IP Communications Service Monitor ユーザ ガイド

CiscoWorks

Customer Order Number: DOC-J-7817056=
Text Part Number: 78-17056-01-J

CONTENTS

このマニュアルについて

このマニュアルでは、IP Communications 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。

製品マニュアル

（注） 初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルのアップデートについては、Cisco.com で確認してください。

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 IP Communications Service Monitor Release 1.0	• 印刷マニュアルが製品に同梱されています。 • Cisco.com の次の場所で入手可能です。http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/ipcsm/relnote/index.htm.
Quick Start Guide for IP Communications Service Monitor 1.0	• PDF が製品 CD に収録されています。 • Cisco.com の次の場所で入手可能です。http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/ipcsm/quicksg/index.htm
User Guide for IP Communications Service Monitor	• PDF が製品 CD に収録されています。 • Cisco.com の次の場所で入手可能です。http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/ipcsm/usergd/index.htm. • 印刷マニュアルを注文します（Part Number DOC-7817056=）。[1]
文脈依存オンライン ヘルプ	• ナビゲーション ツリーのオプションを選択し、次に **Help** をクリックします。 • ダイアログボックスの Help ボタンをクリックします。

1. P.x 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。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法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）

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

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、包括的なライブラリです。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複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation 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（Cisco Direct Customers）の場合、次の URL の Cisco Marketplace から Product Documentation DVD（Product Number DOC-DOCDVD=）を発注できます。

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

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

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

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

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および注意事項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

勧告および注意事項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）フィードにアクセスしてください。

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 8.*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。

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 Technical Support & Documentation 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 Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation 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/techsupport

Cisco Technical Support & Documentation 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） Web 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（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI 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。

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 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

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

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

  デジタル版には、次の URL からアクセスできます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*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

- シスコシステムズ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

- 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

CHAPTER 1

IP Communications Service Monitor 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。

Service Monitor を使用する前に

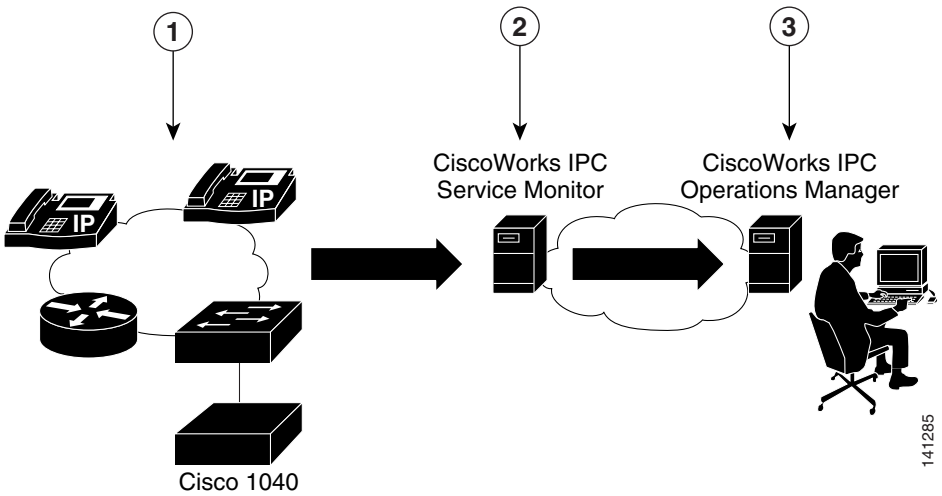
IP Communications Service Monitor（Service Monitor）は、音声ネットワークにインストールされている Cisco 1040 センサー（Cisco 1040）からデータを受信して分析します。ライセンスされている Service Monitor の各インスタンスは、複数の Cisco 1040 のプライマリ Service Monitor として機能します。また、Service Monitor は、Service Monitor のライセンスされている他のインスタンスによって管理される Cisco 1040 のセカンダリおよびターシャリ Service Monitor として動作するように設定することもできます。Service Monitor が使用不能となった場合は、このプライマリ Service Monitor が再び使用可能になるまで、Cisco 1040 はセカンダリまたはターシャリ の 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。

IP Communications 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、サービス品質アラート ダッシュボードでのイベントの表示、および最大 31 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 IP Communications Operations Manager*』を参照してください。

図 1-1 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 1-1　Service Monitor の構成



1	Cisco 1040 は、コール RTP ストリームを監視します。	**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 到達不能トラップの生成（P.1-19）
- 使用される MIB と生成される SNMP トラップ（P.A-1）

Service Monitor の起動

（注） CiscoWorks ホームページに複数の Service Monitor インスタンスが表示される場合は、次のようになります。

- ローカル Service Monitor 名が常にリストの先頭に表示されます。
- Service Monitor インスタンスを、サーバおよびホスト名によって、Common Services インスタンスにマップできます（Service Monitor@*server*、CS@*server*）。

ステップ 1　IP Communications Service Monitor ペインの CiscoWorks ホームページから、**Service Monitor** > **Service Monitor Operations** を選択します。新しいウィンドウが開き、Service Monitor ホームページが表示されます。

Service Monitor のセットアップ

ステップ 1　Service Monitor ホームページから、**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
Auto Registration オプション ボタン	次のいずれかを選択します。 • Enable：Cisco 1040　は、ネットワークに結合されると、デフォルトのコンフィギュレーション ファイルに指定されている情報を使用して、Service Monitor に自動的に登録されます。P.1-9 の「自動登録およびコンフィギュレーション ファイルについて」および P.1-13 の「デフォルト設定の編集（自動登録）」を参照してください。 • Disable：Cisco 1040　は、ネットワークに結合されると、その Cisco 1040 専用のコンフィギュレーション ファイルが作成されている場合にだけ、Service Monitor に登録されます。P.1-10 の「Cisco 1040 の追加（手動登録）」を参照してください。 デフォルト値は Disable です。

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。 デフォルト値は Disable です。 (注) コール メトリックは、Service Monitor をインストールしたときに指定したディレクトリにアーカイブされます。
Image File Directory フィールド	CiscoWorks サーバ上のディレクトリ。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 ファイルが保存されます。編集できないため、グレー表示されています。 (注) このディレクトリは、Service Monitor のインストール時に指定されます。
MOS Threshold フィールド	Service Monitor が SNMP トラップを送信する場合の下限値を入力します。デフォルト値は 3.5 です。最小値は 1.0、最大値は 5.0 です。
Starting Cisco 1040 ID リストおよびフィールド	リスト内のデフォルトの頭文字を受け入れて、フィールドに 3 桁の数字を入力します。Cisco 1040 ID は 1 つの文字と 3 桁の数字から構成されます。たとえば、A100 です。 Service Monitor は、この ID を最初の Cisco 1040 に割り当ててそれを登録し、この ID を基準に増分してそれ以降の Cisco 1040 ID を割り当てます。
TFTP Server フィールドおよび Port フィールド	IP アドレス（または DNS 名）とポート番号を入力します。
トラップ転送パラメータ	
SNMP Community String	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。デフォルトは public です。
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 からのデータを操作および表示するには（たとえば、Service Quality Alerts ダッシュボードを使用するには）、Operations Manager がトラップ レシーバとして設定されているシステムを指定します。 • 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 トラップを生成して、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。

