CSM 3.x：ユーザユーザ権限およびロールのセットアップ

内容

概要

このドキュメントでは、Cisco Security Manager（CSM）のユーザに権限とロールをセットアップする方法について説明します。

前提条件

要件

このドキュメントでは、CSMがインストールされ、正しく動作していることを前提としています。

使用するコンポーネント

このドキュメントの情報は、CSM 3.1に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ユーザ権限の設定

Cisco Security Managerは、ログインする前にユーザ名とパスワードを認証します。認証されると、Security Managerはアプリケーション内でユーザの役割を確立します。このロールは、権限（権限とも呼ばれる）を定義します。権限とは、実行を許可されているタスクまたは操作のセットです。特定のタスクまたはデバイスに対して権限がない場合、関連するメニュー項目、目次アイテム、およびボタンは非表示または無効になります。また、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権限がないというメッセージが表示されます。

Security Managerの認証と認可は、CiscoWorksサーバまたはCisco Secure Access Control Server(ACS)によって管理されます。 デフォルトでは、CiscoWorksは認証と認可を管理しますが、CiscoWorks Common Servicesの[AAA Mode Setup]ページを使用してCisco Secure ACSに変更できます。

Cisco Secure ACSを使用する主な利点は、特殊な権限セット（たとえば、特定のポリシータイプの設定が可能で、他のポリシータイプの設定は不可）を使用して詳細なユーザロールを作成し、ネットワークデバイスグループ(NDG)を設定することで制限できます。

次のトピックでは、ユーザ権限について説明します。

- セキュリティマネージャの権限
- CiscoWorksの役割について
- Cisco Secure ACSの役割について
- セキュリティマネージャの権限とロールのデフォルトの関連付け

セキュリティマネージャの権限

Security Managerは、次のように権限をカテゴリに分類します。

1. **View**：現在の設定を表示できます。詳細については、「権限の表示」を参照してください。
2. **Modify**：現在の設定を変更できます。詳細については、「権限の変更」を参照してください。
3. **割り当て**：デバイスおよびVPNトポロジにポリシーを割り当てることができます。詳細については、「権限の割り当て」を参照してください
4. **承認**：ポリシーの変更と導入ジョブを承認できます。詳細については、「権限の承認」を参照してください。
5. **Import**：デバイスにすでに導入されている設定をSecurity Managerにインポートできます。
6. **Deploy**：ネットワーク内のデバイスに設定変更を導入し、ロールバックを実行して以前に導入した設定に戻すことができます。
7. **制御**:pingなどのデバイスにコマンドを発行できます。

8. **送信**：承認のために設定変更を送信できます。

- 変更、割り当て、承認、インポート、制御、またはデプロイ権限を選択する場合は、対応するビュー権限も選択する必要があります。そうしないと、セキュリティマネージャが正しく機能しません。
- ポリシーの変更アクセス許可を選択する場合は、対応するポリシーの割り当ておよび表示アクセス許可も選択する必要があります。
- ポリシーオブジェクトを定義の一部として使用するポリシーを許可する場合は、これらのオブジェクトタイプに対するビュー権限も付与する必要があります。たとえば、ルーティングポリシーを変更する権限を選択した場合、ルーティングポリシーに必要なオブジェクトタイプであるネットワークオブジェクトとインターフェイスの役割を表示する権限も選択する必要があります。
- 定義の一部として他のオブジェクトを使用するオブジェクトを許可する場合も、同じことが当てはまります。たとえば、ユーザグループを変更する権限を選択した場合、ネットワークオブジェクト、ACLオブジェクト、およびAAAサーバグループを表示する権限も選択する必要があります。

権限の表示

Security Managerの表示（読み取り専用）権限は、次に示すようにカテゴリに分類されます。

- ポリシー権限の表示
- オブジェクト権限の表示
- 追加のビュー権限

ポリシー権限の表示

セキュリティマネージャには、ポリシーに対する次の表示権限が含まれます。

1. **[View] > [Policies] > [Firewall]を選択します。**PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスのファイアウォールサービスポリシー（ファイアウォールの下のポリシーセレクタ）を表示できます。ファイアウォールサービスポリシーの例には、アクセスルール、AAAルール、およびインスペクションルールがあります。
2. **[View] > [Policies] > [Intrusion Prevention System]を選択します。**IOSルータで実行されているIPSのポリシーを含め、IPSポリシー（IPSの下のポリシーセレクタ）を表示できます。
3. **[View] > [Policies] > [Image]。**[Apply IPS Updates]ウィザード（[Tools] > [Apply IPS Update]の順に選択）でシグニチャ更新パッケージを選択できますが、[Modify] > [Policies] > [Image]権限がない限り、特定のデバイスにパッケージを割り当てることはできません。
4. **View > Policies > NAT**の順に選択します。PIX/ASA/FWSMデバイスおよびIOSルータのネットワークアドレス変換ポリシーを表示できます。NATポリシーの例には、スタティックルールやダイナミックルールがあります。
5. **[View] > [Policies] > [Site-to-Site VPN]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスのサイト間VPNポリシーを表示できます。サイト間VPNポリシーの例としては、IKEプロポーザル、IPsecプロポーザル、事前共有キーなどがあります。
6. **[View] > [Policies] > [Remote Access VPN]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスのリモートアクセスVPNポリシーを表示できます。リモートアクセスVPNポリシーの例には、IKEプロポーザル、IPsecプロポーザル、および

PKIポリシーがあります。

7. **[View] > [Policies] > [SSL VPN]**を選択します。PIX/ASA/FWSMデバイスおよびIOSルータ（SSL VPNウィザードなど）のSSL VPNポリシーを表示できます。
8. **[View] > [Policies] > [Interfaces]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、IPSセンサー、およびCatalyst 6500/7600デバイスのインターフェイスポリシー（インターフェイスの下のポリシーセレクタ）を表示できます。PIX/ASA/FWSMデバイスでは、この権限はハードウェアポートとインターフェイスの設定を対象としています。IOSルータでは、インターフェイスの基本設定と詳細設定、およびDSL、PVC、PPP、ダイヤラポリシーなどの他のインターフェイス関連ポリシーが対象となります。IPSセンサーでは、この権限は物理インターフェイスと集約マップを対象としています。Catalyst 6500/7600デバイスでは、この権限はインターフェイスとVLAN設定をカバーします。
9. **[View] > [Policies] > [Bridging]**を選択します。PIX/ASA/FWSMデバイス上のARPテーブルポリシー（Platform > Bridgingの下のポリシーセレクタ）を表示できます。
10. **[View] > [Policies] > [Device Administration]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイス上のデバイス管理ポリシー（[Platform] > [Device Admin]の下のポリシーセレクタ）を表示できます。PIX/ASA/FWSMデバイスでは、デバイスアクセスポリシー、サーバアクセスポリシー、およびフェールオーバーポリシーなどが例として挙げられます。IOSルータの例には、デバイスアクセス（回線アクセスを含む）ポリシー、サーバアクセスポリシー、AAA、およびセキュアデバイスプロビジョニングなどがあります。IPSセンサーでは、この権限はデバイスアクセスポリシーとサーバアクセスポリシーを対象としています。Catalyst 6500/7600デバイスでは、この権限はIDSM設定とVLANアクセスリストを対象としています。
11. **[View] > [Policies] > [Identity]**を選択します。802.1xおよびNetwork Admission Control(NAC)ポリシーを含め、Cisco IOSルータ上のアイデンティティポリシー（プラットフォーム>アイデンティティの下のポリシーセレクタ）を表示できます。
12. **[View] > [Policies] > [Logging]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびIPSセンサー上の口ギングポリシーを（[Platform] > [Logging]の下のポリシーセレクタで）表示できます。口ギングポリシーの例には、口ギングセットアップ、サーバ設定、およびsyslogサーバポリシーがあります。
13. **[View] > [Policies] > [Multicast]**を選択します。PIX/ASA/FWSMデバイス上のマルチキャストポリシー（プラットフォーム>マルチキャストのポリシーセレクタ内）を表示できます。マルチキャストポリシーの例には、マルチキャストルーティングやIGMPポリシーなどがあります。
14. **[View] > [Policies] > [QoS]**を選択します。Cisco IOSルータ上のQoSポリシー（[Platform] > [Quality of Service]の下のポリシーセレクタ）を表示できます。
15. **[View] > [Policies] > [Routing]**を選択します。PIX/ASA/FWSMデバイスおよびIOSルータ上のルーティングポリシー（Platform > Routingの下のポリシーセレクタ）を表示できます。ルーティングポリシーの例には、OSPF、RIP、およびスタティックルーティングポリシーがあります。
16. **[View] > [Policies] > [Security]**を選択します。PIX/ASA/FWSMデバイスおよびIPSセンサー上のセキュリティポリシー（[Platform] > [Security]の下のポリシーセレクタ）を表示できます。PIX/ASA/FWSMデバイスのセキュリティポリシーには、アンチスプーフィング、フラグメント、およびタイムアウトの設定が含まれます。IPSセンサーでは、セキュリティポリシーにブロッキング設定が含まれます。
17. **[View] > [Policies] > [Service Policy Rules]**を選択します。PIX 7.x/ASAデバイス上のサービスポリシールールポリシー（プラットフォーム>サービスポリシールールのポリシーセレクタ内）を表示できます。たとえば、プライオリティキューやIPS、QoS、接続ルールなどがあります。

