IPsec VPN のインターネット キー エクスチェンジの設定

この章では、基本的な IP Security（IPsec; IP セキュリティ）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）用の Internet Key Exchange（IKE; インターネット キー エクスチェンジ）プロトコルの設定方法について説明します。IKE とは、IPsec 標準とともに使用されるキー管理プロトコル標準です。IPsec は、IP パケットに対して強力な認証や暗号化を実現する IP セキュリティ機能です。

IPsec の設定には必ずしも IKE は必要ありませんが、IKE では、IPsec 標準に対する新機能が追加されているほか、設定をより柔軟かつ容易に行えるよう、IPsec のサポートが強化されています。

IKE は、Oakley キー交換や Skeme キー交換を Internet Security Association and Key Management Protocol（ISAKMP; インターネット セキュリティ アソシエーションおよびキー管理プロトコル）フレームワーク内部に実装したハイブリッド プロトコルです（ISAKMP、Oakley、および Skeme は、IKE により実装されるセキュリティ プロトコルです）。

機能情報の入手

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPsec VPN の IKE 設定に関する機能情報」（P.25）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

IKE 設定の前提条件

- 「IPsec を使用した VPN のセキュリティ設定」の章で説明している概念および作業を理解している必要があります。
- ご使用の Access Control List（ACL; アクセス コントロール リスト）が IKE と互換性があることを確認してください。IKE ネゴシエーションではポート 500 で User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用するため、IKE および IPsec が使用するインターフェイスで UDP ポート 500 のトラフィックがブロックされないように ACL を設定しておく必要があります。場合によっては、UDP ポート 500 のトラフィックを明示的に許可するために、ACL にステートメントを追加する必要があります。

IKE 設定の制約事項

IKE ネゴシエーションの設定では、次の制約事項が適用されます。

- ルータの初期化では、リモートピアの認証は*必要ありません*。
- 事前共有キーは、両方のピアで Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用する*必要*があります（事前共有キーを設定するには、**crypto isakmp key** コマンドを入力します）。
- 各通信ルータは、互いの FQDN ホスト エントリを設定に保持している*必要があります*。
- 通信ルータはホスト名で認証するように設定する*必要があります*（IP アドレスでは*ありません*）。このため、**crypto isakmp identity hostname** コマンドを使用する必要があります。

IPsec VPN の IKE 設定について

IPsec VPN の IKE を設定するには、次の概念を理解しておく必要があります。

IKE での使用にサポートされている標準

シスコでは次の標準を採用しています。

- IPsec：IP Security Protocol（IPsec; IP セキュリティ プロトコル）。IPsec はオープン規格のフレームワークであり、これにより、参加ピア間でデータ機密性、データ整合性、およびデータ認証が提供されます。IPsec は、これらのセキュリティ サービスを IP レイヤで提供します。IPsec は、IKE を使用して、ローカル ポリシーに基づいてプロトコルのネゴシエーションおよびアルゴリズムを

処理し、IPsec で使用される暗号化キーと認証キーを生成します。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

- ISAKMP : Internet Security Association and Key Management Protocol（インターネット セキュリティ アソシエーションおよびキー管理プロトコル）。ペイロード形式、キー交換プロトコルの実装メカニズム、およびセキュリティ アソシエーションのネゴシエーションを定義するプロトコル フレームワークです。
- Oakley：キー交換プロトコルの 1 つで、認証済みのキー関連情報を取得する方法を定義します。
- Skeme：キー交換プロトコルの 1 つで、キーをすばやく更新しながら認証済みのキー関連情報を取得する方法を定義します。

IKE での使用に備えて実装されているコンポーネント テクノロジーには次のものがあります。

- AES：Advanced Encryption Standard（AES; 高度暗号化規格）。暗号アルゴリズムの 1 つで、重要ではあるが機密扱いではない情報を保護します。AES は、IPsec および IKE 用のプライバシー変換であり、Data Encryption Standard（DES; データ暗号規格）に代わる規格として開発されました。AES は DES よりセキュリティを向上させるために設計されています。具体的には、AES は、キーのサイズが従来より大きく、侵入者が既知の方式でメッセージを解読するには、キーを総当たりで試すしかありません。AES のキーは可変長であり、アルゴリズムは 128 ビット キー（デフォルト）、192 ビット キー、または 256 ビット キーを指定できます。
- DES：Data Encryption Standard（DES; データ暗号規格）。パケット データの暗号化に使用されるアルゴリズムです。IKE は Explicit IV 標準の 56 ビット DES-CBC を実装しています。Cipher Block Chaining（CBC）では、暗号化の開始に Initialization Vector（IV; 初期ベクター）が必要です。IV は IPsec パケットに明示的に指定されます。

  また Cisco IOS ソフトウェアは、特定のプラットフォームで使用可能なソフトウェア バージョンに応じて、3DES（168 ビット）暗号化も実装します。トリプル DES（3DES）は強力な暗号化方式であり、これにより、機密性の高い情報を非信頼ネットワーク上で送信できます。この暗号化方式を使用することで、（特に金融業界の）お客様はネットワーク レイヤでの暗号化を実現できます。

  （注） 強力な暗号化を使用する Cisco IOS イメージ（56 ビット データ暗号化機能セットを含むがこれに限定されない）は、米国輸出規制の対象となり、配布が制限されます。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合せください。

- SEAL：Software Encryption Algorithm（SEAL; ソフトウェア暗号化アルゴリズム）。ソフトウェア ベースの DES、3DES、および AES に代わるアルゴリズムです。SEAL 暗号化では、160 ビットの暗号キーが使用され、他のソフトウェアベースのアルゴリズムに比べて、CPU に与える影響は小さくなります。
- Diffie-Hellman：公開キー暗号法プロトコルの 1 つで、2 者間に、セキュアでない通信チャネルによる共有秘密を確立できます。Diffie-Hellman は、IKE 内でセッション キーを確立するために使用されます。768 ビット（デフォルト）、1024 ビット、1536 ビットの各 Diffie-Hellman グループがサポートされています。
- MD5：メッセージ ダイジェスト 5（Hash-Based Message Authentication Code（HMAC; ハッシュ ベースのメッセージ認証コード））バリアント）。ハッシュ アルゴリズムの 1 つで、パケット データの認証に使用されます。HMAC は別のレベルのハッシュのバリアントです。
- SHA-2 および SHA-1 ファミリ（HMAC バリアント）：Secure Hash Algorithm（SHA; セキュア ハッシュ アルゴリズム）の 1 および 2。SHA-1 および SHA-2 は、パケット データの認証および IKE プロトコルの整合性確認メカニズムの検証に使用されるハッシュ アルゴリズムです。HMAC は別のレベルのハッシュのバリアントです。SHA-2 ファミリには、SHA-256 ビットのハッシュ ア

