CHAPTER 3

Service Monitor の設定

この項では次のトピックについて説明します。

（注） 詳細については、「Cisco 1040 の管理」（P.4-1）および「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。

トラップ レシーバの設定

Service Monitor が送信する SNMP トラップについては、「使用される MIB と生成される SNMP トラップ」（P.D-1）を参照してください。

ステップ 1 [Administration] > [Configuration] > [Trap Receivers] を選択します。[Trap Receiver Parameters] ページが表示されます。

ステップ 2 次の表で説明するデータを入力します。

GUI の要素	説明 / 処理
SNMP Community String	各トラップ レシーバの SNMP コミュニティ ストリングを入力します。
[Trap Receiver *n*] および [Port] フィールド（*n* は 1 ～ 4 までの番号）	最大 4 つのトラップ レシーバを入力します。 • Trap Receiver *n*：サーバの IP アドレスまたは DNS 名を入力します。Operations Manager を使用して Service Monitor のデータを操作および表示するには（たとえば、[Service Quality Alerts] ダッシュボードを使用するには）、Operations Manager が動作しているシステムの IP アドレスを指定します。 • Port：レシーバが SNMP トラップを受信するポート番号を入力します。デフォルトは 162 です。ただし、この目的でサーバ上の別のポートが使用されることもあります。 Service Monitor は SNMP トラップを生成すると、これらのレシーバに転送します。

ステップ 3　[OK] をクリックします。

データ ソース クレデンシャルの概要と設定

Service Monitor は Unified Communications Manager のクラスタとセンサー（Cisco 1040 および NAM）からデータを収集します。Cisco 1040 についてはクレデンシャルを入力する必要はありません。Cisco 1040 でデータ収集ができるようにする方法については、「Cisco 1040 の管理」（P.4-1）を参照してください。ただし、NAM および Unified Communications Manager パブリッシャ サーバについては、次の作業を行う必要があります。

- Service Monitor にクレデンシャルを設定する。
- クレデンシャルを最新の状態に保つ（NAM または Unified Communications Manager パブリッシャ サーバでクレデンシャルを更新する場合、Service Monitor で対応するクレデンシャルも更新する必要があります）。

Data Source Management ページを表示するには、[Administration] > [Configuration] > [Data Source Management] を選択します。[Data Source Management] ページに、次の項目が表示されます。

- As of：ページを開いた日時、またはページを最後に更新した日時。
- メッセージ（SMTP サーバが設定されていない場合）：詳細については、「E メール通知のイネーブル化」（P.6-7）を参照してください。

[Data Source Management] ページには、次の表の情報も表示されます。

列またはボタン	説明 / 処理
Display Name	クレデンシャルを Service Monitor に追加したときに入力した名前。
IP Address	クラスタまたは NAM の IP アドレス NAM ソフトウェアのログイン ページに進むには、NAM の IP アドレスをクリックします。
Type	データ ソースのタイプ。次のいずれかを指定します。 • CCM：Unified Communications Manager クラスタ。 • NAM：ネットワーク解析モジュール。

列またはボタン	説明 / 処理
Version	Unified Communications Manager または NAM のソフトウェア バージョン。 詳細については、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください。
ID	データ ソースのタイプによって異なります。 • CCM の場合：Unified Communications Manager によってクラスタに割り当てられた ID。 • NAM の場合：IP アドレス。
Credentials	Service Monitor がデータ ソース（Unified Communications Manager クラスタまたは NAM）に接続するために使用するクレデンシャルのステータス。クレデンシャルの詳細については、ステータスをクリックして、「クレデンシャルに関するその他の情報の表示」（P.3-3）を参照してください。
Status	データ収集のステータス。 • Configuration Collection：Service Monitor による、デバイスのタイプやゲートウェイなどの設定データを取得するための最後の試行のステータス。詳細については、リンクをクリックして、「設定収集ステータスに関する詳細情報の表示」（P.3-4）を参照してください（Service Monitor は設定データを夜間に Unified Communications Manager から収集します。詳細については、「設定データ収集の実行」（P.3-6）を参照してください）。 • Call Data：Service Monitor が最後にコール データを受信または取得した時点でのステータス、またはその日時。詳細については、リンクをクリックして、「コール データ ステータスの詳細情報の表示」（P.3-4）を参照してください
ボタン	• Add：「データ ソース クレデンシャルの追加」（P.3-7）を参照してください。 • Edit：「データ ソース クレデンシャルの編集」（P.3-11）を参照してください。 • Delete：「データ ソース クレデンシャルの削除」（P.3-13）を参照してください。 • Verify：選択した Unified Communications Manager クラスタのクレデンシャルを確認します。「データ ソース クレデンシャルを使用したトラブルシューティングとクレデンシャルの確認」（P.3-5）と「設定データ収集の実行」（P.3-6）を参照してください。 • Refresh：ページをリフレッシュします。 **（注）** Cisco Unified Provisioning Manager（Provisioning Manager）と Unified Communications Manager の同期中は、Unified Communications Manager 4.x のクレデンシャルの追加、編集、確認は行わないでください。詳細については、「ネットワーク内で Provisioning Manager の同期中にクレデンシャルの異常が発生しないようにするには」（P.3-11）を参照してください。

クレデンシャルに関するその他の情報の表示

[Credentials] 列のリンクをクリックすると表示される情報の例を次に示します。

```
Credential Type: HTTP/S
Current Status: Success
IP Address: 172.25.109.24
Last Contact Time: Wed 03-Feb-2010 14:46:39 PST
Information: Hostname was updated
```

表 3-1 はデータ ソースに関連付けられているクレデンシャルのタイプです。

表 3-1　クレデンシャルのタイプ

データ ソース タイプ	クレデンシャルのタイプ
CCM	• HTTP/S：パブリッシャ サーバの Unified Communications Manager Administration に対する認証のステータスを表します。Unified Communications Manager 4.x 以降で使用されます（データ ソース タイプが NAM の場合、この列に「N/A」と表示されます）。 • CDR/CDRM DB：次のいずれかのデータベースに対する認証のステータスを表します。 – CDR：Unified Communications Manager 4.x で使用されます。 – CDRM：Unified Communications Manager 5.x 以降で使用されます。正しい HTTP/S クレデンシャルを設定した後、Service Monitor はこのデータベースのクレデンシャルにアクセスできるようになります。 （データ ソース タイプが NAM の場合、この列に「N/A」と表示されます）
NAM	• HTTP/S：NAM に対する認証のステータスを表します（データ ソース タイプが CCM の場合、この列に「N/A」と表示されます）。

設定収集ステータスに関する詳細情報の表示

[Configuration Collection] ステータス リンクをクリックすると表示される情報の例を次に示します。

```
Type: Configuration Data Collection
Current Status: Success
IP Address: 172.20.119.214
Last Attempt Time: Thu 04-Feb-2010 01:05:00 PST
Last Success Time: Thu 04-Feb-2010 01:05:16 PST
Information:
```

（注）　現在のステータスが [Success] ではない場合、[Information] 行を参照して解決してください。

詳細については、「設定データ収集の実行」（P.3-6）を参照してください。

コール データ ステータスの詳細情報の表示

[Call Data] ステータス リンクをクリックすると表示される情報の例を次に示します。

```
Current Status: Success
IP Address: 172.20.119.214
Last Contact Time: Thu 04-Feb-2010 15:43:00 PST
Last Data Received Time: Tue 02-Feb-2010 12:08:38 PST
Information:
```

（注）　現在のステータスが [Success] ではない場合、[Information] 行を参照して解決してください。

詳細については、「データ ソース クレデンシャルを使用したトラブルシューティングとクレデンシャルの確認」（P.3-5）を参照してください。

データ ソース クレデンシャルを使用したトラブルシューティングとクレデンシャルの確認

Service Monitor によるデータ ソースへのアクセスや接続ができなくなる問題が発生すると、コール データと設定データの収集と分析ができなくなる場合があります。[Data Source Management] ページの情報を使用すると、次のことができます。

- クレデンシャルが有効であり、Service Monitor がデータの取得をアクティブに実行していることを確認する。
- データ ソース クレデンシャルやレポートに問題の可能性が見られる場合（時間差が著しい場合など）にトラブルシューティングを行う。

ステップ 1　詳細情報を表示するには、[Data Source Management] ページのステータス リンクをクリックします。

- 「クレデンシャルに関するその他の情報の表示」（P.3-3）
- 「設定収集ステータスに関する詳細情報の表示」（P.3-4）
- 「コール データ ステータスの詳細情報の表示」（P.3-4）

表示される情報には、問題の詳細や、トラブルシューティングの必要性の有無が記録されている場合があります。

ステップ 2　トラブルシューティングを行います。

- NAM の場合：次の内容を確認します。
  - NAM のクレデンシャルが変更されているか：変更されている場合は、Service Monitor でクレデンシャルを更新します。
  - NAM に到達可能か：到達不能な場合は、NAM を到達可能な状態にします。
- CCM の場合：次の作業を行います。
  - Service Monitor とクラスタとの通信が最後に成功したのが最近であるか確認します。最後の接続ステータスが Success の場合は、Service Monitor がデータを受信しておらず、データの受信を待っている状態になっていることがあります。
  - Unified Communications Manager のクラスタのクレデンシャルが Service Monitor のクレデンシャルと一致しているか確認し、必要があれば修正します。
  - Service Monitor サーバで DNS パラメータが正しく指定されており、Unified Communications Manager のホスト名が DNS に追加されているか確認します（Unified Communications Manager が正しい名前を取得できるようにするには、Service Monitor が IP アドレスを解決できる必要があります）。
  - クラスタと Service Monitor の間で正常なデータ交換ができなくなる既知の問題については、『*Release Notes for Cisco Unified Service Monitor 8.5*』を参照してください。
  - コール データ ステータスが、Service Monitor によりデータが破棄されていることを示している場合は、そのまま待機するか、何らかの対処を行ってください。Service Monitor が Unified Communications Manager 5.x 以降から古いデータを受信している場合、データは破棄されます。この現象は、Service Monitor と Unified Communications Manager の間の接続が一時切断され、再確立された後に発生する場合があります。Unified Communications Manager は最初に古いファイルを Service Monitor に送信します。

