機能の相違

このマニュアルは、VPN 3000 シリーズ コンセントレータの現行のユーザがセキュリティ アプライアンスに移行する場合に役立ちます。このマニュアルでは、2 つのデバイス、およびデバイスに付属するソフトウェアの違いについて説明します。セキュリティ アプライアンスの機能の詳細については、次に示すマニュアルを参照してください。

- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5505 Getting Started Guide*
- *Cisco ASA 5550 Getting Started Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 シリーズ製品 CD*
- *Release Notes for Cisco Secure Desktop*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASDM オンライン ヘルプ*
- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*
- *Cisco ASDM Release Notes*

セキュリティ アプライアンスは、VPN 3000 シリーズ コンセントレータのほとんどの機能を実装しますが、状況によっては、それらの機能の設定方法や使用方法が VPN 3000 の従来の方法と異なる場合があります。この章では、セキュリティ アプライアンス ソフトウェアと VPN 3000 シリーズ コンセントレータのソフトウェアの具体的な違いをリストで示します。VPN 3000 Concentrator Manager と Adaptive Security Appliance Device Manager のグラフィカル ユーザ インターフェイスの違いについては、付録 A「VPN 3000 シリーズ コンセントレータと ASDM の項目の比較」にリストを示します。

VPN 3000 コンセントレータと ASA Version 7.1 の機能の比較

表 1-1 は、VPN 3000 シリーズ コンセントレータの機能と、ASA Version 7.1 までで使用できる機能の比較を要約しています。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較