ルゴリズムと SHA-384 ビットのハッシュ アルゴリズムが加わっています。この機能は Suite-B の要件に含まれています。Suite-B は、IKE および IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートで構成され、RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。Cisco IOS での Suite-B サポートに関する詳細については、『Configuring Security for VPNs with IPsec』フィーチャ モジュールを参照してください。

- RSA シグニチャおよび RSA 暗号化ナンス：RSA は、ロナルド・リベスト、アディ・シャミア、レオナルド・エーデルマンの 3 人によって開発された公開キー暗号化システムです。RSA シグニチャは否認防止を実行し、RSA 暗号化ナンスは否認を実行します（否認および否認防止は追跡可能性と関係があります）。

IKE は、X.509v3 証明書と相互運用されます。X.509v3 は、認証に公開キーが必要な場合に IKE プロトコルと使用されます。この認証サポートを使用すると、各装置に同等のデジタル ID カードを付与することで、保護されたネットワークを拡張できます。2 つの装置が通信する際、デジタル証明書を交換することで ID を証明します（これにより、各ピアで公開キーを手動で交換したり、各ピアで共有キーを手動で指定したりする必要がなくなります）。

IKE の利点

IKE は自動で IPsec security associations（SA; セキュリティ アソシエーション）をネゴシエーションするため、手間のかかる手動の事前設定をすることなしに IPsec によるセキュアな通信を実現できます。特に、IKE には次のような利点があります。

- 両ピアのクリプト マップで、すべての IPsec セキュリティ パラメータの手動による指定が不要。
- IPsec SA のライフタイムが指定可能。
- IPsec セッション中に暗号キーの変更が可能。
- IPsec でアンチ リプレイ サービスが使用可能。
- Certification Authority（CA; 認証局）のサポートにより、管理可能でスケーラブルな IPsec を実現可能。
- ピアのダイナミック認証が可能。

IKE のメイン モードとアグレッシブ モード

IKE では、キーのネゴシエーションにフェーズ 1 とフェーズ 2 の 2 つのフェーズがあります。フェーズ 1 では、2 つの IKE ピア間でセキュリティ アソシエーション（キー）をネゴシエーションします。フェーズ 1 でキーをネゴシエーションすることで、フェーズ 2 で IKE ピアがセキュアに通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE が IPsec などのその他のアプリケーションにキー（セキュリティ アソシエーション）を設定します。

フェーズ 1 のネゴシエーションは、メイン モードまたはアグレッシブ モードを使用して実行されます。メイン モードでは、ネゴシエーション中にすべての情報が保護されるため、攻撃者が情報にアクセスできなくなります。メイン モードを使用すると、2 つの IKE ピアの ID が非表示になります。このモードでの運用は非常にセキュアですが、ネゴシエーションの実行に比較的時間がかかります。アグレッシブ モードでは、メインモードよりも少ない時間でピア間のキーのネゴシエーションを実行します。ただし、メイン モードでのネゴシエーションでは可能なセキュリティが一部失われます。たとえば、セキュリティ アソシエーションを確立しようとしている 2 つの装置の ID が傍受者に見えてしまいます。

この 2 つのモードは異なった目的で使用し、それぞれ別の強みがあります。メイン モードは、アグレッシブ モードに比べると低速ですが、アグレッシブ モードよりも IKE ピアのセキュリティが高いため、セキュアで柔軟性があります。アグレッシブ モードは柔軟性とセキュリティの点で劣りますが、より高速です。

Cisco IOS ソフトウェアでは、この 2 つのモードは設定できません。IKE 認証（rsa-sig、rsa-encr、または事前共有）ではデフォルトでメイン モードを起動しますが、認証を起動するために必要な情報がなく、ピアのホスト名に関連づけられている事前共有キーがある場合は、Cisco IOS ソフトウェアはアグレッシブ モードを起動できます。Cisco IOS ソフトウェアでは、アグレッシブ モードを開始した IKE ピアには、アグレッシブ モードで応答します。

IPsec VPN の IKE 設定方法

IPsec 実装で IKE を使用しない場合は、**no crypto isakmp** コマンドを使ってすべての IPsec ピアの IKE を無効にし、この章の残りは実行せずに、IPsec VPN を開始します。

（注） IKE を無効にすると、すべてのピアのクリプト マップですべての IPsec SA を手動で指定する必要があります。また、特定の IPsec セッションでピアの IPsec SA がタイムアウトしなくなり、ピア間の IPsec セッション中に暗号キーが変わらなくなり、ピア間でアンチ リプレイ サービスが使用不可になり、公開キー インフラストラクチャ（PKI）サポートが使用できなくなります。

IKE はデフォルトでイネーブルになっています。各インターフェイスについて IKE を個別にイネーブルにする必要はなく、ルータのすべてのインターフェイスについてグローバルにイネーブルになっています。

IPsec ピアの認証、IPsec SA のネゴシエーション、IPsec キーの確立を実行するには、次の作業を実行します。

- 「IKE ポリシーの作成：IKE ネゴシエーションのセキュリティ パラメータ」（P.5）（必須）
- 「IKE 認証の設定」（P.10）（必須）
- 「IKE モード コンフィギュレーションの設定」（P.17）
- 「IPsec SA ネゴシエーションのための IKE クリプト マップの設定」（P.19）

IKE ポリシーの作成：IKE ネゴシエーションのセキュリティ パラメータ

IKE ポリシーを使い、IKE ネゴシエーション中に使用するセキュリティ パラメータの組み合せを定義します。IKE 交換に関係する各ピアで IKE ポリシーを作成する必要があります。

IKE ポリシーを 1 つも設定しない場合、ルータはデフォルトのポリシーを使用します。デフォルトのポリシーは、常にプライオリティが最低に設定されており、各パラメータはデフォルト値に設定されています。

IKE ポリシーについて

IKE ネゴシエーションは保護する必要があるため、各 IKE ネゴシエーションは、共有（共通）の IKE ポリシーについて両ピアが同意することで開始されます。このポリシーには、次の IKE ネゴシエーションを保護するために使用するセキュリティ パラメータとピアの認証方法を記述します。

