CHAPTER 11

トラブルシューティングおよびプログラミングのヒント

この章には、VPN クライアントのインストール時または実行時に発生する問題を解決する際に役立つ情報を記載しています。また、特殊なニーズに合わせてプログラムを記述する際に役立つ注記も記載しています。

この章の主な内容は、次のとおりです。

VPN クライアントのトラブルシューティング

ここでは、次の作業の実行方法を説明します。

VPN クライアント ログの収集

VPN クライアントのインストール ディレクトリ内の Logs フォルダには、VPN クライアント セッションのログ ファイルが格納されます。ログ ファイルはテキスト ファイルで、そのファイル名の形式は Log-yyyy-MM-dd-hh-mm-ss.txt です。ログ ファイルおよびロギングの情報については、『*VPN Client User Guide for Windows*』の第 7 章「Managing the VPN Client」または『*VPN Client User Guide for Mac OS X*』の第 7 章「Managing the VPN Client」を参照してください。

必要に応じて、これらのログ ファイルを取得し、解析用にカスタマー サポートに送信します。

重大度 1 のイベントに関する情報の取得

重大度 1 のイベントが発生した場合、VPN クライアントはこれらを faultlog.txt というテキスト ファイルに記録します。このファイルは VPN クライアントのインストール ディレクトリにあります。このイベント ロギングは、ログ ビューア アプリケーションが動作しているかどうかに関係なく実行されます。たとえば、サービスの初期化中に発生したエラーはログ ビューアに記録できません。これは、サービス自体がログ ビューアにアタッチされる前に、このエラーが発生したからです。そのため、faultlog.txt ファイルを開いて、このような重大度 1 のイベントを確認できます。このログ ファイルは、発生した現象を分析する際に役立つツールです。また、このログ ファイルを利用することで、カスタマー サポート担当者に問い合わせる場合に、報告する情報が明確になります。

カスタマー サポート用のシステム情報の収集

ご使用の PC 上で VPN クライアントの実行中に問題が発生した場合は、カスタマー サポート担当者が問題を解決する上で役立つシステム情報を収集して、電子メールで送信してください。カスタマー サポートにお問い合わせいただく *前に*、次の作業を実行することを推奨します。

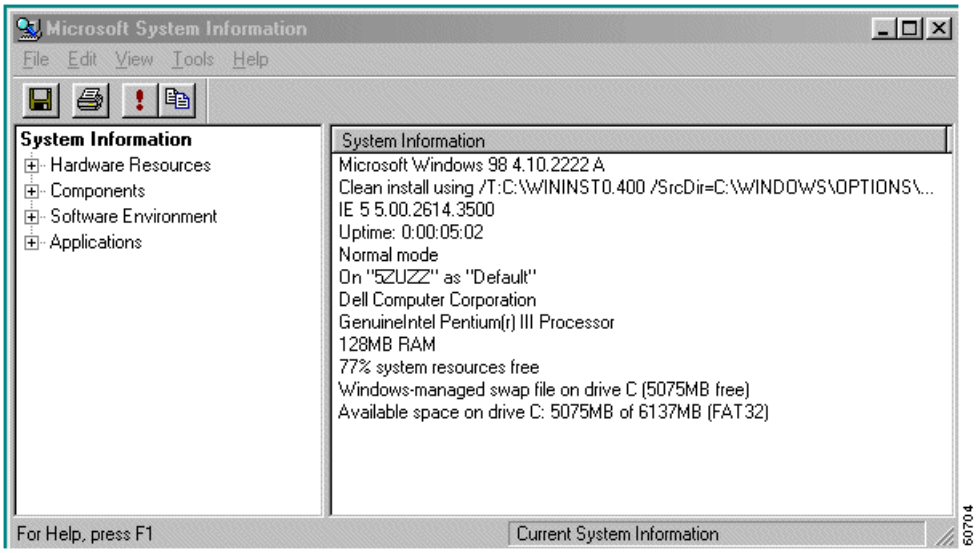
オペレーティング システムが Windows 98、98 SE、ME、2000、または XP の場合

（注） 現在 VPN クライアントは、Windows 95、Windows 98、および Windows ME を正式にサポートしていません。

[Start] メニューから、[Programs] > [Accessories] > [System Tools] > [System Information] を選択します。

図 11-1 のような [Microsoft System Information] 画面が表示されます。

図 11-1　Windows 98 の [System Information] 画面



カテゴリを選択すると、画面にそのカテゴリの詳細情報が表示されます。次に、**Export** コマンドを実行して、名前と保存先を選択できます。テキスト ファイルが作成されます。このファイルを電子メールに添付して、サポート センターに送信できます。

オペレーティング システムが Windows NT または Windows 2000 の場合

Windows NT または Windows 2000 オペレーティング システムでは、コマンドライン プロンプトから WINMSD というユーティリティを実行できます。WINMSD を使用すると、システム構成、インストールされているソフトウェアとドライバに関する情報が格納されたファイルを生成できます。

