CHAPTER 19

Operations Manager の管理

この章では、次の事項について説明します。

Operations Manager の管理タスクの実行

IP Communications Operations Manager（Operations Manager）の Administration タブから、表 19-1 に示しているタスクを実行できます。

表 19-1　Operations Manager の管理タスク

タスク	説明
Polling and Thresholds P.17-1 の「ポーリングとしきい値の設定」を参照してください。	Polling and Thresholds から、次のタスクを実行できます。 • デバイス　グループ別にポーリング間隔、タイムアウト、およびリトライを変更する。 • ポーリング設定をイネーブルおよびディセーブルにする。 • しきい値を変更して、ポーリングされたデータの比較対象となる制限を再設定する。 • しきい値設定をカスタマイズする。 • ポーリングとしきい値に関するグループのプライオリティを再設定する。 • ポーリングとしきい値の変更をシステムに適用する。変更を適用すると、Operations Manager によって、データ コレクタが次のように設定されます。 – アップデートされたポーリング パラメータとしきい値の使用を開始する。 – 以前に一時停止されていたデバイスまたはデバイス要素のポーリングを再開する。
SRST Poll Settings P.18-1 の「SRST ポール設定値の設定」を参照してください。	SRST Poll Settings ページから、SRST モニタリングを設定できます。
Service Quality Settings P.19-7 の「Service Quality Settings の設定」を参照してください。	Service Quality Settings ページから、次のタスクを実行できます。 • リモート IP Communications Service Monitor（Service Monitor）を Operations Manager に対して追加または削除する。 • MOS しきい値を設定する。 **（注）** Operations Manager が Service Monitor からのトラップを処理するようにするには、Service Monitor を Operations Manager に追加し、かつ Service Monitor を使用して Operations Manager をトラップ レシーバとして設定する必要があります。
System Status P.19-10 の「System Status Report の生成と説明」を参照してください。	System Status ページから、System Status Report を生成できます。
Logging P.19-14 の「ロギングを使用したデバッグのイネーブル化およびディセーブル化」を参照してください。	Logging ページから、ログ ファイルに書き込まれるメッセージのタイプ（および数量）を変更したり、デバッグをイネーブルまたはディセーブルにしたりできます。

表 19-1　Operations Manager の管理タスク（続き）

タスク	説明
System Preferences P.19-12 の「System Preferences を使用したシステム全体のパラメータの設定」を参照してください。	System Preferences ページから、次の情報を設定できます。 • SNMP トラップの受信：Operations Manager が SNMP トラップをリッスンするポートを変更します。 • SNMP トラップのフォワーディング：（オプション）パススルー トラップの受信側として、ホストおよびポート番号を設定します。 • デフォルトの SMTP サーバ：電子メール通知用のデフォルト サーバを変更または入力します。 • パージング スケジュール：日次のデータベース パージングの時刻を選択します。 • Common Services サーバ：次のような他の CiscoWorks 製品を実行するリモート サーバを入力します。 — Resource Manager Essentials（RME） — Campus Manager — CiscoView
Add Users P.19-20 の「ユーザの設定（ACS および非 ACS）」を参照してください。	Common Services の Local User Setup ウィンドウを開きます。

詳細については、さらに次のトピック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（P.19-4）
- パージング スケジューラのステータスの表示（P.19-13）

Operations Manager のタスクのスケジュール

Operations Manager を最初にインストールしたときには、デフォルトで、表 19-2 に示しているほとんどのタスクが同時に実行されないようにスケジュールされています。サイトの要件を満たすように、これらのタスクのスケジュールを設定できます。ただし、その場合でも、これらのタスクを同時に実行することは避ける必要があります。

表 19-2　スケジュールの考慮事項

スケジュールするタスク	デフォルトのスケジュール	コメントと注意事項
データベース パージング	毎日午前 0 時に実行する。	データベースのパージにかかる時間は、データベースのサイズによって異なります。
電話機のディスカバリ	毎日、00:00（午前 0 時）、04:00、08:00、12:00、16:00、および 20:00 に実行する。	IP Phone Discovery Schedule ページで最後の収集の開始時刻と終了時刻を比較して、最後の電話機ディスカバリが完了するまでにかかった時間を調べる必要があります。 P.15-25 の「IP 電話検出の使用」を参照してください。電話機ディスカバリが完了するまでに通常かかる時間を認識しておくと、スケジュールするときに役立ちます。
インベントリ収集	毎週月曜日の午前 2:00 に実行する。	デフォルトでは、インベントリ収集はデータベース パージングの 2 時間後に開始されます。

システム管理者は、Operations Manager でのスケジュール設定の他に、データベースのバックアップをスケジュールできます。表 19-2 に示しているタスクと同時に実行しないように、データベース バックアップ スケジュールを慎重に調整する必要があります。

スケジュールの詳細については、次のトピックを参照してください。

- パージング スケジューラのステータスの表示（P.19-13）
- Operations Manager データのバックアップと復元（P.19-25）

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、デバイス上で SNMP をイネーブルにして、次のいずれかを実行する必要があります。

- トラップを直接 Operations Manager に送信するよう SNMP を設定する。
- 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。

トラップを直接 Operations Manager に送信するには、P.19-4 の「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」のタスクを実行します。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、P.19-5 の「SNMP トラップの受信と他のトラップ デーモンまたは NMS との統合」の手順に従います。

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

（注）　デバイスが SNMP トラップを Network Management System（NMS; ネットワーク管理システム）またはトラップ デーモンに送信する場合は、P.19-5 の「SNMP トラップの受信と他のトラップ デーモンまたは NMS との統合」を参照してください。

Operations Manager は SNMP の MIB 変数とトラップを使用してデバイスの状態を調べるため、そ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。

デバイスに適切なコマンドライン 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。

- Cisco IOS ベースのデバイスが Operations Manager にトラップを送信できるようにするための設定（P.19-4）
- Catalyst デバイスが Operations Manager に SNMP トラップを送信できるようにするための設定（P.19-5）

Cisco IOS ベースのデバイスが Operations Manager にトラップを送信できるようにするための設定

Cisco IOS ソフトウェアを実行するデバイスの場合、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 リードオンリー（read-only）コミュニティ ストリングを示し、*[a.b.c.d]* は SNMP トラップの受信ホスト（Operations Manager サーバ）を示しています。

詳細については、適切なコマンド 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 & Services > Cisco IOS Software** を選択します。

ステップ 3　Cisco IOS ベースのデバイスによって使用されている Cisco IOS ソフトウェア リリースのバージョンを選択します。

ステップ 4　**Technical Documentation** を選択し、適切なコマンド リファレンス ガイドを選択します。

Catalyst デバイスが Operations Manager に SNMP トラップを送信できるようにするための設定

Catalyst ソフトウェアを実行するデバイスの場合、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 リードオンリー（read-only）コミュニティ ストリングを示し、[*a.b.c.d*] は SNMP トラップの受信ホスト（Operations Manager サーバ）を示しています。

詳細については、適切なコマンド 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 & Services > Cisco Switches** を選択します。

ステップ 3　適切な 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、適切なコマンド リファレンス ガイドを選択します。

SNMP トラップの受信と他のトラップ デーモンまたは NMS との統合

SNMP トラップの受信を他のトラップ デーモンおよび他のネットワーク管理システム（NMS）と統合するには、次の作業を 1 つ以上完了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のリストに追加する。P.19-4 の「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」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。

  別の NMS が標準 UDP トラップ ポート（162）上ですでにトラップをリッスンしている場合は、別のポート（ポート 9000 など）を使用するように Operations Manager を設定する必要があります。P.19-12 の「System Preferences を使用したシステム全体のパラメータの設定」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、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 19-3 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 19-3　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 が引き続きポート 162 でトラップを受信。 • 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。

