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

この章では、Security Manager サーバーソフトウェアとその他のサーバーアプリケーション（CiscoWorks Common Services 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ー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。

- [管理者（admin）]：管理者ユーザーアカウントは、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）]：casuser ユーザーアカウントは、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

  次の 5 つの権限は Security Manager のインストール時に自動的に割り当てられ、設定されます。
  - ネットワークからこのコンピュータにアクセスする：casusers
  - ネットワークからこのコンピュータへのアクセスを拒否する：casuser
  - ローカルのログオンを拒否する：casuser
  - バッチ処理としてログオンする：casuser、casusers
  - サービスとしてログオンする：casuser

- [システム識別（System Identity）]：システム識別ユーザーアカウントは、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ーは、マルチサーバーセットアップ内の他のサーバー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ー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、「ユーザーアカウントの管理」を参照してください。

（注） Cisco Security Manager 4.21 以降では、以前の ACS サーバーの代わりに Cisco Identity Services Engine（ISE）を認証に使用できます。

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）を行う必要がある場合は、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、直接接続されたディスクドライブ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。Remote Desktop Connection を使用する場合は、Remote Desktop Protocol 非コンソール セッションではなく、コンソール セッションを使用することを推奨します。

、Common Services、および 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 4.2.2：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 4.4 から、[CiscoWorks Common Services（CiscoWorks Common Services）] チェックボックスはコンポーネントの選択ページに表示されなくなりました。Common Services のインストールは、デフォルトで選択されます。

（注） バージョン 4.26 以降では、Azul JRE 1.8.0 Update 322 が新規インストール用にインストールされます。

- Cisco Security Manager 4.27：Security Manager のメイン サーバ ソフトウェアです。

  Security Manager をインストールすると、Cisco Common Works Common Services 4.2.2 および Cisco Security Manager Client 4.27 が CSM 4.27 バンドルの一部としてデフォルトでインストールされます。

（注） zip ファイルを解凍し、フォルダの名前を変更します。名前を変更するときは、フォルダの名前にスペースや「_」以外の特殊文字が含まれていないことを確認してください。

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 （8 ページ）を参照してください。

はじめる前に

- このインストレーションガイドの「Security Manager のライセンス」の章を参照してください。
- 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 （31 ページ）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 の永久ライセンスのインストール時は、Security Manager サーバにとってローカルなディスク上にライセンス ファイルを配置する必要があります。Security Manager を使用してサーバ上のディレクトリを参照する場合、マップされたドライブは表示されません。そのため、インストール時にライセンス ファイルを選択するには、そのライセンス ファイルがサーバ上に存在している必要があります。（Windows ではこの制限が課されますが、これにより Security Manager のパフォーマンスとセキュリティが向上します）。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。

（注） ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

- インストール準備状況チェックリストを完了したことを確認してください。
- サーバがサーバの要件および推奨事項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ー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。
- 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 へのユーザーアクセスに 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 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（このサーバー上または別のサーバー上）を ACS に登録していない場合は、[はい（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、[はい（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ーロールのカスタマイズが失われるため、[いいえ（No）] を選択する必要があります。同じ ACS サーバーを使用するすべての Security Manager サーバー サーバーがユーザーロールを共有します。

手順

Security Manager サーバー、Common Services、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。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。[ソフトウェアのダウンロード（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 Security Manager 4.27 でサポートされているオペレーティングシステム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:\Cisco_Security_Manager\server\installation_directory」より「C:\CSM」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。

ヒント 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、一時ディレクトリを空にして、ウイルスをスキャンし、C:\Program Files (x86)\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。新規インストール中に、次の情報の入力が要求されます。

[バックアップの場所（Backup location）]：特定のバージョンの 、Security Manager、 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。

（注） バックアップに使用するために選択する場所は、*NMSROOT* の外にする必要があります。場所 *NMSROOT* はSecurity Managerインストールディレクトリへのパスです。デフォルトは **C:\Program Files (x86)\CSCOpx** です。特に、*NMSROOT*\backup をバックアップに使用しないように注意してください。

[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。また、デフォルト フォルダ以外のフォルダを指定すると、パスに特殊文字を含めることはできません。Windows Server 2012 R2では、非システムドライブでの8dot3名の生成が無効になるため、ユーザーは非システムドライブパスのProgram Files (x86)フォルダを選択できません。その結果、8dot3表記を設定した後、ユーザーはサーバーを再起動する必要があります。特定のドライブで8dot3命名を有効にすると、既存のフォルダの略称は作成されません。略称を強制的に作成するには、再起動後にフォルダを削除して再作成する必要があります。既存のフォルダが空でない場合は、新しいフォルダを選択してインストールを続行してください。

（注） 非システムドライブのインストールディレクトリ パスに特殊文字「(「および「)」が含まれていないことを確認します。これらの特殊文字が存在する場合、インストールは続行されません。

