Getting Started With Cisco Security Manager

製品の概要

（注）　バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および次のデバイスを含む Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

- Cisco Catalyst 6500 および 7600 シリーズ ファイアウォール サービス モジュール（EOL8184 [英語]）
- Cisco Catalyst 6500 シリーズ Intrusion Detection System サービスモジュール 2（EOL8843 [英語]）
- Cisco Intrusion Prevention System：IPS 4200、4300、および 4500 シリーズ センサー（EOL9916 [英語]）
- Cisco SR 500 シリーズ Secure Router（EOL7687 [英語]、EOL7657 [英語]）
- PIX ファイアウォール（EOL [英語]）

注意 バージョン 4.18 以降、Cisco Security Manager では、ASA 5512、ASA 5506、ASA 5506H、および ASA 5506W モデルの ASA 9.10(1) 以降の SFR はサポートされないため、Image Manager を介して 9.10(1) にアップグレードすると、既存の SFR 設定が失われます。

Cisco Security Manager（Security Manager）を使用すると、シスコセキュリティデバイスのセキュリティポリシーを管理できます。Cisco Security Manager では、複数の ASA セキュリティアプライアンス間でのファイアウォール、およびVPN（サイト間、リモートアクセス、およびSSL）サービスの統合的なプロビジョニングがサポートされています。

Cisco Security Manager でサポートされるデバイスおよび OS バージョンの一覧については、Cisco.com で『Supported Devices and Software Versions for Cisco Security Manager』[英語] を参照してください。

Security Manager では、インターフェイス、ルーティング、ID、QoS、ロギングなど、さまざまなプラットフォーム固有の設定のプロビジョニングもサポートしています。

Security Manager は、数台のデバイスで構成される小規模ネットワークから、数千台のデバイスで構成される大規模ネットワークまで、広範囲のネットワークを効率的に管理します。共有可能なオブジェクトおよびポリシーの持つ豊富なフィーチャセットと、デバイスのグループ化機能により、スケーラビリティが実現されます。

Security Manager では、さまざまなタスク フローと使用例に基づいて最適化された、複数の設定ビューをサポートしています。

ここでは、Security Manager の概要について説明します。

Cisco Security Manager の主な利点

Security Manager を使用する主な利点は、次のとおりです。

- [スケーラブルなネットワーク管理（Scalable network management）]：小規模ネットワーク、または数千台のデバイスで構成される大規模ネットワークのセキュリティポリシーとデバイス設定を集中管理します。ポリシーおよび設定は、定義したあとに、必要に応じて個別のデバイス、デバイスのグループ、または企業内のすべてのデバイスに割り当てます。
- [異なるプラットフォームにまたがる複数のセキュリティテクノロジーのプロビジョニング（Provisioning of multiple security technologies across different platforms）]：ルータ、セキュ

リティアプライアンス、Catalyst デバイスとサービスモジュール、および IPS デバイス上の VPN、ファイアウォール、および IPS テクノロジーを管理します。

- [プラットフォーム固有の設定およびポリシーのプロビジョニング（Provisioning of platform-specific settings and policies）]：特定のデバイスタイプでのプラットフォーム固有の設定を管理します。たとえば、ルータでのルーティング、802.1x、EzSDD、ネットワーク アドミッション コントロールや、ファイアウォール デバイスでのデバイス アクセス セキュリティ、DHCP、AAA、マルチキャストなどがあります。
- [VPN ウィザード（VPN wizards）]：異なる VPN デバイスタイプにわたってポイントツーポイント VPN、ハブアンドスポーク VPN、完全メッシュ、およびエクストラネット サイト間 VPN をすばやく簡単に設定します。ASA、IOS、および PIX デバイスでリモート アクセス IPsec および SSL VPN をすばやく簡単に設定します。
- [複数の管理ビュー（Multiple management views）]：デバイスビュー、ポリシービュー、およびマップビューを使用することにより、ニーズに最も適した環境でセキュリティを管理できます。
- [再利用可能なポリシーオブジェクト（Reusable policy objects）]：ネットワークアドレス、デバイス設定、VPN パラメータなどを表す、再利用可能なオブジェクトを作成します。作成後は、手動で値を入力する代わりに、このオブジェクトを使用します。
- [デバイスのグループ化機能（Device grouping capabilities）]：組織構造を表すデバイス グループを作成します。グループ内のすべてのデバイスを同時に管理します。
- [ポリシー継承（Policy inheritance）]：必須ポリシーおよび組織の下層に適用するポリシーを一元的に指定します。
- [ロールベースの管理（Role-based administration）]：複数のオペレータに対する適切なアクセスコントロールが可能です。
- [ワークフロー（Workflow）]：（任意）ネットワークオペレータとセキュリティオペレータの間で責務分担と作業負荷分散が可能となり、変更管理の承認とトラッキングメカニズムを実現します。
- [チケット管理（Ticket Management）]：チケット ID をポリシーの変更に関連付け、それらの変更に関するコメントを簡単に追加および更新し、Security Manager から外部の変更管理システムにすばやく移動します。
- [単一で一貫性のあるユーザインターフェイスによる共通ファイアウォール機能の管理（Single, consistent user interface for managing common firewall features）]：すべてのプラットフォーム（ルータ、PIX、ASA、および FWSM）に対応した単一のルールテーブル。
- [イメージ管理（Image management）]：ASA デバイス用の完全なイメージ管理。イメージリポジトリのダウンロードと保守、イメージの評価、アップグレードの影響の分析、信頼性が高く安定したデバイスアップグレードの準備と計画、十分なフォールバックと回復メカニズムの確保によって、デバイスのイメージアップグレードのすべての段階を容易にします。

- [ファイアウォールポリシーのインテリジェントな分析（Intelligent analysis of firewall policies）]：競合検出機能を使用して、他のルールと重複または競合するルールを分析およびレポートします。ACL ヒットカウント機能により、パケットが特定のルールに一致したか、または特定のルールがトリガーされたかどうかがリアルタイムでチェックされます。
- [ルールテーブルの高度な編集（Sophisticated rule table editing）]：インライン編集、ルールのカット、コピー、およびペースト機能とルールテーブル内でのルールの順序変更。
- デバイスからのファイアウォールポリシー検出（Discover firewall policies from device）：デバイス上に存在するポリシーを Security Manager にインポートし、あとで管理することができます。
- [柔軟性のある展開オプション（Flexible deployment options）]：デバイスに設定を直接展開する方法と設定ファイルに展開する方法をサポートします。Auto-Update Server（AUS）、Configuration Engine、または Token Management Server（TMS）を使用して、展開することもできます。
- [ロールバック（Rollback）]：必要に応じて以前の設定にロールバックすることができます。
- [FlexConfig（テンプレートマネージャ）（FlexConfig (template manager)）]：デバイスで使用可能な機能を管理するためのインテリジェントな CLI configlet エディタ。ただし、Security Manager では、ネイティブにはサポートしていません。
- [統合されたデバイスモニタリングとレポート（Integrated device monitoring and reporting）]：IPS、ASA、および FWSM デバイスでイベントをモニターし、関連する設定ポリシーにこれらのイベントを関連付けて、セキュリティレポートと使用状況レポートを作成するための機能。これらの機能には、次のスタンドアロン Security Manager アプリケーションが含まれます。
  - [Event Viewer（Event Viewer）]：Event Viewer は、ASA および FWSM デバイス、ならびにセキュリティコンテキストからのシステムログ（syslog）イベント、ならびに IPS デバイスおよび仮想センサーからの SDEE イベントを対象にネットワークをモニターします。Event Viewer は、これらのイベントを収集し、収集したイベントを表示し、グループ化し、その詳細をほぼリアルタイムで調べるためのインターフェイスを備えています。
  - [Report Manager（Report Manager）]：Report Manager を使用すると、ASA および IPS デバイス、および ASA がホストするリモートアクセス IPsec および SSL VPN に関するさまざまなネットワーク使用状況とセキュリティ情報を収集、表示、およびエクスポートできます。これらのレポートは、上位の送信元、宛先、攻撃者、攻撃対象などのセキュリティデータと、上位の帯域幅、期間、スループットユーザなどのセキュリティ情報を集計します。データは、時間、日、および月の期間で利用できます。（Report Manager は、Event Manager サービスによってモニターされるデバイスから収集される情報を集約します。このため、デバイスに関するレポートを表示するには、Event Viewer で該当デバイスをモニタリングしている必要があります）

（注） Event Viewer は FWSM を処理しますが、Report Manager は FWSM イベントについては報告しません。

- [Health and Performance Monitor（Health and Performance Monitor）]：Health and Performance Monitor（HPM）は、モニター対象の ASA デバイス、IPS デバイス、および ASA がホストする VPN サービスを、正常性およびパフォーマンスデータについて定期的にポーリングします。これらのデータには、メモリ使用量、インターフェイスステータス、ドロップされたパケット、トンネルステータスなど、重大な問題、および重大ではない問題が含まれます。この情報は、アラートの生成と電子メール通知に使用され、時間単位、日単位、および週単位で利用可能な集計データに基づいて傾向を表示します。

（注） Health and Performance Monitor は、FWSM デバイスをモニターしません。

- [ダッシュボード（Dashboard）]：ダッシュボードは、IPS と FW タスクをより便利にする Cisco Security Manager で設定可能な起動点です。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Security Manager の他のいくつかの領域にある、IPS Health Monitor ページ、Report Manager、Health and Performance Monitor および IP Intelligence 設定などの多くのタクスを 1 箇所で実行できます。ダッシュボードの詳細については、ダッシュボードの概要を参照してください。

追加機能を使用すると、Cisco Security Monitoring, Analysis and Response System（CS-MARS）、Cisco Performance Monitor、および ASDM（Security Manager に含まれる機能の読み取り専用バージョン）などのデバイスマネージャを含め、関連の深い他のアプリケーションを使用して、Security Manager からデバイスをモニターできます。

Security Manager のポリシーフィーチャセット

Security Manager には、主に次のような設定ポリシーのフィーチャセットが用意されています。

[ファイアウォールサービス（Firewall Services）]

IOS ルータ、ASA/PIX デバイス、Catalyst ファイアウォール サービス モジュール（FWSM）など、複数のプラットフォームにまたがるファイアウォールポリシーの設定および管理です。次の機能が含まれています。

- アクセスコントロールルール：IPv4 と IPv6 の両方のトラフィックに関するアクセスコントロールリストを使用して、インターフェイス上のトラフィックを許可または拒否する。
- ボットネット トラフィック フィルタ ルール：（ASA のみ）。既知のマルウェアサイトに基づいてトラフィックをフィルタ処理し、必要に応じて脅威レベルに基づいてトラフィックをドロップします。

- インスペクションルール：アプリケーション レイヤ プロトコルのセッション情報に基づいて、TCP パケットおよび UDP パケットをフィルタリングする。
- AAA/認証プロキシルール：HTTP、HTTPS、FTP、または Telnet のセッションを経由してネットワークにログインする、またはインターネットにアクセスするユーザの認証と認可に基づいて、トラフィックをフィルタリングする。
- Web フィルタリングルール：Websense などの URL フィルタリングソフトウェアを使用して、特定の Web サイトへのアクセスを拒否する。
- ScanSafe Web セキュリティ：（ルータのみ）。コンテンツスキャンおよびマルウェア保護サービスのために、HTTP/HTTPS トラフィックを ScanSafe Web セキュリティセンターにリダイレクトします。
- トランスペアレント ファイアウォール ルール：トランスペアレントなインターフェイスまたはブリッジングされたインターフェイス上で、レイヤ 2 トラフィックをフィルタリングする。
- ゾーンベースのファイアウォールルール：個々のインターフェイスではなく、ゾーンに基づいて、アクセルルール、インスペクションルール、および Web フィルタリングルールを設定する。

詳細については、ファイアウォール サービスの概要を参照してください。

[サイト間VPN（Site-to-Site VPN）]

IPsec サイト間 VPN のセットアップと設定です。IOS ルータ、PIX/ASA デバイス、Catalyst VPN サービスモジュールなど、複数のデバイスタイプが単一の VPN に参加できます。サポートされる VPN トポロジは、次のとおりです。

- ポイントツーポイント
- ハブアンドスポーク
- 完全メッシュ
- エクストラネット（管理対象外デバイスへのポイントツーポイント接続）

サポートされる IPsec テクノロジーは、次のとおりです。

- 通常の IPsec
- GRE
- GRE ダイナミック IP
- DMVPN
- Easy VPN
- GET VPN

詳細については、サイト間 VPN の管理：基本を参照してください。

[リモートアクセスVPN（Remote Access VPN）]

サーバーと、Cisco VPN Client またはセキュアクライアント ソフトウェアが稼働しているモバイル リモート ワークステーション間の IPsec および SSL VPN のセットアップと設定です。詳細については、リモート アクセス VPN の管理の基礎を参照してください。

[侵入防御システム（IPS）管理（Intrusion Prevention System (IPS) Management）]

Cisco IPS センサー（アプライアンスとサービスモジュール）および IOS IPS デバイス（IPS 対応イメージ搭載の Cisco IOS ルータと Cisco サービス統合型ルータ）の管理および設定です。

詳細については、IPS 設定の概要およびCisco IOS IPS 設定の概要を参照してください。

[ファイアウォールデバイス（PIX/ASA/FWSM）固有の機能（Features Specific to Firewall Devices (PIX/ASA/FWSM)）]

プラットフォーム固有の高度な機能の設定、および PIX/ASA デバイスと Catalyst FWSM の設定です。これらの機能は、セキュリティプロファイルを管理するときに付加価値を提供し、次のものを含みます。

- インターフェイス コンフィギュレーション
- ID 認証ファイアウォール設定
- デバイス管理設定
- セキュリティ
- ルーティング
- マルチキャスト
- ログ
- NAT
- ブリッジング
- フェールオーバー
- セキュリティコンテキスト

詳細については、ファイアウォール デバイスの管理を参照してください。

[IOSルータ固有の機能（Features Specific to IOS Routers）]

プラットフォーム固有の高度な機能の設定、およびIOSルータの設定です。これらの機能は、セキュリティプロファイルを管理するときに付加価値を提供し、次のものを含みます。

- インターフェイス コンフィギュレーション
- ルーティング
- NAT
- 802.1x
- NAC
- QoS

- ダイヤラインターフェイス
- セキュア デバイス プロビジョニング

詳細については、ルータの管理を参照してください。

Catalyst 6500/7600デバイスおよびCatalystスイッチ固有の機能（Features Specific to Catalyst 6500/7600 Devices and Catalyst Switches）

VLAN、ネットワーク接続、およびサービスモジュールの機能の設定と、Catalyst 6500/7600 デバイスおよびその他の Catalyst スイッチの設定です。

詳細については、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理を参照してください。

[FlexConfig（FlexConfig）]

FlexConfig ポリシーおよびポリシーオブジェクトを使用すると、デバイスでは使用できるが、Security Manager でネイティブにサポートされていない機能をプロビジョニングできます。このポリシーやオブジェクトによって、一連の CLI コマンドを手動で指定し、Cisco Security Manager のプロビジョニングメカニズムを使用して、デバイスにコマンドを展開できます。Security Manager で生成されたコマンドの前後にこれらのコマンドを追加すると、セキュリティポリシーをプロビジョニングできます。

詳細については、FlexConfig の管理を参照してください。

Security Manager アプリケーションの概要

Cisco Security Manager クライアントには、6 つの主要アプリケーションとモバイルデバイス用に設計された 1 つのアプリケーションがあります。

- [Configuration Manager（Configuration Manager）]：これがプライマリアプリケーションです。Configuration Manager を使用して、デバイスインベントリの管理、ローカルポリシーと共有ポリシーの作成と編集、VPN設定の管理、およびデバイスへのポリシーの展開を行います。Configuration Manager は最大のアプリケーションであり、ほとんどのマニュアルでこのアプリケーションが扱われています。手順でアプリケーションが明確に言及されていない場合は、手順では Configuration Manager を使用しています。Configuration Manager の概要については、Configuration Manager の使用方法 - 概要 （19 ページ）を参照してください。
- [イベントビューア（Event Viewer）]：これはイベントモニタリングアプリケーションで、Cisco Security Manager にイベントを送信するよう設定した IPS、ASA、および FWSM デバイスから生成されたイベントを表示および分析できます。Event Viewer の使用については、イベントの表示を参照してください。
- [Report Manager（Report Manager）]：これはレポートアプリケーションで、デバイスに関する集約された情報および VPN 統計情報のレポートを表示および作成できます。多くの情報は、Event Viewer で使用可能なイベントから取得されますが、一部の VPN 統計情報は、デバイスと直接通信することで取得されます。Report Manager の使用方法については、レポートの管理を参照してください。

- [Health & Performance Monitor（Health & Performance Monitor）]：HPM アプリケーションを使用すると、デバイスのステータスとトラフィック情報をネットワークレベルで可視化することで、ASA（ASA-SM を含む）デバイス、IPS デバイス、VPN サービスの主要な正常性データとパフォーマンスデータを監視できます。この機能を使用して、主要なネットワークとデバイスのメトリックを監視することで、ネットワーク内のデバイスの誤動作やボトルネックをすばやく検出して解決できます。このアプリケーションの詳細については、ヘルスとパフォーマンスのモニタリングを参照してください。
- [Image Manager（Image Manager）]：Image Manager アプリケーションでは、ASA デバイス用の完全なイメージ管理が提供されるため、イメージの更新のダウンロード、評価、分析、準備、および計画が容易になります。また、イメージの可用性、互換性、デバイスへの影響を評価し、デバイス更新のスケジュール、グループ化、および変更管理が提供されます。さらに、Image Manager には、イメージリポジトリを維持するための機能と、ASA デバイスでのイメージ更新の安定したフォールバックや回復メカニズムを保証するための機能が含まれています。Image Manager の使用方法については、Image Manager の使用を参照してください。
- [ダッシュボード（Dashboard）]：ダッシュボードは、IPS と FW タスクをより便利にする Cisco Security Manager で設定可能な起動点です。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Security Manager の他のいくつかの領域にある、IPS Health Monitor ページ、Report Manager、Health and Performance Monitor および IP Intelligence 設定などの多くのタクスを 1 箇所で実行できます。ダッシュボードの詳細については、ダッシュボードの概要を参照してください。

これらのアプリケーションはすべて、Windows のスタートメニューまたはデスクトップアイコンから直接開くことができます。または、アプリケーションの [起動（Launch）] メニューから開くことができます。アプリケーションを開く方法については、Security Manager へのログインおよび終了 （15 ページ）を参照してください。

Cisco Security Manager クライアントには、モバイルデバイス用に特別に設計された追加のアプリケーションである CSM Mobile があります。

- [CSM Mobile（CSM Mobile）]：CSM Mobile では、モバイルデバイスから Device Health Summary 情報にアクセスできます。この方法で入手できる情報は、Device Health Summary ウィジェットで入手可能な情報と同じ、HPM によって生成される現在の重大度が低いまたは中程度のアクティブなアラートになります。アラートは、Alert-Description、Predefined-Category、Device または Alert Technology 別にグループ化できます。CSM Mobile の詳細については、CSM Mobileを参照してください。Device Health Summary 情報の詳細については、ダッシュボードの概要を参照してください。CSM Mobile の有効化または無効化については、[CSM Mobile] ページを参照してください。

