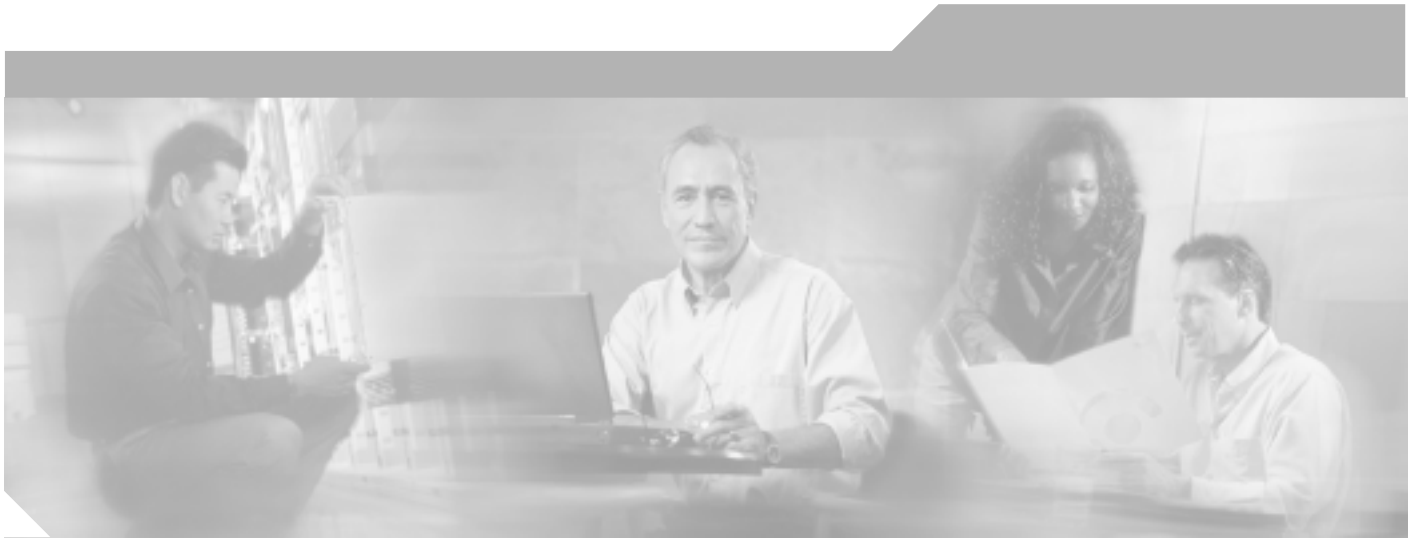

IP Communications Operations Manager（Service Monitor 付属）インストレーション ガイド

CiscoWorks

Customer Order Number: DOC-J-7817027=
Text Part Number: 78-17027-01-J

NetBSD

RSA Data Security, Inc.

AES

CONTENTS

このマニュアルについて

このマニュアルでは、IP Communications Operations Manager（Operations Manager）について説明し、Windows システムに Operations Manager をインストールする手順および Operations Manager を使用するための最初の手順を示します。

対象読者

このマニュアルは、Operations Manager をインストールし、最初に使用する方を対象としています。

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 Operations Manager 1.0	• 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 の次の URL で入手可能です。http://cisco.com/en/US/partner/products/ps6535/products_device_support_table09186a0080552d07.html
Quick Start Guide for IP Communications Operations Manager 1.0	• 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 の次の URL で入手可能です。http://cisco.com/en/US/partner/products/ps6535/products_quick_start09186a008055293a.html
Installation Guide for IP Communications Operations Manager (*Includes Service Monitor*)	• PDF が製品 CD に収録されています。 • Cisco.com の次の URL で入手可能です。http://cisco.com/en/US/partner/products/ps6535/module_installation_and_configuration_guides_book09186a008054e887.html • 印刷マニュアルを注文します（Part Number DOC-7817027=）。[1]
User Guide for IP Communications Operations Manager	• PDF が製品 CD に収録されています。 • Cisco.com の次の URL で入手可能です。http://cisco.com/en/US/partner/products/ps6535/products_user_guide_book09186a008054e88a.htm • 印刷マニュアルを注文します（Part Number DOC-7817026=）。[1]
Supported Devices Table for IP Communications Operations Manager 1.0	Cisco.com の次の URL で入手可能です。http://cisco.com/en/US/partner/products/ps6535/products_device_support_table09186a0080552d07.html
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。 • ページ内の Help ボタンをクリックします。

1. P.xiii の「技術情報の入手方法」を参照してください。

関連マニュアル

（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 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
Release Notes 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 URL で入手可能です。 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/ipcsm/relnote/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 URL 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 7817056=）。[1]
Release Notes for CiscoWorks Common Services 3.0 (Includes CiscoView 6.1) on Windows	• 印刷マニュアルが製品に同梱されています。 • Cisco.com の次の URL で入手可能です。 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/relnotes/index.htm
Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows	• PDF が製品 CD に収録されています。 • Cisco.com の次の URL で入手可能です。 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/ig_win/index.htm • 印刷マニュアルを注文します（Part Number DOC-7816497=）。[1]
User Guide for CiscoWorks Common Services	• PDF が製品 CD に収録されています。 • Cisco.com の次の URL で入手可能です。 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/usrguide/index.htm • 印刷マニュアルを注文します（Part Number DOC-7816571=）。[1]

1. P.xiii の「技術情報の入手方法」を参照してください。

オンラインで得られるその他の情報

新しい Incremental Device Update（IDU）が利用可能になった時点で、Cisco.com から IDU をダウンロードできます。

IDU は累積されます。つまり、新しい IDU には、以前の IDU の内容がすべて含まれています。次の手順に従って、CiscoWorks Server にインストールされている IDU のバージョンを特定してください。

ステップ 1 Operations Manager ホームページで、ウィンドウの右上隅にある **CiscoWorks** をクリックします。CiscoWorks ホームページが開きます。

ステップ 2 CiscoWorks ホームページで、**Software Center > Software Update** をクリックします。Software Update ページが新しいウィンドウに表示されます。

ステップ 3 Products Installed テーブルまでスクロール ダウンし、CiscoWorks IP Communications Operations Manager を見つけます。

ステップ 4 CiscoWorks IP Communications Operations Manager のバージョン番号を調べます。バージョン番号の形式は、*x.y.z* です。

- *x*：メジャー バージョン
- *y*：マイナー バージョン
- *z*：IDU 番号

公開されているパッチは、すべてダウンロード サイトから入手できます。

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

前提条件

この章では、IP Communications Operations Manager（IP Communications Service Monitor を搭載）を Windows システムにインストールするための前提条件について説明します。次のトピックを取り上げます。

製品概要

IP Communications Operations Manager（Operations Manager）は、ネットワーク内の IP コミュニケーション インフラストラクチャとその基盤となる転送インフラストラクチャの両方について、現在のステータスを監視し、評価します。Operations Manager は、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）および Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）などのオープン インターフェイスを使用し、IP コミュニケーションの展開において各種デバイスのデータをリモートでポーリングします。

（注） Operations Manager は、監視対象のデバイスにエージェント ソフトウェアを導入しないため、システムの動作を中断させることはありません。

Operations Manager によって、ネットワーク管理者は次のツールを使用してより迅速に問題を隔離できるため、生産性を高めることができます。

- **コンテキスト診断ツール**：
  - 診断テストは、統合型 IP コミュニケーション インフラストラクチャのさまざまな要素に関するパフォーマンスと接続の詳細を提供します。
  - 統合テストは、エンドユーザのアクティビティを複製し、ゲートウェイのアベイラビリティ、および IP コミュニケーション インフラストラクチャの設定や運用のその他の側面を検証します。
  - IP Service-Level Agreement（SLA; サービスレベル契約）に基づく診断テストは、WAN リンクおよびノード間のネットワーク品質のパフォーマンスを測定できます。
- **通知メッセージ内のクリック可能な情報**：サービス停止に関する詳細情報への状況依存リンクが含まれます。
- **その他の CiscoWorks ツールおよびシスコ ツールへの状況依存リンク**：IP コミュニケーション実装の管理用。

IP Communications Operations Manager はさらに、次の機能も備えています。

- **サービス品質アラートの提示**：CiscoWorks IP Communications Service Monitor 1.0（併せて導入されている場合）からの情報を使用して、次のことを実行します。
  - コールに関わるエンドポイント（Cisco IP Phone、Cisco Unity メッセージング システム、または音声ゲートウェイ）のペア間の劣悪な音声品質に関連付けられた Mean Opinion Score（MOS; 平均オピニオン スコア）、および音声品質の問題に関連するその他の詳細情報を表示する
  - 2 つのエンドポイント間でパス トレースを実行し、パス内の中間ノードの停止または問題を報告可能にする
- **ネットワーク内の Cisco IP Phone に影響する現在の接続関連および登録関連の停止を強調表示**：さらに、関与する IP 電話を特定し識別できるように状況に応じた情報を提供します。
- **IP コミュニケーション デバイスと IP 電話のインベントリを追跡**：Cisco IP Phone のステータスの変化を追跡し、ネットワーク内の Cisco IP Phone に対する移動、追加、変更の各操作を文書化した各種レポートを作成します。
- **リアルタイム通知を提供**：SNMP トラップ、syslog 通知、および電子メールを使用して、監視対象のネットワークのステータスを上位レベルのエンティティ（通常は管理者の管理者）にレポートします。

