Cisco Security Manager サーバーの管理

ここでは、Security Manager 製品の一般的な操作に関連するシステム管理作業について説明します。

Security Manager サーバの管理および運用の概要

Cisco Security Manager は、ソフトウェア アプリケーションの 1 つとして、CiscoWorks Common Services アプリケーションにより提供されるフレームワークで動作します。基本的なサーバ制御機能の多くは、Common Services によって提供されます。たとえば、Security Manager に複数サーバ セットアップを作成するには、Common Services でそのセットアップを作成する必要があります。また、Common Services には、ローカル ユーザ アカウントの作成と管理、データベースのバックアップと復元、システム機能に関する各種レポートの生成を行うためのツールや、その他多くの基本的な機能に対応するツールも備わっています。

Common Services アプリケーションにアクセスするには、次のいずれかを実行します。

- Security Manager クライアントが現在開いている場合は、**[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 [サーバーセキュリティ（Server Security）] を選択します。[Server Security] ページには、Common Services の特定のページにリンクするボタンおよび特定のページを開くボタンが含まれています。任意のボタンをクリックして、Common Services の目的のページにナビゲートできます。

- Web ブラウザを使用し、URL https://*servername* を使用して Security Manager サーバーにリンクします（*servername* はサーバーの IP アドレスまたは DNS 名です）。この URL によって Security Manager ホームページが開きます。[サーバー管理（Server Administration）] または [CiscoWorks] リンクをクリックして、Common Services を開きます。

（注） Windows Server 2012（Standard または Datacenter）64 ビットで Internet Explorer 10.x を使用している場合は、特別な考慮事項が適用されます。これは、Cisco Security Manager のバージョン 4.7 で新たにサポートされます。次のナビゲーション パスを使用する場合は、この考慮事項に注意する必要があります。Windows の [スタート] > [Cisco Security Manager クライアント（Cisco Security Manager Client）] >（ログイン）> [Configuration Manager] > [ツール（Tools）] > [Security Manager管理...（Security Manager Administration...）] > [サーバーセキュリティ（Server Security）]。[サーバーセキュリティ（Server Security）] ページは通常どおり開きますが、そのページではボタン（[ローカルユーザセットアップ（Local User Setup）] など）を使用して、Common Services 内でサーバーセキュリティツールを相互起動することはできません。この問題を回避するには、Internet Explorer 10.x のイントラネット設定のセキュリティレベルを下げます。

Common Services で実行可能な操作の詳細については、Common Services オンライン ヘルプを参照してください。

（注） Common Services の **[ソフトウェアセンター（Software Center）] > [ソフトウェアの更新（Software Update）]** 機能は、Cisco Security Manager ではサポートされていません。

Security Manager サーバのクラスタの管理

Security Manager サーバ クラスタは、ネットワークを管理するために使用される 2 つ以上の Security Manager サーバです。一般的に、そのサーバ間の関係は維持することが求められます。クラスタ内のサーバー間に体系的な関係はありませんが、クラスタのような関係を維持するために使用できるいくつかのテクニックがあります。この章の各項では、Security Manager サーバのグループをクラスタとして管理する方法を説明します。

ここでは、次の内容について説明します。

Security Manager サーバ クラスタの管理

単一の Cisco Security Manager サーバーで多数のデバイスを管理できます。また一方で、ネットワークの管理に 2 つ以上の Security Manager サーバを使用する理由はさまざまです。次に例を示します。

- 管理対象のデバイスが非常に多い、大規模なネットワークの場合、単一のサーバからすべてのデバイスを管理しようとすると、パフォーマンスが許容できなくなる可能性があります。
- 地理的な理由から、管理対象デバイスにより近いサーバを用意した方が改善されると判断する場合。たとえば、世界各地に主要サイトがある場合は、各主要サイトに分けてサーバを置くと、管理を簡易化し、パフォーマンスを向上できます。また、管理対象デバイスに設定を展開する場合を例にすると、バンガロールにあるデバイスへの設定の展開は、サンフランシスコにある Security Manager サーバよりも、バンガロールにある Security Manager サーバの方がはるかに速く展開することができます。単純に物理的なネットワークの距離がとても近いためです。
- 管理されたテクノロジーに基づいて、デバイス管理をセグメント化する場合。たとえば、1 台のサーバでサイト間 VPN を管理し、もう 1 台のサーバで ASA ファイアウォールとリモート アクセス VPN ポリシーを管理し、さらに 3 台目のサーバで IPS を管理する場合があります。
- 分かれた複数の IT 組織がネットワークのそれぞれ別の部分を管理している場合。デバイス レベルでアクセス コントロールを微調整するように ACS を設定できますが、それよりも IT 組織ごとに別個の Security Manager サーバを用意する方が簡易化できます。

2 つ以上の Security Manager サーバをインストールする場合の主な課題は次のとおりです。

- 単一のサーバを 2 つ以上のサーバに分ける：現在、単一の Security Manager サーバを使用していて、複数のサーバの必要性がある場合。1 つの Security Manager サーバを 2 つ以上のサーバに分ける方法については、Security Manager サーバの分割 （3 ページ）を参照してください。
- 同一セットの共有ポリシーの維持：複数のサーバを使用して同じデバイス タイプを管理する場合は、デバイスに割り当てる共有ポリシーを同一に保つことができます。たとえば、同一セットの必須およびデフォルトのアクセス ルールをすべての ASA デバイスで継承させることができます。

同じ共有ポリシーのセットをサーバのクラスタ内で自動的に管理するプロセスは存在しません。代わりに、手動でメイン サーバからポリシーをエクスポートし、その他のサーバにインポートする必要があります。詳細については、Cisco Security Manager サーバー間での共有ポリシーの同期 （5 ページ）を参照してください。

Security Manager サーバの分割

単一の Security Manager サーバを 2 つ以上のサーバに切り替える必要がある場合は、元のサーバで管理しているデバイスのサブセットを新しいサーバに移動することによって、サーバを分

けることができます。特定の 1 つのネットワーク デバイスは単一の Security Manager サーバから管理する必要があるため、移動したデバイスを元のサーバから削除することに留意してください。

ヒント　すべてのサーバーで同じリリースの Security Manager ソフトウェアを使用します。

関連項目

- Security Manager サーバ クラスタの管理 （3 ページ）
- Cisco Security Manager サーバー間での共有ポリシーの同期 （5 ページ）
- 共有ポリシーのエクスポート （14 ページ）

ステップ 1　『Installation Guide for Cisco Security Manager』の説明に従って、新しい Security Manager サーバーをインストールします。

サーバが正しく機能していること、またサーバに移動しようとしているデバイスに対して十分なデバイス数でライセンスをインストールしたことを確認します。Professional ライセンスを必要とするデバイス タイプを管理する場合は、必ずそのライセンスを使用します。ライセンスのインストールの詳細については、Security Manager のライセンス ファイルのインストール （20 ページ）を参照してください。

ステップ 2　元のサーバ上の移動対象デバイスのポリシーで、新しいサーバの IP アドレスからのアクセスが許可されていることを確認します。たとえば、ASA およびルータ上のアクセス ルール、および IPS デバイス上の Allowed Hosts ポリシーを検討します。

ステップ 3　元のサーバで、移動しているデバイスに対するすべての設定変更が送信済みおよび展開済みであることを確認します。スタッフにその変更を送信して展開するように依頼する必要があります。Security Manager 内でこのステータスを確認する簡単な方法はありません。

この手順では、保留中で未確定の変更がないことを確認します。構成の展開については、Workflow モードに基づいた次のトピックを参照してください。

- Workflow 以外のモードでの設定の展開
- Workflow モードでの設定の展開

ステップ 4　**[ファイル（File）] > [エクスポート（Export）] > [デバイス（Devices）]** を選択して、元の Security Manager サーバーから割り当てられたポリシーとポリシーオブジェクトを持つデバイスをエクスポートします。デバイスのエクスポート時に [デバイス、ポリシー、およびオブジェクトのエクスポート（Export Devices, Policies, and Objects）] を選択して、ポリシー情報が含まれるようにします。ファイルタイプは **dev** にする必要があります。詳細については、Security Manager クライアントからのデバイス インベントリのエクスポート （7 ページ）を参照してください。

新規 Security Manager サーバごとに独自のデバイスを含む個別のエクスポート ファイルを作成します。

ヒント　この時点では、元のサーバ内のエクスポートされたデバイスに対してポリシーの変更を行わないでください。また、これらのデバイスに設定を展開しないでください。分割を行う前に元のサーバのデバイスに変更を行う必要性が見つかった場合は、新しいエクスポート ファイルを作成します。

ステップ 5　新しい Security Manager サーバーそれぞれで、**[ファイル（File）] > [インポート（Import）]** を選択して、エクスポートされた情報を新しいサーバーにインポートします。詳細については、ポリシーまたはデバイスのインポート （17 ページ）を参照してください。

ヒント　インポート時にデバイスグループは維持されません。すべてのデバイスが、All グループに配置されます。手動で目的のデバイス グループ構成を再作成し、デバイスを適切なグループに追加する必要があります。

ステップ 6　新しい Security Manager サーバごとに新しくインポートされたデバイスを管理できることを確認します。たとえば、変更されていないデバイスに対しても展開を実行して、新しいサーバーがすべてのデバイスに正常に接続して設定を展開できるようにすることができます。

ヒント　ポリシーまたはデバイスのインポート （17 ページ）で説明されているように、デバイスを設定するための変更が適用される前に、ポリシーを送信する必要があります。展開を行う前にポリシーを送信します。

ステップ 7　元のサーバを使用して、移動対象デバイスのいずれかをモニタしていた場合（つまり、Event Viewer およびオプションの Report Manager を使用していた場合）、新しいサーバに syslog メッセージが送信されるように、また新しいサーバからの接続を許可するように関連ポリシーを更新します。元のサーバのイベントデータまたはレポート データはいずれも、新しいサーバには転送されません。

Security Manager のモニタをイネーブルにするようにデバイスを設定する方法については、次の項を参照してください。

- イベント管理のための ASA と FWSM デバイスの設定
- イベント管理のための IPS デバイスの設定

ステップ 8　元の Security Manager サーバで、**[ファイル（File）] > [デバイスの削除（Delete Devices）]** を選択して、移動したデバイスを元のサーバーから削除します。デバイスの削除の詳細については、Security Manager インベントリからのデバイスの削除を参照してください。

Cisco Security Manager サーバー間での共有ポリシーの同期

複数の Security Manager サーバーがある場合、サーバー間で共有ポリシーを手動で同期できます。共有ポリシーを同期すると、これらの共有ポリシーで使用されるポリシーオブジェクトも同期されます。

ヒント

- 単一の Security Manager サーバーを「プライマリ」サーバー（正式なバージョンの共有ポリシーを含むサーバー）として識別するプログラムを使用した方法はありません。どのサーバーをプライマリとして使用するか決め、そのサーバーだけで共有ポリシーを編集することを定める必要があります。

