CHAPTER 68

IPsec と ISAKMP の設定

この章では、バーチャル プライベート ネットワーク（VPN）を構築するためにインターネット 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 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 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 では、IPsec は LAN-to-LAN VPN 接続に使用され、client-to-LAN VPN 接続にも IPsec を使用できます。IPsec 用語では、*ピア*とは、リモート アクセス クライアントまたは別のセキュアなゲートウェイを意味します。どちらの接続タイプについても、ASA は Cisco のピアだけをサポートします。シスコは VPN の業界標準に従っているので、ASA は他ベンダーのピアとの組み合わせでも動作しますが、シスコはこのことをサポートしていません。

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 は発信側または応答側として機能します。IPsec client-to-LAN 接続では、ASA は応答側としてだけ機能します。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。

サイトツーサイト タスクの設定は、シングル コンテキスト モードおよびマルチ コンテキスト モードの両方で実行されます。

（注） マルチ コンテキスト モードが適用されるのは、IKEv2 および IKEv1 のサイトツーサイトのみであり、AnyConnect、クライアントレス SSL VPN、レガシー Cisco VPN クライアント、Apple ネイティブ VPN クライアント、Microsoft ネイティブ VPN クライアント、および IKEv1 IPsec の cTCP には適用されません。

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。

ASA は、レガシー Cisco VPN Client から接続するための IKEv1、および AnyConnect VPN クライアントの IKEv2 をサポートしています。

ISAKMP ネゴシエーションの条件を設定するには、IKE ポリシーを作成します。このポリシーには、次のものが含まれます。

- IKEv1 ピアに要求する認証タイプ。証明書を使用する RSA 署名または事前共有キー（PSK）です。
- 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 は暗号キーとハッシュ キーを導出します。
- IKEv2 の場合は、別の疑似乱数関数（PRF）。IKEv2 トンネル暗号化などに必要な、キー関連情報とハッシュ操作を導出するためのアルゴリズムとして使用されます。
- 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 は暗号キーを置き換えます。

IKEv1 ポリシーでは、各パラメータに対して 1 個の値を設定します。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 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。

リモート アクセス IPsec VPN のライセンス要件

次の表に、この機能のライセンス要件を示します。

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1]
ASA 5505	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10 または 25 セッション。* *共有ライセンスはサポートされていません。*[2] – AnyConnect Essentials ライセンス[3]：25 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： – 基本ライセンス：10 セッション。 – Security Plus ライセンス：25 セッション。
ASA 5510	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス*[2]*：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンスと Security Plus ライセンス：250 セッション。
ASA 5520	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス*[2]*：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：750 セッション。

モデル	ライセンス要件[1]
ASA 5540	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：2500 セッション。
ASA 5550	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。
ASA 5580	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。

モデル	ライセンス要件[1]
ASA 5512-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：250 セッション。
ASA 5515-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：250 セッション。
ASA 5525-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：750 セッション。

モデル	ライセンス要件[1]
ASA 5545-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：2500 セッション。
ASA 5555-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。
ASA 5585-X（SSP-10）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：5000 セッション。

モデル	ライセンス要件[1]
ASA 5585-X（SSP-20、-40、および -60）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。
ASASM	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN： 基本ライセンス：10000 セッション。

1. すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を越えることはできません。ASA 5505 では、組み合わせセッションの最大数は 10（基本ライセンスの場合）または 25（Security Plus ライセンスの場合）です。
2. 共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

3. AnyConnect Essentials ライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。

   （注）AnyConnect Essentials ライセンスの場合、VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントのダウンロードと起動（WebLaunch）を実行できます。

   このライセンスと AnyConnect Premium SSL VPN ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアントソフトウェアには同じクライアント機能のセットが装備されています。

   特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。

   デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、このライセンスをディセーブルにして他のライセンスを使用するには **no anyconnect-essentials** コマンドを使用します。

   AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングルまたはマルチ コンテキスト モードでサポートされます。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フェールオーバーのガイドライン

IPsec VPN セッションは、アクティブ/スタンバイ フェールオーバー コンフィギュレーションでのみ複製されます。アクティブ/アクティブ フェールオーバー コンフィギュレーションはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

ISAKMP の設定

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

この項では、次のトピックについて取り上げます。

- 「IKEv1 および IKEv2 のポリシーの設定」（P.68-10）

IKEv1 および IKEv2 のポリシーの設定

IKE ポリシーを作成するには、シングルまたはマルチ コンテキスト モードのグローバル 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。たとえば、次のように入力します。

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

ポリシーを作成した後は、そのポリシーの設定を指定できます。

表 68-1 および表 68-2 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 68-1　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
authentication	**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 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 などのレガシーな認証方式を使用し、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 (default)	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。
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	
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。

表 68-1　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
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 による IPsec SA のセットアップ機能が高速になります。

表 68-2　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
integrity	**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。MD5 に対する攻撃の成功例がありますが（これは非常に困難ですが）、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。
	null		AES-GCM が暗号化アルゴリズムとして指定されているときは、IKEv2 整合性アルゴリズムとしてヌルを選択できます。
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。

表 68-2　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
	aes-gcm **aes-gcm-192** **aes-gcm-256** **null**	IKEv2 暗号化に使用する AES-GCM アルゴリズムのオプション	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。
policy_index			IKEv2 ポリシー サブモードにアクセスします。
prf	**sha**（デフォルト）	SHA-1（HMAC バリアント）	疑似乱数関数（PRF）を指定します。これは、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。
priority			ポリシー モードを拡張します。追加の IPsec V3 機能がサポートされ、AES-GCM および ECDH の設定が Suite B サポートに含まれるようになります。
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。
	14 19 20 21 24		AnyConnect クライアントは、非 FIPS モードで DH グループ 1、2、および 5 をサポートし、FIPS モードではグループ 2 だけをサポートします。 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 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 はどちらも、最大 20 個の IKE ポリシーをサポートしますが、値のセットはそれぞれ異なります。作成するポリシーのそれぞれに、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。

一致と見なされるのは、2 つのピアからの両方のポリシーに、同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータ値が含まれているときです。IKEv1 では、リモート ピアのポリシーで指定されているライフタイムが、開始側から送信されたポリシーのライフタイム以下であることも必要です。ライフタイムが等しくない場合、ASA 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、各ピアの間でローカルに管理されるので、ライフタイムを各ピアで個別に設定できます。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 や IKEv2 のポリシーはありません。

