ASA および PIX 7.0+ デバイスでのリモートアクセス VPN の管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

Cisco ASA ソフトウェアまたは PIX 7.0+ を実行するデバイスのリモート アクセス IPsec、および ASA 8.0+ デバイス（PIX デバイスではありません）の SSL VPN を設定および管理できます。また、ASA 8.4(x) デバイスでは、リモートアクセス IPsec VPN で IKE バージョン 2（IKEv2）ネゴシエーションを使用できます。

（注） Cisco Catalyst 6500 シリーズ ASA サービスモジュール、およびモジュールで使用される ASA ソフトウェアリリース 8.5(x) では、VPN 設定はサポートされていません。

これらのリモートアクセス VPN の設定は、これらのデバイスタイプで同じです。IOS および PIX 6.3+ デバイスは、リモートアクセス VPN に異なる設定を使用します。

この章のトピックでは、ASA および PIX 7.0+ デバイスに固有のポリシーを設定する方法を説明します。リモート アクセス VPN の詳細については、次のトピックを参照してください。

- リモート アクセス VPN について
- 各リモート アクセス VPN テクノロジーでサポートされるデバイスについて
- リモート アクセス VPN ポリシーの検出
- Remote Access VPN Configuration ウィザードの使用
  - Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）
  - Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）

- リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス）

この章は次のトピックで構成されています。

ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

ASA または PIX 7.0 以降のデバイスでリモートアクセス VPN を設定する場合、設定する VPN のタイプに基づいて、以下のポリシーを使用します。可能なリモートアクセス VPN タイプは、IKE Version 1（IKEv1; IKE バージョン 1）IPsec、IKE Version 2（IKEv2; IKE バージョン 2）IPsec および SSL です。IKEv2 は、ソフトウェアバージョン 8.4(x) 以降を実行している ASA デバイスでサポートされています。これらのポリシーが必須または任意である条件については、表 1 : ASA デバイスのリモート アクセス VPN ポリシー要件 （5 ページ）を参照してください。

（注） PIX デバイスでは SSL VPN を設定できません。PIX デバイスでは、リモート アクセス IKEv1 IPsec VPN だけをサポートしています。

- **リモート アクセス IKEv1 と IKEv2 IPsec および SSL VPN で使用されているポリシー**：
  - **ASA グループ ロード バランシング**：リモート クライアント コンフィギュレーションで、複数のデバイスを同じネットワークに接続してリモートセッションを処理している場合、それらのデバイスでセッション負荷を分担するように設定できます。この機能は、ロード バランシングと呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロードバランシングは、ASA デバイスで開始されたリモート セッションの場合にだけ有効です。詳細については、グループのロードバランシングについて（ASA） （6 ページ）を参照してください。

- **接続プロファイル**：接続プロファイルは、トンネル自体の作成に関連する属性を含む、VPN トンネルの接続ポリシーが格納されたレコードセットです。接続プロファイルでは、ユーザ指向の属性が含まれる特定の接続のグループポリシーを識別します。詳細については、接続プロファイルの設定（ASA、PIX 7.0+）　（9 ページ）を参照してください。
- **ダイナミックアクセス**：各 VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザーが持つさまざまなロール、および設定とセキュリティレベルが異なるリモートアクセスサイトからのログインなど、複数の変数が影響する可能性があります。Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）により、これらの多くの変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。詳細については、リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス）を参照してください。

（注）　マルチコンテキスト ASA デバイスの場合、ダイナミック アクセス ポリシーは、Cisco Security Manager バージョン 4.12 および ASA バージョン 9.6(2) 以降でのみサポートされます。

- **グローバル設定**：リモートアクセス VPN のすべてのデバイスに適用されるグローバル設定を定義できます。グローバル設定には、Internet Key Exchange（IKE; インターネットキー交換）、IKEv2、IPsec、NAT、フラグメンテーションの定義などがあります。グローバル設定には、通常、ほとんどの状況に適用できるデフォルトが設定されています。そのため、ほとんどの場合、グローバル設定ポリシーの設定はオプションです。デフォルト以外の動作が必要な場合、または IKEv2 ネゴシエーションをサポートする場合だけ設定してください。詳細については、VPN グローバル設定を参照してください。
- **グループポリシー**：リモートアクセス VPN 接続プロファイルに定義されているユーザーグループポリシーを表示できます。このページから、新しい ASA ユーザ グループを指定したり、既存の ASA ユーザ グループを編集したりできます。接続プロファイルを作成するときに、デバイスで使用されていないグループポリシーを指定した場合、このグループ ポリシーは自動的に [Group Policies] ページに追加されます。接続プロファイルを作成する前に、このポリシーに追加する必要はありません。詳細については、リモート アクセス VPN のグループ ポリシーの設定　（36 ページ）を参照してください。
- **Public Key Infrastructure**：Public Key Infrastructure（PKI）ポリシーを作成して、CA 証明書および RSA キーの登録要求を生成し、キーや証明書を管理できます。Certification Authority（CA; 認証局）サーバは、これらの証明書要求を管理し、IPsec または SSL リモート アクセス VPN に接続するユーザに対して証明書を発行するために使用されます。詳細については、Public Key Infrastructure ポリシーについておよびリモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定を参照してください。

（注） マルチコンテキスト ASA デバイスの場合、Public Key Infrastructure ポリシーは、Cisco Security Manager バージョン 4.12 および ASA バージョン 9.6(2) 以降でのみサポートされます。

- **証明書スクリプトのユーザー名**：このポリシーを使用して、証明書のユーザー名のマッピングに使用するスクリプトを定義できます。詳細については、[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス （47 ページ）を参照してください。

（注） マルチコンテキスト ASA デバイスの場合、証明書スクリプトポリシーのユーザー名は、Cisco Security Manager バージョン 4.12 および ASA バージョン 9.6(2) 以降でのみサポートされます。

- **リモート アクセス IPsec VPN だけで使用されるポリシー**：
  - **証明書から接続プロファイルへのマップ、ポリシーとルール**（IKEv1 IPSec のみ）：証明書から接続プロファイルへのマップポリシーを使用すると、指定したフィールドに基づいて、ユーザーの証明書を権限グループと照合するルールを定義できます。認証を確立するため、証明書の任意のフィールドを使用することも、またはすべての証明書ユーザが権限グループを共有することもできます。グループは、DN ルール、[Organization Unit (OU)] フィールド、IKE ID、またはピア IP アドレスから照合できます。これらの方式のいずれかまたはすべてを使用できます。詳細については、Certificate to Connection Profile Map ポリシーの設定（ASA） （50 ページ）を参照してください。
  - **IKE プロポーザル**：インターネットキーエクスチェンジ（IKE）は、ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーションプロトコルです。IKE は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動確立に使用されます。IKE プロポーザル ポリシーは、IKE ネゴシエーションのフェーズ 1 の要件を定義するときに使用します。詳細については、IKE プロポーザルの設定を参照してください。
  - **IPsec プロポーザル（ASA/PIX 7.x）**：IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。このポリシーは、IKE フェーズ 2 ネゴシエーションに使用されます。詳細については、リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス） （56 ページ）を参照してください。
- **リモート アクセス IKEv2 IPSec および SSL VPN だけで使用されるポリシー**：

- **アクセス**：アクセスポリシーには、リモートアクセス SSL または IKEv2 IPsec VPN 接続プロファイルを有効にできるセキュリティアプライアンスのインターフェイス、接続プロファイルで使用するポート、Datagram Transport Layer Security（DTLS）設定、SSL VPNセッションタイムアウト、および最大セッション数を指定します。AnyConnect VPN クライアントまたは Secure Client Essentials を使用するかどうかも指定できます。詳細については、SSL VPN アクセス ポリシーについて（ASA） （61 ページ）を参照してください。
- **その他の設定**：SSL VPN のその他の設定ポリシーでは、キャッシング、コンテンツの書き換え、文字エンコード、プロキシとプロキシバイパス定義、ブラウザプラグイン、セキュアクライアントイメージとプロファイル、Kerberos の制約付き委任、およびその他の詳細設定を定義します。詳細については、他の SSL VPN 設定の定義（ASA） （71 ページ）を参照してください。
- **共有ライセンス**：[SSL VPN共有ライセンス（SSL VPN Shared License）] ページを使用して、SSL VPN 共有ライセンスを設定します。詳細については、SSL VPN 共有ライセンスの設定（ASA 8.2+） （104 ページ）を参照してください。

次の表に、特定のタイプの VPN でポリシーが必須か任意かについて説明します。

表 *1 : ASA* デバイスのリモート アクセス *VPN* ポリシー要件

ポリシー	必須、任意
ASA グループロードバランシング	**任意**：すべての VPN タイプ。
Dynamic Access	**任意**：すべての VPN タイプ。
Dynamic Access	**任意**：すべての VPN タイプ。
グローバル設定	**必須**：IKEv2 IPsec。 **任意**：IKEv1 IPsec、SSL。
グループ ポリシー	**必須**：すべての VPN タイプ。
公開キー インフラストラクチャ	**必須**：IKEv2 IPsec。 IKEv1 IPsec または SSL VPN 用のトラストポイントを設定する場合にも必須。これ以外の場合はオプションです。
Certificate To Connection Profile Maps, Policy and Rules	**任意**：IKEv1 IPsec。 **未使用**：IKEv2 IPsec、SSL。
IKE Proposal	**必須**：IKEv1 IPsec、IKEv2 IPsec。 **未使用**：SSL。

ポリシー	必須、任意
[IPsec Proposal](ASA/PIX 7.x)	**必須**：IKEv1 IPsec、IKEv2 IPsec。 **未使用**：SSL。
アクセス（Access）	**必須**：IKEv2 IPsec。SSL。 **未使用**：IKEv1 IPsec。
その他の設定（Other Settings）	**必須**：IKEv2 IPsec。SSL。 **未使用**：IKEv1 IPsec。
Shared License	**任意**：IKEv2 IPsec、SSL。 **未使用**：IKEv1 IPsec。

グループのロードバランシングについて（ASA）

リモートクライアント設定で、同じネットワークに接続された2つ以上のデバイスを使用してリモートセッションを処理するようになっている場合は、そのセッションの負荷が分散されるようにこれらのデバイスを設定できます。この機能は、ロードバランシングと呼ばれます。ロードバランシングでは、最も負荷の低いデバイスにセッショントラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロードバランシングは、ASA デバイスで開始されたリモートセッションの場合にだけ有効です。

ロードバランシングを実装するには、同じプライベート LAN-to-LAN ネットワークの 2 つ以上のデバイスを、仮想クラスタにグループ化する必要があります。セッションの負荷は、仮想クラスタ内のすべてのデバイスに分散されます。仮想クラスタ内の1つのデバイス（仮想ディレクタと呼ばれる）が、着信コールを他のデバイス（セカンダリデバイスと呼ばれる）に転送します。仮想クラスタディレクタは、クラスタ内のすべてのデバイスをモニターし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。

仮想クラスタは、外部のクライアントには単一の仮想グループ IP アドレスとして表示されます。この IP アドレスは、特定の物理デバイスに関連付けられたアドレスではなく、現在の仮想ディレクタに属するアドレスです。接続を確立しようとする VPN クライアントは、最初にこの仮想グループ IP アドレスに接続します。仮想クラスタディレクタは、クラスタ内で使用できるホストのうち、最も負荷の低いホストのパブリック IP アドレスをクライアントに返します。2 回めのトランザクション（ユーザーに対しては透過的）になると、クライアントはホストに直接接続します。仮想ディレクタは、このようにしてリソース全体に均等かつ効率的にトラフィックを転送します。

仮想ディレクタの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。クラスタ内のマシンで障害が発生すると、終了されたセッションはただちに仮想グループ IP アドレスに再接続できます。次に、仮想ディレクタは、クラスタ内の別のアクティブデバイスにこれらの接続を転送します。仮想ディレクタ自身に障害が発生した場合は、クラスタ内のセカンダリデバイスが、新しい仮想セッションディレクタをただちに引き継

ぎます。クラスタ内の複数のデバイスで障害が発生しても、クラスタ内のデバイスが 1 つでも使用可能である限り、ユーザはクラスタに引き続き接続できます。

Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用したリダイレクションについて

デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、セカンダリ デバイスにリダイレクトされるとその証明書は無効になります。セキュリティアプライアンスは、VPN ディレクタとして、VPN クライアント接続をクラスタデバイス（クラスタ内の別のセキュリティアプライアンス）にリダイレクトする場合に、そのグループデバイスの完全修飾ドメイン名（FQDN）を送信できます。セキュリティ アプライアンスは、逆 DNS ルックアップを使用してデバイスの FQDN を外部 IP アドレスに解決し、接続を転送して VPN ロード バランシングを実行します。グループ内のロードバランシングデバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

FQDN によるロード バランシングをイネーブルにしたあと、ASA 外部インターフェイスごとにエントリが存在しない場合は、このエントリを DNS サーバに追加します。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。ASA での DNS ルックアップをイネーブルにし、ASA 上で DNS サーバの IP アドレスを定義します。

グループロードバランシングの設定手順については、グループのロードバランスポリシーの設定（ASA） （7 ページ）を参照してください。

グループのロードバランスポリシーの設定（ASA）

[ASAクラスタロードバランス（ASA Cluster Load Balance）] ページを使用して、リモートアクセス VPN の ASA デバイスのロードバランシングを有効にします。ロードバランシングはデフォルトでは無効になっているので、明示的に有効にする必要があります。クラスタに参加するすべてのデバイスは、同じクラスタ固有の値（IP アドレス、暗号化設定、暗号キー、およびポート）を共有する必要があります。クラスタ ロードバランシングの詳細については、グループのロードバランシングについて（ASA） （6 ページ）を参照してください。

（注） ロードバランシングには、アクティブな 3DES/AES ライセンス、および Plus ライセンス付きの ASA モデル 5510、または ASA モデル 5520 以降が必要です。ASA デバイスでは、ロードバランシングをイネーブルにする前に、このクリプト ライセンスが存在するかをチェックします。アクティブな 3DES または AES ライセンスを検出できない場合、デバイスは、ロード バランシングを回避し、さらにライセンスがこの使用を許可していないかぎり、ロードバランシング システムによる 3DES の内部コンフィギュレーションも回避します。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [ASAグループロードバランス（ASA Group Load Balance）] 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 [リモートアクセスVPN（Remote Access VPN）] > [ASAグループロードバランス（ASA Group Load Balance）] を選択します。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。

[ASAグループロードバランス（ASA Group Load Balance）] ページが開きます。

ステップ 2 [ロードバランシングクラスタに参加（Participate in Load Balancing Cluster）] を選択して、デバイスがロードバランシングクラスタに属することを示します。

ステップ 3 [VPNグループの設定（VPN Group Configuration）] オプションを設定します。

- [グループIPv4/IPv6アドレス（Group IPv4/IPv6 Address）]：仮想クラスタ全体を表す単一の IP アドレスを指定します。外部インターフェイスと同じサブネット内にある IP アドレスを選択します。バージョン 4.12 以降、Security Manager は、IPv4 アドレスに加えて、IPv6 グループの IPv6 アドレスをサポートします。これはバージョン 9.0 以降を実行している ASA デバイスに適用されます。
- [UDPポート（UDP Port）]：デバイスが属する仮想クラスタの UDP 宛先ポートを指定します。通常、ポート番号は 9023 です。ただし、このポートが別のアプリケーションで使用されている場合、ロードバランシングに使用する UDP 宛先ポート番号を入力します。
- [IPSec暗号化を有効にする（Enable IPSec Encryption）]、[IPSec共有秘密（IPSec Shared Secret）]：必要に応じて、[IPSec暗号化を有効にする（Enable IPSec Encryption）] を選択し、デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにします。このオプションを選択した場合は、共有秘密パスワードも入力（および確認）します。これは、スペースを含まない 4 ～ 16 文字の値で、大文字と小文字が区別されます。仮想グループのセキュリティアプライアンスは、IPsec を使用して LAN-to-LAN トンネルを介して通信します。このパスワードは、クライアントから渡されるパスワードと一致する必要があります。

ステップ 4 [NAT設定（NAT Configuration）] オプションを設定します。

- [NAT IPアドレスIPv4/IPv6（NAT IP Address IPv4/IPv6）]：単一の NAT IP アドレスを指定します。バージョン 4.24 以降、CSM は IPv4 および IPv6 NAT IP アドレス設定をサポートします。

ステップ 5 クラスタ内のサーバーの優先順位を設定します。次のオプションのいずれかを選択します。

- [デバイスのデフォルト値を受け入れる（Accept default device value）]：デバイスに割り当てられたデフォルトの優先順位の値を受け入れます。
- [クラスタ内のすべてのデバイスに同じ優先順位を設定（Configure same priority on all devices in the cluster）]：クラスタ内のすべてのデバイスに同じ優先順位の値を設定します。次に優先順位番号（1 ～ 10）を入力します。この番号は、起動時または既存のディレクタで障害が発生したときに、デバイスが仮想ディレクタになる可能性を表します。

ステップ 6 サーバ上で使用するパブリックおよびプライベート インターフェイスを指定します。

- [パブリックインターフェイス（Public Interfaces）]：サーバーで使用されるパブリックインターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、[選択

（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。

- [プライベートインターフェイス（Private Interfaces）]：サーバーで使用されるプライベート インターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。

ステップ 7 必要に応じて、[リダイレクト時にIPアドレスではなくFQDNを送信する（Send FQDN to client instead of an IP address when redirecting）] を選択し、完全修飾ドメイン名を使用したリダイレクションを有効にします。このオプションは、8.0(2) 移行が動作する ASA デバイスでのみ使用できます。詳細については、グループのロードバランシングについて（ASA） （6 ページ）を参照してください。

接続プロファイルの設定（ASA、PIX 7.0+）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

接続プロファイルは、VPN トンネル接続プロファイルポリシーを含む一連のレコードです。このレコードには、トンネルそのものの作成に関連する属性も含まれます。接続プロファイルでは、ユーザ指向の属性が含まれる特定の接続のグループ ポリシーを識別します。ユーザにグループ ポリシーを割り当てない場合、接続にはデフォルトの接続プロファイルが適用されます。環境に固有の接続プロファイルを 1 つ以上作成できます。ローカル リモートアクセス VPN サーバまたは外部 AAA サーバ上で接続プロファイルを設定できます。

デバイスでリモートアクセス VPN ポリシーを検出すると、Security Manager により、デフォルト接続プロファイルがポリシーに追加されます。これらのプロファイル、および関連する DlftGrpPolicy（Security Manager では <*device_display_name*> DfltGrpPolicy という名前に変更されています）を編集できますが、削除はできません。次に、Security Manager でサポートされているデフォルト接続プロファイルを示します。

- DefaultRAGroup：リモート アクセス IPsec VPN のデフォルトの接続プロファイル。
- DefaultWEBVPNGroup：SSL VPN のデフォルトの接続プロファイル。この接続プロファイルは、ASA 8.0+ デバイスだけで検出されます。

ASA デバイス上で接続プロファイルを設定する場合には、二重認証を設定するオプションがあります。二重認証機能では、Payment Card Industry Standards Council Data Security Standard に従って、ネットワークへのリモートアクセスに対して 2 つの要素からなる認証を実行します。この機能では、ユーザーはログイン ページで異なる 2 組のログイン クレデンシャルを入力する必要があります。たとえば、プライマリ認証をワンタイムパスワード、セカンダリ認証をドメイン（Active Directory）クレデンシャルとする場合が考えられます。プライマリクレデンシャル認証が失敗すると、セキュリティ アプライアンスはセカンダリ クレデンシャルの確認を試行

しません。いずれかの認証に失敗すると、接続が拒否されます。AnyConnect VPN クライアント（SSL VPN または IKEv2 IPSec VPN）およびクライアントレス SSL VPN の両方で二重認証がサポートされています。セキュアクライアント では、Windows コンピュータ（サポート対象 Windows Mobile 装置および Start Before Login など）、Mac コンピュータ、および Linux コンピュータで二重認証がサポートされています。

ここでは、Connection Profile ポリシーを使用して、リモート アクセス VPN サーバで接続プロファイルを作成または編集する方法について説明します。

（注） Remote Access VPN Configuration ウィザードから、接続プロファイルを作成することもできます（Remote Access VPN Configuration ウィザードの使用を参照）。Easy VPN サイト間トポロジについては、Easy VPN における Connection Profile ポリシーの設定を参照してください。

関連項目

- リモート アクセス VPN ポリシーの検出

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA または PIX 7.0 以降のデバイスを選択し、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]** 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 **[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（ASA）（Connection Profiles (ASA)）]** を選択します。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。

[Connection Profiles] ページが開きます。このポリシーでは、すべての接続プロファイルのリストが示され、プロファイルで使用されるグループ ポリシーが表示されます。詳細については、[Connection Profiles] ページ （11 ページ）を参照してください。

ステップ 2 テーブルの下にある [行の追加（Add Row）]（+）をクリックするか、プロファイルを選択して [行の編集（Edit Row）]（鉛筆）をクリックします。[Connection Profiles] ダイアログボックスが開きます。

ステップ 3 （すべてのリモートアクセス VPN タイプ）[General] タブで、接続プロファイル名およびグループ ポリシーを指定して、使用するアドレス割り当て方式を選択します。設定の詳細については、[General] タブ（[Connection Profiles]） （14 ページ）を参照してください。

ステップ 4 （すべてのリモートアクセス VPN タイプ）[AAA] タブをクリックして、接続プロファイルの AAA 認証パラメータを指定します。設定の詳細については、[AAA] タブ（[Connection Profiles]） （17 ページ）を参照してください。

ステップ 5 （リモートアクセス IKEv2 IPsec および SSL VPN のみ）ASA デバイスで接続プロファイルを設定している場合は、セカンダリ認証を設定できます。これを行うには、[セカンダリAAA（Secondary AAA）] タブをクリックします。設定の詳細については、[Secondary AAA] タブ（[Connection Profiles]） （23 ページ）を参照してください。

ステップ 6 （リモートアクセス IPsec VPN のみ）[IPsec] タブをクリックして、接続プロファイルの IPsec および IKE パラメータを指定します。これらの一部の設定は、IKEv1 接続には適用されますが、IKEv2 接続には適用

されません。設定の詳細については、[IPSec] タブ（[Connection Profiles]） （26 ページ）を参照してください。

（注） IKEv2 設定を行うには、[Global Settings] ポリシーの [IKEv2 Settings] タブを使用します。VPN グローバル IKEv2 設定を参照してください。

ステップ 7 （リモートアクセス SSL VPN のみ）[SSL] タブをクリックして接続プロファイルポリシーの WINS サーバーを指定し、SSL VPN エンドユーザログオン Web ページのカスタマイズ済みルックアンドフィールを選択し、クライアントアドレスの割り当てに使用する DHCP サーバーを指定し、インターフェイスとクライアント IP アドレスプール間のアソシエーションを設定します。設定の詳細については、[SSL] タブ（[Connection Profiles]） （30 ページ）を参照してください。

ステップ 8 [OK] をクリックします。

[Connection Profiles] ページ

リモート アクセス VPN または Easy VPN トポロジの接続プロファイル ポリシーを管理するには、[Connection Profiles] ページを使用します。[接続プロファイル（Connection Profiles）] ページには、設定されている接続プロファイルが一覧表示され、それらの接続プロファイルに関連付けられたグループポリシーが表示されます。また、接続プロファイルが 、トンネルネゴシエーション中に特定のトンネルグループが識別されない場合に Citrix クライアントに使用されるデフォルトの接続プロファイルであるかどうかが示されます。

このポリシーの使用法は、設定する VPN のタイプによって異なります。

- [Remote access SSL VPN]：ポリシーは、ASA デバイスに対してだけ使用されます。複数のプロファイルを作成し、[Connection Profiles] ダイアログボックスのすべてのタブの値を設定できます。
- [Remote access IPSec VPN]：ポリシーは、PIX 7.0+ ソフトウェアを実行している ASA デバイスおよびPIX ファイアウォールに対して使用されます。複数のプロファイルを作成できますが、[Connection Profiles] ダイアログボックスの [General]、[AAA]、および [IPSec] タブだけがこの設定に適用されます（場合によってはこれらのタブだけが表示されます）。
- [Easy VPN topologies]：ポリシーは、PIX 7.0+ ソフトウェアを実行している ASA デバイスまたは PIX ファイアウォールである Easy VPN サーバ（ハブ）に対して使用されます。ポリシー ページが [Connection Profiles] ダイアログボックスが実際に埋め込まれるように、単一のプロファイルを作成できます。これにより、プロファイルを定義するタブに直接アクセスできます。[General]、[AAA]、および [IPSec] タブだけが適用されます。

リモート アクセス IPSec および SSL VPN では、次のように行います。

- プロファイルを追加するには、[行の追加（Add Row）] ボタンをクリックし、[接続プロファイル（Connection Profiles）] ダイアログボックスに入力します。
- 既存のプロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックします。

- プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。

接続プロファイルは、次のタブで構成されます。これらのタブには、設定する VPN のタイプに適した値を設定してください。

- [General] タブ（[Connection Profiles]） （14 ページ）
- [AAA] タブ（[Connection Profiles]） （17 ページ）
- [Secondary AAA] タブ（[Connection Profiles]） （23 ページ）（SSL VPN および IKEv2 IPsec VPN のみ）
- [IPSec] タブ（[Connection Profiles]） （26 ページ）（これらの設定の一部は、IKEv1 接続には適用されますが、IKEv2 接続には適用されません。）
- [SSL] タブ（[Connection Profiles]） （30 ページ）（SSL VPN のみ）

ナビゲーション パス

リモートアクセス VPN：

- （デバイスビュー）ASA または PIX 7+ デバイスを選択し、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]** 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 **[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（ASA）（Connection Profiles (ASA)）]** を選択します。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。

Easy VPN では、次のように行います。

- [Site-to-Site VPN Manager] ウィンドウから Easy VPN トポロジを選択し、[接続プロファイル（PIX7.0/ASA）（Connection Profiles (PIX7.0/ASA)）] を選択します。
- （デバイスビュー）Easy VPN トポロジに参加するデバイスを選択し、ポリシーセレクタから [サイト間VPN（Site to Site VPN）] を選択します。Easy VPN トポロジを選択して [VPN ポリシーの編集（Edit VPN Policies）] をクリックし、[Site-to-Site VPN Manager] ウィンドウを開いてポリシーを選択します。
- （ポリシービュー）**[サイト間VPN（Site-to-Site VPN）] > [接続プロファイル（PIX7.0/ASA）（Connection Profiles (PIX7.0/ASA)）]** を選択します。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。

ここでは、次の内容について説明します。

- [General] タブ（[Connection Profiles]） （14 ページ）
- [AAA] タブ（[Connection Profiles]） （17 ページ）
- [Secondary AAA] タブ（[Connection Profiles]） （23 ページ）

• [IPSec] タブ（[Connection Profiles]） （26 ページ）
• [SSL] タブ（[Connection Profiles]） （30 ページ）

リモートアクセス VPN マルチコンテキスト モードでサポートされる CLI - 接続プロファイル

次の CLI は、マルチコンテキストモードのリモートアクセス VPN の接続プロファイル用 ASA 9.5(2) でサポートされています。これらの CLI は、トンネルグループの管理およびユーザコンテキストでサポートされています。

DefaultWEBVPNGroup は、デフォルトの接続プロファイルです。DefaultRAGroup は、ASA 9.5(2) リモートアクセス VPN マルチコンテキストモードではサポートされていません。

（注） サポートされていない設定の場合、Security Manager は無視できる警告メッセージを表示します。デルタは生成されません。

- Type remote-access
- General-attributes
  - Accounting-server-group
  - Address-pool
  - 注釈（Annotation）
  - Authenticated-session-username
  - Authentication-attr-from-server
  - Authentication-server-group
  - Authorization-required
  - Authorization-server-group
  - Default-group-policy
  - Dhcp-server
  - 終了（Exit）
  - Ipv6-address-pool
  - Nat-assigned-to-public-ip
  - Password-management
  - Secondary-authentication-server-group
- Webvpn-attributes

- 認証
- 終了（Exit）
- Group-alias
- Group-url
- なし
- Radius-reject-message

[General] タブ（[Connection Profiles]）

[Connection Profiles] ダイアログボックスの [General] タブを使用して、VPN Connection Profile ポリシーの基本プロパティを設定します。これらのプロパティは、リモートアクセス IPsec および SSL VPN、あるいはサイト間 Easy VPN トポロジで使用されます。

[全般（General）] タブは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

- リモートアクセス VPN：[接続プロファイル（Connection Profiles）] ページ（[Connection Profiles] ページ （11 ページ）を参照）から、[行を追加（Add Row）]（+）ボタンをクリックするか、プロファイルを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックし、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。必要に応じて、[全般（General）] タブをクリックします。
- Easy VPN トポロジ：Easy VPN トポロジを選択して、ポリシー ビューまたはサイト間 VPN Manager のいずれかでサイト間 VPN Connection Profile ポリシーを選択します（[Connection Profiles] ページ （11 ページ）を参照）。必要に応じて、[全般（General）] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ）
- [ASA Group Policies] ダイアログボックス
- ネットワーク/ホストオブジェクトについて
- Easy VPN について
- Easy VPN における Connection Profile ポリシーの設定

フィールド リファレンス

表 2 : [Connection Profile] の [General] タブ

要素	説明
Connection Profile Name	接続プロファイルの名前（トンネル グループ）。
[グループ ポリシー（Group Policy）]	必要な場合、接続プロファイルに関連付けられているデフォルト ユーザ グループを定義する ASA グループ ポリシー オブジェクトの名前。グループ ポリシーはユーザ指向の属性と値のペアの集合であり、デバイスで内部的に、または RADIUS/LDAP サーバで外部的に格納されます。 [選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。
Client Address Assignment	
DHCP サーバ（DHCP Servers）	クライアント アドレス割り当てに使用される DHCP サーバ。これらのサーバは、リスト内の順序で使用されます。 DHCP サーバの IP アドレス、または DHCP サーバのアドレスを定義するネットワーク/ホスト ポリシー オブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
[グローバル IPv4 アドレスプール（Global IPv4 Address Pool）]	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IPv4 アドレスをクライアントに割り当てるために使用されるアドレスプール。アドレス プールは、アドレスの範囲として入力します（10.100.12.2-10.100.12.254 など）。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。 アドレスプール範囲を入力するか、これらのプールを定義するネットワークまたはホストオブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。

