Cisco Unified Service Monitor 2.3 インストレーション ガイド

Installation Guide for Cisco Unified Service Monitor 2.3

ソフトウェア リリース 2.3
Cisco Unified Communications Management Suite

Text Part Number: OL-20789-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

はじめに

このマニュアルでは、Cisco Unified Service Monitor（Service Monitor）と、そのインストール方法およびアップグレード方法について説明します。

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 レベル全体をモニタする管理担当者
- 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

このマニュアルでは、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。

製品マニュアル

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

表 1 に、入手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	次の URL の Cisco.com で入手可能
Release Notes for Cisco Unified Service Monitor 2.3	http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.3/release/notes/ReleaseNotesforCiscoUnifiedServiceMonitor2_3.html
Cisco Unified Service Monitor 2.3 Compatibility Matrix	http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.3/sdt/CiscoUnifiedServiceMonitorCompatibilityMatrix23.html
Installation Guide for Cisco Unified Service Monitor 2.3	http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.3/installation/guide/InstallationGuideforCiscoUnifiedServiceMonitor23.html
User Guide for Cisco Unified Service Monitor 2.3	http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.3/installation/guide/UserGuideforCiscoUnifiedServiceMonitor2_3.html
文脈依存オンライン ヘルプ	ウィンドウの右上隅にある [Help] リンクまたはダイアログボックスの [Help] ボタンをクリックします。

関連資料

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

表 2 に、入手可能なその他のマニュアルを示します。

表 2　関連資料

マニュアル タイトル	次の URL の Cisco.com で入手可能
Quick Start Guide for Cisco 1040 Sensor	http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.1/quick/guide/1040qs21.html
Release Notes for Cisco Unified Operations Manager 2.3	http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_operations_manager/2.3/release/notes/OM_RN23.html
Installation Guide for Cisco Unified Operations Manager 2.3 (Service Monitor を含む)	http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_operations_manager/2.3/installation/guide/InstallationGuideforCiscoUnifiedOperationsManager.html
User Guide for Cisco Unified Operations Manager 2.3	http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_operations_manager/2.3/user/guide/CUOM_UserGuide23.html
Release Notes for CiscoWorks Common Services 3.2	http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/release/notes/cs32rel.html
User Guide for CiscoWorks Common Services 3.2	http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/user/guide/cs32ug.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

前提条件

製品概要

Cisco Unified Communications Management Suite の 1 製品である Cisco Unified Service Monitor（Service Monitor）をご使用の音声ネットワークにインストールして適切に設定すると、次のソースからデータを受信して分析できます。

- Cisco Unified Communications Manager（Unified Communications Manager）クラスタ：Call Detail Record（CDR; コール詳細レコード）および Call Management Record（CMR; コール管理レコード）を維持します。CDR には、Mean Opinion Score（MOS; 平均オピニオン スコア）値が含まれます。これらは、Cisco Voice Transmission Quality（CVTQ）アルゴリズムを使用して IP 電話および音声ゲートウェイで計算されたものです。

  Service Monitor をサポートする Unified Communications Manager のバージョンについては、『*Cisco Unified Service Monitor 2.3 Compatibility Matrix*』を参照してください。Service Monitor と連動するように Unified Communications Manager クラスタを設定する方法については、『*User Guide for Cisco Unified Service Monitor*』を参照してください。

- センサー：Network Analysis Module（NAM; ネットワーク解析モジュール）および Cisco 1040 センサー（Cisco 1040）- 各 RTP ストリームについて MOS を計算します。Service Monitor は、センサーから 60 秒ごとにデータを取得します。

Service Monitor は、MOS と使用中のコーデックのしきい値（デフォルト値またはユーザ設定値）とを比較します。MOS がしきい値を下回っている場合、Service Monitor は SNMP トラップを生成し、そのトラップを最大 4 人の受信者に送信します。Service Monitor は、取得したデータをデータベースに保存します。これは Service Monitor レポートに表示できます。Service Monitor は、データベースを毎日消去して、データを指定期間維持します（詳細については、オンライン ヘルプを参照してください）。

Cisco Unified Operations Manager（Operations Manager）を Service Monitor のトラップ レシーバとして設定すると、Operations Manager でさらに、Service Monitor が生成するトラップを分析、表示、および対処することができます。Operations Manager では、サービス品質イベントの生成、これらのイベントのリアルタイム ダッシュボードでの表示と追跡、およびイベント履歴の表示と保存が可能です。Operations Manager で追加のイベント設定を行い、MOS がしきい値より下がったり、一定期間（分で設定可能）で多すぎるイベント（数を設定可能）が発生した場合に、アラートを発生させることができます。さらに、Operations Manager を設定して、通知を E メール、SNMP トラップ、および Syslog メッセージとして送信できます。

サーバおよびクライアントのシステム要件

サーバ要件

（注）

- Service Monitor と、Cisco Unified Communications Manager System の他のアプリケーションとのシステム上での共存については、『*Installation Guide for Cisco Unified Operations Manager 2.3*』の共存要件を参照してください。
- Service Monitor は VMware による仮想化をサポートしています。詳細については、「VMware に関するガイドライン」（P.1-4）を参照してください。

表 1-1 に、Service Monitor のインストールだけに関する、規模別でのサーバの最小限の要件を示します。

表 1-1　サーバの最小限の要件

	1 分あたりの最大受信データ レートを考慮した最小限の要件	
コンポーネント	**1200 CDR または 5000 NAM/1040 ストリーム、もしくは 666 CDR および 1500 NAM/1040 ストリーム**	**1600 CDR**
プロセッサ[1]	デュアルコア Xeon プロセッサ x 2、2.33 GHz 以上（合計 4 コア）	クワッドコア Xeon プロセッサ x 2、2.33 GHz 以上（合計 8 コア）
使用可能なメモリ（RAM）	4 GB	
ハードウェア	• 表示色数が 256 色以上のビデオ カードとカラー モニタ • CD-ROM ドライブ：注文したものが eDelivery システムで配布できない場合に必要 • 1 GB NIC 1 ～ 2 枚：1 枚は必須で、2 枚目はフェールオーバーをサポートするために必要です。両方の NIC カードは、同じ IP アドレスを持つ必要があります。 • SAS ハード ディスク ドライブ （注）　Cisco MCS 7845-H2、MCS 7845-I2、および MCS 7845-I2-ECS3（8 コア）がこれらの仕様を満たします。これらの製品は、4 台のシリアル接続 SCSI（SAS）ハード ドライブが RAID1+0 で構成されています。注文方法については、Cisco.com を参照してください。	

表 1-1　サーバの最小限の要件 （続き）

コンポーネント	1 分あたりの最大受信データ レートを考慮した最小限の要件	
	1200 CDR または 5000 NAM/1040 ストリーム、もしくは 666 CDR および 1500 NAM/1040 ストリーム	1600 CDR
Windows 用ソフトウェア[2,3]	次のいずれか • Windows Server 2003 Service Pack 2、Standard または Enterprise Edition • Windows Server 2003 R2 Service Pack 2、Standard または Enterprise Edition （注） NTP - サーバが Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用するように設定し、ネットワーク内の Unified Communications Manager で使用されているタイム サーバと同期するようにします。「NTP 設定メモ」（P.2-4）を参照してください。	
使用可能なディスク スペース	• 70 GB 以上：SAS ディスク必須 （注） この 70 GB 中 26 GB が QOVR データベースに割り当てられます。 • 仮想メモリ：8 GB • NTFS ファイル システム[4]	
Cisco Secure ACS（オプション）	Cisco Secure ACS 4.2	

1. プロセッサは Intel Xeon または AMD Opteron を選択可能です。
2. Service Monitor サーバに使用するシステムは、Microsoft 社が Windows 2003 Server に推奨するすべてのセキュリティ ガイドラインを満たしている必要があります。セキュリティ ガイドラインについては、次の Microsoft 社の Web サイトを参照してください。
http://www.microsoft.com/technet/security/prodtech/WindowsServer2003.mspx
（Copyright © 2010, Microsoft Corporation）
3. Windows のターミナル サービスは、リモート管理モードでだけサポートされます。Windows のターミナル サービスやリモート デスクトップ、および Virtual Network Computing（VNC）を使用して、日常の運用（レポートの実行など）のためにサーバ上のタスクをリモート管理することはお勧めしません。詳細については、「Windows 2003 Server 用のターミナル サーバのサポート」（P.1-6）を参照してください。
4. FAT ファイル システムに Service Monitor をインストールしないでください。ファイル システムを確認するには、Windows デスクトップにある [My Computer] を開き、ドライブを右クリックしてポップアップ メニューから [Properties] を選択します。[Properties] ダイアログボックスの [General] タブにファイル システムのフィールドがあります。

クライアント要件

表 1-2 に、Service Monitor のための最小限のクライアント要件を示します。

表 1-2　クライアントの最小限のハードウェアおよびソフトウェア要件

コンポーネント	最小限の要件
ハードウェア / ソフトウェア	• 表示色数が 256 色に設定されたビデオ カードとカラー モニタ • 1.0 GHz 以上の Pentium 4 プロセッサを搭載し、次のいずれかの OS を実行している PC またはサーバ プラットフォーム – Windows XP Professional Service Pack 2 – Windows 2003 Server（Standard および Enterprise Edition）（Windows ターミナル サービスなし） • Internet Explorer 6.0.28、6.0.37、または 7.0 **（注）** 日常の運用（レポートの実行など）には、クライアント システムのブラウザを使用することを強く推奨します。日常の運用に、Windows ターミナル サービス、リモート デスクトップ、または VNC を使用することはお勧めできません。
使用可能なディスク スペース	1 GB の仮想メモリ
使用可能なメモリ（RAM）	512 MB 以上 仮想メモリを RAM のサイズの 2 倍に設定することをお勧めします。

（注）
- ブラウザが LAN でプロキシ サーバを使用するように設定していると、Service Monitor ではいくつかのレポート ウィンドウを開くことができません。[Internet Options] でプロキシ設定をディセーブルにしてください（[Connections] タブで、[LAN Settings] をクリック）。
- Service Monitor を使用するときは、デスクトップにインストールされている、ポップアップ ウィンドウの表示を抑制するすべてのソフトウェアをディセーブルにしてください。Service Monitor は、情報を表示するために複数のウィンドウを開く必要があります。

VMware に関するガイドライン

Service Monitor は、VMware ESX 3.5 および ESXi 4.x をサポートします。仮想環境の内部でも、標準（非仮想）インストールと同じシステム リソースを Service Monitor から使用できる必要があります。仮想セットアップにおける Service Monitor のパフォーマンスを判断するときは、標準インストールであれば通常 Service Monitor が使用できる一部のシステム リソースが VMware インスタンスによって使用されることを考慮する必要があります。仮想環境で Service Monitor を実行するためのその他の要件は、ご使用の環境とシステムの負荷によって異なります。詳細については、次の URL にある『*Best Practices for Cisco Unified Communication Suite on Virtualization*』を参照してください。

http://cisco.com/en/US/products/ps6535/products_user_guide_list.html

仮想環境でサポートされている Service Monitor の構成は次のとおりです。

- Service Monitor の単一インスタンスで最大 45,000 台の電話機がサポートされます。
- 異なる仮想マシンに次の各製品がインストールされます。

- Operations Manager
- Service Monitor
- Service Statistics Manager
- Provisioning Manager

この場合は、それぞれ最大 10,000 台の電話機と 1,000 台の IP デバイスがサポートされます（1 つの仮想マシン上でアプリケーションの 1 つのインスタンスを実行することが、サポートされている唯一の構成です）。

（注） 詳細については、次の URL にある『*Best Practices for Cisco Unified Communication Suite on Virtualization*』を参照してください。
http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html

VMware 環境で Service Monitor をセットアップするときは、次のガイドラインに従ってください。

- リソースは、仮想マシンの必要量の 100% を確保する必要があります。
- ライセンス取得済みの Service Monitor を VMware 環境で使用するには、仮想マシンに静的 MAC アドレスを設定する必要があります。

（注） 評価モードの Service Monitor は、動的 MAC アドレスでも実行できます。ただし、Service Monitor のライセンス取得済みコピーを実行するためには、事前に静的 MAC アドレスを設定する必要があります。

静的 MAC アドレスを設定するには、次の手順に従います。

ステップ 1　仮想マシンを停止します。

ステップ 2　[Inventory] パネルで、仮想マシンを選択します。

ステップ 3　[Summary] タブをクリックし、[Edit Settings] をクリックします。

ステップ 4　[Hardware] リストで、[Network Adapter] を選択します。

ステップ 5　MAC アドレスに対して [Manual] を選択します。

ステップ 6　仮想マシンの現在の MAC アドレスを 00:50:56:00:00:00 ～ 00:50:56:3F:FF:FF の範囲の静的 MAC アドレスに変更します。

静的 MAC アドレスを割り当てるときは、複雑なアドレスを選択することをお勧めします。複雑な MAC アドレスとは、たとえば 00:50:56:01:3B:9F のようなアドレスです。00:50:56:11:11:11 のような MAC アドレスは、1 が繰り返されているため、あまり複雑ではありません。

（注） 複雑なアドレスを選択すると、他のお客様が使用しているアドレスと重複する可能性が低くなります。こうすることで、異なるお客様の間での偶発的なライセンスの重複を避けることができます。

ステップ 7　[OK] をクリックします。

Windows 2003 Server 用のターミナル サーバのサポート

ターミナル サービスがリモート管理モードでイネーブルになっているシステムには、Service Monitor をインストールできます。ただし、ターミナル サービスがアプリケーション モードでイネーブルになっているシステムには、Service Monitor をインストールできません。

アプリケーション モードでターミナル サービスをイネーブルにしていた場合は、ターミナル サーバをディセーブルにしてシステムをリブートし、インストールを再度開始する必要があります。

