Cisco Unified Service Monitor ユーザ ガイド

シスコ ユニファイド コミュニケーション管理スイート

Text Part Number: OL-10405-01-J

CONTENTS

このマニュアルについて

このマニュアルでは、Cisco Unified Service Monitor（Service Monitor）について説明し、これを使用および管理する方法を示します。

対象読者

このマニュアルは、次の方を対象としています。

- IP コミュニケーションおよび IP テレフォニーの管理担当者
- 組織のサービス レベル全体を監視する管理担当者
- IP ネットワーク インフラストラクチャの評価と設計を担当するネットワーク エンジニア

表記法

このマニュアルは、次の表記法を使用しています。

項目	表記法
コマンドおよびキーワード	太字
ユーザが値を指定する変数	イタリック体
セッション情報およびシステム情報の表示出力	`screen` フォント
ユーザが入力する情報	太字の **`screen`** フォント
ユーザが入力する変数	イタリック体の *`screen`* フォント
メニュー項目およびボタン名	太字
本文中のメニュー項目の選択	**Option>Network Preferences**
表中のメニュー項目の選択	Option>Network Preferences

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 **「危険」の意味です。人身事故を予防するための注意事項が記述されています。**

製品マニュアル

(注) 初版の印刷物および電子マニュアルは、製品に同梱されています。初版発行後の変更は Cisco.com に反映され、ここでマニュアルの最新版を確認できます。

表 1 に、ご利用可能な製品マニュアルを示します。

表 1　製品マニュアル

マニュアル タイトル	ご利用形式
Release Notes for Cisco Unified Service Monitor Release 2.0	• PDF が製品 CD に収録されています。 • Cisco.com で入手可能です。 http://cisco.com/en/US/products/ps6536/prod_release_notes_list.html
Quick Start Guide for Cisco Unified Service Monitor 2.0	• 印刷マニュアルが製品に同梱されています。 • PDF が製品 CD に収録されています。 • Cisco.com で入手可能です。 http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html
User Guide for Cisco Unified Service Monitor	• PDF が製品 CD に収録されています。 • Cisco.com で入手可能です。 http://cisco.com/en/US/products/ps6536/products_user_guide_list.html
文脈依存オンライン ヘルプ	ウィンドウの右上隅にある Help リンクまたはダイアログボックスの Help ボタンをクリックします。

関連マニュアル

（注） 初版の印刷物および電子マニュアルは、製品に同梱されています。初版発行後の変更は Cisco.com に反映され、ここでマニュアルの最新版を確認できます。

表 2 に、ご利用可能な関連マニュアルを示します。

表 2　関連マニュアル

マニュアル タイトル	ご利用形式
Quick Start Guide for Cisco 1040 Sensor	Cisco.com で入手可能です。 http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html
Release Notes for Cisco Unified Operations Manager 2.0	次の URL の Cisco.com で入手可能です。 http://cisco.com/en/US/products/ps6535/prod_release_notes_list.html
Quick Start Guide for Cisco Unified Operations Manager 2.0	次の URL の Cisco.com で入手可能です。 http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html
Installation Guide for Cisco Unified Operations Manager	次の URL の Cisco.com で入手可能です。 http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html
User Guide for Cisco Unified Operations Manager	次の URL の Cisco.com で入手可能です。 http://cisco.com/en/US/products/ps6535/products_user_guide_list.html
Release Notes for CiscoWorks Common Services 3.0.3 (Includes CiscoView 6.1.2) on Windows	次の URL の Cisco.com で入手可能です。 http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_note09186a00805af53a.html
Readme for Common Services 3.0.4 on Windows	次の URL の Cisco.com で入手可能です。 http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/prod_installation_guide09186a00805f7d64.html
Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Windows	• 次の URL の Cisco.com で入手可能です。 http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/products_installation_guide_book09186a00805305cb.html • 印刷マニュアルを注文します（Part Number DOC-7817184=）。[1]
User Guide for CiscoWorks Common Services 3.0.3	• 次の URL の Cisco.com で入手可能です。 http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a008053eabf.html • 印刷マニュアルを注文します（Part Number DOC-7817182=）。[1]

1. P.xiii の「技術情報の入手方法」を参照してください。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。ここでは、シスコが提供する製品マニュアル リソースについて説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納したライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関するマニュアルにアクセスすることができます。また、この DVD を使用すると、次の URL のシスコの Web サイトに掲載されている HTML マニュアルおよび PDF ファイルにアクセスすることができます。

http://www.cisco.com/univercd/home/home.htm

Product Documentation DVD は、定期的に作成およびリリースされています。DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store から Product Documentation DVD（Product Number DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/docstore

マニュアルの発注方法（英語版）

Cisco Marketplace にアクセスするには、Cisco.com の登録ユーザとなる必要があります。登録ユーザの場合、Product Documentation Store からシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/docstore

ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードに登録してください。PSIRT RSS フィードへの登録方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または GnuPG などの互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 9.*x* と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

PGP を持っていない、または使用していない場合は、機密情報を送信する前に PSIRT に問い合せ、他のデータ暗号化方法を確認してください。

Product Alerts および Field Notices

シスコ製品に対する変更やアップデートは、Cisco Product Alerts および Cisco Field Notices で通知されます。Cisco.com のプロダクト アラート ツールを使用すると、これらの通知を受け取ることができます。このツールを使用すれば、プロファイルを作成して、情報を受け取る製品を選択できます。

プロダクト アラート ツールにアクセスするには、Cisco.com の登録ユーザとなる必要があります。登録ユーザは、次の URL でこのツールを使用できます。

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Cisco.com にユーザ登録するには、次の URL にアクセスします。

http://tools.cisco.com/RPF/register/register.do

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Support Web サイト

Cisco Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/en/US/support/index.html

Cisco Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） オンラインまたは電話でサービス リクエストを発行する前に、**Cisco Product Identification Tool** を使用して製品のシリアル番号を確認してください。Cisco Support Web サイトでこのツールを使用するには、**Get Tools & Resources** リンクをクリックし、**All Tools (A-Z)** タブをクリックした後、アルファベット順のリストから **Cisco Product Identification Tool** を選択します。このツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

ヒント　Cisco.com での表示および検索

ブラウザが Web ページをリフレッシュしていないと思われる場合は、Ctrl キーを押したまま **F5** を押すことで強制的にブラウザに Web ページを更新させます。

技術情報を検索する場合は、Cisco.com の Web サイト全体ではなく、技術マニュアルに検索対象を絞り込みます。Cisco.com のホームページで Search ボックスを使用した後、表示されたページで Search ボックスの隣の **Advanced Search** リンクをクリックし、**Technical Support & Documentation** オプション ボタンをオンにします。

Cisco.com の Web サイトまたは特定の技術マニュアルに関するフィードバックを送るには、Cisco.com のすべての Web ページの下部にある **Contacts & Feedback** をクリックします。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Online Subscription Center は、シスコのさまざまな E メール ニュースレターやその他の通信に登録できる Web サイトです。プロファイルを作成し、受信を希望する情報を選択してください。Cisco Online Subscription Center には、次の URL からアクセスできます。

  http://www.cisco.com/offer/subscribe

- 『*Cisco Product Quick Reference Guide*』は手軽でコンパクトな参照ツールです。チャネル パートナー経由で販売される多くのシスコ製品に関する簡単な製品概要、主要な機能、サンプル部品番号、および簡単な技術仕様を記載しています。年 2 回の更新の際には、シスコのチャネル製品の最新情報が収録されます。『*Cisco Product Quick Reference Guide*』の注文方法および詳細については、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- 「What' New in Cisco Documentation」は、シスコ製品の最新のマニュアル リリースに関する情報を提供するオンライン出版物です。このオンライン出版物は毎月更新され、製品カテゴリ別に編成されているため、製品のマニュアルを簡単に検索できます。次の URL で「What' New in Cisco Documentation」の最新リリースを見ることができます。

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

Service Monitor を使用する前に

Cisco Unified Service Monitor（Service Monitor）はシスコ ユニファイド コミュニケーション管理スイートの製品で、Cisco Unified CallManager クラスタおよび Cisco 1040 センサーから Mean Opinion Score（MOS; 平均オピニオン スコア）を受信して分析し、違反が発生した場合にトラップを送信します。

この項では次のトピックについて説明します。

(注) Service Monitor を初めて設定するときの詳細については、P.A-1 の「設定のチェックリストおよびヒント」を参照してください。

概要

Service Monitor は、Cisco Unified CallManager クラスタおよび Cisco 1040 センサーから MOS を受信して分析します。Service Monitor は、センサーまたはクラスタ、あるいはこの両方をサポートします。詳細については、P.1-2 の「データの収集および分析」を参照してください。

Service Monitor は、受信したデータを分析して、MOS がしきい値より下回っている場合にはトラップを送信します。Service Monitor には、サポートされるコーデックごとにデフォルトのグローバルしきい値のセットが 1 つ用意されています。また、Service Monitor では、デフォルトのグローバルしきい値の変更、およびしきい値グループ（センサーしきい値グループおよびクラスタしきい値グループ）を作成することにより、このグローバルしきい値を上書きできます。詳細については、P.1-3 の「しきい値とトラップ」およびP.1-4 の「トラップ レシーバ」を参照してください。

Service Monitor 診断レポートに、過去 30 日間に行われたコールのデータが表示されます。クラスタから報告されたデータおよびセンサーから報告されたデータのレポートを作成できます。また、24 時間または 7 日間に違反数が最大であったエンドポイントについてのレポートも作成できます。詳細については、P.2-1 の「レポートの使用方法」を参照してください。

データの収集および分析

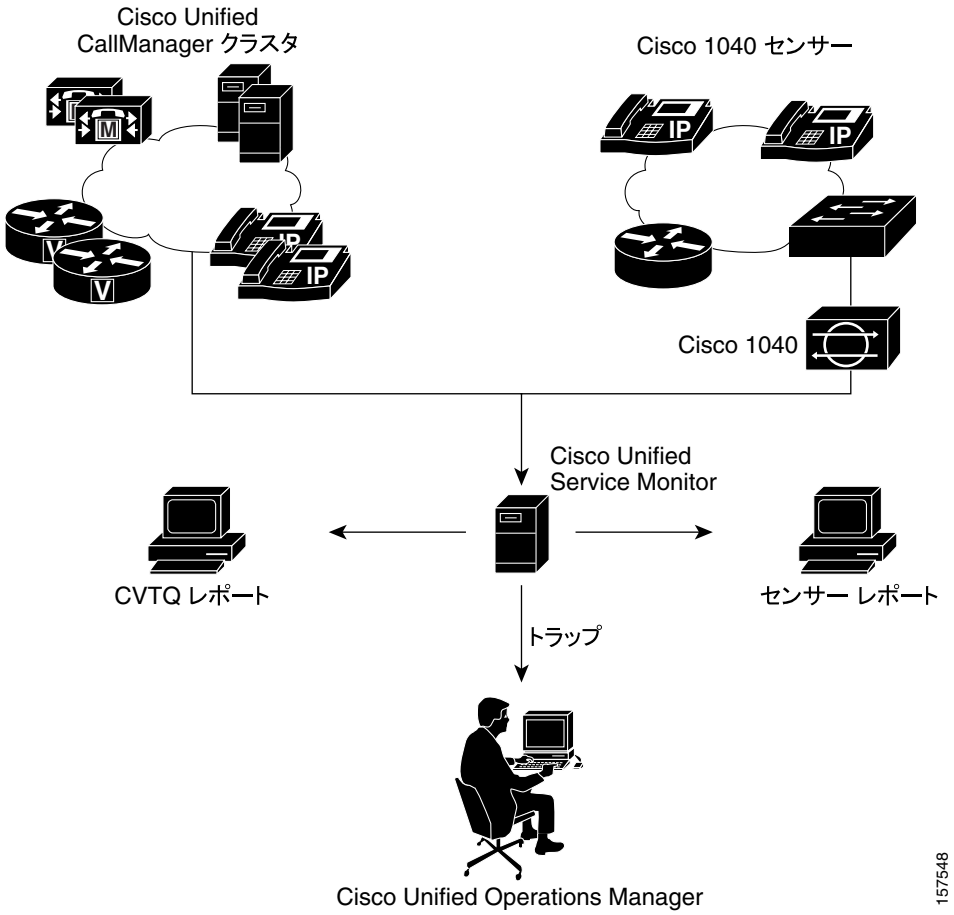
Service Monitor は、次のソースが音声ネットワークにインストールされ、適切に設定されると、これらから MOS を受信して分析します。

- センサー：Cisco 1040 センサーは、各 Real-Time Transport Protocol（RTP）ストリームの MOS を計算して、syslog メッセージを 60 秒ごとに Service Monitor に送信します。
- CVTQ：Cisco Unified CallManager は、Cisco 音声ゲートウェイおよび Cisco IP Phone からデータを収集します。MOS は、Cisco Voice Transmission Quality（CVTQ）アルゴリズムを使用して、ゲートウェイおよび電話機について計算されます。コールの終了時に、Cisco Unified CallManager はデータを Call Detail Records（CDR; コール詳細レコード）と Call Management Records (CMR; コール管理レコード）に保存します。

（注） Service Monitor をサポートする Cisco Unified CallManager のバージョンについては、『*Release Notes for Cisco Unified Service Monitor 2.0*』を参照してください。

図 1-1 に、Service Monitor によるデータの受信、レポートの作成、およびトラップの送信を示します。

図 1-1　Service Monitor の概要



詳細については、次の項を参照してください。

- Service Monitor の設定（P.3-1）
- センサーの管理（P.4-1）

しきい値とトラップ

Service Monitor は、受信したデータを調査して、ユーザ定義しきい値グループの設定値またはグローバルしきい値の設定値の該当するしきい値と MOS を比較します。MOS がしきい値を下回っている場合、Service Monitor は SNMP トラップを生成し、そのトラップを最大 4 つのトラップ レシーバに送信します。

しきい値は、次に対して設定できます。

- センサー グループ：センサーおよびエンドポイントを選択して、1 つまたは複数のサポートされるコーデックの MOS しきい値を設定します。
- CVTQ グループ：Cisco Unified CallManager クラスタおよびエンドポイントを選択して、1 つまたは複数のサポートされるコーデックの MOS しきい値を設定します。
- グローバル設定：1 つまたは複数のサポートされるコーデックのデフォルトしきい値を更新します。グローバルしきい値設定は、他に該当するしきい値がない場合に使用されます。

トラップ レシーバ

Service Monitor は、受信したデータを調査し、コーデックのデフォルトしきい値またはユーザ定義しきい値と MOS を比較します。MOS がしきい値を下回っている場合、Service Monitor は SNMP トラップを生成して、そのトラップを最大 4 つのトラップ レシーバに送信します。また、次からデータを受信したときに、受信したコール メトリックも保存します。

- クラスタ：Service Monitor は、情報をデータベースに最大 30 日間保存します。
- Cisco 1040 センサー：Service Monitor は情報をデータベースに最大 30 日間保存します。オプションで、Service Monitor は、Cisco 1040 から受信したコール メトリックをディスク ファイルに保存します。

Cisco Unified Operations Manager（Operations Manager）を Service Monitor のトラップ レシーバとして設定できます。Operations Manager は、Service Monitor データをさらに分析、表示、および操作できます。Operations Manager では、次の操作を実行できます。

- Service Monitor トラップのイベントの生成
- Service Quality Alerts ダッシュボードへのイベントの表示
- 最大 30 日間のイベント履歴の保存

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

Service Monitor のホーム ページ

Reports タブは Service Monitor のホーム ページであり、ログインすると表示されます。このホーム ページから、最長で過去 30 日間の MOS 統計を表示するレポートを生成できます。

- センサー レポートの使用方法（P.2-5）
- CVTQ レポートの使用方法（P.2-9）
- Most-Impacted Endpoints レポートの使用方法（P.2-13）

Service Monitor の起動

ステップ 1　ブラウザに http://*server_name*:1741 と入力します。ここで、server_name は、Service Monitor がインストールされているサーバの DNS 名または IP アドレスです。ログイン ページが表示されます。

ステップ 2　ユーザ名とパスワードを入力します。ユーザ名がない場合は、次を使用できます。

- ユーザ ID に *admin* と入力します。
- インストール時に admin ユーザ用に入力したパスワードを入力して Enter キーを押します。

Service Monitor のホーム ページが表示されます。

詳細については、次の項を参照してください。

- ユーザの設定（ACS および非 ACS）（P.6-7）

CHAPTER 2

レポートの使用方法

この項では次のトピックについて説明します。

概要：Service Monitor レポート

Service Monitor レポートを使用すると、Service Monitor が過去 30 日間に監視したネットワークの一部の音声伝送品質を調査できます。Service Monitor レポートには、設定されたしきい値を MOS が下回っていた時間、使用されているコーデック、および違反が発生したエンドポイントが表示されます。レポートのデータは、ネットワーク内の Cisco 1040 センサーおよび Cisco Unified CallManager クラスタから取得されます。

Service Monitor は、センサーおよび Cisco Unified CallManager から収集したデータを、Service Monitor データベースに 30 日間保存します。また、Service Monitor はデータベースを毎日消去して、過去 30 日間のデータだけを保持します。詳細については、P.6-2 の「Service Monitor データベースの消去について」を参照してください。

Service Monitor は、次から取得したデータについて、別個にレポートを作成します。

- センサー：センサーから Service Monitor に 60 秒ごとにデータが送信され、1 分ごとの MOS 評価が提供されます。
- Cisco Unified CallManager クラスタ：Service Monitor は、クラスタから CVTQ データを 60 秒ごとに取得します。ただし、指定されたコールのデータが使用可能になるのは、コールが完了してからです。したがって、Service Monitor が MOS を評価し、トラップを送信し、情報をレポートで表示できるのは、コールが発生した後になります。

センサー レポートおよび CVTQ レポートには、次の 2 つのタイプのレポートがあります。

- 診断レポート：このレポートでは、レポート対象を指定でき、また 1 分間のデータから 30 日間のデータまでのレポートを生成できます。レポート ウィンドウでは、表示される列を変更できます。たとえば、デフォルトの列セットを表示するようにレポートを元に戻すこともできます（P.2-3 の「Service Monitor レポートで表示または非表示にする列の選択」を参照）。詳細については、P.2-5 の「センサー レポートの使用方法」および P.2-9 の「CVTQ レポートの使用方法」を参照してください。

- Most-Impacted Endpoint レポート：このレポートには、過去 24 時間に最も多くの違反が報告されたエンドポイントが表示されます。このレポートを自動的に実行するようにスケジュールすることもできます。これにより、過去 24 時間および過去 7 日間のエクスポート済みレポートが作成されます。詳細については、P.2-13 の「Most-Impacted Endpoints レポートの使用方法」を参照してください。

レポートを実行する前の Service Monitor の初期設定

Service Monitor レポートを初めて実行する前に、いくつかの設定作業を行っておく必要があります。Service Monitor は、次によって収集されたデータの監視を開始します。

- Cisco Unified CallManager クラスタ：Service Monitor に資格情報を追加し、Cisco Unified CallManager、または Cisco Unified CallManager が常駐するシステムにいくつかの設定を実行する必要があります。詳細については、次の項を参照してください。
  - Cisco Unified CallManager の資格情報と概要（P.3-2）
  - Cisco Unified CallManager の設定（P.B-1）
- Cisco 1040 センサー：P.4-3 の「Service Monitor でのセンサーの初期設定の実行」に示す作業を完了する必要があります。

Service Monitor レポートには、過去 30 日間までのデータとライセンスを付与された電話機数までのデータが含まれます。

- レポートを生成するには、次の項を参照してください。
  - センサー レポートの指定および生成のためのセンサー レポート フィルタの使用方法（P.2-5）
  - CVTQ レポートの指定および生成のための CVTQ レポート フィルタの使用方法（P.2-9）
- ライセンスの限度、および Service Monitor が監視している電話機の合計数を表示するには（クラスタおよびセンサーから合計数を取得後）、P.3-9 の「監視対象のセンサーおよびクラスタの選択」を参照してください。

Service Monitor レポートを使用する場合には、次の情報が役立ちます。

- レポート ツール ボタンについて（P.2-2）
- Service Monitor レポートで表示または非表示にする列の選択（P.2-3）

レポート ツール ボタンについて

次のレポート ツール ボタンが、Service Monitor レポートの右上隅に表示されることがあります。

	現在のレポートを PDF または CSV ファイルにエクスポートして、ローカル システムに保存します。  **（注）** すべてのレコードまたは所定の範囲のレコード数のデータをエクスポートできます。
	新しいウィンドウが開き、ブラウザから印刷のフォーマット設定がされたレポートが表示されます。
	列セレクタ ダイアログボックスを開きます。このボックスでは、表示または非表示にするレポートの列を選択できます（P.2-3 の「Service Monitor レポートで表示または非表示にする列の選択」を参照）。
	文脈依存ヘルプを開きます。

Service Monitor レポートで表示または非表示にする列の選択

デフォルトでは、センサー レポートおよび CVTQ レポートに、表示可能なデータ列がすべて表示されるわけではありません。表示するデータを選択できます。

ステップ 1　レポートの右上隅の Tool ボタン  をクリックします。列セレクタ ダイアログボックスが表示されます。

ステップ 2　デフォルトで表示される列を使用するようにレポートを元に戻すには、**Restore Default Columns** ボタンをクリックします。列セレクタ ダイアログボックスが閉じて、レポート ウィンドウがリフレッシュされ、デフォルトの列が表示されます。

ステップ 3　レポート列を更新するには、次のようにします。

- 列を非表示にするには、その列を Hidden Column(s) リストに配置します。
  - 列の名前を Displayed Column(s) リストから選択します。
  - **< Remove <<** ボタンをクリックします。Hidden Column(s) リストに列が表示されます。

（注）　隣接する複数の列を選択するには、Shift キーを押したまま選択します。隣接していない複数の列を選択するには、Ctrl キーを押したまま選択します。

- 列を表示するには、その列を Displayed Column(s) リストに配置します。
  - 列の名前を Hidden Column(s) リストから選択します。
  - **< Add <<** ボタンをクリックします。Displayed Column(s) リストに列が表示されます。

Update をクリックします。レポート ウィンドウがリフレッシュされ、Displayed Column(s) リストにある列だけが表示されます。

（注）　選択内容が保存され、他のユーザにも適用されます。

エンドポイントの IP アドレスまたは電話番号の指定

しきい値グループを追加または編集する場合には、エンドポイントを指定する必要があります。これには、完全な電話番号または IP アドレス（いずれか適した方）を入力します。また、ワイルドカードを使用して、電話番号または IP アドレスの範囲を指定することもできます。表 2-1 に、例をいくつか示します。

表 2-1　エンドポイント定義

しきい値グループタイプ	エンドポイントのタイプ	例
CVTQ	電話番号	• 500 は 500 とだけ一致します。 • 5XXX は、5 で始まる 4 桁の番号（たとえば、5876）と一致します。 **（注）** 大文字の X だけを入力します。
次のいずれかです。 • CVTQ • センサー	IP アドレス	• 172.20.119.21 は 172.20.119.21 とだけ一致します。 • 172.*.*.*.* は、172.0.0.1 から 172.255.255.255 までのすべての IP アドレスに一致します。

