



Catalyst 6500 シリーズ スイッチ WebVPN サービス モジュール ソフトウェア コンフィギュレーション ガイド

Software Release 1.2



このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

以下の情報は、クラス A デバイスの FCC 規則遵守のための情報です。本機器について行われたテストの結果、本機器は、FCC 規則第 15 章に基づくクラス A デジタル デバイスの制限に合致していることが判明しております。かかる制限は、商用環境において機器を作動させる場合の障害に対する合理的な予防策の提供を意図して設計されたものです。本機器は、高周波エネルギーを発生、利用、又は放出することがあり、手引書に従ってインストール及び使用されなかった場合、遠距離通信に障害を発生させるおそれがあります。本機器を住宅地域内で作動させる場合、障害が発生するおそれがあり、障害発生時には、ユーザはかかる障害を自己の費用負担で修正するよう求められます。

以下の情報は、クラス B デバイスの FCC 規則遵守のための情報です。本手引書に記載された機器は、高周波エネルギーを発生又は放出することがあります。シスコシステムズの指示する設置手順に従わずに装置を設置した場合、ラジオおよびテレビの受信障害が起こることがあります。本機器について行われたテストの結果、本機器は、FCC 規則第 15 章の仕様に基づくクラス B デジタル デバイスの制限に合致していることが判明しております。かかる仕様は、住宅地域内でインストールを行う場合の上記の障害に対する合理的な予防策の提供を意図して設計されていますが、特定のインストール環境において障害が発生しないという保証はありません。

シスコシステムズの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に適合しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

機器が障害を発生しているか否かは、機器の電源を切ることによって確認することができます。それによって障害が収まれば、障害は、シスコ機器かその周辺機器のいずれかにより発生している可能性が高いこととなります。本件機器がラジオ又はテレビの受信に障害を発生させている場合には、以下の方法を試して、障害を修正してください。

- ・ 障害が収まるまで、テレビ又はラジオのアンテナの向きを変える。
- ・ 本機器を、テレビ又はラジオの片側又はその反対側に移動する。
- ・ 本機器を、テレビ又はラジオから遠ざける。
- ・ 本機器のプラグを、テレビ又はラジオと異なる回路の差込口に差し込む。(本機器とテレビ又はラジオが、異なる遮断機又はヒューズで制御されている回路に接続されるようにする。)

米国シスコシステムズ社では、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うこととなります。

シスコシステムズが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティングシステムの UCB (University of California, Berkeley) パブリック ドメイン バージョンの一部として、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されません。シスコシステムズおよびこれら各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取引によって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその代理店は、このマニュアルの使用または使用不能によって生じた、利益の損失、データの損失または損害を含みますがこれらに限定されず、あらゆる間接的、特殊、結果的、または偶発的な損害に対して、シスコシステムズまたは代理店にかかる損害の可能性が通知されていたとしても、一切の責任を負いません。

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、The Fastest Way to Increase Your Internet Quotient、TransPath は、米国および一部の国における Cisco Systems, Inc. または関連会社の登録商標です。

このマニュアルまたは Web サイトで言及している他の商標はいずれも、それぞれの所有者のものです。「パートナー」という用語を使用しているも、シスコシステムズと他社とのパートナー関係を意味するものではありません。(0601R)

Catalyst 6500 シリーズスイッチ WebVPN サービス モジュール ソフトウェア コンフィギュレーション ガイド

Copyright © 2005、Cisco Systems, Inc.

All rights reserved.

著作権情報

Cisco Web VPN Module Software Release 1.1(1) は、ライセンスに基づくサードパーティ製ソフトウェアを使用しています。これらのサードパーティ製ソフトウェアのライセンスおよび使用に関しては、次のいずれかの通告が適用されることがあります。

GNU General Public License

Catalyst 6500 Series Web VPN Module には、GNU Public License（以下を参照）の対象となるソフトウェアが含まれています。SSL Services Module 内の修正された GPL コードのソースを取得したい場合には、ssl_sw_req@Cisco.com にリクエストを送信してください。

ライセンス文書

Copyright © 1989、1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

このライセンス文書は、逐語的な複製の作成および配布は許可されていますが、内容の変更は許可されていません。

序文

ソフトウェアのライセンスは通常、ソフトウェアの共有および変更を制限することを目的としています。これに対し、GNU General Public License は、すべてのユーザがソフトウェアを自由に使用できるように、フリーソフトウェアの共有および変更の自由を保証することを意図しています。この General Public License は、Free Software Foundation のほとんどのソフトウェア、および著者が使用を表明している任意の他のプログラムに適用されます（その他の一部の Free Software Foundation ソフトウェアには、本ライセンスではなく、GNU Library General Public License が適用されています）。ユーザは、自分で作成したプログラムに本ライセンスを適用することもできます。

フリーソフトウェアという用語は本来、無償という意味ではなく、自由を意味します。この General Public License は、ユーザに対して、フリーソフトウェアの複製を自由に配布できること（および当該配布について任意に課金できること）、ソースコードを受領または任意に取得できること、ソフトウェアまたはその一部を変更して新規のフリープログラムを作成できることを保証し、ユーザに当該行為が可能であることを認識させることを目的としています。

ユーザの権利を保護するためには、あらゆる人物に対して、ユーザの権利を拒否する行為、またはユーザに権利を放棄させる行為を禁止する制約が必要です。これらの制約は、ユーザがソフトウェアの複製を配布、またはソフトウェアを変更する場合、当該ユーザに特定の責任を課すこととなります。

たとえば、ユーザが当該プログラムの複製を配布する場合、無償または有償に関係なく、ユーザは自分が所有する全権利を受領者に供与する必要があります。受領者もまた、ソースコードを受け取る、または取得できる権利が保証されなければなりません。また、ユーザは本条件を受領者に開示し、かかる権利があることを通知する必要があります。

ユーザの権利は、2段階で保護されます。(1) ソフトウェアの著作権保護、および(2) ソフトウェアの複製、配布、変更を合法的に許可する本ライセンスの提供です。

また、各著者および当組織を保護するには、このフリーソフトウェアに何ら保証がないことを、すべての人に理解してもらう必要があります。ソフトウェアが修正されて配布された場合、他者による変更によって発生した問題がオリジナルの著者の評価を損なわないように、受領者に、そのソフトウェアがオリジナルではないことを通知すべきです。

さらに、すべてのフリープログラムは常に、ソフトウェア特許の脅威にさらされています。フリープログラムの再配布者が個人的に特許ライセンスを取得し、その結果、プログラムに占有権が発生することは避けなければなりません。これを防ぐために、当組織では、いかなる特許も、すべての人が自由に使用できるようにライセンス許諾する必要があること、それ以外の特許は認められないことを明確に提示しています。

複製、配布、および修正に関する詳細な条件は、次のとおりです。

複製、配布、および修正に関する条件

0. 本ライセンスは、著作権所有者が General Public License の条件に基づいて配布できることを宣言した通告を含む、すべてのプログラムまたは他の著作物に適用されます。以下、「プログラム」とは当該プログラムまたは著作物を意味し、「プログラムに基づく著作物」とは、プログラム、または著作権法に基づくすべての派生著作物を意味します。つまり、逐語的な、または修正した、または他言語に翻訳したプログラムまたはその一部を含む著作物です（以下、翻訳は、制限なしに「修正」という用語に含まれるものとします）。「ユーザ」は、ライセンス取得者を意味します。

複製、配布、および修正以外の行為は、本ライセンスの範囲外なので言及していません。プログラムを実行する行為は制限されていません。プログラムの出力は、（プログラムの実行により生成されたこととは無関係に）その内容にプログラムに基づく著作物が含まれている場合に限り、対象になります。対象になるかどうかは、プログラムの実行内容によって異なります。

1. ユーザは、受領したプログラムのソースコードの逐語的な複製を任意の媒体により作成および配布できますが、各複製に適切な著作権情報および保証の放棄を明確かつ適正に表示し、本ライセンスおよび無保証を示す全通知を完全に保持し、プログラムのすべての受領者にプログラムと一緒に本ライセンスの複製を配布することを条件とします。

ユーザは、複製の配布という物理的な行為に対して課金することができ、任意に、料金と引き換えに保証を提供できます。

2. ユーザは、プログラムまたはプログラムの一部の複製を修正し、プログラムに基づく著作物を作成し、修正した内容または前述の第1項の条件に基づく著作物を複製および配布できますが、以下のすべての条件を満たす必要があります。

- ユーザは、修正したファイルに、ファイルを変更した事実および変更の日付を示す明確な通知を添付する必要があります。
- プログラムまたはその一部から派生した著作物を、全体または一部として配布または公開する場合、かかる著作物全体に対して、いかなる第三者にも課金することなく、本ライセンスの条件に基づくライセンスを適用する必要があります。
- 修正したプログラムが、実行時に対話形式でコマンドを読み込む場合には、かかる対話形式の最も一般的な方法での起動時に、適切な著作権情報および無保証の通知（または、ユーザが保証を適用することを示す通知）、本ライセンスの条件に基づいてプログラムを再配布できること、および本ライセンスの表示方法を含む告示を出力または表示する必要があります。（例外：プログラム本体が対話形式で、かつ通常の操作でかかる告示が出力されない場合、プログラムに基づく著作物に告示を出力する必要はありません。）

これらの条件は、修正した著作物全体に適用されます。著作物の識別可能なセクションが、プログラムから派生したものではなく、個別の独立した著作物であると妥当に考えられる場合には、個別の著作物として配布すれば、当該セクションには本ライセンスおよび本ライセンスの条件は適用されません。ただし、当該セクションをプログラムに基づく著作物の一部として配布する場合には、配布する全内容が本ライセンスの対象になるので、他のライセンス取得者への許可は、著者が誰であるかに関係なく、著作物のあらゆる部分を含めた全体に対して適用されます。

本項は、ユーザが完全に記述した著作物に対して権利を主張できること、または異議申し立てができることを示すのではなく、プログラムに基づく派生物のまたは集約的な著作物を管理する権利を行使できることを示しています。

また、プログラムから派生したものではない他の著作物を、プログラム（またはプログラムに基づく著作物）と同じストレージ ボリュームまたは配布媒体に収めても、他の著作物が本ライセンスの対象になることはありません。

3. ユーザは、前述の第 1 項および第 2 項の条件に基づいて、プログラム（または第 2 項のプログラムに基づく著作物）をオブジェクト コードまたは実行可能形式で複製および配布できますが、以下のいずれかに準拠することを条件とします。

a) 前述の第 1 項および第 2 項の条件に基づいて配布する必要がある、コンピュータで解読可能な対応する完全なソース コードを、ソフトウェアの交換に慣例的に使用される媒体で添付する。または、

b) 前述の第 1 項および第 2 項の条件に基づいて配布される、コンピュータで解読可能な対応する完全なソース コードを、ソフトウェアの交換に慣例的に使用される媒体により、ソース コード配布の物理的な実行に要した費用未済の料金で、あらゆる第三者に提供するという、最低 3 年間有効な書面による申し出を添付する。または、

c) 受領した、対応するソース コードを配布するという申し出の情報を添付する（この方法は、非営利的な配布に限定され、プログラムのオブジェクト コードまたは実行可能形式を、前述の副項 b) に基づく申し出と共に受領した場合に限り、許可されます）。

著作物のソース コードは、当該著作物を修正する場合の優先的な形式になります。実行可能な著作物の場合、完全なソース コードとは、著作物に含まれる全モジュールのすべてのソース コード、関連するすべてのインターフェイス定義ファイル、および実行ファイルのコンパイルおよびインストール システムを制御するスクリプトを意味します。ただし、特殊な例外として、配布するソース コードには、通常、実行ファイルを実行するオペレーティング システムの主要コンポーネント（コンパイラ、カーネルなど）と一緒に（ソースまたはバイナリ形式のいずれかで）配布されるものを含める必要はありません。ただし、コンポーネントそのものに実行ファイルを添付する場合は除きます。

実行ファイルまたはオブジェクト コードを、指定した場所から複製できるようにアクセス先を提供することによって配布する場合には、同じ場所からソース コードを複製できるように同等のアクセス先を提供すれば、ソース コードを配布したとみなされます。ただし、第三者は、オブジェクト コードと一緒にソース コードを複製する必要はありません。

4. 本ライセンスの条件に規定されている方法以外で、プログラムを複製、修正、サブライセンス供与、または配布することはできません。他の方法でのプログラムの複製、修正、サブライセンス供与、または配布の試みは無効となり、本ライセンスに基づくユーザの権利は自動的に終了します。ただし、本ライセンスに基づいてユーザから複製または権利を受領した当事者のライセンスは、かかる当事者が本ライセンスの条件に従っている限り、終了しません。

5. ユーザは、本ライセンスに署名しないので、本ライセンスに同意する必要はありません。ただし、プログラムまたはプログラムの派生物の修正または配布をユーザに許可するのは、本ライセンスだけです。ユーザが本ライセンスに同意しない場合、これらの行為は法律により禁止されます。したがって、プログラム（またはプログラムに基づく著作物）の修正または配布を行うことにより、ユーザは本ライセンスに同意し、プログラムまたはプログラムに基づく著作物の複製、配布、または修正の全条件に同意したとみなされます。

6. プログラム（またはプログラムに基づく著作物）を再配布するごとに、受領者は最初のライセンス許諾者から、本ライセンスの条件に基づいてプログラムを複製、配布、または修正するライセンスを自動的に取得します。受領者が本ライセンスに基づいて供与される権利を行使することについて、ユーザは一切、制約を課すことはできません。ユーザは、第三者が本ライセンスに従うように強制する責任はありません。

7. 裁判所の判決、特許権侵害の申し立て、または（特許の問題に限定されず）他の何らかの理由により、ユーザに対して（裁判所の命令、契約、その他により）本ライセンスの条件と矛盾する条件が課されたとしても、ユーザが本ライセンスの条件に従わないことの釈明にはなりません。本ライセンスに基づく義務および他の関連する義務を同時に満たす方法で配布できない場合、ユーザはプログラムを一切、配布できません。たとえば、特許ライセンスによって、ユーザから直接的または間接的に複製を受領したすべての第三者に対して、著作権料なしでのプログラムの再配布が許可されない場合、かかる条件と本ライセンスの条件の両方を満たすには、プログラムの配布を完全に停止する方法しかありません。

特定の状況において本項の一部が無効または履行不能となったとしても、本項の残りの条件は適用され、他の状況においては本項の全条件が適用されるものとします。

本項の目的は、ユーザに対して、何らかの特許権または他の所有権主張の侵害、またはかかる主張の有効性に対する異議申し立てを誘発することではありません。本項の唯一の目的は、パブリック ライセンスの慣習により実現されるフリー ソフトウェア配布システムの完全性を保護することです。多数の人々が、このシステムの一貫した継続を信頼して、このシステムにより配布される広範囲のソフトウェアに対して多大な貢献をしてきました。ソフトウェアを他のシステムで配布するかどうかを決定するのは著者 / 寄贈者であり、ライセンス取得者は、その選択を強制することはできません。

本項は、本ライセンスの他の項目がいかに重要であるかを完全に明確にすることを意図しています。

8. 一部の国において、特許または著作権との関連でプログラムの配布または使用が制限される場合、プログラムに本ライセンスを適用した最初の著作権所有者は、制限される国を除く明示的な地域上の配布制限を追加することにより、制限されない国に限定して配布を許可することができます。この場合、かかる制限は、本ライセンスの本文と同様に、本ライセンスに統合されます。

9. Free Software Foundation は、適宜、General Public License の改訂版または新規版を発行することができます。かかる新規版は、方針は現行版と同様ですが、新たな問題または関心事に対応するために詳細が異なることがあります。

各版には、個別のバージョン番号が付けられています。プログラムに、適用される本ライセンスのバージョン番号と「any later version（任意の以降のバージョン）」が指定されている場合、ユーザは適用されるバージョン、または Free Software Foundation により発行された任意の以降のバージョンのどちらかの条件を選択できます。プログラムに本ライセンスのバージョン番号が指定されていない場合、Free Software Foundation により発行された任意のバージョンを選択できます。

10. プログラムの一部を、配布条件が異なる他のフリー プログラムに統合したい場合には、書面により著者に許可を求めてください。Free Software Foundation により著作権保護されているソフトウェアに関しては、Free Software Foundation に問い合わせてください。例外が認められることがあります。当組織の決定は、フリー ソフトウェアのあらゆる派生物のフリー ステータスを保全する、およびソフトウェアの共有および再利用を幅広く促進するという、2 つの目的に基づいています。

無保証

11. プログラムは無料でライセンス供与されるので、適用法令により許可される範囲で、プログラムには保証は適用されません。書面により他に記述されている場合を除き、著作権所有者および他の当事者は、商品性および特定用途への適合性の暗黙の保証を含みますが、これらに限定されず、一切の保証を適用せずに、プログラムを「現状のまま」提供します。

プログラムの品質およびパフォーマンスに関するリスクはすべて、ユーザの責任になります。万一、プログラムに欠陥があった場合には、すべての必要なサービス、修繕、または修正の費用をユーザが負担するものとします。

12. 適用法令により要求された場合、または書面により同意された場合を除き、いかなる場合にも、すべての著作権所有者または前述の条件に従ってプログラムを修正または再配布できる他の当事者は、プログラムの使用または使用不能により生じた一般的、特殊、付随的、または間接的な損害（データ損失、不正確なデータ、ユーザまたは第三者の持続的な損失、またはプログラムと他のプログラムとの相互運用障害を含みますが、これらに限定されません）を含むユーザの損害に対して、当該所有者または他の当事者にかかる損害の可能性が通知されていたとしても、一切の責任を負いません。条件は以上です。



はじめに	xi
対象読者	xi
マニュアルの構成	xii
表記法	xiii
関連資料	xiv
マニュアルの入手方法	xv
Cisco.com	xv
Product Documentation DVD	xv
マニュアルの発注方法	xv
シスコ製品のセキュリティ	xvi
シスコ製品のセキュリティ問題の報告	xvi
テクニカル サポート	xvii
Cisco Technical Support & Documentation Web サイト	xvii
Japan TAC Web サイト	xvii
Service Request ツールの使用	xviii
問題の重大度の定義	xviii
その他の資料および情報の入手方法	xix

CHAPTER 1

概要	1-1
Web VPN の概要	1-1
リモート アクセスのモード	1-2
クライアントレス モード	1-3
シンクライアント モード	1-3
トンネル モード	1-4

CHAPTER 2

初期設定	2-1
CLI の使用方法	2-1
Catalyst 6500 シリーズ スイッチの初期設定	2-2
スイッチ上での VLAN の設定	2-2
レイヤ 2 スイッチング用の LAN ポートの設定	2-3
対応 VLAN へ WebVPN サービス モジュール の追加	2-3

WebVPN サービス モジュールの初期設定	2-4
WebVPN サービス モジュール上でのインターフェイスの設定	2-4
デフォルト ルートの設定	2-5
管理者用の認証の設定	2-5
初期設定の確認	2-6
タイムゾーンの設定	2-6
パスワードを忘れた場合	2-7

CHAPTER 3

WebVPN サービス モジュールの設定	3-1
アドレス解決の設定	3-2
IP アドレスへのホスト名の割り当て	3-2
ドメイン名の指定	3-3
ネーム サーバの指定	3-3
DNS のイネーブル化	3-4
仮想ゲートウェイの設定	3-5
エンド ユーザ認証の設定	3-6
仮想コンテキストの設定	3-8
CSD の設定	3-10
クライアントレス モードの設定	3-11
CIFS を使用したファイル共有の設定	3-13
シンクライアント モードの設定	3-15
ローカル ポートのガイドライン	3-16
ホスト名と IP アドレスの使用方法	3-18
トンネル モードの設定	3-18
ポリシーの設定	3-22
グループ ポリシーの設定	3-22
SSL ポリシーの設定 (任意)	3-23
TCP ポリシーの設定 (任意)	3-25
PKI の設定	3-28
鍵および証明書の設定	3-29
SCEP を使用したトラストポイントの設定	3-29
手動証明書登録	3-36
鍵ペアおよび証明書のインポートおよびエクスポート	3-45
3 レベルの認証局用の PEM ファイルをインポートする例	3-50
証明書およびトラストポイントの確認	3-54
鍵および証明書の共有	3-54
コンフィギュレーションの保存	3-55
保存したコンフィギュレーションの確認	3-56
保存したコンフィギュレーションの消去	3-56

鍵および証明書のバックアップ	3-56
セキュリティ上のガイドライン	3-56
鍵および証明書のモニタおよびメンテナンス	3-57
WebVPN サービス モジュールからの RSA 鍵の削除	3-57
鍵および証明書の表示	3-57
コンフィギュレーションからの証明書の削除	3-58
WebVPN のゲートウェイおよびコンテキストへの証明書の割り当て	3-58
証明書の更新	3-59
証明書の自動更新および自動登録	3-62

APPENDIX A

エンド ユーザ用の WebVPN の設定	A-1
WebVPN の起動	A-2
ユーザ名およびパスワード	A-3
エンド ユーザ インターフェイス	A-4
ページ フロー	A-4
初回の接続	A-5
503 Service Unavailable メッセージ	A-5
Out of Service ページ	A-5
SSL/TLS 証明書	A-6
ログイン ページ	A-7
証明書の認証	A-7
ログアウト ページ	A-8
ポータル ページ	A-8
リモート サーバ	A-9
WebVPN フローティング ツールバー	A-10
DNS および接続エラー	A-11
セッション タイムアウト	A-12
TCP ポート転送およびアプリケーション アクセス	A-12
その他の WebVPN 機能の使用方法	A-15
セキュリティ上の注意事項	A-17
ブラウザ キャッシングとセキュリティの関係	A-17
アプリケーション アクセス ホスト ファイル エラーからの回復	A-18
WebVPN でのホスト ファイルの使用	A-18
エンド ユーザがアプリケーション アクセスを不適切に終了した場合	A-18
対処方法	A-19
WebVPN でのホスト ファイルの自動再設定	A-19
ホスト ファイルの手動での再設定	A-20

APPENDIX B

組み込まれたテスト証明書のインポート B-1

APPENDIX C

ソフトウェアおよびライセンスのインストール C-1

イメージのアップグレード C-2

アプリケーション ソフトウェアのアップグレード C-2

メンテナンス ソフトウェアのアップグレード C-4

クライアント パッケージのインストール C-6

トンネル モード用の SVC パッケージ C-6

CSD パッケージ C-8

ライセンス アップグレードのインストール C-10

APPENDIX D

カラー名および RGB カラー値 D-1

INDEX

索引



はじめに

ここでは、『*Catalyst 6500 シリーズ スイッチ WebVPN サービス モジュール ソフトウェア コンフィギュレーション ガイド*』の対象読者、マニュアルの構成、および手順や情報を記述する表記法について説明します。

このマニュアルには、Catalyst 6500 シリーズ スイッチ シャーシを取り付ける手順は記載されていません。スイッチ シャーシの取り付けの詳細については、『*Catalyst 6500 Series Switch Installation Guide*』を参照してください。

対象読者

このマニュアルは、Catalyst 6500 シリーズ スイッチの設定および保守を担当する、経験豊富なネットワーク管理者を対象としています。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	概要	Catalyst 6500 シリーズ スイッチ WebVPN サービス モジュール の概要について説明します。
第 2 章	初期設定	Catalyst 6500 シリーズ スイッチと WebVPN サービス モジュール の初期設定、およびパスワードの回復手順について説明します。
第 3 章	WebVPN サービス モジュールの設定	WebVPN サービス モジュール の設定手順について説明します。
付録 A	エンド ユーザ用の WebVPN の設定	エンド ユーザ リモート システムの設定要件およびタスクについて説明します。
付録 B	組み込まれたテスト証明書のインポート	組み込まれたテスト証明書をインポートする方法が記載されています。
付録 C	ソフトウェアおよびライセンスのインストール	アプリケーション パーティションおよびメンテナンス パーティションのアップグレード、Cisco Secure Desktop (CSD) および SSL VPN Client (SVC) パッケージのインストールに関する情報が記載されています。
付録 D	カラー名および RGB カラー値	WebVPN コンテキストで、 <code>title-color color</code> コマンドおよび <code>secondary-color color</code> コマンドを入力する場合の有効なカラー名および RGB 値が記載されています。

表記法

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンド、コマンド オプション、およびキーワードは太字で示しています。
イタリック体	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。
[]	角カッコの中の要素は、省略可能です。
{ x y z }	必ずどれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、かぎカッコ (<>) で囲んで示しています。

(注) は、次のように表しています。



(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。

ヒントは、次のように表しています。



ヒント

「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

注意は、次のように表しています。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

インストールおよびコンフィギュレーションの詳細については、次のマニュアルを参照してください。

- 『*Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*』
- 『*Catalyst 6500 Series Switch WebVPN Services Module Installation and Verification Note*』
- 『*Catalyst 6500 Series Switch WebVPN Services Module System Message Guide*』
- 『*Catalyst 6500 Series Switch WebVPN Services Module Command Reference*』
- 『*Catalyst 6500 Series Switch Installation Guide*』
- 『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』
- 『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』
- 『*Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720 and Supervisor Engine 2*』
- MIB（管理情報ベース）については、次の URL を参照してください。
<http://www.cisco.com/go/mibs>

マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手することができます。また、テクニカル サポートおよびその他のテクニカル リソースは、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

シスコの最新のマニュアルは、次の URL からアクセスしてください。

<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>

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

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

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

Product Documentation DVD

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、ポータブル メディアに収容された、技術的な製品マニュアルの総合的なライブラリです。この DVD を使用すると、シスコ製品の各種バージョンのハードウェアのインストール、ソフトウェアのインストール、設定、およびコマンドに関するガイドにアクセスし、HTML で技術マニュアルを表示できます。DVD を使用することで、インターネットに接続しなくてもシスコの Web サイトと同じマニュアルを参照できます。製品によっては、マニュアルの PDF バージョンも用意されています。

Product Documentation DVD は単一製品として、またはサブスクリプションとして入手できます。Cisco.com(Cisco Direct Customers)に登録されている場合、Cisco Marketplace から Cisco Documentation DVD (Customer Order Number DOC-DOCDVD=) 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

Cisco.com に登録されている場合、2005 年 6 月 30 日から、次の URL にある Cisco Marketplace の Product Documentation Store でシスコ製品のマニュアルを発注できます。

<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わせください。

シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

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

このサイトから、以下のタスクを実行できます。

- シスコ製品における脆弱性を報告する。
- シスコ製品のセキュリティ問題に対する支援を受ける。
- シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告および注意のリストを、以下の URL で確認できます。

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

勧告および注意事項が変更された際に、リアルタイムで確認したい場合は、以下の URL から Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) にアクセスできます。

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、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- 緊急度の高い問題 security-alert@cisco.com
緊急度の高い問題とは、システムが激しい攻撃を受けている状態、または急を要する深刻なセキュリティの脆弱性を報告する必要がある状態を指します。それ以外の状態はすべて、緊急度の低い問題とみなされます。
- 緊急度の低い問題 psirt@cisco.com

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

- 1 877 228-7302
- 1 408 525-6532



ヒント

お客様が第三者に知られたいくない情報をシスコに送信する場合、Pretty Good Privacy (PGP) または PGP と互換性のある製品を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.x ~ 8.x と互換性のある暗号化情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT と通信する際に使用する有効な公開鍵は、次の URL にある Security Vulnerability Policy ページの Contact Summary の項にリンクされたものです。

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

このページのリンクには、現在使用中の PGP 鍵の ID が含まれます。

テクニカル サポート

Cisco Technical Support では、評価の高い 24 時間体制のテクニカル 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、広範囲にわたるオンラインでのサポート リソースを提供しています。さらに、シスコシステムズとサービス契約を結んでいる場合は、Technical Assistance Center (TAC) のエンジニアによる電話サポートも提供されます。シスコシステムズとサービス契約を結んでいない場合は、リセラーにお問い合わせください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。この Web サイトは 24 時間ご利用いただけます。次の URL にアクセスしてください。

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

Cisco Technical Support & Documentation Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

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



(注)

テクニカル サポートにお問い合わせいただく前に、Cisco Product Identification (CPI) ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support & Support Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI ツールでは、3 種類の検索オプションを使用できます。製品 ID またはモデル名による検索、ツリー表示または特定の製品の検索、および show コマンドの出力のコピー & ペーストによる検索です。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

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/>

Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカルサポートを受けられます（ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合）。状況をご説明いただくと、TAC Service Request ツールが推奨される解決方法を提供します。これらの推奨リソースを使用しても問題が解決しない場合は、シスコの技術者が対応します。TAC Service Request ツールは次の URL からアクセスできます。

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

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください（運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合）。S1 および S2 の問題にはシスコの技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカルサポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋：+61 2 8446 7411（オーストラリア：1 800 805 227）

EMEA：+32 2 704 55 55

米国：1 800 553-2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

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

問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

重大度 1 (S1) ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

重大度 2 (S2) ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

重大度 3 (S3) ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

重大度 4 (S4) シスコ製品の機能、インストレーション、基本的な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で、業務への影響がほとんどまたはまったくない場合。

その他の資料および情報の入手方法

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することができます。

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL から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、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。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テクニカル ユーザ向けの季刊誌で、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のに役立ちます。『Packet』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『Packet』には、次の URL からアクセスしてください。

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

- 『iQ Magazine』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『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>

または次の URL でデジタル版をご覧ください。

<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、シスコシステムズ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ク製品およびカスタマー サポート サービスについては、次の URL にアクセスしてください。

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

- Networking Professionals Connection は、ネットワークング専門家がネットワークング製品やネットワークング技術に関する質問、提案、情報をシスコの専門家および他のネットワークング専門家と共有するためのインタラクティブな Web サイトです。ディスカッションに参加するには、次の URL にアクセスしてください。

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

- シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの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>



概要

この章では、WebVPN サービス モジュールの概要、機能、およびリモート アクセスのモードについて説明します。内容は、次のとおりです。

- [Web VPN の概要 \(p.1-1\)](#)
- [リモート アクセスのモード \(p.1-2\)](#)

Web VPN の概要

WebVPN サービス モジュールは、Catalyst 6500 シリーズ スイッチに搭載できるレイヤ 4 ~ 7 サービス モジュールです。Web VPN により、エンド ユーザは Web ブラウザを使用してセキュアなリモート アクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェアのクライアントは不要です。Web VPN を使用すると、HTTPS インターネット サイトに接続できるほとんどのコンピュータ上で、広範囲の Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。Web VPN は、Secure Socket Layer Protocol およびそれを継承する Transport Layer Security (SSL/TLS1) を使用して、リモート エンド ユーザと、中央サイトに設定したサポート対象の特定の内部リソース間にセキュアな接続を提供します。WebVPN サービス モジュールにより、プロキシが必要な接続が認識されると、HTTP サーバが認証サブシステムと通信し、エンド ユーザを認証します。

ネットワーク管理者は、グループ単位で、エンド ユーザに WebVPN リソースへのアクセスを提供します。エンド ユーザは、内部ネットワークのリソースに直接アクセスすることはできません。

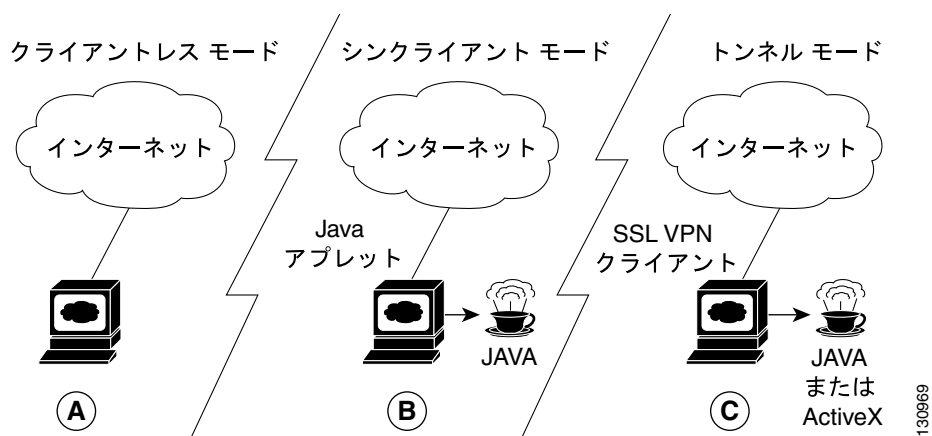
WebVPN サービス モジュール上の接続は、リモート アクセス IPsec 接続とはまったく異なります。WebVPN 接続では、WebVPN サービス モジュールは、エンド ユーザの Web ブラウザとターゲット Web サーバ間のプロキシとして動作します。WebVPN のエンド ユーザが SSL 対応 Web サーバに接続すると、WebVPN サービス モジュールがセキュアな接続を確立し、サーバの SSL 証明書を評価します。エンド ユーザのブラウザは、提示された証明書を受信できないので、証明書を評価したり、確認することはできません。

リモートアクセスのモード

エンド ユーザのログインおよび認証は、Web ブラウザにより、HTTP リクエストを使用して、セキュアゲートウェイに対して実行されます。これにより、クッキーにより参照されるセッションが作成されます。認証されると、エンド ユーザに対して、WebVPN ネットワークにアクセスできるポータル ページが表示されます。ブラウザから送信されるリクエストにはすべて、認証クッキーが含まれます。ポータル ページにより、内部ネットワーク上の使用可能なすべてのリソースが提供されます。たとえば、ポータル ページにより、シンクライアントの Java アプレット (TCP ポート転送) またはトンネリング クライアントをダウンロードおよびインストールできるリンクを、エンド ユーザに提供できます。

図 1-1 に、リモートアクセス モードの概要を示します。

図 1-1 リモートアクセス モードの概要



A	クライアントレス モード	B	シンクライアント モード	C	トンネル モード
	<ul style="list-style-type: none"> ブラウザベース(クライアントレス) Web 対応アプリケーション、ファイル共有 (CIFS)、Outlook Web Access (OWA) ゲートウェイが、アドレスまたはプロトコルの変換、コンテンツの解析と書き換えを実行 		<ul style="list-style-type: none"> TCP ポート転送 Java アプレットを使用 アプリケーション サポートを拡張 Telnet、Eメール、SSH、Meeting Maker、Sametime スタティックなポートベース アプリケーション 		<ul style="list-style-type: none"> 「クライアントレス」IPsec のように動作 Java または ActiveX によりロードされたクライアントのトンネリング (約 500 kB) アプリケーションを認識しないすべての IP ベース アプリケーションをサポート スケーラブル 管理者がインストールを許可

以降のセクションで、サポートされる 3 つのリモートアクセス モードについて説明します。

- [クライアントレス モード \(p.1-3\)](#)
- [シンクライアント モード \(p.1-3\)](#)
- [トンネル モード \(p.1-4\)](#)

クライアントレス モード

クライアントレス モードでは、エンド ユーザは、クライアント マシン上の Web ブラウザを使用して内部ネットワークまたは企業ネットワークにアクセスします。

クライアントレス モードでは、次のアプリケーションがサポートされます。

- Web ブラウジング (HTTP およびセキュア HTTP [HTTPS] を使用) エンド ユーザは、ポータル ページ上の URL ボックスと Web サーバ リnkのリストを使用して、Web をブラウズできます。
- ファイル共有 (Common Internet File System [CIFS] を使用) エンド ユーザは、ポータル ページ上のファイル サーバ リnkのリストを使用して、次の操作を実行できます。
 - ネットワークのブラウズ (ドメインのリスト)
 - ドメインのブラウズ (サーバのリスト)
 - サーバのブラウズ (共有のリスト)
 - 共有ファイルのリスト
 - 新規ファイルの作成
 - ディレクトリの作成
 - ディレクトリの名前変更
 - ファイルの更新
 - ファイルのダウンロード
 - ファイルの削除
 - ファイルの名前変更
- Microsoft Outlook Web Access (OWA) 2003 などの Web ベース E メール (HTTP および HTTPS を使用) および Web Distributed Authoring and Versioning (WebDAV) 拡張機能 エンド ユーザは、リンクを使用して Exchange サーバに接続し、Web ベース E メールを読むことができます。

