CHAPTER 2

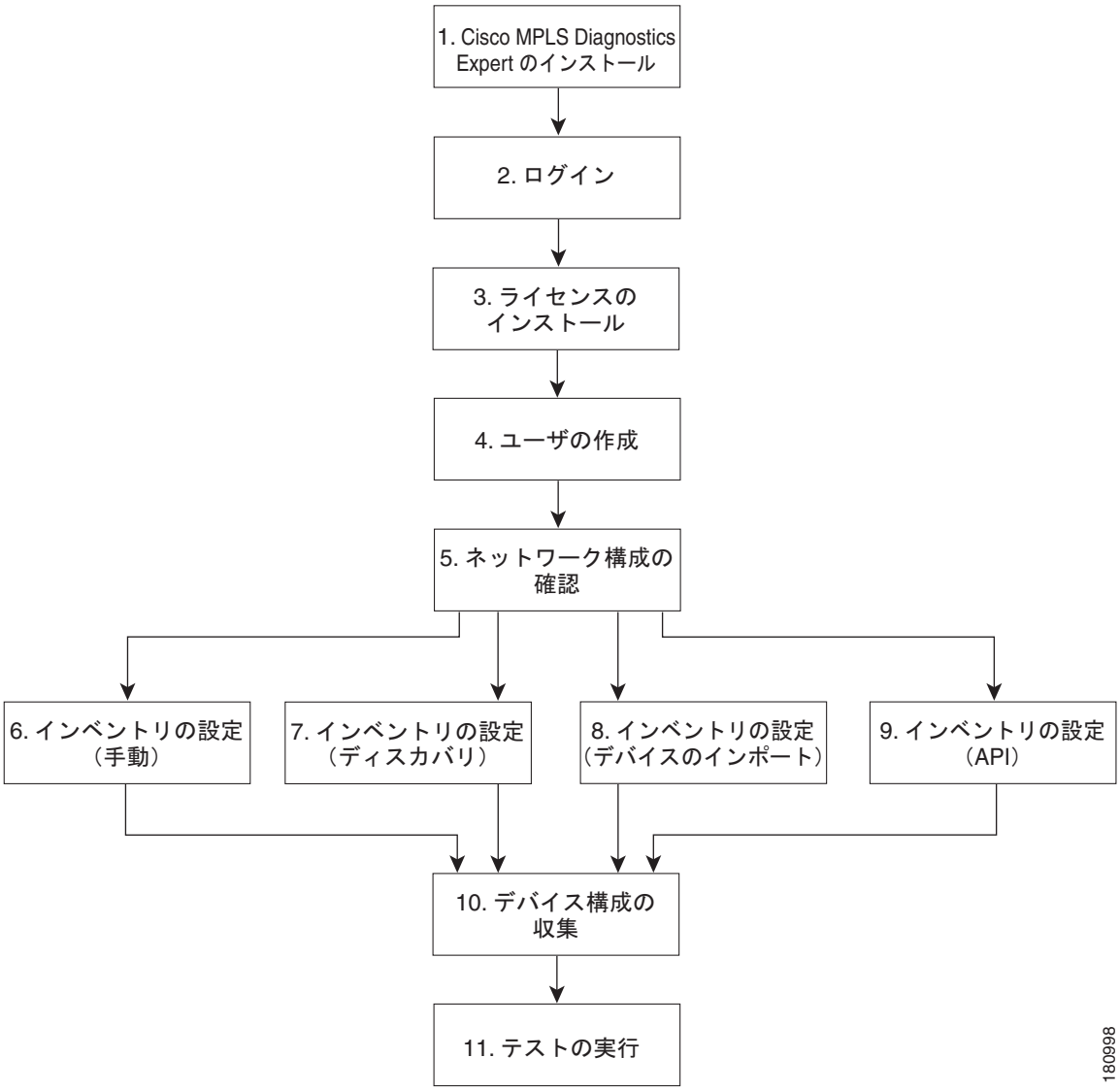
スタートアップ ガイド

この章では、Cisco MPLS Diagnostics Expert（MDE）の使用を開始する手順について説明します。

この章の内容は、次のとおりです。

図 2-1 に、MDE の使用を開始する際のワークフローを示します。

図 2-1　MDE の開始



1. MDE のインストール：MDE アプリケーションをインストールします。「2.1 MDE のインストール」（P.2-3）を参照してください。
2. MDE へのログイン：ログイン方法の詳細については、「2.2 MDE へのログイン」（P.2-3）を参照してください。
3. ライセンスのインストール：MDE ライセンス キーをインストールします。「2.3 ライセンス」（P.2-3）を参照してください。
4. ユーザの作成：ユーザを作成し、MDE ユーザ ロールを割り当てます。「2.4 ユーザ ロール」（P.2-3）、および「2.5 ユーザの作成」（P.2-4）を参照してください。
5. ネットワーク設定の確認：MDE に必要な設定が、すべてのネットワーク デバイスで行われていることを確認します。「2.6 ネットワーク設定」（P.2-4）を参照してください。
6. インベントリの設定（手動）：必要な ISC インベントリ オブジェクトを手動で作成します。「2.7 インベントリの設定」（P.2-5）を参照してください。

7. インベントリの設定（検出）：ISC Discovery を使用して、必要な ISC インベントリ オブジェクトを作成します。「2.7 インベントリの設定」（P.2-5）を参照してください。
8. インベントリの設定（デバイス インポート）：インベントリ マネージャのデバイス インポート機能を使用して、必要な ISC インベントリ オブジェクトを作成します。「2.7 インベントリの設定」（P.2-5）を参照してください。
9. インベントリの設定（API）：必要なインベントリ オブジェクトを ISC API により作成します。「2.7 インベントリの設定」（P.2-5）を参照してください。
10. デバイス設定の収集：インターフェイス設定を含むデバイス設定を収集し、ISC インベントリに追加します。ISC インベントリを実際のデバイス設定と定期的に同期するように、スケジュール タスクを設定できます。「2.7.5 デバイス設定の収集」（P.2-9）を参照してください。
11. テストの実行：MPLS VPN 接続性検証テストを設定して実行します。「3.2 MPLS VPN 接続性検証テストの実行」（P.3-6）を参照してください。

2.1 MDE のインストール

