CHAPTER 26

IPsec と ISAKMP 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）標準を設定して、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。内容は次のとおりです。

トンネリング、IPsec、および ISAKMP に関する情報

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。

ASA 1000V は、ISAKMP と IPsec の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っています。ISAKMP と IPsec は、次の処理を実行できます。

- トンネル パラメータのネゴシエーション
- 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化
- トンネル経由のデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA 1000V は、双方向のトンネル 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 パケットを受信してカプセル化し、トンネルを作成して、カプセル化したパケットをトンネルのもう一方の終端に送信します。トンネルの終端では、パケットのカプセル化が解除されて最終的な宛先に送信されます。また、カプセル化されたパケットをパブリック ネットワークから受信してカプセル化を解除し、プライベート ネットワーク上の最終的な宛先に送信します。

IPsec の概要

ASA 1000V は LAN-to-LAN VPN 接続に IPSec を使用します。IPsec 用語では、ピアとは、別のセキュアなゲートウェイを意味します。ASA 1000V は、シスコのピアだけをサポートします。VPN の業界標準に従っているので ASA は他のベンダーのピアでも動作できますが、サポートはされません。

トンネルを確立する間に、2 つのピアは、認証、暗号化、カプセル化、キー管理を制御する Security Association（SA; セキュリティ アソシエーション）をネゴシエートします。これらのネゴシエーションには、トンネルの確立（IKE SA）と、トンネル内のトラフィックの制御（IPsec SA）という 2 つのフェーズが含まれます。

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。IPsec LAN-to-LAN 接続では、ASA 1000V は発信側または応答側として機能します。発信側は SA を提案し、応答側は、設定された SA パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

（注） ASA 1000V に IPsec VPN を設定する場合、セキュリティ コンテキスト（ファイアウォール マルチモードとも呼ばれる）またはアクティブ/アクティブ ステートフル フェールオーバーをイネーブルにすることはできません。したがって、これらの機能は使用できません。

ISAKMP および IKE の概要

ISAKMP は、2 台のホストで IPsec Security Association（SA; セキュリティ アソシエーション）の構築方法を一致させるためのネゴシエーション プロトコルです。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。このセキュリティ アソシエーションには、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。ISAKMP のネゴシエーションは 2 つのフェーズ（フェーズ 1 とフェーズ 2）に分かれています。フェーズ 1 は、以後の 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を作成します。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。

IKE は、IPsec を使用するための SA の設定に ISAKMP を使用します。IKE は、ピアの認証に使用される暗号キーを作成します。

ISAKMP ネゴシエーションの条件を設定するには、次を含む IKE ポリシーを作成します。

- IKEv1 ピア、または証明書を使用した RSA シグニチャと事前共有キー（PSK）のいずれかの必要な認証タイプ。
- データを保護しプライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code（HMAC）方式。
- 暗号キー決定アルゴリズムの強度を決定するデフィーヘルマン グループ。このアルゴリズムを使用して、ASA 1000V は暗号キーとハッシュ キーを導出します。
- IKEv2 の場合、IKEv2 トンネルの暗号化などに必要なキー関連情報とハッシュ操作を取得するための、アルゴリズムとして使用する別個の疑似乱数関数（PRF）。
- この暗号キーを使用する時間の上限。この時間が経過すると ASA 1000V は暗号キーを置き換えます。

IKEv1 ポリシーを使用して、パラメータごとに値を 1 つ設定します。IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。
ASA 1000V 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。この並べ替えにより、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。

ISAKMP の設定

この項では、Internet Security Association and Key Management Protocol（ISAKMP）およびインターネット キー交換（IKE）プロトコルについて説明します。

ここでは、次の内容について説明します。

IKEv1 と IKEv2 ポリシーの設定

IKE ポリシーを作成するには、グローバル コンフィギュレーション モードで **crypto** ***ikev1*** | ***ikev2*** **policy** コマンドを入力します。プロンプトは、IKE ポリシー コンフィギュレーション モードを表示します。次に例を示します。

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

ポリシーを作成した後は、ポリシーの設定を指定できます。

表 26-1 および表 26-2 に、IKEv1 ポリシーと IKEv2 ポリシーのキーワードおよび値を示します。

表 26-1　CLI コマンド用の IKEv1 ポリシー キーワード

コマンド	キーワード	意味	説明
認証	**rsa-sig**	RSA 署名アルゴリズムによって生成されたキー付きのデジタル証明書	各 IPsec ピアの ID を確立するために ASA 1000V が使用する認証方式を指定します。
	crack	Challenge/Response for Authenticated Cryptographic Keys	CRACK は、クライアントが RADIUS などのレガシーな方式を使用して認証を受け、サーバが公開キーによる認証方式を使用している場合に、強力な相互認証を実現します。
	pre-share（デフォルト）	事前共有キー	事前共有キーは拡大するネットワークに対応して拡張が困難ですが、小規模ネットワークではセットアップが容易です。

表 26-1　CLI コマンド用の IKEv1 ポリシー キーワード （続き）

コマンド	キーワード	意味	説明
encryption	**des**	56 ビット DES-CBC	2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化アルゴリズムを指定します。デフォルトは 168 ビット Triple DES です。
	3des（デフォルト）	168 ビット Triple DES	
	aes **aes-192** **aes-256**		Advanced Encryption Standard（AES; 高度暗号規格）は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。
hash	**sha**（デフォルト）	SHA-1（HMAC バリアント）	データ整合性の確保のために使用するハッシュ アルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
group	**1**	グループ 1（768 ビット）	Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPsec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。
	2（デフォルト）	グループ 2（1024 ビット）	
	5	グループ 5（1536 ビット）	Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。 AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES で必要なより大きいキー長をサポートするには、ISAKMP ネゴシエーションで Diffie-Hellman（DH）のグループ 5 を使用する必要があります。
lifetime	整数値 （86400 = デフォルト）	120 ～ 2147483647 秒	SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は（ある程度まで）高くなります。ただし、ライフタイムが短いほど、ASA 1000V による IPsec SA のセットアップ機能が高速になります。

表 26-2　CLI コマンド用の IKEv2 ポリシー キーワード

コマンド	キーワード	意味	説明
整合性	**sha**（デフォルト）	SHA-1（HMAC バリアント）	データ整合性の確保のために使用するハッシュ アルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、HMAC バリアント IKE ユーザがこの攻撃を防ぎます。

表 26-2　CLI コマンド用の IKEv2 ポリシー キーワード （続き）

コマンド	キーワード	意味	説明
	sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
encryption	**des**	56 ビット DES-CBC	2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化アルゴリズムを指定します。デフォルトは 168 ビット Triple DES です。
	3des（デフォルト）	168 ビット Triple DES	
	aes **aes-192** **aes-256**		Advanced Encryption Standard（AES; 高度暗号規格）は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。
prf	**sha**（デフォルト）	SHA-1（HMAC バリアント）	キー関連情報を生成するために使用されるアルゴリズムである、疑似乱数関数（PRF）を指定します。
	md5	MD5（HMAC バリアント）	デフォルト値は SHA-1 です。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。しかし、MD5 に対する攻撃が成功（これは非常に困難）しても、IKE が使用する HMAC バリアントがこの攻撃を防ぎます。
	sha256	SHA 2、256 ビットのダイジェスト	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha384	SHA 2、384 ビットのダイジェスト	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
	sha512	SHA 2、512 ビットのダイジェスト	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
group	**1**	グループ 1（768 ビット）	Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPsec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。
	2（デフォルト）	グループ 2（1024 ビット）	
	5	グループ 5（1536 ビット）	Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。 AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES で必要なより大きいキー長をサポートするには、ISAKMP ネゴシエーションで Diffie-Hellman（DH）のグループ 5 を使用する必要があります。
lifetime	整数値 （86400 = デフォルト）	120 ～ 2147483647 秒	SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は（ある程度まで）高くなります。ただし、ライフタイムが短いほど、ASA 1000V による IPsec SA のセットアップ機能が高速になります。

IKEv1 と IKEv2 はそれぞれ、最大 20 個の IKE ポリシーをサポートし、ポリシーごとに値セットが異なります。作成するポリシーごとに固有のプライオリティを割り当てます。プライオリティ番号が小さいほど、プライオリティが高くなります。

IKE ネゴシエーションが始まると、ネゴシエーションを開始したピアはそのすべてのポリシーをリモート ピアに送信し、リモート ピアは一致するポリシーを探します。リモート ピアは、一致するポリシーを見つけるまで、設定済みのポリシーに対してピアのすべてのポリシーを 1 つずつプライオリティ順に（最も高いプライオリティから）照合します。