このユーティリティを使用するには、次の手順を実行します。

ステップ 1　[Start] メニューから、[Programs] > [Command Prompt] を選択します。

DOS プロンプト（c:¥ など）が表示されているウィンドウが開きます。

ステップ 2　DOS プロンプトで、次のコマンドを入力します。

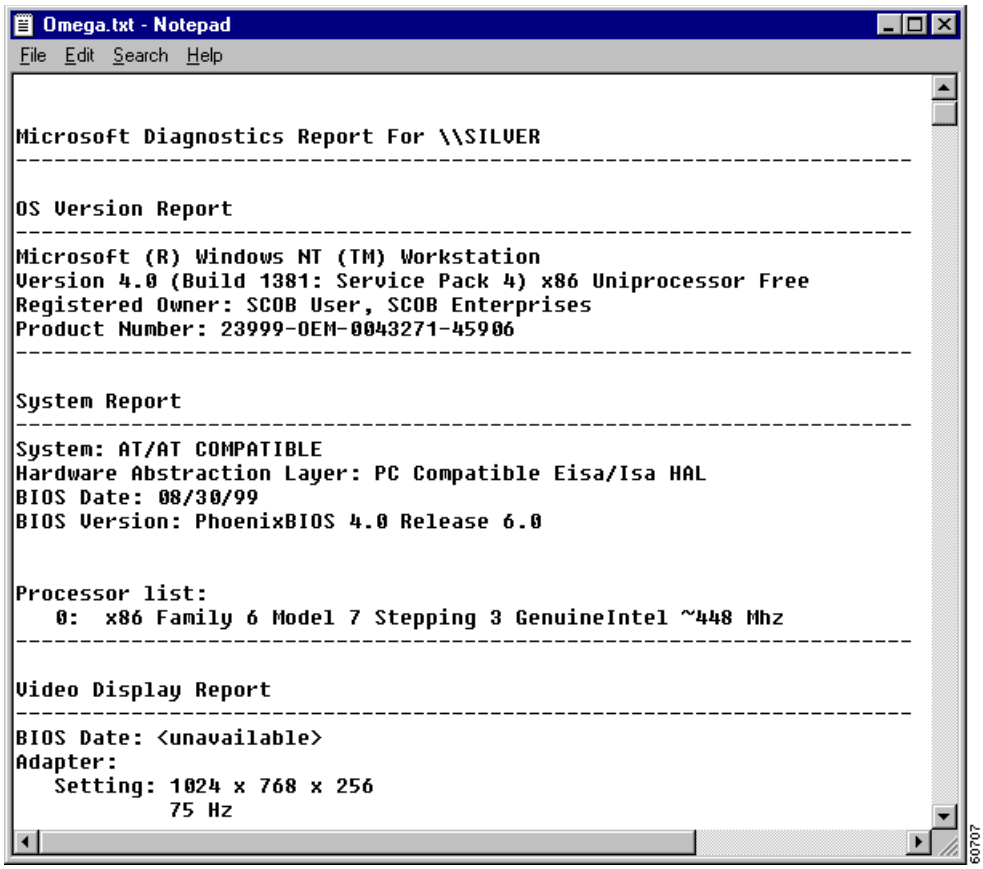
```
C:\>winmsd /a /f
```

ここで、**/a** は「すべて」、**/f** は「ファイルに書き込む」という意味です。

このコマンドを実行すると、コンピュータ名が付いたテキスト ファイル（.txt）が生成され、このコマンドを実行したディレクトリにそのファイルが保存されます。たとえば、コンピュータ名が SILVER で、c: ドライブから上記のようにコマンドを実行した場合、テキスト ファイルの名前は silver.txt です。

メモ帳などのテキスト エディタでファイルを開くと、Windows NT システムで生成された図 11-2 のような内容が表示されます。

図 11-2　システム テキスト ファイル



このファイルを電子メール メッセージに添付して、サポート センターに送信します。

オペレーティング システムが Mac OS X の場合

ステップ 1　コマンドラインから次のコマンドを実行します。

```
ifconfig -a
uname -a
kextstat
```

上記コマンドの出力をコピーして電子メール メッセージにペーストし、サポートに送信してください。

一般的な問題の解決

ここでは、一般的な問題とその対処方法について説明します。

Windows 98 のシャットダウン

VPN クライアント ソフトウェアのインストール時に、Windows 98 システムがシャットダウンするという問題が発生することがあります。このような場合は、次の手順で、高速シャットダウン機能を無効にする必要があります。

ステップ 1　[Microsoft System Information] 画面（図 11-1）で、[Tools] > [System Configuration] を選択します。