シンクライアント モード

シンクライアント モードは、TCP ポート転送とも呼ばれ、クライアントのアプリケーションが TCP を使用して既知のサーバおよびポートに接続することを前提としています。

シンクライアント モードでは、エンド ユーザは、ポータル ページに提供されたリンクをクリックして、Java アプレットをダウンロードします。Java アプレットは、ゲートウェイに設定するサービスに対して、クライアント マシン上の TCP プロキシとして動作します。

シンクライアント モードでサポートされるアプリケーションは、主に E メール ベース (SMTP、POP3、および IMAP4) アプリケーションです。



(注)

TCP ポート転送プロキシが動作するのは、Sun 1.4 Java Virtual Machine (JVM) 以降のリリースだけです。ブラウザが 1.4 JVM をダウンロードするように、HTML が指定されます。アプレットも JVM のバージョンをチェックし、互換性のないバージョンの場合、実行を拒否します。

Java アプレットは、エンド ユーザクライアントから WebVPN ゲートウェイへの HTTP リクエストを開始します。HTTP リクエスト (POST または CONNECT) には、内部 E メール サーバの名前およびポート番号が含まれます。WebVPN ゲートウェイは、指定された内部 E メール サーバおよびポートへの TCP 接続を作成します。

Java アプレットは、すべてのクライアント接続について、新しい SSL 接続を開始します。

シンクライアント モードを使用する場合には、次の制約に注意してください。

- エンド ユーザに、Java アプレットのダウンロードおよびインストールを許可する必要があります。
- ポートがダイナミックにネゴシエートされる FTP などのアプリケーションには、シンクライアント モードを使用できません。TCP ポート転送を使用できるのは、スタティック ポートだけです。
- アプリケーションをシームレスに動作させるには、エンド ユーザに管理者権限を提供する必要があります。エンド ユーザに管理者権限を提供しない場合、エンド ユーザは、アプリケーションを適正に動作させるために、クライアント プログラムの設定を手動で変更する必要があります。

トンネル モード

一般的なクライアントレス リモート アクセスの場合、エンド ユーザは SSL トンネルを確立し、アプリケーション レイヤで内部ネットワークとのデータ通信 (Web および E メールなど) を行います。トンネル モードでは、エンド ユーザは SSL トンネルを使用して、ネットワーク (IP) レイヤでデータ通信を行います。したがって、トンネル モードでは、ほとんどの IP ベース アプリケーションがサポートされます。トンネル モードは、多数の一般的な企業アプリケーション (Microsoft Outlook、Microsoft Exchange、Lotus Notes E-mail、Telnet など) をサポートしています。

トンネル接続は、グループ ポリシー設定により判別されます。エンド ユーザの PC に、SSL VPN クライアント (SVC) がダウンロードおよびインストールされ、エンド ユーザが WebVPN ゲートウェイにログインした時点で、トンネル接続が確立されます。

デフォルトでは、SVC は、接続終了後にクライアントの PC から削除されます。任意に、クライアントの PC に SVC を常時インストールしておくこともできます。



初期設定

この章では、WebVPN サービス モジュール の初期設定の手順について説明します。内容は、次のとおりです。

- [CLI の使用方法 \(p.2-1\)](#)
- [Catalyst 6500 シリーズ スイッチの初期設定 \(p.2-2\)](#)
- [WebVPN サービス モジュールの初期設定 \(p.2-4\)](#)
- [初期設定の確認 \(p.2-6\)](#)
- [タイムゾーンの設定 \(p.2-6\)](#)
- [パスワードを忘れた場合 \(p.2-7\)](#)

CLI の使用方法

WebVPN サービス モジュール のソフトウェア インターフェイスは、Cisco IOS CLI (コマンドライン インターフェイス) です。Cisco IOS CLI および Cisco IOS コマンド モードの詳細については、『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』の第 2 章「Command-Line Interfaces」を参照してください。

スイッチが完全に信頼できる環境に設置されている場合を除き、モジュールのコンソール ポートに直接接続するか、Secure Shell (SSH) を使用した暗号化セッションにより、WebVPN サービス モジュール を設定することを推奨します。モジュール上での SSH 設定の詳細は、「[管理者用の認証の設定](#)」(p.2-5)を参照してください。



(注)

初回の WebVPN サービス モジュール 設定は、モジュールのコンソール ポートに直接接続して実行する必要があります。

Catalyst 6500 シリーズスイッチの初期設定

ここでは、Catalyst 6500 シリーズスイッチ上での次の作業の手順について説明します。

- [スイッチ上での VLAN の設定 \(p.2-2\)](#)
- [レイヤ2スイッチング用の LAN ポートの設定 \(p.2-3\)](#)
- [対応 VLAN へ WebVPN サービス モジュール の追加 \(p.2-3\)](#)

スイッチ上での VLAN の設定

スイッチとモジュールの VLAN ID が一致している必要があります。詳細については、『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』の「Configuring VLANs」の章を参照してください。



(注) WebVPN ソフトウェアがサポートしているのは、標準範囲の VLAN(2 ~ 1005)だけです。WebVPN サービス モジュール には、標準範囲の VLAN だけを設定してください。

スイッチ上で VLAN を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# configure terminal	terminal オプションを選択して、コンフィギュレーションモードを開始します。
ステップ 2	Router(config)# vlan vlan_ID	VLAN コンフィギュレーションモードを開始し、VLAN を追加します。有効範囲は、2 ~ 1001 です。 (注) 外部 VLAN は追加しないでください。
ステップ 3	Router(config-vlan)# end	VLAN データベースを更新し、イネーブル EXEC モードに戻ります。


次に、スイッチ上で VLAN を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# vlan 100
VLAN 100 added:
    Name: VLAN100

Router(config-vlan)# end
```

レイヤ 2 スイッチング用の LAN ポートの設定

レイヤ 2 スイッチング用の LAN ポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# interface <i>type</i> ¹ <i>mod/port</i>	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# switchport	LAN ポートをレイヤ 2 スイッチング用に設定します。  (注) LAN ポートをレイヤ 2 ポートとして設定するには、追加の switchport コマンドをキーワードで入力する前に、 switchport コマンドを 1 回、キーワードを指定しないで入力する必要があります。
ステップ 3	Router(config-if)# switchport mode access	LAN ポートに永続的な非トランク モードを設定し、リンクを非トランク リンクに変換するようにネゴシエートします。近接 LAN ポートが変更に同意しなくても、LAN ポートは非トランク ポートになります。
ステップ 4	Router(config-if)# switchport access vlan <i>vlan_ID</i>	インターフェイスがトランクを停止した場合に使用するデフォルトの VLAN を設定します。
ステップ 5	Router(config-if)# no shutdown	インターフェイスをアクティブにします。


1. *type* = ethernet、fastethernet、gigabithernet、または tengigabithernet

次に、レイヤ 2 スイッチング用の LAN ポートを設定する例を示します。

```
Router(config)# interface gigabithernet 1/1
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 100
Router(config-if)# no shutdown
Router(config-if)# exit
```

対応 VLAN へ WebVPN サービス モジュール の追加

対応 VLAN に WebVPN サービス モジュール を追加するには、次の作業を行います。

コマンド	目的
Router (config)# webvpn module <i>mod</i> allowed-vlan <i>vlan_ID</i>	WebVPN サービス モジュール へのトランク上で許可する VLAN を設定します。  (注) 許可する VLAN の 1 つを管理 VLAN にする必要があります。

次に、スロット 3 に搭載した WebVPN サービス モジュール を、特定の VLAN に追加する例を示します。

```
Router>
Router> enable
Router# configure terminal
Router (config)# webvpn module 3 allowed-vlan 100
Router (config)# end
```

WebVPN サービス モジュールの初期設定



(注) 次に説明する WebVPN サービス モジュールの初期設定は、WebVPN サービス モジュールのコンソールポートに直接接続する方法で行う必要があります。初期設定の完了後、モジュールへの SSH または Telnet 接続により、他のモジュール設定を行うことができます。

WebVPN サービス モジュールの初期設定では、次の作業を行います。

- WebVPN サービス モジュール上でのインターフェイスの設定 (p.2-4)
- デフォルトルートの設定 (p.2-5)
- 管理者用の認証の設定 (p.2-5)

WebVPN サービス モジュール上でのインターフェイスの設定



(注) WebVPN0 インターフェイスはデフォルトでイネーブルに設定されているので、シャットダウンまたは他の設定を行わないでください。

WebVPN インターフェイスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config)# interface webvpn interface-number.subinterface-number</code>	設定するサブインターフェイスを選択します。
ステップ 2	<code>webvpn(config-subif)# encaps dot1q vlan_id</code>	802.1Q を使用して、サブインターフェイスから指定した <i>vlan-id</i> に、カプセル化を使用せずに、イーサネットフレームを送信します。
ステップ 3	<code>webvpn(config-subif)# ip address ip-address ip-address-mask</code>	サブインターフェイス上に IP アドレスを設定します。
ステップ 4	<code>webvpn(config-subif)# no shutdown</code>	サブインターフェイス上で WebVPN アクセスをイネーブルにします。

次に、WebVPN インターフェイスを設定する例を示します。

```
webvpn(config)# interface webvpn 0.1
webvpn(config-subif)# encaps dot1q 100
webvpn(config-subif)# ip address 10.10.1.10
webvpn(config-subif)# no shutdown
webvpn(config-subif)# exit
webvpn(config)#
```

デフォルト ルートの設定

デフォルト ルートを設定するには、次の作業を行います。

コマンド	目的
<code>webvpn(config)# ip route prefix mask ip-address</code>	デフォルト ルートを設定します。

次に、デフォルト ルートを設定する例を示します。

```
webvpn(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.100
webvpn(config)#
```

管理者用の認証の設定

Authentication、Authorization、Accounting (AAA; 認証、許可、アカウントिंग) を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config)# username username secret {0 5} password</code>	指定した検索不能なユーザ名に対し、拡張パスワードセキュリティをイネーブルにします。
ステップ 2	<code>webvpn(config)# enable password password</code>	まだ指定していない場合、ローカル イネーブル パスワードを指定します。
ステップ 3	<code>webvpn(config)# aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	<code>webvpn(config)# aaa authentication login default local</code>	認証にローカル ユーザ名データベースを使用するモジュールを指定します。
ステップ 5	<code>webvpn(config)# line vty line-number ending-line-number</code>	設定する回線範囲を指定し、ライン コンフィギュレーション モードを開始します。
ステップ 6	<code>webvpn(config-line)# transport input [ssh telnet all]</code>	回線で使用するプロトコルを設定します。

次に、WebVPN サービス モジュールへのSSH 接続にAAA を設定する例を示します。

```
webvpn(config)# username admin secret admin-pass
webvpn(config)# enable password enable-pass
webvpn(config)# aaa new-model
webvpn(config)# aaa authentication login default local
webvpn(config)# line vty 0 4
webvpn(config-line)# transport input ssh
webvpn(config-line)# end
webvpn#
```

初期設定の確認

次に、表示された VLAN 情報が VLAN 設定と一致しているかどうかを確認する例を示します。

```
Router# show webvpn mod 3 state
SSL-VPN module 3 data-port:2

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 2-1001
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:100
Vlans allowed and active in management domain: 6-8,10-13,17-18,24,30,80,170,172,255
Vlans in spanning tree forwarding state and not pruned:
    6-8,10-13,17-18,24,30,80,170,172,255
Allowed-vlan : 2-1001
```

タイムゾーンの設定

設定した時刻とタイムゾーン情報は、スーパーバイザー エンジンから WebVPN サービス モジュールに送信されます。状況によっては、WebVPN サービス モジュール上のタイムゾーン情報が正しく設定されないことがあります。

タイムゾーン情報を設定するには、次の作業を行います。

コマンド	目的
webvpn(config)# clock timezone zone hours-offset [minutes-offset]	表示するタイムゾーンを設定します。

次に、タイムゾーンを UTC (協定世界時) より 8 時間遅れの Pacific Standard Time (PST; 太平洋標準時) に設定する例を示します。

```
webvpn(config)# clock timezone PST -8
```

パスワードを忘れた場合



(注) WebVPN サービス モジュールのパスワードを回復するには、スーパーバイザ エンジンにアクセスできる必要があります。スーパーバイザ エンジン上のイネーブル パスワードを回復する手順については、ご使用のソフトウェア プラットフォームのソフトウェア コンフィギュレーション ガイドを参照してください。



(注) パスワードの回復スクリプトを実行するには、WebVPN サービス モジュール が Application Partition (AP; アプリケーション パーティション) に置かれている必要があります。



注意

セキュリティ上、パスワードの回復後は、すべての秘密鍵が使用不可になります。

WebVPN サービス モジュール 上でパスワードを回復するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router> enable	イネーブル モードを開始します。
ステップ 2	Router# copy tftp: pcl#mod-fs:	指定したモジュールにスクリプトをダウンロードします。
ステップ 3	webvpn# copy system:startup-config nvram:running-config	スタートアップ コンフィギュレーションを実行コンフィギュレーションに保存します。
ステップ 4	webvpn(config)# enable password password	ローカル イネーブル パスワードを指定します。
ステップ 5	webvpn(config)# line vty starting-line-number ending-line-number	設定する回線範囲を指定し、ライン コンフィギュレーション モードを開始します。
ステップ 6	webvpn(config-line)# login	ログイン時のパスワード確認をイネーブルにします。
ステップ 7	webvpn(config-line)# password password	回線上にパスワードを指定します。
ステップ 8	webvpn(config-line)# end	ライン コンフィギュレーション モードを終了します。
ステップ 9	webvpn# copy system:running-config nvram:startup-config	設定を NVRAM に保存します。
ステップ 10	Router# hw-module module mod reset	モジュールをリセットします。

次に、スロット 4 に搭載した WebVPN サービス モジュール上で、パスワードを回復する例を示します。

- スーパーバイザ エンジンから、次のコマンドを入力します。

```
Router> enable
Password:
Router# copy tftp: p1c#4-fs:
Address or name of remote host []? 10.1.1.100
Source filename []? images/c6svc-webvpn-pwr.1-1-1.bin
Destination filename [images/c6svc-webvpn-pwr.1-1-1.bin]?
Accessing tftp://10.1.1.100/images/c6svc-webvpn-pwr.1-1-1.bin...
Loading images/c6svc-webvpn-pwr.1-1-1.bin from 10.1.1.100(via Vlan999): !
[OK - 435 bytes]

435 bytes copied in 0.092 secs (4728 bytes/sec)
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:MP upgrade/Password Recovery started.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Uncompress of the file succeeded.
Continuing upgrade/recovery.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:This file appears to be a
PasswordRecovery image. Continuing.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Extraction of password recovery image
succeeded.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Continuing with password recovery.

2003 Nov 10 21:55:03 %SYS-3-SUP_ERRMSGFROMPC:System in password recovery mode.
2003 Nov 10 21:55:03 %SYS-3-SUP_ERRMSGFROMPC>Please recover configuration and reset
board.

Router#
```

- WebVPN サービス モジュールのコンソール ポートから、次のコマンドを入力します。

```
webvpn# copy system:startup-config nvram:running-config

webvpn(config)# enable password cisco
webvpn(config)# line vty 0 4
webvpn(config-line)# login
webvpn(config-line)# password cisco
webvpn(config-line)# end
webvpn# copy system:running-config nvram:startup-config
```

- スーパーバイザ エンジンから、次のコマンドを入力します。

```
Router# hw-module module 4 reset
```

- WebVPN サービス モジュールのコンソール ポートから、バックアップしてある鍵をインポートするか、または鍵を再生成します。

鍵の生成およびインポートの詳細については、「[鍵および証明書の設定](#)」(p.3-29)を参照してください。



WebVPN サービス モジュールの設定

この章では、モジュールの CLI (コマンドライン インターフェイス) から WebVPN サービス モジュールを設定する方法について説明します。

- [アドレス解決の設定 \(p.3-2\)](#)
- [仮想ゲートウェイの設定 \(p.3-5\)](#)
- [エンド ユーザ認証の設定 \(p.3-6\)](#)
- [仮想コンテキストの設定 \(p.3-8\)](#)
- [ポリシーの設定 \(p.3-22\)](#)
- [PKI の設定 \(p.3-28\)](#)

アドレス解決の設定

固有の各 IP アドレスには、関連するホスト名があります。Cisco IOS ソフトウェアは、`connect`、`telnet`、および `ping EXEC` コマンドと、関連する Telnet サポート操作で使用するために、ホスト名とアドレスのマッピングのキャッシュを保持しています。このキャッシュにより、ホスト名を迅速にアドレスに変換できます。

IP には、IP 内の位置によって装置を識別するために、命名規則が定義されています。これは、ドメインを表す階層的な命名規則です。ドメイン名は、区切り文字のピリオド (.) により連結されます。たとえば、Cisco は、IP では `com` のドメイン名で識別される商業組織に属するので、ドメイン名は `cisco.com` になります。このドメイン内の特定の装置、たとえば File Transfer Protocol (FTP; ファイル転送プロトコル) システムは、`ftp.cisco.com` として識別されます。

ドメイン名を追跡できるように、IP は、IP アドレスにマッピングされた名前前のキャッシュ (またはデータベース) を保持する `ネーム サーバ` というコンセプトを定義しています。ドメイン名を IP アドレスにマッピングするには、最初にホスト名を指定し、次に `ネーム サーバ` を指定して、Domain Name System (DNS; ドメイン ネーム システム) をイネーブルにします。DNS は、ネットワーク装置を一意に識別するインターネットのグローバルな命名機構です。

以降では、次の作業について説明します。

- [IP アドレスへのホスト名の割り当て \(p.3-2\)](#)
- [ドメイン名の指定 \(p.3-3\)](#)
- [ネーム サーバの指定 \(p.3-3\)](#)
- [DNS のイネーブル化 \(p.3-4\)](#)

VPN Routing and Forwarding (VRF) インスタンスは、IP ルーティング テーブル、派生したフォワーディング テーブル、フォワーディング テーブルを使用するインターフェイスのセット、およびフォワーディング テーブルへの入力情報を判断する一連のルールとルーティング プロトコルにより構成されます。通常、VRF には、Provider Edge (PE; プロバイダー エッジ) ルータに接続しているカスタマー VPN サイトを定義する、ルーティング情報が含まれています。

VRF 対応の DNS 機能をイネーブルにするには、グローバル コンフィギュレーション モードで、次の作業を行います。

- `ip vrf name` コマンドによる VRF ルーティング テーブルの設定
- `ip name-server vrf name` コマンドによる、VRF の最低 1 つの `ネーム サーバ` の設定
- `ip domain lookup` コマンドによる、ドメイン検索のイネーブル化

任意に、`ip domain name vrf name` コマンドまたは `ip domain list vrf name` コマンドを使用して、VRF 固有のデフォルト ドメイン名またはドメイン リストを設定することもできます。

IP アドレスへのホスト名の割り当て

Cisco IOS ソフトウェアは、ホスト名と対応するアドレスのテーブル (ホスト名とアドレスのマッピング) を保持します。Telnet などの上位レイヤ プロトコルは、ホスト名を使用してネットワーク装置 (ホスト) を識別します。ルータおよび他のネットワーク装置は、他の IP 装置と通信するために、ホスト名と IP アドレスを関連付ける必要があります。ホスト名と IP アドレスは、スタティックまたはダイナミックな方法で、相互に関連付けることができます。

ダイナミック マッピングを使用できない場合には、アドレスに手動でホスト名を割り当てる方法が便利です。

アドレスにホスト名を割り当てるには、グローバル コンフィギュレーション モードで、次の作業を行います。

コマンド	目的
Router(config)# ip host [vrf name] hostname [tcp-port-number] address1 [address2...address8]	ホスト名と IP アドレスをスタティックに関連付けます。VRF 名を指定すると、VRF 固有のキャッシュにネーム エントリが作成されます。VRF 固有のネーム キャッシュが存在しない場合には、キャッシュがダイナミックに作成されます。VRF 名を指定しない場合、ネーム エントリはグローバル キャッシュに作成されます。

ドメイン名の指定

Cisco IOS ソフトウェアがドメイン名リクエストを完了するために使用する、デフォルトのドメイン名を指定できます。単一のドメイン名またはドメイン名のリストを指定します。ドメイン名が含まれていない IP ホスト名はすべて、指定したドメイン名が付加されてから、ホスト テーブルに追加されます。

1 つまたは複数のドメイン名を指定するには、グローバル コンフィギュレーション モードで、次のいずれかの作業を行います。

コマンド	目的
Router(config)# ip domain name [vrf name] name	Cisco IOS ソフトウェアがドメイン名のないホスト名を完成させるために使用する、デフォルトのドメイン名を定義します。VRF 名を指定すると、ドメイン名は、指定した VRF 内のネーム クエリだけに使用されます。
Router(config)# ip domain list [vrf name] name	ドメイン名のないホスト名を完成させる、デフォルトドメイン名のリストを定義します。VRF 名を指定すると、ドメイン名は、指定した VRF 内のネーム クエリだけに使用されます。

次に、いくつかの代替ドメイン名を使用して、ドメイン名のリストを設定する例を示します。

```
Router(config)# ip domain list csi.com
Router(config)# ip domain list telecomprog.edu
Router(config)# ip domain list merit.edu
```

ネーム サーバの指定

DNS の名前情報を提供するネーム サーバとして動作する 1 つまたは複数のホスト(最大 6)を指定するには、グローバル コンフィギュレーション モードで、次の作業を行います。

コマンド	目的
Router(config)# ip name-server [vrf name] server-address1 [server-address2... server-address6]	名前情報を提供する 1 つまたは複数のホストを指定します。

DNS のイネーブル化

ネットワーク装置を、名前の割り当てを制御できないネットワーク上の装置に接続する必要がある場合には、内部ネットワーク全体で装置を一意に識別するデバイス名を指定できます。この作業を行うには、インターネットのグローバル ネーミング機構である DNS を使用します。このサービスは、デフォルトでイネーブルです。

ディセーブルにした DNS を再びイネーブルにするには、グローバル コンフィギュレーション モードで、次の作業を行います。

コマンド	目的
Router(config)# ip domain lookup	DNS ベースのホスト名からアドレスへの変換をイネーブルにします。

ホスト名とアドレスのマッピングのキャッシュは、**connect**、**telnet**、**ping**、**trace**、**write net**、および **configure net EXEC** コマンドの実行時に、名前を迅速にアドレスに変換するために使用されます。このコマンド例では、ダイナミックな名前検索の使用を指定しています。スタティックな名前検索を設定することもできます。

次に、ホスト名からアドレスへのマッピングを設定する例を示します。IP DNS ベースの変換を指定し、ネーム サーバのアドレスを指定し、デフォルトのドメイン名を指定します。

```
Router(config)# ip domain lookup
Router(config)# ip name-server 131.108.1.111 131.108.1.2
Router(config)# ip domain name cisco.com
```

仮想ゲートウェイの設定

仮想ゲートウェイは、`webvpn gateway gateway_name` コマンドを使用して定義します。このゲートウェイは、WebVPN のコンテキスト内で参照されます。

仮想ゲートウェイ サービスを設定するには、次の作業を行います。

コマンド	目的
ステップ 1 <code>webvpn(config)# webvpn gateway gateway_name</code>	仮想ゲートウェイ サービスの名前を定義します。  (注) <code>gateway_name</code> の値は、大文字と小文字が区別されます。
ステップ 2 <code>webvpn(config-webvpn-gateway)# ip address ip_addr [mask_addr]¹ port port [secondary^{2,3,4}]</code>	WebVPN サービス モジュール がプロキシとなる仮想 IP アドレスおよびポート番号を定義します。デフォルトの <code>port</code> は、443 です。  (注) 仮想 IP アドレスが、直接接続しているネットワーク上に存在しない場合には、 <code>secondary</code> キーワードが必要です。
ステップ 3 <code>webvpn(config-webvpn-gateway)# http-redirect [port port]</code>	HTTP ポート (デフォルトの <code>port</code> は 80) をオープンし、仮想ゲートウェイへのすべての HTTP 接続が Secure HTTP (HTTPS) を使用するように指定します。
ステップ 4 <code>webvpn(config-webvpn-gateway)# policy tcp tcp_policy_name⁵</code>	(任意) TCP ポリシーを適用します。TCP ポリシーのパラメータは、「TCP ポリシーの設定 (任意)」(p.3-25)を参照してください。TCP ポリシーは、クライアント側の接続だけに影響します。
ステップ 5 <code>webvpn(config-webvpn-gateway)# policy ssl ssl_policy_name⁵</code>	(任意) SSL ポリシーを適用します。SSL ポリシーのパラメータは、「SSL ポリシーの設定 (任意)」(p.3-23)を参照してください。SSL ポリシーは、クライアント側の接続だけに影響します。
ステップ 6 <code>webvpn(config-webvpn-gateway)# ssl trustpoint trustpoint_label</code>	WebVPN ゲートウェイにトラストポイント設定を適用します。モジュールに組み込まれたテスト証明書をインポートできます。 付録 B' 組み込まれたテスト証明書のインポート を参照してください。  (注) トラストポイントは、認証局サーバ、鍵のパラメータと鍵生成方式、および WebVPN ゲートウェイの証明書登録方式を定義します。トラストポイントの設定の詳細は、「 トラストポイントの宣言 」(p.3-32)を参照してください。
ステップ 7 <code>webvpn(config-webvpn-gateway)# hostname name</code>	(任意) URL およびクッキー マングリング プロセスに使用するホスト名を指定します。ロードバランシング設定の場合、指定したホスト名が、ロードバランシング装置に設定された仮想ゲートウェイの IP アドレスになります。
ステップ 8 <code>webvpn(config-webvpn-gateway)# inservice</code>	ゲートウェイをサービス状態にします。

1. ワイルドカード プロキシ サービスを指定するマスクアドレスを設定します。ワイルドカード プロキシ サービスを設定するには、`secondary` キーワードを入力する必要があります。
2. `secondary` キーワードを入力すると、WebVPN サービス モジュール は、仮想 IP アドレスの ARP リクエストに応答しません。
3. `secondary` キーワードを入力できるのは、WebVPN サービス モジュール がスタンドアロン構成の場合、またはディスパッチ モード (MAC アドレス書き換え) に設定されたロード バランサ (CSM など) 上の実サーバとして WebVPN サービス モジュール を使用する場合です。
4. `secondary` キーワードは、同じ仮想 IP アドレスを使用して複数の装置を設定する場合に使用できます。仮想 IP アドレスは任意の有効な IP アドレスで、WebVPN サービス モジュール に接続された VLAN (サブネット) 上のアドレスである必要はありません。
5. パラメータを指定しないでポリシーを作成すると、デフォルト値を使用するポリシーが作成されます。

エンドユーザ認証の設定

RADIUS 設定の詳細については、『Cisco IOS Security Configuration Guide, Release 12.2』の「Configuring RADIUS」の章を参照してください。URL は次のとおりです。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fsecur_c/fsecsp/scfrad.htm

表 3-1 に、WebVPN RADIUS の AV のペアを示します。



(注) WebVPN アトリビュート (標準 IETF RADIUS アトリビュートを除く) はいずれも次のように、`webvpn:` で始まります。

```
webvpn:urllist-name=cisco
webvpn:nbnslist-name=cifs
webvpn:default-domain=cisco.com
```

表 3-1 WebVPN RADIUS AV ペア

アトリビュート	値のタイプ	値	デフォルト
addr (Framed-IP-Address ¹)	IP アドレス	<i>IP_address</i>	
addr-pool	文字列	<i>name</i>	
banner	文字列		
citrix-enabled	整数	0 (ディセーブル) 1 (イネーブル) ²	0
default-domain	文字列		
dns-servers	IP アドレス	<i>IP_address</i>	
dpd-client-timeout	整数 (秒数)	0 (ディセーブル) ~ 3600	300
dpd-gateway-timeout	整数 (秒数)	0 (ディセーブル) ~ 3600	300
file-access	整数	0 (ディセーブル) 1 (イネーブル) ²	0
file-browse	整数	0 (ディセーブル) 1 (イネーブル) ²	0
file-entry	整数	0 (ディセーブル) 1 (イネーブル) ²	0
hide-urlbar	整数	0 (ディセーブル) 1 (イネーブル) ²	0
home-page	文字列		
idletime (Idle-Timeout ¹)	整数 (秒数)	0 ~ 3600	2100
ie-proxy-exception	文字列	<i>DNS_name</i>	
	IP アドレス	<i>IP_address</i>	
ie-proxy-server	IP アドレス	<i>IP_address</i>	
inacl	整数	1 ~ 199、1300 ~ 2699	
	文字列	<i>name</i>	
keep-svc-installed	整数	0 (ディセーブル) 1 (イネーブル) ²	1
nbnslist-name	文字列	<i>name</i>	

表 3-1 WebVPN RADIUS AV ペア (続き)

アトリビュート	値のタイプ	値	デフォルト
netmask (Framed-IP-Netmask ¹)	IP アドレス	<i>IP_address_mask</i>	
port-forward-name	文字列	<i>name</i>	
primary-dns	IP アドレス	<i>IP_address</i>	
rekey-interval	整数 (秒数)	0 ~ 43200	21600
secondary-dns	IP アドレス	<i>IP_address</i>	
split-dns	文字列		
split-exclude ³	IP アドレス IP アドレス	<i>IP_address IP_address_mask</i>	
	ワード	local-lans	
split-include ³	IP アドレス IP アドレス	<i>IP_address IP_address_mask</i>	
svc-enabled ⁴	整数	0 (デイセーブル) 1 (イネーブル) ²	0
svc-ie-proxy-policy	ワード	none、 auto、 bypass-local	
svc-required ⁴	整数	0 (デイセーブル) 1 (イネーブル) ²	0
timeout (Session-Timeout ¹)	整数 (秒数)	1 ~ 1209600	43200
urllist-name	文字列	<i>name</i>	
user-vpn-group	文字列	<i>name</i>	
wins-server-primary	IP アドレス	<i>IP_address</i>	
wins-servers	IP アドレス	<i>IP_address</i>	
wins-server-secondary	IP アドレス	<i>IP_address</i>	

1. 標準 IETF RADIUS アトリビュートです。
2. この機能をイネーブルにするには、0以外の任意の整数を指定します。
3. split-include または split-exclude のどちらかを指定できます。両方の指定はできません。
4. svc-enable または svc-required のどちらかを指定できます。両方の指定はできません。

仮想コンテキストの設定

仮想コンテキストは、`webvpn context` コマンドを使用して定義します。仮想コンテキストは、設定済みのアドレス解決、ゲートウェイ、および認証設定をリンクします。

クライアントレス モードを設定するには、URL リストおよびグループ ポリシーを設定します。Outlook Web Access (OWA) を使用して E メールにアクセスするには、Microsoft Exchange サーバを宛先とする URL リストを設定します (`http://ipaddr/exchange` など)。

シンクライアント モードを設定するには、転送するポートのリストおよびグループ ポリシーを設定します。

Common Internet File System (CIFS) を使用したファイル共有を設定するには、NetBIOS Name Service (NBNS) リスト、サーバのアドレス、およびグループ ポリシーを設定します。

仮想コンテキストを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config)# webvpn context [context-name]</code>	WebVPN コンテキスト サブコマンド モードを開始します。WebVPN インスタンスを指定するには、オプションの VPN サービス名 <i>name</i> を使用します。
ステップ 2	<code>webvpn(config-webvpn-context)# gateway gateway-name {virtual-host virtual-host-name domain-name domain-name}</code>	セキュア ゲートウェイに設定した対応する仮想ゲートウェイ インスタンス、およびマッピング方式 (IP アドレス、URL、ドメイン名など) を指定します。 <i>gateway-name</i> パラメータは、システムに設定されている仮想ゲートウェイの 1 つと一致している必要があります。 <i>domain-name</i> パラメータは、仮想 WebVPN インスタンスの企業用ドメイン名 (<code>cisco.com</code> など) の指定に使用する ASCII 文字列です。
ステップ 3	<code>webvpn(config-webvpn-context)# csd enable</code>	Cisco Secure Desktop (CSD) Manager を使用してセキュアデスクトップを設定するために、CSD をイネーブルにします。  (注) WebVPN モジュール用の CSD のインストールおよび設定の手順は、「 CSD の設定 」(p.3-10) を参照してください。
ステップ 4	<code>webvpn(config-webvpn-context)# nat-address start-address end-address netmask netmask</code>	サーバ接続をオープンするとき使用する NAT アドレスを指定します。 <code>nat-address</code> コマンドで指定するアドレスは、WebVPN サブインターフェイス上に設定したサブネットの 1 つと一致している必要があります。  (注) このコマンドは、クライアントレス モードおよびシンクライアント モードで必要です。
ステップ 5	<code>webvpn(config-webvpn-context)# url-list listname</code>	ポータル Web ページに表示する URL リストを設定するために、 <code>url</code> サブモードを開始します。URL エントリの設定の詳細は、「 クライアントレス モードの設定 」(p.3-11) を参照してください。
ステップ 6	<code>webvpn(config-webvpn-context)# port-forward listname</code>	エンド ユーザがアクセスできるポートのリストを設定するために、 <code>port-fwd</code> サブモードを開始します。ポート転送の設定の詳細は、「 シンクライアント モードの設定 」(p.3-15) を参照してください。

	コマンド	目的
ステップ 7	<code>webvpn(config-webvpn-context)# policy group default-policy-name</code>	グループポリシーを設定するために、グループ サブモードを開始します。グループポリシーの設定の詳細は、「 グループポリシーの設定 」(p.3-22)を参照してください。グループポリシーを使用したトンネルモードの設定の詳細は、「 トンネルモードの設定 」(p.3-18)を参照してください。
ステップ 8	<code>webvpn(config-webvpn-context)# policy ssl policy-name</code>	(任意)SSL プロトコルが使用する SSL ポリシーを指定します。SSL ポリシーは、サーバ側の接続だけに影響します。
ステップ 9	<code>webvpn(config-webvpn-context)# policy tcp policy-name</code>	(任意)TCP プロトコルが使用する TCP ポリシーを指定します。TCP ポリシーは、サーバ側の接続だけに影響します。
ステップ 10	<code>webvpn(config-webvpn-context)# title string</code>	ブラウザのタイトルおよびタイトル バーに表示する HTML タイトル文字列を指定します。 <i>string</i> の長さは、最大 255 文字です。デフォルトの <i>string</i> は、「WebVPN Service」です。
ステップ 11	<code>webvpn(config-webvpn-context)# login-message string</code>	エンド ユーザにログインを要求するテキストを指定します。 <i>string</i> の長さは、最大 255 文字です。デフォルトの <i>string</i> は、「Please enter your username and password.」です。
ステップ 12	<code>webvpn(config-webvpn-context)# logout-message string</code>	エンド ユーザにログアウトを要求するテキストを指定します。 <i>string</i> の長さは、最大 255 文字です。デフォルトの <i>string</i> は、「Goodbye.」です。
ステップ 13	<code>webvpn(config-webvpn-context)# logo [file filename none]</code>	ログインおよびポータル ページに表示するカスタム ロゴイメージを指定します。 <i>filename</i> は、管理者がセキュリティゲートウェイにアップロードしたファイルです。
ステップ 14	<code>webvpn(config-webvpn-context)# title-color color</code>	ログイン、ホーム、ファイルアクセスのポータル ページ上のタイトル バーのカラーを指定します。デフォルトのカラーは、パープルです。有効なカラー値については、 付録 D「カラー名および RGB カラー値」 を参照してください。
ステップ 15	<code>webvpn(config-webvpn-context)# secondary-color color</code>	ログイン、ホーム、ファイルアクセスのポータル ページ上のセカンダリ タイトル バーのカラーを指定します。デフォルトのカラーは、パープルです。有効なカラー値については、 付録 D「カラー名および RGB カラー値」 を参照してください。
ステップ 16	<code>webvpn(config-webvpn-context)# text-color [black white]</code>	ポータル ページ上のタイトル バーのテキストのカラーを指定します。デフォルト値は、white です。
ステップ 17	<code>webvpn(config-webvpn-context)# secondary-text-color [black white]</code>	ポータル ページ上のセカンダリ バーのテキストのカラーを指定します。デフォルト値は、black です。
ステップ 18	<code>webvpn(config-webvpn-context)# username-prompt prompt</code>	WebVPN ログイン ユーザ名プロンプトの初期値を設定します。 <i>prompt</i> の最大長は、16 文字です。デフォルトの <i>prompt</i> は、「Login:」です。
ステップ 19	<code>webvpn(config-webvpn-context)# password-prompt prompt</code>	WebVPN ログイン パスワード プロンプトの初期値を設定します。 <i>prompt</i> の最大長は、16 文字です。デフォルトの <i>prompt</i> は、「Password:」です。
ステップ 20	<code>webvpn(config-webvpn-context)# aaa authentication [domain domain-name] [list list-name]</code>	認証パラメータを設定します。認証に使用するドメインまたは認証リストのどちらかを指定します。
ステップ 21	<code>webvpn(config-webvpn-context)# default-group-policy policy</code>	仮想 WebVPN コンテキスト インスタンスが使用するデフォルトのグループポリシーを指定します。グループポリシーの詳細は、「 グループポリシーの設定 」(p.3-22)を参照してください。

■ 仮想コンテキストの設定

	コマンド	目的
ステップ 22	<code>webvpn (config-webvpn-context) # vrf-name vrf-name</code>	仮想 WebVPN コンテキスト用に設定した VRF ドメインを指定します。
ステップ 23	<code>webvpn (config-webvpn-context) # max-users number</code>	特定の仮想 WebVPN コンテキストについて、オープンできるクライアント接続の最大数を指定します (VRF ドメイン単位)。
ステップ 24	<code>webvpn (config-webvpn-context) # nbns-list name</code>	NBNS リスト名を作成し、nbnslist サブモードを開始します。ファイル共有の設定の詳細は、「 CIFS を使用したファイル共有の設定 」(p.3-13)を参照してください。
ステップ 25	<code>webvpn (config-webvpn-context) # ssl authenticate verify {all none}</code>	ピアの証明書を検証する動作を設定します。この動作は、WebVPN サービス モジュール が HTTPS サーバに接続を試みたときに、SSL サーバの証明書に適用されます。 <ul style="list-style-type: none"> • all シグニチャの真正性、および関連トラストポイント設定に基づく取り消しステータスを検証します。これがデフォルト設定です。 • none 有効期限が切れていないすべての証明書を受け入れます。
ステップ 26	<code>webvpn (config-webvpn-context) # charset-encoding {shift-jis iso-8859-1}</code>	(任意) WebVPN ゲートウェイでの日本語シフト JIS コード化サポートをイネーブルにします。デフォルトの値は、iso-8859-1 です。
ステップ 27	<code>webvpn (config-webvpn-context) # inservice</code>	コンテキストをサービス状態にします。

CSD の設定

Cisco Secure Desktop (CSD) は、クライアントシステム上にセッションの動作および削除のための単一の安全なロケーションを提供することにより、重要データのすべての追跡を、一貫した信頼性のある手段で削除する方法を提供します。CSD により、リモートユーザがログアウトするか、SSL VPN セッションがタイムアウトになった場合、システム上からクッキー、ブラウザ履歴、一時ファイル、およびダウンロードしたコンテンツが確実に除去されます。CSD は、SSL VPN セッションに関する、または SSL VPN セッション中にダウンロードされた全データおよびファイルを暗号化することにより、データ盗難およびクライアントシステム上のマルウェア (悪意のあるソフトウェア) に対する保護を強化します。

CSD Manager では、次のセキュリティ コンポーネントを構築して管理し、エンド ユーザに配備できます。

- **ロケーション** Microsoft Windows ユーザは、このサイト タイプから企業ネットワークに接続します。ロケーションの設定は、Microsoft Windows ユーザだけに適用されます。CSD の設定およびオプションは、ユーザが接続を開始するロケーションのタイプによって異なります。たとえば、セキュア デスクトップおよび VPN フィーチャ ポリシー コンポーネントを使用するロケーション タイプを設定できます。

一般的なロケーション タイプには、職場、自宅、非セキュア (インターネット カフェなど) があります。Secure Desktop Manager を使用して、必要な数のロケーションを定義し、各ロケーションに異なる設定およびオプションを適用して、セキュリティ プロファイルを構成できます。Windows ロケーションにより、ロケーション単位でセキュア デスクトップ機能を配備できます。

- **セキュア デスクトップ** Windows 2000 および Windows XP のユーザに暗号化スペースを提供し、ユーザはこのスペース内でブラウザを使用してオンライン セッションを実行できます。セキュア デスクトップは、トランスペアレントで完全にセキュアですが、アクセスに必要なのはブラウザだけです。権限は、各ユーザがネットワークにアクセスするロケーションによって異なります。

- VPN フィーチャ ポリシー Web ブラウジング、ファイル アクセス、ポート転送、または SSL VPN クライアント (フル トンネリング) を許可する前に、システム検出チェックを提供します。フィーチャ ポリシーでは、アンチウイルス ソフトウェア、ファイアウォール ソフトウェア、オペレーティング システムのバージョン、または他の CSD コンポーネントなどの特定の保護対策を要求し、検証できます。
- キャッシュ クリーナ キャッシュされたファイル、設定の変更、キャッシュされたブラウザ情報、入力したパスワード、自動完了情報など、ユーザがブラウザでダウンロード、挿入、または作成したすべてのデータを無効にし、消去します。

ここでは、CSD をインストールし、セキュア デスクトップを設定するために必要な手順の概要について説明します。CSD 設定の詳細については、CSD のマニュアルを参照してください。URL は次のとおりです。

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csd/csd31/index.htm>

CSD をインストールし、セキュア デスクトップを設定するには、次の作業を行います。

-
- ステップ 1** CSD パッケージをインストールします。インストールの手順は、「[CSD パッケージ](#)」(p.C-8) を参照してください。
- ステップ 2** ゲートウェイを設定します。設定の手順は、「[仮想ゲートウェイの設定](#)」(p.3-5)を参照してください。
- ステップ 3** コンテキストを設定します。設定の手順は、「[仮想コンテキストの設定](#)」(p.3-8)を参照してください。
- ステップ 4** コンテキスト サブモードで、`csd enable` コマンドを入力し、CSD をイネーブルにします。

