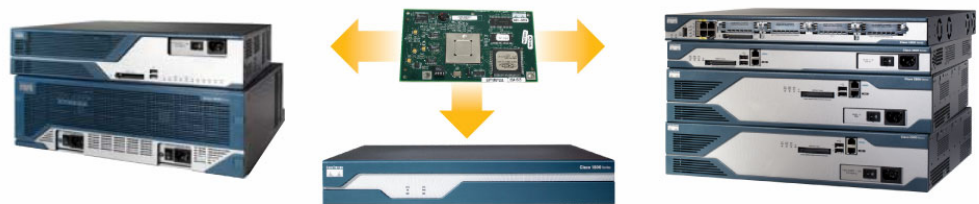


## Cisco ISR 1800/2800/3800 シリーズ用 VPN AIM

Cisco® ISR 1800/2800/3800 シリーズ サービス統合型ルータ用 Virtual Private Network (VPN; 仮想私設網) Advanced Integration Module (AIM) は、IP Security (IPSec) および Secure Sockets Layer (SSL) VPN 導入に最適化された Cisco ISR プラットフォームを構成します。

図 1 AIM-VPN/SSL モジュールを搭載したサービス統合型ルータ



Cisco ISR は、サイト間およびリモート アクセス接続に対応した VPN など、業界をリードする高度なセキュリティ サービスを提供します。Cisco VPN/SSL AIM は、Cisco ISR 1841 と Cisco ISR 2800 および 3800 シリーズ ルータにハードウェア暗号化アクセラレーションを提供し、Dynamic Multipoint VPN (DMVPN) などの堅牢な IPSec VPN の導入を可能にし、Cisco IOS® WebVPN SSL VPN のパフォーマンスを最適化します(図 1 を参照)。

Cisco VPN/SSL AIM は、内蔵の IPSec 暗号化に比べて IPSec VPN のパフォーマンスを最大 40 % 向上し、SSL Web VPN 暗号化の 2 倍のパフォーマンスを実現します。Cisco VPN/SSL AIM は、ハードウェアでの SSL 暗号化、Data Encryption Standard (DES; データ暗号化規格) または Advanced Encryption Standard (AES) を使用したハードウェアでの VPN IPSec 暗号化、およびハードウェアでの IP Payload Compression Protocol (IPPCP) の各機能をすべてサポートします。Cisco VPN/SSL AIM を搭載した Cisco ISR は、中堅・中小企業や小規模企業、および大規模企業のブランチ オフィスでの使用に適しており、リモート オフィス、モバイル ユーザ、およびパートナーのエクストラネットへの接続を提供します。Cisco ISR では、IPSec と SSL VPN を 1 つのシステムで導入できるため、複数のデバイスと管理システムを必要とする他のベンダーの製品と比べて、総所有コストを削減できます。また、Cisco VPN/SSL AIM はサービス プロバイダー向けに設計されており、容易な導入とスケーラブルな管理セキュリティ サービスを提供できます。

Cisco ISR は、Cisco VPN/SSL AIM や Cisco IOS Advanced Security 機能を組み合わせて使用することで、ルーティング、ファイアウォール、侵入防御に対応した豊富な統合パッケージを提供し、シスコの自己防衛型ネットワークに不可欠なコンポーネントとして機能します。

表 1 に、各プラットフォームでサポートされる VPN モジュール ハードウェアと機能を示します。表 2 に、Cisco VPN/SSL AIM でサポートされる機能を示します。表 3 に、Cisco VPN/SSL AIM の機能の利点を示します。

表 1 サポートされるモジュールと機能(プラットフォーム別)

モジュール 製品番号	Cisco ISR 1841	Cisco ISR 2801、2811、 2821、および 2851	Cisco 3725	Cisco ISR 3825	Cisco 3745	Cisco ISR 3845	AES および Triple Data Encryption Standard (3DES)	IPPCP	WebVPN SSL 暗号化	ハード ウェアでの IPv6 暗号化
AIM- VPN/SSL-1	○						○	○	○	○
AIM- VPN/SSL-2		○					○	○	○	○
AIM- VPN/SSL-3			○	○	○	○	○	○	○	○