MDE は標準 ISC インストールの一部としてインストールされます。その後、MDE ライセンスをインストールしてアクティブ化する必要があります。MDE のインストール方法の詳細については、『*Cisco IP Solution Center Installation Guide, 6.0*』を参照してください。

2.2 MDE へのログイン

ログイン方法の詳細については、『*Cisco IP Solution Center Installation Guide, 6.0*』の第 2 章にある「Logging In for the First Time」の項を参照してください。

2.3 ライセンス

MDE 製品には別個のライセンス キーが必要です。このライセンス キーは ISC インストール CD-ROM で提供されます。追加の接続回線用のアップグレード ライセンスは、Cisco.com から購入できます。

MDE のライセンスは、標準 ISC ライセンス メカニズムを使用して実装されます。MDE ライセンス キーのインストール方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の管理の章を参照してください。

（注）　有効なライセンス キーがインストールされていない場合、ISC に [Diagnostics] タブが表示されず、MDE 機能をまったく起動できません。

2.4 ユーザ ロール

ISC ユーザが使用できる機能は、割り当てられているユーザ ロールによって決まります。ユーザ ロールによって、デバイスの作成と削除やデバイス設定の収集、MPLS VPN 接続性検証テストの実行を行うこともできます。

MDE 機能を使用するには、実行する権利が与えられる接続性テストのタイプに応じて、次の定義済み MDE ロールの 1 つ以上が割り当てられている必要があります。

1. MplsDiagnosticsRole：2 つの CE 間で MPLS VPN 接続性テストを実行できます。
2. MplsDiagnosticsPeToAttachedCeTestRole：PE と接続された CE との間で MPLS VPN 接続性テストを実行できます。
3. MplsDiagnosticsCetoPeAcrossCoreTestRole：MPLS コアをまたぐ CE および PE 間で MPLS VPN 接続性テストを実行できます。
4. MplsDiagnosticsPetoPeInVrfTestRole：2 つの PE 間で MPLS VPN 接続性テストを実行できます。
5. MplsDiagnosticsPeToPeCoreTestRole：2 つの PE 間でコア MPLS VPN 接続性テストを実行できます。

