概要

この章では、VPN Acceleration Module 2+（SA-VAM2+）の概要を説明します。内容は次のとおりです。

データ暗号化の概要

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

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

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

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

- DES および Triple DES — DES および Triple DES（3DES）暗号化パケット データです。Cisco IOS ソフトウェアは、Triple DES および DES-CBC with Explicit IV を実装します。Cipher Block Chaining（CBC）は、暗号化の開始に Initialization Vector（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、次のような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 56 ビット DES-CBC with Explicit IV 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（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。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。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。

SA-VAM2+ 概要

VPN Acceleration Module 2+（SA-VAM2+）は、NPE-225、NPE-400、NPE-G1、または NPE-G2 プロセッサを搭載した Cisco 7204VXR と Cisco 7206VXR 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ポート アダプタです（図 1-1 を参照）。

SA-VAM2+ はハードウェアおよび HSP ソフトウェア上での 192/256 ビット AES、DES、Triple DES、および IPv6 IPSec 機能を持ち、サイト間およびリモートアクセス IPSec VPN サービスのパフォーマンスを強化します。Cisco SA-VAM2+ はハードウェアが処理するレイヤ 3 圧縮サービスに暗号化サービスを提供し、帯域を保護してセキュアなリンクに対するネットワーク接続コストを低減します。また、完全なレイヤ 3 ルーティング、Quality Of Service（QoS; サービス品質）、マルチキャストおよびマルチプロトコル トラフィック、統合 LAN/WAN メディアの幅広いサポートも提供します。

SA-VAM2+ は、Cisco 7000VXR シリーズ ルータおよび Cisco 7301 ルータのポート アダプタ スロットに直接搭載できます（図 1-5 を参照）。または SA-VAM2+ を Port Adapter Jacket Card（製品番号：C7200-JC-PA）に装着し、NPE-G1 または NPE-G2 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、Virtual Private Network（VPN; 仮想私設網）のパフォーマンスを維持しながら NPE-G1 または NPE-G2 のパフォーマンスを向上させることができるという利点があります。Port Adapter Jacket Card に SA-VAM2+ を装着すると、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。詳細は『*Port Adapter Jacket Card Installation Guide*』を参照してください。

図 1-1　SA-VAM2+

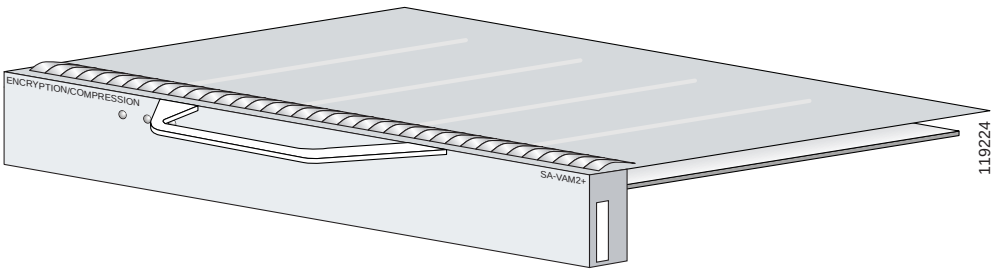
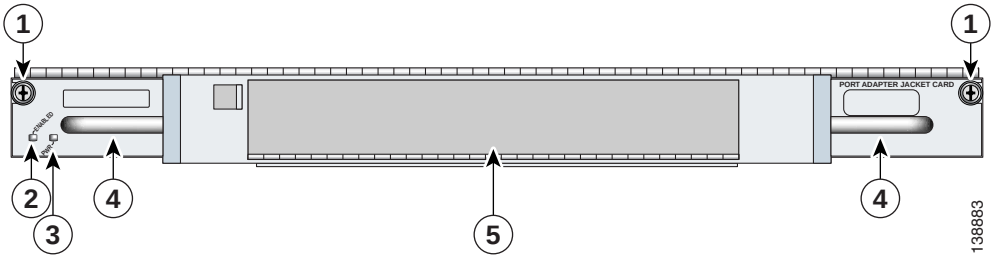