センサー レポートの使用方法

ネットワーク内の Cisco 1040 センサーが Service Monitor に登録されると、発生したすべてのコールのデータがセンサーからその Service Monitor に 60 秒ごとに送信されます。Service Monitor はそのデータをデータベースに最大 30 日間保存します。センサー レポート フィルタを使用すると、センサーによって監視されていたすべてのコールのデータを含むレポート、または次のような一部のデータを含むレポートを生成できます。

- MOS が特定の値よりも小さかったデータ
- 特定のセンサーから報告されたデータ
- 特定のコーデックが使用されていたデータ
- エンドポイント セットのデータ
- すべてのセンサーまたは一部のセンサーのデータ
- 過去 30 日間のうちの特定の期間（1 分から 30 日まで）のデータ

センサー レポートの指定および生成のためのセンサー レポート フィルタの使用方法

ステップ 1　**Reports > Sensor Filter** を選択します。Cisco 1040 Sensor Report Filter ページが表示されます。

ステップ 2　次のいずれかを実行します。

- **Generate Report** をクリックすると、デフォルトの基準を使用したレポートが生成されます。レポートが新しいウィンドウに表示されます。P.2-6 の「センサー レポートについて」を参照してください。
- 次の表に示す、いずれかのレポート入力を変更します。データをレポートに含めるには、それらの各データが指定された基準を満たす必要があります。

フィールド	説明 / 処理
MOS Less than or Equal to	0.0 から 5.0 までの値を入力します。
Jitter Greater than or Equal to	ミリ秒数を入力します。
Packet Loss Greater than or Equal to	パケット損失のパーセントを入力します。
Codec	リストからコーデックを選択します。
Endpoint 1	正確な IP アドレスを入力するか、ワイルドカード（*）を使用して（または、数値とワイルドカードの組み合わせを使用）、次のいずれかの IP アドレスの範囲を指定します。 • Cisco IP Phone • Cisco 会議ブリッジ • Cisco 音声ゲートウェイ **（注）** レポートには、このエンドポイント（コール先エンドポイントまたはコール元エンドポイントのいずれか）からの音声アクティビティが含まれます。 詳細については、P.2-4 の「エンドポイントの IP アドレスまたは電話番号の指定」を参照してください。

フィールド	説明 / 処理
Endpoint 2	正確な IP アドレスを入力するか、ワイルドカード（*）を使用して（または、数値とワイルドカードの組み合わせを使用）、次のいずれかの IP アドレスの範囲を指定します。 • Cisco IP Phone • Cisco 会議ブリッジ • Cisco 音声ゲートウェイ **（注）** レポートには、このエンドポイント（コール先エンドポイントまたはコール元エンドポイントのいずれか）からの音声アクティビティが含まれます。
Sensor ID(s)	センサーを選択するには、次のようにします。 1.  をクリックします。Select Sensors ダイアログボックスが表示されます。 2. チェックボックスを選択します。 3. **OK** をクリックします。
Date and Time	レポート対象の期間の開始日時と終了日時を入力します。

ステップ 3　**Generate Report** をクリックします。レポートが新しいウィンドウに表示されます。

センサー レポートについて

センサーは、音声トラフィックをミラーリングするように設定された Switch Port Analyzer（SPAN）ポートで RTP 音声トラフィックを受信します。2 つの RTP ストリーム（着信および発信）で 1 つの音声コールを構成します。電話機ポートおよび SPAN ポートでミラーリングされる音声 VLAN によっては、センサーは、一方のみまたは両方の RTP ストリームを受信して、60 秒ごとに MOS を計算し、データを Service Monitor に送信することがあります。

センサー レポートには、RTP ストリームについてセンサーが 1 分ごとに計算した MOS を表示できます。センサー レポートには、一方だけまたは両方の RTP ストリームが SPAN ポートでミラーリングされたかどうかに応じて、60 秒ごとに 1 行または 2 行のデータが表示されます。各行に、データを収集したセンサー、関係するエンドポイント、MOS、ジッタ（ミリ秒単位）、およびタイム スタンプが示されます。

表 2-2 に、Cisco 1040 センサー レポートに表示できるすべてのデータの列を示します。デフォルトでは、すべての列が表示されるわけではありません。詳細については、P.2-3 の「Service Monitor レポートで表示または非表示にする列の選択」を参照してください。

表 2-2　センサー レポートの内容

列	説明
Sensor Name	データを収集し、MOS を分析したセンサーの説明的な名前。 **（注）** Cisco 1040 という名前は、デフォルトの設定ファイルを使用してセンサーが Service Monitor に登録されていることを示します。別の名前を入力する場合は、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。
Sensor MAC Address	センサーの MAC アドレス。
Speaker Directory Number	デバイス（下記の Speaker IP Address を参照）が次の Cisco Unified CallManager によって管理されている場合には、電話番号が表示されます。 • 適切な資格情報で Service Monitor に追加されている。 • 監視を中断されていない。
Speaker IP Address	音声ゲートウェイまたは IP Phone の IP アドレス。
Speaker Device Type	次のいずれかです。 • 音声ゲートウェイまたは Cisco IP Phone モデル番号。 • N/A：何らかのエラーによって、Service Monitor はデバイス タイプを取得できません。 • Unavailable：Service Monitor がこの電話機を検出したのが初めてで、デバイス タイプがまだ認識されていません。または、対応する Cisco Unified CallManager が次のいずれかです。 — Service Monitor に追加されていない。 — 有効なデバイス タイプが Service Monitor に指定されていない。
Listener Directory Number	デバイス（下記の Listener IP Address を参照）が次の Cisco Unified CallManager によって管理されている場合には、電話番号が表示されます。 • 適切な資格情報で Service Monitor に追加されている。 • 監視を中断されていない。
Listener IP Address	音声ゲートウェイまたは IP Phone の IP アドレス。
Listener Device Type	次のいずれかです。 • 音声ゲートウェイまたは Cisco IP Phone モデル番号。 • N/A：何らかのエラーによって、Service Monitor はデバイス タイプを取得できません。 • Unavailable：Service Monitor がこの電話機を検出したのが初めてで、デバイス タイプがまだ認識されていません。または、対応する Cisco Unified CallManager が次のいずれかです。 — Service Monitor に追加されていない。 — 有効なデバイス タイプが Service Monitor に指定されていない。
MOS	この 60 秒間の平均 MOS 値。

表 2-2　センサー レポートの内容（続き）

列	説明
Cause	MOS が低下する理由。次のいずれかです。 • ジッタ • パケット損失
Codec	使用されたコーデック。
Time Stamp	この 60 秒間の開始日時。
Jitter (ms)	この 60 秒間のジッタ（ミリ秒単位）。
Packet Loss (%)	この 60 秒間のパケット損失（パーセント）。

CVTQ レポートの使用方法

Cisco Unified CallManager クラスタからデータを受信するように Service Monitor が設定されていた場合、Service Monitor はそのデータをデータベースに最大 30 日間保存します。CVTQ レポート フィルタを使用すると、クラスタからのすべてのコール データを含むレポート、または次のような一部のコール データを含むレポートを生成できます。

- MOS が特定の値よりも小さかったデータ
- 特定のクラスタから報告されたデータ
- 特定のコーデックが使用されていたデータ
- エンドポイント セットのデータ
- すべてのクラスタまたは一部のクラスタのデータ
- 過去 30 日間のうちの特定の期間（1 分から 30 日まで）のデータ

CVTQ レポートの指定および生成のための CVTQ レポート フィルタの使用方法

ステップ 1　**Reports** > **CVTQ Filter** を選択します。CVTQ Report Filter ページが表示されます。

ステップ 2　次のいずれかを実行します。

- **Generate Report** をクリックすると、そのページに表示されたデフォルト値を使用したレポートが生成されます。レポートが新しいウィンドウに表示されます。P.2-11 の「CVTQ レポートについて」を参照してください。
- 次の表に示す、いずれかのレポート入力を変更します。データをレポートに含めるには、それらの各データが指定された基準を満たす必要があります。

フィールド	説明 / 処理
MOS Less than or Equal to	0.0 から 5.0 までの数値を入力します。
Jitter Greater than or Equal to	ミリ秒数を入力します。
Packet Loss Greater than or Equal to	パケット損失のパーセントを入力します。
Codec	リストからコーデックを選択します。
Concealment seconds Greater than or Equal to	音声ストリームの開始からの隠匿イベント（フレームの損失）のあった秒数（厳密に隠匿された秒数、つまり、5 パーセントを超える隠匿フレームのあった合計秒数を含みます）。
Concealment ratio Greater than or Equal to	コールが開始してから観察された、合計フレームに対する隠匿フレームの累積比率。

フィールド	説明 / 処理
Endpoint 1	次のいずれかのオプション ボタンを選択し、該当するデータを入力して、コール先またはコール元エンドポイントを指定します。 • DN：電話番号。正確な電話番号を入力するか、ワイルドカード（X）を使用して（または、数値とワイルドカードの組み合わせを使用）、電話番号の範囲を指定します。 • IP：IP アドレス。正確な IP アドレスを入力するか、ワイルドカード（*）を使用して（または、数値とワイルドカードの組み合わせを使用）、IP アドレスの範囲を指定します。 **（注）** ワイルドカードを入力する場合は、大文字の X を入力する必要があります。詳細については、P.2-4 の「エンドポイントの IP アドレスまたは電話番号の指定」を参照してください。
Endpoint 2	次のいずれかのオプション ボタンを選択し、該当するデータを入力して、コール先またはコール元エンドポイントを指定します。 • DN：電話番号。正確な電話番号を入力するか、ワイルドカード（X）を使用して（または、数値とワイルドカードの組み合わせを使用）、電話番号の範囲を指定します。 • IP：IP アドレス。正確な IP アドレスを入力するか、ワイルドカード（*）を使用して（または、数値とワイルドカードの組み合わせを使用）、IP アドレスの範囲を指定します。 **（注）** ワイルドカードを入力する場合は、大文字の X を入力する必要があります。
Cluster ID(s)	クラスタを選択するには、次のようにします。 1.  をクリックします。Select Clusters ダイアログボックスが表示されます。 2. チェックボックスを選択します。 3. **OK** をクリックします。
Call Termination Date and Time	レポート対象の期間の開始日時と終了日時を入力します。

ステップ 3　**Generate Report** をクリックします。レポートが新しいウィンドウに表示されます。P.2-11 の「CVTQ レポートについて」を参照してください。

CVTQ レポートについて

表 2-3 に、CVTQ レポートに表示できるすべてのデータの列を示します。デフォルトでは、すべての列が表示されるわけではありません。詳細については、P.2-3 の「Service Monitor レポートで表示または非表示にする列の選択」を参照してください。

(注) レポートにはコールごとに 2 行表示されます。1 行はコール先エンドポイントでの受信についてのデータで、もう 1 行はコール元エンドポイントについてのデータです。

表 2-3　CVTQ レポートの内容

列	説明
Cluster ID	Cisco Unified CallManager クラスタ ID。
Caller	• Directory Number：コールを発信した電話番号。 • IP Address：コールの発信元の IP アドレス。 • Device Type：コールを発信しているデバイスのタイプ。次のいずれかです。 — 音声ゲートウェイの IP アドレス — Cisco IP Phone のモデル番号
Called	• Directory Number：コールを受信した電話番号。 • IP Address：コールの送信先 IP アドレス。 • Device Type：コールを受信するデバイスのタイプ。次のいずれかです。 — 音声ゲートウェイの IP アドレス — Cisco IP Phone のモデル番号
Listener DN/IP	MOS または障害の詳細が関係するエンドポイント（コール元またはコール先）を識別します。次のいずれかです。 • リスナの IP アドレス • リスナの電話番号
MOS	コール中の平均 MOS 値。このデータがクラスタから使用できない場合は Unavailable。一部の IP Phone、音声ゲートウェイ、および Cisco Unified CallManager バージョンでは MOS が提供されません。詳細については、『*Release Notes for Cisco Unified Service Monitor 2.0*』を参照してください。
Codec	コールで使用されているコーデック。
Time Stamp	コールの日時。
Call Duration [h][m]s	コールの時間、分、秒の合計。

表 2-3　CVTQ レポートの内容（続き）

列	説明
Impairment Details	• Jitter (ms)：コール中のジッタ（ミリ秒）。 • Packet Loss (%)：コール中のパケット損失（パーセント）。 • Concealment Seconds：音声ストリームの開始からの隠匿イベント（フレームの損失）のあった秒数（厳密に隠匿された秒数を含む）。 • Severely Concealed Seconds：かなりの量の隠匿（50 ミリ秒を超過）が観察された秒数。 • Concealment Ratio：合計フレームに対する隠匿フレームの比率。
Call Release Code	• Caller Termination Cause：コール元エンドポイントでコールが終了した理由を示すコード。 • Called Termination Cause：コール先エンドポイントでコールが終了した理由を示すコード。 詳細については、次のいずれかを参照してください。 • 『*Call Detail Record Definitions for Cisco Unified CallManager 5.0(2)*』の「Call Release Codes」 • 『*Cisco CallManager 4.2(1) Call Detail Record Definition*』の「Cause Codes」 このマニュアルは次の URL にあります。 http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html

Most-Impacted Endpoints レポートの使用方法

Service Monitor は毎日午前 1 時に、保存されているコール データを分析して、前日（00:00:00 から 23:59:59:999 まで）に最も多くの数の違反が発生したエンドポイントを判別します。Service Monitor は、この分析の結果をデータベースに保存して、Most-Impacted Endpoints レポートに表示できるようにします。必要であれば、分析に続いて、毎日および週に 1 回（月曜日）、Most-Impacted Endpoints レポートをエクスポートし、それをサーバに保存できます。

デフォルトでは、Service Monitor は最も影響を受けた 10 個のエンドポイントを判別しますが、Most-Impacted Endpoints レポートはエクスポートしません。Service Monitor が報告する最も影響を受けたエンドポイントの数を変更する場合、また自動エクスポートを設定する場合は、P.3-12 の「エンドポイント数の設定と Most-Impacted Endpoints レポートのエクスポート設定」を参照してください。

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 Most-Impacted Endpoints レポートの生成と概要

（注） デフォルトでは、Most-Impacted Endpoints レポートには、10 個のエンドポイントが含まれます。詳細については、P.3-12 の「エンドポイント数の設定と Most-Impacted Endpoints レポートのエクスポート設定」を参照してください。

ステップ 1　Cisco 1040 センサーの Most-Impacted Endpoints レポートを生成するには、**Reports > Sensor: Impacted Endpoints** を選択します。レポートが新しいウィンドウに表示されます。

Cisco 1040 センサーの Most-Impacted Endpoints レポートには、表 2-4 に示すデータが表示されます。

表 2-4　Cisco 1040 Sensor Most-Impacted Endpoint レポートの内容

列	説明
Endpoint	次のいずれかです。 • 電話番号。 • IP Phone、音声ゲートウェイ、または会議ブリッジの IP アドレス。
Device Type	音声ゲートウェイ。電話機の場合は Cisco 電話機モデルが表示されます。 **（注）** 対応する Cisco Unified CallManager が Service Monitor に追加されていない場合、または無効なデバイス タイプが返された場合、Service Monitor には Unavailable と表示されます。

表 2-4　Cisco 1040 Sensor Most-Impacted Endpoint レポートの内容（続き）

列	説明
Cumulative Talk Time (min)	レポート期間中にこのエンドポイントを経由した音声の累積時間。 **（注）** Reports タブから起動された場合、レポートには前日（00:00:00 から 23:59:59:999 まで）のデータが含まれます。設定されている場合は、サーバにエクスポートされた週次レポートを調査できます。エクスポートされたレポートの場所については、P.3-12 の「エンドポイント数の設定と Most-Impacted Endpoints レポートのエクスポート設定」を参照してください。
Impaired Minutes	MOS がしきい値を下回ってこのエンドポイントを経由した分数。
% of Impaired Minutes	すべての分数に対する障害のあった分数のパーセント。
Average MOS	累積トーク時間中の平均 MOS 値。

CVTQ の Most-Impacted Endpoints レポートの生成と概要

（注） Most-Impacted Endpoints レポートに含めるエンドポイントの数の設定については、P.3-12 の「エンドポイント数の設定と Most-Impacted Endpoints レポートのエクスポート設定」を参照してください。

ステップ 1　CVTQ の Most-Impacted Endpoints レポートを生成するには、**Reports > CVTQ: Impacted Endpoints** を選択します。レポートが新しいウィンドウに表示されます。

CVTQ の Most-Impacted Endpoints レポートには、表 2-5 に示すデータが表示されます。

表 2-5　CVTQ の Most-Impacted Endpoints レポートの内容

列	説明
Endpoint	次のいずれかです。 • 電話番号。 • IP Phone、音声ゲートウェイ、または会議ブリッジの IP アドレス。
IP Address	エンドポイントの IP アドレス。
Device Type	音声ゲートウェイ。電話機の場合は Cisco 電話機モデルが表示されます。

表 2-5　CVTQ の Most-Impacted Endpoints レポートの内容（続き）

列	説明
Cumulative Talk Time (min)	レポート期間中にこのエンドポイントを経由したすべてのコールの累積時間。 **（注）** Reports タブから起動された場合、レポートには前日（00:00:00 から 23:59:59:999 まで）のデータが含まれます。設定されている場合は、サーバにエクスポートされた週次レポートを調査できます。エクスポートされたレポートの場所については、P.3-12 の「エンドポイント数の設定と Most-Impacted Endpoints レポートのエクスポート設定」を参照してください。
# of Calls	レポート期間中にこのエンドポイントを経由したコールの数。
Impaired Calls	レポート期間中にこのエンドポイントを経由した障害のあったコールの数。
% of Impaired Calls	レポート期間中のコールのうち、障害のあったコールのパーセント。
Average MOS	累積トーク時間中の平均 MOS 値。このデータがクラスタから使用できない場合は Unavailable。一部の IP Phone、音声ゲートウェイ、および Cisco Unified CallManager バージョンでは MOS が提供されません。詳細については、『*Release Notes for Cisco Unified Service Monitor 2.0*』を参照してください。

CHAPTER 3

Service Monitor の設定

この項では次のトピックについて説明します。

(注) 詳細については、P.4-1 の「センサーの管理」および P.A-1 の「設定のチェックリストおよびヒント」を参照してください。

トラップ レシーバの設定

ステップ 1　**Configuration** > **Trap Receivers** を選択します。Trap Receiver Parameters ページが表示されます。

ステップ 2　次の表で説明するデータを入力します。

GUI の要素	説明 / 処理
SNMP Community String	各トラップ レシーバの SNMP コミュニティ ストリングを入力します。
Trap Receiver *n* および Port フィールド（*n* は 1 ～ 4 までの番号）	最大 4 つのトラップ レシーバを入力します。 • Trap Receiver *n*：サーバの IP アドレスまたは DNS 名を入力します。Operations Manager を使用して Service Monitor のデータを操作およびデータを表示するには（たとえば、Service Quality Alerts ダッシュボードを使用するには）、Operations Manager が動作しているシステムの IP アドレスを指定します。 • Port：レシーバが SNMP トラップを受信するポート番号を入力します。デフォルトは 162 です。ただし、この目的でサーバ上の別のポートが使用されることもあります。 Service Monitor は SNMP トラップを生成すると、これらのレシーバに転送します。

ステップ 3　**OK** をクリックします。

Cisco Unified CallManager の資格情報と概要

Service Monitor は、サポートされるバージョンの Cisco Unified CallManager から音声データを取得して分析できます。Service Monitor でこれを実行するには、次の作業が必要です。

1. Cisco Unified CallManager を使用するか、または Cisco Unified CallManager がインストールされているシステムにログインして、設定作業を行います。P.B-1 の「Cisco Unified CallManager の設定」を参照してください。
2. 次のようにして Cisco Unified CallManager の資格情報を Service Monitor に追加します。

ステップ 1　**Configuration** > **CallManager Credentials** を選択します。CallManager Credentials ページに、次の表の情報が表示されます。

列またはボタン	説明 / 処理
Display Name	資格情報を Service Monitor に追加したときに入力した、ユーザ指定の名前。
IP Address	クラスタの IP アドレス。
Cluster	• Version：Cisco Unified CallManager ソフトウェアのバージョン。 • ID：Cisco Unified CallManager によってクラスタに割り当てられた ID。
Last Contact Status	次の資格情報のステータス • HTTP/S • CDR/CDRM DB • デバイス DB (注) CDRM データベースは Cisco Unified CallManager 5.x システムに常駐しています。HTTP/S 資格情報を指定した後で、Service Monitor がこのデータベースの資格情報にアクセスできる必要があります。 各資格情報セットについて、次のいずれかのステータスが表示されます。 • Success：リンク。このリンクをクリックすると、最後に正常な接続が行われた時点を確認できます。 (注) ステータス リンクをクリックすると、Service Monitor が最後に Cisco Unified CallManager に接続しようとした時刻、および Service Monitor が正常に接続できた最終時刻などの詳細情報が表示されたダイアログが開きます。 • Verifying：詳細については、リンクをクリックしてください。 • Failure：詳細については、リンクをクリックしてください。 • ブランク：この資格情報は、Service Monitor がこのバージョンの Cisco Unified CallManager から情報を取得するときは不要です。 詳細については、P.3-7 の「最後の接続ステータスと資格情報の検証時期について」を参照してください。
ボタン	• Add：Cisco Unified CallManager クラスタの資格情報を追加します。P.3-4 の「Cisco Unified CallManager の資格情報の追加」を参照してください。 • • Edit：Cisco Unified CallManager クラスタの資格情報を編集します。P.3-6 の「Cisco Unified CallManager の資格情報の編集」を参照してください。 • Delete：P.3-8 の「Cisco Unified CallManager の資格情報の削除」を参照してください。 • Verify：選択した Cisco Unified CallManager クラスタの資格情報を検証します。 • Refresh：ページをリフレッシュします。

サポートされる Cisco Unified CallManager のバージョン

Service Monitor がサポートする Cisco Unified CallManager のバージョンのリストについては、『*Release Notes for Cisco Unified Service Monitor 2.0*』を参照してください。

Cisco Unified CallManager の資格情報の追加

（注） Cisco Unified CallManager 5.x の場合は、次の手順を使用して資格情報を追加するほかに、SFTP パスワードも指定する必要があります。P.3-14 の「その他の設定」を参照してください。

注意 Cisco Unified CallManager 5.x ソフトウェア バージョン クラスタの資格情報を追加する前に、クラスタ ID にスペースが含まれていないことを確認します。詳細については、『*Release Notes for Cisco Unified Service Monitor 2.0*』を参照してください。

ステップ 1　**Configuration > CallManager Credentials** を選択します。CallManager 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。Add CallManager ダイアログボックスが表示されます。

