概要

この章では、VPN Acceleration Module について説明します。内容は次のとおりです。

VAM の概要

VPN Acceleration Module（VAM）は、Cisco 7200 シリーズ 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。

（注）　Cisco 7100 シリーズおよび Cisco 7401ASR ルータの販売は終了しました。

VAM は、LAN/WAN メディアおよびすべてのレイヤ 3 ルーティング サービスをサポートします。VAM 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サービスを提供します。VAM 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。

VAM 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 Data Encryption Standard（DES; データ暗号化規格）標準モード : Cipher Block Chaining（CBC）
- 3 キー トリプル DES（168 ビット）
- Secure Hash Algorithm（SHA）-1 および Message Digest 5（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 鍵交換 RC4-40

VAM はサービス アダプタ（SA-VAM）として、またはサービス モジュール（SM-VAM）としてご利用いただけます。SA-VAM は Cisco 7100 シリーズ ルータ、Cisco 7200 シリーズ ルータ、および Cisco 7401ASR ルータでサポートされます。SM-VAM は Cisco 7100 シリーズ ルータ上でサポートされます。

データ暗号化の概要

ここでは、IPSec、IKE、および CA 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 スタンダードな枠組みで、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、データの認証、リプレイ攻撃防止サービス、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 — Internet Key Exchange（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 — Certificate Authority（CA; 認証局）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/ps1835/products_configuration_guide_chapter09186a00800ca7b2.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 およびトリプル DES — DES および Triple DES（3DES; トリプル DES）暗号化パケット データ。Cisco IOS は 3 キー トリプル DES および DES-CBC を Explicit IV とともに実装します。CBC は、暗号化の開始に Initialization Vector（IV; 初期化ベクター）が必要です。IV は IPSec パケット内に明示的に指定されます。
- MD5（HMAC 系）— 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 系）— 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 シグニチャおよび RSA 暗号化ナンス — RSA は公開鍵暗号システムで、Ron Rivest、Adi Shamir、および Leonard Adleman によって開発されたため RSA と呼ばれています。RSA シグニチャによって否認防止機能が提供され、RSA 暗号化ナンスによって否認機能が提供されます。詳細については、『*Exporting and Importing RSA Keys*』フィーチャ モジュール（http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541cf.html）を参照してください。

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 — 認証ヘッダーは、データ認証およびオプションのリプレイ攻撃防止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 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 系）です。AH プロトコルはリプレイ攻撃防止サービスを提供します。
- ESP — Encapsulating Security Payload は、データ プライバシ サービス、オプションのデータ認証、およびリプレイ攻撃防止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 および Explicit IV またはトリプル DES を実装します。また、認証アルゴリズムとして MD5 または SHA（HMAC 系）を実装します。最新の ESP プロトコルでは、リプレイ攻撃防止サービスを提供します。
- IPPCP — 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 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。

機能

ここでは、VAM の機能について説明します。

機能	説明 / 利点
スループット[1]	3DES で最大 145 Mbps
IPSec で保護されるトンネル数[2]	Cisco 7401ASR ルータで最大 5,000[3] Cisco 7200 シリーズ ルータで最大 5,000 Cisco 7100 シリーズ ルータで最大 3,000[3]
ハードウェアベースの暗号化	データ保護：IPsec DES および 3DES 認証：RSA および Diffie-Hellman データ整合性：SHA-1 および Message Digest 5（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
サポートする規格	IPsec/IKE：RFC 2401 ～ 2411、2451 IPPCP：RFC 2393、2395

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. Cisco 7100 シリーズおよび Cisco 7401ASR ルータの販売は終了しました。

サポート対象の規格、MIB、および RFC

ここでは、VAM でサポートされる規格、Management Information Base（MIB）、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-VAM および SM-VAM の LED について説明します。

SA-VAM

SA-VAM は Cisco 7200 シリーズ ルータ上でサポートされます。

（注）　Cisco 7100 シリーズ ルータおよび Cisco 7401ASR ルータの販売は終了しました。

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

図 1-1　SA-VAM の LED

表 1-1　SA-VAM の LED

LED のラベル	カラー	状態	機能
ENABLE	グリーン	点灯	VAM は通電状態で動作可能です。
BOOT	オレンジ	パルス[1]	VAM は稼働しています。
		点灯	VAM の起動中またはパケットが暗号化 / 復号化されています。
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。