```
webvpn(config-webvpn-context)# csd enable
```

- ステップ 5** Web ブラウザから CSD Manager を起動し、コンテキストのセキュア デスクトップを設定します。

CSD 設定の詳細については、次の URL にある CSD のマニュアルを参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csd/csd31/index.htm>

- ステップ 6** コンテキスト サブモードで `inservice` コマンドを入力し、コンテキストをサービス状態にします。

```
webvpn(config-webvpn-context)# inservice
```

コンテキストをサービス状態にすると、エンド ユーザは各自の PC に CSD をダウンロードしてインストールできるようになります。

クライアントレス モードの設定

クライアントレス モードでは、すべての URL がホットリンクとして表示されるエンド ユーザ ポータル ページを設定します。WebVPN エンド ユーザに表示される HTML インターフェイスは、設定する値によって異なります。エンド ユーザには、イネーブルにした機能だけを含むカスタム ホーム ページ (ポータル ページ) が表示されます。

設定するサーバのタイプには、次のリソースを提供する Web サーバが含まれます。

- 内部 Web サイト
- OWA 用の E メール サーバ

- Citrix サーバへのリンク



(注) グループポリシーで Citrix をイネーブルにした場合、URL リストに Citrix サーバへのリンクを追加できます。また、エンドユーザに Citrix サーバの URL を任意で提供できます。エンドユーザは、フローティングツールバーの URL フィールドに、この URL を入力できます。Citrix サービスのイネーブル化の詳細は、「[グループポリシーの設定](#)」(p.3-22)を参照してください。

グループのメンバーではないエンドユーザのポータルページには、設定したすべてのサーバが表示されます。サーバまたは URL を設定していない場合、ポータルページにはサーバまたは URL は表示されませんが、エンドユーザは、ツールバーに URL を入力することによってサーバにアクセスできます。

URL リストを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config-webvpn-context)# url-list listname</code>	URL リストの名前を指定して、url サブモードを開始します。
ステップ 2	<code>webvpn(config-webvpn-url)# heading text</code>	URL グループのヘッダーテキストを指定します。ヘッダーにスペースを含める場合には、 <i>text</i> を引用符で囲みます。 1 つのリスト名に指定できるヘッダーは 1 つだけです。
ステップ 3	<code>webvpn(config-webvpn-url)# url-text text url-value url</code>	エンドユーザのホームページに表示するリンクのテキストを指定します。 <i>text</i> は、指定したリスト名のなかで固有の値でなければなりません。テキストにスペースを含める場合には、 <i>text</i> を引用符で囲みます。 <i>url</i> パラメータに、リンクの URL を指定します。Web ベースの E メールに OWA を使用する場合には、URL に /exchange を付加します(このキーワードは、Exchange サーバへの認証を必要とします)。 特定のリスト名に、複数の URL を指定できます。
ステップ 4	<code>webvpn(config-webvpn-url)# exit</code>	url サブモードを終了し、WebVPN コンテキスト サブモードに戻ります。

`no` を指定すると、コンフィギュレーションから対応する行が削除されます。URL を含める必要はありません。`no url-list listname` を指定すると、コンフィギュレーションから指定したリストが削除されます。

次に、URL のリストを設定する例を示します。

```
webvpn(config-webvpn-context)# url-list cisco
webvpn(config-webvpn-url)# url-text cisco url-value http://cisco.com
webvpn(config-webvpn-url)# url-text CNN url-value http://cnn.com
webvpn(config-webvpn-url)# url-text yahoo url-value http://yahoo.com
webvpn(config-webvpn-url)# url-text payroll url-value http://10.1.2.215/payroll
webvpn(config-webvpn-url)# url-text finance url-value https://finance.cisco.com
webvpn(config-webvpn-url)# url-text "OWA server" url-value
http://mail.cisco.com/exchange
webvpn(config-webvpn-url)# url-text "CitrixFarm" url-value
http://10.1.2.10/Citrix/MetaFrame/default/default.aspx
webvpn(config-webvpn-url)# exit
webvpn(config-webvpn-context)#
```

CIFS を使用したファイル共有の設定

ここでは、WebVPN サービス モジュールが NetBIOS 名を IP アドレスにマッピングする際に問い合わせを行う NetBIOS Name Service (NBNS) サーバの設定方法について説明します。



WebVPN では、リモート システム上のファイルにアクセスする、またはファイルを共有するために NetBIOS を必要とします。Windows コンピュータの名前を使用して、Windows コンピュータへのファイル共有接続を試みた場合、指定したファイル サーバは、ネットワーク上のリソースを識別する特定の NetBIOS 名に対応します。

NBNS を使用するには、最低 1 つの NetBIOS サーバ (ホスト) を設定する必要があります。冗長構成用に最大 3 つの NBNS サーバを設定できます。アクティブ サーバに障害が発生すると、リスト上の最初の使用可能サーバがバックアップとして動作します。

ファイル共有用の NBNS サーバを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config-webvpn-context)# nbns-list name</code>	NBNS リスト名を作成し、nbmslist サブモードを開始します。
ステップ 2	<code>webvpn(config-webvpn-nbnslist)# nbns-server ip_addr [master] [timeout timeout] [retry retries]</code>	<p>NBNS リストおよび CIFS 名前解決用のサーバのアドレスを指定します。最大 3 つのサーバを設定できます。</p> <p> (注) この機能がサポートされるのは、Windows 2000 および Linux 上で実行される Samba サーバだけです。</p> <p><i>ip_addrs</i> に、Windows ネットワーク上の Primary Domain Controller (PDC) を指定します。</p> <p>master キーワードは、マスタ ブラウザであることを示します。Windows Internet Naming Service (WINS) サーバの場合には、master キーワードを入力しないでください。</p> <p><i>timeout</i> 値には、次のサーバにクエリを送信する前に、NBNS クエリに対する応答を待機する期間の初期値を秒数で指定します。デフォルトの <i>timeout</i> 値は 2 秒で、有効範囲は 1 ~ 30 秒です。</p> <p><i>retries</i> 値には、設定されているサーバに順番に NBNS クエリの送信を再試行する回数を指定します。リストの全サーバに対してここで指定した回数だけ送信を再試行したあと、エラーが戻されます。デフォルトの <i>retries</i> 値は 2 で、有効範囲は 0 ~ 10 です。</p>
ステップ 3	<code>webvpn(config-webvpn-nbnslist)# exit</code>	コンテキスト サブモードに戻ります。
ステップ 4	<code>webvpn(config-webvpn-context)# policy group policy-name</code>	グループ ポリシーの名前を指定し、グループ サブコマンド モードを開始します。グループ ポリシーの設定の詳細は、「 グループ ポリシーの設定 」(p.3-22)を参照してください。
ステップ 5	<code>webvpn(config-webvpn-group)# nbns-list name</code>	<p>定義済みの NBNS リストを指定します。</p> <p> (注) Windows 2000 サーバおよび Linux/UNIX 上でサポートされます。</p>

■ 仮想コンテキストの設定

	コマンド	目的
ステップ 6	webvpn (config-webvpn-group) # functions { file-access file-browse file-entry }	<p>次の機能を指定します。</p> <p>file-access ホームページにリストされているファイルサーバへの、エンド ユーザによるアクセスをイネーブルにします。このキーワードは、デフォルトではディセーブルです。file-access をディセーブルにすると、file-browse および file-entry の設定は削除されます。</p> <p>file-browse エンド ユーザによるファイルサーバのブラウズをイネーブルにします。このキーワードは、デフォルトではディセーブルです。</p> <p> (注) file-browse をイネーブルにするには、file-access がイネーブルである必要があります。</p> <p>file-entry エンド ユーザによるファイルサーバまたはファイル共有への直接入力をイネーブルにします。このキーワードは、デフォルトではディセーブルです。</p> <p> (注) file-entry をイネーブルにするには、file-access がイネーブルである必要があります。</p>
ステップ 7	webvpn (config-webvpn-group) # exit	コンテキスト サブモードに戻ります。
ステップ 8	webvpn (config-webvpn-context) # default-group-policy name	デフォルトのグループ ポリシーを指定します。
ステップ 9	webvpn (config-webvpn-context) # gateway <i>gateway-name domain-name domain-name</i> }	セキュア ゲートウェイに設定した対応する仮想ゲートウェイ インスタンスおよびマッピング方式を指定します。 <i>gateway-name</i> パラメータは、システムに設定されている仮想ゲートウェイの 1 つと一致している必要があります。 <i>domain-name</i> パラメータは、仮想 WebVPN インスタンスの企業用ドメイン名 (cisco.com など) の指定に使用する ASCII 文字列です。
ステップ 10	webvpn (config-webvpn-context) # inervice	コンテキストをサービス状態にします。

次に、ファイル共有用のコンテキストを設定する例を示します。

```
webvpn (config) # webvpn context c1
webvpn (config-webvpn-context) # nbns-list list2
webvpn (config-webvpn-nbnslist) # nbns-server 10.1.1.2
webvpn (config-webvpn-nbnslist) # exit
webvpn (config-webvpn-context) # policy group p1
webvpn (config-webvpn-group) # nbns-list "list2"
webvpn (config-webvpn-group) # functions file-access
webvpn (config-webvpn-group) # functions file-browse
webvpn (config-webvpn-group) # functions file-entry
webvpn (config-webvpn-group) # exit
webvpn (config-webvpn-context) # default-group-policy p1
webvpn (config-webvpn-context) # gateway g1 domain example.com
webvpn (config-webvpn-context) # inervice
```


シンクライアント モードの設定

TCP ポート転送とも呼ばれるシンクライアント モードは、リモート エンド ユーザに対して、既知の固定 TCP ポート上で通信しているクライアントおよびサーバ アプリケーションへのアクセスを提供します。リモート エンド ユーザは、各自のローカル PC にインストールしたクライアント アプリケーションを使用し、これらのアプリケーションをサポートするリモート サーバにセキュアにアクセスできます。

シスコでは、次のアプリケーションをテスト済みです。

- E メール SMTP、POP3、IMAP4
- Virtual Network Computing (VNC)
- Windows Terminal Services
- Telnet
- SSH
- Perforce
- XDDTS
- Sametime Instant Messaging

その他の TCP ベース アプリケーションも動作する可能性はありますが、シスコではテストを実施していません。

シンクライアント モードを使用するには、Sun Microsystems Java Runtime Environment をインストールし、エンド ユーザの PC にアプリケーションを設定する必要があります。いずれも、管理者の許可が必要です。エンド ユーザが、インターネット キオスクまたはインターネット カフェなどの公共リモート システムから接続してアプリケーションを使用できるようになることは、ほとんど考えられません。



(注)

エンド ユーザがデジタル証明書を使用して認証した場合、Java アプレットは動作しません。Java は Web ブラウザのキーストアにアクセスできないので、Java では、ブラウザがエンド ユーザ認証に使用した証明書を使用できず、アプリケーションを起動できません。エンド ユーザがアプリケーションにアクセスできるようにするには、WebVPN エンド ユーザの認証にデジタル証明書を使用しないでください。

アプリケーションの起動時に、WebVPN サービス モジュール がエンド ユーザの PC 上のホスト ファイルに追加するマッピング情報を提供します。このマッピング情報により、必要なアプリケーションをサポートしている中央サイトのサーバに、PC を接続できます。

ポート転送を実行できるのは、リモート サーバ上のアプリケーションを一意に識別でき、ホスト名または IP アドレスとポートのいずれかでアクセスできる場合だけです。できれば、ホスト名を使用することを推奨します。使用方法については、「[ホスト名と IP アドレスの使用方法](#)」(p.3-18)を参照してください。

ポート転送のエントリは、port-fwd サブモードで設定します。指定した *listname* に、複数のエントリを指定できます。*listname* により、ユーザ名またはグループ ポリシーに適用するリストとして、ポート転送エントリをグループ化できます。

ポート転送設定を指定してシンクライアント モードを設定するには、次の作業を行います。

■ 仮想コンテキストの設定

	コマンド	目的
ステップ 1	<code>webvpn(config-webvpn-context)# port-forward listname</code>	転送先ポート リストの名前を指定し、WebVPN port-fwd サブモードを開始します。listname の最大長は、63 文字です。
ステップ 2	<code>webvpn(config-webvpn-port-fwd)# local localport remote-server remoteserver remote-port remoteport description description</code>	<p>WebVPN エンド ユーザに、TCP ベース アプリケーションへのグローバル アクセスを指定します。</p> <p>エンド ユーザの PC 用に、次のように、アプリケーションのローカル TCP ポートを設定します。</p> <ul style="list-style-type: none"> localport パラメータに、待ち受けるローカル ポートを指定します。localport 値は、特定のリスト名について 1 回だけ使用できます。 エンド ユーザのワークステーションで実行している既存サービスとの競合を避けるために、ポートは 1024 ~ 65535 の範囲で設定します。使用方法については、「ローカルポートのガイドライン」(p.3-16)を参照してください。 <p>エンド ユーザがアクセスする必要があるサーバ用に、次のように、リモートサーバおよびリモート TCP ポートを設定します。</p> <ul style="list-style-type: none"> remoteserver パラメータに、リモートサーバに接続するためのホスト名または IP アドレスを指定します。使用方法については、「ホスト名と IP アドレスの使用法」(p.3-18)を参照してください。 remoteport パラメータに、リモートサーバに接続するためのポートを指定します。 <p>description パラメータにより、エンドユーザのアプレットウィンドウに、アプリケーション名または短い説明を表示できます。</p>
ステップ 3	<code>webvpn(config-webvpn-port-fwd)# exit</code>	WebVPN port-fwd サブモードを終了し、WebVPN コンテキストサブモードに戻ります。

次に、ポート転送を設定する例を示します。

```
webvpn(config-webvpn-context)# port-forward abc
webvpn(config-webvpn-port-fwd)# local-port 25 remote-server "mailman" remote-port 25
description "SMTP server"
webvpn(config-webvpn-port-fwd)# local-port 110 remote-server "pop3-ny" remote-port 110
description "POP3-server"
webvpn(config-webvpn-port-fwd)# local-port 143 remote-server "imap-ny" remote-port 143
description "IMAP server"
webvpn(config-webvpn-port-fwd)# exit
webvpn(config-webvpn-context)#
```

ローカルポートのガイドライン

Windows 2000 または XP 上のエンド ユーザシステムでポート転送モードを開始するために Java アプレットをダウンロードすると、(C:\WINNT\system32\drivers\etc\hosts にある) ホスト ファイルが、hosts.webvpn としてバックアップされます。さらに、Java アプレットにより、エンド ユーザに割り当てるポート転送リストに設定した各ポート転送エントリについて、ホスト ファイルにマッピングが追加されます。

たとえば、次のコンフィギュレーションの場合：

```
port-forward "cisco"  
  local-port 25 remote-server "mailman" remote-port 25 description "smtp"  
  local-port 23 remote-server "pc46" remote-port 23 description "telnet"  
  local-port 110 remote-server "sjcd-2" remote-port 110 description "pop3"
```

Java アプレットは、クライアントのホスト ファイルで、「mailman」を 127.0.0.2 に、「pc46」を 127.0.0.3 に、「sjcd-2」を 127.0.0.4 にマッピングします。さらに、Java アプレットは、エンド ユーザの PC 上でリモート ポート 127.0.0.2:25、127.0.0.3:23、および 127.0.0.4:110 を待ち受けます。

マッピングが実行され、Java アプレットが必要なポート上で待ち受けるので、クライアントのアプリケーションを変更する必要はありません。たとえば、クライアントはホスト pc46 への Telnet 接続を作成できますが (telnet pc46)、Telnet 接続は実際には Java アプレットを経由するので、セキュアです。

上記のコンフィギュレーションは、ポート 23、25、および 110 でローカル サーバが実行されていないことを前提としています。アプレットをダウンロードする前に、エンド ユーザの PC がいずれかのポート上でアプリケーションを実行している場合 (たとえば、クライアント PC 上でポート 23 で待ち受ける Telnet サーバを実行している場合) には、アプレットは 127.0.0.1:local-port 上での実行を試みます。この場合、2 つの状況が考えられます。

- local-port が remote-port と同じである場合、Java アプレットは、次の例のように、local-port 127.0.0.1:23 で待ち受けます。

```
local-port 23 remote-server "pc46" remote-port 23 description "telnet"
```

ユーザは、ポート転送エントリを使用できないので、ポート転送は失敗します。

- local-port が remote-port と異なる場合、Java アプレットは、次の例のように、127.0.0.1:1230 で待ち受けます。

```
local-port 1230 remote-server "pc46" remote-port 23 description "telnet"
```

クライアント PC のポート 1230 ではアプリケーションが実行されていないので、ポート転送は成功します。この場合、エンド ユーザは、ホスト pc46 への Telnet 接続をオープンする場合、telnet 127.0.0.1 1230 を入力する必要があります。Java アプレットがローカル ポートで待ち受ける場合には、常に、127.0.0.1:local-port で通信するように、クライアントのアプリケーションを変更する必要があります。

次のように、ポート転送エントリに、ホスト名ではなくリモート サーバの IP アドレスを設定した場合にも、Java アプレットは 127.0.0.1:local-port で待ち受けます。

