IKE および IPsec ポリシーの設定

この章では、インターネットプロトコルセキュリティ（IPSec）および Internet Security Association and Key Management Protocol（ISAKMP または IKE）標準を設定して、サイト間およびリモートアクセス IPsec バーチャルプライベートネットワーク（VPN）を構築する方法について説明します。これらのポリシーは、VPN トンネルを構築するために通常の IPsec および他のタイプの IPsec ベースの VPN テクノロジーで使用されます。

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモートユーザーとプライベートな企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

IPsec ベースの VPN テクノロジーは、ISAKMP および IPsec トンネリング標準を使用して、トンネルの構築と管理を行います。ISAKMP と IPsec は、次を実現します。

- トンネル パラメータのネゴシエート。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネルを経由するデータ転送の管理。
- トンネルエンドポイントまたはルータとしてのインバウンドおよびアウトバウンドのデータ転送の管理。

VPN 内のデバイスは、双方向トンネル エンドポイントとして機能します。プライベートネットワークからプレーンパケットを受信し、それらをカプセル化して、トンネルを作成し、それらをトンネルの他端に送信できます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリック ネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベート ネットワーク上の最終宛先に送信することもできます。

ここでは、基本的な IKE および IPsec ポリシーと、その設定方法について説明します。

- IKE および IPsec 設定の概要　（2 ページ）
- IKE について　（6 ページ）

- IPsec プロポーザルについて （26 ページ）
- VPN グローバル設定 （44 ページ）
- サイト間 VPN での IKEv1 事前共有キー ポリシーについて （65 ページ）
- Public Key Infrastructure ポリシーについて （71 ページ）
- サイト間 VPN での IKEv2 認証の設定 （94 ページ）

IKE および IPsec 設定の概要

インターネット キー エクスチェンジ（IKE）は、IPsec ピアを認証し、IPsec 暗号化キーをネゴシエートして配信し、IPsec セキュリティ アソシエーション（SA）を自動的に確立するために使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE プロポーザルは、2 つのピア間の IKE ネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。IKE Version 1（IKEv1; IKE バージョン 1）では、IKE プロポーザルには、単一のアルゴリズム セットと係数グループが含まれています。各ピアにおいて、複数のポリシーをプライオリティ付きで作成して、少なくとも 1 つのポリシーがリモートピアのポリシーに一致するようにできます。IKEv1 と異なり、IKEv2 プロポーザルでは、フェーズ 1 ネゴシエーション中にピアが選択できる複数のアルゴリズムと係数グループを選択できます。これによって、単一の IKE プロポーザルの作成が可能になります（ただし、最も望ましいオプションにより高いプライオリティを設定するために、異なるプロポーザルが必要になる可能性があります）。1 つの VPN あたり複数の IKE プロポーザルを定義できます。

サイト間またはリモート アクセス VPN で通常の IPsec 接続を正常に確立するために必要な設定を定義するよう、いくつかのポリシーを設定する必要があります。次の手順には、設定を行うために必要な手順の概要が示されており、各手順の詳細情報が記載された他のトピックのリンクがあります。

関連項目

- IKE について （6 ページ）
- IPsec プロポーザルについて （26 ページ）
- サイト間 VPN での IKEv1 事前共有キー ポリシーについて （65 ページ）
- Public Key Infrastructure ポリシーについて （71 ページ）

ステップ 1 [IKEプロポーザル（IKE Proposal）] ポリシーを設定します。

[IKE Proposal] ポリシーでは、VPN 接続の確立に使用する IKE プロポーザル ポリシー オブジェクトを定義します。IKE プロポーザル オブジェクトの定義時に、IKE ネゴシエーションの暗号化と完全性チェックに使用するアルゴリズムと、暗号化アルゴリズムの実行に使用するデフィーヘルマン グループを選択します。IKEv1 では、事前共有キーまたは公開キー インフラストラクチャのいずれを使用するかも判別しますが、IKEv2 では、IKE プロポーザルには、認証モードの指定は含まれていません。

ここでは、[IKE Proposal] ポリシーの設定方法について説明します。

- IKE プロポーザルの設定 （12 ページ）
  - [IKEv1 Proposal] ポリシー オブジェクトの設定 （14 ページ）
  - [IKEv2 Proposal] ポリシー オブジェクトの設定 （19 ページ）
- GET VPN の IKE プロポーザルの設定

ステップ 2 認証モード設定を行います。

IKEv1 プロポーザルで認証モードに選択した項目、および IKEv2 に使用するよう決定したモードによって、認証モード設定を行うために必要な他のポリシーが制御されます。

- 事前共有キー：リモートアクセス IKEv1 IPsec VPN の場合は、[接続プロファイル（Connection Profiles）] ポリシーで事前共有キーを定義します。事前共有キーは、リモートアクセス VPN の IKEv2 ではサポートされません。サイト間 VPN の場合は、使用している IKE バージョンに基づいて [IKEv1事前共有キー（IKEv1 Preshared Keys）] または [IKEv2認証（IKEv2 Authentication）] ポリシーでキーを定義します。

ここでは、事前共有キー設定について説明します。

- [IPSec] タブ（[Connection Profiles]）
- IKEv1 事前共有キー ポリシーの設定 （67 ページ）
- サイト間 VPN での IKEv2 認証の設定 （94 ページ）
- 公開キーインフラストラクチャ認証局サーバー：Certificate Authority（CA; 認証局）サーバーを使用するよう IKE を設定する場合は、[公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーを設定する必要があります。また、このポリシーを使用して、SSL VPN の公開キー インフラストラクチャを定義します。サイト間 VPN の場合は、使用している IKE バージョンに基づいて、ポリシーは [IKEv1公開キーインフラストラクチャ（IKEv1 Public Key Infrastructure）] または [IKEv2認証（IKEv2 Authentication）] です。

[Public Key Infrastructure] ポリシーは、認証局サーバを識別する PKI 登録オブジェクトを特定します。サイト間 VPN の場合は、単一の PKI 登録オブジェクトを選択できます。リモート アクセス VPN の場合は、リモート アクセス接続に必要なすべてのオブジェクトを選択できます。これらのトラストポイントは、（[IPsec] タブにある）リモートアクセスの [接続プロファイル（Connection Profiles）] ポリシーで識別されます。

ここでは、公開キー インフラストラクチャ設定について説明します。

- Public Key Infrastructure ポリシーについて （71 ページ）
- サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （75 ページ）

- サイト間 VPN での複数の IKEv1 CA サーバの定義 （77 ページ）
- 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 （79 ページ）
- [IPSec] タブ（[Connection Profiles]）
- サイト間 VPN での IKEv2 認証の設定 （94 ページ）

ステップ 3 [IPsecプロポーザル（IPsec Proposal）] ポリシーを設定します。[IPsec Proposal] ポリシーは、VPN のセキュアな IPsec トンネルを作成するために使用される IPsec トランスフォーム セット ポリシー オブジェクトを定義します。

ここでは、[IPsec Proposal] ポリシーの設定方法について説明します。

- サイト間 VPN での IPsec プロポーザルの設定 （31 ページ）
  - サイト間 VPN におけるデバイスの IKE バージョンの選択 （36 ページ）
  - 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 （37 ページ）
- Easy VPN での IPsec プロポーザルの設定
- 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）
- 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）

ステップ 4 [グローバル設定（Global Settings）] ポリシーを設定します。

[グローバル設定（Global Settings）]（リモートアクセス）ポリシーおよび[VPNグローバル設定（VPN Global Settings）]（サイト間）ポリシーは、さまざまな ISAKMP、IKEv1、IKEv2、IPsec、NAT、フラグメンテーション、およびその他の設定を定義します。これらの設定には、多くの場合適切であるデフォルト値があるため、通常はデフォルト以外の動作が必要なときにかぎり [Global Settings] ポリシーを設定する必要があります。ただし、リモートアクセス IKEv2 IPsec VPN ではポリシーを設定する必要があります。これは、[IKEv2設定（IKEv2 Settings）] タブでリモート アクセス グローバル トラストポイントを指定する必要があるためです。

ここでは、[Global Settings] ポリシーの設定方法について説明します。

- VPN グローバル設定 （44 ページ）
  - VPN グローバル ISAKMP/IPsec 設定 （47 ページ）
  - VPN グローバル IKEv2 設定 （53 ページ）
  - VPN グローバル NAT 設定 （59 ページ）
  - VPN グローバル一般設定 （61 ページ）
- GET VPN のグローバル設定

ステップ 5 リモート アクセス IKEv2 IPsec VPN を設定する場合は、SSL VPN のいくつかのポリシーも設定する必要があります。IKEv2 は、SSL VPN といくつかの設定を共有します。設定する必要があるその他のポリシーに

ついては、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）を参照してください。

IKE バージョン 1 と 2 の比較

IKE には、バージョン 1（IKEv1）とバージョン 2（IKEv2）の 2 つのバージョンがあります。IKEv2 をサポートするデバイスで IKE を設定する場合は、いずれかのバージョンを単独で設定するか、両方のバージョンを一緒に設定するかを選択できます。デバイスが別のピアとの接続のネゴシエーションを試行する場合は、ユーザが許可したバージョンか、他のピアが受け入れるバージョンのどちらでも使用されます。両方のバージョンを許可すると、最初に選択したバージョン（IKEv2 は、設定されている場合は常に最初に試行されます）とのネゴシエーションが正常に行われなかった場合に、デバイスは他のバージョンに自動的にフォールバックします。ネゴシエーションで使用するには、両方のピアが IKEv2 をサポートする必要があります。

ヒント Security Manager は、ASA 8.4(1)+ だけで IKEv2 をサポートします。リモート アクセス IPsec VPN では、ユーザは AnyConnect 3.0+ クライアントを使用して、IKEv2 接続を実行する必要があり、IKEv2 接続は、SSL VPN 接続に使用される同じライセンス プールを使用します。ASA での IKEv1 リモート アクセス接続には従来の VPN クライアントが使用されます。VPN でのデバイス サポートの詳細については、各 IPsec テクノロジーでサポートされるデバイスについてを参照してください。

IKEv2 は、次の方法で IKEv1 とは異なります。

- IKEv2 は、Photuris スタイルのクッキー メカニズムを修正します。
- IKEv2 では、IKEv1 よりも少ないラウンドトリップが行われます（基本的な交換では、IKEv1 の場合の 5 回に対して 2 回のラウンドトリップ）。
- トランスフォームオプションは論理和演算されます。これは、許可される組み合わせごとに別個の固有のプロポーザルを作成するのではなく、単一のプロポーザルで複数のオプションを指定できることを意味します。
- 組み込みの Dead Peer Detection（DPD; デッドピア検知）。
- 組み込みの設定ペイロードとユーザ認証モード。
- 組み込みの NAT Traversal（NAT-T; NAT 通過）。IKEv2 は、NAT-T にポート 500 と 4500 を使用します。
- 向上したキーの再生成とコリジョン処理。
- 単一の Security Association（SA; セキュリティ アソシエーション）は複数のサブネットを保護でき、これによってスケーラビリティが向上します。
- サイト間 VPN での非対称認証。トンネルのそれぞれの側に、異なる事前共有キーと異なる証明書を設定するか、片側にキー、もう片側に証明書を設定できます。

- リモート アクセス IPsec VPN では、リモート アクセス SSL VPN に対して設定する場合と同じ方法で IKEv2 接続に二重認証を設定できます。IKEv1 は二重認証をサポートしません。

関連項目

- IKE および IPsec 設定の概要 （2 ページ）
- IKE プロポーザルの設定 （12 ページ）

IKE について

Internet Key Exchange（IKE; インターネット キー交換）は、Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれ、2 つのホストが IPsec Security Association（SA; セキュリティ アソシエーション）の構築方法に合意するためのネゴシエーション プロトコルです。これは、SA 属性のフォーマットに合意するための共通のフレームワークを提供します。これには、SA に関するピアとのネゴシエーション、および SA の変更または削除が含まれます。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 セキュリティ アソシエーションの自動確立に使用される暗号キーを作成します。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートして、ピアがフェーズ 2 で安全に通信できるようにする最初のトンネルを作成し、その後の ISAKMP ネゴシエーション メッセージを保護します。フェーズ 2 のネゴシエーション中に、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。これによって、ピア間で送信されるデータが保護されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE プロポーザルは、2 つのピア間の IKE ネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。リモートアクセス IPsec VPN では、VPN ごとに複数の IKE プロポーザルを定義し、各ピアでポリシーに優先順位を付けて、少なくとも 1 つのポリシーがリモートピアのポリシーと一致するようにできます。サイト間 VPN では、単一の IKE プロポーザルを作成できます。

IKE プロポーザルを定義するには、次の内容を指定する必要があります。

- 一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。
- データを保護し、プライバシーを確保するための IKE ネゴシエーションの暗号化方式。使用する暗号化アルゴリズムの決定 （7 ページ）を参照してください。
- 送信者の ID を保証し、メッセージが伝送中に変更されないようにするためのハッシュメッセージ認証コード（HMAC）方式（IKEv2 では整合性アルゴリズムと呼ばれる）。使用するハッシュ アルゴリズムの決定 （8 ページ）を参照してください。
- IKEv2 では、別個の Pseudo-Random Function（PRF; 疑似乱数関数）をアルゴリズムとして使用して、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得していま

した。オプションは、ハッシュ アルゴリズムに使用されるものと同じです。使用するハッシュ アルゴリズムの決定 （8 ページ）を参照してください。

- 暗号化キー判別アルゴリズムの強度を決定する Diffie-Hellman グループ。デバイスは、このアルゴリズムを使用して、暗号化キーとハッシュ キーを派生させます。使用する Diffie-Hellman 係数グループの決定 （9 ページ）を参照してください。
- ピアの ID を確認する認証方式。使用する認証方式の決定 （11 ページ）を参照してください。
- デバイスが暗号化キーを交換するまでに使用できる時間制限。

（注） [IKEv2 Proposal] ポリシー オブジェクトの設定 （19 ページ）

ヒント （ASA デバイスのみ）。IKEv1 ポリシーを使用して、パラメータごとに 1 つの値を設定します。IKEv2 では、複数の暗号化、整合性、PRF、およびデフィーヘルマン オプションを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。

ピアが、暗号化、ハッシュ（IKEv2 の場合は整合性と PRF）、認証、Diffie-Hellman 値を保持し、さらに、送信されたポリシーのライフタイム以下である SA ライフタイムを保持している場合に、IKE ポリシー間に一致が存在します。ライフタイムが等しくない場合は、（リモート ピア ポリシーからの）短い方のライフタイムが適用されます。一致するポリシーがない場合、IKE はネゴシエーションを拒否し、IKE SA は確立されません。

ここでは、IKE プロポーザルの設定方法について説明します。

- IKE プロポーザルの設定 （12 ページ）
- [IKEv1 Proposal] ポリシー オブジェクトの設定 （14 ページ）
- [IKEv2 Proposal] ポリシー オブジェクトの設定 （19 ページ）
- GET VPN の IKE プロポーザルの設定

使用する暗号化アルゴリズムの決定

IKE プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。

次の暗号化アルゴリズムから選択できます。

- Data Encryption Standard（DES; データ暗号規格）は、対称秘密キー ブロック アルゴリズムです。3DES よりも高速であり、使用するシステム リソースも少ないですが、安全性も劣ります。堅牢なデータ機密保持が必要ない場合、およびシステム リソースや速度が重要である場合には、DES を選択します。
- 3DES（トリプル DES）では、毎回異なるキーを使用して各データ ブロックを 3 回処理するため、より安全です。ただし、使用するシステム リソースが多くなり、DES よりも速度が遅くなります。デバイスでサポートされている場合には、3DES 暗号化アルゴリズムを使用することを推奨します。

（注） DES および 3DES 暗号化アルゴリズムは、もはや最新の脅威に対してセキュアではありません。そのため、Cisco Security Manager 4.22 では、ASA 9.15(1) 以降のバージョンのデバイスに対する IKEv1 および IKEv2 プロポーザルのサポートが終了されました。

- AES（Advanced Encryption Standard）は DES よりも安全であり、3DES よりも効率的に計算できます。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。ルータで IKE を設定するには、AES を使用するために Cisco IOS ソフトウェア 12.3T 以降をルータで使用する必要があります。

（注） AES は、ハードウェア暗号化カードとともに使用することはできません。

関連項目

- IKE について （6 ページ）
- IKE プロポーザルの設定 （12 ページ）

使用するハッシュ アルゴリズムの決定

選択可能なハッシュ アルゴリズムは、次のとおりです。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプションに分かれています。1 つは整合性アルゴリズムに使用され、もう 1 つは擬似乱数関数（PRF）に使用されます。

- Secure Hash Algorithm（SHA; セキュア ハッシュ アルゴリズム）には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。ただし、SHA は MD5 よりもリソース消費量が大きくなります。最大レベルのセキュリティを必要とする実装には、SHA ハッシュ アルゴリズムを使用してください。

標準の SHA では、160 ビットのダイジェストが生成されます。

よりセキュアな次のオプションは、ASA 8.4(2+) デバイスの IKEv2 設定で使用できます。

- SHA512：512 ビット キー
- SHA384：384 ビット キー
- SHA256：256 ビット キー
- MD5（Message Digest 5）では、128 ビットのダイジェストが生成され、SHA よりも処理時間が短く、全体的に高いパフォーマンスを発揮しますが、SHA よりもセキュリティ面で弱くなります。

（注） Cisco Security Manager 4.22 で、ASA 9.15(1) 以降のバージョンのデバイスに対する、 IKEv1 および IKEv2 の両方のプロポーザルの MD5 ハッシュアルゴリズムのサポートを終了します。これらは最新の脅威に対して安全であると見なされなくなったためです。

関連項目

- IKE について （6 ページ）
- IKE プロポーザルの設定 （12 ページ）

使用する Diffie-Hellman 係数グループの決定

Security Manager では、IPsec Security Association（SA; セキュリティ アソシエーション）キーを生成するための次のデフィーヘルマン キー導出アルゴリズムがサポートされています。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。両方のピアに、一致する係数グループが存在する必要があります。

ヒント AES 暗号化を選択する場合は、AES で必要な大きいキーサイズをサポートするために、ISAKMP ネゴシエーションで Diffie-Hellman（DH）グループ 5 以降を使用する必要があります。IKEv1 の場合、ASA デバイスはグループ 2 と 5 のみをサポートします。

- Diffie-Hellman グループ 1：768 ビットの係数。768 ビットの素数およびジェネレータ数を使用して IPsec SA キーを生成する場合に使用します。

（注） Cisco Security Manager 4.19 以降、IKEv1 および IKEv2 の DH グループ 1 は、ASA 9.12(1) 以降のデバイスではサポートされません。

- Diffie-Hellman グループ 2：1024 ビットの係数。1024 ビットの素数およびジェネレータ数を使用して IPsec SA キーを生成する場合に使用します。Cisco VPN Client バージョン 3.x 以降では、少なくともグループ 2 が必要です
- Diffie-Hellman グループ 5：1536 ビットの係数。2048 ビットの素数およびジェネレータ数を使用して IPsec SA キーを生成する場合に使用します。128 ビットのキーでは十分な保護レベルですが、グループ 14 の方がより安全です。
- デフィーヘルマン グループ 7：163 文字の楕円曲線フィールド サイズを使用して IPsec SA キーを生成する場合に使用します。グループ 7 は、VPNSM または VPN SPA が設定された Catalyst 6500/7600 デバイスではサポートされていません。
- Diffie-Hellman グループ 14：2048 ビットの係数。128 ビットのキーでは十分な保護レベルです。（ASA 9.0.1 以降のデバイスのみ）。

（注） Cisco Security Manager 4.20 以降では、DH グループ 14 がサポートされており、これが ASA 9.13(1) 以降のデバイスにおける IKEv1 および IKEv2 のデフォルト DH グループです。

- Diffie-Hellman 15：3072 ビットの係数。192 ビットのキーでは十分な保護レベルです。
- Diffie-Hellman グループ 16：4096 ビットの係数。256 ビットのキーでは十分な保護レベルです。

（注） Cisco Security Manager 4.20 以降、DH グループ 15 および 16 は、ASA 9.13(1) 以降のデバイスの IKEv2 でサポートされています。

- Diffie-Hellman グループ 19：（256 ビットの楕円曲線フィールドサイズ）。（ASA 9.0.1 以降のデバイスのみ）。
- Diffie-Hellman グループ 20：（384 ビットの楕円曲線フィールドサイズ）。（ASA 9.0.1 以降のデバイスのみ）。
- Diffie-Hellman グループ 21：（521 ビットの楕円曲線フィールドサイズ）。（ASA 9.0.1 以降のデバイスのみ）。
- Diffie-Hellman グループ 24：（2048 ビット係数および 256 ビット素数位数サブグループ）。（ASA 9.0.1 以降のデバイスのみ）。
- Diffie-Hellman グループ 31：（256 ビットの楕円曲線フィールドサイズ）。（ASA 9.16.1 以降のデバイスのみ）。

（注） Cisco Security Manager 4.22 で、ASA 9.15(1) 以降のバージョンのデバイスに対する、IKEv2 プロポーザルの DH グループ 2 および 24 と IKEv1 の DH グループ 2 のサポートを終了します。これらは最新の脅威に対して安全であると見なされなくなったためです。

（注） Cisco Security Manager 4.23 以降、DH グループ 31 は、ASA 9.16(1) 以降のデバイスの IPsec プロファイルおよび IKEv2 でサポートされます。

関連項目

- IKE について （6 ページ）
- IKE プロポーザルの設定 （12 ページ）

使用する認証方式の決定

Security Manager では、VPN 通信でのピア デバイス認証において 2 つの方式がサポートされています。

- [事前共有キー（Preshared Key）]：事前共有キーを使用すると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。各ピアに同じ共有キーを設定する必要があります。同じキーが設定されていない場合は、IKE SA を確立できません。

このデバイス認証方式を使用して IKE を正常に使用するには、さまざまな事前共有キー パラメータを定義する必要があります。詳細については、次の適切なトピックを参照してください。

- サイト間 VPN、IKEv1 設定： IKEv1 事前共有キー ポリシーの設定 （67 ページ）を参照してください。
- サイト間 VPN、IKEv2 設定： サイト間 VPN での IKEv2 認証の設定 （94 ページ）を参照してください。
- リモート アクセス IPsec VPN、IKEv1：接続プロファイルの [IPsec] タブで設定されています。[IPSec] タブ（[Connection Profiles]）を参照してください。
- リモート アクセス IPsec VPN、IKEv2：リモート アクセス IPSec VPN で IKEv2 を使用する場合は、事前共有キーを使用できません。証明書を使用する必要があります。
- **証明書**：IKE キー管理メッセージを署名および暗号化するために、RSA キーペアが使用される認証方式。証明書によって、2 つのピア間の通信の否認防止を実施します。つまり、実際に通信が行われたことを証明できます。この認証方式を使用する場合は、Certification

Authority（CA; 認証局）からデジタル証明書を取得するようにピアを設定します。CA は、証明書要求を管理して、参加する IPsec ネットワーク デバイスに証明書を発行します。これらのサービスは、参加デバイスのキー管理を一元化して行います。

事前共有キーを使用した場合のスケーラビリティは高くありませんが、CA を使用することによって、IPsec ネットワークを容易に管理できるようになり、スケーラビリティが高まります。CA を使用する場合は、すべての暗号化デバイス間でキーを設定する必要がありません。代わりに、参加する各デバイスは CA に登録され、CA に対して証明書を要求します。自身の証明書と CA の公開キーを持つ各デバイスは、その CA のドメイン内にある他のすべてのデバイスを認証できます。