デバイスモニタリングの概要

Security Manager には、デバイスをモニタするための機能がいくつか備わっています。

- [イベントビューア（Event Viewer）]：この統合ツールを使用すると、ASA、FWSM、およびIPSデバイスでイベントを表示し、関連する設定ポリシーにそのイベントを関連付けることができます。これは、問題の特定、設定のトラブルシューティング、および設定の修正と再展開を行う場合に役立ちます。詳細については、イベントの表示を参照してください。
- [Report Manager（Report Manager）]：これはレポートアプリケーションで、デバイスに関する集約された情報およびVPN統計情報のレポートを表示および作成できます。多くの情報は、Event Viewerで使用可能なイベントから取得されますが、一部のVPN統計情報は、デバイスと直接通信することで取得されます。Report Managerの使用方法については、レポートの管理を参照してください。

Security Managerで使用可能なレポートのすべてのタイプについては、Security Managerで使用可能なレポートのタイプについてを参照してください。

- [Health & Performance Monitor（Health & Performance Monitor）]：HPMアプリケーションを使用すると、ASA（ASA-SMを含む）デバイスの主要な正常性データとパフォーマンスデータを監視できます。このアプリケーションの詳細については、ヘルスとパフォーマンスのモニタリングを参照してください。
- [ダッシュボード（Dashboard）]：ダッシュボードは、IPSとFWタスクをより便利にするCisco Security Managerで設定可能な起動点です。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Security Managerの他のいくつかの領域にある、IPS Health Monitorページ、Report Manager、Health and Performance Monitorおよび IP Intelligence設定などの多くのタクスを1箇所で実行できます。ダッシュボードの詳細については、ダッシュボードの概要を参照してください。
- [パケットトレーサ（Packet Tracer）]：このツールを使用すると、特定のタイプのパケットがASAデバイスを通過するのを許可されているかテストできます。詳細については、Packet Tracerを使用したASAまたはPIXの設定の分析を参照してください。
- [ping、トレースルート、およびNSルックアップ（Ping, Trace route, and NS Lookup）]：管理対象デバイスでpingとトレースルートを使用して、デバイスと特定の宛先の間にルートが存在するかどうかを確認できます。NSルックアップを使用すると、アドレスをDNS名に解決できます。詳細については、ping、トレースルート、またはNSルックアップツールを使用した接続問題の分析を参照してください。
- [Cisco Prime Security Manager（PRSM）の統合（Cisco Prime Security Manager (PRSM) Integration）]：Configuration Managerアプリケーションから PRSMを「クロス起動」できます。PRSMアプリケーションは、ASA CXデバイスの設定と管理に使用されます。詳細については、Cisco Prime Cisco Security ManagerまたはFireSIGHT Management Centerの起動を参照してください。
- [デバイスマネージャの統合（Device Manager Integration）]：Cisco Security Managerには、Adaptive Security Device Manager（ASDM）など、さまざまなデバイスマネージャの読み取り専用コピーが含まれています。これらのツールを使用すると、デバイスステータスの表

示はできますが、デバイス設定の変更はできません。詳細については、デバイス マネージャの起動を参照してください。

- [Cisco Security Monitoring, Analysis and Response System（CS-MARS）の統合（Cisco Security Monitoring, Analysis and Response System (CS-MARS) Integration）]：CS-MARS アプリケーションを使用する場合は、Cisco Security Manager と統合して、CS-MARS のイベントを Cisco Security Manager で表示したり、逆にイベントに関連する Cisco Security Manager ポリシーを CS-MARS で表示できます。詳細については、CS-MARS と Security Manager の統合を参照してください。

Security Manager での IPv6 サポート

Security Manager では、より多くの IPv6 設定、モニタリング、およびレポートのサポートを提供しています。

バージョン 4.12 以降、Security Manager は、IPv6 アドレスまたは IPv4 アドレスを介した Security Manager サーバーから管理対象デバイスへの通信をサポートします。この機能は、ファイアウォールデバイス、つまり、OS タイプが ASA または FWSM のデバイスでのみ使用できます。IPv6 アドレスを介した通信を有効にするには、最初に Security Manager サーバーで IPv6 アドレスを有効にする必要があります。詳細については、Cisco Security Manager サーバーでの IPv6 の設定 （11 ページ）を参照してください。

（注） Security Manager サーバーと Security Manager クライアント間の通信は、IPv4 アドレスのみを介して行われます。サーバーからクライアントへの通信では、IPv6 アドレスはサポートされていません。また、認証に ACS サーバーを使用する場合、ACS には IPv4 アドレスが必要です。ACS サーバーへの IPv6 通信はサポートされていません。Auto Update Server（AUS）は IPv6 アドレスをサポートしていません。

4.12 以前のバージョンで、IPv6 アドレスをサポートするデバイスを Security Manager で管理するには、デバイスの管理アドレスを IPv4 アドレスとして設定する必要があります。ポリシー検出と展開など、デバイスと Security Manager 間のすべての通信で IPv4 トランスポートが使用されます。サポートされるデバイスで IPv6 ポリシーが表示されない場合は、デバイス ポリシーを再検出します。必要に応じて、インベントリからそのデバイスを削除して、再度追加します。

Cisco Security Manager サーバーでの IPv6 の設定

次の手順に従って、IPv6 アドレスを介してデバイスと通信するように Security Manager サーバーで IPv6 を設定します。

ステップ 1 Security Manager サーバーで、**[スタート（Start）] > [コントロールパネル（Control panel）] > [ネットワークとインターネット（Network and Internet）] > [ネットワーク接続（Network Connections）]** に移動します。

ステップ 2 使用可能なネットワーク接続をクリックして、[イーサネットのステータス（Ethernet Status）] ウィンドウを開きます。[プロパティ（Properties）] をクリックします。 [イーサネットのプロパティ（Ethernet Properties）] ウィンドウが表示されます。

ステップ 3 [ネットワーク（Networking）] タブで、[インターネットプロトコルバージョン6（TCP/IPv6）（Internet Protocol Version 6 (TCP/IPv6)）] チェックボックスをオンにし、[プロパティ（Properties）] をクリックします。[インターネットプロトコルバージョン 6（TCP/IPv6）のプロパティ（Internet Protocol Version 6 (TCP/IPv6) Properties）] ウィンドウが表示されます。

ステップ 4 IPv6 スタティックアドレスと DNS サーバーを設定し、[OK（OK）] をクリックします。

（注） Security Manager サーバーのホスト名を、IPv4 アドレスのみに解決されるように設定する必要があります。サーバーのホスト名が IPv6 アドレスに解決されないようにしてください。

IPv6 ポリシーの設定

通常、次のタイプのデバイスで IPv6 ポリシーを設定できます。さらに、IPS、ASA、および FWSM デバイスによって生成された IPv6 アラートをモニタできます。その他のタイプのデバイスでは、FlexConfig ポリシーを使用して IPv6 設定を行います。IPv6 デバイスサポートに関する具体的な情報については、Cisco.com で『Supported Devices and Software Versions for Cisco Security Manager』[英語] を参照してください。

- [ASA（ASA）]：ルータモードで実行されている場合はリリース 7.0 以降、トランスペアレントモードで実行されている場合はリリース 8.2 以降。1 つのセキュリティ コンテキスト デバイスと複数のセキュリティ コンテキスト デバイスの両方がサポートされます。
- [FWSM（FWSM）]：ルータモードで実行されている場合はリリース 3.1 以降。トランスペアレントモードではサポートされません。1 つのセキュリティ コンテキスト デバイスと複数のセキュリティ コンテキスト デバイスの両方がサポートされます。
- [IPS（IPS）]：リリース 6.1 以降。

次に、IPv6 アドレッシングをサポートする Security Manager 機能の要約を示します。

- [ポリシーオブジェクト（Policy Objects）]：次のポリシーオブジェクトで IPv6 アドレスがサポートされます。
  - ネットワーク/ホスト。ネットワーク/ホストオブジェクトについてを参照してください。
  - サービス。このオブジェクトには、IPv6 ポリシーとのみ使用できる、ICMP6 および DHCPv6 用の定義済みサービスが含まれています。他のサービスは、IPv4 と IPv6 の両方に適用されます。サービス オブジェクトの詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。
- **ファイアウォール サービスポリシー**：次のファイアウォール サービス ポリシーとツールでは IPv6 設定がサポートされます。
  - AAA ルール。ファイアウォール AAA ルールの管理を参照してください。

- アクセスルール。アクセス ルールの設定を参照してください。
- インスペクションルール。ファイアウォール インスペクション ルールの管理を参照してください。

  [設定（Settings）] > [アクセス制御（Access Control）]。アクセス コントロール ポリシー設定の指定を参照してください。
- Tools:

[Hit Count]。ヒットカウントの詳細の表示を参照してください。

[Find and Replace]。ルール テーブルの項目の検索と置換を参照してください。

- **ASA および FWSM ポリシー**：次の ASA および FWSM ポリシーでは IPv6 設定がサポートされます。
  - （ASA 7.0 以降のルーテッドモード、ASA 8.2 以降のトランスペアレントモード、FWSM 3.1 以降のルーテッドモード）。インターフェイス：[インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスの [IPv6] タブ。IPv6 インターフェイスの設定（ASA/FWSM）を参照してください。
  - （ASA のみ）。**[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [IPv6 ネイバーキャッシュ（IPv6 Neighbor Cache）]**。IPv6 ネイバー キャッシュの管理を参照してください。
  - （ASA 5505 8.2/8.3 のみ）。**[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [管理IPv6（Management IPv6）]**。[Management IPv6] ページ（ASA 5505）を参照してください。
  - （ASA 8.4.2 以降のみ）。**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS]**。[DNS] ページを参照してください。
- **FlexConfig ポリシー**：デバイスで IPv6 ACL を識別するために使用できる 2 つのファイアウォールシステム変数があります。詳細については、FlexConfig システム変数を参照してください。

これらの変数を使用する定義済みの FlexConfig ポリシー オブジェクト（ASA_add_IPv6_ACE）もあります。

- **イベントビューア**：IPv6 アドレスが含まれているイベントがサポートされ、アドレスは、IPv4 アドレスと同じ列（[送信元（Source）]、[宛先（Destination）]、および [IPLog アドレス（IPLog Address）]（IPS アラートの場合））に表示されます。ただし、Security Manager サーバへのイベントの送信に IPv4 を使用するようデバイスを設定する必要があります。すべてのイベント通信で IPv4 トランスポートが使用されます。Event Viewer の詳細については、イベントの表示を参照してください。

- **ダッシュボード**：ダッシュボードでは、IP アドレスを使用するすべてのウィジェットで IPv6 アドレスがサポートされます。ただし、Cisco Security Manager における他の場合と同様に、Cisco Security Manager サーバーへのイベントの送信時に IPv4 を使用するようデバイスを設定する必要があります。すべてのイベント通信で IPv4 トランスポートが使用されます。ダッシュボードの詳細については、ダッシュボードの概要を参照してください。
- **Report Manager**：レポートには、イベント管理によって収集された IPv6 イベントの統計情報が含まれています。Report Manager の詳細については、レポートの管理を参照してください。

Cisco Security Manager 4.4 でのポリシーオブジェクトの変更

以前は分離していた IPv4 要素と IPv6 要素を統合するために、Security Manager 4.4 のいくつかのポリシーとポリシーオブジェクトに一定の変更が加えられました。これらの変更の中で最も重要なのは、ネットワーク/ホストオブジェクト（それ自体はネットワーク/ホストオブジェクトとネットワーク/ホスト IPv6 オブジェクトの統合を表す）に対する変更です。

- 新しいネットワーク/ホストオブジェクト「All-IPv4-Addresses」によって、IPv4「any」ネットワーク ポリシー オブジェクトは置き換えられます。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、IPv4「any」ネットワーク ポリシー オブジェクトへのすべての参照が「All-IPv4-Addresses」に変更されます。
- 新しいネットワーク/ホストオブジェクト「All-IPv6-Addresses」によって、IPv6「any」ネットワーク ポリシー オブジェクトは置き換えられます。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、IPv6「any」ネットワーク ポリシー オブジェクトへのすべての参照が「All-IPv6-Addresses」に変更されます。
- 新しいネットワーク/ホストオブジェクト「All-Addresses」には、以前のバージョンの Security Manager に対応するポリシーオブジェクトがありません。これは新しいグローバルな「any」ポリシーオブジェクトであり、すべての IPv4 および IPv6 アドレス範囲を含みます。

その他の関連する変更には、アクセスルール、検査ルールといったデバイス固有のポリシーの IPv4 バージョンと IPv6 バージョンの統合が含まれます。

さらに、ポリシーとオブジェクトを編集するとき、IPv4、IPv6、または混合モード（IPv4 と IPv6 の両方）のエントリは、ダイアログボックスなどの要素で自動的にフィルタリングされます（これらのエントリの 1 つ以上が要素に該当しません）。

関連項目

- Policy Object Manager
- ネットワーク/ホストオブジェクトについて

Security Manager へのログインおよび終了

Security Manager には、次の 2 つの主要インターフェイスがあります。

- Cisco Security Management Suite ホームページ：このインターフェイスは、Security Manager クライアントをインストールする場合およびサーバを管理する場合に使用します。Resource Manager Essentials（RME）など、インストール済みの他の CiscoWorks アプリケーションにアクセスすることもできます。
- Security Manager クライアント：これらのインターフェイスは、ほとんどの Security Manager タスクを実行する場合に使用します。6 つのクライアントアプリケーション（Configuration Manager、Event Viewer、Report Manager、Health & Performance Monitor、Image Manager またはダッシュボード）のいずれかに直接記録できます。

ここでは、これらのインターフェイスにログインする方法およびインターフェイスを終了する方法について説明します。

- ユーザの権限について （15 ページ）
- Cisco Security Management Suite サーバへのログイン （16 ページ）
- Security Manager クライアントへのログインおよび終了 （17 ページ）

ユーザの権限について

ユーザがログインする前に、Cisco Security Manager によってユーザ名とパスワードが認証されます。認証されると、Security Manager によってアプリケーション内のユーザのロールが確立されます。このロールによって、実行が認可されるタスクまたは操作のセットである権限（特権とも呼ばれる）が定義されます。特定のタスクまたはデバイスに対して認可されなかった場合は、関連するメニュー項目、目次内の項目、およびボタンが非表示またはディセーブルになります。加えて、選択した情報を表示したり、選択した操作を実行したりするための権限がないことを伝えるメッセージが表示されます。

Security Manager の認証と認可は、CiscoWorks サーバと Cisco Secure Access Control Server（ACS）のどちらかによって管理されます。デフォルトでは CiscoWorks で認証および認可を管理しますが、Security Manager を設定すれば Cisco Secure ACS セットアップを使用できます。

（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。

ACS を使用する場合は、すべての ACS サーバが利用不能な状態になると Security Manager でタスクを実行できません。ログイン済みの場合は、ACS による認可が必要なタスクを実行しようとすると、（変更を保存する間もなく）システムから突然ログアウトされることがあります。この場合、認可を実行できないためにログオフされたことを示すメッセージが表示されま

す。Security Manager と ACS の統合の設定方法については、「Integrating Security Manager with Cisco Secure ACS」を参照してください。

ユーザ権限および AAA 設定の詳細については、『Installation Guide for Cisco Security Manager』を参照してください。

Event Viewer および Report Manager アプリケーションでの認可制御の詳細については、次の項を参照してください。

- Event Viewer のアクセス コントロールについて
- Report Manager のアクセス コントロールについて

Cisco Security Management Suite サーバへのログイン

Security Manager クライアントをインストールしてサーバを管理するには、Cisco Security Management Suite ホームページおよび CiscoWorks Common Services を使用します。RME など、インストール済みの他の CiscoWorks アプリケーションにアクセスすることもできます。

（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。

ステップ 1 Web ブラウザで、次の URL のいずれかを開きます。*SecManServer* は、Security Manager がインストールされているコンピュータの名前です。いずれかの [セキュリティアラート（Security Alert）] ウィンドウで [はい（Yes）] をクリックします。

- SSL を使用していない場合は、http://*SecManServer*:1741 を開きます。
- SSL を使用している場合は、https://*SecManServer*:443 を開きます。

Cisco Security Management Suite のログイン画面が表示されます。ページ上で、JavaScript と cookie がイネーブルになっていることと、サポートされているバージョンの Web ブラウザを実行していることを確認します。Security Manager を実行するためのブラウザの設定方法については、『Installation Guide for Cisco Security Manager』を参照してください。

ステップ 2 ユーザ名とパスワードを使用して、Cisco Security Management Suite サーバにログインします。初めてサーバーをインストールする場合は、ユーザー名 **admin** と、製品のインストール中に定義されたパスワードを使用してログインできます。

ステップ 3 Cisco Security Management Suite ホームページで、少なくとも次の機能にアクセスします。製品のインストール内容によっては、他の機能も使用できる場合があります。

- [Cisco Security Manager Client Installer]：この項目をクリックして、Security Manager クライアントをインストールします。このクライアントが、製品を使用する際の主要なインターフェイスとなります。
- Server Administration：この項目をクリックすると、CiscoWorks Common Services Server のページが開きます。CiscoWorks Common Services は、サーバを管理する基盤ソフトウェアです。このソフトウェア

を使用して、サーバの保守とトラブルシューティングやローカルユーザ定義などのバックエンドサーバ機能を設定して管理します。

- CiscoWorks リンク（ページ右上）：このリンクをクリックすると、CiscoWorks Common Services のホームページが開きます。

ステップ 4 アプリケーションを終了するには、画面右上隅にある [ログアウト（Logout）] をクリックします。ホームページと Security Manager クライアントの両方を同時に開いている場合は、ブラウザ接続を終了しても Security Manager クライアントが終了しません。

次のタスク

（注） PCI コンプライアンスに対応するために、TLS 1.0 は CSM サーバーで無効になっています。そのため、CSM サーバーは TLS 1.0 クライアントの接続を許可しません。この変更は、CSM サーバーからデバイスへの通信には適用されません。既存の CSM サーバーからデバイスへの通信は、引き続きサポートされます。

Security Manager クライアントへのログインおよび終了

Security Manager クライアントを使用して、ほとんどの Security Manager タスクを実行します。

ヒント Security Manager クライアント アプリケーションを十分に活用できる管理者特権が付与された Windows ユーザ アカウントを使用してワークステーションにログインする必要があります。より低い特権を使用してアプリケーションを操作しようとすると、一部の機能が正しく機能しない場合があります。

はじめる前に

コンピュータにクライアントをインストールします。クライアントをインストールするには、Security Manager サーバーにログインし（Cisco Security Management Suite サーバへのログイン（16 ページ）を参照）、[Cisco Security Managerクライアントインストーラ（Cisco Security Manager Client Installer）] をクリックしてインストールウィザードの指示に従ってください。

