CISCO SYSTEMS

C7200 VSA（VPN Services Adapter）インストレーション コンフィギュレーション ガイド

Text Part Number: OL-9129-02-J

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

FCC クラス A 適合装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に適合していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 適合装置に関する記述：このマニュアルに記載された装置は、無線周波エネルギーを生成および放射する可能性があります。シスコシステムズの指示する設置手順に従わずに装置を設置した場合、ラジオおよびテレビの受信障害が起こることがあります。この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に適合していることが確認済みです。これらの仕様は、住宅地で使用したときに、このような干渉を防止する適切な保護を規定したものです。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。

シスコシステムズの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に適合しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

装置の電源を切ることによって、この装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコシステムズの装置またはその周辺機器が干渉の原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

・干渉がなくなるまで、テレビまたはラジオのアンテナの向きを変えます。

・テレビまたはラジオの左右どちらかの側に装置を移動させます。

・テレビまたはラジオから離れたところに装置を移動させます。

・テレビまたはラジオとは別の回路にあるコンセントに装置を接続します（装置とテレビまたはラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

米国シスコシステムズ社では、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

シスコシステムズが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）パブリック ドメイン バージョンの一部として、UCB が開発したプログラムを最適化したものです。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取引によって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

C7200 VSA（VPN Services Adapter）インストレーション コンフィギュレーション ガイド

CONTENTS

はじめに

ここでは、このマニュアルの目的と構成について説明するとともに、関連製品およびサービス情報の入手方法について説明します。具体的な内容は次のとおりです。

対象読者

このマニュアルは、シスコ ルータ ハードウェアおよびケーブル接続に関する知識だけでなく、電子回路や配線手順に関する知識のある読者を対象としています。電子または電気機器の技術者としての経験も必要です。

警告

警告 **システムの過熱を防止するために、室温が 24°C（75°F）を超える環境では使用しないでください。**

この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。

警告 **安全上の重要事項**

「*危険*」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。

注：これらの注意事項を保存しておいてください。

注：このマニュアルは、製品に付属のインストレーション ガイドと併せて利用してください。詳細については、インストレーション ガイド、コンフィギュレーション ガイド、またはその他の添付資料を参照してください。

マニュアルの目的

このマニュアルでは、C7200 VSA（VPN Services Adapter）の取り付け手順および設定手順を説明します。VSA は、NPE-G2 プロセッサを搭載した Cisco 7204VXR および Cisco 7206VXR ルータに装着するダブル幅のアクセラレーション モジュールです。

VSA の部品番号は C7200-VSA(=) です。

（注） 米国の輸出規制を守り、将来的に問題を起こさないために、「暗号化に関する米国輸出規制法の遵守」（p.2-6）を参照し、具体的な重要事項を確認してください。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	内容
1	概要	VSA および VSA の LED について説明します。
2	インストレーションの準備	安全上の注意事項、必要な工具、および取り付け作業を開始する前に必要な準備について説明します。
3	VSA の取り外しおよび取り付け	サポート対象プラットフォームでの VSA の取り付け手順および取り外し手順について説明します。
4	VSA の設定	Cisco 7200VXR シリーズ ルータでの VSA の設定手順について説明します。

関連資料

ここでは、ルータおよびその機能についての関連資料を示します。当社では現在、システムごとにルータ マニュアル一式を自動的には添付していません。これらの資料はオンラインで、または Documentation CD-ROM で利用することができます。

（注） マニュアルの各国語版を利用するには、http://www.cisco.com/ にアクセスし、ページのトップで「Select a Location / Language」を選択してください。

一部のオンライン マニュアルを利用するには、シスコのユーザ登録が必要です。http://tools.cisco.com/RPF/register/register.do で登録手続きを行ってください。

- Cisco 7200VXR シリーズ ルータのハードウェア設置手順およびメンテナンス方法については、次の URL を参照してください。
  http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_series_home.html
- ポート アダプタおよびインターフェイス モジュール：
  - ポート アダプタのインストレーション コンフィギュレーション ガイドは、次の URL で利用できます。
    http://www.cisco.com/en/US/products/hw/modules/ps2033/tsd_products_support_series_home.html
  - インターフェイス モジュールおよびサービス モジュールのインストレーション コンフィギュレーション ガイドは、次の URL で利用できます。
    http://www.cisco.com/en/US/products/hw/modules/tsd_products_support_category_home.html
- Cisco IOS ソフトウェアのコンフィギュレーションおよびサポート マニュアルは、次の URL で利用できます。
  http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
  - シスコ製プラットフォームで特定の Cisco IOS 機能を実行する上で必要となる適切な Cisco IOS ソフトウェアおよびメモリ容量を確認するには、Cisco IOS Software Selection ツールを使用してください。Cisco Direct Customer に登録済みのお客様は、次の URL から Cisco IOS Software Selection ツールにアクセスできます。
    http://tools.cisco.com/ITDIT/ISTMAIN/servlet/index
  - 使用するルータに最低限必要な Cisco IOS ソフトウェアを確認するには、Software Advisor ツールを使用してください。Cisco Direct Customer に登録済みのお客様は、次の URL から Software Advisor にアクセスできます。
    http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl
- セキュリティおよび VPN のマニュアルは、次の URL で利用できます。
  http://www.cisco.com/en/US/tech/tk583/tsd_technology_support_category_home.html
- Cisco Direct Customer に登録済みのお客様は、次の URL から Technical Assistance Center（TAC）ツールおよびサポートにアクセスできます。
  http://www.cisco.com/kobayashi/support/tac/tools.shtml

マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手することができます。ここでは、シスコが提供する製品マニュアルのリリースについて説明します。

Cisco.com

シスコの最新のマニュアルは、次の URL からアクセスしてください。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

http://www.cisco.com/jp

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Product Documentation DVD は、ポータブル メディアに収容された、技術的な製品マニュアルのライブラリです。この DVD を使用すると、シスコのハードウェア製品のインストレーション、ソフトウェア製品のインストール、設定、およびコマンドに関するガイドにアクセスできます。DVD を使用することで、次の URL にあるシスコの Web サイトに収録されている、HTML 形式のマニュアルおよび一部の PDF ファイルにアクセスできます。

http://www.cisco.com/univercd/home/home.htm

Product Documentation DVD は定期的に作成および発行されます。DVD は、単独または購読契約で入手できます。Cisco.com に登録されている場合、次の URL にある Cisco Marketplace の Product Documentation Store で、Product Documentation DVD（製品番号 DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。

http://www.cisco.com/go/marketplace/docstore

マニュアルの発注方法

Cisco Marketplace にアクセスするには Cisco.com にユーザ登録されている必要があります。登録されている場合、次の URL にある Product Documentation Store からシスコ製品のマニュアルを発注できます。

http://www.cisco.com/go/marketplace/docstore

ログイン ID またはパスワードを取得されていない場合は、次の URL で登録手続きをしてください。

http://tools.cisco.com/RPF/register/register.do

シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトから、次の方法に関する情報を利用できます。

- シスコ製品における脆弱性を報告する。
- シスコ製品のセキュリティ問題に対する支援を受ける。
- シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ応答のリストが以下の URL で確認できます。

http://www.cisco.com/go/psirt

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ応答の更新をリアル タイムで確認するには、Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードに登録します。PSIRT RSS フィードの加入に関する詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- 緊急度の高い問題 — security-alert@cisco.com

  緊急度の高い問題とは、システムが激しい攻撃を受けている状態、または急を要する深刻なセキュリティの脆弱性を報告する必要がある状態を指します。それ以外の状態はすべて、緊急度の低い問題とみなされます。
- 緊急度の低い問題 — psirt@cisco.com

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

- 1 877 228-7302
- 1 408 525-6532

ヒント お客様が第三者に知られたくない情報をシスコに送信する場合、Pretty Good Privacy（PGP）または PGP と互換性のある製品（GnuPG など）を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.*x* ～ 9.*x* で暗号化された情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT と通信する際は、次の URL にある Security Vulnerability Policy ページの Contact Summary にリンクされている有効な公開鍵を使用してください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページのリンクに、現在使用されている PGP 鍵の ID があります。

PGP を所有または使用していない場合は、機密情報を送信する前に PSIRT に連絡し、他のデータ暗号化方法についてご確認ください。

Product Alert および Field Notice

シスコ製品に関する変更やアップデートは、Cisco Product Alert および Cisco Field Notice で発表されます。Cisco Product Alert および Cisco Field Notice を受信するには、Cisco.com で Product Alert ツールを使用してください。このツールでプロファイルを作成し、情報の配信を希望する製品を選択できます。

Product Alert Tool にアクセスするには、Cisco.com にユーザ登録されている必要があります（Cisco.com にユーザ登録するには、次の URL にアクセスしてください。http://tools.cisco.com/RPF/register/register.do）。登録ユーザは、次の URL からこのツールにアクセスできます。http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

テクニカル サポート

Cisco Technical Support では、評価の高い 24 時間体制のテクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、広範囲にわたるオンラインでのサポート リソースを提供しています。さらに、シスコシステムズとサービス契約を結んでいる場合は、Technical Assistance Center（TAC）のエンジニアによる電話サポートも提供されます。シスコシステムズとサービス契約を結んでいない場合は、リセラーにお問い合わせください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。この Web サイトは 24 時間ご利用いただけます。次の URL にアクセスしてください。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） テクニカル サポートにオンラインまたは電話でお問い合わせいただく前に、**Cisco Product Identification Tool** を使用して、製品のシリアル番号をご確認ください。このツールにアクセスするには、Cisco Technical Support & Documentation Web サイトの **Tools & Resources** リンク、**All Tools (A-Z)** タブをクリックし、アルファベット順の一覧から **Cisco Product Identification Tool** を選択します。このツールは、製品 ID またはモデル名、ツリー表示、または特定の製品に対する **show** コマンド出力のコピー & ペーストによる 3 つの検索オプションを提供します。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

ヒント Cisco.com での表示と検索

ブラウザで Web ページが更新されていないと思われる場合は、Ctrl キーを押しながら F5 キーを押して、Web ページを強制的に更新してください。

技術情報を検索する場合は、Cisco.com Web サイト全体ではなく、技術マニュアルに限定して検索してください。具体的には、Cisco.com ホームページで、Search ボックスの下にある **Advanced Search** リンクをクリックし、次に **Technical Support & Documentation** オプション ボタンをクリックします。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカル サポートを受けられます（ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合）。状況をご説明いただくと、TAC Service Request ツールが推奨される解決方法を提供します。これらの推奨リソースを使用しても問題が解決しない場合は、シスコの技術者が対応します。TAC Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください（運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合）。S1 および S2 の問題にはシスコの技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカル サポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋：+61 2 8446 7411
オーストラリア：1 800 805 227
EMEA：+32 2 704 55 55
米国：1 800 553 2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

http://www.cisco.com/techsupport/contacts

問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

重大度 1（S1）— 既存のネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

重大度 2（S2）— ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

重大度 3（S3）— ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

重大度 4（S4）— シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要で、業務への影響がほとんどまたはまったくない場合。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手することができます。

- Cisco Online Subscription Center は、シスコの各種 E メール ニュースレターなどの配信を申し込むことができる Web サイトです。プロファイルを作成し、配信を希望する内容を選択してください。Cisco Online Subscription Center には、次の URL からアクセスしてください。

  http://www.cisco.com/offer/subscribe

- 『*Cisco Product Quick Reference Guide*』は、手軽に使えるコンパクトなリファレンス ツールで、チャネル パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。年に 2 回更新され、シスコの最新のチャネル製品が掲載されています。『*Cisco Product Quick Reference Guide*』の発注および詳細については、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコシステムズが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーク製品およびカスタマー サポート サービスについては、次の URL にアクセスしてください。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は、ネットワークの専門家がネットワーク製品やネットワーク技術に関する質問、提案、情報をシスコの専門家および他のネットワーク専門家と共有するためのインタラクティブな Web サイトです。ディスカッションに参加するには、次の URL にアクセスしてください。

  http://www.cisco.com/discuss/networking

- 『*What's New in Cisco Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを簡単に見つけることができます。最新の『*What's New in Cisco Documentation*』には、次の URL からアクセスしてください。

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

概要

この章では、C7200 VSA（VPN Services Adapter）の概要を説明します。内容は次のとおりです。

データ暗号化の概要

ここでは、IP Security Protocol（IPSec）、Internet Key Exchange（IKE）、および Certification Authority（CA; 認証局）インターオペラビリティ機能を含め、データ暗号化について説明します。

(注)　各機能の詳細については、『*Security Configuration Guide*』の「IP Security and Encryption」の章および『*Security Command Reference* 』を参照してください。

IPSec は、Internet Engineering Task Force（IETF）が策定したネットワーク レベルのオープン スタンダードなフレームワークで、インターネットのように保護されていないネットワーク上で機密情報を安全に伝送できるようにします。IPSec には、データ認証、アンチ リプレイ サービス、および機密保護サービスがあります。