証明書認証方式を使用して IKE を正常に使用するには、CA 認証および登録用のパラメータを定義する必要があります。詳細については、次の適切なトピックを参照してください。

- サイト間 VPN、IKEv1 設定： Public Key Infrastructure ポリシーについて （71 ページ）を参照してください。
- サイト間 VPN、IKEv2 設定： サイト間 VPN での IKEv2 認証の設定 （94 ページ）。
- リモート アクセス IPsec VPN、IKEv1：[IPSec] タブ（[Connection Profiles]）で説明されているように、接続プロファイルの [IPsec] タブで設定されています。同じトラストポイントを使用して、公開キー インフラストラクチャ ポリシーも設定する必要があります。Public Key Infrastructure ポリシーについて （71 ページ）を参照してください。
- リモート アクセス IPsec VPN、IKEv2： VPN グローバル IKEv2 設定 （53 ページ）で説明されているように、[Global Settings] ポリシーの [IKEv2 Settings] タブでグローバル トラストポイントを設定します。同じトラストポイントを使用して、公開キーインフラストラクチャ ポリシーも設定する必要があります。 Public Key Infrastructure ポリシーについて （71 ページ）を参照してください。

関連項目

- IKE について （6 ページ）
- IKE プロポーザルの設定 （12 ページ）

IKE プロポーザルの設定

Security Manager では、サイト間またはリモート アクセス IPsec VPN を設定する場合は、IKE プロポーザルは必須ポリシーです。設定ウィザードを使用して、新しい IPsec VPN を作成する場合は、[IKE Proposal] ポリシーは VPN に自動的に割り当てられます。ポリシーは出荷時のデフォルトであるか、VPN 専用に選択された共有ポリシーです。Internet Key Exchange（IKE; インターネット キー交換）キー管理プロトコルの詳細については、 IKE について （6 ページ）を参照してください。

[IKE Proposal] ポリシーを使用して、現在の IKE プロポーザルを調べて、GET VPN トポロジを除く新しいプロポーザルを設定します。GET VPN については、GET VPN の IKE プロポーザルの設定を参照してください。

（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 IKE プロポーザルポリシーを設定および展開できます。

ヒント

- サイト間 VPN では、IKE バージョンごとに最大 1 つの IKE プロポーザルを選択できます。リモート アクセス IPsec VPN では、IKE バージョンごとに複数のプロポーザルを選択できます。リモート アクセス VPN で許可されるすべての IKE プロポーザルを選択します。
- IKEv2（バージョン 2）を設定するには、デバイスは、ASA ソフトウェアリリース 8.4(1) 以降が実行されている ASA である必要があります。
- [IPsec Proposal] ポリシーでは、IKEv1、IKEv2、または両方が、このポリシーで設定する IKE プロポーザルと一致する必要があります。IPsec プロポーザルで IKEv2 を設定できない場合は、Easy VPN トポロジなどでは IKEv2 はサポートされません。詳細については、IPsec プロポーザルについて （26 ページ）を参照してください。
- [IKEv1 Proposal] オブジェクトでは、認証に事前共有キーと証明書のいずれを使用するのかを指定します。IKEv1 プロポーザルオブジェクトが証明書認証タイプの場合は、IKEv1 公開キー インフラストラクチャ ポリシーで適切な CA サーバーを（ポリシーセレクタから）指定していることを確認します。事前共有キーの場合、IKEv1 事前共有キーポリシーが割り当てられていることを確認します。IKEv2 では、オブジェクトでは、事前共有キーまたは証明書のいずれを使用するのかは指定しませんが、他のポリシーでは認証要件を定義する必要があります。詳細については、使用する認証方式の決定 （11 ページ）を参照してください。
- 通常の IPSec VTI テクノロジーの場合、IKE プロポーザルの 1 つ（IKEv1 プロポーザルまたは IKEv2 プロポーザル）のみを指定できます。つまり、（[IKEプロポーザル（IKE Proposal）] ウィンドウで）通常の IPSec VTI に IKE バージョン 1 を選択した場合、[IKEv1 プロポーザル（IKEv1 Proposal）] を指定し、[IKEv2プロポーザル（IKEv2 Proposal）] フィールドを空白のままにしておく必要があり、その逆も同様です。

関連項目

- 使用するハッシュ アルゴリズムの決定 （8 ページ）
- 使用する Diffie-Hellman 係数グループの決定 （9 ページ）
- 使用する認証方式の決定 （11 ページ）

ステップ 1 設定する VPN のタイプに基づいて [IKE Proposal] ポリシーを開くには、次のいずれかを実行します。

- リモート アクセス VPN の場合は、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）] > [IPSec VPN] > [IKEプロポーザル（IKE Proposal）]** 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] > [IKEプロポーザル（IKE Proposal）]** 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。

- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウを開き、VPN セレクタでトポロジ（GET VPN 以外）を選択して、ポリシーセレクタで [IKEプロポーザル（IKE Proposal）] を選択します。
  - （ポリシービュー）ポリシータイプセレクタで **[サイト間VPN（Site-to-Site VPN）] > [IKEプロポーザル（IKE Proposal）]** を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

ステップ 2 適切な IKE バージョンに対して [選択（Select）] をクリックして、IKE バージョン 1 またはバージョン 2 プロポーザルの設定を定義するポリシーオブジェクトを選択します。VPN でサポートされる IKE バージョンのプロポーザルだけを設定します。

（注） 4.16 以降、Cisco Security Manager は分散モードの Firepower 9300 デバイスの IKEv1 設定をサポートしていません。

- サイト間 VPN の IKE プロポーザルを選択するには、使用可能なプロポーザル リストで単に強調表示します。リモートアクセス IPsec VPN では、使用可能なプロポーザルリストで必要なオブジェクトを強調表示して、[>>] をクリックして選択したプロポーザルリストに移動します。
- リモートアクセス IPsec VPN の IKE プロポーザルを削除するには、選択したプロポーザルリストで強調表示し、[<<] をクリックして使用可能なプロポーザルリストに移動します。
- 新しい IKE プロポーザルを作成するには、使用可能なプロポーザルリストの下にある [作成（Create）]（+）ボタンをクリックします。[Add IKEv1 or IKEv2 Proposal] ダイアログボックスが開きます。オブジェクトの作成手順については、次のトピックを参照してください。
  - [IKEv1 Proposal] ポリシー オブジェクトの設定 （14 ページ）
  - [IKEv2 Proposal] ポリシー オブジェクトの設定 （19 ページ）
- オブジェクトを編集するか、オブジェクトの設定を表示するには、そのオブジェクトを選択して、リストの下にある [編集（Edit）]（鉛筆）ボタンをクリックします。

[IKEv1 Proposal] ポリシー オブジェクトの設定

[IKEv1 Proposal] ダイアログボックスを使用して、IKEv1 プロポーザル オブジェクトを作成、コピー、および編集します。

Internet Key Exchange（IKE; インターネット キー交換）バージョン 1 プロポーザル オブジェクトには、リモート アクセス VPN ポリシーおよびサイト間 VPN ポリシーを定義する場合に IKE1 プロポーザルに必要となるパラメータが含まれています。IKE は、IPsec ベースの通信の管理

を簡易化するキー管理プロトコルです。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 セキュリティ アソシエーション（SA）の自動確立に使用されます。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーション中に、IKE は、他のアプリケーション（IPsec など）用の Security Association（SA; セキュリティ アソシエーション）を確立します。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルの詳細については、次の項を参照してください。

- IKE および IPsec 設定の概要 （2 ページ）
- IKE バージョン 1 と 2 の比較 （5 ページ）
- IKE について （6 ページ）
- 使用する暗号化アルゴリズムの決定 （7 ページ）
- 使用するハッシュ アルゴリズムの決定 （8 ページ）
- 使用する Diffie-Hellman 係数グループの決定 （9 ページ）
- 使用する認証方式の決定 （11 ページ）

ナビゲーション パス

[管理（Manage）] > **[ポリシーオブジェクト（Policy Objects）]** を選択し、オブジェクトタイプセレクタから **[IKE プロポーザル（IKE Proposals）]** > **[IKEv1 プロポーザル（IKEv1 Proposals）]** を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

ヒント IKE プロポーザルの設定 （12 ページ）の説明に従って [IKE Proposal] ポリシーを設定する際に、このダイアログボックスにアクセスすることもできます。

関連項目

- [IKEv2 Proposal] ポリシー オブジェクトの設定 （19 ページ）
- ポリシー オブジェクトの作成
- Policy Object Manager
- 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 （37 ページ）

フィールド リファレンス

表 *1 : [IKEv1 Proposal]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 1024 文字を使用できます。
[プライオリティ（Priority）]	IKE プロポーザルのプライオリティ値。このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。 有効な値の範囲は 1 ～ 10000 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、Security Manager によって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。
暗号化アルゴリズム（Encryption Algorithm）	フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される暗号化アルゴリズム： • [AES-128]：128 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-256]：256 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [DES]：56 ビット キーを使用するデータ暗号規格に従って暗号化を実行します。 • [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりも強力なセキュリティを確保しますが、暗号化と復号化に多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。 （注） バージョン 4.22 以降、Cisco Security Manager は、ASA 9.15(1) 以降のバージョンのデバイスに対する DES および 3DES 暗号化アルゴリズムのサポートを終了します。

要素	説明
ハッシュ アルゴリズム（Hash Algorithm）	IKE プロポーザルで使用されるハッシュ アルゴリズム。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。次のオプションがあります。 • SHA (Secure Hash Algorithm)：160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。 • [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 では、処理時間が SHA よりも少なくなります。 （注） バージョン 4.22 以降、Cisco Security Manager は、ASA 9.15(1) 以降のバージョンのデバイスに対する MD5 ハッシュアルゴリズムのサポートを終了します。

要素	説明
係数グループ（Modulus Group）	2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。次のオプションがあります。 ヒント　IKEv1 の場合、ASA デバイスは DH グループ 14 のみをサポートします。 • [1]：Diffie-Hellman グループ 1（768 ビット係数）。 （注）　Cisco Security Manager 4.19 以降、DH グループ 1 は ASA 9.12(1) 以降のデバイスではサポートされません。デフォルト値はグループ 2 です。 • [2]：Diffie-Hellman グループ 2（1024 ビット係数）。 （注）　Cisco Security Manager 4.22 は、ASA 9.15(1) 以降のバージョンのデバイスに対する DH グループ 2 のサポートを終了します。 • [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以降）を使用します。 • [7]：Diffie-Hellman グループ 7（163 ビットの楕円曲線フィールド サイズ）。 • [14]：Diffie-Hellman グループ 14（2048 ビット係数。128 ビット キーの保護に推奨される）。 （注）　Cisco Security Manager 4.20 以降では、DH グループ 14 がサポートされており、これが ASA 9.13(1) 以降のデバイスにおける IKEv1 のデフォルト DH グループです。 • [15]：Diffie-Hellman グループ 15（3072 ビット係数。192 ビット キーの保護に推奨される）。 • [16]：Diffie-Hellman グループ 16（4096 ビット係数。256 ビット キーの保護に推奨される）。 （注）　Diffie-Hellman グループ 15 と 16 がリストされていますが、これらは IKEv1 ではサポートされていないため、IKEv1 ポリシーに選択すると検証エラーが発生します。

要素	説明
保存期間（Lifetime）	セキュリティ アソシエーション（SA）のライフタイム（秒数）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。 60 ～ 2147483647 秒の値を指定できます。デフォルトは 86400 です。
認証方式	2つのピア間で使用する認証方式。設定する必要があるその他のポリシーをこの選択で判別する方法については、使用する認証方式の決定 （11 ページ）を参照してください。次のいずれかを選択します。 • [事前共有キー（Preshared Key）]：事前共有キーを使用すると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。参加ピアの 1 つに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。 • 証明書：IKE キー管理メッセージを署名および暗号化するために、RSA キー ペアが使用される認証方式。この方式によって、2 つのピア間の通信の否認防止が提供されます。つまり、実際に通信が行われたことが証明されます。この認証方式を使用すると、ピアは、Certification Authority（CA; 証明局）からデジタル証明書を取得するように設定されます。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 を参照してください。

[IKEv2 Proposal] ポリシー オブジェクトの設定

[IKEv2 Proposal] ダイアログボックスを使用して、IKEv2 プロポーザル オブジェクトを作成、コピー、および編集します。IKEv2 プロポーザルは、ASA ソフトウェア リリース 8.4(1)+ だけで使用できます。

Internet Key Exchange（IKE; インターネット キー交換）バージョン 2 プロポーザル オブジェクトには、リモート アクセス VPN ポリシーおよびサイト間 VPN ポリシーを定義する場合に IKEv2 プロポーザルに必要となるパラメータが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。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 セキュリティ アソシエーション（SA）の自動確立に使用されます。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーション中に、IKE は、他のアプリケーション（IPsec など）用の Security Association（SA; セキュリティ アソシエーション）を

確立します。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKEv1 とは異なり、IKEv2 プロポーザルでは、ピアがフェーズ 1 ネゴシエーション中に選択できる複数のアルゴリズムと係数グループを選択できます。IKE プロポーザルの詳細については、次の項を参照してください。

- IKE および IPsec 設定の概要 （2 ページ）
- IKE バージョン 1 と 2 の比較 （5 ページ）
- IKE について （6 ページ）
- 使用する暗号化アルゴリズムの決定 （7 ページ）
- 使用するハッシュ アルゴリズムの決定 （8 ページ）
- 使用する Diffie-Hellman 係数グループの決定 （9 ページ）

ヒント IKEv1 とは異なり、IKE プロポーザルで認証方式を指定しません。IKEv2 での認証方式の設定方法に関する詳細については、使用する認証方式の決定 （11 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [IKEプロポーザル（IKE Proposals）] > [IKEv2プロポーザル（IKEv2 Proposals）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

ヒント IKE プロポーザルの設定 （12 ページ）の説明に従って [IKE Proposal] ポリシーを設定する際に、このダイアログボックスにアクセスすることもできます。

関連項目

- [IKEv1 Proposal] ポリシー オブジェクトの設定 （14 ページ）
- ポリシー オブジェクトの作成
- Policy Object Manager
- 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 （37 ページ）

フィールド リファレンス

表 *2 : [IKEv2 Proposal]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 1024 文字を使用できます。
[プライオリティ（Priority）]	IKE プロポーザルのプライオリティ値。このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。 有効な値の範囲は 1 ～ 65535 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、Security Manager によって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。

要素	説明
暗号化アルゴリズム（Encryption Algorithm）	フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される暗号化アルゴリズム。[選択（Select）] をクリックして、VPN で許可するすべてのアルゴリズムを選択します。 • [AES-GCM-256]：256 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（9.0.1+ を実行している ASA 5580 および ASA 5500-X シリーズ デバイスのみ）。 • [AES-GCM-192]：192 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（9.0.1+ を実行している ASA 5580 および ASA 5500-X シリーズ デバイスのみ）。 • [AES-GCM]：128 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（9.0.1+ を実行している ASA 5580 および ASA 5500-X シリーズ デバイスのみ）。 • [AES-256]：256 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES]：128 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりも強力なセキュリティを確保しますが、暗号化と復号化に多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。 • [DES]：56 ビット キーを使用するデータ暗号規格に従って暗号化を実行します。 • [Null]：暗号化アルゴリズムなし。 （注） バージョン 4.22 以降、Cisco Security Manager は、ASA 9.15(1) 以降のバージョンのデバイスに対する DES および 3DES 暗号化アルゴリズムと Null オプションのサポートを終了します。

要素	説明
Integrity (Hash) Algorithm	IKEプロポーザルで使用するハッシュアルゴリズムの整合性部分。このハッシュアルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。[選択（Select）] をクリックして、VPN で許可するすべてのアルゴリズムを選択します。 （注） AES-GCM、AES-GCM-192、または AES-GCM-256 を使用している場合は、整合性アルゴリズムとして Null を選択する必要があります。 • SHA（セキュア ハッシュ アルゴリズム）：SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。 標準の SHA では、160 ビットのダイジェストが生成されます。 よりセキュアな次のオプションは、ASA 8.4(2+) デバイスの IKEv2 設定で使用できます。 • SHA512：512 ビット キー • SHA384：384 ビット キー • SHA256：256 ビット キー • [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 では、処理時間が SHA よりも少なくなります。 （注） バージョン 4.22 以降、Cisco Security Manager は、ASA 9.15(1) 以降のバージョンのデバイスに対する MD5 ハッシュアルゴリズムのサポートを終了します。 • [Null]：暗号化アルゴリズムなし。AES-GCM、AES-GCM-192、および AES-GCM-256 でのみ使用します。
Prf Algorithm	IKE プロポーザルで使用するハッシュ アルゴリズムの Pseudo-Random Function（PRF; 疑似乱数関数）部分。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。[選択（Select）] をクリックして、VPN で許可するすべてのアルゴリズムを選択します。オプションについては、上記の整合性アルゴリズムの項で説明されています。 （注） Cisco Security Manager 4.22 は、最新の脅威に対して安全ではなくなったため、MD5 PRF アルゴリズムのサポートを終了します。

要素	説明
係数グループ（Modulus Group）	

要素	説明
	2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。[選択（Select）] をクリックして、VPN で許可するすべてのグループを選択します。 • [1]：Diffie-Hellman グループ 1（768 ビット係数）。 （注） Cisco Security Manager 4.19 以降、DH グループ 1 オプションは、ASA 9.12(1) 以降のデバイスではサポートされません。 • [2]：Diffie-Hellman グループ 2（1024 ビット係数）。 • [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以降）を使用します。 • [14]：Diffie-Hellman グループ 14（2048 ビット係数。128 ビット キーの保護に推奨される）。（ASA 9.0.1 以降のデバイスのみ）。 （注） Cisco Security Manager 4.20 以降では、DH グループ 14 がサポートされており、これが ASA 9.13(1) 以降のデバイスにおける IKEv1 のデフォルト DH グループです。 • [15]：Diffie-Hellman グループ 15（3072 ビット係数。192 ビット キーの保護に推奨される）。（ASA 9.13.1 以降のデバイスのみ）。 • [16]：Diffie-Hellman グループ 16（4096 ビット係数。256 ビット キーの保護に推奨される）。（ASA 9.13.1 以降のデバイスのみ）。 • [19]：Diffie-Hellman グループ 19（256 ビットの楕円曲線フィールド サイズ）。（ASA 9.0.1 以降のデバイスのみ）。 • [20]：Diffie-Hellman グループ 20（384 ビットの楕円曲線フィールド サイズ）。（ASA 9.0.1 以降のデバイスのみ）。 • [21]：Diffie-Hellman グループ 21（521 ビットの楕円曲線フィールド サイズ）。（ASA 9.0.1 以降のデバイスのみ）。 • [24]：Diffie-Hellman グループ 24（2048 ビット係数および 256 ビット素数位数サブグループ）。（ASA 9.0.1 以降のデバイスのみ）。 • [31]：Diffie-Hellman グループ 31（256 ビットの楕円曲線フィールドサイズ）。（ASA 9.16.1 以降のデバイスのみ）。 （注） バージョン 4.22 以降、Cisco Security Manager は、ASA 9.15(1) 以降のバージョンのデバイスにおける DH グループ 2 および 24 をサポートしていません。 （注） Cisco Security Manager 4.23 以降、DH グループ 31 は、ASA 9.16(1)

要素	説明
	以降のデバイスの IPsec プロファイルおよび IKEv2 でサポートされます。
保存期間（Lifetime）	セキュリティ アソシエーション（SA）のライフタイム（秒数）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。 120 ～ 2147483647 秒の値を指定できます。デフォルトは 86400 です。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 を参照してください。

IPsec プロポーザルについて

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルは、2 つのピア間のセキュアな論理通信パスです。ピアは、サイト間 VPN 内のデバイスまたはリモート アクセス IPsec VPN 内のデバイスとユーザが考えられます。IPsec トンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。

IPsec プロポーザルは、IKE について （6 ページ）で説明されているように、IKE ネゴシエーションのフェーズ 2 で使用されます。プロポーザルの特定のコンテンツは、トポロジ タイプ（サイト間またはリモート アクセス）とデバイス タイプによって異なりますが、プロポーザルは大まかには似ていて、IPsec トランスフォーム セットなど、同じ要素を多数含んでいます。

次の項では、IPsec プロポーザルの概念と手順についてより詳細に説明します。

- Easy VPN での IPsec プロポーザルの設定
- 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）
- 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）

サイト間 VPN の IPsec プロポーザルについて

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。基本 IPsec 設定では、ルーティング プロトコルを使用できません。作成されるポリシーは、基本 IPsec のプロビジョニングに使用されます。基本 IPsec は、Cisco IOS ルータ、PIX ファイアウォール、Catalyst VPN サービス モジュール、および Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスに設定できます。

IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2つのピア間のセキュアで論理的な通信パスです。IPsec トンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。

Security Manager では、[IPsec Proposal] ポリシーを使用して、IPsec トンネルに必要な設定を定義します。IPsec プロポーザルとは、デバイスの VPN インターフェイスに適用される 1 つ以上のクリプト マップの集合です。クリプト マップには、トランスフォーム セットを含む、IPsec セキュリティ アソシエーションを設定するために必要なすべてのコンポーネントが含まれています。クリプト マップでは、Reverse Route Injection（RRI; 逆ルート注入）を設定することもできます。

詳細については、次の項を参照してください。

- クリプト マップについて （27 ページ）
- トランスフォーム セットの概要 （28 ページ）
- 逆ルート注入について （30 ページ）

関連項目

- サイト間 VPN での IPsec プロポーザルの設定 （31 ページ）

クリプト マップについて

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 を定義するために必要なその他のパラメータを含む、IPsec Security Associations（SA; セキュリティ アソシエーション）を設定するため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。クリプト マップ エントリは、一連の CLI コマンドに名前が付けられた形式になっています。同じクリプト マップ名および異なるマップ シーケンス番号を持つ複数のクリプト マップ エントリは、1 つのクリプト マップ セットにグループ化されて、関連するデバイスの VPN

インターフェイスに適用されます。インターフェイスを通過するすべてのIPトラフィックは、適用されたクリプト マップ セットに対して評価されます。

2 つのピアが SA を確立しようとする場合は、それぞれに少なくとも 1 つの互換クリプト マップエントリが必要です。クリプトマップエントリに定義されたトランスフォームセットは、そのクリプトマップの IPsec ルールによって指定されたデータフローを保護するための IPsec セキュリティ ネゴシエーションで使用されます。

不明なリモート ピアがローカル ハブとの間の IPsec セキュリティ アソシエーションの開始を試みた場合、ダイナミック クリプト マップ ポリシーがサイト間 VPN で使用されます。ハブは、セキュリティ アソシエーション ネゴシエーションを開始できません。ダイナミック暗号ポリシーを使用することによって、ハブがリモートピアのアイデンティティを把握していない場合でも、リモートピアはローカルハブとの間で IPsec トラフィックを交換できます。ダイナミック クリプト ポリシーは、個別のハブ、またはハブを含むデバイス グループに作成できます。このポリシーは、ハブに対してだけ書き込まれ、グループにスポークが含まれていてもスポークには書き込まれません。実質的には、ダイナミック暗号マップポリシーによって、すべてのパラメータが設定されていない暗号マップエントリが作成されます。設定されていないパラメータは、IPsec ネゴシエーションの結果として、リモート ピアの要件に合うようにあとで動的に設定されます。ダイナミック クリプトマップまたはスタティック クリプトマップのピア アドレスは、VPN トポロジから推定されます。