表 1-3 に、Windows 2003 Server のターミナル サービス機能の概要を示します。

。

表 1-3　Windows 2003 Server でのターミナル サービス

Windows 2003 Server	機能
ターミナル サーバ	リモート アクセスおよび仮想システム。各クライアントは、それぞれ独自の仮想 OS 環境を持ちます。
リモート デスクトップ管理	リモート アクセスだけ。すべてのクライアントが、同一（かつ唯一）のオペレーティング システムを使用します。 **（注）** Cisco Unified Management Communications Suite アプリケーション（Operations Manager の Service Level View、Service Monitor でのレポート表示など）の日常のタスクの実行には、ターミナル サービスを使用しないでください。

Windows 2003 Server でのターミナル サービスのイネーブルとディセーブル

ターミナル サーバをイネーブルまたはディセーブルにするには、[Manage Your Server] > [Add or Remove a Role] > [Terminal Server] の順に移動します。

リモート デスクトップ管理をイネーブルまたはディセーブルにするには、[Control Panel] > [System] > [Remote] の順に移動します。

Windows 2003 Server での FIPS のイネーブルとディセーブル

Windows サーバでグループ セキュリティのために Federal Information Processing Standard（FIPS; 連邦情報処理標準）準拠の暗号化アルゴリズムがイネーブルにされていることがあります。

FIPS 準拠がオンの場合、Service Monitor サーバでの SSL 認証に失敗することがあります。Service Monitor が正しく動作するためには、FIPS 準拠をディセーブルにする必要があります。

Windows 2003 Server での FIPS のイネーブルとディセーブルの手順は次のとおりです。

ステップ 1　[Start] > [Settings] > [Control Panel] > [Administrative tools] > [Local Security Policy] の順に移動します。

[Local Security Policy] ウィンドウが表示されます。

ステップ 2　[Local Policies] > [Security Options] の順にクリックします。

ステップ 3　[System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing] を選択します。

ステップ 4　選択したポリシーを右クリックし、[Properties] をクリックします。

ステップ 5　[Enabled] または [Disabled] を選択して、FIPS 準拠アルゴリズムをイネーブルまたはディセーブルにします。

ステップ 6　[Apply] をクリックします。

変更を反映するには、サーバをリブートする必要があります。

ポートの使用

Service Monitor をインストールする前に、表 1-4 および表 1-5 の一覧で示されているポートが空いていることを確認してください。

（注） 表 1-4 および表 1-5 にあるポートはスキャンしないでください。

表 1-4 に、Service Monitor で使用されるポートの一覧を示します。Common Services は、Service Monitor と一緒にインストールされます。表 1-5 に、Common Services で使用されるポートの一覧を示します。

表 1-4　Service Monitor で使用されるポート

プロトコル	ポート番号	サービス名
TCP	22	SFTP - Service Monitor は、SFTP を使用して Unified Communications Manager versions 5.x 以降からデータを取得します。
UDP	53	DNS 用です。
UDP	67 および 68	DHCP 用です。
TCP	2000	SCCP：Service Monitor は、SCCP を使用して Cisco 1040 と通信します。
TCP	43459	データベース用です。
UDP	5666	Syslog：Service Monitor は、Cisco 1040 から Syslog メッセージを受信します。
TCP	5665 ～ 5680	ユーザ インターフェイスとバックエンド プロセスとのプロセス間通信用です。 これらのポートは空いている必要があります。

（注） Service Monitor は、TFTP を使用して任意の Cisco 1040 の設定ファイルを見つけ出します。Service Monitor はデフォルトで、TFTP サーバのポート 69 を使用します。

Common Services は、Service Monitor システムにもインストールされます。表 1-5 に、Common Services で使用されるポートの一覧を示します。

表 1-5　Common Services で使用されるポート

プロトコル	ポート番号	サービス名
TCP	23	Telnet
TCP	25	Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）
TCP	49	TACACS+ および ACS

表 1-5　Common Services で使用されるポート （続き）

プロトコル	ポート番号	サービス名
UDP	69	Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）
UDP	161	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
TCP	443	SSL モードの Common Services HTTP サーバ用 システムに IIS が存在する場合、IIS がディセーブルにされていても、インストールまたはアップグレード中に、443 以外の HTTPS ポートを選択するかどうかの確認が求められます。ポートの競合を回避するには、別のポートを選択する必要があります。
TCP	514	リモート コピー プロトコル用
UDP	514	Syslog
UDP	1431	MAC 通知トラップのトラップ リスナ用
TCP	1741	Common Services の HTTP プロトコル用
—	2002	AAA モードが ACS の場合の Cisco Secure ACS サーバとの通信用
TCP	8898	ログ サーバ
TCP	9007	Tomcat のシャットダウン用
TCP	9009	Tomcat で使用される Ajp13 コネクタ用
TCP	15000	ログ サーバ用
UDP	16236	UT ホストの獲得用
TCP	40050-40070	Device and Credential Repository（DCR）などの Common Services アプリケーションで使用される CSTM ポート **（注）**　Service Monitor は、DCR をサポートしません。
TCP	40401	ライセンス サーバ用
TCP	42340	デーモン マネージャ（サーバ プロセスのツール）用
UDP	42342	OSAGENT 用
TCP	42344	ANI HTTP サーバ用
UDP	42350	Event Services Software（ESS; イベント サービス ソフトウェア）用（代替ポートは 44350/udp）
TCP	42351	ESS Listening 用（代替ポートは 44351/tcp）
TCP	42352	ESS HTTP 用（代替ポートは 44352/tcp）
TCP	42353	ESS ルーティング用（代替ポートは 44352/tcp）
TCP	43441	CMF データベース用
TCP	50001	SOAP Monitor 用

CHAPTER 2

Service Monitor のインストール、アンインストール、およびアップグレード

ここでは、次の内容について説明します。

Service Monitor をインストールするための準備

Service Monitor のインストールを正常に実行するには、以下を確認してから Cisco Unified Service Monitor（Service Monitor）をインストールします。

- お使いのハードウェアおよびソフトウェアが、サーバ要件を満たしているようにします。「サーバ要件」（P.1-2）を参照してください。
- Service Monitor サーバをインストールに向けて準備します。「サーバの準備」（P.2-2）を参照してください。
- Service Monitor および Common Services の使用するポートが、使用中でないことを確認します。「必要なポートが使用中でないことの確認」（P.2-3）を参照してください。
- Service Monitor のインストール中に指定する必要のある情報を集めます。「インストール中に指定する情報の収集」（P.2-3）を参照してください。

サーバの準備

（注） Service Monitor サーバに使用するシステムは、Microsoft 社が Windows 2003 Server に推奨するすべてのセキュリティ ガイドラインを満たしている必要があります。NSA Web サイトのセキュリティ ガイドライン（http://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml#microsoft）を参照してください。

特に TCP/IP スタックは、DoS 攻撃を受けないよう堅牢にする必要があります。NSA Web サイトからダウンロード可能な『The Windows Server 2003 - Security Guide, v2.1』の 103 ページにある「Security Consideration for Network Attacks」を参照してください。

Operations Manager をインストールしている場合は、Service Monitor はすでにサーバにインストールされています。このようなサーバにある Service Monitor をアクティブ化するには、Cisco.com に PAK を登録し、Cisco Unified Service Monitor 用のライセンス ファイルをインストールします （「ライセンス」（P.B-1）を参照）。

Service Monitor をインストール、再インストール、およびアップグレードする前に、以下を実行します。

- Windows システムに設定されているプライマリおよびアクティブな地域の設定が、英語（米国）または日本語のいずれかであることを確認します。Service Monitor では、これ以外のオプションはサポートされていません。

  アクティブな地域の設定は、[Control Panel] > [Regional and Language Options] > [Regional Options] で設定できます。

- システムの日付および時刻を正しく設定します。詳細については、URL（http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/release/notes/cs32rel.html#wp55504）にある『*Release Notes for CiscoWorks Common Services 3.2*』の「Time Zone and Acronyms and Offset Settings」を参照してください。
- Service Monitor をインストールするドライブが、NTFS ファイル システムであることを確認します。
- Service Monitor をインストールするシステムの完全修飾ドメイン名が、ドメイン ネーム システム（DNS）による解決が可能なものであることを確認します。DNS 名から IP アドレスの参照と、IP アドレスから DNS 名の参照の両方を実行できる必要があります（DNS の用語では、正引きおよび逆引き）。Service Monitor サーバの名前解決を確認するには、コマンド プロンプトでコマンド「*NMSROOT*¥bin>smNameRes.exe」を実行します。

  （注） NMSROOT は、システム上で Service Monitor がインストールされるディレクトリです。インストール中にデフォルト ディレクトリを選択した場合は、C:¥PROGRA~1¥CSCOpx となります。

- システムのウイルス スキャン ソフトウェアを無効にします。これは、インストールの完了後に再起動できます。
- システムで Cisco Security Agent が実行されている場合は、これをディセーブルにします。これは、インストールの完了後に再起動できます。
- 開いているプログラムやアクティブなプログラムをすべて終了します。インストール処理の間、他のプログラムを実行しないでください。

以下の場所には、Service Monitor をインストールしないでください。

- プライマリ ドメイン コントローラ（PDC）またはバックアップ ドメイン コントローラ（BDC）。

- アプリケーション サーバ モードでイネーブルにされているターミナル サービスが含まれる Advanced Server。

Service Monitor は、固定 IP アドレスを持つシステムにインストールする必要があります。

以下のタスクは、インストール完了の前または後に実行する必要があります。

- Service Monitor サーバを設定し、Unified Communications Manager ユーザと同じ NTP サーバと同じサーバを使用するようにします。「NTP 設定メモ」（P.2-4）を参照してください。
- Service Monitor 用のライセンス ファイルを取得します。「ライセンス」（P.B-1）を参照してください。

以下のインストール メモを確認します。

- Service Monitor は、デフォルト ディレクトリである *SystemDrive*:¥Program Files¥CSCOpx にインストールされます。

  SystemDrive は、Windows オペレーティング システムがインストールされているディレクトリです。

  インストール中に別のディレクトリを選択すると、アプリケーションはそのディレクトリにインストールされます。

  インストール先フォルダには、次の特殊文字を使用できません。

  !@ # $ % ^ & * ( ) + | } { " [ ] ; ' / ?< > , . ` =

  インストール中にエラーが発生した場合、オペレーティング システムがインストールされているドライブのルート ディレクトリにあるインストール ログ ファイルを確認します。インストールごとに新しいログ ファイルが作成されます。次の例を参考にしてください。

  C:¥Ciscoworks_install_*YYYYMMDD_hhmmss*.log。*YYYYMMDD* はインストールの年月日を示し、*hhmmss* はインストールの時分秒を示しています。

  次の例を参考にしてください。

  ```
  C:\Ciscoworks_install_20060721_182205.log
  ```

- いつでも [Cancel] をクリックして、インストールを終了できます。ただし、システムに加えた変更は元に戻りません。

  たとえば、新しいファイルがインストールされたり、それらがシステム ファイルに対する何らかの変更である場合、手動でインストール ディレクトリをクリーンアップする必要があります。

- サードパーティの SNMP 管理ツールを使用して Service Monitor をモニタするには、「システムを SNMP クエリー対応に設定」（P.2-21）を参照してください。

インストール中に指定する情報の収集

インストール中、各種のユーザ アカウントとデータベースにパスワードを設定する必要があります。ユーザ アカウントとパスワードに関するルールの詳細については、「パスワード情報」（P.A-7）を参照してください。メール設定（HTTPS ポートなど）およびセキュリティ証明書情報を指定する必要が生じることがあります。詳細については、「インストール、再インストール、アップグレードのためのユーザ入力」（P.A-1）を参照してください。ライセンス ファイルの場所を指定したり、[Evaluation only] を選択したりする必要が生じることもあります。詳細については、「ライセンス」（P.B-1）を参照してください。

必要なポートが使用中でないことの確認

Service Monitor および Common Services で使用するポートは、使用中でないことが必要です。ポート一覧については、「ポートの使用」（P.1-7）を参照してください。

NTP 設定メモ

Service Monitor レポートに不備なく最新の情報が含まれ、所定の期間のアクティビティが正確に反映されるようにするには、Service Monitor と Unified Communications Manager サーバの時計が同期している必要があります。以下の事項は NTP 設定の簡単な説明であり、完全なガイドではありません。

次のようにします。

1. Unified Communications Manager の管理者と相談し、Service Monitor が同期する必要のあるタイム サーバを特定します。Cisco.com のページ（URL：http://cisco.com/en/US/products/sw/voicesw/ps556/prod_white_papers_list.html）にあるホワイト ペーパー「*Cisco IP Telephony Clock Synchronization: Best Practices*」を参照すると有用です。
2. システムのドキュメントを使用して、Service Monitor のインストール先となる Windows Server 2003 システムに NTP を設定します。ネットワーク内の Cisco Unified Communication Managers で使用されているタイム サーバを使用して、NTP を設定します。この URL（http://support.microsoft.com/kb/816042）の「*How to configure an authoritative time server in Windows Server 2003*」を参照すると有用です。

（注）　この Web サイトは Copyright© 2010, Microsoft Corporation です。

NAM を設定し、Unified Communications Manager インスタンスと同じ NTP サーバを使用することもお勧めします。

Cisco Unified Service Monitor のインストール

システムのインストール準備を完了するため、「Service Monitor をインストールするための準備」（P.2-1）を参照し、必要なタスクを実行します。

（注）　インストール中は、Windows Management Instrumentation（WMI）サービスを実行しないでください。WMI がプロセスをロックし、途中でインストールが終了する可能性があります。WMI サービスが実行中の場合はインストール中に通知が行われ、このサービスを停止し、インストール完了後に再起動する許可を求めるメッセージが表示されます。

（注）　シスコでは、インストールを途中で終了しないことを推奨しています。

ステップ 1　Service Monitor 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、次のいずれかを実行します。

- eDelivery システムを通じて取得した [Cisco_Unified_ServiceMonitor_2.3_with_Common_Services_3.2.exe] をクリックします。
- CD-ROM ドライブに Service Monitor CD を挿入します。

