CHAPTER 16

履歴レポートの使用方法

次の各項では、Cisco Unified Operations Manager（Operations Manager）の Event History レポートおよび Service Quality History レポートの使用方法を説明します。

履歴レポートを使用する前に

Event History レポートと Service Quality History レポートでは、過去に発生したイベントを表示できます。確認できる情報には、イベントのステータスと日付、関連デバイスとデバイス コンポーネント、注釈（ユーザが入力した情報テキスト）、イベントの詳細などがあります。

Event History レポートには、レポートを生成するときに使用した基準に応じて、デバイスとクラスタ両方に関する情報を表示できます。Operations Manager は、日次で Event History データベースをパージして、31 日分の履歴のみを保持します。「パージング スケジューラのステータスの表示」（P.20-13）を参照してください。

Service Quality History では、Cisco Unified Service Monitor（Service Monitor）によって収集される統計情報が必要です。Service Monitor は Cisco Unified Communications Management Suite 製品バンドルの一部として使用でき、スタンドアロン アプリケーションとしても使用できます。詳細については、『*User Guide for Cisco Unified Service Monitor*』を参照するか、またはシスコの営業担当者にご連絡ください。

ここでは、次の内容について説明します。

Event History レポートのツール ボタン

表 16-1 に、履歴レポートの右上隅に表示される各ツール ボタンの説明を示します。

表 16-1　[Event History Report] ウィンドウのツール ボタン

アイコン	意味
	現在のレポートを CSV ファイルにエクスポートします。 （注）　PDF エクスポート オプションは、Event および Service Quality の各イベント履歴レポートで使用できません。
	印刷用にプリンタに適したバージョンを開きます。
	状況依存ヘルプを開きます。

2,000 を超えるレコードを持つレポート

Event History レポートには、最大 2,000 レコードが表示されます。レコードは、スクロールするかページを切り替えて表示することができます。レポートが 2,000 レコードを超える場合にすべてのレコードを表示する必要がある場合は、[Export] ツール ボタンを使用してすべての情報を CSV ファイルに保存します。

Event History を使用する前に

24 時間のコンテキストベースのレポートのさまざまなページ（[Topology] 画面など）から、Operations Manager を生成することができます。また、検索基準や日付範囲を指定して、カスタマイズした履歴レポートを生成することもできます。デバイス、デバイスのコンポーネント、およびクラスタに関して、Event History レポートを作成することもできます。24 時間および 7 日間のレポートの自動エクスポートも可能です。

Event History の表示には、次の問題があります。

ネットワークで一度に 5,000 よりも多いイベントが生成されると、Event History で一部のイベントがドロップされます。これは、Event History で 5,000 よりも多いイベントのバースト中に最大で 5,000 イベントを処理する場合に発生します。

これを解決するには、[Events] 画面でイベントを表示します。これらのイベントは、システムによって処理されて、この画面に表示されます。イベントがクリアされた場合、それらは 30 ～ 60 分後には [Events History] 画面に表示されません。

24 時間のコンテキストベースの Event History レポート

さまざまな Operations Manager ページ（[Events History] 画面など）上で、Event History のリンクやメニュー項目を使用できます。[Event History] リンクをクリックすると、関連する履歴レコードを表示するコンテキストベースのレポートが生成されます。

- 検索基準を入力する必要はありません。
- 過去 24 時間が対象です。

また、選択した期間を対象とし、指定した検索基準に基づいたレコードを含む、カスタマイズした Event History レポートを生成することもできます。Event History レポートには、コンテキストベースのレポートとカスタマイズしたレポートのどちらを生成しても、同じタイプの情報が含まれます。

24 時間のコンテキストベースの履歴レポートは、Operations Manager のさまざまなページから生成できます。たとえば、次のページから生成できます。

- Fault Monitor : Event History レポートは、Device Details を通じて起動できます。
- Service Level View : デバイスまたはクラスタの Event History レポートを起動できます。
- Device Details View
- [Reports] > [Service Quality Events]