ステップ 1 [開始（Start）]>[すべてのプログラム（All Programs）]>[Cisco Security Managerクライアント（Cisco Security Manager Client）] メニューから、次のいずれかのアプリケーションを選択します。

- 設定マネージャ（Configuration Manager）
- イベントビューア
- Report Manager

- Health and Performance Monitor
- Image Manager
- ダッシュボード

ヒント　クライアントがワークステーションにインストールされているのに [Start] メニューに表示されない場合は、別のユーザがクライアントをインストールした可能性があります。クライアントステーションのすべてのユーザに対して、Security Manager クライアントが [Start] メニューに表示されるようにするには、Cisco Security Manager クライアント フォルダを Documents and Settings\<user>\Start Menu\Programs\Cisco Security Manager から Documents and Settings\All Users\Start Menu\Programs\Cisco Security Manager にコピーします。

ステップ 2 アプリケーションのログインウィンドウで、ログインするサーバーを選択して、Security Manager のユーザー名とパスワードを入力します。[ログイン（Login）] をクリックします。

クライアントがサーバにログインし、次の条件に基づいて選択したアプリケーションが開きます。これらの条件はアプリケーション単位であることに注意してください。たとえば、あるワークステーションで Configuration Manager を開いている場合に、別のワークステーションから Event Viewer を開いても、Event Viewer から Configuration Manager を開始しないかぎり、Configuration Manager セッションは影響を受けません。

- Workflow モードと Workflow 以外のモードの両方で、単一のワークステーションからは同じサーバにログインできず、同じユーザアカウントを使用して複数のアクティブセッションを使用することはできません。すでにログインしていることが通知され、既存の開いているアプリケーションを再使用するよう求められます。
- 両方の Workflow モードで、同じ（または別の）ユーザ名を使用して同じワークステーションから異なるサーバにログインできます。
- Workflow 以外のモードでは、特定のサーバでユーザ名が別のワークステーションにログインしている場合は、他のワークステーションのクライアントは自動的にログアウトされ、保存されていない変更はすべて失われます。そのため、ユーザアカウントを共有しないでください。別のワークステーションから同じサーバにログインする必要がある場合は、アクティブクライアントを終了する前に忘れずに変更を保存してください。
- Workflow モードでは、異なるワークステーションだけから、同じユーザアカウントを使用して複数回ログインできます。ただし、複数のクライアントで同時に Configuration Manager で同じアクティビティを開くことはできません。別のアクティビティを開く必要があります。アクティビティは、Event Viewer または Report Manager の使用時には適用されません。

ヒント　クライアントは、アイドル状態が 120 分間続くと自動的に閉じます。アイドルタイムアウトを変更するには、Configuration Manager で [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] の順に選択し、コンテンツテーブルから [デスクトップのカスタマイズ（Customize Desktop）] を選択して、必要なタイムアウト期間を入力します。この機能をディセーブルにして、クライアントが自動的に閉じないようにすることもできます。すべてのアプリケーションが同じタイムアウト設定を使用し、あるアプリケーションでの作業によって、その他すべてのアプリケーションのタイマーがリセットされます。

ステップ 3 アプリケーションを終了するには、[ファイル（File）] > [終了（Exit）] の順に選択します。

Configuration Manager の使用方法 - 概要

ここでは、Configuration Manager で使用できるさまざまなビューの概要、ポリシーを定義してデバイスに展開するための基本タスク フロー、およびいくつかの基本概念について説明します。

Configuration Manager の概要

Configuration Managerアプリケーションには、デバイス ビュー、ポリシー ビュー、およびマップ ビューという 3 つのビューがあり、これらのビューによってデバイスおよびポリシーを管理できます。ツールバーのボタンまたは [View] メニューを使用すると、必要に応じてこれらのビュー間を切り替えることができます。

- デバイス ビュー：デバイス中心のビューを表示します。このビューでは、個々のデバイスのポリシーを設定します。詳細については、 デバイス ビューの概要 （20 ページ）を参照してください。
- ポリシー ビュー：ポリシー中心のビューを表示します。このビューでは、デバイスに依存しない共有ポリシーを作成し、1 つ以上のデバイスに割り当てることができます。詳細については、 ポリシー ビューの概要 （22 ページ）を参照してください。
- マップ ビュー：ネットワークを視覚的に表示します。これは、主にサイト間 VPN を視覚的に表示して設定する場合に役立ちます。詳細については、 マップ ビューの概要 （23 ページ）を参照してください。

各ビューを使用すると、Configuration Manager の機能に異なる方法でアクセスできます。操作できる内容と操作方法は、選択したビューによって決まります。デバイス ビューおよびポリシー ビューでは、左側に 2 つのセレクタ、右側に作業領域が表示されます。それぞれのビューで上部のセレクタから項目を選択すると、下部のセレクタで選択できる項目が決まります。下部のセレクタから項目を選択すると、作業領域に表示される内容が決まります。この設計により、目的のネットワークの詳細まですばやく簡単にドリルダウンして表示または編集できます。

メインのビュー以外にも、サイト間 VPN やポリシー オブジェクトなどの他の項目を設定するとき、またはデバイスをモニタするときに使用するツールがいくつかあります。通常、これらのツールは [Manage] メニューから使用できますが、一部は [Policy]、[Activities]、[Tools]、または [Launch] メニューから使用できます。関連するボタンがツールバーに用意されているツー

ルもあります。これらのツールは別のウィンドウで開くため、現在使用しているメイン ビューの位置を見失うことはありません。

ユーザ インターフェイスの基本機能に関する参照情報については、次の項を参照してください。

- Configuration Manager のメニュー バー リファレンス （38 ページ）
- ツールバー リファレンス（Configuration Manager） （51 ページ）
- セレクタの使用 （59 ページ）
- ウィザードの使用 （63 ページ）
- ルール テーブルの使用
- テキスト フィールドの使用方法 （65 ページ）
- オンライン ヘルプの利用方法 （69 ページ）

デバイス ビューの概要

Configuration Manager のデバイス ビューを使用すると、Security Manager インベントリにデバイスを追加して、デバイス ポリシー、プロパティ、インターフェイスなどを集中管理できます。次の図に、デバイス ビューの機能領域を示します。

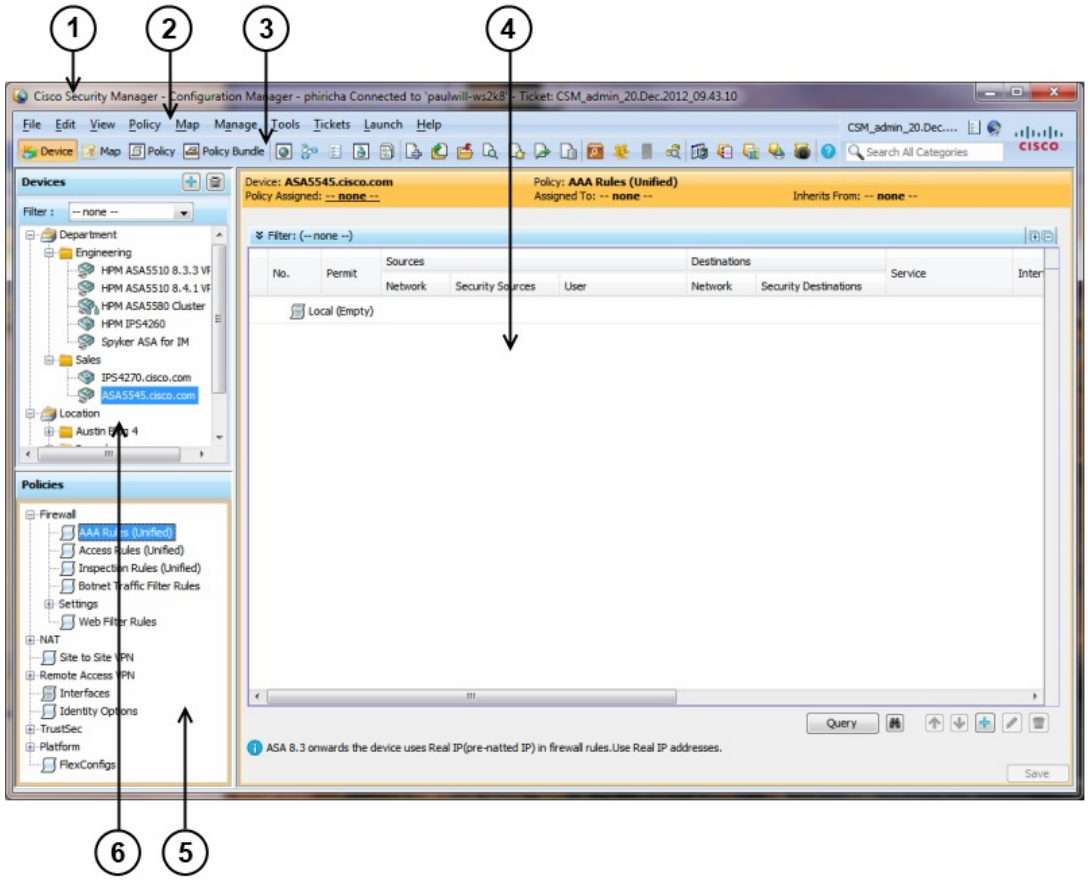
これはデバイス中心のビューであり、すべての管理対象デバイスを表示したり、特定のデバイスを選択してそのプロパティの表示や設定とポリシーの定義を行うことができます。

（注） Security Manager には、Security Manager インベントリ内のデバイスのステータスを表示する機能もあります。デバイスステータスビューにアクセスするには、[表示（View）]>[デバイスステータスビュー（Device Status View）] を選択するか、デバイスセレクタでフォルダノードの 1 つを選択します。詳細については、[デバイスステータスビュー（Device Status View）] の使用を参照してください。

デバイス ビューでは、個々のデバイスのローカルにセキュリティ ポリシーを定義できます。続けて、グローバルに使用できるようにポリシーを共有すれば、他のデバイスに割り当てることができます。

詳細については、デバイス ビューについてを参照してください。

図 *1*: デバイス ビューの概要



1	タイトル バー	2	メニュー バー（Configuration Manager のメニュー バー リファレンス （38 ページ）を参照）
3	ツールバー（ツールバー リファレンス（Configuration Manager） （51 ページ）を参照）	4	作業領域
5	ポリシー セレクタ	6	デバイス セレクタ（セレクタの使用 （59 ページ）を参照）

タイトル バーには Security Manager の次の情報が表示されます。

- ログイン名
- 接続先の Security Manager サーバの名前
- 開いているアクティビティの名前（Workflow モードがイネーブルの場合）

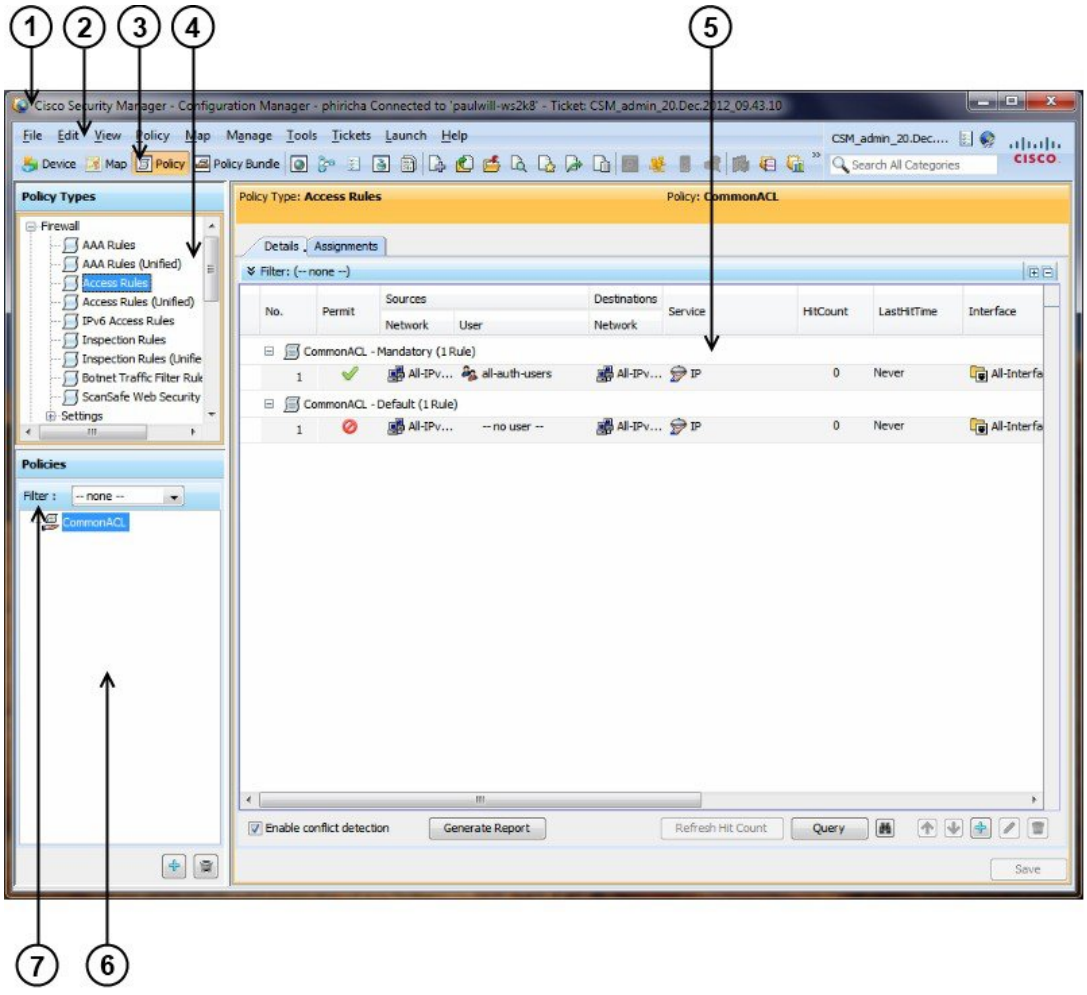
ポリシー ビューの概要

Configuration Manager のポリシー ビューを使用すると、複数のデバイス間で共有できる、再利用可能なポリシーを作成および管理できます。次の図に、ポリシー ビューの機能領域を示します。

これはポリシー中心のビューです。このビューには、Security Manager でサポートされている、共有可能なポリシー タイプがすべて表示されます。特定のポリシー タイプを選択して、そのタイプの共有ポリシーを作成、表示、または変更できます。各共有ポリシーが割り当てられているデバイスを確認し、必要に応じて割り当てを変更することもできます。

詳細については、ポリシー ビューにおける共有ポリシーの管理を参照してください。

図 *2:* ポリシー ビューの概要



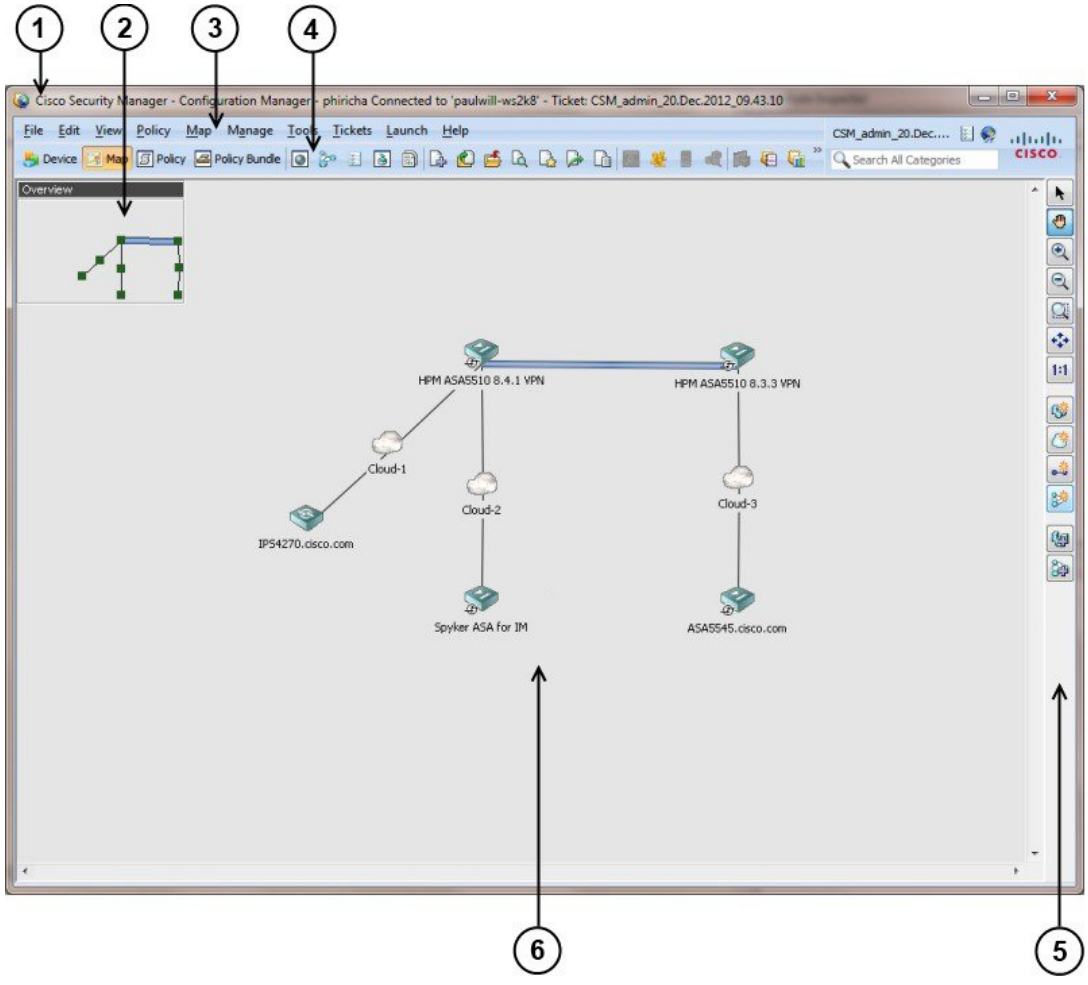
1	タイトル バー	2	メニューバー（Configuration Manager のメニュー バー リファレンス （38 ページ）を参照）

3	ツールバー（ツールバー リファレンス（Configuration Manager） （51 ページ）を参照）	4	ポリシー タイプ セレクタ（セレクタの使用（59 ページ）を参照）
5	作業領域	6	共有ポリシー セレクタ
7	ポリシー フィルタ		

マップ ビューの概要

Configuration Manager のマップ ビューを使用すると、ネットワークのカスタマイズされた視覚的なトポロジ マップを作成できます。このトポロジ マップ内で、デバイス間の接続を表示したり、VPN およびアクセス コントロール設定を簡単に行ったりできます。次の図は、マップ ビューの機能領域を示しています。

