



## システム管理およびデータ管理

---

この項では、次のトピックについて説明します。

- [Service Monitor データベースの消去について \(P.6-2\)](#)
- [センサー アrchive ファイルの消去について \(P.6-4\)](#)
- [ログ ファイルの管理 \(P.6-5\)](#)
- [ユーザの設定 \(ACS および非 ACS\) \(P.6-7\)](#)
- [Service Monitor プロセスの起動および停止 \(P.6-10\)](#)
- [SNMP を使用した Service Monitor の監視方法 \(P.6-10\)](#)
- [Service Monitor サーバのホスト名の変更 \(P.6-14\)](#)
- [Service Monitor サーバの IP アドレスの変更 \(P.6-17\)](#)
- [Service Monitor サーバの時刻の変更 \(P.6-17\)](#)

## Service Monitor データベースの消去について

Cisco Unified Service Monitor (Service Monitor) は、次のソースからコール メトリックを受信して処理し、データベースに格納します。

- Service Monitor に登録されている Cisco 1040
- Service Monitor データベースへのアクセス、または Service Monitor へのデータ送信 (Service Monitor がアプリケーション ビリング サーバとして設定されている場合) ができるように設定されている、Cisco Unified CallManager クラスタ。詳細については、[P.B-1 の「Cisco Unified CallManager の設定」](#)を参照してください。

Service Monitor はデータを 30 日間保存し、古いデータをデータベースから消去するジョブを毎日実行します。Service Monitor データベース全体をバックアップおよび復元することができます。

### データベースのバックアップ

Service Monitor データベースの即時バックアップ、またはスケジュールされたバックアップを実行するには、次の手順を実行します。

- 
- ステップ 1** Service Monitor ホームページの右上にある CiscoWorks リンクをクリックします。新しいウィンドウが開きます。
- ステップ 2** Common Services ペインで、**Server > Admin > Backup** を選択し、**Help** をクリックしてその手順に従います。
- 

### データベースの復元

データベースを復元するには、コマンドライン インターフェイスを使用します (手順はオンラインヘルプで参照可能)。これには、バックアップ ディレクトリ構造 ([表 6-1](#) で説明) を把握しておくことが必要です。

データベース復元のオンライン ヘルプを検索するには、次の手順を実行します。

- 
- ステップ 1** Service Monitor ホームページの右上にある CiscoWorks リンクをクリックします。新しいウィンドウが開きます。
- ステップ 2** Common Services ペインで、**Server > Admin > Backup** を選択し、**Help** をクリックして Restoring Data トピックの **Help** リンクをクリックします。
- 



(注)

データベースを復元すると、ロギング設定がデフォルト値に戻ります。そのため、ログ ファイルに書き込まれるのはエラー メッセージだけになります。問題のデバッグのために、その他の情報もログ ファイルに書き込む必要がある場合は、ロギング設定を再設定します。[P.6-5 の「ログ ファイルの管理およびデバッグのイネーブル化とディセーブル化」](#)を参照してください。

---

Service Monitor データベースのバックアップディレクトリ構造には、次のスイート名 *qovr* が含まれます。

- フォーマット : `/generation_number/suite[/directory]/filename`
- 例 : `/1/qovr/qovr.db`

表 6-1 に、バックアップディレクトリ構造を示します。

表 6-1 Service Monitor 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、および3。3が最新のデータベースバックアップです。
suite	アプリケーション、関数、またはモジュール	バックアップを実行する場合、すべてのスイートのデータがバックアップされます。Service Monitor アプリケーションスイートは <i>qovr</i> です。
directory	保存場所	スイート アプリケーション (適用可能な場合)
filename	バックアップされる特定のファイル	ファイルにはデータベース (.db) が含まれます。  Service Monitor の場合、次のファイルが <code>generationNumber/suite</code> のすぐ下にリストされます。  <i>qovr.db</i>

