クライアントレス SSL VPN の概要

（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。

クライアントレス SSL VPN の概要

クライアントレス SSL VPN を使用すると、エンド ユーザーは SSL 対応 Web ブラウザを使用して、任意の場所から社内ネットワークのリソースに安全にアクセスできます。ユーザーは、まず、クライアントレス SSL VPN ゲートウェイで認証し、事前設定されたネットワーク リソースにアクセスできるようにします。

（注） クライアントレス SSL VPN がイネーブルになっている場合、セキュリティ コンテキスト（ファイアウォール マルチモードとも呼ばれる）とアクティブ/アクティブ ステートフル フェールオーバーはサポートされません。

クライアントレス SSL VPN は、ソフトウェアまたはハードウェア クライアントを必要とせずに、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを作成します。HTTP 経由でインターネットに接続できるほとんどのデバイスから、幅広い Web リソースと、Web 対応およびレガシー アプリケーションに安全かつ簡単にアクセスできます。次の内容で構成されています。

- 内部 Web サイト
- Web 対応アプリケーション

- NT/Active Directory ファイル共有
- Microsoft Outlook Web Access Exchange Server 2010 および 2013。
- Microsoft Web App to Exchange Server 2010（8.4(2) 以降において）
- Application Access（他の TCP ベースのアプリケーションにアクセスするためのスマートトンネルまたはポート転送）

クライアントレス SSL VPN は Secure Sockets Layer（SSL）プロトコルとその後継の Transport Layer Security（SSL/TLS1）を使用し、内部サーバーとして設定されている特定のサポート対象内部リソースと、リモート ユーザーとの間にセキュアな接続を実現します。ASA はプロキシで処理する必要がある接続を認識し、HTTP サーバーは認証サブシステムと対話してユーザーを認証します。

ネットワーク管理者は、クライアントレス SSL VPN セッションのユーザーに対してグループ単位でリソースへのアクセスを提供します。ユーザーは、内部ネットワーク上のリソースに直接アクセスすることはできません。

クライアントレス SSL VPN の前提条件

ASA 上のクライアントレス SSL VPN でサポートされるプラットフォームとブラウザについては、『サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ』を参照してください。

クライアントレス SSL VPN に関する注意事項と制約事項

- ActiveX ページでは、ActiveX リレーをイネーブルにするか、関連するグループ ポリシーに **activex-relay** を入力しておくことが必要です。あるいは、スマート トンネル リストをポリシーに割り当て、エンドポイント上のブラウザプロキシ例外リストにプロキシが指定されている場合、ユーザーはそのリストに「shutdown.webvpn.relay.」エントリを追加する必要があります。
- ASA では、Mozilla Firefox、MS Edge、Google Chrome、macOS、または Linux から Windows 共有（CIFS）Web フォルダへのクライアントレス アクセスはサポートされていません。
- DoD Common Access Card および SmartCard を含む証明書認証は、Safari キーチェーンだけで動作します。
- クライアントレス接続用に信頼できる証明書をインストールしても、クライアントには信頼できない証明書の警告が表示されることがあります。
- ASA は、クライアントレス SSL VPN 接続用の DSA 証明書をサポートしません。RSA 証明書はサポートされます。
- 一部のドメインベースのセキュリティ製品には、ASA から送信された要求を超える要件があります。