2 台のピアの両方のポリシーに同じ暗号化、ハッシュ、認証、および Diffie-Hellman パラメータ値が含まれる場合、一致が生じます。IKEv1 では、リモート ピアのポリシーでは、発信側が送信したポリシーのライフタイム以下のライフタイムを指定する必要もあります。ライフタイムが等しくない場合、ASA 1000V は短い方のライフタイムを使用します。IKEv2 では、ライフタイムはネゴシエートされませんが、各ピア間でローカルに管理され、各ピアでライフタイムを個別に設定できるようにします。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、SA は確立されません。

各パラメータに対して特定の値を選択するときは、セキュリティとパフォーマンスの間に暗黙のトレードオフが発生します。デフォルト値で得られるセキュリティ レベルは、ほとんどの組織のセキュリティ要件に十分に対応します。パラメータに対し 1 つの値だけをサポートしているピアと相互運用する場合は、相手のピアがサポートしている値に選択が制限されます。

（注） 新しい ASA コンフィギュレーションには、デフォルトの IKEv1 または IKEv2 ポリシーはありません。

IKE ポリシーをグローバル コンフィギュレーション モードで設定するには、**crypto *ikev1* | *ikev2* policy** コマンドを使用して、IKE ポリシー コンフィギュレーション モードを開始します。

crypto *ikev1* | *ikev2* policy *priority*

ISAKMP コマンドには、それぞれプライオリティを指定する必要があります。プライオリティ番号によってポリシーが一意に識別され、IKE ネゴシエーションにおけるポリシーのプライオリティが決定されます。

IKE をイネーブルにして設定するには、IKEv1 の例をガイドとして参考にし、次の手順を実行します。

（注） 所定のポリシー パラメータに値を指定しない場合、デフォルト値が適用されます。

ステップ 1　IKEv1 ポリシー コンフィギュレーション モードを開始します。

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

ステップ 2　暗号化アルゴリズムを指定します。デフォルトは Triple DES です。この例では、暗号化を DES に設定します。

encryption [**aes** | **aes-192** | **aes-256** | **des** | **3des**]

次に例を示します。

```
hostname(config-ikev1-policy)# encryption des
```

ステップ 3　ハッシュ アルゴリズムを指定します。デフォルト値は SHA-1 です。この例では、MD5 を設定します。

hash [**md5** | **sha**]

次に例を示します。

```
hostname(config-ikev1-policy)# hash md5
```

ステップ 4　認証方式を指定します。デフォルトは事前共有キーです。この例では、RSA 署名を設定します。

authentication [**pre-share** | **crack** | **rsa-sig**]

次に例を示します。

```
hostname(config-ikev1-policy)# authentication rsa-sig
```

ステップ 5　Diffie-Hellman グループ識別番号を指定します。デフォルトはグループ 2 です。この例では、グループ 5 を設定します。

group [**1** | **2** | **5**]

次に例を示します。

```
hostname(config-ikev1-policy)# group 5
```

ステップ 6　SA ライフタイムを指定します。この例では、4 時間（14400 秒）のライフタイムを設定します。デフォルトは 86400 秒（24 時間）です。

lifetime *seconds*

次に例を示します。

```
hostname(config-ikev1-policy)# lifetime 14400
```

外部インターフェイスでの IKE のイネーブル化

VPN トンネルを終端するインターフェイスでは、IKE をイネーブルにする必要があります。通常は外部（つまり、パブリック）インターフェイスです。IKEv1 または IKEv2 をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto *ikev1*** | ***ikev2*** **enable** コマンドを使用します。

crypto *ikev1* | ***ikev2*** **enable** *interface-name*

次に例を示します。

```
hostname(config)# crypto ikev1 enable outside
```

IKEv1 アグレッシブ モードのディセーブル化

フェーズ 1 の IKEv1 ネゴシエーションでは、メイン モードまたはアグレッシブ モードのいずれかを使用できます。どちらのモードも同じサービスを提供しますが、アグレッシブ モードでは、ピア間で 3 回の合計 6 つのメッセージ交換ではなく、2 回の合計 3 つのメッセージ交換だけですみます。アグレッシブ モードの方が高速ですが、通信パーティの ID は保護されません。このため、セキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。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。

- 交換回数の多いメイン モードは低速ですが、通信しているピアの ID を保護します。
- アグレッシブ モードは高速ですが、ピアの ID を保護しません。

アグレッシブ モードをディセーブルにするには、次のコマンドを入力します。

crypto ikev1 am-disable

次に例を示します。

```
hostname(config)# crypto ikev1 am-disable
```

アグレッシブ モードをいったんディセーブルにした後でイネーブルに戻すには、**no** 形式でコマンドを使用します。次に例を示します。

```
hostname(config)# no crypto ikev1 am-disable
```

IKEv1 および IKEv2 の ISAKMP ピアの識別方式の決定

IKEv1 または IKEv2 のフェーズ I の ISAKMP ネゴシエーションでは、ピアは相互に相手を識別する必要があります。この識別方法は、次のオプションから選択できます。

Address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
Automatic	接続タイプによって ISAKMP ネゴシエーションが決まります。 • 事前共有キーの IP アドレス • 証明書認証の証明書認定者名
Hostname	ISAKMP の識別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（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
Key ID	リモート ピアが事前共有キーの検索に使用する文字列を使用します。

ASA 1000V は、ピアに送信するフェーズ I の ID を使用します。これは、事前共有キーで認証を行うメイン モードでの LAN-to-LAN IKEv1 接続を除いて、すべての VPN シナリオで行われます。

auto 設定がデフォルトです。

ピア識別方式を変更するには、次のコマンドを入力します。

crypto isakmp identity {**address** | **hostname** | **key-id** ***id-string*** | **auto**}

たとえば、次のコマンドはピア識別方法をホスト名に設定します。

```
hostname(config)# crypto isakmp identity hostname
```

IPsec over NAT-T のイネーブル化

NAT-T を使用すると、IPsec ピアは NAT デバイスを介した接続を確立できます。NAT-T は、UDP データグラムの IPsec トラフィックをカプセル化し、ポート 4500 を使用して、NAT デバイスにポート情報を提供することで、これを実行します。NAT-T はすべての NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。この機能はデフォルトで無効に設定されています。

（注） IPsec over TCP がイネーブルになっている場合は、その他のすべての接続方式よりも優先されます。

NAT-T をイネーブルにすると、ASA 1000V は、IPsec がイネーブルになっているすべてのインターフェイス上で自動的にポート 4500 を開きます。

NAT-T の使用

NAT-T を使用するには、次の作業を実行する必要があります。

ステップ 1　ASA 1000V でグローバルに IPsec over NAT-T をイネーブルにするには、次のコマンドを入力します。

crypto isakmp nat-traversal *natkeepalive*

natkeepalive 引数の範囲は 10 ～ 3600 秒です。デフォルトは 20 秒です。

たとえば、次のコマンドを入力して、NAT-T をイネーブルにし、キープアライブ値を 1 時間に設定します。

```
hostname(config)# crypto isakmp nat-traversal 3600
```

ステップ 2　このコマンドを入力して、IPSec フラグメンテーション ポリシーの暗号化前のオプションを選択します。

```
hostname(config)# crypto ipsec fragmentation before-encryption
```

このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作を妨げることはありません。

リブートの前にアクティブ セッションの終了を待機

すべてのアクティブ セッションが自発的に終了した場合に限り、ASA 1000V がリブートするようにスケジュールを設定できます。この機能はデフォルトで無効に設定されています。

ASA 1000V のリブートの前にすべてのアクティブ セッションが自発的に終了するまで待機する機能をイネーブルにするには、次のコマンドを入力します。

```
crypto isakmp reload-wait
```

次に例を示します。

```
hostname(config)# crypto isakmp reload-wait
```

reload コマンドを使用して、ASA 1000V をリブートします。**reload-wait** コマンドを設定すると、**reload quick** コマンドを使用して **reload-wait** 設定を無効にできます。**reload** コマンドと **reload-wait** コマンドは特権 EXEC モードで使用できます。どちらにも **isakmp** プレフィックスは付けません。

接続解除の前にピアに警告

ASA 1000V 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、管理者による停止などいくつかの理由で、LAN-to-LAN セッションがドロップすることがあります。

ASA 1000V では、LAN-to-LAN コンフィギュレーションで限定されたピアに対して、セッションが接続解除される直前に通知できます。アラートを受信するピアは、その理由を解読して、イベント ログまたはポップアップ ペインに表示します。この機能はデフォルトで無効に設定されています。