```
local-port 1230 remote-server 19.0.0.1 remote-port 23 description "telnet"
```

このコンフィギュレーションでは、Java アプレットは 127.0.0.1:1230 で待ち受けます。エンド ユーザは、19.0.0.1 への Telnet 接続をオープンする場合、telnet 127.0.0.1:1230 を入力する必要があります。

使用方法については、「[ホスト名と IP アドレスの使用法](#)」(p.3-18)を参照してください。



(注)

Linux 上で実行するエンド ユーザシステムの場合には、Java アプレットは常に、127.0.0.1:local-port で待ち受けます。したがって、127.0.0.1:local-port に接続するように、すべてのクライアント アプリケーションを変更する必要があります。ホスト ファイルでのマッピングは実行されません。

ホスト名と IP アドレスの使用方法

ホスト名を使用してリモート サーバを識別すると、Java アプレットはホスト ファイルを変更し、各アプリケーション サーバのエントリを作成します（オペレーティング システムが Windows で、PC 上に管理者権限がある場合）。たとえば、最初のポート転送リモート サーバにホスト名 *johndoe2ksrv* を設定した場合、Java アプレットは元のホスト ファイルのバックアップ コピーを作成し、ホスト ファイルを変更して、*johndoe2ksrv* をループバック IP アドレス 127.0.0.2 にマッピングする WebVPN エントリを追加します。2 番目のポート転送エントリが *NotesServer* であれば、Java アプレットは、*NotesServer* を 127.0.0.3 にマッピングするエントリをホスト ファイルに追加します。これらのエントリは、さらに、実リモート アプリケーション ポートに関連付けられます。Java アプレットが割り当てるループバック アドレスは固有なので、各エントリは固有です。

IP アドレスを使用してリモート サーバを識別する場合には、Java アプレットはホスト ファイルのバックアップまたは変更を実行しません。各サーバに、ループバック IP アドレス 127.0.0.1 およびローカル TCP ポートとして設定される TCP ポートを割り当てます。割り当てられる IP アドレスは常に 127.0.0.1 なので、アプリケーションを区別するには、各エントリに固有のローカル TCP ポートを設定する必要があります。

クライアントのアプリケーションが、サーバアドレスと通信するように設定します。ホスト名およびリモート TCP ポートを使用する場合、アプリケーション サーバのアドレス指定情報は、エンドユーザのロケーションに関係なく、同じになります。IP アドレスおよびローカル TCP ポートを使用する場合、アドレス指定情報は、エンドユーザのロケーションによって異なります。エンドユーザの PC のクライアント アプリケーションを再設定する必要があります。

トンネル モードの設定



(注) エンドユーザは、各自の PC に SSL VPN Client (SVC) をダウンロードしてインストールできるので、最初に、WebVPN サービス モジュール 上の内部フラッシュ デバイスに SVC パッケージをインストールする必要があります。SVC パッケージのインストールの詳細については、「[クライアント パッケージのインストール](#)」(p.C-6)を参照してください。




(注) トンネル モードは、グループ ポリシー コマンドを使用して設定します。グループ ポリシー コマンドの詳細については、「[グループ ポリシーの設定](#)」(p.3-22)を参照してください。

ここでは、IP ローカル アドレス プール、WebVPN コンテキスト、および WebVPN グループ ポリシーを指定して、トンネル モードを設定する手順について説明します。



トンネル モードでは、ゲートウェイによって、ゲートウェイにログインした各エンドユーザに SVC IP アドレスが提供されます。SVC IP アドレスを提供するローカル IP アドレス プールを設定するには、`ip local pool` コマンドを使用します。

トンネル モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config)# ip local pool pool-name start-range end-range</code>	各 SVC の IP アドレスを提供するために、WebVPN サービス モジュールが使用する IP アドレス プールを指定します。  (注) WebVPN サブインターフェイスの IP アドレスが、この IP アドレス プールと同じサブネットに存在している必要があります。WebVPN サブインターフェイスの設定の詳細は、「 WebVPN サービス モジュール上でのインターフェイスの設定 」(p.2-4)を参照してください。
ステップ 2	<code>webvpn(config)# webvpn context context-name</code>	コンフィギュレーションで使用する WebVPN コンテキストを指定します。
ステップ 3	<code>webvpn(config-webvpn-context)# policy group policy-name</code>	グループ ポリシーの名前を指定し、グループ サブコマンド モードを開始します。
ステップ 4	<code>webvpn(config-webvpn-group)# functions {svc-enabled svc-required}</code>	グループ ポリシーのトンネル モードをイネーブルにします。トンネル モードは、デフォルトではディセーブルです。 svc-enabled グループのユーザによるトンネル モードの使用をイネーブルにします。エンドユーザの PC に SVC をインストールできない場合、エンドユーザは引き続き、クライアントレス モードまたはシンクライアント モードを使用できます。 svc-required トンネル モードを必須にします。エンドユーザの PC に SVC をインストールできない場合、エンドユーザは他のモードを使用できません。
ステップ 5	<code>webvpn(config-webvpn-group)# svc dpd interval {client gateway} timeout</code>	ユーザまたはグループのトンネル モード WebVPN をイネーブルにした場合、ゲートウェイまたはクライアントの Dead Peer Detection (DPD) インターバル値を指定します。 timeout パラメータに、タイムアウトの値を秒数で指定します。DPD タイマーは、ピアに DPD パケットを送信する必要があるかどうかを判別します。DPD タイマーは、ピアから Cisco SSL Tunnel Protocol (CSTP) フレームを受信することによりリセットされます。ゲートウェイまたはクライアントが DPD 応答を受信しない場合、デフォルトでは、ゲートウェイおよびクライアントの設定はディセーブルになります。 クライアントおよびゲートウェイの DPD インターバルの有効値は、0 (ディセーブル) ~ 3600 秒です。
ステップ 6	<code>webvpn(config-webvpn-group)# svc address-pool name</code>	SVC IP アドレスを提供するローカル IP アドレス プールを設定します。
ステップ 7	<code>webvpn(config-webvpn-group)# svc dns-server {primary ip_addr secondary ip_addr}</code>	Web ブラウジング用のプライマリおよびセカンダリ DNS サーバを指定します。SVC をインストールすると、アクティブな Web ブラウザが非アクティブになり、新しいブラウザが起動します。ここで指定する DNS サーバ情報は、新しく起動するブラウザに適用されます。接続が終了すると、前の DNS 設定が再び適用されます。

■ 仮想コンテキストの設定

	コマンド	目的
ステップ 8	<code>webvpn(config-webvpn-group)# svc homepage url</code>	エンド ユーザのログイン時に表示される Web ページの URL を指定します。url に、URL のパスを指定します。URL の最大長は、255 文字です。この設定は、デフォルトではディセーブルです。
ステップ 9	<code>webvpn(config-webvpn-group)# svc wins-server {primary ip_addr secondary ip_addr}</code>	プライマリおよびセカンダリ WINS サーバを指定します。
ステップ 10	<code>webvpn(config-webvpn-group)# svc default-domain default-domain-name</code>	グループのデフォルトのドメインを指定します。
ステップ 11	<code>webvpn(config-webvpn-group)# svc keep-installed</code>	<p>接続終了後も、エンド ユーザのクライアント PC 上に SVC をインストールしておくように指定します。エンド ユーザの PC に SVC を継続的にインストールしておく、エンド ユーザは新しい接続を確立するときに、再び SVC をダウンロードする必要がありません。</p> <p>トンネルの終了後に VPN クライアントをアンインストールし、ダウンロードしたセットアップファイルを削除する場合には、このコマンドの <code>no</code> 形式を使用します。</p>
ステップ 12	<code>webvpn(config-webvpn-group)# svc rekey [time interval] [method {new-tunnel ssl}]</code>	<p>VPN クライアントが SSL トンネルのキーの再生成 (rekey) を行うタイミング、および WebVPN クライアントが使用するキーの再生成方式を指定します。キーの再生成は、デフォルトではディセーブルです。キーの再生成をイネーブルにした場合、デフォルトのキーの再生成方式は <code>ssl</code> です。</p> <p><code>time interval</code> の有効値は 0 ~ 43200 秒で、デフォルトは 21600 (6 時間) です。</p> <p><code>method new-tunnel</code> キーワードを指定すると、既存のトンネルが終了し、新しいトンネルがリクエストされます。</p> <p><code>method ssl</code> キーワードを指定すると、既存のトンネルを終了せずに、SVC により SSL セキュリティ パラメータがネゴシエートされます。</p>

コマンド	目的
ステップ 13 <code>webvpn(config-webvpn-group)# svc split [dns string]{[include ip-address netmask] [exclude ip-address netmask] local-lans}</code>	<p>すべてのトラフィックをプライベート ネットワークにトンネリングする (include) か、または外部 (非プライベート) ネットワーク宛てのトラフィックを外部 Web サイトに直接送信する (exclude) かを指定します。</p> <p> (注) include または exclude のどちらかのキーワードを指定します。両方のキーワードを指定することはできません。コマンドを複数回入力することにより、include または exclude キーワードのいずれかに、最大 200 のアドレスを指定できます。</p> <p>include キーワードの場合、トンネリングするトラフィックを指定します。その他のトラフィックはすべて、内部ネットワークにトンネリングされません。</p> <p>exclude キーワードの場合、内部ネットワークにトンネリングしないで外部 Web サイトに直接送信するトラフィックを指定します。その他のトラフィックはすべて、トンネリングされます。</p> <p>The exclude local-lans キーワードを指定すると、エンドユーザのローカル LAN が、トンネリング対象から除外されます。</p>
ステップ 14 <code>webvpn(config-webvpn-group)# svc msie-proxy [exception exception-string] [server {ip-address dns_name}: port] [option {none auto bypass-local}]</code>	<p>Microsoft Internet Explorer (MSIE) ブラウザのプロキシ設定を指定します。</p> <p> (注) このコマンドがサポートされるのは、MSIE ブラウザだけです。</p> <p>exception キーワードには、プロキシ経由で送信しないトラフィックの単一の DNS 名またはアドレスを指定します。このキーワードは、デフォルトではディセーブルです。</p> <p>server キーワードには、Socks を除くブラウザのプロキシ設定 (HTTP、Secure、FTP、Gopher) が使用する IP アドレスまたは DNS 名を指定し、任意でコロンとポート番号を指定します。このキーワードは、デフォルトではディセーブルです。</p> <p>ブラウザでプロキシを使用しない場合、option none キーワードを指定します。これがデフォルト設定です。</p> <p>ブラウザのプロキシ設定を自動検出する場合、option auto キーワードを指定します。</p> <p>ローカル アドレスをプロキシから迂回させる場合、option bypass-local キーワードを指定します。</p>
ステップ 15 <code>webvpn(config-webvpn-group)# filter tunnel {name acl_list}</code>	<p>グループ ポリシーで使用するネットワーク レベルのアクセス リスト名を定義します。</p>

ポリシーの設定

WebVPN ゲートウェイにポリシーを適用する手順については、「[仮想ゲートウェイの設定](#)」(p.3-5)を参照してください。

ここでは、次のポリシーの設定方法について説明します。

- [グループポリシーの設定](#) (p.3-22)
- [SSLポリシーの設定 \(任意\)](#) (p.3-23)
- [TCPポリシーの設定 \(任意\)](#) (p.3-25)

グループポリシーの設定






(注) トンネルモード設定に固有のグループポリシー コマンドは、「[トンネルモードの設定](#)」(p.3-18)を参照してください。



(注) 一部のグループポリシー コマンドは、特定のリモート アクセス モードに適用されます。特定のモードの情報は、各コマンドの注釈を参照してください。

各種のグループポリシー パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config-webvpn-context)# policy group policy-name</code>	グループポリシーの名前を指定し、グループサブコマンドモードを開始します。
ステップ 2	<code>webvpn(config-webvpn-group)# citrix enabled</code>	Citrix 機能をイネーブルにします。
ステップ 3	<code>webvpn(config-webvpn-group)# banner string</code>	ポータル ページのパナー スtringを指定します。 <i>string</i> 値には、7 ビット ASCII 値、HTML タグ、およびエスケープシーケンスを指定できます。エンド ユーザがログインすると、このStringが表示されます。
ステップ 4	<code>webvpn(config-webvpn-group) hide-url-bar</code>	ポータル ページ上の URL バーをディセーブルにします。 (注) このコマンドは、クライアントレス モードだけに適用されます。
ステップ 5	<code>webvpn(config-webvpn-group) timeout {idle time session time}</code>	ユーザまたはグループのエンド ユーザ アイドル タイムアウト値、およびセッションの最大タイムアウト値を指定します。 アイドル タイムアウトは、エンド ユーザの無動作によるタイムアウトです。アイドル タイムアウトの有効値は 0 (ディセーブル) ~ 3600 秒で、デフォルト値は 2100 秒 (35 分) です。 セッション タイムアウトは、無動作の時間に関係なく、セッションの合計時間によるタイムアウトです。セッション タイムアウトの有効値は 1 (ディセーブル) ~ 1209600 秒で、デフォルト値は 43200 秒 (12 時間) です。

	コマンド	目的
ステップ 6	<code>webvpn(config-webvpn-group)# nbns-list name</code>	<p>コンテキスト設定に定義した CIFS 用の NBNS リストを指定します。</p> <p>サポート対象は、Windows 2000 サーバおよび Linux/UNIX だけです。</p> <p> (注) このコマンドは、クライアントレス モードだけに適用されます。</p>
ステップ 7	<code>webvpn(config-webvpn-group)# url-list name</code>	<p>コンテキスト設定に定義した URL リストを指定します。コマンドを再入力すると、前の設定が上書きされます。デフォルトでは、指定されるリストはありません。</p> <p> (注) このコマンドは、クライアントレス モードだけに適用されます。</p>
ステップ 8	<code>webvpn(config-webvpn-group)# port-forward name</code>	<p>コンテキスト設定に定義したポート転送リストを指定します。コマンドを再入力すると、前の設定が上書きされます。デフォルトでは、指定されるリストはありません。</p> <p> (注) このコマンドは、シンクライアント モードだけに適用されます。</p>

SSL ポリシーの設定 (任意)

SSL ポリシー テンプレートを使用して、SSL スタックの関連パラメータを定義できます。

設定できるパラメータの 1 つは、SSL close-protocol 動作です。これにより、各 SSL ピアは、接続を正しく終了するために、close-notify アラートを送信し、close-notify アラートを受信する必要があります。SSL 接続が正しく終了されなかった場合、セッションは削除され、ピアは以降の SSL 接続に同じ SSL セッション ID を使用できなくなります。

ただし、SSL の実装状況を見ると、SSL close-protocol に厳密に従っていないものも多数あります (たとえば、SSL ピアは close-notify アラートを送信しますが、リモート SSL ピアからの close-notify アラートを待機せずに、接続を終了するような場合もあります)。

SSL ピアが接続終了シーケンスを開始すると、WebVPN サービス モジュール は close-notify アラート メッセージを監視します。SSL ピアが close-notify アラートを送信しない場合、WebVPN サービス モジュール は、以降の SSL 接続に同じセッション ID が使用されないように、そのセッションをセッション キャッシュから削除します。

WebVPN サービス モジュール が接続終了シーケンスを開始する場合には、次の close-protocol オプションを設定できます。


- **strict** WebVPN サービス モジュール は SSL ピアに close-notify アラート メッセージを送信し、さらに、WebVPN サービス モジュール は SSL ピアからの close-notify アラート メッセージの受信を待機します。WebVPN サービス モジュール が close-notify アラートを受信しない場合、そのセッションの SSL は再開できなくなります。
- **none** WebVPN サービス モジュール は SSL ピアに close-notify アラート メッセージを送信しません。また、WebVPN サービス モジュール は SSL ピアからの close-notify アラート メッセージを待機しません。WebVPN サービス モジュール は、以降の SSL 接続で、その SSL を再開できるように、セッション情報を保持します。




■ ポリシーの設定

- ディセーブル(デフォルト) WebVPN サービス モジュールは、SSL ピアに close-notify アラートメッセージを送信しますが、SSL ピアは close-notify アラートを待機せずにセッションを削除します。SSL ピアが close-notify アラートを送信するかどうかに関係なく、以降の SSL 接続でセッションを再開できるように、セッション情報が保持されます。

特定のプロキシ サーバに SSL ポリシーを関連付けない場合、プロキシ サーバは、デフォルトで、すべてのサポート対象の暗号スイートおよびプロトコルバージョンをイネーブルにします。

SSL ポリシーを定義するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config)# webvpn policy ssl ssl_policy_name</code>	SSL ポリシー テンプレートを定義します。
ステップ 2	<code>webvpn(config-ssl-policy)# cipher {rsa-with-rc4-128-md5 rsa-with-rc4-128-sha rsa-with-des-cbc-sha rsa-with-3des-ede-cbc-sha others...}</code>	プロキシ サーバが受け入れる暗号スイート名のリストを設定します。暗号スイート名の規則は、既存の SSL スタック名と同じです。
ステップ 3	<code>webvpn(config-ssl-policy)# tls-rollback [current any]</code>	ClientHello メッセージの SSL プロトコルのバージョン (SSL2.0、SSL3.0、TLS1.0) を指定します。TLS ロールバックは、デフォルトではディセーブルです。 current キーワードを指定すると、SSL プロトコルバージョンは、サポートされる最新バージョンまたはネゴシエートされたバージョンのどちらかになります。 any キーワードを指定すると、SSL プロトコルバージョンはチェックされません。  (注) デフォルトでは、WebVPN サービス モジュールは、サポートされる最新バージョンを使用します。このコマンドは、クライアントが (ClientHello メッセージに指定された)最新のサポートバージョンではなく、ネゴシエートされたバージョンを使用している場合に入力します。
ステップ 4	<code>webvpn(config-ssl-policy)# version {ssl3 tls1 all}</code>	プロキシ サーバがサポートする各種のプロトコルバージョンを定義します。
ステップ 5	<code>webvpn(config-ssl-policy)# timeout handshake time</code>	モジュールがハンドシェイク フェーズで接続を持続する時間を設定します。有効範囲は、0 ~ 65535 秒です。
ステップ 6	<code>webvpn(config-ssl-policy)# close-protocol {strict none}</code>	SSL close-protocol 動作を設定します。close-protocol は、デフォルトではディセーブルです。
ステップ 7	<code>webvpn(config-ssl-policy)# session-cache</code>	セッション キャッシング機能をイネーブルにします。セッション キャッシングは、デフォルトでイネーブルです。


	コマンド	目的
ステップ 8	<pre>webvpn(config-ssl-policy)# timeout session timeout [absolute¹]</pre>	<p>エントリをセッション キャッシュに保管しておく時間を設定します。有効範囲は、1 ~ 72000 秒です。</p> <p> (注) セッション キャッシュ サイズを設定するには、absolute キーワードが必要です。</p> <p> (注) absolute キーワードを指定すると、指定した <i>timeout</i> が経過するまで、セッション エントリがセッション キャッシュに保管されます。absolute キーワードを指定した場合、セッション キャッシュに空きエントリがない場合、新しい着信接続は拒否されます。</p>
ステップ 9	<pre>webvpn(config-ssl-policy)# session-cache size size</pre>	<p>(任意) セッション キャッシュのサイズを指定します。¹ 有効範囲は、1 ~ 262143 エントリです。</p> <p> (注) timeout session コマンドに absolute キーワードを入力した場合には、セッション キャッシュ サイズを指定してください。このコマンドを入力しない場合、または <i>size</i> を指定しない場合、セッション キャッシュ サイズは最大サイズ (262,144) になります。</p>

1. **absolute** キーワードを指定すると、設定したセッション タイムアウトが経過するまで、セッション エントリを再使用できません。**absolute** を設定する場合、必要なセッション エントリ数は、「新しい接続レート × **absolute** タイムアウト」の値になります。タイムアウトの設定値と新しい接続レートによっては、セッション エントリ数が莫大な数になることがあります。この場合、セッション キャッシュ サイズを設定することで、使用されるセッション エントリ数を制限できます。



TCP ポリシーの設定 (任意)

TCP ポリシー テンプレートをを使用して、TCP スタックの関連パラメータを定義できます。

TCP ポリシーを定義するには、次の作業を行います。

	コマンド	目的
ステップ 1	<pre>webvpn(config)# webvpn policy tcp tcp_policy_name</pre>	TCP ポリシー テンプレートを定義します。特に指定しない場合、すべてデフォルト設定になります。
ステップ 2	<pre>webvpn(config-tcp-policy)# mss max_segment_size</pre>	<p>接続により生成される SYN パケットの Maximum Segment Size (MSS; 最大セグメント サイズ) をバイト数で設定します。</p> <p> (注) このコマンドにより、プロキシ サーバのクライアント側とサーバ側に異なる MSS を設定できます。デフォルトは 1460 バイトです。有効範囲は、256 ~ 2460 バイトです。¹</p>
ステップ 3	<pre>webvpn(config-tcp-policy)# timeout syn time</pre>	接続確立のタイムアウトを設定します。デフォルトは 75 秒です。有効範囲は、5 ~ 75 秒です。

■ ポリシーの設定

	コマンド	目的
ステップ 4	<code>webvpn(config-tcp-policy)# timeout reassembly time</code>	再組み立てキューをクリアするまでの時間を、秒数で設定します。指定した時間内にトランザクションが完了しない場合、再組み立てキューはクリアされ、接続は廃棄されます。デフォルトは 60 秒です。有効範囲は、0 ~ 960 秒 (0 = ディセーブル) です。
ステップ 5	<code>webvpn(config-tcp-policy)# timeout inactivity time</code>	確立した接続を非アクティブにできる時間を、秒数で設定します。デフォルトは 600 秒です。有効範囲は、0 ~ 960 秒 (0 = ディセーブル) です。
ステップ 6	<code>webvpn(config-tcp-policy)# timeout fin-wait time</code>	FIN 待機のタイムアウトを秒数で設定します。デフォルトは 600 秒です。有効範囲は、75 ~ 600 秒です。
ステップ 7	<code>webvpn(config-tcp-policy)# buffer-share rx buffer_limit</code>	各接続の最大受信バッファ シェアをバイト数で設定します。デフォルトは 32768 バイトです。有効範囲は、8192 ~ 262144 バイトです。
ステップ 8	<code>webvpn(config-tcp-policy)# buffer-share tx buffer_limit</code>	各接続の最大送信バッファ シェアをバイト数で設定します。デフォルトは 32768 バイトです。有効範囲は、8192 ~ 262144 バイトです。
ステップ 9	<code>webvpn(config-tcp-policy)# tos carryover</code>	<p>フロー内のすべてのパケットに、Type of Service (ToS; サービス タイプ) を転送します。</p> <p> (注) ポリシーがサーバ TCP ポリシーとして設定されている場合、ToS 値はサーバからクライアントに送信されます。ポリシーが仮想ポリシーとして設定されている場合、ToS 値はクライアントからサーバに送信されます。</p> <p> (注) ToS 値は、伝播する前に学習される必要があります。たとえば、サーバからクライアントへの接続で ToS 値を伝播する場合、ToS 値を学習して伝播する前に、サーバ接続を確立する必要があります。したがって、いくつかの初期パケットは ToS 値を伝送しません。</p>
ステップ 10	<code>webvpn(config-tcp-policy)# [no] nagle</code>	<p>Nagle アルゴリズムをイネーブルにします。</p> <p>nagle キーワードを指定すると、アプリケーションにより書き込まれた少量のデータが接続送信キューに保管されますが、次のいずれかの状況が発生するまで、データは送信されません。</p> <ul style="list-style-type: none"> データが待機中で、前に送信したデータを確認する ACK を受信した場合 フルサイズ セグメントが作成されて送信されるように、アプリケーションによってさらにデータが書き込まれた場合 <p>nagle キーワードをディセーブルにすると、データのキューイングは無効になります。アプリケーションにより書き込まれたすべてのデータは、ただちに送信されます。</p> <p>Nagle は、デフォルトでイネーブルです。</p>

	コマンド	目的
ステップ 11	webvpn(config-tcp-policy)# delayed-ack-threshold <i>packets</i>	window-update ACK を送信する前に、受信する必要があるフルサイズ セグメント数を指定します。 <i>packets</i> の有効値は 1 ~ 10 で、デフォルトは 2 です。
ステップ 12	webvpn(config-tcp-policy)# delay-ack-timeout <i>timer</i>	<p>window-upate ACK を送信するまでの時間を指定します。</p> <p>タイムアウトになる前に (<i>delayed-ack-threshold</i> コマンドで指定した) フルサイズ セグメント数を受信していない場合、その時点までに受信した全データを確認する ACK が送信されますが、ウィンドウは更新されません。<i>timer</i> の有効値は 50 ~ 500 ミリ秒で、デフォルトは 200 です。</p>

1. パケット分割が発生する場合には、分割がなくなるまで MSS 値を減少してください。

PKI の設定

WebVPN サービス モジュール は、SSL プロトコルを使用して、機密、認証、およびデータ完全性によりセキュアなデータ トランザクションを実行します。SSL プロトコルでは、証明書、公開鍵、および秘密鍵を使用します。

デジタル ID カードと同様の証明書は、クライアントに対してサーバの身元を、サーバに対してクライアントの身元を証明するものです。認証局から発行される証明書には、証明書を発行されたエンティティの名前、エンティティの公開鍵、および証明書の有効期限を示すタイムスタンプが含まれています。

公開鍵および秘密鍵は、情報を暗号化および複号化するための暗号です。公開鍵は制約なしに共有できますが、秘密鍵は絶対に共有されません。公開鍵と秘密鍵は、ペアで使用します。公開鍵で暗号化したデータは、対応する秘密鍵でのみ複号化できます。

各 WebVPN モジュールは、最大 64 のゲートウェイをサポートします。各ゲートウェイは、HTTPS サーバとして動作します。認証に証明書を使用するには、各ゲートウェイに鍵のペアを設定する必要があります。

モジュールの起動時に、証明書を取得したり自動登録を行うために認証局にクエリを送信しなくても済むように、証明書を NVRAM に保管しておくことを推奨します。詳細については、「[コンフィギュレーションの保存](#)」(p.3-55)を参照してください。

ユーザがゲートウェイのポータル ページから HTTPS サイトにアクセスを試みた場合、WebVPN サービス モジュール は SSL クライアントとして動作し、そのサイトから受信した証明書を認証する必要があります。証明書の開始時刻、終了時刻、およびシグニチャが検証されます。

**(注)**

WebVPN コンテキストに `ssl authenticate verify none` コマンドを設定した場合には、証明書は確認されません。

鍵のペアが安全でない場合、有効な証明書が失効していることがあります。失効の確認が必要な場合、WebVPN サービス モジュール は認証局から Certificate Revocation List (CRL; 証明書失効リスト) をダウンロードし、受信した証明書のシリアル番号を検索します。

証明書は、特定の証明書アトリビュート値を Access Control List (ACL; アクセス制御リスト) マッピングと照合することにより、フィルタリングすることもできます。信頼できる認証局から発行され、認証された証明書だけが受け入れられます。

**(注)**

認証されるのは証明書だけで、証明書の送信者は認証されません。SSL ハンドシェイクの一部として、証明書の送信者には、証明書の公開鍵に対応する秘密鍵を所有しているかどうかを確認するチャレンジが送信されます。チャレンジに失敗すると、WebVPN サービス モジュール により、SSL ハンドシェイクは中止されます。

ここでは、Public Key Infrastructure (PKI; 公開鍵インフラストラクチャ) の設定方法について説明します。

- [鍵および証明書の設定](#) (p.3-29)
- [証明書およびトラストポイントの確認](#) (p.3-54)
- [コンフィギュレーションの保存](#) (p.3-55)
- [鍵および証明書のバックアップ](#) (p.3-56)

- [鍵および証明書のモニタおよびメンテナンス \(p.3-57\)](#)
- [WebVPN のゲートウェイおよびコンテキストへの証明書の割り当て \(p.3-58\)](#)
- [証明書の更新 \(p.3-59\)](#)
- [証明書の自動更新および自動登録 \(p.3-62\)](#)

鍵および証明書の設定

鍵および証明書は、次のいずれかの方法を使用して設定できます。

- Simple Certificate Enrollment Protocol (SCEP) を使用する場合には、次の手順で鍵および証明書を設定します。
 - 鍵のペアを生成する
 - トラストポイントを宣言する
 - 認証局の証明書を取得する
 - SSL サーバの代わりに認証局に登録リクエストを送信する

詳細については、「[SCEP を使用したトラストポイントの設定](#)」(p.3-29)を参照してください。

- SCEP を使用しない場合には、手動証明書登録 (TFTP およびカットアンドペースト) 機能を使用して、次の手順で、鍵および証明書を設定します。
 - 鍵のペアを生成またはインポートする
 - トラストポイントを宣言する
 - 認証局の証明書を取得し、TFTP またはカットアンドペーストを使用してトラストポイントを登録し、PKCS10 ファイルを作成する
 - PKCS10 パッケージを使用して、オフラインで SSL サーバ証明書をリクエストする
 - TFTP またはカットアンドペーストを使用して、SSL サーバ証明書をインポートする

詳細については、「[手動証明書登録](#)」(p.3-36)を参照してください。

- 外部 PKI システムを使用する場合には、次の作業を行います。
 - PKCS12 または Privacy Enhanced Mail (PEM) ファイルを生成する
 - このファイルをモジュールにインポートする

詳細については、「[鍵ペアおよび証明書のインポートおよびエクスポート](#)」(p.3-45)を参照してください。

外部 PKI システムは、鍵のペアを生成し、認証局または鍵と証明書のアーカイブシステムからの証明書を登録するサーバまたは PKI 管理システムです。Public-Key Cryptography Standards (PKCS) により、秘密鍵および証明書を含む個人身元情報の転送シンタックスが指定されています。この情報は、暗号化ファイルにパッケージされます。暗号化ファイルを開くには、パスフレーズが必要です。暗号鍵は、パスフレーズから抽出されます。



(注)

PKCS12 または PEM ファイルをインポートする前に、トラストポイントを設定する必要はありません。PKCS12 または PEM ファイルから鍵および証明書をインポートする場合、トランスポートが存在しなければ自動的に作成されます。

SCEP を使用したトラストポイントの設定

SCEP を使用してトラストポイントを設定するには、次の作業を行います。

- [RSA 鍵ペアの生成 \(p.3-30\)](#)
- [トラストポイントの宣言 \(p.3-32\)](#)

- [認証局の証明書の取得 \(p.3-33\)](#)
- [証明書のリクエスト \(p.3-33\)](#)

RSA 鍵ペアの生成



(注)

生成する最初の鍵ペアにより、モジュール上の SSH がイネーブルになります。SSH を使用する場合には、SSH 用の鍵ペアを設定してください。「[管理者用の認証の設定 \(p.2-5\)](#)」を参照してください。

RSA は、Ron Rivest、Adi Shamir、および Leonard Aldeman によって開発された公開鍵暗号化システムです。RSA アルゴリズムは、鍵ペアを生成するために、認証局および SSL サーバにより幅広く使用されています。各認証局および各 SSL サーバは、それぞれ独自の RSA 鍵ペアを所有しています。SSL サーバは、証明書を登録するときに、認証局に公開鍵を送信します。SSL サーバは、SSL セッションの確立時に、証明書を使用してクライアントに身元を証明します。

SSL サーバは、セキュアなストレージに秘密鍵を保管し、認証局には公開鍵だけを送信します。認証局は、認証局の秘密鍵を使用して、サーバの公開鍵およびサーバに関する他の身元情報が含まれた証明書に署名します。

各認証局は、秘密鍵の機密を保持し、秘密鍵を使用して、下位の認証局および SSL サーバの証明書に署名します。認証局は、認証局の公開鍵を含む証明書を所有しています。

認証局は、1 つまたは複数のレベルの階層から構成されます。最上位の認証局は、ルート認証局と呼ばれます。下位レベルの認証局は、中間認証局または下位認証局と呼ばれます。ルート認証局は自己署名した証明書を所有し、次に低いレベルの下位認証局の証明書に署名します。この下位認証局は、さらにその次に低いレベルの認証局の証明書に署名し、同様にして下位レベルに引き継がれます。最下位レベルの認証局は、SSL サーバの証明書に署名します。



(注)

WebVPN サービス モジュール は、最大 8 レベルの認証局 (1 つのルート認証局と 7 つまでの下位認証局) をサポートします。3 レベル (3 階層) 登録の例については、「[3 階層の認証局登録の例 \(p.3-34\)](#)」を参照してください。

これらの証明書は、最下位のサーバの証明書から、ルート認証局が自己署名した最上位の証明書までのチェーンを形成します。各シグニチャは、証明書本体のハッシュ ダイジェストを暗号化する、発行認証局の秘密鍵を使用して形成されます。証明書本体の最後にシグニチャが付加されると、証明書は完成します。

SSL セッションの確立時に、SSL サーバは自己の証明書チェーンをクライアントに送信します。クライアントは、次に上位の証明書から公開鍵を取得し、証明書に付加されたシグニチャを複号化して、チェーン上位の各証明書のシグニチャを検証します。複号化した結果は、証明書本体のハッシュ ダイジェストと比較されます。チェーン内の 1 つの認証局の証明書が、クライアントの所有データベースに保管されている信頼できる認証局の証明書と一致すると、検証は終了します。

チェーン最上位の認証局の証明書まで到達し、信頼できる自己署名の証明書と一致しない場合には、クライアントはセッションを終了するか、ユーザに対して証明書の信頼性を確認するように要求するプロンプトを表示します。

SSL はサーバの認証後、サーバ証明書の公開鍵を使用してシークレットを暗号化し、サーバに送信します。SSL サーバは、自己の秘密鍵を使用して、シークレットを複号化します。両サイドは、交換したシークレットと 2 つのランダム番号を使用して、以降の SSL セッションでのデータの暗号化、複号化、完全性チェックに必要な鍵を生成します。



(注) WebVPN サービス モジュール は、汎用の鍵だけをサポートします。

汎用の鍵を生成すると、1 つの RSA 鍵のペアだけが生成されます。名前付きの鍵ペアにより、複数の RSA 鍵のペアを作成し、Cisco IOS ソフトウェアで、各証明書に異なる鍵ペアを保持することができます。鍵ペアには名前を指定することを推奨します。



(注) 生成された鍵ペアは、システムメモリ (RAM) に保管されます。電源障害が発生したり、モジュールをリセットすると、鍵ペアは失われます。実行コンフィギュレーションを保存し、モジュールの NVRAM のプライベート コンフィギュレーション ファイルに鍵ペアを保存するには、`copy system:running-config nvram:startup-config` コマンドを入力する必要があります。

RSA 鍵ペアを生成するには、次の作業を行います。

コマンド	目的
<code>webvpn(config)# crypto key generate rsa general-keys label key-label [exportable¹] [modulus size]</code>	RSA 鍵ペアを生成します。

1. `exportable` キーワードを指定すると、鍵をエクスポートできます。鍵の生成中に、鍵をエクスポートできるように指定できます。エクスポート可能またはエクスポート不可として生成された鍵は、期限が切れるまで変更できません。



(注) RSA 鍵を生成すると、係数長をビット単位で入力するように要求されます。WebVPN サービス モジュール がサポートしている係数長は、512、768、1024、1536、および 2048 ビットです。512 または 768 も指定できますが、係数長は最低 1024 を指定することを推奨します。係数が長いほど生成に時間がかかり、使用時間も長くなりますが、セキュリティは強化されます。

次に、汎用 RSA 鍵を生成する例を示します。

```
webvpn(config)# crypto key generate rsa general-keys label kp1 exportable
```

```
The name for the keys will be: kp1
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

```
Generating RSA keys.... [OK].
```



(注) 鍵ペアを生成したら、自己署名の証明書を生成して、SSL サービスをテストできます。

■ PKI の設定

トラストポイントの宣言

各証明書について、WebVPN サービス モジュール が使用する 1 つのトラストポイントを宣言する必要があります。

モジュールが使用するトラストポイントを宣言し、トラストポイントの特性を指定するには、グローバル コンフィギュレーション モードから開始して、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config)# crypto pki trustpoint trustpoint-label¹</code>	モジュールが使用するトラストポイントを宣言します。このコマンドを入力すると、ca-trustpoint コンフィギュレーション モードが開始されます。
ステップ 2	<code>webvpn(ca-trustpoint)# rsakeypair key-label</code>	証明書に関連付ける鍵ペアを指定します。
ステップ 3	<code>webvpn(ca-trustpoint)# enrollment [mode ra] [retry [period minutes] [count count]] url url</code>	認証局の登録パラメータを指定します。
ステップ 4	<code>webvpn(ca-trustpoint)# ip-address server_ip_addr</code>	(任意) この証明書を使用する WebVPN ゲートウェイの IP アドレスを指定します。 ²
ステップ 5	<code>webvpn(ca-trustpoint)# password password</code>	(任意) チャレンジパスワードを設定します。
ステップ 6	<code>webvpn(ca-trustpoint)# revocation-check method1 [method2[method3]]</code>	(任意) 証明書の失効ステータスをチェックする方法を指定します。 次の方法を指定できます。 <ul style="list-style-type: none"> • crl CRL により、証明書チェックを実行します。これがデフォルト設定です。 • none 証明書チェックを実行しません。 • ocsp Online Certificate Status Protocol (OCSP) サーバにより、証明書チェックを実行します。 ² 番めおよび ³ 番め方法を指定すると、サーバがダウンしているなど、最初に指定した方法がエラーだった場合に、次の方法が使用されます。
ステップ 7	<code>webvpn(ca-trustpoint)# subject-name line^{3, 4}</code>	(任意) WebVPN ゲートウェイのホスト名を設定します。 ⁵
ステップ 8	<code>webvpn(ca-trustpoint)# exit</code>	ca-trustpoint コンフィギュレーション モードを終了します。

1. `trustpoint-label` は鍵の `key-label` と一致しているべきですが、必須ではありません。
2. 一部の Web ブラウザは、SSL サーバ証明書の IP アドレスと、URL に表示される IP アドレスとを比較します。IP アドレスが一致しない場合、ブラウザに、この証明書を受け入れるか拒否するかをクライアントに問い合わせるダイアログボックスが表示されることがあります。
3. たとえば、`subject-name CN=server1.domain2.com` のように入力します。`server1` には URL に表示する SSL サーバ名を指定します。`subject-name` コマンドは、Lightweight Directory Access Protocol (LDAP) 形式を使用します。
4. サブジェクト名に指定する引数は、カンマが含まれている場合、引用符で囲む必要があります (例: `O="Cisco, Inc."`)。
5. 一部のブラウザは、SSL サーバ証明書のサブジェクト名の CN フィールドと、URL に表示されるホスト名を比較します。名前が一致しない場合、ブラウザに、この証明書を受け入れるか拒否するかをクライアントに問い合わせるダイアログボックスが表示されることがあります。また、一部のブラウザは、証明書に CN フィールドが定義されていない場合、SSL セッションの確立を拒否し、セッションを自動終了します。

次に、トラストポイント PROXY1 を宣言し、接続を確認する例を示します。

```
webvpn(config)# crypto pki trustpoint PROXY1
webvpn(ca-trustpoint)# rsakeypair PROXY1
webvpn(ca-trustpoint)# enrollment url http://exampleCA.cisco.com
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# subject-name C=US, ST=California, L=San Jose, O=Cisco, OU=Lab,
CN=host1.cisco.com
webvpn(ca-trustpoint)# end
webvpn# ping example.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
webvpn#
```

認証局の証明書の取得

各トラストポイントについて、認証局の公開鍵を含む証明書を取得する必要があります。複数のトラストポイントに、同じ認証局を使用できます。



(注)

証明書の正しいフィンガープリントを取得して、コンソールに表示されたフィンガープリントを確認する場合には、認証局に問い合わせてください。

認証局の公開鍵を含む証明書を取得するには、グローバル コンフィギュレーション モードで、次の作業を行います。

コマンド	目的
webvpn(config)# crypto pki authenticate <i>trustpoint-label</i>	認証局の公開鍵を含む証明書を取得します。 <i>trustpoint_label</i> には、トラストポイントの宣言時に 入力したものと同じ値を入力します。

次に、認証局の証明書を取得する例を示します。

```
webvpn(config)# crypto pki authenticate PROXY1
Certificate has the following attributes:
Fingerprint: A8D09689 74FB6587 02BFE0DC 2200B38A
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
webvpn(config)# end
webvpn#
```

証明書のリクエスト

各トラストポイントについて、認証局から署名された証明書を取得する必要があります。

署名された証明書を認証局にリクエストするには、グローバル コンフィギュレーション モードで、次の作業を行います。

コマンド	目的
webvpn(config)# crypto pki enroll <i>trustpoint-label</i> ¹	トラストポイント用の証明書をリクエストしま す。

1. コンフィギュレーションに保存されないチャレンジ パスワードを任意で作成できます。このパスワードは、証明書を失効する必要がある場合に要求されるので、忘れないでください。



(注)

pki enroll コマンドを入力し、証明書を受領する前にモジュールまたはスイッチをリブートした場合には、このコマンドを再入力し、認証局の管理者に通知する必要があります。

次に、証明書をリクエストする例を示します。

```
webvpn(config)# crypto pki enroll PROXY1
%
% Start certificate enrollment..

% The subject name in the certificate will be: C=US; ST=California; L=San Jose;
O=Cisco; OU=Lab; CN=host1.cisco.com
% The subject name in the certificate will be: host.cisco.com
% The serial number in the certificate will be: 00000000
% The IP address in the certificate is 10.0.0.1

% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.
Fingerprint: 470DE382 65D8156B 0F84C2AF 4538B913
webvpn(config)# end
```

トラストポイントの設定後、証明書およびトラストポイントの情報を確認する方法は、「[証明書およびトラストポイントの確認](#)」(p.3-54)を参照してください。

3 階層の認証局登録の例

WebVPN サービス モジュール は、最大 8 レベルの認証局 (1 つのルート認証局と 7 つまでの下位認証局) をサポートします。

次に、3 レベルの認証局を設定する例を示します。

- 鍵を生成します。

```
webvpn(onfig)# crypto key generate rsa general-keys label key1 exportable
The name for the keys will be:key1
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
```

- トラストポイントを定義します。

```
webvpn(config)# crypto pki trustpoint 3tier-root
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.1
webvpn(ca-trustpoint)#
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki trustpoint 3tier-sub1
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.2
webvpn(ca-trustpoint)#
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki trustpoint tp-proxy1
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.3
webvpn(ca-trustpoint)# serial-number
webvpn(ca-trustpoint)# password cisco
webvpn(ca-trustpoint)# subject CN=ste.cisco.com
webvpn(ca-trustpoint)# rsakeypair key1
webvpn(ca-trustpoint)# show
  enrollment url tftp://10.1.1.3
  serial-number
  password 7 02050D480809
  subject-name CN=ste.cisco.com
  rsakeypair key1
end
webvpn(ca-trustpoint)# exit
```

- 3つの認証局(1つのルート認証局および2つの下位認証局)を認証します。

```
webvpn(config)# crypto pki authenticate 3tier-root
Certificate has the following attributes:
Fingerprint:84E470A2 38176CB1 AA0476B9 C0B4F478
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
webvpn(config)#
webvpn(config)# crypto pki authenticate 3tier-sub1
Certificate has the following attributes:
Fingerprint:FE89FB0D BF8450D7 9934C926 6C66708D
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
webvpn(config)#
webvpn(config)# crypto pki authenticate tp-proxy1
Certificate has the following attributes:
Fingerprint:6E53911B E29AE44C ACE773E7 26A098C3
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
```

- 3番目のレベルの認証局で登録を行います。

```
webvpn(config)# crypto pki enroll tp-proxy1
%
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be:ste.
% The subject name in the certificate will be:ste.
% The serial number in the certificate will be:B0FFF0C2
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]:yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

webvpn(config)#      Fingerprint: 74390E57 26F89436 6FC52ABE 24E23CD9

webvpn(config)#
*Apr 18 05:10:20.963:%CRYPTO-6-CERTRET:Certificate received from Certificate
Authority
```

手動証明書登録

手動証明書登録 (TFTP およびカットアンドペースト) 機能により、証明書のリクエストを生成し、認証局の証明書およびルータ証明書を受け入れることができます。これらの作業には、TFTP サーバまたは手動でのカットアンドペースト操作を使用します。TFTP または手動カットアンドペーストによる登録は、次の状況で使用できます。

- 認証局が (リクエストおよび証明書を送受信する最も一般的な方法である) SCEP をサポートしていない場合
- (Cisco IOS ソフトウェアを実行しているルータが証明書を取得する方法である) ルータと認証局間のネットワーク接続が不可能な場合

次の URL にある説明に従って、手動証明書登録 (TFTP およびカットアンドペースト) 機能を設定します。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmancr.htm>



(注)

CRL サーバにアクセスできない、または CRL ダウンロードパスが存在しないことが原因で CRL をダウンロードできない場合、証明書のインポートに失敗することがあります。インポート処理に関連するすべてのトラストポイントで、CRL をダウンロードできることを確認してください。CRL パスが存在しない場合、または CRL サーバにアクセスできない場合には、インポート処理に関連するすべてのトラストポイントに、`revocation-check none` コマンドを入力する必要があります。すべての証明書の情報を表示し、認証局の証明書の表示から関連トラストポイントのリストを取得するには、`show crypto pki certificates` コマンドを入力します。これらのすべてのトラストポイントに、`revocation-check none` コマンドを入力します。

たとえば、3 レベルの認証局階層 (ルート CA、下位 CA1、下位 CA2) で、下位 CA1 の証明書をインポートする場合、ルート CA に関連するすべてのトラストポイントに、`revocation-check none` コマンドを入力します。同様に、下位 CA2 の証明書をインポートする場合には、ルート CA および下位 CA1 に関連するすべてのトラストポイントに、`revocation-check none` コマンドを入力します。

証明書を正常にインポートしたあと、トラストポイントの CRL オプションを元に戻すことができます。

例 1 : TFTP を使用した証明書登録の設定 (1 階層の認証局)

1. トラストポイントを設定します。

```
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn(config)# crypto pki trustpoint tftp_example
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.2/win2k
webvpn(ca-trustpoint)# rsakeypair pair3
webvpn(ca-trustpoint)# exit
```

2. トラストポイント用の証明書をリクエストします。

```
webvpn(config)# crypto pki enroll tftp_example
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: ssl-proxy.cisco.com
% The subject name in the certificate will be: ssl-proxy.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 00000000
% Include an IP address in the subject name? [no]:
Send Certificate Request to tftp server? [yes/no]: yes
% Certificate request sent to TFTP Server
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.
webvpn(config)#   Fingerprint:  D012D925 96F4B5C9 661FEC1E 207786B7
!!
```

3. 認証局の公開鍵を含む証明書を取得します。

```
webvpn(config)# crypto pki auth tftp_example
Loading win2k.ca from 10.1.1.2 (via Ethernet0/0.168): !
[OK - 1436 bytes]

Certificate has the following attributes:
Fingerprint: 2732ED87 965F8FEB F89788D4 914B877D
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
webvpn(config)#
```

4. サーバの証明書をインポートします。

```
webvpn(config)# crypto pki import tftp_example cert
% The fully-qualified domain name in the certificate will be: ssl-proxy.cisco.com
Retrieve Certificate from tftp server? [yes/no]: yes
% Request to retrieve Certificate queued

webvpn(config)#
Loading win2k.crt from 10.1.1.2 (via Ethernet0/0.168): !
[OK - 2112 bytes]

webvpn(config)#
*Apr 15 12:02:33.535: %CRYPTO-6-CERTRET: Certificate received from Certificate
Authority
webvpn(config)#
```

例 2 : カットアンドペーストを使用した証明書登録の設定 (1 階層の認証局)

1. RSA 鍵ペアを生成します。

```
webvpn(config)# crypto key generate rsa general-keys label CSR-key exportable
The name for the keys will be:CSR-key
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
```