ステップ 3　次の表に説明するデータを入力します。

フィールド	説明
Display Name	最大 20 文字でクラスタを説明する名前を入力します。
Host Name	（オプション）Cisco Unified CallManager がインストールされているサーバのホスト名を入力します。 **（注）** Service Monitor サーバが Cisco Unified CallManager ホスト名から IP アドレスを解決できない場合は、Cisco Unified CallManager のホスト名を入力する必要があります。この問題は、Service Monitor サーバに誤った DNS パラメータが指定されていた場合、または DNS において Cisco Unified CallManager ホスト名が更新されていなかった場合に発生することがあります。
IP Address	次のソフトウェア バージョンについて、クラスタ内の該当するノードの IP アドレスを入力します。 • 3.3.x：パブリッシャの IP アドレスを入力します。 • 4.x：パブリッシャの IP アドレスを入力します。 • 5.x：パブリッシャまたはサブスクライバの IP アドレスを入力します。

フィールド	説明
Version	クラスタで動作しているソフトウェアのバージョンを、次から選択します。 • 3.3.x • 4.x • 5.x (注) 詳細については、P.3-4 の「サポートされる Cisco Unified CallManager のバージョン」を参照してください。 選択したソフトウェア バージョンによっては、1 つまたは複数のユーザ名およびパスワードを入力する必要があります（ステップ 4 を参照）。

ステップ 4　ユーザ名とパスワードを入力します。

(注) クラスタに複数の Cisco Unified CallManager が存在する場合には、そのいずれかの資格情報を指定するだけでかまいません。クラスタ内の特定のノード（パブリッシャなど）の資格情報を入力する必要がある場合は、そのノードがバージョンの下の箇条書き項目内に指定されています。

必要なユーザ名とパスワードは、Cisco Unified CallManager のバージョンによって異なります。

- 3.3.x:
  - CDR DB ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager パブリッシャがインストールされているサーバ上の Microsoft SQLServer アカウントのユーザ名とパスワードを入力します。このアカウントは、CDR データベースにアクセスできる必要があり、また設定によってはデバイス データベースにもアクセスできる必要があります。詳細については、P.B-7 の「Microsoft SQLServer ユーザ アカウントの追加」を参照してください。
  - デバイス DB ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager パブリッシャがインストールされているサーバ上の Microsoft SQLServer アカウントのユーザ名とパスワードを入力します。このアカウントは、デバイス データベースにアクセスできる必要があります。詳細については、P.B-7 の「Microsoft SQLServer ユーザ アカウントの追加」を参照してください。

(注) 両方のデータベースへのアクセスに 1 つの Microsoft SQLServer アカウントを設定していた場合、CDR データベースとデバイス データベースのユーザ名とパスワードは同じになります。

- 4.x:
  - CDR DB ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager パブリッシャがインストールされているサーバ上の Microsoft SQLServer アカウントのユーザ名とパスワードを入力します。このアカウントは、CDR データベースにアクセスできる必要があります。詳細については、P.B-7 の「Microsoft SQLServer ユーザ アカウントの追加」を参照してください。
  - HTTP/S ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager Administration へのログインに使用できるユーザ名とパスワードを入力します。

（注）　クラスタ内のいずれか 1 つの Cisco Unified CallManager のユーザ名とパスワードを指定するだけでかまいません。

- 5.x:
  - HTTP/S ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager Administration へのログインに使用できるユーザ名とパスワードを入力します。

（注）　クラスタ内のいずれか 1 つの Cisco Unified CallManager のユーザ名とパスワードを指定するだけでかまいません。

ステップ 5　**OK** をクリックします。

Cisco Unified CallManager の資格情報の編集

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

ステップ 2　クラスタを選択して、**Edit** をクリックします。Edit CallManager ダイアログボックスが表示されます。

ステップ 3　次の表に説明するデータを入力します。

フィールド	説明
Display Name	最大 20 文字でクラスタを説明する名前を入力します。
Host Name	Cisco Unified CallManager がインストールされているサーバのホスト名。 （注）　Service Monitor が Cisco Unified CallManager からホスト名を正常に取得すると、ここに表示され、以前に指定されていたホスト名と置き換えられます。
IP Address	このフィールドは編集できないため、グレー表示されています。
Version	ソフトウェア バージョン • 3.3.x • 4.x • 5.x （注）　バージョンは、編集によって変更できません。

ステップ 4　選択した Cisco Unified CallManager バージョンのユーザ名とパスワードを入力します。

- 3.3.x:
  - CDR DB ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager がインストールされているサーバ上の Microsoft SQLServer アカウントのユーザ名とパスワードを入力します。このアカウントは、CDR データベースにアクセスできる必要があり、また設定によってはデバイス データベースにもアクセスできる必要があります。詳細については、P.B-7 の「Microsoft SQLServer ユーザ アカウントの追加」を参照してください。
  - デバイス DB ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager がインストールされているサーバ上の Microsoft SQLServer アカウントのユーザ名とパスワードを入力します。このアカウントは、デバイス データベースにアクセスできる必要があります。詳細については、P.B-7 の「Microsoft SQLServer ユーザ アカウントの追加」を参照してください。

（注） 両方のデータベースへのアクセスに 1 つの Microsoft SQLServer アカウントを設定していた場合、CDR データベースとデバイス データベースのユーザ名とパスワードは同じになります。

- 4.x:
  - CDR DB ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager がインストールされているサーバ上の Microsoft SQLServer アカウントのユーザ名とパスワードを入力します。このアカウントは、CDR データベースにアクセスできる必要があります。詳細については、P.B-7 の「Microsoft SQLServer ユーザ アカウントの追加」を参照してください。
  - HTTP/S ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager Administration へのログインに使用できるユーザ名とパスワードを入力します。
- 5.x:
  - HTTP/S ユーザ名とパスワード / パスワードの再入力：Cisco Unified CallManager Administration へのログインに使用できるユーザ名とパスワードを入力します。

ステップ 5　**OK** をクリックします。

最後の接続ステータスと資格情報の検証時期について

Service Monitor には、Cisco Unified CallManager データを正常に取得するために、1 つまたは複数の資格情報が必要です。CallManager Credentials ページに、Service Monitor と Cisco Unified CallManager 間の最後の接続のステータスが表示されます。

ごくまれに、Cisco Unified CallManager 上の資格情報を訂正して、Service Monitor からその資格情報を検証しなければならないことがあります。

- 最後の接続ステータスが Successful の場合に、Service Monitor がデータを受信しておらず、データの受信を待っている状態になっていることがあります。最後に接続が正常に行われた時点を確認するには、ステータス リンクをクリックします。最後の接続が最新でなかった場合には、Cisco Unified CallManager 上の資格情報についての問題を解決して、Service Monitor から資格情報を検証します。
- Service Monitor が依存する資格情報は、Cisco Unified CallManager プラットフォームに応じて変わることがあります。このような場合は、Cisco Unified CallManager の管理者に問い合わせて、正しい資格情報を取得してください。必要であれば、Service Monitor で資格情報を更新します。更新されていない場合は、資格情報を検証します。

（注） クラスタと Service Monitor との間の正常なデータ交換を妨げることのある既知の問題が特定されているかどうかを判別するには、『*Release Notes for Cisco Unified Service Monitor 2.0*』を参照してください。

手順

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

ステップ 2　資格情報を検証する Cisco Unified CallManager を選択します。

ステップ 3　**Verify** をクリックします。

詳細については、次の項を参照してください。

- Cisco Unified CallManager の設定（P.B-1）

Cisco Unified CallManager の資格情報の削除

次の手順を完了すると、Service Monitor は、関連クラスタの音声品質伝送データを取得できなくなります。さらに、クラスタは Monitored Phones ページに表示されなくなります。クラスタのコールデータは、消去されるまでデータベースに残っています。詳細については、P.6-2 の「Service Monitor データベースの消去について」を参照してください。

次の手順を完了する前に、すべての CVTQ しきい値グループからクラスタを削除します。P.5-6 の「CVTQ しきい値グループの編集」を参照してください。

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

ステップ 2　削除するクラスタのチェックボックスを選択します。

ステップ 3　**Delete** をクリックします。次のいずれかが表示されます。

- 確認のダイアログボックスが表示されます。
- エラー メッセージが表示されて、クラスタが属する CVTQ しきい値グループの一覧が示されます。これらの CVTQ しきい値グループからクラスタを削除し、この手順を繰り返す必要があります。

ステップ 4　**OK** をクリックします。

監視対象のセンサーおよびクラスタの選択

Monitored Phones ページでは、Service Monitor が監視している電話機の合計数を表示できます。また、Service Monitor が認識しているすべてのセンサーと Cisco Unified CallManager クラスタの名前の表示、それぞれが監視対象であるかどうかの確認、監視対象の場合はクラスタ内またはセンサーについて Service Monitor が管理する電話機の数の確認もできます。

（注） Cisco Unified CallManager クラスタおよびセンサーが、同じ電話機の一部について MOS を報告する可能性があるため、次のようになる場合があります。

- Monitored Phones ページに表示される既知の電話機カウント合計が、クラスタまたはセンサーの既知の電話機カウントの合計より少ないことがあります。
- 既知の電話機カウント合計を少なくするには、複数のクラスタまたはセンサーを中断する必要がある場合があります。

ステップ 1　**Configuration** > **Monitored Phones** を選択します。Monitored Phones ページが表示され、次の表の情報が示されます。

GUI の要素	説明
Total known phone count: (*n*)	Service Monitor が監視している電話機の数。電話機の数がライセンス サイズと同じ場合は、次のメッセージが赤色で表示されます。 `Total known phone count (n) has reached or exceeded licensed limit!` 詳細については、P.D-4 の「ライセンス サイズ超過の判別」を参照してください。
License limit: (*n*)	ライセンスで許可された電話機の数。
クラスタ / センサー リスト	
Cluster/Sensor ID 列	次のいずれかです。 • Cluster ID：クラスタ ID は Cisco Unified CallManager によって割り当てられます。 • Sensor ID：センサーの MAC アドレス。
Version 列	Cisco Unified CallManager のソフトウェア バージョン。
Type	次のいずれかです。 • Cluster • Sensor

GUI の要素	説明
State 列	次のいずれかです。 • Monitored：Service Monitor はこのクラスタまたはセンサーからデータを収集し、分析して、違反が発生した場合にはトラップを送信します。 • Suspended：Service Monitor は、次のいずれかの理由のために、このクラスタまたはセンサーからデータを収集したり、分析したりしません。 — ユーザがクラスタまたはセンサーの状態を Suspended に設定した。P.3-10 の「クラスタまたはセンサーの監視の中断および再開」を参照してください。 — 電話機ライセンス カウントに達したため、データを受信したときに Service Monitor が新たに作成されたクラスタまたはセンサーを監視できなくなった。
Known Phone Count	コールを行った電話機の数（クラスタ内、またはセンサーによる監視対象）。したがって、Service Monitor に認識され、監視されています。

クラスタまたはセンサーの監視の中断および再開

Cisco Unified CallManager が適切に設定され、Service Monitor のライセンス制限を超えていない場合、Service Monitor は、クラスタを認識するとクラスタの監視を開始します。Service Monitor は、Cisco Unified CallManager の資格情報が Service Monitor に追加されるとクラスタを認識します（詳細については、P.3-4 の「Cisco Unified CallManager の資格情報の追加」を参照）。

Service Monitor は、センサーが登録されたときにセンサーを認識します。

クラスタまたはセンサーの監視を中断したい場合は（たとえば、別のクラスタまたはセンサーから電話機を監視できるようにする場合）、中断できます。

クラスタまたはセンサーの中断

クラスタまたはセンサーを中断すると、次のようになります。

- 中断されたクラスタまたはセンサーのデータは、Service Monitor レポートに表示されなくなります。
- クラスタまたはセンサーは Monitored Phones ページに Suspended として表示され、そのクラスタまたはセンサーの既知の電話機カウントはゼロ（0）になります。この結果、既知の電話機カウント合計も減少する場合は、他のクラスタ内または他のセンサーの電話機の監視を追加できます（ライセンス制限まで）。

ステップ 1　**Configuration > Monitored Phones** を選択します。

ステップ 2　中断するクラスタまたはセンサーのチェックボックスを選択します。

ステップ 3　**Suspend** 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。

クラスタまたはセンサーの再開

ステップ 1　**Configuration > Monitored Phones** を選択します。

ステップ 2　監視する中断されたクラスタまたはセンサーのチェックボックスを選択します。

ステップ 3　**Resume** 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。

クラスタの既知の電話機カウント合計の更新

Service Monitor は、クラスタから受信または取得したデータ内で検出した、最初から *n* 個の電話機を監視します。クラスタ内の電話機に障害があって交換する場合、Service Monitor には通知されず、障害のある電話機は既知の電話機カウント合計に継続してカウントされます。クラスタの既知の電話機カウント合計をリフレッシュするには、クラスタを中断して再開します。

（注）　クラスタを中断すると、そのクラスタの電話機カウントがゼロにリセットされます。その後、電話機からコールが着信すると電話機カウントは増えます。

エンドポイント数の設定と Most-Impacted Endpoints レポートのエクスポート設定

この手順は、次の項目を設定する場合に使用します。

- 実行時期（毎日、週に　1　回、またはオンデマンド）に関係なく、CVTQ　およびセンサーの Most-Impacted Endpoints レポートに含めるエンドポイント数。
- エクスポートする Most-Impacted Endpoints レポート（CVTQ またはセンサー、あるいは両方）。Most-Impacted Endpoints レポートは、毎日または週に 1 回実行し、結果をカンマ区切りの値ファイル（CSV）または Portable Document Format（PDF）ファイルにエクスポートできます。レポートはサーバに保存できます。また必要であれば、電子メールで自動的に送信するように設定できます。

ステップ 1　**Configuration > Export Settings** を選択します。Export Settings（Most-Impacted Endpoint の場合）ページが表示され、次の表の情報が示されます。

GUI の要素	説明 / 処理
Number of Endpoints フィールド	すべての（エクスポートまたは直接起動された）Most-Impacted Endpoints レポートに表示するエンドポイントの数を入力します。
Daily at 1:00 AM チェックボックス	レポートを毎日生成するには、次の中から少なくとも 1 つを選択します。 • CSV チェックボックス：レポートを CSV フォーマットで保存します。 • PDF チェックボックス：レポートを PDF フォーマットで保存します。 どちらも選択しない場合、Service Monitor はレポートを生成しません。
Weekly at 1:00 AM Monday チェックボックス	レポートを毎週生成するには、次の中から少なくとも 1 つを選択します。 • CSV チェックボックス：レポートを CSV フォーマットで保存します。 • PDF チェックボックス：レポートを PDF フォーマットで保存します。 どちらも選択しない場合、Service Monitor はレポートを生成しません。
Report Type	次の中から少なくとも 1 つを選択します。 • Sensor • CVTQ **（注）** センサーおよび CVTQ データについて、別個のレポートが生成されます。レポート ファイル名については、表 3-1 を参照してください。
Save at	Service Monitor がインストールされているサーバ上のレポートの保存場所を入力します。デフォルトの場所が表示されています。
E-mail to	（オプション）1 つまたは複数の完全な電子メール アドレスをカンマで区切って入力します。
SMTP Server	（オプション）SMTP サーバを入力します。

ステップ 2　**Apply** をクリックします。

選択したレポートおよびフォーマットに応じて、次のレポートが生成されます。

表 3-1　エクスポートされた Most-Impacted Endpoints レポート

レポート タイプ	生成時期	レポート ファイル名
CVTQ	毎日	CVTQ_Daily_ddmmyyyy.csv
		CVTQ_Daily_ddmmyyyy.pdf
	毎週	CVTQ_Weekly_ddmmyyyy.csv
		CVTQ_Weekly_ddmmyyyy.pdf
	（注） 月曜日に生成。	
センサー	毎日	Sensor_Daily_ddmmyyyy.csv
		Sensor_Daily_ddmmyyyy.pdf
	毎週	Sensor_Weekly_ddmmyyyy.csv
		Sensor_Weekly_ddmmyyyy.pdf
	（注） 月曜日に生成。	

その他の設定

Cisco Unified CallManager バージョン 5.x からのコールを監視する場合は、次を設定します。

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

ステップ 2　次の表に説明する情報を入力します。

フィールド	説明 / 処理
SFTP	
Username	ユーザ名は smuser から変更できません。 同じユーザ名（smuser）が Cisco Unified CallManager に設定されている必要があります。P.B-4 の「ビリング 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。
Change password チェックボックス	パスワードを変更するときに選択します。 **注意**　デフォルトのパスワードは　smuser　です。ここでパスワードを変更した場合は、Cisco Unified CallManager の smuser のパスワードも変更する必要があります。P.B-4 の「ビリング 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。
Password	パスワードを入力します。
Re-enter password	パスワードを再入力します。

ステップ 3　**Apply** をクリックします。

CHAPTER 4

センサーの管理

この項では次のトピックについて説明します。

概要：センサーからのデータの検査

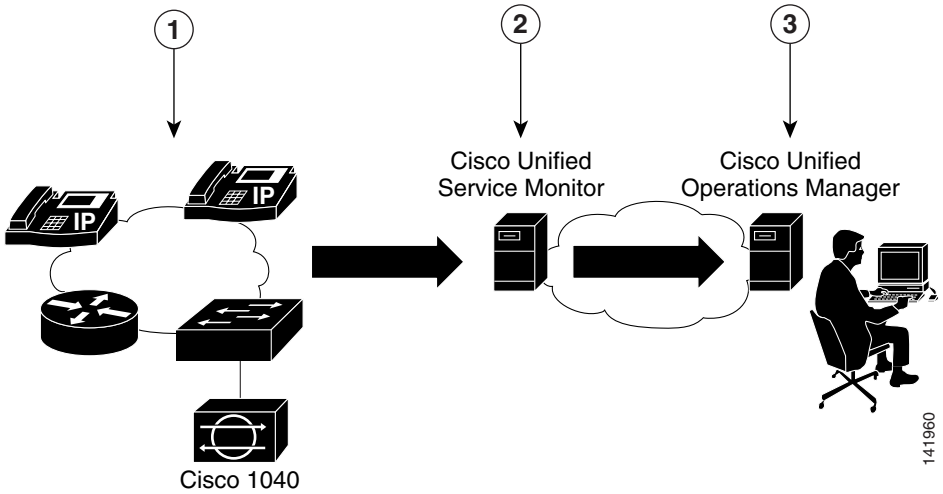
Service Monitor は、音声ネットワークにインストールされている Cisco 1040 センサー（Cisco 1040）からデータを受信して分析します。ライセンスされている Service Monitor の各インスタンスは、複数の Cisco 1040 のプライマリ Service Monitor として機能します。また Service Monitor は、ライセンスされている Service Monitor の他のインスタンスによって管理されている Cisco 1040 に対して、セカンダリ Service Monitor の機能を果たすように設定することもできます。Service Monitor が使用不能になった場合、プライマリ Service Monitor が再び使用可能になるまで、Cisco 1040 はセカンダリ Service Monitor にフェールオーバーできます。

Service Monitor は、RTP ストリームごとに Cisco 1040 が計算した Mean Opinion Score（MOS; 平均オピニオン スコア）とユーザ指定のしきい値とを比較して、Cisco 1040 から受信したデータを調べます。MOS がしきい値を下回っている場合、Service Monitor は SNMP トラップを生成し、そのトラップを最大 4 つのトラップ受信者に送信します。オプションで、Service Monitor は、Cisco 1040 から受信したコール メトリックをディスク ファイルに保存します。

Cisco Unified Operation Manager（Operations Manager）を Service Monitor のトラップ レシーバとして設定して使用することで、Service Monitor データを詳細に分析、表示、および操作することができます。Operations Manager は Service Monitor トラップのイベントの生成、Service Quality Alerts ダッシュボードでのイベントの表示、および最大 30 日間のイベント履歴の格納を実行できます。詳細については、『*User Guide for Cisco Unified Operations Manager*』を参照してください。

図 4-1 に、Operations Manager とともにインストールされた Service Monitor および Cisco 1040 を示します。

図 4-1　Service Monitor の構成



1	Cisco 1040 は、実際の音声コールを監視します。	**3**	Operations Manager がアラート情報を提供します。
2	Service Monitor は MOS 値を評価し、しきい値を超えている場合は SNMP トラップを送信します。また Service Monitor は、Cisco 1040 が到達不能の場合にも、SNMP トラップを送信します。	**—**	—

詳細については、次の項を参照してください。

- Cisco 1040 到達不能トラップについて（P.4-20）
- 使用される MIB と生成される SNMP トラップ（P.C-1）

Service Monitor でのセンサーの初期設定の実行

センサーを設定するには、次の手順を実行します。

1. 使用する Service Monitor およびセンサー用に、TFTP サーバを 1 台または複数追加します。P.4-3 の「センサーのコンフィギュレーション ファイルおよびイメージ ファイル用の TFTP サーバの設定」を参照してください。
2. Service Monitor サーバから TFTP サーバに、バイナリ イメージ ファイルをコピーします。
3. デフォルトのコンフィギュレーション ファイルを作成します。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。

   Service Monitor は、センサーのコンフィギュレーション ファイルを設定した各 TFTP サーバにコピーします。センサーをネットワークに接続すると、センサーは TFTP サーバからコンフィギュレーション ファイルをダウンロードしてから、Service Monitor に登録されます。詳細については、P.4-16 の「センサーが Service Monitor に登録されるしくみについて」を参照してください。

センサーのコンフィギュレーション ファイルおよびイメージ ファイル用の TFTP サーバの設定

Service Monitor は、コンフィギュレーション ファイルおよびバイナリ イメージ ファイルをセンサーに提供するために、1 台または複数の TFTP サーバを使用します。このため、1 台以上の TFTP サーバを Service Monitor 用に定義する必要があります。追加の TFTP サーバを、バックアップとして設定したり、複数の DHCP スコープがある場合に設定したりできます。

センサーを追加または編集すると、Service Monitor はサーバ上でローカルにコンフィギュレーション ファイルをアップデートし、それからコンフィギュレーション ファイルを既知のすべての TFTP サーバにコピーします。コンフィギュレーション ファイルのコピーを各 TFTP サーバに保存することにより、セカンダリ Service Monitor へ効率的にフェールオーバーできます。

TFTP サーバ上で書き込みエラーが発生した場合、Service Monitor が TFTP サーバに保存しているコンフィギュレーション ファイルを使用できます。この場合、Service Monitor から、Service Monitor 用に設定されている各 TFTP サーバにコンフィギュレーション ファイルを手動でコピーできます（TFTP サーバのコンフィギュレーション ファイルを確認するには、P.4-14 の「TFTP サーバ上のコンフィギュレーション ファイルのセンサーからの表示」を参照してください）。

センサーのバイナリ イメージ ファイルは、Service Monitor に追加する各 TFTP サーバにコピーする必要があります。P.4-4 の「バイナリ イメージ ファイルの TFTP サーバへのコピー」を参照してください。