18. **[View] > [Policies] > [User Preferences]**PIX/ASA/FWSMデバイス上の展開ポリシー（[Platform] > [User Preferences]のポリシーセレクタ）を表示できます。このポリシーには、展開時にすべてのNAT変換をクリアするためのオプションが含まれています。
19. **[View] > [Policies] > [Virtual Device]**を選択します。IPSデバイスの仮想センサーポリシーを表示できます。このポリシーは、仮想センサーの作成に使用されます。
20. **[View] > [Policies] > [FlexConfig]**を選択します。FlexConfigを表示できます。FlexConfigは、PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスに導入できる追加のCLIコマンドと手順です。

オブジェクト権限の表示

セキュリティマネージャには、オブジェクトに対する次の表示権限が含まれます。

1. **[View] > [Objects] > [AAA Server Groups]**AAAサーバグループオブジェクトを表示できます。これらのオブジェクトは、AAAサービス（認証、許可、アカウンティング）を必要とするポリシーで使用されます。
2. **[View] > [Objects] > [AAA Servers]**AAAサーバオブジェクトを表示できます。これらのオブジェクトは、AAAサーバグループの一部として定義されている個々のAAAサーバを表します。
3. **[View] > [Objects] > [Access Control Lists - Standard/Extended]**。標準および拡張ACLオブジェクトを表示できます。拡張ACLオブジェクトは、NATやNACなどのさまざまなポリシーや、VPNアクセスの確立に使用されます。標準ACLオブジェクトは、OSPFやSNMPなどのポリシー、およびVPNアクセスの確立に使用されます。
4. **[View] > [Objects] > [Access Control Lists]** - [Web]。Web ACLオブジェクトを表示できます。Web ACLオブジェクトは、SSL VPNポリシーでコンテンツフィルタリングを実行するために使用されます。
5. **[View] > [Objects] > [ASA User Groups]**を選択します。ASAユーザグループオブジェクトを表示できます。これらのオブジェクトは、Easy VPN、リモートアクセスVPN、およびSSL VPN設定のASAセキュリティアプライアンスで設定されます。
6. **[表示] > [オブジェクト] > [カテゴリ]**を選択します。カテゴリオブジェクトを表示できます。これらのオブジェクトは、色を使用してルールとオブジェクトをルール表で簡単に識別するのに役立ちます。
7. **[View] > [Objects] > [Credentials]**。クレデンシャルオブジェクトを表示できます。これらのオブジェクトは、IKE拡張認証(Xauth)中のEasy VPN設定で使用されます。
8. **[View] > [Objects] > [FlexConfigs]**FlexConfigオブジェクトを表示できます。これらのオブジェクトには、追加のスクリプト言語命令を含む設定コマンドが含まれており、Security Managerのユーザインターフェイスでサポートされていないコマンドを設定するために使用できます。
9. **[View] > [Objects] > [IKE Proposals]**IKEプロポーザルのオブジェクトを表示できます。これらのオブジェクトには、リモートアクセスVPNポリシーのIKEプロポーザルに必要なパラメータが含まれています。
10. **[View] > [Objects] > [Inspect - Class Maps** - DNS]。DNSクラスマップオブジェクトを表示できます。これらのオブジェクトは、特定の基準を持つDNSトラフィックと一致するため、そのトラフィックに対してアクションを実行できます。
11. **[View] > [Objects] > [Inspect - Class Maps - FTP]**。FTPクラスマップオブジェクトを表示できます。これらのオブジェクトは、特定の基準を持つFTPトラフィックと一致するため、そのトラフィックに対してアクションを実行できます。
12. **[View] > [Objects] > [Inspect - Class Maps - HTTP]**。HTTPクラスマップオブジェクトを表示できます。これらのオブジェクトは、特定の基準を持つHTTPトラフィックと一致するた

め、そのトラフィックに対してアクションを実行できます。

13. **[View] > [Objects] > [Inspect - Class Maps - IM]**。IMクラスマップオブジェクトを表示できます。これらのオブジェクトは、IMトラフィックと特定の基準を照合し、そのトラフィックに対してアクションを実行できるようにします。
14. **[View] > [Objects] > [Inspect - Class Maps - SIP]**。SIPクラスマップオブジェクトを表示できます。これらのオブジェクトは、特定の基準を持つSIPトラフィックと一致するため、そのトラフィックに対してアクションを実行できます。
15. **[View] > [Objects] > [Inspect - Policy Maps - DNS]。**DNSポリシーマップオブジェクトを表示できます。これらのオブジェクトは、DNSトラフィックのインスペクションマップを作成するために使用されます。
16. **[View] > [Objects] > [Inspect - Policy Maps - FTP]。**FTPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、FTPトラフィックのインスペクションマップを作成するために使用されます。
17. **[View] > [Objects] > [Inspect - Policy Maps - GTP]**。GTPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、GTPトラフィックのインスペクションマップを作成するために使用されます。
18. **[View] > [Objects] > [Inspect - Policy Maps - HTTP(ASA7.1.x/PIX7.1.x/IOS)**。 ASA/PIX 7.1.xデバイスおよびIOSルータ用に作成されたHTTPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、HTTPトラフィックのインスペクションマップを作成するために使用されます。
19. **[View] > [Objects] > [Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2)]**。 ASA 7.2/PIX 7.2デバイス用に作成されたHTTPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、HTTPトラフィックのインスペクションマップを作成するために使用されます。
20. **[View] > [Objects] > [Inspect - Policy Maps - IM (ASA7.2/PIX7.2)]**。 ASA 7.2/PIX 7.2デバイス用に作成されたIMポリシーマップオブジェクトを表示できます。これらのオブジェクトは、IMトラフィックのインスペクションマップを作成するために使用されます。
21. **[View] > [Objects] > [Inspect - Policy Maps - IM (IOS)]** IOSデバイス用に作成されたIMポリシーマップオブジェクトを表示できます。これらのオブジェクトは、IMトラフィックのインスペクションマップを作成するために使用されます。
22. **[View] > [Objects] > [Inspect - Policy Maps - SIP]**。SIPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、SIPトラフィックのインスペクションマップを作成するために使用されます。
23. **View > Objects > Inspect – 正規表現**。正規表現オブジェクトを表示できます。これらのオブジェクトは、正規表現グループの一部として定義された個々の正規表現を表します。
24. **View > Objects > Inspect – 正規表現グループ**。正規表現グループオブジェクトを表示できます。これらのオブジェクトは、特定のクラスマップによって使用され、パケット内のテキストと一致するようにマップを検査します。
25. **[View] > [Objects] > [Inspect - TCP Maps]**。TCPマップオブジェクトを表示できます。これらのオブジェクトは、両方向のTCPフローの検査をカスタマイズします。
26. **[View] > [Objects] > [Interface Roles]**インターフェイスロールオブジェクトを表示できます。これらのオブジェクトは、異なるタイプのデバイスで複数のインターフェイスを表すことができる命名パターンを定義します。インターフェイスの役割により、各インターフェイスの名前を手動で定義しなくても、複数のデバイス上の特定のインターフェイスにポリシーを適用できます。
27. **[View] > [Objects] > [IPsec Transform Sets]**IPsecトランスフォームセットオブジェクトを表示できます。これらのオブジェクトは、IPsecトンネル内のデータの暗号化方法と認証方法を正確に指定するセキュリティプロトコル、アルゴリズム、およびその他の設定の組み合わせを構成します。