（注） Unified Communications Manager 7.x 以降については、古いデータを Service Monitor に送信しないようにすることができます。詳細については、「ビリング サーバとしての Service Monitor の Unified Communications Manager 5.x 以降への追加」（P.B-4）を参照してください。Service Monitor でサポートしている Unified Communications Manager ソフトウェアのバージョンについては、『*Cisco Unified Service Monitor 8.5 Compatibility Matrix*』を参照してください。

- Service Monitor が使用するクレデンシャルは、Unified Communications Manager プラットフォームで変更される場合があります。このような場合は、Unified Communications Manager の管理者に問い合わせて、正しいクレデンシャルを取得してください。必要であれば、Service Monitor でクレデンシャルを更新します。

ステップ 3　クレデンシャルを確認します。

（注） Provisioning Manager で同期化を実行中の場合は、Unified Communications Manager 4.x でクレデンシャルの確認を行わないでください。「ネットワーク内で Provisioning Manager の同期中にクレデンシャルの異常が発生しないようにするには」（P.3-11）を参照してください。

a. [Administration] > [Configuration] > [Data Source Management] を選択します。[Data Source Management] ページが表示されます。

b. クレデンシャルを確認するデータ ソースを選択します。

c. [Verify] をクリックします。[Configuration Data Collection] ダイアログ ボックスが表示された場合は、次のいずれかを実行します。

[Verify Credentials] をクリックして、クレデンシャルのみを確認する。

[Verify Credentials and Collect Data] をクリックして、クレデンシャルを確認し、Unified Communications Manager から設定データを収集する。詳細については、「設定データ収集の実行」（P.3-6）を参照してください。

詳細については、次の項を参照してください。

- 「Unified Communications Manager の設定」（P.B-1）
- 「データ ソース クレデンシャルの概要と設定」（P.3-2）

設定データ収集の実行

Service Monitor は設定データを夜間に Unified Communications Manager から収集します。しかし、Unified Communications Manager の設定データが変更され、ただちに Service Monitor に反映する必要がある場合は、設定データの収集を実行することができます。

（注） Service Monitor は Unified Communications Manager データに対してクエリーを実行し、設定データを収集します。この操作を実行すると、Unified Communications Manager のパフォーマンスに影響が生じる場合があります。

Unified Communications Manager の設定データのうち、変更時に Service Monitor に影響が生じる可能性があるものの例として、次のようなものがあげられます。

- LogCallsWithZeroDuration フラグの設定
- ゲートウェイ、トランク、システムのデフォルト値のオフネット / オンネット設定
- 新しいデバイスの追加

設定データの収集を実行するには、次の手順を実行します。

ステップ 1　[Administration] > [Configuration] > [Data Source Management] を選択します。[Data Source Management] ページが表示されます。

ステップ 2　クラスタを選択します。

ステップ 3　[Verify] をクリックします。[Configuration Data Collection] ダイアログ ボックスが表示されます。

ステップ 4　[Verify Credentials and Collect Data] をクリックします。

サポートされているデータ ソース ソフトウェア バージョン

Service Monitor でサポートする Unified Communications Manager および NAM のバージョンの一覧については、『*Cisco Unified Service Monitor 8.5 Compatibility Matrix*』を参照してください。

データ ソース クレデンシャルの追加

Service Monitor が Operations Manager とともに環境にインストールされている場合、Service Monitor は、Device Credential Repository（DCR）を使用して Unified Communications Manager を追加および同期します。

Service Monitor が Operations Manager と同じサーバにインストールされている場合は、Operations Manager に追加されている Unified Communications Manager パブリッシャは Service Monitor に自動的に追加されます。

Service Monitor と Operations Manager が別のサーバにインストールされている場合は、Operations Manager にクラスタが自動的に追加されるように、Service Monitor サーバを DCR スレーブとして設定する必要があります。DCR マスター / スレーブ設定の詳細については、Common Services オンライン ヘルプの「Understanding DCR」を参照してください。

（注） Common Services のオンラインヘルプは、[Administration] タブにある、[Common Services] ページを使用することでのみ利用できます。Common Services のオンライン ヘルプにアクセスするには、次の手順を使用します。[Administration] > [Server Administration (Common Services)] > [Security] を選択します。[Setting up Security] ページが表示されます。[Help] をクリックします。

Service Monitor がスタンドアロン環境にインストールされている場合、サポートされているバージョンの Unified Communications Manager および NAM から音声データの取得と分析を行うには、次の手順を実行する必要があります。

1. 次の設定作業を行います。
   - Unified Communications Manager :「Unified Communications Manager の設定」（P.B-1）を参照してください。
   - NAM :「NAM 設定」（P.C-1）を参照してください。
2. ソフトウェア バージョンに適した手順を実行して、データ ソース クレデンシャルを Service Monitor に追加します。
   - 「NAM 4.x 以降のクレデンシャルの追加」（P.3-8）
   - 「Unified Communications Manager 5.x 以降のクレデンシャルの追加」（P.3-9）表 3-1
   - 「Unified Communications Manager 4.x のクレデンシャルの追加」（P.3-10）

（注） Service Monitor に追加する各クラスタには、一意のクラスタ ID が必要です。クラスタ ID は Service Monitor の [Data Source Management] ページで確認することができます。追加する Unified Communications Manager のクラスタ ID を表示する方法については、「Unified Communications Manager のエンタープライズ パラメータの設定」（P.B-4）を参照してください。

NAM 4.x 以降のクレデンシャルの追加

Service Monitor でサポートする特定の NAM のハードウェア プラットフォームとソフトウェア バージョンについては、『*Cisco Unified Service Monitor 8.5 Compatibility Matrix*』を参照してください。

ステップ 1　[Administration] > [Configuration] > [Data Source Management] を選択します。[Data Source Management] 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 Credential] ダイアログボックスが表示されます。

ステップ 3　次の表で説明するデータを入力します。

フィールド	説明
Display Name	最大 20 文字で NAM を説明する名前を入力します。
Version	[NAM 4.x] を選択します。 **（注）**　詳細については、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください。
IP Address Host Name	次のいずれかを入力する必要があります。 • NAM の IP アドレス • DNS による解決が可能な NAM のホスト名 IP アドレスとホスト名の両方を入力した場合、Service Monitor は IP アドレスを使用します。ホスト名は、確認や更新を行わずそのまま保存されます。
Protocol	NAM で設定されている Web サーバに対応するオプション ボタンを選択します。 • HTTP：選択されている場合、次のいずれかを選択します。 – Default Port：ポート番号が表示されます。 – Custom Port：ポート番号を入力します。 • HTTPS：選択されている場合、次のいずれかを選択します。 – Default Port：ポート番号が表示されます。 – Custom Port：ポート番号を入力します。
HTTP/S User Name/Password/Re-enter Password	NAM の Web 管理者のユーザ名およびパスワードを入力します（詳細については、「http または https サーバのイネーブル化と Web 管理者ユーザの設定」（P.C-1）を参照してください）。

ステップ 4　[OK] をクリックします。

ステップ 5　エラー メッセージが表示された場合は、次の手順を実行します。

- NAM のクレデンシャルが正しいことを確認します。
- Service Monitor が NAM のハードウェア プラットフォームとソフトウェア バージョンをサポートしているか確認します。『*Cisco Unified Service Monitor 8.5 Compatibility Matrix*』を参照してください。

Unified Communications Manager 5.x 以降のクレデンシャルの追加

注意　Unified Communications Manager 5.x 以降のソフトウェア バージョン クラスタのクレデンシャルを追加する前に、クラスタ ID にスペースが含まれていないことを確認します。詳細については、『*Release Notes for Cisco Unified Service Monitor 8.5*』を参照してください。

（注）　Unified Communications Manager 5.x 以降の場合は、次の手順を使用してクレデンシャルを追加する以外に、SFTP パスワードも指定する必要があります。「その他の設定項目の設定と表示」（P.3-34）を参照してください。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、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください。

ステップ 1　[Administration] > [Configuration] > [Data Source Management] を選択します。[Data Source Management] 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 Credential] ダイアログボックスが表示されます。

ステップ 3　次の表で説明するデータを入力します。

フィールド	説明
Display Name	最大 20 文字でクラスタを説明する名前を入力します。
Version	CM 5.x 以上のバージョンを選択します。 **（注）**　詳細については、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください。
Publisher IP Address Publisher Host Name	次のいずれかを入力する必要があります。 • Publisher IP address：クラスタ内のパブリッシャの IP アドレスを入力します。 • Publisher hostname：ホスト名だけを入力する場合、DNS による解決が可能なものにする必要があります。 IP アドレスとホスト名の両方を入力した場合、Service Monitor は IP アドレスを使用します。ホスト名は、確認や更新を行わずそのまま保存されます。
HTTP/S User Name/Password/Re-enter Password	パブリッシャ サーバ上の Unified Communications Manager Administration へのログインに使用できるユーザ名とパスワードを入力します。ユーザ ロールには Standard AXL API Access 権限が必要です。

ステップ 4　[OK] をクリックします。

（注）　クラスタ ID の重複が原因で Service Monitor が Unified Communications Manager のクレデンシャルを追加できない場合、「Unified Communications Manager のエンタープライズ パラメータの設定」（P.B-4）の手順に従ってクラスタ ID を変更し、もう一度 Unified Communications Manager のクレデンシャルを追加します。Service Monitor に追加する各クラスタには、一意のクラスタ ID が必要です。

Unified Communications Manager 4.x のクレデンシャルの追加

Service Monitor にクレデンシャルを追加する前に、Unified Communications Manager でクレデンシャルを設定する必要があります。「Unified Communications Manager 4.x システムのデータベース認証の設定」（P.B-7）を参照してください。

