CHAPTER 12

AnyConnect セッションの管理、モニタリング、およびトラブルシューティング

この章では、次のテーマおよびタスクについて説明します。

- 「すべての VPN セッションの接続解除」（P.12-1）
- 「個々の VPN セッションの接続解除」（P.12-2）
- 「詳細な統計情報の表示」（P.12-2）
- 「VPN 接続の問題の解決」（P.12-2）
- 「DART を使用したトラブルシューティング情報の収集」（P.12-4）
- 「AnyConnect クライアントのインストール」（P.12-10）
- 「ログ ファイルのインストール」（P.12-10）
- 「AnyConnect の接続解除または初期接続の確立に関する問題」（P.12-12）
- 「トラフィックを渡す際の問題」（P.12-13）
- 「AnyConnect のクラッシュに関する問題」（P.12-14）
- 「VPN サービスへの接続に関する問題」（P.12-15）
- 「PC のシステム情報の取得」（P.12-16）
- 「サードパーティ製アプリケーションとの競合」（P.12-16）

すべての VPN セッションの接続解除

セッションを含め、すべての SSL VPN セッションをログオフするには、グローバル コンフィギュレーション モードで Cisco AnyConnect Secure Mobility Client **vpn-sessiondb logoff svc** コマンドを使用します。

vpn-sessiondb logoff svc

これに応答して、システムは VPN セッションをログオフするかどうかを確認するように要求します。確認するために、**Enter** キーを押すか、または **y** を入力します。ログオフをキャンセルするには、その他のキーを入力します。

次に、すべての SSL VPN セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff svc
INFO: Number of sessions of type "svc" logged off : 1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions logged off : 6
hostname#
```

個々の VPN セッションの接続解除

name オプションまたは **index** オプションのいずれかを使用して、個々のセッションをログオフできます。

vpn-sessiondb logoff name *name*

vpn-sessiondb logoff index *index*

たとえば、ユーザ tester をログオフさせるには、次のコマンドを入力します。

```
hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
hostname#
```

ユーザ名とインデックス番号（クライアント イメージの順序で設定される）は、両方とも **show vpn-sessiondb svc** コマンドの出力で確認できます。

次の例では、**vpn-sessiondb logoff** コマンドの **name** オプションを使用して、セッションを終了します。