Operations Manager が使用するポートとプロトコル

Operations Manager は、次のプロトコルを使用します。

- SNMP
- ICMP
- TCP/IP
- SMTP
- RMI
- HTTP

Operations Manager は、表 19-4 に示している TCP ポートと UDP ポートを使用します。

表 19-4　Operations Manager の着信ポート

ポート番号	使用状況
162	トラップを受信するために Operations Manager によって使用されるデフォルトのポート番号。
40000 ～ 41000	内部アプリケーション メッセージングのために Common Transport Mechanism によって使用される。
42344	Synthetic Testing Web サービスによって使用される。
42350 ～ 42353	メッセージング ソフトウェアによって使用される。
43441 ～ 43459	データベース ポートとして使用される。 • Operations Manager は、次のポートを使用します。 – 43445：Alert History データベース エンジンによって使用される。 – 43446：インベントリ サービス データベース エンジンによって使用される。 – 43447：イベント処理データベース エンジンによって使用される。 – 43449：IP Phone Information Facility データベース エンジンによって使用される。 – 43459：Service Monitor データベース エンジンによって使用される。
9002	IP テレフォニー サーバとデバイス障害サーバの両方をリッスンするためにブローカによって使用される。
9009	デバイス 障害サーバからのトラップを受信するために IP テレフォニー サーバによって使用されるデフォルトのポート番号。

Service Quality Settings の設定

Service Quality Settings では、Service Monitor を Operations Manager と統合できます。

（注）
- IP Communications Service Monitor（Service Monitor）は、個別にライセンスされる製品であり、Operations Manager のインストール時にインストールされます。ライセンスを取得する方法については、シスコの代理店にお問い合せください。
- Operations Manager と同じサーバ上で Service Monitor をライセンスできます。また、スタンドアロン バージョンの Service Monitor を取得し、他のサーバ上でインストールしてライセンスすることもできます。

Operations Manager が Service Monitor からのトラップを処理するようにするには、次の両方を実行する必要があります。

- トラップを Operations Manager に送信するよう Service Monitor を設定する（『*User Guide for IP Communication Service Monitor*』を参照してください）。
- 特定の Service Monitor からのトラップを処理するよう Operations Manager を設定する。P.19-7 の「Service Monitor の追加と削除」を参照してください。Operations Manager は、Operations Manager に追加されていない Service Monitor から受信したトラップをすべて廃棄します。

MOS が Service Monitor に設定されているしきい値を下回る場合、Service Monitor は Operations Manager に MOS 違反トラップを送信します。そのトラップに対応して、Operations Manager は警告アラートを生成します。MOS が Service Monitor によって定義されているレベルよりもさらに重大なレベルになったときに Operations Manager が重大なアラートを生成できるようにするには、Service Monitor に設定されている MOS しきい値よりも低い MOS しきい値を Operations Manager に設定します。P.19-9 の「Service Quality Event Settings の設定」を参照してください。

Service Monitor の追加と削除

Operations Manager によってトラップが処理される Service Monitor を指定するには、次の手順を使用します。この手順で、ローカルにインストールされている Service Monitor も、リモートにインストールされている Service Monitor も追加できます。

ステップ 1　**Administration > Service Quality Settings > Service Monitors** を選択します。Service Monitors ページが表示され、次の表の情報が示されます。

GUI 要素	処理 / 説明
チェックボックス カラム	オンにして Delete ボタンをクリックすると、Service Monitor が削除されます。 （注）Service Monitor を削除すると、Operations Manager はその Service Monitor から受信したトラップをすべて廃棄します。
IP Address カラム	Service Monitor がインストールされているサーバ。 （注）Operations Manager は、ここに示されている Service Monitor からのトラップだけを処理します。
Description カラム	ユーザによって入力された説明。

GUI 要素	処理 / 説明
Add ボタン	Service Monitor を追加する場合にクリックします。P.19-8 の「Operations Manager への Service Monitor の追加」を参照してください。
Configure ボタン	クリックすると、Service Monitor ホームページが開き、Service Monitor を設定できます。P.19-9 の「Service Monitor の設定」を参照してください。
Delete ボタン	クリックすると、選択した Service Monitor が削除されます。P.19-8 の「Operations Manager からの Service Monitor の削除」を参照してください。

Operations Manager への Service Monitor の追加

ローカルまたはリモートにインストールされている Service Monitor を Operations Manager に追加するには、次の手順を使用します。

ステップ 1　**Administration > Service Quality Settings > Service Monitors** を選択します。Service Monitor 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 Service Monitor ページが表示されます。

ステップ 3　次のフィールドにデータを入力します。

- IP Address：Service Monitor がインストールされているリモート サーバの IP アドレス。
- Remarks：オプション。

ステップ 4　**Add** をクリックします。Service Monitor ページが表示され、新しく追加した Service Monitor の情報が示されます。

Operations Manager からの Service Monitor の削除

ローカルまたはリモートにインストールされている Service Monitor を Operations Manager から削除するには、次の手順を使用します。

（注）　Operations Manager から Service Monitor を削除すると、Operations Manager はその Service Monitor から受信したトラップをすべて廃棄します。

ステップ 1　**Administration > Service Quality Settings > Service Monitors** を選択します。Service Monitor ページが表示されます。

ステップ 2　削除する Service Monitor のチェックボックスをオンにします。

ステップ 3　**Delete** をクリックします。確認のダイアログボックスが表示されます。

ステップ 4　**OK** をクリックします。

Service Monitor の設定

選択した Service Monitor の Service Monitor ホームページを起動するには、次の手順を使用します。

ステップ 1　**Administration > Service Quality Settings > Service Monitors** を選択します。Service Monitor ページが表示されます。

ステップ 2　Service Monitor を選択し、**Configure** をクリックします。Service Monitor ホームページが開きます。

（注）　ログインするように要求されることがあります。

ステップ 3　Service Monitor ホームページで **Help** をクリックし、Service Monitor を使用する方法の詳細を参照します。

Service Quality Event Settings の設定

（注）　Service Quality イベントは、Service Quality Alert 画面に表示されます。P.4-1 の「Service Quality Alerts の監視」を参照してください。

後述の手順を使用して、次の情報を設定します。

- CriticalServiceQualityIssue イベントをトリガーする MOS レベル。

  MOS が Service Monitor に設定されているしきい値を下回る場合、Service Monitor はトラップを送信します。Service Monitor に設定されている MOS しきい値よりも低い MOS しきい値を指定するイベント設定値を、Operations Manager に設定できます。Operations Manager は、MOS がそのイベント設定以下であるトラップを受信すると、CriticalServiceQualityIssue イベントを生成します。Operations Manager は、MOS がそのイベント設定を上回るトラップを受信すると、ServiceQualityIssue イベントを生成します。
- イベントが Service Quality Alert Detail 画面に表示されないように、イベントをクリアする頻度。
- 何分以内に何個のトラップを受信すると、MultipleServiceQualityIssue イベントをトリガーするか。

ステップ 1　**Administration > Service Quality Settings > Event Settings** を選択します。Service Quality Event Settings ページが表示されます。

ステップ 2　次のフィールドに値を入力します。

- **Mark the Service Quality Issue event critical when MOS drops below**：重大な Service Quality Issue イベントをトリガーする MOS スコアを入力します。デフォルトは 3.5 です（MOS 値の範囲は .1 ～ 4.9 です）。

（注）　この MOS スコアは、Service Monitor に設定されている MOS しきい値よりも低くなるようにしてください。

- **Generate a Multiple Service Quality Issues event when more than** [*a*] Service Quality Issue events occur in [*b*] minutes：次の数値を入力します。
  - [a]：Service Quality Issue イベントの数。
  - [b]：指定した数の Service Quality Issue イベントがこの時間（分）内に発生すると、Operations Manager によって Multiple Service Quality Issues イベントが生成されます。
- **Clear events after**：Service Quality イベントが何時間を超えると Operations Manager によってクリアされ、Service Quality Alerts ダッシュボードに表示されなくなるかを選択します。

（注）　イベントのクリア後 31 日間は、Service Quality Event History で引き続きそのイベントを表示できます。P.11-15 の「Service Quality Event History レポートを使用する前に」を参照してください。

ステップ 3　**Save** をクリックします。

System Status Report の生成と説明

System Status Report にアクセスするには、**Administration > System Status** を選択します。System Status Report が開きます。

System Status Report をナビゲートするには、次の項目を使用します。

- Go to フィールド：リストからレポートのセクションを選択します。どのセクションの末尾でも、Back to Top リンクをクリックできます。
- Summary：次のいずれかのリンクをクリックして、レポートのセクションを選択します。
  - Failed Processes
  - Inventory
  - Data Purging
  - Diagnostics: Synthetic Tests
  - Diagnostics: Phone Status Tests
  - Diagnostics: Node-to-Node Tests
  - Notifications
  - System Limits