- すべてのサーバーで同じリリースの Security Manager ソフトウェアを使用します。
- 特定のタイプのポリシーオブジェクトは、それらのオブジェクトが共有ポリシーで使用されていない場合でも、サーバー間で同期できます。同期するネットワーク/ホスト、サービス、またはポートリストオブジェクトがある場合は、ポリシーオブジェクトのインポートおよびエクスポートに説明されているコマンドを使用できます。
- 共有ポリシーおよびポリシーオブジェクトのインポート時には、常に同じ名前の既存の共有ポリシーまたはポリシーオブジェクトがインポートされた情報によって置換されます。そのため、ポリシーとオブジェクトをインポートするサーバー上でユーザーが独自の共有ポリシーとオブジェクトを作成できるようにする場合は、ポリシーとオブジェクトの命名規則を作成して、新しくインポートされたポリシーとオブジェクトによってユーザーポリシーとオブジェクトが誤って上書きされないようにすることが重要です。

関連項目

- Security Manager サーバ クラスタの管理 （3 ページ）
- Security Manager サーバの分割 （3 ページ）
- Security Manager クライアントからのデバイス インベントリのエクスポート （7 ページ）

ステップ 1 元のサーバで、共有ポリシーおよびポリシーオブジェクトに対するすべての設定変更が送信済みであることを確認します。スタッフにその変更を送信して承認が行われるように依頼する必要があります。Security Manager 内でこのステータスを確認する簡単な方法はありません。

共有ポリシーをエクスポートする場合、新しい変更がポリシーに割り当てられたデバイスに展開されていることを確認する必要はありません。デバイスの割り当てと展開のステータスは、エクスポートされた情報には含まれません。

ステップ 2 [ファイル（File）] > [エクスポート（Export）] > [ポリシー（Policies）] を選択して、共有ポリシーと共有ポリシーで使用されるポリシーオブジェクトをエクスポートします。エクスポート処理では、拡張子 **pol** を持つファイルが作成されます。

ヒント エクスポートするポリシーは選択できません。選択できるのはポリシータイプだけです。選択したタイプのすべての共有ポリシーがエクスポートされます。

詳細については、共有ポリシーのエクスポート （14 ページ）を参照してください。

ステップ 3 他の Security Manager サーバーのそれぞれで、[ファイル（File）] > [インポート（Import）] を選択して、エクスポートされた共有ポリシー情報をサーバーにインポートします。詳細については、ポリシーまたはデバイスのインポート （17 ページ）を参照してください。

ヒント インポートされるものと同じ名前の共有ポリシーまたはオブジェクトがあれば置換されます。ユーザーがポリシーまたはオブジェクトをすでにロックしている場合、ポリシーまたはオブジェクトのインポートは失敗します。ポリシーまたはデバイスのインポート （17 ページ）で説明されているように、デバイスを設定するための変更が適用される前に、ポリシーを送信する必要があります。

ステップ 4 共有ポリシーをすべてインポートしない場合、他のサーバ上ではインポートする予定のなかった共有ポリシーを削除します。これは手動の処理です。

デバイス インベントリのエクスポート

デバイスインベントリをエクスポートすると、インベントリを他のネットワーク管理アプリケーションにインポートしたり、独自のレポートを生成する目的で出力を操作したりできます。デバイス インベントリをエクスポートするには、相互に関連のない 2 つの方法があります。

- **[ファイル（File）] > [エクスポート（Export）] > [デバイス（Devices）]** コマンドを使用する：このコマンドを使用して、デバイスとその設定ポリシー全体を含む単純なカンマ区切り値（CSV）ファイルまたは圧縮された .dev ファイルを作成できます。CSV ファイルは、CiscoWorks Common Services Device Credential Repository（DCR）、Cisco Security Monitoring, Analysis and Response System（CS-MARS）、Cisco Prime Security Manager（PRSM）、または他の Cisco Security Manager のインストールへのインポートに適した形式です。つまり、スプレッドシートやテキストエディタのプログラムでファイルを開いて表示できます。.dev ファイルは、他の Security Manager サーバへのインポート専用です。詳細については、Security Manager クライアントからのデバイス インベントリのエクスポート （7 ページ）を参照してください。
- Perl スクリプト CSMgrDeviceExport を使用する：この Perl スクリプトでは、Security Manager クライアントを起動せずにインベントリをエクスポートできます。出力を画面または Comma-Separated Value（CSV; カンマ区切り値）ファイルに転送できます。詳細については、コマンドラインからのデバイス インベントリのエクスポート （13 ページ）を参照してください。

（注） 各デバイス設定の最新の 5 つのバージョンのみエクスポートされます。

Security Manager クライアントからのデバイス インベントリのエクスポート

デバイスインベントリをさまざまな形式でエクスポートできます。主な選択肢は次のとおりです。

- [CSVとしてエクスポート（Export as CSV）]（カンマ区切り値）：次のいずれかの形式でインベントリ情報を含む単純な CSV ファイルを作成できます。CSM（Cisco Security Manager で使用）、Device Credential Repository（DCR、CiscoWorks Common Services の場合）、および CS-MARS シードファイル（Cisco Security Monitoring、Analysis and Response System で使用）。スプレッドシート アプリケーションまたはテキストエディタで CSV ファイルを開き、他の Cisco Security Manager サーバーを含む、その形式をサポートするアプリケーションでそのファイルを使用できます。ただし、この形式にはポリシー情報が含まれないため、他の Security Manager サーバで使用する場合は、デバイスの追加時にポリシーを見つける必要があります。

- CSV形式の詳細については、インベントリのインポートまたはエクスポートでサポートされている CSV 形式 （11 ページ）を参照してください。
- CSV ファイルからデバイスをインポートする方法については、インベントリ ファイルからのデバイスの追加を参照してください。

- [デバイス、ポリシー、およびオブジェクトのエクスポート（Export Devices, Policies, and Objects）]：デバイスで使用されるすべてのデバイスのプロパティ、ポリシー、およびポリシーオブジェクトとともにデバイスインベントリをエクスポートします。エクスポートされた情報には、次の内容が含まれています。

（注） *.pol または *.dev ファイルのインポートは、各ファイルのエクスポート時に使用されたものと同じバージョンの Cisco Security Manager でのみサポートされます。あるバージョンの Cisco Security Manager からエクスポートして、別のバージョンを実行しているサーバーにインポートすることはできません。

- ポリシーで使用されるすべてのポリシーオブジェクト、およびオブジェクトのデバイスレベルのオーバーライドを含む、デバイスに割り当てられたすべてのローカルポリシーと共有ポリシー。共有ポリシーの割り当ては維持されます。
- デバイス プロパティおよびデバイス インベントリ。
- デバイスの Configuration Archive データ。
- デバイスの履歴スナップショット。
- デバイス証明書。
- IPS デバイス ライセンスおよび証明書情報。適用されたシグネチャはエクスポートされません（デバイスをインポートする場合は、同じシグネチャパッケージをサーバーに登録する必要があります）。IPS 更新設定は含まれていません。インポート後に再作成する必要があります。
- デバイスが参加している VPN トポロジ。ただし、VPN トポロジは、そのトポロジに参加しているすべてのデバイスがエクスポートに含まれる場合のみエクスポートされます。エクストラネット VPN は常にエクスポートされます。

したがって、エクスポート ファイルには、選択したデバイスのポリシー設定全体が含まれます。作成されたファイルは拡張子 .dev を持ち、他の Security Manager サーバからは読み取り専用にすることができます（ファイルの内容は圧縮されており、解読不能であるため、ユーザのポリシー情報のセキュリティが保持されます）。

.dev ファイルを別の Cisco Security Manager サーバーにインポートする方法については、ポリシーまたはデバイスのインポート （17 ページ）を参照してください。

エクスポートサイズの制限

Cisco Security Manager データベースに多数のデバイス、または多数のポリシーやポリシーオブジェクトが含まれている場合は、エラーを防ぐために、一度にエクスポートするデバイスの数を制限する必要があります。次のガイドラインを使用して、一度に正常にエクスポートできるデバイスの数を見積もることができます。

例 1：データベース内に 1000 以上のデバイス、デバイスごとに約 1500 以上のポリシー、データベース内に約 25,000 のオブジェクトがある場合。

- 一度にエクスポートできるデバイスの最大数（デバイスのみ）= 250
- 一度にエクスポートされるデバイスの最大数（ポリシーやオブジェクトと同時）= 100 ～ 150

例 2：データベース内に 1000 未満のデバイス、デバイスごとに約 1500 以上のポリシー、データベース内に約 10,000 ～ 15,000 のオブジェクトがある場合。

- 一度にエクスポートできるデバイスの最大数（デバイスのみ）= 250 ～ 300
- 一度にエクスポートされるデバイスの最大数（ポリシーやオブジェクトと同時）= 200

ヒント

- [デバイス、ポリシー、およびオブジェクトのエクスポート（Export Devices, Policies, and Objects）] オプションを選択すると、Cisco Security Manager サーバーまたはローカルの Cisco Security Manager クライアントにエクスポートできます。CSV ファイルをエクスポートする場合は、Cisco Security Manager サーバーにのみエクスポートできます。ローカル Cisco Security Manager クライアントにエクスポートまたはインポートする機能は、**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）]** から制御できます。詳細については、[Customize Desktop] ページを参照してください。
- エクスポートされたデバイスは、インベントリから削除されません。別の Cisco Security Manager サーバーからデバイスを管理する場合は、該当デバイスを別のサーバーに正常にインポートした後でデバイスを削除します。
- AUS または Configuration Engine を使用して構成を管理するデバイスを選択する場合は、エクスポートするデバイスのリストでサーバーも選択する必要があります。AUS または Configuration Engine の情報は、CS-MARS 形式にはエクスポートできません。
- 管理対象外のデバイスをエクスポートできます。
- ポリシーとともにデバイスをエクスポートする場合、送信済みかつ承認済みのポリシーおよびポリシーオブジェクトのみエクスポートファイルに含まれます。ポリシーおよびポリシーオブジェクトとともにデバイスをエクスポートする前に、必要なすべての送信と承認が行われていることを確認します。
- イベントデータとレポートデータ（つまり、イベントビューアまたは Report Manager で使用できるデータ）を含むエクスポートファイルのタイプはありません。したがって、別の Cisco Security Manager サーバーに移動する目的でデバイスをエクスポートしている場合、すでに収集されているそのデバイスに関するイベントおよびレポートデータは、新しいサーバーでは使用できません。