（注）　eDelivery システムを利用できるかどうかは、発注方法によって異なります。詳細については、「PAK の入手」（P.B-4）を参照してください。

[Cisco Unified Service Monitor 2.3 Setup Program] ウィンドウが表示されます。

ステップ 2　メッセージが表示された場合は、確認してから続行します。

- WMI サービスが実行中の場合、インストール続行のために WMI サービスを停止し、インストール完了後に WMI サービスを再起動することを伝えるメッセージが表示されます。続行するには [Yes] をクリックします。
- IIS が検出された場合（ディセーブルの場合を含む）は、メッセージが表示されます。IIS とのポート競合を避けるには、[OK] をクリックします。後の手順で、443 以外の HTTPS ポートを選択するよう求められます。

  [Welcome] ウィンドウが表示されます。

ステップ 3　[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 4　[I accept the terms of the license agreement] オプション ボタンを選択し、[Next] をクリックします。

ステップ 5　[Licensing Information] ウィンドウが表示されます。

ステップ 6　次のいずれかを選択し、[Next] をクリックします。

- [License File Location]：参照して場所を入力します。
- [Evaluation Only]：インストールを完了し、後でライセンス ファイルを登録できます。

（注）　ライセンス ファイルの取得方法については、「ライセンス プロセス」（P.B-4）を参照してください。

インストール プログラムによって、名前参照および DHCP が確認されます。システムに固定 IP アドレスが設定されていない場合は、[DHCP-Enabled Network Adapters] ダイアログ ボックスが表示されます。[Yes] をクリックします。

動的 MAC アドレスを使用して仮想マシンをインストールする場合は、また別の警告メッセージが表示されます。[Yes] をクリックします （インストールを完了できても、Service Monitor は機能しません。詳細については、「VMware に関するガイドライン」（P.1-4）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 7　次のいずれかのオプション ボタンを選択します。

- [Typical]：入力情報を最小限に抑えて Service Monitor 2.3（および Common Services 3.2）をインストールします。
- [Custom]：インストール ディレクトリを選択し、ユーザとデータベースのパスワードを入力して Service Monitor 2.3（および Common Services 3.2）をインストールします。

[Typical] インストール モードを選択すると、Common Services インストール用に次の情報が入力されます。guest パスワード、Common Services データベース パスワード、メール設定、および自己署名証明書情報。この手順の残りの部分は、標準インストール用に記述されています。

[Custom] インストール モードを選択すると、インストール中に上記の情報を入力するよう求められます。

ステップ 8　[Next] をクリックします。[Select Components] ウィンドウが表示されます。

ステップ 9　オプション ボタンを選択します。[Next] をクリックします。

インストール プログラムによって、依存関係とシステム要件がチェックされます。[System Requirements] ウィンドウに要件チェックの結果が表示され、インストールの続行が可能かどうかが通知されます。次のいずれかの状態が発生する場合があります。

- ディスク空き容量が不足している場合、適切なオペレーティング システムが存在しない場合、または最低限必要なメモリを確保できない場合、インストール プログラムによりエラー メッセージが表示され、処理が停止します。
- システムのメモリが 4 GB 未満の場合、インストールを続行できますが、次のメッセージを確認する必要があります。

```
WARNING: System memory is less than the requirement for Cisco Unified Service
Monitor system to support high call volume.
Please refer to Service Monitor documentation for more details and upgrade the
memory to at least 4GB if you have high call volume.
```

- ディスク空き容量が 73000 MB 未満の場合、インストールを続行できますが、次のメッセージを確認する必要があります。

```
Current disk space <nnnn> MB is less than Recommended disk space 73000 MB and it
may affect performance.
```

（注）　[System Requirements] ウィンドウに表示されるディスク空き容量は、Service Monitor のインストールと起動に最低限必要な容量です。推奨されるディスク空き容量（表 1-1（P.1-2）を参照）は、Service Monitor の使用に最低限必要な容量です。

- その他の最小要件が満たされていない場合は、インストール プログラムによって対応するメッセージが表示され、インストールが続行されます。

ステップ 10　[Next] をクリックします。[Change Admin Password] ウィンドウが表示されます。

a. admin ユーザのパスワードを入力して確認し、[Next] をクリックします。

（注）　パスワードはメモしておいてください。セキュリティの設定およびその他のユーザの作成が完了するまでは、Service Monitor へのログインにこのパスワードが必要です。

[Enter System Identity Account Password] ウィンドウが表示されます。

b. 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て確認し、[Next] をクリックします。[Create casuser] ダイアログ ボックスが表示されます。

c. [Yes] をクリックし、インストールを続行します。

（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次の情報を入力するよう求められます。guest パスワード、Common Services データベース パスワード、メール設定、および自己署名証明書情報。
- HTTPS ポートを 443 から別の番号に変更する場合、メール設定情報のページが表示されます。

ステップ 11　[Summary] ウィンドウが表示され、現在の設定内容が示されます。[Install] をクリックします。インストール中に、追加の情報メッセージが表示されます。

ステップ 12　追加のメッセージが表示されたら、[OK] をクリックします。これらはインストールの進行を確認するためのものです。

- 次のメッセージを示すダイアログ ボックスが表示されることがあります。

  ```
  Before you reboot this system, configure automatic time synchronization on it using
  NTP. Configure this system to use the time server that is used by Cisco Unified
  Communications Managers in your network.
  ```

  詳細については、「NTP 設定メモ」（P.2-4）を参照してください。

- 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、次のメッセージが表示されます。

  ```
  Windows SNMP service is not installed on your system. This installation will continue.
  To install support for system application and host resources MIBs, you must install
  the Windows SNMP service, using Add/Remove Programs from the Control Panel.
  ```

  評価目的で Service Monitor をインストールする場合は、次のメッセージが表示されます。

  ```
  Please obtain a valid license key from Cisco.com within 90 days.
  ```

[Restart] ウィンドウが表示されます。[Yes, I want to restart my computer now] オプション ボタンが選択されています。

ステップ 13　[Finish] をクリックします（ステップ 14 を開始する前に、コンピュータを再起動する必要があります）。

ステップ 14　インストールが完了したら、以下を実行します。

a.　Service Monitor を起動し、正しくインストールされていることを確認します。「Cisco Unified Service Monitor の起動」（P.2-7）を参照してください。

b.　ウイルス スキャンの対象から、*NMSROOT*¥databases ディレクトリを除外します。ウイルス スキャンのためにデータベース ファイルがロックされると、問題が発生することがあります。

（注）　*NMSROOT* は、Service Monitor がインストールされているシステムのディレクトリです。インストール時にデフォルト ディレクトリを選択した場合は、C:¥Program Files¥CSCOpx です。

Cisco Unified Service Monitor の起動

Service Monitor を起動する前に、以下を実行してください。

- Service Monitor 2.3 のインストールまたはアップグレード インストールの完了後には、システムを再起動します。
- クライアント システムにインストールされているポップアップ ブロッカ ユーティリティをディセーブルにします。

（注）　デフォルトでは、SSL は Common Services でイネーブルにされていません。

ステップ 1　次のようにして、適切なアドレスをブラウザに入力します。

- Service Monitor 2.3 をアップグレード インストールした場合に、SSL が Common Services ですでにイネーブルにされているときは、「https://*servername*:*port number*」と入力します。

  - servername は、Service Monitor がインストールされているサーバの IP アドレスまたは DNS 名です。
  - port number は 443（デフォルト）またはアップグレード中に入力した HTTPS ポート番号です。ログイン ページが表示されます。
- SSL がイネーブルにされていない場合は、「http://*servername*:171 」と入力します。servername は、Service Monitor がインストールされているサーバの IP アドレスまたは DNS 名です。ログイン ページが表示されます。

ステップ 2　ユーザ名とパスワードを入力します。ユーザ名がない場合は、次の手順を実行します。

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

Service Monitor のホーム ページが表示されます

Service Monitor 2.3 にアップグレードする前の準備

ここでは、次の内容について説明します。

アップグレードの方法

Service Monitor 2.1 または Service Monitor 2.2 からだけ、Service Monitor 2.3 に直接アップグレードできます。引き続き既存のコール データに関するレポートを実行できるようコール データを保存するには、アップグレード開始前にコール データを移行する必要があります。詳細については、「（オプション）アップグレード前のデータ移行計画およびコール データ移行計画」（P.2-11）を参照してください。

アップグレードでは、設定データ（TFTP サーバ、トラップ レシーバ、資格情報など）は自動的に移行されます。

（注）　Service Monitor 2.1 よりも前のリリースからの直接アップグレードはサポートされていません。

Service Monitor 2.3 にアップグレードする場合、

- Service Monitor 2.1 からのときは、Common Services がリリース 3.2 にアップグレードされます。詳細については、「サードパーティ製のツールおよびソフトウェアの変更」（P.2-9）を参照してください。

- Service Monitor 2.2 からのときは、Common Services およびサードパーティ製品のバージョンは変更されません。

サードパーティ製のツールおよびソフトウェアの変更

（注）　この説明は、Service Monitor 2.1 からのアップグレードの場合にだけ該当します。

次のサードパーティ製コンポーネントは削除され、Common Services 3.2 のオープン ソース コンポーネントに置き換えられます。

- Visigenic：CORBA 通信に使用されていたものです。JACORB に置き換えられます。
- Tibco：イベント サービスに使用されていたものです。ActiveMQ に置き換えられます。

次のコンポーネントのアップグレードは、Common Services 3.2 で実行されます。

- Sybase ASA がバージョン 9.x から 10.0.1 にアップグレードされます。
- Java ランタイム環境（JRE）が JRE 1.5.0_1 にアップグレードされます。Java Plug-in 1.6.0_05 が提供されます。

Service Monitor ファイルおよびデータベースのバックアップ

アップグレードでは、システムのバックアップは実行されません。アップグレード前に、バックアップを実行する必要があります。

ステップ 1　次の手順で Service Monitor データベースをバックアップします。

a. Service Monitor がインストールされているシステムにログインします。

b. 次のコマンドを使用して、デーモン マネージャを停止します。

net stop crmdmgtd

c. *NMSROOT*¥databases¥qovr から、qovr.db ファイルおよび qovrx.log ファイルをテープ、外部ドライブ、またはネットワーク ディレクトリ（ローカル ディレクトリ以外の場所）にコピーします。こうしておくと、ハードウェア障害に備えてデータの整合性を確保し、バックアップ データがローカル ディスクの空き容量を使い果たさないようにできます。

d. 次のコマンドを使用して、デーモン マネージャを再起動します。

net start crmdmgtd

（注）　データベースを復元するには、ステップ 1 a. および 1 b. を実行し、保存したファイルを復元して、ステップ 1 d. を実行します。

ステップ 2　次の手順で、CiscoWorks バックアップを使用して Service Monitor 設定データをバックアップします。

a. ウィンドウ右上隅の [CiscoWorks] をクリックします。CiscoWorks ホームページが表示されます。

b. [Help] ボタンをクリックし、データのバックアップと復元に関する手順に従います。

（注）　Service Monitor 設定データを復元し、さらにデータベースを復元する必要があります。

Service Monitor データベースと設定データの両方を復元するには、2 つの手順が必要です。データベースを手動で復元し、設定データを復元します（ステップ 2 b. を使用）。

アップグレードがデータに及ぼす影響の確認

レポート データ（コール データ）を移行するには、Service Monitor 2.3 へのアップグレードを開始する前にコール移行ツールを実行する必要があります。詳細については、「（オプション）アップグレード前のデータ移行計画およびコール データ移行計画」（P.2-11）を参照してください。

Service Monitor 2.3 にアップグレードする場合、

- Service Monitor 設定データ（資格情報、しきい値設定など）は維持されます。
- Common Services データは維持されます。

（注）　Service Monitor 2.1 からのアップグレードの場合、Common Services のリリース バージョンは 3.2 にアップグレードされます。詳細については、「サードパーティ製のツールおよびソフトウェアの変更」（P.2-9）を参照してください。

Service Statistics Manager のダイヤル プラン設定データの手動記録

（注）　Service Monitor 2.3 にアップグレードする場合に、ネットワークに Service Statistics Manager がインストールされているとき、この情報は重要です。

Service Monitor 2.3 は Operations Manager 2.3 および Service Statistics Manager 1.3 と相互運用できます。コール分類（コール カテゴリおよびダイヤル プラン）設定は、Service Monitor 2.3 には組み込まれていますが、Service Statistics Manager 1.3 からは削除されています。

注意　Service Statistics Manager 1.3 にアップグレードすると、コール設定データは失われます。

アップグレード前に、スクリーンショットまたはその他の方法で、Service Statistics Manager 1.2 に設定されているダイヤル パターン、ゲートウェイ コード、フリーダイヤル番号、サービス番号を手動で記録してください。Service Monitor 2.3 でコール分類を設定する際に参照できるよう、このスクリーンショットまたはメモを保存しておきます。

（注）　Service Monitor 2.3 にアップグレードする前に、Service Statistics Manager サーバを停止しておく必要があります。

（オプション）アップグレード前のデータ移行計画およびコール データ移行計画

コール データの移行は任意です。ただし、データを維持するには、Service Monitor 2.3 へのアップグレードを開始する前に、移行しておく必要があります。Cisco.com にある Service Monitor 製品が収容されている zip ファイルに、コール移行ツールが収められています。

（注）　Call Migration Tool と共に収められている README_QOVR_CMT.TXT ファイル には、データ移行に要する時間と使用されるディスク容量の評価が記載されています。このほか、ここにはツール実行時の Operations Manager および Service Statistics Manager（ネットワークにインストールされている場合）に対する影響が説明されています。