機能名	VPN 3000	ASA
デフォルトの暗号化アルゴリズム	3DES がすべての暗号化操作のデフォルトです。いずれの暗号化アルゴリズムでもライセンスは必要ありません。	DES が「基本」の暗号化アルゴリズムです。3DES および AES には「追加」ライセンスが必要です。
IKE ネゴシエーション	IKE フェーズ 1 ID は、グループ名（受信専用）、IP アドレス、または証明書 DN のいずれかです。送信されるフェーズ 1 ID は、VPN 3000 コンセントレータが事前共有鍵または証明書のどちらのネゴシエーションを行っているかによって異なります。	ASA は IKE フェーズ 2 の複数のトランスフォームをサポートしており、IKE フェーズ 1 の複数の提案事項を送信できます。IKE フェーズ 1 ID は設定可能で、複数のオプションがあります。
フェーズ 2 データ整合性のデフォルト設定	フェーズ 2 データ整合性のデフォルト設定は MD5 です。	フェーズ 2 データ整合性値のデフォルト設定は、「off」です。この設定により、以前のバージョンの PIX および IOS との互換性が保たれます。VPN 3000 コンセントレータと連携するようにセキュリティ アプライアンスを設定する場合、状況によっては、フェーズ 2 データ整合性をイネーブルにする必要があります。ハッシュ アルゴリズムのいずれか（SHA1 または MD5）を使用して、IPSec データが認証されていることを*保証*するには、ネットワーク管理者はフェーズ 2 データ整合性をオンにする必要があります。 フェーズ 2 データ整合性をイネーブルにするには、この表の次にある項 P.1-12 の「ASA のフェーズ 2 データ整合性のイネーブル化」の手順に従って、使用している暗号マップに関連付けられたトランスフォーム セットで SHA1 または MD5 をオンにします。これらのコマンドは、ハッシュ アルゴリズムとして SHA/HMAC-160 をイネーブルにします。
低メモリ アクション	低メモリ状態は、メモリが不足しているときに新しく接続しないようにします。	デバイスのメモリが不足しているときに、新しく接続しないようにします。「低メモリ」状態は存在しません。
「正常リブート」コンフィギュレーション	「正常リブート」機能をサポートしています。この機能は、一部のアプリケーションが適正にクリーンアップされるまで、VPN 3000 コンセントレータをリブートしないようにします。IKE の場合、すべてのトンネルがダウンになるまでコンセントレータはリブートされません。	「正常リブート」機能は、VPN 3000 の場合と同じように動作しますが、設定方法が異なります。最初に、サブシステムがクリーンアップされるまで待機してからリブートを行うようにリブートを設定します。次に、リブートの通知を受け取り、すべてのトンネルがダウンしたときにリブートを許可するように、IKE を設定します。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
ハブアンドスポーク構成のサポート	ハブアンドスポーク構成をサポートしています。	ハブアンドスポーク構成をサポートしています。ハブアンドスポーク構成では、暗号化されたトラフィックはインターフェイスで受信されてそこで復号化され、ファイアウォール規則の適用後、同じインターフェイスからクリア テキストで送信されます。このような「クライアント U ターン」リモート アクセス接続は、セキュリティ アプライアンスの外部インターフェイスで終端できます。そのため、リモート アクセス ユーザの VPN　トンネルからインターネットへのトラフィックは、ファイアウォール規則の適用後、受信されたのと同じインターフェイスから送信されます。
DoS 攻撃（サービス拒絶攻撃）からの保護	DoS 攻撃を防ぐために、アグレッシブ モードをブロックできます。 DHCP リレーもディセーブルにできます。	DoS 攻撃を防ぐために、アグレッシブ モードをブロックできます。
CLI	メニュー主導の選択。製品の主要なインターフェイスは GUI です。	PIX/IOS に類似の文シンタックス
グラフィカル ユーザ インターフェイス	HTML ベースの管理アプリケーションを使用します。	Java ベースの管理アプリケーションを使用します。
パケット検査	VPN 3000 コンセントレータでは、通過するデータは検査されません。	ASA はファイアウォールなので、すべてのデータの検査と、一定レベルのインテリジェント検査を実行します。
ユーザの設定	User Management でユーザを設定します。	Properties > Device Administration でユーザを設定します。
AIP SSM（Advanced Inspection and Prevention Security Services Module）	利用できません。	使用できる AIP SSM 機能は、ASA モデルによって異なります。
ロギング	13 段階のイベント ロギングの重大度を許可します。	次の 2 つのロギング メカニズムをサポートしています。 • syslog。レベルは 1 ～ 7 です。VPN 3000 イベント ロギング機能と同等です。 • dbgtrace。このトラブルシューティング インターフェイスではレポート機能が制限されており、たとえば dbgtrace はコンソールにしか表示されません。dbgtrace のロギング レベルは、1 ～ 11、および 254 と 255 です（これらのレベルの説明については、付録 B「VPN 3000 シリーズ コンセントレータと ASA のデバッグ レベルまたは イベント レベルの比較」を参照）。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