ダイナミック クリプト マップ ポリシーは、ハブアンドスポーク VPN 設定にだけ適用されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、スタティック クリプト マップ ポリシーだけを適用できます。

（注） （サイト間 VPN）エクストラネット VPN を除き、Security Manager は、トンネルのピアが Security Manager によって管理されている場合だけ、既存の VPN トンネルを管理できます。このような場合、Security Manager では、ピアにおいてトンネルに同じクリプト マップ名が使用されます。以降の展開においては、Security Manager トンネルだけが管理されます（Security Manager では、設定されたすべてのトンネルのログが保持されます）。

関連項目

- IPsec プロポーザルについて （26 ページ）
- トランスフォーム セットの概要 （28 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （31 ページ）

トランスフォーム セットの概要

トランスフォームセットとは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルおよびアルゴリズムの組み合わせです。IPsec Security Association（SA：セキュリティ アソシエーション）のネゴシエーション中に、ピアでは、両方のピアに共通するトランスフォーム セットが検索されます。そのようなトランスフォーム セットは、検出されると適用

され、そのクリプトマップのアクセスリストでデータフローを保護するSAが作成され、VPNでトラフィックが保護されます。

IKEv1とIKEv2には別個のIPsecトランスフォームセットがあります。IKEv1トランスフォームセットを使用して、パラメータごとに1つの値を設定します。IKEv2トランスフォームセットでは、単一のプロポーザルに複数の暗号化アルゴリズムと統合アルゴリズムを設定できます。ASAデバイスは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

1つのIPsecプロポーザル ポリシーごとに複数のトランスフォーム セットを指定できます。スポークまたはスポークのグループに対してポリシーを定義する場合は、通常、複数のトランスフォームセットを指定する必要はありません。これは、スポークに割り当てられたハブが、通常はより高性能なルータであり、スポークがサポートするすべてのトランスフォームセットをサポートできるためです。ただし、ハブでダイナミック クリプトに関してポリシーを定義している場合は、ハブと不明なスポークとの間でトランスフォームセットが一致するように、複数のトランスフォーム セットを指定する必要があります。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。

Security Managerには、トンネル ポリシーで使用できる定義済みのトランスフォーム セットが用意されています。独自のトランスフォームセットを作成することもできます。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 （37ページ）を参照してください。

IKEv1 トランスフォーム セットのトンネル モードの選択

IKEv1 トランスフォーム セットを定義する場合は、使用するIPsecの動作モード（トンネルモードまたはトランスポート モード）を指定する必要があります。AHプロトコルおよびESPプロトコルを使用して、IPペイロード全体を保護するか（トンネル モード）、IPペイロードの上位層プロトコルだけを保護（トランスポート モード）できます。

トンネル モード（デフォルト）では、元のIPデータグラム全体が暗号化され、その暗号化されたデータが新しいIPパケットのペイロードとなります。このモードでは、ルータはIPsecプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元のルータがパケットを暗号化し、IPsecトンネルを使用して転送します。宛先のルータは元のIPデータグラムを復号化し、宛先システムに転送します。トンネルモードの主な利点は、終端システムを変更しなくてもIPsecを利用できる点です。また、トンネル モードを使用すると、トラフィック分析に対しても保護されます。トンネルモードを使用した場合、攻撃者は、トンネルのエンドポイントだけを特定できます。トンネルを通過するパケットの送信元と宛先がトンネルのエンドポイントと同じである場合でも、攻撃者はそのパケットの実際の送信元と宛先を特定できません。

トランスポート モードでは、IPペイロードだけが暗号化され、元のIPヘッダーはそのまま使用されます。このモードの利点は、各パケットに追加されるのが数バイトだけである点です。また、パブリック ネットワーク上のデバイスは、パケットの実際の送信元と宛先を確認できます。ただし、IPヘッダーがクリア テキストで渡されるため、トランスポート モードでは、攻

撃者が一定のトラフィック分析を実行できます。たとえば、攻撃者は、会社の CEO が他のシニアエグゼクティブに多数のパケットを送信したタイミングを把握できます。ただし、攻撃者が把握できるのは、IP パケットが送信されたという事実だけです。パケットの内容は解読できません。トランスポート モードでは、フローの宛先は IPsec 終端デバイスである必要があります。

（注） 通常の IPsec または Easy VPN を使用して、VPN トポロジにトランスポート モードを使用することはできません。

関連項目

- IPsec プロポーザルについて （26 ページ）
- クリプト マップについて （27 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （31 ページ）

逆ルート注入について

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。保護されているこれらのホストおよびネットワークは、リモート プロキシ アイデンティティと呼ばれます。各ルートは、リモート プロキシ ネットワークとマスクを基にして作成され、リモート トンネル エンドポイントがこのネットワークへのネクスト ホップとなります。リモート VPN ルータをネクスト ホップとして使用することによって、トラフィックは強制的に暗号プロセスを通して暗号化されます。

VPN ルータでスタティック ルートが作成されたあと、この情報がアップストリーム デバイスに伝播されます。これにより、アップストリーム デバイスでは、IPsec 状態フローを維持するためのリターン トラフィックの送信先として適切な VPN ルータを特定できるようになります。この機能は、サイトで複数の VPN ルータを使用してロード バランシングやフェールオーバーを提供している場合や、デフォルト ルート経由でリモート VPN デバイスにアクセスできない場合に特に便利です。ルートは、グローバル ルーティング テーブルまたは適切な Virtual Routing and Forwarding（VRF）テーブルに作成されます。

（注） VRF 対応 IPsec が設定されている場合、Security Manager によって、ハイ アベイラビリティ（HA）が設定されているデバイスや IPsec Aggregator に自動的に RRI が設定されます。リモートアクセス VPN 内のデバイスのクリプトマップに RRI を設定することもできます。

Security Manager では、逆ルート注入を設定する場合に次のオプションを使用できます。

- ダイナミック クリプトマップでは、ルートは、リモート プロキシの IPsec Security Association（SA;セキュリティ アソシエーション）が正常に確立されたときに作成されます。リモート プロキシへのネクスト ホップは、リモート VPN ルータ経由となります。リモート VPN

ルータのアドレスは、ダイナミック クリプト マップ テンプレートの作成中に学習および適用されます。ルートは、SA が削除されたあとに削除されます。

- [Remote Peer] オプション（IOS デバイスでだけ使用可能）を使用すると、リモート VPN デバイスへの明示的なネクストホップとして、インターフェイスまたはアドレスを指定できます。2 つのルートが作成されます。1 つめのルートは標準的なリモート プロキシ アイデンティティであり、ネクスト ホップはリモート VPN クライアントのトンネル アドレスとなります。2 つめのルートは、再帰検索において「ネクストホップ」経由でリモートエンドポイントに到達できることが強制される場合のリモート トンネル エンドポイントへの実際のルートです。実際のネクストホップ用の 2 つめのルートを作成することは、デフォルトルートをより明示的なルートで上書きする必要がある場合に VRF 対応 IPsec で非常に重要となります。

（注） VPN Services Module（VPNSM; VPN サービス モジュール）を使用するデバイスでは、ネクスト ホップはクリプト マップが適用されるインターフェイス、サブインターフェイス、または VLAN となります。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）およびリモート 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。

- [Remote Peer IP]（IOS デバイスでだけ使用可能）の場合、ユーザ定義のネクスト ホップを経由したリモート プロキシへのルートが 1 つ作成されます。暗号化された発信パケットを適切に送信するために、ネクスト ホップを使用してデフォルト ルートを上書きできます。このオプションを使用すると、作成されるルートの数を減らすことができます。また、このオプションでは、ルート再帰を容易に使用できないプラットフォームがサポートされます。

関連項目

- IPsec プロポーザルについて （26 ページ）
- クリプト マップについて （27 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （31 ページ）

サイト間 VPN での IPsec プロポーザルの設定

[IPsec Proposal] ページを使用して、Easy VPN トポロジを除いて、サイト間 VPN トポロジの IKE フェーズ 2 ネゴシエーション中に使用される IPsec プロポーザルを設定します。

Easy VPN トポロジで使用される IPsec プロポーザルと、リモート アクセス VPN で使用される IPsec プロポーザルは、ここで説明する基本的なサイト間プロポーザルとは大幅に異なります。これらの他のトポロジで使用される IPsec プロポーザルについては、次の項を参照してください。

- Easy VPN での IPsec プロポーザルの設定

- 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）
- 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）

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ）VPN セレクタで non-Easy VPN 以外のトポロジを選択して、ポリシーセレクタで [IPsecプロポーザル（IPsec Proposal）] を選択します。必要に応じて、[IPsecプロポーザル（IPsec Proposal）] 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で **[サイト間VPN（Site-to-Site VPN）] > [IPsecプロポーザル（IPsec Proposal）]** を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

関連項目

- IKE について （6 ページ）
- サイト間 VPN の IPsec プロポーザルについて （27 ページ）

フィールド リファレンス

表 *3 : [IPsec Proposal]* ページ、サイト間 *VPN*（*Easy VPN* を除く）

要素	説明
Crypto Map Type （ハブアンドスポーク トポロジと完全メッシュ トポロジだけ）	クリプト マップには、IPsec Security Association（SA; セキュリティ アソシエーション）を設定するため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。2 つのピアが SA を確立しようとする場合は、それぞれに少なくとも 1 つの互換クリプト マップ エントリが必要です。詳細については、クリプト マップについて （27 ページ）を参照してください。 生成するクリプト マップのタイプを選択します。 • [スタティック（Static）]：スタティック クリプト マップは、ポイントツーポイントまたは完全メッシュ VPN トポロジで使用します。 • [Dynamic]：ダイナミック クリプト マップは、ハブアンドスポーク VPN トポロジでだけ使用できます。ダイナミック クリプトマップポリシーを使用すると、ハブがリモートピアのアイデンティティを把握していない場合でも、リモートピアはローカルハブとの間で IPsec トラフィックを交換できます。

要素	説明
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、ASA ソフトウェア リリース 8.4(x) だけでサポートされます。同様に、4.16 以降、Cisco Security Manager は分散モードで構成された Firepower 9300 デバイスの IKEv1 構成をサポートしていません。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。トポロジ内のデバイスが IKEv2 をサポートしない場合は、IKEv1 を選択する必要があります。 ハブアンドスポーク トポロジまたは完全メッシュ トポロジで両方のオプションを選択すると、Security Manager は、デバイスで使用される OS のタイプとバージョンに基づいて IKE バージョンをデバイスに自動的に割り当てます。これらの割り当てを変更するには、[IKEバージョン（IKE Version）] タブをクリックして、[IKEv1対応ピア（IKEv1 Enabled Peers）] または [IKEv2対応ピア（IKEv2 Enabled Peers）] の下にある [選択（Select）] ボタンをクリックして、デバイスに割り当てられているバージョンを変更します。各バージョンをサポートするデバイスだけについて割り当てを変更できます。他のデバイスは選択できません。詳細については、サイト間 VPN におけるデバイスの IKE バージョンの選択 （36 ページ）を参照してください。
トランスフォーム セット（Transform Sets） 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 （28 ページ）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 （37 ページ）を参照してください。 （注） IKEv1 トランスフォームセットでは、トンネルモードまたはトランスポート モードの IPsec 動作を使用できます。ただし、IPsec または Easy VPN トポロジではトランスポートモードを使用できません。

要素	説明
Perfect Forward Secrecy の有効化（Enable Perfect Forward Secrecy） 係数グループ（Modulus Group）	暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用するかどうかを指定します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイント デバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。 このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッションキーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （9 ページ）を参照してください。 （注） DH グループ 1 は廃止され、以降の ASA バージョンで削除されます。以降の ASA バージョンでは、デフォルト値はグループ 2 になります。
Lifetime (sec) ライフタイム（KB）（Lifetime (kbytes)）	暗号化 IPsec Security Association（SA; セキュリティ アソシエーション）のグローバルなライフタイム設定。IPsec ライフタイムは、秒、KB、またはその両方で指定できます。 • [Seconds (sec)]：SA が期限切れになるまでに存続できる秒数。デフォルトは 3600 秒（1 時間）です。 • [Kilobytes (kbytes)]：特定の SA が期限切れになる前にその SA を使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。有効な値は、デバイス タイプに応じて異なります。入力できる値の範囲は、IOS ルータでは 10 ～ 2147483647、ASA/PIX7.0+ デバイスでは 2560 ～ 536870912 です。 デフォルト値は 4,608,000 KB です。
QoS Preclassify	7600 デバイスを除く Cisco IOS ルータでサポートされます。 選択されている場合、トンネリングおよび暗号化実行前にパケットを分類できます。 VPN の Quality of Service（QoS）機能を使用すると、インターフェイスで Cisco IOS QoS サービスとトンネリングおよび暗号化を同時に実行できます。出力インターフェイスの QoS 機能によって、データが暗号化およびトンネリングされる前にパケットが分類されて、適切な QoS サービスが適用されます。これにより、輻輳した環境でのトラフィック フローの調整が可能となり、より効率的なパケットのトンネリングを実現できます。

要素	説明
Reverse Route	ASA デバイス、PIX 7.0+ デバイス、および 7600 デバイス以外の Cisco IOS ルータでサポートされます。 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 （30ページ）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）]（ASA、PIX 7.0+、IOS デバイス）：クリプト マップアクセス制御リスト（ACL）に定義された宛先情報に基づいてルートを作成します。これがデフォルトのオプションです。 • [リモートピア（Remote Peer）]（IOS デバイスのみ）：リモートエンドポイント用に1つ、クリプトマップが適用されるインターフェイス経由でのリモートエンドポイントへのルート再帰用に 1 つ、合計 2 つのルートを作成します。 • [リモートピアIP（Remote Peer IP）]（IOS デバイスのみ）：アドレスをリモート VPN デバイスへの明示的なネクストホップとして指定します。IP アドレス、またはアドレスを指定するネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）] をクリックして、リストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） ネットワークまたはホストオブジェクトを使用する場合は、オブジェクトで [デバイスごとの値のオーバーライドを許可（Allow Value Override per Device）] オプションを選択し、必要に応じて、このオブジェクトを使用する特定のデバイスの IP アドレスをオーバーライドできます。
動的RRIの有効化（Enable Dynamic RRI）	（注） このオプションは、ASA 9.7(1) 以降でサポートされています。これは、IKEV2 が有効になっているか、静的クリプトマップが選択されている場合にのみ適用されます。 有効にすると、設定中はクリプトマップによって逆ルートはインストールされず、IPsec セキュリティ アソシエーション（SA）が起動するまで延期されます。
[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。	

要素	説明
[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。
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。

サイト間 VPN におけるデバイスの IKE バージョンの選択

[IPsec Proposal] ページで [IKE Version] タブを使用して、ハブアンドスポークまたは完全メッシュ サイト間 VPN でデバイスごとに使用する IKE のバージョンを選択します。このタブは、Site-to-Site VPN Manager だけで表示されます。ポリシー ビューではオプションを設定できません。これらのオプションは、VPN トポロジ内の実際のデバイスに固有であるためです。

[IKE Version] タブには、[IKEv1 Enabled Peers] と [IKEv2 Enabled Peers] の 2 つのリストが含まれています。サイト間 VPN での IPsec プロポーザルの設定 （31 ページ）の説明に従って IPsec プロポーザルを設定する際に、VPN で許可する IKE バージョン（バージョン 1、バージョン 2、または両方）を選択します。Security Manager は、デバイスによって使用される OS バージョンに基づいてデバイスに使用する IKE バージョンを自動的に選択します。たとえば、IOS ルータは、[IKEv1 Enabled Peers] リストに常に表示されます。デバイスで IKEv1 と IKEv2 の両方がサポートされる場合は、両方のリストに表示されます。

選択を変更する必要があるのは、VPN で両方の IKE バージョンを許可していて、一部の IKEv2 対応デバイスがいずれかの IKE バージョンを使用するのを明示的に防止する場合だけです。

デバイスで許可する IKE バージョンを変更するには、デバイスを削除する（または以前に削除したデバイスを追加する）リストの下にある [選択（Select）] ボタンをクリックします。次の作業を行うことができる選択ダイアログボックスが開きます（選択を確認するには、[OK] をクリックします）。

- デバイスを削除して、IKE バージョンを使用できなくするには、[選択されたピア（Selected Peers）] リストでそのデバイスを強調表示して、[<<] をクリックして [使用可能なピア（Available Peers）] リストに移動します。
- デバイスを追加して、IKE バージョンの使用を許可するには、[使用可能なピア（Available Peers）] リストでそのデバイスを強調表示して、[>>] をクリックして [選択されたピア（Selected Peers）、] リストに移動します。

ヒント　単一のバージョンをサポートするデバイスのバージョン選択は変更できないため、選択リストには、両方の IKE バージョンをサポートするデバイスだけが含まれています。IKEv2 は、ASA ソフトウェア 8.4(1)+ でサポートされます。

ナビゲーション パス

（[Site-to-Site VPN Manager] ウィンドウ）VPN セレクタで non-Easy VPN 以外のトポロジを選択して、ポリシーセレクタで [IPsecプロポーザル（IPsec Proposal）] を選択します。[IKEバージョン（IKE Version）] タブをクリックします。

関連項目

- IKE について　（6 ページ）
- サイト間 VPN での IPsec プロポーザルの設定　（31 ページ）

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

[Add IPSec Transform Set]/[Edit IPSec Transform Set] ダイアログボックスを使用して、IKE ネゴシエーションで使用する IPSec トランスフォーム セットを設定します。

サイト間 VPN およびリモート アクセス VPN における IPSec 保護トラフィックを定義するときに、IPSec プロポーザルに使用する IPSec トランスフォーム セット オブジェクトを作成できます。IPSec セキュリティ アソシエーションのネゴシエーション中、ピアは、特定のデータ フローを保護する場合に特定のトランスフォーム セットを使用することを合意します。

2 つの異なるセキュリティ プロトコルが、IPSec 標準に含まれています。

- [Encapsulating Security Protocol (ESP)]：認証、暗号化、およびアンチリプレイの各サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

- [Authentication Header (AH)]：認証サービスとアンチリプレイ サービスを提供します。AH では暗号化が提供されず、通常は、ESP の方が優先されます。また、ルータだけでサポートされます。AH は、IP プロトコル タイプ 51 です。

（注） IPSec トンネルで暗号化と認証の両方を使用することを推奨します。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec トランスフォーム セット オブジェクトがあります。

- IPSec IKEv1 トランスフォーム セット オブジェクトを作成する場合、IPSec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。また、トランスフォームセットに圧縮を含めるかどうかを選択できます。アルゴリズムに単一のオプションを選択できるため、VPN で複数の組み合わせをサポートするには、複数の IPsec IKEv1 トランスフォーム セット オブジェクトを作成する必要があります。
- IPSec IKEv2 トランスフォーム セット オブジェクトを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。IKEv2 ネゴシエーション中に、ピアは、それぞれでサポートされる最適なオプションを選択します。

（注） デバイスで IPsec IKEv1 または IKEv2 プロポーザルを設定する場合は、そのデバイスに設定されたプロポーザルを使用する必要があります。たとえば、サイト間（ポイントツーポイント）VPN 構成では、IPsec プロポーザルで構成されたエンドポイント（インターフェイス）をクリプトマップの生成に使用できます。ただし、設定されたプロポーザルが Security Manager によってそのデバイスに使用されない場合、後続の設定のプレビューでは、Security Manager は negate コマンドを生成し、設定された IPsec プロポーザルは Security Manager によって否定されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、オブジェクトタイプセレクタから **[IPSec トランスフォームセット（IPSec Transform Sets）] > [IPSec IKEv1 トランスフォームセット（IPSec IKEv1 Transform Sets）]**、または **[IPSec トランスフォームセット（IPSec Transform Sets）] > [IPSec IKEv2 トランスフォームセット（IPSec IKEv2 Transform Sets）]** を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- トランスフォーム セットの概要 （28 ページ）
- IKE および IPsec 設定の概要 （2 ページ）
- IKE バージョン 1 と 2 の比較 （5 ページ）
- IKE について （6 ページ）

- IPsec プロポーザルについて （26 ページ）
- [IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス）
- IPsec Proposal Editor（IOS、PIX 6.3 デバイス）
- 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）
- 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）
- サイト間 VPN での IPsec プロポーザルの設定 （31 ページ）
- Easy VPN での IPsec プロポーザルの設定
- [IKEv1 Proposal] ポリシー オブジェクトの設定 （14 ページ）
- ポリシー オブジェクトの作成
- Policy Object Manager

フィールド リファレンス

表 4 : [IPSec IKEv1 or IKEv2 Transform Set] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 1024 文字を使用できます。
[モード（Mode）] （IKEv1 のみ）	IPSec トンネルが動作するモード： • [Tunnel]：トンネルモードによって、IP パケット全体がカプセル化されます。IPSec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これがデフォルトです。 トンネル モードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネル モードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPSec が実装される標準の方法です。 • [Transport]：トランスポート モードでは、IP パケットの上位層プロトコルだけがカプセル化されます。IPSec ヘッダーは、IP ヘッダーと上位層プロトコル ヘッダー（TCP など）との間に挿入されます。 トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポート モードは、レイヤ 2 またはレイヤ 3 のトンネリング プロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。

要素	説明
ESP 暗号化（ESP Encryption）	

要素	説明
	トランスフォーム セットが使用する Encapsulating Security Protocol（ESP; カプセル化セキュリティ プロトコル）暗号化アルゴリズム。次のオプションの詳細については、使用する暗号化アルゴリズムの決定 （7 ページ）を参照してください。 IKEv1 では、次のいずれかのオプションを選択します。IKEv2 では、[選択（Select）] をクリックして、サポートするすべてのオプションを選択できるダイアログボックスを開きます。 （注） AES-GCM/GMAC は、5580 以降の ASA プラットフォームでのみ設定できます。 • （空白）：ESP 暗号化を使用しません。 • [DES]：56 ビット キーを使用するデータ暗号規格に従って暗号化を実行します。 • [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりも強力なセキュリティを確保しますが、暗号化と復号化に多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。 （注） バージョン 4.22 以降、Cisco Security Manager は、IPsec IKEv1 プロポーザルの DES および 3DES ESP 暗号化アルゴリズムをサポートしません。これらは、現代の脅威に対して安全であると見なされなくなったためです。 • [AES-128 (AES)]：128 ビットキーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-256]：256 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [ESP-Null (NULL)]：ヌル暗号化アルゴリズム。[ESP-Null] を使用して定義されたトランスフォーム セットでは、暗号化なしの認証を提供します。一般的に、テスト目的にだけ使用されます。 • [AES-GCM]（IKEv2のみ）：128 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（ASA 9.0.1 以降のデバイスのみ）。 • [AES-GCM-19]（IKEv2のみ）：192 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（ASA 9.0.1 以降のデバイスのみ）。 • [AES-GCM-256]（IKEv2のみ）：256 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（ASA 9.0.1 以降の

