



Service Monitor を使用する前に

Cisco Prime Unified Service Monitor (Service Monitor) は、Cisco Prime Unified Communications Management Suite の製品の 1 つです。この製品は、Cisco Prime Unified Communications Manager (Unified Communications Manager) クラスタおよびセンサーから Mean Opinion Score (MOS; 平均オピニオン評点) を受信して分析し、違反が発生している場合にトラップを送信します。このセンサーには、Cisco 1040 センサー (Cisco 1040) と Cisco Network Analysis Module (NAM; ネットワーク解析モジュール) があります。



(注)

- このマニュアルでは、別途記載のない限り、Cisco Unified Communications Manager に関する記述は Cisco Prime Unified CallManager も対象とするものとします。
- Service Monitor のマニュアルには、Common Services の機能およびマニュアルの参照に関する記述が含まれていることがあります。Common Services のマニュアルとオンライン ヘルプには、同じネットワーク内にインストール可能な製品である CiscoWorks LAN Management Solution とそのコンポーネントに関する記述が含まれています。Common Services のマニュアルには、LMS Portal や LMS Setup Center などの、Service Monitor には関係しない機能の記述も含まれています。

この項では次のトピックについて説明します。

- 「概要」 (P.1-1)
- 「Service Monitor のホームページ」 (P.1-6)



(注)

Service Monitor の初期設定の方法については、「設定のチェックリストおよびヒント」 (P.A-1) を参照してください。

概要

Service Monitor は、センサー (Cisco 1040 および NAM) および Unified Communications Manager クラスタから MOS を取得して分析します。Service Monitor は、センサーとクラスタの一方だけをサポートすることも、両方をサポートすることもできます。詳細については、「データの収集および分析」 (P.1-2) を参照してください。

Service Monitor は、受信したデータを分析して、MOS がしきい値を下回っている場合にトラップを送信します。Service Monitor のデフォルトのグローバルしきい値は、サポートされるコーデックごとに 1 つずつ定義されています。Service Monitor のデフォルトのグローバルしきい値は変更可能です。ま

た、これよりも優先されるしきい値グループ（センサーしきい値グループおよびクラスタしきい値グループ）を作成することもできます。詳細については、「しきい値とトラップ」(P.1-5) および「トラップ レシーバ」(P.1-6) を参照してください。

Service Monitor の診断レポートには、データ保持期間（「その他の設定項目の設定と表示」(P.3-39) を参照）内に行われたコールのデータが表示されます。CVTQ データとセンサー データのレポートを作成できます。また、24 時間または 7 日間の違反数が上位であるエンドポイントについてのレポートも作成できます。詳細については、「レポートの使用法」(P.2-1) を参照してください。

Service Monitor のデータを詳細に分析、表示、および操作するために、Cisco Prime Unified Operations Manager (Operations Manager) を Service Monitor のトラップ レシーバとして設定して使用できます。Operations Manager を使用すると、Service Monitor トラップに対応するイベントの生成や、Service Quality Alerts ダッシュボードでのイベントの表示、およびイベント履歴の保存と表示を実行できます。詳細については、『*User Guide for Cisco Prime Unified Operations Manager 8.7*』を参照してください。

データの収集および分析

Service Monitor は、次に示すソースが音声ネットワーク内にインストールされて適切に設定されている場合に、これらのソースからの MOS を受信して分析します。

- センサー：Cisco 1040 および NAM は、各 Real-Time Transport Protocol (RTP) ストリームの MOS を計算します。Service Monitor は、次の方法でデータを 60 秒間隔で受信します。
 - Cisco 1040 から送信された syslog メッセージを受信
 - NAM をポーリングしてデータを取得
- CVTQ：Unified Communications Manager は、K ファクタをサポートするエンドポイントからデータを収集します。エンドポイントの MOS の計算には、CVTQ アルゴリズムを使用します。コールの終了時に、Unified Communications Manager はデータを Call Detail Record (CDR; コール詳細レコード) と Call Management Record (CMR; コール管理レコード) に保存します。



(注) K ファクタをサポートするエンドポイントと、Service Monitor でサポートされる Unified Communications Manager のバージョンについては、『*Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix*』を参照してください。