- デバイスグループ情報を含むエクスポートファイルのタイプはありません。デバイスをインポートしたあとに、手動でデバイス グループを再作成し、そのグループにデバイスを割り当てる必要があります。
- セキュリティコンテキストまたは仮想センサーを選択するときは、ホストデバイスも選択してください。また、デバイスが VPN に参加している場合は、デバイス、ポリシー、およびポリシー オブジェクトのエクスポート時に VPN 内のすべてのデバイスを選択するようにします。
- IPS または IOS IPS デバイスを選択する場合は、すでに IPS シグニチャの更新をデバイスに適用済みであることを確認します。基本センサーパッケージ（Sig0）を使用して IPS または IOS IPS デバイスをエクスポートできますが、インポートはできません。インポートエラー「Sig0 パッケージがありません（missing Sig0 package）」が表示されます。
- 別のデバイスに含まれているデバイス タイプのうち、Catalyst 6500/7600 内の任意のモジュール、ルータ内の AIM モジュールまたは NME モジュールを選択すると、ホスティング デバイスも自動的にエクスポートされます。ASA デバイスとその IPS モジュールを別々にエクスポートできます。
- アクティビティ セッションまたは設定セッションの承認中は、デバイスとそのポリシー（.dev 形式）をエクスポートできません。デバイスとそのポリシーをエクスポートするには、先にすべての承認が完了している必要があります。アプルーバのいる Workflow モードでは、アプルーバに問い合わせ、承認をただちに完了させるように依頼します。Workflow 以外のモードまたはアプルーバのいない Workflow モードでは、変更が送信されると承認が自動的に行われるため、数分待ってからエクスポートを再試行します。
- デバイスとそのポリシー（.dev 形式）のエクスポート中は、ポリシーの変更を承認できません。エクスポートファイルが作成されるとすぐにコマンドが終了し、ユーザは再びポリシーの変更を承認できるようになります。このことは、Workflow 以外のモードまたはアプルーバのいない Workflow モードの場合、エクスポート処理中に送信ができないということになります。
- デバイス、ポリシー、およびポリシー オブジェクトをエクスポートするには、ポリシーとオブジェクトのタイプに対するポリシー変更とオブジェクト変更の権限、およびデバイス変更の権限が必要です。これらの権限は、認可制御に ACS を使用するときに、個別のポリシー、オブジェクト、およびデバイスに割り当てることができます。システム管理者、ネットワーク管理者、またはセキュリティ管理者の権限を持つと、それに必要な権限が与えられます。

デバイスを CSV にエクスポートする場合は、[デバイスの変更（Modify Devices）] 権限のみが必要です。

関連項目

- セレクタ内の項目のフィルタリング
- Cisco Security Manager でのファイルまたはディレクトリの選択または指定
- [Customize Desktop] ページ

ステップ 1 デバイスビューで、**[ファイル（File）] > [エクスポート（Export）] > [デバイス（Devices）]** を選択して、[インベントリのエクスポート（Export Inventory）] ダイアログボックスを開きます。

ステップ 2 [CSVとしてエクスポート（Export as CSV）] または [デバイス、ポリシー、およびオブジェクトのエクスポート（Export Devices, Policies, and Objects）] を選択します。これらのオプションについては、上記に説明があります。

ステップ 3 エクスポートファイルに含めるデバイスを選択し、[>>] をクリックして [選択済みデバイス（Selected Devices）] リストに追加します。フォルダを選択して、フォルダ内のすべてのデバイスを選択できます。

デバイスを選択するためのリストには、デバイス変更の権限があるデバイスだけが表示されます。

（注） Cisco Security Manager データベースに多数のデバイス、または多数のポリシーやポリシーオブジェクトが含まれている場合は、エラーを防ぐために、一度にエクスポートするデバイスの数を制限する必要があります。詳細については、前述の「**エクスポートサイズの制限**」を参照してください。

ステップ 4 [参照（Browse）] をクリックして、エクスポートファイルの作成先となるフォルダを選択し、エクスポートファイルの名前を入力します。[ファイルタイプ（File Type）] で、作成するファイルタイプを選択します。CSV ファイルの作成時はこの選択が重要ですが、.dev ファイルの作成時には 1 つのオプションを使用できます。

[保存（Save）] をクリックして [インベントリのエクスポート（Export Inventory）] ダイアログボックスに戻ります。[Export Inventory To] フィールドが、エクスポート ファイル情報で更新されます。

ステップ 5 [OK] をクリックして、エクスポートファイルを作成します。

エクスポートの完了時間、およびエクスポートにエラーがあったかどうかを示すメッセージが表示されます。[OK] をクリックすると、エクスポート中に問題が発生した場合は、ダイアログボックスが開き、メッセージが表示されます。ダイアログボックスに [詳細（Details）] ボタンがある場合は、メッセージを選択して [詳細（Details）] をクリックすると、さらに読みやすい形式のメッセージを確認できます。

インベントリのインポートまたはエクスポートでサポートされている CSV 形式

CSV（カンマ区切り値）ファイルにデバイスをエクスポートする場合（**[ファイル（File）] > [エクスポート（Export）] > [デバイス（Devices）]** を選択して [CSVとしてエクスポート（Export as CSV）] を選択）、または CSV ファイルからデバイスをインポートする場合（**[ファイル（File）] > [新規デバイス（New Device）]** を選択して New Device ウィザードの [ファイル（File）] から [デバイスの追加（Add Device）] を選択）には、次のいずれかの CSV ファイル形式を選択できます。

- **Device Credential Repository（DCR）**：CiscoWorks Common Services 用のデバイス管理システム。この形式の詳細については、次の URL で、Common Services のマニュアルのサンプルバージョン 3.0 CSV ファイルの説明を参照してください。
  http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.3/user/guide/dcr.html#wp1193611

- **CS-MARS シードファイル**：Cisco Security Monitoring、Analysis and Response System。この形式の詳細については、次の URL で、CS-MARS のマニュアルを参照してください。http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/device/configuration/guide/chDvcOver.html#wp162016
- **Cisco Security Manager**：Cisco Security Manager 形式。DCR バージョン 3.0 形式に複数のフィールドを追加した形式です。インベントリを別の Security Manager サーバにインポートしている場合は、この形式を選択すると、デバイスでポリシーを検出せずにインベントリをインポートできます。

（注） ファイルにデバイスの os_type および os_version が指定されていない場合は、デバイスを追加するときにデバイスから直接ポリシーを検出する必要があります。

各行の末尾に表示される追加のフィールドは次のとおりです。

- os_type。オペレーティング システム タイプ。PIX、ASA、IOS、FWSM、IPS のいずれかになります。このフィールドは、すべてのデバイス タイプに必須です。
- os_version。ターゲット オペレーティング システム バージョン。[Add New Device] を選択したときに New Device ウィザードのリストに示されるバージョン番号のいずれかになります。許容できるバージョン番号はデバイス モデルによって異なるため、CSV ファイルを手作業で作成している場合は、このリストに慎重に目を通してください。この方法を使用したデバイスの追加の詳細については、手動定義によるデバイスの追加を参照してください。このフィールドは、すべてのデバイス タイプに必須です。
- fw_os_mode。ファイアウォール デバイスが実行されているモード。TRANSPARENT、ROUTER、MIXED のいずれかになります。このフィールドは、ASA、PIX、および FWSM デバイスに必須です。
- fw_os_context。ファイアウォール デバイスが実行されているコンテキスト。SINGLE または MULTI になります。このフィールドは、ASA、PIX、および FWSM デバイスに必須です。
- anc_os_type。Cisco IOS-IPS デバイスの補助的なオペレーティング システム タイプ。存在する場合は IPS となります。このフィールドは、IOS IPS デバイスに必須です。
- anc_os_version。補助的なターゲット オペレーティング システム バージョンで、IPS ターゲット オペレーティング システム バージョンです。存在する場合は、サポートされている IOS-IPS バージョンのいずれかになります。このフィールドは、IOS IPS デバイスに必須です。

これらの CSV ファイルは、そのファイル形式をサポートする任意のプログラムで使用できます。ユーザ自身で CSV ファイルを作成し、そのファイルを使用して Security Manager にインベントリをインポートすることもできます。

関連項目

- Security Manager クライアントからのデバイス インベントリのエクスポート （7 ページ）
- ポリシーまたはデバイスのインポート （17 ページ）
- インベントリ ファイルからのデバイスの追加

コマンドラインからのデバイス インベントリのエクスポート

Security Manager には、Security Manager クライアントを起動せずにデバイス インベントリをエクスポートするのに使用できる Perl スクリプトが用意されています。このスクリプトを使用すると、組織で必要になるさまざまなオフライン レポート タスクを自動化できます。出力を Comma-Separated Value（CSV; カンマ区切り値）ファイルにパイプできます。また、出力をキャプチャして操作することもできます。

ヒント このコマンドでは、デバイスのインポートまたは「ファイルからの」デバイスの追加に使用できるファイルは生成されません。このコマンドは、インベントリ情報をエクスポートするので、統合されたエクスポート機能のように見えますが、コマンドの有効性は、独自のオフラインレポートプロセス要件を備えた組織でのレポートの用途に限定されます。

Perl コマンドは $NMSROOT\bin（通常は C:\Program Files\CSCSpx\bin）にあります。コマンドの構文は次のとおりです。

perl [*path*]**CSMgrDeviceExport.pl -u** *username* [**-p** *password*] [**-s** {**Dhdoirtg**}] [**-h**] [**>** *filename.csv*]

構文

perl [*path*] **CSMgrDeviceExport.pl**	Perl スクリプト コマンド。システム パス変数内に CSMgrDeviceExport.pl ファイルへのパスが定義されていない場合は、そのパスを追加します。
-u *username*	Security Manager のユーザ名。エクスポートされるデータは、このユーザに割り当てられた権限によって制限されます。ユーザには、デバイス表示の権限が必要です。
-p *password*	（オプション）ユーザーのパスワード。コマンドにパスワードを含めていない場合、パスワードの入力を求められます。

-s {Dhdoirtg}	（オプション）出力に含めるために選択されているフィールド。-s オプションを指定しない場合は、すべてのフィールドが含められます。次の 1 つ以上を指定できます。 • D：表示名。 • h：ホスト名。 • d：ドメイン名。 • o：オペレーティング システム（OS）タイプ。 • I：イメージ名。 • r：実行中の OS バージョン。 • t：ターゲット OS バージョン。 • g：デバイス グループ。
-h	（オプション）コマンドラインのヘルプを表示します。このオプションを指定すると、他のすべてのオプションは無視されます。
> *filename.csv*	（オプション）出力を指定のファイルに渡します。ファイルを指定しない場合、出力は画面に表示されます。

出力形式（Output Format）

出力は標準の Comma-Separated Value（CSV; カンマ区切り値）形式であるため、スプレッドシートプログラムで開いたり、独自のスクリプトで処理したりできます。最初の行はカラムの見出しです。カラムは左から右に、上記の -s オプションで説明したフィールドの順に並んでいます。

特定のフィールドに値がない場合、そのフィールドは出力でブランクになります。

デバイス グループ出力フィールドは二重引用符で囲まれ、複数のグループ名が含まれることがあります。グループ名には、グループのパス構造が含まれています。たとえば、次の出力はデバイスが 2 つのグループの一部であることを示します。[Department] フォルダの East Coast グループと、[New] フォルダの NewGroup グループです。グループは、セミコロンで区切られています。

```
"/Department/East Coast; /New/NewGroup"
```

スクリプトが生成したエラー メッセージがあれば、出力ファイルに書き込まれます。

共有ポリシーのエクスポート

他の Security Manager サーバにインポートするために使用する共有ポリシーおよびポリシー オブジェクトをエクスポートできます。この機能は、Cisco Security Manager サーバー間での共有

