ファイアウォール デバイスでのデバイス アクセスの設定

ポリシーセレクタの [Device Admin] フォルダの下にある [Device Access] セクションには、ファイアウォール デバイスへのアクセスを定義するためのページがあります。

この章は次のトピックで構成されています。

コンソール タイムアウトの設定

[Console] ページを使用して、非アクティブなコンソール セッションのタイムアウト値を指定します。指定した時間制限に達した場合は、コンソール セッションが終了します。

[コンソールタイムアウト（Console Timeout）] フィールドに、コンソールセッションがデバイスによって閉じられる前にアイドル状態でいられる時間（分単位）を入力します。有効値は、0 ～ 60 分です。コンソールセッションがタイムアウトにならないようにするには、0 を入力します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [コンソール（Console）] を選択します。

- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [コンソール（Console）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[HTTP] ページ

[HTTP] ページのテーブルを使用して、デバイス上の HTTP サーバにアクセスするように設定されたインターフェイスと、それらのインターフェイスでの HTTP から HTTPS へのリダイレクトを管理します。このページから、デバイス上の HTTP サーバをイネーブルまたはディセーブルにすることもできます。特定のデバイス マネージャから管理者アクセスを行うには、HTTPS アクセスが必要です。

（注） HTTP をリダイレクトするには、インターフェイスに HTTP を許可するアクセス リストが必要です。このアクセス リストがないと、インターフェイスはポート 80、または HTTP 用に設定した他のポートをリッスンできません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 1 : [HTTP] ページ

要素	説明
[HTTP Interface] テーブル	このテーブルの [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、HTTP-to-HTTPS リダイレクトが設定されているデバイス インターフェイスを管理します。[Add Row] および [Edit Row] を使用すると、[HTTP Configuration] ダイアログボックス （5 ページ）が開きます。

要素	説明
[証明書からユーザー名を取得（Fetch user name from certificate）] 設定	このオプションを選択して、証明書からユーザー名を抽出するためのルールを設定します。次を入力します。 • [証明書からのHTTPユーザー名を有効にする（Enable HTTP username from certificate）]：このボックスをオンにして、認証用に証明書からHTTP ユーザー名を取得します。 • [ユーザー名の事前入力（Prefill Username）]：認証に対するこの名前の使用をイネーブルにするには、[ユーザー名の事前入力（Prefill Username）] チェックボックスをオンにします。イネーブルの場合は、このユーザ名が、ユーザが入力したパスワードと一緒に認証に使用されます。 次のいずれかのオプションを選択します。 （注） この機能は、ASA ソフトウェア バージョン 9.4(1) 以降を実行しているデバイスでのみサポートされています。 • [DN全体をユーザー名として使用（Use the entire DN as the username）]：DN 全体をユーザー名として使用する場合、このオプションを選択します。このオプションはデフォルトでは無効になっています。

要素	説明
[証明書からユーザー名を取得（Fetch user name from certificate）] 設定（続き）	• [個々のDNフィールドをユーザー名として指定（Specify Individual DN fields as the Username）]：ユーザー名の抽出に使用する属性と追加の属性を指定する値を [プライマリDNフィールド（Primary DN Field）] ドロップダウンと [セカンダリDNフィールド（Secondary DN Field）] ドロップダウンから選択します。このオプションは、デフォルトで有効です。 • C：国：ISO 3166 国名コードに準拠する 2 文字の国名コード。 • CN：一般名：個人やシステムなどのエンティティの名前。セカンダリ属性としては使用できません。 • DNQ：ドメイン名修飾子。 • EA：電子メール アドレス。 • GENQ：世代修飾子。 • GN：名。 • I：イニシャル。 • L：地名：組織が所在する市または町。 • N：名前。 • O：組織：会社、団体、機関、協会などのエンティティの名前。 • OU：組織単位：組織（O）内のサブグループ。 • SER：シリアル番号。 • SN：姓。 • SP：州/都道府県：組織が所在する州または都道府県。 • T：肩書き。 • UID：ユーザ識別子。 • UPN：ユーザ プリンシパル名。 • [ASDMによって生成されたLUAスクリプトを使用（Use LUA Script generated by ASDM）]：ASDM によって生成された LUA スクリプトを使用する場合は、このオプションを選択します。このオプションはデフォルトでは無効になっています。
Enable HTTP Server	デバイス上で HTTP サーバをイネーブルまたはディセーブルにします。イネーブルになっている場合は、サーバーの通信用 [ポート（Port）] を指定できます。ポートの範囲は 1 ～ 65535 です。デフォルトは 443 です。

[HTTP Configuration] ダイアログボックス

[HTTP Configuration] ダイアログボックスを使用して、特定のインターフェイスを介してデバイス上のHTTPサーバへのアクセスを許可されるホストまたはネットワークを追加または編集します。HTTP リダイレクトをイネーブルおよびディセーブルにすることもできます。

ナビゲーション パス

[HTTP Configuration] ダイアログボックスには、[HTTP] ページ （2 ページ）からアクセスできます。

フィールド リファレンス

表 *2 : [HTTP Configuration]* ダイアログボックス

要素	説明
Interface Name	デバイス上のHTTPサーバへのアクセスが許可されるインターフェイスを入力または選択します。 （注） Cisco Security Manager バージョン 4.17 以降、ASA 9.9.2 デバイス以降で HTTP の BVI インターフェイスを設定できます。ただし、マルチコンテキストでは、「トランスペアレント」モードのセキュリティコンテキストは BVI インターフェイスのみをサポートします。
IP Address/Netmask	デバイスとのHTTP接続の確立を許可されるホストまたはネットワークのIPアドレスとネットマスクをスラッシュ（「/」）で区切って入力します。または、[Select] をクリックして、ネットワーク/ホストオブジェクトを選択できます。 （注） バージョン 4.13 以降、Cisco Security Manager は、IPv6 デバイスのポリシー（グループ、ホスト、アドレスの範囲、およびネットワーク）をサポートします。
Enable Authentication Certificate	このオプションは、HTTP接続を確立するためにユーザ証明認証を要求する場合に選択します。ASA および PIX 8.0(2) 以降のデバイスでは、認証**ポート**を指定できます。
証明書マップ（Certificate Maps）	[リモートアクセスVPN（Remote Access VPN）]>[証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）]>[ルール（Rules）] で設定した証明書マップ名を選択します。詳細については、[Map Rule] ダイアログボックス（上半分のテーブル）を参照してください。デフォルトでは [None] が選択されています。 この機能は、ASA 9.6(2) 以降のデバイスの Cisco Security Manager バージョン 4.12 以降で使用できます。このオプションは、ASA デバイスのシングル、マルチ、ルーテッド、およびトランスペアレント コンテキストでサポートされています。

要素	説明
Redirect port	セキュリティ アプライアンスが HTTPS にリダイレクトする HTTP 要求をリッスンするポート。HTTP リダイレクトをディセーブルにするには、このフィールドがブランクであることを確認します。

ICMP の設定

[ICMP] ページのテーブルを使用して、インターネット制御メッセージプロトコル（ICMP）規則を管理します。この規則では、セキュリティデバイス上の特定のインターフェイスへの ICMP アクセスを許可または拒否するすべてのホストまたはネットワークのアドレスを指定します。

（注） ASA 8.2(1) 以降、ICMP IPv6 はトランスペアレント ファイアウォール モードでサポートされるようになりました。

ICMP ルールでは、任意のデバイス インターフェイス上で終了する ICMP トラフィックを制御します。ICMP 制御リストが設定されていない場合、デバイスは、外部インターフェイスを含む任意のインターフェイスで終了するすべての ICMP トラフィックを受け入れます。ただし、デフォルトでは、デバイスはブロードキャストアドレスに送信された ICMP エコー要求に応答しません。

ICMP Unreachable メッセージ（タイプ 3）は常に許可することを推奨します。ICMP Unreachable メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになり、IPsec および PPTP トラフィックが停止することがあります。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