## Service Monitor データベースのパスワードの変更

コマンドライン スクリプトを使用すると、データベースのパスワード (Service Monitor データベースのパスワード *qovr.db* を含む) を変更できます。手順はオンライン ヘルプで参照できます。

- 
- ステップ 1** Service Monitor ホームページの右上にある CiscoWorks リンクをクリックします。新しいウィンドウが開きます。
- ステップ 2** Help をクリックします。ヘルプ ウィンドウが開きます。
- ステップ 3** Index タブを選択し、D のエントリまでスクロール ダウンして、*database password changes* を選択します。
-

## センサー アーカイブ ファイルの消去について



(注)

このトピックは、センサーが設置されているシステムに適用されます。

オプションで、Service Monitor はコール メトリック データをサーバ上のディレクトリ内のファイルにアーカイブします。アーカイブをイネーブルおよびディセーブルにするには、P.4-5 の「[センサーのデフォルト設定の設定](#)」を参照してください。

アーカイブがイネーブルの場合（デフォルト）、Service Monitor は次を実行します。

- 毎日午前 0 時に新しいデータ ファイルを作成する。
- 現在のデータ ファイルのサイズが 3 MB を超えると、新しいデータ ファイルを作成する。データ ファイルがこのサイズに達すると、Service Monitor は次を実行します。
  - データ ファイルをバックアップする。ファイル形式の末尾に *.n* が追加されます。たとえば、.csv.1、.csv.2 のように、1 日最大 50 まで追加されます。
  - 新しいデータ ファイルを作成する。元のファイル形式 (.csv) が保持されます。
- データ ファイルを 30 日間保存した後、削除する。データ ファイルを 30 日以上保存する場合は、ファイル システムのバックアップと同じ方法で Service Monitor データ ファイルをバックアップできます (Common Services は Service Monitor データベースだけをバックアップします。Service Monitor データ ファイルは対象外です)。

## ログ ファイルの管理

この項では、次のトピックについて説明します。

- センサーの Syslog の処理について (P.6-5)
- センサーの履歴ログ ファイルの管理 (P.6-5)
- ログ ファイルの管理およびデバッグのイネーブル化とディセーブル化 (P.6-5)

### センサーの Syslog の処理について

Service Monitor は、Cisco 1040 から syslog メッセージを受信して処理します。Service Monitor は、syslog メッセージを処理したら、これらを syslog ファイル `syslog.log` (`NMSROOT\log\qovr` にある) に書き込みます。

### センサーの履歴ログ ファイルの管理

履歴ログ ファイルの `ServiceMonitorHistory.log` には、Cisco 1040 のリセット、設定のアップデート、エラーなどの Cisco 1040 イベントの記録が含まれます。履歴ログ ファイルは、記録が蓄積されるため、サイズが大きくなります。ファイルが過剰に大きくなった場合は、名前を変更して、Service Monitor が新しい履歴ログ ファイルの作成を開始できるようにします。



(注)

Service Monitor は、履歴ログ ファイルをバックアップしません。履歴ログ ファイルをバックアップする場合は、ファイルシステムをバックアップする場合と同じ方法を使用します。

### ログ ファイルの管理およびデバッグのイネーブル化とディセーブル化

次の情報はトラブルシューティング用に提供されます。Service Monitor ログ ファイル (表 6-2 を参照) は、`NMSROOT\log\qovr` ディレクトリにあります。



(注)

NMSROOT は、サーバ上の Service Monitor がインストールされているフォルダです。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` です。

次の手順で、ログ ファイルに書き込まれるメッセージのタイプ (および量) を増減できます。

- ステップ 1** Service Monitor ホームページで、**Logging** を選択します。Logging: Level Configuration ページが表示されます。



(注)

ロギングはディセーブルにできません。Service Monitor は常に、エラーおよび重大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** Service Monitor 機能モジュールごとの Error チェックボックスは常にオンで、これをオフにすることはできません。モジュールおよび関連ログ ファイルの一覧については、表 6-2 を参照してください。