ワイルドカード マスク	VPN 3000 コンセントレータは、0.0.0.255 のバリエーションであるワイルドカード マスク、およびワイルドカード マスクの逆、つまり 255.255.255.0 のバリエーションであるネットワーク マスクを使用します。 VPN 3000 フィルタおよびダウンロード可能な ACL は、ワイルドカード ベースです。	セキュリティ アプライアンスでは、常にネットワーク マスクが予期されているため、ワイルドカード マスクは正しく動作しません。 • VPN 3000 コンセントレータからセキュリティ アプライアンスに移行する場合、ネットワーク管理者は、ワイルドカードではなくネットマスクを使用してセキュリティ アプライアンスの暗号およびインターフェイス ACL を設定する必要があります。 • 既存の VPN 3000 RADIUS DACL コンフィギュレーションを、ネットマスクに変更する必要があります。 • VPN 3000 とセキュリティ アプライアンスが混在して導入されている場合に RADIUS から ACL をダウンロードするときは、VPN 3000 がワイルドカードを使用して DACL を取得し、セキュリティ アプライアンスがネットマスクを使用して DACL を取得できるよう、いくらかのセグメンテーションが必要になります。
セッション タイムアウト	TCP 接続を確立したアプリケーションは、データを渡すことがなくても、無制限にアップ状態にとどまることができます。この動作は VPN 3000 コンセントレータでは許容されますが、セキュリティ アプライアンスでは許容されません。	ASA は TCP 接続を監視して、接続がアクティブであることを確認します。接続が非アクティブな時間が一定の時間（設定可能）に達すると、ASA は TCP 接続を強制的に終了します。長時間使用されていないトンネルを終了するのと同様です。セキュリティ アプライアンスでは、理由が示されることなく、これらのセッションはタイムアウトになります。このため、アプリケーションが続行するにはセッションを再確立する必要があります。
PKI および X.509 証明書のサポート	トラストポイントの概念はありません。	次のように、大きな概念上の変更、および多数のシンタックスの変更があります。 • トラストポイントの新しい概念、およびトラストポイントに証明書を関連付ける方法。 • VPN 3000 PKI 機能が追加された IOS ベースの PKI 機能のサポート。
	RSA 鍵の最大長は 2K です。	暗号化 / 復号化の操作では、セキュリティ アプライアンスは長さが最大 4K の RSA 鍵を処理できます。
	X.509 証明書を使用した VPN クライアント認証をサポートしています。	X.509 証明書のサポートには、n ティア証明書チェーン（複数レベルの認証局階層を使用する環境用）と、手動登録（オフライン認証局を使用する環境用）のサポートが含まれています。ASA は、Cisco IOS で導入された新しい認証局である、ライトウェイト X.509 認証局もサポートしています。この認証局は、PKI がイネーブルになっているサイトツーサイト VPN 環境のロールアウトを簡略化するように設計されています。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
	DSA 鍵と RSA 鍵をサポートしています。	Version 7.0.x と 7.1.x では、DSA 鍵と RSA 鍵をサポートしています。Version 7.2(1) 以上では、RSA 鍵のみをサポートします。
WebVPN	すべてのモデルで設定および使用できます。最新の VPN 3000 コンセントレータ Release 4.7 で使用できる機能を提供します。次の機能が含まれます。 • Cisco Secure Desktop • SSL VPN Client • ネットワーク アドミッション制御 • NTLM 認証 • Citrix • PDA サポート	WebVPN のサポートは、VPN 3000 シリーズ コンセントレータより広い範囲を提供しています。次のサポートが含まれます。 • Cisco Secure Desktop • SSL VPN Client • ネットワーク アドミッション制御 • 認証と認可に関する機能拡張 • Citrix サポート • PDA サポート • シングル サインオン • WebVPN パフォーマンスの最適化 • CIFS ファイルの文字符号化の WebVPN サポート • WebVPN と SSL VPN クライアントの接続の圧縮 • WebVPN 接続のアクティブ / スタンバイ ステートフル フェールオーバー 詳細については『*Cisco ASA 5500 Series Release Notes*』を参照してください。 **注** : WebVPN は、PIX ハードウェアでは利用できません。
SSL VPN Client	Keep Cisco SSL VPN Client 機能が含まれます。この機能は、SVC 常時インストールをイネーブルにするか、または SVC 自動アンインストール機能をディセーブルにします。SVC は後続の SVC 接続に備えてリモート コンピュータにインストールされたまま残り、リモート ユーザの SVC 接続時間を短縮します。	ASA は、Keep Cisco SSL VPN Client（VPN 3000 シリーズ コンセントレータ) の名前を Keep Installer on Client System に変更します。 SVC サポートは、たとえば以下の点で VPN コンセントレータのサポートより優れています。 • 圧縮 : SVC 接続上の圧縮をイネーブルまたはディセーブルにします。 • 鍵再ネゴシエーション設定 : セキュリティ アプライアンスと SVC が鍵の再生成を行うと、暗号鍵と初期ベクトルを再ネゴシエーションし、接続のセキュリティを強化します。 • デッド ピア検知：Dead Peer Detection（DPD; デッド ピア検知）によって、ピアが応答しない状態、または接続が失敗した状態をセキュリティ アプライアンスまたは SVC がすばやく検出することが保証されます。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
ライセンス	ライセンスは必要ありません。	ハードウェア プラットフォームによっては、個別のオプション ライセンスを基本ライセンスに追加することにより、追加の機能にアクセスできます。ハードウェア プラットフォームに見合ったライセンスを独自に組み合せることができます。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の付録 A を参照してください。