表 2 Cisco VPN/SSL AIM でサポートされる機能

機能	説明
物理	Cisco VPN/SSL AIM は、Cisco ISR の空いている AIM スロットに装着される
プラットフォームのサポート	Cisco VPN/SSL AIM は、Cisco ISR 1841 と Cisco ISR 2800、3800、および Cisco 3700 シリーズをサポートする
ハードウェアの前提条件	Cisco ISR 1800、2800、3800、および Cisco 3700 シリーズ用の AIM スロットが必要
サポートされる IPsec 暗号化	すべてのモジュールで IPsec DES および 3DES をサポートする。認証: Rivest, Shamir, and Adelman (RSA) および Diffie Hellman。データ整合性: Secure Hash Algorithm 1 (SHA-1) および Message Digest Algorithm 5 (MD5)。DES、3DES、および AES キーのサイズ: AES128、AES192、および AES256
サポートされるハードウェア SSL 暗号化	Cisco ISR 1800、2800、3800、および Cisco 3700 シリーズの Cisco VPN/SSL AIM のみが SSL Web VPN 暗号化をサポート
IPsec ハードウェアベースの圧縮	Cisco VPN/SSL AIM は、レイヤ 3 IPPCP 圧縮を使用
ソフトウェアの前提条件	Cisco VPN/SSL AIM は、Advanced Security、Advanced IP、または Advanced Enterprise フィーチャ セットを備えた Cisco IOS ソフトウェアを使用
ルータごとの暗号化モジュールの数	Cisco VPN/SSL AIM は、ルータごとに 1 つの暗号化モジュールを使用
Cisco IOS ソフトウェア バージョンの最小要件	Cisco VPN/SSL AIM では、Cisco IOS ソフトウェア バージョン 12.4(9)T 以上が必要
IPsec 暗号化トンネルの最大数	Cisco VPN/SSL AIM は、Cisco ISR 1841 では最大 800 のトンネル、Cisco ISR 2800 シリーズでは最大 1500 のトンネル、Cisco ISR 3800 シリーズでは最大 2000 のトンネルをサポートする。トンネルの最大スケーラビリティのテストは、最大数のみを調べるため、トンネルでデータを渡さずに行われる。サイト間の設計の場合、シスコのアカウント チームまたはシスコ認定リセラーに相談し、次の URL の『Cisco DMVPN Design Guide』を参照することが推奨される。 <a href="http://www.cisco.com/application/pdf/en/us/quest/netsol/ns171/c649/ccmigration_09186a0080739fd3.pdf">http://www.cisco.com/application/pdf/en/us/quest/netsol/ns171/c649/ccmigration_09186a0080739fd3.pdf</a>
VPN/SSL AIM を使用する Cisco IOS WebVPN/SSL VPN ユーザの最大数	Cisco VPN/SSL AIM のみが Cisco IOS WebVPN/SSL VPN をサポートする。Cisco ISR 1841 および 2801 では、75 ユーザをサポートする。Cisco ISR 2811 および 2821 では、100 ユーザをサポートする。Cisco ISR 2851 では、150 ユーザをサポートする。Cisco 3725 および 3745 では、150 ユーザをサポートする。Cisco ISR 3825 および 3845 では、200 ユーザをサポートする。Cisco IOS WebVPN/SSL VPN では、ユーザライセンスを購入する必要がある(サポートされるすべてのプラットフォームには、無料で 2 つのユーザ デモライセンスが含まれている)。
サポート標準	Cisco VPN/SSL AIM は、IPsec Internet Key Exchange (IKE; インターネット キー エクスチェンジ)をサポートし、RFC 2401 ~ 2410、2411、および 2451 に対応する。