```
hostname# vpn-sessiondb logoff name testuser
INFO: Number of sessions with name "testuser" logged off : 1
```

詳細な統計情報の表示

現在の AnyConnect セッションに関する統計情報を表示するには、ユーザの GUI の [詳細（Details）] ボタンをクリックします。

[統計情報詳細（Statistics Details）] ダイアログが表示されます。このウィンドウの [統計情報（Statistics）] タブでは、統計情報のリセットとエクスポート、およびトラブルシューティング用のファイル収集を行えます。

このウィンドウで使用できるオプションは、クライアント PC にロードされているパッケージによって異なります。オプションを使用できない場合は、そのオプションのボタンはアクティブにならず、ダイアログボックスのオプション名の横に [（未インストール）((Not Installed)）] というインジケータが表示されます。オプションは次のとおりです。

- [リセット（Reset）] をクリックすると、接続情報がゼロにリセットされます。AnyConnect による新しいデータの収集がすぐに開始されます。
- [エクスポート ...（Export Stats...）] をクリックすると、接続の統計情報がテキスト ファイルに保存され、あとから分析とデバッグを行えます。
- [トラブルシュート ...（Troubleshoot...）] をクリックすると、AnyConnect Diagnostics and Reporting Tool（DART）ウィザードが起動されます。このウィザードでは、指定したログ ファイルとクライアント接続の分析とデバッグに使用できる診断情報を結び付けます。DART パッケージについては、「DART を使用したトラブルシューティング情報の収集」（P.12-4）を参照してください。

VPN 接続の問題の解決

VPN 接続の問題を解決するために、以下の項を参照してください。

MTU サイズの調整

多くの家庭用エンド ユーザ終端装置（たとえば、ホーム ルータ）は、IP フラグメント（特に UDP）の作成またはアセンブリを適切に処理しません。DTLS は UDP ベースのプロトコルであるため、場合によっては MTU を小さくして、フラグメンテーションを防止する必要があります。MTU パラメータでは、クライアントと ASA にトンネルで転送するパケットの最大サイズが設定されます。VPN ユーザで大量のパケット損失が発生している場合、または Microsoft Outlook などのアプリケーションがトンネル経由で機能しない場合は、フラグメンテーションの問題が発生している可能性があります。ユーザまたはユーザのグループの MTU を減らすことで、問題が解決されることがあります。

AnyConnect が確立する SSL VPN 接続の最大転送ユニット サイズ（256 ～ 1406 バイト）を調整するには、次の手順に従ってください。

ステップ 1　ASDM インターフェイスで、[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）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] の順に選択します。

[内部グループ ポリシーの編集（Edit Internal Group Policy）] ダイアログボックスが表示されます。

ステップ 2　[詳細（Advanced）] > [SSL VPN クライアント（SSL VPN Client）] の順に選択します。

ステップ 3　[継承（Inherit）] チェックボックスをオフにして、MTU フィールドで適切な値を指定します。

デフォルトのグループ ポリシーでは、このコマンドのデフォルトのサイズは 1406 です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

この設定が影響を与えるのは、SSL で確立された AnyConnect 接続と、DTLS を使用する SSL で確立された AnyConnect 接続のみです。

最適 MTU（OMTU）

最適 MTU（OMTU）機能を使用して、クライアントが DTLS パケットを正常に渡すことができる最大エンドポイント MTU を検出します。最大 MTU に埋め込まれた DPD パケットを送信することによって、OMTU を実装します。ヘッドエンドから戻されるペイロードの正しいエコーを受信すると、MTU サイズが受け入れられます。受け入れられなかった場合、MTU は小さくされ、プロトコルで許可されている最小 MTU に到達するまで、繰り返しプローブが送信されます。

（注）　OMTU を使用しても、既存のトンネル DPD 機能を妨げることはありません。

この機能を使用するには、ASA で DPD を有効にする必要があります。DPD は、埋め込みが許可されない標準実装に基づくため、この機能は、IPsec とは併用できません。

DART を使用したトラブルシューティング情報の収集

DART は AnyConnect Diagnostics and Reporting Tool の略で、AnyConnect 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に役立つデータの収集に使用できます。DART は、Windows 7、Windows Vista、Windows XP、Mac バージョン 10.5 と 10.6、および Linux Redhat をサポートします。

DART ウィザードは、AnyConnect が稼働するコンピュータ上で実行されます。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。DART の実行に管理者権限は不要です。

DART は、AnyConnect ソフトウェアのコンポーネントに依存せずに機能しますが、AnyConnect から起動可能で、AnyConnect ログ ファイル（存在する場合）の収集を行います。

現在のところ、DART はスタンドアロン インストールを実行できます。または、管理者は AnyConnect ダイナミック ダウンロード インフラストラクチャの一部として、このアプリケーションをクライアント PC にプッシュできます。インストールされると、[スタート（Start）] ボタンにある Cisco フォルダから、DART ウィザードを起動できます。

DART ソフトウェアの入手

Web 展開方式または AnyConnect の事前展開方式のいずれかを使用して、DART をクライアントにインストールできます。

どのバージョンの DART も、すべてのバージョンの AnyConnect に使用できます。それぞれのバージョン番号は同期化されていません。

表 12-1 に、事前展開インストーラおよび Web 展開（ダウンロード）インストーラの DART を含む AnyConnect のダウンロード（ファイルとパッケージの両方）を示します。3.0.3050 よりも前のリリースでは、DART コンポーネントは Web 展開用に個別のダウンロード（dmg、.sh、または .msi ファイル）になっていました。リリース 3.0.3050 以降では、DART コンポーネントは .pkg ファイルに含まれています。

表 12-1　ASA または Pre-Deployment 用の DART ファイルまたはパッケージ ファイル名

DART	Web-Deploy ファイル名およびパッケージ（ダウンロード）	Pre-Deploy インストーラ
Windows	*リリース 3.0.3050 以降：* anyconnect-win-(ver)-k9.pkg	anyconnect-win-(ver)-pre-deploy-k9.iso
	3.0.3050 よりも前のリリース： anyconnect-dart-win-(ver)-k9.msi*	anyconnect-dart-win-(ver)-k9.msi*
Mac	*リリース 3.0.3050 以降：* anyconnect-macosx-i386-(ver)-k9.pkg	anyconnect-macosx-i386-(ver)-k9.dmg
	3.0.3050 よりも前のリリース： anyconnect-dartsetup.dmg	anyconnect-dart-macosx-i386-(ver)-k9.dmg
Linux	*リリース 3.0.3050 以降：* anyconnect-linux-(ver)-k9.pkg	anyconnect-predeploy-linux-(ver)-k9.tar.gz
