

# Secure Clientの「Hostscan CSD Prelogin Verification Failed」エラー

## 内容

---

## お問い合わせ内容

Windows 11デバイスでCisco Secure Clientを使用してVPNに接続しようとする、と、「Hostscan CSD prelogin verification failed」というエラーメッセージが表示されます。このエラーは、ログインプロンプトが表示される前に発生し、ユーザはVPN接続にアクセスできません。同じユーザが、同じクレデンシャルとVPNプロファイルを使用して別のデバイスからVPNに正常に接続できます。これは、クレデンシャルに関連する問題ではなく、デバイス固有の問題であることを示しています。

その他に確認されたエラーログエントリは次のとおりです。

- CONNECTIFC\_ERROR\_FILE\_OPEN\_FAILED(リターンコード : -30015466 / 0xFE360016)
- ホストスキャン処理に失敗しました
- ネットワークまたはPCの問題により、接続に失敗しました

ユーザは、ポスチャが有効になっていない他のVPNプロファイルには接続できましたが、ポスチャが有効になっているプロファイルには接続できませんでした。以前は、設定に対する既知の変更を行わずにセットアップが動作していました。

## 環境

- Cisco Secure Clientバージョン5.1.7.80
- オペレーティングシステム : Windows 11
- ポスチャリングが有効なVPNプロファイル
- 問題はデバイス固有であり、特定の1つのデバイス上の1人のユーザだけに影響する

- Cisco Bug ID CSCwk54713に関連

## 解決策

この問題の解決には、Cisco Secure Clientの完全なクリーンアンインストールの実行と、ソフトウェアの再インストールが含まれます。標準的なアンインストールおよび再インストール方法では、レジストリエントリの破損やファイルの残存が原因で問題が解決されない場合があります。

### ステップ1：サードパーティサービスを無効にする

プロキシサービスを含め、Msconfigのすべてのサードパーティサービスを無効にし（使用可能な場合）、Cisco Secure Clientモジュールのみをアクティブのままにします。

### ステップ2:Microsoftツールを使用したアンインストールのクリーンアップ

Microsoft Program Install and Uninstall Troubleshooterツールを使用して、該当するデバイスからすべてのシスコモジュールを削除します。このツールは、標準的なWindowsアンインストール方法よりも詳細なアンインストール方法を提供します。

[プログラムのインストールや削除を妨げる問題を修正](#)します。

### ステップ3：ファイルの手動クリーンアップ

アンインストール後、残りのシスコフォルダ、ファイル、実行ファイル、およびDLLファイルを手動で確認し、次のディレクトリから削除します。

```
C:\Program Files (x86)\Cisco  
C:\ProgramData\Cisco\  
C:\Users\
```

これらの場所にある残りのファイルとフォルダは、アンインストール処理の後も常に残るとは限らないため、削除してください。

#### ステップ4：レジストリのクリーンアップ

古いCisco Secure Clientエントリの次のレジストリパスを確認し、エントリがある場合はそれを削除します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco  
HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco
```

#### ステップ5：デバッグロギングの有効化（オプション）

さらにトラブルシューティングが必要な場合は、debuglogconfig.jsonファイルをコピーしてCurlロギングを有効にします。

```
{  
  "web_helper" : 3,  
  "vpn_ipsec_ikev2" : 3,  
  "vpn_curl" : 3,  
  "vpn_state" : 3  
}
```

このディレクトリに移動します。

```
C:\ProgramData\Cisco\Cisco Secure Client
```

#### ステップ6：システムの再起動

エンドポイントをリブートして、すべての変更が反映され、残りのプロセスまたはレジストリロックスがクリアされることを確認します。

## ステップ7: Cisco Secure Clientを再インストールする

Cisco Secure Clientの導入前パッケージをインストールするか、Intuneなどの管理ツールを使用して自動インストールを実行します。インストールが正常に完了したことを確認してから、次に進みます。

## ステップ8: VPN接続をテストする

以前に失敗していたVPNプロファイルへの接続を試みます。問題が解決しない場合は、さらなる分析のために新しいDARTバンドルを生成します。



注意：可能です。ここで説明する詳細には、実行すると重大な影響を与える可能性のあるプロシージャまたはコマンドが含まれています。これらの手順またはコマンドを実行または推奨する前に、SMEまたはビジネスユニットによって評価されていることを確認してください。

---

## 原因

この問題は、破損したレジストリエントリまたはサードパーティ製ソフトウェアの干渉によって、ホストスキャンライブラリおよび実行の起動や更新が適切に行われなかったことが原因です。この破損は、ポスチャが有効なVPNプロファイルに必要なCSD(Cisco Security Desktop)のログイン前検証プロセスに影響を与えます。通常、破損はデバイスレベルで発生し、同じユーザが他のデバイスから正常に接続できる理由を説明します。標準のアンインストール方法では、破損したコンポーネントがすべて必ず削除されるわけではなく、ファイルとレジストリエントリの手動クリーンアップが必要になります。

## 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。