AAA	基本グループ、グループ、およびユーザの概念を使用します。	• ASA には、基本グループの代わりに 3 つのデフォルト トンネル グループがあります。これは、IPSec リモート アクセス、LAN 間 IPSec、および WebVPN の各接続タイプに対応しています。デフォルト グループ ポリシーは 1 つしかありません。証明書ベースのトンネルでデフォルト グループを基本グループとして使用することはできません。 • トンネル グループおよびグループ ポリシーの機能は、VPN 3000 とは異なる方法で分割されています。一部のアトリビュートは、トンネル グループに移動されました。これらのアトリビュートは、外部 AAA サーバでは設定できません。 • 外部グループで使用できないアトリビュートは、次のとおりです。 — strip-realm — peer-id-validate — authorization-required — authorization-dn-attributes — authentication server type selection — authorization server type selection — radius-with-expiry
	ハイブリッド サーバ グループをサポートしています（つまり、1 つのグループに異なるタイプのサーバを配置できます）。	サーバ グループの概念を使用します。1 つのサーバ グループ内のサーバはすべて同じタイプにする必要があります。
	フォールバック メカニズムはありません。	新しいフォールバック メカニズム。ネームド サーバが使用できない場合の LOCAL へのフォールバックが含まれます。
	管理トラフィックのアカウンティングはありません。	強化された AAA 機能。管理トラフィックのアカウンティングが含まれます。
	RADIUS アカウンティング データは、単一のサーバに送信されます。	同時 RADIUS アカウンティングをサポートしています。アカウンティング メッセージを単一サーバに送信するか（Single モード）、グループ内のすべてのサーバに送信するか（Simultaneous モード）を指定できます。
IPSec	トンネル型 ESP（ESP トンネル内の ESP）をサポートしていません。	トンネル型 ESP をサポートしています。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
オブジェクト グループ	使用されていません。その代わり、VPN 3000 はネットワーク リストを使用して、コンフィギュレーションを簡略化します。	オブジェクト グループを使用して、アクセス リストの作成とメンテナンスを簡略化します。
グループ アトリビュート：グループ ロック	グループ ロック機能は、イネーブルかディセーブルのいずれかです。イネーブルにすると、VPN 3000 は、VPN クライアントが接続を確立するときに使用したグループ名が、ユーザに割り当てられたグループ名と同じかどうかをチェックします。同じでない場合、接続はドロップされます。同じである場合、接続は許可されます。	ASA では、group-lock アトリビュートはグループ ポリシーの一部であり、パラメータがとる値はトンネル グループの実際の名前です。group-lock がグループ ポリシーに存在する場合、ASA は接続中に、VPN クライアントで使用されたグループ名が、group-lock アトリビュートにあるトンネル グループ名と同じかどうかをチェックします。
ロード バランシング	Cisco VPN Client（Release 3.0 以降）、Cisco VPN 3002 Hardware Client（Release 3.5 以降）、または Cisco PIX 501/506E（Easy VPN クライアントとして動作）で開始されたリモート セッション用にサポートされています。 ロード バランシングは、IPSec クライアントと WebVPN セッションの両方で機能します。	ASA5520 以上のシステムでのみ使用できます。PIX ハードウェアまたは ASA 5505 または 5510 システムでは使用できません。
モード	同等の概念はありません。	• 仮想コンテキスト、および透過モードとルーテッド モードをサポートしています。 • VPN は単一ルーテッド モードでのみ動作します。例外として、透過モードでも、ASA に対する 1 つの管理セッションを実行できます。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
Quality of Service（QoS）	すべてのモデルで設定できます。	ASA 5520 以上のモデルでのみ設定できます。PIX ハードウェア、ASA 5505 および 5510 では使用できません。
	最大レートでの帯域幅ポリシングを提供します。最大レートを超えるトラフィックはドロップされます。	トンネル型または非トンネル型を問わず、すべてのトラフィックにレート制限（ポリシング）を適用できますが、優先クラス トラフィックにはレート制限を適用できません。ASA では、最大レートを超えるトラフィックも送信されますが、レートは最大レートに抑制されます。
	• トンネル トラフィックの最小帯域幅レートを保証します。この結果、1 人のユーザによってインターフェイスでの回線レートが過剰になり他のユーザが使用できる帯域幅が不足することがなくなります。 • 予約されている未使用の帯域幅を、「盗む」ことを許可します。	帯域幅予約はサポートされていません。最小帯域幅保証はありません。
	低遅延キューイングはありません。	• Low-Latency Queueing（LLQ; 低遅延キューイング）を使用します。その結果、デバイスを経由する特定のトラフィック タイプの優先順位を設定できます。LLQ はレート制限*されません*。 • LLQ トラフィック以外のすべてのトラフィックは、「ベストエフォート」と見なされます。すべての LLQ トラフィックにサービスが提供された後、このトラフィックにベストエフォート サービスが提供されます。上限は、ベストエフォート キューの項目数です。ベストエフォート キューがいっぱいになると、以降のベストエフォート トラフィックはドロップされます。
	トンネル トラフィックにのみ適用されます。通常は、パブリック インターフェイスに適用されます。	トンネルグループ情報または ACL のいずれかに基づいて QoS を設定できます。
VPN を許可するためのファイアウォール機能のロック解除	VPN 3000 には適用されません。	ロック解除は必要ありません。1 つのインターフェイスで ISAKMP をイネーブルにすると、セキュリティ アプライアンスはトンネルをネゴシエートできるようになります。