図 *3:* マップ ビューの概要



1	タイトル バー	2	ナビゲーション ウィンドウ

3	メニューバー（[Map] メニュー（Configuration Manager） （43 ページ）を参照）	4	ツールバー（ツールバー リファレンス（Configuration Manager） （51 ページ）を参照）
5	マップ ツールバー（マップ ツールバーを参照）	6	マップ

セキュリティ ポリシー設定のタスク フロー

デバイスのセキュリティ ポリシーを設定する場合、基本となるユーザ タスク フローは、Security Manager インベントリへのデバイスの追加、ポリシーの定義、およびデバイスへのポリシーの展開です。これらのタスクは Configuration Manager で実行します。次に、一般的なユーザ タスク フローの手順を簡単に説明します。

ステップ 1 **管理するデバイスを準備します。**

Security Manager デバイス インベントリにデバイスを追加して管理する前に、デバイスで最小限の設定を行い、Security Manager がデバイスに接続できるようにする必要があります。詳細については、デバイスを管理するための準備を参照してください。

ステップ 2 **Security Manager デバイス インベントリにデバイスを追加します。**

Security Manager でデバイスを管理するには、まず Security Manager インベントリにそのデバイスを追加する必要があります。Security Manager にはデバイスを追加するいくつかの方式が用意されています。方式には、ネットワーク経由（ライブ デバイス）、別の Security Manager サーバまたは CiscoWorks Common Services Device Credential Repository（DCR）からエクスポートされたインベントリ ファイル経由、Cisco Security Monitoring, Analysis and Response System（CS-MARS）形式のインベントリ ファイル経由、またはデバイス設定ファイル経由があります。Security Manager でデバイスを作成すると、ネットワークにはまだ存在しないが、配置する予定のあるデバイスを追加することもできます。

デバイスを追加した場合は、そのデバイスのインターフェイスと、すでに設定されている特定のポリシーも検出できます。検出された情報は Security Manager データベースに登録され、それ以降も Security Manager によって継続的に管理できます。

詳細については、デバイス インベントリの管理を参照してください。

ステップ 3 **セキュリティ ポリシーを定義します。**

デバイスの追加が完了すると、必要なセキュリティ ポリシーを定義できます。個々のデバイスのポリシーの定義には、デバイス ビューを使用できます。任意の数のデバイスで共有できる、再利用可能なポリシーの作成および管理には、ポリシー ビューを使用できます。共有ポリシーに変更を加えると、そのポリシーが割り当てられているすべてのデバイスに変更が適用されます。

ポリシー定義を簡素化して時間を短縮するために、ポリシー オブジェクトを使用できます。これは、特定の値に名前を付けて再利用可能としたオブジェクトです。オブジェクトを定義すると、複数のポリシーからそのオブジェクトを参照できるため、ポリシーごとに値を個別に定義する必要がなくなります。

（注） Workflowモードを使用している場合は、アクティビティを作成してからポリシーを定義する必要があります。詳細については、ワークフローおよびアクティビティの概要 （26 ページ）を参照してください。

ステップ 4 ポリシー定義を送信して展開します。

ポリシー定義はユーザの専用ビュー内で行われます。ユーザが定義を送信するまで、定義はデータベースに登録されず、他のSecurity Managerユーザがその定義を確認することもできません。ポリシー定義を送信する場合は、その整合性が検証されます。エラーまたは警告があればそれらが表示され、ポリシーをデバイスに展開する前に対処しておく必要のある問題が通知されます。

Security Managerではポリシー定義に従ってCLIコマンドが生成され、すばやく簡単に定義をデバイスに展開できます。セキュアな接続を経由してネットワーク内のライブデバイス（動的にアドレス指定されたデバイスを含む）に直接展開するか、またはファイルに展開していつでもデバイスに転送できます。

Workflow 以外のモードでは、1 回のアクションで変更の送信と展開を実行できます。Workflow モードでは、最初にアクティビティを送信してから、変更を展開する展開ジョブを作成します。

詳細については、展開の管理を参照してください。

ポリシーおよびポリシー オブジェクトの概要

ポリシーとは、ネットワークの特定の設定項目を定義した一連のルールまたはパラメータのことです。Configuration Manager では、デバイスに必要なセキュリティ機能を指定するポリシーを定義します。定義されたポリシーは、関連デバイスに展開可能なCLIコマンドに変換されます。

Security Manager を使用すると、ローカル ポリシーおよび共有ポリシーを設定できます。

- **ローカル ポリシー**は、設定したデバイス限定のポリシーです。このポリシーを設定すると、デバイスに自動的に割り当てられます（適用されます）。未設定ポリシー（デフォルト設定を変更していないポリシー）は、割り当て済みまたは設定済みとは見なされません。ポリシーを削除するには、その割り当てを解除します。
- **共有ポリシー**は、名前が付けられた再利用可能なポリシーであり、一度に複数のデバイスに割り当てることができます。共有ポリシーを変更すると、変更したポリシーが割り当てられているすべてのデバイスに変更が反映されます。このため、デバイスごとに変更を行う必要がありません。

インベントリにデバイスを追加すると、そのデバイスに設定されている既存のポリシーを検出できるようになります。Security Manager はデバイス設定を Security Manager ポリシーに変換し、関連するローカル ポリシーに値を読み込んでデバイスにポリシーを割り当てます。**ポリシー検出**を使用することにより、Security Manager の観点で既存の設定を作成し直す必要がなくなります。CLI を使用して設定を変更した場合は、インベントリにポリシーを追加したあとに再検出することもできます。

多くの場合、ポリシーを作成するときに**ポリシーオブジェクト**を使用できます。ポリシーオブジェクトとは、関連する値のセットを再利用可能な形で定義したものです。（場合によって

は、ポリシーオブジェクトを使用する必要があります。）たとえば、ネットワークの一連のIPアドレスが含まれる、MyNetworkというネットワークオブジェクトを定義できます。これらのアドレスを必要とするポリシーを設定するときは、常にMyNetworkネットワーク オブジェクトを参照するだけで済み、毎回手動でアドレスを入力する必要がありません。さらに、集中管理する場所でポリシーオブジェクトを変更でき、この変更は、オブジェクトを参照しているすべてのポリシーに反映されます。

詳細については、ポリシーの管理およびポリシー オブジェクトの管理を参照してください。

ワークフローおよびアクティビティの概要

柔軟性のあるセキュアなポリシー管理を提供する一方、組織が変更制御プロセスを実行できるようにするために、Security Managerには、Configuration Managerに密接に関連する3つの機能が用意されています。

- [Workflowモード（Workflow Mode）]/[Workflow以外のモード（Non-Workflow Mode）]：Configuration Managerには、Workflowモードおよび Workflow以外のモード（デフォルト）の2つの動作モードがあり、さまざまな組織の作業環境に対応できます。
  - [Workflowモード（Workflow Mode）]：Workflowモードは、セキュリティポリシーを定義するユーザーと管理するユーザーで責務を分担している組織のためのモードです。明示的にアクティビティを作成し、そのコンテキスト内ですべてのポリシー設定を行うことにより、正式な変更追跡と管理のシステムが導入されます。単一のアクティビティには論理的に関連するポリシー変更だけを追加するために、ユーザは複数のアクティビティを作成できます。チェックなしで設定変更が行われないように、個別のアプルーバを必要とするようにWorkflowモードを設定できます。承認後、ユーザは別の展開ジョブを定義して、ポリシー変更をデバイスにプッシュします。詳細については、Workflow モードの作業 （27 ページ）を参照してください。
  - [Workflow以外のモード（Non-Workflow Mode）]：Workflow以外のモードでは、アクティビティを明示的には作成しません。ログインすると、Configuration Managerはアクティビティを作成するか、または以前に使用したアクティビティが送信されていない場合はそのアクティビティを開きます。ポリシーを定義して保存すれば、1回の手順でポリシーを送信して展開できます。詳細については、Workflow 以外のモードの作業 （28 ページ）を参照してください。

モードの選択の詳細については、ワークフロー モードの変更 （36 ページ）を参照してください。

- [アクティビティまたは設定セッション（Activities or Configuration Sessions）]：アクティビティ（Workflow以外のモードでは設定セッション）は、基本的にSecurity Managerデータベースの専用ビューです。Configuration Managerでは、アクティビティを使用して、ポリシーおよびポリシー割り当てに対して行われる変更を制御します。インベントリにデバイスを追加しても、アクティビティは含まれません。ただし、（マルチコンテキストのファイアウォールデバイスの）セキュリティコンテキストまたは（IPSデバイスの）仮想センサーを定義するポリシーを検出する場合は除きます。アクティビティからポリシー変更を分離すると、「処理中の作業」を誤ってアクティブデバイスの設定に送信することを防ぐ

のに役立ちます。アクティビティおよび設定セッションの詳細については、アクティビティについておよびアクティビティ/チケットの操作を参照してください。

- [チケット管理（Ticket Management）]：チケット管理により、チケット ID を Security Manager で行われたポリシー設定の変更に関連付けることができます。チケット管理は、Workflow モードが有効になっているかどうかに応じて、アクティビティまたは設定セッションと連動して機能します。Workflow モードが有効になっている場合は、チケット管理を有効にして、オプションでチケット ID を特定のアクティビティに関連付けることもできます。Workflow モードが有効になっていない場合、チケット管理を使用すると、すべての変更をチケットの一部として実行する必要があり、それらの変更を展開する前にチケットを送信する必要があります。この点で、ワークフローが無効な場合のチケット管理は、ワークフローが有効な場合のアクティビティの機能によく似ています。ただし、送信されたチケットの承認は必要ありません。

さまざまな動作モードの比較については、Workflow モードの比較 （29 ページ）を参照してください。

Workflow モードの作業

Workflow モードは、正式な変更追跡と管理のシステムを導入する高度な動作モードです。このモードは、ポリシーを定義する責務とデバイスにポリシーを展開する責務を、セキュリティ オペレータとネットワーク オペレータの間で分担している組織に適しています。たとえば、あるセキュリティ オペレータはデバイスでセキュリティ ポリシーの定義を担当し、別のセキュリティ オペレータはポリシー定義の承認を担当、およびネットワーク オペレータは承認された設定をデバイスに展開することを担当する場合があります。このように責務を分離すると、展開したデバイス設定の整合性を維持できます。

Workflowモードはアプルーバの有無に関係なく使用できます。アプルーバを設定してWorkflowモードを使用する場合、ユーザが実行したデバイス管理およびポリシー設定の変更は、別のユーザによる確認および承認を経て関連デバイスに展開されます。アプルーバを設定しないでWorkflowモードを使用する場合は、1人のユーザがデバイスおよびポリシー設定の変更を作成して承認できるため、変更プロセスが簡素化されます。

（注） Workflowモードは、チケット管理が有効か無効かに関係なく、同じように機能します。Workflowモードでチケット管理を有効にすると、アクティビティで使用する[チケット（Ticket）]フィールドが有効になります。チケット ID の入力は必須ではありませんが、使用する場合は、外部の変更管理システムにリンクするように[チケット（Ticket）]フィールドを設定できます。詳細については、「チケット管理」を参照してください。

Workflow モードの有効化または無効化、またはチケット管理の有効化または無効化については、ワークフロー モードの変更 （36 ページ）を参照してください。

ワークフロー モードで、次の手順を実行します。

- ユーザは、Configuration Manager でポリシー設定を定義または変更する前にアクティビティを作成する必要があります。アクティビティは、基本的には設定変更を行うためのプロ

ポーザルです。アクティビティ内で行われた変更は、適切な権限を持つユーザがアクティビティを承認したあとにだけ適用されます。アクティビティは、別のユーザーに送信して確認および承認することも、現在のユーザーが承認することもできます。アクティビティを作成、送信、および承認するプロセスの詳細については、アクティビティの管理を参照してください。

- アクティビティを承認したあとは、設定変更を関連デバイスに展開する必要があります。このとき、ユーザーは展開ジョブを作成します。展開ジョブには、設定の展開先デバイスおよび使用する展開方法を定義します。展開ジョブは、別のユーザーに送信して確認および承認することも、現在のユーザーが承認することもできます。展開プリファレンスは、ジョブ承認の有無に関係なく設定できます。詳細については、展開の管理を参照してください。

Workflow 以外のモードの作業

組織によっては、VPN ポリシーとファイアウォール ポリシーを定義および管理する場合に、ユーザ間で責務を分担しない場合があります。これらの組織は、Workflow 以外のモードで作業できます。Workflow 以外のモードを使用する場合は、アクティビティを明示的には作成しません。ログインしたときに、Configuration Managerによってアクティビティ（別名を設定セッションと呼びます）が作成されるか、または以前のログイン時に使用していたアクティビティが開きます（Security Manager をログアウトすると、設定セッションは自動的に閉じます）。このアクティビティはユーザに対して透過的であり、特に管理する必要はありません。設定変更をデータベースに送信した場合、これは Workflow モードにおけるアクティビティの送信および承認に相当します。また、設定変更を送信して展開すると、展開ジョブも作成されます。アクティビティと同様、展開ジョブも透過的であり、管理の必要はありません。

Workflow 以外のモードを使用している場合、同じユーザ名とパスワードを持つ複数のユーザが、同時に Security Manager にログインすることはできません。作業中に、同じユーザ名とパスワードを持つ別のユーザがログインすると、セッションが終了するため再度ログインする必要があります。

Workflow 以外のモードのチケット管理

組織が変更管理システムを使用している場合、Security Manager は、設定に加えられた変更をチケット ID に関連付けることができます。設定を変更する前に、チケットを開いて、チケットに関連付けられた変更を展開できるようにする前に、チケットを送信する必要があります。チケットは必要に応じて開いたり閉じたりでき、チケットに関連する変更が不要になった場合はチケットを破棄できます。チケット ID の入力は必須ではありませんが、使用する場合は、外部の変更管理システムにリンクするように[チケット（Ticket）]フィールドを設定できます。詳細については、「チケット管理」を参照してください。

チケット管理が有効になっている Workflow 以外のモードは、Security Manager のデフォルトモードです。Workflow モードの有効化または無効化、またはチケット管理の有効化または無効化については、ワークフロー モードの変更 （36 ページ）を参照してください。

Workflow モードの比較

次の表に、Workflow モード間の違いを示します。

（注） Workflowモードは、チケット管理が有効か無効かに関係なく、同じように機能します。Workflowモードでチケット管理を有効にすると、アクティビティで使用する[チケット（Ticket）]フィールドが有効になります。チケットIDの入力は必須ではありませんが、使用する場合は、外部の変更管理システムにリンクするように[チケット（Ticket）]フィールドを設定できます。詳細については、「チケット管理」を参照してください。

表 *1 : Configuration Manager* での *Workflow* モードと *Workflow* 以外のモードの比較

質問	チケット管理が有効になっている Workflow 以外のモード	チケット管理が無効になっている Workflow 以外のモード	Workflow モード
Security Manager のデフォルトモードはどれですか。	デフォルト	非デフォルト	非デフォルト。
現在選択されているモードを確認するにはどうすればよいですか。	**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [ワークフロー（Workflow）]** を選択します。[Workflowの有効化（Enable Workflow）]チェックボックスがオンになっている場合、Workflow モードです。 **[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [チケット管理（Ticket Management）]** を選択します。[チケットの有効化（Enable Ticketing）]チェックボックスをオンにすると、チケット管理が有効になります。		
設定を変更するためにアクティビティを明示的に作成する必要がありますか。	設定を変更する前に、明示的にチケットを作成する必要があります。Configuration Manager は、そのチケットに関連付けられたアクティビティを自動的に作成します。	いいえ。ログイン時に Configuration Manager によってアクティビティが自動的に作成されるか、またはログアウト前に以前のセッションを送信しなかった場合はそのセッションが開きます。	はい。
デバイスに設定を展開するために展開ジョブを明示的に作成する必要がありますか。	いいえ。設定変更を展開すると、Configuration Manager によって展開ジョブが作成されます。	いいえ。設定変更を展開すると、Configuration Manager によって展開ジョブが作成されます。	はい。

質問	チケット管理が有効になっている Workflow 以外のモード	チケット管理が無効になっている Workflow 以外のモード	Workflow モード
設定変更をデバイスに展開するにはどうすればよいですか。	次のいずれかを実行します。 • **[ファイル（File）] > [展開（Deploy）]** を選択します。 • **[管理（Manage）] > [展開（Deployments）]** を選択して、[展開ジョブ（Deployment Jobs）] タブで [展開（Deploy）] をクリックします。	次のいずれかを実行します。 • [メイン（Main）] ツールバーで**[変更の送信と展開（Submit and Deploy Changes）]** ボタンをクリックします。 • **[ファイル（File）] > [送信と展開（Submit and Deploy）]** を選択します。 • **[管理（Manage）] > [展開（Deployments）]** を選択して、[展開ジョブ（Deployment Jobs）] タブで [展開（Deploy）] をクリックします。	**[管理（Manage）] > [展開（Deployments）]** を選択して、展開ジョブを作成します。
設定変更用の CLI コマンドはどの段階で生成されますか。	展開の開始時。	展開の開始時。	展開ジョブの作成時。

質問	チケット管理が有効になっている Workflow 以外のモード	チケット管理が無効になっている Workflow 以外のモード	Workflow モード
現在の変更を削除するにはどうすればよいですか。	**[チケット（Tickets）] > [チケットの破棄（Discard Ticket）]** を選択して、現在開いているチケットを破棄するか、Ticket Manager でチケットを選択して [破棄（Discard）] をクリックします。 デバイスの展開をすでに開始している場合は、Deployment Manager でジョブを選択して [中止（Abort）] をクリックし、展開を中止します。	**[ファイル（File）] > [破棄（Discard）]** の順に選択します。 デバイスの展開をすでに開始している場合は、Deployment Manager でジョブを選択して [中止（Abort）] をクリックし、展開を中止します。	**[アクティビティ（Activities）] > [アクティビティの破棄（Discard Activity）]** の順に選択して現在開いているアクティビティを破棄するか、または Activity Manager でアクティビティを選択して [破棄（Discard）] をクリックします。 展開ジョブを作成済みの場合は、Deployment Manager でジョブを選択して [破棄（Discard）] をクリックします。ジョブを展開済みの場合は、[中止（Abort）] を選択するとジョブを中断できます。
複数のユーザが同時に Security Manager にログインできますか。	はい。各ユーザーは異なるチケットを開き、設定変更ができます。一人のユーザーが複数回ログインできますが、ユーザーは別のチケットを開く必要があります。	はい。ただし、各ユーザのユーザ名が異なる場合だけです。同じユーザ名のユーザが Security Manager にログインすると、最初のユーザは自動的にログアウトされます。	はい。各ユーザは異なるアクティビティを開き、設定変更を行うことができます。単一のユーザが複数回ログインできますが、ユーザは別個のアクティビティを開く必要があります。
別のユーザが設定しているデバイスを設定するとどうなりますか。	デバイスがロックされていることを示すメッセージが表示されます。アクティビティとロッキング を参照してください。		