（注）　Summary で View Details リンクをクリックして、レポートのセクションを選択することもできます。

System Status Report には、次のセクションが含まれています。

- **Failed Processes**：失敗したプロセスの名前。
- **Inventory**：次のタイプのデータ収集について、名前、最後の実行時刻、ステータス、および次にスケジュールされている時刻を表示します。
  - Discovery：新しいデバイスを識別し、DCR に追加します（オプション。スケジュールすることも、必要に応じて実行することもできます）。

  - DCR Domain Status：Operations Manager が（Isolated モードで動作するのではなく）デバイスおよびクレデンシャルを同期させるように設定されている場合、他の CiscoWorks サーバから DCR にデバイスを追加します。
  - Device Selection：（DCR に追加されたときに）自動的に、またはユーザが DCR から手動で選択したときに、デバイスを Operations Manager の監視対象に追加します。
  - Device Inventory Collection：Operations Manager の監視対象であるデバイスを調査して、デバイス コンポーネントとそのステータスをアップデートします。デバイスの検出は行いません。
  - Phone Inventory Collection：Operations Manager の監視対象であるすべてのスイッチおよび Cisco CallManager をチェックすることにより、ネットワーク内のすべての IP 電話に関する情報を検出および収集します。デバイスの検出は行いません。
- **Data Purging**：最新のデータベース パージング タスクの開始時刻、終了時刻、およびステータス。
- **Diagnostics: Synthetic Tests**：失敗したテストのテスト名、テスト タイプ、発信元（IP アドレスまたは DNS 名）、宛先（IP アドレスまたは DNS 名）、失敗した時刻、原因。
- **Diagnostics: Phone Status Tests**：失敗したテストのテスト名、発信元ルータ、内線番号、MAC アドレス、IP アドレス、失敗した時刻、原因。
- **Diagnostics: Node-to-Node Tests**：失敗したテストのテスト名、テスト タイプ、エンドポイント、失敗した時刻、原因。
- **Notifications**：デバイスのイベント説明、イベント ID、宛先、失敗した時刻、原因。
- **System Limits**：次のパラメータに対する現在の（Current）値、制限（Limit）値、および制限するもの。
  - Devices：Current：Operations Manager の監視対象インベントリ内のデバイス数。Limit：ライセンスによって許可されているデバイス数。
  - Phones：Current：Operations Manager の監視対象インベントリ内の電話機数。Limit：ライセンスによって許可されている電話機数。
  - IP Communications Service Monitor：ライセンスされているかどうか。
  - Synthetic Tests。
  - Phone Reachability Tests。
  - Node-to-Node Tests。
  - Devices monitored for performance and capacity。
  - Devices monitored for SRST。

System Preferences を使用したシステム全体のパラメータの設定

System Preferences ページから、次のすべてを設定できます。

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　次の表に示すデータを入力します。

GUI 要素	説明 / 処理
Trap Forwarding Parameters テーブル	（オプション）パススルー トラップの受信側を最大 3 つ入力します。 • Trap Server *n*（*n* は 1 ～ 3 の数値）：IP アドレスまたは DNS 名を入力します。 • Port：ホストがトラップを受信できるポート番号を入力します。 **（注）** デフォルトでは、Operations Manager はパススルー トラップを転送しません。 詳細については、次の付録および項を参照してください。 • 処理されるトラップ、パススルー トラップ、および識別されていないトラップとイベント（P.B-1） • SNMP トラップの受信とフォワーディングの設定（P.19-4）
CiscoWorks Servers テーブル	（オプション）各 CiscoWorks サーバ（RME、Campus、および CiscoView）に対して、次の操作を行います。 • Protocol：http（サーバ上で SSL がイネーブルである場合は https）を選択します。 • Server：IP アドレスまたは DNS 名を入力します。 • Port：サーバ上で CiscoWorks を起動するときに使用するポート番号を入力します。通常、プロトコルが http である場合のポート番号は 1741 で、プロトコルが https である場合のポート番号は 443 です。 **（注）** Operations Manager は、この情報を使用して、CiscoWorks 製品を起動します。
SNMP Trap Community フィールド	リード（read）コミュニティ ストリングを入力します。
Trap Receiving Port フィールド	Operations Manager が SNMP トラップをリッスンするポートを変更するには、ポートを入力します。デフォルトは 162 です。詳細については、P.19-4 の「SNMP トラップの受信とフォワーディングの設定」を参照してください。 **（注）** すでに使用されているポートのリストについては、P.19-6 の「Operations Manager が使用するポートとプロトコル」を参照してください。

GUI 要素	説明 / 処理
Default SMTP Server	電子メール通知を送信するときに使用する、Operations Manager の完全修飾 SMTP サーバ名を入力します。詳細については、P.14-1 の「通知の使用方法」を参照してください。 （注）　P.19-13 の「電子メール通知がブロックされていないことの確認」を参照してください。
Daily Purging Schedule	Alert History データベースのパージングを開始する時刻を選択します。 • Hour：0 ～ 23 • Minute：0 ～ 50（10 分間隔） デフォルトは 00:00 です。パージングすると、31 日分のデータがデータベースに保持されます。 （注）　P.19-3 の「Operations Manager のタスクのスケジュール」の情報を確認して、そこに示されている他のスケジュール済みジョブと日次パージングが競合しないようにしてください。

ステップ 3　**Apply** をクリックします。

電子メール通知がブロックされていないことの確認

デフォルト SMTP サーバ上にアンチウイルス アプリケーションが存在する場合は、ポートブロッキング ルールによって通知電子メールの送信が停止されていないことを確認します。アンチウイルス アプリケーションの中には、マスメーリング ワームをブロックするためにポートブロッキングを使用するものもあります。必要に応じて、ポートブロッキング ルールを削除します。

通知電子メールの詳細については、P.14-14 の「登録の設定」を参照してください。

パージング スケジューラのステータスの表示

毎日、Operations Manager データ パージ ジョブの実行後、Job Browser からそのジョブのステータスを確認できます。

（注）　System Status Report で日次パージングのステータスを確認することもできます。P.19-10 の「System Status Report の生成と説明」を参照してください。

ステップ 1　Operations Manager ホームページの右上隅にある **CiscoWorks** リンクをクリックして、CiscoWorks ホームページを起動します。

ステップ 2　CiscoWorks ホームページから、**Common Services > Server > Admin > Job Browser** を選択します。Job Browser ページが表示され、スケジュール済みジョブのテーブルが示されます。

ステップ 3　Type カラムで Operations Manager:DataPurge ジョブを探し、Status カラム内の情報を確認します。

（注）　Job Browser を使用して Operations Manager:DataPurge ジョブを削除すると、デーモン マネージャを再起動するか、サーバをリブートするか、日次パージング スケジュールを再設定するまで、パージングは再開されません。

ロギングを使用したデバッグのイネーブル化およびディセーブル化

Operations Manager は、すべての主要な機能モジュールのアプリケーション ログ ファイルを記述します。デフォルトでは、Operations Manager は、これらのログ ファイルにエラー メッセージと重大なメッセージだけを書き込みます。ロギングをディセーブルにすることはできません。ただし、次の作業を実行できます。

- 必要に応じて、ログレベルを上げ、さらに多くのデータを収集する。
- 標準としてのデフォルト ログレベルに戻す。

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

（注）　ロギングをディセーブルにすることはできません。Operations Manager は、必ず、エラー メッセージと重大なメッセージをアプリケーション ログ ファイルに書き込みます。

ステップ 2　各 Operations Manager 機能モジュールの Error チェックボックスは、常にオンになっています。これをオフにすることはできません。

すべてのモジュールを Error（デフォルトのログレベル）に設定するには、次の手順に従います。

a. **Default** ボタンをクリックします。確認のページが表示されます。

b. **OK** をクリックします。

個々のモジュールのログレベルを変更するには、次の手順に従います。

a. 変更するモジュールごとに、次のログレベルのいずれかを選択します（またはすべてを選択解除します）。

- Warning：エラー メッセージと警告メッセージをロギングします。
- Info：エラー メッセージ、警告メッセージ、および情報メッセージをロギングします。
- Debug：エラー メッセージ、警告メッセージ、情報メッセージ、およびデバッグ メッセージをロギングします。

