Cisco Secure Client のトラブルシューティング

トラブルシューティングに必要な情報の収集

統計詳細情報の表示

管理者またはエンドユーザーは、現在の Cisco Secure Client セッションの統計情報を表示できます。

ステップ 1 Windows では、**[詳細ウィンドウ（Advanced Window）] > [統計情報（Statistics）] > [VPN ドロワ（VPN drawer）]** に移動します。Linux では、ユーザ GUI 上の [詳細（Details）] ボタンをクリックします。

ステップ 2 クライアント コンピュータにロードされたパッケージに応じて、次のオプションから選択します。

- [統計情報のエクスポート（Export Stats）]：後で分析およびデバッグできるようにテキスト ファイルに接続統計情報を保存します。
- [リセット（Reset）]：接続情報をゼロにリセットします。Cisco Secure Client がすぐに新しいデータの収集を開始します。

- [診断（Diagnostics）]：Cisco Secure Client Diagnostics and Reporting Tool（DART）ウィザードを起動します。ウィザードは、クライアント接続を分析およびデバッグできるように、指定されたログファイルと診断情報をバンドルします。

トラブルシューティング用にデータを収集するための DART の実行

DART は Cisco Secure Client Diagnostics and Reporting Tool の略で、Cisco Secure Client のインストールと接続に関する問題のトラブルシューティング用データの収集に使用できます。DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。デフォルトでは、データ収集は米国地域の形式（MM/DD/YY）に基づいています。

DART ウィザードは、Cisco Secure Client を実行するデバイス上で実行されます。DART は Cisco Secure Client から起動できます。または Cisco Secure Client を使用せずにそれ自体を起動できます。

（注） DART でログを収集するには、macOS、Ubuntu 18.04、および Red Hat 7 の管理者権限が必要です。

また、ISE ポスチャの場合のみにおいて、ISE ポスチャ クラッシュの発生直後、またはエンドポイントが準拠しなくなったときに、DART が設定されている場合は自動的に DART を収集できます。自動 DART を有効にするには、DARTCount をゼロを除くすべての値として設定します。0 に設定すると、この機能は無効になります。自動 DART を有効にすると、時間によるデータ損失を防止できます。次の場所に自動収集 DARTS を収集します。

- **Windows**：%LocalAppData%\Cisco\Cisco Secure Client
- **macOS**：~/.cisco/iseposture/log

次のオペレーティング システムがサポートされています。

- Windows
- macOS
- Linux

ステップ 1 DART を起動します。

- Windows デバイスの場合は、Cisco Secure Client を起動します。
- Linux デバイスの場合は、**[アプリケーション（Applications）]** > **[インターネット（Internet）]** > **[Cisco DART]** を選択します。

  または /opt/cisco/anyconnect/dart/dartui を選択します。

- macOS デバイスの場合、**[アプリケーション（Applications）]** > **[Cisco]** > **[Cisco DART]** を選択します。

ステップ 2 歯車アイコンをクリックしてから、[診断（Diagnostics）] をクリックします。

ステップ 3 [デフォルト（Default）] または [カスタム（Custom）] のバンドル作成を選択します。

- [デフォルト（Default）] : Cisco Secure Client ログファイル、コンピュータに関する一般情報、および DART ツールが実行した内容と実行しなかった内容の概要などの一般的なログファイルと診断情報を含みます。バンドルのデフォルト名は `DARTBundle.zip` であり、このバンドルはローカルデスクトップに保存されます。
- [カスタム（Custom）] : バンドルに含めるファイル（またはデフォルト ファイル）、およびバンドルの保存場所を指定できます。

  Linux および macOS での成功したルートおよびフィルタリングの変更がログから除外されるようになり、重要なイベントに注意しやすくなります。そうでない場合、syslog のイベント レートの制限により、重要なイベントがドロップして見落とされる可能性があります。また、キャプチャフィルタ処理設定を使用すると、Cisco Secure Client のフィルタ処理構成ファイルだけでなく、macOS のシステム構成ファイルも表示できるようになります。Linux の場合、これらの設定のほとんどは DART ツールが sudo を介して実行されている場合以外アクセスが制限されているにもかかわらず、iptables および ip6tables の出力が DART に表示されます。

（注） macOS のオプションは、[デフォルト（Default）] のみです。バンドルに含めるファイルは、カスタマイズできません。

（注） [カスタム（Custom）] を選択すると、バンドルに含めるファイルを指定でき、また、ファイルに対して異なる保存場所を指定できます。

ステップ 4 DART がデフォルトリストのファイル収集に時間がかかっていると思われる場合は、[キャンセル（Cancel）] をクリックし、DART を再実行して、[カスタム（Custom）] を選択して含めるファイルを減らします。

ステップ 5 [デフォルト（Default）] を選択すると、DART はバンドルの作成を開始します。[カスタム（Custom）] を選択した場合、ウィザードのプロンプトに従って、ログ、プリファレンス ファイル、診断情報、およびその他のカスタマイズを指定します。