カスタマイズした Event History レポート

次のような場合に、Event History レポートを生成すると便利です。

- イベント画面に重要なアラートが表示されているため、先月にどのような頻度でそのアラートが生成されていたかを確認する必要がある。
- 異常なイベントが発生したことを通知する電子メールを受信した。
- カスタマイズしたイベント画面で、トラッキングしているもの以外のイベントに関する情報を検索する必要がある。

Event History レポートを生成すると、以下に関する情報を収集できます。

- すべてのイベント。
- 特定のデバイスのコンポーネントで発生したイベント。
- 異なるデバイスにおける同じイベント発生回数。
- クラスタ（デバイス グループで選択できる）。
- イベントの問題に対して取れる推奨措置。

24 時間および 7 日間の Event History レポートのエクスポート

24 時間の Event History レポートを毎日午前 0 時に、7 日間の Event History レポートを毎週月曜の午前 0 時にそれぞれ自動的に生成するには、次の手順を実行します。これらのレポートは、カンマ区切り形式（CSV）で生成でき、ディスクに保存するか、電子メールで送信することができます。

ステップ 1　[Reports] > [Event History] > [Export] を選択します。

自動的に [Export Event Reports] ページが表示されます。

ステップ 2　生成するレポートごとに CSV を選択し、レポートをカンマ区切り形式ファイルとして保存します。

生成できるレポートは次のとおりです。

- All events for the last 24 hours : 24 時間のレポートは、EventReports_Daily_ddmmyyyy.filetype という名前（たとえば EventReports_Daily_20Apr2006.csv）が付けられます。
- All events for the last 7 days : 7 日間のレポートは、EventReports_Weekly_ddmmyyyy.filetype という名前（たとえば EventReports_Weekly_17Apr2006.csv）が付けられます。7 日間のレポートは、毎週月曜日の午前 0 時に実行されます。

ステップ 3　レポートを格納または送信する 1 つ以上の場所を入力します。

- レポートをディスクに格納する場合は、サーバ上の場所を入力（または参照して選択）します。

  Casuser および管理者は、デフォルト ディレクトリの書き込み権限を持っています。ディレクトリを変更する場合は、そのディレクトリに対して casuser の書き込み権限を持っていることを確認してください。権限がない場合、エクスポート ファイルは作成されません。
- レポートを電子メールで送信する場合は、完全修飾電子メール アドレスを入力します。

ステップ 4　[Apply] をクリックします。

カスタマイズした Event History レポートの生成

過去 31 日間のイベントに関する履歴情報を収集するには、Operations Manager ホームページで [Reports] > [Event History] を選択して、Event History を起動します。次の各項では、Event History データベースに格納されたすべての情報に基づいて、フィルタを適用し、レポートを生成する方法について説明します。

- イベント ID、デバイス、またはグループによってデバイスのイベントを検索するには、「特定のイベントに関して格納されているすべての情報の取得」（P.16-4）を参照してください。
- Cisco 1040、コールのエンドポイント、または電話モデルでの Service Quality イベントを検索するには、「Service Quality イベントに関して格納されたすべての情報の取得」（P.16-11）を参照してください。

Service Quality History レポートは、Service Monitor のライセンスを購入している場合にのみ使用できます。

特定のイベントに関して格納されているすべての情報の取得

Service Quality イベントについては、「Service Quality イベントに関して格納されたすべての情報の取得」（P.16-11）を参照してください。

Event History データベースでは、次のいずれかの方法でイベントを検索することができます。

- 「イベント ID によるイベントの検索」（P.16-5）
- 「デバイスによるイベントの検索」（P.16-5）
- 「特定のイベントの表示」（P.16-6）
- 「デバイス グループによるイベントの検索」（P.16-7）
- 「日付によるイベントの検索」（P.16-7）

また、デバイス コンポーネントのすべてのイベントの 24 時間レポートを生成するには、[Device Detail] ページの [Event History] リンクをクリックします。「デバイスの詳細の表示」（P.8-38）を参照してください。

イベント ID によるイベントの検索

特定のイベントが発生した頻度を確認するには、イベント ID によってそのイベントを検索します。このイベント ID は [Device Details] 画面に表示されます