シスコでは次の Data Encryption Standard（DES; データ暗号規格）に準拠しています。

- IPSec ― IPSec は、関係するピア間でデータの機密性およびデータの完全性を保証し、データを認証する IP レイヤのオープン スタンダードなフレームワークです。IKE がローカル ポリシーに基づいてプロトコルおよびアルゴリズムのネゴシエーションを処理し、IPSec の使用する暗号鍵および認証鍵を生成します。IPSec により、ホスト間、セキュリティ ルータ間、またはセキュリティ ルータとホスト間の 1 つまたは複数のデータ フローが保護されます。
- IKE ― IKE は、Internet Security Association & Key Management Protocol（ISAKMP）フレームワーク内で、Oakley および Skeme 鍵交換を実行するハイブリッド セキュリティ プロトコルです。IKE は IPSec およびその他のプロトコルと組み合わせて使用できます。IKE は IPSec ピアを認証し、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行い、IPSec 鍵を設定します。IPSec は、IKE とともに設定することも、IKE なしで設定することもできます。
- CA ― CA インターオペラビリティは、Simple Certificate Enrollment Protocol（SCEP）および Certificate Enrollment Protocol（CEP）を使用して、IPSec 規格をサポートします。CEP によって、Cisco IOS デバイスと CA 間の通信が可能になり、Cisco IOS デバイスは CA からデジタル証明書を取得して使用できるようになります。IPSec は、CA とともに設定することも、CA なしで設定することもできます。CA は、証明書を発行できるように正しく設定されていなければなりません。詳細については、『*Security Configuration Guide*』の「Configuring Certification Authority Interoperability」の章（http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html）を参照してください。

IPSec に実装されているコンポーネント テクノロジーは、次のとおりです。

- DES および Triple DES ― DES および Triple DES（3DES）暗号化パケット データです。Cisco IOS は、3 キー Triple DES および DES-CBC with Explicit IV を実装します。Cipher Block Chaining（CBC; 暗号ブロック連鎖）は、暗号化の開始に初期ベクトル（IV）が必要です。IV は IPSec パケット内に明示的に指定されます。
- AES ― Advanced Encryption Standard（高度暗号化規格）。米国政府およびその他の諸国の組織が使用している次世代の対称暗号化アルゴリズムです。
- MD5（HMAC バリアント）― Message Digest 5（MD5）はハッシュ アルゴリズムです。HMAC はデータの認証に使用するキー付きハッシュ バリアントです。
- SHA（HMAC バリアント）― Secure Hash Algorithm（SHA）はハッシュ アルゴリズムです。HMAC はデータの認証に使用するキー付きハッシュ バリアントです。
- RSA 署名および RSA 暗号化 nonce ― RSA は Ron Rivest、Adi Shamir、および Leonard Adleman によって開発された公開鍵暗号システムです。RSA 暗号化 nonce は否認を提供し、RSA 署名を使用すると否認防止が可能になります。

IPSec は Cisco IOS ソフトウェア上で、次のような他の規格もサポートします。

- AH ― Authentication Header（認証ヘッダー）。AH は、データ認証およびオプションのアンチ リプレイ サービスを行うセキュリティ プロトコルです。

  AH プロトコルはさまざまな認証アルゴリズムを使用しますが、Cisco IOS ソフトウェアで実装している認証アルゴリズムは、必須の MD5 および SHA（HMAC バリアント）です。AH プロトコルはアンチ リプレイ サービスを提供します。

- ESP ― Encapsulating Security Payload。ESP は、データ プライバシ サービス、オプションのデータ認証、およびアンチ リプレイ サービスを提供するセキュリティ プロトコルです。ESP は保護対象のデータをカプセル化します。ESP プロトコルは、さまざまな暗号化アルゴリズムと（オプションで）さまざまな認証アルゴリズムを使用します。Cisco IOS ソフトウェアは、暗号化アルゴリズムとして必須の 56 ビット DES-CBC with Explicit IV または Triple DES を実装します。また、認証アルゴリズムとして MD5 または SHA（HMAC バリアント）を実装します。最新の ESP プロトコルでは、アンチ リプレイ サービスを提供します。

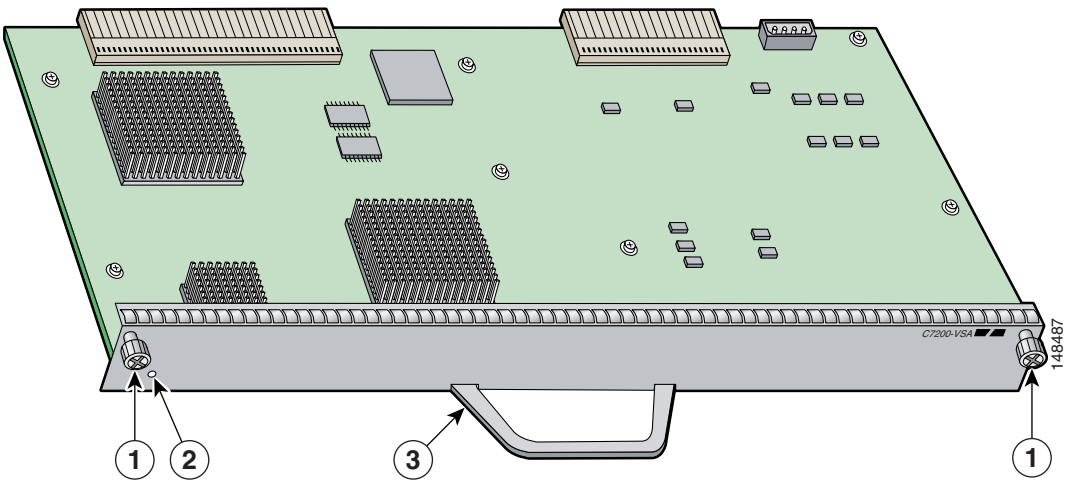
VSA の概要

C7200 VSA（VPN Services Adapter）は、NPE-G2 プロセッサを搭載した Cisco 7204VXR および Cisco 7206VXR ルータの I/O スロットに装着する全ボード幅のサービス アダプタです（図 1-1 を参照）。

（注） C7200 VSA は、NPE-G2 プロセッサを搭載した Cisco 7200VXR でのみサポートされます。

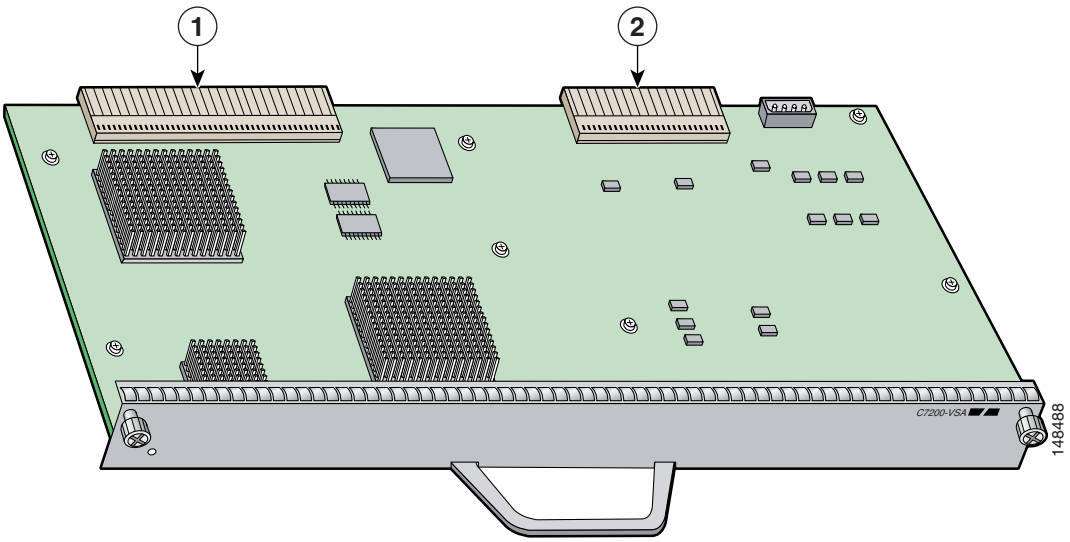
VSA は AES、DES、および Triple DES のハードウェア アクセラレーションを実行し、サイト間およびリモート アクセス IPSec VPN サービスのパフォーマンスを向上させます。Cisco C7200 VSA ソリューションは QoS（Quality of Service）、マルチキャストおよびマルチプロトコル トラフィック、統合型 LAN/WAN メディアの幅広いサポートを提供します。

図 1-1　VSA モジュール ― 前面



1	ネジ	**3**	ハンドル
2	ステータス LED		

図 1-2　VSA モジュール — 背面コネクタ



1	ホスト IO バスおよび PCI-X バス	**2**	電源

VSA は、さまざまな暗号化機能にハードウェア アクセラレーション サポートを提供します。

- ハードウェア上での 128/192/256 ビット AES
- 56 ビット キーの DES 標準モード：CBC
- 最大 900 Mbps の暗号化スループット（300 バイト パケット、1,000 トンネルの場合）のパフォーマンス
- 5,000 トンネル（DES/3DES/AES に対応）
- SHA-1 および MD5 ハッシュ アルゴリズム
- Rivest, Shamir, Adelman（RSA）公開鍵アルゴリズム
- Diffie-Hellman グループ 1、2、5

必要なハードウェア

C7200 VSA が正常に動作するために必要なハードウェアは次のとおりです。

- C7200 VSA は、Cisco 7204VXR または Cisco 7206VXR ルータに搭載された Cisco NPE-G2 プロセッサと互換性があります。
- ROMmon の要件 — 12.4(4r)XD5
- I/O FPGA の要件 — 0x25（10 進 0.37）
- VSA FPGA の要件 — 0x13（10 進 0.19）

機能

ここでは、VSA の機能について表 1-1 で説明します。

表 1-1　VSA の機能

機能	説明 / 利点
スループット[1]	最大 900 Mbps 暗号化スループットのパフォーマンス（Cisco 7204VXR および Cisco 7206VXR ルータで 3DES または AES を使用）
IPSec で保護されるトンネル数[2]	最大 5,000 トンネル[3]
毎秒トンネル数	注：詳細なテストの実施後、更新予定
ハードウェアベースの暗号化	データ保護：IPSec DES、3DES、および AES 認証：RSA および Diffie-Hellman データ整合性：SHA-1 および MD5
VPN トンネリング	IPSec トンネル モード：IPSec による Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）および Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）保護
サポートされる最低限の Cisco IOS ソフトウェア リリース	12.4(4)XD3 fc2 以降の 12.4XD リリース 12.4(11)T 以降の 12.4T リリース
サポートする規格	IPSec/IKE：RFC 2401 ～ 2411、2451

1. IPSec 3DES HMAC-SHA1 を使用し、1,400 バイト パケットで測定
2. サポートされるトンネル数は、搭載メモリの合計によって異なります。
3. NPE-G2 に最低 1 GB のメモリが必要です。

パフォーマンス

表 1-2 に VSA のパフォーマンス情報を示します。

表 1-2　VSA のパフォーマンス

Cisco ルータ	スループット[1 2]	内容
Cisco 7200VXR シリーズ ルータ（NPE-G2 プロセッサを搭載）	最大 900 Mbps 暗号化スループットのパフォーマンス	Cisco IOS リリース：12.4(4)XD3 fc2 7200VXR/NPE-G2/VSA、1GB のシステム メモリ 3DES/HMAC-SHA または AES/HMAC-SHA、事前共有、IKE キープアライブ設定なし

1. IPSec 3DES または AES HMAC-SHA-1 を使用し、1,400 バイト パケットで測定。パフォーマンスはモジュール数、帯域幅、トラフィック量、Cisco IOS ソフトウェア リリースなどによって変化します。
2. Cisco 12.4(4)XD3 fc2 イメージを使用。パフォーマンスは Cisco IOS ソフトウェア リリースによって変化します。

サポート対象の規格、MIB、および RFC

ここでは、VSA でサポートされる規格、Management Information Base（MIB; 管理情報ベース）、および Request for Comment（RFC; コメント要求）について説明します。RFC には、サポートされるインターネット プロトコル スイートについての情報が記載されています。

規格

- IPSec/IKE：RFC 2401 ～ 2411、2451

MIB

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB

サポート対象 MIB のプラットフォーム別リストおよび Cisco IOS リリース別リストを入手する場合、または MIB モジュールをダウンロードする場合には、次の URL から Cisco.com の Cisco MIB Web サイトにアクセスしてください。

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

RFC

- IPSec/IKE：RFC 2401 ～ 2411、2451

VSA のイネーブル / ディセーブル化

ここで説明する内容は次のとおりです。

VSA 暗号カードは 活性挿抜（Online Insertion and Removal; OIR）に対応していません。VSA はシステムの初期化時にのみ起動します。システムがすでに稼働している状態で VSA を取り付けても、VSA は動作しません。CLI のディセーブル コマンドで、VSA をシャットダウンできます。CLI のディセーブル コマンドを実行すると、VSA を取り外す準備が整います。

稼働中の VSA のディセーブル化

VSA を取り外すときは、事前にインターフェイスをシャットダウンして、取り外す VSA にトラフィックが流れないようにすることを推奨します。ポート経由でトラフィックが流れているときに VSA を取り外すと、システム障害を引き起こす可能性があります。

