのみ使用できます。
[動作中のパス LSP 属性リスト（Working Path LSP Attribute List）]、[保護パス LSP 属性リスト（Protection Path LSP Attribute List）]、および [復元パス LSP 属性リスト（Restore Path LSP Attribute List）] [パス タイプ（Path Type）] フィールドで選択した値に基づいて、それぞれのフィールド グループを使用できます。 ここで定義する LSP 属性は、[パス タイプ（Path Type）] フィールドで選択したパス オプションに関連付けられており、これらの属性は送信元デバイスと宛先デバイスに適用できます。 （注） 特定のパス オプションに定義されている値は、インターフェイス トンネル レベルで指定された値をオーバーライドします。たとえば、動作中のパスの LSP 属性を定義した場合、これらの値はインターフェイス トンネル レベルの [トンネル設定（Tunnel Settings）] セクションで定義した値をオーバーライドします。これは、すべてのパス オプションに共通しています。 双方向トンネルでは、[ロックダウンの有効化（Enable Lock Down）] チェックボックスをオフにした場合にのみ、[ワーキングパス（Working Path）] LSP 属性リストを設定できます。	
新しい LSP 属性リスト（New LSP Attribute List）	選択したパス タイプに新しい LSP 属性リストを作成するには、このチェックボックスをオンにします。

属性	説明
既存のLSP属性リスト（Existing LSP Attribute List）	選択したパス タイプの既存の LSP 属性リストを選択します。 （注） このフィールドは、[新規LSP属性リスト（New LSP Attribute List）] チェックボックスをオフにした場合にのみ使用できます。
LSP 属性リスト名（LSP Adjustment Threshold Name）	作成する LSP 属性リストの名前を入力します。 （注） このフィールドを含む以下のすべてのフィールドは、[新しい LSP 属性リスト（New LSP Attribute List）] チェックボックスがオフの場合、読み取り専用として表示されます。
LSPアフィニティ ビット（LSP Affinity Bits）	バックアップ パス（動作中、保護、または復元）の設定時に双方向 TE トンネルが使用するリンク属性を決定する LSP アフィニティ ビットを入力します。
LSPアフィニティ マスク（LSP Affinity Mask）	バックアップ パスの設定時にルータが確認する必要があるリンク属性を決定する LSP アフィニティ マスクを入力します。
LSPセットアップ優先度（LSP Setup Priority）	選択したパス タイプの LSP に割り当てられているセットアップ優先度を入力します。この優先度に基づいて、LSPは、ブロックする既存のトンネルか、または優先度の低い LSP を決定できます。 有効な値の範囲は0～7です。値が小さいほど、プライオリティが高いことを示します。たとえば、セットアップ優先順位が0のLSPは、セットアップ優先順位が 1 ～ 7 の任意の LSP をブロックできます。 （注） LSP セットアップ優先度を LSP 保留優先度より高くすることはできません。 （注） Cisco IOS-XR デバイスの場合、[LSP セットアップ優先度（LSP Setup Priority）] フィールドと [LSP 保留優先度（LSP Hold Priority）] フィールドは適用されません。

属性	説明
LSP 保留優先度（LSP Hold Priority）	選択したパス タイプの LSP に割り当てられている保留優先度を入力します。この優先度に基づいて、LSP はセットアップ優先度の高い別のシグナリング LSP によってブロックする必要があるかどうかを決定できます。 有効な値の範囲は 0 ～ 7 です。値が小さいほど、プライオリティが高いことを示します。たとえば、保留優先度が 0 の LSP は、別の LSP によってブロックすることはできません。 （注） Cisco IOS デバイスの場合、LSP 保持優先度を指定しない場合は、Cisco EPN Manager は [LSP セットアップ優先度（LSP Setup Priority）] フィールドで指定された値を取得します。 （注） Cisco IOS-XR デバイスの場合、[LSP セットアップ優先度（LSP Setup Priority）] フィールドと [LSP 保留優先度（LSP Hold Priority）] フィールドは適用されません。
LSP レコード ルート（LSP Record Route）	チェックボックスをオンにして、LSP が使用するルートを記録します。

シリアル サービスのプロビジョニング

シリアル回線/VC プロビジョニングの前提条件

次に、シリアル回線/VC をプロビジョニングするための前提条件を示します。

- デバイス間の通信は、シリアル回線/VC をプロビジョニングする前にセットアップする必要があります。
- シリアル回線/VC をプロビジョニングするデバイスのインベントリ収集のステータスは [完了（Completed）] である必要があります。これを確認するには、**[インベントリ（Inventory）]**>**[デバイス管理（Device Management）]**>**[ネットワーク デバイス（Network Devices）]** に移動し、[最後のインベントリ収集ステータス（Last Inventory Collection Status）] 列でステータスを確認します。
- 必要に応じて、システムに顧客を作成し、回線/VC の作成およびプロビジョニング プロセス中に顧客に回線/VC を関連付けられるようにする必要があります。左のサイドバーから

[インベントリ（Inventory）] > **[その他（Other）]** > **[顧客（Customers）]** を選択して、顧客を作成および管理します。

新しいシリアル回線/VC（RS232、RS422、RS485）の作成とプロビジョニング

新しいシリアル回線/VC を作成するには、次の手順を実行します。

始める前に

シリアル回線/VCをプロビジョニングする前に満たしている必要がある前提条件については、シリアル回線/VC プロビジョニングの前提条件 （766 ページ）を参照してください。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** の順に選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

ステップ 2 ツールバーで [デバイス グループ（Device Groups）] をクリックし、マップ上に表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブをクリックします。

ステップ 4 [回線/VC（Circuits/VCs）] ペインのツールバーで、[+]（作成）アイコンをクリックします。

マップの右側に新しいペインが開き、[プロビジョニング ウィザード（Provisioning Wizard）] が表示されます。

ステップ 5 [テクノロジー（Technology）] ドロップダウン リストで [シリアル（Serial）] を選択します。

ステップ 6 [サービス タイプ（Service Type）] リストで、作成するシリアル サービスのタイプを選択します。Cisco EPN Manager がサポートしているシリアル サービスのタイプについては、サポートされているシリアル サービス （625 ページ）を参照してください。

ステップ 7 さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 8 **Next** をクリックして [カスタマー サービスの詳細（Customer Service Details）] ページに移動します。

ステップ 9 回線/VC の作成対象顧客を選択します。リストに顧客が表示されない場合は **Inventory** > **Other** > **Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。

ステップ 10 [アクティブ化（Activate）] チェックボックスをオンにして、サービスをアクティブ状態にする必要があるかどうかを指定します。アクティブ状態の場合、トラフィックが回線を通過できるようになり、関連付けられているすべてのエンドポイントのサービス状態が自動的に True に設定されます。

ステップ 11 サービス名と説明を入力します。

ステップ 12 [展開アクション（Deployment Action）] フィールドに、回線/VC の作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 13 [次へ（Next）] をクリックして、エンドポイントを設定するページに移動します。シリアル サービスの詳細のリファレンス （768 ページ）を参照してください。

ステップ 14 エンドポイントのいずれかが Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、その管理対象外デバイスの情報を入力します。アンマネージド エンドポイントを使用した回線/VC のプロビジョニング （778 ページ）を参照してください。

ステップ 15 [次へ（Next）] をクリックして、[回線設定（Line Settings）] ページと [擬似回線の設定（Pseudowire Settings）] ページに移動します。「シリアル サービスの詳細のリファレンス （768 ページ）」を参照してください。

ステップ 16 これはオプションです。回線/VC に参加するデバイスで設定される追加の CLI コマンドがあるテンプレートを追加するには、[テンプレートの詳細（Template Details）] ページで追加してください。詳細については、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

ステップ 17 回線/VC に必要な情報をすべて入力したら、[送信（Submit）] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集（Edit Attributes）] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

回線/VC が、[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに追加されているはずです。

シリアル サービスの詳細のリファレンス

次の表では、シリアル サービスのタイプを定義する属性をリストし、説明しています。

表 *52*：回線セクションのリファレンス：シリアル サービス タイプ

属性	説明
[A エンドポイント（A Endpoint）] と [Z エンドポイント（Z Endpoint）] の設定	
メディア タイプ（Media Type）	シリアルインターフェイス サービス用に選択されたメディアタイプ。
デバイス名（Device Name）	シリアル サービスの送信元と宛先のデバイスの名前。
ポート名および説明（Port Name and Description）	シリアルサービスの送信元デバイスと宛先デバイス上のインターフェイスの名前と説明。
管理されていないデバイス詳細 （注） 以下のフィールドは、[Z エンドポイントの設定（Z Endpoint Configurations）] でのみ使用できます。	
管理対象外デバイス（Unmanaged Device）	Cisco EPN Manager で管理されていないデバイスを含めて、部分的サービスを作成する場合に、このチェックボックスをオンにします。

属性	説明
新規デバイス（New Device）	新しい管理対象外デバイスを作成する場合に、このチェックボックスをオンにします。
メディア タイプ（Media Type）	既存の RS232 または RS422 サービスのメディア タイプとして RS232 または RS422 のいずれかを選択し、ポイントツーポイント RS232 から RS422 へのサービスを作成します。たとえば、既存のメディア タイプ RS232 がある場合、A エンドでは、ポイントツーポイント サービス設定の Z エンドでメディア タイプとして RS232 または RS422 のいずれかを選択できます。 （注） メディア タイプは、作成後に変更することはできません。
デバイス名（Device Name）	作成する新しい管理対象外デバイスの一意の名前を入力します。 （注） [新規デバイス（New Device）] チェックボックスをオフにすると、このフィールドはドロップダウン リストとして使用できます。Zエンドポイントとして管理対象外デバイスを選択できます。
デバイス IP（Device IP）	作成する新しい管理対象外デバイスの IP アドレスを入力します。 （注） このフィールドは、[新規デバイス（New Device）] チェックボックスがオンになっている場合にだけ使用できます。[新規デバイス（New Device）] チェックボックスがオフの場合、[デバイス（Device）] ドロップダウン リストで選択した管理対象外デバイスの IP アドレスがこのフィールドに入力されます。
LDP IP	管理対象外デバイスの有効な LDP IP を入力します。
VC ID	管理対象外デバイスの仮想回線（VC）の固有 ID を入力します。
回線の設定	
速度（Speed）	シリアル リンクの速度（キロ ビット/秒）。
データ ビット（Data Bits）	シリアル回線/VC を介して送信されるパケットあたりの実際のデータの測定値。値は 5、6、7、および 8 です。

属性	説明
ストップ ビット（Stop Bits）	1 つのパケットの通信の終了を示します。値は 1、1.5、および 2 ビットです。 データは回線を横切ってクロックされ、各デバイスには独自のクロックが備わっているため、2 台のデバイスがわずかに同期しなくなる可能性があります。したがって、ストップ ビットは送信の終了を示すだけでなく、異なるクロックを同期するようにも考慮します。ストップ ビットに使用されるビット数が多いほど、異なるクロックを同期するために考慮する幅が大きくなり、データ伝送速度は遅くなります。
パリティ（Parity）	シリアル通信のエラーを確認するために使用されます。値は次のとおりです。 • [なし（None）]：回線/VC に定義されているパリティなし。 • [偶数（Even）]：シリアル ポートはパリティ ビット（データ ビットの後ろの最後のビット）を、伝送に偶数のロジック上位ビットが必ず含まれる値に設定します。たとえば、データが 011 だった場合、偶数パリティでは、パリティ ビットが 0 になり、ロジック上位ビット数を偶数に保ちます。 • [奇数（Odd）]：シリアル ポートはパリティ ビット（データ ビットの後ろの最後のビット）を、伝送に奇数のロジック上位ビットが必ず含まれる値に設定します。たとえば、データが 011 だった場合、奇数パリティでは、パリティ ビットが 1 になり、ロジック上位ビットが 3 つになります。 • [マーク（Mark）]：パリティ ビットを高く設定します。これにより、受信側デバイスはビットの状態を把握して、ノイズがデータを破損させているか、または送信デバイスと受信側のデバイスのクロックが同期していないかを判断できます。 • [スペース（Space）]：パリティビットを低く設定します。これにより、受信側デバイスはビットの状態を把握して、ノイズがデータを破損させているか、または送信デバイスと受信側のデバイスのクロックが同期していないかを判断できます。

属性	説明
デュプレックス モード（Duplex Mode）	シリアル サービスに必要なデュプレックス モードを次のオプションから選択します。 • [半二重（HalfDuplex）]：エンドポイント間の両方向の通信をサポートしますが、同時にはサポートしません。データは一度に単方向に伝送されます。 • [全二重（FullDuplex）]：両方のエンドポイントが全二重をサポートしていると想定し、エンドポイント間での双方向への同時通信をサポートします。一方の側が全二重をサポートしていない場合、ポートはダウンします。 （注） このフィールドは、RS485 および RS422 サービス タイプでのみ使用できます。RS485 および RS422 サービス タイプの詳細は編集できます。これは、RS485 と RS422 では、半二重と全二重からデュプレックス モードを選択できるためです。ただし、RS232 では全二重モードのみしか選択できないため、RS232 サービス タイプの詳細は編集できません。
疑似回線の設定	
優先パス タイプ（Preferred Path Type）	優先パスタイプを双方向または単方向として選択します。
優先経路（Preferred Path）	シリアル サービスを通過させる MPLS 双方向 TE トンネルを選択します。 （注） このフィールドは、優先パス タイプに [双方向（Bidirectional）] を選択したときにのみ使用できます。
優先パス（A～Z）（Preferred Path (A-Z)）	A エンドポイントから Z エンドポイントまで シリアル サービスを移動させるために必要な単方向トンネルを選択します。 （注） このフィールドは、優先パス タイプに [単方向（Unidirectional）] を選択したときにのみ使用できます。
優先パス（Z～A）（Preferred Path (Z-A)）	Z エンドポイントから A エンドポイントまで シリアル サービスを移動させるために必要な単方向トンネルを選択します。 （注） このフィールドは、優先パス タイプに [単方向（Unidirectional）] を選択したときにのみ使用できます。
送信コントロール ワード（Send Control Word）	接続の両側で疑似回線ペイロードを特定するためにコントロール ワードを使用する場合は、このチェックボックスをオンにします。

新しいシリアル回線/VC（raw ソケット）の作成とプロビジョニング

raw ソケット タイプの新しいシリアル回線/VC を作成するには、次の手順を実行します。

始める前に

raw ソケット回線/VC をプロビジョニングする前に満たしている必要がある前提条件については、シリアル回線/VC プロビジョニングの前提条件 （766 ページ）を参照してください。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

ステップ 2 ツールバーで [デバイス グループ（Device Groups）] をクリックし、マップ上に表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブをクリックします。

ステップ 4 [回線/VC（Circuits/VCs）] ペインのツールバーで、[+]（作成）アイコンをクリックします。

マップの右側に新しいペインが開き、[プロビジョニング ウィザード（Provisioning Wizard）] が表示されます。

ステップ 5 [テクノロジー（Technology）] ドロップダウン リストで [シリアル（Serial）] を選択します。

ステップ 6 [サービス タイプ（Service Type）] リストで、[raw ソケット（Raw Socket）] を選択します。raw ソケット回線/VC の詳細については、サポートされているシリアル サービス （625 ページ）を参照してください。

ステップ 7 さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択（Select Profile）] ドロップダウン リストから必要なプロファイルを選択します。回線/VC プロファイル （776 ページ）を参照してください。

ステップ 8 [次へ（Next）] をクリックして [カスタマー サービスの詳細情報（Customer Service Details）] ページに移動します。

ステップ 9 回線/VC の作成対象顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ（Inventory）] > [その他（Other）] > [顧客（Customer）]** の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。

ステップ 10 サービス名と説明を入力します。

ステップ 11 [展開アクション（Deployment Action）] フィールドに、回線/VC の作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 12 [次へ（Next）] をクリックして [サーバー側の設定（Server Side Configuration）] ページに移動します。フィールドと属性の説明については、raw ソケット サービスの詳細のリファレンス （773 ページ）を参照してください。

ステップ 13 [次へ（Next）] をクリックして [クライアント側の設定（Client Side Configuration）] ページに移動します。[raw ソケット クライアント（Raw Socket Client）] テーブルの [+] アイコンをクリックし、クライアント側の設定用の新しい行を追加します。フィールドと属性の説明については、raw ソケット サービスの詳細のリファレンス （773 ページ）を参照してください。

ステップ 14 これはオプションです。回線/VCに参加するデバイスで設定される追加のCLIコマンドがあるテンプレートを追加するには、[テンプレートの詳細（Template Details）] ページで追加してください。詳細については、テンプレートを使用した回線/VC の拡張 （778 ページ）を参照してください。

ステップ 15 回線/VCに必要な情報をすべて入力したら、[送信（Submit）]をクリックします。デバイスに展開されるCLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集（Edit Attributes）]をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

回線/VC が、[ネットワーク トポロジ（Network Topology）] ウィンドウの [回線/VC（Circuits/VCs）] ペインのリストに追加されているはずです。[サービス（Services）] タブから、新たに作成されたシリアル インターフェイス サービスの横にある [i] アイコンをクリックし、最近サーバー上で作成したエンドポイントを、両方のエンドポイント（サーバーと関連クライアント）とともに [回線/VC 360*（Circuits/VCs 360*）] ダイアログボックスに表示します。また、[プロビジョニング状態（Provisioning State）] の横にある [i] アイコンをクリックし、各エンド ポイントにプッシュされている設定を表示します。

raw ソケット サービスの詳細のリファレンス

次の表に、raw ソケット サービスのタイプを定義する属性のリストを示し、説明します。

表 *53 : [raw* ソケットのサービス タイプ（*Raw Socket Service Type*）*]*：サーバー側とクライアント側の設定

属性	説明
[サーバー設定（Server Settings）] と [クライアント設定（Client Settings）]	
メディア タイプ（Media Type）	[メディア タイプ（Media Type）] ドロップダウン リストから次のいずれかを選択し、クロス回線サービスの一部としてマルチポイント RS422 サービスまたは RS4232 サービスを設定します。 • [RS232]：RS232 オプションをメディアタイプとして選択した場合、SyncRS232 チェックボックスは、シリアルインターフェイスのその他の設定とともに、同期操作に使用できます。 （注） RS232 を使用してサービス（シリアル Raw ソケットなど）を作成する場合、対応するサーバーと関連付けられたクライアントを一度に 1 つのメディア タイプのみで設定できるように、サポートされているサービスの設定時に両方のエンドに RS232 または RS422 が搭載されている必要があります。これらの設定は、デバイス上とともに EPNM からも行えます。 • [RS422]：RS 422 マルチポイントサービスのクライアント、サーバー、およびパケット化を設定できます。
RS232 の同期（Sync RS232）	サービスに対して RS232 の同期モードを有効にするには、このチェックボックスをオンにします。

属性	説明
デバイス名（Device Name）	raw ソケット サービスでサーバーとクライアントとして機能するデバイスの名前。
ポート名（Port Name）	raw ソケット サービスのサーバー デバイスとクライアント デバイス上のインターフェイスの名前。
サーバー アドレスとサーバー ポート（Server Address and Server Port）	サーバーの IP アドレスとポート番号。
許容セッション数（Allowed Sessions）	インターフェイスごとの TCP raw ソケットセッション数の制限を事前設定用。デフォルト値は 32 です。
クライアントアドレスとクライアントポート（Client Address and Client Port）	クライアントの IP アドレスとポート番号。
接続アイドルタイムアウト（Connection Idle Timeout）	raw ソケット サービスの TCP セッションのタイムアウト設定。この間隔でクライアントとサーバーの間でデータが転送されない場合、TCP セッションは終了します。その後、クライアントはサーバーとの TCP セッションの再確立を自動的に試みます。
VRF	サーバーとクライアントが接続してデータを転送する Virtual Route Forwarding（VRF）インターフェイス。 （注） VRF 定義がサーバーとクライアントの両方で共通であることを確認します。
速度（Speed）	シリアル リンクの速度（キロ ビット/秒）。この回線設定は、[同期サービス設定（Sync service settings）] ではオプションです。
データ ビット（Data Bits）	シリアル回線/VC を介して送信されるパケットあたりの実際のデータの測定値。値は 5、6、7、および 8 です。この回線設定は、[同期サービス設定（Sync service settings）] ではオプションです。
ストップ ビット（Stop Bits）	1 つのパケットの通信の終了を示します。値は 1、1.5、および 2 ビットです。この回線設定は、[同期サービス設定（Sync service settings）] ではオプションです。
パリティ（Parity）	シリアル通信のエラーを確認します。この回線設定は、[同期サービス設定（Sync service settings）] ではオプションです。
デュプレックス モード（Duplex Mode）	選択したシリアル サービスのデュプレックス モード。この回線設定は、[同期サービス設定（Sync service settings）] ではオプションです。

属性	説明
DTR	次のいずれかのオプションを選択します。 • [使用済み（Used）]：接続されたケーブルがない場合は、顧客エンドからデータ端末レディ（DTR）機器を設定できます。 • [未使用（Not Used）]：接続されたケーブルがない場合は、顧客エンドからデータ端末レディ（DTR）機器を設定できません。 （注） このオプションは、SyncRS232 チェックボックスがオンの場合にのみ使用できます。
クロック レート（Clock Rate）	サービスに対して目的のクロック レートをビット/秒単位（bps）で選択します。有効な値は 48000 と 64000 です。
NRZI エンコーディング（NRZI Encoding）	サービスに対してNonReturn-to-Zero Inverted（NRZI）エンコードメカニズムを有効にするには、このチェックボックスをオンにします。
制御信号トランスポート（Control Signal Transport）	ハードウェア制御信号をリモート PE に送信する必要があるかどうかを指定するには、このチェックボックスをオンにします。
周波数（Frequency）	必要な周波数を入力します。有効な値は、50 ～ 200 です。 （注） このフィールドは、[制御信号トランスポート（Control Signal Transport）] チェックボックスをオンにした場合にのみ使用できます。
フレーム パターン（Frame Pattern）	内部信号の転送に使用する次のオプションから、必要なフレーム形式のいずれかを選択します。 • [BCN]：ビーコン • [CFGR]：テスト用の設定 • [NR0]：非予約 0 • [NR1]：非予約 1 • [NR2]：非予約 2 • [NR3]：非予約 3
接続トポロジ（Connection Topology）	サービスの接続トポロジ（ポイントツーポイントまたはポイントツーマルチポイントのいずれか）が表示されます。
パケット化設定（Packetization Settings）	

属性	説明
パケット長（Packet Length）	シリアル データをピアに送信するルーティング デバイス（サーバーまたはクライアントのいずれか）をトリガーするパケット長。デバイスがバッファ内の指定したバイト数のデータを収集すると、蓄積されたデータをパケット化して raw ソケット ピアに転送します。
フラグメント オフ（Fragment Off）	このチェックボックスをオンにすると、このサービスのフレーム リレーのフラグメント化が無効になります。
パケット タイマー（Packet Timer）	デバイス（サーバーまたはクライアントのいずれか）がストリーム内で次の文字を受信するまでの時間をミリ秒単位で指定します。パケット タイマーの期限終了までに文字が受信されない場合、デバイスがバッファ内で累積したデータはパケット化され、raw ソケット ピアに転送されます。
特殊文字（Special Char）	バッファ内に蓄積されたデータをパケット化し、raw ソケット ピアに送信するためにデバイス（サーバーまたはクライアントのいずれか）をトリガーする文字。指定した特殊文字を受信すると、デバイスは蓄積されたデータをパケット化し、raw ソケット ピアに送信します。

回線/VC プロファイル

プロファイルには、各種回線/VC固有の一連の属性が含まれています。作成したプロファイルは、回線/VCの作成時にすべてのユーザーに対して選択可能になります。プロファイルを選択すると、プロビジョニング ウィザードにプロファイル属性が読み込まれます。ユーザーが行う必要がある操作はサービスのエンドポイントの定義だけです。また必要に応じて、回線/VCのプロビジョニング前に多少変更を行います。

作成できるプロファイルのタイプは、プロビジョニング可能な回線/VCのタイプを反映しています。

各プロファイルには一意の名前が指定されるので、回線/VCタイプごとに、必要に応じて複数のプロファイルを作成できます。

プロファイルを作成するには、次の手順に従います。

ステップ 1 左側のナビゲーション ペインで **Inventory > Other > Profiles** を選択します。[プロファイル（Profiles）] ウィンドウが開き、既存のプロファイルの表が表示されます（存在する場合）。表でプロファイルを選択して、そのプロファイルを編集または削除できます。

ステップ 2 **Create Profile** をクリックします。

ステップ 3 プロファイル作成ウィザードで、プロファイルに一意の名前を指定し、説明を入力します。

ステップ 4 [テクノロジー（Technology）] リストから、[**Carrier Ethernet**]、[**Optical**]、または [**L3VPN**] を選択します。選択したテクノロジーに関連するサービス タイプが表示されます。

ステップ 5 必要なサービス タイプを選択します。

L3VPN のサービスの場合、ほとんどの L3VPN サービス作成フィールドに値を事前に読み込むことができるプロファイルを作成するには、[ユニキャスト（Unicast）] を選択します。L3VPN サービスの IP SLA 固有のオプションを使用してプロファイルを作成するには、[IPSLA 操作（IPSLA Operations）] を選択します。

ステップ 6 **Next** をクリックし、属性定義ページに移動して、選択したサービス タイプの属性を定義します。プロファイルの属性は、プロビジョニング ウィザードの属性と同じであり、次に示す関連セクションで説明しています。

イーサネット VC 属性の詳細については、次のトピックで説明します。

- サービス自体に関連する属性については、次を参照してください：サービス詳細の参考資料（650 ページ）
- UNI 固有の属性については、次を参照してください：新規 UNI の詳細リファレンス （651 ページ）
- サービス内で機能する UNI に関連する属性については、UNI サービス詳細の参照 （652 ページ）を参照してください。
- UNI 属性については、次を参照してください。 UNI としてのデバイスおよびインターフェイスの設定（656 ページ）
- ENNI 属性については、次を参照してください：デバイスとインターフェイスを ENNI として設定する （657 ページ）

OCH 属性と OTN 属性については、OCH 回線タイプの [回線（Circuit）] セクション リファレンス （671 ページ）とOTN 回線タイプの回線セクション参照 （691 ページ）で説明します。

L3VPN 属性については、新規 L3VPN サービスの作成およびプロビジョニング （705 ページ）とL3VPN サービスの詳細表示 （722 ページ）で説明します。

ステップ 7 属性の定義が完了したら、**Create Profile** をクリックします。[プロファイル（Profiles）] ウィンドウの表にプロファイルが追加されます。

顧客の作成

回線/VC プロビジョニング プロセス中に選択に使用できるように、システムに顧客を作成する必要があります。

顧客を作成するには、次の手順を実行します。

ステップ 1 左側のサイドバーから **Inventory > Other > Customers** を選択します。

ステップ 2 **Create Customer** をクリックします。

ステップ 3 顧客の名前と（必要に応じて）説明を入力します。

ステップ 4 **OK** をクリックします。これで、顧客が顧客のテーブルに追加されます。編集または削除する顧客を選択できます。

アンマネージド エンドポイントを使用した回線/VC のプロビジョニング

1 つ以上のエンドポイントが Cisco EPN Manager で管理されないデバイスであっても、回線/VC を作成してプロビジョニングすることができます。[プロビジョニング ウィザード（Provisioning Wizard）] を使用することで、エンドポイント デバイスを「アンマネージド」として識別したり、システムが回線/VC を作成できるようにアンマネージドデバイスに関する情報を指定したりできます。アンマネージドデバイスを識別すると、そのデバイスはシステムのアンマネージド デバイス グループ内で有効になり、他のサービスに使用できるようになります。

ステップ 1 回線/VC のプロビジョニング （629 ページ）の説明に従って、対象のテクノロジーに応じた回線/VC 作成プロセスを開始します。

ステップ 2 ポイントツーポイント EVC および CEM サービスの場合：

a) Z エンドポイントを定義する際に、[アンマネージド デバイス（Unmanaged Device）] チェックボックスをオンにします。[アンマネージドデバイスの詳細（Unmanaged Device Details）] パネルが開きます。

b) システム内ですでに識別されているアンマネージド デバイスの場合、[新規デバイス（New Device）] チェックボックスをオフにして、リストから必要なデバイスを選択します。新しいアンマネージド デバイスを識別する場合は、デバイス名、IP アドレス、および LDP IP を入力します。LDP IP は、管理対象デバイス上の疑似回線のネイバー アドレスとして使用されます。

ステップ 3 ポイントツーマルチポイントまたはマルチポイントツーマルチポイント EVC の場合、[アンマネージド UNI（Unmanaged UNI）] ページでテーブル内のプラス アイコンをクリックして行を追加し、選択した行に対するアンマネージド デバイスの詳細とサービス エンドポイントの詳細を定義します。

ステップ 4 回線/VC のプロビジョニング （629 ページ）の説明に従って、対象テクノロジーの回線/VC の作成およびプロビジョニング プロセスを完了します。

テンプレートを使用した回線/VC の拡張

回線/VC を作成してプロビジョニングすると、Cisco EPN Manager は参加デバイスに一連の CLI コマンドを設定します。同じデバイスに追加のコマンドを設定する必要がある場合は、それらのコマンドを含むテンプレートを作成して、回線/VC の作成プロセス中にそのテンプレートを含めることができます。こうすることで、Cisco EPN Manager による設定内容を超えて、回線/VC を効果的に拡張できます。この機能はプロビジョニング ウィザードで使用できますが、回線/VC の作成前または変更前に作成されるテンプレートに依存しています。

CLI テンプレートを使用した回線/VC の拡張には、次の手順が含まれます。

1. 空白のテンプレートまたは既存のテンプレートを使用して、CLI テンプレートを作成します。空白テンプレートを使用した新しい CLI 設定テンプレートの作成 （577 ページ）および既存のテンプレートを使用した新規 CLI 設定テンプレートの作成 （578 ページ）を参照してください。

2. 回線/VC を作成または変更し、CLI テンプレートを付加します。回線/VC のプロビジョニング （629 ページ）を参照してください。

ステップ 1 CLI テンプレートを作成します。

a) 左のサイドバーで、[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] を選択します。

b) [テンプレート（Templates）] パネルで、[CLI テンプレート（CLI Templates）] > [CLI] を選択します。

c) CLI、グローバル変数、および/またはテンプレート変数を使用して、新しい回線の識別情報を指定し、テンプレートの内容を定義します。「デバイスのインベントリの即時収集（同期）」およびテンプレートでのグローバル変数の使用 （584 ページ）を参照してください。

d) [新しいテンプレートとして保存（Save as New Template）] をクリックします。

e) [マイ テンプレート（My Templates）] > [CLI テンプレート（ユーザー定義）（CLI Templates (User Defined)）] の下に、新しい CLI テンプレートが保存されます。

ステップ 2 作成したテンプレート（または該当する場合には異なるテンプレート）を含むサービスを作成または変更します。

a) 左側のサイドバーから、[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）] を選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

b) [回線/VC（Circuits/VCs）] タブをクリックします。

c) [回線/VC（Circuits/VCs）] ペイン ツールバーから、[+]（[作成（Create）]）アイコンをクリックするか、回線を選択してから鉛筆（[変更（Modify）]）アイコンをクリックします。

マップの右側の新しいペインでプロビジョニング ウィザードが開きます。

d) 必要な回線または VC の作成または変更を開始します。回線/VC のプロビジョニング （629 ページ）および回線/VC の変更 （821 ページ）を参照してください。

e) [サービス テンプレート（Service Template）] ページで、テンプレートをサービス設定のプレフィックスにする場合は [事前設定（Pre-Configuration）] セクションを使用し、テンプレートをサービス設定のサフィックスにする場合は [事後設定（Post-Configuration）] セクションを使用します。

f) [テンプレート（Template）] ドロップダウン メニューで、必要な CLI テンプレートを選択します。

事前設定オプションと事後設定オプションの両方に同じ CLI テンプレートを選択することはできません。

g) [テンプレートの使用（Template Usage）] ドロップダウン メニューで、デバイスに CLI テンプレートを設定する条件を示すオプションを選択します。たとえば [サービス作成のみ（Service Create Only）] を選択した場合、サービスの作成時にのみ、テンプレート CLI がデバイスに設定されます。サービスの変更時には設定されません。

h) テンプレート パラメータの値を入力します。ここに示すパラメータは、テンプレートに定義された変数によって異なります。

i) [送信（Submit）] をクリックします。

（注） デフォルトでは、サービスに参加するすべてのデバイスに、選択された CLI テンプレートが関連付けられます。CLIテンプレートに関連付ける特定のデバイスを選択することはできません。

ステップ 3 設定したテンプレート用のロールバックテンプレートを設定できます。設定例：ロールバックテンプレート （785 ページ） を参照してください。

ステップ 4 インタラクティブテンプレートを設定することもできます。設定例：インタラクティブテンプレート （786 ページ） を参照してください。

設定例：CLI テンプレートを使用した回線/VC の拡張

設定例 1：グローバルおよびテンプレート（ローカル）変数を持つ CLI テンプレートを使用した Cisco ASR 903 デバイスでの L3VPN サービスの拡張：

```
vrf definition Testdoc1
exit
vrf Testdoc1
  vpn id 36B:3
  address-family ipv4 unicast
    import route-target
      65:1
    export route-target
      65:1
  address-family ipv6 unicast
    import route-target
      65:1
    export route-target
      65:1
interface  GigabitEthernet0/0/0/11.2
  vrf   Testdoc1
  ipv4 address 4.5.7.8 255.255.255.0
  mtu 1522
router bgp 140
  vrf  Testdoc1
    rd auto
    address-family ipv6 unicast
    address-family ipv4 unicast
      redistribute static metric 54
    neighbor 3.4.6.8
      remote-as 21
      address-family ipv4 unicast
        exit
      exit
    exit
  exit
  interface GigabitEthernet0/0/6
  desc postconfig
  delay 5988
  mtu 436
  exit
```

設定例 2：グローバル変数とテンプレート（ローカル）変数を持つ CLI テンプレートを使用した CEM サービスの拡張：

```
#set($interfaceNameList = $gv.service-cem-cemInterfaceNameList.split(","))
#set($cemGroupNumberList = $gv.service-cem-cemGroupNumberList.split(","))
#set($count = 0)
#foreach($interfaceName in $interfaceNameList)
  interface $interfaceName
    service-policy input MainInterfacePolicy
    #if($count == 0)
      cem $cemGroupNumberList[0]
    #else
      cem $cemGroupNumberList[1]
    #end
        service-policy input servicePolicy
    #set($count = $count+1)
#end
```

設定例 3：QoS over CEM を設定する CEM サービスの拡張：

```
#set($count = 0)
#foreach($interfaceName in $gv.service-cem-cemInterfaceNameList)
interface $interfaceName
service-policy input MainInterfacePolicy
#if($count == 0)
cem $gv.service-cem-cemGroupNumberList[0]
#else
cem $gv.service-cem-cemGroupNumberList[1]
#end
service-policy input servicePolicy
#set($count = $count+1)
#end
exit
```

設定例 4：Cisco ME3800 デバイス上でのグローバル変数とテンプレート変数を持つ CLI テンプレートを使用した CE サービスの拡張：強調表示されたテキストは、CE サービスのプロビジョニング設定の前後に追加される設定前と設定後の変更を表します。

```
ethernet cfm domain EVC level 4
  service evplextnpseudowireclass_ evc evplextnpseudowireclass_
    continuity-check
    continuity-check interval 1s
ethernet evc evplextnpseudowireclass
interface GigabitEthernet0/11
  no shutdown
  no spanning-tree portfast
  mtu 1522
  ethernet uni id 3800x
  service instance 1 ethernet evplextnpseudowireclass
    encapsulation dot1q 88
    xconnect 192.168.12.29 51 encapsulation mpls  pw-class PWClass_51_192-168-12-29
      mtu 1508
  service instance 1 ethernet evplextnpseudowireclass_
    cfm mep domain EVC mpid 2
    ethernet lmi ce-vlan map 88
ip sla 17
  ethernet y1731 loss SLM domain EVC evc evplextnpseudowireclass_ mpid 1 cos 5 source
mpid 2
    history interval 5
    aggregate interval 60
ip sla schedule 17 life forever start-time after 00:02:00
```

設定例 5：グローバル変数とテンプレート（ローカル）変数を持つ CLI テンプレートを使用したレイヤ 3 リンク サービスの拡張：

```
##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
 "MODIFY")
 ##XE DEVICE
 #if($variant=="IOS-XE")
 #if($gv.service-l3Link-routingProtocolName=="BGP")
   router bgp $gv.service-l3Link-routerProcessId
             address-family ipv4
           neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
    ##assume A End as remote building
           #if($gv.service-l3Link-isRouteReflectorClient=="TRUE" && $prefixListName!=""
 && $gv.service-l3Link-endPointDesignation=="AEND")
    neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list send
                neighbor $gv.service-l3Link-bgpNeighborName prefix-list $prefixListName
 in
                  #elseif($gv.service-l3Link-isRouteReflectorClient=="TRUE" &&
$prefixListName!="" && $gv.service-l3Link-endPointDesignation=="ZEND")
    neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list receive
           #end
                exit
         exit
        #end

        #if($xeMTU!="" || $xeClnsMTU!="")
         interface $gv.service-l3Link-interfaceName
          #if($xeMTU!="")
              mtu $xeMTU
          #end
          #if($xeClnsMTU!="")
              clns mtu $xeClnsMTU
          #end
            exit
        #end

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily !="" && $addressFamily=="vpnv4")
         router bgp $gv.service-l3Link-routerProcessId
          address-family $addressFamily
           neighbor $gv.service-l3Link-bgpNeighborName activate
     neighbor $gv.service-l3Link-bgpNeighborName send-community both
     #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
     neighbor $gv.service-l3Link-bgpNeighborName route-reflector-client
     #end
     bgp additional-paths install
     neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
           exit
         exit
 #end
 #end
 ##XR DEVICE
 #else

  #if($xrMTU!="")
  #if($gv.service-l3Link-subInterfaceName!="")
             interface $gv.service-l3Link-subInterfaceName
                  mtu $xrMTU
                exit
         #else
             interface $gv.service-l3Link-interfaceName
                  mtu $xrMTU
                exit
            #end
        #end
```

```
        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily !="" && $addressFamily=="vpnv4")
         router bgp $gv.service-l3Link-routerProcessId
          address-family $addressFamily unicast
      additional-paths receive
                exit
          neighbor $gv.service-l3Link-bgpNeighborName
           address-family $addressFamily unicast
                     #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
            route-reflector-client
                     #end
          aigp
                     #if( $routePolicyName!="")
          route-policy $routePolicyName in
                     #end
                    exit
               exit
            exit
        #end
        #end


 #end

##DELETE USE CASE
#elseif($gv.service-serviceOperationType == "DELETE")
 ##XE DEVICE
 #if($variant=="IOS-XE")

        #if($xeMTU!="" || $xeClnsMTU!="")
         interface $gv.service-l3Link-interfaceName
          #if($xeMTU!="")
                  no mtu $xeMTU
          #end
          #if($xeClnsMTU!="")
                  no clns mtu $xeClnsMTU
          #end
            exit
       #end

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily !="" && $addressFamily=="vpnv4")
         router bgp $gv.service-l3Link-routerProcessId
          no address-family $addressFamily
            exit
        #end
        #end


 ##XR DEVICE
 #else
  #if($xrMTU!="")
   #if($gv.service-l3Link-subInterfaceName=="")
              interface $gv.service-l3Link-interfaceName
                  no mtu $xrMTU
                exit
            #end
        #end

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily !="" && $addressFamily=="vpnv4")
         router bgp $gv.service-l3Link-routerProcessId
          address-family $addressFamily unicast
    no additional-paths receive
```

```
   exit
   neighbor $gv.service-l3Link-bgpNeighborName
           no address-family $addressFamily unicast
   exit
            exit

        #end
        #end

 #end

#end
```

設定例 6：グローバル変数とテンプレート（ローカル）変数を持つ CLI テンプレートを使用した双方向 TE トンネルの拡張：

```
##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
 "MODIFY")
  #if($variant && $variant=="IOS-XE")
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
         #if($xeBandWidth && $xeBandWidth !="")
               interface Tunnel$gv.service-teTunnel-tunnelId
                  bandwidth $xeMaxBandWidth
                       tunnel mpls traffic-eng auto-bw frequency $xeBandWidth max-bw
$xeMaxBandWidth min-bw $xeMinBandWidth
               exit
          #end
   #end
 #else
      #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
     #if($xrBandWidth && $xrBandWidth!="")
             interface tunnel-te$gv.service-teTunnel-tunnelId
                 bandwidth $xrMaxBandWidth
                 auto-bw
                      bw-limit min $xrMinBandWidth max $xrMaxBandWidth
                     application $xrBandWidth
                exit
             exit
        #end
 #end
 #end
#elseif($gv.service-serviceOperationType == "DELETE")
 #if($variant && $variant=="IOS-XE")
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
  #if($xeBandWidth && $xeBandWidth!="")
              interface Tunnel$gv.service-teTunnel-tunnelId
                 no bandwidth
                 no tunnel mpls traffic-eng auto-bw
              exit
          #end
   #end
 #else
      #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
          #if($xrBandWidth && $xrBandWidth!="")
             interface tunnel-te$gv.service-teTunnel-tunnelId
                 no bandwidth
                 no auto-bw
             exit
          #end
 #end
 #end

#end
```

設定例：ロールバックテンプレート

ロールバックテンプレートを作成して、展開に失敗した場合に使用することができます。[Configuration] > [Templates] > [Features and Technologies] の順に移動し、[CLI Templates] を選択してカスタム ロールバック テンプレートを設定します。テンプレートを設定する際は、ロールバックのフラグとして #ROLLBACK_CONFIG_START と #ROLLBACK_CONFIG_END を使用する必要があります。これらのフラグの間で、CLI がロールバックする必要があるものを指定する必要があります。これは、サービス前とサービス後の両方の設定に使用できます。

（注） これらのロールバックテンプレートは、光サービスには適用されません。

サンプルテンプレート形式

```
#ROLLBACK_CONFIG_START
interface GigabitEthernet0/0/20
mtu 1555
#ROLLBACK_CONFIG_END
```

設定例 1：パラメータのない設定前 CLI のロールバック：

CLI の例：

```
snmp-server enable traps
FAIL here
vrf definition PreConfigTest
 vpn id 12:566
 rd 23.23.23.23:2
 address-family ipv4
  route-target import 32:1
  route-target export 32:1
interface GigabitEthernet0/10
 service instance 3 ethernet
  encapsulation dot1q 521
  rewrite ingress tag pop 1 symmetric
  bridge-domain 8
 exit
interface Vlan8
 no shutdown
 mtu 1522
 vrf forwarding PreConfigTest
 ip address 33.44.24.55 255.255.255.0
router bgp 100
 address-family ipv4 vrf PreConfigTest
  exit
```

設定例 2: パラメータのない設定後 CLI のロールバック：

CLI の例：

```
snmp-server enable traps
vrf definition PreConfigTest
 vpn id 12:566
 rd 23.23.23.23:3
 address-family ipv4
  route-target import 24:1
  route-target export 24:1
```

```
interface GigabitEthernet0/10
 service instance 4 ethernet
  encapsulation dot1q 685
  rewrite ingress tag pop 1 symmetric
  bridge-domain 9
 exit
interface Vlan9
 no shutdown
 mtu 1522
 vrf forwarding PostConfigTest
 ip address 23.44.55.56 255.255.255.0
router bgp 100
 address-family ipv4 vrf PostConfigTest
  exit
 exit
snmp-server enable traps
FAIL here
```

設定例 3：設定前有効テンプレート、設定後無効テンプレート、展開失敗、およびロールバック CLI

CLI の例：

```
snmp-server enable traps
vrf definition PrePostConfig
 vpn id 34:55
 rd 23.23.23.23:4
 address-family ipv4
  route-target import 234:1
  route-target export 234:1
interface GigabitEthernet0/10
 service instance 5 ethernet
  encapsulation dot1q 664
  rewrite ingress tag pop 1 symmetric
  bridge-domain 11
 exit
interface Vlan11
 no shutdown
 mtu 1522
 vrf forwarding PrePostConfig
 ip address 44.55.22.55 255.255.255.0
router bgp 100
 address-family ipv4 vrf PrePostConfig
  exit
 exit
snmp-server enable traps
FAIL here
```

設定例：インタラクティブ テンプレート

設定例 1：単一のプロンプトを含むコマンドのインタラクティブテンプレート：

テンプレートの形式：

```
#INTERACTIVE
no username test<IQ>confirm<R>y
#ENDS_INTERACTIVE
```

CLI の例（サービス前設定として設定されたテンプレート）：

```
no username test
bridge-domain 8
```

```
ethernet cfm domain EVC level 4
  service b_evplan_4Mar evc b_evplan_4Mar vlan 8
    continuity-check
    continuity-check interval 1s
ethernet evc b_evplan_4Mar
  oam protocol cfm domain EVC
interface GigabitEthernet0/0/1
  ethernet uni id UniName3
  service instance 2 ethernet b_evplan_4Mar
    encapsulation dot1q 22
    bridge-domain 8
    cfm mep domain EVC mpid 1
    ethernet lmi ce-vlan map 22
    snmp trap link-status
    exit
  exit
```

設定例 2：複数のプロンプトを含むコマンドのインタラクティブテンプレート：

テンプレートの形式：

```
#INTERACTIVE
crypto key generate rsa<IQ>% Do you really want to replace them? [yes/no]:<EM><R>yes<IQ>How
 many bits in the modulus [512]:<EM><R>512
#ENDS_INTERACTIVE
```

CLI の例（サービス後設定として設定されたテンプレート）：

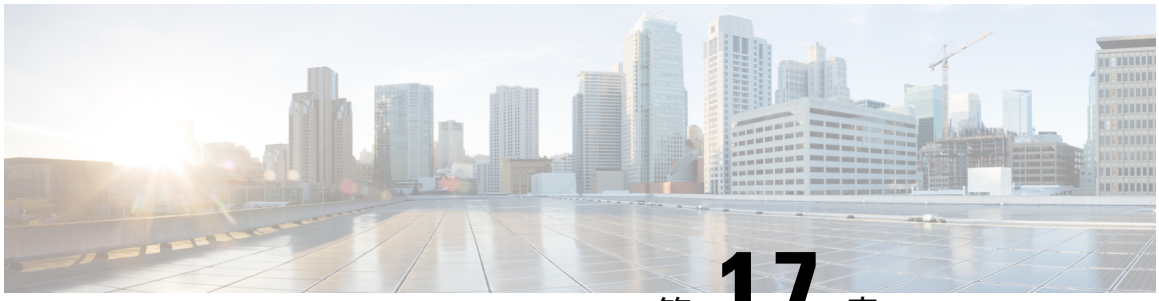
```
bridge-domain 8
ethernet cfm domain EVC level 4
  service b_evplan_4Mar evc b_evplan_4Mar vlan 8
    continuity-check
    continuity-check interval 1s
ethernet evc b_evplan_4Mar
  oam protocol cfm domain EVC
interface GigabitEthernet0/0/0
  ethernet uni id UniName4
  ethernet lmi interface
  service instance 1 ethernet b_evplan_4Mar
    encapsulation dot1q 345
    bridge-domain 8
    cfm mep domain EVC mpid 1
    ethernet lmi ce-vlan map 345
    snmp trap link-status
    exit
  exit
crypto key generate rsa
```

プロビジョニング障害の syslog

サービスプロビジョニングの障害が発生すると、EPNM は syslog を生成し、EPNM で設定された受信者に送信します。この syslog は、作成、変更、削除、および昇格操作のために生成されます。

受信者は、EPNM サーバーにログインすることによって CLI で設定できます。CLI 経由の接続（953 ページ） を参照してください。**conf** モードで **logging security <syslog receiver ip>** を実行します。

syslog の視覚的な表現は、受信側のマシン/サーバーで使用されているソフトウェアによって異なります。



第 17 章

検出/プロビジョニングされた回線/VCの表示と管理

サービス検出の有効化および無効化

Cisco EPN Manager はサービス検出（ディスカバリ）機能を使用して、ネットワーク内に存在する回線/VC、およびプロビジョニング ウィザードを使ってプロビジョニングされた回線/VC を自動的に検出します。

サービス検出機能は、デフォルトで有効になっています。この機能を無効にするように選択できます。サービス検出を無効化すると、Cisco EPN Manager の検出済みサービスがすべて削除されます。ただし、Cisco EPN Manager を使用してプロビジョニングされたサービスは残り、状態が「見つかりません」になります。[履歴設定（History Settings）] オプションを使用して、[回線/VC の履歴（Circuit/VC History）] テーブルに表示される回線/VC の変更が検出されたバージョンの最大数を設定します。変更を適用するには、サーバーを再起動する必要があります。

（注） [履歴設定（History Settings）] の設定は、光回線で検出された変更にのみ関係します。

サービス検出を無効にするには、次の手順を実行します。

ステップ 1 左側のバーから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[回線/VC（Circuits/VCs）] > [ディスカバリ設定（Discovery Settings）]** を選択します。

ステップ 2 [サービス ディスカバリの有効化（Enable Service Discovery）] チェックボックスをオフにします。

ステップ 3 Cisco EPN Manager を再起動し、変更を適用します。Cisco EPN Manager の停止と再起動 （973 ページ）を参照してください

回線または VC の状態

[回線/VC のプライマリ状態（Circuit or Primary States）]：サービサビリティ、検出、アラーム、プロビジョニングの順に回線に関する最も重要な状態情報を伝達します。これは、通常、回線または VC のテーブル内の最初の列に表示されます。

回線または VC のプライマリ状態（Circuit or VC Primary States）	アイコン	サービサビリティ	検出	Alarm	プロビジョニング
欠落（Missing）		—	欠落（Missing）	—	—
Down		Down	—	—	—

クリティカル（Critical）		—	—	クリティカル（Critical）	—
[メジャー（Major）]		—	—	[メジャー（Major）]	—
[マイナー（Minor）]		—	—	[マイナー（Minor）]	—
一部ダウン		一部	—	—	—
管理上ダウン		管理上ダウン	—	—	—
一部検出		—	一部	—	—
失敗しました（Failed）		—	—	—	（作成、変更、または削除）失敗
進行中		—	—	—	（作成、変更、または削除）進行中
警告			—	警告	—
アップ		アップ	—	—	—
自動アップ		自動アップ	—	—	—
情報（Info）		—	—	情報（Info）	—
クリア済み		—	—	クリア済み	—

[回線/VC のサービサビリティ状態（Circuit or VC Serviceability）]：この値は、回線または VC の管理状態と動作状態の組み合わせです。サービスの運用性に影響するため、管理状態が表示されます。光回線の場合は、管理状態によってアクティブ化および非アクティブ化アクションが使用可能かどうかも決定されます。動作状態は、サービスが機能しているかどうかをすばやく特定するために表示されます。

回線または VC のサービサビリティ状態	アイコン	説明
管理上ダウン		管理者が回線または VC を手動でシャットダウンします。
ダウン（Down）		回線または VC は運用上はダウンし、管理上はアップします。

アップ（Up）		回線または VC は、運用上も、管理上もアップします。
自動アップ（Auto Up）		回線または VC は運用上は自動アップ、管理上はアップします。特定のデバイスのみが自動アップの動作状態をサポートしています。
取得不可		回線または VC はまだ検出されていないか、その動作ステータスが取得できません。
一部		回線/VC の動作状態または管理状態が部分的です。 • [部分管理状態（Partial admin state）]：回線または VC に（一部のサービス リソースをアクティブ化し、他のリソースを非アクティブ化する）混在管理要求があるか、または管理上アップしているリソースとダウンしているリソースが混在しているか、あるいは動作状態が取得できないリソースがあります。 • [部分動作状態（Partial operational state）]：回線または VC に一部のリソースのアクティブ化と非アクティブ化が混在しているか、またはリソースの一部の動作状態が取得できません。
Up - Unprotected		保護パスで設定された回線/VC は動作していますが、重大な障害が原因で代替パスに切り替えることはできません。 （注） このサービスアビリティ ステータス表示は、Y 字型ケーブル保護および保護 ODU を使用した OCHCC WSON 回線でサポートされます。

次の表に、さまざまなシナリオでの回線/VC の有用性状態の詳細を示します。

テクノロジー	サービス タイプ	シナリオ	サービスアビリティ状態

キャリア イーサネット	EPL、EVPL、アクセス EPL、およびアクセス EVPL	エンドポイント（サービスインスタンス/サブインターフェイス）、クロス接続、およびサービスに参加している疑似回線の動作状態がアップの場合	アップ
		サービスに参加している送信元と宛先（サービスインスタンス/サブインターフェイス）の両方の管理状態がダウンの場合	管理上ダウン
		他のすべてのシナリオで、サービスに参加している 1 つ以上のエンドポイント（サービスインスタンス/サブインターフェイス）、クロス接続、または疑似回線がダウンしている場合	ダウン（Down）
	EP-LAN、EVP-LAN、EP ツリー、および EVP ツリー	サービスに参加しているすべてのエンドポイント（サービスインスタンス/サブインターフェイス）、ブリッジドメイン、VFI、および疑似回線がアップしている場合	アップ（Up）
		サービスに参加している 2 つ以上のエンドポイント（サービスインスタンス/サブインターフェイス）の動作状態がアップで、残りのエンドポイントがダウンの場合	一部
			管理上ダウン

		サービスに参加しているすべてのエンドポイント（サービスインスタンス/サブインターフェイス）の管理状態がダウンの場合	
		サービスに参加している 1 つ以上のエンドポイント（サービスインスタンス/サブインターフェイス）の動作状態がアップで、残りのエンドポイントがダウンの場合	ダウン（Down）
回線エミュレーション（Circuit Emulation）	すべてのサービスタイプ	サービスに参加しているエンドポイント（cemGroup）、基盤となっている TDM コントローラ、クロス接続、および疑似回線の動作状態がアップの場合	アップ（Up）
		サービスに参加している送信元と宛先のエンドポイント（cemGroup）の両方の管理状態がダウンの場合	管理上ダウン
		他のすべてのシナリオで、サービスに参加しているエンドポイント（cemGroup）、基盤となっている TDM コントローラ、クロス接続、および疑似回線のいずれかの動作状態がダウンの場合	ダウン（Down）

MPLS	単方向 TE トンネル（Unidirectional TE Tunnel）	トンネルインターフェイスの動作状態がアップの場合	アップ（Up）
		トンネルインターフェイスの管理状態がダウンの場合	管理上ダウン（Admin Down）
		他のすべてのシナリオでは、トンネルの動作状態がダウンの場合	ダウン（Down）
	双方向 TE トンネル（Bidirectional TE Tunnel）	トンネルの両端のインターフェイスの動作状態がアップの場合	アップ（Up）
		トンネルの両端のインターフェイスの管理者状態がダウンの場合	管理上ダウン（Admin Down）
		それ以外の場合は、トンネルインターフェイスの動作状態がダウンの場合	ダウン（Down）

シリアル（Serial）	RS232、RS422、および RS485	サービスに参加しているエンドポイント（channelGroup）、基盤となっているシリアルインターフェイス、クロス接続、および疑似回線の動作状態がアップの場合	アップ
		サービスに参加している送信元と宛先のエンドポイント（channelGroup）の両方の管理状態がダウンの場合 送信元または宛先のエンドポイント（channelGroup）のいずれかの管理状態がダウンの場合	管理上ダウン（Admin Down）
		他のすべてのシナリオで、サービスに参加しているエンドポイント（channelGroup）、基盤となっているシリアルインターフェイス、クロス接続、および疑似回線のいずれかの動作状態がダウンの場合	ダウン（Down）
	raw ソケット（Raw Socket）	サーバーと関連付けられているそのすべてのクライアントセッションがアップの場合	アップ（Up）
		サーバーがアップで、関連付けられているそのすべてのクライアントセッションがダウンの場合	ダウン（Down）
			管理上ダウン（Admin Down）

		サービスに参加している送信元と宛先のエンドポイント（channelGroup）の両方の管理状態がダウンの場合 サーバーの管理状態、または参加しているすべてのクライアントの管理状態がダウンの場合	
		サーバーと、関連付けられているそのすべてのクライアント セッションがダウンの場合	ダウン（Down）
		サーバーがアップで、関連付けられているそのいずれかのクライアントがアップの場合	部分（Partial）

レイヤ 3 VPN（Layer 3 VPN）		サービスに参加しているすべてのエンドポイント（サブインターフェイス、BDI、およびBVI）の動作状態がアップの場合	アップ
		サービスに参加している少なくとも 2 つのエンドポイント（サブインターフェイス、BDI、および BVI）の動作状態がアップで、残りのエンドポイントがダウンの場合	Partial
		サービスに参加しているすべてのエンドポイント（サブインターフェイス、BDI、およびBVI）の管理状態がダウンの場合	管理上ダウン
		サービスに参加している 1 つ以上のエンドポイント（サブインターフェイス、BDI、およびBVI）の動作状態がアップで、残りのエンドポイントがダウンの場合	ダウン（Down）
SR TE	SR ポリシー	SR ポリシーの動作状態がアップしている場合	アップ（Up）
		SR ポリシーの管理状態がダウンしている場合	管理上ダウン（Admin Down）
		他のすべてのシナリオでは、SR ポリシーの動作状態がダウンの場合	ダウン（Down）

[回線または VC の検出状態（Circuit or VC Discovery State）]：サービスとそのコンポーネントのネットワークから検出された最新の状態と構造を表します。検出されたバージョンがある場

合は、アプリケーションが実際にサービス自体をモニターしている（たとえば、有意義な動作データとパフォーマンス データを定義できる）ことを意味します。

回線または VC の検出状態（Circuit or VC Discovery State）	アイコン	説明
一部		Cisco EPN Manager によって部分的に検出された回線または VC。その想定エンティティのすべてが検出されたわけではありません。
完全（Full）		Cisco EPN Manager によって完全に検出された回線または VC。そのため、Cisco EPN Manager は、サービスをモニターして、有意義な動作データとフォーマンス データを提供できます。
欠落（Missing）		まだ Cisco EPN Manager によって検出されていない（ただし、プロビジョニング済みである可能性がある）回線または VC。
Resync		回線または VC は再同期されています。

[回線または VC のプロビジョニング状態（Circuit or VC Provisioning State）]：回線または VC についてプロビジョニングする目的があるかどうかと、目的がある場合はそのステータスを表します。調整レポートが生成された場合は、調整アクションの状態が反映されます。

回線または VC プロビジョニングの状態	アイコン	説明
なし（None）		回線または VC が検出されましたが、まだプロビジョニングされていません。回線/VC は変更または削除する場合にプロモートする必要があります。
失敗しました（Failed）		アクションが失敗しました。
進行中（In Progress）		アクションは開始されましたが、まだ完了していません。
計画済み		アクションは計画されましたが、まだ開始されていません。
成功		アクションは正常に完了しました。

回線/VC の表示

Cisco EPN Manager は、回線/VC を表示するためのさまざまな方法を提供します。

以下の回線/VC 情報を表示するには：	以下の手順を参照：
トポロジ マップ、回線/VC 360 ビュー、または回線/VC 詳細ページにおける特定の回線/VC	• 回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ） • 回線/VC に関する総合情報の取得：[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウ （810 ページ）
デバイス	特定のデバイスの回線/VC の表示 （813 ページ）
トポロジ マップまたは拡張テーブルのデバイス グループ	デバイス グループの回線/VC を表示する （813 ページ）
Cisco EPN Manager のすべて	Cisco EPN Manager ですべての回線/VC を表示 （815 ページ）

特定の回線/VC の詳細の表示

Cisco EPN Manager は、必要な詳細に応じて、特定の回線/VC に関する詳細を表示するさまざまな方法を提供します。

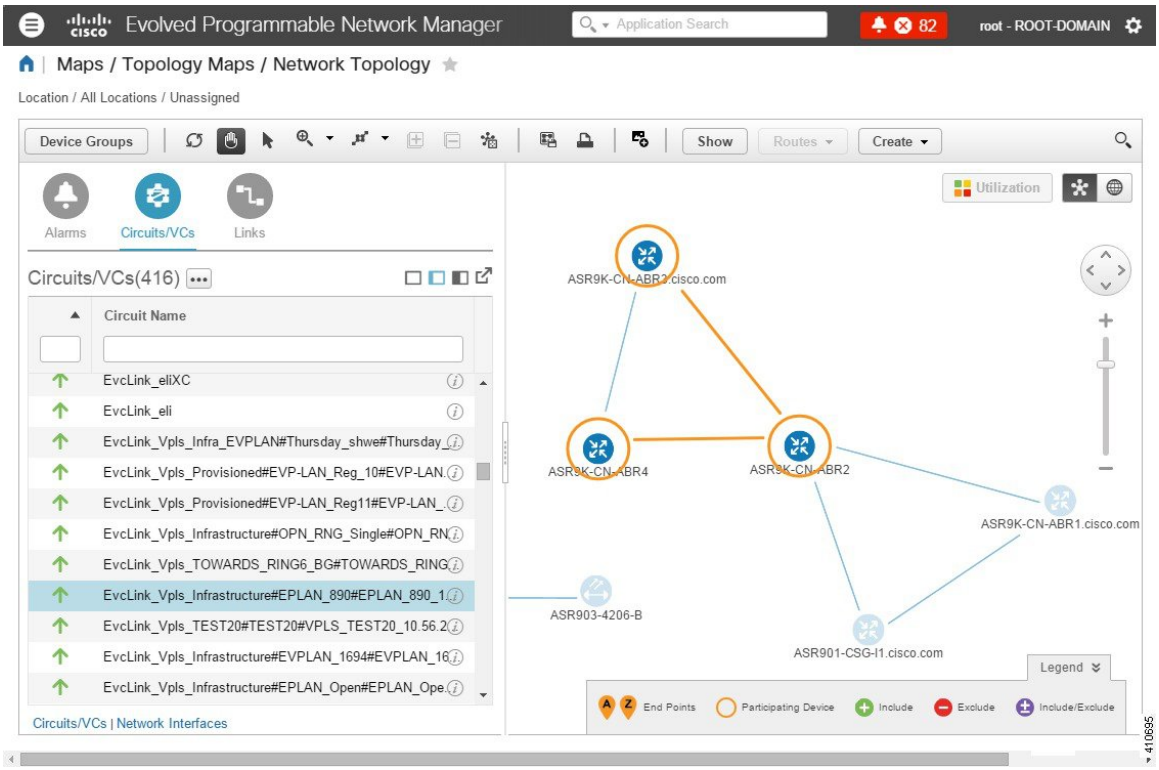
- トポロジ マップ内の特定の回線/VC を表示する （800 ページ）
- 回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ）
- 回線/VC に関する総合情報の取得：[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウ （810 ページ）
- 回線のバージョンの表示と比較（光） （812 ページ）

トポロジ マップ内の特定の回線/VC を表示する

回線/VC の操作には、既存のネットワーク トポロジ内で回線/VC がどのように展開されているかを確認することが非常に役立ちます。Cisco EPN Manager は、既存のトポロジ マップ上に回線/VC をオーバーレイして、回線/VC のエンドポイントとミッドポイント、エンドポイントのロール（該当する場合）、および回線/VC に関連する障害情報をわかりやすく示します。このオーバーレイ機能は、トポロジ マップだけでなく、Geo マップでも使用できます。

MPLS TE トンネルを使用してネットワーク上を伝送される CE サービスと CEM サービスの場合は、基盤となるトンネルもサービス オーバーレイとともにトポロジマップに表示されます。CE サービスまたは CEM サービスでの MPLS TE トンネルの割り当て方法については、キャリ

アイーサネット ネットワークのEVCのプロビジョニング（639ページ）と回線エミュレーション サービスのプロビジョニング（727 ページ）を参照します。



（注）
- 回線の検出状態が [見つからない（Missing）] の場合は、オーバーレイを表示できません。
- 回線/VC に、デバイス グループにまたがるエンドポイントが含まれている場合があります。これは、あるエンドポイントはあるグループに属しており、別のエンドポイントは別のグループに属していることを意味します。この場合は、フル オーバーレイを表示できません。エンドポイントがマップ内に表示されていない場合は、通知リンクがマップの左上に表示されます。選択した回線/VCのエンドポイントを含むすべてのデバイス グループを表示するには、マップを展開するためのリンクをクリックします。
- オーバーレイが表示されると、リンク タイプ フィルタが無効になります。

ネットワーク トポロジ上に回線/VCのオーバーレイを表示するには、次の手順を実行します。

ステップ 1 左側のサイドバーで、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

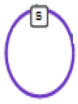
ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックして、必要なグループを選択します。

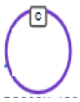
ステップ 3 [回線/VC（Circuits/VCs）] タブに移動して、選択したグループに関連付けられた回路/VC のリストを表示します。

ステップ 4 マップ上に表示する回線/VC を選択します。

選択した回線に参加しているノードとリンクがオーバーレイ内で強調表示され、マップ内の残りのデバイスが無効として表示されます。選択した回線の名前がトポロジ ツールバーのすぐ下に表示されます。オーバーレイをクリアするには、回線名の右側にある [X] ボタンをクリックします。オーバーレイ アイコンの説明については、回線または VC ネットワーク トポロジ オーバーレイのアイコンを参照してください。

回線または VC ネットワーク トポロジ オーバーレイのアイコン

オーバーレイ アイコン	定義
	送信元エンドポイント
	宛先エンドポイント
	ローカル スイッチングを使用した EVC または CEM
	回線の作成中にユーザーによって追加されたエンドポイント。 （注） セグメント ルーティング テクノロジー タイプの隣接およびノード SID の両方に「S」が表示されます。
	回線の作成中にユーザーによって除外されたエンドポイント。
	回線の作成中に追加または除外されたポートの一部を持つエンドポイント。このエンドポイントには、回線のさまざまなルートに参加している複数のポートが含まれています。
	ルートとして指定された E-TREE EVC エンドポイント。
	アイコンの S は、サーバーがデバイス上で設定されていることを示します。

オーバーレイ アイコン	定義
	アイコンの C は、クライアントがデバイス上で設定されていることを示します。
	アイコンの S と C は、サーバーとクライアントの両方が同じデバイス上で設定されていることを表します。
	選択されたエンドポイント。
	ハブ：ハブとルートが同じデバイスにある場合（VPLS シナリオ）、ルート アイコンが茶色の丸で囲まれます。
	回線の作成中に追加されたリンク。
	回線の作成中に除外されたリンク。
	回線の作成中に追加または除外されたポートの一部を持つエンドポイント。これは、同じ回線のさまざまなルートに参加している複数のポートを含む集約リンクを表します。

回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー

[回線/VC 360（Circuit/VC 360）] ビューでは、特定の回線/VC に関する情報を一目で確認できます。[回線/VC 360（Circuit/VC 360）] ビューから、回線/VC に関する詳細情報にアクセスし、回線/VC の 360 度ビューから実行できる操作 （807 ページ）で説明されているアクションを実行できます。

[回線/VC 360（Circuit/VC 360）] ビューの上部には、回線名、状態、および回線/VC とパフォーマンスに関する一般情報が表示されます。より詳細な情報は、ビューの下部にあるタブに表示されます。

[回線/VC 360（Circuit/VC 360）] ビューに示される情報	説明

一般情報	回線/VC のタイプ、そのさまざまな状態（ディスカバリ、有用性、プロビジョニング）、回線/VC に関連付けられている顧客、および監査情報（いつ作成されたか、最後に変更されたのはいつか）。回線/VC の状態の説明については、回線または VC の状態 （790 ページ）を参照してください。 （注） プロビジョニングの状態が [作成失敗（Create Failed）] の場合は、関連する [i]（[情報（information）]）アイコンをクリックすると失敗の理由を確認できます。 [自動更新（Auto-Refresh）]：デバイスのステータスとトラブルシューティングをリアルタイムで更新する場合は、[更新（Refresh）] アイコンをクリックしてオンデマンド更新を有効にします。または、ドロップダウンリストから、自動更新の間隔を 30 秒、1 分、2 分、または 5 分に設定することもできます。デフォルトでは、自動更新はオフになっています。 （注） 自動更新設定は、現在開いている [360° ビュー（360° View）] ポップアップウィンドウにのみ適用されます。このビューを閉じてからもう一度開いた場合または別のビューを開いた場合は、デフォルトでは自動更新がオフになります。 TE トンネルの予約済み帯域幅の利用率が表示されます。利用率の表示はトンネルに設定された帯域幅に基づき、トンネルに関連付けられた Psudowire の設定帯域幅と比較されます。
パフォーマンスデータ	回線/VC のパフォーマンスに関するさまざまな要素を示すグラフ。 （注） データをグラフで表示するためには、該当するデバイスで必要なモニターリング ポリシーが有効化されている必要があります。たとえば、生成および受信された明示的なポインタ調整リレーカウンタ（L ビットや P ビットなど）の数を図示したグラフを表示するには、CEM と擬似回線エミュレーションのエッジからエッジへのモニターリング ポリシーの両方を有効にする必要があります。モニターリング ポリシー リファレンス（1199 ページ）を参照してください。
アラーム	重大度、ステータス、生成時間を含む、回線/VC に関する現在のアラーム。
エンドポイント	この回線/VC のエンドポイントとして機能するデバイスおよびインターフェイス。
EVI	このタブには、EVI のエンドポイントが表示されます。[EVI の詳細（EVI Details）] タブには、選択したエンドポイントに設定されている EVI の詳細、ルートターゲット、およびルートポリシーが表示されます。

履歴（History）	[履歴（History）] タブには回線のすべてのバージョンがリストされ、回線/VC が検出された時点または最初に展開された時点以降に行われた変更を確認できます。リストされている任意のバージョンの [回線 360（Circuit 360）] ビューを開いて、そのエンドポイントやアラームなどを確認できます。 （注） 過去の回線/VC の [回線 360（Circuit 360）] ビューを表示している場合は、[履歴（History）] タブが表示されません。 また、次の手順を実行して、回線/VC のエンドポイント設定の詳細情報を表示することもできます。 **1.** [プロビジョニングの状態（Provisioning State）] 列で、該当する回線/VC バージョンを見つけ、[i]（[情報（information）]）アイコンをクリックします。 [デバイス設定の詳細（Device Configuration Details）] ポップアップ ウィンドウが開きます。 **2.** 設定の詳細情報の表示対象となるエンドポイントのオプション ボタンをクリックします。 エンドポイントが正常にプロビジョニングされている場合は、ポップアップ ウィンドウの下部に設定がリストされます。エンドポイントのプロビジョニングが失敗した場合は、代わりにプロビジョニングの失敗理由の説明が示されます。
関連する回線/VC（Related Circuits/VCs）	選択した回線内の追加の回線。

EVC について、次の情報が表示されます。

- [着信トラフィック（Incoming Traffic）]：一定期間に回線/VC のすべてのエンドポイント インターフェイスに入った着信トラフィックの合計（ビット/秒（bps）単位）。グラフには、すべてのエンドポイントの合計着信トラフィックの最後の 24 個の標本が 1 分間隔で表示されます。ピンク色のバーは最低レベルの着信トラフィックを示し、青色のバーは最高レベルの着信トラフィックを示します。
- [ポート可用性（Port Availability）]：回線/VC のすべてのエンドポイントの平均可用性。すべてのエンドポイントで集計され、パーセントで表されます。使用不可のインターフェイスがない限り、基準は 100% です。
- [発信トラフィック（Outgoing Traffic）]：一定期間に回線/VC のすべてのエンドポイント インターフェイスから発信されたトラフィックの合計（ビット/秒（bps）単位）。
- [損失（Loss）]：回線/VC のすべてのエンドポイントの平均損失（パーセント単位）。
- [遅延（Delay）]：回線/VC のすべてのエンドポイントの平均遅延（マイクロ秒単位）。
- [ジッター（Jitter）]：回線/VC のすべてのエンドポイントの平均ジッター（ミリ秒単位）。

光回線の場合、次の回線タイプに基づいてパフォーマンス データが表示されます。

- OCHCC WSON：フレーム、上位層プロトコルにパケットを配信できない原因となったエラーを含む着信パケットの数、および回線あたりの重大エラー秒数と多重化セクション数を含む、インターフェイスで受信されたオクテットの合計数。
- OCHNC WSON：この回線タイプの平均、最小、および最大の光信号対雑音比（OSNR）と電気信号対雑音比（eSNR）。
- OCH-TRAIL WSON：この回線タイプでの修正不可能な単語の合計数および修正されたエラーの合計数（ビット/秒（bps）単位）。
- OCH-Trail UNI：修正不可能な単語の合計数および修正されたエラーの合計数（ビット/秒（bps）単位）、およびこの回線タイプによって送受信された最小、平均、最大の送出電力（1 ワットを基準としたデシベル（dBW）単位）。
- ODU UNI：バックグラウンド ブロック エラーの合計数、重大エラー秒数の合計、およびパス モニターリングのエラー秒数比率。
- ODU トンネル：バックグラウンド ブロック エラーの合計数、重大エラー秒数の合計、およびセクション モニターリングのエラー秒数比率。

さらに、すべての光回線タイプについて、回線から送受信された送出電力の平均量、最小量、最大量が表示されます。

回線エミュレーション サービスについては、次の情報が表示されます。

- 各回線エンドポイントのジッタ バッファ オーバーランの合計数。
- 各回線エンドポイントで生成および受信された明示的ポインタ調整リレー カウンタ（L ビットや R ビットなど）の合計数。

Cisco ME 1200 デバイス上のサービスでは、着信トラフィックと発信トラフィック、ジッタ、および可用性などの情報が表示されます。

MPLS 双方向 TE トンネルの場合は、パフォーマンス データを表示するために、インターフェイス ヘルス モニターリング ポリシーを必ず有効にしてください。詳細については、モニターリング ポリシー リファレンス（1199 ページ）を参照してください。次のパフォーマンス データが表示されます。

- [トラフィック（Traffic）]：トンネルの両方向の合計トラフィック（ビット/秒（bps）単位）。
- [可用性（Availability）]：トンネルのエンドポイントの平均可用性。
- [帯域幅使用率（Bandwidth Utilization）]：トンネルに関連付けられているすべての疑似回線で設定された帯域幅の合計パーセンテージに対する、そのトンネルで設定された帯域幅のパーセンテージ。
- [実際の帯域幅使用率（Actual Bandwidth Utilization）]：トンネルに関連付けられているすべての疑似回線における着信/発信トラフィックで利用された帯域幅の合計パーセンテージに対する、そのトンネルで設定された帯域幅のパーセンテージ。

Y.1731 プローブが有効になっているキャリア イーサネット サービスの場合は、Y.1731 プローブのより詳しい説明を [Y.1731] タブに表示します。

（注） [エンドポイント（Endpoints）] タブで、関連するエンドポイントを選択した後、[i] アイコンをクリックしてより詳しい説明を表示します。

特定の回線または VC の [回線/VC 360（Circuit/VC 360）] ビューを開くには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。[ネットワーク トポロジ（Network Topology）] ウィンドウとその機能については、ネットワーク トポロジの視覚化（219 ページ）を参照してください。

ステップ 2 **[ネットワーク トポロジ（Network Topology）]** ページのツールバーから、**[デバイス グループ（Device Groups）]** をクリックします。

[デバイス グループ（Device Groups）] ダイアログボックスが開きます。

ステップ 3 回線または VC が関連付けられているデバイス グループを見つけてクリックし、ダイアログボックスを閉じます。

ステップ 4 [回線/VC（Circuits/VCs）] タブをクリックします。

ステップ 5 リストで回線または VC を見つけ、その [i]（[情報（information）]）アイコンをクリックします。

回線/VC の 360 度ビューから実行できる操作

次に、選択した回線または VC の [表示（View）] メニューおよび [アクション（Actions）] メニューから実行できるアクションの一覧を示します。実行可能なアクションは、選択した回線または VC の種類によって異なります。

- **View > Details** を選択し、回線/VC に関するさらに詳しい説明を表示します。回線/VC に関する総合情報の取得：[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウ（810 ページ）を参照してください。

（注） **View > Details** は、IOT サービス（RS232、RS422、RS485、raw ソケット、C37.94、EM-Voice、および X.21 サービスの詳細）ではサポートされていません。

- **View > Service Trace** を選択し、光回線のルートをトレースします。回線のすべてのルートのトレースと視覚化（248 ページ）を参照してください。

- **View > Dashboard** を選択し、回線/VC のサービス パフォーマンス ダッシュボードを表示します。ダッシュボードのセットアップと使用 （7 ページ）を参照してください。
- **View > Performance** を選択し、CEM サービスの回線の詳細と CEM の統計情報を表示します。
- **Actions > Add to Compare** を選択し、サービサビリティおよびプロビジョニングの状態や発生したアラームのような情報に基づいて、別の回線または VC と対照比較する回線または VC を選択します。「回線/VC 情報とステータスの比較」を参照してください。
- **Actions > Multilayer Trace** を選択し、回線をグラフィカルに視覚化します。「回線/VC の完全なルートをトレースおよび可視化する」を参照してください。
- **Actions > Y.1564 Test** を選択し、CE 回線/VC のエンドツーエンドのパフォーマンスをテストします。Y.1564 パフォーマンス テストの実行 （850 ページ）を参照してください。
- **Actions > Y.1731 Test** を選択し、CE 回線/VC のエンドツーエンドのパフォーマンスをテストします。EVC の Y1731 に基づくパフォーマンス テスト （852 ページ）を参照してください。
- **Actions > BERT** を選択し、回線エミュレーション サービスのパフォーマンスをテストします。回線エミュレーション サービスのパフォーマンステスト （856 ページ）を参照してください。
- **Actions > Optical PM Parameters** を選択し、光回線/VC のリアルタイムのパフォーマンス モニターリング データを表示します。オプティカル パフォーマンス モニターリング パラメータ （853 ページ）を参照してください。
- **Actions > PRBS Test** を選択し、光回線/VC のエンドツーエンドのパフォーマンスをテストします。回線（ODU UNI）での PRBS テストの実行 （854 ページ）を参照してください。
- **Actions > Restoration Actions >Upgrade Restore** を選択し、障害が発生した光回線をアクティブなルートにアップグレードし、障害が発生した古いルートを削除します。回線の復元（光） （823 ページ）を参照してください。
- **Actions > Restoration Actions >Manual Revert** を選択して、ルートが障害から回復したときに、光回線を元のルートに復帰させます。回線の復元（光） （824 ページ）を参照してください。
- **Actions** > **Maintenance Actions** > **Repair** を選択して、障害が発生したパスと同じパスで障害が発生した光回線を修復します。回線の修復（光） （825 ページ）を参照してください。
- **[操作（Actions）]>[アクションの再ルーティング（Reroute Actions）]>[現用パス（Working Path）]** または [保護パス（Protected Path）] を選択し、回線用に定義されている現用パスまたは保護パスを通過するトラフィックを再ルーティングします。回線の再ルーティング（光回線） （824 ページ）を参照してください。
- **Actions > Activate** を選択し、トラフィックが光回線を通過するようにします。回線をアクティブにする（光） （822 ページ）を参照してください。

- **Actions > Deactivate** を選択し、トラフィックが光回線を通過するのを停止します。回線をアクティブにする（光）（822 ページ）を参照してください。
- **Actions > Pseodowire OAM** 、**LSP OAM**、**CFM OAM**、または **SR TE OAM** オプションを選択し、OAM コマンドを使用してサービス障害をトラブルシューティングします。OAM コマンドを使用してサービス障害をトラブルシュートする（843 ページ）を参照してください。
- **[アクション（Actions）]>[トポロジに表示（Show in Topology）]** を選択し、トポロジマップに回線/VC オーバーレイを表示します。
- [サービスアビリティ（Serviceability）] ステータスの横にある *i* アイコンをクリックし、回線の障害に関する追加情報を表示します。回線/VC 障害に関する詳細情報の取得（841 ページ）を参照してください。
- **[アクション（Actions）]>[再同期（Resync）]>** を選択し、特定のサービスに関するサービス検出の再同期を実行します。詳細については、「サービス検出の再同期」を参照してください。

回線/VC 情報とステータスの比較

[比較ビュー（Comparison View）] では、複数の回線または VC の対照比較を実行し、検出およびプロビジョニングの状態、発生したアラーム、関連するエンドポイントなどの情報を表示できます。回線または VC を比較するには、次の手順を実行します。

ステップ 1 比較する回線または VC ごとに、次の手順を実行します。

a) 「回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー」に記載されているように、[回線/VC 360（Circuit/VC 360）] ビューを開きます。

b) **[アクション（Actions）] > [追加して比較（Add to Compare）]** を選択します。

選択した回線または VC がページの下部に表示されます。最大 4 つの回線または VC を選択できます。

ステップ 2 [比較（Compare）] をクリックします。

比較ビューが開きます。

ステップ 3 ビューの上部にあるドロップダウン リストで、利用可能なすべての情報をビューに表示するか、デバイスごとに一意の情報だけを表示するかを指定します。

ステップ 4 [比較ビュー（Comparison View）] をクリックして、ビューに表示するカテゴリのチェックボックスをオンにしてから、[保存（Save）] をクリックします。

デフォルトで、すべてのカテゴリがすでに選択されています。

ステップ 5 選択したカテゴリごとに提供される情報が表示されるようにページをスクロール ダウンします。

次の点に注意してください。

- [比較ビュー（Comparison View）] には、一度に 2 つの回線または VC に関する情報しか表示されません。3 つ以上を選択した場合は、現在表示されていない回線または VC に切り替える必要があります。

- 選択した回線または VC の順序を変更するには、[再整理（Rearrange）] をクリックします。
- 各回線または VC の [表示（View）] メニューと [アクション（Actions）] メニューは、[回線/VC 360（Circuit/VC 360）] ビューで提供されるものと同じです。オプションを選択すると、対応するページが開きます。
- 必要に応じて、表示されるカテゴリを最小化または最大化できます。
- [比較ビュー（Comparison View）] は、デバイス、インターフェイス、およびリンクでも利用できます。それぞれの 360 ビューからこれらの要素のいずれかを比較用に選択すると、対応するタブにその要素が表示されます。これにより、必要に応じて要素のタイプを切り替えることができます。
- 回線または VC の比較を終了する場合は、ビューの上部にある [戻る（Back）] をクリックしてから、ページの下部にある [すべての項目をクリア（Clear All Items）] をクリックします。他の要素タイプのタブが表示されている場合は、それらのタブもクリアする必要があります。

回線/VC に関する総合情報の取得：[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウ

[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウには、特定の回線/VC に関する追加の詳細情報（回線/VCに対して定義されている属性を含む）が表示されます。表示されたページに示される情報は、回線/VCのタイプに応じて異なります。また、[回線/VC詳細情報（Circuit/VC Details）] ウィンドウでは特定のアクション（回線/VCの変更または削除、新しい回線/VCの作成、パフォーマンス テストの実行など）を実行することもできます。

[回線/VC詳細情報（Circuit/VC Details）] ウィンドウを表示するには、いずれかの回線/VCテーブルで回線/VC 名のハイパーリンクをクリックします。あるいは、次のように [回線/VC 360（Circuit/VC 360）] ビューから [回線/VC 詳細情報（Circuit/VC Details）] ウィンドウを表示することもできます。

ステップ 1 必要な回線/VC の [回線/VC 360（Circuit/VC 360）] ビューを表示します。回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ）を参照してください。

ステップ 2 **View > Details** を選択します。[回線/VC 詳細情報（Circuit/VC Details）] ページの属性の説明については、キャリア イーサネット ネットワークの EVC のプロビジョニング （639 ページ）および光/DWDM ネットワークの回線のプロビジョニング （665 ページ）を参照してください。

詳細は、次の 2 つのタブに表示されます。

- [要約（Summary）]：回線検出およびプロビジョニング状態、承認しきい値、WSON ラベル、回線タイプ、回線に関連付けられている波長、保護ステータスなどの回線情報を表示します。
- [ポート（Ports）]：回線に関連付けられたポート、ポートの役割、ポートに関連付けられた IP アドレスなどのポート情報を表示します。

[回線/VCの詳細（Circuit/VC Details）] ページから実行できるアクション

[回線/VC の詳細（Circuit/VC Details）] ウィンドウでは、次のアクションを実行できます。

- 回線/VC の変更（Cisco EPN Manager を使用してプロビジョニングされた回線/VC に対して使用可能なアクション）。回線/VC の変更 （821 ページ）を参照してください。
- 回線/VC の削除（検出された回線/VCではなく、Cisco EPN Manager を使用してプロビジョニングされた回線/VC に対して使用可能なアクション）。回線/VC の削除 （830 ページ）を参照してください。
- 新しい回線/VCの作成。[作成（Create）] ボタンをクリックすると、プロビジョニング ウィザードが開き、新しい回線/VC を作成できます。キャリア イーサネット ネットワークの EVC のプロビジョニング （639 ページ）および光/DWDM ネットワークの回線のプロビジョニング （665 ページ）を参照してください。
- **Actions > Y.1564 Test** を選択し、CE 回線/VC のエンドツーエンドのパフォーマンスをテストします。Y.1564 パフォーマンス テストの実行 （850 ページ）を参照してください。
- **Actions > BERT** を選択し、回線エミュレーション サービスのパフォーマンスをテストします。回線エミュレーション サービスのパフォーマンス テスト （856 ページ）を参照してください。
- **Actions > Optical PM Parameters** を選択し、光回線/VC のリアルタイムのパフォーマンス モニターリング データを表示します。オプティカル パフォーマンス モニターリング パラメータ （853 ページ）を参照してください。
- **Actions > PRBS Test** を選択し、光回線/VC のエンドツーエンドのパフォーマンスをテストします。回線（ODU UNI）での PRBS テストの実行 （854 ページ）を参照してください。
- **Actions > Restoration Actions >Upgrade Restore** を選択し、障害が発生した光回線をアクティブなルートにアップグレードし、障害が発生した古いルートを削除します。回線の復元（光） （823 ページ）を参照してください。
- **Actions > Restoration Actions >Manual Revert** を選択して、ルートが障害から回復したときに、光回線を元のルートに復帰させます。回線の復元（光） （824 ページ）を参照してください。
- **Actions** > **Maintenance Actions** > **Repair** を選択して、障害が発生したパスと同じパスで障害が発生した光回線を修復します。回線の修復（光） （825 ページ）を参照してください。
- **Actions > Activate** を選択し、トラフィックが光回線を通過するようにします。回線をアクティブにする（光） （822 ページ）を参照してください。
- **Actions > Deactivate** を選択し、トラフィックが光回線を通過するのを停止します。回線をアクティブにする（光） （822 ページ）を参照してください。
- **Actions > Resync** を選択し、回線を再同期します。回線/VC の再同期 （829 ページ） を参照してください。

回線のバージョンの表示と比較（光）

[回線履歴（Circuit History）]ページを使用して、光回線の2つのバージョンを比較します。[回線履歴（Circuit History）] ページから、次のアクションを実行できます。

- 光回線で発生したイベントの簡単な視覚化と統合ビューを取得します。
- イベントに関連付けられているアラームを表示します。
- 光回線で発生した障害に関する情報を表示します。
- 回線内のルート変更を比較します。

たとえば、光回線で復元が発生したことがあるとします。[回線履歴（Circuit History）]ページを使用すると、次のアクションを実行できます。

1. 回線で発生した変更のリストを表示します。
2. 保護切り替えアクションまたは回線で発生した再ルーティングがある場合、[タイプ（Type）] 列の[i]アイコンをクリックすると、保護切り替えアクションを引き起こしたイベントの詳細、または再ルーティング アクションにより発生した障害の理由を表示できます。
3. [タイム スタンプ（Time Stamp）] 列の [i] アイコンをクリックし、イベントに関連付けられているアラームを表示します。
4. アクティブ パスと保護切り替え時のパスとの間のルート変更をさらに詳細に比較できます。
5. また、アクティブパスと元のパスの間、または元のパスと保護切り替え時のパス間のルートを比較し、参加しているノードの相違を表示し、影響を受けるノードのアクションを取得できます。

光回線の履歴を表示するには、次の手順を実行します。

ステップ 1 左側のサイドバーから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックし、必要な回線/VC が作成された場所を選択します。

（注） デフォルトでは、[すべての場所（All Locations）] グループが選択されます。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで[回線/VC（Circuits/VCs）] をクリックします。

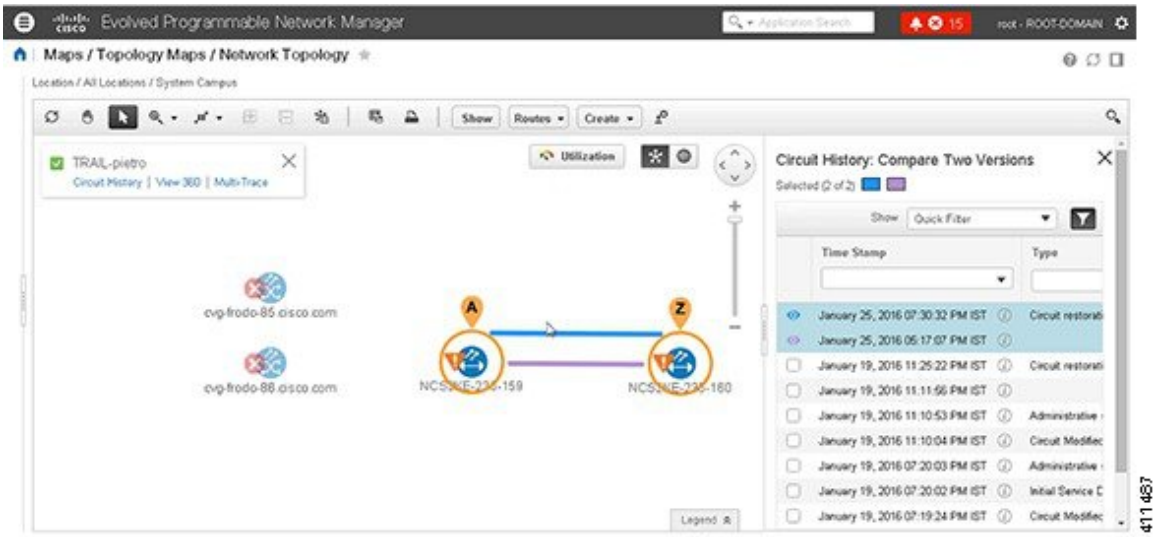
ステップ 5 履歴を表示する光回線を選択します。回線のオーバーレイがマップ上に表示されます。

ステップ 6 トポロジ ツールバーのすぐ下に表示される [回線履歴（Circuit History）] ハイパーリンクをクリックします。

[回線履歴（Circuit History）] 領域は、トポロジ マップの横に表示され、回線のさまざまなバージョンのリストが表示されます。デフォルトでは回線のアクティブ ルートが選択され、マップ上に表示されます。

ステップ 7 [回線履歴（Circuit History）] 領域に表示されるリストから履歴バージョンを選択し、現在のバージョンと比較します。

マップ上のオーバーレイは、選択内容に基づいて変更され、アクティブ ルートと履歴バージョンの両方が表示されます。一度に選択および比較できるバージョンは 2 つのみです。



特定のデバイスの回線/VC の表示

特定のデバイスが参加するすべての回線/VC のリストを表示するには、[デバイス 360（Device 360）] ビューを使用します。これは、特定のデバイスに問題があり、影響を受けるサービスを確認したい場合に便利です。

デバイスが参加する回線/VC のリストを表示するには、以下を行います。

ステップ 1 ネットワーク トポロジで必要なデバイスをクリックします（**[マップ（Map）]**>**[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]**）。

ステップ 2 ポップアップ ウィンドウで **View 360** をクリックします。

ステップ 3 [デバイス 360（Device 360）] ビューの [回線/VC（Circuit/VC）] タブに移動して、そのデバイスに関連する回線をリストしている表を表示します。その表には、回線/VC 名、回線/VC タイプ、作成および変更された時刻、回線/VC の現在のステータスがリストされます。

デバイス グループの回線/VC を表示する

- トポロジ ウィンドウのデバイス グループの回線/VC リストの表示 （814 ページ）
- 拡張テーブルにデバイス グループの回線/VC を表示する （814 ページ）

トポロジ ウィンドウのデバイス グループの回線/VC リストの表示

Cisco EPN Managerは、ネットワーク トポロジ ウィンドウの左側にある [回線/VC（Circuits/VCs）] タブで、検出およびプロビジョニングされた回線/VC を表示します。回線/VC のリストは、選択したデバイス グループに基づいてフィルタ処理されます。回線/VC 名をクリックして [回線/VC の詳細（Circuit/VC Details）] ウィンドウを起動するか、情報アイコンをクリックして [回線/VC 360（Circuit/VC 360）] ビューを起動して、回線/VC の詳細を表示できます。

[回線/VC（Circuits/Vcs）] タブには、検出された回線/VC、および Cisco EPN Manager を使用してプロビジョニングされた回線/VC の最新バージョンが一覧表示されます。回線/VC は、プライマリ状態（デフォルト）でソートされます。

[ネットワーク トポロジ（network topology）] ウィンドウの回線/VC のリストを表示するには、以下を行います。

ステップ 1 左側のナビゲーション ウィンドウで、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。[ネットワーク トポロジ（network topology）] ウィンドウが開きます。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックし、トポロジ マップに表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブに移動して、選択したデバイス グループに関連する回線/VC のリストを表示します。

ステップ 4 回線/VC を選択して回線/VC のオーバーレイをネットワーク トポロジで表示します。つまり、回線/VC のエンドポイントとパスが物理トポロジの上に表示されます。回線名のハイパーリンクをクリックして回線の詳細を表示するか、回線/VC 名の横にある情報アイコンをクリックして [回線/VC 360（Circuit/VC 360）] ビューを開きます。

ステップ 5 別のウィンドウで回線/VC の表のビューを開くには、回線/VC のリストの下の [回線/VC（Circuit/VCs）] をクリックします。

拡張テーブルにデバイス グループの回線/VC を表示する

ネットワーク トポロジ ウィンドウから、選択したデバイス グループに関連付けられた回線/VC のテーブルを別のブラウザ ウィンドウで開くことができます。このテーブルには、各回線/VC に関する詳細情報が表示され、並べ替えや検索が可能なため、情報を簡単に見つけることができます。このテーブルは、特に、回線/VC のプロビジョニング ステータスや Cisco EPN Manager 内でのそれらの管理ステータスの識別に便利です。回線/VC状態とそれらのアイコンの説明については、回線または VC の状態 （790 ページ）を参照してください。

デフォルトで、回線/VC テーブルでは、回線/VC がプライマリ状態の順にソートされます。必要に応じて、テーブルのソート順を変更できます。

展開した回線/VC テーブルは [ネットワーク トポロジ（Network Topology）] ウィンドウと連動するため、テーブルで回線/VC を選択すると、回線/VC が [ネットワーク トポロジ（Network Topology）] ウィンドウ内にトポロジ マップのコンテキストで図示されます。

展開されたより詳細な回線の一覧を別のウィンドウに表形式で表示するには、次の手順を実行します。

ステップ 1 左側のナビゲーション ウィンドウで、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。[ネットワーク トポロジ（network topology）] ウィンドウが開きます。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックし、トポロジ マップに表示するデバイスのグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブに移動して、選択したデバイス グループに関連する回線/VC のリストを表示します。

ステップ 4 回線/VC のリストの下にある [回線/VC（Circuit/VCs）] ハイパーリンクをクリックし、選択したデバイス グループに関連する回線/VC のリストを含む別のウィンドウを開きます。

- 回線/VC 360 ビューを表示することにより、回線/VC の詳細を確認します。回線/VC の表示 （137 ページ）を参照してください。
- マップ上の回線/VCを、表示されたデバイス上のオーバーレイとして表示します。トポロジ マップ内の特定の回線/VC を表示する （800 ページ）を参照してください。
- プロビジョニング ウィザードを起動して、回線/VCをプロビジョニングします。新規キャリア イーサネット EVC の作成およびプロビジョニング （641 ページ）および光/DWDM ネットワークの回線のプロビジョニング （665 ページ）を参照してください。
- 回線障害の詳細を確認します。回線/VC 障害に関する詳細情報の取得 （841 ページ）を参照してください。
- 変更、削除、回線トレース、およびパフォーマンス テスト用の回線/VCを選択します。詳細については、次のトピックを参照してください。
  - 回線/VC の変更 （821 ページ）
  - 回線/VC の削除 （830 ページ）
  - 回線/VC のパフォーマンス テストの実行 （848 ページ）

Cisco EPN Manager ですべての回線/VC を表示

[回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）] ページには、Cisco EPN Manager が現在管理しているすべての回線と VC がリストされています。ここから、名前、タイプ、または顧客などの基本的な基準を使用してリストをフィルタ処理することによって、特定の回線または VC をすばやく見つけることができます。Cisco EPN Manager がプロビジョニングした EFP の数を表示できます。すべての EFP がプロビジョニングされている場合、EFP の数はサービスの数と一致します。重大なアラームまたは特定の状態にあるすべての回線および VC を確認できます（回線と VC の状態（プライマリ状態を含む）については、回線または VC の状態 （790 ページ）を参照してください）。回線および VC の管理タスクを実行し、業績テストを実行することもできます。このページを使用するには、次の手順に従います。

（注） 回線または VC に参加しているデバイスが Cisco EPN Manager から削除された後も、対応する回線または VC は引き続き [回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）] ページに表示されます。

ステップ 1 **[インベントリ（Inventory）] > [その他（Other）] > [回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）]** を選択します。

ステップ 2 次のいずれかの操作を実行します。

- クイック フィルタ フィールド内のいずれかを使用して、特定の回線または VC を検索します。たとえば、[タイプ（Type）] フィールドに「L3VPN」と入力して、そのタイプのすべての回線と VC をリストするか、[サービサビリティ（Serviceability）] クイック フィルタ フィールドをクリックし、[ダウン（Down）] を選択して、現在停止しているすべての回線と VC を表示します。
- トポロジマップで特定の回線または VC を表示するには、そのラジオボタンをクリックし、**[アクション（Actions）] > [トポロジに表示（Show in Topology）]** を選択します。
- 回線または VC を選択した状態で、[アクション（Actions）] メニューを使用して回線または VC を有効化し、パフォーマンス テストを実行します。
- 回線および VC の作成、変更、削除、または強制削除を行うには、[回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）] ページのツールバーにある該当するボタンをクリックします。これにより、プロビジョニング ウィザードが開きます。

検出された回線/VC の特定と管理

Cisco EPN Manager は、既存のネットワーク回線/VC を検出し、回線/VC リストに表示します。検出された回線/VC には、システムによって自動的に名前が付けられます。EVC の名前は **EvcLink_** で始まります（EvcLink_Vpls_Bridge_318#318#VFIVPLS2_541549_10.56.23.48#1 など）。

（注） 回線/VC が検出されると、光回線、CE 回線、または L3VPN 回線/VC のいずれであるかが識別されますが、CE 回線/VC の正確なタイプを識別することはできません。たとえば、CE 回線/VC は [タイプ（Type）] 列に **EVC** が表示されますが、EPL や E-LAN などの EVC のタイプは表示されません。光学系の場合は、回線の正確なタイプが表示されます。

検出された回線/VC では、次の操作を実行できます。

- 検出された回線/VC を名前別に回線/VC リストで識別するか、または状態（**Discovered**）別に回線/VC のテーブルで識別します。
- 検出された回線/VC に関する詳細を、回線/VC のエンドポイントを含めて [回線/VC 360（Circuit/VC 360）] ビューに表示します。

- ネットワーク トポロジ上に回線/VC のオーバーレイを表示します。
- 回線/VC の障害情報を表示します。
- 検出された回線/VC を昇格させます。その後でその回線は編集または削除できます（光回線と選択した EVC に適用されます）。変更/削除前の検出された回線/VCの昇格（819ページ）を参照してください。
- パフォーマンス テストを実行します。

暗黙的な回線の表示/非表示

別の回線の基盤または「伝送」回線である場合、その回線は暗黙的回線と分類されます。たとえば、OCHTRAIL 回線は、OCHCC 回線の伝送回線（および暗黙的回線）である場合があります。デフォルトでは、すべての回線が回線リストに表示されます。ただし、必要に応じて、暗黙的回線をリストから非表示にすることができます。暗黙的回線が非表示の場合、それらの回線はリストには表示されませんが、[回線 360（Circuit/VC 360）] ビューの [伝送回線（Carrying Circuits）] タブに表示できます。

暗黙的回線を回線リストから非表示にするには、次の手順を実行します。

ステップ 1 左側のサイドバーから、[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] を選択します。

ステップ 2 [システム設定（System Settings）] メニューから、[回線/VC（Circuits/VCs）] > [回線/VC の表示（Circuits/VCs Display）] を選択します。

ステップ 3 [暗黙的回線/VC の表示（Show Implicit Circuits/VCs）] チェックボックスをオフにします。

ユーザー定義フィールドに基づいた回線/VC リストのフィルタ処理とエクスポート

ユーザー定義フィールドを作成し、そのフィールドに値を割り当て、それを回線/VC に関連付けることができます。その後に、ユーザー定義フィールドに基づいて回線/VC リストの並べ替え、フィルタ処理、エクスポートがきます。

たとえば、サービスへの影響に基づいて回線/VC リストをフィルタ処理する場合は、次の操作を行う必要があります。

- 「サービスへの影響（Service Impact）」という名前のユーザー定義フィールドの作成
- ユーザー定義フィールドの [サービスへの影響（Service Impact）] を関連付ける回線/VC の選択
- [サービスへの影響（Service Impact] フィールドへの値（ [重大（Critical）]、[中（Moderate）]、または [低（Low）] ）の割り当て

- サービスへの影響の値に基づいた回線/VCリストの並べ替え、フィルタ処理、およびエクスポート

（注） 最大 10 個のユーザー定義フィールドを作成できます。

ステップ 1 ユーザー定義フィールドを作成するには、次のいずれかを実行します。

- **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[全般（General）]** > **[ユーザー定義フィールド（User Defined Fields）]** を選択した後、[+] アイコンをクリックして新しいラベルと説明を作成します。[保存（Save）] をクリックします。

  （注） [管理（Administration）] メニューからはユーザー定義フィールドに値を割り当てることはできません。

- **[インベントリ（Inventory）]** > **[その他（Other）]** > **[回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）]** を選択し、回線/VC を選択した後、**[アクション（Actions）]** > **[ユーザー定義フィールドの管理（Manage User Defined Fields）]** を選択します。[+] アイコンをクリックし、ユーザー定義フィールド、説明、および値を作成します。[保存（Save）] をクリックします。
- **[マップ（Map）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択し、[回線/VC（Circuits/VCs）] タブに移動して回線/VC のリストの下にある [回線/VC（Circuits/VCs）] ハイパーリンクをクリックします。回線/VC の拡張テーブルが別のウィンドウで開きます。回線/VC を選択し、**[アクション（Actions）]** > **[ユーザー定義フィールドの管理（Manage User Defined Fields）]** を選択します。[+] アイコンをクリックし、ユーザー定義フィールド、説明、および値を作成します。[保存（Save）] をクリックします。

ステップ 2 [回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）] ページまたは回線/VC の展開テーブルで、ページの右上にある [設定（Settings）] アイコンをクリックし、[列] を選択します。

ステップ 3 作成したユーザー定義フィールドを選択し、[閉じる（Close）] をクリックします。割り当てられた値を持つユーザー定義フィールドは、回線/VC のテーブル内の列として表示されます。

ステップ 4 テーブルの右上の [設定（Settings）] アイコンの横にある [エクスポート（Export）] アイコンをクリックすると、テーブルのデータがファイル（CSV 形式）にエクスポートされます。

ユーザー定義フィールドは、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[一般（General）]** > **[ユーザー定義フィールド（User Defined Fields）]** からのみ削除できます。

回線に関連付けられているルートの表示

ネットワークトポロジの [ルート（Routes）] ドロップダウンメニューを使用して、回線オーバーレイ内の回線に関連付けられている特定のルートを表示します。Cisco EPN Managerはサー

ビス内のリンクからルートを計算します。また、選択したルートに基づいてオーバーレイをフィルタ処理することもできます。

（注） この機能は、ポイントツーポイントCEサービス、光回線、およびCEMサービスでのみサポートされています。

ステップ1 左側のサイドバーから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ2 [デバイスグループ（Device Group）] リストから、必要なグループを選択します。Cisco EPN Managerは [回線/VC（Circuit/VCs）] タブの選択したグループに関連付けられている回線のリストを表示します。

ステップ3 [回線/VC（Circuit/VCs）] をクリックし、表示する回線を選択します。

ステップ4 [ルート（Routes）] ドロップダウン リストから、必要なルート タイプを選択します。

（注） ルート タイプは、選択した回線で設定されたルートに基づいています。

変更/削除前の検出された回線/VCの昇格

検出された回線は、変更または削除する前に昇格させる必要があります。昇格後、回線/VCのプロビジョニング状態は [正常に昇格（Promote Successful）] に変更されます。

（注） 昇格は、光回線、MPLS-TE、SR-TE、および追加設定のないLMI、QoS、G.8032、ICCP-SMなどの基本的なEVCでサポートされています。基盤のコアがVPLS（E-LANおよびE-Tree EVCs）の場合は昇格がサポートされます。検出された回線/VCを昇格できない場合は、変更または削除できません。また、回線エミュレーションのサービス、単方向サービス、双方向サービス、およびL3VPNサービスの昇格もサポートされています。

CFMドメイン名、CFMドメインレベル、メンテナンスなどのCFMパラメータを使用したCEサービスの昇格。関連付けられた[名前のタイプ（Name Type）]、[ITUキャリアコード（ITU Carrier Code）]、[ITU MEG IDコード（ITU MEG ID Code）]、[継続性チェック間隔（Continuity check interval）]、および[IPSLAプローブ（IPSLA probes）]がサポートされています。[メンテナンス（Maint）]で[ITU]が選択されている場合、ITUキャリアコードとITU MEG IDコードが表示されます。関連付けられた[名前のタイプ（Name Type）]ドロップダウンリスト。XRデバイスでのIPSLAプローブのカスタムプロファイル名のプロモーションはサポートされていません。サービスはカスタムプロファイル名を使用してプロモーションされますが、サービスの変更時にはリストされません。

ME1200デバイスを除き、IOS XEデバイスとIOS XRデバイスでのICCベースのCFM設定の昇格がサポートされています。ICCベースのCFMは、EVPN VPWSではサポートされていません。EVPNベースのE-LANサービスは、昇格ではサポートされていません。

検出された回線/VC を昇格させるには、次の手順を実行します。

始める前に

L3VPN サービスを正常に昇格させるには、L3VPN サービスのルート識別子が **rd device_ip:number** の形式で指定されていることを確認します。

次に例を示します。

```
vrf definition vdvvgfr420
 rd 10.104.120.133:420
  vpn id 36B:420
  !
address-family...
```

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）]**>**[トポロジ マップ（Topology Maps）]**>**[ネットワーク トポロジ（Network Topology）]** の順に選択します。[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックして、必要なグループを選択します。

ステップ 3 [回線/VC（Circuit/VCs）] タブに移動し、[回線/VC（Circuit/VCs）] リンクをクリックして、選択したグループ内の回線/VC の拡張テーブルを開きます。

ステップ 4 昇格させる検出された回線/VC を選択します。

デバイスから検出されたものの、昇格されていない L3VPN サービスを識別するには、プロビジョニング ステータスが [なし（None）] の L3VPN サービスをフィルタ処理で除外します。また、L3VPN サービスの [名前（Name）] フィールドを使用して、検出されたサービスを識別することもできます。検出された L3VPN サービスの [名前（Name）] フィールドは、サービス固有の VLAN ID で表されます。

デバイスから検出されたものの、昇格されていない MPLS TE サービスを識別するには、プロビジョニング ステータスが [なし（None）] の MPLS TE サービスをフィルタ処理で除外します。MPLS TE サービスの [名前（Name）] フィールドを使用して、検出されたサービスを識別することもできます。

ステップ 5 **Modify** をクリックします。プロビジョニング ウィザードが開きます。

ステップ 6 光回線の場合は、必要に応じて回線を変更し、**Create** をクリックします。

ステップ 7 EVC の場合は、次の手順を実行します。

a) [エンドポイントの詳細（Endpoint Details）] ページで、エンドポイントを選択します。選択したエンドポイントに関連するフィールドが下に表示されます。

b) ドロップダウン リストから UNI または ENNI を選択してエンドポイントのタイプを指定し、エンドポイントの名前を入力します。UNI の場合は、バンドル属性と多重化属性を設定することもできます。

c) 次のエンドポイントを選択し、そのタイプ、名前、および属性を定義します。

d) **Next** をクリックします。

e) [検出されたサービスの管理（Manage Discovered Service）] の [サービスの詳細（Service Details）] ページでサービスの [タイプ（Type）] を選択します。リスト内の使用可能なタイプは、定義したエンドポイントのタイプと UNI オプションから派生します。たとえば、[All to one Bundling] オプションで UNI を定義した場合、リストでは EPL、EP-LAN、および EP-Tree が使用できるようになります。ENNI を定義した場合は、アクセス EPL のみがリスト内で使用できるようになります。必要に応じて、前に戻ってエンドポイントを再定義できます。

f) サービスに名前を付けます。必要に応じて説明を入力し、顧客を指定します。
g) E-Tree EVC の場合は、[エンドポイントの指定（Endpoint Designation）] テーブルで各エンドポイントのロール（ルートまたはリーフ）を指定します。ここで指定するロールは、デバイスで設定されているロールと一致する必要があります。
h) **Save** をクリックします。EVC は [回線/VC（Circuit/VCs）] リストに新しい名前で表示され、そのステータスは [作成済み（Created）] および [展開済み（Deployed）] になります。
i) これで、リスト内の昇格された EVC を選択して変更または削除できるようになります。

ステップ 8 L3VPN サービスの場合は、次の手順を実行します。

a) サービスに名前を付けます。必要に応じて説明を入力して顧客を指定し、[次へ（Next）] をクリックします。
b) [展開アクション（Deployment Action）] ドロップダウン メニューで、VPN サービス昇格プロセスの完了時に取得する必要があるタスク（[プレビュー（Preview）] または [展開（Deploy）]）を指定し、[次へ（Next）] をクリックします。
c) UNI 名、MTU 値、およびサービス多重化を有効にするかどうかを指定します。
d) **Save** をクリックします。L3VPN サービスは [回線/VC（Circuit/VCs）] リストに新しい名前で表示され、そのステータスは [正常に昇格（Promote Successful）] になります。
e) これで、昇格した L3VPN サービスをリストから選択し、変更または削除できるようになります。

ステップ 9 MPLS TE トンネル サービスの場合は、次の手順を実行します。

a) 必要に応じて、サービスに名前を付けます。必要に応じて説明を入力して顧客を指定し、[次へ（Next）] をクリックします。
b) [保存（Save）] をクリックします。MPLS TE トンネル サービスは [回線/VC（Circuit/VCs）] リストに表示され、そのステータスは [正常に昇格（Promote Successful）] になります。
c) これで、昇格した MPLS TE トンネル サービスをリストから選択し、変更または削除できるようになります。

（注） アフィニティと優先度のデフォルト値は、トンネルの昇格後に変更フローで再設定されます。

動作中のパスのロックダウンで検出された MPLS TE トンネルは、変更および昇格時にロックダウンが消失します。

回線/VC の変更

プロビジョニング状態が定義済み、導入済み、失敗、または検出済みとなっている回線/VC には、変更を加えることができます。プロビジョニング状態の詳細については、回線または VC の状態 （790 ページ）を参照してください。

（注） UNI またはエンドポイントの選択は変更できません。ただし、UNI の名前は変更できます。別のデバイスをエンドポイントにする場合は、既存の回線/VC を削除してから新しい回線/VC を作成する必要があります。

E-LAN EVC および E-TREE EVC については、エンドポイント（サイト）を追加または削除できます。

回線/VC に変更を加えるには、次の手順に従います。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）]**>**[トポロジ マップ（Topology Maps）]**>**[ネットワーク トポロジ（Network Topology）]** の順に選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

ステップ 2 ツールバーで [デバイス グループ（Device Groups）] をクリックし、必要なグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブをクリックし、変更を加える回線または VC のオプション ボタンをクリックします。

ステップ 4 [回線/VC（Circuits/VCs）] ペインのツールバーで、鉛筆の形をした（[変更（Modify）]）アイコンをクリックします。

プロビジョニング ウィザードが開き、選択した回線または VC の情報が表示されます。

ステップ 5 必要に応じて回線または VC を編集してから、再び展開します。キャリア イーサネット ネットワークの EVC のプロビジョニング （639 ページ）および光/DWDM ネットワークの回線のプロビジョニング （665 ページ）を参照してください。

回線をアクティブにする（光）

光回線をアクティブにして、トラフィックが通過しているかどうかを判断することができます。ネットワーク内で検出され、展開された回線をアクティブにすることができます。また、回線の管理ステータスはダウンにする必要があります。

ステップ 1 左側のサイドバーから、**[マップ（Maps）]**>**[トポロジ マップ（Topology Maps）]**>**[ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックし、対象の回線/VC を作成したデバイス グループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、アクティブにする光回線を特定し、情報アイコンをクリックして、その [回線/VC 360（Circuit/VC 360）] ビューにアクセスします。