JumpStart を使用した Security Manager の理解

JumpStart は Security Manager を紹介する手引きです。製品の使用にかかわる主な概念の説明が記載されています。Security Manager の機能を試しに使用する場合は、JumpStart を使用してください。

JumpStart は、Security Manager を初めて起動したときに自動的に開きます。Security Manager の使用中に JumpStart を起動するには、Configuration Manager のメインメニューから **[ヘルプ（Help）] > [JumpStart]** の順に選択します。

JumpStart には、次のナビゲーション機能があります。

- コンテンツ テーブル。常に右上隅に表示されます。ページを開くにはエントリをクリックします。
- ページ内のリンク。JumpStart 内の詳細情報およびオンライン ヘルプ内の関連情報にドリルダウンできます。

Security Manager の初期設定の実行

Security Manager をインストールしたら、いくつかの設定手順を実行してインストールを完了します。初期設定するほとんどの機能にはデフォルト設定がありますが、機能をよく理解して、デフォルト設定が組織に最適な設定かどうかを判断する必要があります。

次に、初期設定が必要な機能のリストを示します。示されている詳細情報の参照先も参照してください。これらの機能は任意の順序で設定できます。また、まだ使用する必要のない機能の設定は、後回しにすることもできます。

- SMTP サーバおよびデフォルト電子メール アドレスを設定します。Security Manager では、システム内で行われたさまざまなアクションに対して、電子メール通知を送信できます。たとえば、展開ジョブによるネットワーク デバイスの再設定が完了すると、電子メールを受信します。電子メール通知が動作するためには、SMTP サーバを設定する必要があります。

SMTP サーバーおよびデフォルト電子メールアドレスの設定の詳細については、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 （34 ページ）を参照してください。

- ユーザ アカウントを作成します。ユーザが製品を使用する場合は、Security Manager にログインする必要があります。ただし、別のユーザがすでに使用しているアカウントを使用してログインすると、最初のユーザは自動的に切断されます。したがって、ユーザごとに一意のアカウントを設定する必要があります。Security Manager サーバにローカルなアカウントを作成することも、ACS システムを使用してユーザ認証を管理することもできます。詳細については、*Cisco Security Manager インストレーションガイド* [英語] を参照してください。
- デフォルトの展開を設定します。ユーザは、デバイスに設定を展開するときに、設定の展開方法および Security Manager で異常を処理する方法を選択できます。ただし、システム

デフォルト設定を選択する方が、組織の推奨事項への準拠は容易になります。展開のデフォルト値を設定するには、Configuration Manager で [ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] の順に選択し、コンテンツテーブルから [展開（Deployment）] を選択して [展開（Deployment）] 設定ページを開きます（[Deployment] ページを参照）。

特に重要なのは、次の展開設定です。

- • デフォルトの展開方式：デバイスまたは転送サーバに設定の展開を直接書き込むか、または Security Manager サーバの指定したディレクトリに設定ファイルを書き込むかどうか。デフォルトでは、デバイスの設定が行われると、その設定はデバイスまたは転送サーバに直接展開されます。ただし、設定ファイルを展開する独自の方法があるときは、デフォルトの展開方式として [File] を選択する必要がある場合があります。展開方式の詳細については、展開方法についてを参照してください。

  • アウトオブバンド変更の検出時：Security Manager ではなく CLI を使用してデバイスの設定変更が行われたとき、そのことを Security Manager で検出した場合の対処方法。デフォルトでは、警告が発行されて展開が続行し、CLI を介して行われた変更が上書きされます。ただし、この動作は、単に変更チェックをスキップする（つまり、Security Manager は変更を上書きするが警告は行わない）か、または展開をキャンセルしてデバイスを現在の状態にしておくように変更できます。アウトオブバンド変更を処理する方法の詳細については、アウトオブバンド変更の処理方法についてを参照してください。

  • エラー時のダウンロード許可：軽微な設定エラーが検出された場合に、展開の継続を許可するかどうか。デフォルトでは、軽微なエラーが検出された場合は展開を許可しません。

- ワークフローモードを選択します。デフォルトのモードは、チケット管理が有効になっている Workflow 以外のモードです。Workflow 以外のモードでは、設定を作成および展開するときのユーザの自由度が高くなります。ただし、ネットワーク管理に対してトランザクション指向の強い方法を必要とする組織で、別々のユーザがポリシーの作成、承認、および展開を実行する場合は、Workflow モードをイネーブルにすると独自の手順を実行できます。Workflow モードを使用する場合は、必要な作業を分担するためのユーザ アカウントを定義するとき、ユーザ権限を正しく設定します。使用できるワークフロータイプの詳細については、ワークフローおよびアクティビティの概要 （26 ページ）を参照してください。ワークフロー モードを変更する方法の詳細については、ワークフロー モードの変更 （36 ページ）を参照してください。

ヒント Workflow 以外のモードでチケット管理を無効にすると、ほとんどのアクティビティ管理タスクを自動化できます。

- デフォルトのデバイス通信を設定します。デバイスのタイプに基づいてデバイスにアクセスする場合、Security Manager は最も一般的に利用される方式を使用します。たとえば、Security Manager が Catalyst スイッチに接続する場合、デフォルトでは SSH を使用します。

デフォルトのプロトコルが大部分のデバイスで動作する場合は、プロトコルを変更する必要はありません。デフォルト以外のプロトコルを使用するデバイスの場合は、個々のデバイスのデバイス プロパティでプロトコルを変更できます。ただし、Security Manager のデフォルトではないプロトコルを常に使用する場合（たとえば、ルータに Token Management Server（TMS）を使用する場合など）、デフォルト設定を変更する必要があります。デフォルトの通信設定を変更するには、Configuration Manager で [ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] の順に選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します。[Device Connection Settings] グループで、デバイスのタイプごとに最適なプロトコルを選択します。デフォルトの接続タイムアウトおよび再試行の設定を変更することもできます。デバイスの通信設定の詳細については、[Device Communication] ページを参照してください。

- Security Manager で管理するルータ ポリシーおよびファイアウォール ポリシーのタイプを選択します。Security Manager で IPS デバイスを管理すると、必然的に設定全体を管理することになります。ただし、ルータおよびファイアウォール デバイス（ASA、PIX、および FWSM）の場合は、Security Manager で管理するポリシーのタイプを選択できます。その他の部分のデバイス設定は、他のツール（デバイスの CLI を含む）を使用して管理できます。デフォルトでは、すべてのセキュリティ関連のポリシーが管理対象です。管理するポリシーを変更するには、Configuration Manager で [ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [ポリシー管理（Policy Management）] の順に選択します。これらの設定を変更する方法および変更の前後に実行する作業の詳細については、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。
- ファイアウォール イベントおよび IPS イベントの管理に Event Viewer を使用するかどうかを決定します。デバイスから Syslog イベントを収集するためのディスクと場所、および Syslog 通信に使用するポート番号を設定できます。イベント管理に Security Manager を使用しない場合は、この機能をオフにできます（デフォルトではイネーブル）。設定オプションの詳細については、[Event Management] ページを参照してください。
- Cisco Security Monitoring, Analysis and Response System（CS-MARS）と通信するために Security Manager を設定します。CS-MARS を使用してネットワークをモニタする場合は、サーバを識別して Security Manager に登録すると、Security Manager から CS-MARS イベント情報にアクセスできます。この相互通信を設定する方法の詳細については、CS-MARS と Security Manager を統合するためのチェックリストを参照してください。

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

Security Manager では、展開ジョブの完了、アクティビティの承認、または ACL ルールの期限切れなど、さまざまなタイプのイベントの発生時に電子メール通知を送信できます。電子メール通知をイネーブルにするには、Security Manager で電子メールの送信に使用できる SMTP サーバを設定する必要があります。その後、次の設定ページで電子メールアドレスおよび通知の設定を行うことができます（Configuration Manager で [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] の順に選択し、コンテンツテーブルからページを選択します）。

- [Workflow] ページ：展開ジョブとアクティビティ用のデフォルト電子メールアドレスおよび通知設定の場合。展開ジョブおよびアクティビティを管理する場合にデフォルト値を上書きできます。
- [Rules Expiration] ページ：ACL ルールの期限切れに対するデフォルト電子メール アドレスおよび通知設定の場合。ルールが期限切れになるのは、有効期限を設定した場合だけです。
- [IPS Updates] ページ：IPS Update のアベイラビリティを通知する電子メール アドレスの場合。
- [サーバーセキュリティ（Server Security）] ページ：ローカルユーザアカウントを設定するときに（[ローカルユーザ設定（Local User Setup）] をクリック）、ユーザの電子メールアドレスを指定する場合。このアドレスは、展開ジョブの完了などを通知する場合のデフォルト ターゲットとして使用されます。
- [Event Management] ページ：拡張データ ストレージの場所を設定する場合は、少なくとも 1 つの電子メールアドレスを指定する必要があります。電子メールアドレスは、拡張保管場所の使用で問題が発生した場合に通知を受信します。また、Syslog リレーサービスを使用している場合は、syslog リレーサービスが CPU スロットリングを出入りするときに通知される電子メールアドレスを設定できます。

ヒント ユーザ認可に ACS を使用している場合は、ACS 統合手順で、SMTP サーバーおよびシステム管理者の電子メールアドレスを設定済みである必要があります（『Installation Guide for Cisco Security Manager』を参照）。すべての ACS サーバが利用不能な状態になると、Security Manager はこのアドレスに通知を送信します。

（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。

ステップ 1 Security Manager サーバで CiscoWorks Common Services にアクセスします。

- Security Manager クライアントを使用中の場合、最も簡単にアクセスするには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] の順に選択し、コンテンツテーブルから [サーバーセキュリティ（Server Security）] を選択して、そのページのいずれかのボタンをクリックします（[ローカルユーザ設定（Local User Setup）] など）。
- Web ブラウザを使用して Security Manager サーバーのホームページ（https://*servername* /CSCOnm/servlet/login/login.jsp）にログインし、[サーバー管理（Server Administration）] をクリックします。

ステップ 2 [サーバー（Server）] > [管理（Admin）] の順にクリックして、コンテンツテーブルから [システム設定（System Preferences）] を選択します。

ステップ 3 [System Preferences] ページで、Security Manager が使用できる SMTP サーバのホスト名または IP アドレスを入力します。SMTP サーバが電子メール メッセージを送信する場合に、ユーザ認証は必要ありません。セキュア SMTP 統合は、CSM ではサポートされていません。

また、CiscoWorks が電子メールの送信に使用できる電子メール アドレスを入力します。このアドレスは、Security Manager から送信される通知用に設定した電子メール アドレスと同じである必要はありません。ACS を使用して認可を行っている場合は、すべての ACS サーバが利用不能な状態になると、Security Manager はこのアドレスに電子メール メッセージを送信します。このメッセージにより、早急な対応を必要とする問題に対して警告を出すことができます。管理者は、ACS に関連しないイベントについて、Common Services から電子メール メッセージを受け取る場合もあります。

ステップ 4 [Apply] をクリックして変更内容を保存します。

ワークフロー モードの変更

適切な管理者権限がある場合は、Security Manager で実行されるワークフロー モードを変更できます。ワークフローモードを変更すると、ユーザには大きな影響があります。変更を行う場合は、次の点を考慮してください。

- ワークフロー モードを変更すると、同じサーバを使用しているすべての Security Manager ユーザに対して、変更が有効となります。
- Workflow モードから Workflow 以外のモードに変更する場合は、編集可能状態（Edit、Edit Open、Submit、または Submit Open）にあるアクティビティをすべて承認または廃棄し、生成済みのジョブをすべて展開、拒否、廃棄、または中断して、デバイスのロックを解放する必要があります。エラー状態にあるジョブに対しては、何も行う必要はありません。
- Workflow 以外のモードでチケット管理を無効にする前に、編集可能な状態（[編集（Edit）] または [編集オープン（Edit Open）]）になっているすべてのチケットを送信または破棄する必要があります。
- Workflow モードから Workflow 以外のモードに変更したあとに、以前のバージョンのデータベースを復元した場合は、復元されたデータベースに編集可能状態（Edit、Edit Open、Submit、または Submit Open）のアクティビティが存在すると、Security Manager は自動的に Workflow モードに切り替わります。編集可能なアクティビティを承認または削除してから、Workflow モードを再度オフにします。
- Workflow 以外のモードから Workflow モードに変更した場合、または Workflow 以外のモードでチケット管理を有効にした場合、現在の設定セッションは Edit_Open 状態のアクティビティ/チケットとして一覧に表示されるため、これらのアクティビティ/チケットは明示的に管理する必要があります。
- チケット管理が有効または無効になっている場合、Cisco Security Manager にログインしている他のユーザーはすべてログアウトされます。

ワークフローモードの説明については、ワークフローおよびアクティビティの概要 （26 ページ）を参照してください。

ステップ 1 Configuration Manager で **[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** の順に選択し、目次から [ワークフロー（Workflow）] を選択して [ワークフロー（Workflow）] ページを開きます（[Workflow] ページを参照）。

ステップ 2 [Workflow Control] グループでワークフロー モード設定を行います。[Enable Workflow] をオンにして Workflow モードを使用する場合は、次のオプションを選択することもできます。

- [Require Activity Approval]：ポリシー変更をデータベースにコミットする前に、アクティビティの明示的な承認を実行します。
- [送信者がアクティビティを承認可能（Submitter can Approve Activity）]：送信者は、送信ロールと承認ロールを分離する代わりに、自分のアクティビティも承認できます（有効になっている場合）。
- [Require Deployment Approval]：展開ジョブを実行する前に、ジョブの明示的な承認を実行します。
- [送信者が展開ジョブを承認可能（Submitter can Approve Deployment Job）]：有効にすると、送信者は自分が送信した展開ジョブを承認できます。

ステップ 3 電子メール通知設定を行います。ここで設定するのは、電子メール送信者（つまり Security Manager）、アプルーバ、および展開ジョブの完了時に通知が必要な別のユーザまたは電子メール エイリアスのデフォルト電子メール アドレスです。

ジョブ ステータスの通知を送信するときにジョブ展開者を含めたり、展開ジョブのステータスが変更された場合に電子メール通知を送信するように設定することもできます。

ステップ 4 [保存（Save）] をクリックして、変更を保存および適用します。

ステップ 5 目次から [ワークフロー（Workflow）] を選択して、[チケット管理（Ticket Management）] ページを開きます（[Token Management] ページを参照）。

ステップ 6 [チケット管理（Ticket Management）] 設定を設定します。[チケットの有効化（Enable Ticketing）] を選択すると、次のオプションも選択できます。

（注） これらのフィールドの詳細については、[Token Management] ページを参照してください。

- [チケットシステムURL（Ticket System URL）]：チケット ID と外部チケット管理システム間のリンクを提供します。
- [チケット履歴（Ticket History）]：チケットに関連する情報を保持する期間を指定します。

ステップ 7 [保存（Save）] をクリックして、変更を保存および適用します。

Security Manager インターフェイスの基本機能について

ここでは、メニュー コマンドの説明、ツールバーのボタン、およびユーザ インターフェイスの共通要素の使用方法など、基本的なインターフェイス機能について説明します。説明されている機能の多くは、Configuration Manager だけで使用されます。

- Configuration Manager のメニュー バー リファレンス （38 ページ）

Configuration Manager のメニュー バー リファレンス

Configuration Manager のメニュー バーには、Security Manager を使用するためのコマンドを含むメニューがあります。コマンドは、実行中のタスクに応じて利用不能な状態になる場合があります。

ここでは、メニュー バーに含まれるメニュー項目について説明します。

[File] メニュー（Configuration Manager）

次の表に、Configuration Manager の [File] メニューのコマンドを示します。メニュー項目は、ワークフロー モードによって異なります。

表 *2 : [File]* メニュー（*Configuration Manager*）

コマンド	説明
新規デバイス（New Device）	新しいデバイスを追加するウィザードを開始します。デバイス インベントリへのデバイスの追加を参照してください。
Clone Device	既存のデバイスを複製してデバイスを作成します。デバイスの複製を参照してください
デバイスの削除	デバイスを削除します。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。
保存	アクティブなページで行われた変更を保存します。ただし、Security Manager データベースには変更を送信しません。
インポート	別の Security Manager サーバからエクスポートされたポリシーとデバイスをインポートします。ポリシーまたはデバイスのインポートを参照してください。
エクスポート	ポリシーまたはデバイスをエクスポートして、別の Security Manager サーバにインポートできるようにします。デバイスのエクスポートはポリシー情報を含んでいるか、CiscoWorks Common Services Device Credential Repository（DCR）または Cisco Security Monitoring, Analysis and Response System（CS-MARS）にインポートできる単純な CSV ファイルです。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および共有ポリシーのエクスポートを参照してください。
変更の表示 （Workflow 以外のモードのみ）	現在の設定セッションのアクティビティ変更レポート（PDF 形式）を開きます。 Workflow モードで現在のアクティビティの変更を確認するには、**[アクティビティ（Activities）] > [変更の表示（View Changes）]** の順に選択します。
検証（Validate） （Workflow 以外のモードのみ）	保存済みの変更を検証します。アクティビティ/チケットの検証を参照してください。 Workflow モードで現在のアクティビティを検証するには、**[アクティビティ（Activities）] > [アクティビティの検証（Validate Activity）]** の順に選択します。
送信 （Workflow 以外のモードのみ）	Security Manager データベースに最後に送信したあとに行われた変更をすべて送信します。 Workflow モードで現在のアクティビティを検証するには、**[アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）]** の順に選択します。

コマンド	説明
Submit and Deploy （Workflow 以外のモードのみ）	Security Manager データベースに最後に送信したあとに行われた変更をすべて送信し、最後に展開したあとに行われた変更をすべて展開します。展開についてを参照してください。 Workflow モードでは、アクティビティが承認され、デバイスへの変更を展開する展開ジョブを作成する必要があります。
[展開（Deploy）] （Workflow 以外のモードのみ）	最後の展開よりあとに行われた変更をすべて展開します。展開についてを参照してください。 Workflow モードでは、アクティビティが承認され、デバイスへの変更を展開する展開ジョブを作成する必要があります。
廃棄 （Workflow 以外のモードのみ）	最後の送信よりあとの設定変更をすべて廃棄します。 Workflow モードで現在のアクティビティを検証するには、**[アクティビティ（Activities）] > [アクティビティの破棄（Discard Activity）]** の順に選択します。
Edit Device Groups	デバイス グループを編集します。デバイス グループの使用を参照してください。
New Device Group	デバイス グループを追加します。デバイス グループの作成を参照してください。
グループへのデバイスの追加	グループにデバイスを追加します。デバイス グループに対するデバイスの追加と削除を参照してください。
印刷（Print）	アクティブなページを印刷します。 印刷できるのは一部のページだけです。[Print] コマンドが使用不能になっている場合は、アクティブなページを印刷できません。
終了（Exit）	Security Manager を終了します。

[Edit] メニュー（Configuration Manager）

次の表に、Configuration Manager の [Edit] メニューのコマンドを示します。通常、これらのコマンドを使用できるのは、ポリシー内のテーブルを操作している場合、およびルールテーブルに関する作業を行っている場合だけです（ルール テーブルの使用を参照）。