ポリシーの同期（5ページ）で説明されているように、サーバーのグループ間で同じポリシーを維持するのに役立ちます。

（注） *.pol または *.dev ファイルのインポートは、各ファイルのエクスポート時に使用されたものと同じバージョンの Cisco Security Manager でのみサポートされます。あるバージョンの Cisco Security Manager からエクスポートして、別のバージョンを実行しているサーバーにインポートすることはできません。

ヒント

- Security Manager サーバーまたはローカルの Security Manager クライアントにインポートできます。ローカル Security Manager クライアントにエクスポートまたはインポートする機能は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページを参照してください。
- 共有ポリシーおよびポリシー オブジェクトは、送信されて承認済みのものだけがエクスポート ファイルに含まれます。ポリシーをエクスポートする前に、必要なすべての送信と承認が行われていることを確認します。
- 共有ポリシーによって参照されるすべてのポリシーオブジェクトもエクスポートされます。ただし、ポリシーオブジェクトが参照されていない場合はエクスポートされません。ネットワーク/ホスト、サービス、およびポート リストのオブジェクトを直接エクスポートするために使用できる個別のコマンドがあります。詳細については、ポリシーオブジェクトのインポートおよびエクスポートを参照してください。
- アクティビティ セッションまたは設定セッションの承認中は、ポリシーをエクスポートできません。ポリシーをエクスポートするには、先にすべての承認が完了している必要があります。アプルーバのいる Workflow モードでは、アプルーバに問い合わせ、承認をただちに完了させるように依頼します。Workflow 以外のモードまたはアプルーバのいない Workflow モードでは、変更が送信されると承認が自動的に行われるため、数分待ってからエクスポートを再試行します。
- ポリシーのエクスポート中は、ポリシーの変更を承認できません。エクスポート ファイルが作成されるとすぐにコマンドが終了し、ユーザは再びポリシーの変更を承認できるようになります。このことは、Workflow 以外のモードまたはアプルーバのいない Workflow モードの場合、エクスポート処理中に送信ができないということになります。
- ポリシーとそのポリシーオブジェクトをエクスポートするには、そのポリシーとオブジェクトタイプに対するポリシー変更とオブジェクト変更の権限が必要です。これらの権限は、認可制御に ACS を使用するときに、個別のポリシー、オブジェクト、およびデバイスに割り当てることができます。システム管理者、ネットワーク管理者、またはセキュリティ管理者の権限を持つと、それに必要な権限が与えられます。

（注） バージョン 4.21 以降、Cisco Security Manager は Cisco Identity Services Engine（ISE）を介した TACACS+ 認証のみをサポートします。これは、ACS のサポートが終了しているためです。

関連項目

- Security Manager サーバ クラスタの管理 （3 ページ）
- Security Manager サーバの分割 （3 ページ）
- Cisco Security Manager サーバー間での共有ポリシーの同期 （5 ページ）
- Security Manager クライアントからのデバイス インベントリのエクスポート （7 ページ）
- Cisco Security Manager でのファイルまたはディレクトリの選択または指定
- [Customize Desktop] ページ

ステップ 1 Configuration Manager で、[ファイル（File）] > [エクスポート（Export）] > [ポリシー（Policies）] を選択して、[共有ポリシーのエクスポート（Export Shared Policies）] ダイアログボックスを開きます。

ダイアログボックスが開く前に、Security Manager によって、定義済みの共有ポリシーが評価およびロードされている必要があります。

ステップ 2 次のいずれかの方法を使用して、エクスポートする共有ポリシーを選択します。

ヒント 複数の方法を使用してポリシーを選択できます。たとえば、特定の日付以降に変更されたすべての共有ポリシーを選択したり、特定のタイプの共有ポリシーすべてを選択したりすることが可能で、選択したポリシーを同じファイルにエクスポートできます。

- 特定の日付以降に変更されたすべての共有ポリシーを選択するには、その日付を [変更日（Modified）] フィールドに入力し、[変更日（Modified）] フィールドの横にある [選択>>（Select >>）] をクリックします。日付を *MMM DD YYYY* 形式で入力するか、[カレンダー（Calendar）] をクリックして目的の日付を選択します。
- すべての共有ポリシーを選択するには、[すべて（すべて）] フォルダを選択し、[すべての共有ポリシーを参照（Browse All Shared Policies）] で [選択>>（Select >>）] をクリックします。
- 特定のタイプの共有ポリシーすべてを選択するには、共有ポリシーのタイプを選択し、[すべての共有ポリシーを参照（Browse All Shared Policies）] で [選択>>（Select >>）] をクリックします。フォルダを選択して、選択したリストにフォルダ内のすべてのタイプを移動できます。
- エクスポートする特定の共有ポリシーを指定するには、[すべての共有ポリシーを参照（Browse All Shared Policies）] リストからエクスポートする共有ポリシーのタイプを選択し、エクスポートするタイプの共有ポリシーの横にあるチェックボックスをオンにして、[選択>>（Select >>）] をクリックします。それらを [選択済みのポリシー（Selected Policies）] リストに移動します。特定の共有ポリシー

を選択しない場合、選択したタイプのすべてのポリシーが [選択済みのポリシー（Selected Policies）] リストに追加されます。

（注）　共有ポリシーが定義されているポリシー タイプだけが表示されます。

[選択済みのポリシー（Selected Policies）] リストからポリシーを削除するには、ポリシーを選択して [<<削除（<< Remove）] ボタンをクリックします。[選択済みのポリシー（Selected Policies）] リストのすべてのエントリを削除対象に指定するには、[すべて選択（Select All）] チェックボックスを使用します。

ステップ 3 [共有ポリシーのエクスポート先（Export Shared Policies To）] フィールドの横にある [参照（Browse）] をクリックして、エクスポートファイルを作成するフォルダを選択し、ファイルの名前を入力します。ファイル タイプは、.pol としてあらかじめ選択されているため、変更できません。

[OK] をクリックして、ファイル名と場所を保存します。

ステップ 4 [共有ポリシーのエクスポート（Export Shared Policies）] ダイアログボックスの [OK] をクリックして、エクスポートを開始します。エクスポートが完了すると、エクスポートした共有ポリシーの数が通知され、警告やエラーがある場合は、ダイアログボックスが開いて問題が表示されます。

ポリシーまたはデバイスのインポート （17 ページ）で説明したように、これで、別の Security Manager サーバにポリシーをインポートできます。

ポリシーまたはデバイスのインポート

共有ポリシー（.pol）ファイル、または別の Security Manager サーバからエクスポートされたデバイス インベントリとポリシー（.dev）ファイルをインポートできます。

（注）　*.pol または *.dev ファイルのインポートは、各ファイルのエクスポート時に使用されたものと同じバージョンの Cisco Security Manager でのみサポートされます。あるバージョンの Cisco Security Manager からエクスポートして、別のバージョンを実行しているサーバーにインポートすることはできません。

ヒント

- Security Manager サーバーまたはローカルの Security Manager クライアントからインポートできます。ローカルの Cisco Security Manager クライアントにエクスポートまたはインポートする機能は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページを参照してください。
- デバイスのインポート時、サーバには、インポートしているデバイスの数およびタイプに対応する十分な Security Manager ライセンスが必要です。Professional ライセンスを必要とするデバイス タイプをインポートする前に、そのライセンスをインストールするようにします。ライセンスのインストールの詳細については、Security Manager のライセンス ファイルのインストール （20 ページ）を参照してください。

- ポリシーをインポートするときは、デバイスまたは共有ポリシーのインポート中に、Security Manager 管理の [ポリシー管理（Policy Management）] ページで管理用に選択されたポリシータイプのみが表示されます。ただし、すべてのポリシーがインポートされます。以前管理用に選択を解除したポリシー タイプを選択すると、そのインポートされたポリシーは、インポートされた設定とともに表示されます。選択的なポリシー管理の詳細については、ルータおよびファイアウォールデバイスのポリシー管理のカスタマイズを参照してください。
- 共有ポリシーおよびポリシーオブジェクトのインポート時、サーバ上のポリシーまたはオブジェクトがインポートするものと同じ名前の場合は、インポートされるポリシーまたはオブジェクトによって置換されます。ポリシーまたはオブジェクトにロックがある場合、そのポリシーまたはオブジェクトのインポートは失敗します。メッセージには、失敗の原因がロックの問題であることが示されます。問題を回避するには、インポートを実行する前に、すべてのユーザーが共有ポリシーまたはポリシーオブジェクトへの変更を送信して承認していることを確認してください。
- デバイスをインポートすると、デバイスに割り当てられている共有ポリシーとポリシーオブジェクトもインポートされます。これらのポリシーとオブジェクトは、共有ポリシーのインポート時に使用されたのと同じ条件で、既存のポリシーとオブジェクトを置き換えます。
- ポリシー、およびそのポリシーオブジェクトをインポートするには、そのポリシーとオブジェクトタイプに対するポリシー変更とオブジェクト変更の権限が必要です。デバイスをインポートする場合、デバイスの変更権限も持っている必要があります。これらの権限は、認可制御に ACS を使用するときに、個別のポリシー、オブジェクト、およびデバイスに割り当てることができます。システム管理者、ネットワーク管理者、またはセキュリティ管理者の権限を持つと、それに必要な権限が与えられます。
- ファイルは、同じリリースの Security Manager を実行しているサーバーからエクスポートされた場合にのみインポートできます。
- デバイスがすでにインベントリにある場合には、そのデバイスをインポートできません。したがって、インポート ファイルからデバイス ポリシーを更新できません。デバイスを再インポートする場合は、あらかじめインベントリからそのデバイスを削除します。
- AUS または Configuration Engine サーバを使用して設定の展開を管理するデバイスをインポートする場合、そのサーバがインポート ファイルに含まれているか、または Security Manager サーバですでに定義されている必要があります（いずれか一方）。インベントリにすでに定義されている AUS または Configuration Engine がインポート ファイルに含まれている場合は、重複する表示名のエラーが発生します。AUS または Configuration Engine サーバーが割り当てられているデバイスをインポートしようとすると、「サーバーの選択が無効です」というエラーが発生しますが、サーバーがインポートファイルに含まれていないか、インベントリで定義されていません。
- 管理対象外デバイスをインポートできます。
- IPS デバイスのインポート時、サーバは、インポートされるデバイスと同じシグニチャ レベルである必要があります。たとえば、2 つの IPS デバイスがあり、一方がシグニチャ レベル 481 で、もう一方が 530 で稼働していて、これらのデバイスをインポートする場合、

サーバには 481 と 530 の両方がインストールされている必要があります。IPS デバイスをインポートする前に、IPS 更新の確認とダウンロードに説明されているようにシグニチャパッケージのダウンロードが必要な場合があります。

- この手順では、.pol ファイルまたは .dev ファイルのインポート方法について説明します。CSV ファイルからデバイス インベントリをインポートする場合、手順の説明は インベントリ ファイルからのデバイスの追加にあります。これらの手順は異なります。

