CISCO SYSTEMS

Service Adapter VPN Acceleration Module 2 (SA-VAM2) インストレーション コンフィギュレーション ガイド

製品番号：SA-VAM2(=)

Text Part Number: OL-4669-03-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。All rights reserved. Copyright © 1981, Regents of the University of California.

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。

このマニュアルは、ルータに付属の適切なマニュアルと併せて使用してください。

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、iQuick Study は、Cisco Systems, Inc. のサービス マークです。Access Registrar、Aironet、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、*Packet*、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、The Fastest Way to Increase Your Internet Quotient、TransPath は、米国および一部の国における Cisco Systems, Inc. または関連会社の登録商標です。

このマニュアルまたは Web サイトで言及している他の商標はいずれも、それぞれの所有者のものです。「パートナー」という用語を使用していても、シスコシステムズと他社とのパートナー関係を意味するものではありません。（0601R）

Service Adapter VPN Acceleration Module 2 (SA-VAM2) インストレーション コンフィギュレーション ガイド
Copyright © 2006 Cisco Systems, Inc.
All rights reserved.

CONTENTS

はじめに vii

対象読者 viii

警告 viii

マニュアルの目的 ix

マニュアルの構成 ix

関連資料 x

マニュアルの入手方法 xii

Cisco.com xii

Product Documentation DVD xii

マニュアルの発注方法 xii

シスコ製品のセキュリティ xiii

シスコ製品のセキュリティ問題の報告 xiii

テクニカル サポート xiv

Cisco Technical Support & Documentation Web **サイト** xiv

Japan TAC Web **サイト** xiv

Service Request **ツールの使用** xv

問題の重大度の定義 xv

その他の資料および情報の入手方法 xvi

CHAPTER 1 **概要** 1-1

データ暗号化の概要 1-2

SA-VAM2 **の概要** 1-4

機能 1-6

パフォーマンス 1-7

OIR 1-8

SA-VAM2 1-8

Port Adapter Jacket Card 1-8

サポート対象の規格、MIB**、および** RFC 1-8

規格 1-8

MIB 1-8

RFC 1-8

LED 1-9
SA-VAM2 1-9
Port Adapter Jacket Card 1-10
ケーブル、コネクタ、およびピン割り当て 1-11
スロット位置 1-11
Cisco 7200VXR ルータ 1-11
Cisco 7301 ルータ 1-13

CHAPTER 2 インストレーションの準備 2-1
必要な工具および機器 2-2
ハードウェアおよびソフトウェアの要件 2-2
ハードウェア要件 2-2
ソフトウェア要件 2-3
制限 2-3
ISA、SA-VAM、および SA-VAM2 のインターオペラビリティ 2-4
安全に関する注意事項 2-5
安全上の警告 2-5
電気製品の取り扱いに関する注意事項 2-5
静電破壊の防止 2-5
暗号化に関する米国輸出規制法の遵守 2-6

CHAPTER 3 SA-VAM2 の取り外しおよび取り付け 3-1
SA-VAM2 の取り扱い 3-2
OIR 3-2
SA-VAM2 3-2
Port Adapter Jacket Card 3-2
警告および注意事項 3-3
SA-VAM2 の取り外しおよび取り付け 3-4
Cisco 7200VXR ルータの Port Adapter Jacket Card 3-4
Cisco 7200VXR ルータ 3-6
Cisco 7301 ルータ 3-8

CHAPTER 4 SA-VAM2 の設定 4-1
概要 4-2
設定作業 4-3
EXEC コマンド インタープリタの使用方法 4-4
OIR のディセーブル化 4-4
IKE ポリシーの設定 4-5
トランスフォーム セットの設定 4-6

トランスフォーム セットの定義 4-7
IPSec プロトコル：AH および ESP 4-9
適切なトランスフォームの選択 4-9
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 4-9
既存のトランスフォームの変更 4-10
トランスフォームの例 4-10
IPSec の設定 4-10
アクセス リストと IPSec の互換性の確保 4-10
IPSec SA のグローバル ライフタイムの設定 4-11
クリプト アクセス リストの作成 4-12
クリプト マップ エントリの作成 4-12
ダイナミック クリプト マップの作成 4-15
クリプト マップ セットのインターフェイスへの適用 4-16
圧縮の設定 4-17
IKE ポリシーの設定 4-17
IKE 事前共有鍵の設定 4-17
IPSec トランスフォーム セットの設定 4-18
アクセス リストの設定 4-18
クリプト マップの設定 4-18
クリプト マップのインターフェイスへの適用 4-19
IPSec のモニタリングおよびメンテナンス 4-19
IPSec の設定例 4-20
IKE および IPSec の設定の確認 4-21
設定の確認 4-22
設定例 4-24
IKE ポリシーの設定例 4-24
IPSec の設定例 4-24
圧縮の設定例 4-25
IPSec の基本的な設定例 4-26
ルータ A の設定 4-26
ルータ B の設定 4-27
トラブルシューティングのヒント 4-28
SA-VAM2 のモニタおよびメンテナンス 4-30

INDEX 索引

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。この章で説明する内容は、次のとおりです。

- 対象読者（p.viii）
- 警告（p.viii）
- マニュアルの目的（p.ix）
- マニュアルの構成（p.ix）
- 関連資料（p.x）
- マニュアルの入手方法（p.xii）
- シスコ製品のセキュリティ（p.xiii）
- テクニカル サポート（p.xiv）
- その他の資料および情報の入手方法（p.xvi）

対象読者

このマニュアルでは、読者がシスコ製ルータおよびケーブル接続のほか、電子回路および配線方法について知識があることを前提にしています。電子または電気機械技術者としての経験のある人が、このマニュアルを使用するよう推奨します。

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。**

警告 **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、Service Adapter VPN Acceleration Module 2（SA-VAM2）の取り付け手順および設定手順について説明します。SA-VAM2 は、Network Processing Engine（NPE; ネットワーク処理エンジン）225（NPE-225）、400（NPE-400）、および G1（NPE-G1）を搭載した Cisco 7200VXR ルータおよび Cisco 7301 ルータでサポートされるシングル幅のアクセラレーション モジュールです。

SA-VAM2 の部品番号は SA-VAM2(=) 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
第 1 章	概要	SA-VAM2 および SA-VAM2 の LED について説明します。
第 2 章	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。
第 3 章	SA-VAM2 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 SA-VAM2 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。
第 4 章	SA-VAM2 の設定	Cisco 7200 シリーズ ルータおよび Cisco 7301 上での SA-VAM2 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。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。

- Cisco 7200VXR Port Adapter Jacket Card のハードウェア情報については、『*Port Adapter Jacket Card Installation Guide*』を参照してください。
- 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
- Cisco 7301 ルータのマニュアルについては、次の URL を参照してください。
  http://www.cisco.com/en/US/products/hw/routers/ps352/prod_technical_documentation.html
- 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/prod_module_installation_guides_list.html
  および
  http://www.cisco.com/en/US/products/hw/modules/ps2033/products_module_installation_guides_books_list.html
- コンフィギュレーション情報およびサポートについては、ご使用のシスコ ハードウェア製品にインストールされているソフトウェア リリースに対応する Cisco IOS ソフトウェア コンフィギュレーション マニュアル セットのモジュラ コンフィギュレーションおよびモジュラ コマンド リファレンスを参照してください。これらのマニュアルは、次の URL で利用できます。
  http://www.cisco.com/en/US/products/sw/iosswrel/index.html

(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。

  - ルータに最小限必要な Cisco IOS ソフトウェアを確認できるように、シスコシステムズでは Cisco.com に Software Advisor ツールを用意しています。これは、システム内のモジュールの互換性を調べるためではなく、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小限必要な IOS 要件を調べるためのツールです。Cisco Direct Customers 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
- IP セキュリティおよび暗号化については、次の URL を参照してください。
  http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
- FIPS 140 セキュリティ マニュアル：
  http://www.cisco.com/en/US/partner/products/hw/routers/ps341/products_regulatory_approvals_and_compliance09186a00800f009e.html
- VPN Device Manager マニュアル：
  http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2322/products_release_and_installation_notes_list.html
- Cisco Direct Customers に登録済みの場合は、次のツールにアクセスできます。
  - Bug Toolkit：
    http://www.cisco.com/en/US/partner/products/hw/routers/ps341/prod_bug_toolkit.html
  - Bug Navigator：
    http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl
  - Feature Navigator：
    http://www.cisco.com/en/US/partner/products/prod_feature_navigator_for_cisco_IOS_tool_launch.html
  - Output Interpreter：
    https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl

  - Cisco IOS Error Message Decoder：
    http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl
  - Cisco Dynamic Configuration Tool：
    http://www.cisco.com/en/US/ordering/or13/or8/ordering_ordering_help_dynamic_configuration_tool_launch.html
  - MIB Locator：
    http://tools.cisco.com/ITDIT/MIBS/servlet/index
- その他のツール：
  - ツールの一覧：
    http://www.cisco.com/en/US/partner/products/prod_tools_index.html
  - Cisco IOS Software Selector Tool：
    http://tools.cisco.com/ITDIT/ISTMAIN/servlet/index

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。また、テクニカル サポートおよびその他のテクニカル リソースは、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法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総合的なライブラリです。DVD を使用すると、シスコのハードウェア製品およびソフトウェア製品の様々なバージョンの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、コマンド リファレンスにアクセスできます。DVD を使用することで、インターネットに接続しなくてもシスコの Web サイトと同じ HTML 形式のマニュアルを参照できます。製品によっては、マニュアルの PDF バージョンも用意されています。

Product Documentation DVD は単一製品として、またはサブスクリプションとして入手できます。Cisco.com（Cisco Direct Customers）に登録されている場合、Cisco Marketplace から Product Documentation DVD（Customer Order Number DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。Cisco Marketplace の URL は次のとおりです。

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

マニュアルの発注方法

Cisco.com に登録されている場合、次の URL にある Cisco Marketplace の Product Documentation Store でシスコ製品のマニュアルを発注できます。

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

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

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

このサイトでは、次の手順についての情報を検索できます。

- 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、注意のリスト、および対応については、以下の URL で確認できます。