図 1-2　Port Adapter Jacket Card の前面プレート



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。

- 56 ビット キーの DES 標準モード : CBC
- Triple DES（168 ビット）アルゴリズム、最大速度 292 Mbps
- ハードウェア上での 128/192/256 ビット AES
- 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、最大 5,000 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（LZS）
- SHA-1 および MD5 ハッシュ アルゴリズム
- Rivest, Shamir, Adelman（RSA）公開鍵アルゴリズム
- Diffie-Hellman グループ 1、2、5
- Online Insertion and Removal（OIR; ホットスワップ）

機能

ここでは、SA-VAM2+ の機能について表 1-1 で説明します。

表 1-1　SA-VAM2+ 機能

機能	説明 / 利点
スループット[1]	最大 292 Mbps（Cisco 7200VXR ルータで 3DES を使用）、最大 392 Mbps（Cisco 7301 ルータで 3DES を使用） **（注）** IPSec トンネルの数はパケット サイズによって異なります。
IPSec で保護されるトンネル数[2]	最大 5,000 トンネル[3]
毎秒トンネル数	最大 50
ハードウェアベースの暗号化	データ保護：IPSec DES、3DES、AES、IPv6 IPSec 認証：RSA および Diffie-Hellman データ完全性：SHA-1 および MD5
VPN トンネリング	IPSec トンネル モード：IPSec による Generic Routing Encapsulation（GRE）および Layer 2 Tunneling Protocol（L2TP）保護
ハードウェアベースの圧縮	レイヤ 3 IPPCP LZS
サポートする標準	IPSec/IKE：RFC 2401 ～ 2411、2451 IPPCP：RFC 2393、2395
（任意）Port Adapter Jacket Card	Port Adapter Jacket Card は、NPE-G1 または NPE-G2[4] プロセッサを搭載した Cisco 7200VXR ルータで利用可能です。 **（注）** NPE-G1 を搭載した Cisco 7200VXR ルータでサポートされる Port Adapter Jacket Card は、Cisco IOS Release 12.4(6)T および 12.4(7) 以上で利用可能です。 NPE-G2 を搭載した Cisco 7200VXR ルータでサポートされる Port Adapter Jacket Card は、Cisco IOS Release 12.4(4)XD 以上で利用可能です。

1. IPSec 3DES HMAC-SHA1 を使用し、1,400 バイト パケットで測定
2. サポートされるトンネル数は、搭載メモリの合計によって異なります。
3. 5,000 トンネルをサポートするには、512 MB のメモリが必要です。
4. NPE-G2 を搭載した Cisco 7200VXR ルータは、Cisco IOS ソフトウェア バージョン 12.4(4)XD でのみ利用可能です。