[Properties] ページが表示されます。

ステップ 2　[General] ページから、[Advanced] ボタンを選択します。

ステップ 3　[Disable Fast Shutdown] オプションを選択します。

Windows 95 起動時のダイアルアップ ネットワークの自動起動

Windows 95 では、Internet Explorer の一部のバージョンで起動オプションが自動的に制御されています。その結果、システムを起動するたびに、ダイアルアップ ネットワークが起動します。このような場合（たとえば Internet Explorer 3.0）、[View] > [Options] > [Connections] の順に選択し、[Connect to the Internet as needed] オプションをオフにします。

MTU サイズの変更

[Set MTU] オプションは、主に接続性の問題をトラブルシューティングする際に使用します。

（注）　VPN クライアントでは、ユーザの環境に合わせて MTU サイズが自動的に調整されるので、このアプリケーションを実行しないことを推奨します。

最大転送ユニット（MTU）パラメータは、クライアント アプリケーションがネットワークを介して送信できる最大パケット サイズをバイト単位で算出します。MTU サイズが大きすぎると、パケットが宛先に到達しないことがあります。MTU のサイズを調節すると、ネットワーク アダプタを使用するすべてのアプリケーションに影響を与えます。したがって、使用する MTU 設定値により、ネットワーク上の PC のパフォーマンスに影響を与える可能性があります。

MTU のサイズを設定すると、IPsec カプセル化によってパケット サイズが大きくなるため、接続の宛先への IPsec パケットと IPsec through NAT モード パケットのフラグメンテーションに影響を与えます。サイズが大きい場合（たとえば、1300 バイト以上）、フラグメンテーションが増大することがあります。通常、1300 バイト以下に設定すると、フラグメンテーションを防止できます。パケットのフラグメンテーションおよび宛先での再アセンブルによって、トンネリングのパフォーマンスが低下します。また、多くのファイアウォールでは、フラグメント化されたパケットを通過させません。

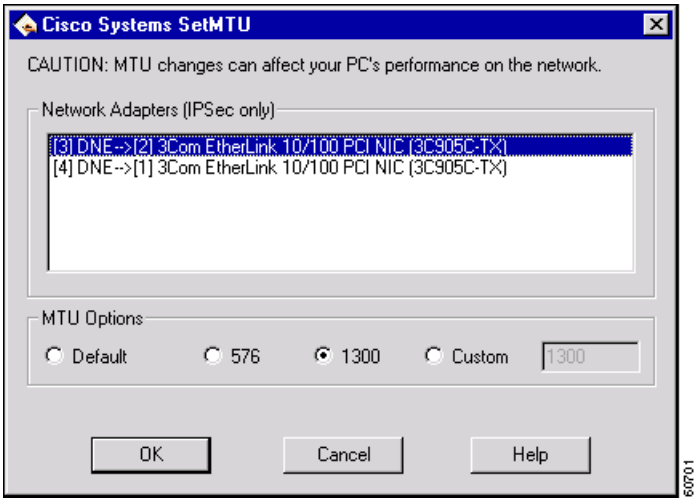
MTU サイズの変更：Windows

Windows において、MTU のサイズを変更するには、次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Cisco System VPN Client] > [Set MTU] の順に選択します。

[Set MTU] ウィンドウが表示されます。

図 11-3　Windows NT での MTU サイズの設定



ステップ 2　ネットワーク アダプタのリストから、ネットワーク アダプタをクリックします。

ステップ 3　[MTU Options] にある次の選択項目のいずれかをクリックします。

デフォルト	このアダプタ タイプの工場出荷時の設定値。
576（バイト単位）	ダイアルアップ アダプタの標準サイズ。
1300（バイト単位）	IPsec 自体と IPsec through NAT の両方にこの値を選択することを推奨します。この値を使用すると、通常の状況においてクライアントでパケットがフラグメント化されなくなります。
Custom	ボックスに値を入力します。MTU サイズの最小値は 68 バイトです。

ステップ 4　[OK] をクリックします。

変更を有効にするには、システムを再起動する必要があります。

MTU サイズの変更：Linux、Solaris、および Mac OS X

MTU サイズを変更するには、次の手順を実行します。

ステップ 1　ターミナル ウィンドウを開きます（Mac OS X のみ）。

ステップ 2　次のコマンドを入力します。

```
sudo ifconfig en0 mtu 1200
```

（en0 を該当するインターフェイスに置き換え、1200 を目的の mtu で置き換えます）。

ステップ 3　変更がすぐに反映されます。

コマンドラインからの MTU の設定

コマンドライン プロンプトで SetMTU コマンドを使用して、MTU サイズを設定できます。SetMTU コマンドの構文は、次のとおりです。

setmtu /*switch value*

ここで、switch は次のいずれかです。

スイッチ	説明
/s *value*	すべてのアダプタの MTU を *value* に設定します。こうすることで、IP レイヤで MTU が設定されます。この操作ではリブートが必要です。
/r	IP レイヤでのすべてのアダプタの MTU をオペレーティング システムのデフォルト値にリセットします。この操作ではリブートが必要です。
/va *value*	仮想アダプタの MTU を *value* に設定します。こうすることで、MAC レイヤでの MTU が設定されます。この操作では、リブートは不要です。
/vaReset	Mac レイヤでの仮想アダプタの MTU をデフォルト値（1500）にリセットします。この操作では、リブートは不要です。
/?	SetMTU スイッチに関するヘルプを表示します。

