使用する前に

この項では、IP Communications Operations Manager（Operations Manager）をセットアップし、診断結果を表示するための手順を簡単に説明します。次のトピックを取り上げます。

デバイスを監視するための Operations Manager の設定

Operations Manager は、CiscoWorks Common Services の Device and Credentials Repository（DCR）から監視するデバイスを取得します。DCR は、個々のアプリケーションが使用するデバイスおよびそれらのクレデンシャルの共通リポジトリです。

Operations Manager がネットワークの監視を開始する前に、次のことを実行する必要があります。

- DCR および Operations Manager デバイス選択を設定する必要があります。DCR を設定するには、オプションを理解し、ユーザのサイトにとって何が最も有用であるかを判断する必要があります。
- Operations Manager がインベントリ収集を完了している必要があります。

表 3-1 に、完了する必要のある手順をすべて示します。

表 3-1　デバイスの監視を開始する方法

	説明	参照箇所
ステップ 1	デバイスを DCR に追加します。 3 つのオプションがあります。 • Operations Manager を使用して、デバイスを DCR に追加する。これは、物理ディスカバリと呼ばれます。 • 他のサーバのアプリケーションとマスター リポジトリを共有する • シード ファイルを使用してバルク インポートを実行し、DCR にデバイスをインポートする	 Operations Manager から DCR へのデバイスの追加（P.3-4） 他の CiscoWorks アプリケーションとの DCR の共有（P.3-3） Common Services のオンライン ヘルプの手順を参照してください。
ステップ 2	デバイス選択を設定します。	Operations Manager のデバイス選択（自動または手動）の設定（P.3-6）
ステップ 3	インベントリ収集を完了し、デバイスの監視を開始できるようにします。	
ステップ 4	Service Level View を使用して、デバイスのインポートを確認します。	Operations Manager に追加されたデバイスの確認（P.3-7）

デバイス インポート用にサポートされる NMS 環境

DCR を使用すると、次のように他のアプリケーションとデバイス リストを共有できます。

- 次の場所から DCR にデバイスをインポートできます。
  - Network Management System（NMS; ネットワーク管理システム）：DCR は、リモート NetView および HP OpenView インストールからのインポートをサポートしています（サポートされるバージョンは、ユーザ インターフェイスに表示されます）。
  - ファイル：ファイルは、別の製品からエクスポートしたものをフォーマットして DCR にインポートできます。ファイル形式は、『*User Guide for CiscoWorks Common Services*』に説明されています。

（注）　Operations Manager の物理デバイス ディスカバリも、検出したデバイスを DCR に追加します。

- すべてのデバイスのマスターリストを管理し、リストをクライアント（スレーブとして設定され、同じ管理ドメイン内にある DCR のその他のインスタンス）と共有するように DCR サーバを設定できます。

他の CiscoWorks アプリケーションとの DCR の共有

DCR を使用すると、CiscoWorks ネットワーク管理アプリケーションは、クライアント / サーバ メカニズムを通じてデバイス リストおよびクレデンシャルを共有できます。Operations Manager サーバでは、デフォルトで、DCR がスタンドアロンまたは独立リポジトリとして設定されています。

オプションで、次のものを含む管理ドメインに加わるように DCR を設定できます。

- 1 つの共有マスター リポジトリ
- マスター リポジトリの正確な複製であり、マスター リポジトリと常に同期している 1 つ以上のクライアント リポジトリ

次のシナリオは、DCR 管理ドメイン内での Operations Manager の使用方法を示しています。

シナリオ：DCR 管理ドメイン内の Operations Manager

このシナリオでは、DCR を使用してデバイス リストとデバイス クレデンシャルを共有するように、Operations Manager および別の CiscoWorks アプリケーションを設定する方法の 1 つを示します。

Operations Manager（専用システムにインストールされている必要がある）と CiscoWorks Resource Manager Essentials（RME）は、個別のシステムにインストールされています。RME システムでは、DCR がサーバ（マスター）として設定されています。Operations Manager システムでは、DCR が RME システムの DCR サーバに対するクライアント（スレーブ）として設定されています。さらに、DCR から Operations Manager システムにデバイスの手動選択が設定されています。