DART で UDID を公開する

DART CLI 内では、クライアントの固有デバイス識別子（UDID) を表示できます。たとえば、Windows で、dartcli.exe（C:\Program Files\Cisco\Cisco Secure Client）が含まれているフォルダに移動し、 **dartcli.exe -u** または **dartclie.exe udid** を入力します。

インストールまたはアンインストールの問題についてデータを収集するためのログの収集（Windows）

Cisco Secure Client のインストールまたはアンインストールに失敗した場合は、DART コレクションはこの状況を診断しないため、ログを収集する必要があります。

Cisco Secure Client ファイルを解凍したのと同じディレクトリで、msiexec コマンドを実行します。

- インストールに失敗した場合は、次のように入力します。

```
C:\temp>msiexec \i cisco-secure-client-win-version-predeploy-k9.msi \lvx
c:\Temp\ac-install.log?
```

ここで *c:/temp/ac-install.log?* は、任意のファイル名にすることができます。

- アンインストールに失敗した場合は、次のように入力します。

```
c:\temp>msiexec \x cisco-secure-client-win-version-predeploy-k9.msi /lvx
c:\Temp\ac-uninstall.log?
```

ここで *c:/temp/ac-uninstall.log?* は、任意のファイル名にすることができます。

（注） アンインストールに失敗した場合は、現在インストールされているバージョン固有の MSI を使用する必要があります。

上記と同じコマンドを変更して、正しくインストールまたはアンインストールされなかった Windows のすべてのモジュールに関する情報をキャプチャすることもできます。

コンピュータ システム情報の取得

Windows の場合は、**msinfo32 /nfo c:\msinfo.nfo** と入力します。

systeminfo ファイル ダンプの取得

Windows の場合、**systeminfo** コマンドを使用して情報を収集し、txt ファイル `systeminfo > c:\temp\sysinfo.txt` に保存します。

レジストリ ファイルの確認

次の SetupAPI ログ ファイル内のエントリは、ファイルが見つからないことを示しています。

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce レジストリ キーが存在することを確認してください。このレジストリ キーが存在しない場合、すべての INF インストール パッケージが禁止されます。

Cisco Secure Client ログファイルの場所

ログは、次のファイル内に保持されます。

- Windows：\Windows\Inf\setupapi.app.log または \Windows\Inf\setupapi.dev.log

（注） Windows では、隠しファイルを表示する必要があります。

展開は手動であるため、Web ポータルでインストーラーファイルをダウンロードし、独自のログファイル名を割り当てることを選択できます。

。

アップグレードがゲートウェイからプッシュされた場合、ログファイルは次の場所にあります。

%WINDIR%\TEMP\cisco-secure-client-win-<version>-core-vpn-webdeploy-k9-install-yyyyyyyyyyyyy.log

インストールするクライアントのバージョンの最新ファイルを取得します。*xxx* はバージョンによって異なり、*yyyyyyyyyyyyy* はインストールの日時を示します。

- macOS（10.12 以降）：ロギングデータベース。「コンソール」アプリまたはログコマンドを使用して、VPN、DART、または Umbrella のログを照会します。
- macOS（レガシーファイルベースのログ）：/var/log/system.log（他のすべてのモジュール）
- Linux Ubuntu：/var/log/syslog
- Linux Red Hat：/var/log/messages

DART を実行してトラブルシューティング データをクリアする

Windows では、DART ウィザードを使用し、生成されたログをクリアできます。

ステップ 1 管理者権限で DART を起動します。

ステップ 2 [**すべてのログをクリア**（Clear All Logs）] をクリックし、ログの消去を開始します。

Cisco Secure Client 接続または接続解除の問題

Cisco Secure Client が初期接続を確立しないか、接続解除しない

問題：Cisco Secure Client が初期接続を確立しないか、または Cisco Secure Client ウィンドウで [接続解除（Disconnect）] をクリックすると予期しない結果が得られます。

解決策：次の点をチェックします。

- ネットワークまたは WiFi アダプタのドライバが古いため、断続的な接続の問題が発生する可能性があります。ドライバをアップグレードして、再試行してください。
- Citrix Advanced Gateway Client Version 2.2.1 を使用している場合は、CtxLsp.dll の問題が Citrix によって解決されるまで Citrix Advanced Gateway Client を削除してください。
- AT&T Sierra Wireless 875 カードと AT&T Communication Manager Version 6.2 または 6.7 を使用している場合は、次の手順に従って問題を修正してください。
  1. Aircard でアクセラレーションを無効にします。
  2. [ツール（Tools）] > [設定（Settings）] > [アクセラレーション（Acceleration）] > [スタートアップ（Startup）] から AT&T Communications Manager を起動します。
  3. **manual** と入力します。
  4. [停止（Stop）] をクリックします。
- Cisco Secure Firewall ASA からコンフィギュレーション ファイルを取得し、次のようにして接続失敗の兆候を探します。
  - Cisco Secure Firewall ASA コンソールから **write net x.x.x.x:ASA-Config.txt** と入力します。この x.x.x.x はネットワーク上の TFTP サーバーの IP アドレスです。
  - Cisco Secure Firewall ASA コンソールから、show running-config と入力します。設定を切り取ってテキスト エディタに貼り付け、これを保存します。
- Cisco Secure Firewall ASA イベントログを表示します。
  1. Cisco Secure Firewall ASA コンソールで、次の行を追加し、ssl、webvpn、anyconnect、および auth のイベントを調べます。