注意　CLI コマンドを入力せずに VSA を取り外すと、VSA が故障する可能性があります。

C7200 VSA をディセーブルにするには、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	`no crypto engine [slot | accelerator] 0`	C7200 VSA をディセーブルにします。
ステップ 2	`crypto engine [slot | accelerator] 0`	ディセーブルになった C7200 VSA をイネーブルにします。 **（注）** 詳細については 表 1-5 を参照してください。

イネーブル化 / ディセーブル化方式

ここでは、OIR に対応しない VSA がどのように動作するかを説明します。

表 1-3 に、電源投入後または reload コマンドの入力後にシステムがブートするときの動作を示します。

表 1-4 に、システム稼働時の動作を示します。

表 1-5 に、**crypto engine** コマンドを入力したときの動作を示します。

表 1-3　電源投入後または reload コマンド入力後のシステム ブート時

条件	システムの初期化
VSA 搭載時	VSA サブシステムが自動的に起動し、初期化を実行します。VSA 以外の暗号エンジンはディセーブルになります。
VSA 非搭載時	VSA サブシステムは初期化せず、システムは他の暗号エンジン（存在する場合）を使用します。

表 1-4　システム稼働時

条件	システムの設定
VSA の取り付け	VSA の電源がオフになります。VSA を起動するには、システムのリロードまたはリセットを実行する必要があります。
CLI による VSA のイネーブル化	サポートされていません。
CLI による VSA のディセーブル化	**Hw-module slot 0 shutdown** ― サポートされていません。 **[no] crypto engine [slot | accelerator] 0** ― 表 1-5 を参照してください。
VSA の取り外し	ハードウェアの故障を防ぐため、カードを取り外す前に、CLI のディセーブル コマンドを入力する必要があります（表 1-5 を参照）。

表 1-5　crypto engine コマンド

コマンド	VSA の動作
Crypto engine slot 0 **Crypto engine accelerator 0** **（注）** VSA はスロット 0（I/O コントローラ スロット）にのみ搭載可能です。	このコマンドにより VSA が起動し、システムに暗号エンジンとして登録されます。 この設定を実行し、VSA が現在ディセーブルになっている場合は、システムをリロードまたはリセットして VSA を起動します。 **（注）** 引き続き現在の暗号エンジンが動作し、次のシステム リブート後に VSA が動作を引き継ぎます。
No crypto engine slot 0 **No crypto engine accelerator 0**	これらの CLI コマンドは VSA をディセーブルにします。この設定を解除し、システムのリロードまたはリセットを実行するまで、VSA はディセーブルの状態を続けます。

LED

VSA には 1 つの LED があります（図 1-3 を参照）。

図 1-3　VSA の LED

表 1-6　VSA の LED

カラー	状態	機能
カラーなし	消灯	VSA はディセーブルです。
グリーン	点灯	VSA は通電状態で動作可能です。
オレンジ	点灯	VSA が起動中か、またはエラーが発生したことを表します。
イエロー	起動中	VSA が起動中ですが、ソフトウェアの初期化はまだ開始されていません。

ENABLE LED は、次の条件が満たされた場合に点灯します。

- VSA がバックプレーンに正しく接続されていて、電力が供給されている。
- システム バスが VSA を認識している。

いずれかの条件が満たされていない場合、またはその他の理由でルータを初期化できなかった場合、ENABLE LED は点灯しません。

コネクタ

VSA のコネクタについては、図 1-2 を参照してください。

スロット位置

ここで説明する内容は次のとおりです。

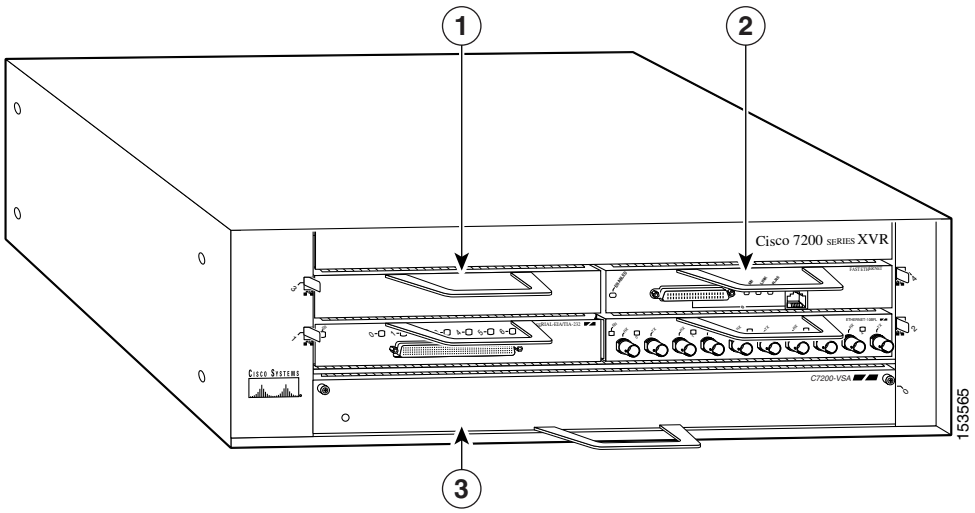
Cisco 7204VXR ルータのスロット番号については、図 1-4 を参照してください。

Cisco 7206VXR ルータのスロット番号については、図 1-5 を参照してください。

Cisco 7204VXR ルータ

VSA は Cisco 7204VXR ルータの I/O コントローラ ポートに搭載できます（図 1-4 の 3 を参照）。

図 1-4　Cisco 7204VXR ルータ — 前面

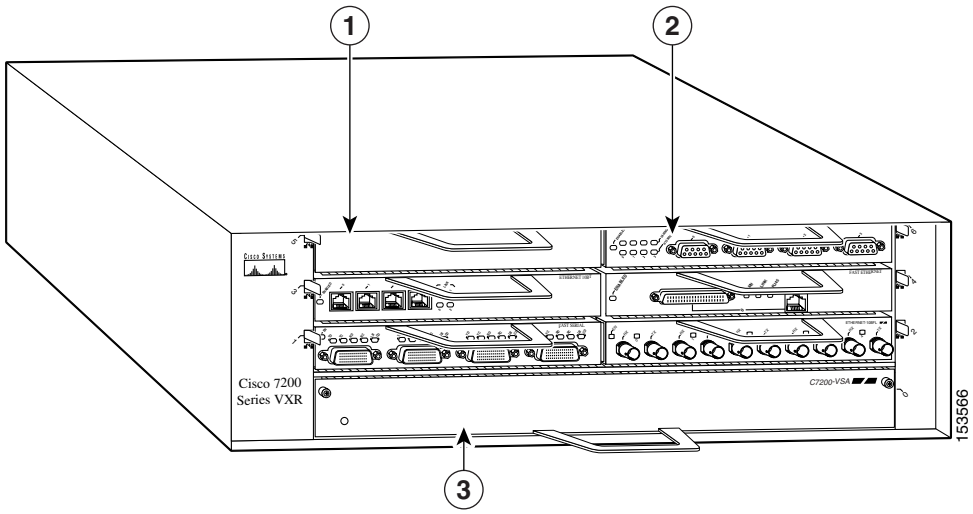


1	ポート アダプタ	3	I/O コントローラ スロットに搭載した VSA
2	ポート アダプタ レバー		

Cisco 7206VXR ルータ

VSA は Cisco 7206VXR ルータの I/O コントローラ ポートに搭載できます（図 1-5 の 3 を参照）。

図 1-5　Cisco 7206VXR ― 前面



1	ブランク ポート アダプタ	**3**	I/O コントローラ スロットに搭載した VSA
2	ポート アダプタ		

インストレーションの準備

この章では、C7200 VSA（VPN Services Adapter）を取り付けるために必要な工具、安全上の注意事項、および設置場所の準備について説明します。この章で説明する内容は、次のとおりです。

必要な工具および機器

VSA を取り付けるには、次の工具および部品が必要です。追加で必要な機器がある場合には、購入された代理店に発注方法をお問い合わせください。

- VSA
- No. 2 プラス ドライバ
- ESD（静電気放電）防止用器具、またはすべてのアップグレード キット、Field-Replaceable Unit（FRU; 現場交換可能ユニット）、およびスペアに付属の使い捨て静電気防止用リスト ストラップ
- 静電気防止用マット
- 静電気防止用容器

ハードウェアおよびソフトウェアの要件

ここでは、VSA を使用するために最低限必要なハードウェアおよびソフトウェアについて説明します。

ソフトウェア要件

表 2-1 に、サポート対象のルータまたはスイッチ プラットフォームで VSA を使用するために最低限必要な、推奨する Cisco IOS ソフトウェア リリースを示します。**show version** コマンドを使用すると、現在ロードされて稼働しているシステム ソフトウェア バージョンが表示されます。

表 2-1　VSA のソフトウェア要件

プラットフォーム	推奨する最低限の Cisco IOS リリース
Cisco 7204VXR Cisco 7206VXR	12.4(4)XD3 fc2

シスコでは、ルータに搭載されているハードウェアに最低限必要な Cisco IOS ソフトウェアを確認できるように、Cisco.com に Software Advisor ツールを用意しています。Cisco Direct Customer に登録済みのユーザは、次の URL から Software Advisor にアクセスできます（http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl）。このツールは、システムで使用するモジュール間の互換性について確認するものではなく、個々のハードウェア モジュールまたはコンポーネントに最低限必要となる Cisco IOS ソフトウェアを確認できます。

（注） このツールを利用するには、Cisco.com のログイン アカウントが必要です。

ハードウェア要件

VSA が正常に動作するために必要なハードウェアは次のとおりです。

- VSA は、Cisco 7204VXR または Cisco 7206VXR ルータに搭載された Cisco NPE-G2 プロセッサと互換性があります。

  Cisco NPE-G2 は Cisco 7204VXR および 7206VXR 用の最新のルーティング エンジンであり、Network Processing Engine（NPE; ネットワーク処理エンジン）ファミリで最高のパフォーマンスとスケーラビリティを実現します。
- ROMmon の要件 — 12.4(4r)XD5
- I/O FPGA の要件 — 0x25（10 進 0.37）
- VSA FPGA の要件 — 0x13（10 進 0.19）

制限事項

VSA には次のような制限があります。

- VSA は、同じルータに搭載された他の ISA または VAM/VAM2/VAM2+ 暗号カードとは連携しません。NPE-G2 プロセッサを搭載した Cisco 7200VXR シリーズ ルータで VSA がアクティブのときは、VAM/VAM2/VAM2+ 暗号カードはディセーブルになります。
- NPE-G2 プロセッサを搭載した Cisco 7200VXR シリーズ ルータで使用できる VSA カードは 1 枚だけです。

（注） NPE-G2 プロセッサを搭載した Cisco 7200VXR シリーズ ルータだけがサポートされます。

- VSA モジュールは活性挿抜（Online Insertion and Removal; OIR）に対応していません。詳細については、「VSA のイネーブル / ディセーブル化」（p.1-7）を参照してください。
- **show access-list** コマンドを入力するとき、クリプト マップ ACL に関するパケット カウント別の詳細情報は表示されません。

  VSA がパケットを処理しているかどうかを確認するには、**show crypto ipsec sa** および **show crypto engine accelerator statistics 0** コマンドの出力など、別のカウンタを使用してください。
- 1024 のアンチ リプレイ ウィンドウ サイズはサポートされません。

OIR

VSA は Cisco 7200VXR シリーズ シャーシの I/O コントローラ スロットに搭載します。VSA 暗号カードは OIR に対応していません。VSA はシステムの初期化時にのみ起動します。システムがすでに稼働している状態で VSA を取り付けても、VSA は動作しません。CLI のディセーブル コマンドで、VSA をシャットダウンできます（「VSA のイネーブル / ディセーブル化」[p.1-7] を参照）。CLI のディセーブル コマンドを実行すると、VSA を取り外す準備が整います。

注意　CLI コマンドを入力せずに VSA を取り外すと、VSA が故障する可能性があります。

VSA を取り外すときは、事前にインターフェイスをシャットダウンして、取り外す VSA にトラフィックが流れないようにすることを推奨します。ポート経由でトラフィックが流れているときに VSA を取り外すと、システム障害を引き起こす可能性があります。

OIR の詳細については、「VSA のイネーブル / ディセーブル化」（p.1-7）を参照してください。

安全に関する注意事項

ここでは、電源または電話配線に接続する機器を取り扱う際に従うべき安全上の注意事項を示します。ここで説明する内容は次のとおりです。

安全上の警告

誤って行うと危険が生じる可能性のある操作については、安全上の警告が記載されています。各警告文に、警告を表す記号が記されています。

警告　**この製品を廃棄処分する際には、各国の法律または規制に従って取り扱ってください。**

システムの稼働中は、バックプレーンに危険な電圧またはエネルギーがかかっています。取り扱いには十分注意してください。

ブランクの前面プレートおよびカバー パネルには、3 つの重要な機能があります。シャーシ内の危険な電圧および電流による感電を防ぐこと、他の装置への EMI（電磁波干渉）の影響を防ぐこと、およびシャーシ内の空気の流れを適切な状態に保つことです。必ずすべてのカード、前面プレート、前面カバー、および背面カバーを取り付けた状態でシステムを運用してください。