ステップ 1　**Configuration** > **Sensor** > **TFTP Servers** を選択します。TFTP Server Setup ページが表示され、次の表の情報が表示されます。

GUI の要素	説明 / 処理
チェックボックス	TFTP サーバを削除する場合に選択します。
TFTP Server	IP アドレスまたは DNS 名です。
Port	カスタム ポート番号は 69 です。
Add ボタン	TFTP サーバを追加する場合にクリックします。
Delete ボタン	チェックボックスを選択してからクリックすると、選択した TFTP サーバが削除されます。

TFTP サーバの追加

センサーを Service Monitor に登録するには、Service Monitor がセンサーにコンフィギュレーション ファイルを提供するための TFTP サーバを 1 台以上定義する必要があります。追加の TFTP サーバを、たとえばバックアップとして設定したり、複数の DHCP スコープがある場合に設定したりできます。

（注） Cisco Unified CallManager 5.x または 4.2 を TFTP サーバとして使用できます。Cisco Unified CallManager のセキュリティ設定により、Service Monitor がコンフィギュレーション ファイルをアップロードできない場合があります。このような場合、コンフィギュレーション ファイルおよびイメージ ファイルを Service Monitor から Cisco Unified CallManager TFTP サーバへ手動でコピーする必要があります。

ステップ 1　**Configuration > Sensor > TFTP Servers** を選択します。TFTP Server Setup ページが表示されます。

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

ステップ 3　次のフィールドにデータを入力します。

- TFTP Server：IP アドレスまたは DNS 名
- Port Number：カスタム ポート番号は 69

ステップ 4　**OK** をクリックします。

（注） バイナリ イメージ ファイルを、Service Monitor に追加する各 TFTP サーバにコピーします。

バイナリ イメージ ファイルの TFTP サーバへのコピー

ステップ 1　バイナリ イメージ ファイル SvcMonAA2_34.img を、Service Monitor サーバの *NMSROOT*\ImageDir から TFTP サーバの root ロケーションにコピーします (*NMSROOT* は Service Monitor がインストールされているディレクトリ。デフォルトの場所は C:\Program Files\CSCOpx)。

TFTP サーバの削除

ステップ 1　**Configuration > Sensor > TFTP Servers** を選択します。TFTP Server Setup ページが表示されます。

ステップ 2　チェックボックスを選択します。

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　**Yes** をクリックします。

センサーのデフォルト設定の設定

次の手順を実行します。

- コール メトリックのアーカイブをイネーブルまたはディセーブルにします。Service Monitor は MOS データをデータベースに保存します。オプションで、MOS データをファイルに保存することもできます。
- アーカイブ データ ファイルおよび Cisco 1040 イメージ ファイルのディレクトリ パスを表示します。
- デフォルトのコンフィギュレーション ファイル QOVDefault を作成します。CNF は、センサーが登録されるプライマリ Service Monitor およびセカンダリ Service Monitor を指定します。

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

ステップ 2　次の表に説明されているデータをアップデートします。

GUI の要素	説明 / 処理
Call Metrics Archiving オプション ボタン	次のいずれかを選択します。 • Enable：分析後、Service Monitor は Cisco 1040 からのデータをディスク ファイルに保存します。 • Disable：分析後、Service Monitor はデータを廃棄します。 デフォルト：Disable
Data File Directory	コール メトリックのアーカイブがイネーブルになっている場合に、ファイルが保存されるディレクトリ。このフィールドは編集できません。 **（注）** コール メトリックは、*NMSROOT*/DataDir にアーカイブされます (*NMSROOT* は Service Monitor がインストールされているディレクトリ。デフォルトの場所は C:\Program Files\CSCOpx)。
Image File Directory	センサーのバイナリ イメージ ファイルおよびコンフィギュレーション ファイルが、ローカルに保存されるディレクトリ *NMSROOT*/ImageDir。*NMSROOT* は Service Monitor がインストールされているディレクトリで、デフォルトの場所は C:\Program Files\CSCOpx です。 このフィールドは編集できません。 **（注）** 詳細については、P.4-17 の「センサー上のイメージ ファイルのアップデート」を参照してください。
Send traps every *n* minutes per endpoint	5 以上の数字を入力します。センサーは 60 秒ごとにデータを Service Monitor に送信します。Service Monitor は、しきい値を超えたかどうかを判断し、そのエンドポイントに 60 秒ごとにトラップを送信する可能性があります。この設定を使用して、Service Monitor がエンドポイントに送信するトラップ数を減らします。特定のエンドポイントに対し、*n* 分ごとにトラップを送信し、その間の追加トラップを抑制します（送信しない）。

GUI の要素	説明 / 処理
TFTP サーバに対するデフォルト設定	
Image Filename	新しいイメージをダウンロードした場合、そのイメージのファイル名を入力します。P.4-17 の「センサー上のイメージ ファイルのアップデート」を参照してください。
Primary Service Monitor	プライマリ Service Monitor の IP アドレスまたは DNS 名
Secondary Service Monitor	セカンダリ Service Monitor の IP アドレスまたは DNS 名。設定されていない場合は空白（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）。

ステップ 3　**OK** をクリックします。Service Monitor はコンフィギュレーション ファイルをローカルに保存し、Service Monitor に追加されている TFTP サーバにコンフィギュレーション ファイルをコピーします。詳細については、P.4-3 の「センサーのコンフィギュレーション ファイルおよびイメージ ファイル用の TFTP サーバの設定」を参照してください。

（注）　Cisco Unified CallManager 5.x または 4.2 を TFTP サーバとして使用している場合、デフォルトのコンフィギュレーション ファイルを、Service Monitor サーバのイメージ ファイル ディレクトリから Cisco Unified CallManager TFTP サーバに手動でアップロードする必要があります。

Service Monitor でのセンサーの設定

（注）　Cisco 1040 を適切に動作させるには、DHCP および DNS を正しく設定する必要があります。詳細については、『*Quick Start Guide for Cisco 1040 Sensor*』を参照してください。

Cisco 1040 を管理するために、次の情報を使用できます。

- Cisco 1040 Sensor Details ページについて（P.4-7）
- センサーの Service Monitor への追加（P.4-9）
- 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（P.4-10）
- センサーのリセット（P.4-12）
- センサーの削除（P.4-12）

Cisco 1040 Sensor Details ページについて

ステップ 1　**Configuration** > **Sensor** > **Management** を選択します。Cisco 1040 Sensor Details ページに、次の表に示す情報が表示されます。

GUI の要素	説明 / 処理
	Cisco 1040 Sensor Details ページから CSV または PDF ファイルにデータをエクスポートします。P.4-8 の「データの CSV または PDF ファイルへのエクスポート」を参照してください。
	ブラウザ ウィンドウから印刷する場合に、印刷用のデータを表示した別のウィンドウを開きます。
Check box カラム	編集、リセット、または削除する Cisco 1040 を選択します。
Name カラム	名前のリンクをクリックして、Cisco 1040 の設定の詳細を表示します。P.4-13 の「Service Monitor での特定センサーの詳細の表示」を参照してください。
Sensor Address カラム	Cisco 1040 の MAC アドレスおよび IP アドレスを表示します。MAC アドレスのリンクをクリックすると、Cisco 1040 に HTML ページが開きます（P.4-14 の「センサーの Web インターフェイスを使用した設定の表示」を参照）。

GUI の要素	説明 / 処理
Service Monitor カラム	次が表示されます。 • Primary：Cisco 1040 に定義されているプライマリ Service Monitor の IP アドレスまたはホスト名 • Secondary：Cisco 1040 に定義されているセカンダリ Service Monitor の IP アドレスまたはホスト名 • Registered with：Cisco 1040 が現在データを送信している Service Monitor の IP アドレスまたはホスト名。センサーが未登録の場合、Waiting と表示されます。 **（注）** システムの時刻を変更したばかりだったり、QOVR プロセスの停止と起動を続けて行ったりすると、Cisco 1040 から syslog メッセージを受信し処理しているのに、Service Monitor がこの Cisco 1040 について Waiting と表示する場合があります。この問題を解決するには、P.4-8 の「Service Monitor のセンサー登録情報をアップデートするプロセスの再起動」を参照してください。
Reset Time カラム	Cisco 1040 が最後にリブートされた日付と時刻
Edit ボタン	このボタンをクリックして、Cisco 1040 の設定を編集します。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。

Service Monitor のセンサー登録情報をアップデートするプロセスの再起動

Cisco 1040 から syslog を受信し処理しているのに、Service Monitor が Waiting と表示する場合があります。この問題は、ユーザが次のいずれかの操作を行った場合に発生します。

- **pdterm** を使用して QOVR プロセスを停止し、すぐに **pdexec** を使用して QOVR プロセスを再起動した。この問題を防ぐには、QOVR プロセスの停止と再起動の間隔を 5 分以上あけます。この問題を解決するには、次の手順を実行します。
  1. コマンドラインから次のコマンドを入力して、QOVR プロセスを再び停止します。

     ```
     pdterm QOVR
     ```

  2. 5 分以上待ちます。
  3. 次のコマンドを入力します。

     ```
     pdexec QOVR
     ```

- Service Monitor がインストールされているシステムの時刻を変更し、その後でデーモン マネージャの停止と再起動を行わなかった。この問題を解決するには、コマンドラインから次のコマンドを入力して、デーモン マネージャの停止と起動を行います。

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

データの CSV または PDF ファイルへのエクスポート

エクスポート アイコンをクリックすると、ダイアログボックスが表示されます。

ステップ 1　CSV または PDF オプション ボタンを選択します。

ステップ 2　ファイルを保存する場所を参照して選択し、**OK** をクリックします。

センサーの Service Monitor への追加

センサーが Service Monitor に登録済みの場合、そのセンサーを選択して Edit ボタンをクリックし、アップデートする必要があります。詳細については、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。

ステップ 1　**Configuration** > **Sensor** > **Management** を選択します。Cisco 1040 Sensor Default 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 a Cisco 1040 Sencor ダイアログボックスが表示されます。

ステップ 3　次の表に示すデータを入力します。

GUI の要素	説明 / 処理
Sensor Name	最大 20 文字を入力します。この名前は、Service Monitor ウィンドウでレポートなどに使用されます。 **(注)** センサー名は、一意である必要はありません。デフォルトのコンフィギュレーション ファイルを使用して Service Monitor に登録されているセンサーは、すべて Cisco 1040 という名前を使用します。
Image File Name	バイナリ イメージ ファイル名を入力します。ファイル名の形式は、次のとおりです。 SvcMon< ベンダー コード ><Cisco 1040 のタイプ >< メジャー バージョン >_< マイナー バージョン >< バグフィックス バージョン >.img。次の例を参考にしてください。 `SvcMonAA2_34.img` 詳細については、P.4-14 の「センサーの Web インターフェイスを使用した設定の表示」および P.4-17 の「センサー上のイメージ ファイルのアップデート」を参照してください。
MAC Address	追加する Cisco 1040 の MAC アドレスを入力します。
Primary Service Monitor	Service Monitor がインストールされているホストの IP アドレスまたは DNS 名を入力します。Service Monitor が到達不能でないかぎり、Cisco 1040 はこの Service Monitor にデータを送信します。
Secondary Service Monitor	（オプション）Service Monitor の別のインスタンスがインストールされているホストの IP アドレスまたは DNS 名を入力します。プライマリ Service Monitor が到達不能な場合にだけ、Cisco 1040 はこの Service Monitor にデータを送信します。詳細については、P.4-14 の「センサーの Web インターフェイスを使用した設定の表示」を参照してください。
Description	最大 80 文字を入力します。

ステップ 4　**OK** をクリックします。コンフィギュレーション ファイルは、Service Monitor がインストールされているサーバに保存され、すべての TFTP サーバにコピーされます（P.4-3 の「センサーのコンフィギュレーション ファイルおよびイメージ ファイル用の TFTP サーバの設定」を参照）。コンフィギュレーション ファイルの名前は QOV<*MAC アドレス* >.CNF です。ここで、<*MAC アドレス* > は Cisco 1040 の MAC アドレスです（MAC アドレスの表示については、P.4-14 の「センサーの Web インターフェイスを使用した設定の表示」を参照してください）。

（注） Cisco Unified CallManager 5.x または 4.2 を TFTP サーバとして使用している場合、MAC 固有のコンフィギュレーション ファイルを、Service Monitor サーバのイメージ ファイル ディレクトリから Cisco Unified CallManager TFTP サーバに手動でアップロードする必要があります。イメージ ファイル ディレクトリは *NMSROOT*/ImageDir です。*NMSROOT* は Service Monitor がインストールされているディレクトリで、デフォルトの場所は C:\Program Files\CSCOpx です。

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

（注） Cisco 1040 コンフィギュレーション ファイルは、テキスト エディタを使用して編集しないでください。Cisco 1040 コンフィギュレーション ファイルは、次の手順でだけ編集できます。

ステップ 1　**Configuration > Sensor > Management** を選択します（詳細については、P.4-7 の「Cisco 1040 Sensor Details ページについて」を参照してください）。

ステップ 2　センサーのチェックボックスを選択し、**Edit** をクリックします。

ステップ 3　次のフィールドをアップデートします。

フィールド	説明 / 処理
Sensor Name	名前を変更する場合、最大 20 文字を入力します。この名前は、Service Monitor ウィンドウでレポートなどに使用されます。
MAC Address	Cisco1040 MAC アドレス **（注）** このフィールドは編集できません。
IP Address	Cisco1040 IP アドレス **（注）** このフィールドは編集できません。センサーの IP アドレスをアップデートするには、センサーをいったん Service Monitor から削除し、再び追加します。

フィールド	説明 / 処理
Image File Name	バイナリ イメージ ファイル名を入力します。ファイル名の形式は、次のとおりです。 SvcMon< ベンダー コード ><Cisco 1040 のタイプ >< メジャー バージョン >_< マイナー バージョン >< バグフィックス バージョン >.img。次の例を参考にしてください。 `SvcMonAA2_34.img` それぞれの説明は次のとおりです。 • A は、この Cisco 1040 のベンダー コードです（内部使用）。 • A は、Cisco 1040 のタイプです（内部使用）。 • 2 は、メジャー リリース番号です。 • 3 は、マイナー リリース番号です。 • 4 は、バグフィックス番号です。 詳細については、P.4-14 の「センサーの Web インターフェイスを使用した設定の表示」および P.4-17 の「センサー上のイメージ ファイルのアップデート」を参照してください。
Primary Service Monitor	Service Monitor がインストールされているホストの IP アドレスまたは DNS 名を入力します。Service Monitor が到達不能でないかぎり、Cisco 1040 はこの Service Monitor にデータを送信します。
Secondary Service Monitor	（オプション）Service Monitor がインストールされているホストの IP アドレスまたは DNS 名を入力します。プライマリ Service Monitor が到達不能な場合にだけ、Cisco 1040 はこの Service Monitor にデータを送信します。
Description	最大 80 文字を入力します。

ステップ 4　**OK** をクリックします。Service Monitor はコンフィギュレーション ファイルをローカル サーバに保存し、すべての TFTP サーバにコピーします。次に Service Monitor はセンサーをリセットし、センサーがアップデートされたコンフィギュレーション ファイルをロードできるようにします。

（注） Cisco Unified CallManager 5.x または 4.2 を TFTP サーバとして使用している場合、アップデートされたコンフィギュレーション ファイルを、Service Monitor サーバのイメージ ファイル ディレクトリから Cisco Unified CallManager TFTP サーバに手動でアップロードする必要があります。その後、センサーをリセットする必要があります（イメージ ファイル ディレクトリは *NMSROOT*/ImageDir です。*NMSROOT* は Service Monitor がインストールされているディレクトリで、デフォルトの場所は C:\Program Files\CSCOpx です）。

センサーのリセット

次の手順で、Cisco 1040 をブートします。Cisco 1040 はブートすると、最初に DHCP を使用して TFTP サーバの IP アドレスを取得します。Cisco 1040 は、TFTP サーバからコンフィギュレーション ファイルを取得します。コンフィギュレーション ファイルに、現在インストールされているイメージとは異なるバイナリ イメージ ファイルが指定されている場合、Cisco 1040 は、TFTP サーバからそのバイナリ イメージ ファイルも取得します。

ステップ 1　**Configuration** > **Sensor** > **Management** を選択します（詳細については、P.4-7 の「Cisco 1040 Sensor Details ページについて」を参照してください）。

ステップ 2　リセットする Cisco 1040 のチェックボックスを選択します。

ステップ 3　**Reset** をクリックします。

センサーの削除

次の手順を実行する前に、すべてのセンサーしきい値グループからセンサーを削除しておく必要があります。P.5-11 の「センサー グループの編集」を参照してください。

ステップ 1　Cisco 1040 のコンフィギュレーション ファイル（QOV*macaddress*.CNF）を TFTP サーバから削除します。

ステップ 2　**Configuration** > **Sensors** を選択します。Cisco 1040 Sensor Details ページが開きます（詳細については、P.4-7 の「Cisco 1040 Sensor Details ページについて」を参照してください）。

ステップ 3　削除する Cisco 1040 のチェックボックスを選択します。

ステップ 4　**Delete** をクリックします。次のいずれかが表示されます。

- 確認のダイアログボックスが表示される。
- エラー メッセージが表示され、削除しようとしているセンサーが属しているセンサーしきい値グループのリストが表示される。これらのセンサーしきい値グループからセンサーを削除して、上記の手順をやり直す必要があります。

ステップ 5　**OK** をクリックします。

センサーの設定の表示

Cisco 1040 センサーの設定データは Service Monitor に保存され、これが各 TFTP サーバ上のセンサーのコンフィギュレーション ファイルにコピーされ、さらにこれがセンサーにコピーされます（センサーは TFTP サーバからコンフィギュレーション ファイルをダウンロードします）。保存されている Cisco 1040 センサーの設定の詳細は、Service Monitor、TFTP サーバ、およびセンサー自体でそれぞれ表示することができます。

- Service Monitor での特定センサーの詳細の表示（P.4-13）
- TFTP サーバ上のコンフィギュレーション ファイルのセンサーからの表示（P.4-14）
- センサーの Web インターフェイスを使用した設定の表示（P.4-14）

Service Monitor での特定センサーの詳細の表示

Cisco 1040 Sensor Detail ダイアログボックスを開くには、Cisco 1040 Sensor Details ページ上の名前のリンクをクリックします。Cisco 1040 Sensor Detail ダイアログボックスには、次に説明する Cisco 1040 Sensor Information テーブルが表示されます。

フィールド	説明 / 処理
	Cisco 1040 Sensor Information テーブルから CSV または PDF ファイルにデータをエクスポートします。P.4-8 の「データの CSV または PDF ファイルへのエクスポート」を参照してください。
	ブラウザ ウィンドウから印刷する場合に、印刷用のデータを表示した別のウィンドウを開きます。
	文脈依存オンライン ヘルプを開きます。
Name link	Cisco 1040 ユーザが入力した名前：クリックすると、Cisco 1040 の Web インターフェイスが開きます。P.4-14 の「センサーの Web インターフェイスを使用した設定の表示」を参照してください。
MAC Address	Cisco 1040 MAC アドレス
IP Address	Cisco 1040 IP アドレス
Primary Service Monitor	プライマリ Service Monitor の IP アドレスまたは DNS 名
Secondary Service Monitor	セカンダリ Service Monitor の IP アドレスまたは DNS 名。設定されていない場合は空白（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）。
Registered with	Cisco 1040 が登録されている Service Monitor の IP アドレスまたは DNS 名。
Image File Name	Cisco 1040 にインストールされているイメージ ファイルの名前。 **（注）** TFTP サーバ上に使用可能な最新のイメージ ファイルがある場合は、Cisco 1040 のコンフィギュレーション ファイルを編集して最新のイメージのファイル名を指定し、Cisco 1040 をリセットする必要があります（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）。
Last Reset Time	Cisco 1040 が最後にリセットされた日付と時刻（P.4-12 の「センサーのリセット」を参照）。
Description	ユーザが入力した Cisco 1040 の説明（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）。

TFTP サーバ上のコンフィギュレーション ファイルのセンサーからの表示

ステップ 1　ブラウザで、http://*<IP アドレスまたは DNS 名>*/Communication と入力します。ここでの IP アドレスは Cisco 1040 のアドレス、DNS 名は Cisco 1040 の DNS 名です。たとえば、次のようになります。

```
http://Cisco-1040-sj/Communication
```

ステップ 2　Communication Log File ウィンドウに、TFTP サーバ上の Cisco 1040 のコンフィギュレーション ファイルからの次の情報が表示されます。

- Receiver：コンフィギュレーション ファイルに定義されている各 Service Monitor（プライマリおよびセカンダリ）の IP アドレスまたは DNS 名。セミコロンで区切られます。
- ID：ユーザ定義の、このコンフィギュレーション ファイルを使用する Cisco 1040 の名前
- Image：Cisco 1040 が TFTP サーバからダウンロードして実行するバイナリ イメージ ファイルの名前
- Last Updated：Service Monitor システムで、このコンフィギュレーション ファイルが最後にアップデートされた時刻
- CDPGlobalRunState：CDP がイネーブル（true）かディセーブル（false）かを示します。
- SyslogPort：syslog を Service Monitor に送信するのに使用するポート プロトコル（UDP）およびポート番号を示します。
- SkinnyPort：Service Monitor との通信に使用するポート プロトコル（TCP）およびポート番号を示します。

センサーの Web インターフェイスを使用した設定の表示

Web インターフェイスを使用して、TFTP サーバ上にある Cisco 1040 のコンフィギュレーション ファイルの内容を表示するには、P.4-14 の「TFTP サーバ上のコンフィギュレーション ファイルのセンサーからの表示」を参照してください。

次のいずれかの方法で、Web インターフェイスを開いて Cisco 1040 に保存されている情報を表示できます。

- Cisco 1040 Sensor Details ページの **(View)** リンクをクリックします。P.4-7 の「Cisco 1040 Sensor Details ページについて」を参照してください。
- ブラウザに http://*<IP アドレス>* と入力します。ここでの IP アドレスは Cisco 1040 のアドレスです。

Cisco 1040 Web インターフェイスに、次の情報を示す Cisco 1040 Information ウィンドウが表示されます。

- **ID**：Cisco 1040 の MAC アドレス
- **MAC Address**：Cisco 1040 の MAC アドレス
- **Time stamp**：Cisco 1040 上の現在の時刻
- **Status**：Cisco 1040 のステータス。次のいずれかになります。
  - operational：Cisco 1040 は RTP ストリームの受信、データの分析、Service Monitor へのデータ送信を実行中です。
  - not communicating with receiver：Service Monitor は到達不能です。
- **Current Service Monitor**：Cisco 1040 がデータを送信している Service Monitor の名前。これは、プライマリ Service Monitor またはセカンダリ Service Monitor です。

