CHAPTER 12

デバイスの検出

Cisco Prime Collaboration Manager ディスカバリ プロセスには、次の 3 つのフェーズが含まれます。

- アクセス レベル検出：Prime CM で行われる処理は次のとおりです。
  a. デバイスに対して ping（ICMP）を実行できるかどうかのチェックが行われます。ICMP がデバイスでイネーブルになっていない場合は、デバイスは [Unreachable] 状態に移行されます。ICMP 検証をディセーブルにする方法については、「デバイスの状態」（P.12-2）を参照してください。
  b. IP アドレスに基づいて、定義済みのクレデンシャル プロファイルがすべて取得されます。クレデンシャル プロファイルの定義方法については、「クレデンシャルの管理」を参照してください。
  c. SNMP クレデンシャルが一致しているかどうかのチェックが行われます。
  d. デバイスのタイプが特定されます。
  e. デバイスのタイプに基づいて、その他すべての必須デバイス クレデンシャルが検査されます。必須クレデンシャルが定義されていない場合、検出は失敗します。

     必須デバイス クレデンシャルについては、『*Cisco Prime Collaboration Manager 1.2 Quick Start Guide*』の「Setting Up the Network」の項を参照してください。
- インベントリ ディスカバリ：Prime CM は、MIB-II とその他のデバイスの MIB をポーリングして、デバイス インベントリ、ネイバー スイッチ、およびデフォルト ゲートウェイに関する情報を収集します。また、ポーリングされたデバイスが Prime CM でサポートされるかどうかを検査します。
- パス トレース検出：Prime CM は、CDP がデバイスでイネーブルになっているかどうかを検査し、CDP に基づいてトポロジを検出します。デバイス間のリンクは CDP を使用して計算され、Prime CM データベースに保持されます。

  Prime CM は、レイヤ 2 とレイヤ 3 の両方のパスを検出します。
  – Cisco 500 シリーズ、1000 シリーズ、および 3000 シリーズの TelePresence システムの場合、Prime CM ではファースト ホップ ルータおよびスイッチの検出が行われます。「CTS-Manager のディスカバリ ライフ サイクル」を参照してください。
  – Cisco C シリーズおよび Ex シリーズの TelePresence システムの場合、Prime CM では、ファースト ホップ ルータおよびスイッチの検出は*行われません*。「TMS の検出ライフ サイクル」を参照してください。

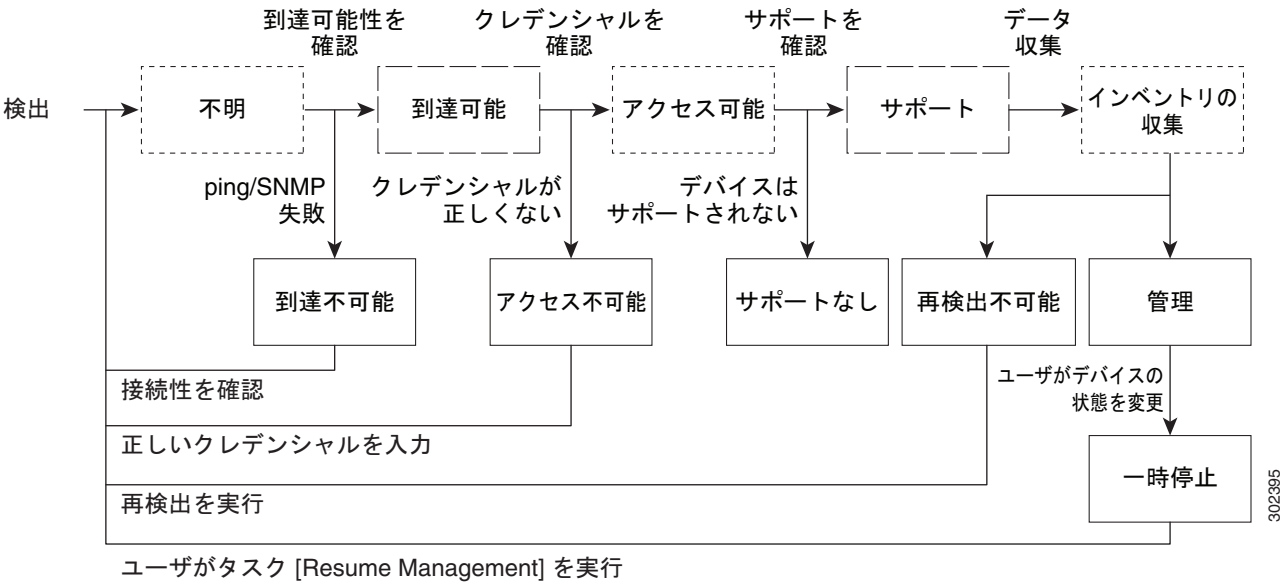
  レイヤ 3 パスは、トラブルシューティング ワークフローが手動で起動されるか自動的に起動されると検出されます。