- [アプリケーション（Applications）]：インストールするアプリケーション（Security Manager）。CiscoWorks Common Services 4.2.2 が Security Manager のインストール時に自動的にインストールされます。
- [License information]：次のいずれかを選択します。
  - [ライセンスファイルロケーション（License File Location）]：ライセンスファイルのフルパス名を入力するか、[参照（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。

    （注） ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

  - [評価のみ（Evaluation Only）]：無料の 90 日の評価期間をイネーブルにします。
- [管理者パスワード（Admin password）]：5 文字以上の管理者ユーザー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 （1 ページ）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。

  （注） パスワードの複雑度の制限に対するセキュリティ ポリシーがある場合、このアカウント作成は失敗することがあります。このような場合は、手動でcasuserアカウントを作成する必要があります（表 A-3、表 1の casuser パスワードの詳細な手順を参照してください）。

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） ソース インストールディレクトリに特殊文字が含まれていないことを確認します。特殊文字が含まれている場合、Security Manager は警告メッセージをスローし、インストーラが終了します。

サードパーティ証明書を使用した Cisco Security Manager へのアクセス

サードパーティ証明書をインストールして、CSM サーバーにアクセスできます。セキュアモードで CSM サーバーを呼び出すには、次の手順を実行します。

- サーバー証明書のホスト名を適切に設定し、同じホスト名を使用して CSM を呼び出します。
- 著名なサードパーティ認証局によって発行されたサーバー証明書を使用します。
- 自己署名証明書を使用している場合は、ブラウザを次のように変更します。
  - Mozilla Firefox 2.0 では、サーバーの ID に確信がある場合は、[サイト証明書の新規作成（New Site Certificate）] ウィザードで [サーバー証明書を永久に（期限切れまで）受け入れる（Accept the Server Certificate forever (until it expires)）] を選択します。
  - Mozilla Firefox 3.0 では、サーバーの ID に確信がある場合は、[セキュリティ例外の追加（Add Security Exception）] ダイアログボックスで [この例外を永久的に保存する（Permanently store this exception）] を選択します。
  - Internet Explorer で、サーバーの ID に確信がある場合は、ブラウザの信頼できる証明書ストアに証明書をインストールします。
- Internet Explorer 6.0 に証明書をインストールするには、「Internet Explorer 6.0 での証明書のインストール：」を参照してください。
- Internet Explorer 7.0 に証明書をインストールするには、「Internet Explorer 7.0 での証明書のインストール：」を参照してください。

Internet Explorer 6.0 での証明書のインストール：

ステップ 1 セキュアモードで CSM を起動します。

ステップ 2 [セキュリティアラート（Security Alert）] ウィンドウで、[証明書の表示（View Certificates）] ボタンをクリックします。

[Certificate] ダイアログボックスが表示されます。

ステップ 3 [証明書（Certificate）] ダイアログボックスで、[証明書のインストール（Install Certificate）] をクリックします。

Internet Explorer 7.0 での証明書のインストール：

ステップ 1 [ツール（Tools）] > [インターネットオプション（Internet Options）] を選択します。

ステップ 2 [コンテンツ（Content）] タブをクリックします。

ステップ 3 [証明書（Certificates）] をクリックします。

[Certificate] ダイアログボックスが表示されます。

ステップ 4 [証明書（Certificate）] ダイアログボックスで [インポート...（Import...）] をクリックします。

[証明書のインポート（Certificate Import）] ウィザードが表示され、証明書をインポートするためのガイドが表示されます。

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。
  - データベースの移行エラーが発生した場合はエラーメッセージが表示されます。これが表示されるのは、停止しなくてもインストールを先に進めることが可能な時点です。

（注） ローカル アップグレード時に、インストーラによって、Performance Monitor または Resource Manager Essentials がインストールされているかどうかがチェックされます。いずれか 1 つ、または両方が検出された場合、「Performance Monitor or Resource Manager Essentials (or both) needs to be uninstalled」というエラー メッセージを表示してインストーラが終了します。

（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 （28 ページ）を参照してください。

- 間接：ローカル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。

（注） イベント管理が有効になっているすべての間接アップグレードには特記事項が適用されます（[Configuration Manager（Configuration Manager）] > [ツール（Tools）] > [Security Managerの管理...（Security Manager Administration...）] > [イベント管理（Event Management）] > [イベント管理グループ（Event Management group）] > [イベント管理の有効化（Enable Event Management）]）。このような状況では、イベントの詳細ビュー（[起動（Launch）] > [イベントビューア（Event Viewer）] > [イベントの詳細（Event Details）] > [詳細（Details）]）でエラーがスローされます。このエラーの根本原因は、古いバージョンのイベントデータベースを復元してからイベントデータをロードしたことです。この問題を回避するには、すべての古いパーティション（間接アップグレードの前に生成されたイベントデータを含むパーティション）を特定し、Security Manager GUI の [拡張データストアの場所（Extended Data Store Location）] でセカンダリパーティションに移動します（[Configuration Manager（Configuration Manager）] > [ツール（Tools）] > [Security Managerの管理...（Security Manager Administration...）] > [イベント管理（Event Management）]）。