要素	説明
[グローバル IPv6 アドレスプール（Global IPv6 Address Pool）]	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IPv6 アドレスをクライアントに割り当てるために使用されるアドレスプール。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。アドレスプールはアドレスの範囲として入力します（例：fe80::60/5 4）。ここで、fe80::60/5 は IPv6 アドレスとプレフィックス長、4 はカウント（アドレスの数）です。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。 アドレスプール範囲を入力するか、これらのプールを定義するネットワークまたはホストオブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
[Interface-Specific Address Pools] テーブル	特定のインターフェイスを介して接続するクライアントがグローバル グループとは異なるプールを使用するように、そのインターフェイスに対して個別の IP アドレス プールを設定する場合は、そのインターフェイスをこのテーブルに追加し、個別のプールを設定します。このテーブルに表示されていないインターフェイスはすべて、グローバル プールを使用します。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。したがって、IPv6 アドレスプールの追加の列が表示されます。 • インターフェイス固有のアドレス プールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add Interface Specific Client Address Pools]/[Edit Interface Specific Client Address Pools] ダイアログボックス （16 ページ）に入力します。 • インターフェイス プールを編集するには、インターフェイス プールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイスを削除するには、インターフェイスを選択し、[行を削除（Delete Row）] ボタンをクリックします。

[Add Interface Specific Client Address Pools]/[Edit Interface Specific Client Address Pools] ダイアログボックス

[Add Interface Specific Client Address Pools]/[Edit Interface Specific Client Address Pools] ダイアログボックスを使用して、Connection Profile ポリシーに対してインターフェイス固有のクライアント アドレス プールを設定します。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [全般（General）] タブ（[General] タブ（[Connection Profiles]） （14 ページ）を参照）を開き、[インターフェイス固有のアドレスプール（Interface-Specific Address Pools）] テーブルの下の [行の追加（Add Row）] をクリックするか、テーブルから行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- ネットワーク/ホストオブジェクトの作成
- インターフェイス ロール オブジェクトの作成

フィールド リファレンス

表 3 : [Add Interface Specific Client Address Pools]/[Edit Interface Specific Client Address Pools] ダイアログボックス

要素	説明
インターフェイス（Interface）	アドレス プールを割り当てるインターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力します。あるいは、[選択（Select）]をクリックしてインターフェイスまたはオブジェクトを選択するか、または新しいオブジェクトを作成します。
IPv4 アドレスプール（IPv4 Address Pool）	インターフェイスに割り当てる IPv4 アドレスプール。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。アドレス プールは、プールの開始および終了 IP アドレスを使用して指定されます。たとえば、10.100.10.2-10.100.10.254 です。IP アドレス範囲を入力するか、アドレス範囲を指定するネットワーク/ホスト オブジェクトを使用できます。[選択（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するか、または新しいオブジェクトを作成します。
IPv6アドレスプール（IPv6 Address Pool）	インターフェイスに割り当てる IPv6 アドレスプール。IPv6 アドレスプールは、IPv6 アドレスとプレフィックス長、およびその後に続くカウントを使用して指定されます。カウントはプール内のアドレスの数を示します。IP アドレス範囲を入力するか、アドレス範囲を指定するネットワーク/ホスト オブジェクトを使用できます。[選択（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するか、または新しいオブジェクトを作成します。

[AAA] タブ（[Connection Profiles]）

[Connection Profile] ダイアログボックスの [AAA] タブを使用して、Connection Profile ポリシーに AAA 認証パラメータを設定します。

AAA の場合、識別名認証設定ポリシーは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされません。

ただし、Security Manager バージョン 4.12 以降、このポリシーはマルチコンテキストモードの ASA 9.6(2) リモートアクセス VPN でサポートされます。管理およびユーザコンテキストでサポートされる CLI は次のとおりです。

- Tunnel-group General-attributes
  - Secondary-username-from-certificate
  - Username-from-certificate

ナビゲーション パス

- リモートアクセス VPN：[接続プロファイル（Connection Profiles）] ページ（[Connection Profiles] ページ （11 ページ）を参照）から、[行を追加（Add Row）]（+）ボタンをクリックするか、プロファイルを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックし、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。[AAA] タブをクリックします。
- Easy VPN トポロジ：Easy VPN トポロジを選択して、ポリシー ビューまたはサイト間 VPN Manager のいずれかでサイト間 VPN Connection Profile ポリシーを選択します（[Connection Profiles] ページ （11 ページ）を参照）。[AAA] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて
- Easy VPN における Connection Profile ポリシーの設定
- Easy VPN について

フィールド リファレンス

表 *4 : [Connection Profile]* の *[AAA]* タブ

要素	説明
認証方式	AAA、証明書、またはその両方、複数の証明書、AAA と複数の証明書、およびSAML を使用して接続を認証するかどうか。[証明書（Certificate）] を選択すると、必要な詳細が証明書から取得されるため、ダイアログボックスのオプションの多くが無効になります。 バージョン 4.10 以降、Security Manager では、認証方法として SAML ID プロバイダーを選択できます。これは、現在のトンネルグループに対して SAML サービスプロバイダーを有効にするためです。SAML ID プロバイダーは、トンネルグループに適用されるまで使用されません。SAML 認証は相互排他認証方式です。詳細については、SAML ID プロバイダの構成を参照してください。 バージョン 4.13 以降、Security Manager では、認証方式として複数の証明書、または AAA と複数の証明書を選択できます。この方式は、ASA 9.7.1 デバイスの複数証明書認証機能をサポートする目的で有効になっています。9.7.1 リリースより前の ASA デバイスに対してこの方式を選択すると、検証エラーメッセージが表示されます。詳細については、複数証明書認証のサポートを参照してください。
Authentication Server Group	認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 クライアントの接続先のインターフェイスに基づいて別の認証サーバ グループを使用する場合は、このタブの一番下にある [Interface-Specific Authentication Server Groups] テーブルでサーバ グループを設定します（後述の説明を参照）。
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Authorization Server Group	認可サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Users must exist in the authorization database to connect	正常に接続するために、クライアントのユーザ名が認可データベース内に存在することを要求するかどうか。ユーザー名が承認データベース内に存在しない場合、接続が拒否されます。

要素	説明
Accounting Server Group	アカウンティング サーバ グループの名前。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）]をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Strip Realm from Username Strip Group from Username	ユーザ名を AAA サーバに渡す前に、ユーザ名からレルムまたはグループ名を削除するかどうか。レルムとは管理ドメインのことです。これらのオプションを有効にすると、ユーザ名だけに基づいて認証できます。 これらのオプションを任意に組み合わせて有効にできます。ただし、サーバーが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
Override Account-Disabled Indication from AAA Server	AAA サーバーからの「account-disabled」インジケータをオーバーライドするかどうか。この設定は、「account-disabled」インジケータを返すサーバー（NT LDAP を使用する RADIUS、Kerberos など）で有効です。 認証に LDAP ディレクトリ サーバーを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。 • **Sun**：Sunディレクトリサーバーにアクセスするためにセキュリティアプライアンスで設定されている DN は、そのサーバー上のデフォルトのパスワードポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザーを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。 • **Microsoft**：Microsoft Active Directory でパスワード管理を有効にするには、LDAP over SSL を設定する必要があります。
Enable Notification Upon Password Expiration to Allow User to Change Password Enable Notification Prior to Expiration Notify Prior to Expiration	セキュリティアプライアンスが、リモートユーザのログイン時に、現在のパスワードの期限切れが近づいていること、または期限が切れていることを通知し、パスワードを変更する機会を提供するかどうか。 パスワードの期限切れが近づいていることを前もってユーザーに警告する場合には、[期限切れ前の通知の有効化（Enable Notification Prior to Expiration）] を選択して、通知を開始する期限切れ前の日数（1 ～ 180）を指定します。このオプションは、RADIUS、RADIUS 対応 NT サーバ、および LDAP サーバなど、このような通知をサポートする AAA サーバで使用できます。他の種類のサーバーについては、事前の通知はありません。

要素	説明
Distinguished Name (DN) Authorization Settings	認可用の識別名を使用する方法。Distinguished Name（DN; 識別名）は、個々のフィールドから構成される一意の識別子であり、ユーザをトンネルグループと照合するときに識別子として使用できます。DNルールは、拡張証明書認証に使用されます。認可中の DN の使用方法を決定するには、以下のオプションを選択します。 • [DN全体をユーザー名として使用（Use Entire DN as the Username）]：特定のフィールドに焦点を当てることなく、DN全体を使用します。 • [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）]：特定のフィールドに焦点を当てます。プライマリフィールドを選択し、オプションでセカンダリフィールドを選択します。デフォルトでは、Common Name（CN; 共通名）をプライマリとして使用し、Organizational Unit（OU; 組織ユニット）をセカンダリとして使用します。 • [ユーザー名選択にスクリプトを使用（Use Script to Select Username）]：バージョン 4.7 以降、Security Manager では、証明書からのユーザー名のマッピングに使用するスクリプトを定義できます。ドロップダウンリストから、定義したスクリプトを選択します。詳細については、[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス （47 ページ）を参照してください。
[Interface-Specific Authentication Server Groups] テーブル	特定のインターフェイスを介して接続するクライアントがグローバルプールとは異なるサーバ グループを使用するように、そのインターフェイスに対して個別の認証サーバ グループを設定する場合は、そのインターフェイスをこのテーブルに追加し、個別のグループを設定します。ここに記載されていないインターフェイスでは、グローバル認証サーバグループを使用します。この表には、サーバグループと、サーバグループが使用可能でない場合にローカル認証を使用するかどうかを示します。 • インターフェイス固有の認証グループをリストに追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add Interface Specific Authentication Server Groups]/[Edit Interface Specific Authentication Server Groups] ダイアログボックス （22 ページ）に入力します。 • インターフェイス設定を編集するには、そのインターフェイス設定を選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイス設定を削除するには、そのインターフェイス設定を選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Add Interface Specific Authentication Server Groups]/[Edit Interface Specific Authentication Server Groups] ダイアログボックス

[Add Interface Specific Authentication Server Groups]/[Edit Interface Specific Authentication Server Groups] ダイアログボックスを使用して、Connection Profile ポリシーにインターフェイス固有の認証を設定します。指定されたインターフェイスにクライアントが接続すると、グローバル認証サーバ グループの設定がこの設定によって上書きされます。

ASA デバイスで SSL VPN のセカンダリ AAA サーバを設定する場合、その設定は、ユーザが入力するセカンダリ クレデンシャル セットに対して使用されます。これは、ダイアログボックスの名前に反映されます。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [AAA] または [セカンダリ AAA] タブ（ [AAA] タブ（[Connection Profiles]） （17 ページ）または [Secondary AAA] タブ（[Connection Profiles]） （23 ページ）を参照）を開き、[インターフェイス固有のアドレス プール（Interface-Specific Address Pools）] テーブルの下の [行の追加（Add Row）] をクリックするか、テーブル内の行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- インターフェイス ロール オブジェクトについて
- AAA サーバおよびサーバ グループ オブジェクトについて

フィールド リファレンス

表 5 : [Add (Secondary) Interface Specific Authentication Server Groups]/[Edit (Secondary) Interface Specific Authentication Server Groups]

要素	説明
インターフェイス（Interface）	認証サーバ グループを設定するインターフェイスまたは（インターフェイスを識別する）インターフェイス ロールの名前。[選択（Select）] をクリックして、インターフェイスまたはインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。
Server Group	認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 セカンダリ AAA を設定する場合、2 番めのクレデンシャルに対してこのグループが使用されます。プライマリ クレデンシャルとセカンダリ クレデンシャルには別々のサーバ グループを指定できます。

要素	説明
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Use Primary Username （セカンダリ認証のみ。ASA 8.2+ でのリモート アクセス SSL または IKEv2 IPSec VPN にかぎります）	プライマリ クレデンシャルに使用したのと同じユーザ名をセカンダリ クレデンシャルに使用するかどうか。このオプションを選択した場合、ユーザは、プライマリ クレデンシャルで認証された後、セカンダリ パスワードだけを要求されます。このオプションを選択しない場合は、セカンダリ プロンプトによってユーザ名とパスワードの両方が要求されます。

[Secondary AAA] タブ（[Connection Profiles]）

[Secondary AAA] タブを使用して、ASA 8.2+ デバイスで使用するリモート アクセス SSL VPN Connection Profile ポリシーまたは ASA 8.4(1)+ デバイスで使用するリモート アクセス IKEv2 IPSec VPN Connection Profile ポリシーにセカンダリ AAA 認証パラメータを設定します。これらの設定は、リモート アクセス IKEv1 IPSec VPN や Easy VPN トポロジ、またはその他のデバイス タイプには適用されません。

ナビゲーション パス

リモートアクセス VPN のみ：[接続プロファイル（Connection Profiles）] ページ（[Connection Profiles] ページ （11 ページ）を参照）から、[行の追加（+）（Add Row(+)）] ボタンをクリックするか、プロファイルを選択して、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックして、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。[セカンダリ AAA（Secondary AAA）] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ）

フィールド リファレンス

表 6 : [Connection Profile] の [Secondary AAA] タブ

要素	説明
Enable Double Authentication	リモート アクセス VPN 接続を完了する前に、ユーザに 2 つのクレデンシャル セット（ユーザ名とパスワード）を要求する二重認証をイネーブルにするかどうか。

要素	説明
Secondary Authentication Server Group	2番めのクレデンシャルセットで使用する認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL です）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 クライアントの接続先のインターフェイスに基づいて別の認証サーバ グループを使用する場合は、このタブの一番下にある [Secondary Interface-Specific Authentication Server Groups] テーブルでサーバ グループを設定します（後述の説明を参照）。
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Use Primary Username for Secondary Authentication	プライマリ クレデンシャルに使用したのと同じユーザ名をセカンダリ クレデンシャルに使用するかどうか。このオプションを選択した場合、ユーザは、プライマリ クレデンシャルで認証された後、セカンダリ パスワードだけを要求されます。このオプションを選択しない場合は、セカンダリ プロンプトによってユーザ名とパスワードの両方が要求されます。
Username for Session	ソフトウェアがユーザ セッションに使用するユーザ名。プライマリ名かセカンダリ名のいずれかとなります。プライマリ名だけを要求する場合は、プライマリを選択します。 （注） デフォルトでは、複数のユーザー名が存在する場合、Secure Client では、複数のセッションの間、両方のユーザー名を記憶します。さらに、ヘッドエンドデバイスでは、クライアントが両方のユーザ名を記憶するか、または両方とも記憶しないかの管理制御を行う機能が提供される場合があります。
Authorization Authentication Server	認可に使用するサーバ。（[AAA] タブで定義されている）プライマリ認証サーバか、このタブで設定されているセカンダリ認証サーバのいずれかです。

要素	説明
Distinguished Name (DN) Secondary Authorization Setting	認可用の識別名を使用する方法。Distinguished Name（DN; 識別名）は、個々のフィールドから構成される一意の識別子であり、ユーザをトンネル グループと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。認可中の DN の使用方法を決定するには、以下のオプションを選択します。 • [DN全体をユーザー名として使用（Use Entire DN as the Username）]：特定のフィールドに焦点を当てることなく、DN 全体を使用します。 • [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）]：特定のフィールドに焦点を当てます。プライマリ フィールドを選択し、オプションでセカンダリ フィールドを選択します。デフォルトでは、User Identification（UID; ユーザ ID）フィールドだけを使用します。 • [ユーザー名選択にスクリプトを使用（Use Script to Select Username）]：バージョン 4.7 以降、Security Manager では、証明書からのユーザー名のマッピングに使用するスクリプトを定義できます。ドロップダウンリストから、定義したスクリプトを選択します。詳細については、[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス （47 ページ）を参照してください。 （注） Distinguished Name (DN) Secondary Authorization Settings は、マルチコンテキストモードでバージョン 9.6(2) を実行している ASA デバイスの Security Manager バージョン 4.12 からサポートされています。管理およびユーザコンテキストでサポートされる CLI は次のとおりです。 • Tunnel-group General-attributes • Secondary-username-from-certificate • Username-from-certificate

要素	説明
[Secondary Interface-Specific Authentication Server Groups] テーブル	特定のインターフェイスを介して接続するクライアントがグローバルプールとは異なるサーバ グループを使用するように、そのインターフェイスに対して個別のセカンダリ認証サーバ グループを設定する場合は、そのインターフェイスをこのテーブルに追加し、個別のグループを設定します。ここに記載されていないインターフェイスでは、グローバル認証サーバ グループを使用します。この表には、サーバ グループと、サーバ グループが使用可能でない場合にローカル認証を使用するかどうかを示します。 • セカンダリインターフェイス固有の認証グループをリストに追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add Interface Specific Authentication Server Groups]/[Edit Interface Specific Authentication Server Groups] ダイアログボックス （22 ページ）に入力します。 • インターフェイス設定を編集するには、そのインターフェイス設定を選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイス設定を削除するには、そのインターフェイス設定を選択し、[行の削除（Delete Row）] ボタンをクリックします。

[IPSec] タブ（[Connection Profiles]）

[Connection Profiles] ページの [IPsec] タブを使用して、接続ポリシーに IPsec および IKE パラメータを指定します。

バージョン 4.8 以降の Security Manager では、Secure Client に加え、標準ベースでサードパーティの IKEv2 リモートアクセス クライアントを介した VPN 接続がサポートされます。認証では、事前共有キー、証明書、拡張認証プロトコル（EAP）を介したユーザ認証などがサポートされます。

IPSec は、マルチコンテキスト モードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。Cisco Security Manager バージョン 4.17 以降、IPSec は ASA 9.9(2) 以降のマルチコンテキストデバイスでサポートされています。ただし、[接続プロファイル（Connection Profile）] > [IPSec] タブにある次の属性は、ASA 9.9(2) 以降のマルチコンテキストデバイスではサポートされていません。

- IKEv2 Mobike RRCを有効にする（Enable IKEv2 Mobike RRC）
- クライアントソフトウェアの更新テーブル（Client Software Update Table）

ナビゲーション パス

- リモートアクセス VPN：[接続プロファイル（Connection Profiles）] ページ（ [Connection Profiles] ページ （11 ページ）を参照）から、[行を追加（Add Row）]（+）ボタンをクリックするか、プロファイルを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックし、

[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。[IPSec] タブをクリックします。

- Easy VPN トポロジ：Easy VPN トポロジを選択して、ポリシー ビューまたはサイト間 VPN Manager のいずれかでサイト間 VPN Connection Profile ポリシーを選択します（[Connection Profiles] ページ （11 ページ）を参照）。[IPSec] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ）
- Easy VPN における Connection Profile ポリシーの設定
- Easy VPN について

フィールド リファレンス

表 7 : [Connection Profiles] の [IPsec] タブ

要素	説明
IKEv1 ピア認証	
事前共有キー（Preshared Key）	接続プロファイルの事前共有キー。事前共有キーの最大長は 127 文字です。確認フィールドでもう一度キーを入力します。
Trustpoint Name	トラストポイント名を定義する PKI 登録ポリシー オブジェクトの名前（トラストポイントが IKEv1 接続で設定されている場合）。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。 [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** トラストポイントを指定した場合、公開キーインフラストラクチャ ポリシーで同じ PKI 登録オブジェクトを選択する必要があります。詳細については、リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定を参照してください。
IKEv2 ピア認証 事前共有キー、証明書、EAP などの 1 つ以上の認証オプションをリモート認証用に構成できます。	
事前共有キー（Preshared Key）	接続プロファイルの事前共有キー。事前共有キーの最大長は 127 文字です。確認フィールドでもう一度キーを入力します。

要素	説明
証明書認証の有効化（Enable Certificate Authentication）	オンにすると、認証に証明書を使用できます。
EAP 認証の有効化（Enable EAP Authentication）	オンにすると、認証に EAP を使用できます。 （注） このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。EAP認証では、サーバーは証明書を使用して認証する必要があるためです。
EAP アイデンティティ要求をクライアントに送信する（Send EAP identity request to the client）	リモートアクセス VPN クライアントに EAP 認証要求を送信できます。
IKEv2 ローカル認証 ローカル認証には、事前共有キーまたはトラストポイント名を設定できます。	
事前共有キー	接続プロファイルの事前共有キー。事前共有キーの最大長は 127 文字です。確認フィールドでもう一度キーを入力します。
Trustpoint Name	トラストポイント名を定義する PKI 登録ポリシー オブジェクトの名前（トラストポイントが IKEv2 接続で設定されている場合）。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。 [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） リモート認証に EAP を選択した場合は、ローカル認証で証明書を使用する必要があります。
IKEv2 Mobike RRCを有効にする（Enable IKEv2 Mobike RRC）	選択すると、Mobike が有効になっている IKE/IPSEC セキュリティ アソシエーションにおけるダイナミック IP アドレス変更のリターン ルータビリティ チェックを有効にします。デフォルトでは、Mobike RRC は無効になっています。 （注） 動的IPアドレス変更のリターンルータビリティチェックは、ASA 9.8.1 以降でのみイネーブルにできます。 （注） このオプションは、ASA 9.9(2) 以降のマルチコンテキストデバイスではサポートされていません。

要素	説明
IKEv2 RSA署名SHA-1を有効にする（Enable IKEv2 RSA Signature SHA-1）	IKEv2 認証の RSA 署名 SHA-1 を有効にする場合に選択します。デフォルトでは、RSA 署名 SHA-1 は無効になっています。 （注） このオプションは、Cisco Security Manager 4.19 以降および ASA 9.12(1) 以降のデバイスでサポートされています。
IKE Peer ID Validation	IKE ピア ID 検証を無視する（確認しない）か、必須とするか、または証明書によってサポートされている場合にかぎり確認するかを選択します。IKE ネゴシエーション中、ピアは互いに自身を識別する必要があります。
Enable Sending Certificate Chain	認可の証明書チェーンの送信をイネーブルにするかどうか。証明書チェーンには、ルート CA 証明書、ID 証明書、およびキー ペアが含まれます。
Enable Password Update with RADIUS Authentication	RADIUS 認証プロトコルを使用してパスワードを更新できるかどうか。詳細については、サポートされる AAA サーバ タイプを参照してください。
ISAKMP Keepalive	ISAKMP キープアライブをモニタするかどうか。[キープアライブのモニター（Monitor Keepalive）] オプションを選択した場合、デフォルトのフェールオーバーおよびルーティングのメカニズムとして IKE キープアライブを設定できます。次のパラメータを入力します。 • [信頼間隔（Confidence Interval）]：IKE キープアライブパケット送信から次の送信までのデバイスの待機時間（秒単位）。 • [再試行間隔（Retry Interval）]：デバイスがリモートピアとの IKE 接続の確立を試行する間隔（秒単位）。デフォルト値は 2 秒です。 詳細については、VPN グローバル ISAKMP/IPsec 設定を参照してください。

要素	説明
[Client Software Update] テーブル	クライアントプラットフォームの VPN クライアントのリビジョン レベルおよび URL。すべての [All Windows Platforms]、[Windows 95/98/ME]、[Windows NT4.0/2000/XP]、または [VPN3002 Hardware Client] に対して別々のリビジョン レベルを設定できます。 プラットフォームにクライアントを設定するには、クライアントを選択して [行の編集（Edit Row）] ボタンをクリックし、[IPSec Client Software Update] ダイアログボックス （30 ページ）に入力します。 （注） このオプションは、ASA 9.9(2) 以降のマルチコンテキストデバイスではサポートされていません。

[IPSec Client Software Update] ダイアログボックス

[IPsec Client Software Update] ダイアログボックスを使用して、VPN クライアントの特定のリビジョン レベルおよびイメージ URL を設定します。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [IPSec] タブを開き（[IPSec] タブ（[Connection Profiles]） （26 ページ）を参照）、[クライアントソフトウェアの更新（Client Software Update）] テーブルからクライアントタイプを選択して、[行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 *8 : [IPSec Client Software Update]* ダイアログボックス

要素	説明
Client Type	変更するクライアントのタイプ。
Client Revisions	クライアントのリビジョン レベル。
イメージ URL	クライアント ソフトウェア イメージの URL。

[SSL] タブ（[Connection Profiles]）

[Connection Profile] ダイアログボックスの [SSL] タブを使用して、Connection Profile ポリシーの WINS サーバの設定、SSL VPN エンドユーザ ログイン Web ページのカスタマイズ済みルックアンド フィールの選択、クライアント アドレス割り当てに使用する DHCP サーバの選択、およびインターフェイスとクライアント IP アドレス プールの関連付けの確立を行います。接続プロファイル エイリアスなどの一部の設定は、リモート アクセス IKEv2 IPsec VPN には適用

されますが、これらの設定は、リモート アクセス IKEv1 IPSec VPN または Easy VPN トポロジには適用されません。

次のポリシーは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN の [SSL] タブでサポートされています。

- Radius-Reject-Message
- Connection alias
- Group-url
- Group-alias

ナビゲーション パス

リモートアクセス VPN のみ：[接続プロファイル（Connection Profiles）] ページ（[Connection Profiles] ページ （11 ページ）を参照）から、[行の追加（+）（Add Row(+)）] ボタンをクリックするか、プロファイルを選択して、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックして、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。[SSL] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ）
- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化 （121 ページ）
- ネットワーク/ホストオブジェクトについて
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （108 ページ）

フィールド リファレンス

表 9 : [Connection Profile] の [SSL] タブ

要素	説明
WINS Servers List	CIFS 名前解決に使用する Windows Internet Naming Server（WINS）サーバ リストの名前。[選択（Select）] をクリックして WINS サーバーリストからポリシーオブジェクトを選択するか、または新しいオブジェクトを作成します。 SSL VPN は、CIFS プロトコルを使用して、リモート システムのファイルにアクセスまたは共有します。Windows コンピュータの名前を使用してそのコンピュータへのファイル共有接続を試行する場合、指定するファイル サーバは、ネットワーク上のリソースを識別する特定の WINS サーバ名と対応しています。 WINS サーバ リストは、Windows ファイル サーバ名を IP アドレスに変換するために使用される WINS サーバのリストを定義するものです。セキュリティ アプライアンスは、WINS サーバを照会して、WINS 名を IP アドレスにマップします。少なくとも 1 台の WINS サーバを設定する必要があります。冗長性のために最大 3 台設定できます。セキュリティ アプライアンスは、リストの最初のサーバを WINS/CIFS 名前解決に使用します。クエリーが失敗すると、次のサーバーが使用されます。
DNS Group	SSL VPN トンネル グループに使用する DNS グループ。DNS グループは、ホスト名をトンネル グループに適した DNS サーバに解決します。リストから目的のグループを選択します。DefaultDNS グループは、デバイスで常に使用できるデフォルト グループです。 **ヒント** DNS グループは、[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] ポリシーで定義されます。DNS ポリシーを使用して、グループで定義されているサーバを変更するか、グループを追加または削除します。[DNS] ページを参照してください。

要素	説明
Portal Page Customization	VPN のデフォルト ポータル ページを定義する [SSL VPN Customization] ポリシー オブジェクトの名前。このプロファイルでは、リモート ユーザが SSL VPN 上で使用可能なすべてのリソースにアクセスできるようにするためのポータル ページの外観を定義します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） カスタマイゼーション プロファイルとグループの組み合わせを使用することで、個々のグループにそれぞれ異なるログイン ウィンドウを設定できます。たとえば、salesgui という名前のカスタマイゼーションプロファイルを作成してあるとすると、そのカスタマイゼーション プロファイルを使用する sales という名前の SSL VPN グループを作成できます。次に、[SSL VPN] > [Settings] タブのグループ ポリシー オブジェクトで、SSL VPN カスタマイゼーション オブジェクトを指定します（ASA グループ ポリシーの SSL VPN 設定を参照）。
SAML ID プロバイダー	[SAML IDプロバイダー（SAML Identity Provider）] を選択します。SAML IDプロバイダーは、トンネルグループで適用されるまで使用されません。詳細については、SAML ID プロバイダの構成を参照してください。
Override SVC Download (ASA 8.0(2) 以降のみ)	特定のトンネルグループでログインしているクライアントレス ユーザには、ダウンロードプロンプトが終了するまで待たせることなく、クライアントレス SSL VPN ホームページを表示するかどうかを指定します。表示する場合、これらのユーザには即時にクライアントレス SSL VPN ホームページが表示されます。
Reject Radius Message (ASA 8.0(2) 以降のみ)	認証の失敗に関する RADIUS メッセージをリモート ユーザに表示するかどうかを指定します。

要素	説明
[Connection Aliases] テーブル	トンネル グループを参照できる代替名のリスト。このステータスは、名前がイネーブル（使用できる）またはディセーブル（使用できない）かを示します。 グループ エイリアスにより、ユーザがトンネル グループの参照に使用できる 1 つ以上の代替名が作成されます。この機能は、同じグループが複数の通常名（「Devtest」や「QA」など）で指定されている場合に便利です。トンネル グループの実際の名前をこのリストに表示する場合は、その名前をエイリアスとして指定する必要があります。ここで指定したグループ エイリアスは、ログイン ページに表示されます。各トンネル グループには複数のエイリアスがあることも、エイリアスがまったくないこともあります。 • エイリアスを追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックして、 [Add Connection Alias]/[Edit Connection Alias] ダイアログボックス （35 ページ）に入力します。 • エイリアスを編集するには、エイリアスを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • エイリアスを削除するには、エイリアスを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。
[Group URLs] テーブル	トンネル グループ接続プロファイルに関連付けられる URL のリスト。このステータスは、URL が使用できるかどうかを示します。使用できる場合、ユーザは、URL を使用できるため、ログイン中にグループを選択する必要がなくなります。 1 つのトンネル グループに対して複数の URL を設定できます。または、URL を設定しないこともできます。各 URL は、個別にイネーブルまたはディセーブルにできます。URL ごとに、HTTP または HTTPS プロトコルを使用して URL 全部を指定することにより、個別の指定を使用する必要があります。 • URL を追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックして、 [Add Connection URL]/[Edit Connection URL] ダイアログボックス （36 ページ）に入力します。 • URL を編集するには、URL を選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • URL を削除するには、URL を選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