ステップ 4 **[アクション（Actions）]**>**[アクティブ化（Activate）]** を選択して、トラフィックが光回線を通過するようにします。

（注） また、[回線/VC の詳細（Circuit/VC Details）] ウィンドウやマルチレイヤ トレース ビューから光回線をアクティブにすることもできます。回線/VC の表示 （137 ページ）および回線/VC の完全なルートをトレースおよび可視化する （860 ページ）を参照してください。

ステップ 5 光回線を再展開します。

光回線を非アクティブにして、それを通過するトラフィックを停止することもできます。ネットワーク内で回線が検出され、展開されており、回線の管理状態がアップになっていることを確認します。**[アクション（Actions）]** > **[非アクティブ化（Deactivate）]** をクリックします。

回線の復元（光）

光回線で連続して複数の障害が発生し、障害が発生した回線が新しいルートで再ルーティングされる場合には、光回線を復元できます。

次の条件を満たす光回線を復元または復帰できます。

- 回線のプロビジョニング状態が [展開済み（Deployed）] または [検出済み（Discovered）] である。
- 回線の [復元（Restoration）] 属性が true に設定されている。
- 回線の復元モードが手動（manual）または自動（automatic）に設定されている。

光回線を復元するには、次の手順を実行します。

ステップ 1 左側のサイドバーから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックし、障害が発生した光回線が含まれているデバイス グループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、障害が発生した光回線を見つけ、情報アイコンをクリックして、その回線の [回線/VC 360（Circuit/VC 360）] ビューにアクセスします。

ステップ 4 **Actions > Restoration Actions > Upgrade Restore** を選択し、障害が発生した光回線をアクティブなルートにアップグレードし、障害が発生した古いルートを削除します。

（注） また、[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウとマルチレイヤ トレース ビューから、障害が発生した回線を復元することもできます。回線/VC の表示 （137 ページ）および回線/VC の完全なルートをトレースおよび可視化する （860 ページ）を参照してください。

アップグレード復元オプションは、復元できない回線に対しては無効になります。

復元が有効になっている場合、必要に応じて制約を追加できます。

OCH-Trail WSON 回線の NCS2K デバイスでは、回線が **[リバーティブ（Revertive）]** として設定されている場合にのみ、復元ステータスパラメータが **[復元（Restored）]** に設定されます。

元のルートが障害から回復したときに、光回線を元のルートに復帰させることもできます。**Actions > Restoration Actions > Manual Revert** をクリックします。

回線の復元（光）

ルートが障害から回復したときに、光回線を元のルートに復帰させることができます。この機能は、Cisco EPN Manager でプロビジョニングまたは検出されたすべての SVO 回線で使用できます。

光回線を復元するには、次の手順を実行します。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジマップ（Topology Maps）] > [ネットワークトポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックし、障害が発生した光回線が含まれているデバイス グループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、障害が発生した光回線を見つけ、情報アイコンをクリックして、その回線の [回線/VC 360（Circuit/VC 360）] ビューにアクセスします。

ステップ 4 **Actions > Restoration Actions > Manual Revert** を選択し、障害が発生した光回線をアクティブなルートにアップグレードし、障害が発生した古いルートを削除します。

動作中のパスまたは復元されたパスの NE-Disconnected アラームがクリアされない場合、回線は復元に失敗します。失敗の理由は、[履歴（History）] タブで確認できます。

OCH-Trail および OCH-NC 回線の NCS2k SVO デバイスでは、[復元（Restoration）] および [元に戻す（Revert）] のデフォルトの再試行回数は 12 であり、再試行間のデフォルトの期間は 5 分です。

復元および元に戻すのデフォルトの試行回数は、**/opt/CSCOlumos/conf/optical-mp.properties** ファイルを使用して変更できます。復元の試行回数を変更する場合はパラメーター **restorationRestoreAttempts** を使用し、元に戻す試行回数を変更する場合は **restorationRevertAttempts** を使用します。

回線の再ルーティング（光回線）

サービスを中断することなくネットワークのメンテナンス作業を行うために、回線を現用パスから保護パスに再ルーティングできます。再ルーティング操作は、Cisco EPN Manager でプロビジョニングまたは検出されたすべての WSON 回線に対して有効です。

（注） 復旧状態が「復旧済み」または「復元可能」となっている回線には、再ルーティング操作を実行することはできません。

再ルーティングを開始する前に、検出された回線を昇格させます。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックし、対象の回線/VC を作成したデバイス グループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、再ルーティングする光回線を見つけ、その情報アイコンをクリックして回線/VC の 360 度ビューにアクセスします。

ステップ 4 回線に定義された現用パスまたは保護パス経由でトラフィックを再ルーティングするには、**[アクション（Actions）] > [再ルーティング アクション（Reroute Actions）] > [現用パス（Working Path）]** または [保護パス（Protected Path）] の順に選択します。

（注） マルチレイヤ トレース ビューから光回線を再ルーティングすることもできます。回線/VC の完全なルートをトレースおよび可視化する （860 ページ） を参照してください。

回線の修復（光）

回線が復元されてもファイバの切断のために [部分（Partial）] 状態のままになっている場合は、回線パスを手動で修復して再同期できます。この機能は、Cisco EPN Manager でプロビジョニングまたは検出されたすべての SVO 回線で使用できます。

光回線を復元するには、次の手順を実行します。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジマップ（Topology Maps）] > [ネットワークトポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックし、障害が発生した光回線が含まれているデバイス グループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブで、障害が発生した光回線を見つけ、情報アイコンをクリックして、その回線の [回線/VC 360（Circuit/VC 360）] ビューにアクセスします。

ステップ 4 **Actions > Maintenance Actions > Repair** を選択して、障害が発生したパスと同じパスで障害が発生した光回線を修復します。

修復が行われるのには約10分かかります。回線が修復されない場合、失敗した理由の説明が[履歴（History）] タブに表示されます。

動作中のパスの **NE-Disconnected** イベントがクリアされた場合、[回線/VC 360°（Circuit/VC 360°）] ページで孤立した相互接続回線を手動で削除および修復する必要はありません。切断されたノードに関連付けられている孤立した相互接続回線はすべて自動的に削除されます。孤立した相互接続回線が削除された後、回線の [検出状態（Discovery State）] が [部分（Partial）] のままである場合、回線は自動的に修復され、手動で行う必要なく再同期されます。

回線/VC のプロビジョニングされたバージョンと検出されたバージョンの比較と調整

（注） この機能は、キャリアイーサネット VC、回線エミュレーション、およびシリアルサービスでのみサポートされています。

Cisco EPN Manager を使用して回線/VC をプロビジョニングすると、関連する CLI コマンドが回線/VC に参加しているデバイス上に設定されます。Cisco EPN Manager を使用して回線/VC がプロビジョニングされると、システムはネットワークからプロビジョニングされた回線/VC を検出します。場合によっては、プロビジョニング後にデバイスに設定変更が加えられた場合など、プロビジョニングされた CLI と検出された CLI に相違がある場合があります。Cisco EPN Manager では、回線/VC のプロビジョニングされたバージョンと検出されたバージョンを比較して、その相違が表示された調整レポートを生成できます。レポートに基づいて、検出されたバージョンを保持するか、プロビジョニングされたバージョンに戻すかを決定できます。検出されたバージョンを保持する場合、 Cisco EPN Manager の回線/VC は、このバージョンと同期されます。

比較および調整機能は、[回線/VC（Circuit/VCs）] テーブルからアクセスします。

回線/VC 検出状態が [欠落（Missing）] か、あるいはプロビジョニング状態が [なし（None）]、[進行中（In Progress）]、または [正常に削除（Delete Succeeded）] の場合は、機能が無効になります。

回線/VC を比較および調整するには、次の手順を実行します。

ステップ 1 システム内のすべての回線/VC の完全なテーブル（[インベントリ（Inventory）] > [その他（Other）] > [回線/VC およびネットワーク インターフェイス（Circuit/VCs and Network Interfaces）]）、または特定のデバイス グループの回線/VC のリスト（[マップ（Maps）] > [ネットワーク トポロジ（Network Topology）] > [回線/VC（Circuit/VCs）] タブ > [回線/VC（Circuit/VCs）] リンク）のいずれかの回線/VC のテーブルを開きます。

ステップ 2 [回線/VC（Circuit/VCs）] テーブルで、必要な回線/VC を見つけて選択します。

ステップ 3 [アクション（Actions）] > [調整レポート（Reconciliation Report）] を選択します。

比較レポートが表示され、回線/VC 内の特定のデバイスでプロビジョニングされた属性と検出された属性の相違が表示されます。プロビジョニングされた属性と検出された属性の間に相違がない場合は、レポートに「使用可能なデータがありません（No data available）」と表示されます。

（注） EVPN ベースのサービスの場合、RD、RT、およびコントロールワードなどの EVI パラメータはレポートから除外されます。

ステップ 4 レポートを確認したら、検出されたバージョンを回線/VC の現在のバージョンとしてデータベースに保存するか、またはプロビジョニングされたバージョンに戻すことができます。ページの上部で、[プロビジョ

ニング済み（Provisioned）]または[検出済み（Discovered）]オプションボタンを選択し、[調整（Reconcile）]をクリックします。

[プロビジョニング済み（Provisioned）]を選択した場合は回線/VCが再展開され、元のプロビジョニングされた回線/VCの属性値がデバイス上に設定されます。[検出済み（Provisioned）]を選択した場合、検出された回線/VCはデータベースに保存され、このバージョンは元がプロビジョニングされたバージョンに置き換わります。プロビジョニングステータスは、調整アクションが成功したかどうかを示します。

ステップ5 調整を完了するために入力が必要な場合は、プロビジョニングウィザードが起動されます。必要な情報を入力し、回線/VC 再展開します。

回線での保護切り替えアクションの開始（光）

光回線で保護切り替えアクションを開始して、トラフィックを1つのパスから別のパスに切り替えることができます。たとえば、光回線内のトラフィックが動作中のパスを流れ、動作中のパスが破損します。この回線で保護切り替えアクションを開始して、トラフィックを動作中のパスから保護パスに切り替えることができます。

（注） 保護切り替えアクションは、1+1または1+1+Rの保護タイプが有効になっている光回線でのみ開始できます。保護タイプの詳細については、OTN 回線タイプの回線セクション参照 （691ページ）を参照してください。

保護切り替えアクションを開始するには、次の手順を実行します。

ステップ1 左側のサイドバーから、**[マップ（Maps）]**>**[トポロジ マップ（Topology Maps）]**>**[ネットワーク トポロジ（Network Topology）]**を選択します。

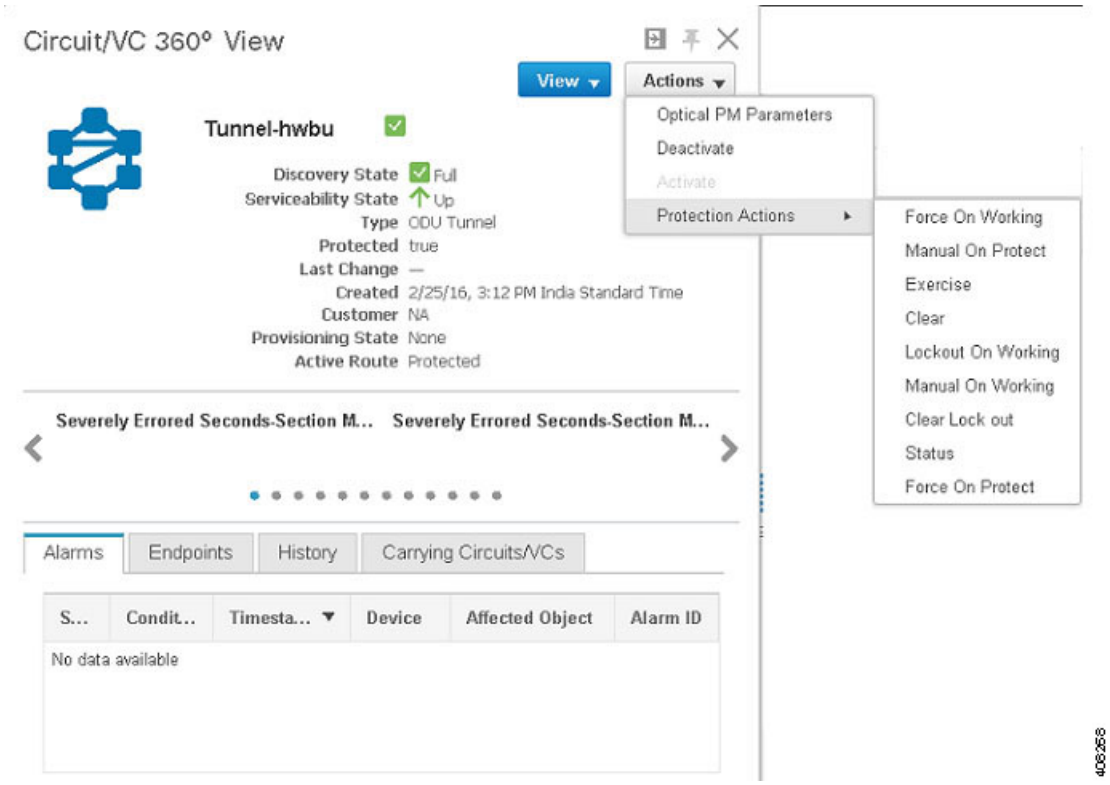
ステップ2 [デバイス グループ（Device Groups）]をクリックし、必要な回線/VCが作成された場所を選択します。

ステップ3 [デバイス グループ（Device Groups）]ポップアップ ウィンドウを閉じます。

ステップ4 [ネットワーク トポロジ（Network Topology）]ウィンドウで[回線/VC（Circuits/VCs）]をクリックします。

ステップ5 [回線/VC（Circuits/VCs）]タブで、必要な回線/VCを見つけて、その回線/VC名の横にある[i]アイコンをクリックします。[回線/VC 360（Circuit/VC 360）]ビューが別のポップアップ ウィンドウに表示されます。

ステップ6 **[アクション（Actions）]**>**[保護アクション（Protection Actions）]**を選択し、必要な保護切り替えアクションを選択します。



次の表に、各保護切り替えアクションの詳細な説明を示します。

保護切り替えアクション	説明	次の場合に適用されます。
動作時に強制（Force On Working）	ネットワークを介してトラフィックを伝送する動作中のパスを設定します。	保護切り替えアクションの現在の状態は、[手動時に保護（Manual On Protect）] または [動作時に手動（Manual On Working）] です。
保護時に手動（Manual On Protect）	トラフィックを動作中のパスから保護されたパスに手動で切り替えます。	回線上で開始された保護切り替えアクションはありません。
クリア（Clear）	回線上の保護切り替えの状態をクリアします。	保護切り替えアクションの現在の状態は[動作時にロックアウト（Lockout On Working）] ではありません。
演習（Exercise）	保護切り替えの準備がODUサブコントローラにできているかどうかを確認します。	回線上で開始された保護切り替えアクションはありません。

動作時に手動（Manual On Working）	保護されたパスから動作中のパスにトラフィックを手動で切り替えます。	回線上で開始された保護切り替えアクションはありません。
動作時にロックアウト（Lockout On Working）	ODU サブコントローラ グループ内のロックアウトされたリソースとして ODUk サブコントローラを設定します。トラフィックを動作中のパスに切り替えることができないように回線をロックします。	保護切り替えアクションの現在の状態は [動作時にロックアウト（Lockout On Working）] ではありません。
ロックアウトのクリア（Clear Lock out）	回線の [動作時にロックアウト（Lockout On Working）] スイッチ状態をクリアします。	保護切り替えアクションの現在の状態は [動作時に手動（Manual On Working）] です。
ステータス（Status）	AID で指定された ODU サブコントローラ グループと保護切り替えの状態の詳細を表示します。	保護されたすべての光回線で使用できます。
保護時に強制（Force On Protect）	ネットワークを介してトラフィックを伝送する保護されたパスを設定します。	保護切り替えアクションの現在の状態は、[手動時に保護（Manual On Protect）] または [動作時に手動（Manual On Working）] です。

回線/VC の再同期

プライマリまたは検出状態がダウンしている、または参加デバイス間にリンクが見つからないなど、回線/VC に問題がある場合は、回線を再同期できます。Cisco EPN Manager は、問題を解決するためのベスト エフォートで、回線を参加デバイスと同期させます。

回線/VC を再同期するには、次の手順を実行します。

ステップ 1 次のいずれかのページにアクセスします。

- [回線/VC 360（Circuit/VC 360）] ビュー。回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ）を参照してください。
- [回線/VC の詳細（Circuit/VC Details）] ウィンドウ。回線/VC に関する総合情報の取得：[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウ （810 ページ）を参照してください。
- [マルチレイヤトレース（Multi-Layer Trace）] ビュー。回線のすべてのルートのトレースと視覚化（248 ページ）を参照してください。

ステップ2 **[アクション（Actions）]** > **[再同期（Resync）]**を選択します。

再同期アクションの進行中に、回線の検出状態が [再同期（Resync）] に変わります。アクションが完了すると、検出状態が [完全（Full）] または [部分（Partial）] に変わります。

サービス検出の再同期

デバイスに競合が生じている場合は、サポートされているシリアルサービス、IOT CEM、および IOT CEM バリアント X.21 C 3794、MPLS-TE、CE、L3VPN、SR-TE、CEM over T1/E1/E3/T3/SONET/SDH のサービスを再同期できます。

[サービス 360（Service 360）] ビュー領域で、[アクション（Action）] ドロップダウンリストから [再同期（Resync）] を選択して関連エンティティを更新します。つまり、特定のサービスに関連するサービスの再同期を実行できます。

（注） [検出状態（Discovery State）] フィールドに現在の状態を表示します。再同期されたステータスとタイムスタンプが [手動再同期状態（Manual Resync State）] に表示されます。

回線/VC の削除

回線/VC の削除または強制的な削除を選択できます。

プロビジョニング状態が [作成成功（Create Succeeded）]、[変更成功（Modify Succeeded）] または [作成失敗（Create Failed）]、[変更失敗（Modify Failed）]、[削除失敗（Delete Failed）] の回線/VC を削除できます。

ネットワーク管理者は、[回線/VC（Circuit/VCs）] ウィンドウで選択したサービスの MPLS TE トンネルとレイヤ3リンクを強制的に削除できます。このオプションは、以前の削除操作で障害が発生した場合や、サービスが見つからない状態にある場合に使用できます。失敗したプロビジョニングの削除状態にある回線/VC は強制的に削除できます。回線/VC を強制的に削除すると、Cisco EPN Manager データベースからも削除されます。この回線/VC は回線/VC のテーブルに表示されなくなります。

注意 ただし、強制削除オプションでは、回線/VCに参加している一部のデバイスから設定が削除されないことがあります。デバイスを手動でクリーンアップする必要があります。

（注） 強制削除オプションは、光回線では使用できません。

回線/VC を削除または強制削除するには、次の手順に従います。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）]>[トポロジ マップ（Topology Maps）]>[ネットワーク トポロジ（Network Topology）]** の順に選択します。

[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。

ステップ 2 ツールバーで [デバイス グループ（Device Groups）] をクリックし、必要なグループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] タブをクリックし、削除する回線または VC のオプション ボタンをクリックします。

ステップ 4 [回線/VC（Circuits/VCs）] ペインのツールバーから次のいずれかを実行します。

- [X]（削除）アイコンのドロップダウンリストから [強制削除（Force Delete）] を選択します。確認メッセージが表示されます。対応するジョブが [ジョブ（Jobs）] ダッシュボードに作成されるため、進行状況を監視できます。ジョブが完了すると、回線/VC が Cisco EPN Manager データベースから削除されます。
- [X]（削除）アイコンをクリックします。プロビジョニング ウィザードが開き、選択した回線または VC の情報が表示されます。

ステップ 5 **Next** をクリックして [サービスの詳細（Service Details）] ページに移動します。

ステップ 6 [展開（Deploy）] エリアで、削除操作の完了時点で予期される内容を指定します。

- [デバイスとCisco EPN Managerから回線またはVCを削除する（Delete the circuit or VC from devices and Cisco EPN Manager）]：回線または VC に参加するすべてのデバイスから設定が削除され、またデータベースからも設定が削除されます。回線または VC が回線と VC の表に表示されず、回線または VC の履歴もなくなります。
- [デバイスのみから回線または VC を削除する（Delete the circuit or VC from devices only）]：回線と VC の履歴はデータベースに残りますが、回線または VC に参加しているデバイスから、関連するすべての設定が削除されます。

（注） これらのオプションは、「失敗（failed）」ステータス（例：[作成失敗（Create failed）]、[変更失敗（Modify failed）] など）の EVC/OVC を削除する場合にのみ、ウィザードで使用できます。

ステップ 7 [展開アクション（Deployment Action）] フィールドで次のように操作します、

- 実際の展開前に、関連デバイスに展開される設定を表示するには **Preview** を選択します。
- 変更内容をプレビューせずに展開するには **Deploy** を選択します。

ステップ 8 **Submit** をクリックします。

- 前のステップで [プレビュー（Preview）] を選択した場合は、[設定のプレビュー（Preview Config）] ページが表示されます。変更点に問題がなければ **Deploy** をクリックします。
- 前のステップで [展開（Deploy）] を選択した場合は、設定がデバイスに即時に展開されます。

展開が完了すると確認メッセージが表示されます。

回線/VC に参加している各デバイスの設定、設定エラー、ロールバック設定、およびロールバック設定エラーの詳細を表示するには、拡張テーブル内の [削除済み回線/VC（Deleted Circuits/VCs）] タブの [プロビジョニング（Provisioning）] 列の横にある [i] アイコンをクリックします。[i] アイコンは、[なし（None）] を除くすべてのプロビジョニング状態で使用できます。拡張テーブルへのアクセス方法については、ネットワークトポロジマップからのアラーム、ネットワークインターフェイス、回線/VC、およびリンクの詳細テーブルの表示（222ページ）を参照してください。

（注） Cisco EPN Manager を使用せずに、別の EMS を介して、または CLI、NETCONF、TL1 インターフェイスを介して Cisco EPN Manager によって管理されているデバイスの回線を削除しても、Cisco EPN Manager では回線は自動的に削除されません。回線を削除するには、[削除（Delete）] または [強制削除（Force Delete）] オプションを使用する必要があります。

L3VPN サービスの削除または強制削除

Cisco EPN Manager を使用して最初に作成された L3VPN サービスを削除または強制削除できます。検出されたものの、Cisco EPN Manager を使用して作成されていない L3VPN サービスは削除できません。

L3VPN サービスを削除または強制削除するには、次の手順を実行します。

ステップ 1 左側のペインで、**[マップ（Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [回線/VC（Circuits/VCs）] パネルで [回線/VC（Circuits/VCs）] リンクをクリックし、Cisco EPN Manager 内のすべてのサービスを表示します。

ステップ 3 削除または強制削除するサービスを選択します。[名前（Name）] フィルタにサービス名を入力して目的の L3VPN サービスをフィルタ処理で除外してから、[X]（[削除（Delete）]）アイコンをクリックします。

ステップ 4 または、[回線/VC（Circuits/VCs）] ペインのツールバーから次のいずれかを実行します。

a) 削除するサービスを選択し、[X]（[削除（Delete）]）アイコンをクリックします。

プロビジョニング ウィザードが開き、選択した回線または VC の情報が表示されます。

[次へ（Next）] をクリックして [サービスの詳細（Service Details）] ページに移動します。

[L3VPN プロビジョニング（L3VPN Provisioning）] ウィザードに、選択した L3VPN に関連付けられている VRF、エンドポイントおよびその他の詳細が表示されます。

b) [X]（削除）アイコンのドロップダウンリストから [強制削除（Force Delete）] を選択します。確認メッセージが表示されます。対応するジョブがジョブ ダッシュボード（**[管理（Administration）] > [ダッシュボード（Dashboard）] > [ジョブ ダッシュボード（Job Dashboard）] > [ユーザー ジョブ（User**

Jobs）] > **[回線の強制削除（Force Delete Circuit）]**）に作成され、進行状況を監視できます。ジョブが完了すると、レイヤ 3 リンクは Cisco EPN Manager データベースから削除されます。

また、GUI からサービスの削除を継続できない場合は、[強制削除（Force Delete）] オプションを使用します。

ステップ 5 [送信（Submit）] をクリックして、デバイスにプッシュする設定をプレビューします。

ステップ 6 設定を再検討してから [展開（Deploy）] をクリックして確認します。展開が完了すると確認メッセージが表示されます。

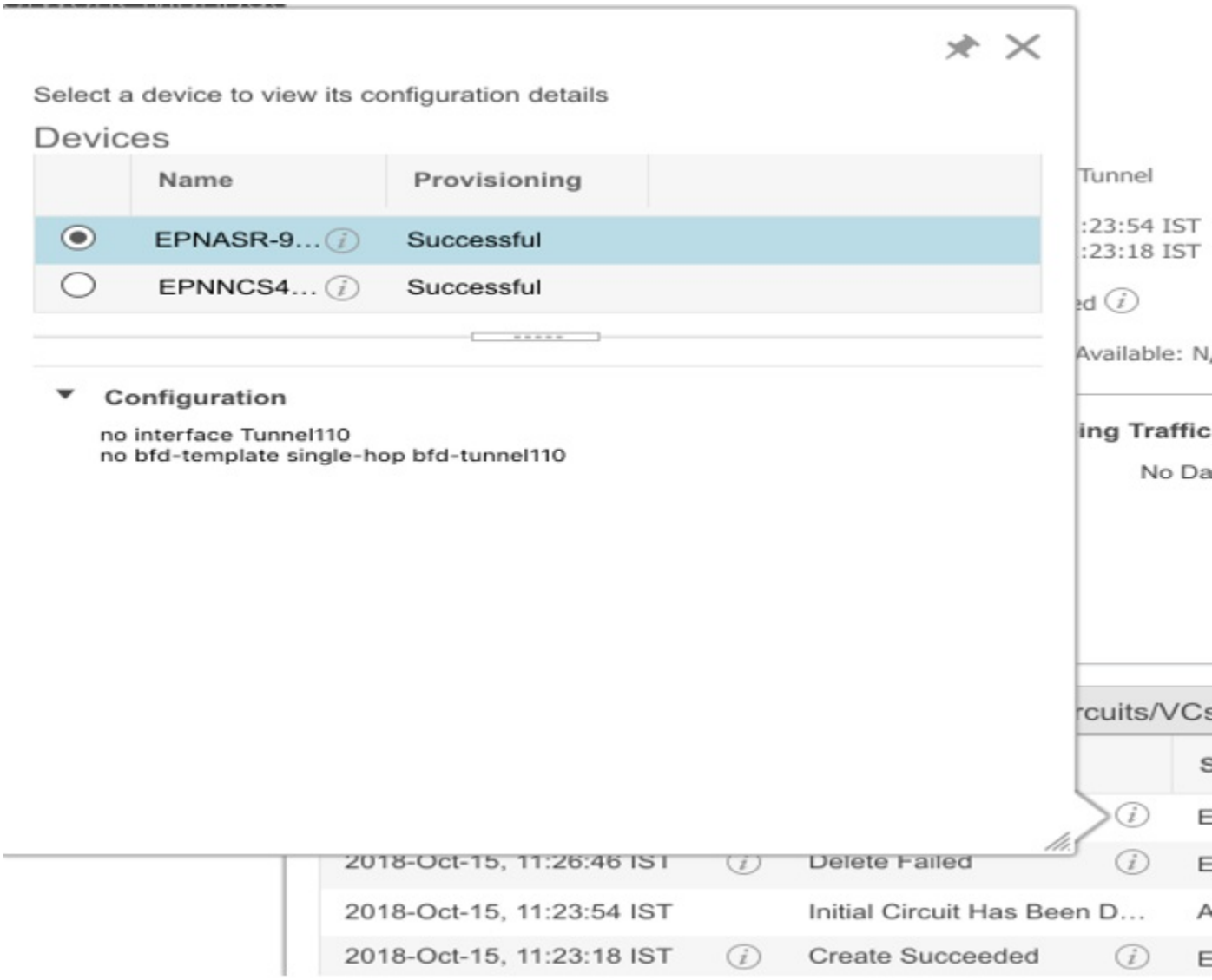
選択した L3VPN サービスがデバイスから削除されます。

（注） 選択した L3VPN サービスで統合ルーティングおよびスイッチング（BVI/仮想インターフェイス）を使用している場合、L3VPN サービスを削除すると、関連付けられている BVI/仮想インターフェイスがデバイスから自動的に削除されます。L3VPN サービスに関連付けられている BGP および VRF の設定も削除されます。

ステップ 7 選択した L3VPN がデバイスから削除されたことを確認するには、[回線/VC（Circuit/VCs）] リストから L3VPN サービスの完全なリストを表示します。

ステップ 8 強制削除されたサービスのデバイス設定を表示するには、[削除された回線/VC（Deleted Circuit/VCs）] タブの [履歴（History）] タブの [プロビジョニング（Provisioning）] 列の横にある [i] アイコンをクリックします。[回線 /VC 360* ビュー（Circuit/VC 360* View）] ウィンドウで、[なし（None）] を除くすべてのプロビジョニング状態で使用できる [i] アイコンをクリックし、選択したデバイスの設定の詳細を表示します。

図 *16 :* 回線*/VC 360** ビュー（*Circuit/VC 360* View*）



L3VPN サービス エンドポイントの削除

Cisco EPN Manager を使用して作成された L3VPN サービスの場合、そのサービスの L3VPN サービス エンドポイントを削除できます。検出されたものの、Cisco EPN Manager を使用して作成されていない L3VPN サービスに関連付けられているエンドポイントは削除できません。

L3VPN サービス エンドポイントを削除するには、次の手順に従います。

ステップ 1 左側のサイドバーで、**[マップ（Maps）]** > **[ネットワークトポロジ（Network Topology）]** の順に選択します。

ステップ 2 [回線/VC（Circuits/VCs）] パネルで [回線/VC（Circuits/VCs）] リンクをクリックし、Cisco EPN Manager 内のすべてのサービスを表示します。

ステップ 3 削除するサービスを選択します。[名前（Name）] フィルタにサービス名を入力して、目的の L3VPN サービスをフィルタリングできます。

ステップ 4 鉛筆の形をした [変更（Modify）] アイコンをクリックします。

[L3VPN プロビジョニング（L3VPN Provisioning）] ウィザードに、選択した L3VPN に関連付けられている VRF、エンドポイントおよびその他の詳細が表示されます。

ステップ 5 [エンドポイントの削除（Delete Endpoint）] を選択し、[次へ（Next）] をクリックします。

ステップ 6 選択した L3VPN サービスとの関連付けを解除する IP エンドポイントを選択します。単一エンドポイントの VRF の場合、エンドポイントを削除すると VRF が無効になり、ダングリング VRF として機能するようになります。この無効になった VRF に新しいエンドポイントを関連付けるには、VRF の属性を編集する必要があります。

ステップ 7 [次へ（Next）] をクリックして、デバイスにプッシュされる設定をプレビューします。

ステップ 8 設定を確認してから [展開（Deploy）] をクリックし、デバイスへの変更を確認して展開します。

選択した L3VPN サービス エンドポイントがデバイスから削除されます。

MPLS TE サービスの削除または強制削除

[計画（Planned）]、[成功（Succeeded）]、[失敗（Failed）]、または [なし（None）] のプロビジョニング状態にある MPLS TE サービスを削除または強制削除できます。プロビジョニング状態の詳細については、回線または VC の状態 （790 ページ）を参照してください。

（注） CEM サービスまたはキャリア イーサネット 回線/VC で MPLS TE サービスを使用している場合は、MPLS TE サービスを削除できません。

ステップ 1 左側のペインから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックし、必要な回線/VC が作成された場所を選択します。

ステップ 3 [デバイス グループ（Device Groups）] ポップアップ ウィンドウを閉じます。

ステップ 4 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 5 [回線/VC（Circuit/VCs）] タブで、回線/VC のリストの下にある [回線/VC（Circuit/VCs）] ハイパーリンクをクリックします。

ステップ 6 回線/VC が表示されているテーブルで、削除する MPLS TE サービスを選択します。

ステップ 7 [削除（Delete）] アイコンまたは [強制削除（Force Delete）] をクリックしてプロビジョニング ウィザードを開き、選択した MPLS TE サービスの情報を表示します。

ステップ 8 [展開アクション（Deployment Action）] ドロップダウン リストから、次のいずれかを選択します。

- [プレビュー（Preview）]：実際の展開前に、関連するデバイスに展開される設定を表示します。
- [展開（Deploy）]：変更内容をプレビューせずにそれらを展開します。

ステップ 9 [送信（Submit）] をクリックします。

- 前のステップで [プレビュー（Preview）] を選択した場合、Cisco EPN Manager は [プレビューの設定（Preview Config）] ページを表示します。変更点に問題がなければ、[展開（Deploy）] をクリックします。
- 前のステップで [展開（Deploy）] を選択した場合、Cisco EPN Manager はその設定をデバイスにすぐに展開します。

強制削除されたサービスのデバイス設定の詳細を表示するには、[回線/VC 360*（Circuit/VC 360*）] ウィンドウの [履歴（History）] タブの [プロビジョニング（Provisioning）] 列の横にある [i] アイコンをクリックします。[i] アイコンは、[なし（None）] を除くすべてのプロビジョニング状態で使用できます。

Cisco EPN Manager は、展開が完了すると確認メッセージを表示します。

プロビジョニングされたネットワーク インターフェイスの管理

Cisco EPN Manager は、プロビジョニングされた回線/VC とは別にネットワーク インターフェイスの詳細を表示および管理できるように、ネットワーク インターフェイス（UNI または ENNI）としてプロビジョニングされたインターフェイスのテーブルを提供します。このテーブルには、識別情報、そのデバイスが属しているデバイス、デバイス上の実際のインターフェイス、ネットワーク インターフェイスが現在参加しているサービスの数など、各ネットワーク インターフェイスに関する情報が表示されます。

次の情報を表示できます。

- 特定のデバイス グループ内のネットワーク インターフェイス（[ネットワーク トポロジ（Network Topology）] ウィンドウから）。
- Cisco EPN Manager で管理されるすべてのネットワーク インターフェイス（[インベントリ（Inventory）] メニューから）。

[編集（Edit）] ボタンをクリックすると、ネットワーク インターフェイスを編集できます。これにより、必要に応じてネットワーク インターフェイスを変更できるウィザードが起動します。ネットワーク インターフェイスが複数のサービスに関連付けられている場合、編集操作はそれらのすべてのサービスに影響することに注意してください。

ネットワーク インターフェイスは、どの回線にも参加していない限り削除できます。

ステップ 1 特定のデバイス グループに属しているネットワーク インターフェイスを表示および管理するには、次の手順を実行します。

a) 左側のサイドバー メニューから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** の順に選択します。

b) [デバイス グループ（Device Groups）] ボタンをクリックして、必要なグループを選択します。

c) [回線/VC（Circuit/VCs）] タブで、[ネットワーク インターフェイス（Network Interfaces）] ハイパーリンク（テーブルの下）をクリックします。

ステップ 2 Cisco EPN Manager で管理されているすべてのネットワーク インターフェイスを表示および管理するには、**[インベントリ（Inventory）]** > **[その他（Other）]** > **[ネットワーク インターフェイス（Network Interfaces）]** を選択します。

ネットワーク インターフェイスの削除

UNI/ENNI が現在どの回線にも参加していない場合は、[ネットワーク インターフェイス（Network Interfaces）] テーブルから UNI/ENNI を削除できます。

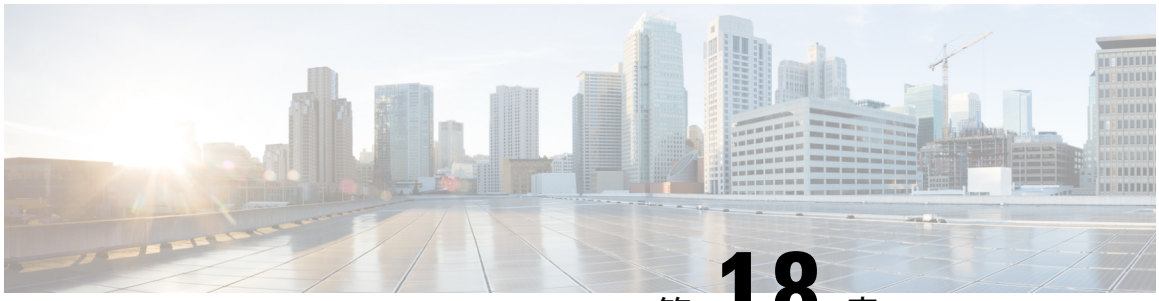
ネットワーク インターフェイスを削除するには、次の手順を実行します。

ステップ 1 左側のサイドバーで、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックして、必要なグループを選択します。

ステップ 3 [回線/VC（Circuit/VCs）] タブで、[ネットワーク インターフェイス（Network Interfaces）] ハイパーリンクをクリックして [ネットワーク インターフェイス（Network Interfaces）] テーブルを表示します。

ステップ 4 削除するネットワーク インターフェイスを選択し、[削除（Delete）] ボタンをクリックします。ネットワーク インターフェイスが 1 つ以上の回線/VC に参加している場合、[削除（Delete）] ボタンは無効になります。[回線/VC 数（No. of Circuit/VCs）] 列には、ネットワーク インターフェイスが含まれている回線/VC の数が表示されます。



第 18 章

回線/VC のモニターリングとトラブルシューティング

回線/VC のエラーのチェック

Cisco EPN Manager には、回線/VC に問題がないかどうかを一括で確認するための複数の方法があります。

- 回線一覧：各回線/VC 名の左側にある色付きのアイコンは、回線/VC のプライマリ状態を示しています。プライマリ状態で回線/VC に問題があることが示された場合は、下記の説明に従って回線/VC の詳細なアラーム情報にアクセスできます。
- 回線/VC の 360 度ビュー：回線/VC の 360 度ビューの [アラーム（Alarms）] タブには、回線/VC が設定されているすべてのデバイスのすべてのアラームが表示されます。回線/VC の 360 度ビューにアクセスするには、回線/VC 名の横にある情報アイコンをクリックします。
- アラーム テーブル：アラーム テーブルには、すべてのデバイス、特定のデバイス グループ、または特定のデバイスのすべてのアラームが表示されます。アラームテーブルにアクセスするには、**Monitor > Monitoring Tools >Alarms and Events** を選択します。回線/VC の 360 度ビューでアラームを特定した場合、アラーム テーブルでそのアラームの詳細を取得できます。アラームまたはアラームを生成したデバイス/リンクは、簡易フィルタまたは高度なフィルタを使用して検索できます。テーブルの各アラームを展開し、アラームの影響を受ける回線/VC など、アラームに関する詳細情報を表示できます。

- ネットワーク トポロジでの回線/VC オーバーレイ：[回線/VC（Circuits/VCs）] 一覧で回線/VC を選択すると、ネットワーク トポロジに、既存のトポロジの上のオーバーレイとして表されます。特定のデバイスのアラームの場合は、アラーム バッジが通常どおりそのデバイス上に表示されます。回線/VC エンドポイント間のリンク上のアラームの場合は、アラーム バッジがそのリンクに表示されます。
- 光回線のマルチレイヤ トレースの詳細については、回線/VC の完全なルートをトレースおよび可視化する （860 ページ）を参照してください。

特定の障害による影響を受けている回線/VC の識別

特定の障害による影響を受けている回線/VC を識別するには、次の手順を実行します。

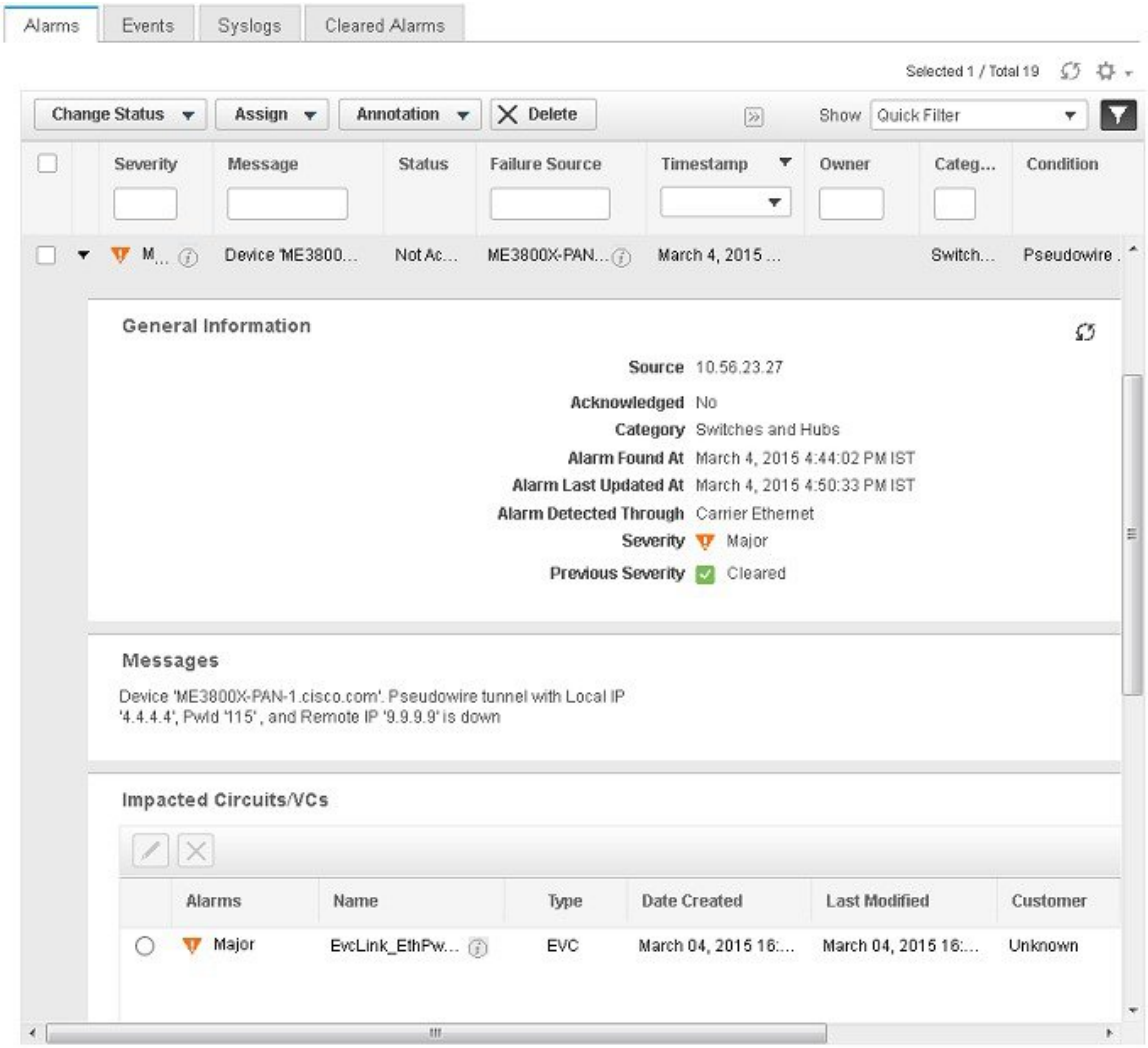
ステップ 1 左側のサイドバーから **Monitor > Monitoring Tools > Alarms and Events** を選択します。

ステップ 2 [アラーム（Alarms）] テーブルで目的のアラームを見つけます。必要に応じてシンプルなフィルタまたは高度なフィルタを使用して、アラームを見つけることができます。

ステップ 3 行の左側にある矢印をクリックしてその行を展開し、アラームの詳細を表示します。

ステップ 4 [影響を受けている回線/VC（Impacted Circuit/VCs）] ペインを見つけます。選択したアラームの影響を受けているすべての回線/VC のリストがこのペインに表示され、各回線/VC の基本情報が示されます。[回線/VC 360（Circuit/VC 360）] ビューにアクセスし、[i] アイコンをクリックすると、回路/VC に関するより詳しい説明を表示できます。

ステップ 5 必要に応じて、回線/VC を選択し、[変更（Modify）] または [削除（Delete）] ボタンをクリックし、[影響を受けている回線/VC（Impacted Circuit/VCs）] ペインから回線/VC を変更または削除します。これにより、プロビジョニング ウィザードが開きます。詳細については、「回線/VC の変更 （821 ページ）」と「回線/VC の削除 （830 ページ）」を参照してください。



回線/VC 障害に関する詳細情報の取得

Cisco EPN Manager には、回線/VC のプロビジョニング操作が失敗した理由に関する情報が表示されるので、問題をトラブルシューティングできます。[回線/VC（Circuits/VCs）] テーブルでは、プロビジョニング状態、サービスアビリティとディスカバリ状態を参照して回線/VC の問題を特定できます。回線/VC のプロビジョニング中にエラーが発生し、回線/VC を作成できなかった場合、プロビジョニング状態は [作成失敗（Create Failed）] になります。[プロビジョニング（Provisioning）] 列の [i] アイコンをクリックすると、この失敗に関連するデバイスの設定と、発生した特定のエラーに関する詳細情報が表示されます。

光回線の場合、サービスアビリティ状態が [ダウン（Down）] でありディスカバリ状態が [部分（Partial）] の場合、回線で問題が発生している可能性があります。この場合、[サービスアビリティ（Serviceability）] 列で [i] アイコンをクリックすると、サービスアビリティ状態が [ダウン（Down）] である理由が表示されます。

（注） 回線/VC の障害に関する情報は、[回線/VC 360（Circuit/VC 360）] ビューからも確認できます。回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ）を参照してください。

[回線/VC（Circuits/VCs）] テーブルから回線/VC プロビジョニングの失敗に関する追加情報を表示するには、次の手順に従います。

ステップ 1 左側のサイドバーのメニューから、**[マップ（Maps）]>[トポロジ マップ（Topology Maps）]>[ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] タブをクリックし、次に [回線/VC（Circuits/VCs）] ハイパーリンクをクリックします。別のウィンドウが開き、すべての回線を示すテーブルが表示されます。

ステップ 3 プロビジョニング操作が失敗した回線を見つけます。プロビジョニング状態は [作成失敗（Create Failed）] です。

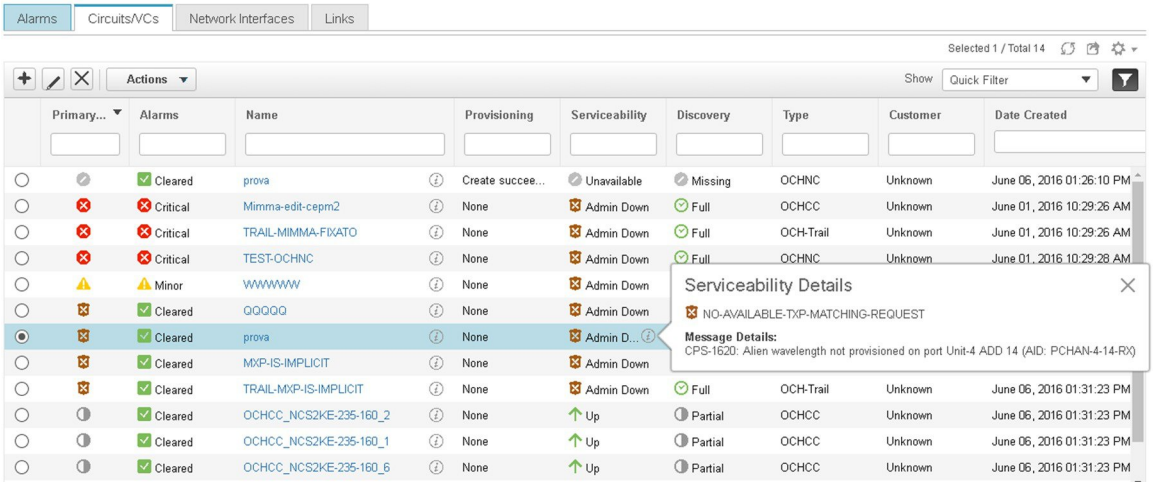
ステップ 4 [プロビジョニング（Provisioning）] 列の横にある [i] アイコンをクリックします。ポップアップ ウィンドウに、プロビジョニング エラーが発生したデバイスのリストが表示されます。

ステップ 5 デバイスを選択し、設定とエラーの詳細を確認します。

ステップ 6 [サービスアビリティ（Serviceability）] 列の横にある [i] アイコンをクリックして [サービスアビリティの詳細（Serviceability Details）] データ ポップアップ ウィンドウを表示します。このウィンドウには、プロビジョニング操作が回線で失敗した理由に関する情報が表示されます。

（注） [i] アイコンは、サービスアビリティ状態が [ダウン（Down）] であり、ディスカバリ状態が [部分（Partial）] の場合にのみ使用可能です。

光回線では、サービスアビリティ状態が [ダウン（Down）] であり、ディスカバリ状態が [部分（Partial）] の場合、[サービスアビリティ（Serviceability）] 列の横にある [i] アイコンをクリックすると、[サービスアビリティの詳細（Serviceability Details）] データ ポップアップ ウィンドウが表示されます。このウィンドウには、回線のサービスアビリティ状態が [ダウン（Down）] である理由に関する情報が表示されます。また、[回線/VC 360（Circuit/VC 360）] ビューから [サービスアビリティの詳細（Serviceability Details）] データ ポップアップ ウィンドウを表示することもできます。[回線/VC 360（Circuit/VC 360）] ビューを表示する方法については、回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ）を参照してください。



OAMコマンドを使用してサービス障害をトラブルシュートする

Cisco EPN Manager には、サービス障害をトラブルシュートするために、ping 機能とトレースルート機能が用意されています。OAM コマンドを使用すると、これらの機能にアクセスし、サービス内の 2 つのエンドポイント間の接続とパスをモニターできます。その後、障害を特定して解決できます。各種 IOS デバイスでサポートされている技術は次のとおりです。

- MPLS LSP、疑似回線、および CFM：Cisco IOS-XE および Cisco IOS-XR
- MPLS 双方向 TE Flex LSP および VRF：Cisco IOS-XE

OAM コマンドの起動ポイントは、以下に基づいて異なります。

- 技術タイプ：ネットワーク デバイス テーブルからの起動 （843 ページ）（この OAM コマンドの起動ポイントは、**MPLS LSP** 技術でのみサポートされています）
- サービス タイプ：回線 360 からの起動 （844 ページ）
- イベント タイプ：アラーム ブラウザからの起動 （844 ページ）

OAM コマンドを使用して ping またはトレースルートを実行すると、サービス障害をトラブルシュートできます。OAM コマンドを使用した ping または traceroute の実行 （845 ページ）を参照してください

ネットワーク デバイス テーブルからの起動

ネットワーク デバイス テーブルから MPLS LSP 技術の OAM コマンドを起動するには：

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルで、MPLS 対応デバイスを選択します。

ステップ 3 [ネットワーク デバイス（Network Devices）] テーブルの上の [>>] アイコンをクリックし、[OAM コマンド（OAM Commands）] を選択します。

回線 360 からの起動

サービス/回線 360 から OAM コマンドを起動する場合は、サポートされる技術が、サービス タイプによって決まります。各種サービス タイプの詳細については、「回線/VC の検出およびプロビジョニングの概要 （605 ページ）」を参照してください。

回線 360 から OAM コマンドを起動するには：

ステップ 1 **[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [ネットワーク トポロジ（Network Topology）] ウィンドウで、[回線/VC（Circuits/VCs）] タブをクリックし、回線の横にある [i] アイコンをクリックして、回線 360 を表示します。選択した回線のサービス タイプに基づいて、サポートされている技術 OAM コマンド（この表に記載）が表示されます。

OAM コマンドを起動できるサービス タイプ：	**サポートされる技術**
キャリア イーサネット	• セグメントルーティング LSP • 疑似回線 • CFM
回線エミュレーション（CEM）	• MPLS LSP • 疑似回線 • 双方向 TE（Flex LSP）
L3VPN	• MPLS LSP • VRF
双方向 TE トンネル（Flex LSP）	• MPLS LSP • 双方向 TE（Flex LSP）

ステップ 3 [アクション（Actions）] をクリックし、選択したサービス タイプに対して表示する**技術 OAM** を選択します。

アラーム ブラウザからの起動

アラーム ブラウザから OAM コマンドを起動する場合は、サポートされる技術が、イベント タイプによって決まります。

アラーム ブラウザから OAM コマンドを起動するには：

ステップ 1 **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [アラームとイベント（Alarms and Events）]** を選択します。

ステップ 2 [アラーム（Alarms）] テーブルで、この表の「OAM コマンドを起動できるイベント タイプ」列に一覧表示されているイベント タイプのアラームを選択します。

サポートされる技術	**OAM コマンドを起動できるイベント タイプ**：
MPLS 双方向 TE トンネル（Flex LSP）	• mplsTunnelUp • mplsTunnelDown • mplstunnelReoptimized • ROUTING-MPLS_TE-5-LSP_UPDOWN • MPLS_TE-5-TUN • MPLS_TE-5-LSP
L3VPN の VRF	• mplsL3VpnVrfUp • mplsL3VpnVrfDown • mplsL3VpnNumVrfRouteMaxThreshCleared • mplsL3VpnVrfNumVrfRouteMaxThreshExceeded • mplsL3VpnVrfRouteMidThreshExceeded
キャリア イーサネットと回線エミュレーションの疑似回線	• cpwVcDown • cpwVcUp • XCONNECT-5-PW_STATUS ダウン • L2-L2VPN_PW-3-UPDOWN
キャリア イーサネットの CFM	• E_CFM-3-REMOTE_MEP_DOWN_TIME_OUT • L2-CFM-6-MEP_CHANGE

ステップ 3 [アラーム（Alarms）] テーブルの上にある [トラブルシュート（Troubleshoot）] をクリックし、[OAM コマンド（OAM Commands）] を選択します。

OAM コマンドを使用した ping または traceroute の実行

OAM コマンドを使用して ping または traceroute あるいは multipath（SR の場合のみ）を実行するには、次の手順を実行します。

ステップ 1 [テクノロジー（Technology）] の [OAM コマンド（OAM Command）] ウィンドウを起動します。サポートされるテクノロジーでの OAM コマンド起動ポイントについては、OAM コマンドを使用してサービス障害をトラブルシュートする （843 ページ）を参照してください。

ステップ 2 起動ポイントに基づいて、この表に示されているように、選択したテクノロジー タイプの必須フィールドの値を選択します。

テクノロジー タイプ	アラーム ブラウザから起動する場合	サービス/回線 360 度ビューから起動する場合
疑似回線	詳細が自動入力されます。	[疑似回線エンドポイント（Pesudowire Endpoint）] ドロップダウン リストから、サービスに参加しているエンドポイントを選択します。
LSP	[宛先 LDP ID（Destination LDP ID）] ドロップダウン リストから、サービスに参加している宛先エンドポイントの LDP ID を選択します。	ドロップダウンリストから [送信元（Source）] と [宛先（Destination）] を指定します。 [宛先（Destination）] フィールドに、次のように入力します。 • LDP 対応デバイスが選択されている場合は、Ping および Traceroute オプションが有効になります。 • SR 対応デバイスが選択されている場合は、Ping、Traceroute、Multipath、Nil FEC Ping、および Nil FEC Traceroute オプションが有効になります（Nil FEC オプションは、ラベル、OutputInterface、および NextHop の各フィールドが入力されている場合にのみ有効になります）。
MPLS 双方向 TE トンネル（Flex LSP）	ping またはトレース ルートを実行するトンネルのパスを [アクティブ（Active）]、[動作中（Working）]、または [保護パス（Path-Protect）] として選択します。Cisco EPN Manager は ping またはトレース ルートを両方向（ヘッドエンドからテールエンドとその逆）に実行します。	ping またはトレース ルートを実行するトンネルのパスを [アクティブ（Active）]、[動作中（Working）]、または [保護パス（Path-Protect）] として選択します。Cisco EPN Manager は ping またはトレース ルートを両方向（ヘッドエンドからテールエンドとその逆）に実行します。
L3VPN での VRF	[エンドポイント（End Points）] ドロップダウン リストから、同じ VPN に属する別の VRF を選択します。	[送信元エンドポイント（Source End Points）] および [宛先エンドポイント（Destination End Points）] ドロップダウン リストから、同じ VPN に属する別の VRF の送信元および宛先エンドポイントを選択します。

テクノロジー タイプ	アラーム ブラウザから起動する場合	サービス/回線 360 度ビューから起動する場合
キャリア イーサネットでの CFM	[宛先 MEP ID（Destination MEP ID）] ドロップダウン リストから、サービスに参加している宛先エンドポイントの MEP ID を選択します。	[送信元 MEP ID（Source MEP ID）] および [宛先 MEP ID（Destination MEP ID）] ドロップダウン リストから、サービスに参加している送信元および宛先エンドポイントの MEP ID を選択します。
SR TE		[ポリシー名（Policy Name）] ドロップダウンリストから、ポリシーを選択します。 注：このオプションは、スタティックおよびダイナミック SR ポリシーまたは EVPN テクノロジーを介して設定されたデバイスに対して有効になります。

ステップ 3 ping を実行する場合は **[アクション（Actions）]** > **[Ping]** を選択し、traceroute を実行する場合は **[アクション（Actions）]** > **[Traceroute]** を選択します。また、multipath アクションを実行するには、**[アクション（Actions）]** > **[Multipath]** を選択します。

ping、traceroute、および multipath コマンドの結果は、次の形式で表示されます。

（注）
- MPLS 双方向 TE トンネルの場合、双方向の結果、つまりヘッドエンドからテールエンドへの方向での結果と、テールエンドからヘッドエンドへの方向での結果が表示されます。
- 疑似回線の場合、結果はビジュアル形式と表形式、および raw データとして表示されます。

- ビジュアル：エンドポイントを使用するサービスとそのサービスのホップがマップ上に表示されます。マウスのカーソルをエンドポイントの上に重ねると、発信インターフェイスや着信インターフェイスなどの詳細情報が表示されます。

（注） すべてのテクノロジーの traceroute コマンドの結果は、ビジュアル形式で表示されます。

- テーブルデータ：発信および着信インターフェイス、デバイス名、サービスに参加するエンドポイントのラベルなどの情報が表形式で表示されます。

（注） traceroute および multipath コマンドの結果が表形式で表示されます。

- raw データ：サービスに参加するエンドポイントの関する情報がフォーマット化されていないソース データとして表示されます。

（注） ping、traceroute、および multipath コマンドの結果が raw データとして表示されます。

EOAM テンプレートを使用した EVC のトラブルシューティング

Cisco EPN Manager では、いくつかの定義済みテンプレートが提供されています。これらを使用して、キャリア イーサネット ネットワーク内の仮想接続（VC）について接続とパフォーマンスをモニターリングできます。これを使用するには、**Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI** を選択します。詳細については、EOAM の接続チェックとパフォーマンス チェックの実行 （548 ページ）を参照してください。

回線/VC のパフォーマンス テストの実行

パフォーマンス テストを実行すると、Cisco EPN Manager はネットワーク要素に接続して、リアルタイム データを提供します。履歴情報を取得するには、回線/VC のパフォーマンス測定指標とレポートを表示する （858 ページ）を参照してください。

- EVC の Y.1564 に基づくパフォーマンス テスト （848 ページ）
- EVC の Y1731 に基づくパフォーマンス テスト （852 ページ）
- 光回線のパフォーマンス テスト （853 ページ）
- 回線エミュレーション サービスのパフォーマンス テスト （856 ページ）

EVC の Y.1564 に基づくパフォーマンス テスト

CE パフォーマンス テストでは、有効化時に CE EVC の正確な構成およびパフォーマンスを確認します。また、CE パフォーマンス テストを使用して、すでに動作している EVC をトラブルシューティングすることもできます。

Y.1564イーサネットサービスの有効化またはパフォーマンステストの手法により、イーサネットベースのサービスの有効化、インストール、およびトラブルシューティングが可能になります。このテストを使用すると、UNI間のサービス設定とパフォーマンスを確認できます。これは、SLA が購入済みの帯域幅プロファイルおよび確約されたサービス クラスに従って満たされることを確認するものです。

これらのテストは、単一のテストでイーサネット サービス レベル契約（SLA）を完全に検証します。トラフィック ジェネレータ パフォーマンス プロファイルを使用すると、要件に基づいてトラフィックを作成できます。スループット、損失、可用性などのネットワークのパフォーマンスは、さまざまな帯域幅プロファイルのレイヤ2トラフィックを使用して分析されます。

（注） パフォーマンス テストは、ネットワーク上に設定され、Cisco EPN Manager によって検出される EVC に対してのみ実行できます。

サポートされるデバイス

Y.1564 パフォーマンス テストは、IOS 15.4(S) または IOS XE 3.12S 以降を実行している次のデバイスでサポートされています。

- 送信元または宛先として指定できるデバイスは、次のとおりです。
  - Cisco ASR 920
  - 送信元と宛先の両方に RSP3 を使用した Cisco ASR907（ループバック）
  - 送信元と宛先の両方に RSP2、RSP3 を使用した Cisco ASR903（ループバック）
  - Cisco ASR 901
  - Cisco ASR9K（ループバックとして）
  - Cisco NCS 4201
  - Cisco NCS 4202
  - Cisco NCS 4206
  - Cisco NCS 4216
  - NCS540（ループバックとして）
  - Cisco NCS55xx（ループバックとして）
  - Cisco ME 1200
  - Cisco ME 3600
  - Cisco ME3800（ループバック）
- 宛先（ループバック）としてのみ指定できるデバイスは次のとおりです。
  - Cisco ME3800X

- Cisco NCS 4206
- Cisco ASR 903 RSP/RSP1

Y.1564 パフォーマンス テストの実行

EVC で Y.1564 パフォーマンス テストを実行するには、次の手順を実行します。

始める前に

ME1200 デバイス上の EVC で Y.1564 パフォーマンス テストを実行するには、テストを実行する前に、送信元と宛先のインターフェイスの両方に、次の QoS 設定を入力します。

```
Interface <interface-name>
qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
```

ステップ 1 **[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択して、[ネットワーク トポロジ（Network Topology）] ページを開きます。

ステップ 2 ツールバーから、[デバイス グループ（Device Groups）] をクリックして、[デバイス グループ（Device Groups）] ポップアップ ウィンドウを開きます。

ステップ 3 テストする回線/VC を含むデバイス グループの位置を確認してクリックし、ポップアップ ウィンドウを閉じます。

ステップ 4 [回線/VC（Circuits/VCs）] タブをクリックし、該当するサービスの位置を確認して、そのサービスの [i]（[情報（Information）]）アイコンをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを開きます。

ステップ 5 ビューの右上隅から、**[アクション（Actions）] > [Y.1564 テスト（Y.1564 Test）]** の順に選択して、Y.1564 パフォーマンス テストの設定ページを開きます。

（注） このテストは、デバイスの [Device 360（デバイス 360）] ビューの [回線/VC（Circuits/VCs）] タブおよび [回線/VC & ネットワーク インターフェイス（Circuits/VCs & Network Interfaces）] ページからも開始できます。デバイス グループの回線/VC を表示する （813 ページ）および回線/VC の表示 （137 ページ）を参照してください。

ステップ 6 パフォーマンス テストの設定を行います。

a) [テスト モード（Test Mode）] フィールドで、適切なオプション ボタンをクリックして、パフォーマンス テストを片方向または双方向のどちらにするかを指定します。双方向テストの場合、ループバックは宛先デバイスのサービス インスタンスに作成されることに注意してください。

b) [エンドポイント（End Points）] 領域で、ドロップダウン リストから送信元と宛先デバイス、インターフェイス、および EFP ID 選択します。

c) [サービス設定テスト（Service Configuration Test）] 領域で、各反復の間隔、生成するパケット サイズ、およびトラフィックを生成するレートを指定します。

- [CIR/EIR] オプションボタンを選択する場合、設定情報レート（CIR）および超過情報レート（EIR）の値（キロビット/秒）を指定します。CIR は長期の平均転送速度で、EIR は長期の平均超過転送速度です。
- [カラー認識テスト（Color Aware Test）] チェックボックスをオンにした場合は、[適合アクション（Conform Action）] と [超過アクション（Exceed Action）] に対して、0 ～ 7 のサービス クラス（CoS）値を指定します。トラフィックを区別して優先順位を付けるため、[適合アクション（Conform Action）] と [超過アクション（Exceed Action）] には異なる CoS 値を設定する必要があります。また、コミット済みバースト サイズ（CBS）と超過バースト サイズ（EBS）の値（1 秒あたりのキロバイト数単位）を指定して、CIR を上回る一時的なレートでバーストで送信できるコミット済みトラフィックまたは超過トラフィックを定義することもできます。

  （注） [カラー認識テスト（Color Aware Test）] チェックボックスは、10G ポートを搭載した FPGA 対応デバイスでのみ有効になります。「カラー認識」は、顧客が緑色または黄色として各フレームをマークするモードを説明するために使用され、帯域幅プロファイリングおよびトラフィック ポリッシング時にネットワークはこのマーキングを考慮します。

- [ステップ ロード CIR（Step Load CIR）] チェックボックスをオンにすると、4 つの異なるレベル（指定した CIR 値の 25 %、50 %、75 %、100 %）でテストのトラフィックが生成されます。このオプションは、CIR の値を 8 kbps 未満に設定する場合は使用できません。
- [カスタム レート（Custom Rates）] オプション ボタンを選択する場合、デフォルトで 1000 kbps に設定されます。必要に応じて、この値を変更します。
- 片方向のパフォーマンステストを実行する場合、指定できるのはカスタム トラフィック レートのみとなります。

d) [サービス合否基準（Service Acceptance Criteria）] 領域で、許容するフレーム損失率の最高値（パーセント）を [FLR] フィールドに入力します。

- また、フレームの転送遅延（FTD）およびフレームの遅延変動（FDV）の値を設定するには、該当するチェックボックスをオンにし、適切な値を（ミリ秒単位で）入力します。

  （注） [FTD] および [FDV] チェックボックスは、10G ポートを搭載した FPGA 対応デバイスでのみ有効になります。

- パフォーマンス テスト中に、設定したいずれかのしきい値を超えた場合、EVC はテストに失敗したと判定されます。

e) （オプション）[フレーム設定（Frame Settings）] 領域で、次のパラメータの値を指定します。

- [IP バージョン（IP version）]：IPv4 または IPv6
- [内部および外部 VLAN ID（Inner and outer VLAN ID）]：テストする VLAN ID の送信元と宛先を識別します

ステップ 7 [テストを実行（Run Test）] をクリックします。

テストが完了すると、[Y.1564 パフォーマンス テスト設定（Y.1564 performance test settings）] ページの下部に結果が表示されます。

EVC の Y1731 に基づくパフォーマンス テスト

Y.1731 パフォーマンス モニターリング（PM）では、イーサネットのフレーム遅延、フレーム遅延変動、フレーム損失、フレーム スループット測定など、標準的なイーサネット PM 機能が提供されます。これらの測定は ITU-T Y-1731 標準で規定され、メトロ イーサネット フォーラム（MEF）標準グループによって認定されています。このテストを使用して、たとえば回線/VC の遅延および損失プローブの状態、遅延および損失プローブの可用性、双方向の遅延、双方向のジッター、転送損失、逆方向の損失など、遅延および損失の測定値を確認できます。

（注） このパフォーマンス テストがサポートされているのは、Cisco IOS、IOS-XR、および IOS-XE デバイスのみです。

始める前に

回線/VC の Y.1731 に基づくパフォーマンス テストを実行するには、以下の前提条件を満たす必要があります。

- 参加デバイスと併せ、パフォーマンス テストを実行する回線/VC が運用状態でなければなりません。
- 回線/VC に参加するすべてのデバイスについて、MEP ID がドメイン名に一致することを確認します。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックし、テスト対象の回線/VC がある場所を選択します。

ステップ 3 [ネットワーク トポロジ（Network Topology）] ウィンドウで [回線/VC（Circuits/VCs）] をクリックします。

ステップ 4 対象の回線/VC を見つけて、その情報アイコンをクリックして回線/VC の 360 度ビューにアクセスします。

ステップ 5 **[アクション（Actions）] > [Y.1731 テスト（Y.1731 Test）]** の順に選択します。

（注） 回線/VC の詳細ウィンドウおよび展開した回線/VC リストからパフォーマンス テストを開始することもできます。デバイス グループの回線/VC を表示する （813 ページ）および回線/VC の表示 （137 ページ）を参照してください。

ステップ 6 必要な送信元および宛先デバイスと、それぞれに対応するインターフェイスを選択します。

ステップ 7 [CoS] ドロップダウン リストから、プローブの優先順位を選択します。デフォルト値は 0 です。

ステップ 8 必要な測定タイプを選択します。オプションは [遅延（Delay）]、[損失（Loss）]、[損失と遅延（Loss & Delay）] です。

（注） 遅延測定は遅延測定メッセージ（DMM）プローブを使用して実行され、損失測定は合成損失測定メッセージ（SLM）プローブにより実行されます。ASR 1K デバイスの場合、損失測定メッセージ（LLM）プローブを使用した遅延測定のみがサポートされています。

ステップ 9 必要に応じて、次の詳細なパフォーマンス テスト パラメータを定義します。

- [プローブの長さ（Probe Length）]：プローブの長さ（秒数）を選択します。たとえば、プローブの長さを 30 秒に設定すると、統計データは 30 秒間隔で収集されてテスト結果領域に表示されます。
- [パケットサイズ（Packet Size）]：各プローブで送信するパケットのサイズ（バイト数）を入力します。
- [バースト間隔（Burst Interval）]：バースト間隔（秒数）を選択します。この設定により、プローブでパケットのセットを送信してから次のパケットのセットを送信するまでの間隔が定義されます。
- [パケット間隔（Packet Interval）]：パケット間隔（ミリ秒数）を選択します。この設定により、バーストでパケットを送信してから次のパケットを送信するまでの間隔が定義されます。
- [パケット数（Packet Count）]：バーストで送信するパケットの数を入力します。

  たとえば、バースト間隔、パケット間隔、パケット数をそれぞれ 30 秒、1000 ミリ秒、10 に設定すると、1000 ミリ秒間の送信間隔でパケットが 1 つずつ 10 個送信されます。10 個のパケットがすべて送信されると、30 秒の間隔をおいてから、次の 10 個のパケットのセットが送信されます。

ステップ 10 [テストを実行（Run Test）]をクリックします。テストが完了すると、[パフォーマンステスト（Performance Test）] ページの下部にある [テスト結果（Test Results）] 領域にテスト結果が表示されます。

光回線のパフォーマンス テスト

Cisco EPN Manager の光回線用パフォーマンス テストは、G.709 と G.798 で規定された ITU-T 推奨事項に基づいています。

Cisco EPN Manager は、次の光回線用のパフォーマンス テストをサポートします。

- オプティカル パフォーマンス モニターリング パラメータ （853 ページ）
- 回線（ODU UNI）での PRBS テストの実行 （854 ページ）

オプティカル パフォーマンス モニターリング パラメータ

光信号の質をモニターするオプティカル パフォーマンス モニターリング パラメータは、光回線でエンドポイント間で送受信される平均光パワーを測定するために使用されます。これらの測定から、チャネルプレゼンスの検証、チャネルの波長、ASE のノイズ、光信号の強度、光信号対雑音比（OSNR）、電気信号対雑音比（eSNR）などの重要なネットワーク パフォーマンス パラメータをチャネルごとに確認できます。したがって、これらのパラメータを使用してネットワークの信頼性とサービス品質を管理することができます。

光回線のパフォーマンス モニターリング パラメータを表示するには、次の手順に従います。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 テスト対象の回線/VC が含まれるデバイス グループを選択します。

ステップ 3 左側の [回線/VC（Circuits/VCs）] ペインで必要なサービスの位置を確認し、[i] アイコンをクリックして [回線/VC 360（Circuits/VC 360）] ビューにアクセスします。

ステップ 4 **Actions > Optical PM Parameters** を選択します。

（注） 回線/VC の詳細ウィンドウおよび展開した回線/VC リストからパフォーマンス テストを開始することもできます。デバイス グループの回線/VC を表示する （813 ページ）および回線/VC の表示（137 ページ）を参照してください。

ステップ 5 表示するパフォーマンス データに基づいてオプティカル モニターリングのタイプを選択します。オプティカル モニターリングのタイプと関連するパフォーマンス カウンタの詳細については、光モニターリング ポリシーのパフォーマンス カウンタ （1210 ページ）を参照してください。

ステップ 6 デバイスからパフォーマンス データを収集するパフォーマンス モニターリング時間間隔として、15 分または 24 時間を選択します。

ステップ 7 パフォーマンス データを自動的に更新する時間間隔を指定します。

ステップ 8 **Auto Refresh** をクリックします。回線のパフォーマンス データは、表形式で表示されます。パフォーマンス データの詳細については、光モニターリング ポリシーのパフォーマンス カウンタ （1210 ページ）を参照してください。

パフォーマンス データを更新するために指定した時間間隔に基づいて、新しく取得されたデータが表の先頭に表示されます。たとえば、時間間隔を 10 行秒に指定した場合、パフォーマンス データは 10 秒ごとに自動的に更新されて、新しく取得されたデータが表の先頭に表示されます。表には、取得されたパフォーマンス データの最後の 20 件のエントリが表示されます。

回線（ODU UNI）での PRBS テストの実行

タイプ ODU UNI の OTN 回線向けの PRBS テストがサポートされます。PRBS のビットエラーカウントで、エンドポイント間のリンクの信頼性を測定します。このテストは NCS4K-20T-O-S カード向けにサポートされています。PRBS テストを 2 つのエンドポイント間（ODU コントローラまたはサブ コントローラ）で実行すると、送信元デバイスから、1 つ以上のミッドポイント（中間コントローラまたはサブコントローラ）を通じてビットパターンが送信され、同じビットパターンが宛先デバイスで受信され、テスト結果は両方のエンドポイントで表示できます。また、相手側のエンドポイントをループバック、ソース、またはソースシンクとして設定して、コントローラで PRBS テストを実行できます。

ODU コントローラに PRBS を設定する方法の詳細は、ODU コントローラ上の PRBS の設定（454 ページ）を参照してください。

光回線に PRBS のパフォーマンス テストを実行するには、次の手順に従います。

ステップ 1 左側のサイドバーから、**[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 テストするタイプ ODU UNI の回線/VC を含むデバイス グループを選択します。

ステップ 3 左側の [回線/VC（Circuits/VCs）] ペインで必要なサービスの位置を確認し、[i] アイコンをクリックして [回線/VC 360（Circuits/VC 360）] ビューにアクセスします。

ステップ 4 **[アクション（Actions）]** > **[PRBS テスト (PRBS Test)]** を選択します。

ステップ 5 権限をエンドポイントに割り当てるには、[エンドポイント（Endpoint）]テーブルで、エンドポイントの権限をクリックし、ドロップダウン リストから次のオプションのいずれかを選択します。

- [ソース（SOURCE）] : この権限を A または Z のいずれかの側に設定する。
- [シンク（SINK）] : この権限を A または Z のいずれかの側に設定する。
- [ソースシンク（SOURCESINK）] : この権限を A または Z のいずれかの側か、両方に設定する。
- [無効（INVALID）] : エンドポイントで PRBS を無効にする。

ステップ 6 パターンをエンドポイントに指定するには、[エンドポイント（Endpoint）]テーブルで、エンドポイントのパターンをクリックし、ドロップダウン リストから希望のパターンを選択します。

NCS4K-20T-O-S カードでは、次のパターンがサポートされます。

- PRBS 31
- PRBS 31 反転
- PRBS 11
- PRBS 11 反転

ステップ 7 ループバック モード変更するには、[ループバック（Loopbacks ）] テーブルで、エンドポイントまたはミッドポイントのループバック モードをクリックし、ドロップダウンから次のオプションのいずれかを選択します。

- [ループバックなし（NO_LOOPBACK）] : ループバックなしのテスト。
- [内部（INTERNAL）] : 同じネットワーク内のテスト。
- [回線（LINE）] : 異なるネットワーク間のテスト。

ステップ 8 [テスト結果（Test Results）] 領域で、[シンク コントローラ（Sink Controller）] ドロップダウン リストからエンドポイントを選択します。

ステップ 9 次のいずれかの [間隔（Interval）] オプション ボタンをクリックし、時間間隔を設定してデバイスからのデータを収集します。

- [現在（Current）]（10 秒ごと）：過去 15 分の結果を 10 秒ごとに表示します。
- [15 分（15 Minutes）] : 過去 15 分のパフォーマンス データの履歴を表示します。
- [1 日（1 Day）] : 過去 1 日のパフォーマンス データの履歴を表示します。

ステップ 10 [移動（Go）] をクリックします。

ステップ 11 [自動更新（Auto Refresh）] をクリックします。エンドポイントのテスト結果は、ビットエラーカウント、パケットの損失と検出のタイムスタンプ、パケットの損失と検出の数を含むテーブルとして表示されます。

テストを更新するための指定した時間間隔に基づいて、新しく取得したデータがテーブルの先頭に表示されます。たとえば、指定した時間間隔が 10 秒の場合、データは 10 秒ごとに自動的に更新され、新しく取得したデータがテーブルの先頭に表示されます。

回線エミュレーション サービスのパフォーマンス テスト

ビット エラー レート テスト（BERT）を使用すると、現場でケーブルをテストして、信号の問題を診断できます。このテストメカニズムは、Cisco NCS 42xx シリーズ（T1/E1 ポートと T3/E3 ポート）でサポートされています。このテストでは、回線コントローラの発信データストリームに特定のパターンを生成し、着信データストリームで同じパターンを分析します。予期されるパターンに一致しないビットはビット エラーとしてカウントされます。

ビットエラーレートは、受信されたエラービットと受信された合計ビット数を比較することで決定されます。回線で送信されたエラー ビットの合計数と、受信されたビットの合計数を表示して分析することができます。テスト中にいつでもエラー統計を取得できます。

次の表に、Cisco NCS 42xx シリーズ（T1/E1 ポートと T3/E3 ポート）デバイスでサポートされているテストパターンを示します。

BERT パターン	**説明**
2^11	2,048 ビットで構成される、疑似ランダム繰り返しテスト パターン。
2^15	32,767 ビットで構成される、疑似ランダム繰り返しテスト パターン。
2^20-O151	1,048,575 ビットで構成される、疑似ランダム繰り返しテスト パターン。
2^20-O153	1,048,575 ビットで構成される、疑似ランダム繰り返しテスト パターン。
2^23	長さ 8,388,607 ビットの疑似ランダム 0.151 テスト パターン。
2^9	疑似乱数 0.151 テストパターン。長さは 511 ビットです。

CEM 回線の BERT パフォーマンス テストを実行するには、次の手順を実行します。

ステップ 1 左側のサイドバーから、**[インベントリ（Inventory）] > [その他（Others）] > [回線/VC およびネットワーク インターフェイス（Circuits/VCs & Network Interfaces）]** を選択します。

ステップ 2 [回線/VC（Circuits/VCs）] タブで、必要な CEM サービスを見つけて [i] アイコンをクリックし、その [回線/VC 360（Circuit/VC 360）] ビューにアクセスします。[回線/VC 360（Circuit/VC 360）] ビューで、**[アクション（Actions）]** > **[パフォーマンス テスト（Performance Test）]** > **[BERT]** を選択します。

または、**[マップ（Maps）]** > **[トポロジマップ（Topology Maps）]** > **[ネットワークトポロジ（Network Topology）]** および [回線/VC（Circuits/VCs）] ペインからこのページを開き、必要な CEM 回線の [回線/VC 360（Circuit/VC 360）] ビューにアクセスすることもできます。

ステップ 3 [テスト（Test）] タブで、テストの方向（送信元および宛先）を選択します。

送信元および宛先を選択すると、理解しやすいように、回線のテストが図で表されます。

ステップ 4 ループバックタイプを選択します。

[リモート側で設定されたループバックの使用（Use configured loopback on remote side）] または **[リモートループバックのローカルでの使用（Use remote loopback locally]** を選択できます。

ステップ 5 定義された時間間隔で自動的にテストデータを更新するには、[設定（Settings）] エリアに時間間隔を分単位で入力します。

ステップ 6 [BERT パターン（BERT Pattern）] ドロップダウン リストからパターンを選択します。

ステップ 7 [テストを実行（Run Test）] をクリックします。テスト結果が [テスト結果（Test Results）] 領域に表示されます。回線エミュレーション サービスのパフォーマンス テストの結果を表示してエクスポートする （857 ページ）を参照してください。

ステップ 8 テストを終了するには、[設定（Settings）] 領域で [停止（Stop）] をクリックし、[カウンタのクリア（Clear Counters）] をクリックして [テスト結果（Test Results）] 領域の値をリセットします。

SONET インターフェイスの場合、テストを終了したら [Clear Counters] ボタンは無効になります。

回線エミュレーション サービスのパフォーマンス テストの結果を表示してエクスポートする

BERT パフォーマンス テストは、一度に、任意の数の CEM 回線に対して実行できますが、1 つの CEM 回線に対して実行できるテストは 1 つだけです。CEM 回線に対する BERT パフォーマンス テストの結果は、[テスト結果（Test Results）] 領域に表示されます。

- いずれかの時点で、CEM 回線に対して最後に実行された/現在実行中の BERT パフォーマンス テストの結果が、[テスト（Test）] タブの [テスト結果（Test Results）] 領域に表示されます。
- [自動更新（Auto refresh）] が有効（オン）になっている場合は、テスト結果が指定された間隔で自動更新されます。
- [テスト結果（Test Results）] 領域では、次のようになります。
  - テストの宛先として管理対象外エンドポイントが選択されている場合は、テスト結果が表示されません。

- 宛先として管理対象エンドポイントが選択されている場合は、エンドポイントごとに 2 組のテスト結果が表示されます。

- **[モニター（Monitor）] > [パフォーマンス テスト（Performance Tests）] > [BERT（BERTs）]** を選択します。ここでは、CEM 回線ごとに 1 つのエントリのみを使用でき、その CEM 回線に対して最後に実行されたテストと現在実行中のテストのどちらかが表示されます。テスト結果を表示する必要のある CEM 回線を選択します。
- 特定の CEM 回線の BERT パフォーマンス結果の履歴を表示するには、[履歴（History）] タブで、[テスト（Test）] ドロップダウン リストから必要なテストを選択して、設定とその結果を表示します。

BERT パフォーマンス テストの結果は、BERT ページ（[回線/VC 360（Circuit/VC 360）] ビューで、**[アクション（Actions）] > [パフォーマンス テスト（Performance Test）] > [BERT]** を選択）の [テスト（Test）] タブと [履歴（History）] タブの右上にあるエクスポート アイコンをクリックすることによってエクスポートできます。

また、次のページから BERT パフォーマンス テストのリストをエクスポートすることもできます。

- [BERT テストの選択（Select BERT Test）] ポップアップ ウィンドウ（[BERT] ページで、[履歴（History）] タブをクリックしてから、[テスト（Test）] ドロップダウン リストをクリックして [BERT テストの選択（Select BERT Test）] ポップアップ ウィンドウを開きます）。
- BERT リスト ページ（**[モニター（Monitor）] > [パフォーマンス テスト（Performance Tests）] > [BERT（BERTs）]** を選択します）。

回線/VC のパフォーマンス測定指標とレポートを表示する

[回線/VC 360（Circuit/VC 360）] ビューは、回線の最新の履歴に関する情報を提供します。一方、レポートは、データベースに保存されたすべての履歴データを取得できます。リアルタイム情報については、パフォーマンス テストを実行します（回線/VC のパフォーマンス テストの実行 （848 ページ）を参照）。

- [回線/VC 360（Circuit/VC 360）] ビューでパフォーマンス グラフを表示する （859 ページ）
- パフォーマンス レポートを使用した回線/VC のモニターおよびトラブルシューティング （859 ページ）
- サービス パフォーマンス ダッシュボードを使用して回線/VC をモニターする （860 ページ）

[回線/VC 360（Circuit/VC 360）] ビューでパフォーマンス グラフを表示する

[回線/VC 360（Circuit/VC 360）] ビューには、回線/VC のパフォーマンスのさまざまな側面を示すグラフが表示されます。このビューでは、回線/VCのパフォーマンスに大きな問題があるかどうかを一目で確認できます。詳細については、回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー （803 ページ）を参照してください。

[回線/VC 360（Circuit/VC 360）] ビューにアクセスするには：

ステップ 1 左側のサイド バーから **[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択します。[ネットワーク トポロジ（Network Topology）] ウィンドウが開きます。[ネットワーク トポロジ（Network Topology）] ウィンドウとその機能の詳細については、「ネットワーク トポロジの視覚化 （219 ページ）」を参照してください。

ステップ 2 左側の [場所（Locations）] ペインで、必要な回線/VC が作成されたデバイス グループを選択します。

ステップ 3 [回線/VC（Circuits/VCs）] ペインで、必要な回線/VC を見つけて、その回線/VC 名の横にある [i] アイコンをクリックします。[回線/VC 360（Circuit/VC 360）] ビューが別のポップアップ ウィンドウに表示されます。

パフォーマンス レポートを使用した回線/VC のモニターおよびトラブルシューティング

Cisco EPN Manager は、光回線と EVC に関する詳細なパフォーマンス情報を得ることができる詳細に及ぶレポート機能を提供します。[レポート起動パッド（Report Launch Pad）] では、すべての Cisco EPN Manager レポートにアクセスできます。[レポート起動パッド（Report Launch Pad）]から、新しいレポートの作成と保存、現在のレポートの表示、特定タイプのレポートのオープン、後で実行するレポートのスケジューリング、およびレポートの結果のカスタマイズを実行できます。

左側のナビゲーション ペインで、**Reports > Report Launch Pad** を選択し、レポートとレポート機能にアクセスします。

キャリアイーサネットのパフォーマンス レポートについては、キャリアイーサネット パフォーマンス レポート （356 ページ）を参照してください。

光回線のパフォーマンス レポートについては、光パフォーマンス レポート （367ページ）を参照してください。

サービス パフォーマンス ダッシュボードを使用して回線/VC をモニターする

サービス パフォーマンス ダッシュボードは、一定期間の選択された回線/VC のパフォーマンス測定結果をさまざまなグラフ形式と表形式で表現します。この情報は、カスタマイズされたダッシュレットの形式で使用できます。ダッシュボード メニューから、使用可能なすべての Cisco EPN Manager ダッシュボードにアクセスできます。

サービス パフォーマンス ダッシュボードの [回線/VC（Circuits/VCs）] ドロップダウン リストから回線/VC を選択して、次の情報（ダッシュレット）を表示する必要があります。

- 一定期間のサービス エンドポイントの平均可用性。
- 指定した期間のサービスの bps 単位で測定された着信トラフィックと発信トラフィック。
- 一定期間のサービス エンドポイント間の平均遅延。
- 一定期間のサービス エンドポイント間の平均パケット損失率。
- 着信トラフィックと発信トラフィックが最も高いサービスのリスト。

[回線/VC 360（Circuit/VC 360）] ビューから特定のサービス用のダッシュボードを起動するには、**[表示（View）]** をクリックしてから、**[ダッシュボード（Dashboard）]** を選択します。

サービス パフォーマンス ダッシュボードおよびダッシュレットの詳細については、[サービス パフォーマンス（Service Performance）] ダッシュボードの概要 （8 ページ）を参照してください。

ダッシュボードとダッシュレットの管理方法については、Cisco EPN Manager スタートアップ ガイド （1 ページ）を参照してください。

回線/VC の完全なルートをトレースおよび可視化する

回線をグラフィカルに視覚化するには、[多層トレース（Multilayer Trace）] ビュー（MLT）を使用します。このビューには、2 つのエンドポイント間の完全な回線スパンとサービストレースが表示されます。このビューでは、送信元ノード、宛先ノード、および中間ノードをグラフィック形式で表示することによって、回線の接続をトレースできます。

次の点に注意してください。

- [マルチレイヤトレース（Multilayer Trace）] ビューは、マルチポイント キャリア イーサネット回線/VC、シリアル（raw ソケット）および L3VPN サービスではサポートされていません。
- 光回線の [多層トレース（Multilayer Trace）] ビューは、A エンド デバイスで LMP が設定されている場合、および光回線に参加しているデバイス間で LMP が設定されている場合にのみ起動できます。

- MPLS-TE および SR-TE トンネルの場合、[多層トレース（Multilayer Trace）] ビューには物理トポロジが必要です。これは、CDP や LLDP などのサポートされているプロトコルのいずれかを使用して物理リンクが検出済みである必要があることを意味します。

回線の完全なルートをトレースして可視化するには：

ステップ 1 左側のサイドバーから **[マップ（Maps）]** > **[トポロジ マップ（Topology Maps）]** > **[ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイス グループ（Device Groups）] をクリックし、必要な回線/VC が作成された場所を選択します。

ステップ 3 [ネットワーク トポロジ（Network Topology）] ページで [回線/VC（Circuits/VCs）] をクリックします。選択したデバイス グループに関連付けられている回線/VC が一覧表示されます。

ステップ 4 完全なルートを表示する回線/VC を選択します。回線のオーバーレイがマップ上に表示されます。

ステップ 5 次のいずれかの方法で [多層トレース（Multilayer Trace）] ビューに切り替えます。

- トポロジ ツールバーのすぐ下に表示されている通知の [多層トレース（Multilayer Trace）] ハイパーリンクをクリックします。

  （注） [マルチレイヤトレース（Multilayer Trace）] ハイパーリンクが表示されるのは、選択した回線/VC で [マルチレイヤトレース（Multilayer Trace）] ビューがサポートされている場合、かつ回線/VC のプライマリの状態が [欠落（Missing）] または [ダウン（Down）] でない場合のみです。

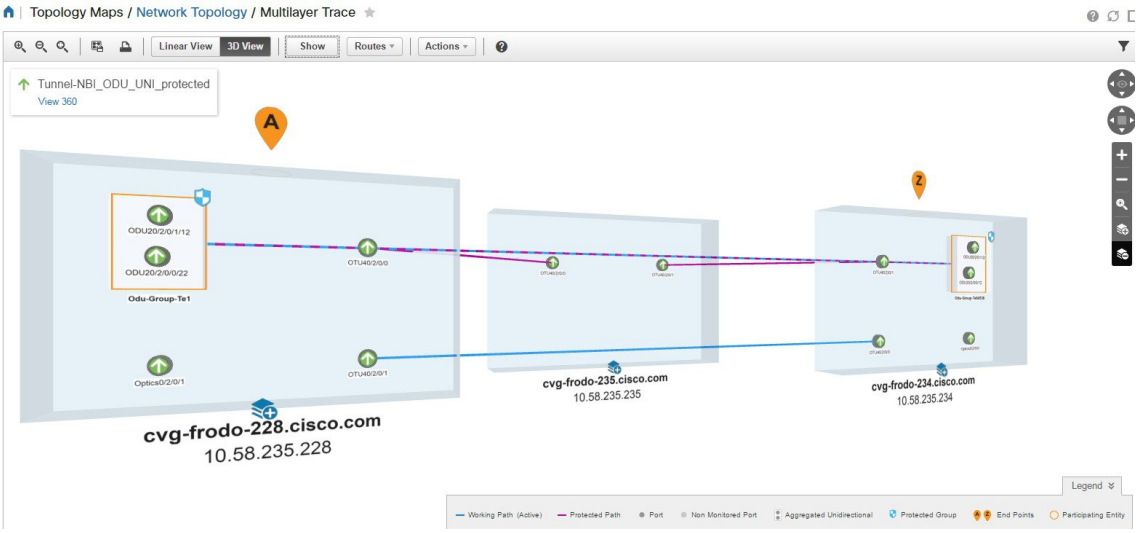
  回線/VC の完全なルートが完全にモデル化されていない場合や、ルートが切断されている場合でも、マルチレイヤ トレースは部分的に表示できます。エラーを解決するために、根本原因と推奨事項を特定できます。

- 回線/VC の横にある情報アイコンをクリックして [回線/VC 360（Circuit/VC 360）] ビューを開き、**View>Multilayer Trace** をクリックします。

選択した回線/VC が簡略 3 次元ビューで表示されます。簡略ビューでは、参加デバイスの送信元と宛先のエンドポイントのみが表示されます。回線/VC のさまざまな層を展開したり、折りたたんだりすることができます。回路の種類によっては、エンドポイント間のルート方向のアニメーションが表示されます。詳細については、[多層トレース（Multilayer Trace）] ビューに回路の特定の情報を表示する（865 ページ）を参照してください。

（注） 回線のトラバースが複数回行われる（入出力接続数が多い）デバイスの場合は、3 次元ビューでも線形ビューでも折りたたみオプションを使用できません。

次の図は回線/VC の簡略ビューです。展開オプションと折りたたみオプションがあります。



3 次元ビューで表示される情報の詳細については、「回線 V/C トレースの 3 次元表示 （863 ページ）」を参照してください。

線形ビューに切り替えるには、[線形表示（Linear View）] をクリックします。線形ビューで表示される情報の詳細については、「回線/VC トレースの線形表示 （865 ページ）」を参照してください。

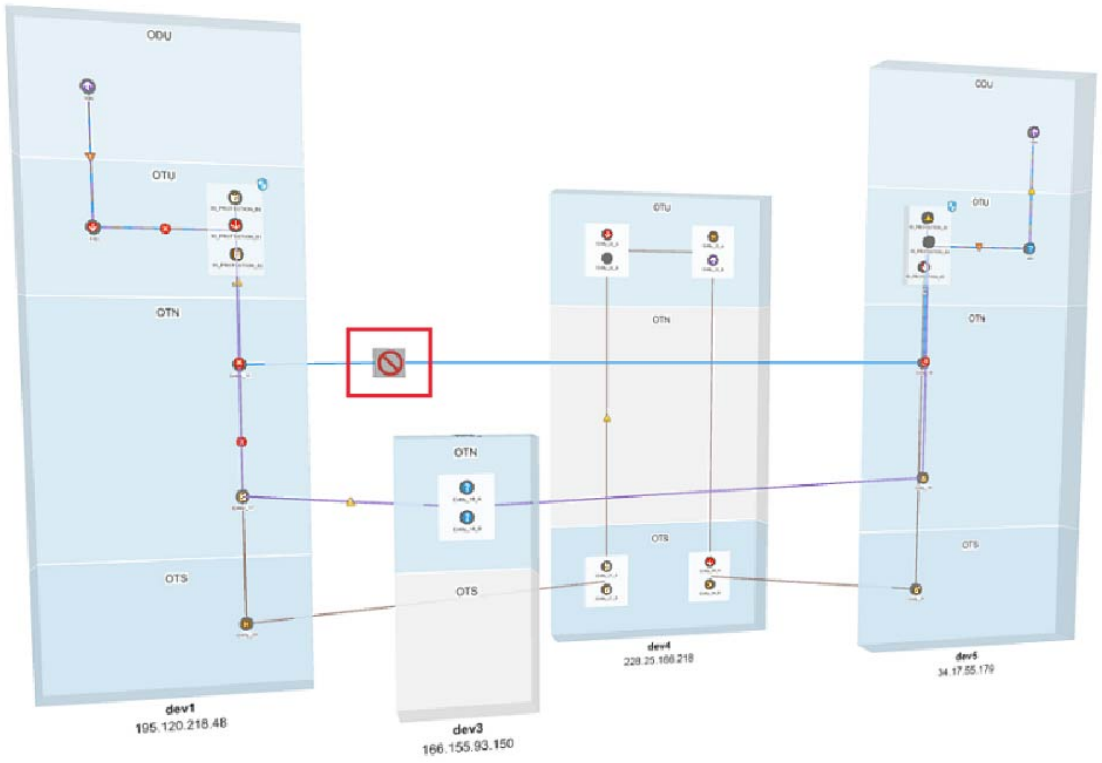
[多層トレース（Multilayer Trace）] ビューには、次のようなグラフィカル マップが表示されます。

- NE やリンクなどのハイレベル スパン情報を使用して回線トレースが表示されます。
- マップ上で論理リンクを使用して回線がトレースされた論理ハイレベルビューが表示されます。たとえば、OCHCC 回線ではトレースに OCH トレールリンクが使用されます。
- マップ上で物理リンクを使用して回線がトレースされた物理ハイレベルビューが表示されます。たとえば、OCHCC 回線ではトレースに OTS リンクが使用されます。
- 選択した回線に関係なく、デバイス上で最も重大なアラームを表すデバイスのバッジが表示されます。トレースビュー内のアラームバッジには、各エンティティ（リンク、ノード、ポイントなど）のアラームが表示されます。
- 選択したハイレベル ビューに応じてリンクが強調表示されます。
- 回線内の各層は異なるシェードで強調表示され、層の間を区分する境界線が表示されます。デバイスに適用できない層は、灰色で表示されます。
- [多層トレース（Multilayer Trace）] ビューには折りたたみ可能な凡例が表示され、そこに各種アイコンとその説明が一覧表示されます。
- 光回線の場合は、回線に含まれるデバイスまたはリンクに共有リスク リソース グループ（SRRG）が割り当てられているかどうかが示されます。リンクまたはデバイス上の SRRG ラベルをクリックすると、そのリンク/デバイス上のすべての SRRG が一覧表示されます。

SRRG は、デバイス上のデフォルトか、割り当て済みか、未割り当てかに基づいて色分けされます。疑問符アイコンをクリックすると、凡例が表示されます。

- OCHCC 回路の場合、送信元または送信先のノードと DWDM コントローラ間の LMP のリンクが表示されます。

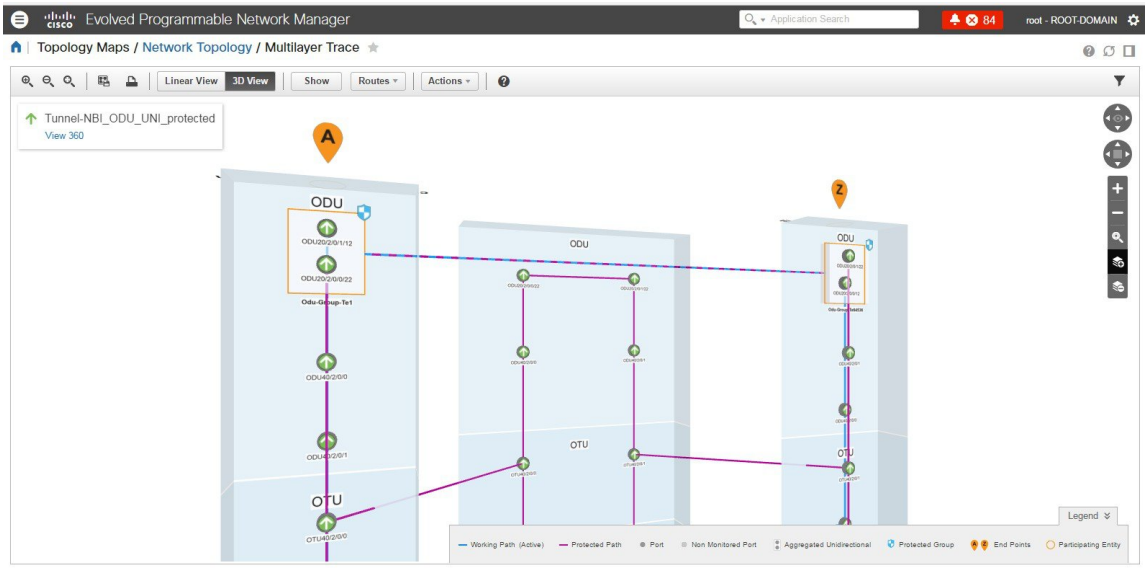
回線/VC に参加している 1 つ以上のデバイスが仮想ドメインの一部ではない場合、多層トレースは部分的なものになります。[多層トレース（Multilayer Trace）] ビューには、アクセスできないデバイスの代わりに、アクセスできないデバイスのアイコンが表示されます（下図を参照）。



回線 V/C トレースの 3 次元表示

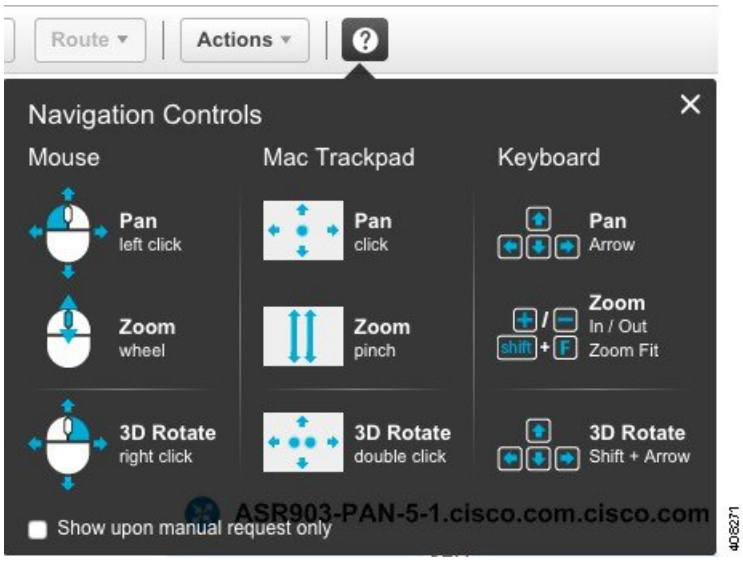
これはデフォルト ビューです。回線/VC の完全なルートの 3 次元ビューが表示されます。このビューへのアクセス方法については、回線/VC の完全なルートをトレースおよび可視化する（860 ページ）を参照してください。

このビューには、選択された回線に使用可能なさまざまなパスが表示されます。たとえば、光回線に現用パス、保護されたパス、および回復パスが存在する場合は、このビュー内でそれぞれのパスが色分けされて表示されます。



3 次元ビューのナビゲーション コントロールについて調べるには、ツールバーのヘルプ アイコンをクリックします。ナビゲーション コントロール データ ポップアップ ウィンドウに、このビュー内でパン、ズーム、および回転するためのマウス、MAC トラックパッド、およびキーボード コントロールが表示されます。

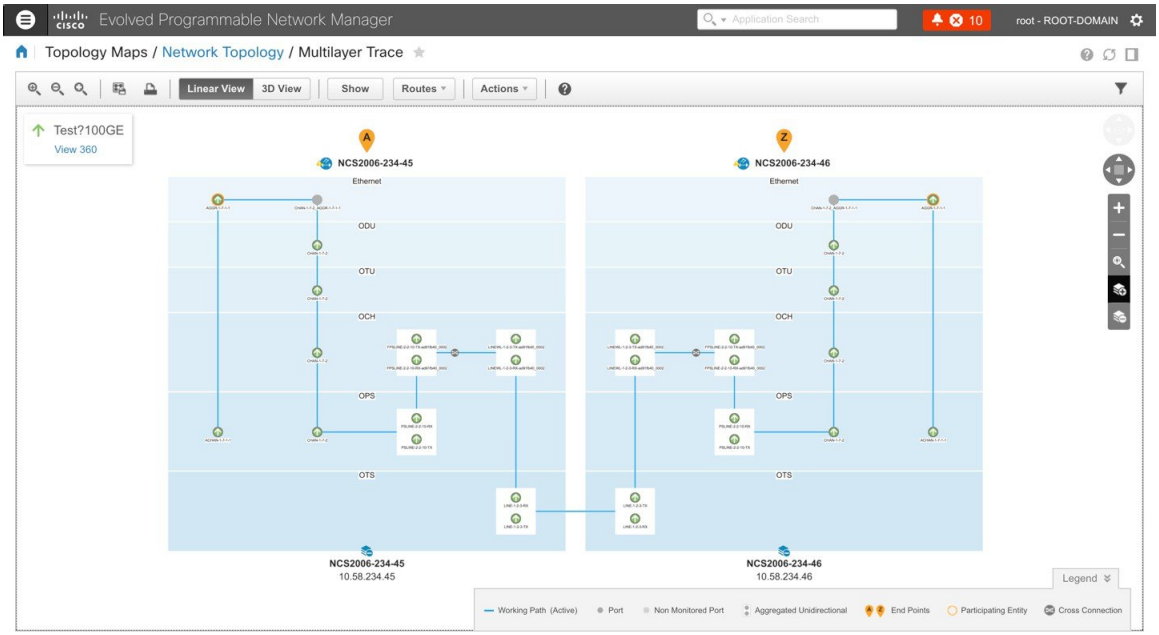
（注） MAC トラックパッド コントロールは、MAC ユーザーの場合にのみ表示されます。



回線/VC トレースの線形表示

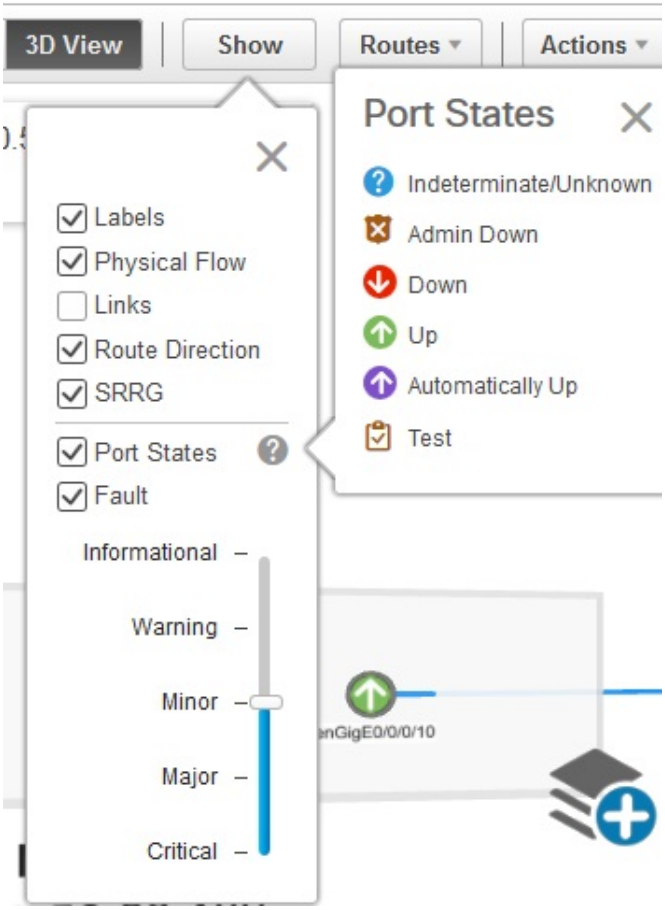
線形表示を使用して、回線/VC のルートを 2 次元表示でトレースおよび視覚化できます。このビューへのアクセス方法については、回線/VC の完全なルートをトレースおよび可視化する（860 ページ）を参照してください。

この表示には、回線のパスが一度に 1 つだけ表示されます。[ルート（Route）] を選択してから、[処理中（Working）]、[保護（Protected）]、または [復元（Restored）] を選択して回線トレースで必要なパスを表示します。パスのオプションは、選択した回線/VC タイプによって異なります。



[多層トレース（Multilayer Trace）] ビューに回路の特定の情報を表示する

回路の [多層トレース（Multilayer Trace）] ビューで、[表示（Show）] メニューから特定のチェックボックスを有効にすることで表示する情報を選択できます。回路におけるラベル、物理的なフロー、リンク、ルート方向、SRRG、ポート状態、電力レベル、スパン損失および障害の表示を選択することができます。チェックボックスは、選択した回線/VC タイプによって異なります。



ポートのアラーム状態またはプライマリ状態のいずれかを表示できます。ポートのプライマリ状態のアイコンと状態の説明については、ポートまたはインターフェイスの状態（123ページ）を参照してください。

回路のルート方向のアニメーションを表示する [ルート方向（Route Direction）] チェック ボックスは、非対称のパスを持つ回路に対してのみ、デフォルトで有効になります。

- A から Z へのパスを持つ単方向回路。たとえば、単方向の TE トンネル。
- A から Z および Z から A への同一ではないパスを持つ双方向非対称回路。たとえば、単方向 TE トンネル上を通過するキャリア イーサネットまたは CEM 回路。

（注） A から Z および Z から A への完全に同じパスを持つ回路、すなわち双方向対称回路の場合は、[表示（Show）] メニューに [ルート方向（Route Direction）] チェック ボックスが表示されません。

デフォルトでは、A から Z 終端へのルート方向が表示されます。反対方向のアニメーションを表示するには、  アイコンをクリックします。ただし、このアイコンは、A から Z および

ZからAへ異なるパスを持つ回路（双方向非対称回路）に対してのみ有効になります。たとえば、2 つの異なる単方向 TE トンネル上を通過するキャリア イーサネットまたは CEM 回路です。これらの回路ではスイッチ アイコンは表示されません。

- A から Z へのパスを持つ単方向回路。たとえば、単方向の TE トンネル。
- A から Z および Z から A への完全に同じパスを持つ双方向対称回路。たとえば、双方向コア ルーテッド TE トンネル（または Flex LSP）。

フィルタ処理をレイヤに適用すると、[ルート方向（Route Direction）] チェック ボックスは、選択したレイヤに応じて無効になります。一度無効になると、自動で有効にはなりません。ルート方向のアニメーションをもう一度を表示するにはチェック ボックスを手動で有効にする必要があります。

部分的に検出された回路や問題またはサポートされていない回路構成の場合、AからZへのデフォルトのルートの方向は起動しない可能性があります。ただしこれらの回路には、別のパスを通過する潜在的な Z から A 方向がある可能性があります。[エンドポイントの変更（Change Endpoints）] ハイパーリンクをクリックして、エンドポイントを構成し反対方向の [多層トレース（Multilayer Trace）] ビューを起動します。

[マルチレイヤトレース（Multilayer Trace）] ビューから実行できるアクション

[マルチレイヤトレース（Multilayer Trace）] ビューから次の操作を実行できます。

- ラベル、物理的なフロー、リンク、ポートの状態、電力レベル、スパン損失および回線の障害を表示するには、[表示（Show）] を選択し、該当するチェックボックスをオンにします。詳細については、[多層トレース（Multilayer Trace）] ビューに回路の特定の情報を表示する （865 ページ）を参照してください。
- リンク、インターフェイス、または回線にカーソルを合わせると、それぞれリンク名、カード名、または回線名が表示されます。

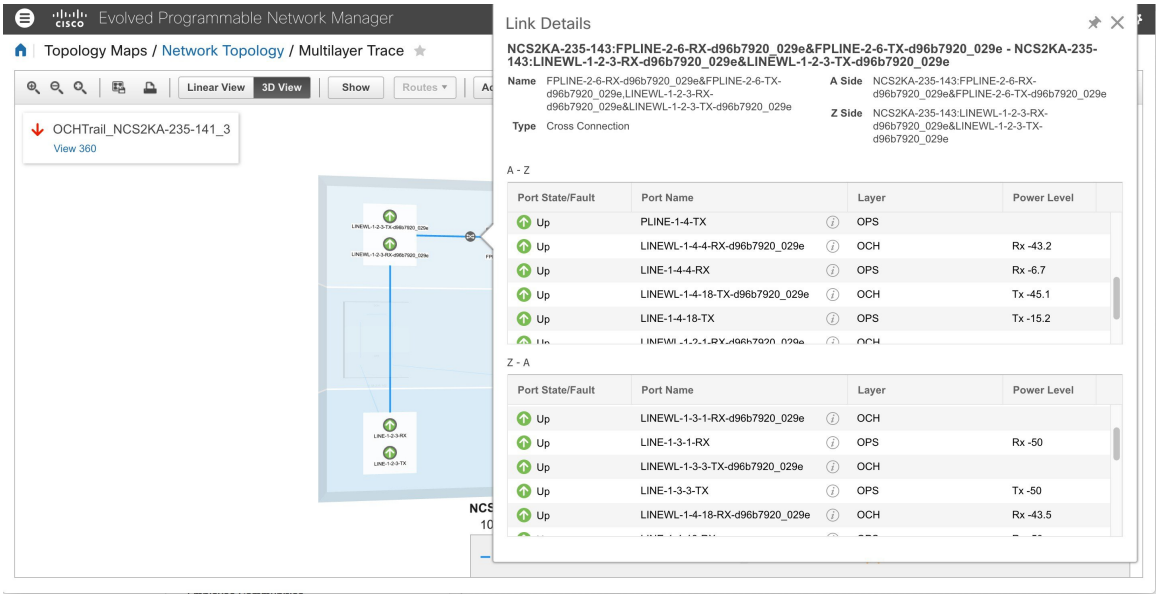
（注） 回線の相互接続インターフェイスの場合、カード名は表示されません。

- [マルチレイヤ トレース（Multilayer Trace）] のツールバーの右下に表示される [ビュー 360（View 360）] ハイパーリンクをクリックし、[回線/VC 360（Circuit/VC 360）] ビューを開きます。回線/VC の情報をすばやく取得する：[回線/VC 360（Circuit/VC 360）] ビュー（803 ページ）を参照してください。
- 回線トレースのポート アイコンをクリックして、[インターフェイス 360（Interface 360）] ビューを開きます。デバイス インターフェイスの概要：[インターフェイス360（Interface 360）] ビュー （129 ページ）を参照してください。

- [デバイス 360（Device 360）] ビューを開くには、デバイスの上部に表示されるデバイス名またはデバイス IP アドレスをクリックします。基本デバイス情報を取得する：[デバイス 360（Device 360）] ビュー （106 ページ）を参照してください。
- [マルチレイヤ トレース（Multilayer Trace）] のリンクをクリックして、[リンク 360（Link 360）] ビューを開きます。特定のリンクの概要：[リンク 360（Link 360）] ビュー （235 ページ）を参照してください。
- 回線トレースの [クロス接続（Cross Connection）] アイコンをクリックし、[リンクの詳細（Link Details）] ポップアップウィンドウを開きます。