関連項目

- Security Manager サーバ クラスタの管理 （3 ページ）
- Security Manager サーバの分割 （3 ページ）
- Cisco Security Manager サーバー間での共有ポリシーの同期 （5 ページ）
- Cisco Security Manager でのファイルまたはディレクトリの選択または指定
- [Customize Desktop] ページ

ステップ 1 Configuration Manager で、[ファイル（File）] > [インポート（Import）] を選択して [インポート（Import）] ダイアログボックスを開きます。

ステップ 2 [参照（Browse）] をクリックしてファイルを選択します。[Select a File] ダイアログボックスの [Files of Type] リストから目的のファイル タイプ（.pol または .dev）を選択するようにします。

ファイルを選択したら、[OK] をクリックします。

ステップ 3 [インポート（Import）] ダイアログボックスで、[OK] をクリックします。

インポートされるポリシーまたはポリシー オブジェクトによる同じ名前のポリシーおよびオブジェクトの置換が警告されます。必要な認可権限（システム管理者または管理変更）がある場合は、[共有ポリシーとインポートしたオブジェクトの警告をすべて表示する（Display a warning on all shared policies and imported objects）] を選択解除するオプションがあります。選択した場合は、共有ポリシーおよびインポートされたオブジェクトのバナーにより、インポート中に共有ポリシーが作成された可能性があること、およびインポート中に特定のオブジェクトが実際に作成されたことがユーザに警告されます。この警告は、ユーザがポリシーまたはオブジェクトを変更する場合に、この変更がそのあとに行われるポリシーのインポートによって上書きされる可能性があるという注意を促します。警告を表示するかどうかを選択し、[はい（Yes）] をクリックします。

ヒント 警告を表示するかどうかをあとで変更する場合は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシー管理（Policy Management）] ページで [共有ポリシーとインポートしたオブジェクトの警告をすべて表示する（Display a warning on all shared policies and imported objects）] オプションを変更できます。

情報がインポートされ、その結果が通知されます。エラーが発生した場合、インポートは行われず、エラーを説明するダイアログボックスが開きます。最も一般的なエラーには、デバイスをインポートするときのデバイスの表示名の重複、インポートされるものと同じ名前を持つ共有ポリシーまたはポリシーオブジェクトのロックなどがあります。

- 表示名の重複問題を解決するには、インベントリからデバイスを削除するか、そのデバイスの名前を変更する必要があります。デバイスを選択してインポートすることはできません。すべてインポートするかインポートしないかのいずれかです。

（注） 重複するデバイス名がすべて表示されるわけではありません。AUS または Configuration Engine を使用して設定の展開を管理している場合、インポートされる AUS 名および設定名は、管理対象デバイス名より先に評価されます。したがって、最初に出るエラーを修正したあとに、新たな重複表示名のエラーが表示されることがあります。

- ロックの問題を解決するには、ユーザがポリシーの変更を送信したら、その変更を承認させるようにする必要があります。デバイスのインポート時、インポートを再試行する前にインポートされたデバイスの削除が必要な場合があります。

ヒント デバイスのインポート時、デバイスがデバイス ビューのデバイス リストに表示されるまで時間がかかる場合があります。また、インポート時にデバイス グループは維持されません。すべてのデバイスが、All グループに配置されます。手動で目的のデバイス グループ構成を再作成し、デバイスを適切なグループに追加する必要があります。

ステップ 4 ポリシーの変更はアクティビティ セッションまたは設定セッションで実行されるため、インポートされるポリシーおよびポリシー オブジェクトは、まだ Security Manager データベースにコミットされていません。変更を送信および承認する必要があります。Workflow モードに基づいて、次のように行います。

- Workflow 以外のモード：[ファイル（File）] > [送信（Submit）] を選択します。
- 承認者のいない Workflow モード：[アクティビティ（Activities）] > [アクティビティの承認（Approve Activity）] を選択します。
- 承認者のいる Workflow モード：[アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）] を選択します。アクティビティは、変更をコミットする前に承認する必要があります。

インポートに問題がある場合は、アクティビティ セッションまたは設定セッションを廃棄できます。ただし、デバイスのインポート時、デバイスがアクティビティ セッションまたは設定セッション以外で追加されます。したがって、アクティビティまたは設定セッションを破棄すると、デバイスポリシーと VPN トポロジが破棄されますが、デバイスはインベントリに残ります。Security Manager インベントリからのデバイスの削除に説明されているように、デバイスを削除する必要もあります。

Security Manager のライセンス ファイルのインストール

ご使用の Security Manager ソフトウェア ライセンスの条件に従って、使用可能な機能や管理できるデバイス数を含めて多くの事柄が決まります。ライセンスの目的で、IP アドレスを使用する物理デバイス、セキュリティ コンテキスト、仮想センサー、または Catalyst セキュリティ サービス モジュールが、デバイスとしてカウントされます。フェールオーバー ペアは 1 つのデバイスとしてカウントされます。PIX ファイアウォール、FWSM、および ASA デバイスが（複数のセキュリティ コンテキストをホストするように）マルチ コンテキスト モードで設定されている場合は、セキュリティ コンテキストだけがデバイスとしてカウントされ、ホスティング デバイスは個別のデバイスとしてカウントされません。

Standard、Professional、および Upgrade の 3 つのライセンス タイプが入手可能です。また、デバイス数が最大 50 に制限される 90 日間の無償評価期間があります。入手可能なライセンスタイプと、サポートされているさまざまなアップグレードパス、および購入可能な Cisco Software Application Support サービス契約の詳細については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html でこのバージョンの Security Manager の製品速報を参照してください。『Installation Guide for Cisco Security Manager』も参照してください。

割り当てられた時間（評価版ライセンスの場合）、またはご使用のライセンスで管理可能なデバイス数を超過すると、ライセンス制限が発生します。評価版ライセンスの権限は、Professional 版ライセンスの権限と同じです。製品を継続して使用できるように、90 日以内にできるだけ早く必要なデバイス数に対して Security Manager を登録することが重要です。アプリケーションを起動するたびに、評価版ライセンスの残りの日数が通知され、評価期間中にアップグレードするように求められます。評価期間終了後は、ライセンスをアップグレードしないとログインできなくなります。

非評価ライセンスについては、ご使用の設定ライセンスで許可された数よりも多くのデバイスがデータベースに含まれる場合、Security Manager クライアントを使用してアプリケーションにログインできません。ログイン中にライセンスを追加するように求められ、適切なライセンスを追加するまでログインを完了できません。

ヒント セキュリティコンテキストを検出したアクティビティを送信していないで、それらが現在デバイスセレクタに表示されていなくても、デバイスの数には検出されたすべてのセキュリティコンテキストと仮想センサーが含まれます。インベントリ内のデバイス数がライセンスで許可されるデバイス数よりも少ないのに、デバイス カウント エラー メッセージが表示される場合は、検出されたデバイスの数を決定するためにすべてのアクティビティを送信してください。管理対象でないデバイスは削除してください。

はじめる前に

- 基本ライセンスまたはアップグレードライセンスと、その他の必要なライセンスを取得します。Cisco.com ユーザ ID が必要です。また、Cisco.com でソフトウェアのコピーを登録する必要があります。登録時に、出荷ソフトウェア パッケージ内の Software License Claim Certificate に対応付けられている Product Authorization Key（PAK; 製品認証キー）を指定する必要があります。
  - Cisco.com ユーザとして登録済みの場合は、http://www.cisco.com/go/license にアクセスしてください。
  - Cisco.com ユーザとして登録されていない場合は、http://tools.cisco.com/RPF/register/register.do にアクセスしてください。

登録後に、基本ソフトウェアライセンスが、登録時に指定した電子メールアドレスに送られます。Security Manager の PAK とライセンスを受信するのに加えて、購入したデバイス カウント パックごとに PAK が 1 つ追加されます。

これらのライセンス ファイルを、Security Manager サーバまたはローカル Security Manager クライアント上のフォルダにコピーします。Security Manager サーバにライセンス ファイルをコピーする場合、ライセンス ファイルは、Security Manager サーバのローカル ディスクに格納する必要があります。サーバに対応付けらたドライブを使用することはできません。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。

（注） ローカルの Security Manager クライアントにあるライセンスファイルをインストールするには、クライアント側のファイル参照を有効にする必要があります（[Customize Desktop] ページ を参照）。

ヒント ライセンスファイルを、Security Manager サーバー上にある製品のインストールフォルダ内の etc/licenses/CSM フォルダに格納しないでください。このフォルダに格納した場合、ライセンスを追加しようとするとエラーが発生します。ファイルは、製品フォルダ以外のフォルダに格納してください。

- Common Services にライセンス ファイルは必要ありません。
- Auto Update Server にライセンス ファイルは必要ありません。

ステップ 1 [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 2 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。このタブの各フィールドの説明については、[CSM] タブ、[Licensing] ページを参照してください。

ステップ 3 [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。

[Install a License] ダイアログボックスには、ライセンスを取得するための Cisco.com へのリンクが含まれています（まだライセンスを取得していない場合）。[参照（Browse）] をクリックしてライセンスファイルを選択し、[ライセンスのインストール（Install a License）] ダイアログボックスで [OK] をクリックしてライセンスをインストールします。

すべてのライセンスのインストールが完了するまで、このプロセスを繰り返します。

証明書信頼管理

Cisco Security Manager は、HTTPS 経由で Cisco.com から ASA イメージと IPS パッケージをダウンロードします。信頼を確立するために証明書を使用します。バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、両方のタイプのダウンロードで Cisco.com 証明書の処理を改善するのに役立ちます。

- ASA イメージのダウンロード。ASA イメージダウンロードの証明書信頼管理に関する詳細なドキュメントについては、[Image Manager] ページを参照するか、または**[ツール（Tools）] > [Security Manager管理...（Security Manager Administration...）] > [Image Manager] > [ヘルプ（Help）]** に移動します。
- IPS パッケージのダウンロード。IPS パッケージダウンロードの証明書信頼管理に関する詳細なドキュメントについては、[Edit Update Server Settings] ダイアログボックスを参照するか、または**[ツール（Tools）] > [Security Manager管理...（Security Manager Administration...）] > [IPS アップデート（IPS Updates）] > [サーバーグループの更新（Update Server group）] > [設定の編集（Edit Settings）] > [ヘルプ（Help）]** に移動します。

証明書信頼管理機能

Security Manager の証明書信頼管理機能には、次の特性があります。

- ブラウザのように動作します。ユーザが意識的に信頼しているものに信頼を与えます。
- これにより、証明書を表示し、自分の裁量でそれを受け入れることができます。
- 証明書を積極的に検証して、受け入れるか拒否するかを判断するのに役立ちます。たとえば、証明書が自己署名されている（信頼できる認証局によって発行されていない）かどうかを確認したり、期限が切れているか、まだ有効でないか、取り消されているかを確認します。
- 証明書を受け入れると、その証明書が Security Manager サーバーに保存されます。
- 透明性と制御を提供します。証明書の取得と追加、証明書の表示、および保存されている証明書の削除ができます。
- Cisco.com との通信中に、ライブサーバー証明書と保存されている証明書を比較し、完全に一致した場合にのみ続行します。ルート証明書だけでなく、完全な証明書チェーンが一致するかどうかを比較します。不一致がある場合、新しい証明書を表示して受け入れるまで、現在の操作は中止されます。
- 証明書の失効と有効性について Security Manager サーバーを毎日チェックし、サーバーから失効した証明書または無効な証明書を削除します。これは、証明書にある CRL 配布ポイント/URL とのライブコンタクトによって行います。デフォルトの固定スケジュールでは、この毎日のチェックは午前 2 時に実行されます。