ICMP 制御リストが設定されている場合、デバイスは ICMP トラフィックとの最初の一致を使用し、続いて暗黙的な deny all を使用します。つまり、最初に一致したエントリが許可エントリの場合は、ICMP パケットの処理を継続します。最初に一致したエントリが拒否エントリの場合、またはエントリが一致しない場合、デバイスは ICMP パケットを廃棄し、syslog メッセージを生成します。ICMP 制御リストが設定されていない場合は、すべてのケースで許可ルールが想定されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ICMP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ICMP]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） ICMP IPv6 サポートは、PIX および FWSM デバイスでは使用できません。

フィールド リファレンス

表 3 : *[ICMP]* ページ

要素	説明
[ICMP Rules] テーブル	このテーブルの下にある [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、ICMP ルールを管理します。[Add Row] を選択すると、[Add ICMP] ダイアログボックスが開きます。[Edit Row] を選択すると、[Edit ICMP] ダイアログボックスが開きます。これらのダイアログボックスについては、[Add ICMP]/[Edit ICMP] ダイアログボックス（7 ページ）を参照してください。
ICMP Unreachable Parameters	
レート制限	このデバイス上のインターフェイスで終了する ICMP トラフィックについて、デバイスが 1 秒間に転送できる ICMP Unreachable メッセージの最大数です。この値は、1 ～ 100 メッセージ/秒です。デフォルトは 1 メッセージ/秒です。
バースト サイズ	ICMP Unreachable メッセージのバースト サイズ。1 ～ 10 の値を指定できます。 （注） このパラメータは、現在システムでは使用されていないため、任意の値を選択できます。

[Add ICMP]/[Edit ICMP] ダイアログボックス

[Add ICMP] ダイアログボックスを使用して、ICMP ルールを追加します。このルールでは、指定したデバイス インターフェイス上で指定した ICMP アクセスを許可または拒否されるホスト/ネットワークを指定します。

（注） [Edit ICMP] ダイアログボックスは、事実上 [Add ICMP] ダイアログボックスと同じであり、既存の ICMP ルールの修正に使用します。次の説明は、両方のダイアログボックスに適用されます。

ナビゲーション パス

[Add ICMP]/[Edit ICMP] ダイアログボックスには、ICMP の設定 （6 ページ）からアクセスできます。

（注） ICMPポリシーを追加するときは、ネットワークとサービスが同じタイプであること、つまり、IPv6 ネットワークが IPv6 サービスをサポートしていることを確認してください。

フィールド リファレンス

表 *4 : [Add ICMP]/[Edit ICMP]* ダイアログボックス

要素	説明
操作	このルールによって、指定したインターフェイス上の指定したネットワークからの選択した ICMP サービス メッセージが許可されるか、または拒否されるか。次のどちらかを選択します。 • [許可（Permit）] : 指定したネットワーク/ホストからの ICMP メッセージは、指定したインターフェイスに対して許可されます。 • [拒否（Deny）] : 指定したネットワーク/ホストから指定したインターフェイスへの ICMP メッセージはドロップされます。
ICMP Service	ルールを適用する特定の ICMP サービス メッセージを入力または選択します。
インターフェイス	これらの ICMP メッセージの送信先のデバイス インターフェイスを入力または選択します。
ネットワーク（Network）	ホスト名、 IPv4 または IPv6 アドレスを入力するか、ネットワーク/ホストオブジェクトを選択して、指定した ICMP メッセージの送信元を定義します。

管理アクセスの設定

[Management Access] ページを使用して、高セキュリティ インターフェイスへのアクセスをイネーブルまたはディセーブルにして、デバイスに対して管理機能を実行できるようにします。内部インターフェイスでこの機能をイネーブルにして、IPsec VPN トンネル上のインターフェイスで管理機能を実行可能にできます。管理アクセス機能は、一度に1つのインターフェイスでだけイネーブルにすることができます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）]> [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [管理アクセス（Management Access）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス**

（**Device Access**）] > [**管理アクセス（Management Access**）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

管理アクセスのイネーブル化とディセーブル化

[管理アクセスインターフェイス（Management Access Interface）] フィールドで、管理アクセス接続を許可するデバイスインターフェイスの名前を入力します。[Select] をクリックすると、インターフェイス オブジェクトのリストからインターフェイスを選択できます。

管理アクセス機能は、一度に 1 つのインターフェイスでだけイネーブルにすることができます。

管理アクセスをディセーブルにするには、[Management Access Interface] フィールドをクリアします。

管理セッションクォータの制限の設定

4.19 以降、Cisco Security Manager では、すべての接続タイプおよびユーザー名にわたる管理セッションの最大数とユーザー名ごとの同時セッションの最大数に加えて、ASA 9.12(1) 以降のデバイスでのプロトコルごとの制限の適用を設定できます。設定された同時セッション制限は、着信管理セッションを認証する前に適用されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [管理セッションクォータ（Management Session Quota）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [管理セッションクォータ（Management Session Quota）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） セッション制限の適用順序は、ユーザー制限、集約制限、プロトコルごとの制限の順です。

フィールド リファレンス

表 5 : [Add ICMP]/[Edit ICMP] ダイアログボックス

要素	説明
アグリゲート	すべての接続タイプにわたる管理セッションの最大数。デフォルトは 15 です。制限は 1 ～ 15 の範囲で設定できます。

要素	説明
HTTP	HTTP の管理セッションクォータ制限を 1 ～ 5 の範囲で入力します。デフォルト値は 5 です。
SSH	SSH の管理セッションクォータ制限を 1 ～ 5 の範囲で入力します。デフォルト値は 5 です。
Telnet	Telnet の管理セッションクォータ制限を 1 ～ 5 の範囲で入力します。デフォルト値は 5 です。
ユーザー（User）	ユーザーの管理セッションクォータ制限を 1 ～ 5 の範囲で入力します。ユーザー制限のデフォルト値は指定されていません。

セキュア シェル アクセスの設定

[Secure Shell] ページを使用して、SSH プロトコルを使用したセキュリティ デバイスへの管理アクセスを許可するルールを設定します。ルールでは、特定の IP アドレスとネットマスクへの SSH アクセスが制限されます。これらのルールに準拠する任意の SSH 接続試行は、AAA サーバまたは Telnet パスワードによって認証される必要があります。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 6 : [Secure Shell] ページ

要素	説明
SSH Version	デバイスによって受け入れられる SSH バージョンを指定します。**1**、**2**、または **1 と 2** を選択します。デフォルトでは、SSH バージョン 1 接続および SSH バージョン 2 接続が受け入れられます。
タイムアウト（Timeout）	セキュア シェル セッションがデバイスによって閉じられる前にアイドル状態でいられる時間（分単位）を 1 ～ 60 で入力します。デフォルト値は 5 分です。

要素	説明
[Allowed Hosts] テーブル	このテーブルの下にある [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、SSH を介したセキュリティ デバイスへの接続を許可するホストを管理します。[Add Row] を選択すると、[Add Host] ダイアログボックスが開きます。[Edit Row] を選択すると、[Edit Host] ダイアログボックスが開きます。これらのダイアログボックスについては、[Add SSH Host]/[Edit SSH Host] ダイアログボックス （11 ページ）を参照してください。
Enable Secure Copy	このボックスをオンにして、セキュリティ アプライアンス上の Secure Copy（SCP; セキュア コピー）サーバをイネーブルにします。これにより、アプライアンスはデバイスとの間でファイルを転送するための SCP サーバとして機能できます。SSH を使用したセキュリティ アプライアンスへのアクセスを許可されるクライアントだけが、セキュア コピー接続を確立できます。 セキュア コピー サーバのこの実装には、次の制限があります。 • サーバはセキュア コピーの接続を受け入れまたは終了できますが、開始はできません。 • サーバーにはディレクトリ サポートがありません。ディレクトリ サポートがないため、セキュリティ アプライアンスの内部ファイルへのリモート クライアント アクセスが制限されます。 • サーバではバナーがサポートされません。 • サーバではワイルドカードがサポートされません。 • セキュリティ アプライアンス ライセンスには、SSH バージョン 2 接続をサポートするための VPN-3DES-AES 機能が必要です。

[Add SSH Host]/[Edit SSH Host] ダイアログボックス

[Add SSH Host] ダイアログボックスを使用して、SSH アクセス ルールを追加します。

（注） [Edit Host] ダイアログは、事実上 [Add Host] ダイアログボックスと同じであり、既存の SSH アクセス ルールの修正に使用されます。次の説明は、両方のダイアログボックスに適用されます。