（注） [クロス接続（Cross Connection）] アイコンは、内部ポートが回線/VC によって使用されているリンクに表示されます。内部ポートは [マルチレイヤ トレース（Multilayer Trace）] ビューに表示されません。

次の図に、影響を受けている内部ポート、ポートの状態、レイヤ、および電力レベルのリストを表示する [リンクの詳細（Link Details）] ポップアップウィンドウを示します。これらの詳細には、影響を受けているすべての内部ポートのリストが両方向（A 側から Z 側とその逆）で表示されます。

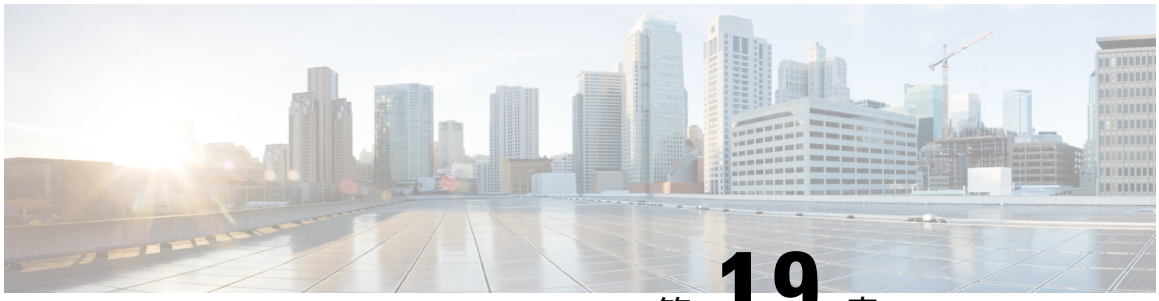


- **Actions > Y.1564 Test** を選択し、CE 回線/VC のエンドツーエンドのパフォーマンスをテストします。Y.1564 パフォーマンス テストの実行 （850 ページ）を参照してください。
- **Actions > BERT** を選択し、回線エミュレーション サービスのパフォーマンスをテストします。回線エミュレーション サービスのパフォーマンス テスト （856 ページ）を参照してください。

- **Actions > Optical PM Parameters** を選択し、光回線/VC のリアルタイムのパフォーマンスモニターリング データを表示します。オプティカル パフォーマンス モニターリング パラメータ （853 ページ）を参照してください。
- **Actions > PRBS Test** を選択し、光回線/VC のエンドツーエンドのパフォーマンスをテストします。回線（ODU UNI）での PRBS テストの実行 （854 ページ）を参照してください。
- **[アクション（Actions）] > [詳細（Details）]** を選択し、回線に関するさらに詳しい説明を表示します。回線/VC に関する総合情報の取得：[回線/VC 詳細情報（Circuit/VC Details）] ウィンドウ （810 ページ） を参照してください。
- **[アクション（Actions）] > [復元アクション（Restoration Actions）] > [アップグレード復元（Upgrade Restore）]** を選択し、障害が発生した光回線をアクティブルートにアップグレードし、障害が発生した古いルートを削除します。回線の復元（光） （823 ページ） を参照してください。
- **[アクション（Actions）] > [再同期（Resync）]** を選択し、回線または VC の状態を再同期します。
- **[アクション（Actions）] > [復元アクション（Restoration Actions）] > [手動復帰（Manual Revert）]** を選択し、ルートが障害から回復したときに、光回線を元のルートに戻します。回線の復元（光） （823 ページ）を参照してください。
- **[操作（Actions）]>[アクションの再ルーティング（Reroute Actions）]>[現用パス（Working Path）]** または [保護パス（Protected Path）] を選択し、回線用に定義されている現用パスまたは保護パスを通過するトラフィックを再ルーティングします。回線の再ルーティング（光回線） （824 ページ）を参照してください。
- **[アクション（Actions）] > [アクティブ化（Activate）]** を選択して、トラフィックが光回線を通過するようにします。回線をアクティブにする（光） （822 ページ） を参照してください。
- **[アクション（Actions）] > [非アクティブ化（Deactivate）]** を選択し、トラフィックが光回線を通過しないようにします。回線をアクティブにする（光） （822 ページ） を参照してください。
- **[アクション（Actions）] > [保護アクション（Protection Actions）]** を選択し、必要な保護切り替えアクションを選択して、保護された光回線内の 1 つのパスから別のパスにトラフィックを切り替えます。回線での保護切り替えアクションの開始（光） （827 ページ）を参照してください。
- [マルチレイヤ トレース（Multilayer Trace）] ビューのツールバーのフィルタ アイコンをクリックして、回線内のさまざまなレイヤを表示します。表示するレイヤを選択します。

第 VII 部

Cisco EPN Manager システムの管理



第 19 章

Cisco EPN Manager サーバーのセットアップ

以降のトピックでは、Cisco EPN Manager をインストールした後に管理者が実行するタスクについて説明します。これらのタスクが完了したら、Cisco EPN Manager スタートアップ ガイド（1 ページ）に説明されているように、ユーザーはログインして作業環境を設定できます。

Cisco EPN Manager のさまざまなタイプのユーザー（CLI ユーザーや Web GUI ユーザーなど）の詳細については、Cisco EPN Manager で CLI ユーザー インターフェイスを切り替える方法（998 ページ）を参照してください。

（注） ベスト プラクティス：Cisco EPN Manager のセキュリティ強化（1157 ページ）の重要な情報を必ず確認してください。

サーバーのセットアップ タスク

タスク	参照先
バックアップ設定の確認	自動アプリケーション バックアップのセットアップ （942 ページ）
必要な製品ライセンスおよびソフトウェア アップデートのインストール	ライセンスおよびソフトウェア アップデート （885 ページ）

タスク	参照先
ソフトウェア アップデートの場合： • 製品ソフトウェア アップデート（重大な修正、デバイス サポート、アドオン）の通知を有効にする • Cisco EPN Manager がソフトウェア アップデートを確認する際に、クレデンシャルを Cisco.com に保存するかどうかを指定する。保存する場合、更新の確認時にユーザーにクレデンシャルについてのプロンプトを表示するかどうかを指定する	ソフトウェア アップデートに関する通知の有効化または無効化 （901 ページ）
サーバーとブラウザベースの GUI クライアントの間のやり取りを保護するためにサーバー上で HTTPS を設定する（HTTP も使用できますが、HTTPS が推奨されています）	Cisco EPN Manager サーバーの接続の保護 （954 ページ）
ハイ アベイラビリティの設定	ハイ アベイラビリティの設定と管理 （1109 ページ）
データの保持および消去の調整	データの収集と消去 （985 ページ）
システムの問題を通知するサーバー関連のトラップでは、しきい値設定と重大度をカスタマイズし、設定した受信者に SNMP トラップ通知としてトラップを転送する	サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送 （981 ページ） SNMP トラップ通知としてのアラームおよびイベントの転送 （1070 ページ）
時間をサーバーとネットワーク デバイスとの間で同期するための NTP（Network Time Protocol）のセットアップ	サーバーでの NTP の設定 （968 ページ）
サーバーとネットワーク デバイス間のファイル転送のためのサーバーにおける FTP/TFTP の設定	サーバーでの FTP/TFTP/SFTP サービスの有効化 （970 ページ）
Cisco EPN Manager サーバーのプロキシの設定	Cisco EPN Manager プロキシ サーバーの設定 （969 ページ）
電子メール サーバーの設定	SMTP 電子メール サーバーの設定 （969 ページ）
コンプライアンス機能を有効にする（デバイス設定からの逸脱を識別するためにこの設定を使用する場合）	コンプライアンス監査の有効化および無効化 （192 ページ）

タスク	参照先
Cisco EPN Manager がネットワーク内に存在するサービス、およびプロビジョニング ウィザードを使用してプロビジョニングされたサービスを検出するように、サービス検出機能を有効化にします。	サービス検出の有効化および無効化（790 ページ）
シスコ製品の向上に寄与する製品フィードバックの設定	シスコサポート リクエストのデフォルトの設定 （983 ページ）
シスコ製品の向上に寄与する製品フィードバックの設定	シスコ製品フィードバックの設定 （984 ページ）

LDAP/Active Directory サーバーを設定して使用する

Cisco EPN Manager への LDAP サーバーの追加

LDAP ディレクトリにリストされ、EPNM に指定されていないユーザーを認証します。

（注） また、Cisco Identity Services Engine（ISE）を使用してユーザーを認証することもできます。詳細については、Cisco ISE と RADIUS または TACACS+ による外部認証 （1043 ページ）を参照してください。

LDAP サーバーを追加するには、次の手順を実行します。

（注） Active Directory サーバーを追加するには、次と同じ手順を使用します。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles, & AAA）]** を選択し、LDAP サーバーを選択します。

（注） このページに表示されている入力フィールドに入力する値には、次の制限が適用されます。

- 先頭または末尾にスペースがない。
- 入力文字列を「#」で始めることはできない。
- 特殊文字：「'+ * " ' / \ \\ < > ; ( ) \u0000（Unicode の Null 文字） \r」は入力できない。

ステップ 2 LDAP サーバーを選択した後、右側のペインで [+] アイコンをクリックして、追加する LDAP サーバーの詳細を作成します。

ステップ 3 LDAP サーバーの必要な詳細（サーバー アドレス、サーバー ポート、パスワード、IP アドレス、DNS 名など）を入力します。

ステップ 4 SSL 通信チャネルを使用する場合は、[セキュア認証を使用する（Use Secure Auth）]チェックボックスをオンにします。LDAP 証明書のインストールの詳細については、「Cisco EPN Manger での LDAP サーバーの設定」に記載されている方法を参照してください。

（注） Web サーバーの接続を保護するため、HTTPS をセットアップします。これは、SSL で LDAP を設定するための前提条件です。管理者は、各 LDAP サーバーのスキーマを設定できます。

ステップ 5 [管理 DN（Admin DN）] 文字列を入力します。

ステップ 6 パスワードと確認パスワードの詳細を入力します。

（注） LDAP 管理者は、文字列と確認パスワードを把握しています。

ステップ 7 次のフィールドにスキーマを入力します。通常、どの LDAP サーバーにもユーザーとグループの固有の設定と連結証明書のファイルがあります。

a) [サブジェクト名属性（Subject Name Attribute）]：この値は、特定のユーザー名が編成されている LDAP サーバー ユーザー プロファイル内の *uid* 属性を表します。

b) [グループ名属性（Group Name Attribute）]：この値は、グループ メンバ（管理者、モニター、コンフィギュレータ）に割り当てられているロールの権限を表し、LDAP サーバー グループ プロファイルの *description* 属性で示されます。ユーザー グループ名の値については、**[管理（Administration）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** > **[ユーザー グループ（User Groups）]** ページを参照してください。

c) [グループ マップ属性（Group Map Attribute）]：この値は、グループとユーザー間の関連付けを表し、LDAP サーバーのグループ プロファイル内の *memberUid* 属性で示されます。

（注） LDAP または Active Directory で複数のユーザーロールを指定するには、同じ名前を持つ複数の属性を作成するか、または 1 つの属性を作成し、カンマで区切られた複数のユーザーロールをリストします。次に例を示します。

- 同じ名前の複数の属性を指定するには、次のコマンドを実行します。

```
description=Admin
description=Monitor Lite
```

- 1 つの属性と複数のユーザーロールを指定するには、次の手順を実行します。

```
description=Admin,Monitor Lite
```

d) [仮想ドメイン属性（Virtual Domain Attribute）]：この値は、ユーザーがアクセスできるネットワークセクションを表し、LDAP サーバーのユーザープロファイル内の *title* 属性に記述されます。この値は、**[管理（Administration）]** > **[ユーザー（Users）]** > **[仮想ドメイン（Virtual Domains）]**ウィンドウに設定されている Cisco EPN Manager の仮想ドメインプロファイルと関連します。仮想ドメインに含める要素とその仮想ドメインへのアクセス権を付与するユーザーを選択できます。

（注） LDAP または Active Directory で複数の仮想ドメインを指定するには、同じ名前の複数の属性を作成するか、1 つの属性を作成し、カンマで区切られた仮想ドメインをリストします。次に例を示します。

- 同じ名前の複数の属性を指定するには、次のコマンドを実行します。

```
description=VirtualDomain1
description=VirtualDomain2
```

- 1 つの属性と複数のユーザーロールを指定するには、次の手順を実行します。

```
description=VirtualDomain1,VirtualDomain2
```

e) [サブジェクト検索ベース（Subject Search Base）]：ユーザーが配置されている場所を検索するパスを指定します。

f) [グループ検索ベース（Group Search Base）]：グループの場所を検索するパスを指定します。

ステップ 8 [再試行（Retries）] フィールドに、ソース ファイルの LDAP 認証を実行する回数を入力します。

ステップ 9 [保存（Save）] をクリックします。

Cisco EPN Manger での LDAP サーバーの設定

Cisco EPN Managerは、単方向 SSL を使用して LDAP サーバーを接続します。つまり、LDAP サーバーの認証局（CA）ルート（および中間）証明書を Cisco EPN Manager にインストールする必要があります。これらの証明書は LDAP サーバーの CA から入手します。次の手順では、ルート（および中間）CA 証明書をインストールするステップについて説明します。

始める前に

LDAP 証明書が Cisco EPN Manager にインストールされていることを確認するには、次の手順を実行します。

1. 顧客が所有する LDAP サーバーの SSL 証明書のルート証明書と中間証明書を取得します。
2. Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ） で説明したように、ssh を使用して CLI 管理者ユーザーとしてログインします。
3. LDAP サーバー証明書の CA ルート/中間証明書を Cisco EPN Manager のローカル ディレクトリにコピーします。たとえば、rootCA.pem を /localdisk/defaultRepo にコピーします。
4. Cisco EPN Manager Admin CLI で、Cisco EPN Manager にこの CA ルート証明書をインポートするコマンドを `EPNMServer/admin# ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository <Repository-name> <certificate-file> truststore {devicemgmt | pubnet | system | user}` として実行します（例：`EPNMServer/admin# ncs certvalidation trusted-ca-store importcacert alias epnm40 repository defaultRepo certnew.cer truststore system`）。これにより、Java インポート信頼ストアに LDAP 証明書がインポートされます。
5. Cisco EPN Manager を再起動します。

（注） 2 台の LDAP サーバーと 2 台の Cisco EPN Manager サーバーがある場合（HA モード）、各 LDAP サーバーのルート/中間証明書をインストールしてから、HA のガイドラインに基づいて各 Cisco EPN Manager サーバーを再起動します。

ステップ 1 **[管理（Administration）]**>**[ユーザー（Users）]**>**[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[AAA モード（AAA Mode）] を選択します。

ステップ 2 [LDAP] オプション ボタンを選択します。

ステップ 3 [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] チェックボックスをオンにすると、外部 AAA サーバーがダウンした場合にローカル データベースの使用が有効になります。

ステップ 4 外部 LDAP サーバーがダウンした場合にローカル認証に戻すには、次の手順を実行します。

a) [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] を選択します。

b) フォールバック条件（[サーバーが応答しないときのみ（Only on no server response）] または [認証に失敗したかサーバーが応答しないとき（On authentication failure or no server response）]）を指定します。

（注） ルートユーザーはローカルで認証されているため、ルートユーザーとしてログインできる必要があります。

ステップ 5 [保存（Save）] をクリックします。

（注） 別のブラウザを使用して、新しいユーザー名とパスワードで LDAP にログインします。

Cisco WAN Automation Engine と Cisco EPN Manager の統合

Cisco WAN Automation Engine（WAE）のプラットフォームは、ソフトウェア モジュールを相互接続し、ネットワークと通信し、外部アプリケーションとインターフェイスする API を提供するオープンでプログラマブルなフレームワークです。

Cisco WAE は、ネットワークの継続的なモニターリングと分析およびネットワーク上のトラフィック需要に基づく現在のネットワークのモデルを作成および維持するためのツールを提供します。このネットワーク モデルには、トポロジ、設定、トラフィック情報など、特定の時点でのネットワークに関するすべての関連情報が含まれています。この情報は、トラフィック要求、パス、ノードとリンクの障害、ネットワークの最適化、またはその他の変更によるネットワークへの影響を分析するための基礎として使用できます。

（注） 詳細については、『*Cisco WAN Automation Engine (WAE) Installation Guide*』と『*Cisco WAN Automation Engine (WAE) User Guide*』を参照してください。

Cisco EPN Manager では、明示的なパスを持つ単方向トンネルまたは双方向トンネルを作成すると、WAN Automation Engine（WAE）との統合により、Cisco EPN Manager から自動的に REST

コールを使用して明示的なパスが提供されます。そのため、明示的なパスを手動で入力する必要がなくなります。WAE は、可能なネットワーク パスのリストを表示し、適切なパスを選択できるようにします。

WAE パラメータの設定

WAE パスの詳細を指定するには、次の手順を実行します。

始める前に

WAE パラメータを設定することを確認します。

1. **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。
2. 回線 VC を展開し、[WAE サーバー設定（WAE Server Settings）] を選択します。
3. 関連する WAE の詳細（バージョン 7.1.3 以降）とフィールドの詳細（[WAE サーバー IP（WAE Server IP）]、[WAE ポートアドレス（WAE Port Address）]、[WAE サーバーユーザー名（WAE Server User Name）]、[WAE サーバーパスワード（WAE Server Password）] など）を入力します。
4. [保存（Save）] をクリックして WAE サーバーの設定を保存するか、または [デフォルトにリセット（Reset to Defaults）] をクリックしてすべての入力をクリアします。

ステップ 1 必要なパラメータを持つ単方向トンネルまたは双方向トンネルを作成します。詳細については、MPLS TE トンネルの作成とプロビジョニング （751 ページ）を参照してください。

ステップ 2 [パスの制約の詳細（Path Constraints Details）] 領域で、パスのタイプを [動作中（Working）] または [保護済み（Protected）] のいずれかとして選択します。フィールドと属性の説明については、パスの制約の詳細に関するフィールド参照：MPLS TE トンネル （762 ページ）を参照してください。

ステップ 3 必要に応じて [新しいパス（New Path）] チェックボックスをオンにして、[WAEサーバーからパスを選択（Choose Path from WAE server）] チェックボックスをオンにします。

ステップ 4 [WAE サーバーからパスを選択（Choose Path from WAE server）] チェックボックスをオンにします。EPNM マネージャは、WAE ネットワークを取得するために REST 要求を WAE に送信します。
WAE は可能なネットワークのリストを返します。

ステップ 5 [WAE ネットワークの選択（Select WAE Network）] ドロップダウン リストから、ネットワークを選択します。
EPNM マネージャは、送信元、宛先、ネットワークなどの必要なすべてのパラメータを持つ REST 設定要求を WAE に送信します。返される最大パスのデフォルト値は 2 です。最大パス値は WAE を介して設定されます。WAE は、要求を満たす可能性のあるパスのリストを表示します。

ステップ 6 [WAE パスの選択（Select WAE Path）] ドロップダウン リストから、返された適切なパスを選択します。
EPNM は、マップ上に選択したパス オーバーレイを表示します。

ステップ 7 [パス名（Path Name）] フィールドにパスの名前を入力します。

最後に選択したパスを明示的なパスとして使用して、順序のプロビジョニングを続行できます。

ユーザー管理セットアップ タスク

タスク	参照先
管理権限を持つ Web GUI ユーザーを作成し、Web GUI root アカウントを無効にします。	管理者権限を持つ Web GUI ユーザーの作成 （1022 ページ） Web GUI ルート ユーザーの無効化および有効化 （998 ページ）
ユーザー認証および許可のセットアップ	外部認証の設定 （1041 ページ） ローカル認証の設定 （1040 ページ）
ユーザー アカウントとユーザー グループの作成	ユーザーが実行できるタスク Web インターフェイスの制御 （999 ページ）
ユーザー セキュリティ設定の調整（ローカル認証のパスワード規則、アイドル時間のログアウト設定）	ローカル認証のためのグローバル パスワード ポリシーの設定 （1027 ページ）
ジョブを許可できるユーザーの指定	ジョブ承認者を設定してジョブを承認する （1027 ページ）
仮想ドメインを作成してデバイス アクセスを制御する	デバイスへのユーザー アクセスを制御するための仮想ドメインの作成 （1030 ページ）
ユーザーが GUI クライアントにログインしたときに表示されるメッセージの作成	ログイン バナー（ログインの免責事項）の作成 （972 ページ）

障害管理セットアップ タスク

タスク	参照先
アラームとイベントを電子メール形式で他の受信者に転送する	
アラームとイベントを SNMP トラップ形式で他の受信者に転送する	SNMP トラップ通知としてのアラームおよびイベントの転送 （1070 ページ）

タスク	参照先
アラームとイベントの表示と検索用のグローバル設定を構成する • アラーム テーブルとイベント テーブルで確認済み、割り当て済み、およびクリア済みのアラームを非表示にする • 確認済みと割り当て済みのアラームを検索結果に含める • デバイス名をアラーム メッセージに含める	確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する （1076 ページ）
特定のイベントの重大度をカスタマイズする	アラーム重大度レベルの変更 （1079ページ）
特定のアラームの自動クリア間隔をカスタマイズする	アラームの自動クリア間隔の変更 （1081ページ）
アラームの [障害ソース（Failure Source）] フィールド内のテキストをユーザーにわかりやすくする	アラーム重大度レベルの変更 （1079ページ）
優先イベントの動作をカスタマイズする	完全優先ベントの動作の変更 （1084ページ）
一般イベント処理を制御する	汎用トラップ処理を有効または無効にする （1088 ページ）
ユーザーがシスコ サポート要求を作成できるかどうかとその方法を制御する	シスコサポートリクエストのデフォルトの設定 （983 ページ）

Web GUI セットアップ タスク（管理者）

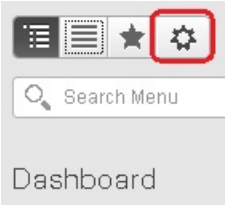
タスク	参照先
展開で使用しない機能またはメニュー項目の無効化	Web GUI メニューのカスタマイズによる Cisco EPN Manager 機能の無効化 （882 ページ）
システムモニターリング管理ダッシュボードのセットアップ	システム監視ダッシュボードを使用して、Cisco EPN Managerサーバーのヘルス、ジョブ、パフォーマンス、および API 統計をチェックする （976 ページ）

Web GUI メニューのカスタマイズによる Cisco EPN Manager 機能の無効化

ルート、スーパーユーザー、または管理者ユーザー グループに属している場合は、特定のメニューが Web GUI に表示されなくなるように Cisco EPN Manager をカスタマイズできます。ユーザー グループとそのメンバーの表示（1003 ページ）を参照してください。これは、展開で Cisco EPN Manager のすべての機能は使用しない場合に役立ちます。メニューを無効にすると、ユーザーのロールに関係なく、すべてのユーザーの Web GUI に表示されなくなります。

機能全体と特定のメニューを無効にして Web GUI をカスタマイズするには、次の手順を実行します。現在無効になっている機能を再び有効にするには、同じ手順を使用しますが、機能のステータスを [有効（Enabled）] に切り替えます（または [すべて有効にする（Enable All）] をクリックします）。

ステップ 1 左側のサイドバー メニューの上に表示される歯車をクリックします。



ステップ 2 機能全体を無効にするには、次の手順を実行します。

1. [機能ナビゲーション グループ（Feature Navigation Groups）] 領域で機能を見つけますます。
2. 機能の [ステータス（Status）] 列でトグルをクリックして [無効（Disabled）] を表示します。
3. 無効にするメニューを確認するには、[メニューの詳細（Menu Details）] 領域のメニューをスクロールします。影響を受けているすべてのメニューが [無効（Disabled）] として表示されます。

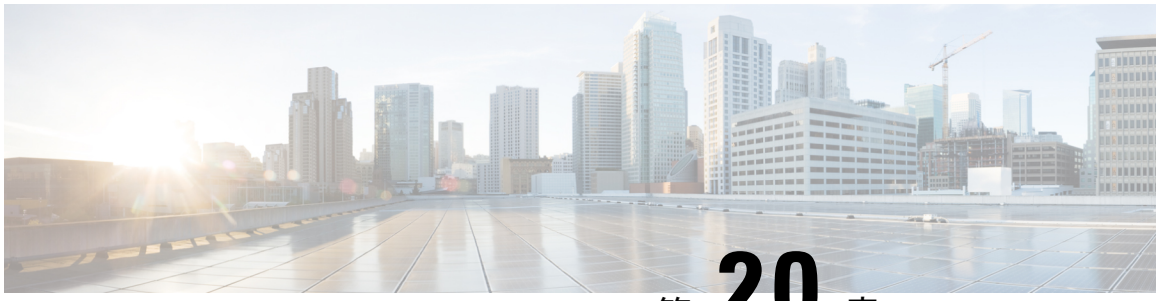
ステップ 3 特定のメニューを無効にするには、次の手順を実行します。

1. [メニューの詳細（Menu Details）] 領域でメニューを見つけます。
2. メニューの [ステータス（Status）] 列でトグルをクリックして [無効（Disabled）] を表示します。サブメニューを含むメニューを無効にすると、サブメニューも無効になります。次に例を示します。
   - [グループ管理（Group Management）] を無効にすると、Cisco EPN Manager は [グループ管理（Group Management）] のサブメニューすべて（[ネットワーク デバイス グループ（Network Device Group）]、[コンピューティング デバイス グループ（Compute Device Groups）]、および [ポート グループ（Port Groups）]）を無効にします。
   - [コンピューティング デバイス グループ（Compute Device Groups）] サブメニューのみを無効にした場合も、Cisco EPN Manager は [グループ管理（Group Management）] の下のサブメニュー、[ネットワーク デバイス グループ（Network Device Groups）] と [ポート グループ（Port Groups）] サブメニューは表示します。

3. 無効にするメニューを確認するには、[メニューの詳細（Menu Details）] 領域のメニューをスクロールします。

ステップ 4 [保存（Save）] をクリックし、Web GUI からログアウトします。

ステップ 5 Web GUI にログインし直し、変更内容を検証します。



第 20 章

ライセンスおよびソフトウェアアップデート

ライセンスの表示と管理

ライセンスによって、使用できる機能と、Cisco EPN Manager で管理できるデバイスのタイプおよび数が決まります。ログインせずに Cisco EPN Manager に接続すると、サーバーが実行しているライセンスのタイプを識別するバナーがログイン ページに表示されます（Cisco EPN Managerのライセンスのタイプ （886ページ）を参照）。Cisco EPN Managerがシングル サインオン（SSO）を使用するように設定されている場合は、バナーの内容を表示してライセンスのタイプを確認します。

Cisco EPN Manager は、シスコ スマート ライセンスと従来のライセンスをサポートしています。現在、従来のライセンスを使用している場合は、スマート ライセンスへの移行が推奨されます。2 種類のライセンスの違いについては、Cisco.com で紹介している Cisco Smart Licensing の概要を参照してください。

次のいずれかのライセンス方法を使用して、Cisco EPN Manager を新しいバージョンにアップグレードできます。

- シスコ スマート ライセンス：この方法では、Cisco EPN Manager の新しいインスタンスを Cisco Smart Software Manager に登録する必要があります。Cisco Smart Software Manager への Cisco EPN Manager の登録 （890 ページ）を参照してください。
- 従来のライセンス：この方法では、ファイルは Cisco EPN Manager の以前のバージョンのバージョンからアップグレードされたバージョンにコピーされます。ただし、アップグレードされたバージョンの基本ライセンスを購入する必要があります。新しい従来のライセンスを購入するには、http://cisco.com/go/license に移動します。

リリース 5.0 以降、Cisco EPN Manager の新規インストールのすべてのインスタンスでスマートライセンスがデフォルトで有効になります。Cisco EPN Manager 5.0 にアップグレードする場合は、既存のライセンスモードが継続されます。

次のトピックでは、シスコ スマート ライセンスと従来のライセンスの使用方法について説明します。

- シスコ スマート ライセンスの使用 （887 ページ）
- 従来のライセンスの使用 （895 ページ）

Cisco EPN Manager のライセンスのタイプ

次のトピックでは、Cisco EPN Manager でサポートされている機能と時間ベースのライセンスについて説明します。

基本ライセンス

基本ライセンスを使用すると、サーバー上のすべてのアプリケーションとすべてのデバイス ドライバが有効になります（デバイス数の制限なし） 。Web GUI には [基本ライセンス（Base License）] として表示されます。

Cisco Advantage Addon Function Right to Manage（RTM）ライセンス

Cisco Advantage Addon Function RTM ライセンスは、Web GUI に **Cisco Advantage Addon Function Right To Manage ライセンス**として表示されます。

このライセンスは、サービスディスカバリ、プロビジョニング、サービスプロモーション、サービスアシュアランス、マルチレイヤトレースの各機能に関連するすべての機能とオプションを有効にします。これらの機能に関連する機能およびメニューオプションは、ライセンスがアクティブでない限り表示されません。また、スケジュールされたプロビジョニングジョブの実行はすべて失敗します。最初の Cisco Advantage Addon Function Right to Manage（RTM）ライセンスをインストールすると、これらの機能とオプションが有効になります。このライセンスの使用状況は、ライセンスダッシュボードで Cisco EPN Manager のライセンス機能によって追跡および報告されます。

デバイスの管理用（RTM）ライセンス

デバイス RTM ライセンスを使用すると、サーバーは特定のデバイス タイプの特定数のデバイスを管理できます。RTM ライセンスの場合、デバイス数はデバイス タイプの横に表示されます。これらのライセンスには、次の 2 つの種類があります。

- コア、エッジ、集約、およびアクセス ネットワーク デバイス用の拡張 RTM ライセンス。これらのライセンスにより、デバイスのライフサイクル管理、ネットワーク プロビジョニング、ネットワーク アシュアランスなど、エンドツーエンドのネットワーク管理が可能になります。
- Wi-Fi アクセス ポイント、WAN ルータ、コア スイッチ、およびデータ センター スイッチを備えたサービス プロバイダの Wi-Fi ネットワークの基盤 RTM ライセンス。これらのライセンスは、デバイスのライフサイクル管理とともに、アシュアランスの可視性とトラブルシューティング機能を可能にします。

サテライトとして設定されたデバイス（Cisco ASR 9000v ホストを備えた Cisco ASR 903）は、独立したデバイスとしてカウントされます。

Cisco EPN Manager はまた、オープン ライセンスの「ベストエフォート」検出プロセスを使用して、サードパーティ製のネットワーク デバイスも検出します。収集された情報は Web GUI に表示されますが、結果は大きく異なる場合があります（Cisco EPN Manager がデバイスから受信した応答によって完全に異なります）。このメカニズムを有効にするために、ライセンスを購入する必要はありません。

RTM ライセンスは、GUI に次のように表示されます。

- シスコ デバイスの場合：**NCS 2002** や **ASR 9001** などのデバイス モデル。
- サード パーティ製のデバイスの場合：**オープン ライセンス**。

高可用性用の SBY ライセンス

スタンバイ（SBY）ライセンスでは、高可用性展開をセットアップできます。高可用性展開では、デバイス ライセンスと機能ライセンスのすべてをプライマリ サーバーにインストールする必要があります。セカンダリ サーバーではライセンスは必要ありません。

時間ベース ライセンス、ラボ ライセンス、および永久ライセンス

ほとんどのライセンスは、ラボ ライセンスまたは時間ベースのライセンスとして購入できます。

- ラボ：ラボ環境またはステージング環境向け。

  ラボライセンスでは、管理できるデバイスの数とタイプに制限はありません。このライセンスを使用して、ステージング環境のすべてのデバイスを管理できます。

（注） デバイスを管理するには、ラボライセンスまたはデバイス管理権限ライセンスのいずれかを選択できます。両方のライセンスを選択すると、Cisco EPN Manager はデフォルトでラボライセンスのみを有効にし、デバイス管理権限ライセンスのライセンスサマリー カウントを自動的に 0 に更新します。

- 時間ベース（評価）：90 日間の試用期間（試用期間が終了すると製品は無効になります）。時間ベースのライセンスを購入した場合、残り日数はライセンス名の横に表示されます。

これらのライセンスは、永久ライセンスに変換できます。

シスコ スマート ライセンスの使用

シスコでは、シンプルで効率的なシスコ スマート ライセンスのメカニズムを使用してライセンスを管理することをお勧めしています。

スマート ライセンスと従来のライセンスの比較は、Cisco.com のシスコ スマート ライセンスの概要に示されています。Cisco EPN Manager でスマート ライセンスを有効にした後、Cisco.com の Cisco Smart Software Manager（CSSM）に Cisco EPN Manager を登録する必要があります。登録後は Cisco EPN Manager のすべてのライセンス タイプが Cisco EPN Manager Web GUI から使用できるようになります。

現在、従来のライセンスを使用している場合は、従来型ライセンスからスマート資格への変換（892 ページ）で説明されているように、既存の Cisco EPN Manager ライセンスをいつでもスマート資格に変換できます。

以降のトピックでは、シスコ スマート ライセンスを使用して Cisco EPN Manager のライセンスをセットアップし、管理する方法について説明します。

Cisco EPN Manager での Cisco Smart Licensing のセットアップ

Cisco Smart Licensing を使用してライセンスを管理できるように、以下の手順に従って Cisco Smart Licensing をセットアップします。現在、従来のライセンスを使用している場合、これらの同じ手順を使用して Cisco Smart Licensing を使用し、都合の良いときに、従来型ライセンスからスマート資格への変換 （892 ページ）で説明されている手順に従って、既存の Cisco EPN Manager ライセンスを変換します。

	手順	参照先：
1.	Cisco Systems でスマート アカウントを作成します。	「Smart Account Request」に移動し、Web サイトの指示に従います。
2.	Cisco EPN Manager と Cisco.com の CSSM の間の通信をセットアップします。	Cisco EPN Manager と Cisco Smart Software Manager との間のトランスポート モードの設定 （889 ページ）
3.	Cisco EPN Manager でスマート ライセンスを有効にします。	Cisco EPN Manager でのスマート ライセンスの有効化 （889 ページ）
4.	CSSM からトークンを取得し、Cisco EPN Manager Web GUI でそのトークンを入力することによって、Cisco EPN Manager を Cisco.com の CSSM に登録します。	Cisco Smart Software Manager への Cisco EPN Manager の登録 （890 ページ）

5.	Cisco EPN Manager で使用するライセンスを選択します。	スマート ライセンシングを使用した Cisco EPN Manager ライセンスの選択 （891 ページ）
6.	ライセンスの使用状況をモニターできるように、スマート ライセンスのダッシュボードをセットアップします。	スマート ライセンス ダッシュボードのライセンスのしきい値の設定 （893 ページ）

Cisco EPN Manager と Cisco Smart Software Manager との間のトランスポート モードの設定

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [スマート ライセンスの転送（Smart Licensing Transport）] タブをクリックして、通信モードを選択します。

- [ダイレクトモード（Direct mode）]：ライセンス情報を直接クラウドに送信します。これがデフォルトです。この URL は編集できません。[接続のテスト（Test Connectivity）] をクリックして、接続ステータスを確認します。
- トランスポート ゲートウェイ：Cisco Smart Call Home トランスポート ゲートウェイまたは Cisco Smart Licensing Software サテライト（顧客宅内にインストール通信にされ、CCSM の機能のサブセットを提供）を使用します。（詳細については Cisco.com を参照してください）。[URLの入力（Enter URL）] フィールドに適切な URL を入力します。[接続のテスト（Test Connectivity）] をクリックして、接続ステータスを確認します。
- HTTP/HTTPS プロキシ：Cisco EPN Manager とクラウドとの間での通信に HTTP または HTTPS プロキシを使用します。このオプションを有効にするには、まずプロキシ設定を行う必要があります。[HTTP/HTTPSプロキシ（HTTP/HTTPS Proxy）] ハイパーリンクをクリックして、または [プロキシ（Proxy）] タブをクリックして、プロキシの設定を追加または編集します。Cisco EPN Manager プロキシ サーバーの設定 （969 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックして、転送設定を保存します。

ステップ 4 デフォルト値に戻すには、[リセット（Reset）] をクリックしてから [保存（Save）] をクリックします。

次のタスク

まだ有効化していない場合は、スマート ライセンスを有効化します。Cisco EPN Manager でのスマート ライセンスの有効化 （889 ページ） を参照してください。

Cisco EPN Manager でのスマート ライセンスの有効化

始める前に

トランスポート モードが設定されていることを確認してください。Cisco EPN Manager と Cisco Smart Software Manager との間のトランスポート モードの設定 （889 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ライセンスとソフトウェア アップデート（Licenses and Software Updates）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）]** の順に選択します。

ステップ 2 Cisco EPN Manager Web GUI で Cisco Smart Licensing を有効にします。

a) [ライセンス設定（Licensing Settings）] タブをクリックします。

b) [ライセンシングモード（Licensing Mode）] フィールドで、[スマートソフトウェアライセンシング（Smart Software Licensing）] ラジオ ボタンをクリックします。

c) [製品名（Product Name）] ドロップダウンリストから、[Evolved Programmable Network Manager Prime Infrastructure]を選択します。

d) [スマート ソフトウェア ライセンシングの有効化（Enable Smart Software Licensing）] をクリックします。この手順が完了したら、設定ステップに進む前に Web GUI を再起動する必要があることを示すダイアログボックスが Cisco EPN Manager に表示されることがあります。

e) ダイアログ ボックスで [OK] をクリックします。

f) 必要に応じて Web GUI からログアウトしてから、再びログインします。

次のタスク

次のいずれかを実行します。

- Cisco.com で CSSM に Cisco EPN Manager をまだ登録していない場合、Cisco EPN Manager は評価モードで実行されます（利用可能な期間は 90 日間）。Cisco Smart Software Manager への Cisco EPN Manager の登録 （890 ページ）の説明に従い、製品を登録します。
- CSSM に Cisco EPN Manager をすでに登録している場合は、使用するライセンスを選択します。スマート ライセンシングを使用した Cisco EPN Manager ライセンスの選択 （891 ページ） を参照してください。

Cisco Smart Software Manager への Cisco EPN Manager の登録

Cisco EPN Manager を CSSM に登録するには、CSSM からトークンを入手して、そのトークンを Cisco EPN Manager の Web GUI に入力する必要があります。この作業が必要になるのは 1 回限りです。何らかの理由で製品インスタンスを再登録する場合は、この手順に従ってください。

（注） CSSM の使用方法やこのアプリケーションで実行できるその他の操作については、『Cisco Smart Software Manager User Guide』を参照してください。たとえば、ライセンス登録やライセンス認証の更新、Cisco Smart Licensing での製品の登録解除などがあげられます。

始める前に

組織にスマート アカウントがない場合は、software.cisco.com へ移動し、**管理**エリアで [スマートアカウントの申請（Request a Smart Account）] を選択し、指示に従ってアカウントを作成します。

ステップ 1 Cisco Software Central の Web サイト（software.cisco.com）に移動します。

ステップ 2 トークンを取得します。すでにトークンを取得している場合（たとえば、従来のライセンシング PAK をスマート資格に変換した場合）は、次のステップに進みます。

製品インスタンスを再登録すると、トークンが CSSM のユーザー インターフェイスにリストされます。トークンが無効になっている場合は、次の手順に従って新しいトークンを取得できます。

1. Cisco Software Central で、**[ライセンス（License）]** > **[スマートソフトウェアライセンシング（Smart Software Licensing）]**を選択します。
2. 該当するバーチャル アカウントを選択します。
3. [全般（General）] タブをクリックし、[新規トークン（New Token）] をクリックします。
4. 指示に従って名前、期間、輸出コンプライアンスの適用性を入力してから、諸条件や責任について同意してください。
5. [トークンの作成（Create Token）] をクリックします。
6. トークン ID をクリップボードにコピーし、次のステップに進みます。

ステップ 3 トークン ID を Cisco EPN Manager の Web GUI に入力し、製品を登録します。

1. **[管理（Administration）]**>**[ライセンスとソフトウェア アップデート（Licenses and Software Updates）]**> **[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** の順に選択します。
2. [ライセンス設定（Licensing Settings）] タブをクリックし、[登録トークン（Registration Token）] フィールドにトークンを貼り付けます。
3. [登録（Register）] をクリックします。

ステップ 4 Cisco EPN Manager の Web GUI からログアウトして、もう一度ログインします。

次のタスク

使用するライセンスを選択します。スマート ライセンシングを使用した Cisco EPN Manager ライセンスの選択 （891 ページ） を参照してください。

スマート ライセンシングを使用した Cisco EPN Manager ライセンスの選択

Cisco EPN Manager を CSSM に登録すると、すべての Cisco EPN Manager ライセンス タイプが Cisco EPN Manager Web GUI にリストされるので、その中から使用するライセンスを選択できます。

ステップ 1 これが初回の場合、スマート ライセンスを選択します。

a) **[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [ライセンス（Licenses）]** を選択します。

しばらくすると、Cisco EPN Manager にダイアログ ボックスが表示され、従来のライセンスを使用していないためページにアクセスできないことが通知されます。これは正常です。

b) ダイアログ ボックスで、[スマート ライセンスの設定（Smart License Settings）] をクリックします。

c) [ライセンス設定（Licensing Settings）] タブをクリックします。

ステップ 2 すでにスマート ライセンスを使用している場合は、以下の手順に従います。

a) **[管理（Administration）]>[ライセンスとソフトウェアアップデート（Licenses and Software Updates）]> [スマートソフトウェアライセンシング（Smart Software Licensing）]** の順に選択します。

b) [ライセンス設定（Licensing Settings）] タブをクリックします。

ステップ 3 [スマート ライセンスの使用状況（Smart License Usage）] で、[ライセンスの選択（Choose Licenses）] をクリックします。

ステップ 4 [使用可能なライセンス（Available Licenses）] ダイアログボックスでライセンスを選択してから、[保存（Save）] をクリックします。Cisco EPN Manager がただちに、そのライセンスを使用し始めます。

次のタスク

新しいライセンスに対するスマート ライセンス ダッシュボードのしきい値を設定します。スマート ライセンス ダッシュボードのライセンスのしきい値の設定 （893 ページ） を参照してください。

従来型ライセンスからスマート資格への変換

従来型のライセンシングを使用して Cisco EPN Manager ライセンスを管理している場合、Cisco EPN Manager での Cisco Smart Licensing のセットアップ （888 ページ） で説明しているセットアップ タスクに従うことで、Smart Licensing を設定できます。都合のよいときに、この手順で説明するように既存の従来型ライセンスをスマート資格に変換してください。Cisco Software Central サイトにあるライセンス登録ポータルで製品アクティベーション キー（PAK）番号を入力する必要があります。

始める前に

- Cisco Software Central にアクセスするには、Cisco.com アカウントが必要です。アカウントをお持ちでない場合は、Cisco Software Central に移動します。
- 既存の従来型ライセンスの PAK 番号が割り当てられていることを確認します。

ステップ 1 Cisco Software Central で、**[ライセンス（License）] > [従来のライセンス（Traditional Licensing）]** の順に選択します。

ステップ 2 [製品ライセンス登録を続行（Continue to Product License Registration）] をクリックしてライセンス登録ポータルを開きます。

ステップ 3 [新規ライセンスの取得（Get New License）] フィールドに PAK 番号を入力します。複数の PAK を入力する場合は、カンマで区切ります。10 PAK まで入力できます。

ステップ 4 [PAK/トークン（PAKs/Tokens）] タブで、スマート資格に変換する PAK を選択してから、**[アクション（Actions）] > [スマート資格への変換（Convert to Smart Entitlements）]** の順に選択します。

スマート ライセンス ダッシュボードのライセンスのしきい値の設定

ライセンスを効率的に管理するには、Cisco EPN Manager のライセンスの失効期限が近づいていることを示すようにスマート ライセンス ダッシュボードを設定します。ここで構成した設定はシステム全体に影響します。

ステップ 1 **[管理（Administration）]>[ライセンスおよびソフトウェア アップデート（Licenses and Software Updates）]> [スマート ソフトウェア ライセンシング（Smart Software Licensing）]** を選択してから、[ライセンス ダッシュボードの設定（License Dashboard Settings）] タブをクリックします。

ステップ 2 [ライセンスタイプ（License Type）] ドロップダウン リストから選択します。

ステップ 3 [しきい値（Threshold Value）] フィールドに、値を入力します。

ステップ 4 [保存（Save）] をクリックします。

しきい値は[ライセンスの要約（License Summary）] と [ライセンスのデバイスディストリビューション（Device Distribution for License）] のグラフ表示の直線として表されます。

Cisco EPN Manager のライセンス使用状況の確認

[スマート ライセンス（Smart Licensing）] ダッシュボードを使用して、現在のライセンスの使用状況を確認します。ダッシュボードを開くには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [スマートライセンスダッシュボード（Smart Licensing Dashboard）]** を選択します。基本的なライセンスのタイプについては、Cisco EPN Manager のライセンスのタイプ （886 ページ）を参照してください。

これらのライセンス数を表示するための手順	ダッシュボードで確認する部分
現在の日付	[ライセンスの要約数（License Summary Count）]：緑は準拠ライセンス数を示します。赤は非準拠ライセンス数を示します。
特定の週または月	[ライセンスの要約（License Summary）]：棒グラフにカーソルを合わせるとより詳しい説明が表示されます。

これらのライセンス数を表示するための手順	ダッシュボードで確認する部分
特定のライセンスタイプ	[ライセンスのデバイス配布（Device Distribution for License）]：[ライセンスの要約（License Summary）] ダッシュレットの上部にあるライセンス リンクのいずれかをクリックします。詳細を表示するには、グラフにカーソルを合わせます。

スマート ライセンスの無効化

ステップ 1 Cisco EPN Manager Web GUI でライセンス設定を変更します。

a) **[管理（Administration）]** > **[ライセンスおよびソフトウェア アップデート（Licenses and Software Updates）]** > **[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** を選択します。

b) ページの下部で [スマート ライセンスの無効化（Disable Smart Licensing）] をクリックして、選択内容を確認します。

ステップ 2 Cisco EPN ManagerWeb GUI からログアウトして、もう一度ログインします。

Cisco EPN Manager はまだ従来のライセンスを使用するよう登録されていないため、再度ログインすると、すべての機能が無効になります。これは正常です。

ステップ 3 Cisco EPN Manager Web GUI で、従来のライセンスを有効にします。（この処理は [スマート ライセンスの設定（Smart License Settings）] ページで行います）

a) **[管理（Administration）]** > **[ライセンスおよびソフトウェア アップデート（Licenses and Software Updates）]** > **[ライセンス（Licenses）]** を選択します。

しばらくすると、Cisco EPN Manager にダイアログボックスが表示され、従来のライセンスを使用していないためページにアクセスできないことが通知されます。これは正常です。

b) ダイアログ ボックスで、[スマート ライセンスの設定（Smart License Settings）] をクリックします。

c) [ライセンス設定（License Settings）] タブをクリックします。

d) [ライセンス モード（Licensing Mode）] で [従来のライセンス（Traditional Licensing）] を選択します。

e) [登録（Register）] をクリックします。

ステップ 4 Cisco EPN Manager からログアウトして、再度ログインします。

参考：スマート製品の登録とライセンス認証ステータス

製品登録ステータス

ライセンス登録ステータスは、製品が Cisco.com のシスコ スマート ソフトウェア ライセンシングに正常に登録されているかどうかを表します。

ライセンス登録ステータス	説明
Unregistered	スマート ソフトウェア ライセンシングは Cisco EPN Manager で有効になっていますが、Cisco EPN Manager は CSSM に登録されていません。
登録済み	Cisco EPN Manager は、CSSM に登録されています。Cisco EPN Manager は ID 証明書を受信しています。この ID 証明書は、将来シスコのライセンス担当者との通信に使用されます。
この登録通知の有効期限が切れました	Cisco EPN Manager は有効期限までに正常に登録を更新できず、CSSM から削除されています。

ライセンス認証ステータス

ライセンス認証ステータスは、購入したライセンスに対するライセンスの使用状況、および Cisco Smart Licensing に準拠しているかどうかを表しています。購入したライセンス数を超えると、その製品ステータスは**コンプライアンス違反**となります。

ライセンス認証ステータス	説明
評価モード	Cisco EPN Manager は、評価モードで実行されています（90 日で期限切れになります）。
承認済み（Authorized）	Cisco EPN Manager に有効なスマート アカウントがあり、登録されています。製品が要求するすべてのライセンスの使用が承認されています。
コンプライアンス違反	Cisco EPN Manager は、購入されたライセンス数を超過しました。（特に、製品インスタンスの仮想アカウントに、1 つ以上のライセンス タイプが不足しています）。
評価期限切れ	評価期間が終了し、Cisco EPN Manager はライセンスなしの状態になります。
認証が期限切れ	Cisco EPN Manager は、認証の有効期限前に、ライセンス認証を正常に更新できませんでした。

従来のライセンスの使用

（注） シスコ スマート ライセンスに変換することをお勧めします。Cisco EPN Manager での Cisco Smart Licensing のセットアップ（888 ページ）を参照してください。スマート ライセンスを使用していて、従来のライセンスをもう一度有効にする場合は、スマート ライセンスの無効化（894 ページ）を参照してください。

Cisco EPN Manager は、4 時間ごとに従来のライセンスを確認し、ステータスをライセンス ログ（/opt/CSOlumos/logs/license.log）に書き込みます。時間ベースのライセンスの有効期限が切れると、アクティブなセッションを使用しているユーザーは [ライセンス（Lisenses）] ページにリダイレクトされ、新しいユーザーはログインできなくなります。RTM ライセンスのデバイス数が超過している場合は、次のいずれかを実行します。

- デバイスの一部を削除します。毎日のインベントリ収集の後、デバイスは [管理対象（Managed）] として表示されます。
- RTM 数が多いライセンスを取得します。従来のライセンスの追加と削除 （896 ページ）を参照してください。

従来のライセンスの詳細については、次のトピックを参照してください。

- Cisco EPN Manager のライセンスのタイプ （886 ページ）
- 従来のライセンスの表示 （896 ページ）
- 従来のライセンスの追加と削除 （896 ページ）
- 従来のライセンスの別のサーバーへの移動 （897 ページ）

従来のライセンスの表示

現在インストールされている従来の Cisco EPN Manager のライセンスを表示するには、**[管理（Administration）] > [ライセンスとソフトウェア更新プログラム（Licenses and Software Updates）] > [ライセンス（Licenses）]** を選択します。Cisco EPN Manager は、[基本ライセンス（Base License）] の下のリストに表示されているライセンスをサポートしています。

（注） マルチシェルフ デバイスの各シャーシは、個別のライセンスを使用します。たとえば、Cisco NCS 2006 デバイスに 3 つのシャーシがある場合、そのデバイスでは 3 つのライセンスが使用されます。

従来のライセンスの追加と削除

新しい従来のライセンスをインストールするには、元のライセンスが既にサーバー上に存在している必要があります。ライセンスのコピーを作成しないでください。新しい従来のライセンスを購入するには、www.cisco.com/go/license に移動します。ライセンスを正しい順序でインストールしていることを確認します。たとえば、他のライセンスで必要となるため、基本ライセンスを最初にインストールする必要があります。

ライセンスを削除すると、ライセンスの情報すべてがサーバーから削除されます。

注意 ライセンス ファイルに手動で変更を加えた場合、Cisco EPN Manager はファイルが破損していると見なしてそのファイルをインストールしません。この場合は、新しいライセンス ファイルを取得します。

ステップ 1 **[管理（Administration）]** > **[ライセンスとソフトウェア アップデート（Licenses and Software Updates）]** > **[ライセンス（Licenses）]** の順に選択します。

ステップ 2 **[ファイル（File）]** > **[ライセンス ファイル（License Files）]**を選択します。

- ライセンスを追加するには、[追加（Add）] をクリックして [ファイルの選択（Choose File）] をクリックし、ライセンス ファイルの場所を参照し、**OK** をクリックします。
- ライセンスを削除するには、ライセンス ファイルを選択して [削除（Delete）] をクリックします。

従来のライセンスの別のサーバーへの移動

ライセンスを別のサーバーに移動する必要があるのは、高可用性を使用していて、サーバーに障害が発生した場合のみです。ライセンスを削除する必要がある場合は、従来のライセンスの追加と削除（896 ページ）を参照してください。ライセンスを移動するには、次の手順を実行します。

ステップ 1 元のサーバーから従来のライセンスを削除します。

ステップ 2 電子メールを licensing@cisco.com に送信し、従来のライセンスの「再ホスト」を要求します。

ステップ 3 従来のライセンスを受け取ったら、新しいサーバーにインストールします。

期限切れのライセンスの更新

Cisco EPN Manager のライセンスの有効期限が切れている場合は、次の手順を実行して更新できます。

ステップ 1 **[管理（Administration）]** > **[ライセンスとソフトウェア アップデート（Licenses and Software Updates）]** > **[ライセンス（Licenses）]** の順に選択します。

[ライセンス（Licenses）] ページを開きます。

ステップ 2 次のいずれかを実行します。

- ページの左上に [要約（Summary）] と [ファイル（Files）] メニューが表示されている場合は、ステップ 4 に進みます。
- これらのメニューが表示されていない場合は、まず従来のライセンスを登録する必要があります。ステップ 3 に進みます。

ステップ 3 従来のライセンスを登録し、この手順のステップ 1 に戻ります。

a) **[管理（Administration）]** > **[ライセンスおよびソフトウェア アップデート（Licenses and Software Updates）]** > **[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** を選択します。

b) [ライセンス設定（Licensing Settings）] タブを選択し、[従来のライセンス（Traditional Licensing）] オプション ボタンをクリックし、[登録（Register）] をクリックします。
c) Cisco EPN Manager からログアウトしてから、ログインし直します。

ステップ 4 ページの左上の領域から、**[ファイル（Files）] > [ライセンス ファイル（License Files）]** を選択します。

[ライセンス ファイル（License Files）] ページが開きます。

ステップ 5 更新するライセンス ファイルを選択します。
a) [追加（Add）] をクリックします。

[ライセンス ファイルの追加（Add A License File）] ダイアログボックスが表示されます。

b) [ライセンス ファイルの選択（Select License File）] フィールドで、[ファイルの選択（Choose File）] をクリックします。
c) 適切なライセンス ファイルまで移動してクリックし、[開く（Open）] をクリックします。
d) [OK] をクリックします。

ステップ 6 Cisco EPN Manager からログアウトしてから、ログインし直します。

ライセンス ダッシュボードの表示

[ライセンス（Licensing）] ダッシュボードから、従来のライセンスまたはスマート ソフトウェア ライセンシングが有効になっているかどうか（[アクティブなライセンス モード（Active Licensing Mode）] フィールドで示される）を判別したり、現在使用されているライセンスの数を表示したりできます。ライセンスモードは、[スマートソフトウェアライセンシング（Smart Software Licensing）] ページ（**[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]**）から設定できます。

このダッシュボードを開くには、次のいずれかを実行します。

- **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ライセンス ダッシュボード（Licensing Dashboard）]** を選択します。
- [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページの右上にある [ライセンス ダッシュボード（Licensing Dashboard）] リンクをクリックします。

ダッシュボードに表示される情報は、有効になっているライセンス モードによって異なります。スマート ソフトウェア ライセンシングが現在有効になっている場合は、次のダッシュレットが表示されます。

- [ライセンスの要約数（License Summary Count）] 領域：使用されるライセンスの数と、各ライセンス タイプのコンプライアンス状態が表示されます。表示されるライセンスの数は、現在の日付に基づいています。
- [ライセンスの要約（License Summary）] ダッシュレット：特定の期間に各ライセンス タイプで使用されるライセンスの棒グラフが表示されます。追加情報を表示するには、グラフの上にカーソルを置きます。

- [ライセンスのデバイス ディストリビューション（Device Distribution for License）] ダッシュレット：特定のライセンスのデバイス ディストリビューション グラフを表示するには、[ライセンスの要約（License Summary）] ダッシュレットに表示されたグラフの上部にあるリンクをクリックします。追加情報を表示するには、グラフの上にカーソルを置きます。

（注） [ライセンス ダッシュボード（License Dashboard）] に表示される情報は、SmartLicense ジョブが午前2時（事前設定されている実行時間）に実行された後、毎日更新されます。[ジョブ ダッシュボード（Job Dashboard）] にこのジョブを表示するには、**[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** を選択します。

従来のライセンスが現在有効になっている場合は、[ライセンス（Licensing）] ダッシュボードに [従来のライセンス（Traditional Licensing）] ダッシュレットが表示されます。[ライセンス タイプ（License Type）] ドロップダウン リストから対応するオプションを選択して、アシュアランスライセンスまたはライフサイクルライセンスに関する情報を表示するかどうかを指定します。ダッシュレットが更新され、そのライセンス タイプを持つデバイス ファミリ、それらのファミリの各デバイスに割り当てられているトークンの数、現在使用されていないトークンの数などの情報が表示されます。

関連トピック

Cisco EPN Manager での Cisco Smart Licensing のセットアップ （888 ページ）
Cisco EPN Manager でのスマート ライセンスの有効化 （889 ページ）
Cisco Smart Software Manager への Cisco EPN Manager の登録 （890 ページ）
スマート ライセンス ダッシュボードのライセンスのしきい値の設定 （893 ページ）
スマート ライセンスの無効化 （894 ページ）
参考：スマート製品の登録とライセンス認証ステータス （894 ページ）

ソフトウェア アップデートの管理

ソフトウェア アップデートとは

シスコでは、Cisco EPN Manager ソフトウェアに対するアップデートを定期的に提供しています。これらのアップデートは、次のカテゴリに分類されます。

- 重要修正：ソフトウェアの重要な修正を提供します。これらのアップデートが利用可能になったら、ただちにこれらのすべてをダウンロードして適用することが強く推奨されます。

- デバイス サポート：Cisco EPN Manager がリリース時点でサポートしていなかったデバイスを管理するサポートを追加します。
- アドオン：現在使用中の Cisco EPN Manager バージョンを補完するための新しい機能を提供します（新しい GUI 画面や機能が含まれることもあります）。これには、Cisco EPN Manager のメンテナンス パックとメンテナンス パック ポイント パッチが含まれます。

Cisco EPN Manager に表示されるアップデート通知は、管理者によって指定された通知設定によって異なります。ソフトウェア アップデートに関する通知の有効化または無効化（901 ページ）を参照してください。すべてのソフトウェア アップデートが .ubf ファイルにパッケージ化されます。大容量のアップデートには、インストールするものを選択可能な個別の小容量のアップデートが含まれている場合があります。アップデートをインストールすると、Cisco EPN Manager が次の処理を実行します。

- ファイルの発行者が Cisco Systems であり、ファイルが改ざんされていないことを確認する
- 必要な他のアップデートを自動的にインストールする

http://www.cisco.com に接続できる場合は、Cisco.com から直接アップデートをダウンロードしてインストールできます。インターネット接続がない場合は、必要な接続を備えたサーバーからアップデートをコピーして、そこからインストールします。

メンテナンス パックのインストール手順については、『Cisco EPN Manager Installation Guide』を参照してください。ポイント パッチのインストール手順については、Cisco.com のソフトウェア ダウンロードのページのパッチ ファイルに付属する readme ファイルを参照してください。

インストール済み製品ソフトウェアのバージョンの表示

次のいずれかの方法で Cisco EPN Manager 製品バージョンを確認します。

- Web GUI から、ページの右上の設定アイコンをクリックし、**[ヘルプ（Help）] > [Cisco EPN Managerについて（About Cisco EPN Manager）]** を選択します。
- CLI から、次の名前のファイルの内容を表示します。

  #cat /opt/CSCOlumos/installedComponentsVersions.xml

CLI を使用するには、Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

インストール済みのソフトウェア アップデートの表示

Web GUI にログインしていない場合は、ログイン ページから [インストール済みアップデートの表示（View Installed Updates）] をクリックすると、ソフトウェア アップデートを一覧表示するポップアップ ウィンドウを表示できます。

Web GUI にログインしている場合は、次の 2 つの方法でソフトウェア アップデートを表示できます。

- **[Cisco EPN Managerのバージョン情報（About Cisco EPN Manager）]** ページで、ページの右上にある設定アイコンをクリックし、**[Cisco EPN Managerのバージョン情報（About Cisco EPN Manager）]** をクリックしてから、[インストール済みアップデートの表示（View Installed Updates）] をクリックします。（[インストール済みアップデートの表示（View Installed Updates）] リンクは、ログイン ページにもあります）。
- **[管理（Administration）]** > **[ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）]** > **[ソフトウェアアップデート（Software Update）]** を選択します（この方法を使用すると、最も詳細な情報が表示されます）。

[ソフトウェアアップデート（Software Update）] ページに 2 つのタブが表示されます。

- インストール済みの更新プログラム（Installed Updates）：Cisco EPN Manager で現在使用されているアップデート。
- アップロード済みアップデート ファイル（Uploaded Update Files）：サーバーにアップロードされているアップデート ファイル（使用されていないファイルを含む）。[対応するアップデート（Corresponding Updates）] フィールドには、アップロード済みの前提条件のアップデートも一覧表示されます。

  アップデート ファイルがまだインストールされていない場合は、削除できます。ファイルを選択し、[削除（Delete）] ボタンをクリックします。

ソフトウェア アップデートに関する通知の有効化または無効化

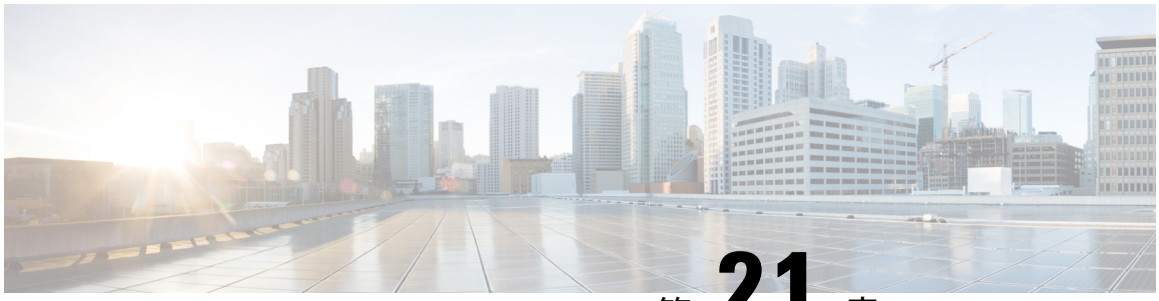
デフォルトでは、Cisco EPN Manager は [ソフトウェアアップデート（Software Updates）] ページに有効なすべてのアップデートに関する情報を表示します。このリストはかなり長くなる場合があるため、表示する内容と通知対象とするアップデートを調整することをお勧めします。また、すべての通知を無効にして、後で再び有効にすることもできます。

ソフトウェア アップデートの通知を設定します。

a) **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** の順に選択し、**[一般（Genera）]** > **[ソフトウェア アップデート（Software Update）]** を選択します。

b) [通知設定（Notification Settings）] で、アップデートのカテゴリをオンまたはオフにします。すべての通知を無効にするには、カテゴリが 1 つもオンになっていない状態にします。カテゴリの説明については、次を参照してください。 ソフトウェア アップデートとは （899 ページ）

c) [保存（Save）] をクリックします。



第 21 章

Cisco EPN Manager セキュリティ

この章は次のトピックで構成されています。

セキュリティの概要

Cisco EPN Manager には、ネットワークとそのデータが侵害されないようにする高レベルのセキュリティが必要です。これは、ネットワークを完全に管理し、デバイスのクレデンシャルを保存するのに特に重要です。この目的のために、Cisco EPN Manager は次のセキュリティ アプローチを利用します。

- **セキュアなアーキテクチャ**：Cisco EPN Manager アーキテクチャは、存在する可能性のある未知のソフトウェアの欠陥へのアクセスを制限し、悪意のある目的に使用できないように設計されています。
- **セキュアなデフォルトの設定**：Cisco EPN Manager は製品のセキュリティを強化するデフォルトの設定が標準装備されています。たとえば、セキュアでない FTP サービスや TFTP サービスがサポートされていても、デフォルト設定ではアクティブ化されません。
- **インストールの強化**：シスコのアドバンスト サービス チームは、Cisco EPN Manager のインストールの具体的な内容を評価し、必要と思われる追加のセキュリティ強化タスクを実行できます。
- **シスコ セキュア開発ライフサイクル（CSDL）プロセス**：開発からリリースまで、CSDL プロセスに従って Cisco EPN Manager のセキュリティを向上させます。
- **二要素認証**：ユーザーは、Cisco EPN Manager へのアクセスが許可される前に、2 つのセキュリティ層を通過する必要があります。

以降の項では、これらのアプローチについてさらに詳しく説明します。

セキュアなアーキテクチャ

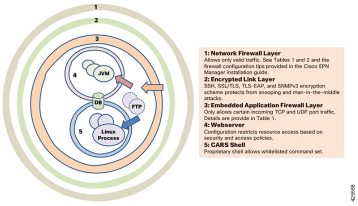
Cisco EPN Managerのアーキテクチャ設計では、攻撃者がシステムに侵入するには次の3つの条件が同時に存在する必要があるという前提に基づいています。

- システムに欠陥がある。
- 攻撃者がその欠陥にアクセスできる。
- 悪意のある目的でこの欠陥を悪用する能力が攻撃者にある（Hughes, J., & Cybenko, G. 2013年。Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity.*Technology Innovation Management Review*, 3(8): 15-24）。

欠陥はそのままのであれば無害です。攻撃者が欠陥にアクセスでき、悪用する方法知っている場合にのみ、その欠陥は脆弱性となります。この欠陥と脆弱性の区別を理解しておくことが重要です。欠陥が公になっただけで、それが自動的に脆弱性となるわけではありません。特定の状況下でのみ、欠陥は脆弱性になり得ます。

セキュリティ リスクを管理するために Cisco EPN Manager で用いられているアプローチの鍵は、システムの欠陥へのアクセスを制限することです。見つかる可能性があるどの欠陥にも攻撃者が容易にアクセスすることができないように Cisco EPN Manager アーキテクチャは設計されています。ユーザーが常に欠陥を排除したり、攻撃者による悪用を防ぐことができるとは限らないため、これは実用的で合理的なアプローチです。複数のセキュリティ レイヤを配置することで、存在する特定の欠陥へのアクセスを制限できます。Cisco EPN Manager は、図 1 に示すように、境界セキュリティの 3 つのレイヤを使用します。

図 *17*：複数レイヤで保護された境界アーキテクチャ：強化された外部シェルを備えた仮想アプライアンスシステム



これら 3 つのレイヤのうち、 1 つは Cisco EPN Manager の内部に存在し、 2 つは外部に存在します。内部レイヤは Cisco EPN Manager で事前に設定され、インストールが完了すると動作できるようになります。2 つの外部レイヤは事前に設定されていないため、外部ネットワーク ファイアウォールと暗号化された通信リンク レイヤを作成して実装する必要があります。会社のテクニカル チームとシスコ アドバンスト サービスとが連携し、これらのアイテムを作成することをお勧めします。

（注） ネットワークに使用するのに適切なタイプの暗号化プロトコルを選択するには、Cisco EPN Manager 内の一部の設定を変更する必要があります。

内部レイヤは Cisco EPN Manager に組み込まれており、次のコンポーネントで構成されています。

- 組み込みファイアウォール：内部コンポーネントに関する最初の保護レイヤーを提供します。これにより、着信トラフィックに対して開かれるポートはごくわずかになります。そのため、Linux OS および Oracle データベースの複数の欠陥（既知と不明の両方）へのアクセスを制限することで、攻撃の領域が減少します。
- CARS シェル：Linux での実行を許可されているコマンドの承認済みリストを適用し、OS とのやり取りを制限することで、Linux に関する保護レイヤを提供します。
- Web サーバー：Linux、Java 仮想マシン、およびデータベースに関する保護レイヤを提供します。このレイヤには、Javaおよびデータベース リソースとメソッドへのアクセスを制限するためのセキュリティ フィルタが設定されています。

この内部レイヤは、次の例で説明するような多くのリスクからシステムを保護します。これらの欠陥は、保護されていないシステムの脆弱性と見なされますが、Cisco EPN Manager には存在しません。次の例では（National Vulnerability Database ID によって識別）、外部ファイアウォールと暗号化されたリンクのレイヤは攻撃者によって侵害されたか、または実在していないかのいずれかです。

- CVE-2013-5211：Linux NTPD コンポーネントの NTP の実装での欠陥。着信 NTP トラフィックにポート 23 からアクセスされた後に DoS 攻撃が発生します。組み込みファイアウォールはこのトラフィックを許可していないため、攻撃者はこの欠陥にアクセスできません。そのため、Cisco EPN Manager でのリスクではありません。
- CVE-2016-0634：Linux bash シェルの欠陥：この攻撃は、ポート 22 を介して bash シェルを標的にした認証済みユーザーによって行われる可能性があります。Cisco EPN Manager は、ポート 22 を介した bash シェルへの直接アクセスを提供していません。代わりに、CARS シェルには通常の認証済みユーザーからアクセスできます。そのため、この欠陥は Cisco EPN Manager のリスクではありません。
- CVE-2017-12617：Apache Tomcat の欠陥：PUT 要求が行われたときにこの攻撃が発生する可能性があります。Cisco EPN Manager の Web サーバーの設定ではこのタイプのアクセスは許可されないため、この欠陥は危険ではありません。
- CVE-2015-4863：Oracle データベースの欠陥：この攻撃はOracle Net プロトコルを介してネットワーク上で発生する可能性があります。Oracle データベースは組み込みファイアウォールと Web サーバーの背後にあるため、この問題は Cisco EPN Manager のリスクではありません。そのため、ネットワークを通じてデータベースにアクセスできません。

セキュリティアーキテクチャの影響

このアーキテクチャのため、 Cisco EPN Manager は非常に密接に統合されたシステムであり、組み込まれている OS やデータベースは、どのような管理目的や操作目的であってもユーザーアクセスに対してオープンではありません。ユーザーは、Cisco EPN Manager の GUI と Cisco EPN Manager の管理 CLI を使用してのみ、システムにアクセスして管理することができます。この管理 CLI は Linux CLI ではありません（ユーザー インターフェイスとユーザー タイプ （995

ページ）を参照）。また、Cisco EPN Manager は想アプライアンスとしてデプロイおよび管理されます。つまり、Cisco EPN Manager はスタンドアロンの仮想マシン（VM）としてデプロイする OVA ファイルとして使用できます。したがって、Cisco EPN Manager の管理は、Linux OS 上で実行されデータベースに接続する Web アプリケーションの管理とは大きく異なります。この結果、ユーザーには次のような制限が生じます。

- サードパーティ製またはシスコ以外のパッチによって個々のコンポーネントに対するパッチ適用やアップグレードを行うことはできません。シスコは、組み込みの Linux や Oracle を含むすべての内部コンポーネントについてパッチをリリースします。
- シスコはテクニカルサポートを提供できないため、組み込みの Red Hat Linux OS にサードパーティ製アプリケーションをインストールすることはできません。
- 組み込みのコンポーネント（Linux、Oracle、Java）を通常のサーバーのように簡単に管理することはできません。
- このガイドでユーザーが変更可能として記載されていない内部設定を変更しないようにしてください。そのような変更を加えた場合、全体のセキュリティが低下したり、システムの機能やパフォーマンスが無効になったり低下したりする可能性があるためです。

（注） Cisco EPN Manager は、Linux と Oracle が組み込まれてはいますが、Linux OS 上で実行され Oracle データベースに接続する通常の Web アプリケーションではありません。言い換えれば、全体としての総和と各部分の総和とが同じではありません。

Cisco EPN Manager は、強化された外部シェルと密接に統合された仮想アプライアンスです。そのため、Linux、Oracle、および通常の Web アプリケーションのセキュリティを評価するために使用する基準を、Cisco EPN Manager の評価に使用することは「できません」。Oracle の評価に Linux OS の基準を使用することはできません。これらは別々の製品であるためです。同様に、Linux を対象とする基準や方法を使用して Cisco EPN Manager を評価したり、Cisco EPN Manager を評価する目的で Oracle 用の基準や方法を使用することもできません。Cisco EPN Manager のセキュリティを評価するには、Cisco EPN Manager のアーキテクチャに適した別の一連の基準やテスト方法が必要になります。

Cisco EPN Manager で使用するポート

Cisco EPN Manager は、正当なトラフィックのみがサーバーに対して許可されるように、組み込みアプリケーションのファイアウォール設定で出荷されています。表 1 に、デバイスからの接続要求をリッスンし、着信トラフィックを承認するポートを示します。ファイアウォール内のこれらのポートの開閉は、特定の機能を有効または無効にすると Cisco EPN Manager によって自動的に行われます。ファイアウォール内のポートを有効または無効にする必要はありません。Cisco EPN Manager を回避するファイアウォール設定を指定しようとすると、そのセキュリティと整合性が損なわれることがあります。

（注） 次の表には、インストール後のセキュリティ強化を実行するために必要な情報も示されています（詳細については、「セキュアなデフォルト設定」を参照してください）。

表 *54* : 組み込みのファイアウォールを介した開いているポートのリスニング

ポート	プロトコル	使用方法	無効にしても安全か?	注記
21	TCP	FTP を使用してデバイスとの間でファイルを転送する。	場合による	これは、TFTP のみをサポートし、SFTP または SCP をサポートしていない古い管理対象デバイスでも必要になる場合があります。 このポートを無効にする方法：Web GUI の [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] から [全般（General）] > [サーバー（Server）] を選択して FTP を無効にします。FTP を無効にした後に CLI 管理者ユーザーとしてサーバーを停止し、再起動します。
22	TCP	Cisco EPN Manager サーバーとの SSH 接続を開始し、SCP または SFTP を使用してファイルを Cisco EPN Manager サーバーにコピーする。	非対応	—
69	UDP	TFTP を使用してデバイスにイメージを配布する。	場合による	SCP、SFTP、HTTPS などの代替プロトコルがイメージ配布に使用され、管理対象デバイスでサポートされている場合にのみ。
162	UDP	ネットワークデバイスから SNMP トラップを受信する。	非対応	—
443	TCP	HTTPS を介した Cisco EPN Manager サーバーへのブラウザアクセスの場合。	非対応	—

ポート	プロトコル	使用方法	無効にしても安全か?	注記
514	UDP	ネットワーク デバイスから syslog メッセージを受信する。	非対応	—
1522	TCP	アクティブとスタンバイ の Cisco EPN Manager サーバー間での高可用性（HA）通信の場合。 Oracle データベース同期用の Oracle JDBC トラフィックを許可するために使用されます。	はい	少なくとも 1 台の Cisco EPN Manager サーバーが HA 用に設定されていないとこのポートは自動的に無効になります。
2021	TCP	FTP を使用してデバイスにイメージを配布する。	非対応	—
6789	TCP	Java Remote Method Invocation（RMI）操作に使用されます。	対応	—
8005	TCP	Tomcat シャットダウン サーバー ソケット ポート	対応	—
8082	TCP	HA ヘルスモニターの Web インターフェイスの場合（HTTPS 経由）。 プライマリサーバーとセカンダリサーバーが HTTPS を介してヘルスステータスを監視するために使用します。	いいえ（HA が設定されている場合）	—
8085	TCP	ユーザーがハイアベイラビリティで準備テストを実行する場合、プライマリサーバーとセカンダリサーバー間のネットワーク帯域幅速度を確認するためにヘルスモニタープロセスで使用されます	いいえ（HA が設定されている場合）	—
8087	TCP	HA セカンダリ バックアップ サーバー上のソフトウェアを更新する（トランスポートとして HTTPS を使用）。	非対応	—
8091	TCP	このポートは Web コンテナによって使用されます。	対応	—

ポート	プロトコル	使用方法	無効にしても安全か?	注記
8456	TCP	これは、HTTP/1.1 リクエストの Tomcat HTTP コネクタで使用されます。	対応	—
8457	TCP	HTTP コネクタは SSL リクエストを処理できないため、このポートは SSL リクエストを処理するコネクタポートとして機能します。	対応	—
9991	UDP	Netflow データ パケットを受信する。	はい	Cisco EPN Manager は Netflow をサポートしていません。ネットワーク ファイアウォールでこのトラフィックを無効にする必要があります。
9992	TCP	HTTP または HTTPS を使用して M-Lync を管理する。	はい	Cisco EPN Manager は M-Lync をサポートしていません。ネットワーク ファイアウォールでこのトラフィックを無効にする必要があります。
11011 ～ 11014	TCP	独自の Cisco Networking Services（CNS）プロトコル トラフィックの PnP 操作の場合。	はい	Cisco EPN Manager は PnP をサポートしていません。ネットワーク ファイアウォールでこのトラフィックを無効にする必要があります。
61617	TCP	Java メッセージング サービス（JMS）接続上での MTOSI NBI 通知の場合。 PnP 操作にも使用されます。	はい	Cisco EPN Manager は JMS または PnP 上で MTOSI をサポートしていません。ネットワーク ファイアウォールでこのトラフィックを無効にする必要があります。

セキュアなデフォルト設定

Cisco EPN Manager 可能な限りセキュアなデフォルトのアプリケーション設定が搭載されています。それらの設定は、脅威モデルを分析し、特定の状況のリスクを評価した後にのみ、変更できます。デフォルト設定では、Cisco EPN Manager は次を行うよう、最善を尽くします。

- デフォルトのパスワードを使用しない。
- 不要な OS や Oracle パッケージ/サービスにアクセスできないようにする。
- Cisco EPN Manager のリリース時に、組み込み OS および Oracle に最新のセキュリティ パッチが適用されます。
- 人間のユーザーによる Oracle アクセスパスワードの使用を許可しない。これらのパスワードはマシンで生成され、内部コンポーネントによって使用されます。

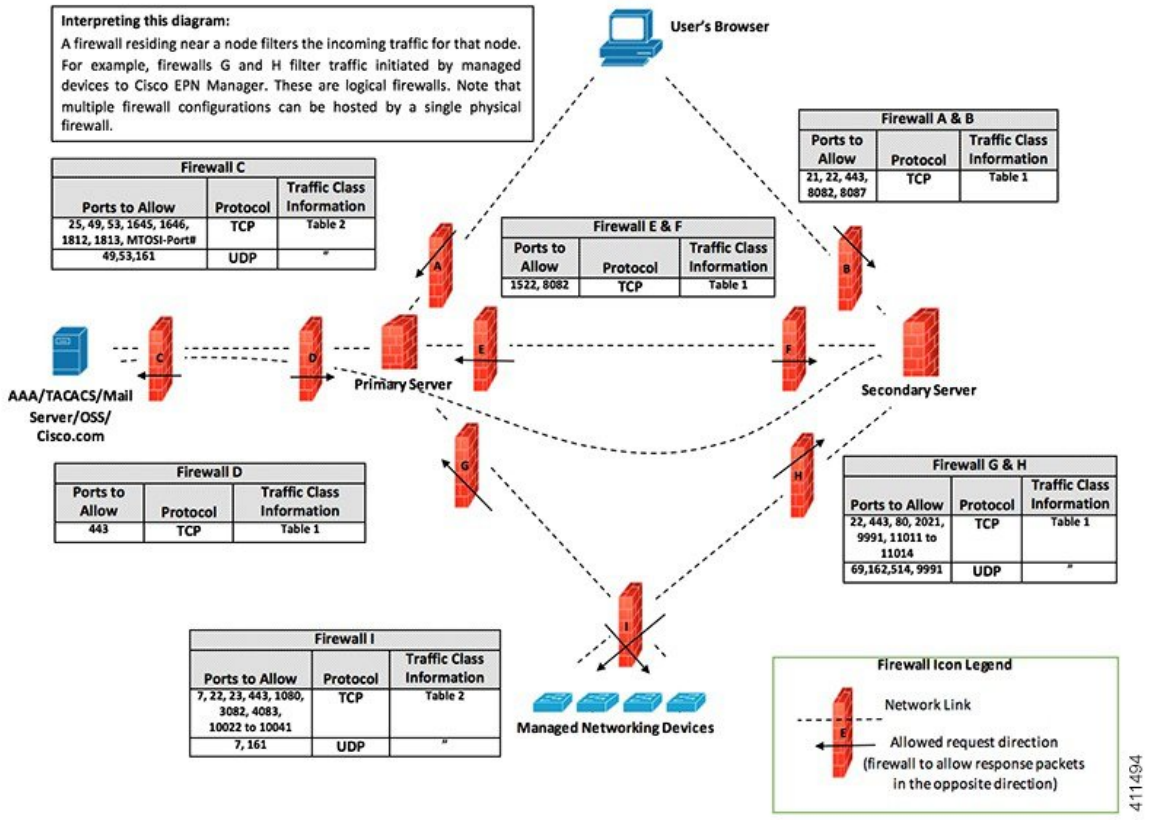
インストールの強化

Cisco EPN Manager のインストールを強化するには、次のタスクを実行する必要があります。

1. 正当なトラフィックのみを許可するように、組み込みの内部および外部のネットワーク ファイアウォールを設定します。
2. すべての着信トラフィックと発信トラフィックに暗号化を使用します。
3. 正当なトランザクションのみを送信できるように、Cisco EPN Manager とそのピア システムを設定します。

先に進む前に、まず Cisco EPN Manager がピア システムとやり取りする方法を理解する必要があります。一般的な HA 展開用の管理トラフィック フローと外部ネットワーク ファイアウォールとともに、これを次の図に示します。

（注） これらのファイアウォールを実装することをお勧めしますが、必須ではありません。



インストール環境によっては、ファイアウォールの設定をカスタマイズしてセキュリティをさらに向上させることが必要になります。一般的なポリシーとして、不要なポートやセキュアでないポート（暗号化されたトラフィックを送信しないなど）をすべて無効にする必要があります。

組み込み型アプリケーション ファイアウォールの設定

アプリケーションファイアウォールを設定するには、インストール環境で実行する必要のない Cisco EPN Manager の機能を無効にする必要があります。これにより、ファイアウォール内の対応するリスニング ポートが自動的にシャットダウンされます。

ステップ 1 現在有効になっているポートを識別します。

a) 外部に公開される展開で使用されるポートのリストを表示するには、Cisco EPN Manager CLI 管理者ユーザーとしてログインし、**show security-status** コマンドを実行します。

b) OS レベルで開いているすべてのリスニングポートのリストを表示するには、CLI 管理者ユーザーとしてログインし、**show netstat** コマンドを実行します。

ステップ 2 ガイダンスについては表 54 : 組み込みのファイアウォールを介した開いているポートのリスニング （907 ページ）を使用して、これらのポートの中で Cisco EPN Manager の通常の機能を中断させることなく安全に無効にできるものを特定します。

次の点に注意してください。

- Cisco EPN Manager は、内部操作に一部のリスニング ポートを使用します。これらのポートは、組み込みファイアウォールの背後に隠されたままになります。
- 表 54 : 組み込みのファイアウォールを介した開いているポートのリスニング （907 ページ）に示す手順のみを使用してポートを有効または無効にする必要があります。

外部ネットワーク ファイアウォールの設定

組み込みファイアウォールに加えて、Cisco EPN Manager とそのピア システムが使用するリスニング ポートを対象とするトラフィックのみを許可するようにネットワーク ファイアウォールを展開することもできます。「インストールの強化」のトピックで示した図では、表 54 : 組み込みのファイアウォールを介した開いているポートのリスニング （907 ページ） および 表 55 : 宛先ポートの使用元 Cisco EPN Manager （912 ページ）に示すポート情報を使用してファイアウォールルールをセットアップする方法を説明しています。この図を使用して、管理ネットワークに適したファイアウォール設定を決定します。

- トラフィッククラスを識別するには、表 54 : 組み込みのファイアウォールを介した開いているポートのリスニング （907 ページ） の「**使用方法**」の列を参照してください。Cisco EPN Manager のインストール環境で使用されていないサービスが使用するポートを無効にすることをお勧めします。
- また、ネットワーク ファイアウォールで（ネットワーク デバイスまたはピア システムに接続するために）Cisco EPN Manager が発信トラフィックに使用する宛先ポートも有効にする必要があります。これらの宛先ポートとそれらの目的のリストについては、表 55 : 宛先ポートの使用元 Cisco EPN Manager （912 ページ）を参照してください。

表 *55 : 宛先ポートの使用元 Cisco EPN Manager*

ポート	プロトコル	使用する場合
7	TCP/UDP	ICMP を使用したエンドポイントの検出。
22	TCP	管理対象デバイスとの SSH 接続の開始。
23	TCP	Telnet を使用した管理対象デバイスとの通信。
25	TCP	SMTP サーバーを使用した電子メールの送信。
49	TCP/UDP	TACACS を使用した Cisco EPN Manager ユーザーの認証。
53	TCP/UDP	DNS サービスへの接続。
161	UDP	SNMP を使用したポーリング。

ポート	プロトコル	使用する場合
443	TCP	HTTPS を使用した Cisco NCS 2000 デバイスのイメージのアップロードおよびダウンロードと設定バックアップ/復元の実行。
1522	TCP	プライマリとセカンダリの HA サーバー間での通信（プライマリとセカンダリのサーバー間での Oracle データベースの同期に Oracle JDBC トラフィックを許可する）。
1080	TCP	Socket Secure（SOCKS）プロトコルを使用した Cisco オプティカル ネットワーキング システム（ONS）および Cisco NCS 2000 シリーズのデバイスとの通信。
1645、1646、および 1812、1813	UDP	RADIUS を使用した Cisco EPN Manager ユーザーの認証。
3082	TCP	TL1 プロトコルを使用した Cisco ONS および Cisco NCS 2000 のデバイスとの通信。
4083	TCP	TL1 プロトコルを使用した Cisco ONS および Cisco NCS 2000 シリーズのデバイスとの通信。
8082	TCP	HTTPS を使用したプライマリとセカンダリの HA サーバー間の通信による相互の正常性の監視。
8085	TCP	ユーザーがハイアベイラビリティで準備テストを実行する場合、プライマリサーバーとセカンダリサーバー間のネットワーク帯域幅速度を確認するためにヘルスモニタープロセスで使用されます
10022 ～ 10041	TCP	パッシブ FTP ファイル転送（デバイスの設定やレポートの取得など）。
MTOSI/RESTCONF TCP ポート番号	TCP	Cisco EPN Manager サーバーに接続された NBI クライアントでリッスンする（このポートが NBI クライアント システムによって設定された後、ポート番号を含む登録通知メッセージが Cisco EPN Manager サーバーに送信される）。詳細については、MTOSI または RESTCONF API のガイドを参照してください。

トラフィック暗号化のセットアップ

次のトラフィック グループを暗号化する必要があります。

- ノースバウンド トラフィック：このグループは、人間のユーザーのブラウザからのクライアント/サーバー トラフィックか、またはビジネス サポート システム/運用サポート シス

テム（BSS/OSS）からの NBI トラフィックで構成されます。このトラフィックは HTTP 経由で送信されるため、HTTPS（TLS で暗号化された HTTP）を実装する必要があります。

- サウスバウンド トラフィック：このグループは、SNMP や HTTP などの幅広いプロトコルを使用して管理対象デバイスを照会または設定する管理トラフィックで構成されます。SSH や SNMPv3 などのプロトコルを使用して、このトラフィックを保護できます。このトラフィックを暗号化するために実行する必要がある設定手順の説明については、「SNMPv3 を使用した Cisco EPN Manager とデバイス間の通信の強化」を参照してください。
- ピア システム間の水平方向のトラフィック：このグループは、Cisco EPN Manager と、外部認証サーバー（TLS-EAP によって保護）や SMTP メール サーバー（TLS によって保護）などの他のさまざまなサポート システム間のトラフィックで構成されます。保護する必要があるアプリケーション プロトコルに応じて、異なる暗号化プロトコルが使用されます。一部のアプリケーション プロトコルには、暗号化が組み込まれている場合もあります。
- HA 展開のプライマリ サーバーとセカンダリ サーバー間の水平方向のトラフィック：このグループは、プライマリ モードとセカンダリ モードで実行している 2 台の Cisco EPN Manager サーバー間のトラフィックで構成されます。各サーバーは、もう一方のサーバーの正常性を監視し、HTTPS で保護されている接続を介してデータベースとその他のファイルのコンテンツの同期を保ちます。

SNMPv3 を使用した Cisco EPN Manager とデバイス間の通信の強化

SNMPv3 は、SNMPv2 よりもセキュリティ機能が高いプロトコルです。デバイスが SNMPv3 をサポートしている場合は、SNMPv3 を使用して Cisco EPN Manager サーバーと通信するようにデバイスを設定します。次の手順は、新しいデバイスを追加するときに SNMPv3 を指定する方法について説明しています。

デバイスの追加方法	SNMPv3 を指定する方法	詳細については、以下を参照してください。
1 つのデバイスの追加	[デバイスの追加（Add Device）] ダイアログボックスで、[SNMP プロパティ（SNMP Properties）] ページに移動し、[バージョン（Versions）] ドロップダウン リストから [v3] を選択します。	手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） （56 ページ）
複数のデバイスの追加（一括インポート）	CSV ファイルを編集するときは、次のように入力します。 • [SNMP バージョン（SNMP Version）] 列で **3** を入力します。 • [snmpv3_user_name]、[snmpv3_auth_type]、[snmpv3_auth_password]、[snmpv3_privacy_type]、および [snmpv3_privacy_password] の各列に適切な値を入力します。	CSV ファイルを使用したデバイスのインポート （55 ページ）

デバイスの追加方法	SNMPv3 を指定する方法	詳細については、以下を参照してください。
ディスカバリを使用した複数のデバイスの追加	[ディスカバリ設定（Discovery Settings）] ダイアログボックスで、[クレデンシャルの設定（Credential Settings）] エリアに移動し、[SNMPv3 クレデンシャル（SNMPv3 Credentials）] をクリックします。[+] 記号をクリックして、デバイス クレデンシャルを追加します。	カスタマイズされたディスカバリ設定でのディスカバリの実行（52 ページ）

始める前に

SNMPv3 をサポートするネットワーク デバイスで、（HMAC-SHA-96 などの適切なセキュリティ アルゴリズムを使用して）SNMPv3 が有効になっていることを確認します。

CLI を使用した外部認証の設定

ユーザー アカウントとパスワードを管理するには、RADIUS や TACACS+ などのセキュアな認証プロトコルで稼働する専用のリモート認証サーバーを使用することを推奨します。以下の手順に従って認証を設定することに加えて、外部認証ベンダーに連絡して、その他のセキュリティ強化案を問い合わせてください。

（注） ローカル ユーザー認証を使用することにした場合は、デフォルトのパスワード ポリシーを確認し、強化する必要があるかどうかを判断してください。ローカル認証のためのグローバル パスワード ポリシーの設定 （1027 ページ）を参照してください。

外部 AAA サーバーを使用してユーザーを認証するように Cisco EPN Manager を設定します。サーバーを設定は、Web GUI を使用しても、コマンドライン インターフェイス（CLI）を使用しても行えます。リモート ユーザー認証を GUI で設定する場合は、外部認証の設定 （1041 ページ）を参照してください。

CLI を使用して外部認証を設定するには、次の手順に従います。EPNM は CLI を介した TACACS+ の設定のみをサポート

ステップ 1 Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）の説明に従って、コマンド ラインを使用して、Cisco EPN Manager にログインします。

ステップ 2 コンフィギュレーション モードを開始します。

ステップ 3 次のコマンドを入力して外部認証 TACACS+ サーバーをセットアップします。

```
aaa authentication tacacs+ server tacacsIP key plain shared-secret
```

ここで、

- *tacacsIP* はアクティブな TACACS+ サーバーの IP アドレスです。
- *shared-secret* はアクティブな TACACS+ サーバーのプレーンテキストの共有秘密です。

ステップ 4 次のコマンドを入力して、管理者権限を持つユーザーを作成します。このユーザーは、前のステップで指定したサーバーによって認証されます。

```
username username password remote role admin [email emailID]
```

ここで、

- *username* はユーザー ID の名前です。
- *password* はユーザーのプレーンテキストのパスワードです。
- *emailID* はユーザーのメール アドレスです（オプション）。

ブルートフォース パスワード攻撃に対する SSH の強化

パスワード ベースの SSH 認証はブルート フォース攻撃に対して脆弱であるため、Cisco EPN Manager のインストール後に、承認されている公開キーのタイプ（PubkeyAcceptedKeyTypes）のいずれかに切り替えることをお勧めします。Cisco EPN Manager で承認されている公開キーのタイプ（PubkeyAcceptedKeyTypes）のリストは次のとおりです。

- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- ssh-ed25519-cert-v01@openssh.com
- ssh-rsa-cert-v01@openssh.com
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519

切り替えるには、次の手順を実行します。

ステップ 1 Linux CLI 管理者ユーザーとしてログインし、シェルにアクセスします。

ステップ 2 現在のユーザーを確認します。

```
# whoami
```

結果の出力は、Linux ルート ユーザーではなく、Linux 管理者ユーザーであることを示す必要があります。

ステップ 3 Cisco EPN Manager 管理者ユーザーの場合は、承認されている公開キー タイプ（PubkeyAcceptedKeyTypes）のいずれかを使用し、2048 ビット以上の強度を持つツール（puTTYgen など）を使用してキー ペアと SSH 文字列を作成します。

たとえば、次のように ed25519 を使用してキーを生成します。

```
$ ssh-keygen -t ed25519 -N ""
```

SSH 文字列は次のようになります。

```
ssh-ed25519 AAAAC3Nza... ......root@localhost.localdomain
```

ヒント 秘密キーをファイルに保存します。できれば、パスフレーズを使用して暗号化された形式で保存してください。また、パスフレーズを手元に置いてください。

ステップ 4 authorized_keys ファイルを作成し、適切なアクセス権限を Cisco EPN Manager 管理者ユーザーに割り当てます。

a) 管理者ユーザーのホームディレクトリで、.sshディレクトリを作成し、このディレクトリの読み取り、書き込み、および実行の権限を管理者ユーザーのみに割り当てます。

```
# cd ~
# mkdir .ssh
# chmod 700 ~/.ssh
```

b) 承認されたキー ファイルを作成します。

```
# cd .ssh
# vi authorized_keys
```

c) ステップ 3 で作成した SSH 文字列を authorized_keys ファイルにコピーして貼り付け、ファイルを保存します。

d) authorized_keys ファイルの読み取り、書き込み、および実行の権限を管理者ユーザーのみに割り当てます。

```
# chmod go= ~/.ssh/authorized_keys
# chmod u=rwx ~/.ssh/authorized_keys
```

e) authorized_kekys ファイルに適切なアクセス権を割り当てたことを確認します。

```
# ls -al
```

結果の出力は次のようになります。

```
total 6
drwx------. 2 admin gadmin 1024 May 10 00:25 .
drwx------. 6 admin gadmin 1024 May 10 00:24 .
-rwx------. 1 admin gadmin 398 May 10 00:25 authorized_keys
```

この例では、Linux 管理者ユーザーは `admin` という名前です

ステップ 5 bash シェルのルート ユーザーに切り替えます。

```
# sudo -i
```

ステップ 6 sshd_config ファイルを更新します。

a) /etc/ssh ディレクトリにある sshd_config ファイルの現在のバージョンと元のバージョンをコピーします。

```
# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig
```

b) vi エディタに sshd_config ファイルを開きます。

```
# vi /etc/ssh/sshd_config
```

c) 次のキーと値のペアを入力します。

```
Protocol 2
MaxAuthTries 3
PasswordAuthentication no
PermitRootLogin no
AuthenticationMethods publickey
PubkeyAuthentication yes
```

重要 デフォルトの sshd_config ファイルでは、これらのキーと値のペアの一部が既に指定されていることがあります。この場合は、次のいずれかを行います。

- 上記の値と一致しない値を変更します。
- 既存のキーと値のペアをコメントアウトし、新しい行に必要なエントリを指定します。

こうすることで、キーと値のペアの競合や重複を防ぐことができます。

d) ファイルを保存します。

ステップ 7 sshd をリロードします。

```
# systemctl reload sshd.service
```

注意 sshd は再起動しないでください。前述の設定手順のいずれかが適切に完了せず、sshd を再起動した場合は、SSH にアクセスできなくなります。現在の SSH セッションは維持されるため、sshd をリロードする方がはるかに安全です（必要な修正を行えるようにします）。

SSH 認証の構成が完了しました。設定が成功したことを確認するには、既存の SSH セッションを開いたままにして（何かを修正する必要がある場合に備えて）、この手順のステップ 3 で作成した秘密キーとパスフレーズを使用して新しい SSH セッションを開きます。

NTP の強化

Network Time Protocol（NTP）は、サーバーの日付と時刻の更新を認証します。NTP での時刻同期を実行するために、Cisco EPN Managerサーバーを設定することをお勧めします。ネットワーク全体の NTP 同期の管理で障害が発生した場合、異常な結果が発生する可能性があります。ネットワーク時刻精度の管理は組織のネットワーク アーキテクチャを含む広範囲の問題であり、このガイドの範囲外です。このトピックの詳細については、シスコ ホワイト ペーパー『Network Time Protocol: Best Practices』などを参照してください。

次の点に注意してください。

- NTP を使用すると、セキュリティ侵害に関連する障害が発生する可能性があるため、NTP バージョン 4（NTPv4）を使用して Cisco EPN Manager サーバーの NTP 機能を強化する必要があります。また、Cisco EPN Manager は NTPv4 には NTPv3 との後方互換性があるため、NTPv3 もサポートしています。
- Cisco EPN Manager には最大 5 台の NTP サーバーを設定できます。
- IPv6 のサポートは NTP では利用できません。

Cisco EPN Manager サーバーでの NTP のセットアップ

Network Time Protocol（NTP）を使用して、NTP サーバーを使用するサーバーとネットワークデバイス上のクロックを同期するには、まず Cisco EPN Manager 上に NTP をセットアップする必要があります。その実行方法については、サーバーでの NTP の設定 （968 ページ） を参照してください。

認証された NTP の更新の有効化

次の手順を実行し、認証された NTP の更新をセットアップします。

ステップ 1 Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）の説明に従って、コマンド ラインを使用して、Cisco EPN Manager にログインします。

ステップ 2 コンフィギュレーション モードを開始します。

ステップ 3 次のコマンドを入力して外部 NTPv4 サーバーをセットアップします。

```
ntp server serverIP ntp-key-id ntp-type password
```

ここで、

- *serverIP* は、使用する認証 NTPv4 サーバーの IP アドレスです。
- *ntp-key-id* は、NTPv4 サーバーの MD5 キー ID です。
- *ntp-type* は、プレーンまたはハッシュのいずれかにすることができます。
- *password* は NTPv4 サーバーの MD5 プレーン テキスト パスワードです。

次に例を示します。

```
ntp server 209.165.202.128 20 plain myPass123
```

または

```
ntp server 209.165.202.128 20 hash myPass123
```

ステップ 4 次のテストを実行して、NTP 認証が正しく動作していることを確認します。

a) NTP 更新の詳細を確認します。

```
show run
```

b) NTP 同期の詳細を確認します。

```
show ntp
```

NFS ベースの外部ストレージ サーバーの設定

NFS サーバーは、特にデータ バックアップの場合、Cisco EPN Manager のインストールで外部ストレージとして使用できます。NFS には組み込みのセキュリティがないので、NFS サーバーをセキュアにするために次のセキュリティ対策をできる限り多く実装する必要があります。

- NFS サーバーの前にファイアウォールを設定します。実質的にはこれを行うには、NFS がさまざまな設定ファイルで使用するポートを固定し、ファイアウォールの設定でこれらのポートを指定します。
- ポート マッパーを使用します。NFS サーバーで、特定の IP アドレスを含む NFS トランザクションのみ許可します。
- 感染した DNS 経由の攻撃を防ぐには、NFS を構成するときに（ドメイン名ではなく）IP アドレスのみ指定します。
- フォルダのエクスポートを設定する際に、/etc/exports ファイルで [root_squash] オプションを使用します。
- /etc/exports ファイルを設定する際に、[セキュア（secure）] オプションを使用します。
- バックアップ ステージングとストレージ フォルダを設定する際に、**nosuid** オプションと **noexec mount** オプションを使用します。

（注） ステージング フォルダを設定することは必須ではありません。

- ストレージ フォルダ（およびオプションのステージング フォルダ）に対して、ファイル アクセス許可値 [755]（すべてのユーザーに読み取りおよび書き込み特権を付与）を設定し、userid [65534]（システム権限を持っていないユーザー [nobody]）を所有者として設定します。
- SSH または SSL/TLS のいずれかを介して NFS トラフィックをトンネリングします。SSH の場合、ユーザー認証ではなく RSA キーベースの認証を使用します。

NFS ベースのストレージの安全性のためには、これらの対策の 1 つのみに頼らないでください。最善策は、状況に合わせて最適な対策の組み合わせを実装することです。また、このリストは網羅的なものではないことに注意してください。ストレージを強化するときは、高レベルの信頼を達成するために、事前に Linux システム管理者およびセキュリティ専門家と状況について相談することをお勧めします。

管理者ユーザーの作成

管理者ユーザーを作成するには、次の手順を実行します。

ステップ 1 Linux CLI 管理者ユーザーとしてログインし、シェルにアクセスします。

ステップ 2 次のコマンドを入力して、ユーザーを作成します。

次に例を示します。

```
admin(config)# username xyzabc password plain Text1234 role network-admin
```

それぞれの説明は次のとおりです。

- **xyzabc** には、必要なユーザー名を指定できます。
- **plain Text1234** には、プレーンテキストのパスワードを指定できます。
- **network-admin** には、ユーザーに割り当てられたロールを指定できます。

デフォルトでは、設定するパスワードには 6 文字以上の英数字を含める必要があります。大文字と小文字がそれぞれ 1 文字以上必要です。パスワードにユーザー名または cisco という単語を含めることはできません。パスワードポリシーを変更して、次の制限付きで特殊文字を含めることができます。

- パスワードが二重引用符で囲まれている場合は、特殊文字の %（パーセント）、,（カンマ）、<（小なり）、>（大なり）、|（パイプ）を使用できます。例：**「Test123%|」**。
- 特殊文字の "（引用符）、?（疑問符）、\（バックスラッシュ）、`（抑音アクセント）は、パスワードフィールドではサポートされていません。
- その他の特殊文字（#（ハッシュ）、*（アスタリスク）、:（コロン）など）は、二重引用符で囲まずに使用できます。

CSDL プロセス

Cisco EPN Manager の開発は、シスコ セキュア開発ライフサイクル（CSDL）プロセスに準拠しています。これは、製品とインストールのセキュリティを向上させるために、開発から展開までの期間全体を対象としています。Cisco EPN Manager の製品設計は、特定の基準に対するセキュリティの観点からレビューされ、製品はセキュリティ ツールとテスト方法を使用してテストされます。さらに、Cisco EPN Manager は外部のセキュリティ専門家や侵入テストの担当者によってレビューされます。（Cisco EPN Manager の更新のライフサイクルの一般としての）セキュリティ修正の展開方法の説明については、「シスコのセキュリティ問題解決プロセス」

シスコのセキュリティ問題解決プロセス

欠陥と脆弱性には、顧客が見つけたものとシスコが発見したものの 2 つのタイプがあります。Cisco EPN Manager についてシスコがそれらにどのように対処しているかについて説明します。

顧客が見つけた欠陥と脆弱性

1. Cisco Technical Assistance Center（TAC）を使用して顧客がサービス要求を行った後、Cisco TAC は Cisco Defect and Enhancement Tracking System（CDETS）障害レポートを開くことができるサポート チーム（問題に応じて異なる）と共にケースを開きます。

2. シスコは欠陥を評価し、その欠陥が Cisco EPN Manager にセキュリティ上のリスクをもたらすかどうかを判断します。この欠陥がセキュリティにリスクをもたらす場合、シスコは脆弱性として分類します。それ以外の場合、シスコは欠陥をソフトウェアの通常の欠陥として扱います。
3. シスコでは、次のいずれかを実行します。
   - セキュリティの脆弱性については、シスコは Cisco Product Security Incident Response Team（PSIRT）に報告し、Cisco PSIRT ガイドラインに準拠した修正プログラムを開発して Cisco PSIRT がクライアントへの脆弱性の開示とパッチの配信の両方を処理できるようにします。
   - 欠陥の場合、シスコはその重大度を判断し、修正プログラムのリリースをスケジュールします。

シスコが発見した欠陥と脆弱性

Cisco EPN Manager のバージョンの販売終了日から 1 年間、シスコは TACS または Cisco.com Web サイトを通じて報告された重大なバグとセキュリティ上の脆弱性に対するバグ修正、メンテナンス リリース、対応策、またはパッチを提供します。

二要素認証

二要素認証機能は、Cisco EPN Manager にログインするための 2 段階認証プロセスを提供します。Cisco EPN Manager は、RADIUS プロトコルを使用した Cisco ACS サーバー経由のユーザーの二要素認証をサポートしています。Cisco ACS は、外部データベースとして RSA SecurID サーバーをサポートしています。

二要素認証は、ユーザーの PIN と個別に登録された RSA SecurID トークンの 2 段階の検証で構成されます。ユーザーが PIN とともに正しいトークンコードを入力すると、認証が成功し、ユーザーは Cisco EPN Manager へのログインが許可されます。

Cisco EPN Manager で二要素認証を有効にするための前提条件

- Cisco EPN Manager：バージョン 3.0.1 以降
- 有効なライセンスがある Cisco ACS サーバー：バージョン 5.x
- 有効なライセンスがある RSA サーバー：バージョン 8.4
- RSA クライアントツール：最新バージョン

Cisco EPN Manager での二要素認証の有効化

Cisco EPN Manager で二要素認証を有効にするには、次のタスクを実行します。

- 二要素認証向けの RSA サーバーの設定 （923 ページ）

• RSA サーバーと Cisco ACS サーバーの同期 （924 ページ）
• Cisco ACS サーバーにクライアントとして Cisco EPN Manager を追加する （926 ページ）
• Cisco EPN Manager での RADIUS サーバーの詳細の追加 （926 ページ）

二要素認証向けの RSA サーバーの設定

Cisco Secure ACS は、外部データベースとして RSA SecurID サーバーをサポートしています。

RSA SecurID の二要素認証は、ユーザーの個人識別番号（PIN）と、タイムコードアルゴリズムに基づいて使い捨てのトークンコードを生成する、個別に登録された RSA SecurID トークンで構成されます。

異なるトークンコードが固定間隔（通常は 30 または 60 秒ごと）で生成されます。RSA SecurID サーバーでは、この動的な認証コードが検証されます。各 RSA SecurID トークンは固有であり、過去のトークンに基づいて将来のトークンの値を予測することはできません。

Cisco ACS 5.x サーバーを、RADIUS プロトコルを介した RSA SecurID サーバー認証と統合できます。

二要素認証のために RSA サーバーを設定するには、次のタスクを実行します。

• RSA サーバーへのユーザーの追加 （923 ページ）
• RSA サーバーでのユーザーへのトークンの割り当て （924 ページ）

RSA サーバーへのユーザーの追加

RSA サーバーにユーザーを追加するには、次の手順を実行します。

ステップ 1 セキュリティコンソールで、**[ID（Identity）] > [ユーザー（Users）] > [新規追加（Add New）]** をクリックします。

ステップ 2 [管理制御（Administrative Control）] セクションで、[セキュリティドメイン（Security Domain）] ドロップダウンリストから、[システムドメイン（System Domain）] を選択します。

ステップ 3 [ユーザーの基本設定（User Basics）] セクションで、次の手順を実行します。

a) （オプション）[名（First Name）] フィールドに、ユーザーの名を入力します。255 文字以下にする必要があります。
b) （オプション）[ミドルネーム（Middle Name）] フィールドに、ユーザーのミドルネームを入力します。255 文字以下にする必要があります。
c) [姓（Last Name）] フィールドに、ユーザーの姓を入力します。255 文字以下にする必要があります。
d) [ユーザーID（User ID）] フィールドに、ユーザーのユーザー ID を入力します。ユーザー ID は 48 文字以下にする必要があります。

ステップ 4 [パスワード（Password）] セクションで、次の手順を実行します。

a) [パスワード（Password）] フィールドに、ユーザーのパスワードを入力します。これは、ユーザーのアイデンティティ ソース パスワードです。

b) [パスワードの確認（Confirm Password）] フィールドに、[パスワード（Password）] フィールドに入力したパスワードを入力します。

ステップ 5 [アカウント情報（Account Information）] セクションで、次の手順を実行します。

a) [アカウントの開始（Account Starts）] ドロップダウンリストで、ユーザーのアカウントをアクティブにする日付と時刻を選択します。タイムゾーンは、ローカルシステム時刻によって決定されます。

b) [アカウントの有効期限（Account Expires）] ドロップダウンリストで、ユーザーのアカウントが期限切れになる日付と時刻を選択するか、または有効期限なしでアカウントを設定します。タイムゾーンは、ローカルシステム時刻によって決定されます。

ステップ 6 [保存（Save）] をクリックします。

RSA サーバーでのユーザーへのトークンの割り当て

トークンを割り当てると、そのトークンが特定のユーザーに関連付けられます。トークンをユーザーに割り当てるには、次の手順を実行します。

始める前に

トークンを割り当てるユーザーごとに、RSA サーバーにアクティブなユーザーレコードが存在することを確認します。

ステップ 1 セキュリティコンソールで、**[ID（Identity）]** > > **[ユーザー（Users）]** > **[既存の管理（Manage Existing）]** をクリックします。

ステップ 2 検索フィールドを使用して、トークンを割り当てるユーザーを検索します。

ステップ 3 検索結果から、トークンの割り当て先となるユーザーをクリックします。

ステップ 4 コンテキストメニューの [SecurID トークン（SecurID Token）] の下で、[追加の割り当て（Assign More）] をクリックします。

ステップ 5 [ユーザーに割り当て（Assign To Users）] ページの使用可能な RSA SecurID トークンのリストから、[フリーのSecureIDソフトウェアトークン（Free SecureID Software Token）] チェックボックスをオンにします。

ステップ 6 [**割り当て（Assign）**] をクリックします。

RSA サーバーと Cisco ACS サーバーの同期

RSA サーバーと Cisco ACS サーバーを同期するには、次のタスクを実行します。

- RSA サーバーでの設定ファイルの生成 （925 ページ）
- Cisco ACS サーバーでの RSA サーバーの設定 （925 ページ）

RSA サーバーでの設定ファイルの生成

この手順では、RSA SecurID サーバー管理者が認証エージェントとコンフィギュレーション ファイルを作成する方法について説明します。認証エージェントは、RSA データベースにアクセスする権限を持つデバイス、ソフトウェア、またはサービスのドメインネームサーバー（DNS）名と IP アドレスです。コンフィギュレーション ファイルには、RSA トポロジと通信について記述します。Cisco ACS サーバーの設定作業を完了するために必要な sdconf.rec ファイルを生成するには、次の手順に従います。従います。

ステップ 1 RSA セキュリティコンソールで、**[アクセス（Access）]** > > **[認証エージェント（Authentication Agents）]** > **[新規追加（Add New）]** の順に移動します。

ステップ 2 [新規認証エージェントの追加（Add New Authentication Agent）] ウィンドウで、追加する各エージェントの [ホスト名（Hostname）] と [IP アドレス（IP Address）] を定義します。

ステップ 3 [Authentication Agent Attributes] ウィンドウで、[Agent Type] を [Standard Agent] として定義します。

ステップ 4 [Access] > [Authentication Agents] > [Generate Configuration File] に移動して sdconf. rec ファイルを生成し、[Generate Configuration File] をクリックします。[Maximum Retries] と [Maximum Time Between Each Retry] については、デフォルト値を使用します。

ステップ 5 [Download Now] をクリックしてコンフィギュレーションファイルをダウンロードします。画面に指示が表示されたら、[Save to Disk] をクリックして、ZIP ファイルのローカルコピーを保存します。.zip ファイルには、実際の設定である sdconf. rec ファイルが含まれています。

Cisco ACS サーバーでの RSA サーバーの設定

この手順では、sdconf.rec コンフィギュレーション ファイルを取得し、Cisco ACS サーバーに送信する方法について説明します。

始める前に

RSA サーバーで sdconf.rec ファイルを生成したことを確認します。

ステップ 1 Cisco Secure ACS バージョン 5.x コンソールで、**[Users And Identity Stores]** > **[External Identity Stores]** > **[RSA SecurID Token Servers]** に移動し、[Create] をクリックします。

ステップ 2 RSA サーバーの名前を入力し、RSA サーバーからダウンロードされた sdconf.rec ファイルを参照します。

ステップ 3 ファイルを選択して [送信（Submit）] をクリックします。

ステップ 4 **[Access Policies]** > **[Identity]** > **[Select]** に移動して RSA サーバーをマッピングし、チェックボックスの [Single result Selection] をオンにします。[Identity Source] フィールドで、RSA サーバーの名前を選択し、[Select] をクリックします。

ステップ 5 認証要求を転送するように RADIUS クライアントデバイスを設定します。**[Users and Identity Stores]** > **[External Identity Stores]** > **[RADIUS Identity Servers]** に移動します。

ステップ 6 [General] タブで、RSA RADIUS ID サーバーの名前を入力します。[Primary Server] 領域の下で、[Hostname AAA]、[Shared Secret]、[Authentication port]、[Server Timeout]、[Connection Attempts] の各フィールドにサーバーの詳細を入力します。

