CHAPTER 23

IPSec バーチャル プライベート ネットワーク共有ポート アダプタ（IPSec VPN SPA）の概要

この章では、IPSec Virtual Private Network Shared Port Adapter（IPSec VPN SPA; IP セキュリティ バーチャル プライベート ネットワーク共有ポート アダプタ）のリリース履歴と機能および Management Information Base（MIB; 管理情報ベース）サポートの概要を示します。

この章の内容は次のとおりです。

リリース履歴

リリース	変更点
Cisco IOS Release 12.2(33)SRB、SRC、SRD	IPSec VPN SPA に関して追加された新しい機能はありません。

Cisco IOS Release 12.2(33)SRA	前のリリースから次の点が変更されていますので注意してください。 • IPSec VPN SPA に関して、次の機能が追加されました。 – フロントサイド VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送） – IPSec Virtual Tunnel Interface（VTI） – Internet Security Association and Key Management Protocol（ISAKMP）プロファイル マッピングの認証 – コール アドミッション制御 – 定期メッセージ オプション（現在は Dead Peer Detction でサポート） – Reverse Route Injection（RRI; 逆ルート注入） – IPSec アンチリプレイ ウィンドウ サイズ – IPSec 優先ピア – ローカル証明書ストレージ場所 – 持続的自己署名証明書 – Easy VPN リモート Rivest, Shamir, and Adelman（RSA）シグニチャの保存 – Cisco VRF-Aware IPSec の IPSec および Internet Key Exchange（IKE; インターネット キー エクスチェンジ）MIB サポート • トンネル キャパシティが 16,000 トンネルに増加されました。 • 次のコマンドにサポートが追加されました。 – **clear crypto engine accelerator counter** コマンド：プラットフォームおよびネットワーク インターフェイスのコントローラの統計情報をクリアします。 – **show crypto engine accelerator counter** コマンド：プラットフォームおよびネットワーク インターフェイスのコントローラの統計情報を表示します。 – **show crypto eli** コマンド：アクティブな IKE Security Association（SA; セキュリティ アソシエーション）および IPSec セッション数および各 IPSec VPN SPA に使用されている Diffie-Hellman キー数を表示します。 • Cisco IOS Release 12.2(33)SRA は Supervisor Engine 32 および Supervisor Engine 720 に限りサポートされます。 • 以前のリリースとは異なり、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）および State Synchronization Protocol（SSP）を使用する IPSec ステートフル フェールオーバーのサポートは含まれません。 • **crypto engine subslot** コマンドは、**crypto engine slot** コマンドに置き換えられました。 • 1 つの長いコンフィギュレーションの章がいくつかの小さい章に再編成され、リリース依存機能を説明する表が追加されました。 • リリースごとのスーパーバイザおよびラインカードのサポートを差別化する表を含むように「相互運用性」（P.23-15）の項が拡張されました。

Cisco IOS Release 12.2(18)SXF6	SX リリース トレインの IPSec アンチリプレイ ウィンドウ サイズ機能のサポートが追加されました。
Cisco IOS Release 12.2(18)SXF2	Supervisor Engine 2、Supervisor Engine 32、および IP multicast over a GRE トンネルのコンフィギュレーションのサポートが追加されました。
Cisco IOS Release 12.2(18)SXE5	次の 2 つの Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）テイクオーバー コマンドにサポートが追加されました。 • **crypto engine gre supervisor** コマンド：ルータがスーパーバイザ エンジン ハードウェアまたは Route Processor（RP; ルート プロセッサ）を使用して総称ルーティング カプセル化（GRE）を処理するように設定します。 • **crypto engine gre vpnblade** コマンド：ルータが IPSec VPN SPA を使用して GRE を処理するように設定します。
Cisco IOS Release 12.2(18)SXE2	Cisco 7600 シリーズ ルータの Cisco 7600 SSC-400 に IPSec VPN SPA のサポートが追加されました。

IPSec VPN SPA の概要

IPSec VPN SPA は、Cisco 7600 シリーズ ルータに搭載し、IPSec 暗号化および復号化、総称ルーティング カプセル化（GRE）、および インターネット キー エクスチェンジ（IKE）鍵生成のためのハードウェア アクセラレーションを提供するギガビット イーサネット IP セキュリティ（IPSec）暗号化 SPA です。

（注） ソフトウェアベースの IP Sec 機能は、IPSec VPN SPA をサポートする Cisco IOS リリースではサポートされません。

Cisco IOS における IPSec の従来のソフトウェアベースの実装では、Authentication Header（AH; 認証ヘッダー）、Encapsulating Security Payload（ESP; カプセル化セキュリティ ペイロード）、および IKE を含めて、あらゆるセキュリティ プロトコルがサポートされています。これらのアクティビティは大量のリソースを消費するので、セキュアな Virtual Private Network（VPN; バーチャル プライベート ネットワーク）上でライン レートの伝送速度を達成するのは困難です。この問題を解決するため、広い VPN 帯域幅が必要な特定のプラットフォームでは、ハードウェアのフォワーディング エンジンと連携する Bump-in-the-Wire（BITW）IPSec ハードウェア カードを実装しています。これらのプラットフォームでは、ポリシー実施のほかにバルク暗号化および転送の動作がルート プロセッサ（RP）からオフロードされるので、ルータを通過する各パケットを処理する必要がありません。その結果、セッションの確立、キーの管理といった他の機能のためにリソースが解放されます。IPSec VPN SPA には、Cisco 7600 シリーズ ルータに対応する Virtual LAN（VLAN; 仮想 LAN）を使用した Bump-in-the-Wire（BITW）IPSec が実装されています。

（注） BITW は、IP スタックがパケットの処理を終了したあとで出力パケットの処理を開始し、IP スタックがパケットを受信する前に、入力パケットの処理を終了する IPSec 実装です。

IPSec VPN SPA は他の Cisco 7600 シリーズ ルータモジュールで複数のファスト イーサネット ポートまたはギガビット イーサネット ポートを使用して、WAN ルータを介してインターネットに接続できます。物理ポートは、ポート VLAN（または pvlan）という VLAN を介して IPSec VPN SPA に接続できます。WAN ルータから受信したパケットは、IPSec 処理のために IPSec VPN SPA を通過します。パケットは、インターフェイスまたは内部 VLAN（または ivlan）という専用 VLAN に出力されます。コンフィギュレーション モード（VRF モードまたは暗号接続モード）に応じて、ivlan または pvlan を明示的に設定したり、システムによって暗黙的に割り当てることができます。