ステップ 1　Cisco.com から、Service Monitor 製品が収容されている zip ファイル（CUSM2_3.zip）をダウンロードします。次の手順に従ってアクセスしてください。

a. この URL（ http://www.cisco.com/en/US/partner/products/ps6536/tsd_products_support_series_home.html）に移動します。

b. Cisco.com にログインしていない場合は、ログインします。

c. [Download Software] リンクをクリックします。

d. オンライン上の指示に従って Cisco Unified Service Monitor 2.3 を選択し、zip ファイルをダウンロードします。

ステップ 2　CUSM2_3.zip ファイルの ¥install¥CallMigrationTool フォルダにある QOVR_CMT.zip ファイルを展開します。

ステップ 3　QOVR_CMT.zip ファイルの README_QOVR_CMT.TXT ファイルを展開し、記載されている情報を利用して移行を計画し実行します。

TFTP サーバからの Cisco 1040 コンフィギュレーション ファイルの削除

アップグレード前に、既存の TFTP サーバから既存の Cisco 1040 コンフィギュレーション ファイルおよびバイナリ イメージ ファイルを削除することをお勧めします。以下のファイルを削除します。

- Cisco 1040 センサー コンフィギュレーション ファイル：QOVDefault.CNF ファイル、および QoV*MACAddress*.CNF ファイル（Cisco 1040 ごと）。
- バイナリ イメージ ファイル：SvcMonAA2_*nn*.img

アップグレード後の追加処理をなくす方法

Unified Communications Manager 5.x 以降からコールをモニタしている場合、以下に留意する必要があります。

- Service Monitor 2.3 へのアップグレード中、すべてのプロセスが停止します。Unified Communications Manager 5.x 以降からのデータ ファイルを受信するときに、Service Monitor を使用できません。
- アップグレード完了後、
  - Unified Communications Manager から Service Monitor に未処理のデータ ファイルがすべて送信されます。これには時間がかかります。
  - Service Monitor では古いファイルが削除されます。

この処理をなくすため、アップグレード前に以下を実行できます。

- Unified Communications Manager 7.x 以降が、未処理データを送信しないようにします。これには、ビリング サーバを編集し、[Resend on Failure] チェック ボックスをオフにします。詳細については、『*User Guide for Cisco Unified Service Monitor 2.3*』の「Unified Communications Manager Configuration」を参照してください。
- バージョン 7.x よりも前の Unified Communications Manager ソフトウェア リリースについては、Unified Communications Manager から Service Monitor アプリケーション ビリング サーバを削除し、CDR Repository Manager サービスを再起動して、データが送信されないようにします。「Unified Communications Manager からの Service Monitor の削除」（P.2-12）を参照してください。アップグレード完了後、Service Monitor を Unified Communications Manager に追加し、CDR Repository Manager サービスを再起動できます。

Unified Communications Manager からの Service Monitor の削除

この手順は、Service Monitor 2.3 にアップグレードする場合に、Unified Communications Manager 5.x または 6.x からコールをモニタしている場合に推奨されるものです。

（注）　Unified Communications Manager 7.x 以降については、障害発生時にデータを再送信しないよう設定できます。詳細については、『*User Guide for Cisco Unified Service Monitor 2.3*』の「Unified Communications Manager Configuration」を参照してください。

ステップ 1　Unified Communications Manager Serviceability を起動します。

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

ステップ 3　Billing Applications Server Parameters までスクロール ダウンし、アップグレードする Service Monitor サーバを探します。[Hostname/IP Address] および [User Name] 列のエントリからサーバを特定できます（[User Name] 列には [smuser] が表示されます）。

ステップ 4　アップグレードする Service Monitor サーバのチェック ボックスを選択します。

ステップ 5　[Delete Selected] をクリックします。

ステップ 6　次のようにして、CDR Repository Service を再起動します。

a. Unified Communications Manager Serviceability から、[Tools] > [Control Center - Network Services] をクリックします。

b. サーバ一覧から、パブリッシャを選択します。

c. CDR Services まで下にスクロールします。

d. [Cisco CDR Repository Manager] オプション ボタンを選択します。

e. [Restart] ボタンをクリックします。

NTP の設定

Unified Communications Manager を Service Monitor に追加する場合に、NTP を使用するよう Service Monitor サーバを設定できていないときは、アップグレードの前または後に設定します。詳細については、「NTP 設定メモ」（P.2-4）を参照してください。

Service Monitor 2.3 へのアップグレード

アップグレードの前に、以下を実行する必要があります。

- システムのウイルス スキャン ソフトウェアを無効にします。これは、アップグレードの完了後に再起動できます。
- システムで Cisco Security Agent が実行されている場合は、これをディセーブルにします。これは、アップグレードの完了後に再起動できます。
- ネットワークで Service Statistics Manager を実行している場合、
  1. Service Statistics Manager のコール分類データを記録します（「Service Statistics Manager のダイヤル プラン設定データの手動記録」（P.2-10）を参照）。
  2. Service Statistics Manager サーバを停止します。

（注）　Service Monitor 2.3 へのアップグレード完了後に、Service Monitor でダイヤル プランを設定し、Service Statistics Manager 1.3 にアップグレードする必要があります。

- 「Service Monitor 2.3 にアップグレードする前の準備」（P.2-8）を参照し、必要なタスクをすべて実行します。以下に留意してください。
  - アップグレードでは、システムに新しいファイルをコピーおよびインストールする前に、バックアップは*実行されません*。バックアップを実行するには、「Service Monitor ファイルおよびデータベースのバックアップ」（P.2-9）を参照してください。
  - レポート データを維持するには、このアップグレードを開始する前に、Call Migration Tool を実行する必要があります。詳細については、「（オプション）アップグレード前のデータ移行計画およびコール データ移行計画」（P.2-11）を参照してください。

（注）　アップグレードの完了後、「アップグレード後に実行する Cisco 1040 向けの設定」（P.2-17）に記載されたタスクを完了するまでは Cisco 1040 は Service Monitor に登録されません。

ステップ 1　Service Monitor 2.1 または Service Monitor 2.2 がインストールされているマシンにローカル管理者としてログインし、次のいずれかを実行します。

- eDelivery システムを通じて取得した [Cisco_Unified_ServiceMonitor_2.3_with_Common_Services_3.2.exe] をクリックします。
- CD-ROM ドライブに Service Monitor CD を挿入します。

（注）　eDelivery システムを利用できるかどうかは、発注方法によって異なります。詳細については、「PAK の入手」（P.B-4）を参照してください。

[Cisco Unified Service Monitor 2.3 Setup Program] ウィンドウが表示されます。

ステップ 2　メッセージが表示された場合は、確認してから続行します。

- WMI サービスが実行中の場合、インストール続行のために WMI サービスを停止し、インストール完了後に WMI サービスを再起動することを伝えるメッセージが表示されます。続行するには [Yes] をクリックします。
- IIS が検出された場合（ディセーブルの場合を含む）は、メッセージが表示されます。IIS とのポート競合を避けるには [Yes] をクリックします。後の手順で、443 以外の HTTPS ポートを選択するよう求められます。
- データベースのバックアップは実行されないことを伝えるメッセージが表示されます （アップグレード前に実行する必要があります）。続行するには、[OK] 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 3　[Next] をクリックします。Call Migration Tool を実行しないで続行すると、コール データが失われることを伝えるダイアログが表示されます （Call Migration Tool を実行するには、インストールを終了します。「（オプション）アップグレード前のデータ移行計画およびコール データ移行計画」（P.2-11）を参照してください）。

ステップ 4　続行するには、[Yes] 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　[I accept the terms of the license agreement] オプション ボタンを選択し、[Next] をクリックします。

ステップ 6　インストール プログラムによって、名前参照および DHCP が確認されます。システムに固定 IP アドレスが設定されていない場合は、[DHCP-Enabled Network Adapters] ダイアログ ボックスが表示されます。[Yes] 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 7　次のいずれかのオプション ボタンを選択します。

- [Typical] : 入力情報を最小限に抑えて Service Monitor 2.3 （および Common Services 3.2）にアップグレードします。
- [Custom] : Service Monitor 2.3 （および Common Services 3.2）にアップグレードします。データを入力しますが、入力しない場合は自動的に入力されます。

（注）　詳細については、「アップグレードがデータに及ぼす影響の確認」（P.2-10）を参照してください。

[Typical] インストール モードを選択すると、インストール中に次の情報が入力されます。guest パスワード、Common Services データベース パスワード、メール設定、および自己署名証明書情報。

[Custom] インストール モードを選択すると、アップグレード中に上記の情報を入力するよう求められます。

ステップ 8　[Next] をクリックします。[Select Applications] ウィンドウが表示されます。

ステップ 9　オプション ボタンをすべて選択し、[Next] をクリックします。インストール プログラムによって、依存関係とシステム要件がチェックされます。

[System Requirements] ウィンドウに要件チェックの結果が表示され、インストールの続行が可能かどうかが通知されます。次のいずれかの状態が発生する場合があります。

- ディスク空き容量が不足している場合、または最低限必要なメモリを確保できない場合、インストール プログラムによりエラー メッセージが表示され、処理が停止します。

- システムのメモリが 4 GB 未満でも最小要件を満たしていればインストールを続行できますが、次のメッセージを確認する必要があります。

```
WARNING: System memory is less than the requirement for Cisco Unified Service
Monitor system to support high call volume.
Please refer to Service Monitor documentation for more details and upgrade the
memory to at least 4GB if you have high call volume.
```

- ディスク空き容量が 73000 MB 未満の場合、インストールを続行できますが、次のメッセージを確認する必要があります。

```
Current disk space <nnnn> MB is less than Recommended disk space 73000 MB and it may
affect performance.
```

[System Requirements] ウィンドウに表示されるディスク空き容量は、Service Monitor のインストールと起動に最低限必要な容量です。推奨されるディスク空き容量（「サーバおよびクライアントのシステム要件」（P.1-2）を参照）は、Service Monitor の使用に最低限必要な容量です。

- その他の最小要件が満たされていない場合は、アップグレード プログラムによって対応するメッセージが表示され、インストールが続行されます。

ステップ 10　[Next] をクリックします。システムに IIS が検出された場合に、デフォルトの HTTPS ポートの変更を選択した場合（ステップ 2を参照）、[Mail Settings] ウィンドウが表示されます。

a. HTTPS ポート番号（デフォルトは 443）、電子メール アドレス、および SMTP サーバを入力します （IIS がインストールされている場合、ポート競合を回避するため HTTPS ポート番号を 443 以外に設定します）。

b. [Next] をクリックします。

[Change casuser Password] ウィンドウが表示されます。

ステップ 11　パスワードを入力して確認し、[Next] をクリックします。[Summary] ウィンドウが表示され、現在の設定内容が示されます。

ステップ 12　[Install] をクリックします。アップグレード処理がしばらく続いた後に、再び入力を求められます。

Service Monitor 2.1 からのアップグレードの場合、

a. Common Services（cmf）および Service Monitor（qovr）データベースは、以降のバージョンの Sybase にアップグレードされます。Common Services データベース内の全データは維持されます。Service Monitor データベースでは設定データが維持されています。Service Monitor データベースがアップグレードされる前に、メッセージが表示されます。

b. アップグレードを続行するには、[OK] をクリックします。

ステップ 13　追加のメッセージが表示された場合は、[OK] をクリックします。これらはアップグレードの進行を確認するためのものです。

- 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、次のメッセージが表示されます。

```
Windows SNMP service is not installed on your system. This installation will continue.
To install support for system application and host resources MIBs, you must install
the Windows SNMP service, using Add/Remove Programs from the Control Panel.
```

[OK] をクリックします。（詳細については、「システムを SNMP クエリー対応に設定」（P.2-21）を参照してください）。

- ダイアログ ボックスに次のメッセージが表示される場合があります。

```
Before you reboot this system, configure automatic time synchronization on it using
NTP. Configure this system to use the time server that is used by Cisco Unified
Communications Managers in your network.
```

[OK] をクリックします。（詳細については、「NTP 設定メモ」（P.2-4）を参照してください）。

ステップ 14　最後のウィンドウが表示されます。[Yes, I want to restart my computer] オプション ボタンを選択し、[Finish] をクリックします。

ステップ 15　コンピュータを再起動したら、以下を実行します。

a. Service Monitor を起動し、アップグレードが行われたことを確認します。「Cisco Unified Service Monitor の起動」（P.2-7）を参照してください。

b. 「アップグレード後に実行する Cisco 1040 向けの設定」（P.2-17）に記載されたタスクを完了します。この手順を完了するまで、Cisco 1040 は Service Monitor に登録されません。

c. Unified Communications Manager 5.x 以降から Service Monitor アプリケーション ビリング サーバを削除した場合は、これを追加します。「Service Monitor を Unified Communications Manager に追加する」（P.2-16）を参照してください。

d. casuser のパスワードを新たに入力したか、またはインストール プログラムでランダムに生成するようにした場合、「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照してください。

（注）　アップグレード後、ロギング設定はデフォルト値に戻されています。そのため、Service Monitor ログ ファイルに書き込まれるのはエラー メッセージだけになります。プログラムのデバッグに役立てるためログ ファイルに情報を追加する必要がある場合は、ロギング設定を更新します。詳細については、Service Monitor のオンライン ヘルプを参照してください。

Service Monitor を Unified Communications Manager に追加する

アップグレード前に Service Monitor アプリケーション ビリング サーバを Unified Communications Manager から削除した場合は、Service Monitor アプリケーション ビリング サーバを Unified Communications Manager に追加します。

（注）　このタスクは、Unified Communications Manager version 5.x 以降で実行します。この作業は、Service Monitor の稼動中に限り行ってください。

ステップ 1　Unified Communications Manager Serviceability を起動します。

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

ステップ 3　Billing Applications Server Parameters までスクロールし、[Add New] をクリックします。

ステップ 4　次のフィールドにデータを入力します。

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

  （注）　smuser 以外のユーザ名を入力しないでください。

- [Password]：パスワードを入力します。デフォルトのパスワードは smuser です。このパスワードを変更するには、次の手順を実行します。
  - まず Service Monitor でパスワードを変更します （[Configuration] > [Other Settings] を選択します。詳細については、オンライン ヘルプを参照してください）。