サーバの要件

表1-1 は、Operations Manager をインストールするためのサーバの最小システム要件を示しています。

表 1-1　サーバのシステム要件

要件のタイプ	最小要件
システム ハードウェア	• 次のいずれかを備える IBM PC 互換コンピュータ： — 小規模な構成（電話機 1,000 台未満）：2.0 GHz Intel プロセッサ、2 GB RAM、60 GB ハード ディスク ドライブ — 中規模な構成（電話機 1,000 ～ 10,000 台）：3.0 GHz Intel プロセッサ、4 GB RAM、60 GB ハード ディスク ドライブ — 大規模な構成（電話機 10,000 台以上）：デュアル 3.0 GHz Intel プロセッサ、4 GB RAM、60 GB ハード ディスク ドライブ • カラー モニタ • CD-ROM ドライブ • 1 つまたは 2 つの 10/100 NIC（1 つは必須、1 つはフェールオーバー用）のサポート
メモリ（RAM）	次のいずれか 1 つ。 2 GB：小規模構成の場合の最小メモリ 4 GB：中規模構成の場合の最小メモリ 4 GB：大規模構成の場合の最小メモリ
空きドライブ スペース[1]	• 60 GB ハード ディスク スペース • メモリ（RAM）量の 2 倍に相当する仮想メモリ。たとえば、システムに 2 GB の RAM がある場合は、4 GB の仮想メモリが必要です。 • NTFS ファイル システム（セキュア オペレーション用に必須） • Windows の一時ディレクトリ（%TEMP%）に、16 MB 以上
システム ソフトウェア[2,3]	• ODBC Driver Manager[4] 3.5.10 以降 • Windows Server 2003 Service Pack 1、Standard Edition および Enterprise Edition **（注）** Windows ターミナル サービスがサポートされるのは、リモート管理モードだけです。

1. Operations Manager は、FAT ファイル システムにインストールしないでください。
2. Operations Manager は、専用システムにインストールする必要があります。Primary Domain Controller（PDC; プライマリ ドメイン コントローラ）または Backup Domain Controller（BDC; バックアップ ドメイン コントローラ）に Operations Manager をインストールしないでください。暗号化ディレクトリに Operations Manager をインストールしないでください。CiscoWorks は、暗号化ディレクトリをサポートしていません。
3. Windows オペレーティング システムのデフォルト ロケールを米国英語または日本語に設定する必要があります。
4. ODBC Driver Manager のバージョンを確認するには、Windows のデスクトップで、**Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)** を選択します。**About** タブを選択します。必要に応じて、Microsoft Data Access Component（MDAC）2.5 以降をインストールします。

クライアントの要件

表 1-2 は、CiscoWorks クライアントの最小システム要件を示しています。

表 1-2　クライアントのシステム要件

要件のタイプ	最小要件
システムのハードウェアとソフトウェア	• 次のいずれかを実行する 1 台の 1.0 GHz プロセッサを搭載した IBM PC 互換システム — Windows XP、Service Pack 2 — Windows ターミナル サービスのない Windows Server 2003 Standard Edition または Enterprise Edition • ビデオ カード付きカラー モニタ（24 色深度に設定） • 1024 × 768 dpi の画面解像度 **（注）** すべての LCD プロジェクタまたはモニタが、最低画面解像度で鮮明な画面を表示するわけではありません。LCD プロジェクタとモニタでは、ドット ピッチが画面の読みやすさに影響します。
メモリ（RAM）	512 MB メモリ（RAM）（1 GB を推奨）
追加ソフトウェア	• Internet Explorer 6.0.28 または 6.0.37 • Adobe Macromedia Flash Player 8.0 以降
環境	クライアントは、Operations Manager にアクセス可能である必要があります。 • ファイアウォールの外側からの場合：クライアント アクセスの設定方法については、ご使用のファイアウォールのマニュアルを参照してください。 • Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を経由する場合：VPN トンネルによって、クライアントおよび VPN ルータ（または同様のデバイス）が接続されている必要があります。

サポートされるデバイス

Operations Manager をインストールするときに、サポートされるすべてのデバイスのデバイス アダプタ パッケージがインストールされます。Operations Manager と一緒にインストールされるデバイスの情報は、Cisco.com で入手できます。

追加のデバイス アダプタ パッケージがリリースされた場合は、Cisco.com にログインして、デバイス アダプタ パッケージを含む IDU をダウンロードできます。

CHAPTER 2

IP Communications Operations Manager のインストールおよびアンインストール

この章では、IP Communications Operations Manager（IP Communications Service Monitor を搭載）を Windows システムにインストールする方法について説明します。次のトピックを取り上げます。

Operations Manager のインストールの準備

ここで説明する内容は、IP Communications Operations Manager（Operations Manager）をインストールする前に次の作業を実行する際に役立ちます。

- サーバのハードウェア要件とソフトウェア要件が満たされていることを確認する（P.1-3 の「サーバの要件」を参照）
- Operations Manager または IP Communications Service Monitor（Service Monitor）の使用するポートが既存のアプリケーションによってすでに使用されているかどうかを調べる（Operations Manager または Service Monitor の使用するポートが既存のアプリケーションによって使用されていない必要があります）。
- Operations Manager のインストールで必要となる可能性がある情報を収集する

Operations Manager が使用する TCP ポートと UDP ポートの確認

Operations Manager をインストールする前に、Operations Manager（および Service Monitor）の使用するポートが、表 2-1 と表 2-2 に表示されているアプリケーション以外で使用されていないことを確認します。

（注） 既存の NMS がポート 162 を使用している場合の詳細については、P.3-13 の「SNMP トラップの受信および転送の設定」を参照してください。

Operations Manager は、次の TCP ポートと UDP ポートを使用します。

表 2-1　Operations Manager が使用するポート

プロトコル	ポート番号	サービス名	アプリケーション
UDP	161	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）	Common Services
	162	トラップ受信（標準ポート）	Common Services
	9000	トラップ受信 CSListener（ポート 162 が使用中の場合の Operations Manager サーバ）	Operations Manager
TCP	9002	DynamID 認証 （Operations ManagerBroker）	Operations Manager
	15000	ログ サーバ	Operations Manager
	43445	itemFh Fault History データベース	Operations Manager
	43446	itemInv Inventory Service データベース	Operations Manager
	43447	itemEpm Event Promulgation Module データベース	Operations Manager
	43500-43520	CSTM	Operations Manager

表 2-2　Service Monitor が使用するポート

プロトコル	ポート番号	サービス名
UDP	53	DNS
UDP	67 および 68	DHCP
UDP	69	TFTP：Service Monitor は TFTP を使用して、所定の Cisco 1040 のコンフィギュレーション ファイルを検索します。
UDP	514	Syslog：Service Monitor は Cisco 1040 から送信された syslog メッセージを受信します。
TCP	2000	SCCP：Service Monitor は SCCP を使用して Cisco 1040 と通信します。
TCP	43459	データベース

インストールに必要な情報の収集

Operations Manager のインストール中に次の情報を入力する必要が生じることがあります。

- user admin パスワード
- システム アイデンティティ アカウント パスワード
- casuser パスワード（カスタム インストールのみ）
- guest パスワード（カスタム インストールのみ）
- Common Services データベース パスワード（カスタム インストールのみ）
- Web サーバ情報（カスタム インストールのみ）

パスワードの作成方法の詳細については、『*Installation and Setup Guide for Common Services* (*Includes CiscoView*) *on Windows*』の付録「Password Information」を参照してください。

- ライセンス情報：インストール スクリプトで次のいずれかを入力するように要求されます。
  - ソフトウェアの権利証明書に印刷されている情報：Product Identification Number（PIN）および Product Authorization Key（PAK）
  - ライセンス ファイルの場所：ライセンス ファイルをすでに取得している場合は、パスを入力します。ライセンス ファイルを取得していない場合は、取得してください。ライセンス ファイルは、IP Communications Operations Manager のインストールの前か後かに関係なく取得できます。P.A-2 の「ライセンスの登録」を参照してください。

（注）　CiscoWorks ホームページで **Common Services > Server > Admin > Licensing** を選択して、ライセンスのステータスを判断できます。

（注）　評価目的で Operations Manager をインストールする場合は、次のとおりです。

- ライセンス ファイル、または PIN および PAK を入力する必要はありません。
- 必要に応じて、次の情報を参照してください。
  - 評価ライセンスのアップグレード（P.A-2）
  - ライセンス リマインダ（P.A-3）