28. **[表示] > [オブジェクト] > [LDAP属性マップ]**を選択します。LDAP属性マップオブジェクトを表示できます。これらのオブジェクトは、カスタム（ユーザ定義）属性名をCisco LDAP属性名にマッピングするために使用されます。
29. **[View] > [Objects] > [Networks/Hosts]**を選択します。ネットワーク/ホストオブジェクトを表示できます。これらのオブジェクトは、ネットワーク、ホスト、またはその両方を表すIPアドレスの論理コレクションです。ネットワーク/ホスト・オブジェクトを使用すると、各ネットワークまたはホストを個別に指定することなく、ポリシーを定義できます。
30. **[View] > [Objects] > [PKI Enrollments]**。PKI登録オブジェクトを表示できます。これらのオブジェクトは、公開キーインフラストラクチャ内で動作する認証局(CA)サーバを定義します。
31. **[View] > [Objects] > [Port Forwarding Lists]**。ポート転送リストオブジェクトを表示できます。これらのオブジェクトは、リモートクライアントのポート番号と、SSL VPNゲートウェイの背後にあるアプリケーションのIPアドレスおよびポートとのマッピングを定義します。
32. **[View] > [Objects] > [Secure Desktop Configurations]**を選択します。セキュアなデスクトップ設定オブジェクトを表示できます。これらのオブジェクトは、SSL VPNポリシーで参照できる再利用可能な名前付きコンポーネントで、SSL VPNセッションの間に共有される機密データのすべてのトレースを排除する信頼性の高い手段を提供します。
33. **[View] > [Objects] > [Services - Port Lists]**。ポートリストオブジェクトを表示できます。これらのオブジェクトは、1つまたは複数の範囲のポート番号を含んでおり、サービスオブジェクトの作成プロセスを合理化するために使用されます。
34. **View > Objects > Services/Service Groupsサービスおよびサービスグループ**オブジェクトを表示できます。これらのオブジェクトは、Kerberos、SSH、POP3などのポリシーで使用されるネットワークサービスを記述するプロトコルおよびポート定義のマッピングとして定義されます。
35. **[View] > [Objects] > [Single Sign On Servers]**サーバーオブジェクトのシングルサインオンを表示できます。シングルサインオン(SSO)を使用すると、SSL VPNユーザはユーザ名とパスワードを1回だけ入力し、複数の保護されたサービスとWebサーバにアクセスできます。
36. **[View] > [Objects] > [SLA Monitors]**を選択します。SLAモニタオブジェクトを表示できます。これらのオブジェクトは、バージョン7.2以降を実行するPIX/ASAセキュリティアプライアンスがルートトラッキングを実行するために使用します。この機能は、プライマリルートの可用性を追跡し、プライマリルートに障害が発生した場合にバックアップルートをインストールする方法を提供します。
37. **[View] > [Objects] > [SSL VPN Customizations]**を選択します。SSL VPNカスタマイズオブジェクトを表示できます。これらのオブジェクトは、ユーザに表示されるSSL VPNページ（ログイン/ログアウト、ホームページなど）の外観を変更する方法を定義します。
38. **[View] > [Objects] > [SSL VPN Gateways]**を選択します。SSL VPNゲートウェイオブジェクトを表示できます。これらのオブジェクトは、SSL VPNの保護されたリソースへの接続のプロキシとしてゲートウェイを使用できるようにするパラメータを定義します。
39. **[表示] > [オブジェクト] > [スタイルオブジェクト]**。スタイルオブジェクトを表示できます。これらのオブジェクトを使用すると、フォントの特性や色などのスタイル要素を設定して、セキュリティアプライアンスに接続したときにSSL VPNユーザに表示されるSSL VPNページの外観をカスタマイズできます。
40. **[表示] > [オブジェクト] > [文字オブジェクト]**を選択します。自由形式のテキストオブジェクトを表示できます。これらのオブジェクトは、名前と値のペアで構成されます。値には、単一の文字列、文字列のリスト、または文字列のテーブルを指定できます。
41. **[表示] > [オブジェクト] > [時間範囲]。**時間範囲オブジェクトを表示できます。これらのオ

ブジェクトは、時間ベースのACLとインスペクションルールを作成するときに使用されます。また、ASAユーザグループを定義してVPNアクセスを特定の時間帯に制限する場合にも使用されます。

42. **[View] > [Objects] > [Traffic Flows]**。トラフィックフローオブジェクトを表示できます。これらのオブジェクトは、PIX 7.x/ASA 7.xデバイスで使用する特定のトラフィックフローを定義します。
43. **[View] > [Objects] > [URL Lists]**。URLリストオブジェクトを表示できます。これらのオブジェクトは、ログインが成功した後にポータルページに表示されるURLを定義します。これにより、ユーザはクライアントレスアクセスモードで動作しているときに、SSL VPN Webサイトで使用可能なリソースにアクセスできます。
44. **[View] > [Objects] > [User Groups]**ユーザグループオブジェクトを表示できます。これらのオブジェクトは、Easy VPNトポロジ、リモートアクセスVPN、およびSSL VPNで使用されるリモートクライアントのグループを定義します。
45. **[View] > [Objects] > [WINS Server Lists]**を選択します。WINSサーバリストオブジェクトを表示できます。これらのオブジェクトはWINSサーバを表します。WINSサーバはSSL VPNによってリモートシステム上のファイルにアクセスまたは共有するために使用されます。
46. **[View] > [Objects] > [Internal - DN Rules]**DNポリシーで使用されるDNルールを表示できます。これは、セキュリティマネージャによって使用される内部オブジェクトで、ポリシーオブジェクトマネージャには表示されません。
47. **[View] > [Objects] > [Internal - Client Updates]**。これは、Policy Object Managerに表示されないユーザグループオブジェクトに必要な内部オブジェクトです。
48. **[View] > [Objects] > [Internal - Standard ACEs]**これは、ACLオブジェクトによって使用される標準アクセスコントロールエントリの内部オブジェクトです。
49. **[View] > [Objects] > [Internal - Extended ACEs]**これは、ACLオブジェクトによって使用される拡張アクセスコントロールエントリの内部オブジェクトです。