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、Security Manager 3.0.x からアップグレードする場合は、3.2.2 にアップグレードしてから、間接アップグレードパスに従って 3.2.2 から 4.27 にアップグレードする必要があります。

表 1 : アプリケーション アップグレード パス 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。

次のアップグレード パスがサポートされています。

- 4.26（サービスパックを含む）> 4.27

（注） 4.26 より前のバージョンからアップグレードする場合は、4.27 にアップグレードする前に 4.26 にアップグレードする必要があります。CSM 4.27 へのローカルアップグレード（インラインアップグレード）は、4.26 からのみサポートされています。他のバージョンから 4.26 にアップグレードする場合の詳細については、『CSM 4.26 Installation Guide』[英語] を参照してください。

表 *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（インライン）	Security Manager 4.27	4.26	**1.** 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 （28 ページ）を参照してください。 **2.** その後で、ソフトウェアをインストールします。 、Common Services、および のインストール （3 ページ）を参照してください。 **3.** 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 （35 ページ）を参照してください。
リモート（Remote）	Security Manager 4.27	4.26	**1.** 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 （28 ページ）を参照してください。 **2.** 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 （31 ページ）を参照してください。 **3.** 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。 、Common Services、および のインストール （3 ページ） **1.** 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。 **2.** データベースを回復します。 サーバ データベースの復元 （34 ページ）を参照してください。 **3.** 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 （35 ページ）を参照してください。
間接（Indirect）	Security Manager 4.27	4.25	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.26 にアップグレードしてから、4.26 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。 **3.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.24	1. 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 （28 ページ）を参照してください。 2. 次に、4.25 にアップグレードしてから、4.25 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。 3. 次に、4.26 にアップグレードしてから、4.26 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。 4. 最後に、4.27 にアップグレードして、4.27 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。
間接（Indirect）	Security Manager 4.27	4.23	1. 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 （28 ページ）を参照してください。 2. 次に、4.25 にアップグレードしてから、4.25 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。 3. 次に、4.26 にアップグレードしてから、4.26 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。 4. 最後に、4.27 にアップグレードして、4.27 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。
間接（Indirect）	Security Manager 4.27	4.22	1. 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 （28 ページ）を参照してください。 2. 次に、4.24 にアップグレードしてから、4.24 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。 3. 次に、4.25 にアップグレードしてから、4.25 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。 4. 次に、4.26 にアップグレードしてから、4.26 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。 5. 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.21	1. 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 （28 ページ）を参照してください。 2. 次に、4.23 にアップグレードしてから、4.23 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。 3. 次に、4.25 にアップグレードしてから、4.25 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。 4. 次に、4.26 にアップグレードしてから、4.26 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。 5. 最後に、4.27 にアップグレードして、4.27 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。
間接（Indirect）	Security Manager 4.27	4.20	1. 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 （28 ページ）を参照してください。 2. 次に、4.22 にアップグレードしてから、4.22 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。 3. 次に、4.24 にアップグレードしてから、4.24 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。 4. 次に、4.25 にアップグレードしてから、4.25 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。 5. 次に、4.26 にアップグレードしてから、4.26 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。 6. 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.19	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.21 にアップグレードしてから、4.21 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。 **3.** 次に、4.23 にアップグレードしてから、4.23 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。 **4.** 次に、4.25 にアップグレードしてから、4.25 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。 **5.** 次に、4.26 にアップグレードしてから、4.26 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。 **6.** 最後に、4.27 にアップグレードして、4.27 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。
間接（Indirect）	Security Manager 4.27	4.18	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.20 にアップグレードしてから、4.20 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。 **3.** 次に、4.22 にアップグレードしてから、4.22 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。 **4.** 次に、4.24 にアップグレードしてから、4.24 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。 **5.** 次に、4.25 にアップグレードしてから、4.25 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。 **6.** 次に、4.26 にアップグレードしてから、4.26 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。 **7.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.17	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.21 にアップグレードしてから、4.21 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。 **3.** 次に、4.23 にアップグレードしてから、4.23 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。 **4.** 次に、4.25 にアップグレードしてから、4.25 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。 **5.** 次に、4.26 にアップグレードしてから、4.26 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。 **6.** 最後に、4.27 にアップグレードして、4.27 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。
間接（Indirect）	Security Manager 4.27	4.16	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.18 にアップグレードしてから、4.18 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。 **3.** 次に、4.20 にアップグレードしてから、4.20 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。 **4.** 次に、4.22 にアップグレードしてから、4.22 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。 **5.** 次に、4.24 にアップグレードしてから、4.24 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。 **6.** 次に、4.25 にアップグレードしてから、4.25 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。 **7.** 次に、4.26 にアップグレードしてから、4.26 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。 **8.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.15	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.17 にアップグレードしてから、4.17 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。 **3.** 次に、4.19 にアップグレードしてから、4.19 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。 **4.** 次に、4.21 にアップグレードしてから、4.21 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。 **5.** 次に、4.23 にアップグレードしてから、4.23 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。 **6.** 次に、4.25 にアップグレードしてから、4.25 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。 **7.** 次に、4.26 にアップグレードしてから、4.26 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。 **8.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.25	4.14	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.16 にアップグレードしてから、4.16 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。 **3.** 次に、4.18 にアップグレードしてから、4.18 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。 **4.