  トラブルシューティング ワークフローの詳細については、「セッションのトラブルシューティング」（P.23-1）を参照してください。

Prime CM でサポートされているデバイスのリストについては、『*Cisco Prime Collaboration Manager 1.2 Supported Devices Table*』を参照してください。

図 12-1 に、デバイス ディスカバリのライフ サイクルを示します。

図 12-1　デバイス ディスカバリのライフ サイクル



デバイスの状態

デバイスの状態は、Prime CM がデバイスにアクセスでき、インベントリを収集できることを示しています。デバイスの状態は、ディスカバリまたはインベントリの更新タスクのいずれかを実行した後に限り更新されます。

Prime CM には、次のデバイスの状態を表示します。

- [Unknown]：これは、デバイスが最初に追加されたときの事前の状態です。
- [Unreachable]：Prime CM からデバイスに対し、ICMP を使用して ping を実行することができません。

  ICMP がデバイスでイネーブルになっていない場合は、デバイスは [Unreachable] 状態に移行されます。
- [Unsupported]：Prime CM は、デバイスをデバイス カタログと比較します。デバイスが一致しないか、SysObjectID が不明な場合は、デバイスはこの状態に移行されます。
- [Accessible]：Prime CM は、要求されたすべてのクレデンシャルからデバイスにアクセスできます。これは、デバイス ディスカバリ中の中間状態である、アクセス レベル ディスカバリの一部です。
- [Inaccessible]：Prime CM は、要求されたいずれのクレデンシャルからもデバイスにアクセスできません（「クレデンシャルの管理」を参照）。クレデンシャルを確認して、デバイスを検出する必要があります。

- [Inventory Collected]：Prime CM は、要求されたデータ コレクタを使用して、必要なデータを収集できます。これは、デバイス ディスカバリ中の中間状態である、インベントリ ディスカバリの一部です。
- [Undiscoverable]：Prime CM では、要求されたデータ コレクタを使用して、必要なデータを収集することができません。
  - [CTS-Manager]：Prime CM は、CTS-Manager からエンドポイント データを収集する必要があります。収集されない場合、CTS-Manager の状態は [Undiscovered] に移行します。Cisco Unified CM、CTS、CTMS、およびその他のネットワーク デバイスには、収集が必要なデータはありません。
  - SNMP や HTTP（HTTPS）のタイムアウトにより、接続性の問題が発生する場合があります。また、HTTP（HTTPS）を使用してデータを収集する場合は、一度に 1 人の HTTP（HTTPS）ユーザだけがログインできます。Prime CM でこれらのいずれかの問題が発生した場合は、デバイスの状態が [Undiscoverable] 状態に移行されます。

  再検出を実行する必要があります。
- [Managed]：Prime CM では、必要なデバイス データがインベントリ データベースへ正常にインポートされています。この状態のデバイスでは、すべてのセッション、エンドポイント、およびインベントリ データを使用できます。この状態になっているデバイスだけをトラブルシューティングできます。
- [Suspended]：ユーザがデバイスのモニタリングを一時停止しています。この状態のデバイスでは、セッションとエンドポイント データは表示されません。この状態のデバイスでは、定期的なポーリングも実行されません。これらのデバイスのインベントリは更新できません。これを行うには、[Resume Management] を実行する必要があります。一時停止されたデバイスの詳細については、「管理対象デバイスの一時停止およびレジューム」（P.14-13）を参照してください。

デバイスを検出するための順序

Prime CM でデバイスを検出する場合は、次の順序に従って操作を行う必要があります。

1. [Manage Credentials] ページ（[Inventory] > [Device Inventory] > [Manage Credentials]）を使用して、デバイスのクレデンシャルを入力します。