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

Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）Feed をサブスクライブすれば、セキュリティ勧告、注意のリスト、および対応が更新されるたびにリアル タイムで通知されます。PSIRT RSS Feed のサブスクライブについては、次の URL で確認できます。

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 を所有していないまたは使用しない場合は、機密情報をお送りなる前に、前述の電子メールアドレスまたは電話番号で PSIRT に連絡し、別のデータ暗号化方法をご利用ください。

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 サポートにお問い合わせいただく前に、Cisco Product Identification（CPI）ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support & Documentation Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI 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。

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 Product Quick Reference Guide*』はコンパクトで使いやすい製品ガイドです。チャネル パートナー経由で販売される多数のシスコ製品に関する簡単な製品概要、主要機能、サンプル部品番号、および技術仕様の要約が掲載されています。年 2 回更新され、最新の情報が収録されます。『*Cisco Product Quick Reference Guide*』の発注方法および詳細については、次の URL から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

- 『*Packet*』は、シスコシステムズが発行するテクニカル ユーザ向けの季刊誌で、インターネットやネットワークへの投資を最大限に活用するのに役立ちます。『*Packet*』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

- 『*iQ Magazine*』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『*iQ Magazine*』には、次の URL からアクセスしてください。

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

  または次の URL でデジタル版をご覧いただけます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*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、ネットワーキング専門家がネットワーキング製品やネットワーキング技術に関する質問、提案、情報をシスコの専門家および他のネットワーキング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

- 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、Service Adapter VPN Acceleration Module 2（SA-VAM2）について概要を説明します。この章で説明する内容は、次のとおりです。

- データ暗号化の概要（p.1-2）
- SA-VAM2 の概要（p.1-4）
- 機能（p.1-6）
- OIR（p.1-8）
- サポート対象の規格、MIB、および RFC（p.1-8）
- LED（p.1-9）
- ケーブル、コネクタ、およびピン割り当て（p.1-11）
- スロット位置（p.1-11）

データ暗号化の概要

ここでは、IP Security Protocol（IPSec）、Internet Key Exchange（IKE）、および 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」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、抗リプレー 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、次のデータ暗号化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整合性を保証し、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 装置は 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」（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 に関して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 3DES ― Data Encryption Standard（DES; データ暗号化規格）および Triple DES（3DES）暗号化パケット データです。Cisco IOS は 3 キー 3DES および DES-CBC（Explicit Initialization Vector [IV] を伴う）を実装します。Cipher Block Chaining（CBC）は、暗号化の開始に 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。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 nonces ― 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 nonces 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、他の規格もサポートします。

- AH ― Authentication Header（AH）は、データ認証およびオプションの抗リプレー 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 プロトコルは抗リプレー 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、および抗リプレー 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 Explicit IV を伴う 56 ビット DES-CBC または 3DES を実装します。また、認証アルゴリズムとして MD5 または SHA（いずれも HMAC バリアント）を実装します。最新の ESP プロトコルでは、抗リプレー サービスを提供します。

- IPPCP ― IP Payload Compression Protocol。レイヤ 3 の暗号化を使用すると、下位レイヤ（レイヤ 2 の PPP［ポイントツーポイント プロトコル］など）は圧縮ができなくなります。すでに暗号化されているパケットを圧縮すると、通常は展開されます。IPPCP は IPSec などの暗号化サービスと組み合わせて使用できる、ステートレスの圧縮を提供します。

SA-VAM2 の概要

SA-VAM2 は、Network Processing Engine（NPE; ネットワーク処理エンジン）225（NPE-225）、400（NPE-400）、および G1（NPE-G1）を搭載した Cisco 7301 ルータおよび Cisco 7200VXR ルータでサポートされる、シングル幅のポート アダプタです（図 1-1 を参照）。

(注)　NPE-300 プロセッサおよび Network Service Engine（NSE; ネットワーク サービス エンジン）（NSE-1）サービス アクセラレータは、サポート対象ではなくなりました。

SA-VAM2 は、セキュリティ、Quality of Service（QoS; サービス品質）、ファイアウォール、侵入検知、サービス レベル検証 / 管理など、Virtual Private Network（VPN; 仮想私設網）リモート アクセスおよびサイト間イントラネット / エクストラネット アプリケーションに必要な、ハードウェア支援トンネリングおよび暗号化 / 圧縮サービスを提供します。SA-VAM2 は IPSec 処理の負担をメイン プロセッサから解放し、プロセッサ エンジンのリソースを他の作業に使用できるようにします。

SA-VAM2 は、Cisco 7000VXR シリーズ ルータ（図 1-5、図 1-6、および図 1-7 を参照）および Cisco 7301 ルータ（図 1-8 を参照）のポート アダプタ スロットに直接搭載できます。または SA-VAM2 を Port Adapter Jacket Card（製品番号：C7200-JC-PA）に装着し、NPE-G1 プロセッサを搭載した Cisco 7200VXR ルータの I/O コントローラ スロットに挿入して帯域を広げることもできます（図 1-2 を参照）。

SA-VAM2 が Port Adapter Jacket Card でサポートされているので、VPN のパフォーマンスを維持しながら NPE-G1 のパフォーマンスを向上させることができます。SA-VAM2 を Port Adapter Jacket Card に装着すると、通常のポート アダプタ スロットよりも帯域を広げることができます。詳細については、『*Port Adapter Jacket Card Installation Guide*』を参照してください。

図 1-1　SA-VAM2

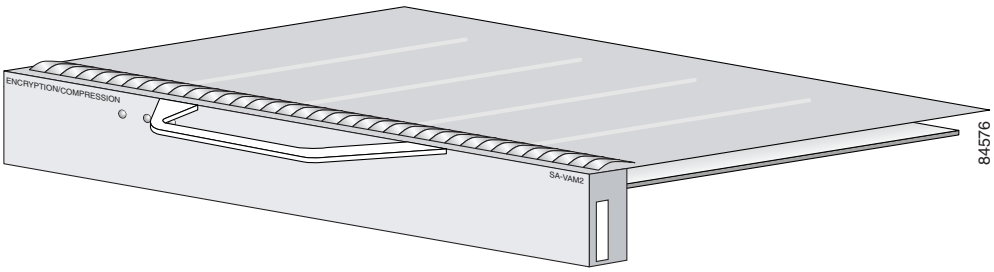
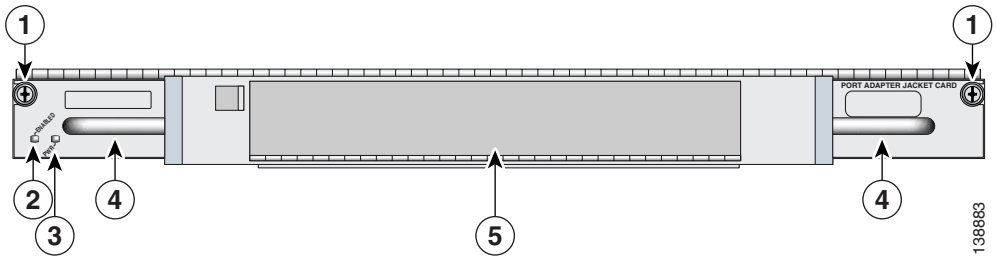


図 1-2　NPE-G1 を搭載した Cisco 7200VXR の Port Adapter Jacket Card の前面プレート



1	非脱落型ネジ	**4**	ハンドル
2	ENABLE LED	**5**	SA-VAM2/ ポート アダプタ スロット
3	PWR（電源）LED		

SA-VAM2 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 ビット AES、および HSP ソフトウェア上での 192/256 ビット
- 56 ビット DES 標準モード：CBC
- 300 バイト パケットで OC3 全二重モードに対応するパフォーマンス
- DES/3DES/AES 用の 5000 トンネル
- オーバーヘッドを追加せずに IPSec による圧縮を提供
- 3 キー 3DES（168 ビット）
- SHA-1 および MD5 ハッシュ アルゴリズム
- RSA 公開鍵アルゴリズム
- Diffie-Hellman 鍵交換 RC4-40
- IPSec トンネル モード
- Online Insertion and Removal（OIR; ホットスワップ）

機能

ここでは、SA-VAM2 の機能（表 1-1 を参照）、および SA-VAM2 のパフォーマンス データ（表 1-2 を参照）について説明します。

表 1-1　SA-VAM2 の機能

機能	説明 / 利点
物理面	サービス アダプタ。任意の Cisco 7200VXR ルータ[1] または Cisco 7301 ルータのシングル ポートアダプタ スロットに搭載
サポート対象プラットフォーム	Cisco 7200VXR シリーズ ルータ（NPE-G1、NPE-400、または NPE-225 プロセッサを搭載）、および Cisco 7301 ルータ
IPSec で保護されるトンネル数[2]	Cisco 7200VXR ルータ：最大 5000 Cisco 7301 ルータ：最大 5000
ハードウェアベースの暗号化	データ保護：IPSec DES、3DES、AES[3] 認証：RSA、Diffie-Hellman データ整合性：SHA-1、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
ハードウェアベースの圧縮	レイヤ 3 IPPCP LZS
LAN/WAN インターフェイスの選択	ほとんどの Cisco7200VXR 互換ポート アダプタで動作
サポートする規格	IPSec/IKE：RFC 2401 ～ 2411、2451 IPPCP：RFC 2393、2395
（任意）Port Adapter Jacket Card	Port Adapter Jacket Card は、NPE-G1 プロセッサを搭載した Cisco IOS Release 12.4(6)T および 12.4(7) 以上のリリースの Cisco 7200VXR ルータで利用可能

1. Cisco 7200VXR は、SA-VAM2 を 2 つまでサポートします。
2. サポートされるトンネル数は、搭載されたシステム メモリの合計および展開されるソリューションによって異なります。
3. AES は 128 ビットをサポートします。