新しい設定は、次回トンネルが確立されたときも引き続き有効です。

理由を示して削除

接続が解除されるとき、VPN クライアントにより、理由コードまたは理由を示すテキストが表示されます。VPN クライアントは、クライアントによって開始された接続解除、セキュア ゲートウェイによって開始された接続解除、および IPsec の削除について、理由を表示して削除する機能をサポートしています。

- GUI VPN クライアントを使用している場合は、接続解除の理由を示すポップアップ メッセージが表示され、このメッセージは通知ログに追加され、IPsec ログ（Log Viewer ウィンドウ）に記録されます。
- コマンドラインのクライアントを使用している場合、メッセージは端末に表示され、IPsec ログに記録されます。
- IPsec の削除では、接続は切断されず、イベント メッセージが IPsec ログ ファイルに表示されますが、メッセージが端末にポップアップしたり表示されたりしません。

（注）　理由を示して削除する機能をサポートするには、接続先のソフトウェア バージョン 4.0 以降のセキュア ゲートウェイが実行されている必要があります。

表 11-1 に、理由コードと対応するメッセージを示します。

表 11-1　理由コードを示して削除

理由コード	翻訳済みメッセージ
IKE_DELETE_SERVER_SHUTDOWN	ピアがシャットダウンしました。
IKE_DELETE_SERVER_REBOOT	ピアがリブートしました。
IKE_DELETE_MAX_CONNECT_TIME	設定されている最大接続時間が超えました。
IKE_DELETE_BY_USER_COMMAND	管理者によって手動で接続解除されました。
IKE_DELETE_BY_ERROR	クライアントとの接続が失われました。
IKE_DELETE_NO_ERROR	不明なエラー。
IKE_DELETE_IDLE_TIMEOUT	セッションの最大アイドル時間を超えました。
IKE_DELETE_P2_PROPOSAL_MISMATCH	ポリシーのネゴシエーションが失敗しました。
IKE_DELETE_FIREWALL_MISMATCH	ファイアウォールのポリシーが一致しません。
IKE_DELETE_CERT_EXPIRED	この接続エントリで使用された証明書は失効しています。
IKE_DELETE_BY_EXPIRED_LIFETIME	設定された最大ライフタイムを超えました。

クライアントによって開始された接続解除に関するすべてのテキスト メッセージは、「Secure VPN Connection terminated terminated locally by the client」で始まります。

セキュア ゲートウェイによって開始された接続解除に関するすべてのテキストメッセージは、「Secure VPN Connection terminated by Peer X.X.X.X」で始まります。この X.X.X.X はセキュア ゲートウェイの IP アドレスです。

この後に、対応する理由コードまたは理由テキストが続きます。

VPN Concentrator での理由を示して削除の設定

4.0 以降の VPN Concentrator から接続解除に関する情報を受信するには、この機能を次のように設定する必要があります。

ステップ 1　[Configuration | Tunneling | IPsec | Alerts] の順に選択します。

ステップ 2　[Alert when disconnecting] をオンにします。

ステップ 3　[Apply] をクリックします。

ステップ 4　設定を保存します。

Start Before Logon および GINA : Windows のみ

VPN クライアントは、Windows NT プラットフォーム（Windows NT 4.0、Windows 2000、および Windows XP）にログインする前にロードできます。この機能により、リモート ユーザは、正常にドメインにログインできるプライベート ネットワークへの VPN 接続を確立できます。Start Before Logon（SBL）が Windows NT プラットフォーム上でイネーブルのときに、VPN クライアントによって、標準の Microsoft ログオン ダイアログボックス（PC を起動したときに、Ctrl+Alt+Del を押した後に表示されるものと同じ、GINA と呼ばれる画面）の置き換えが試行されます。Microsoft GINA の名前は msgina.dll で、このパラメータは次の場所のレジストリにあります。

```
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
GinaDLL = msgina.dll
```

VPN クライアントは、msgina.dll を VPN クライアントの GINA（csgina.dll）で置き換え、引き続き MS GINA を表示して使用できるように、msgina.dll を参照します。PC を起動し、Ctrl+Alt+Del を押すと、VPN Client Dialer アプリケーションおよび MS ログオン ダイアログボックスが起動します。VPN クライアントは、必要な Windows サービスが実行されているかどうかを検出し、実行されていなければ、待機するよう求めるメッセージを表示します。