- Service Monitor の他の設定で smuser に対して入力したのと同じパスワードを入力します。

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

- [SFTP Protocol] を選択します。
- [Directory Path] :「/home/smuser/」と入力します。

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

ステップ 5　[Add] をクリックします。場合によっては、新しく追加されたビリング サーバに CDR/CMR ファイルが送信されるように、まず CDR Repository Management Service を再起動しなければならないことがあります。

a. Unified Communications Manager Serviceability から、[Tools] > [Control Center - Network Services] をクリックします。

b. サーバ一覧から、パブリッシャを選択します。

c. CDR Services まで下にスクロールします。

d. [Cisco CDR Repository Manager] オプション ボタンを選択します。

e. [Restart] ボタンをクリックします。

アップグレード後に実行する Cisco 1040 向けの設定

ここでは、Cisco 1040 を Service Monitor 2.3 に登録するために最低限必要な手順を説明します。NAM および Unified Communications Managers を Service Monitor に追加する方法など、設定手順を完了するには、『*User Guide for Cisco Unified Service Monitor*』の設定チェック リストを参照してください。

ステップ 1　Service Monitor を起動します。「Cisco Unified Service Monitor の起動」（P.2-7）を参照してください。

ステップ 2　次のようにして、デフォルトのコンフィギュレーション ファイルを設定します。

a. [Configuration] > [Cisco 1040] > [Setup] を選択します。Setup ページが表示されます。

b. [Default Configuration to TFTP Server] フィールドを更新します。

- [Image Filename] :「SvcMonAB2_102.img」と入力します。
- [Primary Service Monitor] : IP アドレスまたは DNS 名を入力します。
- [Secondary Service Monitor] :（オプション）IP アドレスまたは DNS 名を入力します。

（注）　更新済みのバイナリ イメージ ファイルがリリースされることがあります。サポートされているバイナリ イメージ ファイルの名前については、『*Cisco Unified Service Monitor 2.3 Compliance Matrix*』を参照してください。

c. [OK] をクリックします。Service Monitor では、デフォルトのコンフィギュレーション ファイルをローカルに保存し、これを Service Monitor で設定されている TFTP サーバにコピーします。

d. Service Monitor サーバの *NMSROOT*¥ImageDir から TFTP サーバの root ロケーションに、バイナリ イメージ ファイル SvcMonAB2_102.img をコピーします（*NMSROOT* は Service Monitor がインストールされているディレクトリ。デフォルトの場所は C:¥Program Files¥CSCOpx）。

e. 新たに作成された QOVDefault.CNF ファイルが TFTP サーバに存在することを確認します。存在しない場合、これを Service Monitor イメージ ファイル ディレクトリの *NMSROOT*¥ImageDir から、TFTP サーバの root ロケーションにアップロードします。コンフィギュレーション ファイルの例については、「Cisco 1040 センサー コンフィギュレーション ファイルのサンプル」（P.2-18）を参照してください。

（注） Unified Communications Manager を TFTP サーバとして使用する場合、そのセキュリティ設定が原因で、Service Monitor は Unified Communications Manager にコンフィギュレーション ファイルをコピーできません。ステップ 2e の説明に従って、手動でコンフィギュレーション ファイルをアップロードする必要があります。コンフィギュレーション ファイルをアップロードできたら、Unified Communications Manager で TFTP サーバをリセットします。詳細については、Unified Communications Manager のマニュアルを参照してください。

ステップ 3　少し時間をおいてから、Cisco 1040 が Service Monitor に登録されていることを確認します。登録されていない場合、Cisco 1040 を電源から取り外し、再度接続することによってリセットします。

警告　Cisco 1040 センサーを取り外す前に、『*Quick Start Guide for Cisco 1040 Sensor*』の規制および安全上の情報をお読みください。

Cisco 1040 センサー コンフィギュレーション ファイルのサンプル

Service Monitor がこれらのファイルを作成するのは、ユーザ インターフェイス経由でコンフィギュレーションが編集されたとき、および Cisco 1040 がデフォルトのコンフィギュレーション ファイルを使用して登録されたときです。これらのサンプルは、センサーのコンフィギュレーション ファイルの内容が適切であることを確認できるよう提供されています。

（注） Service Monitor が正しく機能するように、Service Monitor ユーザ インターフェイスを使用してコンフィギュレーション ファイルを編集してください。TFTP サーバで Cisco 1040 センサー コンフィギュレーション ファイルを編集しないでください。

デフォルトの 1040 センサー コンフィギュレーション ファイル：QOVDefault.CNF

デフォルトのセンサー コンフィギュレーション ファイルでは、ID の A000 がプレースホルダで、Receiver には IP アドレスまたは DNS 名が 指定されます。LastUpdated で示されるデータは、前回、Service Monitor ユーザ インターフェイス経由でデフォルトのコンフィギュレーション ファイルが更新された時刻です。

```
Receiver=10.92.99.22;;
ID=A000
Image=SvcMonAB2_102.img
LastUpdated=11_16_2010-6_59_46.78
CDPGlobalRunState=true
SyslogPort=UDP:5666
SkinnyPort=TCP:2000
```

MAC 固有の 1040 センサー コンフィギュレーション ファイル：QOV001120FFCF18.CNF

MAC 固有のコンフィギュレーション ファイルでは、デフォルト ID の A000 の代わりにセンサーの MAC アドレスが使用されます。レシーバには DNS 名が指定されていますが、IP アドレスが表示されることもあります。LastUpdated で示されるデータは、前回、コンフィギュレーション ファイルが更新された時刻です。この更新は、センサーが Service Monitor に登録されたとき、または、ユーザが Service Monitor ユーザ インターフェイス経由でコンフィギュレーション ファイルを編集したとき生じます。

```
Receiver=qovr-weekly;;
ID=001120FFCF18
Image=SvcMonAB2_102.img
LastUpdated=11_13_2010-4_3_57.578
CDPGlobalRunState=true
SyslogPort=UDP:5666
SkinnyPort=TCP:2000
```

Service Monitor のアンインストールおよび再インストール

ここでは、次の内容について説明します。

Service Monitor のアンインストール

注意　システムから Service Monitor を削除するには、Cisco Unified Service Monitor アンインストール プログラムを使用する必要があります。ファイルやプログラムを手動で削除しようとすると、システムに重大な悪影響が生じるおそれがあります。

以下の手順を使用して、Service Monitor をアンインストールします。

ステップ 1　Service Monitor がインストールされているシステムにローカル管理者としてログインし、[Start] > [All Programs] > [Cisco Unified Service Monitor] > [Uninstall Cisco Unified Service Monitor] を選択し、アンインストール プログラムを起動します。

（注）　WMI サービスが実行中の場合、アンインストール続行のために WMI サービスを停止し、アンインストール完了後に WMI サービスを再起動することを伝えるメッセージが表示されます。続行するには [Yes] をクリックします。

[Uninstallation] ウィンドウが表示され、アンインストールされるコンポーネントの一覧が示されます。

ステップ 2　すべてのチェック ボックスをオンにします。[Next] をクリックします。[Setup] ウィンドウが表示され、アンインストールを選択したコンポーネントが示されます。

ステップ 3　[Next] をクリックします。アンインストールの進行状況を示すメッセージが表示されます。[Uninstallation Complete] ダイアログ ボックスが表示されます。アンインストールを完了するには、サーバを再起動する必要があります （もう一つのオプション ボタンを選択すると、後でサーバを再起動できます）。

ステップ 4　[Finish] をクリックし、システムを再起動します。

ステップ 5　*NMSROOT* ディレクトリに残っているファイルがあれば削除します。*NMSROOT* は Service Monitor がインストールされていたディレクトリで、デフォルトの場所は C:¥Program Files¥CSCOpx です。

Service Monitor の再インストール

（注） Operations Manager がインストールされているシステムで Service Monitor を再インストールするには、Operations Manager と Service Monitor の両方を再インストールする必要があります。『*Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor)*』を参照してください。

Service Monitor を再インストールしても、既存のデータベースは保持されます。ただし、再インストールでは、システムに新しいファイルをコピーおよびインストールする前に、バックアップは実行されません。バックアップを実行するには、「Service Monitor ファイルおよびデータベースのバックアップ」（P.2-9）を参照してください。

再インストール中に設定を求められるパスワードについては、「インストール、再インストール、アップグレードのためのユーザ入力」（P.A-1）を参照してください。必ず「パスワード変更後に起こりうる問題の修正」（P.A-7）をお読みください。

以下の手順は、Service Monitor 2.3 がすでにインストールされているシステムに Service Monitor 2.3 をインストールするために使用します。

ステップ 1　Service Monitor を再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、次のいずれかを実行します。

- eDelivery システムを通じて取得した [Cisco_Unified_ServiceMonitor_2.3_with_Common_Services_3.2.exe] をクリックします。
- CD-ROM ドライブに Service Monitor CD を挿入します。

（注） eDelivery システムを利用できるかどうかは、発注方法によって異なります。詳細については、「PAK の入手」（P.B-4）を参照してください。

ステップ 2　メッセージが表示された場合は、確認してから続行します。

- WMI サービスが実行中の場合、インストール続行のために WMI サービスを停止し、インストール完了後に WMI サービスを再起動することを伝えるメッセージが表示されます。[OK] をクリックします。
- データベースのバックアップが実行されないことを伝えるメッセージが表示されます。[OK] 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 3　[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 4　[I accept the terms of the license agreement] オプション ボタンを選択し、[Next] をクリックします。

インストール プログラムによって、名前参照および DHCP が確認されます。[Setup Type] ダイアログ ボックスが表示されます。

ステップ 5　[Typica] オプション ボタンを選択し、[Next] をクリックします。[Select Applications] ウィンドウが表示されます。

ステップ 6　オプション ボタンを選択します。[Next] をクリックします。

インストール プログラムによって、依存関係とシステム要件がチェックされます。

[System Requirements] ウィンドウに要件チェックの結果が表示され、インストールの続行が可能かどうかが通知されます。次のいずれかの状態が発生する場合があります。

- ディスク空き容量が不足している場合、インストール プログラムによりエラー メッセージが表示され、処理が停止します。
- システムのメモリが 4 GB 未満の場合、インストールを続行できますが、次のメッセージを確認する必要があります。

```
WARNING: System memory is less than the requirement for Cisco Unified Service
Monitor system to support high call volume.
Please refer to Service Monitor documentation for more details and upgrade the
memory to at least 4GB if you have high call volume.
```

- ディスク空き容量が 73000 MB 未満の場合、インストールを続行できますが、次のメッセージを確認する必要があります。

```
Current disk space <nnnn> MB is less than Recommended disk space 73000 MB and it may
affect performance.
```

（注）　[System Requirements] ウィンドウに表示されるディスク空き容量は、Service Monitor のインストールと起動に最低限必要な容量です。推奨されるディスク空き容量（表 1-1 (P.1-2)を参照）は、Service Monitor の使用に最低限必要な容量です。

- その他の最小要件が満たされていない場合は、インストール プログラムによって対応するメッセージが表示され、インストールが続行されます。

ステップ 7　[Next] をクリックします。[Change casuser Password] ウィンドウが表示されます。

ステップ 8　パスワードを入力して確認するか、システムによりランダムにパスワードが生成されるよう [Next] をクリックします。[Summary] ウィンドウが表示され、現在の設定内容が示されます。

ステップ 9　[Install] をクリックします。

ステップ 10　[Summary] ウィンドウが表示され、現在の設定内容が示されます。

ステップ 11　[Install] をクリックします。再インストールが進行し、[Setup Complete] ウィンドウが表示されます。

ステップ 12　[Finish] をクリックします。

システムを SNMP クエリー対応に設定

Service Monitor にはシステム アプリケーション MIB が実装されています。Service Monitor がインストールされているサーバに対して SNMP クエリーを作成するのにサードパーティ製の SNMP 管理ツールを使用する場合、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、システム アプリケーション MIB 内の すべてのオブジェクト ID（OID）に対して SNMP set 操作は許可されていません。Service Monitor 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 サービスの資格情報を変更する必要があります。

Windows SNMP サービスのインストールは、Service Monitor のインストール前でも後でも実行できます。Windows SNMP サービスがインストールされているかどうかの確認には、以下の手順を使用します。

ステップ 1　Service Monitor をインストールする予定のサーバに、Windows SNMP サービスがインストールされているかどうかを確認します。それには次のようにします。

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" かどうか。"Started" の場合は、SNMP サービスが実行中です。

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、「*install SNMP service*」などのキーワードまたは句を入力します。

CHAPTER 3

Service Monitor を使用する前に

ここでは、次の内容について説明します。

セキュリティの設定

Service Monitor は Common Services を使用して設定するセキュリティに依存しています。設定するには、以下のトピックを参照してください。

詳細については、『*User Guide for CiscoWorks Common Services*』の章「Configuring the Server」の「Setting Up Security」を参照してください。

ユーザの設定（ACS および非 ACS）

Service Monitorユーザが何を表示および実行できるかは、ユーザ ロールによって決まります。Service Monitor では、ユーザ認証に次の 2 つの Common Services モードがサポートされています。

- 非 ACS：認証および認可を提供するには、サポートされているログイン モジュールを選択します。Common Services はデフォルトで CiscoWorks Local ログイン モジュールを使用して、ロールとそれらのロールに関連付けられた特権を割り当てます。詳細については、「CiscoWorks Local ログイン モジュールを使用したユーザの設定」（P.3-2）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特定し、ユーザが特定のタスクだけを実行するようにするものです。

  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、「Cisco Secure ACS によるセキュリティの設定」（P.C-1）を参照してください。

（注） Operations Manager が認証および認可に ACS モードを使用する場合に、同一システム上で Service Monitor が実行されているとき、Service Monitor も ACS モードを使用する必要があります。そうでなければ、Service Monitor ユーザはどのような権限も与えられません。