（注） Service Monitor に追加する各クラスタには、一意のクラスタ ID が必要です。使用中のクラスタ ID は [Data Source Management] ページで表示することができます。追加する Unified Communications Manager のクラスタ ID を表示する方法については、「Unified Communications Manager のエンタープライズ パラメータの設定」（P.B-4）を参照してください。

Service Monitor にクレデンシャルを追加する場合、Unified Communications Manager で設定されているデータベース認証モードに対応するデータベース認証モードを選択する必要があります。「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）を参照してください。

（注） Provisioning Manager で同期化を実行中の場合は、Unified Communications Manager 4.x でクレデンシャルの追加を行わないでください。詳細については、「ネットワーク内で Provisioning Manager の同期中にクレデンシャルの異常が発生しないようにするには」（P.3-11）を参照してください。

ステップ 1　[Administration] > [Configuration] > [Data Source Management] を選択します。[Data Source Management] 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 Communications Manager] ダイアログ ボックスが表示されます。

ステップ 3　次の表で説明するデータを入力します。

GUI の要素	説明 / 処理
Display Name	最大 20 文字でクラスタを説明する名前を入力します。
Version	[CM 4.x] を選択します。 **（注）** 詳細については、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください。
Publisher IP Address Publisher Host Name	次のいずれかを入力する必要があります。 • Publisher IP address：クラスタ内のパブリッシャの IP アドレスを入力します。 • Publisher hostname：ホスト名だけを入力する場合、DNS による解決が可能なものにする必要があります。 IP アドレスとホスト名の両方を入力した場合、Service Monitor は IP アドレスを使用します。ホスト名は、確認や更新を行わずそのまま保存されます。

GUI の要素	説明 / 処理
CDR Database （バージョン CM 4.x を選択する場合に表示される）	Unified Communications Manager で使用されている認証モードに対応する認証モードを選択し（「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）を参照）、必要なデータを入力します。 • Windows Authentication • SQL Authentication：これを選択した場合、[SQL User Name] フィールドと [SQL Password/Re-enter SQL password] フィールドにもデータを入力する必要があります。入力するユーザ名とパスワードは、Unified Communications Manager パブリッシャ ノードの Microsoft SQL Server アカウントに設定されているものと一致する必要があります。また、このアカウントには CDR データベースへのアクセス権が必要です。
HTTP/S User Name/Password/Re-enter password （バージョン CM 4.x を選択する場合に表示される）	パブリッシャ サーバ上の Unified Communications Manager Administration へのログインに使用できるユーザ名とパスワードを入力します。

ステップ 4　[OK] をクリックします。

（注） クラスタ ID の重複が原因で Service Monitor がデータ ソースのクレデンシャルを追加できない場合、「Unified Communications Manager のエンタープライズ パラメータの設定」（P.B-4）の手順に従ってクラスタ ID を変更し、もう一度 Unified Communications Manager のクレデンシャルを追加します。Service Monitor に追加する各クラスタには、一意のクラスタ ID が必要です。

ネットワーク内で Provisioning Manager の同期中にクレデンシャルの異常が発生しないようにするには

Provisioning Manager がネットワーク内で実行されている場合、Provisioning Manager 管理者に同期スケジュールを問い合わせてください。この処理は計画により行われます。同期中は、Service Monitor で Unified Communications Manager 4.x のクレデンシャルの追加、編集、確認はしないでください。これらの操作を行うと、同期が完了するまでの間、クレデンシャルに異常が発生し（前回の接続ステータスに [Failure] と表示されます）、データは収集されず、クレデンシャルの確認を正常に行うことができません。

データ ソース クレデンシャルの編集

表示名と HTTP/S ユーザ名およびパスワードは、どのデータ ソースについても変更することができます。それ以外の項目については、表示される情報と変更できる内容は、データ ソースがクラスタか NAM かによって異なります。

（注） ネットワークで Provisioning Manager で同期化を実行中の場合は、Unified Communications Manager 4.x のクレデンシャルを編集しないでください。詳細については、「ネットワーク内で Provisioning Manager の同期中にクレデンシャルの異常が発生しないようにするには」（P.3-11）を参照してください。

ステップ 1　[Administration] > [Configuration] > [Data Source Management] を選択します。[Data Source Management] ページが表示されます。

ステップ 2　データ ソースを選択して、[Edit] をクリックします。[Edit Credential] ダイアログボックスが表示されます。

ステップ 3　次の表で説明するデータを入力します。表示されるデータはソフトウェア バージョンにより異なります。

フィールド	説明
Display Name	最大 20 文字でデータ ソースを説明する名前を入力します。
NAM センサーについて表示されるフィールド	
IP Address	このフィールドは編集できないため、グレー表示されています。
Hostname	Service Monitor は、確認することなく、ホスト名への変更を保存します。
Protocol	NAM で設定されている Web サーバに対応するオプション ボタンを選択します。 • HTTP：選択されている場合、次のいずれかを選択します。 – Default Port：ポート番号が表示されます。 – Custom Port：ポート番号を入力します。 • HTTPS：選択されている場合、次のいずれかを選択します。 – Default Port：ポート番号が表示されます。 – Custom Port：ポート番号を入力します。
HTTP/S Username、Password、Re-enter password	NAM の Web 管理者のユーザ名およびパスワードを入力します（詳細については、「http または https サーバのイネーブル化と Web 管理者ユーザの設定」（P.C-1）を参照してください）。
Unified Communications Manager クラスタについて表示されるフィールド	
Publisher IP Address	このフィールドは編集できないため、グレー表示されています。
Publisher Host Name	Service Monitor は、確認することなく、ホスト名への変更を保存します。

フィールド	説明
Windows Authentication SQL Authentication （クレデンシャルの追加時にバージョン CM 4.x が選択された場合）	Unified Communications Manager データベース認証モード。[Windows Authentication] と [SQL Authentication] のいずれかを選択します。 **（注）** 認証モードの変更については、「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）を参照してください。 SQL 認証を選択する場合、入力するユーザ名とパスワードは Unified Communications Manager パブリッシャ ノードの Microsoft SQL Server アカウントに対して設定されているものと一致している必要があります。 • [SQL User Name] および [Password/Re-enter SQL Password] : Unified Communications Manager バージョン 4 パブリッシャ ノードの CDR データベースへのアクセス権がある Microsoft SQL Server アカウントのユーザ名とパスワードを入力します。 • [SQL CDR-DB User Name] および [SQLCDR-DB Password/Re-enter password] : Unified Communications Manager バージョン 3.3.x パブリッシャ ノードの CDR データベースへのアクセス権がある Microsoft SQL Server アカウントのユーザ名とパスワードを入力します。 詳細については、「Unified Communications Manager 4.x における Microsoft SQL Server ユーザ アカウントの追加」（P.B-9）を参照してください。
HTTP/S Username、Password、Re-enter password	パブリッシャ サーバ上の Unified Communications Manager Administration へのログインに使用できるユーザ名とパスワードを入力します。 **（注）** Unified Communications Manager 5.x 以降の場合、ユーザ ロールに Standard AXL API Access 権限が必要です。

ステップ 4　[OK] をクリックします。

Service Monitor がサポートしている Unified Communications Manager ソフトウェア バージョンについては、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください。

データ ソース クレデンシャルの削除

この手順が完了すると、Service Monitor はクラスタや NAM のデータを取得できなくなります。さらに、データ ソースは [Inventory] ページに表示されなくなります。データ ソースのコール データは、消去されるまでデータベースに残っています。詳細については、「Service Monitor データベースの管理」（P.6-1）を参照してください。

この手順を完了する前に、すべての CVTQ およびセンサーしきい値グループからデータ ソースを削除してください。「CVTQ しきい値グループの編集」（P.5-6）と「センサー グループの編集」（P.5-10）を参照してください。

ステップ 1　[Administration] > [Configuration] > [Data Source Management] を選択します。[Data Source Management] ページが表示されます。

ステップ 2　削除するクラスタまたは NAM のチェックボックスを選択します。

ステップ 3　[Delete] をクリックします。次のいずれかが発生します。

- 確認用のダイアログボックスが表示されます。
- エラー メッセージが表示されて、クラスタが属する CVTQ しきい値グループの一覧が示される。これらの CVTQ しきい値グループからクラスタを削除し、この手順を繰り返す必要があります。
- エラー メッセージが表示され、削除しようとしている NAM が属しているセンサーしきい値グループのリストが表示される。これらのセンサーしきい値グループから NAM を削除し、この手順を繰り返す必要があります。

ステップ 4　[OK] をクリックします。

電話機カウントの管理

[Inventory] ページでは、Service Monitor がモニタしている電話機の合計数を表示することができます。また、Service Monitor が認識しているすべてのセンサー（Cisco 1040 と NAM）と Unified Communications Manager クラスタの名前の表示、それぞれがモニタ対象であるかどうかの確認、モニタ対象の場合はクラスタ内またはセンサーについて Service Monitor が管理する電話機の数の確認もできます。

電話機カウントを管理するには、[Administration] > [Configuration] > [Inventory] を選択します。[Inventory] ページが表示され、次の表の情報が表示されます。

GUI の要素	説明
電話機ライセンス	
Used	Service Monitor がモニタしている電話機の数。電話機の数がライセンス サイズと同じ場合は、次のメッセージが赤色で表示されます。 `Total known phone count (n) has reached or exceeded licensed limit!`
Total	ライセンスで許可された電話機の数。
クラスタ/センサー リスト	
Cluster/Sensor ID	次のいずれか • Cluster ID：Unified Communications Manager により割り当てられたクラスタ ID。 • Sensor ID：センサー MAC アドレス。 • NAM：IP アドレス
Name	表示名（Service Monitor で設定されている場合）。
IP Address	IP アドレス。
Version	次のいずれか • Cisco 1040 のバイナリ イメージ ファイル名。 • NAM ソフトウェア バージョン。 • Unified Communications Manager ソフトウェア バージョン。