2. トラストポイントを設定します。

```
webvpn(config)# crypto pki trustpoint CSR-TP
webvpn(ca-trustpoint)# rsa keypair CSR-key
webvpn(ca-trustpoint)# serial
webvpn(ca-trustpoint)# subject-name CN=abc, OU=hss, O=cisco
webvpn(ca-trustpoint)# enrollment terminal
webvpn(ca-trustpoint)# exit
```


5. サーバの証明書をインポートします（サーバの証明書は、手順4で証明書をインポートした認証局により発行されます）。

```
webvpn(config)# crypto pki import CSR-TP certificate
% The fully-qualified domain name in the certificate will be:ssl-proxy.cisco.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIB7TCCAUYCAQQwDQYJKoZIhvcNAQEEBQAwUjELMAkGA1UEBhMCQVUxEzARBgNV
BAgTC1NvbWUtU3RhdGUxITAfBgNVBAoTGEIudGVybmV0IFdpZGdpdHMgUHR5IEExO
ZDELMAkGA1UEAxMCY2EwHhcNMDMxMTIwMDAxMzE2WhcNMDE5MDAxMzE2WjAs
MQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECzMHaHZNMQwwCgYDVQQDEwNhYmMwZ8w
DQYJKoZIhvcNAQEEBQADgY0AMIGJAoGBALt706tt301BVVK1qAE/agsuzIaa15YZ
ft3bDb9t3pPncKh0ivBTgVKpJiLPWGPjdbtejxQksuSY589V+GMDrO9B4Sxn+5N
p2bQmd745NvI4gorNRvXcdjmE+/SzE+bBSBcKAwNtYSF77R1pmhK0WSKPuu7fJPY
r/Cbo80OUzkRAgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAjqJ9378P6Gz69Ykplw06
Powp+2rbe2iFBrE1xE09BL6G6vzcBQgb5W4uwqxe7SIHrHsS0/7Be3zeJn1OseWx
/KVj7I02iPgrwUa9DLavwrTyaa0KtTpti/i5nIwTNh5xkp2bBJQikD4TEK7HAvXf
HQ9SyB3YZJk/Bjp6/eFHEfU=
-----END CERTIFICATE-----

% Router Certificate successfully imported

webvpn(config)#^Z
```

例3：TFTPを使用した証明書登録の設定（3階層の認証局）

1. RSA 鍵ペアを生成します。

```
webvpn(config)# crypto key generate rsa general-keys label test-3tier exportable
The name for the keys will be:test-3tier
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
```

2. トラストポイントを設定します。

```
webvpn(config)# crypto pki trustpoint test-3tier
webvpn(ca-trustpoint)# serial-number
webvpn(ca-trustpoint)# password cisco
webvpn(ca-trustpoint)# subject CN=test-3tier, OU=hss, O=Cisco
webvpn(ca-trustpoint)# rsa-keypair test-3tier
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.3/test-3tier
webvpn(ca-trustpoint)# exit
```

3. Certificate Signing Request (CSR) を生成し、TFTP サーバに送信します。

```
webvpn(config)# crypto pki enroll test-3tier
%
% Start certificate enrollment ..

% The subject name in the certificate will be:CN=test-3tier, OU=hss, O=Cisco
% The fully-qualified domain name in the certificate will be:ssl-proxy.cisco.com
% The subject name in the certificate will be:ssl-proxy.cisco.com
% The serial number in the certificate will be:B0FFF22E
% Include an IP address in the subject name? [no]:
Send Certificate Request to tftp server? [yes/no]:yes
% Certificate request sent to TFTP Server
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

webvpn(config)# Fingerprint: 19B07392 319B2ACF F8FABE5C 52798971

webvpn(config)#
!!
```

4. CSR を使用して、3 番目のレベルの認証局からオフラインで SSL 証明書を取得します。

5. 3 つの認証局 (1 つのルート認証局および 2 つの下位認証局) を認証します。

```
webvpn(config)# crypto pki trustpoint test-1tier
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.3/test-1tier
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki authenticate test-1tier
Loading test-1tier.ca from 10.1.1.3 (via Ethernet0/0.172):!
[OK - 1046 bytes]

Certificate has the following attributes:
Fingerprint:AC6FC55E CC29E891 0DC3FAAA B4747C10
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.

webvpn(config)# crypto pki trustpoint test-2tier
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.3/test-2tier
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki authenticate test-2tier
Loading test-2tier.ca from 10.1.1.3 (via Ethernet0/0.172):!
[OK - 1554 bytes]

Certificate has the following attributes:
Fingerprint:50A986F6 B471B82D E11B71FE 436A9BE6
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.

webvpn(config)# crypto pki authenticate test-3tier
Loading test-3tier.ca from 10.1.1.3 (via Ethernet0/0.172):!
[OK - 1545 bytes]

Certificate has the following attributes:
Fingerprint:2F2E44AC 609644FA 5B4B6B26 FDBFE569
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
```


6. サーバの証明書をインポートします。

```
webvpn(config)# crypto pki import test-3tier certificate
% The fully-qualified domain name in the certificate will be:ssl-proxy.cisco.com
Retrieve Certificate from tftp server? [yes/no]:yes
% Request to retrieve Certificate queued

webvpn(config)#
Loading test-3tier.crt from 10.1.1.3 (via Ethernet0/0.172):!
[OK - 1608 bytes]

webvpn(config)#
*Nov 25 21:52:36.299:%CRYPTO-6-CERTRET:Certificate received from Certificate
Authority
webvpn(config)# ^Z
```

例4：カットアンドペーストを使用した証明書登録の設定（3階層の認証局）

1. RSA 鍵ペアを生成します。

```
webvpn(config)# crypto key generate rsa general-keys label tp-proxy1 exportable
The name for the keys will be:tp-proxy1
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
```

2. トラストポイントを設定します。

```
webvpn(config)# crypto pki trustpoint tp-proxy1
webvpn(ca-trustpoint)# enrollment ter
webvpn(ca-trustpoint)# rsakeypair tp-proxy1
webvpn(ca-trustpoint)# serial
webvpn(ca-trustpoint)# subject-name CN=test
webvpn(ca-trustpoint)# exit
```

3. トラストポイント用の証明書をリクエストします。

```
webvpn(config)# crypto pki enroll tp-proxy1
% Start certificate enrollment ..

% The subject name in the certificate will be:CN=test
% The fully-qualified domain name in the certificate will be:ssl-proxy.
% The subject name in the certificate will be:ssl-proxy.
% The serial number in the certificate will be:B0FFF14D
% Include an IP address in the subject name? [no]:no
Display Certificate Request to terminal? [yes/no]:yes
Certificate Request follows:

MIIBnDCCAQUCAQAwOzenMA5GA1UEAxMEdGVzdDEqMA8GA1UEBRMIQjBGRkYxNEQw
FwYJKoZIhvcNAQkCFgpzc2wtchJveHkuMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQDFx1o19IXoAx4fyUhaXH6s4p5t9soIZ1gvLtVX6Fp6zfuX47os5TGJH/IX
zv9B4e5Kv+wLMD0AvTh+/tvyAP3TmPcdpHYosd2VaTIgExpHf4M5Ruh8IebVKV25
rraIpNiS0PvPLFcrw4UfJVNpsc2XBxBhpT+FS9y67Lq1hfSN4wIDAQABOCEwHwYJ
KoZIhvcNAQkOMRIwEDA0BgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEEBQADgYEA
kOIjd1KNJdKLMf33YELRd3MW/ujJIuiT1J8RYVbw1eE8JQf68TTdKiYqzQcMgsp
ez3vSPxXFZ/c6naXdVyrTikTX3GZlmu+UOvV6/Jaf5QcXa9tAi3fgyguV7jQMPjk
Qj2GrwhXjczGOMBh6Kq6s5UPSIDgrL036I42B6B3EQ=

---End - This line not part of the certificate request---
```

```
Redisplay enrollment request? [yes/no]:no
```

4. 3番目のレベルの認証局によって署名された、手順3の証明書リクエストを取得します。

5. すべての認証局 (1 つのルート認証局および 2 つの下位認証局) を定義し、インポートします。
 - a. ルート認証局および下位認証局 1 用の 2 つのトラストポイントを定義します。



(注) この例では、下位認証局 2 の証明書をインポートするために、`tp-proxy1` を使用しています。

```
webvpn(config)# crypto pki trustpoint 3tier-root
webvpn(ca-trustpoint)# enrollment terminal
webvpn(ca-trustpoint)# crl op
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki trustpoint 3tier-sub1
webvpn(ca-trustpoint)# enrollment terminal
webvpn(ca-trustpoint)# crl op
webvpn(ca-trustpoint)# exit
```

- b. ルート認証局の証明書をインポートします。

```
webvpn(config)# crypto pki authenticate 3tier-root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIC1zCCAoGgAwIBAgIQadUxzU/i97hDmZRYJ1bBcDANBgkqhkiG9w0BAQUFADB1
MQswCQYDVQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcn5pYTERMA8GA1UEBxMlczFu
IGpvc2UxZDpAMBgNVBAoTBWVpc2NvMjQwYDQwYDQwYDQwYDQwYDQwYDQwYDQw
bXBzBz24tZGV2dGVzdC1yb290LUNBMB4XDFAzMTEwMTEwNDgwM1oXDTEzMTExMTEw
NTczOVowdTElMAkGA1UEBhMCVVMxEzARBgNVBAGTCmNhbG1mb3JuaWExETAPEgNV
BACrTCHNhbiBqb3NlMQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECzMMDaHhZMSAwHgYD
VQDEdXdaW1wc29uLWRLdnRlc3Qtc9vdc1DQTBcMA0GCSqGSIb3DQEBAQUAA0sA
MEGCCQCWEibAnU1VqQNU0Wb94qnHi8FKjmVhibLHGR16J+V7gHgzmf2MTz5WP51
VQ2/1NVu0HjUORRdeCm1/raKJ/7ZAgMBAAGjgewwgewkCwYDVR0PBAQDAgHGMA8G
A1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFYGLUBTKNd9EgUonHnoSvvhg0axMIGX
BgNVHR8EgY8wgYwwQ6BBOD+GPWh0dHA6Ly9jaXNjb3R1b3R1b3R1b3R1b3R1b3R1
cm9sbC9zaW1wc29uLWRLdnRlc3Qtc9vdc1DQs5jcmwwRaBDoEGGP2ZpbGU6Ly9c
XGNpc2NvLWw4ajZvaHBuclxDZXJ0RW5yb2xsXHNpbXBzBz24tZGV2dGVzdC1yb290
LUNBLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAANBACBqelwy
YjalelGZqLVu4bdVMFo6ELCV2AMBgi41K3ix+Z/03Pjd7ct2BIAF41ktv9pCe6IO
EoBcmZteA+TQcKg=
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:AC6FC55E CC29E891 0DC3FAAA B4747C10
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

c. 下位認証局 1 の証明書をインポートします。

```
webvpn(config)# crypto pki authenticate 3tier-sub1
```

```
Enter the base 64 encoded CA certificate.
```

```
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIEtzCCA/mgAwIBAgIKGj0cBwAAAAADjANBgkqhkiG9w0BAQUFADB1MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcmlpYTERMA8GA1UEBxMIc2FuIGpvc2Ux
DjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLLEwNoc3MxIDAeBgNVBAMTF3NpbXBz
b24tZGV2dGVzdC1yb290LUNBMB4XDTAzMTEwMzIyMDQyMVoXDTA0MTEwMzIy
dTElMAkGA1UEBhMCVVMxExARBgNVBAGTCmNhbG1mb3JuaWEwEwETAPBgNVBAC
TCHNhbiBqb3N1MQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECXMdAHNzMSAwHgYD
VQDEXDdzaw1wc29uLWRLdnRlc3Qtc3ViMS1jYTBcMA0GCsqGSIb3DQEBAAQAA0
sAMEgCQQDcv48nC2uukoSyGJ/GymCIEZXzMSzpbkYS7eWPaZYyiJDhCIKuUsMg
FDRNFmQmUSArcWmPizFZc9PFumDa03vAgMBAAGjggJpMIICZTAQBgkrBgEAAI
I3FQEEAwIBADADBgNVHQ4EFggQUWaaNN2U14BaBoU9mY+ncuHpP920wCwYDVR
0PBAQDAGHGMA8GA1UdEwEB/wQFMAMBAf8wga4GA1UdIwSbPjCBo4AUJgYtQFMo
130SBSiceehK9seDRrGhear3MHUxCzAJBgNVBAYTALVTMRMwEQYDVQQLIEwpcjYw
xpZm9ybmlhMRERwDwYDVQQH
EwhzYW4gam9zZTEOMAwGA1UEChMFY21zY28xDDAKBgNVBAsTAA2hzcEgMB4GA
1UEAxMxc21tcHNvbi1kZXZ0ZXN0LXJvb3QtQ0GCEGnVMc1P4ve4Q5mUWCdWwX
AwgZcGA1UdHwSBjzCBjDBDoEGGp4Y9aHR0cDovL2Npc2NvLWw4ajZvaHBuc19D
ZXJ0RW5yb2xsL3NpbXBzZb24tZGV2dGVzdC1yb290LUNBMLmNybDBFoEOgQYY
/ZmlsZTovL1xcY21zY28tbDhqNm9ocG5yXEN1cnRFbnJvbGxccc21tcHNvbi1k
ZXZ0ZXN0LXJvb3QtQ0EuY3JsmIHIBggrBgEFBQcBAQsBuzCBuDBZBggrBgEF
BQcwAoZNaHR0cDovL2Npc2NvLWw4ajZvaHBuc19DZXJ0RW5yb2xsL2Npc2Nv
LWw4ajZvaHBuc19zaW1wc29uLWRLdnRlc3Qtc3ViMS1jYTBcMA0GCsqGSIb3
DQEBAAQAA0sAMEgCQQDcv48nC2uukoSyGJ/jcnQwWwYIKwYBBQUHMAKGT2Zpb
GU6Ly9cXGNpc2NvLWw4ajZvaHBuc1xZDZXJ0RW5yb2xsXGNpc2NvLWw4ajZva
HBuc19zaW1wc29uLWRLdnRlc3Qtc3ViMS1jcnQwDQYJKoZIhvcNAQEFBQADQQA
6kAV3Jx/BOr2h1Sp9ER36ZkDJNIW93gNt2MkpcA07RmcrHln6q5RJ9WbvTxFnON
Dggsag1EcOwn97XErHZZow
```

```
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
```

```
Fingerprint:50A986F6 B471B82D E11B71FE 436A9BE6
```

```
Certificate validated - Signed by existing trustpoint CA certificate.
```

```
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```




(注)

CRL サーバにアクセスできない、または CRL ダウンロードパスが存在しないことが原因で CRL をダウンロードできない場合、証明書のインポートに失敗することがあります。インポート処理に関連するすべてのトラストポイントで、CRL をダウンロードできることを確認してください。CRL パスが存在しない場合、または CRL サーバにアクセスできない場合には、インポート処理に関連するすべてのトラストポイントに、`revocation-check none` コマンドを入力する必要があります。すべての証明書の情報を表示し、認証局の証明書の表示から関連トラストポイントのリストを取得するには、`show crypto pki certificates` コマンドを入力します。これらのすべてのトラストポイントに、`revocation-check none` コマンドを入力します。

たとえば、3 レベルの認証局階層（ルート CA、下位 CA1、下位 CA2）で、下位 CA1 の証明書をインポートする場合、ルート CA に関連するすべてのトラストポイントに、`revocation-check none` コマンドを入力します。同様に、下位 CA2 の証明書をインポートする場合には、ルート CA および下位 CA1 に関連するすべてのトラストポイントに、`revocation-check none` コマンドを入力します。

証明書を正常にインポートしたあと、トラストポイントの CRL オプションを元に戻すことができます。

PKCS12 ファイルのインポートおよびエクスポート

外部 PKI システムを使用して PKCS12 ファイルを生成し、このファイルを WebVPN サービス モジュールにインポートできます。



(注)


PKCS12 ファイルを作成する場合には、サーバ証明書からルート証明書までの完全な証明書チェーン、公開鍵、および秘密鍵を含めます。また、WebVPN サービス モジュール から PKCS12 ファイルを生成し、エクスポートすることもできます。



(注)

SSH を使用する場合には、PKCS12 ファイルをインポートまたはエクスポートするときに、Secure File Transfer (SCP) を使用することを推奨します。SCP は、ホストを認証し、転送セッションを暗号化します。

PKCS12 ファイルをインポートまたはエクスポートするには、次の作業を行います。

コマンド	目的
<pre>webvpn(config)# crypto pki {import export} trustpoint_label pkcs12 {scp: ftp: nvram: rcp: tftp:} [pkcs12_filename¹] pass_phrase²</pre>	<p>PKCS12 ファイルをインポートまたはエクスポートします。</p> <p> (注) PKCS12 ファイルをインポートする前に、トラストポイントを設定する必要はありません。PKCS12 ファイルから鍵および証明書をインポートすると、トラストポイントが存在しなければ自動的に作成されます。</p>

1. `pkcs12_filename` に値を指定しないと、デフォルトのファイル名を受け入れる（デフォルトのファイル名は、`trustpoint_label` です）。あるいはファイル名を入力するためのプロンプトが表示されます。`ftp:` または `tftp:` には、`pkcs12_filename` のフルパス名を指定します。
2. パスフレーズを正しく入力しないと、エラーになります。

次に、SCP を使用して PKCS12 ファイルをインポートする例を示します。

```
webvpn(config)# crypto pki import TP2 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Source username [ssl-proxy]? admin-1
Source filename [TP2]? /users/admin-1/pkcs12/TP2.p12

Password:password
Sending file modes:C0644 4379 TP2.p12
!
webvpn(config)#
*Aug 22 12:30:00.531:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
webvpn(config)#
```

次に、SCP を使用して PKCS12 ファイルをエクスポートする例を示します。

```
webvpn(config)# crypto pki export TP1 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination username [ssl-proxy]? admin-1
Destination filename [TP1]? TP1.p12

Password:

Writing TP1.p12 Writing pkcs12 file to scp://admin-1@10.1.1.1/TP1.p12

Password:
!
CRYPTO_PKI:Exported PKCS12 file successfully.
webvpn(config)#
```

次に、FTP を使用して PKCS12 ファイルをインポートする例を示します。

```
webvpn(config)# crypto pki import TP2 pkcs12 ftp: sky is blue
Address or name of remote host []? 10.1.1.1
Source filename [TP2]? /admin-1/pkcs12/PK-1024
Loading /admin-1/pkcs12/PK-1024 !
[OK - 4339/4096 bytes]
webvpn(config)#
```

次に、FTP を使用して PKCS12 ファイルをエクスポートする例を示します。

```
webvpn(config)# crypto pki export TP1 pkcs12 ftp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination filename [TP1]? /admin-1/pkcs12/PK-1024
Writing pkcs12 file to ftp://10.1.1.1/admin-1/pkcs12/PK-1024

Writing /admin-1/pkcs12/PK-1024 !!
CRYPTO_PKI:Exported PKCS12 file successfully.
webvpn(config)#
```

PKCS12 ファイルをインポートしたあと、証明書およびトラストポイントの情報を確認するには、[「証明書およびトラストポイントの確認」](#)(p.3-54)を参照してください。

PEM ファイルのインポートおよびエクスポート



(注) `crypto pki import pem` コマンドは、秘密鍵 (.prv)、サーバの証明書 (.crt)、および発行認証局の証明書 (.ca) だけをインポートします。証明書チェーンに複数レベルの認証局が含まれている場合には、このコマンドを入力する前に、認証のためにルート認証局および下位認証局の証明書をインポートする必要があります。ルート認証局および下位認証局の証明書をインポートするには、カットアンドペーストまたは TFTP を使用します。





(注) インポートした鍵ペアをエクスポートすることはできません。



(注) SSH を使用する場合には、PEM ファイルをインポートまたはエクスポートするときに、SCP を使用することを推奨します。SCP は、ホストを認証し、転送セッションを暗号化します。

PEM ファイルをインポートまたはエクスポートするには、次の作業を行います。

コマンド	目的
<pre>webvpn(config)# crypto pki import trustpoint_label pem [exportable] {terminal url {scp: ftp: nvram: rcp: tftp:} usage-keys} pass_phrase^{1,2}</pre>	<p>PEM ファイルをインポートします。</p> <p> (注) PEM ファイルをインポートする前に、トラストポイントを設定する必要はありません。PEM ファイルから鍵および証明書をインポートすると、トラストポイントが存在しなければ自動的に作成されます。</p>
<pre>webvpn(config)# crypto pki export trustpoint_label pem {terminal url {scp: ftp: nvram: rcp: tftp:} [des 3des] pass_phrase^{1,2}</pre>	<p>PEM ファイルをエクスポートします。</p> <p> (注) 鍵、サーバの証明書、およびサーバ証明書の発行認証局だけがエクスポートされます。上位のすべての認証局は、カットアンドペーストまたは TFTP を使用してエクスポートする必要があります。</p>

1. パスフレーズを正しく入力しないと、エラーになります。
2. パスフレーズは、秘密鍵を含む PEM ファイルを保護します。PEM ファイルは、DES または 3DES により暗号化されます。暗号鍵は、パスフレーズから抽出されます。証明書が含まれている PEM ファイルは暗号化されず、パスフレーズでは保護されません。

次に、TFTP を使用して PEM ファイルをインポートする例を示します。



(注) TP5.ca、TP5.prv、および TP5.crt ファイルは、サーバ上に存在している必要があります。

```
webvpn(config)# crypto pki import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
webvpn(config)#end
webvpn#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

次に、TFTP を使用して PEM ファイルをエクスポートする例を示します。

```
webvpn(config)# crypto pki export TP5 pem url tftp://10.1.1.1/tp99 3des password
% Exporting CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [tp99.ca]?
% File 'tp99.ca' already exists.
% Do you really want to overwrite it? [yes/no]: yes
!Writing file to tftp://10.1.1.1/tp99.ca!
% Key name: key1
Usage: General Purpose Key
% Exporting private key...
Address or name of remote host [10.1.1.1]?
Destination filename [tp99.prv]?
% File 'tp99.prv' already exists.
% Do you really want to overwrite it? [yes/no]: yes
!Writing file to tftp://10.1.1.1/tp99.prv!
% Exporting router certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [tp99.crt]?
% File 'tp99.crt' already exists.
% Do you really want to overwrite it? [yes/no]: yes
!Writing file to tftp://10.1.1.1/tp99.crt!
webvpn(config)#
```

PEM ファイルをインポートしたあと、証明書およびトラストポイントの情報を確認するには、「[証明書およびトラストポイントの確認](#)」(p.3-54)を参照してください。

3 レベルの認証局用の PEM ファイルをインポートする例

この例では、ルート認証局の証明書（1 番目の階層）および中間認証局の証明書（2 番目の階層）を、オフライン登録のカットアンドペースト オプションを使用して取得しています。中間認証局の証明書（3 番目の階層）、秘密鍵、およびルータの証明書は、PEM ファイルのインポートによって取得します。

1. カットアンドペーストを使用して、ルート認証局（1 番目の階層）の証明書を取得します。

```
webvpn(config)# crypto pki trustpoint 3tier-root
webvpn(ca-trustpoint)# enrollment terminal
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki authenticate 3tier-root
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIC1zCCAoGgAwIBAgIQadUxzU/i97hDmZRYJ1bBcDANBgkqhkiG9w0BAQUFADB1
MQswCQYDVQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcn5pYTERMA8GA1UEBxMIc2Fu
IGpvc2UxZDjAMBgNVBAoTBWVnc2NvMjYwYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZl
YDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZl
YDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZl
NTczOVowdTElMAkGA1UEBhMCVVMxEzARBgNVBAGTCmNhbG1mb3JuaWEwETAPBgNV
BACzTCHNhb3NlMQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECzMdaHNzMSAwHgYD
VQDEdzaW1wc29uLWRldnRlc3Qtc29uLWRldnRlc3Qtc29uLWRldnRlc3Qtc29uLWRldn
MEgCQQCWEibAnU1VqQUN0Wb94qnHi8FKjmVhibLHGR16J+V7gHgzmF2MTz5WP51
VQ2/1NVu0HjUORRdeCm1/raKJ/7ZAgMBAAGjgewwgekWCwYDVR0PBAQDAgHGMA8G
A1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFcYGLUBTKNd9EgUonHnoSvbHg0axMIGX
BgNVHR8EgY8wgYwwQ6BBOD+GPWh0dHA6Ly9jaXNjb3NlYDZlYDZlYDZlYDZlYDZlYDZl
cm9sbC9zaW1wc29uLWRldnRlc3Qtc29uLWRldnRlc3Qtc29uLWRldnRlc3Qtc29uLWRldn
XGNpc2NvLWw4ajZvaHBuclxDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZlYDZl
LUNBLmNybDAQBgkrBgEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAANBACBqelwY
YjalelGZqLVu4bdVMF06ELCV2AMBgi41K3ix+Z/03PJd7ct2BIAF41ktv9pCe6IO
EoBcmZteA+TQcKg=
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
Fingerprint:AC6FC55E CC29E891 0DC3FAAA B4747C10
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```


4. 証明書の情報を表示します (任意)

```
webvpn# show crypto pki certificates tp-proxy1
Certificate
  Status:Available
  Certificate Serial Number:04A0147B00000000010E
  Certificate Usage:General Purpose
  Issuer:
    CN = sub3ca
    C = US
  Subject:
    Name:ssl-proxy.
    Serial Number:B0FFF0C2
    OID.1.2.840.113549.1.9.2 = ssl-proxy.
    OID.2.5.4.5 = B0FFF0C2
  CRL Distribution Point:
    http://sample.cisco.com/sub3ca.crl
  Validity Date:
    start date:18:04:09 UTC Jan 23 2003
    end   date:21:05:17 UTC Dec 12 2003
    renew date:00:00:00 UTC Apr 1 2003
  Associated Trustpoints:tp-proxy1

CA Certificate
  Status:Available
  Certificate Serial Number:6D1E6B0F000000000007
  Certificate Usage:Signature
  Issuer:
    CN = subtest
    C = US
  Subject:
    CN = sub3ca
    C = US
  CRL Distribution Point:
    http://sample.cisco.com/subtest.crl
  Validity Date:
    start date:22:22:52 UTC Mar 28 2003
    end   date:21:05:17 UTC Dec 12 2003
  Associated Trustpoints:tp-proxy1

webvpn# show crypto pki certificates 3tier-subcal
CA Certificate
  Status:Available
  Certificate Serial Number:29A47DEF0000000004E9
  Certificate Usage:Signature
  Issuer:
    CN = 6ebf9b3e-9a6d-4400-893c-dd85dcfe911b
    C = US
  Subject:
    CN = subtest
    C = US
  CRL Distribution Point:
    http://sample.cisco.com/6ebf9b3e-9a6d-4400-893c-dd85dcfe911b.crl
  Validity Date:
    start date:20:55:17 UTC Dec 12 2002
    end   date:21:05:17 UTC Dec 12 2003
  Associated Trustpoints:3tier-sub1

webvpn# show crypto pki certificates 3tier-root
CA Certificate
  Status:Available
  Certificate Serial Number:7FD5B209B5C2448C47F77F140625D265
  Certificate Usage:Signature
  Issuer:
    CN = 6ebf9b3e-9a6d-4400-893c-dd85dcfe911b
    C = US
  Subject:
    CN = 6ebf9b3e-9a6d-4400-893c-dd85dcfe911b
    C = US
```

```

CRL Distribution Point:
  http://sample.cisco.com/6ebf9b3e-9a6d-4400-893c-dd85dcfe911b.crl
Validity Date:
  start date:00:05:32 UTC Jun 13 2002
  end   date:00:11:58 UTC Jun 13 2004
Associated Trustpoints:3tier-root

```

証明書およびトラストポイントの確認

証明書およびトラストポイントの情報を確認するには、EXEC モードで、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(ca-trustpoint)# show crypto pki certificates [trustpoint_label]</code>	指定したトラストポイントに関連する証明書の情報を表示するか、またはすべての証明書、認証局の証明書、および Registration Authority (RA; 登録局) の証明書を表示します。
ステップ 2	<code>webvpn(ca-trustpoint)# show crypto pki trustpoints [trustpoint_label]</code>	すべてのトラストポイントまたは指定したトラストポイントの情報を表示します。

鍵および証明書の共有

WebVPN サービス モジュール では、複数の証明書で同じ鍵ペアを共有できます。ただし、1 つの鍵ペアに問題が生じた場合、すべての証明書を失効し、交換する必要があるため、推奨する方法ではありません。

WebVPN のゲートウェイは、さまざまな時点で追加および削除されるので、証明書もさまざまな時点で期限切れになります。認証局によっては、更新時に鍵ペアを新しくするよう要求されます。複数の証明書が 1 つの鍵ペアを共有している場合、これらの証明書を同時に更新する必要があります。一般的に、各証明書に独自の鍵ペアを設定するほうが、証明書の管理は容易です。

WebVPN サービス モジュール には、複数の WebVPN ゲートウェイおよび複数の WebVPN サービス モジュール で証明書を共有することに対して、特に制約はありません。同じトラストポイントを複数の WebVPN ゲートウェイに割り当てることができます。

業務上の観点では、認証局により制約が課されることがあります (サーバファーム内で同じ証明書を共有できるサーバ数など)。証明書の共有に関して、契約上またはライセンス上の同意が必要になることもあります。業務上の契約に関しては、認証局または法務部門の担当者に問い合わせてください。

実際には、一部の Web ブラウザは、サーバの証明書のサブジェクト名と、URL に表示されるホスト名または IP アドレスを比較します。サブジェクト名がホスト名または IP アドレスと一致しない場合、ユーザに証明書の受け入れを確認するように要求するダイアログボックスが表示されます。このプロセスを回避するには、ホスト名または IP アドレスに基づく証明書の共有を制限してください。

コンフィギュレーションの保存



注意

RSA 鍵ペアは、NVRAM だけに保存されます。 `copy system:running-config file_system:` コマンドで他のファイルシステムを指定した場合、RSA 鍵はコンフィギュレーションに保存されません。

コンフィギュレーションを変更した場合には、必ず作業内容を保存してください。

コンフィギュレーションを NVRAM に保存するには、次の作業を行います。

コマンド	目的
<pre>webvpn# copy [/erase] system:running-config nvrram:startup-config</pre>	<p>コンフィギュレーション、鍵ペア、および証明書を NVRAM に保存します。鍵ペアはプライベート コンフィギュレーション ファイルに保存され、各証明書はバイナリ ファイルとして NVRAM に保存されます。モジュールは起動時に、証明書を取得したり自動登録を行うために認証局にクエリを送信する必要はありません。</p> <p> (注) セキュリティ上の理由から、NVRAM を更新する場合には、事前に /erase オプションを入力して、パブリック コンフィギュレーション ファイルおよびプライベート コンフィギュレーション ファイルを消去することを推奨します。/erase オプションを入力しないと、古いプライベート コンフィギュレーション ファイルの鍵ペアの情報が NVRAM に残る場合があります。</p> <p> 注意 /erase オプションを入力すると、実行コンフィギュレーションを NVRAM に保存する前に、NVRAM に保存されている現在およびバックアップの両方のバッファが消去されます。バッファを消去したあと、実行コンフィギュレーションを保存する前に電力障害またはリブートが発生すると、両方のコンフィギュレーションが失われることがあります。</p>



(注)

NVRAM に多数のファイルが保存されている場合、この作業が完了するまでに 2 分程かかることがあります。

NVRAM へのコンフィギュレーションの自動バックアップ機能により、最後に保存したコンフィギュレーションが自動的にバックアップされます。現在の書き込み処理に失敗した場合、自動的に前のコンフィギュレーションが復元されます。

保存したコンフィギュレーションの確認

保存したコンフィギュレーションを確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	webvpn# <code>show startup-config</code>	スタートアップ コンフィギュレーションを表示します。
ステップ 2	webvpn# <code>directory nvram:</code>	NVRAM に保存されているファイルの名前およびサイズを表示します。

保存したコンフィギュレーションの消去

保存したコンフィギュレーションを消去するには、次のいずれかの作業を行います。

	コマンド	目的
	webvpn# <code>erase nvram:</code>	スタートアップ コンフィギュレーションおよび鍵ペアを消去します。
	webvpn# <code>erase /all nvram:</code>	スタートアップ コンフィギュレーション、鍵ペア、証明書、および他のすべてのファイルを NVRAM から消去します。



(注)

NVRAM に多数のファイルが保存されている場合、この作業が完了するまでに 2 分程かかることがあります。



注意

保存したコンフィギュレーションを消去すると、自動バックアップされたコンフィギュレーションも NVRAM から消去されます。

鍵および証明書のバックアップ

鍵および証明書の NVRAM への保存処理を中断するイベント（電力障害など）が発生すると、保存処理中の鍵および証明書が失われることがあります。公開鍵および証明書は、認証局から取得できます。ただし、秘密鍵を回復することはできません。

セキュア サーバを使用できる場合には、各トラストポイントを PKCS12 ファイルにエクスポートすることによって、鍵ペアおよび関連する証明書をバックアップしてください。PKCS12 ファイルをインポートすれば、鍵および証明書を回復できます。

セキュリティ上のガイドライン

鍵および証明書をバックアップする場合には、次のガイドラインに従ってください。

- 各 PKCS12 について、簡単に推測できないパス フレーズを選択し、パス フレーズを十分に保護する必要があります。PKCS12 ファイルは、クリア形式では保存しないでください。
- バックアップ サーバは、セキュアでなければなりません。バックアップ サーバへのアクセスは、許可された人物だけに制限してください。
- (パス フレーズの入力が必要である) PKCS12 ファイルをインポートまたはエクスポートする場合には、モジュールのコンソールに直接接続するか、SSH セッションを使用してください。
- ファイル転送には、SCP を使用してください。

鍵および証明書のモニタおよびメンテナンス

ここでは、次の任意の作業について説明します。

- WebVPN サービス モジュールからの RSA 鍵の削除 (p.3-57)
- 鍵および証明書の表示 (p.3-57)
- コンフィギュレーションからの証明書の削除 (p.3-58)

WebVPN サービス モジュールからの RSA 鍵の削除



注意

SSH 鍵を削除すると、WebVPN サービス モジュール上の SSH がディセーブルになります。SSH 鍵を削除する場合には、新しい鍵を生成してください。「[管理者用の認証の設定](#)」(p.2-5)を参照してください。

特定の状況では、モジュールから RSA 鍵を削除したほうが良い場合があります。たとえば、RSA 鍵に何らかの問題があると考えられ、使用を中止する場合には、その鍵を削除すべきです。

モジュールから RSA 鍵を削除するには、グローバル コンフィギュレーション モードで、次の作業を行います。

コマンド	目的
webvpn(config)# crypto key zeroize rsa [key-label]	すべての RSA 鍵ペアまたは指定した鍵ペアを削除します。
	<p>注意 鍵を削除すると、その鍵に関連するすべての証明書が削除されます。</p>

モジュールから RSA 鍵を削除したあと、次の 2 つの作業を行います。

- 認証局の管理者に、認証局でモジュールの証明書を失効するように依頼します。最初に証明書を取得したときに、**crypto pki enroll** コマンドで作成したモジュールのチャレンジ パスワードを提供する必要があります。
- コンフィギュレーションから手動でトラストポイントを削除します。「[コンフィギュレーションからの証明書の削除](#)」(p.3-58)を参照してください。

鍵および証明書の表示

鍵および証明書を表示するには、次のいずれかの作業を行います。

コマンド	目的
webvpn# show crypto key mypubkey rsa	モジュールの RSA 公開鍵を表示します。
webvpn# show crypto pki certificates [trustpoint_label]	証明書、認証局の証明書、および任意の登録局の証明書に関する情報を表示します。
webvpn# show running-config [brief]	公開鍵および証明書チェーンを表示します。 brief オプションを指定すると、各証明書の 16 進数ダンプは表示されません。