パフォーマンス

表 1-2 に、SA-VAM2 のパフォーマンスを示します。

表 1-2　パフォーマンス

Cisco ルータ	スループット[1]	内容
Cisco 7301	最大 386 Mbps	Cisco IOS：c7301-jk9o3s-mz.123-1.9[2] 7301/ シングル SA-VAM2、1 GB のシステム メモリ 3DES/SHA、IKE キープアライブ設定なし事前共有
Cisco 7200VXR（NPE-G1 または NPE-400 を搭載）	最大 299 Mbps[2 3]	Cisco IOS：c7200-jk9o3s-mz.123-1M[2] 7200VXR/NPE-G1（700 Mhz）/ シングル SA-VAM2、512 MB のシステム メモリ 3DES/SHA、IKE キープアライブ設定なし事前共有
	最大 489 Mbps[2 3]	同上、ただしデュアル SA-VAM2 を使用
Cisco 7200VXR（NPE-225 を搭載）	最大 218 Mbps	Cisco IOS：c7200-jk9o3s-mz.123-M[2] 7200VXR/NPE-225/ シングル SA-VAM2、256 MB のシステム メモリ 3DES/SHA、IKE キープアライブ設定なし事前共有
Cisco 7200VXR（NSE-1 を搭載）	最大 250 Mbps	Cisco IOS：c7200-jk9o3s-mz.123-1M[2] 7200VXR/SA-VAM2、256 MB のシステム メモリ 3DES/SHA、IKE キープアライブ設定なし事前共有

1. IPSec 3DES HMAC-SHA-1 を使用し 1400 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、トラフィック ボリューム、Cisco IOS リリースによって異なります。
2. Cisco 12.3-1M イメージの使用を推奨します。パフォーマンスは Cisco IOS のリリースによって異なります。Cisco 7200VXR または Cisco 7301 ルータの最新イメージをダウンロードすることを推奨します。
3. UUT でオンボードのファスト イーサネット I/O ボードを 2 枚使用するほうが、ファスト イーサネット ポート アダプタにオンボードのファスト イーサネット I/O ボードを 1 枚装着するよりも 1400 B パフォーマンスが 26 ～ 40% ほど向上します。

OIR

ここでは、OIR 機能について説明します。

SA-VAM2

SA-VAM2 では OIR がサポートされています。SA-VAM2 を取り外す場合は、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 SA-VAM2 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。トラフィックがポートを通過中に SA-VAM2 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。

Port Adapter Jacket Card

Port Adapter Jacket Card は OIR をサポートしませんが、Port Adapter Jacket Card に装着した SA-VAM2 は OIR をサポートします。Port Adapter Jacket Card の取り外しおよび取り付けを行う場合は、シャーシの電源をオフにしておく必要があります。Port Adapter Jacket Card の詳細については、『*Port Adapter Jacket Card Installation Guide*』を参照してください。

サポート対象の規格、MIB、および RFC

ここでは、SA-VAM2 でサポートされる規格、MIB（管理情報ベース）、および Request for Comment（RFC）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

- IPPCP：RFC 2393、2395
- 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

- IPPCP：RFC 2393、2395
- IPSec/IKE：RFC 2401 ～ 2411、2451

LED

ここでは SA-VAM2 および Port Adapter Jacket Card の LED について説明します。Port Adapter Jacket Card の詳細については、『*Port Adapter Jacket Card Installation Guide*』を参照してください。

SA-VAM2

SA-VAM2 には 3 つの LED があります（図 1-3 を参照）。表 1-3 に、各 LED のカラーと機能を示します。

図 1-3　SA-VAM2 の LED

表 1-3　SA-VAM2 の LED

	LED のラベル	カラー	状態	機能
1	ENABLE	グリーン	点灯	SA-VAM2 は通電状態で動作可能です。
2	BOOT	オレンジ	点灯	SA-VAM2 は稼働しています。
3	ERROR	オレンジ	点灯	暗号化エラーが発生しました。この LED は通常、消灯しています。

ENABLE LED は、次の条件が満たされた場合に点灯します。

- SA-VAM2 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 SA-VAM2 を認識している。

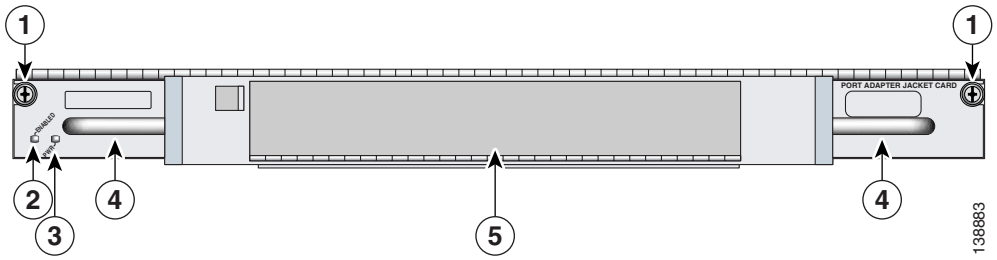
どちらかの条件が満たされていない場合、またはほかの理由でルータを初期化できなかった場合、ENABLE LED は点灯しません。

Port Adapter Jacket Card

Port Adapter Jacket Card には 2 つの LED があります（図 1-4 を参照）。表 1-3 に、各 LED のカラーと機能を示します。

（注） Port Adapter Jacket Card は、NPE-G1 プロセッサを搭載した Cisco 7200VXR ルータでのみ使用できます。

図 1-4　Port Adapter Jacket Card の前面プレート



1	非脱落型ネジ	**4**	ハンドル
2	ENABLE LED	**5**	ポート アダプタ（SA-VAM2）のスロット
3	PWR（電源）LED		

表 1-4　Port Adapter Jacket Card の LED

LED	カラー	意味
ENABLE	グリーン	Port Adapter Jacket Card は動作可能です。
	オフ	Port Adapter Jacket Card は動作不能です。
PWR（電源）	グリーン	Port Adapter Jacket Card に電力が供給されています。
	オフ	Port Adapter Jacket Card に電力が供給されていません。

ケーブル、コネクタ、およびピン割り当て

SA-VAM2 にはインターフェイスがないので、ケーブル、コネクタ、およびピン割り当てはありません。

スロット位置

ここで説明する内容は次のとおりです。

- Cisco 7200VXR ルータ（p.1-11）
- Cisco 7301 ルータ（p.1-13）

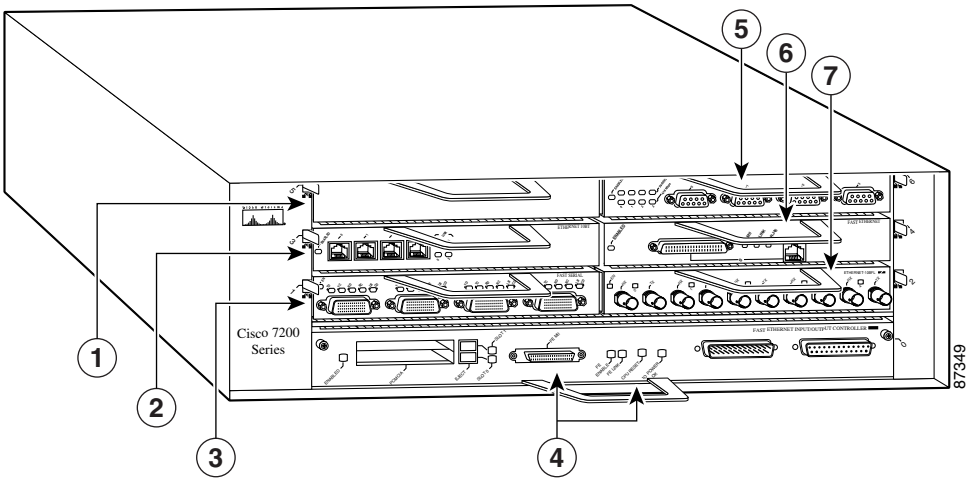
SA-VAM2 は、Cisco 7301 ルータおよび Cisco 7200VXR ルータのポート アダプタ スロットに搭載します。

(注)　使用しないポート アダプタ スロットには、ブランク SM-PA フィラー（部品番号 800-00455-01）を取り付けておいてください。

Cisco 7200VXR ルータ

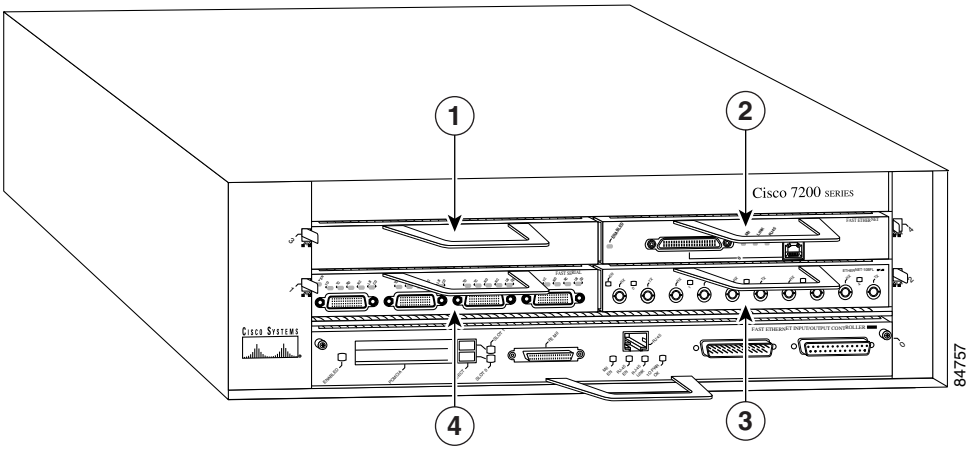
Cisco 7200VXR ルータのスロット番号を、図 1-5、図 1-6、および図 1-7 に示します。

