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

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

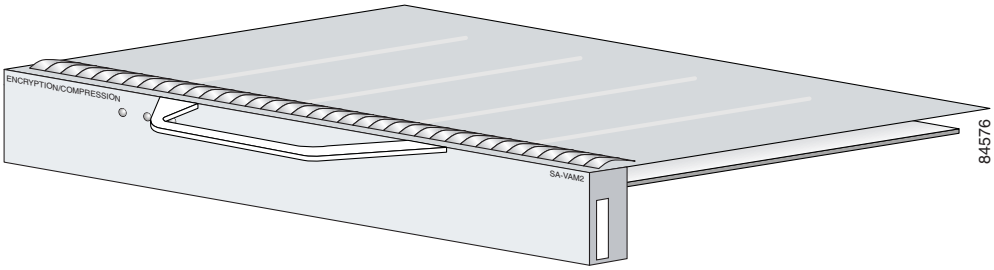
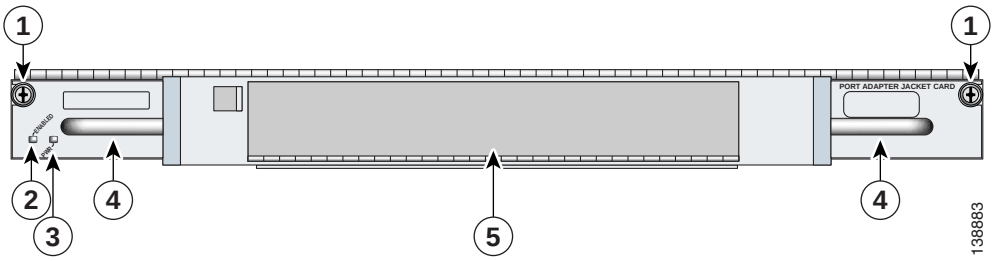


図 1-2　NPE-G1 を搭載した Cisco 7200VXR の Port Adapter Jacket Card の前面プレート



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。

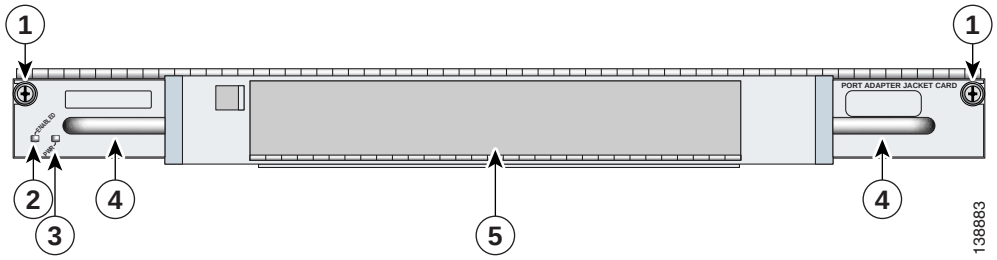
どちらかの条件が満たされていない場合、またはほかの理由でルータを初期化できなかった場合、ENABLE LED は点灯しません。

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。

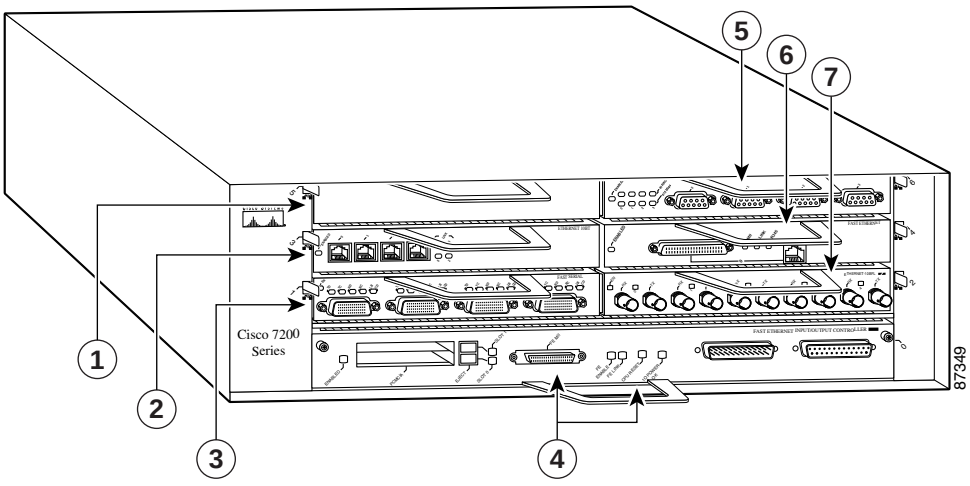
SA-VAM2 は、Cisco 7301 ルータおよび Cisco 7200VXR ルータのポート アダプタ スロットに搭載します。

