CHAPTER 37

トラブルシューティング

この章では、ACE XML Gateway と外部サービスまたはサービス ユーザとの間で発生する問題の診断と解決の方法について説明します。内容は次のとおりです。

サービス接続エラーのトラブルシューティング

ACE XML Gateway のセットアップの際にユーザが直面する問題の最も一般的な原因がパートナー接続です。ほとんどのネットワーク プロトコルのセットアップは複雑であり、それがさまざまな問題につながる可能性があります。

ここでは発生する可能性があるセットアップの問題やその問題に対して採用できる診断手順をすべて紹介することはできませんが、パートナー接続のトラブルシューティングについてその一般的なアプローチを解説します。ここでは、まず、ほとんどの Gateway ユーザが問題に直面する、Simple Object Access Protocol（SOAP）エンベロープの処理と Secure Sockets Layer（SSL; セキュア ソケット レイヤ）接続のセットアップという構成の 2 つのエリアを扱います。

SOAP サービスの問題のトラブルシューティング

SOAP メッセージを処理するとき、他のネットワーク トラフィックの処理と同様に、ACE XML Gateway は、ユーザを識別および認証し、受信および発信メッセージをルーティングし、ロギングについての関連設定に基づきそのアクティビティを記録します。また、ACE XML Gateway は、SOAP メッセージ自体の構造およびコンテンツに関わるいくつかの処理タスクも実行します。

SOAP メッセージの転送で問題が発生する場合、エラーが発生した考えられる段階は数多くあります。このため、トラブルシューティングには系統的に取り組む必要があります。

失敗した SOAP 接続をトラブルシューティングするには、次の手順を示されている順番で行います。

ステップ 1 アプライアンス間の物理ネットワークと IP 接続をチェックします。

詳細については、「ネットワークのチェック」（P.37-388）を参照してください。

ステップ 2 クライアント アプライアンスとサーバ アプライアンスの SOAP 設定をチェックします。

接続の両端が、SOAP メッセージングを正しくサポートできるようにセットアップされていることを確認します。設定のチェックの際に、接続の問題につながる疑いがある設定があればメモしてください。

詳細については、「クライアントとサービスのセットアップのチェック」（P.37-388）を参照してください。

ステップ 3　イベント ログをチェックして、エラーの記録がないかどうか確認します。

エラーの記録が見つかったら、ログ ビューアで詳細を確認し、エラー発生のメカニズムを示す可能性がある手がかりを探します。トラブルシューティングのための一時的な措置として、ロギングのレベルを **Debug** に変更してメッセージ トラフィックを繰り返すことができます。これにより、ACE XML Gateway からできるだけ多くの量の記録を得ることができます。トラブルシューティングが完了したら、ロギングのレベルを設定し直してを最適なスループットを確保してください。

詳細については、「イベント ログのチェック」（P.37-389）を参照してください。

ステップ 4　メッセージ ログをチェックして、記録されたエラー メッセージを調べます。

ここでも、記録されたエラーの詳細を確認して、問題の原因の手がかりを掴みます。前の手順と同様に、ロギングのレベルを変更して記録される情報の量を増やすことができます。

詳細については、「メッセージ ログのチェック」（P.37-389）を参照してください。

ステップ 5　メッセージ ログで、メッセージ処理の 4 つの段階をたどり、失敗に関わるメッセージをトレースします。

エラーが発生した段階を発見できれば、問題の原因にすばやくたどり着けます。

詳細については、「メッセージ ログのチェック」（P.37-389）を参照してください。

ステップ 6　SOAP および Extensible Markup Language（XML）ツールを使用して、メッセージの内容を分析します。

有効であることがわかっているテスト ファイルを作成して、そのファイルをシステム経由で送信し、処理されたファイル データが元のデータと一致するかどうかを確認します。