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　SA-VAM2+ のパフォーマンス

Cisco ルータ	スループット[1,2]	内容
Cisco 7301	最大 392 Mbps	Cisco IOS リリース：c7301-jk9o3s-mz.123-10[2] 7301/ シングル SA-VAM2+、1 GB システム メモリ 3DES/SHA、IKE キープアライブ設定なし
	最大 396 Mbps	Cisco IOS リリース：c7301-jk9o3s-mz.123-10[2] 7301/ シングル SA-VAM2+、1 GB システム メモリ AES/SHA、IKE キープアライブ設定なし
Cisco 7200VXR（NPE-G1 または NPE-G2 を搭載）	最大 263 Mbps	Cisco IOS リリース：c7200-jk9o3s-mz.124-4.T1[3] 7200VXR/NP-G1（700 Mhz）/ シングル SA-VAM2+、 512 MB システム メモリ 3DES/SHA、IKE キープアライブ設定なし
	最大 222 Mbps	Cisco IOS リリース：c7200-jk9o3s-mz.124-4.T1[3] 7200VXR/NP-G1（700 Mhz）/ シングル SA-VAM2+、 512 MB システム メモリ AES/SHA、IKE キープアライブ設定なし
	最大 391 Mbps	Cisco IOS リリース：c7200-jk9o3s-mz.124-4.T1[3] 7200VXR/NP-G1（700 Mhz）/ デュアル SA-VAM2+、 512 MB システム メモリ 3DES/SHA、IKE キープアライブ設定なし
	最大 391 Mbps	Cisco IOS リリース：c7200-jk9o3s-mz.124-4.T1[3] 7200VXR/NP-G1（700 Mhz）/ デュアル SA-VAM2+、 512 MB システム メモリ AES/SHA/IPSec/Tunnel モード、共有済み
Cisco 7200VXR（NPE-400 を搭載）	最大 248 Mbps	Cisco IOS リリース：c7200-jk9o3s-mz.124-4.T1 7200VXR/NPE400/SA-VAM2+、512 MB システム メモリ 3DES/SHA、IKE キープアライブ設定なし
	最大 251 Mbps	Cisco IOS リリース：c7200-jk9o3s-mz.124-4.T1 17200VXR/NPE400/ シングル SA-VAM2+、512 MB システム メモリ AES/SHA、IKE キープアライブ設定なし
Cisco 7200VXR（NPE-225 を搭載）	最大 191 Mbps	Cisco IOS リリース：c7200-jk9o3s-mz.123-10[2] 7200VXR/NPE225/ シングル VAM2、256 MB システム メモリ 3DES/SHA、IKE キープアライブ設定なし

1. IPSec 3DES HMAC-SHA-1 を使用し、1,400 バイト パケットで測定。パフォーマンスは、モジュールの数、帯域、トラフィック量、Cisco IOS リリースなどによって変化します。
2. Cisco 12.3-10 イメージを使用。パフォーマンスは Cisco IOS リリースによって変化します。Cisco 7200VXR または Cisco 7301 ルータの最新イメージのダウンロードを推奨します。
3. NPE-G2 を使用する場合、イメージは c7200p-adventerprisek9-mz.124-4.XD1 になります。

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

OIR

SA-VAM2+

SA-VAM2+ では OIR がサポートされます。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。ポート経由でトラフィックが流れているときに 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。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。

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+LED

表 1-3　SA-VAM2+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。

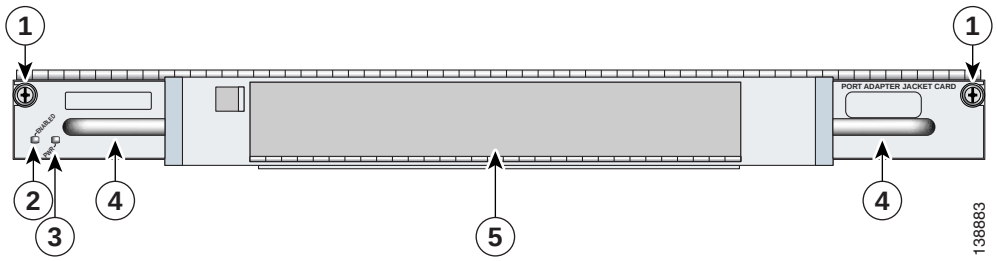
- SA-VAM2+ がバックプレーンに正しく接続されていて、電力が供給されている。
- システム バスが SA-VAM2+ を認識している。

いずれ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。

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+）スロット
3	PWR（電源）LED		

表 1-4　Port Adapter Jacket Card の LED

LED	カラー	機能
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 は電力が供給されています。
	オフ	Port Adapter Jacket Card は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。