（注）　すべての MDE ロールで、デバイスの作成と削除やデバイス設定の収集、MPLS VPN 接続性検証テストの実行を行うことができます。詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の管理の章を参照してください。

2.5 ユーザの作成

ISC ユーザの作成方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の管理の章を参照してください。

2.6 ネットワーク設定

この項では、ネットワークのトラブルシューティングを MDE で行うために必要なネットワーク設定を説明します。

2.6.1 MPLS IP 存続可能時間伝搬

MPLS IP 存続可能時間（TTL）伝搬は、シスコ デバイスではデフォルトでイネーブルになっています。MDE では、MPLS IP TTL 伝搬が MPLS コア内でイネーブルになっている必要があります。MPLS IP TTL 伝搬がイネーブルになっていない場合、MDE は MPLS コア内で問題のトラブルシューティングを実行できません。その状態でも、アクセス回線の問題、または MPLS コアのエッジにおける問題のトラブルシューティングは可能です。

Cisco IOS では、IOS コマンドの **no mpls ttl-propagate forward** を使用すると、MPLS コアに転送されるパケットの MPLS IP TTL 伝搬をディセーブルにできます。このコマンドでは、MPLS コアに転送されるパケットの TTL 伝搬が停止されますが、MPLS コア内部から送信されるパケットの TTL 伝搬は許可されます。MDE は、この状況で正しく機能します。

Cisco IOS コマンドの **no mpls ip propagate-ttl** を使用して、または Cisco IOS XR コマンドの **mpls ip-ttl-propagate disable** を使用して TTL 伝搬をディセーブルにしている場合は、すべての TTL 伝搬がディセーブルになるため、MDE は MPLS ネットワークをトラブルシューティングできません。

（注）　トラブルシューティング対象に選択したデバイスと、同じネットワークの一部であるデバイスに対して、タイムスタンプをディセーブルにする必要があります。

2.6.2 MPLS LSP ping/traceroute のリビジョン

MDE は、バージョン 3 の IETF LSP ping ドラフト（draft-ietf-mpls-lsp-ping-03.txt）に基づいて、IOS MPLS LSP ping/traceroute 実装をサポートします。それよりも後のバージョンの IETF LSP ping ドラフトはサポートされません。最新の IOS バージョン（12.4(6)T を含む）および IOS XR は、以降のバージョンの IETF LSP ping ドラフト /RFC 4379 を実装しています。これらの IOS または IOS XR バージョンで MDE を使用するには、バージョン 3 の IETF LSP ping ドラフトを使用するように IOS または IOS XR を設定する必要があります。そのためには、IOS または IOS XR グローバル コンフィギュレーション モードで **mpls oam** コマンドに続けて **echo revision 3** コマンドを入力する必要があります。必要に応じて、コアのすべてのルータが同じバージョンの IEFT LSP ping ドラフトまたは RFC を使用していることを確認します。

2.6.3 ポイントツーポイント アクセス回線リンクでの 31 ビット プレフィックス

IPv4 アドレッシングを使用するアクセス回線リンクに対して、MDE は、31 ビット プレフィックスで設定されたアクセス回線リンクによるトラブルシューティングをサポートします。ただし、各クラスフル ネットワークに対して、MDE は可能性のある 2 つの 31 ビット プレフィックス設定によるトラブルシューティングをサポートしません。その 2 つとは、クラスフル ネットワーク アドレスまたはネットワーク ブロードキャスト アドレスをホスト アドレスとして使用するサブネットです。たとえば、クラス A ネットワーク 10.0.0.0 において、IP アドレス 10.0.0.0 と 10.0.0.1 をホスト アドレスとして使用する 31 ビット プレフィックス サブネット、および IP アドレス 10.255.255.254 と 10.255.255.255 をホスト アドレスとして使用するサブネットはサポートされません。これらの範囲の間にあるすべてのサブネットはサポートされます。