表 1-1 は、Service Monitor によって使用されるデータ ソースの概要レベルでの比較です。関連するタスクの詳細な実行手順は、このマニュアルの各章で説明しています。

表 1-1 データ ソースの比較

比較	センサー		Unified Communications Manager	
	1040	NAM	4.3	6.x 以降 ¹
互換性の判定 詳細については、 『Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix』 を参照してください。	バイナリ イメージの ファイル名： SvcMonAB2_102.img	<ul style="list-style-type: none"> ネットワーク解析モジュール ソフトウェアのバージョン：4.x および 5.x NAM ハードウェア： NME-NAM NAM-1/NAM-2 NAM 2200 シリーズ アプライアンス 	<ul style="list-style-type: none"> Unified Communications Manager のバージョン 音声ゲートウェイまたは Cisco Unified IP Phone での CVTQ アルゴリズムのサポート 	
Service Monitor での設定	<ul style="list-style-type: none"> TFTP サーバの追加 Cisco 1040 センサー コンフィギュレーション ファイルの編集 	クレデンシャルを Service Monitor に追加		
Service Monitor の外部での設定	<ul style="list-style-type: none"> 『Quick Start Guide for Cisco 1040』を参照 コンフィギュレーション ファイルとバイナリ イメージを TFTP サーバにコピー 	<ul style="list-style-type: none"> http または https サーバと Web 管理者ユーザを NAM 上で設定 NTP サーバをネットワーク解析モジュール ソフトウェア内で設定 	Unified Communications Manager サーバ上でアカウントと権限を設定	パラメータとアプリケーション ビリング サーバを Unified Communications Manager 内で設定
データ収集：プッシュかプルか	プッシュ：Cisco 1040 が syslog メッセージを送信	プル：Service Monitor が NAM をポーリング	プル：Service Monitor Unified Communications Manager のデータベースを照会	プッシュ：Unified Communications Manager が情報をアプリケーション ビリング サーバに送信
MOS の計算	R ファクタに基づく		CVTQ アルゴリズム (Unified Communications Manager のマニュアルでは「K ファクタ」と呼ばれることもあります)	
登録か認証か	自動登録または手動登録： Cisco 1040 を Service Monitor に登録	認証：Service Monitor はクレデンシャルを使用してデータ ソースにアクセス		

表 1-1 データソースの比較 (続き)