	3.0.3050 よりも前のリリース： anyconnect-dartsetup.sh	anyconnect-dart-linux-(ver)-k9.tar.gz
Linux-64	*リリース 3.0.3050 以降：* anyconnect-linux-64-(ver)-k9.pkg	anyconnect-predeploy-linux-64-(ver)-k9.tar.gz
	3.0.3050 よりも前のリリース： anyconnect-dartsetup.sh	anyconnect-dart-linux-64-(ver)-k9.tar.gz

Web 展開および事前展開のパッケージには、ISO イメージ（.iso）が含まれています。ISO イメージ ファイルには、ユーザのコンピュータへの展開に必要なプログラムと MSI インストーラ ファイルが含まれています。.iso イメージとその内容の詳細については、「事前展開パッケージ ファイル情報」（P.2-29）を参照してください。

DART のインストール

管理者は、DART を AnyConnect インストールの一部に含めることができます。

AnyConnect を AnyConnect で動作する PC にダウンロードしたときに、新しいバージョンの DART がある場合は、その DART とともにダウンロードされます。新しいバージョンの AnyConnect が自動アップグレードの一部としてダウンロードされるとき、新しいバージョンの DART がある場合は、それもダウンロードに含まれます。

（注）　グループ ポリシー設定（**svc modules** コマンドまたは対応する ASDM ダイアログで設定）に **dart** キーワードがない場合は、DART がパッケージに含まれていても、AnyConnect は DART をインストールしません。

AnyConnect を使用した DART のインストール

この手順では、次回リモート ユーザが接続するときに、そのユーザのマシンに DART がダウンロードされます。

ステップ 1　他のシスコのソフトウェア パッケージと同様に、DART を含む AnyConnect パッケージを ASA にロードします。

ステップ 2　DART を含む AnyConnect の .pkg ファイルをセキュリティ アプライアンスにインストール後、AnyConnect と一緒に DART をインストールするには、グループ ポリシーで DART を指定する必要があります。これは、次のように ASDM または CLI を使用して実行できます。

ASDM を使用する場合：

a. [設定（Configuration）] をクリックしてから、[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 Policy）] の順にクリックします。

b. 新しいグループ ポリシーを追加するか、既存のグループ ポリシーを編集します。グループ ポリシーのダイアログボックスで、[詳細（Advanced）] を展開し、[SSL VPN クライアント（SSL VPN Client）] をクリックします。

c. [SSL VPN クライアント（SSL VPN Client）] ダイアログボックスで、[ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] オプションの [継承（Inherit）] をオフにします。このオプションのドロップダウン リストから **dart** モジュールを選択します。

d. 使用するバージョンの ASDM に、DART オプションのチェックボックスがない場合は、フィールドにキーワード **dart** を入力します。DART と Start Before Logon の両方をイネーブルにするには、**dart** と **vpngina** の両方を任意の順序でカンマで区切ってそのフィールドに入力します。

[OK] をクリックしてから、[適用（Apply）] をクリックします。

CLI を使用する場合は、**svc modules value dart** コマンドを使用します。

（注）　あとで **svc modules none** に変更したり、[ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] フィールドの DART の選択を解除しても、DART はインストールされたままになります。セキュリティ アプライアンスによって、DART がアンインストールされることはありません。DART を削除するには、Windows のコントロール パネルの、[プログラムの追加/削除（Add/Remove Programs）] を使用してください。この方法で DART を削除しても、ユーザが AnyConnect を使用して再接続すると、自動的に再インストールされます。上位バージョンの DART を含んだ AnyConnect パッケージが ASA にアップロードされ、設定されている場合は、ユーザが接続すると DART が自動的にアップグレードされます。

DART の実行方法については、「Windows での DART の実行」（P.12-8）を参照してください。

Windows デバイスへの DART の手動インストール

Windows デバイスに DART をインストールするには、次の手順を実行します。

ステップ 1　anyconnect-dart-win-(ver)-k9.msi をローカルに保存します。リリース 3.0.3050 以降をインストールしている場合、この DART コンポーネントは、anyconnect-win-(ver)-k9.pkg ダウンロードに含まれています。

ステップ 2　**anyconnect-dart-win-(ver)-k9.msi** ファイルをダブルクリックして、**DART セットアップ ウィザード** を起動します。

ステップ 3　初期画面で [次へ（Next）] をクリックします。

ステップ 4　[ライセンス契約条件に同意します（I accept the terms in the License Agreement）] を選択して、エンド ユーザのライセンス契約に同意し、[次へ（Next）] をクリックします。

ステップ 5　[インストール（Install）] をクリックして、DART をインストールします。インストール ウィザードによって、**DartOffline.exe** が <System Drive>:\Program Files\Cisco\Cisco DART ディレクトリにインストールされます。

ステップ 6　[完了（Finish）] をクリックして、インストールを完了します。

DART の実行方法については、「Windows での DART の実行」（P.12-8）を参照してください。

Linux デバイスへの DART の手動インストール

Linux デバイスに DART をインストールするには、次の手順を実行します。

ステップ 1　anyconnect-dart-linux-(ver)-k9.tar.gz をローカルに保存します。リリース 3.0.3050 以降をインストールしている場合、この DART コンポーネントは、anyconnect-linux-(ver)-k9.pkg ダウンロードに含まれています。

ステップ 2　端末から、**tar -zxvf <***path to tar.gz file including the file name***>** コマンドを使用して tar.gz ファイルを抽出します。

ステップ 3　端末から、抽出したフォルダに移動し、**sudo ./dart_install.sh** コマンドを使用して dart_install.sh を実行します。

ステップ 4　ライセンス契約書に同意し、インストールが完了するまで待機します。

（注）　DART のアンインストールには、**/opt/cisco/anyconnect/dart/dart_uninstall.sh** しか使用できません。

Mac デバイスへの DART の手動インストール

Mac デバイスに DART をインストールするには、次の手順を実行します。

ステップ 1　anyconnect-dart-macosx-i386-(ver)-k0.dmg をローカルに保存します。リリース 3.0.3050 以降をインストールしている場合、この DART コンポーネントは、anyconnect-macosx-i386-(ver)-k9.pkg ダウンロードに含まれています。

