



クライアントレス **SSL VPN** リモート ユーザ

2013年9月13日

この章は、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。

- 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 の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 ASA 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、固有のユーザ名、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。必要なアクセス権があることを確認してください。

表 17-1 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 17-1 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
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

表 17-1 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 (続き)

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
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

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コンピュータやワークステーションと ASA 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 ASA 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 の機能を使用するためのリモートシステムの設定

表 17-2 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、または電子メールプロキシ

表 17-2 には、次の項目に関する情報も記載されています。

- クライアントレス SSL VPN の要件（機能別）
- 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がある情報
- 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 アカウントを異なって設定したことにより、クライアントレス SSL VPN ユーザがそれぞれに使用できる機能が異なる可能性があります。表 17-2 に、ユーザ アクティビティ別の情報をまとめています。使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 17-2 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

タスク	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。 <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
	クライアントレス SSL VPN がサポートされているブラウザ	クライアントレス SSL VPN には、次のブラウザを推奨します。他のブラウザでは、クライアントレス SSL VPN 機能が完全にサポートされていない可能性があります。 <p>Microsoft Windows の場合：</p> <ul style="list-style-type: none"> • Internet Explorer 8 • Firefox 8 <p>Linux の場合：</p> <ul style="list-style-type: none"> • Firefox 8 <p>Mac OS X の場合：</p> <ul style="list-style-type: none"> • Safari 5 • Firefox 8
	ブラウザでイネーブルにされているクッキー	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。 <code>https://address</code> <i>address</i> は、クライアントレス SSL VPN がイネーブルになっている ASA（またはロード バランシング クラスター）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、 <code>https://10.89.192.163</code> または <code>https://cisco.example.com</code> 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 17-2 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)


タスク	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		<p>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。</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、ASA によってクライアントレス SSL VPN セッションを閉じることを求めるメッセージが表示されます。</p> <p></p> <p>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 を押した状態で V を押します (クライアントレス SSL VPN ツールバーでは、右クリックはイネーブルになっていません)。</p>

表 17-2 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)

タスク	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
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>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。</p> <p>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。次に例を示します。</p> <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> - [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。 <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。 • 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。
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。

表 17-2 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)


タスク	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
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) Mac 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、Oracle Java Runtime Environment (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にアクセスできなく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	ユーザは、DNS 名を使用してサーバを指定する場合、hosts ファイルを変更するのに必要になるため、コンピュータに対する管理者アクセス権が必要になります。
	インストール済みの Oracle 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設定されています。	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、インストールを開始できるサイトがユーザに示されます。 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。 <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. 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 17-2 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)

タスク	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"> 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。
	<p>(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。</p>	

表 17-2 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)

タスク	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	<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。</p> <p>他の電子メール クライアント</p>	<p>仕様または使用上の推奨事項</p> <p>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。これにより、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>クライアントレス SSL VPN は、Lotus Notes や 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>
Web アクセス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	<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 8.x 以上、または Firefox 8 で OWA を使用してください。</p> • Lotus Notes <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>
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>ASA 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 では TLS はサポートされません。</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 <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	

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、シスコ 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、ASA 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、キャプチャを必ずオフに切り替えます。

キャプチャ ファイルの作成

手順の詳細

- 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 モードから **capture** コマンドを実行します。

```
capture capture-name type webvpn user csslvpn-username
```

値は次のとおりです。

- *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。
- *csslvpn-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** 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* へのクライアントレス SSL VPN 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

手順の詳細

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 モードから **capture** コマンドを実行します。

capture capture-name type webvpn user csslvpn-username

値は次のとおりです。

- *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。
- *csslvpn-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 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 ブラウザを開き、[Address] ボックスに次のように入力します。

https://IP address or hostname of the ASA/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 キャプチャ コンテンツを調べ終わったら、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。