要素	説明
	デバイスのみ）。 • [AES-GMAC]（IKEv2のみ）：128 ビットキーを使用する高度暗号化規格 Galois メッセージ認証コードに従って暗号化を実行します • [AES-GMAC-192]（IKEv2のみ）：192 ビットキーを使用する高度暗号化規格 Galois メッセージ認証コードに従って暗号化を実行します • [AES-GMAC-256]（IKEv2のみ）：256 ビットキーを使用する高度暗号化規格 Galois メッセージ認証コードに従って暗号化を実行します （注） バージョン 4.22 以降、Cisco Security Manager は、ASA 9.15(1) 以降のバージョンのデバイスに対して IPsec IKEv2 プロポーザルの DES、3DES、AES-GMAC、AES-GMAC-192、および AES-GMAC-256 ESP 暗号化アルゴリズムのサポートを終了します。現代の脅威に対して安全であると見なされなくなったためです。

要素	説明
ESP Hash Algorithm (IKEv1) ESP Integration Algorithm (IKEv2) AH Hash Algorithm (IKEv1 only)	認証のためにトランスフォームセットで使用するハッシュアルゴリズムまたは整合性アルゴリズム。IKEv1 の場合、デフォルトでは、ESP 認証用の SHA を使用し、AH認証は使用しません。IKEv2には、デフォルトはありません。AH ハッシュ アルゴリズムは、ルータだけで使用されます。 IKEv1 では、次のいずれかのオプションを選択します。IKEv2 では、[選択（Select）] をクリックして、サポートするすべてのオプションを選択できるダイアログボックスを開きます。 • [None]：ESP または AH 認証を実行しません。 • [SHA, SHA-1 (Secure Hash Algorithm version 1)]：160 ビットのダイジェストを生成します。SHA は、総当たり攻撃に対して、MD5 よりも高い耐性がありますが、より長い処理時間を必要とします。 よりセキュアな次のオプションは、ASA 8.4(2+) デバイスの IKEv2 設定で使用できます。 • SHA512：512 ビット キー • SHA384：384 ビット キー • SHA256：256 ビット キー • [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 では、SHA よりも処理時間が短くなりますが、セキュリティは低くなります。 （注） バージョン 4.22 以降、Cisco Security Manager は、ASA 9.15(1) 以降のバージョンのデバイスに対して MD5 アルゴリズムのサポートを終了します。現代の脅威に対して安全であると見なされなくなったためです。 • [Null]：暗号化アルゴリズムなし。AES-GCM、AES-GCM-192、AES-GCM-256、AES-GMAC、AES-GMAC-192、および AES-GMAC-256 でのみ使用します。
圧縮 （IKEv1 だけ、IOS デバイスだけ）	Lempel-Ziv-Stac（LZS）アルゴリズムを使用して IPSec トンネル内のデータを圧縮するかどうかを指定します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 を参照してください。

VPN グローバル設定

リモート アクセスまたはサイト間 VPN トポロジ内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や、リモート アクセス IPsec VPN で IKEv2 ネゴシエーションをサポートする場合だけ設定します

（注） サイト間 VPN の [VPN Global Settings] ポリシーは、GET VPN を除くすべてのテクノロジーに適用されます。GET VPN のグローバル設定の説明については、GET VPN のグローバル設定を参照してください。

ステップ 1 設定する VPN のタイプに基づいてグローバル設定ポリシーを開くには、次のいずれかを実行します。

- リモート アクセス VPN の場合は、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）] > [グローバル設定（Global 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）] > [グローバル設定（Global Settings）]** 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。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウを開き、VPN セレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global 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で [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

ステップ 2 必要なタブを選択して、必要に応じて設定を行います。

- [ISAKMP/IPsec設定（ISAKMP/IPsec Settings）]：IKE と IPsec のグローバル設定を行います。オプションの詳細については、VPN グローバル ISAKMP/IPsec 設定 （47 ページ）を参照してください。
- [IKEv2設定（IKEv2 Settings）]：IKE バージョン 2 ネゴシエーションのグローバル設定を行います。オプションの詳細については、VPN グローバル IKEv2 設定 （53 ページ）を参照してください。

- [NAT設定（NAT Settings）]：NAT の動作を設定します。オプションの詳細については、VPN グローバル NAT 設定 （59 ページ）を参照してください。VPN での NAT について （57 ページ）も参照してください。
- [アドレス割り当て（Address Assignment）]：リモートクライアントへのアドレス割り当ての 方法を 1 つ以上指定するには、VPN グローバルアドレス割り当て設定の設定 （45 ページ）を参照してください。アドレスの割り当ては、リモートアクセス VPN にのみ適用されます。
- [全般設定（General Settings）]：フラグメンテーションの動作とその他の一部の各種オプションを設定します。オプションの詳細については、VPN グローバル一般設定 （61 ページ）を参照してください。

VPN グローバルアドレス割り当て設定の設定

[VPN グローバル設定（VPN Global Settings）]ページの[アドレス割り当て（Address Assignment）]タブを使用して、リモートクライアントへのアドレス割り当ての方法を 1 つ以上指定します。使用可能な方法は次のとおりです。

- 認証サーバーから IP アドレスを取得します。
- DHCP サーバーから IP アドレスを取得します。
- 内部設定されたプールから IP アドレスを取得します。

（注） ASA ソフトウェアバージョン 7.0(1) 以降を実行しているデバイスでアドレス割り当てを設定できます。デフォルトでは、すべての方法が有効になっています。

アドレス割り当ては、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 の場合は、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）] > [グローバル設定（Global Settings）] を選択します。[アドレス割り当て（Address Assignment）] 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）] > [グローバル設定（Global Settings）] を選択します。既存のポリシーを選択するか新しいポリシーを作成して、[アドレス割り当て（Address Assignment）] タブをクリックします。

関連項目

- VPN グローバル設定 （44 ページ）

フィールド リファレンス

表 *5 : [VPN* グローバル設定（*VPN Global Settings*）*]* ページ、*[*アドレス割り当て（*Address Assignment*）*]* タブ

要素	説明
[IPv4 アドレス割り当ての優先順位（IPv4 Address Assignment Priority）]	
[認証サーバーを使用する（Use Authentication Server）]	認証サーバーから取得した IPv4 アドレスをユーザー単位で割り当てる場合は、オンにします。IPv4 アドレスが設定された認証サーバー（外部または内部）を使用している場合は、この方式を使用することを推奨します。このオプションをオンにする場合は、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[AAA] ポリシーを使用して、ユーザーアクセスの認証に使用する AAA サーバーグループを定義します。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
DHCP を使用する	DHCP サーバーから IP アドレスを取得する場合に選択します。DHCP を使用する場合は、デバイスポリシーセレクタから [プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[サーバーアクセス（Server Access）]>[DHCP サーバー（DHCP Server）] を使用してサーバーを設定する必要があります。また、DHCP サーバーで使用可能な IP アドレスの範囲も定義する必要があります。この方法は IPv4 の割り当てポリシーに使用できます。
[内部アドレスプールを使用する（Use internal address pools）]	内部設定されたプールから IPv4 アドレスを割り当てる場合は、オンにします。内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方法を使用する場合は、IP アドレスプールを設定する必要があります。IP アドレスプールを設定するには、デバイスビューで、デバイスポリシーセレクタから [NAT]>[アドレスプール（Address Pools）] を選択します。または、ポリシービューで、ポリシータイプセレクタから [NAT（PIX/ASA/FWSM）]>[アドレスプール（Address Pools）] を選択し、共有ポリシーセレクタから既存のポリシーを選択するか、[アドレスプール（Address Pools）] を右クリックして新しいポリシーを作成します。

要素	説明
[IP アドレスが解放されてから - 分後に IP アドレスの再利用を許可する（Allow the reuse of an IP address - minutes after it is released）]	IP アドレスがアドレスプールに返された後、IP アドレスの再利用を遅らせます。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、これはチェックされません。つまり、ASA は遅延時間を課しません。遅延を追加する場合は、チェックボックスをオンにし、IP アドレスを再割り当てするまでの時間を 0 ～ 480 の範囲で指定します。 （注） この機能は、ASA ソフトウェアバージョン 8.0(3) 以降を実行しているデバイスで使用できます。
[IPv6 アドレス割り当ての優先順位（IPv6 Address Assignment Priority）]：バージョン 9.0 以降を実行している ASA デバイスの場合は Security Manager 4.12 以降	
[認証サーバーを使用する（Use Authentication Server）]	認証サーバーから取得した IPv6 アドレスをユーザー単位で割り当てる場合は、オンにします。IPv6 アドレスが設定された認証サーバー（外部または内部）を使用している場合は、この方式を使用することを推奨します。このオプションをオンにする場合は、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[AAA] ポリシーを使用して、ユーザーアクセスの認証に使用する AAA サーバーグループを定義します。
[内部アドレスプールを使用する（Use internal address pools）]	内部設定されたプールから IPv6 アドレスを割り当てる場合は、オンにします。内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方法を使用する場合は、IP アドレスプールを設定する必要があります。IPv6 アドレスプールを設定するには、デバイスビューで、デバイスポリシーセレクタから [NAT] > [アドレスプール（Address Pools）] を選択します。または、ポリシービューで、ポリシータイプセレクタから [NAT（PIX/ASA/FWSM）] > [アドレスプール（Address Pools）] を選択し、共有ポリシーセレクタから既存のポリシーを選択するか、[アドレスプール（Address Pools）] を右クリックして新しいポリシーを作成します。

VPN グローバル ISAKMP/IPsec 設定

[VPN Global Settings] ページの [ISAKMP/IPsec Settings] タブを使用して、Internet Key Exchange（IKE; インターネット キー交換）および IPsec のグローバル設定を指定します。

Internet Key Exchange（IKE; インターネット キー交換）プロトコルは、Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれ、2 つのホスト間で IPsec セキュリティ アソシエーションの構築方法について合意するためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 とフェーズ 2 の 2 段階に分けられます。フェーズ 1

では、ISAKMP ネゴシエーション メッセージを保護する最初のトンネルが作成されます。フェーズ 2 では、データを保護するトンネルが作成されます。

ISAKMP ネゴシエーションの条件を設定するために、IKE プロポーザルを作成します。詳細については、IKE プロポーザルの設定 （12 ページ）を参照してください。

IKE キープアライブについて

IKE キープアライブでは、トンネル ピア間で、トンネル経由でデータを送受信できることを示すメッセージが交換されます。キープアライブ メッセージは、設定された間隔で送信されます。この時間内にメッセージが送信されない場合は、バックアップデバイスを使用して新しいトンネルが作成されます。

耐障害性を確保するために IKE キープアライブを使用しているデバイスでは、他の情報を交換しているかどうかにかかわらず、キープアライブ メッセージが送信されます。そのため、これらのキープアライブ メッセージによって、若干ではあるものの追加の負荷がネットワークにかかります。

キープアライブ（DPD）と呼ばれる IKE キープアライブのバリエーションでは、着信トラフィックを受信しておらず、発信トラフィックを送信する必要がある場合にだけ、ピア デバイス間でキープアライブ メッセージが送信されます。発信トラフィックがあるかどうかにかかわらず、着信トラフィックを受信していない場合に DPD キープアライブ メッセージを送信する場合は、[Periodic] オプションを使用してこのことを指定します。

ナビゲーション パス

- リモート アクセス VPN の場合は、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）] > [グローバル設定（Global Settings）] を選択します。[ISAKMP/IPsec設定（ISAKMP/IPsec Settings）] 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、[Remote Access VPN] > [Global Settings] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[ISAKMP/IPsec設定（ISAKMP/IPsec Settings）] タブをクリックします。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウを開き、VPN セレクタでトポロジを選択して、ポリシー セレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。[ISAKMP/IPsec設定（ISAKMP/IPsec Settings）] タブをクリックします。
  - （ポリシー ビュー）ポリシー タイプ セレクタで [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか新しいポリシーを作成し、[ISAKMP/IPsec設定（ISAKMP/IPsec Settings）] タブをクリックします。

関連項目

- VPN グローバル設定 （44 ページ）

- IKE について （6 ページ）
- IPsec プロポーザルについて （26 ページ）

フィールド リファレンス

表 6 : [VPN Global Settings] ページ、[ISAKMP/IPsec Settings] タブ

要素	説明
ISAKMP 設定（ISAKMP Settings）	
Enable Keepalive	Dead-Peer Detection（DPD; デッドピア検知）設定を行うかどうかを指定します。ピアが応答に失敗する場合は、ピアが使用できなくなっていることを前提に新しいトンネルが構築されます。IKE キープアライブは、ハブアンドスポーク VPN トポロジ内のスポーク、ポイントツーポイント VPN トポロジ内の両方のデバイス、またはリモート アクセス VPN 設定に定義します。 次のオプションを設定します。 • [Interval]：キープアライブのモニタリングを開始するまでピアがアイドル状態を維持できる秒数。範囲は 10 ～ 3600 秒です。デフォルトは 10 ですが、リモート アクセス グループの ASA デバイスのデフォルトは 300 です。 • [Retry]：キープアライブ応答が受信されなくなった後のリトライ間の間隔（秒単位）。範囲は、ASA では 2 ～ 10 秒で、IOS デバイスでは 2 ～ 60 です。デフォルト値は 2 秒です。 • [Periodic]：（IOS ソフトウェア バージョン 12.3(7)T 以降を実行しているルータ、7600 デバイスを除く）IPsec トラフィックに関係なく、一定の間隔で DPD キープアライブ メッセージを送信するかどうか。これによって、間隔値が使用される方法が変更されます。 • [Infinite]：（ASA のみ）間隔と再試行設定を無視するかどうか、およびピアを無制限にアイドル状態にできるかどうか。

要素	説明
ID（Identity）	フェーズ I の IKE ネゴシエーション中に、ピアは相互に識別する必要があります。次のいずれかを選択します。 • [Address]：ISAKMP アイデンティティ情報を交換するホストの IP アドレスを使用します。これがデフォルトです。 • [Hostname]：ISAKMP アイデンティティ情報を交換するホストの完全修飾ドメイン名を使用します。 • [Auto/DN]：デバイス タイプに基づいて自動選択または識別名を使用します。 • [Distinguished Name]（IOS デバイスだけ）：Distinguished Name（DN; 識別名）を使用して、ユーザ グループ名を識別します。 • [Auto]（ASA デバイスだけ）：接続タイプによって ISAKMP ネゴシエーションを決定します。事前共有キーに対しては IP アドレスを、証明書認証に対しては識別名を使用します。
SA Requests System Limit	Cisco IOS ソフトウェア リリース 12.3(8)T 以降を実行しているルータ（7600 ルータを除く）でサポートされます。 IKE が SA 要求の拒否を開始する前に許可される SA 要求の最大数。0 ～ 99999 です。ピアの数以上の値を指定する必要があります。ピアの数未満の値を指定した場合は、VPN トンネルが切断される可能性があります。
SA Requests System Threshold	Cisco IOS ルータおよび Catalyst 6500/7600 デバイスでサポートされます。 IKE が新規 SA 要求の拒否を開始する前に使用できるシステム リソースのパーセンテージ。デフォルトは 75% です。
アグレッシブ モードの有効化（Enable Aggressive Mode） （サイト間 VPN だけ）	ASA デバイスおよび PIX 7.0+ デバイスでサポートされます。 選択されている場合、ISAKMP ネゴシエーションでアグレッシブ モードを使用できます。アグレッシブ モードは、デフォルトでイネーブルになっています。
IPsec 設定	

要素	説明
Enable Lifetime	サイト間またはリモートアクセス VPN のデバイスでクリプト IPsec Security Association（SA; セキュリティ アソシエーション）のグローバル ライフタイム設定を行えるようにする場合は、これを選択します。次を設定します。 • [Lifetime (secs)]：セキュリティ アソシエーションが期限切れになるまでに存続できる秒数。デフォルトは 3,600 秒（1 時間）です。 • [Lifetime (kbytes)]：特定のセキュリティ アソシエーションが期限切れになるまでにそのセキュリティ アソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。デフォルトは 4,608,000 KB です。
Xauth Timeout	リモート アクセス VPN トポロジと Easy VPN トポロジの Cisco IOS ルータおよび Catalyst 6500/7600 デバイスだけでサポートされます。 システムが Xauth チャレンジに応答するまでにデバイスが待機する秒数。 リモート アクセスまたは Easy VPN 設定内に IPsec トンネルを確立するためにトンネル パラメータをネゴシエートする場合、Xauth によって、IPsec 接続を要求するユーザを識別する別の認証レベルが追加されます。Xauth 機能を使用すると、クライアントは IKE SA の確立後、「ユーザ名/パスワード」（Xauth）チャレンジを待機します。エンドユーザがチャレンジに応答すると、その応答は IPsec ピアに転送され、さらに上のレベルの認証が行われます。
最大セッション数（Max Sessions）	ASA デバイスおよび PIX 7.0+ デバイスでサポートされます。 デバイスで同時にイネーブルにできる Security Association（SA; セキュリティ アソシエーション）の最大数。最大数は、デバイス モデルによって異なります。ASA デバイスでは制限は次のとおりです。 • 5505：10 セッション。 • 5510：250 セッション。 • 5520：750 セッション。 • 5540、5550、5585-X（SSP）：10 ～ 5000 セッション。 • 5580、5585-X（その他のモデル）：10000 セッション。

要素	説明
Enable IPsec via Sysopt	ASA デバイスおよび PIX ファイアウォール バージョン 6.3 または 7.0+ でサポートされます。 VPN インターフェイスで VPN トラフィックに対して定義されているアクセス ルールをバイパスするかどうか。 デフォルトでは、デバイスによって VPN トラフィックをインターフェイスで終端させることが許可されています。IKE または ESP（またはその他のタイプの VPN パケット）をインターフェイス アクセス リストで許可する必要はありません。デフォルトでは、復号化された VPN パケットのローカル IP アドレスのインターフェイス アクセス リストも必要ありません。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、設定が簡略化され、デバイスのパフォーマンスはセキュリティ リスクを負うことなく最大化されます。（グループ ポリシーおよびユーザー単位の認可アクセス リストは、引き続きトラフィックに適用されます）。 このオプションの選択を解除すると、インターフェイス アクセス ルールが VPN トラフィックにも適用されます。アクセス リストは、ローカル IP アドレスに適用され、VPN パケットが復号化される前に使用された元のクライアント IP アドレスには適用されません。適用されるコマンドは **no sysopt connection permit-vpn** です。
Enable IPsec inner routing lookup （ASA デバイス 9.6(2) 以降の Security Manager バージョン 4.12 以降）	IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。このチェックボックスは、デフォルトでは選択解除されています。
Enable SPI Recovery （サイト間 VPN だけ）	IOS バージョン 12.3(2)T 以降を実行するルータ、およびバージョン 12.2(18)SXE 以降を実行する Catalyst 6500/7600 デバイスでサポートされます。 選択されている場合、SPI リカバリ機能で、Security Parameter Index（SPI; セキュリティ パラメータ インデックス）が無効であっても IKE SA が開始されるようにデバイスを設定できるようになります。 SPI は、宛先 IP アドレスおよびセキュリティ プロトコルを組み合わせて、特定のセキュリティ アソシエーションを一意に識別する番号です。IKE を使用してセキュリティ アソシエーションを確立する場合、各セキュリティ アソシエーションの SPI は、疑似乱数によって導出された番号となります。IKE を使用しない場合、SPI は、手動で各セキュリティ アソシエーションに指定されます。IPsec パケット処理中に無効な SPI が検出された場合は、SPI リカバリ機能によって、IKE SA が確立されます。

要素	説明
ESPv3 設定（ESPv3 Settings）	
Enable PMTU (Path Maximum Transmission Unit) Aging	ASA デバイスバージョン 9.0.1 以降の IKEv2 でサポートされます。 パスの最大伝送ユニットのエージングをイネーブルにするかどうか。 このオプションを選択した場合、PMTU 値が元の値にリセットされる間隔を分単位で設定します。値は 10 ～ 30 分で設定できます。デフォルトは 10 分です。

VPN グローバル IKEv2 設定

[VPN Global Settings] ページの [IKEv2 Settings] タブを使用して、Internet Key Exchange（IKE; インターネット キー交換）バージョン 2 のグローバル設定を指定します。これらの設定は、ASA 8.4(x) デバイスだけに適用されます。

Internet Key Exchange（IKE; インターネット キー交換）は、Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれ、2 つのホストが IPsec Security Association（SA; セキュリティ アソシエーション）の構築方法に合意するためのネゴシエーション プロトコルです。

IKEv2 オープン SA を制限することで DoS 攻撃を防止

着信 Security Association（SA; セキュリティ アソシエーション）のクッキー チャレンジを常に行うか、オープンな SA の数を制限して追加の接続のクッキー チャレンジを行うことによって、IPsec IKEv2 接続の Denial of Service（DoS; サービス拒否）攻撃を防止できます。デフォルトでは、ASA は、オープンな SA の数を制限せず、SA のクッキー チャレンジを行うことはありません。

許可される SA の数を制限することもできます。これによって、接続がさらにネゴシエーションされないようにして、クッキー チャレンジ機能が阻止できない可能性があるメモリまたは CPU 攻撃から保護します。SA の最大数を制限すると、現在の接続を保護できます。

DoS 攻撃では、攻撃者は、ピア デバイスが SA 初期パケットを送信し、ASA がその応答を送信すると攻撃を開始しますが、ピア デバイスはこれ以上応答しません。ピア デバイスがこれを継続的に行うと、応答を停止するまでASAで許可されるすべてのSA要求を使用できます。

クッキー チャレンジのしきい値パーセンテージをイネーブルにすると、オープンなSAネゴシエーションの数が制限されます。たとえば、デフォルト設定の 50 % では、許可される SA の 50 % がネゴシエーション中（オープン）のときに、ASA は、到着した追加の SA 初期パケットのクッキー チャレンジを行います。10,000 個の IKEv2 SA が許可される Cisco ASA 5580 では、5000 個の SA がオープンになると、その後すべての着信 SA のクッキー チャレンジが行われます。

[ネゴシエーションでの最大SA数（Maximum SAs in Negotiation）] オプションとともに使用する場合は、低いクッキーチャレンジしきい値を設定します。

ナビゲーション パス

- リモート アクセス VPN の場合は、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）] > [グローバル設定（Global Settings）] を選択します。[IKEv2設定（IKEv2 Settings）] 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）] > [グローバル設定（Global Settings）]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[IKEv2設定（IKEv2 Settings）] タブをクリックします。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウを開き、VPN セレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。[IKEv2設定（IKEv2 Settings）] 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で [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか新しい共有ポリシーを作成し、[IKEv2設定（IKEv2 Settings）] タブをクリックします。

関連項目

- VPN グローバル設定 （44 ページ）
- IKE について （6 ページ）
- IPsec プロポーザルについて （26 ページ）
- グループのロードバランスポリシーの設定（ASA）

フィールド リファレンス

表 7: [VPN Global Settings] ページ、[IKEv2 Settings] タブ

要素	説明
Maximum SAs	デバイスで許可される IKEv2 接続（セキュリティ アソシエーション）の数。デフォルトの制限は、デバイス ライセンスによって指定された接続の最大数で、これはデバイス モデルによって異なります。 デバイス ライセンスよりも低い制限を作成する場合にかぎり、数を指定します。範囲は 1 ～ 10000 です。