イベント ID でイベントを検索するには、次の手順を実行します。

ステップ 1　[Reports] > [Event History] > [Event] を選択します。

[Event History: Search by Event ID] ページが表示されます。

ステップ 2　次のように検索基準を設定します。

a. イベント ID を入力します。

b. 日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。
- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Event History レポートが開きます。このレポートには、デバイスとクラスタの両方の情報が含まれます。レポートの内容の説明については、「Event History レポートについて」（P.16-8）を参照してください。

デバイスによるイベントの検索

特定のデバイス上で発生したイベントのタイプを調べるには、次の手順を実行します。

ステップ 1　[Reports] > [Event History] > [Devices] を選択します。

[Event History Search by Device] ページが表示されます。

ステップ 2　次のように検索基準を設定します。

a. 複数のデバイスを（Device Management でリストされるように）カンマで区切って入力します。異なるグループから複数のデバイスを選択することができます。

b. ポップアップ セレクタ ボックスをクリックして検索するイベントを選択し、イベントの説明を入力します。デフォルトでは、すべてのイベントが選択されています（「Event History レポートの [Event Description] の選択」（P.16-6）を参照）。

c. 日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。
- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Event History レポートが開きます。このレポートには、デバイスのみの情報が含まれます。レポートの内容の説明については、「Event History レポートについて」（P.16-8）を参照してください。

Event History レポートの [Event Description] の選択

[Event Descriptions] ダイアログボックスでは、デフォルトですべてのイベントが選択されています。

（注）　[Reports] > [Event History] > [Event History] > [Device Groups] の下の [Event Description] フィルタ ウィンドウに、ユーザ定義のイベント名が表示されます。イベント レポートが起動すると、カスタマイズした名前が表示されます。
カスタマイズしたイベントのデフォルト名を決めるには、[Administration] > [System Settings] > [Event Customization] に移動します。

どのイベントの説明が表示されるようにするかを決定するには、次の手順を実行します。

ステップ 1　[Event Descriptions] ダイアログ ボックスで、Event History レポートに含めないイベントの選択を解除します。

ダイアログボックスの一番上にある [All] チェックボックスがオンになっていた場合は、特定のイベントの選択をオフにするとこのチェックボックスもオフになります。

ステップ 2　次のどちらかを実行します。

- ダイアログボックスの一番上または一番下にある [Select] をクリックして、選択内容を確定します。
- ダイアログボックスの一番上または一番下にある [Cancel] を選択して選択内容をキャンセルし、すべてのイベントのデフォルトのリストに戻ります。

特定のイベントの表示

特定のイベントを表示するには、次の手順を実行します。

ステップ 1　[Reports] > [Event History] > [Event] を選択します。

[Event History: Search by Event ID] ページが表示されます。

ステップ 2　次のように検索基準を設定します。

a.　イベント ID を入力します。

b.　（オプション）ポップアップ セレクタ ボックスをクリックして検索するイベントを選択し、イベントの説明を入力します（「Event History レポートの [Event Description] の選択」（P.16-6）を参照）。

c.　日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。

- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Event History レポートが開きます。このレポートには、デバイスとクラスタの両方の情報が含まれます。レポートの内容の説明については、「Event History レポートについて」（P.16-8）を参照してください。

デバイス グループによるイベントの検索

特定のデバイス グループでどのようなタイプのイベントが発生しているかを確認するには、次の手順を実行します。

ステップ 1　[Reports] > [Event History] > [Device Groups] を選択します。

[Event History: Search by Device Group] ページが表示されます。

ステップ 2　次のように検索基準を設定します。

a. 1 つ以上のデバイス グループを選択します。

b. ポップアップ セレクタ ボックスをクリックして検索するイベントを選択し、イベントの説明を入力します。

c. 検索するすべてのイベント重大度レベルを選択します。

d. 日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。
- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Event History レポートが開きます。このレポートには、デバイスのみの情報が含まれます。レポートの内容の説明については、「Event History レポートについて」（P.16-8）を参照してください。

日付によるイベントの検索

特定の日、週、月、または日付範囲に発生しているイベントのタイプを判別するには、次の手順を使用します。

ステップ 1　[Reports] > [Event History] > [Event History] > [Date] を選択します。

[Event History Search by Date] ページが表示されます。

ステップ 2　日付の範囲を選択し、次のように入力します。

- Today。
- 7 days。

- One Month。
- From: *a date* と to: *a date*：日付を入力または選択します。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Event History レポートが開きます。このレポートには、デバイスとクラスタの両方の情報が含まれます。レポートの内容の説明については、「Event History レポートについて」（P.16-8）を参照してください。