新規インストールの実行

Operations Manager をインストールする場合、次の注意事項に従ってください。

- Operations Manager には専用のシステムが必要です。次のものがインストールされているシステムにはインストールしないでください。
  - サードパーティ製の管理ソフトウェア（HP OpenView または NetView など）
  - Cisco Secure Access Control Server（ACS）
  - Operations Manager 1.0 との共存が可能であることが明示されていない CiscoWorks アプリケーション
- Operations Manager がインストールされるシステムは、DNS 用に設定する必要があります。
- サードパーティ製 SNMP 管理ツールを使用して Operations Manager を監視する場合は、P.2-10 の「システムを SNMP クエリー対応に設定」を参照してください。
- Service Monitor は次のシステムにはインストールしないでください。
  - Primary Domain Controller（PDC; プライマリ ドメイン コントローラ）または Backup Domain Controller（BDC; バックアップ ドメイン コントローラ）
  - FAT ファイル システム
  - ターミナル サービスがアプリケーション サーバ モードでイネーブルになっている Windows Advanced Server
  - Internet Information Services（IIS）がイネーブルになっているシステム
  - 名前の検索機能のないシステム
- 暗号化ディレクトリを選択しないでください。Operations Manager は、ディレクトリの暗号化をサポートしていません。
- CiscoWorks Common Services 3.0 サービス パックは、Operations Manager にインストールしないでください。
- システムの日付と時刻が正確に設定されていることを確認します。
- インストール時間を短縮するため、インストール中にはすべてのウイルス スキャン ソフトウェアをディセーブルにします。

ステップ 1　システムが、次の前提条件を満たしていることを確認します。

- 必要な（または望ましい）オペレーティング システムのアップグレードが実行されている
- 必要なサービス パックがインストールされている

システム要件については、P.1-3 の「サーバの要件」を参照してください。

ステップ 2　開いているプログラムまたはアクティブなプログラムをすべて閉じてください。インストール プロセス中に他のプログラムを実行しないでください。

ステップ 3　Operations Manager ソフトウェアをインストールするマシンにローカル管理者としてログインし、CD-ROM ドライブに IP Communications Operations Manager の CD-ROM を挿入します。IPC Operations Manager 1.0 and Service Monitor 1.0 Setup Program ウィンドウが開きます。

（注）　CD-ROM がすでに CD-ROM ドライブに入っており、プログラムを終了するためにインストール プロセスを停止した場合、または Autostart がディセーブルになっている場合は、**Setup.exe** をクリックしてプロセスを再起動します。

ステップ 4　**Install** をクリックします。Welcome ウィンドウが表示されます。

ステップ 5　**Next** をクリックします。Software License Agreement ウィンドウが表示されます。

ステップ 6　**Accept** をクリックします。Licensing Information ウィンドウが表示されます。

ステップ 7　オプション ボタンを選択し、ライセンスに関する必要な情報を入力して、**Next** をクリックします。

（注）　ライセンス ファイルを取得する方法または PIN および PAK を検索する方法については、P.2-2 の「Operations Manager のインストールの準備」を参照してください。

Setup Type ウィンドウが表示されます。

ステップ 8　Operations Manager 1.0、Common Services 3.0 と Service Pack 1、および Service Monitor 1.0 を含む完全な IP Communications Operations Manager パッケージをインストールするには、**Typical** を選択します。

Typical インストール モードを選択した場合、次の情報が提供されます。

- guest パスワード
- Common Services データベース パスワード
- Web サーバ情報
- 自己署名証明書の情報
- データ転送プロトコル認証用のユーザ名およびパスワード
- Service Monitor コール メトリック データが格納される場所
- Service Monitor プローブ イメージとコンフィギュレーション ファイルが格納される場所

Custom インストール モードを選択した場合、インストール プロセス中にこの情報を入力するように要求されます。

ステップ 9　**Next** をクリックします。Choose Destination Folder ウィンドウが表示されます。

ステップ 10　次のいずれかを実行します。

- **Next** をクリックして、デフォルトのインストール ディレクトリを受け入れます。
- Operations Manager をインストールするフォルダを参照して指定し、**Next** をクリックします。

インストール プログラムにより、依存関係とシステム要件がチェックされます。

System Requirements ウィンドウには、要件チェックの結果と、インストールを続行できるかどうかが表示されます。次のいずれかが表示される場合があります。

- インストールするために十分なディスク　スペースがない場合、インストール　プログラムはエラー メッセージを表示し、インストールを停止します。
- 最小推奨要件が満たされていない場合、インストール プログラムはエラー メッセージを表示して、インストールを続行します。

ステップ 11　**Next** をクリックします。

ステップ 12　user admin パスワードを入力し（さらに、確認のため再入力して）、**Next** をクリックします。

（注）　*Custom* インストール モードを選択した場合、インストールのこの部分で、ステップ 8 に示されている情報を入力するように要求されます。

ステップ 13 システム アイデンティティ アカウント パスワードを入力し（さらに、確認のため再入力して）、**Next** をクリックします。

ステップ 14 Create Casuser ダイアログボックスが表示されます。**Yes** をクリックして、インストールを続行します。

Summary ウィンドウが開き、現在の設定が表示されます。

ステップ 15 **Next** をクリックします。インストールが続行されます。

ステップ 16 **OK** をクリックして、追加のメッセージが表示されている場合はそれらを確認します。

- Windows SNMP サービスがシステムにインストールされていない場合は、それを通知するメッセージが表示されます。
- インストール中にライセンス ファイルを提供しなかった場合、ライセンス ファイルの取得についてのメッセージが表示されます。

ステップ 17 CD-ROM を取り出します。

（注） 保護のため、安全な温度と湿度が調整された場所に CD-ROM を保管します。

ステップ 18 **Finish** をクリックして、マシンをリブートします。

ステップ 19 Operations Manager プロセスが実行されていることを確認するには、CiscoWorks ホームページに管理者としてログインし、**Common Services > Server > Admin > Processes** を選択します。

ステップ 20 Operations Manager を使用するには、Windows デスクトップで **Start > All Programs > IPC Operations Manager 1.0 and Service Monitor 1.0 > IPC Operations Manager 1.0 and Service Monitor 1.0** を選択します。

（注） Windows 2003 システムで拡張セキュリティがイネーブルになっている場合、Operations Manager のホームページを Internet Explorer の信頼済みサイト ゾーンに追加する必要があります。IP Communications Operations Manager ホームページを信頼済みサイトに追加しない限り、ここにアクセスすることはできません。P.3-11 の「Internet Explorer 信頼済みサイト ゾーンへの Operations Manager ホームページの追加」を参照してください。

インストール中にエラーが発生した場合、ドライブのルート ディレクトリにあるインストール ログを調べます（たとえば、CiscoWorks Common Services のインストールでは C:\Ciscoworks_setup001.log が作成され、Operations Manager のインストールで C:\Ciscoworks_setup002.log が作成されます）。Cisco Technical Assistance Center（TAC）では、インストール ログを送信するようにお願いする場合があります。

Operations Manager の再インストール

ステップ 1　開いているプログラムまたはアクティブなプログラムをすべて閉じてください。再インストール プロセス中は、他のプログラムを実行しないでください。

ステップ 2　IP Communications Operations Manager ソフトウェアをインストールするマシンにローカル管理者としてログインし、CD-ROM ドライブに IP Communications Operations Manager の CD-ROM を挿入します。インストーラのウィンドウが開き、IP Communications Operations Manager を再インストールするかどうかを確認するメッセージが表示されます。

（注）　CD-ROM がすでに CD-ROM ドライブに入っており、プログラムを終了するために再インストール プロセスを停止した場合、または Autostart がディセーブルになっている場合は、CD-ROM のトップ ディレクトリで **Setup.exe** をクリックしてプロセスを再起動します。

ステップ 3　**Install** をクリックします。Welcome ウィンドウが表示されます。

ステップ 4　**Next** をクリックします。Software License Agreement ウィンドウが表示されます。

ステップ 5　**Accept** をクリックします。Setup Type ウィンドウが表示されます。

ステップ 6　**Typical** または **Custom** を選択します。

ステップ 7　**Next** をクリックします。Backup Data ウィンドウが表示されます。

ステップ 8　Operations Manager の以前のバージョンをバックアップする場所を入力するか、または参照して指定し、**Next** をクリックします。

ステップ 9　System Requirements ウィンドウは、要件チェックの結果を表示して、再インストールを続行できるかどうかを通知します。**Next** をクリックします。

ステップ 10　Custom インストールを選択した場合、次の情報を入力するように求められます。

- casuser パスワード
- データ転送プロトコル認証用のユーザ名およびパスワード
- Service Monitor のコール メトリック データが格納される場所
- Service Monitor のプローブ イメージとコンフィギュレーション ファイルが格納される場所

Typical インストールでは、この手順は不要です。**Next** をクリックします。

ステップ 11　再インストールを確認する情報ダイアログボックスが表示されます。**OK** をクリックします。

Summary ウィンドウが開き、現在の設定が表示されます。

ステップ 12　**Next** をクリックします。インストールが続行されます。

ステップ 13　ドライブから IP Communications Operations Manager の CD-ROM を取り出します。

（注） 保護のため、安全な温度と湿度が調整された場所に CD-ROM を保管します。

ステップ 14 **Finish** をクリックして、マシンをリブートします。

ステップ 15 Operations Manager Server プロセスが実行されていることを確認するには、CiscoWorks ホームページに管理者としてログインし、**Common Services > Server > Admin > Processes** を選択します。