両ピアがポリシーに同意すると、各ピアに確立されている SA によってポリシーのセキュリティ パラメータが識別され、ネゴシエーションにおける以降すべての IKE トラフィックに適用されます。

各ピアには、パラメータ値の組み合せをそれぞれ変えることでプライオリティをつけたポリシーを複数設定できます。ただし、そのうちの少なくとも 1 つのポリシーには、リモート ピアのポリシーのいずれかとまったく同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値が設定されている必要があります。作成する各ポリシーに対して、一意のプライオリティを割り当てます（1 ～ 10,000 で指定し、1 が最大のプライオリティ）。

ヒント サポートされているパラメータの値が 1 つしかないデバイスを使用する場合は、もう一方の装置でサポートされている値を設定する必要があります。この制限は別にすれば、セキュリティとパフォーマンスには通常トレードオフの関係があり、パラメータ値の多くにはこのトレードオフがあります。ネットワークのセキュリティ リスクのレベルと、そのリスクに対する許容度を評価する必要があります。

一致した IKE ポリシーに同意する IKE ピア

IKE ネゴシエーションが開始されると、IKE は、両方のピアにある同じ IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモート ピアに送信し、リモート ピアの方では一致するポリシーを探そうとします。リモート ピアは、自分のプライオリティ 1 位のポリシーと、相手のピアから受け取ったポリシーを比較し、一致するポリシーを探します。一致するポリシーが見つかるまで、リモート ピアはプライオリティが高い順に各ポリシーをチェックします。

2 つのピアのポリシーが一致するのは、2 つのピアが同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値を持ち、リモート ピアのポリシーに指定されているライフタイムが、比較しているポリシーのライフタイム以下の場合です（ライフタイムが同一でない場合は、リモート ピアのポリシーのライフタイムよりも短いライフタイムが使用されます）。

一致した場合は、IKE がネゴシエーションを完了し、IPsec セキュリティ アソシエーションが作成されます。一致するポリシーが見つからなかった場合は、IKE はネゴシエーションを拒否し、IPsec は確立されません。

（注） このパラメータ値は、IKE SA の確立後 IKE ネゴシエーションに適用されます。

（注） ポリシーに指定する認証方式によっては、追加の設定が必要な場合があります（「IKE 認証の設定」（P.10）の項を参照）。ピアのポリシーに必要な設定がされていないと、一致するポリシーをリモート ピアで検索するときに、ピアはポリシーを送信しません。

制約事項

AES IKE ポリシーの設定には、次のような制約があります。

- ルータが IPsec およびロング キー（「k9」サブシステム）をサポートしている必要がある。
- アクセラレーション カードを使用している場合、AES は IPsec および IKE トラフィックを暗号化できない。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}

5. **hash** {**sha** | **sha256** | **sha384** | **md5**}
6. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
7. **group** {**1** | **2** | **5** | **14** | **15** | **16** | **19** | **20**}
8. **lifetime** *seconds*
9. **exit**
10. **exit**
11. **show crypto isakmp policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp policy** *priority* **例：** `Router(config)# crypto isakmp policy 10`	IKE ポリシーを定義し、config-isakmp コンフィギュレーション モードを開始します。 • *priority* : IKE ポリシーを一意に識別し、ポリシーにプライオリティを割り当てます。有効な値：1 ～ 10,000。1 が最大プライオリティ。
ステップ 4	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**} **例：** `Router(config-isakmp)# encryption aes 256`	暗号化アルゴリズムを指定します。 • デフォルトでは **des** キーワードが使用されます。 – **des** : 56 ビット DES-CBC – **3des** : 168 ビット DES – **aes** : 128 ビット AES – **aes 192** : 192 ビット AES – **aes 256** : 256 ビット AES
ステップ 5	**hash** {**sha** | **sha256** | **sha384** | **md5**} **例：** `Router(config-isakmp)# hash sha`	ハッシュ アルゴリズムを指定します。 • デフォルトでは SHA-1（**sha**）が使用されます。 • **sha256** キーワードは、ハッシュ アルゴリズムに SHA-2 ファミリの 256 ビット（HMAC バリアント）を指定します。 • **sha384** キーワードは、ハッシュ アルゴリズムに SHA-2 ファミリの 384 ビット（HMAC バリアント）を指定します。 • **md5** キーワードは、ハッシュ アルゴリズムに MD5（HMAC バリアント）を指定します。 **（注）** 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。

	コマンドまたはアクション	目的
ステップ 6	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**} **例：** `Router(config-isakmp)# authentication pre-share`	認証方式を指定します。 • デフォルトでは RSA シグネチャが使用されます。 – **rsa-sig**：RSA シグネチャでは、CA から認証書を取得するようにピア ルータを設定する必要があります。 – **rsa-encr**：RSA 暗号化ナンスでは、各ピアが他のピアの RSA 公開キーを保持するように設定する必要があります。 – **pre-share**：事前共有キーでは、事前共有キーを個別に設定する必要があります。
ステップ 7	**group** {**1** | **2** | **5** | **14** | **15** | **16** | **19** | **20**} **例：** `Router(config-isakmp)# group 1`	Diffie-Hellman（DH）グループ ID を指定します。 • デフォルトでは D-H グループ 1 が使用されます。 – **1**：768 ビット DH – **2**：1024 ビット DH – **5**：1536 ビット DH – **14**：2048 ビット DH グループを指定します。 – **15**：3072 ビット DH グループを指定します。 – **16**：4096 ビット DH グループを指定します。 – **19**：256 ビット Elliptic Curve DH（ECDH）グループを指定します。 – **20**：384 ビット ECDH グループを指定します。 **（注）** 1024 ビットおよび 1536 ビットの DH オプションを使用すると、「解読」がより困難になる一方、実行に必要な CPU 時間が増えます。 **（注）** **group 5** は 128 ビット キーに使用できますが、group 14 がより適しています。 **（注）** 選択するグループは、ネゴシエーション中の IPsec キーを保護するため、十分強力（十分なビット数がある）である必要があります。特定のサイズのキーを保護するために Diffie-Hellman クループに必要なビット数についての見解には相違がありますが、一般的に、**group 14** は 128 ビット キー、**group 15** は 192 ビット キー、および **group 16** は 256 ビット キーの保護に適しているとの合意があります。
ステップ 8	**lifetime** *seconds* **例：** `Router(config-isakmp)# lifetime 180`	IKE SA のライフタイムを指定します。 • *seconds*：各 SA が満了するまでの時間（秒）。有効な値：60 ～ 86,400 秒、デフォルト値：86,400。 **（注）** ライフタイムを短くするほど（ポイントまで）、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムを長くすれば、以後の IPsec SA をそれだけ速くセットアップできます。