すべてのモジュールを、デフォルトのロギングレベルである **Error** 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ギン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、次のロギングレベルのいずれかを選択（または、すべて選択解除）します。
  - **Warning** : エラーメッセージと警告メッセージをログに記録します。
  - **Informational** : エラー、警告、および情報メッセージをログに記録します。
  - **Debug** : エラー、警告、情報、およびデバッグメッセージをログに記録します。




(注) モジュールのチェックボックスをすべて選択解除すると、デフォルトのロギングレベルである **Error** に戻ります。

- b. 変更内容を確認します。変更内容をキャンセルするには、**Cancel** ボタンをクリックします。変更内容を適用する場合は、**Apply** ボタンをクリックします。**Apply** ボタンをクリックすると、Service Monitor 機能モジュールが変更されたロギングレベルに即座にリセットされます。

表6-2に、Service Monitor のログファイルを機能またはモジュール別に示します。Technical Assistance Center (TAC) にサポートを求めると、これらのログファイルのいくつかを送信するよう指示されることがあります。

表 6-2 モジュール別 Service Monitor ログファイル

機能 / モジュール	ログファイル
Data Handler	DataHandler.log DataHandler_stdout.log DataHandler_sterr.log dhError.log LicenseCheck.log ServiceMonitorHistory.log tftpmanager.log trapgen.log
Reports	CVTQReports.log SensorReports.log  (注) これらのファイルは NMSROOT\log\qovr\reports にあります。
Skinny Communication	SkinnyServer.log
User Interface	QovrUI.log

## ユーザの設定 (ACS および非 ACS)

Service Monitor ユーザが何を表示および実行できるかは、ユーザ ロールによって決まります。ユーザ認証には、次の 2 種類のメカニズム、つまりモードがあります。

- 非 ACS : 認証および認可を提供する、サポートされるログイン モジュールを選択します。Permission Report に説明されているとおり、Common Services はデフォルトで CiscoWorks Local ログイン モジュールを使用して、ロールとそれらのロールに関連付けられた特権を割り当てます (Permission Report を生成するには、Service Monitor ホームページの右上にある CiscoWorks リンクをクリックし、**Common Services > Server > Reports > Permission Report > Generate Report** を選択します)。詳細については、P.6-7 の「非 ACS モードを使用したユーザの設定 (CiscoWorks Local ログイン モジュール)」を参照してください。
- ACS : ACS モードでは、認証および認可は Cisco Secure Access Control Server (ACS) によって提供されます。Cisco Secure ACS は、ロールに関連付けられた特権を指定します。ただし、デバイススペースのフィルタリングも実行可能となるため、ユーザには認可されたデバイスだけが表示されます。ACS モードを使用するには、Cisco Secure ACS がネットワークにインストールされ、Service Monitor が Cisco Secure ACS に登録されている必要があります。詳細については、P.6-7 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。

Operations Manager が認証および認可に ACS モードを使用し、Service Monitor が同一システム上で稼働している場合は、Service Monitor も ACS モードを使用する必要があります。ACS モードを使用していない場合、Service Monitor ユーザにはアクセス権が一切付与されません。

### 非 ACS モードを使用したユーザの設定 (CiscoWorks Local ログイン モジュール)

ユーザを追加し、CiscoWorks Local ログイン モジュールを使用してユーザ ロールを指定するには、**Administration > Add Users** を選択します。Common Services Local User Setup ウィンドウが開いたら、Help ボタンをクリックして設定手順に関する情報を表示します。

各ユーザ ロールと Service Monitor のタスクとの関係を理解するには、Permission Report を使用します。

- 
- ステップ 1** Service Monitor ホームページの右上にある CiscoWorks リンクをクリックします。新しいウィンドウが開きます。
  - ステップ 2** **Common Services > Server > Reports > Permission Report > Generate Report** を選択します。
  - ステップ 3** Cisco Unified Service Monitor が見つかるまでスクロール ダウンします。
- 