ナビゲーション パス

[Add Host]/[Edit Host] ダイアログボックスには、セキュア シェル アクセスの設定 （10 ページ）からアクセスできます。

フィールド リファレンス

表 *7 : [Add Host]/[Edit Host]* ダイアログボックス

要素	説明
インターフェイス（Interface）	SSH接続が許可されるデバイスインターフェイスの名前を入力または選択します。 （注） Cisco Security Manager バージョン 4.17 以降、ASA 9.9.2 デバイス以降で SSH 接続の BVI インターフェイスを設定できます。ただし、マルチコンテキストでは、「トランスペアレント」モードのセキュリティコンテキストは BVI インターフェイスのみをサポートします。
IP Addresses	指定したインターフェイス上のセキュリティ デバイスとの SSH 接続の確立を許可される各ホストまたはネットワークの名前またはIPアドレスを入力します。複数のエントリを区切るにはカンマを使用します。[Select] をクリックして、リストからネットワーク/ホスト オブジェクトを選択することもできます。 （注） バージョン 4.13 以降、Cisco Security Manager は、IPv6 デバイスのポリシー（グループ、ホスト、アドレス範囲、およびネットワーク）をサポートします。

SSL 設定：[基本（Basic）] タブと [詳細（Advanced）] タブ

バージョン 4.8 以降、Security Manager は、セキュアソケットレイヤ（SSL）を使用して強化されたセキュリティ機能を提供します。

[デバイスアクセス（Device Access）] で SSL を設定するには、[CSM管理（CSM Admin）] > [ポリシー管理（Policy Management）] で SSL を有効にしてください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SSL] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SSL] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *8 : [SSL]* ページの *[*基本（*Basic*）*]* タブ

要素	説明
証明書認証	
[FCAタイムアウト（FCA Timeout）]	1 ～ 120 の範囲で値を入力します。 （注） FCA タイムアウトは、ASA ソフトウェアバージョン 9.1(2) 以降を実行しているデバイスに適用されます。
インターフェイス	[インターフェイス（Interface）] テーブルの下にある [行の追加（Add Row）]、[行の編集（Edit Row）]、および [行の削除（Delete Row）] ボタンを使用して、SSL を介したセキュリティデバイスへの接続を許可するインターフェイスとそのポート番号を管理します。[行の追加（Add Row）] を選択すると、[ホストの追加（Add Host）] ダイアログボックスが開きます。[行の編集（Edit Row）] を選択すると、[ホストの編集（Edit Host）] ダイアログボックスが開きます。[インターフェイスセレクタ（Interface Selector）] ダイアログボックスの利用可能なエントリからインターフェイスを選択できます。ポート番号は 1 ～ 65535 の範囲で入力してください。
クライアント バージョン（Client Version） [SSL/TLSプロトコルバージョン（SSL/TLS Protocol Version）]	[クライアントバージョン（Client Version）] は、デバイスがクライアントとして機能するときに使用する SSL/TLS プロトコルのバージョンです。次のオプションのいずれかを選択します。 • [任意（Any）]：このキーワードを選択すると、SSLv3 クライアントの hello が送信され、SSLv3 以降 がネゴシエートされます。これがデフォルトのキーワードです。 • [SSLV3]：このキーワードを入力すると、SSLv3 クライアントの hello が送信され、SSLv3 以降 がネゴシエートされます。 • [TLSV1]：このキーワードを入力すると、TLSv1 クライアントの hello が送信され、TLSv1 以降 がネゴシエートされます。 • [TLSV1.1]：このキーワードを入力すると、TLSv1.1 クライアントの hello が送信され、TLSv1.1 以降 がネゴシエートされます。 • [TLSV1.2]：このキーワードを入力すると、TLSv1.2 クライアントの hello が送信され、TLSv1.2 以降 がネゴシエートされます。 （注） TLSV1.1 および TLSV1.2 プロトコルバージョンは、ASA ソフトウェアバージョン 9.3(2) 以降を実行しているデバイスに適用できます。

要素	説明
サーバー バージョン [SSL/TLSプロトコルバージョン（SSL/TLS Protocol Version）]	[サーバーバージョン（Server Version）] は、デバイスがサーバーとして機能するときに使用する SSL/TLS プロトコルの最小バージョンです。次のオプションのいずれかを選択します。 • [任意（Any）]：このキーワードを選択すると、SSLv2 クライアントの hello が受け入れられ、共通の最新バージョンがネゴシエートされます。これがデフォルトのキーワードです。 • [SSLV3]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、SSLv3 以降 がネゴシエートされます。 • [SSLV3-Only]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、SSLv3 以降 がネゴシエートされます。 • [TLSV1]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、TLSv1 以降 がネゴシエートされます。 • [TLSV1-Only]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、TLSv1 以降 がネゴシエートされます。 • [TLSV1.1]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、TLSv1.1 以降 がネゴシエートされます。 • [TLSV1.2]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、TLSv1.2 以降 がネゴシエートされます。 **注**： • [任意（Any）] キーワードは、サーバーバージョンとクライアントバージョン両方のデフォルトであり、共通してサポートされている TLS の最新バージョンをデバイスがネゴシエートすることを意味します。 • TLSV1.1 および TLSV1.2 プロトコルバージョンは、ASA ソフトウェアバージョン 9.3(2) 以降を実行しているデバイスに適用できます。 • SSLV3-Only および TLSV1-Only プロトコルバージョンは、9.3(2) より前の ASA ソフトウェアバージョンを実行しているデバイスに適用できます。

表 *9 : [SSL]* ページの *[*詳細（*Advanced*）*]* タブ

要素	説明
9.3(2) より前の ASA ソフトウェアバージョンを実行しているデバイスの詳細な SSL 設定	

要素	説明
暗号化（Encryption）	使用可能なリストから暗号化アルゴリズムを選択します。暗号化アルゴリズムを追加するには、[使用可能なメンバー（Available Members）] リストで項目を選択してから、[>>] をクリックします。項目が [使用可能なメンバー（Available Members）] リストから [選択済みのメンバー（Selected Members）] リストに移動します。複数の暗号化アルゴリズムを追加できます。 使用可能な暗号化アルゴリズムは次のとおりです。 • 3DES-SHA1 • AES128-SHA1 • AES256-SHA1 • DES-SHA1 • RC4-MD5 • RC4-SHA1 • NULL-SHA1 • DHE-AES128-SHA1 • DHE-AES256-SHA1 （注） 4.19 以降、Cisco Security Manager は、ASA 9.12(1) 以降のデバイスの SSL 暗号で NULL SHA1 を使用した TLS プロキシの設定をサポートしていません。 暗号化アルゴリズムを削除するには、[選択済みのメンバー（Selected Members）] リストで項目を選択してから、[<<] をクリックします。項目が [選択済みのメンバー（Selected Members）] リストから [使用可能なメンバー（Available Members）] リストに移動します。 [Save] をクリックして設定を保存します。
ASA ソフトウェアバージョン 9.3(2) 以降を実行しているデバイスの詳細な SSL 設定	
SSL Cipher	[SSL暗号（SSL Cipher）] テーブル下の [行の追加（Add Row）]、[行の編集（Edit Row）]、および [行の削除（Delete Row）] ボタンを使用して、SSL 暗号のバージョンとレベルを管理します。[暗号の追加（Add Cipher）] ダイアログで、バージョンとレベルの組み合わせを選択します。

要素	説明
バージョン	次のいずれかのバージョンを選択します。 • DEFAULT • DTLSV1 • DTLSV1.2 • SSLV3 • TLSV1 • TLSV1.1 • TLSV1.2 （注） DEFAULT キーワードは、デバイスがクライアントとして動作し、サーバーへの接続を確立しているときに、アウトバウンド接続を設定するために使用されます。他のすべてのキーワードは、デバイスがサーバーとして機能し、クライアントからの接続を受け入れているときに使用されます。 （注） SSLV3 バージョンは、ASA バージョン 9.4(1) 以降廃止されています。そのため、バージョン 4.9 以降、Security Manager は検証を実行して、SSLV3 オプションがバージョン 9.4(1) 以降を実行している ASA デバイスに設定されているかどうかを確認します。
レベル	次のいずれかのバージョンを選択します。 • [All]：NULL-SHA を含むすべての暗号が含まれます。 • [LOW]：NULL-SHA を除くすべての暗号が含まれます。 • [MEDIUM]：NULL-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5 を除くすべての暗号が含まれます。 • [FIPS]：FIPS 準拠のすべての暗号が含まれます（つまり NULL-SHA:DES-CBC-SHA:RC4-MD5:RC4-SHA:DES-CBC3-SHA ではない暗号）。 • [HIGH]：SHA-2 暗号を使用する AES-256 のみが含まれます（TLSv1.2 にのみ適用）。