1. 正常に起動すると、BOOT LED が［心拍］パターンで点滅し、VAM が動作していることを表します。暗号トラフィックが増えると、トラフィック レベルに比例してこの LED の表示レベルが上がります。

ENABLE LED は、次の条件が満たされた場合に点灯します。

- SA-VAM 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-VAM 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、またはルータを初期化できなかった場合、ENABLE LED は点灯しません。

SM-VAM

SM-VAM は Cisco 7100 シリーズ ルータ上でサポートされます。

SM-VAM には 3 つの LED があります（図 1-2 を参照）。表 1-2 に、SM-VAM LED のカラーと機能を示します。

図 1-2　SM-VAM の LED

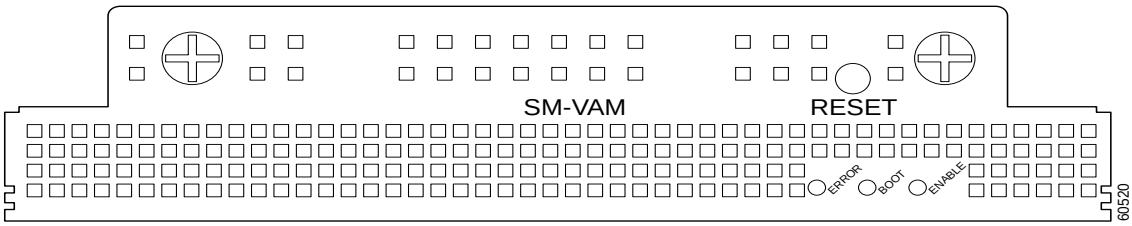


表 1-2　SM-VAM の LED

LED のラベル	カラー	状態	機能
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。
BOOT	オレンジ	パルス[1]	SM-VAM は稼働しています。
		点灯	SM-VAM の起動中またはパケットが暗号化/復号化されています。
ENABLE	グリーン	点灯	SM-VAM は通電状態で動作可能です。

1. 正常に起動すると、BOOT LED が［心拍］パターンで点滅し、VAM が動作していることを表します。暗号トラフィックが増えると、トラフィック レベルに比例してこの LED の表示レベルが上がります。

ENABLE LED は、次の条件が満たされた場合に点灯します。

- SM-VAM 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 SM-VAM 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、またはなんら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。

ケーブル、コネクタ、およびピン割り当て

VAM 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。

VAM のスロット位置

ここではサポート対象プラットフォームでの VAM およびポート アダプタのスロット位置について説明します。

VAM はサービス アダプタ（SA-VAM）として、またはサービス モジュール（SM-VAM）としてご利用いただけます。SA-VAM は、Cisco 7100 シリーズ ルータ、Cisco 7200 シリーズ ルータ、および Cisco 7401ASR ルータのポート アダプタ スロットに搭載します。SM-VAM は、Cisco 7100 シリーズ ルータのサービス モジュール スロットに搭載します。

各プラットフォームにおけるスロット位置の規定を図に示します。

- Cisco 7100 シリーズ ルータのスロット番号（p.1-8）
- Cisco 7200 シリーズ ルータのスロット番号（p.1-9）
- Cisco 7401ASR ルータのスロット番号（p.1-10）

Cisco 7100 シリーズ ルータのスロット番号

SM-VAM は、Cisco 7120 および Cisco 7140 ルータのサービス モジュール スロット 5 に搭載します（図 1-3 を参照）。SA-VAM は、Cisco 7120 ルータのポート アダプタ スロット 3、または Cisco 7140 ルータのポート アダプタ スロット 4 に搭載します（図 1-4 を参照）。

