CHAPTER 2

スタートアップ

以下のトピックでは、Cisco Unified Operations Manager（Operations Manager）の使用を開始するための方法について、作業ごとに説明します。

ワンポイントアドバイス

Operations Manager についてのオンラインのビデオ チュートリアルを見るには、オンライン ヘルプの [E-Learning] アイコンをクリックします。

Operations Managerの設定作業の実行

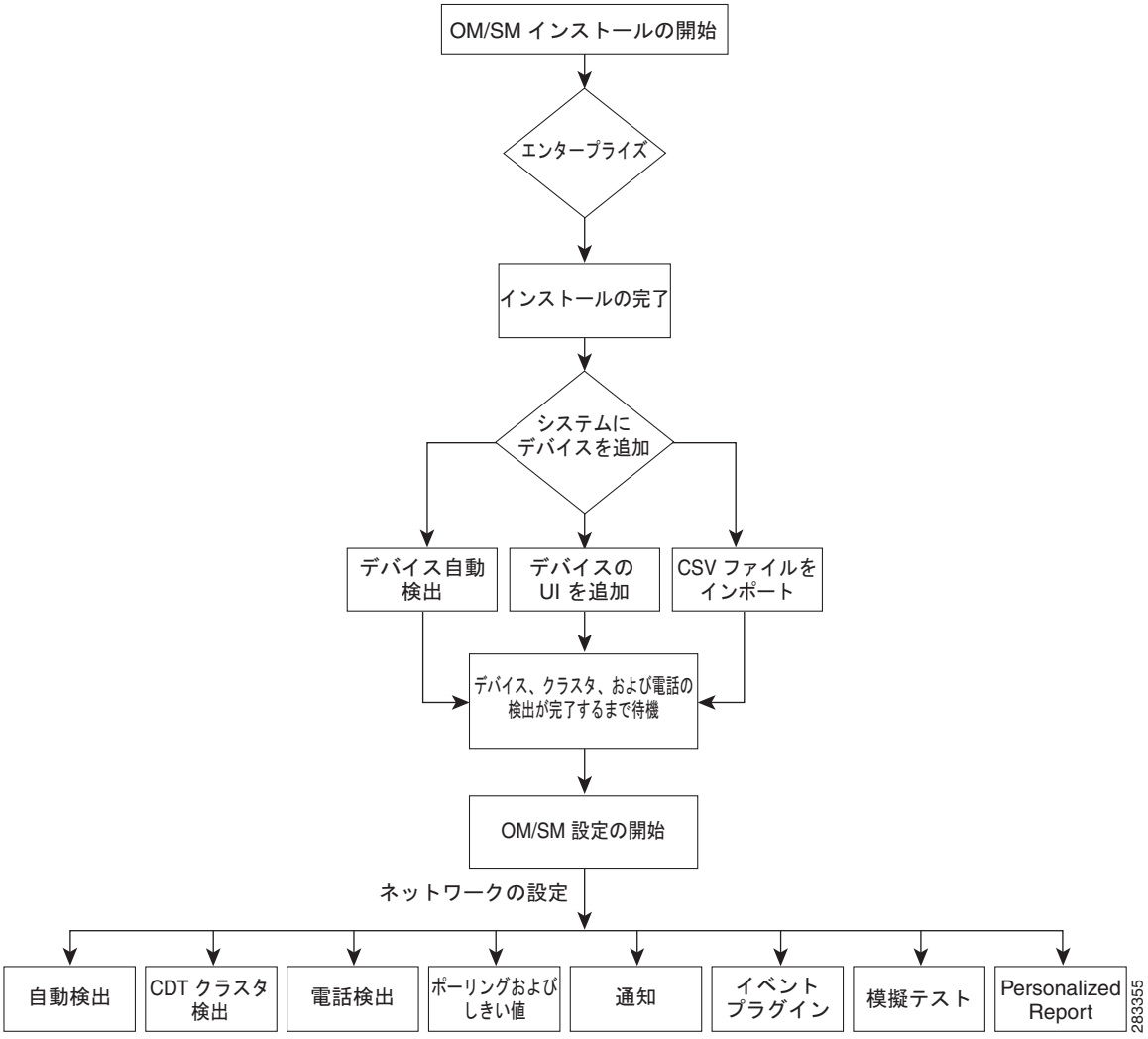
Operations Manager でネットワーク上のユニファイド コミュニケーション デバイスを監視するためには、必要な設定作業が多数あります。導入形態に応じて次のフローチャートを使用し、Operations Manager を使用してユニファイド コミュニケーション ネットワークを監視するために必要な作業を確認してください。設定が終了すれば、データの収集、レポートの実行、ネットワークに影響を及ぼすおそれのある重大なデバイス イベントの監視を行えるようになります。

導入形態に応じた設定作業フローチャートを使用してください。

エンタープライズ バージョンの導入の場合の設定作業

ここでは、Operations Manager のエンタープライズ バージョンを使用してユニファイド コミュニケーション ネットワークの監視をはじめる前に、実行する必要のある作業について説明します。

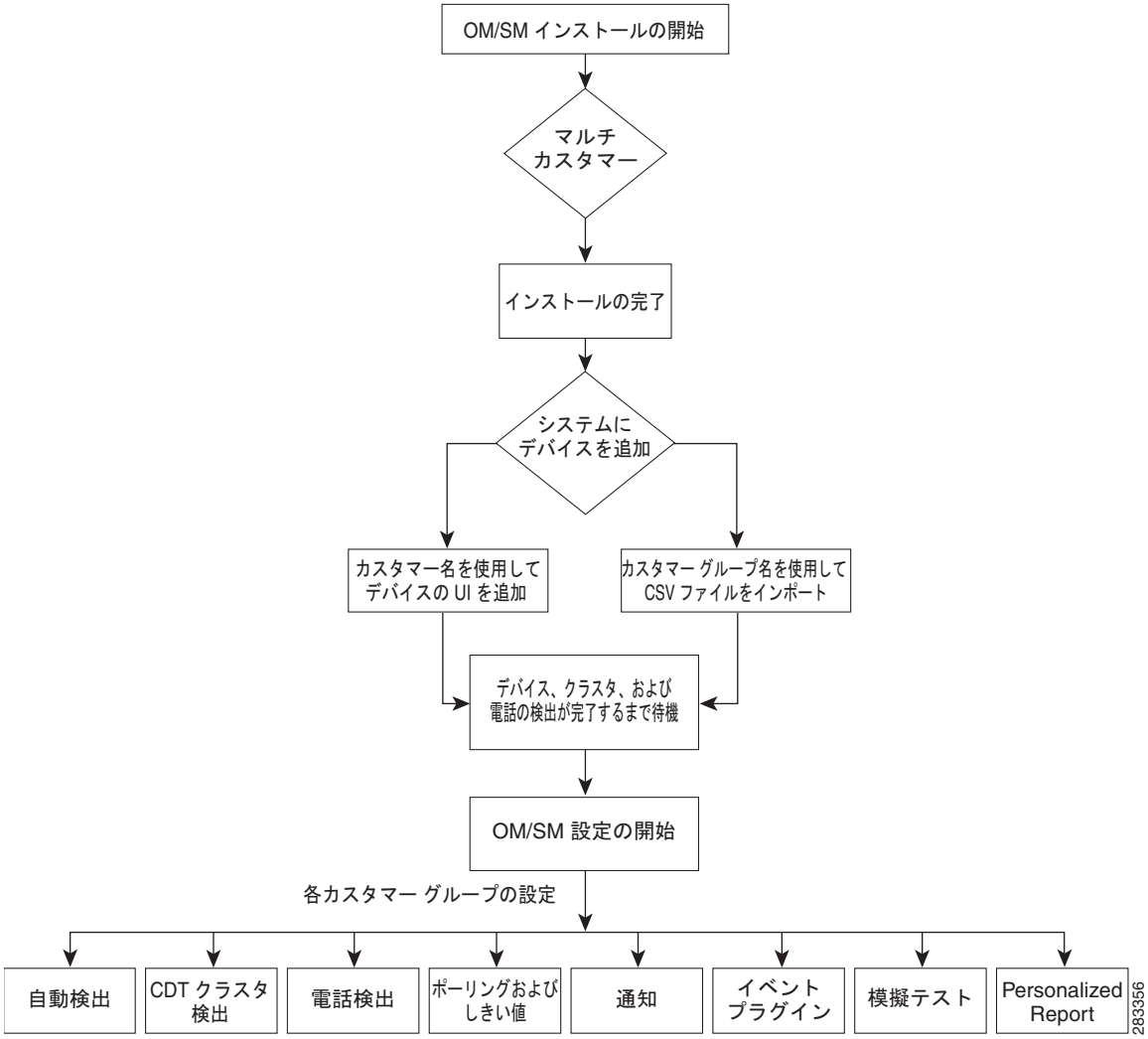
図 2-1　エンタープライズ バージョンの導入のための設定作業



マルチ エンドカスタマー バージョン向けの設定作業

ここでは、Operations Manager のマルチ エンドカスタマー バージョンを使用してユニファイド コミュニケーション ネットワークの監視をはじめる前に、実行する必要のある作業について説明します。

図 2-2　　マルチ エンドカスタマー バージョンの導入の場合の設定作業



Operations Manager の設定

この項では、Operations Manager を正しく使用するために必要な作業について説明します。

- 「デバイスをモニタするための Operations Manager の設定」（P.2-4）
- 「Operations Manager からの [Cisco Unified Communications Management Server] リンクの追加」（P.2-21）
- 「セキュリティの概要と設定について」（P.2-22）