要素	説明
[カスタム文字列（Custom String）]	Security Manager の CUSTOM キーワードを使用し、OpenSSL 暗号定義文字列を使用して暗号スイートを全面的に制御します。 （注） バージョン 4.9 以降、Security Manager は、ASA ソフトウェアバージョン 9.4(1) 以降を実行しているデバイスに対して、次の新しい TLSV1.2 暗号のサポートを提供します。 • ECDHE_RSA_AES128_SHA256 • ECDHE_RSA_AES256_SHA384 • ECDHE_ECDSA_AES128_SHA256 • ECDHE_ECDSA_AES256_SHA384 （注） バージョン 4.16 以降、Security Manager は、ASA ソフトウェアバージョン 9.4(1) 以降を実行しているデバイスに対し、上記の暗号に加えて、次の新しいTLSV1.2 暗号のサポートを提供します。 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • AES128-GCM-SHA256
[ECDH設定（ECDH Configuration）]	ECDH グループのオプション（19、20、21、なし）のいずれかから選択します。この機能は、ASA デバイスバージョン 9.4(1) 以降の Security Manager バージョン 4.9 以降で使用できます。
[SSL DHグループの設定（SSL DH Group Configuration）]	SSL DH グループのオプション（2、5、14、15、24）のいずれかを選択します。DH グループ 14 がデフォルトで使用されます。ASA 9.16(1) 以降のデバイスでは、SSL DH グループで DH グループ 15 を使用できるようになりました。 （注） Cisco Security Manager 4.23 以降、DH グループ 2、5、および 24 は、ASA 9.16(1) 以降のデバイスの SSL DH グループではサポートされません。

（注） 一部の国では輸入規制があるため、Oracleの展開では、暗号化アルゴリズムの強度を制限するデフォルトの暗号管轄ポリシーファイルが提供されています。より強力なアルゴリズムを設定する必要がある場合や、デバイスですでに設定されている場合（たとえば、256 ビットキーを使用する AES、5、14、24 を使用する DH グループなど）は、次の手順に従います。

1. Java 7 の無制限強度の暗号ポリシー .jar ファイルを http://www.oracle.com からダウンロードします。シスコは Oracle の Web サイトで次を検索することを推奨しています。

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files Java 7

（[ダウンロード（download）] ボタンをクリックして、ライセンス契約に同意し、ファイルをダウンロードします。）

1. Security Manager サーバーの CSCOpx\MDC\vms\jre\lib\security フォルダにある local_policy.jar および US_export_policy.jar を置き換えます。
2. Security Manager サーバーを再起動します。

参照 ID

バージョン 4.12 以降、Security Manager を使用すると、ASA ソフトウェアバージョン 9.6(2) 以降を実行しているデバイスでセキュアな Syslog サーバー接続用の参照 ID ポリシーオブジェクトを設定できます。このオブジェクトは、コモンクライテリア要件のサポートを有効にします。

参照 ID は、サーバー証明書で示された ID と比較される 1 つ以上の ID として設定されます。ID は、RFC 6125 で定義されている 4 つの ID タイプの特定のインスタンスです。

[参照 ID の追加/編集（Add/Edit Reference Identity）] ダイアログボックス

新しい参照 ID ポリシーオブジェクトを作成したり既存のポリシーオブジェクトを編集するには、[参照 ID の追加/編集（Add/Edit Reference Identity）] ダイアログボックスを使用します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [参照 ID（Reference Identity）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object] を選択するか [+] ボタンをクリックして新しいオブジェクトを追加するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 *10 : [参照 ID の追加/編集（Add/Edit Reference Identity）] ダイアログボックス*

要素	説明
名前	参照 ID ポリシーオブジェクトの名前。各参照 ID は複数の行の値を持つことができることに注意してください。
説明	参照 ID ポリシーオブジェクトの説明。

要素	説明
[共通名 ID（Common Name ID）]	証明書のサブジェクトフィールドに設定される、共通名（CN）タイプの 1 つの属性タイプと値のペアだけが含まれる相対識別名（RDN）。この値は、完全な形のドメイン名と一致します。CN 値は自由形式のテキストにできません。CN-ID 参照 ID では、アプリケーション サービスは特定されません。
[ドメイン名 ID（Domain Name ID）]	タイプ dNSName の subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。
[サービス名 ID（Service Name ID）]	RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。
[ユニフォーム リソース識別子 ID（Uniform Resource Identifier ID）]	タイプ uniformResourceIdentifier の subjectAltName エントリです。この値には、「scheme」コンポーネントと、RFC 3986 に定義されている「reg-name」ルールに一致する「host」コンポーネント（またはこれに相当するコンポーネント）の両方が含まれます。URI-ID 識別子には、IP アドレスではなく、およびホスト名だけではなく、DNS ドメイン名を含める必要があります。たとえば、「sip:voice.example.edu」という URI-ID は、DNS ドメイン名の「voice.example.edu」とアプリケーション サービス タイプの「sip」に分割できます。
カテゴリ	（任意）CAT-A ～ CAT-J の間でカテゴリを選択します。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[Edit] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[Overrides] フィールドは、このオブジェクトに対するオーバーライドを持つデバイスの数を示します。

（注） 参照 ID は、未使用の名前を設定すると作成されます。参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

SNMP の設定

簡易ネットワーク管理プロトコル（SNMP）は、PC またはワークステーションで実行されているネットワーク管理ステーションが、スイッチ、ルータ、セキュリティアプライアンスなどのさまざまなタイプのデバイスのヘルスとステータスをモニターするための標準的な方法を定義します。[SNMP] ページを使用して、SNMP 管理ステーションによってモニタされるようにファイアウォール デバイスを設定できます。

簡易ネットワーク管理プロトコル（SNMP）は、集中管理する場所からのネットワーク デバイスのモニタリングをイネーブルにします。Cisco セキュリティ アプライアンスでは、SNMP バージョン 1、2c、および 3 を使用したネットワーク モニタリングに加えて、トラップおよび SNMP 読み取りアクセスがサポートされます。SNMP 書き込みアクセスはサポートされません。

ネットワーク管理ステーション（NMS）に「トラップ」（イベント通知）を送信するようにセキュリティアプライアンスを設定したり、NMS を使用してセキュリティアプライアンス上の Management Information Base（MIB）を参照したりできます。CiscoWorks for Windows またはその他の任意の SNMP MIB-II 対応ブラウザを使用して、SNMP トラップを受信し、MIB を参照します。

セキュリティアプライアンスには、指定したイベントが発生した場合（たとえばネットワーク上のリンクが起動またはダウンした場合）に指定した管理ステーションに通知する SNMP エージェントがあります。通知には、管理ステーションに対してデバイスを識別する SNMP システム Object ID（OID; オブジェクト ID）が含まれます。セキュリティ アプライアンス SNMP エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP MIB および OID

SNMP トラップは、ネットワーク デバイスで発生した重要イベント（ほとんどの場合はエラーまたは障害）をレポートします。SNMP トラップは、標準またはエンタープライズ固有の管理情報ベース（MIB）で定義されています。

標準トラップと MIB は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって作成され、各種 RFC に文書化されています。標準トラップは、セキュリティ アプライアンス ソフトウェアにコンパイルされます。必要に応じて、RFC、標準 MIB、および標準トラップを IETF Web サイト http://www.ietf.org/ からダウンロードできます。

Cisco MIB ファイルおよび OID については、http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml を参照してください。OID は、FTP サイト ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz からダウンロードできます。