詳細については、次のトピックを参照してください。

- 「Event History を使用する前に」（P.16-2）
- 「Event History レポートのツール ボタン」（P.16-1）
- 「Event History レポートからのイベントのプロパティの表示」（P.16-10）
- 「処理されるイベント」（P.E-1）

Event History レポートについて

Event History レポート（図 16-1）は、検索基準に基づいて最大 2,000 レコードを表示する、スクロール可能なテーブルです。2,000 レコードを超えるデータベース コンテンツを表示するには、ウィンドウ右上隅の [Export] ツール ボタンをクリックします。

[Events History] 画面を使用するときは、次の点に注意してください。

- 監視対象デバイスがネットワークから取り外された場合、そのデバイスは到達不能でも、次のインベントリの収集が行われるまで Monitored 状態のままとなります。該当のデバイスが到達不能であることがわかるのは、[Events] 画面にそのデバイスの Unreachable イベントが表示されたときだけです。
- デバイスが応答不能になると、このデバイスに既存するすべてのイベントがクリアされ、応答不能イベントが 1 つ生成されます。

ここでは、次の内容について説明します。

- 「Event History レポートからのユーザの注釈の表示」（P.16-10）
- 「Event History レポートからのイベントのプロパティの表示」（P.16-10）

（注） Service Quality イベントは、Service Quality History レポートで報告されます。「Service Quality History レポートについて」（P.16-14）を参照してください。

図 16-1　Event History レポート

	Severity	Event ID	Device Name	Component Name	Event Name	Last Updated Time	Status
1	Critical	00002A6	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 04:06:29	Active
2	Critical	00002A5	blrsd3.cisco.com	blrsd3.cisco.com	PerformancePollingStopped	21-Jul-2010 04:05:53	Cleared
3	Critical	00002A4	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 04:03:27	Cleared
4	Critical	00002A3	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 04:02:26	Active
5	Critical	00002A2	blrsd3.cisco.com	blrsd3.cisco.com	PerformancePollingStopped	21-Jul-2010 04:02:00	Active
6	Critical	00002A1	10.64.95.162	IF-10.64.95.162/65539 [HP NC324i PCIe Dual Port Gigabit Server Adapter #2]	OperationallyDown	21-Jul-2010 03:56:24	Cleared
7	Critical	00002A0	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 03:51:17	Cleared
8	Critical	000029Z	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 03:50:16	Active
9	Informational	000029Y	VE-cm612-cluster	VE-cm612-cluster	RTMTDataMissing	21-Jul-2010 03:49:07	Active
10	Critical	000029X	blrsd3.cisco.com	blrsd3.cisco.com	PerformancePollingStopped	21-Jul-2010 03:48:03	Cleared

Event History レポート ウィンドウには、表 16-1 に示すツールがあります。

表 16-2 に、Event History レポートの内容を示します。

表 16-2　Event History レポート：内容

見出し	説明
Severity	重大、警告、または情報。
Event ID	イベント識別番号。このリンクをクリックすると、そのイベントに関する詳細情報の入った、イベントのプロパティ ウィンドウが表示されます（図 16-2（P.16-10）を参照）。
Device Name	デバイス名または IP アドレス。
Component Name	デバイス タイプ。[Inventory Collection in Progress] は、Operations Manager がイベント発生時にデバイスの検出中であったことを示します。新しいイベントの発生時に実際のデバイス タイプが反映されます。 インベントリ収集中は、デバイス タイプは N/A と表示されます。詳細については、第 8 章「Device Management の使用方法」を参照してください。
Event Name	イベント名。
Last Updated Time	イベントが生成された日付と時刻。
Status	前回のポーリングに基づくイベント ステータス。
	Active：イベントはライブ状態です。
	Cleared：イベントはライブ状態ではありません。また、デバイスが一時停止されると、すべてのイベントがクリアされます。Operations Manager のポーリングにより、アラームが（ポーリングの時点から）30 分以上 Cleared の状態であることが確認されると、アラームは有効期限切れになり、イベントの画面から削除されます。
	Suspended：デバイスが一時停止されています。
	Resumed：デバイスが再開されました。
	Deleted：デバイスは削除されています。