表 3 : [Edit] メニュー（Configuration Manager）

コマンド	説明
切り取り（Cut）	ルールテーブルで選択した行をカットして、クリップボードに保存します。

コマンド	説明
コピー（Copy）	ルールテーブルで選択した行をコピーして、クリップボードに保存します。
貼り付け	ルールテーブルで選択した行のあとに、クリップボードからルール テーブルの行をペーストします。
行を追加（Add Row）	アクティブなテーブルに行を追加します。
Edit Row	選択したテーブル行を編集します。
Delete Row	選択したテーブル行を削除します。
Move Row Up Move Row Down	選択した行をルール テーブル内で上下に移動します。詳細については、ルールの移動とルール順序の重要性を参照してください。
[グローバル検索（Global Search）]	[グローバル検索（Global Search）] ウィンドウが開きます。詳細については、 グローバル検索の使用 （55 ページ）を参照してください。

[View] メニュー（Configuration Manager）

Configuration Manager の [View] メニューには、ユーザ インターフェイス内をナビゲートするか、ツールバーを変更するためのコマンドがあります。

表 4 : [View] メニュー

メニュー コマンド	説明
デバイス ビュー	デバイス ビューを開きます。 デバイス ビューの概要 （20 ページ）を参照してください。
デバイスステータスビュー（Device Status View）	[デバイスステータスビュー（Device Status View）] ウィンドウを開きます。[デバイスステータスビュー（Device Status View）] の使用を参照してください。
Map View	マップ ビューを開きます。 マップ ビューの概要 （23 ページ）を参照してください。
Policy View	ポリシー ビューを開きます。 ポリシー ビューの概要 （22 ページ）を参照してください。
ポリシーバンドルビュー（Policy Bundle View）	ポリシーバンドルビューを開きます。XREFを参照してください。

メニュー コマンド	説明
Customized Toolbar	ツールバーで一部のオプションのボタンを追加または削除できます。ツールバーに表示できるすべてのボタンについては、ツールバー リファレンス（Configuration Manager） （51 ページ）を参照してください。

[Policy] メニュー（Configuration Manager）

Configuration Manager の [Policy] メニューには、ポリシーを管理するためのコマンドがあります。

表 5 : [Policy] メニュー（*Configuration Manager*）

メニュー コマンド	説明
Share Policy	アクティブなローカル ポリシーを共有ポリシーとして保存します。ローカル ポリシーの共有を参照してください。
Unshare Policy	アクティブな共有ポリシーをローカル ポリシーとして保存します。ポリシーの共有解除を参照してください。
Assign Shared Policy	デバイスに共有ポリシーを割り当てます。デバイスまたは VPN トポロジへの共有ポリシーの割り当てを参照してください。
Unassign Policy	選択したデバイスから現在のポリシーの割り当てを解除します。ポリシーの割り当て解除を参照してください。
Copy Policies Between Devices	デバイス間でポリシーをコピーします。デバイス間でのポリシーのコピーを参照してください
Share Device Polices	ローカル デバイス ポリシーを共有できるようにします。ローカル ポリシーの共有を参照してください。
Edit Policy Assignments	デバイスに対する共有ポリシーの割り当てを編集します。ポリシー ビューにおけるポリシー割り当ての変更を参照してください。
ポリシーの複製	新しい名前でポリシーのコピーを作成します。共有ポリシーのクローニング（コピー）を参照してください。
Rename Policy	共有ポリシー名の変更
Add Local Rules	デバイスの共有ポリシーにローカル ルールを追加します。このコマンドを使用するには、ルールベースの共有ポリシーを選択する必要があります。
Inherit Rules	ポリシーの継承を編集します。ルールの継承または継承の解除を参照してください。

メニュー コマンド	説明
Discover Policies on Device	デバイス上のポリシーを検出します。ポリシーの検出を参照してください。
Discover VPN Policies	Discover VPN Policies ウィザードを開きます。サイト間 VPN ディスカバリ を参照してください。

[Map] メニュー（Configuration Manager）

Configuration Manager の [Map] メニューには、マップ ビューを使用するためのコマンドがあります。このメニューのコマンドを使用できるのは、マップ ビューが開いている場合だけです。詳細については、マップ ビューの使用を参照してください。

表 6 : [Map] メニュー（Configuration Manager）

メニュー コマンド	説明
New Map	マップを作成します。新しいマップまたはデフォルト マップの作成を参照してください。
Open Map	保存済みのマップまたはデフォルト マップを開きます。マップを開くを参照してください。
Show Devices On Map	アクティブなマップ上に表示する管理対象デバイスを選択します。マップでの管理対象デバイスの表示を参照してください。
Show VPNs On Map	アクティブなマップ上に表示する VPN を選択します。マップにおける既存 VPN の表示を参照してください。
Add Map Object	開いたマップ上にマップ オブジェクトを作成します。ネットワーク トポロジを表すマップ オブジェクトの使用方法を参照してください。
Add Link	開いたマップ上にレイヤ 3 リンクを作成します。マップにおけるレイヤ 3 リンクの追加と管理を参照してください。
Find Map Node	開いたマップ上のノードを検索します。マップ ノードの検索を参照してください。
Save Map	開いたマップを保存します。マップの保存を参照してください。
Save Map As	開いたマップに新しい名前を付けて保存します。マップの保存を参照してください。
拡大（Zoom In）	マップをズームインします。マップのパン、中央への配置、およびズームを参照してください。

メニュー コマンド	説明
縮小（Zoom Out）	マップをズームアウトします。マップのパン、中央への配置、およびズームを参照してください。
ウィンドウに合わせる	開いたマップをズームしてマップ全体を表示します。マップのパン、中央への配置、およびズームを参照してください。
Display Actual Size	開いたマップをズームして実際のサイズを表示します。マップのパン、中央への配置、およびズームを参照してください。
Refresh Map	更新されたネットワーク データを使用して、開いたマップをリフレッシュします。新しいマップまたはデフォルト マップの作成を参照してください。
Export Map	開いたマップをファイルにエクスポートします。マップのエクスポートを参照してください。
マップの削除	選択したマップをリストから削除します。マップの削除を参照してください。
マップのプロパティ	開いたマップのプロパティを表示または編集します。マップの背景プロパティの設定を参照してください。
Show/Hide Navigation Window	開いたマップのナビゲーション ウィンドウの表示/非表示を切り替えます。ナビゲーション ウィンドウの使用方法を参照してください。
Undock/Dock Map View	マップのウィンドウを切り離して、マップを開いたままで他の機能を使用できるようにします。すでにウィンドウが切り離されている場合は、[Dock Map View] コマンドを選択すると、Security Manager のメイン ウィンドウに再度固定されます。マップ ビューのメイン ページについて を参照してください。

[Manage] メニュー（Configuration Manager）

Configuration Manager の [Manage] メニューには、Security Manager のメイン インターフェイスとは独立したウィンドウで実行されるツールを起動するコマンドがあります。このメニューを使用すると、現在使用中のページを閉じることなく、さまざまな機能にアクセスできます。

表 *7 : [Manage]* メニュー（*Configuration Manager*）

メニュー コマンド	説明
ポリシー オブジェクト	Policy Object Manager を開きます。このツールでは、使用可能なすべてのオブジェクトを、オブジェクト タイプに従ってグループ化して表示できます。また、オブジェクトを作成、コピー、編集、および削除できるほか、使用状況レポートを生成できます。使用状況レポートには、選択したオブジェクトが、他の Security Manager オブジェクトおよびポリシーからどのように使用されているかが記述されます。詳細については、Policy Object Managerを参照してください。
Site-to-Site VPNs	Site-to-Site VPN Manager を開きます。このツールでは、サイト間 VPN を設定できます。サイト間 VPN の管理：基本を参照してください。
アクティビティ （Workflow モード限定）	Activity Manager を開きます。このツールでは、アクティビティを作成および管理できます。アクティビティ/チケット マネージャ ウィンドウを参照してください。
展開（Deployments）	Deployment Manager を開きます。このツールでは、設定の展開および展開ジョブの管理を実行できます。展開の管理を参照してください
設定アーカイブ（Configuration Archive）	デバイス設定のアーカイブされたバージョンを格納し、設定の表示と比較、およびある設定から別の設定へのロールバックを実行できます。[Configuration Archive] ウィンドウを参照してください。
Policy Discovery Status	[Policy Discovery Status] ウィンドウを開きます。このウィンドウでは、ポリシー検出およびデバイス インポートのステータスを確認できます。ポリシー検出タスクのステータスの表示を参照してください。
IPS	デバイスの通信に必要な IPS デバイス証明書を管理します。
Audit Report	監査レポート ページに設定されたパラメータに従って、監査レポートを生成します。[Audit Report] ウィンドウの使用を参照してください。
Change Reports （Workflow 以外のモードのみ）	デバイスに対する変更、共有ポリシー、および以前の設定セッションのポリシー オブジェクトに関するレポートを生成できます。変更レポートの表示を参照してください。 現在の設定セッション中に行われた変更を表示するには、[ファイル（**File**）] > **[変更の表示（View Changes）]** を選択します。]

[Tools] メニュー（Configuration Manager）

に

[Device Properties] ウィンドウを開きます。このウィンドウには、デバイス、クレデンシャル、デバイスの割り当て先グループ、およびポリシーオブジェクトの上書きに関する一般情報が表示されます。詳細については、デバイス プロパティについてを参照してください。

Configuration Manager の [ols] メニューには、Security Manager のメインインターフェイスとは独立したウィンドウで実行されるツールを起動するコマンドがあります。このメニューを使用すると、現在使用中のページを閉じることなく、さまざまな機能にアクセスできます。

表 *8 : [Tools] メニュー（Configuration Manager）*

メニュー コマンド	説明
デバイス プロパティ	
Detect Out of Band Changes	デバイスを分析して、最後に Security Manager が設定を展開してから設定が変更されたかどうかを判別します。この情報を使用して、重要な設定変更が失われないようにできます。アウトオブバンド変更の検出および分析を参照してください。
Packet Capture Wizard	ASA デバイスでパケットの取り込みを設定できる Packet Capture Wizard を開きます。
Ping, TraceRoute and NSLookup	これらのトラブルシューティング コマンドを使用できる ping、TraceRoute、および NSLookup ツールを開きます。ping と TraceRoute は管理対象デバイスで稼働しますが、NSLookup はクライアント ワークステーションで稼働します。ping、トレースルート、または NS ルックアップツールを使用した接続問題の分析を参照してください。
IPインテリジェンス（IP Intelligence）	IP インテリジェンスツールを開きます。ここから、完全修飾ドメイン名（FQDN）、地理的位置情報、WHOIS 情報など、IPv4 アドレスに関するさまざまな情報にアクセスできます。IP インテリジェンスツールの詳細については、IPインテリジェンス（IP Intelligence）を参照してください。 IP インテリジェンス機能を使用する前に、[IP インテリジェンス設定（IP Intelligence Settings）] ページでこれらの機能を有効にして設定する必要があります ([IPインテリジェンス設定（IP Intelligence Settings）] ページを参照)。
壁面	同じ Security Manager サーバーにログインしているすべてのユーザにメッセージを送信できる [ウォール（Wall）] ウィンドウを開きます。ただし、最初に、[ウォール設定（Wall Settings）] ページで有効にする必要があります。[ウォール設定（Wall Settings）] ページを参照してください。

メニュー コマンド	説明
Show Containment	デバイスのセキュリティ コンテキストまたはサービス モジュールを表示します。デバイスに含まれている要素の表示を参照してください。
インベントリ ステータス	すべてのデバイスのデバイス概要情報を表示します。インベントリ ステータスの表示を参照してください。
Catalyst Summary Info	選択した Catalyst スイッチ上で Security Manager が検出したすべてのサービス モジュール、ポート、および VLAN を含む、システム情報の概要を表示します。Catalyst サマリー情報の表示を参照してください。
Apply IPS Update	IPS イメージおよびシグニチャの更新を手動で適用します。IPS 更新の手動適用を参照してください。
Preview Configuration	特定のデバイスの提示された変更、最後に展開された設定、または現在実行中の設定を表示します。設定のプレビューを参照してください。
バックアップ	CiscoWorks Common Services を使用して、Security Manager データベースをバックアップします。Security Manager データベースのバックアップおよび復元を参照してください。
Security Manager Diagnostics	Technical Assistance Center（TAC）からの要求に応じて送信するトラブルシューティング情報を収集します。Cisco Technical Assistance Center 用の診断ファイルの作成を参照してください。 ヒント　Cisco Security Manager バージョン 4.7 以降では、既存の [一般的な診断（General Diagnostics）] の代わりに [ライト診断（Light Diagnostics）] を選択できます。
Security Manager Administration	Security Manager の機能を制御する、システム全体の設定を行います。

[Activities] メニュー（Configuration Manager）

Configuration Manager の [Activities] メニューには、アクティビティを管理するためのコマンドがあります。このメニューは、Workflow モードがイネーブルの場合だけ表示されます。これらのコマンドの詳細については、Workflow モードでのアクティビティ機能へのアクセスを参照してください。

表 *9 : [Activities]* メニュー（*Configuration Manager*）

メニューコマンド	説明
New Activity	新しいアクティビティを作成します。アクティビティ/チケットの作成を参照してください。
Open Activity	アクティビティを開きます。アクティビティ/チケットを開くを参照してください。
Close Activity	開いているアクティビティを閉じます。アクティビティ/チケットを閉じるを参照してください。
変更の表示	アクティビティ変更レポート（PDF形式）を開きます。変更レポートの表示を参照してください。
Validate Activity	開いているアクティビティを検証します。アクティビティ/チケットの検証を参照してください。
Submit Activity	開いているアクティビティを送信します。承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード）を参照してください。
Approve Activity	開いているアクティビティを承認します。アクティビティの承認または拒否（Workflow モード）を参照してください。
Reject Activity	開いているアクティビティを拒否します。アクティビティの承認または拒否（Workflow モード）を参照してください。
Discard Activity	開いているアクティビティを廃棄します。アクティビティ/チケットの破棄 を参照してください。

Tickets Menu（Configuration Manager）

Configuration Manager の [チケット（Tickets）] メニューには、チケットを管理するためのコマンドが含まれています。Workflow 以外のモードでチケット管理が有効になっている場合にのみ表示されます。これらのコマンドの詳細については、Workflow モードでのアクティビティ機能へのアクセスを参照してください。

表 *10 : Tickets Menu*（*Configuration Manager*）

メニュー コマンド	説明
新しいチケット（New Ticket）	新しいチケットを作成します。アクティビティ/チケットの作成を参照してください。
チケットを開く（Open Ticket）	チケットを開きます。アクティビティ/チケットを開くを参照してください。

メニュー コマンド	説明
チケットを閉じる（Close Ticket）	オープンチケットを閉じます。アクティビティ/チケットを閉じるを参照してください。
変更の表示	チケット変更レポート（PDF 形式）を開きます。変更レポートの表示を参照してください。
チケットの検証（Validate Ticket）	オープンチケットを検証します。アクティビティ/チケットの検証を参照してください。
チケットの送信（Submit Ticket）	オープンチケットを送信します。アクティビティ/チケットの状態についてを参照してください。
チケットを破棄（Discard Ticket）	オープンチケットを破棄します。アクティビティ/チケットの検証 を参照してください。

[Launch] メニュー（Configuration Manager）

[Launch] メニューには、他のアプリケーションを起動するコマンドがあります。

表 *11 : [Launch] メニュー（Configuration Manager）*

メニューコマンド	説明
Device Manager	PIX セキュリティ アプライアンス、Firewall Services Module（FWSM; ファイアウォール サービス モジュール）、IPS センサー、IOS ルータ、および Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスなど、サポート対象のすべてのデバイスに関するデバイス マネージャを起動します。デバイス マネージャには、いくつかのモニタリング機能および診断機能があります。この機能を使用すると、デバイスで実行されているサービスに関する情報、およびシステム全体のヘルスのスナップショットを取得できます。デバイス マネージャの起動を参照してください。
Prime Security Manager	ASA CX デバイスの管理に使用される Cisco Prime Security Manager（PRSM）アプリケーションを起動します。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動を参照してください。
FireSight Management Center	FirePOWER モジュールの管理に使用される FireSIGHT Management Center アプリケーションを起動します。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動を参照してください。

メニューコマンド	説明
ダッシュボード	ダッシュボードが開きます。このダッシュボードは、IPS と FW タスクをより便利にする Security Manager で設定可能な起動点です。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Security Manager の他のいくつかの領域にある、IPS Health Monitor ページ、Report Manager、Health and Performance Monitor および IP Intelligence 設定などの多くのタクスを 1 箇所で実行できます。ダッシュボードの詳細については、ダッシュボードの概要を参照してください。
イベントビューア	Event Viewer を開きます。このツールでは、デバイス イベントを表示および分析できます。詳細については、イベントの表示を参照してください。 すでに別の Security Manager アプリケーションにログインしている場合は、同じユーザーアカウントを使用してイベントビューアが開きます。別のユーザーアカウントを使用してイベントビューアを開くには、Windows のスタートメニューまたはデスクトップアイコンからアプリケーションを開きます。
Report Manager	セキュリティ レポートと使用状況レポートを生成して分析できる Report Manager を開きます。詳細については、レポートの管理を参照してください。 すでに別の Security Manager アプリケーションにログインしている場合は、同じユーザーアカウントを使用して Report Manager が開きます。別のユーザーアカウントを使用して Report Manager を開くには、Windows のスタートメニューまたはデスクトップアイコンからアプリケーションを開きます。
Image Manager	ASA デバイスのイメージを管理できる Image Manager を開きます。詳細については、Image Manager の使用を参照してください。 すでに別の Security Manager アプリケーションにログインしている場合は、同じユーザーアカウントを使用して Image Manager が開きます。別のユーザーアカウントを使用して Image Manager を開くには、Windows のスタートメニューまたはデスクトップアイコンからアプリケーションを開きます。
Health and Performance Monitor	Health and Performance Monitor（HPM）を開きます。ここでは、ネットワーク全体のデバイスステータスとトラフィック情報を表示したり、デバイス固有のアラートを表示して確認したりできます。詳細については、ヘルスとパフォーマンスのモニタリングを参照してください。 すでに別の Security Manager アプリケーションにログインしている場合は、同じユーザーアカウントを使用して HPM が開きます。別のユーザーアカウントを使用して HPM を開くには、Windows のスタートメニューまたはデスクトップアイコンからアプリケーションを開きます。

[Help] メニュー（Configuration Manager）

Configuration Manager の [Help] メニューには、製品マニュアルおよびトレーニングにアクセスするためのコマンドがあります。詳細については、オンライン ヘルプの利用方法 （69 ページ）を参照してください。

表 12 : [Help] メニュー（Configuration Manager）

メニュー コマンド	説明
ヘルプ トピック （Help Topics）	オンライン ヘルプ システムを開きます。
Help About This Page	アクティブなページのオンライン ヘルプを開きます。
JumpStart	JumpStart を開きます。
Security Manager Online	Cisco.com の Security Manager Web ページを開きます。
About Configuration Manager	Configuration Manager に関する情報を表示します。