電気機器を扱う際の注意事項

電気機器を取り扱う際には、次の基本的な注意事項に従ってください。

- シャーシ内部の作業を行う前に、室内の緊急電源遮断スイッチがどこにあるかを確認しておきます。
- シャーシを移動するときは、事前にすべての電源コードおよび外付けケーブルを外してください。危険を伴う作業は 1 人では行わないでください。
- 回路の電源が切断されていると思い込まず、必ず確認してください。
- 人身事故や装置障害を引き起こす可能性のある作業は行わないでください。床が濡れていないか、アースされていない電源延長コードや保護アースの不備がないかどうか、作業場所の安全を十分に確認してください。

静電破壊の防止

ESD（静電放電）により、装置や電子回路が損傷を受けることがあります（静電破壊）。静電破壊は電子部品の取り扱いが不適切な場合に発生し、故障または間欠的な障害をもたらします。ポート アダプタおよびプロセッサ モジュールには、金属フレームに固定されたプリント基板があります。EMI（電磁波干渉）シールドおよびコネクタは、フレームを構成する部品です。基板は金属フレームによって ESD から保護されていますが、取り扱いの際には、必ず静電気防止用リスト ストラップを着用してください。

静電破壊を防ぐために、次の注意事項に従ってください。

- 静電気防止用リストまたはアンクル ストラップを肌に密着させて着用してください。
- シャーシ フレームの塗装されていない面にストラップのクリップを取り付けてください。
- コンポーネントを取り付けるときは、イジェクト レバーまたは非脱落型ネジを使用して、バックプレーンまたはミッドプレーンにバス コネクタを適切に固定してください。イジェクト レバーや非脱落型ネジは、基板の脱落を防ぐだけでなく、システムに適切なアースを提供し、バス コネクタを確実に固定させるために必要です。
- コンポーネントを取り外すときは、イジェクト レバーまたは非脱落型ネジを使用して、バックプレーンまたはミッドプレーンからバス コネクタを取り外してください。
- フレームを取り扱うときは、ハンドルまたは端の部分だけを持ち、プリント基板またはコネクタには手を触れないようにしてください。
- 取り外した基板はコンポーネント面を上向きにして、静電気防止用シートに置くか、静電気防止用容器に保管します。コンポーネントを返却する場合には、取り外したあと、基板をただちに静電気防止用容器に入れてください。
- プリント基板と衣服が接触しないように注意してください。リスト ストラップは身体の静電気からコンポーネントを保護するだけです。衣服の静電気が、静電破壊の原因になることがあります。
- 金属フレームからプリント基板を絶対に取り外さないでください。
- 安全のために、静電気防止用ストラップの抵抗値を定期的にチェックしてください。抵抗値は 1 ～ 10 Mohm でなければなりません。

暗号化に関する米国輸出規制法の遵守

この製品は暗号化を実行し、米国政府の輸出規制を受けます。物理的または電子的手段によってこの製品を米国から輸出する場合は、米国商務省輸出管理局の管轄である輸出管理規制を遵守する必要があります。詳細については、http://www.bxa.doc.gov/ を参照してください。

一部の「強力」な暗号化機能を米国外部に輸出できるかどうかは、輸出先、エンドユーザ、および最終利用目的によって決まります。シスコの適格製品、輸出先、エンドユーザ、および最終利用目的の詳細については、http://www.cisco.com/wwl/export/encrypt.html を参照してください。

輸出に先立ち、現地の法律を確認し、必要に応じて輸入および利用条件を調べてください。各国の暗号化関連の法律については、非公式な情報源として、
http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm を参照してください。

CHAPTER 3

VSA の取り外しおよび取り付け

この章では、サポート対象プラットフォームから C7200 VSA（VPN Services Adapter）を取り外す方法、および VSA を新しく取り付けたり交換したりする方法について説明します。

取り付け作業を始める前に、第 2 章「インストレーションの準備」を参照し、取り付けに必要な部品および工具の一覧を確認してください。

この章で説明する内容は、次のとおりです。

(注) システムで I/O コントローラまたは VSA を使用しない場合は、空のスロットでエアフローを確保する必要があります。

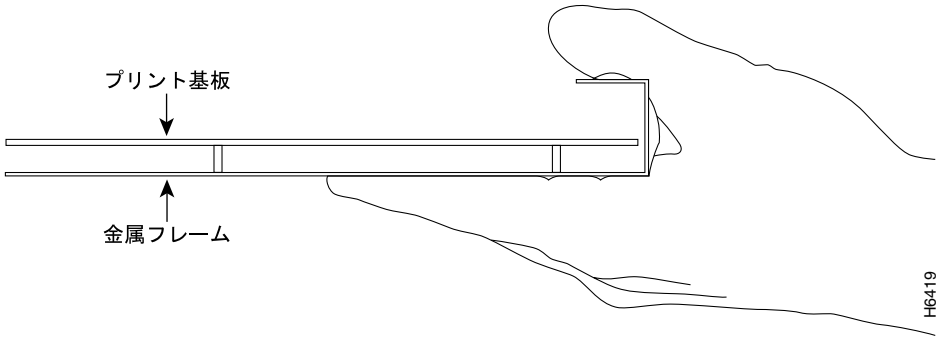
VSA 回路基盤は ESD（静電気放電）による損傷を受けやすい製品です。

VSA の取り扱い

VSA は金属製フレームに取り付けられたダブル幅の回路基盤です（図 3-1 を参照）。

注意　VSA を持つときは必ずフレームの端とハンドルを持ち、VSA コンポーネントまたはコネクタ ピンには触れないでください（図 3-1 を参照）。

図 3-1　VSA の取り扱い



OIR

VSA は Cisco 7200VXR シリーズ シャーシの I/O コントローラ スロットに搭載します。VSA 暗号カードは活性挿抜（Online Insertion and Removal; OIR）に対応していません。VSA はシステムの初期化時にのみ起動します。システムがすでに稼働している状態で VSA を取り付けても、VSA は動作しません。CLI のディセーブル コマンドで、VSA をシャットダウンできます（「VSA のイネーブル / ディセーブル化」[p.1-7] を参照）。CLI のディセーブル コマンドを実行すると、VSA を取り外す準備が整います。

注意　CLI コマンドを入力せずに VSA を取り外すと、VSA が故障する可能性があります。

OIR の詳細については、「VSA のイネーブル / ディセーブル化」（p.1-7）を参照してください。

警告および注意事項

VSA の取り付けまたは取り外しを行うときは、次の警告および注意事項に従ってください。

警告　ブランクの前面プレートおよびカバー パネルには、3 つの重要な機能があります。シャーシ内の危険な電圧および電流による感電を防ぐこと、他の装置への EMI（電磁波干渉）の影響を防ぐこと、およびシャーシ内の空気の流れを適切な状態に保つことです。必ずすべてのカード、前面プレート、前面カバー、および背面カバーを取り付けた状態でシステムを運用してください。

保護カバーは製品に不可欠な部品です。保護カバーを取り付けない状態で装置を稼働させないでください。カバーを取り付けずに装置を稼働させると、安全性の認定が無効になり、発火または感電の危険が生じます。

警告　電源に接続されている装置を扱う場合は、事前に指輪、ネックレス、腕時計などの装身具を外しておいてください。これらの金属が電源やアースに接触すると、金属が過熱して大やけどをしたり、金属類が端子に焼き付くことがあります。

手または指で電源装置ベイに触れないでください。システムの稼働中は、電源バックプレーンに高電圧がかかっています。

VSA の取り外しおよび取り付け

ここでは、VSA の取り外しおよび取り付け手順について説明します。

警告　**以下の手順の実行中は、ESD による損傷を防止するために、必ず静電気防止用リスト ストラップを着用してください。プラットフォームによっては、リスト ストラップを取り付ける ESD コネクタが付いています。手または金属製の工具でミッドプレーンまたはバックプレーンに直接触れないでください。感電する危険性があります。**

（注）　ルータの電源をオフにしたら、少なくとも 30 秒間待ってから電源を再投入してください。

Cisco 7200VXR シリーズ ルータでの VSA の取り外しおよび取り付け手順は、次のとおりです。

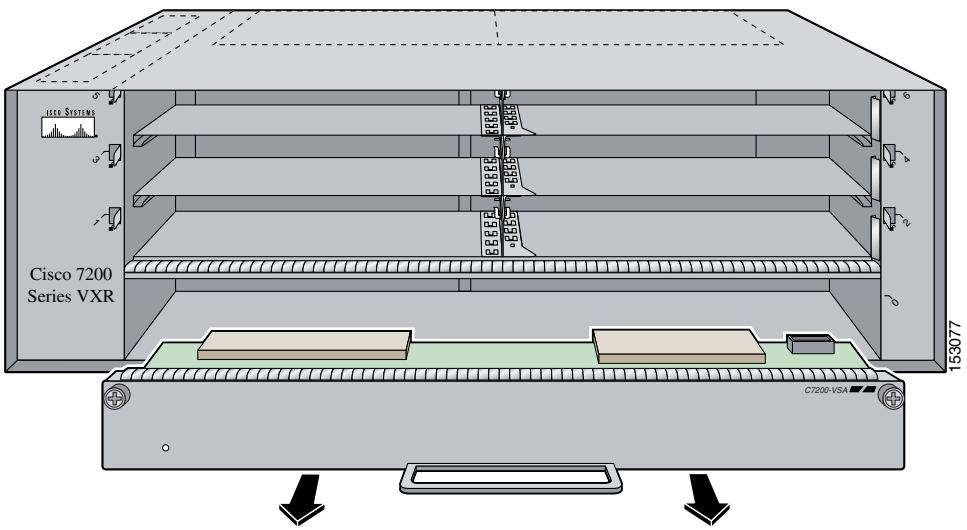
ステップ 1　電源スイッチをオフの位置にしたあと、電源コードを取り外します（Cisco 7200VXR シリーズ ルータの場合は任意です。前述の警告および注意事項 [p.3-3] を参照してください）。

ステップ 2　静電気防止用リスト ストラップを手首に装着し、ストラップの機器側をシャーシの塗装されていない面に接続します。

ステップ 3　スロットに VSA を固定しているネジを取り外します。

ステップ 4　VSA のハンドルを持ち、ルータから VSA を引き出します（図 3-2 を参照）。

図 3-2　Cisco 7206VXR シャーシ ― I/O コントローラ スロットからの VSA の取り外し



ステップ 5　新しい VSA のフレームを、I/O コントローラ スロットの上下のエッジに慎重に合わせます。

注意　I/O コントローラ スロットの上下のエッジ間でフレームが引っかからないように、また、VSA 背面のエッジ コネクタが I/O コントローラ スロット奥のコネクタときちんとかみ合うように、フレームの位置が正しいかどうかを確認してください（図 3-2 を参照）。

ステップ 6　新しい VSA を I/O コントローラ スロットに差し込み、ルータのミッドプレーンに装着します。

注意　VSA のコンポーネントがシステム基盤に接触しないように注意してください。VSA が損傷することがあります。

VSA を取り外すだけで、新しい VSA を取り付けない場合は、内部コンポーネントに冷気が行き渡るようにするため、ブランク サービス アダプタ フィラーを空の I/O コントローラ スロットに取り付けておきます。

ステップ 7　電源コードを接続し、サポート ブラケット（使用している場合）にコードを通します。

ステップ 8　電源スイッチをオンの位置にして、ルータに電源を投入します。

Cisco 7200VXR シリーズ ルータでの VSA の取り外しおよび取り付け手順は、これで完了です。

CHAPTER 4

VSA の設定

この章では、C7200-VSA（VPN Services Adapter）を設定する際に必要な情報および手順を示します。この章で説明する内容は、次のとおりです。

概要

I/O コントローラ スロットの VSA は、NPE-G2 プロセッサを搭載した Cisco 7204VXR または Cisco 7206VXR ルータの I/O コントローラ ポートに暗号化サービスを提供します。IP Security Protocol（IPSec）が設定済みのルータに VSA を搭載すると、VSA は暗号化サービスを自動的に実行します。

（注） Cisco 7204VXR および 7206VXR ルータは 1 つの VSA のみをサポートします。

VSA 上で設定するためのインターフェイスはありません。

ここでは、暗号化および IPSec トンネリング サービスを実施するための基本的な設定に限定して説明します。IPSec、Internet Key Exchange（IKE）、および Certification Authority（CA; 認証局）の設定の詳細については、『*Security Configuration Guide*』の「IP Security and Encryption」の章、および『*Security Command Reference*』を参照してください。

設定作業

VSA は起動した時点で動作可能な状態であり、コンフィギュレーション コマンドは不要です。ただし、VSA で暗号化サービスを提供する場合には、ここで説明する手順を行う必要があります。