ここでは、次の内容について説明します。

SNMP の用語

一般的な SNMP 用語の定義をいくつか示します。

- **エージェント**：セキュリティアプライアンス上で実行されている SNMP サーバー。エージェントは情報の要求と管理ステーションからのアクションに応答します。エージェントは、管理情報ベース（MIB）（SNMP マネージャから表示または変更できるデータ オブジェクトの集合）へのアクセスも制御します。
- **管理ステーション**：SNMPイベントをモニターし、セキュリティアプライアンスなどのデバイスを管理するように設定されたPCまたはワークステーション。管理ステーションは、ハードウェア障害など、対処する必要のあるイベントに関するメッセージも受信できます。
- **MIB**：エージェントは、Management Information Base（MIB）と呼ばれる標準化されたデータ構造をメンテナンスします。MIBは、パケット、接続カウンタ、エラーカウンタ、バッファ使用状況、フェールオーバーステータスなどの情報の収集に使用されます。MIBの番号は、特定の製品、およびほとんどのネットワーク デバイスで使用される共通プロトコルとハードウェア規格に対して定義されています。SNMP管理ステーションでは、MIBを参照したり、特定のフィールドだけを要求したりできます。一部のアプリケーションでは、管理の目的で MIB データを修正できます。
- **OID**：SNMP 標準ではシステムオブジェクト ID（OID）が割り当てられるため、管理ステーションがSNMPエージェントでネットワークデバイスを一意に識別したり、監視および表示される情報のソースをユーザーに示したりできます。
- **トラップ**：SNMPエージェントから管理ステーションへのメッセージを生成する指定されたイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog イベントなどのアラーム条件が含まれます。

SNMP バージョン 3

SNMP バージョン 3 は SNMP バージョン 1 または SNMP バージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバーと SNMP エージェント間でデータをクリア テキストで転送します。SNMP バージョン 3 は認証とプライバシー オプションを追加してプロトコル オペレーションをセキュリティ保護します。また、このバージョンはユーザーベース セキュリティ モデル（USM）とビューベース アクセス コントロール モデル（VACM）を通して SNMP エージェントと MIB オブジェクトへのアクセスをコントロールします。ASA および ASASM は、SNMP グループとユーザーの作成、およびセキュアな SNMP 通信の転送の認証と暗号化をイネーブルにするために必要なホストの作成もサポートします。

（注） SNMP バージョン 3 は、8.2(1) 以降を実行している ASA デバイスおよび 8.5(1) 以降を実行している ASASM デバイスでサポートされています。

セキュリティ モデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティ モデルにまとめられます。セキュリティ モデルはユーザーとグループに適用され、次の 3 つのタイプに分けられます。

- NoAuth：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。
- Auth：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- Priv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザーを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザーは、SNMP グループのセキュリティ モデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

SNMP ユーザー

SNMP ユーザーは、指定されたユーザー名、ユーザーが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES、および AES（128、192、および 256 バージョンで使用可能）です。ユーザーを作成した場合は、それを SNMP グループに関連付ける必要があります。その後、そのユーザーはグループのセキュリティ モデルを継承します。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザーだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザー名を設定する必要があります。SNMP ターゲット IP アドレスとターゲットパラメータ名は ASA および ASA サービスモジュールで一意である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を 1 つだけ持つことができます。SNMP トラップを受信するには、SNMP NMS を設定し、NMS のユーザー クレデンシャルが ASA および ASASM のユーザー クレデンシャルと一致するように設定してください。

ASA、ASA サービスモジュールと Cisco IOS ソフトウェアの導入の相違点

ASA および ASASM での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装と次の点で異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカル エンジン ID は、ASA または ASASM が起動されたとき、あるいはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されます。
- 正しいセキュリティ モデルを使用してユーザーとグループを作成する必要があります。
- 正しい順序でユーザー、グループ、およびホストを削除する必要があります。
- **snmp-server host** コマンドを使用すると、着信 SNMP トラフィックを許可する ASA または ASASM のルールが作成されます。

[SNMP] ページ

[SNMP] ページを使用して、簡易ネットワーク管理プロトコル（SNMP）管理ステーションによってモニタされるようにセキュリティ アプライアンスを設定します。

（注） SNMP バージョン 3 の設定は、グループ、ユーザー、ホストの順に行う必要があります。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP（SNMP）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP（SNMP）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- SNMP の設定 （20 ページ）
- [SNMP Trap Configuration] ダイアログボックス （26 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （31 ページ）
- [SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックス （33 ページ）

- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス（35 ページ）
- [SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （37 ページ）
- [SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックス （41 ページ）

フィールド リファレンス

表 *11 : [SNMP]* ページ

要素	説明
Enable SNMP Servers	このオプションを選択すると、指定したインターフェイスの SNMP 情報がセキュリティ デバイスから提供されます。このオプションの選択を解除すると、設定情報を保持したまま、SNMP モニタリングをディセーブルにできます。
[Read コミュニティ ストリング（Read Community Strin）] 確認（Confirm）	要求をこのデバイスに送信するときに SNMP 管理ステーションで使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。セキュリティデバイスでは、このパスワードを使用して、着信 SNMP 要求が有効かどうかを判断します。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースは使用できません。 [確認（Confirm）] フィールドにパスワードを再度入力し、パスワードが正しく入力されたことを確認します。
System Administrator Name	デバイス管理者またはその他の担当者の名前を入力します。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
参照先	このセキュリティデバイスの場所を記します（**Building 42, Sector 54** など）。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
Port（PIX 7.x、ASA、FWSM 3.x のみ）	着信要求が受け入れられるポートを指定します。デフォルトは 161 です。
SNMP トラップの設定	[SNMP Trap Configuration] ダイアログボックス （26 ページ）で SNMP トラップを設定するには、このボタンをクリックします。

要素	説明
SNMP エンジン ID	デバイスに設定されている SNMP エンジンの ID を表示します。[SNMP エンジンIDの取得（Get SNMP Engine ID）] をクリックして、デバイスからエンジン ID を取得します。
[SNMP Hosts] テーブル	このテーブルには、セキュリティ アプライアンスにアクセスできる SNMP 管理ステーションが一覧表示されます。これは Security Manager の標準のテーブルです。テーブルの使用で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 [Add Row] と [Edit Row] のボタンでは、[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （31 ページ）が開きます。これは管理ステーションのホスト エントリを追加および編集するために使用します。 （注） 9.1(5) 以降を実行している ASA デバイスの場合、最大 129 の SNMP ホストを設定できます。他のデバイスおよび以前の ASA バージョンでは、最大 32 の SNMP ホストのみを設定できます。
SNMP ホストグループテーブル	バージョン 4.12 以降、Security Manager では、SNMP ユーザのホストグループエントリを追加および編集できます。詳細については、[SNMP ホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックス （33 ページ）を参照してください。
SNMPv3 の設定	
SNMP グループタブ	設定されている SNMP グループを一覧表示します。これは Security Manager の標準のテーブルです。テーブルの使用で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 [行の追加（Add Row）] と [行の編集（Edit Row）] ボタンでは、[SNMP グループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （35 ページ）が開きます。これは SNMP グループを追加および編集するために使用します。
SNMP ユーザタブ	設定されている SNMP ユーザをリストします。これは Security Manager の標準のテーブルです。テーブルの使用で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 [行の追加（Add Row）] と [行の編集（Edit Row）] ボタンでは、[SNMP ユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （37 ページ）が開きます。これは SNMP ユーザを追加および編集するために使用します。

要素	説明
SNMPユーザリストタブ	バージョン 4.12 以降、Security Manager では、複数の SNMP ユーザを含むユーザリストを追加できます。詳細については、[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックス （41 ページ）を参照してください。

[SNMP Trap Configuration] ダイアログボックス

[SNMP Trap Configuration] ダイアログボックスを使用して、選択したセキュリティ デバイスの SNMP トラップ（イベント通知）を設定します。

トラップは参照とは異なります。トラップは、生成される**リンクアップイベント**、**リンクダウンイベント**、**Syslog イベント**など、特定のイベントに対する管理対象デバイスから管理ステーションへの割り込み「コメント」です。

デバイスの SNMP オブジェクト ID（OID）は、デバイスから送信される SNMP イベント トラップに表示されます。セキュリティデバイスで実行されている SNMP サービスは、2 つの機能を実行します。