IKE ポリシーを設定するには、グローバル コンフィギュレーション モードで、**crypto *ikev1* | *ikev2* policy** *priority* 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。

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、次の手順を実行します。ここでは、IKEv1 の例を示します。

（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**]

たとえば、次のように入力します。

```
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**]

たとえば、次のように入力します。

```
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**]

たとえば、次のように入力します。

```
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**]

たとえば、次のように入力します。

```
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*

たとえば、次のように入力します。

```
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 トンネルの終端となるインターフェイスで、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、**crypto** ***ikev1*** | ***ikev2*** **enable** *interface-name* コマンドを、シングルまたはマルチ コンテキスト モードのグローバル コンフィギュレーション モードで実行します。

たとえば、次のように入力します。

```
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 モードとアグレッシブ モードのどちらも使用できます。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 モードではピア間の交換が 2 回だけ必要で、合計 3 メッセージとなります（交換が 3 回で、合計 6 メッセージではなく）。Agressive 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 Main 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。
- Agressive 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、シングルまたはマルチ コンテキスト モードで次のコマンドを入力します。

crypto ikev1 am-disable

たとえば、次のように入力します。

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

Agressive 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。たとえば、次のように入力します。

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

（注）　Agressive モードをディセーブルにすると、Cisco VPN Client は、ASA へのトンネルを確立するための事前共有キー認証を使用できなくなります。ただし、証明書に基づく認証（つまり ASA または RSA）を使用してトンネルを確立できます。

IKEv1 および IKEv2 ISAKMP ピアの識別方式の決定

ISAKMP フェーズ I ネゴシエーション中に、IKEv1 と IKEv2 のどちらの場合も、ピアが互いを識別する必要があります。この識別方式は、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 *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

ASA 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、シングルまたはマルチ コンテキスト モードで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式を「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。このことを実現するために、IPsec トラフィックが UDP データグラムとしてカプセル化されます。これにはポート 4500 が使用されるので、これによって、NAT デバイスにポート情報が提供されます。NAT-T は 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）　AnyConnect クライアントの制限により、AnyConnect クライアントが IKEv2 を使用して接続できるようにするには NAT-T のイネーブル化が必要になります。この要件は、クライアントが NAT-T デバイスの背後になくても適用されます。

Cisco ASA 5505 のホーム ゾーンを除き、ASA は、データ交換を行うクライアントによっては、標準の IPsec、IPsec over TCP、NAT-T、および IPsec over UDP を同時にサポートできます。

各オプションがイネーブルのときの接続の状態を次に示します。

オプション	イネーブルの機能	クライアントの位置	使用する機能
オプション 1	NAT-T がイネーブル	およびクライアントが NAT の背後にある場合は、	NAT-T が使用される
		および NAT が存在しない場合は	ネイティブ IPsec（ESP）が使用される
オプション 2	IPsec over UDP がイネーブル	およびクライアントが NAT の背後にある場合は、	IPsec over UDP が使用される
		および NAT が存在しない場合は	IPsec over UDP が使用される
オプション 3	NAT-T と IPsec over UDP の両方がイネーブル	およびクライアントが NAT の背後にある場合は、	NAT-T が使用される
		および NAT が存在しない場合は	IPsec over UDP が使用される

（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 は自動的に、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ポート 4500 を開きます。

ASA は、次の両方のネットワークではなく、どちらか一方のネットワークで動作する単一の NAT/PAT デバイスの背後にある複数の IPsec ピアをサポートします。

- LAN-to-LAN
- リモート アクセス

混合環境では、リモート アクセス トンネルのネゴシエーションに失敗します。これは、すべてのピアが同じパブリック IP アドレス、つまり NAT デバイスのアドレスから発信されたように見えるためです。また、リモート アクセス トンネルは、LAN-to-LAN トンネル グループ（つまり NAT デバイスの IP アドレス）と同じ名前を使用することが多いため、混合環境では失敗します。この名前の一致により、NAT デバイスの背後にあるピアの LAN-to-LAN とリモート アクセスの混合ネットワークでは、複数のピア間のネゴシエーションが失敗する場合があります。

NAT-T の使用

NAT-T を使用するには、次のサイトツーサイトの手順をシングルまたはマルチ コンテキスト モードで実行する必要があります。

ステップ 1　次のコマンドを入力して、ASA 上でグローバルに IPsec over NAT-T をイネーブルにします。

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　IPsec フラグメンテーション ポリシーに対して暗号化前オプションを選択するために、このコマンドを入力します。

```
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。

IPsec with IKEv1 over TCP のイネーブル化

IPsec/IKEv1 over TCP を使用すると、標準の ESP や IKEv1 が機能できない環境や、既存のファイアウォール ルールを変更した場合に限って機能できる環境で、Cisco VPN クライアントが動作できるようになります。IPsec over TCP は、IKEv1 と IPsec の両方のプロトコルを TCP に似たパケットの中にカプセル化するものであり、NAT と PAT の両方のデバイスとファイアウォールを通過するセキュアなトンネリングを実現します。この機能はデフォルトで無効に設定されています。

（注）　この機能は、プロキシベースのファイアウォールでは動作しません。

IPsec over TCP は、リモート アクセス クライアントで動作します。イネーブル化はグローバルに行います。IKEv1 がイネーブルになっているすべてのインターフェイスで動作します。これは、ASA の機能に対するクライアントにすぎません。LAN-to-LAN 接続では機能しません。

ASA は、データ交換を行うクライアントに応じて、標準の IPsec、IPsec over TCP、NAT-Traversal、および IPsec over UDP を同時にサポートできます。IPsec over TCP は、イネーブルになっている場合、その他のすべての接続方式よりも優先されます。

1 度に 1 つのトンネルをサポートする VPN 3002 ハードウェア クライアントは、標準の IPsec、IPsec over TCP、NAT-Traversal、または IPsec over UDP を使用して接続できます。

ASA とその接続先のクライアントの両方で IPsec over TCP をイネーブルにします。

最大 10 個のポートを指定して、それらのポートに対して IPsec over TCP をイネーブルにできます。ポート 80（HTTP）やポート 443（HTTPS）などの周知のポートを入力すると、そのポートに関連付けられているプロトコルがパブリック インターフェイスで機能しなくなることを示すアラートが表示されます。その結果、パブリック インターフェイスを介して ASA を管理するためにブラウザを使用することができなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

デフォルトのポートは 10000 です。

ASA だけでなく、クライアントでも TCP ポートを設定する必要があります。クライアントの設定には、ASA 用に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。

IKEv1 の IPsec over TCP を ASA でグローバルにイネーブルにするには、次のコマンドをシングルまたはマルチ コンテキスト モードで実行します。