ステップ 2　ダウンロードが終了したら、.dmg ファイルは自動的にデスクトップにマウントされ、DART インストール ウィザードが自動的に開始します。インストール ウィザードを手動で開始するには、ダウンロード フォルダに移動し、ダウンロードされた .dmg ファイルをダブルクリックしてデスクトップにマウントします。その後、マウントされたデバイスで dart.pkg をダブルクリックします。

インストール ウィザードに、「This package will run a program to determine if the software can be installed」というメッセージが表示されます。

ステップ 3　[続行（Continue）] をクリックします。ウィザードにライセンス契約書が表示されます。

ステップ 4　[続行（Continue）] をクリックしてから、[承認（Accept）] をクリックし、ライセンス契約書に同意します。

ステップ 5　インストール場所を変更するように求められます。必要に応じて変更し、[続行（Continue）] をクリックします。

ステップ 6　開始するには、インストールの管理者クレデンシャルを入力する必要があります。クレデンシャルを入力したら、[続行（Continue）] をクリックします。インストールが開始されます。

ステップ 7　インストールが完了するまで待機し、[キャンセル（Cancel）] をクリックしてプログラムを終了します。

（注）　DART のアンインストールには、**/opt/cisco/anyconnect/bin/dart_uninstall.sh** しか使用できません。

Windows での DART の実行

Windows 用の DART ウィザードを実行して DART バンドルを作成するには、次の手順を実行します。

ステップ 1　Windows デバイスで実行している場合、AnyConnect GUI を起動します。

ステップ 2　[統計情報（Statistics）] タブをクリックしてから、ダイアログボックス下部の [詳細（Details）] ボタンをクリックします。[統計情報詳細（Statistics Details）] ダイアログボックスが表示されます。

ステップ 3　[統計情報詳細（Statistics Details）] ウィンドウ下部の [トラブルシュート（Troubleshoot）] をクリックします。

ステップ 4　初期画面で [次へ（Next）] をクリックします。[バンドルの作成オプション（Bundle Creation Option）] ダイアログボックスが表示されます。

ステップ 5　[バンドルの作成オプション（Bundle Creation Option）] エリアで、[デフォルト（Default）] または [カスタム（Custom）] を選択します。

- [デフォルト（Default）] オプションでは、代表的なログ ファイルと診断情報が含まれます。たとえば、AnyConnect ログ ファイルや Cisco Secure Desktop ログ ファイル、コンピュータの一般情報、DART が実行した内容と実行しなかった内容についての要約などが含まれます。

  [デフォルト（Default）] を選択してから、ダイアログボックス下部の [次へ（Next）] をクリックすると、DART のバンドル作成が開始されます。バンドルのデフォルト名は DARTBundle.zip で、ローカル デスクトップに保存されます。

- [カスタム（Custom）] を選択した場合は、[次へ（Next）] をクリックすると、DART ウィザードによってさらにダイアログボックスが表示され、バンドルに含めるファイルや、バンドルの保存場所を指定します。

ヒント　[カスタム（Custom）] を選択すると、バンドルに含めるファイルはデフォルトのままにして、ファイルの保存場所だけは別の場所を指定するということもできます。

ステップ 6　DART バンドルを暗号化するには、[暗号化オプション（Encryption Option）] エリアで [バンドル暗号化の有効化（Enable Bundle Encryption）] にチェックを入れてから、[暗号化パスワード（Encryption Password）] フィールドにパスワードを入力します。オプションで [パスワードのマスク（Mask Password）] を選択すると、[暗号化パスワード（Encryption Password）] フィールドおよび [パスワードの再入力（Reenter Password）] フィールドに入力したパスワードが、アスタリスク（*）でマスクされるようになります。

ステップ 7　[次へ（Next）] をクリックします。[デフォルト（Default）] を選択した場合、DART はバンドルの作成を開始します。[カスタム（Custom）] を選択した場合は、ウィザードが次のステップに進みます。

ステップ 8　[ログファイルの選択（Log File Selection）] ダイアログボックスで、バンドルに含めるログ ファイルと設定ファイルを選択します。ネットワーク アクセス マネージャ、テレメトリ、ポスチャ、および Web セキュリティの各ログを含めるオプションがあります。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[デフォルトの復元（Restore Default）] をクリックします。[次へ（Next）] をクリックします。

ステップ 9　[診断情報の選択（Diagnostic Information Selection）] ダイアログボックスで、バンドルに含める診断情報を選択します。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[デフォルトの復元（Restore Default）] をクリックします。[次へ（Next）] をクリックします。

ステップ 10　[コメントとターゲットバンドルの場所（Comments and Target Bundle Location）] ダイアログボックスで、次のフィールドを設定します。

- [コメント（Comments）] エリアに、バンドルに含めるコメントを入力します。DART は、入力したコメントをバンドルに含める comments.txt ファイルに保存します。
- [ターゲットバンドルの場所（Target Bundle Location）] フィールドで、バンドルの保存場所を参照します。

[次へ（Next）] をクリックします。

ステップ 11　[サマリー（Summary）] ダイアログボックスでカスタマイズの内容を確認し、[次へ（Next）] をクリックしてバンドルを作成するか、[戻る（Back）] をクリックしてカスタマイズの内容に変更を加えます。

ステップ 12　DART のバンドル作成が終了したら、[完了（Finish）] をクリックします。

ヒント　状況によっては、DART の実行に数分以上かかったという報告を受けました。デフォルト リストのファイル収集に長い時間を要している思われる場合は、[キャンセル（Cancel）] をクリックしてからウィザードを再実行し、**カスタム** DART バンドルを作成して必要なファイルだけを選択してください。

Linux または Mac での DART の実行

Linux または Mac 用の DART ウィザードを実行して DART バンドルを作成するには、次の手順を実行します。

ステップ 1　Linux デバイスの場合、[アプリケーション（Applications）] > [インターネット（Internet）] > [Cisco DART] または /opt/cisco/anyconnect/dart/dartui から DART を起動します。

Mac デバイスの場合、[アプリケーション（Applications）] > [Cisco] > [Cisco DART] から DART を起動します。

ステップ 2　[統計情報（Statistics）] タブをクリックしてから、ダイアログボックス下部の [詳細（Details）] ボタンをクリックします。[統計情報詳細（Statistics Details）] ダイアログボックスが表示されます。

ステップ 3　[バンドルの作成オプション（Bundle Creation Option）] エリアで、[デフォルト（Default）] または [カスタム（Custom）] を選択します。

- [デフォルト（Default）] オプションでは、代表的なログ ファイルと診断情報が含まれます。たとえば、AnyConnect ログ ファイルや Cisco Secure Desktop ログ ファイル、コンピュータの一般情報、DART が実行した内容と実行しなかった内容についての要約などが含まれます。

  [デフォルト（Default）] を選択してから、ダイアログボックス下部の [次へ（Next）] をクリックすると、DART のバンドル作成が開始されます。バンドルのデフォルト名は DARTBundle.zip で、ローカル デスクトップに保存されます。