GUI の要素	説明
Type	次のいずれか • Cluster：Unified Communications Manager。 • NAM：ネットワーク解析モジュール センサー。 • 1040：Cisco 1040 センサー。
State	次のいずれか • Monitored：Service Monitor はこのクラスタまたはセンサーからデータを収集し、分析して、違反が発生した場合にはトラップを送信します。 • Suspended：Service Monitor は、次のいずれかの理由により、このクラスタまたはセンサーからのデータの収集と分析を行っていません。 – ユーザがクラスタまたはセンサーの状態を [Suspended] に設定した。「クラスタまたはセンサーのモニタリングの中断および再開」（P.3-15）を参照してください。 – 電話機ライセンス カウントに達したため、データを受信したときに Service Monitor が新たに作成されたクラスタまたはセンサーをモニタできなくなった。
Licensed Phone Count	クラスタ内に設定された電話機のうち、ライセンスされた電話機の数。
Total Phone Count	クラスタ内に設定された電話機の数。

クラスタまたはセンサーのモニタリングの中断および再開

Unified Communications Manager が正しく設定されていて、Service Monitor のライセンス数が上限を超えていない場合、Service Monitor はクラスタを認識するとそのクラスタのモニタを開始します。Unified Communications Manager クレデンシャルを Service Monitor に追加すると、Service Monitor はクラスタを認識します（詳細については、「データ ソース クレデンシャルの追加」（P.3-7）を参照してください）。

Service Monitor は次の時点でセンサーを認識します。

- Cisco 1040 センサーが登録される。
- NAM のクレデンシャルが Service Monitor に追加される。

別のクラスタまたはセンサーから電話機をモニタできるようにする場合など、必要に応じてクラスタまたはセンサーのモニタを中断することができます。

クラスタまたはセンサーの中断

クラスタまたはセンサーを中断すると、次のようになります。

- 中断されたクラスタまたはセンサーのデータは、Service Monitor レポートに表示されなくなります。
- [Inventory] ページに、クラスタまたはセンサーが中断したとして表示されます。

ステップ 1　[Administration] > [Configuration] > [Inventory] を選択します。

ステップ 2　中断するクラスタまたはセンサーのチェックボックスを選択します。

ステップ 3　[Suspend] をクリックします。確認用のダイアログボックスが表示されます。

ステップ 4　[OK] をクリックします。

クラスタまたはセンサーの再開

ステップ 1　[Administration] > [Configuration] > [Inventory] を選択します。

ステップ 2　中断されたクラスタまたはセンサーのうち、モニタ対象にするもののチェックボックスを選択します。

ステップ 3　[Resume] をクリックします。確認用のダイアログボックスが表示されます。

ステップ 4　[OK] をクリックします。

クラスタの電話機カウント合計の更新

電話機カウントはクラスタが追加されたときに定義されます。Service Monitor は、クラスタに登録された電話機の数を数え、各電話機に対してライセンスを適用します。夜間にデータ検出が実行された場合、または、クラスタのデバイスおよびクレデンシャル検出が手動で実行された場合に電話機カウントは更新されます。

Most-Impacted Endpoints レポートの設定

この手順は、次の項目を設定する場合に使用します。

- 実行時期（毎日、週に 1 回、またはオンデマンド）に関係なく、CVTQ およびセンサーの Most-Impacted Endpoints レポートに含めるエンドポイント数。
- エクスポートする Most-Impacted Endpoints レポート（CVTQ またはセンサー、あるいは両方）。Most-Impacted Endpoints レポートは、毎日または週に 1 回実行し、結果をカンマ区切りの値ファイル（CSV）または Portable Document Format（PDF）ファイルにエクスポートすることができます。レポートはサーバに保存することができます。また必要であれば、電子メールで自動的に送信するように設定できます。

（注）　PDF ファイルにエクスポートできるレコードの最大数は 2,000 です。CSV ファイルにエクスポートできるレコードの最大数は 30,000 です。詳細については、「診断レポート検索と CSV エクスポート制限の設定」（P.3-36）を参照してください。

ステップ 1　[Administration] > [Configuration] > [Export Settings] を選択します。[Export Settings]（Most-Impacted Endpoints の場合）ページが表示され、次の表の情報が示されます。

GUI の要素	説明 / 処理
[Number of Endpoints] フィールド	すべての（エクスポートまたは直接起動された）Most-Impacted Endpoints レポートに表示するエンドポイントの数を入力します。
[Daily at 1:00 AM] チェックボックス	レポートを毎日生成するには、次の中から少なくとも 1 つを選択します。 • [CSV] チェックボックス：レポートを CSV フォーマットで保存します。 • [PDF] チェックボックス：レポートを PDF フォーマットで保存します。 どちらも選択しない場合、Service Monitor はレポートを生成しません。

GUI の要素	説明 / 処理
[Weekly at 1:00 AM Monday] チェックボックス	レポートを毎週生成するには、次の中から少なくとも 1 つを選択します。 • [CSV] チェックボックス：レポートを CSV フォーマットで保存します。 • [PDF] チェックボックス：レポートを PDF フォーマットで保存します。 どちらも選択しない場合、Service Monitor はレポートを生成しません。
Report Type	次の中から少なくとも 1 つを選択します。 • Sensor • CVTQ **（注）** センサーおよび CVTQ データについて、別個のレポートが生成されます。レポート ファイル名については、表 3-2 を参照してください。
Save at	Service Monitor がインストールされているサーバ上のレポートの保存場所を入力します。デフォルトの場所が表示されています。 **注意** エクスポート設定でファイルを *NMSROOT* の外に保存するよう設定する場合は、Service Monitor サーバにログインし、[Export Settings] ページで入力したフォルダを作成し、ユーザ *casuser* フォルダに書き込みアクセス権限を設定する必要があります。この作業を行わないと、Service Monitor はエクスポート ファイルを作成できません（NMSROOT は、Service Monitor がインストールされている場所です。デフォルトの場所を使用する場合は、C:\Program Files\CSCOpx です）。
E-mail (to)	（オプション）1 つまたは複数の完全な電子メール アドレスをカンマで区切って入力します。 **（注）** サーバの処理の再開に関する通知を Service Monitor が送信できるように、別の電子メール アドレスを設定します（この設定を行わない場合、Service Monitor は通知をこのフィールドで定義されたアドレスに送信します）。詳細については、「E メール通知の受信者の設定」（P.6-8）を参照してください。
SMTP Server	（オプション）SMTP サーバを入力します。

E-mail (from)	（オプション）このフィールドは [Export Settings]（Most-Impacted Endpoints の場合）ページに表示されません。
	[From] フィールドに表示される E メール アドレスを設定するには、qovrExport.properties ファイルに対して次の手順を実行します。
	1. Service Monitor システムで、C:\Program Files\CSCOpx\qovr（インストレーション中にデフォルトの場所が選択された場合）に移動します。
	2. qovrExport.properties ファイルを開きます。
	3. qovrExport.properties ファイルで、EmailFrom=<email address> を追加します。
	4. ファイルを保存し、閉じます。
	5. QOVR プロセスを再起動します。コマンドラインから、次のコマンドを入力します。
	`pdterm QOVR`
	`pdexec QOVR`

ステップ 2　[Apply] をクリックします。

選択したレポートおよびフォーマットに応じて、次のレポートが生成されます。

表 3-2　エクスポートされた Most-Impacted Endpoints レポート

レポートのタイプ	生成時期	レポート ファイル名
CVTQ	毎日	CVTQ_Daily_ddmmyyyy.csv
		CVTQ_Daily_ddmmyyyy.pdf
	毎週	CVTQ_Weekly_ddmmyyyy.csv
	（注）　月曜日に生成。	CVTQ_Weekly_ddmmyyyy.pdf
Sensor	毎日	Sensor_Daily_ddmmyyyy.csv
		Sensor_Daily_ddmmyyyy.pdf
	毎週	Sensor_Weekly_ddmmyyyy.csv
	（注）　月曜日に生成。	Sensor_Weekly_ddmmyyyy.pdf

コール分類の設定

ここで説明する内容は、次のとおりです。

コール分類について

Service Monitor は次の目的でコール分類を使用します。

- CDR コール レポートでコールを分類する（詳細については、「CDR Call レポートの使用方法」（P.2-23）を参照してください）。
- 分類したコール データを Service Statistics Manager でのレポート生成に使用する（Service Statistics Manager がネットワーク上にインストールされている場合）。詳細については、『*User Guide for Cisco Unified Service Statistics Manager*』を参照してください。

Service Monitor は次のカテゴリのセットを使用してコールを分類します。

- System-defined：Service Monitor はコールを表 3-3 の基準を使用して分類します。詳細については「Service Monitor コールをシステム定義コール カテゴリに分類する方式について」（P.3-19）を参照してください。
- User-defined：Service Monitor はコールをシステム定義コール カテゴリ Internal または VG/Trunk-Outgoing に分類します。クラスタのユーザ定義ダイヤル プランが存在する場合、Service Monitor はこのプランを基準にコールを評価することもできます。「Service Monitor コー

ルをユーザ定義コール カテゴリに分類する方式について」（P.3-21）を参照してください。

1 件のコールが複数のコール カテゴリに属する場合があります。たとえば、音声ゲートウェイ経由での発信コールは VG/Trunk-Outgoing システム定義カテゴリに分類されます。同じコールが Long Distance コールとして分類される場合もあります。この場合、Service Monitor はこのコールを両方のカテゴリに登録します。このようなデータを CDR コール レポートで表示すると、該当するすべてのコール カテゴリがレポートに表示されます。詳細については「CDR Call レポートの生成」（P.2-23）および「CDR Call レポートについて」（P.2-28）を参照してください。

Service Monitor コールをシステム定義コール カテゴリに分類する方式について

Service Monitor は CDR や次のような Unified Communications Manager データを分析して、コールがシステム定義カテゴリに該当するかどうかを判別します。