ステップ 16 Operations Manager を使用するには、Windows デスクトップで **Start > Programs > IPC Operations Manager 1.0 and Service Monitor 1.0 > IPC Operations Manager 1.0 and Service Monitor 1.0** を選択します。

再インストール中にエラーが発生した場合、ドライブのルート ディレクトリにあるインストール ログを調べます（たとえば、CiscoWorks Common Services のインストールでは C:\Ciscoworks_setup001.log が作成され、Operations Manager のインストールで C:\Ciscoworks_setup002.log が作成されます）。Cisco Technical Assistance Center（TAC）では、インストール ログを送信するようにお願いする場合があります。

Operations Manager のアンインストール

注意　CiscoWorks のアンインストール プログラムを使用して、システムから Operations Manager を削除する必要があります。手作業でファイルおよびプログラムを削除しようとすると、システムに深刻な損傷を及ぼすことがあります。

（注）　アンインストールする前に、必ず電話器のステータス、ノード間、および SRST のすべてのテストをアプリケーションから削除してください。これらのテストは、削除しないと、ルータ上でそのまま稼働し続けます。テストを削除するには、それぞれのテストのコンフィギュレーション ページを使用します（各テストの削除方法については、IP Communications Operations Manager のオンライン ヘルプを参照してください）。

ステップ 1　ローカル管理者として、IP Communications Operations Manager がインストールされているシステムにログインします。

ステップ 2　アンインストール プロセスを開始するには、Windows デスクトップで **Start > All Programs > IPC Operations Manager 1.0 and Service Monitor 1.0 > Uninstall IPC Operations Manager 1.0 and Service Monitor 1.0** を選択します。

ステップ 3　アンインストールするコンポーネントを選択します。

ステップ 4　**Next** をクリックして、選択したコンポーネントのアンインストールを開始します。

アンインストールの対象として選択したコンポーネントを示すウィンドウが表示されます。

ステップ 5　**Next** をクリックします。

アンインストールの進捗を示すメッセージが表示されます。

次のメッセージが表示されます。

```
Uninstallation is complete. Click OK to finish.
```

ステップ 6　**OK** をクリックします。

システムを SNMP クエリー対応に設定

Operations Manager は、システム アプリケーション MIB を実装しています。サードパーティ製の SNMP 管理ツールを使用して、Operations Manager がインストールされているサーバに SNMP クエリーを行う場合は、Windows SNMP サービスをインストールする必要があります。

（注） セキュリティを強化するために、SNMP set 操作はシステム アプリケーション MIB 内の Object ID（OID; オブジェクト ID）では許可されていません。Operations Manager のインストール後、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 Windows 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。

Windows SNMP サービスは、Operations Manager のインストールの前または後にインストールできます。次の手順で、Windows SNMP サービスがインストールされているかどうかを判断します。

ステップ 1　Operations Manager をインストールするサーバに Windows SNMP サービスがインストールされていることを確認します。次の手順に従います。

a. Windows 管理ツールの Services ウィンドウを開きます。

b. 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。
- SNMP サービスのステータスが Started であるかどうか。Started である場合、SNMP サービスは実行されています。

ステップ 2　Windows SNMP サービスがインストールされていない場合は、インストールします。

（注） 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。

CHAPTER 3

使用する前に

この項では、IP Communications Operations Manager（Operations Manager）をセットアップし、診断結果を表示するための手順を簡単に説明します。次のトピックを取り上げます。

デバイスを監視するための Operations Manager の設定

Operations Manager は、CiscoWorks Common Services の Device and Credentials Repository（DCR）から監視するデバイスを取得します。DCR は、個々のアプリケーションが使用するデバイスおよびそれらのクレデンシャルの共通リポジトリです。

Operations Manager がネットワークの監視を開始する前に、次のことを実行する必要があります。

- DCR および Operations Manager デバイス選択を設定する必要があります。DCR を設定するには、オプションを理解し、ユーザのサイトにとって何が最も有用であるかを判断する必要があります。
- Operations Manager がインベントリ収集を完了している必要があります。

表 3-1 に、完了する必要のある手順をすべて示します。

表 3-1　デバイスの監視を開始する方法

	説明	参照箇所
ステップ 1	デバイスを DCR に追加します。 3 つのオプションがあります。 • Operations Manager を使用して、デバイスを DCR に追加する。これは、物理ディスカバリと呼ばれます。 • 他のサーバのアプリケーションとマスター リポジトリを共有する • シード ファイルを使用してバルク インポートを実行し、DCR にデバイスをインポートする	 Operations Manager から DCR へのデバイスの追加（P.3-4） 他の CiscoWorks アプリケーションとの DCR の共有（P.3-3） Common Services のオンライン ヘルプの手順を参照してください。
ステップ 2	デバイス選択を設定します。	Operations Manager のデバイス選択（自動または手動）の設定（P.3-6）
ステップ 3	インベントリ収集を完了し、デバイスの監視を開始できるようにします。	
ステップ 4	Service Level View を使用して、デバイスのインポートを確認します。	Operations Manager に追加されたデバイスの確認（P.3-7）

デバイス インポート用にサポートされる NMS 環境

DCR を使用すると、次のように他のアプリケーションとデバイス リストを共有できます。

- 次の場所から DCR にデバイスをインポートできます。
  - Network Management System（NMS; ネットワーク管理システム）：DCR は、リモート NetView および HP OpenView インストールからのインポートをサポートしています（サポートされるバージョンは、ユーザ インターフェイスに表示されます）。
  - ファイル：ファイルは、別の製品からエクスポートしたものをフォーマットして DCR にインポートできます。ファイル形式は、『*User Guide for CiscoWorks Common Services*』に説明されています。

（注） Operations Manager の物理デバイス ディスカバリも、検出したデバイスを DCR に追加します。

- すべてのデバイスのマスター リストを管理し、リストをクライアント（スレーブとして設定され、同じ管理ドメイン内にある DCR のその他のインスタンス）と共有するように DCR サーバを設定できます。

他の CiscoWorks アプリケーションとの DCR の共有

DCR を使用すると、CiscoWorks ネットワーク管理アプリケーションは、クライアント / サーバ メカニズムを通じてデバイス リストおよびクレデンシャルを共有できます。Operations Manager サーバでは、デフォルトで、DCR がスタンドアロンまたは独立リポジトリとして設定されています。

オプションで、次のものを含む管理ドメインに加わるように DCR を設定できます。

- 1 つの共有マスター リポジトリ
- マスター リポジトリの正確な複製であり、マスター リポジトリと常に同期している 1 つ以上のクライアント リポジトリ

次のシナリオは、DCR 管理ドメイン内での Operations Manager の使用方法を示しています。

シナリオ：DCR 管理ドメイン内の Operations Manager

このシナリオでは、DCR を使用してデバイス リストとデバイス クレデンシャルを共有するように、Operations Manager および別の CiscoWorks アプリケーションを設定する方法の 1 つを示します。

Operations Manager（専用システムにインストールされている必要がある）と CiscoWorks Resource Manager Essentials（RME）は、個別のシステムにインストールされています。RME システムでは、DCR がサーバ（マスター）として設定されています。Operations Manager システムでは、DCR が RME システムの DCR サーバに対するクライアント（スレーブ）として設定されています。さらに、DCR から Operations Manager システムにデバイスの手動選択が設定されています。

RME システムの DCR にデバイスをインポートする場合、Operations Manager システムの DCR クライアントにもデバイスが追加されます。Operations Manager にデバイスの手動選択が設定されているので、手動で選択しない限り、Operations Manager インベントリにデバイスは追加されません。

DCR のモード（マスターおよびスレーブ）の設定

デフォルトでは、Operations Manager サーバの DCR はスタンドアロンまたは独立リポジトリとして設定されています。Operations Manager の DCR をマスターおよびスレーブのどちらに設定するかを判断する場合の手順は、オンライン ヘルプおよび『*User Guide for CiscoWorks Common Services*』に示されています。前提条件となる作業を実行し、適切な順序でマスターおよびスレーブに設定する必要があります。次の手順は、作業を開始し、オンライン ヘルプで必要な情報を特定するのに役立ちます。

（注） Operations Manager を起動するには、P.3-11 の「Operations Manager の起動」を参照してください。

ステップ 1　Operations Manager ホームページで、ページの右上隅にある **CiscoWorks** リンクをクリックします。CiscoWorks ホームページが別のウィンドウに表示されます。

ステップ 2　CiscoWorks ホームページで、**Common Services > Device and Credentials > Admin** を選択します。Admin ページが表示されます。

ステップ 3　左側のペインにある TOC から Mode Settings を選択します。Mode Settings ウィンドウが表示されます。

ステップ 4　このページの右上隅にある Help リンクをクリックします。マスターとスレーブの設定の前提条件を実行する手順を検索します。次の作業が含まれます。

- マスター DCR によるシステムへのピア サーバ ユーザの追加
- スレーブ DCR によるシステム上でのシステム アイデンティティ ユーザの作成
- セキュリティ証明書のコピー