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

- [カスタム（Custom）] を選択した場合は、[次へ（Next）] をクリックすると、DART ウィザードによってさらにダイアログボックスが表示され、バンドルに含めるファイルや、バンドルの保存場所を指定します。

ヒント　[カスタム（Custom）] を選択すると、バンドルに含めるファイルはデフォルトのままにして、ファイルの保存場所だけは別の場所を指定するということもできます。

ステップ 4　[次へ（Next）] をクリックします。[デフォルト（Default）] を選択した場合、DART はバンドルの作成を開始します。[カスタム（Custom）] を選択した場合は、ウィザードが次のステップに進みます。

ステップ 5　[ログファイルの選択（Log File Selection）] ダイアログボックスで、バンドルに含めるログ ファイルと設定ファイルを選択します。ネットワーク アクセス マネージャ、テレメトリ、ポスチャ、および Web セキュリティの各ログを含めるオプションがあります。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[デフォルトの復元（Restore Default）] をクリックします。[次へ（Next）] をクリックします。

ステップ 6　[診断情報の選択（Diagnostic Information Selection）] ダイアログボックスで、バンドルに含める診断情報を選択します。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[デフォルトの復元（Restore Default）] をクリックします。[次へ（Next）] をクリックします。

ステップ 7　[コメントとターゲットバンドルの場所（Comments and Target Bundle Location）] ダイアログボックスで、次のフィールドを設定します。

- [コメント（Comments）] エリアに、バンドルに含めるコメントを入力します。DART は、入力したコメントをバンドルに含める comments.txt ファイルに保存します。
- [ターゲットバンドルの場所（Target Bundle Location）] フィールドで、バンドルの保存場所を参照します。

[次へ（Next）] をクリックします。

ステップ 8　DART バンドルを暗号化するには、[暗号化オプション（Encryption Option）] エリアで [バンドル暗号化の有効化（Enable Bundle Encryption）] にチェックを入れてから、[暗号化パスワード（Encryption Password）] フィールドにパスワードを入力します。オプションで [パスワードのマスク（Mask Password）] を選択すると、[暗号化パスワード（Encryption Password）] フィールドおよび [パスワードの再入力（Reenter Password）] フィールドに入力したパスワードが、アスタリスク（*）でマスクされるようになります。

（注）　パスワードをマスクするオプションは、MAC オペレーティング システムでは使用できません。

ステップ 9　[完了（Finish）] をクリックしてウィザードを終了します。

ヒント　状況によっては、DART の実行に数分以上かかったという報告を受けました。デフォルト リストのファイル収集に長い時間を要している思われる場合は、[キャンセル（Cancel）] をクリックしてからウィザードを再実行し、**カスタム** DART バンドルを作成して必要なファイルだけを選択してください。

AnyConnect クライアントのインストール

svc image xyz コマンドを使用して AnyConnect イメージを設定する場合、**svc enable** コマンドを発行する必要があります。このコマンドを発行しないと、AnyConnect は想定したとおりに機能せず、**show webvpn svc** は、インストールされた AnyConnect パッケージをリストする代わりに、「SSL VPN client is not enabled」というメッセージを表示します。

ログ ファイルのインストール

ログ ファイルは、次のファイル内に保持されます。

- \Windows\setupapi.log：Windows XP および Windows 2000
- \Windows\Inf\setupapi.app.log：Windows Vista
- \Windows\Inf\setupapi.dev.log：Windows Vista

（注）　Vista では、隠しファイルを表示する必要があります。

レジストリ情報が setupapi.log ファイルから欠落している場合は、Windows XP ベースのコンピュータ上で冗長ロギングをイネーブルにしてください。Windows XP ベースのコンピュータ上で冗長ロギングをイネーブルにするには、次の手順に従ってください。

（注）　レジストリが誤って変更されると、重大な問題が発生する可能性があります。念のため、レジストリを変更する前に、レジストリをバックアップしてください。

ステップ 1　[スタート（Start）] > [実行（Run）] の順にクリックします。

ステップ 2　[オープン（Open）] フィールドに **regedit** と入力し、[OK] をクリックします。

ステップ 3　HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup レジストリ サブキーにある **LogLevel** を見つけてダブルクリックします。

ステップ 4　[DWORD 値の編集（Edit DWORD Value）] ウィンドウの [ベース（Base）] ペインで [16 進数（Hexadecimal）] を選択します。

ステップ 5　[値（Value）] データ ボックスに **0x2000FFFF** と入力します。

ステップ 6　[OK] をクリックします。

（注）　冗長ロギングをイネーブルにすると、Setupapi.log ファイルのサイズは約 4MB に増加します。レジストリ値をリセットするには、上記のステップを繰り返しますが、ステップ 5 で DWORD 値を 0 に設定してください。

ログ ファイルの Web インストール

これが新規の Web 展開インストールの場合、このログは次のユーザ別の temp ディレクトリに格納されます。

%TEMP%\anyconnect-win-2.X.xxxx-k9-install-yyyyyyyyyyyyyy.log

アップグレードが最適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\anyconnect-win-2.X.xxxx-k9-install-yyyyyyyyyyyyyy.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、**yyyyyyyyyyyyyy** はインストールの日時を示します。

ログ ファイルのスタンドアロン インストール

MSI ロギングをオンにし、インストールのログをキャプチャするには、次のコマンドを実行します。

MSIExec.exe/i anyconnect-win-2.X.xxxx-pre-deploy-k9.msi/lvx* c:\AnyConnect.log

ここで、*anyconnect-win-2.X.xxxx-pre-deplay-k9.msi* は、インストールする実際の msi ファイルの完全な名前です。

ログは次の場所に表示されます。

- \Documents and Settings\<username>\Local Settings\Temp（Windows XP および Windows 2000）
- \Users\<username>\AppData\Local\Temp（Vista）
- \Windows\Temp（自動アップグレードの場合）

スタンドアロンのみを使用する（または、システムにインストールされている ActiveX コントロールを使用しない）場合、次のいずれかを実行します。

（注）　以下のアクションを実行しないと、Windows インストーラ パッケージに関する問題を示す Cisco AnyConnect VPN Error 1722 を受け取ることがあります。

- MSI トランスフォームを作成し、ActiveX プロパティをディセーブル（NOINSTALLACTIVEX=1）に設定する。