図 1-5　Cisco 7206 のスロット番号



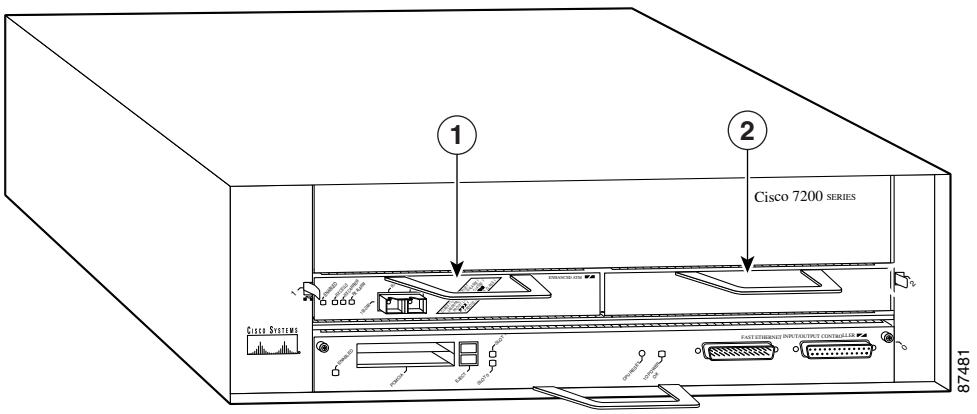
1	ポート アダプタ スロット 5（左側のバス）	5	ポート アダプタ スロット 6（右側のバス）
2	ポート アダプタ スロット 3（左側のバス）	6	ポート アダプタ スロット 4（右側のバス）
3	ポート アダプタ スロット 1（左側のバス）	7	ポート アダプタ スロット 2（右側のバス）
4	ポート アダプタ スロット 0（左側のバス）		

図 1-6　Cisco 7204 のスロット番号



1	ポート アダプタ スロット 3	**3**	ポート アダプタ スロット 2
2	ポート アダプタ スロット 4	**4**	ポート アダプタ スロット 1

図 1-7　Cisco 7202 のスロット番号



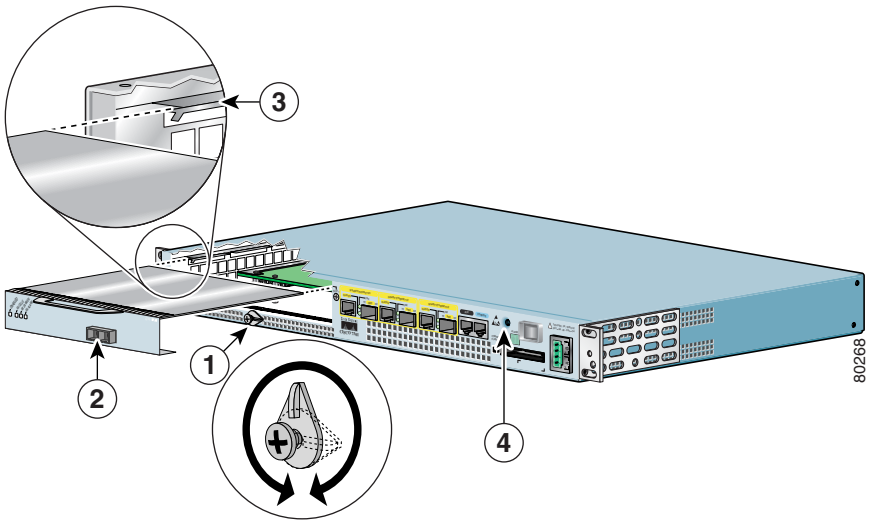
1	ポート アダプタ スロット 1	**2**	ポート アダプタ スロット 2

Cisco 7301 ルータ

図 1-8 に、Cisco 7301 ルータのスロット番号を示します。

(注)　Cisco 7301 ルータは、SA-VAM2（ポート アダプタ）を 1 つだけサポートします。

図 1-8　Cisco 7301 のスロット番号



1	ラッチ	3	スロット ガイド
2	取り外した SA-VAM2	4	静電気防止用リスト ストラップのバナナ ジャック用のアース

インストレーションの準備

この章では、Service Adapter VPN Acceleration Module 2（SA-VAM2）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（p.2-2）
- ハードウェアおよびソフトウェアの要件（p.2-2）
- 安全に関する注意事項（p.2-5）
- 暗号化に関する米国輸出規制法の遵守（p.2-6）

必要な工具および機器

SA-VAM2 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。

- SA-VAM2
- 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 キットに付属の使い捨て静電気防止用リスト ストラップ、Field-Replaceable Unit（FRU）、およびスペア
- 静電気防止用マット
- 静電気防止用容器
- 静電気防止用リスト ストラップ
- （任意）Port Adapter Jacket Card（SA-VAM2 を装着し、NPE-G1 プロセッサを搭載した Cisco 7200VXR ルータの I/O コントローラ スロットに取り付ける）

ハードウェアおよびソフトウェアの要件

ここでは、SA-VAM2 を使用するために最小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。

- ハードウェア要件（p.2-2）
- ソフトウェア要件（p.2-3）
- 制限（p.2-3）
- ISA、SA-VAM、および SA-VAM2 のインターオペラビリティ（p.2-4）

ハードウェア要件

SA-VAM2 の正常な動作を保証するために必要とされる、具体的なハードウェア要件は次のとおりです。

- Cisco 7200VXR ルータで SA-VAM2 を使用するには、ルータに Network Processing Engine（NPE; ネットワーク処理エンジン）225（NPE-225）、400（NPE-400）、または G1（NPE-G1）を搭載している必要があります。
- Cisco 7200VXR ルータは、SA-VAM2 を 2 つまでサポートします。
- Cisco 7301 ルータは、ポート アダプタ スロットで SA-VAM2 を 1 つだけサポートします。
- （任意）SA-VAM2 を Port Adapter Jacket Card に装着する場合、NPE-G1 プロセッサを搭載した Cisco 7200VXR ルータだけがサポートされます。Port Adapter Jacket Card の詳細については、『*Port Adapter Jacket Card Installation Guide*』を参照してください。

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 SA-VAM2 を使用するために最小限必要な、推奨 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　SA-VAM2 ソフトウェア要件

プラットフォーム	推奨する最小限の Cisco IOS リリース[1]
Cisco 7200VXR ルータ	Cisco IOS Release 12.3(1)M 以上の Cisco IOS Release 12.3M リリース Cisco IOS Release 12.3(2)T1 以上の Cisco IOS Release 12.3T1 リリース
Cisco 7301 ルータ	Cisco IOS Release 12.3(3)M 以上の Cisco IOS Release 12.3M リリース Cisco IOS Release 12.3(2)T1 以上の Cisco IOS Release 12.3T1 リリース
（任意）Port Adapter Jacket Card を装着した Cisco 7200VXR ルータ	Cisco IOS Release 12.4(6)T 以上の Cisco IOS Release 12.4T リリース Cisco IOS Release 12.4(7) 以上の Cisco IOS Release 12.4M リリース **（注）** NPE-G1 プロセッサを搭載した Cisco 7200VXR ルータにのみ対応。

1. Cisco IOS Release 12.2(14)SU の販売は終了しました。

シスコでは、ルータに搭載されているハードウェアに最小限必要な Cisco IOS ソフトウェアを確認できるように、Cisco.com で Software Advisor ツールを用意しています。Cisco Direct Customers 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小限必要な 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。

制限

SA-VAM2 には次の制限があります。

- SA-VAM2 には、同一の Cisco 7204VXR または Cisco 7206VXR に搭載した他の暗号化カード（ISA、VAM、SA-VAM2 など）とのインターオペラビリティはありません。（「ISA、SA-VAM、および SA-VAM2 のインターオペラビリティ」[p.2-4] を参照）。
- Cisco 7301 ルータは、ポート アダプタを 1 つだけサポートします。
- デュアル SA-VAM2 カードは、NPE-G1 プロセッサを搭載した Cisco 7200VXR ルータでのみサポートされます。
- SA-VAM2 を使用するルータの推奨するメモリの最小構成は 256 MB です。さらにパフォーマンスを上げたい場合は、512 MB のメモリを推奨します。
- （任意）SA-VAM2 を Port Adapter Jacket Card に装着する場合、NPE-G1 プロセッサを搭載した Cisco 7200VXR ルータだけがサポートされます。Port Adapter Jacket Card の詳細については、『*Port Adapter Jacket Card Installation Guide*』を参照してください。

ISA、SA-VAM、および SA-VAM2 のインターオペラビリティ

(注)　SA-VAM は Integrated Services Adapter（ISA）の後継です。ISA は 2004 年 4 月 15 日で販売を終了しました。

表 2-2 に、ISA、SA-VAM、および SA-VAM2 のインターオペラビリティを示します。次の条件が満たされる場合、SA-VAM2 を ISA または SA-VAM と併用できます。

- Cisco 7200VXR ルータは同一シャーシで SA-VAM2 を 2 つサポートします。システムの起動時に SA-VAM2 が 1 つだけイネーブルで、あとから 2 番めの SA-VAM2 を追加した場合、2 番めの SA-VAM2 がただちにアクティブになり、構成によっては 2 つの SA-VAM2 間でロードバランスが行われます。
- システム起動時に SA-VAM と SA-VAM2 がシャーシに搭載されている場合、Cisco IOS リリースで SA-VAM2 がサポートされていれば、Cisco 7200VXR ルータは新しいバージョン（この場合、SA-VAM2）をサポートし、SA-VAM は非アクティブのままになります。
- システム起動時に ISA と SA-VAM2 がシャーシに搭載されていて、なおかつルータの実行コンフィギュレーションに **encryption mppe** コマンドが含まれている場合、ISA/ISM および SA-VAM2 の両方がシステム起動時にイネーブルになります。ISA/ISM カードは MPPE をサポートし、SA-VAM2 は ISAKMP/IPSec をサポートします。**encryption mppe** をイネーブルにするには、「IPSec の設定」（p.4-10）に記載されている手順に従います。ISA カード上の MPPE をディセーブルにするには、**no encryption mppe** コマンドを使用します。この場合、ISA がディセーブルになります。
- カードをディセーブルにするには、**no crypto engine accelerator** *type slot/port*（ポート アダプタ スロット番号 / インターフェイス ポート番号）コマンドを使用します。