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

Operations Manager から DCR へのデバイスの追加

Operations Manager は、物理ディスカバリを通じて、デバイスを DCR に追加します。

（注）　バルク インポート（NMS またはファイルからのインポート）を使用してデバイスを DCR に追加するには、Common Services のオンライン ヘルプの手順に従ってください。

Operations Manager の物理ディスカバリの実行

ステップ 1　**Devices > Device Management** を選択します。Device Management: Summary ページが表示されます。

ステップ 2　Last Discovery フィールドおよび Next Discovery フィールドの横にある **Configure** ボタンをクリックします。Discovery 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。

フィールド	処理 / 説明
Seed Devices	カンマ区切りの IP アドレスのリストを入力するか、Use all devices currently in Device and Credentials Repository チェックボックスをオンにします。
Ping Sweep	（オプション）これは、シード デバイスに基づいたディスカバリを使用する場合の代替です。 Use Ping Sweep チェックボックスをオンにし、*/netmask* 仕様を使用してカンマ区切りの IP アドレス範囲のリストを指定します。 たとえば、172.20.57.1/24 を使用して、172.20.57.1 ～ 172.20.57.255 の ping スイープ範囲を指定します。

フィールド	処理 / 説明
IP Address	(オプション)次の対象とするデバイスのカンマ区切りの IP アドレスまたは IP アドレス範囲を入力します。 • Include：自動ディスカバリ プロセスの対象にする • Exclude：自動ディスカバリ プロセスの対象から除外する IP アドレス範囲を指定するときにワイルドカードを使用できます。 アスタリスク（*）は、1 ～ 255 のオクテット範囲を示します。また、[xxx-yyy] 表記を使用してオクテット範囲を制限することもできます。 次の例を参考にしてください。 • 172.20.57/24 サブネットのすべてのデバイスを自動ディスカバリ プロセスの対象にするには、172.20.57.* の Include フィルタを入力します。 • 172.20.57.224 ～ 172.20.57.255 の IP アドレス範囲のデバイスを自動ディスカバリ プロセスの対象外にするには、172.20.57.[224-255] の Exclude フィルタを入力します。 両方のタイプのワイルドカードを、たとえば 172.20.[55-57].* のように同じ範囲指定で使用できます。Include フィルタおよび Exclude フィルタの両方が指定されている場合、Exclude フィルタが最初に適用され、次に Include フィルタが適用されます。一旦フィルタが自動ディスカバリ デバイスに適用されると、他のフィルタ条件はそのデバイスには適用されません。デバイスに複数の IP アドレスがあり、その中の 1 つでも Include フィルタの条件を満たしている場合、そのデバイスは自動ディスカバリ プロセスの対象として処理されます。
DNS Domain	(オプション) 次の対象とするデバイスのカンマ区切りの DNS ドメイン名を入力します。 • Include：自動ディスカバリ プロセスの対象にする • Exclude：自動ディスカバリ プロセスの対象から除外する ワイルドカードを使用して DNS 名を指定できます。アスタリスク（*）は、大文字と小文字の英数字、ハイフン（-）、および下線（_）が混在する任意の長さの組み合わせに一致します。疑問符（?）は、大文字または小文字の英数字、ハイフン、または下線の 1 文字に一致します。次の例を参考にしてください。 • *.*cisco.com* は、*.cisco.com* で終わるすべての DNS 名に一致します。 • *.*?abc.com* は、*.aabc.com* や *.babc.com* などで終わるすべての DNS 名に一致します。
SysLocation	(オプション) 次の対象とするデバイスについて、MIB-II 内の sysLocation OID に格納されているストリング値に一致するカンマ区切りのストリングを入力します。 • Include：自動ディスカバリ プロセスの対象にする • Exclude：自動ディスカバリ プロセスの対象から除外する ワイルドカードを使用してロケーション ストリングを指定できます。アスタリスク（*）は、大文字と小文字の英数字、ハイフン（-）、下線（_）、および空白（スペースとタブ）が混在する任意の長さの組み合わせに一致します。疑問符（?）のワイルドカードは、上記の任意の文字の 1 文字に一致します。たとえば、*San * の SysLocation フィルタは、*San Francisco* および *San Jose* などで始まるすべての SysLocation ストリングに一致します。

フィールド	処理 / 説明
Run	オプション ボタンを選択して、スケジュールを入力します。 • Now：すぐに実行する場合に選択します。 • Daily：実行する時刻を入力して、実行する曜日（Sun、Tue、Sat など）を選択します。 • Weekly：週単位での実行頻度（N 週ごと）、時刻、および曜日を入力します。

ステップ 4　**OK** をクリックします。物理ディスカバリの実行が開始されます。完了するまでにしばらく時間がかかります（Device Management: Summary ページのディスカバリ ステータスをチェックしてください）。

Operations Manager のデバイス選択（自動または手動）の設定

DCR から Operations Manager インベントリにデバイスを追加するには、次のいずれかで Operations Manager デバイス選択を設定する必要があります。

- Automatic：サポートされるデバイスが DCR に追加されると、自動的にインベントリにも追加されます（自動選択では、Operations Manager から除外するデバイスのリストも維持されます）。
- Manual：選択したデバイスだけを追加します。

（注）　初めて同期プロセスを実行する場合、Operations Manager に追加されるデバイス数によっては、Operations Manager がすべてのデバイスのインベントリを収集するまでに数時間かかる場合があります。

（注）　事前にデバイスが DCR に存在していないと、デバイスを Operations Manager に追加することはできません。

ステップ 1　**Devices > Device Management** を選択します。Device Management: Summary ページが表示されます。

ステップ 2　Device Selection フィールドの横にある **Configure** ボタンをクリックします。Device Selection ページが表示されます。

ステップ 3　Automatic オプション ボタンをアクティブにします。

ステップ 4　**Apply** をクリックします。Operations Manager が DCR と同期されます。Operations Manager に現在含まれていない DCR デバイスが追加されます。Operations Manager は、追加される新しいデバイスのインベントリ収集を実行します。

DCR から Operations Manager への手動によるデバイスの追加

Operations Manager を自動デバイス選択に設定した場合は、この手順を実行する必要はありません。手動デバイス選択では、監視するデバイスを手動で選択する必要があります。デバイスが DCR に追加された後に、定期的にこの作業を実行する必要があります。たとえば、週単位で Operations Manager の物理ディスカバリを実行する場合は、ディスカバリが終了するたびに監視する新しいデバイスを確認するかどうかを検討する必要があります。

（注） 事前にデバイスが DCR に存在していないと、デバイスを Operations Manager に追加することはできません。

ステップ 1　**Devices > Device Management** を選択します。

ステップ 2　Device Selection フィールドの横にある **Configure** ボタンをクリックします。Device Selection ページが表示されます。

ステップ 3　Manual オプション ボタンを選択します。Operations Manager インベントリに存在しないすべてのデバイスをデバイス セレクタから選択できます。

ステップ 4　次のいずれかの方法でデバイスを選択します。

- Device Display Name にデバイス名または IP アドレスを入力して、**Filter** をクリックする
- グループ セレクタを使用する

ステップ 5　選択したデバイスを表示するには、Selection タブをクリックします。デバイスのリストが表示されます。

ステップ 6　**Select** をクリックします。Operations Manager は、追加対象のデバイスのインベントリ収集を実行します。

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

Operations Manager に追加されたデバイスの確認

デバイスが Operations Manager インベントリに追加されていることを確認する方法の 1 つは、Service Level View を参照することです。また、Service Level View では、多数の Operations Manager ツールへクイック アクセスすることもできます。

インベントリ収集中に問題が発生した場合は、P.3-9 の「デバイス ディスカバリのトラブルシューティング」を参照してください。

Service Level View の起動

ステップ 1　**Monitoring Dashboard** > **Service Level View** を選択します。IP テレフォニー実装の論理トポロジビューを示す Service Level View 画面が表示されます。

詳細については、『*User Guide for IP Communications Operations Manager*』または Operations Manager のオンライン ヘルプを参照してください。

インベントリ収集のスケジュール

デバイスおよび電話器には、それぞれ個別のインベントリ収集スケジュールがあります。デバイスのインベントリ収集スケジュールは 1 つだけです。追加のスケジュールは作成できず、既存のスケジュールを編集することしかできません。IP Phone の場合は、複数のインベントリ収集スケジュールを作成できます。

Inventory Collection Schedule ページ（**Devices** > **Device Management** > **Device**）では、デバイス インベントリ収集スケジュールを編集、一時停止、または再開することができます（P.3-8 の「デバイス インベントリ収集スケジュールの編集」を参照してください）。

IP Phone Discovery Schedule ページ（Devices > Device Management > IP Phone Details）では、IP Phone ディスカバリ スケジュールを追加、編集、または削除することができます（P.3-8 の「電話器のディスカバリ スケジュールの追加」を参照してください）。

