CHAPTER 4

サーバ アプリケーションのインストールとアップグレード

次のトピックで、Security Manager サーバ ソフトウェアとその他のサーバ アプリケーション（Common Services、AUS、Performance Monitor、RME など）のインストール方法について説明します。

必要なサーバ ユーザ アカウントについて

CiscoWorks Common Services と Security Manager は、必要な認可を受けているユーザにのみ特定の機能へのアクセスを許可する多層セキュリティ システムを採用しています。そのため、Common Services 上で動作するアプリケーションがインストールされたシステム上では、事前に定義された次の 3 つのユーザ アカウントが作成されます。

- **admin** : admin ユーザ アカウントは、Windows 管理者と等価で、Common Services、Security Manager、およびその他のアプリケーション タスクのすべてにアクセスできるようにします。インストール中にパスワードを入力する必要があります。このアカウントは、初めてサーバにログインするときに使用して、アプリケーションを日常的に使用するための他のユーザ アカウントを作成できます。
- **casuser** : casuser ユーザ アカウントは、Windows 管理者と等価で、Common Services タスクと Security Manager タスクのすべてにアクセスできるようにします。このアカウントを直接使用することはあまりありません。

  製品のインストール中に設定された casuser（デフォルト サービス アカウント）権限またはディレクトリ権限を変更しないでください。変更した場合は、次の操作ができなくなる可能性があります。

  - Web サーバへのログイン
  - クライアントへのログイン
  - データベースの正常なバックアップ
- *システム識別*: システム識別ユーザ アカウントは、Windows 管理者と等価で、Common Services タスクと Security Manager タスクのすべてにアクセスできるようにします。このアカウントには固定の名前がありません。ニーズに合った名前を使用してアカウントを作成できます。Common Services でアカウントを作成した場合は、そのアカウントにシステム管理者特権を付与する必要があります。ユーザ認証に Cisco Secure Access Control Server（ACS）を使用している場合は、ACS にすべての特権を付与する必要があります。

  Cisco Security Management Suite アプリケーションを別のサーバにインストールする場合（推奨アプローチ）は、マルチサーバ セットアップ内のすべてのサーバ上で同じシステム識別ユーザ アカウントを作成する必要があります。サーバ間の通信は、証明書と共有秘密キーを使用する信頼モデルに依存します。システム識別ユーザは、マルチサーバ セットアップ内の他のサーバから信頼できるアカウントと見なされるため、ドメイン内のサーバ間通信が容易になります。

必要な数のユーザ アカウントを追加できます。アカウントはユーザごとに一意にする必要があります。このような追加のアカウントを作成するには、システム管理者権限（admin アカウントの使用など）を持っている必要があります。ユーザ アカウントを作成したら、それにロールを割り当てる必要があります。このロールによって、表示も含めて、ユーザがアプリケーション内で可能な操作が定義されます。使用可能な権限の種類と ACS を使用してアプリケーションへのアクセスを制御する方法については、第 7 章「ユーザ アカウントの管理」を参照してください。

Remote Desktop Connection または VNC を使用したサーバ アプリケーションのインストール

サーバ アプリケーションは、サーバに直接ログインしてインストールすることを推奨します。

ただし、リモート インストール（別のワークステーション経由のログイン）を行わなければならない場合は、次のヒントを考慮してください。

- リモート ディスクからソフトウェアをインストールしようとしないでください。ソフトウェア インストーラは、サーバ内の DVD ドライブ上で動作している製品 DVD 上に存在するか、直接接続されたディスク ドライブ上に存在する必要があります。リモート ディスクからのインストールが成功したように見える場合がありますが、実際には成功していません。
- ソフトウェアのインストールに Virtual Network Computing（VNC）を使用できます。

- ソフトウェアのインストールに Remote Desktop Connection を使用できます。ただし、複数の Remote Desktop Connection セッションが同時に開いているときに Security Manager をインストールしようとすると、Cisco Security Agent が自動的に停止しないことがあります。これは、Remote Desktop Connection セッションを最初に開いた管理者が、必ず、Cisco Security Agent サービスの停止に関する問い合わせを受け取るという Remote Desktop Connection の制限によるものです。Remote Desktop Connection セッション上で Security Manager をインストールしたが、最初にログインした管理者でない場合は、問い合わせを受け取れません。回避策は、Security Manager をインストールする前に **net stop CSAgent** コマンドを入力することです。または、インストール中に、最初または唯一の Remote Desktop Connection セッションを所有することです。

Security Manager サーバ、Common Services、および AUS のインストール

メインの Security Manager インストール プログラムで次のようなアプリケーションをインストールできます。

- CiscoWorks Common Services 3.3：すべてのサーバ アプリケーションに必要な基盤ソフトウェアです。Security Manager、AUS、Performance Monitor、または RME をインストールする場合は、Common Services 3.3（まだインストールされていない場合）をインストールする必要があります。
- Cisco Security Manager 4.0.1：Security Manager のメイン サーバ ソフトウェアです。

  サーバにフル スタンドアロン バージョンの Cisco Security Agent がインストールされていない場合は、インストール プログラムが次のように対処します。

  - Windows 2003 R2 Enterprise Server（Service Pack 2）（32 ビット）では、インストール プログラムから Cisco Security Agent をインストールするかどうかが尋ねられます。
  - Windows 2008 Enterprise Server（Service Pack 2）（32 ビット）では、インストール プログラムが Cisco Security Agent をインストールしません。
  - Windows 2008 Enterprise Server（Service Pack 2）（64 ビット）では、インストール プログラムが Cisco Security Agent をインストールしません。
- Auto Update Server 4.0
- Cisco Security Manager Client 4.0.1 : Security Manager サーバとデータをやり取りするためのクライアント ソフトウェアです。サーバと同じコンピュータ上にインストールできますが、このセットアップを Security Manager を使用する通常の方法として使用しないでください。推奨されているクライアントのインストールとセットアップの詳細については、第 5 章「クライアントのインストールと設定」を参照してください。

次の手順を使用して、これらのアプリケーションをインストールまたは再インストールします。以前のバージョンのアプリケーションからアップグレードしている場合は、先に進む前に、「サーバ アプリケーションのアップグレード」（P.4-10）を参照してください。

はじめる前に

- （従来の）Security Manager 3.x リリースの有効なライセンスを持っているかどうかに関係なく、3.x 以前のお客様はすべて Security Manager 4.0.1 の新しいライセンスを取得する必要があります。増分ライセンスを除いて、既存の Security Manager 3.x ライセンスは Security Manager 4.0.1 に使用できません。

- すでにサーバ上にインストールされている既存のバージョンのアプリケーションに対するアップグレードとして製品をインストールしている場合は、「リモート アップグレード時のデータベースのバックアップ」（P.4-13）に記載されているようにバックアップを実行してください。アップグレードをインストールする前に、バックアップが正常に終了し、既存のアプリケーションが正しく機能していることを確認してください。
- Security Manager の永久ライセンスを持っている場合は、それをサーバにコピーします。インストール中にライセンス ファイルを選択するためには、それがサーバ上に存在している必要があります。そのファイルは製品をインストールするフォルダに配置しないでください。
- 「インストール準備状況チェックリスト」（P.3-4）を完了したことを確認してください。
- サーバが「サーバ要件」（P.2-3）に記載された要件を満たしていることを確認してください。
- Security Manager は制御環境下の専用サーバにインストールすることを推奨します。他のソフトウェア アプリケーションをインストールした場合は、Security Manager の通常動作と競合したり、サポートされていなかったりする可能性があります。
- Security Manager サーバまたは AUS のインストール後に Common Services を再インストールした場合は、Security Manager または AUS も再インストールする必要があります。
- Common Services のインストール後にシステム時間を変更しないでください。このような変更が一部の時間依存機能の動作に影響する可能性があります。
- Cisco Secure Access Control Server（ACS）を使用して、Security Manager または AUS へのユーザ アクセスに AAA サービスを提供する場合は、アプリケーションをインストールしてから、ACS を使用するように Common Services を設定します。ACS 制御の設定方法については、「Security Manager と Cisco Secure ACS の統合」（P.7-8）を参照してください。