詳細については、「メッセージ内容の分析」（P.37-390）を参照してください。

ネットワークのチェック

重大なトラブルシューティング作業を行う場合は、必ず、最初に、ネットワーク接続をチェックしてください。

- ケーブルの損傷や劣化はありませんか。ケーブルを観察してください。何らかの欠陥があると思える場合は、ケーブル テスターを使用するかまたは問題があると思えるケーブルを問題のないことがわかっているケーブルと代えて、ケーブルが正常かどうかを確認します。
- ケーブルが抜けていませんか。ケーブル接続が正しく行われているかどうかを確認します。
- ドメイン ネーム サーバが停止していませんか。
- ルータやネットワーク ファイアウォールの設定が変更されていませんか。ネットワーク ファイアウォールの設定をチェックして、クライアントが必要なポートでソケット接続を開放できることを確認します。
- `ping` や `telnet` などの簡単なツールを使用してネットワーク接続できますか。クライアントとサービス間の基本接続が機能していることを確認するには、ACE XML Gateway にアクセスできなければならないシステムから ACE XML Gateway に ping を送信します。

クライアントとサービスのセットアップのチェック

ネットワーク接続に問題がないことが判明したら、メッセージの転送レベルに問題がないかどうかを確認できます。

- クライアントとサーバが SOAP トラフィックを送受信できるように正しく設定されていますか。
- クライアントは SOAP メッセージを作成して送信できますか。

- クライアントの SOAP メッセージは、改ざんされることなくバックエンド サーバに届きますか。
- SOAP サーバは正しく設定されていますか。稼動していますか。

上記の確認事項に回答するための具体的なプロセスは、使用するクライアントおよびサーバ ソフトウェア、ならびに使用できる診断ツールにより異なります。上記の確認事項への回答を決めにくい場合は、サポート担当者に問い合せてください。

クライアント システムとサーバ システムの状態について調査するとき、実際に作成され送信されている SOAP メッセージに影響を及ぼしている可能性がある設定に注目します。この場合も、調査対象になる設定は、クライアントおよびサーバ ソフトウェアによって異なりますが、関係があると思えるのであればどんな設定にも注意を払ってください。そのことは決して無駄にはなりません。

また、ドメイン名やパス名が間違っていないかも確認してください。たとえば、SOAP クライアントのメッセージの送信先のアドレスやパスが間違っていないか、ほんとうに対象のサービスにたどり着けるのかをチェックしてください。また、クライアントが Document スタイルの メッセージを送信するように設定されている場合は、ACE XML Gateway 上の対応ハンドラが Document スタイルのメッセージの受信を予想しているかどうかを確認します。同様に、Remote Procedure Call（RPC; リモート プロシージャ コール）スタイルのメッセージを送信するように設定されている場合は、ハンドラが RPC スタイルのメッセージの受信を予想しているかどうかを確認します。

イベント ログのチェック

クライアント ソフトウェアとサーバ ソフトウェアが正しく設定され動作していることとメッセージが正しく送信されていることを確信できたら、次に、ACE XML Manager のイベント ログをチェックしてエラー メッセージがないか確認します。クライアントが何らかのエラーを含む SOAP メッセージを送信している場合や現在のポリシーまたは SOAP 設定で許可されていない方法での配信を試みている場合は、ACE XML Gateway がエラー イベントを記録することが考えられます。「警告」イベントや「エラー」イベントには、特に注意してください。

イベント ログの右側のカラムには、記録された各イベントが示されその横に簡単な説明が表示されます。このカラムの説明に目を通して SOAP メッセージの不具合が原因で発生した可能性がある問題を確認します。必要な場合は、できるだけ多くの情報を記録できるように ACE XML Manager のイベント ロギングのレベルを Debug に切り替え、メッセージを送信し直してみます。