	コマンドまたはアクション	目的
ステップ 9	**exit** **例：** `Router(config-isakmp)# exit`	config-isakmp コンフィギュレーション モードを終了します。
ステップ 10	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show crypto isakmp policy** **例：** `Router# show crypto isakmp policy`	（任意）既存の IKE ポリシーをすべて表示します。
ステップ 12	作成するポリシーそれぞれについて上記の手順を繰り返します。	—

例

次に、**show crypto isakmp policy** コマンドからの出力で、ハードウェアがサポートしていない IKE 暗号化方式を設定しようとしたときに表示される警告メッセージの例を示します。

```
Router# show crypto isakmp policy

Protection suite of priority 1
        encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
        hash algorithm:        Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group:  #1 (768 bit)
        lifetime:              3600 seconds, no volume limit
```

トラブルシューティングのヒント

- **clear crypto sa** EXEC コマンドを使用して IPsec SA を消去（および再初期化）します。

  パラメータを指定せずに **clear crypto sa** コマンドを使用すると、SA データベースの内容が完全に消去されるので、アクティブなセキュリティ セッションが消去されます。SA データベースのサブセットだけを消去するには、**peer**、**map**、または **entry** キーワードも指定します。詳細については、『*Cisco IOS Security Command Reference*』の **clear crypto sa** コマンドを参照してください。

- デフォルト ポリシーおよび設定されているポリシーのデフォルト値は、**show running-config** コマンドの発行時には設定に表示されません。デフォルト ポリシーおよび設定されているポリシーのデフォルト値を確認するには、**show crypto isakmp policy** コマンドを使用してください。

- 使用しているハードウェアがサポートしていない IPsec トランスフォームまたは IKE 暗号化方式はすべて無効にしてください。無効にしておくと、ピアとのネゴシエーションのときに常に無視されます。

  ハードウェアがサポートしていない IPsec トランスフォームまたは IKE 暗号化方式を入力すると、警告メッセージが表示されます。この警告メッセージはブート時にも表示されます。暗号化カードを挿入すると、現在の設定がスキャンされます。ハードウェアがサポートしていない IPsec トランスフォームまたは IKE 暗号化方式が検出されると、警告メッセージが表示されます。

次の作業

IKE ポリシーで指定した認証方式（RSA シグニチャ、RSA 暗号化ナンス、事前共有キー）によっては、IKE および IPsec が IKE ポリシーを正常に使用できるように、特定の設定作業を追加で実行する必要があります。この追加作業実行に関する詳細については、「IKE 認証の設定」（P.10）を参照してください。

AES ベースのトランスフォーム セットを設定する方法については、「IPsec を使用した VPN のセキュリティの設定」の章を参照してください。

IKE 認証の設定

認証方式を指定（またはデフォルト方式を設定）した IKE ポリシーを少なくとも 1 つ作成したら、認証方式を設定する必要があります。認証方式を正常に設定しなければ、IPsec が IKE ポリシーを使用できません。

IKE 認証を設定するには、状況に応じて次の作業のいずれかを実行する必要があります。

- 「RSA 暗号化ナンスの RSA キーの手動設定」（P.11）
- 「事前共有キーの設定」（P.14）

IKE 認証方式：概要

IKE 認証は、RSA シグニチャ、RSA 暗号化ナンス、事前共有キーの 4 つのオプションで構成されています。各認証方式では、次の設定が追加で必要です。

RSA シグニチャ

RSA シグニチャでは、CA から証明書を取得するようにピアを設定できます（証明書を発行するように CA が正しく設定されている必要があります）。CA を使用すると、IPsec ネットワークの管理性とスケーラビリティが大幅に向上します。また、RSA シグニチャ ベースの認証で使用できる公開キー操作は 2 つだけです。これに対し、RSA 暗号化では 4 つの公開キー操作を使用しますが、その分だけ全体のパフォーマンスが下がります。CA サポートを適切に設定するには、「Deploying RSA Keys Within a PKI」の章を参照してください。

証明書は公開キーを安全に交換するために各ピアで使用されます（RSA シグニチャでは、各ピアが、リモート ピアの公開シグニチャ キーを持っている必要があります）。双方のピアが有効な証明書を持っている場合、RSA シグニチャを使用する IKE ネゴシエーションの一環として、ピアの間で公開キーが自動的に交換されます。

公開キーは手動で交換することもできます。これについては、「RSA 暗号化ナンスの RSA キーの手動設定」の項を参照してください。

RSA シグニチャにより、IKE ネゴシエーションで否認防止が可能になります。さらに、リモート ピアとの IKE ネゴシエーションを実際に実行することで、第三者に対する証明が可能になります。

RSA 暗号化ナンス

RSA 暗号化ナンスを使用するには、各ピアが他のピアの公開キーを持つようにする必要があります。

RSA シグニチャとは異なり、RSA 暗号化ナンス方式では、証明書を使って公開キーを交換できません。その代わりに各ピアが他のピアの公開キーを持つようにする必要があります。それには次の方法のいずれかを実行します。

- 「RSA 暗号化ナンスの RSA キーの手動設定」の項の説明に従って、手動で RSA キーを設定する。

- 証明書を使用する RSA シグニチャを使って IKE 交換がピア間で実行されていることを確認する（証明書を使用すると、RSA シグニチャ ベースの IKE ネゴシエーション中にピアの公開キーが交換される）。IKE 交換が実行されるようにするには、RSA 暗号化ナンスによる高プライオリティのポリシーと、RSA シグニチャによる低プライオリティのポリシーの 2 つのポリシーを指定します。RSA シグニチャは IKE ネゴシエーションが実行されるときに初めて使用されます。これは、各ピアが他のピアの公開キーをまだ持っていないためです。公開キーが交換されることで、以後の IKE ネゴシエーションで RSA 暗号化ナンスを使用できるようになります。

（注） この方法では、CA サポートをあらかじめ設定しておく必要があります。

RSA 暗号化ナンスでは IKE ネゴシエーションを否認できます。ただし、RSA シグニチャとは異なり、リモート ピアと IKE ネゴシエーションを実行したことを第三者に対して証明はできません。