要素	説明
デフォルトの Citrix クライアントプロファイル （ASA 9.1(4) 以降のみ）	トンネルネゴシエーション時に特定のトンネルグループが識別されない場合にこの接続プロファイルを Citrix クライアントに使用するデフォルトの接続プロファイルにするかどうかを定義します。 （注） デフォルトの Citrix クライアントプロファイルとして設定できる接続プロファイルは 1 つだけです。ある接続プロファイルがすでにデフォルトの Citrix クライアントプロファイルとして設定されている場合に、別の接続プロファイルをデフォルトとして設定しようとすると、警告メッセージが表示されます。操作を続行すると、選択した接続プロファイルがデフォルトの Citrix クライアントプロファイルになり、デフォルトの Citrix クライアントプロファイルとして選択されていた他の接続プロファイルは選択解除されます。
Disable CSD （ASA 8.2(0) 以降のみ） クライアントレスと Secure Client の両方 Secure Client のみ	この接続プロファイルで Cisco Secure Desktop（CSD）をディセーブルにするかどうかを指定します。Security Manager は、ASA ソフトウェアバージョン 8.2(0) 以降を実行しているすべてのデバイスでこの機能をサポートします。 （注） CSD を無効にする場合、デフォルトでは、Security Manager は SSL クライアントレス VPN と Secure Client の両方のオプションを選択します。

[Add Connection Alias]/[Edit Connection Alias] ダイアログボックス

[Add Connection Alias]/[Edit Connection Alias] ダイアログボックスを使用して、SSL または IKEv2 IPsec VPN 接続プロファイルの接続エイリアスを作成または編集します。接続エイリアスを指定すると、ユーザがトンネル グループの参照に使用できる 1 つ以上の代替名が作成されます。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [SSL] タブ（[SSL] タブ（[Connection Profiles]） （30 ページ）を参照）を開き、[接続エイリアス（Connection Alias）] テーブルの下の [行の追加（Add Row）] をクリックするか、テーブルからエイリアスを選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 10 : [Add Connection Alias]/[Edit Connection Alias] ダイアログボックス

要素	説明
有効	接続エイリアスをイネーブルにするかどうか指定します。エイリアスを使用するユーザには、エイリアスをイネーブルにする必要があります。

要素	説明
Connection Alias	接続プロファイルの代替名。 ここで指定する接続エイリアスは、ユーザーのログインページにあるリストに表示されます。

[Add Connection URL]/[Edit Connection URL] ダイアログボックス

このダイアログボックスを使用して、トンネル グループに着信 URL を指定します。トンネル グループ内の接続 URL がイネーブルになっている場合、ユーザがその URL を使用して接続すると、セキュリティ アプライアンスにより、関連付けられたトンネル グループが選択され、ログイン ウィンドウ内にユーザ名フィールドとパスワード フィールドだけが表示されます。

ヒント

- 1 つのグループに対して複数の URL またはアドレスを設定できます（何も設定しないこともできます）。各 URL またはアドレスは、個別にイネーブルまたはディセーブルにできます。
- 同じ URL またはアドレスを複数のグループに関連付けることはできません。セキュリティ アプライアンスは、トンネル グループの URL またはアドレスを受け入れる前に、URL またはアドレスの一意性を検証します。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [SSL] タブ（[SSL] タブ（[Connection Profiles]） （30 ページ）を参照）を開き、[グループURL（Group URLs）] テーブルの下の [行の追加（Add Row）] をクリックするか、テーブルから URL を選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 11 : [Add Connection URL]/[Edit Connection URL] ダイアログボックス

要素	説明
有効	接続エイリアスをイネーブルにするかどうか指定します。エイリアスを使用するユーザには、エイリアスをイネーブルにする必要があります。
Connection URL	リストからプロトコル（[http] または [https]）を選択し、接続の着信 URL を指定します。

リモート アクセス VPN のグループ ポリシーの設定

[Group Policies] ページでは、ASA リモート アクセス VPN 接続プロファイルに定義されているユーザ グループ ポリシーを参照できます。このページから、新しい ASA ユーザ グループを指

定したり、既存の ASA ユーザ グループを編集したりできます。接続プロファイルを作成するときに、デバイスで使用されていないグループ ポリシーを指定した場合、このグループ ポリシーは自動的に [Group Policies] ページに追加されます。接続プロファイルを作成する前に、このポリシーに追加する必要はありません。接続プロファイルの作成については、接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ）を参照してください。

グループ ポリシーの詳細については、グループ ポリシーについて（ASA） （38 ページ）を参照してください。

ヒント ダイナミック アクセス ポリシーは、グループ ポリシーに優先します。ダイナミック アクセス ポリシーで設定を指定していない場合、ASA デバイスは設定を指定しているグループ ポリシーがないかどうかを確認します。

テーブル内の各行は、ASA グループ ポリシー オブジェクトを表します。これには、リモート アクセス VPN 接続プロファイルに割り当てられているポリシー オブジェクトの名前、そのポリシー オブジェクトが ASA デバイス自体（[Internal]）または AAA サーバ（[External]）のいずれに格納されるか、および、そのグループが IKEv1（IPsec）、IKEv2（IPsec）または SSL、あるいはすべてのタイプの VPN に対応しているかが表示されます。外部グループの場合、プロトコルは認識されず、N/A として表示されます。

- ASA グループ ポリシー オブジェクトを追加するには、[行の追加（Add Row）]ボタンをクリックします。これにより、オブジェクトセレクタが開きます。ここから、既存のポリシー オブジェクトを選択するか、[作成（Create）] ボタンをクリックして新しいオブジェクトを作成します。グループ ポリシーの作成の詳細については、グループ ポリシーの作成（ASA、PIX 7.0+） （39 ページ）を参照してください。

（注） 名前に DfltGrpPolicy を含むグループ ポリシーを複数作成することはできません。DfltGrpPolicy は、デバイスで定義されているデフォルトのポリシーです。Security Manager が、リモートアクセスポリシー検出中にこのグループを検出すると、このグループは、リスト内の <device_display_name> DfltGrpPolicy という名前の下に表示されます。設定をデバイスに展開すると、DfltGrpPolicy が正しく更新されるため、表示名プレフィックスが削除されます。詳細については、リモート アクセス VPN ポリシーの検出を参照してください。

- オブジェクトを編集するには、オブジェクトを選択して [行の編集（Edit Row）] ボタンをクリックし、[ASA Group Policies] ダイアログボックスを開きます。
- オブジェクトをポリシーから削除するには、オブジェクトを選択して [行の削除（Delete Row）]ボタンをクリックします。関連付けられたポリシーオブジェクトは、このポリシーから取り除かれるだけで、削除されません。

（注） デフォルトのグループ ポリシーを削除することはできません。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [グループポリシー（Group Policies）]** を選択します。
- （ポリシービュー）ポリシーセレクタから、**[リモートアクセス VPN（Remote Access VPN）] > [グループポリシー（ASA）（Group Policies (ASA)）]** を選択します。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） Cisco Security Manager 4.24 以降では、ASA デバイス検出時に [グループポリシー（Group Policy）] に vpn-tunnel-protocol を設定しない場合、CSM は [DfltGrpPolicy] から vpn-tunnel-protocol 値を継承することで [グループポリシー（Group Policy）] の検出を行います。

グループ ポリシーについて（ASA）

リモート アクセス IPSec VPN 接続またはリモート アクセス SSL VPN 接続を設定する場合は、リモート クライアントが属するユーザ グループを作成する必要があります。ユーザ グループ ポリシーは、リモート アクセス VPN 接続のためのユーザ指向の属性と値のペアのセットで構成され、デバイス内部（ローカル）または外部の AAA サーバに保存されます。接続プロファイルは、接続確立後のユーザ接続条件を設定するユーザ グループ ポリシーを使用します。グループポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

ヒント ダイナミック アクセス ポリシーは、グループ ポリシーに優先します。ダイナミック アクセス ポリシーで設定を指定していない場合、ASA デバイスは設定を指定しているグループ ポリシーがないかどうかを確認します。

ASA ユーザ グループは、次の属性で構成されます。

- グループポリシーソース。ユーザーグループの属性および値を、セキュリティアプライアンスの内部（ローカル）に格納するか、外部の AAA サーバーに格納するかどうかを指定します。ユーザ グループを外部タイプとした場合は、そのユーザ グループにその他の設定をする必要はありません。詳細については、[ASA Group Policies] ダイアログボックスを参照してください。
- クライアント設定。Easy VPN またはリモート アクセス VPN でユーザ グループの Cisco クライアント パラメータを指定します。詳細については、ASA グループ ポリシーのクライアント設定を参照してください。
- クライアント ファイアウォール属性。Easy VPN またはリモート アクセス VPN で VPN クライアントのファイアウォール設定を行います。詳細については、ASA グループ ポリシーのクライアント ファイアウォール属性を参照してください。

- ハードウェア クライアント属性。Easy VPN またはリモート アクセス VPN で VPN 3002 ハードウェア クライアント設定を行います。詳細については、ASA グループ ポリシーのハードウェア クライアント属性を参照してください。
- IPsec 設定。Easy VPN またはリモート アクセス VPN のユーザ グループにトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定します。詳細については、ASA グループ ポリシーの IPSec 設定を参照してください。
- ASA ユーザ グループのクライアントレス設定。SSL VPN で企業ネットワークへのクライアントレス アクセス モードを設定します。詳細については、ASA グループ ポリシーの SSL VPN クライアントレス設定を参照してください。
- ASA ユーザ グループのフル クライアント設定。SSL VPN で企業ネットワークへのフル クライアント アクセス モードを設定します。詳細については、ASA グループ ポリシーの SSL VPN フル クライアント設定を参照してください。
- 一般設定。SSL VPN でのクライアントレス/ポート転送に必要です。詳細については、ASA グループ ポリシーの SSL VPN 設定を参照してください。
- DNS/WINS 設定。DNS サーバと WINS サーバ、および ASA ユーザ グループに関連付けられたリモート クライアントにプッシュされるドメイン名を定義します。詳細については、ASA グループ ポリシーの DNS/WINS 設定を参照してください。
- スプリット トンネリング。条件に応じて、リモート クライアントがパケットを暗号化された形式で IPsec VPN または SSL VPN トンネル上を送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。詳細については、ASA グループ ポリシーのスプリット トンネリング設定を参照してください。
- ASA ユーザ グループのリモート アクセスまたは SSL の VPN セッション接続設定。詳細については、ASA グループ ポリシーの接続設定を参照してください。

関連項目

- グループ ポリシーの作成（ASA、PIX 7.0+） （39 ページ）
- リモート アクセス VPN のグループ ポリシーの設定 （36 ページ）

グループ ポリシーの作成（ASA、PIX 7.0+）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

[Group Policies] ページを使用して、リモート アクセス IPSec VPN で使用される ASA または PIX 7.0+ デバイス、あるいはリモート アクセス SSL VPN で使用される ASA デバイスのグループ ポリシーを作成します。グループ ポリシーについては、次を参照してください。

- グループ ポリシーについて（ASA） （38 ページ）

• リモート アクセス VPN のグループ ポリシーの設定 （36 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA または PIX 7.0+ デバイスを選択し、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）] 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、[リモートアクセス VPN（Remote Access VPN）] > [グループポリシー（ASA）（Group Policies (ASA)）] を選択します。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。

[Group Policies] ページが開きます。このテーブルには、既存のグループ ポリシーと、それらがデバイスで内部的に定義されるか AAA サーバで外部的に定義されるか、およびグループのプロトコル（IKEv1（IPsec）、IKEv2（IPsec）、または SSL）のリストが示されます。

ステップ 2 [行の追加（Add Row）]（+）をクリックするとダイアログボックスが開き、このダイアログボックスで、定義済みの ASA ユーザー グループ オブジェクトのリストからユーザーグループを選択したり、必要に応じて新しいユーザーグループを作成したりできます。新しいグループを作成するには、ダイアログボックスの [作成（Create）]（+）ボタンをクリックします。

ステップ 3 必要な ASA ユーザーグループをリストから選択して [OK] をクリックします。必要なグループがすでに存在する場合は終了です。

必要な ASA ユーザーグループが存在しない場合、[作成（Create）]（+）をクリックして作成します。[Add ASA User Group] ダイアログボックスが開き、ASA ユーザ グループ オブジェクトに設定可能な設定のリストが表示されます。このダイアログボックスの要素の詳細については、[ASA Group Policies] ダイアログボックスを参照してください。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 ASA ユーザーグループの属性と値をデバイスのローカルに保存するか、外部サーバーに保存するかを選択します。

（注） ASAユーザーグループの属性を外部サーバーに保存することを選択した場合は、テクノロジー設定を行う必要はありません。認証に使用する AAA サーバーグループと AAA サーバーのパスワードを指定して [OK] をクリックし、オブジェクトセレクタでグループを選択して [OK] をクリックすることで、ポリシーにグループを追加します。

ステップ 6 ASA ユーザーグループの属性をデバイスのローカルに保存することを選択した場合は、[テクノロジー（Technology）] リストから、ASA ユーザーグループを作成する VPN のタイプを選択します。

- [Easy VPN/IPSec IKEv1]：IKE バージョン 1 ネゴシエーションを使用するリモート アクセス IPsec VPN 用。
- [Easy VPN/IPSec IKEv2]：（ASA のみ）IKE バージョン 2 ネゴシエーションを使用するリモートアクセス IPsec VPN 用。
- [SSLクライアントレス（SSL Clientless）]：（ASA のみ）SSL VPN、すべてのアクセスモード用（クライアントレスだけではない）。

ステップ 7 Easy VPN/IPSec IKEv1 および Easy VPN/IPSec IKEv2 のユーザ グループを設定するには、[Settings] ペインの [Easy VPN/IPSec VPN] フォルダから次のことを実行します。

a) [クライアント設定（Client Configuration）] を選択して、Cisco クライアントパラメータを設定します。これらの設定の詳細については、ASA グループ ポリシーのクライアント設定を参照してください。

b) [クライアントのファイアウォール属性（Client Firewall Attributes）] を選択して、VPN クライアントのファイアウォール設定を行います。これらの設定の詳細については、ASA グループ ポリシーのクライアント ファイアウォール属性を参照してください。

c) [ハードウェアクライアント属性（Hardware Client Attributes）] を選択して、VPN 3002 ハードウェアクライアント設定を行います。これらの設定の詳細については、ASA グループ ポリシーのハードウェア クライアント属性を参照してください。

d) [IPsec] を選択して、トンネリングプロトコル、フィルタ、接続設定、およびサーバーを指定します。これらの設定の詳細については、ASA グループ ポリシーの IPSec 設定を参照してください。

ステップ 8 SSL VPN のユーザ グループを設定するには、[Settings] ペインの SSL VPN フォルダから次の手順を実行します。

a) [クライアントレス（Clientless）] を選択して、SSL VPN で企業ネットワークへのクライアントレス アクセス モードを設定します。これらの設定の詳細については、ASA グループ ポリシーの SSL VPN クライアントレス設定を参照してください。

b) [フルクライアント（Full Client）] を選択して、SSL VPN で企業ネットワークへのフル クライアント アクセス モードを設定します。これらの設定の詳細については、ASA グループ ポリシーの SSL VPN フル クライアント設定を参照してください。

c) [設定（Settings）] を選択して、SSL VPN のクライアントレス アクセス モードおよびシンクライアント（ポートフォワーディング）アクセスモードに必要な全般設定を行います。これらの設定の詳細については、ASA グループ ポリシーの SSL VPN 設定を参照してください。

ステップ 9 [Settings] ペインの Easy VPN/IPSec IKEv1 または IKEv2 VPN および SSL VPN 設定で、ASA ユーザ グループに次の設定を指定します。

a) [DNS/WINS] を選択して、DNS サーバーと WINS サーバー、および ASA ユーザーグループに関連付けられたクライアントにプッシュされるドメイン名を定義します。これらの設定の詳細については、ASA グループ ポリシーの DNS/WINS 設定を参照してください。

b) [スプリットトンネリング（Split Tunneling）] を選択して、条件に応じてリモートクライアントが暗号化されたパケットをセキュアトンネル経由でセントラルサイトに送信できるようにし、同時にネットワーク インターフェイスを介したインターネットへのクリアテキストトンネルを許可します。これらの設定の詳細については、ASA グループ ポリシーのスプリット トンネリング設定を参照してください。

c) [接続設定（Connection Settings）] を選択して、セッション、アイドルタイムアウト、およびバナーテキストなど、ASA ユーザーグループの SSL VPN 接続設定を行います。これらの設定の詳細については、ASA グループ ポリシーの接続設定を参照してください。

ステップ 10 [OK] をクリック

ステップ 11 ASA ユーザーグループをリストから選択して [OK] をクリックします。

SSL VPN サーバー検証（ASA）について

クライアントレス SSL VPN 経由でリモート SSL 対応サーバに接続する場合は、リモート サーバを信頼できること、また、接続先が実際にサーバであることを認識することが重要です。ASA 9.0 には、クライアントレス SSL VPN の信頼できる認証局（CA）証明書のリストに対する SSL サーバ証明書の検証のためのサポートが追加されています。

HTTPS プロトコルを使用して Web ブラウザ経由でリモート サーバに接続する場合、サーバはサーバ自体を識別するために CA が署名したデジタル証明書を提供します。Web ブラウザには、サーバ証明書の有効性を検証するために使用される一連の CA 証明書が付属しています。これは、公開キー インフラストラクチャ（PKI）の 1 つの形式です。

ブラウザが証明書管理の機能を提供するのと同様に、ASA も信頼できる証明書のプール管理機能の形式を提供します（trustpools）。これは、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には、Web ブラウザで提供されるのと同様のデフォルトの証明書のバンドルが含まれますが、管理者がアクティブにするまで非アクティブとなります。

（注） すでに Cisco IOS の trustpools に精通している場合、ASA バージョンが、似ているが同じではないことがわかります。

信頼できる証明書の管理の詳細については、次のトピックを参照してください。

- SSL VPN サーバー検証の設定（ASA） （102 ページ）
- 信頼できるプール設定の設定（ASA） （42 ページ）
- Trustpool Manager の使用 （45 ページ）

信頼できるプール設定の設定（ASA）

[信頼できるプールの設定（Trusted Pool Settings）] ページを使用して、証明書失効のオプションを設定します。Trustpool Manager を起動することもできます。

ナビゲーション パス

（デバイスビューのみ）ASA デバイスを選択し、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [信頼できるプール（Trusted Pool）]** を選択します。

関連項目

- SSL VPN サーバー検証の設定（ASA） （102 ページ）
- Trustpool Manager の使用 （45 ページ）

フィールド リファレンス

表 *12 : [*信頼できるプール（*Trusted Pool*）*]* ページ

要素	説明
失効チェック	証明書の失効をチェックするかどうかを指定します。適切なオプションを選択します。 • [証明書をチェックする（Check Certificates）] このオプションを選択する場合は、適切な方法（CRL または OCSP）を選択し、[>>] をクリックして、右側のボックスに移動して、失効に使用する方法を 1 つ、または複数指定します。 （注） いずれか一方または両方の方法を選択できます。両方の方法を選択する場合は、使用する順序で方法を追加します。 • [証明書をチェックしない（Do not check Certificates）]
証明書マップの設定	必要に応じて、次のリストからマップを選択して、証明書マップのオーバーライドオプションを指定します。各リストには、デバイスに設定されているすべての証明書マップが含まれます。 • [期限切れの証明書を許可（Allow Expired Certificates）]：期限切れの証明書を許可する証明書マップを選択します。 • [失効チェックをスキップ（Skip Revocation Check）]：失効チェックをスキップする証明書マップを選択します。
CRL Options	証明書失効リストを管理するためのオプションを指定します。 • [キャッシュ更新時間（Cache Refresh Time）]：CRL が古すぎて信頼できないと ASA が判断するまでの分数（1 ～ 1440）。デフォルト値は 60 分です。 • [次のCRL更新を実施（Enforce next CRL update）]：ASA が次の CRL 更新を実施する必要があるかどうかを指定します。

要素	説明
証明書有効期限のアラート（Certificate Expiration Alerts）	バージョン 4.9 以降、Cisco Security Manager では、24 時間ごとに、トラストポイントにおけるすべての CA および ID 証明書の有効期限のチェックが可能になっています。証明書の有効期限がまもなく切れる場合は、syslog がアラートとして発行されます。リマインダおよび繰り返しの間隔を設定できます。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。 [開始（Begin）]：最初のアラートが送信される有効期限までの日数を入力します。範囲は 1 ～ 90 日です。デフォルトでは、リマインダは有効期限の 60 日前に開始されます。 [繰り返し（Repeat）]：証明書が更新されない場合にアラートが繰り返される頻度を日数で入力します。範囲は 1 ～ 14 日です。デフォルトでは、リマインダは 7 日ごとに送信されます。
自動インポート	バージョン 4.10 以降、Cisco Security Manager では Trustpool 証明書バンドルの自動インポートが有効になります。自動インポートを有効にすると、Trustpool 証明書バンドルのダウンロードとインポートに ASA が使用する URL を設定できます。この機能は、ASA ソフトウェアバージョン 9.5(2) 以降を実行しているデバイスでのみサポートされます。 バージョン 4.13 以降、Cisco Security Manager には、ASA が宛先 URL を識別するために使用できる送信元インターフェイスオプションが用意されています。この機能は、9.7.1 より前の ASA バージョンではサポートされていません。 [インターフェイス（Interface）]：[選択（Select）] ボタンをクリックして、インターフェイスを選択します。設定されたインターフェイスが管理専用の場合、宛先 URL は管理 VRF を介してルーティングされます。非管理インターフェイスの場合、URL はデータ VRF を介してルーティングされます。インターフェイスが指定されていない場合、管理 VRF とデータ VRF の両方のルーティングテーブルがポーリングされ、URL に到達するルートが識別されます。 [URLからインポート（Import from a URL）：ASA が Trustpool 証明書バンドルをダウンロードする URL を入力します。 [ダウンロード時刻（Download Time）]：ASA が証明書バンドルをダウンロードする時刻を入力します。インポートは、ここで指定した時刻に毎日実行されます。 URL のデフォルト値は http://www.cisco.com/security/pki/ios_core.p7b で、ダウンロード時刻のデフォルト値は 22:00:00 です。

要素	説明
Trustpool Managerの起動（Launch Trustpool Manager）	Trustpool 証明書の管理に使用される Trustpool Manager を起動します。Trustpool Manager を使用して、以下を実行できます。 詳細については、Trustpool Manager の使用 （45 ページ）を参照してください。

Trustpool Manager の使用

Trustpool Manager を使用して、trustpool に含まれる証明書を管理します。Trustpool Manager は、次の機能を提供します。

- trustpool の更新
- 証明書のバンドルのインポート
- 証明書のバンドルのエクスポート
- trustpool からの証明書の削除

ナビゲーション パス

（デバイスビューのみ）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [Trusted Pool] を選択し、次に [Trustpool Managerの起動（Launch Trustpool Manager）] をクリックします。

trustpool の更新

次のいずれかの条件が満たされる場合は、trustpool を更新する必要があります。

- trustpool の証明書が期限切れまたは再発行されている。
- 公開された CA 証明書のバンドルに、特定のアプリケーションで必要な追加の証明書が含まれている。

trustpool の証明書を更新するには、[証明書の更新（Refresh Certificates）] をクリックします。

証明書のバンドルのインポート

次の形式のいずれかで、さまざまな場所から個々の証明書または証明書のバンドルをインポートできます。

- pkcs7 構造でラップされた DER 形式の x509 証明書
- PEM 形式（PEM ヘッダーに囲まれた）の連結した x509 証明書のファイル

証明書またはバンドルをインポートするには、次の手順を実行します。

1. [Import Bundle] をクリックします。

2. バンドルの場所を選択します。
   - [シスコの公開署名済みルートファイル配布からのインポート（Import from Cisco published signed root file distribution）]：公開配布サイトからインポートするには、このオプションを選択します。
   - [URLからインポート（Import from a URL）]：バンドルがサーバーでホストされている場合は、このオプションを選択します。リストからプロトコルを選択し、ボックスに URL を入力します。
   - [デバイスでファイルをバンドル（Bundle file on device）]：バンドルが ASA フラッシュファイルシステムに保存されている場合はこのオプションを選択し、バンドルへのパスを入力します。
   - [バンドルファイルを選択（Select bundle file）]：バンドルがマシンに保存されている場合は、[ファイルからインポート（Import from a file）] をクリックし、[ローカルファイルを参照（Browse Local Files）] をクリックして、バンドルに移動します。
3. 次のインポートオプションを指定します。
   - [インポートする前にすべての証明書をクリア（Clear all certificates before import）]：バンドルをインポートする前に trustpool をクリアするかどうか。
   - [署名の検証が失敗または実行できない場合にバンドルをインポートし続ける（Continue to import the bundle if signature validation fails or can't be performed）]：署名を検証できない場合にインポートを続行するかどうか。
4. [インポート（Import）] をクリックします。

証明書のバンドルのエクスポート

trustpool を正しく設定したら、プールをエクスポートする必要があります。これにより、このポイントまで（たとえばエクスポート後に trustpool に追加された証明書を削除する場合など）trustpool を復元できます。Security Manager サーバーファイルシステムまたはローカルファイルシステムにプールをエクスポートできます。

証明書のバンドルをエクスポートするには、次の手順を実行します。

1. [バンドルのエクスポート（Export Bundle）] をクリックします。
2. [参照（Browse）] をクリックします。
3. エクスポート先のファイルシステム（ローカルマシンまたは Security Manager サーバー）に対応するタブを選択します。
4. trustpool を保存するフォルダに移動します。
5. [File name] ボックスに、trustpool の一意の覚えやすい名前を入力します。
6. [保存（Save）] をクリックします。

Trustpool からの証明書の削除

次の方法を使用して、trustpool から証明書を削除できます。

- 個別の証明書を削除するには、証明書を選択して [削除（Delete）] をクリックします。
- デフォルトのバンドルの一部ではないすべての証明書を削除するには、[Trustpoolのクリア（Clear Trustpool）] をクリックします。

（注） trustpool をクリアする前に、必要に応じて現在の設定を復元できるように、現在の trustpool をエクスポートする必要があります。

関連項目

- SSL VPN サーバー検証の設定（ASA） （102 ページ）
- 信頼できるプール設定の設定（ASA） （42 ページ）

[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス

[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックスを使用して、証明書のユーザー名のマッピングに使用するスクリプトを定義します。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [証明書スクリプトのユーザー名（Username from Cert Scripts）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [証明書スクリプトのユーザー名（ASA）（Username from Cert Scripts (ASA)）]** を選択します。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 *13 : [*スクリプトの追加/編集（*Add/Edit Scripts*）*]* ダイアログボックス

要素	説明
スクリプト名（Script Name）	スクリプトの名前を指定し、トンネルグループAAA認証および許可でスクリプトを使用します。スクリプト名は、認証と許可で異なる場合があります。ここでスクリプトを定義すると、CLI で同じスクリプトを使用してこの機能を実行できます。
スクリプトパラメータの選択（Select Script Parameters）	スクリプトの属性および内容を指定します。
ユーザー名の値（Value for Username）	ユーザー名（サブジェクト DN）として使用する標準的な DN 属性のドロップダウンリストから属性を選択します。
フィルタリングなし（No Filtering）	指定した DN 名全体を使用することを指定します。
部分文字列によるフィルタ処理（Filter by Substring）	開始インデックス（一致する最初の文字の文字列内の位置）および終了インデックス（検索する文字列数）を指定します。このオプションを選択する場合、開始インデックスは、空白にはできません。終了インデックスを空白にするとデフォルトは-1となり、文字列全体が一致するかどうか検索されます。
正規表現でフィルタ処理（Filter by Regular Expression）	検索に適用する正規表現を [正規表現（Regular Expression）] フィールドに入力します。一般的な正規表現の演算子が適用されます。
カスタムスクリプトをLUA形式で使用（Use Custom Script in LUA format）	検索フィールドを解析するために、LUA プログラム言語で記述されたカスタムスクリプトを指定します。このオプションを選択すると、カスタム LUA スクリプトを入力できるフィールドが使用可能になります。 以下は、LUA 形式のカスタムスクリプトの例です。 • "return findpattern(cert.subject.cn,"%a+")" • local a,b,c; a,b,c = string.find(cert.subject.fulldn, ’,cn=(.+),cn=Users’); cを返します。 （注） LUA では、大文字と小文字が区別されます。 次の表にLUA スクリプトで使用可能な属性名と属性の説明を示します。

表 *14 : LUA* スクリプトの属性

属性	説明
cert.subject.c	Country
cert.subject.cn	Common Name
cert.subject.dnq	DN 修飾子
cert.subject.ea	電子メール アドレス
cert.subject.genq	世代修飾子
cert.subject.gn	名
cert.subject.i	イニシャル
cert.subject.l	地名
cert.subject.n	名前
cert.subject.o	マニュアルの構成
cert.subject.ou	組織単位
cert.subject.ser	サブジェクト シリアル番号
cert.subject.sn	姓
cert.subject.sp	州/県
cert.subject.t	Title
cert.subject.uid	ユーザー ID
cert.issuer.c	Country
cert.issuer.cn	Common Name
cert.issuer.dnq	DN 修飾子
cert.issuer.ea	電子メール アドレス
cert.issuer.genq	世代修飾子
cert.issuer.gn	名
cert.issuer.i	イニシャル
cert.issuer.l	地名
cert.issuer.n	名前

属性	説明
cert.issuer.o	マニュアルの構成
cert.issuer.ou	組織単位
cert.issuer.ser	発行元シリアル番号
cert.issuer.sn	姓
cert.issuer.sp	州/県
cert.issuer.t	Title
cert.issuer.uid	ユーザー ID
cert.serialnumber	証明書シリアル番号
cert.subjectaltname.upn	ユーザー プリンシパル名

IPSec VPN ポリシーの使用

IPSec VPN に対しては、特定のポリシーを設定する必要があります。次のトピックでは、これらのリモート アクセス IPsec VPN ポリシーについて説明します。ただし、IKE プロポーザル ポリシーは、IKE プロポーザルの設定で説明します。