アラートがイネーブルになっているセキュリティ アプライアンスは限定されたピアです。

IPsec ピアに対する接続解除の通知をイネーブルにするには、**crypto isakmp disconnect-notify** コマンドを入力します。

次に例を示します。

```
hostname(config)# crypto isakmp disconnect-notify
```

tunnel-group-map default-group コマンドの使用

このコマンドは、コンフィギュレーションにトンネル グループが指定されていない場合に使用する、デフォルトのトンネル グループを指定します。

コマンドの構文は、**tunnel-group-map** [*rule-index*] **default-group** *tunnel-group-name* です。*rule-index* はルールのプライオリティで、*tunnel-group name* は既存のトンネル グループ名である必要があります。

IPsec の設定

この項では、IPsec に関する背景情報と、IPsec を使用して VPN を実装するときに ASA 1000V を設定する手順について説明します。構成するトピックは、次のとおりです。

IPsec トンネルの概要

IPsec トンネルとは、ASA 1000V がピア間に確立する SA のセットのことです。SA は機密データに適用するプロトコルとアルゴリズムを指定し、ピアが使用するキー関連情報も指定します。IPsec SA は、ユーザ トラフィックの実際の伝送を制御します。SA は単方向ですが、通常ペア（着信と発信）で確立されます。

ピアは SA ごとに使用する設定をネゴシエートします。各 SA は次のもので構成されます。

- IKEv1 トランスフォーム セットまたは IKEv2 プロポーザル
- クリプト マップ
- アクセス リスト
- トンネル グループ
- 事前フラグメンテーション ポリシー

IKEv1 トランスフォーム セットおよび IKEv2 プロポーザルの概要

IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルとは、ASA 1000V によるデータの保護方法を定義したセキュリティ プロトコルとアルゴリズムの組み合わせのことです。IPsec SA のネゴシエーション中、2 つのピアは、両方のピアで一致しているトランスフォーム セットまたはプロポーザル

を識別する必要があります。次に、ASA 1000V は一致しているトランスフォーム セットまたはプロポーザルを適用して、クリプト マップに対するアクセス リストのデータ フローを保護する SA を作成します。

IKEv1 トランスフォーム セットを使用して、パラメータごとに値を 1 つ設定します。IKEv2 プロポーザルでは、単一のプロポーザルに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA 1000V 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。

SA を作成するために使用されるトランスフォーム セットまたはプロポーザルの定義を変更すると、ASA 1000V はトンネルを切断します。詳細については、セキュリティ アソシエーションのクリアを参照してください。

（注） トランスフォーム セットまたはプロポーザルの要素を 1 つだけ消去または削除すると、ASA 1000V はその要素を参照するクリプト マップを自動的に削除します。

クリプト マップの定義

*クリプト マップ*は、IPsec SA でネゴシエートされる IPsec ポリシーを定義します。クリプト マップには、次のものが含まれます。

- IPsec 接続が許可および保護するパケットを識別するためのアクセス リスト
- ピア ID。
- IPsec トラフィックのローカル アドレス。（詳細については、「クリプト マップのインターフェイスへの適用」を参照してください）。
- ピアのセキュリティ設定の照合に使用される最大 11 個の IKEv1 トランスフォーム セットまたは IKEv2 プロポーザル。

*クリプト マップ セット*は、同じマップ名を持つ 1 つまたは複数のクリプト マップで構成されます。最初のクリプト マップを作成したときに、クリプト マップ セットを作成します。クリプト マップを作成または追加するコマンドの構文は次のとおりです。

```
crypto map map-name seq-num match address access-list-name
```

このコマンドを続けて入力すると、クリプト マップをクリプト マップ セットに追加できます。次の例では、クリプト マップを追加するクリプト マップ セットの名前は *mymap* です。

```
crypto map mymap 10 match address 101
```

上記の構文に含まれるシーケンス番号（*seq-num*）によって、同じ名前を持つクリプト マップがそれぞれ区別されます。クリプト マップに割り当てられているシーケンス番号によって、クリプト マップ セット内のクリプト マップ間のプライオリティが決まります。シーケンス番号が小さいほど、プライオリティが高くなります。クリプト マップ セットをインターフェイスに割り当てると、ASA 1000V は、そのインターフェイスを通過するすべての IP トラフィックとクリプト マップ セット内のクリプト マップを、シーケンス番号が低い順に照合して評価します。

クリプト マップに割り当てられている ACL は、同じアクセス リスト名を持つすべての ACE で構成されます。コマンドの構文は次のとおりです。

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

各 ACL は、同じアクセス リスト名を持つ 1 つまたは複数の ACE で構成されます。最初の ACE を作成したときに、ACL を作成します。ACL を作成または追加するコマンドの構文は次のとおりです。

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

次の例では、ASA 1000V は、10.0.0.0 サブネットから 10.1.1.0 サブネットまでのすべてのトラフィック フローに対して、クリプト マップに割り当てられている IPsec 保護を適用します。

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

パケットが一致するクリプト マップによって、SA ネゴシエーションで使用されるセキュリティ設定が決定します。ローカルの ASA 1000V がネゴシエーションを開始する場合は、スタティック クリプト マップで指定されたポリシーを使用して、指定のピアに送信するオファーを作成します。ピアがネゴシエーションを開始する場合、ASA 1000V はスタティック クリプト マップに対するポリシーの照合を試します。これに失敗した場合は、クリプト マップ セットのダイナミック クリプト マップと照合して、ピアのオファーを受け入れるか拒否するかを決定します。

2 つのピアが SA の確立に成功するには、両方のピアが互換性のあるクリプト マップを少なくとも 1 つ持っている必要があります。互換性が成立するには、クリプト マップが次の条件を満たす必要があります。

- クリプト マップに、互換性を持つ暗号 ACL（たとえば、ミラー イメージ ACL）が含まれている。応答するピアがダイナミック クリプト マップを使用する場合、ASA 1000V には、IPSec の適用条件として互換性のあるクリプト ACL も含まれている必要があります。
- 各クリプト マップが他のピアを識別する（応答するピアがダイナミック クリプト マップを使用していない場合）。
- クリプト マップに、共通のトランスフォーム セットまたはプロポーザルが少なくとも 1 つある。

1 つのインターフェイスに適用できるクリプト マップ セットは 1 つだけです。次の条件のいずれかが当てはまる場合は、ASA 1000V 上の特定のインターフェイスに対して複数のクリプト マップを作成します。

- 特定のピアに異なるデータ フローを処理させる。
- さまざまなタイプのトラフィックにさまざまな IPsec セキュリティを適用する。

たとえば、クリプト マップを 1 つ作成し、2 つのサブネット間のトラフィックを識別する ACL を割り当て、IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを 1 つ割り当てます。別のクリプト マップを作成し、別の 2 つのサブネット間のトラフィックを識別する異なる ACL を割り当て、VPN パラメータが異なるトランスフォーム セットまたはプロポーザルを適用します。

1 つのインターフェイスに複数のクリプト マップを作成する場合は、クリプト マップ セット内のプライオリティを決めるシーケンス番号（seq-num）を各クリプト マップ エントリに指定します。

各 ACE には permit 文または deny 文が含まれます。表 26-3 に、クリプト マップに適用される ACL での ACE の許可と拒否の特別な意味を示します。

表 26-3　発信トラフィックに適用されるアクセス リストにおける許可と拒否の特別な意味

クリプト マップ評価の結果	応答
permit 文が含まれている ACE の基準と一致	パケットをクリプト マップ セットの残りの ACE と照合して評価することを停止し、パケット セキュリティ設定を、クリプト マップに割り当てられている IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルと照合して評価します。セキュリティ設定がトランスフォーム セットまたはプロポーザルのセキュリティ設定と一致すると、ASA 1000V は関連する IPsec 設定を適用します。一般に発信トラフィックの場合、IPsec 設定の適用とはパケットの復号化、認証、ルーティングを行うことを意味します。
deny 文が含まれている ACE の基準と一致	パケットを評価中のクリプト マップの残りの ACE と照合して評価することを中断し、次のクリプト マップ（クリプト マップに割り当てられているシーケンス番号で判断する）の ACE との照合と評価を再開します。
クリプト マップ セット内のテスト済みのすべての許可 ACE と不一致	パケットを暗号化せずにルーティングします。

deny 文が含まれている ACE は、IPsec 保護が不要な発信トラフィック（たとえば、ルーティング プロトコル トラフィックなど）をフィルタリングして除外します。したがって、暗号アクセス リストの permit 文と照合して評価する必要のない発信トラフィックをフィルタリングするために、最初の deny 文を挿入します。