メッセージ ログのチェック

イベント ログで手がかりが見つからなかった場合は、メッセージ ログを調べてみます。設定ミスなどの問題がある場合、ACE XML Gateway は SOAP メッセージについて他の操作はもとより処理も行いません。このため、メッセージ ログはそれほど役に立たない可能性があります。そのようなケースでは、ACE XML Gateway が SOAP メッセージを処理しないため、SOAP メッセージは記録されません。一方、ACE XML Gateway がメッセージを受け付け処理している場合は、ログにその記録が残ります。その場合は、メッセージの経過表示をトレースして、4 段階から成る処理のどの位置で問題が発生したかを確認できます。消失したメッセージがあれば、最低でも、要求の処理、メッセージの配信、サーバによる応答の返送のうちどの段階で障害が発生したかの確認に役立ちます。

SOAP メッセージ自体が記録されていなくても、ログにはエラー メッセージが記録されている可能性があります。さらに、処理の前にサーバの応答が拒否されている場合でも、サービスに到達する前の受信および発信要求の記録を確認できるはずです。この場合、記録されたメッセージから、要求処理や応答処理がどの位置まで進んでから失敗したのかがわかります。これは、問題の特性を把握するうえで貴重な手がかりになります。

SOAP の情報交換が正常に行われる場合、SOAP クライアントがメッセージを ACE XML Gateway に送り、ACE XML Gateway がメッセージを検証して、処理し、バックエンド サービスに配信します。その後、サービスは応答を ACE XML Gateway に返します。ACE XML Gateway はその応答を検証、処理した後でクライアントに返します。ログに保存されたイベントとメッセージの記録を使用して、失敗したメッセージがこのプロセスのどの位置まで到達してから失敗したのかを確認してください。これは、問題の特性を推定するための重要な足がかりになります。

メッセージ内容の分析

クライアント、サーバ、および Gateway の設定がすべて正しいと思える場合やログからは問題の特性を解明するための手がかりを見つけられなかった場合は、`xmllint`、XMLSpy などの XML ツールを使用してメッセージ自体を検証します。ご使用の SOAP クライアントを使用してメッセージを生成しファイルに保存します。次に、使い慣れたツールを利用して、メッセージ内の XML データが予想と一致するかどうかを確認します。

この方法で明らかにできる問題のタイプの 1 つに、一部のクライアントがメッセージの SOAP アクション部分の外側に保存されたデータを参照する要素を含む SOAP メッセージを作成する場合があります。たとえば、メッセージが SOAP アクションと何らかの補助 XML 要素を含む XML ドキュメントで構成され、SOAP アクションが補助要素に保存されたデータを参照する要素を含む場合があります。ACE XML Gateway が処理するのは SOAP アクション自体だけなので、メッセージに保存されているがアクションの外部にあるデータは取得できません。そのため、このようにして作成されたメッセージは、ACE XML Gateway がメッセージの検証やそれ以外の処理を試みる際の問題の原因になる可能性があります。

SSL および Transport Layer Security（TLS）接続のトラブルシューティング

SSL 接続は、クライアント側からは、その成否にかかわらずシンプルに見えます。成功している場合は要求と応答が転送され、失敗している場合は転送されません。単にそれだけです。

一方、その背景にはそれより複雑なプロセスがあります。これは、失敗した接続のデバッグを試みると明らかになります。正常な SSL 接続の確立にはいくつかの段階があり、適切でなければならないいくつかの補助リソースがあります。失敗した接続で問題の原因を見つけるには、各段階と補助データを順を追って丁寧に検証する必要があります。