Event History レポートからのユーザの注釈の表示

Event History レポートで [Status] カラムのリンクをクリックすると、イベントの注釈ページが開きます。

ユーザが入力したすべてのメモを一覧表示するイベントの注釈ページが表示されます（詳細については、「デバイスおよびイベントの詳細の取得」（P.4-24）を参照してください）。注釈がない場合は、取得できる注釈がないというメッセージが表示されます。

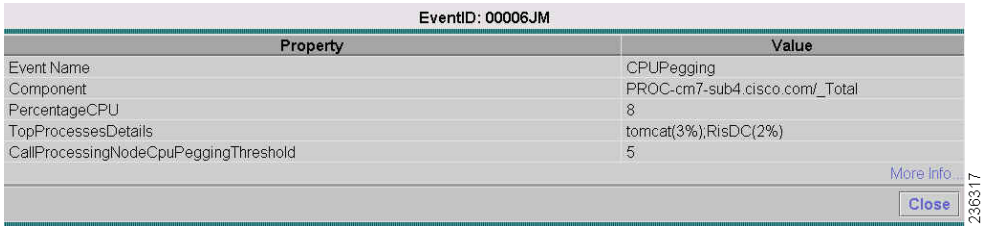
Event History レポートからのイベントのプロパティの表示

Event History レポートで [Event ID] カラムのイベントをクリックすると、イベントのプロパティ ページが開きます。このページには、MIB 属性、ポーリングとしきい値の情報、使用率情報など、イベントに関する詳細な情報が表示されます。

現在の値の横にイベント発生時の値が表示されます。問題を解決するための推奨される措置などのその他のイベント詳細情報については、[More Info] ボタンをクリックしてオンライン ヘルプを参照してください。

図 16-2 にイベントのプロパティ ページの例を示します。

図 16-2　　イベントのプロパティ ページ



Service Quality History レポートを使用する前に

次の事項について説明します。

- 「24 時間および 7 日間の Service Quality History レポートのエクスポート」（P.16-10）
- 「Service Quality イベントに関して格納されたすべての情報の取得」（P.16-11）

24 時間および 7 日間の Service Quality History レポートのエクスポート

24 時間の Service Quality History レポートを毎日午前 0 時に、7 日間の Service Quality History レポートを毎週月曜の午前 0 時にそれぞれ自動的に生成するには、次の手順を実行します。これらのレポートは、カンマ区切り形式（CSV）で生成でき、ディスクに保存するか、電子メールで送信することができます。

ステップ 1　[Reports] > [Service Quality History] > [Event History] > [Export] を選択します。

自動的に [Export Service Quality Reports] ページが表示されます。

ステップ 2　次の 1 つ以上のレポートおよびレポート形式を選択します。

- All issues for the last 24 hours：1 つ以上のチェックボックスをオンにして、24 時間の Service Quality History レポートを CSV（カンマ区切り値のファイル）として生成および保存します。

  24 時間のレポートは、ServiceQualityReports_Daily_ddmmyyyy.filetype という名前（たとえば ServiceQualityReports_Daily_20Apr2006.csv）が付けられます。
- All issues for the last 7 days：1 つ以上のチェックボックスをオンにして、7 日間の Service Quality History レポートを CSV として生成および保存します。

  7 日間のレポートは、ServiceQualityReports_Weekly_ddmmyyyy.filetype という名前（たとえば ServiceQualityReports_Weekly_20Apr2006.csv）が付けられます。7 日間のレポートは、毎週月曜日の午前 0 時に実行されます。

ステップ 3　レポートを格納または送信する 1 つ以上の場所を入力します。

- レポートをディスクに格納する場合は、サーバ上の場所を入力（または参照して選択）します。

  Casuser および管理者は、デフォルト ディレクトリの書き込み権限を持っています。ディレクトリを変更する場合は、そのディレクトリに対して casuser の書き込み権限を持っていることを確認してください。権限がない場合、エクスポート ファイルは作成されません。
- レポートを電子メールで送信する場合は、完全修飾電子メール アドレスを入力します。