事前共有キー

事前共有キーを使用するには、「事前共有キーの設定」の項の説明に従ってキーを設定する必要があります。

セキュアに設定された規模の大きいネットワークでは事前共有キーは扱いづらく、拡大するネットワークではキーをうまく拡張できません。ただし、RSA シグニチャのように CA を使用する必要がないため、10 ノード未満の規模の小さいネットワークではセットアップが簡単です。また、事前共有キーによる認証に比べ、RSA シグニチャによる認証の方がセキュアです。

（注） RSA 暗号化を設定し、シグニチャ モードがネゴシエーションされ、シグニチャ モードに証明書が使用されると、ピアはシグニチャと暗号キーを要求します。基本的にルータは、コンフィギュレーションでサポートされているできる限り多くのキーを要求します。RSA 暗号化が設定されていない場合は、ルータはシグニチャ キーだけを要求します。

前提条件

認証方式を指定した（またはデフォルトの RSA シグニチャを設定した）IKE ポリシーを最低 1 つは設定しておく必要があります。

RSA 暗号化ナンスの RSA キーの手動設定

RSA キーを手動で設定するには、IKE ポリシーで RSA 暗号化ナンスを使用する IPsec ピアそれぞれについて、この作業を実行します。

（注） この作業を実行するのは、CA を使用していない場合だけです。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** {**general-keys** | **usage-keys**} [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*]
4. **crypto key generate ec keysize** [**256** | **384**] [**label** *label-string*]
5. **exit**

6. **show crypto key mypubkey rsa**
7. **configure terminal**
8. **crypto key pubkey-chain rsa**
9. **named-key** *key-name* [**encryption** | **signature**]

   または

   addressed-key *key-address* [**encryption** | **signature**]
10. **address** *ip-address*
11. **key-string** *key-string*
12. **quit**
13. IKE ポリシーで RSA 暗号化ナンスを使用するピアそれぞれについて上記の手順を繰り返します。
14. **exit**
15. **exit**
16. **show crypto key pubkey-chain rsa** [**name** *key-name* | **address** *key-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	`crypto key generate rsa {general-keys | usage-keys} [label key-label] [exportable] [modulus modulus-size]` **例：** `Router(config)# crypto key generate rsa general-keys modulus 360`	RSA キーを生成します。 • *key-label* 引数を指定していない場合、ルータの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）であるデフォルト値が使用されます。
ステップ 4	**crypto key generate ec keysize** [**256** | **384**] [**label** *label-string*] **例：** `Router(config)# crypto key generate ec keysize 256 label Router_1_Key`	EC キーを生成します。 • 256 キーワードは、キーのサイズを 256 ビットに指定します。 • 384 キーワードは、キーのサイズを 384 ビットに指定します。 • **label** キーワードと *label-string* 引数を使用して、EC キーにラベルを指定できます。 **（注）** ラベルを指定しない場合は、FQDN の値が使用されます。

	コマンドまたはアクション	目的
ステップ 5	**exit** **例：** `Router(config)# exit`	（任意）グローバル コンフィギュレーション モードを終了します。
ステップ 6	`show crypto key mypubkey rsa` **例：** `Router# show crypto key mypubkey rsa`	（任意）生成された RSA 公開キーを表示します。
ステップ 7	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**crypto key pubkey-chain rsa** **例：** `Router(config)# crypto key pubkey-chain rsa`	公開キー コンフィギュレーション モード（他のデバイスの RSA 公開キーの手動設定が可能）にします。
ステップ 9	**named-key** *key-name* [**encryption** | **signature**] または **addressed-key** *key-address* [encryption | signature] **例：** `Router(config-pubkey-chain)# named-key otherpeer.example.com` または `Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption`	どのリモート ピアの RSA 公開キーを指定するのかを示し、公開キー コンフィギュレーション モードを開始します。 • リモート ピアが ISAKMP ID にホスト名を使用している場合は、**named-key** コマンドを使用し、リモート ピアの FQDN（somerouter.example.com など）を *key-name* に指定します。 • リモート ピアが ISAKMP ID に IP アドレスを使用している場合は、**addressed-key** コマンドを使用し、リモート ピアの IP アドレスを *key-address* に指定します。
ステップ 10	**address** *ip-address* **例：** `Router(config-pubkey-key)# address 10.5.5.1`	リモート ピアの IP アドレスを指定します。 • **named-key** コマンドを使うのは、このコマンドを使ってピアの IP アドレスを指定する必要がある場合です。

	コマンドまたはアクション	目的
ステップ 11	**key-string** *key-string* **例：** `Router(config-pubkey-key)# key-string` `Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973` `Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5` `Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8` `Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB` `Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B` `Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21`	リモート ピアの RSA 公開キーを指定します。 • （このキーは、リモート ルータの RSA キーが生成されたときに、リモート ピアの管理者が確認したキーです）
ステップ 12	**quit** **例：** `Router(config-pubkey-key)# quit`	公開キー チェーン コンフィギュレーション モードに戻ります。
ステップ 13	—	IKE ポリシーで RSA 暗号化ナンスを使用するピアそれぞれについて上記の手順を繰り返します。
ステップ 14	**exit** **例：** `Router(config-pubkey-key)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**show crypto key pubkey-chain rsa** [**name** *key-name* | **address** *key-address*] **例：** `Router# show crypto key pubkey-chain rsa`	（任意）ルータに保存されているすべての RSA 公開キーのリスト、またはルータに保存されている特定の RSA キーの詳細を表示します。

事前共有キーの設定

事前共有キーを設定するには、IKE ポリシーで事前共有キーを使用するピアそれぞれについて以下の手順を実行します。

事前共有キーの ISAKMP ID の設定

IKE ポリシーで事前共有キーを使用するピアそれぞれについて ISAKMP ID を設定する必要があります。

2 つのピアが IKE を使って IPsec SA を確立する場合、各ピアが自分の ID をもう一方のピア（リモート ピア）に送信します。各ピアは、ルータの ISAKMP ID の設定に従い、ホスト名または IP アドレスを送信します。

デフォルトでは、ピアの ISAKMP ID はピアの IP アドレスになっています。必要に応じて ID をピアのホスト名に変更します。一般的に、すべてのピアの ID は同じ設定にします（すべてのピアで IP アドレスを設定するか、すべてのピアでホスト名を設定）。お互いの識別にホスト名を使うピアと IP アドレスを使うピアが混在していると、リモート ピアの ID が識別されない場合に Domain Name System（DNS; ドメイン ネーム システム）lookup で ID を解決できなくなり、IKE ネゴシエーションが失敗することがあります。