次に、手順の概要を示します。

ステップ 1　アプライアンス間の物理ネットワークと IP 接続をチェックします。

詳細については、「ネットワークのチェック」（P.37-388）を参照してください。

ステップ 2　デバッグ レベルのイベント ロギングをイネーブルにして、問題に関わるポート上でテスト メッセージを送信してみます。

詳細については、「テスト メッセージの送信」（P.37-391）を参照してください。

ステップ 3　ログをチェックして、送信されたメッセージのトレースを見つけます。

詳細については、「ログのチェック」（P.37-392）を参照してください。

ステップ 4　ACE XML Gateway のセキュリティ リソースをチェックします。

詳細については、「セキュリティ リソースのチェック」（P.37-392）を参照してください。

ステップ 5　ユーザの識別名とアクセス権限をチェックします。

詳細については、「オーセンティケータおよびポリシーのチェック」（P.37-393）を参照してください。

ステップ 6　ポリシーをチェックして、予想されているメッセージの処理方法を確認します。

詳細については、「オーセンティケータおよびポリシーのチェック」（P.37-393）を参照してください。

以降では、これらの手順について詳しく説明します。

ネットワークのチェック

重大なトラブルシューティング作業を行う場合は、必ず、最初に、ネットワーク接続をチェックしてください。

- ケーブルの損傷や劣化はありませんか。

  ケーブルを観察してください。何らかの欠陥があると思える場合は、ケーブル テスターを使用するかまたは問題があると思えるケーブルを問題のないことがわかっているケーブルと代えて、ケーブルが正常かどうかを確認します。

- ケーブルが抜けていませんか。

  ケーブル接続が正しく行われているかどうかを確認します。

- ドメイン ネーム サーバが停止していませんか。
- ルータやネットワーク ファイアウォールの設定が変更されていませんか。

  ネットワーク ファイアウォールの設定をチェックして、クライアントが必要なポートでソケット接続を開放できることを確認します。

- `ping` や `telnet` などの簡単なツールを使用してネットワーク接続できますか。

  クライアントとサービス間の基本接続が機能していることを確認するには、ACE XML Gateway にアクセスできなければならないシステムから ACE XML Gateway に ping を送信します。

テスト メッセージの送信

テスト メッセージを送信する前に、ACE XML Gateway で、デバッグ レベルのイベント ロギングをイネーブルにして、テストでできるだけ多くの情報を記録できるようにします。問題が発生している SSL 接続に対するトラフィックがデバッグ レベルで記録されることを確認してください。ログレベルの設定について詳しくは、第 32 章「システム ステータスの監視」を参照してください。

次に、SSL 接続をサポートするクライアントを使用して、1 つまたは複数のテスト メッセージを問題が発生しているサービスに送信してみます。

Microsoft 社では、WFetch という名前のユーティリティを無償で提供しています。このユーティリティは、Web サービス接続のデバッグに役立つ機能を備えています。WFetch は、さまざまな接続に対応しますが、SSL 接続にも対応します。WFetch は、無償でダウンロードできる Microsoft Internet Information Server（IIS; インターネット情報サーバ）6.0 Resource Kit Tools に含まれています。

UNIX 系のプラットフォームから接続をテストする必要がある場合は、`curl` ツールを使用できます。このツールも SSL 接続に対応します。`curl` ツールは、システムにインストール済みの場合があります。このツールは、UNIX 系の多くのシステムに付属しています。システムに付属していない場合は、http://curl.haxx.se から入手できます。

お使いのテスト ツールの SSL 機能を使用して、失敗したメッセージにできるだけよく似たメッセージを送信します。できれば、失敗したメッセージで使われたものと同じクライアント証明書を使用してテスト メッセージを送信します。テスト メッセージは成功するが通常のトラフィックは失敗する場合、失敗の原因は SSL 構成やハンドシェイクの問題にあるのではなく、ポリシーの設定またはメッセージのコンテンツに関する問題にあると思われます。

（注）　『*Cisco ACE XML Gateway Getting Started Guide*』では、Wfetch を使用した ACE XML Gateway のテスト方法を例を使って正しい順序で説明しています。

ログのチェック

テスト メッセージが失敗する場合は、イベント ログを調べて失敗した通信に関する記録を見つけます。イベント ログの検証方法の詳細については、「Monitoring System Status」の「Inspecting the Logs」を参照してください。