### ACS モードを使用したユーザの設定

認証および認可に ACS モードを使用するには、Cisco Secure ACS がネットワークにインストールされ、Service Monitor が Cisco Secure ACS に登録されている必要があります。

- 
- ステップ 1** 次の手順で、認証、認可、アカウントティング (AAA) モードを確認します。
    - a. Service Monitor ホームページの右上にある CiscoWorks リンクをクリックします。新しいウィンドウが表示されます。
    - b. **Server > Security > AAA Mode Setup** を選択し、ACS または非 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確認します。



(注) ACS モードを選択している場合は、Register all installed applications with ACS チェックボックスを選択してください。こうすると、Service Monitor タスクが必ず Cisco Secure ACS サーバにエクスポートされます。

**ステップ 2** Cisco Secure ACS にログインして、Service Monitor が Cisco Secure 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 ロールの変更の詳細については、Cisco Secure ACS のオンラインヘルプ (Cisco Secure ACS サーバ上) を参照してください。



(注) Cisco Secure ACS を使用して Service Monitor ロールを変更すると、同じ Cisco Secure ACS サーバに登録されている Service Monitor のその他のすべてのインスタンスに変更内容が伝播されます。

## ACS モードでの Service Monitor の使用方法

ここで説明するタスクを実行する前に、Service Monitor で Cisco Secure ACS が正常に設定されていることを確認しておく必要があります。CiscoWorks ログインモジュールを ACS モードに設定した後に Service Monitor をインストールした場合、Service Monitor ユーザにはアクセス権が付与されません。ただし、Service Monitor アプリケーションは Cisco Secure ACS に登録されます。



(注) Service Monitor のインストール時に定義されたシステムアイデンティティセットアップユーザが Cisco Secure ACS に追加されて、ネットワーク管理者特権を持っている必要があります。詳細については、Service Monitor ホームページの右上にある CiscoWorks リンクをクリックし、**Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup** を選択します。

CiscoWorks ログインモジュールを使用すると、ネイティブメカニズム (CiscoWorks Local ログインモジュール) 以外の認証ソースによって新しいユーザを追加できます。この目的で、Cisco Secure ACS サーバを使用できます。

デフォルトでは、ACS モードの CiscoWorks Local ログインモジュール認証方式には 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には、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する特権があります。デバイスとやり取りしたり、ネットワークに到達するジョブをスケジュールしたりする特権はありません。  例: Cisco 1040、セットアップ、およびデフォルト設定の詳細表示 (変更は実行できません)。
アプルーバ	このロールのユーザは、一切特権を持っていません (Service Monitor は、このユーザロールに一切タスクを割り当てません)。



ネットワーク オペレータ	このロールのユーザには、ネットワークからのデータ収集に関連したすべてのタスクを実行する特権があります。ネットワークへの書き込みアクセス権はありません。  例: Service Monitor のセットアップ、Cisco 1040 の追加、変更、削除。
ネットワーク管理者	このロールのユーザには、ネットワークを変更する特権があります。また、ネットワーク オペレータ タスクも実行できます。  例: ネットワーク オペレータと同じ。
システム管理者	このロールのユーザには、すべてのシステム管理タスクを実行する特権があります。Permission Report を参照してください (Service Monitor ホームページの右上にある CiscoWorks リンクをクリックし、 <b>Common Services &gt; Server &gt; Reports &gt; Permission Report &gt; Generate Report</b> を選択します)。  例: デバッグのイネーブル化およびディセーブル化、ロギングレベルの設定。

Cisco Secure ACS を使用すると、特権をこれらのロールに変更できます。また、Service Monitor をビジネス ワークフローやニーズに最適化するために有効なカスタム ロールや特権を作成することもできます。デフォルトの特権の変更については、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 でのロールおよび特権の変更