- EXEC コマンド インタープリタの使用（p.4-3）（必須）
- IKE ポリシーの設定（p.4-3）（必須）
- トランスフォーム セットの設定（p.4-5）（必須）
- IPSec の設定（p.4-9）（必須）
- VSA のディセーブル化（任意）（p.4-5）（任意）
- IKE および IPSec の設定の確認（p.4-16）（任意）
- IPSec の設定例（p.4-20）（任意）

（注） スタティック クリプト マップの設定、ダイナミック クリプト マップの作成、ダイナミック クリプト マップのスタティック クリプト マップへの追加ができます。次の URL にあるオンライン マニュアルで設定例およびテクニカル ノートを参照してください。
http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod_configuration_examples_list.html

任意で、CA インターオペラビリティを設定できます（『*Security Configuration Guide*』の「Configuring Certification Authority Interoperability」の章を参照）。

EXEC コマンド インタープリタの使用

EXEC（別名イネーブル モード）というソフトウェア コマンド インタープリタを使用して、ルータのコンフィギュレーションを変更します。**configure** コマンドを使用して新しいインターフェイスを設定する、またはインターフェイスの従来の設定を変更するには、その前に **enable** コマンドで EXEC コマンド インタープリタのイネーブル レベルを開始する必要があります。パスワードが設定されている場合は、パスワードを要求するプロンプトが表示されます。

イネーブル レベルのシステム プロンプトは、かぎカッコ（>）ではなくポンド記号（#）で終わります。コンソール端末から、次の手順でイネーブル レベルを開始します。

ステップ 1　ユーザ レベルの EXEC プロンプトから、**enable** コマンドを入力します。次のように、イネーブル パスワードが要求されます。

```
Router> enable

Password:
```

ステップ 2　パスワードを入力します。パスワードでは大文字と小文字が区別されます。機密保護のために、パスワードは表示されません。
有効なパスワードを入力すると、イネーブル レベルのシステム プロンプト（#）が表示されます。

```
Router#
```

EXEC コマンド インタープリタのイネーブル レベルを開始する手順は、これで完了です。

IKE ポリシーの設定

パラメータ値を指定しない場合は、デフォルト値が使用されます。デフォルト値については、『*Security Command Reference*』の「IP Security and Encryption」の章を参照してください。

IKE ポリシーを設定するには、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto isakmp policy priority`	IKE ポリシーを定義し、Internet Security Association Key Management Protocol（ISAKMP）ポリシー コンフィギュレーション（config-isakmp）モードを開始します。
ステップ 2	`Router(config-isakmp)# encryption {des | 3des | aes | aes 128 | aes 192 | aes 256}`	IKE ポリシーの暗号化アルゴリズムを指定します。 • **des** ― 56 ビット Data Encryption Standard（DES; データ暗号化規格）を暗号化アルゴリズムとして指定します。 • **3des** ― 168 ビット DES を暗号化アルゴリズムとして指定します。 • **aes** ― 128 ビット Advanced Encryption Standard（AES; 高度暗号化規格）を暗号化アルゴリズムとして指定します。 • **aes 128** ― 128 ビット AES を暗号化アルゴリズムとして指定します。 • **aes 192** ― 192 ビット AES を暗号化アルゴリズムとして指定します。 • **aes 256** ― 256 ビット AES を暗号化アルゴリズムとして指定します。
ステップ 3	`Router(config-isakmp)# authentication {rsa-sig | rsa-encr | pre-share}`	（任意）IKE ポリシーの認証方式を指定します。 • **rsa-sig** ― Rivest, Shamir, and Adelman（RSA）シグニチャを認証方式として指定します。 • **rsa-encr** ― RSA 暗号化 nonce を認証方式として指定します。 • **pre-share** ― 事前共有鍵を認証方式として指定します。 **（注）** このコマンドをイネーブルにしない場合、デフォルト値（***rsa-sig***）が使用されます。
ステップ 4	`Router(config-isakmp)# lifetime seconds`	（任意）IKE Security Association（SA; セキュリティ アソシエーション）のライフタイムを指定します。 *seconds* ― 各 SA が期限切れになるまでの秒数。60 ～ 86,400 秒の範囲の整数を使用します。 **（注）** このコマンドをイネーブルにしない場合、デフォルト値（86,400 秒 [1 日]）が使用されます。
ステップ 5	`Router(config-isakmp)# hash {sha | md5}`	（任意）IKE ポリシーのハッシュ アルゴリズムを指定します。 • **sha** ― SHA-1（HMAC バリアント）をハッシュ アルゴリズムとして指定します。 • **md5** ― MD5（HMAC バリアント）をハッシュ アルゴリズムとして指定します。 **（注）** このコマンドをイネーブルにしない場合、デフォルト値（**sha**）が使用されます。

	コマンド	目的
ステップ 6	`Router(config-isakmp)# group {1 | 2 | 5}`	（任意）IKE ポリシーの Diffie-Hellman（DH）グループ識別子を指定します。 **1** ― 768 ビット DH グループを指定します。 **2** ― 1,024 ビット DH グループを指定します。 ***5*** ― 1,536 ビット DH グループを指定します。 **（注）** このコマンドをイネーブルにしない場合、デフォルト値（768 ビット）が使用されます。

IKE ポリシー作成の詳細については、『*Security Configuration Guide*』の「Configuring Internet Key Exchange Security Protocol」の章を参照してください。

VSA のディセーブル化（任意）

VSA はデフォルトでイネーブルに設定されています。

VSA をディセーブルにするには、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	**no crypto engine** [**slot** | **accelerator**] **0** **（注）** VSA はスロット 0 にのみ搭載可能です。	VSA をディセーブルにします。
ステップ 2	**crypto engine** [**slot** | **accelerator**] **0**	次にシステムをリブートする時点で、VSA がイネーブルになります。

これで、VSA をディセーブルにして、次回のシステム リブートで VSA をイネーブルにするように準備する手順は完了です。

トランスフォーム セットの設定

トランスフォーム セット設定の詳細については、『*Advanced Encryption Standard (AES)*』フィーチャ モジュールを参照してください。

ここで説明する内容は次のとおりです。

- トランスフォーム セットの定義
- IPSec プロトコル：AH および ESP
- 適切なトランスフォームの選択
- クリプト トランスフォーム コンフィギュレーション モード
- 既存のトランスフォームの変更
- トランスフォームの例

トランスフォーム セットは、IPSec で保護するトラフィックに対して適用する設定（セキュリティ プロトコル、アルゴリズムなど）の適切な組み合わせです。IPSec SA のネゴシエーションを行うとき、特定のデータ フローを保護するために特定のトランスフォーム セットを使用することがピア間で合意されます。

トランスフォーム セットの定義

トランスフォーム セットは、セキュリティ プロトコルとアルゴリズムの組み合わせです。IPSec SA のネゴシエーションを行うとき、特定のデータ フローを保護するために特定のトランスフォーム セットを使用することがピア間で合意されます。

トランスフォーム セットを定義するには、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

（注） 下記ステップ 4 の **clear** コマンドは、EXEC（イネーブル）モードで実行されます（詳細については「EXEC コマンド インタープリタの使用」[p.4-3] を参照してください）。

	コマンド	目的
ステップ 1	`Router(config)# crypto ipsec transform-set` *transform-set-name transform1* [*transform2* [*transform3*]]	トランスフォーム セットを定義し、クリプト トランスフォーム コンフィギュレーション モードを開始します。 • *transform-set-name* ― 作成（または変更）するトランスフォーム セットの名前を指定します。 • *transform1* [*transform2* [*transform3*] [*transform4*]] ― IPSec セキュリティ プロトコルおよびアルゴリズムを定義します。指定できるトランスフォーム値については、表 4-1 を参照してください。
ステップ 2	`Router(cfg-crypto-tran)# mode [tunnel | transport]`	（任意）トランスフォーム セットに関連付けるモードを変更します。このモード設定は、送信元/宛先アドレスが IPSec ピア アドレスであるトラフィックだけに適用され、その他のトラフィックについては無視されます（他のトラフィックはすべて、トンネル モードのみです）。
ステップ 3	`end`	クリプト トランスフォーム コンフィギュレーション モードを終了してイネーブル モードに戻ります。

ステップ 4	`Router# clear crypto sa`
	または
	`Router# clear crypto sa peer {ip-address | peer-name}`
	または
	`Router# clear crypto sa map map-name`
	または
	`Router# clear crypto sa spi destination-address protocol spi`
		既存の IPSec SA を解消し、今後確立される SA でトランスフォーム セットの変更が有効になるようにします（手動で設定した SA は、ただちに再確立されます）。
		パラメータを指定せずに **clear crypto sa** コマンドを実行すると、SA データベースの全内容が消去されるので、アクティブなセキュリティ セッションも消去されます。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 **spi** キーワードを指定します。

表 4-1 に、Authentication Header（AH; 認証ヘッダー）および Encapsulating Security Protocol（ESP）の有効なトランスフォームの組み合わせを示します。

表 4-1　使用できるトランスフォームの組み合わせ

トランスフォーム タイプ	トランスフォーム	内容
AH トランスフォーム（1 つを選択）	**ah-md5-hmac**	MD5（Message Digest 5）（HMAC バリアント）認証アルゴリズムを使用する AH
	ah-sha-hmac	SHA（Secure Hash Algorithm）（HMAC バリアント）認証アルゴリズムを使用する AH
ESP 暗号化トランスフォーム（注：**ESP 認証トランスフォーム**を使用する場合、いずれか 1 つを選択する必要があります。）	**esp-aes**	128 ビットの AES 暗号化アルゴリズムを使用する ESP
	esp-aes 128	128 ビットの AES 暗号化アルゴリズムを使用する ESP
	esp-aes 192	192 ビットの AES 暗号化アルゴリズムを使用する ESP
	esp-aes 256	256 ビットの AES 暗号化アルゴリズムを使用する ESP
	esp-des	56 ビットの DES 暗号化アルゴリズムを使用する ESP
	esp-3des	168 ビットの DES 暗号化アルゴリズム（3DES [Triple DES]）を使用する ESP
	esp-null	ヌル暗号化アルゴリズム
ESP 認証トランスフォーム（1 つを選択）	**esp-md5-hmac**	MD5（HMAC バリアント）認証アルゴリズムを使用する ESP
	esp-sha-hmac	SHA（HMAC バリアント）認証アルゴリズムを使用する ESP

指定できるトランスフォームの組み合わせを次に示します。

- ***ah-md5-hmac***
- ***esp-des***
- ***esp-3des*** および ***esp-md5-hmac***
- ***ah-sha-hmac***、***esp-des***、および ***esp-sha-hmac***

無効な組み合わせを入力すると、解析プログラムによって拒否されます。たとえば、特定の AH トランスフォームを指定した場合、現在のトランスフォーム セットに別の AH トランスフォーム を指定することはできません。

IPSec プロトコル：AH および ESP

AH プロトコルおよび ESP プロトコルは、IPSec にセキュリティ サービスを実装します。

AH は、データ認証およびアンチ リプレイ サービスを提供します。

ESP は、パケットの暗号化のほかに、任意選択でデータ認証およびアンチ リプレイ サービスを提供します。

ESP は保護対象のデータ（完全な IP データグラムまたはペイロードのみ）を、ESP ヘッダーおよび ESP トレーラーでカプセル化します。AH は保護対象のデータに埋め込まれる形になり、外側の IP ヘッダーの直後、および内側の IP データグラムまたはペイロードの直前に AH ヘッダーを挿入します。IPSec ピア間で送受信されるトラフィックは、トンネル モードまたはトランスポート モードのいずれかで送信できます。その他のトラフィックはすべてトンネル モードで送信されます。トンネル モードは IP データグラム全体をカプセル化して保護するのに対し、トランスポート モードは IP データグラムのペイロードをカプセル化して保護します。モードについての詳細は、**mode（IPSec）** コマンドの説明を参照してください。

適切なトランスフォームの選択

状況に適したトランスフォームを選択するには、次のヒントを参考にしてください。

- データの機密保護を提供するには、ESP 暗号化トランスフォームを使用します。
- データのほかに外側の IP ヘッダーについてもデータ認証が必要な場合は、AH トランスフォームを含めます（IP ヘッダー データの完全性には、あまり利点がないとする見方もあります）。
- ESP 暗号化トランスフォームを使用する場合は、トランスフォーム セットに認証サービスを提供するために、ESP 認証トランスフォームまたは AH トランスフォームを使用することも検討してください。
- （ESP または AH による）データ認証を希望する場合、MD5 または SHA（HMAC キー ハッシュ バリアント）認証アルゴリズムのいずれかを選択できます。SHA アルゴリズムは一般に MD5 よりも強力と考えられますが、やや低速になります。
- IPSec ピアによっては、一部のトランスフォームがサポートされない場合があります。

（注） ハードウェア（IPSec ピア）がサポートしていない IPSec トランスフォームを入力すると、**crypto ipsec transform-set** コマンドを入力した直後に警告メッセージが表示されます。

- 暗号化トランスフォームを指定する必要があっても、実際にはパケットを暗号化しない場合、***esp-null*** トランスフォームを使用できます。

考えられるトランスフォームの組み合わせを次に示します。

- ***esp-aes*** および ***esp-sha-hmac***
- ***ah-sha-hmac***、***esp-aes***、および ***esp-sha-hmac***