サポートされていない 31 ビット プレフィックス サブネットを使用して MDE テストが設定された場合、テストは実行されず、サポートされていない 31 ビット プレフィックス設定であることを通知するメッセージが表示されます。このような状況では、このリンクを手動でトラブルシューティングするか、リンクを再設定してサポートされるサブネット設定を使用する必要があります。

2.7 インベントリの設定

MDE は、他の ISC モジュールにまったく依存することなく使用できます。ただし、使用する前に、ISC リポジトリに多数のオブジェクトを入力する必要があります。最低でも、これにはプロバイダー、プロバイダー リージョン、デバイスおよび PE デバイス オブジェクトが含まれます。これらの各オブジェクトのロールについて、以下で説明します。

- プロバイダー：一般的にプロバイダーとは、ネットワーク サービスをカスタマーに提供するサービス プロバイダーまたは大企業です。プロバイダーは、特定のプロバイダーを表した論理インベントリ オブジェクトです。
- プロバイダー リージョン：プロバイダー リージョンは、1 つのボーダー ゲートウェイ プロトコル（BGP）自律システム内のプロバイダー エッジ ルータ（PE）のグループであると見なされます。プロバイダー リージョンを定義する主な目的は、プロバイダーがヨーロッパ、アジア太平洋などの広い地域で一意の IP アドレス プールを使用できるようにすることです。
- デバイス：ISC のデバイスは、ネットワーク内の物理デバイスを論理的に表したものです。ISC が管理するネットワーク要素はすべて、システムのデバイスとして定義する必要があります。
- PE デバイス：PE デバイスは、特定のプロバイダー リージョンに関連付けられたプロバイダー エッジ（PE）またはプロバイダー（P）ルータを論理的に表したものです。PE デバイスは最初にデバイスとして追加してから、そこに PE デバイス タイプを割り当てる必要があります。

MPLS ネットワークのすべてのプロバイダー エッジ（PE）およびプロバイダー（P）ルータを ISC インベントリに追加する必要があります。各プロバイダー エッジ ルータはデバイスとして作成してから、ロール タイプ N-PE（ネットワーク方向の PE）を割り当てた PE デバイスとする必要があります。各プロバイダー デバイスはデバイスとして作成してから、ロール タイプ P（プロバイダー）を割り当てた PE デバイスとする必要があります。ISC インベントリへの顧客宅内装置（CPE）デバイスの追加はオプションです。

（注） デバイスがプロバイダー デバイスおよびプロバイダー エッジ デバイスの両方として動作する場合は、そのデバイスを、ロール タイプ N-PE（ネットワーク方向の PE）を割り当てた PE デバイスとして作成する必要があります。

多くの MPLS VPN ネットワークがルータ リフレクタを使用します。ルータ リフレクタを ISC インベントリに追加することを推奨します。ルータ リフレクタはデバイスとして追加してから、ロール タイプが P の PE デバイスとして追加する必要があります。ルータ リフレクタを ISC インベントリに追加することにより、MDE は、このデバイスを含む潜在的な障害を識別できます。

（注） その他の ISC 機能を使用して MPLS ネットワークを管理している場合は、必要なインベントリ オブジェクトの多くがすでに存在している可能性があります。たとえば、ISC MPLS VPN 機能を使用している場合に、必要なプロバイダー、プロバイダー リージョン、およびプロバイダー エッジ デバイスはすでに存在することがあります。その場合は、プロバイダー デバイスのみを追加する必要があります。

必要なインベントリ オブジェクトを作成するための、多数のオプションがあります。これらのオブジェクトは ISC GUI により手動で作成することも、ISC Discovery 機能、インベントリ マネージャのデバイス インポート機能、あるいは ISC API を利用するサードパーティの Operations Support System（OSS）クライアント プログラムを使用して作成することもできます。これらのオプションについては、それぞれ次の項を参照してください。

- 「2.7.1 手動作成」（P.2-7）
- 「2.7.2 Discovery」（P.2-7）
- 「2.7.3 インベントリ マネージャのデバイス インポート」（P.2-8）
- 「2.7.4 ISC API」（P.2-9）
- 「2.7.5 デバイス設定の収集」（P.2-9）