CiscoWorks Local ログイン モジュールを使用したユーザの設定

CiscoWorks Local ログイン モジュールを使用してユーザを追加し、ロールを指定するには、CiscoWorks ホームページで [Common Services] > [Server] > [Security] > [Single-Server Management] > [Local User Setup] を選択します。[Local User Setup] ページが表示されたら、[Help] ボタンをクリックし、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 のタスクとの関連付けを確認するには、Permission Report を表示します。

ステップ 1　Service Monitor ホームページの右上隅にある [CiscoWorks] リンクをクリックします。新しいウィンドウが開きます。

ステップ 2　[Common Services] > [Server] >[Reports] > [Permission Report] > [Generate Report] を選択します。新しいウィンドウが開きます。

ステップ 3　[Go to] リストから [Cisco Unified Service Monitor] を選択し、Service Monitor のタスク一覧を表示します。

ブラウザとサーバ間の SSL のイネーブル化

Service Monitor を起動すると、ログイン ページは常にセキュア モードで開かれ、クライアント ブラウザと Service Monitor サーバとの間で安全に通信できます。セキュア モードでは、ブラウザとサーバ間の転送チャネルを暗号化するのに、Secure Socket Layer（SSL）が使用されます。Service Monitor 全体でセキュア モードを使用するには、Common Services の SSL をイネーブルにします。

（注）　Service Monitor と Operations Manager がインストールされているシステムで SSL をイネーブルにすると、SSL は両方のアプリケーションに対してイネーブルにされます。

ステップ 1　[CiscoWorks] > [Common Services] > [Server] > [Security] > [Browser-Server Security Mode Setup] を選択します。[Browser-Server Security Mode Setup] ダイアログ ボックスが表示されます。

ステップ 2　[Enable] オプション ボタンを選択します。

ステップ 3　[Apply] をクリックします。

ステップ 4　Service Monitor をログアウトし、すべてのブラウザ セッションを終了します。

ステップ 5　コマンド ラインから以下のコマンドを入力して、デーモン マネージャを再起動します。

```
net stop crmdmgtd
net start crmdmgtd
```

ステップ 6　ブラウザを再起動し、以下の安全な URL を使用して、Service Monitor を再起動します。

https://<*servername*>:<*https port*>

（注）　ブラウザで「http://<*servername*>:1741」と入力した場合に SSL がイネーブルにされていると、セキュア URL に転送されます。

Service Monitor の設定

Service Monitor CDR Call Report は、システム定義データとユーザ定義ダイヤル プランに依存しています。ダイヤル プランおよびコール カテゴリを定義するには、『*User Guide for Cisco Unified Service Monitor*』の「Configuring Call Classification」を参照してください。

（注）　Service Monitor データの長期レポートのため Service Statistics Manager を使用する場合、以下のことに留意します。

- Service Statistics Manager は Service Monitor に依存してコール データを分類しています。
- Service Monitor のコール分類の設定は、Service Statistics Manager 1.3 のインストールまたはアップグレード インストールの前に実行します。

Service Monitor を設定するには、『*User Guide for Cisco Unified Service Monitor*』の付録「Configuration Checklists and Tips」を参照してください。

APPENDIX A

インストール、再インストール、アップグレードのためのユーザ入力

この付録では、Service Monitor のインストール、再インストール、およびアップグレードの際のユーザ入力に関する情報を提供します。

この付録では、次の内容について説明します。

標準インストールのユーザ入力

表 A-1 に、標準モードで初めて Service Monitor をインストールする際に入力する必要のある情報を示します。

表 A-1　　新規インストールのためのユーザ入力：標準

設定	値
インストールするアプリケーション	インストールするアプリケーションを選択します。
admin ユーザのパスワード	デフォルト値はありません。 管理ユーザのパスワードを入力します。詳細については、「パスワード情報」を参照してください。
システム アイデンティティ アカウントのパスワード	デフォルト値はありません。 システム アイデンティティ アカウントのパスワードを入力します。詳細については、「パスワード情報」を参照してください。

表 A-1　新規インストールのためのユーザ入力：標準 （続き）

設定	値
casuser のパスワード	空白のままにしておくと、パスワードがランダムに生成されます。
メール設定： • HTTPS ポート • 管理者の電子メールアドレス • SMTP サーバ名	**（注）** システムに IIS が検出された場合に、デフォルトの HTTPS ポートを再設定することで IIS と Service Monitor との間にポートの競合が発生しないよう指定したときに表示されます。それ以外の場合、[Mail Settings] はカスタム インストール中にだけ表示されます。 デフォルト値は次のとおりです。 • ポート番号 443：表示された範囲の値を入力します。 • *admin@domain.com* • *localhost 名*

表 A-2 に、標準モードでアップグレードする際に入力する必要のある情報を示します。

表 A-2　アップグレード インストールのためのユーザ入力：標準

設定	値
casuser アカウントのパスワード	空白のままにしておくと、パスワードがランダムに生成されます （「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照）。
インストールするアプリケーション	インストールするアプリケーションを選択します。

表 A-3 に、標準モードで再インストールする際に入力する必要のある情報を示します。

表 A-3　再インストールのためのユーザ入力：標準

設定	値
casuser アカウントのパスワード	空白のままにしておくと、パスワードがランダムに生成されます （「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照）。
インストールするアプリケーション	インストールするアプリケーションを選択します。

カスタム インストールのユーザ入力

表 A-4 に、カスタム モードで初めてインストールする際に入力する必要のある情報を示します。

表 A-4　新規インストールのためのユーザ入力：カスタム

設定	値
インストール先フォルダ	デフォルトの場所は、システム ドライブ:¥Program Files¥CSCOpx です。 特定の場所にインストールする場合は、別の場所を選択します。 インストール先のフォルダには、短いパスを指定することをお勧めします。
インストールするアプリケーション	インストールするアプリケーションを選択します。
admin および *guest* ユーザのパスワード（必須）	デフォルト値はありません。admin ユーザと guest ユーザのパスワードを入力します。詳細については、「パスワード情報」を参照してください。
システム アイデンティティ アカウントのパスワード（必須）	デフォルト値はありません。 システム アイデンティティ アカウントのパスワードを入力します。詳細については、「パスワード情報」を参照してください。
casuser ユーザのパスワード	空白のままにしておくと、パスワードがランダムに生成されます。
データベースのパスワード （必須）	データベースのパスワードを入力します。詳細については、「パスワード情報」を参照してください。
メール設定：（必須） • HTTPS ポート • 管理者の電子メールアドレス • SMTP サーバ名	デフォルト値は次のとおりです。 • *443*：サーバに IIS がインストールされている場合、表示された範囲のポート番号を入力します。 • *admin@domain.com* • *localhost 名*
自己署名証明書のデータ：（必須） • 国番号 • 州 • 都市 • 組織名 • 組織ユニット名 • ホスト名 • 電子メール アドレス	デフォルトでは、自己署名証明書は Windows が登録されている組織およびホスト名を使用して生成されます。 ホスト名を入力する必要があります。それ以外のフィールドは、空白のままにしてかまいません。 **（注）** Common Services では、セキュリティ証明書を作成して、クライアント ブラウザと管理サーバとの間の SSL 通信をイネーブルにできます。自己署名証明書は、作成日から 5 年間有効です。証明書が期限切れになると、ブラウザには、Common Services をインストールしてあるサーバから再度証明書をインストールするよう求めるメッセージが表示されます。標準モードでは、この証明書は自動的に生成されます。

表 A-5 に、カスタム モードでアップグレードする際に入力する必要のある情報を示します。

（注）　ネットワークに Service Statistics Manager がインストールされている場合に、次のいずれかを変更するとき

- admin ユーザのパスワード
- インストール場所（Service Monitor がインストールされているディレクトリ）

Service Statistics Manager は Service Monitor からのデータ収集を中止します。データ収集を再度イネーブルにするには、『*Release Notes for Cisco Unified Service Statistics Manager 1.3*』に記載の手順を実行します。

表 A-5　アップグレード インストールのためのユーザ入力：カスタム

設定	値
インストールするアプリケーション	インストールするアプリケーションを選択します。
admin および *guest* ユーザのパスワード （オプション）	admin ユーザおよび guest ユーザのパスワードを変更できます。既存のパスワードを維持するには、空白のままにしておきます（「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照）。
システム アイデンティティ アカウントのパスワード（必須）	デフォルト値はありません。 システム アイデンティティ アカウントのパスワードを入力します。詳細については、「パスワード情報」を参照してください。
casuser ユーザのパスワード （オプション）	パスワードを入力しない場合、セットアップ プログラムによりパスワードがランダムに生成されます （「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照）。
データベースのパスワード（オプション）	既存のパスワードを使用するには、空白のままにしておきます。

表 A-5　アップグレード インストールのためのユーザ入力：カスタム （続き）

設定	値
メール設定： • HTTPS ポート • 管理者の電子メールアドレス • SMTP サーバ名 （オプション）	既存の情報を維持できます。
自己署名証明書のデータ： （必須） • 国番号 • 州 • 都市 • マニュアルの構成 • 組織ユニット名 • 電子メール アドレス	自己署名証明書の情報は変更できます。デフォルトでは、インストール プログラムは既存の自己署名証明書の情報を使用します。 新しい証明書を生成する場合、[Keep Existing Certificate] チェック ボックスをオフにし、国番号、州、都市、会社、組織、および HTTPS ホスト名を入力します。 ホスト名を入力する必要があります。それ以外のフィールドは、空白のままにしてかまいません。 **（注）** Common Services では、セキュリティ証明書を作成して、クライアント ブラウザと管理サーバとの間の SSL 通信をイネーブルにできます。自己署名証明書は、作成日から 5 年間有効です。証明書が期限切れになると、ブラウザには、Common Services をインストールしてあるサーバから再度証明書をインストールするよう求めるメッセージが表示されます。標準モードでは、この証明書は自動的に生成されます。

表 A-6 に、カスタム モードで再インストールする際に入力する必要のある情報を示します。

（注） Service Statistics Manager がインストールされている場合に、次のいずれかを変更するとき

- admin ユーザのパスワード
- インストール場所（Service Monitor がインストールされているディレクトリ）

Service Statistics Manager は Service Monitor からのデータ収集を中止します。データ収集を再度イネーブルにするには、『*Release Notes for Cisco Unified Service Statistics Manager 1.3*』に記載の手順を実行します。

表 A-6　再インストールのためのユーザ入力：カスタム

設定	値
インストール先フォルダ	デフォルトの場所は、*システム ドライブ*:¥Program Files¥CSCOpx です。 インストール先のフォルダには、短いパスを指定することをお勧めします。
admin および *guest* ユーザのパスワード （オプション）	admin ユーザおよび guest ユーザのパスワードを変更できます。既存のパスワードを維持するには、空白のままにしておきます （admin ユーザのパスワードを変更する場合は、「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照してください）。

表 A-6　再インストールのためのユーザ入力：カスタム （続き）

設定	値
システム アイデンティティ アカウントのパスワード（必須）	システム アイデンティティ アカウントのパスワードを変更できます。既存のパスワードを維持するには、空白のままにしておきます。
casuser ユーザのパスワード （オプション）	パスワードを入力しない場合、セットアップ プログラムによりパスワードがランダムに生成されます （「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照）。
データベースのパスワード （オプション）	既存のパスワードを維持するには、空白のままにしておきます。
メール設定： • HTTPS ポート • 管理者の電子メールアドレス • SMTP サーバ名 （オプション）	既存の情報を維持できます。
自己署名証明書のデータ：（必須） • 国番号 • 州 • 都市 • 組織名 • 組織ユニット名 • ホスト名 • 電子メール アドレス	デフォルトでは、自己署名証明書は Windows が登録されている組織およびホスト名を使用して生成されます。 ホスト名を入力する必要があります。それ以外のフィールドは、空白のままにしてかまいません。 （注）　Common Services では、セキュリティ証明書を作成して、クライアント ブラウザと管理サーバとの間の SSL 通信をイネーブルにできます。自己署名証明書は、作成日から 5 年間有効です。証明書が期限切れになると、ブラウザには、Common Services をインストールしてあるサーバから再度証明書をインストールするよう求めるメッセージが表示されます。標準モードでは、この証明書は自動的に生成されます。

パスワード情報

ここでは、インストール中のパスワードの使用に関する情報を提供します。

以下の内容について説明します。

新規インストールのパスワードに関するルール

新規インストールには、以下のルールが適用されます。

- 標準モードでは、admin、casuser、システム アイデンティティ アカウントのパスワードが必須です。guest およびデータベースのパスワードは、インストール プログラムによりランダムに生成されます。
- カスタム モードでは、admin、guest、システム アイデンティティ アカウント、およびデータベースのパスワードが必須です。casuser パスワードは、入力するか、またはインストール プログラムによりランダムに生成されるようにできます。

パスワード変更後に起こりうる問題の修正

アップグレードおよび再インストールの際に、admin ユーザおよび casuser アカウントのパスワードを変更できます。表 A-7 に、起こりうる問題とその対処法を示します。

表 A-7　起こりうる問題

変更したパスワード	起こりうる問題	対処方法：
admin	Service Statistics Manager は、Operations Manager および Service Monitor と接続できなくなる。	ネットワークに Service Statistics Manager がインストールされている場合、『*Release Notes for Cisco Unified Service Statistics Manager 1.3*』の手順を実行して、接続を再度確立します。
casuser	Windows 認証が構成されている Unified Communications Manager version 4.x システムにアクセスする場合に、Service Monitor 資格情報が認められない。	Service Monitor サーバの casuser パスワードは、Unified Communications サーバの casuser パスワードと一致していなければなりません。Unified Communications Manager がインストールされている Windows サーバにログインし、casuser パスワードを更新します。 **（注）** Service Monitor サーバの casuser パスワードがわからない場合は、「casuser パスワードの変更」を参照してください。

