VPN Client に関する FAQ

内容

概要

このドキュメントでは Cisco VPN Client に関する FAQ について説明します。

注：さまざまなVPNクライアントの命名規則を次に示します。

- Cisco Secure VPN Client バージョン 1.0 ~ 1.1a のみ
- Cisco VPN 3000 Client バージョン 2.x のみ
- Cisco VPN Client 3.x 以降のみ

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

VPN Client ソフトウェアのダウンロード

Q. Cisco VPN Clientソフトウェアはどこでダウンロードできますか。

A. Cisco VPN Clientソフトウェアにアクセスするには、ログインしていて、有効なサービス契約が必要です。Cisco VPN Client ソフトウェアは Cisco の [Download Software] (登録ユーザ専用) ページからダウンロードできます。**Cisco.com プロファイルに関連する有効なサービス契約が結ばれていない場合はログインすることができず、VPN Client ソフトウェアをダウンロードできません。**

有効なサービス契約を取得するには、次のいずれかを実行してください。

- 直接購入契約書をお持ちの場合は、Cisco の営業担当にご連絡ください。
- サービス契約をご購入になる場合は、Cisco のパートナーまたは販売代理店にご連絡ください。
- Cisco.com プロファイルを更新してサービス契約への関連付けをリクエストするには、

Profile Manager (登録ユーザ専用) をご利用ください。

Q. Cisco VPN Clientのダウンロードエリアが空のように表示されます。これは、なぜですか。

A.ソフトウェアセンターのVPNクライアント領域(登録ユーザ専用)にアクセスする場合は、ページの中央で必ず目的のオペレーティングシステムのダウンロードエリアを選択してくださいい。

Q. Cisco VPN Clientのインストール中にステートフルファイアウォール機能を無効にするにはどうすればよいのですか。

A. 5.0 より前の VPN Client バージョンの場合：

『VPN Client Rel 4.7 リリース ノート』の「ドキュメントの変更」セクションにある次の 2 つのトピック「MSI を使用した、ステートフル ファイアウォールを使用しない Windows VPN Client のインストール」および「InstallShield を使用した、ステートフル ファイアウォールを使用しない Windows VPN Client のインストール」を参照してください。

5.0 以降の VPN Client バージョンの場合：

Cisco VPN Client リリース 5.0.3.0560 から、ファイアウォール ファイルのギルドのインストールを回避するために、MSI インストール フラグが追加されました。

```
msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1
```

これについての詳細は、「ステートフル ファイアウォールが不要の場合、ファイアウォール ファイルのインストールをバイパスする」セクションを参照してください。

Q. Cisco VPN Clientをアンインストールまたはアップグレードするにはどうすればよいのですか。

A. Windows 2000およびWindows XPでCisco VPN Clientバージョン3.5以降を手動でアンインストール(InstallShield)した後、アップグレードする方法については、『MSIインストーラでインストールされたVPN Clientバージョンの削除』を参照してください。

Windows 2000 および Windows XP ソフトウェア用 Cisco VPN Client は、通知を表示できる VPN 3000 コンセントレータや他の VPN サーバからトンネルを経由して、アップデートおよび新しいバージョンを自動的かつ安全にダウンロードできます。このための最小必要条件は、自動アップデート機能を使用するために、リモート ユーザの PC に Windows 4.6 以降に対応する VPN Client がインストールされている必要があることです。

自動アップデートと呼ばれるこの機能を使用すれば、ユーザはソフトウェアの古いバージョンをアンインストールしてリブートし、新しいバージョンをインストールして再度リブートする必要はありません。代わりに、管理者が Web サーバ上でアップデートとプロファイルを利用可能にし、リモート ユーザが VPN Client を起動したときに、ソフトウェアによってダウンロードが可能であることが検出され、ダウンロードが自動的に行われます。詳細については、「自動アップデートの管理」および「自動アップデートが動作する仕組み」を参照してください。