（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

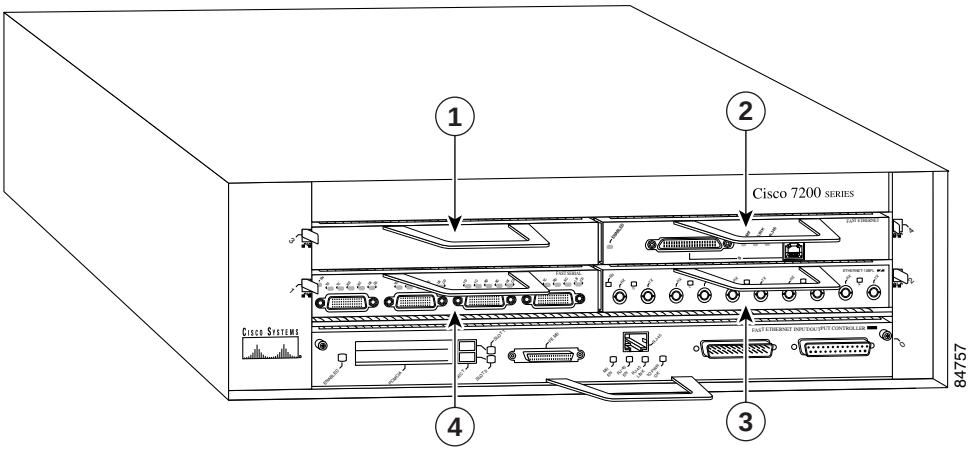
Cisco 7200VXR ルータのスロット番号を、図 1-5、図 1-6、および図 1-7 に示します。

図 1-5　Cisco 7206 のスロット番号



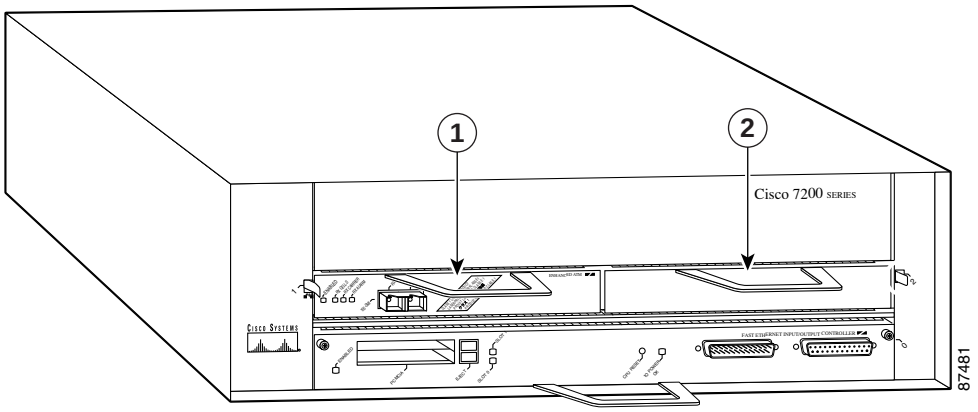
1	ポート アダプタ スロット 5（左側のバス）	5	ポート アダプタ スロット 6（右側のバス）
2	ポート アダプタ スロット 3（左側のバス）	6	ポート アダプタ スロット 4（右側のバス）
3	ポート アダプタ スロット 1（左側のバス）	7	ポート アダプタ スロット 2（右側のバス）
4	ポート アダプタ スロット 0（左側のバス）		

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



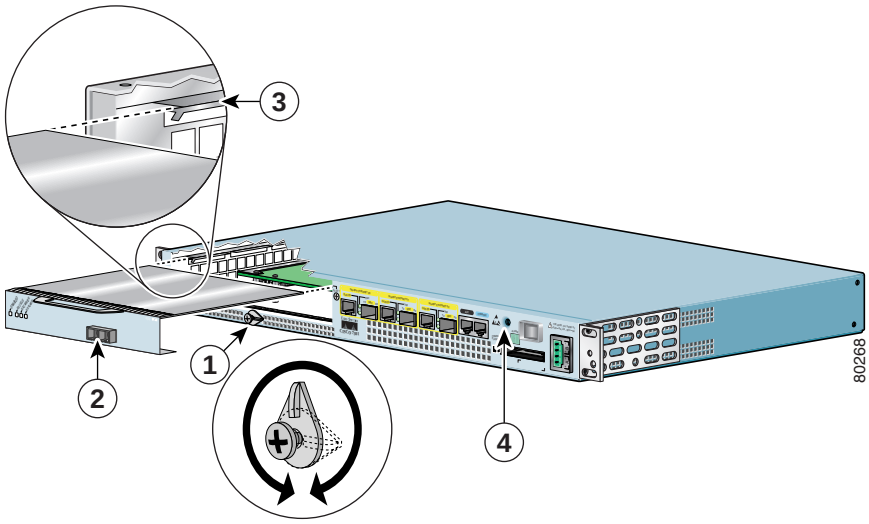
1	ポート アダプタ スロット 1	**2**	ポート アダプタ スロット 2

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