（注）　モジュールのすべてのチェックボックスをオフにすると、そのモジュールが Error（デフォルトのログレベル）に戻ります。

b. 変更を確認します。変更をキャンセルするには、**Cancel** ボタンをクリックします。キャンセルしない場合は、**Apply** ボタンをクリックします。**Apply** ボタンをクリックすると、ただちに、Operations Manager の機能モジュールが、変更したログレベルに再設定されます。

システム アプリケーション MIB のログレベルを変更する方法については、P.19-32 の「システム アプリケーション MIB のログ ファイルの表示」を参照してください。

ログ ファイルへのアクセスと削除

各 Operations Manager モジュールは、<*NMSROOT*>\log\itemLogs フォルダ内の独自のフォルダにログ ファイルを書き込みます。表 19-5 は、各 Operations Manager モジュール、ログ ファイルが格納されるフォルダの名前、および関連ログ ファイルを示しています。

（注）　NMSROOT は、Operations Manager がインストールされているサーバ上のフォルダです。インストール時にデフォルト ディレクトリを選択した場合は C:\Program Files\CSCOpx になります。

ログ ファイルが、プリセットされている最大サイズに達すると、モジュールによってそのファイルがバックアップされ、新しいログ ファイルへの書き込みが開始されます。ログ ファイルの最大サイズは、モジュールによって異なります。モジュールが保持するバックアップ ログ ファイルの最大数も異なります。

（注）　Operations Manager は、DFMServer ログ ファイル（DFM.log）を自動的にリセットしません。良好なシステム パフォーマンスを保つために、このファイルが 30 MB を超えた場合はファイルをバックアップしてください。P.19-29 の「DFM ログ ファイルの保持」を参照してください。

デフォルトでは、Operations Manager はログ ファイルにエラー メッセージだけを書き込みます。ログレベルを変更することにより、ログ ファイルに格納される情報量に影響を及ぼすことができます。この方法については、P.19-14 の「ロギングを使用したデバッグのイネーブル化およびディセーブル化」を参照してください。

表 19-5　Operations Manager モジュール別のログ ファイル

機能 / モジュール	<*NMSROOT*> 内のフォルダ	ログ ファイル
Alert and Event History	\log\itemLogs\FH	FHUI.log FHCollector.log
Alerts and Events Display	\log\itemLogs\AAD	AAD.log
Application and Connectivity Poller	\log\itemLogs\VHM	VHMPoller.log TISPollerLogger.log
Detailed Device View	\log\itemLogs\DDV	DDV.log
Device Management	\log\itemLogs\tis	DCRAdapter.log DeviceManagement.log TISServer.log
Event Processing Adapters	\log\itemLogs\epa	adapterServer.log dfmEvents.log vhmEvents.log
Event Promulgation Module	\log\itemLogs\EPM	EPM.log

表 19-5　Operations Manager モジュール別のログ ファイル（続き）

機能 / モジュール	<*NMSROOT*> 内のフォルダ	ログ ファイル
Graphics Utility	\log\itemLogs\TGU	TGU.log TGU_DataProcessor.log
IP Phone Information Facility	\log\ipiu	ipiuapp.log
IP Phone Information Facility Server	\log	pif.log
IP Phone Status	\log\itemLogs\PR	PhoneReachability.log
IP Phone Status Display	\log\itemLogs\PAD	PAD.log
IP SLA Library	\log\itemLogs\IPSLA	STL.log
IPC Discovery	\log\itemLogs\discovery	discovery.log
IPT Health Report	log\itemLogs\ipthr	ipthr.log
Inventory Collection Schedule	\log\itemLogs\Rediscovery	Rediscovery.log
Inventory Collector	\log\itemLogs\vhm	connectivityProgress.log DFMCollector.log InventoryCollector.log Poller.log TISPollerLogger.log VHMGSUPoller.log VHMIntegrator.log
Inventory Interactor	\log\itemLogs\vhm	CiscoCallManagerOrClusterGrouping.log Interactor.log
Inventory Service	\log\itemLogs\tis	DCRAdapter.log TISServer.log
Node-to-Node Tests Common Utilities	\log\itemLogs\IPSLA	DAL.log plib.log
Node-to-Node Tests Data Poller	\log\itemLogs\IPSLA	WPUSS.log WPU_DataPoller.log
Node-to-Node Tests Device Management	\log\itemLogs\IPSLA	DMAudit.log WPUDM.log
Node-to-Node Tests Management	\log\itemLogs\IPSLA	SM.log SMAudit.log
Notification Services	\log\itemLogs\nots	nots.log notifications_audit.log notifications_failures.log notifications_success.log
PTM Adapter for Data Settings	\log\itemLogs\cfi	PollingThresholdAdapter.log
PTM Adapter for Voice Settings	\log\itemLogs\vhm	VHMPollingThresholdAdapter.log

表 19-5　Operations Manager モジュール別のログ ファイル（続き）

機能 / モジュール	<*NMSROOT*> 内のフォルダ	ログ ファイル
Polling and Threshold Manager	\log\itemLogs\PTM	PTMClient.log PTMDB.log PTMOGS.log PTMPTA.log PTMServer.log
Purging Scheduler	\log\itemLogs\DPS	DPS.log
SRST Monitoring	\log\itemLogs\srst	srst_audit.log srst_import_errors.log srst_test_creation_results.log srst_import.log srst_ui.log srst_server.log
Self Diagnostic Report	\log\itemLogs\sdr	sdr.log
Service Impact Reports Server	\log\itemLogs\sir	sir.log
Service Level View Server	\log\itemLogs\topo	Topology_Client.log Topology_Server.log
Service Quality Alerts Display	\log\itemLogs\QOVAD	QOVAD.log
Service Quality Manager	\log\itemLogs\QoVM	QoVMServer.log
Synthetic Testing Server	\log	STServer.log
Synthetic Testing UI	\log	ct-ui.log
View Manager	\log\itemLogs\VGM	vgm.log
View Severity Manager	\log\itemLogs\vsm	AlertInfo.log GroupHandler.log UserInfo.log vsmServer.log

（注）　Operations Manager アプリケーション ロギング サービスも、<*NMSROOT*>\log\itemLogs フォルダの下にログ ファイルを保持します。

セキュリティ上の考慮事項

次の各トピックでは、Operations Manager の重要なセキュリティ問題をいくつか説明します。

ファイルの所有権と保護

Operations Manager ファイルのセキュリティは、CiscoWorks と同じ標準に基づいています。

注意　ファイルまたはディレクトリに対して、その保護を緩めるような変更はしないでください。必要に応じて、保護をより厳しくすることができます。

すべての Operations Manager ファイルは、所有者 CASUSER でインストールされます。CASUSER だけが、*NMSROOT* にインストールされるファイルを作成、削除、または編集できます。*NMSROOT* は、CiscoWorks 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。インストール時にデフォルト ディレクトリを選択した場合は C:\Program Files\CSCOpx になります。

（注）　FAT パーティションにはファイル保護が適用されません。

SSL

Secure Socket Layer（SSL）は、プライバシー、認証、およびデータ整合性によってデータのセキュアなトランザクションを可能に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。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。デフォルトでは、Operations Manager で SSL がイネーブルになっていません。SSL をイネーブルにする方法については、Common Services のオンライン ヘルプを参照してください。

SNMPv3

CiscoWorks Common Services と同様に、Operations Manager は、機密情報の漏洩を防ぐために、サーバとデバイスの間で SNMPv3（認証とアクセス制御を行うが、データ暗号化は行わない）をサポートしています。これにより、パケットレベルのセキュリティ、完全性保護、およびリプレイ保護が実現されますが、パケットは暗号化されません。

Operations Manager データベースのパスワードの変更

始める前に

このトピックの手順では、次の Operations Manager データベースのパスワードを変更できます。

- itemEPM：イベント公表
- itemFH：Alert History
- itemInv：インベントリ
- itemIpiu：IP 電話情報
- qovr：IP Communications Service Monitor

ステップ 1　Operations Manager サーバのコマンド プロンプトで、次のコマンドを入力してデーモン マネージャを停止します。

```
net stop crmdmgmt
```