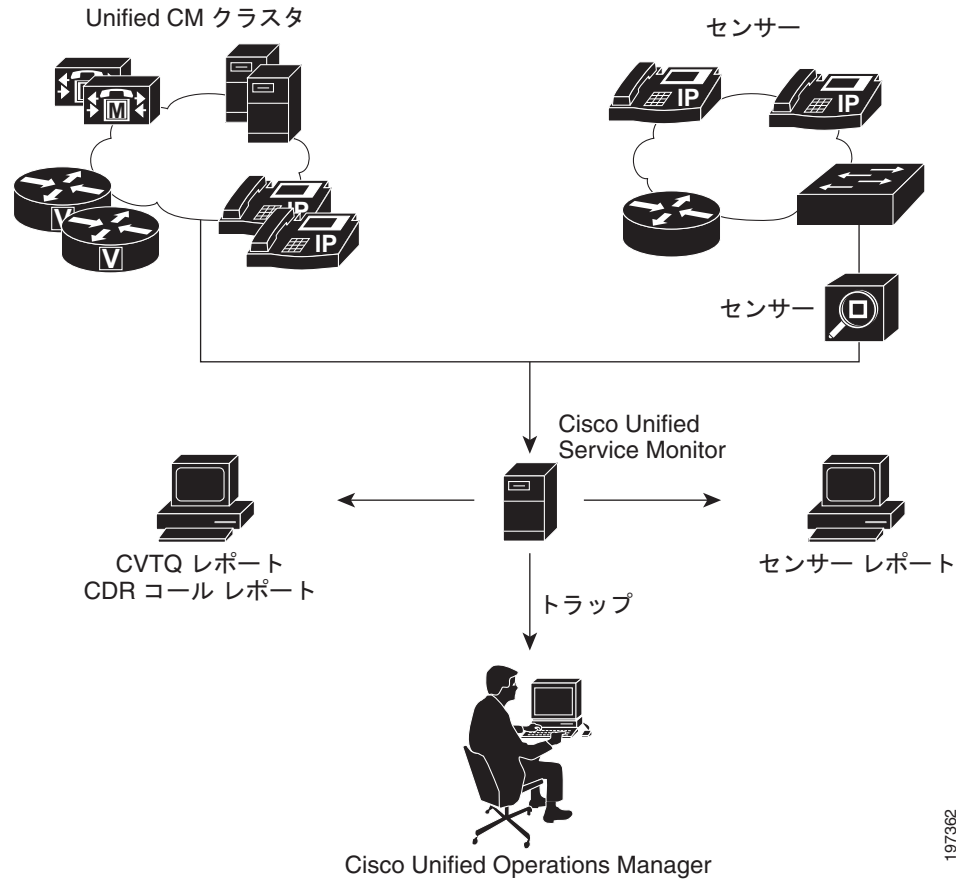
比較	センサー		Unified Communications Manager	
	1040	NAM	4.3	6.x 以降 ¹
レポート	Sensor Diagnostic レポート ([Sensor Stream Correlation] ウィンドウへのリンクあり) : 複数のセンサーからのストリームと Call Detail Record (CDR; コール詳細レコード) の相互関係を示す		<ul style="list-style-type: none"> • CVTQ Diagnostic レポート • CDR Call レポート 	
	Sensor Most-Impacted Endpoints		CVTQ Most-Impacted Endpoints	
しきい値	センサー グループ (注) Service Monitor 内で設定されたしきい値がネットワーク解析モジュール ソフトウェアに伝播されることはありません。同様に、ネットワーク解析モジュール ソフトウェア内で設定されたしきい値が Service Monitor に伝播されることはありません。		CVTQ グループ	
	(注) センサー グループまたは CVTQ が定義されていないか適用対象外の場合は、Service Monitor はグローバルしきい値を使用します。			
時刻の同期	Service Monitor から 1 時間に 1 回、時刻同期メッセージが 1040 に送信されます。	Service Monitor で使用されているのと同じ NTP サーバを使用するように NAM を設定することを強く推奨します。	Unified Communications Manager で使用されている NTP サーバを使用するように Service Monitor を設定する必要があります。	
タイミング	データのプッシュまたはプルの間隔は 60 秒です。		データはコール完了後に使用可能になります。	

1. Service Monitor でサポートされる Unified Communications Manager ソフトウェアのバージョンについては、『Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix』を参照してください。

図 1-1 に、ネットワーク内のセンサーおよびクラスタと、データを受信および取得し、レポートを作成し、トラップを送信する Service Monitor を示します。

図 1-1

Service Monitor の概要



詳細については、次の項を参照してください。

- 「Service Monitor の設定」 (P.3-1)
- 「Cisco 1040 の管理」 (P.4-1)

しきい値とトラップ

Service Monitor は、受信したデータを調査して、ユーザ定義のしきい値グループ設定とグローバルしきい値設定のうち、該当するしきい値と MOS を比較します。MOS がしきい値を下回っている場合、Service Monitor は SNMP トラップを生成し、そのトラップを最大 4 つのトラップ レシーバに送信します。

しきい値は、次のレベルで設定できます。

- センサー グループ：センサーおよびエンドポイントを選択して、1 つまたは複数のサポートされるコーデックの MOS しきい値を設定します。
- CVTQ グループ：Unified Communications Manager クラスタおよびエンドポイントを選択して、1 つまたは複数のサポートされるコーデックの MOS しきい値を設定します。

- グローバル設定：1 つまたは複数のサポートされるコーデックのデフォルトしきい値を更新します。グローバルしきい値設定は、他に該当するしきい値がない場合に使用されます。