ダウンロード要件

Cisco.com からイメージをダウンロードするには、最新のイメージメタデータロケータ証明書とダウンロードサイトの最新の証明書 URL の両方を取得、表示、および受け入れる必要があります。Security Managerインターフェイスには、主要拠点のユーザを支援するためのメッセージがあり、詳細なドキュメントは[Image Manager] ページおよび[Edit Update Server Settings] ダイアログボックスを参照することで入手できます。

トラブルシューティング

証明書の失効と有効性を毎日チェックしている間、CRL 失効リストは Security Manager サーバーに保存されません。そのため、接続が失われた場合、毎日のチェックでは証明書の失効の可能性を検出できません。この問題は、接続が復元された後に解決されます。

ASAイメージのダウンロード中またはIPSアップデートパッケージの確認中にエラーが発生した場合、最もあり得る原因は次のとおりです。

- サイトの証明書が Security Manager サーバーで見つからない
- サイトから受け取った証明書と保存されている証明書が一致しない
- サイトの証明書の有効期限が切れている

上記の 3 つの場合すべてで、操作は中止され、エラーの原因と失敗したサイトの URL を示すメッセージが表示されます。回復するには、証明書機能のユーザインターフェイス ([ツール（Tools）] > [Security Manager管理...（ Security Manager Administration...）] > [Image Managerまたはツール（Image Manager or Tools）] > [Security Manager管理...（Security Manager Administration...）] > [IPSアップデート（IPS Updates）] > [サーバーグループの更新（Update Server group）] > [設定の編集（Edit Settings）] に移動し、次にサイトから新しい証明書を取得、表示、および受け入れて、ダウンロードを再試行します。

IPS アップデートのチェック中にエラーが発生した場合は、IPS パッケージのメタデータ情報の取得に使用された Cisco.com サイトの証明書と、IPS パッケージの実際のダウンロードサイトの証明書の両方を受け入れていることを確認してください。ジョブの実行ステータスを通知する電子メールを常に設定することをお勧めします。それにより、エラーから回復するための推奨されるアクションを電子メールで表示できます。電子メールメッセージから失敗したダウンロード URL をコピーして、証明書を取得します。

証明書が保存されるため、以前のバージョンから Security Manager 4.4 にアップグレードすると、Cisco.com とのすべての通信が失敗します。この問題を解決するには、イメージメタデータロケータとダウンロードサイトの URL から証明書を取得する必要があります。

ユーザーインターフェイスに保存されている証明書テーブルに特定の証明書の追加が表示されない場合は、証明書の失効と有効性の毎日のチェックで、失効または有効期限切れにより証明書が削除されていないかどうかを確認します。これを行うには、tomcat ログで証明書失効チェックタスクを探します。このログにより、保存されていた証明書が削除された正確な理由を確認できます。

監査レポートの使用

Security Manager で状態が変更されると、監査ログ内に監査エントリが作成されます。このエントリを表示するには、[管理（Manage）] > [監査レポート（Audit Report）] を選択します。ここでは、監査レポートについて詳しく説明します。

- 監査レポートについて （25 ページ）
- 監査レポートの生成 （25 ページ）

• 監査ログ エントリのパージ （29 ページ）

監査レポートについて

Security Manager で状態が変更されると、監査ログ内に監査エントリが作成されます。このエントリを表示するには、[管理（Manage）] > [監査レポート（Audit Report）] を選択します。

次の状態変更が行われると、イベントが生成され、監査エントリが作成されます。

- 実行時環境に対する変更：
  - システム変更（ログイン試行（成功または失敗）、ログアウト、計画的なバックアップなど）
  - 認可の問題（試行の失敗やセキュリティ違反など）
  - マップの変更（バックグラウンド マップ ビューの保存、削除、変更など）
  - 管理上の変更（ワークフロー モードの変更など）
- Security Manager オブジェクトの状態の変更：
  - アクティビティの変更（アクティビティの作成、編集、送信、承認など）
  - 展開の変更（展開ジョブの作成、編集、送信など）
- 管理対象デバイスの状態の変更：
  - オブジェクトの変更（ポリシー オブジェクトの変更など）
  - インベントリの変更（インベントリ内のデバイスの追加、削除、変更など）
  - ポリシーの変更（ポリシーの作成、復元、変更、削除など）
  - VPN の作成、修正、または削除などの VPN の変更

監査レポートを表示するとき、目的のレコードだけが選択されるように検索基準を指定することにより、エントリのサブセットを表示できます。

関連項目

- 監査レポートについて （25 ページ）
- 監査ログ エントリのパージ （29 ページ）

監査レポートの生成

監査ログを確認して、Security Manager システムで発生したイベントを分析できます。この情報は、ユーザーがデバイスに加えた変更を追跡したり、重要な他のシステムイベントを識別し

たりするのに役立ちます。[Audit Report] ウィンドウに、興味のある特定の監査ログ エントリを表示するために役立つ拡張的な検索基準が表示されます。

ヒント CiscoWorks Common Services を使用して監査ログを表示することもできます。[Common Servicesサーバー管理（Common Services Server Administration）] ページから [サーバー（Server）]>[レポート（Reports）] を選択し、コンテンツテーブルから [監査ログ（Audit Log）] を選択します。[レポートの生成（Generate Report）] をクリックすると、1 日ごとに 1 つのログリストが表示されます。目的のログのリンクをクリックすると、そのログが開きます。これらのログは、Program Files/CSCOpx/MDC/Logs/audit/ ディレクトリに格納されています。Common Services へのログインの詳細については、Cisco Security Management Suite サーバへのログインを参照してください。

関連項目

- 監査レポートについて （25 ページ）

ステップ 1 [管理（Manage）] > [監査レポート（Audit Report）] を選択して、[監査レポート（Audit Report）] ウィンドウを開きます。

ステップ 2 レポートを重要な領域に関連した特定のレコードセットに限定するには、該当する検索条件を左側ペインに入力して、[検索（Search）] をクリックします。検索フィールドの詳細については、[Audit Report] ウィンドウの使用 （26 ページ）を参照してください。

次に、検索基準の例について説明します。

- デバイス router1 が Security Manager 管理から削除された日時を調べるには、[アクションで検索（Search by action）] セレクタから [デバイス（Devices）] > [削除（Delete）] を選択します。[オブジェクトの名前の全体または一部で検索（Search by all or part of the object name）] フィールドに、デバイスの表示名（router1）を入力します。
- システムでログイン試行失敗が発生したかどうかを調べるには、[アクションで検索（Search by action）] セレクタから [システム（System）] > [許可（Authorization）] > [ログイン（Login）] > [失敗（Failed）] を選択します。

ステップ 3 レポート内のエントリの内容を表示するには、そのエントリをダブルクリックします。この処理によりダイアログボックスが開き、エントリに関連するメッセージが表示されます。このダイアログボックス内で、上矢印ボタンと下矢印ボタンを使用して、レポート全体をスクロールできます。

[Audit Report] ウィンドウの使用

[Audit Report] ウィンドウを使用して、Security Manager の状態変更のレコードを表示します。

[Audit Report] ページには、2 つのペインが含まれます。左側のペインを使用して、監査レポートを生成するためのパラメータを定義します。右側のペインには、監査エントリまたはメッ

セージごとに1行ずつ使用して監査レポートが表示されます。監査レポートの内容は、左側のペインで定義したパラメータによって異なります。このため、表に示されたすべてのカラムが生成済みの監査レポートに表示されるとはかぎりません。

ナビゲーション パス

[管理（Manage）] > [監査レポート（Audit Report）] を選択します。

関連項目

- 監査レポートについて （25 ページ）
- 監査レポートの生成 （25 ページ）

フィールド リファレンス

表 1 : [Audit Report] ウィンドウ

要素	説明
検索基準（左側のペイン） [Audit Report] ウィンドウの左側には、レポートの検索基準が表示されます。デフォルトのレポートには、昨日から今日にかけてのすべての状態変更が、新しい順に上から表示されます。	
Search by action	監査レポートに含める 1 つ以上の処理ソース。何も選択しない場合、レポートは処理に基づいてフィルタリングされません。すべての処理ソースを含める場合は、[All] を選択できます。
Search by date	レポートに含める期間。開始日から終了日までに発生した処理が表示されます。カレンダーアイコンをクリックして、日付を選択します。 このフィルタのデフォルト（リセット位置）では、昨日から今日までのアクションが含められます。
Search for activity by state	このフィールドは他の検索フィールドとは異なり、主にWorkflowモードで使用されます。このフィールドを使用して、レポートに含める 1 つ以上のアクティビティを選択できます。アクティビティは、ドロップダウンリストの下の表示ボックスに示されます。ドロップダウンリストを使用すると、レポートするアクティビティを簡単に見つけることができます。 この検索メカニズムを使用するには、レポートするアクティビティのアクティビティ状態を選択してから、アクティビティを選択します。複数のアクティビティを選択するには、Ctrl を押しながらそれらのアクティビティをクリックします。 アクティビティに基づいてフィルタリングしない場合は、[No Activity] を選択します。

要素	説明
Search by message warning level	メッセージ警告レベル。レポートには、選択した重大度のメッセージだけが表示されます。複数のレベルを選択するには、Ctrl を押しながらそれらのレベルをクリックします。
Search by user name	レポートに含める処理実行者のユーザ名。Security Manager システムにより生成された処理を表示するには、ユーザ名 System を入力します。
Search by a phrase in the message body	監査レポートエントリのメッセージ内に表示するテキスト文字列。最大 1025 文字を入力できます。 メッセージはレポート表には表示されません。エントリに関連するメッセージを表示するには、そのエントリをダブルクリックします。
Search by all or part of the object name	監査エントリが生成されたオブジェクトの名前に表示するテキスト文字列。最大 1025 文字を入力できます。
[Search] ボタン	このボタンをクリックすると、右側のペイン内にレポートが生成されます。
リセット ボタン	このボタンをクリックすると、検索条件がリセットされ、選択した値または項目がすべて削除されます。
監査レポート（右側のペイン） [Audit Report] ウィンドウの右側には、監査レポートが含まれます。それぞれの行が 1 つの監査エントリを表しています。行をダブルクリックすると、[Audit Message Details] ダイアログボックスが開きます。このダイアログボックスでは、より読みやすいレイアウトで情報が表示され、エントリに関連付けられた特定のメッセージが表示されます。[Audit Message Details] ダイアログボックス内から、レポートのエントリ全体をスクロールできます。	
Message Level	メッセージ警告レベル：[Information]、[Warning]、[Success]、[Failure]、および [Internal System Error]。
日付	処理が行われた日時。
ソース	監査エントリの送信元：[Objects]、[License]、[Admin]、[Firewall]、[Policy Manager]、[Devices]、[Topology]、[VPN]、[Config Archive]、[Deployment]、[System]、および [Activity]。
操作	実行された処理：[Add]、[Assign]、[Create]、[Delete]、[Open]、[Purge]、[Unassign]、および [Update]。