要素	説明
Maximum SAs in Negotiation	許可される最大の Security Association（SA; セキュリティ アソシエーション）のパーセンテージとして指定する、いつでもネゴシエーション中にできる IKEv2 SA の最大数。デフォルトでは、ネゴシエーション中の SA に関する制限はないため、すべての使用可能な SA をネゴシエーション中にできます。範囲は 1 ～ 100 % です。 このオプションを設定する場合に、カスタムのクッキーチャレンジもイネーブルにするときは、この制限よりも低いクッキーチャレンジしきい値を設定します。
Enable Cookie Challenge	SA 開始パケットの応答としてピア デバイスにクッキー チャレンジを送信するかどうかを指定します。これは、サービス妨害（DoS）攻撃の防止に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキーチャレンジを使用します。次のオプションのいずれか 1 つを選択します。 • [カスタム（Custom）]：ネゴシエーション中の SA の数が、パーセンテージ（ネゴシエーション中の SA が許可された総SA数に対する割合）に基づいて、デバイスで許可された SA の総数を超えると、クッキーチャレンジを行います。[Custom Cookie Challenge] に、将来の SA ネゴシエーションでクッキー チャレンジをトリガーするパーセンテージを入力します。範囲は 1 ～ 100 % です。デフォルトは 50% です。 • [常にしない（Never）]：デバイスではクッキーチャレンジを使用しません。 • [常時（Always）]：デバイスでは、ネゴシエーション中の SA のパーセンテージに関係なく、常にクッキーチャレンジを使用します。
Remote Access Authentication RA Trustpoint （リモート アクセス VPN だけ）	（IKEv2 ネゴシエーションをサポートする場合は必須）デバイスがリモートユーザに対して自身を認証するために使用できる Certificate Authority（CA; 認証局）サーバーを識別する PKI 登録オブジェクト。この認可は、ユーザが接続プロファイルを選択して、VPN にログインする前に必要です。この CA サーバは、リモートアクセス IKEv2 IPsec VPN だけで使用されます。[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） Cisco Security Manager バージョン 4.17 以降、ASA 9.9(2) 以降のマルチコンテキストデバイスでリモートアクセス認証を設定できます。 ヒント この PKI 登録オブジェクトは、[Remote Access VPN] > [Public Key Infrastructure] ポリシーでも選択する必要があります。

要素	説明
Load Balancing Settings Redirect Connections During （リモート アクセス VPN だけ）	ロードバランシングを設定する場合は、[ASAグループロードバランス（ASA Group Load Balance）] ポリシーを使用して、ユーザをグループ内の別のデバイスにリダイレクトできるIKEv2ネゴシエーションフェーズを指定できます。次のオプションのいずれか 1 つを選択します。 • [INIT]：グループまたはユーザ認証の前に、未認証の開始要求（最初の IKEv2 メッセージ IKE_SA_INIT）をリダイレクトします。 • 長所：このオプションを使用すると、メインサーバーは、接続をリダイレクトする前に、最小の処理を行って、（CPU とメモリを使用して）状態を維持できます。 • [Cons]：このオプションは、（セキュリティ リスクは最小ですが）[AUTH] ほどセキュアではありません。これは、誰でも、完全に認証なしでリダイレクトされるIPアドレスを取得できるためです。 • [AUTH]（デフォルト）：認証中（IKE_AUTH 中）にリダイレクトします。デバイスは、この時点ではまだユーザを識別または認証していませんが、クライアントは、サーバを認証して、受信するリダイレクトを信頼できることを確認できます。 • [Pros]：応答は IKEv2 トンネルで暗号化され、クライアント側はサーバを認証してから、リダイレクトされるIPアドレスで試行できるため、このオプションはよりセキュアです。これによって、INITオプションよりもさらにDoSから保護されます。 • [Cons]：このオプションでは、リダイレクト前に IKEv2 トンネルをほとんど起動する必要があるため、さらに処理が必要です。ただし、子 SA とデータ トンネルを起動する必要はありません。クライアントは、まったく認証されません。トンネルの両方の側のグループ認証後に、IKEv1 リダイレクトが行われることに注意してください。
無効なセレクタの通知を有効にする（Enable Invalid Selectors Notification）	着信パケットが、SAのトラフィックセレクタと一致しないSAで受信された場合にIKE通知のピアへの送信をイネーブルにします。この機能は、バージョン9.4(1)以降のASAデバイスで、Security Managerバージョン 4.9 以降で使用できます。
フラグメンテーション設定（Fragmentation Settings）（ASA デバイス 9.6(1) 以降）	

要素	説明
暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation before Encryption）	IKEv2 メッセージのフラグメンテーションをイネーブルにするかどうかを指定します。インターネット キー エクスチェンジ バージョン 2（IKEv2）フラグメンテーション プロトコルは、大きな IKEv2 メッセージを IKE フラグメント メッセージと呼ばれる一連の小さなメッセージに分割します。 フラグメンテーションは、ソフトウェアバージョン 9.6(1) 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。
ローカルMTUサイズ（ASA）（Local MTU Size (ASA)）	MTUサイズの値を入力します。MTUサイズは、クリアテキストパケットをチャンクに分割するために使用されます。使用するMTU値には、IPヘッダー+UDPヘッダーのサイズが含まれます。デフォルトのMTUサイズは 576 です。
フラグメンテーションモード（ASA）（Fragmentation Mode (ASA)）	次のいずれかを選択します。 • [CSCO]：現在のシスコ独自のフラグメンテーション方式を指します。 • [IETF]： IETF 標準で定義されている方式を指します（draft-ietf-ipsecme-ikev2-fragmentation）。デフォルトでは、IETF が選択されています。

VPN での NAT について

ネットワーク アドレス変換（NAT）によって、内部IPアドレスを使用するデバイスがインターネット経由でデータを送受信できるようになります。NAT では、デバイスがインターネット上のデータへのアクセスを試みたときに、プライベートな内部 LAN アドレスが、グローバルにルーティング可能な IP アドレスに変換されます。このように、NAT を使用すると、少ない数のパブリック IP アドレスで多数のホストにグローバル接続を提供できます。

NAT では、ハブアンドスポーク VPN トンネルまたはリモート アクセス接続における安定性が向上します。これは、VPN 接続に必要なリソースが他の目的に使用されず、VPN トンネルが完全なセキュリティを必要とするトラフィックに対して継続して使用可能になるためです。VPN 内部のサイトでは、スプリット トンネル経由で NAT を使用して外部デバイスとセキュアでないトラフィックを交換できます。重要でないトラフィックを VPN トンネル経由で送信することによって、VPN 帯域幅を浪費したり、トンネル ヘッドエンドのハブに過負荷をかけたりすることがありません。

Security Manager では、ダイナミック IP アドレッシングによる NAT だけがサポートされており、ポート レベルの NAT またはポート アドレス変換（PAT）と呼ばれる方式を可能にするオーバーロード機能に適用されます。PAT では、ポート アドレッシングを使用して、何千ものプライベート NAT アドレスが少数のパブリック IP アドレスのグループに関連付けられます。PAT は、ネットワークのアドレッシング要件がダイナミック NAT プールで使用可能なアドレスを超える場合に使用されます。

（注） Cisco IOS ルータで PAT をイネーブルにすると、展開時に、スプリット トンネリングされるトラフィック用に追加の NAT ルールが暗黙的に作成されます。（外部インターフェイスを IP アドレス プールとして使用して）VPN トンネリングされるトラフィックを拒否し、他のすべてのトラフィックを許可するこの NAT ルールは、ルータ プラットフォーム ポリシーとしては反映されません。この機能をディセーブルにすることによって、NAT ルールを削除できます。詳細については、[NAT] ページ - [Dynamic Rules]を参照してください。

サイト間VPNトラフィックでNAT設定を無視するようにトラフィックを設定できます。Cisco IOS ルータで NAT 設定を無視するには、[NATダイナミックルール（NAT Dynamic Rule）] プラットフォームポリシーで [VPNトラフィックを返還しない（Do Not Translate VPN Traffic）] オプションが選択されていることを確認します（[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックスを参照）。PIX ファイアウォールまたは ASA デバイスで NAT を除外するには、[NAT Translation Options] プラットフォーム ポリシーでこのオプションが選択されていることを確認します（[Translation Options] ページを参照）。

NAT 通過について

NAT 通過は、VPN 接続ハブアンドスポークの間にデバイス（中間デバイス）があり、そのデバイスが IPsec フローで NAT を実行する場合に、キープアライブ メッセージの送信に使用されます。

スポークの VPN インターフェイスの IP アドレスがグローバルにルーティング可能でない場合、中間デバイスにおける NAT でこのアドレスが新しいグローバルにルーティング可能な IP アドレスに置換されます。この変更は、IPsec ヘッダーで行われるため、スポークのチェックサムが無効となり、ハブにおけるチェックサムの計算が一致しなくなります。これにより、ハブとスポークとの間の接続が失われます。

NAT 通過を使用すると、スポークでペイロードに UDP ヘッダーが追加されます。中間デバイスにおける NAT では、この UDP ヘッダーの IP アドレスが変更され、IPsec ヘッダーおよびチェックサムは変更されないままとなります。スタティック NAT を使用する中間デバイスでは、（グローバルにルーティング可能な）スタティック NAT IP アドレスを内部インターフェイスに指定する必要があります。スタティック NAT IP アドレスは、そのインターフェイスを通過し NAT を必要とするすべてのトラフィックに提供されます。ただし、NAT IP アドレスが不明なダイナミック NAT を中間デバイスで使用する場合は、スポークからのすべての接続要求に対応できるように、ハブにダイナミック クリプトを定義する必要があります。Security Manager によって、スポークに必要なトンネル設定が生成されます。

（注） NAT 通過は、IOS バージョン 12.3T 以降を実行するルータではデフォルトでイネーブルになっています。NAT 通過機能をディセーブルにする場合は、デバイスで手動でディセーブルにするか、FlexConfig を使用してディセーブルにする必要があります（FlexConfig の管理を参照）。

VPN グローバル NAT 設定 （59 ページ）の説明に従って、[Global VPN Settings] ページの [NAT Settings] タブで、グローバルな NAT 設定を定義できます。

VPN グローバル NAT 設定

[Global Settings] ページの [NAT Settings] タブを使用して、グローバル ネットワーク アドレス変換（NAT）設定を定義します。これにより、内部IPアドレスを使用するデバイスがインターネット経由でデータを送受信できるようになります。

（注） サイト間 VPN では、IOS ルータで NAT 設定を無視する場合は、[NATダイナミックルール（NAT Dynamic Rule）] プラットフォームポリシーで [VPNトラフィックを変換しない（Do Not Translate VPN Traffic）] オプションが選択されていることを確認します（[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックスを参照）。PIX ファイアウォールまたはASA デバイスで NAT を除外するには、[NAT Translation Options] プラットフォーム ポリシーでこのオプションが選択されていることを確認します（[Translation Options] ページを参照）。

ナビゲーション パス

- リモート アクセス VPN の場合は、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）] > [グローバル設定（Global Settings）] を選択します。[NAT設定（NAT Settings）] 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）] > [グローバル設定（Global Settings）]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[NAT設定（NAT Settings）] タブをクリックします。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウを開き、VPN セレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。[NAT設定（NAT Settings）] 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で [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか新しいポリシーを作成し、[NAT設定（NAT Settings）] タブをクリックします。

関連項目

- VPN での NAT について （57 ページ）
- VPN グローバル設定 （44 ページ）

フィールド リファレンス

表 *8 : [VPN Global Settings]* ページ、*[NAT Settings]* タブ

要素	説明
Enable Traversal Keepalive インターバル	NAT 通過キープアライブをイネーブルにするかどうかを指定します。VPN接続ハブとスポークとの間にデバイス（中間デバイス）が配置されている場合、キープアライブ メッセージを転送するためにNAT トラバーサル キープアライブを使用します。このデバイスでは、IPsec フローで NAT を実行します。 このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス間でキープアライブ信号が送信される間隔（秒）を設定します。値は、5 ～ 3600 秒の範囲で指定します。デフォルトは 10 秒です。 （注） Cisco IOS ルータでは、NAT 通過がデフォルトでイネーブルになります。NAT 通過機能をディセーブルにする場合は、デバイスで手動でディセーブルにするか、FlexConfig を使用してディセーブルにする必要があります。
Enable Traversal over TCP TCP ポート（TCP Ports） （リモート アクセス VPN だけ）	ASA および PIX 7.0+ デバイスでサポートされます。 選択すると、IKE プロトコルと IPsec プロトコルの両方が TCP パケット内にカプセル化され、NAT デバイスと PAT デバイスおよびファイアウォールの両方を経由するセキュアなトンネリングがイネーブルになります。 このオプションを選択する場合は、NAT Traversal（NAT-T; NAT 通過）をイネーブルにする TCP ポートを指定します。リモート クライアントおよび VPN デバイスで TCP ポートを設定する必要があります。クライアント設定には、セキュリティ アプライアンスに対して設定したポートを少なくとも 1 つ含める必要があります。最大 10 個のポートを入力できます。 ヒント これらのポートは、IKEv1 接続だけに使用されます。IKEv2 は、NAT-T にポート 500 と 4500 を使用します。指定するすべてのポートが、適切なインターフェイスのアクセスルールで開いていることを確認します。

要素	説明
Enable PAT (Port Address Translation) on Split Tunneling for Spokes （サイト間 VPN だけ）	Cisco IOS ルータおよび Catalyst 6500/7600 デバイスでサポートされます。 選択されている場合、VPN トポロジのスポークで、スプリット トンネリングされるトラフィックでのポート アドレス変換（PAT）の使用がイネーブルになります。 PAT では、ポート アドレッシングを使用して、何千ものプライベート NAT アドレスを少数のパブリック IP アドレスのグループに関連付けることができます。PAT は、ネットワークのアドレッシング要件がダイナミック NAT プールで使用可能なアドレスを超える場合に使用されます。 （注） このオプションを選択する場合、Security Manager では、展開時に、スプリット トンネリングされるトラフィック用に追加の NAT ルールが暗黙的に作成されます。（外部インターフェイスを IP アドレス プールとして使用して）VPN トンネリングされるトラフィックを拒否し、他のすべてのトラフィックを許可するこの NAT ルールは、ルータ プラットフォーム ポリシーとしては反映されません。 ダイナミック NAT ルールをルータ プラットフォーム ポリシーとして作成または編集する詳細については、[NAT] ページ - [Dynamic Rules]を参照してください。

VPN グローバル一般設定

[VPN Global Settings] ページの [General Settings] タブを使用して、サイト間およびリモート アクセス VPN の最大伝送単位（MTU）処理パラメータを含む、フラグメンテーション設定を定義します。

フラグメンテーションでは、パケットの元のサイズをサポートできない物理インターフェイス経由でパケットが送信されるときに、パケットがより小さな単位に分割されます。フラグメンテーションを使用することによって、分割しないと大きすぎて送信できない保護対象パケットを送信できるようになるため、VPN トンネルにおけるパケット損失を最小限に抑えることができます。このことは、特に GRE を使用する場合に当てはまります。IPsec と GRE を組み合わせて使用するとパケットのペイロードに 80 バイトが追加されますが、1420 バイトを超えるパケットにはこのための余裕がヘッダーにないためです。

最大伝送単位（MTU）によって、インターフェイスが処理できる最大パケット サイズがバイト単位で指定されます。通常、パケットが MTU を超える場合は、暗号化のあとにパケットがフラグメント化されます。Do Not Fragment（DF）ビットが設定されている場合、パケットはドロップされます。DF ビットは、デバイスでパケットをフラグメント化できるかどうかを示す、IP ヘッダー内にあるビットです。カプセル化されたヘッダーの DF ビットをデバイスでクリア、設定、またはコピーできるかどうかを指定する必要があります。

暗号化されたパケットを再構築することは困難であるため、フラグメンテーションによってネットワークのパフォーマンスが低下する可能性があります。ネットワークパフォーマンスの

問題を回避するには、[暗号化前のフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）] を選択して、暗号化前にフラグメンテーションが行われるように設定できます。

ナビゲーション パス

- リモート アクセス VPN の場合は、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）] > [グローバル設定（Global Settings）] を選択します。[一般設定（General Settings）] 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）] > [グローバル設定（Global Settings）] を選択します。既存のポリシーを選択するか新しいポリシーを作成してから、[全般設定（General Settings）] タブをクリックします。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウを開き、VPN セレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。[全般設定（General Settings）] 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で [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか新しい共有ポリシーを作成してから、[全般設定（General Settings）] タブをクリックします。

関連項目

- VPN グローバル設定 （44 ページ）

フィールド リファレンス

表 9 : [VPN Global Settings] ページ、[General Settings] タブ

要素	説明
Fragmentation Settings	

要素	説明
Fragmentation Mode Local MTU Size	Cisco IOS ルータおよび Catalyst 6500/7600 デバイスでサポートされます。 フラグメンテーションを行うと、パケットの元のサイズをサポートできない物理インターフェイスを介してパケットが送信されるときの、VPN トンネル内のパケット損失が最小限に抑えられます。フラグメンテーション モードを選択します。 • [フラグメンテーションなし（No Fragmentation）]：IPsec 暗号化の前にフラグメント化しません。カプセル化のあと、デバイスで、MTU 設定を超えるパケットがフラグメント化されたあと、パブリック インターフェイスを介して送信されます。 • [エンドツーエンドMTUの検出（End to End MTU Discovery）]：ICMP メッセージを使用して、最大 MTU を判別します。このオプションは、IPsec VPN で使用します。 エンドツーエンドMTUディスカバリでは、インターネット制御メッセージプロトコル（ICMP）メッセージを使用して、フラグメンテーションを発生させずにホストが VPN トンネルを介してパケットを送信するために使用できる最大 MTU を決定します。送信パス内の各リンクの MTU 設定がチェックされて、送信されるいずれのパケットもそのパス内の最小MTUを超えていないことが確認されます。検出されたMTUを使用して、フラグメンテーションが必要であるかどうかが決定されます。ICMPがブロックされている場合は、MTUディスカバリに失敗し、パケットが失われるか（DF ビットが設定されている場合）、または暗号化のあとにパケットがフラグメント化されます（DF ビットが設定されていない場合）。 （注） （サイト間 VPN）Catalyst 6500/7600 デバイスでは、エンドツーエンドパスMTUディスカバリはイメージ12.2(33)SRA、12.2(33)SRB、12.2(33)SXH、12.2(33)SXI またはそれ以降だけでサポートされています。 • [ローカルMTU処理（Local MTU Handling）]：デバイスでMTUをローカルに設定します。このオプションは通常、ICMPがブロックされているか、サイト間 IPsec/GRE VPN 内にある場合に使用されます。このオプションを選択する場合は、ローカル MTU サイズを指定します。この値には、VPN インターフェイスに応じて 68 ～ 65535 バイトを指定できます。

要素	説明
DF ビット（DF Bit）	Cisco IOS ルータ、Catalyst 6500/7600 デバイス、PIX 7.0+、および ASA デバイスでサポートされます。 IP ヘッダー内の Do Not Fragment（DF）ビットによって、デバイスでパケットのフラグメント化が許可されているかどうかが決定されます。DF ビットの処理方法を選択します。 • [コピー（Copy）]：現在のパケットのカプセル化されたヘッダーの DF ビットを、すべてのデバイスのパケットにコピーします。パケットの DF ビットがフラグメント化を許可するように設定されている場合、以降のすべてのパケットはフラグメント化されます。これがデフォルトのオプションです。 • [設定（Set）]：送信するパケットの DF ビットを設定します。MTU を超える大きなパケットはドロップされ、パケットの送信者に ICMP メッセージが送信されます。 • [クリア（Clear）]：元の DF ビット設定にかかわらず、パケットをフラグメント化します。ICMP がブロックされていると、MTU ディスカバリは失敗し、パケットは暗号化されたあとでだけフラグメント化されます。
暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）	Cisco IOS ルータ、Catalyst 6500/7600 デバイス、PIX 7.0+、および ASA デバイスでサポートされます。 選択されている場合、想定されるパケット サイズが MTU を超えるときには暗号化の前にフラグメント化できます。 Look Ahead Fragmentation（LAF）は、IPsec SA に設定されているトランスフォーム セットに応じて、暗号化後のパケット サイズを計算するために暗号化の実行前に使用されます。パケット サイズが指定した MTU を超える場合は、暗号化の前にパケットがフラグメント化されます。
Enable Notification on Disconnection	ASA および PIX 7.0+ デバイスでサポートされます。 選択されている場合、デバイスは、認定されたピアに、切断されようとしているセッションを通知できます。アラートを受け取ったピアは、理由をデコードし、イベント ログまたはポップアップ ウィンドウにそれを表示します。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。 IPsec セッションがドロップされる理由としては、セキュリティ アプライアンスのシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、管理者による切断などが考えられます。

要素	説明
Enable Split Tunneling （サイト間 VPN だけ）	選択されている場合（デフォルト）、サイト間 VPN トポロジでスプリット トンネリングを設定できます。 スプリット トンネリングを使用すると、同じインターフェイスで、保護されるトラフィックと保護されないトラフィックの両方を送信できます。スプリット トンネリングを使用する場合は、保護対象のトラフィック、およびそのトラフィックの宛先を正確に指定して、指定したトラフィックだけが IPsec トンネルに入り、その他のトラフィックはパブリック ネットワークに暗号化なしで送信されるようにする必要があります。
Enable Spoke-to-Spoke Connectivity through the Hub	ASA および PIX 7.0+ デバイスでサポートされます。 選択すると、ハブアンドスポーク VPN トポロジ内のスポーク間のダイレクト通信がイネーブルになります。ここでのハブは ASA または PIX 7.0+ デバイスです。
Enable Default Route	Cisco IOS ルータおよび Catalyst 6500/7600 デバイスでサポートされます。 選択されている場合、デバイスは、設定された外部インターフェイスをすべての着信トラフィックのデフォルトの発信ルートとして使用します。
[すべてのセッションが終了するまで再起動しない（ASA）（Do not reboot until all the sessions are terminated (ASA)）]	すべてのアクティブセッションが終了するまで、スケジュールされた再起動を ASA で延期する場合は、このオプションを選択します。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） ASA ソフトウェアの **crypto isakmp reload-wait** コマンドは、マルチコンテキストモードの ASA デバイスのシステムコンテキストでのみサポートされます。ただし、VPN 設定ではシステムコンテキストがサポートされないため、Security Manager は、VPN 設定に含まれるマルチコンテキストモードのデバイスに対してこのコマンドを生成しません。マルチコンテキストモードのデバイスで **crypto isakmp reload-wait** コマンドを機能させるには、システムコンテキストで FlexConfig ポリシーを使用する必要があります。FlexConfig ポリシーを使用すると、Security Manager ではサポートされていないデバイス コマンドを設定できます。詳細については、FlexConfig の管理 を参照してください。

サイト間 VPN での IKEv1 事前共有キー ポリシーについて

IKEv1 ネゴシエーションの認証方式として事前共有キーを使用する場合は、2 つのピア間のトンネルごとに共有キーを定義する必要があります。この共有キーは、接続を認証するための共有秘密となります。キーはピアごとに設定されます。トンネルの両方のピアのキーが同じでない場合は、接続を確立できません。事前共有キーの設定に必要なピア アドレスは、VPN トポロジから推定されます。

ヒント　IKEv2 ネゴシエーションに事前共有キーを使用することもできますが、ルールと要件があるため、設定は、IKEv1 に使用する設定とは異なります。IKEv2 ネゴシエーションの事前共有キーの設定については、サイト間 VPN での IKEv2 認証の設定 （94 ページ）を参照してください。