表 3 Cisco VPN/SSL AIM の機能と利点

機能	利点
メイン プロセッサからのオーバーヘッドの多い IPsec 処理	ルーティング、ファイアウォール、音声など、他のサービス用に重要な処理リソースを予約
IPsec MIB	Cisco IPsec 構成をモニタし、さまざまな VPN 管理ソリューションへの統合を実現
デジタル証明書を使用した自動認証を容易にするための証明書のサポート	複数のサイト間で安全な接続を必要とする大規模なネットワークにも暗号化の使用を拡大

機能	利点
VPN モジュールを既存の Cisco ISR 1841 と Cisco ISR 2800、3800、および Cisco 3700 シリーズ ルータに容易に統合	複数デバイスのソリューションと比較して、システム コスト、管理の複雑さ、および導入作業を大幅に軽減
IPSec による機密保持、データ整合性、およびデータ発信元の認証	WAN における公衆交換網とインターネットの安全な使用を促進
Cisco IOS WebVPN	企業が SSL VPN を使用してネットワークをインターネット対応の場所に安全かつ透徹的に拡張できるようにする。Cisco IOS WebVPN は、HTML ベースのイントラネット コンテンツ、E メール、ネットワーク ファイル共有、Citrix などのアプリケーション、および Cisco SSL VPN Client へのクライアントレス アクセスをサポートし、ほぼすべてのアプリケーションへの完全なリモートアクセスを実現
圧縮	Cisco VPN/SSL AIM は、IPSec レイヤ 3 IPPCP にハードウェア サポートを提供し、暗号化の前にパケットを圧縮できる。これにより WAN リンクのスループットを向上

### Cisco WebVPN/SSL VPN のパフォーマンス

- Cisco ISR 1841 シリーズ モジュール(AIM-VPN/SSL-1)は、最大 75 ユーザに 5 Mbps の Web/VPN SSL ハードウェアベースの暗号化を提供します。<sup>1</sup>
- Cisco ISR 2800 シリーズ モジュール(AIM-VPN/SSL-2)は、Cisco ISR 2801 で最大 75 ユーザに 5 Mbps、Cisco ISR 2811 で最大100 ユーザに 5 Mbps、Cisco ISR 2821 で最大 100 ユーザに 10 Mbps、Cisco ISR 2851 で最大 150 ユーザに 14 Mbps の Web/VPN SSL ハードウェアベースの暗号化を提供します。<sup>2</sup>
- Cisco ISR 3800 シリーズ モジュール(AIM-VPN/SSL-3)は、Cisco ISR 3825 で最大 175 ユーザに 20 Mbps、Cisco ISR 3845 で最大 200 ユーザに 26 Mbps の Web/VPN SSL ハードウェアベースの暗号化を提供します。<sup>2</sup>

### 機能

#### SSL WEB VPN

- Cisco VPN/SSL AIM は、SSL 暗号化処理の負荷を軽減することで、Cisco IOS WebVPN のパフォーマンスを向上します。
- Cisco IOS WebVPN は、データ、音声、およびワイヤレスが統合されたプラットフォーム上でセキュリティと業界をリードするルーティング機能を備えた SSL VPN リモート アクセス接続を提供する、初のルータベースのソリューションです。
- SSL VPN が優れているのは、セキュリティがエンド ユーザに対して透徹的であり、IT 担当者が管理しやすい点です。企業は Web ブラウザのみを使用して、自宅のコンピュータ、インターネット キオスク、ワイヤレス ホットスポットなど、インターネットを使用できる場所に安全なエンタープライズ ネットワークを拡張できるようにすることで、従業員の生産性を向上し、企業データを保護する一方で、パートナーやコンサルタントが一時的にネットワークにアクセスできるようにします。

<sup>1</sup> IPSec 数は、Spirent IPSec IMIX 定義と 1400 バイトのパケット サイズに基づく最大値。各テストは 1 つのトンネルで実行される。シスコのアカウント チームに相談し、導入のオプションと拡大の詳細については、すべての Cisco VPN ソリューション設計ガイドを参照することが推奨される。IPSec ユーザは、拡大の詳細について、以下の URL の『Cisco Solution Design Guides』も参照することが推奨される。