```
crypto ikev1 ipsec-over-tcp [port port 1...port0]
```

次の例では、IPsec over TCP をポート 45 でイネーブルにしています。

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

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ら ASA を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。

すべてのアクティブ セッションが自発的に終了するのを待って ASA をリブートする機能をイネーブルにするには、次のサイトツーサイト タスクをシングルまたはマルチ コンテキスト モードで実行します。

```
crypto isakmp reload-wait
```

たとえば、次のように入力します。

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

reload コマンドを使用して、ASA 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

リモート アクセスや LAN-to-LAN のセッションがドロップする理由には、さまざまなものがあります。たとえば、ASA 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、管理者による停止です。

ASA は、限定されたピア、つまり Cisco VPN Client と VPN 3002 ハードウェア クライアントに対して、セッションが接続解除される直前に通知できます（LAN-to-LAN コンフィギュレーションの場合）。アラートを受信したピアまたはクライアントは、その理由を復号化してイベント 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。

限定されたクライアントとピアには次のものが含まれます。

- 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
- Cisco VPN クライアントのうち、バージョン 4.0 以降のソフトウェアを実行しているもの（コンフィギュレーションは不要）
- VPN 3002 ハードウェア クライアントのうち、バージョン 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっているもの
- VPN 3000 シリーズ コンセントレータのうち、バージョン 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっているもの

IPsec ピアへの切断通知をイネーブルにするには、**crypto isakmp disconnect-notify** コマンドをシングルまたはマルチ コンテキスト モードで入力します。

たとえば、次のように入力します。

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

IKEv1 の証明書グループ照合の設定

トンネル グループは、ユーザの接続条件とアクセス権を定義します。証明書グループ照合では、ユーザ証明書のサブジェクト DN または発行者 DN を使用して、ユーザとトンネル グループを照合します。

（注）　証明書グループ照合は IKEv1 と IKEv2 LAN-to-LAN 接続だけに適用されます。IKEv2 リモート アクセス接続は、トンネルグループの webvpn 属性および certificate-group-map の webvpn コンフィギュレーション モードなどに設定されるグループ選択のプルダウンをサポートしています。

証明書のこれらのフィールドに基づいてユーザをトンネル グループと照合するには、まず照合基準を定義したルールを作成し、次に各ルールを目的のトンネル グループに関連付ける必要があります。

証明書マップを作成するには、**crypto ca certificate map** コマンドを使用します。トンネル グループを定義するには、**tunnel-group** コマンドを使用します。

また、証明書グループ照合ポリシーも設定する必要があります。これには、ルールからグループを照合する、Organizational Unit (OU) フィールドからグループを照合する、すべての証明書ユーザにデフォルトのグループを使用する、という方式があります。これらの方式のいずれかまたはすべてを使用できます。

次のセクションでさらに詳しく説明します。

- 「証明書グループ照合のルールとポリシーの作成」（P.68-19）
- 「tunnel-group-map default-group コマンドの使用」（P.68-20）

証明書グループ照合のルールとポリシーの作成

証明書ベースの ISAKMP セッションをトンネル グループにマッピングするためのポリシーとルールを設定し、証明書マップ エントリをトンネル グループに関連付けるには、**tunnel-group-map** コマンドをシングルまたはマルチ コンテキスト モードで入力します。

このコマンドの構文は次のとおりです。

tunnel-group-map enable {*rules* | *ou* | *ike-id* | *peer ip*}

tunnel-group-map [*rule-index*] **enable** *policy*

policy	証明書からトンネル グループ名を取得するためのポリシーを指定します。*policy* は次のいずれかです。 *ike-id*：トンネル グループがルール ルックアップに基づいて特定されず、OU からも取得されない場合に、証明書ベースの ISAKMP セッションをフェーズ 1 ISAKMP ID の内容に基づいてトンネル グループにマッピングすることを示します。 *ou*：トンネル グループをルール検索によって決定しない場合、サブジェクト認定者名（DN）の OU の値を使用することを示します。 *peer-ip*：トンネル グループがルール ルックアップに基づいて特定されず、*OU* や *ike-id* 方式からも取得されない場合に、ピアの IP アドレスを使用することを示します。 *rules*：証明書ベースの ISAKMP セッションが、このコマンドによって設定された証明書マップの関連付けに基づいて、トンネル グループにマッピングされることを示します。
rule index	（任意）**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

次のことに注意してください。

- 各呼び出しが一意であり、マップ インデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。
- ルールは 255 文字以下です。
- 1 つのグループに複数のルールを割り当てられます。複数のルールを割り当てるには、まずルールのプライオリティを追加し、グループ化します。次に、各グループに必要な数だけ基準文を定義します。1 つのグループに複数のルールを割り当てた場合、テストされる最初のルールの照合結果は一致します。
- ルールを 1 つだけ作成すると、すべての条件に一致したときにのみユーザを特定のトンネル グループに割り当てることができるようになります。すべての照合基準が必要であることは、論理 AND 操作に相当します。または、ユーザを特定のトンネル グループに割り当てる前にすべての照合基準が必要な場合は、基準ごとに 1 つのルールを作成します。照合基準が 1 つだけ必要であることは、論理 OR 操作に相当します。

次の例では、フェーズ 1 の ISAKMP ID の内容に基づいて、証明書ベースの ISAKMP セッションをトンネル グループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

次の例では、ピアの IP アドレスに基づいて、証明書ベースの ISAKMP セッションをトンネル グループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

次の例では、サブジェクト認定者名（DN）の組織ユニット（OU）に基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

次の例では、設定されたルールに基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

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 を設定する手順について説明します。次の項目について説明します。

- 「IPsec トンネルの概要」（P.68-21）
- 「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」（P.68-21）
- 「クリプト マップの定義」（P.68-22）

IPsec トンネルの概要

IPsec トンネルとは、ASA がピア間に確立する SA のセットのことです。SA とは、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するものであり、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 セットや IKEv2 プロポーザルは、ASA によるデータ保護の方法を定義するセキュリティ プロトコルとアルゴリズムの組み合わせです。IPsec SA のネゴシエート時に、ピアはそれぞれトランスフォーム セットまたはプロポーザルを指定しますが、これは両ピアで同一であることが必要です。ASA は、この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使用して SA を作成し、この SA によってクリプト マップに対するアクセス リストのデータ フローが保護されます。

IKEv1 トランスフォーム セットでは、各パラメータに対して 1 個の値を設定します。IKEv2 プロポーザルでは、単一のプロポーザルに対して、複数の暗号化および認証のタイプ、および複数の整合性アルゴリズムを設定できます。ASA 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 の作成に使用されたトランスフォーム セットまたはプロポーザルの定義が変更された場合は、ASA 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」（P.68-41）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唯一の要素が消去または削除された場合は、ASA はそのトランスフォーム セットまたはプロポーザル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。使用できるキーワードには次のものがあります。

- 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）。
- 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。ピアのセキュリティ設定の照合に使用されます。

*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。次のサイトツーサイト タスクでは、シングルまたはマルチ コンテキスト モードでクリプト マップを作成またはクリプト マップに追加します。

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

access-list-name では、アクセス リスト ID を、最大 241 文字の文字列または整数として指定します。

ヒント　すべて大文字にすると、アクセス リスト ID がコンフィギュレーション内で見つけやすくなります。

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 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。

