

# セキュアアクセスRA-VPN IPv6接続障害 – プロトコル設定の問題

## お問い合わせ内容

IPv6を介したCisco Secure AccessへのRA-VPN接続が確立できず、Cisco Secure Client UIに一般的な接続失敗メッセージが表示されます。この問題は、既存のRA-VPNプロファイルを使用したIPv6ベースのリモートアクセス接続のテストに影響を与えます。調査によると、SSE RA-VPNプロファイルではIPv6接続のプロトコルフィールドが正しく設定されていません。

## 環境

- テクノロジー：ソリューションサポート（SSPT – 契約が必要）
- サブテクノロジー：セキュアアクセス – セキュアクライアントリモートアクセス（VPN、ポスチャ、プライベートリソース）
- ソフトウェアバージョン：すべて
- Cisco Secure ClientがIPv6 RA-VPN接続を試みている
- Cisco Secure Access SSEプラットフォーム
- 既存のRA-VPNプロファイル設定

## 解決策

IPv6 RA-VPN接続障害を解決するには、RA-VPNプロファイルでIP Protocol Supported設定が正しく設定されている必要があります。IPv6サポートを有効にするには、次の手順に従います。

### ステップ1：クライアント設定へのアクセス

Cisco Secure Access管理インターフェイスで、Client Settingsセクションに移動します。

### ステップ2：管理者設定の構成

Client Settingsで、Administrator Settingsセクションを見つけてアクセスします。

### ステップ3：サポートされるIPプロトコルの設定

IP Protocol Supportedドロップダウンを設定してIPv6をサポートする。この設定は、クライアント接続に対してRA-VPNプロファイルがサポートするIPプロトコルを制御します。

### ステップ4：設定の保存

更新されたRA-VPNプロファイル設定を保存して、IPv6プロトコル設定が適用されていることを確認します。

### ステップ5：接続のテスト

Cisco Secure Clientを使用してIPv6 RA-VPN接続を再テストし、接続が正常に確立されたことを確認します。

## 原因

IPv6 RA-VPN接続障害の根本原因は、RA-VPNプロファイルのIP Protocol Supported設定がIPv6接続をサポートするように設定されていないことです。SSE RA-VPNプロファイルでは、IPv6接続を有効にするためにプロトコルフィールドを明示的に設定する必要があります。この設定が正しく設定されていないと、Cisco Secure ClientはCisco Secure AccessプラットフォームへのIPv6ベースのVPN接続を確立できません。

## 関連コンテンツ

- [シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。