[http://www.cisco.com/application/pdf/en/us/guest/netso/ns171/c649/ccmigration\\_09186a0080739fd3.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso/ns171/c649/ccmigration_09186a0080739fd3.pdf) および [http://www.cisco.com/en/US/netso/ns656/networking\\_solutions\\_design\\_guidances\\_list.html](http://www.cisco.com/en/US/netso/ns656/networking_solutions_design_guidances_list.html)

<sup>2</sup> シスコのアカウント チームに相談し、導入のオプションと拡大の詳細については、すべての Cisco Web VPN ソリューション設計ガイドを参照することが推奨される。IOS SSLVPN のパフォーマンスは、設定されているクライアントによって異なる。SSLVPN クライアント ユーザは、若干パフォーマンスが低下する SSLVPN クライアントレス設定に比べて、全体のパフォーマンスが向上する。

- Cisco IOS WebVPN は、クライアントレスと完全なネットワーク アクセスの両方の SSL VPN 機能をサポートします。

Cisco IOS WebVPN の詳細については、以下の URL を参照してください。

<http://www.cisco.com/go/ioswebvpn>

**注:** Cisco IOS WebVPN は、今日現在、日本語環境での動作はサポートされておりません。  
また、AnyConnect クライアントの日本語パッケージはサポートされておりません。

### IPSec VPN

シスコシステムズは、IPSec と関連プロトコルを記述する RFC(RFC 2401 ~ 2410)に完全に対応しています。

- **DES、3DES、および AES** — National Institute of Standards and Technology(NIST; 国立標準技術研究所)は、DES、IPSec、および IKE を置き換えるために、Federal Information Processing Standard(FIPS; 連邦情報処理標準)の出版物として AES を作成しました。AES のキーは可変長であり、アルゴリズムは 128 ビット キー(デフォルト)、192 ビット キー、または 256 ビット キーを指定できます。AES の詳細については、以下の URL を参照してください。  
<http://csrc.nist.gov/encryption/aes/>
- **IPSec** — このプロトコルは暗号化テクノロジーを使用して、プライベート ネットワークに参加しているピア間にデータの機密性、整合性、および信頼性を提供します。シスコでは、Encapsulating Security Payload(ESP)と認証ヘッダーを完全にサポートしています。
- **IKE** — Internet Security Association Key Management Protocol(ISAKMP)または Oakley を使用することで、IKE はセキュリティ アソシエーション管理を提供します。IKE は IPSec トランザクションで各ピアを認証し、セキュリティ ポリシーをネゴシエートして、セッション キーの交換を処理します。
- **認証管理** — シスコでは、デバイス認証と Simple Certificate Enrollment Protocol(SCEP)に対応した X509.V3 証明書システムを完全にサポートしています。SCEP は、認証局と通信するためのプロトコルです。Verisign、Entrust Technologies、Microsoft など、複数のベンダーが Cisco SCEP をサポートしており、各製品はシスコ製デバイスと相互運用できます。
- **RSA 署名および Diffie-Hellman** — IKE セキュリティ アソシエーションを認証するために、IPSec トンネルが確立されるたびに RSA および Diffie-Hellman が使用されます。Diffie-Hellman は、使用される IPSec ポリシーのネゴシエーションなど、IKE セキュリティ アソシエーションでデータを保護するための共有秘密暗号鍵を導出するために使用されます。
- **セキュリティ強化** — ハードウェアベースの暗号化は、鍵の保護の強化など、ソフトウェアベースのソリューションに比べてセキュリティの面でいくつかの利点があります。

Cisco IOS IPSec VPN の詳細については、以下の URL を参照してください。

[http://www.cisco.com/en/US/products/ps6635/products\\_ios\\_protocol\\_group\\_home.html](http://www.cisco.com/en/US/products/ps6635/products_ios_protocol_group_home.html)

