CHAPTER 5

エンドユーザ無線ネットワークのトラブルシューティング

この章では、一般的なユーザの問題に対して推奨されるトラブルシューティングの方法について説明します。この章の内容は、次のとおりです。

- Cisco SSC 簡易ユーザ インターフェイスの使用方法（P. 5-2）
- アソシエーションの失敗（P. 5-3）
- 認証の失敗（P. 5-5）
- IP 接続の失敗（P. 5-6）
- 他の無線クライアント マネージャとの共存（P. 5-7）
- ログおよびパケット トレースの収集（P. 5-9）

Cisco SSC 簡易ユーザ インターフェイスの使用方法

SSC は、管理者が展開した 802.1X の設定をエンドユーザが変えてしまうことのないように設計されています。ユーザが展開された設定プロファイルを編集することはできません。また、802.1X 無線設定は、不適切に設定される可能性が低くなるように、展開前に検証およびテストされます。

SSC GUI は、エンドユーザが手動入力で間違いを犯す可能性を最小限に抑えられるようにもなっています。検出されたホーム SSID（ネットワーク名）をダブルクリックするか、SSC トレイ アイコンから選択するだけで、ホーム ネットワークを作成できます。ユーザがホーム ネットワークの WEP キーを入力するときには、キー入力がマスキングされないので、視覚的に簡単に確認できます。

SSC では、ユーザ インターフェイスが最小限に抑えられ、802.1X に関する不要な情報がエンドユーザに表示されることがないので、ユーザは簡単に無線接続の設定を診断できます。

- 信号の強さによって、ユーザの PC が無線ネットワークの範囲内にあるかどうかがすぐにわかります（SSID が非表示でない場合）。
- 特定のネットワーク プロファイルを右クリックして **Connect Exclusively** を選択すると、ユーザはすぐにそのプロファイルに接続できます。
- エラーが不適切なクレデンシャルによるものかどうかをユーザがすぐに判断できます。
- 認証に失敗した場合、ユーザは SSC システム トレイ アイコンを右クリックして **Connection Status** を選択し、接続情報を表示して設定を確認できます。
- ユーザは、SSC システム トレイ アイコンを右クリックして **Repair** を選択することにより、以前の無線アソシエーションを修復できます。
- ユーザがシステム トレイの Microsoft 無線ネットワーク接続アイコンをクリックし、該当の無線ネットワーク接続を右クリックして **Repair** を選択すると、Windows で以前の無線アソシエーションの修復が試行されます。
- ユーザは、SSC システム トレイ アイコンを右クリックして **Enable Wi-Fi Radio** を選択することにより、Wi-Fi 無線のオンとオフを切り替えることができます。チェックマークが付いている場合、無線はオンになっています。
- SSC Help メニューでは、ユーザが役立つ情報を参照できます。

ユーザが上記の方法でネットワークの問題を解決できない場合は、サポート ヘルプ デスクに問い合わせて問題を解決しなければならなくなることがあります。

ヘルプ デスクへの問い合わせでは、ユーザから次のいずれかの問題が報告されることがあります。

- アソシエーションの失敗：「アソシエーションの失敗」の項（P.5-3）を参照
- 認証の失敗：「認証の失敗」の項（P.5-5）を参照
- IP 接続の失敗：「IP 接続の失敗」の項（P.5-6）を参照

アソシエーションの失敗

ここでは、ユーザの側で一般的に発生する可能性のある、2 つのアソシエーションの問題について説明します。

例 1 - ホーム アクセス ポイントに接続できない

ユーザが SSC を設定してホーム アクセス ポイントを使用できません。その場合、ユーザは、ホーム環境で次のいずれかのアソシエーション モードを使用している可能性があります。

- オープン（セキュリティなし）
- オープン（静的 WEP キー使用）
- 共有（静的 WEP キー使用）
- WPA Personal (PSK) - TKIP（パスフレーズ使用）
- WPA Personal (PSK) - AES（パスフレーズ使用）
- WPA2 Personal (PSK) - TKIP（パスフレーズ使用）
- WPA2 Personal (PSK) - AES（パスフレーズ使用）

サポート ヘルプ デスクでは、問題の修正を支援する必要があるので、ユーザに次の操作を行うよう指示することがあります。

1. すべての無線ネットワーク　コンポーネントの電源を切り、3　分間待機します。次の順番で各ネットワーク コンポーネントの電源を入れます。ただし、1 つのコンポーネントの電源が完全に入ってから次のコンポーネントの電源を入れるようにします。
   a. モデム（ケーブル、DSL、または衛星）
   b. ルータ
   c. アクセス ポイント
   d. PC

