このマニュアルについて

ここでは、『*Cisco セキュリティ アプライアンス コマンド ライン コンフィギュレーション ガイド*』の概要を示します。次の項について説明します。

マニュアルの目的

このマニュアルは、コマンドライン インターフェイスを使用してセキュリティ アプライアンスを設定する際に役立ちます。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

セキュリティ アプライアンスの設定と監視は、ASDM（Web ベースの GUI アプリケーション）を使用して行うこともできます。ASDM では、コンフィギュレーション ウィザードを使用して、いくつかの一般的なコンフィギュレーションを設定できます。また、あまり一般的ではない事例には、オンラインのヘルプが用意されています。詳細については、http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm を参照してください。

このマニュアルは、Cisco PIX 500 シリーズのセキュリティ アプライアンス（PIX 515E、PIX 525、および PIX 535）と、Cisco ASA 5500 シリーズのセキュリティ アプライアンス（ASA 5505、ASA 5510、ASA 5520、および ASA 5540、ASA 5550）に利用できます。このマニュアル全体で、「セキュリティ アプライアンス」という用語は、特に指定がない限り、サポートされているすべてのモデルを意味します。PIX 501、PIX 506E、および PIX 520 セキュリティ アプライアンスは、サポートされていません。

対象読者

このマニュアルは、次の作業を担当するネットワーク管理者を対象としています。

- ネットワーク セキュリティの管理
- ファイアウォールとセキュリティ アプライアンスのインストールおよび設定
- VPN の設定
- 侵入検知ソフトウェアの設定

関連資料

詳細については、次のマニュアルを参照してください。

- *Cisco PIX Security Appliance Release Notes*
- *Cisco ASDM Release Notes*
- *Cisco PIX 515E Quick Start Guide*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Cisco Security Appliance Command Reference*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco Security Appliance Logging Configuration and System Log Messages*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*

マニュアルの構成

このマニュアルは、表 1 に示す章と付録で構成されています。

表 1　マニュアルの構成

章 / 付録	内容
Part 1：準備と一般情報	
第 1 章「セキュリティ アプライアンスの概要」	セキュリティ アプライアンスの概要を示します。
第 2 章「はじめに」	コマンドライン インターフェイスへのアクセス方法、ファイアウォール モードの設定方法、およびコンフィギュレーションの処理方法について説明します。
第 3 章「マルチコンテキスト モードのイネーブル化」	セキュリティ コンテキストの使用方法とマルチコンテキスト モードをイネーブルにする方法について説明します。
第 4 章「Cisco ASA 5505 適応型セキュリティ アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定」	ASA 5505 適応型セキュリティ アプライアンスのスイッチ ポートと VLAN インターフェイスの設定方法について説明します。
第 5 章「イーサネットとサブインターフェイスの設定」	物理インターフェイスのイーサネットの設定方法、およびサブインターフェイスの追加方法について説明します。
第 6 章「セキュリティ コンテキストの追加と管理」	セキュリティ アプライアンスにマルチセキュリティ コンテキストを設定する方法について説明します。
第 7章「インターフェイス パラメータの設定」	各インターフェイスおよびサブインターフェイスの名前、セキュリティ レベル、IP アドレスの設定方法について説明します。
第 8 章「基本設定」	機能を果たすコンフィギュレーションに通常必要とされる基本設定を行う方法について説明します。
第 9 章「IP ルーティングの設定」	IP ルーティングの設定方法について説明します。
第 10 章「DHCP、DDNS、WCCP サービスの設定」	DHCP サーバと DHCP リレーの設定方法について説明します。
第 11 章「マルチキャスト ルーティングの設定」	マルチキャスト ルーティングの設定方法について説明します。
第 12 章「IPv6 の設定」	IPv6 をイネーブルにする方法および設定する方法について説明します。
第 13 章「AAA サーバとローカル データベースの設定」	AAA サーバとローカル データベースの設定方法について説明します。
第 14 章「フェールオーバーの設定」	セキュリティ アプライアンスのフェールオーバー機能について説明します。この機能を使用すると、2 つのセキュリティ アプライアンスを設定して、一方の装置が故障した場合に、もう一方の装置が動作を引き継ぐようにできます。
Part 2：ファイアウォールの設定	
第 15 章「ファイアウォール モードの概要」	セキュリティ アプライアンスの 2 つのオペレーション モード（ルーテッド モードと透過モード）、および各モードでのデータの処理方法の違いについて詳細に説明します。
第 16 章「アクセスリストによるトラフィックの指定」	アクセスリストを使用してトラフィックを指定する方法について説明します。
第 17 章「NAT の適用」	アドレス変換の実行方法について説明します。
第 18 章「ネットワーク アクセスの許可または拒否」	セキュリティ アプライアンスを経由するネットワーク アクセスを、アクセスリストを使用して制御する方法について説明します。
第 19 章「ネットワーク アクセスへの AAA の適用」	ネットワーク アクセスに対して AAA をイネーブルにする方法について説明します。