Service Monitor の別のインスタンスが同じ Cisco Secure ACS に登録されている場合、Service Monitor のインスタンスはこれらのロール設定を継承します。さらに、Service Monitor ロールに加えた変更は、Cisco Secure ACS を通じて Service Monitor のその他のインスタンスに伝播されます。Service Monitor を再インストールすると、Cisco Secure ACS 設定が Service Monitor の再起動時に自動的に適用されます。

- 
- ステップ 1** **Shared Profile Components > Cisco Unified Service Monitor** を選択して、変更する Service Monitor ロールをクリックします。
  - ステップ 2** ビジネス ワークフローおよびニーズに適した Service Monitor 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。
-

## Service Monitor プロセスの起動および停止

Service Monitor プロセスを開始および停止するには、Service Monitor ホームページの右上にある CiscoWorks リンクをクリックし、**Common Services > Server > Admin > Processes** を選択し、**Help** をクリックして手順を参照します。表 6-3 に、Service Monitor 関連のプロセスの一覧を示します。

表 6-3 Service Monitor 関連のプロセス

名前	説明	依存関係
QOVR	Service Monitor サーバ	QOVRDbMonitor
QOVRDbMonitor	Service Monitor データベース モニタ	QOVRDbEngine
QOVRDbEngine	Service Monitor データベース	—
QOVRMultiProcLogger	Service Monitor プロセス ロギング	—
SSHD	Service Monitor SFTP サーバ	—

## SNMP を使用した Service Monitor の監視方法

Service Monitor は、システム アプリケーション MIB をサポートします。このサポートにより、サードパーティの SNMP 管理ツールを使用して Service Monitor を監視できます。したがって、次のことを実行できます。

- 複数のプラットフォームの一貫した監視 : Service Monitor が常駐する 1 つのプラットフォーム、およびシスコ ユニファイド管理スイートのアプリケーションが常駐する 1 つ以上のプラットフォーム
- システム アプリケーション MIB を使用したアプリケーション ヘルスの評価。次の情報が提供されます。
  - Service Monitor 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たプロセスと現在のプロセス ステータス
  - 以前に実行されたプロセスおよびアプリケーションの終了状態

MIB 実装の詳細と MIB ウォークのサンプルについては、P.E-1 の「[Service Monitor の SNMP MIB サポート](#)」を参照してください。



(注)

MIB サポートはアンインストールできません。ただし、Windows SNMP サービスを停止して、起動タイプを Manual または Disabled に設定できます。P.6-12 の「[Windows SNMP サービス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。

## システムを SNMP クエリー対応に設定

SNMP クエリーをイネーブルにするには、SNMP サービスをインストールして、イネーブルにする必要があります。

- 
- ステップ 1** Service Monitor がインストールされているサーバに SNMP サービスがインストールされ、イネーブルになっていることを確認します。P.6-11 の「[Windows SNMP サービスのステータスの判別](#)」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と判断された場合は、Windows SNMP サービスをインストールします。P.6-12 の「[Windows SNMP サービスのインストールおよびアンインストール](#)」を参照してください。
- 

### Windows SNMP サービスのステータスの判別

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。Service Monitor がサポートする MIB に対して SNMP クエリーをイネーブルにするには、SNMP サービスをインストールし、イネーブルにする必要があります。Windows SNMP サービスのステータスを確認するには、次の手順に従います。

---

**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** 次を確認します。

- SNMP サービスが Windows 管理ツールの Services ウィンドウに表示されているかどうか。表示されている場合は、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には、P.6-12 の「[Windows SNMP サービスのインストールおよびアンインストール](#)」を参照してください。

---

- SNMP サービスの起動タイプが Automatic か Manual であるかどうか。Automatic の場合、Windows SNMP サービスはイネーブルです。