** 次に、4.20 にアップグレードしてから、4.20 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。 **5.** 次に、4.22 にアップグレードしてから、4.22 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。 **6.** 次に、4.24 にアップグレードしてから、4.24 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。 **7.** 次に、4.25 にアップグレードしてから、4.25 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。 **8.** 次に、4.26 にアップグレードしてから、4.26 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。 **9.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.13	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.15 にアップグレードしてから、4.15 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。 **3.** 次に、4.17 にアップグレードしてから、4.17 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。 **4.** 次に、4.19 にアップグレードしてから、4.19 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。 **5.** 次に、4.21 にアップグレードしてから、4.21 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。 **6.** 次に、4.23 にアップグレードしてから、4.23 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。 **7.** 次に、4.25 にアップグレードしてから、4.25 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。 **8.** 次に、4.26 にアップグレードしてから、4.26 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。 **9.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.12	**1.** すべての保留データをコミットします。次を参照してください。 • Cisco Security Manager 4.12 SP2 からのアップグレード中のデータベースエラー解決 （28 ページ）。 • Security Manager の保留データが送信および承認されることの確認 （28 ページ）。 **2.** 次に、4.14 にアップグレードしてから、4.14 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。 **3.** 次に、4.16 にアップグレードしてから、4.16 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。 **4.** 次に、4.18 にアップグレードしてから、4.18 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。 **5.** 次に、4.20 にアップグレードしてから、4.20 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。 **6.** 次に、4.22 にアップグレードしてから、4.22 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。 **7.** 次に、4.24 にアップグレードしてから、4.24 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。 **8.** 次に、4.25 にアップグレードしてから、4.25 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。 **9.** 次に、4.26 にアップグレードしてから、4.26 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。 **10.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.11	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.13 にアップグレードしてから、4.13 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。 **3.** 次に、4.15 にアップグレードしてから、4.15 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。 **4.** 次に、4.17 にアップグレードしてから、4.17 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。 **5.** 次に、4.19 にアップグレードしてから、4.19 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。 **6.** 次に、4.21 にアップグレードしてから、4.21 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。 **7.** 次に、4.23 にアップグレードしてから、4.23 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。 **8.** 次に、4.25 にアップグレードしてから、4.25 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。 **9.** 次に、4.26 にアップグレードしてから、4.26 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。 **10.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.10	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.12 にアップグレードしてから、4.12 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。 **3.** 次に、4.14 にアップグレードしてから、4.14 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。 **4.** 次に、4.16 にアップグレードしてから、4.16 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。 **5.** 次に、4.18 にアップグレードしてから、4.18 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。 **6.** 次に、4.20 にアップグレードしてから、4.20 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。 **7.** 次に、4.22 にアップグレードしてから、4.22 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。 **8.** 次に、4.24 にアップグレードしてから、4.24 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。 **9.** 次に、4.25 にアップグレードしてから、4.25 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。 **10.** 次に、4.26 にアップグレードしてから、4.26 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。 **11.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.9	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.11 にアップグレードしてから、4.11 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。 **3.** 次に、4.13 にアップグレードしてから、4.13 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。 **4.** 次に、4.15 にアップグレードしてから、4.15 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。 **5.** 次に、4.17 にアップグレードしてから、4.17 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。 **6.** 次に、4.19 にアップグレードしてから、4.19 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。 **7.** 次に、4.21 にアップグレードしてから、4.21 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。 **8.** 次に、4.23 にアップグレードしてから、4.23 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。 **9.** 次に、4.25 にアップグレードしてから、4.25 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。 **10.** 次に、4.26 にアップグレードしてから、4.26 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。 **11.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.8	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.10 にアップグレードしてから、4.10 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。 **3.** 次に、4.12 にアップグレードしてから、4.12 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。 **4.** 次に、4.14 にアップグレードしてから、4.14 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。 **5.** 次に、4.16 にアップグレードしてから、4.16 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。 **6.** 次に、4.18 にアップグレードしてから、4.18 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。 **7.** 次に、4.20 にアップグレードしてから、4.20 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。 **8.** 次に、4.22 にアップグレードしてから、4.22 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。 **9.** 次に、4.24 にアップグレードしてから、4.24 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。 **10.** 次に、4.25 にアップグレードしてから、4.25 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。 **11.** 次に、4.26 にアップグレードしてから、4.26 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。 **12.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.7	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.9 にアップグレードしてから、4.9 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。 **3.** 次に、4.11 にアップグレードしてから、4.11 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。 **4.** 次に、4.13 にアップグレードしてから、4.13 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。 **5.** 次に、4.15 にアップグレードしてから、4.15 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。 **6.** 次に、4.17 にアップグレードしてから、4.17 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。 **7.** 次に、4.19 にアップグレードしてから、4.19 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。 **8.** 次に、4.21 にアップグレードしてから、4.21 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。 **9.** 次に、4.23 にアップグレードしてから、4.23 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。 **10.** 次に、4.25 にアップグレードしてから、4.25 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。 **11.** 次に、4.26 にアップグレードしてから、4.26 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。 **12.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.6	