ここでは、次の内容について説明します。

- Certificate to Connection Profile Map ポリシーの設定（ASA） （50 ページ）
- リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）（56 ページ）

Certificate to Connection Profile Map ポリシーの設定（ASA）

Certificate to Connection Profile Map ポリシーは、リモート アクセス IKEv1 IPSec VPN の ASA デバイスでの拡張証明書認証に使用されます。これらは、リモート アクセス IKEv2 IPSec または SSL VPN では使用されません。

Certificate to Connection Profile Map ポリシーにより、指定したフィールドに基づいて、ユーザーの証明書を権限グループと照合するルールを定義できます。認証を確立するため、証明書の任意のフィールドを使用することも、またはすべての証明書ユーザが権限グループを共有することもできます。グループは、DN ルール、[Organization Unit (OU)] フィールド、IKE ID、またはピア IP アドレスから照合できます。これらの方式のいずれかまたはすべてを使用できます。

証明書の DN フィールドに基づいてユーザ権限グループを照合するには、照合するフィールドを指定したルールをグループに定義し、その選択グループに対して各ルールをイネーブルにし

ます。接続プロファイルにルールを作成するには、設定に接続プロファイルが存在している必要があります。

ここでは、ASA サーバデバイスに接続を試みるリモート クライアントの Certificate to Connection Profile Map ポリシーを設定する方法について説明します。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [IPSec VPN] > [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）] > [ポリシー（Policies）] 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 [リモートアクセス VPN（Remote Access VPN）] > [IPSec VPN] > [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）] > [ポリシー（Policies）] を選択します。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。

[Certificate to Connection Profile Map Policies] ページが開きます。

ステップ 2 次のいずれか、またはすべてのオプションを選択して、認証を確立し、クライアントをマッピングする接続プロファイル（トンネル グループ）を決定します。

- [設定されているルールを使用して証明書をグループと照合（Use Configured Rules to Match a Certificate to a Group）]：[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）] ポリシーで定義されているルールを使用します。ルールの設定については、証明書/接続プロファイル マップ ルールの設定（ASA） （51 ページ）を参照してください。
- [証明書の組織ユニット（OU）フィールドを使用してグループを決定（Use Certificate Organization Unit (OU) Field to Determine the Group）]：クライアント証明書の組織ユニット（OU）フィールドを使用します。
- [IKE ID を使用してグループを決定（Use IKE Identify to Determine the Group）]：IKE ID を使用します。
- [ピアの IP アドレスを使用してグループを決定（Use Peer IP address to Determine the Group）]：ピアの IP アドレスを使用します。
- [グループ URL と証明書マップが異なる接続プロファイルと一致する場合はグループ URL を使用する（Use Group URL if Group URL and Certificate Map match different Connection profiles）] は、マルチコンテキストモードの ASA 9.5（2）リモートアクセス VPN でサポートされます。

証明書/接続プロファイル マップ ルールの設定（ASA）

証明書/接続プロファイルマップを設定して、[設定されているルールを使用して証明書をグループと照合（Use Configured Rules to Match a Certificate to a Group）]（Certificate to Connection Profile Map ポリシーの設定（ASA） （50 ページ）を参照）オプションを選択した場合、ユーザ証明書に基づいたユーザと接続プロファイルとの照合に必要なルールを設定する必要があります。

証明書のフィールドに基づいてユーザ権限グループを照合するには、照合するフィールドを指定したルールをグループに定義し、その選択グループに対して各ルールをイネーブルにします。ルールを作成してマッピングする前に、接続プロファイル（トンネル グループ）を定義する必要があります。

ここでは、証明書/接続プロファイル マップ ルール、および ASA サーバ デバイスに接続を試みるリモート クライアントのパラメータを設定する方法について説明します。

ヒント Certificate to Connection Profile Map ポリシーは、リモート アクセス IKEv1 IPSec VPN だけに適用されます。IKEv2 または SSL VPN には適用されません。

はじめる前に

- マッピング ルールを作成する接続プロファイルがデバイスで設定されていることを確認してください。接続プロファイルの設定（ASA、PIX 7.0+）　（9 ページ）を参照してください。
- [証明書から接続プロファイルへのマップポリシー（Certificate to Connection Profile Maps Policies）] ポリシーで [設定されているルールを使用して証明書をグループと照合（Use Configured Rules to Match a Certificate to a Group）] を選択したことを確認します。Certificate to Connection Profile Map ポリシーの設定（ASA）　（50 ページ）を参照してください。

ステップ 1　（デバイス ビュー限定）ASA デバイスを選択して、ポリシー セレクタから **[リモートアクセス VPN（Remote Access VPN）] > [IPSec 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）]** を選択します。

[Certificate to Connection Profile Map Rules] ページが表示されます。ポリシーには次の 2 つのテーブルがあります。

- **マップテーブル（上半分のテーブル）**：上半分のテーブルには、証明書/接続マップルールを定義するすべての接続プロファイルのリストが示されます。各行はプロファイル マップであり、マップされる接続プロファイルの名前、マップのプライオリティ（数字が小さいほどプライオリティが高い）およびマップ名が含まれます。同じ接続プロファイルに複数のマップを設定できます。
  - このマップに規則を設定するには、規則を選択し、規則テーブルを使用して規則を作成、編集、および削除します。
  - マップを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Map Rule] ダイアログボックス（上半分のテーブル）　（54 ページ）に入力します。
  - （ルールではなく）マッププロパティを編集するには、マッププロパティを選択し、[行の編集（Edit Row）] ボタンをクリックします。
  - マップ全体を削除するには、マップを選択し、[行の削除（Delete Row）] ボタンをクリックします。

- **ルールテーブル（下半分のテーブル）**：上半分のテーブルで選択されているマップのルール。マップが上半分のテーブルで実際に選択されていることを確認する必要があります。ルールテーブルの上にあるグループタイトルに、[（接続プロファイル名）の詳細（Details for (Connection Profile Name)）] と表示されます。

マップを選択すると、そのマップに設定されているすべての規則がテーブルに表示されます。このテーブルには、フィールド（[subject] または [issuer]）、証明書コンポーネント、一致演算子、および規則によって検索される値などが表示されます。デバイスがマップされた接続プロファイルを使用するには、リモート ユーザはすべての設定済みルールをマップと照合する必要があります。

- ルールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Map Rule] ダイアログボックス（下半分のテーブル） （55 ページ）に入力します。
- ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- ルールを削除するには、ルールを選択し、[Delete Row] ボタンをクリックします。

ステップ 2 ルールをマップに追加するには、次の手順を実行します。

a) 上半分のテーブルでマップを選択します。

マップが存在しない場合、上側のテーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックして作成し、マップ作成に関する情報を [マップルール（Map Rule）] ダイアログボックスに入力します。このダイアログボックスでは、マップの接続プロファイルを選択して、1 ～ 65535（数値が低いほどプライオリティが高くなります）の相対的プライオリティを割り当て、一意のマップ名を割り当てる必要があります。

b) マップが実際に選択されていることを確認してください。テーブルのマップが強調表示されているだけでは選択されていることにはなりません。下側のテーブルの上にあるヘッダーは、[（接続プロファイル名）の詳細（Details for (Connection Profile Name)）] でなければなりません。新規に作成されたマップでないかぎり、テーブルには、いくつかのルールが表示されます。

c) リモートクライアントがこのマップのプロファイルを使用するデバイスに接続するために満たす必要がある新しい証明書を、接続プロファイル照合ルールに追加するには、下側のテーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックします。これにより、さまざまなフィールドを示す [Map Rule] ダイアログボックスが開きます。

（注） 「設定が見つかりません。マッピングフィールドには値IDが必要です。マッピングを選択してください（Missing Settings, A value ID required for Mapping field, Please select a Mapping）」というエラーメッセージが表示された場合、上側のテーブルでマップが正常に選択されていません。必要なマップをもう一度クリックしてください。

d) [フィールド（Field）] リストから、ルールにより、クライアント証明書の Subject フィールドまたは Issuer フィールドが検証されるかどうかを選択します。

e) [コンポーネント（Component）] リストから、一致ルールに対して使用するクライアント証明書のコンポーネントを選択します。

f) [演算子（Operator）] フィールドから、コンポーネントと [値（Value）] フィールドの比較方法を [次と等しい（Equals）]（完全一致）、[次を含む（Contains）]（値全体が存在）、[次に等しくない（Does Not Equal）]、[次を含まない（Does Not Contain）] から選択します。

g) [値（Value）] フィールドで、照合する値を指定し、[OK] をクリックしてルールを保存します。

h) 必要に応じて、別の記録をマップに追加します。

ステップ 3 [デフォルトの接続プロファイル（Default Connection Profile）] フィールドで、いずれのマップルールにも一致しないユーザに使用する接続プロファイルを選択します。

[Map Rule] ダイアログボックス（上半分のテーブル）

[Certificate to Connection Profile Maps] > [Rules policy] の上側にマップ テーブルに対して開かれた [Map Rule] ダイアログボックスを使用して、マップを設定します。次に、このマップに対して、[Rules policy] の下半分のテーブルでルールを設定できます。これらのマップおよび関連付けられるルールの詳細については、を参照してください。 証明書/接続プロファイル マップ ルールの設定（ASA） （51 ページ）

ナビゲーション パス

（デバイスビューだけ）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [証明書/接続プロファイルマップ（Certificate to Connection Profile Maps）] > [ルール（Rules）] を選択します。上側のテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、上側のテーブルでマップを選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 *15 : [Map Rule]* ダイアログボックス（上半分のテーブル）

要素	説明
マップ名（Map Name）	接続プロファイル マップの名前。
プライオリティ	一致ルールのプライオリティ番号（1 ～ 65535）。番号が小さいほどプライオリティが高くなります。たとえば、プライオリティ番号が 2 の一致ルールは、プライオリティ番号が 5 の一致ルールよりもプライオリティが高くなります。 複数のマップを作成した場合、それらのマップはプライオリティの順に処理されます。ユーザがマップされるプロファイルは最初の一致ルールによって決まります。
接続プロファイル	一致ルールを作成する IPSec 用および SSL 用の接続プロファイルを選択します。いずれかの接続プロファイルまたは両方の接続プロファイルを選択する必要があります。この接続プロファイルに接続しようとするクライアントは、デバイスに接続するための関連付けられた一致ルールの条件を満たす必要があります。 IPSec 用の接続プロファイルは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

[Map Rule] ダイアログボックス（下半分のテーブル）

[Certificate to Connection Profile Maps] > [Rules policy] の下側のルール テーブルに対して開かれた [Map Rule] ダイアログボックスを使用して、マップ テーブル（[Rules policy] の上側のテーブル）で選択されているマップのルールを設定します。これらのルールの設定の詳細については、証明書/接続プロファイル マップ ルールの設定（ASA） （51 ページ）を参照してください。

ナビゲーション パス

（デバイスビューのみ）ASA デバイスを選択し、ポリシーセレクタから **[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）]** を選択します。下半分のテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、下半分のテーブルでルールを選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 *16 : [Map Rule]* ダイアログボックス（下半分のテーブル）

要素	説明
フィールド	クライアント証明書の [件名（Subject）] または [発行元（Issuer）] に従って、一致ルールのフィールドを選択します。
コンポーネント	一致規則に対して使用するクライアント証明書のコンポーネントを選択します。
演算子	一致ルールの演算子を次のうちから選択します。 • [Equals]：証明書コンポーネントは、入力された値と一致する必要があります。完全に一致しない場合、接続は拒否されます。 • [Contains]：証明書コンポーネントには、入力された値が含まれている必要があります。コンポーネントにその値が含まれていない場合、接続は拒否されます。 • [等しくない（Does Not Equal）]：証明書コンポーネントは、入力された値と異なっている必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値が US と等しければ、接続が拒否されます。 • [次を含まない（Does Not Contain）]：証明書コンポーネントには、入力された値が含まれていない必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値に US が含まれていると、接続が拒否されます。

要素	説明
値	一致ルールの値。入力された値は、選択されたコンポーネントおよび演算子と関連付けられています。
Default Connection Profile	このオプションは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

リモートアクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、サーバが ASA または PIX 7.0+ デバイスである場合のリモート アクセス VPN サーバの IPsec プロポーザルを作成または編集する方法について説明します。

（注） Cisco Security Manager バージョン 4.17 以降では、ソフトウェアバージョン 9.9(2) 以降を実行している ASA マルチコンテキストデバイスで IPSec プロポーザルポリシーを設定および展開できます。

Catalyst 6500/7600 デバイスなど、IOS または PIX 6.3 デバイスの IPsec プロポーザルを設定する場合は、リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）を参照してください。

IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプトマップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。

IPsec プロポーザルを設定する場合は、リモート アクセス クライアントがサーバに接続する外部インターフェイス、IKE ネゴシエーション中に使用する IKE バージョン、および VPN トンネル内のデータを保護する暗号化と認証のアルゴリズムを定義する必要があります。逆ルート注入および NAT 通過をイネーブルにすることもできます。

IPsec トンネルの概念の詳細については、IPsec プロポーザルについてを参照してください。

関連項目

- テーブル カラムおよびカラム見出しの機能

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（ASA/PIX 7.x）（IPsec Proposal (ASA/PIX 7.x)）]** 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、[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（ASA/PIX 7.x）（IPsec Proposal (ASA/PIX 7.x)）] を選択します。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。

[IPsec Proposal] ページが開き、VPN エンドポイント、IPsec トランスフォーム セット、および逆ルート注入がプロポーザルで設定されているかどうかなど、設定されているプロポーザルが一覧表示されます。

ステップ 2 次のいずれかを実行します。

- 新しいIPsecプロポーザルを追加するには、[行の追加（Add Row）]（+）ボタンをクリックして、[IPsec Proposal Editor] ダイアログボックスに入力します。使用可能なオプションの詳細については、[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス）（57 ページ）を参照してください。
- 既存のプロポーザルを編集するには、プロポーザルを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- プロポーザルを削除するには、そのプロポーザルを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

[IPsec Proposal Editor] を使用して、ASA または PIX 7.0+ デバイスの IPsec プロポーザルを作成または編集します。

このダイアログボックスの要素は、選択したデバイスによって異なります。次の表に、ASA または PIX 7.0+ デバイスを選択したときの [IPsec Proposal Editor] ダイアログボックス内の [General] タブの要素を示します。

（注） PIX 7.0+ または ASA デバイスを選択したときのダイアログボックス内の要素の詳細については、IPsec Proposal Editor（IOS、PIX 6.3 デバイス）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（ASA/PIX 7.x）（IPsec Proposal (ASA/PIX 7.x)）] を選択します。[Add Row]（+）または [Edit Row]（鉛筆）ボタンをクリックします。

- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）]>[IPSec VPN]>[IPsecプロポーザル（ASA/PIX 7.x）（IPsec Proposal (ASA/PIX 7.x)）]を選択します。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。[Add Row]（+）または [Edit Row]（鉛筆）ボタンをクリックします。

関連項目

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）
- IPsec プロポーザルについて
- インターフェイス ロール オブジェクトの作成
- AAA サーバ グループ オブジェクトの作成

フィールド リファレンス

表 *17 : [IPsec Proposal Editor]*（*ASA* および *PIX 7.0+* デバイス）

要素	説明
外部インターフェイス	リモート アクセス クライアントがサーバへの接続に使用する外部インターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力します。あるいは、[選択（Select）]をクリックして選択するか、または新しいオブジェクトを作成します。
Enable IKEv1 Enable IKEv2	IKE ネゴシエーション中に使用する IKE バージョン。IKEv2 は、Anyconnect 3.0+ クライアントの ASA ソフトウェア リリース 8.4(1)+ だけでサポートされます。必要に応じて、いずれかまたは両方のオプションを選択します。

要素	説明
クライアントサービスの有効化（Enable Client Services） Client Services Port Number	IKEv2 を有効にした場合だけ使用できます。 この接続の ASA のクライアント サービス サーバをイネーブルにするかどうかを選択します。クライアントサービスサーバーは、HTTPS（SSL）アクセスを提供します。これにより、Secure Client ダウンローダは、ソフトウェアアップグレード、プロファイル、ローカリゼーションおよびカスタマイゼーションファイル、CSD、SCEP、および セキュアクライアント が必要とするその他のファイルダウンロードを受信できます。このオプションを選択する場合、クライアント サービス ポート番号（デフォルトは 443）を指定します。 クライアントサービスサーバーを有効にしない場合、ユーザーは、セキュアクライアント が必要とする可能性があるこれらのファイルをダウンロードできません。 **ヒント** 同じデバイスで実行する SSL VPN に対して同じポートを使用できます。SSL VPN を設定した場合でも、IKEv2 IPsec クライアントで SSL を介してファイルをダウンロードするには、このオプションを選択する必要があります。
IKEv1 トランスフォーム セット IKEv2 トランスフォーム セット	トンネル ポリシーで使用するトランスフォーム セット。トランスフォーム セットは、トンネル内のトラフィックの確立に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。トランスフォーム セットは、各 IKE バージョンで異なるため、サポートされているバージョンごとにオブジェクトを選択します。それぞれ最大 11 個のトランスフォーム セットを選択できます。詳細については、トランスフォーム セットの概要を参照してください。 選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォーム セットが使用されます。 [選択（Select）] をクリックして、トポロジで使用する IPsec トランスフォーム セット ポリシー オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクトリストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定を参照してください。

要素	説明
リバース ルート インジェクション（Reverse Route Injection）	リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。詳細については、逆ルート注入についてを参照してください。 次のいずれかのオプションを選択して、クリプト マップで RRI を設定します。 • [なし（None）]：クリプトマップで RRI の設定を無効にします。 • [標準（Standard）]：クリプトマップのアクセス制御リスト（ACL）で定義されている宛先情報に基づいて、ルートが作成されます。これがデフォルトのオプションです。
Enable Network Address Translation Traversal	Network Address Translation Traversal（NAT-T; ネットワーク アドレス変換通過）を許可するかどうか。 NAT 通過は、VPN 接続されたハブとスポークの間に、IPsec トラフィックに対してネットワーク アドレス変換（NAT）を実行するデバイスがある場合に使用します。NAT 通過については、VPN での NAT についてを参照してください。
[ESPv3設定（ESPv3 Settings）]（ASA 9.0.1+ のみ） 着信 ICMP エラーメッセージの検証先を暗号化マップとダイナミック暗号化マップのどちらにするかを指定し、セキュリティ単位のアソシエーションポリシーを設定するか、トラフィック フローパケットを有効にします。	
[着信ICMPのエラーメッセージを検証（Validate incoming ICMP error messages）]	IPsec トンネル経由で受信し、プライベートネットワーク上の内部ホストが宛先である ICMP エラーメッセージを検証するかどうかを指定します。
[フラグメント禁止（DF）ポリシーを有効にする（Enable Do Not Fragment (DF) Policy）]	IP ヘッダーに Do-Not-Fragment（DF）ビット セットを持つ大きなパケットを IPsec サブシステムがどのように処理するかを定義します。次のいずれかを実行します。 • 設定（Set）：DF ビットを設定して使用します。 • コピー（Copy）：DF ビットを保持します。 • クリア（Clear）：DF ビットを無視します。

要素	説明
トラフィック フロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）	トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。 （注） TFC を有効にする前に、[トンネルポリシー（クリプトマップ）（Tunnel Policy (Crypto Map)）] の [基本（Basic）] タブで IKE v2 IPsec プロポーザルを設定しておく必要があります。IKEv1 が有効になっている場合、トラフィックフローの機密性は利用できません。 バースト、ペイロードサイズ、およびタイムアウトパラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

SSL および IKEv2 IPSec VPN ポリシーの使用

SSL VPN に対しては、特定のポリシーを設定する必要があります。これらのポリシーは、リモートアクセス IKEv2 IPSec VPN でも使用されます。次に示すトピックでは、これらのリモートアクセス VPN ポリシーについて説明します。

ここでは、次の内容について説明します。

- SSL VPN アクセス ポリシーについて（ASA） （61 ページ）
- 他の SSL VPN 設定の定義（ASA） （71 ページ）
- SSL VPN 共有ライセンスの設定（ASA 8.2+） （104 ページ）

SSL VPN アクセス ポリシーについて（ASA）

アクセス ポリシーには、リモート アクセス SSL または IKEv2 IPsec VPN 接続プロファイルをイネーブルにできるセキュリティ アプライアンスのインターフェイス、接続プロファイルで使用するポート、Datagram Transport Layer Security（DTLS）設定、SSL VPN セッション タイムアウト、および最大セッション数を指定します。AnyConnect VPN クライアントまたは Secure Client Essentials を使用するかどうかも指定できます。

Anyconnect VPN クライアントの詳細については、SSL VPN セキュアクライアント の設定について （86 ページ）を参照してください。この他のトピックでは、DTLS および Secure Client Essentials について詳しく説明します。

Datagram Transport Layer Security（DTLS）

Datagram Transport Layer Security（DTLS）を有効にすると、SSL VPN 接続を確立している セキュアクライアント で、2 つのトンネル（SSL トンネルと DTLS トンネル）を同時に使用できます。DTLS を使用すると、SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。デ

フォルトでは、DTLS がイネーブルになるのは、インターフェイスで SSL VPN アクセスをイネーブルにした場合です。DTLS をディセーブルにすると、SSL VPN 接続は SSL VPN トンネルだけに接続します。

（注） DTLS が TLS 接続にフォールバックするためには、フォールバック トラストポイントを指定する必要があります。フォールバック トラストポイントが指定されていない場合に DTLS 接続に問題が発生すると、その接続は指定されたトラストポイントにフォールバックすることなく終了します。

AnyConnect Essentials VPN クライアント

Secure Client Essentials は SSL または IKEv2 IPsec の独立ライセンスの VPN クライアントで、適応型セキュリティアプライアンス全体に設定します。このクライアントは、次の例外を除き、Secure Client のすべての機能を備えています。

- CSD を使用できない（HostScan/Vault/Cache Cleaner を含む）
- クライアントレス SSL VPN 非対応
- Windows Mobile サポートがオプション

Secure Client Essentials により、Microsoft Windows Vista、Windows Mobile、Windows XP、Windows 2000、Linux、または Macintosh OS X を実行しているリモートエンドユーザーは、Cisco VPN Client の利点を得ることができます。この機能がディセーブルの場合は、AnyConnect VPN クライアント一式が使用されます。この機能は、デフォルトではディセーブルになっています。

（注） このライセンスは、SSL VPN の共有ライセンスと同時には使用できません。

ここでは、次の内容について説明します。

- [SSL VPN Access Policy] ページ （62 ページ）
- Access ポリシーの設定 （69 ページ）

[SSL VPN Access Policy] ページ

[SSL VPN Access Policy] ページを使用して、リモート アクセス SSL または IKEv2 IPsec VPN のアクセス パラメータを設定します。Access ポリシーの設定の詳細については、Access ポリシーの設定 （69 ページ）を参照してください。

ヒント このポリシーで指定するトラストポイントは、[公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーでも選択されている必要があります。詳細については、リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [アクセス（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、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [アクセス（ASA）（Access (ASA)）] を選択します。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

- SSL VPN アクセス ポリシーについて（ASA） （61 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 *18 : [SSL VPN Access Policy]* ページ

要素	説明
[Access Interface] テーブル	[Access Interface] テーブルには、リモート アクセス SSL または IKEv2 IPSec VPN 接続に設定されたインターフェイスのリストが表示されます。このテーブルには、インターフェイスがイネーブルでVPNアクセスが可能かどうか、DTLS がイネーブルにされているかどうか、クライアント証明書が必要かどうか、およびインターフェイスに使用されるトラストポイントなど、各インターフェイスのアクセス設定が表示されます。 • インターフェイスでアクセスを設定するには、[行の追加（Add Row）]（+）ボタンをクリックします（[Access Interface Configuration] ダイアログボックス （67 ページ）を参照）。 • インターフェイスのアクセス設定を編集するには、インターフェイスを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします（[Access Interface Configuration] ダイアログボックス （67 ページ）を参照）。 • インターフェイスのアクセス設定を削除するには、インターフェイスを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

要素	説明
[サーバー名指定（Server Name Indication）] テーブル	[サーバー名指定（Server Name Indication）] テーブルには、定義済みのサーバー名指定マッピングが一覧表示されています。 • サーバー名指定マッピングを定義するには、[行の追加（Add Row）]（+）ボタンをクリックします（[サーバー名表示（Server Name Indication）] ダイアログボックス （68 ページ）を参照）。 • 既存のマッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします（[サーバー名表示（Server Name Indication）] ダイアログボックス （68 ページ）を参照）。 • サーバー名指定マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
ポート番号（Port Number）	VPN セッションに使用するポート。HTTPS トラフィックの場合、デフォルト ポートは 443 です。HTTP ポート リダイレクションがイネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。デフォルト以外のポートを指定するには、1024 ～ 65535 の数値を指定します。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。 ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてポートリストオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） ポート番号を変更すると、現在の SSL VPN 接続がすべて（設定展開時に）終了するため、現在のユーザは再接続が必要になります。
DTLS Port Number	DTLS 接続に使用する UDP ポート。デフォルトのポートは 443 です。DTLS の詳細については、SSL VPN アクセス ポリシーについて（ASA） （61 ページ）を参照してください。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。 ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてポートリストオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Fallback Trustpoint	トラストポイントが割り当てられていないインターフェイスで使用するトラストポイント（認証局または CA サーバ）。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクト選択するか、新しいオブジェクトを作成します。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
Default Idle Timeout	SSL または IKEv2 IPSec VPN セッションがアイドル状態になってから、セキュリティアプライアンスがセッションを終了するまでの時間を指定します（秒単位）。 この値が適用されるのは、ユーザのグループ ポリシー内の [Idle Timeout] 値がゼロ（0）に設定されている場合、つまり、タイムアウト値がない場合だけです。それ以外の場合、グループ ポリシーの [Idle Timeout] 値が、ここで設定したタイムアウトに優先されます。入力可能な最小値は、60秒（1分）です。デフォルトは 30 分（1800 秒）です。最大値は 24 時間（86400 秒）です。 この属性は短い時間に設定することを推奨します。これは、クッキーをディセーブルにするブラウザ設定（またはプロンプトでクッキーを要求してから拒否するブラウザ設定）によって、ユーザが接続していないにもかかわらずセッションデータベースに表示されることがあるためです。グループ ポリシーの [Simultaneous Logins] 属性が 1 に設定されている場合は、すでに最大接続数に達していることがデータベースによって示されるため、ユーザーは再びログインできません。アイドル タイムアウトを短く設定すると、このようなファントムセッションを迅速に削除し、ユーザーが再ログインできるようにすることができます。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

要素	説明
Max Session Limit	許可される SSL または IKEv2 IPSec VPN セッションの最大数。次に示すように、ASA モデルによって、最大セッション数が異なるので注意してください。 • ASA 5505：25 • ASA 5510：250 • ASA 5520：750 • ASA 5540：2500 • ASA 5550、5585-X（SSP-10）：5000 • ASA 5580、5585-X（その他のモデル）：10,000 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
[証明書認証のタイムアウト（Certificate Authentication Timeout）] （ASA 8.4(5) または ASA 9.1(2)+）	証明書認証がタイムアウトするまでの待機時間（分単位）。有効な値は、1 ～ 120 分です。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
Allow Users to Select Connection Profile in Portal Page	ログイン時（たとえば、SSL VPN ポータルページ）にユーザが適切なプロファイルを選択するときに使用できる設定済み接続プロファイル（トンネル グループ）のリストを提供するかどうかを指定します。このオプションを選択しない場合、ユーザはプロファイルを選択できず、接続にはデフォルト プロファイルを使用する必要があります。 **ヒント** リモート アクセス IKEv2 IPSec VPN ではこのオプションを選択する必要があります。SSL VPN の場合、選択は任意です。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

要素	説明
Secure Client アクセスの有効化	ユーザが AnyConnect VPN クライアントを使用して SSL または IKEv2 IPSec VPN 接続を確立できるようにするかどうかを指定します。このオプションは、デフォルトでオンになっています。AnyConnect VPN クライアントの詳細については、SSL VPN セキュアクライアント の設定について （86 ページ）を参照してください。 ヒント　リモート アクセス IKEv2 IPSec VPN ではこのオプションを選択する必要があります。SSL VPN の場合、フル クライアント アクセスをイネーブルにする場合、このオプションを選択します。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
Secure Client Essentials の有効化	SSL および IKEv2 IPSec VPN の両方で使用できる、Secure Client Essentials 機能をイネーブルにするかどうかを指定します。AnyConnect Essentials VPN クライアントの詳細については、SSL VPN アクセス ポリシーについて （ASA） （61 ページ）を参照してください。

[Access Interface Configuration] ダイアログボックス

[Access Interface Configuration] ダイアログボックスを使用して、リモート アクセス SSL または IKEv2 IPSec VPN 接続の ASA デバイスでインターフェイスを設定します。

ナビゲーション パス

SSL VPN アクセスポリシー（[SSL VPN Access Policy] ページ （62 ページ）を参照）を開き、インターフェイステーブルの下にある [行の追加（Add Row）] をクリックするか、テーブルの行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- Access ポリシーの設定 （69 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 19 : [Access Interface Configuration] ダイアログボックス

要素	説明
Access Interface	SSL または IKEv2 IPSec VPN アクセスを設定するインターフェイスまたはインターフェイス ロール オブジェクト。インターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックしてリストから名前を選択するか、新しいインターフェイス ロール オブジェクトを作成します。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
Trustpoint Load Balancing Trustpoint	インターフェイスでのユーザの認証に使用するトラストポイント（認証局または CA サーバ）。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックして選択するか、新しいオブジェクトを作成します。 ロードバランシングが設定されている場合、ロードバランシング トラストポイントに個別の PKI 登録オブジェクトを選択することもできます。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
Allow Access	このインターフェイス経由の VPN アクセスをイネーブルにする場合は、このオプションを選択します。このオプションを選択しない場合、インターフェイスでアクセスは設定されますが、ディセーブルになります。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
Enable DTLS	選択すると、インターフェイスで Datagram Transport Layer Security（DTLS）がイネーブルになり、AnyConnect VPN Client は 2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用して SSL VPN 接続を確立できます。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