追加のビュー権限

セキュリティマネージャには、次の追加ビュー権限が含まれます。

1. **[View] > [Admin]**。セキュリティマネージャの管理設定を表示できます。
2. [View] > [CLI] **を選択します。**デバイスに設定されているCLIコマンドを表示し、展開しようとしているコマンドをプレビューできます。
3. **[View] > [Config Archive]**。設定アーカイブに含まれる設定のリストを表示できます。デバイス設定やCLIコマンドは表示できません。
4. **[View] > [Devices]**。デバイスの設定、プロパティ、割り当てなどを含む、デバイスビューとすべての関連情報を表示できます。
5. [View] > [Device Managers] を選択します。Cisco RouterやCisco IOSルータのSecurity Device Manager(SDM)など、個々のデバイスのデバイスマネージャの読み取り専用バージョンを起動できます。
6. **[View] > [Topology]**を選択します。マップビューで設定されたマップを表示できます。

権限の変更

Security Managerの変更（読み取り/書き込み）権限は、次に示すようにカテゴリに分類されます。

ポリシー権限の変更

注：ポリシーの変更権限を指定する場合は、対応する割り当て権限と表示ポリシー権限も選択していることを確認してください。

セキュリティマネージャには、ポリシーに対する次の変更権限が含まれます。

1. **[Modify] > [Policies] > [Firewall]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスのファイアウォールサービスポリシー（ファイアウォールの下のポリシーセレクタ）を変更できます。ファイアウォールサービスポリシーの例には、アクセスルール、AAAルール、およびインスペクションルールがあります。
2. **[Modify] > [Policies] > [Intrusion Prevention System]**を選択します。IOSルータで実行されているIPSのポリシーを含め、IPSポリシー（IPSの下のポリシーセレクタ）を変更できます。この権限を使用すると、シグニチャの更新ウィザード（[Tools] > [Apply IPS Update]の下）でシグニチャを調整することもできます。
3. **[Modify] > [Policies] > [Image]**を選択します。[Apply IPS Updates]ウィザード（[Tools] > [Apply IPS Update]の下）で、デバイスにシグニチャ更新パッケージを割り当てることができます。 この権限を使用すると、特定のデバイス（[Tools] > [Security Manager Administration] > [IPS Updates]にある）に自動更新設定を割り当てることもできます。
4. **Modify > Policies > NAT**の順に選択します。PIX/ASA/FWSMデバイスおよびIOSルータのネットワークアドレス変換ポリシーを変更できます。NATポリシーの例には、スタティックルールやダイナミックルールがあります。
5. **[Modify] > [Policies] > [Site-to-Site VPN]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスのサイト間VPNポリシーを変更できます。サイト間VPNポリシーの例としては、IKEプロポーザル、IPsecプロポーザル、事前共有キーなどがあります。
6. **[Modify] > [Policies] > [Remote Access VPN]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスのリモートアクセスVPNポリシーを変更できます。リモートアクセスVPNポリシーの例には、IKEプロポーザル、IPsecプロポーザル、およびPKIポリシーがあります。
7. **[Modify] > [Policies] > [SSL VPN]**を選択します。PIX/ASA/FWSMデバイスおよびIOSルータ（SSL VPNウィザードなど）でSSL VPNポリシーを変更できます。
8. **[Modify] > [Policies] > [Interfaces]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、IPSセンサー、およびCatalyst 6500/7600デバイスのインターフェイスポリシー（インターフェイスの下のポリシーセレクタ）を変更できます。PIX/ASA/FWSMデバイスでは、この権限はハードウェアポートとインターフェイスの設定を対象としています。IOSルータでは、インターフェイスの基本設定と詳細設定、およびDSL、PVC、PPP、ダイヤラポリシーなどの他のインターフェイス関連ポリシーが対象となります。IPSセンサーでは、この権限は物理インターフェイスと集約マップを対象としています。Catalyst 6500/7600デバイスでは、この権限はインターフェイスとVLAN設定をカバーします。
9. **Modify > Policies > Bridging**の順に選択します。PIX/ASA/FWSMデバイスのARPテーブルポリシー（Platform > Bridgingの下のポリシーセレクタ）を変更できます。
10. **[Modify] > [Policies] > [Device Administration]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスで、デバイス管理ポリシーを（Platform >

Device Adminの下のPolicy Selector内にある）変更できます。PIX/ASA/FWSMデバイスでは、デバイスアクセスポリシー、サーバアクセスポリシー、およびフェールオーバーポリシーなどが例として挙げられます。IOSルータの例には、デバイスアクセス（回線アクセスを含む）ポリシー、サーバアクセスポリシー、AAA、およびセキュアデバイスプロビジョニングなどがあります。IPSセンサーでは、この権限はデバイスアクセスポリシーとサーバアクセスポリシーを対象としています。Catalyst 6500/7600デバイスでは、この権限はIDSM設定とVLANアクセスリストを対象としています。

11. **[Modify] > [Policies] > [Identity]**を選択します。802.1xおよびNetwork Admission Control(NAC)ポリシーを含め、Cisco IOSルータのアイデンティティポリシー（プラットフォーム>アイデンティティの下のポリシーセレクタ）を変更できます。
12. **[Modify] > [Policies] > [Logging]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびIPSセンサーのロギングポリシーを（Platform > Loggingの下のPolicy Selectorにある）変更できます。ロギングポリシーの例には、ロギングセットアップ、サーバ設定、およびsyslogサーバポリシーがあります。
13. **[Modify] > [Policies] > [Multicast]**を選択します。PIX/ASA/FWSMデバイスのマルチキャストポリシー（Platform > Multicastの下のPolicy Selector）を変更できます。マルチキャストポリシーの例には、マルチキャストルーティングやIGMPポリシーなどがあります。
14. **[Modify] > [Policies] > [QoS]**を選択します。Cisco IOSルータのQoSポリシー（[Platform] > [Quality of Service]の下のポリシーセレクタ）を変更できます。
15. **[Modify] > [Policies] > [Routing]**を選択します。PIX/ASA/FWSMデバイスおよびIOSルータ上のルーティングポリシー（Platform > Routingの下のポリシーセレクタ）を変更できます。ルーティングポリシーの例には、OSPF、RIP、およびスタティックルーティングポリシーがあります。
16. [Modify] > [Policies] > [Security] **を選択します。**PIX/ASA/FWSMデバイスおよびIPSセンサー上のセキュリティポリシー（Platform > Securityの下のPolicy Selector内）を変更できます。PIX/ASA/FWSMデバイスのセキュリティポリシーには、アンチスプーフィング、フラグメント、およびタイムアウトの設定が含まれます。IPSセンサーでは、セキュリティポリシーにブロッキング設定が含まれます。
17. **[Modify] > [Policies] > [Service Policy Rules]**を選択します。PIX 7.x/ASAデバイスのサービスポリシールールポリシーを変更できます([プラットフォーム(Platform)] > [サービスポリシールール(Service Policy Rules)]のポリシーセレクタにあります)。たとえば、プライオリティキューやIPS、QoS、接続ルールなどがあります。
18. **[Modify] > [Policies] > [User Preferences]**PIX/ASA/FWSMデバイスの展開ポリシー（Platform > User Preferencesのポリシーセレクタ）を変更できます。このポリシーには、展開時にすべてのNAT変換をクリアするためのオプションが含まれています。
19. **[Modify] > [Policies] > [Virtual Device]**を選択します。IPSデバイスの仮想センサーポリシーを変更できます。このポリシーを使用して、仮想センサーを作成します。
20. **[Modify] > [Policies] > [FlexConfig]**を選択します。FlexConfigを変更できます。FlexConfigは、PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスに導入できる追加のCLIコマンドと手順です。