表 2-2　ISA、SA-VAM、および SA-VAM2 のインターオペラビリティ

SA-VAM2 （ISA と併用）[1]	SA-VAM2（SA-VAM と併用）	SA-VAM2 （SA-VAM2 と併用）
• MPPE をサポートする	• MPPE をサポートしない	• MPPE をサポートしない
• ISAKMP/IPSec をサポートする	• ISAKMP/IPSec をサポートする	• ISAKMP/IPSec をサポートする
• 起動時にシャーシで ISA および SA-VAM2 がイネーブルの場合、ルータの実行コンフィギュレーションに **encryption mppe** コマンドが含まれていれば、ISA は MPPE に使用され、SA-VAM2 は ISAKMP/IPSec に使用されます。	• 起動時に SA-VAM2 および SA-VAM がシャーシに搭載されている場合、ルータは SA-VAM2 をサポートし、SA-VAM は非アクティブのままになります。	• 起動時に SA-VAM2 および SA-VAM2 がシャーシに搭載されている場合、ルータは両方ともサポートします。
• 起動時にシャーシで ISA がイネーブルで、あとから SA-VAM2 を追加した場合、SA-VAM2 は次の起動時まで、または SA-VAM2 をイネーブルにするように設定が変更されるまで、非アクティブのままになります。	• 起動時にシャーシで SA-VAM がイネーブルで、あとから SA-VAM2 を追加した場合、SA-VAM2 は次の起動時まで、または SA-VAM2 をイネーブルにするように設定が変更されるまで、非アクティブのままになります。	• システムの起動時にシャーシで SA-VAM2 がイネーブルで、あとから 2 番めの SA-VAM2 を追加した場合、2 番めの SA-VAM2 がただちにアクティブになり、構成によっては 2 つの SA-VAM2 間でロードバランスが行われます。

1. ISA は 2004 年 4 月 15 日で販売を終了しました。

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（p.2-5）
- 電気製品の取り扱いに関する注意事項（p.2-5）
- 静電破壊の防止（p.2-5）

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。**

警告　**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。**

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 つの重要な役割があります。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。**

電気製品の取り扱いに関する注意事項

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 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 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。

ESD による損傷を防ぐために、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

SA-VAM2 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 Service Adapter VPN Acceleration Module 2（SA-VAM2）を取り外す方法、および SA-VAM2 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。

- SA-VAM2 の取り扱い（p.3-2）
- OIR（p.3-2）
- 警告および注意事項（p.3-3）
- SA-VAM2 の取り外しおよび取り付け（p.3-4）

(注) ルータ内部で十分なエアフローを確保し、EMI（電磁波干渉）防止規格に適合させるために、空のポート アダプタ スロットにはブランク ポート アダプタ（部品番号 800-00455-01）を取り付ける必要があります。

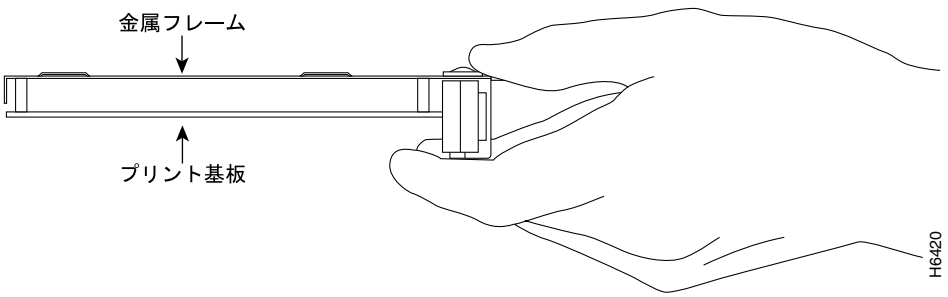
SA-VAM2 基板は ESD（静電気放電）による損傷を受けやすい製品です。

SA-VAM2 の取り扱い

SA-VAM2 は金属フレームにマウントされたシングル幅の基板です（図 3-1 を参照）。

注意　SA-VAM2 を取り扱うときは必ず、フレームの端とハンドルを持ちます。SA-VAM2 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　SA-VAM2 の取り扱い



OIR

ここでは、Online Insertion and Removal（OIR; ホットスワップ）機能について説明します。

SA-VAM2

SA-VAM2 では OIR がサポートされています。SA-VAM2 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 SA-VAM2 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。トラフィックがポートを通過中に SA-VAM2 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。

VAM2 上の OIR の影響については、次の URL にある『*IPSec Stateful Failover (VPN High Availability) Feature Module*』を参照してください。
http://www.cisco.com/en/US/products/ps6550/products_white_paper09186a0080116d4c.shtml

Port Adapter Jacket Card

Port Adapter Jacket Card は OIR をサポートしませんが、Port Adapter Jacket Card に装着した SA-VAM2 は OIR をサポートします。Port Adapter Jacket Card の取り付けおよび取り外しを行う場合は、シャーシの電源をオフにしておく必要があります。Port Adapter Jacket Card の詳細については、『*Port Adapter Jacket Card Installation Guide*』を参照してください。

警告および注意事項

VAM の取り付けまたは取り外しを行うときには、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 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スロットに正しく取り付けた状態で、システムを運用してください。**

警告　**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。**

警告　**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。**

SA-VAM2 の取り外しおよび取り付け

ここでは、SA-VAM2 の取り外し手順および取り付け手順について説明します。具体的な内容は次のとおりです。

- Cisco 7200VXR ルータの Port Adapter Jacket Card（p.3-4）
- Cisco 7200VXR ルータ（p.3-6）
- Cisco 7301 ルータ（p.3-8）

（注） Port Adapter Jacket Card は OIR をサポートしませんが、SA-VAM2 ではサポートされています。Port Adapter Jacket Card の取り外しおよび取り付けを行うときは、シャーシの電源をオフにしておく必要があります。

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。

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。**

Cisco 7200VXR ルータの Port Adapter Jacket Card

NPE-G1 プロセッサを搭載した Cisco 7200VXR ルータの I/O コントローラ スロットに、SA-VAM2 を装着した Port Adapter Jacket Card を取り付けることができます。NPE-G1 に 3 番めの専用 Peripheral Component Interconnect（PCI）バスが加わることで、シャーシの帯域が広がります。

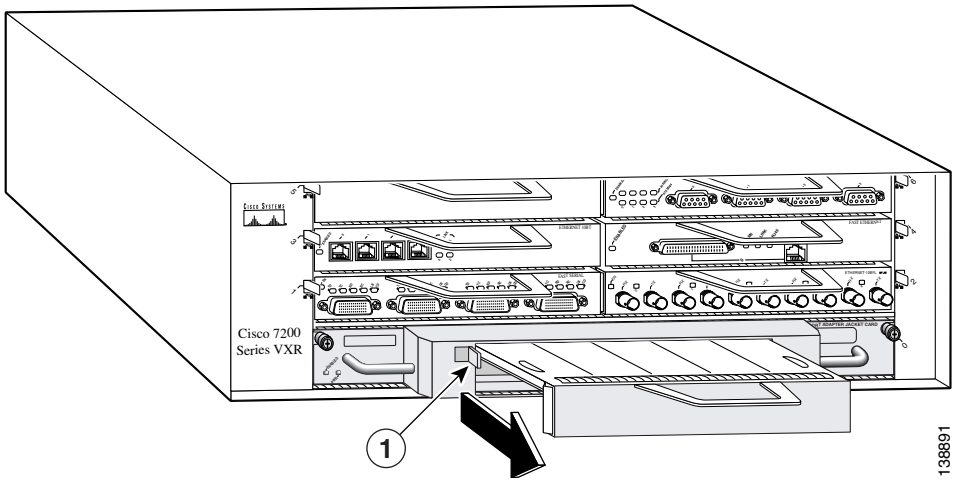
ルータに取り付けた Port Adapter Jacket Card に SA-VAM2 を装着する手順は、次のとおりです。Cisco 7200VXR ルータに Port Adapter Jacket Card を取り付ける手順については、『*Port Adapter Jacket Card Installation Guide*』を参照してください。

ステップ 1　ポート アダプタ ブランク パネルが取り付けられている場合は取り外します（図 3-2 を参照）。

a. Port Adapter Jacket Card の左上のロック レバーを解除して、ポート アダプタ ブランク パネルを外します。

b. Port Adapter Jacket Card からポート アダプタ ブランク パネルを引き出します。

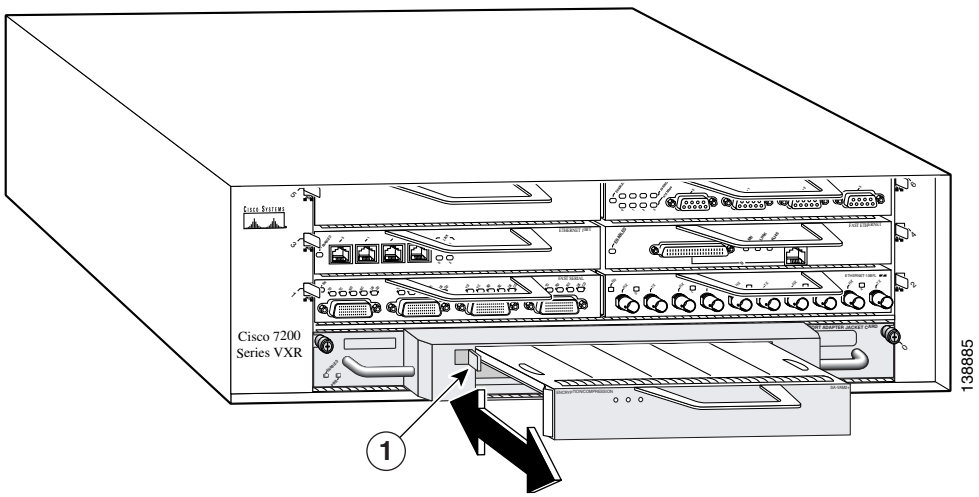
図 3-2　ポート アダプタ ブランク パネルの取り外し



1	ポート アダプタ ロック レバー

ステップ 2　Port Adapter Jacket Card に SA-VAM2 を挿入し、完全に装着します（図 3-3 を参照）。

図 3-3　Port Adapter Jacket Card へのポート アダプタの取り付け



1	ポート アダプタ ロック レバー

ステップ 3　ポート アダプタ ロック レバーをロック位置まで動かします。

ステップ 4　処理エンジンおよびポート アダプタを取り外した場合は、下から上の順に交換します。

Cisco 7200VXR ルータ

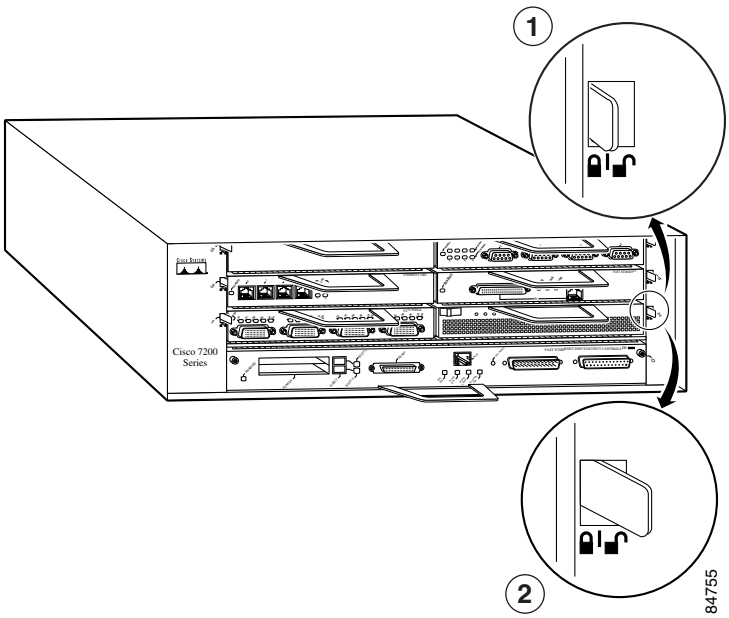
Cisco 7200VXR ルータでの SA-VAM2 の取り外しおよび取り付け手順は、次のとおりです。