LAN 側では、LAN ポート間のトラフィックは複数のファスト イーサネットまたはギガビット イーサネット ポートでルーティングまたはブリッジングできます。LAN トラフィックは暗号化または復号化の対象にならないので、IPSec VPN SPA を通過しません。

IPSec VPN SPA は、ルーティング情報の維持、ルーティング、またはパケットの Media Access Control（MAC; メディア アクセス制御）ヘッダーの変更は（1 つの VLAN から別の VLAN への VLAN ID は例外）実行しません。

IPSec および IKE 設定の基本概念の概要

ここでは、セキュリティ アソシエーション（SA）、Access List（ACL; アクセス リスト）、暗号マップ、トランスフォーム セット、IKE ポリシーなど、IPSec VPN SPA の設定全体で使用される基本的な IPSec および IKE の概念について説明します。ここに記載された情報は一部に過ぎず、すべてが網羅されているわけではありません。

（注） IPSec および IKE の概念や手順の詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。

IPSec の設定情報

IPSec は 2 つのピア（2 つのルータなど）を結ぶセキュアなトンネルを確立します。より正確に言えば、これらのトンネルは、2 つの IPSec ピア間に確立されたセキュリティ アソシエーション（SA）のセットです。SA は、重要なパケットに適用されるプロトコルおよびアルゴリズムを定義し、2 つのピアで使用されるキー関連情報を指定します。SA は単一方向であり、セキュリティ プロトコル（Authentication Header（AH; 認証ヘッダー）またはカプセル化セキュリティ ペイロード（ESP））ごとに確立されます。2 つのピア間に複数の IPSec トンネルを確立し、トンネルごとに個別の SA セットを使用して、各データ ストリームを保護できます。たとえば、あるデータ ストリームには認証だけを行い、別のデータ ストリームには暗号化と認証を行わなければならないことがあります。

（注） ここで「トンネル」という用語を使用していても、IPSec をトンネル モードで使用するという意味ではありません。

IPSec では、ACL を設定し、暗号マップを使用してこれらの ACL をインターフェイスに適用して、2 つの IPSec ピア間で保護する必要があるトラフィックを定義します （IPSec で使用される ACL は、IPSec で保護するトラフィックを判別する場合に限り使用します。インターフェイスの通過をブロックまたは許可するトラフィックを判別する場合には、使用しません。インターフェイスでのブロックや許可は、別の ACL で定義します）。

あるトラフィックに特定の組み合わせの IPSec 保護（認証だけなど）を適用し、その他のトラフィックに別の組み合わせの IPSec 保護（認証と暗号化など）を適用する場合は、2 つの異なる暗号 ACL を作成して、2 つの異なるタイプのトラフィックを定義するする必要があります。これらの ACL をそれぞれ異なる暗号マップ エントリで使用して、異なる IPSec ポリシーを指定します。

IPSec 暗号マップ エントリに対応付けられた暗号 ACL には、主に 4 つの機能があります。

- IPSec で保護される発信トラフィックを選択します（permit = protect）。
- IPSec セキュリティ アソシエーションのネゴシエーションを開始する場合に、新しい SA で保護されるデータ フローを指定します（単一の許可エントリで指定）。
- 着信トラフィックを処理して、IPSec で保護されていたトラフィックを除外し、ドロップします。

- IPSec ピアからの IKE ネゴシエーションを処理する場合に、要求されたデータ フローの代わりに IPSec セキュリティ アソシエーションの要求を受け入れるかどうかを判別します。ネゴシエーションが実行されるのは、ipsec-isakmp 暗号マップ エントリに対してだけです。要求を受け入れるには、ピアが IPSec ネゴシエーションを開始した場合に、ipsec-isakmp 暗号マップ エントリに対応付けられた暗号 ACL で「許可する」データ フローを指定する必要があります。

IPSec 用に作成される暗号マップ エントリは、IPSec SA の設定に使用される、次のような情報を集めたものです。

- IPSec で保護されるトラフィック（暗号 ACL 単位）
- SA セットで保護されるフローの粒度
- IPSec で保護されたトラフィックの送信先（リモート IPSec ピアの名前）
- IPSec トラフィックで使用されるローカル アドレス
- 現在のトラフィックに適用される IPsec SA（1 つまたは複数のトランスフォーム セットのリストから選択）
- SA を手動で確立するか、または IKE を使用して確立するか
- IPSec SA を定義するために必要なその他のパラメータ

暗号マップ エントリが順に検索されます。ルータは該当するエントリで指定されたアクセス リストとパケットを照合しようとします。

暗号マップ エントリには、トランスフォーム セットも含まれます。トランスフォーム セットは、IPSec で保護されたトラフィックに適用される、セキュリティ プロトコル、アルゴリズム、およびその他の設定の有効な組み合わせです。

複数のトランスフォーム セットを指定してから、暗号マップ エントリ内でこれらのトランスフォーム セットを 1 つまたは複数指定できます。IPSec セキュリティ アソシエーションと IKE のネゴシエーション中に、ピアは両方のピアに同じトランスフォーム セットがあるか検索します。両方のピアで同じトランスフォーム セットが検出された場合は、このトランスフォーム セットが選択されて、両方のピアの IPSec SA の一部として、保護対象トラフィックに適用されます（SA を手動で確立した場合は、ピアとのネゴシエーションが行われないため、両方のピアで同じトランスフォーム セットを指定する必要があります）。

（注） キーの再生成中のパケット損失の可能性を最小限に抑えるために、ボリュームベースではなくタイムベースの IPSec SA の有効期限を使用することを推奨します。タイムベースの SA の有効期限を使用するには、**set security-association lifetime kilobytes 536870912** コマンドを使用してライムタイム ボリュームを最大値に設定します。

IKE の設定情報

IKE は、IPSec 標準と組み合わせて使用されるキー管理プロトコル標準です。

IKE は、Security Association and Key Management Protocol（ISAKMP）フレームワーク内で Oakley 鍵交換および Skeme 鍵交換を実装するハイブリッド プロトコルです （ISAKMP、Oakley、および Skeme は IKE によって実装されるセキュリティ プロトコルです）。

Cisco IOS Release 12.2(33)SXF 以前のリリースでは、IKE を使用しなくても IPSec を設定できますが、IKE を使用すると IPSec 標準に機能が追加され、柔軟性が高まり、設定が容易になって、IPSec が強化されます。IKE はデフォルトでイネーブルです。

crypto isakmp policy コマンドを使用して各ピアに IKE ポリシーを作成し、IKE を設定します。IKE ポリシーは、IKE ネゴシエーション中に使用されるセキュリティ パラメータの組み合わせを定義し、ピアの認証方法を規定します。