```
[no] crypto map <map_name> <map_index> set pfs [group1 | group2 | group5 | group14 |
group19 | group20 | group21 | group24]
```

暗号化マップの Perfect Forward Secrecy（FCS）に使用する ECDH グループを指定します。暗号化マップに対して group14 および group24 オプションを設定することはできなくなります（IKEv1 ポリシーを使用するとき）。

```
[no]crypto map <name> <priority> set validate-icmp-errors
OR
[no]crypto dynamic-map <name> <priority> set validate-icmp-errors
```

着信 ICMP エラー メッセージを、暗号化マップとダイナミック暗号化マップのどちらに対して検証するかを指定します。

```
[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df}
OR
[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]
```

暗号化マップまたはダイナミック暗号化マップの、既存の Do Not Fragment（DF）ポリシー（セキュリティ アソシエーション レベル）を設定します。

- *clear-df* : DF ビットを無視します。

- *copy-df* : DF ビットを維持します。
- *set-df* : DF ビットを設定して使用します。

```
[no] crypto map <name> <priority> set tfc-packets [burst <length | auto] [payload-size
<bytes | auto> [timeout <seconds | auto>
OR
[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto]
[payload-size <bytes | auto> [timeout <seconds | auto>
```

管理者は、IPsec セキュリティ アソシエーションにおける、ランダムな長さおよび間隔のダミーのトラフィック フローの機密性（TFC）パケットをイネーブルにできます。TFC をイネーブルにするには、IKEv2 IPsec プロポーザルが設定されている必要があります。

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 は 10.0.0.0 サブネットから 10.1.1.0 サブネットへのすべてのトラフィックに対して、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 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は、ASA はポリシーに一致するスタティック クリプト マップを探しますが、見つからない場合は、クリプト マップ セット内のダイナミック クリプト マップの中で見つかるものを探します。これは、ピアのオファーを受け入れるか拒否するかを決定するためです。

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。応答側ピアがダイナミック クリプト マップを使用している場合は、ASA 側でも互換性のあるクリプト ACL が含まれていることが、IPsec を適用するための要件の 1 つです。
- 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 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 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 68-3 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 68-3　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	Response
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 プロポーザルの中の設定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したら、ASA は関連付けられた 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。

