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）がインストールされ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 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 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、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。

Common Services Local ログイン モジュール認証ロール

Common Services ログイン モジュールでは、固有の認証メカニズムである Common Services Local ログイン モジュール以外の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、Common Services 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 つめのロールである 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 : Common Services Local ログイン モジュール	
Help Desk	Service Monitor および Common Services の一部の情報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	特権はありません（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	すべての Service Monitor タスクおよび一部の Common Services タスク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	すべての Service Monitor タスクおよび複数の Common Services タスク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	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。
ACS モード	
Super Admin	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 Common Services ログイン モジュールが ACS に設定されている場合にだけ、ユーザをこのロール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を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（[Administration] > [Server Administration (Common Services)] > [Reports] > [Permission Report] > [Generate Report] の順に選択します）。

（注）　詳細については、Common Services のオンライン ヘルプを参照してください。

デフォルトの Common Services ロールを変更しないことを推奨します。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 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、Common Services オンライン ヘルプの「Setting up system identity account」のトピック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（「Common Services 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 Common Services 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（[Administration] > [Server Administration (Common Services)] > [Security] > [Multi-Server Trust Management] > [System Identity Setup] の順に選択します）。

詳細については、Common Services のオンライン ヘルプを参照してください。

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。
   - 入力する共有秘密キーを書き留めます。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
   - Common Services

以前の各タスクを実行する方法については、Common Services のオンライン ヘルプを参照してください。

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-3）にあるタスクを完了してください。

ステップ 1　[Administration] > [Server Administration (Common Services)] > [Security] > [AAA Mode Setup] の順に選択します。[AAA Mode Setup] ページが表示されます。

ステップ 2　[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 3　[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 4　[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-3）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-3）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キーを入力します（「Cisco Secure ACS サーバのセットアップ」（P.C-3）を参照）。

ステップ 5　[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 6　[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 7　[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 8　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：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 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*』
- Common Services 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-5）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。

問題が発生した場合は、Common Services オンライン ヘルプの「Authentication Failure in ACS Mode」を参照してください。