デバイスをモニタするための Operations Manager の設定

Operations Manager は、Common Services Device and Credentials Repository (DCR) から監視するデバイスを取得します。DCR は、デバイスおよびそのクレデンシャルの共通リポジトリで、個々のアプリケーションによって使用されます。

ここでは、次の内容について説明します。

- 「DCR のモード（マスターおよびスレーブ）の設定」
- 「DCR へのデバイスの追加」
- 「DCR へのデバイスのインポート」
- 「DCR から Operations Manager への手動によるデバイスの追加」
- 「デバイスの状態について」
- 「Operations Manager に追加したデバイスの確認」
- 「インベントリ収集のスケジュール」
- 「デバイス インポートおよびインベントリ収集のトラブルシューティング」
- 「デバイスの設定とクレデンシャルの編集」
- 「SNMP タイムアウトと再試行の変更」
- 「デバイスのインベントリ収集の手動実行」（P.2-17）

Operations Manager でデバイスをモニタするには、あらかじめデバイスを DCR に追加しておく必要があります。デバイスを DCR に追加した後は、DCR とは別の Operations Manager インベントリにデバイスを追加することができます。

（注）　Operations Manager エンタープライズ バージョンは、インストールすると自動的に DCR と同期し、インベントリを追加します。これはデフォルトの設定です。マルチ エンドカスタマー バージョンのインストールでは、デバイスは手作業で追加する必要があります。

エンタープライズ バージョンの場合は、自動同期を有効にすると、デバイスが DCR から Operations Manager に自動的に追加されます（デフォルト）。[Device Selection] ページから手作業で追加することもできます。

マルチ エンドカスタマー バージョンでは、[Device Add] ページまたは [Device Import] を使用して手作業で追加します。Operations Manager が DCR から受ける影響の詳細については、「Device and Credentials Repository（DCR）について」を参照してください。

NMSROOT ディレクトリは、ウイルス スキャンから除外する必要があります。ウイルス スキャンが原因でファイルがロックされていると、問題が発生することがあります。

NMSROOT は、Operations Manager がインストールされているシステム上のディレクトリです。インストール中にデフォルト ディレクトリを選択した場合は、C:¥PROGRA~1¥CSCOpx となります。

表 2-1 に、考えられるいくつかの Operations Manager 展開シナリオと、デバイスを Operations Manager インベントリに追加するために必要な作業を示します。

表 2-1　デバイスをインベントリに追加するシナリオ

展開シナリオ	対処法
• Operations Manager を独立したサーバとして配置する。 • インベントリを DCR と自動的に同期させる。	自動同期を使用してデバイスを DCR から追加します。自動同期はデフォルトの設定です。[1] 同期の設定を自動から変更した場合は、設定を元に戻す必要があります。「Operations Manager の自動デバイス選択の設定」（P.2-12）を参照してください。
• Operations Manager を独立したサーバとして配置する。 • インベントリに追加するデバイスを手動で制御する。	デバイスを DCR から手動で追加します。「DCR から Operations Manager への手動によるデバイスの追加」（P.2-13）を参照してください。
• Operations Manager を独立したサーバとして配置する。 • 自動検出を使用するが、自動検出で検出されたすべてのデバイスを Operations Manager で管理する必要があるわけではない。	• 自動同期を使用してデバイスを DCR から追加します。[1] • 設定したパラメータに基づいてデバイスが選択されるように自動同期を設定します。「Operations Manager の自動デバイス選択の設定」（P.2-12）を参照してください。
• Operations Manager を CiscoWorks LAN Management Solution（LMS）とともに配備する。 • Operations Manager DCR をマスター DCR として使用する。 • インベントリを DCR と自動的に同期させる。	• Operations Manager DCR をマスターとして設定し、LMS DCR をスレーブとして設定します。「DCR のモード（マスターおよびスレーブ）の設定」（P.2-6）。 • 物理ディスカバリを実行します。「DCR へのデバイスの追加」（P.2-7）を参照してください。 • Operations Manager に自動同期が設定されていることを確認します。「Operations Manager の自動デバイス選択の設定」（P.2-12）を参照してください。

表 2-1　デバイスをインベントリに追加するシナリオ（続き）

展開シナリオ	対処法
• Operations Manager を LMS とともに配備する。 • Operations Manager DCR を既存のマスター DCR と同期させる。 • インベントリを DCR と自動的に同期させる。	• Operations Manager サーバの DCR をスレーブとして設定し、いずれか 1 つの LMS DCR をマスターとして設定します。「DCR のモード（マスターおよびスレーブ）の設定」（P.2-6）。 • デバイスがマスター DCR に追加されるように Operations Manager を設定します。「DCR へのデバイスの追加」（P.2-7）を参照してください。 • 物理ディスカバリを実行します。「DCR へのデバイスの追加」（P.2-7）を参照してください。 • Operations Manager に自動同期が設定されていることを確認します。「Operations Manager の自動デバイス選択の設定」（P.2-12）を参照してください。
• Operations Manager を LMS とともに配備する。 • Operations Manager を既存のマスター DCR と同期させる。 • Operations Manager で管理するデバイスを手動で制御する。	• Operations Manager サーバの DCR をスレーブとして設定し、LMS サーバの DCR をマスターとして設定します。「DCR のモード（マスターおよびスレーブ）の設定」（P.2-6）。 • デバイスがマスター DCR に追加されるように Operations Manager を設定します。「DCR へのデバイスの追加」（P.2-7）を参照してください。 • 物理ディスカバリを実行します。「DCR へのデバイスの追加」（P.2-7）を参照してください。 • Operations Manager に手動同期が設定されていることを確認します。「Operations Manager の自動デバイス選択の設定」（P.2-12）を参照してください。

1. ネットワーク デバイスにデバイス クレデンシャルを設定済みであることを確認してください。

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。DCR を Operations Manager に対してマスターまたはスレーブとして設定する場合、その手順は CiscoWorks のオンライン ヘルプに記載されています。

CiscoWorks のオンライン ヘルプにアクセスするには、Operations Manager のホームページで [Administration] を選択し、見出し（[CiscoWorks/Common Services]）の下にある任意のリンクを選択します。新しいウィンドウが開いたら、[Help] リンクをクリックします。

Operations Manager および CiscoWorks が互換性のあるバージョンであることを確認してから、マスター モードとスレーブ モードを設定します。互換性の詳細については、『*Supported and Interoperable Devices and Software Table for Cisco Unified Operations Manager 8.0*』を参照してください。

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探し出すのに役立ちます。

（注）　Operations Manager を起動するには、「Operations Manager の起動」（P.1-22）を参照してください。

DCR をマスター モードおよびスレーブ モードに設定する手順は次のとおりです。

ステップ 1　[Administration] > [Device and Credentials (Common Services)] > [Administration] を選択します。

[Common Services] ウィンドウが開きます。

ステップ 2　左ペインにある [Mode Settings] リンクをクリックします。

[Mode Settings] ウィンドウが表示されます。

ステップ 3　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。次の作業を行います。

- 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 ID ユーザの作成
- セキュリティ証明書のコピー

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

DCR へのデバイスの追加

デバイスを DCR に追加するには、[Operations Manager Add Devices] ページ（[Administration] > [Device Management] > [Device Configuration] > [Add Devices]）を使用します。

ここでは、次の内容について説明します。

- 「Operations Manager の物理ディスカバリの設定」
- 「クレデンシャルの設定」
- 「Operations Manager の物理ディスカバリのフィルタリング」

（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 DCR にデバイスを追加するには、「DCR へのデバイスのインポート」（P.2-12）を参照してください。

ステップ 1　[Administration] > [Device Management] > [Device Configuration] > [Add Devices] を選択します。

[Add Devices] ページが表示されます。

ステップ 2　次を入力します。

- IP アドレスまたはホスト名。カンマ区切りのリストを使用して、複数のデバイスを同時に入力できます。デバイスのホスト名は DNS で解決できる名前を指定してください。複数のデバイスを一緒に追加するときは、すべてのデバイスが同じタイプであり、同じクレデンシャルを使用している必要があります。
- SNMPv2c/SNMPv1 クレデンシャルを入力します。
- SNMPv3 クレデンシャルを入力します。
- HTTP クレデンシャルを入力します（Cisco Unified Communications Manager にのみ必須）。
- Windows クレデンシャルを入力します（Windows ベースの MCS アプリケーション サーバにのみ必須）。

ステップ 3　[OK] をクリックします。

Operations Manager の物理ディスカバリの設定

Operations Manager の物理検出を設定する手順は次のとおりです。

ステップ 1　[Devices] > [Device Management] > [Auto-Discovery Configuration] を選択します。

[Auto-Discovery Configuration] ページが表示されます。

[Discovery Configuration] ページは、[Device Management: Summary] ページで [Configure] ボタンをクリックして表示することもできます。

検出には、SNMP または SNMPv3（またはその両方）のクレデンシャルが必要です。

このクレデンシャルが設定されていないと、[Discovery Configuration] をクリックしたときに空の [Discovery Configuration] ページが表示され、クレデンシャルを設定するオプションが示されます。

a.　[Credentials] オプション ボタンを選択します。

b.　[Add] をクリックします。

[Configure Credentials] ページが表示されます（「クレデンシャルの設定」（P.2-9）を参照）。

[Discovery] オプション ボタンが選択されていない場合は、それを選択します。

ステップ 2　次のどちらかを実行します。

- [Use Communications Manager or Cisco Discovery Protocol (CDP)] チェックボックスをオンにし、次のいずれかを実行します。
  - カンマ区切りの IP アドレスのリストを使用して、シード デバイスを入力します。