- ソース エンドポイントとターゲット エンドポイントのデバイス タイプ。
- コールの方向（着信または発信）。
- プロトコル（H.323、MGCP、SIP）。

表 3-3 に、システム定義コール カテゴリのタイプと名前を示します。また、各カテゴリ タイプに該当するコールについても説明します。

表 3-3　システム定義コール カテゴリ

カテゴリ タイプ	説明	カテゴリ名
Voicemail	ボイスメールとの間でのコール。	Unity Voicemail：ボイスメール コールのシステム定義基準を満たすコール。Cisco Unity や Cisco Unity Connection との間で送受信されるコールなどが該当します。 **（注）** このカテゴリ タイプにユーザ定義のカテゴリ名を追加することができます。
Conference	会議システムとの間で送受信されるコール。	Conference Bridge：コンファレンス ブリッジを使用するコールのシステム定義基準を満たすコール。 **（注）** このカテゴリ タイプにユーザ定義のカテゴリ名を追加することができます。
ICT	クラスタ間トランク（ICT）との間で送受信されるコール。	• ICT GK Controlled：ゲートキーパーにより制御される ICT コール。 • ICT Non-GK Controlled：ゲートキーパーにより制御されない ICT コール。

表 3-3　システム定義コール カテゴリ （続き）

カテゴリ タイプ	説明	カテゴリ名
VG/Trunk-Outgoing	音声ゲートウェイまたはトランクへのコール。オフネット コールのみが対象となります（「オフネット コールとオンネット コールについて」（P.3-22）を参照）。 **（注）** ユーザ定義ダイヤル プランは、VG/Trunk-Outgoing コール カテゴリのコールに適用されます。詳細については、表 3-4 を参照してください。	• MGCP Gateway Outgoing : MGCP 音声ゲートウェイへのコール。 • H.323 Gateway Outgoing : H.323 音声ゲートウェイへのコール。 • H.323 Trunk Outgoing : H.323 トランクへのコール。 • SIP Trunk Outgoing : SIP トランクへのコール。
VG/Trunk-Incoming	音声ゲートウェイまたはトランクへのコール。オフネット コールのみが対象となります（「オフネット コールとオンネット コールについて」（P.3-22）を参照）。	• MGCP Gateway Incoming : MGCP 音声ゲートウェイからのコール。 • H.323 Gateway Incoming : H.323 音声ゲートウェイからのコール。 • H.323 Trunk Incoming : H.323 トランクからのコール。 • SIP Trunk Incoming : SIP トランクからのコール。
Tandem	タンデム コールは、両方のエンドポイントが音声ゲートウェイまたはトランクである場合に発生します。	Tandem
OnNet Trunk	一方のエンドポイントがトランクであり、オフネット コールではないコール（「オフネット コールとオンネット コールについて」（P.3-22）を参照）。 たとえば、トランクは WebEx または PBX への接続に使用することができます。	• OnNet H.323 Trunk • OnNet SIP Trunk
Internal	上記のどのカテゴリにも該当しないコール。たとえば、一方のエンドポイントが IP 電話で、もう一方のエンドポイントが音声ゲートウェイであり、オフネット コールではないコールなどが該当します（「オフネット コールとオンネット コールについて」（P.3-22）を参照）。	Internal
Unknown	システム関連の理由により、Service Monitor がエンドポイントのデバイス タイプを判別できませんでした。	不明

Service Monitor コールをユーザ定義コール カテゴリに分類する方式について

Service Monitor は次の場合に、コールがユーザ定義コール カテゴリに該当するか判別します。

- コールがすでに [Internal]、[VG/Trunk-Outgoing]、[OnNet Trunk] のいずれかに分類されている（「Service Monitor コールをシステム定義コール カテゴリに分類する方式について」（P.3-19）を参照）。
- ユーザ定義ダイヤル プランがコールが発生したクラスタに割り当てられている（「クラスタへのユーザ定義ダイヤル プランの割り当て」（P.3-30）を参照）。

ダイヤル プランには優先順位が設定されたダイヤル パターンのリストがあります。これらのダイヤル パターンには、次のコール カテゴリ タイプのいずれかからユーザ定義コール カテゴリ名を割り当てる必要があります。

- Conference：デフォルトのコール カテゴリ名はないため、ユーザが定義する必要があります。
- International：デフォルトのコール カテゴリ名は International です。
- Emergency：デフォルトのコール カテゴリ名は Emergency です。
- Local：デフォルトのコール カテゴリ名は Local です。
- Long Distance：デフォルトのコール カテゴリ名は Long Distance です。
- Service：デフォルトのコール カテゴリ名は Service です。
- Toll Free：デフォルトのコール カテゴリ名は Toll Free です。
- Voicemail：デフォルトのコール カテゴリ名はないため、ユーザが定義する必要があります。

（注）　詳細については、「ユーザ定義コール カテゴリの管理」（P.3-29）を参照してください。

表 3-4 に、ダイヤル パターンをユーザ定義ダイヤル プランから Internal、VG/Trunk-Outgoing、または OnNet Trunk コール カテゴリのコールに割り当てる方法を示します。

表 3-4　ダイヤル パターンを VG/Trunk-Outgoing、Internal、OnNet Trunk コールに割り当てる方法

Service Monitor が適用するダイヤル パターンのカテゴリ	適用先の電話番号の種類	対象となるコールのシステム定義カテゴリ
• Conference • Emergency • International • Local • Long Distance • Service • Toll Free • Voicemail	宛先	VG/Trunk-Outgoing
• Conference • Voicemail	ソース	
• Conference • Voicemail	• ソース • 宛先	• Internal • OnNet Trunk

オフネット コールとオンネット コールについて

少なくとも一方のエンドポイントがゲートウェイまたはトランクで、そのエンドポイントが次のいずれかを満たす場合、コールはオフネットと見なされます。

- Unified Communications Manager（Administration）で、[Call Classification] パラメータがゲートウェイの設定またはトランクの設定で [Offnet] に設定されている。
- Unified Communications Manager で、次の両方が満たされている。
  - [Call Classification] パラメータがゲートウェイの設定またはトランクの設定で [System Default] に設定されている。
  - [System Default] サービス パラメータが [Offnet] に設定されている。
- エンドポイントがアナログ ゲートウェイである。

オフネット コールの基準を満たさないコールはすべてオンネット コールと見なされます。

ユーザ定義ダイヤル プランの設定

ダイヤル プランには一意の名前が必要です。フリーダイヤル番号のセットを登録することもできますが、ダイヤル パターンのセットを必ず登録する必要があります。ダイヤル パターンではコール カテゴリの名前とタイプが識別されています。ダイヤル パターンで指定されているルールまたはパターンと電話番号が一致すると、コールは該当するカテゴリに分類されます。

Service Monitor には、ユーザが独自にダイヤル プランを定義するための基礎となるデフォルト ダイヤル プランがあります。デフォルト ダイヤル プランには、デフォルトのダイヤル パターン（コール カテゴリの名前、タイプ、ルール）があります。ダイヤル プランの設定時には、コール カテゴリを更新して、デフォルト ダイヤル プランで指定されているルールの追加、変更、削除を行うことができます。詳細については、「デフォルト ダイヤル プランについて」（P.3-24）を参照してください。

ダイヤル プランは複数作成することができます。1 つのクラスタに割り当てることができるダイヤル プランは 1 つだけですが、同じダイヤル プランを複数のクラスタに割り当てることはできます。ダイヤル プランの管理方法については、次を参照してください。

- ダイヤル プランを追加する場合、次のいずれかのデータを使用することができます。
  - 既存のダイヤル プラン：「ダイヤル プランのコピー」（P.3-22）を参照してください。
  - デフォルト ダイヤル プラン：「ダイヤル プランの追加」（P.3-23）を参照してください。
- ダイヤル プランの編集については、「ダイヤル プランの編集」（P.3-26）を参照してください。
- ダイヤル プランの削除については、「ダイヤル プランの削除」（P.3-26）を参照してください。
- ダイヤル プランの割り当てについては、「クラスタへのユーザ定義ダイヤル プランの割り当て」（P.3-30）を参照してください。

ダイヤル プランのコピー

最初に既存のダイヤル プランをコピーして新しいダイヤル プランを定義するには、次の手順を実行します。

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Dial Plan Configuration] を選択します。

[Dial Plan Configuration] ページが表示されます。

ステップ 2　ダイヤル プランを選択して、[Copy] をクリックします。[Add Dial Plan] ウィンドウが表示されます。

ステップ 3　次の表に説明するデータを更新します。

フィールド	説明
Dial Plan Name	ダイヤル プラン名を入力します（「Copy of *ダイヤル プラン名*」を書き換えます）。
テーブルの各行はダイヤル パターンを表します。ダイヤル パターンの内容は次の各カラムで示されています。 • Condition • No.of Chars • Pattern • Call Category	ダイヤル パターンを追加、編集、または削除することによって、ダイヤル プランを更新します。詳細については、次の説明を参照してください。 • 「ダイヤル プランへのダイヤル パターンの追加」（P.3-27）。 • 「ダイヤル プランのダイヤル パターンの編集」（P.3-28）。 • 「ダイヤル プランからのダイヤル パターンの削除」（P.3-28）。 **（注）** ダイヤル パターンを追加すると、優先レベルが最下位になります。ダイヤル パターンの優先レベルを変更するには、この表の「[Priority] カラム」を参照してください。
[Priority] カラム	適用する順序にしたがってダイヤル パターンに番号を設定します。1 が最上位の優先レベルです。
Toll-Free Numbers	フリーダイヤル番号をカンマで区切って入力します。

ステップ 4　ダイヤル プランを設定の途中で保存するには、[Apply] をクリックします。

ステップ 5　ダイヤル プランを保存して設定を完了するには、[OK] をクリックします。[Dial Plan Configuration] ページが表示されます。

ダイヤル プランの追加

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Dial Plan Configuration] を選択します。