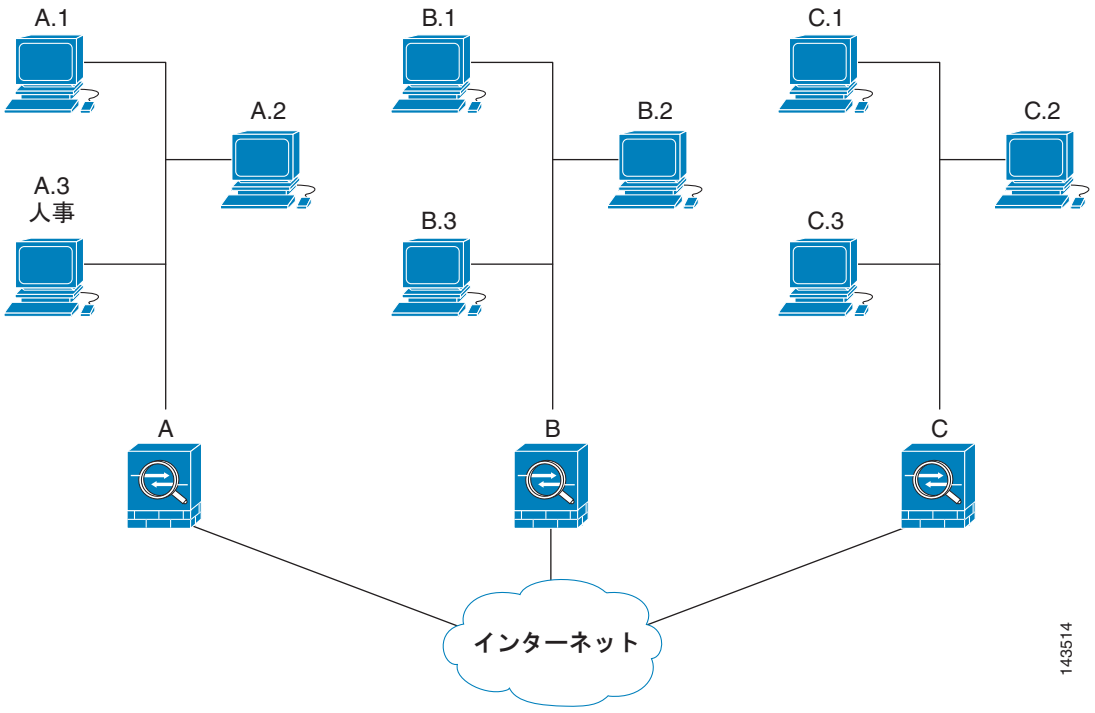
暗号化された着信パケットに対しては、セキュリティ アプライアンスは送信元アドレスと ESP SPI を使用して、パラメータの復号化を決定します。セキュリティ アプライアンスは、パケットを復号化した後で、復号化されたパケットの内部ヘッダーを、そのパケットの SA に関連付けられている ACL の許可 ACE と比較します。内部ヘッダーがプロキシと一致しない場合、セキュリティ アプライアンスはそのパケットをドロップします。内部ヘッダーがプロキシと一致する場合、セキュリティ アプライアンスはそのパケットをルーティングします。

暗号化されていない着信パケットの内部ヘッダーを比較する場合は、セキュリティ アプライアンスはすべての拒否ルールを無視します。これは、拒否ルールによってフェーズ 2 の SA の確立が妨げられるためです。

（注）　暗号化されていない着信トラフィックをクリア テキストとしてルーティングするには、ACE の許可の前に ACE の拒否を挿入します。

図 26-1 に、ASA 1000V の LAN-to-LAN ネットワークの例を示します。

図 26-1　ACE の許可と拒否がトラフィックに及ぼす影響（概念上のアドレス）



この図に示され、また以下の説明で使用されている単純なアドレス表記は、抽象化したものです。実際の IP アドレスを使用した例は、この説明の後に示します。

この LAN-to-LAN ネットワーク例において、セキュリティ アプライアンス A、B、および C を設定する目的は、図 26-1 に示したホストのいずれか 1 台から発信され、別のホストを宛先とするすべてのトラフィックのトンネリングを許可することです。ただし、ホスト A.3 から発信されるトラフィックには人事部の機密データが含まれるため、他のトラフィックよりも強固な暗号化と頻繁なキー再生が必要です。そのため、ホスト A.3 から発信されるトラフィックには特別なトランスフォーム セットを割り当てることができます。

セキュリティ アプライアンス A の発信トラフィックを設定するために、2 つのクリプト マップを作成します。1 つはホスト A.3 の発信トラフィック用で、もう 1 つはネットワーク A の他のホストの発信トラフィック用です。次に例を示します。

```
Crypto Map Seq_No_1
    deny packets from A.3 to B
    deny packets from A.3 to C
    permit packets from A to B
    permit packets from A to C
Crypto Map Seq_No_2
    permit packets from A.3 to B
    permit packets from A.3 to C
```

ACL を作成したら、一致するパケットごとに必要な IPsec を適用するためのトランスフォーム セットを各クリプト マップに割り当てます。

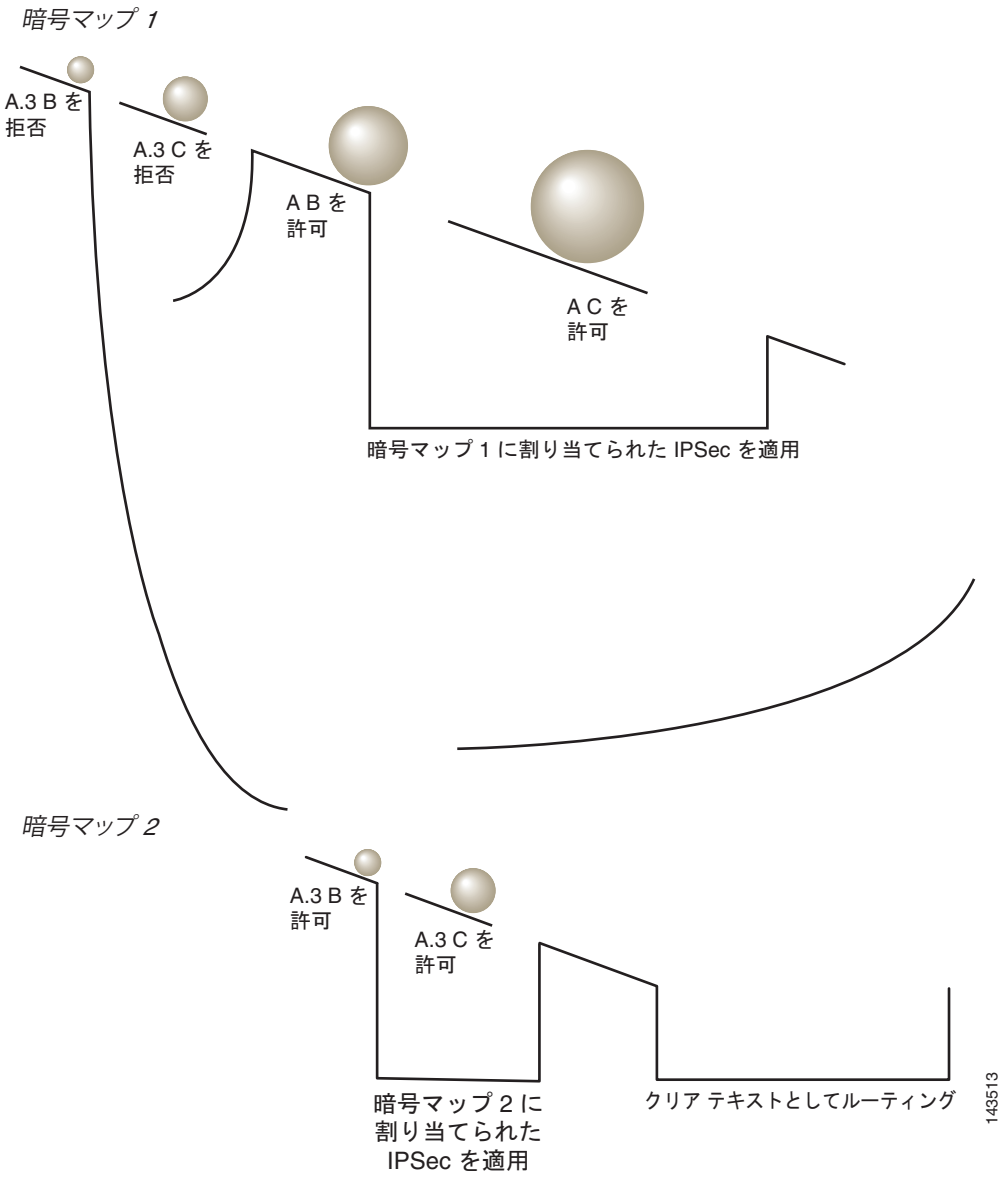
カスケード ACL とは、拒否 ACE を挿入することで、ACL の評価をバイパスし、クリプト マップ セット内の次の ACL の評価を再開するものです。クリプト マップごとに異なる IPsec 設定を関連付けることができるため、拒否 ACE を使用することで、特別なトラフィックを対応するクリプト マップでの以後の評価から除外し、異なるセキュリティを提供する別のクリプト マップ、または異なるセキュ