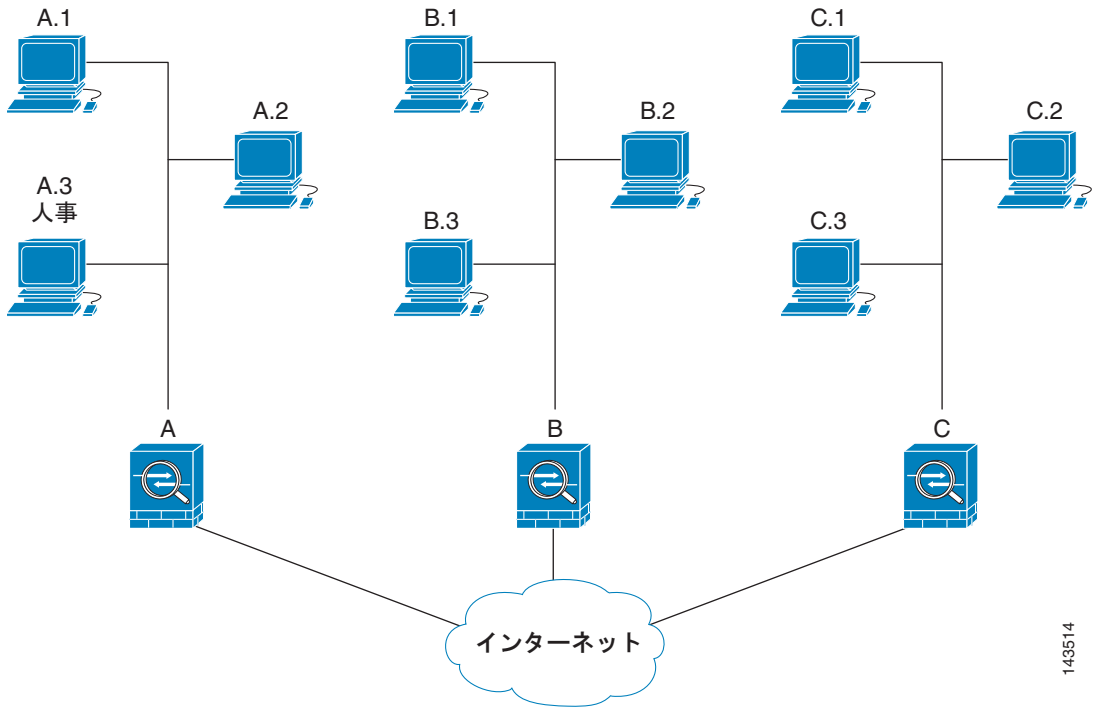
暗号化された着信パケットに対しては、セキュリティ アプライアンスは送信元アドレスと ESP SPI を使用して、パラメータの復号化を決定します。セキュリティ アプライアンスは、パケットを復号化した後で、復号化されたパケットの内部ヘッダーを、そのパケットの SA に関連付けられている ACL の許可 ACE と比較します。内部ヘッダーがプロキシと一致しない場合、セキュリティ アプライアンスはそのパケットをドロップします。内部ヘッダーがプロキシと一致する場合、セキュリティ アプライアンスはそのパケットをルーティングします。

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 68-1 に、ASA の LAN-to-LAN ネットワークの例を示します。

図 68-1　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 68-1 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 セットを割り当てます。

セキュリティ アプライアンス A を発信トラフィック用に設定するには、2 つのクリプト マップを作成します。1 つはホスト A.3 からのトラフィック用で、もう 1 つはネットワーク A の他のホストからの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。

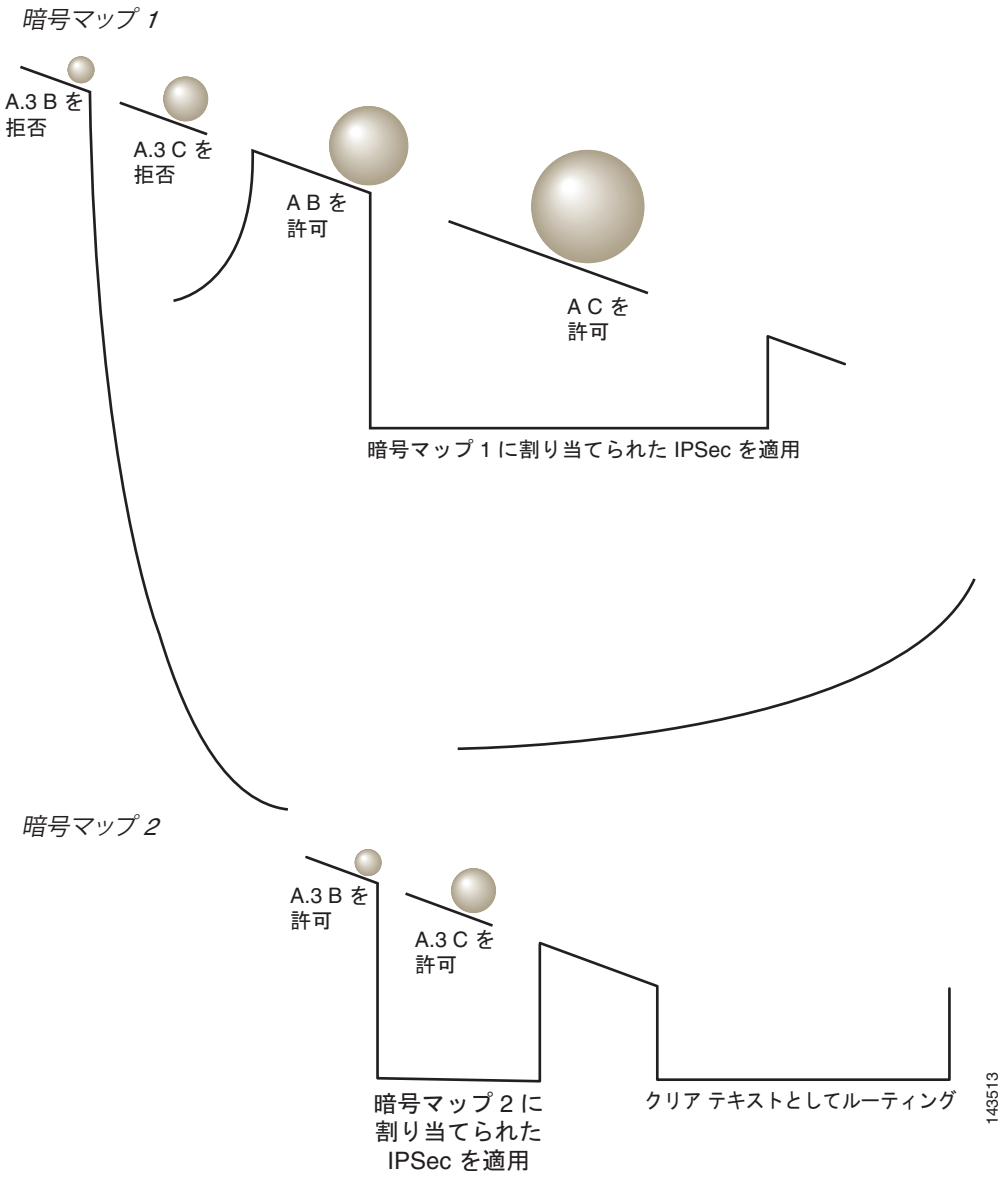
カスケード ACL とは、拒否 ACE を挿入することで、ACL の評価をバイパスし、クリプト マップ セット内の次の ACL の評価を再開するものです。クリプト マップごとに異なる IPsec 設定を関連付けることができるため、拒否 ACE を使用することで、特別なトラフィックを対応するクリプト マップでの以後の評価から除外し、異なるセキュリティを提供する別のクリプト マップ、または異なるセキュ

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 68-2 に、この例の概念的な 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 68-2　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 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。

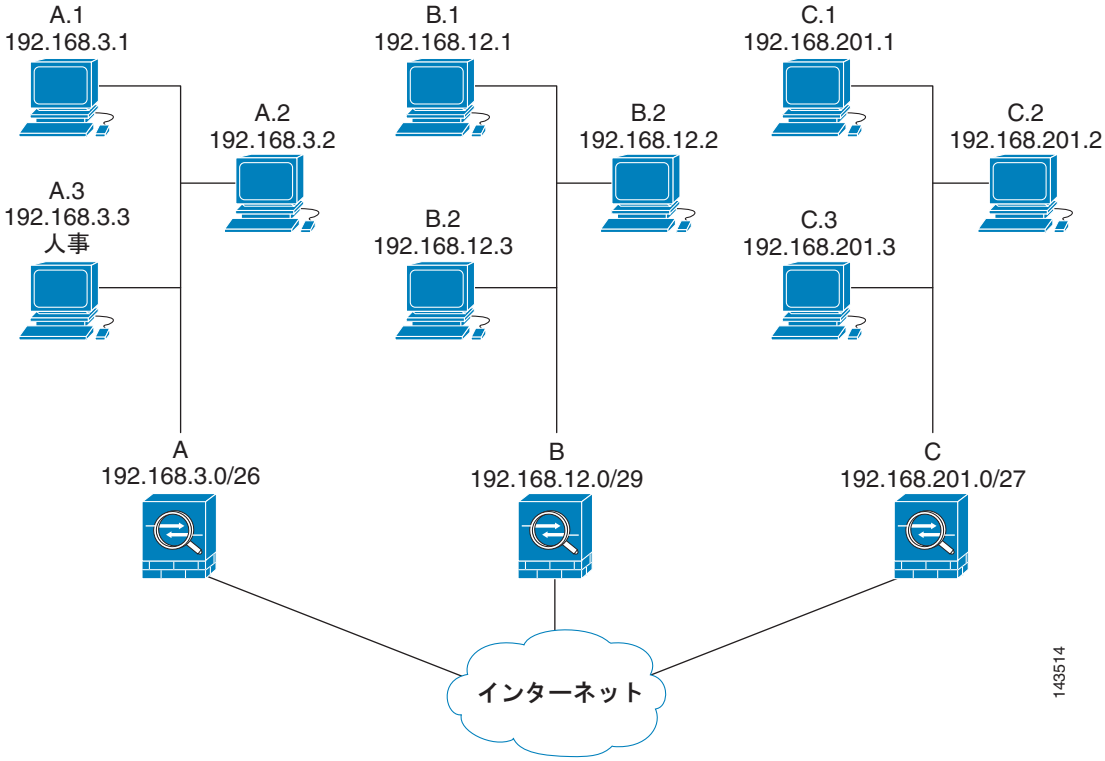
表 68-4 に、図 68-1 の 3 台の ASA 用に設定されたクリプト マップに割り当てられている ACL を示します。

表 68-4　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 68-3 では、図 68-1 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 68-3　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 68-3 の IP アドレスを表 68-4 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 68-5　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

この例のネットワークで示した論法を応用すると、カスケード ACL を使用して、1 台の ASA 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それぞれ異なる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 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、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。それには、そのネットワークとの間のトラフィックを許可する ACE を挿入します。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
```