表 1　マニュアルの構成（続き）

章 / 付録	内容
第 20 章「フィルタリング サービスの適用」	Web トラフィックをフィルタリングして、セキュリティ リスクを低減したり不適切な使用を防止したりする方法について説明します。
第 21 章「モジュラ ポリシー フレームワークの使用」	モジュラ ポリシー フレームワークを使用して、TCP、一般的な接続設定、検査、および QoS に関するセキュリティ ポリシーを作成する方法について説明します。
第 22 章「AIP SSM および CSC SSM の管理」	セキュリティ アプライアンスを設定してトラフィックを AIP SSM または CSC SSM に送信する方法、SSM のステータスを確認する方法、およびインテリジェント SSM のソフトウェア イメージを更新する方法について説明します。
第 23 章「ネットワーク攻撃の防止」	ネットワーク攻撃を代行受信して対応するように保護機能を設定する方法について説明します。
第 24 章「QoS ポリシーの適用」	フレーム リレー、Asynchronous Transfer Mode（ATM; 非同期転送モード）、イーサネットと 802.1 ネットワーク、SONET、IP ルーティング型ネットワークなど、多様なテクノロジーを通じて、特定のネットワーク トラフィックに、より良いサービスを提供するネットワークの設定方法について説明します。
第 25 章「アプリケーション レイヤ プロトコル検査の設定」	アプリケーション検査の使用方法と設定方法について説明します。
第 26 章「ARP 検査およびブリッジング パラメータの設定」	ARP 検査をイネーブルにする方法と、ブリッジング オペレーションをカスタマイズする方法について説明します。
Part 3：VPN の設定	
第 27 章「IPSec と ISAKMP の設定」	ISAKMP と IPSec を設定して、VPN の「トンネル」、つまり、リモート ユーザとプライベートな企業ネットワークとの間のセキュアな接続を構築および管理する方法について説明します。
第 28 章「L2TP over IPSec の設定」	セキュリティ アプライアンスに L2TP over IPSec を設定する方法について説明します。
第 29 章「IPSec VPN の一般パラメータの設定」	さまざまな VPN 設定手順について説明します。
第 30 章「トンネルグループ、グループポリシー、およびユーザの設定」	VPN のトンネルグループ、グループポリシー、およびユーザの設定方法について説明します。
第 31 章「VPN の IP アドレスの設定」	プライベート ネットワークのアドレッシング方式で IP アドレスを設定する方法について説明します。この方式では、クライアントがトンネルのエンドポイントとして機能します。
第 32 章「リモートアクセス IPSec VPN の設定」	リモートアクセス VPN 接続の設定方法について説明します。
第 33 章「ネットワーク アドミッション コントロールの設定」	ネットワーク アドミッション コントロール（NAC）の設定方法について説明します。
第 34 章「ASA 5505 上での Easy VPN サービスの設定」	ASA 5505 適応型セキュリティ アプライアンスに Easy VPN を設定する方法について説明します。
第 35 章「PPPoE クライアントの設定」	セキュリティ アプライアンスで対応している PPPoE クライアントを設定する方法について説明します。
第 36 章「LAN-to-LAN IPSec VPN の設定」	LAN-to-LAN VPN 接続の構築方法について説明します。
第 37 章「WebVPN の設定」	ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを確立する方法について説明します。
第 38 章「SSL VPN クライアントの設定」	SSL VPN クライアントをインストールし、設定する方法について説明します。