ステップ 4　[Apply] をクリックします。レポートが毎日午前 0 時に生成されます。

Service Quality イベントに関して格納されたすべての情報の取得

Service Quality History では、Cisco Unified Service Monitor（Service Monitor）によって収集される統計情報が必要です。Service Monitor は Cisco Unified Communications Management Suite 製品バンドルの一部として使用でき、スタンドアロン アプリケーションとしても使用できます。

詳細については、『*User Guide for Cisco Unified Service Monitor*』を参照するか、またはシスコの営業担当者にご連絡ください。

Event History データベースでは、次のいずれかの方法で Service Quality イベントを検索することができます。

- 「MOS による Service Quality イベントの検索」（P.16-11）
- 「宛先による Service Quality イベントの検索」（P.16-12）
- 「コーデックによる Service Quality イベントの検索」（P.16-12）
- 「電話モデルによる Service Quality イベントの検索」（P.16-13）
- 「Cisco 1040 による Service Quality イベントの検索」（P.16-13）
- 「日付による Service Quality イベントの検索」（P.16-14）

MOS による Service Quality イベントの検索

指定した値よりも低い MOS の Service Quality イベントを表示するには、次の手順を実行します。

ステップ 1　[Reports] > [Service Quality History] > [Event History] > [MOS] を選択します。

[Service Quality History: Search by MOS] ページが表示されます。

ステップ 2　次のように検索基準を設定します。

a.　MOS less than：最低値を入力します。MOS 値の範囲は、0.1 ～ 4.9 です。

b. 日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。
- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Service Quality History レポートが開きます。レポートの内容の説明については、「Service Quality History レポートについて」（P.16-14）を参照してください。

宛先による Service Quality イベントの検索

コールのエンドポイントに対応する Service Quality イベントを表示するには、次の手順を実行します。

ステップ 1　[Reports] > [Service Quality History] > [Event History] > [Destination] を選択します。

[Service Quality History: Search by Destination] ページが表示されます。

ステップ 2　次のように検索基準を設定します。

a. 演算子を選択します。

- Is exactly
- Begins with
- Contains

b. 宛先（電話、音声ゲートウェイ、または Cisco 1040 の IP アドレス）を入力します。

c. 日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。
- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Service Quality History レポートが開きます。レポートの内容の説明については、「Service Quality History レポートについて」（P.16-14）を参照してください。

コーデックによる Service Quality イベントの検索

特定のコーデックの Service Quality イベントを表示するには、次の手順を実行します。

ステップ 1　[Reports] > [Service Quality History] > [Event History] > [Codec] を選択します。

[Service Quality History: Search by Codec] ページが表示されます。

ステップ 2　次のように検索基準を設定します。

a. リストからコーデックを選択します。

b. 日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。
- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Service Quality History レポートが開きます。レポートの内容の説明については、「Service Quality History レポートについて」（P.16-14）を参照してください。

電話モデルによる Service Quality イベントの検索

特定の電話モデルに対応する Service Quality イベントを表示するには、次の手順を実行します。

ステップ 1　[Reports] > [Service Quality History] > [Event History] > [Phone Model] を選択します。

ステップ 2　[Service Quality History: Search by Phone Model(s)] ページが表示されます。

ステップ 3　次のように検索基準を設定します。

a. ポップアップ セレクタ ボックスをクリックして検索する電話モデルを選択します。

b. 日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。
- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 4　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Service Quality History レポートが開きます。レポートの内容の説明については、「Service Quality History レポートについて」（P.16-14）を参照してください。

Cisco 1040 による Service Quality イベントの検索

特定の Cisco 1040 に対応する Service Quality イベントを表示するには、次の手順を実行します。

ステップ 1　[Reports] > [Service Quality History] > [Event History] > [Cisco 1040] を選択します。

[Service Quality History: Search by Cisco 1040] ページが表示されます。

ステップ 2　次のように検索基準を設定します。

a. 演算子（[Is exactly]、[Begins with]、[Contains]）を選択して、Cisco 1040 の ID または Cisco 1040 の ID の一部を入力します。