Syslog ファイル サイズの確認

Service Monitor は、Cisco 1040 から syslog メッセージを受信します。syslog ファイルが過剰に大きくなると、Service Monitor は受信したメッセージを処理できません。syslog ファイルのサイズをチェックし、大きい場合は削除します。P.2-4 の「Syslog ファイルの管理」を参照してください。

TFTP サーバへのイメージ ファイルおよびコンフィギュレーション ファイルのコピー

Service Monitor をインストールするときに、Service Monitor が Cisco 1040 用のファイルを保存するイメージ ファイル ディレクトリの名前を指定します。Service Monitor をインストールすると、ディレクトリが作成され、Cisco 1040 のバイナリ イメージ ファイルとデフォルトのコンフィギュレーション ファイルが保存されます。

サイトにセキュリティ手順が設定されている場合があるため、それを適用できるようにするために、Service Monitor は TFTP サーバへのファイルのコピーを行いません。次のように、Cisco 1040 のバイナリ イメージ ファイルとコンフィギュレーション ファイルを、TFTP サーバに手動でコピーする必要があります。

- Cisco 1040 バイナリ イメージ ファイル：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、次のようになります。

  ```
  SvcMonAA2_24.img
  ```

- Cisco 1040 コンフィギュレーション ファイル：次の表に示すように、コンフィギュレーション ファイルをアップデート後にコピーします。

コンフィギュレーション ファイルをコピーする前の操作	イメージ ファイル ディレクトリから TFTP サーバにコピーするファイル
デフォルト コンフィギュレーション ファイルの編集（自動登録をイネーブルにする場合は、デフォルト コンフィギュレーション ファイルも編集する必要があります）	QOVDefault.CNF
Cisco 1040 の追加（手動登録）	QOV*macaddress*.CNF：MAC アドレスが指定された、Cisco 1040 のコンフィギュレーション ファイル
Cisco 1040 のコンフィギュレーション ファイルの編集	

イメージ ファイルのディレクトリ パスと TFTP サーバの IP アドレスが Setup ページに表示されます。P.1-3 の「Service Monitor のセットアップ」を参照してください。

（注）

- 複数の Service Monitor インスタンスが同じ TFTP サーバを使用するように設定しており、自動登録がイネーブルの場合は、すべての Cisco 1040 が同じプライマリ Service Monitor に登録されます。別の Service Monitor に登録する必要のある Cisco 1040 の場合は、それぞれについてのコンフィギュレーション ファイルをアップデートします。P.1-11 の「特定の Cisco 1040 の設定の編集」を参照してください。
- 複数の Service Monitor インスタンスが複数の TFTP サーバを使用するように設定している場合は、P.1-9 の「複数の TFTP サーバを使用する場合の Service Monitor および Cisco 1040 の設定」を参照してください。

Cisco 1040 の管理

（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 Details ページについて

ステップ 1　Service Monitor ホームページで、**Cisco 1040 Management** を選択します。Cisco 1040 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 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.1-7 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	削除、リセット、または時刻を設定する Cisco 1040 を選択します。
ID カラム	ID をクリックすると、Cisco 1040 の HTML ページが表示されます（P.1-17 の「Cisco 1040 Web インターフェイスの使用方法」を参照）。
Status カラム	次のいずれかを表示します。 • Not Registered：どの Service Monitor にも登録されていません。 • Registered：プライマリ Service Monitor に登録済みです。 • Failover：セカンダリまたはターシャリ Service Monitor に登録済みです。 • Unreachable：応答していません。
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。

GUI の要素	説明 / 処理
Service Monitor カラム	次の両方を表示します。 • Assigned：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 • Active：Cisco 1040 が現在データを送信中の Service Monitor の IP アドレスまたはホスト名（Cisco 1040 がセカンダリまたはターシャリ Service Monitor にフェールオーバーしている場合にだけ割り当てられる Service Monitor とは異なります）。
Last Reset Time カラム	Cisco 1040 が最後にリブートされた日付と時刻
Edit カラム	(Edit) リンクをクリックして、Cisco 1040 の設定を編集します。P.1-11 の「特定の Cisco 1040 の設定の編集」を参照してください。
View カラム	(**View**) リンクをクリックして、Cisco 1040 の設定の詳細を表示します。

（注） Service Monitor は、12 台以上の Cisco 1040 が登録されている場合でも、Cisco 1040 Details ページには最大 11 台の Cisco 1040 を表示します。

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　Comma-Separated Values（CSV; カンマ区切り形式）ファイルまたは PDF のいずれかのオプション 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。

特定の Cisco 1040 の詳細の表示

Cisco 1040 Detail ダイアログボックスを開くと、次に説明する Cisco 1040 Information テーブルが表示されます。

フィールド	説明 / 処理
	Cisco 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.1-7 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。

フィールド	説明 / 処理
ID リンク	Cisco 1040 ID：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.1-17 の「Cisco 1040 Web インターフェイスの使用方法」を参照してください。
Status	次のいずれかを表示します。 • Not Registered：どの Service Monitor にも登録されていません。 • Registered：プライマリ Service Monitor に登録済みです。 • Failover：セカンダリまたはターシャリ Service Monitor に登録済みです。 • Unreachable：応答していません。
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.1-11 の「特定の Cisco 1040 の設定の編集」を参照）。
Tertiary Service Monitor	ターシャリ 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.1-11 の「特定の Cisco 1040 の設定の編集」を参照）。
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、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 TFTP サーバにコピーして、Cisco 1040 をリセットする必要があります（P.1-11 の「特定の Cisco 1040 の設定の編集」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.1-14 の「Cisco 1040 のリセット」を参照）。
Description	ユーザが入力した Cisco 1040 の説明（P.1-11 の「特定の Cisco 1040 の設定の編集」を参照）。

Cisco 1040 の Service Monitor への登録

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。

（注） このコンフィギュレーション ファイルは自動登録プロセスによって作成されます。また、Cisco 1040 を手動で追加しても作成されます。このコンフィギュレーション ファイルを TFTP サーバにコピーする必要があります。詳細については、P.1-10 の「Cisco 1040 の追加（手動登録）」および P.1-5 の「TFTP サーバへのイメージ ファイルおよびコンフィギュレーション ファイルのコピー」を参照してください。

- QOVDefault.CNF：デフォルトのコンフィギュレーション ファイル。Service Monitor で自動登録がイネーブルの場合に使用されます（P.1-3 の「Service Monitor のセットアップ」を参照）。