ステップ 2　*NMSROOT*\conf\itemDb\bin ディレクトリに移動します。次の例を参考にしてください。

```
cd Program Files\CSCOpx\conf\itemDb\bin
```

（注）　NMSROOT は、Operations Manager がインストールされているサーバ上のフォルダです。インストール時にデフォルト ディレクトリを選択した場合は C:\Program Files\CSCOpx になります。

ステップ 3　ChangeItemDbPasswd.pl と入力した後、新しいパスワードを指定します。次の例を参考にしてください。

```
ChangeItemDbPasswd.pl newpassword
```

ステップ 4　次のコマンドを入力してデーモン マネージャを再起動します。

```
net start crmdmgmt
```

デバイス サポート

Operations Manager で新しいデバイスのサポートが可能になると、Cisco.com の Operations Manager 用 planner ページで Incremental Device Updates（IDU）が公表されます。入手可能になった IDU の告知、ダウンロード、およびインストール手順については、planner ページを参照してください。

新しい IDU が入手可能になると、Cisco.com からその IDU をダウンロードできます。

システム管理タスクの実行

CiscoWorks を使用して、次のような多くのシステム管理タスクを実行できます。

CiscoWorks ホームページの起動

ステップ 1　Operations Manager ホームページの右上隅で、CiscoWorks リンクをクリックします。CiscoWorks ホームページが開きます。

ユーザの設定（ACS および非 ACS）

CiscoWorks サーバは、CiscoWorks アプリケーションのユーザを認証および認可するためのメカニズムを提供します。ユーザが何を表示して何を実行できるかは、ユーザ ロールによって決まります。システム管理者は、CiscoWorks ホームページから **Server > Security > Single-Server Management > Local User Setup** を選択することにより、ユーザ ロールを設定できます。ここから、ユーザを追加、編集、または削除できます。

CiscoWorks サーバは、CiscoWorks アプリケーションのユーザを認証するために、次の 2 つの異なるメカニズムつまり「モード」を提供します。

- CiscoWorks ローカル モード：デフォルトでは、CiscoWorks サーバは CiscoWorks ローカル モードつまり「非 ACS モード」を使用します。CiscoWorks ローカル モードでは、CiscoWorks がロールおよびそのロールに関連付けられている特権を割り当てます。これらは、Common Services Permission Report に表示されます（Permission Report を生成するには、Common Services ホームページから **Server > Reports > Permission Report** を選択し、**Help** をクリックします）。詳細については、P.19-21 の「CiscoWorks ローカル モードを使用したユーザの設定」を参照してください。
- CiscoSecure Access Control Server（ACS）モード：ACS が、ロールに関連付けられる特権を指定します。ACS では、デバイスベースのフィルタリングも実行できるため、表示を許可したデバイスだけをユーザに表示できます。ACS の使用（「ACS モード」と呼ばれる）は、ネットワークに ACS がインストールされており、Operations Manager が ACS に登録されている場合にサポートされます。詳細については、P.19-21 の「ACS モードを使用したユーザの設定」を参照してください。

Common Services が ACS モードを使用している場合は、Operations Manager も ACS モードを使用する必要があります。ACS モードを使用しないと、Operations Manager のユーザが何も権限を持たなくなります。ただし、別の Operations Manager インスタンスがすでに ACS と統合されている場合、新しい Operations Manager も ACS に統合されます。

CiscoWorks ローカル モードを使用したユーザの設定

CiscoWorks ローカル モードを使用して、ユーザを追加し、ユーザ ロールを指定するには、次の手順を使用します。

ステップ 1　**Administration > Add Users** を選択します。Common Services の Local User Setup ウィンドウが開きます。

ステップ 2　Local User Setup ウィンドウで Help ボタンをクリックし、設定手順の詳細を参照します。

各ユーザ ロールが Operations Manager のタスクにどのように関連付けられているかを理解するには、CiscoWorks Permission Report を使用します。Common Services ホームページから **Server > Reports > Permission Report > Generate Report** を選択し、IP Communications Operations Manager を見つけるまで下にスクロールします。

ACS モードを使用したユーザの設定

Operations Manager でこのモードを使用するには、ネットワークに Cisco Secure ACS がインストールされており、Operations Manager が ACS に登録されている必要があります。

ステップ 1　CiscoWorks サーバが使用しているモードを確認します。Common Services ホームページから **Server > Security > AAA Mode Setup** を選択し、ACS と Non-ACS のどちらの Type オプション ボタンが選択されているかを調べます。

ステップ 2　ACS サーバを調べて、Operations Manager が ACS に登録されているかどうかを確認します（ACS が選択されている場合）。

ステップ 3　ACS のロールを編集するには、次の作業を行います。

- ACS のオンライン ヘルプ（ACS サーバ上）を参照し、ロールを編集する方法を調べます。
- Common Services のオンライン ヘルプを参照し、DCR（特にロールの依存関係）に対する ACS の影響を調べます。

（注）　ACS を使用して Operations Manager のロールを編集すると、同じ ACS サーバに登録されている Common Services サーバを使用している他のすべての Operations Manager インスタンスにその変更が伝搬されます。

ACS モードでの Operations Manager の使用方法

ここで述べるタスクを実行する前に、Cisco Secure ACS に CiscoWorks サーバを正常に設定したことを確認する必要があります。CiscoWorks ログイン モジュールを ACS モードに設定した後で Operations Manager をインストールすると、Operations Manager のユーザには何も権限が付与されません。ただし、Operations Manager アプリケーションは Cisco Secure ACS に登録されます。

（注）　CiscoWorks サーバに定義されている System Identity Setup ユーザを Cisco Secure ACS に追加する必要があります。このユーザにはネットワーク管理者特権が必要です。

CiscoWorks ログイン モジュールを使用して、CiscoWorks サーバのネイティブ メカニズム（CiscoWorks Local ログイン モジュール）以外の認証ソースで新しいユーザを追加できます。この目的で、Cisco Secure ACS サービスを使用できます。

ACS モードの場合は、デフォルトで、CiscoWorks サーバの認証スキームに 5 つのロールがあります。ここでは、これらのロールを特権が小さなものから順に示します。

ヘルプ デスク	このロールのユーザは、固定的なデータからネットワーク ステータス情報にアクセスできます。デバイスと通信することも、ネットワークに到達するジョブをスケジュールすることもできません。 例：Service Level View の起動。
アプルーバ	このロールのユーザは、すべての Operations Manager タスクを承認できます。また、ヘルプ デスクのすべてのタスクを実行できます。 例：Alerts and Events の起動。
ネットワーク オペレータ	このロールのユーザは、ネットワークからのデータ収集に関連するすべてのタスクを実行できます。ネットワークに対する書き込みアクセス権は持ちません。また、アプルーバのすべてのタスクを実行できます。 例：模擬テストの追加。
ネットワーク管理者	このロールのユーザは、ネットワークを変更できます。また、ネットワーク オペレータのタスクを実行できます。 例：Service Level View のデフォルト ビューの設定。
システム管理者	このロールのユーザは、CiscoWorks のすべてのシステム管理タスクを実行できます。CiscoWorks ホームページから Permission Report を参照してください（**Common Services > Server > Reports > Permission Report**）。 例：LDAP の設定。

Cisco Secure ACS を使用して、これらのロールの特権を編集できます。カスタム ロールおよびカスタム特権を作成することで、独自のビジネス ワークフローやニーズに合せて Common Services クライアント アプリケーションをカスタマイズできます。

デフォルトの CiscoWorks 特権を編集する方法については、Cisco Secure ACS のオンライン ヘルプを参照してください（Cisco Secure ACS で、**Online Documentation > Shared Profile Components > Command Authorization Sets** をクリックします）。

Cisco Secure ACS での CiscoWorks のロールと特権の編集

別の Operations Manager インスタンスが同じ Cisco Secure ACS に登録されている場合、新しい Operations Manager インスタンスはそのロール設定を継承します。さらに、Operations Manager のロールに加えた変更は、Cisco Secure ACS によって他の Operations Manager インスタンスに伝搬されます。Operations Manager を再インストールすると、Operations Manager の再起動時に Cisco Secure ACS の設定が自動的に適用されます。

ステップ 1　**Shared Profile Components >** Operations Manager を選択し、編集する Operations Manager ロールをクリックします。