図 1-3　Cisco 7120 ルータのサービス モジュール スロット 5 に搭載した SM-VAM

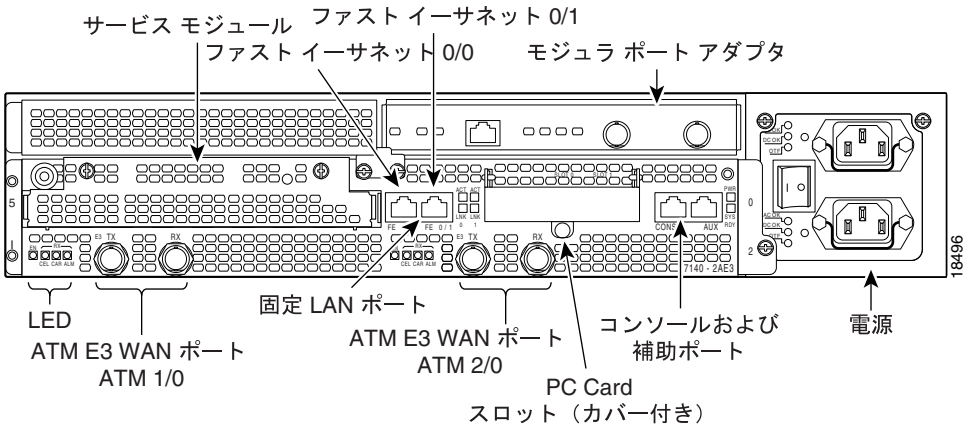
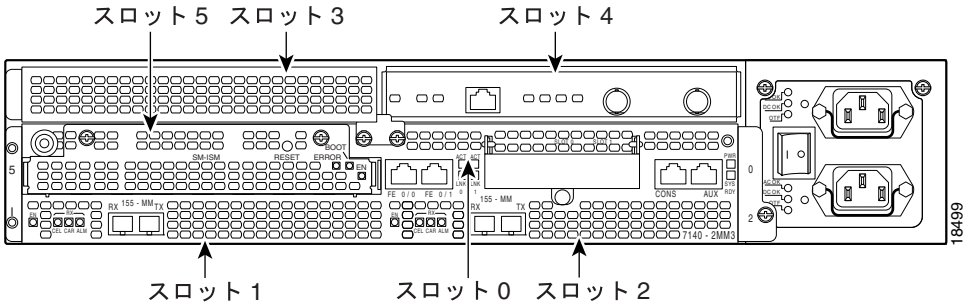


図 1-4　Cisco 7140 ルータのポート アダプタ スロット 4 に SA-VAM を搭載可能



Cisco 7200 シリーズ ルータのスロット番号

Cisco 7204 ルータ（図 1-5）および Cisco 7206 ルータ（図 1-6）の場合、シングル幅の任意のポート アダプタ スロットに SA-VAM を搭載できます。

（注）　Cisco 7200 シリーズ ルータの奇数スロットに PA-T3 または PA-FE を搭載している場合は、偶数スロットに VAM を搭載し、バスのロードバランスを図ってください。