マスク事前共有キー

マスク事前共有キーを使用すると、認証レベルが同じリモート ユーザのグループで、IKE 事前共有キーを共有できます。IKE 認証を実行するには、リモート ピアの事前共有キーと、ローカル ピアの事前共有キーが一致している必要があります。

マスク事前共有キーは通常、アウトオブバンドのセキュアなチャネルを使って配信されます。リモート ピアとローカル ピアが通信する場合、IKE 事前共有キーが設定されているリモート ピアとローカル ピアとの間で、IKE SA を確立できます。

mask キーワードの指定を **crypto isakmp key** コマンドで行う場合、サブネット アドレスを使用するかどうかをユーザが決めます。サブネット アドレスを使うと、より多くのピアとの間で同じキーを共有できます。つまり、事前共有キーが 2 人のユーザ間の使用に制限されないということです。

（注） サブネット アドレスとして 0.0.0.0 の使用は推奨しません。この設定ではグループで事前共有キーを保持できるため（すべてのピアが同じグループ キーを持つことが可能）、ユーザ認証のセキュリティが低下するからです。

特定の IPsec ピアの Xauth の無効化

スタティックな IPsec ピアの拡張認証（Xauth）を無効にすると、ルータで Xauth 情報（ユーザ名とパスワード）が表示されなくなります。

Xauth を無効にできない場合、ユーザは、同じクリプト マップのどのピアに Xauth を使用させるかを選択できません。つまり、ルータ間 IPsec がクライアント対 Cisco IOS IPsec と同じクリプト マップにある場合、どちらのピアでもユーザ名とパスワードを入力するプロンプトが表示されます。また、リモート スタティック ピア（Cisco IOS ルータ）は、ローカル Cisco IOS ルータと IKE SA を確立できません（Xauth は任意のエクスチェンジではないため、ピアが Xauth 要求に応答しない場合、IKE SA は削除されます）。したがって、この機能を実装しない限り、（Xauth に応答できない）他の Cisco IOS ルータだけでなく（Xauth が必要な）VPN クライアントへの IPsec を終了するのに同じインターフェイスは使用できません。

（注） Xauth は、事前共有キーが指定の暗号マップの認証メカニズムとして使用されている場合だけ、ディセーブルにできます。

制約事項

- 事前共有は、規模が拡大しているネットワークではうまく拡張できない。
- マスク事前共有キーの制約事項
  - 同じ事前共有キーのすべての IPsec ピアを設定するまで、IPsec ピア間に SA を確立できない。
  - マスク事前共有キーは、さまざまなレベルの認証を要求しているリモート ユーザごとに、明確に異なっている必要がある。認証のレベルごとに新しい事前共有キーを設定し、適切なキーを適切なユーザに割り当てる必要があります。正しく設定しないと、認証を受けていない人物が、保護されているデータに対するアクセス権を取得するおそれがあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp identity** {**address** | **dn** | **hostname**}
4. **ip host** *hostname address1* [*address2...address8*]
5. **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**]

   または

   crypto isakmp key *keystring* **hostname** *hostname* [**no-xauth**]
6. **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**]

   または

   crypto isakmp key *keystring* **hostname** *hostname* [**no-xauth**]
7. 事前共有キーを使用するピアそれぞれについて上記の手順を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp identity** {**address** | **dn** | **hostname**} **例：** `Router(config)# crypto isakmp identity address`	ローカル ピアの IP アドレスまたは Distinguished Name（DN; 認定者名）ホスト名を使ってピアの ISAKMP ID を指定します。 • **address**：ピアが IKE ネゴシエーションに使用するインターフェイスが 1 つだけ（したがって IP アドレスが 1 つだけ）で、IP アドレスがわかっている場合に通常使用します。 • **dn**：IKE 処理中、ISAKMP ID としてルータ証明書の DN が指定および選択される場合に通常使用します。dn キーワードは、証明書ベースの認証にだけ使用します。 • **hostname**：IKE ネゴシエーションに使用するインターフェイスがピアに複数ある場合か、インターフェイスの IP アドレスが不明の場合（IP アドレスのダイナミック割り当ての使用など）に使用します。
ステップ 4	`ip host` *`hostname address1`* `[`*`address2...address8`*`]` **例：** `Router(config)# ip host RemoteRouter.example.com 192.168.0.1`	ホスト名を使ってローカル ピアの ISAKMP ID を指定した場合、すべてのリモート ピアについて、ピアのホスト名を IP アドレスにマップします （ホスト名または IP アドレスが DNS サーバでマップ済みの場合はこの手順は不要）。

	コマンドまたはアクション	目的
ステップ 5	**crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**] または **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**] **例：** `Router(config)# crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth` または `Router(config) crypto isakmp key sharedkeystring hostname RemoteRouter.example.com`	特定のリモート ピアで使用する共有キーをローカル ピアで指定します。 • リモート ピアで ISAKMP ID を IP アドレスで指定した場合は、この手順で **address** キーワードを使用し、それ以外の場合は、この手順で **hostname** キーワードを使用します。 – **no-xauth**：ルータがピアに Xauth 情報のプロンプトを出力しないようにします。このキーワードを使用するのは、ルータ間 IPsec が VPN クライアント対 Cisco IOS IPsec と同じクリプト マップにある場合です。 **（注）** 事前共有キーは、IKE メイン モードでの事前共有キー認証の設計に従い、ピアの IP アドレスを基にしている必要があります。事前共有キー認証の ID としてホスト名を送信できますが、キーはピアの IP アドレスを基に検索されます。（IP アドレスに基づいて）キーが検索されなかった場合、ネゴシエーションが失敗します。
ステップ 6	**crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**] または **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**] **例：** `Router(config) crypto isakmp key sharedkeystring address 10.0.0.1` または `Router(config) crypto isakmp key sharedkeystring hostname LocalRouter.example.com`	ローカル ピアで使用する共有キーをリモート ピアで指定します。 • これは、ローカル ピアで指定したキーと同じキーです。 • ローカル ピアで ISAKMP ID を IP アドレスで指定した場合は、この手順で **address** キーワードを使用し、ホスト名で指定した場合はこの手順で **hostname** キーワードを使用します。
ステップ 7	IKE ポリシーで事前共有キーを使用するピアそれぞれについて上記の手順を繰り返します。	—