[Dial Plan Configuration] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- 既存のダイヤル プランを選択して [Copy] をクリックする。
- [Add] をクリックして、デフォルト ダイヤル プランに基づきダイヤル プランを追加する（詳細については、「デフォルト ダイヤル プランについて」（P.3-24）を参照してください）。

[Add Dial Plan] ページが表示され、ダイヤル プランが表示されます。

ステップ 3　次の表に示すデータを入力します。

フィールド	説明
Dial Plan Name	ダイヤル プラン名を入力します。
テーブルの各行はダイヤル パターンを表します。ダイヤル パターンの内容は次の各カラムで示されています。 • Condition • No.of Chars • Pattern • Call Category	ダイヤル パターンを追加、編集、または削除することによって、ダイヤル プランを更新します。詳細については、次の説明を参照してください。 • 「ダイヤル プランへのダイヤル パターンの追加」（P.3-27）。 • 「ダイヤル プランのダイヤル パターンの編集」（P.3-28）。 • 「ダイヤル プランからのダイヤル パターンの削除」（P.3-28）。 （注）　ダイヤル パターンを追加した後、優先レベルを更新します。この表の「[Priority] カラム」を参照してください。
[Priority] カラム	[Priority] カラムに適用する順序にしたがってダイヤル パターンに番号を設定します。1 が最上位の優先レベルです。
Toll-Free Numbers	フリーダイヤル番号をカンマで区切って入力します。

ステップ 4　ダイヤル プランを設定の途中で保存するには、[Apply] をクリックします。

ステップ 5　ダイヤル プランを保存して設定を完了するには、[OK] をクリックします。[Dial Plan Configuration] ページが表示されます。

デフォルト ダイヤル プランについて

ダイヤル プランの追加時に、デフォルト ダイヤル プランのコピーが表示され、更新できるようになります。次の作業を実行します。

- 独自のコール カテゴリ名を定義する。ただし、コール カテゴリのタイプは表 3-5 に記載されているものの中から選択する必要があります。
- ダイヤル パターンを追加、更新、または削除する（表 3-5 の各行はダイヤル パターンを表しています）。

ダイヤル プランの設定中の変更は、デフォルト ダイヤル プランには影響しません。デフォルト ダイヤル プランは North American Numbering Plan（NANP; 北米番号計画）に基づいています。

表 3-5 にデフォルト ダイヤル プランの値を示します。

表 3-5　デフォルト ダイヤル プランの値

条件	文字数	デフォルト パターン	コール カテゴリ名	コール カテゴリタイプ	説明	プライオリティ
>	3	011!	International	International	ダイヤルされた番号が 3 桁より長く、011 で始まっている場合は、このコールは International として分類されます。	1
=	7	!	Local	Local	ダイヤルされた番号が 7 桁で、パターンが！（1 桁より長い。ここでは 7 桁）の場合、このコールは Local として分類されます。	2

表 3-5　デフォルト ダイヤル プランの値 （続き）

条件	文字数	デフォルト パターン	コール カテゴリ名	コール カテゴリタイプ	説明	プライオリティ
=	10	T!	Toll Free[1]	Toll Free	ダイヤルされた番号が 10 桁で、パターンが T!（1 桁より長い。ここでは、ダイヤル プランで定義されているフリーダイヤル番号のいずれかで始まる 10 桁の番号）の場合、このコールは Toll Free として分類されます。 （注）　Service Monitor でフリーダイヤル番号を定義するには、「ユーザ定義ダイヤル プランの設定」（P.3-22）を参照してください。	3
=	10	G!	Local[2]	Local	ダイヤルされた番号が 10 桁で、パターンが G!（1 桁より長い。ここでは、Service Monitor で定義されているゲートウェイ コードのいずれかで始まる 10 桁の番号）の場合、このコールは Local として分類されます。	4
=	10	!	Long Distance	Long Distance	ダイヤルされた番号が 10 桁で、パターンが !（1 桁より長い。ここでは 10 桁の番号）の場合、コールは Long Distance として分類されます。	5
=	11	T!	Toll Free[1]	Toll Free	ダイヤルされた番号が 11 桁で、パターンが T!（1 桁より長い。ここでは、ダイヤル プランで定義されているフリーダイヤル番号のいずれかで始まる 11 桁の番号）の場合、このコールは Toll Free として分類されます。 （注）　Service Monitor でフリーダイヤル番号を定義するには、「ユーザ定義ダイヤル プランの設定」（P.3-22）を参照してください。	6
=	11	XG!	Local	Local	ダイヤルされた番号が 11 桁で、パターンが XG!（1 桁より長い。ここでは、任意の 1 桁で始まり、その直後に Service Monitor で定義されているゲートウェイ コードのいずれかがある 11 桁の番号）の場合、このコールは Local として分類されます。	7
=	11	!	Long Distance	Long Distance	ダイヤルされた番号が 11 桁で、パターンが !（1 桁より長い。ここでは 11 桁の番号）の場合、コールは Long Distance として分類されます。	8

1. クラスタに割り当てられているダイヤル プランに当該のフリーダイヤル番号が登録されている場合、このコールは Toll Free として分類されます（「ユーザ定義ダイヤル プランの設定」（P.3-22）を参照）。
2. Service Monitor は定義されたゲートウェイ コードを使用します（『Managing Gateway Codes』を参照）。

ダイヤル プランの編集

ダイヤル プラン名を編集するには、ダイヤル プランをコピーし、目的の名前を設定して、新しいダイヤル プランを保存し、以前のダイヤル プランを削除します（「ダイヤル プランのコピー」（P.3-22）と「ダイヤル プランの削除」（P.3-26）を参照）。

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Dial Plan Configuration] を選択します。

ステップ 2　ダイヤル プランを選択し、[Edit] をクリックします。[Edit Dial Plan] ウィンドウが表示されます。

ステップ 3　次の表に示すデータを入力します。

フィールド	説明
Dial Plan Name	変更できないため、グレー表示されています。
テーブルの各行はダイヤル パターンを表します。ダイヤル パターンの内容は次の各カラムで示されています。 • Condition • No.of Chars • Pattern • Call Category	ダイヤル パターンを追加、編集、または削除することによって、ダイヤル プランを更新します。詳細については、次の説明を参照してください。 • 「ダイヤル プランへのダイヤル パターンの追加」（P.3-27）。 • 「ダイヤル プランのダイヤル パターンの編集」（P.3-28）。 • 「ダイヤル プランからのダイヤル パターンの削除」（P.3-28）。 **（注）**　ダイヤル パターンを追加すると、優先レベルが最下位になります。ダイヤル パターンの優先レベルを変更するには、この表の「[Priority] カラム」を参照してください。
[Priority] カラム	適用する順序にしたがってダイヤル パターンに番号を設定します。1 が最上位の優先レベルです。
Toll-Free Numbers	フリーダイヤル番号をカンマで区切って入力します。

ステップ 4　ダイヤル プランを設定の途中で保存するには、[Apply] をクリックします。

ステップ 5　ダイヤル プランを保存して設定を完了するには、[OK] をクリックします。[Dial Plan Configuration] ページが表示されます。

ダイヤル プランの削除

（注）　ダイヤル プランに割り当てられているクラスタがある場合、ダイヤル プランは削除できません（「クラスタへのユーザ定義ダイヤル プランの割り当て」（P.3-30）を参照）。

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Dial Plan Configuration] を選択します。

ステップ 2　ダイヤル プランを選択します。

ステップ 3　[Delete] をクリックします。確認ウィンドウが表示されます。

ステップ 4　[OK] をクリックします。

ユーザ定義ダイヤル プランでのダイヤル パターンの設定

ダイヤル プランの設定時にダイヤル パターンを管理するには、次の手順を実行します。

- 「ダイヤル プランへのダイヤル パターンの追加」（P.3-27）
- 「ダイヤル プランのダイヤル パターンの編集」（P.3-28）
- 「ダイヤル プランからのダイヤル パターンの削除」（P.3-28）

ダイヤル プランへのダイヤル パターンの追加

追加または編集中のダイヤル プランに、ダイヤル パターンを追加できます。

ステップ 1　[Add Dial Plan] または [Edit Dial Plan] ページで [Add] をクリックします。[Add Dial Pattern] ダイアログ ボックスが表示されます。

ステップ 2　次の各フィールドにデータを入力して、ダイヤル パターンを作成します。

- Condition：文字数に適用されます。いずれかを選択します。
  - 左矢印（<）：未満
  - 右矢印（>）：より大きい
  - 等号記号（=）：等しい
- Number of Chars：数字と、プラス（+）、ポンド（#）、アスタリスク（*）、カンマ（,）、およびアットマーク（@）などの数字以外の文字数の合計数を入力します。

  ダイヤル パターンが適用される電話番号の文字数を表します。
- Pattern：数字に対して適用するパターンを次のように入力します。
  - G は数字がゲートウェイ コードを表していることを示します（詳細については、「ゲートウェイ コードの管理」（P.3-31）を参照してください）。
  - T が設定されている場合、Service Monitor は数字をダイヤル プランのフリーダイヤル番号と比較します。
  - ! は複数桁の数値（1234 や 5551234 のように、長さが 1 桁より長い数値）を示します。
  - X は 1 桁の数値（0、1、または 9 など）を示します。
- Call Category Name：次のいずれかのオプション ボタンを選択し、必要に応じてデータを入力します。
  - Existing：既存のカテゴリ名を選択します。
  - New：一意の名前を入力し、コール カテゴリのタイプを選択します。

ステップ 3　[OK] をクリックします。[Add Dial Pattern] ダイアログ ボックスが閉じます。

詳細については、次の項を参照してください。

- 「ダイヤル プランの追加」（P.3-23）
- 「ダイヤル プランの編集」（P.3-26）

ダイヤル プランのダイヤル パターンの編集

ダイヤル プランの追加時や編集時に、そのダイヤル プランにあるダイヤル パターンを編集することができます。

（注）　ダイヤル パターンの編集時にコール カテゴリ名は変更できません。コール カテゴリ名を変更するには、ダイヤル パターンを削除してからそのダイヤル パターンを再度追加します（「ダイヤル プランからのダイヤル パターンの削除」（P.3-28）および「ダイヤル プランへのダイヤル パターンの追加」（P.3-27）を参照）。