### 認定

シスコでは、世界中のお客様のために、製品の認定と評価をアクティブに行うプログラムの維持に努めています。シスコは、お客様にとって認定と評価が重要であることを認識し、認定および評価を受けた製品を市場に提供するリーダーであり続けています。シスコでは、国際セキュリティ標準機構と引き続き協力して、認定および評価を受けた製品の将来を方向づけ、認定と評価のプロセスを迅速化するように努めます。認定と評価は、会社の製品の開発サイクルにおいて最も早い段階で検討されます。シスコでは、お客様がニーズに合わせて認定および評価を受けたさまざまな製品を

利用できるように、セキュリティ製品を引き続き販売する予定です。シスコは ICSA、Common Criteria (EAL)、および FIPS 140-2 認定基準に従っています(図 2 を参照)。

図 2



### FIPS

Cisco VPN モジュールは、FIPS 140-2 レベル 2 セキュリティを満たすように設計されています。現在、FIPS 140-2 認定を受けているのは特定のモデルのみです。FIPS で認定されているシスコ製品の現在の状態については、認定タイプ別の製品認定を参照してください。

- [http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking\\_solutions\\_audience\\_business\\_benefit0900aecd8009a16f.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html)
- <http://csrc.nist.gov/cryptval/>

### ICSA IPsec

Internet Computer Security Association (ICSA) は、各種セキュリティ製品に対して ICSA IPsec 認定および ICSA Firewall 認定を提供する民間のセキュリティ認定会社です。シスコは、ICSA の IPsec および Firewall 認定プログラムに参加しています。現在 ICSA で認定されているシスコ製品については、認定タイプ別の製品認定を参照してください。

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking\\_solutions\\_audience\\_business\\_benefit0900aecd8009a16f.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html)

### Common Criteria

Common Criteria は、IT セキュリティを評価するための国際標準です。すでに多数存在していた各国独自のセキュリティ評価プログラムを統一し、国際的に使用できる単一の標準を確立することを目的として、複数の国からなるコンソーシアムによって開発されました。現在、正式には 14 カ国が Common Criteria を承認しています。現在、複数のバージョンの Cisco ISR ルータが、Information Technology Security Evaluation Criteria (ITSEC) および Common Criteria に従い評価されています。現在 Common Criteria で認定されているシスコ製品については、認定タイプ別の製品認定を参照してください。

- [http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking\\_solutions\\_audience\\_business\\_benefit0900aecd8009a16f.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html)
- <http://www.commoncriteriaportal.org/>

## Cisco ISR 1841 と Cisco ISR 2800、3800、および Cisco 3700 シリーズの VPN モジュール ソフトウェア

VPN モジュールを装備している場合、ルータは Cisco IOS ソフトウェアのフィーチャ セットで動作しますが、モジュールは IPSec または SSL Web VPN フィーチャ セットでのみ使用されます。

### VPN モジュールの輸出規制

VPN モジュールの DES、3DES、および AES ソフトウェアは、暗号化製品に関する米国の輸出規制によって管理されます。米国の規制では、DES および 3DES ソフトウェアの受領者の名前と住所を記録する必要があります。シスコでは、DES および 3DES ソフトウェアの発注プロセスでこれらの要件を実行します。

### 仕様

#### 製品番号と説明

- **AIM-VPN/SSL-1**: Cisco 1841 DES、3DES、AES、SSL、およびレイヤ 3 (IPPCP) 圧縮 VPN 暗号化
- **AIM-VPN/SSL-2**: Cisco 2800 シリーズ DES、3DES、AES、SSL、およびレイヤ 3 (IPPCP) 圧縮 VPN 暗号化
- **AIM-VPN/SSL-3**: Cisco 3800 シリーズ DES、3DES、AES、SSL、およびレイヤ 3 (IPPCP) 圧縮 VPN 暗号化
- **AIM-VPN/BPII-PLUS**: DES、3DES、AES、およびレイヤ 3 (IPPCP) 圧縮 VPN 暗号化
- **AIM-VPN/EPII-PLUS**: DES、3DES、AES、およびレイヤ 3 (IPPCP) 圧縮 VPN 暗号化
- **AIM-VPN/HPII-PLUS**: DES、3DES、AES、およびレイヤ 3 (IPPCP) 圧縮 VPN 暗号化

