概要

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

データ暗号化の概要

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

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

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

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

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

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

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

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

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

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

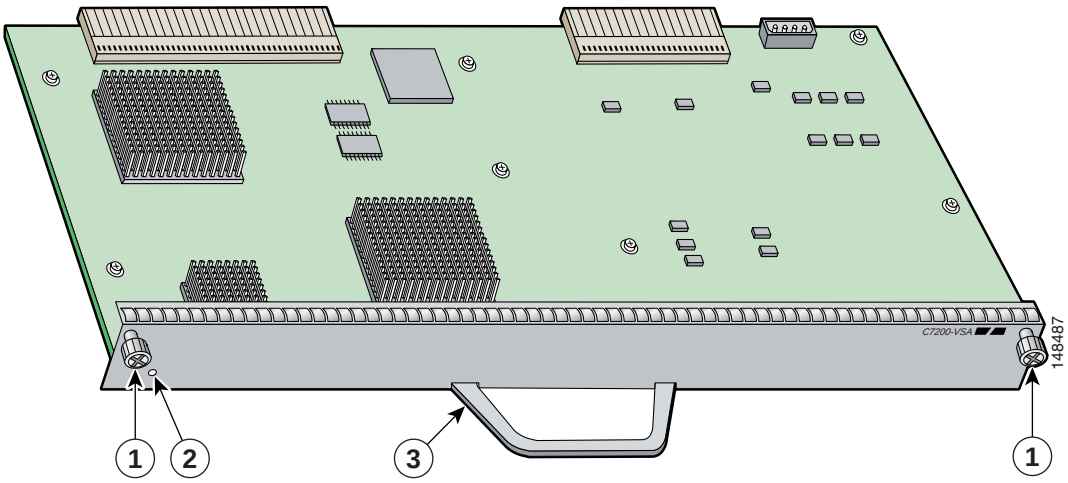
VSA の概要

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

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

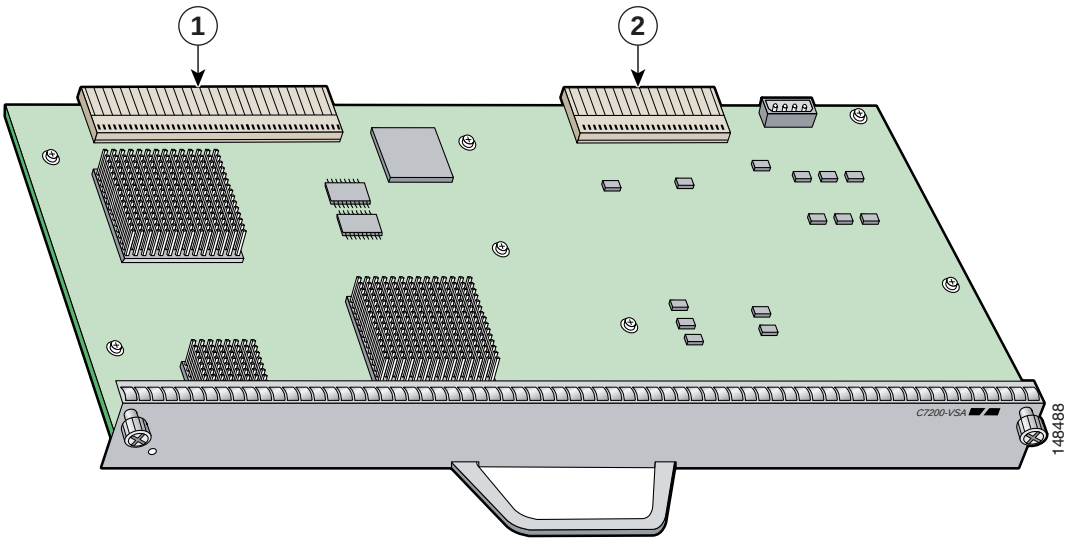
VSA は AES、DES、および Triple DES のハードウェア アクセラレーションを実行し、サイト間およびリモート アクセス IPSec VPN サービスのパフォーマンスを向上させます。Cisco C7200 VSA ソリューションは QoS（Quality of Service）、マルチキャストおよびマルチプロトコル トラフィック、統合型 LAN/WAN メディアの幅広いサポートを提供します。

図 1-1　VSA モジュール — 前面



1	ネジ	3	ハンドル
2	ステータス LED		

図 1-2　VSA モジュール — 背面コネクタ



1	ホスト IO バスおよび PCI-X バス	2	電源

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

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

必要なハードウェア

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

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

機能

ここでは、VSA の機能について表 1-1 で説明します。

表 1-1　VSA の機能

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

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

パフォーマンス

表 1-2 に VSA のパフォーマンス情報を示します。

表 1-2　VSA のパフォーマンス

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

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

サポート対象の規格、MIB、および RFC

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

規格

- IPSec/IKE：RFC 2401 ～ 2411、2451

MIB

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

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

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

RFC

- IPSec/IKE：RFC 2401 ～ 2411、2451

VSA のイネーブル / ディセーブル化

ここで説明する内容は次のとおりです。

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

稼働中の VSA のディセーブル化

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

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

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

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

イネーブル化 / ディセーブル化方式

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

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

表 1-4 に、システム稼働時の動作を示します。

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

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

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

表 1-4　システム稼働時

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

表 1-5　crypto engine コマンド

コマンド	VSA の動作

`Crypto engine slot 0`
`Crypto engine accelerator 0`
 	
（注） VSA はスロット 0（I/O コントローラ スロット）にのみ搭載可能です。
	このコマンドにより VSA が起動し、システムに暗号エンジンとして登録されます。
	