(注)　デフォルトのコンフィギュレーション ファイルは、Service Monitor が設定されているサーバにインストールされます。Cisco 1040 がこのファイルを使用できるようにするには、自動登録をイネーブルにし、デフォルトのコンフィギュレーション ファイルを編集して（P.1-13 の「デフォルト設定の編集（自動登録）」を参照）、それを TFTP サーバにコピーする必要があります（P.1-5 の「TFTP サーバへのイメージ ファイルおよびコンフィギュレーション ファイルのコピー」を参照）。

自動登録およびコンフィギュレーション ファイルについて

自動登録がイネーブルの場合、新たに接続された Cisco 1040 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。Cisco 1040 が Service Monitor に登録されると、コンフィギュレーション ファイル QOV<*MAC アドレス*>.CNF が、イメージ ファイル ディレクトリに作成されます。このコンフィギュレーション ファイルを TFTP サーバにコピーする必要があります。P.1-5 の「TFTP サーバへのイメージ ファイルおよびコンフィギュレーション ファイルのコピー」を参照してください。その後、Cisco 1040 は、リセットされるたびに、QOV<*MAC アドレス*>.CNF を使用して Service Monitor に登録されます。

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。したがって、同じ TFTP サーバを使用する各 Cisco 1040 は同じ Service Monitor に登録されます。

(注)　複数の Service Monitor が同じ TFTP サーバを共有しており、いずれかの Cisco 1040 をデフォルトのコンフィギュレーション ファイルにリストされている Service Monitor とは異なるプライマリ、セカンダリ、およびターシャリ Service Monitor に登録する場合は、自動登録が完了した後に、該当する Cisco 1040 のコンフィギュレーション ファイルを編集する必要があります。P.1-11 の「特定の Cisco 1040 の設定の編集」を参照してください。

複数の TFTP サーバを使用する場合の Service Monitor および Cisco 1040 の設定

ライセンスが付与されている複数の Service Monitor インスタンスがある場合は、それらが 1 つの TFTP サーバを使用するか、または複数の TFTP サーバを使用するかを設定できます。複数の TFTP サーバを使用する場合は、各 TFTP サーバが Cisco 1040 ごとのコンフィギュレーション ファイルの現在のコピーを保持しているように保証します。任意のファイル複製メカニズムを使用して、各 TFTP サーバ上のすべての QOV<*macaddress*>.CNF ファイルを、他の TFTP サーバに完全に複製する必要があります。

これを実行しておくと、Cisco 1040 は、異なる TFTP サーバを使用する Service Monitor にフェールオーバーしたときでも、その Cisco 1040 用に作成された特定のコンフィギュレーション ファイルを検索してロードできます。TFTP サーバの正しいコンフィギュレーション ファイルにアクセスすることで、Cisco 1040 は、別の TFTP サーバを使用するフェールオーバー Service Monitor に登録されている間も自身の ID を保持できます。

(注)　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ても、Cisco 1040 はそのコンフィギュレーション ファイルをロードしません。Cisco 1040 が TFTP サーバからコンフィギュレーション ファイルをロードするのは、フェールオーバー時またはリセット時だけです（P.1-14 の「Cisco 1040 のセカンダリまたはターシャリ Service Monitor へのフェールオーバーについて」および P.1-14 の「Cisco 1040 のリセット」を参照）。

Cisco 1040 の追加（手動登録）

（注）　自動登録がイネーブルの場合は、必要に応じて、Cisco 1040 を接続する前に、Cisco 1040 を Service Monitor に手動で追加できます。

ステップ 1　Service Monitor ホームページから、**Cisco 1040 Management** を選択します。

ステップ 2　**Add** をクリックします。Add Cisco 1040 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
Cisco 1040 ID	デフォルトの頭文字を受け入れて、3 桁の数字を入力します。Cisco 1040 ID は 1 つの文字と 3 桁の数字から構成されます。たとえば、A100 です。 （注）　既存の Cisco 1040 ID を入力すると、Service Monitor がエラー メッセージを表示します。この場合は、別の 3 桁の数字を入力します。
Image Filename	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。 SvcMng< 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、次のようになります。 `SvcMonAA2_24.img` 詳細については、P.1-5 の「TFTP サーバへのイメージ ファイルおよびコンフィギュレーション ファイルのコピー」および P.1-15 の「Cisco 1040 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。
Tertiary 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。プライマリおよびセカンダリ 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。コンフィギュレーション ファイルが、Service Monitor がインストールされているサーバに保存されます。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（MAC アドレスの表示については、P.1-17 の「Cisco 1040 Web インターフェイスの使用方法」を参照してください）。

ステップ 5　コンフィギュレーション ファイルを、Service Monitor がインストールされているサーバのイメージ ファイル ディレクトリから TFTP サーバにコピーします。Cisco 1040 を接続して、リセットすると、このコンフィギュレーション ファイルがロードされます。

（注）　イメージ ファイル ディレクトリ パスと TFTP サーバ アドレスが Setup ページに表示されます（P.1-3 の「Service Monitor のセットアップ」を参照してください）。

複数の TFTP サーバを使用している場合は、P.1-9 の「複数の TFTP サーバを使用する場合の Service Monitor および Cisco 1040 の設定」を参照してください。

特定の Cisco 1040 の設定の編集

（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。

この手順では、Cisco 1040 のコンフィギュレーション ファイルをアップデートします。コンフィギュレーション ファイルの編集後は、それを TFTP サーバにコピーして、Cisco 1040 をリセットする必要があります。

ステップ 1　Service Monitor ホームページで、**Cisco 1040 Management** を選択します（P.1-6 の「Cisco 1040 Details ページについて」を参照）。

ステップ 2　変更する Cisco 1040 の（**Edit**）リンクをクリックします。

ステップ 3　次のフィールドをアップデートします。

GUI の要素	説明 / 処理
Cisco 1040 ID	ID を変更する場合は、デフォルトの頭文字を受け入れて、3 桁の数字を入力します。Cisco 1040 ID は 1 つの文字と 3 桁の数字から構成されます。たとえば、A100 です。 **（注）** 既存の Cisco 1040 ID を入力すると、Service Monitor がエラー メッセージを表示します。
Image Filename	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。たとえば、次のようになります。 `SvcMonAA2_24.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。 • 1 は、マイナー リリース番号です。 • 6 は、バグフィックス番号です。 詳細については、P.1-5 の「TFTP サーバへのイメージ ファイルおよびコンフィギュレーション ファイルのコピー」および P.1-15 の「Cisco 1040 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。
Tertiary 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。プライマリおよびセカンダリ 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。