- コンフィギュレーション制御の検査機能およびモジュラ ポリシー フレームワークにおけるその他の検査機能はサポートされません。
- グループ ポリシーの **vpn-filter** コマンドは、クライアントベースのアクセス用であり、サポートされません。グループ ポリシーのクライアントレス SSL VPN モードの**フィルタ**は、クライアントレス ベースのアクセス用です。
- NAT および PAT はクライアントに適用可能ではありません。
- ASA は、**police** や **priority-queue** などの QoS レート制限コマンドの使用をサポートしません。
- ASA は、接続制限の使用、スタティックまたはモジュラ ポリシー フレームワークの **set connection** コマンドを使用した確認をサポートしません。
- AnyConnect は Web コンテンツに依存せずに下位のネットワーク層で動作するため、クライアントレス WebVPN でサポートされていないと思われる Web アプリケーションにアクセスするように ASA で AnyConnect を設定することを推奨します。
- クライアントレス SSL VPN の一部のコンポーネントには、Java Runtime Environment（JRE）が必要です。macOS v10.12 以降では、Java はデフォルトでインストールされません。macOS での Java のインストール方法については、http://java.com/en/download/faq/java_mac.xml を参照してください。
- クライアントレス VPN セッションを開始すると、RADIUS アカウンティング開始メッセージが生成されます。クライアントレス VPN セッションにはアドレスが割り当てられないため、開始メッセージには Framed-IP-Address が含まれません。レイヤ 3 VPN 接続がクライアントレス ポータルページから順番に開始されるとアドレスが割り当てられ、暫定アップデート アカウンティング メッセージで RADIUS サーバーに報告されます。weblaunch 機能を使用してレイヤ 3 VPN トンネルが確立される場合、同様の RADIUS の動作が期待できます。この状況では、ユーザーが認証された後、レイヤ 3 トンネルが確立される前にアカウンティング開始メッセージがフレーム化 IP アドレスなしで送信されます。レイヤ 3 トンネルが確立されると、この開始メッセージに暫定アップデート メッセージが続きます。
- HTML ページは RFC 2616 に準じている必要があります。ヘッダーの後の空の行は、本文の開始と解釈されます。したがって、ヘッダー間に空の行を挿入すると、一部のヘッダーが本文に表示され、ユーザーがページの問題を修正するためにウィンドウを更新する必要が生じる場合があります。
- Java コード処理に使用されるクライアントレス WebVPN Java リライタは、Oracle Forms をサポートしていません。
- クライアントレス WebVPN リライタは、実行時に動的に設定されるため、JavaScript オブジェクトのブラケット表記の割り当てを検出できません。
- クライアントレス WebVPN は、サーバーの応答に含まれるチャンクサイズと CRLF 間のスペースをサポートしていません。これは、ASA がチャンクサイズのスペースを予期しておらず、チャンクをまとめることができないためです。

- コンテンツ セキュリティ ポリシー（CSP）はサポートされていません。
- クライアントレス WebVPN リライタを使用すると、Angular のカスタムイベントリスナーおよびロケーション変更が正しく機能しない場合があります。
- クライアントレス WebVPN は、サーバー側の Cross-Origin Resource Sharing（CORS）フィルタをサポートしていません。
- クライアントレス WebVPN リライタは、現在、HTML5 および Javascript Blog API をサポートしていません。
- WebVPN アーキテクチャに従い、Fetch API はサポートされていません。
- クライアントレス WebVPN は、認証時に MDM 属性を RADIUS サーバーと共有しません。
- クライアントレス ポータル用に設定された複数のグループ ポリシーがある場合は、ログイン ページのドロップダウンに表示されます。リストにある最初のグループ ポリシーで証明書が必要な場合は、ユーザーはマッチング証明書が必要です。グループポリシーの一部が証明書を使用しない場合、非証明書ポリシーを最初に表示するには、リストを設定します。また、「0-Select-a-group」の名前でダミー グループ ポリシーを作成することもできます。

ヒント グループポリシーの名前をアルファベット順に付けることで、最初に表示されるポリシーを制御できます。また、ポリシーの先頭に数字を付けることもできます。たとえば、1-AAA、2-Certificate とします。

- 別のサーバー上のページへのリンクは ASA からルーティング可能である必要があります。それ以外の場合、ユーザーに次のエラーが表示されることがあります。リンクが使用可能で、アクセス制御ルール、SSL 構成、またはその他のファイアウォール機能によってブロックされていないこと、およびサーバーへのルートがあることを確認します。

```
Connection failed, Server "<DNS name>" unavailable.
```

クライアントレス SSL VPN のライセンス

AnyConnect セキュア モビリティ クライアントを使用するには、AnyConnect Plus および Apex ライセンスを購入する必要があります。必要なライセンスは、使用する予定の AnyConnect VPN Client および Secure Mobility の機能と、サポートするセッションの数によって異なります。これらのユーザーベースのライセンスには、一般的な BYOD のトレンドに合わせたサポートとソフトウェア更新へのアクセスが含まれます。

AnyConnect 4.4 ライセンスは、ASA（および ISR、CSR、ASR）で使用され、また、Identity Services Engine（ISE）、クラウド Web セキュリティ（CWS）、Web セキュリティ アプライアンス（WSA）などの非 VPN ヘッドエンドでも使用されます。ヘッドエンドに関係なく一貫したモデルが使用されるため、ヘッドエンドの移行が発生した場合も影響はありません。

AnyConnect のライセンス モデルについての詳細は、http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf を参照してください。

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。