ステップ 2　独自のビジネス ワークフローやニーズに合せて任意の Operations Manager タスクを選択または選択解除します。

ステップ 3　**Submit** をクリックします。

デバイスベース フィルタリング

すべての Operations Manager 画面へのアクセスを制限するように ACS を設定できます。デバイスおよびアプリケーションへのアクセスを制限するように ACS を設定することもできます。デバイスベースおよびアプリケーションベースのフィルタリングは、次のものに影響を及ぼします。

- デバイス：デバイスに関する情報の表示、デバイスの設定、およびデバイスに関連する診断テストの設定を行うには、そのデバイスにアクセスできる必要があります。
- 電話機：電話機に関する情報を表示するには、その電話機に接続されているスイッチ、またはその電話機が登録されている Cisco CallManager にアクセスできる必要があります。

（注）　ACS は、VLAN に対するフィルタリングを実行しません。

（注）　デバイスベース フィルタリングは、Cisco CallManager クラスタ レベルで実行されません。すべてのユーザが、クラスタレベルのアラートおよび Alert History を表示できます。

デバイスベース フィルタリングは、次の Operations Manager 画面に対してだけ実行できます。

- **Monitoring Dashboards**：すべての画面
- **Diagnostics**：すべての画面
- **Device Management**：すべての画面

（注）　ユーザがインベントリ収集プロセスを起動すると、(そのユーザがアクセスできるデバイスだけでなく)Operations Manager によって管理されているすべてのデバイスが調査されます。

- **Notifications > Notification Criteria**

（注）　ACS でデバイス アクセスをアップデートしても、Operations Manager は実行中の通知をアップデートしません。

- **Reports**：
  - **Alert and Event History**：すべての画面
  - **Service Quality History**：すべての画面
- **Administration > Polling and Thresholds**

（注）　Polling Parameters Summary ページと Thresholds Parameters Summary ページだけがフィルタリングされます。

ほとんどの Operations Manager タスクはデバイス中心です。Operations Manager タスクの実行時に表示されるデバイスは、Cisco Secure ACS に定義されているロールおよび関連付けられている特権に基づきます。

（注）　ACS のカスタム ロールが DCR およびデバイスベース フィルタリングに及ぼす影響に関する重要な情報については、Common Services のオンライン ヘルプを参照してください。

自己署名セキュリティ証明書の年次作成

Operations Manager をインストールすると、Operations Manager によってサーバ上に自己署名セキュリティ証明書が作成されます。クライアント システムの中には、ユーザが証明書をインストールする必要があるものもあります。P.1-23 の「Security Alerts への応答」を参照してください。自己署名セキュリティ証明書は、作成日から 1 年で期限切れになります。

毎年、自己署名セキュリティ証明書が期限切れになる前に、新しい証明書を作成してください。証明書が期限切れになった後でも、新しい証明書を作成できます。ただし、次のタスクを完了するまで、ユーザが Operations Manager にアクセスできないことがあります。

ステップ 1　**Common Services > Server > Admin > Security Management > Create Self Signed Certificates** を選択します。Create Certificates ページが表示されます。

ステップ 2　次の表に示すフィールドに値を入力します。

フィールド	説明	使用方法
Country Name	国の名前	2 文字の国番号を使用します。
State or Province	州または地域の名前	2 文字の州コードまたは地域コード、あるいは州または地域の完全な名前を使用します。
Locality	市または町の名前	2 文字の市コードまたは町コード、あるいは市または町の完全な名前を使用します。
Organization Name	組織の名前	組織の完全な名前または省略形を使用します。
Organization Unit Name	組織内の部署の名前	部署の完全な名前または省略形を使用します。
Host Name	Operations Manager がインストールされているサーバの名前	サーバの DNS 名を使用します。 **（注）** 正しいドメイン名を使用してください。これは、Host Name フィールドにすでに表示されています。
Email Address	自分の電子メール アドレス	—

ステップ 3　**Submit** をクリックします。または、**Restore to Default** をクリックしてすべてのフィールドをクリアし、情報を再入力します。

Operations Manager データのバックアップと復元

ここでは、バックアップ アプリケーション（Back Up Data Now や Schedule Backup など）にアクセスする方法について説明します。また、オンライン ヘルプでデータの復元手順を見つける方法についても説明します。

ステップ 1　CiscoWorks ホームページから **Common Services > Server > Admin > Backup** を選択します。Backup Job ページが表示されます。

ステップ 2　Help ボタンをクリックし、データのバックアップ手順および復元手順に従います。

データベース ファイルは、表 19-6 に示しているバックアップ ディレクトリ構造を使用して格納されます。

- 形式：*/generation_number/suite/directory/filename*
- 例：/1/itemFh/database/itemFh.db

表 19-6　Operations Manager のバックアップ ディレクトリ構造

オプション	説明	使用方法
generationNumber	バックアップ番号	たとえば、1、2、3（3 が最新のデータベース バックアップ）。
suite	アプリケーション、機能、またはモジュール	バックアップを実行すると、すべてのスイートのデータがバックアップされます。CiscoWorks サーバ スイートは cmf です。Operations Manager アプリケーション スイートは、次のとおりです。 • dfm：IP インフラストラクチャ内のデバイスのデータ収集および分析 • itemEpm：イベント公表 • itemFh：Alert History • itemInv：デバイス インベントリ • itemIPIU：電話情報 • qovr：サービス品質 • vhm：音声対応デバイスのデータ収集および分析 • wpu：ノード間テスト
directory	何が格納されているか	一覧表示されている各アプリケーションまたはスイート。ディレクトリには、データベースおよび任意のスイート アプリケーションが含まれます。
filename	バックアップされたファイル	ファイルには、データベース（.db）、ログ（.log）、バージョン（DbVersion.txt）、マニフェスト（.txt）、tar（.tar）、およびデータ ファイル（datafiles.txt）が含まれます。

Operations Manager プロセスの起動と停止

（注） 実行中の従属プロセスを持つプロセスは、停止することも登録解除することもできません。まず、すべての従属プロセスを停止または登録解除してから、プロセスを停止または登録解除する必要があります。

ステップ 1　システム管理者として Operations Manager にログインし、CiscoWorks ホームページを起動します。

ステップ 2　**Common Services > Server > Admin > Processes** を選択します。Process Management ページが表示されます。

（注） プロセスが表示されない場合、そのプロセスはまだ起動されていません。

ステップ 3　次のどちらかを実行します。

- 実行しているプロセスの横にあるチェックボックスをオンにして、**Stop** をクリックします。
- 停止しているプロセスの横にあるチェックボックスをオンにして、**Start** をクリックします。

表 19-7 は、Operations Manager 関連の CiscoWorks プロセスの完全なリストを示しています。

表 19-7　Operations Manager 関連の CiscoWorks プロセス

名前	説明	依存関係
AdapterServer	イベント アダプタがバックエンド サーバからイベントを取得します。	なし
DataPurge	データベースおよびデータ ファイルのパージング。	jrm
DfmBroker	DFM Broker は、VHM および DFM のドメイン マネージャに関するレジストリを保守します。ドメイン マネージャは、その初期化が完了するときに、次の情報をブローカに登録します。 • ドメイン マネージャのアプリケーション名 • ドメイン マネージャが動作しているホスト名 • HTTP サーバがリッスンしている TCP ポート クライアントは、ドメイン マネージャにアクセスする必要がある場合、まずブローカに接続して、ホスト名、およびそのサーバの HTTP サービスがリッスンしている TCP ポートを調べます。次に、ブローカから接続解除し、ドメイン マネージャへの接続を確立します。	なし
DfmServer	インフラストラクチャ デバイス ドメイン マネージャ、つまり Operations Manager にバックエンド サービスを提供するプログラム。サービスには、SNMP データの取得やイベント分析が含まれます。DfmServer ログは *NMSROOT*/objects/smarts/logs/DFM.log です。詳細については、P.19-29 の「DFM ログ ファイルの保持」を参照してください。	DfmBroker
EPMDbEngine	Event Promulgation Module（EPM）データベース エンジン：EPM モジュールのリポジトリ。	なし
EPMDbMonitor	EPM データベース モニタ。	EPMDbEngine
EPMServer	通知サービスにイベントを送信します。	EPMDbEngine
FHDbEngine	Alert History データベース エンジン：アラートとイベントのリポジトリ。	なし
FHDbMonitor	Alert History データベース モニタ。	FHDbEngine
FHPurgeTask	Alert History パージ タスク。	なし
FHServer	Alert History サーバ。	FHDbMonitor、FHDbEngine、EPMDbEngine、EPMServer
GPF	パフォーマンスおよびキャパシティのモニタリング データの収集。	ITMOGSServer、INVDbEngine
GpfPurgeTask	パフォーマンス ポーリング レコードをパージします。	なし
INVDbEngine	デバイス インベントリ データベース エンジン。	なし
INVDbMonitor	デバイス インベントリ データベース モニタ。	INVDbEngine
InventoryCollector	電話インベントリ コレクタ。	EssMonitor
IPCDiscovery	物理デバイスのディスカバリ。	なし。
IPIUDataServer	IP 電話に関する情報を提供します。	ESS
IPIUDbEngine	電話インベントリ データベース エンジン。	なし
IPIUDbMonitor	電話インベントリ データベース モニタ。	IPIUDbEngine
IPSLAPurgeTask	ノード間テストのレコードをパージします。	なし