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
			1. 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 （28 ページ）を参照してください。 **2.** 次に、4.8 にアップグレードしてから、4.8 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。 **3.** 次に、4.10 にアップグレードしてから、4.10 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。 **4.** 次に、4.12 にアップグレードしてから、4.12 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。 **5.** 次に、4.14 にアップグレードしてから、4.14 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。 **6.** 次に、4.16 にアップグレードしてから、4.16 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。 **7.** 次に、4.18 にアップグレードしてから、4.18 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。 **8.** 次に、4.20 にアップグレードしてから、4.20 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。 **9.** 次に、4.22 にアップグレードしてから、4.22 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。 **10.** 次に、4.24 にアップグレードしてから、4.24 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。 **11.** 次に、4.25 にアップグレードしてから、4.25 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。 **12.** 次に、4.26 にアップグレードしてから、4.26 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。 **13.** 次に、4.25 にアップグレードしてから、4.25 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。 **14.** 次に、4.26 にアップグレードしてから、4.26 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。

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
			15. 最後に、4.27 にアップグレードして、4.27 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。
間接（Indirect）	Security Manager 4.25	4.5	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.7 にアップグレードしてから、4.7 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。 **3.** 次に、4.9 にアップグレードしてから、4.9 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。 **4.** 次に、4.11 にアップグレードしてから、4.11 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。 **5.** 次に、4.13 にアップグレードしてから、4.13 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。 **6.** 次に、4.15 にアップグレードしてから、4.15 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。 **7.** 次に、4.17 にアップグレードしてから、4.17 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。 **8.** 次に、4.19 にアップグレードしてから、4.19 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。 **9.** 次に、4.21 にアップグレードしてから、4.21 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。 **10.** 次に、4.23 にアップグレードしてから、4.23 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。 **11.** 次に、4.25 にアップグレードしてから、4.25 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。 **12.** 次に、4.26 にアップグレードしてから、4.26 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。 **13.** 最後に、4.27 にアップグレードして、4.27 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。

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（Indirect）	Security Manager 4.27	4.4	**1.** 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 （28 ページ）を参照してください。 **2.** 次に、4.6 にアップグレードしてから、4.6 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。 **3.** 次に、4.8 にアップグレードしてから、4.8 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。 **4.** 次に、4.10 にアップグレードしてから、4.10 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。 **5.** 次に、4.12 にアップグレードしてから、4.12 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。 **6.** 次に、4.14 にアップグレードしてから、4.14 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。 **7.** 次に、4.16 にアップグレードしてから、4.16 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。 **8.** 次に、4.18 にアップグレードしてから、4.18 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。 **9.** 次に、4.20 にアップグレードしてから、4.20 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。 **10.** 次に、4.22 にアップグレードしてから、4.22 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。 **11.** 次に、4.24 にアップグレードしてから、4.24 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。 **12.** 次に、4.25 にアップグレードしてから、4.25 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。 **13.** 次に、4.26 にアップグレードしてから、4.26 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。 **14.** 最後に、4.27 にアップグレードして、4.27 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。

Cisco Security Manager 4.12 SP2 からのアップグレード中のデータベースエラー解決

Cisco Security Manager 4.12 SP2 からのインライン（ローカル）アップグレードまたはリモートアップグレードの実行中に、デバイスの展開と設定に影響を与えるデータベース移行エラーが発生する可能性があります。

（注） Cisco Security Manager 4.12 SP2 からのアップグレードでは、インラインアップグレードはサポートされていません。リモートアップグレード手順に従い、以下の手順を参照してデータベース移行の問題を解決します。

データベース移行の問題を解決するには、次の手順を実行します。

ステップ 1 Cisco Security Manager 4.27 をインストールしたら、~CSCOpx\upgrade\data\412999999 に移動し、メモ帳などのテキストエディタで Admin_properties.sql ファイルを開きます。

ステップ 2 次のコンテンツを探します。

```
INSERT INTO ADMIN_PROPERTIES (PROPERTY,VALUE,DEFAULTVALUE) values
('workflow.deployjob.submittercanapprove','true','true')
```