ツールバー リファレンス（Configuration Manager）

メインツールバーには、Configuration Manager のアクションを実行するボタンがあります。

メインツールバーに表示されるボタンは、Workflow/チケット管理モードが有効かどうか、およびツールバーをカスタマイズした方法によって異なります。選択すると、ツールバーに含まれているいくつかのボタンを選択できます。多数のボタンは永続的にツールバーに存在し、削除できません。

次の表に、すべてのボタンを示します。

表 13 : Configuration Manager ツールバー

ボタン	説明
	デバイス ビューを開きます。 詳細については、デバイス ビューについてを参照してください。
	マップ ビューを開きます。 詳細については、マップ ビューの使用を参照してください。
	ポリシー ビューを開きます。 詳細については、ポリシー ビューにおける共有ポリシーの管理を参照してください。
	ポリシーバンドルウィンドウを開きます。 詳細については、ポリシーバンドルの管理を参照してください。

ボタン	説明
	Policy Object Manager を開きます。 詳細については、ポリシー オブジェクトの管理を参照してください。
	Site-to-Site VPN Manager を開きます。 詳細については、サイト間 VPN の管理：基本を参照してください。
	Deployment Manager を開きます。 詳細については、展開の管理を参照してください。
	Audit Report を開きます。 詳細については、監査レポートについてを参照してください。
	（チケット管理が無効になっている Workflow 以外モードのみ。）変更を送信および展開します。 詳細については、展開の管理を参照してください。
	現在選択されているデバイスで定義されている設定ポリシーを検出します。 詳細については、ポリシーの検出を参照してください。
	現在選択されているデバイスのアウトオブバンド変更（Security Managerの外部のデバイスに対して行った変更）を検出します。 詳細については、アウトオブバンド変更の検出および分析を参照してください。
	IP インテリジェンスツールを開きます。ここから、完全修飾ドメイン名（FQDN）、地理的位置情報、WHOIS 情報など、IPv4 アドレスに関するさまざまな情報にアクセスできます。IP インテリジェンスツールの詳細については、IPインテリジェンス（IP Intelligence）を参照してください。 IP インテリジェンス機能を使用する前に、[IP インテリジェンス設定（IP Intelligence Settings）] ページでこれらの機能を有効にして設定する必要があります ([IPインテリジェンス設定（IP Intelligence Settings）] ページを参照)。
	同じ Security Manager サーバーにログインしているすべてのユーザにメッセージを送信できる [ウォール（Wall）] ウィンドウを開きます。ただし、最初に、[ウォール設定（Wall Settings）] ページで有効にする必要があります。 詳細については、[Workflow] ページを参照してください。

ボタン	説明
	選択した Catalyst スイッチ上で Security Manager が検出したすべてのサービス モジュール、ポート、および VLAN を含む、システム情報の概要を表示します。 詳細については、Catalyst サマリー情報の表示を参照してください。
	現在選択されているデバイスの設定をプレビューします。 詳細については、設定のプレビューを参照してください。
	Security Manager の機能を制御する、システム全体の設定を行います。詳細については、Security Manager の管理設定値の設定を参照してください。
	現在選択されているデバイスのデバイス マネージャを開きます。 詳細については、デバイス マネージャの起動を参照してください。
	ASA CX デバイスの管理に使用される Cisco Prime Security Manager（PRSM）アプリケーションを起動します。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動を参照してください。
	FirePOWER モジュールの管理に使用される FireSIGHT Management Center アプリケーションを起動します。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動を参照してください。
	ダッシュボード アプリケーションを開きます。 詳細については、ダッシュボードの概要を参照してください。
	Event Viewer アプリケーションを開きます。 詳細については、イベントの表示を参照してください。
	Report Manager アプリケーションを開きます。 詳細については、レポートの管理を参照してください。
	Image Manager アプリケーションを開きます。 詳細については、Image Manager の使用を参照してください。
	ヘルスとパフォーマンスのモニターアプリケーションを開きます。 詳細については、ヘルスとパフォーマンスのモニタリングを参照してください。
	現在のページのオンライン ヘルプを開きます。 詳細については、 オンライン ヘルプの利用方法 （69 ページ） を参照してください。

ボタン	説明
（注）	チケット管理が無効になっている場合、Workflow 以外のモードでは次のボタンを使用できません。
	Workflow モードで [Activity Manager] ウィンドウを開くか、または Workflow 以外モードでチケット管理が有効になっている場合は、[Ticket Manager] ウィンドウを開きます。これらのウィンドウを使用して、アクティビティ/チケットを作成および管理できます。詳細については、アクティビティ/チケット マネージャ ウィンドウを参照してください。 [アクティビティ（activity）] ボタン、およびこれらのボタンが有効になる条件の詳細については、Workflow モードでのアクティビティ機能へのアクセスを参照してください。 [チケット（ticket）] ボタン、およびこれらのボタンが有効になる条件の詳細については、Workflow 以外のモードでのチケット機能へのアクセスを参照してください。
	新しいアクティビティ/チケットを作成します。
	アクティビティ/チケットを開きます。
	アクティビティ/チケットが開いている間に行われた変更をすべて保存して閉じます。
	アクティビティ/チケットで行われたすべての変更を評価し、PDF 形式の変更レポートを別のウィンドウ内に生成します。詳細については、変更レポートの表示を参照してください。
	現在のアクティビティ/チケット内で変更されたポリシーの整合性を検証します。
	（承認者のWorkflow モードのみ。) アクティビティ承認者がいる Workflow モードを使用している場合、承認のためにアクティビティを送信します。 （チケット管理が有効になっている Workflow 以外モードのみ。）チケットを送信します。チケットを送信すると、提案された変更がデータベースに保存されます。チケットに関連付けられたデバイスはロック解除されるため、ポリシー定義に含めたり、他のチケットで変更したりできます。チケットは、[編集（Edit）] 状態または [編集オープン（Edit Open）] 状態にある場合に送信できます。
	（Workflow モード限定）アクティビティ内で提案された変更を承認します。
	（Workflow モード限定）アクティビティ内で提案された変更を拒否します。

ボタン	説明
	選択したアクティビティ/チケットを破棄します。

グローバル検索の使用

Security Manager には、関心のある情報を簡単に見つけて操作するためのグローバル検索機能が用意されています。グローバル検索機能を使用すると、特定の検索文字列を含むデバイス、ポリシーオブジェクト、ポリシー、およびチケットを検索できます。検索の範囲は、デバイス、ポリシーオブジェクト、ポリシー、またはチケットのみに制限できます。

（注） 検索は、コミットされたデータを使用してのみ実行されます。データベースにまだ送信されていない変更は、検索結果に含まれません。

ワイルドカード照合

検索文字列では、次のワイルドカード文字の使用がサポートされています。

- **アスタリスク（*）**：0 個以上の文字と一致します
- **疑問符（?）**は、任意の 1 文字に一致します

セマンティック検索

入力された検索文字列が IP アドレスの場合、Security Manager はセマンティック検索を実行します。たとえば、検索文字列に「192.168.0.0/16」と入力すると、そのサブネットに一致するアイテムに加え、そのサブネットに属する、またはそのサブネットが属する特定のホストまたは他のサブネットが返されます。

グローバル検索範囲

グローバル検索は、すべてではなく、一連のポリシーおよびポリシーオブジェクト内でのみサポートされます。サポートされているポリシーとポリシーオブジェクトは、お客様導入事例で最も頻繁に使用されるポリシーとオブジェクトです。サポートされているポリシーとポリシーオブジェクトは次のとおりです。

- デバイス：すべてのデバイス
- ポリシーオブジェクト：
  - AAA サーバグループ
  - AAAサーバ
  - アクセス コントロール リスト
  - As Path Policies

- ASA グループポリシー
- BFD テンプレート（BFD Template）
- カテゴリ
- Cisco Secure Desktop（ルータ）
- コミュニティリストポリシー
- 資格情報
- DHCPv6 プール
- ファイルオブジェクト
- FlexConfig
- アイデンティティ ユーザー グループ
- IKE プロポーザル
- Interface Roles
- IPsec トランスフォームセット
- LDAP 属性マップ
- ネットワーク/ホスト（IPv4 および IPv6）
- PKI 登録
- ポリシーリストポリシー
- Port Forwarding List
- プレフィックス リスト ポリシー
- ルートリストポリシー
- サービス
- シングルサインオンサーバー
- SLA モニター
- SSL VPN ブックマーク
- SSL VPN カスタマイズ
- SSL VPN ゲートウェイ
- SSL VPN スマートトンネル自動サインオンリスト
- SSL VPN スマートトンネル
- テキスト オブジェクト

- 時間範囲
- トラフィック フロー
- ユーザー グループ
- WINS サーバーリスト

- ポリシー：
  - AAA ルール
  - アクセル ルール
  - IPv6 アクセスルール
  - インスペクション ルール
  - 変換ルール
  - Web フィルタ ルール
  - ゾーンベースのファイアウォールルール

- チケット
  - 設定マネージャ（Configuration Manager）
  - Image Manager

グローバル検索の実行

グローバル検索を実行するには、次のいずれかを実行します。

- [編集（Edit）]>[グローバル検索（Global Search）] を選択するか、Ctrl+F を押して [グローバル検索（Global Search）] ウィンドウを開きます。[検索（search）] フィールドの左側にあるドロップダウンリストで検索の範囲を選択し、[検索（search）] フィールドに検索文字列を入力して、[検索（Search）] をクリックします。

（注） 現在 [ルールテーブル（rule table）]を表示している場合、**Ctrl+F** を押すと、[グローバル検索（Global Search）] ウィンドウではなく、[検索と置換（Find and Replace）] ダイアログボックスが開きます。検索と置換機能の代わりに、他の方法のいずれかを使用して、グローバル検索機能にアクセスします。

- [設定マネージャ（Configuration Manager）] ウィンドウの右上隅にある [検索（search）] フィールドを使用し、[検索（Search)] アイコンをクリックして検索の範囲を選択し、 [検索（search）] フィールドに検索文字列を入力して、**Enter** キーを押します。

[グローバル検索（Global Search）] ウィンドウには、検索条件に一致する結果が表示されます。カテゴリセレクタツリーから目的のデータタイプを選択して、そのカテゴリの結果を表示します。

検索結果への対応

検索から返されたアイテムに対して、次のアクションを実行できます。

- **データのエクスポート（すべて）**：選択したカテゴリの検索結果をCSV形式でエクスポートできます。[グローバル検索（Global Search）] ウィンドウのカテゴリセレクタツリーから目的のデータタイプを選択して、そのカテゴリの結果を表示し、検索結果の上にあるツールバーの [エクスポート（Export）] をクリックして、そのデータのテーブルを CSV 形式でエクスポートします。
- **印刷（すべて）**：選択したカテゴリの検索結果を印刷できます。[グローバル検索（Global Search）] ウィンドウのカテゴリセレクタツリーから目的のデータタイプを選択して、そのカテゴリの結果を表示し、検索結果の上にあるツールバーの [印刷（Print）] をクリックして、そのデータのテーブルを印刷します。
- **デバイスプロパティ（デバイス）**：検索結果で返されたデバイスのデバイスプロパティを表示できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のデバイスグループを選択して、そのカテゴリの結果を表示します。[結果（results] テーブルでデバイスを選択して強調表示し、デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。選択したデバイスの [デバイスプロパティ（Device Properties）] ダイアログ ボックスが表示されます。詳細については、デバイス プロパティの表示または変更を参照してください。
- **移動（ポリシー）**：検索結果からポリシーに移動できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のポリシータイプを選択して、そのポリシータイプの結果を表示します。[結果（results] テーブルでアイテムを選択して強調表示し、アイテムを右クリックして、[移動（Go To）] を選択します。選択したアイテムに関連するポリシーが表示されます。
- **フィルタ（ポリシー）**：標準のテーブルフィルタを使用して検索結果をフィルタ処理できます。詳細については、テーブルのフィルタリング （64 ページ）を参照してください。
- **表示（ポリシーオブジェクト）**：検索結果のオブジェクトのポリシーオブジェクトの詳細を表示できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のポリシーオブジェクトタイプを選択して、そのオブジェクトタイプの結果を表示します。[結果（results）] テーブルでオブジェクトを選択して強調表示し、検索結果の上にあるツールバーで [表示（View）] をクリックします（または、オブジェクトを右クリックして [表示（View）] を選択します)。選択したポリシーオブジェクトに関連する [編集（Edit）] ダイアログボックスが読み取り専用モードで表示されます。
- **編集（ポリシーオブジェクト）**：検索結果からポリシーオブジェクトを編集できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のポリシーオブジェクトタイプを選択して、そのオブジェクトタイプの結果を表示します。[結果（results）] テーブルでオブジェクトを選択して強調表示し、検索結果の上にあるツールバーで [編集（Edit）] をクリックします（または、オブジェクトを右クリックして [編集

（Edit）] を選択します)。選択したポリシーオブジェクトに関連する [編集（Edit）] ダイアログボックスが表示されます。

（注） チケットまたはアクティビティが現在開かれていない場合、ポリシーオブジェクトを編集する前に、チケットまたはアクティビティを作成するか、既存のものを開くように求められます。

- **使用状況の検索（ポリシーオブジェクト）**：検索結果で、オブジェクトを使用しているポリシー、オブジェクト、VPN、およびデバイスを見つけることができます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のポリシーオブジェクトタイプを選択して、そのオブジェクトタイプの結果を表示します。[結果（results）] テーブルでオブジェクトを選択して強調表示し、検索結果の上にあるツールバーで [使用状況の検索（Find Usage）] をクリックします（または、オブジェクトを右クリックして [使用状況の検索（Find Usage）] を選択します)。選択したポリシーオブジェクトの [オブジェクトの使用状況（Object Usage）] ダイアログボックスが表示されます。詳細については、オブジェクト使用状況レポートの生成を参照してください。
- **チケットの表示（チケット）**：検索結果で返されたチケットの[チケットマネージャ（Ticket Manager）] ウィンドウに移動できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のチケットグループを選択して、そのカテゴリの結果を表示します。表示するチケットの [結果（results）] テーブルの [チケット（Ticket）] 列をクリックします。選択したチケットが強調表示された状態で、[チケットマネージャ（Ticket Manager）] ウィンドウが表示されます。詳細については、アクティビティ/チケット マネージャ ウィンドウを参照してください。

セレクタの使用

セレクタは、ユーザインターフェイスのさまざまな場所に表示されます。たとえば、デバイスビューのデバイスセレクタなどがあります（図 1-1 を参照）。これらのツリー構造を使用すると、アクションを実行する（デバイスなどの）項目を選択できます。セレクタには、実行しているタスクに応じていくつかのタイプの項目が表示されます。

セレクタの項目は、フォルダの階層に表示されます。セレクタ内の項目を参照するには、フォルダを展開および縮小します。フォルダには、他のフォルダ、項目、またはフォルダと項目の組み合わせを格納できます。フォルダを展開および縮小するには、フォルダの横にある [+] または [-] をクリックします。

項目を選択するには、その項目をクリックします。（デバイスセレクタなどで）複数の項目に対してアクションを実行できる場合は、Ctrl を押しながら項目をクリックして 1 つ 1 つ項目を選択するか、または Shift を押しながら項目範囲の最初と最後の項目をクリックして、範囲内の項目をすべて選択できます。多くのセレクタでは自動選択をサポートしています。つまり、文字を 1 文字入力すると、その文字で始まる次のフォルダまたは項目がセレクタ内で選択されます。

項目を右クリックすると、その項目で使用できるコマンドが表示されます。右クリック メニューのコマンドには固有のコマンドもあり、その場合は通常のメニューに表示されません。

多くの場合、ダイアログボックスに表示されるデバイス セレクタは、[Available Devices] および [Selected Devices] の 2 つのペインに分割されています。これらのダイアログボックスでは、使用可能デバイスのリストでデバイスを選択し、[>>] をクリックして選択済みリストにデバイスを移動して、デバイスを実際に選択する必要があります。デバイスの選択を解除するには、選択済みデバイス リストでデバイスを選択し、[<<] をクリックします。

セレクタに多数の項目が含まれている場合は、項目をフィルタリングして一部の項目を表示できます。詳細については、セレクタ内の項目のフィルタリング （60 ページ）を参照してください。

セレクタ内の項目のフィルタリング

セレクタに含まれる項目の一部を表示するには、指定した基準に一致する項目だけを表示するフィルタを作成します。セレクタごとに、ユーザ 1 人につき最大 10 個のフィルタを作成できます。そのあとにフィルタをもう 1 個作成すると、最も古いフィルタが新しいフィルタで置き換えられます。作成したフィルタの重複チェックは行われません。フィルタは手動では削除できません。

フィルタ リストは、フィルタリング可能なすべてのセレクタの上部に表示されます。このリストから、次の動作を行うことができます。

- 以前作成したフィルタを選択する。
- [なし（None）] を選択して、フィルタを適用せずにツリーを表示する。
- [フィルタの作成（Create Filter）] を選択してフィルタを作成する。

各フィルタには、複数のフィルタ ルールを含めることができます。各フィルタ ルールには、ルール タイプ、基準、および値を指定します。セレクタに表示されるときに、項目が一部または全部のフィルタ ルールに一致する必要があるかどうかを選択します。

フィルタを作成してフィルタリングできるフィールドは、フィルタに表示される項目のタイプによって異なります。ただし、一般的な手順は、どのセレクタの場合でも同じです。

テーブルのフィルタリングの詳細については、テーブルのフィルタリング （64 ページ）を参照してください。

ヒント セレクタをフィルタリングすると、そのセレクタが含まれる別のウィンドウを開いたとき、セレクタにフィルタが適用されている場合があります。たとえば、デバイス ビューでデバイス セレクタにフィルタを適用すると、New Device ウィザードを開いた場合に、セレクタにフィルタが適用されています。セレクタで項目が見つからない場合は、[Filter] フィールドをオンにして、フィルタが適用されているかどうかを確認してください。

ステップ 1 [セレクタフィルタ（selector filter）] フィールドから [フィルタの作成（Create Filter）] を選択して、[フィルタの作成（Create Filter）] ダイアログボックスを開きます。

ステップ 2 次のオプション ボタンのいずれかを選択して、一致基準を決定します。次の選択項目があります。

- [Match Any of the Following]：フィルタ基準の間に OR 関係を作成します。基準のいずれかに一致するポリシーがフィルタに追加されます。
- [Match All of the Following]：フィルタ基準の間に AND 関係を作成します。すべての基準に一致するポリシーだけがフィルタに追加されます。

ステップ 3 次のように、3 つの基準を入力してフィルタ ルールを設定します。

- 最初のリストから、フィルタリングするタイプを選択します（*Name* など）。
- 次のリストから、フィルタの動作基準を選択します（*contains* など）。
- 最後のフィールドで、フィルタする値を入力または選択します（*Cisco* など）。