クリプト トランスフォーム コンフィギュレーション モード

crypto ipsec transform-set コマンドを入力すると、クリプト トランスフォーム コンフィギュレーション モードが開始されます。このモードでは、モードをトンネルまたはトランスポートに変更できます（これらの変更は任意選択です）。これらの変更を行ったあと、グローバル コンフィギュレーション モードに戻るには **exit** を使用します。これらの任意選択の変更についての詳細は、**match address**（IPSec）および **mode**（IPSec）コマンドの説明を参照してください。

既存のトランスフォームの変更

既存のトランスフォーム セットに関して **crypto ipsec transform-set** コマンドで 1 つまたは複数のトランスフォームを指定すると、そのトランスフォーム セットの既存のトランスフォームが、指定したトランスフォームに置き換えられます。

トランスフォーム セットの定義を変更した場合、そのトランスフォーム セットを参照するクリプト マップ エントリに対してのみ変更が適用されます。変更は既存の SA には適用されませんが、新しい SA を確立する今後のネゴシエーションで使用されます。新しい設定をすぐに有効にするには、**clear crypto sa** コマンドを使用して SA データベースの全体または一部を消去します。

トランスフォームの例

次の例では、2 つのトランスフォーム セットを定義しています。最初のトランスフォーム セットは、新しい ESP プロトコルおよび AH プロトコルをサポートする IPSec ピアで使用されます。2 番めのトランスフォーム セットは、従来のトランスフォームだけをサポートする IPSec ピアで使用されます。

```
crypto ipsec transform-set newer esp-3des esp-sha-hmac
crypto ipsec transform-set older ah-rfc-1828 esp-rfc1829
```

IPSec の設定

ここで説明する内容は次のとおりです。

- アクセス リストと IPSec の互換性の確保（必須）
- IPSec SA のグローバル ライフタイムの設定（必須）
- クリプト アクセス リストの作成（必須）
- クリプト マップ エントリの作成（必須）
- ダイナミック クリプト マップの作成（必須）
- クリプト マップ セットのインターフェイスへの適用（必須）
- 設定の確認（任意）

IPSec の設定例は、「IPSec の設定例」（p.4-20）を参照してください。

IPSec の設定の詳細については、『*Cisco IOS Security Configuration Guide*』の「Configuring IPSec Network Security」の章を参照してください。

アクセス リストと IPSec の互換性の確保

IKE は、UDP ポート 500 を使用します。IPSec の ESP および AH プロトコルは、プロトコル番号 50 および 51 を使用します。プロトコル番号 50、51、および UDP ポート 500 のトラフィックが、IPSec を適用するインターフェイス上で阻止されないように、インターフェイスのアクセス リストを設定してください。状況によっては、これらのトラフィックを明示的に許可するステートメントを、アクセス リストに追加する必要があります。

IPSec SA のグローバル ライフタイムの設定

新しい IPSec SA をネゴシエートするときに使用されるグローバル ライフタイム値を変更できます（特定のクリプト マップ エントリについて、これらのグローバル ライフタイム値を上書きできます）。

これらのライフタイムが適用されるのは、IKE で確立する SA だけです。手動で確立する SA には、期限がありません。

IPSec SA のグローバル ライフタイムを変更するには、次のコマンドを 1 つまたは複数使用します。

(注)　下記ステップ 5 の **clear** コマンドは、EXEC（イネーブル）モードで実行されます（詳細については「EXEC コマンド インタープリタの使用」[p.4-3] を参照してください）。

	コマンド	目的
ステップ 1	`Router# enable`	イネーブル 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場合は、パスワードを入力してください。
ステップ 2	`Router# configure terminal`	グローバル コンフィギュレーション モードになります。
ステップ 3	`Router(config)# crypto ipsec security-association lifetime seconds` *seconds*	IPSec SA をネゴシエートするときに使用されるグローバル ライフタイム値を変更します。ライフタイムをデフォルト値に戻すには、このコマンドの no 形式を使用します。 SA が期限切れになるまでの秒数を指定します。デフォルトは 3,600 秒（1 時間）です。
ステップ 4	`Router(config)# crypto ipsec security-association lifetime kilobytes` *kilobytes*	IPSec SA のグローバル ライフタイム（トラフィック量）を変更します。 SA が期限切れになるまでに SA を使って IPSec 間で送受信されるトラフィック量をキロバイト単位で指定します。デフォルトは 4,608,000 キロバイトです。

ステップ 5	`Router# clear crypto sa`
	
	または
	
	`Router# clear crypto sa peer {`*ip-address* | *peer-name*`}`
	
	または
	
	`Router# clear crypto sa map` *map-name*
	
	または
	
	`Router# clear crypto sa spi` *destination-address protocol spi*
		（任意）既存の SA を消去します。この場合、既存の SA はただちに期限切れになり、今後の SA は新しいライフタイムを使用するようになります。これらのコマンドを使用しない場合、既存の SA はあらかじめ設定されたライフタイムに応じて期限切れになります。
		
		(注)　パラメータを指定せずに **clear crypto sa** コマンドを実行すると、SA データベースの全内容が消去されるので、アクティブなセキュリティ セッションも消去されます。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 **spi** キーワードを指定します。詳細については、**clear crypto sa** コマンドを参照してください。

クリプト アクセス リストの作成

クリプト アクセス リストでは、暗号化によって保護する IP トラフィックを定義します（これらのアクセス リストは、インターフェイスで転送またはブロックすべきトラフィックを指定する通常のアクセス リストとは*異なります*）。たとえば、サブネット A とサブネット Y の間の IP トラフィックをすべて保護するアクセス リストや、ホスト A とホスト B の間の Telnet トラフィックをすべて保護するアクセス リストを作成できます。

クリプト アクセス リストを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的

ステップ 1	`Router(config)# access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard [log]`
	
	または
	
	`Router(config)# ip access-list extended name`
		保護する IP パケットを判別するための条件を指定します[1]（これらの条件に適合するトラフィックに対して、暗号化をイネーブルまたはディセーブルにします）。
		
		IPSec には「ミラー イメージ」のクリプト アクセス リストを設定し、**any** キーワードは使用しないことを推奨します。

ステップ 2	必要に応じて、**permit** および **deny** ステートメントを追加します。	アクセス リストに許可または拒否のステートメントを追加します。
ステップ 3	**End**	コンフィギュレーション コマンド モードを終了します。

1. 条件を設定するには、対応する IP アクセス リストの番号または名前を指定します。**access-list** コマンドには、拡張アクセス リストの番号を指定します。**ip access-list extended** コマンドには、アクセス リストの名前を指定します。

アクセス リストの設定の詳細については、『*Security Configuration Guide*』の「Configuring IPSec Network Security」の章を参照してください。

クリプト マップ エントリの作成

クリプト マップ セットは、1 つのインターフェイスに対して 1 つのみ適用できます。クリプト マップ セットには、IPSec/IKE エントリおよび IPSec/ 手動エントリの組み合わせを含めることができます。複数のインターフェイスで同じクリプト マップ セットを共有させ、複数のインターフェイスに同じポリシーを適用できます。

IKE を使用せずに SA を確立するクリプト マップ エントリを作成するには、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto map map-name seq-num ipsec-manual`	作成（または変更）するクリプト マップ エントリを指定します。 このコマンドを使用すると、クリプト マップ コンフィギュレーション モードが開始されます。
ステップ 2	`Router(config-crypto-m)# match address access-list-id`	IPSec アクセス リストの名前を指定します。このアクセス リストによって、このクリプト マップ エントリのコンテキストの中で、IPSec で保護するトラフィックと保護しないトラフィックが決定されます（IKE を使用しない場合、アクセス リストに指定できる **permit** エントリは 1 つだけです）。
ステップ 3	`Router(config-crypto-m)# set peer {hostname | ip-address}`	リモート IPSec ピアを指定します。これは、IPSec で保護したトラフィックの転送先となるピアです。 （IKE を使用しない場合は、1 つのピアしか指定できません。）

	コマンド	目的
ステップ 4	Router(config-crypto-m)# **set transform-set** *transform-set-name*	使用するトランスフォーム セットを指定します。 リモート ピアの対応するクリプト マップ エントリに指定されているものと同じトランスフォーム セットでなければなりません。 （IKE を使用しない場合は、1 つのトランスフォーム セットしか指定できません。）
ステップ 5	Router(config-crypto-m)# **set session-key inbound ah** *spi hex-key-string* および Router(config-crypto-m)# **set session-key outbound ah** *spi hex-key-string*	指定したトランスフォーム セットに AH プロトコルが含まれている場合に、保護対象の着信および発信トラフィックに対して適用する AH Security Parameter Index（SPI）および鍵を設定します。 （保護するトラフィックに使用する AH SA を手動で指定します。）
ステップ 6	Router(config-crypto-m)# **set session-key inbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*] および Router(config-crypto-m)# **set session-key outbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]	指定したトランスフォーム セットに ESP プロトコルが含まれている場合に、保護対象の着信および発信トラフィックに対して適用する ESP SPI および鍵を設定します。トランスフォーム セットに ESP 暗号化アルゴリズムが含まれている場合に、暗号鍵を指定します。トランスフォーム セットに ESP 認証アルゴリズムが含まれている場合に、認証鍵を指定します。 （保護するトラフィックに使用する ESP SA を手動で指定します。）
ステップ 7	Router(config-crypto-m)# **exit**	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

IKE を使用して SA を確立するクリプト マップ エントリを作成するには、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**	作成（または変更）するクリプト マップ エントリの名前を指定します。 このコマンドを使用すると、クリプト マップ コンフィギュレーション モードが開始されます。
ステップ 2	Router(config-crypto-m)# **match address** *access-list-id*	拡張アクセス リストの名前を指定します。このアクセス リストによって、このクリプト マップ エントリのコンテキストの中で、IPSec で保護するトラフィックと保護しないトラフィックが決定されます。
ステップ 3	Router(config-crypto-m)# **set peer** {*hostname* | *ip-address*}	リモート IPSec ピアを指定します。これは、IPSec で保護したトラフィックの転送先となるピアです。 複数のリモート ピアに対して、同じ作業を繰り返します。
ステップ 4	Router(config-crypto-m)# **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。プライオリティの高い順から、複数のトランスフォーム セットを指定します（最優先するセットを最初に指定します）。

	コマンド	目的

ステップ 5	`Router(config-crypto-m)# set security-association lifetime seconds seconds`
	
	および
	
	`Router (config-crypto-m)# set security-association lifetime kilobytes kilobytes`
		（任意）クリプト マップ エントリの SA ライフタイムを指定します。
		
		グローバル ライフタイム以外の IPSec SA ライフタイムを使用してクリプト マップ エントリの SA をネゴシエートする場合に、このコマンドを使用します。

ステップ 6	`Router(config-crypto-m)# set security-association level per-host`	（任意）送信元 / 宛先ホストのペアごとに、個別の SA を確立するよう指定します。 このコマンドを使用しない場合、1 つの IPSec 「トンネル」で複数の送信元ホストおよび宛先ホストのトラフィックが伝送されます。 このコマンドを使用すると、ルータは新しい SA を要求するとき、ホスト A とホスト B の間のトラフィック用と、ホスト A とホスト C の間のトラフィック用にそれぞれ 1 つずつ SA を確立します。 サブネット間の複数のストリームによって急速にリソースが消費される可能性があるので、このコマンドは十分に注意して使用してください。
ステップ 7	`Router(config-crypto-m)# set pfs [group1 | group2 | group5]`	（任意）IPSec がこのクリプト マップ エントリの新しい SA を要求する場合に Perfect Forward Secrecy（PFS）を要求するように、または IPSec ピアから受信する要求に PFS が含まれることを要求するように指定します。
ステップ 8	`Router(config-crypto-m)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ダイナミック クリプト マップの作成

ダイナミック クリプト マップ エントリは、一部のパラメータが設定されていないクリプト マップ エントリです。設定されていないパラメータは（IPSec ネゴシエーションの結果）動的に設定されます。ダイナミック クリプト マップは IKE でのみ使用可能です。

ダイナミック クリプト マップ エントリは、セットにまとめられます。セットとは、*dynamic-map-name* が同じで、*dynamic-seq-num* がそれぞれ異なるダイナミック クリプト マップ エントリのグループです。