ステップ 3 このコンテンツを次に置き換えます。

```
if not exists (select 1 from ADMIN_PROPERTIES where PROPERTY = 'workflow.deployjob.submittercanapprove')
then

INSERT INTO ADMIN_PROPERTIES (PROPERTY,VALUE,DEFAULTVALUE) values
('workflow.deployjob.submittercanapprove','true','true')

end if;
```

ステップ 4 Admin_properties.sql ファイルを保存します。

ステップ 5 Cisco Security Manager 4.12 SP2 データベースのバックアップの復元に進みます。

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。Approver 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。

- ワークフロー以外のモードで、次の手順を実行します。
  - 変更をコミットするには、[ファイル（File）] > [送信（Submit）] を選択します。
  - コミットされていない変更を廃棄するには、[ファイル（File）] > [廃棄（Discard）] を選択します。
  - 別のユーザーの変更をコミットまたは廃棄する必要がある場合は、そのユーザー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、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [ユーザーセッションの引き継ぎ（Take Over User Session）] を選択し、[セッションの引き継ぎ（Take Over Session）] をクリックします。
- ワークフロー モードで、次の手順を実行します。
  - 変更をコミットして承認するには、[ツール（Tools））] > [Activity Manager（Activity Manager）] を選択します。[Activity Manager] ウィンドウからアクティビティを選択し、[承認（Approve）] をクリックします。Activity Approver を使用している場合は、[送信（Submit）] をクリックして、Approver にアクティビティを承認してもらいます。
  - コミットされていない変更を破棄するには、[ツール（Tools）] > [Activity Manager（Activity Manager）] を選択します。[Activity Manager（Activity Manager）] ウィンドウで、アクティビティを選択してから、[廃棄（Discard）] をクリックします。廃棄できるのは、Edit または Edit Open の状態にあるアクティビティだけです。

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 (x86)\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後の csm.properties ファイルの編集

リモートアップグレード後、csm.properties ファイルを編集して、新しく追加されたプロパティを含める必要があります。次の手順に従ってください。

ステップ 1 *$NMSROOT* \MDC\athena\config\ サブディレクトリから、メモ帳などのテキストエディタで csm.properties を開きます。

（*$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 (x86)\CSCOpx）のフルパス名です）。

ステップ 2 csm.properties ファイルの末尾に次の内容を追加します。

```
##
# アクティビティレポート生成のカスタマイズ
##
# レポート生成タイムアウト（分単位）
# デフォルトで 10 分に設定
#generate_activity_report_timeout=10
# PDF レポートの生成
#generate_activity_pdf_report=true
# HTML レポートの生成
#generate_activity_html_report=false
#CSCup28957：これにより、ユーザーは、適用可能なすべてのポリシーの操作行のリストをアクティビティ変更レポートから除外できます。
# 除外操作はカンマで区切る必要があり、空またはコメント化されている場合は、すべての操作が含まれます。
# 除外操作：Add,Delete,Modify,Move,ReOrder,Assign,UnAssign。これらの名前は変更しないでください。
# デフォルトでは空です。除外操作が必要な場合は、必要な除外操作を追加します。
```

例：1.ActChangeReport.excludedOperations=ReOrder、2.ActChangeReport.excludedOperations=Add,ReOrder、3.ActChangeReport.excludedOperations=Add,Modify,Move,ReOrder

ActChangeReport.excludedOperations=

上記のコード行は、デフォルトでコメント化されています。デフォルト値を使用する場合、またはファイル内の特定のプロパティの値を変更する場合は、最初に特定のコード行のコメントを解除する必要があります。たとえば、Security Manager でアクティビティレポートを PDF 形式で生成する場合は、次のように特定のプロパティを変更する必要があります。

PDF レポートの生成

generate_activity_pdf_report=true

ステップ 3 編集したファイルを保存して閉じます。

ステップ 4 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] から Cisco Security Manager Daemon Manager サービスを再起動します。

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。

（注） Security Manager 4.4 から、新しい属性の PURGE_DBBACKUP_LOG が backup.properties ファイルに追加されました。デフォルト値は 20 で、20 日経過した後にバックアップを削除するという意味です。この新しい属性が NIL に設定されている場合、バックアップは削除されません。dbbackup.log は dbbackup_[YYYY-MM-DD_HH-mm-ss].log のタイムスタンプ形式で作成されます。削除設定に関係なく、常時、dbbackup.log ファイルは少なくとも 5 個維持されます。

（注） データベースをバック アップするには、Short Date フォーマットは M/d/YYYY または M/d/yy にする必要があります。Short Date フォーマットを M/d/YYYY または M/d/yy に変更するには、[Start] > [Control Panel] > [Region and Language] > [Formats] > [Short Date] を選択し、次に Short Date フォーマットを M/d/YYYY または M/d/yy に変更します。

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 （36 ページ）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ーをバックアップしている場合は、Security Manager クライアントの [ツール（Tools）] > [バックアップ（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 （28 ページ）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を参照）。

b) [サーバー管理（Server Administration）] パネルをクリックします。次に、[サーバー（Server）] > [管理者（Admin）] > [バックアップ（Backup）] を選択します。