表 1　マニュアルの構成（続き）

章 / 付録	内容
第 39 章「証明書の設定」	デジタル証明書を設定する方法について説明します。デジタル証明書には、ユーザまたはデバイスを識別する情報が含まれています。このような情報には、名前、シリアル番号、社名、部署、IP アドレスなどがあります。デジタル証明書には、ユーザまたは装置の公開キーのコピーが含まれています。
Part 4：システム管理	
第 40 章「システム アクセスの管理」	Telnet、SSH、および HTTPS を介してシステム管理のためにセキュリティ アプライアンスにアクセスする方法について説明します。
第 41 章「ソフトウェア、ライセンス、およびコンフィギュレーションの管理」	ライセンス キーを入力し、ソフトウェアとコンフィギュレーション ファイルをダウンロードする方法について説明します。
第 42 章「セキュリティ アプライアンスのモニタリング」	セキュリティ アプライアンスの監視方法について説明します。
第 43 章「セキュリティ アプライアンスのトラブルシューティング」	セキュリティ アプライアンスのトラブルシューティングの方法について説明します。
Part 5: 参考資料	
付録 A「機能のライセンスと仕様」	機能のライセンスと仕様について説明します。
付録 B「設定例」	セキュリティ アプライアンスを実装するいくつかの一般的な方法について説明します。
付録 C「コマンドライン インターフェイスの使用」	CLI を使用してセキュリティ アプライアンスを設定する方法について説明します。
付録 D「アドレス、プロトコル、およびポート」	IP アドレス、プロトコル、およびアプリケーションのクイック リファレンスを提供します。
付録 E「認可および認証用の外部サーバの設定」	LDAP および RADIUS 認可サーバの設定について説明します。
「Glossary」	一般用語および略語についての便利なリファレンスを提供します。
「Index」	このマニュアルの索引を提供します。

表記法

コマンドの説明では、次の表記法を使用しています。

- 選択する必要があるものは、波カッコ（{ }）で囲んで示しています。
- オプションの要素は、角カッコ（[ ]）で囲んで示しています。
- どちらか選択する必要がある要素は、縦棒（|）で区切って示しています。
- 記載されているとおりに入力するコマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。

例では、次の表記法を使用しています。

- 画面に表示される情報およびコマンドラインは、`screen` フォントで示しています。
- ユーザが入力する情報は、太字の **`screen`** フォントで示しています。
- ユーザが値を指定する変数は、イタリック体の *`screen`* フォントで示しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスできます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと HTML の同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Cisco Marketplace から Product Documentation DVD（Product Number DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

マニュアルの発注方法（英語版）

Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトで、次に関する情報を確認できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードに登録してください。PSIRT RSS フィードへの登録方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合のみ：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または GnuPG などの互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 9.*x* を使用して暗号化された情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

PGP を持っていない、または使用していない場合は、機密情報を送信する前に前述のメール アドレスまたは電話番号で PSIRT に問い合せ、他のデータ暗号化方法を確認してください。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

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

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：既存のネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- 『*Cisco Product Quick Reference Guide*』は手軽でコンパクトな参照ツールです。チャネル パートナー経由で販売される多くのシスコ製品に関する簡単な製品概要、主要な機能、サンプル部品番号、および簡単な技術仕様を記載しています。年 2 回の更新の際には、シスコの最新情報が収録されます。『*Cisco Product Quick Reference Guide*』の注文方法および詳細については、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

  デジタル版には、次の URL からアクセスできます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html