[サーバー名表示（Server Name Indication）] ダイアログボックス

バージョン 4.8 以降、Cisco Security Manager では、有効な VPN インターフェイスによって認証に使用される [サーバー名表示（Server Name Indication）] マッピングを設定できます。この機能には、トラストポイントへのドメイン名のマッピングが含まれます。

[サーバー名表示（Server Name Indication）] ダイアログボックスを使用して、各インターフェイスのドメインやトラストポイントを定義または変更します。

注：

- トラストポイントには一意のドメイン名を設定できます。トラストポイントは複数のドメイン名にマッピングできます。最大で 16 個の一意のトラストポイントを設定できます。
- トラストポイントへのドメイン名の [サーバー名表示（Server Name Indication）] マッピングは、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でサポートされています。

ナビゲーション パス

SSL VPN アクセスポリシー（ [SSL VPN Access Policy] ページ （62 ページ）を参照）を開き、ServerNameIndication テーブルの下にある [行の追加（Add Row）] をクリックするか、テーブルの行を選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 *20 : [サーバー名表示（Server Name Indication）] ダイアログボックス*

要素	説明
ドメインマスク	トラストポイントを設定するドメイン名を入力します。このドメインは、特定のインターフェイスには関連付けられません。ドメインが関連付けられている証明書は、任意のインターフェースで使用できます。
Trustpoint	インターフェイスでのユーザの認証に使用するトラストポイント（認証局または CA サーバ）。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックして選択するか、新しいオブジェクトを作成します。

Access ポリシーの設定

ここでは、ASA デバイスに Access ポリシーを設定する方法について説明します。アクセス ポリシーは、リモートアクセス SSL および IKEv2 IPSec VPN 接続に必要です。アクセス ポリシーの詳細については、 SSL VPN アクセス ポリシーについて（ASA） （61 ページ）を参照してください。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] > [アクセス（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、[リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] > [アクセス（ASA）（Access (ASA)）] を選択します。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。

[Access] ページが開きます。このページの要素の詳細については、[SSL VPN Access Policy] ページ （62 ページ）を参照してください。

ステップ 2 ポリシー上部のインターフェイス テーブルで、リモート アクセス SSL または IKEv2 IPSec VPN 接続を許可するすべてのインターフェイスを設定します。

- インターフェイスを追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックして、[アクセスインターフェイス設定の追加（Add Access Interface Configuration）] ダイアログボックスに入力します。インターフェイス名（または目的のインターフェイスを識別するインターフェイス ロール オブジェクト）、およびインターフェイスでアクセスを許可するかどうかを指定する必要があります。

インターフェイスの Certificate Authority（CA; 認証局）サーバ トラストポイント（およびロード バランシングを使用する場合はロード バランシング トラストポイント）を識別する PKI 登録オブジェクト、DTLS 接続をイネーブルにするかどうか、およびクライアントが接続を確立するために有効な証明書が必要かどうかを指定できます。オプションの詳細については、[Access Interface Configuration] ダイアログボックス（67 ページ）を参照してください。

- インターフェイスの設定を編集するには、そのインターフェイスを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- インターフェイスを削除するには、インターフェイスを選択し、[行を削除（Delete Row）] ボタンをクリックします。インターフェイス設定を編集してアクセスをディセーブルにできます。そのため、インターフェイスを削除する場合、VPN から完全に削除する場合だけにしてください。

ステップ 3 残りの設定を行います。設定については、[SSL VPN Access Policy] ページ （62 ページ）で詳しく説明されています。特に重要な設定を次に示します。

- [フォールバック トラストポイント（Fallback Trustpoint）]：インターフェイスにテーブルで設定されているトラストポイントがない場合に使用する Certificate Authority（CA; 認証局）サーバー トラストポイント。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックして選択するか、新しいオブジェクトを作成します。
- [ユーザにポータルページでの接続プロファイルの選択を許可する（Allow Users to Select Connection Profile in Portal Page）]：複数のトンネルグループがある場合、このオプションを選択すると、ユーザは、ログイン時に正しいトンネルグループを選択できます。このオプションは、IKEv2 IPSec VPN で選択する必要があります。
- **[Secure Clientアクセスの有効化（Enable Secure Client Access）]**：AnyConnect VPN クライアントは、フルクライアントです。VPN へのフルクライアントアクセスを許可する場合は、Secure Client アクセスをイネーブルにする必要があります。このオプションは、IKEv2 IPSec VPN で選択する必要があります。

Secure Client など、Secure Client の詳細については、SSL VPN セキュアクライアント の設定について （86 ページ）を参照してください。

- [Secure Client Essentialsの有効化（Enable Secure Client Essentials）]：Secure Client Essentials を使用する場合、このオプションを選択します。これは、リモートアクセス SSL または IKEv2 IPSec VPN で使用できます。

ステップ 4 このポリシーで指定するトラストポイントは、[公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーでも選択されている必要があります。詳細については、リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定を参照してください。

他の SSL VPN 設定の定義（ASA）

ASA デバイスの SSL VPN のその他の設定ポリシーは、キャッシング、コンテンツの書き換え、文字エンコード、プロキシおよびプロキシバイパス定義、ブラウザプラグイン、セキュアクライアント イメージおよびプロファイル、Kerberos Constrained Delegation、その他の一部の高度な設定を含む設定を定義します。

その他の設定ポリシーを設定するには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] 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、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）] を選択します。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。

次のタブで設定を定義できます。

- [Performance] タブ：SSL VPN パフォーマンスを向上するようにキャッシングを設定します。 SSL VPN パフォーマンス設定の定義（ASA） （73 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Content Rewrite] タブ：ユーザがセキュリティ アプライアンス自体を介することなく特定のサイトおよびアプリケーションを参照できるように許可するルールを作成します。SSL VPN コンテンツ書き換えルールの定義（ASA） （74 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Encoding] タブ：CIFS サーバから配信される Web ページのデフォルト以外のエンコーディングを設定します。エンコーディングは、通常、リモートユーザーのブラウザにより判別されます。 SSL VPN エンコーディング ルールの設定（ASA） （77 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Proxy] タブ：HTTP または HTTPS プロキシ サーバ（ネットワークで必要な場合）、およびプロキシ バイパス ルールを定義します。SSL VPN プロキシおよびプロキシ バイパスの設定（ASA） （79 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Plug In] タブ：Web ブラウザが専用の機能を実行するために起動する、個々のプログラムである、ブラウザプラグインを定義します。SSL VPN ブラウザ プラグインの設定（ASA）

（83 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

- [クライアント設定（Client Settings）] タブ：クライアントへのダウンロードのために セキュアクライアントイメージおよびプロファイルを設定します。次のトピックを参照してください。
  - SSL VPN セキュアクライアント の設定について （86 ページ）
  - SSL VPN セキュアクライアント 設定の構成（ASA） （89 ページ）

この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN で部分的にサポートされています。ASA 9.5(2) マルチコンテキストモードでは、Secure Client イメージ クライアントイメージのみがサポートされます。バージョン 4.12 以降、Security Manager は、管理コンテキストおよびユーザーコンテキストのマルチコンテキスト ASA 9.6(2) 以降のデバイスをサポートしています。サポートされている CLI は次のとおりです。

- Secure Client イメージ
- Secure Client プロファイル

検出中、ASA 9.5(2) リモートアクセス VPN マルチコンテキストモードの Secure Client イメージ イメージは検出されません。検出後に Secure Client イメージ 設定を削除する場合は、FlexConfig を使用する必要があります。

- [Microsoft KCD Server]：クライアントレス SSL VPN 接続で使用する Kerberos Constrained Delegation（KCD）を設定します。次のトピックを参照してください。
  - SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA） （93 ページ）
  - SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA） （96 ページ）

この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

- [Secure Clientカスタム属性（Secure Client Custom Attributes）] タブ：Secure Client カスタム属性を設定します。 Secure Client カスタム属性（ASA）の設定 （98 ページ）を参照してください。[Secure Clientカスタム属性（Secure Client Custom Attributes）] タブは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Advanced] タブ：メモリ、オンスクリーン キーボードおよび内部パスワード機能を設定します。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

（注） 4.15 以降、Cisco Security Manager は HTTP Strict Transport Security（HSTS）をサポートしています。HSTS は、プロトコルダウングレード攻撃および Cookie のハイジャックから Web サイトを保護するのに役立つ Web セキュリティ ポリシー メカニズムです。

[詳細（Advanced）] タブで、HSTS を有効または無効にしたり、タイムアウト値を指定したりすることができます。 SSL VPN の高度な設定の定義（ASA） （100 ページ）を参照してください。

- [SSLサーバー検証（SSL Server Verification）] タブ：クライアントレス SSL VPN ユーザーの HTTPS サーバー検証を有効にします。 SSL VPN サーバー検証の設定（ASA） （102 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ヒント デバイスで Connection Profile ポリシーを設定する必要があります。 接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ） を参照してください。

SSL VPN パフォーマンス設定の定義（ASA）

キャッシングによって SSL VPN パフォーマンスが向上します。頻繁に再利用されるオブジェクトをシステムキャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。SSL VPN と、リモート サーバとエンドユーザ ブラウザの両方との間のトラフィックが削減され、その結果、多数のアプリケーションがより効率的に実行されます。

ここでは、ASA セキュリティ アプライアンスでキャッシングをイネーブルにする方法について説明します。

関連項目

- 他の SSL VPN 設定の定義（ASA） （71 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASAデバイスを選択して、ポリシーセレクタから**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。まだ選択されていない場合、[パフォーマンス（Performance）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。まだ選択されていない場合、[パフォーマンス（Performance）] タブをクリックします。

ステップ 2 [有効（Enable）] を選択して、セキュリティアプライアンスでのキャッシングをイネーブルにします。

このオプションを選択しない場合、セキュリティ アプライアンスで定義されているキャッシュ設定は有効になりません。

ステップ 3 次のオプションを設定します。

- [最小オブジェクトサイズ（Minimum Object Size）]：セキュリティアプライアンスでキャッシュに格納可能な HTTP オブジェクトの最小サイズ（KB 単位）。有効な範囲は 0 ～ 10,000 KB です。デフォルトは 0 KB です。

- [最大オブジェクトサイズ（Maximum Object Size）]：セキュリティアプライアンスでキャッシュに格納可能な HTTP オブジェクトの最大サイズ（KB 単位）。有効な範囲は 0 ～ 10,000 KB です。デフォルトは 1000 KB です。最大サイズは、最小サイズよりも大きくする必要があります。
- [最終変更係数（Last Modified Factor）]：最後に更新されたタイムスタンプだけを持ち、サーバーにより設定されたその他の有効期限値を持たないキャッシングオブジェクトの再検証ポリシーを設定する整数を指定します有効な範囲は 1 ～ 100 です。デフォルトは 20 です。

また、発信 Web サーバからセキュリティアプライアンス要求に対して、応答が期限切れになる時間を示す Expires応答が送信されますが、この応答もキャッシングに影響を及ぼします。この応答ヘッダーは、応答が古くなり（条件付き GET 操作を使用して）最新のチェックなしでクライアントに送信できなくなる時刻を示します。

また、セキュリティアプライアンスでは、Web オブジェクトごとに、オブジェクトがディスクに書き込まれる前にオブジェクトの有効期限を計算できます。オブジェクトのキャッシュ有効期限データを計算するためのアルゴリズムは、次のとおりです。

有効期限 = (今日の日付 - オブジェクトの最終変更日付) X 有効期間係数

有効期限が経過するとオブジェクトが古いと見なされ、それ以降の要求に対しては、セキュリティアプライアンスによってコンテンツが新しく取得されます。最終変更係数を 0 に設定することは、即時の再検証を強制することに相当します。100 に設定すると、再検証までの時間が許容される範囲で最も長くなります。

- [有効期間（Expiration Time）]：セキュリティアプライアンスがオブジェクトを再検証せずにキャッシュに格納する時間（分単位）。範囲は 0 ～ 900 分です。デフォルトは 1 分です。

再検証では、キャッシュされたオブジェクトの経過時間が有効期間を超過している場合、要求されたコンテンツをクライアントブラウザに提供する前に、発信サーバからそのオブジェクトを拒否します。キャッシュされたオブジェクトの経過時間とは、セキュリティアプライアンスが発信サーバーに明示的に接続してオブジェクトがまだ有効期間内であるかどうかをチェックすることなく、オブジェクトがセキュリティアプライアンスのキャッシュに格納されている時間のことです。

- [スタティックコンテンツのキャッシュ（Cache Static Content）]：セキュリティアプライアンスでスタティックコンテンツをキャッシュできるかどうかを指定します。各 Web ページは、スタティック オブジェクトとダイナミック オブジェクトで構成されます。セキュリティアプライアンスでは、イメージファイル（*.gif、*.jpeg）、Java アプレット（.js）、カスケーディング スタイル シート（*.css）の個々のスタティック オブジェクトをキャッシュします。

SSL VPN コンテンツ書き換えルールの定義（ASA）

SSL VPN は、高度な要素（JavaScript、VBScript、Java、およびマルチバイト文字など）に対応したコンテンツ変換/書き込みエンジンを介してアプリケーショントラフィックを処理し、ユーザが SSL VPN デバイス内でアプリケーションを使用しているか、デバイスとは無関係に使用しているかに応じて、HTTP トラフィックをプロキシします。

一部のアプリケーションおよび Web リソース（パブリック Web サイトなど）がセキュリティアプライアンスを通過しないようにする場合は、セキュリティアプライアンス自体を経由せずに、ユーザが特定のサイトおよびアプリケーションをブラウズできるようにする書き換え規則を作成できます。これは、IPSec VPN 接続におけるスプリット トンネリングによく似ています。

[SSL VPN Other Settings] ページの [Content Rewrite] タブでは、複数のコンテンツ書き換え規則を作成できます。[Content Rewrite] タブには、コンテンツ書き換えがイネーブルまたはディセーブルな、すべてのアプリケーションが一覧表示されます。

ヒント セキュリティアプライアンスは、最も小さい番号から順番に書き換えルールを検索して、一致した最初のルールを適用します。

ここでは、コンテンツ書き換えルールを作成または編集する方法を示します。

関連項目

- 他の SSL VPN 設定の定義（ASA） （71 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** 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、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。

ステップ 2 [その他の設定（Other Settings）] ページで [コンテンツ書き換え（Content Rewrite）] タブをクリックします。[Content Rewrite] タブには、コンテンツ書き換えがイネーブルまたはディセーブルな、すべてのアプリケーションが表示されます。

セキュリティアプライアンスは、最も小さい番号から順番に書き換えルールを検索して、一致した最初のルールを適用します。リソースマスクは、ルールと照合するアプリケーション ストリングを定義します。

番号がないルールは、番号付きのすべてのルールのあとに評価されます。

ステップ 3 次のいずれかを実行します。

- ルールを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、[コンテンツ書き換えの追加（Add Content Rewrite）] ダイアログボックスに入力します。これらのオプションについては、[Add Content Rewrite]/[Edit Content Rewrite] ダイアログボックス （76 ページ）で詳しく説明されています。
- ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックして、[コンテンツ書き換えの編集（Edit Content Rewrite）] ダイアログボックスで変更を加えます。

- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）]ボタンをクリックします。削除の確認が求められます。

（注） Cisco Security Manager 4.24 以降、[コンテンツ書き換え（Content Rewrite）] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

[Add Content Rewrite]/[Edit Content Rewrite] ダイアログボックス

[Add or Edit Content Rewrite] ダイアログボックスを使用して、SSL VPN 接続を介するプロキシ HTTP トラフィックに対して拡張要素（JavaScript、VBScript、Java、マルチバイト文字など）を含む書き換えエンジンを設定します。コンテンツ書き換えルールの詳細については、SSL VPN コンテンツ書き換えルールの定義（ASA） （74 ページ）を参照してください。

ナビゲーション パス

ASA デバイスの SSL VPN のその他の設定ポリシーの [コンテンツのリライト（Content Rewrite）] タブから、[行の追加（Add Row）]ボタンをクリックするか、ルールを選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、SSL VPN コンテンツ書き換えルールの定義（ASA） （74 ページ）を参照してください。

関連項目

- 他の SSL VPN 設定の定義（ASA） （71 ページ）

フィールド リファレンス

表 *21 : [Add or Edit Content Rewrite]* ダイアログボックス

要素	説明
有効化（Enable）	選択すると、セキュリティアプライアンスで、書き換えルールに対するコンテンツ書き換えがイネーブルになります。 外部のパブリック Web サイトなどの一部のアプリケーションでは、この処理が必要ないものもあります。これらのアプリケーションでは、コンテンツ リライトをオフにできます。
ルール番号	このルールの番号。この番号は、リスト内のルールの位置を指定します。番号がないルールはリストの最後に配置されます。範囲は 1 ～ 65534 です。 ルールは、低い番号から高い番号の順に処理され、最初に一致したルールがトラフィックに適用されます。
ルール名	コンテンツ書き換えルールを説明する英数字文字列。最大長は 128 文字です。

要素	説明
リソース マスク	ルールが適用されるアプリケーションまたはリソースの名前。最大長は300文字です。 次のワイルドカードを使用できます。 • *：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 • ?：単一文字と一致します。 • [!x-y]：シーケンスにない任意の文字と一致します。 • [x-y]：シーケンス内の任意の文字と一致します。

SSL VPN エンコーディング ルールの設定（ASA）

[SSL VPN Other Settings] ページの [Encoding] タブを使用して、リモート ユーザに配信される SSL VPN ポータル ページでエンコードする文字セットを指定します。デフォルトでは、SSL VPN ポータル ページの文字セットはリモート ブラウザで設定されているエンコーディング タイプ セットによって決定されるため、ブラウザで適切なエンコーディングが行われることを確認する必要がある場合を除き、文字エンコーディングを設定する必要はありません。

文字エンコーディングは、データを表すために（0 や 1 などの）raw データと文字を組み合わせたものです。使用する文字エンコード方式は、言語によって決まります。ある言語では同じ方式を使用していても、別の言語でも同じとはかぎりません。通常、ブラウザで使用されるデフォルトのエンコード方式は地理上の地域によって決まりますが、リモートユーザはこれを変更できます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。

エンコード属性を使用すると、SSL VPN ポータル ページに文字エンコード方式の値を指定し、ユーザがブラウザを使用している地域、またはブラウザに対して行われた変更に関係なく、ブラウザにページが正しく表示されることを保証できます。

文字エンコード属性は、デフォルトですべての SSL VPN ポータル ページが継承するグローバル設定です。ただし、文字エンコード属性の値と異なる文字エンコードを使用する Common Internet File System（CIFS）サーバのファイル エンコード属性を上書きできます。異なる文字エンコードが必要な CIFS サーバには、異なるファイル エンコード値を使用できます。

CIFS サーバから SSL VPN ユーザにダウンロードされた SSL VPN ポータル ページのエンコードは、サーバ指定の SSL VPN ファイル エンコード属性の値となります。サーバで指定されていない場合、ポータル ページは文字エンコード属性の値を継承します。リモートユーザーのブラウザでは、ブラウザの文字エンコードセットのエントリにこの値がマップされ、使用する適切な文字セットが決定されます。SSL VPN 設定に CIFS サーバのファイル エンコード エントリを指定せず、文字エンコード属性も設定されていない場合は、SSL VPN ポータル ページに値が指定されません。SSL VPN ポータル ページで文字エンコードを指定しなかった場合、またはブラウザがサポートしていない文字エンコード値を指定した場合、リモート ブラウザでは独自のデフォルト エンコードが使用されます。

[SSL VPN Global Settings] ページの [Encoding] タブでは、ポータル ページでエンコードされる、CIFS サーバに関連付けられた現在設定済みの文字セットを表示できます。このタブから、文字セットを作成または編集できます（次の手順を参照）。

関連項目

- 他の SSL VPN 設定の定義（ASA）　（71 ページ）

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** 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、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。

ステップ 2　[その他の設定（Other Settings）] ページで [エンコーディング（Encoding）] タブをクリックします。[Encoding] タブには、デフォルトのエンコーディング、およびエンコーディング ルールが設定される CIFS サーバのリストが表示されます。

ステップ 3　[グローバルSSL VPNエンコーディングタイプ（Global SSL VPN Encoding Type）] リストから、テーブルに表示された CIFS サーバからの属性を除き、すべての SSL VPN ポータルページが継承する文字エンコードを決定する属性を選択します。

（注）　[なし（None）] を選択するか、SSL VPN クライアントのブラウザでサポートされていない値を指定した場合は、デフォルトのエンコーディングが使用されます。デフォルトのグローバル エンコーディングは [None] です。

次のエンコーディング タイプから選択できます。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

（注）　日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [ページ フォントの選択（Select Page Font）] ペインの [フォントファミリ（Font Family）] エリアにある [指定しない（Do Not specify）] をクリックして、このフォントファミリを削除します。

- unicode
- windows-1252
- none

ステップ 4　次のいずれかを実行します。

- ルールを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、[ファイルエンコーディングの追加（Add File Encoding）] ダイアログボックスで次の設定を行います。
  - [CIFSサーバーIP、CIFSサーバーホスト（CIFS Server IP, CIFS Server Host）]：これらのオプションのいずれかを選択して、IPアドレスまたはホスト名のいずれかによりCIFSサーバを指定します。IP アドレスを選択する場合、IP アドレスまたは 1 つ以上の個々の IP アドレスを指定するネットワーク/ホスト オブジェクトの名前のいずれかを入力できます。

ホスト名を指定する場合、セキュリティ アプライアンスでは指定した大文字と小文字が保持されますが、名前をサーバと照合するときは大文字と小文字の違いが無視されます。

- [エンコーディングタイプ（Encoding Type）]：エンコーディングタイプを選択します。オプションは、前述のグローバル設定と同じです。

- ルールを編集するには、そのルールを選択し、[行の編集（Edit Row）] ボタンをクリックして、[ファイルエンコーディングの編集（Edit File Encoding）] ダイアログボックスで変更を加えます。

- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）]ボタンをクリックします。削除の確認が求められます。

SSL VPN プロキシおよびプロキシ バイパスの設定（ASA）

[SSL VPN Other Settings] ページの [Proxy] タブを使用して、HTTPS 接続を終了して HTTP/HTTPS 要求を HTTP および HTTPS プロキシ サーバに転送するようにセキュリティ アプライアンスを設定します。このタブでは、最小コンテンツ書き換えを実行するようにセキュリティアプライアンスを設定したり、書き換えるコンテンツのタイプ（外部リンクまたは XML、あるいはどちらでもない）を指定したりすることもできます。

セキュリティ アプライアンスは、HTTPS 接続を終了し、HTTP および HTTPS プロキシ サーバに HTTP/HTTPS 要求を転送できます。これらのサーバは、ユーザとインターネット間を中継する機能を果たします。すべてのインターネット アクセスがユーザ制御のサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネット アクセスと管理制御が保証されます。

（注） HTTP/HTTPS プロキシは、Personal Digital Assistant への接続をサポートしていません。

HTTP プロキシ サーバからダウンロードする Proxy Auto-Configuration（PAC）ファイルを指定できます。ただし、PAC ファイルを指定する場合は、プロキシ認証を使用できません。

ユーザは、プロキシバイパスを使用するようにセキュリティアプライアンスを設定できます。これは、この機能が提供するコンテンツ リライトを使用した方が、アプリケーションや Web リソースをより有効活用できる場合に設定します。プロキシバイパスはコンテンツの書き換えに代わる手法であり、元のコンテンツの変更を最小限に抑えます。カスタム Web アプリケーションで役立ちます。

プロキシバイパスには複数のエントリを設定できます。エントリを設定する順序は重要ではありません。インターフェイスとパスマスク、またはインターフェイスとポートにより、プロキシ バイパス ルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシ バイパスを設定した場合、ネットワーク設定によっては、これらのポートからセキュリティアプライアンスにアクセスできるようにファイアウォール設定を変更することが必要になる場合があります。この制限を回避するには、パスマスクを使用します。ただし、このパス マスクは変更される場合があるため、複数のパス マスク ステートメントを使用して、この可能性を排除する必要がある可能性があることに注意してください。

ここでは、SSL VPN のプロキシおよびプロキシ バイパス ルールを定義する方法を示します。

関連項目

- 他の SSL VPN 設定の定義（ASA） （71 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** 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、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。

ステップ 2 [その他の設定（Other Settings）] ページで [プロキシ（Proxy）] タブをクリックします。[Proxy] タブには、現在定義されているプロキシおよびプロキシ ルールが表示されます。

ステップ 3 [プロキシタイプ（Proxy Type）] フィールドから、SSL VPN 接続に使用する外部プロキシサーバーのタイプを選択します。

- [HTTP/HTTPSプロキシサーバー（HTTP/HTTPS Proxy Server）]：プロキシサーバーを指定して、HTTP または HTTPS 要求を処理します。
- [PACを使用したプロキシ（Proxy Using PAC）]：プロキシ自動構成（PAC）ファイルを指定して、HTTP プロキシサーバーからユーザーのブラウザにダウンロードします。ダウンロードが完了すると、PAC ファイルは JavaScript 機能を使用して各 URL のプロキシを識別します。

このオプションを選択する場合、PAC ファイルの URL を [プロキシ自動構成ファイルのURLを指定（Specify Proxy Auto Config file URL）] フィールドに入力します。URL は、**http://** から開始する必要があります。開始しない場合、セキュリティアプライアンスは PAC ファイルを使用しません。

ステップ 4 プロキシ タイプで [HTTP/HTTPS Proxy Server] を選択した場合、HTTP および HTTPS プロキシ サーバの設定を行います。HTTP および HTTPS サーバは個別に設定できるため、異なるサーバを使用したり、いずれか 1 つのタイプだけを指定したりできます。次のオプションを設定します。

- [HTTPプロキシサーバーの有効化（Enable HTTP Proxy Server）]、[HTTPSプロキシサーバーの有効化（Enable HTTPS Proxy Server）]：これらのオプションのいずれかまたは両方を選択して、プロキシサーバーを設定します。

- [HTTPプロキシサーバー（HTTP Proxy Server）]、[HTTPSプロキシサーバー（HTTPS Proxy Server）]：IP アドレス、または単一 プロキシサーバーの IP アドレスを含むネットワーク/ホストオブジェクトの名前を、設定するプロキシサーバーのタイプごとに入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。

HTTP のデフォルト ポートは 80、HTTPS のデフォルト ポートは 443 です。

バージョン 4.12 以降、Security Manager は ASA 9.0(1) 以降のデバイスの IPv6 アドレスをサポートします。入力した IPv6 アドレスが無効な場合、Security Manager にはエラーが表示されます。リストからプロキシサーバーを選択したときにオブジェクトが使用できない場合、Security Manager は警告メッセージを表示します。

- [HTTPプロキシポート（HTTP Proxy Port）]、[HTTPSプロキシポート（HTTPS Proxy Port）]：HTTP または HTTPS 要求が転送されるプロキシサーバーのポートを入力します。また、ポートを定義するポートリストオブジェクトの名前を入力できます。または、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成することもできます。
- [除外アドレス一覧（Exception Address List）]：HTTP または HTTPS プロキシサーバーに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリスト。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。
  - ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字文字列とともに使用する必要があります。
  - **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
  - [x-y] は、x から y までの範囲の任意の 1 文字と一致します。x は ANSI 文字セット内のある 1 文字を表し、y は別の 1 文字を表します。
  - [!x-y] は、範囲外の任意の 1 文字と一致します。
- [認証ユーザー名（Authentication User Name）]、[認証パスワード（Authentication Password）]、[確認（Confirm）]：プロキシサーバーでユーザー認証が必要な場合は、有効なユーザー名およびパスワードを入力します。

ステップ 5 必要に応じて、タブの一番下にある [Proxy Bypass] テーブルでプロキシ バイパス ルールを設定します。プロキシ バイパスは、プロキシ バイパスに設定されている ASA インターフェイス、ポートおよびターゲット URL を指定します。次のいずれかを実行します。

- プロキシバイパスルールを追加するには、[行の追加（Add Row）] ボタンをクリックして、[プロキシバイパスの追加（Add Proxy Bypass）] ダイアログボックスに入力します。プロキシ バイパス ルールの属性の詳細については、[Add or Edit Proxy Bypass Dialog Box] ダイアログボックス （82 ページ）を参照してください。
- プロキシバイパスルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

ヒント　プロキシ バイパス ルールを設定する場合、SSL VPN Access ポリシーも設定する必要があります。詳細については、Access ポリシーの設定　（69 ページ）を参照してください。

[Add or Edit Proxy Bypass Dialog Box] ダイアログボックス

[Add or Edit Proxy Bypass] ダイアログボックスを使用して、セキュリティ アプライアンスがコンテンツ書き換えをほとんど、またはまったく実行しない場合のプロキシ バイパス ルールを設定します。

ナビゲーション パス

ASA デバイスの SSL VPN のその他の設定ポリシーの [プロキシ（Proxy）] タブから、[行の追加（Add Row）] ボタンをクリックするか、ルールを選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、SSL VPN エンコーディング ルールの設定（ASA）　（77 ページ）を参照してください。

フィールド リファレンス

表 22 : [Add or Edit Proxy Bypass Dialog Box] ダイアログボックス

要素	説明
インターフェイス（Interface）	セキュリティ アプライアンスでプロキシ バイパスに使用されるインターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストからオブジェクトを選択するか新しいオブジェクトを作成します。
Bypass On Port	プロキシ バイパスのポート番号を使用する場合、このオプションを選択します。有効なポート番号は、20000 ～ 21000 です。ポートリスト オブジェクトのポートまたは名前を入力します。または、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。 （注）　パス マスクではなくポートを使用してプロキシ バイパスを設定した場合、ネットワーク設定によっては、これらのポートからセキュリティ アプライアンスにアクセスできるようにファイアウォール設定を変更することが必要になる場合があります。この制限を回避するには、パス マスクを使用します。