デバイス インベントリ収集スケジュールの編集

ステップ 1　**Devices** > **Device Management** > **Device** を選択します。Device Inventory Collection ページが表示されます。

ステップ 2　**Edit** をクリックします。Inventory Collection Schedule: Edit ページが表示されます。

ステップ 3　必要なスケジュール情報を変更します。

ステップ 4　**OK** をクリックします。

ステップ 5　**Yes** をクリックします。

電話器のディスカバリ スケジュールの追加

ステップ 1　**Devices** > **Device Management** > **IP Phone Details** を選択します。IP Phone Discovery Schedule ページが表示されます。

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

ステップ 3　次の情報を入力します。

- ディスカバリ スケジュールの名前
- ディスカバリを実行する曜日
- ディスカバリを実行する時間帯

ステップ 4　**OK** をクリックします。

デバイス ディスカバリのトラブルシューティング

物理ディスカバリの実行中（Operations Manager がデバイスを DCR に追加する間）に問題が発生したり、インベントリ収集の実行中（Operations Manager が監視用にデバイスをインベントリに追加する間）に問題が発生したりすることがあります。

デバイスのインベントリ収集をトラブルシューティングするには、次のことを試してみます。

- デバイスが応答していない場合は、すべてのデバイス クレデンシャルを確認し、デバイスを再度追加します。P.3-9 の「デバイス クレデンシャルの変更」を参照してください。
- デバイスのインベントリ収集が複数のデバイスでタイムアウトする場合は、SNMP タイムアウトの設定値を大きい値にします。P.3-9 の「SNMP タイムアウトと再試行の変更」を参照してください。
- View/Refresh/Delete Device ページのデバイス エラー情報を表示します。P.3-10 の「デバイスのインベントリ収集の実行」を参照してください。
- デバイスがインポート中に動作可能な状態で、MIB II をサポートしていることを確認します。
- 到達不能状態になっているデバイスの原因をチェックします。P.3-10 の「インベントリ収集メッセージについて」を参照してください。
- 問題をトラブルシューティングしたら、デバイスのステータスを確認します。P.3-7 の「Operations Manager に追加されたデバイスの確認」を参照してください。

デバイス クレデンシャルの変更

Common Services の DCR を使用して、デバイス クレデンシャルを変更します。Common Services のオンライン ヘルプを参照してください。

SNMP タイムアウトと再試行の変更

SNMP クエリーが時間内に応答しない場合、Operations Manager がタイムアウトします。Operations Manager は、ユーザが指定した回数だけデバイスへのアクセスを再試行します。タイムアウト期間は、後続の再試行ごとに 2 倍になります。

たとえば、タイムアウト値が 4 秒で、再試行値が 3 回の場合、Operations Manager は、4 秒間待ってから 1 回目の再試行を実行し、次に 8 秒間待ってから 2 回目の再試行を実行し、さらに 16 秒間待ってから 3 回目の再試行を実行します。

SNMP のタイムアウトと再試行値は、グローバル設定です。次のように値を変更します。

ステップ 1　**Devices > Device Management > SNMP Configuration** を選択します。SNMP Configuration ページが表示されます。

ステップ 2　新しい SNMP タイムアウトの設定値を選択します。デフォルトは 4 秒です。

ステップ 3　新しい Number of Retries の設定値を選択します。デフォルトの試行回数は 3 回です。

ステップ 4　**Apply** をクリックします。確認のために **Yes** をクリックします。

デバイスのインベントリ収集の実行

View/Refresh/Delete Devices ページから、デバイスまたはデバイス グループのインベントリ収集を起動できます。インベントリ収集の実行時に、デバイスまたはグループの設定が変更されていた場合は、新しい設定値によって以前の設定値が上書きされます。

インベントリ収集は、アクティブなデバイスに対してのみ実行されます。Operations Manager は、一時停止中のデバイスのインベントリは収集しません。インベントリ収集の対象として選択しているデバイスの中に一時停止中のデバイスがある場合、Operations Manager は、アクティブなデバイスだけをディスカバリの対象とすることを通知するメッセージを表示します。

（注）　Operations Manager インベントリ収集プロセスと DCR 同期プロセスとを混合しないでください。Operations Manager インベントリ収集は、Operations Manager インベントリだけに影響するプロセスです。

ステップ 1　**Devices > Device Management > View/Refresh/Delete** を選択します。View/Refresh/Delete Devices ページが表示されます。

ステップ 2　インベントリ収集を実行するデバイスまたはグループを選択します。

ステップ 3　**Update** をクリックします。インベントリ収集が起動します。

インベントリ収集メッセージについて

表 3-2 に、到達不能状態のデバイスについて表示されることのあるメッセージを示します。

表 3-2　インベントリ収集エラー メッセージ

メッセージ	意味	処理
SNMP Timeout	デバイスの SNMP 読み取り専用コミュニティ ストリングが不正なため、デバイスは到達不能状態です。	デバイスの正しいリード（read）コミュニティ ストリングを入力するには、P.3-9 の「デバイス クレデンシャルの変更」を参照してください。
Others: Missing IP Address or Data Collector Timeout	その他の理由で、デバイスは到達不能状態です。デバイスの DNS 解決が失敗したか、データ コレクタがタイムアウトした可能性があります。	Rediscover/Delete Devices ページでデバイスをクリックします。エラー メッセージに、問題が正確に表示されます。 • IP アドレスが検出されない場合 — 正しい IP アドレスでデバイスを再度追加します。 または — Operations Manager がデバイス名を解決可能であることを確認します。ドメイン名をデバイス名の一部として追加します。 • データ コレクタがタイムアウトした場合は、デーモン マネージャを再起動して、同時にすべてのデータ コレクタを取得します。

Operations Manager の起動

Operations Manager を起動するには、Windows デスクトップで **Start > Programs > IPC Operations Manager 1.0 and Service Monitor 1.0 > IPC Operations Manager 1.0 and Service Monitor 1.0** を選択します。

（注） Windows 2003 システムで拡張セキュリティがイネーブルになっている場合は、Operations Manager のホームページを Internet Explorer の信頼済みサイト ゾーンに追加する必要があります。IP Communications Operations Manager ホームページを信頼済みサイトに追加しない限り、ここにアクセスすることはできません。

Internet Explorer 信頼済みサイト ゾーンへの Operations Manager ホームページの追加

Windows 2003 システムで拡張セキュリティがイネーブルになっている場合は、Operations Manager ホームページにアクセスする前に、次の手順を実行する必要があります。

ステップ 1　Operations Manager を開き、**Start > Programs > IPC Operations Manager 1.0 and Service Monitor 1.0 > IPC Operations Manager 1.0 and Service Monitor 1.0** を選択します。

ステップ 2　File メニューで、**Add this site to** を選択します。

ステップ 3　**Trusted Sites Zone** をクリックします。

ステップ 4　**Trusted Sites** ダイアログボックスで、**Add** をクリックして、サイトをリストに移動します。

ステップ 5　**Close** をクリックします。

ステップ 6　ページをリフレッシュして、新しいゾーンからサイトを表示します。

ステップ 7　ブラウザのステータス バーをチェックして、サイトが信頼済みサイト ゾーンにあることを確認します。

セキュリティの概要と設定について

Operations Manager は、次のセキュリティ関連のメカニズムをサポートしています。

- SNMPv3 プロトコル（認証 / 非プライバシー オプション）：Operations Manager は、サーバとデバイス間で認証 / 非プライバシー オプションをサポートしています。
- CiscoWorks サーバ上のセキュリティ：Operations Manager が常駐するサーバに次のセキュリティを設定できます。
  - **Secure Socket Layer（SSL）**：Operations Manager は、サーバとブラウザ間で SSL プロトコルを使用できます。サーバの SSL をイネーブルおよびディセーブルにできます。SSL をイネーブルにする場合は、自己署名セキュリティ証明書を設定して、SSL 通信をイネーブルにする必要があります。詳細については、『*User Guide for IP Communications Operations Manager*』を参照してください。
  - **ローカル セキュリティまたは Cisco Secure ACS**：Operations Manager 内のタスクへのアクセスは、ローカル セキュリティによって制御されるか、Common Services または Cisco Security ACS によって提供されます。デフォルトでは、ローカル セキュリティがサーバ上でイネーブルになっています。Operations Manager は、Cisco Secure ACS との統合をサポートしています。詳細については、P.B-1 の「Cisco Secure ACS による Operations Manager の設定」を参照してください。

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

サポートされる NMS 統合

Operations Manager は、次のように NMS との統合をサポートしています。

- Operations Manager は、ポート 162（デフォルト）で管理対象デバイスからのトラップを受信します。Operations Manager を搭載したシステムの別の NMS がポート 162 を使用している場合は、次の手順に従います。
  - インストール スクリプトが、このことを警告します。
  - インストールが完了した後、Operations Manager トラップの受信用に別のポートを指定する必要があります。P.3-14 の「NMS またはトラップ デーモンへの Operations Manager トラップ受信の統合」を参照してください。
- Operations Manager は、次のように、ユーザが指定した宛先にトラップを転送します。
  - パススルー トラップを転送するには、P.3-13 の「SNMP トラップの受信および転送の設定」を参照してください。
  - 処理済みのトラップを転送するには、『*User Guide for IP Communications Operations Manager*』の「Using Notification Services」の章の「Managing SNMP Trap Notifications」を参照してください。