コンフィギュレーションからの証明書の削除

WebVPN サービス モジュール には、自身の証明書および認証局の証明書が保存されています。モジュールに保存されている証明書は削除できます。

モジュールのコンフィギュレーションから証明書を削除するには、グローバル コンフィギュレーション モードで、次の作業を行います。

コマンド	目的
<code>webvpn(config)# no crypto pki trustpoint trustpoint-label</code>	証明書を削除します。

WebVPN のゲートウェイおよびコンテキストへの証明書の割り当て

(`webvpn gateway gateway_name` コマンドを入力後に) `ssl trustpoint trustpoint_label` サブコマンドを入力し、指定した WebVPN ゲートウェイに証明書を割り当てます。ゲートウェイには、`ssl trustpoint` サブコマンドを複数回、入力できます。

トラストポイント ラベルを変更すると、ゲートウェイはその移行中に瞬間的にサービスを中断します。既存の接続は、接続が終了またはクリアされるまで、元の証明書を引き続き使用します。新しい接続は、新しいトラストポイントからの証明書を使用し、サービスが再開されます。

ただし、新しいトラストポイントに証明書がない場合、サービスの運用ステータスはダウンのままになります。新しい証明書を使用できるまで、新しい接続は確立されません。`no ssl trustpoint` サブコマンドを使用して証明書を削除した場合、既存の接続は、接続が終了またはクリアされるまで、その証明書を引き続き使用します。証明書が古くても、すべての接続が終了またはクリアされるまでは、証明書は WebVPN ゲートウェイから排除されません。



(注)

WebVPN ゲートウェイには、生成した自己署名の証明書を割り当ててはできますが、インポートした自己署名の証明書を WebVPN ゲートウェイに割り当ててはできません。インポートした証明書に署名した認証局の鍵ペアは、インポートできないからです。

次に、ゲートウェイにトラストポイントを割り当てる例を示します。

```
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn(config)# webvpn gateway gw1
webvpn(config-webvpn-gateway)# ip address 10.1.1.2
webvpn(config-webvpn-gateway)# ssl trustpoint tp-1
webvpn(config-webvpn-gateway)# end
webvpn#
webvpn# show webvpn gateway gw1
Admin Status: up
Operation Status: up
IP: 10.1.1.2, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: tp-1
Certificate chain for new connections:
Certificate:
  Key Label: tp-1, 1024-bit, not exportable
  Key Timestamp: 12:09:27 UTC Dec 25 2004
  Serial Number: 0FE5
Root CA Certificate:
  Serial Number: 01
rsa-general-purpose certificate
Certificate chain complete

webvpn#
```

次に、WebVPN ゲートウェイのトラストポイントを変更する例を示します。



(注)

既存の接続は、接続が終了するまで、元の証明書を引き続き使用します。サービスの運用ステータスは、アップからダウンに変わり、再びアップに戻ります。新しい接続は、新しい証明書を使用します。

```
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn(config)# webvpn gateway gw1
webvpn(config-webvpn-gateway)# ssl trustpoint tp-2
webvpn(config-webvpn-gateway)# end
webvpn#
webvpn# show webvpn gateway gw1
Admin Status: up
Operation Status: up
IP: 10.1.1.2, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: tp-2
Certificate chain for new connections:
Certificate:
  Key Label: tp-2, 1024-bit, not exportable
  Key Timestamp: 12:09:27 UTC Dec 25 2004
  Serial Number: 0FE5
Root CA Certificate:
  Serial Number: 01
rsa-general-purpose certificate
Certificate chain complete
webvpn#
```

証明書の更新

認証局によっては、証明書を更新するときに新しい鍵ペアの生成を要求しますが、期限切れになった証明書の鍵ペアを使用して証明書を更新できる認証局もあります。WebVPN サービス モジュールは、両方の状況をサポートしています。

SSL サーバの証明書は通常、1 ~ 2 年以内に期限切れになります。証明書のグレースフル ロールオーバーにより、突然のサービス中止を回避できます。

次に、ゲートウェイ gw2 をトラストポイント t2 に割り当てる例を示します。

```
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn(config)# webvpn gateway gw2
webvpn(config-gateway)# ssl trustpoint t2
webvpn(config-gateway)# end
webvpn#

webvpn# show webvpn gateway gw2
Admin Status: up
Operation Status: up
IP: 2.100.100.202, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: t2
Certificate chain for new connections:
Certificate:
  Key Label: k2, 1024-bit, not exportable
  Key Timestamp: 18:38:53 UTC Jan 24 2005
  Serial Number: 67A6
Root CA Certificate:
  Serial Number: 01
rsa-general-purpose certificate
Certificate chain complete
```

次に、トラストポイント t2 の鍵ペアを更新し、古い証明書を Cisco IOS データベースから削除する例を示します。ゲートウェイ gw2 のグレースフル ロールオーバーは、自動的に開始されます。

```
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn(config)# crypto key generate rsa general-keys label k2 exportable
% You already have RSA keys defined named k2.
% Do you really want to replace them? [yes/no]:yes
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
*May 7 17:47:10.718: %WEBVPN-6-PKI_CERT_ROLLOVER_BEGIN: The process of rolling over
the certificate without the sudden loss of services has begun for the proxy service:
gw2, trustpoint: t2
webvpn(config)#end
webvpn# show show webvpn gateway gw2
Admin Status:up
Operation Status:up
IP: 2.100.100.202, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: t2
Certificate chain in graceful rollover, being renewed:
Certificate:
  Key Label:k2 1024-bit, exportable
  Key Timestamp: 17:47:10 UTC May 7 2005
  Serial Number:47AF
Root CA Certificate:
  Serial Number:01
rsa-general-purpose certificate
Server certificate in graceful rollover
```

次に、トラストポイント t2 が再登録されるまで、既存の接続および新しい接続で古い証明書を使用する例を示します。トラストポイント t2 が再登録されると、新しい接続は新しい証明書を使用し、既存の接続は、接続が終了するまで古い証明書を引き続き使用します。

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# crypto pki enroll t2
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will be: CN=2.100.100.202
% The fully-qualified domain name will not be included in the certificate Request
certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

CRYPTO_PKI:   Fingerprint:  36DC4511 CE0353DB A7194317 E2D10481

May  7 18:34:22.967: %PKI-6-CERTRET: Certificate received from Certificate Authority
May  7 18:34:24.195: %WEBVPN-6-PKI_SERVICE_CERT_INSTALL: Proxy: gw2, Trustpoint: t2,
Key: k2, Serial#: 47AF, Index: 4
May  7 18:34:24.203: %WEBVPN-6-PKI_CERT_ROLLOVER_END: The process of rolling over the
certificate without the sudden loss of services has ended for the proxy service: gw2,
trustpoint: t2
webvpn(config)# end

webvpn# show show webvpn gateway gw2
Admin Status: up
Operation Status: up
IP: 2.100.100.202, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: t2
  Obsolete certificate chain for old connections:
    Certificate:
      Key Label: k2, 1024-bit, not exportable
      Key Timestamp: 18:38:53 UTC Jan 24 2005
      Serial Number: 67A6
    Root CA Certificate:
      Serial Number: 01
  Certificate chain for new connections:
    Certificate:
      Key Label: k2, 1024-bit, exportable
      Key Timestamp: 17:47:10 UTC May 7 2005
      Serial Number: 47AF
    Root CA Certificate:
      Serial Number: 01
  rsa-general-purpose certificate
  Certificate chain complete

May 7 18:34:44.191: %WEBVPN-6-PKI_SERVICE_CERT_DELETE: Proxy: gw2, Trustpoint: t2,
Key: k2, Serial#: 67A6, Index: 0
```

次に、すべての既存の接続が終了したあとで、古い証明書が削除された例を示します。

```
webvpn# show show webvpn gateway gw2
IP: 2.100.100.202, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: t2
Certificate chain for new connections:
Certificate:
  Key Label: k2, 1024-bit, exportable
  Key Timestamp: 17:47:10 UTC May 7 2005
  Serial Number: 47AF
Root CA Certificate:
  Serial Number: 01
rsa-general-purpose certificate
Certificate chain complete
```

証明書の自動更新および自動登録

自動登録を設定すると、WebVPN サービス モジュール は、コンフィギュレーションのパラメータに基づいて、認証局に自動的に証明書をリクエストします。



有効期間の特定の割合が経過したあと、証明書が自動的に更新されるように設定できます。たとえば、証明書の有効期間が 300 日で、*renewal_percent* を 80 に設定した場合、証明書の有効期間の開始日から 240 日が経過した時点で、証明書は自動的に更新されます。



(注)

自動登録または自動更新を行うには、データベースに認証局の証明書が保管されている必要があります。自動登録を設定する前に、トラストポイントを確認します。また、トラストポイントの SCEP 登録 URL を設定します。

自動登録および自動更新をイネーブルにし、タイマー情報を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn(config)# crypto pki trustpoint trustpoint-label</code>	トラストポイントを宣言します。
ステップ 2	<code>webvpn(ca-trustpoint)# auto-enroll {renewal_percent regenerate}</code>	指定したトラストポイントの自動更新および自動登録をイネーブルにします。  (注) <i>renewal_percent</i> の有効値は、0 (1 分以内に登録) ~ 100 です。  (注) regenerate キーワードを指定すると、名前付きの鍵が存在していても、証明書用の新しい鍵が生成されます。
ステップ 3	<code>webvpn# show crypto pki timers</code>	各タイマーが期限切れになるまでの残り時間を表示します。

次に、自動登録および自動更新をイネーブルにする例を示します。

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# crypto pki trustpoint tk21
webvpn(ca-trustpoint)# auto-enroll 90
webvpn(ca-trustpoint)# end
webvpn# show crypto pki timers
PKI Timers
|          44.306
|          44.306  RENEW tp-new
|255d 5:28:32.348  RENEW tk21
webvpn#
```




エンド ユーザ用の WebVPN の設定

この付録は、WebVPN をエンド ユーザ用に設定するシステム管理者を対象にしています。エンド ユーザ リモート システムの設定要件およびタスクの概要について説明します。また、WebVPN の使用を開始できるように、エンド ユーザと通信するための情報を示します。



(注)

エンド ユーザ用に WebVPN を設定する前に、WebVPN サービス モジュール を設定しておく必要があります。

ここでは、次の項目について説明します。

- [WebVPN の起動 \(p.A-2\)](#)
- [ユーザ名およびパスワード \(p.A-3\)](#)
- [エンド ユーザ インターフェイス \(p.A-4\)](#)
- [その他の WebVPN 機能の使用法 \(p.A-15\)](#)
- [セキュリティ上の注意事項 \(p.A-17\)](#)
- [アプリケーション アクセス ホスト ファイル エラーからの回復 \(p.A-18\)](#)

WebVPN の起動

エンドユーザのリモートシステム上で WebVPN を起動するための要件は、次のとおりです。

- インターネットへの接続 以下を含む任意のインターネット接続がサポートされます。
 - 住宅用の DSL、ケーブル、またはダイヤルアップ
 - 公共キオスク
 - ホテルでの接続
 - 空港のワイヤレス ノード
 - インターネット カフェ
- WebVPN 対応ブラウザ 次のブラウザは WebVPN への対応が確認されています。その他のブラウザの場合、WebVPN 機能が完全にサポートされないことがあります。

Microsoft Windows :

- Internet Explorer 6.0 SP1 (Windows XP には SP2 が必要)
- Netscape 7.2

Linux :

- Netscape version 7.2

- クッキー対応 ポート転送によりアプリケーションにアクセスするには、ブラウザ上でクッキーを使用できる必要があります。
- ポップアップ対応 フローティング WebVPN ツールバーおよびタイムアウト警告を表示するには、ブラウザにポップアップを表示できる必要があります。ポップアップが表示されない場合は、ブラウザの設定を変更し、in-page ツールバー上の WebVPN フローティング ツールバーアイコンをクリックして、フローティング ツールバーを表示します。

ブラウザ上でポップアップが無効になっていると、アイドル タイムアウトまたは最大接続時間による切断の前に、エンドユーザに WebVPN の警告が表示されません。

- WebVPN 用の URL 次の形式の HTTPS アドレスを使用します。

`https://address`

`address` は、`https://10.89.192.163` または `https://vpn.company.com` などの WebVPN モジュールのインターフェイスの IP アドレスまたは DNS ホスト名です。

- WebVPN のユーザ名およびパスワード
- (任意) ローカル プリンタ WebVPN は、Web ブラウザからネットワーク プリンタへのプリント出力をサポートしていません。ローカル プリンタへのプリント出力はサポートされます。

ユーザ名およびパスワード

表 A-1 に、WebVPN ユーザに必要なユーザ名とパスワードのタイプを示します。

表 A-1 WebVPN ユーザ用のユーザ名およびパスワード

ログイン ユーザ名/ パスワードのタイプ	目的	入力する状況
コンピュータ	コンピュータへのアクセス	コンピュータの起動時
インターネット プロ バイダー	インターネットへのアクセス	インターネット プロバイダーへの接続 時
WebVPN	リモート ネットワークへのア クセス	WebVPN の起動時
ファイル サーバ	リモート ファイル サーバへの アクセス	WebVPN ファイル ブラウジング機能を使 用してリモート ファイル サーバにア クセスする場合
企業アプリケーション へのログイン	ファイアウォールにより保護さ れた内部サーバへのアクセス	WebVPN の Web ブラウジング機能を使 用して、内部の保護された Web サイトに アクセスする場合
メール サーバ	WebVPN 経由でのリモート メール サーバへのアクセス	E メール メッセージの送受信時

エンドユーザインターフェイス

WebVPN を設定している企業のエンドユーザは、ブラウザを起動して、企業ネットワークがホスティングしている WebVPN ゲートウェイに接続することにより、企業ネットワークにアクセスできます。エンドユーザは、各自のクレデンシャルおよび認証情報を提示し、企業サイトのポータルページ（ホームページ）にアクセスします。ポータルページには、エンドユーザが各自のクレデンシャルに基づいてアクセスできる各種機能（Eメール、Webブラウジングなど）が表示されます。エンドユーザが WebVPN ゲートウェイのすべての機能にアクセスできる場合には、ホームページにすべての機能へのリンクが提供されます。



(注) エンドユーザインターフェイスは、主として HTML インターフェイスです。

次の項目で、エンドユーザインターフェイスについて、より詳細に説明します。

- [ページフロー](#) (p.A-5)
- [初回の接続](#) (p.A-5)
- [ログインページ](#) (p.A-7)
- [証明書の認証](#) (p.A-7)
- [ログアウトページ](#) (p.A-8)
- [ポータルページ](#) (p.A-8)
- [リモートサーバ](#) (p.A-9)
- [DNS および接続エラー](#) (p.A-11)
- [セッションタイムアウト](#) (p.A-12)
- [TCP ポート転送およびアプリケーションアクセス](#) (p.A-12)

ページフロー

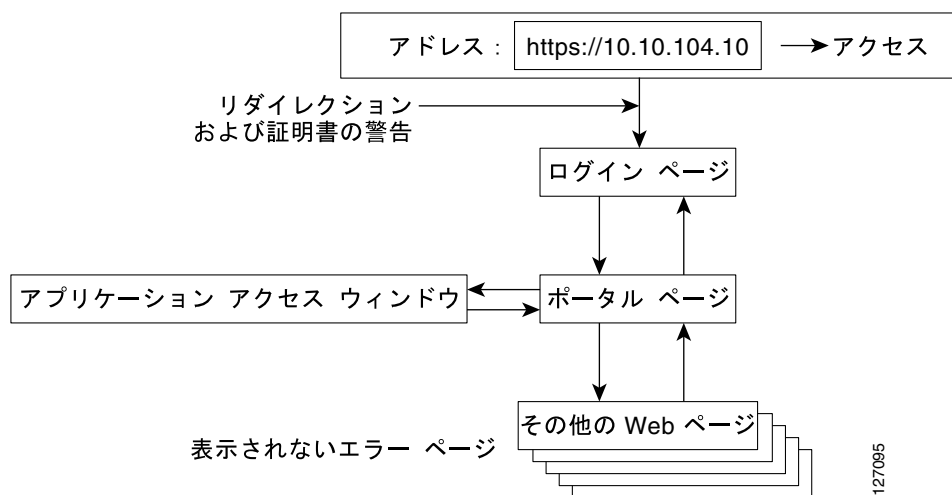
ここでは、WebVPN セッションのページフロー プロセス (図 A-1 を参照) について説明します。エンドユーザが、各自のブラウザに Hypertext Transfer Protocol Secure(HTTPS)URL(`https://address`)を入力すると、エンドユーザは、ログイン ページのある `https://address/index.html` にリダイレクトされます。



(注)

ブラウザの設定によっては、このリダイレクションによって、エンドユーザのブラウザに、セキュアな接続にリダイレクトされていることを示す警告が表示されることがあります。

図 A-1 ページフロー



初回の接続

エンドユーザの初回の接続では、次のいずれかの状況が発生することがあります。

- [503 Service Unavailable メッセージ \(p.A-5 \)](#)
- [Out of Service ページ \(p.A-6 \)](#)
- [SSL/TLS 証明書 \(p.A-6 \)](#)

503 Service Unavailable メッセージ

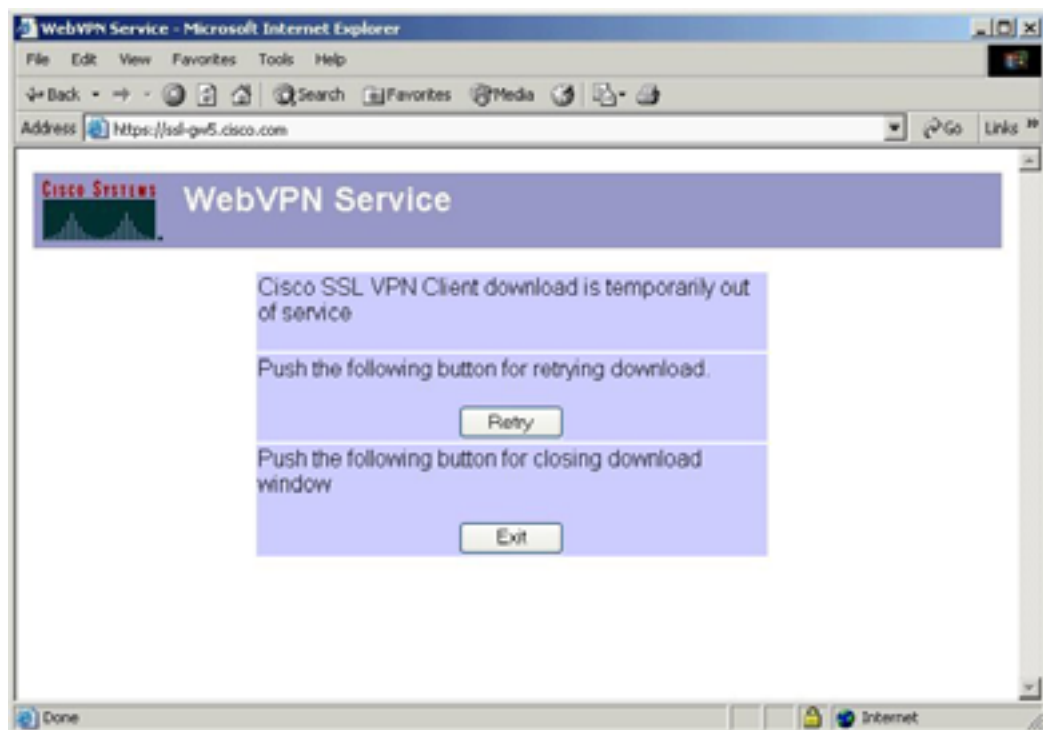
モジュールのトラフィック負荷が大きい場合、エンドユーザに「503 Service Unavailable」メッセージが表示されることがあります。このメッセージを受信したエンドユーザは、以降で、再び接続を試みる必要があります。

Out of Service ページ

エンドユーザが SSL VPN Client (SVC) のダウンロードを試みたときに、SVC バイナリが保管されているファイルシステムが、一時的にサービス停止になっていることがあります。この場合には、エンドユーザのブラウザに Out of Service ページ (図 A-2 を参照) が表示されます。Out of Service ページには、ダウンロードの再試行またはプロセスの終了を問い合わせるプロンプトが表示されます。

ほとんどの場合、エンドユーザが Retry ボタンをクリックすると、SVC を正常にダウンロードできます。ただし、ゲートウェイの応答が引き続き Out of Service ページだった場合には、エンドユーザは、プロセスを終了し、ゲートウェイ管理者にエラーを報告する必要があります。

図 A-2 Out of Service ページ



SSL/TLS 証明書

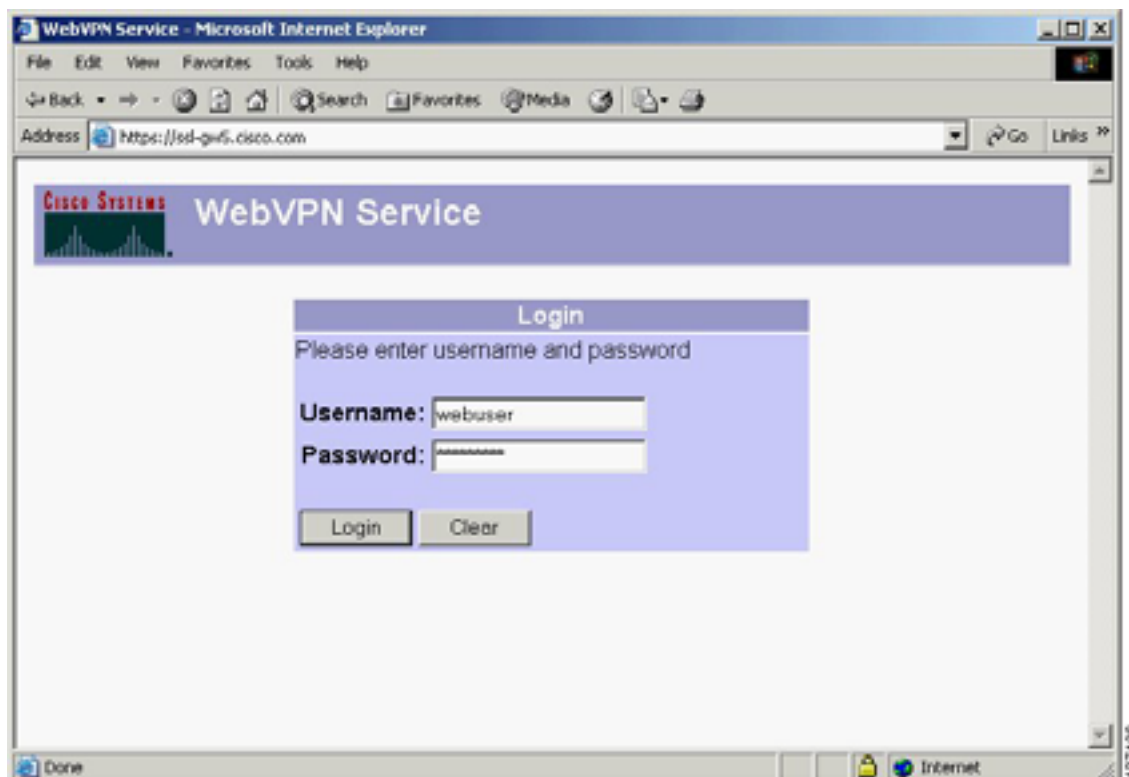
HTTPS 接続を確立したとき、SSL/TLS 証明書に関する警告が表示されることがあります。この警告が表示された場合、エンドユーザは、この証明書をインストールする必要があります。警告が表示されない場合には、ブラウザを信頼する証明書がすでにシステムに存在しています。

エンドユーザは、ログインページに接続します。

ログイン ページ

ログイン ページ (図 A-3 を参照) には、エンド ユーザにユーザ名およびパスワードの入力を要求するプロンプトが表示されます。エンド ユーザおよびパスワードは、HTML フォームに入力されます。認証に失敗すると、ログイン ページにエラー メッセージが表示されます。

図 A-3 デフォルトのログイン ページ



ログイン ページは、管理者によってカスタマイズされたロゴ、タイトル、メッセージ、カラーで表示されます。

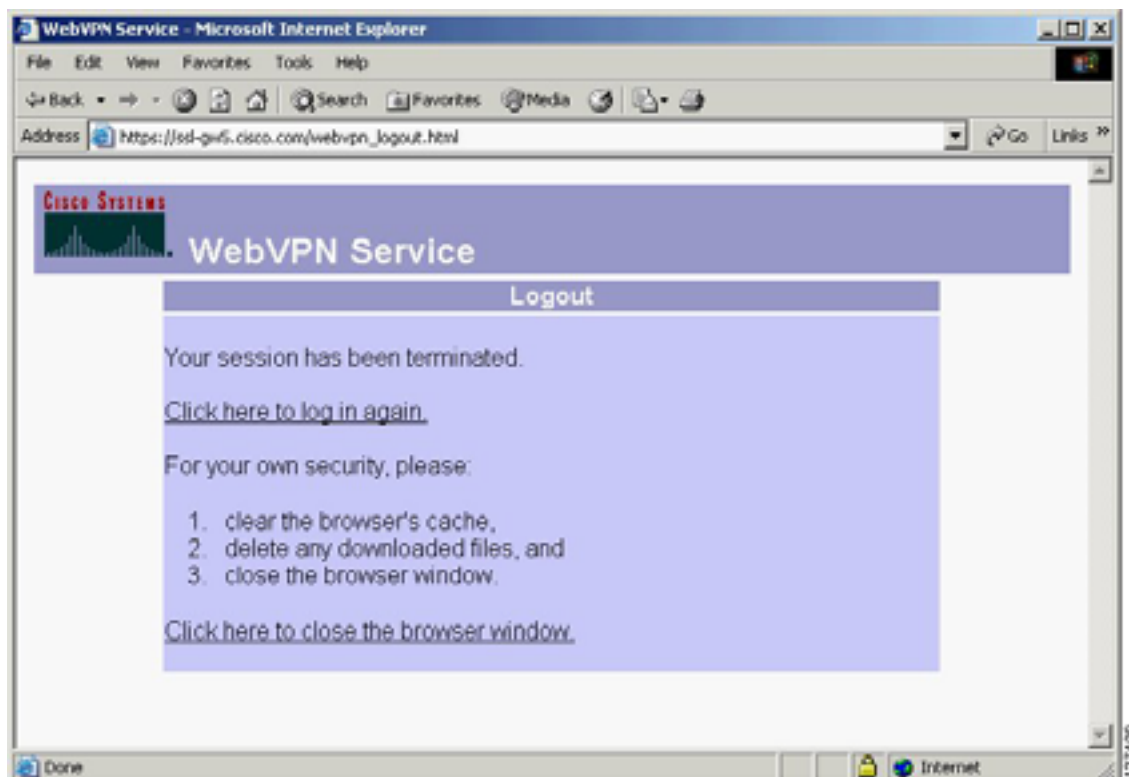
証明書認証

クライアントの証明書認証は、サポートされません。ユーザ名およびパスワードの認証だけがサポートされます。

ログアウト ページ

ログアウト ページ (図 A-4 を参照) は、エンドユーザがログアウトのリンクをクリックしたとき、またはアイドル タイムアウトまたは最大接続時間の経過によりセッションが終了したときに表示されます。

図 A-4 ログアウト ページ



ポータル ページ

ポータル ページ (図 A-5 を参照) は、WebVPN 機能のメイン ページです。このページはカスタマイズすることができ、次の内容を表示できます。

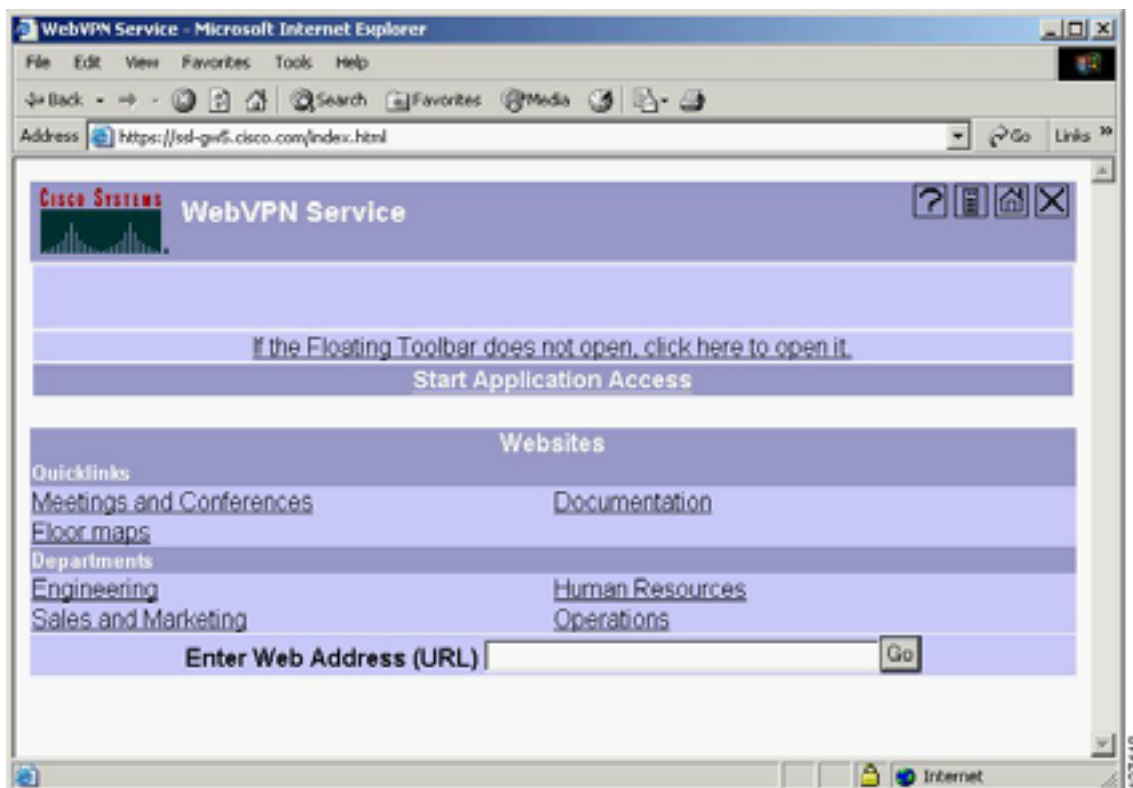
- カスタム ロゴ (デフォルトは、シスコ社のブリッジ ロゴ)
- カスタム タイトル (デフォルトは、「WebVPN Service」)
- カスタム パナー (デフォルトは空白ストリング)
- カスタム カラー (デフォルトはホワイトとパープルの組み合わせ)
- Web サーバ リンクのリスト (カスタマイズ可能)
- URL 入力ボックス (常時表示)
- アプリケーション アクセス リンク (常時表示)
- ヘルプ、ホーム (このポータル ページ) およびログアウトのアイコン リンク
- ポップアップ、フローティング ツールバーへのリンク

設定されていない項目は、ポータル ページに表示されません。



(注) シンクライアントモードでは、アプリケーション アクセス リンクを使用してダウンロードする Eメール アクセスがサポートされます。

図 A-5 ポータル ページ



リモート サーバ

エンドユーザは、ポータルページ上のテキストボックスまたはフローティングツールバーのテキストボックスに、アクセスしたい Web サイトのアドレスまたは URL パスを入力できます。リモートサーバからのページは、ブラウザのウィンドウに表示されます。エンドユーザは、ページ上の他のリンクを使用できます。

図 A-6 に、標準的な Web サイトのポータルページを示します。フローティングツールバー(図 A-7 を参照)のホーム アイコン ボタンをクリックすると、エンドユーザはポータルページに戻ります。

図 A-6 Web サイトとツールバー



WebVPN フローティング ツールバー

フローティング ツールバー (図 A-7 を参照) により、メイン ブラウザ ウィンドウを表示したまま、URL を入力し、ファイルの場所を検索し、設定済みの Web 接続を選択できます。

フローティング ツールバーは、WebVPN セッションを表示します。エンド ユーザがウィンドウの「閉じる」ボタンをクリックすると、WebVPN モジュールにより、セッションを終了することを確認するプロンプトが表示されます。



(注)

Hotmail.com および CNN.com などの特定の Web ページの表示中にホーム アイコンをクリックすると、新しいブラウザ ウィンドウが表示されます。これらのサイトの動作の一環として、WebVPN ブラウザ ウィンドウの名前が変更されているからです。



ヒント

テキストをテキスト フィールドにペーストするには、Ctrl-V を押します。WebVPN ツールバーでは、右クリックはディセーブルです。

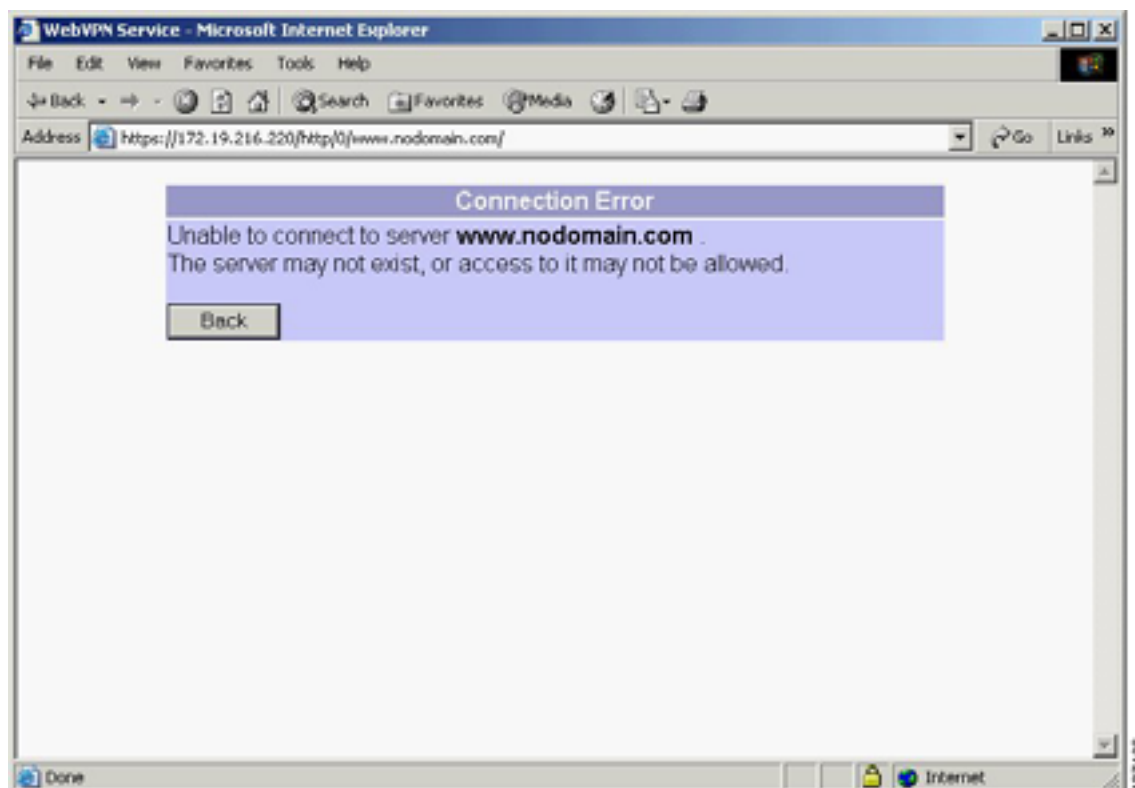
図 A-7 フローティングツールバー



DNS および接続エラー

エンドユーザが、Domain Name System (DNS; ドメインネームシステム) または他の接続エラーにより、接続できないリモートサーバを指定すると、エラーが表示されます (図 A-8 を参照)。TCP のタイムアウトにより、エンドユーザに接続エラーが戻されるまでに、しばらくかかることがあります。