  ACS を使用するように Common Services を設定してから Security Manager または AUS をインストールした場合は、インストール中に、インストールしたアプリケーションを ACS に登録する必要があることが通知されます。まだアプリケーション（このサーバ上または別のサーバ上）を ACS に登録していない場合は、[Yes] を選択します。すでにアプリケーションを登録している場合は、[Yes] を選択すると、アプリケーションの ACS 内で設定されたユーザ ロールのカスタマイズが失われるため、[No] を選択する必要があります。同じ ACS サーバを使用するすべての Security Manager サーバと AUS サーバがユーザ ロールを共有します。

手順

Security Manager サーバ、Common Services、AUS、またはメインの Security Manager インストール プログラムを使用する複数のアプリケーションをインストールするには、次の手順を実行します。

ステップ 1　インストール プログラムを入手または検索します。次のいずれかの操作を実行できます。

- サーバの DVD ドライブに Security Manager インストール DVD を挿入します。インストール アプリケーションが自動的に起動しなかった場合は、**csm**<*version*>**_win_server** フォルダ内の **Setup.exe** ファイルを実行します。
- Cisco.com アカウントにログインして、http://www.cisco.com/go/csmanager にある Security Manager ホームページにアクセスします。[Download Software] をクリックして、圧縮された Security Manager のインストール ファイルをダウンロードします。
  - WinZip や圧縮フォルダの展開ウィザードなどの Windows Server 2003 に付属しているファイル圧縮ユーティリティのいずれかを使用して、圧縮されたソフトウェア インストール ファイル内のすべてのファイルを一時ディレクトリで解凍します。パス名があまり長くないディレクトリを使用してください。たとえば、C:¥Documents and Settings¥Administrator¥Desktop よりは C: を選択してください。通常は、圧縮ファイルと同じディレクトリに解凍される、インストール プログラムの **Setup.exe** を開始します。

- ファイルの内容を解凍できないというエラー メッセージが表示された場合は、Temp ディレクトリを空にして、ウイルスをスキャンし、C:¥Program Files¥Common Files¥InstallShield ディレクトリを削除してから、リブートしてもう一度試してみてください。

ステップ 2　インストール ウィザードの指示に従います。インストール中に、次の情報の入力が要求されます。

- Backup location：特定のバージョンの Common Services、Security Manager、または AUS がすでにインストールされている場合は、インストール プログラムによってインストール中のデータベース バックアップが許可されます。バックアップを実施する場合は、バックアップに使用する場所を選択します。ただし、バックアップは、インストールを開始する前に実施することを推奨します。
- Destination folder：アプリケーションをインストールするフォルダ。他の場所にインストールする特別な理由がなければ、デフォルトを受け入れます。デフォルト フォルダ以外のフォルダを指定した場合は、その下にファイルが存在しないことと、パス名が 256 文字未満であることを確認してください。
- Applications：インストールするアプリケーション。まだ Common Services がインストールされていない場合は、Common Services を選択して Security Manager または AUS をインストールする必要があります。
- License information：次のいずれかを選択します。
  - **License File Location**：ライセンス ファイルのフル パス名を入力するか、[Browse] をクリックして検索します。永久ライセンス ファイルを事前にサーバ上に配置してあった場合は、そのファイルを指定できます。
  - **Evaluation Only**：無料の 90 日の評価期間をイネーブルにします。
- Admin password：5 文字以上の **admin** ユーザ アカウント用パスワード。このアカウント、システム識別アカウント、および casuser アカウントの詳細については、「必要なサーバ ユーザ アカウントについて」（P.4-1）を参照してください。
- System Identity user：システム識別ユーザとして使用するアカウントのユーザ名とパスワード。Cisco Security Management Suite アプリケーションを複数のサーバ上にインストールする場合は、すべてのサーバ上で同じシステム識別ユーザ アカウントを使用してください。
- Create casuser：新しいインストールで casuser アカウントを作成するかどうか。このユーザ アカウントは作成する必要があります。

ステップ 3　インストールの完了後に、サーバが自動的に再起動しない場合は、サーバを再起動します。

（注）　インストール後の再起動中は、不定期かつランダムに、Windows on VMware ESX が応答を停止（ストール）します。この場合は、VMware GUI コントロールを使用して VMware ESX のインスタンスをリブートします。

Performance Monitor のインストール

Performance Monitor 4.0.1 は次の場所にインストールできます。

- CiscoWorks Common Services 3.3 のインストール後のスタンドアロン サーバ。これが推奨されている設定です。
- CiscoWorks Common Services 3.3 のインストール後の Security Manager、AUS、RME のいずれかまたは全部をインストールしたサーバ。ただし、Event Management を使用またはイネーブルにする場合は、「Event Management のイネーブル化の影響」（P.1-8）を参照してください。Security Manager サーバ上で MCP または RME に関する syslog を使用する場合は、そのサーバ上で Event Management をイネーブルにできません。

ヒント　この設定は、小規模ネットワークにのみ推奨されています。

Performance Monitor ライセンスは、Security Manager ライセンス ファイルとは別のファイルであり、RME 4.3 のライセンスも含まれています。ライセンスは、Performance Monitor のインストールの前と後のどちらでもインストールできます。ライセンス ファイルの取得手順については、「インストールに対するライセンスの影響とライセンスの取得」（P.1-6）を参照してください。

はじめる前に

すでに Performance Monitor、Common Services、またはその他の CiscoWorks アプリケーションが存在するシステム上にインストールしている場合は、サーバ上に Performance Monitor をインストールする前に次の推奨事項を考慮してください。

- Performance Monitor の永久ライセンスを持っている場合は、それをサーバにコピーします。インストール中にライセンス ファイルを選択するためには、それがサーバ上に存在している必要があります。
- Common Services をバックアップします。バックアップには、Common Services を使用するすべてのインストール済みアプリケーションに関するデータが含まれています。Performance Monitor インストール プログラムは、インストール中のバックアップを実施しません。バックアップの実施方法については、「リモート アップグレード時のデータベースのバックアップ」（P.4-13）を参照してください。
- Common Services と Performance Monitor を 1 台のサーバ上にインストールしてから、後で、Common Services を再インストールした場合は、Performance Monitor も再インストールする必要があります。
- Cisco Secure Access Control Server（ACS）を使用して、Performance Monitor へのユーザ アクセスに AAA サービスを提供する場合は、Performance Monitor をインストールしてから、ACS を使用するように Common Services を設定します。ACS 制御の設定方法については、「Security Manager と Cisco Secure ACS の統合」（P.7-8）を参照してください。