  パススルー トラップと処理済みのトラップの詳細については、『*User Guide for IP Communications Operations Manager*』の付録「Processed and Pass-through Traps, and Other Unidentified Traps and Events」を参照してください。

標準 User Datagram Protocol（UDP; ユーザ データグラム プロトコル）のトラップ ポート（162）が別の NMS で使用されている場合は、Operations Manager の SNMP トラップ受信で別の UDP ポート（ポート 9000 など）を使用するように設定する必要があります。P.3-13 の「SNMP トラップの受信および転送の設定」を参照してください。

SNMP トラップの受信および転送の設定

Operations Manager は、使用可能なポートでトラップを受信し、それらをデバイスとポートのリストに転送できます。この機能によって、Operations Manager はその他のトラップ処理アプリケーションと簡単に連携して動作できます。ただし、デバイスの SNMP をイネーブルにして、Operations Manager または次のいずれかに直接トラップを送信するように SNMP を設定する必要があります。

- 1 つの NMS
- 1 つのトラップ デーモン

トラップを直接 Operations Manager に送信するには、P.3-13 の「デバイスの Operations Manager へのトラップ送信のイネーブル化」の作業を実行します。SNMP トラップ受信を NMS またはトラップ デーモンに統合するには、P.3-14 の「NMS またはトラップ デーモンへの Operations Manager トラップ受信の統合」の手順に従います。

SNMP トラップの受信ポートのアップデート

デフォルトでは、Operations Manager はポート 162 で SNMP トラップを受信します。必要に応じて、ポートは変更することができます（たとえば、ポート 9000）。

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

ステップ 2　Trap Receiving Port フィールドに、ポート番号を入力します。

ステップ 3　**Apply** をクリックします。

Operations Manager が使用するポートのリストについては、P.2-2 の「Operations Manager が使用する TCP ポートと UDP ポートの確認」を参照してください。

デバイスの Operations Manager へのトラップ送信のイネーブル化

Operations Manager は SNMP MIB の変数とトラップを使用してデバイスのヘルスを判別するため、この情報を提供するようにデバイスを設定する必要があります。Operations Manager が監視するシスコ デバイスでは、SNMP をイネーブルにし、SNMP トラップを Operations Manager サーバに送信するように設定する必要があります。

デバイスに適したコマンドラインまたは GUI インターフェイスを使用して、デバイスが Operations Manager にトラップを送信可能であることを確認します。

- P.3-13 の「Cisco IOS ベースのデバイスの Operations Manager へのトラップ送信のイネーブル化」
- P.3-14 の「Catalyst デバイスの Operations Manager への SNMP トラップ送信のイネーブル化」

Cisco IOS ベースのデバイスの Operations Manager へのトラップ送信のイネーブル化

Cisco IOS ソフトウェアを実行しているデバイスの場合は、次のコマンドを入力します。

```
(config)# snmp-server [community string] ro
(config)# snmp-server enable traps
(config)# snmp-server host [a.b.c.d] traps [community string]
```

ここで、[*community string*] は SNMP 読み取り専用コミュニティ ストリング、[*a.b.c.d*] は SNMP トラップの受信ホスト（Operations Manager サーバ）です。

詳細については、該当するコマンド リファレンス ガイドを参照してください。

ステップ 1　Cisco.com にログインします。

ステップ 2　**Products & Solutions** > **Cisco IOS Software** を選択します。

ステップ 3　Cisco IOS ベースのデバイスが使用する Cisco IOS ソフトウェア リリース バージョンを選択します。

ステップ 4　**Technical Documentation** を選択して、該当するコマンド リファレンス ガイドを選択します。

Catalyst デバイスの Operations Manager への SNMP トラップ送信のイネーブル化

Catalyst ソフトウェアを実行しているデバイスの場合は、次のコマンドを入力します。

```
(enable)# set snmp community read-only [community string]
(enable)# set snmp trap enable all
(enable)# set snmp trap [a.b.c.d] [community string]
```

ここで、[*community string*] は SNMP 読み取り専用コミュニティ ストリング、[*a.b.c.d*] は SNMP トラップの受信ホスト（Operations Manager サーバ）です。

詳細については、該当するコマンド リファレンス ガイドを参照してください。

ステップ 1　Cisco.com にログインします。

ステップ 2　**Products & Solutions** > **Switches** を選択します。

ステップ 3　該当する Cisco Catalyst シリーズ スイッチを選択します。

ステップ 4　**Technical Documentation** を選択して、該当するコマンド リファレンス ガイドを選択します。

NMS またはトラップ デーモンへの Operations Manager トラップ受信の統合

SNMP トラップ受信をその他のトラップ デーモンや NMS に統合するには、次の手順に従う必要があります。

- Operations Manager が実行されているホストを、ネットワーク デバイス内のトラップ宛先リストに追加します。P.3-13 の「デバイスの Operations Manager へのトラップ送信のイネーブル化」を参照してください。ポート 162 を宛先トラップ ポートとして指定します。

  別の NMS がすでに標準 UDP トラップ ポート（162）でトラップを受信している場合は、Operations Manager がポート 9000 などの別のポートを使用するように設定する必要があります。P.3-13 の「SNMP トラップの受信ポートのアップデート」を参照してください。
- ネットワーク デバイスがすでにトラップを別の管理アプリケーションに送信している場合は、Operations Manager にトラップを転送するようにそのアプリケーションを設定します。

表 3-3 に、SNMP トラップ受信のシナリオの説明とそれぞれの利点を示します。

表 3-3　トラップ受信の設定シナリオ

シナリオ	利点
ネットワーク デバイスは、Operations Manager が実行されているホストのポート 162 にトラップを送信します。Operations Manager は、トラップを受信して、NMS に転送します。	• NMS の再設定は不要です。 • ネットワーク デバイスの再設定は不要です。 • Operations Manager は、信頼できるトラップの受信、保存、および転送メカニズムを提供します。 • NMS は継続して、ポート 162 でトラップを受信します。 • ネットワーク デバイスは継続して、トラップをポート 162 に送信します。
NMS は、デフォルトのポート 162 でトラップを受信して、Operations Manager が実行されているホストのポート 162 に転送します。	• NMS の再設定は不要です。 • ネットワーク デバイスの再設定は不要です。 • Operations Manager は、NMS によって廃棄されたトラップは受信しません。

SNMP トラップ転送の設定

デフォルトでは、Operations Manager は未処理の SNMP トラップを転送しません。ただし、転送するように設定することはできます。

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

ステップ 2　Trap Forwarding Parameters に、次の情報を入力します。

- サーバの IP アドレスまたは DNS 名
- トラップの受信が可能なサーバのポート番号

ステップ 3　**Apply** ボタンをクリックします。

アラートの表示

Monitoring Dashboard 画面を使用して、アラートを表示できます。**Monitoring Dashboard** を選択して、次のいずれかの画面を選択します。

- Service Level View
- Alerts and Events
- Service Quality Alerts
- IP Phone Status

次の作業

この章の作業を完了すると、Operations Manager はイベントの監視と分析、およびアラートの通知を実行できるようになります。

表 3-4 に、Operations Manager の追加のセットアップ方法を要約します。

表 3-4　Operations Manager のセットアップ

作業	説明
Monitoring Dashboard 画面のビューの設定	ビューは、Monitoring Dashboard 画面に表示されるデバイスの論理グループです（Service Level View、Alerts and Events、Phone Activities、および Service Quality Alerts）。Group Administration and Configuration ページに新しいユーザ定義のグループを作成すると、必ず対応するビューも作成されます。
通知の設定	Monitoring Dashboard 画面を監視してアラートを確認します。また、アラートに応じて、ユーザが電子メールを受信したり、ホストが Operations Manager によって生成された SNMP トラップを受信したりするように登録できます。
ポーリング パラメータとしきい値の設定	Operations Manager には、ポーリング パラメータとしきい値のデフォルト値があります。ただし、ネットワークの必要に応じて、値をアップデートできます。Operations Manager サーバのアクティビティが低い場合は、変更の適用を計画する必要があります。 デフォルトでは、Operations Manager は音声使用率のポーリング設定値を設定します。Operations Manager のパフォーマンス モニタリング機能を使用する場合は、最初に音声使用率のポーリングをイネーブルにする必要があります。
消去の設定	デフォルトでは、Operations Manager は毎日午前 0 時にデータベースを消去します。このスケジュールは変更できます。
インベントリ収集の設定	Operations Manager では、インベントリ収集のデフォルト スケジュールを 1 つ用意しています。そのスケジュールを使用することもできれば、一時停止することもできます。

Operations Manager の機能を十分に活用するために、追加の設定作業を実行する必要が生じる場合があります。Operations Manager の使用と設定については、オンライン ヘルプまたは『*User Guide for IP Communications Operations Manager*』を参照してください。