    Cisco Unified Communications Manager をシード デバイスとして使用している場合は、次のタイプのデバイスが検出されます。

    - ネットワーク内の他の Cisco Unified Communications Managers
    - Cisco Unity
    - MGCP 音声ゲートウェイ
    - H.323 音声ゲートウェイ
    - ゲートキーパー

    Cisco Unified Communications Manager ベースの検出に加えて次のタイプの検出が行われます。この結果として、次のデバイスがインベントリに追加されます。

    - CDP ベースの検出
    - ARP ベースの検出
    - ルート テーブル ベースの検出
  - [Use devices currently in the system] チェックボックスを選択します。
  - ホップ カウントを選択します。

  ディスカバリは、選択したホップ カウントより多くのホップをスキップする場合があります。ディスカバリは複数の技術を使用してデバイスを検出します。その結果、デバイスが L2 ホップまたは L3 ホップに違反する場合があります。

  ディスカバリを制限するためにホップ カウントを使用する場合は、別の方法でその目的を実現できます。それは、[Discovery Configuration] ページの Include フィルタおよび Exclude フィルタを使用する方法です（「Operations Manager の物理ディスカバリのフィルタリング」（P.2-10）を参照してください）。

または

- [Use ping sweep] チェックボックスを選択します。シード デバイス オプションと ping スイープ オプションは、どちらか一方しか使用できません。

  [Use Ping Sweep] チェックボックスをオンにするときは、*/netmask* 指定を使用して、IP アドレス範囲をカンマで区切って指定します。

  たとえば、172.20.57.1 から始まり、172.20.57.255 で終わる ping スイープ範囲を指定する場合は、172.20.57.1/24 を使用します。

ステップ 3　[Run] ペインで、いつ物理ディスカバリを実行するかを設定します。

- 物理検出をただちに実行する場合は、[now] オプション ボタンを選択します。
- 物理検出を一定の間隔で実行するようにスケジュールする場合、次のいずれかの手順を実行します。
  - [daily] オプション ボタンを選択します。物理検出を実行する時刻を入力し、日付を選択します。
  - [every] オプション ボタンを選択します。物理検出を実行する頻度を選択し、実行する間隔を入力し、実行する曜日を選択します。

ステップ 4　[OK] をクリックします。

クレデンシャルの設定

検出には、SNMP または SNMPv3（またはその両方）のクレデンシャルが必要です。クレデンシャルが設定されていない場合は、検出を設定しようとしても [Configure Credentials] ページにしかアクセスできません。検出を実行する前に、SNMP または SNMPv3（またはその両方）のクレデンシャルを入力する必要があります。

ステップ 1　[Devices] > [Device Management] > [Auto-Discovery Configuration] > [Credentials] を選択します。

[Configure Credentials] ページが表示されます。

ステップ 2　[Add] をクリックします。

デバイスの既存のクレデンシャルを変更する場合は、宛先デバイスを選択して [Edit] をクリックします。この [Edit] オプションを使用すると、クレデンシャルのみを変更できます。宛先デバイスを変更するには、行全体を削除して、詳細をすべて追加し直す必要があります。

ステップ 3　次を入力します。

- IP アドレスまたはホスト名。カンマ区切りのリストを使用して、複数のデバイスを同時に入力できます。

  複数のデバイスを同時に追加する場合は、すべてのデバイスが同じタイプのデバイスで、同じクレデンシャルを使用している必要があります。ワイルドカード エントリを使用する場合は、*.*.*.* または 10.76.93.[39-43] という形式のみがサポートされています。
- （オプション）SNMP のタイムアウトと再試行を変更します。
- SNMPv2c/SNMPv1 クレデンシャル
- SNMPv3 クレデンシャル
- HTTP クレデンシャル（Cisco Unified Communications Manager に必須）
- Windows クレデンシャル（Windows ベースの MCS アプリケーション サーバに必須）

ステップ 4　[OK] をクリックします。

Operations Manager の物理ディスカバリのフィルタリング

デバイスをフィルタリングするように Operations Manager 物理検出を設定できます。これはオプションであり、物理検出を実行するのに必須ではありません。

ステップ 1　[Devices] > [Device Management] > [Auto-Discovery Configuration] > [Filters and Schedule] を選択します。

[Filters and Schedule] ページが表示されます。

ステップ 2　[Filters] オプション ボタンを選択します。表 2-2 では、物理検出を実行するときに使用できるオプションのフィルタについて説明します。

表 2-2　物理検出のフィルタ

フィルタ	説明
IP Address	（オプション）次の操作の対象となるデバイスの IP アドレスまたは IP アドレス範囲を、カンマで区切って入力します。 • Include：自動検出プロセスに含めます。 • Exclude：自動検出プロセスから除外します。 IP アドレスの範囲を指定する場合は、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表します。また、[xxx-yyy] の表記によっ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 のサブネット内にあるすべてのデバイスを自動検出プロセスに含めるには、172.20.57.* という Include フィルタを入力します。 • 172.20.57.224 ～ 172.20.57.255 の IP アドレス範囲内にあるデバイスを自動検出プロセスから除外する場合は、172.20.57.[224-255] という Exclude フィルタを入力します。 172.20.[55-57]* のように、同じ範囲指定の中で両方のタイプのワイルドカードを使用することもできます。Include フィルタと Exclude フィルタの両方が指定されている場合は、先に Exclude フィルタが適用されてから Include フィルタが適用されます。 自動検出のデバイスに一度フィルタが適用されると、そのデバイスには他のフィルタ基準は適用されません。デバイスに複数の IP アドレスがある場合は、Include フィルタの条件を満たす IP アドレスが 1 つでもあれば、そのデバイスは自動検出で処理されます。
Domain	（オプション）次の操作の対象となるデバイスのドメイン名を、カンマで区切って入力します。 • Include：自動検出プロセスに含めます。 • Exclude：自動検出プロセスから除外します。 ドメイン名は、ワイルドカードを使用して指定できます。アスタリスク（*）は、大文字と小文字が混ざった英数字、ハイフン（-）、およびアンダースコア（_）の任意の長さの任意の組み合わせに一致します。 疑問符（?）は、1 つの大文字または小文字の英数字、ハイフン、またはアンダースコアに一致します。次の例を参考にしてください。 • *.*cisco.com* は、*.cisco.com* で終わる任意の名前に一致します。 • *.*?abc.com* は、*.aabc.com* や *.babc.com* などで終わるすべての名前に一致します。
SysLocation	（オプション）次の操作の対象となるデバイスの MIB-II の sysLocation OID に格納された文字列値に一致する文字列を、カンマで区切って入力します。 • Include：自動検出プロセスに含めます。 • Exclude：自動検出プロセスから除外します。 場所の文字列はワイルドカードを使用して指定できます。アスタリスク（*）は、大文字と小文字が混ざった英数字、ハイフン（-）、アンダースコア（_）、および空白（スペースとタブ）の任意の長さの任意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 回の出現に一致します。たとえば、*San* * という SysLocation フィルタは、*San Francisco* や *San Jose* などで始まるすべての SysLocation 文字列に一致します。

ステップ 3　[Apply] をクリックします。

DCR へのデバイスのインポート

Operations Manager では、バルク インポート（NMS またはファイルからのインポート）用に DCR への直接リンクを用意しています（[Device Management] > [Device Configuration] > [Import Devices]）。

ステップ 1　[Administration] > [Device Management] > [Device Configuration] > [Import Devices] を選択します。

Common Services の [Import Devices] ページが表示されます。

ステップ 2　インポート情報を入力します。

インポートのヘルプが必要な場合は、このページの [Help] ボタンをクリックし、CiscoWorks オンライン ヘルプを開いてください。

Operations Manager の自動デバイス選択の設定

Operations Manager は、デフォルトで自動的な同期化を使用します。手動の同期化を自動的な同期化に変更するには、次の手順を実行します。

同期化プロセスを初めて実行する場合は、Operations Manager に追加されるデバイスの数によっては、Operations Manager がすべてのデバイスのインベントリを収集する際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。

自動デバイス選択を設定する手順は次のとおりです。

ステップ 1　[Administration] > [Device Management] > [Device Configuration] > [DCR Device Selection] を選択します。

[Device Selection] ページが表示されます。

ステップ 2　[Automatic] オプション ボタンをアクティブにします。

ステップ 3　[Apply] をクリックします。

Operations Manager は DCR と同期します。現在 Operations Manager にない 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に対してインベントリ収集を実行します。

ステップ 4　[Administration] > [Device Management] > [Device Configuration] > [IP Address Report] を選択して、重複デバイスがないかどうかを確認します。

この重複デバイスが導入環境に必要ない場合は削除します（デバイスの削除方法については、「デバイスの削除」（P.8-60）を参照してください）。

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、モニタ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モニタ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。

デバイスを手動で追加する手順は次のとおりです。

ステップ 1　[Administration] > [Device Management] > [Device Configuration] > [DCR Device Selection] を選択します。

[Device Selection] ページが表示されます。

ステップ 2　[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がデバイス セレクタに表示されます。

ステップ 3　次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。

選択したデバイスを確認する場合は、[Selection] タブをクリックすると、デバイスのリストが表示されます。

ステップ 4　[Select] をクリックします。

Operations Manager は、追加する対象となるデバイスのインベントリ収集を実行します。

ステップ 5　[Administration] > [Device Management] > [Device Configuration] > [IP Address Report] を選択して、重複デバイスがないかどうかを確認します。

この重複デバイスが導入環境に必要ない場合は削除します（デバイスの削除方法については、「デバイスの削除」（P.8-60）を参照してください）。

デバイスの状態について

[Device Management: Summary] ページには、Operations Manager インベントリのすべてのデバイスの状態が表示されます。このページを表示するには、[Administration] > [Device Management] > [Device Configuration] > [Device Summary] を選択します。