Cisco ACS サーバーにクライアントとして Cisco EPN Manager を追加する

ステップ 1 管理ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ネットワーク リソース（Network Resources）]** > > **[ネットワーク デバイス（Network Devices）]** > **[ネットワーク デバイスおよび AAA クライアント（Network Devices and AAA Clients）]** の順に選択します。

ステップ 3 [ネットワーク デバイス（Network Devices）] ページで [作成（Create）] をクリックします。

ステップ 4 Cisco EPN Manager サーバーのデバイス名と IP アドレスを入力します。

ステップ 5 認証オプションとして [RADIUS] を選択し、共有秘密を入力します。

この共有秘密は、Cisco EPN Manager で Cisco ACS サーバーを RADIUS サーバーとして追加したときに入力した共有秘密と

必ず一致するようにします。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco EPN Manager での RADIUS サーバーの詳細の追加

Cisco EPN Manager で Cisco ACS サーバーの詳細を追加し、RADIUS モードを設定するには、次の手順を使用します。

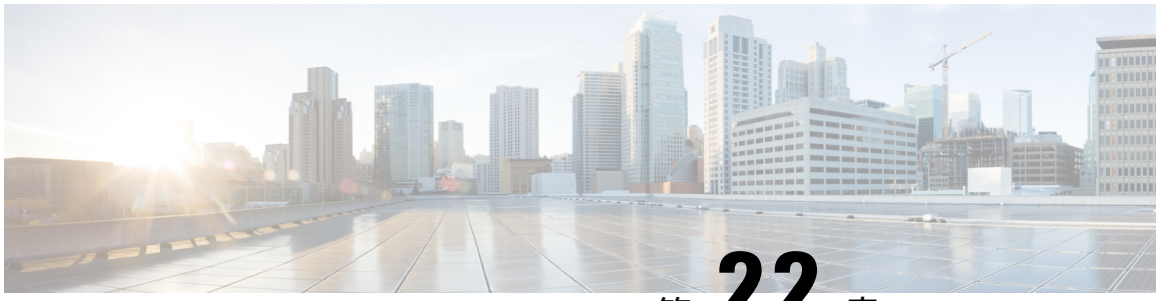
- Cisco EPN Manager への RADIUS または TACACS+ サーバーの追加 （1041 ページ）
- Cisco EPN Manager サーバー上で RADIUS または TACACS+ モードを設定する （1042 ページ）

二要素認証のワークフロー

Cisco EPN Manager 二要素認証ワークフローの手順を以下に示します。

1. Cisco EPN Manager への最初のログインでは、RSA サーバーで定義されたモード（user-defined-pin または pin-generated-by-system）に基づいて、ユーザーが覚えておく必要がある固有の PIN が生成されます。ユーザーは RSA SecurID クライアントツールでこの PIN を入力して RSA SecureID トークンを生成します。

2. Cisco EPN Manager のログインページで、ユーザーはユーザー名と RSA SecureID トークン（ステップ 1 で生成したもの）を入力します。
3. Cisco EPN Manager は、RADIUS プロトコルを介して Cisco ACS サーバーにユーザー名とトークンの詳細を含むログイン要求を送信します。
4. Cisco ACS サーバーは、RSA サーバーにログイン要求を転送します。
5. RSA サーバーはユーザーの詳細を認証し、Cisco ACS サーバーに対して正常なユーザー認証を確認します。
6. Cisco ACS サーバーは、設定されている認証プロファイルとユーザーを照合し、ユーザーが Cisco EPN Manager にログインできるようにします。



第 22 章

バックアップと復元

バックアップと復元の概念

バックアップ タイプ：アプリケーションとアプライアンス

Cisco EPN Manager は次の 2 種類のバックアップをサポートしています。

- アプリケーション バックアップ：これには、Cisco EPN Manager アプリケーション データが含まれますが、プラットフォーム データ（サーバーのホスト名や IP アドレスなどのホスト固有の設定）は含まれません。アプリケーションデータのみを移動し、プラットフォーム/ホスト固有の設定は移動しない場合は、Cisco EPN Manager のアップグレード時にアプリケーション バックアップを使用する必要があります。
- アプライアンス バックアップ：すべてのアプリケーションデータとプラットフォームデータ（ホスト名、IP アドレス、サブネット マスク、デフォルト ゲートウェイなどのホスト固有の設定）が含まれます。障害回復（またはプラットフォームのハードウェアまたはソ

フトウェア障害からの回復）の場合はアプライアンス バックアップを使用する必要があります。たとえば、ディスクまたはファイルシステムの障害から回復するには、標準の回復プロセスでは Cisco EPN Manager を再インストールしてからアプライアンスのバックアップを復元し、すべてのデータとプラットフォーム固有の設定を復元します。その後、アプライアンスのバックアップに含まれていない HA の設定を手動で再構築する必要があります。

（注） 何をアプリケーション データと見なすか、何をプラットフォーム データと見なすかの詳細については、バックアップされる情報 （933 ページ）を参照してください。

アプリケーションとアプライアンス バックアップについては、次の点に注意してください。

- ハードウェアとソフトウェアの構成が元のホストでの構成と同じであれば、アプリケーションおよびアプライアンスバックアップは、バックアップを作成した同じホストまたは新しいホストのどちらに復元することもできます。
- アプライアンスのバックアップは、バックアップを作成した元のサーバーと同じバージョンの Cisco EPN Manager サーバー ソフトウェアを実行しているホストにのみ復元できます。
- それ以降のバージョンの Cisco EPN Manager にアップグレードする場合、アプリケーションのバックアップと復元は、アップグレードパスがサポートされている限り異なるリリース間で実行できます。
- アプライアンスの復元コマンドを使用してアプリケーションのバックアップを復元することはできません。アプリケーションの復元コマンドを使用してアプライアンスのバックアップを復元することもできません。

次のベスト プラクティスを推奨します。

- Cisco EPN Manager を評価中の場合、ローカル リポジトリへのデフォルトの自動アプリケーション バックアップを使用します。
- 仮想アプライアンスとして実稼働環境で Cisco EPN Manager を実行中の場合は、アプリケーション バックアップを定期的に実行してリモート バックアップ サーバーに保管します。アプリケーション バックアップは、サーバー ハードウェアの完全な故障を除くすべての障害に対してサーバーを復元するために使用できます。

バックアップのスケジューリング

Cisco EPN Manager は自動で定期的にアプリケーション バックアップを実行します。この機能はデフォルトで有効になっていて毎日 1 つのアプリケーション バックアップ ファイルをデフォルトのローカル バックアップ リポジトリに作成します。

必要に応じてこのスケジュールを変更できます。また、随時、Web GUI から自動アプリケーション バックアップを実行できます。アプライアンス バックアップは、コマンド ラインからしか実行できません。

自動アプリケーション バックアップは、バックアップ リポジトリが Cisco EPN Manager サーバーに対してローカルな場合に保存スペースの問題を引き起こす可能性があります。このことはテスト実装ではあまり問題になりませんが、実稼働環境のリモート サーバーに対する定期バックアップの代用として使用することはできません。

実稼働環境では、次のことをお勧めします。

- バックアップ ファイルを保管するようにリモート リポジトリをセットアップする。
- 自動定期アプリケーション バックアップを使用して、定期的にリモート リポジトリ上でバックアップを作成する。

スケジュールされたバックアップを使用している場合でも、コマンドラインを使用してアプリケーションまたはアプライアンスのバックアップをいつでも作成できます。

（注） デフォルトでは、ジョブ作成のジョブ実行時間に 2 分が追加されます。

バックアップ リポジトリ

自動アプリケーション バックアップ機能は、デフォルトで、ローカル バックアップ リポジトリの **/localdisk/defaultRepo** にバックアップ ファイルを保存します。Web GUI を使用して新しいローカル バックアップ リポジトリを作成しておき、自動アプリケーション バックアップを設定するときにそれを選択できます。リモート リポジトリも指定できますが、まず、リポジトリのセットアップと管理（935 ページ）の説明に従ってリポジトリを作成しておく必要があります。

コマンド ラインを使用してアプリケーションまたはアプライアンス バックアップを作成する場合、バックアップを保存するローカルまたはリモート リポジトリを指定する必要があります。実稼働環境では、通常、NFS、SFTP、または FTP でアクセスするリモート リポジトリです。NFS は通常は他のプロトコルより高速で信頼性が高いので、NFS を使用することを推奨します。

アプリケーション バックアップは、コマンド ラインと Web GUI のどちらから実行しても違いはありません。どちらの操作によっても、同じバックアップ ファイルが作成されます。

NFS を使用してバックアップの作成やリモート バックアップからのデータの復元を行う場合は、バックアップや復元の操作中、マウントされた NFS サーバーが、常にアクティブになるようにしてください。プロセスのいずれかの時点で NFS サーバーがシャットダウンした場合、バックアップや復元の操作は、警告やエラー メッセージなしで異常終了します。

バックアップ ファイル名

Web GUI から開始されるアプリケーション バックアップ：自動または手動のいずれかで次の形式のファイル名が割り当てられます。

*host-yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_APP_CK*checksum*.tar.gpg

CLI から開始されるアプリケーション バックアップでは、同じ形式が使用されますが、ファイルがサーバー名ではなくユーザーの指定したファイル名から始まる点が異なります。

filename-*yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_APP_CK*checksum*.tar.gpg

CLI から開始されるアプライアンス バックアップのファイルもユーザーの指定したファイル名から始まりますが、形式は APP ではなく SYS です。

filename-*yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_**SYS**_CK*checksum*.tar.gpg

次の表に、バックアップ ファイルで使用される変数の説明を示します。

変数	説明
host	バックアップが作成されたサーバーのホスト名（Web GUI から開始されるアプリケーション バックアップの場合）
filename	コマンドラインでユーザーが指定したファイル名（CLI から開始されるアプリケーション バックアップおよびアプライアンス バックアップの場合）
yymmdd-hhmm	バックアップが作成された日時
ver	内部バージョン
size	バックアップの合計サイズ
cpus	バックアップが作成されたサーバーの CPU の総数
target	バックアップが作成されたサーバーのシステム メモリの合計量
ram	バックアップが作成されたサーバーの RAM の合計量
swap	バックアップが作成されたサーバーのスワップ ディスクの合計サイズ
checksum	バックアップ ファイルのチェックサム

バックアップ検証プロセス

Cisco EPN Manager は次の処理を行って、バックアップ ファイルを検証します。

1. バックアップ プロセスを開始する前に、ディスク サイズ、高速リカバリ領域、制御ファイルを検証します。
2. 復元可能であることを確認するために、作成されたバックアップ データベースを検証します。

3. バックアップされたファイルに対して、圧縮されたアプリケーション データを検証します。
4. TAR ファイルを検証して、ファイルが正しく完全であることを確認します。
5. GPG ファイルを検証して、ファイルが正しいことを確認します。

バックアップ ファイルを手動で転送する場合やバックアップ ファイルの転送が完了したことを検証する場合は、ファイルの md5CheckSum とファイル サイズを参照してください。

バックアップを検査するもう 1 つのベスト プラクティスは、それを Cisco EPN Manager のスタンドアロンの「test」インストール環境に復元することです。

バックアップされる情報

次の表に、バックアップ ファイルに含まれる情報に関する説明を示します。この情報は、バックアップからサーバーに復元されます。

バックアップ メカニズムによって保存されないデータに関する詳細については、バックアップされない情報 （935 ページ）を参照してください。

（注） /opt/CSCOlumos/conf/Migration.xml ファイルには、バックアップされたすべてのコンフィギュレーション ファイルとレポートが含まれています。このファイルがバックアップに含まれており、復元されます。

データ タイプ	機能	保存および復元される情報

アプリケーションデータ	バックグラウンドジョブの設定	データベース内のデータ
	設定アーカイブ（デバイスコンフィギュレーション ファイル）	データベース内のデータ
	構成テンプレート	• /opt/CSCOlumos 内のファイル： • /conf/ootb • /xmp_inventory/dar/customized-feature-parts/CONFIGURATION • データベース内のデータ
	資格情報	データベース内のデータ
	デバイスインベントリ データ	データベース内のデータ
	ライセンス	/opt/CSCOlumos/licenses 内のファイル
	マップ（Maps）	• /opt/CSCOlumos/domainmaps 内のファイル • データベース内のデータ
	レポート	• /localdisk/ftp 内のファイル： • /reports • /reportsOnDemand • データベース内のデータ
	管理対象デバイスのソフトウェアイメージ ファイル	データベース内のデータ
	システム設定	データベース内のデータ
	ユーザー設定	• /opt/CSCOlumos/conf/wap/datastore/webacs/xml/prefs 内のファイル • データベース内のデータ
	CEPNM ユーザー、グループ、およびロール	データベース内のデータ

	仮想ドメイン	データベース内のデータ
プラットフォーム データ	CLI 設定	すべての CLI 情報と設定が保持されます。これには、バックアップ リポジトリのリスト、FTP ユーザー名、CLI を使用して作成したユーザー、CLI 経由で指定した AAA 情報、その他の CLI 設定（端末タイムアウトなど）が含まれます。
	資格情報	Linux OS クレデンシャル ファイル
	ネットワーク設定（Network settings）	/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml 内のファイル
	Linux ユーザー プリファレンス	Linux データ構造
	Linux ユーザー、グループ、およびロール	Linux データ構造

バックアップされない情報

バックアップを実行する前に、次の情報を手動でメモする必要があります。これは、これらの情報がバックアップ プロセスの一部として保存されないためです。データの復元後にこれらの設定を再構成する必要があります。

- ハイ アベイラビリティ設定
- ローカル カスタマイズ（レポート ヒープ サイズなど）

パッチ履歴情報も保存されません。

バックアップされる情報のリストについては、バックアップされる情報（933 ページ）を参照してください。

リポジトリのセットアップと管理

Cisco EPN Manager は次のリポジトリ タイプをサポートしています。

- リモート リポジトリ：NFS、FTP、SFTP

これら異なるタイプのリポジトリをセットアップおよび管理する方法については、以降のトピックを参照してください。

ローカル バックアップ リポジトリの作成

Cisco EPN Manager は、デフォルトのローカル バックアップ リポジトリ **/localdisk/defaultRepo** にバックアップ ファイルを自動的に保存します。必要に応じて、別のローカル バックアップ リポジトリを作成して、それを使用することができます。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）]** > **[インフラストラクチャ（Infrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] 一覧で、[サーバーのバックアップ（Server Backup）] チェックボックスをオンにします。

ステップ 4 [編集（Edit）]（鉛筆アイコン）をクリックして、[ジョブ プロパティの編集（Edit Job Properties）] ダイアログボックスを開きます。

ステップ 5 [ジョブ プロパティの編集（Edit Job properties）] ダイアログボックスを使用して、新しいローカル リポジトリを作成します。

1. [作成（Create）] をクリックします。[バックアップ リポジトリの作成（Create Backup Repository）] ダイアログボックスが開きます。
2. 作成するローカル リポジトリの名前を入力します。
3. バックアップをパスワードで保護する場合は、パスワードを入力します。

   （注） バックアップを復元するには、パスワードを覚えておく必要があることに注意してください。

4. FTP リポジトリの場合は、[FTP] チェックボックスをオンにし、場所とクレデンシャルを入力します。
5. [送信（Submit）] をクリックします。新しいリポジトリが、[ジョブ プロパティの編集（Edit Job properties）] ダイアログボックスの [バックアップ リポジトリ（Backup Repository）] ドロップダウン リストに追加されます。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 今後の自動アプリケーション バックアップにリポジトリを使用する場合は、自動バックアップ用のバックアップ リポジトリの指定 （943 ページ）の説明に従ってそれを指定します。

リモート バックアップ リポジトリの使用

実稼働環境では、ネットワーク管理データがハードウェアやサイトの障害から保護されるように、バックアップにリモート リポジトリを使用することをお勧めします。ほとんどの場合、これは次のことを行う必要があることを意味します。

1. Cisco EPN Manager バックアップ ファイルを保持するための 1 つ以上のリモート リポジトリを作成します。組織でまだリモート バックアップ サーバーを使用していない場合は、独自にセットアップする必要があります。
2. 自動アプリケーション バックアップの保存先としてリモート リポジトリを指定します。

3. 必要な場合、自動アプリケーションバックアップの間隔とその実行時刻を指定します。リモート リポジトリに保存された自動アプリケーション バックアップをモニターして、手動でアーカイブする必要があります（[保持する最大バックアップ数（Max backups to keep）] の設定はリモート リポジトリには適用されないため）。
4. CLI バックアップ コマンドを使用してアプリケーションまたはアプライアンス バックアップを実行する場合は、バックアップ先としてリモート リポジトリを指定します。

リモート アクセスを計画しているリソースと同様に、セットアップ時に正しいサーバー IP アドレスとログイン クレデンシャルを指定することが、リモート バックアップ リポジトリと Cisco EPN Manager の使用を成功させる秘訣です。

リモート NFS バックアップ リポジトリの使用

NFS ベースのリモート バックアップ リポジトリを使用するには、NFS ファイル サーバー（ファイル システム内の指定されたフォルダをクライアントにエクスポートする）と Cisco EPN Manager（サーバーのクライアントとして機能する）が必要です。Cisco EPN Manager システムは、エクスポートされたフォルダをマウントし、他のローカル フォルダと共に、それらを Cisco EPN Manager サーバーで使用できるようにします。これをセットアップするには、次の 3 つのタスクを実行します。

1. バックアップをステージングし、保存する NFS サーバー上に 2 つのフォルダのパスを指定した後、これらのパスをエクスポートするように NFS サーバーを設定します。これは Cisco EPN Manager のセットアップの範囲外であるため、このタスクは NFS サーバーのシステム管理者が実行する必要があります。
2. Cisco EPN Manager をセットアップし、指定したフォルダのステージングと保存を使用します。これは、Cisco EPN Manager 管理者が実行する必要があります。
3. NFS サーバーと Cisco EPN Manager 間のセキュアな通信は、NFS がそれ自体ではセキュアでないため、極めて重要です。これは、NFS とそのインストールに伴うセキュリティ上の問題を確実に理解している Linux 管理者が実行する必要があります。NFS の強化に関するヒントについては、「NFS ベース ストレージの強化」を参照してください。

NFS バックアップ設定をセットアップする前に

設定を始める前に、次の点を確認してください。

- バックアップをステージングして保存する NFS サーバーの IP アドレスを知っていること。ステージング フォルダと保存フォルダは、同じ NFS サーバーに配置することも、別々の NFS サーバーに配置することもできます。ステージングと保存を別々の NFS サーバー上で計画している場合は、両方のサーバーの IP アドレスが必要です。
- NFS サーバー上のステージング フォルダと保存フォルダのパス名を知っていること。同じ NFS サーバー上でステージングおよび保存することを選択した場合は、ステージング フォルダと保存フォルダを違う名前にする必要があります。
- Cisco EPN Manager サーバー上のルート権限付き管理者ユーザー ID を持っていること。

- NFS サーバーの保存フォルダを指す Cisco EPN Manager サーバー上のリポジトリ名を選択していること。

NFS ベースのリモート リポジトリの設定

Cisco EPN Manager がバックアップに使用する NFS ベースのリモートリポジトリを設定するには、次の手順を実行します。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 バックアップ処理中に作成される一時ファイルをステージングする NFS リモートリポジトリを設定し、完了したバックアップファイルを保存します。

```
config# backup-staging-url nfs://Staging_Server_IP_Address:/Staging_Server_Path
config# repository repositoryName
config-Repository# url nfs://Storage_Server_IP_Address:/Storage_Server_Path
```

ここで、

- *Staging_cdg_Server_IP_Address* は、ステージングリポジトリがある NFS サーバーの IP アドレスです。
- *Staging_Server_Path* は、そのホスト NFS サーバー上のステージング リポジトリのフル パスです。
- *repositoryName* は、完了したバックアップ ファイルを保存するリモート リポジトリの名前です。
- *Storage_cdg_Server_IP_Address* は、ストレージリポジトリがある NFS サーバーの IP アドレスです。
- *Storage_Server_Path* は、そのホスト NFS サーバー上のストレージ リポジトリのフル パスです。

注意 *Staging_cdg_Server_IP_Address* および *Storage_cdg_Server_IP_Address* については IP アドレスのみを入力することをお勧めします。DNS サービスが侵害を受け、代わりに URL を入力した場合、悪意のある NFS サーバーにトラフィックをリダイレクトすることになる可能性があります。このため、やむをえず URL を指定する場合には、ローカル名の解決を使用するために（DNS サービスに依存する代わりに）Cisco EPN Managerを構成することをお勧めします。これは、[/etc/hosts] ファイルに NFS サーバーの名前と IP アドレスを入力することで行うことができます。そうすることでシステムのセキュリティを向上できます。

ステップ 4 コンフィギュレーション モードを終了します。

```
config-Repository# exit
config# exit
```

リモート FTP バックアップ リポジトリの使用

（注） リモート NFS リポジトリを使用することを推奨します。

リモート FTP サーバー上でバックアップ リポジトリを作成し、それを使用するように Cisco EPN Manager サーバーを設定できます。

バックアップをホストする FTP サーバーは、次の要件を満たしていれば、ネットワーク上のどこにでもセットアップできます。

- Cisco EPN Manager サーバーからアクセス可能な IP アドレスを持っている。
- ユーザー（FTP ユーザー）が FTP サーバー ディスクへの書き込みアクセス権を持っている。
- Cisco EPN Manager サーバー上で指定されたリポジトリ名と一致するローカル サブディレクトリが存在する。
- 16 文字以下のパスワードが設定されている。

これらの要件以外に、FTP バックアップ サーバー上で必要な設定はありません。

SFTP サーバーの詳細が Web GUI の [バックアップ リポジトリ（Backup Repository）] ドロップダウン リストに表示されるように、CLI を使用して FTP サーバーを設定する必要があります。FTP サーバーは CLI のみを使用して設定できます。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 リモート FTP サーバーへのシンボリック リンクを設定した後、設定モードを終了します。

```
config# repository repositoryName
config-Repository# url ftp://RemoteServerIP//sharedFolder
config-Repository# user userName password plain userPassword
config-Repository# exit
config# exit
```

ここで、

- *repositoryName* はリポジトリの名前です（**MyRepo**、**EPNManager** など）。
- *RemoteServerIP*は、共有バックアップ フォルダをホストする FTP サーバーの IP アドレスです。
- *sharedFolder* は、FTP サーバー上の共有バックアップ フォルダの名前です。
- *userName* は FTP サーバー上のリポジトリへの書き込み権限を持つユーザーの名前です。

- *userPassword* は、そのユーザーの対応するパスワードです。パスワードは 16 文字以下であることが必要です。

ステップ 4 シンボリック リンクの作成を確認します。

```
show repository repositoryName
```

次のタスク

手動バックアップを実行する場合、新しいリポジトリをバックアップ コマンドのレポジトリ名として指定します。次に例を示します。

```
backup MyBackupFileName repository MyRepo application NCS
```

このリポジトリを自動バックアップに使用する場合は、自動バックアップ用のバックアップ リポジトリの指定 （943 ページ）を参照してください。

リモート SFTP バックアップ リポジトリの使用

（注） リモート NFS リポジトリを使用することを推奨します。

リモート SFTP サーバー上でバックアップ リポジトリを作成し、それを使用するように Cisco EPN Manager サーバーを設定できます。

バックアップをホストする SFTP サーバーは、次の要件を満たしていれば、ネットワーク上のどこにでもセットアップできます。

- Cisco EPN Manager サーバーからアクセス可能な IP アドレスを持っている。
- ユーザーが SFTP サーバー ディスクへの書き込みアクセス権を持っている。
- バックアップが保存されるローカル共有フォルダが存在する。

これらの要件以外に、SFTP バックアップ サーバー上で必要な設定はありません。

SFTP サーバーの詳細が Web GUI の [バックアップ リポジトリ（Backup Repository）] ドロップダウン リストに表示されるように、CLI を使用して SFTP サーバーを設定する必要があります。SFTP サーバーは CLI のみを使用して設定できます。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 リモート SFTP サーバーへのシンボリック リンクを設定した後、設定モードを終了します。

```
config# repository repositoryName
config-Repository# url sftp://RemoteServerIP//sharedFolder
config-Repository# user userName password plain userPassword
config-Repository# exit
config# exit
```

ここで、

- *repositoryName* はリポジトリの名前です（**MyRepo**、**EPNManager** など）。
- *RemoteServerIP* は、共有バックアップ フォルダをホストする SFTP サーバーの IP アドレスです。上の例は、共有フォルダへの絶対パスを指定していることに注意してください。共有フォルダへの相対パスを指定するには、URL で 1 本のスラッシュのみを使用します（**url sftp://***RemoteServerIP/sharedfolder* など）。
- *sharedFolder* は、SFTP サーバー上の共有バックアップ フォルダの名前です。
- *userName* は SFTP サーバー上のリポジトリへの書き込み権限を持つユーザーの名前です。
- *userPassword* は、そのユーザーの対応するパスワードです。

ステップ 4 シンボリック リンクの作成を確認します。

```
show repository repositoryName
```

次のタスク

手動バックアップを実行する場合、新しいリポジトリをバックアップ コマンドのレポジトリ名として指定します。次に例を示します。

```
backup MyBackupFileName repository MyRepo application NCS
```

このリポジトリを自動バックアップに使用する場合は、自動バックアップ用のバックアップ リポジトリの指定 （943 ページ）を参照してください。

ローカル バックアップ リポジトリの削除

ローカル バックアップ リポジトリを削除するには、以下の手順に従います。この手順に従うことにより、管理インターフェイスで確実に更新済みの情報が使用されるようになります。

ステップ 1 Cisco EPN Manager CLI 管理ユーザーとしてサーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 2 ローカル アプリケーション バックアップ リポジトリを一覧表示し、削除するリポジトリを特定します。

```
show running-config | begin repository
```

ステップ 3 コンフィギュレーション モードを開始して、リポジトリを削除します。

```
configure terminal
(config)# no repository repositoryName
```

ステップ 4 ステップ 2 を繰り返して、リポジトリが削除されたことを確認します。

自動アプリケーション バックアップのセットアップ

インストール後、自動アプリケーションバックアップはデフォルトで有効になっています。スケジュールをカスタマイズしたり、別のバックアップリポジトリを指定したり、あるいは保存されるバックアップの数を調整したりできます。

どのデータがバックアップメカニズムによって保存されるかを確認する（およびバックアップされないデータを手動で保存する必要があるかどうかを確認する）には、以下のトピックを参照してください。

- バックアップされる情報 （933 ページ）
- バックアップされない情報 （935 ページ）

自動アプリケーション バックアップのスケジューリング

自動アプリケーション バックアップはデフォルトで有効になっていますが、これらのバックアップを実行する日付および間隔を調整できます。バックアップの実行は、リソースを消費するため、Cisco EPN Manager サーバーのパフォーマンスに影響します。トラフィックがピークの時間帯に自動バックアップが発生するスケジューリングは避けてください。

自動バックアップ アプリケーションが失敗すると、Cisco EPN Manager からバックアップ失敗アラームが（メジャーな重大度で）発生します。これらのアラームは他のアラームと同様に表示できます（アラームの検索および表示 （318 ページ）を参照）。

（注） 自動アプリケーション バックアップに失敗すると、それ以降、ログインしようとするたびにポップアップ メッセージが表示されます。このメッセージは、該当のアラームに対する確認応答をするまで、表示され続けます。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）] > [インフラストラクチャ（Infrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] リストで、[サーバーのバックアップ（Server Backup）] チェックボックスをオンにして、[スケジュールの編集（Edit Schedule）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが開きます。

ステップ 4 [スケジュール（Schedule）] ダイアログボックスで、開始日、繰り返し間隔、およびオプションの終了時間を選択します。

ステップ 5 [送信（Submit）] をクリックします。これらの設定が、今後の自動アプリケーション バックアップに使用されます。

自動バックアップ用のバックアップ リポジトリの指定

Cisco EPN Manager インターフェイスを使用して、自動アプリケーション バックアップ用の別のバックアップ リポジトリを指定できます。バックアップ リポジトリは、ローカルまたはリモートにすることができます。このインターフェイスを使用すれば、まだ存在しない新しいローカル バックアップ リポジトリを作成することもできます。

始める前に

自動バックアップ用のリモート リポジトリを使用するには、最初にリポジトリを作成する必要があります。ローカル リポジトリのみが、この手順を使用して作成できます。リポジトリのセットアップと管理 （935 ページ）を参照してください。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）]** > **[インフラストラクチャ（Infrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] のリストで、[サーバーのバックアップ（Server Backup）] チェックボックスをオンにします。

ステップ 4 [編集（Edit）]（鉛筆アイコン）をクリックします。[ジョブ プロパティの編集（Edit Job Properties）] ダイアログボックスが開きます。

ステップ 5 [バックアップ リポジトリ（Backup Repository）] ドロップダウン リストからリポジトリを選択し、[保存（Save）] をクリックします。Cisco EPN Manager は、次の自動アプリケーション バックアップを実行するときに新しいリポジトリを使用します。

保存する自動アプリケーション バックアップ数の変更

ローカル リポジトリに保存する自動アプリケーション バックアップの数を調整するには、この手順に従います。バックアップの数がこの手順で指定する数を超えると、Cisco EPN Manager は最も古いバックアップをリポジトリから削除します。

自動アプリケーション バックアップにリモート リポジトリが使用されている場合は、[保持する最大 UI バックアップ数（Max UI backups to keep）] 設定が適用されません。独自の方法を使用して、リモート リポジトリ上の古いバックアップをモニターし、アーカイブまたは削除する必要があります。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）] > [インフラストラクチャ（Infrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] 一覧で、[サーバーのバックアップ（Server Backup）] チェックボックスをオンにします。

ステップ 4 [編集（Edit）]（鉛筆アイコン）をクリックして、[ジョブ プロパティの編集（Edit Job Properties）] ダイアログボックスを開きます。

ステップ 5 [保持する最大 UI バックアップ数（Max UI backups to keep）] フィールドに値を入力してから、[保存（Save）] をクリックします。Cisco EPN Manager は、この設定を次のバックアップから適用します。

手動バックアップの実行

この項のトピックでは、手動アプリケーション バックアップまたは手動アプライアンス バックアップを実行する方法について説明します。

どのデータがバックアップ メカニズムによって保存されるかを確認する（およびバックアップされないデータを手動で保存する必要があるかどうかを確認する）には、以下のトピックを参照してください。

- バックアップされる情報 （933 ページ）
- バックアップされない情報 （935 ページ）

即時アプリケーション バックアップの実行

Cisco EPN Manager は、バックアップのスケジューリング （930 ページ）に記載されているように、自動アプリケーションバックアップを実行します。必要に応じて、次のトピックの説明に従って、手動でアプリケーション バックアップをトリガーできます。

Web GUI を使用した即時アプリケーション バックアップの実行

Web GUI を使用して即時アプリケーション バックアップをトリガーするには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）] > [インフラストラクチャ（Infrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] リストで [サーバーのバックアップ（Server Backup）] チェックボックスをオンにし、[実行（Run）] をクリックします。

ステップ 4 バックアップ ステータスを確認するには、テーブル上部までスクロールし、新しいジョブを見つけ、そのステータスと結果を確認します。

CLI を使用した即時アプリケーション バックアップの実行

CLI を使用して即時アプリケーション バックアップをトリガーするには、次の手順に従います。

ステップ 1 Cisco EPN Manager CLI admin ユーザーとしてサーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 2 バックアップのリストを表示します。ここで *repositoryName* はバックアップ リポジトリの名前です。

```
show repository repositoryName
```

ステップ 3 リモート バックアップを開始します。

```
backup filename repository repositoryName application NCS
```

ここで、filename は、アプリケーション バックアップ ファイルに付ける名前です（myBackup など）。ファイル名の長さは 26 文字です。その他の情報はファイル名に自動的に付加されます。バックアップ ファイル名 （932 ページ）を参照。

手動アプライアンス バックアップの実行

リモート リポジトリへのアプライアンスのバックアップを実行するには、次の手順に従います。NFS ベースのリモート リポジトリの設定 （938 ページ）の説明のように、リモート リポジトリを設定していることを確認します。

ステップ 1 リモート ホストが使用可能であることを確認します。

ステップ 2 admin として Cisco EPN Manager サーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 3 リモート バックアップを開始します。

```
(admin)# backup filename repository repositoryName
```

ステップ 4 バックアップ転送が完了していることを確認するため、md5CheckSum とファイル サイズを確認します。

Cisco EPN Manager データの復元

復元操作はすべて、CLI を使用して実行します。バックアップが実行されたホスト（ローカル ホスト）またはリモート ホストにデータを復元できます。バックアップは全体の復元のみが可能です（バックアップの一部のみを復元することはできません）。

詳細については、次のトピックを参照してください。

- アプリケーション バックアップの復元 （946 ページ）

• アプライアンス バックアップの復元 （946 ページ）

アプリケーション バックアップの復元

（注） アプライアンスのバックアップを復元するには、「アプライアンス バックアップの復元 （946 ページ）」の手順に従います。

アプリケーションのバックアップを復元するときは、同じサイズまたはより大きい OVA インストールに復元されることを確認します。OVA インストールが小さいと、復元は失敗します。

始める前に

高可用性を使用している場合、データを復元する前に「復元中の HA の削除 （1155 ページ）」のガイドラインを参照してください。

ステップ 1 Cisco EPN Manager CLI admin ユーザーとしてサーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 2 以前の復元の試行に失敗した場合、データベースが破損している可能性があります。次のコマンドを実行して、データベースを再作成します。

```
ncs run reset db
```

ステップ 3 保存済みのアプリケーション バックアップを一覧し、復元するバックアップを特定します。*repositoryName* は、バックアップ ファイルを格納しているリポジトリです。

```
show repository repositoryName
```

ステップ 4 vmWare vSphere クライアント（OVA）または Cisco IMC サーバー（ベア メタル）からデータを復元します。

```
restore backupFileName repository repositoryName application NCS
```

ステップ 5 Cisco Smart Licensing を使用している場合は、Cisco.com で Cisco Smart Software Manager（CSSM）に Cisco EPN Manager を再登録します。を参照してくださいCisco Smart Software Manager への Cisco EPN Manager の登録 （890 ページ）。

アプライアンス バックアップの復元

（注） アプリケーション バックアップを復元するには、アプリケーション バックアップの復元 （946 ページ） の手順を使用します。

アプライアンスのバックアップを復元するときは、同じサイズまたはより大きい OVA インストールに復元されることを確認します。OVA インストールが小さいと、復元は失敗します。

復元したサーバーの IP アドレス、サブネットマスク、デフォルト ゲートウェイを変更することが推奨されます。

- 復元したホストが古いホストと同じサブネット上に存在し、古いホストがまだアクティブのままである。
- 復元したホストが古いホストとは別のサブネット上に存在する。

始める前に

ハイアベイラビリティを使用している場合は、データを復元する前に復元中のHAの削除（1155ページ）の情報を参照してください。

ステップ 1 Cisco EPN Manager CLI admin ユーザーとしてサーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 2 以前の復元の試行に失敗した場合、データベースが破損している可能性があります。外部リポジトリに保存されているバックアップで、同じリリースを使用してセットアップを再インストールし、復元をやり直します。

ステップ 3 保存されているアプライアンス バックアップをリストし、復元するバックアップを指定します。*repositoryName* は、バックアップ ファイルが格納されているリポジトリです。

```
show repository repositoryName
```

ステップ 4 vmWare vSphere クライアント（OVA）または Cisco IMC サーバー（ベア メタル）からデータを復元します。

```
restore backupFileName repository repositoryName
```

ステップ 5 IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを変更するかどうかを決定します。

a) インストール環境が次の条件に該当するかどうかを確認します。

- 復元したホストが古いホストと同じサブネット上に存在し、古いホストがまだアクティブのままである。
- 復元したホストが古いホストとは別のサブネット上に存在する。

該当する場合は、次のステップを実行します。

b) 復元したサーバーで、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、およびオプションでホスト名を変更します。

c) サーバーの実行コンフィギュレーションに変更を書き込み、Cisco EPN Manager サービスを再起動します。次に例を示します。

```
configure terminal
(config)# int GigabitEthernet 0
(config-GigabitEthernet)# ip address IPAddress subnetMask
(config-GigabitEthernet)# exit
(config)# ip default-gateway gatewayIP
(config)# hostname hostname
```

```
(config)# exit
(admin)# write mem
(admin)# ncs stop
(admin)# ncs start
(admin)# exit
```

ステップ 6 Cisco Smart Licensing を使用している場合は、Cisco.com で Cisco Smart Software Manager（CSSM）に Cisco EPN Manager を再登録します。を参照してくださいCisco Smart Software Manager への Cisco EPN Manager の登録 （890 ページ）。

失敗した復元からの回復

復元が完了しなかったり、エラーが報告されたりすることがあります。復元が失敗した場合は、常に、データベース破損のリスクが伴い、それ以上の復元または再インストールができなくなることがあります。別の復元または再インストールを試行する前に、破損したデータベースを復元するには次の手順を実行します。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開きます（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 2 次のコマンドを入力して、破損したデータベースをリセットします。

```
ncs run reset db
```

バックアップおよび復元中のディスク容量に関する問題の管理

バックアップまたは復元時にディスクの問題が発生した場合は、バックアップと復元を使用した別の仮想アプライアンスへの移行 （949 ページ）の手順に従って十分なディスク領域を持つサーバーにインストールを移動します。

既存のシステムを復元した後に、バックアップを作成できない場合は、データベースの圧縮 （977 ページ） に記載されている手順に従ってディスク領域を解放し、正常なバックアップを作成します。**ncs cleanup** コマンドを使用した後もバックアップを作成できない場合は、リモート バックアップ リポジトリの使用 （936 ページ）の説明のように、バックアップにリモートリポジトリを使用します（NFS、FTP、または SFTP を使用）。

バックアップと復元を使用した別の仮想アプライアンスへの移行

以下の場合のように、既存の仮想アプライアンス（OVA サーバー インストール構成）から新しいインストール構成に Cisco EPN Manager データを移行する必要が生じることがあります。

- 致命的なハードウェア障害が発生した場合などは、古いサーバーを丸ごと交換します。この場合は、古いインストール メディアを使用して交換用サーバー上で新しいホストを作成し直してから、古いホストから新しいホストにアプリケーションデータを移行することができます。
- Cisco EPN Manager を使用してネットワークをさらに管理できるように、より大規模なまたはより強力なサーバーに移行します。この場合、OVA インストール ファイルが存在すること、および、より大きなサーバーにインストールできる機能を使用して、そのファイルを新しいサーバーにインストールできることを確認してから、古く小さいサーバーを取り外すことができます。その後で、古いホストからアプリケーションデータを移行できます。

いずれの場合も、古いホストから作成したアプライアンスバックアップまたはアプリケーションバックアップを新しいホストに復元することによって、比較的簡単に古いデータを新しい仮想アプライアンスに移行できます。

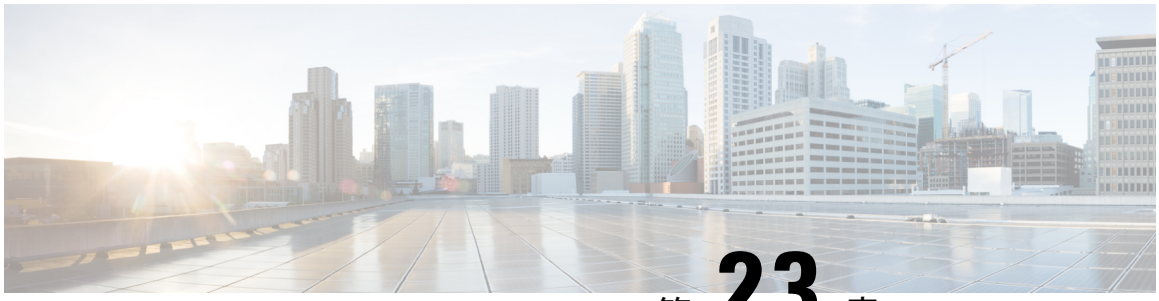
ステップ 1 まだ実行していない場合は、古いホストのリモート バックアップ リポジトリをセットアップします（リモート バックアップ リポジトリの使用 （936 ページ）を参照）。

ステップ 2 古いホストのアプリケーションバックアップを実行し、リモートリポジトリにバックアップを保存します（CLI を使用した即時アプリケーション バックアップの実行 （945 ページ）を参照）。

ステップ 3 新しいホストをインストールします（インストール手順は『Cisco Evolved Programmable Network Manager Installation Guide』に記載されています）。

ステップ 4 古いホストと同じリモートバックアップリポジトリを使用するように新しいホストを設定します（リモート バックアップ リポジトリの使用 （936 ページ）を参照）。

ステップ 5 リモートリポジトリ上のアプリケーションバックアップを新しいホストに復元します（アプリケーション バックアップの復元 （946 ページ）を参照）。



第 23 章

サーバーの正常性と構成

Cisco EPN Manager サーバーの構成の表示

現在のサーバー時間、カーネル バージョン、オペレーティング システム、ハードウェア情報などの Cisco EPN Manager サーバーの構成情報を表示するには、以下の手順を使用します。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム監視ダッシュボード（System Monitoring Dashboard）]** を選択します。

ステップ 2 [概要（Overview）] タブをクリックします。

ステップ 3 ダッシュボードの左上にある [システム情報（System Information）] をクリックして、[システム情報（System Information）] フィールドを展開します。

Cisco EPN Manager のホスト名の変更

Cisco EPN Manager では、サーバーへのインストール時にホスト名の入力を求めるプロンプトが表示されます。さまざまな理由により、Cisco EPN Manager サーバーに設定されたホスト名と他の場所に設定されたホスト名の間で不一致が発生することがあります。この問題は、Cisco EPN Manager を再インストールしなくてもサーバーでホスト名を変更すれば解決できます。次の手順を実行します。

（注） 状況によっては、ホスト名を変更した後にファイル `tnsnames.ora` と `listener.ora` でホスト名が正しく反映されていないことがあります。これを回避するには、作業を開始する前に次の手順を実行します。

1. プライマリサーバーとセカンダリサーバーで次のファイルのバックアップを作成します。
   - /base/product/12.1.0/dbhome_1/network/admin/tnsnames.ora
   - /base/product/12.1.0/dbhome_1/network/admin/listener.ora
   - /opt/oracle/templates/netcaxmp_prod.rsp
2. ホスト名を変更した後、3 つのバックアップファイルを使用して、新しく指定したホスト名が反映されるようにすべてのホスト名を編集します。
3. Oracle リスナーを再起動します（Cisco EPN Manager がダウンしている場合に Cisco EPN Manager の再起動が必要で、ステップ 2 を実行できる場合を除く）。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開き、**configure terminal** モードを開始します。

「CLI 経由の接続」を参照してください。

ステップ 2 次のコマンドを入力します。

```
Cisco_EPN_Manager_Server/admin(config)#hostname newHostName
```

newHostName には、Cisco EPN Manager サーバーに割り当てるホスト名を指定します。

ステップ 3 **ncs stop** および **ncs start** コマンドを使用して、Cisco EPN Manager サーバーを再起動します。

ステップ 4 SSL サーバー証明書用に設定されているホスト名を確認します。

- ホスト名がステップ 2 で指定したホスト名と同じであれば、ここで手順を終了します。

- ホスト名が違う場合は、ステップ 2 で指定したホスト名で新しい SSL サーバー証明書を作成し、インストールする必要があります。。

CLI 経由の接続

管理者は、コマンド ライン インターフェイス（CLI）経由で Cisco EPN Manager サーバーに接続できます。Cisco EPN Manager CLI 経由でのみアクセス可能なコマンドとプロセスを実行する場合は、CLI アクセス権が必要です。これらには、サーバーの起動および停止、ステータスの確認などを行うコマンドが含まれます。

始める前に

手順を開始する前に、次の点を確認してください。

- そのサーバーまたはアプライアンスへの CLI アクセス権を持っている管理ユーザーのユーザー ID とパスワードがわかっていること。明示的に禁止されていない限り、すべての管理ユーザーには CLI アクセス権が与えられます。
- Cisco EPN Manager サーバーの IP アドレスまたはホスト名がわかっていること。

ステップ 1 SSH クライアントを起動し、ローカル マシンのコマンド ラインから SSH セッションを開始するか、Cisco EPN Manager の物理アプライアンスまたは仮想アプライアンスの専用コンソールに接続します。

ステップ 2 該当する方法でログインします。GUI クライアントを使用している場合：CLI アクセス権を持つアクティブな管理者の ID と Cisco EPN Manager サーバーの IP アドレスまたはホスト名を入力します。その後で、接続を開始します。コマンドライン クライアントまたはセッションを使用している場合：[localhost]# ssh username@IPHost のようなコマンドを使用してログインします。username はサーバーへの CLI アクセス権を持つ Cisco EPN Manager 管理者のユーザー ID で、 IPHost は Cisco EPN Manager サーバーまたはアプライアンスの IP アドレスまたはホスト名です。コンソールを使用している場合：管理者ユーザー名を入力するためのプロンプトが表示されます。ユーザー名を入力します。

Cisco EPN Manager により、入力した管理者 ID のパスワードを要求されます。

ステップ 3 管理 ID パスワードを入力します。Cisco EPN Manager によって次のようなコマンド プロンプトが表示されます。

```
Cisco_EPN_Manager_Server/admin#
```

ステップ 4 コマンドを入力するために **configure terminal** モードを開始する必要がある場合は、プロンプトで次のコマンドを入力します。

```
Cisco_EPN_Manager_Server/admin#configure terminal
```

プロンプトが `Cisco_EPN_Manager_Server/admin#` から `Cisco_EPN_Manager_Server/admin/conf#` に変わります。

Cisco EPN Manager サーバーの接続の保護

データ セキュリティのため、Cisco EPN Manager は、標準の公開キー暗号化方式と Public Key Infrastructure（PKI）を使用して送信中のデータを暗号化します。インターネット上で、これらのテクノロジーに関する詳細情報を得ることができます。Cisco EPN Manager は、次の接続間で交換されるデータを暗号化します。

- Web サーバーと Web クライアント間
- CLI クライアントと Cisco EPN Manager CLI シェル インターフェイス間（SSH で処理）
- Cisco EPN Manager、AAA のようなシステム、および外部ストレージ間

Web サーバーと Web クライアント間の通信を保護するには、HTTPS メカニズムの一部として組み込まれる公開キー暗号化サービスを使用します。そのためには、Cisco EPN Manager Web サーバーの公開キーを生成し、それをサーバーに保存して、Web クライアントと共有する必要があります。これは、標準 PKI 証明書のメカニズムを使用して実現できます。このメカニズムを使用することによって、Web サーバーの公開キーを Web クライアントと共有するだけでなく、アクセスする Web サーバー（URL）に公開キーが必ず属することが保証されます。これにより、第三者が Web サーバーと見せかけて、Web クライアントが Web サーバーに送信する機密情報を収集することを防ぎます。

以下のトピックでは、Web サーバーを保護するために実行できるその他の手順について説明します。

- シスコでは、Cisco EPN Manager Web サーバーは証明書ベースの認証を使用して、Web クライアントを認証するようお勧めします。このセキュリティを強化する手順については、次を参照してください。 Web クライアントの証明書ベースの認証の設定 （1161 ページ）
- CLI クライアントと Cisco EPN Manager CLI インターフェイスの間の接続を保護するには、Cisco EPN Manager サーバーの強化 （1165 ページ）のセキュリティを強化する手順を参照してください。
- Cisco EPN Manager、AAA などのシステム、および外部ストレージの間の接続を保護するには、Cisco EPN Manager ストレージの強化 （1166 ページ）の推奨事項を参照してください。

Web サーバーの接続を保護する HTTPS のセットアップ

HTTPS 操作では、公開キー暗号化アルゴリズムを使用して生成されたサーバー キーおよびサーバー キーを使用して生成された信頼チェーン証明書が使用されます。これらの証明書は、Cisco EPN Manager Web サーバーに適用されます。証明書の生成方法によっては、ブラウザが Web サーバーに初めて接続したときにこれらの証明書を信頼するようにクライアント ブラウザに要求することが必要になる場合があります。HTTPS メカニズムは、サーバー マシンのセキュリティを確保します（これにより、他のすべての関連システムのセキュリティが強化されます）。

署名エンティティ	説明	次を参照してください。
認証局（CA）署名付き証明書	認証局（CA）は、これらの証明書を生成し、発行します。証明書は、証明書で識別されるエンティティ（サーバー、デバイスなど）の名前に公開キーをバインドします。Cisco EPN Manager サーバーからの証明書署名要求（CSR）ファイルを生成し、（サーバー キーを含む）CSR ファイルを CA に送信する必要があります。証明書を受信したら、Web サーバーにこれらを適用します。 これらの証明書は、外部 CA または内部 CA によって生成される場合があります。 • 外部 CA：外部 CA 組織は、通常は有料でアイデンティティを検証し、証明書を発行します（一般的なブラウザは、通常、外部 CA 組織によって発行されたルート証明書と中間証明書を使用して事前にインストールされます）。 • 内部 CA：組織内の証明書生成サーバーを使用します（料金はかかりません）。内部 CA は、外部の有料 CA とまったく同じように機能します。 この方法は、次の場合に使用できます。 • HA を使用しない導入 • 仮想 IP アドレスを使用する HA 導入（ブラウザベース クライアント間の SSL 接続を含む） （注） 導入によっては、ブラウザまたは OS 証明書ストアに CA 署名付きルートおよび中間証明書をインストールするようにユーザーに指示することが必要になる場合があります。これが必要かどうかは、組織の IT 管理者に確認してください。手順については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （965 ページ）を参照してください。	CA 署名済み Web サーバー証明書の生成および適用 （955 ページ）

CA 署名済み Web サーバー証明書の生成および適用

次のトピックでは、CA 署名付き証明書の生成および Cisco EPN Manager Web サーバーへの適用方法について説明します。手順は、HA を使用した導入かどうか、および HA を使用した導入の場合は HA を仮想 IP アドレスとともに使用しているかどうかに応じて若干異なります。

ルートおよび中間 CA 証明書をブラウザまたは OS の証明書ストアにインストールするようユーザーに指示することが必要な場合があります。これが必要かどうかは、組織の IT 管理者に確認してください。手順については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （965 ページ）を参照してください。

展開タイプ	手順の概要
HA なしの導入	HA なしの導入の場合、次のトピックの説明に従って、証明書を要求し、Webサーバーにインポートし、Webサーバーを再起動して証明書を適用する必要があります。 1. CA 署名付き Web サーバー証明書の要求 （956 ページ） 2. CA 署名付き Web サーバー証明書のインポートおよび適用：HA なし （958 ページ）
仮想 IP アドレスを使用しないハイ アベイラビリティ導入	仮想 IP を使用しない HA 導入の場合、プライマリとセカンダリ サーバーに個別の証明書を要求し、各サーバーに適切な証明書をインポートする必要があります。証明書を適用するためにサーバーを再起動する場合は、特定の順序で再起動する必要があります。全体の手順については、次のトピックを参照してください。 1. CA 署名付き Web サーバー証明書の要求 （956 ページ） 2. CA 署名付き Web サーバー証明書のインポートおよび適用（仮想 IP アドレスを使用しない HA の場合） （960 ページ）
仮想 IP アドレスを使用するハイ アベイラビリティ導入	仮想 IP を使用する HA 導入の場合、両方のサーバーに単一の証明書を要求する必要があります。サーバーの HA を削除し、両方のサーバーに証明書をインポートしてから、サーバーを再起動して証明書を適用する必要があります（サーバーは特定の順序で再起動する必要があります）。最後に、プライマリ サーバーにセカンダリ サーバーを登録することによって HA を再設定します。全体の手順については、次のトピックを参照してください。 1. CA 署名付き Web サーバー証明書の要求、インポート、適用（仮想 IP アドレスを使用した HA の場合） （962 ページ） 2. プライマリ サーバーとセカンダリ サーバー間の HA の設定方法（1119 ページ）

CA 署名付き Web サーバー証明書の要求

展開環境で使用する CA 署名付き Web サーバー証明書を要求するには、次の手順に従います。次の条件に該当する場合にはこの手順を使用する必要があります。

- 展開環境で HA が使用されていない
- 展開環境で HA が使用されているが、仮想 IP アドレッシングが使用されていない（両方のサーバーで次の手順を実行する必要があります）

（注） 展開環境で HA と仮想 IP アドレスを使用している場合は、CA 署名付き Web サーバー証明書の要求、インポート、適用（仮想 IP アドレスを使用した HA の場合）（962 ページ）の手順を使用します。

始める前に

ご使用のマシンで SCP が有効であり、すべての関連ポートが開いていることを確認します。これは、サーバーとの間でファイルをコピーするために必要です。

ステップ 1 Cisco EPN Manager サーバーの証明書署名要求（CSR）ファイルを生成します。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) 以下のコマンドを入力して、デフォルトのバックアップ リポジトリ（defaultRepo）に CSR ファイルを生成します。

```
ncs key genkey -newdn -csr CertName.csr repository defaultRepo
```

CertName は任意の名前です。

ステップ 2 Cisco EPN Manager サーバーからローカル マシンに CSR ファイルをコピーします。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) Cisco EPN Manager サーバーからローカル マシンにファイルをコピーします。次に例を示します。

```
scp /localdisk/defaultRepo/CertName.csr clientUserName@clientIP:/destinationFolder
```

ステップ 3 任意の認証局に CSR ファイルを送信します。

（注） 認証用の CSR ファイルを生成して送信した後は、同じ Cisco EPN Manager サーバーで新しいキーを生成する際に **genkey** コマンドを使用しないでください。生成した場合、署名付き証明書ファイルをインポートしようとしたときに、ファイルと Cisco EPN Manager サーバーの間でキーが一致しないためにエラーが発生します。

CA は、デジタル署名付き証明書を *CertFilename*.**cer** という名前の 1 つのファイルまたは複数ファイルのセットとして送信します。

ステップ 4 （仮想 IP アドレスを使用しない HA 展開環境）セカンダリ サーバーでこの手順を繰り返します。

次のタスク

CA から証明書を受信した場合は、証明書をインポートして適用します。展開環境に応じて、次のいずれかの手順を使用します。

- CA 署名付き Web サーバー証明書のインポートおよび適用：HA なし（958 ページ）
- CA 署名付き Web サーバー証明書のインポートおよび適用（仮想 IP アドレスを使用しない HA の場合）（960 ページ）

CA 署名付き Web サーバー証明書のインポートおよび適用：HA なし

このトピックでは、HA を使用しない展開環境に CA 署名付き Web サーバー証明書をインポートして適用する方法について説明します。

始める前に

- CA 署名付き証明書が必要です。証明書を受け取るまでは、次に示す手順は実行できません。
- ローカル マシン上で SCP が有効になっていて、関連するすべてのポートが開いていることを確認します。このようになっていなければ、サーバーとの間でファイルをコピーできません。

ステップ 1 CA から 1 つの CER ファイルだけを受け取っている場合は、ステップ 2 に進みます。 複数の（チェーン）証明書を受け取っている場合は、これらの証明書を結合（連結）して 1 つの CER ファイルにします。3 つのファイル（SSL サーバー証明書ファイル、中間 CA 証明書ファイル、およびルート CA サーバー証明書ファイル）を受け取ります。

a) テキスト エディタを使用して、受け取った 3 つの証明書ファイルを開きます。新しい 1 つのファイルに、次のように証明書の内容を上から順に貼り付けます。SSL サーバー証明書、中間 CA 証明書、およびルート CA サーバー証明書。空白行はすべて削除します。次のようなファイルが作成されます（簡潔にするため証明書の内容は省略されています）。

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) この新しいファイルに *CertFilename*.**cer** 形式の新しい名前を付けて保存します。

ステップ 2 ローカル マシンから Cisco EPN Manager サーバーのバックアップ リポジトリに CER ファイルをコピーします。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) ファイルをローカル マシンから取得し、Cisco EPN Manager サーバーのデフォルト バックアップ リポジトリ（defaultRepo）にコピーします。

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

ステップ 3 Cisco EPN Manager CLI admin ユーザーとして CER ファイルをインポートします。

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

ステップ 4 この証明書をアクティブにするため、Cisco EPN Manager を再起動します。Cisco EPN Manager の停止と再起動 （973 ページ）を参照してください。

次のタスク

展開環境によっては、ルート CA 証明書と中間 CA 証明書をブラウザまたは OS 証明書ストアにインストールするように、ユーザーに指示する必要があります。詳細については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （965 ページ）を参照してください。

CA 署名付き Web サーバー証明書のインポートおよび適用：HA なし

このトピックでは、HA を使用しない展開環境に CA 署名付き Web サーバー証明書をインポートして適用する方法について説明します。

始める前に

- CA 署名付き証明書が必要です。証明書を受け取るまでは、次に示す手順は実行できません。
- ローカル マシン上で SCP が有効になっていて、関連するすべてのポートが開いていることを確認します。このようになっていなければ、サーバーとの間でファイルをコピーできません。

ステップ 1 CA から 1 つの CER ファイルだけを受け取っている場合は、ステップ 2 に進みます。 複数の（チェーン）証明書を受け取っている場合は、これらの証明書を結合（連結）して 1 つの CER ファイルにします。3 つのファイル（SSL サーバー証明書ファイル、中間 CA 証明書ファイル、およびルート CA サーバー証明書ファイル）を受け取ります。

a) テキスト エディタを使用して、受け取った 3 つの証明書ファイルを開きます。新しい 1 つのファイルに、次のように証明書の内容を上から順に貼り付けます。SSL サーバー証明書、中間 CA 証明書、およびルート CA サーバー証明書。空白行はすべて削除します。次のようなファイルが作成されます（簡潔にするため証明書の内容は省略されています）。

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) この新しいファイルに *CertFilename*.**cer** 形式の新しい名前を付けて保存します。

ステップ 2 ローカル マシンから Cisco EPN Manager サーバーのバックアップ リポジトリに CER ファイルをコピーします。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) ファイルをローカル マシンから取得し、Cisco EPN Manager サーバーのデフォルト バックアップ リポジトリ（defaultRepo）にコピーします。

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

ステップ 3 Cisco EPN Manager CLI admin ユーザーとして CER ファイルをインポートします。

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

ステップ 4 この証明書をアクティブにするため、Cisco EPN Manager を再起動します。Cisco EPN Manager の停止と再起動 （973 ページ）を参照してください。

次のタスク

展開環境によっては、ルート CA 証明書と中間 CA 証明書をブラウザまたは OS 証明書ストアにインストールするように、ユーザーに指示する必要があります。詳細については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （965 ページ）を参照してください。

CA 署名付き Web サーバー証明書のインポートおよび適用（仮想 IP アドレスを使用しない HA の場合）

このトピックでは、仮想 IP アドレスを使用しない HA 展開に CA 署名付き Web サーバー証明書をインポートして適用する方法を説明します（HA 展開で仮想 IP を使用している場合は、CA 署名付き Web サーバー証明書の要求、インポート、適用（仮想 IP アドレスを使用した HA の場合） （962 ページ）を参照してください）。この手順は HA を使用する展開での手順と同様ですが、プライマリ サーバーとセカンダリ サーバーの両方で手順を実行しなければならないという点が異なります。

（注） サーバーは特定のシーケンスで再起動する必要があるため、サーバーを再起動するときは、以下の手順に忠実に従ってください。

始める前に

- CA 署名付き証明書が必要です。各サーバーの証明書を受信するまでは、以下の手順を実行することはできません。
- ローカル マシン上で SCP が有効になっていて、関連するすべてのポートが開いていることを確認します。このようになっていなければ、サーバーとの間でファイルをコピーできません。

ステップ 1 プライマリ サーバーにプライマリ証明書をインポートします。

a) CA から受け取った CER ファイルが 1 つだけである場合は、ステップ 1(b) に進みます。 複数の（チェーン）証明書を受け取った場合は、それらの証明書を 1 つの CER ファイルに結合（連結）します。3 つのファイル（SSL サーバー証明書ファイル、中間 CA 証明書ファイル、およびルート CA サーバー証明書ファイル）を受け取ります。

1. テキスト エディタを使用して、受け取った 3 つの証明書ファイルを開きます。新しい 1 つのファイルに、次のように証明書の内容を上から順に貼り付けます。SSL サーバー証明書、中間 CA 証明書、およびルート CA サーバー証明書。空白行はすべて削除します。次のようなファイルが作成されます（簡潔にするため証明書の内容は省略されています）。

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

2. この新しいファイルに *CertFilename*.**cer** 形式の新しい名前を付けて保存します。

b) Cisco EPN Manager CLI 管理ユーザーとしてプライマリ Cisco EPN Manager サーバーにログインします。
c) ローカル マシンから CER ファイルを取得して、Cisco EPN Manager サーバーのデフォルト バックアップ リポジトリ（defaultRepo）にコピーします。

scp *clientUserName*@*clientIP*:/*fullPathToCERfile* **/localdisk/defaultRepo**

ステップ 2 セカンダリ サーバーで上記の手順を行います。

ステップ 3 セカンダリ サーバーで、CER ファイルをインポートします。

a) Cisco EPN Manager CLI 管理ユーザーとしてログインし、サーバーを停止します。

ncs stop

b) セカンダリ サーバーが停止していることを確認します。
c) CER ファイルをインポートします。

ncs key importsignedcert *CertFilename*.**cer repository** *RepoName*

（注） ステップ 5 に到達するまでは、セカンダリ サーバーを再起動しないでください。

ステップ 4 プライマリ サーバーで、CER ファイルをインポートします。

a) Cisco EPN Manager CLI 管理ユーザーとしてログインし、サーバーを停止します。

ncs stop

b) プライマリ サーバーが停止していることを確認します。
c) CER ファイルをインポートします。

ncs key importsignedcert *CertFilename*.**cer repository** *RepoName*

（注） ステップ 6 に到達するまでは、プライマリ サーバーを再起動しないでください。

ステップ 5 セカンダリ サーバーで、次のコマンドを実行します。

a) **ncs start** コマンドを実行してサーバーを再起動します。
b) セカンダリ サーバーが再起動したことを確認します。
c) **ncs status** コマンドを実行し、セカンダリ サーバーの HA ステータスが [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] であることを確認します。

ステップ 6 プライマリ サーバーで、次のコマンドを実行します。

a) **ncs start** コマンドを実行してサーバーを再起動します。
b) プライマリ サーバーが再起動したことを確認します。

c) **ncs status** コマンドを実行して、ヘルス モニター プロセスとその他のプロセスが再開していることを確認します。

プライマリ サーバーですべてのプロセスが稼働したら、セカンダリ サーバーとプライマリ サーバーの間で HA 登録が自動的にトリガーされます（また、登録されている電子メール アドレスに電子メールが送信されます）。自動 HA 登録は通常、数分で完了します。

ステップ 7 プライマリ サーバーとセカンダリ サーバーで **ncs ha status** コマンドを実行し、両方のサーバーの HA ステータスを確認します。次が表示されます。

- プライマリ サーバーの状態は [プライマリ アクティブ（Primary Active）] です。
- セカンダリ サーバーの状態は [セカンダリ同期（Secondary Syncing）] です。

次のタスク

展開環境によっては、ルート CA 証明書と中間 CA 証明書をブラウザまたは OS 証明書ストアにインストールするように、ユーザーに指示する必要があります。詳細については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （965 ページ）を参照してください。

CA 署名付き Web サーバー証明書の要求、インポート、適用（仮想 IP アドレスを使用した HA の場合）

仮想 IP アドレスを使用したハイ アベイラビリティ展開を使用している場合でも、証明書を要求する必要があるのは 1 回だけです。CA から証明書を受け取ったら、プライマリ サーバーとセカンダリ サーバーの両方にその同じ証明書をインストールします。この点が、IP アドレスを使用しない HA 展開との違いです。IP アドレスを使用しない HA 展開では、2 つの証明書要求を行って、一方の証明書をプライマリ サーバーにインストールし、もう一方の（異なる）証明書をセカンダリ サーバーにインストールします。

仮想 IP および HA の詳細については、次を参照してください。HA での仮想 IP アドレッシングの使用 （1117 ページ）

始める前に

ご使用のマシンで SCP が有効であり、すべての関連ポートが開いていることを確認します。これは、サーバーとの間でファイルをコピーするために必要です。

ステップ 1 1 つの CSR ファイルおよび秘密キーをプライマリ サーバーとセカンダリ サーバー用に生成します。秘密キーを両方のサーバーにインストールし、CSR ファイルを任意の認証局に送信します。次の例では、Linux で openssl を使用して、これらのファイルを作成する方法を説明しています。

a) デフォルトのバックアップ リポジトリで CSR ファイルを生成します。

```
openssl req -newkey rsa:2048 -nodes -keyout ServerKeyFileName -out CSRFileName -config
opensslCSRconfigFileName
```

引数の説明

- *ServerKeyFileName* は、秘密キー ファイルに使用するファイル名です。
- *CSRFileName* は、CA に送信する CSR 要求ファイルに使用するファイル名です。
- *opensslCSRconfigFileName* は、CSR ファイルを生成するために使用した openssl 設定が含まれるファイルの名前です。

b) テキスト エディタを使用して、openssl 設定が含まれるファイル（(a) の *opensslCSRconfigFileName*）を編集し、次のような内容にします。

```
[req]
 distinguished_name = req_distinguished_name
 req_extensions = v3_req

 [req_distinguished_name]
 countryName = Country
 countryName_default = US
 stateOrProvinceName = State
 stateOrProvinceName_default = CA
 localityName = City
 localityName_default = San Jose
 organizationName = Organization
 organizationName_default = Cisco Systems
 organizationalUnitName = Organizational Unit
 organizationalUnitName_default = CSG
 commonName = Common Name
 commonName_default = example.cisco.com
 commonName_max = 64

 [ v3_req ]
 # Extensions to add to a certificate request
 basicConstraints = CA:FALSE
 keyUsage = nonRepudiation, digitalSignature, keyEncipherment
 subjectAltName = @alt_names

 [alt_names]
 DNS.1 = example.cisco.com
 DNS.2 = example-pri.cisco.com
 DNS.3 = example-sec.cisco.com
 IP.1 = 209.165.200.224
 IP.2 = 209.165.200.225
 IP.3 = 209.165.200.226
```

この例では、次のようになります。

- 仮想 IP アドレスは 209.165.200.224 です。FQDN は **example.cisco.com** です。FQDN は、DNS サーバー名にも使用されます。
- プライマリ サーバーの IP アドレスは 209.165.200.225 です。そのホスト名は **example-pri** です。/etc/hosts およびその他のホスト名設定ファイルに、このホスト名を含める必要があります。
- セカンダリ サーバーの IP アドレスは 209.165.200.226 です。そのホスト名は **example-sec** です。

ステップ 2 任意の認証局に CSR ファイルを送信します。CA は、デジタル署名付き証明書を *CertFilename*.**cer** という名前の 1 つのファイルまたは複数ファイルのセットとして送信します。

ステップ 3 CA から 1 つの CER ファイルだけを受け取っている場合は、ステップ 4 に進みます。 複数の（チェーン）証明書を受け取っている場合は、これらの証明書を結合（連結）して 1 つの CER ファイルにしま

す。3 つのファイル（SSL サーバー証明書ファイル、中間 CA 証明書ファイル、およびルート CA サーバー証明書ファイル）を受け取ります。

a) テキスト エディタを使用して、受け取った 3 つの証明書ファイルを開きます。新しい 1 つのファイルに、次のように証明書の内容を上から順に貼り付けます。SSL サーバー証明書、中間 CA 証明書、およびルート CA サーバー証明書。空白行はすべて削除します。次のようなファイルが作成されます（簡潔にするため証明書の内容は省略されています）。

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) この新しいファイルに *CertFilename*.**cer** 形式の新しい名前を付けて保存します。

ステップ 4 プライマリ サーバーで、CER ファイルを各サーバー上のバックアップ リポジトリにコピーします。

a) Cisco EPN Manager CLI admin ユーザーとして Cisco EPN Manager サーバーにログインします。

b) ローカル マシンからファイルを取得して、サーバーのデフォルト バックアップ リポジトリ（defaultRepo）にコピーします。

ステップ 5 セカンダリ サーバーで上記の手順を繰り返します。

ステップ 6 プライマリ サーバーで、Cisco EPN Manager CLI admin ユーザーとして HA 設定を削除します。

```
ncs ha remove
```

ncs ha status を実行して HA 設定が削除されていることを確認してから、次のステップに進んでください。

（注） HA が未割り当ての場合は、TOFU 証明書を手動で削除する必要があります。詳細については、任意の状態の TOFU エラーの解決 （1155 ページ）を参照してください。

ステップ 7 プライマリ サーバーとセカンダリ サーバーの両方で、CER ファイルをインポートします。

```
ncs key importkey ServerKeyFileNameCertFilename.cer repository RepoName
```

ステップ 8 プライマリ サーバーとセカンダリ サーバーを再起動します。プライマリ サーバーとセカンダリ サーバーはまだ HA ペアとして設定されていないため、順番は重要ではありません。Cisco EPN Manager の停止と再起動 （973 ページ）を参照してください。

（注） サーバーが再起動しない場合、（インポート操作は成功したように見えても）連結した証明書ファイルではなく、誤って個々の証明書をインポートした可能性があります。この問題を解決するには、（正しい）連結された証明書ファイルを使用してインポート操作を繰り返してください。

ステップ 9 プライマリ サーバーとセカンダリ サーバーで **ncs status** コマンドを実行し、両方のサーバーのステータスを確認します。

ステップ 10 セカンダリ サーバーをプライマリ サーバーに HA 用に登録します。プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （1119 ページ）を参照してください。

次のタスク

展開環境によっては、ルート CA 証明書と中間 CA 証明書をブラウザまたは OS 証明書ストアにインストールするように、ユーザーに指示する必要があります。詳細については、ブラウザ/OS 信頼ストアに CA 署名付きルート証明書と中間証明書を追加する （965 ページ）を参照してください。

ブラウザ/*OS* 信頼ストアに *CA* 署名付きルート証明書と中間証明書を追加する

ユーザーがブラウザまたは OS の証明書ストアに CA ルート証明書と中間 CA 証明書をインストールする必要があるかどうかを組織の IT 管理者に確認します。証明書のインストールが必要な状況で証明書がインストールされていないと、ユーザーのブラウザにブラウザが信頼されていないことを示す通知が表示されます。

ブラウザのタイプやバージョンによっては、以下の手順の細かい部分が多少異なる可能性があります。

始める前に

Internet Explorer ブラウザに証明書を追加する場合、クライアント マシンの管理者権限が必要になります。

ステップ 1 Firefox のブラウザでは、次の手順に従って、証明書をインポートします。

a) **[ツール（Tools）]**>**[オプション（Options）]** の順に選択し、左側のオプションから [詳細（Advanced）] をクリックします。
b) ウィンドウ上部にあるリストから [証明書（Certificates）] をクリックしてから、[証明書を表示（View Certificates）] をクリックします。この操作によって、ブラウザの [証明書マネージャ（Certificate Manager）] ダイアログボックスが開きます。
c) [証明書マネージャ（Certificate Manager）] ダイアログボックスで、[認証局（Authorities）] タブをクリックし、ダイアログの下部にある [インポート（Import）] をクリックします。
d) [...ファイルを選択してください（Select File...）] ダイアログボックスで、CA 署名付きルート証明書ファイルを参照し、[開く（Open）] をクリックします。
e) ファイルをインポートします。
f) CA 署名付き中間証明書ファイルについて、インポート手順を繰り返します。

ステップ 2 Internet Explorer ブラウザでは、Microsoft の証明書マネージャ ツールを使用して、証明書をインポートします。このツールを使用するには、ユーザーにクライアント マシンの管理者権限がなければなりません。

a) Windows 7 では、[スタート（Start）] をクリックします。
b) 検索テキスト ボックスに「certmgr.msc」と入力し、Enter キーを押します。
c) 検索結果のプログラムのアイコンをクリックすると、Microsoft 証明書マネージャが起動します。

d) 証明書マネージャの GUI の左側の列で、[信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択します。
e) [証明書（Certificates）] を右クリックし、**[すべてのタスク（All Tasks）]** > **[インポート（Import）]** を選択します。
f) [次に（Next）] をクリックし、CA 署名付きルート証明書ファイルを参照し、インポートします。
g) CA署名付き中間証明書ファイルについてインポート手順を繰り返します。ただし、証明書をインポートする最初の手順として [中間証明書機関（Intermediate Certification Authorities）] を選択します。

（注） CA 署名付き証明書がインストールされていない場合、Cisco EPN Manager はアラートを表示します。

HTTPS サーバー ポートの変更

多くのデバイスで設定情報のリレーに HTTPS が使用されるため、Cisco EPN Manager では HTTPS がデフォルトで有効になっています（HTTP は Cisco EPN Manager で使用されないため、デフォルトでは無効になっています）。必要に応じて、次の手順に従ってHTTPSサーバーのポートを変更できます。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択してから、**[一般（General）]** > **[サーバー（Server）]** を選択します。
ステップ 2 [HTTPS] 領域に新しいポート番号を入力し、[保存（Save）] をクリックします。
ステップ 3 Cisco EPN Manager を再起動し、変更を適用します。Cisco EPN Manager の停止と再起動 （973 ページ） を参照してください。

証明書の検証設定

TLS/HTTPS 接続のようなセキュアなトランザクション時のユーザー認証（証明書ベースの認証が有効になっている場合）では、Cisco EPNM は外部エンティティから証明書を受信します。Cisco EPNM はこれらの証明書を検証して証明書の整合性と証明書の所有者のアイデンティティを確認する必要があります。証明書の検証機能により、ユーザーは他のエンティティから受信した証明書を検証する方法を制御できます。

証明書の検証が適用されると、他のエンティティから受信した証明書は、その証明書が Cisco EPNM によって信頼されている認証局（CA）が署名している場合にのみ、Cisco EPNM によって受け入れられます。信頼ストアは、ユーザーが信頼できる CA 証明書を維持できる場所です。署名付き証明書チェーンが信頼ストア内のいずれかの CA 証明書がルートでない場合、検証は失敗します。

信頼ストアの管理

ユーザーは信頼ストア内の信頼できる CA を管理できます。Cisco EPNM は、さまざまな信頼ストア、つまり、pubnet、system、devicemgmt、および user を提供します。

- pubnet：パブリックネットワーク内のサーバーに接続したときにリモートホストから受信した証明書の検証中に使用されます。
- system：ネットワーク内のシステムに接続したときにリモートシステムから受信した証明書の検証中に使用されます。
- devicemgmt：管理対象デバイスから受信した証明書の検証中に使用されます。
- user：ユーザー証明書の検証に使用されます（証明書ベースの認証が有効になっている場合）。

信頼ストアを管理する *CLI*

次に、信頼ストアを管理するために使用される CLI を示します。

- 信頼ストアへの CA 証明書のインポート （967 ページ）
- 信頼ストアでの CA 証明書の表示 （967 ページ）
- 信頼ストアからの CA 証明書の削除 （967 ページ）

信頼ストアへの CA 証明書のインポート

次に、信頼ストアに CA 証明書をインポートするコマンドを示します。

```
ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository
<Repository-name><certificate-file> truststore {devicemgmt | pubnet |
system | user}
```

信頼ストアでの CA 証明書の表示

次に、信頼ストアで CA 証明書を表示するコマンドを示します。

```
ncs certvalidation trusted-ca-store listcacerts truststore {devicemgmt
| pubnet | system | user}
```

信頼ストアからの CA 証明書の削除

次に、信頼ストアから CA 証明書を削除するコマンドを示します。

```
ncs certvalidation trusted-ca-store deletecacert alias <ALIAS> truststore
{devicemgmt | pubnet | system | user}
```

Cisco EPN Manager サーバーとの SSH セッションの確立

サーバーに接続するときには、admin ユーザーとして SSH を使用してログインします。（詳細については、ユーザー インターフェイス、ユーザー タイプ、およびそれらの間の遷移 （995 ページ）を参照してください）。

ステップ 1 SSH セッションを開き、Cisco EPN Manager admin ユーザーとしてログインします。

- コマンド ラインから次のように入力します。*server-ip* は Cisco EPN Manager です。

```
ssh admin server-ip
```

- SSH クライアントを開き、**admin** としてログインします。

（注） ユーザーは、SSH または PuTTY に接続する新しいアルゴリズムを作成してカスタマイズできるようになりました。

ステップ 2 admin パスワードを入力します。プロンプトが次のように変化します。

```
(admin)
```

管理ユーザーが実行できる操作のリストを表示するには、プロンプトで **?** と入力します。

admin コンフィギュレーション モードを開始するには、次のコマンドを入力します（プロンプトの変化に注意してください）。

```
(admin) configure terminal
(config)
```

サーバーでの NTP の設定

Network Time Protocol（NTP）は、ネットワーク内のすべてのデバイスと Cisco EPN Manager サーバーで正しく同期される必要があります。ネットワーク全体の NTP 同期の管理で障害が発生した場合、Cisco EPN Manager で異常な結果が発生する可能性があります。これには、Cisco EPN Manager バックアップに使用する任意のリモート FTP サーバー、セカンダリ Cisco EPN Manager 高可用性サーバーなど、すべての Cisco EPN Manager 関連サーバーが含まれます。

Cisco EPN Manager サーバーのインストール時にデフォルトおよびセカンダリの NTP サーバーを指定します。また、Cisco EPN Manager の **ntp server** コマンドを使用して、インストール後に NTP サーバーのリストを追加または変更することもできます。

（注） Cisco EPN Manager は NTP サーバーとして設定できません。NTP クライアントとしてだけ機能します。最大 5 台の NTP サーバーを設定できます。

ステップ 1 Cisco EPN Manager サーバーに管理者ユーザーとしてログインし、コンフィギュレーション モードを開始します。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

ステップ 2 次の方法のいずれかのコマンドを使用して、NTP サーバーを設定します。

認証されていない NTP サーバーのセットアップの場合：

```
ntp server ntp-server-IP
```

認証済み NTP サーバーのセットアップの場合：

```
ntp server ntp-server-IP ntp-key-id ntp-type password
```

ここで、

- *ntp server IP* は、Cisco EPN Manager サーバーにクロック同期を提供するサーバーの IP アドレスまたはホスト名です
- *ntp-key-id* は、認証済み NTP サーバーの MD5 キー ID MD5 キーです。
- *ntp-type* は、プレーンまたはハッシュのいずれかにすることができます。
- *password* は NTPv4 サーバーの MD5 プレーン テキスト パスワードです。

Cisco EPN Manager プロキシ サーバーの設定

サーバーのプロキシと、そのローカル認証サーバー（設定されている場合）のプロキシを設定するには、次の手順に従います。ネットワークとインターネットの間のセキュリティ バリアとしてプロキシ サーバーを使用する場合、次の手順に従ってプロキシを設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [プロキシ（Proxy）] タブをクリックします。

ステップ 3 [プロキシの有効化（Enable Proxy）] チェックボックスをオンにし、Cisco.com に接続してプロキシとして機能するサーバーに関する必須情報を入力します。

ステップ 4 [認証プロキシ（Authentication Proxy）] チェックボックスをオンにし、プロキシ サーバーのユーザー名とパスワードを入力します。

ステップ 5 [接続のテスト（Test Connectivity）] をクリックして、プロキシ サーバーに接続できることを確認します。

ステップ 6 [保存（Save）] をクリックします。

SMTP 電子メール サーバーの設定

Cisco EPN Manager で（アラーム、ジョブ、レポートなどの）電子メール通知の送信を可能にするには、システム管理者はプライマリ SMTP 電子メール サーバーを（また、できればセカンダリ電子メール サーバーも）設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、次に **[メールと通知（Mail and Notification）] > [メール サーバー設定（Mail Server Configuration）]** を選択します。

ステップ 2 [プライマリ SMTP サーバー（Primary SMTP Server）] で、Cisco EPN Manager が使用する電子メール サーバーに合わせて、[ホスト名/IP（Hostname/IP）]、[ユーザー名（User Name）]、[パスワード（Password）]、および [パスワードの確認（Confirm Password）] フィールドに入力します。物理サーバーの IP アドレスを入力し、プライマリ SMTP サーバーのホスト名を入力します。

（注） 仮想 IP アドレスを [ホスト名/IP（Hostname/IP）] フィールドに入力することはできません。また、IP アドレスをロード バランサの後に配置することはできません。

ステップ 3 （オプション）[セカンダリ SMTP サーバー（Secondary SMTP Server）] で同じ各フィールドに入力します。SMTP サーバーのユーザー名とパスワード。

ステップ 4 [送信者および受信者（Sender and Receivers）] で、Cisco EPN Manager の正当なメール アドレスを入力します。

ステップ 5 完了したら、[保存（Save）] をクリックします。

サーバーでの FTP/TFTP/SFTP サービスの有効化

FTP/TFTP/SFTP は、デバイス設定およびソフトウェア イメージ ファイルの管理のために、サーバーとデバイスの間でファイルを転送する目的で使用されます。また、これらのプロトコルは、高可用性導入環境において、セカンダリ サーバーにファイルを転送するためにも使用されます。これらのサービスは、通常はデフォルトで有効になっています。FIPS モードで Cisco EPN Manager をインストールした場合、これらはデフォルトで無効になります。このページを使用してこれらのサービスを有効にすると、Cisco EPN Manager は FIPS に準拠しなくなります。

SFTP は、セキュリティで保護されたバージョンのファイル転送サービスです。デフォルトでこれが使用されます。FTP は、セキュリティで保護されていないファイル転送サービス バージョンです。TFTP は、セキュリティで保護されていない、単純なサービス バージョンです。FTP または TFTP のいずれかを使用するには、サーバーの追加後にサービスを有効化する必要があります。

FTP/TFTP/SFTP パスワードを変更するには、FTP ユーザー パスワードの変更 （973 ページ） を参照してください。

ステップ 1 FTP、TFTP、または SFTP サーバーを使用するように Cisco EPN Manager を設定します。

a) **[管理（Administration）] > [サーバー（Servers）] > [TFTP/FTP/SFTP サーバー（TFTP/FTP/SFTP Servers）]** を選択します。

b) [コマンドの選択（Select a command）] ドロップダウン リストから、[TFTP/FTP/SFTP サーバーの追加（Add TFTP/FTP/SFTP Server）] を選択し、[移動（Go）] をクリックします。

- **[サーバータイプ（Server Type）]** ドロップダウンリストから、**[FTP]**、**[TFTP]**、**[SFTP]**、または **[すべて（All）]** を選択します。
- サーバーのユーザー定義名を入力します。
- サーバーの IP アドレスを入力します。

c) [保存（Save）] をクリックします。

ステップ 2 FTP または TFTP を使用する場合には、Cisco EPN Manager サーバーでそれを有効化します。

a) **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[一般（General）]** > **[サーバー（Server）]** を選択します。
b) [FTP] または [TFTP] エリアに移動します。
c) [有効（Enable）] をクリックします。
d) **[保存（Save）]** をクリックします。

ステップ 3 Cisco EPN Manager を再起動し、変更を適用します。Cisco EPN Manager の停止と再起動 （973 ページ） を参照してください。

（注） [ハイアベイラビリティ設定（High Availability setup）] では、FTP または TFTP サービスがプライマリサーバーで有効になっている場合は、ハイアベイラビリティを設定する前にセカンダリサーバーでも有効にする必要があります。これは、コンフィギュレーションファイルを編集し、変更を適用するためにサーバーを再起動することで、セカンダリサーバーで手動で実行する必要があります。

セカンダリサーバーで実行する必要があるステップを次に示します。

- セカンダリサーバーで FTP または TFTP を有効にするには、次のようにします。
  1. 次のプロパティを `/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml` ファイルで値を「**true**」に設定します。
     - <entry key="FtpEnable">true</entry>
     - <entry key="TftpEnable">true</entry>
  2. Cisco EPN Manager セカンダリサーバーを再起動します。
- セカンダリサーバーで FTP または TFTP を無効にするには、次の手順を実行します。
  1. 次のプロパティを `/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml` ファイルで値「**false**」に設定します。
     - <entry key="FtpEnable">false</entry>
     - <entry key="TftpEnable">false</entry>
  2. Cisco EPN Manager セカンダリサーバーを再起動します。

ログイン バナー（ログインの免責事項）の作成

すべてのユーザーに対してログイン前に表示するメッセージがある場合は、ログインの免責事項を作成します。テキストは GUI クライアント ログイン ページのログイン フィールドとパスワード フィールドの下に表示されます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [ログインの免責事項（Login Disclaimer）]** を選択します。

ステップ 2 ログインの免責事項テキストを入力（または編集）します。

（注） 改行文字は無視されます。

変更はすぐに反映されます。

Cisco EPN Manager の停止と再起動

Cisco EPN Manager製品ソフトウェアのアップグレード、ログファイルの設定変更、セキュアポート設定のハンギング、レポートファイルの圧縮、サービス検出設定の変更、LDAP 設定の構成の後などに、再起動が必要です。Cisco EPN Manager サーバーを停止すると、すべてのユーザー セッションが終了します。

サーバーを停止するには、サーバーとの CLI セッションを開いて、以下を入力します。

```
ncs stop
```

サーバーを再起動するには、サーバーとの CLI セッションを開いて、以下を入力します。

```
ncs start
```

管理パスワードの管理

FTP ユーザー パスワードの変更

Cisco EPN Manager では、FTP を使用して他のサーバーにアクセスするために、ID として **ftp-user** を使用します。管理権限を持つユーザーは、FTP パスワードを変更できます。

ステップ 1 admin ユーザーとして Cisco EPN Manager サーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）。

ステップ 2 Cisco EPN Manager サーバーの FTP パスワードを変更するには、次のように入力します。

```
ncs password ftpuser username password password
```

例

```
(admin) ncs password ftpuser ftp-user password FTPUserPassword
Initializing...
Updating FTP password.
This may take a few minutes.
Successfully updated location ftpuser
```

Web GUI ルート ユーザー パスワードの変更

Cisco EPN Manager は**ルート** ID を使用して、Web GUI へのルート アクセス権が必要な特別なタスクを実行します

始める前に

Web GUI ルート ユーザー パスワードを変更するには、現在のパスワードを知っている必要があります。

ステップ 1 **ルート** ユーザーとして Cisco EPN Manager 管理 CLI にログインします（管理 CLI の詳細については、ユーザー インターフェイスとユーザー タイプ （995 ページ）を参照してください）。

ステップ 2 次のコマンドを入力します（*newpassword* は新しい Web GUI ルート パスワードです）。

```
ncs password root password  newpassword
```

（注） 入力する新しいパスワードは、現在のパスワードポリシーに従う必要があります。詳細については、ローカル認証のためのグローバル パスワード ポリシーの設定 （1027 ページ）を参照してください。

例

```
ncs password root password NewWebGUIRootPassword
Password updated for web root password
```

仮想アプライアンスの管理者パスワードの回復

このトピックでは、Cisco EPN Manager 仮想マシン（別名 OVA）の管理パスワードを回復してリセットする方法を説明します。

はじめる前に

次の条件が満たされていることを確認します。

- Cisco EPN Manager サーバーに対する物理アクセス。
- ソフトウェアのバージョンに適切なインストール ISO イメージのコピー。
- VMware vSphere クライアントへのアクセスと、vSphere インベントリ、データストア、およびオブジェクトの各機能へのアクセス。このようなアクセスがない場合は、VMware 管理者にお問い合わせください。vSphere クライアントから ESX に直接アクセスしないでください。

ステップ 1 Cisco EPN Manager OVA サーバーで、VMware vSphere クライアントを起動します。

ステップ 2 次のように、OVA 仮想マシン上のデータストアにインストール ISO イメージをアップロードします。

a) vSphere インベントリで、[**Datastores**] をクリックします。
b) [**Objects**] タブで、ファイルをアップロードするデータストアを選択します。
c) **Navigate to the datastore file browser**アイコンをクリックします。
d) 必要に応じて、[**Create a new folder**] アイコンをクリックして新しいフォルダを作成します。
e) 作成したフォルダを選択するか、既存のフォルダを選択して、[**Upload a File**] アイコンをクリックします。

[クライアント統合アクセス制御（Client Integration Access Control）] ダイアログ ボックスが表示されたら、[**Allow**] をクリックしてプラグインからオペレーティング システムにアクセスできるようにし、ファイルのアップロードに進みます。

f) ローカル コンピュータで、ISO ファイルを検索して、そのファイルをアップロードします。
g) データストア ファイル ブラウザを更新して、アップロードされたファイルを一覧表示します。

ステップ 3 ISO イメージがデータストアにアップロードされたら、次のように、それをデフォルトのブート イメージにします。

a) VMware vSphere クライアントを使用して、導入済みの OVA を右クリックして **Power > Shut down guest** を選択します。
b) **[Edit] [Settings] [>] [Hardware]** を選択してから、**[CD/DVD] [drive] [1]** を選択します。
c) [**Device Type**] で [**Datastore ISO File**] を選択してから、[**Browse**] ボタンを使用して、データストアにアップロードした ISO イメージ ファイルを選択します。
d) **[Device] [Status,]** で **[Connect] [at] [power] [on]** を選択します。
e) [**Options**] タブをクリックして [**Boot Options**] を選択します。[**Force BIOS Setup**] で、**Next time VM boots, force entry into BIOS setup Screen** を選択します。これにより、仮想マシンを再起動すると、仮想マシンの BIOS からブートが開始されます。
f) **OK** をクリックします。
g) VMware vSphere クライアントで、導入済みの OVA を右クリックして **Power > Power On** を選択します。
h) BIOS セットアップ メニューでデバイスのブート順序を制御するオプションを探して、**DVD/CDROM** を一番上に移動します。

ステップ 4 次の手順に従って、サーバー管理者パスワードをリセットします。

a) BIOS 設定を保存して、BIOS セットアップ メニューを終了します。仮想マシンが ISO イメージからブートし、ブート オプションのリストが表示されます。
b) キーボードとモニターを使用して OVA にアクセスしている場合は **3**、コマンド ラインまたはコンソール経由でアクセスしている場合は **4** を入力します。vSphere クライアントに、管理者ユーザー名のリストが表示されます。
c) パスワードをリセットする管理者ユーザー名の横に表示された番号を入力します。
d) 新しいパスワードを入力し、2 回目の入力でそれを確認します。
e) **Y** と入力し、変更を保存してリブートします。
f) 仮想マシンがリブートしたら、vSphere クライアントを使用して、CD アイコンをクリックし、[**Disconnect ISO image**] を選択します。

ステップ 5 新しい管理パスワードを使ってログインします。

システム監視ダッシュボードを使用して、Cisco EPN Manager サーバーのヘルス、ジョブ、パフォーマンス、および API 統計をチェックする

システム監視ダッシュボードは、Cisco EPN Manager サーバーの設定とパフォーマンスに関する情報を提供します。ダッシュボードにアクセスするには、**[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[システム監視ダッシュボード（System Monitoring Dashboard）]** を選択します（ユーザー ID がこのダッシュボードにアクセスするための管理者権限を持っている必要があります）。[概要（Overview）] タブや [パフォーマンス（Performance）] タブに表示されるダッシュレットをカスタマイズするには、事前定義のダッシュレットをダッシュボードに追加する （28 ページ）に記載された手順に従ってください。

[Dashboard] タブ	説明
概要	バックアップおよびデータ消去ジョブ、Cisco EPN Manager システム アラーム、およびサーバー CPU、ディスク、メモリの使用状況統計。この情報をチェックするために別々の時間枠を指定できます。 サーバータイム、カーネルバージョン、オペレーティングシステム、ハードウェア情報などを表示するには、ダッシュボードの左上にある [システム情報（System Information）] をクリックして、その情報を含むフィールドを開きます。 [概要（Overview）] ダッシュボードからダッシュレットを追加または削除できます。
パフォーマンス	サーバーの syslog とトラップ、および入出力。[パフォーマンス（Performance）] ダッシュボードから、このデータの異なる時間枠を指定したり、ダッシュレットを追加または削除したりできます。
[管理者（Admin）]	• [状況（Health）]：システム アラーム、実行中のジョブの数、ログインしたユーザーの数、およびデータベースの使用状況の分布。履歴情報の異なる時間枠を指定できます。 • [API ヘルス（API Health）]：すべての API サービスとともにそれらの応答時間統計を一覧表示します。 • [サービスの詳細（Service Details）]：特定のサービスの統計（応答カウントと時間傾向）、クライアントあたりのコール数（クライアントはIPアドレスで識別されます）。チェックするサービスを選択できます。

Cisco EPN Manager サーバーのパフォーマンスの改善

OVA サイズの確認

Cisco EPN Manager が、ご利用のシステム リソース、またはインストールした OVA のサイズに推奨されるデバイス/インターフェイス/フロー数の 80% 以上を使用している場合、パフォーマンスに悪影響が及ぶ可能性があります。インストール マニュアルで指定されているデバイス、インターフェイス、およびフロー レコードの推奨値を OVA が超えていないことを確認します。これらの推奨値は、指定されている各 OVA サイズの最大値です。管理ダッシュボードでこれらを確認できます（システム監視ダッシュボードを使用して、Cisco EPN Manager サーバーのヘルス、ジョブ、パフォーマンス、および API 統計をチェックする （976 ページ）を参照）。容量の問題に対処するには、サーバーのディスク容量に関する問題の管理 （977 ページ）を参照してください。

データベースの圧縮

ステップ 1 admin ユーザーとして サーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）。

ステップ 2 次のコマンドを入力して、アプリケーション データベースを圧縮します。

```
(admin)# ncs cleanup
```

ステップ 3 プロンプトが表示されたら、ディープ クリーンアップ オプションに対し **[Yes]** を選択します。

サーバーのディスク容量に関する問題の管理

Cisco EPN Manager は、サーバーのディスク容量が少なくなると、次のしきい値でアラームをトリガーします。

- 60% の使用率でメジャー アラームをトリガーする
- 65% の使用率でクリティカル アラームをトリガーする

アラートを受信した場合は、次のアクションを実行することを検討してください。

- データベースの圧縮 （977 ページ）の説明に従って、既存のデータベース領域を解放します。

- バックアップをローカル リポジトリに保存する場合は、リモート バックアップ リポジトリの使用を検討してください。「NFSベースのリモート リポジトリの設定（938ページ）」を参照してください。
- データの収集と消去（985ページ）の説明に従って、ネットワーク インベントリ、パフォーマンス、レポート、その他のクラスのデータの保持期間を短縮します。
- ディスク容量を追加します。VMware OVA テクノロジーを使用すれば、簡単に既存のサーバーのディスク容量を増やすことができます。物理ディスク容量を拡張する場合は、Cisco EPN Manager サーバーをシャットダウンしてから、VMware 指定の手順を実行する必要があります。仮想アプライアンスを再起動すると、Cisco EPN Manager は追加されたディスク容量を自動的に利用します（データの収集と消去 （985 ページ）を参照）。
- 1 レベル上の OVA の RAM、ディスク容量、およびプロセッサの最小要件を満たす新しいサーバーをセットアップします。既存のシステムをバックアップして、より高いレベルのサーバー上の仮想マシンに復元します。

ネットワークチーム（リンク集約）の設定

Cisco EPN Manager では、冗長性を維持するために NIC チーミングを作成できます。これにより、1 つの IP アドレスを持つ 1 つの論理インターフェイスに最大 256 の物理インターフェイスをバインドできます。これは、いずれかのインターフェイスがダウンした場合でも接続が中断されないことを意味します。論理インターフェイスでは、通常のインターフェイス操作を実行できます。

（注） チーミングは、NBI に使用される Eth 0/Gigabitethernet 0 ポートではサポートされません。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 論理インターフェイスを設定してから、コンフィギュレーション モードを終了します。

```
config# interface interfaceName
config-InterfaceName# ip addressIP_addresssubnet_mask
config-InterfaceName# member interface1
config-InterfaceName# member interface2
config-InterfaceName# exit
config# exit
```

ここで、

- *interfaceName* には、論理インターフェイスの名前（Team0 など）を指定します。

- *IP_address*、*subnet_mask* には、論理インターフェイスに割り当てる IP アドレスとサブネットマスクを指定します。
- *interface1*、*interface2* には、論理インターフェイスにバインドする物理インターフェイスの名前（GigabitEthernet 1、GigabitEthernet 2 など）を指定します。

ステップ 4 論理インターフェイスの作成を確認します。

```
show interface interfaceName
```

ネットワークトラフィックをフィルタ処理するための IP アクセスリストの作成または変更

Cisco EPN Manager は、*default* という名前の事前設定されたデフォルト IP アクセスリストを維持します。このリストは変更できませんが、NIC に割り当てたり、割り当てを解除することができます。

新しい IP アクセスリストを作成するか変更して、Cisco EPN Manager への入力ネットワークトラフィックをフィルタ処理できます。デフォルトの動作では、IP アクセスリストで明示的に指定されていない限り、ネットワークトラフィックはブロックされます。新しい IP アクセスリストを作成するには、次の手順を実行します。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 ポートおよびプロトコルの情報を指定して IP アクセスリストを作成してから、コンフィギュレーション モードを終了します。

```
config-InterfaceName# ip access-list listname
config-ACL-listname# permit protocol1 port1
config-ACL-listname# permit protocol2 port2
config-ACL-listname# exit
config# exit
```

ここで、

- *listname*：新しい IP アクセスリストの名前（test_acl など）。
- **permit**：ネットワークトラフィックをルーティングするためのプロトコルとポートの情報を追加するコマンド。

（注） ポートを通過する特定の種類のネットワークトラフィックをブロックする場合は、permit コマンドの no 形式を使用します。

ステップ 4 4. 新しく作成された IP アクセスリストを表示するには、次のコマンドを使用します。

```
show running-config
```

インターフェイスへの IP アクセスリストの割り当て

IP アクセスリストをインターフェイスに割り当てるには、次の手順に従います。アクセスグループ（リスト）がすでにNICに割り当てられている場合に新しいものを割り当てると、Cisco EPN Manager によって古いリストが新しいリストに置き換えられます。

重要 異なるインターフェイスに異なるアクセスリストを使用するには、インターフェイスに割り当てられている IP アドレスが同じネットワークまたはサブネットにないことを確認します。

ステップ 1 Cisco EPN Manager CLI 管理者ユーザーとしてサーバーにログインします。Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

ステップ 2 コンフィギュレーション モードを開始します。

```
configure terminal
config#
```

ステップ 3 3. インターフェイスに IP アクセスリストを割り当てます。

```
config# interface interfaceName
config-InterfaceName# ip access-group acl_name  in
config-InterfaceName# exit
config# exit
```

ここで、

- *interfaceName*：インターフェイスの名前。
- **ip access-group**：IP アクセスリストをインターフェイスに追加するコマンド。
- *acl_name*：インターフェイスに割り当てる IP アクセスリスト。
- **in** ：受信の場合。

  （注） 現時点では、この方向のみがサポートされています。

ステップ 4 4. アクセスリストがデバイスに割り当てられているかどうかを確認します。

```
show running-config
```

例

```
config# interface GigabitEthernet 0
config-GigabitEthernet-0# ip access-group test_acl
```

システムの問題を示すサーバー内部 SNMP トラップの使用

Cisco EPN Manager は、システム コンポーネントに関する潜在的な問題を示す内部 SNMP トラップを生成します。これには、ハードウェア コンポーネントの障害、ハイ アベイラビリティ状態の変化、バックアップ ステータスなどが含まれます。障害トラップは、障害または状態の変化が検出されるとすぐに生成され、クリアリング トラップは、障害が修正されると生成されます。TCA（CPU、メモリ、ディスクの高い使用率に関するトラップなど）では、しきい値を超えるとトラップが生成されます。

サーバーの内部 SNMP トラップの完全なリストについては、『Cisco Evolved Programmable Network Manager のサポート対象アラーム』に記載されています。Cisco EPN Manager は通知宛先のポート 162 にトラップを送信します。このポートは現時点ではカスタマイズできません。

以下のトピックの説明に従って、これらのトラップをカスタマイズしたり、管理したりできます。

- サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送 （981 ページ）
- サーバー内部 SNMP トラップをトラブルシュートする （982 ページ）

サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送

トラップの重大度または（TCA の場合）しきい値を調整することで、サーバーの内部 SNMP トラップをカスタマイズできます。また、トラップを無効化/有効化することもできます。サーバーの内部 SNMP トラップは、「*Cisco Evolved Programmable Network* でサポートされているアラーム」で確認できます。

（注） Cisco EPN Manager は SNMPv2 通知も SNMPv3 通知も送信しません。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[アラームおよびイベント（Alarms and Events）]** > **[システム イベントの設定（System Event Configuration）]** を選択します。

ステップ 2 設定する各 SNMP イベントに対して、次の手順を実行します。

a) そのイベントの行をクリックします。

b) 必要に応じて、[イベントの重大度（Event Severity）] を [重大（Critical）]、[メジャー（Major）]、または [マイナー（Minor）] に設定します。

c) CPU、ディスク、およびメモリの使用率や、その他のハードウェアのトラップに対しては、[しきい値値（Threshold）] にパーセンテージ（1 ～ 99）を入力します。これらのイベントは、使用率がしきい値限度を超えたときに、関連の SNMP トラップを送信します。（しきい値設定が NA と表示されるイベントのしきい値は設定できません）。これらのイベントは、関連付けられた障害が検出されるたびにトラップを送信します。

d) [EPNM ユーザーセッション（EPNM User Sessions）] イベントの場合、[しきい値（Threshold）] の値を 1 ～ 150 の範囲で入力します。デフォルトでは、このしきい値の値は 5 です。

e) バックアップしきい値と証明書の有効期日（重要）に対しては、[しきい値値（Threshold）] に日数（*x* ～ *y*）を入力します。ここで、*x* は最小の日数、*y* は最大の日数です。

f) トラップを生成するかどうかを制御するには、[イベントステータス（Event Status）] を設定します。

ステップ 3 **[その他の設定（Other Settings）]** で、**[アラーム反復の作成とクリア（Create and Clear Alarm Iteration）]** に必要な値を入力します。

ステップ 4 トラップの変更内容を保存するには、（テーブルの下にある）[保存（Save）] をクリックします。

ステップ 5 アラームとイベントの最新のリストを表示するには、**[モニター（Monitor）]** > **[モニターリングツール（Monitoring Tools）]** > **[アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 6 サーバーの内部 SNMP トラップの受信者を設定するには、を参照してくださいアラーム通知先の設定（1065 ページ））。

サーバー内部 SNMP トラップをトラブルシュートする

「Cisco Evolved Programmable Network Manager のサポート対象アラーム」では、サーバーの内部 SNMP トラップの完全なリスト、その推定原因、および問題を解決するための推奨処置が提供されています。必要な情報がこのドキュメントに記載されていない場合は、次の手順に従って、Cisco EPN Manager サーバーの問題をトラブルシュートし、詳細情報を入手してください。

ステップ 1 Cisco EPN Manager サーバーから通知レシーバに ping を実行し、Cisco EPN Manager と管理アプリケーション間の接続を確認します。

ステップ 2 ファイアウォールの ACL 設定がポート 162 をブロックしていないかを確認し、必要に応じてそのポートの通信を開きます。

ステップ 3 管理者権限を持つユーザー ID を使用して Cisco EPN Manager にログインします。**Administration > Logging** を選択してログ ファイルをダウンロードします。次に、これらのログ ファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

- ncs_nbi.log：これは Cisco EPN Manager が送信したすべてのノースバウンド SNMP トラップ メッセージのログです。受信していないメッセージの有無をチェックします。
- ncs-#-#.log：これはその他の最新の Cisco EPN Manager アクティビティのログです。受信していないハードウェア トラップ メッセージの有無をチェックします。

- hm-#-#.log：これはすべてのヘルス モニター アクティビティのログです。未受信のハイ アベイラビリティ状態の変更およびアプリケーション プロセス障害に関する、最近のメッセージをチェックします。

これらのログに表示されるメッセージは、管理アプリケーションに表示されるアクティビティと一致する必要があります。大きな違いがある場合は、Cisco Technical Assistance Center（TAC）でサポート ケースを開き、疑わしいログ ファイルをケースに添付してください。シスコ サポート ケースの登録（1090 ページ）を参照してください。

シスコサポート リクエストのデフォルトの設定

デフォルトでは、Cisco EPN Manager GUI のさまざまな部分からシスコサポート リクエストを作成できます。必要に応じて、送信者の電子メール アドレスやその他の電子メールの特性を設定できます。これらを設定しない場合、ユーザーがケースを登録するときに情報を入力できます。

ユーザーが GUI クライアントからリクエストを作成できないようにするには、その機能を無効にします。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、**[一般（General）]** > **[アカウント設定（Account Settings）]** を選択します。

ステップ 2 [サポート リクエスト（Supporte Request）] タブをクリックします。

ステップ 3 必要なインタラクション タイプを選択します。

- [サーバーから直接インタラクションを有効にしてください（Enable interactions directly from the server）]：Cisco EPN Manager サーバーから直接サポート ケースを作成する場合は、このオプションを指定します。サポート プロバイダへの電子メールは、Cisco EPN Manager サーバーに関連付けられているメール アドレス、または指定したメール アドレスから送信されます。
- [クライアントシステムを介したインタラクションのみ（Interactions via client system only）]：サポート ケースに必要な情報をクライアント マシンにダウンロードする場合は、このオプションを指定します。この場合、ダウンロードしたサポート ケースの詳細および情報をサポート プロバイダに電子メールで送信する必要があります。

ステップ 4 テクニカル サポート プロバイダを選択します。

- [Cisco] をクリックし、シスコ テクニカル サポートにサポート ケースを登録し、各自の Cisco.com クレデンシャルを入力し、[接続のテスト（Test Connectivity）] をクリックして次のサーバーへの接続を確認します。
  - Cisco EPN Manager メール サーバー
  - シスコ サポート サーバー
  - フォーラム サーバー

- [サードパーティ サポート プロバイダ（Third-party Support Provider）] をクリックして、サードパーティ サポート プロバイダへのサービス要求を作成します。プロバイダの電子メールアドレス、件名、Web サイト URL を入力します。

シスコ製品フィードバックの設定

シスコ製品の向上のために、Cisco EPN Manager は以下のデータを収集してシスコに送信します。

- 製品情報：製品タイプ、ソフトウェア バージョン、インストール済みライセンス。
- システム情報：サーバーのオペレーティング システムおよび利用可能なメモリ。
- ネットワーク情報：ネットワーク上のデバイスの数とタイプ。

この機能はデフォルトでイネーブルになっています。データは日単位、週単位、または月単位で収集され、HTTPS を使用してシスコ クラウドの REST URL に送信されます。**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[一般（General）] > [改善にご協力ください（Help Us Improve）]** を選択します。

- シスコが収集するデータの種類を確認するには、[シスコが収集するデータについて（What data is Cisco collecting?）] をクリックします。
- この機能を無効にするには、[今回は協力しない（Not at this time, thank you）] を選択し、[保存（Save）] をクリックします。

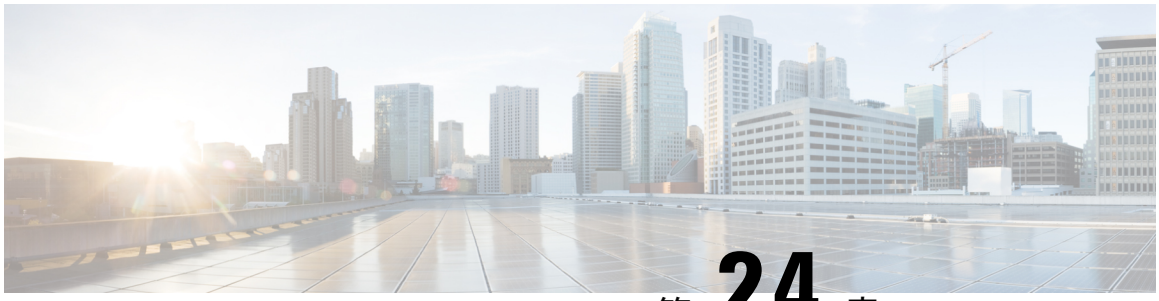
バックアップのモニターリング

ファイル名、サイズ、使用可能なサイズ、データなど、Cisco EPN Manager のバックアップ情報を表示するには、次の手順を使用します。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム監視ダッシュボード（System Monitoring Dashboard）]** を選択します。

ステップ 2 [概要（Overview）] タブをクリックします。このタブに [バックアップ情報（Backup Information）] ダッシュレットが表示されます。

（注） バックアップ ダッシュレットの情報は、バックアップ リポジトリがローカルの場合にのみ使用できます。



第 24 章

データの収集と消去

データ収集ジョブの制御

すべてのデータ収集タスク（およびデータ消去タスク）がジョブ ダッシュボードから制御されます。「ジョブ ダッシュボードを使用したジョブの管理 （32 ページ）」を参照してください。データ収集ジョブは、「システム ジョブ」に一覧表示されています。

システム ジョブについて

次の表に、Cisco EPN Manager が実行するバックグラウンド データ収集ジョブの説明を示します。

表 *56 :* インベントリ データ収集ジョブ

タスク名（Task Name）	デフォルト スケジュール（Default Schedule）	説明	編集可能なオプション
インフラストラクチャ ジョブ			

タスク名（**Task Name**）	デフォルト スケジュール（**Default Schedule**）	説明	編集可能なオプション
データのクリーンアップ（Data Cleanup）	2 時間	このジョブは、日単位のデータファイルのクリーンアップをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
デバイス設定の外部バックアップ（Device Config Backup-External）	15 分	このジョブは、すべてのデバイス設定（Zip形式のテキストファイル）を事前定義された外部リポジトリにエクスポートします。リポジトリの設定や作成は CLI コマンドで行うことができます。サポートされているリポジトリは FTP、SSH FTP（SFTP）、ネットワーク ファイル システム（NFS）です。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。 [編集（Edit）] アイコンをクリックし、[最新の設定のみをエクスポートする（Export only Latest Configuration）] チェックボックスをオンにすると、最新の設定のみが転送されます。 ロールベース アクセス コントロール（RBAC）で設定されたユーザー権限に基づいて、ジョブのプロパティを編集することができます。
インデックス検索エンティティ（Index search Entities）	3 時間	このジョブは、インデックス検索エンティティをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
サーバーのバックアップ（Server Backup）	1 日	このジョブは、Cisco EPN Managerサーバーの自動バックアップをスケジュールします。作成されるバックアップは、アプリケーション バックアップです。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名（**Task Name**）	デフォルト スケジュール（**Default Schedule**）	説明	編集可能なオプション
スマート ライセンスのコンプライアンス ステータス（Smart License Compliance Status）	無効	このジョブは、スマートライセンスに対してデフォルトのスケジュールで実行されます。	編集不可。
インベントリおよびディスカバリ ジョブ			
スイッチインベントリ（Switch Inventory）	1 日	このジョブは、特定のスケジュールに従って定期的に到達可能な検出済みデバイスのインベントリを収集します。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
failedFeatureSync	30 分	このジョブは、CWW 内のデバイスの失敗した機能のみのインベントリを収集し、デバイス CF の定期的な完全同期を実行します。このジョブはデフォルトで一時停止されます。顧客は選択に基づいて有効化できます。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ステータス ジョブ			
自律型 AP の動作ステータス（Autonomous AP Operational Status）	5 分	このジョブは、自律型ワイヤレスアクセスポイントのステータスポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
スイッチの動作ステータス（Switch Operational Status）	5 分	このジョブは、ノードの到達可能性をチェックします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名（Task Name）	デフォルト スケジュール（Default Schedule）	説明	編集可能なオプション
サードパーティ アクセス ポイントの動作ステータス（Third party Access Point Operational Status）	3 時間	このジョブは、サードパーティ AP の動作ステータス ポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
サードパーティ コントローラの動作ステータス（Third party Controller Operational Status）	3 時間	このジョブは、サードパーティコントローラの動作ステータスポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ワイヤレス AP 検出（Wireless AP Discovery）	5 分	このジョブは、ワイヤレス AP検出をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

データ保持設定が Web GUI データに及ぼす影響

[データの保持（Data Retention）] ページで加えた変更に従って、Web GUI に表示される情報が決まります。[データの保持（Data Retention）] ページを開くには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、さらに **[一般（General）] > [データの保持（Data Retention）]** を選択します。

たとえば、7 日より前の古い履歴パフォーマンス データが不要な場合、パフォーマンス データ保持の値を次のように変更できます。

- [短期データ保持期間（Short-term Data Retention Period）] : 1 日
- [中期データ保持期間（Medium-term Data Retain Period）] : 3 日
- [長期データ保持期間（Long-term Data Retain Period）] : 7 日

このような設定に変更すると、パフォーマンス レポートおよびパフォーマンス ダッシュボードに表示されるすべてのデータは、過去 7 日間のみが対象になります。パフォーマンス レポートを作成すると、過去 7 日間より長いレポート期間を選択した場合でも、レポートには過去 7 日間のデータのみが含まれます（これは、保持するように選択したデータが 7 日間分であるためです）。

同様に、パフォーマンス ダッシュボードを表示して1週間を超える時間枠を選択しても、ダッシュボードには過去 7 日間の日付のみが含まれます。

インターフェイスのモニターリング ポリシーを作成する際に、15 分ごと、5 分ごと、または1分ごとのポーリング間隔を定義できます。選択したポーリング間隔に基づいてデバイスデータがポーリングされ、Oracle データベースに保存されます。データは 1 時間ごとに AHxxx テーブルに集約されます。また、1/5/15 分に設定されたポーリング間隔に関係なく、ADxxx テーブルへの集約が 1 日に 1 回行われます。

