



WebVPN エンド ユーザ設定

この項は、エンド ユーザのために WebVPN を設定するシステム管理者を対象にしています。ここでは、ユーザ リモート システムの設定要件と作業の概要を説明します。また、ユーザが WebVPN の使用を開始するために、ユーザに伝える必要のある情報も明確にします。この項は、次の内容で構成されています。

- [ユーザ名とパスワードの要求](#)
- [セキュリティのヒントの通知](#)
- [WebVPN 機能を使用するためのリモートシステムの設定](#)
- [WebVPN データのキャプチャ](#)



(注)

すでに WebVPN に対してセキュリティ アプライアンスを設定済みであるものと想定します。

ユーザ名とパスワードの要求

ネットワークによっては、リモートセッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、WebVPN、メール サーバ、ファイル サーバ、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、一意のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。

表 30-1 に、WebVPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 30-1 WebVPN ユーザに通知するユーザ名とパスワード

ログイン ユーザ名 / パスワードタイプ	目的	入力するタイミング
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
インターネット サービス 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 サービス プロバイダーへの接続
WebVPN	リモート ネットワークへのアクセス	WebVPN の起動
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とき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	WebVPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	WebVPN 経由によるリモート メールサーバへのアクセス	電子メール メッセージの送受信

セキュリティのヒントの通知

必ず WebVPN セッションからログアウトするようにユーザに通知してください (WebVPN からログアウトするには、WebVPN ツールバーの logout アイコンをクリックするか、またはブラウザを閉じます)。

WebVPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。WebVPN は、企業ネットワーク上のリモート PC やワークステーションとセキュリティ アプライアンスとの間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース (インターネット上や内部ネットワーク上にあるもの) にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

WebVPN 機能を使用するためのリモート システムの設定

表30-2 に、WebVPN を使用するためのリモート システムの設定に関する、次の各種情報を示します。

- WebVPN の起動
- WebVPN フローティング ツールバーの使用
- Web ブラウジング
- ネットワーク ブラウジングとファイル管理
- アプリケーションの使用（ポート転送）
- ポート転送を介した電子メールの使用
- Web アクセスを介した電子メールの使用
- 電子メールプロキシを介した電子メールの使用

また、表 30-2 には、次の項目に関する情報も記載されています。

- WebVPN の要件（機能別）
- WebVPN をサポートするアプリケーション
- クライアントアプリケーションのインストールとコンフィギュレーションの要件
- エンド ユーザに提供する必要のある情報
- エンド ユーザのためのヒントや使用上の推奨事項

ユーザ アカウントを別々に設定し、各ユーザがそれぞれ異なる WebVPN 機能を使用できるようにすることが可能です。表 30-2 には機能別の情報をまとめてあります。利用できない機能の情報についてはスキップしてください。

表 30-2 WebVPN リモート システム コンフィギュレーションとエンド 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事項
WebVPN の起動	インターネットへの接続	サポートされているインターネット接続は、次のとおりです。 <ul style="list-style-type: none"> • 家庭の DSL、ケーブル、ダイヤルアップ • 公共のキオスク • ホテルの回線 • 空港の無線ノード • インターネットカフェ
	WebVPN 対応のブラウザ	WebVPN には次のブラウザを推奨します。他のブラウザでは、WebVPN 機能を完全にはサポートできない場合があります。 <p>Microsoft Windows の場合：</p> <ul style="list-style-type: none"> • Internet Explorer バージョン 6.0 • Netscape バージョン 7.2 • Mozilla バージョン 1.7 以降 • Firefox 1.x <p>Linux の場合：</p> <ul style="list-style-type: none"> • Mozilla バージョン 1.7 • Netscape バージョン 7.2 • Firefox 1.x <p>Solaris の場合：</p> <ul style="list-style-type: none"> • Netscape バージョン 7.2 <p>Macintosh OS X の場合：</p> <ul style="list-style-type: none"> • Safari バージョン 1.0 • Firefox 1.x
	ブラウザでのクッキーのイネーブル化	ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
	WebVPN 用の URL	https アドレスの形式は次のとおりです。 https://address address は、WebVPN がイネーブルになっているセキュリティ アプライアンスのインターフェイスの IP アドレスまたは DNS ホスト名(またはロードバランシング クラスター) です。たとえば、https://10.89.192.163 または https://cisco.example.com のようになります。
WebVPN のユーザ名とパスワード		
(オプション) ローカルプリンタ		WebVPN は、Web ブラウザからネットワーク プリンタへの印刷をサポートしていません。ローカルプリンタへの印刷はサポートされています。