---

(注) Windows SNMP サービスをイネーブルにするには、P.6-12 の「[Windows SNMP サービス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。

---

## Windows SNMP サービスのインストールおよびアンインストール

Windows 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。手順を検索するには、Windows オンライン ヘルプの Index タブを選択し、「installing SNMP service」などのキーワードまたは句を入力します。

Windows SNMP サービスをアンインストールするには、Windows コンポーネントの削除に関する Windows ヘルプの指示に従います。

## Windows SNMP サービスのイネーブル化およびディセーブル化

Windows SNMP サービスをイネーブルまたはディセーブルにするには、Windows 管理ツールの Services を使用します。Services ウィンドウを開く手順については、Windows 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 サービスを見つけます。ステータスと起動タイプが表示されます。



**(注)** SNMP サービス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.6-12 の「Windows SNMP サービスのインストールおよびアンインストール」を参照してください。

**ステップ 2** SNMP サービスを右クリックして、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 に設定して、**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 に設定して、**OK** をクリックします。



**(注)** SNMP サービスをイネーブルにした後で起動するには、SNMP サービスを右クリックして Start を選択します。

## セキュリティを SNMP クエリー対応に設定

セキュリティを強化するには、SNMP set 操作をすべてのオブジェクト ID (OID) で拒否します。また、デフォルトまたは既知のコミュニティ ストリングを使用しないように SNMP サービスの資格情報を変更する必要があります。



**(注)** この目的で資格情報を変更するために、SNMP サービスを再起動する必要はありません。

SNMP サービスの資格情報は、Windows 管理ツールの Services を使用して変更できます。

- 
- ステップ 1 Services ウィンドウで SNMP サービスを見つけます。
  - ステップ 2 SNMP サービスを右クリックして、Properties を選択します。SNMP Service Properties ウィンドウが表示されます。
  - ステップ 3 Security タブを選択します。
  - ステップ 4 受け入れたコミュニティ名を編集して、OK をクリックします。
- 

## システム アプリケーション MIB ログ ファイルの表示

システム アプリケーション MIB ログ ファイルの SysAppl.log は、Service Monitor がインストールされているサーバの *NMSROOT*\log にあります。



---

(注) NMSROOT は、システム上の Service Monitor がインストールされているディレクトリです。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 です。

---

## Service Monitor サーバのホスト名の変更

Service Monitor サーバのホスト名を変更するには、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て、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、Service Monitor 上のコンフィギュレーションをアップデートする必要があります。

### ホスト名の変更、サーバのリブート、および証明書の再生成



(注)