（注）　ユーザのホーム ネットワークでは、独立したアクセス ポイントではなく無線ルータが使用されている場合があります。無線ルータは、アクセス ポイントが統合されたルータです。

2. 無線接続が確立できることを確認します。
3. 無線接続に失敗した場合は、アクセス ポイントの IP アドレスをユーザが知っていれば、クライアントのプロファイルの設定がアクセス ポイントの設定と一致していることを確認します。次のいずれかの方法で確認します。
   a. アクセス ポイントの Ethernet ポートに直接接続し、アクセス ポイントの GUI を表示します。
   b. ユーザが　Ethernet　ポートを備えた有線ルータまたは無線ルータを使用している場合は、Ethernet ポートに接続してアクセス ポイントの Web ウィンドウを開き、アクセス ポイントの設定を確認します。
4. 無線接続に失敗し、アクセス ポイントの IP アドレスをユーザが知らない場合は、次の方法で、クライアントのプロファイルの設定がアクセス ポイントの設定と一致していることを確認します。
   a. **Settings** > **Enable Client** の順にクリックして、SSC を無効にします。チェックマークが付いていれば、SSC は有効になっています。
   b. 既に設定済みのクライアントを使用します（たいていの場合は Windows のネイティブ クライアントです）。

c. アクセス ポイントへの接続に成功すれば、ユーザはアクセス ポイントの Web ウィンドウを表示してアクセス ポイントの設定を確認できます。

5. ユーザがアクセス ポイントの設定を文書化してある場合は、一般的に、次のいずれかの問題が発生する可能性があります。

   - WEP キーを使用する 802.11 認証のオープン モードまたは共有モード

     ユーザが、誤って *Shared WEP* の代わりに *Open WEP* を使用してクライアントを設定したか、その逆の可能性があります。SSC を使用して設定を切り替え、別のモードを試すことができます。

   - 誤った WEP キーの生成または手動入力の誤り

     一部のアクセス ポイントでは、パスフレーズを使用して WEP キーを生成します。ユーザは、接続を選択して **Edit** > **Generate Router WEP key** の順にクリックし、パスフレーズを入力して、正しい WEP キーを生成する必要があります。

     パスフレーズを使用しない場合は、SSC GUI で接続を選択し、**Edit** をクリックしてから **Show password** をオンにして、入力したパスワードを目視で確認します。

   - WPA/WPA2 パスフレーズの手動入力の誤り

     ユーザが、以前に使用していたクライアント アプリケーションでクレデンシャルを非表示にしていたために、パスワードを忘れてしまうことがあります。場合によっては、ユーザが新規パスワードを使用してアクセス ポイントを設定し直さなければならないこともあります（手順 3 および 4 を参照）。

   - WEP キー インデックスの不一致

     一部のアクセス ポイントでは、複数のキー インデックスを使用して WEP キーを設定できます。シスコでは、静的 WEP キーに最初のキー インデックスを設定することを推奨しています。場合によっては、ユーザがアクセス ポイントの WEP キーを設定し直さなければならないこともあります（手順 3 および 4 を参照）。

   - アクセス ポイントで MAC フィルタリングが有効化されている。

     ユーザの PC で複数の無線ネットワーク アダプタがインストールされ、有効になっている場合は、SSC で、アクセス ポイントの MAC フィルタの設定によってブロックされている無線ネットワーク アダプタが使用されている可能性があります。場合によっては、ユーザがアクセス ポイントを設定し直さなければならないこともあります（手順 3 および 4 を参照）。

それでもアクセス ポイントに接続できない場合は、ユーザがアクセス ポイントを出荷時のデフォルト設定にリセットしてから、アクセス ポイントを設定し直す必要があります。

例 2 - 企業ネットワークに接続できない

ユーザが、パーティションで仕切られたスペース、会議室、またはオフィス ビルで、無線接続を使用して企業ネットワークに接続できません。

ネットワーク管理者は、企業内で事前設定済みの設定プロファイルを展開します。企業環境で 802.11 アソシエーションが失敗する原因としては、主に次の 2 つが考えられます。