- **TFTP IP Address**：Cisco 1040 のバイナリ イメージ ファイルおよびコンフィギュレーション ファイルのダウンロード元となる TFTP サーバ
- **Switch IP Address**：Cisco 1040 が接続されているスイッチ
- **Switch Port**：Cisco 1040 が接続されているスイッチ ポート
- **Software Version**：Cisco 1040 にインストールされているバイナリ イメージ ファイルの名前。P.4-17 の「センサー上のイメージ ファイルのアップデート」を参照してください。
- **Last Updated**：Service Monitor 上で Cisco 1040 の設定が最後にアップデートされた時刻。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。

センサーの Service Monitor への登録について

センサーのデフォルトのコンフィギュレーション ファイル QOVDefault.CNF を設定すると、センサーは自動的に Service Monitor に登録されます。センサーが自動的に登録されると、Service Monitor はデフォルトのコンフィギュレーション ファイルの情報を使用して、新しく登録されたセンサー用に MAC 固有のコンフィギュレーション ファイル QOV*macaddress*.CNF を作成します。センサーのデフォルトのコンフィギュレーション ファイルが作成されたら、センサーを手動で Service Monitor に追加する場合は、追加してからセンサーを接続します。

Cisco 1040 はスイッチに接続されると、DHCP を使用して TFTP サーバの IP アドレスを取得します。Cisco 1040 は、TFTP サーバでコンフィギュレーション ファイルをチェックし、次のうち最初に検出したファイルを使用します。

- QOV*macaddress*.CNF：macaddress は、Cisco 1040 の MAC アドレスです。
- QOVDefault.CNF：デフォルトのコンフィギュレーション ファイルは、Cisco 1040 固有のコンフィギュレーション ファイルが見つからなかった場合に使用されます（P.4-5 の「センサーのデフォルト設定の設定」を参照）。

センサーが Service Monitor に登録されるしくみについて

新しく接続されたセンサーは、そのセンサー固有のコンフィギュレーション ファイル QOV<*MAC アドレス*>.CNF を使用して、またはデフォルトのコンフィギュレーション ファイル QOVDefault.CNF を使用して Service Monitor に登録されます。デフォルトのコンフィギュレーション ファイルを使用する場合、Service Monitor はこのファイルから MAC 固有のコンフィギュレーション ファイル QOV<*MAC アドレス*>.CNF をそのセンサー用に作成します。

TFTP サーバ上のデフォルトのコンフィギュレーション ファイルは 1 つだけです。デフォルトのコンフィギュレーション ファイルによって、プライマリ Service Monitor が指定されます。このため、同じ TFTP サーバを使用するセンサーは、同じデフォルトのコンフィギュレーション ファイルを使用し、同じプライマリ Service Monitor に登録されます。

センサーのセカンダリ Service Monitor へのフェールオーバーについて

Cisco 1040 は、登録先の Service Monitor にキープアライブ メッセージを送信し、その Service Monitor から確認応答を受信します。3 回キープアライブを送信しても確認応答を受信できない場合、Cisco 1040 はセカンダリ Service Monitor へのフェールオーバー処理を開始します。

1. Cisco 1040　は、コンフィギュレーション　ファイルにリストされているセカンダリ　Service Monitor にキープアライブを送信し、確認応答を受け取るとその Service Monitor に登録します。
2. セカンダリ Service Monitor は、Cisco 1040 の最新のコンフィギュレーション ファイルを TFTP サーバから取得して、Cisco 1040 をフェールオーバー Cisco 1040 として登録します。
3. Cisco 1040 は、プライマリ Service Monitor が回復したかどうかを判断するために引き続きキープアライブを送信する一方で、セカンダリ Service Monitor への syslog メッセージの送信を開始します。セカンダリ Service Monitor は、フェールオーバー Cisco 1040 からの syslog メッセージを処理します。
4. プライマリ Service Monitor が回復すると、Cisco 1040 はセカンダリ Service Monitor の登録を解除し、プライマリ Service Monitor に再登録します。

センサー上のイメージ ファイルのアップデート

ステップ 1　新しいイメージ ファイルが入手可能な場合は、Cisco ソフトウェアのダウンロード サイトからダウンロードします。

a. ブラウザで http://www.cisco.com を参照します。

b. **Technical Support & Documentation > Downloads** を選択します。

c. Cisco Unified Service Monitor のリンクをクリックし、使用可能なイメージを確認してダウンロードします。

ステップ 2　次の両方にイメージ ファイルをコピーします。

- Service Monitor をインストールしたときに指定したイメージ ファイル ディレクトリ：ローカル コピーをバックアップとして保持するため、イメージ ファイルをここにコピーします。イメージ ファイル ディレクトリ パスについては、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。
- TFTP サーバ：イメージを使用するように設定された Cisco 1040 がアクセスできるように、ファイルをここにコピーします。TFTP サーバ アドレスについては、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。

（注）　イメージ ファイル名の形式は、次のとおりです。
SvcMon< ベンダー コード ><Cisco 1040 のタイプ >< メジャー バージョン >_< マイナー バージョン >< バグフィックス バージョン >.img。たとえば、SvcMonAA2_34.img など。

ステップ 3　各 Cisco 1040 の設定を変更して、新しいイメージ ファイル名を入力します。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。

センサーの移動

警告　**センサーを移動する前に、『*Quick Start Guide for Cisco 1040 Sensor*』の規制および安全上の情報をお読みください。**

ステップ 1　（オプション）新しいプライマリ Service Monitor を参照するように Cisco 1040 を設定する場合は、このステップを実行します。Cisco 1040 のコンフィギュレーション ファイルを編集します。詳細については、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。

ステップ 2　Cisco 1040 を切断します。

ステップ 3　新しい場所で Cisco 1040 を接続します。Cisco 1040 は、TFTP サーバからコンフィギュレーション ファイルをダウンロードします。

（注）　Cisco 1040 は、移動後も自身の名前を保持します。

センサーのコール メトリック アーカイブ ファイルについて

Service Monitor は Cisco 1040 から受信したデータをデータベースに保存し、データベースはこのデータをレポート用に 30 日間保存します。コール メトリックのアーカイブをイネーブルにした場合、Service Monitor はデータをサーバ上のディレクトリに保存することもできます。コール メトリックのアーカイブをイネーブルまたは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。

Service Monitor は、毎日午前 0 時に新しいデータ ファイルを作成します。データ ファイル名は QoV_*YYYYMMDD*.csv です。ここで、*YYYY* は 4 桁の年、*MM* は 2 桁の月、*DD* は 2 桁の日です。たとえば、QOV_20061101.csv は 2006 年 11 月 1 日のデータ ファイルです。Service Monitor は、サイズ制限を超えたデータ ファイルをバックアップしたり、古いデータ ファイルを削除したりできます。詳細については、P.6-4 の「センサー アーカイブ ファイルの消去について」を参照してください。

詳細な分析にデータを使用したり、アーカイブをディセーブルにしたりできます (Service Monitor は他のアプリケーションにアーカイブされたデータを送信しません)。表 4-1 に、コール メトリック データ ファイルの形式を示します。

表 4-1　Service Monitor アーカイブ コール メトリックのファイル形式

説明	値
Cisco 1040 MAC アドレス	Cisco 1040 センサーの MAC アドレス
タイム スタンプ	日付および時刻
送信元デバイスの IP アドレス	IPv4 アドレス。次に例を示します。 172.020.119.043
宛先デバイスの IP アドレス	IPv4 アドレス。次に例を示します。 172.020.119.025
コール データ レコードのコーデック	2：G711Alaw 64k 3：G711Alaw 56k 4：G711Ulaw 64k 5：G711Ulaw 56k 6：G722 64k 7：G722 56k 8：G722 48k 10：G728 11：G729 12：G729AnnexA 15：G.729AnnexB 16：G729AnnexAwAnnexB
計算された MOS スコア	1 桁目と 2 桁目の間に暗黙の小数点が含まれる 2 桁の数値
コール劣化の主な原因	J：ジッタ P：パケット損失
直前の 1 分間に失われた実際のパケット数	< 数値 >
直前の 1 分間に生じた実際のジッタ（ミリ秒単位）	< 数値 >

(注)　コール メトリック データ ファイルは、ディスクに 30 日間保存されます。その後、Service Monitor はこれらのファイルを削除します。これらのファイルを保存する場合は、ディスクの一般的なバックアップ方法を使用して、ファイルをバックアップする必要があります。詳細については、P.6-4 の「センサー アーカイブ ファイルの消去について」を参照してください。

Cisco 1040 到達不能トラップについて

Service Monitor は、登録されている Cisco 1040 からのキープアライブの受信が停止すると、Cisco 1040 到達不能 SNMP トラップを生成します。Service Monitor は、このトラップを最大 4 つの受信先に送信します。詳細については、P.4-5 の「センサーのデフォルト設定の設定」および P.C-1 の「使用される MIB と生成される SNMP トラップ」を参照してください。

(注)　Service Monitor からトラップを受信するように Operations Manager を設定している場合、Cisco 1040 到達不能トラップは、Alerts and Events モニタリング ダッシュボード上で、不明のトラップ デバイス タイプとして表示されます。

Cisco Unified CallManager の到達可能性の詳細については、P.3-7 の「最後の接続ステータスと資格情報の検証時期について」を参照してください。

CHAPTER 5

しきい値の設定

この項では次のトピックについて説明します。

しきい値およびしきい値グループについて

Service Monitor は、MOS 値（センサーから報告されるか、Cisco Unified CallManager クラスタからの CDR に含まれている）が到達不能レベルに下がっているかどうかを判断するのに、しきい値を使用します。MOS 値がしきい値を下回った場合、Service Monitor は QoVMOSViolation トラップを最大 4 つのトラップ レシーバに送信します。

Service Monitor には、グローバルなしきい値とそれらのデフォルト値を設定してあります。Service Monitor は、グローバルなしきい値をセンサーやクラスタから報告される MOS 値と比較します。コールに使用されているコーデックによって MOS のしきい値が異なる場合があるため、グローバルなしきい値には、次のような一般に使用されているコーデックに対応したさまざまな値が含まれています。

- G711Alaw64k
- G711Alaw56k
- G711Ulaw64k
- G711Ulaw56k
- G722 64K
- G722 56k
- G722 48k
- G728
- G729
- G729AnnexA
- G729AnnexB
- G729AnnexAwAnnexB

(注) コーデックの詳細については、次の URL で 『*Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation*』を参照してください。
URL: http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml

グローバルなしきい値のデフォルト値をアップデートして、システムの平均 MOS 値を下回る MOS 値を反映させることができます。Service Monitor のレポートを観察して平均 MOS 値を決定し、その値に応じてグローバルなしきい値を調整できます。また、グローバルなしきい値を、Service Monitor で定められたデフォルト値に戻すことも簡単にできます。

特定のセンサー、クラスタ、またはセンサーかクラスタから報告されるエンドポイント グループに対して別のしきい値を使用する場合、次のしきい値グループを追加して、グローバルなしきい値を無効にすることができます。

- CVTQ グループ：CVTQ グループは、1 つまたは複数のクラスタ、2 組のエンドポイント、および一般に使用されているコーデックに対する 1 つまたは複数のしきい値で構成されます。
- センサー グループ：センサー グループは、1 つまたは複数のセンサー、2 組のエンドポイント、および一般に使用されているコーデックに対する 1 つまたは複数のしきい値で構成されます。

最大 10 個の CVTQ グループと最大 10 個のセンサー グループを作成できます。CVTQ グループには、最も高いレベル（1）から最も低いレベル（10）までの優先レベルがつけられます。これは、センサー グループも同様です。1 つのエンドポイントが複数の CVTQ グループまたは複数のセンサー グループに属する場合、Service Monitor はそのエンドポイントの MOS を、最も高い優先レベルのグループと比較します。

詳細については、次の項を参照してください。

- グローバルなしきい値の設定（P.5-3）
- CVTQ グループの設定（P.5-4）
- センサー グループの設定（P.5-9）

グローバルなしきい値の設定

適用可能な CVTQ グループまたはセンサー グループが設定されていない場合、Service Monitor は、センサーおよびクラスタから報告される MOS をグローバルなしきい値と比較します。グローバルなしきい値は、削除もクリアもできません。グローバルなしきい値をアップデートし、後でデフォルト値に戻すことができます。ユーザ定義のしきい値グループを作成して、グローバルなしきい値を無効にすることができます。詳細については、P.5-4 の「CVTQ グループの設定」および P.5-9 の「センサー グループの設定」を参照してください。

グローバルなしきい値をアップデートするには、次の手順を実行します。

ステップ 1　**Thresholds > Global** を選択します。Global Thresholds ページが表示され、次の表の情報が表示されます。

フィールドおよびボタン	説明 / 処理
Codec	コーデック名。編集できないため、グレー表示されています。
MOS	
Suggested Default	コーデックの推奨デフォルト値。 編集できないため、グレー表示されています。
Current Value	0.0 ～ 5.0 の値を入力します。
Revert to Suggested Defaults ボタン	各コーデックの現在の値を推奨デフォルト値に戻す場合にクリックします。
Apply ボタン	変更内容を現在の値に適用する場合にクリックします。

ステップ 2　表中の任意のコーデックに新しい現在値を入力し、**Apply** をクリックします。

グローバルなしきい値のデフォルト値への復元

グローバルなしきい値を、Global Thresholds ページに表示されている推奨デフォルト値に戻すには、次の手順を実行します。

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

ステップ 2　**Revert to Suggested Defaults** ボタンをクリックします。

CVTQ グループの設定

CVTQ は、1 つまたは複数の Cisco Unified CallManager クラスタ、2 組のエンドポイント、および一般に使用されているコーデックに対する 1 つまたは複数のしきい値で構成されます。最大 10 個の CVTQ しきい値グループを定義できます。Service Monitor は、CVTQ しきい値グループに 1（最も高い優先レベル）から 10（最も低い優先レベル）の優先レベルをつけます。このレベルは、初めはグループの作成順につけられます（ユーザがグループの優先レベルを変更できます）。1 つのエンドポイントが複数の CVTQ グループに属する場合、Service Monitor は、最も高い優先レベルの CVTQ しきい値グループのしきい値を適用します。

ステップ 1　**Thresholds > CVTQ Groups** を選択します。CVTQ Threshold Group ページが表示され、最大 10 個のユーザ定義の CVTQ しきい値グループが、次の表の情報とともに表示されます。

フィールドおよびボタン	説明 / 処理
Check box カラム	CVTQ しきい値グループを削除する場合に選択します。
Name カラム	CVTQ しきい値グループの一意のユーザ定義名。
Priority カラム	最も高い優先レベルから最も低い優先レベルを示す、1 ～ 10 の数字です。優先レベルを変更するには、2 つ以上の CVTQ しきい値グループに対し、各グループのこのカラムに 1 桁または 2 桁の数字を入力し、**Update Priority** ボタンをクリックします。
Add ボタン	CVTQ しきい値グループ（最大 10 個の CVTQ しきい値グループ）を追加する場合に、クリックします。P.5-4 の「CVTQ しきい値グループの追加」を参照してください。
Edit カラム	このグループをアップデートする場合に、このカラムの Edit リンクをクリックします。P.5-6 の「CVTQ しきい値グループの編集」を参照してください。
Delete ボタン	CVTQ しきい値グループを削除する場合に、1 つまたは複数のチェックボックスを選択し、Delete ボタンをクリックします。
Update Priority ボタン	Priority カラムに一意の数字を入力した後にクリックします。CVTQ しきい値グループが優先レベル順に並べ替えられ、再びこのページが表示されます。

CVTQ しきい値グループの追加

CVTQ グループを追加すると、既存の CVTQ しきい値グループの中で最も低い優先レベルが割り当てられます。この優先レベルを調整するには、P.5-7 の「CVTQ しきい値グループの優先レベルのアップデート」を参照してください。

（注）　最大 10 個の CVTQ しきい値グループを追加できます。

ステップ 1　**Thresholds > CVTQ Groups** を選択します。CVTQ Threshold Groups 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 CVTQ Threshold Group ページが表示されます。

ステップ 3　次の表に示すデータを入力します。

GUI の要素	説明 / 処理
Group Name フィールド	名前を入力します。この名前は、すべての CVTQ グループ内で一意である必要があります。
Select Clusters リスト	リスト ボックスに「All current and future clusters.（現在および将来のすべてのクラスタ）」と表示されます。 **（注）** クラスタを選択しないと、現在管理されているクラスタおよび将来管理されるクラスタに、このグループのしきい値が適用されます。 次の手順でクラスタを選択します。 **1.** をクリックします。Select Clusters ダイアログボックスが表示され、Service Monitor が CMR および CDR から取得したクラスタ ID が表示されます。 **2.** チェックボックスを選択します。 **3.** **OK** をクリックします。 デフォルト：なし
Override Thresholds リスト	次の手順でしきい値をアップデートします。 **1.** をクリックします。MOS Threshold Settings ダイアログボックスが表示されます。 **2.** 1 つ以上のコーデックに対し、MOS しきい値を入力します。 **3.** **OK** をクリックします。
Endpoint 1	次のいずれかのオプション ボタンを選択して適切なデータを入力し、送信元または宛先エンドポイントを指定します。 • DN：電話番号。正確な電話番号を入力するか、ワイルドカード（x）を使用するか、数字とワイルドカードを組み合わせて電話番号の範囲を指定します。 • IP：IP アドレス。IP アドレスを入力するか、ワイルドカード（*）を使用するか、数字とワイルドカードを組み合わせて IP アドレスの範囲を指定します。 **（注）** 詳細については、P.2-4 の「エンドポイントの IP アドレスまたは電話番号の指定」を参照してください。
Endpoint 2	次のいずれかのオプション ボタンを選択して適切なデータを入力し、送信元または宛先エンドポイントを指定します。 • DN：電話番号。正確な電話番号を入力するか、ワイルドカード（x）を使用するか、数字とワイルドカードを組み合わせて電話番号の範囲を指定します。 • IP：IP アドレス。IP アドレスを入力するか、ワイルドカード（*）を使用するか、数字とワイルドカードを組み合わせて IP アドレスの範囲を指定します。 **（注）** 詳細については、P.2-4 の「エンドポイントの IP アドレスまたは電話番号の指定」を参照してください。

ステップ 4　**OK** をクリックします。CVTQ Threshold Group ページが表示され、最新の CVTQ しきい値グループがリストの最後（最も低い優先レベルの位置）に表示されます。

CVTQ しきい値グループの編集

（注） CVTQ しきい値グループの優先レベルを変更するには、P.5-7 の「CVTQ しきい値グループの優先レベルのアップデート」を参照してください。

ステップ 1　**Thresholds** > **CVTQ Groups** を選択します。CVTQ Threshold Groups ページが表示されます。

ステップ 2　グループを選択して **Edit** をクリックします。Edit CVTQ Threshold Group ページが表示されます。

ステップ 3　次の表に示すデータを入力します。

GUI の要素	説明 / 処理
Group Name フィールド	名前は変更できます。この名前は、すべての CVTQ グループ内で一意である必要があります。
Select Clusters リスト	クラスタを選択しないと、リスト ボックスに「All current and future clusters.（現在および将来のすべてのクラスタ）」と表示されます。 **（注）** クラスタの資格情報を削除したときに、クラスタがすでに CVTQ グループに含まれている場合、そのクラスタはグループに保持されます。 次の手順でクラスタを選択します。 1. をクリックします。Select Clusters ダイアログボックスが表示され、Service Monitor が CMR および CDR から取得したクラスタ ID が表示されます。 2. チェックボックスを選択します。 3. **OK** をクリックします。 **（注）** クラスタを選択しないと、現在管理されているクラスタおよび将来管理されるクラスタに、このグループのしきい値が適用されます。
Override Thresholds リスト	次の手順でしきい値をアップデートします。 1. をクリックします。MOS Threshold Settings ダイアログボックスが表示されます。 2. 1 つ以上のコーデックに対し、MOS しきい値を入力します。 3. **OK** をクリックします。

GUI の要素	説明 / 処理
Endpoint 1	次のいずれかのオプション ボタンを選択して適切なデータを入力し、送信元または宛先エンドポイントを指定します。 • DN：電話番号。正確な電話番号を入力するか、ワイルドカード（x）を使用するか、数字とワイルドカードを組み合わせて電話番号の範囲を指定します。 • IP：IP アドレス。IP アドレスを入力するか、ワイルドカード（*）を使用するか、数字とワイルドカードを組み合わせて IP アドレスの範囲を指定します。 (注)　詳細については、P.2-4 の「エンドポイントの IP アドレスまたは電話番号の指定」を参照してください。
Endpoint 2	次のいずれかのオプション ボタンを選択して適切なデータを入力し、送信元または宛先エンドポイントを指定します。 • DN：電話番号。正確な電話番号を入力するか、ワイルドカード（x）を使用するか、数字とワイルドカードを組み合わせて電話番号の範囲を指定します。 • IP：IP アドレス。IP アドレスを入力するか、ワイルドカード（*）を使用するか、数字とワイルドカードを組み合わせて IP アドレスの範囲を指定します。 (注)　詳細については、P.2-4 の「エンドポイントの IP アドレスまたは電話番号の指定」を参照してください。

CVTQ しきい値グループの優先レベルのアップデート

エンドポイントの電話番号または IP アドレスが複数の CVTQ グループに属している場合、Service Monitor は、最も高い優先レベルの CVTQ しきい値グループのしきい値を適用します。

ステップ 1　**Thresholds > CVTQ Groups** を選択します。CVTQ Threshold Group ページが表示され、最大 10 個のユーザ定義の CVTQ しきい値グループが表示されます。

ステップ 2　Priority カラムに一意の数字（最大 2 桁）を入力します。

ステップ 3　**Update Priority** をクリックします。Service Monitor は CVTQ しきい値グループを並べ替えて、優先レベル順に表示します。

CVTQ しきい値グループの削除

ステップ 1　**Thresholds** > **CVTQ Groups** を選択します。CVTQ Threshold Group ページが表示され、最大 10 個のユーザ定義の CVTQ しきい値グループが表示されます。

ステップ 2　削除する CVTQ しきい値グループのチェックボックスを選択します。

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　**Yes** をクリックします。Service Monitor は残った CVTQ しきい値グループを優先レベル順に表示します。

センサー グループの設定

センサー グループは、1 つまたは複数のセンサー、2 組のエンドポイント、および一般に使用されているコーデックに対する 1 つまたは複数のしきい値で構成されます。最大 10 個のセンサーしきい値グループを定義できます。Service Monitor は、センサーしきい値グループに 1（最も高い優先レベル）から 10（最も低い優先レベル）の優先レベルをつけます。このレベルは、初めはグループの作成順につけられます（ユーザがグループの優先レベルを変更できます）。1 つのエンドポイントが複数のセンサー グループに属する場合、Service Monitor は、最も高い優先レベルのセンサーしきい値グループのしきい値を適用します。

ステップ 1　**Thresholds > Sensor Groups** を選択します。Sensor Threshold Group ページが表示され、最大 10 個のユーザ定義のセンサー グループが、次の表の情報とともに表示されます。