電話の検出収集のステータスを表示するには、「電話 XML 検出ステータスの確認とスケジュール」（P.8-65）を参照してください。

表 8-3 に、[Device Management Summary] ページに表示される情報を示します。

表 2-3 は、デバイスをインベントリに追加するときのデバイスの状態遷移を表しています。

表 2-3　インベントリに追加されたときのデバイスの状態遷移

インベントリ収集の開始	インベントリ収集の結果	結果のデバイス状態
インベントリ収集が進行中である。	正常に検出された。	Monitored
インベントリ収集が進行中である。	すべてのクレデンシャルが入力されていないか、または、一部のサービスが停止している。	Partially Monitored
インベントリ収集が進行中である。	• SNMP 情報が設定されていない。 • デバイスが応答していない。 • デバイスは到達不能である。 • デバイス クレデンシャルが正しくない。	Unreachable
インベントリ収集が進行中である。	• デバイス モデルが認識されない。 • ソフトウェア バージョンがサポートされていない。	Unsupported

Operations Manager に追加したデバイスの確認

デバイスが Operations Manager のインベントリに追加されたことを確認するには、それらのデバイスが [Device Summary] で Monitored の状態になっているかどうかを調べます。デバイスを確認する手順は次のとおりです。

ステップ 1　[Administration] > [Device Management] > [Device Summary] を選択します。

ステップ 2　デバイスを探して Monitored の状態になっていることを確認します。

インベントリ収集中に問題が発生した場合は、「デバイス インポートおよびインベントリ収集のトラブルシューティング」（P.2-15）を参照してください。

インベントリ収集のスケジュール

デバイスと電話には、個別のインベントリ収集スケジュールがあります。デバイス用のインベントリ収集スケジュールは 1 つだけです。スケジュールをさらに作成することはできません。既存のスケジュールの変更のみ行うことができます。IP 電話の場合は、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（[Administration] > [Device Management] > [Inventory Collection] > [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（「デバイスのインベントリ収集スケジュールの編集」（P.2-15）を参照）。

[IP Phone Discovery Schedule] ページ（[Devices] > [Device Management] > [Inventory Collection] > [IP Phone]）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（「電話機のディスカバリ スケジュールの追加」（P.2-15）を参照）。

デバイスのインベントリ収集スケジュールの編集

デバイスのインベントリ収集スケジュールを編集する手順は次のとおりです。

ステップ 1　[Administration] > [Device Management] > [Inventory Collection] > [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　目的の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。

電話機のディスカバリ スケジュールの追加

電話機のディスカバリ スケジュールを追加する手順は次のとおりです。

ステップ 1　[Devices] > [Device Management] > [Inventory Collection] > [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　次を入力します。

- 検出スケジュールの名前
- 検出を実行する曜日
- 検出を実行する時刻

ステップ 4　[OK] をクリックします。

デバイス インポートおよびインベントリ収集のトラブルシューティング

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、次のことを試してください。

- 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。「デバイスの設定とクレデンシャルの編集」（P.2-16）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。「SNMP タイムアウトと再試行の変更」（P.2-17）を参照してください。
- [Modify/Delete Device] ページのデバイス エラー情報を表示します。「デバイスのインベントリ収集の手動実行」（P.2-17）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。
- デバイスが DNS で解決可能であることを確認します。「Cisco Unified Communications のデバイスの DNS 設定」（P.2-36）を参照してください。

- 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。「Operations Manager をさらに活用するために、デバイス、レポート、その他の機能に特有の設定手順があります。詳細については、「デバイス収集前のデバイスの設定」（P.2-18）を参照してください。Operations Manager を開始する前に」（P.2-20）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。「Operations Manager に追加したデバイスの確認」（P.2-14）を参照してください。

[Modify/Delete Devices] ページには、デバイス情報とデータ収集情報が表示されます。[Modify/Delete Devices] ページを使用して、デバイスの現在の状態を判別したり、データ収集エラーを表示したりできます。

ステップ 1　[Administration] > [Device Management] > [Device Configuration] > [Modify/Delete Devices] を選択します。

[Modify/Delete Devices] ページが開きます。

ステップ 2　デバイスのインベントリ収集ステータスに応じて、目的のデバイスがあるフォルダを展開します（「Operations Manager に追加したデバイスの確認」（P.2-14）を参照してください）。

ステップ 3　デバイス名または IP アドレスをクリックします。

デバイス情報が表示されます。

ステップ 4　[Data Collection Status Information] にエラー情報がないか確認します（「Operations Manager をさらに活用するために、デバイス、レポート、その他の機能に特有の設定手順があります。詳細については、「デバイス収集前のデバイスの設定」（P.2-18）を参照してください。Operations Manager を開始する前に」（P.2-20）を参照してください）。

ステップ 5　エラーをクリアするために必要なアクションを実行します。

表 8-9 に、部分的に監視されるデバイスについて、[Modify/Delete Devices] ページに表示されるエラー コードの考えられる原因を示します。

デバイスの設定とクレデンシャルの編集

デバイスを追加した後は、以下のように設定を変更することができます。デバイス設定とクレデンシャルを編集するには、次の手順に従います。

ステップ 1　[Administration] > [Device Management] > [Device Configuration] > [Device Credentials] を選択します。

Common Services の [Device Summary] ページが開きます。

ステップ 2　デバイスが含まれているフォルダを展開します。

ステップ 3　更新するデバイスまたはデバイス グループを選択します。

ステップ 4　[Edit Credentials] をクリックします。

[Edit Device Configuration: Change Credentials] ページが表示されます。

- 単一デバイスを選択した場合は、そのデバイスに対して既存のすべてのクレデンシャルが [Edit Device Configuration: Change Credentials] ページで設定されます（アスタリスクがフィールドに設定される）。
- 複数のデバイスを選択した場合は、カンマ区切りの IP アドレスのリストのみが表示されます。

自動的に設定されるクレデンシャル（アスタリスク）は、実際のクレデンシャルを反映していません。これらは、クレデンシャルが使用可能であることを示しているにすぎません。

ステップ 5　次のクレデンシャルを更新できます。

- SNMPv2c/SNMPv1
- SNMPv3
- HTTP
- WMI

重複したデバイスの一方のクレデンシャルを変更する場合は、プライマリ デバイスが削除された場合のために、必ず両方のデバイスのクレデンシャルを変更してください。

ステップ 6　[OK] をクリックします。

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。リトライ回数を重ねるごとにタイムアウト期間が倍になります。

たとえば、タイムアウト値が 4 秒で、再試行値が 3 秒の場合、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] > [Inventory Collection] > [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 のタイムアウト設定を選択します。デフォルトは 4 秒です。

ステップ 3　新しいリトライ回数の設定を選択します。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。

ステップ 5　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手動実行

[Modify/Delete Devices] ページを使用して、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手動で実行することができます。インベントリ収集が発生すると、デバイスまたはグループの設定に変更があった場合は、新しい設定によって以前のすべての設定が上書きされます。

（注）　Operations Manager でデバイスの設定変更が検出されるのは、デバイスの検出（インベントリ収集）が実行されている間だけです。したがって、デバイスの設定への変更は、設定を変更した後に次回インベントリ収集が実行されるまで Operations Manager では表示されません。

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。一時停止されたデバイスは、インベントリ収集の対象にはなりません。インベントリ収集の対象として選択したデバイスの一部が一時停止中の場合は、Operations Manager にアクティブなデバイスだけがインベントリ収集の対象になるというメッセージが表示されます。

Operations Manager 物理検出プロセス（デバイスを DCR に追加するプロセス）や Operations Manager インベントリ収集プロセス（デバイスを調査して Operations Manager インベントリのコンポーネントをアップデートするプロセス）を、DCR 同期化プロセスと混同しないでください。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。

次のイベントが発生したときもインベントリ収集が実行されます。

- Operations Manager インベントリ全体がポーリングされる。このイベントは、インベントリ収集スケジュールによって制御されます（「インベントリ収集のスケジュール」（P.2-14）を参照）。
- Operations Manager が DCR との自動的な同期化を使用している場合に、DCR にデバイスが追加されるか、DCR 内のデバイスが変更される。このような DCR の変更には、デバイスの削除や、デバイスのクレデンシャル（IP アドレス、SNMP クレデンシャル、MDF タイプ）の変更なども含まれます。
- Operations Manager が DCR との手動の同期化を使用している場合に、[Device Selection] ページを使用して Operations Manager にデバイスが追加される。

ACS ログイン モジュールを使用している場合、ACS に設定されているシステム ID ユーザは Common Services のすべてのジョブ管理関連タスクと Operations Manager の再検出タスクを実行する権限を持っている必要があります。

再検出が実行されると、システム内のすべてのデバイスが検出されます。そのため、このタスクはネットワーク内のすべてのデバイスにアクセスできるユーザのみが使用できるようにする必要があります。

ステップ 1　[Administration] > [Device Management] > [Device Configuration] > [Modify/Delete Devices] を選択します。

[Modify/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　[Rediscover] をクリックします。

インベントリ収集が開始されます。

デバイス収集前のデバイスの設定

この項では、次の項目の概要について説明します。

- 「音声アプリケーション システムおよびソフトウェアの使用」（P.2-26）
- 「Operations Manager にイベントを送信する syslog レシーバの設定」（P.2-29）

Operations Manager へのデバイスの追加

この項では、デバイス ディスカバリとインベントリ収集の手順の概要について説明します。

デバイスを Operations Manager に追加するためには、多数のオプションがあります。導入形態に応じて、表 2-4 に示すオプションを使用してデバイスを追加できます。