[インターフェイスヘルスポリシー（Interface Health Policy）] タブでは、頻度が 5 分に設定されている場合は、1 時間あたり 12 個のサンプルを表示できます。1 時間ごとにデータが集約テーブルに移動されてインターフェイス統計の平均値が算出され、1 時間ごとの集約テーブルに 1 つのエントリが表示されます。ポーリング間隔に関係なく、集約はすべてのポリシーで同一です。

データ保持の詳細とデータストレージの期間、イベント時間（ミリ秒単位）、および各データベースのエンティティ ID とイベント時間を表示できます。パフォーマンスデータと集約データは、[パフォーマンス ダッシュレット（Performance Dashlet）] > [インターフェイス（Interfaces）] > [トラフィック使用率（Traffic Utilization）] タブに表示されます。

パフォーマンスおよびシステムのヘルス データ保持

（注） デフォルト設定はインタラクティブ グラフから最も役立つ情報を取得するように最適化されているため、トレンド、デバイス ヘルス、システム ヘルス、およびパフォーマンス データの保持期間を変更しないことをお勧めします。

次の表に、[データの保持（Data Retention）] ページに表示される情報を示します。

データのタイプ	説明	デフォルトの保持設定	保持設定範囲
傾向データの保持期間（Trend Data Retain Periods）	デバイス関連の履歴情報。トレンドデータは全体として収集され、最小、最大、または平均として要約されます。	毎時データの保持期間：15（日） 日次データの保持期間：90（日） 週次データの保持期間：54（週）	時間単位のデータ：1 ～ 31（日） 日単位のデータ：7 ～ 365（日） 週単位のデータ：2 ～ 108（週）

データのタイプ	説明	デフォルトの保持設定	保持設定範囲
デバイスヘルスデータの保持期間（Device Health Data Retain Periods）	デバイスの到達可能性などの SNMP ポーリングされたデバイスデータ、およびCPU、メモリ、インターフェイスの使用率。	毎時データの保持期間：15（日） 日次データの保持期間：90（日） 週次データの保持期間：54（週）	時間単位のデータ：1 ー 31（日） 日単位のデータ：7 ー 365（日） 週単位のデータ：2 ～ 108（週）
パフォーマンスデータの保持期間（Performance Data Retain Periods）	トラフィック統計などの保証データ。 • 短期データは 5 分ごとに集約されます。 • 中期データは 1 時間ごとに集約されます。 • 長期データは 1 日ごとに集約されます。 （注） **[詳細設定（Advanced Settings）]** をクリックして、使用可能な属性の **[経過時間（日）（Age (In days)）]** と **[最大レコード数（Max Records）** を設定できます。	短期データの保持期間：7（日） 中期データの保持期間：31（日） 長期データの保持期間：378（日）	短期の範囲：1 ー 31（日） 中期の範囲：7 ー 365（日） 長期の範囲：2 ー 756（日）
ユーザージョブデータ保持期間	完了状態のユーザージョブのすべてのレコード。	ユーザージョブデータ保持期間：7（日）	2 ～ 365（日）

データのタイプ	説明	デフォルトの保持設定	保持設定範囲
システムヘルスデータの保持期間（System Health Data Retain Periods）	管理ダッシュボードに表示されるほとんどのデータが含まれます。	毎時データの保持期間：1（日） 日次データの保持期間：7（日） 週次データの保持期間：54（週）	時間単位のデータ範囲：1 ー 31（日） 日単位のデータ範囲：7 ー 365（日） 週単位のデータ範囲：2 ー 108（週）

たとえば、これらは光パフォーマンス データの保持設定です。

- [オプティカル30秒（Optical 30 secs）] のパフォーマンスデータ（短期）は 1 時間保存されます。
- 光回線の 15 分間のパフォーマンスデータ（短期）はデフォルトでは 1 日間保存されます。1 ー 14日の範囲で日数を変更できます。
- 光回線の 1 日のパフォーマンスデータ（中期）は、デフォルトで 30 日間保存されます。30 ー 90 日の範囲で日数を変更できます。

データベース テーブル別のデータ保持の指定

管理者は、[データ保存（Data Retention）] ページの [その他のデータ保存基準（Other Data Retention Criteria）] セクションを使用して、特定の Cisco EPN Manager データベース テーブルの保持期間を設定できます。次の属性を使用して保持期間を指定できます。

- [期間（時間単位）（Age (in hours)）]：データベース内のすべてのレコードの最大データ保持期間を時間単位で指定します。
- [最大レコード数（Max Records）]：特定のデータベース テーブルに保持するレコードの最大数を指定します。[最大レコード数（Max Records）] の値が「NA」の場合、考慮される保持条件が [経過時間（Age）] 属性のみであることを意味します。

セクションは、複数のサブセクションに分類されます。それぞれのサブセクションには、各データベース テーブル名と現在の [経過時間（Age）] および [最大レコード数（Max Records）] の値が一覧表示されます。これらの値によって、テーブル内の個々のレコードが保持されるか破棄されるかが決定されます。このページには、テーブル内のデータの期間経過を計算するために使用される [経過時間（Age）] 属性テーブルも一覧表示されます。

このセクションのいずれかのテーブルの値を変更するときは、事前に Cisco Technical Assistance Center に相談することを強くお勧めします。支援なしに変更すると、システム パフォーマンスに悪影響を与える可能性があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）]l > [データの保持（Data Retention）]** の順に選択します。

ステップ 2 [その他のデータ保存基準（Other Data Retention Criteria）] セクションを展開します。

ステップ 3 [経過時間（Age）] および [最大レコード数（Max Records）] の値を指定するデータベース テーブル サブセクションを展開します。

ステップ 4 一覧表示しているデータベース テーブルをクリックし、必要に応じて新しい値を入力します。

ステップ 5 [保存（Save）] をクリックします。

アラーム、イベント、および Syslog の消去

（注） これらのデフォルトの消去設定は、最適なパフォーマンスを保証するために用意されています。これらの設定を調整するときには、特に Cisco EPN Manager が非常に大規模なネットワーク（これらの設定値を大きくすると悪影響が生じる可能性がある）を管理している場合に注意が必要です。

Cisco EPN Manager は、最大 8000000 個のイベントと 2000000 個の syslog をデータベースに格納します。

システム パフォーマンスを保護するため、Cisco EPN Manager は次の表の設定に従ってアラーム、イベント、および syslog を消去します。これらの設定はすべてデフォルトで有効化されます。データは毎日削除されます。アラーム テーブルは毎時チェックされ、アラーム テーブルが 300,000 の上限を超えた場合、Cisco EPN Manager は、アラーム テーブルのサイズが制限内に収まるまで、最も古いクリア済みアラームを削除します。

データ タイプ	削除されるまでの日数：	デフォルト設定
アラーム：クリア済みのセキュリティ アラーム	30日間	有効
アラーム：クリア済みの非セキュリティ アラーム	7 日	有効
イベント	60 日	有効
Syslogs	30日間	有効
アラーム	30日間	無効

設定を変更するには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択して、**[アラームおよびイベント（Alarms and Events）]** > **[アラームおよびイベント（Alarms and Events）]** を選択し、[アラームおよびイベントのクリーンアップ オプション（Alarm and Event Cleanup Options）] エリアの設定を変更します。

ログの消去

ログの消去設定を調整するには、**[管理（Administration）]** > **[設定（Settings）]** > **[ロギング（Logging）]** を選択します。ログは最大サイズに達するまで保存されます。最大サイズに達した時点で、ログ ファイルに番号が追加され、新しいログが開始されます。ログの数が最大数を超えると、最も古いログが削除されます。

次の表に、一般ログと SNMP ログのデフォルトの消去値をリストします。

ログ タイプ	ログのサイズ	ログの数	設定を変更する場合の参照先：
一般	10 MB	10	一般的なログ ファイルの設定とデフォルト サイズの調整 （1098 ページ）
SNMP	10 MB	5	一般的なシステム ログを表示して管理する（1097 ページ）

レポートの消去

デフォルトでは、リポジトリに保存されているレポートは 7 日後に削除されます。

リポジトリのディレクトリパスは次のとおりです。

- **スケジュール済みレポートのリポジトリ**：/localdisk/ftp/reports
- **オンデマンドレポートのリポジトリ**：localdisk/ftp/reportsOnDemand

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** の順に選択し、**[一般（Genera）]** > **[レポート（Reports）]** を選択します。

ステップ 2 必要に応じて、サーバー上のレポート リポジトリの場所を変更します。リポジトリは、FTP ルート パーティションの下になければなりません。

ステップ 3 デフォルトの消去までの経過期間を変更する場合は、[ファイルの保持期間（File Retain Period）] フィールドを 1 ～ 366 日の範囲の値で更新します。デフォルトの保持期間は 7 日間です。

ステップ 4 [保存（Save）] をクリックします。

保持期間を更新すると、Cisco EPN Manager はレポートをすぐには消去せず、一晩経過した後にのみ消去します。

バックアップの消去

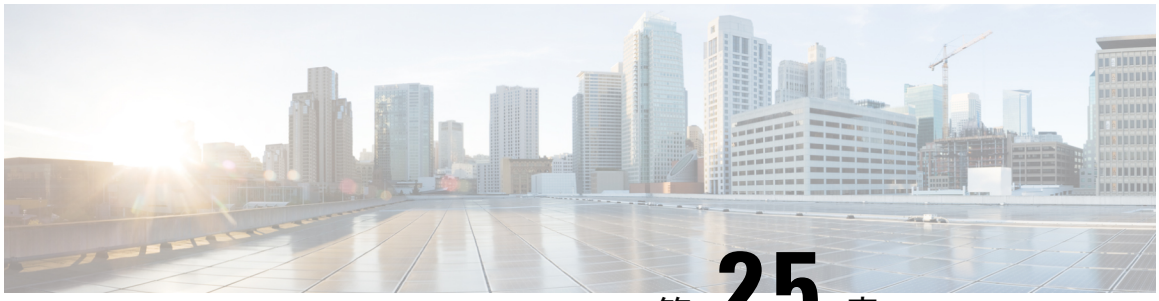
デフォルトで、2つのバックアップがローカル リポジトリに保存されます。リモート リポジトリを使用している場合は、自動バックアップ消去メカニズムがありません。古いバックアップを手動で削除する必要があります。保存する自動アプリケーション バックアップ数の変更（943 ページ） を参照してください。

デバイス コンフィギュレーション ファイルの消去

デバイスごとに、5つのコンフィギュレーション ファイルが設定アーカイブに保存されます。30 日より前のファイルは消去されます。デバイス コンフィギュレーション ファイルは手動で削除することができません。デバイス コンフィギュレーション ファイルの詳細については、デバイス コンフィギュレーション ファイルの管理 （141 ページ）を参照してください。

ソフトウェア イメージ ファイルの消去

デバイス ソフトウェア イメージ ファイルは、データベースから自動的には消去されません。このファイルは、GUI クライアントを使用して手動で削除する必要があります。詳細については、イメージ リポジトリからのソフトウェア イメージ ファイルの削除 （189 ページ）を参照してください。



第 25 章

ユーザー権限とデバイス アクセス

ユーザーインターフェイス、ユーザータイプ、およびそれらの間の遷移

これらのトピックでは、Cisco EPN Manager で使用される GUI と CLI インターフェイス、および Cisco EPN Manager と Linux CLI インターフェイス間の遷移について説明します。

ユーザー インターフェイスとユーザー タイプ

次の表に、Cisco EPN Manager （CEPNM）によって採用されたユーザー インターフェイスと、各インターフェイスにアクセス可能なユーザーのタイプの説明を示します。

CEPNMユーザーインターフェイス	インターフェイスの説明	CEPNM ユーザー タイプ
CEPNM Web GUI	Web GUI を使用して日常業務と管理業務を容易にする Web インターフェイス。これらのユーザーは、さまざまなレベルの権限を持つことができ、ロールベース アクセス コントロール（RBAC）クラスとサブクラスに分類されます。 このインターフェイスは、Cisco EPN Manager の CLI 管理ユーザーと CLI 構成ユーザーによって提供される操作のサブセットを提供します。	[Cisco EPN Manager Web GUI通常ユーザー（Cisco EPN Manager web GUI everyday users）]：Web GUI のルートユーザーによって作成されます。このユーザーは、さまざまなレベルの権限を持ち、ユーザー グループ（管理者、スーパー ユーザー、構成マネージャなど）と呼ばれるロールベース アクセス コントロール（RBAC）クラスとサブクラスに分類されます。ユーザー グループについては、ユーザー グループのタイプ （999 ページ）を参照してください。 **Cisco EPN Manager** Web GUI ルート ユーザー：インストール時に作成され、Web GUI への 1 回目のログインと他のユーザー アカウントの作成に使用されます。このアカウントは、管理者権限を持つ少なくとも 1 人の Web GUI ユーザー、つまり、管理者ユーザーまたはスーパー ユーザー ユーザー グループに属している Web GUI ユーザーの作成後に無効にする必要があります。Web GUI ルート ユーザーの無効化および有効化 （998 ページ）を参照してください。 （注） Cisco EPN Manager Web GUI ルート ユーザーは、Linux CLI ルート ユーザーと同じではなく、Cisco EPN Manager CLI 管理者ユーザーとも異なります。
[ノースバウンドインターフェイス（NBI）REST API（North Bound Interface (NBI) REST API）]	NBI は REST アプリケーション プログラミング インターフェイスであり、クライアントシステムが Cisco EPN Manager と通信して通常の操作および管理操作を実行できるようにします。NBI は REST アプリケーション プログラミング インターフェイスであり、クライアントシステムが Cisco EPN Manager と通信して日常的な操作および管理操作を実行できるようにします。 また、これらの NBI ユーザーは、さまざまなレベルの権限を持つこともでき、ロールベース アクセス コントロール（RBAC）クラスとサブクラスにも分類されます。	[Cisco EPN Manager NBIユーザー（Cisco EPN Manager NBI users）]：Web GUI ルートユーザーによって作成されます。これらのユーザーには、3 種類の異なる権限があり、ロールベース アクセス コントロール（RBAC）クラスと NBI ユーザーグループというサブクラス（NBI 読み取りおよび NBI 書き込み）に分類されます。ユーザーグループの詳細については、次の項を参照してください。 ユーザー グループ - NBI （1000 ページ）

CEPNM ユーザー インターフェイス	インターフェイスの説明	CEPNM ユーザー タイプ
CEPNM 管理者 CLI	システムへのセキュアで限定的なアクセスを提供するシスコ独自のシェル（Linux シェルと比較した場合）。この管理者シェルと CLI は、高度な Cisco EPN Manager 管理タスク用のコマンドを提供します。これらのコマンドについては、このガイドを通して説明します。この CLI を使用するには、Cisco EPN Manager CLI 管理者ユーザー アクセス権を持っている必要があります。SSH を使用してリモート コンピュータからこのシェルにアクセスできます。	**Cisco EPN Manager CLI 管理者ユーザー**：インストール時に作成され、アプリケーションの停止と再起動やリモート バックアップ リポジトリの作成などの管理操作に使用されます（この管理操作のサブセットは、Web GUI で使用できます）。 このユーザーが実行可能な操作のリストを表示するには、プロンプトで **?** と入力します。 一部のタスクは、コンフィギュレーション モードで実行する必要があります。コンフィギュレーション モードに移行するには、Cisco EPN Manager 管理 CLI と Cisco EPN Manager 構成 CLI の切り替え （998 ページ）内の手順を使用します。
CEPNM 構成 CLI	Linux シェルよりセキュアで限定されたシスコ独自のシェル。この構成シェルと CLI は、Cisco EPN Manager システム設定タスク用のコマンドを提供します。これらのコマンドについては、このガイドを通して説明します。この CLI を使用するには、管理者レベルのユーザー アクセス権を持っている必要があります（この表の [ユーザー タイプ（User Types）] 列内の情報を参照）。管理者 CLI シェルでこのシェルにアクセスできます。	管理者 CLI ユーザーは、次のコマンドを使用して、さまざまな理由で他の CLI ユーザーを作成できます。 `(config) username username password role {admin|user} password` これらのユーザーには、作成期間に定義された管理者に準ずる権限/ロールまたはより低レベルの権限を付与できます。管理者権限を持つ Cisco EPN Manager CLI ユーザーを作成するには、**admin** キーワードを指定して **username** コマンドを実行します。それ以外のユーザーを作成する場合は、**user** キーワードを使用します。パスワードの制限については、管理者ユーザーの作成 （920 ページ）を参照してください。
Linux CLI	すべての Linux コマンドを提供する Linux シェル。Linux シェルは、シスコ テクニカル サポート担当者のみが使用できます。標準のシステム管理者は、Linux シェルを使用しないでください。SSH を使用してリモート コンピュータからこのシェルに到達することはできません。到達するには、Cisco EPN Manager 管理者シェルと CLI を経由する必要があります。	**Linux CLI 管理ユーザー**：インストール時に作成され、Linux レベルの管理目的に使用されます。

Cisco EPN Manager で CLI ユーザー インターフェイスを切り替える方法

Cisco EPN Manager 管理 CLI と Cisco EPN Manager 設定 CLI 間の移行方法については、次のセクションを参照してください

Cisco EPN Manager 管理 CLI と Cisco EPN Manager 構成 CLI の切り替え

Cisco EPN Manager 管理 CLI から Cisco EPN Manager 構成 CLI に移行するには、admin プロンプトで **config** と入力します。

```
(admin)# config
(config)#
```

構成 CLI から管理 CLI に戻るには、config プロンプトで **exit** または **end** と入力します。

```
(config)# exit
(admin)#
```

Cisco EPN Manager Web GUI のルートへのアクセスの有効化および無効化

管理者権限またはスーパーユーザー権限を持つ他の Web GUI ユーザーを 1 人以上作成したら、Cisco EPN Manager Web GUI **root** ユーザーを無効にする必要があります。Web GUI ルート ユーザーの無効化および有効化 （998 ページ）を参照してください。

Web GUI ルート ユーザーの無効化および有効化

ステップ 1 ルートとして Cisco EPN Manager Web GUI にログインし、ルート権限を持つ別の Web GUI ユーザー（つまり、管理ユーザー グループまたはスーパー ユーザー グループに属する Web GUI ユーザー）を作成します。上記のステップが完了すると、Web GUI **root** アカウントを無効化できるようになります。

ステップ 2 次のコマンドを実行して Cisco EPN Manager Web GUI ルート ユーザー アカウントを無効化します（Web GUI 管理アカウントはアクティブな状態に維持されるので、必要なすべての CLI 関数を実行できます）。

```
ncs webroot disable
```

ステップ 3 アカウントを再び有効にするには、次のコマンドを実行します。

```
ncs webroot enable
```

ユーザーが実行できるタスクWebインターフェイスの制御

Web インターフェイス ユーザーの場合、Cisco EPN Manager では、ユーザー認証はユーザーグループを使用して実装されます。ユーザー グループには、ユーザーがアクセスできる Cisco EPN Manager の部分およびユーザーがその部分で実行できるタスクを制御するタスクの一覧が含まれています。

ユーザー グループはユーザーの操作を制御しますが、仮想ドメインはユーザーがこれらのタスクを実行できるデバイスを制御します。仮想ドメインの詳細については、「デバイスへのユーザー アクセスを制御するための仮想ドメインの作成 （1030 ページ）」を参照してください。

Cisco EPN Manager では、いくつかのユーザー グループが事前定義されています。ユーザーがユーザー グループに属している場合、ユーザーはそのグループのすべての認証設定を継承します。ユーザーは通常、アカウントが作成されるときにユーザー グループに追加されます。

次のトピックでは、ユーザー認証の管理方法について説明します。

ユーザー グループのタイプ

Cisco EPN Manager は、次の事前定義のユーザー グループを提供します。

CLIユーザーについては、ユーザーインターフェイスとユーザータイプ （995ページ）を参照してください）。

ユーザー グループ：Web UI

Cisco EPN Manager は、次の表にリストされているデフォルトの Web GUI ユーザーグループを提供します。Monitor Liteユーザーグループに属するユーザーを除き、ユーザーを複数のグループに割り当てることができます（Monitor Lite は、権限が制限されているユーザー向けであるためです）。

各ユーザーグループとデフォルト設定に関係するタスクについては、グループで実行できるタスクを表示および変更する （1019 ページ）を参照してください。

ユーザー グループ	グループ タスク フォーカス
Root	すべての操作。このグループの権限は編集できません。インストール後に、root Web UI ユーザーが使用可能になります。ユーザー インターフェイスとユーザー タイプ（995 ページ）を参照してください。Web GUI ルート ユーザーの無効化および有効化（998 ページ）に説明されているとおり、Admin または Super Users 権限で別のユーザーを作成し、root Web UI ユーザーを無効にすることをお勧めします。
Super Users	すべての操作（デフォルトなし）。このグループの権限は編集できます。ルートユーザーの権限に類似した権限を有効にすることができます。
Admin	システムとサーバーを管理します。モニターリングや設定に関する操作を実行できます。このグループの権限は編集できます。
Config Managers	ネットワークを設定およびモニターします（管理タスクは行いません）。このグループに割り当てられる権限は、編集可能です。
System Monitoring	ネットワークをモニターします（設定タスクは行いません）。このグループの権限は編集できます。
Help Desk Admin	ヘルプデスクとユーザー設定関連のページにしかアクセスできません。これは、ユーザーインターフェイスへのアクセスがない特殊なグループです。
Lobby Ambassador	ゲスト ユーザーのみのユーザー管理。このユーザー グループのメンバーは、他のユーザー グループのメンバーを兼ねることはできません。
User–Defined 1 ～ 50	N/A：これらはブランクのグループで、必要に応じて編集したり、カスタマイズしたりできます。
Monitor Lite	ネットワーク トポロジおよびユーザー タグを表示します。このグループの権限は編集できません。このユーザー グループのメンバーは、他のユーザー グループのメンバーを兼ねることはできません。
North Bound API	SOAP API にアクセスします。
User Assistant	ローカル ネット ユーザー管理のみ。このユーザー グループのメンバーは、他のユーザー グループのメンバーを兼ねることはできません。
mDNS Policy Admin	mDNS ポリシー管理機能。

ユーザー グループ - NBI

Cisco EPN Manager は、次の表に記載されているデフォルトの NBI ユーザーグループを提供します。これらのグループ内の権限は編集できません。

各ユーザー グループとデフォルト設定に関係するタスクについては、グループで実行できるタスクを表示および変更する （1019 ページ）を参照してください。

ユーザー グループ	アクセス対象：
NBI Read	RESTCONF NBI 読み取り操作（HTTP GET）。他の NBI または Web UI ユーザー グループに属することもできます。
NBI Write	RESTCONF NBI 書き込み操作（HTTP PUT、POST、DELETE）。他の NBI または Web UI ユーザー グループに属することもできます。

ユーザーが実行できるタスクの表示と変更

ユーザーが実行できるタスクは、ユーザーが所属するユーザー グループによって制御されます。ユーザーが所属するグループと、ユーザーが実行する権限を持つタスクを確認するには、次の手順を実行します。

（注） ユーザーがアクセスできるデバイスを確認する場合は、ユーザーへの仮想ドメインの割り当て（1037 ページ）を参照してください。

ステップ 1 **[管理（Administrration）]>[ユーザー（Users）]>[ユーザー、ロール、およびAAA（Users, Roles & AAA）]** を選択し、ユーザー名を見つけます。

ステップ 2 ユーザー名を見つけて、[以下のメンバー（Member of）] の列をチェックして、ユーザーが所属するユーザー グループを見つけます。

ステップ 3 ユーザー グループのハイパーリンクをクリックします。[グループの詳細（Group Detail）] ウィンドウで、グループのメンバーが実行できるタスクと実行できないタスクのリストを表示します。

- チェックが付けられているチェックボックスは、グループ メンバーがそのタスクを実行する権限を持っていることを意味します。チェックボックスがグレー表示されている場合は、タスクを無効にできません。たとえば、Cisco EPN Manager では、Monitor Lite ユーザー グループの [タグの表示（View tags）] タスクを削除できません。これは、そのユーザー グループにとって不可欠なタスクであるためです。
- チェックボックスがオフの場合は、グループ メンバーがそのタスクを実行できないことを示します。オフのチェックボックスがグレー表示されている場合は、そのユーザー グループに対してタスクを有効にすることができません。

Web GUI ルートと Monitor Lite グループ、および NBI グループは編集できません。

ステップ 4 権限を変更するには、次の選択肢があります。

（注） この操作は慎重に行ってください。[グループ詳細（Group Detail）] ウィンドウでタスクのチェックボックスをオンまたはオフにすると、すべてのグループ メンバーに変更が適用されます。

- すべてのユーザー グループのメンバーの権限を変更します。グループで実行できるタスクを表示および変更する （1019 ページ）を参照してください。
- 別のユーザー グループにユーザーを追加します。事前定義されたユーザー グループについては、ユーザー グループ：Web UI （999 ページ） とユーザー グループ - NBI （1000 ページ） で説明します。これらのトピックでは、グループの制限についても説明します。たとえば、ユーザーが事前定義済みの Monitor Lite ユーザー グループに属している場合、そのユーザーは他のグループに所属することはできません。
- このグループからユーザーを削除します。ユーザーが属しているグループを表示して変更する （1002 ページ）を参照してください。
- カスタマイズされたユーザー グループを使用し、ユーザーをそのグループに追加します。既存のカスタマイズされたグループを確認するには、グループで実行できるタスクを表示および変更する （1019 ページ）を参照してください。新たにカスタマイズされたグループを作成するには、カスタム ユーザー グループの作成 （1019 ページ）を参照してください。

ユーザーが属しているグループを表示して変更する

ユーザーが実行可能なタスクは、そのユーザーが属しているユーザー グループによって決定されます。通常は、ユーザー アカウントの作成時に設定されます（ユーザーの追加および削除 （1023 ページ）を参照）。ユーザー グループについては、ユーザー グループのタイプ （999 ページ）で説明します。

この手順では、ユーザーが属しているグループを表示し、必要に応じて、ユーザーのグループ メンバーシップを変更する方法について説明します。

ステップ 1 ＞[管理（Administration）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] を選択してから、[ユーザー（Users）] をクリックします。

ステップ 2 [ユーザー名（User Name）] 列で、ユーザー名のハイパーリンクを探してクリックし、[ユーザーの詳細（User Details）] ウィンドウを開きます。すべてのユーザー グループが [一般（General）] タブの下に一覧表示されます。

- オンになっているチェックボックスは、ユーザーがそのグループに属していることを意味します。オンになっているボックスが灰色表示されている場合は、そのグループからユーザーを削除できないことを意味します。たとえば、Cisco EPN Manager では、ルート ユーザー グループから **root** という名前のユーザーを削除できません。
- オフになっているチェックボックスは、ユーザーがそのグループに属していないことを意味します。オフになっているチェックボックスが灰色表示されている場合は、そのグループにユーザーを追加できないことを意味します

（グループが実行可能なタスクをチェックするには、左側のサイドバー メニューで、[ユーザー グループ（User Groups）] を選択し、グループ名をクリックします）。

ステップ 3 ユーザーが属しているグループを変更するには、[ユーザーの詳細（User Details）] ウィンドウで該当するグループを選択して選択解除してから、[保存（Save）] をクリックします。

ユーザー グループとそのメンバーの表示

ユーザーは、Monitoring Lite などの非常に制限されたグループに属していない限り、複数のグループに所属できます。この手順では、既存のユーザー グループとそのメンバーを表示する方法を説明します。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザー グループ（User Groups）] をクリックします。

[ユーザー グループ（User Groups）] ページには、既存のすべてのユーザー グループとそのメンバーの短いリストが表示されます。これらのグループの詳細については、ユーザー グループのタイプ （999 ページ）を参照してください。

ステップ 2 グループのすべてのメンバーを表示するには、グループのハイパーリンクをクリックして[グループの詳細（Group Details）] ウィンドウを開き、[メンバー（Members）] タブをクリックします。

ステップ 3 これらのグループを変更する場合は、以下を参照してください。

- グループで実行できるタスクを表示および変更する （1019 ページ）
- ユーザーが属しているグループを表示して変更する （1002 ページ）

ユーザーグループの権限とタスクの説明

次の表に、ユーザーグループの権限とタスクの説明を示します。

表 *57 :* ユーザーグループの権限とタスクの説明

タスクグループ名	タスク名	説明
Administrative Operations	デバイスコンソール設定	ユーザーはデバイスコンソールで設定コマンドを実行できます
	デバイスコンソール表示	ユーザーはデバイスコンソールで show コマンドを実行できます
	監査ログのエクスポート（Export Audit Logs Access）	ユーザーは [管理メガ（Admin Mega）] メニューから [インポートポリシーの更新（Import Policy Update）] にアクセスできます
	ヘルスモニターの詳細（Health Monitor Details）	ユーザーはサイトのヘルススコア定義を変更できます
	ハイ アベイラビリティ設定	ユーザーはプライマリサーバーとセカンダリサーバーのペアリングに [ハイアベイラビリティ（High Availability）] を設定できます
	インポートポリシーの更新（Import Policy Update）	ユーザーはポリシーの更新を手動でダウンロードし、コンプライアンスおよび監査マネージャエンジンにインポートできます
	ライセンスセンター/スマートライセンス（License Center/Smart License）	ユーザーはライセンスセンター/スマートライセンスにアクセスできます
	ログ	ユーザーはログレベルを設定できるメニュー項目にアクセスできます
	スケジュールされたタスクとデータコレクション（Scheduled Tasks and Data Collection）	バックグラウンドタスクを表示する画面へのアクセスを制御します
	システム設定（System Settings）	

タスクグループ名	タスク名	説明
		[管理（Administration）] > [システム設定（System Settings）] メニューへのアクセスを制御します
	ユーザー定義フィールド	ユーザーはユーザー定義フィールドを作成できます
	ユーザー設定	[管理（Administration）] > [ユーザー設定（User Preference）] メニューへのアクセスを制御します。
	監査ログの表示へのアクセス（View Audit Logs Access）	ユーザーは [ネットワーク（Network）] および [システム監査（System audits）] を表示できます

タスクグループ名	タスク名	説明
Alerts and Events	ACK アラートおよび UNACK アラート（Ack and Unack Alerts）	ユーザーは既存のアラームの確認応答または確認応答解除を実行できます
	アラームポリシー（Alarm Policies）	ユーザーはアラームポリシーにアクセスできます。
	アラームポリシーの編集アクセス（Alarm Policies Edit Access）	ユーザーはアラームポリシーを編集できます
	アラートの削除およびクリア（Delete and Clear Alerts）	ユーザーはアクティブアラームをクリアおよび削除できます
	電子メール通知	ユーザーは電子メール通知の転送を設定できます
	通知ポリシーの読み取りアクセス（Notification Policies Read Access）	ユーザーはアラーム通知ポリシーを表示できます
	通知ポリシーの読み取り/書き込みアクセス（Notification Policies Read-Write Access）	ユーザーはアラーム通知ポリシーを設定できます
	アラートの選択および選択解除（Pick and Unpick Alerts）	ユーザーはアラートを選択および選択解除できます
	トラブルシューティング	ユーザーはアラームで traceroute や ping などの基本的なトラブルシューティングを実行できます
	アラート状態の表示（View Alert Condition）	ユーザーはアラート条件を表示できます。
	アラートとイベントの表示（View Alerts and Events）	ユーザーはイベントおよびアラームのリストを表示できます
ライセンスの確認	ライセンスの確認	ユーザーはコントローラライセンスやMSEライセンスなどのライセンスの有効性を確認できます

タスクグループ名	タスク名	説明
[設定（Configure）] メニュータスク	[設定（Configure）] メニューアクセス	ユーザーは設定メニューのすべての機能にアクセスできます
	デバイス設定エクスポートのサニタイズの解除	ユーザーは、サニタイズされていない設定アーカイブを公開できます
診断タスク（Diagnostic Tasks）	診断情報（Diagnostic Information）	[診断（Diagnostic）] ページへのアクセスを制御します。
	デバイス設定エクスポートのサニタイズの解除	ユーザーは、サニタイズされていない設定アーカイブを公開できます
フィードバックタスクとサポートのタスク	自動フィードバック（Automated Feedback）	自動フィードバックにアクセスできます
	TAC ケース管理ツール（TAC Case Management Tool）	ユーザーは TAC ケースを開くことができます
グローバル変数の設定（Global Variable Configuration）	グローバル変数へのアクセス（Global Variable Access）	ユーザーはグローバル変数にアクセスできます。
グループ管理（Groups Management）	グループメンバーの追加（Add Group Members）	ユーザーはデバイスやポートなどのエンティティをグループに追加できます
	グループの追加（Add Groups）	ユーザーはグループを作成できます
	グループメンバーの削除（Delete Group Members）	ユーザーはグループからメンバーを削除できます
	グループの削除	ユーザーはグループを削除できます
	グループのエクスポート（Export Groups）	ユーザーはグループをエクスポートできます
	グループのインポート（Import Groups）	ユーザーはグループをインポートできます
	グループの変更（Modify Groups）	ユーザーは名前、親、ルールなどのグループ属性を編集できます

タスクグループ名	タスク名	説明
[ヘルプ（Help）] メニュータスク	[ヘルプ（Help）] メニューアクセス	ユーザーは [ヘルプ（Help）] メニューにアクセスできます
[ホーム（Home）] メニュータスク	[ホーム（Home）] メニューアクセス	ユーザーはホームページにアクセスできます

タスクグループ名	タスク名	説明
ジョブ管理	ジョブの承認（Approve Job）	ユーザーは別のユーザーに承認を得るためにジョブを送信できます
	ジョブのキャンセル（Cancel Job）	ユーザーは実行中のジョブをキャンセルできます
	[ジョブの削除（Delete Job）]	ユーザーは [ジョブ（Jobs）] ダッシュボードからジョブを削除できます
	[ジョブの編集（Edit Job）]	ユーザーは [ジョブ（Jobs）] ダッシュボードからジョブを編集できます
	ジョブの一時停止（Pause Job）	ユーザーは実行中のジョブとシステムジョブを一時停止できます
	ジョブのスケジュール（Schedule Job）	ユーザーはジョブをスケジュールできます
	ジョブの表示（Schedule Job）	ユーザーはスケジュール済みのジョブを表示できます
	編集ジョブの展開の設定（Config Deploy Edit Job）	ユーザーは展開済みのジョブの設定を編集できます
	デバイス設定バックアップジョブの編集アクセス（Device Config Backup Job Edit Access）	ユーザーはリポジトリやファイル暗号化パスワードなどの外部バックアップ設定を変更できます
	ジョブ通知メール（Job Notification Mail）	ユーザーはさまざまなジョブタイプに関して通知メールを設定できます
	ジョブの実行（Run Job）	ユーザーは一時停止されたジョブとスケジュール済みのジョブを実行できます
	[システムジョブ（System Jobs）] タブへのアクセス	ユーザーはシステムジョブを表示できます
[モニター（Monitor）] メニュータスク	[モニター（Monitor）] メニューアクセス	ユーザーは [モニター（Monitor）] メニューのすべての機能にアクセスできます

タスクグループ名	タスク名	説明
ネットワーク構成	デバイスの追加アクセス（Add Device Access）	ユーザーは Cisco EPN Manager にデバイスを追加できます
	管理テンプレートへの書き込みアクセス（Admin Templates Write Access）	ユーザー定義ロールの管理テンプレートへの書き込みアクセスを有効にするには、このチェックボックスをオンにします
	自動プロビジョニング（Auto Provisioning）	自動プロビジョニングにアクセスできます
	アラームモニターポリシー	アラームモニターポリシーにアクセスできます
	コンプライアンス監査の修正アクセス（Compliance Audit Fix Access）	ユーザーはコンプライアンス修正ジョブおよびレポートを表示、スケジュール、エクスポートできます
	コンプライアンス監査 PAS へのアクセス（Compliance Audit PAS Access）	ユーザーは「PSIRT」および「EOX」のジョブおよびレポートを表示、スケジュール、エクスポートできます。
	コンプライアンス監査ポリシーへのアクセス（Compliance Audit Policy Access）	ユーザーはコンプライアンスポリシーを作成、変更、削除、インポート、エクスポートできます
	コンプライアンス監査プロファイルへのアクセス（Compliance Audit Profile Access）	ユーザーはコンプライアンス監査ジョブまたはレポートについては表示、スケジュール、エクスポートでき、違反概要については表示およびダウンロードできます
	コンプライアンス監査プロファイル編集アクセス（Compliance Audit Profile Edit Access）	ユーザーはコンプライアンスプロファイルについては作成、変更、削除でき、コンプライアンス監査ジョブまたはレポートについては表示、スケジュール、エクスポートでき、違反概要については表示およびダウンロードできます

タスクグループ名	タスク名	説明
	設定アーカイブの読み取りタスク	設定アーカイブの読み取りアクセスを許可します
	設定アーカイブの読み取り/書き込みタスク	設定アーカイブの読み取り/書き込みアクセスを許可します
	設定テンプレートへの読み取りアクセス（Configuration Templates Read Access）	読み取り専用モードで設定テンプレートにアクセスできます
	ACS View Server の設定（Configure ACS View Servers）	ACS View Server にアクセスして管理できます
	設定グループの設定（Configure Config Groups）	設定グループにアクセスできます
	ISE サーバーの設定	ユーザーは Cisco EPN Manager で ISE サーバーを管理できます
	テンプレートの設定（Configure Templates）	ユーザーは機能テンプレートの CRUD 操作を実行してテンプレートを設定できます
	クレデンシャルプロファイルの Add_Edit へのアクセス（Credential Profile Add_Edit Access）	ユーザーはクレデンシャルプロファイルを追加および編集できます
	クレデンシャルプロファイルの削除アクセス（Credential Profile Delete Access）	ユーザーはクレデンシャルプロファイルを削除できます
	クレデンシャルプロファイルの表示アクセス（Credential Profile View Access）	ユーザーはクレデンシャルプロファイルを表示できます
	デバイスアクセスの削除（Delete Device Access）	ユーザーは Cisco EPN Manager からデバイスを削除できます
	アクセス設定の展開（Deploy Configuring Access）	ユーザーは設定と IWAN テンプレートを展開できます
	設計設定テンプレートへのアクセス（Design Configuration Template Access）	

タスクグループ名	タスク名	説明
		ユーザーは、[設定（Configuration）] から共有ポリシー オブジェクト テンプレートや設定グループテンプレートを作成できます
	デバイス一括インポートアクセス（Device Bulk Import Access）	ユーザーはCSV ファイルからデバイスの一括インポートを実行できます
	デバイス表示設定アクセス（Device View configuration Access）	ユーザーはデバイスワークセンターでデバイスを設定できます
	デバイスアクセスの編集（Edit Device Access）	ユーザーはデバイスクレデンシャルやデバイスのその他の詳細情報を編集できます
	デバイスアクセスのエクスポート（Export Device Access）	ユーザーはクレデンシャルなどのデバイスのリストを CSV ファイルとしてエクスポートできます。
	ネットワーク デバイス	ユーザーはネットワークデバイスにアクセスできます
	ネットワークトポロジの編集（Network Topology Edit）	ユーザーはトポロジマップでデバイス、リンク、ネットワークを作成でき、手動で作成したリンクを編集して、インターフェイスを割り当てることができます
	プロビジョニングアクセス	プロビジョニングにアクセスできます
	QoS プロファイル設定アクセス	ユーザーは次の操作を行えます。QoS プロファイルの作成/変更/削除、QoS プロファイルの展開ジョブのスケジュール、またはインターフェイスの関連付け/関連付け解除、および検出済み QoS プロファイルのインポート/エクスポート

タスクグループ名	タスク名	説明
ネットワーク モニターリング	管理ダッシュボードへのアクセス（Admin Dashboard Access）	ユーザーは管理ダッシュボードにアクセスできます
	シャーシビューの読み取り	シャーシビューの読み取りにアクセスできます
	シャーシビューの読み取り/書き込み	シャーシビューの読み取り/書き込みにアクセスできます
	設定監査ダッシュボード（Config Audit Dashboard）	ユーザーは設定監査ダッシュボードにアクセスできます
	データ収集管理アクセス（Data Collection Management Access）	ユーザーは [アシュアランス データソース（Assurance Data Sources）]ページにアクセスできます
	詳細ダッシュボードへのアクセス（Details Dashboard Access）	ユーザーは詳細ダッシュボードにアクセスできます
	インシデントアラームイベントへのアクセス（Incidents Alarms Events Access）	ユーザーはインシデントアラームイベントにアクセスできます。
	最新の設定監査レポート（Latest Config Audit Report）	ユーザーは最新の設定監査レポートを表示できます
	ネットワーク トポロジ	ユーザーはネットワークトポロジマップを起動し、マップ内のデバイスとリンクを表示できます
	パフォーマンス ダッシュボードへのアクセス（Performance Dashboard Access）	ユーザーはパフォーマンス ダッシュボードにアクセスできます

タスクグループ名	タスク名	説明
OTDR	OTDR 設定プロファイル	OTDR 設定プロファイルにアクセスできます
	OTDR 実行スキャン	ユーザーは OTDR スキャンにアクセスできます
	OTDR 設定基準	OTDR 基準にアクセスできます
	OTDR ビューのスキャン結果	ユーザーは OTDR スキャン結果を表示できます
製品使用状況レポート	製品のフィードバック	ユーザーは [改善にご協力ください（Help Us Improve）] ページにアクセスできます

タスクグループ名	タスク名	説明
レポート	デバイス レポート	ユーザーはデバイスに関連する特定のレポートのモニターリングに固有のレポートを実行できます
	読み取り専用デバイスレポート（Device Reports Read Only）	ユーザーは生成されたデバイスレポートを読むことができます。
	Network Summary レポート	ユーザーはネットワーク サマリー レポートを作成および実行できます。
	読み取り専用ネットワーク サマリー レポート（Network Summary Reports Read Only）	ユーザーはすべてのサマリーレポートを表示できます
	光パフォーマンス レポート	ユーザーは光パフォーマンスレポートを作成できます
	読み取り専用光パフォーマンスレポート	ユーザーは光パフォーマンスレポートを表示できます
	パフォーマンス レポート	ユーザーはパフォーマンスレポートを作成できます
	読み取り専用パフォーマンスレポート（Performance Reports Read Only）	ユーザーはパフォーマンスレポートを表示できます
	レポート ラウンチ パッド	ユーザーは [レポート（Report）] ページにアクセスできます
	レポート実行履歴（Report Run History）	ユーザーはレポート履歴を表示できます
	レポートリストの実行（Run Reports List）	ユーザーはレポートを実行できます
	保存済みレポートリスト（Saved Reports List）	ユーザーはレポートを保存できます
	システム モニターリング レポート	ユーザーはシステム モニターリング レポートを表示できます

タスクグループ名	タスク名	説明
	仮想ドメインリスト（Virtual Domains List）	ユーザーは仮想ドメインの関連のレポートを作成できます。

タスクグループ名	タスク名	説明
ソフトウェア イメージの管理	ソフトウェアイメージ管理サーバーの追加（Add Software Image Management Servers）	ユーザーはソフトウェアイメージ管理サーバーを追加できます
	イメージ詳細ビュー	ユーザーはイメージの詳細を表示できます
	プロトコルの管理	ユーザーはプロトコルを管理できます
	SWIM のアクセス権限	SWIM のアクセス権限
	SWIM の有効化	SWIM の有効化
	SWIM 収集	SWIM 収集
	SWIM の削除	SWIM の削除
	SWIM のディストリビューション	SWIM のディストリビューション
	SWIM のユーザー設定の保存	ユーザーは [システム設定（System Settings）] > [イメージ管理（Image Management）] ページで設定オプションを保存できます
	ソフトウェア情報の更新	ユーザーは最小 RAM、最小 FLASH、最小ブート ROM のバージョンなど、イメージのプロパティを編集して保存できます
	SWIM の推奨事項	ユーザーは Cisco.com およびローカルリポジトリからイメージを推奨できます
	SWIM のアップグレード分析	ユーザーはソフトウェアイメージを分析して、ソフトウェアのアップグレードを実行する前に、ハードウェアのアップグレード（該当する場合はブート ROM、フラッシュメモリ、RAM、ブートフラッシュ）が必要かどうかを判断できます

タスクグループ名	タスク名	説明
ユーザー管理	監査証跡	ユーザーはユーザーのログインおよびログアウトに関する[監査証跡（Audit trails）]にアクセスできます
	LDAP サーバー（LDAP Server）	ユーザーは [LDAPサーバー（LDAP Server）] メニューにアクセスできます
	RADIUS サーバー	ユーザーは [RADIUSサーバー（RADIUS Servers）] メニューにアクセスできます
	SSO サーバー AAA モード（SSO Server AAA Mode）	ユーザーは [AAA] メニューにアクセスできます。
	SSO サーバー	ユーザーは [SSO] メニューにアクセスできます。
	TACACS+ サーバー	ユーザーは [TACACS+サーバー（TACACS+ Servers）] メニューにアクセスできます。
	ユーザーとグループ	ユーザーは[ユーザーとグループ（Users and Groups）] メニューにアクセスできます
	仮想ドメイン管理（Virtual Domain Management）	ユーザーは[仮想ドメイン管理（Virtual Domain Management）] メニューにアクセスできます
	[仮想要素（Virtual Elements）] タブへのアクセス（Virtual Elements Tab Access）	仮想ドメインを作成、またはメンバーを仮想ドメインに追加する場合、ユーザーは[仮想要素（Virtual Elements）] タブにアクセスすることができ、仮想要素（データセンター、クラスタ、ホスト）を仮想ドメインに追加できます
オンラインヘルプの表示（View Online Help）	OnlineHelp	ユーザーはオンラインヘルプにアクセスできます

カスタム ユーザー グループの作成

Cisco EPN Manager に用意されている一連の定義済みユーザー グループを利用してユーザーの権限を制御できます。これらの定義済みグループ（ユーザー グループのタイプ （999 ページ）を参照）に含まれているユーザー定義グループをカスタマイズすることで、展開に固有のユーザー グループを作成できます。次の手順で、4つの定義済みユーザー定義グループテンプレートのうちの 1 つを使用してカスタム グループを作成する方法を説明します。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[ユーザー グループ（User Groups）] を選択します。

ステップ 2 メンバーがないユーザー定義グループを見つけて、そのグループ名のハイパーリンクをクリックします。

ステップ 3 [グループの詳細（Group Detail）] ウィンドウでタスクをオンまたはオフにして、グループ アクセス権限をカスタマイズします。タスクが灰色で表示されている場合、その設定を調整することはできません。ユーザーグループの名前を変更することはできません。.

ステップ 4 [保存（Save）] をクリックして設定を保存します。

ステップ 5 グループにメンバーを追加するには、該当するユーザー アカウントを編集して、そのユーザーを新しいグループに追加します。ユーザーアカウントの調整の詳細については、ユーザーの追加および削除 （1023 ページ）を参照してください。

グループで実行できるタスクを表示および変更する

既存のユーザー グループに関する情報と、グループ メンバーが実行できるタスクに関する情報を入手するには、次の手順に従ってください。事前定義されているユーザー グループの詳細については、「ユーザー グループとそのメンバーの表示 （1003 ページ）」を参照してください。

（注） デバイスアクセスを変更する場合は、「ユーザーへの仮想ドメインの割り当て （1037ページ）」を参照してください。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザー グループ（User Groups）] を選択します。

[ユーザー グループ（User Groups）] ページには、既存のすべてのユーザー グループが一覧表示されます。

ステップ 2 ユーザー グループのハイパーリンクをクリックします。[グループの詳細（Group Detail）] ウィンドウに、グループのアクセス許可が一覧表示されます。

- チェックマークの付いているタスクは、グループ メンバーがそのタスクを実行する権限を持っていることを示します。チェックボックスがグレー表示されている場合は、タスクを無効にできません。

- チェックボックスがオフの場合は、グループ メンバーがそのタスクを実行できないことを示します。オフのチェックボックスがグレー表示されている場合は、そのユーザー グループに対してタスクを有効にすることができません。

Web GUI ルートと Monitor Lite グループ、および NBI グループは編集できません。

ステップ 3 すべてのグループ メンバーに影響するグループの権限を変更する場合は、タスクのチェックボックスをオンまたはオフにして、[保存（Save）] をクリックします。

（注） この操作は慎重に行ってください。[グループ詳細（Group Detail）] ウィンドウでタスクのチェックボックスをオンまたはオフにすると、すべてのグループ メンバーに変更が適用されます。この操作の代わりに、[ユーザー定義（User Defined）] グループ テンプレートの 1 つを使用して新しいグループを作成する方法もあります。「カスタム ユーザー グループの作成（1019 ページ）」を参照してください。

RADIUS および TACACS+ での Cisco EPN Manager ユーザー グループの使用

Cisco EPN Manager に存在するユーザー グループを認識するように、RADIUS または TACACS+ サーバーを設定する必要があります。RADIUS および TACACS+ の Cisco EPN Manager ユーザー グループとロール属性のエクスポート（1020 ページ）の手順に従って、これを実行できます。

RADIUS および TACACS+ の Cisco EPN Manager ユーザー グループとロール属性のエクスポート

RADIUS または TACACS+ を使用している場合は、すべての Cisco EPN Manager ユーザー グループおよびロール情報を Cisco Access Control Server（ACS）または Cisco Identity Services Engine（ISE）サーバーにコピーする必要があります。これを行うには、Cisco EPN Manager Web GUI にある [タスク リスト（Task List）] ダイアログボックスを使用します。データを Cisco ACS または Cisco ISE サーバーにエクスポートしない場合、Cisco EPN Manager は、ユーザーに割り当てられたタスクの実行を許可しません。

次の情報をエクスポートする必要があります。

- TACACS+：仮想ドメインおよびロールの情報が必要です（タスクは自動的に追加されます）。
- RADIUS：仮想ドメインおよび権限の情報が必要です（タスクは自動的に追加されます）。

[タスク リスト（Task List）] ダイアログの情報は、Cisco ACS サーバー用に事前に書式設定されています。

（注） 外部サーバーにタスクを追加するときには、[ホーム メニュー アクセス（Home Menu Access）] タスクを必ず追加してください。これはすべてのユーザーで必須です。

始める前に

「外部認証の設定 （1041 ページ）」の説明に従い、AAA サーバーを追加し、AAA モードを設定していることを確認してください。

ステップ 1 Cisco EPN Manager で、次の手順を実行します。

a) **[管理（Administration）] > [ユーザー（Users）] > [ユーザーグループ（User Groups）]** を選択します。

b) [ユーザーグループ（User Groups）] テーブルで、ユーザー グループ行の末尾にある [タスクリスト（Task List）] ハイパーリンクをクリックして、各ユーザー グループのロールをコピーします。

- RADIUS を使用している場合は、[RADIUSカスタム属性（RADIUS Custom Attributes）] フィールドの role0 行を右クリックして、[コピー（Copy）] を選択します。
- TACACS+ を使用している場合は、[TACACS+カスタム属性（TACACS+ Custom Attributes）] フィールドの role0 行を右クリックして、[コピー（Copy）] を選択します。

ステップ 2 Cisco ACS または Cisco ISE サーバーに情報を貼り付けます。次の手順は、Cisco ACS の既存のユーザー グループに情報を追加する方法を示しています。この情報をまだ Cisco ACS または Cisco ISE に追加していない場合は、次を参照してください。

- Cisco ACS と RADIUS または TACACS+ を使用した外部認証
- Cisco ISE と RADIUS または TACACS+ による外部認証 （1043 ページ）

a) [ユーザー設定（User Setup）] または [グループ設定（Group Setup）] に移動します。

b) 該当するユーザーまたはグループの [設定の編集（Edit Settings）] をクリックします。

c) 該当するテキスト ボックスに属性一覧を貼り付けます。

d) これらの属性を有効にするチェックボックスをオンにしてから、[送信して再起動（Submit + Restart）] をクリックします。

ユーザーの追加およびユーザー アカウントの管理

管理者権限を持つ Web GUI ユーザーの作成

インストール後、Cisco EPN Manager には **root** という名前の GUI ルート アカウントが作成されています。このアカウントは、サーバーに初めてログインして次のものを作成するために使用されます。

- 製品および機能を管理する、管理者権限を持つ Web GUI ユーザー
- その他すべてのユーザー アカウント

通常の操作には Web GUI root アカウントを使用しないでください。セキュリティ上の理由から、管理者権限（およびすべてのデバイスへのアクセス権）を持つ新しい Web GUI ユーザーを作成した後には Web GUI root アカウントを無効にしてください。

ステップ 1 **[管理（Administration）]**>**[ユーザー（Users）]**>**[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザー（Users）] を選択します。

ステップ 2 [ユーザー名（Username）] テキストボックスにユーザー名を入力します。

ステップ 3 パスワードを入力します。新しいパスワードは、パスワードポリシーで指定された条件を満たす必要があります。[?] アイコンをクリックして、パスワードポリシーを表示します。

（オプション）[新しいパスワードを生成（Generate New Password）] ボタンをクリックして、システムによって生成されるセキュアなパスワードを設定します。このボタンをクリックすると、新しいパスワードが隣のテキストボックスに表示されます。[新しいパスワード（New password）] および [パスワードの確認（Confirm password）] テキストボックスにも同じものが表示されます。目のアイコンをクリックするとパスワードの表示/非表示が切り替わります。[コピー（Copy）] ボタンをクリックして、パスワードをクリップボードにコピーすることもできます。

ダイアログボックス内の値をクリアするには、[リセット（Reset）] ボタンをクリックします。

ステップ 4 （オプション）ユーザーの [名（First Name）]、[姓（Last Name）]、および [説明（Description）] を入力します。

ステップ 5 [電子メールアドレス（Email Address）] テキストボックスに電子メールアドレスを入力します。

ステップ 6 [一般（General）] タブの [このユーザーに割り当てられているグループ（Groups Assigned to This User）] で、[管理（Admin）] をクリックします。

ステップ 7 [仮想ドメイン（Virtual Domains）] タブをクリックして、ユーザーがアクセスできるデバイスを指定します。すべてのデバイスへのアクセス権を持つ管理者 Web GUI ユーザー（ROOT-DOMAIN）を 1 つ以上作成する必要があります。仮想ドメインの詳細については、デバイスへのユーザー アクセスを制御するための仮想ドメインの作成 （1030 ページ）を参照してください。

（注） 親仮想ドメインを選択すると、その下の子（従属）仮想ドメインも選択されます。

ステップ 8 [保存（Save）] をクリックします。

（注） 新しいユーザーを作成するときは、ブラウザにユーザーのログイン情報を自動入力したり保存したりしないでください。

次のタスク

まだ行っていない場合は、セキュリティ上の理由から、Web GUI ルート ユーザーの無効化および有効化 （998 ページ）の説明に従って Web GUI root アカウントを無効にしてください。

ユーザーの追加および削除

ユーザー アカウントを作成する前に、デバイス アクセスを制御するための仮想ドメインを作成し、アカウントの作成時にそれらの仮想ドメインを適用できるようにします。この作業を行わないと、ユーザー アカウントを編集してドメイン アクセスを追加しなければならなくなります。デバイスへのユーザー アクセスを制御するための仮想ドメインの作成 （1030 ページ）を参照してください。

アカウントを（削除するのではなく）一時的に無効にするには、ユーザー アカウントの無効化（ロック） （1024 ページ）を参照してください。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザー（Users）] を選択します。

ステップ 2 [ユーザーの追加（Add User）] をクリックします。

ステップ 3 ユーザー アカウントを設定します。

a) ユーザー名とパスワードを入力します。

（注） パスワードを自動生成するには、ユーザー名と電子メールアドレスを入力します。詳細については、ユーザーのパスワードの自動生成 （1024 ページ）を参照してください。

b) ユーザーの名、姓、説明を入力します。

c) ユーザーが実行できるアクションを制御するために、1 つ以上のユーザー グループを選択します。ユーザー グループについては、ユーザー グループとそのメンバーの表示 （1003 ページ）を参照してください。

d) ユーザーがアクセスできるデバイスを制御するために、[仮想ドメイン（Virtual Domains）] タブをクリックし、ドメインをユーザーに割り当てます。（デバイスへのユーザー アクセスを制御するための仮想ドメインの作成 （1030 ページ）を参照）。

ステップ 4 **[保存（Save）]** をクリックします。

（注） 新しいユーザーを作成するときは、ブラウザにユーザーのログイン情報を自動入力したり保存したりしないでください。

ステップ 5 ユーザーを削除するには、ユーザーを選択して **[ユーザーの削除（Delete User(s)）]** をクリックします。

ユーザー アカウントの無効化（ロック）

一時的にユーザーが Cisco EPN Manager GUI にログインできないようにするには、ユーザー アカウントを無効にします。ユーザーが一時的にジョブ機能を変更する場合にこのように設定することがあります。ユーザーがログインしようとすると、Cisco EPN Manager では、アカウントがロックされているためにログインが失敗したことを伝えるメッセージが表示されます。ユーザーを再作成することなく、後でアカウントをアンロックできます。ユーザーアカウントを削除する場合は、ユーザーの追加および削除 （1023 ページ）を参照してください。

期限失効前にパスワードを変更しなかった場合は、自動的にユーザーアカウントが無効になります。この場合、パスワードをリセットできるのは管理者だけです。ユーザーのパスワードを変更する （1024 ページ）およびローカル認証のためのグローバル パスワード ポリシーの設定（1027 ページ）を参照してください。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、次に [ユーザー（Users）] をクリックします。

ステップ 2 アクセスを無効または有効にするユーザーを選択します。

ステップ 3 [ユーザーのロック（Lock User(s)）]（または [ユーザーのロック解除（Unlock User(s)）] をクリックします。

ユーザーのパスワードを変更する

パスワードルールを設定して、ユーザーにパスワードの変更を義務付けることができます（ローカル認証のためのグローバル パスワード ポリシーの設定 （1027 ページ）を参照）。ユーザーは、パスワードの変更 （4 ページ）の説明に従って、自分のパスワードを変更できます。ユーザーのパスワードを手動で変更するには、次の手順を実行します。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[ユーザー（Users）] をクリックします。

ステップ 2 ユーザー名のハイパーリンクをクリックします。

ステップ 3 新しいパスワードをパスワード フィールドに入力してから、[保存（Save）] をクリックします。

ユーザーのパスワードの自動生成

Cisco EPN Manager には、電子メールサーバーの可用性に基づいて新規および既存のユーザーのパスワードを自動生成するオプションが用意されています。このオプションが有効になっている場合、システムはパスワードの詳細を含む電子メールをユーザーに送信します。

（注） [パスワードの自動生成（Auto-generate Passwords）] オプションは、電子メールサーバーが設定されている場合にのみ使用できます。

パスワードを自動生成してユーザーに電子メールで送信するには、次の手順を実行します。

始める前に

電子メールサーバーを設定します。詳細については、SMTP 電子メール サーバーの設定 （969 ページ）を参照してください。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles, & AAA）]** > **[ローカルパスワードポリシー（Local Password Policy）]** を選択します。

ステップ 2 [パスワードの自動生成（Auto-generate Passwords）] チェックボックスをオンにします。

ステップ 3 [保存（Save）] をクリックして変更を保存します。

ステップ 4 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** に移動し、[ユーザー（Users）] をクリックします。

a) 新しいユーザーの場合は、ユーザー名と電子メールアドレスを入力します。

b) 既存のユーザーの場合は、[パスワードのリセット（Reset Password）] を選択します。

ステップ 5 [保存（Save）] をクリックして変更を保存し、ユーザーに電子メール通知を送信します。

現在ログイン中のユーザーの確認

現在 Cisco EPN Manager サーバーにログインしているユーザーを確認するには、この手順に従います。また、現在の Web GUI セッションおよび過去のセッションでユーザーが実行した操作の履歴リストを参照することもできます。

（注） デフォルトでは、Cisco EPN Manager は後続の 50 個のレコードをページネーションなしで表示します。50 個を超えるレコードを表示するには、画面の右上隅にある [settings] アイコンをクリックし、**[My Preferences]** > **[General]** > **[Items per Page List]** フィールドに必要な値を入力します。

ステップ 1 **[管理（Administration）]** > **[ユーザ（Users）]** > **[ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択し、[アクティブなセッション（Active Sessions）] をクリックします。Cisco EPN Manager により、Cisco EPN Manager サーバに現在ログインしているすべてのユーザと、各ユーザのクライアントマシンの IP アドレスがリストされます。ユーザーが管理対象デバイスに対して何らかのアクションを実行すると（ユーザーが新しいデバイスを Cisco EPN Manager に追加する場合など）、デバイスの IP アドレスが [デバイスの IP アドレス（Device IP Address）] 列にリストされます。

ステップ 2 このユーザーが実行したすべてのアクションの履歴リストを表示するには、ユーザー名に対応する監査証跡アイコンをクリックします。

ステップ 3 アクティブなユーザーセッションを終了する場合は、[セッションの終了（End Session）] をクリックします。

（注） [セッションの終了（End Session）] は、アクティブなユーザーセッションのみを終了します。ユーザーが再度ログインしないようにするには、ユーザーアカウントの無効化（ロック） （1024 ページ）を参照してください。

ユーザーが実行するタスクを表示する（監査証跡）

Cisco EPN Manager は、アクティブな Web GUI セッションおよび過去の Web GUI セッションでユーザーが実行したすべてのアクションの履歴を保持します。特定のユーザーまたは特定のユーザー グループのすべてのメンバーが実行したタスクの履歴を一覧表示するには、次の手順に従ってください。監査情報には、タスクの説明、ユーザーがタスクを実行したクライアントの IP アドレス、およびタスクが実行された時刻が含まれます。タスクが管理対象デバイスに影響した場合（ユーザーが新しいデバイスを追加したまたは [デバイスコンソール（Device Console）] を使用してネットワーク要素上でコマンドを発行した場合など）は、影響を受けたデバイスの IP アドレスが [デバイスの IP アドレス（Device IP Address）] 列に表示されます。複数のデバイスが変更された場合（たとえば、ユーザーが構成テンプレートを 10 個のスイッチに展開した場合）は、Cisco EPN Manager によって、各スイッチの監査エントリが表示されます。

Cisco EPN Manager Web GUI に現在ログインしているユーザーを確認するには、「現在ログイン中のユーザーの確認 （1025 ページ）」を参照してください。

ユーザー固有ではない監査を表示するには、次のトピックを参照してください。

- GUI から実行されたアクションを監査する（システムの監査） （1095 ページ）
- ユーザーによって行われる変更の監査（変更の監査） （1093 ページ）

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択します。

ステップ 2 特定のユーザーが実行するタスクを表示するには：

1. [ユーザー（Users）] を選択します。
2. ユーザー名を見つけて、そのユーザーに対応する [監査証跡（Audit Trail）] アイコンをクリックします。

ステップ 3 ユーザー グループのすべてのメンバーが実行したタスクの履歴リストを表示するには、次の手順に従ってください。

1. [ユーザー グループ（User Groups）] を選択します。
2. ユーザー グループ名を見つけて、そのグループに対応する [監査証跡（Audit Trail）] アイコンをクリックします。

ジョブ承認者を設定してジョブを承認する

ネットワークに大きな影響を与える可能性があるジョブを制御するには、ジョブ承認を使用します。ジョブを承認する必要がある場合は、Cisco EPN Manager が管理者権限を持っているすべてのユーザーに電子メールを送信し、彼らの誰かが承認するまでジョブを実行しません。ジョブが承認者によって拒否された場合は、そのジョブがデータベースから削除されます。デフォルトでは、どのジョブでも承認は不要です。

ジョブ承認がすでに有効になっており、承認が必要なジョブを表示したり、ジョブを承認したり、ジョブを拒否したりする場合は、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）]** を選択してから、[ジョブ承認（Job Approval）] リンクをクリックします。

ジョブ承認を有効にし、実行する前に承認が必要なジョブを設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[一般（General）] > [ジョブ承認（Job Approval）]** を選択します。

ステップ 2 [ジョブ承認の有効化（Enable Job Approval）] チェックボックスをオンにします。

ステップ 3 承認用に設定するジョブを探して、それらを左側のフィールドから右側のフィールドに移動します。たとえば、管理ユーザーがデバイスの新規追加を承認するように設定する場合は、[インポートジョブ（Import job）] タイプを移動します。

ステップ 4 カスタマイズされたジョブのタイプを指定するには、正規表現を使用して [ジョブ タイプ（Job Type）] フィールドに文字列を入力し、[追加（Add）] をクリックします。たとえば、Config で始まるすべてのジョブ タイプに対してジョブ承認を有効にするには、「**Config.***」と入力します。

ステップ 5 [保存（Save）] をクリックします。

ローカル認証のためのグローバルパスワードポリシーの設定

ローカル認証（Cisco EPN Manager の認証メカニズム）を使用している場合、Web GUI からグローバル パスワード ポリシーを制御します。外部認証を使用して Cisco EPN Manager ユーザー

を認証している場合、ポリシーは、外部アプリケーションによって制御されます（CLI を使用した外部認証の設定 （915 ページ）を参照）。

デフォルトでは、ユーザーは、任意の期間の経過後にパスワードの変更が強制されることはありません。パスワード変更を強制し、他のパスワード ルールを設定するには、**[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ローカル パスワード ポリシー（Local Password Policy）] を選択します。

（注） 新しいユーザーが Cisco EPN Manager への初回ログイン時にデフォルトのパスワードを変更するように要求するには、[パスワードの変更（Change password）] を選択する必要があります。このチェックボックスをオフにすると、ログイン時に [ホームダッシュボード（Home Dashboard）] ページが開きます。

許可される同時セッションの数の設定

Cisco EPN Manager は、同時に実行できる同時セッションの数を設定するオプションを提供します。最大 15 の同時セッションを設定できます。

（注） この設定は、Cisco EPN Manager Web インターフェイスからログインしたセッションにのみ適用されます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバー（Server）]** を選択します。

ステップ 2 [Parallel Sessions] で、[Number of parallel sessions allowed] フィールドに 1 ～ 50 の範囲の値を入力します。

ステップ 3 [保存（Save）] をクリックします。この変更を有効にするには、システムを再起動する必要があります。

アイドル ユーザー用のグローバル タイムアウトを設定する

Cisco EPN Manager には、アイドル ユーザーを自動的にログアウトするタイミングと方法を制御する、以下の 2 つの設定があります。

- [ユーザー アイドル タイムアウト（User Idle Timeout）]：タイムアウトになったときにユーザー セッションを自動的に終了するこの設定を無効にするか設定することができます。この設定はデフォルトで有効になっており、15 分に設定されています。

- [グローバル アイドル タイムアウト（Global Idle Timeout）]：[ユーザー アイドル タイムアウト（User Idle Timeout）] 設定よりも優先されます。[グローバルアイドルタイムアウト（Global Idle Timeout）] はデフォルトで有効になっており、15 分に設定されています。管理者権限を持つユーザーのみが [グローバル アイドル タイムアウト（Global Idle Timeout）] の設定を無効化したり、そのタイムリミットを変更できます。

アイドルタイムアウト機能は、ブラウザが開くと動作し始めますが、ユーザーの操作はありません。つまり、アイドルタイムアウトが 10 分で、ブラウザが開いており、ユーザーにキーストロークやマウスクリックがない場合、ユーザーは 10 分間非アクティブになるとログアウトされます。ただし、ブラウザが Cisco EPN Manager からログアウトすることなく強制終了されると、デフォルトでは Cisco EPN Manager に設定されたアイドルタイムアウト値に関わらず、60 分後に期限切れになります。

デフォルトで、クライアント セッションは無効になっており、ユーザーは 15 分間非アクティブだった場合に自動的にログアウトされます。これは、すべてのユーザーに適用されるグローバル設定です。セキュリティ上の理由から、このメカニズムは無効にしないでください。ただし、次の手順を使用して、タイムアウト値を調整できます。アイドルユーザーのタイムアウトを無効にするか変更するには、アイドルユーザーのタイムアウトの無効化（1029ページ）を参照してください。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択してから、**[一般（General）]** > **[サーバー（Server）]** を選択します。

ステップ 2 [グローバル アイドル タイムアウト（Global Idle Timeout）] 領域で、[すべてのアイドル ユーザーをログアウトする（Logout all idle users）] チェックボックスがオンになっていること確認します（これは、メカニズムが有効になっていることを意味します）。

ステップ 3 [後にすべてのアイドル ユーザーをログアウトする（Logout all idle users after）] ドロップダウン リストで、値を選択することによって、タイムアウトを設定します。

ステップ 4 [保存（Save）] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

アイドル ユーザーのタイムアウトの無効化

デフォルトでは、一定の期間にわたって何も行われないと、クライアントセッションが無効になりユーザーは自動的にログアウトされます。これはすべてのユーザーに適用されるグローバル設定です。インストール中にログアウトしないようにするには、次の手順に従って、システム設定でアイドル ユーザーの自動ログアウトを無効にすることを推奨します。

（注） [グローバル アイドル タイムアウト（Global Idle Timeout）] 設定は、[ユーザー アイドル タイムアウト（User Idle Timeout）] 設定より優先されます。[グローバル アイドル タイムアウト（Global Idle Timeout）] の設定を行うには、アイドルユーザー用のグローバル タイムアウトを設定する （1028 ページ）を参照してください。

顧客がシステム設定で [すべてのアイドルユーザーをログアウト（Logout all idle users）] を無効にするか、またはルートユーザーのマイプリファレンス設定で [アイドルユーザーをログアウト（Logout idle user）] を無効にするか、あるいはその両方で無効にするかに関係なく、Web サーバーのセッションタイムアウトに到達すると、セッションは最終的にタイムアウトします。これは、基本的にセキュリティポスチャを維持するためです。セッションタイムアウトの増減に関するガイドラインについては、https://owasp.org/www-community/Session_Timeout を参照してください。

（注） セッションは非アクティブな場合にのみタイムアウトしますが、アクティブなユーザーセッションはタイムアウトしません。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバー（Server）]** を選択します。

ステップ 2 [グローバル アイドル タイムアウト（Global Idle Timeout）] エリアで、[すべてのアイドル ユーザーをログアウトする（Logout all idle users）] チェックボックスをオフにし、[保存（Save）] をクリックします。

ステップ 3 Web GUI ウィンドウの右上にある ⚙ をクリックし、[マイ プリファレンス（My Preferences）] を選択します。

ステップ 4 [ユーザー アイドル タイムアウト（User Idle Timeout）] エリアで [アイドル状態ユーザーのログアウト（Logout idle user）] チェックボックスをオフにし、[保存（Save）] をクリックします。

アイドルタイムアウトの値を変更する必要がある場合は、[アイドル状態ユーザーのログアウト（Logout idle user）] チェックボックスをオンにし、[アイドルユーザーをログアウトするまでの時間（Logout idle user after）] ドロップダウンリストから、アイドルタイムアウト制限を 1 つ選択します。（ただし、この値は [グローバル アイドル タイムアウト（Global Idle Timeout）] に設定されている値を超えることはできません）。

ステップ 5 [保存（Save）] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

デバイスへのユーザーアクセスを制御するための仮想ドメインの作成

仮想ドメインとは

仮想ドメインは、デバイス、サイト、およびその他の NE の論理グループで、それらの NE にアクセスできるユーザーを制御するために使用されます。仮想ドメインに含める要素とその仮想ドメインへのアクセス権を付与するユーザーを選択します。仮想ドメインは、物理サイト、デバイス タイプ、ユーザー コミュニティ、または選択するあらゆる指定項目に基づいて設定できます。すべてのデバイスはROOT-DOMAINに属します。ROOT-DOMAINはすべての新しい仮想ドメインの親ドメインです。

仮想ドメインは、ユーザー グループと連携します。仮想ドメインは、ユーザーがアクセスできるデバイスを制御しますが、ユーザー グループは、ユーザーがそれらのデバイスで実行できるアクションを決定します。仮想ドメインへのアクセス権を持つユーザーは、ユーザーの権限に応じて、デバイスを設定したり、アラームを表示したり、仮想ドメインの NE に関するレポートを生成したりできます。

デバイスを Cisco EPN Manager に追加したら、仮想ドメインを作成できます。各仮想ドメインには名前が必要です。オプションで説明、電子メール アドレス、およびタイム ゾーンを設定できます。Cisco EPN Manager は、指定されたタイム ゾーンと電子メール アドレスを使用して、ドメイン固有のレポートをスケジュールして電子メール送信します。

ユーザーは、一度に 1 つの仮想ドメインで作業します。ユーザーは、[仮想ドメイン（Virtual Domain）] ドロップダウン リストから別の仮想ドメインを選択することによって、現在の仮想ドメインを変更できます（別の仮想ドメインで作業する （32ページ）を参照してください）。

仮想ドメインをセットアップする前に、ネットワークの特定の領域を管理するユーザーを決定します。次に、ニーズに応じて（たとえば、地域ごと、デバイス タイプごと、ネットワークが機能するユーザー コミュニティごと）仮想ドメインを編成します。

仮想ドメインが Cisco EPN Manager 機能に及ぼす影響

仮想ドメインは、階層構造で編成されています。ROOT-DOMAIN ドメインには、すべての仮想ドメインが含まれています。

ネットワーク要素は階層的に管理されるため、デバイス（および一部の関連する機能とコンポーネント）のユーザー ビューがユーザーの仮想ドメインの影響を受けます。次のトピックでは、これらの機能に対する仮想ドメインの影響について説明します。

レポートと仮想ドメイン

レポートには、アクティブ仮想ドメインに属しているコンポーネントのみが含まれています。親仮想ドメインは、その子ドメインからのレポートは表示できません。新しいコンポーネントは、その追加後に生成されたレポートにのみ反映されます。

検索と仮想ドメイン

検索結果には、アクティブ ドメインに属しているコンポーネントのみが含まれます。検索が実行され保存されたドメインと同じドメインに位置している場合にのみ保存した検索結果が表示されます。親ドメインで作業する場合、子ドメインで実行した検索結果は表示されません。

アラームと仮想ドメイン

コンポーネントが仮想ドメインに追加された場合、そのコンポーネントの以前のアラームは、該当する仮想ドメインに表示されません。新しいアラームだけが表示されます。たとえば、ネットワーク要素が Cisco EPN Manager に追加され、追加の前後でそのネットワーク要素がアラームを生成した場合は、追加後に生成されたアラームのみがアラーム履歴に記録されます。

（注） アラーム電子メール通知の場合は、ROOT-DOMAIN 仮想ドメインだけがロケーション通知、ロケーション サーバー、および Cisco EPN Manager 電子メール通知を有効にできます。

マップおよび仮想ドメイン

マップには、アクティブな仮想ドメインのメンバーであるネットワーク要素のみが表示されます。

設定テンプレートと仮想ドメイン

仮想ドメインで作成または検出した設定テンプレートは、その仮想ドメイン内のネットワーク要素にのみ適用できます。テンプレートをデバイスに適用してから、そのデバイスを子ドメインに追加した場合は、その子ドメイン内の同じデバイスでもテンプレートを使用できるようになります。

（注） 子ドメインを作成してから、設定テンプレートを仮想ドメイン内の両方のネットワーク要素に適用した場合は、テンプレートが適用されたパーティションの数が Cisco EPN Manager に正しく反映されない場合があります。

グループおよび仮想ドメインの設定

親ドメインは、子ドメインの設定グループ内のネットワーク要素を表示できます。親ドメインは、子ドメインの設定グループを編集することもできます。

電子メール通知と仮想ドメイン

仮想ドメインごとに電子メール通知を設定できます。

アラーム電子メール通知の場合は、ROOT-DOMAIN だけがロケーション通知、ロケーションサーバー、および電子メール通知を有効にできます。

新しい仮想ドメインの作成

新しい仮想ドメインを作成するには、仮想ドメインの目的の階層に応じて、次のいずれかの手順を実行します。

新しい仮想ドメイン（***new-domain***）の作成場所：	手順の参照先：
ROOT-DOMAIN > ***new-domain***	ROOT-DOMAIN 直下での仮想ドメインの作成 （1033 ページ）
ROOT-DOMAIN > *existing-domain* > ***new-domain***	子仮想ドメイン（サブドメイン）の作成 （1034 ページ）
ROOT-DOMAIN > *existing-domain* > *existing-domain* > ***new-domain***	
（その他）	

ROOT-DOMAIN 直下での仮想ドメインの作成

ROOT-DOMAIN の下に空の仮想ドメインを作成する手順を次に示します。また、複数の仮想ドメインを一括に作成するには、仮想ドメインのリストのインポート（1035ページ）の手順を使用します。

ROOT-DOMAIN の下に仮想ドメインがすでに存在しており、その仮想ドメインの下に新しいドメイン（子ドメイン）を作成するには、子仮想ドメイン（サブドメイン）の作成（1034ページ）を参照してください。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで [+] アイコン（[新規ドメインの追加（Add New Domain）]）をクリックします。

ステップ 3 [名前（Name）] テキスト ボックスに名前を入力します。これは必須です。

ステップ 4 （オプション）新しいドメインのタイム ゾーン、電子メール アドレス、および説明を入力します。

ステップ 5 [送信（Submit）] をクリックして、新しく作成された仮想ドメインの概要を表示します。

次のタスク

仮想ドメインへのネットワーク デバイスの追加 （1036ページ）の説明に従って、仮想ドメインにデバイスを追加します。

子仮想ドメイン（サブドメイン）の作成

次の手順を実行すると、仮想子ドメイン（サブドメインともいう）が作成されます。子仮想ドメインはROOT-DOMAINの直下にあるドメインではなく、ROOT-DOMAIN直下のドメインの下にあるドメインです。

ROOT-DOMAIN の直下に新しい仮想ドメインを表示させるには、この手順を使用しないでください。その場合には、ROOT-DOMAIN直下での仮想ドメインの作成 （1033ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）]** を選択します。

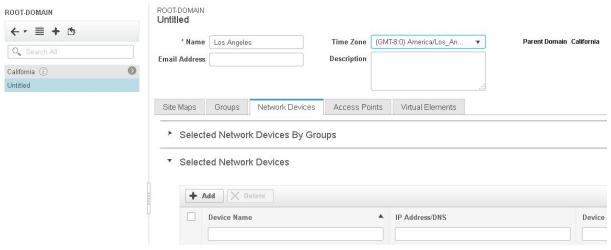
ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、次の手順を実行します。

a) その下に新しい子ドメインを作成するドメインを見つけます。（これは親ドメインと呼ばれます。）この例では、親ドメインは **California** です。

b) ドメイン名の隣にある情報（[i]）アイコンをクリックします。データ ポップアップ ウィンドウが開きます。

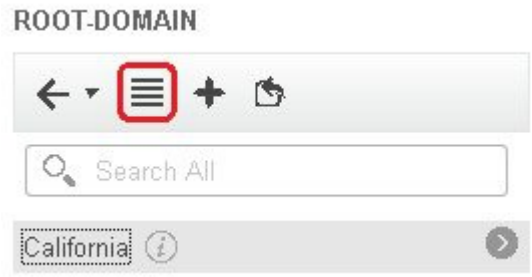
c) ポップアップ ウィンドウで、[サブドメインの作成（Create Sub Domain）] をクリックします。ナビゲーション ペインがリスト ビューに切り替わり、親ドメイン [California] が [無題（Untitled）] の上に表示されます。

ステップ 3 [名前（Name）]テキストボックスに名前を入力します。これは必須です。この例では、新しい子ドメインに **Los Angeles** という名前を付けます。（ナビゲーション ペインに表示される名前は、新しい子ドメインを保存するまでは、[無題（Untitled）] から [Los Angeles] に変更されません。）

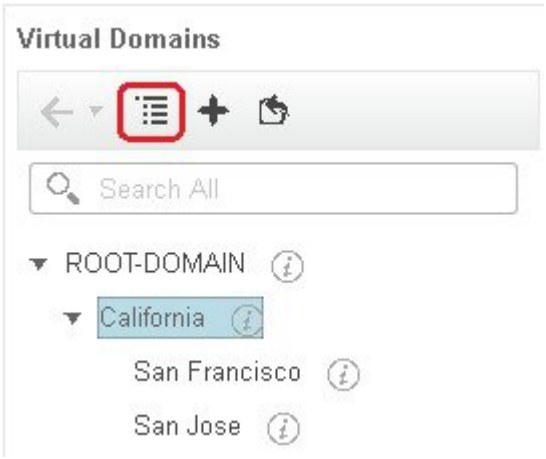


ステップ 4 （オプション）新しいドメインのタイム ゾーン、電子メール アドレス、および説明を入力します。

ステップ 5 [送信（Submit）]をクリックし、新しい子ドメインを作成することを確認します。階層ビューに戻るには、ナビゲーション ペイにの上部にある表示トグル ボタンをクリックします。



表示が階層ビューに戻ります。



次のタスク

仮想ドメインへのネットワーク デバイスの追加（1036ページ）の説明に従って、仮想ドメインにデバイスを追加します。

仮想ドメインのリストのインポート

複数の仮想ドメインを作成する予定の場合、またはドメインを複雑な階層にする場合は、より簡単な方法として、それらを正しくフォーマットされた CSV ファイルで指定して、そのファイルをインポートできます。CSV フォーマットを使用すれば、作成した仮想ドメインだけでなく、その親ドメインの名前、説明、タイム ゾーン、および電子メール アドレスも指定できます。仮想ドメインへのネットワーク要素の追加は、別途行う必要があります。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [ドメインのインポート（Import Domain(s)）] アイコンをクリックし、ポップアップに表示されるリンクからサンプル CSV ファイルをダウンロードして CSV ファイルを用意します。

ステップ 3 [ファイルの選択（Choose File）] をクリックし、CSV ファイルに移動します。

ステップ 4 [インポート（Import）] をクリックして、CSV ファイルをインポートし、指定した仮想ドメインを作成します。

次のタスク

仮想ドメインにデバイスを追加します（仮想ドメインへのネットワーク デバイスの追加 （1036 ページ）を参照）。

仮想ドメインへのネットワーク デバイスの追加

ネットワーク デバイスを仮想ドメインに追加するには、次の手順に従います。新しいネットワーク デバイスを既存の仮想ドメインに追加すると、そのドメインへのアクセス権を持つユーザーに対し、追加されたネットワーク デバイスがただちにアクセス可能になります（Web GUI を再起動する必要はありません）。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、ネットワーク デバイスを追加する仮想ドメインをクリックします。

ステップ 3 [ネットワーク デバイス（Network Devices）] タブをクリックし、[追加（Add）] をクリックします。

ステップ 4 ドメインに追加するネットワーク デバイスを選択します。[ネットワーク デバイスの選択（Select Network Devices）] ダイアログには、親ドメインに含まれるデバイスだけでなく、管理対象デバイスのすべてがリストされることに注意してください。親ドメインに含まれていないデバイスを追加すると、Cisco EPN Manager により、そのデバイスは子ドメインと親ドメインの両方に追加されます。

a) ドメインに追加するデバイスを選択します。[フィルタ条件（Filter By）] ドロップダウン リストを使用して、追加するデバイスを見つけることができます。

b) [選択（Select）] をクリックします。

（注） [すべて選択（Select All）] 機能を使用して、1 つのショットに 500 を超えるネットワークデバイスを追加することはできません。500 を超えるデバイスを追加するには、[フィルタ条件（Filter By）] オプションを複数回使用します。

ステップ 5 [送信（Submit）] をクリックして、仮想ドメインの内容を表示します。

ステップ 6 [保存（Save）] をクリックして変更を確定します。

次のタスク

ユーザーへの仮想ドメインの割り当て （1037 ページ）で説明されている手順に従って、仮想ドメインへのアクセス権をユーザーに付与します。

ユーザーへの仮想ドメインの割り当て

仮想ドメインをユーザーアカウントに割り当てると、そのユーザーが表示して操作を実行できるデバイスは、ユーザーに割り当てられたドメイン内のデバイスに制限されます。

（注） 外部 AAA を使用しているときは、外部 AAA サーバーの該当するユーザーまたはグループ設定に仮想ドメインのカスタム属性を追加してください。RADIUS と TACACS+ で Cisco EPN Manager 仮想ドメインを使用する （1038 ページ）を参照してください。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** > **[ユーザー（Users）]** の順に選択します。

ステップ 2 デバイス アクセス権を付与するユーザーを選択します。

ステップ 3 [仮想ドメイン（Virtual Domains）] タブをクリックします。

ステップ 4 [追加（Add）] ボタンと [削除（Remove）] ボタンを使用して割り当てを変更してから、[保存（Save）] をクリックします。

仮想ドメインの編集

仮想ドメインを調節するには、左側のサイドバー メニューの [仮想ドメイン階層（Virtual Domain Hierarchy）] から仮想ドメインを選択し、このドメインに割り当てられているネットワーク デバイスを表示または編集します。ROOT-DOMAIN の設定はすべて編集できません。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、編集する仮想ドメインをクリックします。

ステップ 3 名前、電子メール アドレス、タイム ゾーン、説明を調整するには、テキスト ボックスに変更内容を入力します。

ステップ 4 デバイス メンバーを調整するには、次の手順を実行します。

- デバイスを追加するには、[追加（Add）] をクリックし、仮想ドメインへのネットワーク デバイスの追加 （1036 ページ）の手順に従います。
- デバイスを削除するには、デバイスのチェックボックスを使用してデバイスを選択し、[削除（Delete）] をクリックします。

ステップ 5 [送信（Submit）] をクリックし、変更内容のサマリーを確認します。

ステップ 6 [保存（Save）] をクリックして編集内容を適用、保存します。

仮想ドメインの削除

仮想ドメインを Cisco EPN Manager から削除するには、以下の手順に従います。この手順では、仮想ドメインだけが削除され、ネットワーク要素は Cisco EPN Manager から削除されません（ネットワーク要素は引き続き Cisco EPN Manager で管理されます）。

始める前に

仮想ドメインを削除できるのは、以下の場合に限られます。

- 仮想ドメインにネットワーク要素も子ドメインも一切含まれていない場合。
- ユーザーがアクセスできる唯一のドメインではない場合。つまり、Cisco EPN Manager ユーザーがそのドメインにしかアクセスできない場合、ドメインを削除することはできません。
- ドメインにログインしているユーザーがいない場合。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、仮想ドメイン名の横にある情報（[i]）アイコンをクリックします。これにより、データ ポップアップ ウィンドウが開きます。

ステップ 3 ポップアップ ウィンドウで [削除（Delete）] をクリックします。

ステップ 4 [OK] をクリックして、仮想ドメインの削除を確認します。

RADIUS と TACACS+ で Cisco EPN Manager 仮想ドメインを使用する

RADIUS または TACACS+ サーバーは、Cisco EPN Manager 内に存在する仮想ドメインを認識するように設定する必要があります。これを実行するは、「RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （1038 ページ）」の手順を使用します。

RADIUS または TACACS+ サーバーにユーザー向けの仮想ドメイン情報が保存されていない場合は、Cisco EPN Manager で設定された仮想ドメインの数に応じて、以下が発生します。

- Cisco EPN Manager に 1 つの仮想ドメイン（ROOT-DOMAIN）しか割り当てられていない場合は、デフォルトで ROOT-DOMAIN がユーザーに割り当てられます。
- Cisco EPN Manager に複数の仮想ドメインが割り当てられている場合は、ユーザーがログインできなくなります。

RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート

RADIUS または TACACS+ を使用する場合は、Cisco EPN Manager 仮想ドメイン情報をすべて Cisco ACS または Cisco ISE サーバーにコピーする必要があります。Cisco EPN Manager Web GUI に表示される [仮想ドメイン カスタム属性（Virtual Domains Custom Attributes）] ダイアログボッ

クスを使用して、この操作を実行できます。Cisco ACS または Cisco ISE サーバーにデータをエクスポートしない場合、Cisco EPN Manager ではユーザーがログインできなくなります。

使用するプロトコルに応じて、次の情報をエクスポートする必要があります。

- TACACS+：仮想ドメイン、権限、およびタスク情報が必要です。
- RADIUS：仮想ドメインとロールの情報が必要です（タスクは自動的に追加されます）。

既存の仮想ドメインの子ドメインを作成すると、親仮想ドメインで RADIUS/TACACS+ カスタム属性のシーケンス番号も更新されます。これらのシーケンス番号は表示専用で、AAA 統合には影響しません。

[仮想ドメイン カスタム属性（Virtual Domains Custom Attributes）] ダイアログボックスの情報は、Cisco ACS サーバーで使用できるように事前にフォーマットされています。

（注） 外部サーバーにタスクを追加するときには、[ホーム メニュー アクセス（Home Menu Access）] タスクを必ず追加してください。これはすべてのユーザーで必須です。

始める前に

外部認証の設定 （1041 ページ）の説明に従い、AAA サーバーを追加し、AAA モードを設定していることを確認してください。

ステップ 1 Cisco EPN Manager で、次の手順を実行します。

a) **[管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

b) ウィンドウ右上の [カスタム属性のエクスポート（Export Custom Attributes）] をクリックします。これにより、[仮想ドメイン カスタム属性（Virtual Domains Custom Attributes）] ダイアログが表示されます。

c) 属性リストをコピーします。

- RADIUS を使用する場合は、[RADIUS カスタム属性（RADIUS Custom Attributes）] フィールドのすべてのテキストを選択して右クリックし、[コピー（Copy）] を選択します。
- TACACS+ を使用する場合は、[TACACS+カスタム属性（TACACS+ Custom Attributes）] フィールドのすべてのテキストを選択して右クリックし、[コピー（Copy）] を選択します。

ステップ 2 Cisco ACS または Cisco ISE サーバーに情報を貼り付けます。次の手順は、Cisco ACS の既存のユーザー グループに情報を追加する方法を示しています。この情報をまだ Cisco ACS または Cisco ISE に追加していない場合は、次を参照してください。

- Cisco ACS と RADIUS または TACACS+ による外部認証 （1049 ページ）
- Cisco ISE と RADIUS または TACACS+ による外部認証 （1043 ページ）

a) [ユーザー設定（User Setup）] または [グループ設定（Group Setup）] に移動します。

ユーザーベースで仮想ドメインを指定する場合、すべてのカスタム属性情報（たとえば、タスク、ロール、仮想ドメインなど）を [ユーザー（User）] カスタム属性ページに追加していることを確認する必要があります。

a) 該当するユーザーまたはグループの [設定の編集（Edit Settings）] をクリックします。
b) 該当するテキスト ボックスに属性一覧を貼り付けます。
c) これらの属性を有効にするチェックボックスをオンにしてから、[送信して再起動（Submit + Restart）] をクリックします。

ローカル認証の設定

Cisco EPN Manager はデフォルトでローカル認証を使用します。つまり、ユーザー パスワードが Cisco EPN Manager データベースに保管されて、データベース内のパスワードが検証されます。使用中の認証モードを確認するには、**[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、**[AAA モードの設定（AAA Mode Settings）]** を選択します。これにより、[AAA モードの設定（AAA Mode Settings）] ページが表示されます。ローカル認証を使用する場合、必ず強力なパスワードポリシーを設定する必要があります。ローカル認証のためのグローバルパスワードポリシーの設定 （1027 ページ）を参照してください。

ローカル認証で SSO を使用するには、ローカル認証での SSO の使用 （1040 ページ）を参照してください。

外部認証については、「外部認証の設定 （1041 ページ）」を参照してください。

ローカル認証での SSO の使用

ローカル認証で SSO を使用するには、SSO サーバーを追加し、ローカル モードで SSO を使用するように Cisco EPN Manager を設定する必要があります。

プライマリ サーバーとバックアップ サーバーが存在するハイ アベイラビリティ環境で Cisco EPN Manager を導入した場合、HA 環境での SSO サーバーの設定 （1123 ページ）の手順を参照してください。

Cisco EPN Manager は、SSO サインイン ページでのローカライズをサポートしていません。

以下のトピックでは、外部認証用に SSO を設定する方法について説明していますが、同じ手順を使用して、ローカル認証用に SSO を設定することもできます。唯一の違いは、Cisco EPN Manager サーバーで SSO モードを設定するときに、[ローカル（Local）] モード（RADIUS や TACACS+ ではない）を選択することです。

-
- SSO サーバーの追加 （1056 ページ）
- Cisco EPN Manager サーバー上で SSO モードを設定する （1057 ページ）

外部認証の設定

Web GUI のルートユーザーまたはスーパーユーザー権限を持つユーザーは、外部認証、認可、およびアカウンティング（AAA）のために外部 LDAP、RADIUS、TACACS+、SSO サーバーと通信するように Cisco EPN Manager を設定できます。外部認証を設定することを選択した場合、ユーザー グループ、ユーザー、認証プロファイル、認証ポリシー、およびポリシー ルールが、Cisco EPN Manager へのすべてのアクセス要求がルーティングされる外部サーバーで作成済みである必要があります。

最大 3 つの AAA サーバーを使用できます。ユーザーは、最初のサーバーが到達不能であるかネットワークに問題がある場合にのみ、2 番目のサーバーで認証されます。

（注） 同じ RADIUS、TACACS+、または LDAP プロトコルをサポートしている場合にのみ、最大 3 つの AAA サーバーを一緒に使用できます。プロトコルが異なるサーバーどうしを一緒に使用することは、サポートされていません。ただし、異なるプロトコルを実行している複数の AAA サーバーを使用する場合は、Cisco ISE または ACS を EPNM と AAA サーバー間のプロキシとして使用する必要があります。この場合、Cisco ISE または Cisco ACS の設定に基づいて認証ロジックを設定する必要があります。

CLI から外部認証を設定するには、CLI を使用した外部認証の設定 （915 ページ）を参照してください。

詳細については、次のトピックを参照してください。

- Cisco ISE と RADIUS または TACACS+ による外部認証
- Cisco ISE と RADIUS または TACACS+ による外部認証 （1043 ページ）
- Cisco ACS と RADIUS または TACACS+ による外部認証 （1049 ページ）
- SSO による外部認証 （1056 ページ）

外部認証での RADIUS または TACACS+ の使用

以下のトピックでは、RADIUS または TACACS+ サーバーを使用するように Cisco EPN Manager を設定する方法について説明します。

- Cisco EPN Manager への RADIUS または TACACS+ サーバーの追加 （1041 ページ）
- Cisco EPN Manager サーバー上で RADIUS または TACACS+ モードを設定する （1042 ページ）

Cisco EPN Manager への RADIUS または TACACS+ サーバーの追加

RADIUS または TACACS+ サーバーを Cisco EPN Manager に追加するには、次の手順に従います。

ステップ 1 **[管理（Administration）]**>**[ユーザー（Users）]**>**[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[RADIUS サーバー（RADIUS Servers）] を選択します。

ステップ 2 追加するサーバーのタイプを選択します。

- RADIUS の場合は、[RADIUS サーバー（RADIUS Servers）] を選択します。[コマンドの選択（Select a command）] ドロップダウン リストから、[RADIUS サーバーの追加（Add RADIUS Server）] を選択し、[実行（Go）] をクリックします。
- TACACS+ の場合は、[TACACS+ サーバー（TACACS+ Servers）] を選択します。[コマンドの選択（Select a command）] ドロップダウン リストから、[TACACS+ サーバーの追加（Add TACACS+ Server）] を選択し、[実行（Go）] をクリックします。

（注） [上へ移動（Move Up）] および [下へ移動（Move Down）] 矢印を使用して、使用可能な IP アドレスの順序を並べ替えることができます。

ステップ 3 必要な情報（IP アドレス、DNS 名など）を入力します。Cisco EPN Manager が外部認証サーバーと通信するためには、このページで入力する共有秘密が RADIUS また TACACS+ サーバーに設定された共有秘密と一致している必要があります。サードパーティ製の TACACS+ または RADIUS サーバー用の共有秘密キーを入力するときに、'（一重引用符）と "（二重引用符）を除く、アルファベット、数字、および特殊文字を使用できます。再送信タイムアウトと再試行の回数を入力します。

ステップ 4 認証タイプを選択します。

- PAP：パスワード ベースの認証は、2 つのエンティティが 1 つのパスワードを事前に共有し、そのパスワードを認証の基準に使用するプロトコルです。
- CHAP：チャレンジ ハンドシェイク認証プロトコルでは、クライアントとサーバーの両方がプレーンテキストの秘密キーを認識しており、その秘密キーは絶対にネットワーク上に送信されないことが必要になります。CHAP は、パスワード認証プロトコル（PAP）より優れたセキュリティを提供します。

ステップ 5 高可用性機能を有効にして、**[ローカルインターフェイス IP（Local Interface IP）]** に仮想 IP アドレスを設定した場合、**eth0** の仮想 IP アドレスを選択します。（セカンダリ サーバーでの高可用性の設定とインストールについては、『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください）。

（注） 外部認証サーバーに設定された IP アドレスは、[ローカル インターフェイス IP（Local Interface IP）] の値と一致していなければなりません。

ステップ 6 [保存（Save）] をクリックします。

Cisco EPN Manager サーバー上で RADIUS または TACACS+ モードを設定する

ステップ 1 **[管理（Administration）]**>**[ユーザー（Users）]**>**[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[AAA モード（AAA Mode）] を選択します。

ステップ 2 [TACACS+] または [RADIUS] を選択します。

ステップ 3 [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] チェックボックスをオンにすると、外部 AAA サーバーがダウンした場合にローカル データベースの使用が有効になります。

ステップ 4 外部 RADIUS または TACACS+ サーバーがダウンした場合にローカル認証に戻すには、次の手順を実行します。

a) [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] を選択します。

b) フォールバック条件（[サーバーが応答しないときのみ（ONLY on no server response）] または [認証に失敗したかサーバーが応答しないとき（on authentication failure or no server response）]）を指定します。

ステップ 5 シングルサインアウトを有効にする場合は、[シングルサインアウトの有効化（Enable Single Sign-Out）] チェックボックスをオンにします。

ステップ 6 ドロップダウンリストから [チケット認可チケットタイムアウト（Ticket Granting Ticket Timeout）] を選択します。

ステップ 7 [保存（Save）] をクリックします。

Cisco ISE と RADIUS または TACACS+ による外部認証

Cisco Identity Services Engine（ISE）は、認証、認可、およびアカウンティング（AAA）に RADIUS または TACACS+ プロトコルを使用します。Cisco ISE に Cisco EPN Manager を統合し、RADIUS または TACACS+ プロトコルを使用して Cisco EPN Manager ユーザーを認証できます。外部認証を使用する場合は、ユーザー、ユーザー グループ、パスワード、認証プロファイル、認証ポリシー、ポリシー規則などの AAA に必要な詳細を Cisco ISE データベースから保存および確認する必要があります。

（注） Cisco EPN Manager は LDAP をネイティブにサポートしています。

Cisco ISE で外部認証に RADIUS または TACACS+ プロトコルを使用するには、次のタスクを実行します。

外部認証に Cisco ISE を使用するために実行するタスク	詳細については、次を参照してください。
Cisco ISE のサポートされるバージョンを使用していることを確認します。	Cisco EPN Manager でサポートされる Cisco ISE のバージョン（1044 ページ）
Cisco ISE で Cisco EPN Manager を AAA クライアントとして追加します。	Cisco ISE にクライアントとして Cisco EPN Manager を追加する （1044 ページ）
Cisco ISE でユーザー グループを作成します。	Cisco ISE でのユーザー グループの作成 （1045 ページ）

Cisco ISE でユーザーを作成し、そのユーザーを Cisco ISE で作成したユーザー グループに追加します。	Cisco ISE でのユーザーの作成およびユーザー グループへのユーザーの追加（1045ページ）
（RADIUS を使用する場合）Cisco ISE でネットワーク アクセスの認証プロファイルを作成し、Cisco EPN Manager で作成したユーザー ロールと仮想ドメインを使用して RADIUS カスタム属性を追加します。 （注） RADIUS では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。	Cisco ISE での RADIUS の認証プロファイルの作成（1045ページ）
（TACACS+ を使用する場合）Cisco ISE でネットワーク アクセスの認証プロファイルを作成し、で作成したユーザー ロールおよび仮想ドメインを使用した TACACS+ カスタム属性を追加します。 Cisco EPN Manager （注） TACACS+ では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。	Cisco ISE での TACACS+ の認証プロファイルの作成 （1046ページ）
Cisco ISE で認証ポリシーを作成し、Cisco ISE で作成したユーザー グループと認証プロファイルにポリシーを関連付けます	Cisco ISE で の認可ポリシーを設定する （1048 ページ）
認証ポリシーを作成して、Cisco ISE が Cisco EPN Manager と通信するために使用する必要があるプロトコルと Cisco EPN Manager に対してユーザーを認証するために使用するアイデンティティ ソースを定義します。	Cisco ISE での認証ポリシーの作成 （1048 ページ）
Cisco EPN Manager で RADIUS または TACACS+ サーバーとして Cisco ISE を追加します。	
Cisco EPN Manager サーバーで RADIUS または TACACS+ モードを設定します。	Cisco EPN Manager サーバー上で RADIUS または TACACS+ モードを設定する （1042ページ）

Cisco EPN Manager でサポートされる Cisco ISE のバージョン

Cisco EPN Manager は Cisco ISE 1.*x* および 2.*x* リリースをサポートしています。

Cisco ISE にクライアントとして Cisco EPN Manager を追加する

ステップ 1 admin ユーザーとして Cisco ISE にログインします。

ステップ 2 **[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 3 [ネットワーク デバイス（Network Devices）] ページで [追加（Add）] をクリックします。

ステップ 4 Cisco EPN Manager サーバーのデバイス名と IP アドレスを入力します。

ステップ 5 [認証設定（Authentication Settings）] チェックボックスをオンにして、共有秘密を入力します。

（注） この共有秘密は、Cisco EPN Manager で Cisco ISE サーバーを RADIUS サーバーとして追加したときに入力した共有秘密と必ず一致するようにします。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ISE でのユーザー グループの作成

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[管理（Administration）]** > **[ID管理（Identity Management）]** > **[グループ（Groups）]** を選択します。

ステップ 3 [ユーザー アイデンティティ グループ（User Identity Groups）] ページで、[追加（Add）] をクリックします。

ステップ 4 [アイデンティティ グループ（Identity Group）] ページで、ユーザー グループの名前と説明を入力します。

ステップ 5 **[送信（Submit）]** をクリックします。

Cisco ISE でのユーザーの作成およびユーザー グループへのユーザーの追加

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[管理（Administration）]** > **[ID管理（Identity Management）]** > **[ID（Identities）]** を選択します。

ステップ 3 [ネットワーク アクセス ユーザー（Network Access Users）] ページで [追加（Add）] をクリックします。

ステップ 4 [項目の選択（Select an item）] ドロップダウン リストから、ユーザーを割り当てるユーザー グループを選択します。

ステップ 5 **[送信（Submit）]** をクリックします。

Cisco ISE での RADIUS の認証プロファイルの作成

許可プロファイルを作成して、さまざまなタイプのユーザーにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN 接続を介してネットワークへのアクセスを試みるユーザーには、有線接続を介してネットワークへのアクセスを試みるユーザーよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、Cisco EPN Manager 内に作成したユーザー ロール、タスク、仮想ドメインに関連付けられている RADIUS カスタム属性を追加する必要があります。

（注） RADIUS の場合、タスクの属性を追加せずにユーザー ロールの属性を追加できます。タスクはユーザー ロールによって自動的に追加されます。

Cisco ISE の認証プロファイルの詳細については、『Cisco Identity Services Engine Administrator Guide』の認証ポリシーとプロファイルの管理に関する情報を参照してください。

Cisco ISE で RADIUS の認証プロファイルを作成するには、次の手順を実行します。

始める前に

次に示す RADIUS のすべての Cisco EPN Manager カスタム属性のリストがあることを確認します。次の手順では、この情報を Cisco ISE に追加する必要があります。

- Cisco EPN Manager ユーザー ロールとタスク：を参照してください。RADIUS および TACACS+ の Cisco EPN Manager ユーザー グループとロール属性のエクスポート （1020 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （1038 ページ）を参照してください。

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）]** を選択します。

ステップ 3 左側のサイドバーのメニューから **[認証（Authorization）] > [認証プロファイル（Authorization Profiles）]** の順に選択します。

ステップ 4 [標準認証プロファイル（Standard Authorization Profiles）] ページで、[追加（Add）] をクリックします。

ステップ 5 [認証プロファイル（Authorization Profile）] ページで、認証プロファイルの名前と説明を入力します。

ステップ 6 [アクセス タイプ（Access Type）] ドロップダウンリストから、[ACCESS_ACCEPT] を選択します。

ステップ 7 [詳細な属性設定（Advanced Attributes Settings）] エリアで、次のアイテムのずべての RADIUS カスタム属性のリストを貼り付けます。

- ユーザー ロール
- 仮想ドメイン

（注） ユーザー タスクを追加する場合は、必ずホーム メニュー アクセス タスクを追加してください。これは必須です。

ステップ 8 **[送信（Submit）]** をクリックします。

Cisco ISE での TACACS+ の認証プロファイルの作成

権限プロファイルを作成して、さまざまなタイプのユーザーにネットワークへのアクセスを認可する方法を定義できます。たとえば、VPN接続を介してネットワークへのアクセスを試みる

ユーザーには、有線接続を介してネットワークへのアクセスを試みるユーザーよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、Cisco EPN Manager 内に作成したユーザー ロール、タスク、仮想ドメインに関連付けられている TACACS+ カスタム属性を追加する必要があります。

Cisco ISE 認証プロファイルの詳細については、『Cisco Identity Services Engine Administrator Guide』の認証ポリシーおよび認証プロファイルの管理に関する情報を参照してください。

Cisco ISE で TACACS+ 用の認証プロファイルを作成するには、次の手順に従います。

始める前に

次に示す TACACS+ のすべての Cisco EPN Manager カスタム属性のリストがあることを確認します。次の手順では、この情報を Cisco ISE に追加する必要があります。

- Cisco EPN Manager ユーザー ロールとタスク：を参照してください。RADIUS および TACACS+ の Cisco EPN Manager ユーザー グループとロール属性のエクスポート （1020 ページ）
- Cisco EPN Manager 仮想ドメイン。参照先：RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （1038 ページ）

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[ワークセンター（Work Center）]** > **[デバイス管理（Device Administration）]** > **[ポリシー要素（Policy Elements）]** を選択します。

ステップ 3 左側のサイドバーから、**[結果（Results）]** > **[TACACS プロファイル（TACACS Profiles）]** を選択します。

ステップ 4 [TACACS プロファイル（TACACS Profiles）] ページで、[追加（Add）] をクリックします。

ステップ 5 [アクセス タイプ（Access Type）] ドロップダウンリストから、[ACCESS_ACCEPT] を選択します。

ステップ 6 [TACACS プロファイル（TACACS Profiles）] ページで、認証プロファイルの名前と説明を入力します。

ステップ 7 [プロファイル属性の raw ビュー（Raw View Profile Attributes）] 領域に、次についての TACACS+ のカスタム属性の完全なリストを貼り付けます。

- タスクを含むユーザー ロール
- 仮想ドメイン

（注） [ホーム メニュー アクセス（Home Menu Access）] タスクを必ず追加してください。これは必須です。

ステップ 8 **[送信（Submit）]** をクリックします。

Cisco ISE での認可ポリシーを設定する

認可ポリシーは、認可プロファイルで定義された特定の権限のセットを形成する、ユーザー定義のルールまたはルールのセットで構成されます。認可プロファイルに基づいて、Cisco EPN Manager へのアクセス要求が処理されます。

設定可能な認可ポリシーには、次の 2 つのタイプがあります。

- 標準：標準ポリシーは、安定化を目的としており、長期間にわたって効果を発揮し、より大きなユーザーのグループ、デバイス、または権限の共通セットを共有するグループに適用するために作成します。
- 例外：例外ポリシーは、限定数のユーザー、デバイス、またはグループにネットワーク リソースへのアクセスを許可するなどの、即時または短期間のニーズを満たすために作成します。例外ポリシーを使用すると、1 人のユーザーまたはユーザーのサブセットに合わせて調整された、ID グループ、条件、または権限に対する、カスタマイズされた値の特定のセットを作成できます。

認可ポリシーの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Manage Authorization Policies and Profiles」の章を参照してください。

Cisco ISE で認可ポリシーを作成するには、次の手順を実行します。

ステップ 1 管理者ユーザーとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）] > [許可（Authorization）]** を選択します。

ステップ 3 [標準（Standard）] 領域で、右端にある下矢印をクリックし、[新規ルールを上に挿入（Insert New Rule Above）] または [新規ルールを下に挿入（Insert New Rule Below）] のどちらかを選択します。

ステップ 4 ルール名を入力して、認可ポリシーの ID グループ、条件、属性、および権限を選択します。

たとえば、ユーザーグループを Cisco EPN Manager-System Monitoring-Group として定義して、そのグループを [アイデンティティグループ（Identity Groups）] ドロップダウンリストから選択することができます。同様に、認証プロファイルを Cisco EPN Manager-System Monitoring-authorization プロファイルとして定義し、[権限（Permissions）] ドロップダウンリストからこのプロファイルを選択します。これで、Cisco EPN Manager システム モニターリング アイデンティティ グループに属しているすべてのユーザーに、システム モニターリングのカスタム属性が定義された適切な認証ポリシーが適用されます。

ステップ 5 [完了（Done）] をクリックしてから、[保存（Save）] をクリックします。

Cisco ISE での認証ポリシーの作成

認証ポリシーは、Cisco ISE が Cisco EPN Manager と通信するために使用するプロトコルを定義します。また、Cisco EPN Manager に対するユーザーの認証に使用するアイデンティティ ソースを特定します。アイデンティティ ソースは、ユーザー情報が格納されている内部または外部データベースです。

Cisco ISE で作成できる認証ポリシーには、次の 2 つのタイプがあります。

- シンプルな認証ポリシー：このタイプのポリシーでは、ユーザーの認証に使用できるプロトコルとアイデンティティ ソースを選択できます。
- ルールベースの認証ポリシー：このタイプのポリシーでは、許可するプロトコルとアイデンティティ ソースを Cisco ISE に動的に選択させるための条件を定義できます。

認証ポリシーの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Manage Authentication Policies」の章を参照してください。

Cisco ISE で認証ポリシーを作成するには、次の手順に従います。

ステップ 1 上級管理ユーザーまたはシステム管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）] > [認証（Authentication）]** の順に選択します。

ステップ 3 必要な認証ポリシーを作成するために、[ポリシー タイプ（Policy Type）] として [シンプル（Simple）] または [ルールベース（Rule-Based）] を選択します。

ステップ 4 選択したポリシー タイプに基づいて、必要な情報を入力します。

ステップ 5 [保存（Save）] をクリックします。

Cisco ACS と RADIUS または TACACS+ による外部認証

Cisco Secure Access Control System（ACS）は販売されなくなりました。詳細については、「Cisco Secure Access Control System の販売終了およびライフサイクル終了のお知らせ」を参照してください。Cisco Evolved Programmable Network Manager と Cisco ACS との統合については、今後新たな開発は予定されていません。ACS との統合のサポート終了日は、2020 年 8 月 31 日に予定されており、同日に ACS 製品が廃止される予定です。

Cisco Secure Access Control System（ACS）は、認証、認可、およびアカウンティング（AAA）に RADIUS および TACACS+ プロトコルを使用します。Cisco ACS に Cisco EPN Manager を統合し、RADIUS または TACACS+ プロトコルを使用して Cisco EPN Manager ユーザーを認証できます。外部認証を使用する場合は、ユーザー、ユーザー ロール、パスワード、認証プロファイル、認証ポリシー、ポリシー規則などの AAA に必要な詳細を Cisco ACS データベースから保存および確認する必要があります。

Cisco ACS で外部認証に RADIUS または TACACS+ プロトコルを使用するには、次のタスクを実行します。

外部認証に Cisco ACS を使用するために実行するタスク	詳細については、次を参照してください。
Cisco ACS のサポートされるバージョンを使用していることを確認します。	Cisco EPN Manager でサポートされる Cisco ACS のバージョン （1051 ページ）

Cisco ACS で Cisco EPN Manager を AAA クライアントとして追加します。	Cisco ACS にクライアントとして Cisco EPN Manager を追加する （1051 ページ）
Cisco ACS でユーザー グループを作成します。	Cisco ACS でのユーザー グループの作成 （1051 ページ）
Cisco ACS でユーザーを作成し、そのユーザーを Cisco ACS のユーザー グループに追加します。	Cisco ACS でのユーザーの作成とユーザー グループへのユーザーの追加 （1051 ページ）
（RADIUS を使用する場合）Cisco ACS でネットワーク アクセスの認証プロファイルを作成し、Cisco EPN Manager で作成したユーザー ロールと仮想ドメインの RADIUS カスタム属性を追加します。 （注） RADIUS では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。	Cisco ACS での RADIUS 用の認証プロファイルの作成 （1052 ページ）
（TACACS+ を使用する場合）Cisco ACS でデバイス管理の認証プロファイルを作成し、Cisco EPN Manager で作成したユーザー ロールおよび仮想ドメインを使用した TACACS+ カスタム属性を追加します。 （注） TACACS+ では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。	Cisco ACS での TACACS+ の認証プロファイルの作成 （1053 ページ）
Cisco ACS でアクセス サービスを作成し、アクセス サービスのポリシー構造を定義します。	Cisco ACS での Cisco EPN Manager 用アクセス サービスの作成 （1054 ページ）
Cisco ACS で認証ポリシー規則を作成し、アクセス タイプ（ネットワーク アクセスまたはデバイス管理）に基づいて認証またはシェル プロファイルをマッピングします。	Cisco ACS での認証ポリシー ルールの作成 （1054 ページ）
Cisco ACS でサービス選択ポリシーを設定し、着信要求にアクセス サービスを割り当てます。	Cisco ACS でのサービス セレクション ポリシーの設定 （1055 ページ）
Cisco EPN Manager で RADIUS または TACACS+ サーバーとして Cisco ACS を追加します。	Cisco EPN Manager への RADIUS または TACACS+ サーバーの追加 （1041 ページ）
Cisco EPN Manager サーバーで RADIUS または TACACS+ モードを設定します。	Cisco EPN Manager サーバー上で RADIUS または TACACS+ モードを設定する （1042 ページ）