公開キー インフラストラクチャ（PKI）キーの管理

キー ペアを生成またはゼロ化するときに Suite-B ECDSA アルゴリズムを選択できるようにするには、公開キー インフラストラクチャ（PKI）を設定する必要があります。

前提条件

RSA または ECDSA のトラスト ポイントを認証に使用するように暗号化マップを設定する場合は、最初にキー セットを生成する必要があります。これで、そのトラスト ポイントを作成して、トンネル グループ コンフィギュレーションの中で参照できるようになります。

制約事項

4096 ビットの RSA キーは、5580、5585、およびそれ以降のプラットフォームでのみサポートされます。

手順の詳細

ステップ 1　キー ペアを生成するときに Suite-B ECDSA アルゴリズムを選択します。

```
crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 |
4096 ] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521]
| noconfirm] ]
```

ステップ 2　キー ペアをゼロ化するときに Suite-B ECDSA アルゴリズムを選択します。

```
crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]
```

暗号化コアのプールの設定

AnyConnect TLS/DTLS トラフィックに対してより適切なスループット パフォーマンスが得られるように、対称型マルチプロセッシング（SMP）プラットフォーム上での暗号化コアの割り当てを変更することができます。この変更によって、SSL VPN データパスが高速化され、AnyConnect、スマートトンネル、およびポート転送において、ユーザが認識できるパフォーマンス向上が実現します。暗号化コアのプールを設定するには、次の手順を実行します。

制限事項

- 暗号化コア再分散ができるのは、次のプラットフォームです。
  - 5585
  - 5580
  - 5545/5555
  - ASA-SM
- ラージ モジュラス演算を使用できるのは、5510、5520、5540、および 5550 プラットフォームだけです。

手順の詳細

ステップ 1　次の 3 つの相互排他的オプションの 1 つを指定して暗号化コアのプールを設定します。

- balanced：暗号化ハードウェア リソースを均等に分散します（Admin/SSL および IPsec コア）。
- ipsec：IPsec を優先するように暗号化ハードウェア リソースを割り当てます（SRTP 暗号化音声トラフィックを含む）。

- ssl：Admin/SSL を優先するように暗号化ハードウェア リソースを割り当てます。

```
asa1(config)# crypto engine ?

configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors

asa1(config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl - Allocate crypto hardware resources to favor SSL

asa1(config)# crypto engine accelerator-bias ssl
```

ステップ 2　ハードウェアでラージ モジュラス演算を実行します。

```
large-mode-accel
```

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 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 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 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 エントリが関連付けられているデータ フローを許可する必要があります。これは、ネゴシエーション中に確実に受け入れられるようにするためです。

トラフィックが着信か発信かに関係なく、ASA 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。

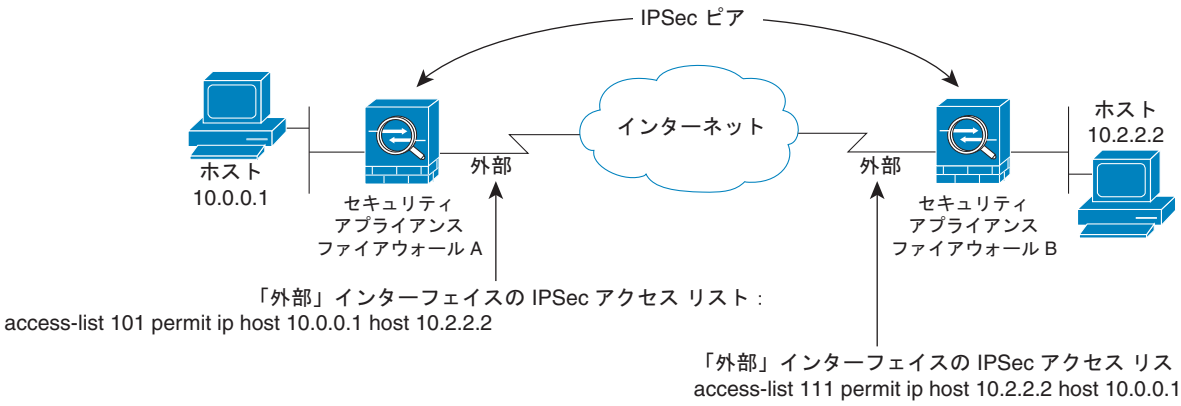
ステップ 2　作成したアクセス リストを、同じクリプト マップ名を使用して 1 つまたは複数のクリプト マップにマッピングします。