ダイナミック クリプト マップ エントリを設定するには、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto dynamic-map dynamic-map-name dynamic-seq-num`	ダイナミック クリプト マップ エントリを作成します。
ステップ 2	`Router(config-crypto-m)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。プライオリティの高い順から、複数のトランスフォーム セットを指定します（最優先するセットを最初に指定します）。 ダイナミック クリプト マップ エントリに必須の設定ステートメントは、これだけです。
ステップ 3	`Router(config-crypto-m)# match address access-list-id`	（任意）拡張アクセス リストのアクセス リスト番号または名前。このアクセス リストによって、このクリプト マップ エントリのコンテキストの中で、IPSec で保護するトラフィックと保護しないトラフィックが決定されます。 **（注）** ダイナミック クリプト マップ エントリではアクセス リストは任意指定ですが、アクセス リストを指定することを強く推奨します。 設定する場合、IPSec ピアによって提示されるデータ フローのアイデンティティは、このクリプト アクセス リストの **permit** ステートメントで許可されるものでなければなりません。 設定しない場合、ルータは IPSec ピアが提示する任意のデータ フロー アイデンティティを受け入れます。ただし、設定されていても指定されたアクセス リストが存在しない場合、または空である場合には、ルータはすべてのパケットを廃棄します。スタティック クリプト マップの場合もアクセス リストを指定する必要があるので、同様の結果になります。 アクセス リストはネゴシエーションだけでなくパケット フィルタリングにも使用されるので、アクセス リストに **any** キーワードを使用する場合は注意が必要です。
ステップ 4	`Router(config-crypto-m)# set peer {hostname | ip-address}`	（任意）リモート IPSec ピアを指定します。複数のリモート ピアに対して、同じ作業を繰り返します。 このコマンドをダイナミック クリプト マップ エントリで設定することは、ほとんどありません。通常、ダイナミック クリプト マップ エントリは不明のリモート ピアを対象に使用します。

ステップ 5	`Router(config-crypto-m)# set security-association lifetime seconds seconds`
	
	および
	
	`Router (config-crypto-m)# set security-association lifetime kilobytes kilobytes`
		（任意）グローバルに指定されたライフタイムではなく、短い IPSec SA ライフタイムを使用してこのクリプト マップの SA をネゴシエートするには、クリプト マップ エントリのライフタイムを指定します。

	コマンド	目的
ステップ 6	`Router(config-crypto-m)# set pfs [group1 | group2 | group5]`	（任意）IPSec がこのクリプト マップ エントリの新しい SA を要求する場合に PFS を要求するように、または IPSec ピアから受信する要求に PFS が含まれることを要求するように指定します。
ステップ 7	`Router(config-crypto-m)# exit`	クリプト マップ コンフィギュレーション モードを終了し、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	この手順を繰り返して、必要な数だけクリプト マップ エントリを作成します。	

クリプト マップ セットにダイナミック クリプト マップ セットを追加するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name`	ダイナミック クリプト マップ セットをスタティック クリプト マップ セットに追加します。

クリプト マップ セットのインターフェイスへの適用

IPSec トラフィックが流れるインターフェイスごとに、クリプト マップ セットを適用します。接続または SA ネゴシエーションが行われるとき、ルータはインターフェイス トラフィックをクリプト マップ セットに照らし合わせて評価し、保護対象のトラフィックに指定されたポリシーを使用します。

クリプト マップ セットをインターフェイスに適用するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# crypto map map-name`	クリプト マップ セットをインターフェイスに適用します。

冗長インターフェイスを指定し、識別するインターフェイスに名前を付けるには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# crypto map map-name local-address interface-id`	冗長インターフェイスが同じローカル アイデンティティを使用して同じクリプト マップを共有できるようにします。

IPSec のモニタリングおよびメンテナンス

IPSec SA を消去（および再初期化）するには、EXEC（イネーブル）モードで次のいずれかのコマンドを使用します（詳細については「EXEC コマンド インタープリタの使用」[p.4-3] を参照）。

コマンド	目的
Router# **clear crypto sa** または Router# **clear crypto sa counters** または Router# **clear crypto sa peer** {*ip-address* | *peer-name*} または Router# **clear crypto sa map** *map-name* または Router# **clear crypto sa spi** *destination-address protocol spi*	IPSec SA を消去します。 **（注）** パラメータを指定せずに **clear crypto sa** コマンドを実行すると、SA データベースの全内容が消去されるので、アクティブなセキュリティ セッションも消去されます。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 **spi** キーワードを指定します。詳細については、**clear crypto sa** コマンドを参照してください。

IPSec の設定に関する情報を表示するには、EXEC モードで次のいずれかのコマンドを使用します。

コマンド	目的
Router# **show crypto ipsec transform-set**	トランスフォーム セットの設定を表示します。
Router# **show crypto map** [**interface** *interface* | **tag** *map-name*]	クリプト マップの設定を表示します。
Router# **show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**]	IPSec SA に関する情報を表示します。
Router# **show crypto dynamic-map** [**tag** *map-name*]	ダイナミック クリプト マップに関する情報を表示します。
Router# **show crypto ipsec security-association lifetime**	グローバルな SA ライフタイム値を表示します。

IKE および IPSec の設定の確認

IPSec の設定に関する情報を表示するには、**show crypto ipsec transform-set** EXEC コマンドを使用します。

（注） ハードウェア（IPSec ピア）がサポートしていない IPSec トランスフォームを入力すると、**show crypto ipsec transform-set** コマンドの出力に警告メッセージが表示されます。

次に示す **show crypto ipsec transform-set** コマンドの出力例では、ハードウェアがサポートしていない IPSec トランスフォームを設定しようとしたので、警告メッセージが表示されています。

```
Router# show crypto ipsec transform-set
Transform set transform-1:{esp-256-aes esp-md5-hmac}
   will negotiate = {Tunnel, },

WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

IKE の設定に関する情報を表示するには、**show crypto isakmp policy** EXEC コマンドを使用します。

（注） ハードウェアがサポートしていない IKE 暗号化方式を入力すると、**show crypto isakmp policy** の出力に警告メッセージが表示されます。

次に示す **show crypto isakmp policy** コマンドの出力例では、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ので、警告メッセージが表示されています。

```
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
```

設定の確認

設定変更によっては、SA のネゴシエーション後に初めて有効になります。新しい設定値がただちに有効になるようにするには、既存の SA を消去します。

IPSec SA を消去（および再初期化）するには、表 4-2 のいずれかのコマンドを EXEC（イネーブル）モードで使用します（詳細については「EXEC コマンド インタープリタの使用」[p.4-3] を参照）。

表 4-2　IPSec SA を消去するコマンド

コマンド	目的
clear crypto sa or **clear crypto sa peer** {*ip-address* | *peer-name*} or **clear crypto sa map** *map-name* or **clear crypto sa spi** *destination-address protocol spi*	IPSec SA を消去します。 パラメータを指定せずに **clear crypto sa** コマンドを実行すると、SA データベースの全内容が消去されるので、アクティブなセキュリティ セッションも消去されます。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 **spi** キーワードを指定します。

設定を確認する手順は、次のとおりです。

ステップ 1　**show crypto ipsec transform-set** コマンドを入力し、トランスフォーム セットの設定を表示します。

```
Router# show crypto ipsec transform-set
Transform set combined-des-md5: {esp-des esp-md5-hmac}
   will negotiate = {Tunnel,},
Transform set t1: {esp-des esp-md5-hmac}
   will negotiate = {Tunnel,},
Transform set t100: {ah-sha-hmac}
   will negotiate = {Transport,},
Transform set t2: {ah-sha-hmac}
   will negotiate = {Tunnel,},
   {esp-des}
   will negotiate = {Tunnel,},
```

ステップ 2　**show crypto map** [**interface** *interface* | **tag** *map-name*] **コマンド**を入力し、クリプト マップの設定を表示します。

```
Router# show crypto map
Crypto Map: "router-alice" idb: Ethernet0 local address: 172.21.114.123
Crypto Map "router-alice" 10 ipsec-isakmp
        Peer = 172.21.114.67
        Extended IP access list 141
            access-list 141 permit ip
                source: addr = 172.21.114.123/0.0.0.0
                dest:   addr = 172.21.114.67/0.0.0.0
        Current peer: 172.21.114.67
        Security-association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={t1,}
```

ステップ 3　**show crypto ipsec sa** [**map** map-name | **address** | **identity** | **detail** | **interface**] コマンドを入力し、IPSec SA 情報を表示します。

```
Router# show crypto ipsec sa
interface: Ethernet0
    Crypto map tag: router-alice, local addr. 172.21.114.123
   local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
     local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
     path mtu 1500, media mtu 1500
     current outbound spi: 20890A6F
     inbound esp sas:
      spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     outbound esp sas:
      spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
```

```
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
      outbound ah sas:
interface: Tunnel0
   Crypto map tag: router-alice, local addr. 172.21.114.123
   local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
   current_peer: 172.21.114.67
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
     local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
     path mtu 1500, media mtu 1500
     current outbound spi: 20890A6F
     inbound esp sas:
      spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     outbound esp sas:
      spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
```

show コマンドによって表示される情報の詳細については、『*Security Command Reference*』の「IP Security and Encryption」の章を参照してください。

設定例

ここでは、次の設定例を紹介します。

IKE ポリシーの設定例

次の例では、2 つの IKE ポリシーを作成し、ポリシー 15 に最高のプライオリティ、ポリシー 20 にその次に高いプライオリティを与え、既存のデフォルト プライオリティを最下位のプライオリティにします。さらに、IP アドレス 192.168.224.33 のリモート ピアに対して、ポリシー 20 で使用する事前共有鍵を作成します。

```
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
```

IPSec の設定例

次に、IKE によって SA が確立される最小限の IPSec の設定例を示します。

IPSec アクセス リストで、保護するトラフィックを定義します。

```
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.2.2.0 0.0.0.255
```

トランスフォーム セットで、トラフィックの保護方法を定義します。この例では、トランスフォーム セット [myset1] で DES 暗号化および SHA を使用して、データ パケットを認証します。

```
crypto ipsec transform-set myset1 esp-des esp-sha
```

次のトランスフォーム セットの例 [myset2] では、3DES 暗号化および MD5（HMAC バリアント）を使用して、データ パケットを認証します。

```
crypto ipsec transform-set myset2 esp-3des esp-md5-hmac
```

クリプト マップは IPSec アクセス リストとトランスフォーム セットを結合し、保護するトラフィックの送信先（リモート IPSec ピア）を指定します。

```
crypto map toRemoteSite 10 ipsec-isakmp
 match address 101
 set transform-set myset2
 set peer 10.2.2.5
```

クリプト マップをインターフェイスに適用します。

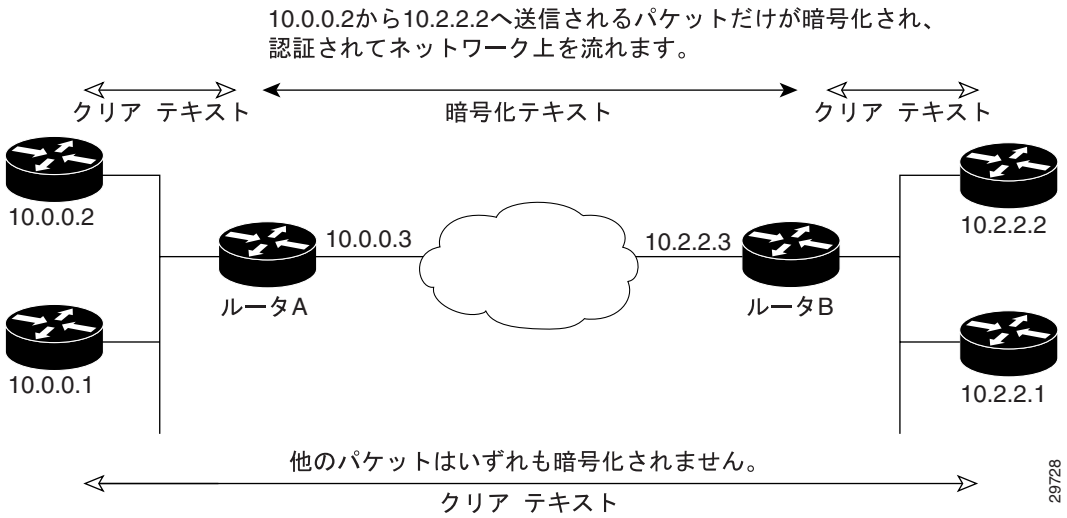
```
interface Serial0
 ip address 10.0.0.2
 crypto map toRemoteSite
```

(注)　この例では、IKE をイネーブルにする必要があります。

IPSec の基本的な設定例

次に、IKE によって SA が確立される、IPSec の設定例を示します。この例では、アクセス リストを使用して、暗号化 / 復号化するパケットを制限します。この例では、IP アドレス 10.0.0.2 から IP アドレス 10.2.2.2 へのすべてのパケットが暗号化 / 復号化され、さらに IP アドレス 10.2.2.2 から IP アドレス 10.0.0.2 へのすべてのパケットが暗号化/復号化されます。IKE ポリシーも 1 つ作成します。

図 4-1　IPSec の基本設定



ルータ A の設定

IKE ネゴシエーションで使用するパラメータを指定します。

```
crypto isakmp policy 15
  encryption des
  hash md5
  authentication pre-share
  group 2
  lifetime 5000

crypto isakmp key 1234567890 address 10.2.2.3
crypto isakmp identity address
```

(注)　上記の例では、ポリシー 15 の暗号化 DES は、書き込まれるコンフィギュレーションに含まれません。暗号化アルゴリズム パラメータのデフォルト値だからです。

トランスフォーム セットで、トラフィックの保護方法を定義します。