表 2-4　Operations Manager のインベントリへのデバイスの追加

導入のタイプ	インベントリ収集オプション	説明
エンタープライズ バージョンのみ	1. デバイスを自動的に検出します。[1]	• デフォルト設定を使用します（エンタープライズ バージョンでは操作不要）。詳細については、「エンタープライズ導入のためのデバイスの自動検出」（P.8-3）を参照してください。
		• 自動検出のための設定を行います。「DCR からの特定のデバイスの追加」（P.8-8）を参照してください。 • 自動デバイス検出のビデオ チュートリアルを見るには、オンライン ヘルプの [E-Learning] アイコンをクリックします。
エンタープライズ バージョンまたはマルチ エンドカスタマー バージョン	2. デバイスを手動で追加します。 （エンタープライズ バージョンまたはマルチ エンドカスタマー バージョンのみ）	「DCR へのデバイスの追加」（P.8-9）
エンタープライズ バージョンまたはマルチ エンドカスタマー バージョン	3. デバイスをインポートします。 （エンタープライズ バージョンまたはマルチ エンドカスタマー バージョンのみ）	「DCR へのデバイスのインポート」（P.2-12）

1. インベントリ情報を収集するには、デバイス クレデンシャルが必要です。エンタープライズ バージョンの場合、自動検出がデフォルトです。マルチ エンドカスタマー バージョンを導入した場合に検出を処理する方法の詳細については、「DCR へのデバイスの追加」（P.8-9）または「DCR へのデバイスのインポート」（P.2-12）を参照してください。

Operations Manager のカスタマイズ

この項では、必須ではないものの、Operations Manager の機能を拡張する操作について説明します。

- 「サポートされる NMS 統合」（P.2-22）
- 「イベントの表示」（P.2-36）

ネットワークを監視する Operations Manager にデバイスを追加した後、特別な導入向けに Operations Manager をカスタマイズするための作業を表 2-5 に要約します。

（注）　これらの作業はすべてオプションです。Operations Manager がネットワークをモニタするための必須の作業ではありません。

表 2-5　Operations Manager のセットアップ

作業	説明
通知の設定	Unified Dashboard 画面を監視してイベントを確認するほか、イベントに応じて、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。
デバイス グループの設定	[Fault Monitor] 画面や、通知サービスの通知グループで使用するデバイス グループを作成します。

表 2-5　Operations Manager（続き）のセットアップ

作業	説明
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せん。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	エンタープライズ バージョンのみ。Operations Manager では、インベントリ収集用にデフォルトのスケジュールを 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。
Diagnostics View のカスタマイズ	Diagnostic Summary、Server、Phone、Gateway、Cluster の各 View に表示するビューのポートレットを変更できます。
特定のデバイス イベントのアクティブ化	デバイスが Operations Manager データベースに追加されると、ほとんどのデバイス イベントがユーザ インターフェイスに表示されます。 ただし、いくつかのイベントは、Operations Manager で設定しなければ表示されません。 次のイベントを Operations Manager で表示するには、それをアクティブ化する必要があります。 • HardwareFailure • Number Of Registered Gateways Increased • Number Of Registered Gateways Decreased • Number Of Registered MediaDevices Increased • Number Of Registered MediaDevices Decreased

Operations Manager をさらに活用するために、デバイス、レポート、その他の機能に特有の設定手順があります。詳細については、「デバイス収集前のデバイスの設定」（P.2-18）を参照してください。

Operations Manager を開始する前に

Operations Manager は Operations Manager サーバまたはクライアント システムからアクセスできます。

- クライアント システムが使用可能な場合は、すべての設定と日常的なアクティビティをクライアント システムから実行することを推奨します。クライアント システムが使用できない場合は、Operations Manager サーバでもクライアント システムのすべてのシステム要件を満たしている必要があります。クライアント システムの要件については『*Installation Guide for Cisco Unified Operations Manager*』を参照してください。
- クライアント システムにインストールされているすべてのポップアップ ブロッカー ユーティリティをディセーブルにしてから、Operations Manager を起動します。

- デフォルトでは、SSL は Common Services でイネーブルにされていません。Operations Manager 8.6 にアップグレードし、SSL をイネーブルにしてからアップグレードした場合、アップグレード後もイネーブルのままです。

クライアント システムでの Operations Manager の起動

Internet Explorer で、Operations Manager サーバの IP アドレスまたは DNS 名に続けてポート番号 1741 を入力します。たとえば、http://*om_server name*:1741 と入力します。

Operations Manager サーバでの Operations Manager の起動

Windows デスクトップで、[Start] > [All Programs] > [Cisco Unified Operations Manager] > [Cisco Unified Operations Manager] を選択します。

（注） Windows 2003 または Windows 2008 システムで拡張セキュリティをイネーブルにしている場合は、Internet Explorer の信頼済みサイト ゾーンに Operations Manager ホーム ページを追加する必要があります。信頼済みサイトに追加するまでは、Operations Manager ホーム ページにアクセスできません。

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 または Windows 2008 システムでセキュリティ強化をイネーブルにしている場合、Operations Manager のホームページにアクセスできるようにするには、次の手順を実行する必要があります。

Operations Manager ホーム ページを追加する手順は次のとおりです。

ステップ 1　Operations Manager を開き、[Start] > [All Programs] > [Cisco Unified Operations Manager] > [Cisco Unified Operations Manager] を選択します。

ステップ 2　[File] メニューから [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] をクリックしてこのサイトをリストに移します。

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この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。

Operations Manager からの [Cisco Unified Communications Management Server] リンクの追加

ローカルまたはリモートでインストールされた Service Monitor、Service Statistics Manager、Provisioning Manager サーバに Operations Manager からリンクを追加するには、[UC Management Suite] タブを使用します。

ステップバイステップの説明については、「Cisco Unified Communications 管理アプリケーション リンクの設定」（P.21-1）を参照してください。

Service Monitor のイベントやトラップの処理についての詳細は、「処理される SNMP トラップ」（P.C-1）を参照してください。未解決の問題については、『*Release Notes for Cisco Unified Operations Manager*』を参照してください。

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。
- Local security or 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（Common Services Local Login Module）または Cisco Security ACS によって制御されます。デフォルトで、サーバ上のローカル セキュリティはイネーブルです。

  Operations Manager は Cisco Secure ACS との統合をサポートします。詳細については、『*Installation Guide for Cisco Unified Operations Manager*』の C-1 ページ、「Security Configuration with Cisco Secure ACS」を参照してください。
- SSL : Secure Socket Layer（SSL）は、プライバシー、認証、およびデータ整合性を通じて、データの安全なトランザクションを実現するアプリケーション レベルのプロトコルです。SSL は、証明書、公開鍵、および秘密鍵に依存しています。（デフォルトでは、SSL は Common Services でイネーブルにされていません）。

  セキュアなアクセスの必要性に応じて、SSL をイネーブルまたはディセーブルにすることができます。Operations Manager は、クライアントとサーバの間の SSL をサポートしています。

セキュリティの設定を開始するには、Common Services のヘルプの「Setting Up Security」のトピックを参照してください。

サポートされる NMS 統合

Operations Manager は、使用しているネットワーク内にある Network Management Systems（NMS; ネットワーク管理システム）との統合に対応しています。Operations Manager は Operations Manager と同じシステムに混在する NMS をサポートしません。

- 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。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、トラップを Operations Manager に転送するようそのアプリケーションを設定してください。
- 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、「SNMP トラップの受信とフォワーディングの設定」（P.2-22）を参照してください。
  - 処理されたトラップを転送するには、「通知の設定」（P.15-8）を参照してください。

  パススルー トラップおよび処理されたトラップの詳細については、「処理される SNMP トラップ」（P.C-1）を参照してください。

SNMP トラップの受信とフォワーディングの設定

Operations Manager は、使用可能な任意のポートでトラップを受信し、そのトラップをデバイスおよびポートのリストに転送できます。この機能により、Operations Manager は、他のトラップ処理アプリケーションと簡単に連携できます。

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

ここでは、次の内容について説明します。

- 「SNMP トラップ受信ポートの更新」（P.2-23）
- 「Operations Manager にトラップを送信するためのデバイスの設定」（P.2-23）
- 「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 トラップ転送の設定」（P.2-24）
- 「SNMP トラップとしての Windows イベントの転送」（P.20-7）

トラップを直接 Operations Manager に送信するには、「Operations Manager にトラップを送信できるようにするためのデバイスの設定」（P.20-6）の作業を実行します。

SNMP トラップの受信を NMS またはトラップ デーモンと統合するには、「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」（P.2-24）の手順に従います。

SNMP トラップ受信ポートの更新

デフォルトで、Operations Manager はポート 162 で SNMP トラップを受信します。このポートは、必要に応じて変更することができます。

SNMP トラップ受信ポートを更新する手順は次のとおりです。

ステップ 1　[Administration] > [System Settings] > [Miscellaneous] > [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] 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、「Operations Manager が監視するポートとインターフェイス」（P.8-6）を参照してください。

Operations Manager にトラップを送信するためのデバイスの設定

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 の監視対象とするすべてのシスコ デバイスで SNMP をイネーブルにし、Operations Manager サーバに SNMP トラップを送信するようそのデバイスを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 インターフェイスまたは GUI インターフェイスを使用して、デバイスが Operations Manager にトラップを送信できるようにします。「Operations Manager にトラップを送信できるようにするためのデバイスの設定」（P.20-6）を参照してください。

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 トラップの受信を他のトラップ デーモンおよび他の Network Management System（NMS; ネットワーク管理システム）と統合するには、次の作業を 1 つ以上実施する必要がある場合があります。