GUI の要素	説明 / 処理
Check box カラム	優先レベルをアップデートする、または削除するセンサー グループを選択します。
Name カラム	センサー グループの一意のユーザ定義名。この名前は、すべてのセンサー グループ内で一意である必要があります。
Priority カラム	最も高い優先レベルから最も低い優先レベルを示す、1 ～ 10 の数字です。優先レベルを変更するには、2 つ以上のセンサーしきい値グループに対し、各グループのこのカラムに 1 桁または 2 桁の数字を入力し、**Update Priority** ボタンをクリックします。
Add ボタン	センサーしきい値グループ（最大 10 個のセンサーしきい値グループ）を追加する場合に、クリックします。P.5-10 の「センサー グループの追加」を参照してください。
Edit カラム	このグループをアップデートする場合に、このカラムの Edit リンクをクリックします。P.5-11 の「センサー グループの編集」を参照してください。
Delete ボタン	センサーしきい値グループを削除する場合に、1 つまたは複数のチェックボックスを選択し、Delete ボタンをクリックします。
Update Priority ボタン	Priority カラムに一意の数字を入力した後にクリックします。センサーしきい値グループが優先レベル順に並べ替えられ、再びこのページが表示されます。

センサー グループの追加

センサー グループを追加すると、既存のセンサー グループの中で最も低い優先レベルが割り当てられます。この優先レベルを調整するには、P.5-12 の「センサー グループの優先レベルのアップデート」を参照してください。

(注)　最大 10 個のセンサー グループを追加できます。

ステップ 1　**Thresholds** > **Sensor Groups** を選択します。Sensor Threshold Group 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 Sensor Threshold Group ページが表示されます。

ステップ 3　次の表に示すデータを入力します。

GUI の要素	説明 / 処理
Group Name フィールド	名前を入力します。この名前は、すべてのセンサー グループ内で一意である必要があります。
Select Sensors リスト	リスト ボックスに「All current and future sensors.（現在および将来のすべてのセンサー）」と表示されます。 (注)　センサーを選択しないと、現在管理されているセンサーおよび将来管理されるセンサーに、このグループのしきい値が適用されます。 次の手順でセンサーを選択します。 1.  をクリックします。Select Sensors ダイアログボックスが表示されます。 2. チェックボックスを選択します。 3. **OK** をクリックします。
Override Thresholds リスト	次の手順でしきい値をアップデートします。 1.  をクリックします。MOS Threshold Settings ダイアログボックスが表示されます。 2. 1 つ以上のコーデックに対し、MOS しきい値を入力します。 3. **OK** をクリックします。
Endpoint 1	音声ゲートウェイまたは IP Phone の IP アドレスを入力します。IP アドレスの範囲を指定するには、IP アドレスの一部と、任意の数字を表すアスタリスク（*）を入力します。デフォルト：*.*.*.*
Endpoint 2	音声ゲートウェイまたは IP Phone の IP アドレスを入力します。IP アドレスの範囲を指定するには、IP アドレスの一部と、任意の数字を表すアスタリスク（*）を入力します。デフォルト値：*.*.*.*

ステップ 4　**OK** をクリックします。Sensor Threshold Group ページが表示され、最新のセンサーしきい値グループがリストの最後（最も低い優先レベルの位置）に表示されます。

センサー グループの編集

(注)　センサー グループの優先レベルを変更するには、P.5-12 の「センサー グループの優先レベルのアップデート」を参照してください。

ステップ 1　**Thresholds** > **Sensor Groups** を選択します。Sensor Threshold Group ページが表示されます。

ステップ 2　グループを選択し、センサー グループの **Edit** リンクをクリックします。Edit Sensor Threshold Group が表示されます。

ステップ 3　次の表に示すデータを入力します。

GUI の要素	説明 / 処理
Group Name フィールド	名前は変更できます。この名前は、すべてのセンサー グループ内で一意である必要があります。
Select Sensors リスト	センサーを選択しないと、リスト ボックスに「All current and future sensors.（現在および将来のすべてのセンサー）」と表示されます。 次の手順でセンサーを選択します。 1.  をクリックします。Select Sensors ダイアログボックスが表示されます。 2. チェックボックスを選択します。 3. **OK** をクリックします。 (注)　センサーを選択しないと、現在管理されているセンサーおよび将来管理されるセンサーに、このグループのしきい値が適用されます。
Override Thresholds リスト	次の手順でしきい値をアップデートします。 1.  をクリックします。MOS Threshold Settings ダイアログボックスが表示されます。 2. 1 つ以上のコーデックに対し、MOS しきい値を入力します。 3. **OK** をクリックします。
Endpoint 1	音声ゲートウェイまたは IP Phone の IP アドレスを入力します。IP アドレスの範囲を指定するには、IP アドレスの一部と、任意の数字を表すアスタリスク（*）を入力します。すべての IP アドレスを指定するには、*.*.*.* を入力します。
Endpoint 2	音声ゲートウェイまたは IP Phone の IP アドレスを入力します。IP アドレスの範囲を指定するには、IP アドレスの一部と、任意の数字を表すアスタリスク（*）を入力します。すべての IP アドレスを指定するには、*.*.*.* を入力します。

センサー グループの優先レベルのアップデート

1 つのセンサーが複数のセンサー グループに属する場合、Service Monitor は、最も高い優先レベルのセンサーしきい値グループのしきい値を適用します。

ステップ 1　**Thresholds > Sensor Groups** を選択します。Sensor Threshold Group ページが表示され、最大 10 個のユーザ定義のセンサー グループが表示されます。

ステップ 2　Priority カラムに一意の数字（最大 2 桁）を入力します。

ステップ 3　**Update Priority** をクリックします。Service Monitor はセンサーしきい値グループを並べ替えて、優先レベル順に表示します。

センサー グループの削除

ステップ 1　**Thresholds > Sensor Groups** を選択します。Sensor Threshold Group ページが表示され、最大 10 個のユーザ定義のセンサー グループが表示されます。

ステップ 2　削除するセンサー グループのチェックボックスを選択します。

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　**Yes** をクリックします。Service Monitor は残ったセンサー グループを優先レベル順に表示します。

CHAPTER 6

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

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 qovr 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 *generationNumber*/*suite* のすぐ下にリストされます。 qovr.db

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

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 イベントのレコードが含まれます。履歴ログ ファイルは、レコードが蓄積されるため、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、デバイスベ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、**Common Services > Server > Reports > Permission Report > Generate Report** 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で含まれます。