表 30-2 WebVPN リモート システム コンフィギュレーションとエンド 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事項
WebVPN フローティング ツールバーの使用		<p>フローティング ツールバーを使用すると、WebVPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。</p> <p>ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。</p> <p>フローティング ツールバーは、現在の WebVPN セッションを表します。Close ボタンをクリックすると、セキュリティ アプライアンスは WebVPN セッションの終了を確認するプロンプトを表示します。</p> <p> ヒント ヒント：テキストをテキスト フィールドに貼り付けるには、Ctrl+V キーを使用します (WebVPN ツールバーでは右クリックはディセーブルになっています)。</p>
Web ブラウジング	保護されている Web サイトのユーザ名とパスワード	<p>WebVPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。「セキュリティのヒントの通知」を参照してください。</p> <p>WebVPN での Web ブラウジングのルックアンドフィールは、ユーザが見慣れたものではない場合があります。次の例を参考にしてください。</p> <ul style="list-style-type: none"> • WebVPN タイトル バーが各 Web ページの上部に表示される • Web サイトへのアクセス方法： <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 を入力する – WebVPN ホームページ上にある設定済みの Web サイトリンクをクリックする – 上記 2 つのどちら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する <p>また、特定のアカウントの設定によっては、次のようになる場合もあります。</p> <ul style="list-style-type: none"> • 一部の Web サイトがブロックされている • 使用可能な Web サイトが、WebVPN ホームページ上にリンクとして表示されるものに限られる

表 30-2 WebVPN リモート システム コンフィギュレーションとエンド 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事項
ネットワーク ブラウジングとファイル管理	共有リモートアクセス用に設定されたファイルアクセス権	WebVPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。
	保護されているファイル サーバのサーバ名とパスワード	—
	フォルダとファイルが存在するドメイン、ワークグループ、およびサーバ名	ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。
	—	コピー処理の進行中は、 Copy File to Server コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。
アプリケーションの使用 (ポート転送またはアプリケーションアクセスと呼ばれる)	 (注) Macintosh OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。	
	 (注) この機能を使用するには、Sun Microsystems Java™ Runtime Environment 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ます。これには、ローカルシステムで管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。	
	 注意 ユーザは、 Close アイコンをクリックしてアプリケーションを終了したら、必ず Application Access ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、 Application Access またはアプリケーション自体がディセーブルになる可能性があります。	
	インストール済みのクライアント アプリケーション	—
	ブラウザでイネーブルにされているクッキー	—
管理者特権	ユーザが DNS 名を使用してサーバを指定する場合、そのユーザは PC の管理者用アクセス特権を持つ必要があります。これは、hosts ファイルを修正するのにこの特権が必要なためです。	
インストール済みの Sun Microsystems Java Runtime Environment (JRE) バージョン 1.4.x と 1.5.x	JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。	
ブラウザで Javascript をイネーブルにする必要があります。デフォルトでは、イネーブルになっています。	まれに、JAVA 例外エラーで WebVPN ポート転送アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。 <ol style="list-style-type: none"> 1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。 2. JAVA アイコンがコンピュータのタスク バーに表示されていないことを確認します。JAVA のインスタンスをすべて閉じます。 3. WebVPN セッションを確立し、ポート転送 JAVA アプレットを起動します。 	