ASDM を使用して Cisco ASA シリーズ 5500 適応型セキュリティ アプライアンスのクライアント アップデートを設定する方法の詳細は、「ASDM を使用したクライアント ソフトウェア アップデートの設定」を参照してください。

Q. Vista用のVPNクライアントをカスタマイズしたいのですが、新しいバージョンの Vista 用 VPN Client には、oem.mst のようなファイルがありません。VPN Client の新しいバージョン (5.x) をカスタマイズするにはどうすればよいのですか。あるいは、このファイルはどこで入手できるのですか。

A. MSTファイルはVPN Clientに提供されなくなりましたが、Download Software (登録ユーザ専用) ページからダウンロードできます。

Filename :英語版の Windows にインストールする場合の Readme および MST。

オペレーティング システム

Q. CiscoではWindows Vista用のVPNクライアントを提供していますか。

A.新しいリリースのCisco VPN Client 5.0.07では、x86 (32ビット) とx64の両方でWindows Vistaがサポートされています。詳細については、5.0.07.0240リリースノートを参照してくださ い。

注：Cisco VPN ClientはWindows Vistaクリーンインストールでのみサポートされます。つまり、Windowsオペレーティングシステムから Windows Vistaへのアップグレードは、VPNクライアントソフトウェアではサポートされません。Windows Vista を新規でインストールしてから、Vista VPN Client ソフトウェアのインストールを行う必要があります。

注： Cisco.com プロファイルに関連する有効なサービス契約が結ばれていない場合はログインすることができず、VPN Client ソフトウェアをダウンロードできません。詳細は、「VPN Client ソフトウェアのダウンロード」を参照してください。

ヒント：Cisco AnyConnect VPN Clientは、Vista 32および64ビットを含むWindowsオペレーティングシステムで使用できるようになりました。AnyConnect クライアントでは、SSL および DTLS がサポートされています。現時点では、IPSec はサポートされていません。また、AnyConnect は、バージョン 8.0(2) 以降が稼働する Cisco 適応型セキュリティ アプライアンスとともに使用する場合にのみ使用できます。AnyConnect クライアントは、バージョン 12.4(15)T が稼働している IOS アプライアンスとともに、Web 起動モードで使用することもできます。VPN 3000 はサポートされていません。

Cisco AnyConnect VPN Client と ASA 8.0 は、Software Center (登録ユーザ専用) から入手できます。 AnyConnect Client の詳細は、『Cisco AnyConnect VPN Client リリース ノート』を参照してください。ASA 8.0 の詳細は、『Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのリリース ノート』を参照してください。

注： お客様の Cisco.com プロファイルに有効なサービス契約が関連付けられていない場合は、ログイン、および AnyConnect VPN Client または ASA ソフトウェアのダウンロードを行うことができません。 詳細は、「VPN Client ソフトウェアのダウンロード」を参照してください。

Q. Microsoft Windows PCからPPTP接続をセットアップするにはどうすればよいのですか。

A.セットアップは、実行しているMicrosoft Windowsのバージョンによって異なります。詳細は、Microsoft にお問い合せください。次に、Windows の一般的なバージョン用のセットアップ手順を示します。

Windows 95

1. Msdun13.exe をインストールします。
2. [Programs] > [Accessories] > [Dial Up Networking] の順に選択します。
3. 「PPTP」という名前で新しい接続を作成します。
4. 接続用のデバイスとして [VPN Adapter] **を選択します。**
5. スイッチのパブリック インターフェイスの IP アドレスを入力し、[Finish] をクリックします。
6. 先ほど作成した接続に戻り、右クリックして、[Properties] を選択します。
7. Allowed Network Protocols の下で、少なくとも netbeui のチェックをはずします。
8. [Advanced Options] を次のように設定します。 スイッチとクライアントに認証方法を自動ネゴシエートさせる場合は、デフォルト設定のままにします。チャレンジ ハンドシェーク認証プロトコル（CHAP）認証を適用する場合は、[Require Encrypted Password] **をイネーブルにします。**MS-CHAP 認証を要求する場合は、[Require Encrypted Password] **と [Require Data Encryption] をイネーブルにします。**