それぞれ異なるパラメータ値が組み合わされた複数の IKE ポリシーを作成できます。ただし、これらのポリシーの少なくとも 1 つに、リモート ピアのポリシーの 1 つとまったく同じ暗号、ハッシュ、認証、および Diffie-Hellman パラメータ値を格納する必要があります。作成したポリシーごとに、一意のプライオリティを割り当てます（1 ～ 10,000 で、1 が最大プライオリティ）。

ポリシーを設定しない場合は、デフォルト ポリシー（常に最小プライオリティに設定され、各パラメータのデフォルト値を格納しているポリシー）が使用されます。

各 IKE ポリシーでは、5 つのパラメータを定義します。

- 暗号化アルゴリズム
- ハッシュ アルゴリズム
- 認証方式
- Diffie-Hellman グループ ID
- セキュリティ アソシエーションのライフタイム

IKE の詳細については、「IKE の概要」（P.27-2）を参照してください。

IPSec VPN SPA を使用した VPN の設定

IPSec VPN SPA を使用して VPN を設定するために、暗号接続モードと VPN ルーティングおよび転送（VRF）モード の 2 つの基本オプションがあります。いずれかのモードで、VPN トンネル内の幅広いプロトコル パケット タイプ（マルチキャスト パケットを含む）をカプセル化するよう GRE トンネリングを設定することもできます。

（注） 暗号接続モードと VRF モードを切り替える場合は、リロードが必要です。

（注） VPN セッションがアクティブな間は、VPN 設定を変更しないことを推奨します。システムが中断しないように、定期メンテナンス時間を設定し、**clear crypto sessions** コマンドを使用してすべての VPN セッションをクリアしてから、VPN 設定を変更することを推奨します。

暗号接続モード

これまで、IPSec VPN SPA に VPN を設定するには、暗号マップをインターフェイス VLAN に適用し、そのインターフェイス VLAN に物理ポートを暗号接続していました。この方法は暗号接続モードといい、Cisco IOS ソフトウェアが稼動するルータに VPN を設定するための方法と似ています。暗号接続モードを使用して IPSec VPN SPA に VPN を設定する場合は、（インターフェイス VLAN を使用して）VLAN に暗号マップを適用します。Cisco IOS ソフトウェアが稼動するルータに VPN を設定する場合は、個々のインターフェイスを設定します。

（注） IPSec VPN SPA を使用する場合も、個々のインターフェイスに暗号マップを適用しますが、許可されるインターフェイスのセットはインターフェイス VLAN に限定されます。

暗号接続モードの VPN 設定については、第 24 章「暗号接続モードでの VPN の設定」を参照してください。

VRF モード

VRF モード（別名 VRF 対応 IPSec）を使用すると、公衆向けのアドレス を 1 つ使用して IPSec トンネルを VPN ルーティングおよび転送（VRF）インスタンスにマッピングできます。VRF インスタンスは、Provider Edge（PE; プロバイダー エッジ）ルータに接続されたカスタマー サイトの VPN メンバーシップを定義する、VPN 単位のルーティング情報リポジトリです。VRF は IP ルーティング テーブル、派生した Cisco Express Forwarding（CEF）テーブル、フォワーディング テーブルを使用する一連のインターフェイス、およびルーティング テーブルに含まれる情報を制御する一連の規則とルーティング プロトコル パラメータで構成されます。VPN カスタマーごとに、異なるルーティング テーブルおよび CEF テーブルのセットが保持されます。

VRF モードを使用して IPSec VPN SPA に VPN を設定する場合、インターフェイス VLAN のモデルは残されていますが、**crypto connect vlan** コマンドは使用しません。代わりに、特定の VRF の特定のサブネットを宛先とするパケットが、そのインターフェイス VLAN に到達するように、ルートを構築する必要があります。

VRF モードを使用して VPN を設定する場合は、GRE を使用した Tunnel Protection（TP; トンネル保護）、および Virtual Tunnel Interface（VTI）の追加トンネリング オプションを使用できます。これらのオプションのいずれかを指定すると、VRF（通常の VRF モード）またはグローバル コンテキストでトンネルを終端できます。

VRF モードの VPN 設定については、第 25 章「仮想ルーティングおよび転送（VRF）モードでのバーチャル プライベート ネットワーク（VPN）の設定」を参照してください。

IPsec 機能のサポート

ここでは、各 VPN モードにおける IPsec VPN モジュールの IPSec 機能のサポート状況をソフトウェア リリース別に表に示します。

- 「すべての VPN モードに共通の IPSec 機能」（P.23-8）
- 「暗号接続モードでの IPSec 機能」（P.23-13）
- 「VRF モードでの IPSec 機能」（P.23-13）

（注） ここでは、サポートされているテスト済の IPSec VPN SPA の機能とアプリケーションについて記載します。この表および後続の章に明示的に記載されていない機能およびアプリケーションは、サポート対象外とお考えください。ここに記載されていない設定を実装する場合は、事前にシスコ アカウント チームにご連絡ください。