#### IPSec RFC のサポート

- IPSec (RFC 2401 ~ 2410)
- DES および 3DES を使用する IPSec ESP (RFC 2406)
- MD5 または SHA を使用する IPSec 認証ヘッダー (RFC 2403 ~ 2404)
- IKE (RFC 2407 ~ 2409)

#### 環境

- 動作温度: 0 ~ 40°C (32 ~ 104°F)
- 保管温度: -20 ~ 65°C (-4 ~ 149°F)
- 相対湿度: 動作時: 10 ~ 85% (結露しないこと)、非動作時: 5 ~ 95% (結露しないこと)

#### 寸法および重量

表 4 に、プラットフォーム別の寸法と重量を示します。

表 4 寸法および重量

モジュール	AIM-VPN/BPII-PLUS	AIM-VPN/EPII-PLUS	AIM-VPN/HPII-PLUS	AIM-VPN/SSL-1	AIM-VPN/SSL-2	AIM-VPN/SSL-3
幅	13.3 cm (5.25 インチ)	13.3 cm (5.25 インチ)	13.3 cm (5.25 インチ)	13.3 cm (5.25 インチ)	13.3 cm (5.25 インチ)	13.3 cm (5.25 インチ)
高さ	2.41 cm (0.95 インチ)	2.41 cm (0.95 インチ)	2.41 cm (0.95 インチ)	2.41 cm (0.95 インチ)	2.41 cm (0.95 インチ)	2.41 cm (0.95 インチ)

モジュール	AIM-VPN/BPII-PLUS	AIM-VPN/EPII-PLUS	AIM-VPN/HPII-PLUS	AIM-VPN/SLL-1	AIM-VPN/SSL-2	AIM-VPN/SSL-3
奥行	8.26 cm (3.25 インチ)	8.26 cm (3.25 インチ)	8.26 cm (3.25 インチ)	8.26 cm (3.25 インチ)	8.26 cm (3.25 インチ)	8.26 cm (3.25 インチ)
重量	0.27 kg (0.6 ポンド)	0.27 kg (0.6 ポンド)	0.27 kg (0.6 ポンド)	0.27 kg (0.6 ポンド)	0.27 kg (0.6 ポンド)	0.27 kg (0.6 ポンド)

### 適合規格、安全性、EMC、電気通信、ネットワーク ホモロゲーション

VPN モジュールを Cisco 1700、2600、3600、3700 シリーズまたは Cisco ISR 1800(モジュール)、2800、3800 シリーズ ルータにインストールした場合でも、ルータ自体の標準規格(適合規格、安全性、EMC、テレコミュニケーション、またはネットワーク ホモロゲーション)に変更はありません。Cisco 1700、2600、3600、3700 シリーズまたは Cisco ISR 1800(モジュール)、2800、3800 シリーズ ルータのデータシートを参照してください。

### ソフトウェアのダウンロード

Cisco IOS ソフトウェアをダウンロードするには、[Cisco Software Center](http://www.cisco.com/go/ios) にアクセスしてください。

### サービスおよびサポート

シスコは、お客様がそのネットワーク サービスを最大限に活用するため、各種サービスプログラムを用意しています。これらのサービスは、スタッフ、プロセス、ツールをそれぞれに組み合わせて提供され、お客様から高い評価を受けています。ネットワークへの投資を無駄にすることなく、ネットワーク運用を最適化しネットワーク インテリジェンスの強化や事業拡張を進めていただくためにシスコのサービスを是非お役立てください。サービスについての詳細は、以下の URL を参照してください。

テクニカル サポート サービス

<http://www.cisco.com/jp/go/tac/>

サービス プログラム

<http://www.cisco.com/jp/services/>

### 関連情報

Cisco VPN モジュールの詳細については、シスコの代理店までお問い合わせください。

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0701R)

この資料に記載された仕様は予告なく変更する場合があります。



#### シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日 10:00～12:00、13:00～17:00

#### お問い合わせ先