- Operations Manager を実行しているホストを、ネットワーク デバイスのトラップ宛先リストに追加します。「Operations Manager にトラップを送信するためのデバイスの設定」（P.2-23）を参照してください。宛先トラップ ポートとしてポート 162 を指定します。
- 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、トラップを Operations Manager に転送するようそのアプリケーションを設定する。

表 2-6 は、SNMP トラップ受信のシナリオを示し、それぞれの利点を挙げています。

表 2-6　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 デバイスが、Operations Manager を実行しているホストのポート 162 にトラップを送信する。 Operations Manager はトラップを受信し、そのトラップを NMS に転送します。	• NMS の再設定が不要。 • ネットワーク デバイスの再設定が不要。 • Operations Manager が信頼性の高いトラップ受信、ストレージ、およびフォワーディング メカニズムを提供。 • NMS は継続して、NMS が実行されているホストのポート 162 でトラップを受信します。 • ネットワーク デバイスが引き続きポート 162 にトラップを送信。
NMS がデフォルト ポート 162 でトラップを受信し、Operations Manager を実行しているホストのポート 162 にそのトラップを転送する。	• NMS の再設定が不要。 • ネットワーク デバイスの再設定が不要。 • Operations Manager は、NMS によってドロップされたトラップを受信しない。

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。

トラップの転送を設定する手順は次のとおりです。

ステップ 1　[Administration] > [System Settings] > [Miscellaneous] > [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 アドレスまたは名前
- トラップの受信が可能なサーバのポート番号

  他の Cisco Unified Communications Manager アプリケーションが使用するポートの一覧については、「Operations Manager および他の CUCM アプリケーションが使用するポートとプロトコル」（P.20-9）を参照してください。

ステップ 3　[Apply] ボタンをクリックします。

Health Monitor の設定

Health Monitor ユーティリティは、Operations Manager プロセスをモニタし、プロセスが停止して再起動したときに気づき、電子メールの更新を送信できます。

電子メールの更新を受信する手順は次のとおりです。

ステップ 1　*NMSROOT*/HealthMonitor/conf/HealthMonitor.cfg ファイルを編集します。

ステップ 2　次の各パラメータ値を入力します。

- SMTP_Server：SMTP メール サーバのアドレス。
- Receiver_Email_ID：通知先の管理者の電子メール ID
- Sender_Email_ID：送信者を特定する電子メール ID

ステップ 3　ファイルを更新したら、HealthMonitor を再起動して更新を有効にします。コマンドラインから、次のコマンドを入力します。

```
net stop HealthMonitor
net start HealthMonitor
```

詳細については、「通知の設定」（P.15-8）を参照してください。

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 または Windows 2008 システムでセキュリティ強化をイネーブルにしている場合、Operations Manager のホームページにアクセスできるようにするには、次の手順を実行する必要があります。

Operations Manager ホーム ページを追加する手順は次のとおりです。

ステップ 1　Operations Manager を開き、[Start] > [All Programs] > [Cisco Unified Operations Manager] > [Cisco Unified Operations Manager] を選択します。

ステップ 2　[File] メニューから [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] をクリックしてこのサイトをリストに移します。

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この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。

Operations Manager サーバでの DSCP トラフィックの優先順位付けの設定

Operations Manager サーバで、設定可能な DSCP の優先順位がマークされるパケットをマークできるようにするには、次の手順を実行します（Windows 2008 サーバのみ）。

1. Windows の [Start] > [Run] を選択します。
2. gpedit.msc と入力して、[Enter] をクリックし、[Local Group Policy Editor] を開きます。
3. [Local Computer Policy] > [Computer Configuration] > [Windows Settings] > [Policy-based QoS] を選択して、ポリシーを作成します。たとえば、dscp_settings という名前で作成します。
4. [Policy Profile] タブで、このポリシーに対する DSCP 値を指定します。たとえば 55 と入力します。
5. [Application Name] タブで、[All Applications] を選択します。
6. [IP Addresses] タブで、[This QoS policy applies to Any source IP address and any destination IP address] を選択します。
7. [Protocol and Ports] タブで、[this QosS policy applies to TCP and UDP] を選択します。また、送信元ポートと宛先ポートも選択します。
8. [OK] をクリックします。
9. これらのポリシーの変更を適用するには、gpupdate /force コマンドを実行する必要があります。

音声アプリケーション システムおよびソフトウェアの使用

次のトピックでは、ハードウェア固有およびバージョン固有のタスクと動作について説明します。

（注）　Cisco Unified Communications Manager のバージョンおよびサポートに関する最新の詳細情報は、Cisco.com の Cisco Unified Communications Manager 互換性マトリクスを参照してください。

Operations Manager で使用するための音声アプリケーション システムおよびソフトウェアの設定

表 2-7 に、Cisco Unified Operations Manager（Operations Manager）が Cisco 音声アプリケーション ソフトウェアを正常に監視できるようにするために、事前に実行する必要のあるタスクを示します。

表 2-7　アプリケーション ソフトウェアのバージョンおよびシステム別のコンフィギュレーション タスク

使用する音声アプリケーション ソフトウェア...	使用する音声アプリケーション システム...	実行する必要のあるタスク
Operations Manager がサポートする任意のアプリケーション ソフトウェア	Media Server	「メディア サーバの SNMP サービス コミュニティ ストリング権限の設定」（P.2-29）
Cisco Unified Communications Manager 3.3 以降	Media Server	「Cisco Unified CM のクラスタ名の変更」（P.2-27）
Cisco Unified Communications Manager 6.x 以降	Media Server	「Cisco Unified CM での syslog レシーバの設定」（P.2-29）
	Media Server	「Cisco Unified CM での CDR の転送の設定」（P.2-28）
Cisco Unified Communications Manager Express	ルータ	ルータの **CCMEEnabled** を true に設定します。1.3.6.1.4.1.9.9.439.1.1.1.0 の **snmp get** が 1 を返すように設定します。
SRST Router	ルータ	このルータの SRST サービスをイネーブルにします。1.3.6.1.4.1.9.9.441.1.2.1.0 の **snmp get** が 1 を返すように設定します。
Cisco Unity Connection	N/A	「Cisco Unity Connection での syslog レシーバの設定」（P.2-32）
Cisco Unified Communications Manager 5.1.3 以降（Syslog/RTMT の場合）	Voice Gateways Media Server	「Operations Manager でのイベントのアクティブ化」（P.E-82）
Cisco Unified Presence	N/A	「Cisco Unified Presence での syslog レシーバの設定」（P.2-33）

Cisco Unified CM のクラスタ名の変更

（注） この手順を実行する必要があるのは、メディア サーバを Cisco Unified CM 3.3 以降で実行している場合だけです。

Operations Manager は、同じ名前を持つ 2 つのクラスタは管理できません。複数の Cisco Unified CM クラスタを管理する場合は、デフォルトのクラスタ名を変更する必要があります。Cisco Unified CM 3.3 以降では、デフォルトのクラスタ名として *StandAloneCluster* を使用しています。

Cisco Unified CM の設定の詳細な説明については、Cisco Unified CM のマニュアルを参照してください。

Cisco Unified CM のクラスタ名を変更する手順は次のとおりです。

ステップ 1　Cisco Unified CM のクラスタ名を変更するには、[Cisco Unified Communications Manager Administration] ページを開きます。

ステップ 2　メニューバーの [System] を選択し、次に [Enterprise Parameters] を選択します。

[Enterprise Configuration] ページが開きます。

ステップ 3　Cluster ID フィールドに、新しいクラスタ名を入力します。

ステップ 4　[Update] をクリックします。

Cisco Unified CM での CDR の転送の設定

Operations Manager を使用して、使用する Unified CM の Call Detail Record（CDR; 呼詳細レコード）のトランク利用率を監視できます。

Service Monitor を Operations Manager で監視される UC 管理アプリケーションとして追加する必要があります。詳細については、「Service Monitor サーバへのアクセス」（P.21-2）を参照してください。

また、Operations Manager でポーリングをイネーブルにする必要があります。詳細については、「ポーリング パラメータの編集」（P.19-16）を参照してください。

Operations Manager および Service Monitor を使用して CDR ベースのトランク データを監視する手順は次のとおりです。

ステップ 1　Unified Communications Manager で、[Administration] を選択します。

ステップ 2　[System] > [Service Parameters] を選択して、[Service Parameters Configuration] ページを開きます。

ステップ 3　次のパラメータを設定します。

- [CDR Enabled Flag] : [System] まで下方にスクロールして、[True] を選択します。
- [Call Diagnostics Enabled] : [Cluster wide Parameters (Device - General)] まで下方にスクロールして、[Set to Enable Only When CDR Enabled Flag is True] を選択します。

ステップ 4　Cisco Unified CM で Operations Manager を課金サーバとして追加する手順は次のとおりです。

a.　[Tools] > [CDR Management] を選択します。

b.　[Billing Applications Server Parameters] までスクロール ダウンし、[Add New] をクリックします。

c.　次を入力します。

- [Host Name]/[IP Address] : Operations Manager がインストールされているシステムの IP アドレスです。
- [User Name] : *smuser* と入力します。
- [Password] : デフォルトのパスワードは *smuser* です。

d.　[SFTP Protocol] を選択します。

e.　[Directory Path] : */home/smuser/* と入力します。

f.　[Resend on failure] チェックボックスを選択します。

ステップ 5　[Add] をクリックします。

メディア サーバの SNMP サービス コミュニティ ストリング権限の設定

（注）　この手順は、音声アプリケーション ソフトウェアを実行しているメディア サーバで実行します。Operations Manager のインストールによってそのサーバに SNMP サービスがインストールされてイネーブルになっていることを確認します。