- 管理ステーションからの SNMP 要求に応答します。
- セキュリティ アプライアンスからのトラップを受信するように登録されている管理ステーションまたはその他のデバイスにトラップを送信します。

Cisco セキュリティ デバイスでは、3 種類のトラップがサポートされます。

- ファイアウォール
- generic
- syslog

[SNMP Trap Configuration] ダイアログボックスでは、使用できるトラップが、[Standard]、[Entity MIB]、[Resource]、[Other] の 4 つのタブ付きパネルに表示されます。

ナビゲーション パス

[SNMP Trap Configuration] ダイアログボックスには、[SNMP] ページ （23 ページ）からアクセスできます。

関連項目

- SNMP の設定 （20 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （31 ページ）

フィールド リファレンス

表 *12 : [SNMP Trap Configuration]* ダイアログボックス

要素	説明
Enable All SNMP Traps	4 つすべてのタブ付きパネルをすばやく選択するには、このチェックボックスをオンにします。
Enable Syslog Traps	トラップ関連の Syslog メッセージの送信をイネーブルにするには、このチェックボックスをオンにします。 トラップされる Syslog メッセージの重大度は、[Logging Filters] ページで設定されます。
次の 4 つのタブ付きパネルで、目的のイベント通知トラップを選択します。選択したデバイスに適用できるトラップだけがダイアログボックスに表示されます。	
標準	• [認証（Authentication）] : 未認可の SNMP アクセス。この認証エラーは、間違ったコミュニティ ストリングが付いたパケットによって発生します。 • [リンクアップ（Link Up）] : 通知に示されているとおり、デバイスの通信リンクの 1 つが使用可能になりました。 • [リンクダウン（Link Down）] : 通知に示されているとおり、デバイスの通信リンクの 1 つにエラーが発生しました。 • [コールドスタート（Cold Start）] : デバイスが自動で再初期化しているときに、その設定またはプロトコルエンティティの実装が変更されることがあります。 • [ウォームスタート（Warm Start）] : デバイスが自動で再初期化しているときに、その設定またはプロトコルエンティティの実装が変更されることはありません。

要素	説明
Entity MIB	• [現場交換可能ユニット挿入（Field Replaceable Unit Insert）]：示されているとおり、現場交換可能ユニット（FRU）が挿入されました（FRUには電源装置、ファン、プロセッサ モジュール、インターフェイス モジュールなどの組み立て部品が含まれます）。 • [現場交換可能ユニット除外（Field Replaceable Unit Remove）]：通知に示されているとおり、現場交換可能ユニット（FRU）が取り外されました。 • [設定変更（Configuration Change）]：通知に示されているとおり、ハードウェアに変更がありました。 • [ファン障害（Fan Failure）]：通知に示されているとおり、デバイスの冷却ファンに障害が発生しました。 • [CPU温度（CPU Temperature）]：中央処理装置の温度が、設定した制限に達しました。 • [電源装置障害（Power-Supply Failure）]：通知に示されているとおり、デバイスの電源装置に障害が発生しました。 • [冗長スイッチオーバー（Redundancy Switchover）]：通知に示されているとおり、冗長コンポーネントでスイッチオーバーが発生しました。 • [アラームがアサートされた（Alarm Asserted）]：アラームで示されている状態が存在します。 • [アラームがクリアされた（Alarm Cleared）]：アラームで示されている状態は存在しません。
リソース（Resource）	• [接続制限到達（Connection Limit Reached）]：このトラップは、設定した接続制限に達したため、接続試行が拒否されたことを示します。 • [リソース制限到達（Resource Limit Reached）]：通知に示されているとおり、この通知は設定したリソース制限に達すると生成されます。 • [リソースレート制限到達（Resource Rate Limit Reached）]：通知に示されているとおり、この通知は設定したリソースのレート制限に達すると生成されます。

要素	説明
その他	

要素	説明
	• [IKEv2 開始（IKEv2 Start）]：インターネット キー エクスチェンジ バージョン 2（IKEv2）の交換が起動しました。 • [IKEv2 停止（IKEv2 Stop）]：インターネット キー エクスチェンジ バージョン 2（IKEv2）の交換が停止しました。 • [メモリしきい値（Memory Threshold）]：通知に示されているとおり、使用可能な空きメモリが、設定したしきい値を下回りました。 • [ASA の CPU 上昇しきい値（ASA CPU Rising Threshold）]：CPU リソースの使用率が、[期間（Period）] で指定した期間に [パーセンテージ（Percentage）] の値を超過すると、この通知が起動します。 [パーセンテージ（Percentage）]：CPU リソースの使用率の上限を、使用可能なリソース全体のパーセンテージとして入力します。有効な値の範囲は 10 ～ 94 です。デフォルトは 70 % です。 [期間（Period）]：時間の長さを分単位で入力します。この期間内に [パーセンテージ（Percentage）] で指定した使用可能なパーセンテージを超過すると通知が発行されます。有効値の範囲は 1 ～ 60 です。 • [インターフェイスしきい値（Interface Threshold）]：物理インターフェイスの使用率が、[パーセンテージ（Percentage）] で指定した、帯域幅全体のパーセンテージを超過すると、この通知が発行されます。 [パーセンテージ（Percentage）]：インターフェイスの使用率の上限を、使用可能な帯域幅全体のパーセンテージとして入力します。有効な値の範囲は 30 ～ 99 です。デフォルトは 70 % です。 • [IPSec 開始（IPSec Start）]：通知に示されているとおり、IPSec が起動しました。 • [IPSec 停止（IPSec Stop）]：通知に示されているとおり、IPSec が停止しました。 • [リモートアクセスセッションのしきい値を超過（Remote Access Session Threshold Exceeded）]：通知に示されているとおり、リモートアクセスセッションの数が、定義した制限に達しました。 • [NAT パケット破棄（NAT Packet Discard）]：IP パケットが NAT 機能により廃棄されると、この通知が生成されます。ネットワーク アドレス変換の使用可能なアドレスまたはポートが、設定したしきい値を下回りました。 • [CPU 上昇しきい値（CPU Rising Threshold）]：CPU リソースの使用率が、[期間（Period）] で指定した期間に [パーセンテージ（Percentage）] の値を超過すると、この通知が起動します。

要素	説明
	[パーセンテージ（Percentage）]：CPU リソースの使用率の上限を、使用可能なリソース全体のパーセンテージとして入力します。有効な値の範囲は 10 ～ 100 です。デフォルトは 70 % です。 [期間（Period）]：時間の長さを秒単位で入力します。この期間内に [パーセンテージ（Percentage）] で指定した使用可能なパーセンテージを超過すると通知が発行されます。有効な値の範囲は、60 ～ 3600 です。

[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス

[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスを使用して、[SNMP] ページにある [SNMPホスト（SNMP Hosts）] テーブルのエントリを追加および編集します。これらのエントリは、セキュリティデバイスへのアクセスが許可されている SNMP 管理ステーションを示します。

9.1(5) から 9.3(2) までのソフトウェアバージョンを実行している ASA デバイスの場合、129 の SNMP ホストを設定できます。9.1(5) より前のソフトウェアバージョンを実行している ASA デバイスの場合、設定できる SNMP ホストは 32 だけです。

バージョン 4.9 以降、Cisco Security Manager では、ソフトウェアバージョン 9.4(1) 以降を実行している ASA デバイスに最大 4096 の SNMP ホストを設定できます。ただし、この数の 129 のみがトラップに使用できます。129 を超えるトラップ設定の SNMP ホストを設定することはできません。

ナビゲーション パス

[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスには、[SNMP] ページ （23 ページ）からアクセスできます。

関連項目

- SNMP の設定 （20 ページ）
- [SNMP Trap Configuration] ダイアログボックス （26 ページ）
- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （35 ページ）
- [SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （37 ページ）