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。

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　SA-VAM2 の固定レバーをロック解除の位置にします（図 3-4 の 1 を参照）。

図 3-4　ポート アダプタ レバーのロック位置 / ロック解除位置（Cisco 7206VXR の場合）



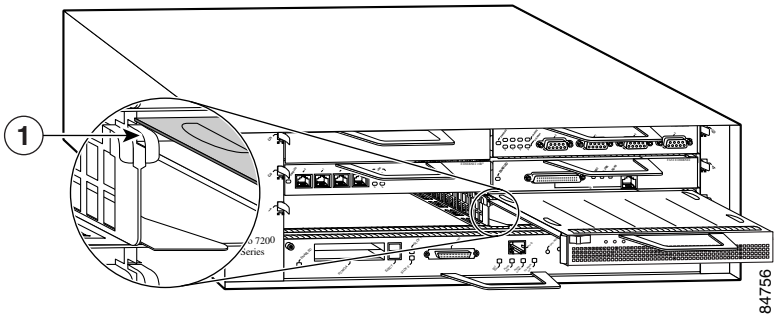
1	ロック解除位置	2	ロック位置

ステップ 4　SA-VAM2 のハンドルを持って、SA-VAM2 をルータから引き抜きます。ブランク ポート アダプタを取り外す場合は、シャーシ スロットからブランク ポート アダプタを完全に引き出します。

ステップ 5　新しい SA-VAM2 のフレームを、ポート アダプタ スロットの上下のエッジに慎重に合わせます（図 3-5 を参照）。

注意　ポート アダプタ 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、SA-VAM2 背面のエッジ コネクタがポート アダプタ スロット奥のコネクタときちんとかみ合うように、図 3-5 の拡大図を参照し、フレームの位置を確認してください。

図 3-5　SA-VAM2 のポート アダプタ スロットへの差し込み（Cisco 7206VXR の場合）



1	ポート アダプタ スロットの上端

ステップ 6　新しい SA-VAM2 をポート アダプタ 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　SA-VAM2 のコンポーネントがシステム基板に接触しないように注意してください。SA-VAM2 が損傷することがあります。

ステップ 7　SA-VAM2 を正しく装着したあと、SA-VAM2 のポート アダプタ レバーをロック位置にします（図 3-4 の 2 を参照）。

（注）　固定用レバーがロック位置まで動かない場合は、モジュールがミッドプレーンに完全に装着されていません。スロットからモジュールを静かに引き出して、改めて挿入し、固定用レバーまたは他の固定機構をロック位置に合わせてください（図 3-4 を参照）。

注意　ポート アダプタ スロットを使用しない場合には、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（部品番号 800-20675-01）をスロットに取り付けておきます。

ステップ 8　電源をオフにしている場合には、

a.　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。

b.　電源スイッチをオンの位置にして、ルータに電源投入します。

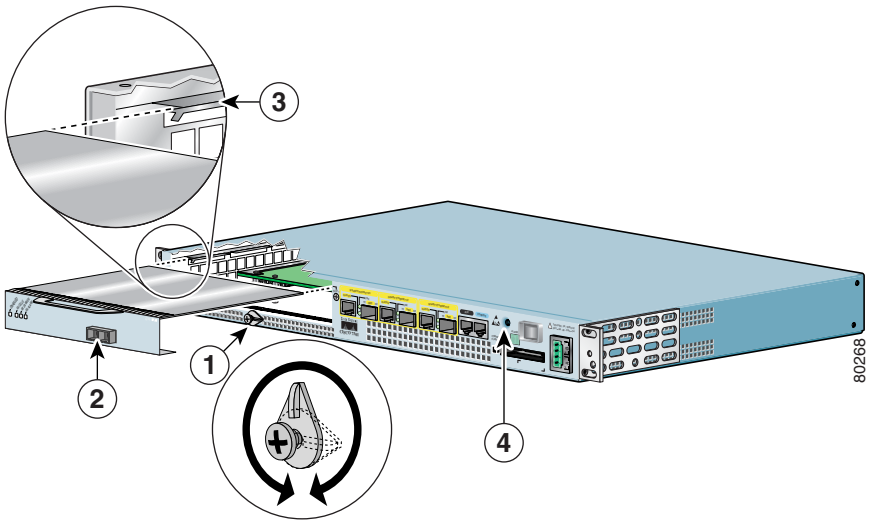
Cisco 7200VXR ルータでの SA-VAM2 の取り外しおよび取り付け手順は、これで完了です。

Cisco 7301 ルータ

Cisco 7301 ルータでの SA-VAM2 の取り付けおよび取り外し手順は、次のとおりです（図 3-6 を参照）。

（注） Cisco 7301 ルータは、SA-VAM2（ポート アダプタ）を 1 つだけサポートします。

図 3-6　Cisco 7301 ポート アダプタ /SA-VAM2 スロット



1	ラッチ	**3**	スロット ガイド
2	取り外した SA-VAM2	**4**	静電気防止用リスト ストラップのバナナ ジャック用のアース

ステップ 1　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ルータに接続します。バナナジャック用のアースは、電源スイッチの左側にあります。

ステップ 2　SA-VAM2 を取り外すには、プラス ドライバを使用してラッチを固定しているネジを回します。ネジを緩めたあと、ラッチを回転させてロック解除位置にします（1）。ラッチは 360 度回転します。

ステップ 3　ハンドルを持ち、SA-VAM2 をルータのスロットから中ほどまで引き出します。ブランク ポート アダプタを取り外す場合は、シャーシ スロットからブランク ポート アダプタを完全に引き出します。

注意　シャーシの天板のすぐ下にあるスロット ガイドに SA-VAM2 を差し込みます。SA-VAM2 のコンポーネントがシステム基板に接触しないように注意してください。SA-VAM2 が損傷することがあります。

ステップ 4　SA-VAM2 を取り付けるには、SA-VAM2 のフレームをスロット ガイドに慎重に合わせ、SA-VAM2 をスロットに完全に差し込んで SA-VAM2 を装着します。

ステップ 5　SA-VAM2 を正しく装着したあと、ラッチを回して上向きのロック位置にします。ネジを締め、SA-VAM2 が固定されていることを確認します。

ステップ 6　電源コードを接続します。

ステップ 7　電源スイッチをオンの位置にして、ルータに電源投入します。

Cisco 7301 ルータでの SA-VAM2 の取り外しおよび取り付け手順は、これで完了です。

CHAPTER 4

SA-VAM2 の設定

この章では、Service Adapter VPN Acceleration Module 2（SA-VAM2）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（p.4-2）
- 設定作業（p.4-3）
- 設定例（p.4-24）
- IPSec の基本的な設定例（p.4-26）
- トラブルシューティングのヒント（p.4-28）
- SA-VAM2 のモニタおよびメンテナンス（p.4-30）

概要

SA-VAM2 は、Network Processing Engine（NPE; ネットワーク処理エンジン）225（NPE-225）、400（NPE-400）、G1（NPE-G1）を搭載した Cisco 7200VXR ルータ、および Cisco 7301 ルータの任意のインターフェイス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 SA-VAM2 を搭載すると、SA-VAM2 は暗号化サービスを自動的に実行します。2 番めの SA-VAM2 を搭載すると、両方の SA-VAM2 が自動的にイネーブルになります。

（注） Cisco 7301 ルータは、SA-VAM2 を 1 つだけサポートします。

（注） Cisco 7200VXR ルータに 2 つの SA-VAM2 を搭載する場合、パケット単位でのロードバランスはサポートされません。2 つの SA-VAM2 を搭載した場合には、パケット単位でなく、IPSec トンネル単位でロードバランスが行われます。

SA-VAM2 上には設定する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 CA（認証局）の設定の詳細については、『*Security Configuration Guide*』の「IP Security and Encryption」、および『*Security Command Reference*』を参照してください。

設定作業

(注) Cisco 7200VXR Port Adapter Jacket Card は設定不要です。ここで説明するとおりに SA-VAM2 を設定します。

起動時に ENABLED LED が点灯した場合、SA-VAM2 は完全に動作しており、コンフィギュレーション コマンドは不要です。ただし、SA-VAM2 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方法（p.4-4）（必須）
- OIR のディセーブル化（p.4-4）（必須）
- IKE ポリシーの設定（p.4-5）（必須）
- トランスフォーム セットの設定（p.4-6）（必須）
- IPSec の設定（p.4-10）（必須）
- 圧縮の設定（p.4-17）（任意）
- IPSec の設定例（p.4-20）（任意）
- IKE および IPSec の設定の確認（p.4-21）（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。オンライン マニュアル『*Configuring the VPN Acceleration Module*』（http://www.cisco.com/univercd/cc/td/doc/product/core/7100/7100pacn/vam1/vamconf.htm）を参照してください。