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

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 68-4 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 68-4　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 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 マップに対して指定するすべてのクリプト アクセス リストについて、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推奨します。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 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 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** が設定されているときに、外部インターフェイスのアクセス グループが deny ip any any アクセス リストを呼び出すように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は許可されます。

保護されたネットワークへの、サイトツーサイトまたはリモート アクセス VPN 経由でのアクセスをコントロールするために、**no sysopt permit** コマンドを外部インターフェイス上のアクセス コントロール リスト（ACL）と組み合わせて使用しようとしても、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

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 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 に不可欠な要素です。キーは同時にタイムアウトするので、キーのリフレッシュが必要です。各 SA には、「指定時刻」と「トラフィック量」の 2 種類のライフタイムがあります。それぞれのライフタイムを過ぎると SA は失効し、新しい SA のためのネゴシエーションが開始します。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 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 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*

たとえば、次のように入力します。

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

access-list-name では、アクセス リスト ID を、最大 241 文字の文字列または整数として指定します。*destination-netmask* と *source-netmask* では、IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。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　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 セットを設定するには、次のコマンドを入力します。

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

encryption では、IPsec データ フローを保護するための暗号化方式を指定します。

- esp-aes：AES と 128 ビット キーを使用します。
- esp-aes-192：AES と 192 ビット キーを使用します。
- esp-aes-256：AES と 256 ビット キーを使用します。
- esp-des：56 ビット DES-CBC を使用します。
- esp-3des：トリプル DES アルゴリズムを使用します。
- esp-null：暗号化なし。

authentication では、IPsec データ フローを保護するための暗号化方式を指定します

- esp-md5-hmac：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用します。
- esp-sha-hmac：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用します。
- esp-none：HMAC 認証なし。

たとえば、次のように入力します。

```
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。

IKEv2 プロポーザルを設定するとともに、トラフィックを保護する方法も定義するには、**crypto ipsec ikev2 ipsec-proposal** コマンドを入力すると、プロポーザルが作成され、IPsec プロポーザル コンフィギュレーション モードが開始します。ここで、プロポーザルの暗号化と整合性のタイプを複数指定することができます。

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]
proposal tag は IKEv2 IPsec プロポーザルの名前で、1 ～ 64 文字の文字列です。

たとえば、次のように入力します。

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

この例では、secure がプロポーザルの名前です。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
```

逆に、次のコマンドでは、どの AES-GCM または AES-GMAC アルゴリズムを使用するかを選択します。

```
hostname(config-ipsec-proposal)# [no] protocol esp encryption [3des | aes | aes-192 |
aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 |
des | null]
```

SHA-2 またはヌルが選択されている場合は、どのアルゴリズムを IPsec 整合性アルゴリズムとして使用するかを選択する必要があります。AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

```
hostname(config-ipsec-proposal)# [no] protocol esp integrity [md5 | sha-1 | sha-256 |
sha-384 | sha-512 | null]
```

（注） AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

ステップ 3　（任意）管理者はパス最大伝送単位（PMTU）エージングをイネーブルにして、PMTU 値を元の値にリセットする間隔を設定することができます。

```
hostname(config-ipsec-proposal)# [no] crypto ipsec security-association pmtu-aging
<reset-interval>
```

ステップ 4　クリプト マップを作成するには、シングルまたはマルチ コンテキスト モードを使用して、次のサイトツーサイト手順を実行します。

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*

クリプト マップ セットとは、クリプト マップ エントリの集合です。エントリはそれぞれ異なるシーケンス番号（*seq-num*）を持ちますが、*map name* が同じです。*access-list-name* では、アクセス リスト ID を、最大 241 文字の文字列または整数として指定します。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*

たとえば、次のように入力します。

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

ASA 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。1 つのクリプト マップに最大 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。次の 2 つのいずれかのコマンドを使用します。

```
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]
```

proposal-name1 と *proposal-name11* では、IKEv2 の IPsec プロポーザルを 1 つ以上指定します。各クリプト マップ エントリは、最大 11 個のプロポーザルをサポートします。

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 に一致したときに、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}
```

map-name では、クリプト マップ セットの名前を指定します。*seq-num* では、クリプト マップ エントリに割り当てる番号を指定します。

たとえば、次のように入力します。

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

この例では、クリプト マップ mymap 10 の指定時刻ライフタイムを 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]
```

たとえば、次のように入力します。

```
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 は、1024 ビット Diffie-Hellman プライム モジュラス グループを新しい SA で使用します。

ステップ 5　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
```

map-name では、クリプト マップ セットの名前を指定します。*interface-name* では、ISAKMP IKEv1 ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

たとえば、次のように入力します。

```
crypto map mymap interface outside
```

この例では、ASA 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 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 のピア、およびリモート アクセスするピアは、両方とも DHCP を使用してパブリック IP アドレスを取得できます。ASA 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。通常、VPN クライアントには、スタティック IP アドレスがなく、IPsec ネゴシエーションを発生させるためのダイナミック クリプト マップが必要です。たとえば、ヘッドエンドは IKE ネゴシエーション中に IP アドレスを Cisco VPN Client に割り当て、クライアントはこのアドレスを使用して IPsec SA をネゴシエートします。

（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。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 クリプト マップは、Cisco VPN Client（モバイル ユーザなど）、および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対して使用してください。

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 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 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 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 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 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。

次の手順に従って、ダイナミック クリプト マップ エントリを、シングルまたはマルチ コンテキスト モードを使用して作成します。

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。*dynamic-map-name* では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。

たとえば、次のように入力します。

```
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。マップのシーケンス番号は 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、どの IKEv1 トランスフォーム セットまたは IKEv2 プロポーザル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に（最高のプライオリティのものが最初）指定します。IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルに応じたコマンドを使用してください。

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*]

dynamic-map-name では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。*transform-set-name* は、作成または変更するトランスフォーム セットの名前です。*proposal-name* では、IKEv2 の IPsec プロポーザルの名前を 1 つ以上指定します。

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 に一致したときに、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*}

dynamic-map-name では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。

たとえば、次のように入力します。

```
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 の指定時刻ライフタイムを 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**]

dynamic-map-name では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。*dynamic-seq-num* では、ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。

たとえば、次のように入力します。

```
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*

map-name では、クリプト マップ セットの名前を指定します。*dynamic-map-name* では、既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。

たとえば、次のように入力します。

```
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 マップを使用して複数の IKEv1 ピアを定義すると、冗長性を持たせることができます。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 ではサポートされません。