SNMP サービスのコミュニティ ストリング権限が *none* に設定されていると、Operations Manager はメディア サーバで稼動中のサポートされる音声アプリケーションを監視できません。コミュニティ ストリングの権限が*読み取り専用（read-only）*、*読み取りと書き込み（read-write）*、または*読み取りと作成（read-create）*に変更されないかぎり、SNMP クエリーは正常に実行されません。

ステップ 1　メディア サーバ システムで、[Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Services] の順に選択します。

[Services] ウィンドウが開きます。

ステップ 2　[SNMP Service] をダブルクリックします。

[SNMP Services Properties] ウィンドウが開きます。

ステップ 3　[Security] タブを選択します。

ステップ 4　[Community String] を選択して、[Edit] をクリックします。

ステップ 5　権限を [NONE] から [READ ONLY] に変更します。

Operations Manager には、読み取り専用権限が必要です。権限を「読み取りと書き込み」または「読み取りと作成」に設定する必要はありません。

Operations Manager にイベントを送信する syslog レシーバの設定

Cisco Unified Communications Manager、Unity Connection、Unified Presence の syslog メッセージを Operations Manager で正しく受信するには、デバイスの管理用またはサービスアビリティの Web ページから syslog レシーバを追加する必要があります。必要な操作を実行するには、次の手順に従ってください。

Operations Manager でサポートされている syslog イベントとして、現在 Service Down イベントが含まれています。

- 「Cisco Unified CM での syslog レシーバの設定」（P.2-29）
- 「Cisco Unity Connection での syslog レシーバの設定」（P.2-32）
- 「Cisco Unified Presence での syslog レシーバの設定」（P.2-33）

Cisco Unified CM での syslog レシーバの設定

Cisco Unified Communications Manager の syslog メッセージを正常に受信するには、デバイスのサービスアビリティ Web ページで syslog の受信者を追加する必要があります。

syslog のプロセスによって、次に示すような Unified CM クラスタに登録されたエンティティが検出されます。

- 電話、ボイスメールのエンドポイント、ゲートウェイなどに対する登録の変更。

- クラスタ内でプロビジョニングされた新しい電話。

プロビジョニングされた新しい電話は、既存のデバイス プールに対してプロビジョニングされた場合には検出されます。そのクラスタに対するデバイス検出が終わった後で、クラスタに追加された新しいデバイス プールに電話を追加した場合は、[Run Now] を使用してこれらの電話を Operations Manager に表示する必要があります。

どの syslog イベントが Unified Communications Manager のリリースにマップされるか、詳細については、[Fault Monitor] に一覧表示されているイベントを確認するか、表 E-2 を参照してください。

Cisco Unified Communications Manager で syslog レシーバを設定する手順は次のとおりです。

ステップ 1　Cisco Unified Communications Manager で、デバイスのホーム画面の右上隅にある [Navigation] ドロップダウンから、[Cisco Unified CM Administration] を選択します。

ステップ 2　[System] > [Enterprise Parameters] を選択します。

ステップ 3　[Cisco Syslog Agent] セクションで、次の必須フィールドを更新します。

- [Remote Syslog Server Name] に Operations Manager の IP アドレスを指定します。
- [Syslog Severity For Remote Syslog Messages] のドロップダウン メニューから [Informational] を選択します。

ステップ 4　デバイスのホーム画面の右上隅にある [Navigation] ドロップダウンから、[Cisco Unified Serviceability] を選択します。

ステップ 5　[Alarm] > [Alarm Configuration] を選択します。

注意　Operations Manager の syslog を統合するために syslog の受信者を設定する際に、CCM エンタープライズ サービス パラメータを使用しないでください。エンタープライズ パラメータがイネーブルになっていると、Operations Manager が処理する予定であるかどうかにかかわらず、重大度レベルが一致するすべての syslog メッセージが送信されます。

ステップ 6　特定のマシンに対して正しいアラーム設定要素を（[Server]、[Service Group]、[Service]）を選択し、[Go] をクリックします。次の例を参考にしてください。

- Operations Manager サーバの名前とアドレスを [Server] テキスト ボックスに入力します。
- 次の表に基づいて、[Service Group] および [Service] オプションを選択します。

次の Unified Communications Manager バージョンの場合	次のアラーム設定要素を選択します
4.x	Cisco CallManager

次の Unified Communications Manager バージョンの場合	次のアラーム設定要素を選択します
5.1	• [Server] > [Service] > [Cisco AMC Service] • [Server] > [Service] > [Cisco CDR Agent] • [Server] > [Service] > [Cisco CDR Repository Manager] • [Server] > [Service] > [Cisco CallManager] • [Server] > [Service] > [Cisco Database Layer Monitoring] • [Server] > [Service] > [Cisco DRF Client] • [Server] > [Service] > [Cisco DRF Master]
6.x 以降	• [Service Group] > [CM Services] > [Service] > [Cisco CallManager] • [Service Group] > [CDR Service] > [Cisco CDR Agent and Cisco CDR Repository Manager] • [Service Group] > [Database and Admin Services] > [Cisco Database Layer Monitoring] • [Service Group] > [Performance and Monitoring Services] > [Cisco AMC Service] • [Service Group] > [Backup and Restore] > [Cisco DRF Client and Cisco DRF Master] • [Service Group] > [Remote Syslogs]

ステップ 7　[Enable Alarm] チェックボックスをクリックして、適切な [Alarm Event Level] を選択します。

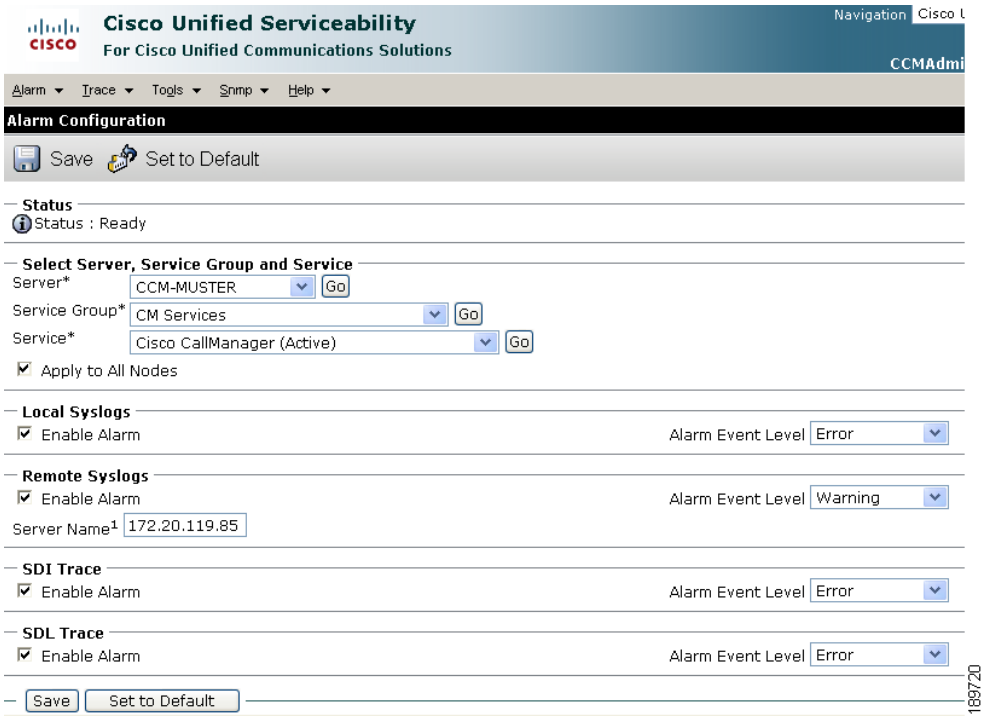
Cisco.com の『*Cisco Unified Serviceability Administration Guide for Cisco Unified Communications Manager*』の「Alarm Configuration Settings」を確認します。

たとえば [Local Syslogs] の場合は、アラーム イベント レベルを [Error] に設定します。

ステップ 8　使用している Unified Communications Manager に基づいて、必要な情報を入力します。デバイス クラスタ検出またはリモート syslog 通知の場合は、アラーム イベント レベルを [Informational] に設定します。

ステップ 9　[Apply to all nodes] をオンにします（サービスアビリティ ページの例については、図 2-3（P.2-32）を参照してください。サービスアビリティの Web ページは、設定しているデバイスのバージョンによって異なる場合があります）。

図 2-3　バージョン 6.0 の Cisco Unified Serviceability ページ



ステップ 10　[Save] をクリックします。

syslog メッセージは 1,024 文字までに制限されています（見出しを含む）。この syslog の制限のため、syslog ベースのイベントの詳細に完全な情報が含まれない場合があります。syslog メッセージがこの制限を超えた場合、syslog の送信者によって 1,024 文字に切り捨てられます。

Cisco Unity Connection での syslog レシーバの設定

Cisco Unity Connection の syslog メッセージを正常に受信するには、デバイスのサービスアビリティ Web ページで syslog の受信者を追加する必要があります。

どの syslog イベントが Unity Connection のリリースにマップされるか、詳細については、[Fault Monitor] に一覧表示されているイベントを確認するか、表 E-2 を参照してください。

Cisco Unity Connection で syslog レシーバを設定する手順は次のとおりです。

ステップ 1　Cisco Unity Connection で、デバイスのホーム画面の右上隅にある [Navigation] ドロップダウンから、[Cisco Unity Connection Administration] を選択します。

ステップ 2　[System] > [Enterprise Parameters] を選択します。

ステップ 3　[Cisco Syslog Agent] セクションで、次の必須フィールドを更新します。

- [Remote Syslog Server Name] に Operations Manager の IP アドレスを指定します。
- [Syslog Severity For Remote Syslog Messages] のドロップダウン メニューから [Informational] を選択します。