リティを必要とする別のクリプト マップの permit 文と特別なトラフィックを照合することができます。暗号 ACL に割り当てられているシーケンス番号によって、クリプト マップ セット内の評価の順序が決まります。

図 26-2 に、上記の概念 ACE から作成されたカスケード ACL を示します。この図で使用されている各記号の意味は、次のとおりです。

	クリプト マップ セット内のクリプト マップ。
	（すき間がある直線）パケットが ACE に一致した時点でクリプト マップの照合を終了します。
	1 つの ACE の説明と一致したパケット。それぞれの大きさのボールは、図中の別々の ACE に一致する異なるパケットを表しています。大きさの違いは、各パケットの発信元と宛先が異なることを示しています。
	クリプト マップ セット内での次のクリプト マップへのリダイレクション。
	パケットが ACE に一致するか、またはクリプト マップ セット内のすべての許可 ACE に一致しない場合の応答。

図 26-2　クリプト マップ セット内のカスケード ACL



セキュリティ アプライアンス A は、ホスト A.3 から発信されたパケットが許可 ACE と一致するまで評価し、クリプト マップに関連付けられている IPsec セキュリティの割り当てを試行します。このパケットが拒否 ACE と一致すると、ASA 1000V はこのクリプト マップの残りの ACE を無視し、次のクリプト マップ（クリプト マップに割り当てられているシーケンス番号で判断する）との照合と評価を再開します。この例では、セキュリティ アプライアンス A がホスト A.3 から発信されたパケットを受信すると、このパケットを最初のクリプト マップの拒否 ACE と照合し、次のクリプト マップでの照合と評価を再開します。パケットが 2 番目のクリプト マップの許可 ACE と一致すると、関連付けられた IPsec セキュリティ（強固な暗号化と頻繁なキー再生）がパケットに適用されます。

このネットワーク例におけるセキュリティ アプライアンスの設定を完了するために、ミラー クリプト マップをセキュリティ アプライアンス B と C に割り当てます。しかし、セキュリティ アプライアンスは、暗号化された着信トラフィックの評価では拒否 ACE を無視するため、deny A.3 B と deny A.3 C

の ACE のミラーに相当するものを無視できます。したがって、クリプト マップ 2 のミラーに相当するものを無視できます。このため、セキュリティ アプライアンス B と C のカスケード ACL の設定は不要です。

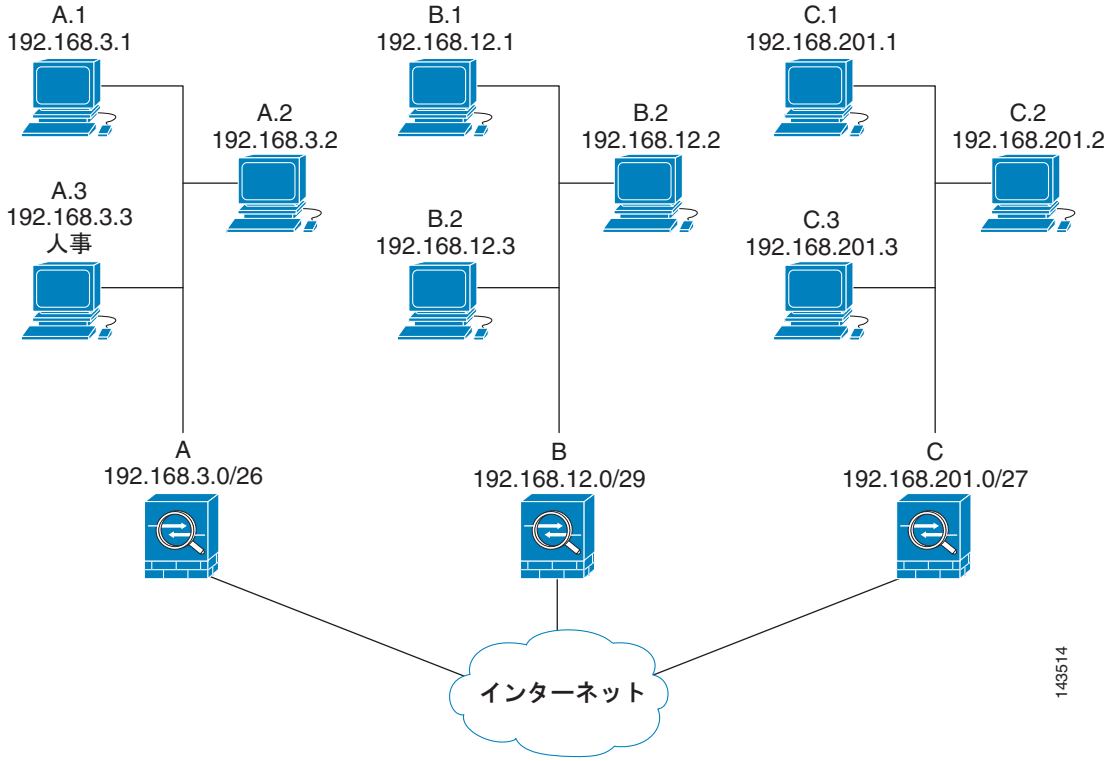
表 26-4 に、図 26-1 の 3 台の ASA 1000V 用に設定されたクリプト マップに割り当てられている ACL を示します。

表 26-4　許可文と拒否文の例（概念図）

セキュリティ アプライアンス A		セキュリティ アプライアンス B		セキュリティ アプライアンス C	
クリプト マップ シーケンス番号	ACE パターン	クリプト マップ シーケンス番号	ACE パターン	クリプト マップ シーケンス番号	ACE パターン
1	A.3 B を拒否	1	B A を許可	1	C A を許可
	A.3 C を拒否				
	A B を許可				
	A C を許可		B C を許可		C B を許可
2	A.3 B を許可				
	A.3 C を許可				

図 26-3 では、図 26-1 の概念アドレスを実際の IP アドレスにマッピングしています。

図 26-3　ACE の許可と拒否がトラフィックに及ぼす影響（実際のアドレス）



次の表は、図 26-3 の IP アドレスを表 26-4 の概念と結合したものです。これらの表に示されている実際の ACE によって、このネットワーク内で評価を受けたすべての IPsec パケットに適切な IPsec 設定が適用されます。

表 26-5　セキュリティ アプライアンス A の permit 文と deny 文の例

セキュリティ アプライアンス	クリプト マップ シーケンス番号	ACE パターン	実際の ACE
A	1	A.3 B を拒否	deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		A.3 C を拒否	deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
		A B を許可	permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248
		A C を許可	permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.224
	2	A.3 B を許可	permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		A.3 C を許可	permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
B	必要なし	B A を許可	permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192
		B C を許可	permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.224
C	必要なし	C A を許可	permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.192
		C B を許可	permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.248

このネットワーク例で示されている論法を応用して、カスケード ACL を使用することにより、Cisco ASA 1000V で保護されているさまざまなホストまたはサブネットにさまざまなセキュリティ設定を割り当てることができます。

（注） デフォルトでは、ASA 1000V は、IPsec トラフィックが入ってきたインターフェイスと同じインターフェイスを宛先とする IPsec トラフィックはサポートしません このタイプのトラフィックには、U ターン、ハブアンドスポーク、ヘアピニングなどの名称があります。ただし、ネットワークを出入りするトラフィックを許可する ACE を挿入することで、U ターン トラフィックをサポートするように IPSec を設定できます。たとえば、セキュリティ アプライアンス B で U ターン トラフィックをサポートするには、概念上の「B B を許可」ACE を ACL1 に追加します。実際の ACE は次のようになります。

```
permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248
```