     ```
     config terminal
     logging enable
     logging timestamp
     logging class auth console debugging
     logging class webvpn console debugging
     logging class ssl console debugging
     logging class anyconnect console debugging
     ```

  2. Cisco Secure Client の接続を試行し、接続エラーが発生した場合は、そのコンソールのログ情報を切り取ってテキストエディタに貼り付け、保存します。
  3. **no logging enable** と入力し、ロギングを無効にします。
- Windows イベントビューアを使用してクライアントコンピュータから Cisco Secure Client ログを取得します。
  1. [スタート（Start）] > [ファイル名を指定して実行（Run）] の順に選択し、**eventvwr.msc /s** と入力します。
  2. [アプリケーションとサービスログ（Applications and Services Logs ）]（Windows 7）で、Cisco Secure Client を見つけ、[ログファイルの名前を付けて保存...（Save Log File As...）] を選択します。。

3. ファイル名（たとえば、 `CiscoSecureClientLog.evt`）を割り当てます。`.evt` ファイル形式を使用する必要があります。

- Windows 診断デバッグ ユーティリティを変更します。

1. WinDbg のマニュアルに記載されているとおりに vpnagent.exe プロセスを接続します。
2. IPv6/IPv4 IP アドレス割り当てで競合が存在するかどうかを確認します。特定済みの競合がないか、イベント ログで確認します。
3. 競合が特定されていた場合は、使用するクライアント コンピュータのレジストリにルーティングのデバッグを追加します。このような競合は、Cisco Secure Client イベントログで次のように表示されます。

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
 Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

4. 特定のレジストリ エントリ（Windows）またはファイル（Linux および macOS）を追加して、接続用にワンタイム単位でルートのデバッグを有効にします。
   - 32 ビット Windows の場合、DWORD レジストリ値は `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client\DebugRoutesEnabled` である必要があります。
   - 64 ビット Windows の場合、DWORD レジストリ値は `HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco Secure Client\DebugRoutesEnabled` である必要があります。
   - Linux または macOS の場合、sudo touch コマンドを使用してパス `/opt/cisco/secureclient/vpn/debugroutes` にファイルを作成します。

（注） トンネル接続が開始されると、キーまたはファイルは削除されます。デバッグを有効にするには、ファイルまたはキーが存在するだけで十分であり、キーの値またはファイルの内容は重要ではありません。

VPN接続を開始します。このキーまたはファイルが見つかった場合、2つのルート デバッグ テキスト ファイルがシステムの一時ディレクトリに作成されます（通常、Windows では C:\Windows\Temp、macOS または Linux では /opt/cisco/secureclient/vpn）。2 つのファイル（debug_routechangesv4.txt4 と debug_routechangesv6.txt）がすでに存在する場合、これらのファイルは上書きされます。

Cisco Secure Client トラフィックを通過させない

問題：Cisco Secure Client クライアントは、接続後、プライベートネットワークにデータを送信できません。

解決策：次の点をチェックします。

- AT&T Sierra Wireless 875 カードと AT&T Communication Manager Version 6.2 または 6.7 を使用している場合は、次の手順に従って問題を修正してください。
  1. Aircard でアクセラレーションを無効にします。
  2. [ツール（Tools）] > [設定（Settings）] > [アクセラレーション（Acceleration）] > [スタートアップ（Startup）] から AT&T Communications Manager を起動します。
  3. **manual** と入力します。
  4. [停止（Stop）] をクリックします。
- **show vpn-sessiondb detail anyconnect filter name <username>** コマンドの出力を取得します。出力にフィルタ名 XXXXX が指定されている場合は、show access-list XXXXX コマンドの出力も取得してください。ACL によってトラフィック フローがブロックされていないか確認してください。
- [Cisco Secure Client] > [統計情報（Statistics）] > [詳細（Details）] > [エクスポート（Export）] の順に選択し、DART のファイルまたは出力（AnyConnect-ExportedStats.txt）を取得します。統計情報、インターフェイス、およびルーティング テーブルを調べます。
- Cisco Secure Firewall ASA コンフィギュレーション ファイルの NAT 文を確認します。NAT が有効になっている場合は、クライアントに返されるデータをネットワーク アドレス変換から除外する必要があります。たとえば、Cisco Secure Client プールから IP アドレスを NAT 除外するには、次のコードが使用されます。