Windows 98

1. PPTP 機能をインストールするには、次の手順を実行します。 [Start] > [Settings] > [Control Panel] > [Add New Hardware] の順に選択し、[Next] をクリックします。[Select from List] をクリックし、[Network Adapter] を選択して、[Next] をクリックします。左パネルで [Microsoft]、右パネルで [Microsoft VPN Adapter] **を選択します。**
2. PPTP 機能を設定するには、次の手順を実行します。 [Start] > [Programs] > [Accessories] > [Communications] > [Dial Up Networking] の順に選択します。[Make new connection] をクリックし、[Select a device] に対して [Microsoft VPN Adapter] を選択します。VPN サーバ IP アドレスには 3000 トンネル エンドポイントの IP アドレスを指定します。
3. パスワード認証プロトコル（PAP）も使用できるように PC の設定を変更するには、次の手順を実行します。 **注：**Windows 98のデフォルト認証では、パスワード暗号化（CHAPまたはMS-CHAP）が使用されます。[Properties] > [Server types] の順に選択します。[Require encrypted password] のチェックマークを外します。この領域でデータの暗号化（Microsoft Point-to-Point Encryption [MPPE] または MPPE なし）を設定できます。

Windows 2000

1. [Start] > [Programs] > [Accessories] > [Communications] > [Network and Dialup connections] の順に選択します。
2. [Make new connection] をクリックし、[Next] をクリックします。
3. [Connect to a private network through the Internet and Dial a connection prior] を選択し（LAN がある場合はこれを選択しないでください）、[Next] をクリックします。
4. トンネル エンドポイント（3000）のホスト名または IP アドレスを入力します。
5. パスワード タイプを変更する場合は、[Properties] > [Security for the connection] > [Advanced] の順に選択します。デフォルトは MS-CHAP と MS-CHAP v2 です（CHAP または PAP ではありません）。 この領域でデータの暗号化（MPPE または MPPE なし）を設定できます。

Windows NT

『Installing, Configuring, and Using PPTP with Microsoft Clients and Servers』sを参照してください。

Q. Cisco VPN Clientをサポートしているオペレーティングシステムのバージョンを

教えてください。

A. VPNクライアントでは、常に追加のオペレーティングシステムのサポートが追加されます。これを確認するには、VPN Client 5.0.07 のリリース ノートに記載されているシステム要件を参照するか、『IPSec/PPTP/L2TP をサポートする Cisco ハードウェアと VPN クライアント』を参照してください。

注：

- VPN クライアントには、Windows XP および Windows Vista のデュアルプロセッサ ワークステーションおよびデュアルコア ワークステーションのサポートが含まれています。
- Windows VPN Client リリース 4.8.00.440 は、Windows 98 オペレーティング システム サポートで公式にされた最後のバージョンです。
- Windows VPN Client リリース 4.6.04.0043 は、Windows NT オペレーティング システムで公式にサポートされた最後のバージョンです。
- Cisco VPN Client ver 5.0.07 は、x86（32 ビット）および x64（64 ビット）エディションの両方で Windows Vista および Windows 7 をサポートします。
- Cisco VPN Client は、Windows XP 32 ビットのみをサポートし、Windows XP 64 ビットはサポートされません。**注：** Windows Vista 32ビットサポートは5.xのすべてのリリースで利用可能でした。Cisco VPN Client バージョン 5.0.07 に 64 ビット サポートが追加されました。