Cisco 1040 の ID は、1 つの文字と 3 桁の数字で構成されています。

b. 日付の範囲を選択します。

- Today。
- One Month（*date* から *date* まで）。
- From: *date* と to: *date* : 日付を選択します（または dd-Mmm-yyyy の形式で日付を入力します。たとえば 04-Mar-2006）。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Service Quality History レポートが開きます。レポートの内容の説明については、「Service Quality History レポートについて」（P.16-14）を参照してください。

日付による Service Quality イベントの検索

特定の日付の Service Quality イベントを表示するには、次の手順を実行します。

ステップ 1　[Reports] > [Service Quality History] > [Event History] > [Date] を選択します。

[Service Quality History: Search by Date] ページが表示されます。

ステップ 2　次のいずれかを選択し、必要に応じて日付を入力します。

- Today。
- 7 days。
- 1 month。
- From: *a date* および to: *a date* : 日付を入力します。

ステップ 3　[View] をクリックします。

1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに検出されたレコードの合計数が示されます。

Service Quality History レポートが開きます。レポートの内容の説明については、「Service Quality History レポートについて」（P.16-14）を参照してください。

詳細については、次のトピックを参照してください。

「処理されるイベント」（P.E-1）

Service Quality History レポートについて

Service Quality History では、Cisco Unified Service Monitor（Service Monitor）によって収集される統計情報が必要です。Service Monitor は Cisco Unified Communications Management Suite 製品バンドルの一部として使用でき、スタンドアロン アプリケーションとしても使用できます。

詳細については、『*User Guide for Cisco Unified Service Monitor*』を参照するか、またはシスコの営業担当者にご連絡ください。

Service Quality History レポートは、検索基準に基づいて最大 2,000 レコードを表示する、スクロール可能なテーブルです。2,000 レコードを超えるデータベース コンテンツを表示するには、ウィンドウ右上隅の [Export] ツール ボタンをクリックします。

Service Quality History レポート ウィンドウには、表 16-1 に示すツールがあります。

表 16-3 に、Service Quality History レポートの内容を示します。

表 16-3　Service Quality History レポート：内容

見出し	説明
Severity	イベントの重大度。 • Warning：MOS が Service Monitor で設定された MOS しきい値よりも低くなっています。詳細については、『*User Guide for Cisco Unified Service Monitor*』を参照してください。 • Critical：MOS が Operations Manager で設定された MOS しきい値よりも低くなっています。
Event ID	このリンクをクリックすると、イベント プロパティ ウィンドウが開きます。「Service Quality イベント プロパティの表示」（P.16-16）を参照してください。
Destination Type	次のいずれかです。 • Endpoint • IP Phone
Destination	IP アドレスまたは内線電話番号。
IP Address	宛先の IP アドレス。
MOS	イベントをトリガーした Mean Opinion Score。
Cause	次のいずれかです。 • Jitter • Latency
Time	イベントが発生した日付と時刻。
Codec	次のいずれかです。 • G711Alaw64k • G711Alaw56k • G711Ulaw64k • G711Ulaw56k • G722 64k • G722 56k • G722 48k • G728 • G729 • G729AnnexA • G729AnnexB • G729AnnexAwAnnexB
Source Type	次のいずれかです。 • Endpoint • IP Phone

表 16-3　Service Quality History レポート：内容（続き）

見出し	説明
Source	IP アドレスまたは内線電話番号。
IP Address	発信元の IP アドレス。
Customer	マルチ エンドカスタマー バージョンでデバイス追加手順の実行中に入力したカスタマー名。

Service Quality イベント プロパティの表示

Service Quality イベント プロパティを表示するには、Service Quality History レポートのイベント ID のリンクをクリックします。「Service Quality History レポートについて」（P.16-14）を参照してください。