ライセンス

この付録では、Operations Manager のライセンスについて説明します。この付録は、次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、Operations Manager 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 スクリプトは、Common Services 3.0 に最初にアプリケーションをインストールするときに、ライセンス情報の入力を要求します。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。タイプは次のいずれかになります。 • 評価インストール：評価コピーの場合、ライセンスの詳細は必要ありません。 • 新規インストール • アップグレード インストール
Product Authorization Key（PAK）	PAK は Cisco.com で Operations Manager 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。必要に応じて、後で PAK 番号を入力できます。
- 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、Operations Manager 1.0 のインストール前でも、インストール後でも取得できます（P.A-2 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

Operations Manager 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.A-2 の「ライセンスの登録」を参照してください。

Operations Manager 1.0 の評価コピーの場合、ライセンスの詳細は必要ありません。Operations Manager 1.0 の評価コピーの場合は、Licensing Information 画面で **Evaluation only** オプション ボタンを選択します。

（注） インストール終了時に、90 日以内に Cisco.com から有効なライセンス キーを取得するように促すメッセージが表示されます。

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、ソフトウェアの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 Common Services 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）。

評価ライセンスのアップグレード

評価ライセンスを、Operations Manager 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わせください。

ステップ 2　PAK を入手したら、P.A-2 の「ライセンスの登録」の手順に従います。評価コピーが、Operations Manager 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、Operations Manager 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

Operations Manager 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.A-2 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。

評価ライセンスの有効期限が切れる前に、次のプロンプトが表示されます。

```
This software is provided for evaluation purposes only and will expire in XX days. If
this is not an evaluation copy, please click this link for information about obtaining
a valid purchase license. Click here for current licensing information. Otherwise,
please contact your Cisco representative for purchasing information.
```

このメッセージは、ログインして Operations Manager 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。評価ライセンスをアップグレードしなかった場合は、Operations Manager のすべてのプロセスは動作しますが、Operations Manager 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

購入バージョンの Operations Manager をインストールした場合は、PAK 番号を使用して Operations Manager を登録する必要があります。詳細については、P.A-2 の「ライセンスの登録」を参照してください。Operations Manager 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 Operations Manager 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。

```
The license file is invalid. Please click this link for information about obtaining a
valid purchase license. Click here for current licensing information. Otherwise,
please contact your Cisco representative for purchasing information.
```

Operations Manager 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。

制限付きバージョン：デバイス制限を超過した場合

制限付きライセンスの場合は、デバイス インベントリがデバイス制限に近づくと、Operations Manager がそのことを通知します。デバイス制限に達すると、Operations Manager は次のメッセージを表示します。

- デバイス制限を超過した場合

  ```
  You have exceeded the device limit for IP Communications Operations Manager.
  Devices will not be managed.
  ```

- 電話器の制限を超過した場合

  ```
  You have exceeded the phone limit for IP Communications Operations Manager. Please
  click here for current licensing information. Please contact your Cisco
  representative to determine if additional licenses can be purchased for this
  server.
  ```

Operations Manager 1.0 はそのまま機能しますが、すぐに管理対象インベントリへのデバイスの追加が停止します。

Cisco Secure ACS による Operations Manager の設定

この項では、Cisco Secure ACS を使用して Operations Manager を設定する方法を説明します。

CiscoWorks ログイン モジュール

Common Services は、CiscoWorks アプリケーションのユーザを認証するセキュリティ メカニズムを提供します。CiscoWorks ログイン モジュールを設定して、ユーザ認証および認可に対して次のいずれかのモードを使用できます。

- 非 ACS：このモードでは、CiscoWorks サーバが認証および認可サービスを提供します。
- ACS：このモードでは、Cisco Secure Access Control Server（ACS）が認証および認可サービスを提供します。このモードを使用するには、ネットワークに Cisco Secure ACS がインストールされている必要があります。Cisco Secure ACS for Windows のサポートされるバージョンは、3.2、3.2.3、および 3.3.2 です。

  ACS 3.2.3 を使用している場合は、Admin HTTPS PSIRT パッチをインストールすることをお勧めします。

  1. http://www.cisco.com/kobayashi/sw-center/ciscosecure/cs-acs.shtml にアクセスします。
  2. Download Cisco Secure ACS Software (Windows) リンクをクリックします。テーブルに Admin HTTPS PSIRT パッチへのリンクがあります。

  Operations Manager 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、Operations Manager を Cisco Secure ACS の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）クライアントとして設定する必要があるためです。

  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 は次の処理を行います。

  1. 非 ACS モード（CiscoWorks ローカル モード）で認証を試みます。
  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（この操作を非 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。

詳細については、『*User Guide for CiscoWorks Common Services*』および Common Services のオンライン ヘルプを参照してください。

CiscoWorks サーバの認証ロール

デフォルトでは、CiscoWorks サーバの ACS モードには 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、ネットワークにアクセスする必要のあるジョブをスケジュールリングしたりする特権はありません。

  たとえば、このユーザは Alerts および Activities の画面を使用できます。
- アプルーバ：このロールを持つユーザには、すべての Operations Manager タスクを承認する特権があります。ヘルプ デスクのすべてのタスクも実行できます。

  たとえば、このユーザは Alert History データベースを検索できます。
- 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するすべてのタスクを実行する特権があります。また、アプルーバ タスクもすべて実行できます。ネットワークへの書き込みアクセス権はありません。

  たとえば、このユーザはロギング パラメータを設定できます。

（注） Operations Manager では、このロールのユーザはデフォルトでネットワーク管理者と同じ Operations Manager タスクを実行できます。

- 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。ユーザは、ネットワーク オペレータ タスクも実行できます。

  たとえば、このユーザは DCR から Operations Manager にデバイスを追加できます。
- 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 サーバのアクセス権レポートを参照してください（Common Services > Server > Reports > Permission Report）。

  たとえば、このユーザは、SNMP トラップ転送を設定できます（Administration > Preferences）。

（注） Cisco Secure ACS を使用してこれらのロールを変更し、タスクを削除したり、特定のロールから別のロールにタスクを再割り当てしたりした場合には、アクセス権レポートには変更内容は反映されません。

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 Operations Manager** を選択します。

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

ステップ 3　ビジネス ワークローおよびニーズに適した Operations Manager 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。

始める前に：統合の注意事項

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。

- CiscoWorks サーバと Cisco Secure ACS の統合は、必ずすべてのアプリケーションをインストールした*後*に実行してください。
- CiscoWorks ログイン モジュールを ACS モードに設定した後にアプリケーションをインストールした場合、アプリケーションのユーザには、どのアクセス権も付与されません。ただし、アプリケーションは Cisco Secure ACS に登録されます。Cisco Secure ACS サーバで、アプリケーションに適切なアクセス権を割り当てる必要があります。

  P.B-5 の「Cisco Secure ACS での Operations Manager の設定」を参照してください。
- 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 Operations Manager 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、IP Communications 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 Operations Manager 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 10 台の CiscoWorks サーバを設定し、Cisco Secure ACS で Operations Manager のロールを作成します（*IPCOMSU* など）。このロールは、10 台すべての CiscoWorks サーバで動作する Operations Manager アプリケーションによって共有されます。
- ユーザは、Operations Manager 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 *CWSU* は、次の特権を持つことができます。
  - Common Services のシステム管理者
  - RME のアプルーバ
  - Campus Manager のネットワーク オペレータ
  - Operations Manager のネットワーク管理者
  - Internet Performance Monitor（IPM）のヘルプ デスク
- CiscoWorks で、次のタスク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。
  - 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。Operations Manager 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。

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 Operations Manager 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 Operations Manager アプリケーション エントリがあることを確認します。

(注) Operations Manager をインストールする*前*に CiscoWorks Common Services を Cisco Secure ACS に統合した場合は、再度 ACS モードを設定し、ACS にすべてのアプリケーションを登録する必要があります。Common Services のオンライン ヘルプを参照してください。また、Operations Manager を再インストールしても、Cisco Secure ACS の設定は失われません。Cisco Secure ACS に Operations Manager を再登録した後は、Cisco Secure ACS で使用可能な設定が Operations Manager によって継承されます。

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、ユーザ単位またはグループ単位の IP Communications Operations Manager の設定を確認します。

3. ユーザまたはグループに適切な Operations Manager 特権を割り当てます。

   Operations Manager 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。

Operations Manager と Cisco Secure ACS の設定の確認

P.B-5 の「Cisco Secure ACS での Operations Manager 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、次のようになります。

   - デバイスのサマリーは表示できます。
   - 管理する Operations Manager のデバイスは選択できません。

3. Cisco Secure ACS のユーザまたはグループのネットワーク デバイス設定に基づいて、CiscoWorks サーバで特定のデバイスだけを表示できます。

(注) デバイスに基づいたフィルタリングを実行する Operations Manager 画面のリストについては、Cisco Secure ACS で Operations Manager 固有のオンライン ヘルプを参照してください。

S

い

え

く

さ

す

せ

た

ち

つ

て

と

に

は

ひ

へ

ほ

ま

め

ゆ

ら

ろ