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 Operations Manager 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

Operations Manager 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、Operations Manager がインストールされている以外のネットワーク内のサーバに、Cisco Secure Access Control Server（ACS）をインストールする必要があります。

サポートされるデバイスとソフトウェアの詳細については、「Supported and Interoperable Devices and Software for Cisco Unified Operations Manager8.5」を参照してください。

Operations Manager の統合に関する注意事項

Operations Manager、Service Monitor、および Common Services はいずれも、共有プロファイル コンポーネントとして Cisco Secure ACS と統合されています。複数インスタンスの同じアプリケーション（Operations Manager など）が認証および認可のために同じ Cisco Secure ACS サーバを使用できます。

Cisco Unified Operations Manager、Cisco Unified Service Monitor および Common Services を Cisco Secure ACS に登録するときに、アプリケーション タスクおよびユーザ ロールが Cisco Secure ACS にインポートされます。

タスクおよびロールをインポートするには、アプリケーションの 1 インスタンスだけを Cisco Secure ACS に登録する必要があります。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。

CiscoWorks 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、固有のメカニズムである、Common Services Local ログイン モジュール以外の認証元を使用できます。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。デフォルトでは、Common Services Local ログイン モジュール認可方式に 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	
ヘルプ デスク	このロールのユーザには、Operations Manager および Common Services の一部の情報を表示する特権があります。 例：Alert History データベースを検索できます。
アプルーバ	このロールのユーザは、一切特権を持っていません（Operations Manager は、このユーザ ロールに一切タスクを割り当てません）。
ネットワーク オペレータ	このロールのユーザには、すべての Operations Manager タスクと一部の Common Services タスクを実行する特権があります。 例：ロギング パラメータを設定できます。 このロールのユーザはデフォルトで Network Administrator と同じ Operations Manager タスクを実行できます。
ネットワーク管理者	このロールのユーザには、すべての Operations Manager タスクと一部の 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 オペレータのタスクを実行できます。 例：DCR から Operations Manager にデバイスを追加できます。
システム管理者	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。
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 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。

Operations Manager および Common Services に定義されているタスク、およびタスクを実行する特権を持つロールについては、Common Services の Permission Report を参照してください（[Administration] > [Service Administration (Common Services)] > [Reports] > [Permission Report] の順に選択します）。

（注）　詳細については、CiscoWorks 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 Operations Manager 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

Operations Manager 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。

ローカル ユーザをシステム アイデンティティ ユーザとして設定できます。（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）。

ステップ 1　ローカル ユーザを作成し、すべてのロールをこのユーザに割り当てます。

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場合（表 C-1 を参照）、Operations Manager 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。

ステップ 2　ユーザ名をステップ 1 で作成したシステム アイデンティティ ユーザで置き換えて、システム アイデンティティ ユーザを更新します。

この操作を実行するには、[Administration] > [Service 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 [Help] リンクをクリックしてください。

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。

ステップ 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。

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

ステップ 2　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。

ステップ 3　Operations Manager サーバを AAA クライアントとして Cisco Secure ACS に追加します。

ステップ 4　Cisco Secure ACS で Operations Manager 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。

ステップ 5　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。

ステップ 6　Operations Manager、Service Monitor、および Common Services アプリケーションが Cisco Secure ACS にすで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 Operations Manager
- Cisco Unified Service Monitor
- Common Services

ステップ 7　Cisco Secure ACS 上の認証設定（ユーザ単位またはグループ単位）に基づいて、[User Setup] または [Group Setup] のどちらかをクリックします。

ステップ 8　[Interface Configuration] > [TACACS + (Cisco IOS)] を使用して、Cisco Unified Operations Manager のユーザ単位またはグループ単位の設定を確認します。

詳細は、『User Guide for Cisco Secure Access Control Server 4.x』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。

ステップ 2　[Select a Type] の横にある [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 :「Cisco Secure ACS サーバのセットアップ」（P.C-3）の手順 1 で作成した管理者の名前を入力します。
- 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）。
- ACS Shared Secret Key : 手順 3（「Cisco Secure ACS サーバのセットアップ」（P.C-3）を参照）で AAA クライアントとして Operations Manager サーバを Cisco Secure ACS に追加したときに入力した共有秘密を入力します。

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。

Operations Manager が ACS に登録されていて、再登録する場合、Operations Manager 用に Cisco Secure ACS に設定したカスタム ロールはすべて失われます。

Service Monitor と Common Services の場合も同様です（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] をクリックします。
  - ACS に Operations Manager、Service Monitor および Common Services の各タスクおよびユーザを登録します。
  - Operations Manager、Service Monitor および Common Services の既存のカスタム ロールを上書きします。
- [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。

ステップ 9　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

アプリケーションを ACS に登録すると、アプリケーション タスクがインポートされ、Cisco Secure ACS のアプリケーション用に設定されているすべてのカスタム ロールは上書きされます。

Common Services で AAA モードを ACS に変更したときに、[Register all installed applications with ACS] を選択しなかった場合、このセクションの情報を使用して、アプリケーションを Cisco Secure ACS に登録することもできます。

<*NMSROOT*>¥bin¥AcsRegCli.pl というスクリプトを使用すると、アプリケーションを選択して Cisco Secure ACS に登録できます。

（注）　*NMSROOT* は Operations Manager がインストールされているディレクトリです。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 **application name**

application name は、次のいずれかと置き換えます。

- itm：Operations Manager だけを登録します。
- qovr：Service Monitor だけを登録します。
- cmf：Common Services だけを登録します。
- all：サーバ上のすべてのアプリケーションを登録します（Cisco Unified Operations Manager、Cisco Unified Service Monitor、および Common Services）。

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 Operations Manager] を選択します。詳細については、次の説明を参照してください。

- 『*User Guide for Cisco Secure Access Control Server 4.x*』
- CiscoWorks 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」

Operations Manager 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。

ステップ 1　Cisco Secure ACS に定義されているユーザ名で Operations Manager にログインします。

ステップ 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、次のようになります。

- Fault History レポートを表示できます。
- DCR から Operations Manager にデバイスを追加できません。

Cisco Secure ACS のユーザまたはグループのネットワーク デバイス設定に基づいて、Operations Manager サーバで特定のデバイスだけを表示できます。

デバイスに基づくフィルタリングを使用できる Operations Manager タスクのリストについては、Cisco Secure ACS の Operations Manager 固有のオンライン ヘルプを参照してください。

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