   Prime CM を使用してモニタするすべてのビデオ コラボレーション デバイスについてクレデンシャルを入力する必要があります。詳細については、「クレデンシャルの管理」を参照してください。
2. [Inventory] ページ（[Inventory] > [Device Inventory] > [Discover Devices]）を使用して、デバイスを検出します。

   ネットワーク内に CTS-Manager、TMS、Cisco Unified CM、VCS などの管理デバイスやコール/セッション制御デバイスが導入されている場合は、これらのデバイスを最初に検出することができます。アプリケーション マネージャやコール プロセッサの検出を実行すると、登録されているすべてのビデオ コラボレーション デバイスが検出されます。

（注）
- Prime CM のライセンス付きバージョンをインストールしている場合は、CTS-Manager Reporting API の設定が必須です。CTS-Manager 1.7 または 1.8 でこの機能が設定されていない場合、Prime CM は CTS-Manager を管理しません。
- Cisco TMS 13.0 または 13.1 を使用している場合は、Cisco TMS Booking API 機能の設定が必須です。この機能が設定されていない場合、セッションはモニタされません。

  Cisco TMS 13.2 以降では、Cisco TMS Booking API 機能を設定する必要はありません。

- DMZ 内で Cisco VCS Expressway が設定されている場合は、Prime CM から SNMP を介して Cisco VCS Expressway にアクセスすることができます。アクセスできない場合、このデバイスは [Inaccessible] 状態になります。

Cisco Unified IP Phone 8900 および 9900 シリーズ、Cisco Cius、および Cisco TelePresence Movi エンドポイント以外のデバイス（エンドポイント、テレプレゼンス サーバなど）を個別に検出することもできます。これらのエンドポイントは、登録されているコール プロセッサの検出を介してのみ検出されます。

（注） Cisco Cius と Cisco Unified IP Phone 8900 および 9900 シリーズの検出では、HTTP インターフェイスを有効にする必要があります。HTTP インターフェイスが有効になっていないと、これらのデバイスはインベントリ テーブルに表示されません。

Cisco MSE Supervisor を使用している場合は、その Cisco MSE Supervisor が TMS に登録されていることを確認してください。

入力したデバイスのクレデンシャルが正しいことを確認する必要があります。Prime CM は、ディスカバリ プロセス中に、検出するデバイスに基づいて、CLI、HTTP（HTTPS）、または SNMP を使用してデバイスに接続します。CTS エンドポイント、CTMS、およびネットワーク デバイス（ルータおよびスイッチ）では、いずれにおいても CDP がイネーブルになっている必要があります。

Cisco Unified CM クラスタの検出

Prime CM は、Cisco Unified CM クラスタをサポートしています。クラスタ ID が一意であることを確認する必要があります。Cisco Unified CM パブリッシャでは、必要なロールを使用して JTAPI アプリケーションのユーザ アカウントを作成する必要があります。

管理が必要なエンドポイントはすべて、Cisco Unified CM のアクセス コントロール リストに含まれている必要があります。Cisco Unified CM の SNMP ユーザの設定に、アクセス コントロール リストの使用が指定されている場合は、クラスタ内に含まれるすべての Cisco Unified CM ノードで Prime CM サーバの IP アドレスを入力する必要があります。

Prime CM は、クラスタを管理するために、Cisco Unified CM パブリッシャだけを検出して管理する必要があります。すべてのサブスクライバは、パブリッシャを経由した場合だけ検出できます。サブスクライバは直接検出できません。

Prime CM は、クラスタをモニタするためにクラスタ パブリッシャを管理する必要があります。JTAPI は、クラスタ パブリッシャで設定する必要があり、すべてのサブスクライバでコンピュータ テレフォニー インテグレーション（CTI）サービスが実行されている必要があります。

Cisco VCS クラスタの検出

Prime CM は、Cisco VCS クラスタをサポートしています。クラスタ名は一意でなければなりません。Prime CM で管理が必要なエンドポイントはすべて、Cisco VCS マスターに登録する必要があります。