VPN クライアントのレジストリのパラメータおよび値は、次のとおりです。

```
HKLM\Software\Cisco Systems\VPN Client\
GinaInstalled = 1
PreviousGinaPath = msgina.dll
```

（注）　Start Before Logon を初めてイネーブルにしたとき、csgina をロードできるようにシステムをリブートする必要があります。

フォールバック モード

サードパーティ製プログラムによって MS GINA が置き換えられることがあります。この場合、VPN クライアントがサードパーティ製プログラムと共に作動することもあれば、動作しないこともあります。VPN クライアントは、共に動作しない、互換性のない GINA のリストを保持し、使用中の GINA ファイルを置き換えません。これは、*フォールバック* モードと呼ばれます。互換性がない GINA のリストは vpnclient.ini ファイル内に存在し、VPN クライアントはインストール中にだけそのリストを参照します。次に、エントリの例を示します。

```
IncompatibleGinas=PALgina.dll,nwgina.dll,logonrem.dll,ngina.dll
```

フォールバック モードでは、Start Before Logon が使用されているときの VPN クライアントの動作が異なります。VPN Dialer は、Ctrl+Alt+Del を押したときにロードされるのではなく、VPN サービスが起動した直後にロードされます。フォールバック モードで動作しているときに、VPN クライアントは、必要な Windows サービスが起動しているかどうかを確認しません。その結果、VPN 接続の開始が早すぎると、接続が失敗することがあります。フォールバック モードでは、VPN 接続が成功した後に、Ctrl+Alt+Del を押して、Microsoft ログオン ダイアログボックスを表示します。このモードでは、次の VPN クライアントのレジストリ パラメータおよび値が表示されます。

```
HKLM\Software\Cisco Systems\VPN Client\
GinaInstalled = 0
PreviousGinaPath = msgina.dll
```

互換性のない GINA

VPN クライアントのリリース後、GINA に新しい問題が検出された場合は、vpnclient.ini ファイル内の互換性のない GINA リストにその GINA を追加できます。このリストに GINA を追加すると、VPN クライアントをインストールする際に、レジストリ内の IncompatibleGinas リストにその GINA が追加され、VPN クライアントがフォールバック モードになります。したがって、競合が発生する可能性を回避できます（「Start Before Logon および GINA：Windows のみ」（P.11-8）を参照）。

ファイアウォール ダイアログのディセーブル化

ファイアウォールが実行されていないときに、SBL 期間中にユーザに表示されるファイアウォール ダイアログをディセーブルにできます。この機能は、レジストリ キー DisableSBLFirewallCheck によって制御されます。

このレジストリの場所は、次のとおりです。

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\VPN Client\Secure

キーは、DisableSBLFirewallCheck で、次の値と共に指定します。

- 0 (FALSE)：ファイアウォールのチェックをディセーブルにしません。ファイアウォール ダイアログがユーザに表示されます。
- 1- (TRUE)：ファイアウォールのチェックをディセーブルにします。[Firewall] ダイアログがユーザに表示 *されません*。

プログラミングのヒント

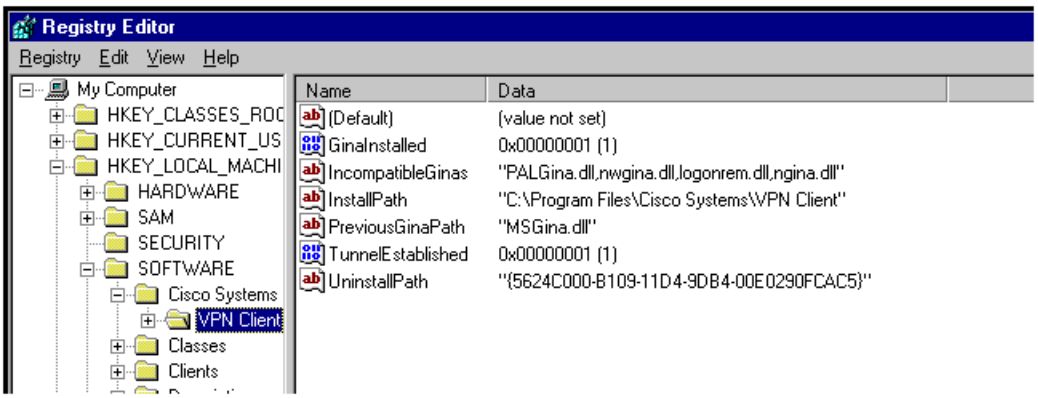
ここでは、ルーチン タスクを実行するプログラムを記述する際にプログラマに役立つ情報を記載します。

接続のテスト

プログラムの一部として、プログラムの目的であるタスクを実行する前に、接続がアクティブであるかどうかを確認するために、接続のテストを実行できます。接続をテストするために、HKEY_LOCAL_MACHINE レジストリ内の TunnelEstablished エントリをポーリングすることができます。