クリプト マップのインターフェイスへの適用

クリプト マップ セットは、IPsec トラフィックが通過する各インターフェイスに割り当てる必要があります。ASA 1000V は、すべてのインターフェイスで IPsec をサポートします。クリプト マップ セットをインターフェイスに割り当てると、ASA 1000V は、すべてのトラフィックをクリプト マップ セットと照合して評価し、接続中またはネゴシエーション中は指定されたポリシーを使用します。

クリプト マップをインターフェイスに割り当てると、SA データベースやセキュリティ ポリシー データベースなどのランタイム データ構造も初期設定されます。クリプト マップを修正してインターフェイスに再割り当てすると、ランタイム データ構造はクリプト マップ設定と再同期化されます。また、新しいシーケンス番号を使用して新しいピアを追加し、クリプト マップを再割り当てしても、既存の接続が切断されることはありません。

インターフェイス アクセス リストの使用

ASA 1000V では、デフォルトで IPsec パケットがインターフェイス ACL をバイパスするようになっています。インターフェイス アクセス リストを IPsec トラフィックに適用する場合は、**no** 形式の **sysopt connection permit-vpn** コマンドを使用します。

発信インターフェイスにバインドされているクリプト マップ アクセス リストは、VPN トンネルを通過する IPsec パケットの許可と拒否を行います。IPsec は、IPsec トンネルから来たパケットの認証と解読を行い、トンネルに関連付けられている ACL とパケットを照合して評価します。

アクセス リストは、どの IP トラフィックを保護するかを定義します。たとえば、2 つのサブネット間または 2 台のホスト間のすべての IP トラフィックを保護するためのアクセス リストを作成できます（これらのアクセス リストは、**access-group** コマンドで使用されるアクセス リストとよく似ています。ただし、**access-group** コマンドでは、アクセス リストがインターフェイスで転送するトラフィックと阻止するトラフィックを決めます）。

クリプト マップを割り当てるまで、アクセス リストは IPsec の使用に限定されません。各クリプト マップはアクセス リストを参照し、パケットがアクセス リストのいずれか 1 つで permit と一致した場合に適用する IPsec プロパティを決めます。

IPsec クリプト マップに割り当てられているアクセス リストには、次の 4 つの主要機能があります。

- IPSec で保護する発信トラフィックを選択する（permit に一致したものが保護の対象）。
- 確立された SA がない状態で移動するデータに対して ISAKMP ネゴシエーションをトリガーする。
- 着信トラフィックを処理して、IPSec で保護すべきであったトラフィックをフィルタリングして廃棄する。
- ピアからの IKE ネゴシエーションを処理するときに、IPsec SA の要求を受け入れるかどうかを決定する （ネゴシエーションは **ipsec-isakmp crypto map** エントリだけに適用されます）。ピアは **ipsec-isakmp crypto map** コマンド エントリに関連付けられているデータ フローを許可し、ネゴシエーション中に要求が受け入れられるようにする必要があります。

トラフィックが着信か発信かに関係なく、ASA 1000V は、インターフェイスに割り当てられているアクセス リストとトラフィックを照合して評価します。インターフェイスに IPsec を割り当てるには、次の手順を実行します。

ステップ 1　IPsec に使用するアクセス リストを作成します。

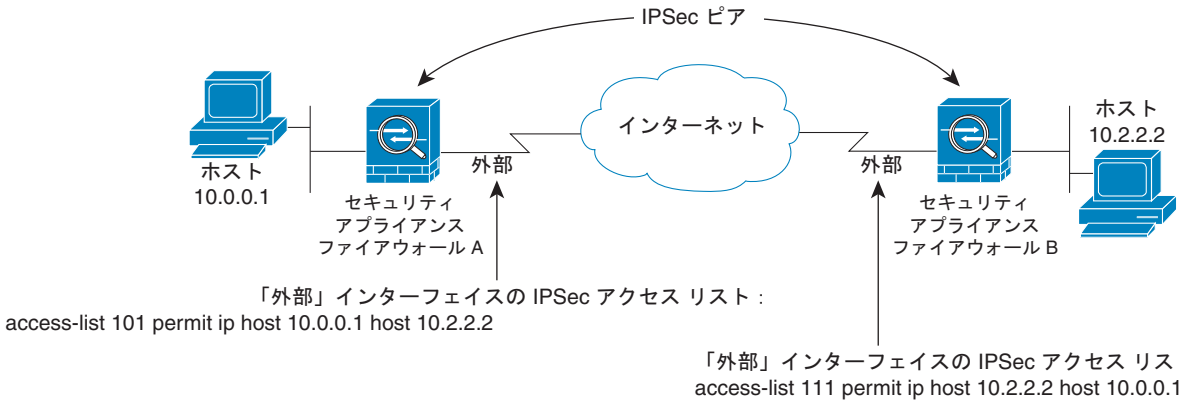
ステップ 2　作成したアクセス リストを、同じクリプト マップ名を使用して 1 つまたは複数のクリプト マップにマッピングします。

ステップ 3　データ フローに IPsec を適用するために、IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルをクリプト マップにマッピングします。

ステップ 4　共有するクリプト マップ名を割り当てて、クリプト マップを一括してクリプト マップ セットとしてインターフェイスに適用します。

図 26-4 では、データがセキュリティ アプライアンス A 上の外部インターフェイスを出てホスト 10.2.2.2 に向かうときに、ホスト 10.0.0.1 とホスト 10.2.2.2 の間のトラフィックに IPsec 保護が適用されます。

図 26-4　暗号アクセス リストを IPsec に適用する方法



ホスト 10.0.0.1 と 10.2.2.2 の間で交換されるトラフィックは、セキュリティ アプライアンス ファイアウォール A の「外側」とセキュリティ アプライアンス ファイアウォール B の「外側」の間で保護されます。

92616

セキュリティ アプライアンス A は、ホスト 10.0.0.1 からホスト 10.2.2.2 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.0.0.1
- 宛先 = ホスト 10.2.2.2

またセキュリティ アプライアンス A は、ホスト 10.2.2.2 からホスト 10.0.0.1 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.2.2.2
- 宛先 = ホスト 10.0.0.1

評価中のパケットと最初に一致した permit 文によって、IPsec SA のスコープが決まります。

（注） アクセス リストの要素を 1 つだけ削除すると、ASA 1000V は関連付けられているクリプト マップも削除します。

現在 1 つまたは複数のクリプト マップが参照しているアクセス リストを修正する場合は、**crypto map interface** コマンドを使用して SA データベースのランタイムを再初期化します。詳細については、**crypto map** コマンドを参照してください。

ローカル ピアで定義するスタティック クリプト マップに指定したすべてのクリプト アクセス リストに対して、リモート ピアで「ミラー イメージ」クリプト アクセス リストを定義することをお勧めします。また、クリプト マップは共通トランスフォームをサポートし、他のシステムをピアとして参照する必要があります。これにより、両方のピアで IPsec が正しく処理されます。

（注） すべてのスタティック クリプト マップでアクセス リストと IPsec ピアを定義する必要があります。どちらかが定義されていないと、クリプト マップは不完全なものになり、ASA 1000V は、前の完全なクリプト マップにまだ一致していないトラフィックをドロップします。**show conf** コマンドを使用して、すべてのクリプト マップが完全なものになるようにします。不完全なクリプト マップを修正するには、クリプト マップを削除し、欠けているエントリを追加してからクリプト マップを再適用します。

暗号アクセス リストで送信元アドレスまたは宛先アドレスの指定に **any** キーワードを使用すると問題が発生するため、このキーワードの使用は避けてください。**permit any any** コマンド文を使用すると次の現象が発生するため、使用は極力避けてください。

- すべての発信トラフィックが保護されます。これには、対応するクリプト マップで指定されているピアに送信される保護済みのトラフィックも含まれます。
- すべての着信トラフィックに対する保護が必要になります。

  このシナリオでは、ASA 1000V は IPsec 保護されていないすべての着信パケットを通知なしでドロップします。

保護するパケットを定義したことを必ず確認してください。**permit** 文に **any** キーワードを使用する場合は、その文の前に一連の **deny** 文をおき、保護対象外のトラフィックをすべてフィルタリングして排除します。これを行わないと、その **permit** 文に保護対象外のトラフィックが含まれることになります。

（注） no sysopt connection permit-vpn が設定されている間は、外部インターフェイスで access-group が設定されていたとしても、クライアントからの復号化された通過トラフィックが許可されます。これは、**deny ip any any** アクセス リストを呼び出します。