アップグレード インストールのパスワードに関するルール

アップグレード インストールの際に、casuser パスワードが要求されます。それ以外のパスワードは維持されます。

再インストールのパスワードに関するルール

再インストールには次のルールが適用されます。

- 標準モードでは、インストール プログラムは、admin、guest、およびデータベースのパスワードを維持します。casuser パスワードは、入力するか、またはインストール プログラムによりランダムに生成されるようにできます （「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照）。
- カスタム モードでは、新しい admin、guest、システム アイデンティティ アカウント、およびデータベースのパスワードを入力するか、または既存のパスワードを維持できます。casuser パスワードは、入力するか、またはインストール プログラムによりランダムに生成されるようにできます （「パスワード変更後に起こりうる問題の修正」（P.A-7）を参照）。

パスワードの説明

パスワードの種類は、次のとおりです。

- 「Common Services 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」
- 「Common Services guest パスワード」
- 「Common Services のデータベース パスワード」

Common Services admin パスワード

admin ユーザのパスワードを入力する際は、5 文字以上含まれるようにします。

admin ユーザ アカウントはデフォルトの管理者です。初回インストール後に Service Monitor にログインするには、admin ユーザ名とパスワードを使用する必要があります （パスワードはメモしておいてください）。

インストールでは標準モードでもカスタム モードでも、このパスワードの入力が求められます。

システム アイデンティティ アカウント パスワード

システム アイデンティティ アカウント パスワードを入力する際は、5 文字以上使用します。

インストールでは標準モードでもカスタム モードでも、このパスワードの入力が求められます。

システム アイデンティティ アカウントは、マルチサーバ環境で使用されます。複数サーバ間の通信は、資格情報および共有秘密鍵により実現される「trust」モデルによって可能になります。詳細については、『*User Guide for CiscoWorks Common Services*』を参照してください。

（注） Cisco Secure ACS（別のサーバにインストール済み）でセキュリティを設定し、マスター モードおよびスレーブ モードで DCR を設定するには、システム アイデンティティ アカウントが必要です（Operations Manager では DCR がサポートされていますが、Service Monitor ではサポートされていません）。

Common Services guest パスワード

Common Services guest アカウントのパスワードを入力する際は、5 文字以上使用します。

このパスワードを使用し、Common Services サーバに guest ユーザとして ログインします。カスタム モードのインストールでは、このパスワードの入力が求められます。標準モードでは、このパスワードはランダムに生成されます。

Common Services のデータベース パスワード

データベースのパスワードを入力する際は、

- 5 文字以上使用し、15 文字を上限とします。
- 先頭に数字は使用しません。
- 文字間に空白が含まれないようにします。
- 特殊文字は使用しません。

パスワードの変更

ここでは、ユーティリティ（または、可能な場合は Common Services のユーザ インターフェイス）を使用して admin ユーザと casuser アカウントのパスワードを変更する方法を説明します。

- 「Common Services admin パスワードの変更」
- 「casuser パスワードの変更」

Common Services admin パスワードの変更

Common Services admin パスワードを変更します。admin ユーザのパスワードを変更する前に、以下の認識が必要です。

（注） admin パスワードを変更する場合に、ネットワークに Service Statistics Manager がインストールされているとき、Service Statistics Manager は Operations Manager および Service Monitor と接続できなくなります。接続を再度確立するには、『*Release Notes for Cisco Unified Service Statistics Manager 1.3*』の手順を実行します。

Common Services admin パスワードを変更する場合は、Common Services のユーザ パスワード リカバリ ユーティリティまたは GUI から変更できます。

- 「ユーザ パスワード リカバリ ユーティリティを使用した admin パスワードの変更」
- 「Common Services からの admin パスワードの変更」

ユーザ パスワード リカバリ ユーティリティを使用した admin パスワードの変更

ステップ 1　シェル プロンプトで次のコマンドを入力して、デーモン マネージャを停止します。

```
net stop crmdmgtd
```

ステップ 2　*NMSROOT*¥bin ディレクトリに移動し、次のように入力します。

NMSROOT\bin\resetpasswd *username*

NMSROOT は、Service Monitor をインストールしたディレクトリです。

次のメッセージが表示されます。

```
Enter new password for username:
```

ステップ 3　*username* に対するパスワードを入力します。

ステップ 4　コマンド プロンプトで次のように入力して、デーモン マネージャを起動します。

```
net start crmdmgtd
```

Common Services からの admin パスワードの変更

ステップ 1　ユーザ名 admin を使用してログインします。

ステップ 2　Service Monitor のホームページの右上隅の [CiscoWorks] リンクを選択します。

ステップ 3　CiscoWorks ホームページで、[Common Services] > [Server] > [Security] > [Single-Server Management] > [Local User Setup] を選択します。

[Local User Setup] ページが表示されます。

ステップ 4　[Modify My Profile] をクリックします。

[My Profile] ポップアップ ウィンドウが表示されます。

ステップ 5　[Password] フィールドにパスワードを入力します。

ステップ 6　[Verify] フィールドにパスワードを再入力します。

ステップ 7　[E-mail] フィールドに電子メール ID を入力します。

ステップ 8　[OK] をクリックします。

casuser パスワードの変更

注意　casuser パスワードを変更すると、Windows 認証が構成されている Unified Communications Manager version 4.x システムにアクセスする場合に、Service Monitor 資格情報が認められない場合があります。入力する新しい casuser パスワードと整合するように casuser パスワードを更新するには、Unified Communications Manager がインストールされている Windows サーバにログインしておく必要があります。

ステップ 1　コマンド プロンプトで、次のように入力します。

NMSROOT\setup\support\resetCasuser.exe

次の 3 つのオプションが表示されます。

1. Randomly generate the password
2. Enter the password
3. Exit

ステップ 2　「**2**」と入力し、Enter を押します。

メッセージが表示され、パスワードの入力が求められます。

ステップ 3　パスワードを確認します。

Service Monitor サーバにローカル ユーザ ポリシーが設定されている場合に、パスワード ポリシーに一致しないパスワードを入力すると、アプリケーションが終了し、エラー メッセージが表示されます。詳細については、『*User Guide for CiscoWorks Common Services*』の「Setting up Local User Policy」を参照してください。

APPENDIX B

ライセンス

この付録では、Cisco Unified Service Monitor（Service Monitor）のライセンスについて説明します。次の事項について説明します。

ライセンスの概要

Service Monitor は、ソフトウェアベースの製品登録とライセンス キー技術を特長としています。ライセンスの付与によって、Service Monitor のライセンス取得済みコピーを所有できます。

（注）

- ライセンスの付与時にはノードロック技術が使用されます。ライセンス ファイルを使用できるのは、ユーザが入力した MAC アドレスを持つサーバだけです。
- VMware で Service Monitor のライセンス付与、インストール、および実行を行うには、仮想マシンに固定アドレスを設定する必要があります。

Service Monitor にライセンスが付与されているかどうかを確認するには、「ライセンス ステータスの確認」（P.B-2）を参照してください。まだライセンスを取得していないか、ライセンスのアップグレードを希望する場合は、「ライセンス付与のシナリオ」（P.B-3）を参照してください。製品の評価中に表示されるメッセージについては、「ライセンスに関するメッセージ」（P.B-3）を参照してください。

ライセンス ステータスの確認

ステップ 1　Service Monitor のホームページの右上隅の [CiscoWorks] リンクを選択します。CiscoWorks のホームページ ウィンドウが表示されます。

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

カラム	説明
[Name]	製品の省略名：Service Monitor の場合は SM です。
[Version]	製品のバージョン：*A.b.c*。ここで、*A* はメジャー バージョン番号、*b* はマイナー バージョン番号、*c* はサービス パック番号です。たとえば、SM 2.0.0 は、サービス パックなしのバージョン 2.0 を示します。 Service Monitor 2.0 ライセンスでは、Service Monitor 2.3 もサポートされます。
[Size]	限度：Service Monitor でのサポートが許諾されている電話台数の最大値。 **（注）** ライセンス付与の手順では、結果として電話台数がこの最大値を超えることになっても、有効なライセンスをすべてインストールできます。ある Service Monitor サーバから別のサーバにライセンスを移動するには、サービス リクエストを実行する必要があります。詳細については、「マニュアルの入手方法およびテクニカル サポート」を参照してください。
[Status]	次のいずれか • Purchased：製品は登録済みで、ライセンスが付与されています。 • Evaluation：このライセンスは有効期限日付で期限が切れ、Service Monitor は実行を停止します。
[Expiration Date]	Service Monitor が実行を停止する日付。評価ライセンスに適用されます。評価期間は 90 日です。

（注） インストールされているソフトウェア バージョンを表示するには、Service Monitor のホームページの右上隅にある [About] リンクを選択します。

ライセンス付与のシナリオ

表 B-1 では、ライセンス付与され登録されている Service Monitor のコピーを所有していない場合、または、サポートされる電話台数を増やしたい場合、さまざまなシナリオでどのように対処するかを説明します。

表 B-1　ライセンスの取得および登録方法

シナリオ	対処方法
購入ライセンスを使用したインストール	1. インストールの前に、ライセンス ファイルを取得します。*「ライセンス プロセス」（P.B-4）*を参照してください。 **（注）** ライセンス ファイルなしで Service Monitor をインストールし、インストール後に、ライセンスをアップグレードできます。「Service Monitor でのライセンス ファイルの登録」（P.B-5）を参照してください。 2. インストール中に [License File Location] を選択し、ライセンス ファイルの場所を指定します。
評価ライセンスを使用したインストール **（注）** 評価ライセンスでモニタできる電話台数は 1,000 台までです。	インストール中に [Evaluation Only] を選択します。評価バージョンは 90 日間有効です。期限切れになると購入を求められます。 インストール後に購入バージョンにアップグレードするには、Service Monitor ソフトウェア バージョンの PAK およびライセンス ファイルを取得します。ライセンス付与の手順については、「ライセンス プロセス」（P.B-4）を参照してください。
ライセンスのアップグレード：以下のいずれかを実行します。 • 評価ライセンスから購入ライセンスにアップグレードする • サポートされる電話機の台数を増やすために、追加ライセンスをインストールする	「ライセンス プロセス」（P.B-4）を参照してください。
Service Monitor を別のサーバに移動する	Cisco TAC にお問い合わせください。詳細については、「マニュアルの入手方法およびテクニカル サポート」を参照してください。

ライセンスに関するメッセージ

Service Monitor の評価バージョンをインストールした場合、90 日の評価期間経過後も製品を使用するには、Cisco.com からライセンス ファイルを取得する必要があります。詳細については、「ライセンス プロセス」（P.B-4）を参照してください。