```
MISExec /i anyconnect-win-x.x.xxxx-pre-deploy-k9.msi NOINSTALLACTIVEX=1
```

- リブートせずに、次のコマンドを実行して Quiet Install を実行する。

```
msiexec /quiet /i "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
msiexec /quiet /norestart /i "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi
```

- リブートせずに、次のコマンドを実行して Quiet Uninstall を実行する。

```
msiexec /quiet /x "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
```

（注）　*x.x.xxx* の値は、インストールされているバージョンによって異なります。

AnyConnect の接続解除または初期接続の確立に関する問題

AnyConnect クライアントの接続解除または初期接続の確立で問題が発生する場合は、以下の推奨事項に従ってください。

1. 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。
   - 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 サーバの IP アドレスです。
   - 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。
2. ASA イベント ログを表示します。
   a. ASA コンソールで、以下の行を追加し、ssl、webvpn、svc、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 svc console debugging
```

   b. AnyConnect クライアントの接続を試行し、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。
   c. **no logging enable** と入力し、ロギングをディセーブルにします。
3. クライアント PC の Windows イベント ビューアから Cisco AnyConnect VPN クライアント ログを取得します。
   a. [スタート（Start）] > [実行（Run）] の順に選択し、**eventvwr.msc /s** と入力します。

b. アプリケーションおよびサービス ログ（Windows Vista および Windows 7 の）で、**Cisco AnyConnect VPN 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。

c. AnyConnectClientLog.evt などのファイル名を割り当てます。.evt ファイル形式を使用する必要があります。

4. AnyConnect GUI を接続解除または終了する際に問題が発生する場合は、vpnagent.exe プロセスを Windows 診断デバッグ ユーティリティにアタッチします。詳細については、WinDbg のマニュアルを参照してください。

5. IPv6/IPv4 IP アドレスの割り当てに競合が確認された場合は、スニファ トレースを取得し、使用中のクライアント PC のレジストリにルーティング デバッグを追加します。このような競合は、AnyConnect 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
```

VPN 接続を確立する前に特定のレジストリ エントリ（Windows）またはファイル（Mac または Linux）を追加すると、ルート デバッグを 1 つの接続に対して 1 回だけイネーブルできます。

トンネル接続が開始され、このキーまたはファイルが検出されると、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（通常 Windows では C:\Windows\Temp、Mac または Linux では /tmp）に作成されます。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。

トラフィックを渡す際の問題

いったん接続されたプライベート ネットワークに AnyConnect クライアントがデータを送信できない場合は、次の推奨事項に従ってください。

1. show vpn-sessiondb detail svc 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。

2. [AnyConnect VPN クライアント（AnyConnect VPN 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。

3. 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、AnyConnect 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
```

4. 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、次のように非暗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 0.0.83.145.50.1
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 または SSL の 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 83.145.50.1 にルーティングされます。

5. AnyConnect 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。
6. 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、ASA のキャプチャをイネーブルにします。

（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 svc 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。

AnyConnect のクラッシュに関する問題

UI のクラッシュが発生した場合、結果は %temp% ディレクトリ（C:\DOCUME~1\jsmith\LOCALS~1\Temp など）に書き込まれます。リブート後に「The System has recovered from a serious error」というメッセージが表示される場合は、C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson または同様のアプリケーションから生成された .log ファイルおよび .dmp ファイルを収集します。これらのファイルをコピーするか、以下の手順に従ってファイルをバックアップしてください。

ステップ 1　[スタート（Start）] > [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 PC 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 AnyConnect VPN クライアント ログを取得します。

ステップ 4　（Windows Vista および Windows 7 の）[アプリケーションとサービス ログ（Applications and Services Logs）] で **Cisco AnyConnect VPN 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。AnyConnectClientLog.evt などのファイル名を .evt ファイル形式で割り当ててください。

ステップ 5　ドライバ クラッシュが VPNVA.sys で発生する場合は、Cisco VPNVA 仮想アダプタにバインドされた中間ドライバを確認し、それらをオフにします。

ステップ 6　ドライバ クラッシュが vpnagent.exe で発生する場合は、vpnagent.exe プロセスを Windows のデバッグ ツールにアタッチします。ツールがインストールされた後、次の手順を実行します。

a. c:\vpnagent という名前のディレクトリを作成します。

b. 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。

c. 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。

d. **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst** と入力します。この *PID* は、ステップ b で判別した番号です。

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。

e. 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。

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

VPN サービスへの接続に関する問題

「Unable to Proceed, Cannot Connect to the VPN Service」というメッセージが表示される場合、AnyConnect の VPN サービスは実行されていません。VPN エージェントが予期せず終了した可能性があります。別のアプリケーションがサービスと競合したかどうかにかかわらず、トラブルシューティングするには、次の手順を実行します。

ステップ 1　Windows 管理ツールでサービスを確認して、Cisco AnyConnect 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、またはエラー 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ディセーブルにする必要があります。また、このアプリケーションのアンインストール、リブート、または再テストが必要になる場合があります。

ステップ 2　Cisco AnyConnect VPN エージェントを起動してみます。こうすることで、起動時にサーバの初期化または別の実行中のサービス（サービスの起動に失敗したため）と競合しているかどうかを判断します。

ステップ 3　イベント ビューアの AnyConnect ログに、サービスを起動できなかったこと示すメッセージがないか確認します。手順 2 での手動による再起動のタイム 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、AnyConnect クライアントをスタンドアロン 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ディセーブルにして、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。

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、アンチウイルス ソフトウェアなど）をディセーブルにします。リブート後も VPN エージェント サービスが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。

PC のシステム情報の取得

PC のシステム情報を取得するには、次のコマンドを入力し、約 2 分間待機します。

- **winmsd /nfo c:\msinfo.nfo**：Windows XP または Windows 2000
- **msinfo32 /nfo c:\msinfo.nfo**：Windows Vista

Systeminfo ファイル ダンプの取得

Windows XP または Vista の場合、コマンド プロンプトに次を入力し、Systeminfo ファイル ダンプを取得します。

systeminfo >> c:\sysinfo.txt

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。

サードパーティ製アプリケーションとの競合

一部のサードパーティ製アプリケーションでは、AnyConnect 仮想アダプタ ドライバのインストールが禁止されます。この場合、画面がブルー スクリーンになり、ルーティング テーブルを更新できなくなることがあります。DART ツール（「DART を使用したトラブルシューティング情報の収集」（P.12-4）を参照）を使用して、お客様のオペレーティング システム環境に関する情報を収集できます。この診断に基づいて、シスコは次のサードパーティ製アプリケーションとの競合を識別し、解決策を推奨することができます。