要素	説明
オブジェクト	処理のオブジェクトのID。たとえば、カテゴリがデバイスの場合、オブジェクト ID はデバイス名または IP アドレスとなります。カテゴリが展開の場合、オブジェクトIDはジョブ名やジョブ ID などになります。特定のオブジェクト名がないこともよくあります。
ユーザー名	処理実行者のユーザ名。
アクティビティ	処理が行われたアクティビティの名前（ある場合）。
# of rows per page	各ページに表示する行数。
[<] 矢印	このボタンをクリックすると、監査レポートの直前のページに戻ります。
[>] 矢印	このボタンをクリックすると、監査レポートの次のページに進みます。

監査ログ エントリのページ

Security Manager は、ログ エントリの経過時間に基づいて、自動的に監査ログを削除します。ログのサイズを自分で管理する必要はありません。ただし、デフォルトを変更して、ログの最大サイズを拡大または縮小することにより、データベースの全体的なサイズを管理することはできます。

監査ログのデフォルト設定を変更するには、[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 [ログ（Logs）] を選択します（[Logs] ページを参照）。ログのサイズは、エントリの最大経過日数と、ログ内の全体的な最大エントリ数によって制御されます。これらの設定は同時に機能し、ログが常に最大エントリ数を超えないように、また最大日数を経過したエントリが含まれないように、エントリは定期的に削除されます。ログの最大サイズを縮小する場合は、[今すぐ消去（Purge Now）] をクリックして、通常の削除サイクルよりも前に超過エントリを削除します。

（注） [Purge Now] ボタンは、データベースから監査レポートを削除するだけです。<install_dir>\CSCOpx\MDC\log\audit フォルダの *.csv ファイルは削除されません。これらの *.csv ファイルは、直接削除できます。

また、ログ内に取り込まれるイベントの重大度レベルを変更することによっても、ログのサイズを制御できます。たとえば、重大なイベントだけを取り込むようにすれば、ログのサイズが小さく保たれます。ただし、情報のレベルを縮小すると、ログの価値も低下する可能性があります。

関連項目

- 監査レポートについて （25 ページ）
- 監査レポートの生成 （25 ページ）
- [Audit Report] ウィンドウの使用 （26 ページ）

別のユーザの作業の引き継ぎ

管理権限を持つユーザは、Workflow 以外のモードで別のユーザの作業を引き継ぐことができます。あるユーザがデバイスおよびポリシーに対する操作を実行していて、デバイスおよびポリシーがロックされ、別のユーザが同じデバイスおよびポリシーへのアクセスを必要としている場合、別のユーザの作業を引き継ぐと便利です。

ステップ 1 [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ユーザセッションの引き継ぎ（Take Over User Session）] を選択して、[ユーザセッションの引き継ぎ（Take Over User Session）] ページを開きます（[Take Over User Session] ページを参照）。

ステップ 2 引き継ぐユーザ セッションを選択します。

ステップ 3 [セッションの引き継ぎ（Take over session）] をクリックします。選択されたユーザが行った変更が転送されます。まだコミットされていない変更はすべて廃棄されます。

選択されたユーザが変更の引き継ぎ時にログインしている場合、ユーザに警告メッセージが表示され、進行中の変更が失われて、ユーザがログアウトされます。

管理ユーザまたは他のユーザのパスワード変更

管理ユーザは、すべての Security Manager 機能にアクセスできる事前定義ユーザです。製品をインストールするときに、管理ユーザのパスワードを設定します。パスワードを忘れた場合は、次の手順を使用してパスワードを変更します。この手順は、他のユーザアカウントのパスワードをリセットする場合にも使用できます。

ステップ 1 Security Manager サーバ上の Windows にログインし、Windows コマンドライン ウィンドウを開きます。

ステップ 2 次のコマンドを使用して、デーモン マネージャ サービスを停止します。

net stop crmdmgtd

ヒント デーモン マネージャの停止と起動は、[Services] コントロール パネルを使用して行うこともできます。

ステップ 3 ユーザー名として admin を指定して、ResetPasswd.pl を実行します。この例では、製品が次のデフォルトディレクトリにインストールされていることを想定しています。別のディレクトリを使用した場合は、ディレクトリ パスを変更してください。

C:\Program Files\CSCOpx\bin\perl ResetPasswd.pl admin

新しいパスワードを入力するように求められます。

ヒント　別のユーザーのパスワードを変更する場合は、**admin** をそのユーザー名に置き換えてください。

ステップ 4 次のコマンドを使用して、デーモン マネージャ サービスを開始します。

net start crmdmgtd

Security Manager データベースのバックアップおよび復元

作業の復元が必要な場合に備えて、Security Manager データベースを定期的にバックアップする必要があります。

ヒント　Security Manager データベース バックアップには、Event Manager サービスで使用されるイベント データ ストアは含まれません。イベント管理データをバックアップする場合は、イベント データ ストアのアーカイブまたはバックアップと復元を参照してください。

ここでは、Security Manager データベースのバックアップおよび復元の方法について説明します。

- サーバ データベースのバックアップ （31 ページ）
- サーバ データベースの復元 （34 ページ）

サーバ データベースのバックアップ

Security Manager では、CiscoWorks Common Services 機能を使用してデータベースのバックアップおよび復元を行います。Security Manager クライアントで、[ツール（Tools）] > [バックアップ（Backup）] を選択して、バックアップスケジュールを作成するための [CiscoWorks Common Services のバックアップ（CiscoWorks Common Services Backup）] ページを開きます。必要な場合にデータベースを復元できるように、定期的にデータベースをバックアップしておく必要があります。

バックアップが完了すると、Security Manager によりバックアップが圧縮されます。[CiscoWorks Common Services backup] ページで電子メール アドレスを設定した場合、バックアップおよび圧縮のプロセスが完了したことを示す通知を受け取ります。ファイル圧縮で問題が発生する場合、またはバックアップを圧縮しない場合は、バックアップ圧縮をオフに切り替えることができます。%NMSROOT%\conf フォルダ（通常は C:\Program Files\CSCOpx\conf）の backup.properties ファイルを編集し、バックアップ圧縮プロパティを VMS_FILEBACKUP_COMPRESS=NO のように変更します（YES の代わりに NO を指定します）。

ヒント バックアップには、設定データベースおよびレポート データベースが含まれますが、イベント保管領域は含まれません。backup.properties ファイル内の SKIP_RPT_DB_BACKUP プロパティ値を YES に変更することで、レポート データベースを除外できます。YES を指定した場合でも、バックアップには、レポート スケジュールで生成されるレポートが含まれます。イベント データ ストアのバックアップについては、イベント データ ストアのアーカイブまたはバックアップと復元を参照してください。

データのバックアップおよび復元中、Common Services と Security Manager の両方のプロセスがシャットダウンされてから再起動されます。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。

古いバックアップを復元する前に、現在のシステムのバックアップを作成することを強く推奨します。

旧バージョンの Security Manager のバックアップに保留中のデータが含まれている場合、そのデータはまだデータベースにコミットされていないデータであるため、そのバージョンからバックアップを復元することはできません。新しいバージョンの Cisco Security Manager にアップグレードする前に、コミットされていない変更をコミットまたは廃棄してから、データベースのバックアップを作成することを推奨します。次の手順を使用すると、保留中のデータをコミットまたは廃棄する場合に便利です。

- **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。

保留中のデータを持つユーザが複数存在する場合、それらのユーザの変更もコミットまたは廃棄する必要があります。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、[管理（Manage）]>[アクティビティ（Activities）] 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廃棄するには、[管理（Manage）] > [アクティビティ（Activities）] 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、[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。

また、Windows コマンド プロンプトから次のコマンドを使用してデータベースをバックアップすることもできます。

[*path*]**perl** [*path*]**backup.pl** *backup_directory* [*log_filename* [**email=***email_address* [*number_of_generations* [**compress**]]]]

構文

[*path*]**perl** [*path*]**backup.pl**	Perl スクリプト コマンド。システム パス変数内に perl コマンドおよび backup.pl ファイルへのパスが定義されていない場合は、そのパスを追加します。両方とも、通常のパスは C:\Progra~1\CSCOpx\bin\ です。
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。
log_filename	（オプション）バックアップ中に生成されたメッセージのログファイル。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。 名前を指定しない場合、ログは %NMSROOT%\log\dbbackup.log となります。
email=*email_address*	（オプション）通知が送信され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、後続のパラメータを指定する必要がある場合、等号またはアドレスを指定せずに **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。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定を参照してください。
number_of_generations	（オプション）バックアップディレクトリに保存するバックアップ世代の最大数。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	（オプション）バックアップファイルを圧縮するかどうかを指定します。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。