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

- トンネリングされたデフォルト ゲートウェイがその設定に対して有効になっているかどうかを確認してください。従来型のデフォルト ゲートウェイは、次のように非復号化トラフィックのラスト リゾート ゲートウェイです。

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

VPN クライアントが、VPN ゲートウェイのルーティング テーブルに存在しないリソースにアクセスする必要がある場合、パケットは標準デフォルト ゲートウェイによってルーティングされます。VPN ゲートウェイは、完全な内部ルーティング テーブルを必要としません。トンネリングされたキーワードを使用する場合、IPsec/SSL VPN 接続から受信した復号化トラフィックはルーティングによって処理されます。VPN ルートから受信したトラフィックは 10.0.4.2 にルーティングされて復号化されますが、標準トラフィックは最終的に 209.165.200.225 にルーティングされます。

- Cisco Secure Client でトンネルを確立する前後の、ipconfig /all のテキストダンプおよび route print の出力を収集します。
- クライアントでネットワーク パケット キャプチャを実行するか、Cisco Secure Firewall ASA のキャプチャを有効にします。

（注） 一部のアプリケーション（Microsoft Outlook など）がトンネルで動作しない場合、受け入れられるサイズを確認するために、一定の基準に従って大きくした ping（たとえば、ping -| 500, ping -| 1000, ping -| 1500, and ping -| 2000）を使用して、ネットワーク内の既知のデバイスに ping します。ping の結果から、ネットワークにフラグメンテーションの問題が発生しているかがわかります。その後、フラグメンテーションが発生していると思われるユーザの特別なグループを設定して、このグループの anyconnect mtu を 1200 に設定できます。また、古い IPsec クライアントから Set MTU.exe ユーティリティをコピーして、物理アダプタの MTU を強制的に 1300 に設定できます。リブート時に、違いがあるかどうか確認してください。

VM ベースのサブシステムに関する接続の問題

ホスト（Windows 10 または macOS 11 以降）で AnyConnect VPN がアクティブになっている場合に、Windows Subsystem for Linux（WSL2）または VMware Fusion VM で接続の問題が発生するときは、次の手順に従って、ローカル LAN のスプリット除外トンネリングを仮想アダプタ サブネットのみに制限するように設定します。

ステップ 1 ASDM で、[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [詳細（Advanced）] > [AnyConnectカスタム属性（AnyConnect Custom Attributes）] に移動して新しいカスタム属性タイプを設定します。

ステップ 2 [追加（Add）] を選択し、[カスタム属性の作成（Create Custom Attribute）] ペインで次の設定を行います。

a) 新しいタイプとして、IPv4 の場合は **BypassVirtualSubnetsOnlyV4**、IPv6 の場合は **BypassVirtualSubnetsOnlyV6** と入力します。

b) 必要に応じて、説明を入力します。

c) [AnyConnectカスタム属性名（AnyConnect Custom Attributes Names）] で名前と値を *true* に設定します。

特定の IP プロトコルのグループポリシーでローカル LAN のワイルドカードによるスプリット除外がすでに設定されている場合は、同じ IP プロトコルに対してカスタム属性が有効になっていれば、クライアントによって仮想サブネットのみに制限されます。ローカル LAN のワイルドカードによるスプリット除外がグループポリシーで設定されていない場合は、カスタム属性が有効な IP プロトコルに対してクライアントによって追加され、それに応じて、制限されたローカル LAN のスプリット除外が適用されます。他の split-exclude ネットワークが設定されていない場合、すべての物理アダプタトラフィックは tunnel-all 構成と同様にトンネリングされます。

ステップ 3 以前に作成したカスタム属性のタイプと名前をグループポリシーにアタッチします。それには、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network（Client）Access）] > [グループポリシー（Group Policies）] > [編集（Edit）] > [詳細（Advanced）] > [AnyConnectクライアント（AnyConnect Client）] > [カスタム属性（Custom Attributes）]** に移動します。

次のタスク

属性値が正しく設定されているかどうかを確認するには、Cisco Secure Client ログで「Received VPN Session Configuration」で始まるメッセージをチェックします。その内容から、ローカル LAN のワイルドカードが仮想サブネットに制限されていることがわかります。

VPN サービスの障害

VPN サービス接続に失敗

問題：「処理を進めることができません。VPN サービスに接続できません（Unable to Proceed, Cannot Connect to the VPN Service）」というメッセージが表示されます。Cisco Secure Client の VPN サービスが実行されていません。

解決策：別のアプリケーションがサービスと競合していないかを確認してください。11-7 ページの「何がサービスと競合しているかの特定」を参照してください。

何がサービスと競合しているかの特定

次の手順では、サーバーが起動されないため、競合が起動時にサーバの初期化との間で生じたか、または他の実行中のサービスとの間で生じたかを判別します。

ステップ 1 Windows 管理ツールでサービスを確認して、Cisco Secure Client VPN エージェントが動作していないか確認します。このエージェントが動作している場合にエラーメッセージが引き続き表示される場合は、ワークステーション上の別の VPN アプリケーションを無効にするか、アンインストールすることが必要になる可能性があります。その操作を実行した後、リブートし、この手順を繰り返します。