図 A-8 DNS エラー



セッション タイムアウト

無動作によりセッションが終了する場合、エンドユーザに対して約 1 分前に警告が表示され、セッション終了時にも別の警告が表示されます (図 A-9 を参照)。また、メッセージの表示時刻を示すために、ワークステーションのローカル時刻が表示されます。

最初のメッセージは、次のような内容です。

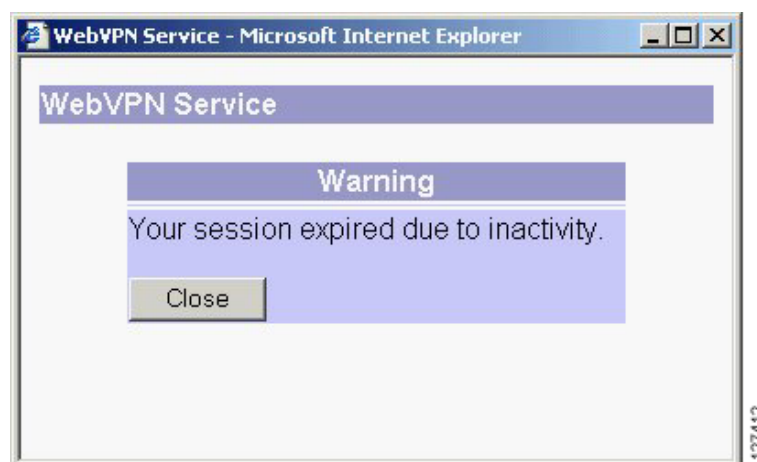
- 「無動作により、 x 秒以内にセッションが終了します。無動作タイマーをリセットする場合には、[Close] をクリックしてください。(ブラウザの時刻および日付)」

アイドル警告メッセージの [Close] ボタンをクリックすると、無動作タイマーがリセットされます。

次の終了メッセージには、(セッション終了の理由が既知かどうかにより) タイムアウトの時刻が表示されます。

- 「無動作のため、セッションが終了しました」

図 A-9 無動作またはタイムアウトによるセッション終了ウィンドウ



TCP ポート転送およびアプリケーション アクセス



(注) この機能は、SSL 接続を適正にサポートするために、Java 1.4 Java Virtual Machine (JTM) を必要とします。



(注) この機能は、JRE をインストールしてローカルクライアントを設定する必要があり、ローカルシステム上での管理者の許可が必要になるので、エンドユーザが公共リモートシステムから接続している場合には、ほとんどの場合、アプリケーションを使用できません。

エンドユーザがアプリケーション アクセス リンクをクリックすると、新しいウィンドウが表示されます。このウィンドウにより、ポート転送アプレットのダウンロードが開始されます。さらに、別のウィンドウが表示されます。このウィンドウは、エンドユーザに、アプレットが署名されている証明書を確認するように要求します。エンドユーザが証明書を受け入れると、アプレットが起動し、ポート転送エントリが表示されます（図 A-10 を参照）。また、アクティブな接続数および送受信バイト数がウィンドウにリストされます。



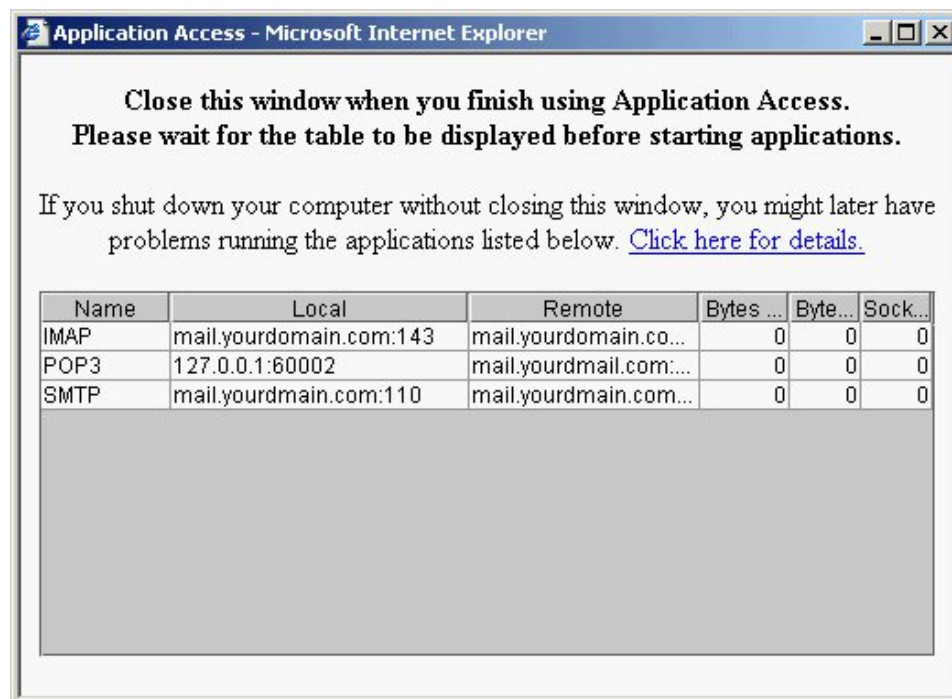
(注)

エンドユーザがアプリケーション アクセスを起動すると、システムによってはデジタル証明書に関するダイアログボックスが表示されることがあります。また、このダイアログボックスは、他のブラウザ ウィンドウの背後に表示されることもあります。エンドユーザの接続が保留されているようであれば、エンドユーザにブラウザのウィンドウを最小化して、このダイアログボックスを確認するように通知してください。

E メールサーバには、IP アドレス、DNS 名、およびポート番号が設定されている必要があります。エンドユーザは、E メールサーバと通信して E メールを送受信する E メールクライアントを起動できます。Point of Presence3 (POP3)、Internet Message Access Protocol (IMAP)、および Simple Mail Transfer Protocol (SMTP) プロトコルがサポートされます。

エンドユーザが JavaScript を使用してログアウトすると、ウィンドウは自動的に閉じます。セッションが終了してから、新しいポート転送接続が確立されると、アプレットによりエラーメッセージが表示されます。

図 A-10 TCP ポート転送ページ



**注意**

アプリケーションの使用が終了したら、[閉じる] アイコンをクリックして、必ずアプリケーション アクセス ウィンドウを閉じるようにユーザに通知する必要があります。ウィンドウが適正に終了されなかった場合、アプリケーション アクセスまたはアプリケーションが使用不可になることがあります。詳細については、「[アプリケーション アクセス ホスト ファイル エラーからの回復](#)」(p.A-18)を参照してください。

表 A-2 に、エンドユーザのリモートシステム上でのアプリケーション アクセス (ポート転送) の要件を示します。


表 A-2 WebVPN リモートシステム アプリケーション アクセスの要件

リモートシステムまたはエンドユーザの要件	仕様または使用上の推奨
クライアント アプリケーションがインストールされている	—
ブラウザがクッキー対応である	—
管理者権限	エンドユーザは、各自の PC のローカル管理者である必要があります。
Sun Microsystems Java Runtime Environment (JRE) version 1.4 以上がインストールされている	エンドユーザがアプリケーション アクセスを開始すると、WebVPN は自動的に JRE をチェックします。JRE をインストールする必要がある場合、エンドユーザに JRE を入手できるサイトを示すポップアップウィンドウが表示されます。
必要に応じて、クライアント アプリケーションが設定されている	クライアント アプリケーションを設定するには、サーバがローカルにマッピングした IP アドレスとポート番号を使用します。この情報は、次の方法で取得します。
 (注) Microsoft Outlook クライアントの場合、この設定は不要です。	<ol style="list-style-type: none"> 1. リモートシステムで WebVPN を起動し、WebVPN ホームページ上のアプリケーション アクセス リンクをクリックします。アプリケーション アクセス ウィンドウが表示されます。 2. Name カラムで、使用するサーバの名前を検索し、(Local カラムで) 対応するクライアントの IP アドレスおよびポート番号を確認します。 3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、各クライアント アプリケーションによって異なります。
Windows XP SP2 パッチ	Windows XP SP2 を実行しているエンドユーザは、次のアドレスから入手できる Microsoft のパッチをインストールする必要があります。 http://support.microsoft.com/?kbid=884020 これは、Microsoft の既知の問題です。

その他の WebVPN 機能の使用法


表 A-3 に、各種の WebVPN 機能の要件を示します。

表 A-3 WebVPN リモート システムの設定およびエンド ユーザの要件

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨
Web ブラウジング	保護された Web サイト用のユーザ名およびパスワード	WebVPN を使用しても、すべてのサイトとの安全な通信を確保できるわけではありません。「 セキュリティ上の注意事項 」(p.A-17)を参照してください。
		<p>WebVPN での Web ブラウジングの画面表示は、ユーザが慣れているものと異なることがあります。たとえば、WebVPN を使用した場合、次のようになります。</p> <ul style="list-style-type: none"> 各 Web ページの上部に WebVPN のタイトルバーが表示されます。 Web サイトには、次の方法でアクセスします。 <ul style="list-style-type: none"> WebVPN ホームページ上の Enter Web Address フィールドに URL を入力します。 WebVPN ホームページ上に設定されている Web サイトリンクをクリックします。 上記のいずれかの方法でアクセスした Web ページ上のリンクをクリックします。 <p>また、特定のアカウントの設定方法によって、次の結果が生じることがあります。</p> <ul style="list-style-type: none"> 一部の Web サイトがブロックされます。 WebVPN ホームページ上にリンク表示されている Web サイトだけを使用できます。
ネットワーク ブラウジング およびファイル管理	共有リモート アクセス用に設定されたファイル許可	WebVPN でアクセスできるのは、共有フォルダおよび共有ファイルだけです。
	保護されたファイル サーバのサーバ名およびパスワード	
	フォルダおよびファイルがあるドメイン名、ワークグループ名、およびサーバ名	ユーザは、企業ネットワーク上のファイルの場所の検索に慣れていないことがあります。
	 (注) コピーの実行中は、Copy File to Server コマンドを中断したり、別のスクリーンに移動しないでください。操作を妨害すると、サーバに不完全なファイルが保存される原因になります。	

■ その他の WebVPN 機能の使用方法

表 A-3 WebVPN リモート システムの設定およびエンド ユーザの要件 (続き)

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨
Eメールの使用: アプリケーション アクセス	アプリケーション アクセスの要件に準拠 (「TCP ポート転送およびアプリケーション アクセス」 [p.A-12] を参照)	Eメールを使用するには、WebVPN ホームページからアプリケーション アクセスを開始します。Eメールクライアントを使用できるようになります。
	 (注) エンド ユーザが IMAP クライアントを使用し、Eメール サーバとの接続が失われたり、新しい接続を開始できない場合、エンド ユーザは IMAP アプリケーションを終了し、WebVPN を再起動する必要があります。	
	その他のメール クライアント	シスコでは、Microsoft Outlook Express version 5.5 および 6.0 をテスト済みです。 WebVPN は、Netscape Mail、Lotus Notes、Eudora など、他の SMTPS、POP3S、または IMAP4S Eメール プログラムをサポートできるはずですが、シスコでは動作確認をしていません。
Eメールの使用: Web アクセス	Web ベースの Eメール製品のインストール	サポートされる製品 : <ul style="list-style-type: none">Outlook Web Access(OWA)5.5、2000、および 2003 Netscape、Mozilla、Internet Explorer は、OWA 5.5 および 2000 でサポートされます。 Internet Explorer 6.0 以上には、OWA 2003 が必要です。Netscape および Mozilla は、OWA 2003 ではサポートされません。 <ul style="list-style-type: none">Lotus iNotes その他の Web ベース Eメール製品も動作するはずですが、シスコでは確認していません。
WebVPN フローティング ツールバーの使用	ほとんどのプラットフォームに PocketPC が必要	テキストをテキスト フィールドにペーストするには、Ctrl-V を押します。フローティング ツールバーでは、右クリックはディセーブルです。
Cisco SSL VPN Client(SVC) の使用		Windows Event Viewer を使用して SVC ログ メッセージを検索するには、Windows で、Program Files > Administrative Tools > Event Viewer を選択します。
Secure Desktop Manager の使用	Secure Desktop Manager のサポート対象ブラウザ	Microsoft Windows : <ul style="list-style-type: none">Internet Explorer version 6.0Netscape version 7.2 Linux : <ul style="list-style-type: none">Netscape version 7.2
Cache Cleaner または Secure Desktop の使用	Cisco Secure Desktop のサポート対象ブラウザ	Secure Desktop Manager のすべてのサポート対象ブラウザ

セキュリティ上の注意事項

エンドユーザには、WebVPN セッションの終了後、必ずログアウトするように通知してください（WebVPN からログアウトするには、WebVPN ツールバー上のログアウト アイコンをクリックするか、ブラウザを終了します）。

エンドユーザに、WebVPN を使用しても、すべてのサイトと安全に通信できるわけではないことを通知してください。WebVPN は、リモート エンドユーザの PC またはワークステーションと、企業ネットワーク上の WebVPN モジュール間のデータ転送のセキュリティを確保します。エンドユーザが（インターネットまたは内部ネットワーク上の）HTTPS 以外の Web リソースにアクセスした場合、企業の WebVPN モジュールと宛先 Web サーバ間の通信は、セキュアではありません。

ブラウザ キャッシングとセキュリティの関係

エンドユーザが、インターネット カフェまたはキオスクなどの公共または共有のインターネット システムから WebVPN を使用する場合、WebVPN セッションの終了後またはログアウト後に情報のセキュリティを確保するには、エンドユーザが WebVPN セッション中に PC に保存した全ファイルを削除する必要があります。これらのファイルは、切断しても自動的に削除されません。



(注)

WebVPN は、セッション中に表示した Web ページのコンテンツを保存しません。ただし、セキュリティを強化するために、エンドユーザはブラウザのキャッシュも消去することを推奨します。PC からコンテンツを削除しても、回復できないとは限りません。重要なデータをダウンロードするときは、十分に注意してください。

アプリケーション アクセス ホスト ファイル エラーからの回復

エンドユーザに、「閉じる」アイコンをクリックしてアプリケーション アクセス ウィンドウを正しく終了するように通知することは、非常に重要です。ウィンドウを正しく終了しない場合、次の状態が発生することがあります。

- エンドユーザが次にアプリケーション アクセスを起動しようとしたとき、ディセーブルになり、「Backup HOSTS File Found」エラーメッセージが表示されます。
- エンドユーザがローカルに実行しても、アプリケーションが使用不可または異常動作になります。

これらのエラーは、エンドユーザが、次のような不適切な方法でアプリケーション アクセス ウィンドウを終了した場合に発生します。

- アプリケーション アクセスの使用中にブラウザがクラッシュした
- アプリケーション アクセスの使用中に電力障害またはシステム シャットダウンが発生した
- アプリケーション アクセス ウィンドウを最小化し、ウィンドウが（最小化されていても）アクティブな状態でコンピュータをシャットダウンした

WebVPN でのホスト ファイルの使用

エンドユーザシステム上のホスト ファイルは、IP アドレスをホスト名にマッピングします。エンドユーザがアプリケーション アクセスを起動すると、WebVPN は、WebVPN 特定のエントリを追加することにより、ホスト ファイルを書き換えます。アプリケーション アクセス ウィンドウを正しく終了し、エンドユーザがアプリケーション アクセスを停止すると、WebVPN はホスト ファイルを元の状態に戻します。ホスト ファイルのステータスは、次のように変化します。

- アプリケーション アクセスの起動前は、ホスト ファイルは元のステートです。
- アプリケーション アクセスが起動すると、WebVPN は以下を実行します。
 - a. ホスト ファイルを `hosts.webvpn` にコピーし、バックアップを作成します。
 - b. ホスト ファイルを編集し、WebVPN 特定情報を挿入します。
- アプリケーション アクセスが停止すると、WebVPN は以下を実行します。
 - a. バックアップ ファイルをホスト ファイルにコピーし、ホスト ファイルを元のステートに復元します。
 - b. `hosts.webvpn` を削除します。
- アプリケーション アクセスの終了後、ホスト ファイルは元のステートです。

エンドユーザがアプリケーション アクセスを不適切に終了した場合

エンドユーザがアプリケーション アクセスを不適切に終了すると、ホスト ファイルは、WebVPN カスタム ステートのまま存続します。WebVPN は、エンドユーザが次にアプリケーション アクセスを起動したときに、`hosts.webvpn` ファイルを検索し、この状態になっていないかどうかをチェックします。WebVPN により、ファイルが検出された場合、エンドユーザに「Backup HOSTS File Found」エラーメッセージが表示され、アプリケーション アクセスは一時的にディセーブルになります。

エンド ユーザーがアプリケーション アクセスを不適切な方法でシャットダウンした場合、リモート アクセス クライアント / サーバ アプリケーションは、保留状態になります。エンド ユーザーが、これらのアプリケーションを、WebVPN を使用せずに起動しようとする、アプリケーションは正常に動作しません。エンド ユーザーは、通常使用しているホストに接続できません。たとえば、エンド ユーザーが自宅からリモートでアプリケーションを実行し、アプリケーション アクセス ウィンドウを閉じないでコンピュータをシャットダウンし、次にオフィスからアプリケーションを実行しようとした場合、この状況が発生します。

対処方法

アプリケーション アクセスまたは正常に動作しないアプリケーションを回復する場合、エンド ユーザーは、次のように対処する必要があります。

- エンド ユーザーがリモート アクセス サーバに接続できる場合、「[WebVPN でのホスト ファイルの自動再設定](#)」(p.A-19)の手順に従います。
- エンド ユーザーが現在のロケーションからリモート アクセス サーバに接続できない場合、またはホスト ファイルをカスタム編集している場合には、「[ホスト ファイルの手動での再設定](#)」(p.A-20)の手順に従います。

WebVPN でのホスト ファイルの自動再設定

エンド ユーザーがリモート アクセス サーバに接続できない場合、次の作業を行ってホスト ファイルを再設定し、アプリケーション アクセスおよびアプリケーションの両方を再イネーブル化する必要があります。

-
- ステップ 1** WebVPN を起動し、ログインします。ポータル ページが表示されます。
- ステップ 2** アプリケーション アクセス リンクをクリックします。「Backup HOSTS File Found」メッセージが表示されます。
- ステップ 3** 次のいずれかのオプションを選択します。
- **バックアップからの復元** WebVPN は、適正なシャットダウンを強制します。WebVPN は hosts.webvpn バックアップ ファイルをホスト ファイルにコピーし、元の状態に復元し、hosts.webvpn を削除します。アプリケーション アクセスを再起動する必要があります。
 - **何もしない** アプリケーション アクセスは起動しません。リモート アクセスのホームページに戻ります。
 - **バックアップの削除** WebVPN は hosts.webvpn ファイルを削除しますが、ホスト ファイルは WebVPN カスタム ステートのまま存続します。ホスト ファイルの元の設定は失われます。次にアプリケーション アクセスを起動すると、WebVPN カスタム ステートが、ホスト ファイルの新しい元の設定として使用されます。このオプションは、ホスト ファイルの設定が失われてもよい場合にのみ、使用してください。アプリケーション アクセスが不適切にシャットダウンされたあと、ホスト ファイルを編集した場合には、別のオプションを選択するか、ホスト ファイルを手動で編集します（「[ホスト ファイルの手動での再設定](#)」[p.A-20] を参照）。
-

ホスト ファイルの手動での再設定

エンドユーザが現在のロケーションからリモート アクセス サーバに接続できない場合、またはエンドユーザがカスタマイズしたホスト ファイルの設定を失いたくない場合には、次の手順を実行して、ホスト ファイルを再設定し、アプリケーション アクセスおよびアプリケーションの両方を再イネーブル化する必要があります。

ステップ 1 ホスト ファイルを検索して、編集します。

ステップ 2 「added by WebVpnPortForward」の文字列を含む行がないかどうかをチェックします。

この文字列を含む行がある場合、ホスト ファイルは WebVPN によりカスタマイズされています。ホスト ファイルがカスタマイズされている場合、次の例のように出力されます。

```
123.0.0.3 server1 # added by WebVpnPortForward
123.0.0.3 server1.example.com vpn3000.com # added by WebVpnPortForward
123.0.0.4 server2 # added by WebVpnPortForward
123.0.0.4 server2.example.com.vpn3000.com # added by WebVpnPortForward
123.0.0.5 server3 # added by WebVpnPortForward
123.0.0.5 server3.example.com vpn3000.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

123.0.0.1      localhost
```

ステップ 3 「added by WebVpnPortForward」の文字列を含む行を削除します。

ステップ 4 ファイルを保存して、終了します。

ステップ 5 WebVPN を起動し、ログインします。ホームページが表示されます。


ステップ 6 アプリケーション アクセス リンクをクリックします。アプリケーション アクセス ウィンドウが表示されます。アプリケーション アクセスはイネーブルです。



組み込まれたテスト証明書のインポート

モジュールの WebVPN ソフトウェアには、テスト用の PKCS12 ファイル (testssl.p12) が組み込まれています。このファイルをフラッシュメモリにインストールして、テストを行ったり、コンセプトを確認できます。PKCS12 ファイルをインストールしたあと、トラストポイントにインポートし、テスト用に設定した WebVPN ゲートウェイに割り当てます。

テスト ファイルをインストールしてインポートするには、次の作業を行います。

	コマンド	目的
ステップ 1	<pre>webvpn# test webvpn platform certificate install</pre>	テスト用の PKCS12 ファイルを NVRAM にインストールします。
ステップ 2	<pre>webvpn# configure terminal</pre>	terminal オプションを選択して、コンフィギュレーション モードを開始します。
ステップ 3	<pre>webvpn(config)# crypto ca import trustpoint_label pkcs12 flash:testssl.p12 passphrase</pre>	テスト用の PKCS12 ファイルをモジュールにインポートします。  (注) テスト証明書の場合、 <i>passphrase</i> は <i>cisco</i> です。
ステップ 4	<pre>webvpn(config)# ssl-proxy service test_service</pre>	テスト用のプロキシ サービスの名前を定義します。
ステップ 5	<pre>webvpn(config-ssl-proxy)# certificate rsa general-purpose trustpoint trustpoint_label</pre>	プロキシ サーバにトラストポイント設定を適用します。
ステップ 6	<pre>webvpn# show ssl-proxy stats test_service</pre>	テスト用の統計情報を表示します。

次に、テスト用の PKCS12 ファイルをインポートする例を示します。

```
webvpn# test webvpn platform certificate install
% Opening file, please wait ...
% Writing, please wait ...
% Please use the following config command to import the file.
  "crypto ca import <trustpoint-name> pkcs12 flash:testssl.p12 cisco"
% Then you can assign the trustpoint to a WebVPN gateway for testing.

*May 5 20:15:57.831: %WEBVPN-6-PKI_TEST_CERT_INSTALL: Test key and certificate was
installed into Flash in a PKCS#12 file.
webvpn#
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn(config)# crypto ca import test123 pkcs12 flash:testssl.p12 cisco
Source filename [testssl.p12]?
% You already have RSA keys named test123.
% If you replace them, all router certs issued using these keys
% will be removed.
% Do you really want to replace them? [yes/no]: yes
RPTO_PKI: Imported PKCS12 file successfully.
webvpn(config)#
*May 5 20:16:25.883: %PKI-6-PKCS12IMPORT_SUCCESS: PKCS #12 Successfully Imported.
webvpn(config)# webvpn gateway test123
webvpn(config-webvpn-gateway)# ip address 2.100.100.77
webvpn(config-webvpn-gateway)# ssl trustpoint test123
*May 5 20:16:43.683: %WEBVPN-6-PKI_SERVICE_CERT_INSTALL: Proxy: test123, Trustpoint:
test123, Key: test123, Serial#: 01, Index: 10
*May 5 20:16:43.683: %WEBVPN-6-PKI_CA_CERT_INSTALL: Root, Subject Name:
cn=testca.cisco.com,ou=Security,o=Cisco Systems Inc,l=San Jose,st=California,c=US,
Serial#: 00, Index: 11
webvpn(config-webvpn-gateway)# inservice
webvpn(config-webvpn-gateway)# exit
webvpn(config)#
*May 5 20:16:46.159: %SSLVPN-5-UPDOWN: sslvpn gateway : test123 changed state to UP
webvpn# show webvpn gateway test123
Admin Status: up
Operation Status: up
IP: 2.100.100.77, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: test123
Certificate chain for new connections:
Certificate:
  Key Label: test123, 1024-bit, not exportable
  Key Timestamp: 20:16:25 UTC May 5 2005
  Serial Number: 01
Root CA Certificate:
  Serial Number: 00
rsa-general-purpose certificate
Certificate chain complete
webvpn#
```



ソフトウェアおよびライセンスのインストール

イメージをコピーするには、TFTP または FTP サーバが必要です。TFTP サーバがスイッチに接続され、TFTP サーバに接続しているポートがスイッチ上のいずれかの VLAN に含まれている必要があります。

ここでは、各種ソフトウェアのインストールまたはアップグレードの手順について説明します。

- [イメージのアップグレード \(p.C-2\)](#)
- [クライアント パッケージのインストール \(p.C-6\)](#)
- [ライセンス アップグレードのインストール \(p.C-10\)](#)

イメージのアップグレード

WebVPN サービス モジュール 上のコンパクト フラッシュには、2つのブータブルパーティションがあります。Application Partition (AP; アプリケーションパーティション) および Maintenance Partition (MP; メンテナンスパーティション) です。デフォルトでは、毎回、AP がブートします。AP には、WebVPN イメージの実行に必要なバイナリが含まれています。MP をブートするのは、AP のアップグレードが必要な場合のみです。

アプリケーション ソフトウェアおよびメンテナンス ソフトウェアの両方をアップグレードできます。ただし、両方のイメージを同時にアップグレードする必要はありません。AP および MP の最新ソフトウェアバージョンは、WebVPN サービス モジュール のリリースノートを参照してください。

完全な AP および MP は、FTP または TFTP サーバに保存されます。どちらのイメージをアップグレードするのに応じて、イメージをダウンロードし、AP または MP に保存します。

AP をアップグレードするには、ブートシーケンスを変更して、MP からモジュールをブートします。MP をアップグレードするには、ブートシーケンスを変更して、AP からモジュールをブートします。モジュールのブートシーケンスは、スーパーバイザエンジンの CLI (コマンドラインインターフェイス) コマンドを使用して設定します。MP は、アプリケーションイメージをダウンロードしてインストールします。MP にネットワークアクセスするには、スーパーバイザエンジンがランタイムイメージを実行している必要があります。

アップグレードを開始する前に、TFTP サーバに、AP イメージまたは MP イメージをダウンロードする必要があります。

ここでは、AP および MP のイメージをアップグレードする手順について説明します。

[アプリケーションソフトウェアのアップグレード \(p.C-2\)](#)

[メンテナンスソフトウェアのアップグレード \(p.C-4\)](#)


アプリケーションソフトウェアのアップグレード




(注)

イメージがアップグレードされるまでは、モジュールをリセットしないでください。イメージのアップグレードには、最大 8 分程かかります。

AP ソフトウェアをアップグレードするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# <code>hw-module module mod reset cf:1</code>	MP からモジュールをリブートします。  (注) このコマンドを入力すると、通常、モジュールのコンソール上に「Press Key」などのメッセージが表示されます。
ステップ 2	Router# <code>show module</code>	モジュールの MP がブートしたことを表示します。
ステップ 3	Router# <code>copy tftp: pcl#mod-fs:</code>	イメージをダウンロードします。

	コマンド	目的
ステップ 4	Router# hw-module module mod reset cf:4	モジュールをリセットし、AP をブートします。  (注) コンソールに「You can now reset the module」メッセージが表示されるまでは、モジュールをリセットしないでください。このメッセージが表示される前にモジュールをリセットすると、アップグレードに失敗することがあります。
ステップ 5	Router# show module	モジュールの AP がブートしたことを表示します。

次に、AP ソフトウェアをアップグレードする例を示します。

```
Router# hw-module module 2 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]y
% reset issued for module 2
supervisor#
16:17:54: SP: The PC in slot 2 is shutting down. Please wait ...
16:18:15: SP: PC shutdown completed for module 2
*May 10 16:50:28.771: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
16:20:54: SP: OS_BOOT_STATUS(2) MP OS Boot Status: finished booting
*May 10 16:53:34.599: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimum Diagnostics...
*May 10 16:53:40.363: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
*May 10 16:53:40.759: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now online
```

```
Router# show module
Mod Ports Card Type Model Serial No.
-----
 1 2 Catalyst 6000 supervisor 2 (Active) WS-X6K-S2U-MSFC2 SAD055006RZ
 2 2 SSL VPN Accelerator (MP) WS-SVC-WEBVPN-K9
```

(テキスト出力は省略)

```
Router# copy tftp: pclc#2-fs:
copy tftp pclc#2-fs:
Address or name of remote host []? 10.10.10.1
Source filename []? c6svc-webvpn-k9y9.1-1-1.bin
Destination filename [c6svc-webvpn-k9y9.1-1-1.bin]?
Accessing tftp://10.10.10.1/c6svc-webvpn-k9y9.1-1-1.bin...
Loading narenr/c6svc-webvpn-k9y9.1-1-1-1.bin from 10.10.10.1 (via Vlan6):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

(テキスト出力は省略)

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 24944624 bytes]

24944624 bytes copied in 203.164 secs (122781 bytes/sec)
supervisor#
*May 10 17:01:40.323: %SVCLC-SP-5-STRRECVD: mod 2: <Application upgrade has started>
*May 10 17:01:40.323: %SVCLC-SP-5-STRRECVD: mod 2: <Do not reset the module till
upgrade completes!!>
*May 10 17:07:01.423: %SVCLC-SP-5-STRRECVD: mod 2: <Application upgrade has succeeded>
*May 10 17:07:01.423: %SVCLC-SP-5-STRRECVD: mod 2: <You can now reset the module>
```

■ イメージのアップグレード

```
Router# hw-module module 2 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]y
% reset issued for module 2
16:38:34: SP: The PC in slot 2 is shutting down. Please wait ...
16:38:57: SP: PC shutdown completed for module 2
*May 10 17:11:10.065: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
16:39:50: SP: OS_BOOT_STATUS(2) AP OS Boot Status: finished booting
*May 10 17:13:18.119: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimum Diagnostics...
*May 10 17:13:18.863: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
*May 10 17:13:19.195: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now
online
```

```
Router# show module
```

Mod	Ports	Card Type	Model	Serial No.
1	2	Catalyst 6000 supervisor 2 (Active)	WS-X6K-S2U-MSFC2	SAD055006RZ
2	2	SSL VPN Accelerator	WS-SVC-WEBVPN-K9	

(テキスト出力は省略)

メンテナンス ソフトウェアのアップグレード



(注)

イメージがアップグレードされるまでは、モジュールをリセットしないでください。イメージのアップグレードには、最大 8 分程かかります。

MP ソフトウェアをアップグレードするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# <code>hw-module module mod reset cf:4</code>	AP からモジュールをリブートします。
ステップ 2	Router# <code>show module</code>	モジュールの AP がブートしたことを表示します。
ステップ 3	Router# <code>copy tftp: pcl#mod-fs:</code>	イメージをダウンロードします。
ステップ 4	Router# <code>hw-module module mod reset cf:1</code>	MP でモジュールをリセットします。 <div data-bbox="820 1512 869 1556" data-label="Image"> </div> <div data-bbox="813 1550 882 1585" data-label="Text"> <p>(注)</p> </div> <div data-bbox="901 1550 1489 1742" data-label="Text"> <p>コンソール上に「Upgrade of MP was successful. You can now boot MP」メッセージが表示されるまでは、モジュールをリセットしないでください。このメッセージが表示される前にモジュールをリセットすると、アップグレードに失敗することがあります。</p> </div>
ステップ 5	Router# <code>show module</code>	モジュールの MP がブートしたことを表示します。

次に、MP ソフトウェアをアップグレードする例を示します。

```
Router# hw module 2 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]y
% reset issued for module 2
16:43:51: SP: The PC in slot 2 is shutting down. Please wait ...
16:44:12: SP: PC shutdown completed for module 2
*May 10 17:16:25.271: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
16:45:05: SP: OS_BOOT_STATUS(2) AP OS Boot Status: finished booting
*May 10 17:18:33.363: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimum Diagnostics...
*May 10 17:18:34.103: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
*May 10 17:18:34.439: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now
online
```

```
Router# show module
```

Mod	Ports	Card Type	Model	Serial No.
1	2	Catalyst 6000 supervisor 2 (Active)	WS-X6K-S2U-MSFC2	SAD055006R2
2	2	SSL VPN Accelerator	WS-SVC-WEBVPN-K9	

(テキスト出力は省略)

```
Router# copy tftp: p1c#2-fs:
Address or name of remote host []? 10.10.10.1
Source filename []? mp.3-3-1.bin.gz
Destination filename [mp.3-3-1.bin.gz]?
Accessing tftp://10.10.10.1/mp.3-3-1.bin.gz...
Loading mp.3-3-1.bin.gz from 10.10.10.1 (via Vlan6):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

(テキスト出力は省略)

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 12342623 bytes]

12342623 bytes copied in 99.908 secs (123540 bytes/sec)
*May 10 17:21:05.423: %SVCLC-SP-5-STRRECVD: mod 2: <MP upgrade/Password Recovery
started.>
*May 10 17:21:05.991: %SVCLC-SP-5-STRRECVD: mod 2: <Uncompress of the file succeeded.
Continuing upgrade/recovery.>
*May 10 17:21:06.015: %SVCLC-SP-5-STRRECVD: mod 2: <This file appears to be a MP
upgrade. Continuing upgrade.>
*May 10 17:21:06.039: %SVCLC-SP-5-STRRECVD: mod 2: <Install of the MBR succeeded .
Continuing upgrade.>
*May 10 17:21:06.115: %SVCLC-SP-5-STRRECVD: mod 2: <Install of GRUB succeeded.
Continuing upgrade.>
*May 10 17:22:02.295: %SVCLC-SP-5-STRRECVD: mod 2: <Copying of MP succeeded.
Continuing upgrade.>
*May 10 17:22:02.311: %SVCLC-SP-5-STRRECVD: mod 2: <fsck of MP partition succeeded.>
*May 10 17:22:02.343: %SVCLC-SP-5-STRRECVD: mod 2: <Upgrade of MP was successful. You
can now boot MP.>
Router#
Router# hw mod 2 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]y
% reset issued for module 2
17:02:03: SP: The PC in slot 2 is shutting down. Please wait ...
17:02:23: SP: PC shutdown completed for module 2
*May 10 17:34:36.399: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
17:05:02: SP: OS_BOOT_STATUS(2) MP OS Boot Status: finished booting
*May 10 17:37:42.223: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimum Diagnostics...
*May 10 17:37:48.007: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
*May 10 17:37:48.303: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now
```

■ クライアントパッケージのインストール

```

online
Router#
Router# show module
Mod Ports Card Type Model Serial No.
-----
1 2 Catalyst 6000 supervisor 2 (Active) WS-X6K-S2U-MSFC2 SAD055006RZ
2 2 SSL VPN Accelerator (MP) WS-SVC-WEBVPN-K9

```

(テキスト出力は省略)

クライアントパッケージのインストール

ここでは、SSL VPN Client (SVC) および Cisco Secure Desktop (CSD) パッケージをインストールする手順について説明します。

- [トンネルモード用の SVC パッケージ \(p.C-6\)](#)
- [CSD パッケージ \(p.C-8\)](#)

トンネルモード用の SVC パッケージ

エンドユーザが各自の PC に SVC をダウンロードしてインストールできるようにするには、事前に SVC パッケージをインストールしておく必要があります。



(注)