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している必要があります。

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。

a. コマンド プロンプトを開いて、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 ビリング 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「ビリング 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
```

設定のチェックリストおよびヒント

この項では次のトピックについて説明します。

初期設定チェックリスト

表 A-1 に、Service Monitor が MOS の監視およびトラップの送信を開始する前に、行う必要のある設定作業を示します。

表 A-1　初期設定作業チェックリスト

作業	説明および参照先
Service Monitor および Cisco Unified CallManager（ネットワークで使用している場合）の設定	
	P.B-1 の「Cisco Unified CallManager の設定」の説明に従って、Cisco Unified CallManager を設定します。
	Cisco Unified CallManager の資格情報を Service Monitor に追加します。P.3-2 の「Cisco Unified CallManager の資格情報と概要」を参照してください。
Service Monitor およびセンサー（ネットワークで使用している場合）の設定	
	1 台以上の TFTP サーバを追加します。P.4-3 の「センサーのコンフィギュレーション ファイルおよびイメージ ファイル用の TFTP サーバの設定」を参照してください。
	センサーのデフォルト コンフィギュレーション ファイル設定します。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。
	バイナリ イメージ ファイルを TFTP サーバの root ロケーションにコピーします。P.4-4 の「バイナリ イメージ ファイルの TFTP サーバへのコピー」を参照してください。
トラップ レシーバの設定	
	Service Monitor は、生成された SNMP トラップを最大 4 つのトラップ レシーバに送信できます。P.3-2 の「トラップ レシーバの設定」を参照してください。

サーバおよびクライアントの設定作業

Service Monitor サーバでは、*NMSROOT*\databases ディレクトリをウイルス スキャンから除外する必要があります。ウイルス スキャンのためにデータベース ファイルがロックされると、問題が発生することがあります。

(注)　*NMSROOT* は、Service Monitor がインストールされているシステム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 です。

Service Monitor クライアントでは、ポップアップ ウィンドウの表示をブロックするソフトウェアをすべてディセーブルにする必要があります。Service Monitor は、情報を表示するために複数のウィンドウが開けるようにする必要があります。

結果の表示について

表 A-1 の作業が完了すると、Service Monitor は次のようにデータの受信、分析、および表示ができるようになります。

- センサーは、60 秒ごとにレコードを Service Monitor に送信し、コールの処理中に計算された MOS を報告します。このため、Service Monitor がトラップ生成を開始した後でも、コールを処理できます。同様に、コールの処理中でも、センサー データを Service Monitor レポートに表示できます。
- コール データ レコード（CDR）は、コールが完了してから Cisco Unified CallManager によって書き込まれます。Service Monitor が Cisco Unified CallManager から 60 秒ごとにデータを取得したとしても、コールが完了しないと、Service Monitor はトラップを生成できません。同様に、コールが完了しないと、CVTQ データは Service Monitor レポートに表示できません。

オプションの設定チェックリスト

オプションの設定作業により、次のことが可能になります。

- Service Monitor がトラップ生成の起動に使用する、デフォルトのグローバルなしきい値（コーデックごとに 1 つ）をアップデートおよび無効にする。
- 最も影響の大きいエンドポイント レポートを、毎晩および毎週自動的に作成する。

作業	説明および参照先
グローバルなしきい値のアップデートおよび無効化	
	グローバルなしきい値をアップデートします。P.5-3 の「グローバルなしきい値の設定」を参照してください。
	グローバルなしきい値を無効にし、選択したセンサーに値を設定します。P.5-9 の「センサー グループの設定」を参照してください。
	グローバルなしきい値を無効にし、選択したクラスタに値を設定します。P.5-4 の「CVTQ グループの設定」を参照してください。
最も影響の大きいエンドポイント レポートのエクスポート	
	P.3-12 の「エンドポイント数の設定と Most-Impacted Endpoints レポートのエクスポート設定」を参照してください。

Cisco Unified CallManager の設定

(注) Service Monitor がサポートしている Cisco Unified CallManager のバージョンについては、『*Release Notes for Cisco Unified Service Monitor 2.0*』を参照してください。

Service Monitor が Cisco Unified CallManager のデータを収集して分析するには、次の項の説明に従って、まず Cisco Unified CallManager システムを設定する必要があります。

サポートされているバージョンの Cisco Unified CallManager の設定作業

Service Monitor が CVTQ データを Cisco Unified CallManager から取得するには、まず、次のシステムにログインして設定作業を行う必要があります。

- Cisco Unified CallManager：Cisco Unified CallManager Administration および Cisco Unified CallManager Serviceability にアクセスするため。
- Cisco Unified CallManager がインストールされているサーバ：Microsoft SQLServer にアクセスするため。

ご使用の Cisco Unified CallManager のバージョンに応じて、この項で記載されている作業の一部を実行する必要があります。Cisco Unified CallManager のバージョンによって作業が多少異なる場合は、バージョン固有の手順を示してあります。

表 B-1 に、Service Monitor によって CVTQ データを Cisco Unified CallManager から取得する場合について、Cisco Unified CallManager のバージョン別に実行する必要のある設定作業を示します。

表 B-1　Cisco Unified CallManager および Microsoft SQLServer の設定作業

設定作業	Cisco Unified CallManager のバージョン別の設定作業の必要性		
	5.x	4.x	3.3.x
Cisco Unified CallManager の設定			
Cisco Unified CallManager のサービス パラメータの設定（P.B-3）	X	X	X
Cisco Unified CallManager のエンタープライズ パラメータの設定（P.B-4）	X	X	X
ビリング サーバとしての Service Monitor の Cisco Unified CallManager 5.x への追加（P.B-4）	X	—	—
Cisco Unified CallManager を使用しているサーバ上での Microsoft SQLServer の設定			
Microsoft SQL Server における CallManager 4.x の混合認証のイネーブル化（P.B-6）	—	X	— **（注）** 3.3.x では、デフォルトで混合認証が設定されている必要があります。設定されていない場合は、この手順を実行して 3.3.x に混合認証を設定します。
Microsoft SQLServer ユーザ アカウントの追加（P.B-7）	—	X	X

Cisco Unified CallManager の設定

この項では、次のトピックについて説明します。

Cisco Unified CallManager のサービス パラメータの設定

（注） サービス パラメータは、クラスタ内の Cisco Unified CallManager ごとに設定します。

ステップ 1　Cisco Unified CallManager Administration にログインします。

ステップ 2　次の手順で、Service Parameters Configuration ページに進みます。

- Cisco Unified CallManager 3.3 および 4.x では、**Service > Service Parameters** を選択します。
- Cisco Unified CallManager 5.x では、**System > Service Parameters** を選択します。

Service Parameters Configuration ページが表示されます。

ステップ 3　次の手順で、サーバとサービスを選択します。

a. Cisco Unified CallManager サーバの名前を選択します。これは、Service Monitor によるデータ収集の対象となる Cisco Unified CallManager です。

b. Cisco CallManager サービスを選択します。

ステップ 4　次のパラメータを設定します。

- Cisco Unified CallManager バージョン 3.3.x および 4.x の場合：
  - CDR Enabled Flag：System までスクロール ダウンします。**True** に設定します。
  - Call Diagnostics Enabled：Clusterwide Parameters (Device - General) までスクロール ダウンします。**True** に設定します。
- Cisco Unified CallManager 5.x の場合：
  - CDR Enabled Flag：System までスクロール ダウンします。**True** に設定します。
  - Call Diagnostics Enabled：Clusterwide Parameters (Device - General) までスクロール ダウンします。**Enable Only When CDR Enabled Flag is True** に設定します。

ステップ 5　**Update** をクリックします。

Cisco Unified CallManager のエンタープライズ パラメータの設定

この手順は、Cisco Unified CallManager バージョン 3.3、4.x、および 5.x で実行します。

ステップ 1　Cisco Unified CallManager Administration にログインします。

ステップ 2　**System > Enterprise Parameters** を選択します。Enterprise Parameters Configuration ページが表示されます。

ステップ 3　CDR Parameters にスクロール ダウンし、次のパラメータを設定します。

- Cisco Unified CallManager 3.3 および 4.x の場合：
  - CDR File Time Interval (min)：**1** を設定します。
  - CDR Format：**CDRs will be inserted into database** を選択します。
- Cisco Unified CallManager 5.x の場合、CDR File Time Interval (min) に **1** を設定します。

ステップ 4　**Update** をクリックします。

ビリング サーバとしての Service Monitor の Cisco Unified CallManager 5.x への追加

（注）
- この作業は、Cisco Unified CallManager バージョン 5.x のみで行ってください。
- この作業は、Service Monitor の稼働中にのみ行ってください。

ステップ 1　Cisco Unified CallManager Serviceability を起動します。

ステップ 2　**Tools > CDR Manageability** を選択します。

ステップ 3　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。

ステップ 4　次を入力します。

- Host Name / IP Address：Cisco Unified Service Monitor がインストールされているシステムの IP アドレスを入力します。
- User Name：smuser を入力します。

（注）　smuser 以外のユーザ名を入力しないでください。

- Password：パスワードを入力します。デフォルトのパスワードは smuser です。このパスワードを変更するには、次の手順を実行します。
  - まず Service Monitor でパスワードを変更します（詳細については、P.3-14 の「その他の設定」を参照）。
  - Service Monitor の他の設定で smuser に対して入力したのと同じパスワードを入力します。

（注）　Service Monitor でパスワードを変更した場合、Cisco Unified CallManager でその新しいパスワードをすぐに受け付けるわけではないので、しばらく待ってから新しいパスワードを再入力してください。

- SFTP Protocol を選択します。
- Directory Path：/home/smuser/ を入力します。

（注）　/home/smuser 以外のディレクトリ パスを入力しないでください。

ステップ 5　**Add** をクリックします。

（注）　場合によっては、新しく追加されたビリング サーバに CDR/CMR ファイルを送信するとき、まず CDR Repository Service を再起動しなければならないこともあります。このような場合、Cisco Unified CallManager Serviceability で、**Tools > Control Center - Network Services** を選択します。次に **publisher > stop / start or restart Cisco CDR Repository Manager** を選択します。

Cisco Unified CallManager 5.x での smuser のパスワード変更

（注）　この作業は、Cisco Unified CallManager バージョン 5.x のみで行ってください。

Service Monitor における smuser の SFTP パスワードと、Cisco Unified CallManager 5.x における Service Monitor アプリケーション ビリング サーバ smuser のパスワードは同じである必要があります。どちらか一方を変更したら、もう一方も変更して一致させる必要があります。Service Monitor における smuser の SFTP パスワードを変更するには、P.3-14 の「その他の設定」を参照してください。

Cisco Unified CallManager 5.x における Service Monitor アプリケーション ビリング サーバ smuser のパスワードを変更するには、次の手順を実行します。

ステップ 1　Cisco Unified CallManager Serviceability を起動します。

ステップ 2　**Tools > CDR Manageability** を選択します。

ステップ 3　Billing Applications Server Parameters までスクロール ダウンし、Service Monitor のリンクをダブルクリックします。

ステップ 4　新しいパスワードを入力します。

（注）　Service Monitor でパスワードを変更した場合、Cisco Unified CallManager でその新しいパスワードをすぐに受け付けるわけではないので、しばらく待ってから新しいパスワードを再入力してください。

その他のフィールド、Host Name / IP Address、User Name、SFTP Protocol、および Directory Path の値は変更せず、元のままにしておいてください。

ステップ 5　**Update** をクリックします。

Cisco Unified CallManager システム上での MicroSoft SQLServer の設定

Service Monitor には、Cisco Unified CallManager システム上の Microsoft SQLServer で設定されたユーザ アカウントが必要です。このアカウントは次の目的で使用します。

- Cisco Unified CallManager 4.x および 3.3.x から CDR にアクセスする。
- Cisco Unified CallManager 3.3.x から デバイス データベース（CCM0300、CCM030*n*）にアクセスする。

Microsoft SQL Server における CallManager 4.x の混合認証のイネーブル化

この作業は、Cisco Unified CallManager 4.x のみで行ってください。

ステップ 1　Cisco Unified CallManager がインストールされているサーバにログインします。

ステップ 2　**Start > Programs > Microsoft SQL Server Enterprise Manager** を選択します。

ステップ 3　**Console Root > Microsoft SQL Servers > SQL Server Group** を選択し、右クリックします（**local**）。ダイアログボックスが表示されます。

ステップ 4　**Security** タブを選択します。

a. Authentication で、**SQL Server and Windows** を選択します。

b. **OK** をクリックします。SQL サーバを再起動するかどうかをたずねるメッセージが表示されます。**No** をクリックします。

ステップ 5　次の手順で SQL サーバを再起動します。

a. **Start > Settings > Control Panel** > **Administrative Tools > Services** を選択します。Services ウィンドウが表示されます。

b. MSSQLSERVER を右クリックし、**Stop** をクリックします。MSSQLSERVER とともに停止されるサービスの一覧が表示されます。停止されるサービスに注意してください。これらは 1 つずつステップ 5c. で再開する必要があります。

c. MSSQLSERVER を右クリックし、**Start** をクリックします。前のステップで停止されたその他のサービスに対し、サービスを 1 つずつ右クリックし、**Start** をクリックします。

Microsoft SQLServer ユーザ アカウントの追加

Service Monitor には、Cisco Unified CallManager を使用しているシステム上のローカル データベースにアクセスするために、Microsoft SQLServer ユーザ アカウントが必要です。次の手順を実行して、次の Cisco Unified CallManager バージョンのいずれかにユーザ アカウントを追加します。

- 4.x：アカウントを追加し、Service Monitor が CDR データベースにアクセスできるようにする。
- 3.3.x：ユーザ アカウントを追加し、Service Monitor が CDR データベースおよびデバイス データベースにアクセスできるようにする。デバイス データベースの名前は CCM030n（CCM0300 など）です。または、2 つのアカウントを追加し、1 つは CDR データベース用、もう 1 つは CCM030*n* データベース用にします。

ステップ 1　Cisco Unified CallManager がインストールされているサーバにログインします。

ステップ 2　**Start > Programs > Microsoft SQL Server Enterprise Manager > Security** を選択します。

ステップ 3　**Logins** を右クリックし、**New Login** を選択します。ウィンドウが表示されます。

ステップ 4　General タブで次を実行します。

a. ユーザ名を入力します。

b. **SQL Authentication** を選択し、パスワードを入力します。

（注） Windows Authentication *ではなく*、SQL Authentication が選択されていることを確認してください。デフォルトで Windows Authentication が選択されていることがあります。

ステップ 5　Server Roles タブを選択し、System Administrators ロールを選択します。

ステップ 6　Database Access タブを選択し、次を実行します。

a. 次の手順でデータベースを選択します。

- Cisco Unified CallManager バージョン 4.x では、CDR データベースの Permit カラムにチェックマークを付けます。
- Cisco Unified CallManager バージョン 3.3.x では、CDR データベースおよびデバイス データベース（CCM030n、たとえば CCM0300）の Permit カラムにチェックマークを付けます。または、CDR データベースかデバイス データベースのどちらかを選択し、アカウントの作成を続行します。アカウントを作成したら、この手順を繰り返し、もう一方のデータベース用にもう 1 つアカウントを作成します。

（注） Cisco Unified CallManager をアップグレードするたび、CCM030*n* の *n* が 1 ずつ増加し、新しいデータベースが作成されます。複数のデバイス データベースがある場合は、最新のもの、つまり数字が最も大きいもの（CCM0302 など）を選択します。このステップの実行後に Cisco Unified CallManager 3.3 をアップグレードした場合は、この手順に戻ってこのステップ（ステップ 6）をやり直してください。

（注） または、CDR データベースかデバイス データベースのどちらかを選択し、アカウントの作成を続行します。アカウントを作成したら、この手順を繰り返し、もう一方のデータベース用にもう 1 つアカウントを作成します。

ウィンドウの下に、選択したデータベースのデータベース ロールが表示されます。デフォルトでは public にチェックマークが付いています。

b. db_owner ロールにチェックマークを付けます（これにより public および db_owner にチェックマークが付く）。

ステップ 7　**OK** 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 8　このダイアログボックスに再度パスワード（ステップ 4b で入力したもの）を入力し、パスワードを確定します。

使用される MIB と生成される SNMP トラップ

使用される MIB

Service Monitor は CISCO-SYSLOG-MIB を使用して SNMP トラップを生成します。

生成される SNMP トラップ

Cisco Unified Service Monitor（Service Monitor）は、次のトラップを生成します。

- MOS 違反
- Cisco 1040 到達不能

トラップの詳細は、clogMessageGenerated 通知の clogHistMsgText フィールドに名前と値のペアで示されます。表 C-1 に、MOS 違反 SNMP トラップの詳細を記載します。

表 C-1　MOS 違反 SNMP トラップ

タグ	説明	値
TT	トラップ タイプ	1：センサーからのデータ 3：Cisco Unified CallManager クラスタからのデータ
01	Cisco 1040 センサーの MAC アドレス（TT = 1 の場合）または Cisco Unified CallManager クラスタ ID（TT = 3 の場合）	テキスト ストリング
02	タイム スタンプ	<YYYYMMDDhhmm>
03	しきい値	サンプル値：3.5
A	実際のデータか、またはサンプリングされたデータかを示すフラグ	0：実際 1：サンプル（未使用）
B	送信元デバイスの IP アドレス。送信元デバイスには、次のものがあります。 • IP Phone または音声ゲートウェイ（TT = 1 および TT = 3 の場合） • リモート Cisco Unified CallManager（TT = 3 で、コールがクラスタ間コールの場合）	IPv4 アドレス。次に例を示します。 172.20.4.18

表 C-1　MOS 違反 SNMP トラップ（続き）

タグ	説明	値
C	受信デバイスの IP アドレス。受信デバイスには、次のものがあります。 • IP Phone または音声ゲートウェイ（TT = 1 および TT = 3 の場合） • リモート Cisco Unified CallManager（TT = 3 で、コールがクラスタ間コールの場合）	IPv4 アドレス。次に例を示します。 `172.20.5.12`
D	コール データ レコードのコーデック（この表の CDC も参照）	次のいずれかです。 2：G711Alaw 64k 3：G711Alaw 56k 4：G711Ulaw 64k 5：G711Ulaw 56k 6：G722 64k 7：G722 56k 8：G722 48k 10：G728 11：G729 12：G729AnnexA 15：G729AnnexB 16：G729AnnexAwAnnexB
E	センサー（TT = 1 の場合）または CVTQ（TT = 3 の場合）によって計算された MOS スコア	サンプル値：3.4
F	コール劣化の主な原因	TT = 1 の場合 • J：ジッタ • P：パケット損失 TT = 3 の場合は N/A
G	直前の 1 分間に失われた実際のパケット数	サンプル値：0.0
H	直前の 1 分間に生じた実際のジッタ（ミリ秒単位）	サンプル値：0 TT = 3 の場合、値は NA

表 C-1　MOS 違反 SNMP トラップ（続き）

タグ	説明	値
CDC	コール データ レコードのコーデック	次のいずれかです。 • G711Alaw64k • G711Alaw56k • G711Ulaw64k • G711Ulaw56k • G722 64k • G722 56k • G722 48k • G728 • G729 • G729AnnexA • G729AnnexB • G729AnnexAwAnnexB
CCR	Cumulative Concealment Ratio：コールが開始してから観察された、音声時間に対する隠匿時間の累積比率。	サンプル値：0.0 TT = 1 の場合、値は NA
ICR	Interval Concealment Ratio：間隔ベースの平均隠匿レート。音声がアクティブな状態の最後の 3 秒間における、音声時間に対する隠匿時間の比率。	サンプル値：0.0 TT = 1 の場合、値は NA
ICRmx	Interval Concealment Ratio Max：コール中に観察された最大の隠匿比率。	サンプル値：0.0 TT = 1 の場合、値は NA
CS	Concealment Seconds：コール中になんらかの隠匿が観察された秒数。	サンプル値：0 TT = 1 の場合、値は NA
SCS	Severely Concealed Seconds：かなりの量の隠匿が観察された秒数。観察された隠匿が平均で 50 ミリ秒または約 5 パーセントより大きい場合、おそらく音声はあまり聞き取れません。	サンプル値：0 TT = 1 の場合、値は NA
MLQK	MOS Listening Quality または CVTQ Score：Cisco Voice Transmission Quality（CVTQ）アルゴリズムで、リスニング品質（LQK）の Mean Opinion Score（MOS; 平均オピニオン スコア）の客観的な評価（5（優秀）から 1（不良）までの格付け）が提示されます。このスコアは、音声ストリームの直前の 8 秒間隔でのフレーム損失による可聴隠匿イベントに基づきます。 **（注）** CVTQ スコアは、Cisco Unified IP Phone が使用するコーデックのタイプによって異なる場合があります。	サンプル値：4.5 TT = 1 の場合、値は NA
MLQKmn	MOS Listening Quality CVTQ Min：コールの開始以降に観察された最低スコア。サウンドが最も不良な 8 秒間隔を表します。	サンプル値：4.1 TT = 1 の場合、値は NA

表 C-1　MOS 違反 SNMP トラップ（続き）

タグ	説明	値
MLQKmx	MOS Listening Quality CVTQ Max：コールの開始以降に観察された最高スコア。サウンドが最良の 8 秒間隔を表します。	サンプル値：4.5 TT = 1 の場合、値は NA
MLQKvr	CVTQ 計算のバージョン	サンプル値：0.95 TT = 1 の場合、値は NA
DRTN	コールの時間（秒単位）	サンプル値：120 TT = 1 の場合、値は NA
NST	開始時刻から終了時刻までに抑止されたトラップの数（TT = 1 の場合）。詳細については、P.4-5 の「センサーのデフォルト設定の設定」の *n* 分ごとの送信トラップのエントリを参照してください。	サンプル値：9 TT = 3 の場合、値は 0
ST	TT = 1 の場合は開始時刻。エンドポイントに対して最初のトラップが送信された時刻。	UTC 時間 TT = 3 の場合、値は 0
ET	TT = 1 の場合は終了時刻。最新のトラップが送信された時刻。	UTC 時間 TT = 3 の場合、値は 0

表 C-2 に、Cisco 1040 到達不能 SNMP トラップの詳細を示します。

表 C-2　Cisco 1040 到達不能 SNMP トラップ

タグ	説明	値
TT	トラップ タイプ	2
01	Cisco 1040 ID	Cisco 1040 MAC アドレス
02	タイム スタンプ	<YYYYMMDDhhmm>

ライセンス

この付録では、Cisco Unified Service Monitor（Service Monitor）のライセンスについて説明します。この章は、以下の項で構成されています。

Service Monitor ライセンスの検証

次の手順は、Service Monitor ライセンスのステータスおよびサイズ（サポートされる電話機の数）を判別する場合に使用します。

ステップ 1　Service Monitor のホーム ページの右上隅の CiscoWorks リンクを選択します。新しいウィンドウが開きます。

ステップ 2　**Common Services > Server > Admin > Licensing** を選択します。Licensing Information ページが表示され、次の表に説明する情報が示されます。

列	説明
Name	省略された製品名：SM。
Version	製品のバージョン：*A.b.c*。ここで、*A* はメジャー バージョン番号、*b* はマイナー バージョン番号、*c* はサービス パック番号です。たとえば、SM 2.0.0 は、サービス パックなしのバージョン 2.0 を示します。
Size	制限：Service Monitor にライセンスが付与されている、サポートする電話機の累積数を示します。最大は 30,000 です。 **（注）** ライセンス処理による結果としてサイズが最大値を超えても、任意数の有効なライセンスのインストールが許可されます。Service Monitor サーバ間でライセンスを移動する場合は、Cisco Technical Assistance Center（TAC）に問い合わせてください。
Status	次のいずれかです。 • Purchased：製品は登録済みで、ライセンスが付与されています。 • Evaluation：ライセンスは有効期限日付で期限が切れ、Service Monitor は実行を停止します。
Expiration Date	Service Monitor が実行を停止する日付。評価ライセンスに適用されます。

Service Monitor ライセンスの入手および登録

Service Monitor をインストールした後、次の操作を行うことができます。

- 同一バージョンの Service Monitor についての、評価ライセンスから購入ライセンスへのアップグレード。
- Service Monitor がサポートする電話機の数を増やす。最大は 30,000 です。

（注） インストールまたは以前のバージョンからアップグレードする場合の Service Monitor のライセンスの詳細については、『*Quick Start Guide for Cisco Unified Service Monitor 2.0*』を参照してください。

Service Monitor ソフトウェアを購入すると、製品または電話機の増分サポートのいずれの場合も、Product Authorization Key（PAK）が付属しています。PAK を受け取ったら、次の手順を実行してください。

ステップ 1　PAK と、Service Monitor がインストールされているサーバの MAC アドレスを、次の URL から入力します。

http://www.cisco.com/go/license

ライセンス ファイルは電子メールで送信されます。

ステップ 2　ライセンス ファイルを Service Monitor サーバにコピーします。このファイルの読み取り権限を casuser に与える必要があります。

（注） Service Monitor は casuser を使用して、管理者権限が必要なタスクを実行します。

（注） ライセンス ファイルを含むフォルダを Service Monitor サーバにコピーする場合には、そのフォルダおよびライセンス ファイルの読み取りアクセス権を casuser に必ず付与してください。

ステップ 3　ライセンス ファイルを登録します。

注意 この手順を行った結果としてライセンス サイズが最大値を超える場合でも、ライセンスは登録されます。Service Monitor が管理する電話機の台数は、ライセンス サイズが最大数（30,000）を超えている場合でも、30,000 台までです。

a. Service Monitor のホーム ページの右上隅の CiscoWorks リンクをクリックします。

b. **Common Services > Server > Admin >Licensing** を選択します。License Information ページが表示されます。

c. **Update** ボタンをクリックします。Select License File ダイアログボックスが表示されます。

d. ライセンス ファイルを参照して選択します。

- **Browse** ボタンをクリックします。
- ステップ 2 でライセンス ファイルをコピーした場所を参照して移動します。
- ライセンス ファイルを選択します。
- **OK** をクリックします。Licensing Information ページが更新されます。詳細については、表 D-1 を参照してください。

表 D-1　ライセンス登録結果

登録ライセンス	Licensing Information ページの予期される結果
評価ライセンスからのアップグレード	Status 列の項目が Evaluation から Purchased に変わる。
サポートされる電話機数の増加	Size 列の項目がライセンス サイズに応じて増える。

評価ライセンスの使用法

Service Monitor の評価バージョンがインストールされている場合は、Service Monitor を開始すると、ライセンス リマインダが表示されます。有効期限切れ後に評価ライセンスをアップグレードしなかった場合は、Service Monitor 機能へのアクセスが禁止されます。評価ライセンスからのアップグレードについては、P.D-3 の「Service Monitor ライセンスの入手および登録」を参照してください。

ライセンス サイズ超過の判別

Service Monitor は、ライセンスに指定された数より少し多くの電話機をサポートします（P.D-2 の「Service Monitor ライセンスの検証」を参照）。電話機の数がライセンス サイズを超える場合は、ライセンスを購入してサポートされる電話機数を増やすか（最大 30,000）、または追加ソフトウェア ライセンスを購入して追加システムに Service Monitor をインストールできます。P.D-3 の「Service Monitor ライセンスの入手および登録」を参照してください。

注意　Service Monitor は、ライセンスで指定された数に若干の数を加えた台数までの電話機を監視します。Service Monitor での電話機の数が制限を超えると、追加の電話機からのデータは収集または分析されません。

Service Monitor の SNMP MIB サポート

Service Monitor は、SNMP v2 を使用してシステム アプリケーション MIB を実装し、SNMP サブエージェントを提供します。シンプルな SNMP クエリーを使用して、MIB をサポートするシスコ ユニファイド コミュニケーション管理スイートのアプリケーションのヘルスを監視できます。

SNMP を使用して Service Monitor などのシスコ ユニファイド アプリケーションを管理するようにシステムを設定する方法の詳細については、P.6-10 の「SNMP を使用した Service Monitor の監視方法」を参照してください。

システム アプリケーション MIB の実装

RFC 2287 に定義されるシステム アプリケーション MIB は、インストールされているアプリケーション、アプリケーションに対して実行されているプロセス、および過去の実行に関する情報を提供します。システム アプリケーション MIB の情報を使用して、Service Monitor 全体のヘルスを判別し、アプリケーションで稼動している実際のプロセスを詳細に把握できます。

システム アプリケーション MIB の詳細については、次の URL で MIB 情報を参照できます。

http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4

この MIB に格納されているデータの例については、P.E-8 の「システム アプリケーション MIB のサンプル MIB ウォーク」を参照してください。

http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4

システム アプリケーションのリソース MIB テーブル

ここでは、次の情報を含め MIB テーブルについて説明します。

インストールされているパッケージ

表 E-1 に、システム アプリケーション MIB をサポートするシスコ ユニファイド管理スイートのアプリケーション（Service Monitor など）について、インストール済みパッケージの情報を示します。

表 E-1　sysApplInstallPkgTable

MIB の行エントリ	MIB から見た説明	シスコ ユニファイド コミュニケーション管理スイートでの使用方法
sysApplInstallPkgIndex	このテーブルのインデックスの一部。インデックス付けのためだけに使用される整数。一般に、新規アプリケーションがインストールされると 1 から単調に増加します。	SNMP サブエージェントに登録されている各アプリケーションの実行番号
sysApplInstallPkgManufacturer	ソフトウェア アプリケーション パッケージの製造業者	Cisco Systems, Inc.
sysApplInstallPkgProductName	製造業者によってソフトウェア アプリケーション パッケージに割り当てられた名前	Cisco Unified Service Monitor 2.0 などのアプリケーションが SNMP サブエージェントに登録されたときに指定された名前 **（注）** この名前を使用して、監視するアプリケーションを選択します。
sysApplInstallPkgVersion	ソフトウェア製造業者によってアプリケーション パッケージに割り当てられたバージョン番号	2.0.2 などのバージョン番号。ここで、1 はメジャー バージョン、0 はマイナー バージョン、2 はパッチ バージョンまたは Incremental Device Update（IDU）番号です。
sysApplInstallPkgSerialNumber	製造業者によって割り当てられたソフトウェアのシリアル番号	「適用なし」
sysApplInstallPkgDate	ソフトウェア アプリケーションがホストにインストールされた日付および時刻	—
sysApplInstallPkgLocation	アプリケーション パッケージのインストール場所の完全パス名	*NMSROOT*：Service Monitor がインストールされているディレクトリ。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~1\CSCOpx です。

インストールされている要素

インストールされているパッケージ テーブル（表 E-1）のエントリは、インストールされている要素テーブル（表 E-2）の複数のエントリに対応する場合があります。パッケージのインストールされている要素数は、そのパッケージに関して監視されているプロセス数に相当します。

表 E-2 に、sysApplInstallElmtTable の内容を示します。

表 E-2　sysApplInstallElmtTable

MIB の行エントリ	MIB から見た説明	シスコ ユニファイド コミュニケーション管理スイートでの使用方法
sysApplInstallPkgIndex	このテーブルのインデックスの一部。この値は、このプロセスが属するアプリケーションの、インストールされているソフトウェア パッケージを識別します。	sysApplInstallPkgTable（表 E-1 の値
sysApplInstallElmtIndex	アプリケーション全体で固有の番号	実行番号
sysApplInstallElmtName	製造業者によってソフトウェア要素パッケージに割り当てられた名前	デーモン マネージャで使用されるプロセス名（RFC 2287 に指定されたファイル名または実行可能ファイル名とは異なります）。
sysApplInstallElmtType	インストールされているアプリケーションの一部である要素のタイプ	デフォルト アプリケーション（5）
sysApplInstallElmtDate	このコンポーネントがシステムにインストールされた日付および時刻	**（注）** 日付および時刻はすべて、SNMPv2 テキスト表記規則に従って形式化されています。
sysApplInstallElmtPath	このアプリケーションのインストール場所	*NMSROOT*：Service Monitor がインストールされているディレクトリ。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~1\CSCOpx です。
sysApplInstallInstallElmt SizeHigh	インストールされたファイルのサイズ（2^{32} バイト ブロック単位）	デフォルトは 0（未実装）
sysApplInstallInstallElmt SizeLow	インストールされたファイルのサイズ（2^{32} バイト ブロック単位）	デフォルトは 0（未実装）
sysApplInstallElmtRole	アプリケーション ステータスの判別に使用されるオペレータが割り当てた値	アプリケーション ステータスの判別に使用される値は、次のとおりです。 • 必須（3）：実行中と見なされるアプリケーションで稼働している必要のあるプロセス • 不明（5）：オプションのプロセス
sysApplInstallElmtModifyDate	この要素が最後に変更された日付および時刻	**（注）** 日付および時刻はすべて、SNMPv2 テキスト表記規則に従って形式化されています。
sysApplInstallCurSizeHigh	現在のファイル サイズ（2^{32} バイト ブロック単位）	デフォルトは 0（未実装）
sysApplInstallCurSizeLow	現在のファイル サイズ（2^{32} バイト ブロック単位）	デフォルトは 0（未実装）

パッケージ ステータス情報

表 E-3 に、システム アプリケーション MIB をサポートするシスコ ユニファイド管理スイートのアプリケーション（Service Monitor など）の現在のステータスを示します。

表 E-3　sysApplRunTable

MIB の行エントリ	MIB から見た説明	シスコ ユニファイド コミュニケーション管理スイートでの使用方法
sysApplInstallPkgIndex	このテーブルのインデックスの一部。この値は、このプロセスが属するアプリケーションの、インストールされているソフトウェア パッケージを識別します。	sysApplInstallPkgTable（表 E-1 の値
sysApplRunIndex	このテーブルのインデックスの一部。インデックス付けのためだけに使用される任意の整数。一般に、ホスト上で新規アプリケーションが起動されると 1 から単調に増加します。この方法により、アプリケーションの起動を一意に識別します。	実行番号
sysApplRunStarted	アプリケーションが起動された日付および時刻	(注)　日付および時刻はすべて、SNMPv2 テキスト表記規則に従って形式化されています。
sysApplRunCurrentState	実行中のアプリケーション インスタンスの現在の状態。値は、実行中（1）、実行可能だが CPU などのリソースの待機中（2）、イベントの待機中（3）、終了（4）、その他（5）のいずれかです。	次の値は、アプリケーション ヘルスの判断基準となります。 • 実行中（1）：すべての必須プロセスが動作中 • その他（5）：1 つ以上の必須プロセスが動作していない すべての必須プロセスが停止しているか、またはデーモン マネージャが停止している場合、このエントリは sysApplPastRun テーブルに移動します。

要素ステータス情報

表 E-4 に、動作中の各アプリケーションに属するプロセスの、現在のステータスを示します。

表 E-4　sysApplElmtRunTable

MIB の行エントリ	MIB から見た説明	シスコ ユニファイド コミュニケーション管理スイートでの使用方法
sysApplElmtRunInstallPkg	このテーブルのインデックスの一部。この値は、このプロセスが属するアプリケーションの、インストールされているソフトウェア パッケージを識別します。	sysApplInstallPkgTable（表 E-1 の値
sysApplElmtRunInvocID	このテーブルのインデックスの一部。この値は、このプロセスが属するアプリケーションの起動を識別します。	デフォルトは 0 です。 **（注）** Service Monitor プロセスは独立して実行され、他のプロセスによって起動されることはありません。
sysApplElmtRunIndex	このテーブルのインデックスの一部。ホストで動作している各プロセスに一意の値。	オペレーティング システムでのプロセス ID
sysApplElmtRunInstallID	このテーブルのインデックスの一部。このオブジェクトの値は、このエントリが動作中のインスタンスを表すアプリケーション要素の sysApplInstallElmtIndex と同じ値です。	sysApplInstallElmtTable（表 E-2 の値
sysApplElmtRunTimeStarted	プロセスが起動された時刻	—
sysApplElmtRunState	実行中のプロセスの現在の状態。値は、実行中（1）、実行可能だが CPU などのリソースの待機中（2）、イベントの待機中（3）、終了（4）、その他（5）のいずれかです。	すべてのプロセスが正常に動作している場合、値は実行中（1）です。 **（注）** プロセスが終了すると、プロセス エントリが sysElmtPastRun テーブルに移動します。
sysApplElmtRunName	プロセスのフル パスおよびファイル名	—
sysApplElmtRunParameters	プロセスの起動パラメータ	—
sysApplElmtRunCPU	このプロセスで消費されたシステム CPU リソースの合計（1/100 秒単位）	オペレーティング システムから取得します。
sysApplElmtRunMemory	このプロセスに現在割り当てられている実システム メモリの合計（KB 単位）	オペレーティング システムから取得します。
sysApplElmtRunNumFiles	プロセスが現在開いている正規のファイル数	デフォルトは 0（未実装）
sysApplElmtRunUser	プロセス所有者のログイン名	casuser または SYSTEM

パッケージが以前に実行されたときのステータス

表 E-5 に、アプリケーションが以前に実行されたときのステータスを示します。

表 E-5　sysApplPastRunTable

MIB の行エントリ	MIB から見た説明
sysApplInstallPkgIndex	sysApplInstallPkgTable（表 E-1 の値
sysApplPastRunIndex	このテーブルのインデックスの一部。インデックス付けのためだけに使用される任意の整数。一般に、ホスト上で新規アプリケーションが起動されると 1 から単調に増加します。この方法により、アプリケーションの起動を一意に識別します。
sysApplPastRunStarted	アプリケーションが起動された日付および時刻 (注)　日付および時刻はすべて、SNMPv2 テキスト表記規則に従って形式化されています。
sysApplPastExitState	アプリケーション インスタンスの終了時の状態
sysApplPastRunEnded	アプリケーション インスタンスがすでに動作していないと判別された日付および時刻 (注)　日付および時刻はすべて、SNMPv2 テキスト表記規則に従って形式化されています。

要素が以前に実行されたときのステータス

表 E-6 に、プロセスが以前に実行されたときのステータスを示します。

表 E-6　sysApplElmtPastRunTable

MIB の行エントリ	MIB から見た説明
sysApplElmtPastRunInvocID	このテーブルのインデックスの一部。このプロセスが属するアプリケーションの起動を識別します。
sysApplElmtPastRunIndex	このテーブルのインデックスの一部。ホストで動作している各プロセスに一意の値。
sysApplElmtPastRunInstallID	このテーブルのインデックスの一部。このオブジェクトの値は、このエントリが動作中のインスタンスを表すアプリケーション要素の sysApplInstallElmtIndex と同じ値です。
sysApplElmtPastRunTimeStarted	プロセスが起動された時刻
sysApplElmtPastRunTimeEnded	プロセスが終了した時刻
sysApplElmtPastRunName	プロセスのフル パスおよびファイル名
sysApplElmtPastRunParameters	プロセスの起動パラメータ
sysApplElmtPastRunCPU	このプロセスで消費されたシステム CPU リソースの合計（1/100 秒単位）のうち最後の既知の数値
sysApplElmtPastRunMemory	終了するまでにこのプロセスに割り当てられた実システム メモリの合計（KB 単位）のうち最後の既知の値
sysApplElmtPastRunNumFiles	プロセスが現在開いている正規のファイル数
sysApplElmtPastRunUser	プロセス所有者のログイン名

スカラ変数

次の変数は、MIB テーブル サイズの制御に使用されます。これはアップデートできません。

表 E-7　スカラ

MIB の行エントリ	MIB から見た説明	デフォルト値
sysApplPastRunMaxRows	sysApplPastRun テーブルで許容される最大エントリ数	2000
sysApplPastRunTableRemItems	エントリの最大数（sysApplPastRunMaxRows）を超えた後に、sysApplPastRun テーブルから削除されるエントリのカウンタ	20 エントリ
sysApplPastRunTblTimeLimit	削除されるまでに sysApplPastRun テーブル内のエントリが存在できる最大時間	86400 秒（1 日）
sysApplElemPastRunMaxRows	sysApplElmtPastRuntable で許容される最大エントリ数	2000 エントリ
sysApplElemPastRunTableRemItems	エントリの最大数（sysApplElemPastRunMaxRows）を超えた後に、sysApplElmtPastRun テーブルから削除されるエントリのカウンタ	20 エントリ
SysApplElemPastRunTblTimeLimit	削除されるまでに sysApplElmtPastRunTable 内のエントリが存在できる最大時間	86400 秒（1 日）
sysApplAgentPollInterval	管理対象リソースのステータスを取得するポーリングが実行される最小間隔	60 秒

プロセス マップ

sysApplMapTable には、現在システムで動作中の各プロセスに 1 つずつのエントリが含まれます。表 E-8 に、プロセス識別子、起動されたアプリケーション、インストールされている要素、およびインストールされているアプリケーション パッケージへのインデックス マッピングを示します。

表 E-8　sysApplMapTable

MIB の行エントリ	MIB から見た説明
sysApplElmtRunIndex	プロセス識別番号
sysApplElmtRunInvocID	起動されたアプリケーション（sysApplRunIndex）
sysApplMapInstallElmtIndex	インストールされている要素（sysApplInstallElmtIndex）
sysApplMapInstallPkgIndex	インストールされているアプリケーション パッケージ（sysApplInstallPkgIndex）

システム アプリケーション MIB のサンプル MIB ウォーク

次の例は、Cisco Unified Operations Manager と Service Monitor がインストールされているシステムにおける SYSAPPL-MIB の MIB ウォークの出力（要約）です。