ステップ 2 Cisco Secure Client VPN エージェントを起動してみます。

ステップ 3 イベントビューアの Cisco Secure Client ログに、サービスを起動できなかったことを示すメッセージがないか確認します。ステップ 2 での手動によるリスタートのタイムスタンプおよびワークステーションが起動した時間に注目します。

ステップ 4 イベントビューアのシステムログおよびアプリケーションログに、競合メッセージの同一の一般的なタイム スタンプがないかを確認します。

ステップ 5 サービスの起動に失敗したことをログが示している場合、同一のタイム スタンプの前後にある、次のいずれかを示すその他の情報メッセージを探します。

- 欠落したファイル：欠落したファイルを除外するには、Cisco Secure Client をスタンドアロン MSI インストールから再インストールします。
- 別の依存するサービスでの遅延：起動アクティビティを無効にして、ワークステーションのブート時間を短縮します。
- 別のアプリケーションまたはサービスとの競合：別のサービスが、vpnagent が使用するポートと同じポート上で受信していないか、または一部の HIDS ソフトウェアによって、シスコのソフトウェアがポート上で受信できなくなっているかどうかを判別します。

ステップ 6 ログに原因が直接示されていない場合は、試行錯誤的な方法で競合を識別してください。最も可能性の高い候補を識別したら、[サービス（Services）] パネルから該当するサービス（VPN 製品、HIDS ソフトウェア、spybot クリーナ、スニファ、ウイルス対策ソフトウェアなど）を無効にします。

ステップ 7 リブートします。VPN エージェント サービスが依然として起動に失敗する場合は、オペレーティング システムのデフォルト インストールでインストールされなかったサービスをオフにします。

VPNクライアントドライバで（MicrosoftWindowsアップデート後に）エラーが発生する

問題：最近 Microsoft certclass.inf ファイルを更新し、その後、VPN 接続を確立しようとすると、次のメッセージが表示されます。

```
The VPN client driver has encountered an error.
```

C:\WINDOWS\setupapi.log を確認すると、次のエラーが表示される場合があります。

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or invalid.
 Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver
signing policy.
```

解決策：コマンドプロンプトで **C:\>systeminfo** と入力するか、C:\WINDOWS\WindowsUpdate.log を確認して、最近インストールされた更新プログラムを確認してください。VPN ドライバを修正する手順に従ってください。

VPN クライアント ドライバ エラーの修復

上記の手順を実行すると、カタログが破損していないことが示される場合がありますが、キーファイルが無署名のもので上書きされた可能性があります。障害が解消されない場合は、ドライバ署名のデータベースの破損原因を特定するために Microsoft に依頼してケースをオープンしてください。

ステップ 1 コマンド プロンプトを管理者として開きます。

ステップ 2 **net stop CryptSvc** と入力します。

ステップ 3 **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** と入力してデータベースを分析し、そのデータベースの妥当性を検証するか、%/WINDIR%\system32\catroot2ディレクトリの名前を catroot2_old に変更します。

ステップ 4 プロンプトが表示されたら、[OK] を選択して修復を試行します。コマンドプロンプトを終了し、リブートします。

ドライバのクラッシュ

VPNVA.sys でのドライバ クラッシュの修復

問題：VPNVA.sys ドライバがクラッシュします。

解決策：Cisco Secure Client 仮想アダプタにバインドされている中間ドライバを検索し、オフにしてください。

vpnagent.exe でのドライバ クラッシュの修復

ステップ 1 c:\vpnagent という名前のディレクトリを作成します。

ステップ 2 タスク マネージャの [プロセス（process）] タブを調べ、vpnagent.exe のプロセスの PID を判別します。

ステップ 3 コマンドプロンプトを開き、デバッグ ツールをインストールしたディレクトリに移動します。デフォルトでは、Windows のデバッグ ツールは `C:\Program Files\Debugging Tools` にあります。

ステップ 4 **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst** と入力します。ここで、*PID* は **vpnagent.exe** の PID です。

ステップ 5 オープン ウィンドウを最小化した状態で実行します。モニタリングしている間は、システムをログオフできません。

ステップ 6 クラッシュが発生すると、c:\vpnagent の中身を zip ファイルに収集します。

ステップ 7 **!analyze -v** を使用して、crashdmp ファイルをさらに診断します。

Network Access Manager に関するリンク/ドライバの問題

Network Access Managerが有線接続のアダプタの認識に失敗した場合は、ネットワーク ケーブルのプラグを抜き、もう一度差し込んでみてください。これでうまくいかない場合は、リンクに問題がある可能性があります。Network Access Managerがアダプタの適切なリンク ステートを判別できない可能性があります。NIC ドライバの接続プロパティを確認してください。[詳細（Advanced）] パネルに [リンクを待機（Wait for Link）] オプションが表示される場合があります。この設定がオンになっている場合、有線接続の NIC ドライバの初期化コードは、自動ネゴシエーションが完了するまで待機してから、リンクが存在するかどうかを判別します。

その他のクラッシュ

Cisco Secure Client のクラッシュ

問題：リブート後に「システムは重大なエラーから回復しました（the system has recovered from a serious error）」というメッセージを受け取りました。

解決策：%temp% ディレクトリ（C:\DOCUME~1\jsmith\LOCALS~1\Temp など）から .log および .dmp の生成済みファイルを収集します。ファイルをコピーするか、またはバックアップします。「.log ファイルまたは .dmp ファイルのバックアップ方法」を参照してください。

.log ファイルまたは .dmp ファイルのバックアップ方法

ステップ 1 [スタート（Start）] > [ファイル名を指定して実行（Run）] メニューからワトソン博士（Drwtsn32.exe）という Microsoft ユーティリティを実行します。

ステップ 2 次のように設定し、[OK] をクリックします。