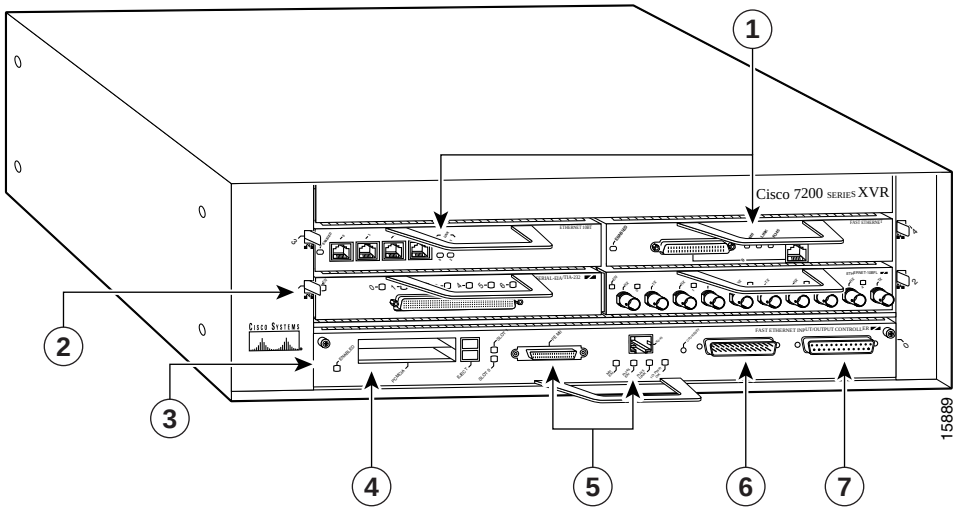
SA-VAM2+ は、Cisco 7200VXR シリーズ ルータおよび Cisco 7301 ルータのポート アダプタ スロットでサポートされます。また、Port Adapter Jacket Card に装着して、NPE-G1 または NPE-G2 プロセッサを搭載する Cisco 7200VXR ルータの I/O コントローラ ポートに取り付けることでもサポートされます。

（注）　ポート アダプタ使用しないポート 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 I/O コントローラおよびポートを、図 1-5 に示します。

図 1-5　Cisco 7200VXR のスロット番号



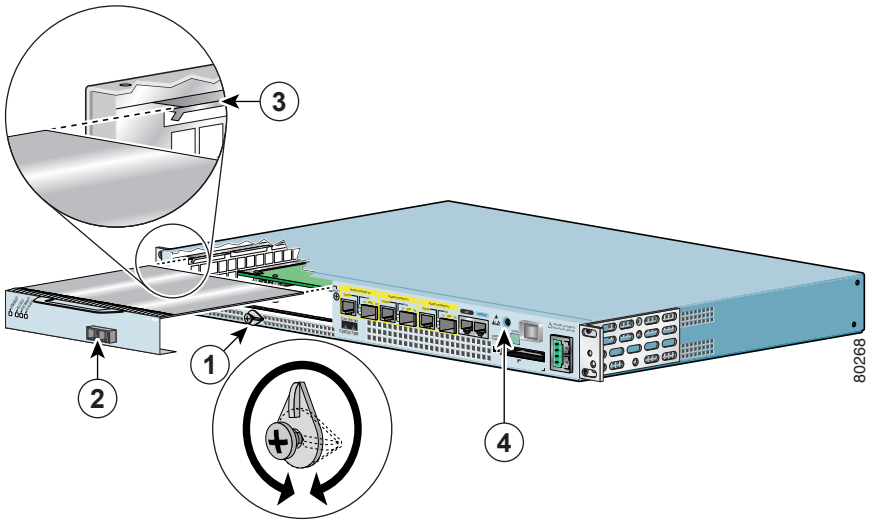
1	ポート アダプタ	5	MII および RJ-45 ファスト イーサネット ポート
2	ポート アダプタ ラッチ	6	AUX ポート
3	I/O コントローラ	7	コンソール ポート
4	PC カード スロット		

Cisco 7301 ルータ

Cisco 7301 ルータのポート番号を、図 1-6 に示します。

（注）　Cisco 7301 ルータは、1 つの SA-VAM2+（ポート アダプタ）をサポートします。

図 1-6　Cisco 7301 のスロット番号



1	ラッチ	3	スロット ガイド
2	ポート アダプタ（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