図 12-2 に、Cisco TelePresence Manager（CTS-Manager）のディスカバリ ライフ サイクルを示します。

図 12-2　CTS-Manager のディスカバリ ライフ サイクル

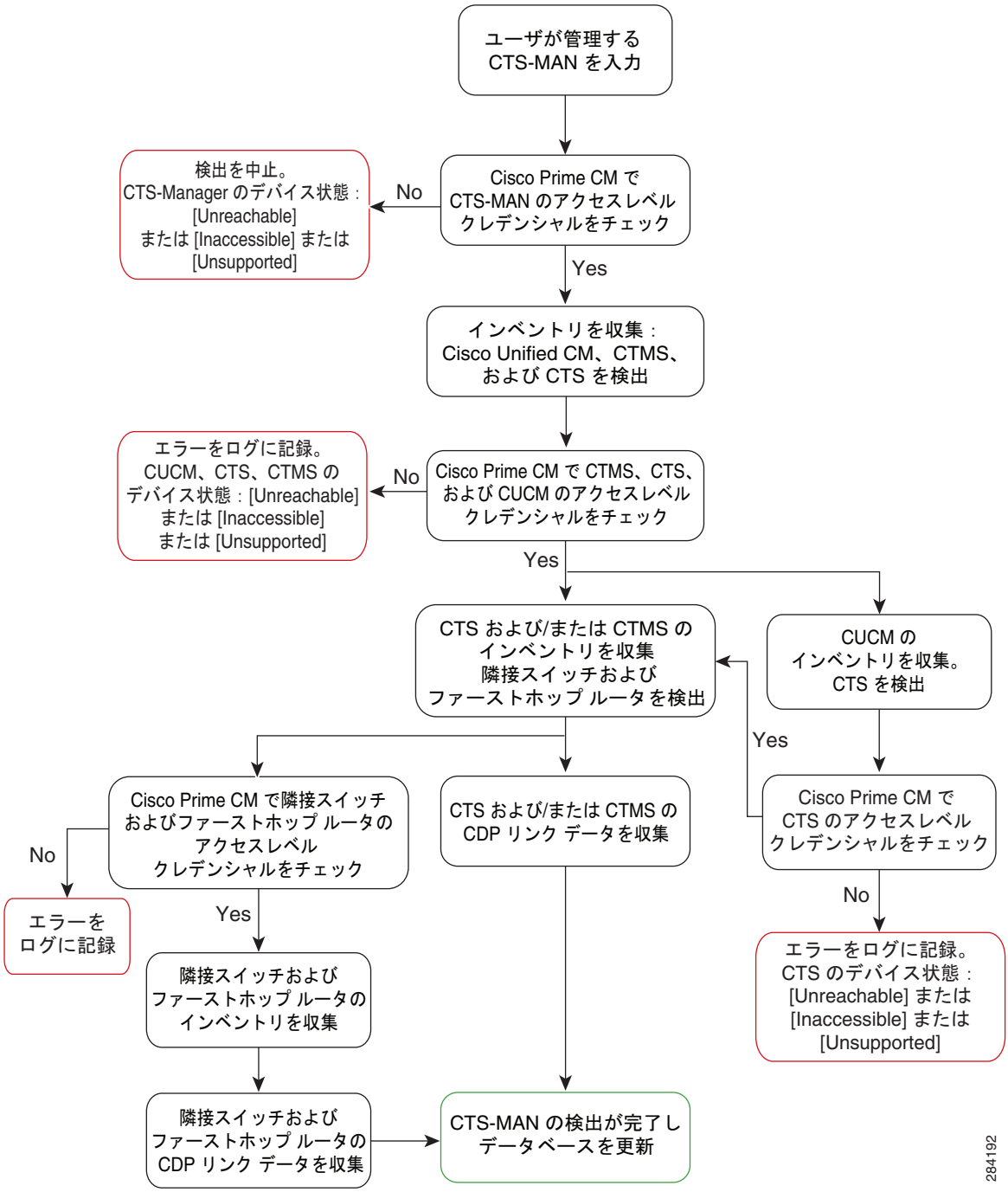
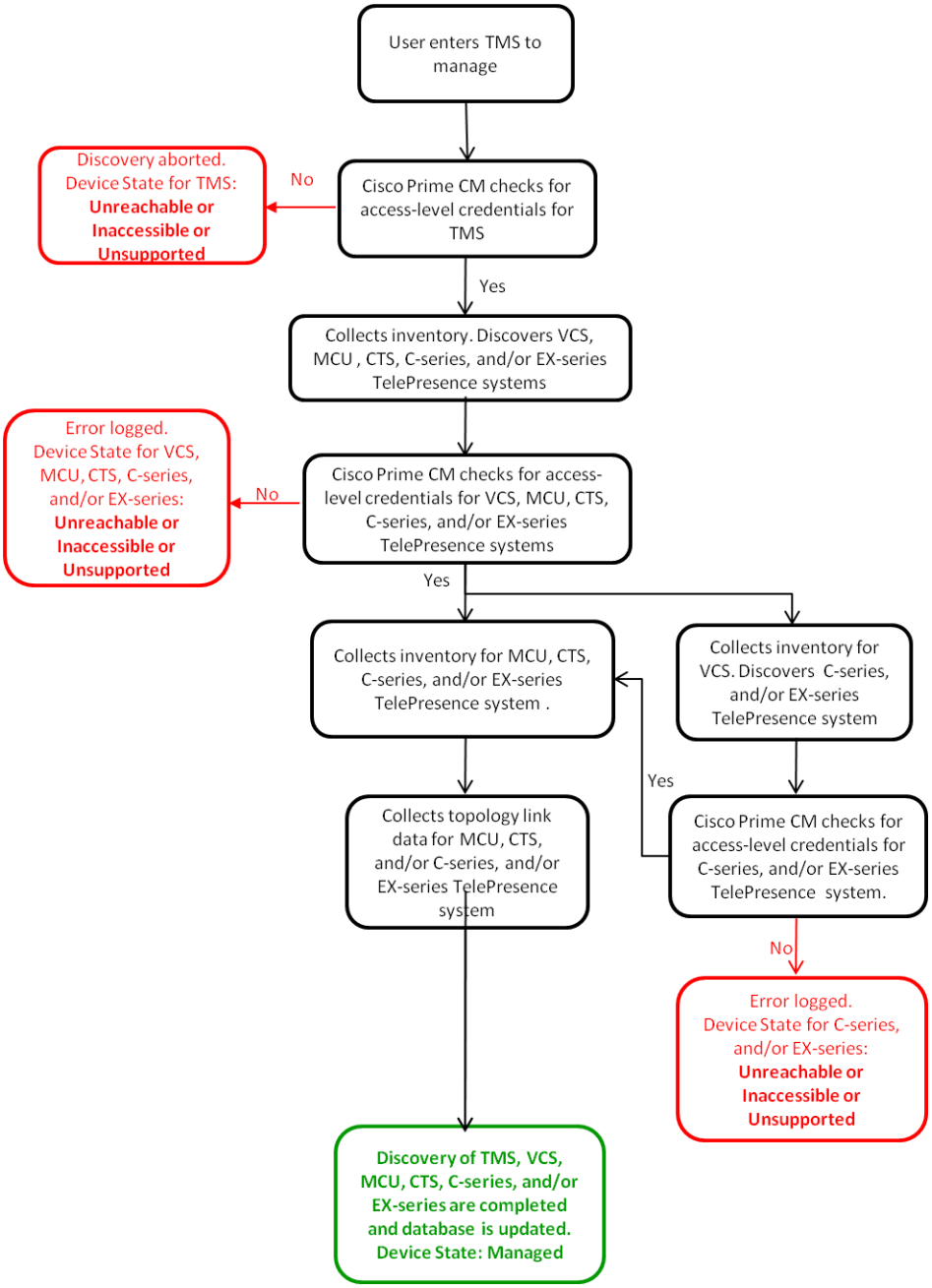