エンドユーザが、SVC パッケージのインストール実行中に SVC のダウンロードを試みた場合、エンドユーザのブラウザに Out of Service ページが表示されることがあります。エンドユーザは、Retry ボタンをクリックして、SVC のダウンロードを再試行する必要があります。詳細は、「[初回の接続](#)」(p.A-5)を参照してください。

インストール実行中に、SVC パッケージファイル (svc.pkg) は、webvpn ディレクトリにインストールされます。SVC ファイルをインストールする前に、dir flash: コマンドを入力して、フラッシュデバイス上に webvpn ディレクトリが存在することを確認します。存在しない場合には、mkdir flash:/webvpn コマンドを入力して、フラッシュデバイス上に webvpn ディレクトリを作成します。

インストール実行後、フラッシュデバイスから SVC インストールファイル (sslclient*.pkg.zip) を削除します。



(注)

エンドユーザがパッケージをダウンロードできないようにする、またはパッケージを必要とするコンテンツにアクセスできないようにするには、no webvpn install svc コマンドを使用して、ゲートウェイからパッケージをアンインストールします。ただし、*.pkg ファイルはフラッシュデバイス上に存続するので、webvpn install svc flash:/webvpn/svc.pkg コマンドを入力すれば、ゲートウェイに再インストールできます。

delete flash:/webvpn/svc.pkg コマンドを使用すると、フラッシュからパッケージが削除されますが、既存のインストールには影響しません。エンドユーザは、引き続き、パッケージをダウンロードでき、パッケージを必要とするコンテンツにアクセスできます。



(注) WebVPN サービス モジュール をリセットまたはリブートすると、ゲートウェイ上に SVC がインストールされます。

SVC パッケージをインストールするには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn# dir flash:</code>	WebVPN サービス モジュール 上のフラッシュ デバイスのコンテンツを表示します。webvpn ディレクトリがあることを確認します。ない場合、 <code>mkdir flash:/webvpn</code> コマンドを入力します。
ステップ 2	<code>webvpn# copy tftp: flash:</code>	WebVPN サービス モジュール 上のフラッシュ デバイスに、SVC パッケージをコピーします。
ステップ 3	<code>webvpn# dir flash:</code>	WebVPN サービス モジュール 上のフラッシュ デバイスのコンテンツを表示します。SVC パッケージ ファイルがあることを確認します。
ステップ 4	<code>webvpn# configure terminal</code>	terminal オプションを選択して、コンフィギュレーション モードを開始します。
ステップ 5	<code>webvpn(config)# webvpn install svc flash:filename</code>	SVC パッケージをゲートウェイ上にインストールします。
ステップ 6	<code>webvpn(config)# end</code>	コンフィギュレーション モードを終了します。
ステップ 7	<code>webvpn# dir flash:/webvpn</code>	flash:webvpn ディレクトリのコンテンツを表示します。svc.pkg ファイルが存在することを確認します。

次に、SVC パッケージをダウンロードして、インストールする例を示します。

```
webvpn# copy tftp: flash:/webvpn
Address or name of remote host [10.1.1.1]?
Source filename []? <username>/sslclient-win-1.0.0.pkg.zip
Destination filename [sslclient-win-1.0.0.pkg.zip]?
Accessing tftp://10.1.1.1/<username>/sslclient-win-1.0.0.pkg.zip...
Loading <username>/sslclient-win-1.0.0.pkg.zip from 10.1.1.1
(via WebVPN0.1): !!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 352117 bytes]
352117 bytes copied in 8.032 secs (37384 bytes/sec)
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/

   4  -rwx      352117  Sep 14 2005 13:06:15 -08:00 sslclient-win-1.0.0.pkg.zip

16386048 bytes total (16072704 bytes free)
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn1(config)# webvpn install svc flash:/webvpn/sslclient-win-1.0.0.pkg.zip
SSLVPN Package SSL-VPN-Client : installed successfully
webvpn1(config)# end
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/

   4  -rwx      352117  Sep 14 2005 13:06:15 -08:00  svc.pkg

16386048 bytes total (16072704 bytes free)
webvpn#
```

CSD パッケージ

エンド ユーザが各自の PC に CSD をダウンロードしてインストールできるようにするには、事前に CSD パッケージをゲートウェイ インストールしておく必要があります。



(注) ゲートウェイの CSD ファイルのアップグレード中に、エンド ユーザがゲートウェイから CSD をダウンロードしようとする、エンド ユーザに以降で再試行するように通知する「503 Service Unavailable」メッセージが表示されることがあります。また、コンソールまたは他のロギング装置にもメッセージが表示されます。

CSD のインストール実行中に、CSD パッケージ ファイル (`sdesktop.pkg`) は、`webvpn` ディレクトリにインストールされます。CSD ファイルをインストールする前に、`dir flash:` コマンドを入力して、フラッシュ デバイス上に `webvpn` ディレクトリが存在することを確認します。存在しない場合には、`mkdir flash:/webvpn` コマンドを入力して、フラッシュ デバイス上に `webvpn` ディレクトリを作成します。

インストール実行後、CSD インストール ファイル (`securedesktop_ios_3_1*.pkg`) は、フラッシュ デバイスから削除されます。



(注) エンド ユーザがパッケージをダウンロードできないようにする、またはパッケージを必要とするコンテンツにアクセスできないようにするには、`no webvpn install csd` コマンドを使用して、ゲートウェイからパッケージをアンインストールします。ただし、`*.pkg` ファイルはフラッシュ デバイス上で維持されるので、`webvpn install csd flash:/webvpn/sdesktop.pkg` コマンドを入力すれば、ゲートウェイに再インストールできます。

`delete flash:/webvpn/sdesktop.pkg` コマンドを使用すると、フラッシュからパッケージが削除されますが、既存のインストールには影響しません。エンド ユーザは、引き続き、パッケージをダウンロードでき、パッケージを必要とするコンテンツにアクセスできます。



(注) WebVPN サービス モジュール をリセットまたはリポートすると、ゲートウェイ上に CSD がインストールされます。

CSD パッケージをダウンロードしてインストールするには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>webvpn# dir flash:</code>	WebVPN サービス モジュール 上のフラッシュ デバイスのコンテンツを表示します。 <code>webvpn</code> ディレクトリがあることを確認します。ない場合、 <code>mkdir flash:/webvpn</code> コマンドを入力します。
ステップ 2	<code>webvpn# copy tftp: flash:</code>	WebVPN サービス モジュール 上のフラッシュ デバイスに、CSD パッケージをコピーします。
ステップ 3	<code>webvpn# dir flash:</code>	WebVPN サービス モジュール 上のフラッシュ デバイスのコンテンツを表示します。CSD パッケージ ファイルがあることを確認します。

	コマンド	目的
ステップ 4	webvpn# configure terminal	terminal オプションを選択して、コンフィギュレーションモードを開始します。
ステップ 5	webvpn(config)# webvpn install csd flash:filename	CSD パッケージをゲートウェイ上にインストールします。
ステップ 6	webvpn(config)# end	コンフィギュレーションモードを終了します。
ステップ 7	webvpn# show webvpn install status csd	インストールした CSD パッケージのステータスを表示します。

次に、CSD パッケージをダウンロードして、インストールする例を示します。

```

webvpn# copy tftp: flash:/webvpn
Address or name of remote host [10.1.1.1]?
Source filename []? <username>/securedesktop_ios_3_1*.pkg
Destination filename [/webvpn/securedesktop_ios_3_1*.pkg]?
Accessing tftp://10.1.1.1/<username>/securedesktop_ios_3_1*.pkg...
Loading <username>/securedesktop_ios_3_1*.pkg from 10.1.1.1 (via
WebVPN0.1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1996130 bytes]
1996130 bytes copied in 33.948 secs (58800 bytes/sec)
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/

   4  -rwx      352117  Sep 14 2005 13:06:15 -08:00  svc.pkg
   5  -rwx      1996130  Sep 15 2005 15:14:04 -08:00  securedesktop_ios_3_1*.pkg

16386048 bytes total (14020608 bytes free)
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn(config)# webvpn install csd flash:/webvpn/securedesktop_ios_3_1*.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully

webvpn(config)#end
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/

   4  -rwx      352117  Sep 14 2005 13:06:15 -08:00  svc.pkg
   5  -rwx      1996130  Sep 15 2005 15:14:04 -08:00  sdesktop.pkg

16386048 bytes total (14020608 bytes free)
webvpn#
    
```

ライセンス アップグレードのインストール

WebVPN サービス モジュール は、デフォルトで最大 2560 のエンド ユーザをサポートします。ライセンス アップグレードを使用すると、WebVPN サービス モジュール で最大 8000 のエンド ユーザをサポートできます。次の 4 つのライセンス オプションがあります。

- デモ ライセンス 8000 エンド ユーザをサポートする 30 日間のライセンスです。デモ期間が終了すると、システムは元のライセンス レベル(2560 または 5000 エンド ユーザ)に戻ります。
- 2560 ~ 5000 エンド ユーザ エンド ユーザ数を 2560 から 5000 に増加するライセンス アップグレードです。
- 2560 ~ 8000 エンド ユーザ エンド ユーザ数を 2560 から 8000 に増加するライセンス アップグレードです。
- 5000 ~ 8000 エンド ユーザ エンド ユーザ数を 5000 から 8000 に増加するライセンス アップグレードです。

5000 または 8000 ユーザのライセンスにアップグレードするには、次の作業を行います。

ステップ 1 標準の製品発注チャネル(オンライン発注ツールまたは代理店など)に、適切なライセンス アップグレードを発注します。

Product Authorization Key (PAK) が提供されます。

ステップ 2 PAK を受領したら、次の URL にある Software Infrastructure and Fulfillment Technology (SWIFT) サイトにアクセスします。

<https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet>

ステップ 3 ライセンス アップグレードの PAK を入力します。

ステップ 4 Submit をクリックします。

発注内容が表示されます。

ステップ 5 内容を確認し、Continue をクリックします。



(注) 次の手順では、WebVPN サービス モジュールの MAC アドレスを入力する必要があります。MAC アドレスを表示するには、`show webvpn platform mac address` コマンドを入力します。

Customer Registration ページの MAC アドレス フィールドは、入力された最初の 12 文字だけを受け入れます。12 文字の MAC アドレスだけを入力してください。区切り文字は入力しません。

ステップ 6 Customer Registration ページの入力を完了します。

ステップ 7 Submit をクリックします。

レジストレーションが完了すると、ライセンス (WEBVPN*.lic) が添付された E メールが送信されます。また、WebVPN サービス モジュール にライセンスをインストールするための製品専用の説明書が提供されます。

ステップ 8 E メールに添付された説明書に従って、ライセンス ファイルをインストールします。

デモ ライセンスをダウンロードするには、次の作業を行います。

ステップ 1 次の URL にある SWIFT サイトにアクセスします。

<https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet>

ステップ 2 Catalyst 6500/7600/ WebVPN Demo License リンクをクリックします。



(注) 次の手順では、WebVPN サービス モジュールの MAC アドレスを入力する必要があります。MAC アドレスを表示するには、`show webvpn platform mac address` コマンドを入力します。

Customer Registration ページの MAC アドレス フィールドは、入力された最初の 12 文字だけを受け入れます。12 文字の MAC アドレスだけを入力してください。区切り文字は入力しません。

ステップ 3 Customer Registration ページの入力を完了します。

ステップ 4 Submit をクリックします。

レジストレーションが完了すると、ライセンス (WEBVPN*.lic) が添付された E メールが送信されます。また、WebVPN サービス モジュール にライセンスをインストールするための製品専用の説明書が提供されます。

ステップ 5 E メールに添付された説明書に従って、ライセンス ファイルをインストールします。

■ ライセンス アップグレードのインストール



カラー名および RGB カラー値

表 D-1 に、`title-color color` コマンドおよび `secondary-color color` コマンドを入力する場合の、`color` の有効値を示します。デフォルトのカラーは、パープルです。

値は、HTML で認識されるカラー名（ワードまたは文字間のスペースなし）と同じにするか、または Red、Green、Blue（RGB）値をカンマで区切って入力します。値の長さは 32 文字までです。



(注)

ブラウザはすべて RGB 値をサポートしていますが、カラー名をサポートしているとは限りません。カラー名を入力し、予想した結果が得られない場合には、RGB 値を使用してください。

次に、タイトル カラーを設定する場合の 2 つの例を示します。

- `webvpn(config-webvpn-context)# title-color darkseagreen`
- `webvpn(config-webvpn-context)# title-color 143,188,143`

表 D-1 カラー名および RGB 値

カラー名	R	G	B
AliceBlue	240	248	255
AntiqueWhite	250	235	215
AntiqueWhite1	255	239	219
AntiqueWhite2	238	223	204
AntiqueWhite3	205	192	176
AntiqueWhite4	139	131	120
Aquamarine	127	255	212
Aquamarine1	127	255	212
Aquamarine2	118	238	198
Aquamarine3	102	205	170
Aquamarine4	69	139	116
Azure	240	255	255
Azure1	240	255	255
Azure2	224	238	238
Azure3	193	205	205
Azure4	131	139	139

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Beige	245	245	220
Bisque	255	228	196
Bisque1	255	228	196
Bisque2	238	213	183
Bisque3	205	183	158
Bisque4	139	125	107
Black	0	0	0
BlanchedAlmond	255	235	205
Blue	0	0	255
Blue1	0	0	255
Blue2	0	0	238
Blue3	0	0	205
Blue4	0	0	139
BlueViolet	138	43	226
Brown	165	42	42
Brown1	255	64	64
Brown2	238	59	59
Brown3	205	51	51
Brown4	139	35	35
Burlywood	222	184	135
Burlywood1	255	211	155
Burlywood2	238	197	145
Burlywood3	205	170	125
Burlywood4	139	115	85
CadetBlue	95	158	160
CadetBlue1	152	245	255
CadetBlue2	142	229	238
CadetBlue3	122	197	205
CadetBlue4	83	134	139
Chartreuse	127	255	0
Chartreuse1	127	255	0
Chartreuse2	118	238	0
Chartreuse3	102	205	0
Chartreuse4	69	139	0
Chocolate	210	105	30
Chocolate1	255	127	36
Chocolate2	238	118	33
Chocolate3	205	102	29
Chocolate4	139	69	19
Coral	255	127	80
Coral1	255	114	86

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Coral2	238	106	80
Coral3	205	91	69
Coral4	139	62	47
CornflowerBlue	100	149	237
Cornsilk	255	248	220
Cornsilk1	255	248	220
Cornsilk2	238	232	205
Cornsilk3	205	200	177
Cornsilk4	139	136	120
Cyan	0	255	255
Cyan1	0	255	255
Cyan2	0	238	238
Cyan3	0	205	205
Cyan4	0	139	139
DarkBlue	0	0	139
DarkCyan	0	139	139
DarkGoldenrod	184	134	11
DarkGoldenrod1	255	185	15
DarkGoldenrod2	238	173	14
DarkGoldenrod3	205	149	12
DarkGoldenrod4	139	101	8
DarkGray	169	169	169
DarkGreen	0	100	0
DarkKhaki	189	183	107
DarkMagenta	139	0	139
DarkOliveGreen	85	107	47
DarkOliveGreen1	202	255	112
DarkOliveGreen2	188	238	104
DarkOliveGreen3	162	205	90
DarkOliveGreen4	110	139	61
DarkOrange	255	140	0
DarkOrange1	255	127	0
DarkOrange2	238	118	0
DarkOrange3	205	102	0
DarkOrange4	139	69	0
DarkOrchid	153	50	204
DarkOrchid1	191	62	255
DarkOrchid2	178	58	238
DarkOrchid3	154	50	205
DarkOrchid4	104	34	139
DarkRed	139	0	0

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
DarkSalmon	233	150	122
DarkSeaGreen	143	188	143
DarkSeaGreen1	193	255	193
DarkSeaGreen2	180	238	180
DarkSeaGreen3	155	205	155
DarkSeaGreen4	105	139	105
DarkSlateBlue	72	61	139
DarkSlateGray	47	79	79
DarkSlateGray1	151	255	255
DarkSlateGray2	141	238	238
DarkSlateGray3	121	205	205
DarkSlateGray4	82	139	139
DarkTurquoise	0	206	209
DarkViolet	148	0	211
DeepPink	255	20	147
DeepPink1	255	20	147
DeepPink2	238	18	137
DeepPink3	205	16	118
DeepPink4	139	10	80
DeepSkyBlue	0	191	255
DeepSkyBlue1	0	191	255
DeepSkyBlue2	0	178	238
DeepSkyBlue3	0	154	205
DeepSkyBlue4	0	104	139
DimGrey	105	105	105
DodgerBlue	30	144	255
DodgerBlue1	30	144	255
DodgerBlue2	28	134	238
DodgerBlue3	24	116	205
DodgerBlue4	16	78	139
Firebrick	178	34	34
Firebrick1	255	48	48
Firebrick2	238	44	44
Firebrick3	205	38	38
Firebrick4	139	26	26
FloralWhite	255	250	240
ForestGreen	34	139	34
Gainsboro	220	220	220
GhostWhite	248	248	255
Gold	255	215	0
Gold1	255	215	0

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Gold2	238	201	0
Gold3	205	173	0
Gold4	139	117	0
Goldenrod	218	165	32
Goldenrod1	255	193	37
Goldenrod2	238	180	34
Goldenrod3	205	155	29
Goldenrod4	139	105	20
Gray0	0	0	0
Gray1	3	3	3
Gray10	26	26	26
Gray100	255	255	255
Gray11	28	28	28
Gray12	31	31	31
Gray13	33	33	33
Gray14	36	36	36
Gray15	38	38	38
Gray16	41	41	41
Gray17	43	43	43
Gray18	46	46	46
Gray19	48	48	48
Gray2	5	5	5
Gray20	51	51	51
Gray21	54	54	54
Gray22	56	56	56
Gray23	59	59	59
Gray24	61	61	61
Gray25	64	64	64
Gray26	66	66	66
Gray27	69	69	69
Gray28	71	71	71
Gray29	74	74	74
Gray3	8	8	8
Gray30	77	77	77
Gray31	79	79	79
Gray32	82	82	82
Gray33	84	84	84
Gray34	87	87	87
Gray35	89	89	89
Gray36	92	92	92
Gray37	94	94	94

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Gray38	97	97	97
Gray39	99	99	99
Gray4	10	10	10
Gray40	102	102	102
Gray41	105	105	105
Gray42	107	107	107
Gray43	110	110	110
Gray44	112	112	112
Gray45	115	115	115
Gray46	117	117	117
Gray47	120	120	120
Gray48	122	122	122
Gray49	125	125	125
Gray5	13	13	13
Gray50	127	127	127
Gray51	130	130	130
Gray52	133	133	133
Gray53	135	135	135
Gray54	138	138	138
Gray55	140	140	140
Gray56	143	143	143
Gray57	145	145	145
Gray58	148	148	148
Gray59	150	150	150
Gray6	15	15	15
Gray60	153	153	153
Gray61	156	156	156
Gray62	158	158	158
Gray63	161	161	161
Gray64	163	163	163
Gray65	166	166	166
Gray66	168	168	168
Gray67	171	171	171
Gray68	173	173	173
Gray69	176	176	176
Gray7	18	18	18
Gray70	179	179	179
Gray71	181	181	181
Gray72	184	184	184
Gray73	186	186	186
Gray74	189	189	189

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Gray75	191	191	191
Gray76	194	194	194
Gray77	196	196	196
Gray78	199	199	199
Gray79	201	201	201
Gray8	20	20	20
Gray80	204	204	204
Gray81	207	207	207
Gray82	209	209	209
Gray83	212	212	212
Gray84	214	214	214
Gray85	217	217	217
Gray86	219	219	219
Gray87	222	222	222
Gray88	224	224	224
Gray89	227	227	227
Gray9	23	23	23
Gray90	229	229	229
Gray91	232	232	232
Gray92	235	235	235
Gray93	237	237	237
Gray94	240	240	240
Gray95	242	242	242
Gray96	245	245	245
Gray97	247	247	247
Gray98	250	250	250
Gray99	252	252	252
Green	0	255	0
Green1	0	255	0
Green2	0	238	0
Green3	0	205	0
Green4	0	139	0
GreenYellow	173	255	47
Grey	190	190	190
Grey0	0	0	0
Grey1	3	3	3
Grey10	26	26	26
Grey100	255	255	255
Grey11	28	28	28
Grey12	31	31	31
Grey13	33	33	33

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Grey14	36	36	36
Grey15	38	38	38
Grey16	41	41	41
Grey17	43	43	43
Grey18	46	46	46
Grey19	48	48	48
Grey2	5	5	5
Grey20	51	51	51
Grey21	54	54	54
Grey22	56	56	56
Grey23	59	59	59
Grey24	61	61	61
Grey25	64	64	64
Grey26	66	66	66
Grey27	69	69	69
Grey28	71	71	71
Grey29	74	74	74
Grey3	8	8	8
Grey30	77	77	77
Grey31	79	79	79
Grey32	82	82	82
Grey33	84	84	84
Grey34	87	87	87
Grey35	89	89	89
Grey36	92	92	92
Grey37	94	94	94
Grey38	97	97	97
Grey39	99	99	99
Grey4	10	10	10
Grey40	102	102	102
Grey41	105	105	105
Grey42	107	107	107
Grey43	110	110	110
Grey44	112	112	112
Grey45	115	115	115
Grey46	117	117	117
Grey47	120	120	120
Grey48	122	122	122
Grey49	125	125	125
Grey5	13	13	13
Grey50	127	127	127

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Grey51	130	130	130
Grey52	133	133	133
Grey53	135	135	135
Grey54	138	138	138
Grey55	140	140	140
Grey56	143	143	143
Grey57	145	145	145
Grey58	148	148	148
Grey59	150	150	150
Grey6	15	15	15
Grey60	153	153	153
Grey61	156	156	156
Grey62	158	158	158
Grey63	161	161	161
Grey64	163	163	163
Grey65	166	166	166
Grey66	168	168	168
Grey67	171	171	171
Grey68	173	173	173
Grey69	176	176	176
Grey7	18	18	18
Grey70	179	179	179
Grey71	181	181	181
Grey72	184	184	184
Grey73	186	186	186
Grey74	189	189	189
Grey75	191	191	191
Grey76	194	194	194
Grey77	196	196	196
Grey78	199	199	199
Grey79	201	201	201
Grey8	20	20	20
Grey80	204	204	204
Grey81	207	207	207
Grey82	209	209	209
Grey83	212	212	212
Grey84	214	214	214
Grey85	217	217	217
Grey86	219	219	219
Grey87	222	222	222
Grey88	224	224	224

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Grey89	227	227	227
Grey9	23	23	23
Grey90	229	229	229
Grey91	232	232	232
Grey92	235	235	235
Grey93	237	237	237
Grey94	240	240	240
Grey95	242	242	242
Grey96	245	245	245
Grey97	247	247	247
Grey98	250	250	250
Grey99	252	252	252
Honeydew	240	255	240
Honeydew1	240	255	240
Honeydew2	224	238	224
Honeydew3	193	205	193
Honeydew4	131	139	131
HotPink	255	105	180
HotPink1	255	110	180
HotPink2	238	106	167
HotPink3	205	96	144
HotPink4	139	58	98
IndianRed	205	92	92
IndianRed1	255	106	106
IndianRed2	238	99	99
IndianRed3	205	85	85
IndianRed4	139	58	58
Ivory	255	255	240
Ivory1	255	255	240
Ivory2	238	238	224
Ivory3	205	205	193
Ivory4	139	139	131
Khaki	240	230	140
Khaki1	255	246	143
Khaki2	238	230	133
Khaki3	205	198	115
Khaki4	139	134	78
Lavender	230	230	250
LavenderBlush	255	240	245
LavenderBlush1	255	240	245
LavenderBlush2	238	224	229

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
LavenderBlush3	205	193	197
LavenderBlush4	139	131	134
LawnGreen	124	252	0
LemonChiffon	255	250	205
LemonChiffon1	255	250	205
LemonChiffon2	238	233	191
LemonChiffon3	205	201	165
LemonChiffon4	139	137	112
LightBlue	173	216	230
LightBlue1	191	239	255
LightBlue2	178	223	238
LightBlue3	154	192	205
LightBlue4	104	131	139
LightCoral	240	128	128
LightCyan	224	255	255
LightCyan1	224	255	255
LightCyan2	209	238	238
LightCyan3	180	205	205
LightCyan4	122	139	139
LightGoldenrod	238	221	130
LightGoldenrod1	255	236	139
LightGoldenrod2	238	220	130
LightGoldenrod3	205	190	112
LightGoldenrod4	139	129	76
LightGoldenrodYellow	250	250	210
LightGreen	144	238	144
LightGrey	211	211	211
LightPink	255	182	193
LightPink1	255	174	185
LightPink2	238	162	173
LightPink3	205	140	149
LightPink4	139	95	101
LightSalmon	255	160	122
LightSalmon1	255	160	122
LightSalmon2	238	149	114
LightSalmon3	205	129	98
LightSalmon4	139	87	66
LightSeaGreen	32	178	170
LightSkyBlue	135	206	250
LightSkyBlue1	176	226	255
LightSkyBlue2	164	211	238

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
LightSkyBlue3	141	182	205
LightSkyBlue4	96	123	139
LightSlateBlue	132	112	255
LightSlateGray	119	136	153
LightSteelBlue	176	196	222
LightSteelBlue1	202	225	255
LightSteelBlue2	188	210	238
LightSteelBlue3	162	181	205
LightSteelBlue4	110	123	139
LightYellow	255	255	224
LightYellow1	255	255	224
LightYellow2	238	238	209
LightYellow3	205	205	180
LightYellow4	139	139	122
LimeGreen	50	205	50
Linen	250	240	230
Magenta	255	0	255
Magenta1	255	0	255
Magenta2	238	0	238
Magenta3	205	0	205
Magenta4	139	0	139
Maroon	176	48	96
Maroon1	255	52	179
Maroon2	238	48	167
Maroon3	205	41	144
Maroon4	139	28	98
MediumAquamarine	102	205	170
MediumBlue	0	0	205
MediumOrchid	186	85	211
MediumOrchid1	224	102	255
MediumOrchid2	209	95	238
MediumOrchid3	180	82	205
MediumOrchid4	122	55	139
MediumPurple	147	112	219
MediumPurple1	171	130	255
MediumPurple2	159	121	238
MediumPurple3	137	104	205
MediumPurple4	93	71	139
MediumSeaGreen	60	179	113
MediumSlateBlue	123	104	238
MediumSpringGreen	0	250	154

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
MediumTurquoise	72	209	204
MediumVioletRed	199	21	133
MidnightBlue	25	25	112
MintCream	245	255	250
MistyRose	255	228	225
MistyRose1	255	228	225
MistyRose2	238	213	210
MistyRose3	205	183	181
MistyRose4	139	125	123
Moccasin	255	228	181
NavajoWhite	255	222	173
NavajoWhite1	255	222	173
NavajoWhite2	238	207	161
NavajoWhite3	205	179	139
NavajoWhite4	139	121	94
Navy	0	0	128
NavyBlue	0	0	128
OldLace	253	245	230
OliveDrab	107	142	35
OliveDrab1	192	255	62
OliveDrab2	179	238	58
OliveDrab3	154	205	50
OliveDrab4	105	139	34
Orange	255	165	0
Orange1	255	165	0
Orange2	238	154	0
Orange3	205	133	0
Orange4	139	90	0
OrangeRed	255	69	0
OrangeRed1	255	69	0
OrangeRed2	238	64	0
OrangeRed3	205	55	0
OrangeRed4	139	37	0
Orchid	218	112	214
Orchid1	255	131	250
Orchid2	238	122	233
Orchid3	205	105	201
Orchid4	139	71	137
PaleGoldenrod	238	232	170
PaleGreen	152	251	152
PaleGreen1	154	255	154

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
PaleGreen2	144	238	144
PaleGreen3	124	205	124
PaleGreen4	84	139	84
PaleTurquoise	175	238	238
PaleTurquoise1	187	255	255
PaleTurquoise2	174	238	238
PaleTurquoise3	150	205	205
PaleTurquoise4	102	139	139
PaleVioletRed	219	112	147
PaleVioletRed1	255	130	171
PaleVioletRed2	238	121	159
PaleVioletRed3	205	104	137
PaleVioletRed4	139	71	93
PapayaWhip	255	239	213
PeachPuff	255	218	185
PeachPuff1	255	218	185
PeachPuff2	238	203	173
PeachPuff3	205	175	149
PeachPuff4	139	119	101
Peru	205	133	63
Pink	255	192	203
Pink1	255	181	197
Pink2	238	169	184
Pink3	205	145	158
Pink4	139	99	108
Plum	221	160	221
Plum1	255	187	255
Plum2	238	174	238
Plum3	205	150	205
Plum4	139	102	139
PowderBlue	176	224	230
Purple	160	32	240
Purple1	155	48	255
Purple2	145	44	238
Purple3	125	38	205
Purple4	85	26	139
Red	255	0	0
Red1	255	0	0
Red2	238	0	0
Red3	205	0	0
Red4	139	0	0

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
RosyBrown	188	143	143
RosyBrown1	255	193	193
RosyBrown2	238	180	180
RosyBrown3	205	155	155
RosyBrown4	139	105	105
RoyalBlue	65	105	225
RoyalBlue1	72	118	255
RoyalBlue2	67	110	238
RoyalBlue3	58	95	205
RoyalBlue4	39	64	139
SaddleBrown	139	69	19
Salmon	250	128	114
Salmon1	255	140	105
Salmon2	238	130	98
Salmon3	205	112	84
Salmon4	139	76	57
SandyBrown	244	164	96
SeaGreen	46	139	87
SeaGreen1	84	255	159
SeaGreen2	78	238	148
SeaGreen3	67	205	128
SeaGreen4	46	139	87
Seashell	255	245	238
Seashell1	255	245	238
Seashell2	238	229	222
Seashell3	205	197	191
Seashell4	139	134	130
Sienna	160	82	45
Sienna1	255	130	71
Sienna2	238	121	66
Sienna3	205	104	57
Sienna4	139	71	38
SkyBlue	135	206	235
SkyBlue1	135	206	255
SkyBlue2	126	192	238
SkyBlue3	108	166	205
SkyBlue4	74	112	139
SlateBlue	106	90	205
SlateBlue1	131	111	255
SlateBlue2	122	103	238
SlateBlue3	105	89	205

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
SlateBlue4	71	60	139
SlateGray	112	128	144
SlateGray1	198	226	255
SlateGray2	185	211	238
SlateGray3	159	182	205
SlateGray4	108	123	139
Snow	255	250	250
Snow1	255	250	250
Snow2	238	233	233
Snow3	205	201	201
Snow4	139	137	137
SpringGreen	0	255	127
SpringGreen1	0	255	127
SpringGreen2	0	238	118
SpringGreen3	0	205	102
SpringGreen4	0	139	69
SteelBlue	70	130	180
SteelBlue1	99	184	255
SteelBlue2	92	172	238
SteelBlue3	79	148	205
SteelBlue4	54	100	139
Tan	210	180	140
Tan1	255	165	79
Tan2	238	154	73
Tan3	205	133	63
Tan4	139	90	43
Thistle	216	191	216
Thistle1	255	225	255
Thistle2	238	210	238
Thistle3	205	181	205
Thistle4	139	123	139
Tomato	255	99	71
Tomato1	255	99	71
Tomato2	238	92	66
Tomato3	205	79	57
Tomato4	139	54	38
Turquoise	64	224	208
Turquoise1	0	245	255
Turquoise2	0	229	238
Turquoise3	0	197	205
Turquoise4	0	134	139

表 D-1 カラー名および RGB 値 (続き)

カラー名	R	G	B
Violet	238	130	238
VioletRed	208	32	144
VioletRed1	255	62	150
VioletRed2	238	58	140
VioletRed3	205	50	120
VioletRed4	139	34	82
Wheat	245	222	179
Wheat1	255	231	186
Wheat2	238	216	174
Wheat3	205	186	150
Wheat4	139	126	102
White	255	255	255
WhiteSmoke	245	245	245
Yellow	255	255	0
Yellow1	255	255	0
Yellow2	238	238	0
Yellow3	205	205	0
Yellow4	139	139	0
YellowGreen	154	205	50



C		W	
Cisco Secure Desktop		WebVPN	
CSD を参照	3-10	エンド ユーザの設定	A-1
CSD		クッキー対応	A-14
インストール	C-8	クライアントの要件	
概要	3-10	E メール	A-16
設定	3-11	Web ブラウジング	A-15
O		起動	A-2
Outlook Web Access (OWA) および WebVPN	A-16	ネットワーク ブラウジング	A-15
P		ファイル管理	A-15
PEM ファイルのインポート	3-48	サポートされるインターネット接続のタイプ	A-2
PEM ファイルのエクスポート	3-48	使用上の推奨	A-1
PKCS12 ファイルのインポート	3-46	セキュリティ上の注意事項	A-17
PKCS12 ファイルのエクスポート	3-46	トラブルシューティング	A-18
PKI		WebVPN での Web ブラウジング	A-15
概要	3-28	あ	
設定	3-28	アプリケーション アクセス	
Public Key Infrastructure		E メール プロキシ	A-16
PKI を参照		Eメールの使用	A-16
S		IMAP クライアント	A-16
SCEP、鍵および証明書の設定	3-29	Web アクセス	A-16
Simple Certificate Enrollment Protocol		クライアント アプリケーションの設定	A-14
SCEP を参照		権限	A-14
SSL ポリシー、設定	3-23	再イネーブル化	A-19
Sun Microsystems Java™ Runtime Environment (JRE) およ び WebVPN	A-14	適正な終了	A-14, A-18
		ブラウザをクッキー対応にする	A-14
		ホスト ファイル エラー	A-18
		か	
		鍵	
		削除	3-57
		バックアップ	3-56
		表示	3-57

- 鍵および証明書の共有 3-54
- 鍵および証明書のバックアップ 3-56
- 鍵および証明書の表示 3-57
- 鍵の削除 3-57
- 関連資料 xiv

- く
- 組み込まれたテスト証明書のインポート B-1

- こ
- コンフィギュレーションの保存 3-55
- コンフィギュレーション、保存 3-55

- し
- 証明書
 - 確認 3-54
 - 共有 3-54
 - 更新 3-59
 - 削除 3-58
 - 自動登録および自動更新 3-62
 - バックアップ 3-56
 - 表示 3-57
- 証明書およびトラストポイントの確認 3-54
- 証明書の更新 3-59
- 証明書の削除 3-58
- 証明書の自動登録および自動更新 3-62

- せ
- 設定
 - PKI 3-28
 - SSL ポリシー 3-23
 - WebVPN ゲートウェイ 3-8
 - WebVPN コンテキスト 3-8
- 鍵および証明書
 - SCEP の使用、RSA 鍵の生成 3-30
 - SCEP の使用、証明書のリクエスト 3-33
 - SCEP の使用、トラストポイントの宣言 3-32
 - SCEP の使用、認証局の証明書の取得 3-33
 - SCEP の使用、例 3-34
 - 鍵ペアおよび証明書のインポート 3-45
 - 手動証明書登録 3-36
- 仮想ゲートウェイ 3-5

- た
- 対象読者 xi

- て
- テスト証明書、インポート B-1

- と
- トラストポイント、確認 3-54

- に
- 認証局
 - 下位 3-30
 - 証明書の取得 3-33
 - 登録、3 階層の例 3-34
 - ルート 3-30

- は
- パスワードを忘れた場合 2-7

- ふ
- プロキシ サービスへの証明書の割り当て 3-58

- ほ
- ポート転送
 - クライアント アプリケーションの設定 A-14
- ホスト ファイル
 - エラー A-18

- ま
- マニュアル
 - 関連資料 xiv
 - 構成 xii
 - 表記法 xiii
- マニュアルの構成 xii