オブジェクトの変更権限

セキュリティマネージャには、オブジェクトに対する次の表示権限が含まれます。

1. **[Modify] > [Objects] > [AAA Server Groups]**AAAサーバグループオブジェクトを表示できます。これらのオブジェクトは、AAAサービス（認証、許可、アカウンティング）を必要とするポリシーで使用されます。

2. **[Modify] > [Objects] > [AAA Servers]**AAAサーバオブジェクトを表示できます。これらのオブジェクトは、AAAサーバグループの一部として定義されている個々のAAAサーバを表します。
3. **[Modify] > [Objects] > [Access Control Lists - Standard/Extended]**。標準および拡張ACLオブジェクトを表示できます。拡張ACLオブジェクトは、NATやNACなどのさまざまなポリシーや、VPNアクセスの確立に使用されます。標準ACLオブジェクトは、OSPFやSNMPなどのポリシー、およびVPNアクセスの確立に使用されます。
4. **[Modify] > [Objects] > [Access Control Lists - Web]**。Web ACLオブジェクトを表示できます。Web ACLオブジェクトは、SSL VPNポリシーでコンテンツフィルタリングを実行するために使用されます。
5. **[Modify] > [Objects] > [ASA** User Groups]。ASAユーザグループオブジェクトを表示できます。これらのオブジェクトは、Easy VPN、リモートアクセスVPN、およびSSL VPN設定のASAセキュリティアプライアンスで設定されます。
6. **修正>オブジェクト>カテゴリ**。カテゴリオブジェクトを表示できます。これらのオブジェクトは、色を使用してルールとオブジェクトをルール表で簡単に識別するのに役立ちます。
7. **[Modify] > [Objects] > [Credentials]**を選択します。クレデンシャルオブジェクトを表示できます。これらのオブジェクトは、IKE拡張認証(Xauth)中のEasy VPN設定で使用されます。
8. **[Modify] > [Objects] > [FlexConfigs]**を選択します。FlexConfigオブジェクトを表示できます。これらのオブジェクトには、追加のスクリプト言語命令を含む設定コマンドが含まれており、Security Managerのユーザインターフェイスでサポートされていないコマンドを設定するために使用できます。
9. **[Modify] > [Objects] > [IKE Proposals]**IKEプロポーザルのオブジェクトを表示できます。これらのオブジェクトには、リモートアクセスVPNポリシーのIKEプロポーザルに必要なパラメータが含まれています。
10. **[Modify] > [Objects] > [Inspect - Class Maps - DNS]**。DNSクラスマップオブジェクトを表示できます。これらのオブジェクトは、特定の基準を持つDNSトラフィックと一致するため、そのトラフィックに対してアクションを実行できます。
11. **Modify > Objects > Inspect - Class Maps - FTP**。FTPクラスマップオブジェクトを表示できます。これらのオブジェクトは、特定の基準を持つFTPトラフィックと一致するため、そのトラフィックに対してアクションを実行できます。
12. **Modify > Objects > Inspect - Class Maps - HTTP**。HTTPクラスマップオブジェクトを表示できます。これらのオブジェクトは、特定の基準を持つHTTPトラフィックと一致するため、そのトラフィックに対してアクションを実行できます。
13. **[Modify] > [Objects] > [Inspect - Class Maps - IM]**。IMクラスマップオブジェクトを表示できます。これらのオブジェクトは、IMトラフィックと特定の基準を照合し、そのトラフィックに対してアクションを実行できるようにします。
14. **[Modify] > [Objects] > [Inspect - Class Maps - SIP]**。SIPクラスマップオブジェクトを表示できます。これらのオブジェクトは、特定の基準を持つSIPトラフィックと一致するため、そのトラフィックに対してアクションを実行できます。
15. **[Modify] > [Objects] > [Inspect - Policy Maps - DNS]**。DNSポリシーマップオブジェクトを表示できます。これらのオブジェクトは、DNSトラフィックのインスペクションマップを作成するために使用されます。
16. **[Modify] > [Objects] > [Inspect - Policy Maps - FTP]**を選択します。FTPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、FTPトラフィックのインスペクションマップを作成するために使用されます。
17. **Modify > Objects > Inspect - Policy Maps - HTTP(ASA7.1.x/PIX7.1.x/IOS)**。 ASA/PIX 7.xデバイスおよびIOSルータ用に作成されたHTTPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、HTTPトラフィックのインスペクションマップを作成するため

に使用されます。

18. **Modify > Objects > Inspect - Policy Maps - HTTP(ASA7.2/PIX7.2)**。 ASA 7.2/PIX 7.2デバイス用に作成されたHTTPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、HTTPトラフィックのインスペクションマップを作成するために使用されます。
19. **Modify > Objects > Inspect - Policy Maps - IM(ASA7.2/PIX7.2)**。 ASA 7.2/PIX 7.2デバイス用に作成されたIMポリシーマップオブジェクトを表示できます。これらのオブジェクトは、IMトラフィックのインスペクションマップを作成するために使用されます。
20. **[Modify] > [Objects] > [Inspect - Policy Maps - IM (IOS)]**。 IOSデバイス用に作成されたIMポリシーマップオブジェクトを表示できます。これらのオブジェクトは、IMトラフィックのインスペクションマップを作成するために使用されます。
21. **[Modify] > [Objects] > [Inspect - Policy Maps - SIP]**。SIPポリシーマップオブジェクトを表示できます。これらのオブジェクトは、SIPトラフィックのインスペクションマップを作成するために使用されます。
22. **Modify > Objects > Inspect – 正規表現**。正規表現オブジェクトを表示できます。これらのオブジェクトは、正規表現グループの一部として定義された個々の正規表現を表します。
23. **Modify > Objects > Inspect – 正規表現グループ**。正規表現グループオブジェクトを表示できます。これらのオブジェクトは、特定のクラスマップによって使用され、パケット内のテキストと一致するようにマップを検査します。
24. **[Modify] > [Objects] > [Inspect - TCP Maps]**。TCPマップオブジェクトを表示できます。これらのオブジェクトは、両方向のTCPフローの検査をカスタマイズします。
25. **[Modify] > [Objects] > [Interface Roles]**インターフェイスロールオブジェクトを表示できます。これらのオブジェクトは、異なるタイプのデバイスで複数のインターフェイスを表すことができる命名パターンを定義します。インターフェイスの役割により、各インターフェイスの名前を手動で定義しなくても、複数のデバイス上の特定のインターフェイスにポリシーを適用できます。
26. **[Modify] > [Objects] > [IPsec Transform Sets]**IPsecトランスフォームセットオブジェクトを表示できます。これらのオブジェクトは、IPsecトンネル内のデータの暗号化方法と認証方法を正確に指定するセキュリティプロトコル、アルゴリズム、およびその他の設定の組み合わせを構成します。
27. **[Modify] > [Objects] > [LDAP Attribute Maps]**を選択します。LDAP属性マップオブジェクトを表示できます。これらのオブジェクトは、カスタム（ユーザ定義）属性名をCisco LDAP属性名にマッピングするために使用されます。
28. **Modify > Objects > Networks/Hosts**の順に選択します。ネットワーク/ホストオブジェクトを表示できます。これらのオブジェクトは、ネットワーク、ホスト、またはその両方を表すIPアドレスの論理コレクションです。ネットワーク/ホスト・オブジェクトを使用すると、各ネットワークまたはホストを個別に指定することなく、ポリシーを定義できます。
29. **Modify > Objects > PKI Enrollments**。PKI登録オブジェクトを表示できます。これらのオブジェクトは、公開キーインフラストラクチャ内で動作する認証局(CA)サーバを定義します。
30. **[Modify] > [Objects] > [Port Forwarding Lists]**。ポート転送リストオブジェクトを表示できます。これらのオブジェクトは、リモートクライアントのポート番号と、SSL VPNゲートウェイの背後にあるアプリケーションのIPアドレスおよびポートとのマッピングを定義します。
31. **[Modify] > [Objects] > [Secure Desktop Configurations]**を選択します。セキュアなデスクトップ設定オブジェクトを表示できます。これらのオブジェクトは、SSL VPNポリシーで参照できる再利用可能な名前付きコンポーネントで、SSL VPNセッションの間に共有される機密データのすべてのトレースを排除する信頼性の高い手段を提供します。
32. **[Modify] > [Objects] > [Services - Port Lists]**を選択します。ポートリストオブジェクトを表