ステップ 5　コンフィギュレーション ファイルを、Service Monitor がインストールされているサーバのイメージ ファイル ディレクトリから TFTP サーバにコピーします。Cisco 1040 を接続して、リセットすると、このコンフィギュレーション ファイルがロードされます。

（注） イメージ ファイル ディレクトリ パスと TFTP サーバ アドレスが Setup ページに表示されます（P.1-3 の「Service Monitor のセットアップ」を参照してください）。

複数の Service Monitor インスタンスがあり、それらが異なる TFTP サーバを使用するように設定している場合は、P.1-9 の「複数の TFTP サーバを使用する場合の Service Monitor および Cisco 1040 の設定」を参照してください。

ステップ 6　Cisco 1040 をリセットします。P.1-14 の「Cisco 1040 のリセット」を参照してください。

デフォルト設定の編集（自動登録）

デフォルトのコンフィギュレーション ファイルを編集する場合、Cisco 1040 は、Service Monitor に自動的に登録するように指定した情報を使用できます。デフォルトのコンフィギュレーション ファイルを編集して、プライマリ、セカンダリ、およびターシャリ Service Monitor と、Cisco 1040 のイメージ ファイル名を指定します。ファイルを編集した後、それを Service Monitor に指定された TFTP サーバにコピーする必要があります。

（注）　デフォルトの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。デフォルトの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　Service Monitor ホームページで、**Default Configuration** を選択します。Cisco 1040 Default Configuration ページが表示されます。

ステップ 2　次のフィールドに情報を入力します。

- 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。
- 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。
- Tertiary 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。
- Image Filename：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。たとえば、次のようになります。

  ```
  SvcMonAA2_24.img
  ```

ステップ 3　**OK** をクリックします。Service Monitor が変更を保存します。

ステップ 4　デフォルトのコンフィギュレーション ファイル QOVDefault.CNF を、Service Monitor がインストールされているサーバのイメージ ファイル ディレクトリから TFTP サーバにコピーします。

（注）　イメージ ファイル ディレクトリ パスと TFTP サーバ アドレスが Setup ページに表示されます（P.1-3 の「Service Monitor のセットアップ」を参照）。

Cisco 1040 のセカンダリまたはターシャリ Service Monitor へのフェールオーバーについて

ここでは、Cisco 1040 がどのように Service Monitor が到達不能であることを判別し、別の Service Monitor にフェールオーバーするかを説明します。

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が受信されない場合、Cisco 1040 はセカンダリ（またはターシャリ）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。

（注） Cisco 1040 は同じ ID を保持します。複数の TFTP サーバを使用している場合は、P.1-9 の「複数の TFTP サーバを使用する場合の Service Monitor および Cisco 1040 の設定」を参照してください。

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。

Cisco 1040 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　Service Monitor ホームページで、**Cisco 1040 Management** を選択します（P.1-6 の「Cisco 1040 Details ページについて」を参照）。

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 Cisco 1040** をクリックします。

Cisco 1040 の時刻の設定

（注）　Service Monitor がインストールされているサーバに、Windows タイム サービスが正しく設定され、動作していることを確認してください。

次の手順で、Service Monitor がインストールされているサーバから現在の時刻を取得して、選択された各 Cisco 1040 にその時刻を設定します。

ステップ 1　Service Monitor ホームページで、**Cisco 1040 Management** を選択します（P.1-6 の「Cisco 1040 Details ページについて」を参照）。

ステップ 2　時刻を設定する Cisco 1040 のチェックボックスを選択します。

（注）　Cisco 1040 の Status カラムに Failover と表示されている場合は、それを選択解除します。現時点では時刻は設定できません。

ステップ 3　**Set Time** をクリックします。

（注）　セカンダリまたはターシャリ Service Monitor にフェールオーバーした Cisco 1040 に時刻を設定するには、次のいずれかを実行します。

- ステータスが Registered になるまで待機します。このステータスは、Cisco 1040 が再びプライマリ Service Monitor によって管理されていることを示しています。時刻を設定できます。
- Cisco 1040 の設定を編集し、プライマリ Service Monitor をアクティブ Service Monitor に設定します。P.1-11 の「特定の Cisco 1040 の設定の編集」を参照してください。その後、Cisco 1040 に時刻を設定します。

Cisco 1040 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. IP Communications 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.1-3 の「Service Monitor のセットアップ」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.1-3 の「Service Monitor のセットアップ」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_24.img となります。

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.1-11 の「特定の Cisco 1040 の設定の編集」を参照してください。

Cisco 1040 の移動

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、次の手順を実行します。Cisco 1040 のコンフィギュレーション ファイルを編集して、それを TFTP サーバにコピーします（P.1-11 の「特定の Cisco 1040 の設定の編集」を参照）。

ステップ 2　Cisco 1040 を切断します。

ステップ 3　Cisco 1040 を新しい場所に接続します。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 ID を保持します。

Cisco 1040 の削除

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　Service Monitor ホームページで、**Cisco 1040 Management** を選択します（P.1-6 の「Cisco 1040 Details ページについて」を参照）。

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。

Cisco 1040 Web インターフェイスの使用方法

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.1-17 の「TFTP サーバ上のコンフィギュレーション ファイルの表示」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 Details ページの **(View)** をクリックします。P.1-6 の「Cisco 1040 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 Device Information ウィンドウが表示されます。

- **ID**：Cisco 1040 ID
- **MAC Address**：Cisco 1040 の MAC アドレス
- **Time stamp**：Cisco 1040 の現在時刻
- **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 のデータ送信先の Service Monitor の名前。これは、プライマリ、セカンダリ、またはターシャリ Service Monitor のいずれかになります。
- **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
- **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.1-15 の「Cisco 1040 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.1-11 の「特定の Cisco 1040 の設定の編集」を参照してください。

TFTP サーバ上のコンフィギュレーション ファイルの表示

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、セカンダリ、およびターシャリ）の IP アドレスまたは DNS 名。セミコロンで区切られます。
- ID：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 ID
- 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

Cisco 1040 コール メトリックのアーカイブ

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.1-3 の「Service Monitor のセットアップ」を参照してください。デフォルトでは、Service Monitor は、Cisco 1040 から受信したデータを保存しません。ただし、コール メトリックのアーカイブをイネーブルにすると、Service Monitor はサーバ上のディレクトリにデータを保存します。ディレクトリは、Service Monitor のインストール時に指定されます。

Service Monitor は、毎日午前 0 時にこのディレクトリに新しいアーカイブ ファイルを作成します。アーカイブ 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_20051101.csv は、2005 年 11 月 1 日のアーカイブ ファイルです。

詳細な分析にデータを使用したり、アーカイブをオフにしたりできます (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 1-1 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 1-1　Service Monitor アーカイブ コール メトリックのデータ形式

説明	値
Cisco 1040 ID	Cisco 1040 ID は 1 つの文字と 3 桁の数字から構成されます。たとえば、A100 です。
タイム スタンプ	日付および時刻
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
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 6：G722 64k 9：G7231 10：G728 11：G729
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 >