このエントリを表示するには、レジストリ エディタを表示し、[SOFTWARE] > [Cisco Systems] > [VPN Client] の順に選択します。（図 11-4 を参照）。エントリのリストに TunnelEstablished が表示されます。このエントリには、2 つの値（1 または 0）のみを指定できます。接続が確立されている場合、値は 1 で、確立されていない場合、値は 0 です。

図 11-4　　シスコ VPN クライアントのレジストリ エントリ



vpngui コマンド用のコマンドライン スイッチ：Windows のみ

vpngui コマンドを実行すると、VPN Client GUI アプリケーションが起動し、コマンドラインからの接続が開始されます。このコマンドでパラメータを指定する場合は、スイッチを使用できます。スイッチの前に、スラッシュ（/）またはハイフン（-）を付ける必要があります。Windows 以外のプラットフォームでは、プレフィックスにハイフンのみを使用できます。

表 11-2 に、vpngui コマンドに指定できるスイッチと、各スイッチで実行されるタスクを示します。接続エントリ名にスペースやその他の特殊文字が含まれている場合は、接続エントリ名を引用符で囲む必要があります。次の例で、towork は接続エントリの名前です。

表 11-2　コマンドライン スイッチ

スイッチ	パラメータ	説明
/c	Auto-connect	指定された接続エントリに対して VPN クライアント アプリケーションを開始し、認証ダイアログを表示します。接続エントリが指定されていない場合、VPN クライアントはデフォルトの接続エントリを使用します。c スイッチと sc スイッチは相互に排他的です。 例：**vpngui /c towork**
/eraseuserpwd	Erase User Password	クライアント PC に保存されたユーザ パスワードを消去し、それに伴って VPN クライアントは強制的にパスワードを要求します。 例：**vpngui /c /eraseuserpwd towork** **（注）** 接続エントリに保存済みのパスワードが設定されていると、バッチ ファイルを使用して接続したときに、パスワードの入力要求が表示されません。接続時に、コンソールからパスワードの入力を要求するように戻すには、eraseuserpwd オプションを使用してください。このスイッチを pwd スイッチと組み合わせることはできません。このスイッチと組み合わせることができるのは、/c または /sc スイッチのみです。
/user	Username	認証用のユーザ名を指定します。認証ダイアログでユーザ名の入力を求めるプロンプトが表示されなくなります。pwd スイッチと共に使用すると、認証ダイアログが完全に表示されなくなります。.pcf ファイル内のユーザ名を更新します。このパラメータと共に使用できるのは、/c または /sc スイッチのみです。 例：**vpngui /c /user robron /pwd siltango towork** **（注）** 入力した名前が無効な場合、VPN クライアントは以降の認証要求で認証ダイアログを表示します。

表 11-2　コマンドライン スイッチ （続き）

スイッチ	パラメータ	説明
/pwd	Password	認証用のパスワードを指定します。認証ダイアログでパスワードの入力を求めるプロンプトが表示されなくなります。pwd スイッチと共に使用すると、認証ダイアログが完全に表示されなくなります。認証中に .pcf ファイル内のパスワードを更新し、.pcf ファイルからパスワードを消去します。このスイッチと共に使用できるのは、/c または /sc スイッチのみです。 例：**vpngui /c /user robron /pwd siltango towork** **（注）** 入力したパスワードが無効な場合、VPN クライアントは以降の認証要求で認証ダイアログを表示します。パスワードを暗号化して接続した後、VPN クライアントは .pcf ファイルのパスワードをクリアします。コマンド ラインでこのオプションを使用すると、セキュリティが低下するため、推奨しません。
/sd	Silent disconnect	「Your IPsec connection has been terminated」のような接続終了メッセージが表示されなくなります。このパラメータは、自動接続プロセスを改善するために使用できます。このスイッチと共に使用できるのは、/c または /sc スイッチのみです。 例：**vpngui /sd towork**

