CHAPTER 35

クライアントレス SSL VPN のエンドユーザ設定

この項は、エンド ユーザのためのクライアントレス（ブラウザベース）SSL VPN を設定するシステム管理者を対象としています。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、ユーザがクライアントレス SSL VPN 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。ここでは、次の項目について説明します。

- 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
- クライアントレス SSL VPN 機能を使用するためのリモート システムの設定
- クライアントレス SSL VPN データのキャプチャ

（注） 次の説明では、すでにクライアントレス SSL VPN 用にセキュリティ アプライアンスが設定済みと想定しています。

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、クライアントレス SSL VPN、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 35-1 に、クライアントレス SSL VPN 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 35-1　クライアントレス SSL VPN 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	コンピュータを起動するとき
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 プロバイダーに接続するとき
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN セッションを開始するとき
ファイル サーバ	リモート ファイル サーバへのアクセス	クライアントレス SSL VPN 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	クライアントレス SSL VPN 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	クライアントレス SSL VPN 経由でのリモート メール サーバへのアクセス	電子メール メッセージを送受信するとき

セキュリティのヒントの通知

セッションから必ずログアウトするようにユーザに通知してください（クライアントレス SSL VPN からログアウトするには、クライアントレス SSL VPN 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）。

クライアントレス SSL VPN 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。クライアントレス SSL VPN 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。

クライアントレス SSL VPN 機能を使用するためのリモート システムの設定

表 35-2 に、クライアントレス SSL VPN 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。

- クライアントレス SSL VPN の起動
- クライアントレス SSL VPN 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

表 35-2 には、次の項目に関する情報も記載されています。

- 機能ごとのクライアントレス SSL VPN の要件
- クライアントレス SSL VPN がサポートされてい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、クライアントレス SSL VPN ユーザがそれぞれ異なる機能を使用できるようにすることが可能です。表 35-2 では、機能別に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 35-2　クライアントレス SSL VPN 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
クライアントレス SSL VPN 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。 • 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
	クライアントレス SSL VPN がサポートされているブラウザ	次のオペレーティング システムとブラウザでクライアントレス SSL VPN の動作をテスト済みですが、他にも使用可能な製品があります。 • Microsoft Windows XP と Internet Explorer 6.0 または 7.0、あるいは Firefox 1.5 または 2.0 の組み合せ • Microsoft Windows Vista と Internet Explorer 7.0 または Firefox 2.0 の組み合せ • Macintosh OS X と Safari 2.0 または Firefox 2.0 の組み合せ • Linux と Firefox 1.5 または 2.0 の組み合せ
	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。
	クライアントレス SSL VPN の URL	https アドレスの形式は次のとおりです。 https://*address* *address* は、クライアントレス SSL VPN 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（またはロードバランシング クラスタ）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。たとえば、https://10.89.192.163 または https://cisco.example.com のようになります。
	クライアントレス SSL VPN のユーザ名とパスワード	
	（オプション）ローカル プリンタ	クライアントレス SSL VPN 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 35-2　クライアントレス SSL VPN 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
クライアントレス SSL VPN 接続でのフローティング ツールバーの使用		フローティング ツールバーを使用すると、クライアントレス SSL VPN 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。 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。 フローティング ツールバーは、現在のクライアントレス SSL VPN 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、クライアントレス SSL VPN セッションの終了を確認するプロンプトを表示します。 **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（クライアントレス SSL VPN ツールバーでは右クリックがディセーブルになっています）。
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	クライアントレス SSL VPN 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。 クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次の例を参考にしてください。 • クライアントレス SSL VPN のタイトルバーが各 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： 　– Clientless SSL VPN Home ページ上の Enter Web Address フィールドに URL を入力する 　– Clientless SSL VPN Home 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 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。 • 一部の Web サイトがブロックされている • アクセス可能な Web サイトが、Clientless SSL VPN Home ページにリンクとして表示されるサイトに限定される

表 35-2　クライアントレス SSL VPN 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	クライアントレス SSL VPN 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 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。	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。 まれに、JAVA 例外エラーで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。 **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.** クライアントレス SSL VPN 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 35-2　クライアントレス SSL VPN 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
	設定済みのクライアント アプリケーション（必要な場合） **（注）** Microsoft Outlook クライアントの場合、この設定手順は不要です。 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。 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。 • 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。	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。 **1.** リモート システムでクライアントレス SSL VPN を起動し、Clientless SSL VPN Home ページで 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。 **2.** 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。 **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、クライアント アプリケーションによって異なります。
	（注） クライアントレス SSL VPN で実行されているアプリケーションで URL（電子メール内の URL など）をクリックしても、クライアントレス SSL VPN ではそのサイトは開きません。クライアントレス SSL VPN でこのようなサイトを開くには、Enter (URL) Address フィールドに URL をカット アンド ペーストします。	

表 35-2　クライアントレス SSL VPN 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
Application Access を介した電子メールの使用	Application Access の要件を満たす（「アプリケーションの使用」を参照）	電子メールを使用するには、Clientless SSL VPN Home 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。
	（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たり、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クライアントレス SSL VPN を再起動します。	
	その他のメール クライアント	Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。 クライアントレス SSL VPN 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。
電子メール プロキシを介した電子メールの使用	インストールされている Web ベースの電子メール製品	サポートされている製品は次のとおりです。 • Outlook Web Access 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。 • Louts iNotes 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。
電子メール プロキシを介した電子メールの使用	インストール済みの SSL 対応メール アプリケーション 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。	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。 • 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 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。
	設定済みのメール アプリケーション	

クライアントレス SSL VPN データのキャプチャ

CLI キャプチャ コマンドにより、クライアントレス SSL VPN 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）　クライアントレス SSL VPN 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クライアントレス SSL VPN 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　クライアントレス SSL VPN 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　ユーザがログインするとクライアントレス SSL VPN セッションが開始します。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、クライアントレス SSL VPN セッションに関するデータをキャプチャし、ブラウザに表示します。

ステップ 1　クライアントレス SSL VPN 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　ユーザがログインするとクライアントレス SSL VPN セッションが開始します。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://*asdm_enabled_interface_of_the_security_appliance***:***port***/admin/capture/***capture_name*/pcap

次のサンプル コマンドを実行すると、hr という名前のキャプチャが表示されます。

https://192.0.2.1:60000/admin/capture/hr/pcap

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えたら、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。