Cisco 1040 到達不能トラップの生成

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.1-3 の「Service Monitor のセットアップ」および P.A-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。

CHAPTER 2

データ管理とシステム管理

この項では、次のトピックについて説明します。

Service Monitor データの管理

IP Communications Service Monitor（Service Monitor）は、登録されている Cisco 1040 からコール メトリック データを受信し処理します。オプションで、Service Monitor は、インストール時にアーカイブ用として指定されたディレクトリに、コール メトリック データをアーカイブします。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.1-3 の「Service Monitor のセットアップ」を参照してください。

(注)　コール メトリックのアーカイブがイネーブルの場合、Service Monitor は、1 日あたり 1 つのデータ ファイルを作成します。各ファイルは午前 0 時に作成が開始されます。Service Monitor は、このファイルのバックアップや削除を行いません。

アーカイブがイネーブルの場合、次の操作を行う必要があります。

- ファイル システムをバックアップする方法と同じ方法で、Service Monitor データ ファイルをバックアップします（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）。
- どの時点でサーバから古いデータ ファイルを削除するかを決定します。

Service Monitor データベースのバックアップおよび復元

Service Monitor データベースには、Cisco 1040 の設定に関する情報が保存されます。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、Common Services ペインの CiscoWorks ホームページから、**Server** > **Admin** > **Backup** を選択し、Help をクリックして、その手順に従います。

Common Services には、データを復元するためのコマンドライン スクリプトがあります。手順を参照するには、Common Services ペインの CiscoWorks ホームページから **Server** > **Admin** > **Backup** を選択し、Help をクリックします。さらに、Restoring Data トピックへの Help リンクをクリックします。

Service Monitor データベースを復元するには、スイート名（*qovr*）を含むバックアップ ディレクトリ構造がわかっている必要があります。

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

表 2-1 に、バックアップ ディレクトリ構造を示します。

表 2-1　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。CiscoWorks Common Services スイートは cmf です。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）

表 2-1　Service Monitor バックアップ ディレクトリ構造（続き）

オプション	説明	使用方法
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

Common Services には、qovr.db のパスワードを含むデータベース パスワードを変更するためのコマンドライン スクリプトがあります。手順を参照するには、CiscoWorks ホームページで Help をクリックし、*データベース パスワード*を検索します。

Syslog ファイルの管理

syslog ファイルが過剰に大きくなると、Service Monitor はメッセージの処理を停止します。したがって、ファイルのサイズをチェックし、過剰に大きくなった場合はそれを削除する必要があります。

ステップ 1　Service Monitor サーバのコマンド プロンプトで、次のコマンドを入力し、syslog サービスとデーモン マネージャを停止します。

```
net stop crmlog
net stop crmdmgtd
```

ステップ 2　syslog.log ファイルを削除します。通常、このファイルは次の場所にあります。

```
NMSROOT\log\syslog.log
```

（注）　NMSROOT は、システム上の CiscoWorks 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。

ステップ 3　次のコマンドを入力して、syslog サービスとデーモン マネージャを再開します。

```
net start crmlog
net start crmdmgdt
```

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）　Common Services バックアップは、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 ファイルは、*NMSROOT*\log\qovr ディレクトリにあります。

- ProbeMgr.log：Cisco 1040 の通信が含まれます。
- QovrUI.log：Service Monitor ユーザ インターフェイスの処理が含まれます。
- Trapgen.log：アーカイブです。

（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。

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。

システム アプリケーション MIB のロギング レベルの変更の詳細については、P.2-13 の「システム アプリケーション MIB ログ ファイルの表示」を参照してください。

ユーザの設定（ACS および非 ACS）

CiscoWorks サーバには、CiscoWorks アプリケーションのユーザを認証および認可するためのメカニズムがあります。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。CiscoWorks サーバには、CiscoWorks アプリケーションのユーザを認証するための 2 種類のメカニズム（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。デフォルトでは、CiscoWorks サーバは CiscoWorks Local ログイン モジュールを使用します。Common Services の Permission Report に説明されているとおり、CiscoWorks は 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（Common Services ホームページから Permission Report を生成するには、**Server** > **Reports** > **Permission Report** を選択して、**Help** をクリックします）。詳細については、P.2-6 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.2-6 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、CiscoWorks Permission Report を使用します。CiscoWorks ホームページから、**Common Services** > **Server** > **Reports** > **Permission Report** > **Generate Report** を選択し、IP Communications Service Monitor 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　CiscoWorks サーバの AAA モードを確認します。Common Services ホームページから、**Server** > **Security** > **AAA Mode Setup** を選択し、ACS 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。

ステップ 2　Cisco Secure ACS サーバをチェックして、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 ロールを変更するには、次の手順に従います。

- 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。
- DCR への Cisco Secure ACS の影響（特に、ロールの依存関係）の詳細については、Common Services のオンライン ヘルプを参照してください。

（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 サーバに登録された Common Services サーバを使用している 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、CiscoWorks サーバに 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） CiscoWorks サーバ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 に追加されており、ネットワーク管理者特権を持っている必要があります。

CiscoWorks ログイン モジュールを使用すると、CiscoWorks サーバのネイティブ メカニズム（CiscoWorks Local ログイン モジュール）以外の認証ソース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 サービスを使用できます。

デフォルトでは、ACS モードの CiscoWorks サーバ認証方式には 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。
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、CiscoWorks システム管理タスクをすべて実行する特権があります。CiscoWorks ホームページで Permission Report を参照してください（**Common Services > Server > Reports > Permission Report**）。 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、Common Services クライアント アプリケーションをビジネス 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 CiscoWorks 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 CiscoWorks 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 > IP Communication 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 プロセスを起動および停止するには、Common Services ペインの CiscoWorks ホームページで、**Server** > **Admin** > **Processes** を選択し、Help をクリックして操作手順を参照してください。表 2-2 に、Service Monitor 関連の CiscoWorks プロセスをすべて示します。

表 2-2　Service Monitor 関連の CiscoWorks 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	—

CiscoWorks ホームページでの Service Monitor の追加登録

追加の Service Monitor を登録して、CiscoWorks ホームページに表示されるようにすることができます。登録可能な Service Monitor の数は無制限です。CiscoWorks ホームページは、各種アプリケーションのポータルにすぎません。ローカル Service Monitor 名が常に、CiscoWorks ホームページ上で最初に表示されます。

ホームページに複数の Service Monitor インスタンスがある場合は、常に、サーバ ホスト名（Service Monitor*@server*、CS*@server*）によって Service Monitor インスタンスを Common Services インスタンスにマップできます。