IKE プロポーザル

表 11-3 に、VPN クライアントがサポートする IKE プロポーザルを記載します。

表 11-3　VPN クライアントの有効な IKE プロポーザル

プロポーザル名	認証モード	認証アルゴリズム	暗号化アルゴリズム	Diffie-Hellman グループ
CiscoVPNClient-3DES-MD5	事前共有キー（XAUTH）	MD5/HMAC-128	3DES-168	グループ 2（1024 ビット）
CiscoVPNClient-3DES-SHA	事前共有キー（XAUTH）	SHA/HMAC-160	3DES-168	グループ 2（1024 ビット）
CiscoVPNClient-DES-MD5	事前共有キー（XAUTH）	MD5/HMAC-128	DES-56	グループ 2（1024 ビット）
CiscoVPNClient-AES128-MD5	事前共有キー（XAUTH）	MD5/HMAC-128	AES-128	グループ 2（1024 ビット）
CiscoVPNClient-AES128-SHA	事前共有キー（XAUTH）	SHA/HMAC-160	AES-128	グループ 2（1024 ビット）
CiscoVPNClient-AES256-MD5	事前共有キー（XAUTH）	MD5/HMAC-128	AES-256	グループ 2（1024 ビット）
CiscoVPNClient-AES256-SHA	事前共有キー（XAUTH）	SHA/HMAC-160	AES-256	グループ 2（1024 ビット）
IKE-3DES-MD5	事前共有キー	MD5/HMAC-128	3DES-168	グループ 2（1024 ビット）
IKE-3DES-SHA	事前共有キー	SHA/HMAC-160	3DES-168	グループ 2（1024 ビット）
IKE-DES-MD5	事前共有キー	MD5/HMAC-128	DES-56	グループ 2（1024 ビット）
IKE-AES128-MD5	事前共有キー	MD5/HMAC-128	AES-128	グループ 2（1024 ビット）
IKE-AES128-SHA	事前共有キー	SHA/HMAC-160	AES-128	グループ 2（1024 ビット）
IKE-AES256-MD5	事前共有キー	MD5/HMAC-128	AES-256	グループ 2（1024 ビット）
IKE-AES256-SHA	事前共有キー	SHA/HMAC-160	AES-256	グループ 2（1024 ビット）
CiscoVPNClient-3DES-MD5-RSA	RSA デジタル証明書（XAUTH）	MD5/HMAC-128	3DES-168	グループ 2（1024 ビット）
CiscoVPNClient-3DES-SHA-RSA	RSA デジタル証明書（XAUTH）	SHA/HMAC-160	3DES-168	グループ 2（1024 ビット）
CiscoVPNClient-DES-MD5-RSA-DH1	RSA デジタル証明書（XAUTH）	MD5/HMAC-128	DES-56	グループ 1（768 ビット）
CiscoVPNClient-AES128-MD5-RSA	RSA デジタル証明書（XAUTH）	MD5/HMAC-128	AES-128	グループ 2（1024 ビット）

プロポーザル名	認証モード	認証アルゴリズム	暗号化アルゴリズム	Diffie-Hellman グループ
CiscoVPNClient-AES128-SHA-RSA	RSA デジタル証明書（XAUTH）	SHA/HMAC-160	AES-128	グループ 2（1024 ビット）
CiscoVPNClient-AES256-MD5-RSA	RSA デジタル証明書（XAUTH）	MD5/HMAC-128	AES-256	グループ 2（1024 ビット）
CiscoVPNClient-AES256-SHA-RSA	RSA デジタル証明書（XAUTH）	SHA/HMAC-160	AES-256	グループ 2（1024 ビット）
CiscoVPNClient-3DES-MD5-RSA-DH5	RSA デジタル証明書（XAUTH）	MD5/HMAC-128	3DES-168	グループ 5（1536 ビット）
CiscoVPNClient-3DES-SHA-RSA-DH5	RSA デジタル証明書（XAUTH）	SHA/HMAC-160	3DES-168	グループ 5（1536 ビット）
CiscoVPNClient-AES128-MD5-RSA-DH5	RSA デジタル証明書（XAUTH）	MD5/HMAC-128	AES-128	グループ 5（1536 ビット）
CiscoVPNClient-AES128-SHA-RSA-DH5	RSA デジタル証明書（XAUTH）	SHA/HMAC-160	AES-128	グループ 5（1536 ビット）
CiscoVPNClient-AES256-MD5-RSA-DH5	RSA デジタル証明書（XAUTH）	MD5/HMAC-128	AES-256	グループ 5（1536 ビット）
CiscoVPNClient-AES256-SHA-RSA-DH5	RSA デジタル証明書（XAUTH）	SHA/HMAC-160	AES-256	グループ 5（1536 ビット）
CiscoVPNClient-3DES-MD5-RSA	RSA デジタル証明書（XAUTH）	MD5/HMAC-128	3DES-168	グループ 2（1024 ビット）
HYBRID-3DES-SHA-RSA	RSA デジタル証明書（HYBRID）	SHA/HMAC-160	3DES-168	グループ 2（1024 ビット）
HYBRID-DES-MD5-RSA-DH1	RSA デジタル証明書（HYBRID）	MD5/HMAC-128	DES-56	グループ 1（768 ビット）
HYBRID-AES128-MD5-RSA	RSA デジタル証明書（HYBRID）	MD5/HMAC-128	AES-128	グループ 2（1024 ビット）
HYBRID-AES128-SHA-RSA	RSA デジタル証明書（HYBRID）	SHA/HMAC-160	AES-128	グループ 2（1024 ビット）
HYBRID-AES256-MD5-RSA	RSA デジタル証明書（HYBRID）	MD5/HMAC-128	AES-256	グループ 2（1024 ビット）
HYBRID-AES256-SHA-RSA	RSA デジタル証明書（HYBRID）	SHA/HMAC-160	AES-256	グループ 2（1024 ビット）
HYBRID-3DES-MD5-RSA-DH5	RSA デジタル証明書（HYBRID）	MD5/HMAC-128	3DES-168	グループ 5（1536 ビット）
HYBRID-3DES-SHA-RSA-DH5	RSA デジタル証明書（HYBRID）	SHA/HMAC-160	3DES-168	グループ 5（1536 ビット）
HYBRID-AES128-MD5-RSA-DH5	RSA デジタル証明書（HYBRID）	MD5/HMAC-128	AES-128	グループ 5（1536 ビット）
HYBRID-AES128-SHA-RSA-DH5	RSA デジタル証明書（HYBRID）	SHA/HMAC-160	AES-128	グループ 5（1536 ビット）
HYBRID-AES256-MD5-RSA-DH5	RSA デジタル証明書（HYBRID）	MD5/HMAC-128	AES-256	グループ 5（1536 ビット）