1. 無線のカバレッジが不十分であるか、無線ノイズが過多である。

   無線展開が適切に設計されていない場合や、環境内の他のデバイス（電子レンジなども含まれる可能性があります）に起因する多くのノイズが周波数帯で発生している場合に、このような状況に陥ります。

2. 古い無線 NIC デバイスが使用されている。

   無線ネットワークが長期間にわたって使用されており、ユーザの PC に古いバージョンの無線 NIC ドライバがインストールされたままになっている場合がよくあります。ネットワーク管理者が、自社の企業環境内で使用されている NIC ドライバ チップセット用の既知の良好な NIC ドライバを、すべてのユーザに再配布することを推奨します。

認証の失敗

802.1X の設定が SSC によって正しく展開され、ネットワーク インフラストラクチャのコンポーネント（アクセス ポイント、コントローラ、RADIUS サーバなど）が正しく設定されている企業環境では、次のような問題が原因で認証に失敗する場合があります。

- ユーザが誤ったクレデンシャルを入力した。
- ユーザが、知らないうちに、誤ったクレデンシャルを設定された回数入力したために、アカウントがロックされ、正しいクレデンシャルを入力しても機能しなくなった。
- ユーザのクレデンシャルが期限切れになった。
- ネットワーク インフラストラクチャ、PKI（Public Key Infrastructure; 公開鍵インフラストラクチャ）、またはユーザ データベースに問題がある。すなわち、アクセス ポイントが認証サーバと通信できないか、認証サーバが機能していないか、認証サーバの設定が変更された。
- スマート カード、スマート カード リーダ、トークンなどの、認証プロセスに関係するデバイスが正しく機能していない。
- ユーザの PC に Windows Internet Explorer 5.0 以降がインストールされていない。

問題が解決されない場合、サポート ヘルプ デスクは、パケット キャプチャを有効にして作成されたシスコ サポート レポートの提供をユーザに求めます。サポート レポートの作成については、「ログおよびパケット トレースの収集」の項（P.5-9）を参照してください。

IP 接続の失敗

802.1X 認証が成功すると、SSC では、有効な IP アドレスの取得が試みられます。一部のネットワークでは、IP アドレスを更新するのに 40 秒かかる場合があります。無線 LAN アダプタが有効な IP アドレスの受信に失敗する場合は、次の方法で、問題を解決したり、原因を特定したりできる場合があります。

- 無線 NIC アダプタを一度無効にしてから有効にする。
- SSC のシステム トレイ アイコンを右クリックして **Repair** を選択し、接続を修復する。
- SSC の GUI でネットワーク接続を右クリックして **Connect Exclusively** を選択する。
- ARP、ping、ipconfig などのネットワーク ツールを使用して、レイヤ 2 またはレイヤ 3 の接続状態、および IP アドレスが使用可能であるかどうかを確認する。

DHCP サーバで使用可能な IP アドレスがなくなったというような単純なことが、問題の根本的な原因となっている場合があります。

統合された VPN 接続の失敗

SSC では、ユーザが、無線プロファイルへの接続後、自動的に VPN 接続を確立できます（プロファイルがそのように設定されている場合）。

しかし、エンドユーザが、SSC を使用して自社の企業ネットワークに対する VPN トンネルを確立できない場合があります。その場合は、VPN に関する次のような問題が発生することがあります。

1. SSC のメイン ウィンドウに SSC VPN Connect ボタンが表示されない。

   管理者が、ユーザに対して *Allow VPN* オプションが有効なプロファイルを展開しなかった場合は、このような状態に陥ることがあります。

2. SSC VPN Connect ボタンは表示されるが、グレー表示される。

   Cisco VPN クライアントが 4.8 より前のバージョンの場合は、このような状態に陥ることがあります。ユーザは、PC の VPN クライアントをアップグレードする必要があります。

3. ユーザが VPN サービスにアクセスできない。

   ユーザがスタンドアロンの Cisco VPN クライアント インターフェイスを使用して VPN 接続を確立しようとした場合に、このような状態に陥ることがあります。VPN 接続の接続および切断に Cisco VPN クライアント インターフェイスが使用されていると、SSC により VPN 機能が制御されなくなります。

   この問題を解決するには、ユーザがスタンドアロンの Cisco VPN クライアント インターフェイスを使用して接続を確立しないようにする必要があります。SSC が VPN 接続を確立できるようにしなければなりません。ただし、必要な場合は、Cisco VPN クライアント インターフェイスを使用して接続の状態を表示できます。