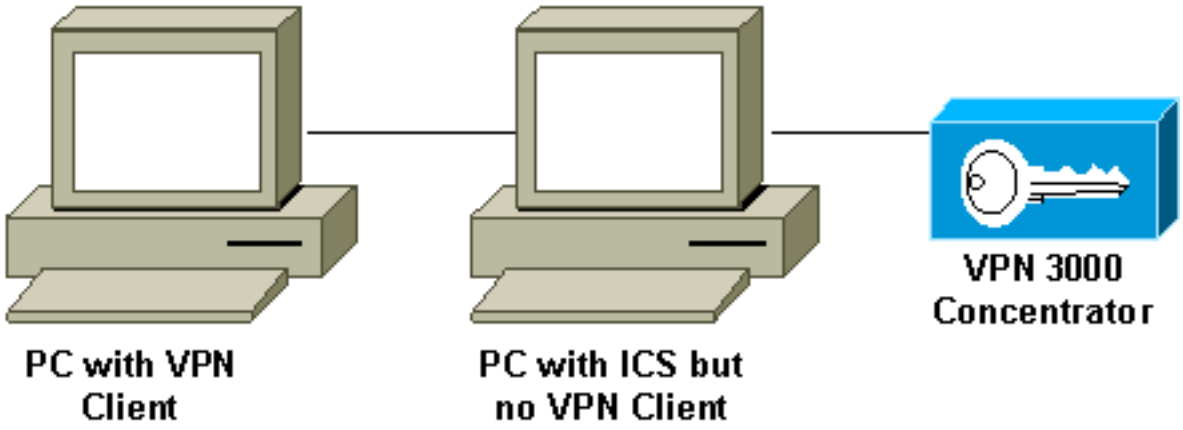
Q. VPN Clientをロードするには、Windows NT/2000マシンの管理者である必要がありますか。

A.はい。Windows NTおよびWindows 2000にVPN Clientをインストールするには、管理者権限が必要です。これらのオペレーティングシステムでは、既存のネットワークドライバにバインドしたり、新しいネットワークドライバをインストールしたりする管理者権限が必要です。VPN Client ソフトウェアはネットワーキング ソフトウェアです。インストールするには管理者権限が必要です。

Q. Cisco VPN Clientは、同じマシンにインストールされたMicrosoft Internet Connection Sharing(ICS)と連携できますか。

A.いいえ。Cisco VPN 3000 Clientは、同じマシン上のMicrosoft ICSと互換性がありません。VPN Client をインストールする前に、ICS をアンインストールする必要があります。詳細は、『Microsoft Windows XP での Cisco VPN Client 3.5.X の新規インストールまたはアップグレードの準備の際の ICS の無効化』を参照してください。

同じ PC 上に VPN Client と ICS があると動作しませんが、次の配置であれば動作します。



Q. VPNクライアントが特定のアドレスにのみ接続しているようです。稼働 OS は Windows XP です。どうすればよいでしょうか。

A. Windows XPの組み込みファイアウォールが無効になっていることを確認します。

Q. Cisco VPN ClientはWindows XPのステートフルファイアウォールと互換性がありますか。

A.この問題は解決しました。Bug Toolkit で Cisco Bug ID CSCdx15865（登録ユーザ専用）を調べると、より詳細な情報を得ることができます。

Q. Windows XPとWindows 2000にVPN Clientをインストールすると、マルチユーザインターフェイスは無効になりますか。

A.インストールでは、初期画面とユーザーの高速切り替えが無効になります。Bug Toolkit で Cisco Bug ID CSCdu24073（登録ユーザ専用）を調べると、より詳細な情報を得ることができます。

Q. Linux用VPN Clientを実行後にバックグラウンドに移動するにはどうすればよいのですか。vpnclient connect foo などで接続を開始した場合、サインインできますが、シェルが返されます。

A.サインオン後に、次のように入力します。

- ^Z
- bg

Q. Windows XP Home EditionにCisco VPN Clientをインストールすると、タスクバーが表示されません。これを元に戻すにはどうすればいいですか。

A.この設定を調整するには、[Control Panel] > [Network Connections] > [Remove Network Bridge]を選択します。