図 12-3 は、Cisco TelePresence 管理システム（Cisco TMS）の検出ライフ サイクルを示したものです。

図 12-3　TMS の検出ライフ サイクル



デバイスの追加

次の場合に、検出を行う必要があります。

- Prime CM データベースに新しいデバイスを追加する場合。
- デバイスの IP アドレスを変更した場合。

  Cisco VCS に登録されているエンドポイントは、IP アドレスが変更されると自動的に検出されます。

  Cisco Unified CM に登録されている DHCP 対応エンドポイントの IP アドレスが変更された場合、Prime CM では、そのエンドポイントを自動的には検出できない場合があります。Cisco Unified CM に登録されているすべての Cisco TelePresence システムについても同様です。以下をもう一度検出する必要があります。

  - エンドポイント（新しい IP アドレスまたはホスト名を指定して）。
  - エンドポイントが登録されている Cisco Unified CM インスタンス。
  - エンドポイントが登録されている CTS-Manager。

  ネットワーク デバイスおよびインフラストラクチャ デバイス（CTS-Manager、Cisco Unified CM、CTMS、Cisco MCU、Cisco VCS、Cisco TS など）に対して IP アドレスが変更された場合は、新しい IP アドレスまたはホスト名を指定して、これらのデバイスの検出を行う必要があります。