IKE モード コンフィギュレーションの設定

IKE モード コンフィギュレーションについて

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって定義されているように、IKE モード コンフィギュレーションにより、ゲートウェイで IP アドレス（およびその他のネットワーク レベルの設定）を、IKE ネゴシエーション中にクライアントにダウンロードできます。この交換を使うことで、IP アドレスはゲートウェイによって IKE クライアントに渡され、IPsec でカプセル化された「内部」IP アドレスとして使用されます。この方式では、IPsec ポリシーと一致する可能性のある、クライアントの既知の IP アドレスが渡されます。

ダイナミック IP アドレスと会社のゲートウェイが設定されたリモート アクセス クライアント間に IPsec VPN を実装するには、各クライアントが認証された後、拡張可能な IPsec ポリシーをゲートウェイでダイナミックに管理する必要があります。IKE モード コンフィギュレーションにより、各クライアントの IP アドレスに関係なく、非常に規模の大きいクライアント群に対して拡張可能なポリシーをゲートウェイでセットアップできます。

IKE モード コンフィギュレーションには次の 2 つのタイプがあります。

- ゲートウェイ始動：ゲートウェイがクライアントでコンフィギュレーション モードを開始する。クライアントが応答すると、IKE が送信者の ID を変更し、メッセージが処理され、クライアントが応答を受信します。
- クライアント始動：クライアントがゲートウェイでコンフィギュレーション モードを開始する。クライアントに割り当てた IP アドレスでゲートウェイが応答します。

制約事項

IKE モード コンフィギュレーションには次の制約事項があります。

- IKE モード コンフィギュレーションに設定されているクリプト マップを持つインターフェイスでは、接続のセットアップ時間がやや長くなることがあります。これは、設定を拒否する IKE ピア、またはコンフィギュレーション モードの要求に応答しない IKE ピアの場合であっても同様です。どちらの場合も、ゲートウェイがクライアントの設定を初期化します。
- この機能は、すべての IKE 接続のコンフィギュレーション モードをデフォルトで有効にするようには設計されていません。グローバル クリプト マップ レベルでこの機能を設定してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip local pool** *pool-name start-addr end-addr*
4. **crypto isakmp client configuration address-pool local** *pool-name*
5. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip local pool** *pool-name start-addr end-addr* **例：** `Router(config) ip local pool pool1 172.16.23.0 172.16.23.255`	アドレス一式が定義されている既存のローカル アドレス プールを定義します。

	コマンドまたはアクション	目的
ステップ 4	**crypto isakmp client configuration address-pool local** *pool-name* **例：** `Router(config) crypto isakmp client configuration address-pool local pool1`	IKE コンフィギュレーションのローカル アドレス プールを参照します。
ステップ 5	**crypto map** *tag* **client configuration address** [**initiate** | **respond**] **例：** `Router(config)# crypto map dyn client configuration address initiate`	グローバル コンフィギュレーション モードで IKE モード コンフィギュレーションを設定します。

IPsec SA ネゴシエーションのための IKE クリプト マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *tag sequence* **ipsec-isakmp**
4. **set pfs** {**group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group19** | **group20**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto map** *tag sequence* **ipsec-isakmp** **例：** `Router(config)# crypto map example 1 ipsec-ipsec-isakmp`	クリプト マップを指定し、クリプト マップ コンフィギュレーション モードを開始します。 • *tag* 引数には、クリプト マップを指定します。 • *sequence* 引数には、クリプト マップ エントリに挿入するシーケンスを指定します。 • **ipsec-isakmp** キーワードには、IKEv1 を使用する IPsec（ISAKMP）を指定します。
ステップ 4	**set pfs** {**group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group19** | **group20**} **例：** `Router(config-isakmp)# set pfs 19`	IPSec SA ネゴシエーションの Diffie-Hellman（DH）グループ ID を指定します。 • デフォルトでは DH グループ 1 が使用されます。 – **group1**：768 ビット DH – **group2**：1024 ビット DH – **group5**：1536 ビット DH – **group14**：2048 ビット DH グループを指定します。 – **group15**：3072 ビット DH グループを指定します。 – **group16**：4096 ビット DH グループを指定します。 – **group19**：256 ビット Elliptic Curve DH（ECDH）グループを指定します。 – **group20**：384 ビット ECDH グループを指定します。 **（注）** 1024 ビットおよび 1536 ビットの DH オプションを使用すると、「解読」がより困難になる一方、実行に必要な CPU 時間が増えます。 **（注）** **group 5** は 128 ビット キーに使用できますが、group 14 がより適しています。 **（注）** 選択するグループは、ネゴシエーション中の IPsec キーを保護するため、十分強力（十分なビット数がある）である必要があります。特定のサイズのキーを保護するために Diffie-Hellman グループに必要なビット数についての見解には相違がありますが、一般的に、**group 14** は 128 ビット キー、**group 15** は 192 ビット キー、および **group 16** は 256 ビット キーの保護に適しているとの合意があります。

IKE コンフィギュレーションの設定例

ここでは、次の設定例を示します。

- 「IKE ポリシーの作成：例」（P.21）
- 「IKE 認証の設定：例」（P.22）

IKE ポリシーの作成：例

ここでは次の例を使って、3DES IKE ポリシーおよび AES IKE ポリシーの設定方法について説明します。

3DES IKE ポリシーの作成：例

この例では、2 つの IKE ポリシー（最大のプライオリティとして policy 15、次のプライオリティとして policy 20）を作成し、最小のプライオリティとして既存のデフォルト プライオリティを使用します。また、IP アドレスが 192.168.224.33 のリモート ピアに、policy 20 で使用する事前共有キーも作成します。

```
crypto isakmp policy 15
 encryption 3des
 hash md5
 authentication rsa-sig
 group 2
 lifetime 5000
!
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
!
crypto isakmp key 1234567890 address 192.168.224.33
```

この例では、暗号化アルゴリズム パラメータのデフォルト値のため、policy 15 の暗号化 DES は記述した設定に表示されません。

この設定で **show crypto isakmp policy** コマンドを発行すると、出力は次のようになります。

```
Protection suite priority 15
encryption algorithm:3DES - Triple Data Encryption Standard (168 bit keys)
hash algorithm:Message Digest 5
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#2 (1024 bit)
lifetime:5000 seconds, no volume limit
Protection suite priority 20
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:preshared Key
Diffie-Hellman group:#1 (768 bit)
lifetime:10000 seconds, no volume limit
Default protection suite
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#1 (768 bit)
lifetime:86400 seconds, no volume limit
```

