クライアントレス SSL VPN リモート ユーザー

（注） **シスコは、ASA バージョン 9.17(1) で有効なクライアントレス SSL VPN の非推奨機能を発表しました。**9.17(1) より前のリリースでは、限定的なサポートが継続されます。より堅牢で新しいソリューション（たとえば、リモート Duo ネットワークゲートウェイ、AnyConnect、リモートブラウザの分離機能など）への移行オプションに関する詳細なガイダンスを提供します。

この章では、ユーザー 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、ユーザーがクライアントレス SSL VPN の使用を開始できるようにします。内容は次のとおりです。

（注） ASA がクライアントレス SSL VPN 用に設定されていることを確認します。

クライアントレス SSL VPN リモート ユーザー

（注） **シスコは、ASA バージョン 9.17(1) で有効なクライアントレス SSL VPN の非推奨機能を発表しました。**9.17(1) より前のリリースでは、限定的なサポートが継続されます。より堅牢で新しいソリューション（たとえば、リモート Duo ネットワークゲートウェイ、AnyConnect、リモートブラウザの分離機能など）への移行オプションに関する詳細なガイダンスを提供します。

この章では、ユーザー 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、ユーザーがクライアントレス SSL VPN の使用を開始できるようにします。内容は次のとおりです。

（注） ASA がクライアントレス SSL VPN 用に設定されていることを確認します。

ユーザー名とパスワード

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ーが、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SSLVPN、メールサーバー、ファイルサーバー、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。ユーザーはさまざまなコンテキストで認証を行うために、固有のユーザー名、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。

次の表に、クライアントレス SSL VPN ユーザーが理解しておく必要のあるユーザー名とパスワードのタイプを示します。

表 *1:* クライアントレス *SSL VPN* ユーザーに通知するユーザー名とパスワード

ログイン ユーザー名/ パスワードのタイプ		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
Internet Service Provider：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
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 セッションするとき
File Server	リモート ファイル サーバーへのアクセス	クライアントレス SSL VPN ファイルグ機能を使用して、リモート ファイ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ーへのアクセス	クライアントレス SSL VPN Web ブラ能を使用して、保護されている内部にアクセスするとき
メール サーバー	クライアントレスSSLVPN経由によるリモート メール サーバーへのアクセス	電子メール メッセージの送受信

セキュリティ ヒントの通知

次のセキュリティのヒントを通知してください。

- クライアントレスSSL VPNセッションから必ずログアウトします。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になるわけではありません。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、ユーザーが 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リソース）にアクセスする場合、企業の ASA から目的の Web サーバー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

次の表に、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連するタスク、タスクの要件と前提条件、および推奨される使用法を示します。

各ユーザー アカウントを異なる設定にしたことにより、クライアントレス SSL VPN ユーザー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。この表では、情報をユーザー アクティビティ別にまとめています。

表 *2*: クライアントレス *SSL VPN* リモート システムの設定およびエンド ユーザーの要件

タスク	リモート システムまたはエンド ユーザーの要件	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	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。 Microsoft Windows の場合： • Internet Explorer 8 • Firefox 8 Linux の場合： • Firefox 8 Mac OS X の場合： • 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 フォワーディング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 ASA（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。

タスク	リモート システムまたはエンド ユーザーの要件	仕様または使用上の推奨事項
	クライアントレス SSL VPN のユーザー名とパスワード	
	（任意）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。
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、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。 **ヒント** テキスト フィールドにテキストを貼り付けるには、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、右クリックは有効ではありません）。

タスク	リモート システムまたはエンド ユーザーの要件	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 サイトのユーザー名とパスワード	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 ヒントの通知 （2 ページ）」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、ユーザー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。 • 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。

タスク	リモート システムまたはエンド ユーザーの要件	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 サーバーのサーバー名とパスワード	—
	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、およびサーバー名	ユーザーは、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ーに保存される可能性があります。

タスク	リモート システムまたはエンド ユーザーの要件	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 フォワーディング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、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であるため、ユーザーがパブリック リモート システムから接続した場合は、アプリケーションを使用できない可能性があります。	
	アプリケーションを使用した後、ユーザーは[**Close**]アイコンをクリックして必ず[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	ユーザーは、DNS 名を使用してサーバーを指定する場合、ホスト 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。
	Java Runtime Environment（JRE）がインストール済み。 ブラウザで JavaScript をイネーブルにする必要があります。デフォルトでは有効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、ユーザー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 フォワーディング 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 フォワーディング Java アプレットを起動します。

タスク	リモート システムまたはエンド ユーザーの要件	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] にサーバー 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ーの 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、使用するサーバー名を確認し、このサーバー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。	
アプリケーションアクセス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。これにより、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 サーバー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。	
	他の電子メール 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。

タスク	リモート システムまたはエンド ユーザーの要件	仕様または使用上の推奨事項
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	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 8.x 以上、または Firefox 8 で OWA を使用してください。 • Lotus Notes 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 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。	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 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 capture コマンドを使用すると、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 （11 ページ）
- ブラウザによるキャプチャ データの表示 （11 ページ）

（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 のパフォーマンスが影響を受けます。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

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してパケットをキャプチャします。

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

- *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ー名です。

例：

```
hostname# capture hr type webvpn user user2
```

ステップ 2 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*

例：

```
hostname# no capture hr
```

キャプチャ ユーティリティは *capture-name*.zip ファイルを作成します。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。

ブラウザによるキャプチャ データの表示

手順

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します。

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

- *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ー名です。

例：

```
hostname# capture hr type webvpn user user2
```

ステップ 2 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 3 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*

例：

```
hostname# no capture hr
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。