（注） デバイスの作成時に、デバイス アクセス情報（ログインおよびパスワード）が、物理デバイスに設定されている情報と一致している必要があります。

2.7.1 手動作成

手動作成では、必要な設定を ISC グラフィカル ユーザ インターフェイス（GUI）により入力することで、オブジェクトを ISC リポジトリに追加できます。オブジェクトの手動作成は、ISC リポジトリに追加するオブジェクト数が少ない場合に推奨されます。オブジェクトの手動作成の手順を次に示します。

1. プロバイダーを作成します。
2. プロバイダー リージョンを作成します。
3. デバイスを作成します。
4. インターフェイス設定などのデバイス設定を収集します。
5. PE デバイスを作成し、プロバイダー デバイスおよびプロバイダー エッジ デバイスのロールを割り当てます。

（注）　プロバイダー（P）デバイスおよびプロバイダー エッジ（PE）デバイスは、どちらも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして ISC リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「2.7 インベントリの設定」（P.2-5）を参照してください。ISC サーバおよびデバイス間で使用するトランスポート メカニズムを選択する場合、Cisco CNS Configuration Engine は MDE に必要なコマンドをサポートしないため、MDE と組み合わせて使用できません。Cisco CNS Configuration Engine を MDE と使用しようとすると、MDE はデバイスに接続できないと間違って報告します。

プロバイダー、プロバイダー リージョン、デバイスおよび PE デバイス オブジェクトを手動で作成する方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の第 3 章を参照してください。

デバイスを手動作成する場合は、対象のデバイスのインターフェイス設定も追加する必要があります。

インターフェイス設定は、デバイス作成時に手動で追加することも、タスク マネージャの Collect Configuration タスクを使用して追加することもできます。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「2.7.5 デバイス設定の収集」（P.2-9）を参照してください。Collect Configuration タスクを使用することを推奨します。

2.7.2 Discovery

Discovery では、XML ファイルに最低限のデバイスおよびトポロジ情報を設定することにより、ネットワークのデバイスを ISC リポジトリに追加できます。次に、Discovery プロセスはこれらのデバイスを照会し、必要なデバイスおよびトポロジ情報を ISC リポジトリに入力します。リポジトリに追加するオブジェクト数が多い場合は、Discovery の使用を推奨します。

ISC Discovery には、デバイスを検出するための方法として CDP とデバイス / トポロジの 2 つが用意されています。デバイス検出を実行する前に、Discovery に必要な XML コンフィギュレーション ファイルを作成することが必要です。デバイスの検出方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の第 4 章を参照してください。

（注）　プロバイダー（P）デバイスおよびプロバイダー エッジ（PE）デバイスは、どちらも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして ISC リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「2.7 インベントリの設定」（P.2-5）を参照してください。

（注）　Discovery の完了後に、検出されたすべてのデバイスに対してタスク マネージャの Collect Configuration タスクを実行する必要があります。Collect Configuration タスクを実行しないと、MDE は検出されたデバイスにログインして、トラブルシューティングを実行できません。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「2.7.5 デバイス設定の収集」（P.2-9）を参照してください。

2.7.3 インベントリ マネージャのデバイス インポート

インベントリ マネージャのデバイス インポート機能を使用すると、デバイスの Cisco IOS 実行コンフィギュレーションを含むファイルから ISC リポジトリに複数のデバイスをインポートできます。リポジトリに追加するオブジェクト数が多い場合は、インベントリ マネージャのデバイス インポート機能の使用を推奨します。デバイスのインポート方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の第 3 章にある「Inventory Manager」の項を参照してください。

プロバイダー（P）およびプロバイダー エッジ（PE）デバイスをインポートする前に、必要なプロバイダーおよびプロバイダー リージョン オブジェクトを作成する必要があります。プロバイダーおよびプロバイダー リージョン オブジェクトを手動で作成する方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の第 3 章を参照してください。

デバイスをインポートするときは、Cisco IOS 実行コンフィギュレーションを含むファイルがあるディレクトリを指定する必要があります。ファイル名は指定しないでください。ファイルは、ISC サーバからアクセスできるファイル システムのディレクトリに存在する必要があります。