すべての VPN モードに共通の IPSec 機能

表 23-1 に、すべての VPN モードに共通のサポートされる IPSec 機能およびサポートされない IPSec 機能を示します。

表 23-1　すべての VPN モードにおける IPSec 機能のサポート（リリース別）

機能名	Cisco IOS ソフトウェア リリース 12.2				
	SXE	SXF	SRA	SRB、SRC、SRD	SXH[1]
ソフトウェア暗号を使用する IPSec トンネル	非サポート	非サポート	非サポート	非サポート	非サポート
拡張された GRE テイクオーバー（スーパーバイザ エンジンが処理できない場合）	サポート	サポート	サポート	サポート	サポート
GRE を介したマルチキャスト	非サポート	サポート	サポート	サポート	サポート
Multipoint GRE（mGRE; マルチポイント GRE）/ Dynamic Multipoint VPN（DMVPN）を介した マルチキャスト	非サポート	非サポート	非サポート	非サポート	非サポート
マルチキャスト スケーラビリティ拡張機能（シングル SPA モード）	非サポート	サポート	サポート	サポート	サポート
Advanced Encryption Standard（AES; 高度暗号化規格）	サポート	サポート	サポート	サポート	サポート
ISAKMP キーリング	サポート	サポート	サポート	サポート	サポート
SafeNet Client サポート	サポート	サポート	サポート	サポート	サポート
ピア フィルタリング（SafeNet Client サポート）	非サポート	非サポート	非サポート	非サポート	非サポート
ISAKMP プロファイル マッピングの認証	サポート	サポート	サポート	サポート	サポート
暗号化事前共有キー	サポート	サポート	サポート	サポート	サポート
IKE アグレッシブ モードの開始	非サポート	非サポート	非サポート	非サポート	非サポート
IKE の Call Admission Control（CAC; コール アドミッション制御）	非サポート	非サポート	サポート	サポート	サポート
Dead Peer Detection（DPD）オンデマンド	サポート	サポート	サポート	サポート	サポート
DPD 定期メッセージ オプション	非サポート	非サポート	サポート	サポート	サポート
IPsec プリフラグメンテーション（Look-Ahead Fragmentation（LAF））	サポート	サポート	サポート	サポート	サポート
逆ルート注入（RRI）	サポート	サポート	サポート	サポート	サポート
オプション パラメータを使用する逆ルート	非サポート	非サポート	非サポート	非サポート	非サポート
調整可能な IPSec アンチリプレイ ウィンドウ サイズ	非サポート	サポート	サポート	サポート	サポート
IPSec 優先ピア	サポート	サポート	サポート	サポート	サポート
暗号マップ単位の（およびグローバルな）IPSec セキュリティ アソシエーション（SA）アイドル タイマー	サポート	サポート	サポート	サポート	サポート

表 23-1　すべての VPN モードにおける IPSec 機能のサポート（リリース別）（続き）

機能名	Cisco IOS ソフトウェア リリース 12.2				
	SXE	SXF	SRA	SRB、SRC、SRD	SXH[1]
Distinguished Name（DN; 識別名）ベースの暗号マップ	サポート	サポート	サポート	サポート	サポート
シーケンス番号付き Access Control List（ACL; アクセス コントロール リスト）（暗号 ACL）	サポート	サポート	サポート	サポート	サポート
拒否ポリシー設定の拡張機能（drop、jump、clear）	サポート	サポート	サポート	サポート	サポート
インターフェイス単位のボリューム ライフタイムのディセーブル化	非サポート	非サポート	非サポート	非サポート	非サポート
IPSec VPN SPA の Quality of Service（QoS）キューイング	サポート	サポート	サポート	サポート	サポート
複数の RSA キー ペアのサポート	非サポート	非サポート	サポート	サポート	サポート
保護された秘密鍵ストレージ	非サポート	非サポート	サポート	サポート	サポート
トラストポイント Command-Line Interface（CLI; コマンドライン インターフェイス）	非サポート	非サポート	サポート	サポート	サポート
トラストポイントごとのクエリー モード	非サポート	非サポート	非サポート	非サポート	非サポート
ローカル証明書ストレージ場所	非サポート	非サポート	サポート	サポート	サポート
Certificate Authority（CA; 認証局）サーバへの HTTP による直接登録	サポート	サポート	サポート	サポート	サポート
手動での証明書登録（Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）およびカットアンドペースト）	非サポート	非サポート	サポート	サポート	サポート
証明書の自動登録	非サポート	非サポート	サポート	サポート	サポート
キーのロールオーバーによる認証局（CA）の更新	非サポート	非サポート	非サポート	非サポート	非サポート
Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）クエリーの複数のサーバ	非サポート	非サポート	非サポート	非サポート	非サポート
Online Certificate Status Protocol（OCSP）	非サポート	非サポート	非サポート	非サポート	非サポート
オプションの OCSP ナンス	非サポート	非サポート	非サポート	非サポート	非サポート
証明書のセキュリティ アトリビュートに基づくアクセス制御	非サポート	非サポート	非サポート	非サポート	非サポート
件名全体を使用する PKI Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）許可	非サポート	非サポート	非サポート	非サポート	非サポート
件名を使用した PKI ローカル認証	非サポート	非サポート	サポート	サポート	サポート

表 23-1　すべての VPN モードにおける IPSec 機能のサポート（リリース別）（続き）

機能名	Cisco IOS ソフトウェア リリース 12.2				
	SXE	SXF	SRA	SRB、SRC、SRD	SXH[1]
認証局での発信トラフィックの送信元インターフェイス選択	非サポート	非サポート	非サポート	非サポート	非サポート
Cisco IOS CA サーバとしての永続的自己署名証明書	非サポート	非サポート	非サポート	非サポート	非サポート
証明書チェーン検証	非サポート	非サポート	非サポート	非サポート	非サポート
マルチティア証明書のサポート	サポート	サポート	サポート	サポート	サポート
Easy VPN サーバの拡張機能	非サポート	非サポート	非サポート	非サポート	非サポート
Easy VPN サーバの基本的な機能	サポート	サポート	サポート	サポート	サポート
事前共有キーを使用する Easy VPN Remote のある相互運用	サポート	サポート	サポート	サポート	サポート
RSA シグニチャを使用する Easy VPN Remote のある相互運用	非サポート	非サポート	サポート	サポート	サポート
ホットスタンバイ ルータ プロトコル（HSRP）を使用したステートレス フェールオーバー	サポート	サポート	サポート	サポート	サポート
HSRP および SSP を使用するシャーシ間のステートフル フェールオーバー、および事前共有キー（暗号マップあり）を使用するサイト間 IPSec	サポート	サポート	非サポート	非サポート	非サポート
DMVPN、GRE/TP、VTI、Easy VPN、または PKI を使用するシャーシ間フェールオーバー（IPSec ステートフル フェールオーバー）	非サポート	非サポート	非サポート	非サポート	非サポート
ブレード間でのステートフル フェールオーバー	サポート	サポート	サポート	サポート	サポート
IPSec VPN モニタリング（IPSec フロー MIB）	サポート	サポート	サポート	サポート	サポート
IPSec VPN アカウンティング（開始/停止/暫定）	サポート	サポート	サポート	サポート	サポート
Crypto Conditional Debug のサポート	非サポート	サポート	サポート	サポート	サポート
show crypto engine accelerator statistic コマンド	非サポート	非サポート	サポート	サポート	サポート
その他の **show crypto engine** コマンド	非サポート	非サポート	非サポート	非サポート	非サポート
clear crypto engine accelerator counter コマンド	非サポート	非サポート	サポート	サポート	サポート
ループバック インターフェイスに適用される crypto コマンド	非サポート	非サポート	非サポート	非サポート	非サポート