  ACS を使用するように Common Services を設定してから Performance Monitor をインストールした場合は、インストール中に、インストールしたアプリケーションを ACS に登録する必要があることが通知されます。まだ Performance Monitor（このサーバ上または別のサーバ上）を ACS に登録していない場合は、[Yes] を選択します。すでに Performance Monitor を登録している場合は、[Yes] を選択すると、アプリケーションの ACS 内で設定されたユーザ ロールのカスタマイズが失われるため、[No] を選択する必要があります。同じ ACS サーバを使用するすべての Performance Monitor サーバがユーザ ロールを共有します。

  次の手順には、ACS を使用するように Common Services を設定した後に Performance Monitor をインストールする場合に従うべき追加の手順が含まれています。

手順

Performance Monitor をインストールするには、次の手順を実行します。

ステップ 1　すでにサーバに CiscoWorks Common Services 3.3 がインストールされている場合は、Security Manager インストール DVD を使用して Common Services をインストールします。インストール手順については、「Security Manager サーバ、Common Services、および AUS のインストール」（P.4-3）を参照してください。Performance Monitor は Common Services 3.3 がなければ機能できません。また、Performance Monitor をインストールする前に、Common Services をインストールするか、バージョン 3.3 にアップグレードする必要があります。

ステップ 2　インストール プログラムを入手または検索します。次のいずれかの操作を実行できます。

- サーバの DVD ドライブに Security Manager インストール DVD を挿入します。インストール プログラムは **mcp**<*version*>**¥Setup.exe** です。
- Cisco.com アカウントにログインして、http://www.cisco.com/go/csmanager にある Security Manager ホームページにアクセスします。[Download Software] をクリックして、Performance Monitor のインストール ユーティリティをダウンロードします。

ステップ 3　インストールを開始するには、インストール プログラムをダブルクリックしてから、プロンプトに従います。

ステップ 4　ライセンス情報を選択するように要求されたら、次のいずれかを選択します。

- **License File Location**：ライセンス ファイルのフル パス名を入力するか、[Browse] をクリックして検索します。永久ライセンス ファイルをサーバ上に配置してあった場合は、そのファイルを指定できます。
- **Evaluation Only**：無料の 90 日の評価期間をイネーブルにします。

Performance Monitor と ACS

まだ ACS を使用するように Common Services を設定していない場合は、この手順の残りのステップを省略します。ただし、ACS を使用するように Common Services を設定してから Performance Monitor をインストールする場合は、この手順の追加のステップを完了する必要があります。

ステップ 5　ACS サーバにログインします。

ステップ 6　ACS サーバ上で、[Shared Profile Components] に移動します。Performance Monitor がアプリケーション リストに掲載されていることを確認します。

ステップ 7　ACS サーバ上で、[Group Setup] に移動します。Security Manager の設定に使用したグループ名を選択します。

ステップ 8　[Edit Settings] をクリックします。

ステップ 9　[Group Setup] ページで、Performance Monitor を探します。チェックボックスをオンにして、ACS 統合用の Performance Monitor を含めます。

ステップ 10　また、[Group Setup] ページ上で、次のセクション（Performance Monitor）に移動します。

ステップ 11　[Assign a Performance Monitor on a per Network Device Group Basis] オプション ボタンをクリックします。

ステップ 12　[Device Group] ドロップダウン メニューで、[CSM_Servers] を選択します。

ステップ 13　[Performance Monitor] ドロップダウン メニューで、[System Administrator] を選択します。

ステップ 14　[Submit + Restart] をクリックします。

ステップ 15　Security Manager サーバ上で、Daemon Manager を再起動します。

ステップ 16　数分間待って、デーモンの開始を確認してから、Performance Monitor サーバにログインします。

Resource Manager Essentials（RME）のインストール

RME 4.3 は次の場所にインストールできます。

- CiscoWorks Common Services 3.3 のインストール後のスタンドアロン サーバ。これが推奨されている設定です。
- CiscoWorks Common Services 3.3 のインストール後に Security Manager、AUS、MCP のいずれかまたは全部をインストールしたサーバ。ただし、Event Management を使用またはイネーブルにする場合は、「Event Management のイネーブル化の影響」（P.1-8）を参照してください。Security Manager サーバ上で RME または MCP に関する syslog を使用する場合は、そのサーバ上で Event Management をイネーブルにできません。

ヒント　この設定は、小規模ネットワークにのみ推奨されています。

RME ライセンスは、Security Manager ライセンス ファイルとは別のファイルであり、Performance Monitor のライセンスも含まれています。ライセンスは、RME のインストールの前と後のどちらでもインストールできます。ライセンス ファイルの取得手順については、「インストールに対するライセンスの影響とライセンスの取得」（P.1-6）を参照してください。

はじめる前に

すでに RME、Common Services、またはその他の CiscoWorks アプリケーションが存在するシステム上にインストールしている場合は、サーバ上に RME をインストールする前に次の推奨事項を考慮してください。

- RME の永久ライセンスを持っている場合は、それをサーバにコピーします。インストール中にライセンス ファイルを選択するためには、それがサーバ上に存在している必要があります。
- Common Services をバックアップします。バックアップには、Common Services を使用するすべてのインストール済みアプリケーションに関するデータが含まれています。RME インストール プログラムは、インストール中のバックアップを実施しません。バックアップの実施方法については、「リモート アップグレード時のデータベースのバックアップ」（P.4-13）を参照してください。
- Common Services と RME を 1 台のサーバ上にインストールしてから、後で、Common Services を再インストールした場合は、RME も再インストールする必要があります。
- Cisco Secure Access Control Server（ACS）を使用して、RME へのユーザ アクセスに AAA サービスを提供する場合は、RME をインストールしてから、ACS を使用するように Common Services を設定します。ACS 制御の設定方法については、「Security Manager と Cisco Secure ACS の統合」（P.7-8）を参照してください。

  ACS を使用するように Common Services を設定してから RME をインストールした場合は、インストール中に、インストールしたアプリケーションを ACS に登録する必要があることが通知されます。まだ RME（このサーバ上または別のサーバ上）を ACS に登録していない場合は、[Yes] を選択します。すでに RME を登録している場合は、[Yes] を選択すると、アプリケーションの ACS 内で設定されたユーザ ロールのカスタマイズが失われるため、[No] を選択する必要があります。同じ ACS サーバを使用するすべての RME サーバがユーザ ロールを共有します。

手順

RME をインストールするには、次の手順を実行します。

ステップ 1　すでにサーバに CiscoWorks Common Services 3.3 がインストールされている場合は、Security Manager インストール DVD を使用して Common Services をインストールします。インストール手順については、「Security Manager サーバ、Common Services、および AUS のインストール」（P.4-3）を参照してください。RME は Common Services 3.3 がなければ機能できません。また、RME をインストールする前に、Common Services をインストールするか、バージョン 3.3 にアップグレードする必要があります。

RME をインストールする前に Common Services をインストールしてシステムを再起動しないと、Common Services のインストールが失敗する可能性があります。

ステップ 2　インストール プログラムを入手または検索します。次のいずれかの操作を実行できます。

- サーバの DVD ドライブに Security Manager インストール DVD を挿入します。インストール プログラムは **rme**<*version*>**¥Setup.exe** です。
- Cisco.com アカウントにログインして、http://www.cisco.com/go/csmanager にある Security Manager ホームページにアクセスします。[Download Software] をクリックして、RME のインストール ユーティリティをダウンロードします。