ステップ 2 [頻度（Frequency）] に対して [即時（Immediate）] を選択して、必要に応じて他のフィールドを設定し、[適用（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には数分かかる可能性があるため、再起動の完了前にユーザがクライアントを起動してしまうことがあります。この場合、デバイスポリシーのウィンドウに「error loading page」というメッセージが表示されることがあります。

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 （36 ページ）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 （28 ページ）を参照）。

ステップ 2 コマンドプロンプトで、**net stop crmdmgtd** と入力してすべてのプロセスを停止します。

ステップ 3 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 (x86)\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 などです。

（注） バックアップに使用するために選択する場所は、*NMSROOT* の外にする必要があります。場所 *NMSROOT* はSecurity Managerインストールディレクトリへのパスです。デフォルトは**C:\Program Files (x86)\CSCOpx** です。特に、*NMSROOT*\backup をバックアップに使用しないように注意してください。

（注） バックアップディレクトリには特殊文字を含めることはできません。

- *log_filename*：（任意）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にバックアップを作成する場合は、そのパスを追加します。C:\BackupLogs などです。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*：（任意）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 を設定して、通知をイネーブルにする必要があります。
- *number_of_generations*：（任意）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。最大数に達すると、古いバックアップが削除されます。デフォルトは 0 で、保存される世代数に制限はありません。
- **compress**：（任意）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いと、backup.properties ファイル内に VMS_FILEBACKUP_COMPRESS=NO が指定されている場合、バックアップは圧縮されません。指定されていない場合は、このキーワードを入力しなくてもバックアップは圧縮されます。バックアップは圧縮することを推奨します。

たとえば、次に示されているコマンドは、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。（ただし、該当ディレクトリの場合でも、DOS 8.1 形式（スペースなし）の完全修飾された、perl と backup.pl の完全なパスを指定する必要があります）。

次に示されているコマンドでは、バックアップディレクトリ内に圧縮されたバックアップおよびログファイルが作成され、admin@domain.com に通知が送信されます。

backup.pl コマンドを使用する場合、圧縮パラメータを含めるには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する場合は、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。

次の例では、$NMSROOT は D:\CSM であり、デフォルト値の C:\Program Files (x86)\CSCOpx ではありません。

D:\CSM\bin\perl D:\CSM\bin\backup.pl C:\backups C:\backups\backup.log email=admin@domain.com 0 compress

ステップ 4 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。

（注） データベースのバックアッププロセス中にSecurity Managerが予期せず再起動した場合、バックアップは中断され、バックアップロックファイル backup.lock が NMSROOT ディレクトリに作成されます。バックアップを続行するには、backup.lock ファイルを削除します。

ステップ 5 コマンドプロンプトで、**net start crmdmgtd** と入力して、すべてのプロセスを再起動します。

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り、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から再起動する必要があります。ここでは、サーバ上のバックアップデータベースを復元する方法について説明します。バックアップおよび復元のための機能は1つだけであり、CiscoWorksサーバにインストールされているすべてのアプリケーションをバックアップおよび復元できます。個々のアプリケーションをバックアップまたは復元することはできません。

複数のサーバにアプリケーションをインストールした場合は、インストールされているアプリケーションに適したデータが含まれるデータベースバックアップを復元する必要があります。

ヒント

- 以前のリリースのアプリケーションから作成したバックアップは、このバージョンのアプリケーションへのダイレクト ローカル インライン アップグレードがサポートされているバージョンからのバックアップであれば、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 （8 ページ）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 （36 ページ）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ように入力して、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 help**] [-m Email]

値は次のとおりです。

- $NMSROOT：Common Servicesインストールディレクトリ（デフォルトはC:\Program Files (x86)\CSCOpx）のフルパス名。
- **-t** *temporary_directory*：（任意）復元プログラムで一時ファイルを保存するために使用されるディレクトリまたはフォルダ。デフォルトでは、このディレクトリは *$NMSROOT* \tempBackupData です。

- **-gen** *generationNumber*：（任意）復元するバックアップ世代番号。デフォルトでは、最新の世代です。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含まれるバックアップディレクトリ。
- **-h**：（任意）ヘルプを表示します。**-d** *BackupDirectory* とともに使用すると、適切な構文と、使用可能なスイートおよび世代がヘルプに表示されます。
- -m：成功または失敗の復元ステータスに関する電子メールを送信するために使用します。

たとえば、c:\var\backup ディレクトリから最新のバージョンを復元する場合は、次のコマンドを入力します（これは 64 ビット OS の場合です）。

C:\Progra~2\CSCOpx\bin\perl C:\Progra~2\CSCOpx\bin\restorebackup.pl -d C:\var\backup

ステップ 3 ログファイル *NMSROOT***log\restorebackup.log** を調べて、データベースが復元されたことを確認します。

ステップ 4 次のように入力して、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 パックのインストール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