4. SSC に、VPN の接続が失敗したというエラーが表示される。

   ユーザが SSC に入力したクレデンシャルが誤っていた場合は、このような状態に陥ることがあります。SSC で SoftToken オプションを使用する場合、SSC に入力されるユーザ クレデンシャルは、SofToken-II アプリケーションに入力したユーザ名およびユーザ PIN であることが必要です。

（注） VPN のユーザ名と PIN の入力を求められたときに、SofToken II アプリケーションによって生成された独自のソフトトークン パスワードを SSC に入力してはいけません。

VPN の問題が解決されない場合は、シスコ サポート レポートをサポート ヘルプ デスクに提出して、問題の分析および根本原因の特定を依頼します（「ログおよびパケット トレースの収集」の項（P.5-9）を参照）。

他の無線クライアント マネージャとの共存

Cisco Aironet Client Utility（ACU）と SSC を共存させるには、ユーザが、Windows でアダプタが設定されるように無線ネットワーク アダプタを設定する必要があります。無線ネットワーク アダプタの設定手順は、次のとおりです。

ステップ 1　デスクトップの **My Networks** を右クリックします。

ステップ 2　無線ネットワーク アダプタを右クリックして、**Properties** を選択します。

ステップ 3　**Wireless Networks** をクリックして、**Use Windows to configure my wireless network settings** をオンにします。

ステップ 4　**OK** をクリックして Network Connections ウィンドウを閉じます。

Cisco Aironet Desktop Utility（ADU）を SSC と共存させるには、ユーザが、SSC によりアダプタが制御されるように ADU を設定する必要があります。

（注）　最新バージョンの ADU は、Cisco Software Center からダウンロードできます。URL は、http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875243 です。

Client Adapters and Client Software をクリックして、画面の指示に従います。ソフトウェアをダウンロードするには、Cisco.com に登録するか、登録済みのユーザである必要があります。

ADU を設定するには、次の手順を実行します。

ステップ 1　ADU タスクバー アイコンをダブルクリックして ADU を開きます。

ステップ 2　**Options** > **Select Client Software** の順にクリックすると Select Client Software ポップアップ ウィンドウが表示されます。

ステップ 3　ポップアップ ウィンドウで **Third-Party Tool** をオンにして **OK** をクリックします。

ステップ 4　Select Client Software ポップアップ ウィンドウでの設定が正常に完了したことが表示されたら、**OK** をクリックします。

ステップ 5　ADU を閉じます。

SSC がアクティブな場合は、Microsoft Windows ネイティブ無線クライアントではなく、SSC によってアダプタが制御されます。つまり、Windows ネイティブ クライアントでは、SSID の表示は可能ですが、無線接続の設定は不可能です。SSC による無線アダプタの制御を停止するには、**Settings** をクリックして **Enable Client** を選択し（チェックマークが付いていれば SSC が有効）、SSC を無効にする必要があります。SSC を無効にすると、無線接続を管理可能な別の無線クライアント管理アプリケーションによって無線アダプタが制御されるようになります。

（注）　SSC と Odyssey Access Client Manager アプリケーションを、ユーザの PC に同時にインストールしないでください。

ユーザが Wi-Fi パブリック ホット スポット（空港など）を使用している場合は、次の手順に従って iPassConnect クライアント ソフトウェアと SSC を共存させることができます。

ステップ 1　SSC トレイ アイコンを右クリックして Wi-Fi 接続の名前を選択します。

ステップ 2　SSC アイコンが青色になって動かなくなったら、iPASS アプリケーションを有効にし、IPASS を使用してユーザ認証を行い、VPN 接続を確立する必要があります。

ステップ 3　iPassConnect で **Available Connections** を選択してから、SSC を使用して接続済みの接続名を選択します。

ステップ 4　iPassConnect で、ユーザ名とパスワードの入力を求められます。企業ネットワークのユーザ名を入力し、ソフトトークン アプリケーションを使用してパスワードを生成します。

ステップ 5　iPassConnect による認証が完了し、Cisco VPN アプリケーションが起動します。この時点で Cisco VPN アプリケーションを終了し、SSC アイコンを右クリックして **Connect VPN** を選択します。