要素	説明
Bypass Matching Specific Pattern	プロキシバイパスの照合にURLパスマスクを使用する場合、このオプションを選択します。パスは、URL 内のドメイン名に続くテキストです。たとえば、www.mycompany.com/hrbenefits という URL では、*hrbenefits* がパスになります。 次のワイルドカードを使用できます。 • *****：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 • **?**：単一文字と一致します。 • **[x-y]**：シーケンス内の任意の文字と一致します。 • **[!x-y]**：シーケンスにない任意の文字と一致します。 最大値は 128 バイトです。 （注） パス マスクが変更される可能性をなくすために、複数のパス マスク ステートメントを使用することが必要になる場合があります。
URL	[http] または [https] プロトコルを選択し、プロキシバイパスを適用する URL を入力します。 プロキシバイパスに使用する URL では、最大 128 バイトが許可されます。別のポートを指定しない限り、HTTP のポートは 80、HTTPS のポートは 443 です。
Rewrite XML	セキュリティ アプライアンスによってバイパスされるように、XML サイトおよびアプリケーションが書き換えられるかどうかを指定します。
Rewrite Hostname	セキュリティ アプライアンスによってバイパスされるように、外部リンクが書き換えられるかどうかを指定します。

SSL VPN ブラウザ プラグインの設定（ASA）

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。セキュリティ アプライアンスを使用すると、クライアントレス SSL VPN セッション中に、リモート ブラウザにダウンロードするプラグインをインポートできます。

シスコでは、Java ベースのオープン ソース コンポーネントを再配布しています。これは、クライアントレス SSL VPN セッションで Web ブラウザのプラグインとしてアクセスされるコンポーネントで、次のものがあります。シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。プラグインファイルは、Cisco Security Manager サーバーの製品インストールフォルダ（通常は C:\Program

Files\CSCOpx）内の \files\vms\repository フォルダにあります。実際のファイル名には、リリース番号が含まれています。

- rdp-plugin.jar：Remote Desktop Protocol プラグインにより、リモート ユーザは Microsoft Terminal Services が実行されているコンピュータに接続できます。再配布されるプラグインのソースがある Web サイトは http://properjavardp.sourceforge.net/ です。
- ssh-plugin.jar：Secure Shell-Telnet プラグインにより、リモート ユーザはリモート コンピュータとセキュア シェル接続または Telnet 接続を確立できます。この再配布プラグインのソースがある Web サイトは、http://javassh.org/ です。

（注） ssh-plugin.jar は、SSH プロトコルおよび Telnet プロトコルの両方をサポートします。SSH クライアントは SSH バージョン 1.0 をサポートします。

- vnc-plugin.jar：Virtual Network Computing プラグインにより、リモート ユーザはモニタ、キーボード、およびマウスを使用して、リモート デスクトップ共有がオンになっているコンピュータを表示および制御できます。この再配布プラグインのソースがある Web サイトは、http://www.tightvnc.com です。

（注） シスコでは、GNU 一般公的使用許諾（GPL）に従い、変更を加えることなくプラグインを再配布しています。GPL により、これらのプラグインを直接改良できません。

フラッシュ デバイスにプラグインをインストールすると、セキュリティ アプライアンスにより次のことが実行されます。

- （Cisco 配布のプラグイン限定）URL で指定された jar ファイルのアンパック
- セキュリティ アプライアンス ファイル システム上の csco-config/97/plugin ディレクトリへのファイルの書き込み
- 将来のすべてのクライアントレス SSL VPN セッションに対するプラグインのイネーブル化、およびメイン メニュー オプションの追加とポータル ページの [Address] フィールドの隣にあるドロップダウン メニューへのオプションの追加

クライアントレス SSL VPN セッションのユーザがポータル ページで関連するメニュー オプションをクリックすると、ポータル ページにインターフェイスへのウィンドウが開き、ヘルプ ペインが表示されます。ドロップダウン メニューに表示されたプロトコルをユーザーが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

（注） Java プラグインの中には、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインのステータスをレポートするプラグインもあります。オープン ソースのプラグインはステータスをレポートしますが、セキュリティ アプライアンスはステータスをレポートしません。

[SSL VPN Global Settings] ページの [Plug-in] タブで、クライアントレス SSL VPN ブラウザ アクセスに現在設定されているブラウザ プラグインを表示できます。このタブから、プラグイン ファイルを作成または編集できます（次の手順を参照）。

プラグインの要件および制約事項

プラグインへのリモート アクセスを提供するには、セキュリティ アプライアンスでクライアントレス SSL VPN がイネーブルになっている必要があります。リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。リモート コンピュータ上に必要な Java のバージョンは、プラグインによって自動的にインストールまたは更新されます。ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザーはフェールオーバー後に再接続する必要があります。

プラグインをインストールする前に、セキュリティ アプライアンスで次の準備を行います。

- セキュリティ アプライアンスのインターフェイスでクライアントレス SSL VPN がイネーブルであることを確認します。
- リモート ユーザが Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用して接続するセキュリティ アプライアンス インターフェイスに、SSL 証明書をインストールします。

（注） SSL 証明書の一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、FQDN を使用してセキュリティ アプライアンスとの通信を試みます。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

関連項目

- SSL VPN サポート ファイルの概要と管理
- 他の SSL VPN 設定の定義（ASA） （71 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ASA デバイスを選択して、ポリシー セレクタから **[リモート アクセス VPN（Remote Access VPN）] > [SSL VPN（SSL VPN）] > [その他の設定（Other Settings）]** 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、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN（SSL VPN）] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。

ステップ 2 [その他の設定（Other Settings）] ページで [プラグイン（Plug-in）] タブをクリックします。[Plug-in] タブには、プラグインのタイプおよび実際のプラグイン ファイルを定義するファイル ポリシー オブジェクトの名前など、設定されているすべてのプラグインのリストが表示されます。

ステップ 3 次のいずれかを実行します。

- プラグインを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、次のように、[プラグインエントリの追加（Add Plug-In Entry）] ダイアログボックスに入力します。
  - [プラグイン（Plug-in）]：追加するプラグインのタイプを選択します。
  - [Remote Desktop (RDP) or RDP2]：Remote Desktop Protocol サービス。
  - [Secure Shell (SSH), Telnet]：Secure Shell および Telnet サービス。
  - [VNC]：Virtual Network Computing サービス。
  - [Citrix (ICA)]：Citrix MetaFrame サービス。
  - [Post]：ポスト サービス。
  - [プラグインファイル（Plug-in File）]：プラグインファイルを定義するファイルポリシー オブジェクトの名前。ファイルオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。ファイル オブジェクトの作成の詳細については、[Add File Object]/[Edit File Object] ダイアログボックスを参照してください。
- プラグインを編集するには、そのプラグインを選択し、[行の編集（Edit Row）] ボタンをクリックして、[プラグインエントリの編集（Edit Plug-In Entry）] ダイアログボックスで変更を加えます。
- プラグインを削除するには、そのプラグインを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

SSL VPN セキュアクライアント の設定について

Cisco AnyConnect VPN クライアントは、セキュリティ アプライアンスへのセキュアな SSL および IKEv2 IPsec 接続をリモート ユーザに提供します。このクライアントにより、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、リモート ユーザーは SSL または IKEv2 IPsec VPN クライアントを活用できます。

ヒント IKEv2 IPsec 接続では、AnyConnect 3.0 以降のクライアントが必要です。

事前にクライアントがインストールされていない場合、リモート ユーザーは、SSL または IKEv2 IPsec VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。セキュリティアプライアンスが http:// 要求を https:// にリダイレクトするように設定されている場合を除いて、ユーザは https://<*address*> 形式で URL を入力する必要があります。

URL を入力すると、ブラウザがそのインターフェイスに接続して、ログイン画面が表示されます。ユーザがログイン認証に成功し、セキュリティアプライアンスによってそのユーザがクライアントを要求していると識別されると、リモート コンピュータのオペレーティング システムに適合するクライアントがダウンロードされます。ダウンロード後、クライアントは自分自身でインストールと設定を行い、セキュアな接続を確立します。接続の終了時には、（セキュリティアプライアンスの設定に応じて）そのまま残るか、または自分自身をアンインストールします。

事前にクライアントがインストールされている場合、ユーザ認証時に、セキュリティアプライアンスはクライアントのリビジョンを検査し、必要な場合はクライアントをアップグレードします。

クライアントがセキュリティ アプライアンスとの接続をネゴシエートする場合は、Transport Layer Security（TLS）、および任意で Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

セキュアクライアントは、セキュリティアプライアンスからダウンロードできます。または、システム管理者が手動でリモートワークステーションにインストールできます。クライアントの手動インストールの詳細については、『*Cisco Secure Client Administrator Guide*』を参照してください。Secure Client マニュアルは、http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html [英語] で入手できます。Secure Client の一般情報については、http://www.cisco.com/go/secure-client [英語] を参照してください。

セキュリティ アプライアンスは、接続を確立しているユーザのグループ ポリシーまたはユーザ名属性に基づいてクライアントをダウンロードします。自動的にクライアントをダウンロードするようにセキュリティ アプライアンスを設定できます。または、クライアントをダウンロードするかどうかをリモートユーザに確認するように設定することもできます後者でユーザが応答しなかった場合に、タイムアウト時間の経過後にクライアントをダウンロードするか、またはログイン ページを表示するように、セキュリティ アプライアンスを設定できます。

セキュアクライアント プロファイル

Secure Client プロファイル は、XML ファイルに保存された一連の設定パラメータです。クライアントでは、クライアントユーザーインターフェイスに表示される接続エントリを設定するときにこれらのパラメータを使用します。これらのパラメータ（XML タグ）には、ホスト コンピュータの名前とアドレス、および追加のクライアント機能を有効にする設定が含まれています。

セキュアクライアント インストールには、*AnyConnectProfile.tmpl* という名前のプロファイルテンプレートが含まれています。このテンプレートはテキストエディタを使用して編集したり、

これを基にして他のプロファイルファイルを作成したりできます。ユーザインターフェイスからは使用できない高度なパラメータを設定することもできます。また、インストールには、*AnyConnectProfile.xsd* という名前の XML スキームファイル一式も含まれています。

その他の設定ポリシーの [Client Settings] タブにプロファイルを追加して、これをセキュリティアプライアンスにロードし、そのあとで、グループポリシーおよびユーザ名属性に基づいてクライアント ワークステーションにダウンロードできます。

関連項目

- SSL VPN サポート ファイルの概要と管理
- SSL VPN セキュアクライアント 設定の構成（ASA） （89 ページ）
- Cisco Secure Client プロファイルエディタ （88 ページ）

Cisco Secure Client プロファイルエディタ

プロファイルは、Secure Client プロファイルエディタ を使用して設定できます。このエディタは、Cisco Security Manager から起動する便利な GUI ベースの構成ツールです。Windows 用の Secure Client ソフトウェアパッケージ。バージョン 2.5 以降にはエディタが含まれていて、このエディタは、適切な Secure Client パッケージを Secure Client イメージリストに追加している場合に限り、セキュアクライアント プロファイルの追加/編集ダイアログボックスからエディタを起動するとアクティベートされます。

（注） Secure Client プロファイルエディタを使用して WSO ファイルを編集できないため、[Webセキュリティ WSO（Web Security WSO）] タイプが選択されると、**[Secure Clientプロファイルの追加（Add Secure Client Profile）]** の下の [エディタの起動（Launch Editor）] オプションが自動的に無効になります。

（注） Cisco Secure Client プロファイルエディタ は独立したプログラムです。Secure Clientプロファイルの設定、および Secure Client プロファイルエディタ プロファイルエディタでできることについては、http://www.cisco.com/en/US/products/ps10884/products_installation_and_configuration_guides_list.html [英語] でオンラインで入手可能な資料を参照してください。

ナビゲーション パス

[Secure Clientプロファイルの追加/編集（Add/Edit セキュアクライアント Profile）] ダイアログボックスを開き、[エディタの起動（Launch Editor）] をクリックします（[Secure Clientプロファイルの追加/編集（Add/Edit セキュアクライアント Profile）] ダイアログボックスにアクセスする前に、まず適切な Secure Client パッケージを Secure Client イメージリストに追加する必要があります）。Secure Client プロファイルエディタが表示されます。

関連項目

- SSL VPN セキュアクライアント の設定について （86 ページ）
- SSL VPN セキュアクライアント 設定の構成（ASA） （89 ページ）
- SSL VPN サポート ファイルの概要と管理

（注） バージョン 4.7 以降、Security Manager は AnyConnect バージョン 3.2 のサポートを提供します。

SSL VPN セキュアクライアント 設定の構成（ASA）

ここでは、SSL および IKEv2 IPsec VPN クライアント イメージおよびプロファイルを定義する方法を示します。Secure Client イメージおよびプロファイルの詳細については、SSL VPN セキュアクライアント の設定について （86 ページ）を参照してください。

ヒント 必要なリリースの Secure Client イメージを追加していることを確認してください。たとえば、IKEv2 IPsec VPN を設定する場合は、AnyConnect 3.0 以降のイメージを含める必要があります。通常、イメージ バージョンは、リモート アクセス VPN で展開する機能をサポートする必要があります。

関連項目

- SSL VPN セキュアクライアント の設定について （86 ページ）
- Cisco Secure Client プロファイルエディタ （88 ページ）
- SSL VPN サポート ファイルの概要と管理
- 他の SSL VPN 設定の定義（ASA） （71 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** 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、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。

ステップ 2 [その他の設定（Other Settings）] ページで [クライアント設定（Client Settings）] タブをクリックします。このタブには、設定されている セキュアクライアント およびプロファイルのリストを個別に表示する 2 つのテーブルがあります。

Secure Client イメージには、順番を示す番号が含まれます。セキュリティアプライアンスは、最も大きい順番から始めて、オペレーティングシステムと一致するまで、Secure Client イメージの一部をリモートコン

ピュータにダウンロードします。そのため、最も一般的なオペレーティング システムで使用されるイメージに、最も大きい値を入力する必要があります。

モバイル ユーザは接続速度が遅いため、リストの先頭にある Windows Mobile の Secure Client イメージをロードする必要があります。また、正規表現 **Windows CE** を指定し、Windows Mobile デバイスのユーザーエージェントを照合して、接続時間を短縮することもできます。モバイル デバイスのブラウザは ASA に接続するときに、HTTP ヘッダーにユーザエージェント文字列を含めます。ASA は文字列を受信して、他の Secure Client イメージが適切かどうかを確認せずに、すぐに Secure Client をダウンロードします。

ステップ 3 セキュアクライアントイメージを追加する、または既存のリストを変更するには、次のいずれかを実行します。

- Secure Client イメージを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、[Secure Client Imageの追加（Add Secure Client イメージ）] ダイアログボックスに入力します。イメージを定義するファイル オブジェクトの名前、およびイメージのプライオリティ順を指定する必要があります。また、接続クライアントのダウンロード速度を改善するために正規表現を指定することもできます。オプションの詳細については、[Secure Client Imageの追加/編集（Add/Edit Secure Client イメージ）] ダイアログボックス （92 ページ）を参照してください。
- イメージを編集するには、イメージを選択し、[行の編集（Edit Row）] ボタンをクリックして、[Secure Client Imageの編集（Edit Secure Client イメージ）] ダイアログボックスで変更を行います。
- イメージを削除するには、イメージを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

ステップ 4 Secure Client プロファイルを追加する、または既存のリストを変更するには、次のいずれかを実行します。

- Secure Client プロファイル を追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、[Secure Client Profileの追加（Add Secure Client プロファイル）] ダイアログボックスで次のオプションを設定します。
  - [Secure Clientプロファイル名（Secure Client Profile Name）]：プロファイルの名前。

このプロファイルを使用するには、（ASA グループ ポリシーの SSL VPN フル クライアント設定で説明されているように [Full Client] の設定ページで）セキュリティ アプライアンスに割り当てられる ASA Group Policy オブジェクトのプロファイル名を指定していることを確認します。デバイスのリモート アクセス Connection Profile ポリシーを介して ASA Group Policy オブジェクトを設定します（接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ）を参照）。

- [Secure Clientプロファイルタイプ（Secure Client Profile Type）]：追加または編集する Secure Client プロファイルプロファイルのタイプを次から選択します。VPN、ネットワークアクセス マネージャ、テレメトリ、Web セキュリティ、ISE ポスチャ、またはカスタマーエクスペリエンス フィードバック。
- [Secure Clientプロファイルファイル（Secure Client Profile File）]：Secure Client プロファイル XML ファイルを識別するファイルオブジェクトの名前。ファイル名の拡張子は、Secure Client プロファイルのタイプによって異なります。VPN（.xml）、ネットワークアクセス マネージャ（.nsp）、テレメトリ（.tsp）、Web セキュリティ（.wsp）、Web セキュリティ WSO（.wso）、ISE ポスチャ（. isp）、カスタマーエクスペリエンス フィードバック（.fsp）。[選択（Select）] をクリックしてオブジェクトを選

択するか、新しいオブジェクトを作成します。ファイル オブジェクトの詳細については、[Add File Object]/[Edit File Object] ダイアログボックスを参照してください。

（注） バージョン 4.22 以降、Cisco Security Manager は、[Secure Clientイメージの追加（Add Secure Client Image）] にある新しい [Webセキュリティ WSO（Web Security WSO）] プロファイルタイプを介した WSO ファイルの直接アップロードをサポートします。ただし、[Webセキュリティ WSO（Web Security WSO）] プロファイルタイプを選択すると、Secure Client プロファイルエディタを使用して WSO ファイルを編集できないため、[エディタの起動（Launch Editor）] オプションが自動的に無効になります。

（注） バージョン 4.7 以降、Security Manager は AnyConnect バージョン 3.2 のサポートを提供します。Secure Client プロファイルタイプとして ISE ポスチャを選択した場合、Secure Client プロファイルファイルのファイル名拡張子は .isp である必要があります。

- [ストレージURLの有効化（Enable Storage URL）]：バージョン 4.12 以降、Security Manager では、ASA 9.6(2) 以降のマルチコンテキストデバイスに対して、プライベートまたは共有オプションのいずれかを選択できます。
- [エディタの起動（Launch Editor）]：[エディタの起動（Launch Editor）] をクリックし、Secure Client プロファイルエディタを使用して、Secure Client プロファイルファイルで指定されたプロファイルを編集するか、プロファイルファイルが指定されていない場合は新しいプロファイルを作成します。ファイル オブジェクトの詳細については、Cisco Secure Client プロファイルエディタ （88 ページ）を参照してください。

  （注） Secure Client プロファイルエディタを使用して新しいプロファイルを作成する場合は、Secure Client プロファイルファイルを指定しないでください。

- プロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックして、[Secure Client Profileの編集（Edit Secure Client プロファイル）] ダイアログボックスで変更を行います。
- プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

（注） [Secure Clientイメージ/プロファイル（Secure Client Image/Profile）] 設定を保存するには、デバイスをマルチコンテキストデバイスとして Cisco Security Manager に追加する必要があります。Security Manager が [ストレージURL（Storage URL）] を取得するにはシステムコンテキストが必須であり、デフォルトの [ストレージURL（Storage URL）]（disk0:/csm）がデフォルトで割り当てられるため、マルチコンテキストデバイスをスタンドアロンとして追加すると、[Secure Clientイメージ/プロファイル（Secure Client Image/Profile）]設定を追加するときに展開エラーが発生する可能性があります。このデフォルトの割り当ては、スタンドアロンデバイスとして追加されたマルチコンテキストデバイスのシステムコンテキストがないため、Security Manager が **ストレージ URL** をフェッチできなくなるために発生します。

[Secure Client Imageの追加/編集（Add/Edit Secure Client イメージ）] ダイアログボックス

[Secure Client Imageの追加または編集（Add or Edit Secure Client イメージ）] ダイアログボックスを使用して、クライアントイメージとしてパッケージファイルを作成または編集し、セキュリティアプライアンスがイメージをリモートワークステーションにダウンロードする順序を確立します。

ナビゲーション パス

ASA デバイスの [SSL VPNのその他の設定（SSL VPN Other Settings）] ポリシーの [クライアント設定（Client Settings）] タブから、Secure Client イメージテーブルの [行の追加（Add Row）] ボタンをクリックするか、イメージを選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、SSL VPN セキュアクライアント の設定について （86 ページ）を参照してください。

関連項目

- SSL VPN セキュアクライアント の設定について （86 ページ）
- SSL VPN セキュアクライアント の設定について （86 ページ）
- SSL VPN サポート ファイルの概要と管理

フィールド リファレンス

表 *23 : [Secure Client Image*の追加/編集（*Add or Edit Secure Client* イメージ）*]* ダイアログボックス

要素	説明
Secure Client イメージ	Secure Client を識別するファイルオブジェクトの名前。[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。ファイル オブジェクトの詳細については、[Add File Object]/[Edit File Object] ダイアログボックスを参照してください。
Image Order	セキュリティ アプライアンスがクライアント イメージをリモート ワークステーションにダウンロードする順序。イメージは、プライオリティ順でダウンロードされます。そのため、最も一般的なオペレーティング システムで使用されるイメージに、より小さい値を入力する必要があります。

要素	説明
正規表現	ユーザエージェントを照合する正規表現。既存の正規表現のポリシーオブジェクトの名前を入力するか、[選択（Select）] をクリックして [正規表現セレクタ（Regular Expressions Selector）] ダイアログボックスからエントリを選択します。新しい正規表現を追加するには、[正規表現セレクタ（Regular Expressions Selector）] ダイアログボックスの [追加]（+）（Add (+)）] ボタンをクリックします。詳細については、正規表現の追加/編集を参照してください。 Windows Mobile の Secure Client パッケージを追加する場合、正規表現の **Windows CE** を指定して、Windows Mobile デバイスのユーザーエージェントを照合します。これにより、モバイルデバイスの接続時間を短縮できます。モバイルデバイスのブラウザは適応型セキュリティアプライアンスに接続するときに、HTTP ヘッダーにユーザエージェント文字列を含めます。適応型セキュリティ アプライアンスは、文字列を受信して、他の Secure Client イメージが適切かどうかを確認せずに、すぐに Windows Mobile 用の Secure Client をダウンロードします。
ストレージ URL を有効にします。 （ASA 9.6(2) 以降のマルチコンテキストデバイスのみ）	バージョン 4.12 以降、Security Manager では、ASA 9.6(2) 以降のマルチコンテキストデバイスに対して、プライベートまたは共有オプションのいずれかを選択できます。 （注） Secure Client イメージ/プロファイル設定を保存するには、デバイスをマルチコンテキストデバイスとして Cisco Security Manager に追加する必要があります。Security Manager が [ストレージ URL（Storage URL）] を取得するにはシステムコンテキストが必須であり、デフォルトの [ストレージURL（Storage URL）]（disk0:/csm）がデフォルトで割り当てられるため、マルチコンテキストデバイスをスタンドアロンとして追加すると、[Secure Client イメージ/プロファイル（Secure Client Image/Profile）]設定を追加するときに展開エラーが発生する可能性があります。このデフォルトの割り当ては、スタンドアロンデバイスとして追加されたマルチコンテキストデバイスのシステムコンテキストがないため、Security Manager が**ストレージ URL** をフェッチできなくなるために発生します。

SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA）

認証によりネットワーク リソースを保護するには、多くの方法があります。多くの組織は、Kerberos を使用して特定の Web アプリケーションを保護し、ユーザ名とパスワード、デジタル証明書、RSA SecureID または SmartCards などのその他の認証技術を使用して、SSL VPN へのアクセスを制御します。ただし、Kerberos プロトコルの制限により、ユーザがすでに別の技術を使用して VPN に対する認証を行っている場合、Kerberos 認証は行われません。

Microsoft では、Windows Server 2003 より、この Kerberos における制限を解決しています。プロトコル移行および制約委任を使用することで、ASA は、Windows ドメイン コントローラで

の Kerberos Key Distribution Center（KCD）に対する認証を行い、Kerberos 以外のプロトコルを使用して ASA に対する認証を行っているユーザの代替チケットを取得できます。ASA は、代替チケットを使用して、リモート ユーザの他の Kerberos サービス チケットを取得できます。

Kerberos Constrained Delegation が機能するようにドメイン コントローラを設定するには、次のようにする必要があります。

- Kerberos認証を使用するサービスの各インスタンスでは、クライアントがネットワーク上で識別できるように、Service Principle Name（SPN）が定義されている必要があります。SPN は、サービスのインスタンスが実行している Windows アカウントの Active Directory [Service-Principal-Name] 属性に登録します。特定のコンピュータで実行している別のサービスに対してあるサービスを認証する必要がある場合、そのサービスの SPN により、該当するコンピュータで実行中の他のサービスと区別します。

SPN のシンタックスは、*service_class/host_name:port* です。

- *service_class* は、サービスを識別します。これは、http などの組み込みサービス、またはユーザ定義サービスです。
- *host_name* は、サービスをホストするサーバーの完全修飾ドメイン名または NetBIOS 名を識別します。IP アドレスにすることはできません。
- *port* は、サービスが実行するポートを識別します。デフォルト サービス ポートを使用する場合は、port を省略できます。
- ASA が使用できるサービス アカウント ユーザ名およびパスワードを作成します。任意の認証プロトコルに対して Kerberos Constrained Delegation を許可するアカウントを設定します。また、ユーザ アカウントには、委任できない機密アカウントを使用しないでください。

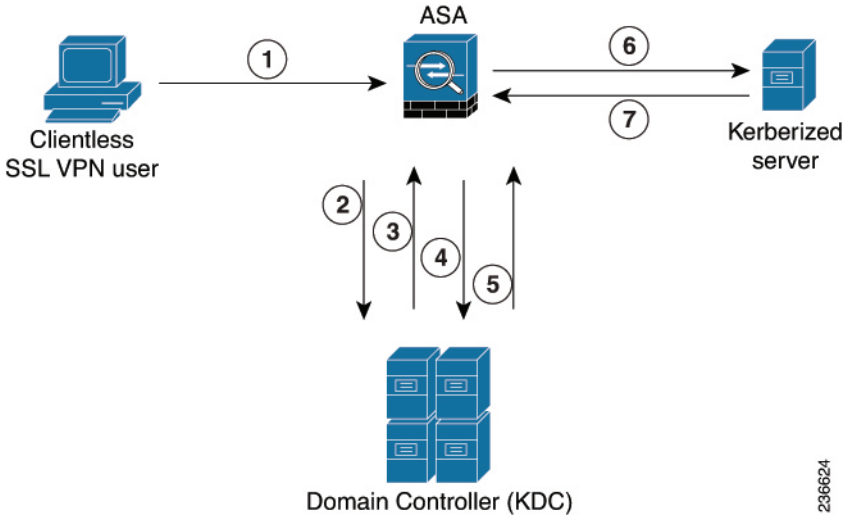
KCD を許可するように ASA を設定するには、ASA がドメインに参加したら、ASA のドメイン コントローラの [Users and Computers] リスト下にエントリが表示される必要があります。[委任（Delegation）] タブの [プロパティ（Properties）] ダイアログボックスで、[指定されたサービスの委任にのみこのコンピュータを信頼する（Trust this computer for delegation to specified services only）] を選択してから、[任意の認証プロトコルを使用する（Use any authentication protocol）] を選択します。認可サービスのテーブルで、ユーザに代わり ASA が認証を委任されるすべてのサービスを追加します。

ヒント Windows ドメイン コントローラでこの機能を設定する方法の詳細については、Microsoft のマニュアルを参照してください。

ASA が Kerberos Constrained Delegation を使用できるようにするには、SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA） （96 ページ）で説明されているように ASA を設定する必要があります。この機能を使用できるのは、ASA Software リリース 8.4 以降のみです。

次の例では、Kerberos Constrained Delegation が ASA でホストされるクライアントレス SSL VPN でどのように機能するかについて説明しています。

図 *1 : Kerberos Constrained Delegation* の例



設定されている認証メカニズムで SSL VPN ユーザーのアイデンティティを確認した後、ASA は、プロトコル移行を使用して、ユーザーの代わりに認証を行うために Kerberos プロトコルに切り替えます。次に、ユーザーのログイン情報ではなく Kerberos サービスチケットを、認証のために Kerberos を受け入れる公開済み Web サーバーに送信します。これらのステップを次に示します。

1. SSL VPN ユーザ セッションが、ユーザに設定されている認証メカニズムを使用して ASA により認証されます。たとえば、Smartcard クレデンシャルの場合、ASA は、デジタル証明書から必要な情報（ユーザーのプリンシパル名）を抽出して、Windows Active Directory に対して LDAP 認可を実行します。
2. 認証が成功すると、ユーザは、ASA SSL VPN ポータル ページにログインします。VPN ユーザは、URL をポータルページに入力するか、ブックマークをクリックして、Web サービスにアクセスします。このアクセスで認証が必要な場合、サーバは、ASA クレデンシャルの認証確認を行い、同時に、サーバでサポートされている認証メカニズムのリストを送信します。認証確認時の HTTP ヘッダーに基づいて、ASA は、サーバで Kerberos 認証が必要かどうかを決定します。バックエンド サーバとの接続で、Kerberos 認証が必要な場合、ASA は、ユーザの代わりにそれ自体のために、代替チケットを KDC から要求します。
3. KDC は、要求されたチケットを ASA に返します。これらのチケットは ASA に渡されますが、ユーザーの許可データが含まれています。

（注） これらの最初のステップでは、プロトコル移行が行われます。これらのステップの後、Kerberos 以外の認証プロトコルを使用して ASA に対して認証を行ったユーザは、透過的に、Kerberos を使用して KDC に対して認証されます。

1. ここで、ASA は、ユーザがアクセスする特定のサービス用の KDC からのサービス チケットを要求します。サービス チケット要求には、サービスの SPN（一意な ID）が含まれます。
2. KDC は、特定のサービスのサービス チケットを ASA に返します。
3. ASA は、このサービス チケットを使用して、Web サービスへのアクセスを要求します。前述の例の場合、これは、HTTP GET 要求で Web サーバに送信されます。
4. Web サーバは、Kerberos サービス チケットを認証して、サービスへのアクセスを付与します。認証に失敗すると、表示されるポータルを確認したあとで、該当するエラー メッセージが表示されます。

SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA）

[SSL VPN Other Settings] ページの [Microsoft KCD Server] タブを使用して、ASA でホストされるクライアントレス SSL VPN の Kerberos Constrained Delegation（KCD）を設定します。