ステップ 1　[Add Dial Plan] または [Edit Dial Plan] ページで [Edit] をクリックします。[Edit Dial Pattern] ダイアログ ボックスが表示されます。

ステップ 2　次のフィールドのデータを必要に応じて更新します。

- Condition：文字数に適用されます。いずれかを選択します。
  - 左矢印（<）：未満
  - 右矢印（>）：より大きい
  - 等号記号（=）：等しい
- Number of Chars：数字と、プラス（+）、ポンド（#）、アスタリスク（*）、カンマ（,）、およびアットマーク（@）などの数字以外の文字数の合計数を入力します。
- Pattern：コールの分類に使用するパターンを次のように入力します。
  - G は数字がゲートウェイ コードを表していることを示します（詳細については、「ゲートウェイ コードの管理」（P.3-31）を参照してください）。
  - T が設定されている場合、Service Monitor は数字をダイヤル プランのフリーダイヤル番号と比較します。
  - ! は複数桁の数値（1234 や 5551234 のように、長さが 1 桁より長い数値）を示します。
  - X は 1 桁の数値（0、1、または 9 など）を示します。

  「デフォルト ダイヤル プランについて」（P.3-24）の例を参考にしてください。
- Call Category Name：このフィールドは変更できないため、グレー表示されています。

ステップ 3　[OK] をクリックします。[Edit Dial Pattern] ダイアログ ボックスが閉じます。

ダイヤル プランからのダイヤル パターンの削除

ダイヤル プランの追加時や編集時に、そのダイヤル プランにあるダイヤル パターンを削除することができます。

ステップ 1　[Add Dial Plan] または [Edit Dial Plan] ページで削除するダイヤル パターンを選択します。

ステップ 2　[Delete] をクリックします。

ステップ 3　ダイヤル プランを保存するには、次のいずれかを実行します。

- ダイヤル プランを保存してその後も [Add Dial Plan] または [Edit Dial Plan] ページで作業を続行する場合は、[Apply] をクリックします。
- ダイヤル プランを保存して [Dial Plan Configuration] ウィンドウに戻る場合は、[OK] をクリックします。

ユーザ定義コール カテゴリの管理

ユーザ定義コール カテゴリにより、ダイヤル パターンに有意な名前が設定されます。コール カテゴリ名を追加または編集する場合、選択できるのは次のコール カテゴリ タイプのみです。

- Conference
- Emergency
- International
- Local
- Long Distance
- Service
- Toll Free
- Voicemail

コール カテゴリ タイプはあらかじめ定義されていて、変更できません。

ダイヤル パターンをダイヤル プランに追加するときに、コール カテゴリ名を作成することができます（「ダイヤル プランへのダイヤル パターンの追加」（P.3-27）を参照）。また、次の各トピックの手順を実行すると、コール カテゴリ名の追加、更新、削除ができます。

- 「コール カテゴリ名の追加」（P.3-29）
- 「コール カテゴリ名の編集」（P.3-30）
- 「コール カテゴリ名の削除」（P.3-30）

コール カテゴリ名の追加

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Call Category] を選択します。[Call Category Configuration] 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 Call Category] ダイアログ ボックスが表示されます。

ステップ 3　次のフィールドにデータを入力します。

- Call Category Name：一意の名前を入力します。
- Call Category Type：いずれかを選択します（詳細については、「ユーザ定義コール カテゴリの管理」（P.3-29）を参照してください）。

ステップ 4　[OK] をクリックします。コール カテゴリをダイヤル パターンで使用できるようになります。

コール カテゴリ名の編集

（注）　コール カテゴリ名とコール カテゴリ タイプの両方を変更するには、新しいコール カテゴリを追加します（「コール カテゴリ名の追加」（P.3-29）を参照）。

コール カテゴリ名を変更するには、次の手順を実行します。

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Call Category] を選択します。[Call Category Configuration] ページが表示されます。

ステップ 2　コール カテゴリを選択して [Edit] を選択します。[Edit Call Category] ダイアログ ボックスが表示されます。

ステップ 3　[Call Category Name] フィールドに一意の名前を入力します（[Call Category Type] は編集できないため、グレー表示されています）。

ステップ 4　[OK] をクリックします。更新されたコール カテゴリをダイヤル パターンで使用できるようになります。

コール カテゴリ名の削除

（注）　コール カテゴリを削除できるのは、そのコール カテゴリがどのダイヤル プランでも使用されていない（ダイヤル パターンと関連付けられていない）場合のみです。

コール カテゴリを削除するとコール カテゴリ名も削除されますが、コール カテゴリ タイプには影響しません。

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Call Category] を選択します。[Call Category Configuration] ページが表示されます。

ステップ 2　コール カテゴリを選択して [Delete] を選択します。確認メッセージが表示されます。

ステップ 3　[OK] をクリックします。

クラスタへのユーザ定義ダイヤル プランの割り当て

同じダイヤル プランをすべてのクラスタに割り当てることができます。また、Service Monitor に追加された各クラスタにそれぞれ異なるダイヤル プランを割り当てることもできます。クラスタを追加する方法については、「データ ソース クレデンシャルの概要と設定」（P.3-2）を参照してください。

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Dial Plan Assignment] を選択します。Service Monitor に追加されたクラスタのリストが表示されます。

ステップ 2　[Assign New Dial Plan] カラムで、ダイヤル プランを選択するか、[None for any cluster] を選択します。

（注）　ダイヤル プランをクラスタに割り当てるには、少なくとも 1 つのダイヤル プランが設定されている必要があります（「ユーザ定義ダイヤル プランの設定」（P.3-22）を参照）。

ステップ 3　[Update Dial Plan Assignment] をクリックして割り当てを保存します。

ゲートウェイ コードの設定

Service Monitor は設定したゲートウェイ コードを使用して外部コールのコール分類（ローカルか長距離か、など）を判別します。

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Gateway Code] を選択します。[Gateway Code Summary] ページが開き、次の情報が表示されます。

- Cluster ID：Unified Communications Manager で割り当てられているクラスタの ID。
- Gateway Code Summary：Service Monitor でゲートウェイ コードが設定されているゲートウェイの数と、クラスタ内のゲートウェイの数。

（注）　Service Monitor がクラスタ内のゲートウェイを確認した最新の時点を確認する方法については、「データ ソース クレデンシャルの概要と設定」（P.3-2）を参照してください。

ステップ 2　ゲートウェイ コードを設定するには、クラスタを選択して、[Manage Gateway Code] をクリックします。[Manage Gateway Code] ページが表示されます。詳細については、「ゲートウェイ コードの管理」（P.3-31）を参照してください。

ステップ 3　ゲートウェイ コードがすでに設定されているゲートウェイを表示するには、クラスタを選択して [View] をクリックします。ゲートウェイ コード設定レポートが開きます。詳細については、「ゲートウェイ コード設定レポートについて」（P.3-33）を参照してください。

ゲートウェイ コードの管理

[Manage Gateway Code] ウィンドウを開く方法については、「ゲートウェイ コードの設定」（P.3-31）を参照してください。[Manage Gateway Code] ウィンドウに、表 3-6 の情報が表示されます。

表 3-6　[Manage Gateway Code] ウィンドウ

フィールドまたはボタン	説明 / 処理
[Cluster ID] フィールド	選択したクラスタの ID。
[Gateway Code] フィールド	ゲートウェイ コードを入力します。
[Filtered by] フィールド	使用中のフィルタ。テーブルに表示されるゲートウェイのリストが生成されます。
[Gateway Name] テーブル カラム	名前または IP アドレス。
[Route Group] テーブル カラム	名前（ゲートウェイが Unified Communications Manager のルート グループに所属していない場合は空白）。
[Gateway Code] テーブル カラム	Service Monitor でゲートウェイに設定されている市外局番。コードが設定されていない場合は空白です。
[Search] ボタン	表示するゲートウェイを制御するフィルタを更新します。
[Apply] ボタン	変更を保存します。

ゲートウェイ コードの追加、編集、削除を行うには、次の項を参照してください。

- 「設定するゲートウェイの検索」（P.3-32）
- 「ゲートウェイ コードの更新」（P.3-32）

設定するゲートウェイの検索

目的のゲートウェイが [Manage Gateway Code] ページに表示されない場合、次の手順を実行してゲートウェイを検索し、[Manage Gateway Code] ページに表示します。

ステップ 1　[Search] をクリックします。[Search Criteria] ダイアログ ボックスが表示され、次のフィールドが表示されます。

- Cluster Name：選択されたクラスタ。このフィールドは編集できません。
- Route Group
- Gateway Name
- Gateway Code

ステップ 2　次のようにデータを入力します。

- 特定のゲートウェイを検索するには、ゲートウェイ名のみを入力します。
- 特定のルート グループに属するゲートウェイを検索するには、ルート グループ名のみを入力します。
- クラスタ内のすべてのゲートウェイを検索するには（リストが長くなる場合があります）、すべての入力フィールドを空白にします。
- 特定のゲートウェイ コードがすでに設定されているすべてのゲートウェイを検索するには、ゲートウェイ コードのみを入力します。

ステップ 3　[Search] をクリックします。[Manage Gateway Code] ページが再度表示されます。テーブルの上にある [Filter by] 情報が更新され、検索条件に一致するゲートウェイがテーブルに追加されます。

（注）　Service Monitor がクラスタ内のゲートウェイのリストを最後に更新した時点に関する詳細については、「データ ソース クレデンシャルの概要と設定」（P.3-2）を参照してください。