フィールド リファレンス

表 *13 : [SNMP*ホストアクセスエントリの追加/編集（*Add/Edit SNMP Host Access Entry*）*]* ダイアログボックス

要素	説明
Interface Name	このSNMP管理ステーションがデバイスにアクセスするインターフェイスを入力または選択します。
IPアドレス	IPアドレスを入力するか、またはSNMP管理ステーションを表すネットワークまたはホストのオブジェクトを選択します。 （注） Cisco Security Manager バージョン 4.17 以降、SNMP ポリシーの IPv6 アドレスは ASA 9.9.2 デバイス以降でサポートされます。 （注） IPv6 アドレスのネットワークまたは範囲を設定できるようになりました。
UDP ポート（UDP Port）	（任意）SNMP ホストからの要求用の UDP ポートを入力します。このフィールドを使用して、[SNMP] ページの指定したグローバル値を上書きできます。
コミュニティストリング（Community String） 確認（Confirm）	要求をセキュリティデバイスに送信するときにSNMP管理ステーションで使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。そのため、着信 SNMP 要求が有効かどうかを判断するためにパスワードが使用されます。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースは使用できません。 [確認（Confirm）] フィールドにパスワードをもう一度入力します。
SNMP バージョン（SNMP Version）	管理ステーションで使用する SNMP のバージョン（**1**、**2c**、または **3**）を選択します。
SNMP ユーザ名	SNMPバージョン3を選択した場合は、SNMPユーザを選択します。SNMP ユーザについては、[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （37 ページ）を参照してください。
Server Poll/Trap Specification	この管理ステーションとの通信タイプを指定します（ポーリングのみ、トラップのみ、またはトラップとポーリングの両方）。次のいずれかまたは両方をオンにします。 • [Poll]：セキュリティ デバイスは、管理ステーションからの定期的な要求を待機します。 • [Trap]：トラップイベントが発生すると、デバイスはトラップイベントを送信します。

[SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックス

Cisco Security Manager バージョン 4.12 以降では、[SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックスを使用して、[SNMP] ページの [SNMPホストグループ（SNMP Host Group）] テーブルのエントリを追加および編集できます。これらのエントリは、セキュリティ デバイスへのアクセスが許可されている SNMP 管理ステーションを示します。

9.1(5) から 9.4 までのソフトウェアバージョンを実行している ASA デバイスの場合、129 の SNMP ホストを設定できます。9.1(5) より前のソフトウェアバージョンを実行している ASA デバイスの場合、設定できる SNMP ホストは 32 だけです。

バージョン 4.9 以降、Cisco Security Manager では、ソフトウェアバージョン 9.4(1) 以降を実行している ASA デバイスに最大 4096 の SNMP ホストを設定できます。ただし、この数の 129 のみがトラップに使用できます。129 を超えるトラップ設定の SNMP ホストを設定することはできません。

（注） [SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ページで [SNMPホスト（SNMP Host）] または [ホストグループ（Host Group ）] エントリを追加または編集した後に、Networks/Host Policy Object Manager で使用されているアドレスの範囲またはネットワークオブジェクトを編集すると、Cisco Security Manager では SNMP トラップの総数が検証されません。したがって、トラップエントリ数が 129 を超えると、展開が失敗します。

ナビゲーション パス

[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスには、[SNMP] ページ （23 ページ）からアクセスできます。

関連項目

- SNMP の設定 （20 ページ）
- [SNMP Trap Configuration] ダイアログボックス （26 ページ）
- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （35 ページ）
- [SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （37 ページ）

フィールド リファレンス

表 *14 : [SNMP*ホストアクセスエントリの追加/編集（*Add/Edit SNMP Host Access Entry*）*]* ダイアログボックス

要素	説明
Interface Name	この SNMP 管理ステーションがデバイスにアクセスするインターフェイスを入力または選択します。
IPアドレス	IP アドレスを入力するか、または SNMP 管理ステーションを表すネットワークまたはホストのオブジェクトを選択します。 （注） SNMP ホストグループエントリは、ASA 9.17(1) 以降のデバイスの IPV6 グループ化をサポートします。[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスで、IPV6 ネットワークまたは範囲を設定できます。[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （31 ページ）
UDP ポート（UDP Port）	（任意）SNMP ホストからの要求用の UDP ポートを入力します。このフィールドを使用して、[SNMP] ページの指定したグローバル値を上書きできます。
コミュニティ ストリング（Community String） 確認（Confirm）	要求をセキュリティ デバイスに送信するときに SNMP 管理ステーションで使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。そのため、着信 SNMP 要求が有効かどうかを判断するためにパスワードが使用されます。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースは使用できません。 [確認（Confirm）] フィールドにパスワードをもう一度入力します。
SNMP バージョン（SNMP Version）	管理ステーションで使用する SNMP のバージョン（**1**、**2c**、または **3**）を選択します。

要素	説明
Server Poll/Trap Specification	この管理ステーションとの通信タイプを指定します（ポーリングのみ、トラップのみ、またはトラップとポーリングの両方）。次のいずれかまたは両方をオンにします。 • [Poll]：セキュリティデバイスは、管理ステーションからの定期的な要求を待機します。 • [Trap]：トラップ イベントが発生すると、デバイスはトラップ イベントを送信します。 （注） 同じSNMPホストグループに対して、トラップとポーリングの両方を有効にすることはできません。両方有効にする必要がある場合は、該当するホストに対して snmp-server host コマンドを使用することを推奨します。

[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス

[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックスを使用して、[SNMP] ページにある [SNMPグループ（SNMP Groups）] テーブルのエントリを追加または編集します。SNMP グループはユーザーを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMPグループ内のユーザーは、SNMPグループのセキュリティモデルに一致する必要があります。これらのパラメータは、SNMPグループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

設定上の目的のために、認証とプライバシーのオプションはセキュリティモデルにまとめられます。セキュリティモデルはユーザーとグループに適用され、次の3つのタイプに分けられます。

- NoAuth：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。
- Auth：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- Priv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

注記

- グループを削除する前に、そのグループに関連付けられているすべてのユーザーが削除されていることを確認する必要があります。削除する必要があるユーザーに関連付けられて

いるホストがある場合は、ユーザーを削除する前にそれらのホストを削除する必要があります。

- 特定のセキュリティモデルを使用して特定のグループに属するようにユーザーが設定されている場合、そのグループのセキュリティレベルを変更するには、次の手順を実行する必要があります。

  1. グループに属するユーザーに関連付けられているすべてのホストエントリを削除します。
  2. そのグループからユーザーを削除します。
  3. 変更をデバイスに展開します。
  4. グループのセキュリティ レベルを変更します。
  5. そのグループに属するユーザーを追加します。
  6. グループに追加したユーザーに属するホストを追加します。
  7. 変更をデバイスに展開します。

ナビゲーション パス

[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックスには、[SNMP] ページ （23 ページ）からアクセスできます。

関連項目

- SNMP の設定 （20 ページ）
- [SNMP Trap Configuration] ダイアログボックス （26 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （31 ページ）
- [SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （37 ページ）

フィールド リファレンス

表 *15 : [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス*

要素	説明
グループ名（Group Name）	SNMP グループの名前を入力します。グループ名は 32 文字以下にする必要があります。

要素	説明
セキュリティ レベル（Security Level）	グループのセキュリティレベルを指定します。 • NoAuth：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。 • Auth：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。 • Priv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス

[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックスを使用して、ユーザを SNMP グループに追加するか、[SNMP] ページの [SNMPユーザ（SNMP User）] テーブルのエントリを編集します。SNMP ユーザは、割り当てられたグループのセキュリティモデルを継承します。

注記

- ユーザーが作成された後は、そのユーザーが属するグループは変更できません。
- ユーザを削除するには、そのユーザ名に関連付けられているホストが設定されていないことを確認する必要があります。

ナビゲーション パス

[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックスには、[SNMP] ページ （23 ページ）からアクセスできます。

関連項目

- SNMP の設定 （20 ページ）
- [SNMP Trap Configuration] ダイアログボックス （26 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （31 ページ）
- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （35 ページ）

フィールド リファレンス

表 *16 : [SNMP*ユーザエントリの追加/編集（*Add/Edit SNMP User Entry*）*]* ダイアログボックス

要素	説明
グループ名（Group Name）	このユーザが所属する SNMP グループを選択します。SNMP グループについては、[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （35 ページ）を参照してください。
セキュリティ レベル（Security Level）	選択したグループのセキュリティレベルを表示します。 • NoAuth：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。 • Auth：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。 • Priv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。
ユーザー名	SNMP ユーザの名前を入力します。ユーザ名は 32 文字以下で、選択した SNMP サーバー グループで一意である必要があります。