KCD は、Kerberos における制限に対処します。Kerberos 以外の方法を使用して SSL VPN に対する認証を行うユーザは、Kerberos で保護されたリソースにアクセスできません。この場合、ASA などのリモート アクセス デバイスは、Kerberos 以外の方法を使用するユーザを認証できません。ただし、企業内で Kerberos を使用して認証された Web アプリケーションへのシングル サインオン アクセスは提供されます。

この制限がネットワークに適用される場合、KCD を設定してこの制限を回避できます。KCD は、ASA に対する Kerberos 認証をオフロードします。ユーザは、SSL VPN ポータルを使用して企業ネットワークにログインすると、これ以降、Kerberos 保護サービスに透過的にアクセスします。

ヒント

- KCD では、ASA リリース 8.4+ が必要です。これ以外のリリースで KCD を設定しても、設定は無視されます。
- この機能は、クライアントレス SSL VPN アクセスだけで使用されます。
- KCD では、ドメイン コントローラとして設定された、Microsoft Windows Server（2003 または 2008）が必要です。
- SSL VPN Bookmark ポリシー オブジェクトを使用して、SSL VPN ポータル ページに含めるブックマークを定義した場合、サービスがデフォルト以外のポートを使用していると、場合によっては、明示的な Service Principle Name（SPN）パラメータをブックマークに追加する必要があります。Kerberos 認証を使用するサービスでは、SPN は、サービスが実行するアカウントの Service-Principle-Name 属性で定義される必要があります。

ブックマークは、この設定を反映する必要があります。SPN は、URL: http://<url>?SPN=<spn> or http://<url>?SPN=<spn> でのパラメータです。たとえば、**http://owa.example.com?SPN=http/owa:444** など。SPN 構文の詳細については、SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA） （93 ページ）を参照してください。

- この機能を設定するには、ホスト名、DNS および NTP ポリシーも設定する必要があります。ホスト名ポリシーでは、ホスト名およびドメイン名の両方を設定します。
- Kerberos 認証では、ホスト間のクロックは、5 分（デフォルト設定）以下で同期化される必要があります。この制限は、ASA、ドメイン コントローラおよびアプリケーション サーバのクロックに適用されます。すべてのサーバで同じ NTP サーバを設定すると、この要件に対処できます。

関連項目

- 他の SSL VPN 設定の定義（ASA） （71 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** 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、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。

ステップ 2 [その他の設定（Other Settings）] ページで、[Microsoft KCDサーバー（Microsoft KCD Server）] タブをクリックします。

ステップ 3 [KCDの設定（Configure KCD）] を選択して、次のオプションを設定します。

- [KCDサーバー（KCD Server）]：Kerberos Constrained Delegation で使用する Microsoft KCD サーバー（ドメインコントローラ）を識別する AAA サーバー グループ オブジェクト。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。オブジェクトは、Kerberos AAA サーバ ポリシー オブジェクトを使用して、ドメイン コントローラを識別する必要があります。
- [ユーザー名、パスワード、確認（Username, Password, Confirm）]：ASA が Active Directory ドメインに参加するために使用できるユーザーアカウント。

ASA が Kerberos プロトコル移行および Kerberos Constrained Delegation を使用し、リモート アクセス ユーザの代わりにサービス チケットを取得するには、ドメイン コントローラ認証のために ASA により使用されるアカウントは、Active Directory に含まれている必要があり、任意のプロトコルで Kerberos Constrained Delegation を許可できるように設定される必要があります。また、ユーザ アカウントには、委任できない機密アカウントを使用しないでください。Active Directory の設定要件の詳細については、 SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA） （93 ページ）を参照してください。

Secure Client カスタム属性（ASA）の設定

Secure Client カスタム属性が、ASA ソフトウェアをアップグレードすることなく、新しいクライアントコントロールの追加を総合的にサポートする機能を ASA に提供することで、新しいエンドポイント機能のより迅速な配信と展開が可能になります。

[SSL VPNのその他の設定（ SSL VPN Other Settings）] ページの [Secure Clientカスタム属性（Secure Client Custom Attribute）] タブでは、設定済みの Secure Client カスタム属性を表示したり、新しい属性を追加したり、既存の属性を変更または削除したりできます。

関連項目

- SSL VPN サポート ファイルの概要と管理
- 他の SSL VPN 設定の定義（ASA） （71 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASAデバイスを選択して、ポリシーセレクタから**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** 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、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。

ステップ 2 [その他の設定（Other Settings）] ページで、[Secure Clientカスタム属性（Secure Client Custom Attribute）] タブをクリックします。[Secure Clientカスタム属性（Secure Client Custom Attribute）] タブには、定義済みのすべてのカスタム属性が一覧表示されます。

ステップ 3 次のいずれかを実行します。

- カスタム属性を追加するには、テーブルの下にある [行の追加（Add Row）] ボタンをクリックし、[Secure Clientカスタム属性の追加（Add Secure Client Custom Attribute）] ダイアログボックスに入力します。これらのオプションについては、[Secure Clientカスタム属性の追加/編集（Add/Edit Secure Client Custom Attribute）] ダイアログボックス （98 ページ）で詳しく説明されています。
- カスタム属性を編集するには、そのカスタム属性を選択し、[行の編集（Edit Row）] ボタンをクリックして、[プラグインエントリの編集（Edit Plug-In Entry）] ダイアログボックスで変更します。
- カスタム属性を削除するには、カスタム属性を選択して [行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

[Secure Clientカスタム属性の追加/編集（Add/Edit Secure Client Custom Attribute）] ダイアログボックス

[Secure Clientカスタム属性の追加または編集（Add or Edit Secure Client Custom Attribute）] ダイアログボックスを使用して、Secure Client カスタム属性を追加または変更します。Secure Client カスタム属性が、ASA ソフトウェアをアップグレードすることなく、新しいクライアントコン

トロールの追加を総合的にサポートする機能を ASA に提供することで、新しいエンドポイント機能のより迅速な配信と展開が可能になります。

バージョン 4.7 以降、Security Manager では、ソフトウェアバージョン 9.3(1) 以降を実行している ASA デバイスの既存のカスタム属性タイプにカスタム属性データを追加できます。[Secure Clientカスタム属性の追加または編集（Add or Edit Secure Client Custom Attribute Data）] ダイアログボックスを使用して、既存の Secure Client カスタム属性タイプの属性名と属性値を追加または変更します。詳細については、[Secure Clientカスタム属性データの追加/編集（Add/Edit Secure Client Custom Attribute Data）] ダイアログボックス （99 ページ）を参照してください。

ナビゲーション パス

ASA デバイスの SSL VPN の [その他の設定（Other Settings）] ポリシーに含まれる [Secure Client カスタム属性（Secure Client Custom Attribute）] タブから、[Secure Clientカスタム属性（Secure Client Custom Attribute）] テーブルの [行の追加（Add Row）] ボタンをクリックするか、属性を選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、Secure Client カスタム属性（ASA）の設定 （98 ページ）を参照してください。

関連項目

- SSL VPN セキュアクライアント の設定について （86 ページ）
- SSL VPN セキュアクライアント 設定の構成（ASA） （89 ページ）
- SSL VPN サポート ファイルの概要と管理

フィールド リファレンス

表 *24 : [Secure Client*カスタム属性の追加または編集（*Add or Edit Secure Client Custom Attribute***）*]* ダイアログボックス**

要素	説明
タイプ	Secure Client カスタム属性のタイプ。Security Manager で属性を参照する場合、およびセキュアクライアントに送信される集約認証プロトコルメッセージで使用されます。最大長は 32 文字です。
説明	属性の使用方法の自由形式の説明。このテキストは、カスタム属性がグループポリシー属性コンフィギュレーションモードから参照された場合に、コマンドヘルプで表示されます。最大長は 128 文字です。

[Secure Clientカスタム属性データの追加/編集（Add/Edit Secure Client Custom Attribute Data）] ダイアログボックス

Security Manager version 4.7 以降、[Secure Clientカスタム属性データの追加または編集（Add or Edit Secure Client Custom Attribute Data）] ダイアログボックスを使用して、既存の Secure Client カスタム属性タイプの属性名と属性値を追加または変更できます。

ナビゲーション パス

ASA デバイスに対する SSL VPN のその他の設定ポリシーの [Secure Clientカスタム属性（Secure Client Custom Attribute）] タブをクリックします。[カスタム属性（Custom Attribute）] テーブルで属性タイプを選択し、[カスタム属性データ（Custom Attribute Data）] テーブルの [行の追加（Add Row）] ボタンをクリックします。または、[カスタム属性データ（Custom Attribute Data）] テーブルで既存のカスタム属性データを選択し、[行の編集（Edit Row）] ボタンをクリックします。

属性タイプごとに、対応する値を持つ複数の属性名を定義できます。

属性タイプの追加または変更については、SSL VPN セキュアクライアント の設定について（86 ページ）を参照してください。

関連項目

- SSL VPN セキュアクライアント の設定について （86 ページ）
- [Secure Clientカスタム属性の追加/編集（Add/Edit Secure Client Custom Attribute）] ダイアログボックス （98 ページ）
- SSL VPN セキュアクライアント 設定の構成（ASA） （89 ページ）
- SSL VPN サポート ファイルの概要と管理

フィールド リファレンス

表 *25 : [Secure Client*カスタム属性データの追加/編集（*Add/Edit Secure Client Custom Attribute Data***）*]*ダイアログボックス**

要素	説明
Attribute Name	Secure Client カスタム属性の名前。この名前は、group-policy および dynamic-access-policy-record 設定モードで属性を参照するときに使用します。最大長は 32 文字です。
属性値（Attribute Value）	属性値を含む自由形式の文字列。この属性値は、属性名に関連付けられ、接続の設定中にクライアントに渡されます。文字列の最大長は 420 文字です。 属性値には、複数のテキスト行を含めることができます。

SSL VPN の高度な設定の定義（ASA）

[SSL VPN Other Settings] ページの [Advanced] タブを使用して、メモリ、オンスクリーン キーボードおよび内部パスワード機能を ASA デバイスで設定します。Cisco Security Manager 4.15 以降では、HSTS サポートを有効にして、タイムアウト値を指定することもできます。これらの設定はすべて任意です。

関連項目

- 他の SSL VPN 設定の定義（ASA） （71 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASAデバイスを選択して、ポリシーセレクタから**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** 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、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。

ステップ 2 [その他の設定（Other Settings）] ページで [詳細（Advanced）] タブをクリックします。

ステップ 3 [メモリサイズ（Memory Size）] フィールドで、SSL VPN セッションに割り当てるメモリ容量を指定します。デフォルトは 50% です。

設定を変更するには、次のいずれかのオプションを選択して、目的の数値を入力します。

- [物理メモリ合計の割合（% of Total Physical Memory）]：全体のメモリに対するパーセンテージで指定します。デフォルトは 50% です。
- [キロバイト（Kilobytes）]：KB 単位で指定します。許可される最小設定値は、20 KB です。次の例に示すように、ASA モデルのタイプによって合計のメモリ量が異なるため、KB 単位では指定することは推奨されません。

（注） メモリ サイズを変更した場合、新しい設定は、システムをリブートしないと有効になりません。

ステップ 4 [オンスクリーンキーボードの有効化（Enable On-Screen Keyboard）] フィールドで、次のいずれかのオプションを選択します。

- [無効（Disabled）]：オンスクリーンキーボードは表示されません。ユーザは、標準のキーボードを使用してクレデンシャルを入力する必要があります。これがデフォルトです。
- [すべてのページ（On All Pages）]：ユーザーは、ログインクレデンシャルが必要になると表示されるオンスクリーンキーボードを使用してクレデンシャルを入力できます。
- [ログインページのみ（On Logon Page Only）]：ユーザーは、ログインページに表示される（クレデンシャルを必要としないページでは表示されません）オンスクリーンキーボードを使用してクレデンシャルを入力できます。

（注） Cisco Security Manager 4.24 以降、オンスクリーンキーボードの有効化機能は、ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

ステップ 5 内部サイトにアクセスするときに追加パスワードを要求する場合は、[内部パスワードの入力を許可（Allow Users to Enter Internal Password）] を選択します。この機能は、内部パスワードを SSL VPN パスワードとは別のパスワードにする必要がある場合に役立ちます。たとえば、ASA への認証にはあるワンタイム パスワードを使用して、内部サイトには別のパスワードを使用できます。

（注） HSTS オプションは、ASA 9.8.2 以降のデバイスでのみ使用できます。

ステップ 6 [HTTP厳重トランスポートセキュリティ（HSTS）（HTTP Strict Transport Security (HSTS)）] 領域で、次の手順を実行します。

- HSTS サポートを有効にするには、[HSTSヘッダーの有効化（Enable HSTS Header）] チェックボックスをオンにします。HSTS 機能は、ヘッダーをクライアントに送信することで有効にできます。サポートを無効にするには、このチェックボックスをオフにします。
- [HSTSヘッダーの有効化（Enable HSTS Header）] チェックボックスを選択した場合は、[HSTSヘッダーのタイムアウト（HSTS Header Timeout）] にタイムアウト値を入力します。このフィールドを空白のままにすると、Cisco Security Manager はデフォルトのタイムアウト値である 10886400 を使用します。
- ヘッダーにサブドメイディレクティブを含める場合は、[サブドメインを含める（Include Sub Domains）] チェックボックスをオンにします。
- ヘッダーにペイロードディレクティブを含める場合は、[ペイロード（Payload）] チェックボックスをオンにします。
- [HSTSクライアントの有効化（Enable HSTS-Client）] チェックボックスをオンにすると、HSTS ホストの HSTS ポリシーの適用が制御されます。
- [X-Content-Type-Optionsの有効化（Enable X-Content-Type-Options）] チェックボックスをオンにすると、X-Content-Type-Options 応答ヘッダーをクライアントに送信できます。
- [X-XSS-Protectionの有効化（Enable X-XSS-Protection）] チェックボックスをオンにすると、X-XSS-Protection 応答ヘッダーをクライアントに送信できます。

（注） [ペイロード（Payload）] チェックボックスを選択すると、[サブメインを含める（Sub Domains）] もデフォルトで選択されます。

- ペイロードを選択する場合は、HSTS ヘッダーのタイムアウト値が 31536000 以上であることを確認してください。

（注） バージョン 4.21 以降、Cisco Security Manager は HSTS サーバーコマンドで [HSTSクライアントの有効化（Enable HSTS-Client）]、[X-Content-Type-Optionsの有効化（Enable X-Content-Type-Options）]、および [X-XSS-Protectionの有効化（Enable X-XSS-Protection）] CLI オプションのサポートを開始します。ただし、[コンテンツセキュリティポリシー（Content-Security-Policy）] はサポートされていません。これは Flex Config を介してのみ設定できます。

SSL VPN サーバー検証の設定（ASA）

クライアントレス SSL VPN 経由でリモート SSL 対応サーバに接続する場合は、リモート サーバを信頼できること、また、接続先が実際にサーバであることを認識することが重要です。ASA 9.0 には、クライアントレス SSL VPN の信頼できる認証局（CA）証明書のリストに対する SSL サーバ証明書の検証のためのサポートが追加されています。

HTTPS プロトコルを使用して Web ブラウザ経由でリモート サーバに接続する場合、サーバはサーバ自体を識別するために CA が署名したデジタル証明書を提供します。Web ブラウザに

は、サーバ証明書の有効性を検証するために使用される一連の CA 証明書が付属しています。これは、公開キー インフラストラクチャ（PKI）の 1 つの形式です。

ブラウザが証明書管理の機能を提供するのと同様に、ASA も信頼できる証明書のプール管理機能の形式を提供します（trustpools）。これは、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には、Web ブラウザで提供されるのと同様のデフォルトの証明書のバンドルが含まれますが、管理者がアクティブにするまで非アクティブとなります。

（注） すでに Cisco IOS の trustpools に精通している場合、ASA バージョンが、似ているが同じではないことがわかります。

ここでは、クライアントレス SSL VPN ユーザーの HTTPS サーバー検証を有効にする方法について説明します。

関連項目

- 他の SSL VPN 設定の定義（ASA） （71 ページ）
- 信頼できるプール設定の設定（ASA） （42 ページ）
- Trustpool Manager の使用 （45 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASAデバイスを選択して、ポリシーセレクタから**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。[SSLサーバー検証（SSL Server Verification）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。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。[SSLサーバー検証（SSL Server Verification）] タブをクリックします。

ステップ 2 クライアントレス SSL VPN ユーザーの HTTPS サーバー検証を有効にするには、[有効（Enable）] を選択します。

ステップ 3 サーバー証明書の検証に失敗した場合に実行するアクションを指定します。

- [ユーザーをHTTPSから切断（Disconnect user from Https）] ページ：サーバーを検証できなかった場合は切断します。
- [ユーザーにHTTPSへの接続を許可（Allow user to continue to Https）] ページ：チェックが失敗した場合でも、ユーザーが接続を継続できるようにします。

SSL VPN 共有ライセンスの設定（ASA 8.2+）

[SSL VPN Shared License] ページを使用して、SSL VPN 共有ライセンスを設定します。

多数の SSL またはリモート アクセス IKEv2 IPsec VPN セッションに対応した共有ライセンスを購入し、ASA デバイスの 1 つを共有ライセンス サーバ、残りのデバイスをクライアントとして設定すると、必要に応じて ASA デバイスのグループ全体でセッションを共有できます。サーバ ライセンスの場合、500 単位で 500 ～ 50,000 ライセンス、1000 単位で 50,000 ～ 1,040,000 ライセンスを共有できます。

ライセンスは、SSL または IKEv2 IPsec 接続を確立する各リモート アクセス ユーザにより使用されます。

（注） 共有ライセンスは、Secure Client Essentials ライセンスと同時には使用できません。

ここでは、共有ライセンスの設定手順について説明します。

- 共有ライセンス クライアントとしての ASA デバイスの設定 （106 ページ）
- 共有ライセンス サーバとしての ASA デバイスの設定 （107 ページ）

ナビゲーション パス

- （デバイスビュー）バージョン 8.2 以降を使用する ASA デバイスを選択し、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（Shared License）] 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、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（ASA 8.2+）（Shared License (ASA 8.2+)）] を選択します。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 26 : [SSL VPN Shared License] ページ

要素	説明
Select Role	設定するロール（[Shared License Client] または [Shared License Server]）。選択した項目によって、表示されるフィールドが異なります。
Shared License Client	
共有秘密鍵（Shared Secret）	共有ライセンス サーバとの通信に使用される、大文字と小文字が区別される文字列（4 ～ 128 文字）。

要素	説明
ライセンス サーバ	ライセンス サーバとして設定されている ASA デバイスを識別するネットワーク/ホスト オブジェクトの IP アドレスまたは名前。[選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。
License Server Port	ライセンス サーバが通信する TCP ポートの番号。ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。
Select Backup Role of Client	クライアントのバックアップ ロール。 • [Client Only]：選択すると、クライアントはクライアントとしてだけ機能します。この場合は、別のデバイスをバックアップ サーバとして指定できます。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。 • [Backup Server]：選択すると、クライアントはバックアップ サーバとしても機能します。この場合は、この目的に使用されるインターフェイスも指定する必要があります。インターフェイス名またはインターフェイス ロール オブジェクトのカンマ区切りリストを入力します。あるいは、[選択（Select）] をクリックして、インターフェイスまたはオブジェクトを選択するか、新しいオブジェクトを作成します。
Shared License Server	
共有秘密鍵（Shared Secret）	共有ライセンス サーバとの通信に使用される、大文字と小文字が区別される文字列（4 ～ 128 文字）。
License Server Port	ライセンス サーバが通信する TCP ポートの番号。ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。
更新間隔（Refresh Interval）	10 ～ 300 秒のリフレッシュ間隔。デフォルトは 30 秒です。
インターフェイス	クライアントとの共有ライセンスの通信に使用されるインターフェイスのカンマ区切りリスト。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックしてインターフェイスまたはオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Configure Backup shared SSL VPN License Server	共有ライセンス サーバのバックアップ サーバを設定するかどうかを指定します。このオプションを選択した場合は、次の項目を設定します。 • [バックアップライセンスサーバー（Backup License Server）]：現在のサーバーが使用できなくなった場合のバックアップ ライセンス サーバーとして機能するサーバーの IP アドレス、またはアドレスを含むネットワーク/ホストオブジェクト。[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。 • [バックアップサーバーのシリアル番号（Backup Server Serial Number）]：バックアップ ライセンス サーバーのシリアル番号。 • [HAペアのシリアル番号（HA Peer Serial Number）]：（任意）フェールオーバーペアのバックアップサーバーのシリアル番号。

ここでは、次の内容について説明します。

- 共有ライセンス クライアントとしての ASA デバイスの設定 （106 ページ）
- 共有ライセンス サーバとしての ASA デバイスの設定 （107 ページ）

共有ライセンス クライアントとしての ASA デバイスの設定

ここでは、ASA デバイスを共有ライセンス クライアントとして設定する方法について説明します。

ヒント SSL VPN Shared License Client アクティベーション キーがデバイスに存在することを確認する必要があります。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（Shared License）] 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、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（ASA 8.2+）（Shared License (ASA 8.2+)）] を選択します。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。

[SSL VPN Shared License] ページが表示されます（SSL VPN 共有ライセンスの設定（ASA 8.2+） （104 ページ）を参照）。

ステップ 2 デバイスのロールとして [共有ライセンスクライアント（Shared License Client）] を選択します。

ステップ 3 [Shared Secret] フィールドに、共有ライセンス サーバとの通信に使用されるストリング（4 ～ 128 文字で、大文字と小文字が区別される）を入力して、確認します。

ステップ 4 [License Server] フィールドで、ライセンス サーバとして設定されている ASA デバイスを識別するネットワーク/ホスト オブジェクトの IP アドレスまたは名前を入力します。

ステップ 5 [License Server Port] フィールドに、ライセンス サーバが通信する TCP ポートの番号を入力します。

ステップ 6 クライアントのロールを選択します。

- [クライアントのみ（Client Only）]：選択すると、クライアントはクライアントとしてのみ機能します。この場合は、別のデバイスをバックアップ サーバとして指定できます。
- [バックアップサーバー（Backup Server）]：選択すると、クライアントはバックアップサーバーとしても機能します。この場合は、この目的に使用されるインターフェイスも指定する必要があります。

共有ライセンス サーバとしての ASA デバイスの設定

ここでは、ASA デバイスを共有ライセンス サーバとして設定する方法について説明します。

ヒント SSL VPN Shared License Server アクティベーション キーがデバイスに存在することを確認する必要があります。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（Shared License）] 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、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（ASA 8.2+）（Shared License (ASA 8.2+)）] を選択します。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。

[SSL VPN Shared License] ページが表示されます（SSL VPN 共有ライセンスの設定（ASA 8.2+） （104 ページ）を参照）。

ステップ 2 デバイスのロールとして [共有ライセンスサーバー（Shared License Server）] を選択します。

ステップ 3 [Shared Secret] フィールドに、共有ライセンス サーバとの通信に使用されるストリング（4 ～ 128 文字で、大文字と小文字が区別される）を入力して、確認します。

ステップ 4 [License Server Port] フィールドに、ライセンス サーバが通信する TCP ポートの番号を入力します。

ステップ 5 [Refresh Interval] フィールドに、リフレッシュ間隔として使用される 10 ～ 300 秒の間の値を入力します。デフォルトは 30 秒です。

ステップ 6 [Interfaces] フィールドに、クライアントとの通信に使用されるインターフェイスを入力または選択します。

ステップ 7 （オプション）（任意）[共有SSL VPNライセンスサーバーのバックアップを設定（Configure Backup shared SSL VPN License Server）] を選択して、共有ライセンスサーバーのバックアップサーバーを設定します。設定項目は次のとおりです。

- [バックアップライセンスサーバー（Backup License Server）]：現在のサーバーが使用できなくなった場合のバックアップ ライセンス サーバーとして機能するサーバーの IP アドレス、またはアドレスを含むネットワーク/ホストオブジェクト。
- [バックアップサーバーのシリアル番号（Backup Server Serial Number）]：バックアップ ライセンス サーバーのシリアル番号。
- [HAペアのシリアル番号（HA Peer Serial Number）]：（任意）フェールオーバーペアのバックアップ サーバーのシリアル番号。

クライアントレス SSL VPN ポータルのカスタマイズ

ブラウザベースのクライアントレス SSL VPN のポータル ページに使用する Web サイトとそのコンテンツは、カスタマイズできます。ASA デバイスでは、IOS デバイスよりもさまざまなカスタマイゼーションが可能です。ユーザが VPN にログインしたとき、または VPN からログアウトしたときに表示される Web ページの外観、ポータルのホームページ、およびユーザが使用可能なブックマークとスマート トンネルを定義する、さまざまなポリシー オブジェクトを作成できます。

ここでは、次の内容について説明します。

SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

SSL VPN カスタマイゼーション オブジェクトは、ユーザに表示される、ブラウザベースのクライアントレス SSL VPN Web ページの外観を記述します。これには、ユーザが ASA セキュリ

ティ アプライアンスに接続したときに表示されるログイン ページ、認証後に表示されるホームページ、およびユーザが SSL VPN サービスからログアウトしたときに表示されるログアウト ページが含まれます。

SSL VPN カスタマイゼーション オブジェクトは、ASA デバイスに ASA グループ オブジェクトまたは Remote Access VPN Connection ポリシーを定義する場合に使用します。それぞれのユーザ グループに対して、そのグループ専用に設計された Web ページが表示されるように、いくつかのカスタマイゼーション オブジェクトを作成し、複数の ASA グループまたは接続プロファイルを定義できます。カスタマイゼーションには、各グループに適した言語で Web ページをローカライズすることも含まれています。ローカリゼーションの詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （112 ページ）を参照してください。

まず、ユーザが初めて接続するとき、接続プロファイルで識別されたデフォルトのカスタマイゼーション オブジェクトによって、ログイン画面の表示方法が決定されます。ユーザがログイン ページの接続プロファイル リストとは異なるグループを選択した場合、そのグループに独自のカスタマイゼーションが設定されていれば、選択したグループのカスタマイゼーション オブジェクトを反映するように画面が変更されます。リモート ユーザが認証されると、グループ ポリシーに割り当てられているカスタマイゼーション オブジェクトによって、画面の外観が決定されます。

この手順で説明した SSL VPN カスタマイゼーション オブジェクトを作成したあとは、このオブジェクトを使用して、次のポリシーのポータル特性を指定できます。

- ASA グループ ポリシー オブジェクトの [SSL VPN] > [設定（Settings）] ページで（ASA グループ ポリシーの SSL VPN 設定を参照）、次のポリシーのいずれかを選択します。
  - **[Remote Access VPN] > [Group Policies]**
  - [全般（General）] タブの [リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]
- [リモートアクセスVPN（Remote Access VPN）]>[接続プロファイル（Connection Profiles）] ポリシーで、[SSL] タブの SSL VPN カスタマイゼーション オブジェクトを指定することもできます（[SSL] タブ（[Connection Profiles]） （30 ページ）を参照）。

関連項目

- ASA デバイスの SSL VPN Web ページのローカライズ （112 ページ）
- ポリシー オブジェクトの作成
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Managerを参照）。

ヒント SSL VPN カスタマイゼーション オブジェクトは、このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに作成することもできます。詳細については、ポリシーのオブジェクトの選択を参照してください。

ステップ 2 オブジェクトタイプセレクタから [SSL VPNのカスタマイズ（SSL VPN Customization）] を選択します。[SSL VPN Customization] ページが開き、既存の SSL VPN カスタマイゼーション オブジェクトのリストが表示されます。

ステップ 3 作業領域を右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add SSL VPN Customization] ダイアログボックスが表示されます（[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックスを参照）。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 さまざまなページの設定を行う前に、[Preview] ボタンを使用してデフォルト設定を表示します。[レビュー（Preview）] をクリックすると [参照（browser）] ウィンドウが開き、[ログイン（Logon）] ページ、[ポータル（Portal）] ページ、または [ログアウト（Logout）] ページのうち、コンテンツテーブルで選択されたいずれかのページの現在の設定が表示されます（これらのフォルダのいずれかのページを選択することは、親フォルダを選択することと同じです）。

ヒント 設定を変更したあと、希望したとおりに変更されているかを確認するには [プレビュー（Preview）] をクリックします。

ステップ 6 ログイン ページの設定を行います。この Web ページは、ユーザが SSL VPN ポータルに接続したときに最初に表示されるページです。VPN へのログインに使用されます。ダイアログボックスの左側のコンテンツ テーブルで、[Logon Page] フォルダから次の項目を選択し、設定を表示および変更します。

- [ログインページ（Logon Page）]：ブラウザのタイトルバーに表示される、Web ページのタイトルを定義します。
- [タイトルパネル（Title Panel）]：[ログイン（Logon）] ページで、Web ページ内にタイトルを表示するかどうかを定義します。タイトル パネルをイネーブルにすると、使用するタイトル、フォント、フォント サイズとフォントの太さ、スタイル、および色を指定できます。ロゴのグラフィックを識別するファイル オブジェクトを選択することもできます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Title Panel]を参照してください。
- [言語（Language）]：ASA デバイスで他言語への変換テーブルを設定し、そのテーブルを使用する場合は、サポートされる言語を設定して、ユーザが自分の言語を選択するようにできます。変換テーブルおよびローカリゼーション サポートの詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （112 ページ）を参照してください。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Language]を参照してください。
- [ログインフォーム（Logon Form）]：ユーザのログイン情報を入力するフォームで使用されるラベルおよび色を設定します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Logon Form]を参照してください。
- [情報パネル（Informational Panel）]：ユーザに追加情報を表示する場合は、情報パネルを有効にして、テキストおよびロゴのグラフィックを追加できます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Informational Panel]を参照してください。
- [著作権パネル（Copyright Panel）]：[ログイン（Logon）] ページに著作権情報を表示する場合は、著作権パネルを有効にして、著作権ステートメントを入力できます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Copyright Panel]を参照してください。

- [フルカスタマイズ（Full Customization）]：セキュリティアプライアンスの組み込みログインページを使用しない（カスタマイズもしない）場合は、代わりにフルカスタマイズを有効にして独自の Web ページを指定できます。必要なファイルの作成の詳細については、ASA デバイスの独自 SSL VPN ログイン ページの作成 （114 ページ）を参照してください。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Full Customization]を参照してください。