ステップ 3　McAfee VirusScan がサーバ上にインストールされている場合は、VirusScan とその「オンアクセス スキャン」機能が動作していることを確認してください。

VirusScan がインストールされているが、オフになっている場合、または、そのオンアクセス スキャン機能がオフになっていた場合は、RME をインストールできない可能性があります。加えて、この理由で RME のインストールが失敗した場合は、同じサーバにインストールされた Security Manager が正しく動作しない可能性があります（Security Manager を再インストールする必要があります）。

ステップ 4　インストールを開始するには、インストール プログラムをダブルクリックしてから、プロンプトに従います。

インストール中に、次の情報の入力が要求されます。

- License information：次のいずれかを選択します。
  - **License File Location**：ライセンス ファイルのフル パス名を入力するか、[Browse] をクリックして検索します。永久ライセンス ファイルを事前にサーバ上に配置してあった場合は、そのファイルを指定できます。
  - **Evaluation Only**：無料の 90 日の評価期間をイネーブルにします。
- Setup type（Typical または Custom）：[Typical] を選択します。標準とカスタムの違いは、カスタム インストールで標準インストール中にランダムに生成されたデータベース パスワードを指定できることだけです。データベース パスワードを指定する場合は、5 ～ 15 文字を使用し、先頭は数字以外に、文字間にスペースを挿入しないようにしてください。このパスワードは、データベースの復元やトラブルシューティングにも使用されます。
- Restart CiscoWorks Daemons : CiscoWorks デーモンを再起動するかどうかが尋ねられます。[Yes] を選択します。

サーバ アプリケーションのアップグレード

アプリケーションのアップグレードとは、古いバージョンからのデータを維持しながら、新しいバージョンのアプリケーションをインストールするプロセスです。3 種類のアップグレード パスがあります。

- ローカル：古いバージョンをアンインストールせずに、古いバージョンを実行中のサーバ上に新しいバージョンをインストールします。既存のデータが保存され、新しくインストールされたバージョンで使用できます。ローカル アップグレードを実施する場合は次の点に注意してください。
  - この方式を使用する前に、アップグレードするすべてのアプリケーションが正しく機能していることを確認してください。また、アップグレード対象のアプリケーションをインストールする前に、データベースのバックアップを実施して、正常に終了したことを確認してください。
  - サーバ上のオペレーティング システムもアップグレードしている場合、たとえば、Windows 2003 から Windows 2008 にアップグレードしている場合は、この方式が使用できません。オペレーティング システムのアップグレードも行いながら Security Manager をアップグレードしている場合は、代わりに、リモート バックアップ/復元アップグレード方式を使用します。同じ Security Manager リリースを維持しながらオペレーティング システムをアップグレードしている場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.4-17）に記載された手順を実行します。
- リモート（バックアップ/復元）：新しいバージョンをクリーン サーバ（古いアプリケーションがインストールされていないサーバ）にインストールしてから、古いバージョンから作成したバックアップからデータベースを復元します。新しいサーバ上にインストールする場合、または、インストールを実施する前にサーバをクリーンオフする（アプリケーションをアンインストールする前にバックアップを作成する）場合に、この手順を使用します。

（注）　Security Manager サーバ アプリケーションを実行しているサーバのバックアップを作成する前に、すべての保留データがコミットされていることを確認する必要があります。「Security Manager の保留データが送信および承認されることの確認」（P.4-12）を参照してください。

- 間接：ローカルまたはリモート アップグレードでサポートされていない古いバージョンのアプリケーションを使用している場合は、2 段階プロセスを実行する必要があります。ローカルまたはリモート アップグレードでサポートされているバージョンにアップグレードしてから、ローカルまたはリモート アップグレードを実施します。中間のバージョンを Cisco.com からダウンロードします。

  使用中のバージョンが下の表に間接アップグレード用として掲載されておらず、古いデータを保存する必要がある場合は、3 つ以上の中間アップグレード手順を実施する必要があります。たとえば、Performance Monitor 3.0 からアップグレードする場合は、まず、3.2 にアップグレードしてから、4.0 にアップグレードし、4.0.1 にアップグレードする必要があります。また、Security Manager 3.0.x の場合は、3.1.1 にアップグレードしてから、4.0 にアップグレードし、4.0.1 にアップグレードする必要があります。

通常、以前のバージョンのアプリケーションからアップグレードする場合は、評価ライセンスと永久ライセンスの両方が保存されます。ただし、（従来の）Security Manager 3.x リリースの有効なライセンスを持っているかどうかに関係なく、3.x 以前のお客様はすべて Security Manager 4.0.1 の新しいライセンスを取得する必要があります。増分ライセンスを除いて、既存の Security Manager 3.x ライセンスは Security Manager 4.0.1 に使用できません。

表 4-1 に、アップグレード パスごとにサポートされているソフトウェアのバージョンに関する説明を示します。

（注）　Security Manager 3.x ユーザは、Security Manager 4.0.1 に直接アップグレードすることはできません。まず 4.0 にアップグレードしてから、4.0.1 にアップグレードする必要があります。

表 4-1　アプリケーション アップグレード パス

アップグレード パス	アプリケーション	サポートされている古いバージョン	アップグレード手順
ローカル	Security Manager 4.0.1 Auto Update Server 4.0	4.0	すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.4-12）を参照してください。 その後で、ソフトウェアをインストールします。「Security Manager サーバ、Common Services、および AUS のインストール」（P.4-3）を参照してください。 最後に、アップグレード後の必要な変更を加えます。「アップグレード後の必要な変更の実施」（P.4-16）を参照してください。
	Performance Monitor 4.0.1	4.0	（推奨）データベースをバックアップします。「リモート アップグレード時のデータベースのバックアップ」（P.4-13）を参照してください。 その後で、ソフトウェアをインストールします。「Performance Monitor のインストール」（P.4-6）を参照してください。
	RME 4.3	4.2	（推奨）データベースをバックアップします。「リモート アップグレード時のデータベースのバックアップ」（P.4-13）を参照してください。 その後で、ソフトウェアをインストールします。「Resource Manager Essentials（RME）のインストール」（P.4-8）を参照してください。
リモート	Security Manager 4.0.1 Auto Update Server 4.0	4.0	1. データベースをバックアップします。「リモート アップグレード時のデータベースのバックアップ」（P.4-13）を参照してください。 2. アプリケーションをインストールします。次の項を参照してください。 「Security Manager サーバ、Common Services、および AUS のインストール」（P.4-3） 「Performance Monitor のインストール」（P.4-6） 「Resource Manager Essentials（RME）のインストール」（P.4-8） 3. 必要に応じて、データベースのバックアップをサーバに転送します。 4. データベースを回復します。「サーバ データベースの復元」（P.4-15）を参照してください。 5. 最後に、アップグレード後の必要な変更を加えます。「アップグレード後の必要な変更の実施」（P.4-16）を参照してください。
	Performance Monitor 4.0.1	4.0	
	RME 4.3	4.2	