要素	説明

エンジンID（Engine ID）
 	
（SNMP バージョン v3 のみ）
	v3 で認証に使用される SNMP EngineID 識別子。
	
	複数のエンジン ID をカンマで区切って入力できます。エンジン ID 識別子は有効である必要があり、各エンジン ID は 1 ～ 257 文字の範囲内である必要があります。
	
	• MD5 アルゴリズムを使用して SNMP ユーザの EngineID を構成する場合、EngineID は有効なものである必要があります。EngineID が有効でない場合、設定のプレビューは「未処理の設定の生成に失敗しました（failed to generate raw config）」というエラーで失敗します。たとえば、入力された EngineID が 111 の場合、設定のプレビューは失敗します。
	
	• セキュリティレベルが NoAuth の SNMP グループの場合は、EngineID 識別子を指定しないでください。展開時に、ASA はこのエンジン ID を無視し、デフォルトのローカルエンジン ID を使用するためです。
	
	• デバイスの次のダイナミック動作は、Security Manager では処理できません。
	
	  • フェールオーバー ASA デバイスをバージョン 8.x または 9.x からバージョン 9.6(2) にアップグレードすると、デバイスは複数の SNMP エンジン ID に対して複数の SNMP ユーザコマンドを自動的に作成します。デバイスからエンジン ID を取得して、この [エンジン ID（Engine ID）] テキストボックスにコピーする必要があります。デバイスからエンジン ID を取得する方法については、[SNMP] ページ （23 ページ）を参照してください。
	
	  • ASA デバイスをフェールオーバー構成に追加する、またはフェールオーバー構成から削除する場合、ASA デバイスは既存のエンジン ID に対して新しい SNMP ユーザコマンドを自動的に削除または作成するため、エンジン ID を手動で入力する必要があります。

パスワード暗号化タイプ（Encrypt Password Type）	使用するパスワードのタイプを指定します（[クリアテキスト（Clear Text）] または [暗号化（Encrypted）]）。 パスワードタイプが [クリアテキスト（Clear Text）] の場合、Security Manager はデバイスへの展開時にパスワードを暗号化します。パスワードタイプが [暗号化（Encrypted）] の場合、Security Manager は暗号化されたパスワードを直接展開します。Security Manager がクリアテキストのパスワードをデバイスに直接展開することはありません。

要素	説明
認証アルゴリズムタイプ（Auth Algorithm Type）	使用する認証のタイプを指定します（MD5、SHA、または SHA256）。 （注） バージョン 4.21 以降、Cisco Security Manager は ASA 9.14(1) 以降のデバイスに対して SHA256 認証タイプをサポートします。MD5 認証タイプは、今後の ASA バージョンで廃止されます。
認証パスワード（Authentication Password） 確認（Confirm）	認証に使用するパスワードを入力します。パスワード暗号化タイプに [暗号化（Encrypted）] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。 （注） パスワードの長さは、選択した認証アルゴリズムによって異なります。すべてのパスワードの長さを 256 文字以下とする必要があります。 暗号化パスワードタイプに [クリア テキスト（Clear Text）] を選択した場合、[確認（Confirm）] フィールドにパスワードをもう一度入力してください。
暗号化タイプ（Encryption Type）	使用する暗号化のタイプを指定します（AES128、AES192、AES256、3DES、DES）。 （注） AES または 3DES 暗号化を使用するには、デバイスに適切なライセンスをインストールしておく必要があります。
Encryption Password 確認（Confirm）	暗号化に使用するパスワードを入力します。パスワード暗号化タイプに [暗号化（Encrypted）] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。 暗号化を行う場合のパスワードの長さは選択された暗号化のタイプにより異なります。パスワードの長さは次のとおりです（各 xx は 1 つのオクテットを示します）。 • AES 128 では 16 オクテットとする必要があります • AES 192 では 24 オクテットとする必要があります • AES 256 では 32 オクテットとする必要があります • 3DES では 32 オクテットとする必要があります • DES の長さはさまざまです。 （注） すべてのパスワードの長さを 256 文字以下とする必要があります。 暗号化パスワードタイプに [クリア テキスト（Clear Text）] を選択した場合、[確認（Confirm）] フィールドにパスワードをもう一度入力してください。

[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックス

バージョン4.12以降、Security Managerでは、[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックスを使用して、複数の SNMP ユーザを含むユーザリストを追加できます。

注記

- 特定のホストグループで使用されているユーザリストは削除できません。
- 特定のユーザリストで参照されている SNMP ユーザを削除することはできません。

ナビゲーション パス

[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックスには、[SNMP] ページ （23 ページ）からアクセスできます。

フィールド リファレンス

表 *17 : [SNMP*ユーザリストエントリの追加/編集（*Add/Edit SNMP User List Entry*）*]* ダイアログボックス

要素	説明
ユーザリスト名	ユーザリストの名前を入力します。ユーザリスト名の長さは 1 ～ 33 文字にする必要があります。
ユーザ名	ドロップダウンリストからユーザ名を選択します。

関連項目

- SNMP の設定 （20 ページ）
- [SNMP Trap Configuration] ダイアログボックス （26 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （31 ページ）
- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス（35 ページ）

[Telnet] ページ

[Telnet] ページを使用して、Telnet プロトコルを使用したファイアウォール デバイスへの接続を、特定のホストまたはネットワークにだけ許可するルールを設定します。

このルールにより、ファイアウォール デバイス インターフェイスを介した管理 Telnet アクセスが特定の IP アドレスおよびネットマスクに制限されます。このルールに準拠する接続試行

は、設定済みの AAA サーバまたは Telnet パスワードによって認証される必要があります。Telnet セッションは、[Monitoring] > [Telnet Sessions] を使用してモニタできます。

（注） シングルコンテキスト モードでは一度に 5 つの Telnet セッションだけアクティブにできます。ASA 上のマルチコンテキスト モードでは、コンテキストあたり 5 つの Telnet だけをアクティブにでき、ブレードあたり 100 個の Telnet セッションをアクティブにできます。リソース クラスでは、管理者がこのパラメータをさらに調整できます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Telnet]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Telnet]** を選択します。[Telnet] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Telnet Configuration] ダイアログボックス （42 ページ）

フィールド リファレンス

表 *18 : [Telnet]* ページ

要素	説明
タイムアウト（Timeout）	Telnet セッションがファイアウォール デバイスによって閉じられる前にアイドル状態でいられる時間（分単位）。値の範囲は 1 ～ 1440 分です。
Telnet Access Table	
インターフェイス	クライアントから Telnet パケットを受信するインターフェイス。
IP Addresses	指定されたインターフェイスを通じて Telnet コンソールにアクセスできる各ホストまたはネットワークの IP アドレスおよびネットワーク マスク。

[Telnet Configuration] ダイアログボックス

[Telnet Configuration] ダイアログボックスを使用して、インターフェイスの Telnet オプションを設定します。

ナビゲーション パス

[Telnet Configuration] ダイアログボックスには、[Telnet] ページ （41 ページ）からアクセスできます。

フィールド リファレンス

表 *19 : [Telnet Configuration]* ダイアログボックス

要素	説明
Interface Name	クライアントからの Telnet パケットを受信できるインターフェイスを入力または選択します。 （注） Cisco Security Manager バージョン 4.17 以降、ASA 9.9.2 以降のデバイスで Telnet の BVI インターフェイスを設定できます。ただし、マルチコンテキストでは、「トランスペアレント」モードのセキュリティコンテキストは BVI インターフェイスのみをサポートします。
IP Addresses/Netmask	指定したインターフェイスを通じてファイアウォールデバイスの Telnet コンソールへのアクセスを許可される各ホストまたはネットワークの IP アドレスとネットマスクを「/」で区切って入力または選択します。複数のエントリを指定する場合は、カンマで区切ります。 （注） アクセスを単一 IP アドレスに制限するには、ネットマスクとして 255.255.255.255 または 32 を使用します。内部ネットワークのサブネットワーク マスクは使用しないでください。 （注） バージョン 4.13 以降、Cisco Security Manager は、IPv6 デバイスのポリシー（グループ、ホスト、アドレス範囲、およびネットワーク）をサポートします。

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。