ステップ 7 ポータルページの設定を行います。これは SSL VPN ポータルのホームページで、ユーザがログインしたあとに表示されます。ダイアログボックスの左側のコンテンツテーブルで、ポータルページフォルダから次の項目を選択し、設定を表示および変更します。

- [ポータルページ（Portal Page）]：ブラウザのタイトルバーに表示される、Web ページのタイトルを定義します。
- [タイトルパネル（Title Panel）]：ポータルページで、Web ページ内にタイトルを表示するかどうかを定義します。タイトルパネルをイネーブルにすると、使用するタイトル、フォント、フォントサイズとフォントの太さ、スタイル、および色を指定できます。ロゴのグラフィックを識別するファイル オブジェクトを選択することもできます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Title Panel]を参照してください。
- [ツールバー（Toolbar）]：ポータルページに、参照する URL を入力するフィールドを含むツールバーを表示するかどうかを定義します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Toolbar]を参照してください。
- [アプリケーション（Applications）]：ページ上に表示されるアプリケーションボタンを定義します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Applications]を参照してください。
- [カスタムペイン（Custom Panes）]：ポータルページの本文を整理する方法を定義します。デフォルトは、内部ペインのない 1 カラム型のページです。複数カラム レイアウトの作成、テキストまたは URL への参照を表示する内部ペインの作成、およびペインを配置するカラムと行の指定ができます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Custom Panes]を参照してください。
- [ホームページ（Home Page）]：ホームページに URL リストを表示するかどうか、その表示方法、およびポータルページの本文に独自の Web ページを使用するかどうかを定義します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Home Page]を参照してください。

ステップ 8 [ログアウトページ（Logout Page）] を選択して、ユーザが SSL VPN からログアウトするときに表示されるページの設定を行います。タイトル、メッセージ テキスト、フォント、および色を設定できます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Logout Page]を参照してください。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用を参照してください。

ステップ 10 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可を参照してください。

ステップ 11 [OK] をクリックしてオブジェクトを保存します。

ASA デバイスの SSL VPN Web ページのローカライズ

ローカリゼーションとは、ターゲット ユーザに適した言語のテキストを指定するプロセスです。ASA デバイスでホストされる、ブラウザベースのクライアントレス SSL VPN Web ページの外観を定義するための SSL VPN カスタマイゼーション オブジェクトを作成するときに、目的の言語を使用するページを設定できます。

ローカライズされた Web ページを正しく表示するには、ユーザは UTF-8 エンコードを使用するようにブラウザを設定する必要があります（たとえば、Internet Explorer では [表示（View）] > [エンコーディング（Encoding）] > [ユニコード（UTF-8）（Unicode (UTF-8)）] を選択します）。また、[Regional and Language Options] コントロール パネルを使用して、言語に必要なフォントまたは言語サポート ファイルをインストールする必要もあります。[Languages] タブで、[Details] をクリックして必要な言語をインストールし、東アジア言語、文字体系の複雑な言語、および右から左に記述する言語の適切な補助言語設定を選択します。[Advanced] タブで、適切なコードページ変換テーブルを選択します。ユーザがブラウザを正しく設定しなかった場合は、文字ではなく四角形が表示されることがあります。

ASA デバイスでホストされる SSL VPN Web ページは、2 つの方法でのローカライズできます。これらの方法は互いに排他的ではなく、両方を使用できます。その方法は次のとおりです。

- **必要な言語を使用して SSL VPN カスタマイゼーション オブジェクトを設定**：SSL VPN カスタマイゼーション オブジェクトを作成すると、UTF-8 エンコードで英語以外、ASCII 文字以外の言語のラベルおよびメッセージのテキストを入力できます。ASCII 文字以外の言語を UTF-8 エンコードで入力するには、適切なロケール設定で Windows を設定し、必要なフォントをインストールしておく必要があります。システムを設定して、文字体系の複雑な言語または東アジア言語に必要なファイルをインストールするには、[Regional and Language Options] コントロール パネルを使用します。テキストを直接入力する場合は、適切なキーボードもインストールする必要があります。キーボードをインストールしない場合は、その言語の文字をサポートするテキストエディタを使用して、使用するテキストが含まれるドキュメントからそのテキストをコピーアンドペーストできます。

SSL VPN ブックマーク オブジェクトに、ASCII 文字以外の言語を入力することもできます。

- **使用可能にする言語をサポートする ASA デバイスで変換テーブルを設定**：ユーザに表示されるポータルおよび画面の言語変換をセキュリティアプライアンスが提供できるようにするには、必要な言語を変換テーブルに定義して、セキュリティアプライアンスにそのテーブルをインポートする必要があります。セキュリティアプライアンスのソフトウェア イメージ パッケージには、変換テーブルのテンプレートが含まれています。SSL VPN カスタマイゼーション オブジェクトに表示されるすべての言語では、対応する変換テーブルがデバイスに設定されている必要があります。逆に、SSL VPN カスタマイゼーション オブジェクトに表示されていない言語の変換テーブルは無視されます。

この方法を使用する場合は、ASA CLI または ASDM を使用して、変換テーブルを設定およびアップロードする必要があります。Security Manager では変換テーブルを管理できません。ただし、SSL VPN カスタマイゼーション オブジェクトの設定を使用すると、ブラウザ言語を自動的に設定し、ユーザによる適切な言語の選択をイネーブルにできます。したがって、10 言語の変換テーブルをインストールした場合は、そのすべての言語のユーザが、SSL VPN カスタマ

イゼーション オブジェクトに定義されたページを使用できます。これらの設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Language]を参照してください。

次のどちらの機能にも変換テーブルが必要ですが、これらは独立した相補的な機能です。

- **ブラウザ言語の自動選択**：ブラウザ言語の自動選択は、ユーザのブラウザ設定に基づき、適切な言語の選択を試行します。この方法ではユーザ入力が要求されません。SSL VPN カスタマイゼーション オブジェクトでは、ブラウザとのネゴシエーションに使用される言語のリストを作成します。接続時には、セキュリティアプライアンスがブラウザから言語のリスト（およびそのプライオリティ）を受信し、一致する言語が検出されるまで言語のリストを上から下までもれなく調べます。一致する言語がなかった場合は、リストに定義された言語がデフォルト言語として使用されます。デフォルト言語が指定されていない場合は英語が使用されます。

セキュリティアプライアンス上の言語は、変換テーブルのラベルとなります。この言語はブラウザの言語を反映する必要があり、（アルファベット文字で始まる）最大 8 文字の英数字をハイフンで区切ったグループで構成されます。たとえば、fr-FR-paris-univ8 などとなります。ただし、Security Manager のリストに言語を追加するときに使用できるのは、先頭の 2 文字だけです。

一致を検索するとき、セキュリティアプライアンスは最も長い言語名から開始し、一致しない場合は名前の右端のグループを廃棄します。たとえば、ブラウザの優先言語が fr-FR-paris-univ8 で、セキュリティ アプライアンスが fr-FR-paris-univ8、fr-FR-paris、fr-FR、および fr をサポートする場合は、fr-FR-paris-univ8 が一致するので、この変換テーブルの変換ストリングが使用されます。セキュリティ アプライアンス上の言語が fr だけの場合、セキュリティ アプライアンスはこの言語も一致する言語と見なし、その変換テーブルを使用します。

変換テーブルの設定の詳細については、ASA デバイスおよびオペレーティング システムのユーザ マニュアル、または ASDM オンライン ヘルプを参照してください。

- **言語セレクタ**：言語セレクタを有効にすると、サポートする言語のリストから必要な言語をアクティブに選択する機能をユーザに提供します。この方法は、正しく設定されているブラウザ言語設定に依存しません。言語セレクタはログインページに表示されます。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （108 ページ）
- ポリシー オブジェクトの作成
- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス

ASA デバイスの独自 SSL VPN ログイン ページの作成

ブラウザベースのクライアントレス SSL VPN には、セキュリティ アプライアンスから提供されるページを使用するのではなく、独自のカスタム SSL VPN ログイン ページを作成できます。これはフル カスタマイゼーションと呼ばれ、SSL VPN カスタマイゼーション ポリシー オブジェクトでの設定を置き換えます。

独自のログイン ページを表示するには、ページを作成し、作成したページを Security Manager サーバにコピーして、[SSL VPN Customization object] ダイアログボックスの [Full Customization] ページでこのページを指定する必要があります。SSL VPN カスタマイゼーション オブジェクトの作成の詳細については、SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （108 ページ）を参照してください。

フル カスタマイゼーションをイネーブルにすると、ポリシー オブジェクトに設定された、ログイン ページの他のすべての設定が無視されます。ASA デバイスに設定を展開すると、Security Manager によってカスタム ページがデバイスにコピーされます。

作成するログイン ページには、ページを正しく表示するために必要なすべての HTML コード、およびログイン フォームと [Language Selector] ドロップダウン リストの機能を提供するシスコ独自の HTML コードが含まれている必要があります。HTML ファイルを作成する場合は、次の点を考慮してください。

- ファイル拡張子は **.inc** とする。
- カスタム ログイン ページのすべてのイメージを、セキュリティ アプライアンスに配置する必要がある。ファイルパスをキーワード **/+CSCOU+/** で置き換える。これは、ASA デバイスの内部ディレクトリです。イメージをデバイスにアップロードすると、そのイメージはこのディレクトリに保存されます。
- **csco_ShowLoginForm('lform')** JavaScript 関数を使用して、ログインフォームをページに追加する。このフォームによって、ユーザ名、パスワード、およびグループ情報の入力が要求されます。この関数をページのいずれかの場所に記述しておく必要があります。
- JavaScript 関数 **csco_ShowLanguageSelector('selector')** を使用して、[言語セレクタ（Language Selector）] ドロップダウンリストをページに追加する。複数言語の使用をサポートしない場合、この関数を使用する必要はありません。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （108 ページ）
- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス
- [SSL VPN Customization] ダイアログボックス - [Full Customization]

ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定

ブラウザベースのクライアントレス SSL VPN を設定する場合は、SSL VPN ポータル ページに追加するブックマークまたは URL のリストを定義できます。ブックマーク リストを定義するには、SSL VPN ブックマーク ポリシー オブジェクトを使用します。

IOS デバイスまたは ASA デバイスでホストされる SSL VPN に対する SSL VPN ブックマーク オブジェクトを作成できます。ただし、作成できるブックマーク設定はデバイスタイプによって異なり、ASA デバイスの方が IOS デバイスより多くの設定オプションを設定できます。設定できるオプションが多いほか、ASA デバイスには英語以外、ASCII 文字以外の言語のブックマークも作成できます。ASA デバイスのブックマークおよびポータルのローカライズの詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （112 ページ）を参照してください。

この手順に従って SSL VPN ブックマークオブジェクトを作成したあと、このオブジェクトを使用して、次のポリシーの [ポータルWebページ（Portal Web Pages）] フィールドまたは [ブックマーク（Bookmarks）] フィールドでブックマークオブジェクトを指定できます。

- ASA デバイス：ASA グループ ポリシー オブジェクトの [SSL VPN] > [クライアントレス（Clientless）] ページで（ASA グループ ポリシーの SSL VPN クライアントレス設定を参照）、次のポリシーのいずれかを選択します。
  - **[Remote Access VPN] > [Group Policies]**
  - [全般（General）] タブの [リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]
- ASA デバイス：[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] ポリシーの [メイン（Main）] > [ブックマーク（Bookmarks）] タブで、SSL VPN ブックマークオブジェクトを指定できます（[Main] タブを参照）。
- IOS デバイス：SSL VPN 用に設定されるユーザー グループ ポリシー オブジェクトの [クライアントレス（Clientless）] ページ（[User Group] ダイアログボックス - クライアントレス設定を参照）。このページの [全般（General）] タブの [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] ポリシーで選択します。

関連項目

- グループ ポリシーの作成（ASA、PIX 7.0+） （39 ページ）
- ダイナミック アクセス ポリシーの設定
- 接続プロファイルの設定（ASA、PIX 7.0+） （9 ページ）
- SSL VPN ポリシーの設定（IOS）
- ポリシー オブジェクトの作成
- Policy Object Manager

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（ Policy Object Managerを参照）。

ヒント　SSL VPN ブックマーク オブジェクトは、このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに作成することもできます。詳細については、ポリシーのオブジェクトの選択を参照してください。

ステップ 2 オブジェクトタイプセレクタから [SSL VPNブックマーク（SSL VPN Bookmarks）] を選択します。[SSL VPN Bookmarks] ページが開き、既存の SSL VPN ブックマーク オブジェクトのリストが表示されます。

ステップ 3 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add SSL VPN Bookmark] ダイアログボックスが表示されます（[Add Bookmarks]/[Edit Bookmarks] ダイアログボックスを参照）。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 IOS デバイスでホストされる SSL VPN のオブジェクトを作成する場合は、ブックマークリストの上に表示される見出しの名前を [ブックマークの見出し（IOS）（Bookmarks Heading (IOS))] フィールドで入力できます。

ステップ 6 Bookmarks テーブルに、オブジェクトに定義されたすべての URL が表示されます。ブックマークを追加するには、テーブルの下にある [行の追加（Add Row）] ボタンをクリックします。既存のブックマークを編集するには、ブックマークを選択して [行の編集（Edit Row）] ボタンをクリックします。

[Add/Edit SSL VPN Bookmark Entry] 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のフィールドの詳細については、[ブックマークエントリの追加（Add Bookmark Entry）]/[ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックスを参照してください。

- [ブックマークオプション（Bookmark Option）] フィールドで、ブックマークを定義するか（[ブックマークの入力（Enter Bookmark）]）、別の SSL VPN ブックマークオブジェクトからブックマークを追加するか（[既存のブックマークを含める(Include Existing Bookmarks）]）を選択します。既存のオブジェクトを追加する場合は、オブジェクトの名前を入力するか、または [選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択します。
- IOS デバイスで使用するオブジェクトを作成する場合は、ユーザに表示されるブックマークのタイトルと、URL を入力します。URL には正しいプロトコルを選択するように注意してください。[OK] をクリックして、ブックマークをブックマークテーブルに追加します。
- ASA デバイスで使用するオブジェクトを作成する場合は、さらに多くのオプションがあります。タイトルと URL のほか、ブックマークのサブタイトルとイメージ アイコンおよびその他のオプションを定義できます。

ヒント　プロトコル RDP、SSH、Telnet、VNC、または ICA を選択する場合は、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] ポリシーで、プロトコルのプラグインを設定する必要があります（ SSL VPN ブラウザ プラグインの設定（ASA）（83 ページ）を参照）。

Get 方式ではなく Post 方式を使用するブックマークを設定することもできます。Post を使用する場合は、[Postパラメータ（Post Parameters）] テーブルの下の [行の追加（Add Row）] をクリックして Post パラメータを設定する必要があります。Post パラメータの詳細については、次の項を参照してください。

• SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用 （117 ページ）
• [Add Post Parameter]/[Edit Post Parameter] ダイアログボックス

[OK] をクリックして、ブックマークをブックマークテーブルに追加します。

ステップ 7 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用を参照してください。

ステップ 8 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可を参照してください。

ステップ 9 [OK] をクリックしてオブジェクトを保存します。

SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用

ASA デバイスでホストされる SSL VPN のブックマークを設定する場合には、URL で使用される方式として Get または Post を選択するというオプションがあります。標準の方式は Get 方式であり、この場合、ユーザが URL をクリックすると Web ページに移動します。Post 方式は、データの格納や更新、製品の注文、または電子メールの送信など、データの処理にそのデータの変更が含まれる場合に有効です。

Post URL 方式を選択する場合は、ブックマーク エントリに Post パラメータを設定する必要があります。これらは、ユーザ ID とパスワード、または他の入力パラメータを含む個人別のリソースであることが多く、クライアントレス SSL VPN マクロ置換を定義する必要がある場合があります。

クライアントレス SSL VPN マクロ置換を使用すると、ユーザ ID とパスワード、または他の入力パラメータを含む個人別のリソースにユーザがアクセスできるように設定できます。このようなリソースの例には、ブックマーク エントリ、URL リスト、およびファイル共有などがあります。

（注） セキュリティ上の理由から、パスワード置換はファイル アクセス URL（cifs://）に対してはディセーブルにされています。同様に、セキュリティ上の理由から、Web リンク（特に非 SSL インスタンス）にパスワード置換を導入する場合は注意が必要です。

次のマクロ置換を使用できます。

- ログイン情報置換：セキュリティアプライアンスは、SSL VPN ログインページからこれらの置換のための値を取得します。ユーザ要求内のこれらのストリングを認識し、このストリングをユーザ固有の値で置き換えてから、リモート サーバに要求を渡します。

使用可能なマクロ置換は、次のとおりです。

- CSCO_WEBVPN_USERNAME

SSL VPN へのログインに使用するユーザ名

- CSCO_WEBVPN_PASSWORD

SSL VPN へのログインに使用するパスワード

- CSCO_WEBVPN_INTERNAL_PASSWORD

SSL VPN へのログイン時に入力する内部リソース パスワード

- CSCO_WEBVPN_CONNECTION_PROFILE

SSL VPN へのログイン時に選択されるユーザ グループに関連付けられた接続プロファイル

たとえば、URL リストにリンク http://someserver/homepage/CSCO_WEBVPN_USERNAME.html が含まれている場合、このリンクはセキュリティアプライアンスによって次の一意なリンクに変換されます。

- USER1 の場合、リンクは http://someserver/homepage/USER1.html になります。
- USER2 の場合、リンクは http://someserver/homepage/USER2.html になります。

次の例では、cifs://server/users/CSCO_WEBVPN_USERNAME により、セキュリティアプライアンスでファイル ドライブが特定のユーザにマップされます。

- USER1 の場合、リンクは cifs://server/users/USER1 になります。
- USER2 の場合、リンクは cifs://server/users/USER2 になります。
- RADIUS/LDAP ベンダー固有属性（VSA）：これらの置換を使用すると、RADIUS サーバーまたはLDAP サーバーのいずれかに設定された置換を設定できます。使用可能なマクロ置換は、次のとおりです。
  - CSCO_WEBVPN_MACRO1
  - CSCO_WEBVPN_MACRO2

ブックマークの設定については、ASA デバイスおよび IOS デバイスの SSL VPN ブックマークリストの設定 （115 ページ）を参照してください。

ASA デバイスの SSL VPN スマート トンネルの設定

スマートトンネルは、ユーザーのワークステーションで動作するアプリケーションとプライベートサイト間の接続です。この接続は、セキュリティアプライアンスをパスおよびプロキシサーバとして使用するクライアントレス（ブラウザベース）SSL VPN セッションを使用します。スマート トンネルではユーザのアプリケーションがローカル ポートに接続する必要がないため、ユーザに管理権限を指定することなく、フル トンネル サポートが必要な場合と同様にアプリケーションがネットワークにアクセスできます。ただし、アプリケーションへのアクセスを許可するようにネットワークを設定していない場合は、サポートするアプリケーションのスマート トンネルを作成できます。

アプリケーションへのスマート トンネル アクセスは、次の条件下で設定できます。

- アプリケーションが Winsock 2 の TCP ベースのアプリケーションであり、アプリケーションにブラウザ プラグインが存在する。シスコでは、SSH（SSH セッションおよび Telnet セッション）、RDP、および VNC を含め、クライアントレス SSL VPN で使用するため、一部のアプリケーション向けにプラグインを配布しています。他のアプリケーションについては、プラグインを提供または入手する必要があります。プラグインは、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] ポリシーの [プラグイン（Plug-Ins）] タブで設定します。
- ユーザーのワークステーションは、サポートされているプラットフォームです。サポートされているプラットフォームについては、使用している ASA バージョンに対応する Cisco ASA 5500 シリーズ適応型セキュリティアプライアンスのマニュアル（http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html [英語]）を参照してください。

スマート トンネル（またはポート転送）を使用する Microsoft Windows Vista のユーザは、ASA デバイスの URL を信頼済みサイト ゾーンに追加する必要があります。信頼済みサイトゾーンは、Internet Explorer（[ツール（Tools）] > [インターネットオプション（Internet Options）] の [セキュリティ（Security）] タブ）で設定します。

- ユーザーのブラウザで Java、Microsoft ActiveX、またはその両方をイネーブルにする必要があります。
- ユーザーのワークステーションがセキュリティアプライアンスに接続するためにプロキシサーバーを必要とする場合は、接続の終端側の URL が、プロキシサービスから除外される URL のリストに含まれている必要があります。この設定では、スマート トンネルは基本認証だけをサポートします。

ヒント ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されません。ユーザーはフェールオーバー後に再接続する必要があります。

アプリケーションにスマート トンネル アクセスを設定する場合は、SSL VPN スマート トンネル リスト ポリシー オブジェクトを作成し、このオブジェクトを ASA グループ ポリシー オブジェクトに追加します。次に、[リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）] ポリシーで、ASA グループ ポリシー オブジェクトをデバイスに割り当てます。

関連項目

- グループ ポリシーについて（ASA） （38 ページ）
- ポリシー オブジェクトの作成
- Policy Object Manager

ステップ 1 SSL VPN スマート トンネル リスト ポリシー オブジェクトを作成します。

a) [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開き（Policy Object Managerを参照）、コンテンツテーブルから [SSL VPNスマートトンネルリスト（SSL VPN Smart Tunnel Lists）] を選択します。

ヒント　ASA グループ ポリシー オブジェクトを作成または編集するときに、SSL VPN スマート トンネル リスト オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択を参照してください。

b) [オブジェクトの追加（Add Object）] ボタンをクリックして、[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックスを開きます。

c) オブジェクトの名前を、最大 64 文字で入力します。

d) アプリケーションのテーブルに、スマートトンネルアクセスを付与するアプリケーションを追加します（[行の追加（Add Row）] ボタンをクリックして[Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックスを開きます）。以下の点に注意してください。

- わかりやすいアプリケーション名を入力し、複数のバージョンをサポートする場合はバージョン番号を含めます。たとえば、Microsoft Outlook などと入力します。
- アプリケーション パスの場合、たとえば、outlook.exe などのファイル名だけを入力すると、わかりやすく、メンテナンスも簡単です。このようにすると、ユーザは任意のフォルダにアプリケーションをインストールできます。特定のインストール構造を強制する場合は、フル パスを入力します。
- ハッシュ値はオプションですが、スプーフィングの防止に使用できます。ハッシュ値が設定されていない場合、ユーザはアプリケーションの名前をサポートされているファイル名に変更できます。この場合、セキュリティ アプライアンスはファイル名とパスだけをチェックします（指定された場合）。ただし、ハッシュ値を入力すると、ユーザがパッチを適用するとき、またはアプリケーションをアップグレードするときにそのハッシュ値を保守する必要があります。ハッシュ値の決定の詳細については、[Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックスを参照してください。

[OK] をクリックしてエントリを保存します。

e) 他の SSL VPN スマート リスト オブジェクトをこのオブジェクトに組み込むこともできます。このようにすると、核となるスマートリストオブジェクトセットを作成し、他のオブジェクトで繰り返し使用できます。

f) [OK] をクリックしてオブジェクトを保存します。

ステップ 2　（任意）SSL VPN スマート トンネル自動サインオン リスト ポリシー オブジェクトを作成します。

a) [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開き（Policy Object Managerを参照）、コンテンツテーブルから [SSL VPNスマートトンネル自動サインオンリスト（SSL VPN Smart Tunnel Auto Signon Lists）] を選択します。

ヒント　ASA グループ ポリシー オブジェクトを作成または編集するときに、SSL VPN スマート トンネル自動サインオン リスト オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択を参照してください。

b) [オブジェクトの追加（Add Object）] ボタンをクリックして、[Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックスを開きます。

c) オブジェクトの名前を、最大 64 文字で入力します。
d) スマートトンネル自動サインオンエントリのテーブルに、スマートトンネル設定中のログイン情報の発行を自動化するサーバーを追加します（[行の追加（Add Row）] ボタンをクリックして[Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックスを開きます）。
e) 他の SSL VPN スマート トンネル自動サインオン リスト オブジェクトをこのオブジェクトに組み込むこともできます。このようにすると、核となるスマートトンネル自動サインオン リストオブジェクトセットを作成し、他のオブジェクトで繰り返し使用できます。
f) [OK] をクリックしてオブジェクトを保存します。

ステップ 3 SSL VPN スマート トンネル リスト オブジェクトを使用するための ASA グループ ポリシー オブジェクトを設定します。

a) Policy Object Managerまたは [リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）] ポリシーから、ASA グループ ポリシー オブジェクトを編集（または作成）します。このオブジェクトは、SSL VPN をサポートするように設定する必要があります（これらのオブジェクトは、[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）] ポリシーの個々のプロファイルから編集することもできます）。
b) コンテンツテーブルから [SSL VPN] > [クライアントレス（Clientless）] フォルダを選択してASA グループ ポリシーの SSL VPN クライアントレス設定を開きます。
c) [スマートトンネル（Smart Tunnel）] フィールドに SSL VPN スマート トンネル リスト オブジェクトの名前を入力します。
d) [スマートトンネルの自動開始（Auto Start Smart Tunnel）] を選択して、ユーザーが SSL VPN ポータルに接続したときに、アプリケーションのスマートトンネルが自動的に開始されるようにします。

   このオプションを選択しない場合、ユーザーはクライアントレス SSL VPN ポータルページで [アプリケーションアクセス（Application Access）] > [スマートトンネルの開始（Start Smart Tunnels）] ボタンを使用して、スマートトンネルアクセスを開始する必要があります。

e) [スマートトンネル自動サインオンサーバーリスト（Smart Tunnel Auto Signon Server List）] フィールドに SSL VPN スマートトンネル自動サインオン リスト オブジェクトの名前を入力します。
f) 汎用命名規則（ドメイン\ユーザー名）が認証に必要な場合、Windows ドメインを指定して、[ドメイン名（Domain Name）] フィールドの自動サインオン中のユーザー名に追加します。たとえば、ユーザ名 qa_team の認証を行う場合、CISCO と入力して CISCO\qa_team を指定します。自動サインオン サーバ リストで関連エントリを設定する場合は、[Use Domain] オプションも選択する必要があります。

WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

クライアントレス SSL VPN では、WINS および Common Internet File System（CIFS）プロトコルを使用して、リモート システム上のファイル、プリンタ、および他のマシン リソースにアクセス、またはこれらを共有します。ASA デバイスまたは IOS デバイスは、プロキシ CIFS クライアントを使用して、このアクセスを透過的に提供します。このため、ユーザには（個々のファイルおよびユーザの権限に従って）ファイル システムに直接アクセスしているように見えます。

ユーザがコンピュータ名を使用して Windows コンピュータへのファイル共有接続を試みる場合、ユーザが指定するファイル サーバは、ネットワーク上のリソースを識別する特定の WINS 名に対応します。セキュリティ アプライアンスは WINS サーバまたは NetBIOS ネーム サーバにクエリーを行い、WINS 名を IP アドレスにマップします。SSL VPN は NetBIOS に再クエリーを行い、リモート システム上のファイルにアクセス、またはファイルを共有します。

これらの Microsoft のファイルおよびディレクトリ共有名の解決に使用される WINS サーバのリストを設定するには、WINS サーバ リスト ポリシー オブジェクトを使用します。WINS サーバーリストオブジェクトでは、Common Internet File System（CIFS）の名前解決に、（**nbns-list** コマンドおよび **nbns-server** コマンドを使用して）デバイスの NetBIOS Name Service（NBNS）サーバーを定義します。

WINS サーバ リスト ポリシー オブジェクトを作成したあと、次のポリシーおよびポリシー オブジェクト内で、このポリシー オブジェクトを設定できます。また、許可するファイル アクセス サービスを選択することもできます。

- ASA デバイス：**[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]** ポリシーで、[SSL] タブの WINS サーバーリストオブジェクトを指定します（[SSL] タブ（[Connection Profiles]） （30 ページ）を参照）。

ASA グループ ポリシー オブジェクトの **[SSL VPN] > [クライアントレス（Clientless）]** ページでファイルアクセスオプションを選択し（ASA グループ ポリシーの SSL VPN クライアントレス設定を参照）、次のポリシーのいずれかを選択します。

- **[リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）]**
- [全般（General）] タブの **[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]**
- IOS デバイス：SSL VPN 用に設定されるユーザー グループ ポリシー オブジェクトの [クライアントレス（Clientless）] ページ（[User Group] ダイアログボックス - クライアントレス設定を参照）。このページの [全般（General）] タブの [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] ポリシーで選択します。

関連項目

- ポリシー オブジェクトの作成

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、Policy Object Managerを開きます。

ヒント　WINS サーバ リスト オブジェクトは、このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに作成することもできます。詳細については、ポリシーのオブジェクトの選択を参照してください。

ステップ 2　オブジェクトタイプセレクタから [WINSサーバーリスト（WINS Server Lists）] を選択します。

[WINS Server List] ページが開き、現在定義されている WINS サーバ リスト オブジェクトが表示されます。

ステップ 3　作業領域を右クリックし、[新規オブジェクト（New Object）] を選択して [Add WINS Server List]/[Edit WINS Server List] ダイアログボックスを開きます。

ステップ 4　オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5　テーブルの下にある [行を追加（Add Row）] ボタンをクリックするか、またはテーブル内のサーバーを選択して [行を編集（Edit Row）] をクリックし、オブジェクトに定義された WINS サーバーを設定します。設定する項目は次のとおりです。

- [サーバー（Server）]：WINS サーバーの IP アドレス。ネットワーク/ホスト オブジェクトを選択するか、またはアドレスを直接入力できます。
- [プライマリブラウザとして設定（Set as Primary Browser）]：サーバーがプライマリブラウザの場合にこのオプションを選択します。プライマリブラウザは、コンピュータおよび共有リソースのリストを保持します。

他のフィールドはオプションです。デフォルト値以外の値が必要な場合は、これらのフィールドを変更してください。詳細については、[Add WINS Server]/[Edit WINS Server] ダイアログボックスを参照してください。

[OK] をクリックして変更を保存します。

ステップ 6　（任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用を参照してください。

ステップ 7　（任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可を参照してください。

ステップ 8　[OK] をクリックしてオブジェクトを保存します。

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。