表 23-1　すべての VPN モードにおける IPSec 機能のサポート（リリース別）（続き）

機能名	Cisco IOS ソフトウェア リリース 12.2				
	SXE	SXF	SRA	SRB、SRC、SRD	SXH[1]
トンネル インターフェイスまたはインターフェイス VLAN 上の Policy Based Routing（PBR; ポリシー ベース ルーティング）	非サポート	非サポート	非サポート	非サポート	非サポート
トンネル インターフェイス上の ACL	非サポート	非サポート	非サポート	非サポート	非サポート
トンネルインターフェイス上の Modular QoS Command Line Interface（MQC; モジュラ QoS コマンドライン インターフェイス）QoS（サービス ポリシー）	非サポート	非サポート	非サポート	非サポート	非サポート
すべてのトンネル インターフェイス（IPsec、GRE、mGRE）上の **mls qos** コマンド	非サポート	非サポート	非サポート	非サポート	非サポート
QoS pre-classify CLI	非サポート	非サポート	非サポート	非サポート	非サポート
インターフェイス VLAN 上の Network Address Translation（NAT; ネットワーク アドレス変換）（暗号接続モードでテイクオーバーされた GRE）（暗号マップあり）	非サポート	非サポート	非サポート	非サポート	非サポート
16K トンネル（IKE および IPsec トンネル）	非サポート	非サポート	サポート	サポート	サポート
VRF モードと暗号接続モードの切り替えによりリブートが必要	サポート	サポート	サポート	サポート	サポート
トンネル保護（TP）トンネル上の GRE キープアライブ	非サポート	非サポート	非サポート	非サポート	非サポート
mGRE/DMVPN トンネル上の GRE キープアライブ	非サポート	非サポート	非サポート	非サポート	非サポート
IPsec Network Address Translation（NAT; ネットワーク アドレス変換）の透過機能（NAT-T）（トランスポート モード、ESP のみ）	サポート	サポート	サポート	サポート	サポート
Dynamic Multipoint VPN Phase 2（DMVPN）（mGRE; TP および Next Hop Resolution Protocol（NHRP））	サポート	サポート	サポート	サポート	サポート
DMVPN フェーズ 3	非サポート	非サポート	非サポート	非サポート	非サポート
NAT ゲートウェイの後ろの DMVPN ハブ ルータ：トンネル モード	非サポート	非サポート	非サポート	非サポート	非サポート
NAT ゲートウェイの後ろの DMVPN ハブ ルータ：トランスポート モード（スポークツースポークではない）	非サポート	非サポート	非サポート	非サポート	サポート
NAT ゲートウェイの後ろの DMVPN スポーク ルータ：トンネル モード	非サポート	非サポート	非サポート	非サポート	非サポート

表 23-1　すべての VPN モードにおける IPSec 機能のサポート（リリース別）（続き）

機能名	Cisco IOS ソフトウェア リリース 12.2				
	SXE	SXF	SRA	SRB、SRC、SRD	SXH[1]
NAT ゲートウェイの後ろの DMVPN スポーク ルータ：トランスポート モード（スポークツースポークではない）	サポート	サポート	サポート	サポート	サポート
DMVPN トンネル上のマルチキャスト トランジット トラフィック	非サポート	非サポート	非サポート	非サポート	非サポート
TP（DMVPN、ポイントツーポイント GRE、Static Virtual Tunnel Interface（sVTI））トンネル上の 非 IP トラフィック	非サポート	非サポート	非サポート	非サポート	非サポート
Virtual Private Network Services Module（VPNSM; VPN サービス モジュール）のサポート	サポート	サポート	非サポート	非サポート	非サポート
暗号接続モードのシリアル Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）インターフェイスすべてには **ip unnumber null 0** コマンドが含まれている必要がある	非サポート	非サポート	非サポート	サポート	サポート
手動キー	非サポート	サポート	非サポート	非サポート	非サポート
トンネル エンドポイント ディスカバリ	サポート	サポート	非サポート	非サポート	非サポート
転送隣接およびネストされたトンネル	非サポート	非サポート	非サポート	非サポート	非サポート
IPSec パケットの転送	非サポート	サポート	非サポート	非サポート	サポート
Virtual Switching System（VSS）を搭載した IPSec VPN SPA	非サポート	非サポート	非サポート	非サポート	非サポート
IPSec トンネル経由の IP ヘッダー オプション	非サポート	非サポート	非サポート	非サポート	非サポート
無効な Security Parameter Index（SPI; セキュリティ パラメータ インデックス）リカバリ	非サポート	非サポート	サポート	サポート	サポート
IPsec 圧縮	非サポート	非サポート	非サポート	非サポート	非サポート
Multilink PPP（MLPPP; マルチリンク PPP）	サポート	サポート	サポート	サポート	サポート
マルチリンクまたはダイヤラ インターフェイス	非サポート	非サポート	非サポート	非サポート	非サポート
Group Encrypted Transport VPN（GETVPN）	非サポート	非サポート	非サポート	非サポート	非サポート
IPsec パッシブ モード	非サポート	非サポート	非サポート	非サポート	非サポート
ATM Permanent Virtual Circuit（PVC; 相手先固定接続）バンドル	非サポート	非サポート	非サポート	非サポート	非サポート

1. SXH は、Catalyst 6500 シリーズ スイッチ用のソフトウェア リリースです。このリリースは、Cisco 7600 シリーズ ルータには適用されません。

暗号接続モードでの IPSec 機能

表 23-2 に、暗号接続モードでサポートされる IPSec 機能およびサポートされない IPSec 機能を示します。

表 23-2　暗号接続モードにおける IPSec 機能のサポート（リリース別）

機能名	Cisco IOS ソフトウェア リリース 12.2				
	SXE	SXF	SRA	SRB、SRC、SRD	SXH[1]
トンネル保護および VTI を使用したポイントツーポイント GRE	非サポート	非サポート	非サポート	非サポート	非サポート
Path MTU Discovery（PMTUD）	非サポート	非サポート	サポート	サポート	サポート
PMTUD（NAT-T）	非サポート	非サポート	非サポート	非サポート	非サポート
IPSec Static Virtual Tunnel Interface（sVTI）	非サポート	非サポート	非サポート	非サポート	非サポート
暗号機能と組み合わせた VRF の使用	非サポート	非サポート	非サポート	非サポート	非サポート
ポイントツーポイント GRE を介した IPX と Appletalk	サポート	サポート	サポート	サポート	サポート
テイクオーバー時の GRE での **ip tcp adjust-mss** コマンド	非サポート	非サポート	非サポート	非サポート	非サポート