評価ライセンスの有効期間の間は、次のメッセージが表示されます。

```
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 Service Monitor にアクセスしようとすると警告メッセージ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い場合、すべての Service Monitor プロセスは実行されますが、Service Monitor 機能へのアクセスは禁止されます。

ライセンス プロセス

Service Monitor ライセンス ファイルには、定められた台数の電話サポートが含まれています。サポートされる電話台数を増やし、単一の Service Monitor で最大台数までの電話をモニタするには、追加ライセンスを購入します。購入した増分ライセンスごとに PAK が提供されるので、その PAK を使用してライセンス ファイルを入手する必要があります。

このプロセスは、次のような新規インストールとライセンスのアップグレードに適用されます。

1. Product Authorization Key（PAK）の入手：PAK は Cisco.com で Service Monitor を登録したり、後から購入することのある Service Monitor の追加の電話サポートを登録したりするために使用されます。PAK にはリソース制限が含まれます。「PAK の入手」（P.B-4）を参照してください。
2. ライセンス ファイルの入手：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。「ライセンス ファイルの入手」（P.B-4）を参照してください。
3. Service Monitor をインストールするサーバに、ライセンス ファイルをコピーします。Service Monitor をすでにインストールしていて、ライセンス ファイルをアップグレードしている場合は、Service Monitor でライセンス ファイルを登録する必要があります。「Service Monitor でのライセンス ファイルの登録」（P.B-5）を参照してください。

PAK の入手

PAK はソフトウェア権利証明書に記載されています。ソフトウェア権利証明書は次のいずれかの場合に提供されます。

- 発注書にハードウェアが含まれる場合、ソフトウェア権利証明書はパッケージに含まれています。
- 発注書にハードウェアが含まれない場合、eDelivery システムを通じてソフトウェア権利証明書を取得できます。eDelivery については、http://www.cisco.com/web/partners/tools/edelivery.html を参照してください。

ライセンス ファイルの入手

（注）　VMware サーバに Service Monitor をインストールする場合、ライセンス ファイルの取得には固定 MAC アドレスを入力する必要があります。仮想マシンに動的 MAC アドレスが設定されていると、Service Monitor は機能しません。詳細については、「VMware に関するガイドライン」（P.1-4）を参照してください。

ステップ 1　PAK と、Service Monitor がインストールされているシステムの MAC アドレスを Cisco.com（http://www.cisco.com/go/license）に登録します。このとき、ログインするように求められます。ログインするには、Cisco.com の登録ユーザである必要があります。

（注）　ライセンス処理ではノードロック テクノロジーが使用されるため、MAC アドレスは必須です。ライセンス ファイルを使用できるのは、ユーザが入力した MAC アドレスを持つサーバだけです。

ライセンス ファイルは電子メールで送信されます。ライセンス ファイルを入手したら、ライセンスを Service Monitor サーバに登録します。

Service Monitor でのライセンス ファイルの登録

注意　この手順ではライセンスを登録します。結果として、ライセンス サイズが単一サーバ上の Service Monitor でサポートされる電話台数の最大値を超えることがあります。Service Monitor 内の電話台数が最大値を超えると、追加の電話機からはデータの収集も分析も行われません。

ステップ 1　ライセンス ファイルを Service Monitor サーバにコピーし、ユーザ名 casuser または ユーザ グループ casuser に読み取り権限が付与されたディレクトリに保存します。

（注）　ライセンス ファイルを含むフォルダを Service Monitor サーバにコピーする場合は、そのフォルダおよびライセンス ファイルの読み取り権限を casuser に付与してください。

ステップ 2　次のようにしてライセンスをインストールします。

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

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

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

d. ライセンス ファイルを参照して選択します。

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

2 つ以上のライセンスを購入した場合は、ステップ 2 を繰り返して各ライセンスをインストールしてください。

エラーが発生した場合は、ライセンス ファイルについて以下を確認します。

- ユーザ名 *casuser* または ユーザ グループ *casusers* に読み取り権限が付与されたディレクトリに存在しているかどうか。
- HOSTID=<*MAC*> に正しい MAC アドレスが指定されているかどうか（ライセンス ファイルの内容を確認するには、テキスト エディタを使用します）。HOSTID の値が正しくない場合は、サービス リクエストを実行する必要があります。「マニュアルの入手方法およびテクニカル サポート」を参照してください。

表 B-2　ライセンス登録結果

登録されたライセンス	[Licensing Information] ページの予期される結果
評価ライセンスからのアップグレード	[Status] 列のエントリが [Evaluation] から [Purchased] に変わる。
サポートされる電話台数の増加	[Size] 列のエントリがライセンス サイズに応じて増える。

APPENDIX C

Cisco Secure ACS によるセキュリティの設定

認証と認可に Cisco Secure ACS を使用するように Service Monitor を設定するには、次のトピックを順番に学習してください。

Cisco Secure ACS のサポート

Service Monitor は、認証と認可の ACS モードをサポートします。このモードを使用するには、ネットワーク内の Service Monitor がインストールされているものとは異なるサーバに、Cisco Secure Access Control Server（ACS）をインストールしている必要があります。サポートされるソフトウェア バージョンについては、「表 1-1 サーバの最小限の要件」（P.1-2）を参照してください。

Service Monitor 統合の注意事項

Service Monitor（および Common Services）は、共有プロファイル コンポーネントとして Cisco Secure ACS と統合されます。同一アプリケーション（Service Monitor など）の複数インスタンスは、認証と認可に同じ Cisco Secure ACS サーバを使用できます。

Cisco Unified Service Monitor（および CiscoWorks Common Services）を Cisco Secure ACS に登録すると、データ ソース資格情報を Service Monitor に追加するなどのアプリケーションタスク、およびアプリケーションのためのネットワーク 管理者などのユーザ ロールが、Cisco Secure ACS にインポートされます。

タスクとロールのインポートは、Cisco Secure ACS にアプリケーションのインスタンスを 1 つ登録するだけで済みます。再度アプリケーションを登録すると、カスタム ロールの作成などでロール設定に加えたすべての変更が失われます。

（注） Service Monitor を Cisco Secure ACS と統合しても、特定のデバイスの選択的除外はできません。例として、次のタスクを含むユーザ ロールで可能なことを示します。

- データ ソース資格情報：追加、編集および検証 ── 任意の NAM または任意の Unified Communications Manager について、Service Monitor で資格情報の追加、編集、および検証が可能です。
- Cisco 1040：詳細表示 - 任意の Cisco 1040 について、Service Monitor から詳細を表示できます。

CiscoWorks Local ログイン モジュール認証ロール

CiscoWorks ログイン モジュールを使用すると、ネイティブ メカニズムである CiscoWorks Local ログイン モジュール以外の認証ソースを使用できます。この目的で、Cisco Secure ACS サーバを使用できます。

ユーザ認証後に、ユーザ ロールで認可が制御されます。ロールとは、ユーザが実行特権を持つ一連のタスクのことです。デフォルトで、CiscoWorks Local ログイン モジュール認可方式には 5 つのロールがあります。6 つ目のロールである Super Admin は、ACS モードで利用できますが、Cisco Secure ACS システムだけに表示されます。表 C-1 に、特権が小さなロールから大きなロールへと並べた一覧を示します。

表 C-1　Common Services ユーザ ロールおよび特権

ロール	説明
非 ACS モード - CiscoWorks Local ログイン モジュール	
Help Desk	このロールのユーザには、Service Monitor および Common Services 内の情報の一部を表示する特権があります。 例：レポートの生成と表示および Cisco 1040 の詳細の表示 （変更はできません）。
Approver	このロールのユーザは、一切特権を持っていません （Service Monitor は、このユーザ ロールに一切タスクを割り当てません）。
Network Operator	このロールのユーザには、Service Monitor タスクのすべてと Common Services タスクの一部を実行する特権があります。 例：Service Monitor のセットアップ、データ ソース資格情報の追加、変更、検証。
Network Administrator	このロールのユーザには、Service Monitor タスクすべてと Common Services タスクのいくつかを実行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。
System Administrator	このロールのユーザには、すべてのシステム管理タスクを実行する特権があります。 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。

表 C-1　Common Services ユーザ ロールおよび特権 （続き）

ロール	説明
ACS モード	
Super Admin	このロールのユーザには、AAA モードが ACS に設定され、かつ認証に Cisco Secure ACS が使用されている場合に、すべてのタスクを実行する特権があります。 Common Services でローカル ユーザ セットアップを実行する場合は、Super Admin ロールは表示されません。Cisco Secure ACS にログインし、かつ CiscoWorks ログイン モジュールが ACS に設定されている場合にだけ、このロールをユーザに割り当てることができます。

Service Monitor と Common Services に定義されたタスク、およびこれらのタスク実行する特権のあるロールについては、Common Services の Permission Report を参照してください（Service Monitor ホームページの右上にある [CiscoWorks] リンクをクリックし、[Common Services] > [Server] > [Reports] > [Permission Report] > [Generate Report] を選択します）。

（注）　詳細については、『*User Guide for CiscoWorks Common Services 3.2*』を参照してください。

デフォルトの Common Services ロールを変更しないことをお勧めします。ただし、Cisco Secure ACS で Service Monitor 用の独自のロールを作成できます。

Common Services のシステム アイデンティティ ユーザの設定

Service Monitor サーバを Cisco Secure ACS と統合する前に、すべての特権を作成して Common Services のシステム アイデンティティ ユーザに割り当てていることを確認します。このトピックでは、ローカル ユーザをシステム アイデンティティ ユーザとしてセットアップする方法を説明します（Common Services の admin ユーザをシステム アイデンティティ ユーザとして使用するには、『*User Guide for CiscoWorks Common Services 3.2*』のトピック「Setting up System Identity Account」を参照してください）。

1. ローカル ユーザを作成し、すべてのロールをそのユーザに割り当てます （「CiscoWorks Local ログイン モジュールを使用したユーザの設定」（P.3-2）を参照）。

   （注）　システム アイデンティティ ユーザがすべての CiscoWorks Local ログイン モジュール ロールで構成されていないと（表 C-1 を参照）、Service Monitor および Common Services で特定のタスクを実行しようとしたときに認可に失敗します。

2. システム アイデンティティ ユーザをアップデートし、ユーザ名をステップ 1. で作成したもので置き換えます（CiscoWorks のホーム ページから [Common Services] > [Server] > [Security] > [Multi-Server Trust Management] > [System Identity Setup] の順に移動します。詳細については [Help] リンクをクリックしてください）。

詳細については、『*User Guide for CiscoWorks Common Services 3.2*』を参照してください。

Cisco Secure ACS サーバのセットアップ

Common Services の AAA モードを ACS に変更する前に、次のタスクを Cisco Secure ACS で実行します。

1. ACS 管理者を設定します。

   Cisco Secure ACS で、管理者ユーザにすべての特権を設定します。

   （注）　管理者ユーザにすべての特権を設定しないと、Service Monitor の Cisco Secure ACS への登録に失敗します。

   管理者用のユーザ名とパスワードを書き留めます。Common Services で AAA モードを ACS に変更する際にこれらの入力が必要になります。

2. Service Monitor サーバを AAA クライアントとして Cisco Secure ACS に追加します。

   Cisco Secure ACS で Service Monitor サーバを AAA クライアントとして設定し、次の操作を行います。

   - [TACACS + (CISCO IOS)] による認証を選択します。
   - 入力する共有秘密鍵を書き留めます。Common Services で AAA モードを ACS に変更する際に、Common Services への入力が必要になります。

3. システム アイデンティティ ユーザおよび Common Services ユーザを Cisco Secure ACS に追加します。

   グループを作成して、そこにユーザを追加することができます。

4. Service Monitor および Common Services アプリケーションがすでに Cisco Secure ACS に登録されているかどうかを確認します。そのためには、[Shared Profile Components] を選択し、次の項目を探します。

   - Cisco Unified Service Monitor
   - CiscoWorks Common Services

上記の各タスクを実行する方法の詳細については、Cisco.com で次のマニュアルを参照してください。

- 『*User Guide for Cisco Secure Access Control Server 4.x*』
  http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html
- 『*User Guide for CiscoWorks Common Services 3.2*』
  http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html

Common Services での AAA モードから ACS への変更

この手順を実行する前に、「Common Services のシステム アイデンティティ ユーザの設定」（P.C-3）および「Cisco Secure ACS サーバのセットアップ」（P.C-4）にあるタスクを完了してください。

ステップ 1　[CiscoWorks] > [Common Services] > [Server] > [Security] > [AAA Mode Setup] の順に選択します。

ステップ 2　[OK] をクリックします。[AAA Mode Setup] ページが表示されます。

ステップ 3　[Select a Type] の隣で、[ACS] オプション ボタンを選択します。ページが最新の情報に更新され、適切なオプションが表示されます。

ステップ 4　[Server Details] の下で、Cisco Secure ACS サーバの IP アドレスを入力し、ポートを入力します。

ステップ 5　[Login] で、次を入力します。

- ACS Admin Name - ステップ 1. で作成した管理者の名前を入力します（「Cisco Secure ACS サーバのセットアップ」（P.C-4）を参照してください）。
- ACS Admin Password - ステップ 1. で作成した管理者のパスワードを入力します（「Cisco Secure ACS サーバのセットアップ」（P.C-4）を参照してください）。
- ステップ 2. で Service Monitor サーバを AAA クライアントとして Cisco Secure ACS に追加したときに入力した秘密鍵を入力します（「Cisco Secure ACS サーバのセットアップ」（P.C-4）を参照してください）。

ステップ 6　[Register all installed applications with ACS] を選択するかどうかを決定します。

（注） Service Monitor が ACS に登録されている場合に Service Monitor を再度登録すると、Service Monitor 用に Cisco Secure ACS で以前に設定したすべてのカスタム ルールが失われます。これは、Common Services についても同様です （アプリケーションを選択して登録するには、「コマンドラインでの Cisco Secure ACS へのアプリケーションの登録」（P.C-5）を参照してください）。

ステップ 7　[Current ACS Administrative Access Protocol] の下で、適切なオプション ボタン（[HTTP] または [HTTPS]）を選択します。

ステップ 8　[Apply] をクリックし、モード変更を完了します。ACS の検証ステータス メッセージが表示されます。次のいずれかの操作を実行します。

- [OK] をクリック - Registers Service Monitor および Common Services のタスクとユーザを ACS に登録します。Service Monitor および Common Services の既存のカスタム ロールはすべて上書きされます。
- [Cancel] をクリック - ACS に登録しません。

ステップ 9　変更を反映するために、デーモン マネージャを再起動します。コマンドラインから、次のコマンドを入力します。

```
net stop crmdmgtd
net start crmdmgtd
```

コマンドラインでの Cisco Secure ACS へのアプリケーションの登録

<NMS ルート>¥bin¥AcsRegCli.pl スクリプトを使用して、Cisco Secure ACS にアプリケーションを登録できます。

（注） NMS ルートとは、Service Monitor がインストールされているディレクトリのことです。デフォルト ディレクトリを選択した場合は、C:¥PROGRA~1¥CSCOpx になります。

CLI からこのスクリプトを実行する場合に、次のパラメータを使用できます。

`AcsRegCli.pl -register <`*アプリケーション名*`>`

アプリケーション名は、次のいずれかと置き換えます。

- qovr - Service Monitor だけを登録

- cmf - CiscoWorks Common Services だけを登録
- all - サーバ上のすべてのアプリケーション（Cisco Unified Service Monitor および CiscoWorks Common Services）を登録

Cisco Secure ACS でのユーザおよびユーザ グループへのロールの割り当て

Cisco Secure ACS 内のシステム アイデンティティ ユーザにすべてのロールが割り当てられていること、および Common Services ユーザまたはユーザ グループに適切な特権が割り当てられていることを確認する必要があります。

Cisco Secure ACS で、[Shared Profile Components] > [Cisco Unified Service Monitor] の順に選択します。詳細については、次のマニュアルを参照してください。

- 『*User Guide for Cisco Secure Access Control Server 4.x*』
- 『*User Guide for CiscoWorks Common Services 3.2*』または Common Services のオンライン ヘルプ。次のトピックを探してください。
  - 「Roles in ACS」
  - 「Assigning Roles to Users and User Groups in ACS」

Service Monitor および Cisco Secure ACS 設定の検証

「Cisco Secure ACS でのユーザおよびユーザ グループへのロールの割り当て」（P.C-6）から「Common Services のシステム アイデンティティ ユーザの設定」（P.C-3）までのタスクを実行した後で、設定を次のように検証します。

1. Cisco Secure ACS に定義されているユーザ名で Service Monitor にログインします。
2. タスクを試行し、Cisco Secure ACS で割り当てられたロールに基づいて実行権限を与えられたタスクだけを実行できることを確認します。

   たとえば、特権が Help Desk の場合、

   - Service Monitor で管理されている Cisco 1040 を表示できます。
   - Service Monitor の管理対象となる Cisco 1040 の追加や削除はできません。

問題が発生したときは、『*User Guide for CiscoWorks Common Services*』の「Authentication Failure in ACS Mode」を参照してください。

INDEX

け

こ

し

せ

そ

た

ち

て

と

に

は

ひ

ま

ゆ

ら

れ

ろ