```
Number of Instructions     : 25
Number of Errors to Save : 25
Crash Dump Type   : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

ステップ 3 クライアントデバイス で [スタート（Start）] > [実行（Run）] メニューの順に選択し、**eventvwr.msc /s** と入力して、Windows イベントビューアから Cisco Secure Client VPN クライアントログを取得します。

ステップ 4 [アプリケーションとサービスログ（Applications and Services Logs）]（Windows）で、Cisco Secure Client を見つけ、[ログファイルの名前を付けて保存...（Save Log File As...）] を選択します。。.evt ファイル形式のファイル名（例： CiscoSecureClientLog.evt）を割り当てます。

Cisco Secure Client が vpndownloader でクラッシュする（Layered Service Provider（LSP）モジュールおよび NOD32 AV）

問題：LSP または NOD32 AV を使用している場合、Cisco Secure Client は、接続を確立しようとした際、認証に成功し、SSL セッションを構築するものの、その後 vpndownloader でクラッシュします。

解決策：ESET NOD32 AV のバージョン 2.7 で Internet Monitor コンポーネントを削除し、バージョン 3.0 にアップグレードしてください。

ブルー スクリーン（AT & T Dialer）

問題：AT&T Dialer を使用している場合に、クライアント オペレーティング システムでブルー スクリーンが発生して、ミニ ダンプファイルが作成されることがあります。

解決策：AT&T Global Network Client を最新の 7.6.2 にアップグレードしてください。

セキュリティの警告

Microsoft Internet Explorer のセキュリティの警告

問題：Microsoft Internet Explorer で、[セキュリティアラート（security alert）] ウィンドウが表示され、次のテキストが示されます。

```
Information you exchange with this site cannot be viewed or changed by others. However,
 there is a problem with the site's security certificate. The security certificate was
issued by a company you have not chosen to trust. View the certificate to determine
whether you want to trust the certifying authority.
```

解決策：このアラートは、信頼済みサイトとして認識されていない Cisco Secure Firewall ASA に接続すると表示されることがあります。このアラートを回避するには、クライアントに信頼できるルート証明書をインストールします。「クライアントでの信頼できるルート証明書のインストール」を参照してください。

「不明な機関による認証」アラート

問題：「不明な機関による Web サイト認証」アラート ウィンドウがブラウザに表示されることがあります。[セキュリティの警告（Security Alert）] ウィンドウの上半分に、次のテキストが表示されます。

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

解決策：このセキュリティアラートは、信頼済みサイトとして認識されていない Cisco Secure Firewall ASA に接続すると表示されることがあります。このアラートを回避するには、クライアントに信頼できるルート証明書をインストールします。「クライアントでの信頼できるルート証明書のインストール」を参照してください。

クライアントでの信頼できるルート証明書のインストール

始める前に

信頼できるルート証明書として使用する証明書を生成または取得します。

（注） クライアントで信頼できるルート証明書として自己署名証明書をインストールすることによって、短期的にセキュリティ証明書の警告を回避できます。ただし、これはお勧めしません。理由は、ユーザが誤って不正なサーバー上の証明書を信頼するようにブラウザを設定する可能性があるため、また、ユーザがセキュア ゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。

ステップ 1 [セキュリティの警告（Security Alert）] ウィンドウの [証明書の表示（View Certificate）] をクリックします。

ステップ 2 [証明書のインストール（Install Certificate）] をクリックします。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] を選択します。

ステップ 5 [参照（Browse）] をクリックします。

ステップ 6 ドロップダウン リストで、[信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択します。

ステップ 7 [証明書のインポート（Certificate Import）] ウィザードのプロンプトに従って続行します。

接続のドロップ

有線接続が導入された場合のワイヤレス接続のドロップ（Juniper Odyssey クライアント）

問題：Odyssey クライアントでワイヤレスサプレッションが有効である場合、有線接続が導入されると、ワイヤレス接続がドロップします。ワイヤレス サプレッションが無効である場合、ワイヤレス機能は期待どおりに動作する。