表 4-1　アプリケーション アップグレード パス（続き）

アップグレード パス	アプリケーション	サポートされている古いバージョン	アップグレード手順
間接	Security Manager 4.0.1	3.2.2、3.3、および 3.3.1	4.0 にアップグレードしてから、4.0 のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。 その後で、ローカルまたはリモート アップグレード パスを使用します。
	Performance Monitor 4.0.1	3.2.2、3.3、および 3.3.1	4.0 バージョンにアップグレードしてから、ローカルまたはリモート アップグレード パスを使用します。4.0 のインストレーション ガイドを参照してください。
	RME 4.3	該当なし	該当なし。サポートされる最新の RME リリースは 4.0.3 です。 これはローカルまたはリモート アップグレードでサポートされます。

Security Manager の保留データが送信および承認されることの確認

Security Manager のアップグレードを成功させるためには、既存の Security Manager データベースに保留データが含まれていないことを確認する必要があります。保留データとは、データベースに対してコミットされていないデータのことです。保留データが残っている以前のバージョンの Security Manager からのデータベースは復元できません。復元できるのは、バックアップと同じバージョンを実行しているシステム上に保留データが残っているデータベースだけです。

ユーザごとに変更を送信または破棄する必要があります。アプルーバでワークフロー モードを使用している場合は、このような送信も承認する必要があります。すべてのデバイス設定と Security Manager データベースを同期させるためには、すべてのデータのコミット後に展開を実施する必要もあります。

- 非ワークフロー モードの場合：
  - 変更をコミットするには、[File] > [Submit] を選択します。
  - コミットされていない変更を破棄するには、[File] > [Discard] を選択します。
  - 他のユーザの変更をコミットまたは破棄する必要がある場合は、そのユーザのセッションを引き継ぐことができます。セッションを引き継ぐには、[Tools] > [Security Manager Administration] > [Take Over User Session] を選択してから、[Take Over Session] をクリックします。
- ワークフロー モードの場合：
  - 変更をコミットして承認するには、[Tools] > [Activity Manager] を選択します。[Activity Manager] ウィンドウで、アクティビティを選択して、[Approve] を選択します。アクティビティ アプルーバを使用している場合は、[Submit] をクリックして、アプルーバにアクティビティを承認させます。
  - コミットされていない変更を破棄するには、[Tools] > [Activity Manager] を選択します。[Activity Manager] ウィンドウで、アクティビティを選択してから、[Discard] を選択します。Edit 状態または Edit Open 状態のアクティビティしか破棄できません。

プロパティ ファイルに対する変更の復元

すべての Security Manager インストールにいくつかのプロパティ ファイルが含まれています。このファイルには、使用中に変更されたデータが保存されます。

- *$NMSROOT*¥MDC¥athena¥config¥csm.properties
- *$NMSROOT*¥MDC¥athena¥config¥DCS.properties
- *$NMSROOT*¥MDC¥athena¥config¥taskmgr.prop

ヒント　*$NMSROOT* は、Common Services インストール ディレクトリ（デフォルトは C:¥Program Files¥CSCOpx）のフル パス名です。

現在のインストールに対してサービス パックのアップグレードまたはインストールを実施した場合の Security Manager の動作は次のとおりです。

- アップグレードまたはサービス パックに関連する新しいファイルをインストールします。
- 新しいファイルと使用中に変更されたファイルを比較します。
- 新しいファイルと使用中に変更されたファイルが異なる場合は警告を発します。その場合は、Security Manager が次のように処理します。
  - 使用中に変更されたファイルを *<filename>.org* という名前で保存します。
  - 参考用として、差分ファイルを *<filename>.diff* という名前で保存します。

新しいファイルと使用中に変更されたファイルが異なるという内容の警告を受け取った場合は、*<filename>.org* と *<filename>.diff* 内の情報を使用して、アップグレードまたはサービス パックのインストール前に、加えた変更をプロパティ ファイルに復元します。

リモート アップグレード時のデータベースのバックアップ

CiscoWorks Common Services は、データベースのバックアップと復元に使用される Common Services バックアップ/復元ユーティリティで、すべてのサーバ アプリケーションのデータベースを管理します。そのため、バックアップを作成すると、サーバ上にインストールされたすべての CiscoWorks アプリケーションのバックアップが作成されます。

ヒント　このバックアップ手順はデータベースのみをバックアップします。イベント データ ストアをバックアップする必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.4-17）に記載されているデータ ストア コピー手順を使用します。

ステップ 1　Security Manager を実行しているサーバをバックアップしている場合は、Security Manager クライアントの [Tools] > [Backup] というショートカットを使用してバックアップ ページを表示できます。また、保留データがコミットされていることを確認します（「Security Manager の保留データが送信および承認されることの確認」（P.4-12）を参照）。

Security Manager を実行していないサーバの場合は、次の手順でバックアップ ページを表示します。

a. サーバ上の Cisco Security Management Server デスクトップにログインします（「Web ブラウザを使用したサーバ アプリケーションへのログイン」（P.5-11）を参照）。

b. [Server Administration] パネルをクリックします。[Server] > [Admin] タブで CiscoWorks Common Services が開きます

（CiscoWorks ホームページにログインした場合は、[Common Services] > [Server] > [Admin] を選択します）。

c. [Server] タブで、[Admin] > [Backup] を選択します。

ステップ 2　[Immediate for Frequency] を選択して、必要に応じて他のフィールドを設定し、[Apply] をクリックしてデータをバックアップします。

CLI を使用したサーバ データベースのバックアップ

この項の手順では、サーバ上の Windows コマンドラインからスクリプトを実行することによって、サーバ データベースをバックアップする方法について説明します。

データベースのバックアップ中に、Common Services と Security Manager の両方のプロセスがシャットダウンされ、再起動されます。Security Manager の再起動が完了するまで数分かかるため、ユーザがその間にクライアントを開始する可能性があります。その場合は、デバイス ポリシー ウィンドウに「error loading page」というメッセージが表示されます。

CiscoWorks サーバ上にインストールされたすべてのアプリケーションをバックアップするのに 1 つのバックアップ スクリプトしか使用されません。個別のアプリケーションをバックアップできません。

ヒント　このバックアップ コマンドはデータベースのみをバックアップします。イベント データ ストアをバックアップする必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.4-17）に記載されているデータ ストア コピー手順を使用します。

ステップ 1　保留データがコミットされていることを確認します（「Security Manager の保留データが送信および承認されることの確認」（P.4-12）を参照）。

ステップ 2　次のコマンドを入力することによって、データベースをバックアップします。

$NMSROOT¥**bin**¥**perl** *$NMSROOT*¥**bin**¥**backup.pl** *backup_directory* [*log_filename* [**email**=*email_address* [*number_of_generations* [**compress**]]]]

値は次のとおりです。

- *$NMSROOT*：Common Services インストール ディレクトリ（デフォルトは C:¥Program Files¥CSCOpx）のフル パス名。
- *backup_directory*：バックアップを作成するディレクトリ。C:¥Backups など。
- *log_filename*：（オプション）バックアップ中に生成されるメッセージ用のログ ファイル。現在のディレクトリ以外の場所で作成した場合のパスが含まれます。C:¥BackupLogs など。名前を指定しなかった場合は、*$NMSROOT*¥log¥dbbackup.log になります。
- **email**=*email_address*：（オプション）通知を送信する電子メール アドレス。電子メール アドレスは指定しないが、後続のパラメータは指定する必要がある場合は、サイズまたはアドレスが一致しない **email** を入力します。CiscoWorks Common Services で SMTP 設定を実施して通知をイネーブルにする必要があります。