ステップ 4　ゲートウェイ コードを更新する方法については、「ゲートウェイ コードの更新」（P.3-32）を参照してください。

ゲートウェイ コードの更新

デフォルトでは、Service Monitor ではゲートウェイ コードは設定されておらず、[Manage Gateway Code] ページに表示されるのは、ゲートウェイ コードが設定されているゲートウェイのみです（ゲートウェイの表示に使用する基準は、テーブルの上の [Filter by] 情報で確認できます）。目的のゲートウェイが [Manage Gateway Code] ページに表示されていない場合については、「設定するゲートウェイの検索」（P.3-32）を参照してください。

ゲートウェイのゲートウェイ コードを追加、更新、または削除するには、次の手順を実行します。

ステップ 1　1 つ以上のゲートウェイを選択します。

ステップ 2　コードをカンマ区切りで [Gateway Code] フィールドに入力します。このとき、次の点に注意してください。

- [Gateway Code] フィールドに値を入力すると、設定済みのゲートウェイコードがすべて置き換えられます。
- [Gateway Code] フィールドを空白にすると、設定済みのゲートウェイコードはすべて削除されます。

ステップ 3　[Apply] をクリックします。変更が保存され、[Manage Gateway Code] ページに反映されます。

ステップ 4　[Close] をクリックします。[Gateway Code Summary] ページに戻ります。

ゲートウェイ コード設定レポートについて

ゲートウェイ コード設定レポートには、選択されているクラスタについて、Service Monitor でゲートウェイ コードが設定されているゲートウェイのみが表示されます。このレポートに表示される情報は次のとおりです。

- Cluster ID：選択されたクラスタの名前。
- Gateway Name：DNS 名または IP アドレス。
- Route Group：ルート グループ名。ゲートウェイが Unified Communications Manager のルート グループに属していない場合は空白です。
- Gateway Code：Service Monitor で設定されたゲートウェイ コードのカンマ区切りのリスト。

トランク利用率の設定

トランクの最大容量（最大同時コール数）およびゲートウェイの最大容量（最大チャネル数）を設定できます。特定のトランクまたはゲートウェアに最大容量を設定することも、CSV ファイルを使用してすべてのクラスタのトランク利用率設定データをインポートすることもできます。

トランクまたはゲートウェイの最大容量の設定

ステップ 1　[Administration] > [Configuration] > [Trunk Utilization] を選択します。[Trunk Utilization Configuration] ページが表示されます。

ステップ 2　クラスタを選択します。

ステップ 3　次のゲートウェイまたはトランクの種類のいずれかを選択します。

- MGCP Gateway：デフォルト設定を使用して自動的に設定されます。
- H.323 Gateway：自動的には設定されません。
- H.225 Trunk：自動的には設定されません。
- SIP Trunk：自動的には設定されません。
- Intercluster Trunk：自動的には設定されません

ステップ 4　ゲートウェイまたはトランクの種類を選択し、[Configure Maximum Capacity] をクリックします。対応する [Maximum Capacity Configuration] ページが表示されます。

ステップ 5　[Configure Channels]（または [Configure Concurrent Calls]）フィールドに最大容量を入力します。

ステップ 6　設定を適用するゲートウェイまたはトランクを選択します。

ステップ 7　[Apply] をクリックします。

ステップ 8　[Close] をクリックします。

すべてのクラスタのトランク利用率データのインポートおよびエクスポート

ヒント　設定ファイルを作成する最も簡単な方法は、エクスポート機能を使用してファイルにエクスポートすることです。続いて、必要に応じてファイルのデータを変更します。すべてのゲートウェイおよびトランクがファイルに示されているため、ファイルに値を入力するだけです。

ステップ 1　[Administration] > [Configuration] > [Trunk Utilization] を選択します。[Trunk Utilization Configuration] ページが表示されます。

ステップ 2　クラスタを選択します。

ステップ 3　[Bulk Import]（または [Bulk Export]）をクリックします。[Import (Export) Trunk Utilization Configuration] ダイアログ ボックスが表示されます。

ステップ 4　CSV ファイルの場所を参照して選択し、[Import]（または [Export]）をクリックします。データがインポートまたはエクスポートされます。

その他の設定項目の設定と表示

この手順は、次の目的で使用します。

- ユーザ インターフェイス外で設定された設定を表示する（「診断レポート検索と CSV エクスポート制限の設定」（P.3-36）と「低ボリューム スケジュールおよびデータ消去の設定」（P.6-2）を参照）。
- Unified Communications Manager バージョン 5.x 以降からのコールをモニタする場合に SFTP 設定を設定する（Service Monitor がサポートしている Unified Communications Manager ソフトウェア バージョンについては、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください）。

ステップ 1　[Administration] > [System Settings] > [Other Settings] を選択します。[Other Settings] ページが表示されます。

ステップ 2　設定を表示し、次の表の説明に従い SFTP 設定を更新します。

フィールド	説明 / 処理
Low-Volume Schedule Hours	
< 曜日 > < 時間範囲 >; < 時間範囲 > 例： Mon 0-6; 22-24	各曜日について、時間範囲は Service Monitor が処理するレコードが少なくなる時間帯を表します。この時間帯に処理されるレコード数は、ピーク時に処理されるレコード数の約 20% となります。少量スケジュールの期間中、Service Monitor はデータベースのメンテナンスを実行します。 **（注）**　このスケジュールを設定できるのは、Service Monitor サーバへのアクセス権がある Windows ユーザです。「低ボリューム スケジュールおよびデータ消去の設定」（P.6-2）を参照してください。
Miscellaneous	
Wait for Diagnostic Report (min)	データが大量である場合、Service Monitor による検索時にここで指定した時間が経過すると、その時点までに検出された一致レコードが診断レポート（センサー レポートまたは CVTQ レポート）用に表示されます。この設定項目を設定するには、「診断レポート検索と CSV エクスポート制限の設定」（P.3-36）を参照してください。

フィールド	説明 / 処理

Report Data Retention Period (days)	データが Service Monitor データベースに保持される日数。この日数が経過すると、データは消去されます。デフォルト値は設定によって異なります。
	• サーバに Service Monitor が単独で設定されている場合：7 日間。
	• サーバに Service Monitor と Operations Manager が設定されている場合：3 日間。
	Service Monitor サーバでは、ユーザが *NMSROOT*\qovr\qovrconfig.properties ファイルの data-retention-days プロパティの値を変更することができます（NMSROOT は Service Monitor がインストールされている場所です。デフォルトの場所は C:\Program Files\CSCOpx です）。qovrconfig.properties を編集した後に変更を反映するには、QOVR プロセスを停止して再開する必要があります。Service Monitor がインストールされているサーバにログインしている状態で、コマンド ラインから次のコマンドを入力します。
	`pdterm QOVR`
	`pdexec QOVR`

Operations Manager サーバ	Service Monitor が登録されている Operations Manager の IP アドレスを入力します。 **（注）** Operations Manager と Service Monitor が同じシステムで実行されている場合でも、デフォルト値（localhost）を正しい IP アドレスに置き換える必要があります。 IP アドレスを入力すると、ユーザが Service Monitor のレポートから Operations Manager の [Detailed Device View] ページまたは [Phone Detail] ウィンドウを起動できるようになります（「センサー診断レポートについて」（P.2-8）と「CVTQ 診断レポートについて」（P.2-17）を参照）。 **（注）** ユーザが Operations Manager にログインしなくても Operations Manager のウィンドウを表示できるようにするには、シングル サインオンを設定します。詳細については、Common Services のオンライン ヘルプの「Enabling Single Sign-On」を参照してください。 **（注）** Common Services のオンラインヘルプは、[Administration] タブにある、[Common Services] ページを使用することでのみ利用できます。Common Services のオンライン ヘルプにアクセスするには、次の手順を使用します。[Administration] > [Server Administration (Common Services)] > [Security] を選択します。[Setting up Security] ページが表示されます。[Help] をクリックします。
SFTP	
Username	ユーザ名は smuser から変更できません。 同じユーザ名（smuser）が Unified Communications Manager に設定されている必要があります。「ビリング サーバとしての Service Monitor の Unified Communications Manager 5.x 以降への追加」（P.B-4）を参照してください。

フィールド	説明 / 処理
[Change password] チェックボックス	パスワードを変更するときに選択します。 **注意** デフォルトのパスワードは smuser です。ここでパスワードを変更した場合は、Unified Communications Manager の smuser のパスワードも変更する必要があります。「ビリング サーバとしての Service Monitor の Unified Communications Manager 5.x 以降への追加」（P.B-4）を参照してください。
Password	パスワードを入力します。
Re-enter password	パスワードを再入力します。

ステップ 3　[Apply] をクリックします。

診断レポート検索と CSV エクスポート制限の設定

表 3-7 は診断レポートに関連するプロパティの一覧です。*NMSROOT*\qovr\qovrconfig.properties ファイルでこれらのプロパティの値を変更できるのは、Service Monitor サーバへのアクセス権がある Windows ユーザです。

（注） NMSROOT は、Service Monitor がインストールされている場所です。デフォルトの場所を使用した場合は、C:\Program Files\CSCOpx です。

表 3-7　診断レポートとエクスポートの設定

プロパティ	説明と制限値
WaitForDiagReport	データが大量である場合、Service Monitor による検索時にここで指定した時間が経過すると、その時点までに検出された一致レコードが診断レポート（センサー レポートまたは CVTQ レポート）用に表示されます。 デフォルト：2。 最大値：4。 **（注）** Service Monitor のレポートには、最大 2,000 件のレコードを表示できます。これより多くのレコードを表示するには、診断レポートを CSV ファイルにエクスポートします。
ExportCSVLimit	Service Monitor が CSV ファイルにエクスポートするレコードの数。最大数は 30,000 です。

qovrconfig.properties を編集した後、変更を有効にするには、QOVR プロセスを停止してから開始する必要があります。Service Monitor がインストールされているサーバにログインしている状態で、コマンド ラインから次のコマンドを入力します。

```
pdterm QOVR
pdexec QOVR
```