表 19-7　Operations Manager 関連の CiscoWorks プロセス（続き）

名前	説明	依存関係
IPSLAServer	ノード間テストのサーバ。	INVDbMonitor、InventoryCollector
ITMCTMStartup	内部通信プロセス。	なし
ITMDiagServer	診断サーバ。	INVDbEngine、ESS
ITMOGSServer	Operations Manager Object Grouping Service サーバが、グループ メンバシップを評価します。	CmfDbEngine、ESS、DCRServer
IVR	内部プロセス。	なし
NOTSServer	通知サーバがアラートを監視し、登録に基づいて通知を送信します。	EPMDbEngine、EPMServer、INVDbEngine、ITMOGSServer
PIFServer	電話機のディスカバリ、CDP 近隣探索、および電話到達可能性のモニタリングを実行します。	PIFDbEngine、ESS
PTMServer	ポーリングとしきい値のサーバ。	ITMOGSServer
QoVMServer	Service Monitor サーバ。	ESS
QOVR	Service Quality Alerts プロセス。	QOVRDbMonitor
QOVRDbEngine	Service Monitor データベース エンジン。	なし
QOVRDbMonitor	Service Monitor データベース モニタ。	QOVRDbEngine
QOVRMultiProcLogger	Service Monitor ロギング。	なし
SDRPurgeTask	自己診断レポートをパージします。	なし
SIRServer	Service Impact レポートを生成するための音声モデルおよびルールベース エンジン。	EPMDbEngine、ESS
SRSTServer	SRST テストを設定および実行します。	PIFServer、PMServer、ESS、TISServer
STServer	Cisco CallManager に対して定期的に模擬テストを実行し、Operations Manager にリアルタイムのステータス アップデートを提供します。	INVDbEngine、ESS
TISServer	インベントリ サーバ。	INVDbEngine、EssMonitor
TopoServer	Service Level View サーバ。	SIRServer、ITMOGSServer
VHMIntegrator	音声データとインフラストラクチャ データを統合します。	ESS
VHMServer	音声データを保持します。	DfmBroker
VsmServer	ビューを保持し、評価します。	ITMOGSServer

DFM ログ ファイルの保持

DFM.log ログ ファイルが 30 MB を超えると、Operations Manager にパフォーマンスの問題が生じる恐れがあります。そのような問題を避けるため、ログ ファイルをバックアップして、新しいログ ファイルを開始する必要があります。

ステップ 1　次のコマンドを入力して CiscoWorks デーモン マネージャを停止します。

```
net stop crmdmgtd
```

ステップ 2　DFM.log ファイルの名前を変更するか、または DFM.log ファイルを別の場所にコピーして Operations Manager サーバから削除します。DFM.log ファイルは、*NMSROOT*/objects/smarts/logs/ ディレクトリにあります。

（注）　NMSROOT は、Operations Manager がインストールされているサーバ上のフォルダです。インストール時にデフォルト ディレクトリを選択した場合は C:\Program Files\CSCOpx になります。

ステップ 3　ステップ 1 を完了してから 15 分待ち、次のコマンドを入力して CiscoWorks デーモン マネージャを再起動します。

```
net start crmdmgtd
```

新しい DFM.log ファイルが作成されます。

SNMP を使用した Operations Manager の監視

Operations Manager は、ホスト リソース MIB とシステム アプリケーション MIB をサポートしています。このサポートにより、サードパーティ製の SNMP 管理ツールを使用して Operations Manager を監視できます。したがって、次のことが可能になります。

- 複数のプラットフォーム（Operations Manager が存在する 1 つのプラットフォーム、および IP Telephony Environment Monitor（ITEM）スイートのアプリケーションが存在する 1 つまたは複数のプラットフォーム）を常に監視する。
- ホスト リソース MIB を使用して、完全なハードウェア情報およびオペレーティング システム情報にアクセスする。
- システム アプリケーション MIB を使用して、アプリケーションの状態にアクセスする。これにより、次の情報が提供されます。
  - Operations Manager によってインストールされたアプリケーション。
  - アプリケーションに関連付けられているプロセス、およびプロセスの現在のステータス。
  - 以前に実行したプロセス、およびアプリケーションの終了状態。

MIB 実装の詳細および MIB ウォークのサンプルについては、付録 H「Operations Manager による SNMP MIB サポート」を参照してください。

（注）　MIB サポートをアンインストールすることはできません。ただし、Windows SNMP サービスを停止して、スタートアップの種類を Manual または Disabled に設定できます。P.19-31 の「Windows SNMP サービスのイネーブル化とディセーブル化」を参照してください。

SNMP 照会用のシステムの設定

SNMP 照会をイネーブルにするには、SNMP サービスがインストールされてイネーブルである必要があります。

ステップ 1　Operations Manager がインストールされているサーバ上で、SNMP サービスがインストールされてイネーブルであることを確認します。P.19-30 の「Windows SNMP サービスのステータスの確認」を参照してください。

ステップ 2　SNMP サービスがインストールされていないことを確認した場合は、Windows SNMP サービスをインストールします。P.19-31 の「Windows SNMP サービスのインストールとアンインストール」を参照してください。

Windows SNMP サービスのステータスの確認

Windows SNMP サービスは、必要に応じて追加または削除できる Windows コンポーネントです。Operations Manager によってサポートされている MIB に対する SNMP 照会をイネーブルにするには、SNMP サービスがインストールされてイネーブルである必要があります。次の手順に従って、Windows SNMP サービスのステータスを確認できます。

ステップ 1　Windows 管理ツールの Services ウィンドウを開きます。

ステップ 2　次の点を確認します。

- Windows 管理ツールの Services ウィンドウに SNMP Service が表示される。その場合は、Windows SNMP サービスがインストールされています。

（注）　Windows SNMP サービスをインストールする方法については、P.19-31 の「Windows SNMP サービスのインストールとアンインストール」を参照してください。

- SNMP Service のスタートアップの種類が Automatic または Manual である。その場合は、Windows SNMP サービスがイネーブルになっています。

（注）　Windows SNMP サービスをイネーブルにする方法については、P.19-31 の「Windows SNMP サービスのイネーブル化とディセーブル化」を参照してください。

Windows SNMP サービスのインストールとアンインストール

Windows のオンライン ヘルプに、Windows SNMP サービスなどの Windows コンポーネントを追加および削除する手順が記載されています。その手順を見つけるには、Windows のオンライン ヘルプで Index タブを選択し、*installing SNMP service* などのキーワードまたはフレーズを入力します。

Windows SNMP サービスをアンインストールするには、Windows ヘルプを参照し、Windows コンポーネントを削除する手順に従います。

（注）　Operations Manager がインストールされているサーバから Windows SNMP サービスをアンインストールすると、ホスト リソース MIB およびシステム アプリケーション MIB のサポートも削除されます。サポートを再びインストールする場合は、P.19-30 の「SNMP 照会用のシステムの設定」を参照してください。

Windows SNMP サービスのイネーブル化とディセーブル化

Windows 管理ツールの Services を使用して、Windows SNMP サービスをイネーブルまたはディセーブルにできます。Services ウィンドウを開く方法については、Windows のオンライン ヘルプを参照してください。