ログを調べて、テスト セッションが ACE XML Gateway に接続されたことと SSL 接続経由でテスト メッセージの送信が試みられたことの証拠になる記録を探します。できるだけ詳しい情報を得るために、メッセージの送信前に、イベント ログを「デバッグ」レベルでの記録に設定します。次に、イベント ログを参照して、メッセージが受理され処理されたことの証拠になる記録を探します。

ロギングのレベルを「デバッグ」に設定すると、イベント ログとメッセージ ログに記録されたエラーの検索に加えて、ACE XML Gateway が記録する SSL トレース項目だけに焦点を合わせてイベント ログをチェックできます。SSL トレースにより記録されたエラーや警告は、問題の原因に直接結び付くことがあります。たとえば、クライアントが ACE XML Gateway のサーバ証明書を拒否すると、通常、SSL トレースにより「client unexpectedly terminated connection（クライアントが予想に反して接続を切断しました）」などの内容のエントリが生成されます。

ログを検索するとき、クライアントが提供した証明書の DN または サムプリント（Thumbprint、拇印）を探します。DN やサムプリントが見つからない場合は、クライアントが送信していない可能性があります。クライアントの設定をチェックしてください。

ログで DN またはサムプリントが見つかったがエラー メッセージと関連付けられている場合は、ACE XML Gateway が何らかの理由で接続を拒否しています。このメッセージを処理しているハンドラに関連付けられたオーセンティケータおよび権限付与グループをチェックし、その後で、ACE XML Gateway とクライアント上のセキュリティ リソースをチェックします。セキュリティ リソースの詳細については、「セキュリティ リソースのチェック」（P.37-392）を参照してください。

DN またはサムプリントが見つかったがトラフィックの記録やエラー メッセージは見つからない場合は、ACE XML Gateway が受信メッセージをどのオーセンティケータにもマッピングしていません。この場合は、オーセンティケータの設定をチェックします。

クライアントと ACE XML Gateway との間で発生する問題は、ACE XML Gateway とサービス間でも発生します。そのため、同じトラブルシューティングの方法が適用されます。

セキュリティ リソースのチェック

ユーザと ACE XML Gateway は、X.509 証明書を使って SSL 接続を確立します。

- X.509 証明書は、接続の両側で有効でなければなりません。
- 証明書は、その証明書の用途に適合するものでなければなりません。
- ACE XML Gateway とクライアントまたはサービスは、実際に証明書を使用できなければなりません。

よくある問題の 1 つが、ACE XML Gateway が自身を識別するために提供するサーバ証明書をクライアントが拒否することです。クライアントが証明書を拒否するのには、次に示すようにさまざまな理由があります。

- その用途フィールドがサーバの識別に適合していない証明書をアップロードした可能性があります。

- 証明書の署名を行った Certificate Authority（CA: 認証局）がクライアントで信頼するように設定されている CA でない可能性があります。
- 証明書のデータと特定のクライアントのライブラリの間にわずかな違いがあることがあります。
- 証明書が失効している可能性があります。

クライアントまたは ACE XML Gateway が尊重している Certificate Revocation List（CRL; 失効証明書リスト）をチェックします。

- 証明書の有効期間に現在の日時が含まれていない可能性があります。証明書の有効期間をチェックします。

このような問題については、証明書を別のものと取り換えてみたり、別のクライアンで試してみたりすることで検証できます。他の処理と同様に、この処理もクライアント ソフトウェア側と ACE XML Gateway 側に接続の確立方法について共通の認識があるかどうかを確認することから始めます。

また、証明書をチェックして複数の段階から成る検証チェーンがあるかどうかを確認します。検証チェーンがある場合、証明書を使用するには、チェーンの各段階の証明書が ACE XML Gateway にインストールされていなければなりません。