1. SXH は、Catalyst 6500 シリーズ スイッチ用のソフトウェア リリースです。このリリースは、Cisco 7600 シリーズ ルータには適用されません。

VRF モードでの IPSec 機能

表 23-3 に、VRF モードでサポートされる IPSec 機能およびサポートされない IPSec 機能を示します。

表 23-3　VRF モードにおける IPSec 機能のサポート（リリース別）

機能名	Cisco IOS ソフトウェア リリース 12.2				
	SXE	SXF	SRA	SRB、SRC、SRD	SXH[1]
グローバル VRF	サポート	サポート	サポート	サポート	サポート
Front-Door VRF（FVRF; 前面扉 VRF）	非サポート	非サポート	サポート	サポート	サポート
DMVPN ハブに設定された mGRE トンネル上の FVRF	非サポート	非サポート	サポート	サポート	サポート
DMVPN スポークに設定された mGRE トンネル上の FVRF	非サポート	非サポート	非サポート	非サポート	非サポート
VRF 内の IP アドレス スペースのオーバーラップ	サポート	サポート	サポート	サポート	サポート
インターフェイスでのセカンダリ IP アドレス	非サポート	非サポート	非サポート	非サポート	非サポート
MPLS over GRE/IPSec（トンネル インターフェイス上でのタグ スイッチング）	非サポート	非サポート	非サポート	非サポート	非サポート

表 23-3　VRF モードにおける IPSec 機能のサポート（リリース別）（続き）

機能名	Cisco IOS ソフトウェア リリース 12.2				
	SXE	SXF	SRA	SRB、SRC、SRD	SXH[1]
MPLS 上での PE 間での暗号化（IPSec のみ）	非サポート	非サポート	非サポート	非サポート	非サポート
MPLS 上での PE 間での暗号化（トンネル保護）	非サポート	非サポート	非サポート	非サポート	非サポート
GRE/TP を使用する MPLS PE/Customer Edge（CE; カスタマー エッジ）間 での暗号化（Tag2IP）	非サポート	非サポート	非サポート	サポート	サポート
sVTI を使用する MPLS PE/CE 間での暗号化（Tag2IP）	非サポート	非サポート	非サポート	非サポート	非サポート
暗号マップを使用する MPLS PE/CE 間での暗号化（Tag2IP）	非サポート	非サポート	非サポート	非サポート	非サポート
VRF-lite の暗号マップ	サポート	サポート	サポート	サポート	サポート
RADIUS のある VRF 単位の AAA	非サポート	非サポート	非サポート	サポート	サポート
TACACS のある VRF 単位の AAA	非サポート	非サポート	非サポート	サポート	非サポート
IPSec Static Virtual Tunnel Interface（sVTI）	非サポート	非サポート	サポート	サポート	サポート
sVTI を介したマルチキャスト	非サポート	非サポート	非サポート	非サポート	非サポート
sVTI または GRE での **ip tcp adjust-mss** コマンド	非サポート	非サポート	非サポート	非サポート	非サポート
sVTI、GRE/TP、mGRE トンネル上の入力および出力機能（ACL、QOS）	非サポート	非サポート	非サポート	非サポート	非サポート
外部インターフェイス上の入力機能（ACL、PBR、インバウンド サービス ポリシー）	非サポート	非サポート	非サポート	非サポート	非サポート
外部インターフェイス上のアウトバウンド サービス ポリシー	サポート	サポート	サポート	サポート	サポート
グローバル コンテキストでの TP サポート	非サポート	非サポート	サポート	サポート	サポート
トランスポート モードで作成された暗号マップを使用した IPSec SA	非サポート	非サポート	非サポート	非サポート	非サポート
Path MTU Discovery（PMTUD）	非サポート	非サポート	非サポート	非サポート	非サポート
TP トンネル上の非 IPv4 トラフィック	非サポート	非サポート	非サポート	非サポート	非サポート
IPv6 IPsec sVTI IPv6-in-IPv6	非サポート	非サポート	非サポート	非サポート	非サポート

1. SXH は、Catalyst 6500 シリーズ スイッチ用のソフトウェア リリースです。このリリースは、Cisco 7600 シリーズ ルータには適用されません。

ソフトウェア要件

IPsec VPN モジュールでは、次のいずれかの暗号イメージがルータで実行されていることが必要です。

- Supervisor Engine 720（10G を含む）
  - s72033-adventerprisek9_wan-mz
  - s72033-advipservicesk9_wan-mz
  - s72033-adventerprisek9_wan-vz
  - s72033-advipservicesk9_wan-vz
- Supervisor Engine 32（10G を含む）
  - s3223-adventerprisek9_wan-mz
  - s3223-advipservicesk9_wan-mz
  - s3223-adventerprisek9_wan-vz
  - s3223-advipservicesk9_wan-vz

（注）　「-vz」で終わるイメージには、Cisco IOS Release 12.2(33)SRA 以降のリリースが必要です。

相互運用性

スーパーバイザ エンジンのサポートは、リリースによって異なります。

表 23-4 に、各リリースのサポート対象スーパーバイザ エンジンを示します。

表 23-4　IPSec VPN SPA のスーパーバイザ エンジンのサポート（リリース別）

リリース	サポート対象のスーパーバイザ
Cisco IOS Release 12.2(33)SRC	Supervisor Engine RSP720-1GE Supervisor Engine 720 Supervisor Engine 32
Cisco IOS Release 12.2(33)SRA	Supervisor Engine 720 Supervisor Engine 32
Cisco IOS Release 12.2(18)SXF2	Supervisor Engine 720 Supervisor Engine 32 Supervisor Engine 2
Cisco IOS Release 12.2(18)SXE5	Supervisor Engine 720
Cisco IOS Release 12.2(18)SXE2	Supervisor Engine 720

ラインカード モジュールのサポートは、リリースによって異なります。

IPSec VPN SPA は、次の相互運用性機能をサポートします。

- IPSec VPN SPA と同じシャーシ内に次のサービス モジュールを取り付けることができます。
  - ファイアウォール サービス モジュール（WS-SVC-FWM-1-K9）
  - ネットワーク解析モジュール 2（WS-SVC-NAM-2）

表 23-5 に、各リリースのサポート対象であることが判明しているラインカード モジュールを示します。この表を使用する場合は、次の注意事項に従ってください。

- 承認カラムの「○」は、モジュールがテスト済みであることを示します。サポート対象カラムの「○」は、モジュールがサポート対象であることを示します。
- モジュールのサポート対象カラムの「○」に脚注がついている場合、モジュールがサポート対象でも一部の制約事項が適用されます。制約事項の詳細は、表の下の脚注を参照してください。
- モジュールのサポート対象カラムに「○」があり、承認カラムにはない場合、モジュールは厳密な意味でテスト済みではありませんが、サポート対象です。