- *number_of_generations*：（オプション）バックアップ ディレクトリに保存しておくバックアップの最大世代数。最大値に到達した場合は、古いバックアップが削除されます。デフォルトは、保存しておく世代数が無制限になる 0 です。
- **compress**：（オプション）バックアップ ファイルを圧縮するかどうか。このキーワードを入力しなかった場合は、バックアップ プロパティ ファイルで VMS_FILEBACKUP_COMPRESS=NO が指定されていれば、バックアップが圧縮されません。そうでない場合は、バックアップが圧縮されます。バックアップは圧縮することを推奨します。

たとえば、次のコマンドは、perl コマンドと backup.pl コマンドが存在するディレクトリで発行することを想定しています。このコマンドは、backups ディレクトリに圧縮されたバックアップとログ ファイルを作成して、admin@domain.com に通知を送信します。圧縮パラメータを含めるようにバックアップ世代を指定する必要があります。ログ ファイル パラメータの後ろにパラメータを指定した場合は、先行するすべてのパラメータの値を含める必要があります。

perl backup.pl C:¥backups C:¥backups¥backup.log email=admin@domain.com 0 compress

ステップ 3　ログ ファイルを調査して、データベースがバックアップされていることを確認します。

サーバ データベースの復元

コマンドラインからスクリプトを実行することによって、データベースを復元できます。データの復元中に、CiscoWorks をシャットダウンして再起動する必要があります。この手順では、サーバ上でバックアップされたデータベースを復元する方法について説明します。CiscoWorks サーバ上にインストールされたすべてのアプリケーションをバックアップして復元するためのバックアップおよび復元ファシリティが 1 つだけ存在します。個別のアプリケーションをバックアップまたは復元できません。

複数のサーバ上にアプリケーションをインストールしている場合は、インストールされたアプリケーションに適切なデータが保存されたデータベース バックアップかどうかを確認してください。

ヒント

- バックアップが、このバージョンのアプリケーションへの直接ローカル インライン アップグレードに対応したバージョンからのものである場合は、以前のリリースのアプリケーションから取得されたバックアップを復元できます。アップグレードに対応したバージョンの詳細については、「サーバ アプリケーションのアップグレード」（P.4-10）を参照してください。
- restore コマンドは、データベースのみを復元します。イベント データ ストアを復元する必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.4-17）に記載されているデータ ストア コピー手順を使用します。

手順

ステップ 1　コマンドラインで次のコマンドを入力することによって、すべてのプロセスを停止します。

net stop crmdmgtd

ステップ 2　次のコマンドを入力することによって、データベースを復元します。

$NMSROOT¥**bin¥perl** *$NMSROOT*¥**bin¥restorebackup.pl** [**-t** *temporary_directory*] [**-gen** *generationNumber*] **-d** *backup_directory* [**-h**]

値は次のとおりです。

- *$NMSROOT*：Common Services インストール ディレクトリ（デフォルトは C:¥Program Files¥CSCOpx）のフル パス名。

- **-t** *temporary_directory*：（オプション）復元プログラムで一時ファイルを保存するために使用されるディレクトリまたはフォルダ。デフォルトで、このディレクトリは *$NMSROOT*¥tempBackupData です。
- **-gen** *generationNumber*：（オプション）復元するバックアップ世代番号。デフォルトで、最新世代です。第 1 ～ 5 世代が存在する場合は、第 5 世代が最新です。
- **-d** *backup_directory*：復元するバックアップが保存されたバックアップ ディレクトリ。
- **-h**：（オプション）ヘルプを表示します。**-d** *BackupDirectory* を使用した場合は、ヘルプに正しい構文と使用可能なスイートおよび世代が表示されます。

たとえば、c:¥var¥backup ディレクトリから最新バージョンを復元するには、次のコマンドを入力します。

C:¥Progra~1¥CSCOpx¥bin¥perl C:¥Progra~1¥CSCOpx¥bin¥restorebackup.pl -d C:¥var¥backup

ヒント RME データが保存されたデータベースを復元している場合は、インベントリ データを収集するかどうかを尋ねられる場合があります。このデータの収集には長い時間がかかる可能性があります。[No] を選択して、インベントリをスケジュールするように RME を設定することもできます。RME で、[Devices] > [Inventory] を選択します。

ステップ 3　ログ ファイルの *NMSROOT*¥**log¥restorebackup.log** を調べて、データベースが復元されていることを確認します。

ステップ 4　次のコマンドを入力することによって、システムを再起動します。

net start crmdmgtd

ステップ 5　Security Manager サービス パックをインストールする前にバックアップされたデータベースを復元する場合は、データベースの復元後にサービス パックを再適用する必要があります。

アップグレード後の必要な変更の実施

アプリケーションをアップグレードすると、特定の情報の処理方法が変わって、手動で変更しなければならなくなる場合があります。このバージョンの製品にアップグレードしたら、下の必要な変更リストを参照して、状況に合わせて変更を適用する必要があります。

- 3.3.1 より以前のバージョンからアップグレードする場合は、4 ポート Gigabit Ethernet Fiber インターフェイス カード（ハードウェア タイプ：i82571EB 4F）が実装された ASA 5580 デバイス上でインベントリを再検出する必要があります。インベントリの再検出によって、デバイス上での速度非ネゴシエート設定を変更できない以前のリリースからのバグが解決されます。インベントリを再検出するには、Security Manager クライアントのデバイス ビューでデバイスを右クリックして、[Discover Policies on Device] を選択してから、[Policies to Discover] グループ内の [Live Device discovery and only the Inventory] チェックボックスをオンにします。再検出によって、デバイスに関するインターフェイス ポリシーが置き換えられます。
- 3.3.1 以前のバージョンからアップグレードしており、未サポートの Shared Port Adapter（SPA; 共有ポート アダプタ）を使用する Cisco ASR 1000 Series Aggregation Services Router を管理している場合は、Security Manager で、サポートされているバージョン 4.0 以降の SPA が検出できるように、デバイスに関するポリシーを再検出する必要があります。新しくサポートされる SPA には、すべてのイーサネット（すべての速度）、シリアル、ATM、および Packet over Sonet（POS）SPA が含まれますが、サービス SPA は含まれません。デバイス CLI で ATM、PVC、またはダイヤラ関連ポリシーを設定した場合は、再検出が必要です。

新しいコンピュータまたはオペレーティング システムへの Security Manager の移行

Security Manager を新しいサーバに移行しなければならない場合があります。この移行を新しい物理コンピュータに対して行う場合と、サーバ上のオペレーティング システムにメジャー アップグレードを施す場合（Windows 2003 から Windows 2008 に移行する場合など）があります。

Security Manager のバージョンは変更しないが、物理ハードウェアまたはオペレーティング システムを変更する場合は、移行プロセスを通過する必要があります。この移行プロセスは、基本的に、「サーバ アプリケーションのアップグレード」（P.4-10）に記載されているリモート バックアップ/復元アップグレード プロセスと同じものですが、Event Manager データ ストアに保存されたデータを移行する場合は追加のステップが必要です。Security Manager サーバの移行を実施する場合は、この手順を使用します。

（注）　オペレーティング システムに対するマイナー サービス パック アップデートは、それが Security Manager サーバ移行要件になるまで、アップグレードとは見なされません。サーバ移行は、オペレーティング システムの正式名称が変更される場合のように、異なるメジャー バージョンのオペレーティング システム同士を移行する場合に必要になります。