ステップ 4　デバイスのホーム画面の右上隅にある [Navigation] ドロップダウンから、[Cisco Unity Connection Serviceability] を選択します。

ステップ 5　[Alarm] > [Configuration] を選択します。

次のように特定のマシンに適したアラーム設定要素を選択します。

- Unity Connection 8.x の場合は次のように設定します。
  - [Informational Alarms for Local syslogs] をイネーブルにします。
  - [Informational Alarms Remote Syslogs] をイネーブルにして、Operations Manager Server の IP アドレスとしてサーバ名を入力します。

ステップ 6　[Save] をクリックして設定を保存すれば、syslog の設定は完了します。

Cisco Unified Presence での syslog レシーバの設定

Cisco Unified Presence の syslog メッセージを正常に受信するには、デバイスのサービスアビリティ Web ページで syslog の受信者を追加する必要があります。

どの syslog イベントが Cisco Unified Presence のリリースにマップされるか、詳細については、[Fault Monitor] または他のインターフェイスに一覧表示されているイベントを確認するか、表 E-2 を参照してください。

Cisco Unified Presence で syslog レシーバを設定する手順は次のとおりです。

ステップ 1　Cisco Unified Presence で、デバイスのホーム画面の右上隅にある [Navigation] ドロップダウンから、[Cisco Unified Presence Serviceability] を選択します。

ステップ 2　[Alarm] > [Configuration] を選択します。

ステップ 3　特定のマシンに対して正しいアラーム設定要素を（[Server]、[Service Group]、[Service]）を選択し、[Go] をクリックします。次の例を参考にしてください。

- Operations Manager サーバの名前とアドレスを [Server] テキスト ボックスに入力します。
- [Service Group] で [CUP Services] を選択します。
- [Remote Syslogs] に対しては、[Enable Alarms] を選択して、アラーム イベント レベルを [Informational] に設定します。

ステップ 4　[Save] をクリックして設定を保存すれば、syslog の設定は完了します。

Unity の Event Monitoring Service の設定

Event Monitoring Service（EMS）は、Remote Serviceability Kit と一緒にインストールされている必要があります。

Operations Manager での次の Unity イベントに対応できるよう、Event Monitoring Service を設定します。

- OutOfDiskSpace：イベント ソース：ESE、イベント ID：482。
- HardDiskError：イベント ソース：Cissesrv、イベント ID：24600。
- ExchangeLoginFailed：イベント ソース：CiscoUnity_Doh、イベント ID：32013。

これらのイベントの詳細については、「サポートされるイベント」（P.E-3）を参照してください

Event Monitoring Service を設定する手順は次のとおりです。

ステップ 1　[Desktop] で [Tools Depot] を開き、[Diagnostic Tools] > [Event Monitoring Service] の順に移動します。

ステップ 2　ダブルクリックして実行します。

ステップ 3　通知を受信する受信者を作成します。[File] > [New] > [Recipient] を選択するか、ナビゲーション ツリーの [Recipients] ノードを選択して、[Create New Recipient] をクリックします。

ステップ 4　[Recipient Name] に入力して、受信者を 1 人指定します（あるいは [SMTP] の下に複数の電子メール アドレスを指定してグループを指定します）。

ステップ 5　任意の通知方法タブを選択します。

- SNMP トラップのタブは、Remote Serviceability Kit と連携して、トラップ（Windows の SNMP サービス プロパティで定義）を宛先に送信します。
- syslog のタブでは、イベントに対して Syslog サーバのアドレスを入力できます。
- フェールオーバーのタグは通知ではありませんが、特別なイベントを受信したときにフェールオーバーの強制的な実行を指定できます。

ページの上部にある [Test] ボタンを使用すると、定義した受信者にテスト イベントが送信されます。これらの内容は次のとおりです。

- イベント ソース：EMSTest
- イベント ID：10001
- 説明：Event Monitoring Service のテスト メッセージ

ステップ 6　監視するイベントを作成します。[File] > [New] > [Event] を選択するか、ナビゲーション ツリーの [Monitored Events] ノードを選択して、[Create New Event] をクリックします。

イベントが現在 Windows Event Viewer にある場合は、次の手順に従って、[Add New Event] ダイアログにそのイベント情報を入力してください。

- Windows Event Viewer でイベントを選択します。
- [Copy Event to Clipboard] を選択します。
- [Add New Event] ダイアログの [Import Event From Clipboard] を使用します。

手動でイベントを追加する手順は次のとおりです。

ステップ 1　プルダウン メニューから [Event Source] を選択します。

ステップ 2　[Event ID] を選択して、任意の ID を入力します。[All Event IDs] を使用して、指定したイベント ソースからのすべてのイベントを対象にすることもできます。

ステップ 3　[Type] を選択して、送信する必要のある通知レベルをフィルタします。

ステップ 4　すべてのレベルのイベントおよび [Type] が **unknown** のイベントに対して [Errors]、[Warnings]、および [Informational] を選択します。

ステップ 5　[Notes] に、トラブルシューティングの手順など、通知に含める情報を入力します。

コンテンツ セクションには、[Recipient Voicemail] オプションを使用するイベント用にカスタマイズした WAV を登録できます。

[Email Subject and Body] は、[Recipient Email] に対して送信されるメッセージの形式および SMTP 通知方式をカスタマイズするために使用します。カスタマイズが不要の場合は、デフォルトのままにしておきます。

ステップ 6　新しいイベントを追加したら、[OK] を選択します。

新しいイベントを有効にするには、1 人以上の受信者を追加する必要があります。

ステップ 1　新しく追加したイベントを選択して、[Add Recipients] アイコンをクリックします。[Recipients] と通知方式は、チェックボックスを使用して細かく定義できます。

ステップ 2　[Active] チェックボックスをチェックし、[Apply] をクリックしてイベントを有効にします。

この手順は、ナビゲーション ツリーの [Monitored Events] ノードから実行することもできます。

他の基準を満たすイベントを除外または無視することもできます。その場合は、[File] > [New] > [Exclusion] を選択するか、ナビゲーション ツリーの [Exclusions] ノードを選択して [Create New Exclusion] をクリックします。

イベントが現在 Windows Event Viewer にある場合は、[Add Exclusion] ダイアログにそのイベント情報を入力できます。その場合は、Windows Event Viewer でイベントを選択し、[Copy Event to Clipboard] をクリックします。[Add Exclusion] ダイアログで、[Import Event From Clipboard] を使用します。

手動でイベントを除外する手順は次のとおりです。

ステップ 1　プルダウン メニューから [Event Source] を選択します。

ステップ 2　[Specific Event ID] を選択して、任意の ID を入力します。[All Event IDs] を使用して、指定したイベント ソースからのすべてのイベントを対象にすることもできます。

ステップ 3　新しい除外対象を追加し終えたら、[OK] を選択します。

Cisco Unified CM での RTMT の設定

Operations Manager は、RTMT と同じポーリング レートとしきい値の設定を使用します。通常の操作では、何もする必要はありません。デフォルトで適切に機能します。

（注）　この設定は、Unified Communications Manager（Unified CM）のパフォーマンスと Operations Manager に影響します。

ポーリング レートを低くする場合は、リアルタイムで監視するポーリング レートを高くし、Unified CM のパラメータ設定を更新して、次の手順を使用します。

- ポーリングとしきい値のパラメータ設定を更新するには、Unified Communications Manager Administration ページに移動します。
- CallManager 6.x 以降の場合は、[System] > [Service Parameter] > [publisher] > [Cisco AMC Service] の順に選択して、[Data Collection Polling] のレートの値を変更します。

- しきい値のパラメータを変更するには、RTMT をインストールして起動し、[AlarmCentral] を選択し、特定のアラートを選択し、右クリックして Alert Property を起動します。

Cisco Unified CM での HTTP クレデンシャルの設定

Operations Manager は、SNMP の他にも AVVID XML Layer（AXL）API を使用して Cisco Communications Manager を管理します。これは、Operations Manager が AXL インターフェイスを使用して HTTP 経由で SOAP を呼び出し、Cisco Unified Communications Manager からエラー情報やパフォーマンス情報を収集することを意味しています。これらの照会を実行するために、Operations Manager には HTTP ユーザ名とパスワードが必要です。

このユーザ名とパスワードには管理者特権は必要ありません。*http://server-name/ccmadmin* に対する読み取りレベルのアクセスを持つクレデンシャルが必要です。

Cisco Unified Communications のデバイスの DNS 設定

Operations Manager では、Unified CM の名前を Domain Name Service（DNS; ドメイン ネーム サービス）で解決できないと、正しいモニタリング情報を収集できません。

デバイス名が解決可能であることを確認してください（フォワードとバックワードの両方）。

DNS については、次のことに注意してください。

- デバイスが IP アドレスだけで設定されている場合、DNS 設定は問題になりません。
- デバイスが DNS 名で設定されている場合は、DNS サーバによって名前が解決されます。
- デバイスは syslog を Operations Manager サーバに送信するよう設定する必要もあります。手順の詳細については、「Cisco Unified CM での syslog レシーバの設定」（P.2-29）を参照してください。
- DNS 解決についての詳細は、「DCR へのデバイスの追加」（P.8-9）と、Cisco.com にある『Deployment Guide』を参照してください（URL：http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html）。

イベントの表示

Unified Dashboard 画面を使用して、イベントを表示できます。Unified Dashboard から [Diagnostics] タブを選択して、任意のビュー表示からイベント情報を参照します。

他にも、次の場所でイベントが表示されます。

- Fault Monitor
- レポート
- Service Level View