表に明記されていない他のラインカードは、TAC/BU でサポートされません。

表 23-5　IPSec VPN SPA のラインカードのサポート（リリース別）

ラインカード モジュール	Cisco IOS Release 12.2(18)SX		Cisco IOS Release 12.2(33)SR	
	承認	サポート対象	承認	サポート対象
7600-SIP-200 次の SPA 付き： SPA-2XOC3-ATM= SPA-2XOC3-POS= SPA-2XT3/E3	○	○	○	○
7600-SIP-400 次の SPA 付き： SPA-1XOC12-ATM= SPA-2X0C3-ATM= SPA-2X1GE		○[1]	○[2]	○
7600-SIP-600 次の SPA 付き： SPA-1X10GE SPA-10X1GE			○[3]	○
7600-SSC-400	○	○	○	○
OSM-2OC48/1DPT-SI		○		○
OSM-2OC48/1DPT-SL		○		○
OSM-2OC48/1DPT-SS	○	○		○
OSM-8OC3-POS-MM	○	○	○	○
OSM-8OC3-POS-SI		○		○
OSM-8OC3-POS-SI+		○		○
OSM-8OC3-POS-SL		○		○
OSM-16OC3-POS-MM+	○	○	○	○
OSM-16OC3-POS-SI		○		○
OSM-16OC3-POS-SI+		○		○
OSM-16OC3-POS-SL		○		○
OSM-2+4GE-WAN+	○	○		○
WS-6182-2PA	○	○	○	○
WS-6582-2PA	○	○	○	○

表 23-5　IPSec VPN SPA のラインカードのサポート（リリース別）（続き）

ラインカード モジュール	Cisco IOS Release 12.2(18)SX		Cisco IOS Release 12.2(33)SR	
WS-6802-2PA 次の PA 付き： PA-A3-OC3MM PA-A3-T3 PA-MC-T3	○	○		○
WS-SVC-FWM-1	○	○		○
WS-SVC-IDSM2	○	○		
WS-SVC-IDSUPG	○	○		
WS-SVC-NAM2	○	○		
WS-SVC-WEBVPN-K9	○	○		○
WS-X6148-GE-TX	○	○	○	○
WS-X6408A-GBIC	○	○		○
WS-X6416-GBIC	○	○		○
WS-X6416-GE-MT		○		○
WS-X6502-10GE	○	○	○	○
WS-X6516-GBIC	○	○	○	○
WS-X6516-GE-TX	○	○	○	○
WS-X6516A-GBIC	○	○	○	○
WS-X6548-GE-TX	○	○	○	○
WS-X6548V-GE-TX		○		○
WS-X6548-RJ-21		○		○
WS-X6548-RJ-45	○	○	○	○
WS-X6704-10GE	○	○	○	○
WS-X6748-GE-TX	○	○	○	○
WS-X6748-SFP	○	○	○	○

1. Cisco IOS Release 12.2(18)SXF2：Cisco 7600 SIP-400 がシャーシ内にあるとき、スイッチ ポート コンフィギュレーションはサポートされません。
2. Cisco IOS Release 12.2(33)SRA：Cisco 7600 SIP-400 がシャーシ内にあるとき、スイッチ ポート コンフィギュレーションはサポートされません。
3. Cisco IOS Release 12.2(33)SRA：Cisco 7600 SIP-600 が搭載されていて、VRF をイネーブルにするときは、MPLS トンネル再循環がイネーブルになっている必要があります。つまり、Cisco 7600 SIP-600 がシャーシにある場合、**crypto engine mode vrf** コマンドを入力する前に、**mls mpls tunnel-recir** コマンドを追加する必要があります。

制約事項

（注） その他の SPA Services Card（SSC; SPA サービス カード）固有の機能および制約事項については、このマニュアルの第 3 章「SPA インファーフェイス プロセッサ（SIP）および SPA サービス カード（SSC）の概要」も参照してください。

次の制約事項は IPSec VPN SPA を対象としています。

- IPSec VPN SPA には Cisco IOS Release 12.2(18)SXE2 以降のリリースが必要です。
- IPSec VPN SPA は、Cisco 7600 SSC-400 に限りサポートされます。
- Cisco 7600 SSC-400 は、Route Processor Redundancy Plus（RPR+）または Stateful Switchover（SSO; ステートフル スイッチオーバー）対応ではありません。その結果、RPR+ または SSO の設定時に Cisco 7600 SSC-400 がリセットされます。
- Cisco IOS Release 12.2(33)SRA では、IPSec VPN SPA は最小 512 MB メモリの Supervisor Engine 720（MSFC3 および PFC3）または Supervisor Engine 32 を使用する Cisco 7600 シリーズ ルータに限りサポートされます。各リリースでサポートされるスーパーバイザ エンジンのリストについては、表 23-4（P.23-15）を参照してください。

（注）　IPSec VPN SPA MSFC DRAM の要件は次のとおりです。

– 最大 8,000 トンネルの 512 MB DRAM
– 最大 16,000 トンネルの 1 GB DRAM

これらの数値は、ルーティング プロトコルおよびその他のアプリケーションが使用できるように、一部のメモリを残して選択されます。ただし、MSFC の使用状況によっては、上記よりも多くのメモリが必要になる場合があります。極端なケースでは、トンネルを 1 つしか使用しなくても、MSFC 上で動作する他のプロトコルおよびアプリケーション用に 512 MB の DRAM が必要になる場合も考えられます。

- 次の Cisco 7600 シリーズ ルータだけがサポートされます。
  - 7603 ルータ（CISCO7603）
  - 7606 ルータ（CISCO7606）
  - 7609 ルータ（CISCO7609）
  - 7609 ルータ（OSR-7609）
  - 7613 ルータ（CISCO7613）
- シャーシあたり最大 10 の IPSec VPN SPA がサポートされます。
- Cisco IOS Release 12.2(33)SRA では、PKI が IPSec VPN SPA とともに設定されているとき、最大 2000 の IPSec トンネルがサポートされます。
- Cisco IOS Release 12.2(33) SRB では、VTI トンネルで TCP ADJUST-MSS はサポートされません。

（注）　Cisco IOS Release 12.2(18)SXF2 以降のリリースでは、それまでのリリースで使用されていた **crypto engine subslot** コマンドは、**crypto engine slot** コマンド（形式は **crypto engine slot** *slot/subslot* {**inside** | **outside**}）に置き換えられました。**crypto engine subslot** コマンドはサポートされなくなりました。