表 1-1　VPN コンセントレータと ASA Version 7.1 までの機能の比較（続き）

機能名	VPN 3000	ASA
フィルタ /ACL	フィルタは、トラフィックに適用される規則で構成されています。これらの規則は、フィルタに配置された順序で適用されます。規則で指定したすべてのパラメータにパケットが一致すると、その規則で指定されたアクションがシステムによって実行されます。一致しない規則パラメータが 1 つでもあれば次の規則が適用され、その後も同様に続行されます。一致する規則がない場合は、フィルタで指定されたデフォルトのアクションがシステムにより実行されます。 • WebVPN では、フィルタを使用して、指定された URL へのアクセスを制御します。 • VPN 3000 コンセントレータで使用するフィルタを、VPN コンセントレータまたは外部の RADIUS サーバで設定できます。 フィルタを設定するには次の 2 つの手順に従います。 • 基本フィルタ パラメータ（名前、デフォルト アクションなど）の設定 • フィルタへの規則の割り当て インターフェイスにフィルタを適用します。これらのフィルタは、インターフェイスを経由するすべてのトラフィックを管理するため、セキュリティ上、最も重要なフィルタです。グループとユーザにもフィルタを適用することにより、インターフェイスを経由するトンネル型トラフィックを管理します。	• ACL はすべてのトラフィックを管理します。 • Cisco ASA 5500 シリーズ セキュリティ アプライアンスは、発信 ACL と時間ベース ACL（既存の着信 ACL サポートの上に構築）をサポートしています。管理者は、トラフィックがインターフェイスで受信されるかインターフェイスから送信されるときに、アクセス コントロールを適用できます。時間ベースのアクセス コントロール リストを使用すると、管理者は、特定の ACL エントリをアクティブにする時間を定義することにより、リソースの使用方法をより強力に制御できます。管理者は新しいコマンドを使用して、時間範囲を定義し、それらの時間範囲を特定の ACL に適用できます。 • 特定の ACL エントリに「active」または「inactive」キーワードを追加することにより、それらのエントリをイネーブルまたはディセーブルにできます（キーワードのない規則はアクティブです）。このトラブルシューティング ツールを使用すると、ACL を簡単に微調整できます。

VPN 3000 コンセントレータと ASA Version 7.2 の機能の比較

表 1-2 に、ASA が VPN コンセントレータからさまざまな方法で実装する新しい機能の比較を要約しています。

表 1-2　VPN コンセントレータと ASA Version 7.2 の新しい機能の比較

機能名	VPN 3000	ASA
L2TP、L2TP over IPSec、および PPTP のサポート	L2TP、L2TP over IPSec、および PPTP 機能をサポートしています。	Release7.2(1) では、L2TP over IPSec のサポートが追加されています。ASA では、L2TP 機能も PPTP 機能もサポートされません。 • 1 つまたは複数の NAT デバイスへの複数のクライアントへのリモート　アクセス L2TP-over-IPSec 接続を正常に確立する機能が含まれます。 • グループ　ポリシーまたはユーザ　ベースの L2TP over IPSec を設定します。 • さらに、IPSec トランスフォーム セットをトンネル モードでなくトランスポート モードで設定する必要があります。
ネットワーク アドミッション制御	NAC は、PPP、IPSec などのアクセス方法が提供する ID ベースの検証に加えて、ピアをそのポスチャまたは状態に基づいて検証する方法を提供します。	NAC の ASA サポートには、VPN 3000 コンセントレータ シリーズが提供するすべての NAC 機能が含まれます。
	• ステートフル フェールオーバーはサポートされません。	• NAC ステートフル フェールオーバーは、セキュリティ アプライアンス上の VPN ステートフル フェールオーバー機能を使用します。フェールオーバーが発生すると、それまでアクティブ ユニットに接続されていた VPN 接続がスタンバイ ユニットに接続されます。スタンバイ ユニットの状態変化によって、該当するすべての VPN セッションのフル ポスチャ検証がトリガーされます。
	• グループ ベースまたはユーザ ベースの NAC セッションを初期設定または再検証できます。	• トンネル　グループに関連付けられたすべての NAC セッションを初期設定または再検証できます。
	• グループ ベースまたはユーザ ベースのポスチャ検証の対象から除外するオペレーティング システムを設定できます。	• グループ　ポリシーごとに、ポスチャ検証の対象から除外するオペレーティング システムのリストを設定できます。
証明書失効チェック	CRL をチェックし、証明書のステータスを確認します。	CRL チェックに加えて、Online Certificate Status Protocol（OCSP）もサポートします。OCSP は、CRL チェックに代わって X.509 デジタル証明書の失効ステータスを確認します。クライアントが大きな証明書失効リスト全体をダウンロードする必要はなく、OCSP が Validation Authority（VA; 検証局）の証明書ステータスを確認します。OCSP は、個々の証明書のステータスについてこの検証局に照会します。