解決策：Odyssey クライアントの設定。

Odyssey クライアントの設定

ステップ 1 [ネットワーク接続（Network Connections）] で、アダプタの名前を接続プロパティの表示どおりにコピーします。レジストリを編集する場合、誤って変更すると重大な問題が発生する可能性があるため、バックアップを実行してから、細心の注意を払って変更してください。

ステップ 2 レジストリを開き、HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual に移動します。

ステップ 3 virtual の下に新しい文字列値を作成します。アダプタの名前をネットワーク プロパティからレジストリ部分にコピーします。追加のレジストリ設定を保存すると、MSI が作成されて他のクライアントにプッシュされたときに、この設定が移植されます。

Cisco Secure Firewall ASA への接続に失敗（Kaspersky AV Workstation 6.x）

問題：Kaspersky 6.0.3 がインストールされると（無効であっても）、CSTP state＝CONNECTED の直後に Cisco Secure Firewall ASA への Cisco Secure Client 接続が失敗します。次のメッセージが表示されます。

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway
(proxy authentication, handshake, bad cert, etc.).
```

解決策：Kaspersky をアンインストールし、Kaspersky のフォーラムを参照して追加のアップデートがないか確認してください。

UDP DTLS 接続なし（McAfee Firewall 5）

問題：McAfee Firewall 5 を使用しているときに、UDP DTLS 接続を確立できません。

解決策：McAfee Firewall のセンターコンソールで、[高度なタスク（Advanced Tasks）] > [高度なオプションとロギング（Advanced options and Logging）] を選択し、McAfee Firewall の [着信フラグメントを自動的にブロック（Block incoming fragments automatically）] チェックボックスをオフにします。

ホストデバイスへの接続に失敗（Microsoftルーティングとリモートアクセス サーバー）

問題：RRAS を使用している場合に、Cisco Secure Client がホストデバイスへの接続を確立しようとすると、イベントログに次の終了エラーが返されます。

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the Cisco Secure
Client.
```

解決策：RRAS サービスを無効にします。

接続障害/クレデンシャル不足（ロード バランサ）

問題：ログイン情報がないために、接続が失敗します。

解決策：サードパーティ製ロードバランサでは、Cisco Secure Firewall ASA デバイスにかかる負荷を把握できません。一方、ASA のロードバランス機能は非常にインテリジェントで、VPN

の負荷をデバイス全体で均等に分散できるため、Cisco Secure Firewall ASA 内蔵のロードバランシングを使用することをお勧めします。

インストールの失敗

根本原因なしに Windows レジストリを編集できない

Cisco Secure Client のインストール、アンインストール、またはアップグレード中にエラーが発生した場合は、Windows インストーラのレジストリキーを直接変更することはお勧めしません。変更すると、望ましくない結果が生じる可能性があります。Microsoft が提供するツールにより、根本原因の特定後、インストーラの問題をトラブルシューティングできます。

Cisco Secure Client がダウンロードに失敗する（Wave EMBASSY Trust Suite）

問題：Cisco Secure Client がダウンロードに失敗し、次のエラーメッセージが表示されます。

```
"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close."
```

ソリューション：dll の問題をすべて解決するために、パッチアップデートをバージョン 1.2.1.38 に更新してください。

非互換性の問題

ルーティング テーブルの更新に失敗（Bonjour Printing Service）

問題：Bonjour Print Service を使用している場合に、Cisco Secure Client イベント ログに IP 転送テーブルの識別に失敗したことが示されます。

解決策：コマンドプロンプトで **net stop "bonjour service"** と入力し、Bonjour Print Service を無効にします。mDNSResponder の新しいバージョン（1.0.5.11）が Apple から提供されています。この問題を解決するために、Bonjour の新しいバージョンが iTunes にバンドルされ、個別のダウンロードとして Apple の Web サイトで配布されています。

TUN のバージョンに互換性がない（OpenVPN クライアント）

問題：このバージョンの TUN がこのシステムにすでにインストールされていて、Cisco Secure Client と互換性がないことを示すエラーが表示されます。

解決策：Viscosity OpenVPN Client をアンインストールします。

Winsock カタログの競合（LSP 症状 2 競合）

問題：クライアント上に LSP モジュールが存在する場合、Winsock カタログが競合することがあります。

解決策：LSP モジュールをアンインストールしてください。

データ スループット低下（LSP 症状 3 競合）

問題：Windows で NOD32 Antivirus V4.0.468 x64 を使用すると、データスループットが低下する場合があります。

解決策：SSL プロトコルスキャンを無効にします。「SSL プロトコルスキャンの無効化」を参照してください。

SSL プロトコル スキャンの無効化

ステップ 1 [詳細設定（Advanced Setup）] の **[プロトコルフィルタリング（Protocol Filtering）]** > **[SSL]** を選択し、SSL プロトコルスキャンを有効にします。