図 1-5　Cisco 7204 ルータのポート アダプタ スロット

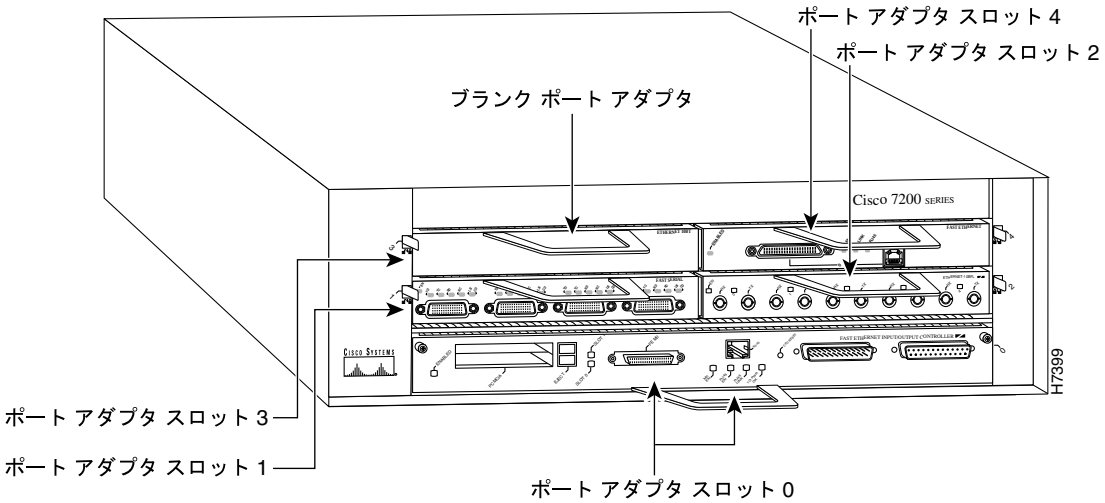
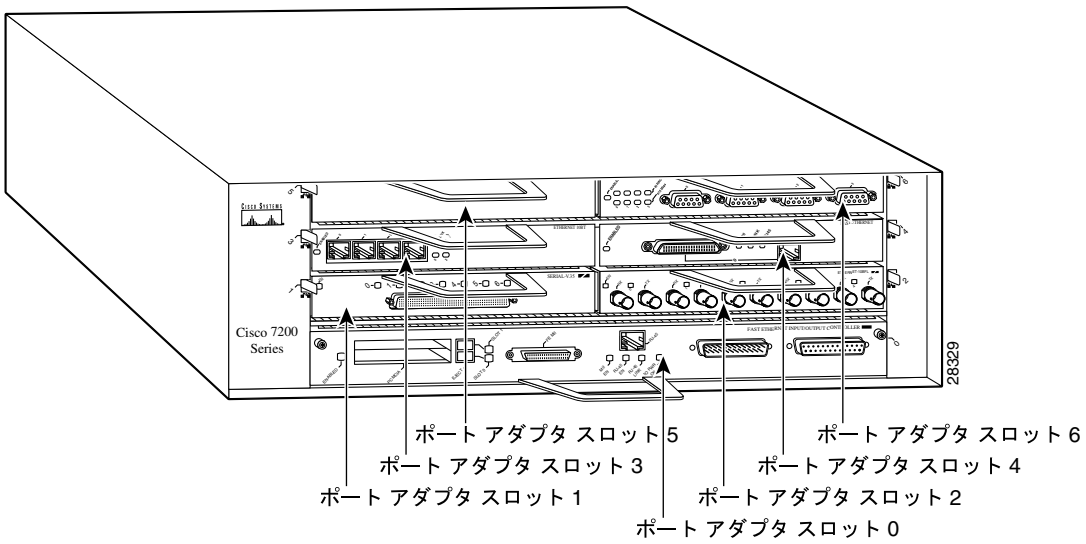


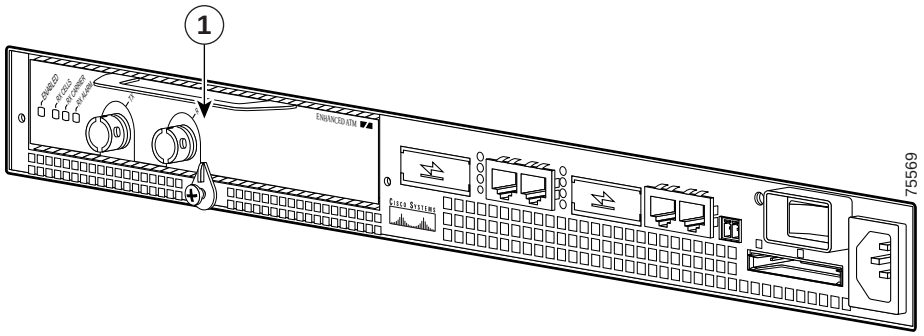
図 1-6　Cisco 7206 ルータのポート アダプタ スロット



Cisco 7401ASR ルータのスロット番号

Cisco 7401ASR ルータの場合、SA-VAM を搭載できるスロットは 1 つだけです（図 1-7 を参照）。

図 1-7　Cisco 7401ASR ルータのポート アダプタ スロット



1	ポート アダプタ スロット

（注）　インターフェイス ポートには、左から右へ、0 から始まる番号が割り振られています。