事前共有キーは、スポークに設定されます。ハブアンドスポーク VPN トポロジでは、スポークとハブのキーが同じものになるように、Security Manager によってスポークの事前共有キーがミラーリングされ、割り当てられているハブに設定されます。ポイントツーポイント VPN トポロジでは、両方のピアに同じ事前共有キーを設定する必要があります。完全メッシュ VPN トポロジでは、接続される任意の 2 つのデバイスが同じ事前共有キーを持っている必要があります。

Preshared Key ポリシーでは、特定のキーを使用することも、各通信セッションに参加するピアに対して自動的に生成されたキーを使用することもできます。VPN 内のすべての接続で同じ事前共有キーを使用するとセキュリティが侵害される可能性があるため、自動的にキーを生成する方法（デフォルトの方法）を推奨します。

4.16 以降、Cisco Security Manager は分散モードの Firepower 9300 デバイスの IKEv1 関連の設定をサポートしていません。

デバイスの 1 つがクラスタ分散モード（IKEv2 が設定されている）であり、他のデバイスが非クラスタモード（IKEv1 および IKEv2 が設定されている）である VPN トポロジを検出しているときに、Cisco Security Manager はエラーを表示しません。ただし、プレビュー設定中に、IKEv1 関連の設定を削除するためのアクティビティ検証エラーが表示されます。

キー情報のネゴシエーションおよび IKE Security Association（SA; セキュリティ アソシエーション）の設定には、3 種類の方式があります。

- メイン モード（アドレス）：IP アドレスに基づいてネゴシエーションが行われます。メイン モードは、発信側と受信側の間に 3 つの双方向交換を持つため、最も高いセキュリティを提供します。これはデフォルトのネゴシエーション方式です。

この方式では、キーを作成するための 3 つのオプションがあります。

- 各ピアの一意の IP アドレスに基づいて各ピアに対してキーを作成できます。このオプションを使用すると、高いセキュリティが確保されます。
- ハブアンドスポーク VPN トポロジ内のハブにグループ事前共有キーを作成して、指定したサブネット内の任意のデバイスとの通信で使用できます。各ピアは、デバイスの IP アドレスが不明である場合でも、サブネットによって識別されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、グループ事前共有キーがピアに作成されます。
- ハブアンドスポーク VPN トポロジ内のハブ、またはハブを含むグループに対して、ワイルドカード キーを作成できます。ワイルドカード キーは、スポークが固定 IP アドレスを持っていない場合や、特定のサブネットに属していない場合にダイナミック クリプトで使用されます。ハブに接続するすべてのスポークは同じ事前共有キーを持っているため、セキュリティが侵害される可能性があります。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、ワイルドカード キーがピアに作成されます。

（注） DMVPN にスポーク間での直接接続を設定する場合は、スポークにワイルドカードキーを作成します。

- メインモード（Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名））：IP アドレスに依存しないで、DNS 解決に基づいてネゴシエーションが行われます。このオプションは、ホストで DNS 解決サービスが利用できる場合にだけ使用できます。このオプションは、ダイナミック IP アドレスを使用する、DNS 解決機能を持つデバイスを管理する場合に役立ちます。
- アグレッシブ モード：ホスト名（DNS 解決は行いません）およびドメイン名に基づいてネゴシエーションが行われます。アグレッシブ モードで提供されるセキュリティは、メイン モードよりも低くなります。ただし、ホストの VPN インターフェイスの IP アドレスが不明であり、ダイナミック IP ピアの FQDN が DNS で解決できない場合には、グループ事前共有キーを使用するよりも高いセキュリティが提供されます。このネゴシエーション方式は、GRE ダイナミック IP または DMVPN フェールオーバーおよびルーティング ポリシーでの使用が推奨されます。

関連項目

- 使用する認証方式の決定 （11 ページ）
- IKEv1 事前共有キー ポリシーの設定 （67 ページ）

IKEv1 事前共有キー ポリシーの設定

[IKEv1 Preshared Key] ページを使用して、サイト間 VPN トポロジでの IKEv1 の使用時に事前共有キー設定を定義します。IKEv2 を使用する場合の事前共有キーの設定については、サイト間 VPN での IKEv2 認証の設定 （94 ページ）を参照してください。

（注） Preshared Key ポリシーは、Easy VPN トポロジには適用されません。

（注） 4.16 以降、Cisco Security Manager は、分散モードの Firepower 9300 デバイスの IKEv1 事前共有キー設定をサポートしていません。

[IKEv1 Preshared Key] ページを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ）VPN セレクタでトポロジを選択して、ポリシー セレクタで [IKEv1事前共有キー（IKEv1 Preshared Key）] を選択します。

- （ポリシービュー）ポリシータイプセレクタで[サイト間VPN（Site-to-Site VPN）]>[IKEv1事前共有キー（IKEv1 Preshared Key）]を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

次の表で、このポリシーで定義できる設定について説明します。

表 *10 : [IKEv1 Preshared Key]* ページ

要素	説明
Key Specification キーを手動で定義する（[User Defined]）か、キーを自動的に生成するかを選択します。自動生成キーの使用時に設定できる追加のオプションがあります。	
ユーザー定義	選択されている場合、手動で定義した事前共有キーを使用できます。 [キー（Key）]フィールドに必要な事前共有キーを入力して、[確認（Confirm）]フィールドに再度そのキーを入力します。
Auto Generated	選択されている場合、参加するピアにランダムなキーが割り当てられます。生成されるキーは、ハブとスポークとの間の接続ごとに異なるため、セキュリティが確保されます。[Auto Generated]がデフォルトの選択です。 [Auto generated] は、VPN（たとえば、エクストラネット VPN の場合）内のすべてのノードを管理しないときは有効なオプションではありません。 （注） キーは、デバイスへの最初の展開時に割り当てられ、[Regenerate Key (Only in Next Deployment)] チェックボックスを選択するまでは、同じデバイスに対するそれ以降のすべての展開で常にこのキーが使用されます。
キーの長さ（Key Length）	自動生成する事前共有キーの必要な長さ（1 ～ 127）です。デフォルトは 24 です。
Same Key for All Tunnels	ポイントツーポイント VPN トポロジでは使用できません。 選択されている場合、すべてのトンネルで自動生成された同じキーを使用できます。 （注） このオプションを選択しない場合は、トンネルで異なるキーが使用されます。ただし、DMVPN 設定など、同じネットワーク内の異なるマルチポイント GRE インターフェイスで同じ事前共有キーを使用する必要がある場合を除きます。

要素	説明
Regenerate Key (Only in Next Deployment)	選択されている場合、デバイスに対する次の展開時に Security Manager によって新しいキーが生成されます。キーの機密性が侵害された可能性がある場合に役立ちます。 ジョブを展開用に送信すると、このチェックボックスはクリアされます。新しいキーは、新しい展開に対してだけ生成され、以降の展開では（再度チェックボックスを選択しないかぎり）生成されないため、このチェックボックスがクリアされます。
Negotiation Method ネゴシエーション方式のタイプを選択します。方式については、サイト間 VPN での IKEv1 事前共有キー ポリシーについて （65 ページ）で詳細に説明します。	

要素	説明
Main Mode Address	デバイスのIPアドレスが判明している場合は、このネゴシエーション方式を使用してキー情報を交換します。IPアドレスに基づいてネゴシエーションが行われます。メインモードは、発信側と受信側の間に3つの双方向交換を持つため、最も高いセキュリティを提供します。メインモード（アドレス）がデフォルトのネゴシエーション方式です。 ネゴシエーション アドレス タイプを定義するには、次のいずれかのオプションを選択します。 • [ピアアドレス（Peer Address）]：各ピアの一意のIPアドレスに基づいてネゴシエーションが行われます。キーはピアごとに作成されるため、高いセキュリティが確保されます。これがデフォルトです。 • [サブネット（Subnet）]：ハブアンドスポークトポロジ内のハブでグループ事前共有キーを作成して、指定したサブネット内の任意のデバイスとの通信に使用します。デバイスのIPアドレスが不明な場合でも使用できます。各ピアは、それぞれのサブネットによって識別されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、グループ事前共有キーがピアに作成されます。表示されるフィールドにサブネットを入力します（たとえば、10.10.10.0/24）。 • [ワイルドカード（Wildcard）]：ハブアンドスポークトポロジ内のハブまたはハブのグループに対してワイルドカードキーを作成して、スポークが固定IPアドレスを持っていない場合や、特定のサブネットに属していない場合に使用します。この場合、ハブに接続するすべてのスポークは同じ事前共有キーを持っているため、セキュリティが侵害される可能性があります。ハブアンドスポーク VPN トポロジ内のスポークでダイナミックIPアドレスが使用されている場合にこのオプションを使用します。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、ワイルドカード キーがピアに作成されます。 （注） DMVPN にスポーク間での直接接続を設定する場合は、スポークにワイルドカード キーを作成します。
Main Mode FQDN	IP アドレスが不明であり、デバイスで DNS 解決を使用できる場合は、このネゴシエーション方式を選択してキー情報を交換します。IPアドレスに依存しないで、DNS 解決に基づいてネゴシエーションが行われます。

要素	説明
Aggressive Mode	ハブアンドスポーク VPN トポロジでのみ使用できます。 IP アドレスが不明であり、デバイスで DNS 解決を使用できない可能性がある場合は、このネゴシエーション方式を選択してキー情報を交換します。ホスト名およびドメイン名に基づいてネゴシエーションが行われます。 （注） スポーク間での直接のトンネリングがイネーブルになっている場合には、アグレッシブ モードを使用できません。

関連項目

- サイト間 VPN での IKEv1 事前共有キー ポリシーについて （65 ページ）

Public Key Infrastructure ポリシーについて

Security Manager では、証明書要求を管理し、VPN トポロジ内のデバイスに対して証明書を発行する、Certification Authority（CA; 認証局）サーバでの IPsec 設定がサポートされています。Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）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。これにより、参加するデバイスについてキーを中央で管理できます。

CA サーバ（トラストポイントとも呼ばれます）では、公開 CA 証明書要求を管理して、参加する IPsec ネットワーク デバイスに対して証明書を発行します。IKE プロポーザル ポリシーおよび IPsec プロポーザル ポリシーの認証方式として証明書を使用する場合、ピアは CA サーバからデジタル証明書を入手するように設定されます。CA サーバでは、すべての暗号化デバイス間にキーを設定する必要はありません。代わりに、参加する各デバイスを CA サーバに個別に登録します。CA サーバは、アイデンティティを確認し、デバイスのデジタル証明書を作成することを明示的に信任されています。登録が完了すると、参加する各ピアは、もう一方の参加するピアのアイデンティティを確認し、証明書に含まれている公開キーを使用して暗号化されたセッションを確立できます。

また、CA では、IPsec VPN トポロジに参加しなくなったピアの証明書を無効化することもできます。無効化された証明書は、Online Certificate Status Protocol（OCSP; オンライン証明書状態プロトコル）サーバで管理されるか、または LDAP サーバに格納されている Certificate Revocation List（CRL; 証明書失効リスト）に記載されます。各ピアでは、他のピアからの証明書を受け入れる前に、この CRL をチェックできます。

PKI 登録は、複数の CA で構成される階層型フレームワークに設定できます。階層の最上位にはルート CA があり、自己署名証明書を保持しています。階層全体の信頼性は、ルート CA の RSA キー ペアから導出されます。階層内の下位 CA は、ルート CA または他の下位 CA に登録できます。階層型 PKI 内では、ピア間で信頼できるルート CA 証明書または共通の下位 CA が共有されている場合、登録されたすべてのピアが相互の証明書を確認できます。

次の点を考慮してください。

- PKI ポリシーは、バージョン 12.3(7)T 以降を実行する Cisco IOS ルータ、PIX ファイアウォール、およびサイト間およびリモート アクセス VPN の Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスに設定できます。
- サイト間 VPN では、[IKEv1 Public Key Infrastructure] ポリシーを使用して、IKEv1 ネゴシエーション専用の CA サーバを特定します。IKEv2 ネゴシエーションでは、サイト間 VPN での IKEv2 認証の設定 （94 ページ）の説明に従って、[IKEv2 Authentication] ポリシーで CA サーバを特定します。
- リロード間に RSA キーペアと CA 証明書を PIX Firewall リリース 6.3 のフラッシュメモリに永続的に保存するには、**ca save all** コマンドを設定する必要があります。この操作は、デバイスで手動で行うか、FlexConfig を使用して行うことができます。

CA サーバの認証方式

次のいずれかの方式を使用して CA サーバを認証できます。

- Simple Certificate Enrollment Protocol（SCEP）を使用して、CA サーバーから CA の証明書を取得します。SCEP を使用すると、デバイスと CA サーバとの間に直接接続を確立できます。登録プロセスを開始する前に、デバイスが CA サーバに接続されていることを確認してください。この方式を使用してルータの CA 証明書を取得する場合は、対話形式の操作が必要となるため、PKI ポリシーをライブ デバイスだけに展開できます。ファイルには展開できません。

（注） SCEP を使用する場合は、CA サーバのフィンガープリントを入力する必要があります。入力した値が証明書のフィンガープリントと一致しない場合、証明書は拒否されます。サーバーに直接アクセスして、または Web ブラウザにアドレス（**http://<URLHostName>/certsrv/mscep/mscep.dll**）を入力して、CA のフィンガープリントを取得できます。

- CA サーバーの証明書を他のデバイスからコピーすることによって、オフラインで CA サーバーに送信できる登録要求を手動で作成します。

この方式は、デバイスが CA サーバへの直接接続を確立できない場合、またはいったん登録要求を生成してから、あとで登録要求をサーバに送信する場合に使用します。

（注） この方式を使用すると、デバイスまたはファイルに PKI ポリシーを展開できます。

詳細については、[PKI Enrollment] ダイアログボックス （81 ページ）を参照してください。

（注） Cisco Secure Device Provisioning（SDP; セキュア デバイス プロビジョニング）を使用して、ルータの証明書を登録することもできます。SDP を使用した証明書登録の詳細については、Cisco IOS ルータにおけるセキュア デバイス プロビジョニングを参照してください。

ここでは、公開キー インフラストラクチャ設定についてより詳細に説明します。

PKI 登録を正常に行うための前提条件

ネットワークに PKI ポリシーを設定するためには、次の前提条件が必要です。

- IKEv1 では、IKE プロポーザルで、IKE 認証方式の証明書を指定する必要があります。[IKEv1 Proposal] ポリシー オブジェクトの設定 （14 ページ）を参照してください。
- PKI 登録を正常に行うには、デバイスにドメイン名が定義されている必要があります（CA サーバのニックネームを指定する場合を除く）。
- CA サーバーに直接登録するには、サーバーの登録 URL を指定する必要があります。
- TFTP サーバを使用して CA サーバに登録するには、TFTP サーバに CA 証明書ファイルが保存されている必要があります。PKI ポリシーを展開したあと、TFTP サーバから CA サーバに証明書要求をコピーする必要があります。
- 登録要求で使用する RSA 公開キーを指定できます。RSA キー ペアを指定しない場合は、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）キーが使用されます。

RSA キーを使用する場合は、証明書が承認されると、証明書に公開キーが組み込まれます。ピアは、この公開キーを使用して、デバイスに送信するデータを暗号化できます。秘密キーはデバイスに保持されて、ピアから送信されるデータの復号化、およびピアとのネゴシエーション時のトランザクションのデジタル署名に使用されます。既存のキーペアを使用することも、新しいキー ペアを生成することもできます。ルータ デバイスの証明書で使用する新しいキー ペアを生成する場合は、キーのサイズを特定する係数も指定する必要があります。

詳細については、[PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （88 ページ）を参照してください。

- Cisco Easy VPN IPsec リモート アクセス システムで PKI 登録要求を行う場合は、各リモート コンポーネント（スポーク）に、接続するユーザ グループの名前を設定する必要があります。この情報は、[PKI Enrollment Editor] ダイアログボックスの [Certificate Subject Name] タブにある [Organization Unit (OU)] フィールドで指定します。

（注） ハブ（Easy VPN サーバ）にユーザ グループの名前を設定する必要はありません。

詳細については、[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （92 ページ）を参照してください。

- PKI ポリシーを（ライブ デバイスではなく）ファイルに展開する場合は、次の前提条件を満たしている必要があります。
  - ルータは、Cisco IOS ソフトウェア 12.3(7)T 以降を実行している必要があります。
  - CA 認証が対話形式で行われず、ライブ デバイスとの通信が必要とならないように、CA 認証証明書を Security Manager ユーザ インターフェイスにカット アンド ペーストする必要があります。
- ライブ デバイスに展開する場合、PKI サーバがオンラインである必要があります。
- Security Manager では、Microsoft、VeriSign、および Entrust の PKI がサポートされています。
- Security Manager では、Cisco IOS 証明書サーバがサポートされています。Cisco IOS 証明書サーバ機能では、限定的な CA 機能を持つ簡易証明書サーバが Cisco IOS ソフトウェアに組み込まれます。IOS 証明書サーバは、FlexConfig ポリシーとして設定できます。詳細については、FlexConfig の管理を参照してください。
- IOS ルータにおいて、PKI に被認証者名全体を使用する AAA 認可を設定するには、IOS_PKI_WITH_AAA という名前の定義済み FlexConfig オブジェクトを使用します。

TFTP を使用した PKI 登録の前提条件

CA サーバに継続的に直接アクセスしていない場合は、デバイスが Cisco IOS ソフトウェア 12.3(7)T 以降を実行するルータであれば、TFTP を使用して登録を行うことができます。

展開時に、Security Manager によって対応する CA トラストポイント コマンドおよび認証コマンドが生成されます。トラストポイント コマンドは、TFTP を使用して CA 証明書を取得するための登録 URL tftp://<certserver> <file_specification> のエントリを使用して設定されます。file_specification が指定されていない場合は、ルータの FQDN が使用されます。

このオプションを使用する前に、TFTP サーバに CA 証明書ファイル（.ca）が保存されている必要があります。このためには、次の手順を実行します。

1. http://servername/certsrv に接続します。servername は、アクセスする CA がある Windows 2000 Web サーバの名前です。
2. [CA証明書または証明書失効リストの取得（Retrieve the CA certificate or certificate revocation list）] を選択して、[次へ（Next）] をクリックします。
3. [Base 64エンコード済み（Base 64 encoded）] をクリックして、[CA証明書をダウンロード（Download CA certificate）] をクリックします。
4. ブラウザの別名保存機能を使用して、.crt ファイルを .ca ファイルとして TFTP サーバーに保存します。

展開後、TFTP サーバーの Security Manager が生成した証明書要求を CA に転送し、デバイスの証明書を CA からデバイスに転送する必要があります。

TFTP サーバから CA サーバへの証明書要求の転送

Security Manager によって、TFTP サーバに PKCS#10 フォーマットの登録要求（.req）が作成されます。次の手順を実行して、この登録要求を PKI サーバに転送する必要があります。

1. http://servername/certsrv に接続します。servername は、アクセスする CA がある Windows 2000 Web サーバの名前です。
2. [証明書の要求（Request a certificate）] を選択し、[次へ（Next）] をクリックします。
3. [詳細な要求（Advanced request）] を選択して、[次へ（Next）] をクリックします。
4. [base64エンコード済みPKCS #10ファイルを使用して証明書要求を送信またはbase64エンコード済みPKCS #7ファイルを使用して更新要求を送信（Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file）] を選択して、[次へ（Next）] をクリックします。
5. ファイルの参照を選択して TFTP サーバを参照し .req ファイルを選択するか、または先ほど TFTP で受信した .req ファイルをワードパッドまたはメモ帳で開いてその内容を最初のウィンドウにコピーアンドペーストします。
6. CA から .crt ファイルをエクスポートして、TFTP サーバに配置します。
7. 「crypto ca import <label> certificate」を設定して、tftp サーバーからデバイスの証明書をインポートします。

関連項目

- サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （75 ページ）
- 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 （79 ページ）
- [PKI Enrollment] ダイアログボックス （81 ページ）
- Easy VPN における User Group ポリシーの設定

サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定

Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）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、VPN トポロジ内の参加デバイスに対して証明書を発行するために使用されます。

Security Manager では、CA サーバは、PKI ポリシーで使用できる PKI 登録オブジェクトとして事前に定義されています。PKI 登録オブジェクトには、CA 証明書の登録要求を作成するために必要なサーバ情報および登録パラメータが含まれています。

Public Key Infrastructure ポリシーの詳細については、Public Key Infrastructure ポリシーについて（71 ページ）を参照してください。

この手順では、VPN トポロジで IKEv1 Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーの作成に使用する CA サーバを指定する方法について説明します。

ヒント　IKEv2 ネゴシエーションで使用する CA サーバの指定については、サイト間 VPN での IKEv2 認証の設定　（94 ページ）を参照してください。

はじめる前に

PKI の正常な設定に関する重要な情報については、PKI 登録を正常に行うための前提条件　（73 ページ）を参照してください。

関連項目

- サイト間 VPN での複数の IKEv1 CA サーバの定義　（77 ページ）
- 使用する認証方式の決定　（11 ページ）
- セレクタ内の項目のフィルタリング

ステップ 1　次のいずれかを実行します。

- （[Site-to-Site VPN Manager] ウィンドウ）既存のトポロジを選択して、ポリシーセレクタで [IKEv1公開キーインフラストラクチャ（IKEv1 Public Key Infrastructure）] を選択します。
- （ポリシービュー）**[サイト間VPN（Site-to-Site VPN）] > [IKEv1公開キーインフラストラクチャ（IKEv1 Public Key Infrastructure）]** を選択して、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。

[公開キーインフラストラクチャ（Public Key Infrastructure）] ページが開き、[選択済み（Selected）] フィールドに、現在選択されている CA サーバー（存在する場合）が表示されます。

ステップ 2　[Available CA Servers] リストで必要な CA サーバを定義する PKI 登録ポリシー オブジェクトを選択します。リストされているオブジェクトを変更するには、次の手順を実行できます。

- 新しい PKI 登録オブジェクトを追加するには、[作成（Create）]（+）ボタンをクリックします。[Add PKI Enrollment] ダイアログボックスが開きます。PKI 登録オブジェクトの属性に関する詳細については、[PKI Enrollment] ダイアログボックス　（81 ページ）を参照してください。
- 既存のオブジェクトの設定を変更するには、そのオブジェクトを選択して、[編集（Edit）]（鉛筆）ボタンをクリックします。

（注） Easy VPN トポロジで PKI 登録要求を行う場合は、各リモート コンポーネント（スポーク）に、接続するユーザ グループの名前を設定する必要があります。この情報は、[PKI Enrollment] ダイアログボックスの [Certificate Subject Name] タブにある [Organization Unit (OU)] フィールドで指定します。ハブ（Easy VPN サーバ）にユーザ グループの名前を設定する必要はありません。詳細については、[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （92 ページ）を参照してください。

サイト間 VPN での複数の IKEv1 CA サーバの定義

サイト間 VPN で IKEv1 Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーを定義する場合は、1 つの CA サーバだけを選択できます。このことは、IKEv1 の使用時に VPN 内のデバイスが異なる CA サーバに登録するときに問題となります。たとえば、スポーク デバイスとハブ デバイスとで異なる CA サーバに登録する場合や、VPN のある部分のスポークが VPN の他の部分のスポークとは異なる CA サーバに登録する場合があります。