	この設定を実行し、VSA が現在ディセーブルになっている場合は、システムをリロードまたはリセットして VSA を起動します。
	
	（注） 引き続き現在の暗号エンジンが動作し、次のシステム リブート後に VSA が動作を引き継ぎます。

`No crypto engine slot 0` `No crypto engine accelerator 0`	これらの CLI コマンドは VSA をディセーブルにします。この設定を解除し、システムのリロードまたはリセットを実行するまで、VSA はディセーブルの状態を続けます。

LED

VSA には 1 つの LED があります（図 1-3 を参照）。

図 1-3　VSA の LED

表 1-6　VSA の LED

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

ENABLE LED は、次の条件が満たされた場合に点灯します。

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

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

コネクタ

VSA のコネクタについては、図 1-2 を参照してください。

スロット位置

ここで説明する内容は次のとおりです。

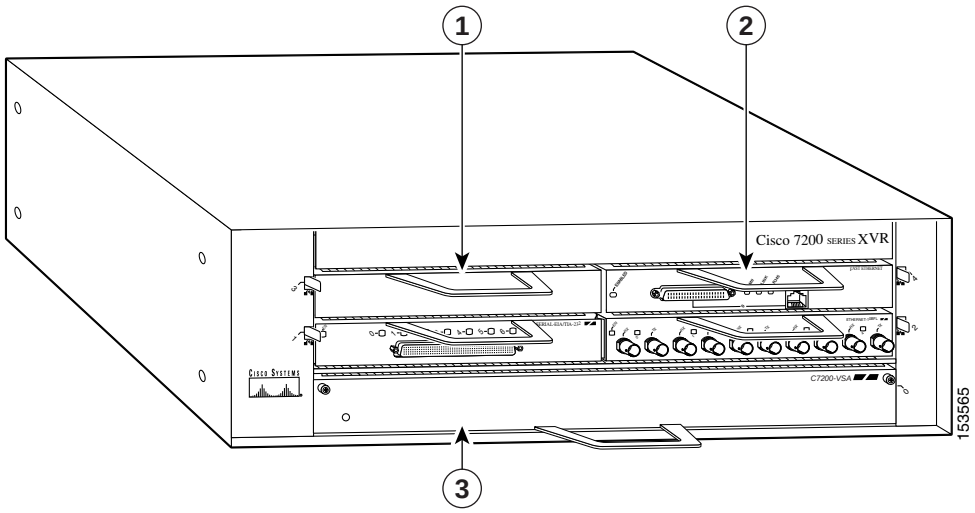
Cisco 7204VXR ルータのスロット番号については、図 1-4 を参照してください。

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

Cisco 7204VXR ルータ

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

図 1-4　Cisco 7204VXR ルータ — 前面

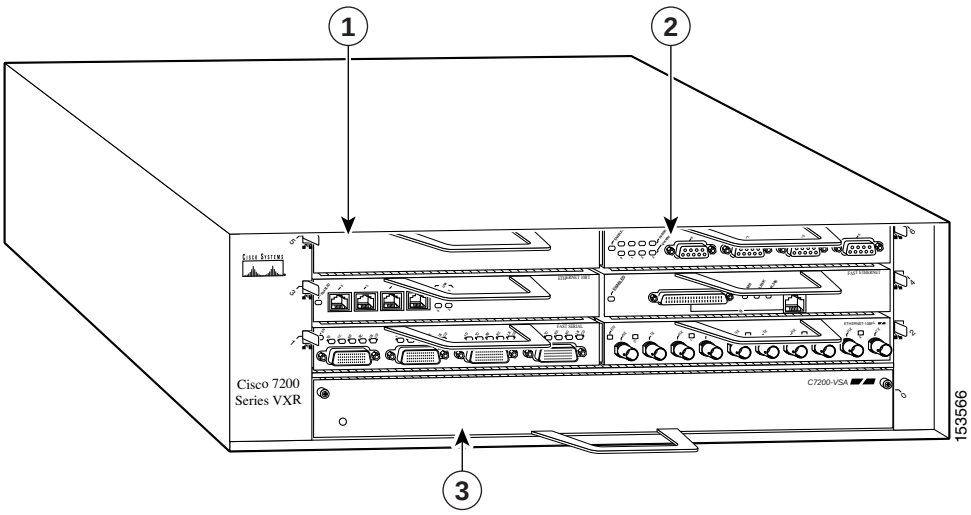


1	ポート アダプタ	3	I/O コントローラ スロットに搭載した VSA
2	ポート アダプタ レバー		

Cisco 7206VXR ルータ

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

図 1-5　Cisco 7206VXR — 前面



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