Service Monitor からは、トラップも送信されます。送信されるのは、センサーが到達不能になったときと、同じセンサーが再び到達可能になったときです。

トラップ レシーバ

Service Monitor は、受信したデータを調査し、コーデックのデフォルトまたはユーザ定義のしきい値と MOS を比較します。MOS がしきい値を下回っている場合、Service Monitor は SNMP トラップを生成し、そのトラップを最大 4 つのトラップ レシーバに送信します。

Service Monitor がクラスタやセンサーから受信したコール データは、データベースに保存されます。保存される日数は設定可能です。（「その他の設定項目の設定と表示」(P.3-39) の「Report Data Retention Period」の説明を参照）。さらに、Service Monitor がセンサーから受信したコール データをディスク ファイルに保存することもできます。（「Cisco 1040 センサーのデフォルト設定の設定」(P.4-4) を参照）。

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

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

詳細については、『*User Guide for Cisco Prime Unified Operations Manager 8.7*』を参照してください。

Service Monitor のホームページ

ログイン直後に表示される Service Monitor のホームページは、[Reports] タブです。このホームページから、MOS 統計のレポートを生成できます。レポート用のデータを保存しておく日数は設定可能です。詳細については、次のトピックを参照してください。

- 「[診断レポートの使用法](#)」(P.2-3)
- 「[CVTQ 診断レポートの生成](#)」(P.2-14)
- 「[Most-Impacted Endpoints レポートの使用法](#)」(P.2-23)

Service Monitor の起動

ステップ 1 次のとおりにアドレスをブラウザに入力します。

- Secure Socket Layer (SSL) がイネーブルになっていない場合は、`http://server_name:1741` とブラウザに入力します。server_name は、Service Monitor がインストールされているサーバの DNS 名または IP アドレスです。
- SSL がイネーブルの場合は、`https://server_name:443` と入力します。



(注) Service Monitor のインストール時に HTTPS ポートを変更した場合は、443 の代わりに、インストール時に入力したポート番号を入力してください。

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、次の方法を使用できる可能性があります。

- 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 を押します。

Service Monitor のホーム ページが表示されます。

詳細については、「[レポートの使用方法](#)」(P.2-1) を参照してください。

Operations Manager からの Service Monitor の起動

Operations Manager から Service Monitor を起動するには、次の手順に従います。

ステップ 1 [UC Management Suite] を選択してから、[Service Monitor] の [Launch Home Page] を選択します。

[List Service Monitors - Cisco Prime Unified Operations Manager] 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 Service Monitor - Cisco Prime Unified Operations Manager] ページが表示されます。

ステップ 3 次を入力します。

- IP アドレス / ホスト名 : Service Monitor サーバの IP アドレスまたはホスト名です。
- プロトコル : ドロップダウン リストから [http] または [https] を選択します。
- ポート : ポート番号は 1741 です。
- リマーク : コメントがある場合は入力します。
- ユーザ名
- パスワード
- HTTPS ポート : デフォルトは 443 です。

ステップ 4 [Add] をクリックします。

[List Service Monitor] ページに Service Monitor サーバの詳細が表示されます。

ステップ 5 表示された IP アドレスの横のチェックボックスを選択してから、[Launch] をクリックします。

Service Monitor ホームページが表示されます。

ステップ 6 [Edit] をクリックして、Service Monitor の詳細を編集します。

ステップ 7 [Configure] をクリックして、トラップ レシーバ パラメータを設定します。

エンタープライズおよび MSP 導入モードについて

Service Monitor 8.7 は、要件に基づいて次のどちらのモードでもインストールできます。

- 企業ネットワーク導入モード
- マネージド サービス プロバイダー (MSP) ネットワーク導入モード

モードは、製品をインストールするときに指定できます。



(注)

MSP ネットワーク導入モードでは、Operations Manager と Service Monitor を同じマシンに配置されている必要があるため、Operations Manager と Service Monitor を同一の仮想または物理マシンにインストールする必要があります。MSP ネットワーク導入モードは、Service Monitor のスタンドアロンインストールでは選択できません。

どちらのモードでも Service Monitor は常に固有の Operations Manager インスタンスと連携して動作し、Operations Manager と Service Monitor の両方で同じ Unified Communications Manager が管理されます。