示できます。これらのオブジェクトは、1つまたは複数の範囲のポート番号を含んでおり、サービスオブジェクトの作成プロセスを合理化するために使用されます。

33. **[Modify] > [Objects] > [Services/Service Groups]。**サービスおよびサービスグループオブジェクトを表示できます。これらのオブジェクトは、Kerberos、SSH、POP3などのポリシーで使用されるネットワークサービスを記述するプロトコルおよびポート定義のマッピングとして定義されます。
34. **Modify > Objects > Single Sign On Servers.**サーバーオブジェクトのシングルサインオンを表示できます。シングルサインオン(SSO)を使用すると、SSL VPNユーザはユーザ名とパスワードを1回だけ入力し、複数の保護されたサービスとWebサーバにアクセスできます。
35. **[Modify] > [Objects] > [SLA Monitors]**を選択します。SLAモニタオブジェクトを表示できます。これらのオブジェクトは、バージョン7.2以降を実行するPIX/ASAセキュリティアプライアンスがルートトラッキングを実行するために使用します。この機能は、プライマリルートの可用性を追跡し、プライマリルートに障害が発生した場合にバックアップルートをインストールする方法を提供します。
36. **[Modify] > [Objects] > [SSL VPN Customizations]**を選択します。SSL VPNカスタマイズオブジェクトを表示できます。これらのオブジェクトは、ユーザに表示されるSSL VPNページ（ログイン/ログアウト、ホームページなど）の外観を変更する方法を定義します。
37. **[Modify] > [Objects] > [SSL VPN Gateways]**を選択します。SSL VPNゲートウェイオブジェクトを表示できます。これらのオブジェクトは、SSL VPNの保護されたリソースへの接続のプロキシとしてゲートウェイを使用できるようにするパラメータを定義します。
38. **修正>オブジェクト>スタイルオブジェクト。**スタイルオブジェクトを表示できます。これらのオブジェクトを使用すると、フォントの特性や色などのスタイル要素を設定して、セキュリティアプライアンスに接続したときにSSL VPNユーザに表示されるSSL VPNページの外観をカスタマイズできます。
39. **[修正] > [オブジェクト] > [テキストオブジェクト]**を選択します。自由形式のテキストオブジェクトを表示できます。これらのオブジェクトは、名前と値のペアで構成されます。値には、単一の文字列、文字列のリスト、または文字列のテーブルを指定できます。
40. **Modify > Objects > Time Ranges.**時間範囲オブジェクトを表示できます。これらのオブジェクトは、時間ベースのACLとインスペクションルールを作成するときに使用されます。また、ASAユーザグループを定義してVPNアクセスを特定の時間帯に制限する場合にも使用されます。
41. **[Modify] > [Objects] > [Traffic Flows]。**トラフィックフローオブジェクトを表示できます。これらのオブジェクトは、PIX 7.x/ASA 7.xデバイスで使用する特定のトラフィックフローを定義します。
42. **[Modify] > [Objects] > [URL Lists]**を選択します。URLリストオブジェクトを表示できます。これらのオブジェクトは、ログインが成功した後にポータルページに表示されるURLを定義します。これにより、ユーザはクライアントレスアクセスモードで動作しているときに、SSL VPN Webサイトで使用可能なリソースにアクセスできます。
43. **[Modify] > [Objects] > [User Groups]。**ユーザグループオブジェクトを表示できます。これらのオブジェクトは、Easy VPNトポロジ、リモートアクセスVPN、およびSSL VPNで使用されるリモートクライアントのグループを定義します
44. **[Modify] > [Objects] > [WINS Server Lists]**を選択します。WINSサーバリストオブジェクトを表示できます。これらのオブジェクトはWINSサーバを表します。WINSサーバはSSL VPNによってリモートシステム上のファイルにアクセスまたは共有するために使用されます。
45. **[Modify] > [Objects] > [Internal - DN Rules]。**DNポリシーで使用されるDNルールを表示できます。これは、セキュリティマネージャによって使用される内部オブジェクトで、ポリシーオブジェクトマネージャには表示されません。

46. **[Modify] > [Objects] > [Internal - Client Updates]**。これは、Policy Object Managerに表示されないユーザグループオブジェクトに必要な内部オブジェクトです。
47. **[修正] > [オブジェクト] > [内部 – 標準ACE]**を選択します。これは、ACLオブジェクトによって使用される標準アクセスコントロールエントリの内部オブジェクトです。
48. **Modify > Objects > Internal - Extended ACE**。これは、ACLオブジェクトによって使用される拡張アクセスコントロールエントリの内部オブジェクトです。

追加の変更権限

セキュリティマネージャには、次に示す追加の変更権限が含まれます。

1. **[Modify] > [Admin]**を選択します。セキュリティマネージャの管理設定を変更できます。
2. **[Modify] > [Config Archive]**。設定アーカイブでデバイス設定を変更できます。さらに、設定をアーカイブに追加したり、設定アーカイブツールをカスタマイズしたりできます。
3. **[Modify] > [Devices]**を選択します。デバイスを追加および削除したり、デバイスのプロパティや属性を変更したりできます。追加するデバイスのポリシーを検出するには、インポート権限も有効にする必要があります。また、[Modify] > [Devices]権限を有効にする場合は、[Assign] > [Policies] > [Interfaces]権限も有効にしてください。
4. **Modify > Hierarchy**。デバイスグループを変更できます。
5. **[Modify] > [Topology]**を選択します。マップビューでマップを修正できます。

権限を割り当てる

セキュリティマネージャには、次に示すポリシー割り当て権限が含まれます。

1. **[Assign] > [Policies] > [Firewall]**を選択します。ファイアウォールサービスポリシー（ファイアウォールの下のポリシーセレクタ）を、PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスに割り当てることができます。ファイアウォールサービスポリシーの例には、アクセスルール、AAAルール、およびインスペクションルールがあります。
2. **[Assign] > [Policies] > [Intrusion Prevention System]**を選択します。IOSルータで実行されているIPSのポリシーを含め、IPSポリシー（IPSの下のポリシーセレクタ）を割り当てることができます。
3. **[Assign] > [Policies] > [Image]**を選択します。このアクセス許可は、現在セキュリティマネージャによって使用されていません。
4. **Assign > Policies > NAT**の順に選択します。ネットワークアドレス変換ポリシーをPIX/ASA/FWSMデバイスおよびIOSルータに割り当てることができます。NATポリシーの例には、スタティックルールやダイナミックルールがあります。
5. **[Assign] > [Policies] > [Site-to-Site VPN]**を選択します。サイト間VPNポリシーをPIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスに割り当てることができます。サイト間VPNポリシーの例としては、IKEプロポーザル、IPsecプロポーザル、事前共有キーなどがあります。
6. **[Assign] > [Policies] > [Remote Access VPN]**を選択します。リモートアクセスVPNポリシーをPIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスに割り当てることができます。リモートアクセスVPNポリシーの例には、IKEプロポーザル、IPsecプロポーザル、およびPKIポリシーがあります。
7. **[Assign] > [Policies] > [SSL VPN]**を選択します。SSL VPNウィザードなどのPIX/ASA/FWSMデバイスおよびIOSルータにSSL VPNポリシーを割り当てることができます。