（注） Service Monitor のリモート バージョンを起動すると、CiscoWorks はユーザ自体を再認証するためのプロンプトを表示します。

ステップ 1　Common Services ホームページから、**Home Page > Application Registration** を選択します。Application Registration Status ページが表示されます。

ステップ 2　**Registration** をクリックします。Registration Location ページが開きます。

ステップ 3　Import from Other Servers オプション ボタンを選択して、**Next** をクリックします。Import Server's Attributes ページが開きます。

ステップ 4　Import Server's Attributes ページに、次の情報を入力します。

- Server Name：ホスト名または IP アドレス。
- Server Display Name：CiscoWorks ホームページに表示されるユーザ指定の名前。Service Monitor インスタンスを選択した場合は、その Service Monitor ホームページのタイトルとしても表示されます。
- Port：1741

ステップ 5　**Next** をクリックします。CiscoWorks は、リモート サーバが到達可能であることを確認します。

CiscoWorks ホームページで新しい Service Monitor サーバ インスタンスを選択する場合は、リモート ホストのユーザ名とパスワードを入力して認証する必要があります。

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環した監視：Service Monitor が常駐する 1 つのプラットフォーム、および CiscoWorks IP Communications Management Suite 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、付録 C「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.2-12 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.2-11 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.2-12 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.2-12 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.2-12 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、*SNMP サービスのインストール* 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.2-12 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 サービスのクレデンシャルを変更する必要があります。

（注） この目的でクレデンシャルを変更するために、SNMP サービスを再起動する必要はありません。

SNMP サービスのクレデンシャルは、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 CiscoWorks 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。また、一部の手順を実行するために、CiscoWorks デーモン マネージャと syslog マネージャを停止します。

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、CiscoWorks デーモン マネージャを停止します。

```
net stop crmdmgtd
```

b. **My Computer** > **Properties** > **Computer Name** > **Change** 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 サービスと syslog 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、次の両方のサービスの起動モードを Manual に変更します。

- CW2000 Daemon Manager
- CWCS syslog サービス

d. サーバをリブートします。

ステップ 2　md.properties ファイル（*NMSROOT*\lib\classpath\md.properties）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 を完了するためにこのホスト名が必要です。
  - 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、次の両方のサービスの起動モードを Automatic に変更します。

- CW2000 Daemon Manager
- CWCS syslog サービス

ステップ 11 サーバをリブートします。

ステップ 12 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.2-16 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.2-14 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 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.1-13 の「デフォルト設定の編集（自動登録）」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.1-11 の「特定の Cisco 1040 の設定の編集」を参照してください。

ステップ 2 Service Monitor サーバから TFTP サーバに、アップデートしたコンフィギュレーション ファイルをコピーします。P.1-5 の「TFTP サーバへのイメージ ファイルおよびコンフィギュレーション ファイルのコピー」を参照してください。

ステップ 3 Cisco 1040 をリセットします。P.1-14 の「Cisco 1040 のリセット」を参照してください。

ステップ 4 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.1-3 の「Service Monitor のセットアップ」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。

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

IP Communications 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 A-1 に、MOS 違反 SNMP トラップの詳細を記載します。

表 A-1　MOS 違反トラップの詳細

タグ	説明	値
TT	トラップ タイプ	1
01	Cisco 1040 ID	< 文字 ><1000 未満の 3 桁の数値 >
02	タイムスタンプ	<YYYYMMDDhhmm>
03	しきい値	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
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
B	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。 F0.F0.F0.58
C	受信デバイスの IP アドレス	IPv4 アドレス。次に例を示します。 F0.F0.F0.58

表 A-1　MOS 違反トラップの詳細（続き）

タグ	説明	値
D	コール データ レコードのコーデック	2：G711Alaw 64k 6：G722 64k 9：G7231 10：G728 11：G729
E	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
F	コール劣化の主な原因	J：ジッタ P：パケット損失
G	直前の 1 分間に失われた実際のパケット数	< 数値 >
H	直前の 1 分間に生じた実際のジッタ（ミリ秒単位）	< 数値 >

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

表 A-2　Cisco 1040 到達不能トラップの詳細

タグ	説明	値
TT	トラップ タイプ	2
01	Cisco 1040 ID	< 文字 ><1000 未満の 3 桁の数値 >
02	タイムスタンプ	<YYYYMMDDhhmm>

ライセンス

この付録では、IP Communications Service Monitor（Service Monitor）のライセンス情報を提供します。この章は、以下の項で構成されています。

ライセンスの概要

インストールを行う場合には、Service Monitor 1.0 の登録済みでライセンスを付与されたコピーを所持していることを確認してください。インストール スクリプトで、ライセンス情報の入力が要求されます。次のライセンス情報は、製品に付属し、ソフトウェア権利証明書に印刷されています。

フィールド	説明
Product Identification Number（PIN）	PIN はインストールのタイプを識別します。Service Monitor 1.0 は新規インストールです。 **（注）** 評価目的で Service Monitor をインストールする場合は、インストール時にライセンスの詳細情報を入力する必要はありません。
Product Authorization Key（PAK）	PAK は Cisco.com で Service Monitor 1.0 を登録するために使用され、リソース制限が含まれます。Cisco.com で PAK を登録すると、ライセンス ファイルを取得できます。

インストール時に、ライセンス情報を入力するように要求された場合は、次のいずれかを入力できます。

- PIN（および PAK）：PIN は必須です。PAK 番号は必要に応じて後から入力できます。
- ライセンス ファイルの場所：Cisco.com で PAK を登録して、ライセンス ファイルを受信している場合は、その場所を参照して入力できます。ライセンス ファイルは、Service Monitor 1.0 のインストールの前でも、または後でも取得できます（P.B-3 の「ライセンスの登録」を参照）。

新規インストールのライセンス

Service Monitor 1.0 のインストール スクリプトでは、PIN および PAK、またはライセンス ファイルの場所の情報を入力する必要があります。ライセンス ファイルの取得の詳細については、P.B-3 の「ライセンスの登録」を参照してください。

ライセンスの登録

ステップ 1　Cisco.com に PAK を登録して、ライセンス ファイルを取得します。

- Cisco.com の登録ユーザの場合は、次の URL から取得します。
  http://www.cisco.com/go/license
- Cisco.com の登録ユーザでない場合は、次の URL から取得します。
  http://www.cisco.com/go/license/public

（注）　PAK は、ソフトウェア権利証明書に印刷されています。

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 CiscoWorks 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。

ステップ 3　CiscoWorks ホームページで、ライセンス ファイルの場所を入力します（**Common Services > Server > Admin >Licensing** を選択します。詳細については、Common Services のオンライン ヘルプを参照してください）。

Service Monitor のライセンスの取得

Service Monitor のライセンスをまだ購入していない場合は、製品を購入された代理店から PAK を入手し、P.B-3 の「ライセンスの登録」の指示に従い、それを使用してライセンス ファイルを取得します。