外部インターフェイスのアクセス コントロール リスト（ACL）と共に **no sysopt permit** コマンドを使用して、サイトツーサイト VPN またはリモート アクセス VPN 経由での保護されたネットワークへのアクセスを制御しようとしても、うまくいきません。

このような状況では、内部の管理アクセスがイネーブルになっていると、ACL は適用されず、ユーザはまだセキュリティ アプライアンスへの SSH を使用して接続できます。内部ネットワーク上のホストへのトラフィックは ACL によって正しくブロックされますが、内部インターフェイスへの復号化された通過トラフィックはブロックできません。

ssh および **http** コマンドは、ACL よりもプライオリティが高くなります。つまり、VPN セッションからデバイスへの SSH、Telnet、または ICMP トラフィックを拒否するには、IP ローカル プールを拒否する **ssh**、**telnet**、および **icmp** コマンドを追加する必要があります。

IPsec SA のライフタイムの変更

ASA 1000V が新しい IPsec SA とネゴシエートするときに使用する、グローバル ライフタイム ASA 1000V 値を変更できます。特定のクリプト マップのグローバル ライフタイム値を上書きできます。

IPsec SA では、取得された共有秘密キーが使用されます。このキーは SA に不可欠な要素で、キーにリフレッシュが必要な場合、キーは SA と同時にタイムアウトします。各 SA には、時間とトラフィック量の 2 つのライフタイムがあります。SA は、それぞれのライフタイムとネゴシエーションが新しい SA 用に開始された後、期限切れになります。デフォルトのライフタイムは、28,800 秒（8 時間）および 4,608,000 キロバイト（10 メガバイト/秒で 1 時間）です。

グローバル ライフタイムを変更すると、ASA 1000V はトンネルをドロップします。変更後に確立された SA のネゴシエーションでは、新しい値が使用されます。

クリプト マップに設定されたライフタイム値がなく、ASA 1000V から新しい SA を要求された場合、クリプト マップは、ピアに送信される新しい SA 要求に、既存の SA で使用されているグローバル ライフタイム値を挿入します。ピアがネゴシエーション要求を受け取ると、このピアが提案するライフタイム値とローカルに設定されているライフタイム値のうち小さい方の値を、新しい SA のライフタイム値として使用します。

既存 SA のライフタイムのしきい値を超える前に、ピアは新しい SA をネゴシエートします。このようにして、既存 SA の有効期限が切れる前に、新しい SA の準備が整います。既存 SA の残りのライフタイムが約 5 ～ 15% になると、ピアは新しい SA をネゴシエートします。

基本的な IPsec コンフィギュレーションの作成

スタティックまたはダイナミック クリプト マップを使用する基本的な IPsec コンフィギュレーションを作成できます。

スタティック クリプト マップを使用する基本的な IPsec コンフィギュレーションを作成するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、保護するトラフィックを定義するアクセス リストを作成します。

access-list *access-list-name* {**deny | permit**} **ip** *source source-netmask destination destination-netmask*

次に例を示します。

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

この例では、**permit** キーワードによって、指定の条件に一致するトラフィックすべてが暗号で保護されます。

ステップ 2　次のコマンドを入力して、トラフィックを保護する方法を定義する IKEv1 トランスフォーム セットを設定します。

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

次に例を示します。

```
hostname(config)# crypto ipsec ikev1 transform-set myset1 esp-des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set myset2 esp-3des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

この例では、myset1、myset2、aes_set がトランスフォーム セットの名前です。

トラフィックを保護する方法も定義する IKEv2 プロポーザルを設定するには、**crypto ipsec ikev2 ipsec-proposal** コマンドを入力してプロポーザルを作成し、そのプロポーザルに対して複数の暗号化および整合性のタイプを指定できる ipsec プロポーザル コンフィギュレーション モードを開始します。

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]

次に例を示します。

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
```

この例では、プロポーザルの名前は secure です。プロトコルおよび暗号化タイプを入力します。

```
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
```

ステップ 3　クリプト マップを作成するには、次の手順を実行します。

a.　アクセス リストをクリプト マップに割り当てます。

crypto map *map-name seq-num* **match address** *access-list-name*

次の例では、mymap がクリプト マップ セットの名前です。マップ セットのシーケンス番号は 10 です。シーケンス番号は、1 つのクリプト マップ セット内の複数のエントリにランクを付けるために使用します。シーケンス番号が小さいほど、プライオリティが高くなります。

```
crypto map mymap 10 match address 101
```

この例では、アクセス リスト 101 がクリプト マップ「mymap」に割り当てられます。

b.　IPsec で保護されたトラフィックの転送先となるピアを指定します。

crypto map *map-name seq-num* **set peer** *ip-address*

次に例を示します。

```
crypto map mymap 10 set peer 192.168.1.100
```

ASA 1000Vは、ピアに IP アドレス 192.168.1.100 が割り当てられている SA をセットアップします。このコマンドを繰り返して、複数のピアを指定します。

c. このクリプト マップに対して、IKEv1 トランスフォーム セットと IKEv2 プロポーザルのどちらを許可するかを指定します。複数のトランスフォーム セットまたはプロポーザルをプライオリティ順（最高のプライオリティのものが最初）に列挙します。これら 2 つのコマンドのいずれかを使用して、クリプト マップで最大 11 個のトランス フォーム セットまたはプロポーザルを指定できます。

```
crypto map map-name seq-num set ikev1 transform-set transform-set-name1
[transform-set-name2, …transform-set-name11]

crypto map map-name seq-num set ikev2 ipsec-proposal proposal-name1
[proposal-name2, … proposal-name11]
```

例（IKEv1 の場合）:

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

この例では、トラフィックがアクセス リスト 101 に一致すると、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、myset1（第 1 プライオリティ）と myset2（第 2 プライオリティ）のいずれかを使用できます。

d. （任意）グローバル ライフタイムを上書きする場合は、クリプト マップの SA ライフタイムを指定します。

```
crypto map map-name seq-num set security-association lifetime {seconds seconds |
kilobytes kilobytes}
```

次に例を示します。

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

この例では、クリプト マップ mymap 10 の時間ライフタイムを 2700 秒（45 分）に短縮します。トラフィック量ライフタイムは変更されません。

e. （任意）IPsec がこのクリプト マップに対して新しい SA を要求するときに Perfect Forward Secrecy（PFS; 完全転送秘密）を要求するか、または IPsec ピアから受け取る要求に PFS を要求するかを指定します。

```
crypto map map-name seq-num set pfs [group1 | group2 | group5]
```

次に例を示します。

```
crypto map mymap 10 set pfs group2
```

この例では、クリプト マップ mymap 10 に対して新しい SA をネゴシエートするときに PFS が必要です。ASA 1000V は、新しい SA の 1024 ビットの Diffie-Hellman プライム モジュラス グループを使用します。

ステップ 4　IPsec トラフィックを評価するために、クリプト マップ セットをインターフェイスに適用します。

```
crypto map map-name interface interface-name
```

次に例を示します。

```
crypto map mymap interface outside
```

この例では、ASA 1000V は外部インターフェイスを通過するトラフィックをクリプト マップ mymap と照合して評価し、保護が必要かどうかを判断します。

ダイナミック クリプト マップの使用

ダイナミック クリプト マップは、いずれのパラメータも設定されていないクリプト マップです。ダイナミック クリプト マップは、不足しているパラメータが、ピアの要件に合うように後でダイナミックに取得される（IPsec ネゴシエーションの結果として）ポリシー テンプレートの役割を果たします。ASA 1000Vは、スタティック クリプト マップでピアの IP アドレスがまだ指定されていない場合、ピアでトンネルをネゴシエートさせるためにダイナミック クリプト マップを適用します。これは、次のタイプのピアで発生します。

- パブリック IP アドレスがダイナミックに割り当てられるピア。

  LAN-to-LAN ピアは、DHCP を使用してパブリック IP アドレスを取得できます。ASA 1000Vは、トンネルを開始するときだけこのアドレスを使用します。

- プライベート IP アドレスがダイナミックに割り当てられるピア。

  通常、リモート アクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられたプライベート IP アドレスを持っています 一般に、LAN-to-LAN トンネルには事前に決定されたプライベート ネットワークのセットがあります。これがスタティック マップの設定に使用されるので、結果として IPsec SA の確立にも使用されます。

管理者がスタティック クリプト マップを設定するため、（DHCP または別の方法で）ダイナミックに割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。