上記の問題はどれも、接続の両方の側（ACE XML Gateway とサービス間およびユーザと Gateway 間）で発生する可能性があります。接続のどちら側をトラブルシューティングする場合も、診断方法は同じです。

オーセンティケータおよびポリシーのチェック

ユーザが開いているポートに接続するかまたはメッセージを送信するには、事前に、ACE XML Gateway のポリシーでそのユーザの有効なオーセンティケータが定義され、サービスのハンドラがオーセンティケータを含む権限付与グループにプロビジョニングされていなければなりません。

セキュリティ リソースを含む、セットアップに関するその他の項目が正しいと思われるのに SSL 接続が失敗する場合は、クライアントに関連付けられたオーセンティケータをチェックします。

- ACE XML Gateway のポリシーで、クライアントに対して有効なオーセンティケータが定義されていることを確認します。
- オーセンティケータが要求する認証方法が、クライアントが実際に使用しているものと一致することを確認します。

また、次のように操作して、メッセージをサービスにルーティングするハンドラもチェックします。

- クライアントが実際に送信するメッセージを受け入れるようにハンドラが設定されていることを確認します。
- クライアントのメッセージを正しいサービスに配信するようにハンドラが設定されていることを確認します。
- ハンドラをユーザの権限付与グループにプロビジョニングしたことを確認します。

診断スナップショットの生成

ACE XML Manager は、システムの問題のトラブルシューティングに役立つ診断スナップショットを生成できます。シスコのサポート担当者は、システムで実際に機能している設定とポリシーに関する詳細情報を集めたこのアーカイブを使用してセキュリティやパフォーマンスに関する問題を分析および診断できます。

診断スナップショットは Cisco ACE XML ゲートウェイ システムの状態に関する非常に詳しい記録を生成するため、慎重に保護する必要があります。診断スナップショットを作成できるのは、Web コンソールで Administrator のロールを持つユーザだけです。このロールの付与は慎重に行い、ネットワークの最も機密性が高いデータへのアクセスを必要とするユーザ以外には与えないでください。

[Diagnostic Snapshot] ページでは、セキュリティ ポリシーに含まれる機密情報の管理を強化するために、暗号鍵、ログの内容など、特定の情報をスナップショットに含めるかどうかを指定できます。

診断スナップショットの生成手順

診断スナップショットを生成するには、次の手順を実行します。

ステップ 1　サポート担当者に問い合せて、診断スナップショットの生成が必要かどうかを確認します。

サポート担当者は、診断スナップショットの生成が適切であることを確認すると、シスコ診断スナップショット アップロード ページへのログインに使用できるユーザ名とパスワードをユーザに割り当てます。また、任意で、トラブル チケット番号を提供することもあります。このチケット番号は、サポート ケースとそのサポート ケースに関連付けられたファイル（スナップショットなど）の識別に使用できます。

ステップ 2　ACE XML Manager の Web コンソールに `Administrator` ユーザでログインします。

（注）　セキュリティを考慮して、Administrator ユーザ以外は診断スナップショットを作成できないようになっています。

ステップ 3　ナビゲーション メニューの [Administration] セクションで [Diagnostic Snapshot] リンクをクリックします。

ステップ 4　[Diagnostic Snapshot] ページで、次のオプションからスナップショットの内容を選択します。

- [Private/Keypair resource files]：デフォルトでは、このチェックボックスは選択されていません。サポート担当者が要求する場合を除いて、スナップショットには公開鍵と秘密鍵ペアのデータは含めないようにしてセキュリティを確保してください。このようなファイルから、通常、機密扱いにする必要がある暗号鍵の情報が漏れることがあります。
- [Extension (SDK) files]：ACE XML Gateway SDK を使用して開発されアプライアンスにインストールされている、Jars ファイルおよびリソース ファイルをスナップショットに含めます。