次の手順で、Service Monitor のライセンスを購入済みかどうかを判別できます。

ステップ 1　CiscoWorks ホームページで、**Common Services > Server > Admin > Licensing** を選択します。License Information ページが表示され、ライセンスを付与された製品を示す表が表示されます。

ステップ 2　Name カラムで Service Monitor を検索します。

- Name カラムに Service Monitor がない場合は、有効なライセンスを持っていません。
- Name カラムに Service Monitor があるが、Status カラムに Purchased と表示されていない場合は、有効なライセンスを持っていません。

評価ライセンスのアップグレード

評価ライセンスを、Service Monitor 1.0 の登録済みでライセンスを付与されたコピーにアップグレードできます。

ステップ 1　PAK の入手については、製品を購入された代理店にお問い合せください。

ステップ 2　PAK を入手したら、P.B-3 の「ライセンスの登録」の手順に従います。評価コピーが、Service Monitor 1.0 の登録済みコピーに変換されます。

ライセンス リマインダ

次のバージョンの場合、Service Monitor 1.0 はリマインダ（注意喚起）を提供します。

評価バージョン：有効期限切れの前

Service Monitor の評価バージョンをインストールしている場合は、デフォルトの評価ライセンスの有効期限が切れる前に、Cisco.com からライセンス ファイルを入手する必要があります。詳細については、P.B-4 の「評価ライセンスのアップグレード」を参照してください。

Service Monitor を起動すると、ライセンス リマインダが表示されます。評価ライセンスの有効期限が切れる前に、次のプロンプトが 1 日間表示されます。

```
Go to Cisco.com and purchase Service Monitor
```

このメッセージは、ログインして Service Monitor にアクセスしようとするとアラートとして表示されます。1 日以内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。

購入バージョン：ライセンス ファイルなし

Service Monitor 1.0 を購入して、Service Monitor のインストール時に PIN を指定した場合は、PAK 番号を使用してそれを登録する必要があります。詳細については、P.B-3 の「ライセンスの登録」を参照してください。Service Monitor 1.0 は、インストールしてから 50 日以内に登録する必要があります。50 日以内に Service Monitor 1.0 を登録しなかった場合は、次のプロンプトが表示されます。

```
Go to Cisco.com and get the product registered.
```

Service Monitor 1.0 は完全に機能します。ただし、ライセンスが登録されるまで、継続してアラートが表示されます。

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 IP Communications Management Suite 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 およびその他の IP コミュニケーション 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.2-11 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.C-9 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。

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 C-1 に、システム アプリケーション MIB をサポートする CiscoWorks IP Communications Management Suite の Service Monitor などのアプリケーションに対応するインストール済みのパッケージについての情報を示します。

表 C-1　sysApplInstallPkgTable

MIB の行エントリ	MIB から見た説明	IP Communications Management Suite 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.

表 C-1　sysApplInstallPkgTable（続き）

MIB の行エントリ	MIB から見た説明	IP Communications Management Suite での使用方法
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	IP Communications Service Monitor 1.0 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	1.0.2 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 C-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 C-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 C-2 に、sysApplInstallElmtTable の内容を示します。

表 C-2　sysApplInstallElmtTable

MIB の行エントリ	MIB から見た説明	IP Communications Management Suite 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 C-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	CiscoWorks 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）

表 C-2　sysApplInstallElmtTable（続き）

MIB の行エントリ	MIB から見た説明	IP Communications Management Suite での使用方法
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 C-3 に、システム アプリケーション MIB をサポートする CiscoWorks IP Communications Management Suite の Service Monitor などのアプリケーションの現在のステータスを示します。

表 C-3　sysApplRunTable

MIB の行エントリ	MIB から見た説明	IP Communications Management Suite 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 C-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 CiscoWorks 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 C-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 C-4　sysApplElmtRunTable

MIB の行エントリ	MIB から見た説明	IP Communications Management Suite 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 C-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 C-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 C-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 C-5　sysApplPastRunTable

MIB の行エントリ	MIB から見た説明
sysApplInstallPkgIndex	sysApplInstallPkgTable（表 C-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 C-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 C-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 C-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プロセスごとに 1 つずつのエントリが含まれます。表 C-8 に、プロセス識別子から、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 C-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、IP Communications Operations Manager と Service Monitor がインストールされているシステムでの SYS-APPL-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.2
    0.53.79.73.74.65.6D.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.2
    0.53.79.73.74.65.6D.73.2C.20.49.6E.63.2E (hex)]
3: sysApplInstallPkgProductName.1 (octet string) IP Communications Service Monitor
    [49.50.20.43.6F.6D.6D.75.6E.69.63.61.74.69.6F.6E.73.20.53.65.72.76.69.63.65.20.4D.6
    F.6E.69.74.6F.72 (hex)]
4:  sysApplInstallPkgProductName.2 (octet string) IP Communications Operations Manager
    [49.50.20.43.6F.6D.6D.75.6E.69.63.61.74.69.6F.6E.73.20.4F.70.65.72.61.74.69.6F.6E.7
    3.20.4D.61.6E.61.67.65.72 (hex)]
5:  sysApplInstallPkgVersion.1 (octet string) 1.0.0 [31.2E.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) 2005-8-30,21:18:32 [07.D5.08.1E.15.12.20
    (hex)]
10: sysApplInstallPkgDate.2 (octet string) 2005-8-30,21:18:32 [07.D5.08.1E.15.12.20
    (hex)]
11: sysApplInstallPkgLocation.1 (octet string) D:\PROGRA~1\CSCOpx
    [44.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]
12: sysApplInstallPkgLocation.2 (octet string) D:\PROGRA~1\CSCOpx
    [44.3A.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)

111: sysApplInstallElmtDate.1.1 (octet string) 2005-8-30,21:18:32
    [07.D5.08.1E.15.12.20 (hex)]

112: sysApplInstallElmtDate.1.2 (octet string) 2005-8-30,21:18:32
    [07.D5.08.1E.15.12.20 (hex)]

160: sysApplInstallElmtPath.1.1 (octet string) D:\PROGRA~1\CSCOpx
    [44.3A.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) 2005-8-30,21:18:32
    [07.D5.08.1E.15.12.20 (hex)]

357: sysApplInstallElmtModifyDate.1.2 (octet string) 2005-8-30,21:18:32
    [07.D5.08.1E.15.12.20 (hex)]

405: sysApplInstallElmtCurSizeHigh.1.1 (integer) 0

454: sysApplInstallElmtCurSizeLow.1.1 (integer) 0

503: sysApplRunStarted.1.4 (octet string) 2005-9-27,15:51:53 [07.D5.09.1B.0F.33.35
    (hex)]

505: sysApplRunCurrentState.1.4 (integer) running(1)