（注） ダイナミック クリプト マップには **transform-set** パラメータだけが必要です。

ダイナミック クリプト マップを使用すると、IPsec のコンフィギュレーションが簡単になります。ダイナミック クリプト マップは、ピアが常に事前に決定されるとは限らないネットワークで使用することを推奨します。ダイナミックに割り当てられた IP アドレスを取得するルータにダイナミック クリプト マップを使用します。

ヒント ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合は、注意が必要です。このような **permit** エントリの対象となるトラフィックにマルチキャストやブロードキャストのトラフィックが含まれる場合、該当するアドレス範囲について **deny** エントリをアクセス リストに挿入します。ネットワークとサブネット ブロードキャスト トラフィックに対して、また IPsec で保護しないその他のトラフィックに対しては、必ず **deny** エントリを挿入してください。

ダイナミック クリプト マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。ASA 1000Vは、ダイナミック クリプト マップを使用してリモート ピアとの接続を開始することはできません。ダイナミック クリプト マップ エントリでは、発信トラフィックがアクセス リストの permit エントリと一致しても、対応する SA がまだ存在しない場合、ASA 1000V はそのトラフィックをドロップします。

クリプト マップ セットには、ダイナミック クリプト マップを含めることができます。ダイナミック クリプト マップのセットには、クリプト マップ セットで一番低いプライオリティ（つまり、一番大きいシーケンス番号）を設定し、ASA 1000V が他のクリプト マップを先に評価するようにする必要があります。セキュリティ アプライアンスは、他の（スタティック）マップのエントリが一致しない場合にだけ、ダイナミック クリプト マップのセットを調べます。

スタティック クリプト マップ セットと同様に、ダイナミック クリプト マップ セットにも、同じ dynamic-map-name を持つすべてのダイナミック クリプト マップを含めます。dynamic-seq-num によって、セット内のダイナミック クリプト マップが区別されます。ダイナミック クリプト マップを設定する場合は、IPsec ピアのデータ フローを暗号アクセス リストで識別するために、ACL の許可を挿入します。このように設定しないと、ASA 1000V は、ピアが提示するあらゆるデータ フロー ID を受け入れることになります。

注意　ダイナミック クリプト マップ セットを使用して設定された、ASA 1000V インターフェイスにトンネリングされるトラフィックに対して、モジュールのデフォルト ルートを割り当てないでください。トンネリングされるトラフィックを指定するには、ダイナミック クリプト マップに ACL を追加します。リモート アクセス トンネルに関連付けられた ACL を設定する場合は、適切なアドレス プールを指定してください。逆ルート注入を使用してルートをインストールするのは、必ずトンネルがアップ状態になった後にしてください。

ダイナミック クリプト マップ エントリを使用するための手順は、スタティック クリプト マップを作成する代わりにダイナミック クリプト マップ エントリを作成するという点を除いて、基本的な IPsec コンフィギュレーションの作成で説明した基本的なコンフィギュレーションと同じです。1 つのクリプト マップ セットの中でスタティック マップ エントリとダイナミック マップ エントリを組み合わせることもできます。

暗号ダイナミック マップ エントリを次のように作成します。

ステップ 1　（任意）アクセス リストをダイナミック クリプト マップに割り当てます。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num match address access-list-name
```

これによって、保護するトラフィックと保護しないトラフィックが決まります。

次に例を示します。

```
crypto dynamic-map dyn1 10 match address 101
```

この例では、アクセス リスト 101 がダイナミック クリプト マップ dyn1 に割り当てられます。マップ シーケンス番号は 10 です。

ステップ 2　このダイナミック クリプト マップに対して、IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルのどちらを許可するかを指定します。IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルのコマンドを使用して、プライオリティ順（最高のプライオリティのものが最初）に複数のトランスフォーム セットまたはプロポーザルをリストします。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev1 transform-set
transform-set-name1, [transform-set-name2, …transform-set-name9]

crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev2 ipsec-proposal
proposal-name1
[proposal-name2, … proposal-name11]
```

例（IKEv1 の場合）：

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

この例では、トラフィックがアクセス リスト 101 に一致すると、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、myset1（第 1 プライオリティ）と myset2（第 2 プライオリティ）のいずれかを使用できます。

ステップ 3　（任意）グローバル ライフタイムを無効にする場合は、ダイナミック クリプト マップの SA ライフタイムを指定します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

次に例を示します。

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

この例では、ダイナミック クリプト マップ dyn1 10 の時間ライフタイムを 2700 秒（45 分）に短縮します。トラフィック量ライフタイムは変更されません。

ステップ 4　（任意）IPsec がこのダイナミック クリプト マップに対して新しい SA を要求するときに PFS を要求するか、または IPsec ピアから受け取る要求に PFS を要求するかを指定します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs** [**group1** | **group2** | **group5** | **group7**]

次に例を示します。

```
crypto dynamic-map dyn1 10 set pfs group5
```

ステップ 5　ダイナミック クリプト マップ セットをスタティック クリプト マップ セットに追加します。

ダイナミック マップを参照するクリプト マップは、必ずクリプト マップ セットの中でプライオリティ エントリを最低（シーケンス番号が最大）に設定してください。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

次に例を示します。

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

サイトツーサイト冗長性の定義

クリプト マップを使用して冗長性を定義することによって、複数の IKEv1 ピアを定義できます。このコンフィギュレーションはサイトツーサイト VPN に便利です。この機能は、IKEv2 ではサポートされていません。

あるピアが失敗すると、ASA 1000V は、クリプト マップに関連付けられている次のピアへのトンネルを確立します。ネゴシエーションが成功したピアにデータが送信されると、そのピアはアクティブなピアになります。アクティブなピアとは、後続のネゴシエーションに対して、ネゴシエーションが失敗するまで ASA 1000V が常に最初に試みるピアのことです。ネゴシエーションが失敗した時点で、ASA 1000V は次のピアに移ります。クリプト マップに関連付けられているすべてのピアが失敗すると、ASA 1000V のサイクルは最初のピアに戻ります。

IPsec コンフィギュレーションの表示

表 26-6 に、IPsec コンフィギュレーションに関する情報を表示するために入力できるコマンドのリストを示します。

表 26-6　IPsec コンフィギュレーション情報を表示するためのコマンド

コマンド	目的
show running-configuration crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。
show running-config crypto ipsec	IPsec コンフィギュレーション全体を表示します。
show running-config crypto isakmp	ISAKMP コンフィギュレーション全体を表示します。
show running-config crypto map	クリプト マップ コンフィギュレーション全体を表示します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show all crypto map	すべてのコンフィギュレーション パラメータ（デフォルト値を持つパラメータも含む）を表示します。

セキュリティ アソシエーションのクリア

一部のコンフィギュレーション変更は、後続の SA をネゴシエートしている間だけ有効になります。新しい設定をただちに有効にするには、既存の SA をクリアして、変更後のコンフィギュレーションで SA を再確立します。ASA 1000V がアクティブに IPsec トラフィックを処理している場合は、SA データベースのうち、コンフィギュレーション変更の影響を受ける部分だけをクリアします。SA データベースを完全にクリアするのは、大規模な変更の場合や、ASA 1000V が処理している IPsec トラフィック量が少ない場合に限定するようにしてください。

表 26-7 に、IPsec SA のクリアと再初期設定に使用できるコマンドのリストを示します。

表 26-7　IPsec SA のクリアおよび再初期設定用のコマンド

コマンド	目的
clear configure crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を削除します。
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップを削除します。特定のダイナミック クリプト マップを削除できるキーワードもあります。
clear configure crypto map	すべてのクリプト マップを削除します。特定のクリプト マップを削除できるキーワードもあります。
clear configure crypto isakmp	ISAKMP コンフィギュレーション全体を削除します。
clear configure crypto isakmp policy	すべての ISAKMP ポリシーまたは特定のポリシーを削除します。
clear crypto isakmp sa	ISAKMP SA データベース全体を削除します。

クリプト マップ コンフィギュレーションのクリア

clear configure crypto コマンドには、IPsec、クリプト マップ、ダイナミック クリプト マップ、CA トラストポイント、すべての証明書、証明書マップ コンフィギュレーション、ISAKMP など、暗号コンフィギュレーションの要素を削除できる引数が含まれます。

引数を指定しないで **clear configure crypto** コマンドを入力すると、暗号コンフィギュレーション全体（すべての認証も含む）が削除されることに注意してください。

詳細については、コマンド リファレンスの **clear configure crypto** コマンドを参照してください。