あるピアが失敗すると、ASA 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、そのピアがアクティブ ピアになります。アクティブ ピアとは、後続のネゴシエーションのときに、ASA が常に最初に試みるピアのことです。これは、ネゴシエーションが失敗するまで続きます。ネゴシエーションが失敗した時点で、ASA 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 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 68-6 に示すコマンドをシングルまたはマルチ コンテキスト モードで入力すると、IPsec コンフィギュレーションに関する情報を表示できます。

表 68-6　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。

表 68-6　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 （続き）

コマンド	目的
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。
show crypto ikev2 sa detail	暗号化統計情報での Suite-B アルゴリズム サポートを表示します。
show crypto ipsec sa	シングルまたはマルチ コンテキスト モードでの Suite-B アルゴリズム サポートおよび ESPv3 IPsec 出力を表示します。
show ipsec stats	シングルまたはマルチ コンテキスト モードでの IPsec サブシステムに関する情報を表示します。ESPv3 統計情報は、受信した TFC パケットおよび有効および無効な ICMP エラーに表示されます。

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 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 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 68-7 に示すコマンドを入力すると、シングルまたはマルチ コンテキスト モードで IPsec SA をクリアして再初期化することができます。

表 68-7　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。

表 68-7　IPsec SA のクリアおよび再初期設定用のコマンド（続き）

コマンド	目的
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。

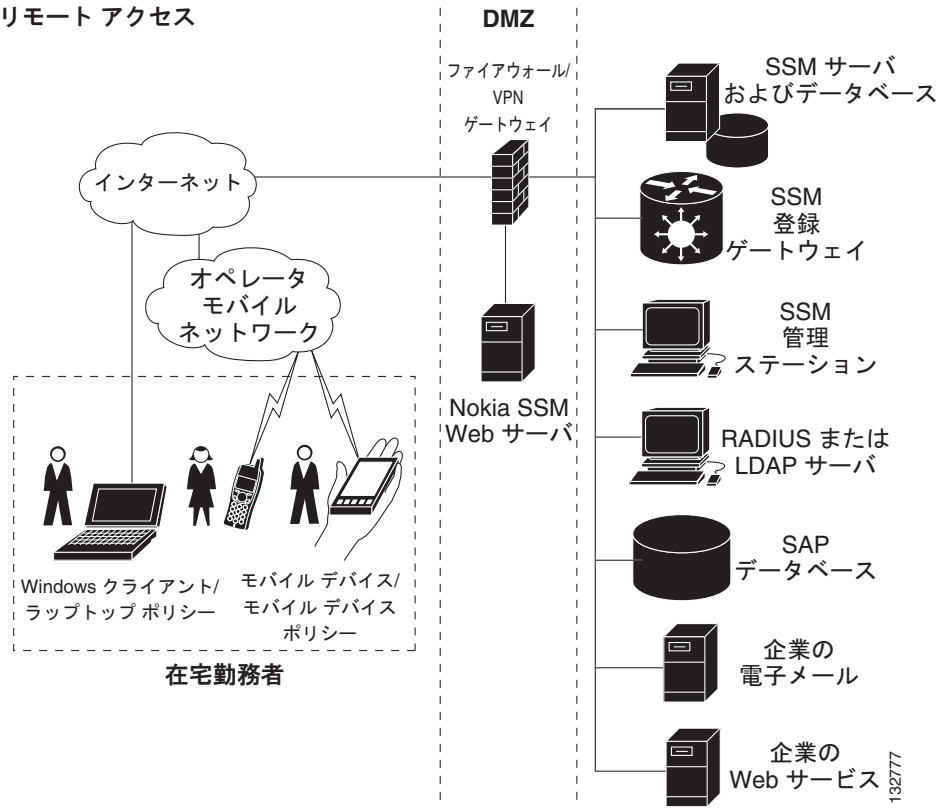
詳細については、『*Cisco ASA Series Command Reference*』の **clear configure crypto** コマンドを参照してください。

Nokia VPN クライアントのサポート

ASA は、Nokia 92xx Communicator シリーズ電話機上の Nokia VPN クライアントからの接続をサポートするために、Challenge/Response for Authenticated Cryptographic Keys（CRACK）プロトコルを使用します。CRACK は、デジタル証明書ではなくレガシーな認証技術を使用している、IPsec に対応したモバイル クライアントに最も適しています。クライアントがレガシーな方式に基づいた秘密キー認証技術（RADIUS など）を使用し、ゲートウェイが公開キー認証を使用している場合に、このプロトコルは相互認証を提供します。

Nokia のクライアントと CRACK プロトコルの両方をサポートするには、Nokia バックエンド サービスが稼働している必要があります。この要件には、図 68-5 に示すように、Nokia Security Services Manager（NSSM）と Nokia のデータベースが含まれます。

図 68-5　Nokia 92xx Communicator サービスの要件



Nokia VPN クライアントをサポートするには、ASA で次の手順を実行します。

- グローバル コンフィギュレーション モードで、**crypto isakmp policy** *priority* **authentication** コマンドに **crack** キーワードを指定して使用し、CRACK 認証をイネーブルにします。たとえば、次のように入力します。

```
hostname(config)# crypto isakmp policy 2
hostname(config-isakmp-policy)# authentication crack
```

クライアント認証にデジタル証明書を使用する場合は、さらに次の手順を実行します。

ステップ 1　トラストポイントを設定し、完全修飾ドメイン名を不要にします。トラストポイントは、NSSM やその他の CA の場合があります。次の例では、トラストポイントには CompanyVPNCA という名前が付いています。

```
hostname(config)# crypto ca trustpoint CompanyVPNCA
hostname(config-ca-trustpoint)# fqdn none
```

ステップ 2　ISAKMP ピアの ID を設定するには、次のいずれかの手順を実行します。

- **crypto isakmp identity** コマンドに **hostname** キーワードを指定して使用します。たとえば、次のように入力します。

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

- **crypto isakmp identity** コマンドに **auto** キーワードを指定して使用し、接続タイプから ID が自動的に判定されるように設定します。たとえば、次のように入力します。

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

（注）　**crypto isakmp identity auto** コマンドを使用する場合は、クライアント証明書に含まれる DN 属性が CN、OU、O、C、St、L の順になっていることを確認します。

Nokia クライアントで CRACK プロトコルをサポートするために必要な Nokia サービスの詳細、およびこれらのサービスのインストールと設定については、Nokia の代理店にお問い合わせください。