```
***** SNMP QUERY STARTED *****
1: sysApplInstallPkgManufacturer.1 (octet string) Copyright (c) 2004 by Cisco Systems,
Inc.[43.6F.70.79.72.69.67.68.74.20.28.63.29.20.32.30.30.34.20.62.79.20.43.69.73.63.6F.20.53.79.73.74.65.6D
.73.2C.20.49.6E.63.2E (hex)]
2: sysApplInstallPkgManufacturer.2 (octet string) Copyright (c) 2004 by Cisco Systems,
Inc.[43.6F.70.79.72.69.67.68.74.20.28.63.29.20.32.30.30.34.20.62.79.20.43.69.73.63.6F.20.53.79.73.74.65.6D
.73.2C.20.49.6E.63.2E (hex)]
3: sysApplInstallPkgProductName.1 (octet string) Cisco Unified Service Monitor
[43.69.73.63.6F.20.55.6E.69.66.69.65.64.20.53.65.72.76.69.63.65.20.4D.6F.6E.69.74.6F.72 (hex)]
4: sysApplInstallPkgProductName.2 (octet string) Cisco Unified Operations Manager and Service Monitor
[43.69.73.63.6F.20.55.6E.69.66.69.65.64.20.4F.70.65.72.61.74.69.6F.6E.73.20.4D.61.6E.61.67.65.72.20.61.6E.
64.20.53.65.72.76.69.63.65.20.4D.6F.6E.69.74.6F.72 (hex)]
5: sysApplInstallPkgVersion.1 (octet string) 2.0.0 [32.2E.30.2E.30 (hex)]
6: sysApplInstallPkgVersion.2 (octet string) 2.0.0 [32.2E.30.2E.30 (hex)]
7: sysApplInstallPkgSerialNumber.1 (octet string) n/a [6E.2F.61 (hex)]
8: sysApplInstallPkgSerialNumber.2 (octet string) n/a [6E.2F.61 (hex)]
9: sysApplInstallPkgDate.1 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]
10: sysApplInstallPkgDate.2 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]
11: sysApplInstallPkgLocation.1 (octet string) C:\PROGRA~1\CSCOpx
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]
12: sysApplInstallPkgLocation.2 (octet string) C:\PROGRA~1\CSCOpx
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]
13: sysApplInstallElmtName.1.1 (octet string) QOVR [51.4F.56.52 (hex)]
14: sysApplInstallElmtName.1.2 (octet string) QOVRDbEngine [51.4F.56.52.44.62.45.6E.67.69.6E.65 (hex)]
15: sysApplInstallElmtName.1.3 (octet string) QOVRDbMonitor [51.4F.56.52.44.62.4D.6F.6E.69.74.6F.72 (hex)]
16: sysApplInstallElmtName.1.4 (octet string) Apache [41.70.61.63.68.65 (hex)]
17: sysApplInstallElmtName.1.5 (octet string) CmfDbEngine [43.6D.66.44.62.45.6E.67.69.6E.65 (hex)]
18: sysApplInstallElmtName.1.6 (octet string) JRunProxyServer
[4A.52.75.6E.50.72.6F.78.79.53.65.72.76.65.72 (hex)]
19: sysApplInstallElmtName.1.7 (octet string) Tomcat [54.6F.6D.63.61.74 (hex)]
20: sysApplInstallElmtName.1.8 (octet string) WebServer [57.65.62.53.65.72.76.65.72 (hex)]
21: sysApplInstallElmtName.2.9 (octet string) AdapterServer [41.64.61.70.74.65.72.53.65.72.76.65.72 (hex)]
22: sysApplInstallElmtName.2.10 (octet string) Apache [41.70.61.63.68.65 (hex)]
23: sysApplInstallElmtName.2.11 (octet string) CmfDbEngine [43.6D.66.44.62.45.6E.67.69.6E.65 (hex)]
24: sysApplInstallElmtName.2.12 (octet string) DCRServer [44.43.52.53.65.72.76.65.72 (hex)]
25: sysApplInstallElmtName.2.13 (octet string) DfmBroker [44.66.6D.42.72.6F.6B.65.72 (hex)]
26: sysApplInstallElmtName.2.14 (octet string) DfmServer [44.66.6D.53.65.72.76.65.72 (hex)]
27: sysApplInstallElmtName.2.15 (octet string) EDS [45.44.53 (hex)]
28: sysApplInstallElmtName.2.16 (octet string) EPMDbEngine [45.50.4D.44.62.45.6E.67.69.6E.65 (hex)]
29: sysApplInstallElmtName.2.17 (octet string) EPMServer [45.50.4D.53.65.72.76.65.72 (hex)]
30: sysApplInstallElmtName.2.18 (octet string) ESS [45.53.53 (hex)]
31: sysApplInstallElmtName.2.19 (octet string) FHDbEngine [46.48.44.62.45.6E.67.69.6E.65 (hex)]
32: sysApplInstallElmtName.2.20 (octet string) FHServer [46.48.53.65.72.76.65.72 (hex)]
33: sysApplInstallElmtName.2.21 (octet string) GPF [47.50.46 (hex)]
34: sysApplInstallElmtName.2.22 (octet string) INVDbEngine [49.4E.56.44.62.45.6E.67.69.6E.65 (hex)]
35: sysApplInstallElmtName.2.23 (octet string) IVR [49.56.52 (hex)]
36: sysApplInstallElmtName.2.24 (octet string) IPIUDbEngine [49.50.49.55.44.62.45.6E.67.69.6E.65 (hex)]
37: sysApplInstallElmtName.2.25 (octet string) IPSLAServer [49.50.53.4C.41.53.65.72.76.65.72 (hex)]
38: sysApplInstallElmtName.2.26 (octet string) ITMDiagServer [49.54.4D.44.69.61.67.53.65.72.76.65.72
(hex)]
39: sysApplInstallElmtName.2.27 (octet string) Interactor [49.6E.74.65.72.61.63.74.6F.72 (hex)]
40: sysApplInstallElmtName.2.28 (octet string) InventoryCollector
[49.6E.76.65.6E.74.6F.72.79.43.6F.6C.6C.65.63.74.6F.72 (hex)]
41: sysApplInstallElmtName.2.29 (octet string) IPIUDataServer [49.50.49.55.44.61.74.61.53.65.72.76.65.72
(hex)]
42: sysApplInstallElmtName.2.30 (octet string) ITMOGSServer [49.54.4D.4F.47.53.53.65.72.76.65.72 (hex)]
43: sysApplInstallElmtName.2.31 (octet string) jrm [6A.72.6D (hex)]
44: sysApplInstallElmtName.2.32 (octet string) LicenseServer [4C.69.63.65.6E.73.65.53.65.72.76.65.72
(hex)]
45: sysApplInstallElmtName.2.33 (octet string) NOTSServer [4E.4F.54.53.53.65.72.76.65.72 (hex)]
46: sysApplInstallElmtName.2.34 (octet string) PTMServer [50.54.4D.53.65.72.76.65.72 (hex)]
47: sysApplInstallElmtName.2.35 (octet string) PIFServer [50.49.46.53.65.72.76.65.72 (hex)]
48: sysApplInstallElmtName.2.36 (octet string) QoVMServer [51.6F.56.4D.53.65.72.76.65.72 (hex)]
49: sysApplInstallElmtName.2.37 (octet string) SRSTServer [53.52.53.54.53.65.72.76.65.72 (hex)]
```

```
50: sysApplInstallElmtName.2.38 (octet string) SIRServer [53.49.52.53.65.72.76.65.72 (hex)]
51: sysApplInstallElmtName.2.39 (octet string) STServer [53.54.53.65.72.76.65.72 (hex)]
52: sysApplInstallElmtName.2.40 (octet string) Tomcat [54.6F.6D.63.61.74 (hex)]
53: sysApplInstallElmtName.2.41 (octet string) TISServer [54.49.53.53.65.72.76.65.72 (hex)]
54: sysApplInstallElmtName.2.42 (octet string) TopoServer [54.6F.70.6F.53.65.72.76.65.72 (hex)]
55: sysApplInstallElmtName.2.43 (octet string) VsmServer [56.73.6D.53.65.72.76.65.72 (hex)]
56: sysApplInstallElmtName.2.44 (octet string) VHMIntegrator [56.48.4D.49.6E.74.65.67.72.61.74.6F.72
(hex)]
57: sysApplInstallElmtName.2.45 (octet string) VHMServer [56.48.4D.53.65.72.76.65.72 (hex)]
58: sysApplInstallElmtName.2.46 (octet string) ITMCTMStartup [49.54.4D.43.54.4D.53.74.61.72.74.75.70
(hex)]
59: sysApplInstallElmtName.2.47 (octet string) IPSLAPurgeTask [49.50.53.4C.41.50.75.72.67.65.54.61.73.6B
(hex)]
60: sysApplInstallElmtName.2.48 (octet string) GpfPurgeTask [47.70.66.50.75.72.67.65.54.61.73.6B (hex)]
61: sysApplInstallElmtName.2.49 (octet string) FHPurgeTask [46.48.50.75.72.67.65.54.61.73.6B (hex)]
62: sysApplInstallElmtType.1.1 (integer) application(5)
63: sysApplInstallElmtType.1.2 (integer) application(5)

111: sysApplInstallElmtDate.1.1 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]
112: sysApplInstallElmtDate.1.2 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]

160: sysApplInstallElmtPath.1.1 (octet string) C:\PROGRA~1\CSCOpx
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]

209: sysApplInstallElmtSizeHigh.1.1 (integer) 0

258: sysApplInstallElmtSizeLow.1.1 (integer) 0

307: sysApplInstallElmtRole.1.1 (integer) required(3)

356: sysApplInstallElmtModifyDate.1.1 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]

405: sysApplInstallElmtCurSizeHigh.1.1 (integer) 0

454: sysApplInstallElmtCurSizeLow.1.1 (integer) 0

503: sysApplRunStarted.1.2 (octet string) 2006-10-18,17:13:24 [07.D6.0A.12.11.0D.18 (hex)]

505: sysApplRunCurrentState.1.2 (integer) running(1)

507: sysApplElmtRunInstallID.0.0.888 (integer) 0

563: sysApplElmtRunTimeStarted.0.0.888 (octet string) 2006-10-18,17:15:35 [07.D6.0A.12.11.0F.23 (hex)]

619: sysApplElmtRunState.0.0.888 (integer) running(1)

675: sysApplElmtRunName.0.0.888 (octet string) C:\PROGRA~1\CSCOpx\lib\vbroker\bin\osagent.exe
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6C.69.62.5C.76.62.72.6F.6B.65.72.5C.62.69.6E.5C.
6F.73.61.67.65.6E.74.2E.65.78.65 (hex)]

731: sysApplElmtRunParameters.0.0.888 (octet string) -p 42342 [2D.70.20.34.32.33.34.32 (hex)]

787: sysApplElmtRunCPU.0.0.888 (timeticks) 0 days 00h:04m:27s.39th (26739)

843: sysApplElmtRunMemory.0.0.888 (integer) 676

899: sysApplElmtRunNumFiles.0.0.888 (integer) 0

955: sysApplElmtRunUser.0.0.888 (octet string) SYSTEM [53.59.53.54.45.4D (hex)]

1000: sysApplElmtRunUser.2.0.9220 (octet string) casuser [63.61.73.75.73.65.72 (hex)]

1011: sysApplElmtPastRunInstallID.2.0.6180 (integer) 44
1012: sysApplElmtPastRunTimeStarted.2.0.6180 (octet string) 2006-10-18,17:16:27 [07.D6.0A.12.11.10.1B
(hex)]
1013: sysApplElmtPastRunTimeEnded.2.0.6180 (octet string) 2006-11-5,12:45:49 [07.D6.0B.05.0C.2D.31 (hex)]
1014: sysApplElmtPastRunName.2.0.6180 (octet string) C:\PROGRA~1\CSCOpx\bin\cwjava.exe
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.62.69.6E.5C.63.77.6A.61.76.61.2E.65.78.65 (hex)]
1015: sysApplElmtPastRunParameters.2.0.6180 (octet string)
```

```
-Dcom.smarts.conf.clientConnect=C:\PROGRA~1\CSCOpx\objects\smarts\conf\clientConnect.conf
-Djava.security.policy=C:\PROGRA~1\CSCOpx\lib\jre2\lib\security\java.policy -Xmx128m  -cw:jre
C:\PROGRA~1\CSCOpx\lib\jre  -cw:xrs  -cp:pmf conf\vhm\vhm.classpath
[2D.44.63.6F.6D.2E.73.6D.61.72.74.73.2E.63.6F.6E.66.2E.63.6C.69.65.6E.74.43.6F.6E.6E.65.63.74.3D.43.3A.5C.
50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6F.62.6A.65.63.74.73.5C.73.6D.61.72.74.73.5C.63.6F.6E.66.5
C.63.6C.69.65.6E.74.43.6F.6E.6E.65.63.74.2E.63.6F.6E.66.20.20.2D.44.6A.61.76.61.2E.73.65.63.75.72.69.74.79
.2E.70.6F.6C.69.63.79.3D.43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6C.69.62.5C.6A.72.65.32.
5C.6C.69.62.5C.73.65.63.75.72.69.74.79.5C.6A.61.76.61.2E.70.6F.6C.69.63.79.20.2D.58.6D.78.31.32.38.6D.20.2
0.2D.63.77.3A.6A.72.65.20.43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6C.69.62.5C.6A.72.65.20
.20.2D.63.77.3A.78.72.73.20.20.2D.63.70.3A.70.6D.66.20.63.6F.6E.66.5C.76.68.6D.5C.76.68.6D.2E.63.6C.61.73.
73.70.61.74.68.20.20 (hex)]
1016: sysApplElmtPastRunCPU.2.0.6180 (timeticks) 0 days 00h:01m:52s.06th (11206)
1017: sysApplElmtPastRunMemory.2.0.6180 (integer) 970216
1018: sysApplElmtPastRunNumFiles.2.0.6180 (integer) 0
1019: sysApplElmtPastRunUser.2.0.6180 (octet string) SYSTEM [53.59.53.54.45.4D (hex)]
1020: sysApplPastRunMaxRows.0 (integer) 2000
1021: sysApplPastRunTableRemItems.0 (integer) 20
1022: sysApplPastRunTblTimeLimit.0 (integer) 86400
1023: sysApplElemPastRunMaxRows.0 (integer) 2000
1024: sysApplElemPastRunTableRemItems.0 (integer) 20
1025: sysApplElemPastRunTblTimeLimit.0 (integer) 86400
1026: sysApplAgentPollInterval.0 (integer) 60
1027: sysApplMap.2.888.0.0 (integer) 0

1082: sysApplMap.2.15056.0.28 (integer) 2
***** SNMP QUERY FINISHED *****
```

Cisco Secure ACS によるセキュリティの設定

ここでは、Cisco Secure ACS を使用して Service Monitor を設定する方法を説明します。

始める前に：統合の注意事項

(注) Service Monitor と Cisco Secure ACS を統合できるのは、これらが個別のシステムにインストールされている場合だけです。これは、Service Monitor を Cisco Secure ACS の AAA クライアントとして設定する必要があるためです。

Common Services ログイン モジュールとユーザ ロールの詳細については、P.6-7 の「ユーザの設定（ACS および非 ACS）」を参照してください。

ここでは、次の注意事項について説明します。Cisco Secure ACS と Service Monitor の統合を開始する前に必ずお読みください。

- 同じ Cisco Secure ACS を使用する同じアプリケーションの複数のインスタンスが設定を共有します。どの変更も、そのアプリケーションのすべてのインスタンスに影響を及ぼします。

  たとえば、Cisco Secure ACS で 3 つの Service Monitor を設定して、Service Monitor のロールを Cisco Secure ACS に作成します（たとえば、*SMSU*）。このロールは、3 つのサーバすべてで動作する Service Monitor の、ライセンスが付与されたバージョンによって共有されます。
- ユーザは、シスコ ユニファイド コミュニケーション管理スイートのアプリケーションごとに異なるアクセス特権を持つことができます。

  たとえば、ユーザ *SMSU* は、次の特権を持つことができます。
  - Service Monitor のシステム管理者
  - Operations Manager のネットワーク オペレータ
  - Service Monitor のネットワーク管理者
  - Operations Manager のヘルプ デスク

- アプリケーションを Cisco Secure ACS を使用して設定した後に再度インストールすると、そのアプリケーションは古い設定を継承します。

（注） これは、Cisco Secure ACS バージョン 3.2.3 以前を使用している場合に当てはまります。

- Common Services を使用するには、次を実行する必要があります。
  - AAA モードを ACS に設定：このタスクを完了するには、Cisco Secure ACS から取得した、IP アドレスまたはホスト名、ポート、admin ユーザ名およびパスワード、共有秘密鍵の情報を指定する必要があります。

（注） Common Services AAA モードを ACS に設定すると、同じサーバ上で動作するすべてのシスコ ユニファイド コミュニケーション管理スイートのアプリケーションが Cisco Secure ACS に登録され、認証および認可に使用されます。Service Monitor および Operations Manager が ACS モードでサーバにインストールされると、Service Monitor、Operations Manager、および Common Services はすべて Cisco Secure ACS を使用します。

  - システム アイデンティティ セットアップ ユーザ名のセットアップ：このユーザは、Service Monitor のインストール時に設定されています。詳細については、Service Monitor ホーム ページ上の CiscoWorks リンクをクリックして、**Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup** の順に選択します。
- Cisco Secure ACS 上では、システム アイデンティティ セットアップ ユーザと同じユーザ名でユーザを設定する必要があります。Service Monitor の場合、そのユーザには、Cisco Secure ACS のネットワーク管理者特権が必要です。
- ACS モードでは、フォールバックは認証目的でだけ提供されています（ログイン モジュールに障害が発生した場合や、誤って自分自身または他のユーザをロック アウトしてしまった場合は、フォールバック オプションを使用して Service Monitor にアクセスできます）。ACS での認証が失敗すると、Service Monitor は次の処理を行います。
  1. 非 ACS モード（CiscoWorks ローカル モード）での認証を試みます。
  2. 非 ACS 認証に成功すると、ログイン モードを CiscoWorks ローカルに変更するように指示するダイアログボックスが表示されます（その操作を非 ACS モードで実行する権限がある場合にだけ実行できます）。

（注） 非 ACS モードでの認証に失敗した場合、ログインは許可されません。

ACS モードの設定の詳細については、Service Monitor ホーム ページ上の CiscoWorks リンクをクリックして、**Common Services > Server > Security > AAA Mode** を選択し、**Help** をクリックします。

Cisco Secure ACS での Service Monitor の設定

Cisco Secure ACS を使用して CiscoWorks サーバを ACS モードに設定したら、Cisco Secure ACS で次のタスクを実行します。

1. **Shared Profile Components** をクリックして、Cisco Unified Service Monitor（Service Monitor）アプリケーション エントリが存在することを確認します。
2. Cisco Secure ACS 上の認証設定（ユーザ単位またはグループ単位）に基づいて、User Setup または Group Setup のどちらかをクリックします。

   Cisco Secure ACS で、**Interface Configuration > TACACS + (Cisco IOS)** を使用して、Cisco Unified Service Monitor のユーザ単位またはグループ単位の設定を確認します。
3. ユーザまたはグループに適切な Service Monitor 特権を割り当てます。

   Service Monitor の場合、必ずシステム アイデンティティ セットアップ ユーザと同じ名前のユーザを Cisco Secure ACS に設定し、ネットワーク管理者特権を付与する必要があります。

（注）システム アイデンティティ セットアップ ユーザは、Service Monitor のインストール時に設定されています。詳細については、Service Monitor ホーム ページ上の CiscoWorks リンクをクリックして、**Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup** の順に選択します。

Cisco Secure ACS 上のロールは変更できます。

ステップ 1　**Shared Profile Components > Cisco Unified Service Monitor** を選択します。

ステップ 2　変更する Service Monitor ロールをクリックします。

ステップ 3　ビジネス ワークフローおよびニーズに適した Service Monitor タスクを選択します。

ステップ 4　**Submit** をクリックします。

（注）必要な場合は、Cisco Secure ACS で新たなロールを作成することもできます。

Service Monitor および Cisco Secure ACS の設定の確認

P.F-3 の「Cisco Secure ACS での Service Monitor の設定」のタスクを実行した後、次の手順で設定を確認します。

1. Cisco Secure ACS に定義されているユーザ名で Service Monitor にログインします。
2. タスクを実行する場合、実行できるのは、Cisco Secure ACS での特権に基づいて実行できる権限のあるタスクだけです。

   たとえば、特権がヘルプ デスクの場合、

   - Service Monitor によって管理されている Cisco 1040 を表示できます。
   - Service Monitor の管理対象となる Cisco 1040 を追加したり削除したりすることはできません。

A

C

D

H

I

M

O

P

S

T

W

あ

い

う

え

き

く

け

こ

さ

し

せ

た

ち

つ

て

と

に

は

ひ

ふ

へ

ほ

ま

ゆ

ら

れ

ろ