Cisco EPN Manager でサポートされる Cisco ACS のバージョン

Cisco EPN Manager は Cisco ACS 5.*x* リリースをサポートしています。

Cisco ACS にクライアントとして Cisco EPN Manager を追加する

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** > **[ネットワーク デバイスおよび AAA クライアント（Network Devices and AAA Clients）]** の順に選択します。

ステップ 3 [ネットワーク デバイス（Network Devices）] ページで [作成（Create）] をクリックします。

ステップ 4 Cisco EPN Manager サーバーのデバイス名と IP アドレスを入力します。

ステップ 5 認証オプションで [RADIUS] または [TACACS+] を選択し、共有秘密を入力します。

（注） この共有秘密は、Cisco EPN Manager で Cisco ACS サーバーを RADIUS または TACACS+ サーバーとして追加したときに入力した共有秘密と必ず一致するようにします。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS でのユーザー グループの作成

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ユーザーと ID ストア（Users and Identity Stores）]** > **[アイデンティティ グループ（Identity Groups）]** の順に選択します。

ステップ 3 [アイデンティティグループ（Identity Groups）] ページで [作成（Create）] をクリックします。

ステップ 4 グループの名前と説明を入力します。

ステップ 5 ユーザー グループの親ネットワーク デバイス グループを選択します。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS でのユーザーの作成とユーザー グループへのユーザーの追加

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ユーザーとIDストア（Users and Identity Stores）]** > **[内部IDストア（Internal Identity Stores）]** > **[ユーザー（Users）]** の順に選択します。

ステップ 3 [内部ユーザー（Internal Users）] ページで [作成（Create）] をクリックします。

ステップ 4 次の必須詳細情報を入力します。

ステップ 5 [アイデンティティ グループ（Identity Group）] フィールドで [選択（Select）] を選択して、ユーザーを割り当てるユーザー グループを選択します。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS での RADIUS 用の認証プロファイルの作成

許可プロファイルを作成して、さまざまなタイプのユーザーにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN 接続を介してネットワークへのアクセスを試みるユーザーには、有線接続を介してネットワークへのアクセスを試みるユーザーよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、Cisco EPN Manager 内に作成したユーザー ロール、タスク、仮想ドメインに関連付けられている RADIUS カスタム属性を追加する必要があります。

（注） RADIUS の場合、タスクの属性を追加せずにユーザー ロールの属性を追加できます。タスクはユーザー ロールによって自動的に追加されます。

Cisco ACS 認証プロファイルおよびポリシーの詳細については、『User Guide for Cisco Secure Access Control System』のポリシー要素およびアクセス ポリシーの管理に関する章を参照してください。

Cisco ACS で RADIUS 用の認証プロファイルを作成するには、次の手順に従います。

始める前に

RADIUS 用の次の Cisco EPN Manager カスタム属性を完全に網羅したリストを用意しておきます。次の手順では、この情報を Cisco ACS に追加する必要があります。

- Cisco EPN Manager ユーザー ロールとタスク：を参照してください。RADIUS および TACACS+ の Cisco EPN Manager ユーザー グループとロール属性のエクスポート （1020 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （1038 ページ）を参照してください。

ステップ 1 管理ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ポリシー要素（Policy Elements）]** > **[認証と許可（Authorizations and Permissions）]** > **[ネットワーク アクセス（Network Access）]** > **[認証プロファイル（Authorization Profiles）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 [一般（General）] タブで、認証プロファイルの名前と説明を入力します。

ステップ 5 [RADIUS 属性（RADIUS Attributes）] タブをクリックし、以下についての RADIUS カスタム属性の完全なリストを貼り付けます。

- ユーザー ロール

- 仮想ドメイン

（注） ユーザー タスクを追加する場合は、必ずホーム メニュー アクセス タスクを追加してください。これは必須です。

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS での TACACS+ の認証プロファイルの作成

デバイス管理用の認証プロファイルを作成するには、Cisco EPN Manager で作成されたユーザー ロールおよび仮想ドメインに関連付けられている TACACS+ カスタム属性を追加する必要があります。

（注） TACACS+では、ユーザータスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。

Cisco ACS 認証プロファイルとポリシーの詳細については、『User Guide for Cisco Secure Access Control System』のポリシー要素とアクセス ポリシーの管理に関する章を参照してください。

Cisco ACS で TACACS+ の認証プロファイルを作成するには、次の手順を実行します。

始める前に

次に示すすべての Cisco EPN Manager カスタム属性のリストがあることを確認します。次の手順では、この情報を Cisco ACS に追加する必要があります。

- Cisco EPN Manager ユーザー ロールとタスク：を参照してください。RADIUS および TACACS+ の Cisco EPN Manager ユーザー グループとロール属性のエクスポート （1020 ページ）
- Cisco EPN Manager 仮想ドメイン：RADIUS および TACACS+ の Cisco EPN Manager 仮想ドメイン属性のエクスポート （1038 ページ）を参照してください。

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ポリシー要素（Policy Elements）]** > **[認証と許可（Authorizations and Permissions）]** > **[デバイス管理（Device Administration）]** > **[シェル プロファイル（Shell Profiles）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 [一般（General）] タブで、認証プロファイルの名前と説明を入力します。

ステップ 5 [カスタム属性（Custom Attributes）] タブをクリックし、次のアイテムのずべての TACACS+ カスタム属性のリストを貼り付けます。

- タスクを含むユーザー ロール
- 仮想ドメイン

ステップ 6 **[送信（Submit）]** をクリックします。

Cisco ACS での Cisco EPN Manager 用アクセス サービスの作成

アクセス サービスには、アクセス要求の認証および認可ポリシーが含まれています。使用事例（デバイス管理（TACACS+）やネットワーク アクセス（RADIUS）など）ごとに異なるアクセス サービスを作成できます。

Cisco ACS でアクセス サービスを作成するときに、サービスに含まれるポリシーのタイプとポリシー構造を定義します。たとえば、デバイス管理やネットワーク アクセス用のポリシーがあります。

（注） サービス選択ルールを定義する前に、アクセス サービスを作成する必要がありますが、サービスにポリシーを定義する必要はありません。

Cisco EPN Manager の要求用にアクセス サービスを作成するには、次の手順を実行します。

ステップ 1 管理ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセス ポリシー（Access Policies）]** > **[アクセス サービス（ Access Services）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 アクセス サービスの名前と説明を入力します。

ステップ 5 アクセス サービスのポリシー構造を定義するために、次のいずれかのオプションを選択します。

- [サービス テンプレート ベース（Based on service template）]：定義済みテンプレートに基づいたポリシーを含むアクセス サービスを作成します。
- [既存のサービス ベース（Based on existing service）]：既存のアクセス サービスに基づいたポリシーを含むアクセス サービスを作成します。ただし、新しいアクセス サービスには既存のサービスのポリシー ルールは含まれません。
- [ユーザー選択のサービス タイプ（User selected service type）]：ユーザーがアクセス サービスのタイプを選択できます。選択可能なオプションには、ネットワーク アクセス（RADIUS）、デバイス管理（TACACS+）、外部プロキシ（外部 RADIUS または TACACS+ サーバー）があります。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 サービス アクセスに使用できる認証プロトコルを選択します。

ステップ 8 [終了（Finish）] をクリックします。

Cisco ACS での認証ポリシー ルールの作成

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセスポリシー（Access Policies）]** > **[アクセスサービス（Access Services）]** > **[サービス（service）]** > **[認証（Authorization）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 ルール名を入力し、ルール ステータスを選択します。

ステップ 5 ルールの必須条件を設定します。

たとえば、ロケーション、デバイス タイプ、または作成したユーザー グループに基づいてルールを作成できます。

ステップ 6 ネットワーク アクセス（RADIUS）の認証ポリシー ルールを作成する場合は、認証ポリシー ルールにマッピングする必須認証プロファイルを選択します。

あるいは、デバイス管理（TACACS+）の認証ポリシー ルールを作成する場合は、認証ポリシー ルールにマッピングする必須シェル プロファイルを選択します。

（注） 複数の認証プロファイルまたはシェル プロファイルを使用する場合は、優先順位の高い順に並べる必要があります。

ステップ 7 [OK] をクリックします。

Cisco ACS でのサービス セレクション ポリシーの設定

サービス セレクション ポリシーでは、着信要求に適用するアクセス サービスを決定します。たとえば、TACACS+プロトコルを使用するアクセス要求にデバイス管理アクセス サービスを適用するサービス セレクション ポリシーを設定できます。

次の 2 種類のサービス セレクション ポリシーを設定できます。

- 単純なサービス セレクション ポリシー：すべての要求に同じアクセス サービスを適用します。
- ルール ベースのサービス セレクション ポリシー：1 つ以上の条件とその結果（着信要求に適用されるアクセス サービス）が設定されています。

サービス セレクション ポリシーを設定するには、次の手順を実行します。

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセス ポリシー（Access Policies）]** > **[アクセス サービス（Access Services）]** > **[サービス セレクション ルール（Service Selection Rules）]** の順に選択します。

ステップ 3 単純なサービス セレクション ポリシーを設定するには、[単一結果の選択（Single result selection）] オプション ボタンをクリックし、すべての要求に適用するアクセス サービスを選択します。

または、ルールベースのサービスセレクションポリシーを設定するには、[ルールベースの結果選択（Rule based result selection）] オプション ボタンをオンにし、[作成（Create）] をクリックします。

ステップ 4 ルール名を入力し、ルール ステータスを選択します。

ステップ 5 サービス セレクション ポリシーのプロトコルとして [RADIUS] または [TACACS+] を選択します。

ステップ 6 必要な複合条件を設定し、着信要求に適用するアクセス サービスを選択します。

ステップ 7 [OK] をクリックし、[変更の保存（Save Changes）] をクリックします。

SSO による外部認証

（RADIUS または TACACS+ サーバーの有無にかかわらず）SSO をセットアップおよび使用するには、これらのトピックを参照してください。

- SSO サーバーの追加 （1056 ページ）
- SSO サーバーの削除 （1056 ページ）
- Cisco EPN Manager サーバー上で SSO モードを設定する （1057 ページ）

Cisco EPN Manager では、SSO サインイン ページのローカリゼーションをサポートしていません。

SSO サーバーの追加

プライマリ サーバーとバックアップ サーバーが含まれる高可用性環境に Cisco EPN Manager が導入されている場合は、HA 環境での SSO サーバーの設定 （1123 ページ）の手順を参照してください。

Cisco EPN Manager には最大 3 つの AAA サーバーを設定できます。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[SSO サーバー（SSO Servers）] を選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから、[SSO サーバーの追加（Add SSO Server）] を選択し、[実行（Go）] をクリックします。

ステップ 3 SSO 情報を入力します。SSO サーバー認証要求のサーバー再試行回数は最大 3 回です。

ステップ 4 [保存（Save）] をクリックします。

（注） SSO サーバーとして使用している EPNM サーバーを追加することもできます。**[コマンドの選択（Select a command）]** ドロップダウンリストから、**[SSO サーバーとして自身を追加（Add self as SSO Servers）]** を選択し、**[実行（Go）]** をクリックします。

SSO サーバーの削除

EPNM に追加された SSO サーバーを削除できます。SSO サーバーを削除するには、次の手順を実行します。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[SSO サーバー（SSO Servers）] を選択します。

ステップ 2 削除するサーバーを選択します。

ステップ 3 **[コマンドの選択（Select a command）]** ドロップダウンリストから、**[SSO サーバーの削除（Delete SSO Server(s)）]** を選択し、**[実行（Go）]** をクリックします。

ステップ 4 **[OK]** をクリックして、サーバーの削除を確認します。

Cisco EPN Manager サーバー上で SSO モードを設定する

SSO サーバーが SSO クライアントに追加されたときに、SSO 機能によって CA 証明書が配布されます。

Cisco EPN Manager は、CA および自己署名証明書をサポートしますが、その場合、SSO クライアントおよびSSOサーバーの両方にあるサーバーの完全修飾ドメイン名（FQDN）が証明書の Common Name（CN）フィールドに含まれていることが必要です。このサーバーは、IP アドレスから FQDN に名前解決できることが必要です。さらに、ホスト名が FQDN の最も左のコンポーネントと一致する必要があります。SSO には正確な DNS 設定が必要です。完全修飾ドメイン名（FQDN）を使用して DNS を定義する必要があります。たとえば、FQDN を使用して DNS を設定する場合の nslookup コマンドと予想されるデータは次のとおりです。

```
hostname CUSTOMER_HOSTNAME
nslookup CUSTOMER_HOSTNAME
Server:...
Address:...
Name: CUSTOMER_HOSTNAME.example.com
Address:....
```

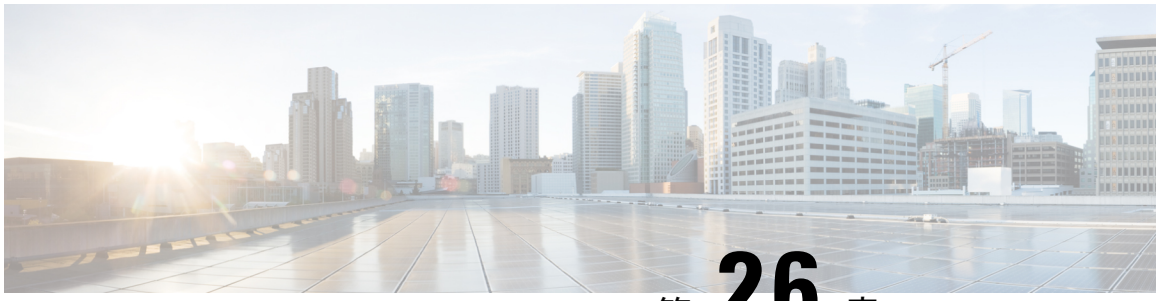
SSO 操作の場合、Cisco EPN Manager は、SSL/TLS 証明書の CN フィールドに FQDN が含まれていることを必要とします。Cisco EPN Manager サーバーが使用する証明書の CN フィールドにFQDNが含まれていることを確認するには、ブラウザを使用して証明書を表示します。証明書の CN フィールドに FQDN が含まれていない場合は、証明書を再生成して、古い証明書を使用しているすべてのユーザーに再配布する必要があります。

（注） 次の手順を使用して SSO を設定するが、ローカル認証を使用する場合は、ステップ 2 で [ローカル（Local）] を選択します。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[SSO サーバーの設定（SSO Server Settings）] を選択します。

ステップ 2 使用する SSO サーバー AAA モードを選択します。一度に 1 つのみ選択できます。

ステップ 3 [OK] をクリックします。



第 26 章

障害管理タスク

（注） アドバンス ユーザーは、Cisco EPN Manager の Representational State Transfer（REST）API を使用して、デバイスの障害情報にアクセスすることもできます。API の詳細については、Cisco EPN Manager ウィンドウの右上にある⚙をクリックし、**[ヘルプ（Help）]**>**[APIヘルプ（API Help）]** を選択します。

イベントの受信、転送、および通知

Cisco EPN Manager は、デバイスから受信した syslog と SNMPv1、v2、および v3 トラップを処理します。サーバーは、自動的に UDP ポート 162 でこれらのイベントをリッスンします。サー

バー上でイベント リスニング設定を実行する必要はありませんが、適切なポート上で Cisco EPN Manager にトラップと syslog を転送するようにデバイスを設定する必要があります。

通知は、SNMPv2 または SNMPv3 形式で転送されます。対応する通知ポリシーがセットアップされている場合は、電子メール受信者にも通知が転送されます。通知タイプ UDP の通知受信者を追加する場合、その追加する受信者はそれが設定されている同じポート上で UDP をリッスンしている必要があります。INFO レベル イベントだけが、選択されたカテゴリに対して処理され、アラームはクリティカル、メジャー、マイナー、および警告レベルで処理されます。

（注） SNMPv3 形式を使用する通知受信者には、一意のユーザー名が必要です。2 つ以上の通知受信者が同じユーザー名でパスワードが異なる場合、そのうちの 1 つが機能しません。

Cisco EPN Manager は、受信した syslog、トラップ、および TL/1 アラームを処理することによって発生したアラームとイベントをノースバウンド通知の受信者に転送できます。アラームは任意の重大度のものを転送できますが、イベントは INFO 重大度のものしか転送できません。情報は以下の形式で転送できます。

- 電子メール形式。電子メール通知のデフォルト設定 （1071 ページ）を参照してください
- SNMP トラップ形式。SNMP トラップ通知としてのアラームおよびイベントの転送（1070 ページ）を参照してください

また、SNMP トラップ通知メカニズムを使用して、サーバーの問題を示すSNMP トラップを転送することもできます。

アラートおよびイベントは SNMPv2 として送信されます。

アラーム通知設定を構成するためのユーザー ロールとアクセス権限

次の表に、通知先を設定して、カスタマイズされた通知ポリシーを作成するためのユーザー ロールとアクセス権限の説明を示します。

（注） 通知先と通知ポリシーを表示、作成、および編集するには、次のユーザー ロール用のタスク権限が有効になっていることを確認します。

- [アラートとイベント（Alerts and Events）] の通知ポリシーの読み取り/書き込みアクセス
- 仮想ドメインリスト（Virtual Domains List）

詳細については、ユーザーが実行できるタスクの表示と変更（1001 ページ）を参照してください。

ユーザー ロール	アクセス権限
ルート ドメインを持つルート ユーザー	通知先と通知ポリシーを表示、作成、削除、および編集します。
非ルート ドメインを持つルート ユーザー	通知先と通知ポリシーを表示します。
ルート ドメインを持つ管理者ユーザー	通知先と通知ポリシーを表示、作成、削除、および編集します。
ルート ドメインを持つスーパー ユーザー	通知先とアラーム通知ポリシーを表示、作成、削除、および編集します。
ルートドメインを持つシステム モニターリング ユーザー	通知先と通知ポリシーを表示します。
ルート ドメインを持つ構成マネージャ	通知先と通知ポリシーを表示します。
非ルート ドメインを持つ管理者ユーザー	それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。
非ルート ドメインを持つスーパー ユーザー	それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。
非ルートドメインを持つシステム モニターリング ユーザー	それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。
非ルート ドメインを持つ構成マネージャ	それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。

新しい通知ポリシーを追加する場合の注意事項

次の表に、新しい通知ポリシーを追加する場合に覚えておく必要があるいくつかのポイントを示します。

通知ポリシー ページで選択されたカテゴリ	注意事項
E メール	• 各仮想ドメインには、一意の連絡先名と電子メール アドレス（電子メール受信者）を割り当てる必要があります。 • 電子メール受信者は、ROOT-DOMAINからのみ、追加、変更、および削除できます。 • 1 つの電子メール アドレスを複数の仮想ドメインに関連付けることができます。 • Cisco EPN Manager は、アラーム通知を送信するために、電話番号、携帯番号、および郵便先住所の詳細を使用しません。
トラップ受信者	• 連絡先名は、トラップ受信者ごとに一意です。 • トラップ受信者は、ROOT-DOMAINからしか追加、変更、および削除することができません。トラップ受信者は ROOT-DOMAIN でのみ適用可能です。 • ノースバウンド トラップ受信者だけが、通知ポリシー エンジンから転送されたアラーム/イベントを受信できます。 • ゲスト アクセス トラップ受信者は、ゲスト クライアントに関係するアラームだけを受信します。

通知ポリシー ページで選択されたカテゴリ	注意事項
通知ポリシー	

通知ポリシー ページで選択されたカテゴリ	注意事項
	• 各通知ポリシーは、アラームカテゴリ、アラーム重大度、アラームタイプ、デバイスグループ、通知先、および時間範囲という条件で構成されます。 • 通知ポリシーはそれぞれ一意の仮想ドメインに関連付けられます。 • 必要な条件を選択するときに、ツリービュー ドロップダウン リストをドリルダウンして、個別のカテゴリ（スイッチやルータなど）と重大度（メジャーなど）を選択できます。さらに、特定のアラーム タイプ（リンク ダウンなど）を選択できます。 • ポリシー内の条件と一致したアラームがそれぞれの通知先に転送されます。 • アラームが同じ仮想ドメイン内の複数のポリシーと一致し、それらのポリシーに同じ宛先が設定されている場合は、1つの通知だけがそれぞれの宛先に送信されます。 • 通知ポリシーに関連付けられた仮想ドメインを削除すると、どのアラームもこのポリシーと一致しなくなります。この通知ポリシーはメインの通知ポリシー ページに一覧表示されますが、この通知ポリシーの詳細を変更または表示することはできません。ただし、このポリシーを削除することはできます。 • ポリシーで指定された 1 つ以上のデバイス グループを削除すると、どのアラームもこのポリシーと一致しなくなります。この通知ポリシーはメインの通知ポリシー ページに一覧表示されますが、この通知ポリシーの詳細を変更または表示することはできません。ただし、このポリシーを削除することはできます。 • 既存のアラーム ポリシーによって抑制されているアラームは、通知先に転送されません。

通知ポリシー ページで選択されたカテゴリ	注意事項
	• ルール条件にシステム カテゴリ アラームと非システム カテゴリ アラームの両方が含まれている通知ポリシーの場合は、非システム カテゴリ アラーム用のデバイス グループを選択する必要があります。 • 指定された期間に発生したアラームだけが通知先に送信されます。たとえば、期間を 8:00 ～ 17:00 に指定した場合は、午前 8 時 00 分から午後 5 時 00 分の間のアラームのみが通知されます。

アラーム通知先の設定

Cisco EPN Managerによって生成されたアラームを転送するために、電子メール通知およびノースバウンドトラップの受信者を設定できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メールと通知（Mail and Notification）] > [通知先（Notification Destination）]** の順に選択します。

ステップ 2 [追加（Add）] アイコンをクリックして、新しい通知先を作成します。

ステップ 3 電子メールの宛先を設定するには、次の手順を実行します。

a) [連絡先のタイプの選択（Select Contact Type）] ドロップダウン リストから [電子メール（Email）] を選択します。
b) [連絡先の名前（Contact Name）] テキスト ボックスに連絡先の名前を入力します。
c) [メール宛先（Email To）] テキスト ボックスに有効な電子メール ID を入力します。
電子メールは [メール宛先（Email To）] フィールドに入力した電子メール ID に送信されます。
d) [連絡先の氏名（Contact Full Name）] に連絡先の氏名を入力します。
e) [仮想ドメイン（Virtual Domain）] ドロップダウン リストから仮想ドメインを選択します。
f) [電話番号（Telephone Number）]、[携帯電話の番号（Mobile Number）]、[郵便先住所（Postal Address）] の各フィールドに値を入力します。
g) [保存（Save）] をクリックします。

ステップ 4 IP アドレスを使用してノースバウンド トラップの受信者を設定するには、次の手順を実行します。

a) [連絡先のタイプの選択（Select Contact Type）] から [ノースバウンド トラップの受信者（Northbound Trap Receiver）] を選択します。
b) [IP アドレス（IP Address）] オプション ボタンを選択し、[IP アドレス（IP Address）] および [サーバー名（Server Name）] に値を入力します。
c) [受信者のタイプ（Receiver Type）] および [通知タイプ（Notification Type）] で必要なタイプを選択します。
d) [ポート番号（Port Number）] に値を入力し、[SMNP バージョン（SMNP Version）] を選択します。

e) [SMNP バージョン（SMNP Version）] として [v2c] を選択する場合、必要に応じて [コミュニティ（Community）] 設定に値を入力します。
f) [SMNP バージョン（SMNP Version）] として [v3] を選択する場合、[ユーザー名（Username）]、[モード（Mode）]、[認証タイプ（Auth.Type）]、[認証パスワード（Auth.Password）]、[認証パスワードの確認（Confirm Auth.Password）]、[プライバシー タイプ（Privacy Type）]、[プライバシー パスワード（Privacy Password）]、[プライバシー パスワードの確認（Confirm Privacy Password）] の各フィールドに値を入力します。
g) [保存（Save）] をクリックします。

ステップ 5 DNS を使用してノースバウンド トラップの受信者を設定するには、次の手順を実行します。

a) [連絡先のタイプの選択（Select Contact Type）] から [ノースバウンド トラップの受信者（Northbound Trap Receiver）] を選択します。
b) [DNS] オプション ボタンを選択し、[DNS 名（DNS Name）] に値を入力します。
c) [受信者のタイプ（Receiver Type）] および [通知タイプ（Notification Type）] で必要なタイプを選択します。
d) [ポート番号（Port Number）] に値を入力し、[SMNP バージョン（SMNP Version）] を選択します。
e) [SMNP バージョン（SMNP Version）] として [v2c] を選択する場合、必要に応じて [コミュニティ（Community）] 設定に値を入力します。
f) [SMNP バージョン（SMNP Version）] として [v3] を選択する場合、[ユーザー名（Username）]、[モード（Mode）]、[認証タイプ（Auth.Type）]、[認証パスワード（Auth.Password）]、[認証パスワードの確認（Confirm Auth.Password）]、[プライバシー タイプ（Privacy Type）]、[プライバシー パスワード（Privacy Password）]、[プライバシー パスワードの確認（Confirm Privacy Password）] の各フィールドに値を入力します。
g) [保存（Save）] をクリックします。

ステップ 6 Restconf の宛先を設定するには、次の手順を実行します。

a) **[連絡先のタイプの選択（Select Contact Type）]** ドロップダウンリストから **[Restconf]** を選択します。
b) [宛先名（Destination Name）] を入力します。
c) 通知する [ユーザーグループ（User Groups）] を選択します。
d) [保存（Save）] をクリックします。

（注）

- [受信者のタイプ（Receiver Type）] として [ゲスト アクセス（Guest Access）] を選択すると、Cisco EPN Manager は通知ポリシーに従ってノースバウンド トラップの受信者にアラームを転送することはしません。ゲスト アクセス受信者は、ゲスト クライアント関連のイベントだけを受信します。通知ポリシーで使用するのは、ノースバウンド トラップの受信者のみです。外部 SNMPv3 トラップの受信者を設定する際は、必ず同じエンジン ID と同じ認証パスワードおよびプライバシー パスワードを使用してください。
- 通知の宛先トラップの受信者を更新中、動作状態には、次のポーリングによって状態が更新されるまで以前のトラップの受信者が表示されます。
- [Notification Policies] ページには、[Monitor] > [Monitoring Tools] > [Alarm Notification Policies] の順に選択して移動することもできます。
- 受信者の電子メール ID が複数の通知ポリシーで設定されていると、条件が一致した場合、アラームはその電子メール ID に一度だけ転送されます。
- 通知ポリシーに関連付けられている通知先を削除することはできません。
- NBI に転送されるアラームには、アラームの作成時に「correlationType」、「serviceImpacting」、「UDF」などのフィールドはありません。これらのフィールドは、次のアラーム更新時にのみ送信されます。
- EPNM によって生成される SNMP エンジン ID は、snmpv3 RFC の実装に応じて、EPNM の各インスタンスで静的である場合とそうでない場合があり、システムの再起動によって変化する可能性があります。

通知先の削除

次の手順に従い、通知先を削除します。

始める前に

通知ポリシーに関連付けられている通知先を削除することはできません。通知ポリシーから通知先の関連付けを解除したことを確認します。これを行うには、アラーム通知ポリシーを編集し、別の通知先を割り当てます。詳細については、アラーム通知ポリシーのカスタマイズ（1068 ページ）を参照してください。

（注） 通知先が複数の通知ポリシーに関連付けられている場合は、関連付けられているすべての通知ポリシーから通知先の関連付けが解除されていることを確認します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メールと通知（Mail and Notification）] > [通知先（Notification Destination）]** に移動します。

ステップ 2 削除する通知先の横にあるチェックボックスをオンにして、その通知先を選択します。

ステップ 3 [Delete] アイコンをクリックします。

アラーム通知ポリシーのカスタマイズ

新しいアラーム通知ポリシーを追加するか、または既存のアラーム通知ポリシーを編集して、特定のデバイスグループで生成される特定のアラームに関する通知を、特定の電子メール受信者、ノースバウンドトラップ受信者、および restconf 受信者宛てに送信するようにできます。

ステップ 1 [Administration] > [Settings]> [System Settings] > [Alarms and Events] > [Alarm Notification Policies] の順に選択します。新しいアラーム通知ポリシーを追加するには、次の手順に従います。

a) [追加（Add）] アイコンをクリックし、[仮想ドメインの選択（Select a Virtual Domain）] ポップアップ ウィンドウで必要な仮想ドメインを選択します。

Cisco EPN Manager により、仮想ドメインのデバイスから受信したアラームが、同じ仮想ドメインの通知ポリシーと照合されます。Cisco EPN Manager によって生成されるシステムカテゴリアラームは、すべてのアラーム通知ポリシーと照合できます。

（注） 非ルート ドメインの場合、デバイスから送信されたアラームが転送されるのは、仮想ドメイン ページの [ネットワーク デバイス（Network Devices）] タブでそのデバイスまたはデバイスを含むデバイス グループが追加または選択されている場合だけです。

b) [OK] をクリックします。
[通知ポリシー（Notification Policies）] ウィザードが表示されます。

c) 通知をトリガーする必要がある重大度、カテゴリ、およびイベント状態を選択します。デフォルトでは、すべての重大度タイプ、カテゴリ、および状態が選択されています。

d) [次へ（Next）] をクリックし、アラーム通知をトリガーするデバイス グループを選択します。

アラーム通知は、選択したデバイスグループに対してのみトリガーされます。

たとえば、デバイスグループのタイプに [ユーザー定義（User Defined）] を選択すると、設定されているユーザー定義のすべてのデバイスグループに対してアラーム通知がトリガーされます。同様に、デバイスグループのタイプに [ユーザー定義（User Defined）] と [場所（Locations）] の両方を選択した場合は、設定されているユーザー定義と場所のすべてのデバイスグループに対してアラーム通知がトリガーされます。

デバイスグループタイプを選択して、他のデバイスグループからの重要でないアラーム通知の受信を抑制します。

前のステップでシステム カテゴリ アラームだけを選択した場合は、[デバイス グループ（Device Group）] タブに「『システム』ベースのアラームだけが選択されている場合、デバイス グループは選択できません（Device Groups are not applicable when only 'System' based alarms are selected）」というメッセージが表示されます。ただし非システム カテゴリ アラームを選択した場合は、1 つ以上のデバイス グループを選択する必要があります。

e) [次へ（Next）] をクリックし、[通知の宛先（Notification Destination）] ページで必要な宛先を選択します。
ステップ 1-a でルートドメインを選択した場合、Cisco EPN Manager で作成されたすべての電子メール、ノースバウンドトラップ、Restconf の受信者の宛先が **[通知先（Notification Destination）]** ペー

ジに表示されます。非ルート ドメインを選択している場合、特定のドメインで作成された電子メールの宛先が [通知宛先（Notification Destination）] ページに表示されます。アラーム通知先の設定（1065 ページ） を参照してください。

f) あるいは、追加アイコンのドロップダウンリストで**[電子メール（Email）]**、**[ノースバウンドトラップの受信者（Northbound Trap Receiver）]**、**[Restconf]** オプションを選択し、必要なフィールドに情報を入力します。

g) 通知の宛先を選択したら、[期間の変更（Change Duration）] をクリックします。

h) [期間の設定（Set Duration）] ポップアップ ウィンドウで [開始（From）] と [終了（To）] のタイミングを選択し、[OK] をクリックします。
指定した期間内に生成されるアラームだけが、通知宛先に送信されます。

i) [次へ（Next）] をクリックし、[サマリー（Summary）] ページでアラーム通知ポリシーの [名前（Name）] と [説明（Description）] を入力します。

j) **[保存（Save）]** をクリックします。

（注） 「インターフェイス」は予約語であるため、アラーム通知ポリシーの名前として使用しないでください。

ステップ 2 アラーム通知ポリシーを編集するには、次の手順を実行します。

a) ポリシーを選択し、編集アイコンをクリックします。
[通知ポリシー（Notification Policies）] ウィザードが表示されます。

b) ステップ 1 の説明に従い、[状態（Conditions）]、[デバイス グループ（Device Groups）]、および [宛先（Destination）] を選択します。

c) [保存（Save）] をクリックします。

古い電子メールとトラップ通知データを新しいアラーム通知ポリシーに変換する

Cisco EPN Manager を以前のリリースから最新のバージョンにアップグレードすると、Cisco EPN Manager の以前のリリースで作成された電子メールとトラップ通知データが新しいアラーム通知ポリシーに変換されます。

移行されたアラーム通知ポリシーは、[アラームおよびイベント通知ポリシー（Alarms and Events Notification Policies）] ページで確認できます。

Cisco EPN Manager では、次のアラームカテゴリがサポートされます。

- アプリケーション パフォーマンス
- 変更監査
- クライアント
- コンピューティング サーバー
- コンテキスト認識型通知
- コントローラ
- 汎用

- モビリティ サービス
- Nexus VPC スイッチ
- パフォーマンス
- SE で検出された干渉源
- セキュリティ
- スイッチとルータ
- システム（System）

Cisco EPN Manager では、次のアラームカテゴリがサポートされていません。

- アドホック不正
- AP
- 自律 AP
- Cisco UCS シリーズ
- カバレッジ ホール
- メッシュリンク（Mesh Links）
- ルータ
- 不正 AP
- RRM
- スイッチおよびハブ
- サード パーティ AP
- サードパートコントローラ（Third Part Controller）
- ワイヤレス コントローラ

移行されたアラーム通知ポリシーを編集するには、「アラーム通知ポリシーのカスタマイズ（1068 ページ）」を参照してください。

SNMP トラップ通知としてのアラームおよびイベントの転送

Cisco EPN Manager は、SNMPv2c および SNMPv3 トラップ通知として、アラームとイベントを EPM-NOTIFICATION-MIB 形式で転送できます。次を指定することができます。

- 特定のアラームまたはイベントのカテゴリ（たとえば、内部サーバー SNMP トラップの場合は [システム（System）]）。
- 特定の重大度のアラーム。INFO イベントだけが転送されます。イベントの他の重大度を指定することはできません。

詳細については、アラーム通知先の設定 （1065 ページ）を参照してください。

電子メール通知のデフォルト設定

メールサーバーを設定していない場合は、「SMTP電子メールサーバーの設定 （969ページ）」に記載の手順を実行してください。この手順を実行しないと、通知は送信されません。

すべてのアラームおよびイベントのメール通知に適用される特定のデフォルト設定を設定できます。これらの設定は、ユーザーが個別の通知と受信者を設定するときに、上書きできます。

デフォルトでは、電子メールの件名にアラームの重大度とカテゴリが含まれます。次の設定も使用できますが、デフォルトでは無効になっています。

- [件名（Subject line）]：より重要なアラーム重大度を含めるか、カスタム テキストを追加します。また、件名全体をカスタム テキストに置き換えることもできます。
- [電子メールの本文（Body of the email）]：カスタム テキスト、アラーム条件、およびアラームの詳細ページへのリンクを含めます。
- [セキュアなメッセージ モード（Secure message mode）]：このモードを有効にすると、IP アドレスとコントローラ名がマスクされます。

これらの設定を有効化、無効化、または調整するには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、さらに **[アラームおよびイベント（Alarms and Events）]** > **[アラームおよびイベント（Alarms and Events）]** を選択します。[アラーム電子メール オプション（Alarm Email Options）] エリアで変更を加えます。

アラームクリーンアップ、表示、および電子メールオプションの指定

[管理（Administration）]>[システム設定（System Settings）]>[アラームおよびイベント（Alarms and Events）]ページでは、アラームのクリーンアップ、表示、電子メール送信のタイミングと方法を指定できます。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [アラームおよびイベント（Alarms and Events）] > [アラームおよびイベント（Alarms and Events）] を選択します。

ステップ 2 [アラームおよびイベントのクリーンアップ オプション（Alarm and Event Cleanup Options）] を次のように変更します。

- [クリアされた非セキュリティ アラームを次の後で削除（Delete cleared non-security alarms after）]：セキュリティ アラーム以外のアラームが削除されるまでの日数を入力します。セキュリティアラーム以外のアラームには、[セキュリティ（Security）] カテゴリまたは [アドホック不正（Adhoc Rogue）] カテゴリに属するアラーム以外のすべてのアラームが含まれます。
- [クリアされたセキュリティアラームを次の後で削除（Delete cleared security alarms after）]：セキュリティアラームとアドホック不正アラームが削除されるまでの日数を入力します。

- [すべての（アクティブおよびクリアされた）アラームを次の後で削除（Delete all (active & cleared) alarms after）]：アクティブなアラームまたはクリアされたアラームが削除されるまでの日数を入力します。
- [すべてのイベントを次の後で削除（Delete all events after）]：すべてのイベントを削除するまでの日数を入力します。

最大値は、8000000 イベントまたは指定された日数のいずれか小さい方です。

ステップ 3 [syslog クリーンアップ オプション（Syslog Cleanup Options）] を次のように変更します。

- [すべての syslog を次の後で削除（Delete all Syslogs after）]：すべての古い syslog について、削除するまでの日数を入力します。
- [最大保持 syslog 数（Max Number of Syslog to Keep）]：データベースで保持する必要がある syslog の数を入力します。

ステップ 4 必要に応じて、[アラーム表示オプション（Alarm Display Options）] を変更します。

- [確認済みのアラームを非表示（Hide acknowledged alarms）]：このチェックボックスをオンにすると、承認済みのアラームは [アラーム（Alarm）] ページに表示されません。このオプションは、デフォルトで有効です。重大度の変化に関係なく、確認応答済みのアラームに対して電子メールは生成されません。
- [割り当て済みのアラームを非表示（Hide assigned alarms）]：このチェックボックスをオンにすると、割り当て済みのアラームは [アラーム（Alarm）] ページに表示されません。
- [Hide cleared alarms]：このチェックボックスをオンにすると、クリアされたアラームは [Alarm] ページに表示されません。このオプションは、デフォルトで有効です。
- [[アラーム]タブにアクティブアラームのみを表示（Show only Active Alarms in Alarms tab）]：このチェックボックスをオンにすると、アクティブなアラームのみが [アラーム（Alarms）] タブのアラームリストに表示されます。
- [アラーム メッセージにデバイス名を追加（Add device name to alarm messages）]：このチェックボックスをオンにすると、デバイスの名前がアラーム メッセージに追加されます。

これらのオプションの変更は、[アラーム（Alarm）]ページにのみ適用されます。エンティティに対するアラームのクイック検索は、アラームの状態に関係なく、そのエンティティのすべてのアラームを表示します。

ステップ 5 アラームの [障害ソース パターン（Failure Source Pattern）] を次のように変更します。

- カスタマイズするカテゴリを選択し、[編集（Edit）] をクリックします。
- 利用可能な選択肢から障害ソースパターンを選択し、[OK] をクリックします。
- セパレータをカスタマイズするカテゴリを選択し、[セパレータの編集（Edit Separator）] をクリックします。使用可能なオプションの 1 つを選択し、[OK] をクリックします。

選択したカテゴリに対して生成されるアラームには、ユーザーが設定するカスタム パターンが使用されます。たとえば、[クライアント（Clients）] カテゴリを選択し、セパレータが # になるように編集するとします。サポートされるクライアント アラームが生成されたときにユーザーが [モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択すると、そのアラームの [障害のソース（Failure Source）] 列は *MAC* アドレス#名前となります。

（注） 障害のソースは、カスタム トラップ、syslog 生成イベント、およびカスタム syslog 変換ではサポートされません。

ステップ 6 [アラーム電子メールのオプション（Alarm Email Options）] を次のように変更します。

- [Add Cisco EPN Manager address to email notifications]：このチェックボックスをオンにすると、電子メール通知に Cisco EPN Manager のアドレスが追加されます。
- [電子メールの件名行にアラームの重要度を含める（Include alarm severity in the email subject line）]：このチェックボックスをオンにすると、電子メールの件名にアラーム重大度が含まれるようになります。このオプションは、デフォルトで有効です。
- [電子メールの件名行にアラームカテゴリを含める（Include alarm Category in the email subject line）]：このチェックボックスをオンにすると、電子メールの件名にアラームのカテゴリが含まれるようになります。このオプションは、デフォルトで有効です。
- [電子メールの件名行に優先アラーム重要度を含める（Include prior alarm severity in the email subject line）]：このチェックボックスをオンにすると、電子メールの件名に事前アラーム重大度が含まれるようになります。
- [電子メールの件名行にカスタムテキストを含める（Include custom text in the email subject line）]：このチェックボックスをオンにすると、電子メールの件名にカスタムテキストが追加されます。[電子メールの件名行をカスタム テキストで置換する（Replace the e-mail subject line with custom text）] チェックボックスをオンにして、電子メールの件名をカスタム テキストに置き換えることもできます。
- [電子メールの本文にカスタムテキストを含める（Include custom text in body of email）]：このチェックボックスをオンにすると、電子メールの本文にカスタム テキストが追加されます。
- [電子メールの本文にアラーム状態を含める（Include alarm condition in body of email）]：このチェックボックスをオンにすると、電子メールの本文にアラーム状態が含まれるようになります。
- [電子メールの本文にアラーム アプリケーション カテゴリ データを含める（Include alarm application category data in body of email）]：このチェックボックスをオンにすると、電子メールの本文にアラームカテゴリが含まれるようになります。
- [電子メールの本文にアラームの詳細ページへのリンクを追加する（Add link to Alarm detail page in body of email）]：このチェックボックスをオンにすると、電子メールの本文に [アラームの詳細（Alarm detail）] ページへのリンクが追加されます。
- [セキュア メッセージモードの有効化（Enable Secure Message Mode）]：チェックボックスをオンにすると、セキュア メッセージ モードが有効になります。[IP アドレスをマスク（Mask IP Address）] および [コントローラ名をマスク（Mask Controller Name）] チェックボックスをオンにした場合、アラーム電子メールはセキュア モードで送信され、すべての IP アドレスとコントローラ名はマスクされます。
- [電子メール送信間隔（Email Send Interval）]：電子メールの送信間隔を指定します。

（注） Cisco EPN Managerはアラームの最初のインスタンスに関するアラーム通知電子メールを送信し、その後の通知はアラーム重大度が変更された場合にのみ送信されます。

ステップ 7 [アラームのその他のオプション（Alarm Other Options）] を次のように変更します。

- [コントローラライセンス数のしきい値（Controller License Count Threshold）]：しきい値のパーセンテージを入力します。コントローラに接続されているアクセスポイントの数が、コントローラで使用可能なライセンスの指定レートに達すると、アラームがトリガーされます。たとえば、コントローラのアクセスポイントライセンスが 100、しきい値が 80% で設定されている場合、コントローラに接続されているアクセスポイントの数が 80 を超えると、アラームがトリガーされます。
- [AP カウントしきい値アラームの有効化（Enable AP count threshold alarm）]：このチェックボックスをオンにすると、しきい値アラームの AP カウントを有効にします。
- [コントローラ アクセス ポイント数のしきい値（Controller Access Point Count Threshold-）]：しきい値のパーセンテージを入力します。コントローラに接続されているアクセスポイントの数が、コントローラでサポートされているアクセスポイントの最大数の指定レートに達すると、アラームがトリガーされます。たとえば、コントローラが最大6000アクセスポイントをサポートしており、しきい値が80%に設定されている場合、コントローラに接続されているアクセスポイントの数が 4800 を超えるとアラームがトリガーされます。
- [Admin Down 状態のインターフェイスで光 SFP TCA を抑制（Suppress Interface Optical SFP TCA in Admin Down State）]：このチェックボックスをオンにすると、Admin Down 状態のインターフェイスで光 SFP TCA の発生を防ぐことができます。
- [サービス影響分析の有効化（Enable Service Impact Analysis）]：このチェックボックスをオンにすると、サービス影響分析が有効になります。
- [ツリーの根本原因がクリアされたときに相関ツリーからのサブツリー作成を有効化（Enable creation of subtrees from a correlation tree when root cause of the tree clears）]：相関ツリーの根本原因がクリアされたときに、この相関ツリーのサブツリーが作成されます。各サブツリーには未解決の根本原因がある場合にこのチェックボックスをオンにすると機能が有効になります。
- **[インターフェイスステータスポーリングからのアラームの有効化（Enable alarms from interface status polling）]**：このチェックボックスが選択されている場合、イーサネットとバンドルインターフェイスのインターフェイスステータスをポーリングすることで、LinkDown アラームが発生およびクリアされます。
- [EPNM インベントリ収集に基づくアラーム生成の有効化（Enable alarm generation based on EPNM inventory collection）]：EPNM はエンティティのインベントリステータスを使用して特定のアラームを生成およびクリアします。このメカニズムは、（デバイスでこれらが生成されず、ネットワーク内で失われたことなどが原因で）失われたか欠けている可能性のある syslog およびトラップのバックアップとして機能します。
- [ユーザー定義フィールドの有効化（Enable User Defined Field）]：この設定が有効になっている場合、[アラーム（Alarms）] タブのアラームリストに、ハードウェアアラームの PRODUCT_NAME と PRODUCT_ID が条件付きで入力されます。この設定は既存のアラームには影響せず、以前に発生したアラームに遡ってを適用されません。デフォルトでは、この設定はディセーブルになっています。

- **[イベントスロットルの有効化（Enable Event Throttle）]**：このチェックボックスをオンにすると、デバイスのイベントカウントがしきい値カウントを超えた場合（デフォルトでは、1 時間以内に発生したイベントが 3,600 を超える場合）、Cisco EPN Manager によってイベントがプロアクティブにドロップされます。詳細については、デバイスごとのイベントスロットルのカスタマイズ（1082 ページ）を参照してください。
- **[SVO へのアラーム相互起動の有効化（Enable Alarms Cross Launch to SVO）]**：このチェックボックスをオンにすると、アラームテーブル（**[モニター（Monitor）]** > **[監視ツール（Monitoring Tools）]** > **[アラームおよびイベント（Alarms and Events）]**）から SVO ノードクラフトへの相互起動が有効になります。

  （注） SVO UI に移動するたびにログイン情報を入力しないようにするには、Cisco EPN Manager から SVO ノードクラフトへのシングルサインオン（SSO）を有効にします。詳細については、Cisco EPN Manager から SVO UI へのシングルサインオン（SSO）を有効にする （66 ページ）を参照してください。
- **[一時的な状態アラームの有効化（Enable Transient Condition Alarms）]**：このチェックボックスをオンにすると、Cisco EPN Manager は一時的なイベントをアラームとして処理し、これらのイベントを **[アラーム（Alarms）]** テーブルに表示します。このチェックボックスをオフにすると、一時的なイベントはアラームとして処理されません。デフォルトでは、このチェックボックスはオフになっています。
- **[ネットワークアラームビューの有効化（Enable Network Alarms View）]**：このオプションを選択すると、**[ネットワークアラーム（Network Alarms）]** タブが **[アラーム（Alarms）]** タブに追加されます。**[ネットワークアラーム（Network Alarms）]** タブには、ネットワークに影響するすべてのアラームが一覧表示されます。デフォルトでは、このオプションは無効になっています。
- **[NBI Web Socketのクライアントに対して通知ポリシーベースのフィルタを有効にする（Enable Notification Policy based filter for NBI WebSocket's Client）]**：このチェックボックスをオンにすると、アラーム通知ポリシーで restconf が有効になり、ノースバウンド WebSocket の接続先が追加されます。
- [Netconfセッションの最大再試行回数（Max no. of Netconf Session Retry）]：SVO 障害を処理するために Netconf セッションが接続を試みる回数を入力します。
- [Netconfセッションの再試行間隔（Netconf Session Retry Interval）]：Netconf セッションが SVO 障害を処理できるようにするために、再試行の間隔を秒単位で入力します。
- [通知で送信されるデバイス UDF の有効化（Enable Device UDF to be sent in notifications）]：このチェックボックスをオンにすると、デバイス UDF のアラーム通知が有効になります。
- [アラームなし（NA）状態アラームの有効化（Enable Not Alarmed (NA) Condition Alarms）]：このチェックボックスをオンにすると、イベントが光デバイスのアラームとして処理されなくなります。
- [SVOデバイスのアラームとイベントの再生サポートの有効化（Enable Alarms & Events Replay support for SVO Devices-）]：このチェックボックスをオンにすると、SVO デバイスの Netconf 再生が有効になります。これにより、ネットワーク接続障害、SVO スイッチオーバー、デバイスのダウンタイム、またはその他の接続障害中に失われたイベントが再生されます。
- [SVOデバイスのアラームとイベントの再生時間（Duration for the Alarms & Events Replay for SVO Devices）]：アラームとイベントの同期に必要な最長期間を入力します。デフォルトオプションは 720 分または 12 時間です。このフィールドに長い期間を入力しないことをお勧めします。

ステップ 8 [アラームマネージャの設定（Alarm Manager Settings）] については、Cisco IOS XR デバイスでのアラームマネージャの設定 （1077 ページ）を参照してください。

ステップ 9 [保存（Save）] をクリックします。

確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する

次の表に、確認済み、クリア済み、および割り当て済みのアラーム用の表示オプションの一部を示します。これらの設定は、個別のユーザーが（表示設定で）調整することができません。これは、非常に大規模なシステムの場合に、ユーザーがシステムパフォーマンスに影響を及ぼすような変更を加える可能性があるためです。

[アラームおよびイベント（Alarms and Events）] ページに表示されるその他の設定はユーザーが調整できますが、ここではグローバル デフォルトを設定できます。これらの設定については、次のトピックを参照してください。

- 電子メール通知のデフォルト設定
- アラーム、イベント、および Syslog の消去 （992 ページ）

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[アラームおよびイベント（Alarms and Events）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 2 [表示オプションのアラーム（Alarm Display Options）] 領域で、必要に応じて、これらの設定を有効または無効にします。

アラーム表示オプション	説明	設定が検索結果にも影響するかどうか
確認済みのアラームを非表示（Hide acknowledged alarms）	[アラーム（Alarms）] リストに確認済みのアラームを表示しないか、それらを検索結果に含めません。	○
割り当て済みのアラームを非表示（Hide assigned alarms）	[アラーム（Alarms）] リストまたは検索結果に割り当て済みのアラームを表示しません。	○

クリア済みのアラームを非表示（Hide cleared alarms）	[アラーム（Alarms）] リストまたは検索結果にクリア済みのアラームを表示しません。 たとえば、4000 アラームのうちの 3900 がクリアされたアラームである場合、この設定を有効にすると、[アラーム（Alarms）] > [アクティブアラームの表示（Showing Active Alarms）] のアラームリストにはクリアされていない 100 のアラームが表示されます。 （注） クリア済みのアラームは、[クリア済みのアラーム（Cleared Alarms）] タブでは表示可能なままです。	なし
[アラーム（Alarms）] タブにアクティブアラームのみを表示（Show only Active Alarms in Alarms tab）	[アラーム（Alarms）] タブのアラームリストにアクティブなアラームのみを表示します。 たとえば、4000 アラームのうちの 3900 がクリアされたアラームである場合、この設定を有効にすると、[アラーム（Alarms）] > [アクティブアラームの表示（Showing Active Alarms）] のアラームリストには最新のクリアされていない 4000 のアラームが表示されます。 （注） クリア済みのアラームは、[クリア済みのアラーム（Cleared Alarms）] タブでは表示可能なままです。	なし
アラームメッセージにデバイス名を追加（Add device name to alarm messages）	電子メール通知にデバイス名を追加します。	なし

ステップ 3 変更を適用するには、[アラームおよびイベント（Alarms and Events）] ウィンドウの下部にある [保存（Save）] をクリックします。

Cisco IOS XR デバイスでのアラームマネージャの設定

信頼性の高いアラームの一部として、Cisco EPN Manager は Cisco IOS XR デバイスのアラームマネージャをポーリングして未処理のアラームまたはイベントを確認します。

（注） アラームマネージャのサポートは、Cisco IOS XR デバイスの NCS 10xx、NCS 40xx、および NCS 55xx のみに限定されています。

Cisco EPN Manager GUI でアラームマネージャを有効または無効にするには、次の手順に従います。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択してから、**[アラームおよびイベント（Alarms and Events）]** > **[アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 2 [Alarm Manager Settings] で、デバイスタイプを選択して、必要に応じてアラームマネージャを有効または無効にします。

（注） デフォルトでは、アラームマネージャは、[Alarm Manager Settings] 領域の下に一覧表示されているすべてのデバイスタイプに対して有効になっています。

ステップ 3 [保存（save）] をクリックして変更を適用します。

ステップ 4 [Alarms and Events] ウィンドウの下部にある [Save] をクリックします。

アラームマネージャが有効になっている場合、Cisco EPN Manager は 5 分ごとにデバイスをポーリングします。このポーリング間隔は変更できません。アラームマネージャによって発生したすべてのアラームは、**[Monitor]** > **[Monitoring Tools]** > **[Alarms and Events]** ページの **[Alarm]** タブに一覧表示されます。このリストでは、重大度を変更したり、アラームマネージャによって発生したアラームをクリアまたは削除したりすることはできません。アラームマネージャによって発生したアラームについては、アラームのソースが「Synthetic_Event」と表示されます。

アラームマネージャを無効にした場合は、アラームマネージャによって以前に発生したすべてのアラームがクリアされます。Cisco EPN Manager はデバイスをポーリングしなくなりますが、引き続きデバイスから直接アラームを受信します。すべての PKT-INFRA-FM アラームは、**[Monitor]** > **[Monitoring Tools]** > **[Alarms and Events]** ページの **[Events]** タブに一覧表示されます。

Cisco IOS XE デバイスでのアラーム再同期の設定

「show facility」コマンドに基づくアラーム再同期機能は、Cisco IOS XE デバイス用の信頼性の高いアラームの一部です。この機能は、Cisco NCS 42xx デバイスのソフトウェアバージョン 16.6.6vS および 16.9.1 でサポートされています。`/conf/fault/ncs42xx/resources/NCS42xxAlarmManager.properties` ファイルを変更することにより、アラームの再同期を有効または無効にすることができます。

アラーム再同期が有効になっている場合、デバイスから受信したアラームは、**[Monitor]** > **[Monitoring Tools]** > **[Alarms and Events]** ページの [Alarm] タブに表示されます。Cisco EPN Manager を使用して、重大度を変更したり、これらのアラームをクリアまたは削除したりすることはできません。

（注） アラーム再同期機能は、DSX、SONET、およびシステムアラームを選択する場合にのみサポートされます。詳細は Cisco Evolved Programmable Network Manager のサポート対象 Syslog を参照してください。

Cisco NCS 42xx デバイスでアラームマネージャを有効または無効にする手順を次に示します。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開きます。詳細については、「CLI 経由の接続 （953 ページ）」を参照してください。

ステップ 2 `/conf/fault/ncs42xx/resources/NCS42xxAlarmManager.properties` ファイルを開きます。

ステップ 3 必要に応じて、`shfacilityenabled`、`resyncperiodmillis`、および `pollerperiodmillis` を変更します。

- `shfacilityenabled`：アラームマネージャを有効または無効にするフラグ。このフラグを true に設定すると、アラーム再同期が有効になります。デフォルトでは、この値は true に設定されています。この値を変更する場合、システムの再起動は必要ありません。
- `resyncperiodmillis`：デバイスをポーリングするポーリング間隔。これらの値は必要に応じて変更できます。デフォルト値は、600000 ミリ秒（10 分）です。この変更を有効にするには、システムを再起動する必要があります。
- `pollerperiodmillis`：アラームマネージャをポーリングするためにデバイスリストを更新するポーラ。この値は必要に応じて変更できます。デフォルト値は 3600000 ミリ秒（1 時間）です。この変更を有効にするには、システムを再起動する必要があります。

Cisco IOS XE デバイスでのアラームプロファイリングの設定

Cisco EPN Manager は、Cisco IOS XE デバイスのアラームプロファイリングをサポートしています。Cisco EPN Manager でアラームプロファイリングの変更を反映するには、`alarmprofileEnabled` を `true` に設定します。手順は次のとおりです。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開きます。詳細については、「CLI 経由の接続 （953 ページ）」を参照してください。

ステップ 2 `/conf/fault/ncs42xx/resources/NCS42xxVersion.properties` ファイルを開きます。

ステップ 3 `alarmprofileEnabled` を `true` に設定し、変更を保存します。デフォルトでは、`alarmprofileEnabled` は有効になっています。

（注） `alarmprofileEnabled` が false に設定されている場合、Cisco EPN Manager はアラームプロファイリングの変更を反映しません。

アラーム重大度レベルの変更

Cisco EPN Manager の各アラームには重大度が設定されます。アラームの重大度は、アラームに関連付けられている最も重大なイベントによって決定します。新たに生成されたイベントの重大度を変更することにより、アラームの重大度を調整できます。

（注） ハイ アベイラビリティなど Cisco EPN Manager のシステム管理に関連付けられたアラームについては、サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送 （981 ページ）を参照してください。

entsensor アラームの場合、デフォルトの重大度設定ページを使用してデフォルトの重大度を変更しないでください。

次の 2 つの方法で、ネットワーク レベルおよびデバイス レベルのアラームの重大度を変更できます。

- オプティカル、キャリア イーサネット、デバイス ヘルス、インターフェイス ヘルス モニターリング ポリシーによって生成されたしきい値超過のアラーム：関連するモニターリング ポリシーの設定を変更します。モニターリング ポリシーのしきい値およびアラーム動作の変更 （296 ページ）を参照してください。
- 特定のアラーム：このセクションの手順を使用します。

ステップ 1 **[管理（Administration）]**>**[システム設定（System Settings）]** を選択し、**[アラームおよびイベント（Alarms and Events）]** > **[アラームの重大度および自動クリア（Alarm Severity and Auto Clear）]** の順に選択します。

ステップ 2 **[アラーム状態（Alarm Condition）]** 列で使用可能なカテゴリを拡張するか、または列見出しのすぐ下にある **[アラーム状態（Alarm Condition）]** フィールドにイベントテキスト全体または一部を入力して必要な [アラーム状態（Alarm Condition）]を検索します。

ステップ 3 イベントを選択し、新しい重大度を設定します。

1. イベントのチェックボックスをオンにします。
2. [重大度（Severity）] ドロップダウン リストから重大度を選択し、[保存（Save）] をクリックします。

アラームのトラブルシューティング テキストのカスタマイズ

トラブルシューティングと説明の情報をアラームに関連付けると、[アラームおよびイベント（Alarms and Events）] テーブルへのアクセス権を持つユーザーがその情報を表示できるようになります。ポップアップ ウィンドウに表示される情報を追加または変更するには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[アラームおよびイベント（Alarms and Events）] > [アラームの重大度および自動クリア（Alarm Severity and Auto Clear）]** を選択します。

ステップ 2 アラームを選択し、[推奨アクション（Recommended Action）] をクリックします。

ステップ 3 [説明（Explanation）] および [推奨アクション（Recommended Actions）] フィールドの内容を追加または変更して、[保存（Save）] をクリックします。デフォルトのテキストに戻すには、[リセット（Reset）] をクリックしてから [保存（Save）] をクリックします。

アラームの自動クリア間隔の変更

特定の期間が経つと自動的にアラームがクリアされるように設定できます。この設定は、クリアイベントがない場合などに役立ちます。アラームの自動クリアによって、アラームに関連するイベントの重大度が変更されることはありません。

自動クリアの期間は、55 分までは 5 分間隔で設定できます。この時間を超えると、1 時間または 60 分の倍数で間隔を設定できます。

（注）
- アラームの自動クリアを有効にしている場合、作成されたアラームのクリアに遅延が生じることがあります。
- 自動クリア間隔を 1 時間未満に設定すると、システムパフォーマンスに影響する可能性があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[アラームおよびイベント（Alarms and Events）] > [アラームの重大度および自動クリア（Alarm Severity and Auto Clear）]** を選択します。

ステップ 2 [イベントタイプ（Event Types）] 列の下に表示されているカテゴリを展開します。または、列ヘッダーの下にある [イベントタイプ（Event Types）] 検索フィールドにイベントのテキストの全部または一部を入力することにより、イベントタイプを検索します。

ステップ 3 自動クリアの期間を変更するには、次の手順を実行します。

- 単一のイベントの場合、チェックボックスをオンにしてイベントを選択し、[アラームの自動クリア（Alarm Auto Clear）] ボタンをクリックするか、**または**、選択したイベントの [自動クリア期間（Auto Clear Duration）] 列の下のフィールドをダブルクリックします。新しい期間を入力します。
- 複数のイベントの場合、イベントまたはイベントのグループのチェックボックスをオンにし、[アラームの自動クリア（Alarm Auto Clear）] ボタンをクリックして、新しい期間を入力します。

ステップ 4 [OK] または [保存（Save）] をクリックして、自動クリア期間を保存します。

アラームの失敗の原因に表示される情報を変更する

アラームが生成された場合は、失敗の原因に関する情報がそれに含まれています。情報は特定の形式を使用して表示されます。たとえば、パフォーマンスの失敗の場合は、*MACAddress*:*SlotID* という形式が使用されます。他のアラームの失敗の原因として、ホスト名、IP アドレス、またはその他のプロパティが含まれている場合があります。次の手順を使用して、アラームの失敗の原因に表示されるプロパティと区切り文字（コロン、ダッシュ、またはシャープ記号）を調整します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[アラームおよびイベント（Alarms and Events）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 2 [失敗の原因パターン（Failure Source Pattern）] 領域で、カスタマイズするアラーム カテゴリを選択します。

ステップ 3 次のように失敗の原因形式を調整します。

- 表示されるプロパティをカスタマイズするには、[編集（Edit）] をクリックして、プロパティを選択し、[OK] をクリックします。プロパティが灰色表示されている場合は、それを削除することができません。
- プロパティの間に表示される区切り文字をカスタマイズするには、[区切り文字の編集（Edit Separator）] をクリックします。

ステップ 4 変更を適用するには、[アラームおよびイベント（Alarms and Events）] 設定ウィンドウの下部にある [保存（Save）] をクリックします。

デバイスごとのイベントスロットルのカスタマイズ

デバイスによって発生したイベントの数がしきい値を超えると、Cisco EPN Manager はイベントをプロアクティブにドロップします。下限しきい値に到達すると、イベント処理が再開されます。

デフォルトでは、1 時間以内に 3,600 を超えるイベントが発生した場合、Cisco EPN Manager はデバイスからイベントをプロアクティブにドロップします。イベント数が 3,000 に低下すると、イベント処理が再開されます。

デフォルトのしきい値を変更するには、次の手順を実行します。

始める前に

この機能を有効にするには、次の手順を実行します。

1. [管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[アラームおよびイベント（Alarms and Events）]>[アラームおよびイベント（Alarms and Events）]に移動します。
2. [イベントスロットルの有効化（Enable Event Throttle）]チェックボックスをオンにします。

ステップ 1 Cisco EPN Manager で CLI セッションを開きます（詳細については、CLI 経由の接続 （953 ページ）を参照）。

ステップ 2 `/conf/fault/cep/EventThrottleRules.xml` ファイルを開きます。

ステップ 3 次のルールで必要な値を指定します。

- `Add_Suppress_Event_Based_On_Count_Per_Device_Rule`

  ：デバイスによって発生したイベントを Cisco EPN Manager がプロアクティブにドロップするしきい値カウント。デフォルトでは、この値は 3600 です。
- `Remove_Suppress_Event_Based_On_Count_Per_Device_Rule`：Cisco EPN Manager がイベントの処理を再開するしきい値カウント。デフォルト値は 3000 です。

システムのイベントスロットル

Cisco EPN Manager は、イベントスロットルを設定してシステムレベルでイベントをチェックすることにより、ネットワークの輻輳をチェックします。

ネットワーク内のキュー占有率が 60% を超えると、イベントのドロップが開始されます。このようなシナリオでは、次のメッセージが表示されます。

「システムイベント処理キューが、設定されている上限しきい値に達しました。イベントのドロップを回避するには、持続的に高いネットワークイベントレートをチェックしてください。（The system event processing queue has reached the configured upper threshold value. Please check for sustained high network event rate to avoid dropping of events.）」

ネットワーク内のキュー占有率が完全な容量に達した場合、次のメッセージが表示されます。

「システムイベント処理キューが満杯であり、最も古いイベントがキューからドロップされます。ドロップされたイベントの詳細は、assure_fault.logで確認してください。（The system event processing queue is full and oldest events from the queue will be dropped. Please find the details of the dropped events in assurance_fault.log.）」

どちらのシナリオでも、ネットワーク障害や、大量の着信ネットワークイベントの原因となる要因を確認することをお勧めします。

上限しきい値のパーセント値はキュー容量の 60% に設定され、超えるとアラームが生成されます。システムが下限しきい値の 30% に達すると、アラームはクリアされます。

完全優先ベントの動作の変更

Cisco EPN Manager は、デバイスから設定変更イベントを受信すると、他の関連するイベントが送信される場合に備えて特定の時間待機してからインベントリ収集を開始します。これにより、複数の収集プロセスの同時実行が回避されます。これは、インベントリ収集保留時間と呼ばれ、デフォルトで 10 分に設定されています。この設定は、[インベントリ（Inventory）] システム設定ページ（**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）]**）で制御されています。

次のイベントは、デフォルトの時間間隔である 10 分以内に Cisco EPN Manager によって処理されます。

タイプ（**Type**）	サポートされるイベント
リンク	LINK-3-UPDOWN
カード保護	CARD_PROTECTION-4-PROTECTION CARD_PROTECTION-4-ACTIVE
VLAN	PORT_SECURITY-6-VLAN_REMOVED PORT_SECURITY-6-VLAN_FULL
ICCP SM	L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION_CLEAR L2-L2VPN_ICCP_SM-3-CONFIG_LOCAL_ERROR L2-L2VPN_ICCP_SM-3-CONFIG_REMOTE_ERROR L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION_CLEAR L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_FAILURE L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_CLEAR L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE_CLEAR INFRA-ICCP-5-ISOLATION INFRA-ICCP-5-ISOLATION_CLR INFRA-ICCP-5-NEIGHBOR_STATE_UP INFRA-ICCP-5-NEIGHBOR_STATE_DOWN INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_UP INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_DOWN L2-BM-6-ACTIVE_CLEAR L2-BM-6-ACTIVE_PROBLEM L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID_CLEAR
衛星	PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_PROBLEM PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_CLEAR
クラスタ	PLATFORM-REDDRV-7-ROLE_CHANGE PLATFORM-CE_SWITCH-6-UPDN PLATFORM-CLUSTER_CLM-6-UPDN LINK_UP LINK_DOWN
Celeborn カード	UEA_SPA_MODE-6-UEA_SPA_MODE_CHG

タイプ（Type）	サポートされるイベント
コンフィギュレーション コミット syslog	MGBL-CONFIG-6-DB_COMMIT SYS-5-CONFIG_I

ただし、次の重大なイベントが発生した場合はすぐに、Cisco EPN Manager によってデバイスのフルディスカバリが実行されます。

```
SYS-5-RELOAD
SYS-5-RESTART
OIR-6-INSCARD
OIR-SP-6-INSCARD
SWT_CEFC_STATUS_CHANGE
cefcFRURemoved
cefcFRUInserted
```

局所的インベントリのイベントフローコントローラ

局所的インベントリでは、生成されたイベントが識別され、デバイスで行われた変更のみが処理されます。イベントの流入によるデバイスの連続的な同期を避けるため、詳細なインベントリではイベント バースト フロー コントローラと連続イベントフローコントローラが使用されます。

イベントバーストおよび連続イベントは、**/opt/CSCOlumos/conf/fault/correlationEngine/CE-EventBasedInventoryRules.xml** ファイルからのみ設定できます。

イベント バースト フロー コントローラ

管理対象デバイスのいずれかのテクノロジーについて、着信イベントの数がしきい値（BurstHoldOffTimer の BurstThreshold）を超えると、Cisco EPN Manager によってイベントバースト状態と見なされます。このシナリオでは、イベントバースト状態がクリアされるまで、しきい値違反となっているイベントの詳細なインベントリ同期が一定の期間（BurstHoldOffTimer）保留されます。この状態チェックは定期的に繰り返されます。指定の再試行回数（BurstCheckRetryCount）が経過した後もまだしきい値違反となっている場合は、Cisco EPN Manager によってデバイスの詳細なインベントリ処理がすべて停止されます。

イベントバースト状態が検出され、3回の再試行の前にクリアされた場合は、イベント バースト フロー コントローラによって、対応するテクノロジーの機能の同期がトリガーされます。イベントバースト状態が検出され、3 回の再試行の後も継続している場合は、コントローラによってすべての詳細なインベントリ処理が停止され、DISABLE_GRANULAR_INVENTORY_EVENT イベントが生成されて、デバイスの詳細なインベントリが無効になります。

表 *58* : イベントバーストアクションのプロパティ

プロパティ名	説明	デフォルト値
BurstThreshold	一定の期間において特定のタイプのイベントが「バースト」と見なされる数。	100 のイベント。
BurstHoldOffTimer	インベントリ同期が保留される期間。	300000 ミリ秒（5 分）
BurstCheckRetryCount	許容される再試行回数。	3 回

局所的インベントリが無効になると、特定のデバイスについてイベントバースト状態をモニターするためのシステムチェックが開始されます。このシステムチェックによって、イベントバースト状態が継続しているかどうかが確認されます。イベントバースト状態がない場合は、システムによって DISABLE_GRANULAR_INVENTORY_EVENT がクリアされた後、デバイスの完全同期が実行されます。新しい着信イベントに対しては、デバイスの局所的インベントリ処理が再開されます。

（注） デバイスの局所的インベントリを手動で有効にすると（局所的インベントリの有効化または無効化（1087 ページ）を参照）、対応する DISABLE_GRANULAR_INVENTORY_EVENT がクリアされます。

継続イベントフローコントローラ

管理対象デバイスの着信イベントの数がしきい値（contEventsCheckPeriod の contEventsThresholdCount）よりも大きい場合は、Cisco EPN Manager によって継続イベント状態と見なされます。このシナリオでは、継続イベント状態がクリアされるまで、しきい値違反となっているイベントの詳細なインベントリ同期が一定の期間（contEventsDropPeriod）保留されます。

継続イベント状態が検出されると、継続イベントフローコントローラによって、デバイスの詳細なインベントリ処理がすべて停止され、デバイスが継続状態であることを示す INVENTORY_SYNC_SUPPRESSED アラームが発生します。継続イベント状態がクリアされるまでは、特定されたすべてのイベントについて、一定間隔で機能の同期の実行が継続されます。

表 *59* : 継続イベントアクションのプロパティ

プロパティ名	説明	デフォルト値
contEventsThresholdCount	キュー内で一度に許可されるイベントの最大数。	50 のイベント

プロパティ名	説明	デフォルト値
contEventsCheckPeriod	着信イベントカウントを確認するための時間間隔（ミリ秒単位）。	300000 ミリ秒（5 分）
contEventsDropPeriod	継続イベントの場合に一定間隔で機能の同期をトリガーする時間間隔（ミリ秒単位）。	300000 ミリ秒（5 分）

局所的インベントリの有効化または無効化

局所的インベントリの有効化または無効化は、[システム設定（System Settings）] ページからグローバルレベルで行えます。[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] > > > > の順に選択し、[局所的インベントリを有効にする（Enable Granular Inventory）] チェックボックスをオンまたはオフにします。デフォルトで、この設定は有効になっています。

（注） 局所的インベントリを無効にすると、すべての管理対象デバイスの局所的インベントリ処理がすべて停止されます。

また、[ネットワークデバイス（Network Devices）] ページからデバイスレベルで局所的インベントリを有効または無効にすることもできます。デバイスの局所的インベントリを無効にするには、[ネットワークデバイス（Network Devices）] ページで目的のデバイスを選択し、[管理状態（Admin State）] > [局所的インベントリを無効にする（Disable Granular Inventory）] > を選択します。これで、選択したデバイスについてのみ、局所的インベントリが無効になり、システムにある他のデバイスの詳細なインベントリ処理には影響を与えません。デバイスの局所的インベントリを再度有効にするには、[ネットワークデバイス（Network Devices）] ページで目的のデバイスを選択し、[管理状態（Admin State）]>[局所的インベントリを有効にする（Enable Granular Inventory）] > を選択します。1 つまたは複数のデバイスを選択して、これらのアクションを適用することができます。ただし、複数のデバイスを選択する場合は、選択したデバイスのすべてが 2 つの状態のいずれかになっている必要があります。選択したデバイスの状態が互いに異なる場合、これらのオプションは有効になりません。

（注） 局所的インベントリがグローバルレベルで無効になっている場合は、デバイスレベルでの局所的インベントリ設定よりも優先します。局所的インベントリがグローバルレベルで有効になっている場合は、デバイスレベルでの局所的インベントリ設定の方が優先します。

Web GUI に表示される汎用イベントのカスタマイズ

SNMP トラップおよびsyslogによって生成される汎用イベントの説明と重大度をカスタマイズすることができます。カスタマイズした内容は、SNMP トラップ イベントの [イベント（Events）] タブに表示されます。MIB モジュールがロードされていない場合は、手動でロードし、その MIB で提供される通知をカスタマイズすることができます。

これらの汎用イベントをカスタマイズする方法については、「SNMP トラップに基づく汎用イベントのカスタマイズ （1089 ページ）」を参照してください。

汎用トラップおよび Syslog の処理の無効化および有効化

デフォルトでは、Cisco EPN Managerは受信したsyslogまたはトラップを廃棄しません。アラームおよびイベントはどのように作成および更新しますか。 （308 ページ）に記載されているように、Cisco EPN Managerは、受信したsyslogまたはトラップについてCisco EPN Managerが新規イベントを作成すべきかどうかを決定する（新規イベントを作成する場合は、アラームを作成するかどうかも決定する）イベント カタログを保持しています。Cisco EPN Managerがイベントを作成しない場合、トラップまたはsyslogは汎用イベントと見なされます。

デフォルトでは、Cisco EPN Managerにより次のことが実行されます。

- イベント一覧に汎用イベントが表示されます。
- 汎用イベントは、CISCO-EPM-NOTIFICATION-MIBを使用して正規化された後、電子メールまたはSNMP トラップ通知で転送されます。詳細については、本ガイドの「CISCO-EPM-NOTIFICATION-MIB」を参照してください。

トラップの内容に関係なく、これらのすべてのイベントにMINOR重大度が割り当てられ、アラーム カテゴリ [汎用（Generic）] に分類されます。

汎用トラップ処理を有効または無効にする

genericTrap.sh コマンドを使用して一般的なsyslogを管理します。

操作の目的：	使用するコマンド：
汎用トラップ処理をオフにする	**/opt/CSCOlumos/bin/genericTrap.sh -l**
汎用トラップ処理をオンにする	**/opt/CSCOlumos/bin/genericTrap.sh -u**

SNMP トラップに基づく汎用イベントのカスタマイズ

Cisco EPN Manager では、GUI での汎用イベントのカスタマイズ表現がサポートされています。管理対象オブジェクトは通常、SNMP トラップと通知を生成します。これらの通知には、SNMP トラップ オブジェクトの ID（SnmpTrapOID）と可変バインド オブジェクト ID（VarBindOIDs）が数値形式で含まれています。Cisco EPN Manager は、カスタマイズされた MIB モジュールを使用して、SnmpTrapOID および VarBindOID の数値をわかりやすい名前に変換し、その後 Web GUI（イベント テーブル、[デバイス 360（Device 360）] ビューなど）に汎用イベントを表示します。汎用イベントの詳細については、アラームおよびイベントはどのように作成および更新しますか。（308 ページ）を参照してください。

Cisco EPN Manager にパッケージされている SNMP MIB ファイルを使用して、各自の展開環境のテクノロジー要件に合わせて、定義されている MIB をカスタマイズできます。

次の表に、ObjectID の復号化方法と GUI での表示方法を示します。

表 *60 :* 例：*ObjectID* 表現

復号化前の OID	復号化後の OID
`snmpTrapOID = 1.3.6.1.4.1.9.10.120.0.1', Values: 1.3.6.1.4.1.9.10.119.1.1.2.1.11.7.1=1`	`mplsL3VpnVrfDown, values: mplsL3VpnVrfOperStatus.("vrf1").(1) = 1`

次の手順に従い、カスタム汎用イベントを作成します。

ステップ 1 **[モニター（Monitor）]>[モニターリング ツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]** の順に選択します。

ステップ 2 [イベント（Events）] タブをクリックします。

ステップ 3 [カスタム トラップ イベント（Custom Trap Events）] をクリックし、次に [新しい MIB のアップロード（Upload New Mibs）] をクリックします。

ステップ 4 [MIB のアップロード（Upload Mib）] ウィンドウで、[新しい MIB のアップロード（Upload New MIB）] をクリックし、MIB ファイルをアップロードします。

ステップ 5 新しい MIB ファイルをアップロードする場合は、ファイルのアップロードが完了するまで待機してから、[MIB の更新（Refresh MIBs）] をクリックします。新しく追加された MIB が [MIB] ドロップダウンリストに含まれるようになります。

ステップ 6 [OK] をクリックします。

Cisco EPN Manager は、指定されたトラップの新しいイベント タイプとアラーム条件を作成します。

障害処理エラーのトラブルシュート

導入環境で障害処理に問題が発生している場合、次の手順に従って障害ログを確認します。

ステップ 1 管理者権限を持つユーザー ID を使用して Cisco EPN Manager にログインします。

ステップ 2 **[管理（Administration）]**>**[設定（Settings）]**> **[ロギング（Logging）]** を選択し、[グローバル設定（Global Settings）] タブを選択します。

ステップ 3 [ダウンロード（Download）] をクリックしてすべてのサーバーのログファイルをダウンロードします。

ステップ 4 これらのログ ファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

console.log

ncs-x-x.log

decap.core.java.log

xmp_correlation.log

decap.processor.log

（注） [EPNMからのリセット（Reset from EPNM）] をクリックしてグローバル設定をリセットすることはできません。

次のタスク

シスコ サポート コミュニティからも援助を受けられます。サポート ケースを開く必要がある場合は、疑わしいログファイルをケースに添付します。シスコ サポート コミュニティとテクニカルアシスタンスセンター（TAC）から支援を受ける（1090ページ）を参照してください。

シスコ サポート コミュニティとテクニカル アシスタンス センター（TAC）から支援を受ける

シスコ サポート ケースの登録

Web GUI からサポート ケースを登録すると、Cisco EPN Manager ではデバイスから取得できる情報が、このケース フォームに自動的に読み込まれます。これには、デバイスの技術的な詳細、デバイスでの設定変更、および過去 24 時間以内に発生したすべてのデバイス イベントなどがあります。また、ケースに各自のファイルを添付することもできます。

始める前に

次の状況では、Web GUI でサポート ケースを登録できます。

- 管理者により、ユーザーがこの作業を実行できるように Cisco EPN Manager が設定されている。シスコサポート リクエストのデフォルトの設定 （983 ページ）を参照してください。
- Cisco EPN Manager サーバーがインターネットに直接接続しているか、またはプロキシ サーバー経由で接続している。
- Cisco.com のユーザー名とパスワードがある。

ステップ 1 次のいずれかを実行します。

- **[モニター（Monitor）] > [モニターリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** の順に選択します。アラームを 1 つクリックし、**[トラブルシュート（Troubleshoot）] > [サポート ケース（Support Case）]** を選択します。[トラブルシュート（Troubleshoot）] ボタンが表示されない場合は、ブラウザ ウィンドウを拡大します。
- [デバイス 360（Device 360）] ビューで、次の手順に従います。デバイスの IP アドレスの上にマウスを移動し、情報アイコンをクリックします。[アクション（Actions）] ドロップダウン メニューから [サポート リクエスト（Support Request）] を選択します。

ステップ 2 Cisco.com ユーザー名とパスワードを入力します。

ステップ 3 [作成（Create）] をクリックします。Cisco EPN Manager は、デバイスから取得するデータをこのフォームに読み込みます。

ステップ 4 （オプション）組織のトラブル チケット システムに対応したトラッキング番号を入力します。

ステップ 5 [次へ（Next）] をクリックして、問題の説明を入力します。

Cisco EPN Manager では、デバイスから取得したデータがフォーム読み込まれ、必要なサポート ドキュメントが自動的に生成されます。

必要に応じて、ローカル マシンからファイルをアップロードします。

ステップ 6 [サービス リクエストの作成（Create Service Request）] をクリックします。

シスコ サポート コミュニティへの参加

オンライン シスコ サポート コミュニティ内のディスカッション フォーラムにアクセスして、参加できます。Cisco.com のユーザー名とパスワードが必要です。

ステップ 1 次のいずれかを実行します。

- **[Monitor] [>] [Monitoring Tools] [>] [Alarms and Events]** に移動します。いずれかのアラームをクリックし、**Troubleshoot > Support Forum** を選択します。**[Troubleshoot]** ボタンが表示されない場合は、ブラウザ ウィンドウの幅を広げてください。

- [デバイス 360（Device 360）] ビューで、次の手順に従います。デバイスの IP アドレスの上にマウスを移動し、情報アイコンをクリックします。[アクション（Actions）] ドロップダウン メニューから、[サポート コミュニティ（Support Community）] を選択します。

ステップ 2 シスコ サポート コミュニティ フォーラムのページで、必要な情報を見つけるための検索パラメータを入力します。

第 27 章

監査およびログ

ユーザーによって行われる変更の監査（変更の監査）

Cisco EPN Manager では、以下の方法で、変更の監査データの管理がサポートされています。

変更監査通知の有効化および syslog レシーバの設定

必要に応じて、システムに変更が加えられると Cisco EPN Manager が変更監査通知を送信するように設定できます。これらの変更には、デバイス インベントリと設定の変更、設定テンプレートおよびモニターリング テンプレートの操作、ユーザー操作（ログイン、ログアウト、ユーザー アカウントの変更など）が含まれます。

次の動作を行うように Cisco EPN Manager を設定できます。

- 変更監査通知として変更を Java メッセージ サーバー（JMS）に転送する
- これらのメッセージを特定の syslog レシーバに送信する

syslog レシーバを設定しても syslog を受信しない場合は、宛先 syslog レシーバでのウイルス対策またはファイアウォールの設定を変更して、syslog メッセージの受信を許可するようにしなければならない可能性があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[メールと通知（Mail and Notification）] > [監査通知の変更（Change Audit Notification）]** を選択します。

ステップ 2 [監査の変更通知の有効化（Enable Change Audit Notification）] チェックボックスをオンにして通知を有効にします。

ステップ 3 メッセージを特定の syslog レシーバに送信するには、次の手順に従います。

a) [追加（Add）] ボタン（+）をクリックして、Syslog レシーバを指定します。

b) [syslogレシーバ（Syslog Receiver）] 領域で、syslog レシーバの IP アドレス、プロトコル、およびポート番号を入力します。

さらに追加の syslog レシーバを指定するには、必要に応じてこの手順を繰り返します。

ステップ 4 [保存（Save）] をクリックします。

（注） レコードをセキュアな tls ログに反映するために Cisco EPN Manager サーバーの再起動をお勧めします。

監査の変更の詳細表示

ステップ 1 Cisco EPN Manager に管理者としてログインします。

ステップ 2 **[モニター（Monitor）] > [ツール（Tools）] > [変更監査ダッシュボード（Change Audit Dashboard）]** を選択します。

[変更監査ダッシュボード（Change Audit Dashboard）] に次の情報が表示されます。

- 監査データの変更元（Change audit data from）：
  - デバイス管理
  - ユーザー管理
  - 設定テンプレートの管理（Configuration template management）
  - デバイス コミュニティとクレデンシャルの変更
  - デバイスのインベントリ変更（Inventory changes of devices）

[監査レポートの変更（Change Audit report）] と [監査の変更（Change Audit）] ダッシュボードには、ログインしている仮想ドメインに関係なく詳細が表示されます。

[変更監査ダッシュボード（Change Audit Dashboard）] 画面には、IP アドレス、監査の説明、ユーザー名、監査名、クライアントの IP アドレスなどの詳細とは別に、デバイス名も表示されます。[IP アドレス（IP Address）] フィールドの横にある [i] アイコンをクリックしてデバイス 360 の詳細を表示します。

（注） ルートユーザーとしてログインしている場合は、すべての監査変更を表示できます。非ルートユーザーとしてログインしている場合は、自分が実行した監査変更のみを表示できます。

Cisco EPN Manager は、[変更監査ダッシュボード（Change Audit Dashboard）] のすべての詳細を `/opt/CSCOlumos/logs/audit.log` に記録します。詳細については、監査ログ （1100 ページ）を参照してください。

GUI から実行されたアクションを監査する（システムの監査）

（注） Cisco EPN Manager は、すべての監査変更通知を XML 形式でトピック **ChangeAudit.All** に送信します。通知を受信するためには、**ChangeAudit.All** に登録する必要があります。

[システムの監査（System Audit）] ウィンドウに、ユーザーがアクセスしたすべての Cisco EPN Manager GUI ページが一覧表示されます。[システムの監査（System Audit）] を表示するには、**[管理（Administration）] > [設定（Settings）] > [システムの監査（System Audit）]** を選択します。

次の表に、クイック フィルタを使用して [システムの監査（System Audit）] ページで見つかる情報の一部を示します。クイック フィルタを有効にするには、[表示（Show）] ドロップダウン リストから [クイック フィルタ（Quick Filter）] を選択します。

実行されたアクションの検索対象：	次の手順を実行します。
特定のユーザー	[ユーザー名（Username）] クイック フィルタ フィールドにユーザー名を入力します。
ユーザー グループ内のすべてのユーザー	[ユーザー グループ（User Group）] クイック フィルタ フィールドにグループ名を入力します
特定の仮想ドメイン内のデバイス	[アクティブ仮想ドメイン（Active Virtual Domain）] クイック フィルタ フィールドに仮想ドメイン名を入力します。
Web GUI ルート ユーザー	[表示（Show）] ドロップダウン リストから、[ルート ユーザー ログ（Root User Logs）] を選択します。
特定のデバイス	[IP アドレス（IP Address）] クイック フィルタ フィールドに IP アドレスを入力します。
特定の日付	[監査時間（Audit Time）] クイック フィルタ フィールドに日付を入力します（*yyyy–mmm–dd* の形式）。

OS ログをリモートシステムに転送する

EPNM によるリモートシステムへの OS CLI ログの転送や、ログレベルの設定を有効にするには、コンフィギュレーション モードで下記の logging コマンドを使用します。

（注） ログを転送するリモートシステムは 1 つだけ設定できます。

logging {ip-address | hostname} {loglevel level}

それぞれの説明は次のとおりです。

構文	説明
ip-address	ログを転送するリモートシステムの IP アドレス。最大 32 文字の英数字。
hostname	ログを転送するリモートシステムのホスト名。最大 32 文字の英数字。
loglevel	logging コマンドのログ レベルを設定するコマンド。
level	ログ メッセージを設定する希望のプライオリティ レベルの番号。プライオリティ レベルは以下のとおりです（キーワードの番号を入力）。 • 0 - emerg—Emergencies：システム使用不可 • 1 - alert—Alerts：ただちに処置が必要 • 2 - crit—Critical：重大な状態 • 3 - err—Error：エラー状態 • 4 - warn—Warning：警告状態 • 5 - notif—Notifications：正常ではあるが注意を要する状態 • 6 - inform：（デフォルト）Informational（情報提供）メッセージ • 7 - debug：デバッグメッセージ

この機能をディセーブルにするには、このコマンドの no 形式を使用します。

このコマンドには **IP address** または **hostname** または **loglevel** キーワードが必要です。これらの引数を複数入力すると、エラーが発生します。

例 1：

```
ncs/admin(config)# logging 209.165.200.225
ncs/admin(config)#
```

例 2：

```
ncs/admin(config)# logging loglevel 0
ncs/admin(config)#
```

システム ログ

Cisco EPN Manager は、**[管理（Administration）]** > **[設定（Settings）]** > **[ロギング（Logging）]** を選択して制御される 3 つのクラスのログを提供しています。

ログの種類	説明	次を参照してください。
一般	システムでのアクションに関する情報を取得します。	一般的なシステム ログを表示して管理する （1097 ページ）
SNMP	管理対象デバイスとの対話を取得します。	SNMP トレースの有効化および SNMP ログ設定（レベル、サイズ）の調整 （1100 ページ）
Syslog	Cisco EPN Manager 監査ログを（syslog として）他の受信者に転送します。	Syslog としてのシステム監査ログの転送 （1099 ページ）

一般的なシステム ログを表示して管理する

システム ログは、ローカル サーバーにダウンロード後に表示することができます。

特定のジョブのログを表示する

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** を選択します。

ステップ 2 [ジョブ（Jobs）] ペインからジョブタイプを選択し、[ジョブ（Jobs）] ウィンドウからジョブインスタンス リンクをクリックします。

ステップ 3 [ジョブインスタンス（Job instance）] ウィンドウの左上にある [ログファイル（Log file）] を見つけ、[ダウンロード（Download）] をクリックします。

（注） 設定アーカイブソフトウェア、設定ロールバック、設定上書き、設定展開のジョブタイプのログのみをダウンロードできます。

ステップ 4 必要に応じてファイルを開くか保存します。

一般的なログ ファイルの設定とデフォルト サイズの調整

デフォルトでは、Cisco EPN Manager は、すべての管理対象デバイスで生成されたすべてのエラー、情報、およびトレースメッセージをログに記録します。また、受信したすべての SNMP メッセージと Syslog もログに記録します。これらの設定を調整して、デバッグ目的のログ レベルを変更することができます。

操作の目的：	**[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** での操作：
ログのサイズ、保存するログの数、ファイル圧縮のオプションを変更する	ログ ファイルの設定を調整します。 （注） システムへの影響を避けるため、これらの設定は慎重に変更してください。 Log4j MaxBackupIndex ごとに、メインファイルが 1 つ存在し、バックアップファイルのセット数が伴います。たとえば、ログファイルの数が 3 に設定されている場合は、1 つのメインファイル（.log）と 3 つのバックアップファイル（.log.1、.log.2、.log.3）が存在します。 [ファイルの数（Number of files）] を以前に設定した値よりも小さい値に変更した場合、ログファイルの設定は新しく生成されたファイルにのみ適用されます。たとえば、設定済みの値が 5 の場合、ここで 2 に変更すると、設定は .log ファイル .log.1 および .log.2 にのみ適用されます。files.log.3、.log.4、および .log.5 に変更はありません。 **[圧縮（Zip）（Compression (Zip)）]** オプションを選択すると、ログファイルが圧縮され、プロセスの **`./logs/backup/[logging_module]`** フォルダにアーカイブされます。圧縮されたログファイルの保持は、次の基準に従います。 • [ストレージ（MB）（Storage (MB)）]：フォルダの最大サイズ（MB） • [日数（Number of Days）]：ログファイルの最大経過時間 いずれかの条件が満たされると、消去が開始されます。 必要に応じて、[外部ロケーションへのバックアップ（Backup to external location）] が有効になっている場合、クリーンアップ対象としてマークされたログファイルは、削除前に指定された外部リポジトリにコピーされます。

操作の目的：	**[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）] での操作：**
特定のモジュールのログ レベルを変更する	[一般的なログ設定（General Log Settings）] で、ファイルと必要なレベルを選択して [**Save**] をクリックします。たとえば、[メッセージレベル（Message Level）] ドロップダウンリストから、現在のログ レベルとして次のいずれかを選択します。 • [エラー（Error）]：システム上のエラー ログをキャプチャします。 • [情報（Information）]：システム上の情報ログをキャプチャします。 • [トレース（Trace）]：詳細情報をログに記録するために、システムで管理対象デバイスの問題を再現します。 • [デバッグ（Debug）]：システムのデバッグログをキャプチャします。 Cisco EPN Manager を再起動すると、ログレベルが [Error] にリセットされます。
トラブルシューティングの目的でログ ファイルをダウンロードする	[グローバル設定（Global Settings）] タブで **Download** をクリックします。

Syslog としてのシステム監査ログの転送

始める前に

Syslog としてシステム監査ログを転送するには、ユーザーが監査の変更通知を有効化して syslog レシーバを設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** の順に選択してから、**[Syslog]** タブを選択し、**[Syslog ロギングオプション（Syslog Logging Options）]** を表示します。

ステップ 2 システム ログの収集および処理を有効にするために、[Syslog の有効化（Enable Syslog）] チェックボックスをオンにします。

ステップ 3 [Syslog ホスト（Syslog Host）] フィールドに、メッセージ送信先の宛先サーバーの IP アドレスを入力します。

ステップ 4 [Syslog ファシリティ（Syslog Facility）] ドロップダウン リストから、8 つのローカル用途のファシリティのうち、Syslog メッセージを送信するために使用するファシリティを選択します。このローカル用途のファシリティは予約されておらず、一般的な用途で使用可能です。

ステップ 5 [保存（Save）] をクリックします。

（注） 管理 CLI を使用してリモートサーバーへのシステムログ転送を有効にすると、ログは ade.log ファイルに登録されません。

SNMP トレースの有効化および SNMP ログ設定（レベル、サイズ）の調整

SNMP トレースを有効にし、SNMP によって送受信されるパケットに関する詳細情報にアクセスします。これは、トラップのドロップ時など、トラブルシューティングの際に必要になることがあります。

次の変更を行うには、**[管理（Administration）]** > **[設定（Settings）]** > **[ロギング（Logging）]** を選択してから、**[SNMP ログ（SNMP Log）]** タブを選択します。

目的	次の手順を実行します。
特定のデバイスでの SNMP トレースの有効化	[SNMP ログ設定（SNMP Log Settings）] 領域で、次のようにします。 1. [SNMP トレースの有効化（Enable SNMP Trace）] チェックボックスと [値の表示（Display Values）] チェックボックスをオンにします。 2. トレースするデバイスの IP アドレスまたは DNS アドレス、あるいはその両方を入力し、[保存（Save）] をクリックします。
ログのサイズと保存されるログ番号の変更	[SNMP ログ ファイル設定（SNMP Log File Settings）] 領域で、次のようにします。 （注） これらの設定を変更するときは、（非常に多くのデータを保存するなどして）システム パフォーマンスに影響を与えないように注意してください。 1. ファイルの最大数とファイル サイズを調整します。 2. Cisco EPN Manager を再起動して、変更内容を有効にします。Cisco EPN Manager の停止と再起動 （973 ページ） を参照してください。

監査ログ

Cisco EPN Manager は、`audit.log` の **[モニター（Monitor）]** > **[ツール（Tools）]** > **[監査ダッシュボードの変更（Change Audit Dashboard）]** の下に表示される情報をログに記録します。デフォルトでは、ロギングはイネーブルです。この情報は、メッセージレベルかログモジュールの変更に関係なく記録されます。

`audit.log` を表示するには、管理者 CLI で `/opt/CSCOlumos/logs/audit.log` に移動します（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ） を参照）。

デバイス固有のロギング

Cisco EPN Manager では、特定のデバイスのデバッグモードで XDE およびインベントリログを保存できます。SSH CLI からロギングを有効または無効にすることができます。（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ） を参照）。

デバイス固有のロギングの有効化

重要 XDE またはインベントリログのデバイス固有のロギングを有効にする前に、次のコマンドを実行して、グローバルログレベルが INFO に設定されていることを確認します。

```
/opt/CSCOlumos/bin/setLogLevel.sh logName INFO
```

logName：必要に応じて xde または inventory と入力します。

デバイス固有のロギングを有効にするには、次のコマンドを実行します。

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh logName DEBUG deviceIP
```

ここで、

- *logName*：必要に応じて xde または inventory と入力します。インベントリログのデバイス固有のロギングを有効にすると、ifm_inventory ログのロギングも有効になります。
- *deviceIP*：ロギングをイネーブルにするデバイスの IP アドレスを指定します。同じコマンドで複数の IP アドレスをカンマで区切って指定できます。

指定されたデバイスに対してのみ、デバッグモードでインベントリまたは XDE のログを保存します。他のデバイスの場合、情報ログのみが保存されます。同期中に生成されるログファイルは *xde.log.**、*inventory.log.**、および *ifm_inventory.log.** です。

Cisco EPN Manager は、このコマンドを実行するたびに、ユーザーが指定した IP アドレスを使用して、以前に指定された IP アドレスを上書きします。

例

インベントリログの場合：

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh inventory DEBUG 1.2.3.4,5.6.7.8
```

XDE ログの場合：

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh xde DEBUG 1.2.3.4,5.6.7.8
```

デバイス固有のロギングが有効になっているデバイスのリストの表示

デバイス固有のロギングが有効になっているデバイスのリストを表示するには、次のコマンドを実行します。

```
/opt/CSCOlumos/bin/listDeviceLevelDebug.sh logName
```

logName：必要に応じて xde または inventory と入力します。

例

```
/opt/CSCOlumos/bin/listDeviceLevelDebug.sh inventory
```

デバイス固有のロギングの無効化

指定したログのデバイス固有のロギングを無効にするには、ログレベルを INFO に設定します。これにより、すべてのデバイスのデバイス固有のロギングが無効になります。

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh logName INFO
```

logName：必要に応じて xde または inventory と入力します。

（注） 特定のデバイスに対してロギングを無効にすることはできません。

例

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh inventory INFO
```

インベントリ検出プロセスのログ

inventory-discovery-process のログは、 `/opt/CSCOlumos/logs/inventory-discovery-process` で確認できます。

inventory-discovery-process のログレベルを変更するには、管理者 CLI で次のコマンドを入力します（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

- ログレベルを INFO に変更するには、次のコマンドを実行します。

  ```
  /opt/CSCOlumos/bin/setLogLevel.sh logName INFO inventory-discovery-process
  ```

- ログレベルを DEBUG に変更するには、次のコマンドを実行します。

  ```
  /opt/CSCOlumos/bin/setLogLevel.sh logName DEBUG inventory-discovery-process
  ```

logName：必要に応じて XDE または Inventory と入力します。

外部ロケーションへのシステム ログの同期

ncs（Cisco EPN Manger ログ）および os ログをローカルまたは NFS ベースのリポジトリに同期するように設定できます。

ログをリポジトリに同期するには、次の手順を実行します。

始める前に

ログを同期するローカルまたは NFS ベースのリポジトリを作成します。この方法の詳細については、リポジトリのセットアップと管理 （935 ページ）を参照してください。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開きます。「CLI 経由の接続 （953 ページ）」を参照してください。

ステップ 2 コンフィギュレーション モードで次のコマンドを入力してシステムログを同期します。

- ncs ログを同期する場合：

```
logging sync-logs ncs repository repository-name
```

- os ログを同期する場合：

```
logging sync-logs os repository repository-name
```

repository-name は自身で設定したリポジトリです。

（注） 同期を無効にするには、代わりに configure terminal モードで次のコマンドを入力します。

- ncs ログの同期を無効にする場合：

```
no logging sync-logs ncs repository repository-name
```

- os ログの同期を無効にする場合：

```
no logging sync-logs os repository repository-name
```

ステップ 3 コンフィギュレーション モードを終了します。

```
exit
```

例

例 1

```
(config)# logging sync-logs ncs repository myrepository
(config)# logging sync-logs os repository myrepository
config# exit
```

例 2

```
(config)# no logging sync-logs ncs repository myrepository
(config)# no logging sync-logs os repository myrepository
config# exit
```

セキュリティ ログ

Cisco EPN Manager では、過去のアクティブな Web GUI または CLI セッションで、ルート ユーザーと admin および super-user ユーザー グループのメンバーが実行したセキュリティ関連アクションのログが保持されます。

ログに記録される情報には、イベントの説明、ユーザーがタスクを実行したクライアントの IP アドレス、およびタスクが実行された時刻が含まれます。次のイベントがログに記録されます。

- ユーザーのログイン
- ユーザーのログアウト
- ユーザーの作成
- ユーザーの追加
- ユーザーの削除
- ユーザーのロック
- ユーザーのロック解除
- Linux シェルの入力
- ユーザーの変更（メール、パスワード）

このログの詳細を表示するには、次のコマンドを入力します。このコマンドを使用するには、管理 CLI ユーザーとしてログインする必要があります。詳細については、Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

```
show logging security
```

Cisco EPN Manager は、セキュリティ関連アクションのログを常にローカルに保持します。

CLI からのイベント エントリにはプレフィックス「SYSTEM-CLI:」、Web インターフェイスからのエントリにはプレフィックス「SYSTEM-WEB:」が付いています。各イベント エントリの構造は JSON 形式に基づいており、JSON は有効です。

イベント CLI	• SYSTEM-CLI:SSH:LOGIN:FAILED:WRONG_PASSWORD • SYSTEM-CLI:SSH:LOGIN:FAILED:MAXIMUM_ATTEMPTS_REACHED • SYSTEM-CLI:SSH:LOGIN:SUCCESSFUL • SYSTEM-CLI:SSH:LOGOUT:SUCCESSFUL • SYSTEM-CLI:CONSOLE:LOGIN:WRONG_PASSWORD • SYSTEM-CLI:CONSOLE:LOGIN:SUCCESSFUL • SYSTEM-CLI:CONSOLE:LOGOUT:SUCCESSFUL • SYSTEM-CLI:USER:ADD

	• SYSTEM-CLI:USER:DELETE • SYSTEM-CLI:USER:GROUP • SYSTEM-CLI:USER:PASSWORD • SYSTEM-CLI:USER:PASSWORD:POLICY • SYSTEM-CLI:USER:ROLE • SYSTEM-CLI:USER:STATE:LOCK • SYSTEM-CLI:USER:STATE:UNLOCK • SYSTEM-CLI:USER:MAIL • SYSTEM-CLI:USER:OS:SHELL:ENTERED • SYSTEM-CLI:OS:SHELL:ENABLED • SYSTEM-CLI:OS:SHELL:DISABLED
イベント UI	• SYSTEM-WEB:UI:NCS:BODGE:LOGIN:SUCCESSFUL • SYSTEM-WEB:UI:LOGOUT • SYSTEM-WEB:UI:LOGIN:SUCCESSFUL • SYSTEM-WEB:UI:LOGIN:AUTHENTICATION_FAILED • SYSTEM-WEB:UI:USER:DELETE • SYSTEM-WEB:UI:USER:ADD • SYSTEM-WEB:UI:USER:STATE:UNLOCK • SYSTEM-WEB:UI:USER:STATE:LOCK • SYSTEM-WEB:UI:USER:UPDATE • SYSTEM-WEB:HM:LOGIN:AUTHENTICATION_FAILED

外部ロケーションへのセキュリティ ログの送信

リモート ロギングがサポートされているため、セキュリティ関連のイベントをリモート syslog サーバーに転送するように設定できます。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開き、configure terminal モードを開始します。「CLI 経由の接続 （953 ページ）」を参照してください。

ステップ 2 次のコマンドを入力します。

```
logging security hostname[:port]
```

hostname はリモート ロギング ホスト サーバーの名前または IP アドレスです。

（注） このコマンドは、ポートが指定されていない場合、デフォルトでUDPポート514にログを送信します。

ステップ3 コンフィギュレーション モードを終了します。

```
exit
```

例

```
/admin(config)# logging security a.b.c.d
/admin(config)# exit
```

セキュリティイベントログ

Cisco EPN Manager は、次のイベントのログを security_events.log ファイルに保持します。

- 暗号プロトコルを介して作成または破棄されたセッション
- セキュリティ攻撃と考えられるもの

デフォルトでは、セキュリティ攻撃に関連するイベントはログに記録されます。暗号化セッションに関連する情報のロギングを有効にするには、ログレベルを **Info** に設定する必要があります。これを行うには、サーバーパスの /opt/CSCOlumos/bin の管理 CLI で次のコマンドを実行します。

```
./setLogLevel.sh SecurityEvents.crypto INFO
```

Event type	イベント	記録される情報
セキュリティ攻撃に関連するイベント	SQL インジェクションと LDAP インジェクション	入力検証エラー（データのソースには無関係）。ログに記録されるデータには、データが無効である理由が記載されています。
暗号化セッションに関連する情報	次のプロトコルを介して作成および破棄されたセッション。 • raw • SSH2、Telnet • NETCONF • TL1	• 通知の種類（Notification type） • ターゲットデバイス • 接続ポート • [ユーザー名（Username）] • 接続タイプ • セッションの詳細を

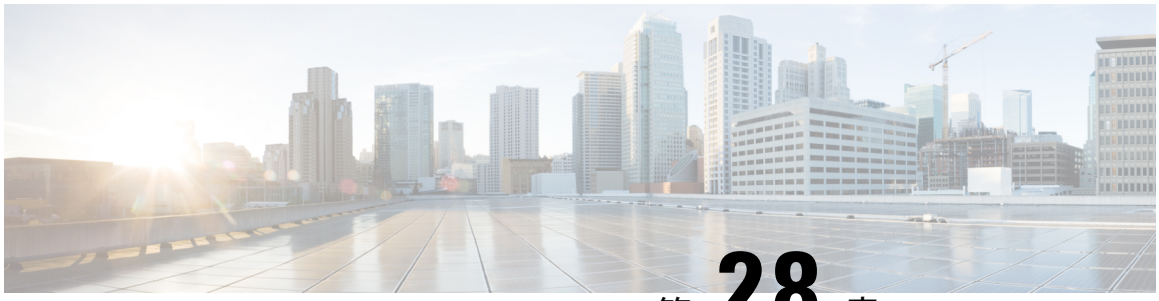
管理CLIで次のコマンドを入力して、ログの内容を表示できます。詳細については、Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照してください。