はじめる前に

この手順では、ターゲット サーバ（Security Manager を移行するサーバ）にソース コンピュータと同じデータベースとイベント データ ストアの内容を保存するものとします。ターゲット サーバ上で Security Manager の使用を開始している場合は、ソース システムとターゲット システムのデータベースまたはイベント データ ストアをマージできません。ターゲット データをソース データで置き換える必要があります。移行前にターゲット システム上に存在していたすべてのデータが、移行完了後に使用できなくなります。古いターゲット システム データを新しく移行するフォルダにコピーしないでください。

また、イベント データ ストアのコピーおよび復元ステップは、そのデータを保存する場合にのみ必要なことに注意してください。新しい空のイベント データ ストアから始める場合は、このステップを省略できます。

ステップ 1　ソース Security Manager サーバ（移行元のサーバ）上で次の手順を実行します。

a. イベント データ ソース フォルダの名前を決定します。Security Manager クライアントを使用して、[Tools] > [Security Manager Administration] を選択し、目次から [Event Management] を選択します。フォルダが [Event Data Store Location] フィールドに表示されます。デフォルトは、*NMSROOT*¥**MDC¥eventing¥database** です。ここで、NMSROOT はインストール ディレクトリです（通常は、C:¥Program Files¥CSCOpx）。

b. コマンドラインで次のコマンドを入力することによって、すべてのプロセスを停止します。

net stop crmdmgtd

c. *NMSROOT*¥**MDC¥eventing¥config¥collector.properties** ファイルのコピーとイベント データ ストア フォルダを作成します。そのコピーをターゲット コンピュータからアクセス可能なディスクに配置します。

d. 「CLI を使用したサーバ データベースのバックアップ」（P.4-14）に記載されているコマンドライン方式を使用して、Security Manager データベースをバックアップします。

ステップ 2　新しいターゲット コンピュータを準備します。次の例を参考にしてください。

- オペレーティング システムをアップグレードするだけで、新しいハードウェアに移行しない場合は、オペレーティング システム アップグレードを実施して、オペレーティング システムが正しく機能していることを確認します。その後で、Security Manager をインストールします。
- 新しいコンピュータに移行する場合は、そのコンピュータが正しく機能していることを確認して、Security Manager をインストールします。

ステップ 3　ターゲット Security Manager サーバ上で次の手順を実行します。

a. コマンドラインで次のコマンドを入力することによって、すべてのプロセスを停止します。

net stop crmdmgtd

b. 「サーバ データベースの復元」（P.4-15）に記載されている手順を使用して、データベースを復元します。

c. データベース復元の完了後にプロセスを再起動しなかった場合は、ここで再起動します。

net start crmdmgtd

d. Security Manager クライアントを使用して新しいサーバにログインしてから、[Tools] > [Security Manager Administration] を選択して、目次から [Event Management] を選択します。

e. イベント データ ストア フォルダが存在し、それが空であることを確認します（必要に応じてファイルを削除します）。このフォルダには、ソース サーバ上のイベント データ ストアと同じ名前と場所を設定する必要があります。

f. 正しい [Event Data Store Location]（デフォルトが正しいフォルダでない場合）を選択して、[Enable Event Management] チェックボックスをオフにし、Event Manager サービスを停止します。[Save] をクリックして変更を保存します。サービスを停止するかどうかの確認が要求されます。[Yes] をクリックしてサービスの停止が通知されるまで待ちます。

g. バックアップされたイベント データ ストアをソース コンピュータからターゲット サーバ上の新しい場所にコピーします。

h. バックアップされた *NMSROOT*¥**MDC¥eventing¥config¥collector.properties** ファイルをソース コンピュータからターゲット コンピュータにコピーして、ターゲット サーバ上のファイルを上書きします。

i. Security Manager クライアントを使用して、[Tools] > [Security Manager Administration] を選択し、目次から [Event Management] を選択します。[Enable Event Management] チェックボックスをオンにして、[Save] をクリックします。サービスを開始するかどうかの確認が要求されます。[Yes] をクリックしてサービスの開始が通知されるまで待ちます。

Security Manager、Performance Monitor、および RME ライセンスの更新

インストール時に永久ラインセンス ファイルを指定できますが、Security Manager、Performance Monitor、または RME のインストール後にもライセンスを追加できます。他の Cisco Security Management Suite アプリケーションにはライセンスは必要ありません。

Security Manager のライセンス追加プロセスは、Performance Monitor や RME のプロセスと異なります。次の手順では、両方のプロセスについて説明します。Performance Monitor/RME 共用ライセンスは、Security Manager ライセンス ファイルとは別のファイルであることに注意してください。

ライセンスの取得方法については、「インストールに対するライセンスの影響とライセンスの取得」（P.1-6）を参照してください。

はじめる前に

ライセンス ファイルをサーバにコピーしてから、アプリケーションに追加します。

手順

Security Manager、Performance Monitor、または RME 用のライセンスをインストールするには、次の手順を実行します。

ステップ 1　Security Manager ライセンスをインストールするには：

a. Security Manager クライアント アプリケーションを使用してサーバにログインします（「Security Manager クライアントを使用した Security Manager へのログイン」（P.5-10）を参照）。

b. [Tools] > [Security Manager Administration] を選択して、目次から [Licensing] を選択します。

c. タブがアクティブになっていない場合は、[CSM] をクリックします。

d. [Install a License] をクリックして、[Install a License] ダイアログボックスを開きます。このダイアログボックスを使用して、ライセンス ファイルを選択し、[OK] をクリックします。このプロセスを繰り返して他のライセンスを追加します。

ステップ 2　Performance Monitor または RME ライセンスをインストールするには：

a. Cisco Security Management Server デスクトップにログインします（「Web ブラウザを使用したサーバ アプリケーションへのログイン」（P.5-11）を参照）。

b. [Server Administration] パネルをクリックします。[Server] > [Admin] タブで CiscoWorks Common Services が開きます

（CiscoWorks ホームページにログインした場合は、[Common Services] > [Server] > [Admin] を選択します）。

c. [Licensing] を選択します。[License Information] ページに、ライセンス名、ライセンス バージョン、ライセンスのステータス、およびライセンスの有効期限が表示されます。

d. [Update] をクリックして、[License] フィールドに新しいライセンス ファイルへのパスを入力するか、[Browse] をクリックして新しいファイルを探します。

e. [OK] をクリックします。ライセンス ファイルが有効かどうか確認され、ライセンスが更新されます。更新されたライセンス情報が [License Information] ページに表示されます。

サービス パックとポイント パッチの入手

注意　Security Manager のサービス パックまたはポイント パッチは、シスコから入手してください。それ以外のファイルをダウンロードしたり、開いたりしないでください。サードパーティ製のサービス パックとポイント パッチはサポートされていません。

Security Manager またはその他のアプリケーションをインストールしたら、シスコシステムズから入手したサービス パックまたはポイント パッチをインストールして、バグを修復したり、新しいデバイス タイプをサポートしたり、アプリケーションを強化したりできます。

- 新しいサービス パックの入手可能な時期を知って、必要なサービス パックをダウンロードするには、Security Manager を開いて、[Help] > [Security Manager Online] を選択します。または、http://www.cisco.com/go/csmanager にアクセスします。
- 企業から Cisco TAC サービス リクエストが提出されると、TAC が、その問題の解決に役立つ未公開のポイント パッチがあるかどうかを通知します。これ以外の方法で Security Manager ポイント パッチが配布されることはありません。