ライフタイムに「no volume limit」と出力されていますが、time ライフタイム（86,400 秒など）だけは設定できます。volume limit ライフタイムは設定できません。

AES IKE ポリシーの作成：例

次に、**show running-config** コマンドからの出力例を示します。この例では、AES 256 ビット キーが有効になっています。

```
Current configuration : 1665 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "Router1"
!
!
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
 mode transport
!
crypto map aesmap 10 ipsec-isakmp
 set peer 10.0.110.1
 set transform-set aesset
 match address 120
!
.
.
.
```

IKE 認証の設定：例

次の例は、2 つの IPsec ピアの RSA 公開キーを手動で指定する方法を示しています。10.5.5.1 のピアは汎用キーを使用し、もう一方のピアは特殊な用途のキーを使用しています。

```
crypto key pubkey-chain rsa
 named-key otherpeer.example.com
 address 10.5.5.1
 key-string
 005C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C5E23B 55D6AB22
 04AEF1BA A54028A6 9ACC01C5 129D99E4
 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
 BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
 D58AD221 B583D7A4 71020301 0001
 quit
 exit
 addressed-key 10.1.1.2 encryption
 key-string
 00302017 4A7D385B 1234EF29 335FC973
 2DD50A37 C4F4B0FD 9DADE748 429618D5
 18242BA3 2EDFBDD3 4296142A DDF7D3D8
 08407685 2F2190A0 0B43F1BD 9A8A26DB
 07953829 791FCDE9 A98420F0 6A82045B
 90288A26 DBC64468 7789F76E EE21
```

```
quit
exit
addressed-key 10.1.1.2 signature
key-string
0738BC7A 2BC3E9F0 679B00FE 53987BCC
01030201 42DD06AF E228D24C 458AD228
58BB5DDD F4836401 2A2D7163 219F882E
64CE69D4 B583748A 241BED0F 6E7F2F16
0DE0986E DF02031F 4B0B0912 F68200C4
C625C389 0BFF3321 A2598935 C1B1
quit
exit
exit
```

関連情報

IKE ネゴシエーションを正常に設定したら、IPsec の設定を開始します。この作業実行の詳細については、「IPsec を使用した VPN のセキュリティの設定」の章を参照してください。

その他の参考資料

関連資料

内容	参照先
IPsec の設定	「*Configuring Security for VPNs with IPsec*」
IKE バージョン 2	「Configuring Internet Key Exchange Version 2 (IKEv2)」
CA から証明書を取得するように RSA キーを設定	「*Deploying RSA Keys Within a PKI*」
IKE、IPsec および PKI コンフィギュレーション コマンド：完全なコマンド構文、コマンド モード、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS Security Command Reference*』
Suite-B の ESP トランスフォーム	『Configuring Security for VPNs with IPsec』フィーチャ モジュール
Suite-B 整合性アルゴリズム タイプのトランスフォームの設定	『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman（ECDH）のサポート	『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール
PKI の証明書登録のための Suite-B サポート	『Configuring Certificate Enrollment for a PKI』フィーチャ モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2408	『*Internet Security Association and Key Management Protocol (ISAKMP)*』
RFC 2409	『*The Internet Key Exchange (IKE)*』
RFC 2412	『*The OAKLEY Key Determination Protocol*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

IPsec VPN の IKE 設定に関する機能情報

表 1 に、この機能のリリース履歴を示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IPsec VPN の IKE 設定に関する機能情報

機能名	リリース	機能情報
スタティック IPsec ピアの拡張認証を無効にする機能	12.2(4)T	この機能により、ルータ間 IPsec の事前共有キー設定中に Xauth を無効にできます。したがって、ルータによりピアのユーザ名およびパスワードは要求されません。これらは、VPN クライアント対 Cisco IOS IPsec の Xauth が発生するときに転送されます。 この機能に関する詳細については、次の項を参照してください。 • 「事前共有キーの設定」（P.14） この機能により、**crypto isakmp key** コマンドが変更されました。
Advanced Encryption Standard（AES; 高度暗号化規格）	12.2(8)T	この機能により、新しい暗号化規格 AES に対するサポートが追加されます。AES は、DES の後継として開発された IPsec および IKE のプライバシー トランスフォームです。 この機能に関する詳細については、次の各項を参照してください。 • 「IKE での使用にサポートされている標準」（P.2） • 「IKE ポリシーの作成：IKE ネゴシエーションのセキュリティ パラメータ」（P.5） この機能により、**crypto ipsec transform-set**、**encryption**（IKE ポリシー）、**show crypto ipsec transform-set**、**show crypto isakmp policy** の各コマンドが変更されました。

表 1　IPsec VPN の IKE 設定に関する機能情報 （続き）

機能名	リリース	機能情報
SEAL 暗号化	12.3(7)T	この機能により、IPsec での SEAL 暗号化に対するサポートが追加されました。 この機能に関する詳細については、次の項を参照してください。 • 「IKE での使用にサポートされている標準」（P.2） この機能により、**crypto ipsec transform-set** コマンドが変更されました。
IOS SW の暗号化での Suite-B のサポート	15.1(2)T	Cisco IOS で、パケット データの認証および IKE プロトコルの整合性確認メカニズムの検証に使用される SHA-2 ファミリ（HMAC バリアント）のハッシュ アルゴリズムに、Suite-B のサポートが追加されました。HMAC は別のレベルのハッシュのバリアントです。この機能により、IPsec SA ネゴシエーションに Elliptic Curve Diffie-Hellman（ECDH）のサポートも追加されました。 Cisco IOS での Suite-B サポートに関する詳細については、『Configuring Security for VPNs with IPsec』フィーチャ モジュールを参照してください。 この機能に関する詳細については、次の各項を参照してください。 • 「IKE での使用にサポートされている標準」（P.2） • 「一致した IKE ポリシーに同意する IKE ピア」（P.6） • 「IPsec SA ネゴシエーションのための IKE クリプト マップの設定」（P.19） この機能により次のコマンドが変更されました。**authentication**、**crypto key generate ec keysize**、**crypto map**、**group**、**hash**、**set pfs**