ヒント IKEv2 の使用時に、PKI 登録ポリシー オブジェクトにデバイス レベルのオーバーライドを作成する代わりに、[IKEv2 Authentication] ポリシー グローバル設定のオーバーライドを作成することによって、さまざまなデバイスに異なる CA サーバを設定できます。ただし、ここでの説明に従って、IKEv2 にデバイス レベルのオーバーライドを使用することもできます。IKEv2 の CA サーバの設定については、サイト間 VPN での IKEv2 認証の設定 （94 ページ）を参照してください。

IKEv1 PKI ポリシーを定義するには、デバイスが登録する CA サーバを指定する PKI 登録オブジェクトを選択します。デフォルトでは、ポリシー オブジェクトは単一の CA サーバをグローバルに参照していますが、デバイス レベルのオーバーライドを使用して、選択したデバイスにおいて異なる CA サーバをオブジェクトが参照するように設定できます。

たとえば、PKI 登録オブジェクト PKI_1 が CA_1 という CA サーバを参照している場合、PKI_1 を持つ選択したデバイスにデバイス レベルのオーバーライドを作成して、CA_2 などの異なる CA サーバを参照できます。理論的には、オーバーライドを使用して、VPN 内の各デバイスに異なる CA サーバを定義することもできます。

この手順では、PKI 登録オブジェクトにオーバーライドを作成するための基本的な手順について説明します。

（注） 共通の信頼できる CA サーバの下の PKI 階層に CA サーバが配置されている場合でも、デバイス レベルのオーバーライドを使用できます。このためには、[PKI Enrollment] ダイアログボックスの [Trusted CA Hierarchy] タブで、オブジェクトのグローバル定義およびデバイス レベルのオーバーライドの両方によって、信頼できる CA サーバが指定されている必要があります。[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （93 ページ） を参照してください。

関連項目

- Public Key Infrastructure ポリシーについて （71 ページ）
- 使用する認証方式の決定 （11 ページ）

ステップ 1 PKI 登録オブジェクトを作成するには、[PKI Enrollment] ダイアログボックスを開きます。このダイアログボックスには、次の 2 つの方法でアクセスできます。

- [公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーから：[選択済み（Selected）] フィールドの下にある [作成（Create）]（+）ボタンをクリックします。 サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （75 ページ）を参照してください。
- Policy Object Manager から（[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択します）：オブジェクトタイプセレクタから [PKI 登録（PKI Enrollments）] を選択して、[新規オブジェクト（New Object）]（+）ボタンをクリックします。

ステップ 2 オブジェクトが参照する CA サーバを含む、PKI 登録オブジェクトのグローバル定義を設定します。[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を必ず選択します。このオプションによって、個別のデバイスでオブジェクトをオーバーライドできるようになります。[PKI Enrollment] ダイアログボックス （81 ページ）を参照してください。

オブジェクトのグローバル定義では、VPN 内の最も多くのデバイスで使用される CA サーバを使用します。これにより、必要となるデバイスレベルのオーバーライドの数を減らすことができます。

ステップ 3 PKI 登録オブジェクトの定義が終了したら、[OK] をクリックします。そのため、次の点に注意してください。

- PKI ポリシーからダイアログボックスにアクセスした場合は、ポリシーページの [Selected] フィールドに新しいオブジェクトが表示されます。
- Policy Object Manager を使用してダイアログボックスにアクセスした場合は、[Policy Object Manager] ウィンドウの作業領域に新しいオブジェクトが表示されます。[Overridable] カラムに緑色のチェックマークが表示されている場合、このオブジェクトに対してデバイスレベルのオーバーライドを作成できることを示しています（このチェック マークは、オーバーライドが実際に存在しているかどうかを示すものではありません）。

ステップ 4 PKI 登録オブジェクトに対してデバイスレベルのオーバーライドを作成します。この処理は、次の 2 つの方法のいずれかで実行できます。

- [デバイスのプロパティ（Device Properties）]（デバイスビューでデバイスが選択された状態で、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択）から：単一のデバイスに対してデバイスレベルのオーバーライドを作成する場合は、このオプションを推奨します。[デバイスのプロパティ（Device Properties）] で、[ポリシー オブジェクト オーバーライド（Policy Object Overrides）] > [PKI 登録（PKI Enrollments）] を選択し、オーバーライドする PKI 登録オブジェクトを選択して、[オーバーライドの作成（Create Override）] ボタンをクリックします。その後、オブジェクトによって定義された CA サーバを含むオーバーライドの内容を定義できます。

詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集を参照してください。

- Policy Object Manager から：このオプションは、複数のデバイスに対して同時にデバイスレベルのオーバーライドを作成する場合に推奨します。[Overridable] カラムの緑色のチェック マークをダブルクリックし、オーバーライドを適用する必要があるデバイスを選択して、オブジェクトによって定義された CA サーバを含むオーバーライドの内容を定義します。

詳細については、複数デバイスのオブジェクト オーバーライドの一括での作成または編集を参照してください。

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

Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）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。

Security Manager では、CA サーバは、PKI ポリシーで使用できる PKI 登録オブジェクトとして事前に定義されています。PKI 登録オブジェクトには、CA 証明書の登録要求を作成するために必要なサーバ情報および登録パラメータが含まれています。

Public Key Infrastructure ポリシーの詳細については、Public Key Infrastructure ポリシーについて（71 ページ）を参照してください。

（注） バージョン 4.12 以降、Cisco Security Manager は、ソフトウェアバージョン 9.5(2) 以降を実行している ASA マルチコンテキストデバイスの公開キー インフラストラクチャ ポリシーのサポートを提供します。

ここでは、リモート アクセス VPN で Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーの作成に使用する CA サーバを指定する方法について説明します。

はじめる前に

次の点を考慮してください。

- PKI の正常な設定に関する重要な情報については、PKI 登録を正常に行うための前提条件（73 ページ）を参照してください。
- IPsec リモートアクセス VPN の [IKEプロポーザル（IKE Proposal）] ポリシーでは、IKEv1 の設定時に証明書認可を必要とする IKE プロポーザルオブジェクトを使用する必要があります。
- ASA または PIX 7.x+ デバイスで定義されるリモート アクセス VPN では、[Public Key Infrastructure] ポリシーは次のポリシーに直接関連していることに注意してください。これ

らのポリシーで定義されるすべてのトラストポイントも [Public Key Infrastructure] ポリシーで選択する必要があります。これはポリシーに自動的に追加されません。最初に、リモート アクセス VPN で必要な PKI 登録オブジェクトを判別するようこれらのポリシーを設定することもできます。

- [接続プロファイル（Connection Profiles）]：CA トラストポイントを使用する必要がある IPsec 接続プロファイルの作成時に、[IPsec] タブでトラストポイントを識別する PKI 登録オブジェクトを選択します。
- [SSL VPNアクセス（SSL VPN Access）]：インターフェイスごとにトラストポイントを設定して、フォールバック トラストポイントも設定できます。
- [グローバル設定、IKEv2設定（Global Settings, IKEv2 Settings）] タブ：IKEv2 IPsec では、グローバルトラストポイントを指定する必要があります。

関連項目

- 使用する認証方式の決定 （11 ページ）
- セレクタ内の項目のフィルタリング

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）]>[公開キーインフラストラクチャ（Public Key Infrastructure）]** 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）]>[公開キーインフラストラクチャ（Public Key Infrastructure）]** 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。

[Public Key Infrastructure] ページが開き、現在使用可能な CA サーバと選択されている CA サーバ（PKI 登録オブジェクト）（存在する場合）が表示されます。

ステップ 2 必要な CA サーバーを定義する PKI 登録ポリシーオブジェクトを [使用可能なCAサーバー（Available CA Servers）] リストで選択して、[>>] をクリックして、[選択済みCAサーバー（Selected CA Servers）] リストに移動します。不要なオブジェクトを削除するには、選択済みリストでオブジェクトを選択して [<<] をクリックします。

（注） [サイト間VPN（Site-to-Site VPN）] で IKEv2 を設定し、認証方式として PKI を選択する場合、ここに表示される必要があるオブジェクト名を [選択済みCAサーバー（Selected CA Servers）] の下で指定する必要があります（サイト間 VPN での IKEv2 認証の設定 （94 ページ）のステップ 2 を参照）。したがって、必要な CA サーバーが [選択済みCAサーバー（Selected CA Servers）] リストに含まれていることを確認してください。

ASA および PIX 7.x+ デバイスでは、選択されている PKI 登録オブジェクトのリストには、リモート アクセス VPN に対して定義されている接続プロファイルで指定されたすべてのオブジェクトが含まれている必要があります。接続プロファイルの詳細については、接続プロファイルの設定（ASA、PIX 7.0+）を参照してください。また、[Global Settings] ポリシーで IKEv2 に対して設定されているすべてのトラストポイントも含まれている必要があります。 VPN グローバル IKEv2 設定 （53 ページ）を参照してください。

リストされているオブジェクトを変更するには、次の手順を実行できます。

- 新しいPKI登録オブジェクトを追加するには、使用可能なサーバーのリストの下にある [作成（Create）]（+）ボタンをクリックします。[Add PKI Enrollment] ダイアログボックスが開きます。PKI 登録オブジェクトの属性に関する詳細については、[PKI Enrollment] ダイアログボックス （81 ページ）を参照してください。
- 既存のオブジェクトの設定を変更するには、いずれかのリストでそのオブジェクトを選択して、[編集（Edit）]（鉛筆）ボタンをクリックします。

[PKI Enrollment] ダイアログボックス

[PKI Enrollment] ダイアログボックスを使用して、Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）登録オブジェクトを表示、作成、コピー、または編集します。PKI 登録オブジェクトは、ネットワーク内のデバイスからの証明書要求に応答する外部 Certification Authority（CA; 証明局）サーバを表します。

PKI 登録オブジェクトを作成して、デバイスが IPsec ネットワークの一部として証明書を交換するときに使用する CA サーバのプロパティを定義します。PKI 登録オブジェクトを作成する場合は、登録用のサーバ名および URL を定義します。このサーバーに登録するデバイスが、Simple Certificate Enrollment Process（SCEP）を使用して CA サーバー独自の証明書を取得するか、またはデバイス設定に手動で入力した証明書を使用するかを指定する必要があります。CA サーバが失効確認に使用するサポート方式も選択する必要があります。

（注） Security Manager でトラストポイントを作成またはインポートするために登録パラメータを定義する必要はありません。

さらに、任意で次を定義できます。

- CA サーバが Registration Authority（RA; 登録局）サーバとして機能するかどうかを指定します。
- 再試行の設定および RSA キー ペアの設定を含む、登録パラメータ。
- 証明書要求に含める追加の属性。
- PKI 階層においてこのサーバの上位に位置する、信頼できる CA サーバのリスト。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [PKI登録（PKI Enrollments）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

ヒント　このダイアログボックスは、リモートアクセスまたはサイト間 VPN の [公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーから開くこともできます。

関連項目

- Public Key Infrastructure ポリシーについて　（71 ページ）
- PKI 登録を正常に行うための前提条件　（73 ページ）
- サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定　（75 ページ）
- サイト間 VPN での IKEv2 認証の設定　（94 ページ）
- 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　（79 ページ）
- Policy Object Manager

フィールド リファレンス

表 11 : [PKI Enrollment] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
[CA Information] タブ	このタブを使用して、認証局サーバ、その証明書、およびその失効確認サポート レベルに関する設定値を入力します。特定の設定については、[PKI Enrollment] ダイアログボックス - [CA Information] タブ（83 ページ）を参照してください。
[Enrollment Parameters] タブ	このタブを使用して、PKI 登録に関する設定を入力します。特定の設定については、[PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ　（88 ページ）を参照してください。 （注）　Security Manager でトラストポイントを作成またはインポートするために登録パラメータを定義する必要はありません。
[Certificate Subject Name] タブ	このタブを使用して、サブジェクト属性など、証明書に含める任意の情報を入力します。特定の設定については、[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ　（92 ページ）を参照してください。

要素	説明
[Trusted CA Hierarchy] タブ	このタブを使用して、階層フレームワークに配置する、信頼できる CA サーバを定義します。特定の設定については、[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （93 ページ）を参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[PKI Enrollment] ダイアログボックス - [CA Information] タブ

[PKI Enrollment] ダイアログボックスの [CA Information] タブを使用して、次のことを実行できます。

- 外部 Certificate Authority（CA; 認証局）サーバの名前と位置を定義する。
- 証明書を手動で貼り付ける（既知の場合）。
- サーバーの失効確認サポートレベルを定義する。

ナビゲーション パス

[PKI 登録（PKI Enrollment）] ダイアログボックスに移動して、[CA 情報（CA Information）] タブをクリックします。このダイアログボックスを開く方法については、[PKI Enrollment] ダイアログボックス （81 ページ）を参照してください。

関連項目

- [PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （88 ページ）
- [PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （92 ページ）
- [PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （93 ページ）

フィールド リファレンス

表 12 : [PKI Enrollment] ダイアログボックス - [CA Information] タブ

要素	説明
CA Server Nickname	証明書要求内の CA サーバの識別に使用する名前。このフィールドを空白のままにすると、ドメイン名が使用されます。Verisign CA の場合は、このフィールドを空白のままにする必要があります。また、次の点を考慮してください。 • 名前は同じであるが、URL が異なる 2 つの CA サーバは、同じデバイス上で設定できません。 • この CA 名は、同じ PKI 登録オブジェクトの一部として設定されている信頼できる CA の名前（[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （93 ページ）で定義）と同じにできません。 • デバイスが VPN の一部として設定されている場合、いずれかのピアで使用される CA サーバ名と同じ CA サーバ名を使用する、デバイスレベルのオーバーライドを設定しないでください（これは、デバイスおよびそのピアが階層化された PKI 階層を使用する場合は問題になりません）。
Enrollment Type	実行する登録のタイプ。Security Manager は、URL 登録を設定している場合にだけ登録を実行します。別のタイプを選択する場合、独自の方法を使用して登録を実行する必要があります。 • [自己署名証明書（Self-Signed Certificate）]（ASA のみ）：**enrollment self** コマンドを設定する場合。 • [端末（Terminal）]（ASA のみ）：**enrollment terminal** コマンドを設定する場合。 • [URL]：CA サーバの URL を設定することで、自動登録を実行する場合。 • [None]：登録コマンドを設定しない場合。
プロトコル	SCEP CA URL または CMP CA URL のどちらを設定するかを指定します。

要素	説明
Enrollment URL （URL 登録のみ）	デバイスが登録を試行する先の CA サーバの URL。この URL は次の形式になります。 • [SCEP]：**http://CA_name:port** の形式の HTTP URL を使用します。ここで、CA_name は CA サーバーのホスト DNS 名または IP アドレスです。ポート番号は必須です。 • [TFTP]：**tftp://certserver/file_specification** の形式を使用します。CA サーバに直接アクセスできないときにこのオプションを使用します。TFTP サーバが、証明書要求および証明書を転送します。 • サポートされているその他の形式には、bootflash、cns、flash、ftp、null、nvram、rcp、scp、system などがあります。 （注） CA での CA cgi-bin スクリプト位置がデフォルト（/cgi-bin/pkiclient.exe）でない場合は、その標準以外のスクリプト位置を **http://CA_name:port/script_location** の形式で URL に含める必要があります。ここで、script_location は CA スクリプトへのフルパスです。

要素	説明
CA Certificate Source フィンガープリント（Fingerprint） 証明書 （URL 登録のみ）	証明書の取得方法： • [SCEP を使用した CA 証明書の取得（Retrieve CA Certificate Using SCEP）]（デフォルト）：ルータが、Simple Certificate Enrollment Process（SCEP）を使用して CA サーバーから証明書を取得するようにします。CA サーバのフィンガープリントを 16 進数形式で入力します。入力した値が証明書のフィンガープリントと一致しない場合、証明書は拒否されます。 フィンガープリントを使用して CA の証明書の真正性を確認すると、不正な第三者が、本物の証明書を偽の証明書に置き換えることを阻止できます。 **ヒント** サーバーに直接アクセスして、または Web ブラウザにアドレス（**http://URLHostName/certsrv/mscep/mscep.dll**）を入力して、CA のフィンガープリントを取得できます。フィンガープリントの使用は、Cisco IOS ソフトウェアリリース 12.3(12) 以降、12.3(14)T 以降、12.4 以降（15.x を含む）、12.2(33)XNA 以降だけでサポートされます。 • [CA サーバーからの CA 証明書を手動で入力する（Enter CA Certificate from CA Server Manually）]：別のデバイスから最大 3 つの証明書をコピーし、[証明書（Certificate）] フィールドに貼り付けます（ブラウザの貼り付け機能、またはキーボードショートカット Ctrl+V を使用します）。PKI 登録オブジェクトが定義済み証明書を表すようにするには、このオプションを使用します。各証明書は、「certificate」という単語で始まり、「quit」という単語で終わる必要があります。CMP 認証では、認証に Base 64 でエンコードされた CA 証明書が必要です。CMP の場合、このフィールドで、Base 64 でエンコードされた CA 証明書を設定できます。Base 64 でエンコードされた CA 証明書を CA サーバーからコピーして貼り付け、最後に「quit」という単語を付けます。 **（注）** 証明書の詳細を「-----BEGIN CERTIFICATE----」という文字列と「----END CERTIFICATE----」という文字列の間に入力します。
CA 証明書のチェック	デフォルトでは、CA フラグのない証明書を CA 証明書として ASA にインストールできなくなりました。基本制約拡張は、証明書のサブジェクトが CA で、この証明書を含む有効な認証パスの最大深さかどうかを示すものです。バージョン 4.9 以降、Security Manager を使用すると、必要に応じて、これらの証明書のインストールを許可するように ASA 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。 デフォルトでは CA 証明書のチェックは有効になっています。

要素	説明
Revocation Check Support	実行する証明書失効確認のタイプ。 • [Checking Not Performed]：これがデフォルトです。デバイスは、CRL がデバイス上に存在する場合も、失効確認を実行しません。 • [CRL Check Required]：デバイスは CRL を確認する必要があります。デバイス上に CRL が存在せず、デバイスが CRL を取得できない場合、証明書は拒否され、トンネルは確立されません。 • [OCSP Check Required]：デバイスは、OCSP サーバからの失効ステータスをチェックする必要があります。チェックに失敗すると、その証明書は拒否されます。 • [CRL Check Attempted]：デバイスは、指定された LDAP サーバから最新の CRL をダウンロードしようとします。ダウンロードに失敗しても、証明書は受け入れられます。 • [OCSP Check Attempted]：デバイスは、OCSP サーバからの失効ステータスをチェックしようとします。チェックに失敗した場合でも、証明書は受け入れられます。 • [CRL or OCSP Check Required]：デバイスは最初に CRL に対するチェックを行います。CRL が存在しない、または取得できない場合、デバイスは OCSP サーバからの失効ステータスをチェックしようとします。両方のオプションが失敗した場合、証明書は拒否されます。 • [OCSP or CRL Check Required]：デバイスは、最初に OCSP サーバからの失効ステータスをチェックしようとします。このチェックが失敗すると、デバイスは CRL をチェックします。両方のオプションが失敗した場合、証明書は拒否されます。 • [CRL and OCSP Checks Attempted]：デバイスは、最初に CRL をチェックします。CRL が存在しない、または取得できない場合、デバイスは OCSP サーバからの失効ステータスをチェックしようとします。両方のオプションが失敗した場合でも、証明書は受け入れられます。 • [OCSP and CRL Checks Attempted]：デバイスは、最初に OCSP サーバからの失効ステータスをチェックしようとします。このチェックが失敗すると、デバイスは最新の CRL をダウンロードしようとします。両方のオプションが失敗した場合でも、証明書は受け入れられます。
OCSP Server URL	OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。この URL は、**http://** で始まる必要があります。

要素	説明
CRL Server URL	CRL チェックを必須としている場合に、CRL をダウンロードできる LDAP サーバの URL。この URL は、**ldap://** で始まる必要があります。 （注） AAA サーバを ASA デバイスで使用する場合は、ポート番号を URL に含める必要があります。含めないと、LDAP が失敗します。
Enable Registration Authority Mode (PIX 6.3)	PIX 6.3 デバイスの場合に、CA サーバが Registration Authority（RA; 登録局）モードで動作するかどうかを指定します。登録局は、実際の CA のプロキシとして動作するサーバであるため、CA サーバがオフラインの場合でも CA の運用を続行できます。 （注） Cisco IOS ルータは、必要に応じて、RA モードを自動的に設定します。

[PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ

[PKI Enrollment] ダイアログボックスの [Enrollment Parameters] タブを使用して、デバイスが CA サーバに接続するときに使用する再試行設定、および証明書に関連付ける RSA キー ペアを生成するための設定を定義します。

PKI 登録オブジェクトが Microsoft CA を表す場合、ルータのアイデンティティの検証に必要なチャレンジパスワードを定義できます。

（注） Security Manager でトラストポイントを作成またはインポートするために登録パラメータを定義する必要はありません。

ナビゲーション パス

[PKI登録（PKI Enrollment）] ダイアログボックスに移動して、[登録パラメータ（Enrollment Parameters）] タブをクリックします。このダイアログボックスを開く方法については、[PKI Enrollment] ダイアログボックス （81 ページ）を参照してください。

関連項目

- [PKI Enrollment] ダイアログボックス - [CA Information] タブ （83 ページ）
- [PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （92 ページ）
- [PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （93 ページ）

フィールド リファレンス

表 13 : [PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ

要素	説明
Challenge Password 確認（Confirm）	CA サーバがデバイスの ID を検証するために使用するパスワード。このパスワードは、PIX 6.3 デバイスの場合は必須ですが、PIX/ASA 7.0+ デバイスおよび Cisco IOS ルータの場合は任意です。 CA サーバに直接アクセスして、または Web ブラウザにアドレス（**http://URLHostName/certsrv/mscep/mscep.dll**）を入力して、パスワードを取得できます。このパスワードは、CA サーバから取得した時間から 60 分間有効です。したがって、パスワードは、作成後、できるだけ迅速に配布する必要があります。 （注） 各パスワードは、単一デバイスごとの単一登録に対して有効です。このため、VPN の各デバイスにデバイスレベルのオーバーライドを最初に設定している場合を除き、このフィールドが VPN に対して定義されている PKI 登録オブジェクトを割り当てることは推奨しません。詳細については、個々のデバイスのポリシーオブジェクト オーバーライドについてを参照してください。
Retry Period	証明書要求の試行間隔（分数）。値には 1 ～ 60 分を指定できます。デフォルトは 1 分です。
再試行回数（Retry Count）	最初の要求時に証明書が発行されていない場合、実行する再試行回数。値には 1 ～ 100 を指定できます。デフォルトは 10 です。
Certificate Auto-Enrollment （IOS デバイスのみ）	現在の証明書のライフタイムのパーセンテージです。ルータは、このパーセンテージに達してから新しい証明書を要求します。たとえば、70 を入力した場合、ルータは、現在の証明書のライフタイムが 70% に達成したあとに、新しい証明書を要求します。値の範囲は 10 ～ 100 % です。 値を指定しない場合、ルータは、古い証明書が期限切れになってから、新しい証明書を要求します。
自動登録の有効化（Enable Auto-Enrollment）	有効にすると、設定可能なトリガーに基づいて証明書が自動的に要求されます。 次の具体的なパラメータを設定することもできます。 • CMPv2 アップデートを使用するかどうか • いつトリガーするか • 現在のキーペアが使用されるか、新しいキーペアが生成されるか