ステップ 2 **[Webアクセス保護（Web access protection）]** > **[HTTP, HTTPS]** の順に選択し、[HTTPSプロトコルチェックを使用しない（Do not use HTTPS protocol checking）] をオンにします。

ステップ 3 **[プロトコルフィルタリング（Protocol Filtering）]** > **[SSL]** に戻り、**SSL プロトコルスキャン**を無効にします。

DPD 障害（EVDO ワイヤレス カードおよび Venturi ドライバ）

問題：クライアントの接続解除中に、EVDO ワイヤレスカードおよび Venturi ドライバを使用すると、イベントログに次のことが報告されます。

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
 DPD failure.
```

ソリューション：

- アプリケーション、システム、および Cisco Secure Client の各イベントログに関係する接続解除イベントがないか確認すると同時に、NIC カードのリセットが適用されたかどうか判別してください。
- Venturi ドライバが最新のものであるか確認してください。AT&T Communications Manager バージョン 6.7 の [ルール エンジンの使用（Use Rules Engine）] を無効にします。

DTLS トラフィック障害（DSL ルータ）

問題：DSL ルータに接続している場合、正常にネゴシエーションされても、DTLS トラフィックが失敗することがあります。

解決策：工場出荷時の設定を使用して Linksys ルータに接続してください。この設定により、DTLS セッションが安定し、ping で中断が発生しません。DTLS リターン トラフィックを許可するルールを追加してください。

NETINTERFACE_ERROR（CheckPoint と、Kaspersky などの他のサードパーティ製ソフトウェア）

問題：SSL 接続に使用されるコンピュータ ネットワークのオペレーティング システム情報を取得しようとしたときに、セキュア ゲートウェイへの接続を完全には確立できなかったことが Cisco Secure Client ログに示されることがあります。

ソリューション：

- 整合性エージェントをアンインストールしてから Cisco Secure Client をインストールする場合は、TCP/IP を有効にしてください。
- 整合性エージェントのインストール時に SmartDefense を無効にすると、TCP/IP がチェックされます。
- サードパーティ製のソフトウェアがネットワーク インターフェイス情報の取得中に、オペレーティング システムの API コールを代行受信またはブロックしている場合は、疑わしい AV、FW、AS などがないか確認してください。
- デバイスマネージャに Cisco Secure Client アダプタのインスタンスが 1 つだけ表示されていることを確認してください。インスタンスが 1 つだけの場合は、Cisco Secure Client で認証し、5 秒後にデバイスマネージャからアダプタを手動で有効にしてください。
- 疑わしいドライバが Cisco Secure Client アダプタ内で有効にされている場合は、これらのドライバを [Cisco Secure Client 接続（Cisco AnyConnect VPN Client Connection）] ウィンドウでオフにして無効にしてください。

パフォーマンスの問題（Virtual Machine Network Service ドライバ）

問題：一部の Virtual Machine Network Service デバイスで Cisco Secure Client を使用しているときに、パフォーマンスの問題が発生しました。

解決策：Cisco Secure Client 仮想アダプタ内のすべての IM デバイスに対するバインドをオフにしてください。アプリケーション dsagent.exe は、C:\Windows\System\dgagent にあります。これはプロセス リストに表示されませんが、TCPview（sysinternals）でソケットを開くと表示できます。このプロセスを終了すると、Cisco Secure Client が正常の動作に戻ります。

既知のサードパーティ製アプリケーション競合

次のサードパーティ アプリケーションは、Cisco Secure Client との間に既知の複雑な問題があります。

- Adobe および Apple：Bonjour Print Service
  - Adobe Creative Suite 3
  - BonJour Print Service
  - iTunes
- AT&T Communications Manager バージョン 6.2 および 6.7
  - AT&T Sierra Wireless 875 カード
- AT&T Global Dialer
- CheckPoint と、Kaspersky など他のサードパーティ製ソフトウェア
- macOS で Cisco Secure Client と同時に実行されている Apple M1 デバイス上の Apple iOS 用 Cisco Secure Client
- ユニバーサル Windows プラットフォーム上の Cisco Secure Client
- Citrix Advanced Gateway Client バージョン 2.2.1
- DSL ルータ
- EVDO ワイヤレスカードおよび Venturi ドライバ
- ファイアウォールとの競合
  - サードパーティ製のファイアウォールが、Cisco Secure Firewall ASA グループポリシーで設定されたファイアウォール機能と干渉する可能性があります。
- Juniper Odyssey Client
- Kaspersky AV Workstation 6.x
- Layered Service Provider（LSP）モジュールおよび NOD32 AV
- ロード バランサ
- McAfee Firewall 5
- Microsoft Internet Explorer 8
- Microsoft Routing and Remote Access Server
- Microsoft VPN
- OpenVPN クライアント

- Pulse Secure
- Virtual Machine Network Service ドライバ
- Wave EMBASSY Trust Suite

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。