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」を参照）。

EXEC コマンド インタープリタの使用方法

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。

OIR のディセーブル化

SA-VAM2 では、デフォルトで Online Insertion and Removal（OIR; ホットスワップ）がイネーブルです。

SA-VAM2 の OIR 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 モードを開始し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 accelerator** *<slot number>*	SA-VAM2 の OIR をディセーブルにします。
ステップ 2	**crypto engine accelerator** *<slot number>*	SA-VAM2 の OIR をイネーブルにします。

OIR をディセーブルおよびイネーブルにする手順は、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」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 モードを開始して、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 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 DES 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 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** ― 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 nonces を認証方式として指定します。 **（注）** Cisco IOS Release 12.3(10) 以降では、rsa-encr は SA-VAM2 暗号化カードでイネーブルです。 • **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）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。

	コマンド	目的
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。
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** ― 1024 ビット DH グループを指定します。 ***5*** ― 1536 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」を参照してください。

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 モードを開始して、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 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	**clear crypto sa** または **clear crypto sa peer** {*ip-address* | *peer-name*} または **clear crypto sa map** *map-name* または **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 **entry** キーワードを指定します。

表 4-1 に、Authentication Header（AH）および Encapsulating Security Payload（ESP）プロトコル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（最大で 1 つを選択）	**ah-md5-hmac**	Message Digest 5（MD5）（HMAC バリアント）認証アルゴリズムを使用する AH
	ah-sha-hmac	Secure Hash Algorithm（SHA）（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 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 Data Encryption Standard（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 つまり 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（最大で 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
IP 圧縮トランスフォーム（最大で 1 つを選択）	**comp-lzs**	Lempel-Ziv-Stac（LZS）アルゴリズムを使用する IP 圧縮

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*** および ***esp-des*** および ***esp-sha-hmac***
- ***comp-lzs***

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、データ認証および抗リプレー サービスを提供します。

ESP は、パケット認証のほかに、任意選択でデータ認証および抗リプレー 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 データの整合性には、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るので注意してください。

（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-eas*** および ***esp-sha-hmac***
- ***ah-sha-hmac*** および ***esp-eas*** 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で置き換えられます。

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、旧来のトランスフォームしかサポートしない 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
```

次に、入力した IPSec トランスフォームがハードウェアでサポートされていない場合に表示される警告メッセージの例を示します。

```
crypto ipsec transform transform-1 esp-aes 256 esp-md5
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

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」を参照してください。

IPSec の設定についての詳細は、『*Cisco IOS Security Configuration Guide*』の「Configuring IPSec Network Security」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、グローバル コンフィギュレーション 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
ステップ 1	`Router(config)# crypto ipsec security-association lifetime seconds seconds`	IPSec SA のグローバル ライフタイム（時間）を変更します。 このコマンドを使用した場合、SA は指定した秒数が経過すると期限切れになります。
ステップ 2	`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。 このコマンドを使用した場合、SA を使用する IPSec「トンネル」を指定した量（単位：キロバイト）のトラフィックが通過した時点で、SA が期限切れになります。

ステップ 3	`Router(config)# clear crypto sa`
	
	または
	
	`Router(config)# clear crypto sa peer {ip-address | peer-name}`
	
	または
	
	`Router(config)# clear crypto sa map map-name`
	
	または
	
	`Router (config)# clear crypto sa entry 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 **entry** 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される 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」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-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 を使用しない場合は、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。）

	コマンド	目的
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。）
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。

	コマンド	目的
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）。
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 つずつの 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**]	（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）を要求するか、または IPSec ピアから受信する要求に PFS が含まれていなければならないことを指定します。
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。 このコマンドは、ダイナミック クリプト マップ エントリではめったに設定しません。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。

	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）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。

ステップ 6	`Router(config-crypto-m)# set pfs [group1 | group2]`	（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 を要求するか、または IPSec ピアから受信する要求に PFS が含まれていなければならないよう指定します。
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。

圧縮の設定

ここで説明する内容は次のとおりです。

- IKE ポリシーの設定（必須）
- IKE 事前共有鍵の設定（必須）
- IPSec トランスフォーム セットの設定（必須）
- アクセス リストの設定（必須）
- クリプト マップの設定（必須）
- クリプト マップのインターフェイスへの適用（必須）

IPSec の設定例は、「圧縮の設定例」を参照してください。

IPSec の設定についての詳細は、『*Cisco IOS Security Configuration Guide*』の「Configuring IPSec Network Security」を参照してください。

IKE ポリシーの設定

IKE ポリシーを設定するには、「IKE ポリシーの設定」（p.4-5）の手順に従い、グローバル コンフィギュレーション モードのコマンドを使用します。

IKE 事前共有鍵の設定

ピア側で事前共有鍵を指定するには、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)# crypto isakmp key` *keystring* `address peer-address`
	
	または
	
	`Router (config)# crypto isakmp key` *keystring* `hostname peer-hostname`
		ローカル ピア：
		特定のリモート ピアと使用する共有鍵を指定します。
		
		リモート ピアがアドレスを使用して ISAKMP アイデンティティを指定している場合は、このステップで **address** キーワードを使用します。そうでない場合は、このステップで **hostname** キーワードを使用します。

ステップ 2	`Router (config)# crypto isakmp key_`*keystring* `address peer-address`
	
	または
	
	`Router (config)# crypto isakmp key_`*keystring* `hostname peer-hostname`
		リモート ピア：
		ローカル ピアと使用する共有鍵を指定します。これはローカル ピアで指定した鍵と同じです。
		
		ローカル ピアがアドレスを使用して ISAKMP アイデンティティを指定している場合は、このステップで **address** キーワードを使用します。そうでない場合は、このステップで **hostname** キーワードを使用します。

ステップ 3	各リモート ピアについて、上記の 2 ステップを繰り返します。	

IKE ポリシーで事前共有鍵を使用するピアごとに、これらの作業を繰り返します。

IPSec 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（セキュリティ プロトコルとアルゴリズムの可能な組み合わせ）を定義するには、**crypto ipsec transform-set** グローバル コンフィギュレーション コマンドを使用します。トランスフォーム セットを削除するには、このコマンドの **no** 形式を使用します。

コマンド	目的
`Router (config)# crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]`	*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* IPSec セキュリティ プロトコルおよびアルゴリズムを定義するトランスフォームを最大 3 つ（最低でも 1 つ）指定します。

アクセス リストの設定

MAC（メディア アクセス制御）アドレス アクセス リストを設定するには、**access-list** グローバル コンフィギュレーション コマンドを使用します。特定のアクセス リスト エントリを削除するには、このコマンドの **no** 形式を使用します。

コマンド	目的
`Router (config)# access-list access-list-number {permit | deny} address mask`	*access-list-number* このリストの番号（700 ～ 799 の範囲の整数）を指定します。 **permit** フレームを許可します。 **deny** フレームを禁止します。 *address mask* 48 ビットの MAC アドレス（ドット付きの 3 つの数字列で表記）を指定します。この引数で 1 のビットが、アドレス値で無視されるビットになります。

クリプト マップの設定

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`	クリプト マップを作成し、クリプト マップ コンフィギュレーション モードを開始します。
ステップ 2	`Router (config)# 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。

	コマンド	目的
ステップ 3	`Router (config)# 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）。
ステップ 4	`Router (config)# match address access-list-id`	拡張アクセス リストを指定します。このアクセス リストでは、トラフィックを IPSec で保護するものと、保護しないものを特定します。

クリプト マップのインターフェイスへの適用

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、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)# interface type number`	クリプト マップを適用するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router (config)# 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。
ステップ 3	`Router (config)# end`	インターフェイス コンフィギュレーション モードを終了します。

SA-VAM2 に圧縮を設定する手順は、これで完了です。

IPSec のモニタリングおよびメンテナンス

IPSec SA を消去（再初期化）するには、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

コマンド	目的

`Router(config)# clear crypto sa`
 	
または
 	
`Router(config)# clear crypto sa peer {ip-address | peer-name}`
 	
または
 	
`Router(config)# clear crypto sa map map-name`
 	
または
 	
`Router(config)# clear crypto sa entry 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 **entry** 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。

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。IKE の詳細については、「Configuring Internet Key Exchange Security Protocol」を参照してください。

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。

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** 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、その後、SA のネゴシエーションが行われて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（再初期化）するには、グローバル コンフィギュレーション モードで表 4-2 のいずれかのコマンドを使用します。

表 4-2　IPSec SA を消去するコマンド

コマンド	目的
clear crypto sa または **clear crypto sa peer** {*ip-address* | *peer-name*} または **clear crypto sa map** *map-name* または **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」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（p.4-24）
- IPSec の設定例（p.4-24）
- 圧縮の設定例（p.4-25）

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。

圧縮の設定例

次に、圧縮を設定する簡単な例を示します。

IKE ポリシーの設定：

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

IKE 事前共有鍵の設定：

```
crypto isakmp key 12abcjhrweit345 address 16.0.0.2
```

IPSec トランスフォーム セットの設定：

```
crypto ipsec transform-set proposal_01 esp-3des esp-md5-hmac comp-lzs
```

アクセス リストの設定：

```
access-list 101 permit ip host 16.0.0.1 host 16.0.0.2
```

クリプト マップの設定：

```
crypto map MAXCASE 10 ipsec-isakmp
set peer 16.0.0.2
set transform-set proposal_01
match address 101
```