サービス パックとポイント パッチは、クライアント ソフトウェア アップデートにサーバ サポートを提供し、クライアントとサーバ間のバージョン レベルのミスマッチを検出します。

サーバ ホームページへのアプリケーションの追加

同じサーバ上に Cisco Security Management Suite アプリケーションがインストールされている場合は、サーバ上のホームページにアプリケーションへのリンクが表示されます。ただし、複数のサーバ上にアプリケーションがインストールされている場合は、アプリケーションを他のサーバに登録しなければ、そのサーバのホームページにアプリケーションが表示されません。

1 つのホームページからすべての関連アプリケーションに接続できた方が便利な場合にのみこの作業を行う必要があります。そうでない場合は、各サーバに直接ログインすることによって、アプリケーションを使用できます。サーバにログインしてホームページを開く方法については、「Web ブラウザを使用したサーバ アプリケーションへのログイン」（P.5-11）を参照してください。

ステップ 1　Cisco Security Manager Suite のホームページで、[Server Administration] リンクをクリックします。[Common Services Admin] ページが開きます。

ステップ 2　[Server] > [HomePage Admin] を選択して、目次から [Application Registration] を選択します。[Application Registrations Status] ページが開きます。

ステップ 3　[Register] をクリックします。[Choose Location for Registrations] ページが開きます。

ステップ 4　[Register From Templates] を選択してから、[Next] をクリックします。

ステップ 5　ホームページにリンクするアプリケーション（[Monitoring, Analysis and Response System] や [RME]）を選択してから、[Next] をクリックします。

ステップ 6　サーバ名、サーバ表示名、選択されたアプリケーションを実行しているデバイスに関するポートおよびプロトコル情報を入力してから、[Next] をクリックします。

ステップ 7　登録情報を確認してから、[Finish] をクリックします。アプリケーションの起動点が Cisco Security Manager Suite のホームページに表示されます。

サーバ アプリケーションのアンインストール

サーバ アプリケーションをアンインストールするには、この手順を使用します。アプリケーションをアンインストールする前に、アプリケーションの再インストールが必要な場合にデータを復元できるようにバックアップの実施を検討してください。バックアップの実施方法については、「リモート アップグレード時のデータベースのバックアップ」（P.4-13）を参照してください。

はじめる前に

任意のバージョンの Windows Defender がインストールされている場合は、それをディセーブルにしてからサーバ アプリケーションをアンインストールします。そうしなければ、アンインストール アプリケーションを起動できません。

手順

サーバ アプリケーションをアンインストールするには、次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Cisco Security Manager] > [Uninstall Cisco Security Manager] を選択します。Performance Monitor と RME のどちらかだけがインストールされているサーバの場合は、[Start] > [Programs] > [Performance Monitor] > [Uninstall Performance Monitor] または [CiscoWorks] > [Uninstall CiscoWorks] を使用します。

ステップ 2　インストールされているアプリケーションのリストが表示されます。アンインストールするすべてのアプリケーションを選択します。すべての Cisco Security Management Suite アプリケーションをアンインストールするつもりがない場合は、Common Services を選択しないでください。

Windows 2003 R2 Enterprise Server（Service Pack 2）（32 ビット）では、インストール プログラムから Cisco Security Agent をアンインストールするかどうかが尋ねられます。

この方式では、外部 Cisco Security Agent はアンインストールできません（外部 Cisco Security Agent とは Cisco Security Manager インストールの一部としてインストールされない Cisco Security Agent のことです）。すべての Cisco Security Agent をアンインストールする場合は、[Start] > [Programs] > [Cisco Security Agent] > [Uninstall Cisco Security Agent] を選択します。詳細については、「同梱 Cisco Security Agent のアンインストール」（P.B-2）を参照してください。

ステップ 3　[Next] を 2 回クリックします。

アンインストーラによって、選択されたアプリケーションが削除されます。

（注）　アンインストール中にエラーが発生した場合は、「アンインストール中のサーバ障害」（P.A-8）および『*Installing and Getting Started With CiscoWorks LAN Management Solution 3.1*』の「Troubleshooting and FAQs」の章を参照してください。このマニュアルの URL は次のとおりです。
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html

ステップ 4　リブートは必須ではありませんが、アンインストール後はサーバをリブートして、サーバ上のレジストリ エントリと実行中のプロセスが将来の再インストールに適切な状態になるようにすることを推奨します。

ステップ 5　Common Services を含むすべての Cisco Security Management Suite アプリケーションをアンインストールする場合のみ：

a.　*NMSROOT* が残っている場合は、それを削除、移動、または名前を変更します。*NMSROOT* は Security Manager インストール ディレクトリへのパスです。*NMSROOT* のデフォルト値は **C:¥Program Files¥CSCOpx** です。**E:¥Program Files¥CSCOpx** などのその他の値も使用できます。

b.　C:¥CMFLOCK.TXT ファイルが存在する場合は、それを削除します。

c. アプリケーションを再インストールする前に、レジストリ エディタを使用して、次のレジストリ エントリを削除します。

- `My Computer¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Cisco¥Resource Manager`
- `My Computer¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Cisco¥MDC`

ステップ 6　アプリケーションをアンインストールする前に Windows Defender をディセーブルにした場合は、ここで、もう一度イネーブルにします。

サーバ アプリケーションのダウングレード

Security Manager アプリケーションを以前のリリースにダウングレードして、この製品リリースで作成した設定を保持することはできません。このリリースの Security Manager を使用しない場合は、これをアンインストールし、必要な古いバージョンの製品を再インストールします（これは、必要なライセンスと古いバージョンのインストール メディアが揃っていることが前提です）。その後で、「サーバ データベースの復元」（P.4-15）に記載されているように、ダウングレードされたバージョンの以前のインストールで保存した必要なデータベースのバックアップを復元できます。

Security Manager をダウングレードする場合は、Auto Update Server、Performance Monitor、および RME も、再インストールする Security Manager のバージョンでサポートされるバージョンにダウングレードする必要があります。

古いデータベースを復元した場合、管理対象デバイスの現在の状態と同期しなくなったデバイスのプロパティやポリシーが含まれる可能性があることに注意してください。たとえば、デバイス上のオペレーティング システムを、古いバージョンの Security Manager では直接サポートされないものにアップグレードしたり、古いバージョンには存在しないポリシーを設定し、展開したりした可能性があります。データベースとデバイスを正しく同期させるために、すべての管理対象デバイスのデバイス ポリシーを再検出することを検討してください。大幅な変更（オペレーティング システムのメジャー リリースのアップグレードなど）では、デバイスをインベントリから削除し、再度追加しなければならない場合があることに注意してください。一部の例では、オペレーティング システムのアップグレードを元に戻す必要がある場合もあります（たとえば、ASA ソフトウェア リリース 8.3 は特別な処理が必要で、下位互換モードではサポートできないため、使用する Security Manager のバージョンで直接サポートされている必要があります）。詳細については、『User Guide for Cisco Security Manager』の「Managing the Device Inventory」の章を参照してください。

ヒント　古いバージョンの Security Manager では管理できないデバイスとオペレーティング システム リリースの組み合わせを管理しようとした場合、展開エラーが発生します。