（注）　通常、ほとんどのホット スポットで使用可能な webauth システムでは、認証が 1 時間以上有効です。接続が失われた場合は、もう一度接続する必要があります。SSC アイコンを右クリックして、**Connect VPN** を選択可能であれば、このオプションを選択します。初回に接続に成功しなかった場合は、数分後にもう一度 **Connect VPN** を選択してみてください。それでもうまくいかない場合は、Web ウィンドウを起動して、インターネットに接続しているかどうか、または Web ウィンドウでユーザ認証を要求されるかどうかを確認します。Web ウィンドウで認証情報を要求される場合は、iPassConnect の手順をステップ 4 から繰り返す必要があります。

ログおよびパケット トレースの収集

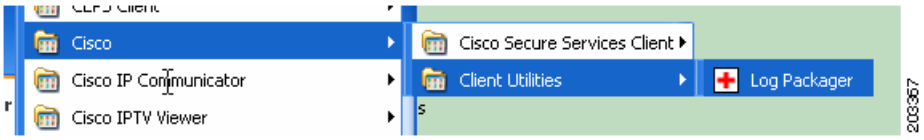
SSC には、Cisco Client Utilities の一部として、Log Packager と呼ばれる診断ユーティリティが用意されています。このユーティリティは、単独でインストールされ、Windows の Start > Program メニューから使用できます。このユーティリティでは、SSC の現在の状態、インターフェイスとドライバの詳細、FIPS の状態、および無線 LAN 情報（検出された SSID、アソシエーション状態など）などの情報が提供されます。SSC と NIC アダプタを使用している場合は、接続の問題を診断するためにこの情報が役立ちます。

SSC に関するシスコ サポート レポートの作成

シスコ サポート レポートを作成する手順は、次のとおりです。

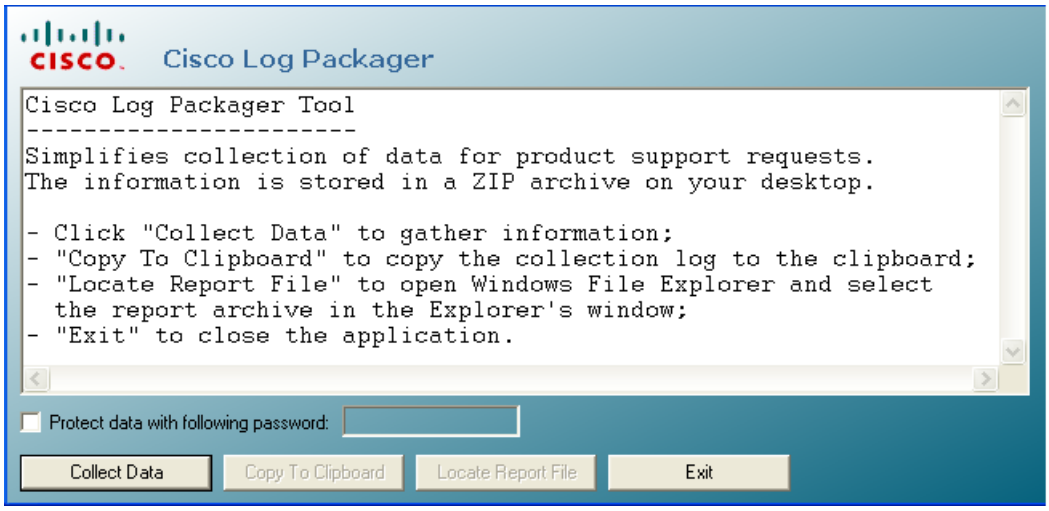
ステップ 1　**Start** > **All Programs** > **Cisco** > **Client Utilities** > **Log Packager** の順にクリックします（図 5-1 を参照）。

図 5-1　Windows の Program メニューで Client Utility にアクセスする



Log Packager プログラムが開くと、図 5-2 の画面が表示されます。

図 5-2　Log Packager ウィンドウ



ステップ 2　**Collect Data** をクリックします。

ステップ 3　もう一度ボタンが表示されたら **Locate Report File** をクリックします。Microsoft Explorer ウィンドウが開き、圧縮されたレポート ファイルが存在するディレクトリが表示されます。ファイル名は CiscoSupportReport.zip で、PC のデスクトップに配置されています。この zip ファイルには、複数のログ ファイル、キャプチャ ファイル、.xslt ファイル、および設定 .xml ファイルが含まれています。

Copy to Clipboard をクリックすると、CiscoSupportReportLog.txt ファイルの内容が Windows のクリップボードにコピーされます。

ステップ 4　Windows エクスプローラおよび Cisco Log Packager を閉じます。