アップグレード時には、余計なメンテナンス時間がかからないように、このコマンドが起動コンフィギュレーション内で変更されていることを確認してください。

サポートされる MIB

Cisco 7600 シリーズ ルータに Cisco 7600 SSC-400 および IPSec VPN SPA が搭載されている場合、Cisco IOS Release 12.2(18)SXE2 では次の MIB がサポートされます。

- CISCO-IPSEC-FLOW-MONITOR-MIB

（注）　ギガビット イーサネット ポート Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）統計情報（ifHCOutOctets、ifHCInOctets など）は、内部 IPSec VPN SPA トランク ポートには提供されません。これらのポートは外部的には動作中のモードではなく、設定専用に使用されるためです。

Cisco 7600 シリーズ ルータの MIB サポートの詳細については、次の URL にある『*Cisco 7600 Series Router MIB Specifications Guide*』を参照してください。

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

選択されたプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに対応する MIB を検索し、ダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://tools.cisco.com/ITDIT/MIBS/servlet/index

必要な MIB 情報が Cisco MIB Locator でサポートされていない場合は、次の URL にある Cisco MIB ページからサポート対象 MIB のリストを入手して、MIB をダウンロードすることもできます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cisco MIB Locator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたか、紛失した場合は、cco-locksmith@cisco.com に空の E メールを送信してください。送信された E メール アドレスが Cisco.com に登録されているかどうか、自動チェック機能によって確認されます。チェックに成功すると、アカウントの詳細と新規のランダム パスワードが E メールで通知されます。承認されたユーザは次の URL の指示に従って、Cisco.com のアカウントを確立できます。

http://www.cisco.com/register

IPSec VPN SPA ハードウェア設定時の注意事項

IPSec VPN SPA ハードウェアを設定するときは、次の注意事項に従ってください。

- システム イメージおよびコンフィギュレーション ファイルの管理については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』Release 12.2 および『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。
- 一部の CLI コマンドでは、*slot/subslot/port* の形式で IPsec VPN モジュールの内部ポートと外部ポートを指定する必要があります。IPsec VPN モジュール ポートは実際にはギガビット イーサネット ポートではなく、外部ギガビット イーサネット インターフェイスのすべてのプロパティを共有しているとは限りませんが、次のポート番号を使用してギガビット イーサネット トランク ポートとして設定できます。
  - ポート 1：内部ポート、インターフェイス VLAN に適用
  - ポート 2：外部ポート、ポート VLAN に適用

  たとえば、Cisco 7600 シリーズ ルータのスロット 6 に Cisco 7600 SSC-400 が搭載され、その最初のサブスロット（subslot 0）に IPsec VPN モジュール が搭載されている場合に、外部ポートを設定するには次のコマンドを入力します。

```
Router(config)# interface GigabitEthernet6/0/2
```

- 暗号接続が確立されていない場合、シャーシにアダプタが取り付けられていても、**show crypto engine configuration** コマンドで IPSec VPN SPA のサブスロット番号は表示されません。
- 暗号接続で使用中のポートを備えた IPSec VPN SPA を取り外しても、その暗号接続は保持されます。同じスロットに同じタイプの IPSec VPN SPA を取り付けると、暗号接続は再度確立されます。IPSec VPN SPA を別のスロットに移動する場合、IPSec VPN SPA を取り外す前に、まず暗号接続を手動で削除する必要があります。対応する物理ポートを取り外した場合には、任意のインターフェイスから **no crypto connect vlan** コマンドを入力します。
- 暗号接続で使用している IPSec VPN SPA を再起動しても、既存の暗号接続は保持されます。IPSec VPN SPA を再起動すると、暗号接続は再度確立されます。暗号接続が確立されていても、IPSec VPN SPA の内部ポートに対応するインターフェイス VLAN がない場合には、IPSec VPN SPA を再起動した時点でその暗号接続は削除されます。
- **no interface vlan** コマンドを使用してポート VLAN またはインターフェイス VLAN を削除すると、対応付けられた暗号接続も削除されます。

SPA ハードウェア タイプの表示

Cisco 7600 シリーズ ルータには、IPSec VPN SPA ハードウェア情報を表示するいくつかのコマンドがあります。

- ルータに搭載された SPA ハードウェアのタイプを確認するには、**show module** コマンドを使用します。
- IPSec VPN SPA のハードウェア情報を表示するには、**show crypto eli** コマンドを使用します。

コマンドの詳細については、『*Cisco 7600 Series Router Command Reference, 12.2SR*』を参照してください。

show module コマンドの例

次に、Cisco 7600 シリーズ ルータのスロット 4 に搭載された Cisco 7600 SSC-400 のサブスロット 0 にある IPSec VPN SPA について、**show module** コマンドの出力例を示します。

```
Router#show module 4
Mod Ports Card Type                                   Model              Serial No.
--- ----- ------------------------------------------ ------------------ -----------
  4    0  2-subslot Services SPA Carrier-400     7600-SSC-400       JAB1104013N

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  4  001a.a1aa.95f0 to 001a.a1aa.962f   2.0   12.2(33)SXH  12.2(33)SXH  Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------- -------
 4/0 2 Gbps IPSec SPA            SPA-IPSEC-2G       JAB1048075L  1.0    Ok

Mod  Online Diag Status
---- -------------------
  4  Pass
 4/0 Pass

Router#
```

show crypto eli コマンドの例

次に、Cisco 7600 シリーズ ルータのスロット 3 に搭載された Cisco 7600 SSC-400 のサブスロット 0 および 1 にある IPSec VPN SPA について、**show crypto eli** コマンドの出力例を示します。出力には、アクティブな IKE SA および IPSec セッション数および各 IPSec VPN SPA に使用されている Diffie-Hellman キー数が表示されます。

```
Router# show crypto eli

Hardware Encryption : ACTIVE
Number of hardware crypto engines = 2

CryptoEngine SPA-IPSEC-2G[3/0] details: state = Active
Capability      :
    IPSEC: DES, 3DES, AES, RSA

IKE-Session   :     0 active, 16383 max, 0 failed
DH            :     0 active,  9999 max, 0 failed
IPSec-Session :     0 active, 65534 max, 0 failed

CryptoEngine SPA-IPSEC-2G[3/1] details: state = Active
Capability      :
    IPSEC: DES, 3DES, AES, RSA

IKE-Session   :     1 active, 16383 max, 0 failed
DH            :     0 active,  9999 max, 0 failed
IPSec-Session :     2 active, 65534 max, 0 failed

Router#
```