例

次のコマンドでは、現在のディレクトリに perl コマンドと backup.pl コマンドが含まれていることを想定しています。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。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 パラメータのあとに何らかのパラメータを指定した場合、その前にあ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
```

ヒント　進行中のバックアップを中止する場合は、他のバックアップを実行する前に、Security Manager のインストール ディレクトリ（通常は C:\Progra~1\CSCOpx）にある backup.LOCK ファイルを削除する必要があります。

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。アップグレードがサポートされているバージョンの詳細については、この製品リリースの『Installation Guide for Cisco Security Manager』を参照してください。

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　次のように入力して、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**]

引数の説明

- *$NMSROOT* —The full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx)
- **-t** *temporary_directory*：（任意）復元プログラムで一時ファイルを保存するために使用されるディレクトリまたはフォルダ。デフォルトでは、このディレクトリは *$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。世代 1 ～ 5 が存在する場合、5 が最新の世代となります。
- **-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。

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。

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

ヒント　RME データが含まれるデータベースを復元する場合は、インベントリ データを収集するかどうか尋ねられることがあります。このデータの収集には時間がかかることがあります。No で応答して、インベントリをスケジュールするように RME を設定できます。RME で、[デバイス（Devices）] > [インベントリ（Inventory）] を選択します。

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。

Cisco Technical Assistance Center 用データの生成

Cisco Technical Assistance Center（TAC）の担当者は、アプリケーションの使用中に発生する問題の識別や解決に役立てるため、さまざまなデータを送信するようにユーザに依頼することがあります。次の項を参考に必要な情報を生成できます。ただし、これらのタスクを実行するのは、TAC の指示がある場合だけにしてください。問題の解決にその情報が必ずしも必要であるとは限らないためです。

- Cisco Technical Assistance Center 用の診断ファイルの作成　（35 ページ）
- 展開ステータス レポートまたは検出ステータス レポートの生成　（38 ページ）
- Cisco Technical Assistance Center 用の差分データベース バックアップの生成　（39 ページ）

Cisco Technical Assistance Center 用の診断ファイルの作成

問題レポートの提出時に、Cisco Technical Assistance Center（TAC）の担当者により、診断ファイルの形式でシステム設定情報の提出を求められることがあります。診断ファイルは、TAC による問題の診断に役立ちます。診断ファイルの提出は、担当者から求められた場合だけでかまいません。

診断ファイルを作成する前に、レポートに記載の問題の原因となったアクションを実行してください。必要に応じて、[デバッグオプション（Debug Options）] ページ（[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デバッグオプション（Debug Options）]）で設定を変更することにより、診断ファイルの詳細レベルを調整できます。[Debug Options] ページを参照してください。

バージョン 4.7 以降、Cisco Security Manager は、新しい軽量のバリアントで診断をサポートします。このバリアント「Light Diagnostics」は基本的な情報のみを収集します。その結果、診断ファイルのサイズが小さくなり、その生成が速くなります。既存のバリアント「General Diagnostics」は、4.7 でも 4.6 以前のバージョンの場合と同じものです。

General Diagnostics ファイル

General Diagnostics ファイル（CSMDiagnostics.zip）には、次のファイルと情報が含まれています。

- コンフィギュレーション ファイル
- Apache 構成ファイルおよびログファイル
- Tomcat 構成ファイルおよびログファイル
- インストール、監査および操作のログファイル
- CiscoWorks Common Services レジストリサブツリー（[HKEY_LOCAL_MACHINE][SOFTWARE][Cisco][MDC]）
- Windows のシステム イベント ログ ファイルおよびアプリケーション イベント ログ ファイル
- ホスト環境情報（オペレーティングシステムのバージョンとインストール済みサービス パック、RAM の大きさ、すべてのボリュームのディスク容量、コンピュータ名、および仮想メモリサイズ）

GUI を使用して CSMDiagnostics.zip を作成するには、次の手順に従います。

1. Security Manager クライアントを使用して、**[ツール（Tools）] > [Security Manager Diagnostics...] > [General Diagnostics...]** を選択します。ダイアログボックスが開きます。
2. [OK] をクリックして、ファイル生成を開始します。ダイアログボックスに経過が表示されます。
3. ファイルが生成されたら、[閉じる（Close）] をクリックします。

CLI を使用して CSMDiagnostics.zip を作成するには、次の手順に従います。

1. Security Manager サーバーでコマンドラインウィンドウを開きます。
2. **~MDC\bin\CSMDiagnostics** プログラムを実行します。
3. CSMDiagnostics.zip ファイルは <*installation_location*>/MDC/etc フォルダに格納されます。<*installation_location*> は、CiscoWorks Common Services をインストールしたドライブおよ

びディレクトリです。<*installation_location*> のデフォルト値は C:\Program Files (x86)\CSCOpx です。

4. 必要に応じて、CSMDiagnostics.zip を格納する別のフォルダを指定することもできます。たとえば、**CSMDiagnostics D:\temp** のように指定できます。

5. CSMDiagnostics.zip は、作成後に移動するか名前を変更する必要があります。このファイルは 2 回目の生成時に上書きされ、1 つ前のバージョン（「_old」が追加されます）のみが保存されるためです。

（注） CLI を使用して CSMDiagnostics.zip を作成する場合は、コマンドが完了してからウィンドウを閉じる必要があります。そうしないと、その後 **CSMDiagnostics** を実行しても正常に動作しません。誤ってウィンドウを閉じた場合は、C:\Program Files\CSCOpx\MDC\etc\mdcsupporttemp フォルダを削除してから、コマンドを再試行してください。

Light Diagnostics ファイル

Light Diagnostics ファイル（CSMDiagnostics_light.zip）には、General Diagnostics ファイル（CSMDiagnostics.zip）のサブセットが含まれているため、サイズが小さく、速く生成されます。

GUI を使用して CSMDiagnostics_light.zip を作成するには、次の手順に従います。

1. Security Manager クライアントを使用して、**[ツール（Tools）] > [Security Manager Diagnostics...] > [Light Diagnostics...]** を選択します。ダイアログボックスが開きます。

2. [OK] をクリックして、ファイル生成を開始します。ダイアログボックスに経過が表示されます。

3. ファイルが生成されたら、[閉じる（Close）] をクリックします。

CLI を使用して CSMDiagnostics_light.zip を作成するには、次の手順に従います。

1. Security Manager サーバーでコマンドラインウィンドウを開きます。

2. <*installation_location*>\MDC\diagnostics\script>rundiag.bat コマンドを実行します。<*installation_location*> は、CiscoWorks Common Services をインストールしたドライブおよびディレクトリです。<*installation_location*> のデフォルト値は C:\Program Files (x86)\CSCOpx です。

3. 次の 3 つのパラメータを含むコマンドを、示されている順序で実行してください。

3.1. Installation Folder：Security Manager がインストールされているフォルダ。これを変更または修正することはできません。パスにエラーがあると、診断ファイルの生成に失敗します。例: C:\PROGRA~2\CSCOpx\MDC

3.2. Destination Folder：生成後に診断ファイルが格納されるフォルダ。ファイルを保存する任意のパスとフォルダを指定できます。ファイルをデフォルトのパスに保存する場合は、デフォルトのパスを明示的に指定する必要があります。パスを指定しないと、生成時にエラーが発生します。例: C:\PROGRA~2\Light_Diagnostics

3.3. スペースのない文字列「LightDiagnostics」。この文字列ではアルファベットの大文字と小文字が区別されません。大文字または小文字を使用できますが、スペースは使用しないでください。この文字列を指定しなかった場合、General Diagnostics（つまり、Light Diagnostics ではない）ログの一部が宛先フォルダに自動的に収集されます。

1. 完全なコマンド画面の例:

C:\Program Files (x86)\CSCOpx\MDC\diagnostics\script>rundiag.bat C:\PROGRA~2\CSCOpx\MDC C:\PROGRA~2\Light_Diagnostics LightDiagnostics

展開ステータス レポートまたは検出ステータス レポートの生成

展開ジョブおよびポリシー検出ジョブについて、ステータス レポートを生成できます。展開または検出に伴う問題が発生した場合は、これらのレポートは、Cisco Technical Support（TAC）の担当者による問題の解決に役立ちます。主にレポートはトラブルシューティングのためのものですが、個人で使用するためのレポートを生成することもできます。

ステータス レポートは、ご使用のワークステーション上に Adobe Acrobat（PDF）ファイルとして生成されます（PDF ファイルを保存する場所を選択するように指示されます）。レポートには、ジョブの概要、およびそのジョブのデバイス別の概要が含まれます。展開ステータス レポートには、完全な設定とデルタ設定、および Security Manager とデバイス間通信のトランスクリプトも含まれます。

次の方法で展開レポートまたは検出レポートを生成できます。

- **展開ステータス レポート**
  - 展開ジョブが成功または失敗して完了した場合は、[展開ステータス（Deployment Status）] ダイアログボックスにある [レポートの生成（Generate Report）] ボタンをクリックします。[Deployment Status Details] ダイアログボックスを参照してください。
  - 以前完了したジョブの場合は、Deployment Manager でジョブを選択して、[レポートの生成（Generate Report）] ボタンをクリックします。[Deployment Manager] ウィンドウを参照してください。
- **検出ステータス レポート**
  - 検出ジョブ（デバイスの追加時、またはインベントリにすでに存在するデバイスのポリシーを再検出する際に発生するジョブ）の実行中に、[検出ステータス（Discovery Status）] ダイアログボックスにある [レポートの生成（Generate Report）] ボタンをクリックします。[Discovery Status] ダイアログボックスを参照してください。
  - 以前完了したジョブの場合は、[ポリシー検出ステータス（Policy Discovery Status）] ダイアログボックスでジョブを選択して、[レポートの生成（Generate Report）] ボタンをクリックします。[Policy Discovery Status] ページ を参照してください。

Cisco Technical Assistance Center 用の差分データベース バックアップの生成

注意 この項では、差分データベース バックアップの作成方法について説明します。差分バックアップは不完全なものであり、これをフル バックアップの代わりとしては使用できません。差分バックアップは、トラブルシューティングでの使用に限定されます。Cisco Technical Assistance（TAC）の担当者が指示した場合にかぎり、生成するようにしてください。

差分データベースバックアップには、定期バックアップと同じ特徴がありますが、それよりも限定されたデータ セットです。差分バックアップを作成する場合は、Configuration Archive のデータを含めるかどうか確認され、含める場合は、（デバイス単位に）アーカイブのバージョンをいくつ分含めるか確認されます（定期バックアップには Configuration Archive 全体が含まれます）。定期バックアップの説明については、サーバ 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。

ヒント 差分バックアップでは、サーバ データベースのバックアップ （31 ページ）に説明されているように、backup.properties ファイルの設定に基づいてレポート データベースを含めたり、除外したりします。

データのバックアップおよび復元中、Common Services と Security Manager の両方のプロセスがシャットダウンされてから再起動されます。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。差分バックアップを復元しようとする場合、システムにより、それが差分バックアップであることが指摘されるため、ユーザは差分バックアップの復元を行うことを確認する必要がある点に注意してください。

差分バックアップを生成するには、Security Manager サーバ上の Windows コマンド プロンプトで次のコマンドを使用します。

[*path*]**perl** [*path*]**partial_backup.pl** *backup_directory* [*log_filename* [**email**=*email_address* [*number_of_generations* [**compress**]]]]

構文

[*path*]**perl** [*path*]**partial_backup.pl**	Perl スクリプト コマンド。システムパス変数内に perl コマンドおよび partial_backup.pl ファイルへのパスが定義されていない場合は、そのパスを含めます。両方とも、通常のパスは C:\Progra~1\CSCOpx\bin\ です。
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。

log_filename	（オプション）バックアップ中に生成されたメッセージのログファイル。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。 名前を指定しない場合、ログは %NMSROOT%\log\dbbackup.log となります。
email=*email_address*	（オプション）通知が送信され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、後続のパラメータを指定する必要がある場合、等号またはアドレスを指定せずに **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。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定を参照してください。
number_of_generations	（オプション）バックアップディレクトリに保存するバックアップ世代の最大数。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	（オプション）バックアップファイルを圧縮するかどうかを指定します。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。

例

次のコマンドでは、現在のディレクトリに perl コマンドと partial_backup.pl コマンドが含まれていることを想定しています。バックアップディレクトリ内に圧縮された差分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。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 パラメータのあとに何らかのパラメータを指定した場合、その前にあるすべてのパラメータの値を含める必要があります。また、Configuration Archive を含めるかどうか確認されることも留意してください。含める場合は、バックアップに含めるアーカイブ バージョンの数が確認されます。この例では、デバイス単位に 5 つのアーカイブ バージョンをバックアップに含めます。

```
perl partial_backup.pl C:\backups C:\backups\pbackup.log email=admin@domain.com 0 compress
Root: c:\backups
Do you also want to take config-archive backup(Yes/No): Yes
How many previous config-archive you want to restore: 5
```

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。