この手順の間にサーバを 2 回リブートします。いくつかの手順を実行するため、デーモン マネージャも停止します。

**ステップ 1** 次のように、サーバ上のホスト名を変更します。

- a. 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 crmdmgtd
```

- b. **My Computer > Properties > Computer Name > Change** を選択し、ホスト名を変更します。
- c. リブート後、デーモン マネージャ サービスが再開しないように設定します。Control Panel または Start から Services ウィンドウを開いて、CW2000 デーモン マネージャ サービスの起動モードを Manual に変更します。
- 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) 内のホスト名を変更します。



(注)

*NMSROOT* は、Service Monitor をインストールしたディレクトリです。デフォルト ディレクトリを選択した場合は、C:\Program Files\CSCOpX です。

**ステップ 3** 次のレジストリ エントリの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 エントリの下で旧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ます。

**ステップ 4** 次のファイル内のホスト名を変更します。

- regdaemon.xml (*NMSROOT*\MDC\etc\regdaemon.xml):
  - 旧ホスト名をメモします。ステップ 5 を完了するために必要です。
  - 新規ホスト名は大文字で入力します。
- 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、旧ホスト名と新規ホスト名が大文字で次の形式に含まれます。

`OLDHOSTNAME:NEWHOSTNAME`



(注) このファイル内のホスト名は大文字小文字を区別します。大文字で入力する必要があります。新規ホスト名は、`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** サーバに Service Monitor だけがインストールされている場合は、[ステップ 8](#) に進みます。Service Monitor が Operations Manager と同じサーバにインストールされている場合は、次のファイルに出現するすべての旧ホスト名を変更します。

- `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不明の場合は、次のようにパスワードをリセットします。

- コマンドプロンプトを開いて、`NMSROOT\bin` に移動します。
- 次のコマンドを入力します。

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

ここで、`newpassword` は新規パスワードです。



(注) このパスワードを覚えておいてください。[ステップ 9](#) を完了するために必要です。

- ステップ 9** ホスト名を変更する前に追加されたデバイスが Device Center で適切に分類されていることを確認するため、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 のデータベースパスワードです。
- `NMSROOT` は、Service Monitor をインストールしたディレクトリです。
- `NewhostName` は、新規ホスト名です。
- `OldhostName` は、旧ホスト名です。

- ステップ 10** Control Panel または Start から Services ウィンドウを開いて、CW2000 デーモンマネージャ サービスの起動モードを Automatic に変更します。

**ステップ 11** サーバをリブートします。

**ステップ 12** 自己署名セキュリティ証明書内の旧ホスト名を新規ホスト名に置き換え、証明書を再生成します。

- a. **Common Services > Server > Security > Certificate Setup** を選択します。
- b. 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 を再設定します。P.6-16 の「[ホスト名を変更後の Service Monitor の再設定](#)」を参照してください。

---

## ホスト名を変更後の Service Monitor の再設定

P.6-14 の「[ホスト名の変更、サーバのリブート、および証明書の再生成](#)」の手順を完了後、次の手順を完了する必要があります。

**ステップ 1** Operations Manager にトラップを送信するように Service Monitor が設定されている場合は、次を実行します。

- 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、新規ホスト名または IP アドレスにトラップを送信するように Service Monitor をセットアップします。P.4-5 の「[センサーのデフォルト設定の設定](#)」を参照してください。
- 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 上で Service Monitor を削除して再度追加します。詳細については、Operations Manager のオンラインヘルプを参照してください。

**ステップ 2** システムで Cisco 1040 センサーを使用している場合は、次の手順を実行します。

- a. 次の各コンフィギュレーションファイル内の IP アドレスまたはホスト名を変更します。
  - デフォルトのコンフィギュレーションファイル：P.4-5 の「[センサーのデフォルト設定の設定](#)」を参照してください。
  - Service Monitor によって管理される各 Cisco 1040 固有のコンフィギュレーションファイル：P.4-10 の「[特定のセンサーのコンフィギュレーションファイルの編集](#)」を参照してください。
- b. Cisco 1040 をリセットします。P.4-12 の「[センサーのリセット](#)」を参照してください。

**ステップ 3** Service Monitor で Cisco Unified CallManager バージョン 5.x を監視している場合、アプリケーションビルディングサーバとして設定されている Service Monitor の IP アドレスをアップデートします。詳細については、P.B-4 の「[ビルディングサーバとしての Service Monitor の Cisco Unified CallManager 5.x への追加](#)」を参照してください。

---



## Service Monitor 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、サーバ上の Service Monitor がインストールされているフォルダです。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 です。

**ステップ 3** Service Monitor 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 を実行してから 15 分経過したら、次のコマンドを入力して、デーモン マネージャを再開します。

```
net start crmdmgtd
```

**ステップ 5** Service Monitor を再設定します。P.6-16 の「[ホスト名を変更後の Service Monitor の再設定](#)」を参照してください。

## Service Monitor サーバの時刻の変更

Service Monitor がインストールされているサーバの時刻を変更したら、次の手順でデーモン マネージャを停止および起動します。

**ステップ 1** コマンドラインから次のコマンドを実行します。

```
Net stop crmdmgtd  
Net start crmdmgtd
```