アプリケーションのアップグレードによって、Cisco Security Manager で特定のタイプの情報を処理する方法が変更される場合があります。このため、手動で変更を加える必要があります。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。

（注） また、アップグレード後の Security Manager のインストールに適用される可能性のある他の考慮事項については、このリリースのリリースノートの「特記事項」の項を参照してください。

- 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、[デバイスでポリシーを検出（Discover Policies on Device）] を選択してから、[検出するポリシー（Policies to Discover）] グループ内の [ライブデバイス（Live Device）] 検出と [インベントリ（Inventory）] チェックボックスのみをオンにします。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、未サポートの共有ポートアダプタ（SPA）を使用する Cisco ASR 1000 シリーズアグリゲーション サービスルータを管理し

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

（注） Cisco Security Manager 4.9 以降への移行中にオペレーティングシステムをアップグレードする場合は、適切な Windows ライセンスを購入する必要があります。

特定の状況では、Security Manager を新しいサーバーに移行する必要があります。この移行は、新しい物理マシンに対する移行である場合や、サーバー上のオペレーティングシステムのメジャーアップグレード（Microsoft Windows Server 2008 R2 with SP1 Enterprise（64 ビット）から Microsoft Windows Server 2012 Standard（64 ビット）または Microsoft Windows Server 2012 Datacenter（64 ビット）への移行など）を実行する場合である可能性があります。

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 （8 ページ）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。サーバーの移行は、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 ストア フォルダの名前を特定します。Security Manager クライアントで、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント管理（Event Management）] を選択します。フォルダは、[イベントデータストアの場所（Event Data Store Location）] フィールドに表示されています。デフォルトは *NMSROOT***MDC\eventing\database** で、NMSROOT はインストールディレクトリ（通常は C:\Program Files (x86)\CSCOpx）です。

b) コマンドラインで次のように入力して、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 （32 ページ）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。次に例を示します。

- 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ように入力して、すべてのプロセスを停止します。

net stop crmdmgtd

b) 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、ターゲットサーバー上のファイルを上書きします。

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 クライアントで、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント管理（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 [イベントデータストアの場所（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、[イベント管理の有効化（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。[保存（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求められます。[はい（Yes）] をクリックし、サービスが停止したこと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) Security Manager クライアントで、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント管理（Event Management）] を選択します。[イベント管理の有効化（Enable Event Management）] チェックボックスをオンにして、[保存（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求められます。[はい（Yes）] をクリックし、サービスが開始されたことが通知されるまで待ちます。

Security Manager の更新

インストール時に永久ライセンス ファイルを指定できますが、Security Manager のインストール後にもライセンスを追加できます。

はじめる前に

ライセンス ファイルをサーバ マシンまたはクライアント マシンにコピーしてから、ライセンスをアプリケーションに追加します。クライアントマシンを使用する場合は、クライアント側のブラウザをイネーブルにする必要があります。

（注） ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

ヒント Security Manager にログインする際にライセンスを適用することもできます。Security Manager から「ライセンスをアップグレード（Upgrade license）」または「評価を続行（Continue Evaluation）」というメッセージが表示されます。[ライセンスをアップグレード（Upgrade License）] をクリックすると、ライセンスを適用できます。

手順

Security Manager 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 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 へのログインを参照）。

ステップ 2 [ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ライセンス（Licensing）] を選択します。

ステップ 3 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。

ステップ 4 [ライセンスのインストール（Install a License）] をクリックして、[ライセンスのインストール（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（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。

（注） パスとファイル名は、英語のアルファベット文字に制限されます。日本語文字はサポートされません。Windows 日本語 OS システムでファイルを選択する場合は、通常のファイル区切り文字\がサポートされますが、これは円記号（U+00A5）として表示されることがあることに注意する必要があります。

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、[ヘルプ（Help）] > [Security Manager Online（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 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 （31 ページ）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ー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 [スタート（Start）]>[プログラム（Programs）]>[Cisco Security Manager（Cisco Security Manager）]>[Cisco Security Managerのアンインストール（Uninstall Cisco Security Manager）] を選択します。

デフォルトでは、すべてのアプリケーションがアンインストールされます。

ステップ 2 アンインストーラによって、すべての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、インストール中のサーバ障害と http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html にある『*Installing and Getting Started With CiscoWorks LAN Management Solution 3.1*』の「Troubleshooting and FAQs」[英語] の章を参照してください。

ステップ 3 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 4 次のステップは、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にのみ実行します。

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 (x86)\CSCOpx** です。**E:\Program Files (x86)\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\Wow6432Node\Cisco\Resource Manager
- My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\MDC

d) アンインストール中に削除されなかった *NMSROOT* の下のフォルダを削除します。

ステップ 5 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そろっていることが

前提です）。その後で、サーバ データベースの復元 （34 ページ）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。

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 [英語] 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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。