MSP ネットワーク導入モードでは、サービス プロバイダー導入された 1 つの Operations Manager インスタンスから、複数のカスタマーを表示および管理できます。複数のカスタマーに及ぶタスクと、1 つのカスタマーに対するタスクのどちらも実行できます。

Service Monitor は、複数の Call Manager から CDR と CMR を収集してレポートします。複数のカスタマー ビューでは、Service Monitor 内に存在する Call Manager のユーザ認可に基づいて、表示と処理の制限がサポートされます。

Role-Based Access Control (RBAC; ロールベース アクセス コントロール) を使用することで、Operations Manager 8.7 は、カスタマーごとのクラスタ、アプリケーション、およびデバイスのカスタマイズに使用する System Defined Groups に基づいて、ユーザを認証および認可する機能を提供します。

Operations Manager で定義されたカスタマーは Service Monitor に表示されます。Operations Manager のカスタマー用クラスタの表示権限でログインしたユーザは、同じクラスタを Service Monitor で表示できます。ユーザは、自分のロールに対して許可されたものだけの表示と実行に制限されます。RBAC の詳細については、[RBAC の概要](#)を参照してください。

Service Monitor には、該当するカスタマー名が表示されます。Service Monitor が MSP ネットワーク導入モードで Operations Manager と組み合わせてインストールされた場合は、Service Monitor のホームページの右上にある [Customer] リンクに、管理対象カスタマーのリストが表示されます。MSP ネットワーク導入モードと複数のカスタマー ビューの詳細については、『*User Guide for Cisco Prime Unified Operations Manager 8.7*』を参照してください。

ネットワーク導入モードでは、NAT 対応デバイスが存在する場合、Service Monitor を NAT 用に設定する必要がありません。Service Monitor が共同配置または共存する Operation Manager インスタンスと連携している限り、Service Monitor は NAT を使用しているクラスタをモニタできます。詳細については、『*User Guide for Cisco Prime Unified Operations Manager 8.7*』を参照してください。



(注)

Cisco 1040 センサーと NAM は MSP ネットワーク導入モードでサポートされません。

RBAC の概要

Role Based Access Control (RBAC) は Common Services の内蔵機能です。Operations Manager 8.7 および Service Monitor 8.7 は RBAC 機能を使用して、デバイス グループへのアクセスに対するユーザ ロールベースの認証および認可を実現します。

Common Services を使用すると、Operations Manager にデバイスグループを作成し、ユーザをロールに割り当てることができます。Common Services で作成したユーザ ロールは、Operations Manager と Service Monitor に共通のものとなります。

ロールからタスクへの Service Monitor マッピングは、Operations Manager と共有されます。その結果、次のどちらも実行できます。

- ロールに割り当てられたタスクの表示
- 新しいユーザ ロールの作成時にタスクを選択。

Operations Manager で新しいユーザを作成するときは、他の Operations Manager タスクと同時に Service Monitor タスクのリストを表示および選択できます。Operations Manager と Service Monitor が同一サーバ上にある場合は、Common Services データベースが共有されるため、DCR 同期が自動的に行われます。

Service Monitor は次のユーザ ロールをサポートしています。

- Super Admin : Network Administrator ロールおよび System Administrator ロールのすべての権限。
- System Administrator
- Network Administrator
- Network Operator
- Help Desk

タスクからロールへのマッピングについては、アクセス権レポート ([Administration] > [Server Administration (Common Services)] > [Reports] > [Permissions Report]) を参照してください。

エンタープライズ導入モードでは、Cisco Secure ACS を使用してセキュリティを設定することを推奨します。

次の追加情報を参照できます。

- ユーザ設定の詳細については、『*Installation Guide for Cisco Prime Unified Service Monitor*』の「Configuring Security」を参照してください。
- 認証および認可に Cisco Secure ACS を使用するための Service Monitor の設定については、『*Installation Guide for Cisco Prime Unified Service Monitor*』の付録「Security Configuration with Cisco Secure ACS」を参照してください。
- ユーザの作成とロールの割り当ての詳細については、『*Administration of CiscoWorks LAN Management Solution 4.0*』の「[Adding and Modifying a Local User](#)」を参照してください。