ステップ 4 [追加（Add）] をクリックします。

ヒント フィルタルールを作成するときに誤りがあった場合は、ルールを選択して [削除（Remove）] をクリックし、ルールを削除してください。

ステップ 5 必要なフィルタ ルールをさらに追加します。作業が完了したら [OK] をクリックします。

新しいフィルタ基準に従ってセレクタがフィルタリングされ、新しいフィルタがフィルタ リストに追加されます。

[Create Filter] ダイアログボックス

セレクタまたはテーブル内のサブセット項目をフィルタリングおよび表示するには、[Create Filter] ダイアログボックスを使用します。フィルタを作成すると、大きなリストを表示する場合に項目の検索が容易になります。

フィルタリングの詳細については、次の項を参照してください。

- セレクタ内の項目のフィルタリング （60 ページ）
- テーブルのフィルタリング （64 ページ）

ナビゲーション パス

次のいずれかを実行します。

- セレクタツリーの [フィルタ（Filter）] フィールドから [フィルタの作成（Create Filter）] を選択します。
- テーブルの上にある [フィルタ（Filter）] フィールドから [高度なフィルタ（Advanced Filter）] を選択します。

フィールド リファレンス

表 *14 : [Create Filter]* ダイアログボックス

要素	説明
Match All of the Following	このオプションを選択すると、定義したフィルタリング基準間に AND 関係が作成されます。項目がリストに表示されるには、その項目がフィルタのすべてのルールに一致する必要があります。 たとえば、次の基準を定義する場合があります。 • 名前に OSPF が含まれる • 名前に West が含まれる [OK] をクリックすると、フィルタが Name contains OSPF および Name contains West と定義されます。
Match Any of the Following	このオプションを選択すると、定義したフィルタリング基準間に OR 関係が作成されます。項目がリストに表示されるには、その項目がフィルタのルールのいずれか1つに一致する必要があります。 たとえば、次の基準を定義する場合があります。 • 名前に OSPF が含まれる • 名前に RIP が含まれる [OK] をクリックすると、フィルタが Name contains OSPF または Name contains RIP と定義されます。
Filter Type （最初のフィールド）	フィルタリングするプロパティのタイプ。テーブルのカラム見出しに相当します。特定のリストでは、フィルタリングするオプションが1つだけの場合もあります（たとえば、フィルタリングできるのが項目の名前だけの場合など）。
Filter Operator （2 番めのフィールド）	フィルタ タイプとフィルタ値の関係。使用できるオプションは選択したタイプによって異なります。
Filter Value （3 番めのフィールド）	フィルタリングする値。選択したタイプに応じて、このフィールドにはテキスト文字列を入力するか、またはリストから値を選択します。
Filter Content Area [追加（Add）] ボタン [Remove] ボタン	各基準に対して選択したフィルタ タイプ、演算子、および値。 • 基準を追加するには、この領域の上にあるフィールドで基準を作成し、[追加（Add）] をクリックします。 • 基準を削除するには、基準を選択し、[削除（Remove）] をクリックします。

ウィザードの使用

Security Manager を使用して実行できるタスクには、ウィザード形式のタスクもあります。ウィザードは、タスクを実行できる一連のダイアログボックス（または手順）のことです。ウィザードのタイトルバーには、現在の手順の番号およびそのウィザードに含まれる手順の合計数が表示されます。

次のボタンは、各ウィザードに共通です。

- [戻る（Back）]：前のダイアログボックスに戻ります。ウィザードの前の手順で定義した設定を確認および変更できます。
- [次へ（Next）]：次のダイアログボックスに進みます。 このボタンを使用できない場合は、現在のダイアログボックスで、次に進むための必須の設定を定義する必要があります。必須の設定には、アスタリスク（*）のマークが付いています。
- [終了（Finish）]：ウィザードを終了して、定義した設定を保存します。 このボタンが使用可能な場合は、いつでもウィザードを終了できます。このボタンを使用できない場合は、定義する設定が残っています。
- [キャンセル（Cancel）]：設定を保存しないでウィザードを閉じます。
- [ヘルプ（Help）]：ウィザードのオンラインヘルプを開きます。

テーブルの使用

Security Manager の多くのポリシーでは、テーブルを使用します。少数ですが、ルール テーブルと呼ばれる特別なタイプのテーブルを使用するポリシーもあります。標準テーブルと比較すると、ルール テーブルには追加機能が用意されています。詳細については、ルール テーブルの使用を参照してください。

標準テーブルの基本機能は、次のとおりです。

- テーブル フィルタ：行をフィルタリングして表示し、大きいテーブルで項目を検索しやすくします。詳細については、テーブルのフィルタリング （64 ページ）を参照してください。
- テーブルのカラム見出し：カラムによるソート、カラムの移動、カラムの表示/非表示の切り替えを実行できます。詳細については、テーブル カラムおよびカラム見出しの機能（65 ページ）を参照してください。
- テーブルのボタン：テーブルの下にあるボタンは、次の手順を実行する場合に使用します。
  - [Add Row] ボタン（[+] アイコン）：テーブルに項目を追加するには、このボタンをクリックします。
  - [Edit Row] ボタン（鉛筆アイコン）：プロパティを編集するには、行を選択してこのボタンをクリックします。

- [Delete Row] ボタン（ゴミ箱アイコン）：テーブルから行を削除するには、行を選択してこのボタンをクリックします。

テーブルのフィルタリング

テーブル内の項目をフィルタリングすると、特定の基準を満たすサブセットを表示できます。テーブルをフィルタリングしてもテーブルの内容は変更されず、現在関心のあるエントリだけに注目できます。この機能は、テーブルに数百ものエントリがある場合に有効です。

テーブルをフィルタリングするには、テーブルの上にある [Filter] フィールドを使用します。これらのコントロールを使用すると、次の作業を実行できます。

- 簡単なフィルタリングを実行するには、フィルタリングする列の名前を選択し、検索する関係（「begins with」など）を選択して、目的のテキスト文字列を入力（場合によっては事前定義されたオプションのいずれかを選択）してから [適用（Apply）] をクリックします。

もう 1 回基準を選択して [Apply] をクリックすると、結果をフィルタリングできます。フィルタがまとめられ、すべての基準を満たす結果が表示されます。たとえば、最初に「Service begins with IP」と入力して [適用（Apply）] をクリックしたあと、「Source contains 10.100.10.10」と入力して [適用（Apply）] をクリックしたとします。結果のテーブルには、サービスが IP かつ送信元に 10.100.10.10 が含まれるすべての行が表示されます（他の IP アドレスが含まれる場合もあります）。

- 高度なフィルタリングを実行するには、左端のメニュー（列の見出しを含むメニュー）から [高度なフィルタ（Advanced Filter）] を選択します。この操作によって [Create Filter] 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を使用すると、通常のフィルタコントロールを使用する場合と同様に、複数のフィルタ基準を作成できます。ただし、[次のいずれかと一致（Match Any of the Following）] を選択し、分割して論理和を取った基準のリストを作成することもできます。つまり、「サービスの IP または送信元アドレスが 10.100.10.10 であるすべての行を表示する」ことを指定できます。
  - 基準を追加するには、基準を入力して [追加（Add）] をクリックします。
  - 基準を削除するには、不要な基準を選択して [削除（Remove）] をクリックします。

簡単な方式を使用してテーブルをフィルタリングする場合も、[Advanced Filter] を選択すると、必要に応じて既存のフィルタを変更したり、基準を追加または削除できます。ダイアログボックスには、現在テーブルに適用されているフィルタ基準がすべて表示されます。

- 現在のフィルタは、フィルタ制御領域の [Filter] ラベルの横に表示されます。フィルタを削除してすべての行を表示するには、[クリア（Clear）] をクリックします。
- 適用するすべてのフィルタは、[Advanced Filter] エントリの下の左端のメニューに保持されます。フィルタを適用するには、リストからフィルタを選択します。ただし、このリストに登録できるエントリは最大 10 エントリです。11 番めのフィルタを作成すると、最も古いフィルタがリストから削除されます。フィルタを選択して基準を追加する場合は、新

しいフィルタの作成ではなくフィルタの変更になります。リストに表示されているフィルタは削除できません。

ヒント　別のデバイスを選択するか、ログアウトしてから再度ログインした場合でも、特定のタイプのテーブルに対して同じフィルタが維持されます。たとえば、あるデバイスの [アクセスルール（Access Rules）] テーブルをフィルタリングすると、他のデバイスも同じ方法でフィルタリングされます。フィルタをクリアすると、すべてのデバイスの同じタイプのテーブルのフィルタもクリアされます。フィルタは他のユーザの表示内容には影響しません。

テーブル カラムおよびカラム見出しの機能

テーブルにはカラムがあり、それぞれのカラムの見出し行にはカラム見出しがあります。これらのカラムおよびその見出しには、次のような機能があります。

- カラムの表示/非表示：テーブルの見出し行を右クリックしてコンテキスト メニューを開き、[Show Columns] を選択します。このメニューを使用すると、表示されるカラムを選択できます。カラムの表示または非表示は、テーブルに定義された項目の内容には影響せず、表示だけに影響します。

デフォルトでは、一部のポリシーのテーブルには、使用可能な一部のカラムだけが表示されます。

- [詳細の表示（Show Details）]/[サマリーの表示（Show Summary）]：テーブルの見出し行を右クリックしてコンテキストメニューを開き、[詳細の表示（Show Details）] または [サマリーの表示（Show Summary）] のいずれかを選択します。この切り替えメニューを使用すると、テーブルに詳細情報を表示するか概要情報を表示するかを選択できます。
- カラムの移動：カラム見出しをクリックしてドラッグし、新しい位置にカラムを移動します。
- カラムのサイズ変更：カラム見出しディバイダをクリックして（カーソルが矢印に変化したら）、ディバイダをドラッグしてカラムのサイズを変更します。
- カラム見出しによるソート：カラム見出しをクリックして、そのカラムの内容でテーブルをソートします。同じカラム見出しを再度クリックすると、ソート順序が逆になります。ソートされたカラムには、見出しの横に矢印が表示されます。

テキスト フィールドの使用方法

テキストフィールドには、そのフィールドの目的に応じて、1行を入力する場合または複数行を入力する場合があります。複数のテキスト行を入力できるテキストフィールドには、フィールドの使い勝手を向上させる機能がいくつか備わっています。ここでは、テキストフィールドの制限および機能に付いて説明します。

- テキストの ASCII 制限について　（66 ページ）

テキストの ASCII 制限について

通常、デバイスではテキストが ASCII 文字に制限されています。デバイス設定ファイルで、コマンドの生成に使用される Security Manager のテキスト フィールドに ASCII 文字以外の文字を入力すると、その文字が原因で設定ファイルがデバイスにロードされなくなる可能性があります。たとえば、FWSM のインターフェイスの説明に ASCII 文字以外の文字があると、デバイスを再起動したときに、そのデバイスのスタートアップ コンフィギュレーションがロードされないことがあります。

デバイス設定に ASCII 文字以外、英語以外の言語を入力できるのは、SSL VPN ブックマークおよび SSL VPN カスタマイゼーションのポリシー オブジェクトだけです。これらのポリシー オブジェクトは、ASA デバイスでブラウザベースのクライアントレス SSL VPN の設定に使用されます。これらのオブジェクトのローカル言語をサポートする方法の詳細については、ASA デバイスの SSL VPN Web ページのローカライズを参照してください。

テキスト ボックス内のテキストの検索

複数行テキスト フィールド内のテキストを検索するには、[Find] ダイアログボックスを使用します。

ステップ 1 複数行テキスト フィールドをクリックします。
ステップ 2 Ctrl+F を押します。[Find] ダイアログボックスが開きます。
ステップ 3 検索するテキストを [Find what] フィールドに入力します。
ステップ 4 検索の方向を指定するには、[方向（Direction）] フィールドで [上（Up）] または [下（Down）] のいずれかを選択します。
ステップ 5 入力したテキストの大文字と小文字を区別するには、[大文字と小文字を区別（Match Case）] チェックボックスをオンにします。
ステップ 6 [検索（Find）] をクリックします。次に出現する検索テキストが、テキスト フィールド内で強調表示されます。

テキスト ボックス内のナビゲート

複数行テキスト フィールドで特定の行にナビゲートするには、[Goto line] ダイアログボックスを使用します。

ステップ 1 複数行テキスト フィールドをクリックします。
ステップ 2 Ctrl+G を押します。[Goto line] ダイアログボックスが開きます。
ステップ 3 [Line number] フィールドに行番号を入力します。

ステップ 4 [OK] をクリック入力した行番号までテキスト フィールドがスクロールします。

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

Cisco Security Manager は標準的なファイル システム ブラウザを使用しており、ディレクトリまたはファイルを選択したり、ファイルを指定できます。

次のファイル操作を実行するときに、クライアント ファイル システムとサーバーファイルシステムを選択できます。

- Security Manager のライセンス ファイルのインストール
- デバイス インベントリ ファイルのインポート/エクスポート
- 共有ポリシーのインポート/エクスポート
- 次のファイル オブジェクトの作成
  - Cisco Secure Desktop Package
  - Plug-In：ブラウザ プラグイン ファイル用。
  - セキュアクライアント プロファイル
  - セキュアクライアント イメージ
  - Hostscan Image

他のすべてのファイル操作については、Security Manager サーバーでのみファイルを作成または選択できます。サーバーにマウントされたドライブは使用できず、クライアントシステムも使用できません。

ヒント Security Manager クライアントでファイル操作を許可するかどうかは、[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。

通常、ファイルを作成または選択するには、[参照（Browse）] ボタンをクリックして、実行するアクションに関連するタイトルのダイアログボックスを開きます（たとえば、設定ファイルの選択時は [ファイルの選択（Choose Files）]）。[Browse] ボタンは、製品全体でさまざまなダイアログボックスに表示されます。

目的のフォルダにナビゲートするには、このダイアログボックスの左側にあるフォルダ ツリーを使用します。

- クライアント側のファイルのブラウズがイネーブルのとき、クライアント側のブラウズをサポートしている機能（上記を参照）を実行する場合は、インポートまたはエクスポートするシステムに対応したタブを選択します。
- ファイルを選択する場合は、フォルダツリーでファイルを検索し、右側のペインで選択します。複数のファイルを選択できるアクションを実行している場合は、Ctrl を押しながらクリックしてファイルを個別に選択するか、または Shift を押しながらクリックしてファイルの範囲を選択します。ファイルタイプを選択して、アクションに適用されるファイルだけを表示することが必要な場合もあります。
- ファイルを指定（作成）する場合は、ファイルを作成するフォルダにナビゲートし、ファイル名を入力して、適切なファイル タイプを選択します。

（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。

ユーザインターフェイスに問題がある場合のトラブルシューティング

次のヒントを参照すると、ユーザインターフェイスに関する一般的な問題が発生した場合に、その問題の解決に役立つ場合があります。

- **インターフェイスがフリーズしたように見える**：Security Manager のダイアログボックスから他のアプリケーション（電子メールのチェックなど）に移動して Security Manager に戻ったときに、クリックしてもまったく応答がない場合があります。インターフェイスがフリーズしているように見えます。

これは、開いたダイアログボックスの上に別の Security Manager ウィンドウが重なっていることが原因の場合があります。このダイアログボックスを閉じるまで、アプリケーションの他のウィンドウは使用できません。隠れているダイアログボックスを見つけるには、Alt を押しながら Tab を押します。この操作によって、現在開いているすべてのウィンドウのアイコンが表示された Windows のパネルが開きます。Alt を押したまま Tab を何回か押し、適切なアイコンが見つかるまでアイコンを順に選択します（アイコンは Security Manager のアイコンではなく、一般的な Java のアイコンになっている場合があります）。Tab キーを使用してアイコンを順に選択するのではなく、マウスを使用して目的のアイコンをクリックすることもできます。

- **ボタンをクリックすると、テキストおよびリストの要素が見つからないという Java のエラーが発生する**：Security Manager クライアントの実行中に Windows のカラースキームを変更した場合は、クライアントを閉じて再起動する必要があります。再起動しないと、クライアントの動作を予測できなくなります。

カラースキームを変更していないのに、これらの問題が発生する場合も、アプリケーションを閉じて再起動する操作を試してください。

- **画面に対してダイアログボックスが大きすぎる**：実際には、多くのラップトップで対応している最適な画面解像度より、Security Manager クライアントの最小画面解像度の方が大きくなります（画面解像度の要件については、『Installation Guide for Cisco Security Manager』でクライアントのシステム要件を参照してください）。非常に大きなダイアログボックスもあるため、クライアントをラップトップで実行している場合は、ダイアログボックスが大きすぎて画面に収まりきらないことがあります。

通常は、ダイアログボックスの位置を変更すれば、[OK]、[Cancel]、および [Help] の各ボタンにアクセスできます。ただし、これらのボタンも画面に表示されない場合は、次の方法で同じアクションを実行できます。

- [OK]：フィールド内のカーソルをダイアログボックスの下部付近に置き、Tab を押してフィールド間を移動します。通常は、画面外の最初のフィールドが [OK] ボタンです。カーソルの強調表示が画面外に移動したら、Enter を押します。

復帰を使用できないフィールド（一般的には [Name] フィールドなど）にカーソルを置き、Enter を押すこともできます。多くの場合、これは [OK] のクリックに相当します。

- [キャンセル（Cancel）]：ウィンドウのタイトルバーの右側にある [X] をクリックします。
- [ヘルプ（Help）]：F1 を押します。

オンライン ヘルプの利用方法

Security Manager のオンライン ヘルプにアクセスするには、次のいずれかを実行します。

- Security Manager オンラインヘルプのメインページを開くには、[ヘルプ（Help）] > [ヘルプトピック（Help Topics）] の順に選択します。
- アクティブなページの状況依存オンラインヘルプを開くには、[ヘルプ（Help）] > [このページについてのヘルプ（Help About This Page）] の順に選択するか、またはツールバーで [?] をクリックします。
- ダイアログボックスの状況依存オンラインヘルプを開くには、ダイアログボックスの [ヘルプ（Help）] をクリックします。

ヒント オンライン ヘルプがブロックされずに開くようにするには、コンピュータでアクティブ コンテンツの実行を許可するように Internet Explorer を設定する必要があります。Internet Explorer で、[ツール（Tools）] > [インターネット オプション（Internet Options）] を選択し、[詳細設定（Advanced）] タブを選択します。[セキュリティ（Security）] セクションまでスクロールして、[マイコンピュータのファイルでのアクティブコンテンツの実行を許可する（Allow active content to run in files on My Computer）] を選択します。[OK] をクリックして変更を保存します。Internet Explorer および Firefox の各ブラウザでの設定要件の一覧については、『Installation Guide for Cisco Security Manager』を参照してください。

オンラインヘルプページは、ユーザー認証なしで表示されます。ヘルプページは直接 URL アクセスで開きますが、それらは静的コンテンツページに過ぎず、Cisco Security Manager 内で機能します。

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。