デバイスを即時に検出するか、検出ジョブをスケジューリングできます。

デバイスを検出するには、次のようにします。

ステップ 1　[Inventory] > [Device Inventory] を選択します。

[Inventory] ページが表示されます。

ステップ 2　[Discover Devices] をクリックします。

[Discovery Setup] ウィンドウが表示されます。

ステップ 3　ジョブ名を入力します。

ステップ 4　[True] をクリックして、デバイス検出時のデバイス アクセシビリティの検証を有効にします。

Prime CM は、SNMP、CLI、HTTP（HTTPS）、および JTAPI を使用して、デバイスのアクセシビリティを検査します。

ステップ 5　デバイスの IP アドレスまたはホスト名を入力します。

サポートされる区切り文字（コンマ、コロン、パイプ、またはブランク スペース）のいずれかを使用して、複数の IP アドレスまたはホスト名を入力できます。

クラスタを管理するには、コール プロセッサ パブリッシャの IP アドレスだけを入力します。すべてのサブスクライバは、パブリッシャを経由した場合だけ検出できます。サブスクライバは直接検出できません。

定期的な検出ジョブをスケジューリングするか、検出ジョブを即時に実行できます。ジョブを即時に実行するには、ステップ 7 に進みます。

ステップ 6　スケジューリングの詳細を入力して、検出ジョブをスケジュールします。

- [Start Time] : [Start Time] をクリックして、開始日と開始時刻をそれぞれ *yyyy/MM/dd* と *hh:mm AM/PM* 形式で入力します。

- カレンダーから開始日と開始時刻を選択する場合は、日付ピッカーをクリックします。表示される時刻は、クライアント ブラウザの時刻です。スケジューリングされた定期的ジョブは、この指定時刻に実行されます。
- [Recurrence] : [None]、[Hourly]、[Daily]、[Weekly]、または [Monthly] をクリックして、ジョブ期間を指定します。
- [Settings] : ジョブ期間の詳細を指定します。
- [End Time] : 終了日時を指定しない場合は、[No End Date/Time] をクリックします。[Every number of Times] をクリックして、指定した期間にジョブが終了するまで、そのジョブが実行される回数を設定します。終了日と終了時刻をそれぞれ *yyyy/MM/dd* と *hh:mm AM/PM* 形式で入力します。

ステップ 7　[Run Now] をクリックして、検出ジョブをすぐに実行するか、[Schedule] をクリックして、定期的な検出ジョブを後で実行するようにスケジューリングします。

デバイスの検出は、入力したデバイスに基づいて、[Current Inventory] テーブルに表示されるまで数分かかることがあります。

[Inventory] ページの [List Discovery Jobs] ボタンを使用して、ジョブの進捗状況とステータスを確認できます。[Job Management] ページに、検出ジョブのリストが表示されます。

検出ジョブが完了したら、ジョブのステータスを確認します。クレデンシャルが正しくないために検出されなかったデバイスが存在する場合もあります。これらのデバイスについては、クレデンシャルを検証し（「クレデンシャルの検証」（P.11-8）を参照）、検出を再度実行します。

CTS-Manager を検出できず、「`UNDISCOVERABLE Exception:: null`」というエラーが表示された場合は、検出を再度実行します。この問題が発生するのは、同時に複数のユーザが CTS-Manager にアクセスしている場合です。

デバイスを初めて検出する場合は、検出ジョブの完了後に、[Sessions Monitoring]（[Monitoring] > [Session Monitoring]）ページの [Import Sessions] リンクを使用して、セッションをインポートする必要があります。

詳細については、「CTS-Manager および Cisco TMS からのセッションのインポート」（P.15-8）を参照してください。

同じデバイスを複数回検出する場合は、再検出オプションを使用します。詳細については、「デバイスの再検出」（P.12-8）を参照してください。

追加されたデバイスの可視性設定を確認できます。エンドポイントの可視性機能によって、Prime CM がエンドポイントの動作をモニタするレベルが判別されます。詳細については、「エンドポイントのリアルタイム可視性」（P.15-12）を参照してください。

デバイスの再検出

すでに検出されたデバイスを再検出できます。以前に入力したクレデンシャルを Prime CM データベースで使用できます。システムによって新しい変更が更新されます。どの状態のデバイスでも再検出できます。