8. **[Assign] > [Policies] > [Interfaces]**を選択します。PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスにインターフェイスポリシー（インターフェイスの下のポリシーセレクタ）を割り当てることができます。PIX/ASA/FWSMデバイスでは、この権限はハードウェアポートとインターフェイスの設定を対象としています。IOSルータでは、インターフェイスの基本設定と詳細設定、およびDSL、PVC、PPP、ダイヤラポリシーなどの他のインターフェイス関連ポリシーが対象となります。Catalyst 6500/7600デバイスでは、この権限はインターフェイスとVLAN設定をカバーします。
9. **[Assign] > [Policies] > [Bridging]**を選択します。ARPテーブルポリシー（[Platform] > [Bridging]の下のポリシーセレクタ）をPIX/ASA/FWSMデバイスに割り当てることができます。
10. **[Assign] > [Policies] > [Device Administration]**を選択します。デバイス管理ポリシー（Platform > Device Adminの下のPolicy Selectorにある）を、PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスに割り当てることができます。PIX/ASA/FWSMデバイスでは、デバイスアクセスポリシー、サーバアクセスポリシー、およびフェールオーバーポリシーなどが例として挙げられます。IOSルータの例には、デバイスアクセス（回線アクセスを含む）ポリシー、サーバアクセスポリシー、AAA、およびセキュアデバイスプロビジョニングなどがあります。IPSセンサーでは、この権限はデバイスアクセスポリシーとサーバアクセスポリシーを対象としています。Catalyst 6500/7600デバイスでは、この権限はIDSM設定とVLANアクセスリストを対象としています。
11. **[Assign] > [Policies] > [Identity]**を選択します。802.1xおよびNetwork Admission Control(NAC)ポリシーを含むCisco IOSルータに、アイデンティティポリシー（プラットフォーム>アイデンティティのポリシーセレクタ内）を割り当てることができます。
12. **[Assign] > [Policies] > [Logging]**を選択します。ロギングポリシー（Platform > Loggingの下のPolicy Selectorにある）を、PIX/ASA/FWSMデバイスおよびIOSルータに割り当てることができます。ロギングポリシーの例には、ロギングセットアップ、サーバ設定、およびsyslogサーバポリシーがあります。
13. [Assign] > [Policies] > [Multicast] を選択します。マルチキャストポリシー（[Platform] > [Multicast]の下のポリシーセレクタ）をPIX/ASA/FWSMデバイスに割り当てることができます。マルチキャストポリシーの例には、マルチキャストルーティングやIGMPポリシーなどがあります。
14. **[Assign] > [Policies] > [QoS]**を選択します。QoSポリシー（[Platform] > [Quality of Service]のポリシーセレクタにある）をCisco IOSルータに割り当てることができます。
15. **[Assign] > [Policies] > [Routing]**を選択します。（Platform > Routingの下のPolicy Selectorにある）ルーティングポリシーを、PIX/ASA/FWSMデバイスおよびIOSルータに割り当てることができます。ルーティングポリシーの例には、OSPF、RIP、およびスタティックルーティングポリシーがあります。
16. **[Assign] > [Policies] > [Security]**を選択します。PIX/ASA/FWSMデバイスにセキュリティポリシーを割り当てることができます（[Platform] > [Security]の下のポリシーセレクタにあります）。セキュリティポリシーには、アンチスプーフィング、フラグメント、およびタイムアウト設定が含まれます。
17. **[Assign] > [Policies] > [Service Policy Rules]**を選択します。サービスポリシールールポリシー（[Platform] > [Service Policy Rules]のポリシーセレクタにある）をPIX 7.x/ASAデバイスに割り当てることができます。たとえば、プライオリティキューやIPS、QoS、接続ルールなどがあります。
18. **[Assign] > [Policies] > [User Preferences]**PIX/ASA/FWSMデバイスに導入ポリシー（Platform > User Preferencesのポリシーセレクタ）を割り当てることができます。このポリシーには、展開時にすべてのNAT変換をクリアするためのオプションが含まれています。

19. **[Assign] > [Policies] > [Virtual Device]**を選択します。IPSデバイスに仮想センサーポリシーを割り当てることができます。このポリシーを使用して、仮想センサーを作成します。
20. **[Assign] > [Policies] > [FlexConfig]**を選択します。FlexConfigを割り当てることができます。これは、PIX/ASA/FWSMデバイス、IOSルータ、およびCatalyst 6500/7600デバイスに展開できる追加のCLIコマンドおよび手順です。

注：割り当て権限を指定する場合は、対応するビュー権限も選択していることを確認してください。

権限の承認

セキュリティマネージャは、次に示すように承認の権限を提供します。

1. [Approve] > [CLI] **を選択します。**導入ジョブに含まれるCLIコマンドの変更を承認できます。
2. [Approve] > [Policy] **を選択します。**ワークフローアクティビティで設定されたポリシーに含まれる設定変更を承認できます。

CiscoWorksの役割について

ユーザがCiscoWorks Common Servicesで作成されると、1つ以上のロールが割り当てられます。各ロールに関連付けられた権限によって、各ユーザがSecurity Managerで実行する権限を与えられる操作が決まります。

次のトピックでは、CiscoWorksの役割について説明します。

- CiscoWorks Common Servicesのデフォルトロール
- CiscoWorks Common Servicesのユーザへのロールの割り当て

CiscoWorks Common Servicesのデフォルトロール

CiscoWorks Common Servicesには、次のデフォルトロールが含まれています。

1. **ヘルプデスク**：ヘルプデスクユーザは、デバイス、ポリシー、オブジェクト、およびトポロジマップを表示（変更はできません）できます。
2. **ネットワークオペレータ**：ネットワークオペレータは、アクセス許可の表示に加えて、CLIコマンドとSecurity Managerの管理設定を表示できます。ネットワークオペレータは、設定アーカイブを変更し、デバイスに対してコマンド（pingなど）を発行することもできます。
3. **承認者**：権限の表示に加えて、承認者は配置ジョブを承認または拒否できます。導入を実行できません。
4. **ネットワーク管理者**：ネットワーク管理者は、管理設定の変更を除き、完全な表示および変更の権限を持っています。これらのデバイスで設定されているデバイスとポリシーを検出し、デバイスにポリシーを割り当て、デバイスにコマンドを発行できます。ネットワーク管理者はアクティビティや導入ジョブを承認できません。ただし、他のユーザが承認したジョブを導入できます。
5. **システム管理者**：システム管理者は、変更、ポリシー割り当て、アクティビティとジョブの承認、検出、導入、デバイスへのコマンドの発行など、すべてのSecurity Manager権限に完全にアクセスできます。

注：サーバに追加のアプリケーションがインストールされている場合、エクスポートデータなどの追加の役割がCommon Servicesに表示されることがあります。エクスポートデータの役割はサードパーティの開発者向けで、Security Managerでは使用されません。