RME システムの DCR にデバイスをインポートする場合、Operations Manager システムの DCR クライアントにもデバイスが追加されます。Operations Manager にデバイスの手動選択が設定されているので、手動で選択しない限り、Operations Manager インベントリにデバイスは追加されません。

DCR のモード（マスターおよびスレーブ）の設定

デフォルトでは、Operations Manager サーバの DCR はスタンドアロンまたは独立リポジトリとして設定されています。Operations Manager の DCR をマスターおよびスレーブのどちらに設定するかを判断する場合の手順は、オンライン ヘルプおよび『*User Guide for CiscoWorks Common Services*』に示されています。前提条件となる作業を実行し、適切な順序でマスターおよびスレーブに設定する必要があります。次の手順は、作業を開始し、オンライン ヘルプで必要な情報を特定するのに役立ちます。

（注）　Operations Manager を起動するには、P.3-11 の「Operations Manager の起動」を参照してください。

ステップ 1　Operations Manager ホームページで、ページの右上隅にある **CiscoWorks** リンクをクリックします。CiscoWorks ホームページが別のウィンドウに表示されます。

ステップ 2　CiscoWorks ホームページで、**Common Services > Device and Credentials > Admin** を選択します。Admin ページが表示されます。

ステップ 3　左側のペインにある TOC から Mode Settings を選択します。Mode Settings ウィンドウが表示されます。

ステップ 4　このページの右上隅にある Help リンクをクリックします。マスターとスレーブの設定の前提条件を実行する手順を検索します。次の作業が含まれます。

- マスター DCR によるシステムへのピア サーバ ユーザの追加
- スレーブ DCR によるシステム上でのシステム アイデンティティ ユーザの作成
- セキュリティ証明書のコピー

オンライン ヘルプの手順に従って、前提条件を実行し、正しい順序でマスターおよびスレーブに設定します。

Operations Manager から DCR へのデバイスの追加

Operations Manager は、物理ディスカバリを通じて、デバイスを DCR に追加します。

（注）　バルク インポート（NMS またはファイルからのインポート）を使用してデバイスを DCR に追加するには、Common Services のオンライン ヘルプの手順に従ってください。

Operations Manager の物理ディスカバリの実行

ステップ 1　**Devices > Device Management** を選択します。Device Management: Summary ページが表示されます。

ステップ 2　Last Discovery フィールドおよび Next Discovery フィールドの横にある **Configure** ボタンをクリックします。Discovery ページが表示されます。

ステップ 3　次の表に示すデータを入力します。

フィールド	処理 / 説明
Seed Devices	カンマ区切りの IP アドレスのリストを入力するか、Use all devices currently in Device and Credentials Repository チェックボックスをオンにします。
Ping Sweep	（オプション）これは、シード デバイスに基づいたディスカバリを使用する場合の代替です。 Use Ping Sweep チェックボックスをオンにし、*/netmask* 仕様を使用してカンマ区切りの IP アドレス範囲のリストを指定します。 たとえば、172.20.57.1/24 を使用して、172.20.57.1 ～ 172.20.57.255 の ping スイープ範囲を指定します。

フィールド	処理 / 説明
IP Address	(オプション)次の対象とするデバイスのカンマ区切りの IP アドレスまたは IP アドレス範囲を入力します。 • Include：自動ディスカバリ プロセスの対象にする • Exclude：自動ディスカバリ プロセスの対象から除外する IP アドレス範囲を指定するときにワイルドカードを使用できます。 アスタリスク（*）は、1 ～ 255 のオクテット範囲を示します。また、[xxx-yyy] 表記を使用してオクテット範囲を制限することもできます。 次の例を参考にしてください。 • 172.20.57/24 サブネットのすべてのデバイスを自動ディスカバリ プロセスの対象にするには、172.20.57.* の Include フィルタを入力します。 • 172.20.57.224 ～ 172.20.57.255 の IP アドレス範囲のデバイスを自動ディスカバリ プロセスの対象外にするには、172.20.57.[224-255] の Exclude フィルタを入力します。 両方のタイプのワイルドカードを、たとえば 172.20.[55-57].* のように同じ範囲指定で使用できます。Include フィルタおよび Exclude フィルタの両方が指定されている場合、Exclude フィルタが最初に適用され、次に Include フィルタが適用されます。一旦フィルタが自動ディスカバリ デバイスに適用されると、他のフィルタ条件はそのデバイスには適用されません。デバイスに複数の IP アドレスがあり、その中の 1 つでも Include フィルタの条件を満たしている場合、そのデバイスは自動ディスカバリ プロセスの対象として処理されます。
DNS Domain	(オプション) 次の対象とするデバイスのカンマ区切りの DNS ドメイン名を入力します。 • Include：自動ディスカバリ プロセスの対象にする • Exclude：自動ディスカバリ プロセスの対象から除外する ワイルドカードを使用して DNS 名を指定できます。アスタリスク（*）は、大文字と小文字の英数字、ハイフン（-）、および下線（_）が混在する任意の長さの組み合わせに一致します。疑問符（?）は、大文字または小文字の英数字、ハイフン、または下線の 1 文字に一致します。次の例を参考にしてください。 • *.*cisco.com* は、.*cisco.com* で終わるすべての DNS 名に一致します。 • *.*?abc.com* は、.*aabc.com* や .*babc.com* などで終わるすべての DNS 名に一致します。
SysLocation	(オプション) 次の対象とするデバイスについて、MIB-II 内の sysLocation OID に格納されているストリング値に一致するカンマ区切りのストリングを入力します。 • Include：自動ディスカバリ プロセスの対象にする • Exclude：自動ディスカバリ プロセスの対象から除外する ワイルドカードを使用してロケーション ストリングを指定できます。アスタリスク（*）は、大文字と小文字の英数字、ハイフン（-）、下線（_）、および空白（スペースとタブ）が混在する任意の長さの組み合わせに一致します。疑問符（?）のワイルドカードは、上記の任意の文字の 1 文字に一致します。たとえば、*San** の SysLocation フィルタは、*San Francisco* および *San Jose* などで始まるすべての SysLocation ストリングに一致します。

フィールド	処理 / 説明
Run	オプション ボタンを選択して、スケジュールを入力します。 • Now：すぐに実行する場合に選択します。 • Daily：実行する時刻を入力して、実行する曜日（Sun、Tue、Sat など）を選択します。 • Weekly：週単位での実行頻度（N 週ごと）、時刻、および曜日を入力します。

ステップ 4　**OK** をクリックします。物理ディスカバリの実行が開始されます。完了するまでにしばらく時間がかかります（Device Management: Summary ページのディスカバリ ステータスをチェックしてください）。

Operations Manager のデバイス選択（自動または手動）の設定

DCR から Operations Manager インベントリにデバイスを追加するには、次のいずれかで Operations Manager デバイス選択を設定する必要があります。

- Automatic：サポートされるデバイスが DCR に追加されると、自動的にインベントリにも追加されます（自動選択では、Operations Manager から除外するデバイスのリストも維持されます）。
- Manual：選択したデバイスだけを追加します。

（注）　初めて同期プロセスを実行する場合、Operations Manager に追加されるデバイス数によっては、Operations Manager がすべてのデバイスのインベントリを収集するまでに数時間かかる場合があります。

（注）　事前にデバイスが DCR に存在していないと、デバイスを Operations Manager に追加することはできません。

ステップ 1　**Devices > Device Management** を選択します。Device Management: Summary ページが表示されます。

ステップ 2　Device Selection フィールドの横にある **Configure** ボタンをクリックします。Device Selection ページが表示されます。

ステップ 3　Automatic オプション ボタンをアクティブにします。

ステップ 4　**Apply** をクリックします。Operations Manager が DCR と同期されます。Operations Manager に現在含まれていない DCR デバイスが追加されます。Operations Manager は、追加される新しいデバイスのインベントリ収集を実行します。

DCR から Operations Manager への手動によるデバイスの追加

Operations Manager を自動デバイス選択に設定した場合は、この手順を実行する必要はありません。手動デバイス選択では、監視するデバイスを手動で選択する必要があります。デバイスが DCR に追加された後に、定期的にこの作業を実行する必要があります。たとえば、週単位で Operations Manager の物理ディスカバリを実行する場合は、ディスカバリが終了するたびに監視する新しいデバイスを確認するかどうかを検討する必要があります。

（注）　事前にデバイスが DCR に存在していないと、デバイスを Operations Manager に追加することはできません。

ステップ 1　**Devices > Device Management** を選択します。

ステップ 2　Device Selection フィールドの横にある **Configure** ボタンをクリックします。Device Selection ページが表示されます。

ステップ 3　Manual オプション ボタンを選択します。Operations Manager インベントリに存在しないすべてのデバイスをデバイス セレクタから選択できます。

ステップ 4　次のいずれかの方法でデバイスを選択します。

- Device Display Name にデバイス名または IP アドレスを入力して、**Filter** をクリックする
- グループ セレクタを使用する

ステップ 5　選択したデバイスを表示するには、Selection タブをクリックします。デバイスのリストが表示されます。

ステップ 6　**Select** をクリックします。Operations Manager は、追加対象のデバイスのインベントリ収集を実行します。

詳細については、『*User Guide for IP Communications Operations Manager*』を参照してください。

Operations Manager に追加されたデバイスの確認

デバイスが Operations Manager インベントリに追加されていることを確認する方法の 1 つは、Service Level View を参照することです。また、Service Level View では、多数の Operations Manager ツールへクイック アクセスすることもできます。

インベントリ収集中に問題が発生した場合は、P.3-9 の「デバイス ディスカバリのトラブルシューティング」を参照してください。

Service Level View の起動

ステップ 1　**Monitoring Dashboard > Service Level View** を選択します。IP テレフォニー実装の論理トポロジ ビューを示す Service Level View 画面が表示されます。

詳細については、『*User Guide for IP Communications Operations Manager*』または Operations Manager のオンライン ヘルプを参照してください。

インベントリ収集のスケジュール

デバイスおよび電話器には、それぞれ個別のインベントリ収集スケジュールがあります。デバイスのインベントリ収集スケジュールは 1 つだけです。追加のスケジュールは作成できず、既存のスケジュールを編集することしかできません。IP Phone の場合は、複数のインベントリ収集スケジュールを作成できます。

Inventory Collection Schedule ページ（**Devices > Device Management > Device**）では、デバイス インベントリ収集スケジュールを編集、一時停止、または再開することができます（P.3-8 の「デバイス インベントリ収集スケジュールの編集」を参照してください）。

IP Phone Discovery Schedule ページ（Devices > Device Management > IP Phone Details）では、IP Phone ディスカバリ スケジュールを追加、編集、または削除することができます（P.3-8 の「電話器のディスカバリ スケジュールの追加」を参照してください）。

デバイス インベントリ収集スケジュールの編集

ステップ 1　**Devices > Device Management > Device** を選択します。Device Inventory Collection ページが表示されます。

ステップ 2　**Edit** をクリックします。Inventory Collection Schedule: Edit ページが表示されます。

ステップ 3　必要なスケジュール情報を変更します。

ステップ 4　**OK** をクリックします。

ステップ 5　**Yes** をクリックします。

電話器のディスカバリ スケジュールの追加

ステップ 1　**Devices > Device Management > IP Phone Details** を選択します。IP Phone Discovery Schedule ページが表示されます。

ステップ 2　**Add** をクリックします。Add Schedule ダイアログボックスが表示されます。

ステップ 3　次の情報を入力します。

- ディスカバリ スケジュールの名前
- ディスカバリを実行する曜日
- ディスカバリを実行する時間帯

ステップ 4　**OK** をクリックします。

デバイス ディスカバリのトラブルシューティング

物理ディスカバリの実行中（Operations Manager がデバイスを DCR に追加する間）に問題が発生したり、インベントリ収集の実行中（Operations Manager が監視用にデバイスをインベントリに追加する間）に問題が発生したりすることがあります。

デバイスのインベントリ収集をトラブルシューティングするには、次のことを試してみます。

- デバイスが応答していない場合は、すべてのデバイス クレデンシャルを確認し、デバイスを再度追加します。P.3-9 の「デバイス クレデンシャルの変更」を参照してください。
- デバイスのインベントリ収集が複数のデバイスでタイムアウトする場合は、SNMP タイムアウトの設定値を大きい値にします。P.3-9 の「SNMP タイムアウトと再試行の変更」を参照してください。
- View/Refresh/Delete Device ページのデバイス エラー情報を表示します。P.3-10 の「デバイスのインベントリ収集の実行」を参照してください。
- デバイスがインポート中に動作可能な状態で、MIB II をサポートしていることを確認します。
- 到達不能状態になっているデバイスの原因をチェックします。P.3-10 の「インベントリ収集メッセージについて」を参照してください。
- 問題をトラブルシューティングしたら、デバイスのステータスを確認します。P.3-7 の「Operations Manager に追加されたデバイスの確認」を参照してください。

デバイス クレデンシャルの変更

Common Services の DCR を使用して、デバイス クレデンシャルを変更します。Common Services のオンライン ヘルプを参照してください。

SNMP タイムアウトと再試行の変更

SNMP クエリーが時間内に応答しない場合、Operations Manager がタイムアウトします。Operations Manager は、ユーザが指定した回数だけデバイスへのアクセスを再試行します。タイムアウト期間は、後続の再試行ごとに 2 倍になります。

たとえば、タイムアウト値が 4 秒で、再試行値が 3 回の場合、Operations Manager は、4 秒間待ってから 1 回目の再試行を実行し、次に 8 秒間待ってから 2 回目の再試行を実行し、さらに 16 秒間待ってから 3 回目の再試行を実行します。

SNMP のタイムアウトと再試行値は、グローバル設定です。次のように値を変更します。

ステップ 1　**Devices > Device Management > SNMP Configuration** を選択します。SNMP Configuration ページが表示されます。

ステップ 2　新しい SNMP タイムアウトの設定値を選択します。デフォルトは 4 秒です。

ステップ 3　新しい Number of Retries の設定値を選択します。デフォルトの試行回数は 3 回です。

ステップ 4　**Apply** をクリックします。確認のために **Yes** をクリックします。

デバイスのインベントリ収集の実行

View/Refresh/Delete Devices ページから、デバイスまたはデバイス グループのインベントリ収集を起動できます。インベントリ収集の実行時に、デバイスまたはグループの設定が変更されていた場合は、新しい設定値によって以前の設定値が上書きされます。

インベントリ収集は、アクティブなデバイスに対してのみ実行されます。Operations Manager は、一時停止中のデバイスのインベントリは収集しません。インベントリ収集の対象として選択しているデバイスの中に一時停止中のデバイスがある場合、Operations Manager は、アクティブなデバイスだけをディスカバリの対象とすることを通知するメッセージを表示します。

（注）　Operations Manager インベントリ収集プロセスと DCR 同期プロセスとを混合しないでください。Operations Manager インベントリ収集は、Operations Manager インベントリだけに影響するプロセスです。

ステップ 1　**Devices > Device Management > View/Refresh/Delete** を選択します。View/Refresh/Delete Devices ページが表示されます。

ステップ 2　インベントリ収集を実行するデバイスまたはグループを選択します。

ステップ 3　**Update** をクリックします。インベントリ収集が起動します。

インベントリ収集メッセージについて

表 3-2 に、到達不能状態のデバイスについて表示されることのあるメッセージを示します。

表 3-2　インベントリ収集エラー メッセージ

メッセージ	意味	処理
SNMP Timeout	デバイスの SNMP 読み取り専用コミュニティ ストリングが不正なため、デバイスは到達不能状態です。	デバイスの正しいリード（read）コミュニティ ストリングを入力するには、P.3-9 の「デバイス クレデンシャルの変更」を参照してください。
Others: Missing IP Address or Data Collector Timeout	その他の理由で、デバイスは到達不能状態です。デバイスの DNS 解決が失敗したか、データ コレクタがタイムアウトした可能性があります。	Rediscover/Delete Devices ページでデバイスをクリックします。エラー メッセージに、問題が正確に表示されます。 • IP アドレスが検出されない場合 – 正しい IP アドレスでデバイスを再度追加します。 または – Operations Manager がデバイス名を解決可能であることを確認します。ドメイン名をデバイス名の一部として追加します。 • データ コレクタがタイムアウトした場合は、デーモン マネージャを再起動して、同時にすべてのデータ コレクタを取得します。

Operations Manager の起動

Operations Manager を起動するには、Windows デスクトップで **Start > Programs > IPC Operations Manager 1.0 and Service Monitor 1.0 > IPC Operations Manager 1.0 and Service Monitor 1.0** を選択します。

（注）　Windows 2003 システムで拡張セキュリティがイネーブルになっている場合は、Operations Manager のホームページを Internet Explorer の信頼済みサイト ゾーンに追加する必要があります。IP Communications Operations Manager ホームページを信頼済みサイトに追加しない限り、ここにアクセスすることはできません。

Internet Explorer 信頼済みサイト ゾーンへの Operations Manager ホームページの追加

Windows 2003 システムで拡張セキュリティがイネーブルになっている場合は、Operations Manager ホームページにアクセスする前に、次の手順を実行する必要があります。

ステップ 1　Operations Manager を開き、**Start > Programs > IPC Operations Manager 1.0 and Service Monitor 1.0 > IPC Operations Manager 1.0 and Service Monitor 1.0** を選択します。

ステップ 2　File メニューで、**Add this site to** を選択します。

ステップ 3　**Trusted Sites Zone** をクリックします。

ステップ 4　**Trusted Sites** ダイアログボックスで、**Add** をクリックして、サイトをリストに移動します。

ステップ 5　**Close** をクリックします。

ステップ 6　ページをリフレッシュして、新しいゾーンからサイトを表示します。

ステップ 7　ブラウザのステータス バーをチェックして、サイトが信頼済みサイト ゾーンにあることを確認します。

セキュリティの概要と設定について

Operations Manager は、次のセキュリティ関連のメカニズムをサポートしています。

- SNMPv3 プロトコル（認証 / 非プライバシー オプション）：Operations Manager は、サーバとデバイス間で認証 / 非プライバシー オプションをサポートしています。
- CiscoWorks サーバ上のセキュリティ：Operations Manager が常駐するサーバに次のセキュリティを設定できます。
  - **Secure Socket Layer（SSL）**：Operations Manager は、サーバとブラウザ間で SSL プロトコルを使用できます。サーバの SSL をイネーブルおよびディセーブルにできます。SSL をイネーブルにする場合は、自己署名セキュリティ証明書を設定して、SSL 通信をイネーブルにする必要があります。詳細については、『*User Guide for IP Communications Operations Manager*』を参照してください。
  - **ローカル セキュリティまたは Cisco Secure ACS**：Operations Manager 内のタスクへのアクセスは、ローカル セキュリティによって制御されるか、Common Services または Cisco Security ACS によって提供されます。デフォルトでは、ローカル セキュリティがサーバ上でイネーブルになっています。Operations Manager は、Cisco Secure ACS との統合をサポートしています。詳細については、P.B-1 の「Cisco Secure ACS による Operations Manager の設定」を参照してください。

（注）　詳細については、『*User Guide for IP Communications Operations Manager*』を参照してください。

サポートされる NMS 統合

Operations Manager は、次のように NMS との統合をサポートしています。

- Operations Manager は、ポート 162（デフォルト）で管理対象デバイスからのトラップを受信します。Operations Manager を搭載したシステムの別の NMS がポート 162 を使用している場合は、次の手順に従います。
  - インストール スクリプトが、このことを警告します。
  - インストールが完了した後、Operations Manager トラップの受信用に別のポートを指定する必要があります。P.3-14 の「NMS またはトラップ デーモンへの Operations Manager トラップ受信の統合」を参照してください。
- Operations Manager は、次のように、ユーザが指定した宛先にトラップを転送します。
  - パススルー トラップを転送するには、P.3-13 の「SNMP トラップの受信および転送の設定」を参照してください。
  - 処理済みのトラップを転送するには、『*User Guide for IP Communications Operations Manager*』の「Using Notification Services」の章の「Managing SNMP Trap Notifications」を参照してください。

  パススルー トラップと処理済みのトラップの詳細については、『*User Guide for IP Communications Operations Manager*』の付録「Processed and Pass-through Traps, and Other Unidentified Traps and Events」を参照してください。

標準 User Datagram Protocol（UDP; ユーザ データグラム プロトコル）のトラップ ポート（162）が別の NMS で使用されている場合は、Operations Manager の SNMP トラップ受信で別の UDP ポート（ポート 9000 など）を使用するように設定する必要があります。P.3-13 の「SNMP トラップの受信および転送の設定」を参照してください。

SNMP トラップの受信および転送の設定

Operations Manager は、使用可能なポートでトラップを受信し、それらをデバイスとポートのリストに転送できます。この機能によって、Operations Manager はその他のトラップ処理アプリケーションと簡単に連携して動作できます。ただし、デバイスの SNMP をイネーブルにして、Operations Manager または次のいずれかに直接トラップを送信するように SNMP を設定する必要があります。

- 1 つの NMS
- 1 つのトラップ デーモン

トラップを直接 Operations Manager に送信するには、P.3-13 の「デバイスの Operations Manager へのトラップ送信のイネーブル化」の作業を実行します。SNMP トラップ受信を NMS またはトラップ デーモンに統合するには、P.3-14 の「NMS またはトラップ デーモンへの Operations Manager トラップ受信の統合」の手順に従います。

SNMP トラップの受信ポートのアップデート

デフォルトでは、Operations Manager はポート 162 で SNMP トラップを受信します。必要に応じて、ポートは変更することができます（たとえば、ポート 9000）。

ステップ 1　**Administration > Preferences** を選択します。System Preferences ページが表示されます。

ステップ 2　Trap Receiving Port フィールドに、ポート番号を入力します。

ステップ 3　**Apply** をクリックします。

Operations Manager が使用するポートのリストについては、P.2-2 の「Operations Manager が使用する TCP ポートと UDP ポートの確認」を参照してください。

デバイスの Operations Manager へのトラップ送信のイネーブル化

Operations Manager は SNMP MIB の変数とトラップを使用してデバイスのヘルスを判別するため、この情報を提供するようにデバイスを設定する必要があります。Operations Manager が監視するシスコ デバイスでは、SNMP をイネーブルにし、SNMP トラップを Operations Manager サーバに送信するように設定する必要があります。

デバイスに適したコマンドラインまたは GUI インターフェイスを使用して、デバイスが Operations Manager にトラップを送信可能であることを確認します。

- P.3-13 の「Cisco IOS ベースのデバイスの Operations Manager へのトラップ送信のイネーブル化」
- P.3-14 の「Catalyst デバイスの Operations Manager への SNMP トラップ送信のイネーブル化」

Cisco IOS ベースのデバイスの Operations Manager へのトラップ送信のイネーブル化

Cisco IOS ソフトウェアを実行しているデバイスの場合は、次のコマンドを入力します。

```
(config)# snmp-server [community string] ro
(config)# snmp-server enable traps
(config)# snmp-server host [a.b.c.d] traps [community string]
```

ここで、[*community string*] は SNMP 読み取り専用コミュニティ ストリング、[*a.b.c.d*] は SNMP トラップの受信ホスト（Operations Manager サーバ）です。

詳細については、該当するコマンド リファレンス ガイドを参照してください。

ステップ 1　Cisco.com にログインします。

ステップ 2　**Products & Solutions > Cisco IOS Software** を選択します。

ステップ 3　Cisco IOS ベースのデバイスが使用する Cisco IOS ソフトウェア リリース バージョンを選択します。

ステップ 4　**Technical Documentation** を選択して、該当するコマンド リファレンス ガイドを選択します。

Catalyst デバイスの Operations Manager への SNMP トラップ送信のイネーブル化

Catalyst ソフトウェアを実行しているデバイスの場合は、次のコマンドを入力します。

```
(enable)# set snmp community read-only [community string]
(enable)# set snmp trap enable all
(enable)# set snmp trap [a.b.c.d] [community string]
```

ここで、[*community string*] は SNMP 読み取り専用コミュニティ ストリング、[*a.b.c.d*] は SNMP トラップの受信ホスト（Operations Manager サーバ）です。

詳細については、該当するコマンド リファレンス ガイドを参照してください。

ステップ 1　Cisco.com にログインします。

ステップ 2　**Products & Solutions > Switches** を選択します。

ステップ 3　該当する Cisco Catalyst シリーズ スイッチを選択します。

ステップ 4　**Technical Documentation** を選択して、該当するコマンド リファレンス ガイドを選択します。

NMS またはトラップ デーモンへの Operations Manager トラップ受信の統合

SNMP トラップ受信をその他のトラップ デーモンや NMS に統合するには、次の手順に従う必要があります。

- Operations Manager が実行されているホストを、ネットワーク デバイス内のトラップ宛先リストに追加します。P.3-13 の「デバイスの Operations Manager へのトラップ送信のイネーブル化」を参照してください。ポート 162 を宛先トラップ ポートとして指定します。