```
less /opt/CSCOlumos/logs/security_events.log
```

```
less /opt/CSCOlumos/logs/security_events.log.x
```

ここで、

- *x* は 1 以上の数になります（ローリング イベント ログファイルであるため）。



第 28 章

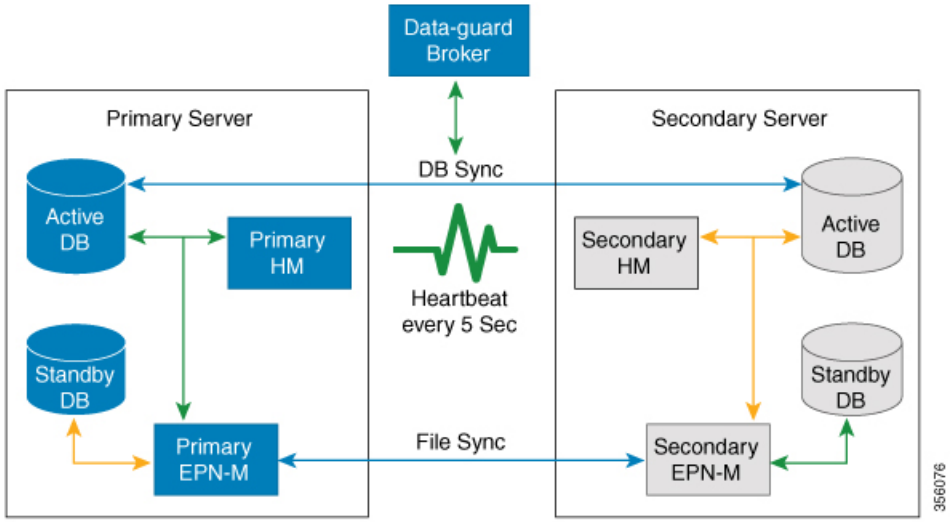
ハイ アベイラビリティの設定と管理

ハイ アベイラビリティの仕組み

Cisco EPN Manager ハイ アベイラビリティ（HA）フレームワークでは、障害が発生してもシステム動作が継続されます。HA では、リンクされて同期された Cisco EPN Manager サーバーのペアを使用して、いずれかのサーバーで発生する可能性のあるアプリケーション障害またはハードウェア障害による影響を最小限に、あるいは完全に排除します。サーバーの障害は、以下の 1 つ以上の領域での問題が原因で発生する可能性があります。

- アプリケーション プロセス：サーバー、TFTP、FTP などのプロセスの失敗。CLI **ncs status** コマンドを使用して、これらのプロセスのステータスを確認できます。
- データベース サーバー：データベース関連のプロセスの失敗（データベース サーバーは Cisco EPN Manager でサービスとして実行されます）。
- ネットワーク：ネットワーク アクセスまたは到達可能性に関連する問題。
- システム：サーバーの物理ハードウェアまたはオペレーティング システムに関連する問題。
- 仮想マシン（HA が VM 環境で稼動している場合）：プライマリ サーバーとセカンダリ サーバーがインストールされている VM 環境に関する問題。

次の図は、HA セットアップの主なコンポーネントとプロセス フローを示しています。



HA展開は、プライマリ サーバーとセカンダリ サーバーで構成され、両方のサーバー上にヘルス モニター（HM）インスタンス（アプリケーション プロセスとして実行）が存在します。プライマリ サーバーに障害が発生（自動的に発生、または手動で停止したために発生）すると、プライマリ サーバーへのアクセスが復元されるまでの間はセカンダリ サーバーがネットワークの管理を引き継ぎます。展開で自動フェールオーバーを設定すると、セカンダリ サーバーはフェールオーバー後 2 ～ 3 分以内にアクティブ ロールを引き継ぎます。この HA は、アクティブ/パッシブまたはコールド スタンバイの動作モデルに基づいています。クラスタ化されたシステムではないため、プライマリ サーバーに障害が発生した場合、セッションはセカンダリ サーバーに保持されません。

プライマリ サーバーの問題が解決してサーバーが実行状態になっても、アクティブなセカンダリ サーバーとのデータの同期を開始する間はスタンバイ モードのままになります。プライマリ サーバーが再び使用可能になった時点で、フェールバック操作を開始できます。フェールバックがトリガーされると、プライマリ サーバーがアクティブ ロールを再度引き継ぎます。このようなプライマリ サーバーとセカンダリ サーバー間でのロールの切り替えは、2 ～ 3 分以内に実行されます。

HA 設定によってプライマリ サーバーでの変更が確認されると、変更内容がセカンダリ サーバーと同期されます。これらの変更には、次の 2 種類があります。

- ファイルの変更。HTTPS プロトコルを使用して同期されます。対象となる項目には、レポート設定、設定テンプレート、TFTP ルート ディレクトリ、管理設定、ライセンス ファイル、キー ストアなどがあります。ファイルの同期は、以下のいずれかで行われます。
  - 頻繁に更新されないファイル（ライセンス ファイルなど）の同期は、一括で行われます。これらのファイルは、500 秒間隔で同期されます。
  - 頻繁に更新されるファイルの同期は、ほぼリアルタイムで行われます。これらのファイルは、11 秒間隔で同期されます。

- データベースの変更（設定、パフォーマンス、およびモニターリングデータに関連する更新など）。Oracle Recovery Manager（RMAN）が最初のスタンバイ データベースを作成し、変更が発生すると、Oracle Active Data Guard がデータベースを同期します。

プライマリ HA サーバーとセカンダリ HA サーバーは、次のメッセージを交換して 2 つのサーバー間の同期を維持します。

- データベース同期：プライマリ サーバーとセカンダリ サーバー上のデータベースが稼働および同期するために必要なすべての情報が含まれます。
- ファイル同期：頻繁に更新されるコンフィギュレーション ファイルが含まれます。これらのファイルは 11 秒間隔で同期され、他の頻繁に更新されないコンフィギュレーション ファイルは 500 秒間隔で同期されます

（注） プライマリで手動で更新されたコンフィギュレーション ファイルは、セカンダリに同期されません。プライマリでコンフィギュレーション ファイルを手動で更新する場合は、セカンダリ上のファイルも更新する必要があります。

- プロセス同期：アプリケーションおよびデータベースに関連するプロセスの実行が継続されるようにします。これらのメッセージは、ハートビート カテゴリに分類されます。
- ヘルス モニター同期：これらのメッセージは、ネットワーク、システム、およびヘルス モニターの障害状態の有無を確認します。

プライマリサーバーとセカンダリサーバーについて

どの EPN Manager 高可用性（HA）実装でも、プライマリサーバーのある特定のインスタンスに対して専用のセカンダリサーバーが 1 台のみ必要です。

通常、HA サーバーごとに独自の IP アドレスまたはホスト名が設定されています。同一サブネット上に配置されているサーバーは、仮想 IP を使用して同じ IP を共有できます。これにより、デバイスの設定が容易になります。

HA 導入を設定するには、ネットワーク インターフェイス eth0 または NIC チーミングインターフェイスを使用できます。HA 導入に NIC チーミングインターフェイスを使用する場合は、「ノースバウンドインターフェイス」として指定する必要があります。詳細については、「HA を使用した NIC チーミング （1122 ページ）」を参照してください。

（注） NIC チーミングインターフェイスで仮想 IP を設定すると機能する場合があります。ただし、このタイプの設定は公式には認定されていません。

HA をセットアップした後は、HA サーバーの IP アドレスやホスト名を変更しないください。変更すると、HA のセットアップが失われます。

詳細については、サーバーの IP アドレスまたはホスト名のリセット（1155 ページ）を参照してください。

（注）
- HA 構成サーバーの場合、EPNM タイトルバーには、接続しているサーバーのタイプ、つまり、プライマリサーバーに接続しているかセカンダリサーバーに接続しているかが表示されます。
- プライマリサーバーがアクティブで、セカンダリサーバーが設定された保持時間よりも長い期間ダウンしている場合、HA 設定は削除されます。デフォルトでは、設定された保持時間は 6 時間です。

HA の導入計画

HA 機能は、以下の導入モデルをサポートしています。

- **ローカル**：HA サーバーの両方を同じサブネットに配置します（サーバーにレイヤ 2 近接性を与えます）。通常は、両方のサーバーが同じデータ センター内に配置されます。
- **キャンパス**：HA サーバーのそれぞれを、LAN で接続された異なるサブネットに配置します。通常、これらのサーバーは同じ 1 つのキャンパスに導入されますが、キャンパス内で配置される場所は異なります。
- **リモート**：HA サーバーのそれぞれを、WAN で接続された異なるリモート サブネットに配置します。各サーバーが、異なる施設に配置されます。これらの施設は、国や大陸間にまたがり、地理的に分散されています。

以降の項で、各モデルの利点および欠点と、すべての導入モデルに影響する基本的な制約事項について説明します。

HA は、サポートされているいずれの導入モデルでも機能します。主な制約事項は、HA のパフォーマンスと信頼性に関して存在し、これらは帯域幅と遅延の基準によって異なります（「HA のネットワーク スループットに関する制限事項」参照）。これらのパラメータを正常に管理できる限り、使用可能な導入モデルのどれを選んで実装するかは、（コスト、企業の規模、地理、コンプライアンス標準などのビジネスパラメータに基づく）ビジネス上の意思決定です。

HA のネットワーク スループットに関する制限事項

Cisco EPN Manager の HA パフォーマンスは、常に以下の制限要因の影響を受けます。

- すべての操作を処理するために Cisco EPN Manager で利用できる正味の帯域幅。これらの操作には、HA 設定、データベース同期、ファイル同期、フェールバックのトリガーが含まれます（ただし、これらに限定されません）。

- プライマリ サーバーとセカンダリ サーバー間のリンク全体における正味のネットワーク遅延。この2台のサーバーの物理的な近接性に関わらず、サーバー間のリンクで発生する遅延が大きい場合、Cisco EPN Manager によるプライマリ サーバーとセカンダリ サーバー間のセッション維持状態に影響が及ぶ可能性があります。
- プライマリ サーバーとセカンダリ サーバーを接続するネットワークが提供できる正味のスループット。正味のスループットは正味の帯域幅と遅延によって異なり、これら2つの要因の関数と見なすことができます。

モデルによって問題の大きさが異なりますが、これらの制限は、少なくとも何らかのレベルであらゆる導入モデルに当てはまります。たとえば、リモート導入モデルは、地理的な分散が大きいため、帯域幅と遅延の両方で問題が発生しがちです。一方、ローカルモデルとキャンパスモデルの場合も、正しく構成されていなければ、帯域幅の問題が発生する可能性が高くなります。これは、低帯域幅、高遅延、高ネットワーク使用率によって制限を受ける可能性があるためです。

スループットの問題がフェールバックやフェールオーバーに影響することはほとんどありません。2 つの HA サーバーがほとんど常に通信して、データベースの変更内容が即座に複製されるためです。ほとんどのフェールオーバーおよびフェールバックは、約 2 ～ 3 分を要します。

この原則の最大の例外は、データベースのフル コピー動作における遅延です。この種類のアクションは、プライマリ サーバーがデータ保持期間を超えてダウンした後、これを再度稼働させる場合にトリガーされます。Express、Express-Plus、Standard の各構成サーバーのデータ保持期間は 6 時間で、Professional および Gen 2 アプライアンス サーバーでは 12 時間です。

Cisco EPN Manager はセカンダリ サーバーからプライマリ サーバーへのデータベースのフル コピー動作をトリガーします。この期間中のフェールバックはできませんが、[ヘルス モニター（Health Monitor）] ページには、データベースのコピー進行中に発生したすべてのイベントが表示されます。コピーが完了するとすぐに、プライマリ サーバーが「プライマリ同期中（Primary Synching）」状態に移行し、フェールバックのトリガーが可能になります。データベースのフル コピーが行われている間は、プライマリ サーバーの再起動やネットワーク接続切断を行わないでください。

データベースのフル コピー動作中の正味スループットの変動は、データベースのサイズやその他の要因とは無関係に、データベースのフル コピー動作が 1 時間未満で正常に完了するケースと、まったく完了できないケースという違いを生じるぐらいの意味を持ちます。次のことを推奨します。

- ネットワーク スループット：最小 500 Mbps（メガビット毎秒）。可能であればこれ以上を推奨。
- ネットワーク遅延：最大 100 ミリ秒。可能であれば 70 ミリ秒を推奨。

パフォーマンスが低いとシステムの安定性が低下し、ハイアベイラビリティのシナリオ（主に登録とフェールバック）を完了できなくなる可能性があります。

ローカル モデルの使用

ローカル導入モデルの主要なメリットは、仮想 IP アドレスをシステムの単一管理ドレスとして使用することが許可される点です。ユーザーはこの仮想 IP アドレスを使用して Cisco EPN Manager に接続でき、デバイスでは SNMP トラップおよびその他の通知の宛先としてこの仮想 IP アドレスを使用できます。

仮想 IP アドレスを割り当てる際の唯一の制約は、仮想 IP アドレスが、プライマリ サーバーの IP アドレスおよびセカンダリ サーバーの IP アドレスと同じサブネット上のアドレスでなければならない点です。例：プライマリ サーバーとセカンダリ サーバーに対し、1 つのサブネット内の次の IP アドレスが割り当てられている場合、この両方のサーバーの仮想 IP アドレスは次のように割り当てることができます。

- サブネット マスク：255.255.255.224 (/27)
- プライマリ サーバーの IP アドレス：10.10.101.2
- セカンダリ サーバーの IP アドレス：10.10.101.3
- 仮想 IP アドレス：10.10.101.[4-30]（例：10.10.101.4）仮想 IP アドレスは、特定のサブネットマスクで有効かつ未使用のアドレス範囲内の任意のアドレスになることに注意してください。

この主な利点に加え、ローカル モデルには以下の利点もあります。

- 通常、高帯域幅と低遅延を実現します。
- 管理が簡素化されます。
- syslog および SNMP 通知を転送するようにデバイスを設定するのが、大幅に簡単になります。

ローカル モデルには、以下の欠点があります。

- 同じデータ センター内に配置されることから、停電や自然災害など、サイト全体の障害の危険にさらされます。
- 破壊的なサイト障害の危険が高くなることから、ビジネス継続性の計画が複雑になります。また、損害保険のコストも高くなる可能性があります。

キャンパス モデルの使用

キャンパス モデルでは、HA を導入する組織が、同じ都道府県の同じ市区町村内の 1 つ以上のロケーションを拠点にしていて、これらの複数ロケーションによって「キャンパス」を形成していることが前提となります。このモデルには、以下の利点があります。

- 通常、ローカル モデルに匹敵するか、それ以上の帯域幅と遅延を提供します。
- リモート モデルより簡単に管理できます。

キャンパス モデルには、以下の欠点があります。

- ローカル モデルより、管理が複雑になります。
- 仮想 IP アドレスをシステムの単一管理アドレスとして使用することを許可しないでください。このため、多くのデバイス設定が必要となります（仮想 IP アドレッシングを使用できない場合の対処 （1119 ページ）を参照）。
- ローカルモデルと比べると、帯域幅が小さくなり、遅延が大きくなる可能性があります。これは HA の信頼性に影響を与える可能性があり、是正するには管理者の介入が必要になる場合もあります（「HA のネットワーク スループットに関する制限事項（1112 ページ）」を参照）。
- 同じサイトに配置されてはいませんが、それでも都道府県全体、または市区町村全体の災害の危険にさらされます。そのため、ビジネス継続性の計画が複雑になり、災害復旧のコストが高くなる可能性があります。

リモート モデルの使用

リモート モデルでは、導入する組織に複数のサイトまたはキャンパスがあること、そしてこれらのロケーション間では、地理的な境界を超えて WAN リンクで通信することが前提となります。このモデルには、以下の利点があります。

- 自然災害による影響を受ける可能性が最小限になります。ビジネス継続性および災害復旧という点では、通常、これが最も複雑でなく、コストのかからないモデルになります。
- 事業保険のコストを節約できる可能性があります。

リモート モデルには、以下の欠点があります。

- ローカルまたはキャンパス モデルより、管理が複雑です。
- 仮想 IP アドレスをシステムの単一管理アドレスとして使用できないため、多くのデバイス設定が必要となります（仮想 IP アドレッシングを使用できない場合の対処 （1119 ページ）を参照）。
- 通常、他の 2 つのモデルよりも提供される帯域幅が低く、遅延が大きくなります。これは HA の信頼性に影響を与える可能性があり、是正するには管理者の介入が必要になる場合もあります（「HA のネットワーク スループットに関する制限事項（1112 ページ）」を参照）。

自動フェールオーバーと手動フェールオーバーの違い

自動フェールオーバーを行うように HA を設定すると、ネットワーク管理者による HA の管理の必要性が減少します。また、セカンダリ サーバーが自動的に起動されるため、フェールオーバーの発生原因となった状況への対応に要する時間が削減されます。

ただし、ほとんどの場合は、システムで手動フェールオーバーを設定することが推奨されます。この推奨に従うことで、断続的なネットワークの停止を理由に Cisco EPN Manager がセカ

ンダリ サーバーに頻繁にフェールオーバーすることがなくなります。この状況が発生する可能性が最も高いのは、リモートモデルを使用してHAを導入する場合です。このモデルは、特に帯域幅と遅延の急激な変化による影響を受けます（HAの導入計画 （1112ページ）およびHAのネットワーク スループットに関する制限事項 （1112 ページ）を参照）。

フェールオーバー タイプが [自動（Automatic）] に設定されている場合に、ネットワーク接続がダウンするか、またはプライマリ サーバーとセカンダリ サーバー間のネットワーク リンクが到達不能になると、プライマリ サーバーとセカンダリ サーバーの両方が同時にアクティブになる可能性がわずかながらあります。これは「スプリット ブレーン状況」と呼ばれます。

この状況を防ぐため、プライマリ サーバーはセカンダリ サーバーがアクティブかどうかを常に確認します。ネットワーク接続またはリンクが復元され、プライマリ サーバーからセカンダリ サーバーに再び到達可能になると、プライマリ サーバーはセカンダリ サーバーの状態を確認します。セカンダリ サーバーの状態がアクティブな場合、プライマリ サーバーは自らダウンします。続いてユーザーがプライマリ サーバーへの標準の手動フェールバックを実行できます。

この状況が発生するのは、プライマリ HA サーバーで自動フェールオーバーが設定されている場合だけであることに注意してください。プライマリ サーバーで手動フェールオーバーを設定することで、この状況が発生する可能性が排除されます。これが、手動フェールオーバー設定を推奨するもう 1 つの理由です。

大企業では特に、自動フェールオーバーは不適切です。特定の HA 導入環境で自動フェールオーバーを実行することになった場合、管理者はプライマリ サーバーまたはセカンダリ サーバーに新規に追加されたデータのいずれかを選択しなければならないことがあります。つまり、スプリットブレーンの状況が発生するたびにデータが失われる可能性があります。この問題に対処する際のヘルプについては、を参照してください。 スプリット ブレイン シナリオからの回復方法 （1147 ページ）

HA を適切に管理するために、Cisco EPN Manager 管理者は、フェールオーバーまたはフェールバックを開始する前に、以下を含むHA導入の全体的な状態を必ず確認することが推奨されます。

- プライマリ サーバーの現在の状態。
- セカンダリ サーバーの現在の状態。
- 2 台のサーバー間の現在の接続状態。

ハイ アベイラビリティのセットアップ

ハイ アベイラビリティ導入環境にプライマリ サーバーとセカンダリ サーバーをインストールする方法については、『Cisco Evolved Programmable Network Manager Installation Guide』で説明しています。インストールの一環として、管理者は HA 導入環境で手動または自動フェールオーバーが使用されるように設定します。現在のフェールオーバー設定は、**ncs ha status** コマンドを使用して確認するか、[ヘルスモニター（Health Monitor）] Web ページで確認できます（ヘルス モニター Web ページの使用 （1129 ページ）を参照）。

プライマリ サーバーとセカンダリ サーバーをインストールしたら、プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （1119 ページ）で説明する HA 設定手順を実行する必要があります。

次のトピックで、HA の導入に関する追加情報を提供します。

HA での仮想 IP アドレッシングの使用

仮想 IP アドレスは、アクティブ HA サーバーの管理 IP アドレスを表します。フェールオーバーまたはフェールバック中は、仮想 IP アドレスが 2 つの HA サーバー間で自動的に切り替えられます。これには次の 2 つのメリットがあります。

- Cisco EPN Manager Web GUI に接続するために、どのサーバーがアクティブかを把握する必要がありません。仮想 IP を使用すれば、要求がアクティブな HA サーバーに自動的に転送されます。
- プライマリ サーバーとセカンダリ サーバーの両方に通知を転送するように管理対象デバイスを設定する必要がありません。通知を仮想 IP アドレスに転送するだけで済みます。

プライマリ サーバーと一緒にセカンダリ サーバーを設定するときに、仮想 IP アドレッシングを有効にすることができます。両方のサーバーで共有する仮想アドレス（IPv4 は必須で IPv6 はオプション）を入力する必要があります。プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （1119 ページ）を参照してください。

仮想 IP アドレスを使用しても、フェールオーバーまたはフェールバックの発生時に、アクティブなクライアント/サーバー セッションが終了するという事実は変わりません。仮想 IP アドレスが使用可能な状態であっても、新しいサーバーが新しい要求の処理を開始すると、アクティブなクライアント/サーバー セッション（Web GUI または NBI）が終了します。Web GUI ユーザーは、ログアウトしてログインし直す必要があります。中断した NBI セッションの処理方法については、Cisco Evolved Programmable Network Manager MTOSI API ガイド（OSS 統合） を参照してください。

（注） 仮想 IP を使用するには、プライマリ サーバーとセカンダリ サーバーの IP アドレスが同じサブネット上に存在する必要があります。

HA での複数の仮想 IP アドレッシング

Cisco EPN Manager では、独自の仮想 IP アドレスを持つように最大 3 つのインターフェイスを設定できます。さらに、仮想 IP アドレスを使用して、複数のインターフェイスのチーム（論理バインディング）を設定できます。これを行うには 2 つの方法があります。

- （**推奨**）CLI からすべての仮想 IP アドレスを設定します。

  この場合は Cisco EPN Manager UI で [仮想 IPの有効化（Enable Virtual IP）] チェックボックスをオンにしないでください。このフィールドのチェックボックスには、CLI から設定した最初の仮想 IP アドレスが自動的に入力されます。

- Cisco EPN Manager UI から最初の仮想IPアドレスを設定し、残りの仮想 IP アドレスは CLI から設定します。

（注） HA 登録時の問題を回避するには、CLI から設定する最初の仮想 IP が UI で設定したものと一致していることを確認します。不一致がある場合は HA 登録がブロックされ、エラーメッセージが表示されます。

このプロセスは HA 登録を実行するための前提条件です。

CLI から複数の仮想 IP を有効にするには、次の手順を実行します。

ステップ 1 Cisco EPN Manager の CLI 管理者ユーザーとしてサーバーにログインします。

ステップ 2 コンフィギュレーション モードを入力します。

```
configure terminal
```

ステップ 3 仮想 IP を設定するインターフェイスを選択します。

```
interface <name of interface>
```

ステップ 4 プロンプトで次のコマンドを入力します。

```
virtual-ip
```

ステップ 5 プライマリおよびセカンダリの HA サーバーで共有する IPv4 仮想 IP アドレスを指定します。必要に応じて、IPv6 仮想 IP アドレスを指定します（IPv4 アドレスは必須ですが、IPv6 アドレスはオプションです）。

- （必須）IPv4 アドレスを設定するには、次の手順を実行します。

  ```
  ip-address IPv4 address
  ```

- （オプション）IPv6 アドレスを設定するには、次の手順を実行します。

  ```
  ipv6-address IPv6 address
  ```

ステップ 6 サブメニューを終了します。

```
exit
```

ステップ 7 インターフェイス コンフィギュレーションを終了します。

```
exit
```

ステップ 8 コンフィギュレーション モードを終了します。

```
exit
```

ステップ 9 （オプション）インターフェイスで次のコマンドを実行して設定を確認します。

```
show running-config
```

HA 登録が正常に完了すると、仮想 IP アドレスがプライマリサーバーで有効になります。仮想 IP アドレスは HA 登録時にセカンダリサーバーにコピーされますが、フェールオーバーの場合にのみ有効になります。

（注）
- Cisco EPN Manager UI には、最初のインターフェイスである GigabitEthernet 0（または Ethernet 0）に設定された仮想 IP のみが表示されます。残りのインターフェイスに設定された仮想 IP アドレスは、Web UI に表示されません。
- インターフェイスに設定されているすべての仮想 IP アドレスを表示するには、CLI で `show running config` コマンドを実行します。

仮想 IP アドレッシングを使用できない場合の対処

選択する導入モデルによっては、仮想IPアドレスを設定しないでおくと、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーが発生した場合に syslog と SNMP 通知がセカンダリ サーバーに転送されるようにするために、管理者が追加の作業を行わなければならない状況になることがあります。一般的な方法は、両方のサーバーにすべてのsyslogとトラップを転送するようにデバイスを設定することです。このためには通常、転送先をプライマリ サーバーとセカンダリ サーバーの両方を含む特定のサブネットまたは IP アドレス範囲に設定します。

この設定作業は、HA のセットアップと同時に行う必要があります。つまりセカンダリ サーバーをインストールした後、プライマリ サーバーでHAを登録する前に行います。これはフェールオーバーが発生する前に完了しておく必要があります。これにより、データが失われる可能性を解消または削減できます。仮想 IP アドレスを使用しない場合、セカンダリ サーバーのインストール手順は変更されません。ただし通常どおり、個別の IP アドレスを使用してプライマリ サーバーとセカンダリ サーバーをプロビジョニングする必要があります。

プライマリ サーバーとセカンダリ サーバー間の HA の設定方法

HA を有効にするには、プライマリ サーバーで HA を設定する必要があります。プライマリ サーバーが HA 設定に参加するために、インストール中に必要となる設定はありません。プライマリサーバーを設定する前に次の情報が必要です。

- すでにインストールおよび設定済みのセカンダリ HA サーバーの IP アドレスまたはホスト名（セカンダリサーバーのインストールについては、『*Cisco Evolved Programmable Network Manager Installation Guide*』を参照してください）。
- セカンダリ サーバーのインストール時に設定した認証キー。
- （オプション）通知の送信先となる 1 つ以上の電子メール アドレス。
- フェールオーバータイプ（自動フェールオーバーと手動フェールオーバーの違い（1115ページ）を参照してください）。

仮想 IP アドレッシングを使用する場合は、HA での仮想 IP アドレッシングの使用（1117 ページ）を参照してください。

NIC チーミングインターフェイスを使用する場合は、HA を使用した NIC チーミング（1122 ページ）を参照してください。

次の手順では、プライマリサーバーで HA を設定する方法について説明します。HA を再設定する場合も、同じ手順を実行します。

始める前に

複数の仮想 IP アドレスを使用する場合は、この手順の前に必ず CLI を使用してそれらのアドレスを設定してください。詳細については、HA での複数の仮想 IP アドレッシング（1118 ページ）を参照してください。

（注） 1 つの仮想 IP アドレスのみを使用する場合は、HA 登録時に Cisco EPN Manager UI から設定できます。CLI から設定する必要はありません。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Cisco EPN Manager にログインします。

ステップ 2 メニューから、**[管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]** の順に選択します。Cisco EPN Manager によって HA ステータス ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択し、次のフィールドに入力します。

1. [セカンダリ サーバー（Secondary Server）]：セカンダリ サーバーの IP アドレスまたはホスト名を入力します。

   （注） ホスト名を IP アドレスに解決するには、DNS サーバーを使用することをお勧めします。DNS サーバーの代わりに「/etc/hosts」ファイルを使用している場合は、ホスト名の代わりにセカンダリ IP アドレスを入力します。

2. [認証キー（Authentication Key）]：セカンダリ サーバーのインストール中に設定したパスワードを認証キーとして入力します。

3. [電子メールアドレス（Email Address）]：（任意）HA の状態変更に関する通知の送信先アドレス（またはコンマで区切ったアドレスのリスト）を入力します。[メールサーバー設定（Mail Server

Configuration）] ページで電子メール通知をすでに設定している場合、ここに入力した電子メールアドレスは、メールサーバーですでに設定されているアドレスのリストに追加されます。

4. [フェールオーバー タイプ（Failover Type）] : [手動（Manual）] または [自動（Automatic）] を選択します。[手動（Manual）] を選択することが推奨されます。

ステップ 4 （仮想 IP アドレスを CLI を使用してすでに設定している場合は、このステップを無視してステップ 5 に進んでください。）仮想 IP 機能を使用する場合は、[仮想IPの有効化（Enable Virtual IP）] チェックボックスをオンにし、追加フィールドに次のように入力します。

1. [IPV4仮想IP（IPV4 Virtual IP）] : 両方の HA サーバーに使用する仮想 IPv4 アドレスを入力します。
2. [IPV6仮想IP（IPV6 Virtual IP）] : （オプション）両方の HA サーバーに使用する仮想 IPv6 アドレスを入力します。

（注） 両方のサーバーが同一サブネット上にないと仮想 IP アドレッシングは機能しません。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックし、HA 関連の環境パラメータが設定を行える状態になっているかを確認します。

詳細については、HA 設定の準備状況の確認 （1124 ページ）を参照してください。

（注） 準備状況チェックによって HA 設定がブロックされることはありません。すべてのテストに合格しなくも、HA を設定できます。

ステップ 6 [保存（Save）] をクリックして変更を保存します。Cisco EPN Manager によって HA 設定プロセスが開始されます。設定が正常に完了すると、**[コンフィギュレーションモード（Configuration Mode）]** に、**[HA対応（HA Enabled）]** という値が表示されます。

（注） FTP または TFTP サービスがプライマリサーバーで実行されている場合は、フェールオーバーが失敗しないようにするために、設定の完了後にセカンダリサーバーを再起動する必要があります。

注意すべき重要点：

- 高可用性機能は、HA 登録後に追加された仮想 IP アドレスを管理しません。HA 登録後に仮想 IP アドレスを追加しないことをお勧めします。
- HA 登録に失敗すると、設定されているすべての仮想 IP アドレスが削除されます。HA 登録の前に、これらを再設定する必要があります。
- 高可用性を有効にした後で仮想 IP アドレスを削除すると、高可用性は失敗します。
- 回線上でファイバが切断されると、復元操作がトリガーされます。復元中にプライマリサーバーとセカンダリサーバーの間で HA スイッチオーバーが発生すると、スイッチオーバーされた EPNM サーバーで回線の**検出**状態が [部分（Partial）] になることがあります。これを解決するには、デバイスを手動で同期するか、毎晩同期をスケジュールします。
- すでに設定した仮想 IP アドレスを変更するには、次の手順を実行します。
  1. 既存の HA 設定を削除します。

2. 仮想 IP アドレスを設定します。
3. HA 登録を再度実行します。

HA を使用した NIC チーミング

Cisco EPN Manager では、NIC チーミングインターフェイスを HA 導入に使用する「ノースバウンドインターフェイス」として指定する必要があります。NIC チーミングの指定は、CLI から設定できます。

NIC チーミングインターフェイスの設定と「ノースバウンド インターフェイス」の指定は、HA 導入の前提条件としてプライマリサーバーとセカンダリサーバーで同じに設定する必要があります。

（注） NIC チーミングインターフェイスがメンバーとして eth0 で設定されている場合、NIC チーミングインターフェイスが NBI に対して自動的に選択されます。

NIC チーミングインターフェイスがメンバーとして eth0 なしで設定されている場合、NIC チーミングインターフェイスは SBI にのみ使用されます。

CLI から NIC チーミングインターフェイスを「ノースバウンド インターフェイス」として指定するには、次の手順を実行します。

ステップ 1 CLI 管理者権限を持つユーザー ID とパスワードを使用して Cisco EPN Manager にログインします。

ステップ 2 プロンプトで次のコマンドを入力します。

```
ncs ha Northbound interface Team <0-2>
```

ステップ 3 HA 導入の「ノースバウンド インターフェイス」として指定する NIC チーミングインターフェイス番号を指定します。

ステップ 4 設定を保存します。

```
write memory
```

ステップ 5 （オプション）次のコマンドを実行して設定を確認します。

```
show running-config
```

（注） 上記の手順は、NIC チーミングインターフェイスに対してのみ認定されています。

その他の「ノースバウンドインターフェイス」設定も機能する可能性はありますが、正式には認定されていません。

HA 環境での SSO サーバーの設定

シングルサインオン（SSO）認証は、マルチユーザー、マルチリポジトリ環境でのユーザーの認証および管理に使用されます。SSOは、さまざまなシステムにログインするために使用されるクレデンシャルを格納および取得します。Cisco EPN Manager の他のインスタンス用の SSO サーバーとして Cisco EPN Manager をセットアップできます。

ハイ アベイラビリティ環境で SSO サーバーを設定するには、表 61 : HA 展開における SSO の設定に記載されているいずれかの手順を選択します。詳細については、次のトピックを参照してください。

- SSO サーバーを設定するには、「Cisco EPN Manager への RADIUS または TACACS+ サーバーの追加 （1041 ページ）」を参照してください。
- HA サーバーを設定するには、『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください。

表 *61 : HA* 展開における *SSO* の設定

SSO の設定	SSO サーバーのセットアップ	サーバーのフェールオーバー シナリオ	SSOサーバーの障害シナリオ
スタンドアロン サーバーとして SSO を設定	1. スタンドアロンの SSO サーバーを設定します。 2. プライマリおよびセカンダリ HA サーバーを設定します。	プライマリ サーバーに障害が発生すると、セカンダリ サーバーが有効化されます。プライマリ サーバーに接続されているすべてのマシンが、セカンダリ サーバーにリダイレクトされます。	SSOサーバで障害が発生すると、SSO機能が無効になります。Cisco EPN Managerはローカル認証を使用します。
セカンダリ サーバーで SSO を設定	1. 1 台のサーバーを SSOサーバーとプライマリ サーバーに設定します（つまり、プライマリ サーバーは SSO サーバーでもあります）。 2. セカンダリ HA サーバーを設定します。	プライマリ サーバーに障害が発生すると、セカンダリ サーバーが有効化されます。プライマリ サーバーに接続されているすべてのマシンは、セカンダリ サーバーにリダイレクトされません（これは、プライマリ サーバーで SSO が設定されているためです）。	SSO（プライマリ）サーバーで障害が発生した場合は、セカンダリ サーバーを SSO のフェールバック オプションとして設定できます。これにより、すべてのインスタンスをセカンダリ サーバーに接続できます。 セカンダリ サーバーが SSO サーバーのフェールバック オプションとして設定されていない場合、Cisco EPN Manager はローカル認証を使用します。

HA 設定の準備状況の確認

HA 設定時に、HA に関連する他の環境パラメータ（システム仕様、ネットワーク構成、サーバー間の帯域幅など）によって HA 設定が完了したかが判別されます。

15のチェックがシステムで実行され、エラーや障害なくHA設定が完了したことが確認されます。準備状況の確認機能を実行すると、チェックリストの名前および対応するステータスが、該当する場合は推奨事項とともに表示されます。

（注） **準備状況の確認**によってHA設定がブロックされることはありません。すべてのチェックに合格しなくても、HA を設定できます。

プライマリとセカンダリの認証キーが異なる場合、準備状況チェックは続行されません。HA登録を続行できます。

HA 設定の準備状況を確認するには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Cisco EPN Manager にログインします。

ステップ 2 メニューから、**[管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]** の順に選択します。Cisco EPN Manager によって HA ステータス ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択します。

ステップ 4 [セカンダリサーバー（Secondary Server）] フィールドにセカンダリサーバーの IP アドレスを入力し、[認証キー（Authentication Key）] フィールドにセカンダリの認証キーを入力します。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックします。

ポップアップウィンドウが開き、システム仕様およびその他のパラメータが表示されます。画面には、チェックリスト項目の名前、ステータス、影響、推奨事項の詳細が示されます。

その下に、準備状況の確認に使用されたチェックリストのテスト名と説明のリストが表示されます。

表 *62 :* チェックリストの名前と説明

チェックリストのテスト名	テストの説明
システム - CPU数の確認（SYSTEM - CHECK CPU COUNT）	プライマリサーバーとセカンダリサーバーのCPU数を確認します。 両方のサーバーのCPU数が要件を満たしている必要があります。
システム - ディスク IOPS の確認（SYSTEM - CHECK DISK IOPS）	プライマリサーバーとセカンダリサーバーのディスク速度を確認します。 必要な最小ディスク速度は 200 Mbps です。

システム - RAM サイズの確認（SYSTEM - CHECK RAM SIZE）	プライマリサーバーとセカンダリサーバーの RAM サイズを確認します。 両方のサーバーの RAM サイズが要件を満たしている必要があります。
システム - ディスクサイズの確認（SYSTEM - CHECK DISK SIZE）	プライマリサーバーとセカンダリサーバーのディスクサイズを確認します。 両方のサーバーのディスクサイズが要件を満たしている必要があります。
システム - サーバーへの ping 確認（SYSTEM - CHECK SERVER PING REACHABILITY）	プライマリサーバーが ping を介してセカンダリサーバーに到達できることを確認します。
システム - OS互換性の確認（SYSTEM - CHECK OS COMPATABILITY）	プライマリ サーバーとセカンダリ サーバーの OS バージョンが同じであることを確認します。
システム - ヘルス モニターのステータス（SYSTEM - HEALTH MONITOR STATUS）	ヘルスモニタープロセスがプライマリサーバーとセカンダリサーバーで実行されているかどうかを確認します。
ネットワーク - ネットワーク インターフェイスの帯域幅確認（NETWORK - CHECK NETWORK INTERFACE BANDWIDTH）	インターフェイス eth0 の速度がプライマリサーバーとセカンダリサーバーで推奨されている 500 Mbps に一致しているかどうかを確認します。 このテストでは、プライマリサーバーとセカンダリサーバー間でのデータ送信によるネットワーク帯域幅の測定は行いません。
ネットワーク - データベース ポートの開閉についてファイアウォールの確認（NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY）	データベース ポート 1522 がシステム ファイアウォールで開いているかどうかを確認します。 このポートが無効になっていると、テストは IP テーブルリストで 1522 の権限を付与します。
データベース - オンラインステータスの確認（DATABASE - CHECK ONLINE STATUS）	データベースファイルのステータスがオンラインになっており、プライマリサーバーとセカンダリサーバーでアクセス可能であるかどうかを確認します。
データベース - メモリターゲットの確認（DATABASE - CHECK MEMORY TARGET）	HA セットアップの「/dev/shm」データベース メモリ ターゲット サイズを確認します。
データベース - リスナーのステータス（DATABASE - LISTENER STATUS）	プライマリサーバーとセカンダリサーバーでデータベースリスナーが稼働中であるかどうかを確認します。 障害が発生した場合、テストによってリスナーの起動とステータスの報告が試行されます。

データベース - リスナー設定ファイルの破損確認（DATABASE - CHECK LISTENER CONFIG CORRUPTION）	すべてのデータベースインスタンスがデータベースリスナー設定ファイル「listener.ora」に存在するかどうかを確認します。
データベース - TNS 設定ファイルの破損確認（DATABASE - CHECK TNS CONFIG CORRUPTION）	すべての「WCS」インスタンスがデータベース TNS リスナー設定ファイル「tnsnames.ora」に存在するかどうかを確認します。
データベース - TNS 到達可能性のステータス（DATABASE - TNS REACHABILITY STATUS）	プライマリサーバーとセカンダリサーバーで TNSPING が成功しているかどうかを確認します。

ステップ 6 すべてのパラメータのチェックが完了したら、パラメータのステータスを確認し、[クリア（Clear）] をクリックしてウィンドウを閉じます。

（注） **準備状況の確認**中のフェールバック イベントとフェールオーバー イベントは、[アラームおよびイベント（Alarms and Events）] ページに転送されます。設定障害イベントは [アラームおよびイベント（Alarms and Events）] リストに表示されません。

HA サーバーにパッチを適用する方法

次のいずれかの方法で HA サーバーの UBF パッチをダウンロードおよびインストールできます。

- 現在ペアリングされていない HA サーバーにパッチをインストールします。Cisco EPN Manager 用に HA が設定されていない場合は、この方法をお勧めします。
- 手動フェールオーバーを使用して、ペアリングされている既存の HA サーバーにパッチをインストールします。HA がすでに設定されている場合はこの方法が推奨されます。
- 自動フェールオーバーを使用して、ペアリングされている既存の HA サーバーにパッチをインストールします。

それぞれの方法について詳しくは、以下を参照してください。

新しい HA サーバーへのパッチ適用方法

新しい Cisco EPN Manager ハイ アベイラビリティ（HA）実装のセットアップで、新しいサーバーのパッチ レベルが異なる場合は、次の手順に従って両方のサーバーにパッチをインストールし、同じパッチ レベルにします。

ステップ 1 パッチをダウンロードして、プライマリ サーバーにインストールします。

a) ブラウザで Cisco EPN Manager のソフトウェア パッチ リストにアクセスします（「Software patches listing for Cisco Evolved Programmable Network Manager」参照してください）。

b) インストールする必要があるパッチ ファイル（UBF ファイル拡張子で終わるファイル）に対応する [ダウンロード（Download）] ボタンをクリックし、そのファイルをローカルに保存します。
c) 管理者特権を持つ ID を使用してプライマリ サーバーにログインし、[管理（Administration）] > [ライセンスおよびソフトウェア アップデート（Licenses and Software Updates）] > [ソフトウェア アップデート（Software Update）] を選択します。
d) ページ上部の [アップロード（Upload）] リンクをクリックし、パッチ ファイルの保存場所に移動します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) 次のオプションのいずれかを使用して、UBF ファイルをアップロードします。

1. ローカル コンピュータからアップロード

- [アップデートのアップロード（Upload Update）] ウィンドウの [ローカルコンピュータからアップロード（Upload from local computer）] ラジオ ボタンをクリックします。
- [参照（Browse）] をクリックし、ファイルまで移動して [OK] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

2. サーバーのローカル ディスクからコピー

- [アップデートのアップロード（Upload Update）] ウィンドウの [サーバーのローカルディスクからコピー（Copy from server's local disk）] ラジオ ボタンをクリックします。
- [選択（Select ）] をクリックして、[ローカルディスクからファイルを選択（Select file from local disk）] ポップアップから UBF ファイルを選択し、[選択（Select）] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

g) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
h) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
i) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。
j) プライマリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 2 セカンダリ サーバーに同じパッチをインストールします。

a) ブラウザで以下の URL にアクセスして、セカンダリ サーバーの Health Monitor（HM）Web ページを表示します。

https://*ServerIP***:8082**

ここで、*ServerIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

b) セカンダリ サーバーの認証キーの入力を求めるプロンプトが出されます。パスワードを入力してから、[ログイン（Login）] をクリックします。

c) HM Web ページの [ソフトウェア アップデート（Software Update）] リンクをクリックします。再び、認証キーの入力を求めるプロンプトが出されます。パスワードを入力し、[ログイン（Login）] を再びクリックします。
d) [アップデート ファイルのアップロード（Upload Update File）] をクリックし、パッチ ファイルを保存した場所を参照します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) ページ上部の [アップロード（Upload）] リンクをクリックします。
g) 次のオプションのいずれかを使用して、UBF ファイルをアップロードします。

1. ローカル コンピュータからアップロード

- [アップデートのアップロード（Upload Update）] ウィンドウの [ローカルコンピュータからアップロード（Upload from local computer）] ラジオ ボタンをクリックします。
- [参照（Browse）] をクリックし、ファイルまで移動して [OK] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

2. サーバーのローカル ディスクからコピー

- [アップデートのアップロード（Upload Update）] ウィンドウの [サーバーのローカルディスクからコピー（Copy from server's local disk）] ラジオ ボタンをクリックします。
- [選択（Select ）] をクリックして、[ローカルディスクからファイルを選択（Select file from local disk）] ポップアップから UBF ファイルを選択し、[選択（Select ）] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

h) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
i) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
j) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。
k) セカンダリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 3 両方のサーバーのパッチ ステータスが同一であることを次のように確認します。

a) 上記のステップ 1 と同じ方法でプライマリ サーバーにログインし、[ソフトウェア アップデート（Software Update）] ページにアクセスします。インストールされているすべてのパッチの [ステータス（Status）] 列で [インストール済み（Installed）] と表示されていることを確認します。
b) 上記のステップ 2 と同じ方法でセカンダリ サーバーのヘルス モニター Web ページにアクセスします。インストールされているすべてのパッチの [ステータス（Status）] 列で [インストール済み（Installed）] と表示されていることを確認します。

ステップ 4 サーバーを登録します。

詳細については、「Software patches listing for Cisco Evolved Programmable Network Manager」およびCisco EPN Manager の停止と再起動 （973 ページ）を参照してください。

ペアリング済み HA サーバーへのパッチ適用方法

現在の Cisco EPN Manager 実装に含まれているハイ アベイラビリティ サーバーのパッチ レベルが同一ではない場合、または両方の HA サーバーに新しいパッチを適用する必要がある場合は、次の手順を実行します。

ペアリング済み HA サーバーへのパッチの適用はサポートされていません。HA が設定されている状態ではCisco EPN Managerサーバーのアップデートが実行できないことを示すポップアップ エラー メッセージが表示されます。そのため、パッチを適用する前に、まずプライマリおよびセカンダリ サーバーを接続解除しなければなりません。

1. GUI での HA の削除 （1154 ページ）の手順に従って、プライマリ サーバーとセカンダリ サーバーの接続を解除します。
2. 新しいHAサーバーへのパッチ適用方法（1126ページ）の手順に従ってパッチを適用します。
3. ハイ アベイラビリティのセットアップ（1116ページ）の手順に従ってHAの設定を復元します。

HA ステータスとイベントのモニター

次のトピックでは、HA 環境の全体的な正常性をモニターリングする方法を説明します。

- ヘルス モニター Web ページの使用 （1129 ページ）
- HA コンフィギュレーション モード （1149 ページ）
- HA の状態と遷移 （1149 ページ）
- HA ステータスと全体的な健全性の確認 （1131 ページ）
- HA イベントの表示とカスタマイズ （1132 ページ）
- HA エラー ロギングの使用 （1133 ページ）

ヘルス モニター Web ページの使用

ヘルス モニターは、HA 操作を管理する主要コンポーネントの 1 つです。ヘルス モニター インスタンスはアプリケーションプロセスとして両方のサーバーで実行され、各サーバーにそれぞれの Web ページが表示されます。LMP は、次の機能を実行します。

- HA に関連するデータベースおよびコンフィギュレーション データを同期します（Oracle Data Guard を使用して別途同期されるデータベースは除きます）。

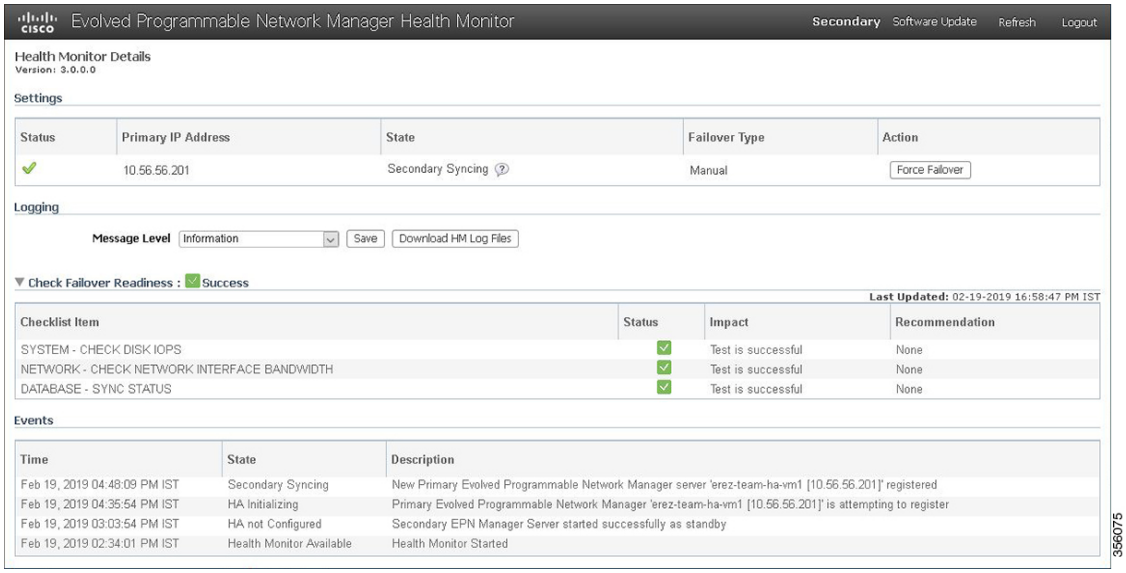
- プライマリ サーバーとセカンダリ サーバーの間で 5 秒間隔でハートビート メッセージを交換し、サーバー間の通信が維持されていることを確認します。正常なサーバーは、もう一方の冗長サーバーからのハートビートを 3 回連続して受信できなかった場合、10 秒間待機します。その後、正常なサーバーは冗長サーバーで Web URL を開こうとします。この試行が失敗すると、正常なサーバーがアクティブ サーバーになります。
- 両方のサーバー上で使用可能なディスク容量を定期的に確認し、ストレージ容量が不足するとイベントを生成します。
- リンクされた HA サーバーの全体的な健全性を管理、制御、モニターします。プライマリ サーバーで障害が発生すると、ヘルス モニターによってセカンダリ サーバーがアクティブ化されます。

HA 設定が正常に完了した後は、ブラウザで以下の URL を指定することにより、プライマリ サーバーまたはセカンダリ サーバーのヘルス モニター Web ページにアクセスできます。

https://*ServerIP***:8082**

ServerIP はプライマリ サーバーまたはセカンダリ サーバーの IP アドレスかホスト名です。

次の例は、**[セカンダリ同期中（Secondary Syncing）]** 状態のセカンダリ サーバーのヘルス モニター Web ページを示しています。



1	[設定（Settings）]：ヘルス モニターの状態と設定の詳細が 5 つのセクションに表示されます。	2	[ステータス（Status）]：HA セットアップの現在の機能ステータスを示します（緑色のチェック マークは、HA が有効化されていて機能していることを示します）。

3	[イベント（Events）]：現在の HA 関連イベントが最新のイベントを先頭に時系列順に表示されます。	4	[プライマリ IP アドレス（Primary IP address）]/[セカンダリ IP アドレス（Secondary IP address）]：ペアリングされたサーバーの IP アドレスが表示されます。このヘルス モニター インスタンスはセカンダリ サーバーで実行されているため、プライマリ サーバーの IP アドレスが表示されています。
5	[ダウンロード（Download）]：ヘルス モニター ログ ファイルをダウンロードできます。	6	[状態（State）]：このヘルス モニター インスタンスが実行されているサーバー（この例ではセカンダリ サーバー）の現在の状態が示されます。
7	[メッセージレベル（Message Level）]：現在のログ レベル（[エラー（Error）]、[情報（Informational）]、および [トレース（Trace）]）を示します。変更可能です。ログ レベルを変更するには、[保存（Save）] をクリックする必要があります。	8	タイトル バー：表示しているヘルス モニター Web ページの対象 HA サーバーと、[更新（Refresh）] および [ログアウト（Logout）] ボタンが表示されます。[ソフトウェアアップデート（Software Updates）] はセカンダリ サーバーに対してのみ表示されます。
9	[フェールオーバータイプ（Failover Type）]：設定されているフェールオーバー タイプ（[手動（Manual）] または [自動（Automatic）]）を示します。	10	[アクション（Actions）]：実行できるアクション（フェールオーバーやフェールバックなど）を示します。使用可能なアクションのみがここに表示されます。
11	[フェールオーバーの準備状況の確認（Check Failover Readiness）]：HA 設定を有効にした後のディスク速度、ネットワーク インターフェイス帯域幅、および DB 同期ステータスのチェック結果が表示されます。		

（注） **準備状況の確認**によってセカンダリへのフェールオーバー（自動または手動）がブロックされることはありません。

HA ステータスと全体的な健全性の確認

Cisco EPN Manager の Web GUI または CLI を使用して、HA ステータスを確認できます。どちらの方法でも、サーバーの状態が一覧表示されます。状態については、HA の状態と遷移（1149 ページ）で説明します。

Web GUI を使用して HA ステータスを確認するには、次のいずれかを実行します。

- Cisco EPN Manager の Web GUI で **[管理（Administration）]** > **[設定（Settings）]** > **[ハイアベイラビリティ（High Availability）]** の順に選択し、[HAステータス（HA Status）] を選択します。現在の HA ステータスとイベントの状態が表示されます。
- ヘルス モニターを使用します。「ヘルス モニター Web ページの使用 （1129 ページ）」を参照してください。

CLI を使用して HA ステータスを確認するには、CLI 管理ユーザーとしていずれかのサーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。**ncs ha status** コマンドは、次の例のような HA 固有の出力を提供します。

```
ncs ha status
[Role] Secondary [Primary Server] cisco-ha1(192.0.2.133) [State] Secondary Active [Failover
 Type] Manual
```

ncs status コマンドを使用して、ヘルス モニターとその他のサーバー プロセスを確認します。次の例のような出力が表示されます。

```
ncs status
Health Monitor Server is running. ( [Role] Primary [State] Primary Active )
Database server is running
FTP Service is disabled
TFTP Service is disabled
NMS Server is running.
SAM Daemon is running ...
DA Daemon is running ...
```

HA イベントの表示とカスタマイズ

HA 関連のアラームは、[アラームおよびイベント（Alarms and Events）]テーブルに一覧表示されます。これらのアラームのリストについては、『Cisco Evolved Programmable Network Manager のサポート対象アラーム』を参照してください。次の手順では、Web GUI でこれらのアラームを表示する方法について説明します。

必要に応じて、次の操作を行うこともできます。

- アラームの重大度を調整する
- アラームの通知を設定する

詳細については、システムの問題を示すサーバー内部 SNMP トラップの使用 （981 ページ）を参照してください。

HA 関連アラームを表示する手順は次のとおりです。

ステップ 1 **[モニター（Monitor）]**>**[モニターリング ツール（Monitoring Tools）]**>**[アラームおよびイベント（Alarms and Events）]** を選択し、[アラーム（Alarms）] タブをクリックします

ステップ 2 テーブルの右上にある [表示（Show）] ドロップダウンリストから [クイックフィルタ（Quick Filter）] を選択します。

ステップ 3 [メッセージ（Message）] フィールドに、**High Availability** と入力します。

HA エラー ロギングの使用

ディスク容量を節約して最大限のパフォーマンスを達成するために、HA エラー ロギングはデフォルトで無効になっています。HA に問題がある場合は、次の手順に従ってエラー ロギングを有効化してログ ファイルを確認します。

ステップ 1 問題のあるサーバーのヘルス モニターを起動します（ヘルス モニター Web ページの使用 （1129 ページ）を参照）。

ステップ 2 [ロギング（Logging）] 領域で、[メッセージレベル（Message Level）] ドロップダウンリストからエラー ロギング レベルを選択し、[保存（Save）] をクリックします。

ステップ 3 確認するログ ファイルをダウンロードします。

1. [ダウンロード（Download）] をクリックします。

   .zip ファイルがデフォルトのダウンロード場所にコピーされます。

2. ログ ファイルを抽出し、ASCII テキスト エディタを使用して表示します。

フェールオーバーのトリガー

フェールオーバーでは、プライマリ サーバーで検出された障害への対応として、セカンダリ サーバーがアクティブ化されます。

ヘルス モニターは、2 台の HA サーバー間で交換されるハートビート メッセージを使用して障害状態を検出します。ハートビート メッセージが 5 秒ごとに送信され、セカンダリ サーバーからのハートビート メッセージにプライマリ サーバーが 3 回連続して応答しないと、ヘルス モニターはプライマリ サーバーに障害が発生したと見なします。ヘルス チェック中に、ヘルス モニターはアプリケーション プロセスのステータスとデータベースの健全性もチェックします。これらのチェックに対して適切な応答がない場合は、障害が発生したものと見なされます。

セカンダリ サーバーの HA システムがプライマリ サーバーのプロセス障害を検出するのに約 15 秒かかります。ネットワークの問題によってセカンダリ サーバーがプライマリ サーバーに接続できない場合、障害を検出してフェールオーバーを開始するまでにさらに時間がかかることがあります。また、セカンダリ サーバーでのアプリケーション プロセスが完全に機能するようになるまでにも時間がかかることがあります。

ヘルス モニターは障害を検出するとすぐに電子メール通知を送信します。この電子メールには、障害ステータスに加え、セカンダリ サーバーのヘルス モニター Web ページへのリンクも

記載されます。HA に自動フェールオーバーが設定されている場合、セカンダリ サーバーは自動的にアクティブ化されます。

手動フェールオーバーを実行する手順は次のとおりです。

始める前に

- プライマリ サーバーとセカンダリ サーバーの状態を確認します。
- 2 台のサーバー間の接続を検証します。
- 仮想 IP アドレスを使用していない場合は、トラップと syslog を両方のサーバーに転送するようにすべてのデバイスが設定されていることを確認します。

ステップ 1 電子メール通知に記載されている Web リンクを使用するか、ブラウザで次の URL を入力して、セカンダリ サーバーのヘルス モニター Web ページにアクセスします。

https://*ServerIP*:8082

ステップ 2 [フェールオーバー（Failover）] をクリックします。

フェールバックのトリガー

フェールバックとは、オンライン状態に戻ったプライマリ サーバーをアクティブ化するプロセスのことです。また、アクティブ ステータスをセカンダリ サーバーからプライマリ サーバーに移して、セカンダリ サーバーでのアクティブなネットワーク モニターリング プロセスを停止します。

フェールバックがトリガーされると、セカンダリ サーバーはその現行のデータベース情報と更新済みファイルをプライマリ サーバーに複製します。セカンダリ サーバーからプライマリ サーバーへのフェールバックを完了するまでの所要時間は、複製する必要のあるデータの量と使用可能なネットワーク帯域幅によって異なります。

データが正常に複製されると、HA はプライマリ サーバーの状態を [プライマリアクティブ（Primary Active）] に変更し、セカンダリ サーバーの状態を [セカンダリ同期中（Secondary Syncing）] に変更します。

フェールバック中のセカンダリサーバーの可用性は、フェールオーバー後に Cisco EPN Manager がプライマリサーバーに再インストールされたかどうかによって次のように異なります。

- フェールオーバー後に Cisco EPN Manager がプライマリサーバーに再インストールされた場合は、完全なデータベースコピーが必要になり、フェールバックプロセス中はセカンダリサーバーを使用できません。
- Cisco EPN Manager がプライマリサーバーに再インストールされていない場合は、プライマリサーバーでプロセスが開始されてセカンダリサーバーで停止されるまでの期間を除き、セカンダリサーバーを使用できます。両方のサーバーの Health Monitor Web ページに

アクセスして、フェールバックの進行状態をモニターすることができます。さらに、ユーザーはセカンダリ サーバーに接続して、通常のすべての機能を使用することもできます。

以下の手順で説明するように、常に手動でフェールバックをトリガーする必要があります。（注）

- フェールバックの進行中は、設定またはプロビジョニングのアクティビティを開始しないでください。
- フェールバックが正常に完了すると、セカンダリ サーバーがダウンして、制御がプライマリ サーバーに切り替わります。このプロセス中は、しばらくの間、ユーザーが Cisco EPN Manager にアクセスできなくなります。

始める前に

- プライマリ サーバーとセカンダリ サーバーの状態を確認します。
- 2 台のサーバー間の接続を検証します。
- 仮想 IP アドレスを使用していない場合は、トラップと syslog を両方のサーバーに転送するようにすべてのデバイスが設定されていることを確認します。
- プライマリサーバーに Cisco EPN Manager を再インストールしてオフライン Geo マップを使用する場合は、フェールバックをトリガーする前に、プライマリサーバーに Geo マップ リソースを再インストールする必要があります。『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください。

ステップ 1 電子メール通知に記載されているリンクを使用するか、ブラウザで次の URL を入力して、セカンダリ サーバーのヘルス モニター Web ページにアクセスします。

`https://ServerIP:8082`

ステップ 2 [フェールバック（Failback）] をクリックします。

フェールオーバーの強制実行

強制フェールオーバーは、プライマリ サーバーが稼働している間に、セカンダリ サーバーをアクティブにするプロセスです。このオプションは、たとえば、HA セットアップは完全に機能しているかどうかをテストする場合に使用します。

強制フェールオーバーを使用できるのは、プライマリがアクティブで、セカンダリが「セカンダリ同期中（Secondary Syncing）」状態であり、すべてのプロセスが両方のサーバーで実行中の場合に限られます。プライマリ サーバーがダウンしている場合、強制フェールオーバーは無効になります。この状況では、通常のフェールオーバーのみが有効です。

強制フェールオーバーが完了すると、セカンダリ サーバーがアクティブになり、プライマリ サーバーは自動的にスタンバイ状態で再起動します。通常のフェイルバックをトリガーすると、元の通りプライマリ サーバーがアクティブになり、セカンダリ サーバーがスタンバイ状態になります。

ステップ 1 「ヘルス モニター Web ページの使用」の手順に従って、セカンダリサーバーのヘルスモニター Web ページにアクセスします。

ステップ 2 [強制フェールオーバー（Force Failover）]ボタンをクリックして強制フェールオーバーをトリガーします。強制フェールオーバーは 2 ～ 3 分で完了します。

その他の HA イベントに対する応答

HA 関連のすべてのイベントは、[HA ステータス（HA Status）] ページ、Health Monitor Web ページ、および Cisco EPN Manager の [アラームおよびイベント（Alarms and Events）] ページに表示されます。ほとんどのイベントには、オペレータの応答は不要ですが、フェールオーバーおよびフェールバックのトリガーは例外です。次のトピックで説明するように、複雑なイベントもいくつかあります。

HA 登録が失敗した場合

HA 登録が失敗すると、各サーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[HA 初期化中（HA Initializing）]	元の状態：[HA 初期化中（HA Initializing）]
次の状態：[HA 未設定（HA not Configured）]	次の状態：[HA 未設定（HA not Configured）]

HA 登録の失敗から回復するには、次の手順に従います。

ステップ 1 ping または他のツールを使用して、2 台の Cisco EPN Manager サーバー間のネットワーク接続を確認します。プライマリ サーバーからセカンダリ サーバーに接続できること、その逆も可能であることを確認します。

ステップ 2 ゲートウェイ、サブネットマスク、仮想IPアドレス（設定されている場合）、サーバーのホスト名、DNS、NTP 設定がすべて正しいことを確認します。

ステップ 3 設定された DNS および NTP サーバーにプライマリ サーバーとセカンダリ サーバーから接続可能であること、そして DNS および NTP サーバーの両方が遅延や他のネットワーク固有の問題を伴うことなく応答していることを確認します。

ステップ 4 すべての Cisco EPN Manager ライセンスが正しく設定されていることを確認します。

ステップ 5 接続または設定の問題を解決したら、プライマリ サーバーとセカンダリ サーバー間の HA の設定方法（1119 ページ）の手順を再試行します。

ネットワークがダウンしている場合（自動フェールオーバー）

フェールオーバー タイプが [自動（Automatic）] に設定されている場合、2 台の Cisco EPN Manager サーバー間のネットワーク接続が失われると、それぞれのサーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリのフェールオーバー（Secondary Failover）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

セカンダリ サーバーがアクティブであることを示す電子メール通知を受信します。

ステップ 1 2台のサーバー間のネットワーク接続を確認し、復元します。ネットワーク接続が復旧し、セカンダリ サーバーがアクティブなことをプライマリ サーバーが検出できるようになったら、プライマリ サーバー上のすべてのサービスが自動的に再開し、パッシブ状態になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリ アクティブ（Secondary Active）]

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ同期中（Primary Syncing）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 2 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ同期中（Primary Syncing）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

ネットワークがダウンしている場合（手動フェールオーバー）

フェールオーバー タイプが [手動（Manual）] に設定されている場合、2 台の Cisco EPN Manager サーバー間のネットワーク接続が失われると、それぞれのサーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

各サーバーがもう一方のサーバーを失ったことを通知する電子メールを受信します。

ステップ 1 2 台のサーバー間のネットワーク接続を確認し、必要に応じて復元します。

ネットワーク接続が復元されると、次ように状態が遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

管理者による応答は不要です。

ステップ 2 何らかの理由でネットワーク接続を復元できない場合は、セカンダリ サーバーの HM Web ページを使用して、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリのフェールオーバー（Secondary Failover）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

セカンダリ サーバーがアクティブになったことを通知する電子メールを受信します。

ステップ 3 2台のサーバー間のネットワーク接続を確認し、復元します。ネットワーク接続が復旧し、セカンダリ サーバーがアクティブなことをプライマリ サーバーが検出したら、プライマリ サーバー上のすべてのサービスが自動的に再開し、パッシブ状態になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ同期中（Primary Syncing）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 4 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。

以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ同期中（Primary Syncing）]	元の状態：[セカンダリ アクティブ（Secondary Active）]

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

プロセスを再開できない場合（自動フェールオーバー）

Cisco EPN Manager Health Monitor プロセスは、失敗した Cisco EPN Manager サーバー プロセスの再開を試行します。通常、そのような障害が発生した時点でのプライマリ サーバーとセカンダリ サーバーの状態は、[プライマリ アクティブ（Primary Active）] および [セカンダリ同期中（Secondary Syncing）] となっているはずです。

HM がプライマリ サーバーで重要なプロセスを再開できない場合は、プライマリ サーバーは障害が発生したものとみなされます。現在設定されているフェールオーバー タイプが [自動（automatic）] の場合、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリが状態を確認できません（Primary Uncertain）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリのフェールオーバー（Secondary Failover）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

このプロセスが完了すると、セカンダリ サーバーがアクティブになったことを通知する電子メールでの通知を受信します。

ステップ 1 プライマリ サーバーを再起動し、稼働していることを確認します。プライマリ サーバーが再起動すると、その状態は [プライマリ同期中（Primary Syncing）] になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ フェールオーバー（Primary Failover）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリがフェールバックの準備中（Primary Preparing for Failback）]	次の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ同期中（Primary Syncing）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 2 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ同期中（Primary Syncing）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

プロセスをリスタートできない場合（手動フェールオーバー）

Cisco EPN Manager Health Monitor プロセスは、失敗した Cisco EPN Manager サーバー プロセスの再開を試行します。通常、そのような障害が発生した時点でのプライマリ サーバーとセカンダリ サーバーの状態は、[プライマリ アクティブ（Primary Active）] および [セカンダリ同期中（Secondary Syncing）] となっているはずです。HM がプライマリ サーバーで重要なプロセスを再開できない場合は、プライマリ サーバーは障害が発生したものとみなされます。その場合、障害を通知する電子メールを受信します。現在設定されているフェールオーバー タイプが [手動（Manual）] の場合、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリが状態を確認できません（Primary Uncertain）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

ステップ 1 セカンダリ サーバーで、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリが状態を確認できません（Primary Uncertain）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリのフェールオーバー（Secondary Failover）]
次の状態：[プライマリ フェールオーバー（Primary Failover）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 2 プライマリ サーバーを再起動し、稼働していることを確認します。プライマリ サーバーが再起動すると、プライマリ サーバーの HA 状態は [プライマリ同期中（Primary Syncing）] になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ フェールオーバー（Primary Failover）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリがフェールバックの準備中（Primary Preparing for Failback）]	次の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ同期中（Primary Syncing）]	次の状態：[セカンダリ アクティブ（Secondary Active）]

ステップ 3 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ同期中（Primary Syncing）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

同期中にプライマリ サーバーが再起動した場合（手動フェールオーバー）

セカンダリ サーバーとの同期中にプライマリ Cisco EPN Manager サーバーが再起動された場合は、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリ単独（Primary Alone）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

[プライマリ単独（Primary Alone）] および [プライマリ アクティブ（Primary Active）] 状態への遷移は、プライマリ サーバーがオンライン状態に戻った直後に行われます。管理者による応答は必要ありません。

同期中にセカンダリ サーバーが再起動した場合

プライマリ サーバーとの同期中にセカンダリ Cisco EPN Manager サーバーが再起動された場合は、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[プライマリ アクティブ（Primary Active）]	元の状態：[セカンダリ同期中（Secondary Syncing）]
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	元の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

管理者による応答は必要ありません。

HA サーバーが両方ともダウンしている場合

プライマリ サーバーおよびセカンダリ サーバーが同時にダウンした場合、次の手順で説明するように正しい順序で稼働中の状態に戻すことで復旧できます。

ステップ 1 セカンダリ サーバーと、セカンダリ サーバー上で稼働する Cisco EPN Manager インスタンスを再起動します。何らかの理由でセカンダリ サーバーを再起動できない場合は、HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （1145 ページ）を参照してください。

ステップ 2 セカンダリ サーバーで Cisco EPN Manager が稼働中になったら、セカンダリ サーバーの Health Monitor Web ページにアクセスします。セカンダリ サーバーの状態が [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] に遷移します。

ステップ 3 プライマリ サーバーと、プライマリ サーバー上で稼働する Cisco EPN Manager インスタンスを再起動します。Cisco EPN Manager がプライマリ サーバー上で稼働している場合、プライマリ サーバーは自動的にセカンダリ サーバーと同期します。これを確認するには、プライマリ サーバーの Health Monitor Web ページにアクセスします。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

両方の HA サーバーの電源がダウンしている場合

プライマリ サーバーおよびセカンダリ サーバーの電源が同時にダウンした場合、次の手順で説明するように正しい順序で稼働中の状態に戻すことで復旧できます。

ステップ 1 セカンダリ サーバーと、セカンダリ サーバー上で稼働する Cisco EPN Manager インスタンスの電源をオンにします。この状態ではプライマリ サーバーに到達できないため、セカンダリ HA の再起動は失敗します。ただし、セカンダリ サーバーの HM プロセスは実行され、エラーが表示されます。

ステップ 2 セカンダリ サーバーで Cisco EPN Manager が稼働中になったら、セカンダリ サーバーの HM Web ページにアクセスします（ヘルス モニター Web ページの使用 （1129 ページ）を参照）。セカンダリ サーバーが [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] 状態に遷移します。

ステップ 3 プライマリ サーバーと、プライマリ サーバー上で稼働する Cisco EPN Manager インスタンスの電源をオンにします。

ステップ 4 Cisco EPN Manager がプライマリ サーバー上で稼働している場合、プライマリ サーバーは自動的にセカンダリ サーバーとの同期を開始します。これを確認するには、プライマリ サーバーの HM Web ページにアクセスします。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：[プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）]	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

ステップ 5 セカンダリ サーバーと、セカンダリ サーバー上で稼働する Cisco EPN Manager インスタンスを再起動します。この時点では、プロセスのすべてがセカンダリ サーバーで実行されているわけではないため、この操作が必要です。

何らかの理由でセカンダリ サーバーを再起動できない場合は、HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （1145 ページ）を参照してください。

ステップ 6 Cisco EPN Manager がセカンダリ サーバーでの再起動を完了したときには、すべてのプロセスが実行されています。これを確認するには、**ncs ha status** コマンドを実行します。

HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合

両方の HA サーバーが同時にダウンし、セカンダリサーバーが再起動しない場合は、セカンダリサーバーが交換できるまで、プライマリサーバーをスタンドアロンサーバーとして使用するために、プライマリサーバーから HA 設定を削除する必要があります。

以下の手順では、すでにセカンダリ サーバーの再起動を試み、再起動に失敗したものとしています。

ステップ 1 Cisco EPN Manager のプライマリ インスタンスの再起動を試みます。プライマリ サーバーの再起動が可能である場合は、HA 設定の削除が必要であることを示すエラー メッセージが表示されて再起動が中断されます。

ステップ 2 プライマリ サーバーとの CLI セッションを開きます（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 3 次のコマンドを入力して、プライマリ サーバーの HA 設定を削除します。

```
ncs ha remove
```

（注） HA 設定を削除すると、プライマリサーバーは以前のセカンダリサーバーに登録できなくなるため、セカンダリサーバーを再インストールする必要があります。

ステップ 4 HA 設定を削除することを確認します。

エラー メッセージが表示されることなく Cisco EPN Manager のプライマリ インスタンスの再起動が可能になり、スタンドアロン サーバーとして使用できるようになります。セカンダリサーバーを交換できる場合は、プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （1119 ページ）の説明に従って続行します。

プライマリ サーバーの交換方法

通常の状況下では、プライマリ サーバーの状態は [プライマリアクティブ（Primary Active）]、セカンダリ サーバーの状態は [セカンダリ同期中（Secondary Syncing）] になります。何らかの

理由でプライマリ サーバーに障害が発生した場合、セカンダリ サーバーへのフェールオーバーが自動または手動で行われます。

HA への完全なアクセスを復旧するには、新しいハードウェアを使用してプライマリサーバーを再インストールする必要があることがあります。この場合、次の手順に従うことで、データを失うことなく新しいプライマリ サーバーを起動できます。

始める前に

セカンダリ サーバーでHAを設定したときに指定したパスワード（認証キー）があることを確認します。以下の手順では、これが必要となります。

ステップ 1 セカンダリ サーバーが[セカンダリアクティブ（Secondary Active）]状態であることを確認します。プライマリ サーバーで手動フェールオーバーが設定されている場合は、セカンダリ サーバーへのフェールオーバーをトリガーする必要があります（フェールオーバーのトリガー （1133 ページ）を参照）。

ステップ 2 交換する古いプライマリ サーバーがネットワークから切断していることを確認します。

ステップ 3 新しいプライマリ サーバーが使用可能な状態であることを確認します。これには、新しいサーバーをネットワークに接続し、古いプライマリ サーバーと同様に設定する（IPアドレス、サブネットマスクなど）ことが含まれます。セカンダリ サーバーに HA をインストールするときに使用した同じ認証キーを入力する必要があります。

ステップ 4 プライマリサーバーとセカンダリサーバーが同じパッチレベルであることを確認します。プライマリサーバーを置換する場合は、次の手順を実行する必要があります。

a) セカンダリサーバーの CLI で次のコマンドを実行して、プライマリサーバーとセカンダリサーバーが TOFU モードになっていることを確認します。

```
admin# ncs certvalidation certificate-check trust-on-first-use trustzone system
```

b) セカンダリサーバー管理 CLI にログインします。

c) セカンダリサーバーの CLI で次のコマンドを実行します。

```
admin# ncs certvalidation tofu-certs deletecert host <primaryserver's-IP-address appended with "_8082">
```

例：**ncs certvalidation tofu-certs deletecert host 10.56.58.91_8082**

これは、プライマリサーバーとセカンダリサーバー間の通信を再確立するために必要です。

ステップ 5 次に示すように、IP テーブルのエントリを更新します。

- プライマリの場合：1522 ポートの iptables にセカンダリ IP アドレスと仮想 IP アドレスを追加します（設定されている場合）。
- セカンダリの場合：1522 ポートの iptables にプライマリ IP アドレスと仮想 IP アドレスを追加します（設定されている場合）。

例:

```
iptables -A INPUT -s IP address -p tcp --dport 1522 -j ACCEPT
iptables -A INPUT -s IP address -j ACCEPT
```

ステップ 6 セカンダリ サーバーから新たにインストールしたプライマリ サーバーへのフェールバックをトリガーします。新しいプライマリ HA サーバーへのフェールバック中にはデータベースのフル コピーが実行されるため、使用可能な帯域幅とネットワーク遅延によってはこの処理の完了に時間がかかります。2台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：[HA 未設定（HA not configured）]	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ フェールバック（Secondary Failback）]
次の状態：[プライマリ フェールバック（Primary Failback）]	次の状態：[セカンダリ ポスト フェールバック（Secondary Post Failback）]
次の状態：[プライマリ アクティブ（Primary Active）]	次の状態：[セカンダリ同期中（Secondary Syncing）]

スプリット ブレイン シナリオからの回復方法

スプリット ブレインのシナリオでは、プライマリ サーバーとセカンダリ サーバーの両方が同時にアクティブになります。これは、ネットワークの停止または一時的にダウンしたリンクが原因となっている可能性があります。ただし、プライマリ サーバーはセカンダリ サーバーを継続的にチェックするため、接続が再確立されてセカンダリ サーバーがアクティブになると、プライマリ サーバーはダウンします。

「スプリットブレーン状況」が発生するまれな状況では、データが失われる可能性が常にあります。この場合、以下の手順に従い、新しく追加されたデータをセカンダリに保存し、追加されたデータをプライマリには保存しないようにすることができます。

ステップ 1 ネットワークが起動し、セカンダリ サーバーが起動すると、プライマリ サーバーはスタンバイ データベースを使用して自動的に再起動します。プライマリ サーバーの HA ステータスはまず「プライマリフェールオーバー（Primary Failover）」になり、その後「プライマリ同期中（Primary Syncing）」に遷移します。これを確認するには、プライマリ サーバーの Health Monitor Web ページにログオンします。

ステップ 2 プライマリ サーバーのステータスが「プライマリ同期中（Primary Syncing）」になったら、ユーザーが Web ブラウザを使用してセカンダリ サーバーの Cisco EPN Manager ページ（たとえば、https://server-ip-address:443）にログインできることを確認します。確認が済むまで、手順を進めないでください。

ステップ 3 セカンダリ サーバーにアクセスできることが確認できたら、セカンダリ サーバーのヘルス モニター Web ページから、フェールバックを開始します（フェールバックのトリガー（1134 ページ）を参照）。プライ

マリ サーバーへのスイッチオーバーが完了するまで、セカンダリ サーバーでモニターリング アクティビティを続行できます。

セカンダリ サーバーがダウンした場合

このシナリオでは、スタンバイ サーバーとして機能しているセカンダリ サーバーがダウンします。

セカンダリ サーバーを再び稼働させる手順は次のとおりです。

ステップ 1 セカンダリ サーバーの電源を入れます。

ステップ 2 セカンダリ サーバーで Cisco EPN Manager を起動します。

ステップ 3 プライマリ サーバーで、プライマリ サーバーの HA ステータスが「プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）」から「プライマリアクティブ（Primary Active）」に変わっていることを確認します。[管理（Administration）] > [設定（Settings）] > [ハイアベイラビリティ（High Availability）] > [HA設定（HA Configuration）] に移動します。

ステップ 4 ブラウザに URL **https://*serverIP*:8082** を入力して、セカンダリ サーバーのヘルス モニター ページにログインします。

ステップ 5 セカンダリ サーバーの HA ステータスが「セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）」から「セカンダリ同期中（Secondary Syncing）」に変わっていることを確認します。
上記のステータスが表示されたら、それ以上の操作は必要ありません。ただし、HA ステータスが変わらない場合、セカンダリ サーバーは自動的に回復できません。この場合は、次の手順に進みます。

ステップ 6 プライマリ サーバーで HA 設定を削除します。[管理（Administration）] > [設定（Settings）] > [ハイアベイラビリティ（High Availability）] > [HA設定（HA Configuration）] に移動して、[削除（Remove）] をクリックします。

ステップ 7 セカンダリ サーバーをプライマリ サーバーに登録します。を参照してくださいプライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （1119 ページ）。
HA 登録が成功した場合、それ以上の操作は必要ありません。ただし、HA 登録が失敗した場合は、セカンダリ サーバーでハードウェアまたはソフトウェアの損失が発生している可能性があります。この場合は、次の手順に進みます。

ステップ 8 プライマリ サーバーで HA 設定を削除します。

ステップ 9 プライマリ サーバーと同じリリースおよびパッチ（該当する場合）を使用してセカンダリ サーバーを再インストールします。

ステップ 10 セカンダリ サーバーをプライマリ サーバーに登録します。を参照してくださいプライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （1119 ページ）。

データベースの同期の問題を解決する方法

データベースの同期の問題を解決するには、プライマリ サーバーが「プライマリ アクティブ」状態で、セカンダリ サーバーが「セカンダリ同期」状態になっているときに、次の手順に従います。

ステップ 1 HA を削除します（CLI での HA の削除 （1154 ページ）および GUI での HA の削除 （1154 ページ）を参照）。

ステップ 2 プライマリ サーバーとセカンダリ サーバーの両方が「HA未設定（HA Not Configured）」状態になったら、HA の設定を実行します。ハイ アベイラビリティのセットアップ （1116 ページ） を参照してください。

ハイ アベイラビリティの参照情報

次のトピックでは、HA の参考情報を提供します。

HA コンフィギュレーション モード

HA コンフィギュレーション モードは、完全な HA 設定の全体的なステータスを表します（サーバー固有の HA 状態とは異なります）。

モード	説明
HA未設定（HA Not Configured）	このサーバーでは HA が設定されていません。
HA 初期化中（HA Initializing）	プライマリ サーバーとセカンダリ サーバー間の HA 設定プロセスが開始されました。
HA対応（HA Enabled）	プライマリ サーバーとセカンダリ サーバー間で HA が有効になっています。
HA単独（HA Alone）	1 台のサーバーがダウンしているか、同期していないか、到達不能であるため、サーバーが単独で稼働しています。

HA の状態と遷移

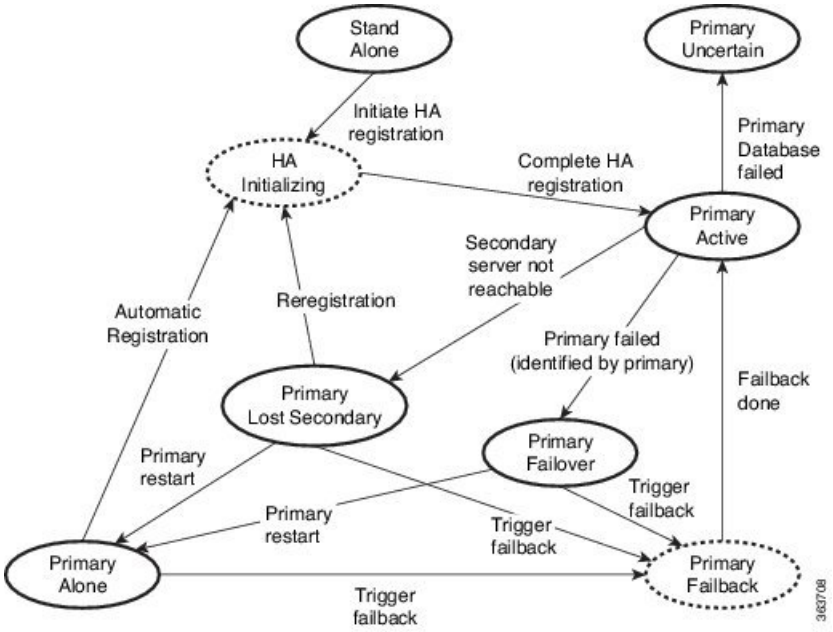
次の表に、HA の状態を示します（ユーザーによる応答が不要なものも含む）。これらの状態は、[HAステータス（HA Status）] ページ（**[管理（Administration）] > [設定（Settings）] > [ハイアベイラビリティ（High Availability）] > [HAステータス（HA Status）]**）またはヘルス モニターで確認できます。HA イベントの一覧と、イベントの有効化、無効化、および調整の手順については、サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送 （981 ページ）を参照してください。

状態	[サーバー（Server）]	説明
スタンドアロン（Stand Alone）	両方	このサーバーでは HA が設定されていません。
プライマリ単独（Primary Alone）	プライマリ（Primary）	プライマリ サーバーは、セカンダリ サーバーとの接続を失った後に再起動しました（この状態で実行されるのはヘルス モニターのみです）。
HA 初期化中（HA Initializing）	両方	プライマリ サーバーとセカンダリ サーバー間の HA 設定プロセスが開始されました。
プライマリ アクティブ（Primary Active）	プライマリ（Primary）	プライマリ サーバーは現在アクティブであり、セカンダリ サーバーと同期中です。
プライマリ データベースのコピーに失敗しました（Primary Database Copy Failed）	プライマリ（Primary）	再起動したプライマリ サーバーがデータ ギャップを検出してアクティブなセカンダリ サーバーからのデータ コピーをトリガーし、データベースのコピーに失敗しました。プライマリ サーバーは再起動すると必ず、自身が 24 時間以上ダウンしていたためにデータ ギャップが生じていないかを確認します。このコピーが失敗することはほとんどありませんが、まれに失敗した場合は、データベース コピーが正常に終了するまで、プライマリへのフェールバックの試行はすべてブロックされます。データベース コピーが正常に終了するとすぐに、プライマリ サーバーの状態が [プライマリ同期中（Primary Syncing）] に設定されます。
プライマリ フェールオーバー（Primary Failover）	プライマリ（Primary）	プライマリ サーバーで障害が検出されました。
プライマリ フェールバック（Primary Failback）	プライマリ（Primary）	ユーザーによってトリガーされたフェールバックが進行中です。
プライマリがセカンダリとの接続を失いました（Primary Lost Secondary）	プライマリ（Primary）	プライマリ サーバーは、セカンダリ サーバーと通信できません。

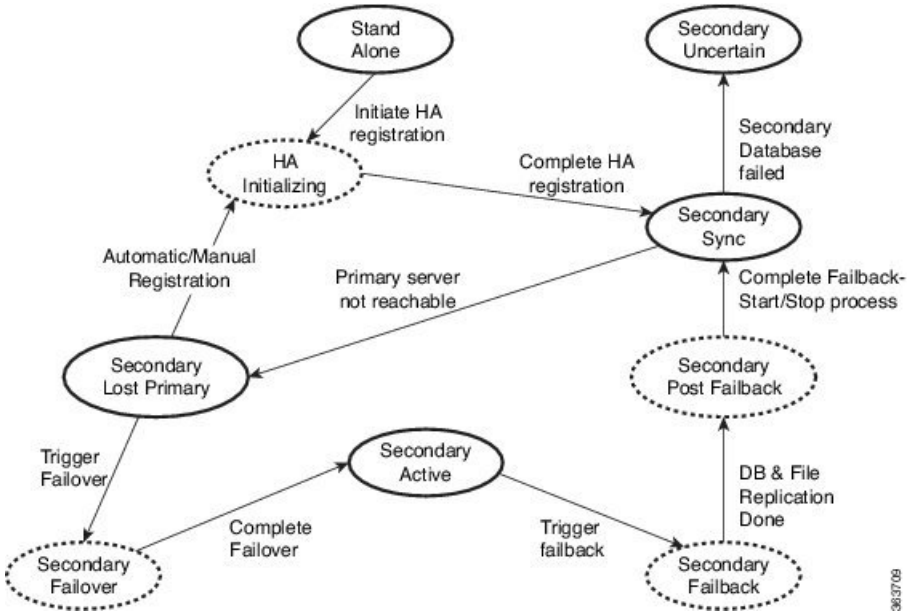
プライマリがフェールバックの準備中（Primary Preparing for Failback）	プライマリ（Primary）	フェールオーバー後にプライマリ サーバーがスタンバイ モードで起動しました（セカンダリ サーバーがまだアクティブであるため）。プライマリ サーバーでフェールバックの準備ができると、その状態が [プライマリ同期中（Primary Syncing）] に設定されます。
プライマリ同期中（Primary Syncing）	プライマリ（Primary）	プライマリ サーバーは、データベースおよびコンフィギュレーション ファイルを、アクティブなセカンダリ サーバーと同期しています。フェールオーバー後にプライマリ プロセスが起動すると（かつセカンダリ サーバーがアクティブ ロールを果たしている場合）、この状態になります。
プライマリが状態を確認できません（Primary Uncertain）	プライマリ（Primary）	プライマリ サーバーのアプリケーション プロセスがデータベースに接続できません。
セカンダリ単独（Secondary Alone）	セカンダリ（Secondary）	プライマリ サーバーの再起動後、セカンダリ サーバーからプライマリ サーバーに到達できません。
セカンダリ同期中（Secondary Syncing）	セカンダリ（Secondary）	セカンダリ サーバーは、データベースおよびコンフィギュレーション ファイルをプライマリ サーバーと同期しています。
セカンダリ アクティブ（Secondary Active）	セカンダリ（Secondary）	プライマリ サーバーからセカンダリ サーバーへのフェールオーバーが正常に完了しました。
セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）	セカンダリ（Secondary）	セカンダリ サーバーがプライマリ サーバーに接続できません（この状態は、プライマリ サーバーで障害が発生した場合、またはネットワーク接続が失われた場合に発生します）。 自動フェールオーバーの場合、セカンダリ サーバーは自動的に [セカンダリアクティブ（Secondary Active）] 状態に移ります。手動フェールオーバーの場合は、フェールオーバーをトリガーしてセカンダリ サーバーをアクティブにする必要があります（フェールオーバーのトリガー（1133 ページ）を参照）。
セカンダリのフェールオーバー（Secondary Failover）	セカンダリ（Secondary）	フェールオーバーがトリガーされて進行中です。

セカンダリ フェールバック（Secondary Failback）	セカンダリ（Secondary）	フェールバックがトリガーされ、データベースおよびファイルの複製が進行中です。
セカンダリ ポスト フェールバック（Secondary Post Failback）	セカンダリ（Secondary）	フェールバックがトリガーされ、関連するプロセスの停止と再起動が進行中です。データベースおよびコンフィギュレーション ファイルがセカンダリ サーバーからプライマリ サーバーに複製されました。プライマリ サーバーのステータスが [プライマリアクティブ（Primary Active）] に変わり、セカンダリ サーバーの HA ステータスが [セカンダリ同期中（Secondary Syncing）] に変わります。
セカンダリが状態を確認できません（Secondary Uncertain）	セカンダリ（Secondary）	セカンダリ サーバーのアプリケーション プロセスが、サーバーのデータベースに接続できません。

次の図は、プライマリ サーバーの HA 状態の変化を示しています。



次の図は、セカンダリ サーバーの HA 状態の変化を示しています。



ハイ アベイラビリティ CLI コマンド リファレンス

次の表に、HA 管理に使用できる CLI コマンドをリストします。これらのコマンドを使用するには、管理 CLI ユーザーとしてログインする必要があります。出力には、使用しているサーバーのステータスが反映されます。つまり、プライマリ サーバーから **ncs ha status** を実行すると、Cisco EPN Manager によってプライマリ サーバーのステータスが報告されます。

表 *63* : ハイ アベイラビリティ コマンド

コマンド	説明
ncs ha ?	コマンドの使用方法に関するメッセージを表示します。
ncs ha authkey *newAuthkey*	認証キーを *newAuthKey* に更新します。
ncs ha remove	HA 設定を削除します。
ncs ha status	HA の現在のステータスを表示します。

HA 認証キーのリセット

管理者権限を持つユーザーは、**ha authkey** コマンドを使用して HA 認証キーを変更できます。新しい認証キーがパスワード標準を満たすようにする必要があります。

ステップ 1 Cisco EPN Manager CLI 管理ユーザーとしてプライマリ サーバーにログインします（Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）を参照）。

ステップ 2 コマンドラインに次のように入力します。

ha authkey *newAuthKey*

newAuthKey は新しい認証キーです。

GUI での HA の削除

既存の HA 実装を削除するには、以下の手順で説明するように、GUI を使用するのが最も簡単な方法です。また、コマンド ラインから HA 設定を削除することもできます。

この方法を使用するには、プライマリ Cisco EPN Manager サーバーの現在の状態が「プライマリアクティブ（Primary Active）」であることを確認する必要があります。何らかの理由でセカンダリ サーバーが現在アクティブである場合、フェールバックが完了してセカンダリ サーバーが自動的に再起動してから、フェールバックを実行して HA 設定を削除します。

ステップ 1 管理者権限を持つユーザー ID を使用してプライマリ Cisco EPN Manager サーバーにログインします。

ステップ 2 [管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]>[HA 設定（HA Configuration）] の順に選択します。

ステップ 3 [削除（Remove）] を選択します。HA 設定の削除には 3 ～ 4 分かかります。

削除が完了したら、ページに表示されている HA 設定モードが「HA 未設定（HA not Configured）」になっていることを確認します。

CLI での HA の削除

何らかの理由でプライマリ サーバー上の Cisco EPN Manager GUI にアクセスできない場合、管理者は以下の手順に従い、コマンド ラインから HA 設定を削除することができます。

この方法を使用するには、プライマリ Cisco EPN Manager サーバーの現在の状態が「プライマリアクティブ（Primary Active）」であることを確認する必要があります。何らかの理由でセカンダリ サーバーが現在アクティブである場合、フェールバックが完了してセカンダリ サーバーが自動的に再起動してから、フェールバックを実行して HA 設定を削除します。

ステップ 1 CLI を使用してプライマリ サーバーに接続します。「configure terminal」モードにしないでください。

ステップ 2 コマンドラインに次のように入力します。

admin# **ncs ha remove**。

アップグレード中の HA の削除

HA を使用した Cisco EPN Manager 実装をアップグレードするには、以下の手順に従います。

ステップ 1 GUI を使用して、プライマリ サーバーから HA 設定を削除します。「GUI での HA の削除 （1154 ページ）」を参照してください。

ステップ 2 必要に応じてプライマリ サーバーをアップグレードします。

ステップ 3 現在のイメージを使用してセカンダリ サーバーを再インストールします。

セカンダリ サーバーを以前のバージョンやベータ版からアップグレードすることはできません。セカンダリ サーバーは常に新規インストールでなければなりません。

ステップ 4 アップグレードが完了したら、HA 設定プロセスを再度実行します。

復元中の HA の削除

Cisco EPN Manager は、ハイ アベイラビリティ関連の構成時の設定をバックアップしません。HA を使用した実装を復元する場合は、データをプライマリ サーバーのみに復元する必要があります。復元されたプライマリ サーバーは、そのデータを自動的にセカンダリ サーバーに複製します。セカンダリ サーバーで復元を実行しようとすると、Cisco EPN Manager によってエラー メッセージが生成されます。

HA を使用している実装を復元する場合は、次の手順を実行してください。

1. GUI を使用して、プライマリ サーバーから HA 設定を削除します。「GUI での HA の削除 （1154 ページ）」を参照してください。
2. プライマリ サーバーでデータを復元します。「Cisco EPN Manager データの復元 （945 ページ）」を参照してください。
3. 復元プロセスが完了したら、HA 設定プロセスを再度実行します。プライマリ サーバーとセカンダリ サーバー間の HA の設定方法 （1119 ページ） を参照してください。

サーバーの IP アドレスまたはホスト名のリセット

プライマリ サーバーまたはセカンダリ サーバーの IP アドレスまたはホスト名は、できるだけ変更しないようにしてください。IP アドレスまたはホスト名を変更しなければならない場合は、変更を行う前に、プライマリ サーバーから HA 設定を削除します。変更が終わったら、HA を再登録します。

任意の状態の TOFU エラーの解決

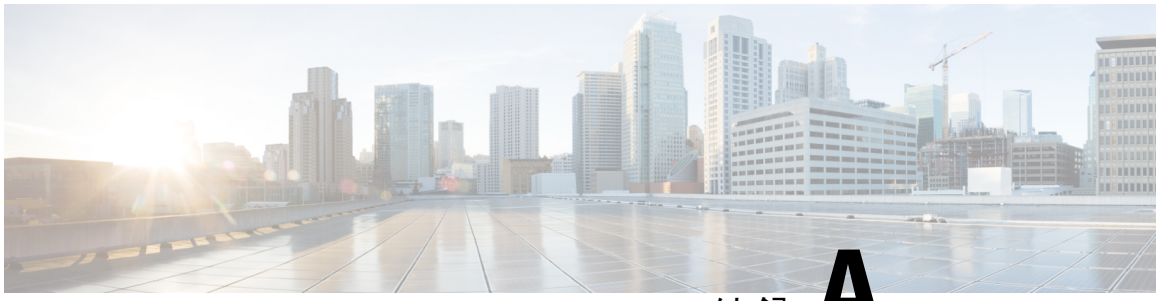
プライマリサーバーとセカンダリサーバーが通信する場合、次の TOFU エラーが発生する可能性があります。

続行する前に、次のエラーを修正する必要があります。「この接続には、ゼロトラスト（*TOFU*）ベースの証明書が設定されています。リモートホストの現在の証明書は、以前に使用されていたものとは異なります。（*A Trust-on-first-use (TOFU) based Certificate is configured for this connection. The current certificate on the remote host is different than what was used earlier.*）」

この問題を解決する手順は、次のとおりです。

- プライマリサーバーとセカンダリサーバーの両方で NCS CLI コマンドを使用して既存の証明書をクリアします。

```
ncs certvalidation tofu-certs deletecert host <server-hostname>
```



付録 A

ベスト プラクティス：Cisco EPN Manager のセキュリティ強化

セキュリティを強化するには、次のコンポーネントがセキュリティ メカニズムを最適化できるように調整する必要があります。

- Cisco EPN Manager Web サーバー
- Cisco EPN Manager サーバー
- Cisco EPN Manager ストレージ システム（ローカルまたは外部）
- Cisco EPN Manager とデバイス間の通信
- ユーザー認証システム（ローカルまたは外部）
- Network Time Protocol（NTP）を使用する時刻同期システム

この付録ではまず、管理者が知っておくべきいくつかの主要なセキュリティの概念を紹介します。次に、Cisco EPN Manager のセキュリティを最適化するために実行する必要がある特定のタスクについて説明します。

主要なセキュリティ概念

Cisco EPN Manager 製品のセキュリティの最適化を目指す管理者は、次のセキュリティ概念をよく理解しておく必要があります。

HTTPS

Hypertext Transfer Protocol Secure（HTTPS）では、チャネルを介して送信されるデータの暗号化に、セキュア ソケット レイヤ（SSL） またはその後続の標準規格である Transport Layer Security（TLS）が使用されます。SSL で複数の脆弱性が見つかったため、Cisco EPN Manager では現在 TLS のみがサポートされています。

（注） TLS は大まかに SSL と呼ばれることが多いため、本ガイドでもこの表記に従います。

SSL は、プライバシー、認証、およびデータ整合性を組み合わせることで、クライアントとサーバーの間のデータ転送を保護します。これらのセキュリティメカニズムを有効にするために、SSL は証明書、秘密キー/公開キー交換ペア、および Diffie-Hellman 鍵共有パラメータを使用します。

（注） デバイスで HTTPSS 通信に使用している TLS のバージョンが 1.2 未満の場合、デバイスデータベースのバックアップは失敗します。たとえば、NCS2000/ONS 10.5 バージョンなどです。

SSL 証明書

SSL 証明書と秘密キー/公開キー ペアは、ユーザー認証および通信パートナーの ID 検証に使われるデジタル ID の一種です。VeriSign や Thawte などの認証局（CA）は、エンティティ（サーバーまたはクライアント）を識別するための証明書を発行します。クライアントまたはサーバー証明書には、発行認証局の名前とデジタル署名、シリアル番号、証明書が発行されたクライアントまたはサーバーの名前、公開キー、および証明書の有効期限が含まれます。CA は、1 つ以上の署名証明書を使用して SSL 証明書を作成します。各署名証明書には、CA 署名の作成に使用される照合秘密キーがあります。CA は署名付き証明書（公開キーが埋め込まている）を簡単に入手できるようにしているため、誰でもその証明書を使用して、SSL 証明書が実際に特定の CA によって署名されたことを確認できます。

一般に、ハイ アベイラビリティ（HA）と非 HA の両方の環境で証明書を設定するには、次の手順が必要です。

1. サーバーの ID 証明書を生成する。
2. サーバーに ID 証明書をインストールする。
3. 対応するルート証明書をクライアントまたはブラウザにインストールする。

実行する必要がある具体的なタスクは、ご利用の環境によって異なります。

次の点に注意してください。

- サーバーの開始/停止シーケンシングは、HA 環境で慎重に行う必要があります。

- 仮想 IP アドレスが設定されている非 HA 環境では、より複雑な証明書要求プロセスを完了する必要があります。

1 方向 SSL 認証

これは、クライアントが適切なサーバー（中間サーバーではなく）に接続していることを保証する必要がある場合に使用される認証方法で、オンライン バンキングの Web サイトなどのパブリック リソースに適しています。認証は、クライアントがサーバー上のリソースへのアクセスを要求したときに開始されます。リソースが存在するサーバーは、その ID を証明するために、サーバー証明書（別名 SSL 証明書）をクライアントに送信します。クライアントは受信したサーバー証明書を、クライアントまたはブラウザにインストールする必要がある別の信頼できるオブジェクト（サーバー ルート証明書）と照合して検証します。サーバーの検証後、暗号化された（つまりセキュアな）通信チャネルが確立されます。ここで、Cisco EPN Manager サーバーは HTML フォームへの有効なユーザー名とパスワードの入力を求めます。SSL 接続が確立された後にユーザー クレデンシャルを入力すると、未認証の第三者による傍受を防ぐことができます。最終的に、ユーザー名とパスワードが受け入れられた後、サーバー上に存在するリソースへのアクセスが許可されます。

（注） クライアントは複数のサーバーとやり取りするために、複数のサーバー証明書を格納する必要がある場合があります。

クライアントにルート証明書をインストールする必要があるかどうかを判断するには、ブラウザの URL フィールドでロック アイコンを探します。通常このアイコンが表示される場合は、必要なルート証明書がすでにインストール済みであることを示します。多くの場合、これはより大きいいずれかの認証局（CA）によって署名されたサーバー証明書に該当します。一般的なブラウザではこれらの CA からのルート証明書が含まれているからです。

クライアントがサーバー証明書に署名した CA を認識しない場合は、接続がセキュリティで保護されていないことを意味します。これは必ずしも大きな問題ではなく、接続するサーバーの ID が検証されていないことを示しているだけです。1 つは必要なルート証明書をクライアント

またはブラウザにインストールできます。ブラウザの URL フィールドにロック アイコンが表示された場合は、証明書が正常にインストールされたことを意味します。

Cisco EPN Manager セキュリティ強化の概要

Cisco EPN Manager のセキュリティを強化するには、次のタスクを完了する必要があります。

（インストール時）

- HTTPS の設定、スタンドアロン サーバーおよび HA 環境の 1 方向 SSL 認証のセットアップ
- 非セキュア ポートと未使用ポートのシャットダウン
- ネットワーク ファイアウォールの設定
- 外部認証の設定

（インストール後）

- 変更（新しいホスト名または IP アドレスの設定など）に応じた証明書の更新
- 必要に応じた Cisco EPN Manager サーバーの強化

主な情報源として、シスコの担当者が各導入環境に固有のサーバー強化ガイダンスをご提供しますが、以下の手順に従って Cisco EPN Manager を保護することもできます。

強化手順	強化手順の対象：
HTTPS を使用した Web サーバー接続の保護 （1161 ページ）	Cisco EPN Manager Web サーバー
Web クライアントの証明書ベースの認証の設定 （1161 ページ）	
サーバーでの OCSP の設定と管理 （1164 ページ）	
非セキュアなポートおよびサービスの無効化 （1165 ページ）	Cisco EPN Manager サーバー
SNMPv3 を使用した Cisco EPN Manager とデバイス間の通信の強化（914 ページ）	
CLI を使用した外部認証の設定 （915 ページ）	
日常業務に不要なアカウントの無効化 （1166 ページ）	
NTP の強化 （918 ページ）	
Cisco EPN Manager ストレージの強化 （1166 ページ）	Cisco EPN Manager ストレージ システム（ローカルまたは外部）

Cisco EPN Manager Web サーバーの強化

Cisco EPN Manager Web サーバーを強化するには、以下を実行します。

1. HTTPS を使用した Web サーバー接続の保護 （1161 ページ）
2. Web クライアントの証明書ベースの認証の設定 （1161 ページ）
3. サーバーでのカスタム OCSP レスポンダの設定 （1164 ページ）

HTTPS を使用した Web サーバー接続の保護

Cisco EPN Manager Web サーバーは、HTTP の代わりに HTTPS を使用するように設定されている必要があります。これにより、Cisco EPN Manager Web サーバーに接続するシステムが保護され、いずれかのクライアントが Web サーバーやその他の参加システムに間接的に侵入する可能性が回避されます。HTTPS では、Web サーバー内の認証局（CA）証明書と、適切な SSL メカニズムを使用することが必要です。セットアップ方法の詳細は。

Web クライアントの証明書ベースの認証の設定

セキュリティを強化するには、Cisco EPN Manager サーバーでクライアント認証に証明書ベースの認証を使用する必要があります。この認証方式では、Cisco EPN Manager は最初にクライアントに関連付けられている証明書を検証してクライアントが正当であることを確認し、次にユーザー名とパスワードを検証します。このメカニズムにより、未承認のマシン（証明書が存在しないマシン）は Web サーバーに接続できません。Cisco EPN Manager はオンライン証明書ステータス プロトコル（OCSP）を使用してこの機能を実行します。

（注） このトピックで説明する証明書は、クライアントを一意に識別します。これは、HTTPS 操作の設定に使用された *Web* サーバーの証明書とは異なります。この手順は、Web サーバー証明書の CER ファイルの生成手順に似ていますが、完全に同一というわけではありません。場合によっては、その他のツール（OpenSSL など）を使用する必要があります。また、CA 証明書ファイルの生成方法は複数あります。サポートが必要な場合は、シスコ担当者にお問い合わせください。

証明書ベースの認証を設定するには、次の手順を実行します。

ステップ 1 CA を使用してクライアント証明書ファイルを生成します。これには、通常次の手順が含まれます。

a) 公開キーを生成します。
b) 公開キーを含む CSR ファイルを生成します。
c) 証明書ファイルを取得するため、CSR ファイルを CA に送信します。
d) 複数のファイルを受信する場合は、ファイルを連結して 1 つの CER/PEM ファイルを作成しないでください。代わりに次のようにします。

ベスト プラクティス：Cisco EPN Manager のセキュリティ強化

- クライアント マシンで保持するためにクライアント証明書ファイルをアプリケーション ユーザーに配布します。
- ルート CA 証明書とすべての中間 CA 証明書を維持します。これらの証明書は、ステップ 4 でサーバーにインポートします。

（注） ルート CA サーバーと中間 CA サーバーからこれらの証明書を取得する必要があります。信頼できないソースから受信したファイルは使用しないでください。

（注） クライアント CA 証明書を Web サーバーにインポートしないでください。このファイルは、クライアント マシン（挿入可能なカード、ハードウェアまたはソフトウェア トークン デバイスなど）で維持します。クライアント ブラウザが Cisco EPN Manager Web サーバーへの接続を試行すると、Web サーバーはクライアント ブラウザに対し、クライアント証明書を要求するよう指示します。ユーザーはクライアント証明書を提供し、ユーザー名とパスワードを入力する必要があります。

ステップ 2 Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）の説明に従って、コマンド ラインを使用して、Cisco EPN Manager サーバーにログインします。コンフィギュレーション モードを開始しないでください。

ステップ 3 ルート CA 証明書ファイルと中間 CA 証明書ファイルを、1 つずつ Cisco EPN Manager Web サーバーにインポートします。

a) このコマンドでルート CA 証明書ファイルをインポートします。

```
ncs key importcacert aliasName rootCACertFile repository repoName
```

ここで、

- *aliasName* は CA 証明書に対して指定されている短い名前です。
- *rootCACertFile* はルート CA 証明書ファイル名です。
- *repoName* は証明書ファイルが格納されている Cisco EPN Manager リポジトリの場所です。

（注） このコマンドは、サーバー証明書を適用するコマンドとは大きく異なることに注意してください。

b) このコマンドで中間 CA 証明書ファイルをインポートします。

```
ncs key importcacert aliasName intermediateCACertFile repository repoName
```

ここで、

- *intermediateCACertFile* は中間 CA 証明書ファイル名です。

ステップ 4 サーバーを再起動します。展開環境がハイ アベイラビリティに対応して設定されているかどうかに応じて、実行する手順は異なります。

ハイ アベイラビリティを使用しない展開環境では、変更を適用するため Cisco EPN Manager サーバーを再起動します。

ベスト プラクティス：Cisco EPN Manager のセキュリティ強化

```
ncs stop
ncs start
```

ハイ アベイラビリティを使用する展開環境では、次の手順に従い、サーバーを正しい順序で再起動します。

a) セカンダリ サーバーで Cisco EPN Manager CLI admin ユーザーとしてログインし、サーバーを停止します。

```
ncs stop
```

（注） ステップ 5（e）まではセカンダリ サーバーを再起動しないでください。

b) セカンダリ サーバーが停止していることを確認します。

c) プライマリ サーバーで Cisco EPN Manager CLI admin ユーザーとしてログインし、サーバーを停止します。

```
ncs stop
```

（注） ステップ 5（f）まではプライマリ サーバーを再起動しないでください。

d) プライマリ サーバーが停止していることを確認します。

e) セカンダリ サーバーで、次のコマンドを実行します。

1. **ncs start** コマンドを実行してサーバーを再起動します。
2. セカンダリ サーバーが再起動したことを確認します。
3. **ncs status** コマンドを実行して、ヘルス モニター プロセスが実行中であることを確認します。
4. **ncs ha status** コマンドを実行し、セカンダリ サーバーの HA ステータスが [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] であることを確認します。

f) プライマリ サーバーで、次のコマンドを実行します。

1. **ncs start** コマンドを実行してサーバーを再起動します。
2. プライマリ サーバーが再起動したことを確認します。
3. **ncs status** コマンドを実行して、ヘルス モニター プロセスとその他のプロセスが再開していることを確認します。

プライマリ サーバーですべてのプロセスが稼働したら、セカンダリ サーバーとプライマリ サーバーの間で HA 登録が自動的にトリガーされます（また、登録されている電子メール アドレスに電子メールが送信されます）。自動 HA 登録は通常、数分で完了します。

g) プライマリ サーバーとセカンダリ サーバーで **ncs ha status** コマンドを実行し、両方のサーバーの HA ステータスを確認します。次が表示されます。

- プライマリ サーバーの状態は [プライマリ アクティブ（Primary Active）] です。

• セカンダリ サーバーの状態は [セカンダリ同期（Secondary Syncing）] です。

サーバーでの OCSP の設定と管理

Online Certificate Status Protocol（OCSP）は、OCSP レスポンダを使用して Web クライアントの証明書ベース認証を可能にします。通常、OCSP レスポンダの URL は証明書の Authority Information Access（AIA）から読み取られます。フェールオーバー メカニズムとして、Cisco EPN Manager サーバーで OCSP レスポンダの URL を設定します。

サーバーでのカスタム OCSP レスポンダの設定

Cisco EPN Manager サーバーでカスタム OCSP レスポンダの URL を設定する手順は次のとおりです。

ステップ 1 Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）の説明に従って、コマンド ラインを使用して、Cisco EPN Manager サーバーにログインします。コンフィギュレーション モードを開始しないでください。

ステップ 2 （オプション）次のコマンドを入力して、サーバーに設定されている内容を確認できます。

```
show security-status
```

ステップ 3 次のコマンドを入力して、クライアント証明書認証を有効化します。

```
ncs run client-auth enable
```

ステップ 4 次のコマンドを入力して、カスタム OCSP レスポンダ URL を有効にし、証明書の OCSP レスポンダ URL の値を上書きします。

```
ncs certvalidation custom-ocsp-responder enable
```

ステップ 5 次のコマンドを入力して、カスタム OCSP レスポンダの URL を設定します。

```
ncs certvalidation custom-ocsp-responder set url1 responderURL
```

ここで、

• *responderURL* は、クライアントの CA 証明書から取得される OCSP レスポンダ の URL です。

サーバーからのカスタム OCSP レスポンダの削除

Cisco EPN Manager サーバーで定義されている既存のカスタム OCSP レスポンダを削除する手順は次のとおりです。

ステップ 1 **show security-status** コマンドを実行して、サーバーに現在設定されているカスタム OCSP レスポンダを表示し、削除するレスポンダの番号を特定します。

ステップ 2 次のコマンドで OCSP レスポンダをサーバーから削除します。

```
ncs certvalidation custom-ocsp-responder clear url1
```

Cisco EPN Manager サーバーの強化

Cisco EPN Manager サーバーを強化するには、次の手順に従ってください。

1. 非セキュアなポートおよびサービスの無効化 （1165 ページ）
2. SNMPv3 を使用した Cisco EPN Manager とデバイス間の通信の強化 （914 ページ）
3. CLI を使用した外部認証の設定 （915 ページ）
4. 日常業務に不要なアカウントの無効化 （1166 ページ）
5. NTP の強化 （918 ページ）

非セキュアなポートおよびサービスの無効化

一般的なポリシーとして、不要なポートや非セキュアなポートをすべて削除する必要があります。まず、どのポートが有効になっているかを確認した後、ご使用の導入環境で Cisco EPN Manager の通常の機能を妨げることなく安全に無効化できるポートを判別する必要があります。これを行うには、開いているポートを一覧表示して、安全に無効化できるポートの一覧と比較します。

安全に無効化できるポートの一覧は、『Cisco Evolved Programmable Network Manager Installation Guide』、（Cisco EPN Manager で使用されるポートとサービスを示す）から取得できます。

有効になっているポートを確認するには、次の手順に従います。

ステップ 1 Cisco EPN Manager サーバーとの SSH セッションの確立 （967 ページ）の説明に従い、コマンド ラインを使用して Cisco EPN Manager にログインします。コンフィギュレーション モードを開始しないでください。

ステップ 2 show security-status コマンドは、現在開いている（有効化されている）サーバーの TCP/UDP ポート、システムで使用している他のサービスのステータス、およびその他のセキュリティ関連の設定情報を表示します。次のような出力が表示されます。

```
show security-status
Open TCP Ports       22 443 1522 8082
Open UDP Ports       162 514 9991
FIPS Mode            enabled
TFTP Service         disabled
FTP Service          disabled
JMS port (61617)     disabled
Root Access          disabled
Client Auth          enabled
```

```
OCSP Responder1      http://209.165.200.224/ocsp
OCSP Responder2      http://209.165.202.128/ocsp
```

ステップ 3 『Cisco Evolved Programmable Network Manager Installation Guide』にある、Cisco EPN Manager で使用されるポートの一覧表を調べて、その表にご使用のポートが示されているかどうかを確認します。この表を参考にすると、どのサービスがポートを使用しているか、およびどのサービスが不要で、安全に無効化できるかを判別できます。この場合の「安全」とは、製品に悪影響を及ぼさずにポートを安全に無効化できることを意味します。

（注） ポートまたはサービスを無効化する必要があるかどうかが不明の場合は、Cisco の担当者にお問い合わせください。

ステップ 4 Cisco EPN Manager GUI を使用して、非セキュア ポートを無効化します。

この例では、非セキュアなプロトコルとして無効化すべき FTP と TFTP を無効化します（代わりに SFTP または SCP を使用します）。TFTP および FTP は通常、ネットワーク デバイスと Cisco EPN Manager の間でファームウェアやソフトウェアのイメージを転送するために使用されます。

a) 管理者権限を持つユーザー ID を使用して Cisco EPN Manager にログインします。
b) **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバー（Server）]** を選択します。
c) [FTP] および [TFTP] の下で、[無効化（Disable）] を選択して [保存（Save）] をクリックします。
d) Cisco EPN Manager を再起動します。「Cisco EPN Manager の停止と再起動 （973 ページ）」を参照してください。

（注） ハイアベイラビリティ設定では、ハイアベイラビリティを設定する前に、セカンダリサーバーで FTP サービスおよび TFTP サービスが無効になっていることを確認します。詳細については、サーバーでの FTP/TFTP/SFTP サービスの有効化 （970 ページ）を参照してください。

ステップ 5 ネットワークにファイアウォールがある場合は、Cisco EPN Manager の動作に必要なトラフィックのみを許可するようにファイアウォールを設定してください。詳細については、『Cisco Evolved Programmable Network Manager Installation Guide』を参照してください（特に、Cisco EPN Manager で使用されるポートに関する情報と、推奨されるファイアウォール設定）。さらに支援が必要な場合は、Cisco の担当者にお問い合わせください。

日常業務に不要なアカウントの無効化

Cisco EPN Manager Web GUI のルート ユーザーは、ルート権限を持つ他の Web GUI ユーザーを 1 人以上作成した後に無効化する必要があります。Web GUI ルート ユーザーの無効化および有効化 （998 ページ） を参照してください。

Cisco EPN Manager ストレージの強化

データベース、バックアップ サーバーなど、Cisco EPN Manager のインストールに含めるすべてのストレージ要素を保護することをお勧めします。

内部ストレージまたは外部ストレージの強化の詳細については、シスコの担当者にお問い合わせください。外部ストレージの場合は、ストレージ ベンダーにもご連絡ください。

Cisco EPN Manager をアンインストールまたは削除する場合は、センシティブ データを含む可能性があるすべての VM 関連ファイルがデジタルで破棄（単に削除されるのではなく）されていることを確認してください。

NFS ベース ストレージの強化

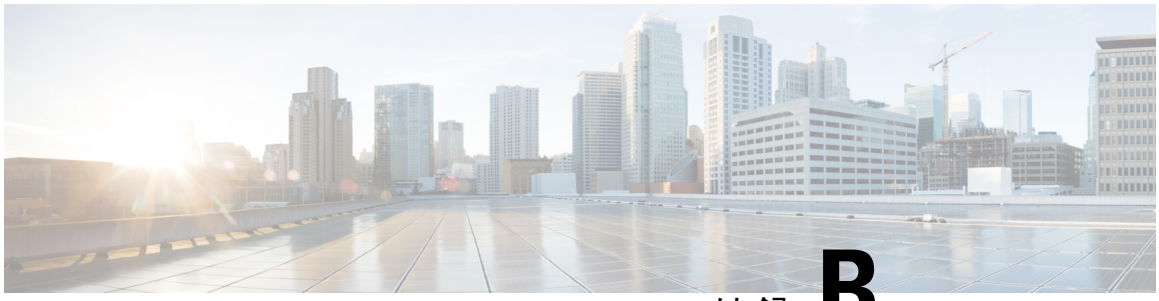
NFS には組み込みのセキュリティがないので、NFS サーバーをセキュアにするために次のセキュリティ対策をできる限り多く実装する必要があります。

- NFS サーバーの前にファイアウォールを設定します。実質的にはこれを行うには、NFS がさまざまな設定ファイルで使用するポートを固定し、ファイアウォールの設定でこれらのポートを指定します。
- ポート マッパーを使用します。NFS サーバーで、特定の IP アドレスを含む NFS トランザクションのみ許可します。
- 感染した DNS 経由の攻撃を防ぐには、NFS を構成するときに（ドメイン名ではなく）IP アドレスのみ指定します。
- フォルダのエクスポートを設定する際に、/etc/exports ファイルで [root_squash] オプションを使用します。
- /etc/exports ファイルを設定する際に、[セキュア（secure）] オプションを使用します。
- バックアップ ステージングとストレージ フォルダを設定する際に、[nosuid] と [noexec] マウント オプションを使用します。

（注） ステージング フォルダを設定することは必須ではありません。

- ストレージ フォルダ（およびオプションのステージング フォルダ）に対して、ファイル アクセス許可値 [755]（すべてのユーザーに読み取りおよび書き込み特権を付与）を設定し、userid [65534]（システム権限を持っていないユーザー [nobody]）を所有者として設定します。
- SSH または SSL/TLS のいずれかを介して NFS トラフィックをトンネリングします。SSH の場合、ユーザー認証ではなく RSA キーベースの認証を使用します。

NFS ベースのストレージの安全性のためには、これらの対策の 1 つのみに頼らないでください。最善策は、状況に合わせて最適な対策の組み合わせを実装することです。また、このリストは網羅的なものではないことに注意してください。ストレージを強化するときは、高レベルの信頼を達成するために、事前に Linux システム管理者およびセキュリティ専門家と状況について相談することをお勧めします。



付録 B

アイコンと状態の参照

デバイスの到達可能性状態と管理状態

デバイスの到達可能性状態：Cisco EPN Manager が設定されたすべてのプロトコルを使用してデバイスと通信できるかどうかを表します。

表 *64 :* デバイスの到達可能性状態

アイコン	デバイスの到達可能性状態	説明	トラブルシューティング
✅	到達可能	Cisco EPN Manager は、SNMP を使用してデバイスに、または ICMP を使用して NCS 2K デバイスにアクセスすることができます。	—

アイコンと状態の参照

	ping 到達可能	Cisco EPN Manager は、ping を使用してデバイスに到達できますが、SNMP 経由では到達できません。	ICMP ping は成功しますが、SNMP 通信が失敗する原因すべてをチェックします。デバイス SNMP クレデンシャルがデバイスと Cisco EPN Manager の両方で同じであること、SNMP がデバイス上で有効になっているかどうか、またはトランスポートネットワークが設定ミスなどの理由で SNMP パケットをドロップしていないかどうかをチェックします。基本的なデバイスプロパティの変更 （398 ページ）を参照してください。
	到達不能	Cisco EPN Manager は、ping を使用してデバイスに到達できません。	物理デバイスが動作中でネットワークに接続されていることを確認します。
	不明	Cisco EPN Manager は、デバイスに接続できません。	デバイスをチェックします。

デバイスの管理状態：デバイスの設定状態を表します（たとえば、デバイスが ping によって到達できないためにダウンしている場合や、管理者が手動でデバイスをシャットダウンした場合などです）。

表 *65*：デバイスの管理状態

デバイスの管理状態	説明	トラブルシューティング
管理対象	Cisco EPN Manager は、デバイスを積極的にモニターしています。	該当なし。
メンテナンス	Cisco EPN Manager は、デバイスの到達可能性をチェックしていますが、トラップ、syslog、または TL1 メッセージを処理していません。	デバイスを管理対象状態に移行するには、デバイスのメンテナンス状態の切り替え （86 ページ）を参照してください。

管理対象外	Cisco EPN Manager は、デバイスをモニターしていません。	[ネットワーク デバイス（Network Devices）] テーブルで、デバイスを特定し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列でデータの横にある [i] アイコンをクリックします。ポップアップ ウィンドウに、詳細とトラブルシューティングのヒントが表示されます。収集問題の一般的な原因は次のとおりです。 • デバイス SNMP クレデンシャルが間違っている。 • Cisco EPN Manager 展開がライセンスで許可されているデバイスの数を上回っている。 • デバイスがスイッチ パス トレース専用になっている。 デバイス タイプがサポートされていない場合は、その [デバイス タイプ（Device Type）] が [不明（Unknown）] になります。そのデバイス タイプのサポートが Cisco.com で提供されているかをチェックするには、**[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [ソフトウェアアップデート（Software Update）]** を選択してから、[更新の確認（Check for Updates）] をクリックします。
不明	Cisco EPN Manager は、デバイスに接続できません。	デバイスをチェックします。

デバイス同期状態

[デバイスの同期状態（Device Sync State）]：デバイスで実行された同期操作のステータスを示します。

表 *66*：デバイス同期状態

アイコン	デバイス同期状態	説明
	同期中	デバイスの同期を実行中です。
	完了	デバイスの同期が正常に完了しました。

	エラー/警告（Error/Warning）	以下の一覧に示すエラーまたは警告： • 追加開始（Add Initiated） • 収集の失敗（Collection Failure） • 警告付き完了（Completed with Warning） • 削除処理中（Delete In Progress） • サービス中（In Service） • サービスメンテナンス中（In Service Maintenance） • ライセンスなし • 収集一部失敗（Partial Collection Failure） • SNMP 接続失敗（SNMP Connectivity Failed） • SNMP ユーザー認証失敗（SNMP User Authentication Failed） • スイッチ ポート トレース（Switch Port Trace） • 誤った CLI クレデンシャル（Wrong CLI Credentials）

（注） サービスメンテナンスフィルタは、最後のインベントリ収集ステータスには使用できません。

ポートまたはインターフェイスの状態

ポートまたはインターフェイスのプライマリ状態：管理者と運用状態を組み合わせることでポートまたはインターフェイスの最も重要な状態情報を伝えます。[多層トレース（Multilayer Trace）]には、ポートのプライマリ状態またはアラーム状態が表示されます。[シャーシビュー（Chassis View）]の場合は、要素が状態変化を示す色の変化をサポートしていない場合でも、生成されたアラームから状態変更情報を取得できます。

（注） ポート/インターフェイスにアラームが関連付けられている場合、アラーム アイコンが表示され、ポートアイコンは表示されません。このアラームは、ポートがテスト中または管理ダウン状態でない場合にのみ表示されます。

アイコンと状態の参照

ポートまたはインターフェイスのプライマリ状態	アイコン	管理ステータス	動作状態
不明		不明	不明
ダウン		アップ	ダウン
テスト		テスト	—
管理上ダウン		管理上ダウン	—
アップ		アップ	アップ
自動アップ		アップ	自動アップ

ポートまたはインターフェイスの管理状態：ポートまたはインターフェイスの設定状態を表します（たとえば、管理者が手動でポートをシャットダウンした場合など）。

ポートまたはインターフェイスの管理状態	アイコン	説明
不明		ポートまたはインターフェイスの管理状態は不明です。デバイスからの応答（または不十分な応答）はありません。
管理上ダウン		ポートまたはインターフェイスは管理者によって手動でシャットダウンされました。
アップ		ポートまたはインターフェイスは管理者によって有効にされています。
テスト		ポートまたはインターフェイスは管理者によってテストされています。

ポートまたはインターフェイスの動作状態：ポートまたはインターフェイスの実行状態と、それが適切に動作しているかどうかを伝えます。

ポートまたはインターフェイスの動作状態	アイコン	説明
不明		ポートまたはインターフェイスの動作状態は不明です。デバイスからの応答（または不十分な応答）はありません。
ダウン		ポートまたはインターフェイスは正しく動作していません。

アップ		ポートまたはインターフェイスがデータを送受信しています。
自動アップ		ポートまたはインターフェイスがデータを送受信しています（特定のデバイスのみがこの状態をサポートしています。他のデバイスは [アップ（Up）] を使用します）。

回線または VC の状態

[回線/VC のプライマリ状態（Circuit or Primary States）]：サービサビリティ、検出、アラーム、プロビジョニングの順に回線に関する最も重要な状態情報を伝達します。これは、通常、回線または VC のテーブル内の最初の列に表示されます。

回線または VC のプライマリ状態（Circuit or VC Primary States）	アイコン	サービサビリティ	検出	Alarm	プロビジョニング
欠落（Missing）		—	欠落（Missing）	—	—
Down		Down	—	—	—
クリティカル（Critical）		—	—	クリティカル（Critical）	—
[メジャー（Major）]		—	—	[メジャー（Major）]	—
[マイナー（Minor）]		—	—	[マイナー（Minor）]	—
一部ダウン		一部	—	—	—
管理上ダウン		管理上ダウン	—	—	—
一部検出		—	一部	—	—
失敗しました（Failed）		—	—	—	（作成、変更、または削除）失敗
進行中		—	—	—	（作成、変更、または削除）進行中

アイコンと状態の参照

警告			—	警告	—
アップ		アップ	—	—	—
自動アップ		自動アップ	—	—	—
情報（Info）		—	—	情報（Info）	—
クリア済み		—	—	クリア済み	—

[回線/VC のサービサビリティ状態（Circuit or VC Serviceability）]：この値は、回線または VC の管理状態と動作状態の組み合わせです。サービスの運用性に影響するため、管理状態が表示されます。光回線の場合は、管理状態によってアクティブ化および非アクティブ化アクションが使用可能かどうかも決定されます。動作状態は、サービスが機能しているかどうかをすばやく特定するために表示されます。

回線または VC のサービサビリティ状態	アイコン	説明
管理上ダウン		管理者が回線または VC を手動でシャットダウンします。
ダウン（Down）		回線または VC は運用上はダウンし、管理上はアップします。
アップ（Up）		回線または VC は、運用上も、管理上もアップします。
自動アップ（Auto Up）		回線または VC は運用上は自動アップ、管理上はアップします。特定のデバイスのみが自動アップの動作状態をサポートしています。
取得不可		回線または VC はまだ検出されていないか、その動作ステータスが取得できません。
一部		回線/VC の動作状態または管理状態が部分的です。 • [部分管理状態（Partial admin state）]：回線または VC に（一部のサービス リソースをアクティブ化し、他のリソースを非アクティブ化する）混在管理要求があるか、または管理上アップしているリソースとダウンしているリソースが混在しているか、あるいは動作状態が取得できないリソースがあります。 • [部分動作状態（Partial operational state）]：回線または VC に一部のリソースのアクティブ化と非アクティブ化が混在しているか、またはリソースの一部の動作状態が取得できません。

アイコンと状態の参照

Up - Unprotected		保護パスで設定された回線/VC は動作していますが、重大な障害が原因で代替パスに切り替えることはできません。 （注） このサービスアビリティ ステータス表示は、Y 字型ケーブル保護および保護 ODU を使用した OCHCC WSON 回線でサポートされます。

次の表に、さまざまなシナリオでの回線/VC の有用性状態の詳細を示します。

テクノロジー	サービス タイプ	シナリオ	サービスアビリティ状態

キャリア イーサネット	EPL、EVPL、アクセス EPL、およびアクセス EVPL	エンドポイント（サービスインスタンス/サブインターフェイス）、クロス接続、およびサービスに参加している疑似回線の動作状態がアップの場合	アップ
		サービスに参加している送信元と宛先（サービスインスタンス/サブインターフェイス）の両方の管理状態がダウンの場合	管理上ダウン
		他のすべてのシナリオで、サービスに参加している1つ以上のエンドポイント（サービスインスタンス/サブインターフェイス）、クロス接続、または疑似回線がダウンしている場合	ダウン（Down）
	EP-LAN、EVP-LAN、EP ツリー、および EVP ツリー	サービスに参加しているすべてのエンドポイント（サービスインスタンス/サブインターフェイス）、ブリッジドメイン、VFI、および疑似回線がアップしている場合	アップ（Up）
		サービスに参加している2つ以上のエンドポイント（サービスインスタンス/サブインターフェイス）の動作状態がアップで、残りのエンドポイントがダウンの場合	一部
			管理上ダウン

アイコンと状態の参照

		サービスに参加しているすべてのエンドポイント（サービスインスタンス/サブインターフェイス）の管理状態がダウンの場合	
		サービスに参加している1つ以上のエンドポイント（サービスインスタンス/サブインターフェイス）の動作状態がアップで、残りのエンドポイントがダウンの場合	ダウン（Down）
回線エミュレーション（Circuit Emulation）	すべてのサービスタイプ	サービスに参加しているエンドポイント（cemGroup）、基盤となっている TDM コントローラ、クロス接続、および疑似回線の動作状態がアップの場合	アップ（Up）
		サービスに参加している送信元と宛先のエンドポイント（cemGroup）の両方の管理状態がダウンの場合	管理上ダウン
		他のすべてのシナリオで、サービスに参加しているエンドポイント（cemGroup）、基盤となっている TDM コントローラ、クロス接続、および疑似回線のいずれかの動作状態がダウンの場合	ダウン（Down）

MPLS	単方向 TE トンネル（Unidirectional TE Tunnel）	トンネルインターフェイスの動作状態がアップの場合	アップ（Up）
		トンネルインターフェイスの管理状態がダウンの場合	管理上ダウン（Admin Down）
		他のすべてのシナリオでは、トンネルの動作状態がダウンの場合	ダウン（Down）
	双方向 TE トンネル（Bidirectional TE Tunnel）	トンネルの両端のインターフェイスの動作状態がアップの場合	アップ（Up）
		トンネルの両端のインターフェイスの管理者状態がダウンの場合	管理上ダウン（Admin Down）
		それ以外の場合は、トンネルインターフェイスの動作状態がダウンの場合	ダウン（Down）

アイコンと状態の参照

シリアル（Serial）	RS232、RS422、および RS485	サービスに参加しているエンドポイント（channelGroup）、基盤となっているシリアルインターフェイス、クロス接続、および疑似回線の動作状態がアップの場合	アップ
		サービスに参加している送信元と宛先のエンドポイント（channelGroup）の両方の管理状態がダウンの場合 送信元または宛先のエンドポイント（channelGroup）のいずれかの管理状態がダウンの場合	管理上ダウン（Admin Down）
		他のすべてのシナリオで、サービスに参加しているエンドポイント（channelGroup）、基盤となっているシリアルインターフェイス、クロス接続、および疑似回線のいずれかの動作状態がダウンの場合	ダウン（Down）
	raw ソケット（Raw Socket）	サーバーと関連付けられているそのすべてのクライアントセッションがアップの場合	アップ（Up）
		サーバーがアップで、関連付けられているそのすべてのクライアントセッションがダウンの場合	ダウン（Down）
			管理上ダウン（Admin Down）

		サービスに参加している送信元と宛先のエンドポイント（channelGroup）の両方の管理状態がダウンの場合 サーバーの管理状態、または参加しているすべてのクライアントの管理状態がダウンの場合	
		サーバーと、関連付けられているそのすべてのクライアント セッションがダウンの場合	ダウン（Down）
		サーバーがアップで、関連付けられているそのいずれかのクライアントがアップの場合	部分（Partial）

アイコンと状態の参照

レイヤ 3 VPN（Layer 3 VPN）		サービスに参加しているすべてのエンドポイント（サブインターフェイス、BDI、およびBVI）の動作状態がアップの場合	アップ
		サービスに参加している少なくとも 2 つのエンドポイント（サブインターフェイス、BDI、および BVI）の動作状態がアップで、残りのエンドポイントがダウンの場合	Partial
		サービスに参加しているすべてのエンドポイント（サブインターフェイス、BDI、およびBVI）の管理状態がダウンの場合	管理上ダウン
		サービスに参加している 1 つ以上のエンドポイント（サブインターフェイス、BDI、およびBVI）の動作状態がアップで、残りのエンドポイントがダウンの場合	ダウン（Down）
SR TE	SR ポリシー	SR ポリシーの動作状態がアップしている場合	アップ（Up）
		SR ポリシーの管理状態がダウンしている場合	管理上ダウン（Admin Down）
		他のすべてのシナリオでは、SR ポリシーの動作状態がダウンの場合	ダウン（Down）

[回線または VC の検出状態（Circuit or VC Discovery State）]：サービスとそのコンポーネントのネットワークから検出された最新の状態と構造を表します。検出されたバージョンがある場

アイコンと状態の参照

合は、アプリケーションが実際にサービス自体をモニターしている（たとえば、有意義な動作データとパフォーマンス データを定義できる）ことを意味します。

回線または VC の検出状態（Circuit or VC Discovery State）	アイコン	説明
一部		Cisco EPN Manager によって部分的に検出された回線または VC。その想定エンティティのすべてが検出されたわけではありません。
完全（Full）		Cisco EPN Manager によって完全に検出された回線または VC。そのため、Cisco EPN Manager は、サービスをモニターして、有意義な動作データとフォーマンス データを提供できます。
欠落（Missing）		まだ Cisco EPN Manager によって検出されていない（ただし、プロビジョニング済みである可能性がある）回線または VC。
Resync		回線または VC は再同期されています。

[回線または VC のプロビジョニング状態（Circuit or VC Provisioning State）]：回線または VC についてプロビジョニングする目的があるかどうかと、目的がある場合はそのステータスを表します。調整レポートが生成された場合は、調整アクションの状態が反映されます。

回線または VC プロビジョニングの状態	アイコン	説明
なし（None）		回線または VC が検出されましたが、まだプロビジョニングされていません。回線/VC は変更または削除する場合にプロモートする必要があります。
失敗しました（Failed）		アクションが失敗しました。
進行中（In Progress）		アクションは開始されましたが、まだ完了していません。
計画済み		アクションは計画されましたが、まだ開始されていません。
成功		アクションは正常に完了しました。

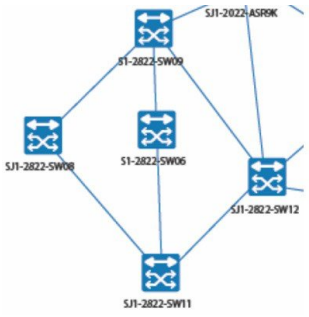
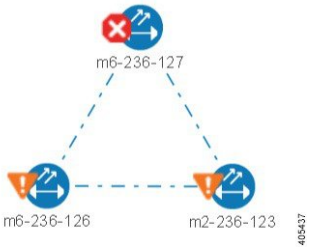
リンクの有用性状態

サービスアビリティ状態	アイコン	説明
管理上ダウン		リンクは意図的に管理者によってシャットダウンされました。
ダウン		リンクがダウンしています（ただしダウンは不適切な状態）。
アップ		リンクはアップの状態で、トラフィックがリンクを通過しています。
自動アップ		信号が検出されたためリンクはアップ状態です（この状態は光デバイスでのみサポートされています）。
取得不可		リンクがまだ検出されていないか、またはそのステータスが取得できません。
一部		リンクの要求、リソース、またはリソース状態に不一致があります。例： • リンクが、一部のサービス リソースをアクティブ化し、他のサービス リソースを非アクティブにする要求を処理している。 • リンクにいくつかのアクティブ リソースといくつかの非アクティブ リソースがある。 • アップしているリンク リソースとダウンしているリンク リソースがある。 • リンクのリソースのいずれかの状態が不明である。

リンクの特徴

以下の表では、Cisco EPN Manager の [トポロジマップ（Topology Map）] ビューでデバイス間の接続を表すために使用されるさまざまなタイプのリンクについて説明します。

リンク タイプ	説明

	[実線（Solid Line）]：2 つのデバイス間のリンクなど、物理リンク、トポロジ リンク、またはサービス リンクを示します。
	[破線（Dashed Line）]：EVC、VPLS サービス インスタンス、または VPN コンポーネントなど、要素間の関連性またはビジネス リンクを示します。

機器の動作状態（シャーシ ビュー）

機器の動作状態はネットワーク要素の実行状態を表しています。

機器の動作状態	アイコン	説明
サービス中（In Service）	（なし）	機器が正常に動作しています。
事前プロビジョニング済み		（Cisco NCS 2000 および Cisco ONS デバイスのみ）機器は設定されていますが、シャーシには物理的に存在していません。
失敗/無効/ダウン/休止中/メンテナンス中のため休止中		機器は正常に動作していません。
不明		機器の動作状態は不明です。デバイスからの応答はありません（または不十分な応答）。

アラーム重大度アイコン

次の表に、Web GUI のさまざまな部分に表示されるアイコンのアラームの色とその重大度を示します。

重大度アイコン	説明	カラー
	クリティカル アラーム	赤
	メジャーアラーム	オレンジ
	マイナーアラーム	黄
	警告アラーム	ライト ブルー
	アラームはクリア済み。正常、OK	緑
	情報アラーム	青
	不確定アラーム	暗い青色

デバイス タイプのアイコン

次の表では、Cisco EPN Manager の [トポロジ（Topology）] ビューと [マルチレイヤトレース（Multi-layer Trace）] ビューでさまざまなデバイス タイプを表すために使用されるアイコンを定義します。

アイコン	定義
	スイッチ（Switch）
	ルータ（Router）

アイコンと状態の参照

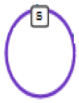
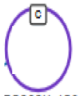
アイコン	定義
	ルータ集約
	セキュア ドメイン ルータ（SDR）が搭載された Cisco NCS 6000 デバイス。SDR の名前はデバイスのアイコン上に直接表示されます。 （注） クラスタまたはユーザー定義グループに属するデバイスの SDR ラベルが表示されない場合（自動クラスタリングがデバイスのプロキシミティに基づいてデバイスに適用されるため）などがあります。
	L3VPN サービスで構成されたルータ。
	スイッチ集約
	アクセス ポイント（Access Point）
	サービス モジュール
	UCS C シリーズ
	NAM ブレード
	グループ

アイコン	定義
	汎用デバイス
	仮想サーバー
	ワイヤレス LAN コントローラ
	[不明（Unknown）]
	DWDM ROADM 再生/NCS 2000

回線または VC ネットワーク トポロジ オーバーレイのアイコン

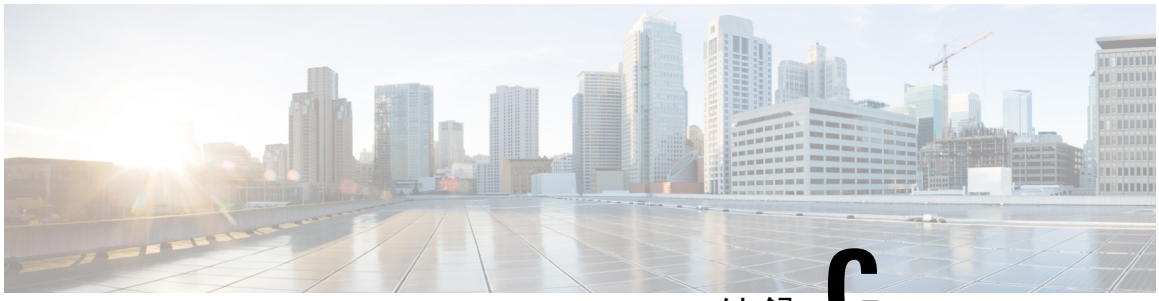
オーバーレイ アイコン	定義
	送信元エンドポイント
	宛先エンドポイント
	ローカル スイッチングを使用した EVC または CEM

アイコンと状態の参照

オーバーレイ アイコン	定義
	回線の作成中にユーザーによって追加されたエンドポイント。 （注） セグメント ルーティング テクノロジー タイプの隣接およびノード SID の両方に「S」が表示されます。
	回線の作成中にユーザーによって除外されたエンドポイント。
	回線の作成中に追加または除外されたポートの一部を持つエンドポイント。このエンドポイントには、回線のさまざまなルートに参加している複数のポートが含まれています。
	ルートとして指定された E-TREE EVC エンドポイント。
	アイコンの S は、サーバーがデバイス上で設定されていることを示します。
	アイコンの C は、クライアントがデバイス上で設定されていることを示します。
	アイコンの S と C は、サーバーとクライアントの両方が同じデバイス上で設定されていることを表します。
	選択されたエンドポイント。
	ハブ：ハブとルートが同じデバイスにある場合（VPLS シナリオ）、ルート アイコンが茶色の丸で囲まれます。
	回線の作成中に追加されたリンク。
	回線の作成中に除外されたリンク。

アイコンと状態の参照

オーバーレイ アイコン	定義
	回線の作成中に追加または除外されたポートの一部を持つエンドポイント。これは、同じ回線のさまざまなルートに参加している複数のポートを含む集約リンクを表します。



付録 C

Cisco EPM Notification MIB

CISCO-EPM-NOTIFICATION-MIB

この付録では、CISCO-EPM-NOTIFICATION-MIB について説明します。

SNMP Varbind	データ タイプ	Varbind OID	SNMP Varbing の説明	例
cenAlarmVersion	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.2	この MIB のリリース バージョン。	1.0
cenAlarmTimestamp	Timestamp	.1.3.6.1.4.9.9.311.1.1.2.1.3	アラームが発生した時刻。 （注） これは、UTC の 1970 年 1 月 1 日（エポック以降）からの秒数です。	1523608787
cenAlarmUpdatedTimestamp	Timestamp	.1.3.6.1.4.9.9.311.1.1.2.1.4	アラームはしばらく存続し、フィールドが変更されると値が自動的に更新されます。更新時刻は時間を示します。各アラームは一意のアラーム インスタンス ID で識別されます。 たとえば、cenAlarmInstanceID などです。	1523608788
cenAlarmInstanceID	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.5	一意のアラーム インスタンス ID。	1185098114
cenAlarmStatus	整数（Integer）	.1.3.6.1.4.9.9.311.1.1.2.1.6	アラーム ステータスは、アラームのステータスを整数値で示します。	Active=2, Cleared=3

SNMP Varbind	データ タイプ	Varbind OID	SNMP Varbing の説明	例
cenAlarmStatusDefinition	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.7	アラームのステータスに関する簡単な説明。文字列は「,」タプルの形式で表されます。 値は、「cenAlarmStatus」属性が保持する値と同じです。生成されたアラームステータスの 1 行の説明が含まれます。	2、ACTIVE3、CLEARED
cenAlarmType	整数（Integer）	.1.3.6.1.4.9.9.311.1.1.2.1.8	• unknown(1)：この属性の値を特定できなかった場合。 • direct(2)：すべてのイベントが管理対象オブジェクトの観測をもとに報告される一連のイベントによって生成されたアラームを示します。 • indirect(3)：ネットワーク管理システムが指定した管理対象オブジェクトのステータスをもとにすべてのイベントが推定または推測される一連のイベントによって生成されたアラームを示します。 • mixed(4)：direct または indirect の一連のイベントによって生成されたアラームを示します。	2
cenAlarmCategory	整数（Integer）	.1.3.6.1.4.9.9.311.1.1.2.1.9	整数値で表される、生成されたアラームのカテゴリ。 （注） この整数フィールドは、EPN Manager では使用されません。代わりに、文字列で表す cenAlarmCategoryDefinition が使用されます。	—

SNMP Varbind	データ タイプ	Varbind OID	SNMP Varbing の説明	例
cenAlarmCategoryDefinition	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.10	生成されたアラームのカテゴリに関する簡単な説明。 文字列は「,」タプルの形式で表されます。値は、「cenAlarmCategory」属性が保持する値と同じです。生成されたアラームカテゴリの 1 行の説明が含まれます。 アラーム タイプのリストについては、次のドキュメントの「Alarm Name」列を参照してください。これらは2.1（Derecho）用です。その他のバージョンについては、cisco.com で公開されている必要なバージョンのドキュメントを使用してください。 Cisco Evolved Programmable Network Manager Supported SNMP Traps Cisco Evolved Programmable Network Manager のサポート対象 Syslog Cisco Evolved Programmable Network Manager のサポート対象 TL1 メッセージ Cisco Evolved Programmable Network Manager のサポート対象アラーム	"LINK_DOWN", "SWT_AUTH_FAIL", "LINK_UP"
cenAlarmServerAddressType	InetAddressType	.1.3.6.1.4.9.9.311.1.1.2.1.11	サーバーに到達可能なインターネット アドレスの種類。 サーバーは、このトラップを生成しているサーバーです。	0: unknown 1:ipv4 2:ipv6
cenAlarmServerAddress	InetAddress	.1.3.6.1.4.9.9.311.1.1.2.1.12	管理の IP アドレスまたは DNS 名。このアラームの発生元サーバーに通知されます。	10.127.101.145

SNMP Varbind	データ タイプ	Varbind OID	SNMP Varbing の説明	例
cmAlarmManagedObjectClass	SnmpAdminString	.1.3.6.1.4.1.9.9.311.1.1.2.1.13	このアラームが生成された管理対象オブジェクトのクラス。たとえば、ルータ、スイッチ、ゲートキーパー、音声ポートなどです。 カテゴリのリストについては、次のドキュメントの「Category」列を参照してください。これらは2.1（Derecho）用です。その他のバージョンについては、cisco.com で公開されている必要なバージョンのドキュメントを使用してください。 Cisco Evolved Programmable Network Manager Supported SNMP Traps Cisco Evolved Programmable Network Manager のサポート対象 Syslog Cisco Evolved Programmable Network Manager のサポート対象 TL1 メッセージ Cisco Evolved Programmable Network Manager のサポート対象アラーム	"Optical", "Carrier Ethernet"
cmAlarmManagedObjectAddressType	InetAddressType	.1.3.6.1.4.1.9.9.311.1.1.2.1.14	管理対象オブジェクトに到達可能なインターネット アドレスの種類。	0: unknown 1: ipv4 2: ipv6
cmAlarmManagedObjectAddress	InetAddress	.1.3.6.1.4.1.9.9.311.1.1.2.1.15	管理対象オブジェクトの IP アドレスまたは DNS 名。	2405:200:204:138::1723:9:121

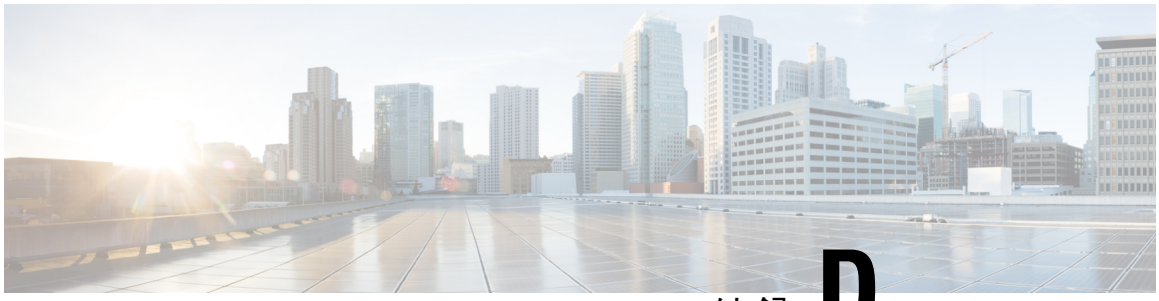
SNMP Varbind	データ タイプ	Varbind OID	SNMP Varbing の説明	例
cenAlarmDescription	OctetString	.1.3.6.1.4.9.9.311.1.1.2.1.16	アラームの詳細。 アラームの説明のリストについては、次のドキュメントの「Description/Probable Cause」列を参照してください。これらは 2.1（Derecho）用です。その他のバージョンについては、cisco.com で公開されている必要なバージョンのドキュメントを使用してください。 Cisco Evolved Programmable Network Manager Supported SNMP Traps Cisco Evolved Programmable Network Manager のサポート対象 Syslog Cisco Evolved Programmable Network Manager のサポート対象 TL1 メッセージ Cisco Evolved Programmable Network Manager のサポート対象アラーム	Port 'GigabitEthernet0/0/6' (Description: ' # TO GigabitEthernet0/0/7 #') is down on device '240520020-04:138:172.30.9.121'Lost Carrier
cenAlarmSeverity	整数（Integer）	.1.3.6.1.4.9.9.311.1.1.2.1.17	アラームの重大度はそのアラームの重大度を整数値で示します。 • 0：重大 • 1：メジャー • 2：マイナー • 3：警告 • 4：クリア • 5：情報	4

SNMP Varbind	データ タイプ	Varbind OID	SNMP Varbing の説明	例
cenAlarmSeverityDefinition	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.18	生成されたアラームの重大度に関する簡単な説明 。文字列は「,」タプルの形式で表されます 。値は、 「cenAlarmCategory」属性が保持する値と同じです。 。1 行を含む 生成されたアラーム重大度の 1 行の説明が含まれます。 • 0：重大 • 1：メジャー • 2：マイナー • 3：警告 • 4：クリア • 5：情報	4.CLEARED
cenAlarmTriageValue	整数（Integer）	.1.3.6.1.4.9.9.311.1.1.2.1.19	アラームのトリアージ値とは、アラーム間の影響、関係、またはユーザーが指定したその他の機能を人工的な形式で評価できるようにする、階層型の重み付け値です。アプリケーションによって適用されますが、さらに重要な点はエンド ユーザーによるカスタマイズが可能なことです。値は正の数またはゼロ（判別不能または計算不可能な値を示す）です。 （注） EPN Manager はこのフィールドをサポートしていません。	—
cenEventIDList	OctetString	.1.3.6.1.4.9.9.311.1.1.2.1.20	このアラームの生成につながった一意のイベント識別子のコンマ区切りリスト。 （注） EPN Manager はこのフィールドをサポートしていません。	—

SNMP Varbind	データ タイプ	Varbind OID	SNMP Varbing の説明	例
cenUserMessage1	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.21	ユーザー入力メッセージ。アラームに関する情報。これには、アラームが根本原因アラームであるか、サービスに影響するアラームであるかが含まれます。 srcObjectDisplayName=GigabitEthernet0/0/0/18, rootCauseId=0, hostName=ASR9001-156.156.cisco, serviceImpacting=0, applicationSpecificAlarmID=LINK_DOWN:10.127.101.156:If: GigabitEthernet0/0/0/18##SubAlarm@@_7, correlationType=UNKNOWN, srcObjectBusinessKey=4c2b8aa7[1589721133_10.127.101.156, GigabitEthernet0/0/0/18 chassisId = 0. srcObjectDisplayName refers to the Location in EPNM UI. chassisId refers to Satellite Id in EPNMUI. If any of the above information is not populated, then corresponding value is not sent to NBI.	—
cenUserMessage2	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.22	ユーザー入力メッセージ。この値は設定可能です。 （注） EPN Manager はこのフィールドをサポートしていません。	—
cenUserMessage3	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.23	ユーザー入力メッセージ。この値は設定可能です。 （注） EPN Manager はこのフィールドをサポートしていません。	—
cenAlarmMode	整数（Integer）	.1.3.6.1.4.9.9.311.1.1.2.1.24	• unknown(1)：この属性の値を特定できなかった場合。 • alert(2)：管理対象オブジェクトのポーリングや SNMP 通知のリッスンを行うことですべてのイベントが報告される一連のイベントによって生成されたアラームを示します。 • event(3)：管理対象オブジェクトのポーリングやSNMP通知のリッスンによって生成されたイベントを示します。	2

SNMP Varbind	データ タイプ	Varbind OID	SNMP Varbing の説明	例
cenPartitionNumber	整数（Integer）	.1.3.6.1.4.9.9.311.1.1.2.1.24	管理アプリケーションによって生成された、複数のパーティションをサポートするトラップでは、管理対象デバイスが存在する論理グループを識別するために割り当てられた整数値が属性によって伝送されます。 （注） EPN Manager はこのフィールドをサポートしていません。	0
cenPartitionName	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.26	管理アプリケーションによって生成された、複数のパーティションをサポートするトラップでは、管理対象デバイスが存在する論理グループを識別するために割り当てられた名前が属性によって伝送されます。	—
cenCustomerIdentification	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.27	ユーザー入力メッセージ。属性には自由書式のテキストが使用されます。この属性は、高度な管理アプリケーションで障害管理サーバーからの応答を並べ替えるために使用できます。 （注） EPN Manager はこのフィールドをサポートしていません。	—
cenCustomerRevision	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.28	ユーザー入力メッセージ。属性には自由書式のテキストが使用されます。この属性は、高度な管理アプリケーションで障害管理サーバーからの応答を並べ替えるために使用できます。 （注） EPN Manager はこのフィールドをサポートしていません。	—
cenAlertID	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.29	イベントベースの通知の場合、この属性には、生成されたイベントがロールアップされたアラート ID が含まれます。アラートベースの通知では、cenAlarmInstanceId と cenAlertID は同一になります。	1185098114

（注） null のアラームの情報は NBI に転送されません。



付録 D

モニターリング ポリシー リファレンス

ここでは、Cisco EPN Manager で使用されるモニターリング ポリシーについて説明します。サポート対象の MIB オブジェクトの詳細については、Cisco Evolved Programmable Network Manager のサポート対象デバイス を参照してください。

デバイスのヘルス モニターリング ポリシー

デバイスのヘルス モニターリング ポリシーは、ネットワーク内のすべてのデバイスのデバイス CPU 使用率、メモリ プール使用率、環境温度、およびデバイス アベイラビリティをモニターします。デフォルトでは、ポリシーは 5 分ごとにデバイスにこの情報をポーリングし、CPU 使用率、メモリ プール使用率、または環境温度のしきい値を超えると、アラームが生成されます。

このモニターリング ポリシーは、インストール後にデフォルトで有効になります。

（注） このポリシーは、サポートされている Cisco ONS または Cisco NCS 2000 デバイスのデバイス CPU 使用率およびメモリ プール使用率はモニターしませんが、メモリ使用率とデバイス アベイラビリティをモニターします。

このポリシーの管理方法の詳細については、「基本的なデバイス ヘルス モニターリングのセットアップ （283 ページ）」を参照してください。

（注） デバイス ヘルス モニターリング ポリシーの配下には 100 台を超えるデバイスを含めないでください。たとえば、100 台を超える cBR-8 デバイスを Cisco EPN Manager に追加する場合は、複数のポリシーを作成してそれらのポリシー間でデバイスを分割してください。

インターフェイスのヘルス モニターリング ポリシー

インターフェイスのヘルス モニターリング ポリシーは、30 を超える属性をモニターし、インターフェイスの動作ステータスとパフォーマンスをチェックします。デバイスインターフェイスを 5 分ごとにポーリングし、インターフェイスの廃棄、エラー、使用率、またはバイト レートのしきい値を超えた場合にアラームを生成します。

大規模導入のパフォーマンスを保護するために、このポリシーは既定では有効化されません。

（注） このポリシーでは、光インターフェイスがモニターされません。光インターフェイスの情報をモニターするには、光ポリシーを使用します。[オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、および [オプティカル30秒（Optical 30 secs）] モニターリング ポリシー （1208 ページ）を参照してください。

このポリシーを管理する方法については、次のトピックを参照してください。

- インターフェイスのヘルス ポリシーがインターフェイスをアクティブにモニターしているかどうかを確認する方法については、「Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）」を参照してください。
- インターフェイスのモニターリングをセットアップするには、「基本的なインターフェイス モニターリングの設定 （283 ページ）」を参照してください。
- インターフェイスのモニターリング ポリシーを調整するには、「モニター対象を調整する（291 ページ）」を参照してください。

カスタム MIB ポーリング モニターリング ポリシー

カスタム MIB ポーリング モニターリング ポリシーは、サポートされていないパラメータ（既存のモニターリング ポリシー タイプでポーリングされないパラメータ）のモニターリングに使用できるカスタマイズ可能なポリシーです。カスタム MIB ポーリング ポリシーを作成する場合は、シスコおよびその他の MIB の広範なリストから選択するか、新しい MIB をポリシーにインポートすることができます。カスタム MIB ポーリング ポリシーがデバイスのパフォーマンス情報を収集する場合は、汎用ダッシュレットを作成して（[デバイス トレンド（Device Trends）]ダッシュボードへのカスタマイズ済みダッシュレットの追加（29ページ）を参照）、[パフォーマンス（Performance）]ダッシュボードにそのデータを表示できます。カスタム MIB ポーリング モニターリング ポリシーの管理の詳細については、次のトピックを参照してください。

- カスタム MIB ポーリング ポリシーが情報のモニターリングに使用されているかどうかを確認するには、Cisco EPN Manager によるモニターリング対象のチェック（287ページ）を参照してください。
- 新しいカスタム MIB ポーリング ポリシーを作成するには、サポートされないパラメータとサードパーティ デバイスを対象としたモニターリング ポリシーの作成（293ページ）を参照してください。
- 既存のカスタム MIB ポーリング ポリシーを調整するには、モニター対象を調整する（291ページ）を参照してください。

IP SLA Y.1731 モニターリング ポリシー

IP SLA Y.1731 モニターリング ポリシーは、Y.1731 ITU-T の推奨事項を使用して、メトロ イーサネット ネットワークでの 70 以上の障害およびパフォーマンス属性をモニターします。

IP SLA Y.1731 モニターリングポリシーを作成した場合は、デフォルトでは 15 分ごとにパラメータがポーリングされ、遅延、ジッター、フレーム損失、ccm フレーム損失、その他のしきい値を超えたときにアラームが生成されます。

Cisco EPN Manager は、データがデバイスの履歴バケットに保存されるのと同じ間隔でデータを保存します。たとえば、デバイスの履歴バケットが 5 分ごとに更新され、モニターリングポリシーが 15 分ごとにデバイスをポーリングするように設定されている場合、Cisco EPN Manager は 15 分ごとに 3 バケットのデータを保存します。

バケットなしですべてのポーリングされたデータを収集するには、次の手順を実行します。

1. 集約された履歴バケットの時間間隔がモニタリングポリシーのポーリング間隔よりも長いことを確認します。
2. デバイスに少なくとも 2 つの履歴バケットを設定します。

この拡張機能は次の場所で利用できます。

- 6.1.1 以降の OS バージョンを実行する Cisco IOS-XR デバイス。すべてのプローブタイプ（損失および遅延）のデータ収集は、すべてのデバイスで同時にトリガーする必要があります。すべてのデバイスは、同じ履歴バケット期間で設定する必要があります。
- Cisco IOS-XE デバイス：17.3.1 以降の OS バージョンを実行する NCS 42xx および NCS 520 デバイス。

（注） この拡張機能が適用されないデバイス（古いソフトウェアバージョンを実行しているデバイス、または上記の収集条件を満たしていないデバイス）の場合、Cisco EPN Manager はポリシー収集間隔に従って関連するバケットからデータを収集し、集約します。

各測定では、前方向、後方向、および双方向のデータが収集されます。ビン統計データはデフォルトではポーリングされません。このデータの収集を有効にするには、ポーリング頻度を選択します。詳しくは「モニターリング ポリシーのポーリングの変更」を参照してください

（注） このポリシーは、ME 1200、NCS 42xx、および ASR 9xx デバイスで統計データを収集します。

ME 1200 デバイスでは、MEG ID が 18 文字より長い場合、ビン統計データは収集されず、[Y1731] ダッシュボードタブに表示されません。

IP SLA Y.1731 モニターリング ポリシーを設定および管理する方法については、次のトピックを参照してください。

- IP SLA Y.1731 パラメータがモニターされているかどうかを確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- 新しい IP SLA Y.1731 モニターリング ポリシーを作成するには、事前設定されたポリシータイプを使用した新規モニターリング ポリシーの作成 （293 ページ）を参照してください。
- 既存の IP SLA Y.1731 モニターリング ポリシーを調整するには、モニター対象を調整する（291 ページ）を参照してください。

疑似回線エミュレーション（エッジ間）モニターリング ポリシー

疑似回線エミュレーション（エッジ間）（PWE3）モニターリング ポリシーは、パケット スイッチド ネットワーク（PSN）を介してエッジ間サービスをエミュレートする約 20 の属性をポーリングします。このポリシー タイプを使用するモニターリング ポリシーを作成して有効にすると、属性はデフォルトで15分ごとにポーリングされます。さらに、疑似仮想回線（PW VC）で以下の属性のしきい値を上回ると、Cisco EPN Manager はマイナー アラームを生成します。

- [HC パケットおよびバイト（HC packets and bytes）]：入力レートの合計と出力レートの合計
- [動作ステータス（Operational status）]：[アップ（Up）]、[インバウンドおよびアウトバウンドの動作ステータス（inbound and outbound operational status）]：[アップ（Up）]

PWE3 モニターリング ポリシーを設定および管理する方法の詳細については、次のトピックを参照してください。

- PWE3 パラメータがモニターされているかどうかを確認するには、「Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）」を参照してください。
- 新しい PWE3 モニターリング ポリシーを作成するには、「事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成（293 ページ）」を参照してください。
- 既存の PWE3 モニターリング ポリシーを調整するには、「モニター対象を調整する （291 ページ）」を参照してください。

PTP/SyncE モニターリングポリシー

PTP/SyncE モニターリングポリシーは、PTP と SyncE のパフォーマンスを測定します。PTP/SyncE モニターリングポリシーを作成すると、デフォルトでは 30 分ごとにパラメータがポーリングされます。ポーリング頻度を、5 分、15 分、または 60 分に設定することもできます。

PTP/SyncE モニターリングポリシーを設定および管理する方法の詳細については、次のトピックを参照してください。

- PTP/SyncE モニターリングポリシーのモニターリング対象を確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- 新しい PTP/SyncE モニターリングポリシーを作成するには、事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成（293 ページ）を参照してください。
- 既存の PTP/SyncE モニターリング ポリシーを調整するには、モニター対象を調整する （291 ページ）を参照してください。

QoS サービス モニターリング ポリシー

QoS モニターリング ポリシーは、60 を超えるサービス パラメータをポーリングして、ネットワーク デバイス上で実行されているサービスの品質を検証します。QoS モニターリング ポリシーを作成すると、15 分ごとにパラメータがポーリングされ、一定のしきい値を超えた場合にアラームが生成されます。次に、アラームを発生させる可能性のあるパラメータの一部を示します。

- ドロップ/廃棄されたバイトとパケットのレート
- プレポリシーのバイトとパケットのレート、使用率、設定情報レート（CIR）のパーセンテージ、最大情報レート（PIR）

- ポストポリシーバイト レート、使用率、設定情報レート（CIR）のパーセンテージ、最大情報レート（PIR）

TCA を引き起こす可能性があるすべての QoS パラメータを表示するには、「モニターリング ポリシーによりポーリングされるパラメータとカウンタの確認（289ページ）」を参照してください。

QoS モニターリング ポリシーを設定および管理する方法の詳細については、次のトピックを参照してください。

- QoS パラメータがモニターされているかどうかを確認するには、「Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）」を参照してください。
- 新しい QoS モニターリング ポリシーを作成するには、事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成 （293 ページ）を参照してください。
- 既存の QoS モニターリング ポリシーを調整するには、モニター対象を調整する （291 ページ）を参照してください。

IP SLA モニターリング ポリシー

IP SLA モニターリング ポリシーは、約 20 のパラメータをモニターし、リアルタイムのパフォーマンス情報を提供します。IP SLA モニターリング ポリシーを作成すると、15 分ごとにパラメータがポーリングされます。このモニターリング ポリシーはアラームを生成しません。IP SLA ベースのアラームを生成する場合は、IP SLA Y.1731 モニターリング ポリシーを使用します。

IP SLA モニターリング ポリシーを設定および管理する方法については、次のトピックを参照してください。

- IP SLA パラメータがモニターされているかどうかを確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ） を参照してください。
- 新しい IP SLA モニターリング ポリシーを作成するには、事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成 （293 ページ） を参照してください。
- 既存の IP SLA モニターリング ポリシーを調整するには、モニター対象を調整する （291 ページ） を参照してください。

ME1200 EVC QoS モニターリング ポリシー

ME1200 QoS モニターリングポリシーは、28 個のサービスパラメータをポーリングして、ME1200 デバイス上で実行されている指定のサービスの品質を検証します。ME1200 QoS モニターリングポリシーを作成すると、デフォルトで 15 分ごとにパラメータがポーリングされますが、一定のしきい値を超えてもアラームは生成されません。ポーリング頻度は、ドロップダウンリストから優先値を選択することで変更できます。

ME1200 QoS モニターリング ポリシーによってポーリングされるパラメータの一部を次に示します。

- 送信および廃棄されたバイトとパケットのレート。
- 緑色（適合）トラフィック、黄色（超過）トラフィック、赤色（違反）トラフィック、および廃棄トラフィック（インバウンドとアウトバウンドの両方）の平均ビット レートと平均フレーム レート

（注） 正確な ME1200 QoS データが表示されるようにするには、ME1200 EVC QoS モニターリング ポリシーを有効にする際に、まずは ME1200 デバイスで EVC パフォーマンス モニターリング セッションを無効にします。

ポーリングされるすべての ME1200 QoS パラメータを表示するには、モニターリング ポリシーによりポーリングされるパラメータとカウンタの確認 （289 ページ）を参照してください。

ME1200 QoS モニターリング ポリシーを設定および管理する方法の詳細については、次のトピックを参照してください。

- ME1200 QoS パラメータがモニターされているかどうかを確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- 新しい ME1200 QoS モニターリング ポリシーを作成するには、事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成 （293 ページ）を参照してください。
- 既存の ME1200 QoS モニターリング ポリシーを調整するには、モニター対象を調整する （291 ページ）を参照してください。

MPLS リンク パフォーマンス モニターリング ポリシー

MPLS リンク パフォーマンス モニターリング ポリシーでは、MPLS のリンクの遅延を測定します。MPLS リンク パフォーマンス モニターリング ポリシーを作成すると、デフォルトで 15 分ごとにパラメータがポーリングされます。ポーリング間隔は、1 分、5 分、または 60 分に設定することもできます。

（注） このポリシーは、次のデバイス上のデータを収集します。

- リンク遅延の場合：
  - ASR 9000 デバイスのバージョン 7.0.1 以降。
  - NCS 5500 デバイスのバージョン 7.1.1 以降。
- TWAMP Light レスポンダメトリックの場合：
  - ASR 9000 デバイスのバージョン 7.0.1 以降。
  - NCS 540 デバイスのバージョン 7.2.1 以降。

このポリシーによってポーリングされるパラメータは次のとおりです。

- 平均遅延（Average Delay）
- 最短遅延（Min Delay）
- 最長遅延（Max Delay）
- RX packets
- TX packets

MPLS リンク パフォーマンス モニターリング ポリシーを設定および管理する方法の詳細については、次のトピックを参照してください。

- MPLS リンク パフォーマンス モニターリング ポリシーのモニターリング対象を確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- 新しい MPLS リンク パフォーマンス モニターリング ポリシーを作成するには、事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成（293 ページ）を参照してください。
- 既存の MPLS リンク パフォーマンス モニターリング ポリシーを調整するには、モニター対象を調整する （291 ページ）を参照してください。

BNG セッションおよび IP プール モニターリング ポリシー

このモニターリング ポリシーは 5 個を超えるパラメータをポーリングして、BNG セッション、および IP プールからリースされた IP アドレスをモニターリングします。BNG セッションおよび IP プール モニターリング ポリシーを作成すると、15 分ごとにパラメータがポーリングされ、一定のしきい値を超えた場合にアラームが生成されます。次に、アラームを発生させる可能性のあるパラメータの一部を示します。

- IP プール内の使用済み IP アドレスまたは空き IP アドレスの数。
- 認証済みサブスクライバとアップ サブスクライバのセッション数。

TCA の原因になる可能性があるすべての BNG セッションおよび IP プール パラメータを確認するには、モニターリング ポリシーによりポーリングされるパラメータとカウンタの確認（289 ページ）を参照してください。

BNG セッションおよび IP プール モニターリング ポリシーを設定および管理する方法の詳細については、次のトピックを参照してください。

- BNG セッションおよび IP プール パラメータがモニターリングされているかどうかを確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- 新しい BNG セッションおよび IP プール モニターリング ポリシーを作成するには、事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成（293 ページ）を参照してください。
- 既存の BNG セッションおよび IP プール モニターリング ポリシーを調整するには、モニター対象を調整する （291 ページ）を参照してください。

TDM/SONET ポート モニターリング ポリシー

TDM/SONET ポートモニターリングポリシーを作成すると、選択したポーリング頻度に基づいて パラメータがポーリングされます。 パラメータのいずれかのしきい値を超えた場合に生成されるアラームを定義できます。

TDM/SONET ポート モニターリング ポリシーを設定および管理する方法の詳細については、次のトピックを参照してください。

- TDM/SONET ポート パラメータがモニターリングされているかどうかを確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- 新しい TDM/SONET ポート モニターリング ポリシーを作成するには、事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成（293 ページ）を参照してください。
- 既存の TDM/SONET ポート モニターリング ポリシーを調整するには、モニター対象を調整する （291 ページ）を参照してください。

光 SFP モニターリング ポリシー

光 SFP モニターリング ポリシーは、光 SFP（Small Form-Factor Pluggable）インターフェイスのヘルスおよびパフォーマンス情報をポーリングします。このポリシーは、温度、電圧、電流、

および光 TX/RX 電力をポーリングします。光 SFP モニターリング ポリシーを作成すると、1 分ごとにパラメータがポーリングされます。

光 SFP モニターリング ポリシーを設定および管理する方法については、次のトピックを参照してください。

- 光 SFP パラメータがモニターされているかどうかを確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ） を参照してください。
- 新しい光 SFP モニターリング ポリシーを作成するには、事前設定されたポリシー タイプを使用した新規モニターリング ポリシーの作成 （293 ページ） を参照してください。
- 既存の光 SFP モニターリング ポリシーを調整するには、モニター対象を調整する （291 ページ） を参照してください。

[オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、および [オプティカル30秒（Optical 30 secs）] モニターリングポリシー

[オプティカル1日（Optical 1 day）] モニタリングポリシーは、次のオプティカル インターフェイスをポーリングします。

- Cisco NCS 4000、ASR 9K、NCS 55xx、および NCS 1K デバイスの物理、OTN、イーサネット、SONET/SDH の各インターフェイス
- Cisco NCS 2000 および Cisco ONS デバイスの DWDM インターフェイス

[オプティカル15分（Optical 15 mins）] モニタリングポリシーは、次のオプティカル インターフェイスをポーリングします。

- Cisco NCS 4000、ASR 9K、NCS 55xx、NCS 57xx、CISCO 8xxx、および NCS 1K デバイスの物理、OTN、OTU FEnd、OTU NEnd、ODU FEnd、ODU NEnd、OTN GFP、OTN FEC、イーサネット、SONET/SDH の各インターフェイス
- Cisco NCS 2000 および Cisco ONS デバイスの DWDM インターフェイス

[オプティカル30秒（Optical 30 secs）] モニタリングポリシーは、Cisco NCS 1001 および NCS 1004 デバイスの物理、OTN、イーサネットの各パラメータをポーリングします。

これらのポリシーでポーリングされるパラメータの一覧については、光モニターリング ポリシーのパフォーマンス カウンタ （1210 ページ）を参照してください。

[オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、および [オプティカル30秒（Optical 30 secs）] モニタリングポリシーの設定および管理方法については、次のトピックを参照してください。

- [オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、および[オプティカル30秒（Optical 30 secs）] のパラメータがモニタリングされているかどうかを確認するには、Cisco EPN Manager によるモニターリング対象のチェック （287 ページ）を参照してください。
- [オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、および[オプティカル30秒（Optical 30 secs）] モニターリングポリシーを新規に作成するには、事前設定されたポリシータイプを使用した新規モニターリング ポリシーの作成 （293 ページ）を参照してください。
- 既存の [オプティカル1日（Optical 1 day）]、[オプティカル15分（Optical 15 mins）]、および [オプティカル30秒（Optical 30 secs）] モニターリングポリシーを調整するには、モニター対象を調整する （291 ページ）を参照してください。

（注） IOS-XR デバイスの場合、収集された OTN 15 分レポートを生成するか、特定の OTN 15 分パラメータを選択して個別の設定レポートを生成できます。次のさまざまなオプションがあります。

- OTU FEnd
- OTU NEnd
- ODU FEnd
- ODU NEnd
- OTN GFP
- OTN FEC

CEM モニターリング ポリシー

CEM モニターリング ポリシーを使用して、次の CEM パラメータをポーリングします。

- ジッターバッファオーバーラン（Jitter Buffer Overruns）
- 生成したLビット（Generated Lbits）
- 受信したLビット（Received Lbits）
- 生成したRビット（Generated Rbits）
- 受信したRビット（Received Rbits）
- 生成したNビット（Generated Nbits）
- 受信したNビット（Received Nbits）
- 生成したPビット（Generated Pbits）

- 受信したPビット（Received Pbits）

ポーリングはCLIを介して行われ、現在の収集と最後の収集の差分が現在のエントリとして使用されます。

（注） このポーリング データはダッシュボードに表示されません。

デバイス センサー モニターリング ポリシー

デバイス センサー モニターリング ポリシーを使用して、このポリシーに追加されたデバイスにSNMPを介してセンサー情報をポーリングします。電圧、電力、現在の温度などのセンサーの詳細がデバイスにポーリングされます。

（注） デバイス センサー データに関連する計算はありません。

光モニターリング ポリシーのパフォーマンス カウンタ

次のトピックでは、光モニターリング ポリシーで使用されるパフォーマンス カウンタをリストします。この情報は、Web GUIから入手することができないため、ここで提供しています。

- 参考：物理インターフェイスのパフォーマンス カウンタ （1210 ページ）
- 参考：OTN-FEC インターフェイス用のパフォーマンス カウンタ （1213 ページ）
- 参考：OTN-ODU インターフェイスのパフォーマンス カウンタ （1214 ページ）
- 参考：OTN-OTU インターフェイスのパフォーマンス カウンタ （1215 ページ）
- 参考：イーサネット インターフェイス用のパフォーマンス カウンタ （1216 ページ）
- 参考：SONET インターフェイス用のパフォーマンス カウンタ （1218 ページ）
- 参考：SDH インターフェイスのパフォーマンス カウンタ （1218 ページ）
- 参考：DS1/DS3 のパフォーマンスカウンタ （1220 ページ）

参考：物理インターフェイスのパフォーマンス カウンタ

次の表は、物理インターフェイスをモニターするために、光ポリシータイプによって使用されるパフォーマンス カウンタを示しています。

アスタリスク（*）でマークが付けられたパフォーマンス カウンタは、すべてのCiscoオプティカル ネットワーキング サービス（ONS）およびCisco NCS 2000 シリーズ デバイスで適用可能です。二重のアスタリスク（**）でマークが付けられたパフォーマンス カウンタは、Cisco Network Convergence System（NCS）4000 シリーズ デバイスで適用可能です。

物理インターフェイス パフォーマンス カウンタ	説明
OPR-MIN	光回路によって受信された最小送出電力。
OPR-AVG	光回路によって受信された平均送出電力。
OPR-MAX	光回線によって受信された最大送出電力。
OPT-MIN	光回路から送信された最小送出電力。
OPT-AVG	光回線から送信された平均送出電力。
OPT-MAX	光回線から送信された最大送出電力。
OSC_PWR	光回線によって受信された電力。
LBC-MIN* LBCL-MIN	光回路の最小レーザー バイアス電流。
LBC-AVG* LBCL-AVG	光回線の平均レーザー バイアス電流。
LBC-MAX* LBCL-MAX	光回線の最大レーザー バイアス電流。
DGD-MIN**	光回路の最小微分群遅延。
DGD-AVG**	光回線の平均微分群遅延。
DGD-MAX**	光回線の最大微分群遅延。
SOPMD-MIN**	光回路の最小 2 次偏光モード分散。
SOPMD-AVG**	光回路の平均 2 次偏光モード分散。
SOPMD_MAX**	光回線の最大 2 次偏光モード分散。
OSNR-MIN**	光回線の最小 Optical Signal to Noise Ratio。
OSNR-AVG**	光回線の平均 Optical Signal to Noise Ratio。
OSNR-MAX**	光回線の最大 Optical Signal to Noise Ratio。
eSNR-MIN**	光回線の最小 Electrical Signal to Noise Ratio。

eSNR-AVG**	光回線の平均 Electrical Signal to Noise Ratio。
eSNR-MAX **	光回線の最大 Electrical Signal to Noise Ratio。
PDL-MIN**	光回線の最小偏波依存損失。
PDL-AVG**	光回線の平均偏波依存損失。
PDL-MAX**	光回線の最大偏波依存損失。
PCR-MIN**	光回路の最小偏波変化率。
PCR-AVG**	光回線の平均偏波変化率。
PCR-MAX**	光回線の最大偏波変化率。
PMD-AVG*、**	光回線の平均偏波モード分散。
PMD-MIN*、**	光回線の最小偏波モード分散。
PN-MIN**	光回線の最小位相ノイズ。
PN-AVG**	光回線の平均位相ノイズ。
PN-MAX**	光回線の最大位相ノイズ。
PREFEC-BER*	光回線の事前前方誤り訂正ビットエラーレート。
CD-MIN**	光回線の最小波長分散。
CD-AVG**	光回線の平均波長分散。
CD-MAX**	光回線の最大波長分散。

（注） PMD-MIN および PMD-AVG は、SVO デバイスには適用されません。

次の表は、物理インターフェイスをモニターするために光ポリシータイプによって使用され、NCS1004、NCS560、NCS5500、CISCO8XXX、NCS540、ASR9K の各デバイスからリアルタイムでデータを収集するパフォーマンスカウンタを示しています。

物理インターフェイス パフォーマンス カウンタ	説明
CD	波長分散
DGD	微分群遅延
SOPMD	2 次偏波モード分散

PCR	偏波変化速度
PDL	偏波依存損失
OSNR	光信号対雑音比
TX-POWER	送信光パワー
RX-POWER	受信光パワー
LBC	レーザーバイアス電流
RX-SIG	受信信号強度（Received Signal Power）
FREQ-OFF	周波数の差
Q ファクタ	品質係数
Q マージン	品質係数マージン
BAUDRATE	情報転送レート（ビット/秒）
Pre-FEC-Val	前方誤り訂正値
Pre-FEC-BER	事前の前方誤り訂正値ビットエラーレート
Post-FEC-BER	事後の前方誤り訂正値ビットエラーレート

参考：OTN-FEC インターフェイス用のパフォーマンス カウンタ

次の表に、光ポリシー タイプが OTN-FEC インターフェイスをモニターするために使用するパフォーマンス カウンタを示します。

アスタリスク（*）でマークされたパフォーマンス カウンタは、すべてのシスコ オプティカル ネットワーキング サービス（ONS）デバイスと Cisco Network Convergence System（NCS）2000 シリーズ デバイスに適用されます。

OTN-FEC インターフェイス パフォーマンス カウンタ	**説明**
BIT-EC* BIEC	修正されたビット エラーの数。
UNC-WORDS* UCW	修正不可能な単語の数。

参考：OTN-ODU インターフェイスのパフォーマンス カウンタ

次の表に、OTN-ODU インターフェイスをモニターするために、オプティカル ポリシー タイプによって使用されるパフォーマンス カウンタを示します。

OTN-ODU インターフェイスのパフォーマンス カウンタ	説明
BBE-PM	パス モニターリングでのバックグランドブロック エラーの数。
BBER-PM	パス モニターリングでのバックグランドブロック エラーの割合。
ES-PM	パス モニターリングでのエラー秒数。
ESR-PM	パス モニターリングでのエラー秒数の割合。
SES-PM	パス モニターリングでの重大エラーの秒数。
SESR-PM	パス モニターリングでの重大エラーの秒数の割合。
UAS-PM	パス モニターリングで利用不可であった秒数。
FC-PM	パス モニターリングでの障害カウント（AIS/RFI が検出された）の数。
gfpStatsRxFrames	受信した Generic Framing Procedure（GFP）フレームの数。
gfpStatsTxFrames	送信された GFP フレームの数。
gfpStatsRxOctets	受信した GFP のバイト数。
gfpStatsTxOctets	送信された GFP のバイト数。
gfpStatsRxCRCErrors	ペイロード フレーム チェック シーケンス（FCS）エラーで受信したパケットの数。
gfpStatsRxMBitErrors	複数ビット エラーの数。GFP コア ヘッダーの GFP-transparent（GFP-T）レシーバでは、これらは修正できません。
gfpStatsRxSBitErrors	単一ビット エラーの数。GFP コア ヘッダーの GFP-T レシーバでは、これらは修正できません。
gfpStatsRxTypeInvalid	無効な GFP タイプで受信されたパケットの数。これには、予期しないユーザー ペイロード識別子（UPI）タイプとコア ヘッダー エラー チェック（CHEC）のエラーが含まれます。

gfpStatsRxCIDInvalid	無効 CID で受信されたパケットの数。
gfpStatsRoundTripLatencyUSec	エンドツーエンドのファイバ チャネル トランスポートのラウンド トリップの遅延（ミリ秒単位）。
gfpStatsTxDistanceExtBuffers	GFP-T トランスミッタ用に送信されたバッファクレジットの数（距離延長が有効な場合にのみ有効）。
gfpStatsRxSblkCRCErrors	スーパーブロックの巡回冗長検査（CRC）エラーの数。
gfpStatsCSFRaised	GFP-T レシーバで検出された GFP クライアント シグナル障害（CSF）フレームの数。
gfpStatsLFDRaised	検出された GFP フレーム損失表示（LFD）の数。
gfpRxCmfFrame	受信されたクライアント管理フレーム（CMF）の数。
gfpTxCmfFrame	送信されたクライアント管理フレーム（CMF）の数。
gfpStatsCHecRxMBitErrors	コア ヘッダー エラー制御（cHEC）CRC 複数ビット エラーの数。
gfpStatsTHecRxMBitErrors	タイプ ヘッダー エラー制御（tHEC）CRC 複数ビット エラーの数。

参考：OTN-OTU インターフェイスのパフォーマンス カウンタ

次の表は、OTN-OTU インターフェイスをモニターするために、光ポリシー タイプによって使用されるパフォーマンス カウンタを示しています。

OTN-OTU インターフェイス パフォーマンス カウンタ	説明
BBE-SM	セクション モニターリングのバックグラウンド ブロック エラーの数。
BBER-SM	モニターリング セクションのバックグラウンド ブロック エラーの比率。
ES-SM	セクション モニターリングのエラーの秒数。
ESR-SM	セクション モニターリングのエラーの秒の比率。
SES-SM	セクション モニターリングの重大なエラーの秒数。
SESR-SM	セクション モニターリングの重大なエラーの秒の比率。
UAS-SM	セクション モニターリングを使用できない秒数。

FC-SM	セクション モニターリングの障害カウント（AIS/RFI が検出された）の数。

参考：イーサネット インターフェイス用のパフォーマンス カウンタ

次の表に、光ポリシー タイプがイーサネット インターフェイスをモニターするために使用するパフォーマンス カウンタを示します。

イーサネット インターフェイス パフォーマンス カウンタ	説明
ifInOctets	インターフェイス上で受信されたオクテットの総数（フレーミング オクテットを含む）。
ifInErrors	エラーが原因で破棄された受信パケットの総数。
ifOutOctets	送信されたオクテットの総数（フレーミング パケットを含む）。
ifInUcastPkts	最後にカウンタがリセットされてから受信されたユニキャスト パケットの総数。
ifOutUcastPkts	上位プロトコルから送信が要求され、宛先がこのサブレイヤのマルチキャストまたはブロードキャスト アドレスでなかったパケットの総数（廃棄されたまたは送信されなかったパケットを含む）。
ifInMulticastPkts	最後にカウンタがリセットされてから受信されたマルチキャスト パケットの総数。
ifOutMulticastPkts	エラーなしで送信されたマルチキャスト フレームの総数。
ifInBroadcastPkts	最後にカウンタがリセットされてから受信されたブロードキャスト パケットの総数。
ifOutBroadcastPkts	上位プロトコルから要求され、宛先がこのサブレイヤのブロードキャストアドレスだったパケットの総数（送信されなかったパケットを含む）。
txTotalPkts	送信パケットの総数。
rxTotalPkts	受信パケットの総数。
etherStatsOctets	ネットワーク上で受信されたデータ（不良パケット内のデータを含む）のオクテットの総数（フレーミング ビットを除くが、FCS オクテットは含む）。

etherStatsOversizePkts	1518 オクテットより長い（フレーミング ビットは除くが、FCS オクテットは含む）が、それ以外は適切な形式の受信パケットの総数。タグ付けされたインターフェイスの場合は、この数が 1522 バイトになることに注意してください。
dot3StatsFCSErrors	長さが整数のオクテットであるものの、FCS チェックに合格しない、特定のインターフェイスで受信したフレームの数。
dot3StatsFrameTooLongs	特定のインターフェイスで受信され、最大許可フレーム サイズを超えたフレームのカウント。
etherStatsJabbers	1518 オクテットより長く（フレーミング ビットは除くが、FCS オクテットは含む）、整数のオクテットを伴う不良 FCS（FCS エラー）または整数でないオクテットを伴う不良 FCS（アライメント エラー）のどちらかを含む受信パケットの総数。
etherStatsPkts64Octets	長さが 64 オクテット（フレーミング ビットは除くが、FCS オクテットは含む）の受信パケットの総数（不良パケットを含む）。
etherStatsPkts65to127 Octets	長さが 65 ～ 127 オクテット（65 および 127 を含む、フレーミング ビットは除くが、FCS オクテットは含む）の受信パケットの総数（不良パケットを含む）。
etherStatsPkts128to255 Octets	長さが 128 ～ 255 オクテット（128 および 255 を含む、フレーミング ビットは除くが、FCS オクテットは含む）の受信パケットの総数（不良パケットを含む）。
etherStatsPkts256to511 Octets	長さが 256 ～ 511 オクテット（256 および 511 を含む、フレーミング ビットは除くが、FCS オクテットは含む）の受信パケットの総数（不良パケットを含む）。
etherStatsPkts512to1023Octets	長さが 512 ～ 1023 オクテット（512 および 1023 を含む、フレーミング ビットは除くが、FCS オクテットは含む）の受信パケットの総数（不良パケットを含む）。
etherStatsPkts1024to1518Octets	長さが 1024 ～ 1518 オクテット（1024 および 1518 を含む、フレーミング ビットは除くが、FCS オクテットは含む）の受信パケットの総数（不良パケットを含む）。
etherStatsMulticastPkts	マルチキャスト アドレス宛ての正常な受信パケットの総数。
etherStatsBroadcastPkts	ブロードキャスト アドレス宛ての正常な受信パケットの総数。
etherStatsUndersizePkts	長さが 64 オクテット未満（フレーミング ビットは除くが、FCS オクテットは含む）で、それ以外は適切な形式の受信パケットの総数。

参考：SONET インターフェイス用のパフォーマンス カウンタ

次の表に、光ポリシー タイプが SONET インターフェイスをモニターするために使用するパフォーマンス カウンタを示します。

アスタリスク（*）でマークされたパフォーマンス カウンタは、すべてのシスコ オプティカル ネットワーキング サービス（ONS）デバイスと Cisco Network Convergence System（NCS）2000 シリーズ デバイスに適用されます。

SONET インターフェイス パフォーマンス カウンタ	説明	使用可能先
エラー秒数（ES）*	近端デバイスと遠端デバイスのエラー秒数。	回線* パス VT パス セクション*（近端デバイスにのみ適用）
重大エラー秒数（SES）*	近端デバイスと遠端デバイスの重大エラー秒数。	回線* パス VT パス セクション*（近端デバイスにのみ適用）
重大エラーフレーム秒数（SEFS）*	近端デバイスの重大エラーフレーム秒数。	セクション*（近端デバイスにのみ適用）
コーディング違反（CV）*	近端デバイスと遠端デバイスのコーディング違反の数。 。	回線* パス VT パス セクション*（近端デバイスにのみ適用）
使用不可秒数（UAS）*	近端デバイスと遠端デバイスの使用不可秒数。	回線* パス VT パス

参考：SDH インターフェイスのパフォーマンス カウンタ

次の表に、SDHインターフェイスをモニターするために、オプティカルポリシータイプによって使用されるパフォーマンス カウンタを示します。

SDH インターフェイスのパフォーマンス カウンタ	説明
MS-ES	近端と遠端のデバイスの多重化セクションごとのエラー秒数。
MS-ESR	近端と遠端のデバイスの多重化セクションごとのエラー秒数の割合。
MS-SES	近端と遠端のデバイスの多重化セクションごとの重大エラーの秒数。
MS-SESR	近端と遠端のデバイスの多重化セクションごとの重大エラーの秒数の割合。
MS-BBE	近端と遠端のデバイスの多重化セクションごとのバックグランド ブロック エラーの数。
MS-BBER	近端と遠端のデバイスの多重化セクションごとのバックグランド ブロック エラーの割合。
MS-UAS	近端と遠端のデバイスの多重化セクションごとの利用不可であった秒数。
MS-EB	近端と遠端のデバイスの多重化セクションごとのエラー ブロック数。
MS-FC	近端と遠端のデバイスの多重化セクションごとの障害カウント数。
MS-PSC	多重化セクションごとの保護スイッチング カウント。PSC は、サービスが現用カードから保護カードに切り替わり、戻った回数です。
MS-PSC-R	多重化セクションごとの保護スイッチング カウント リング。このカウントは、リング スイッチングが使用されている場合のみ、増加します。
MS-PSC-S	多重化セクションごとの保護スイッチング カウント スパン。このカウントは、スパン スイッチングが使用されている場合のみ、増加します。
MS-PSC-W	多重化セクションごとの保護スイッチング カウント処理。これは、トラフィックが、障害が発生した回線の処理キャパシティから切り替わり、障害が解決された後にその処理キャパシティに戻った回数のカウントです。PSC-W は、運用回線が失敗した時点で増加します。
MS-PSD	保護スイッチング時間は、サービスが別の回線で実行される時間の長さ（秒数）に適用されます。
MS-PSD-R	保護スイッチング時間リングは、サービスを実行するために保護回線を使用した秒数のカウントです。このカウントは、リング スイッチングが使用されている場合のみ、増加します。
MS-PSD-S	保護スイッチング時間スパンは、サービスを実行するために保護回線を使用した秒数のカウントです。このカウントは、スパン スイッチングが使用されている場合のみ、増加します。

MS-PSD-W	多重化セクションごとの保護スイッチング時間処理。
RS-ES	リジェネレータ セクションごとのエラー秒数。
RS-ESR	リジェネレータ セクションごとのエラー秒数の割合。
RS-SES	リジェネレータ セクションごとの重大エラーの秒数。
RS-SESR	リジェネレータ セクションごとの重大エラーの秒数の割合。
RS-BBE	リジェネレータ セクションごとのバックグランド ブロック エラーの数。
RS-BBER	リジェネレータ セクションごとのバックグランドブロック エラーの割合。
RS-UAS	リジェネレータ セクションごとの利用不可であった秒数。
RS-EB	リジェネレータ セクションごとのエラー ブロックの数。
RS-OFS	リジェネレータ セクションごとの枠外の秒数。

参考：DS1/DS3 のパフォーマンスカウンタ

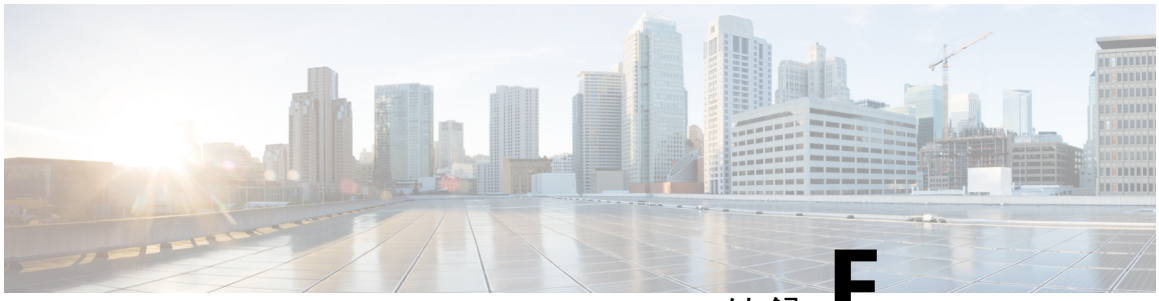
DS1 のパフォーマンスカウンタ

DS1 のパフォーマンスカウンタ	説明
使用不可秒数（UAS）	近端デバイスと遠端デバイスの使用不可秒数。
コード違反（CV）	近端デバイスと遠端デバイスのコード違反の数。
制御スリップ秒数（CSS）	近端デバイスと遠端デバイスの制御されたスリップの秒数。
エラー秒数（ES）	近端デバイスと遠端デバイスのエラー秒数。
重大エラー秒数（SES）	近端デバイスと遠端デバイスの重大エラー秒数。
重大エラーフレーム秒数（SEFS）	近端デバイスと遠端デバイスの重大エラーフレーム秒数。
バーストエラー秒数（BES）	近端デバイスと遠端デバイスのバーストエラー秒数。
低下分数（DM）	近端デバイスと遠端デバイスの低下分数。

DS3 のパフォーマンスカウンタ

DS3 のパフォーマンスカウンタ	説明
エラー秒数（ES）	近端デバイスと遠端デバイスのエラー秒数。
重大エラー秒数（SES）	近端デバイスの重大エラー秒数。
コード違反（CV）	近端デバイスと遠端デバイスのコード違反の数。
P ビットコード違反（CVP）	近端デバイスの P ビットコード違反の数。
P ビットエラー秒数（ESP）	遠端デバイスの P ビットエラー秒数。
重大エラー秒数 P ビット（SESP）	近端デバイスと遠端デバイスの P ビット重大エラー秒数。
重大エラーフレーム秒数（SEFS）	近端デバイスの重大エラーフレーム秒数。
使用不可秒数（UAS）	近端デバイスと遠端デバイスの使用不可秒数。
C ビットコーディング違反（CVC）	近端デバイスと遠端デバイスの C ビットコーディング違反の数。
C ビットエラー秒数（ESC）	近端デバイスと遠端デバイスのC ビットエラー秒数。
重大エラー秒数 CP ビット（SESCP）	近端デバイスと遠端デバイスのCP ビット重大エラー秒数。

モニターリング ポリシー リファレンス



付録 E

Cisco Evolved Programmable Network Manager RESTful API

Cisco EPN ManagerSDK

Cisco EPN Manager SDK は、Cisco EPN Manager の機能を拡張したり、データにアクセスしたり、アプリケーションから自動化操作を呼び出したりできるテクノロジーの集合です。Cisco EPN Manager SDK には、RESTful API と Open Automation が含まれています。RESTful API で「wget および cURL ユーティリティを使用した bash」、「Python」、「Ruby」、Java などのスクリプト言語を使用できます。

Cisco EPN Manager SDK テクノロジーを使用して、次のことが可能です。

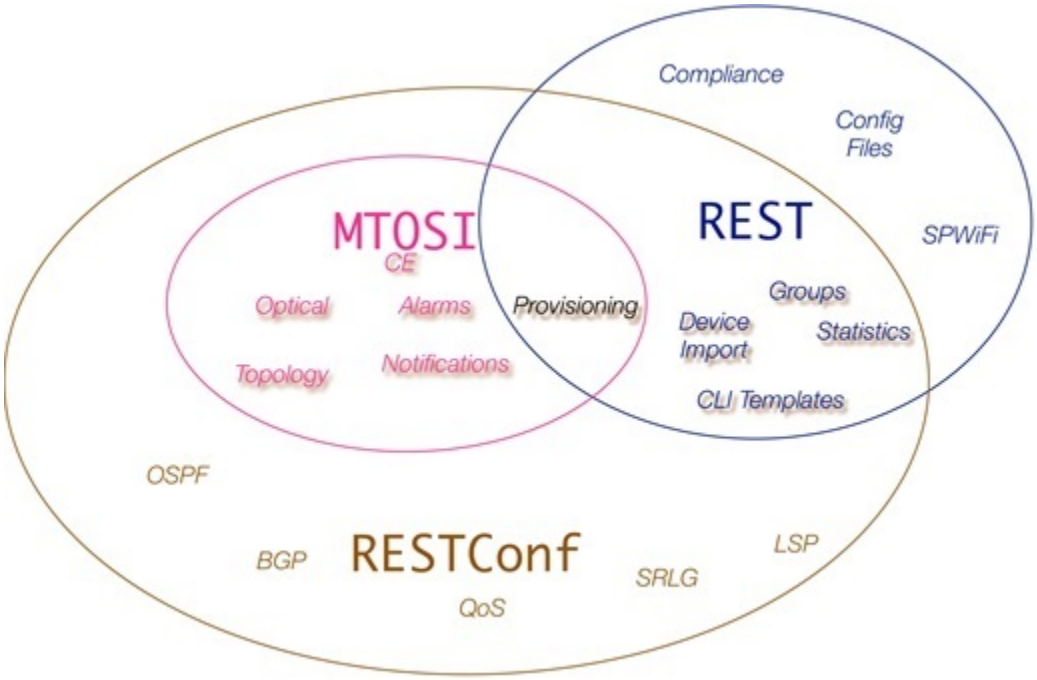
- プログラムによる Cisco EPN Manager へのアクセス：Cisco EPN Manager RESTful API を使用してワークフローを呼び出し、レポートを取得できます。
- Cisco EPN Manager のカスタマイズ：カスタムワークフロータスクを作成し、スクリプトモジュールに独自の jar ファイルおよびスクリプトライブラリを展開して、Cisco EPN Manager をカスタマイズできます。スクリプト バンドルからカスタム タスクを使用します。

Cisco EPN Manager API

Cisco EPN Managerは、あらゆる標準規格の OSS システム ノース バウンドとの統合を可能にする、使いやすく包括的な API を提供します。これらの API では、最も一般的に使用される 3 つの標準規格である MTOSI、RESTConf、および RESTful API を使用してコア機能を拡張します。

自動化向けの迅速な開発設計を実現するためには、開発者が一貫性を持って API を開発し、わかりやすく使いやすい設計ガイドラインを示せるようにすることが重要です。一貫性を保つことで、チームは一般的なコード、パターン、ドキュメント、および設計上の決定事項を活用できます。Cisco EPN Manager では、シンプルで広範な例を使用してアプリケーション内で RESTful API を簡単に利用可能にできます。次の図は、Cisco EPN Manager において *すべて* の API 全体で確認される一般的な動作を示した例です。

図 *18 : EPNM RESTful API* の一般的な動作



この章は、Cisco EPN Manager 開発キット（SDK）および関連技術の使用に関心がある、以下の技術担当者を対象としています。次のようなユーザーが対象です。

- Cisco EPN Manager を使用してリソースを自動化する機能を拡張したいと考えているシステム管理者および REST API 開発者。
- Cisco EPN Manager SDK または API テクノロジーを比較し、どちらがアプリケーションに最適であるかを判断したいその他のユーザー。

Cisco EPN Managerは、MTOSI、REST、および RESTConf の 3 つのノースバウンド API インターフェイス タイプを提供します。この 3 つの API によって提供される機能はかなり類似していますが、すべての API が同じ機能を提供するわけではありません。

MTOSI API は、動作の点で最も異なる API です。光イーサネットおよびキャリア イーサネット機能の基本的なプロビジョニングが可能な SOAP over HTTPS インターフェイスを提供します。DWDM や OTN などの光サービスをプロビジョニングする必要がある場合に、RESTConf API を使用できないときは、MTOSI インターフェイスを使用します。

REST API は、コンフィギュレーション ファイル、グループ管理、およびデバイス インポート機能を処理するその他の機能に加えて、システム情報、ほとんどの統計情報、およびアシュアランス情報を提供します。

RESTConf API は、上記の REST API と同様に RESTful インターフェイスに準拠しています。コア ルーティングとスイッチングだけでなく、キャリア イーサネット、L2/L3 VPN、回線エミュレーション、OTN および DWDM テクノロジーに関するすべてのプロビジョニングを提供します。

詳細については、cisco.com で入手できる個々の Cisco EPNM 統合ガイドを参照してください。

Cisco EPN Manager RESTful API の用途

Cisco EPN ManagerRESTful API は、HTTP 要求を作成可能なプログラムまたはスクリプトで使用できる、言語に依存しないインターフェイスです。別のプログラムまたはプロセスから Cisco EPN Manager 上の操作を呼び出す場合は、REST API を使用してください。

アプリケーションは、RESTful API を使用して以下を実行できます。

- Cisco EPN Manager ドメイン内の物理デバイスと仮想デバイス、ネットワーク、アプライアンス、グループとユーザー、ポリシー、およびその他のモニター対象エンティティに関する Cisco EPN Manager レポートを取得する。
- Cisco EPN Manager 独自の追加操作の呼び出し。

Cisco EPN Manager RESTful API の使用方法

RESTful API クライアントは標準の HTTP 要求および応答を使用して Cisco EPN Manager とやり取りするため、RESTful API 応答はあらゆる Web ブラウザと互換性があります。多くのプログラミング言語には、HTTP 要求の作成と送信、および HTTP 応答の処理に専用のライブラリがあります。

REST API コールの大部分は、要求または応答内のデータをそれぞれ送信および返信します。これらのデータ ペイロードは、RESTful API コールに応じて 2 つの方法のいずれかでフォーマット化されます。JavaScript Object Notation（JSON）ペイロードを使用する RESTful API コールもあれば、XML ペイロードを使用するものもあります。通常の場合、複雑と見なされるアプリケーションには両方を使用する必要があります。

JSON ベースの RESTful API コールは、JSON ペイロードを使用した単純な HTTP 要求および応答です。JSON は、判読可能なデータ交換のために設計された軽量テキストベースのオープンスタンダードです。JSON は、単純なデータ構造と連想配列を表します。アプリケーションは、

特殊な RESTful API ライブラリを使用することなく JSON ベースの API を直接呼び出し、アプリケーションに固有の方法を使用して JSON データを解析します。

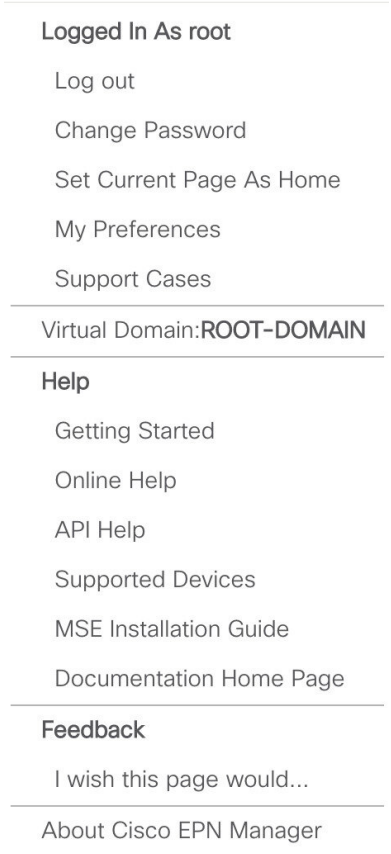
Cisco EPN Manager API へのすべての要求でユーザー認証が必要です。認証の詳細については、「Authentication and Authorization」を参照してください。

RESTful API の認証は、Cisco EPN Manager の登録済みユーザーのみが API 要求を作成できることを要求することによって実行されます。Cisco EPN Manager の場合、API へのアクセスは、NBI 読み取り、NBI 書き込みなどの 3 つのユーザーグループによって制御されます。これらの各グループは、異なる API セットへのアクセスを制御します。必要に応じて、複数のグループにユーザーを割り当てることができます。API リソースのドキュメントページで、アクセスに必要なユーザー グループを確認できます。Cisco EPN Manager で作成および登録したユーザーには、一意の RESTful API アクセス キーが割り当てられます。

RESTConf トポロジ リンク取得リソースを入手するには、RESTful トポロジ リンク リソースを使用してこれらの値を取得し、必要な関連付けを実行します。

Cisco EPN Manager RESTful API のドキュメントにアクセスするには、次の操作を行います。

- Cisco EPN Manager を起動して右上隅にある⚙をクリックすると、ウィンドウ設定メニューが開きます。



- **[ヘルプ（Help）]** > **[APIヘルプ（API Help）]** > **[REST API]** を選択し、システム要件、開発環境のセットアップ方法、ライブラリのインストール方法、RESTful API の使用方法、

すべての Cisco EPN Manager REST API 関数のリスト、REST API リソース、さまざまな使用例、クエリなどを確認します。

RESTConf API：概要

Cisco EPN Manager での実装は、RESTConf/Yang 仕様情報モデルおよび運用 API プロトコルに準拠しています。必要に応じて情報モデルおよび運用 API は標準的な方法で拡張され、RESTConf/Yang インターフェイスに対するシスコのベンダー拡張をサポートします。これらの拡張は、情報モデル拡張の一連の xml および yang スキーマ定義として追加されます。

RESTCONF：構造化データ（XML または JSON）および YANG を使用して REST ライクな API を提供します。これによりさまざまなネットワーク デバイスにプログラムを使用してアクセスできます。RESTCONF API は HTTPs メソッドを使用します。

YANG：モデル構成および操作機能に使用されるデータ モデリング言語。YANG は、NETCONF および RESTCONF API によって実行できる関数の有効範囲と種類を決定します。

RESTConf API の基本的な構造を次に示します。

- HTTP ヘッダー：HTTP ヘッダーは、HTTP 要求内で送信または要求されるコンテンツの説明に使用されます。HTTP ヘッダーには次のものが含まれます。
  - Content-Type：サーバー側で、着信要求にエンティティがアタッチされている場合があります。タイプを特定するために、サーバーは HTTP 要求ヘッダーの Content-Type を使用します。
  - Accept：同様に、クライアント側で必要な表現のタイプを特定するために、HTTP ヘッダーの ACCEPT が使用されます。通常、要求に Accept ヘッダーが存在しない場合、サーバーは事前設定されたデフォルトの表現タイプを送信できます。
- **HTTP メソッド**：API の呼び出しには次のメソッドが使用されます。
  - Get：GET メソッドは、リソースのデータとメタデータを取得するためにクライアントによって送信されます。
  - Post：新しいエンティティの作成に使用されますが、エンティティの更新にも使用できます。POST メソッドは、データ リソースを作成したり、操作リソースを呼び出したりするためにクライアントによって送信されます。
  - Put：PUT 要求はべき等です。PUT メソッドは、ターゲット データ リソースを作成または置換するためにクライアントによって送信されます。
  - Delete：リソースの削除を要求します。DELETE メソッドは、ターゲット リソースを削除するために使用されます。
- **メッセージ**：RESTCONF プロトコルは HTTP メッセージを使用します。1 つの HTTP メッセージは、1 つのプロトコル メソッドに対応します。
- メディア タイプ：XML と JSON。

- クエリ パラメータ：
  - Content
  - Depth
  - Fields
  - Filter
  - Insert
  - Point
  - Start-time
  - Stop-time
  - With-defaults

標準的な使用方法：Get メソッド

「GET All RESTConf API コール」は、既存のエンドポイント スキーマ セクションを返します。

GET /restconf/data/ietf-yang-library:modules-state

すべての RESTConf API エンドポイントを取得します。

スキーマ URL は、多くの列挙変数とモジュールの構造コンポーネントに関する詳細を提供します。

スキーマ取得の例：

GET /restconf/schema/v1/cisco-resource-optical

モジュールの YANG スキーマをプレーン テキストとして返します。

多くの場合、RESTConf API コールでは複数の URL パラメータを使用できます。これらは、すべてのコールで実装されるわけではありません。

- .maxCount
- .startIndex
- .depth

```
GET /restconf/data/v1/module:resource
The general format for a RESTConf GET call.
```

表 *67 :* クエリ パラメータ

クエリー パラメータ	説明
.depth（整数）	取得する詳細レベルの数。
.maxCount（整数）	取得される行数の制限。
.startIndex（整数）	取得する最初の行。

```
GET /restconf/data/v1/module:resource HTTP/1.1
```

RESTful API ユーティリティ

- 完全に識別可能な名前：このインターフェイスのインベントリ オブジェクトには、FDN（完全識別名）を表す属性があります。これらの属性はオブジェクトの識別子として使用されたり、オブジェクトへの参照が必要な場合にクエリ パラメータや返されるデータ内のオブジェクト参照として使用されたりします。この FDN は、「!」で区切った <type>=<value> ペアのシーケンスを含むタイプ/値ペアのセットで構成されるフォーマット済みの文字列です。
  - <type> は、データ モデルで定義された、階層内のインベントリ オブジェクトを表す一定値です（例：MD、ND、EQ、PTP、FTP、CTP、TL、VC、CFS など）。
  - <value> は、インベントリ オブジェクトの属性/値ペアを表す任意のテキストまたは「;」で区切られた <attrName>=<attrValue> ペアのシーケンスで、タイプで表されるオブジェクトのローカル範囲内の一意の値を構成します。

詳細については、『Cisco EPNM RESTConf ガイド』を参照してください。

RESTConf API 機能エリア

- アラーム：アラーム モジュールは、アラームとイベントを取得して確認するメカニズムを提供します。推奨されるアラーム管理方法は、通知 API を介してリッスンすることです。サービスは異なるタイプまたは重要度のイベントを収集し、この API 経由で処理できます。
- パフォーマンス テスト：サービス パフォーマンス テストは、サービス プロビジョニングの一環としても、スタンドアロンでも実行できます。Restconf NBI は、スタンドアロンのパフォーマンス テストの実行をサポートしています。
- Quality of Service（QoS）：QoS は、ネットワーク トラフィックの差別化サービスを配信できるようにする一連の機能です。Cisco EPN Manager を使用して、キャリア イーサネット インターフェイスで QoS を設定できます。
- OAM：EPNM RESTConf API の OAM テストは、2 つの一般的なカテゴリに分類されます（サービス OAM 設定とネットワーク リソース OAM 設定）。Y.1731、Y.1564、および BERT テストでは、service-oam-config エンドポイントが使用されます。OTDR の場合は、network-resource-oam-config エンドポイントが使用されます。EPNM RESTConf OAM コールは、テストを開始するための POST コマンドを提供します。この要求によって、テスト ID とテスト要求 ID が生成されます。通常は、このテスト ID を後続のコールで使用して結果を取得します。ほとんどのテスト タイプには個々の URL があります。
- サービス プロファイル：サービス プロファイルには、各回線/VC タイプのプロビジョニングに使用できる事前定義済みのプロビジョニング要求（注文データ）が含まれています。NBI プロビジョニング要求では、サービス プロファイル リファレンスを使用して、プロビジョニングで使用するプロビジョニング要求データを取得できます。要求でプロビジョニング データがサービス プロファイル リファレンスとともに提供されているにもか

かわらず、ユーザーがデータを提供した場合、要求が送信されてプロビジョニングが実行される前に、サービスプロファイルに格納されているデータがユーザー提供データとマージされて、プロファイル データがオーバーライドされます。サービス プロファイルは、EPNM サービス プロファイル ウィザード GUI を使用して作成できます。

- 顧客向けサービス（CFS）：CFS は回線/VC の顧客向けデータを表します。CFS は検出された RFS から派生し、ネットワーク内の回線/VC のエンドポイントを表します。CFS 検出時に、検出された RFS オブジェクトに対して CFS オブジェクトが作成されます。
- リソース向けサービス（RFS）：RFS は異なるデバイス上のリソース間の関係を表します。RFS 検出時に、デバイス レベルのオブジェクトとネットワーク レベルのオブジェクトが作成されます。デバイス レベルの RFS オブジェクトは、デバイス レベル設定の回線/VC 設定部分を表します。ネットワーク レベルの RFS オブジェクトは、デバイスまたはその他のネットワーク レベルのオブジェクトを集約して、ネットワーク レベルのエンティティを表します。

認証および承認

Cisco EPN Manager APIのすべての要求でユーザー認証が必要です。要求で認証の詳細が指定されていない場合、要求はログインページにリダイレクトされます。認証の詳細は、要求のHTTP ヘッダーを介して渡される場合があります。詳細については、Cisco EPN Manager API ドキュメントの「Authentication, Authorization, and Security」のトピック（[ホーム（Home）] > [認証、認可、セキュリティ（Authentication, Authorization, and Security）]）を参照してください。

Cisco EPN Manager の場合、API へのアクセスは、NBI 読み取り、NBI 書き込みなどのユーザーグループによって制御されます。これらの各グループは、異なる API セットへのアクセスを制御します。必要に応じて、複数のグループにユーザーを割り当てることができます。API リソースのドキュメント ページで、アクセスに必要なユーザー グループを確認できます。

（注） 実稼働環境では、JSESSIONID を使用することをお勧めします。

Cisco EPN Manager REST API スタートアップ ガイド

Cisco EPN Manager REST API を使用すると、アプリケーションはプログラムによって Cisco EPN Manager とやり取りできます。これらの要求を通じて、Cisco EPN Manager のリソースへのアクセス権が付与されます。API コールを使用して、Cisco EPN Manager ワークフロー、アラームとイベントのモニターリング、デバイスインベントリの収集、ネットワーククライアントと使用状況のモニターリング、デバイスの設定、デバイスインベントリなどを実行できます。詳細については、Cisco Evolved Programmable Network Manager API ドキュメントの「Getting Started」トピック（**Home** > **Getting Started**）を参照してください。

REST API の基本および機能エリア

Cisco EPN Managerの REST 実装では、複数のコールとフィルタを使用します。たとえば統計情報を取得する場合、最初のコールは後続のコールの URL を提供します。これらの URL は、より詳細な情報を取得するために使用できます。一般に、詳細情報が追加されるにつれて、コールごとに URL パラメータが複雑になります。

REST API の基本

- HTTPS ヘッダー：次の HTTP ヘッダーを使用して、データがクライアントに返される方法を制御します。
  - Accept
  - Accept-Language
  - Content-Type
  - Accept-Encoding
  - Content-Encoding
- **クエリ パラメータ**：

APIは、ほぼすべての要求のクエリーパラメータをサポートしています。次の表で、一般的な REST クエリ パラメータについて説明します。

表 *68 :* 一般的な *REST* クエリ パラメータ

クエリー パラメータ	適用性	意味
.json	/api/*	指定されている場合は、応答を json 形式で返す必要があります。
.xml	/api/*	指定されている場合は、応答を xml 形式で返す必要があります。これは、.json パラメータが存在しない場合のデフォルトです。
_docs	/api/*	ドキュメント ページを表示します。
.full	/api/v1/data/T	「true」の場合、エンティティの ID だけではなくオブジェクト全体が返されます。
.group	api/v1/data/T	文字列値で指定されたグループの内容と、適用された演算子の結果に基づいて応答をフィルタ処理します。

クエリー パラメータ	適用性	意味
.transform	GET/POST	XML または JSON にレンダリングする直前に適用される変換の論理名を指定します。
.maxresults	GET Paged	返されたインスタンス ツリーのヘッドに関する結果の最大数。
.firstResult	GET Paged	インスタンス ツリーのヘッドに関する最初の結果。
.strict	/api/v1/data/T	「true」の場合は、クエリで使用されるプロパティ名が検証され、必要に応じてエラーがスローされます（デフォルトの strict=false の場合、無効なプロパティ名が無視されて簡単なログ メッセージが表示されます）。
.case_sensitve	/api/v1/data/T	「true」の場合は、フィルタ クエリで使用される文字列値の大文字と小文字が区別されます(デフォルトの .case_sensitive=false の場合は、大文字と小文字を区別せずに比較を行います）。
.nocount	/api/v1/data/T	「true」の場合、「count」、「first」、および「last」属性は応答に含まれません。これらの属性の値を取得するには余分に時間がかかるため、「true」に設定しておくとパフォーマンスが向上します。デフォルトは「false」です。

クエリー パラメータ	適用性	意味
_ctx.domain	GET	アクティブなドメインとしてクエリ パラメータ値で指定されたドメインを設定します。デフォルトは「sticky」で、1度設定するとアクティブドメインが設定されたままになります。「stickiness」はRESTfulではないため、設定でオフにすることができます。

REST API 機能エリア

- 統計：統計サービスは、システムに関する概要、事前定義された統計情報を提供します。統計のリソースの一部を以下に示します。
  - GET All Border Routers
  - GET All IMEs
  - GET All RCs
  - GET All TCAs
  - GET All WANInterfaces
- レポート サービス：レポート サービスは、レポートを検出および実行する操作を行えるようにします。API を介してアクセスする前に、レポートをシステムで定義する必要があります。次の API がサポートされています。
  - GET Get Available Report Templates
  - （廃止）GET Get a Report
  - GET Get a ZIP Report
  - GET Run a ZIP Report
- CLI テンプレート コンフィギュレーション：CLI テンプレート コンフィギュレーション サービスを使用すると、CLI コンフィギュレーション テンプレートを 1 台以上のターゲット デバイスに適用できます。また、システム内の CLI テンプレートをアップロード、削除、取得することもできます。次の API がサポートされています。
  - GET CLI Configuration Templates
  - DELETE Delete Configuration Template
  - DELETE Delete Configuration Template Folder
  - GET Download Configuration Template
  - GET List Configuration Template Folders

- GET List Configuration Templates
- GET List Device Types
- POST Create Configuration Template Folder
- POST Upload Configuration Template
- PUT Deploy Configuration Template
- PUT Deploy Configuration Template Through Job
- PUT Modify Configuration Template Content

統計情報

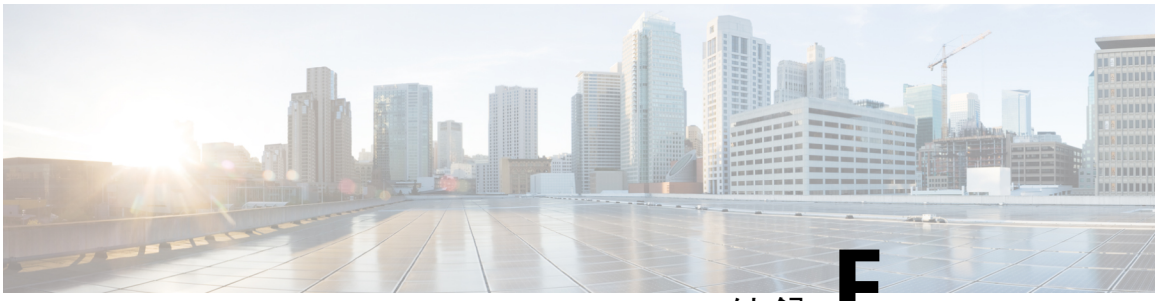
EPNMから簡単な段階的プロセスで統計データを取得できます。これは、複数のREST統計エンドポイント間でかなり一貫性のある一般的な使用パターンです。一般に、概略的な最初のコールでは、使用可能なメトリックのリストが返されます。そのコールから特定のメトリックに関する詳細な統計の2番目のリストが返され、そこから実際のデータ系列が返されます。

統計の例「エンドポイント コールの継承：特定の回線のESR PMデータ」を次に示します。

```
GET /webacs/api/v1/op/statisticsService/circuits?circuitName=VSO5_TO_HUB2
 GET
/webacs/api/v1/op/statisticsService/circuits/metrics?circuitType=ODUUNI&circuitId=161374613

 GET
/webacs/api/v1/op/statisticsService/circuits/metrics/ESR_PM?maxResults=24&timeInterval=6&endpoint-
Name=ODU20/4/0/0/1&location=FEND&circuitType=ODUUNI&deviceId=124606492_10.201.1.174&circuitId=161374613
```

（注） 最後の2つのコールのURLは、前のコールの本文で提供されました。



付録 F

イベントフローコントローラでサポートされているイベントおよびサポートされていないイベント

サポートされるイベント

次に、バーストおよび連続イベントフローコントローラのモニター対象となるイベントのリストを示します。

表 *69*：サポートされるイベント

テクノロジー	イベント
MPLS	MPLS_TE-5-LSP_Down MPLS_TE-5-LSP_Active_StandBy MPLS_TE-5-LSP_CLEAR ROUTING-MPLS_TE-5-LSP_UPDOWN ROUTING-MPLS_TE-5-S2L_SIGNALLING_STATE
疑似回線	cpwVcUp cpwVcDown L2-L2VPN_PW-3-UPDOWN L2-L2VPN_PW-3-UPDOWN_Clear XCONNECT-5-PW_STATUS XCONNECT-5-PW_STATUS_Clear EVPN-5-VC_STATUS EVPN-5-VC_STATUS_Clear
LDP	mplsLdpSessionDown mplsLdpSessionUp

テクノロジー	イベント
OSPF	OSPF-5-ADJCHG OSPF-5-ADJCHG_DOWN OSPF-5-ADJCHG_UP OSPFv3-5-ADJCHG OSPFv3-5-ADJCHG_DOWN OSPFv3-5-ADJCHG_UP ROUTING-OSPF-5-ADJCHG ROUTING-OSPFv3-5-ADJCHG ROUTING-OSPFv3-5-ADJCHG_DOWN ROUTING-OSPFv3-5-ADJCHG_UP
BGP	cbgpBackwardTransition cbgpFsmStateChange cbgpPrefixThresholdExceeded cbgpPrefixThresholdClear bgpBackwardTransition bgpEstablished cbgpPeer2BackwardTransition cbgpPeer2FsmStateChange cbgpPeer2FsmStateChangeUp cbgpPeer2FsmStateChangeDown cbgpPeer2PrefixThresholdClear cbgpPeer2PrefixThresholdExceeded BGP-5-ADJCHANGE BGP-5-ADJCHANGE_DOWN BGP-5-ADJCHANGE_UP BGP-3-NOTIFICATION ROUTING-BGP-5-ADJCHANGE ROUTING-BGP-5-UPDATE_FILTERED
ISIS	CLNS-5-ADJCHANGE CLNS-5-ADJCHANGE_UP CLNS-5-ADJCHANGE_DOWN ROUTING-ISIS-5-ADJCHANGE ROUTING-ISIS-5-ADJCHANGE_UP ROUTING-ISIS-5-ADJCHANGE_DOWN ROUTING-ISIS-4-ADJCHANGE ROUTING-ISIS-4-ADJCHANGE_UP ROUTING-ISIS-4-ADJCHANGE_DOWN isisAdjacencyChange isisAdjacencyChangeDown isisAdjacencyChangeUp isisAdjacencyChangeInit isisRejectedAdjacency

サポートされていないイベント

次に、バーストおよび連続イベントフローコントローラでモニターリングされないイベントのリストを示します。

イベントフローコントローラでサポートされているイベントおよびサポートされていないイベント

表 *70* : サポートされていないイベント

テクノロジー	イベント
G8032	G8032-STATE_IDLE G8032-STATE_PENDING G8032-STATE_PROTECTION G8032-STATE_FORCED_SWITCH G8032-STATE_MANUAL_SWITCH L2-G8032-3-APS_CHANNEL_INACTIVE L2-G8032-6-APS_CHANNEL_ACTIVE

イベントフローコントローラでサポートされているイベントおよびサポートされていないイベント

テクノロジー	イベント
CEM	SONET-4-ALARM_SLOS SONET-4-ALARM_SLOS_Clear SONET-4-ALARM_SLOF SONET-4-ALARM_SLOF_Clear SONET-4-ALARM_LAIS SONET-4-ALARM_LAIS_Clear SONET-4-ALARM_LRDI SONET-4-ALARM_LRDI_Clear SONET-4-ALARM_PAIS SONET-4-ALARM_PAIS_Clear SONET-4-ALARM_PLOP SONET-4-ALARM_PLOP_Clear SONET-4-ALARM_PUNEQ SONET-4-ALARM_PUNEQ_Clear SONET-4-ALARM_PPLM SONET-4-ALARM_PPLM_Clear SONET-4-ALARM_PRDI SONET-4-ALARM_PRDI_Clear SONET-4-ALARM_LOM SONET-4-ALARM_LOM_Clear SONET-4-ALARM_B1-TCA SONET-4-ALARM_B1-TCA_Clear SONET-4-ALARM_B2-TCA SONET-4-ALARM_B2-TCA_Clear SONET-4-ALARM_B3-TCA SONET-4-ALARM_B3-TCA_Clear SONET-4-ALARM_APS SONET-4-ALARM_APS_Clear SONET-4-UPSR_Working SONET-4-UPSR_Working_Clear SONET-4-UPSR_Protect SONET-4-UPSR_Protect_Clear CONTROLLER-5-UPDOWN_Clear CONTROLLER-5-UPDOWN dsx1LoopbackState dsx1LoopbackState_CLEAR dsx1RcvAIS dsx1RcvAIS_CLEAR dsx3RcvAIS dsx3RcvAIS_CLEAR dsx3LOS dsx3LOS_CLEAR dsx3LoopbackState dsx3LoopbackState_CLEAR dsx1LossOfSignal dsx1LossOfSignal_CLEAR SONET-4-ALARM_VT_TRACE_MISMATCH SONET-4-ALARM_VT_TRACE_MISMATCH_Clear SONET-4-ALARM_VT_PATH_LOP SONET-4-ALARM_VT_PATH_LOP_Clear SONET-4-ALARM_VT_UNEQUIPPED SONET-4-ALARM_VT_UNEQUIPPED_Clear SONET-4-ALARM_VT_PATH_RDI SONET-4-ALARM_VT_PATH_RDI_Clear CONTROLLER-5-UPDOWN_VT_PATHAIS CONTROLLER-5-UPDOWN_VT_PATHAIS_Clear CONTROLLER-5-UPDOWN_VT_PATHLOP CONTROLLER-5-UPDOWN_VT_PATHLOP_Clear CONTROLLER-5-UPDOWN_VT_UNEQUIPPED CONTROLLER-5-UPDOWN_VT_UNEQUIPPED_Clear

イベントフローコントローラでサポートされているイベントおよびサポートされていないイベント

テクノロジー	イベント
	CONTROLLER-4-ACR_DCR_CLOCK_DS1 CONTROLLER-4-ACR_DCR_CLOCK_DS3 CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3 CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3 CONTROLLER-4-ACR_DCR_CLOCK_DS1_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_DS1_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_DS1_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_DS3_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_DS3_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_DS3_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_DS3_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_HOLDOVER SONET-4-UPSR DSX-ALARM_DS1_LOS DSX-ALARM_DS1_LINK_DOWN DSX-ALARM_DS1_AIS DSX-ALARM_DS1_RAI DSX-ALARM_DS1_LOF DSX-ALARM_DS1_RX_LOMF DSX-ALARM_DS3_RX_RAI DSX-ALARM_DS3_TX_RAI DSX-ALARM_DS3_RX_AIS DSX-ALARM_DS3_TX_AIS DSX-ALARM_DS3_RX_LOF DSX-ALARM_DS3_RX_LOS DSX-ALARM_DS3_RX_IDLE DSX-ALARM_DS3_OTHER_FAILURE DSX-ALARM_DS3_LINK_DOWN DSX-ALARM_DS3_ADMIN_DOWN DSX-ALARM_DS1_OOF SDH-ALARM_DS3_TX_AIS SDH-ALARM_DS3_TX_AIS_Clear SDH-ALARM_DS3_RX_LOF SDH-ALARM_DS3_RX_LOF_Clear SDH-ALARM_DS3_RX_LOS SDH-ALARM_DS3_RX_LOS_Clear SDH-ALARM_DS3_OTHER_FAILURE SDH-ALARM_DS3_OTHER_FAILURE_Clear SDH-ALARM_DS3_RX_IDLE SDH-ALARM_DS3_RX_IDLE_Clear SDH-ALARM_LO_PAIS SDH-ALARM_LO_PAIS_Clear SDH-ALARM_LO_PLOP SDH-ALARM_LO_PLOP_Clear

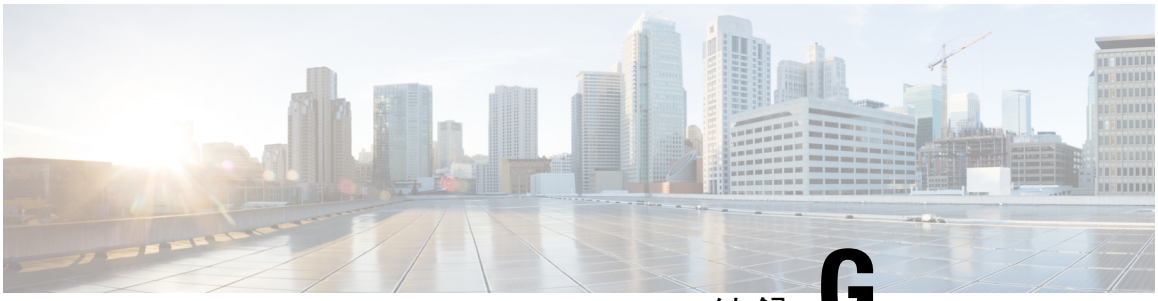
イベントフローコントローラでサポートされているイベントおよびサポートされていないイベント

テクノロジー	イベント
	SDH-ALARM_LO_PTIM SDH-ALARM_LO_PTIM_Clear SDH-ALARM_LO_PUNEQ SDH-ALARM_LO_PUNEQ_Clear SDH-ALARM_LO_PPLM SDH-ALARM_LO_PPLM_Clear SDH-ALARM_LO_PRDI SDH-ALARM_LO_PRDI_Clear SDH-ALARM_LO_BER_SD_B3 SDH-ALARM_LO_BER_SD_B3_Clear SDH-ALARM_LO_BER_SF_B3 SDH-ALARM_LO_BER_SF_B3_Clear SDH-ALARM_LO_LOM SDH-ALARM_LO_LOM_Clear SDH-ALARM_LO_PRFI SDH-ALARM_LO_PRFI_Clear SDH-ALARM_DS1_LOS SDH-ALARM_DS1_LOS_Clear SDH-ALARM_DS1_OOF SDH-ALARM_DS1_OOF_Clear SDH-ALARM_DS1_AIS SDH-ALARM_DS1_AIS_Clear SDH-ALARM_DS1_RAI SDH-ALARM_DS1_RAI_Clear SDH-ALARM_DS1_RX_LOMF SDH-ALARM_DS1_RX_LOMF_Clear SDH-ALARM_DS3_RX_AIS SDH-ALARM_DS3_RX_AIS_Clear SDH-ALARM_DS3_TX_RAI SDH-ALARM_DS3_TX_RAI_Clear SDH-ALARM_DS3_RX_RAI SDH-ALARM_DS3_RX_RAI_Clear SDH-ALARM_SONET_LINK_DOWN SDH-ALARM_SONET_LINK_DOWN_Clear SDH-ALARM_LRFI SDH-ALARM_LRFI_Clear SDH-ALARM_SONET_ADMIN_DOWN SDH-ALARM_SONET_ADMIN_DOWN_Clear SDH-ALARM_PRFI SDH-ALARM_PRFI_Clear SDH-ALARM_SLOS SDH-ALARM_SLOS_Clear SDH-ALARM_SLOF SDH-ALARM_SLOF_Clear SDH-ALARM_LAIS SDH-ALARM_LAIS_Clear SDH-ALARM_LRDI SDH-ALARM_LRDI_Clear SDH-ALARM_PAIS SDH-ALARM_PAIS_Clear SDH-ALARM_PLOP SDH-ALARM_PLOP_Clear SDH-ALARM_PUNEQ SDH-ALARM_PUNEQ_Clear SDH-ALARM_PPLM SDH-ALARM_PPLM_Clear SDH-ALARM_PRDI SDH-ALARM_PRDI_Clear SDH-ALARM_LOM SDH-ALARM_LOM_Clear SDH-ALARM_B1

イベントフローコントローラでサポートされているイベントおよびサポートされていないイベント

テクノロジー	イベント
	SDH-ALARM_B1_Clear SDH-ALARM_B2 SDH-ALARM_B2_Clear SDH-ALARM_SF SDH-ALARM_SF_Clear SDH-ALARM_SD SDH-ALARM_SD_Clear
SyncE	ciscoNetsyncSelectedT0Clock ciscoNetsyncInputAlarmStatus ciscoNetsyncInputSignalFailureStatus NETCLK-6-SRC_ADD NETCLK-6-SRC_UPD NETCLK-6-SEL_CLOCK_SRC NETCLK-6-ENTER_HOLDOVER NETCLK-6-SRC_REM
VCOP	SSFP_VCOP-4-CONF_ADD SSFP_VCOP-4-CONF_DEL SSFP_VCOP-4-CONF_EXIST SSFP_VCOP-4-DEV_REM SSFP_VCOP-4-DEV_INS IOSXE_OIR-6-REMSSFP IOSXE_OIR-6-INSSSFP
セグメント ルーティング	OS-XTC-5-SR_POLICY_UPDOWN
その他（プライオリティイベント）	SYS-5-RELOAD SYS-5-RESTART OIR-6-INSCARD OIR-SP-6-INSCARD SWT_CEFC_STATUS_CHANGE cefcFRURemoved cefcFRUInserted

イベントフローコントローラでサポートされているイベントおよびサポートされていないイベント



付録 G

リファレンス - Apache VTL 構文

リファレンス - Apache VTL 構文

変数	構文	出力
通常の変数	`#set($a = "ValueA")` `show $a`	`ValueA`
整数の配列	`#set($a = [1..3])` `show $a[2]`	`3`
文字列の配列	`#set($a = ["ValueA", $ValueB, "ValueC"])` `show $a[2]`	`ValueC`
マップ	`#set($a = {"ValueA" : "ValueB", "ValueC" : "ValueD"})` `show ${a.ValueA}`	`ValueB`

リファレンス - Apache VTL 構文