要素	説明
Certificate Auto-Enrollment （ASA 9.7.1 以降）	現在の証明書のライフタイムのパーセンテージです。ルータは、このパーセンテージに達してから新しい証明書を要求します。たとえば、50 と入力した場合、ルータは、現在の証明書のライフタイムが 50% に達してから新しい証明書を要求します。値の範囲は 10 ～ 99% です。 値を指定しない場合、ルータは、古い証明書が期限切れになってから、新しい証明書を要求します。 （注） デフォルト値は 70% です。
自動登録再生成キー（Auto Enroll Regenerate Key）（ASA 9.7.1 以降）	選択して、証明書を更新する際に新しいキーを生成します。
キー ペアの再生成（Regenerate Key Pair）（ASA 9.7.1 以降）	選択して、トラストポイント要求を登録する前に、新しいキー ペアを再生成します。
共有キー（Shared Key）（ASA 9.7.1 以降）	アウトオブバンドで CA から取得したユーザーログイン情報を指定します。この情報は、CA および ASA が交換するメッセージの信頼性および整合性を確認するために使用されます。キー長は、64 文字以下です。 （注） 共有キーは「参照:共有キー」の形式にする必要があります。
証明書の署名（Signing Certificate）（ASA 9.7.1 以降）	CMP 登録要求に署名するために使用された、以前の発行済みデバイス証明書を含むトラストポイントの名前を指定します。
（注） CMP プロトコルの場合、セキュリティ上の理由から、[証明書（Certificate）]、[共有キー（Shared Key）]、[証明書の署名（Signing Certificate）] などのオプションは検出されません。その結果、PKI 登録ダイアログでは再検出時にオーバーライドが作成されます。	
キーペア（Key Pair）	すべての CMP 手動および自動登録用に自動的に新しいキーペアが生成されます。この機能をサポートするために、トラストポイントでキーペアパラメータを設定する機能が追加されました。 キー ペアの生成に使用するアルゴリズム（RSA または EDCSA）を選択します。 （注） RSA アルゴリズムには、係数オプション（1024| 2048| 4096| 512|768）があります。EDCSA アルゴリズムには、キーペアを生成するための楕円曲線オプション（256|384|521）があります。

要素	説明
デバイスのシリアル番号を含める（Include Device's Serial Number）	デバイスのシリアル番号を証明書に含めるかどうかを指定します。 ヒント　CA は、このシリアル番号を使用して、証明書を認証するか、またはあとで証明書を特定のデバイスに関連付けます。シリアル番号を含めるかどうか判断できない場合は、デバッグに役立つため、含めてください。
RSA Key Pair Name （PIX 7.0+、ASA、IOS デバイスのみ）	証明書に関連付けるキー ペアがすでに存在する場合、このフィールドでは、そのキー ペアの名前を指定します。 キー ペアが存在しない場合、このフィールドでは、登録時に生成されるキー ペアに割り当てる名前を指定します。 （注）　RSA キー ペアを指定しない場合、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）が代わりに使用されます。PIX デバイスおよび ASA デバイスでは、展開の前にデバイス上にキー ペアが存在する必要があります。
RSA Key Size （IOS デバイスのみ）	キー ペアが存在しない場合は、必要なキー サイズ（係数）をビットで定義します。512 ～ 1024 の係数が必要な場合は、64 の倍数となる整数を入力します。1024 よりも大きい値が必要な場合は、1536 または 2048 を入力します。推奨サイズは 1024 です。 （注）　係数のサイズが大きくなるほど、キーがよりセキュアになります。ただし、係数のサイズが大きいキーほど、生成に時間がかかり（512 ビットより大きい場合は 1 分以上）、交換するときの処理にも時間がかかります。
RSA Encryption Key Size （IOS デバイスのみ）	個別の暗号化、シグニチャ キー、および証明書を要求する場合に使用する、2 番めのキーのサイズ。

要素	説明
送信元インターフェイス（Source Interface） （IOS デバイスおよび ASA 9.5(1) 以降）	認証中、登録中、および失効リストの取得時に、CA または LDAP サーバに送信されるすべての発信接続の送信元アドレス。このパラメータは、CA サーバまたは LDAP サーバが、（ファイアウォールなどが原因で）接続の生成元のアドレスに応答できない場合に必要となる場合があります。 このフィールドで値を定義しない場合、発信インターフェイスのアドレスが使用されます。 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します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） Cisco Security Manager 4.9 は、ASA 9.5(1) 以降を実行しているデバイスの管理トラフィック用に個別のルーティングテーブルをサポートしています。この機能により、ASA 上の他のデータトラフィックから管理トラフィックを完全に分離できます。IOS デバイスとは別に、ソフトウェアバージョン 9.5(1) 以降を実行している ASA デバイスを選択できるようになりました。

[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ

[PKI Enrollment] ダイアログボックスの [Certificate Subject Name] タブを使用して、CA サーバに送信される証明書要求内のデバイスに関する追加情報を任意で定義します。この情報は、証明書に格納され、このルータから証明書を受信するすべての第三者が表示できます。

標準の LDAP X.500 形式を使用して、すべての情報を入力します。

ナビゲーション パス

[PKI登録（PKI Enrollment）] ダイアログボックスに移動して、[証明書のサブジェクト名（Certificate Subject Name）] タブをクリックします。このダイアログボックスを開く方法については、[PKI Enrollment] ダイアログボックス （81 ページ）を参照してください。

関連項目

- [PKI Enrollment] ダイアログボックス - [CA Information] タブ （83 ページ）
- [PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （88 ページ）
- [PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （93 ページ）

フィールド リファレンス

表 *14 : [PKI Enrollment]* ダイアログボックス - *[Certificate Subject Name]* タブ

要素	説明
FQDN を含める	デバイスの完全修飾ドメイン名（FQDN）を証明書要求に含めるかどうかを指定します。 この名前は、[Hostname] ポリシーから取得されます（有効な完全修飾ドメイン名を取得するには、このポリシーでホスト名とドメイン名の両方を必ず指定してください）。ホスト名ポリシーを設定しない場合、この名前は Security Manager のデバイスの表示名 *display_name***.null** から取得されますが、望ましい結果を得られない可能性が高くなります。
デバイスの IP アドレスを含める	IP アドレスが証明書要求に含まれてい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の名前を入力するか、[選択（Select）]をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。
Common Name（CN）	証明書に含める X.500 共通名。
Organization Unit (OU)	証明書に含める組織単位の名前（部門名など）。 （注） Cisco Easy VPN Remote コンポーネントの PKI 登録オブジェクトを設定する場合、このフィールドには、コンポーネントが接続するクライアント グループの名前を含める必要があります。含めないと、このコンポーネントは接続できません。ただし、この情報は、設定の問題は発生しないなどの理由から、Easy VPN サーバでは必須ではありません。Easy VPN の詳細については、Easy VPN についてを参照してください。
Organization（O）	証明書に含める組織名または会社名。
Locality（L）	証明書に含める都市。
州（State）（ST）	証明書に含める州。
Country（C）	証明書に含める国。
Email (E)	証明書に含める電子メール アドレス。

[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ

[PKI Enrollment] ダイアログボックスの [Trusted CA Hierarchy] タブを使用して、階層 PKI フレームワーク内に信頼できる CA サーバを定義します。このフレームワーク内で、すべての登録済

みピアは、信頼できるルート CA 証明書または共通の下位 CA を共有している場合、互いの証明書を検証できます。

（PKI 登録オブジェクトとして定義されている）CA サーバを選択して [Available Servers] リストの階層に含め、[>>] をクリックしてそれらのサーバを選択済みリストに移動します。サーバを削除するには、この反対を実行します。

必要な PKI 登録オブジェクトをまだ定義していない場合は、使用可能なサーバーリストの下の [作成（Create）]（+）ボタンをクリックして、オブジェクトを作成します。必要な場合は、オブジェクトを選択し、[編集（Edit）] ボタンをクリックして、オブジェクトの定義を変更することもできます。

ナビゲーション パス

[PKI登録（PKI Enrollment）] ダイアログボックスに移動して、[信頼できるCA階層（Trusted CA Hierarchy）] タブをクリックします。このダイアログボックスを開く方法については、[PKI Enrollment] ダイアログボックス （81 ページ）を参照してください。

関連項目

- [PKI Enrollment] ダイアログボックス - [CA Information] タブ （83 ページ）
- [PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （88 ページ）
- [PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （92 ページ）

サイト間 VPN での IKEv2 認証の設定

サイト間 VPN で IKE Version 2（IKEv2; IKE バージョン 2）を設定する場合は、認証設定を定義するよう [IKEv2 Authentication] ポリシーを設定する必要があります。IKEv1 と異なり、認証設定は、IKEv2 プロポーザルの一部ではありません。

Security Manager では、サイト間 VPN の IKEv2 認証を設定する際に、VPN トポロジで使用するデフォルト設定を行います。例外をデフォルトに設定して、VPNの特定のセグメントに異なる事前共有キーまたはトラストポイントを指定できます。事前共有キーとトラストポイントの混合を使用できます。たとえば、グローバル事前共有キーを設定して、VPN の選択したメンバーにはトラストポイントを設定できます。

IKEv2 トンネルの非対称認証の設定

IKEv2 を使用すると、IKEv1 とは異なり非対称認証を使用できます。これは、2 つのピアが、異なる事前共有キーまたは異なるトラストポイントを使用したり、1 つのピアが事前共有キーを使用して、他のピアがトラストポイントを使用したりできることを意味します。Security Manager では、次の操作を行って、非対称認証を設定できます。

- [グローバルIKEv2認証設定（Global IKEv2 Authentication Settings）] タブで、自動生成キーを選択して、[すべてのトンネルに同じキー（Same Keys for All Tunnel）] または [トンネルのエンドポイントに同じキー（Same Key at Tunnel Endpoints）] オプションを選択**しない**場

合は、異なる事前共有キーを設定できます。各トンネルの終端ごとに異なる事前共有キーが生成されます。

- [Override IKEv2 Authentication Settings] タブで、グローバル設定のオーバーライドを作成できます。ローカル ピアとリモート ピアのサブセットに異なるキーまたはトラストポイントを指定するオーバーライドを追加します。デバイスまたは特定のトンネルに複数のオーバーライドを作成できるため、ピアが認証する事前共有キーとトラストポイントのセットを設定できます。

ヒント [IKEv2 Authentication] ポリシーは共有ポリシーではありません。IKEv2 ネゴシエーションをサポートする VPN トポロジごとにポリシーを設定する必要があります。すべての VPN トポロジで使用するグローバル IKEv2 認証オプションは設定できません。[Create VPN] ウィザードの使用時に、IKEv2 をサポートするよう選択する場合でも、[IKEv2 Authentication] ポリシーが設定されることはありません。

はじめる前に

[IKEv2 Authentication] ポリシーは、[IKE Proposal] ポリシーと [IPsec Proposal] ポリシーの VPN で IKEv2 をイネーブルにする場合、およびトポロジ内の少なくとも一部のデバイスが IKEv2 をサポートする場合にかぎり使用されます。

IKEv2 を設定するには、デバイスは、ASA ソフトウェアリリース 8.4(1) 以降が実行されている ASA でなければなりません。デバイス サポートの詳細については、各 IPsec テクノロジーでサポートされるデバイスについてを参照してください。

ヒント トポロジで IKEv2 だけをサポートする場合は、検証の警告を回避するために、[IKEv1 Preshared Keys] ポリシーと [IKEv1 Public Key Infrastructure] ポリシーの割り当てを解除してください。

関連項目

- IKE について （6 ページ）
- 使用する認証方式の決定 （11 ページ）

ステップ 1 [Site-to-Site VPN Manager] ウィンドウを開き、VPN セレクタで（IKEv2 をサポートする）通常の IPsec トポロジを選択して、ポリシーセレクタで [IKEv2認証（IKEv2 Authentication）] を選択します。

ポリシーの参照情報については、 [IKEv2 Authentication] ポリシー （97 ページ）を参照してください。

ステップ 2 [グローバルIKEv2認証設定（Global IKEv2 Authentication Settings）] タブで、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブでオーバーライドが設定されていない VPN 内のデバイスに使用する必要がある認証タイプを設定します。VPN 内のほとんどのデバイスで使用されるオプションを選択します。グローバル事前共有キーまたはトラストポイントを設定できます。

- [グローバル事前共有キー（Global Preshared Keys）]：グローバル事前共有キーを設定するには、[キーの仕様（Key Specification）] を選択して、次のいずれかのオプションを設定します。
  - [User Defined]：必要なグローバル キーを入力して、[Confirm] フィールドに再度入力します。
  - [Auto Generated]：生成する必要があるキーの長さを入力して、すべてのトンネルに同じキーを使用するか、単一のトンネルの両方の終端で同じキーを使用するかを選択します。いずれのオプションも選択しない場合は、すべてのエンド ポイントで固有のキーが生成されます。

新しいキーを生成するには、[キーの登録（次回の展開時）（Regenerate Key (On Next Deployment)）] を選択することもできます。これによって、VPN のキーを定期的に再生成できます。このチェックボックスは、次回に展開が正常に行われたあとでオフにされます。

- [グローバルトラストポイント（CAサーバー）（Global Trustpoint (CA Servers)）]：トラストポイント証明書認可を設定するには、[PKIの仕様（PKI Specification）] を選択して、認証局（CA）サーバーを識別する PKI 登録オブジェクトの名前を入力します。

（注） PKIポリシーで展開されたものと同じオブジェクト名を入力していることを確認します（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 （79 ページ）のステップ 2 を参照）。

[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。

- [IKEv2認証ペイロードにSHA1で署名（Sign IKEv2 Authentication Payload with SHA1）]：IKEv2 ペイロードで SHA1 認証を有効にするには、このチェックボックスをオンにします。このオプションは、Cisco Security Manager 4.19 および ASA 9.12(1) 以降のデバイスでのみ使用できます。

ステップ 3 特定のデバイスのグローバル IKEv2 認証設定をオーバーライドする場合は、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブをクリックして、次のいずれかを実行します。

- オーバーライドを追加するには、[行の追加（+）（Add Row (+)）] ボタンをクリックし、[IKEv2認証（IKEv2 Authentication）] ダイアログボックスに入力します。オーバーライドを作成するローカル ピアとリモート ピアを選択して、使用する必要がある CA サーバの事前共有キーを指定します。[IKEv2 Authentication (Override)] ダイアログボックス （99 ページ）を参照してください。
- オーバーライドを編集するには、テーブルでそのオーバーライドを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- オーバーライドを削除するには、テーブルでオーバーライドを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

（注） オーバーライド IKEV2 認証設定は、ハブアンドスポーク VPN およびフルメッシュ VPN トポロジにのみ適用されます。

（注） サイト間 VPN で非対称認証を設定できます。ここでは、トンネルの両側で異なる事前共有キーを使用できます。サイト間トポロジの一部であるピアデバイスごとに、IKEv2 認証用の非対称キーを作成するには、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブに 2 つの行を追加する必要があります。詳細については、[IKEv2 Authentication (Override)] ダイアログボックス （99 ページ）を参照してください。

[IKEv2 Authentication] ポリシー

[IKEv2 Authentication] ポリシーを使用して、サイト間 VPN で Internet Key Exchange（IKE; インターネット キー交換）バージョン 2 のデバイス認証設定を行います。これらの設定は、ASA 8.4(1)+ デバイスだけに適用されます。IKEv2 認証の設定の詳細については、サイト間 VPN での IKEv2 認証の設定 （94 ページ）を参照してください。

ポリシーには 2 つのタブが含まれています。

- [Global IKEv2 Authentication Settings]：グローバル設定は、[Overrides] タブでオーバーライドが設定されている場合を除き、VPN 内のすべてのデバイスに適用されます。VPN 内のほとんどのデバイスで使用される認証スキームを表すグローバル設定を行います。
- [Override IKEv2 Authentication Settings]：オーバーライド設定によって、固有の認証設定が特定のトンネルに適用され、VPN 内のさまざまなトンネルで必要な固有の事前共有キーとトラストポイントの組み合わせを作成できます。このタブで行う設定は、最初に使用され、常にグローバル設定に優先されます。

ナビゲーション パス

[Site-to-Site VPN Manager] ウィンドウを開き、VPN セレクタで（IKEv2 をサポートする）通常の IPsec トポロジを選択して、ポリシーセレクタで [IKEv2認証（IKEv2 Authentication）] を選択します。

このポリシーは、共有ポリシーとしては使用できません。

関連項目

- IKE について （6 ページ）
- サイト間 VPN の IPsec プロポーザルについて （27 ページ）
- テーブルのフィルタリング
- テーブル カラムおよびカラム見出しの機能

フィールド リファレンス

表 *15 : [IKEv2 Authentication]* ポリシー

要素	説明
[Global IKEv2 Authentication Settings] タブ	
Key Specification	VPN での認証に事前共有キーを使用します。次のいずれかを設定します。 • [ユーザー定義（User Defined）]：必要なグローバルキーを入力して、[確認（Confirm）] フィールドに再度入力します。キーは 1 ～ 128 文字の範囲で指定できます。 • [自動生成（Auto Generated）]：Security Manager にキーを生成させます。キーを生成する方法を示す次のオプションを指定します。 • [キーの長さ（Key Length）]：生成するキーの長さ（1 ～ 128）。 • [すべてのトンネルに同じキーを生成（Same Keys for All Tunnels）]：VPN 内のすべてのトンネルに同じキーを生成するには、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は、トンネルごとに異なるキーまたはキー ペア（[Same Key for Tunnel Endpoints] を選択した場合）が使用されます。 • [トンネルエンドポイントに同じキーを生成（Same Key for Tunnel Endpoints）]：VPN 内の各トンネルの各終端で同じキーを生成するには、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は、トンネルの各終端で異なるキーが生成されます。 • [キーの再生成（次の展開時）（Regenerate Key (On Next Deployment)）]：デバイスへの次の展開で新しいキーを生成するには、このオプションを選択します。これによって、VPN のキーを容易に再生成できます。 展開が正常に行われたあとで、後続の展開でキーが再生成されないように、このチェックボックスはオフにされます。VPN のキーを再生成するたびに、このオプションを選択します。
PKI Specification	IKEv2 接続のトラストポイントを定義する 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。PKI 登録オブジェクトを選択する場合や、新しいオブジェクトを作成する場合は、[選択（Select）] をクリックします。

要素	説明
[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブ	このテーブルには、VPNに対して定義されているIKEv2認証オーバーライドがリストされます。これらのポリシーは、グローバル設定で定義された事前共有キーまたはPKI設定に優先されます。オーバーライドを設定するには、次のいずれかを実行します。 • オーバーライドを追加するには、[行の追加（+）（Add Row (+)）] ボタンをクリックし、[IKEv2認証（IKEv2 Authentication）] ダイアログボックスに入力します。オーバーライドを作成するローカルピアとリモートピアを選択して、使用する必要がある CA サーバの事前共有キーを指定します。 [IKEv2 Authentication (Override)] ダイアログボックス （99 ページ）を参照してください。 • オーバーライドを編集するには、テーブルでそのオーバーライドを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • オーバーライドを削除するには、テーブルでオーバーライドを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。 （注） サイト間 VPN で非対称認証を設定できます。ここでは、トンネルの両側で異なる事前共有キーを使用できます。サイト間トポロジの一部であるピアデバイスごとに、IKEv2 認証用の非対称キーを作成するには、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブに 2 つの行を追加する必要があります。詳細については、「[IKEv2 Authentication (Override)] ダイアログボックス （99 ページ）」を参照してください。

[IKEv2 Authentication (Override)] ダイアログボックス

[IKEv2 Authentication] ダイアログボックスを使用して、サイト間 VPN の IKEv2 認証グローバル設定に対するオーバーライドを設定します。IKEv2 グローバル認証設定とオーバーライド認証設定の詳細については、サイト間 VPN での IKEv2 認証の設定 （94 ページ）を参照してください。

ナビゲーション パス

[IKEv2認証（IKEv2 Authentication）] ポリシーの [IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブ（[IKEv2 Authentication] ポリシー （97 ページ）を参照）で、[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルでオーバーライドを選択して [行の編集（Edit Row）]（鉛筆）をクリックします。

フィールド リファレンス

表 16 : [IKEv2 Authentication] ダイアログボックス

要素	説明
Local Peers Remote Peers	このオーバーライドを定義するトンネルのローカル側とリモート側。 リストにデバイスを追加するには、リストの右側にある [選択（Select）] ボタンをクリックして、[ローカルまたはリモートピアの選択（Local or Remote Peer Selection）] ダイアログボックスを開きます。このダイアログボックスで、[選択可能（Available）] リストで必要なピアを選択して、[>>] をクリックして [選択済み（Selected）] リストに移動します。逆の操作を行って（[<<] ボタンを使用して）、デバイスの選択を解除できます。 使用可能なデバイスのリストには、IKEv2 接続をサポートするデバイスだけが含まれています。これは、VPN 内のすべてのデバイスではないことがあります。
IKEv2 Authentication Mode	選択したローカル ピアとリモート ピア間で使用する IKEv2 認証モード。次のいずれかを選択します。 • [Key Specification]：ユーザ定義の事前共有キー（1 ～ 128 文字）。必要なキーを入力して、[Confirm] フィールドに再度入力します。 • [PKI Specification]：IKEv2 接続のトラストポイントを定義する PKI 登録ポリシー オブジェクトの名前。PKI 登録オブジェクトを選択する場合や、新しいオブジェクトを作成する場合は、[選択（Select）] をクリックします。

IKEv2 認証用の非対称キーの設定

サイト間 VPN で非対称認証を設定できます。ここでは、トンネルの両側で異なる事前共有キーを使用できます。サイト間トポロジの一部であるピアデバイスごとに、IKEv2 認証用の非対称キーを作成するには、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブに 2 つの行を追加する必要があります。次の手順を実行します。

1. [IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブをクリックしてから、[行の追加（Add Row）]（+）ボタンをクリックします。[IKE認証（IKE Authentication）] ダイアログボックスが開きます。ピアの指定で、サイト間 VPN トポロジの一部であるローカルピアデバイスとリモートピアデバイスを選択します。[IKEv2認証モード（IKEv2 Authentication Mode）] で [キーの指定（Key Specification）] を選択し、キーを指定して確認します。Security Manager は、このキーを、選択したローカルピアデバイスのローカル事前共有キーと見なし、選択したリモートピアデバイスのリモート事前共有キーとも見なします。[OK] をクリックして、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブに戻ります。
2. [IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブを選択した状態で、[行の追加（Add Row）]（+）ボタンをクリックします。[IKE認証（IKE

Authentication）] ダイアログボックスが開きます。ピアの指定で、ローカルピアの場合はステップ 1 のリモートピアデバイスを選択し、リモートピアの場合はステップ 1 のローカルピアデバイスを選択します。[IKEv2認証モード（IKEv2 Authentication Mode）] で [キーの指定（Key Specification）] を選択し、キーを指定して確認します。このキーは、ステップ 1 で指定したキーとは異なる必要があります。

次の表は、IKEv2 認証用の非対称キーの設定を示しています。

	ローカルピアデバイス	リモートピアデバイス	認証方式（事前共有キー）
行 1 を追加	ピア 1	Peer2	test123
行 2 を追加	Peer2	ピア 1	sample123

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。