  別の NMS がすでに標準 UDP トラップ ポート（162）でトラップを受信している場合は、Operations Manager がポート 9000 などの別のポートを使用するように設定する必要があります。P.3-13 の「SNMP トラップの受信ポートのアップデート」を参照してください。
- ネットワーク デバイスがすでにトラップを別の管理アプリケーションに送信している場合は、Operations Manager にトラップを転送するようにそのアプリケーションを設定します。

表 3-3 に、SNMP トラップ受信のシナリオの説明とそれぞれの利点を示します。

表 3-3　トラップ受信の設定シナリオ

シナリオ	利点
ネットワーク デバイスは、Operations Manager が実行されているホストのポート 162 にトラップを送信します。Operations Manager は、トラップを受信して、NMS に転送します。	• NMS の再設定は不要です。 • ネットワーク デバイスの再設定は不要です。 • Operations Manager は、信頼できるトラップの受信、保存、および転送メカニズムを提供します。 • NMS は継続して、ポート 162 でトラップを受信します。 • ネットワーク デバイスは継続して、トラップをポート 162 に送信します。
NMS は、デフォルトのポート 162 でトラップを受信して、Operations Manager が実行されているホストのポート 162 に転送します。	• NMS の再設定は不要です。 • ネットワーク デバイスの再設定は不要です。 • Operations Manager は、NMS によって廃棄されたトラップは受信しません。

SNMP トラップ転送の設定

デフォルトでは、Operations Manager は未処理の SNMP トラップを転送しません。ただし、転送するように設定することはできます。

ステップ 1　**Administration > Preferences** を選択します。System Preferences ページが表示されます。

ステップ 2　Trap Forwarding Parameters に、次の情報を入力します。

- サーバの IP アドレスまたは DNS 名
- トラップの受信が可能なサーバのポート番号

ステップ 3　**Apply** ボタンをクリックします。

アラートの表示

Monitoring Dashboard 画面を使用して、アラートを表示できます。**Monitoring Dashboard** を選択して、次のいずれかの画面を選択します。

- Service Level View
- Alerts and Events
- Service Quality Alerts
- IP Phone Status

次の作業

この章の作業を完了すると、Operations Manager はイベントの監視と分析、およびアラートの通知を実行できるようになります。

表 3-4 に、Operations Manager の追加のセットアップ方法を要約します。

表 3-4　Operations Manager のセットアップ

作業	説明
Monitoring Dashboard 画面のビューの設定	ビューは、Monitoring Dashboard 画面に表示されるデバイスの論理グループです（Service Level View、Alerts and Events、Phone Activities、および Service Quality Alerts）。Group Administration and Configuration ページに新しいユーザ定義のグループを作成すると、必ず対応するビューも作成されます。
通知の設定	Monitoring Dashboard 画面を監視してアラートを確認します。また、アラートに応じて、ユーザが電子メールを受信したり、ホストが Operations Manager によって生成された SNMP トラップを受信したりするように登録できます。
ポーリング パラメータとしきい値の設定	Operations Manager には、ポーリング パラメータとしきい値のデフォルト値があります。ただし、ネットワークの必要に応じて、値をアップデートできます。Operations Manager サーバのアクティビティが低い場合は、変更の適用を計画する必要があります。 デフォルトでは、Operations Manager は音声使用率のポーリング設定値を設定します。Operations Manager のパフォーマンス モニタリング機能を使用する場合は、最初に音声使用率のポーリングをイネーブルにする必要があります。
消去の設定	デフォルトでは、Operations Manager は毎日午前 0 時にデータベースを消去します。このスケジュールは変更できます。
インベントリ収集の設定	Operations Manager では、インベントリ収集のデフォルト スケジュールを 1 つ用意しています。そのスケジュールを使用することもできれば、一時停止することもできます。

Operations Manager の機能を十分に活用するために、追加の設定作業を実行する必要が生じる場合があります。Operations Manager の使用と設定については、オンライン ヘルプまたは『*User Guide for IP Communications Operations Manager*』を参照してください。