  拡張ファイルを利用すれば、独自に決めている認証スキーマやメッセージ全体を変更できます。これらのファイルにアクセスできれば、攻撃者がそれを利用して、認証スキーマに攻撃を加え、転送中のメッセージからデータを抽出したりメッセージに悪意のあるコードを埋め込んだりする可能性が生まれます。拡張ファイルを含めるかどうかを選ぶ際には十分に注意してください。
- [Event log]：通常、システムが予想外の動作をする場合の最初に調査すべき場所はいくつかありますが、その 1 つがイベント ログです。サポート担当者がスナップショットにイベント ログのデータを含める必要はないと言っている場合を除いて、[Event log] チェックボックスはチェックしたままにしておく必要があります。

  スナップショットに含めるイベント ログ データの量を制限するには、[Event log] フィールドにイベントの数を入力します。デフォルトでは、ログ内の最近の 1000 個のエントリが含まれます。サポート担当者と相談してチェックを行った後、スナップショットに含めるエントリの数を調整できます。
- [Message Traffic Log]：貴重な診断情報を提供します。サポート担当者が推奨する場合を除いて、メッセージ トラフィック ログはスナップショットから除外しないでください。

スナップショットに含めるメッセージ トラフィック ログの量に制限を加えるため、[most recent] フィールドにメッセージ トラフィック ログの数を入力します。

大量のトラフィックを扱う ACE XML Gateway やメッセージを詳細に記録する ACE XML Gateway では、メッセージ トラフィック ログのサイズが非常に大きくなる可能性があります。その場合、スナップショットに含めるログ データの量を制限することができます。デフォルトでは、スナップショットには最近のメッセージ トラフィック ログ ファイルだけが含まれます。サポート担当者と相談してチェックを行った後、スナップショットへのメッセージ トラフィック ログ ファイルの追加を指定できます。

ステップ 5　スナップショットは、ユーザが [Encryption Passphrase] フィールドに入力したパスフレーズを使用して暗号化されます。ACE XML Manager は、パスフレーズを使用して診断スナップショットのデータを暗号化します。

パスフレーズはサポート担当者に知らせて、担当者が診断スナップショットの復号に使用できるようにする必要があります。このため、所属している組織あるいは個人で独自に使っているパスフレーズは選ばないでください。サポート担当者に正確に伝えるために、パスフレーズはメモしておくことを推奨します。ただし、セキュリティのために、スナップショットの生成または転送に使うコンピュータにパスフレーズを記録しないでください。

ステップ 6　[Repeat Passphrase] フィールドにパスフレーズを再入力します。この値は、[Encryption Passphrase] フィールドに入力したパスフレーズと一字一句一致する必要があります。

ステップ 7　シスコサポートと協力してトラブル チケットを開いている場合は、[Trouble Ticket #] フィールドにその番号を入力します。また、独自のトラッキング番号を指定することもできます。ユーザとシスコのサポート担当者は、[Trouble Ticket #] フィールドの値を使用して、スナップショットに記述されている問題の処理経過を追跡できます。

ステップ 8　次のいずれかのオプションを選択して、スナップショットのファイル名を指定します。

- ファイル名を自動的に生成する場合（デフォルト）は、ページの [Snapshot Output Options] セクションの [Generate Automatically] ボタンをクリックします。ACE XML Manager により `snapshot[ タイムスタンプ ].tgz` という形式で名前が自動生成されます。
- 別のファイル名を指定するには、[Custom] をクリックして固有の識別名を [Custom] ボタンの右のフィールドに入力します。

  ファイル拡張子 `.tgz` は、入力したファイル名に自動的に追加されます。たとえば、`myFile` という名前を指定すると、そのスナップショットには `myFile.tgz` という名前が付けられます。

ステップ 9　[Generate Diagnostic Snapshot] ボタンをクリックして、スナップショット ファイルを生成します。ダイアログボックスで、ファイルの保存先にするファイル システムの位置を選択します。

ファイルを保存したら、取り決めた方法でスナップショットをサポート担当者に送信します。