ヒント： CiscoWorksロールの定義は変更できませんが、各ユーザに割り当てるロールを定義できます。詳細については、「CiscoWorks Common Servicesのユーザへのロールの割り当て」を参照してください。

CiscoWorks Common Servicesのユーザへのロールの割り当て

CiscoWorks Common Servicesでは、各ユーザに割り当てるロールを定義できます。ユーザのロール定義を変更することで、このユーザがSecurity Managerで実行できる操作のタイプを変更できます。たとえば、ヘルプデスクの役割を割り当てた場合、ユーザは表示操作に制限され、データを変更できません。ただし、ネットワークオペレータの役割を割り当てると、ユーザは設定アーカイブを変更することもできます。各ユーザに複数のロールを割り当てることができます。

注意：ユーザーのアクセス許可を変更した後は、セキュリティマネージャーを再起動する必要があります。

手順：

1. Common Servicesで、「サーバー」>「セキュリ**ティ」を選択**し、目次から「**単一サーバーの信頼管理」>「ローカルユーザーの設定」**を選択します。**ヒント： Security Managerから[Local User Setup]ページにアクセスするには**、[Tools] > [Security Manager Administration] > [Server Security]を選択し、[Local User Setup]をクリックします。
2. 既存のユーザーの横にあるチェックボックスをオンにし、「編集」をクリ**ックします。**
3. [ユーザ情報(User Information)]ページで、チェックボックスをクリックして、このユーザに割り当てるロールを選択します。各役割の詳細については、『CiscoWorks Common Services Default Roles』を参照してください。
4. 「**OK**」をク**リック**して、変更を保存します。
5. セキュリティマネージャを再起動します。

Cisco Secure ACSの役割について

Cisco Secure ACSは、Security Managerの権限をCiscoWorksよりも柔軟に管理できます。これは、設定可能なアプリケーション固有の権限をサポートするためです。各ロールは、セキュリティマネージャタスクの許可レベルを決定する一連の権限で構成されます。Cisco Secure ACSでは、各ユーザグループにロールを割り当てます（オプションで個々のユーザにもロールを割り当てることができます）。これにより、そのグループ内の各ユーザは、そのロールに対して定義された権限によって承認された操作を実行できます。

さらに、これらのロールをCisco Secure ACSデバイスグループに割り当てることで、アクセス許可をさまざまなデバイスセットで区別できます。

注：Cisco Secure ACSデバイスグループは、Security Managerデバイスグループから独立しています。

次のトピックでは、Cisco Secure ACSの役割について説明します。

- Cisco Secure ACSのデフォルトロール

- Cisco Secure ACSロールのカスタマイズ

Cisco Secure ACSのデフォルトロール

Cisco Secure ACSには、CiscoWorksと同じロール(「CiscoWorksロールについて」を参照)に加え、次の追加ロールが含まれています。

1. **セキュリティ承認者**：セキュリティ承認者は、デバイス、ポリシー、オブジェクト、マップ、CLIコマンド、および管理設定を表示（変更はできません）できます。さらに、セキュリティ承認者は、アクティビティに含まれる設定変更を承認または拒否できます。導入ジョブを承認または拒否したり、導入を実行したりすることはできません。
2. **セキュリティ管理者**：表示権限に加えて、セキュリティ管理者はデバイス、デバイスグループ、ポリシー、オブジェクト、およびトポロジマップを変更できます。また、デバイスとVPNトポロジにポリシーを割り当て、検出を実行して新しいデバイスをシステムにインポートすることもできます。
3. **ネットワーク管理者**：権限の表示に加えて、ネットワーク管理者は設定アーカイブの変更、導入の実行、デバイスへのコマンドの発行を行うことができます。

注：Cisco Secure ACSネットワーク管理者ロールに含まれる権限は、CiscoWorksネットワーク管理者ロールに含まれる権限とは異なります。詳細については、「CiscoWorksの役割について」を参照してください。

CiscoWorksとは異なり、Cisco Secure ACSでは、各Security Managerロールに関連付けられた権限をカスタマイズできます。デフォルトのロールの変更の詳細については、「Cisco Secure ACSロールのカスタマイズ」を参照してください。

注：Security Managerの認証には、Cisco Secure ACS 3.3以降をインストールする必要があります。

Cisco Secure ACSロールのカスタマイズ

Cisco Secure ACSでは、各Security Managerロールに関連付けられた権限を変更できます。また、特定のSecurity Managerタスクを対象とした権限を持つ専用のユーザロールを作成して、Cisco Secure ACSをカスタマイズすることもできます。

注意：ユーザーのアクセス許可を変更した後は、セキュリティマネージャーを再起動する必要があります。

手順：

1. Cisco Secure ACSで、ナビゲーションバーの**Shared Profile Components**をクリックします。
2. [Shared Components]**ページで[Cisco Security Manager]**をクリックします。セキュリティマネージャに設定されているロールが表示されます。
3. 次のいずれかを実行します。ロールを作成するには、[追加]をクリ**ックします**。ステップ 4 に進みます。既存のロールを変更するには、ロールをクリックします。手順 5 に進みます。
4. ロールの名前と、必要に応じて説明を入力します。
5. 権限ツリーのチェックボックスをオンまたはオフにして、このロールの権限を定義しますツリーの分岐のチェックボックスをオンにすると、その分岐のすべての権限が選択されます。たとえば、[割り当て]を選択**すると**、すべての割り当て権限が選択されます。Security

Managerの権限の完全なリストについては、Security Managerの権限を参照してください。
注：変更、承認、割り当て、インポート、制御、またはデプロイ権限を選択する場合は、対応するビュー権限も選択する必要があります。そうしないと、セキュリティマネージャが正しく機能しません。

6. [Submit] をクリックして、変更内容を保存します。
7. セキュリティマネージャを再起動します。

セキュリティマネージャの権限とロールのデフォルトの関連付け

次の表に、Security ManagerのCiscoWorks Common ServicesのロールおよびCisco Secure ACSのデフォルトロールにどのように関連付けられているかを示します。

権限	ロール							
	System Admin	Security Admin (ACS)	セキュリティ承認者 (ACS)	ネットワーク管理者 (CW)	ネットワーク管理者 (ACS)	承認者	ネットワークオペレータ	ヘルプデスク
権限の表示								
デバイスの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ポリシーの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
オブジェクトの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
トポロジの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLIの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
管理者の表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
構成アーカイブの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
デバイスマネージャの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
権限の変更								
デバイスの変更	Yes	Yes	No	Yes	No	No	No	No
階層の変更	Yes	Yes	No	Yes	No	No	No	No

ポリシーの変更	Yes	Yes	No	Yes	No	No	No	No
イメージの変更	Yes	Yes	No	Yes	No	No	No	No
オブジェクトの修正	Yes	Yes	No	Yes	No	No	No	No
トポロジの変更	Yes	Yes	No	Yes	No	No	No	No
管理者の変更	Yes	No	No	No	No	No	No	No
構成アーカイブの変更	Yes	Yes	No	Yes	Yes	No	Yes	No
追加の権限								
ポリシーの割り当て	Yes	Yes	No	Yes	No	No	No	No
ポリシーの承認	Yes	No	Yes	No	No	No	No	No
CLIの承認	Yes	No	No	No	No	Yes	No	No
検出（インポート）	Yes	Yes	No	Yes	No	No	No	No
展開	Yes	No	No	Yes	Yes	No	No	No
Control	Yes	No	No	Yes	Yes	No	Yes	No
Submit	Yes	Yes	No	Yes	No	No	No	No

関連情報

- Cisco Security Manager のサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems