「Configuring Internet Key Exchange for IPsec VPNs」

この章では、基本的な IP Security（IPsec）バーチャル プライベート ネットワーク（VPN）用のインターネット キー エクスチェンジ（IKE）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（ISAKMP）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）。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IKE 設定の前提条件

- 「Configuring Security for VPNs with IPsec」モジュールで説明している概念およびタスクを理解している必要があります。
- ご使用のアクセス コントロール リスト（ACL）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）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

- プロファイルがロックされたり、DMI 劣化状態が発生したりしないようにするには、**config-replace** コマンドを使用して設定を置き換える前に、必ず、トンネルインターフェイスをシャットダウンして、すべての暗号セッションとトンネル設定を停止させてください。
- 開始ルータでは、リモートピアに関連付けられた証明書が必要ありません。
- 事前共有キーは、両方のピアで完全修飾ドメイン名（FQDN）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 アドレスでは必要ありません）。このため、**crypto isakmp identity hostname** コマンドを使用する必要があります。
- **show crypto eli** コマンドを使用して、デバイスのソフトウェア暗号化制限事項を決定します。ハードウェア モジュールがない場合の制限事項は次のとおりです。
  - IPSec セキュリティ アソシエーション（SA）数：1000
  - IKE SA 数：100
  - Diffie-Hellman（DH）セッション キー数：50
- サイト間 VPN での TCP フローのパフォーマンスを向上させるには、**no crypto batch allowed** コマンドを使用して暗号バッチ機能を無効にします。ただし、暗号バッチ機能を無効にすると、CPU 使用率が影響を受ける可能性があります。
- Cisco IOS リリース 15.0(1)SY 以降では、Cisco Catalyst 6500 シリーズ スイッチで **crypto ipsec** コマンドを使用して IPsec ネットワークセキュリティ機能を設定できません。これらのスイッチで IPsec をサポートするには、ハードウェア暗号化エンジンを使用する必要があります。

IPsec VPN の IKE 設定に関する情報

IKE での使用でサポート対象となる標準

シスコでは次の標準を採用しています。

- 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：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実装の方法、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。

（注） シスコは現在、DES、3DES、MD5（HMAC バリアント含む）、および Diffie-Hellman（DH）グループ 1、2、および 5 の使用は推奨していません。代わりに、AES、SHA-256、および DH グループ 14 以降を使用する必要があります。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

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）。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、データ暗号規格（DES）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：データ暗号規格（DES）。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、暗号化の開始に初期ベクター（IV）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、Triple DES（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層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 データ暗号化フィーチャ 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 までお問い合わせください。

- SEAL：ソフトウェア暗号化アルゴリズム（SEAL）。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。
- SHA-2 および SHA-1 ファミリ（HMAC バリアント）：セキュア ハッシュ アルゴリズム（SHA）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、追加レベルのハッシュを提供するバリアントです。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 サポートについての詳細は、「Configuring Security for VPNs with IPsec」機能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）。
- Diffie-Hellman：公開キー暗号法プロトコルの 1 つで、2 者間に、安全でない通信チャネルでの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。これは、768 ビット（デフォルト）、1024 ビット、1536 ビット、2048 ビット、3072 ビット、および 4096 ビット DH グループをサポートします。また、256 ビット サブグループを含む 2048 ビット DH グループと、256 ビットと 384 ビットの Elliptic Curve DH（ECDH）もサポートします。Cisco では、2048 ビット以上の DH キー交換または ECDH キー交換を使用することを推奨します。
- MD5：Message Digest 5（ハッシュ ベースのメッセージ認証コード（HMAC））バリアント）。パケット データの認証に使用するハッシュ アルゴリズム。HMAC は、追加レベルのハッシュを提供するバリアントです。

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プロトコルに沿って使用されます。この証明書サポートを使用すると、各デバイスに同等のデジタル 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 セキュリティ アソシエーション（SA）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。

- 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。
- 認証局（CA）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です。

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）のネゴシエーションをします。フェーズ 1 でキーのネゴシエーションをすることで、フェーズ 2 で IKE ピアが安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE が IPsec など他の適用でのキー（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 つのモードの設定はできません。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、認証の起動に対応する情報がなく、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、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。

IKE ネゴシエーション用 IKE ポリシー 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わせを定義します。IKEエクスチェンジに参加する各ピアでIKEポリシーを作成する必要があります。

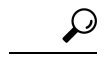
IKE ポリシーを 1 つも設定しない場合、ルータはデフォルトのポリシーを使用します。デフォルトのポリシーは、常にプライオリティが最低に設定されており、各パラメータはデフォルト値に設定されています。

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わ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、もう一方のデバイスでサポートされている値を設定する必要があります。この制限を別にすれば、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。

一致する IKE ポリシーでの IKE ピアの合意

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 ピアは優先順位が高い順に各ポリシーをチェックします。

一致が成立するのは、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。

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。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。詳細については、IKE認証の設定 （11 ページ）を参照してください。

ピアのポリシーに必要な関連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。

IKE 認証

IKE 認証は次のオプションで構成され、各認証方式には追加の設定が必要です。

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、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拡張性が大幅に改善されます。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 サポートを正しく設定するには、モジュール「PKI 内での RSA キーの展開」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 シグネチャでは、各ピアに、リモートピアの公開シグネチャキーが必要です。双方のピアに有効な証明書がある場合、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 （11 ページ） 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 キーを手動で設定する（「RSA 暗号化ナンスの RSA キーの手動設定 （11 ページ）」を参照）。
- 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ます）。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、各ピアに他のピアの公開キーがまだないためです。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。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

事前共有キーの概要

事前共有キーは、大規模なセキュア ネットワークでは、成長するネットワークにうまく対応できないため、適していません。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安全です。

（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。

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（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）にします。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ドメイン ネーム システム（DNS）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安全なチャネル経由で配信されます。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はユーザーが決定します。使用すると、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

静的 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。

IKE モード設定

Internet Engineering Task Force（IETF）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では、ゲートウェイにより、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ネゴシエーションの一環で、クライアントにダウンロードできます。このエクスチェンジを使用することで、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。

IPsec VPN 用 IKE の設定方法

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。

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。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

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。

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。これらの追加作業の完了に関する詳細については、IKE 認証の設定 （11 ページ） 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、モジュール「Configuring Security for VPNs with IPsec」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。

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

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。

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

（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。

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。

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. 次のいずれかを実行します。
   - **named-key** *key-name* [**encryption** | **signature**]
   - **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 モードを有効にします。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、ルータの完全修飾ドメイン名（FQDN）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	次のいずれかを実行します。
	• **named-key** *key-name* [**encryption** | **signature**]
	• **addressed-key** *key-address* [**encryption** | **signature**]
	例：
	`Router(config-pubkey-chain)# named-key otherpeer.example.com`
	例：
	`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** コマンドを使用するのは、このコマンドを使用してピアの IP アドレスを指定する必要がある場合です。

ステップ 11	**key-string** key-string
	例：
	`Router(config-pubkey-key)# key-string`
	例：
	`Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973`
	例：
		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）

	コマンドまたはアクション	目的

	`Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5`
	例：
	`Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8`
	例：
	`Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB`
	例：
	`Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B`
	例：
	`Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21`	

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。

（注） 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には次の制約事項があります。

- 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可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場合があります。

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. 次のいずれかを実行します。
   - **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**]
   - **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**]
6. 次のいずれかを実行します。
   - **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**]
   - **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**]
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以上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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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 アドレスまたは認定者名（DN）ホスト名を使ってピアの ISAKMP ID を指定します。 • **address**：通常は、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使用します。

	コマンドまたはアクション	目的
		• **dn**：通常は、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、（IP アドレスのダイナミック割り当てなどで）インターフェイスの IP アドレスが不明の場合に使用する必要があります。
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）。

ステップ 5	次のいずれかを実行します。
	• **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**]
	• **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**]
	例：
	`Router(config)# crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth`
	例：
	`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。
		（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	次のいずれかを実行します。 • **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**] • **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**] 例：	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

	コマンドまたはアクション	目的

	`Router(config) crypto isakmp key sharedkeystring address 10.0.0.1`
	例：
	`Router(config) crypto isakmp key sharedkeystring hostname LocalRouter.example.com`
		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。

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以上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

（注） 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。

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*

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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。
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。

IPsec SA ネゴシエーションのための IKE 暗号マップの設定

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

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**}

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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 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、暗号マップを指定します。 • *sequence* 引数には、暗号マップ 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**} 例： `Router(config-isakmp)# set pfs 14`	IPSec SA ネゴシエーションの 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（非推奨） • **group2**：1024 ビット DH（非推奨） • **group5**：1536 ビット DH（非推奨）

	コマンドまたはアクション	目的
		• **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。 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。一般に受け入れられているガイドラインでは、2013 年以降（2030 年まで）は 2048 ビット グループの使用が推奨されています。このガイドラインを満たすには、いずれかの group14 を選択してください。より長期にわたるセキュリティ方式が必要であっても、楕円曲線暗号の使用が推奨されますが、group15 と group16 も検討できます。

IKE コンフィギュレーションの設定例

例：IKE ポリシーの作成

このセクションには、AES IKE ポリシーおよび 3DES IKE ポリシーの設定方法を示す次の例が含まれています。

（注） シスコでは、3DES の使用は推奨していません。代わりに、AES を使用してください。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

例：3DES IKE ポリシーの作成

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 DES のポリシーのデフォルト値は、暗号化アルゴリズム パラメータのデフォルト値のため、記述した設定には表示されません。

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。

例：AES IKE ポリシーの作成

次に、**show running-config** コマンド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

.
.
.
```

例：IKE 認証の設定

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
```

次の作業

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。このタスクの実行についての詳細は、モジュール「Configuring Security for VPNs with IPsec」を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IPsec の設定	『Configuring Security for VPNs with IPsec』
IKE バージョン 2	「Configuring Internet Key Exchange Version 2 and FlexVPN」
CA から証明書を取得するように RSA キーを設定	PKI 内での RSA キーの展開
Suite-B の ESP トランスフォーム	『Configuring Security for VPNs with IPsec』
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 and FlexVPN」
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 and FlexVPN」
PKI の証明書登録のための Suite-B サポート	「Configuring Certificate Enrollment for a PKI」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
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、およびフィーチャセットの 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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

IPsec VPN の IKE 設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IPsec VPN の IKE* 設定の機能情報

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。 この機能により、次のコマンドが変更されました。**crypto isakmp key.**
Advanced Encryption Standard（AES）	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。 この機能により、次のコマンドが変更されました。**crypto ipsec transform-set, encryption (IKE policy), show crypto ipsec transform-set, crypto ipsec transform-set, show crypto isakmp policy.**
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。 この機能により、次のコマンドが変更されました。**crypto ipsec transform-set.**
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、追加レベルのハッシュを提供するバリアントです。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 サポートについての詳細は、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。 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.**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。