（注）　プロバイダー（P）デバイスおよびプロバイダー エッジ（PE）デバイスは、どちらも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして ISC リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「2.7 インベントリの設定」（P.2-5）を参照してください。

（注）　イネーブル シークレット パスワードは、Cisco IOS 実行コンフィギュレーションに追加される前に暗号化されます。その結果、デバイス インポート機能は、ISC リポジトリにインポートするデバイスに対してイネーブル シークレット パスワードを設定できません。インポートするすべてのデバイスにイネーブル シークレット パスワードが設定されている場合は、ISC リポジトリでこれらのデバイスに手動でイネーブル パスワードを設定する必要があります。イネーブル シークレット パスワードとイネーブル パスワードの両方がデバイスに設定されている場合、インベントリ マネージャのデバイス インポート機能は ISC リポジトリに追加するデバイスにイネーブル パスワードを使用します。このパスワードは正しいイネーブル シークレット パスワードで上書きする必要があります。ISC リポジトリのデバイスのイネーブル パスワードは、デバイスのインポート中にも、デバイスのインポート後にも設定できます。

（注）　デバイス インポートの完了後に、インポートされたすべてのデバイスに対してタスク マネージャの Collect Configuration タスクを実行する必要があります。Collect Configuration タスクを実行しないと、MDE はインポートされたデバイスにログインして、トラブルシューティングを実行できません。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「2.7.5 デバイス設定の収集」（P.2-9）を参照してください。

2.7.4 ISC API

Cisco IP Solution Center（ISC）アプリケーション プログラム インターフェイス（API）を使用すると、Operations Support System（OSS）クライアント プログラムを使用して ISC システムに接続できます。ISC API は、ISC サーバからデータの挿入、取得、更新、および削除を行うためのメカニズムを提供します。API を使用して、必要なプロバイダー、プロバイダー リージョン、デバイスおよび PE デバイス オブジェクトを追加できます。

（注）　ISC API は MDE に標準では含まれておらず、別途購入できます。

ISC API の使用方法の詳細については、『*Cisco IP Solution Center API Programmer Guide, 6.0*』および『*Cisco IP Solution Center API Programmer Reference, 6.0*』を参照してください。

2.7.5 デバイス設定の収集

タスク マネージャの Collect Configuration タスクを使用して、ISC リポジトリのデバイスにインターフェイス設定を追加することを推奨します。タスク マネージャの Collect Configuration タスクはネットワークの物理デバイスに接続し、ルータからデバイス情報（インターフェイス設定を含む）を収集して、その情報を ISC リポジトリに入力します。

タスク マネージャの Collect Configuration タスクを使用してデバイス インターフェイス設定を追加する方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の第 7 章にある「Inventory Manager」の項を参照してください。

オフラインの設定収集は MDE に対してのみ使用可能で、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』に説明があります。

2.7.5.1 ISC リポジトリとデバイス設定との同期

（注）　MDE の精度は最新のデバイス情報に依存します。デバイス設定に何らかの変更を加えた後および定期的に、デバイス設定を物理デバイスと再同期することを推奨します。これにより、ISC インベントリに保持されているデバイス設定がネットワークの物理デバイスと一致します。

タスク マネージャのスケジュール タスクを使用して、デバイス設定を最新に保つことを推奨します。Collect Configuration と Collect Configuration from File のどちらでも使用できます。タスク マネージャのスケジュール タスク Collect Configuration を作成する方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の第 7 章にある「Inventory Manager」の項を参照してください。MPLS ネットワークの PE および P ルータは、すべてがタスク マネージャのスケジュール タスク Collect Configuration を使用してその設定を収集する必要があります。タスク マネージャの Collect Configuration タスクでは、インターフェイス設定およびその他のデバイス属性の詳細が収集されます。タスク マネージャの Collect Configuration タスクの実行スケジュール間隔は、ネットワークに対する設定変更の頻度に依存します。タスク マネージャの Collect Configuration タスクを各 P および PE ルータで毎日実行することを推奨します。