表 30-2 WebVPN リモート システム コンフィギュレーションとエンド 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事項
	<p>設定済みのクライアント アプリケーション (必要な場合)</p> <p> (注) Microsoft Outlook クライアントの場合、この設定手順は不要です。</p> <p>Windows 以外のすべてのクライアントアプリケーションでは、設定が必要です。</p> <p>Windows アプリケーションの設定が必要かどうかを確認するには、Remote Server の値をチェックします。</p> <ul style="list-style-type: none"> Remote Server にサーバ ホスト名が含まれている場合、クライアントアプリケーションの設定は不要です。 Remote Server フィールドに IP アドレスが含まれている場合、クライアントアプリケーションを設定する必要があります。 	<p>クライアントアプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。</p> <ol style="list-style-type: none"> リモートシステム上で WebVPN を起動し、WebVPN ホームページの Application Access リンクをクリックします。Application Access ウィンドウが表示されます。 Name カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を Local カラムで確認します。 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、クライアントアプリケーションによって異なります。
	<p> (注) WebVPN でアプリケーションを実行している場合、アプリケーションで表示される URL (電子メール内の URL など) をクリックしても、WebVPN ではそのサイトは開きません。WebVPN でこのようなサイトを開くには、Enter WebVPN (URL) Address フィールドに URL をカットアンドペーストします。</p>	
Application Access を介した電子メールの使用	<p>Application Access の要件を満たす (「アプリケーションの使用」を参照)</p> <p> (注) IMAP クライアントの使用中にメールサーバとの接続が中断し、新しく接続を確立できない場合は、IMAP アプリケーションを終了して WebVPN を再起動します。</p> <p>その他のメールクライアント</p>	<p>電子メールを使用するには、WebVPN ホームページから Application Access を起動します。これによって、メールクライアントが使用できるようになります。</p> <p>Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。</p> <p>WebVPN は、Netscape Mail、Lotus Notes、および Eudora などの、ポート転送を介したその他の SMTPS、POP3S、または IMAP4S 電子メールプログラムをサポートしますが、動作確認は行っていません。</p>
電子メール プロキシを介した電子メールの使用	<p>インストールされている Web ベースの電子メール製品</p>	<p>サポートされている製品は次のとおりです。</p> <ul style="list-style-type: none"> Outlook Web Access <p>最適な結果を得るために、Internet Explorer 6.x 以上、Mozilla 1.7、または Firefox 1.x で OWA を使用してください。</p> <ul style="list-style-type: none"> Lotus iNotes <p>その他の Web ベースの電子メール製品も動作しますが、動作確認は行っていません。</p>

表 30-2 WebVPN リモート システム コンフィギュレーションとエンド 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事項
電子メール プロキシを介した電子メールの使用	<p>インストール済みの SSL 対応メール アプリケーション</p> <p>セキュリティ アプライアンス SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express は TLS をサポートしていません。</p>	<p>サポートされているメール アプリケーションは次のとおりです。</p> <ul style="list-style-type: none"> • Microsoft Outlook • Microsoft Outlook Express バージョン 5.5 および 6.0 • Netscape Mail バージョン 7 • Eudora 4.2 for Windows 2000 <p>その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。</p>
	設定済みのメール アプリケーション	

WebVPN データのキャプチャ

CLI キャプチャ コマンドにより、WebVPN 接続では正しく表示されない Web サイトに関する情報を記録できます。このデータは、Cisco カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。次の各項では、キャプチャ コマンドの使用方法について説明します。

- [キャプチャ ファイルの作成](#)
- [キャプチャ データを表示するためのブラウザの使用](#)



(注)

WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、WebVPN キャプチャを必ずディセーブルにしてください。

キャプチャ ファイルの作成

次の手順を実行して WebVPN セッションに関するデータをファイルにキャプチャします。

- ステップ 1** WebVPN キャプチャ ユーティリティを開始するには、特権 EXEC モードで **capture** コマンドを使用します。

```
capture capture_name type webvpn user webvpn_username
```

パラメータは次のとおりです。

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn_user* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

- ステップ 2** WebVPN ユーザが WebVPN セッションを開始するためにログインします。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

```
no capture capture_name
```

キャプチャ ユーティリティは *capture_name.zip* ファイルを作成し、このファイルはパスワード **koleso** で暗号化されます。

- ステップ 3** .zip ファイルをシスコシステムズに送信するか、Cisco TAC サービス リクエストに添付します。

- ステップ 4** .zip ファイルの内容を確認するには、パスワード **koleso** を使用してファイルを解凍します。

次の例では、*hr* という名前のキャプチャを作成します。これは、*user2* への WebVPN トラフィックを次のようにファイルにキャプチャします。

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
  capture name    hr
  user name      user2
hostname# no capture hr
```

キャプチャ データを表示するためのブラウザの使用

次の手順を実行して WebVPN セッションに関するデータをキャプチャし、これをブラウザに表示します。

- ステップ 1** WebVPN キャプチャ ユーティリティを開始するには、特権 EXEC モードで **capture** コマンドを使用します。

```
capture capture_name type webvpn user webvpn_username
```

パラメータは次のとおりです。

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn_username* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

- ステップ 2** WebVPN ユーザが WebVPN セッションを開始するためにログインします。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

- ステップ 3** ブラウザをオープンし、アドレスを指定するボックスに次のように入力します。

```
https://IP_address またはセキュリティ アプライアンスのホスト名 /webvpn_capture.html
```

キャプチャされたコンテンツが **sniffer** 形式で表示されます。

- ステップ 4** コンテンツをキャプチャし終わったら、コマンドの **no** バージョンを使用してキャプチャを停止します。