表 16-4 に、Service Quality イベント プロパティ ウィンドウの内容を示します。

表 16-4　Service Quality イベント プロパティ ウィンドウ：内容

見出し	説明
Destination	内線番号、または N/A（宛先タイプがエンドポイントの場合）。
Destination IP Address	エンドポイントまたは IP 電話の IP アドレス。
Destination Type	次のいずれかです。 • Endpoint • IP Phone • Media Server
Destination Model	電話モデル、または N/A（宛先タイプがエンドポイントの場合）。
Switch for Destination	IP アドレス、または N/A（宛先タイプがエンドポイントの場合）。
Destination Port	ポート タイプおよびスロット（Gi1/0/23 など）。
Source	内線番号または IP アドレス。
Source IP Address	IP アドレス、または N/A（宛先タイプがエンドポイントの場合）。
Source Type	次のいずれかです。 • IP Phone • Endpoint
Source Model	電話モデル、または N/A（ソース タイプがエンドポイントの場合）。
Switch for Source	IP アドレス、または N/A（ソース タイプがエンドポイントの場合）。
Source Port	ポート タイプとスロット、または N/A（ソース タイプがエンドポイントの場合）。

表 16-4　Service Quality イベント プロパティ ウィンドウ：内容（続き）

見出し	説明
Detection Algorithm	MOS の計算に使用されるアルゴリズム。次のいずれかです。 • ITU G.107：1040 センサ ベースの音声品質 Cisco 1040 センサで MOS が計算されることを示します。 • CVTQ：電話ベースの音声品質 Cisco Voice Transmission Quality アルゴリズムを使用して、IP 電話または Cisco 音声ゲートウェイで MOS が計算されることを示します。
MOS	イベント発生時の MOS 値。
Critical MOS Threshold	Operations Manager に設定された MOS しきい値。
Cause	次のいずれかです。 • Jitter • Latency • Packet Loss
Codec	宛先で使用されるコーデック。次のいずれかです。 • G711Alaw64k • G711Alaw56k • G711Ulaw64k • G711Ulaw56k • G722 64k • G722 56k • G722 48k • G728 • G729 • G729AnnexA • G729AnnexB • G729AnnexAwAnnexB
Jitter	ミリ秒。
Packet loss	パケット数。
Customer	カスタマー名。
センサからのデータに基づいたイベントの詳細	
Sensor MAC	Sensor MAC：センサの MAC アドレス。
Number of suppressed traps	抑制開始時刻から抑制終了時刻までの間に Cisco Unified Service Monitor が抑制したトラップの数 Service Monitor は、指定されたエンドポイントに対して *n*（設定可能な数字）分ごとに 1 つのトラップを送信します。その間のその他のトラップは抑制されます（送信されません）。詳細については、『*User Guide for Cisco Unified Service Monitor*』を参照してください。

表 16-4　Service Quality イベント プロパティ ウィンドウ：内容（続き）

見出し	説明
Suppression start time	このエンドポイントに対して Service Monitor がトラップの抑制を開始した日付と時刻。
Suppression end time	このエンドポイントに対して Service Monitor がトラップの抑制を終了した日付と時刻。
クラスタからのデータに基づいたイベントの詳細	
CVTQ version	MOS の計算に使用される CVTQ アルゴリズムのバージョン。
Cluster ID	Cisco Unified Communications Manager のクラスタ ID。
Cumulative Concealment Ratio	隠蔽フレームの合計数を音声ストリームの開始以降に受信した音声フレームの合計数で割った値。
Interval Concealment Ratio	アクティブな音声の直前の 3 秒間の音声フレームに対する隠蔽フレームの比率。音声アクティビティ検出（VAD）を使用する場合は、アクティブな音声を 3 秒集めるために、もっと長い間隔が必要になる可能性があります。
Max Incremental Concealment Ratio	音声ストリームの開始以降の最大間隔の隠蔽比率。
Concealment Seconds	音声ストリームの開始以降に隠蔽イベント（フレームの喪失）が発生した秒数（大幅に隠蔽された秒数）。
Severely Concealed Seconds	5 % を超えるフレームが隠蔽された秒数。
Call duration	時間、分、秒。*n*h *n*m *n*s という形式で表します。たとえば、123 秒の通話は 2m 3s と表示されます。
MOS during last 8 secs	コールの最後の 8 秒間の MOS 値。
Min MOS during call	コール中の MOS の最小値。
Max MOS During Call	コール中の MOS の最大値。