次の場合に、再検出タスクを実行できます。

- 削除したデバイスを再検出する必要がある場合。詳細については、「削除されたデバイスの再検出」（P.12-9）を参照してください。
- ファースト ホップ ルータ設定に変更があり、ソフトウェア イメージを更新する場合。[Rediscover] ボタンを使用して、単一デバイスの再検出を実行できます。

- クレデンシャル、場所、タイムゾーン、およびデバイス設定（IP アドレス、ホスト名、SIP URI、H323 ゲートキーパー アドレスなど）に変更がある場合。詳細については、「クレデンシャル更新後のデバイスの再検出」（P.12-9）を参照してください。

再検出のワークフローは、検出の場合と同じです。詳細については、図 12-1 を参照してください。

削除されたデバイスの再検出

[Current Inventory] ペインにある [Rediscover] ボタンを使用して、[Current Inventory] テーブルにリストされているデバイスを再検出することができます。単一のデバイスを選択して、再検出を実行できます。

削除されたデバイスを再検出するには、次のようにします。

ステップ 1　[Inventory] > [Device Inventory] を選択します。

[Device Inventory] ページが表示されます。

ステップ 2　[Current Inventory] テーブルから状態が [Deleted] のデバイスをフィルタリングします。

クイック フィルタとして [Deleted] を使用すると、この状態にあるデバイスのリストを取得できます。

ステップ 3　再検出するデバイスを選択します。

ステップ 4　[Rediscover] をクリックします。

「Are you sure you want to Rediscover the selected devices?」というメッセージが表示されます。

ステップ 5　[OK] をクリックします。

「Selected devices Rediscovered successfully.」というメッセージが表示されます。

[Inventory] ページの [List Discovery Jobs] ボタンを使用して、ジョブの進捗状況とステータスを確認できます。[Job Management] ページに、検出ジョブのリストが表示されます。

クレデンシャル更新後のデバイスの再検出

クレデンシャル（「クレデンシャルの管理」を参照）を変更後にデバイスを再検出するには、次のようにします。

ステップ 1　[Inventory] > [Device Inventory] を選択します。

[Inventory] ページが表示されます。

ステップ 2　[Discover Devices] をクリックします。

[Discovery Setup] ウィンドウが表示されます。

ステップ 3　[True] をクリックして、デバイス検出時のデバイス アクセシビリティの検証を有効にします。

Prime CM は、SNMP、CLI、HTTP（HTTPS）、および JTAPI を使用して、デバイスのアクセシビリティを検査します。IP アドレス / ホスト名を使用してデバイスを再検出するには、ステップ 5 に進みます。

ステップ 4　デバイスのタイプまたはデバイスのステータスに基づいてデバイスを再検出するには、[Re-discover devices based on a criteria] チェックボックスをオンにします。（このオプションを選択すると、IP アドレスまたはホスト名を入力してデバイスを再検出することはできなくなります）。

- [Device type] : Cisco Unified IP Phone 8900 および 9900 シリーズ、Cisco Cius、および Cisco TelePresence Movi エンドポイント以外のすべてのデバイスを再検出できます。

– [Device status] : [Inaccessible]、[Unreachable]、[Undiscoverable]、[Unknown]、[Deleted]、および [Unsupported] の各ステータスのデバイスを再検出できます。

（注） Cisco Unified IP Phone 8900 および 9900 シリーズ、Cisco Cius、および Cisco TelePresence Movi エンドポイントを再検出するには、エンドポイントの IP アドレスを入力します（ステップ 5）。

ステップ 5　デバイスの IP アドレスを入力します。

サポートされる区切り文字（コンマ、コロン、パイプ、またはブランク スペース）のいずれかを使用して、複数の IP アドレスまたはホスト名を入力できます。

ステップ 6　[Run Now] をクリックして、再検出ジョブをすぐに実行するか、[Schedule] をクリックして、定期的な再検出ジョブを後でスケジューリングします。

定期的な再検出ジョブをスケジューリングするには（定期的な検出ジョブのスケジューリングと同様）、「デバイスの追加」（P.12-7）のステップ 6 に進みます。

[Inventory] ページの [List Discovery Jobs] ボタンを使用して、ジョブの進捗状況とステータスを確認できます。[Job Management] ページに、検出ジョブのリストが表示されます。