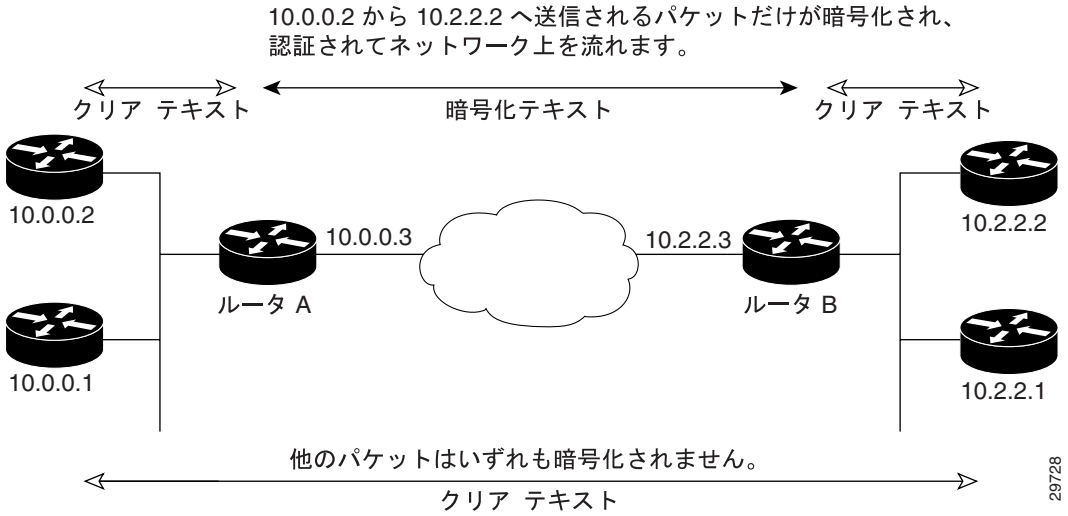
クリプト マップのインターフェイスへの適用：

```
interface FastEthernet1/0
crypto map MAXCASE
```

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
```

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
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
```

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
  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 SA-VAM2 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。たとえば、ルータのスロット 1 に SA-VAM2 が搭載されている場合、次のような出力が得られます。

```
Router# show diag
Slot 6:
        VAM2 Encryption/Compression engine, Port adapter
        Port adapter is analyzed
        Port adapter insertion time 00:01:32 ago
        EEPROM contents at hardware discovery:
        Hardware Revision        :1.0
        PCB Serial Number        :
        Part Number              :73-8491-00
        Board Revision           :
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        Deviation Number         :0-0
        Product Number           :SA-VAM2
        Top Assy. Part Number    :800-22836-00
        CLEI Code                :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00:04 FF 40 03 E4 41 01 00 C1 8B 00 00 00 00 00 00
          0x10:00 00 00 00 00 82 49 21 2B 00 42 00 00 03 00 81
          0x20:00 00 00 00 04 00 80 00 00 00 00 CB 94 53 41 2D
          0x30:56 41 4D 32 20 20 20 20 20 20 20 20 20 20 20 20
          0x40:20 C0 46 03 20 00 59 34 00 C6 8A 00 00 00 00 00
          0x50:00 00 00 00 00 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
```

SA-VAM2 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 pas vam interface** コマンドを入力します。次に、出力例を示します。

```
Router# show pas vam interface
VPN Acceleration Module Version II in slot : 3
        Statistics for Hardware VPN Module since the last clear
         of counters 314 seconds ago
               5290894 packets in                    5290895 packets out
            1882478960 bytes in                   1327439698 bytes out
                 16850 paks/sec in                     16850 paks/sec out
                 47940 Kbits/sec in                    33805 Kbits/sec out
               4222173 pkts compressed                     0 pkts not compressed
            1190662374 bytes before compress        405331872 bytes after compress
                 2.9:1 compression ratio               2.9:1 overall
                    58 commands out                       58 commands acknowledged
               Last 5 minutes:
               4855704 packets in                    4855705 packets out
                 16185 paks/sec in                     16185 paks/sec out
              46723079 bits/sec in                  32921855 bits/sec out

Errors:
           ppq full errors         :        0   ppq rx errors           :        0
           cmdq full errors        :        0   cmdq rx errors          :        0
           no buffer               :        0   replay errors           :        0
           dest overflow           :        0   authentication errors   :        0
           Other error             :        0   RNG self test fail      :        0
           DF Bit set              :        0   Hash Miscompare         :        0
    Unwrappable object      :        0   Missing attribute       :        0
           Invalid attrribute value:        0   Bad Attribute           :        0
           Verification Fail       :        0   Decrypt Failure         :        0
           Invalid Packet          :        0   Invalid Key             :        0
           Input Overrun           :        0   Input Underrun          :        0
           Output buffer overrun   :        0   Bad handle value        :        0
           Invalid parameter       :        0   Bad function code       :        0
           Out of handles          :        0   Access denied           :        0

        Warnings:
           sessions_expired        :        0   packets_fragmented      :        0
           general                 :        0   compress_bypassed       :        4

        HSP details:
           hsp_operations          :       75   hsp_sessions            :        6
```

SA-VAM2 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、SA-VAM2 に送信されたパケット数を示します。[packets in] カウンタは、SA-VAM2 から受信したパケット数を示します。

(注) **show pas vam interface** コマンドの出力には [compression ratio] が含まれますが、これは圧縮されたパケットと IPSec ヘッダーに対する元のパケットの比率（すなわちトンネル帯域幅の効率性）を示しています。これは圧縮された IPSec ペイロードと圧縮前の IPSec ペイロードとの比率を示しているわけではありません。

この比率は、パケットが小さく圧縮できない場合には 1 まで低下し、暗号化されたパケットと IPSec ヘッダーを加えたものに対する、暗号化されていないパケットの比率になります。

IKE/IPSec パケットが SA-VAM2 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 SA-VAM2 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 Layer :  ACTIVE
 Number of crypto engines = 1 .

 CryptoEngine-0 (slot-5) details.
 Capability-IPSec :IPPCP, 3DES, AES, RSA

 IKE-Session   :    0 active,  5120 max, 0 failed
 DH-Key        :    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。

起動時または OIR 時に、Cisco IOS ソフトウェアが SA-VAM2 に暗号トラフィックを転送することで合意した場合、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-1
    ...switching to hardware crypto engine
```

SA-VAM2 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 <slot>
    Router#
    3w4d:%ISA-6-SHUTDOWN:VAM2 shutting down
    3w4d:%ISA-6-INFO:Crypto Engine 0 in slot 1 going DOWN
    3w4d:...switching to software crypto engine
```

SA-VAM2 のモニタおよびメンテナンス

SA-VAM2 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 pas isa interface**	ISA インターフェイスの設定を表示します。
Router# **show pas isa controller**	ISA コントローラの設定を表示します。
Router# **show pas vam interface**	SA-VAM2 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 pas vam controller**	SA-VAM2 コントローラの設定を表示します。
Router# **Show version**	インターフェイスの一部として統合サービス アダプタを表示します。

A

access-list 暗号化コマンド　4-12

C

clear crypto sa コマンド　4-19, 4-22
crypto dynamic-map コマンド　4-15
crypto ipsec security-association lifetime コマンド　4-11
crypto map コマンド　4-12, 4-13
crypto sa コマンド、clear　4-22

E

ESD の防止　2-5
EXEC コマンド インタープリタ　4-4

I

IKE
　設定　4-4
　ポリシーの設定例　4-24
IPSec
　アクセス リスト　4-10
　確認　4-22
　トランスフォーム セット
　　定義　4-7
IPSec の基本設定　4-26
　図　4-25
IPSec の設定　4-26
IPSec（IPSec ネットワーク セキュリティ プロトコル）
　クリプト アクセス リスト　4-12
　　作成　4-12
　クリプト マップ
　　エントリ、作成　4-12 - 4-16
　　ダイナミック
　　　作成　4-15
　　　定義　4-15
　設定　4-19
　　（例）　4-20
　トランスフォーム
　　使用できる組み合わせ　4-8
　　選択　4-9
　　変更　4-10

L

LED　1-9
　SA-VAM　1-4, 1-9

M

match address コマンド　4-13, 4-15
MIB　1-8

R

RFC　1-8

S

sa コマンド、clear crypto　4-22
SA（セキュリティ アソシエーション）
　消去　4-11, 4-19
　ライフタイム
　　グローバルな値、設定　4-11
set peer コマンド　4-13, 4-15
set pfs コマンド　4-14, 4-16
set security-association level per-host コマンド　4-14
set security-association lifetime コマンド　4-14, 4-16
set session-key コマンド　4-13
set transform-set コマンド　4-13, 4-14, 4-15
show crypto dynamic-map コマンド　4-20

show crypto ipsec sa コマンド　4-20
show crypto ipsec security-association lifetime コマンド　4-20
show crypto ipsec transform-set コマンド　4-20
show crypto map コマンド　4-20

V

VAM
　概要　ix, 4-2
　機能　1-6
　ソフトウェア要件　2-3
　取り扱い　3-2
　モニタおよびメンテナンス　4-30
VPN Acceleration Module（VAM を参照）　1-2

あ

アクセラレーション モジュール、VPN（VAM を参照）　1-2
安全上の警告　2-5
安全に関する注意事項　2-5

い

インタープリタ、EXEC コマンド　4-4

き

規格
　サポート対象　1-8
機器
　電気製品の取り扱いに関する注意事項　2-5
　必要な工具　2-2

く

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、開始　4-9

け

警告および注意事項　3-3
警告、安全上　2-5
ケーブル、コネクタ、ピン割り当て　1-11

こ

コマンド
　clear crypto sa　4-22
　crypto isakmp policy　4-4
コマンド インタープリタ、EXEC　4-4

せ

静電気放電
　破壊防止　2-5
静電破壊
　ESD の防止を参照
設定
　IKE　4-4
　IKE の例　4-24
　IPSec の例　4-24
　確認　4-28
　基本的な IPSec　4-26
　作業　4-3
　ルータ A の例　4-26
　ルータ B の例　4-27
　例　4-24
設定、IPSec
　例　4-24

そ

ソフトウェア
　要件　2-3

ち

注意事項、安全に関する　2-5
注意事項、および警告　3-3
注意事項、電気製品の取り扱いに関する　2-5

て

データ暗号化
　概要　1-6
適合
　FCC クラス A　2-6
　暗号化に関する米国輸出規制法　2-6
電気製品の取り扱いに関する注意事項　2-5

と

トラブルシューティングのヒント　4-28

は

ハードウェアおよびソフトウェアの互換性　x, 2-3
ハードウェア要件　2-2

ひ

必要な工具および機器　2-2
ヒント、トラブルシューティング　4-28

ほ

防止、ESD　2-5
ホットスワップ　3-2

ま

マニュアル
　関連資料　x

め

メンテナンス、VIP のインストレーションに必要な部品
　2-2

も

モジュール、VPN アクセラレーション（VAM を参照）
　1-2

よ

要件
　ハードウェア　2-2