```
crypto ipsec transform-set auth1 ah-md5-hmac esp-des esp-md5-hmac
  mode tunnel
```

(注)　上記の例では、mode tunnel は書き込まれるコンフィギュレーションには含まれません。transform-set のデフォルト値だからです。

クリプト マップはトランスフォーム セットと結合し、保護するトラフィックの送信先（リモート IPSec ピア）を指定します。

```
crypto map toRemoteSite 10 ipsec-isakmp
match address 101
set peer 10.2.2.3
set transform-set auth1
```

クリプト マップをインターフェイスに適用します。

```
  interface Serial0
  ip address 10.0.0.3
crypto map toRemoteSite
```

IPSec アクセス リストで、保護するトラフィックを定義します。

```
access-list 101 permit ip host 10.0.0.2 host 10.2.2.2
access-list 101 permit ip host 10.0.0.3 host 10.2.2.3
```

ルータ B の設定

IKE ネゴシエーションで使用するパラメータを指定します。

```
crypto isakmp policy 15
  encryption des
  hash md5
  authentication pre-share
  group 2
  lifetime 5000

crypto isakmp key 1234567890 address 10.0.0.3
crypto isakmp identity address
```

トランスフォーム セットで、トラフィックの保護方法を定義します。

```
crypto ipsec transform-set auth1 ah-md5-hmac esp-des ah-md5-hmac
  mode tunnel
```

(注)　上記の例では、パラメータ「mode tunnel」は書き込まれるコンフィギュレーションには含まれません。この設定のデフォルト値だからです。

クリプト マップはトランスフォーム セットと結合し、保護するトラフィックの送信先（リモート IPSec ピア）を指定します。

```
crypto map toRemoteSite 10 ipsec-isakmp
  match address 101
  set peer 10.0.0.3
  set transform-set auth1
```

クリプト マップをインターフェイスに適用します。

```
interface Serial0
  ip address 10.2.2.3
  crypto map toRemoteSite
```

IPSec アクセス リストで、保護するトラフィックを定義します。

```
access-list 101 permit ip host 10.2.2.2 host 10.0.0.2
access-list 101 permit ip host 10.2.2.3 host 10.0.0.3
```

トラブルシューティングのヒント

Cisco IOS ソフトウェアが VSA を認識しているかどうかを確認するには、**show diag** コマンドを入力し、出力を調べます。次の例では、IOS ソフトウェアはルータのスロット 0 に搭載されている C7200-VSA を認識しています。

```
Router# show diag 0
Slot 0:
        VSA IPsec Card Port adapter
        Port adapter is analyzed
        Port adapter insertion time 00:23:25 ago
        EEPROM contents at hardware discovery:
        PCB Serial Number        : PRTA4404055
        Product (FRU) Number     : C7200-VSA
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF C1 8B 50 52 54 41 34 34 30 34 30 35 35 40
          0x10: 05 0D CB 94 43 37 32 30 30 2D 56 53 41 20 20 20
          0x20: 20 20 20 20 20 20 20 20 D9 03 C1 40 CB FF FF FF
          0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

VSA が現在、暗号化パケットを処理しているかどうかを確認するには、**show crypto engine accelerator statistic 0** コマンドを入力します。次に、出力例を示します。

```
Router# show crypto engine accelerator statistic 0

Device:   VSA
Location: Service Adapter: 0
 VSA Traffic Statistics

  Inbound rate: 0pps 0kb/s  Outbound rate: 0pps 0kb/s
  TXR0 PKT: 0x00000000000028B2  Byte: 0x0000000000006ACF6  Full: 0x0000000000000000
  RXR0 PKT: 0x00000000000028B2  Byte: 0x00000000000A86398
  TXR1 PKT: 0x0000000000000000  Byte: 0x0000000000000000  Full: 0x0000000000000000
  RXR1 PKT: 0x0000000000000000  Byte: 0x0000000000000000
  TXR2 PKT: 0x0000000000000000  Byte: 0x0000000000000000  Full: 0x0000000000000000
  RXR2 PKT: 0x0000000000000000  Byte: 0x0000000000000000
  Inbound Traffic:
  Decrypted  PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  SPI Error  PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  Pass clear PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  SPD Drop:          0x0000000000000000  IKE Bypass:    0x0000000000000000
  Outbound Traffic:
  Encry CEF: 0x0000000000000000  FS: 0x0000000000000000  PROC: 0x0000000000000000
  Pass  CEF: 0x0000000000000000  FS: 0x0000000000000000  PROC: 0x0000000000000000
  ICMP Unreachable: 0x0000000000000000  ICMP Unreach Fail: 0x0000000000000000
  SPD Drop:  0x0000000000000000
  Special Traffic:
  VAM mode  PKT:     0x0000000000000000  Exception:     0x0000000000000000
  N2 Message:    :   0x00000000000028B2  Exception:     0x0000000000000000
  IP PKT Exception:  0x0000000000000000  DJ Overflow:   0x0000000000000000
  RAE Report PKT::   0x0000000000000000  PKT Consumed:  0x0000000000000000
  TCAM WR:           0x0000000000000001  TCAM RD:       0x0000000000000000
  SARAM WR:          0x0000000000008422  SARAM RD:      0x0000000000000000
  RAE WR:            0x0000000000080000  RAE RD:        0x0000000000000000
  Warnings:
  N2 interrupt:      0x0000000000000000  Invalid Op:    0x0000000000000000
  RX CTX error:      0x0000000000000000  TX CTX low:    0x0000000000000000
  PKT CTX Low:       0x0000000000000000  PKT Info Low:  0x0000000000000000
  PKT Header Low:    0x0000000000000000  Particle Low:  0x0000000000000000
  Missing SOP:       0x0000000000000000  Missing EOP:   0x0000000000000000
  TX Drop IB:        0x0000000000000000  TX Drop OB:    0x0000000000000000
  MSG Unknown:       0x0000000000000000  MSG too Big:   0x0000000000000000
```

```
  MSG Empty:          0x0000000000000000  MSG No Buffer: 0x0000000000000000
  PKT Info Missing:   0x0000000000000000  IB SB Error:   0x0000000000000000
  TX Drop Fastsend:   0x0000000000000000  IDMA Full:     0x0000000000000000
  Particle Fallback: 0x0000000000000000  STATISTIC:     0x0000000000000000

 Elrond statistic:
  TXDMA PKT Count:    0x00000000000028B2  Byte Count:    0x000000000006ACF6
  RXDMA PKT Count:    0x00000000000028B2  Byte Count:    0x0000000000A86398
  IPPE  PKT Count:    0x00000000000028B2  EPPE PKT Count:0x00000000000028B2
  PL3TX PKT Count:    0x00000000000028B2  Byte Count:    0x000000000009DADE
  PL3RX PKT Count:    0x00000000000028B2  Byte Count:    0x0000000000A86398
  CAM search IPPE:    0x0000000000000000  EPPE:          0x0000000000000000
  SARAM Req IPPE:     0x0000000000000000  EPPE:          0x0000000000000000
  RAE Frag Req IPPE: 0x0000000000000000  EPPE:          0x0000000000000000
  RAE ReAssembly:     0x0000000000000000  Re-Ordering:   0x0000000000000000
  REA Frag Finished: 0x0000000000000000
  Frag Drop Count:
   IPPE:              0x0000000000000000  EPPE:          0x0000000000000000
   FIFO:              0x0000000000000000  RAE:           0x0000000000000000

VSA RX Exception statistics:
   IRH Not valid           :        0   Invalid SA              :        0
   SA configuration error  :        0   Enc Dec mismatch        :        0
   Insufficient Push       :        0   Next Header mismatch    :        0
   Pad mismatch            :        0   MAC mismatch            :        0
   Atomic OP failed        :        0   L2 UDD GE 256           :        0
   Max BMI Read too small  :        0   Max BMI Read No payload :        0
   Anti replay failed      :        0   Enc Seq num overflow    :        0
   Dec IPver mismatch      :        0   Enc IPver mismatch      :        0
   TTL Decr                :        0   Selector checks         :        0
   UDP mismatch            :        0   Reserved                :        0
   Soft byte lifetime      :        0   hardbyte lifetime       :        0
   IP Parse error          :        0   Fragmentation Error     :        0
   Unknown Exception       :        0
```

VSA がパケットを処理すると、「packets in」および「packets out」カウンタが変化します。「packets out」カウンタは、VSA に送られたパケット数を示します。「packets in」カウンタは、VSA から受信したパケット数を示します。

IKE/IPSec パケットが VSA に転送されて IKE ネゴシエーションおよび IPSec 暗号化 / 復号化が行われているかどうかを調べるには、**show crypto eli** コマンドを入力します。次に、Cisco IOS ソフトウェアが VSA にパケットを転送している場合の出力例を示します。

```
Router# show crypto eli
Hardware Encryption : ACTIVE
 Number of hardware crypto engines = 1

 CryptoEngine VSA details: state = Active
 Capability      : DES, 3DES, AES, RSA

 IKE-Session   :     0 active,  5120 max, 0 failed
 DH            :     0 active,  5120 max, 0 failed
 IPSec-Session :     0 active, 10230 max, 0 failed
```

ソフトウェア暗号化エンジンがアクティブな場合、**show crypto eli** コマンドを入力しても出力は得られません。

Cisco IOS ソフトウェアが VSA に暗号トラフィックを転送することに合意した場合、次のようなメッセージが出力されます。

```
%ISA-6-INFO:Recognised crypto engine (0) at slot-0
    ...switching to hardware crypto engine
```

VSA をディセーブルにするには、次のように、コンフィギュレーション モードで **no crypto engine accelerator** <*slot*> コマンドを使用します。

```
Router(config)# no crypto engine accelerator 0
...switching to SW crypto engine
Router(config)#
*Feb  6 11:57:26.763: %VPN_HW-6-INFO_LOC: Crypto engine: slot 0  State changed to:
Disabled
*Feb  6 11:57:26.779: %PA-3-DEACTIVATED: port adapter in bay [0] powered off.
*Feb  6 11:57:26.779: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
Router(config)#end
```

VSA のモニタリングおよびメンテナンス

ここで説明する内容は次のとおりです。

アクセス リストでの拒否ポリシーの使用

アクセス リストに拒否アドレスの範囲を指定すると、「ジャンプ」動作が発生します。拒否されているアドレス範囲にヒットした時点で、クリプト マップの次のシーケンスに対応付けられたアクセス リストの先頭に「ジャンプ」し、そこから検索が続けられます。これらのアドレスにクリア トラフィックを送信するには、クリプト マップのシーケンスごとに拒否アドレスの範囲を挿入しなければなりません。アドレスの許可リストはそれぞれ、アクセス リストで指定されたすべての拒否アドレスの範囲を継承します。拒否アドレスの範囲を指定することで、ソフトウェアは許可リストから拒否アドレスの範囲を差し引き、ハードウェアにプログラムする必要のある複数の許可アドレスの範囲を作成します。この動作によって、拒否アドレスの範囲 1 つのために、ハードウェアへのアドレス範囲のプログラミングが繰り返される場合があるため、1 つのアクセス リストに複数の許可アドレスの範囲が存在する結果になります。

この問題を回避するには、**crypto ipsec ipv4 deny-policy** {jump | clear | drop} コマンドが役立ちます。clear キーワードを使用すると、拒否アドレスの範囲がハードウェアにプログラムされたあと、その拒否アドレスは暗号化 / 復号化の対象外になります。拒否アドレスにヒットすると、検索が停止し、トラフィックがクリアな（暗号化されていない）状態で通過できるようになります。drop キーワードを使用すると、拒否アドレスにヒットした時点でトラフィックが廃棄されます。これら 2 つの新しいキーワードを使用して、アドレス範囲がハードウェアに繰り返しプログラムされるのを防ぎ、スペース利用を効率化することができます。

設定時の注意事項と制約事項

- **crypto ipsec ipv4 deny-policy** {jump | clear | drop} コマンドは、VSA モジュールに適用できるグローバル コマンドです。指定したキーワード（jump、clear、または drop）は VSA モジュールの ACE ソフトウェアに伝播されます。デフォルトの動作は jump です。
- VSA　モジュールにクリプト　マップがすでに設定されている場合に特定のキーワード（jump、clear、または drop）を適用すると、既存の IPSec セッションがすべて一時的に削除されてから再開され、ネットワークのトラフィックに影響します。
- アクセス リストに指定できる拒否エントリの数は、指定するキーワードによって異なります。
  - jump ― アクセス リストごとに最大 8 つの拒否エントリを使用できます。
  - clear ― アクセス リストごとに最大 1000 個の拒否エントリを使用できます。
  - drop ― アクセス リストごとに最大 1000 個の拒否エントリを使用できます。

モニタリングおよびメンテナンス用のコマンド

VSA のモニタおよびメンテナンスには、次のコマンドを使用します。

コマンド	目的
`Router# show crypto engine accelerator statistic 0`	VSA が現在暗号パケットを処理しているかどうかを確認します。
`Router# Show version`	インターフェイスの一部として組み込まれているサービス アダプタを表示します。

A

C

E

I

L

M

O

R

S

V

あ

い

か

き

く

け

こ

せ

そ

ち

て

は

ひ

ほ

ま

め

も

よ