プロポーザル名	認証モード	認証アルゴリズム	暗号化アルゴリズム	Diffie-Hellman グループ
HYBRID-AES256-SHA-RSA-DH5	RSA デジタル証明書（HYBRID）	SHA/HMAC-160	AES-256	グループ 5（1536 ビット）
IKE-3DES-MD5-RSA	RSA デジタル証明書	MD5/HMAC-128	3DES-168	グループ 2（1024 ビット）
IKE-3DES-SHA-RSA	RSA デジタル証明書	SHA/HMAC-160	3DES-168	グループ 2（1024 ビット）
IKE-AES128-MD5-RSA	RSA デジタル証明書	MD5/HMAC-128	AES-128	グループ 2（1024 ビット）
IKE-AES128-SHA-RSA	RSA デジタル証明書	SHA/HMAC-160	AES-128	グループ 2（1024 ビット）
IKE-AES256-MD5-RSA	RSA デジタル証明書	MD5/HMAC-128	AES-256	グループ 2（1024 ビット）
IKE-AES256-SHA-RSA	RSA デジタル証明書	SHA/HMAC-160	AES-256	グループ 2（1024 ビット）
IKE-DES-MD5-RSA-DH1	RSA デジタル証明書	MD5/HMAC-128	DES-56	グループ 1（768 ビット）
IKE-3DES-MD5-RSA-DH5	RSA デジタル証明書	MD5/HMAC-128	3DES-168	グループ 5（1536 ビット）
IKE-3DES-SHA-RSA-DH5	RSA デジタル証明書	SHA/HMAC-160	3DES-168	グループ 5（1536 ビット）
IKE-AES128-MD5-RSA-DH5	RSA デジタル証明書	MD5/HMAC-128	AES-128	グループ 5（1536 ビット）
IKE-AES128-SHA-RSA-DH5	RSA デジタル証明書	SHA/HMAC-160	AES-128	グループ 5（1536 ビット）
IKE-AES256-MD5-RSA-DH5	RSA デジタル証明書	MD5/HMAC-128	AES-256	グループ 5（1536 ビット）
IKE-AES256-SHA-RSA-DH5	RSA デジタル証明書	SHA/HMAC-160	AES-256	グループ 5（1536 ビット）

表 11-4 に、VPN クライアントから送信される フェーズ 2 プロポーザルを示します。

表 11-4　フェーズ 2 プロポーザル

AES256	MD5	IPCOMPRESSION
AES256	SHA	IPCOMPRESSION
AES128	MD5	IPCOMPRESSION
AES128	SHA	IPCOMPRESSION
AES256	MD5	
AES256	SHA	
AES128	MD5	
AES128	SHA	
3DES	MD5	IPCOMPRESSION
3DES	SHA	IPCOMPRESSION
3DES	MD5	
3DES	SHA	
DES	MD5	IPCOMPRESSION
DES	MD5	
NULL	MD5	
NULL	SHA	

VPN クライアント アプリケーション プログラム インターフェイス

VPN クライアント ソフトウェアには、VPN クライアントのタスクを実行するために使用できる API が組み込まれています。これにより、標準的なコマンドラインまたは、シスコが提供するグラフィカル インターフェイスを使用する必要がなくなります。API は共用ライブラリを構成し、この共用ライブラリにより、プログラマは、以下を実行するアプリケーションにリンクできます。

- VPN トンネルの接続および接続解除
- ユーザの認証
- トンネルが確立および終了したときの通知の受信
- トンネルの統計情報（バイト数やパケット数など）の取得

API はプログラマ ユーザ ガイド『*VPN Client: API Overview*』に付属しています。このガイドには、コード ベースに精通していないプログラマが API を使用する際に役立つ情報が記載されています。このプログラマ ガイドでは、関数とデータ型、特定のタスクの実行方法の概要、およびサンプルとして使いやすいプログラム例について説明しています。