Adobe および Apple：Bonjour Printing Service

- Adobe Creative Suite 3
- BonJour Print Service

- iTunes

症状　IP 転送テーブルを正常に検証できない。

考えられる原因　AnyConnect イベント ログは、IP 転送テーブルの識別に失敗したことを示し、ルーティング テーブル内の次のエントリを示しています。

```
Destination 169.254.0.0
Netmask 255.255.0.0
Gateway 10.64.128.162
Interface 10.64.128.162
Metric 29
```

推奨処置　コマンド プロンプトで **net stop "bonjour service"** と入力し、Bonjour Print Service をディセーブルにします。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。

AT&T Communications Manager バージョン 6.2 および 6.7

症状　一部の PC に AT&T Sierra Wireless 875 カードを装着すると、接続に失敗したり、トラフィックが通過できなくなったりする。バージョン 6.2 ～ 6.7 が AnyConnect と競合していると思われる。

考えられる原因　CSTP 転送障害は、AnyConnect 仮想アダプタによってトランスポート層に障害が発生していることを示します。

推奨処置　この問題を解決するには、次の手順を実行します。

1. Aircard でアクセラレーションをディセーブルにします。
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。

AT&T Global Dialer

症状　クライアントのオペレーティング システムでブルー スクリーンが発生し、ミニ ダンプ ファイルが生成されることがある。

考えられる原因　AT&T Dialer の中間ドライバが保留パケットを適切に処理できず、これがオペレーティング システムのクラッシュの原因となっています。他の NIC カード ドライバ（Broadcom など）では、この問題は発生していません。

推奨処置　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。

Citrix Advanced Gateway Client バージョン 2.2.1

症状　AnyConnect セッションを接続解除するときに、次のようなエラーが発生する。

```
VPN Agent Service has encountered a problem and needs to close. We are sorry for
the inconvenience.
```

考えられる原因　メモリを解放するときに、Winsock を使用して Citrix CtxLsp.dll がすべてのプロセスにロードされるため、クラッシュが発生します。

推奨処置　CtxLsp.dll に関するこの問題が解決されるまで、Citrix Advanced Gateway Client を削除してください。

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、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

症状　ワイヤレス サプレッションが有効のときに有線接続を導入すると、無線接続がドロップする。ワイヤレス サプレッションがディセーブルのとき、ワイヤレス機能は期待どおりに動作する。

考えられる原因　Odyssey Client がネットワーク アダプタを管理していません。

推奨処置　次の手順に従って、Odyssey Client を設定します。

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。
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。
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。

Kaspersky AV Workstation 6.x

症状　Kaspersky 6.0.3 がインストールされると（ディセーブルであっても）、CSTP state = CONNECTED の直後に ASA への AnyConnect 接続が失敗する。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.).
```

考えられる原因　Kaspersky AV Workstation 6.x と AnyConnect の間に既知の非互換性が存在します。

推奨処置　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。

McAfee Firewall 5

症状　UDP DTLS 接続を確立できない。

考えられる原因　McAfee Firewall は、デフォルトで受信 IP フラグメントをブロックするため、フラグメント化されている場合、DTLS はブロックされます。

推奨処置　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 [Block incoming fragments automatically] チェックボックスをオフにします。

Microsoft Internet Explorer 8

症状　Internet Explorer 8 を Windows XP SP3 で使用する場合、AnyConnect を WebVPN ポータルからインストールできない。

考えられる原因　ブラウザがインストールでクラッシュします。

推奨処置　Microsoft の推奨策に従って、MSJVM を削除してください。Microsoft のサポート技術情報 KB826878 を参照してください。

Microsoft Routing and Remote Access Server

症状　AnyConnect がホスト デバイスへの接続の確立を試行するときに、次の終了エラーがイベントログに返されます。

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

考えられる原因　ルーティング テーブル上で RRAS と AnyConnect が競合しています。RRAS では、PC はイーサネット ルータとして機能するので、AnyConnect と同様にルーティング テーブルが変更されます。AnyConnect はトラフィックを適切に転送するためにルーティング テーブルに依存するので、この 2 つを一緒に実行できません。

推奨処置　RRAS サービスをディセーブルにします。

Microsoft Windows の更新プログラム

症状　VPN 接続の確立を試行すると、次のメッセージが表示される。

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

考えられる原因　最近、certclass.inf ファイルに Microsoft 更新プログラムが適用されました。次のエラーが C:\WINDOWS\setupapi.log に表示されます。

```
#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.
```

推奨処置　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。修復を試行するには、次の手順を実行します。

1. コマンド プロンプトを管理者として開きます。
2. **net stop CryptSvc** と入力します。
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。
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。

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。

Windows XP（Service Pack 3）

症状　AnyConnect クライアントをインストールできない。次のエラー メッセージが表示されます。

```
This application has failed to start because dot3api.dll was not found.
Re-installing the application may fix this problem.
```

考えられる原因　dot3api.dll ファイルが欠落することは、既知の問題です。

推奨処置　regsvr32 dot3api.dll を再インストールし、オペレーティング システムをリブートします。

OpenVPN クライアント

症状　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、AnyConnect クライアントと互換性がないことを示すエラーが表示される。

考えられる原因　MAC OS X Shimo VPN Client は、この問題を引き起こす可能性があります。

推奨処置　Viscosity OpenVPN Client をアンインストールします。

ロード バランサ

症状　クレデンシャルがないために、接続が失敗する。

考えられる原因　ブラウザが DNS 結果をキャッシュしていても、ポート転送やスマート トンネルなどの追加アプリケーションが DNS 結果をキャッシュしないことがあります。ユーザが X.4 にログインした後、DNS リゾルバが x.15 を使用するように設定されている場合、PF アプレットまたはスマート トンネル アプリケーションは DNS を解決して X.15 に接続します。セッションが確立されていないので、クレデンシャルがないことが原因で接続が失敗します。

推奨処置　サードパーティ製ロード バランサでは、ASA デバイスにかかる負荷を把握できません。ASA のロード バランシング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、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。

Ubuntu 8.04 i386

症状　Ubuntu バージョン 8.04 を使用すると、AnyConnect クライアントが ASA への接続確立に失敗する。VPN クライアント エージェント SSL エンジンでエラーが発生したことがエラー メッセージに示される。

考えられる原因　バージョン 7.04 と 8.04 とで、NSS ライブラリ エクステンションが変更されているため、AnyConnect クライアントは Network Security Service ライブラリを検出できません。

推奨処置　次のスクリプトを使用して NSS ライブラリのリンクを修正してください。