表 1-2　VPN コンセントレータと ASA Version 7.2 の新しい機能の比較

機能名	VPN 3000	ASA
RIPv2　アクティブおよびパッシブ	サポートされています。	ASA は、現在 RIP Version 1 と RIP Version 2 をサポートします。セキュリティ アプライアンス上で唯一の RIP ルーティング プロセスをイネーブルにできます。RIP ルーティング プロセスをイネーブルにすると、すべてのインターフェイス上で RIP がイネーブルになります。セキュリティ アプライアンスは、デフォルトで RIP Version 1 アップデートを送信し、RIP Version 1 と Version 2 のアップデートを受け入れます。
DDNS	サポートされていません。	ダイナミック DNS（DDNS）アップデート方法を作成し、必要な任意の頻度で DNS サーバ上の Resource Records（RR）をアップデートするように設定できます。 DDNS は DHCP を補足します。DHCP を使用すると、ユーザはクライアントに再利用可能な IP アドレスを動的かつ透過的に割り当てることができます。さらに、DDNS はダイナミック アップデートおよび DNS サーバ上の名前 / アドレス マップとアドレス / 名前マップの同期を可能にします。このバージョンにより、セキュリティ アプライアンスは DNS レコード アップデートのための IETF 標準をサポートします。
Zone Labs Integrity サーバ	Zone Labs Integrity システムを導入するネットワーク内のセキュリティ アプライアンスは、リモート VPN クライアントにセキュリティ ポリシーを強制的に適用するように設定できます。	ASA が実装するこの機能は、VPN コンセントレータと次のように異なります。 • アプライアンス SSL 証明書を受信する場合に、Integrity サーバが接続するセキュリティ アプライアンス上の特定のポートを設定できます。 • Integrity サーバ通信に使用するセキュリティ アプライアンス上のインターフェイスを指定できます。

ASA のフェーズ 2 データ整合性のイネーブル化

ハッシュ アルゴリズム（SHA1 または MD5）のいずれかを使用して IPSec データが認証されていることを保証するには、ネットワーク管理者はフェーズ 2 データ整合性をオンにする必要があります。フェーズ 2 データ整合性をイネーブルにするには、次の手順に従って、使用している暗号マップに関連付けられたトランスフォーム セットで SHA1 または MD5 をオンにします。これらのコマンドは、ハッシュ アルゴリズムとして SHA/HMAC-160 をイネーブルにします。

（注）　次の説明では、IKE と ISAKMP は同等です。VPN のマニュアルでは IKE が使用され、ASA では ISAKMP が使用されます（PIX と同様）。ASA では、すべてのコマンドが **isakmp** を使用します。

ステップ 1　使用しているトランスフォーム セットの SHA/HMAC-160 をイネーブルにします。

crypto ipsec transform-set *transform-set-name* **esp-3des esp-sha-hmac**

ステップ 2　使用している暗号マップにトランスフォーム セットをバインドします。

crypto map *map-name seq-num* **set transform-set** *transform-set-name*

次の例では、ttt という名前のトランスフォーム セットで SHA1 をイネーブルにし、ttt を abc という名前の暗号マップにバインドします。シーケンス番号（seq-num）は 1 です。

```
hostname(config)# crypto ipsec transform-set ttt esp-3des esp-sha-hmac
hostname(config)# crypto map abc 1 set transform-set ttt
hostname(config)#
```