507: sysApplPastRunStarted.1.2 (octet string) 2005-9-27,14:43:4 [07.D5.09.1B.0E.2B.04
    (hex)]

509: sysApplPastRunExitState.1.2 (integer) complete(1)

511: sysApplPastRunTimeEnded.1.2 (octet string) 2005-9-27,15:43:42
    [07.D5.09.1B.0F.2B.2A (hex)]

513: sysApplElmtRunInstallID.0.0.2468 (integer) 0

569: sysApplElmtRunTimeStarted.0.0.2468 (octet string) 2005-9-27,15:54:12
    [07.D5.09.1B.0F.36.0C (hex)]

625: sysApplElmtRunState.0.0.2468 (integer) running(1)

681: sysApplElmtRunName.0.0.2468 (octet string) D:\PROGRA~1\CSCOpx\bin\cwjava.exe
    [44.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.62.69.6E.5C.63.77.6A.61.7
    6.61.2E.65.78.65 (hex)]
737: sysApplElmtRunParameters.0.0.2468 (octet string) -DNMSROOT=D:\PROGRA~1\CSCOpx
    -cp:a lib\classpath\servlet.jar -Dvbroker.agent.port=42342
    com.inprise.vbroker.gatekeeper.GateKeeper -props
    D:\PROGRA~1\CSCOpx\lib\vbroker\gatekeeper.cfg
    [2D.44.4E.4D.53.52.4F.4F.54.3D.44.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.7
    8.20.2D.63.70.3A.61.20.6C.69.62.5C.63.6C.61.73.73.70.61.74.68.5C.73.65.72.76.6C.65.
    74.2E.6A.61.72.20.2D.44.76.62.72.6F.6B.65.72.2E.61.67.65.6E.74.2E.70.6F.72.74.3D.34
    .32.33.34.32.20.63.6F.6D.2E.69.6E.70.72.69.73.65.2E.76.62.72.6F.6B.65.72.2E.67.61.7
    4.65.6B.65.65.70.65.72.2E.47.61.74.65.4B.65.65.70.65.72.20.2D.70.72.6F.70.73.20.44.
    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.67.61.74.65.6B.65.65.70.65.72.2E.63.66.67 (hex)]

793: sysApplElmtRunCPU.0.0.2468 (timeticks) 0 days 00h:00m:03s.33th (333)

849: sysApplElmtRunMemory.0.0.2468 (integer) 4716

905: sysApplElmtRunNumFiles.0.0.2468 (integer) 0

961: sysApplElmtRunUser.0.0.2468 (octet string) casuser [63.61.73.75.73.65.72 (hex)]

1017: sysApplElmtPastRunInstallID.0.0.1132 (integer) 0

1064: sysApplElmtPastRunTimeStarted.0.0.1132 (octet string) 2005-9-27,14:43:45
    [07.D5.09.1B.0E.2B.2D (hex)]

1111: sysApplElmtPastRunTimeEnded.0.0.1132 (octet string) 2005-9-27,15:43:42
    [07.D5.09.1B.0F.2B.2A (hex)]

1158: sysApplElmtPastRunName.0.0.1132 (octet string) D:\PROGRA~1\CSCOpx\bin\cwjava.exe
    [44.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.62.69.6E.5C.63.77.6A.61.7
    6.61.2E.65.78.65 (hex)]

1206: sysApplElmtPastRunParameters.0.0.2060 (octet string) itemIpiu -app IPIUDbMonitor
    -dbserver IPIUDbEngine -sleep 1200 -error 90 -retry 10 -sterror 10 -stretry 5
    [69.74.65.6D.49.70.69.75.20.2D.61.70.70.20.49.50.49.55.44.62.4D.6F.6E.69.74.6F.72.2
```

```
    0.2D.64.62.73.65.72.76.65.72.20.49.50.49.55.44.62.45.6E.67.69.6E.65.20.2D.73.6C.65.
    65.70.20.31.32.30.30.20.2D.65.72.72.6F.72.20.39.30.20.2D.72.65.74.72.79.20.31.30.20
    .2D.73.74.65.72.72.6F.72.20.31.30.20.2D.73.74.72.65.74.72.79.20.35 (hex)]

1252: sysApplElmtPastRunCPU.0.0.1132 (timeticks) 0 days 00h:00m:00s.26th (26)

1299: sysApplElmtPastRunMemory.0.0.1132 (integer) 7488

1346: sysApplElmtPastRunNumFiles.0.0.1132 (integer) 0

1393: sysApplElmtPastRunUser.0.0.1132 (octet string) casuser [63.61.73.75.73.65.72
    (hex)]

1440: sysApplPastRunMaxRows.0 (integer) 2000
1441: sysApplPastRunTableRemItems.0 (integer) 20
1442: sysApplPastRunTblTimeLimit.0 (integer) 86400
1443: sysApplElemPastRunMaxRows.0 (integer) 2000
1444: sysApplElemPastRunTableRemItems.0 (integer) 20
1445: sysApplElemPastRunTblTimeLimit.0 (integer) 86400
1446: sysApplAgentPollInterval.0 (integer) 60
1447: sysApplMap.2.752.0.1 (integer) 1

1502: sysApplMap.2.10596.0.9 (integer) 2
***** SNMP QUERY FINISHED *****
```

Cisco Secure ACS による Service Monitor 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.2-6 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 CiscoWorks サーバ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。
- 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。

- CiscoWorks サーバで動作している IP Communications Management Suite アプリケーションごとに、Cisco Secure ACS 内でロールを作成する必要があります。

  たとえば、Service Monitor のロールを Cisco Secure ACS に作成する必要があります。これらのロールは、その他の IP Communications Management Suite アプリケーションとは共有されません。
- Cisco Secure ACS に作成したロールは、同じ Cisco Secure ACS に設定されたすべての CiscoWorks サーバによって共有されます。

  たとえば、Cisco Secure ACS で 3 つの CiscoWorks サーバを設定して、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 CiscoWorks 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、IP Communications Management Suite 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
- CiscoWorks で、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 CiscoWorks 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 CiscoWorks 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

- Cisco Secure ACS 上では、CiscoWorks サーバのシステム 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 CiscoWorks にアクセスできます）。ACS での認証が失敗すると、CiscoWorks は次の処理を行ないます。
  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。

CiscoWorks サーバを ACS モードで設定する方法の詳細については、『*User Guide for CiscoWorks Common Services*』の「Configuring the Server」の章を参照してください。

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、IP Communications 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、IP Communications 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 CiscoWorks サーバのシステム 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。

Cisco Secure ACS 上のロールは変更できます。

ステップ 1　**Shared Profile Components > IP Communications 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.D-4 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 CiscoWorks 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

I

M

O

P

S

T

W

い

か

き

こ

さ

し

せ

た

ち

て

と

に

は

ひ

ふ

へ

ほ

ま

ゆ

ら

り

ろ