```
#!/bin/sh
if [ `id | sed -e `s/(.*//' ` != "uid=0" ]; then
    echo "Sorry, you need super user privileges to run this script.
    exit 1
fi
echo Creating Firefox NSS compatible symlinks...
ln -s /usr/lib/libnspr4.so.0d /usr/lib/libnspr4.so || exit 1
ln -s /usr/lib/libnss3.so.1d /usr/lib/libnss3.so || exit 1
ln -s /usr/lib/libplc4.so.0d /usr/lib/libplc4.so || exit 1
ln -s /usr/lib/libsmime3/so/1d /usr/lib/libsmime3.so || exit 1
echo "Success!"
```

また、AnyConnect で Ubuntu 64 ビットを使用可能にするための解説が Ubuntu フォーラムにないか確認することもできます。

Wave EMBASSY Trust Suite

症状　AnyConnect クライアント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る。

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

考えられる原因　mdmp ファイルを収集している場合は、クラッシュ mdmp ファイルをデコードすると、サードパーティ製 dll が存在することが示されます。

推奨処置　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。

Layered Service Provider（LSP）モジュールおよび NOD32 AV

症状　AnyConnect が接続の確立を試行するときに、認証および SSL セッションの構築は正常に行われるが、AnyConnect クライアントが vpndownloader でクラッシュする。

考えられる原因　LSP コンポーネントの imon.dll に非互換性問題があります。

推奨処置　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。

LSP の症状 2：競合

症状　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。

考えられる原因　impbw.dll などの Intel モバイル帯域幅の LSP モジュールによって、Intel コードで障害が発生した可能性があります。

推奨処置　LSP モジュールをアンインストールしてください。

LSP のデータ スループット低下症状 3：競合

症状　NOD32 V4.0 を使用すると、データ スループットが低下することがあります。

考えられる原因　この競合は、Windows 7 で Cisco AnyConnect と NOD32 アンチウイルス 4.0.468 x64 を使用したときに発生します。

推奨処置　[プロトコル フィルタリング（Protocol Filtering）] > [詳細設定（Advanced Setup）] の [SSL] を選択し、SSL プロトコル スキャンをイネーブルにします。次に、[Web アクセス保護（Web access protectio）] > [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。設定がイネーブルになったら、[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（SSL protocol scanning）] スキャンをディセーブルにします。

EVDO ワイヤレ スカードおよび Venturi ドライバ

症状　クライアントが接続解除され、イベント ログに次のようなメッセージが生成される。

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

考えられる原因　アプリケーション、システム、および AnyConnect 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。

推奨処置　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）] をディセーブルにします。

DSL ルータがネゴシエーションに失敗する

症状　DTLS トラフィックが正常にネゴシエーションされたが、DTLS トラフィックに障害が発生した。

考えられる原因　DSL ルータがリターン DTLS トラフィックをブロックしていました。エアー リンク上の設定により、安定した DTLS 接続が許可されません。

推奨処置　工場出荷時の設定で Linksys ルータに接続すると、安定した DTLS セッションが許可され、ping が中断されません。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。

チェックポイント（および Kaspersky などの他のサードパーティ製ソフトウェア）

症状　AnyConnect ログに、セキュア ゲートウェイへの接続を完全に確立できなかったことが示される。

考えられる原因　クライアント ログに、NETINTERFACE_ERROR_INTERFACE_NOT_AVAILABLE が複数発生したことが示されています。これらのエラーは、セキュア ゲートウェイへの SSL 接続の確立に使用する PC のネットワーク インターフェイス上でクライアントがオペレーティング システム情報を取得しようとしているときに発生します。

推奨処置　整合性エージェントをアンインストールしてから AnyConnect をインストールする場合は、TCP/IP をイネーブルにしてください。整合性エージェントのインストール時に SmartDefense をディセーブルにすると、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 AnyConnect 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、AnyConnect 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イネーブルにしてください。疑わしいドライバが AnyConnect アダプタ内でイネーブルにされている場合は、これらのドライバを [Cisco AnyConnect VPN Client Connection] ウィンドウでオフにしてディセーブルにしてください。

Virtual Machine Network Service ドライバでのパフォーマンス問題

症状　一部のクライアント PC で AnyConnect を使用すると、パフォーマンスの問題が発生した。

考えられる原因　仮想マシン ネットワーク ドライバは物理的なネットワーク カードまたは接続を仮想化します。Cisco AnyConnect VPN クライアント接続ネットワーク アダプタに他の仮想マシン ネットワーク サービスをバインドしたときに、パフォーマンス問題が発生しています。クライアント デバイスが何らかのマルウェアに感染し、SSL_write () の周囲で遅延が発生しました。

推奨処置　AnyConnect 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、AnyConnect が正常に動作します。

Kaspersky AntiVirus およびテレメトリ モジュール

症状　テレメトリ モジュールがインストールされている場合、AnyConnect は Kaspersky AntiVirus 8 スイート（avp.exe）のメイン実行可能ファイルを削除する場合があります。

考えられる原因　AnyConnect 3.0.5080 以降を備える 64 ビットでドイツ語の Windows 7 と Kaspersky AV 8 を使用すると、競合の原因となります。

推奨処置　テレメトリ モジュールを取り外します。