ステップ 1　Services ウィンドウで SNMP Service を確認します。ステータスとスタートアップの種類が表示されています。

（注）　SNMP Service が表示されていない場合、Windows SNMP サービスはインストールされていません。P.19-31 の「Windows SNMP サービスのインストールとアンインストール」を参照してください。

ステップ 2　SNMP Service を右クリックして Properties を選択します。SNMP Service Properties ウィンドウが開きます。

- SNMP サービスをディセーブルにするには、Startup Type を Disable に設定し、**OK** をクリックします。
- SNMP サービスをイネーブルにするには、Startup Type を Automatic または Manual に設定し、**OK** をクリックします。

（注）　イネーブルにした後に SNMP サービスを開始するには、SNMP Service を右クリックし、Start を選択してください。

SNMP 照会用のセキュリティの設定

セキュリティを向上させるため、どのオブジェクト ID（OID）でも SNMP set 操作は許可されていません。また、SNMP サービスのクレデンシャルを編集して、デフォルトのコミュニティ ストリングやよく知られているコミュニティ ストリングを使用しないようにする必要があります。

（注）　SNMP サービスのクレデンシャルを編集するために SNMP サービスを再開する必要はありません。

Windows 管理ツールの Services を使用して、SNMP サービスのクレデンシャルを編集できます。

ステップ 1　Services ウィンドウで SNMP Service を確認します。

ステップ 2　SNMP Service を右クリックして Properties を選択します。SNMP Service 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　受け付けるコミュニティ名を編集し、**OK** をクリックします。

システム アプリケーション MIB のログ ファイルの表示

システム アプリケーション MIB のログ ファイル SysAppl.log は、Operations Manager がインストールされているサーバ上の *NMSROOT*/log にあります。

（注）　NMSROOT は、CiscoWorks 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。インストール時にデフォルト ディレクトリを選択した場合は C:\Program Files\CSCOpx になります。

Operations Manager サーバのホスト名の変更

Operations Manager サーバのホスト名を変更する場合は、いくつかのファイルをアップデートし、サーバをリブートし、自己署名セキュリティ証明書を再生成する必要があります。その後、ライセンスされている Service Monitor を保有している場合は、その設定をアップデートする必要があります。

（注）　この手順の間に、サーバを 2 回リブートします。また、一部の手順を実行するために、CiscoWorks デーモン マネージャおよび syslog マネージャを停止します。

ステップ 1　次の手順に従って、サーバのホスト名を変更します。

a. 次のコマンドを入力して CiscoWorks デーモン マネージャを停止します。

```
net stop crmdmgtd
```

b. **My Computer > Properties > Computer Name > Change** でホスト名を変更します。

c. リブート後にデーモン マネージャ サービスおよび syslog マネージャ サービスが再開されないようにします。Control Panel または Start から Services を開き、次の両方のサービスのスタートアップ モードを Manual に変更します。

- CW2000 Daemon Manager
- CWCS syslog サービス

d. サーバをリブートします。

ステップ 2　md.properties ファイル（*NMSROOT*\lib\classpath\md.properties）でホスト名を変更します。

（注）　NMSROOT は Operations Manager をインストールしたディレクトリです。デフォルトを選択した場合は C:\Program Files\CSCOpx になります。

ステップ 3　次のレジストリ エントリでホスト名を変更します。

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
- HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager

（注）　これらのレジストリ エントリの下で古いホスト名のインスタンスをすべて検索し、それらを新規ホスト名に置き換えてください。

ステップ 4　次の各ファイルでホスト名を変更します。

- regdaemon.xml（*NMSROOT*\MDC\etc\regdaemon.xml）
  - 古いホスト名を書き留めます。ステップ 5 で古いホスト名が必要になります。
  - 大文字で新しいホスト名を入力します。
- web.xml（*NMSROOT*\MDC\tomcat\webapps\classic\WEB-INF\web.xml）

ステップ 5　ファイル *NMSROOT*\conf\cmic\changehostname.info を作成します。このファイルには、次の形式で古いホスト名と新しいホスト名を大文字で入力します。

```
OLDHOSTNAME:NEWHOSTNAME
```

（注）　このファイル内のホスト名は大文字と小文字が区別されます。ホスト名は大文字で入力する必要があります。新しいホスト名は、regdaemon.xml に入力したホスト名と正確に一致する必要があります。

ステップ 6　次のディレクトリから gatekeeper.ior ファイルを削除します。

NMSROOT\www\classpath

ステップ 7　次の各ファイルで古いホスト名をすべて変更します。

- *NMSROOT*\objects\vhmsmarts\local\conf\runcmd_env.sh
- *NMSROOT*\conf\dfm\Broker.info

ステップ 8　cmf データベースのパスワードがわからない場合は、次の手順に従ってパスワードを再設定します。

a.　Command Prompt を開き、NMSROOT\bin に移動します。

b.　次のコマンドを入力します。

```
perl dbpasswd.pl dsn=cmf npwd=newpassword
```

ここで、newpassword は新しいパスワードです。

（注）　このパスワードを覚えておいてください。ステップ 9 でこのパスワードが必要になります。

ステップ 9　ホスト名の変更前に追加されたデバイスが Device Center で正しく分類されることを保証するために、次のコマンドを入力します。

```
dbisqlc -c
"uid=cmfDBA;pwd=dbpassword;eng=cmfEng;dsn=cmf;dbf=NMSROOT\databases\cmf\cmf.db" -q
update PIDM_app_device_map SET app_hostname=`NewhostName' where
app_hostname=`OldhostName'
```

それぞれの説明は次のとおりです。

- dbpassword は Common Services のデータベースのパスワードです。
- NMSROOT は Operations Manager をインストールしたディレクトリです。
- NewhostName は新しいホスト名です。
- OldhostName は古いホスト名です。

ステップ 10　Control Panel または Start から Services を開き、次の両方のサービスのスタートアップ モードを Automatic に変更します。

- CW2000 Daemon Manager
- CWCS syslog サービス

ステップ 11　サーバをリブートします。

ステップ 12　**Common Services > Server > Security > Certificate Setup** を選択し、自己署名セキュリティ証明書内の古いホスト名を新しいホスト名に置き換え、自己署名セキュリティ証明書を再生成します。

詳細については、Help をクリックしてください。

ステップ 13　Service Monitor のライセンスを持っている場合は、そのライセンスを再設定します。

a.　Service Monitor ホームページを開きます（P.19-9 の「Service Monitor の設定」を参照してください）。

b.　Help をクリックし、「*Reconfiguring Service Monitor after a Hostname Change*」というトピックに記載されている手順に従います。

（注）　Service Monitor のオンライン ヘルプには、次のタスクを実行するための詳細な手順が記載されています。

- 次の各コンフィギュレーション ファイルで IP アドレスまたはホスト名を変更する。
  - デフォルトのコンフィギュレーション ファイル
  - Service Monitor によって管理されている各 Cisco 1040 の特定のコンフィギュレーション ファイル
- アップデートしたコンフィギュレーション ファイルを Service Monitor サーバから TFTP サーバにコピーする。
- Cisco 1040 をリセットする。
- Operations Manager にトラップを送信するよう Service Monitor が設定されている場合：
  - Operations Manager が Service Monitor と同じサーバにインストールされている場合は、新しいホスト名または IP アドレスにトラップを送信するよう Service Monitor を設定する。
  - Operations Manager が別のサーバにインストールされている場合は、Operations Manager で Service Monitor を削除してから再び追加する。

Operations Manager サーバの IP アドレスの変更

ステップ 1　次のコマンドを入力して CiscoWorks デーモン マネージャを停止します。

```
net stop crmdmgtd
```

ステップ 2　次のディレクトリから gatekeeper.ior ファイルを削除します。

NMSROOT\www\classpath

（注）　NMSROOT は、Operations Manager がインストールされているサーバ上のフォルダです。インストール時にデフォルト ディレクトリを選択した場合は C:\Program Files\CSCOpx になります。

ステップ 3　Operations Manager サーバの IP アドレスを変更します。

ステップ 4　ステップ 1 を完了してから 15 分待ち、次のコマンドを入力して CiscoWorks デーモン マネージャを再起動します。

```
net start crmdmgtd
```