Q. RedHat 8.0にLinux VPN Clientをインストールしようとすると、モジュールがGCC 2でコンパイルされ、カーネルがGCC 3.2でコンパイルされているため、モジュールをロードできないというエラーが表示されます。どうすればよいのですか。

A.これは、RedHatの新しいリリースに新しいバージョンのGCCコンパイラ(3.2+)が搭載されているため、現在のCisco VPN Clientで障害が発生するためです。この問題は修正されており、Cisco VPN 3.6.2a で提供されています。Bug Toolkit で Cisco bug ID CSCdy49082（登録ユーザ専用）を調べてより詳細な情報を得るか、VPN Software Center（登録ユーザ専用）からソフトウェアをダウンロードしてください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。

Q. Windows XPにVPN Client 3.1をインストールすると、なぜソフトウェアがFast User Switching(FAST)を無効にするのですか。

A. GINA.dllがレジストリで指定されている場合、MicrosoftはWindows XPのFast User Switchingを自動的に無効にします。Cisco VPN Client は、「Start Before Login」機能を実装するために CSgina.dll をインストールします。Fast User Switching が必要な場合は、「Start Before Login」機能をディセーブルにしてください。登録ユーザであれば、Bug ToolkitでCisco Bug ID CSCdu24073(登録ユーザ専用)を調べられます。

Q. IPsec VPNクライアントはWindows 7のStart Before Logon(SBL)機能をサポートしていますか。

A. SBL機能は、Windows7のIPsec VPNクライアントではサポートされていません。AnyConnect VPNクライアントではサポートされています。

エラー メッセージ

Q. Cisco VPN Client 4.xをインストールすると、次のエラーメッセージが表示されます。 `Warning 201:The necessary VPN sub-system is not available.You can not connect to the remote VPN server`

A.この問題は、VPNクライアントコンピュータにファイアウォールパッケージがインストールされている場合に発生する可能性があります。このエラー メッセージが表示されないようにするには、ファイアウォール プログラムやアンチウイルス プログラムがインストールされていないこと、またはインストール時に PC 上で稼働していないことを確認してください。

Q. Mac OS X 10.3（Pantherと呼ばれる）にアップグレードしましたが、Cisco VPN Client 4.xに次のエラーメッセージが表示されます。 `Secure VPN Connection terminated locally by the Client Reason:Unable to contact the security gateway`

A. Cisco VPN Client 4.xがMac OS X 10.3 ("Panther")で動作するには、/etc/CiscoSystemsVPNClient/Profiles/ディレクトリにあるプロファイル（.pcfファイル）にUseLegacyIKEPort=0を追加する必要があります。

Q. VPN Clientをアンインストールしようとすると、次のエラーメッセージが表示されます。 `Error msg:failed to find the uninstall file...`このエラー メッセージはどういう意味ですか。また、アンインストールを正常に完了するにはどうすればよいのですか。

A.ネットワークコントロールパネルをチェックして、Deterministic NDIS Extender(DNE)がインストールされていないことを確認してください。また、[Microsoft] > [Current Version] > [Uninstall] の順に選択して、アンインストール ファイルを確認します。

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5624C000-B109-11D4-9DB4-00E0290FCAC5} ファイルを削除して、もう一度アンインストールを実行します。

Q. Windows 2000 ProfessionalでVPN Clientをインストールできません。ASA が深刻なパフォーマンスの低下を示すパケットをドロップするときに、次のエラーが発生します。`An installation support file could not be installed.`Catastrophic Failure.どうすればよいでしょうか。

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstallキーを削除します。次にコンピュータをリブートし、VPN Client を再インストールします。

注：パスHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<*key to be determined*>で*Cisco VPN Client*ソフトウェアの正しいキーを検索するには、*HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems*に移動し、**[VPN Client]をクリックします**。右側のウィンドウの Name 列の下にある Uninstall Path を確認します。 対応する Data 列に VPN Client キーの値が表示されます。このキーに注目するには、HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\ に移動し、確認したキーを選択して削除します。

詳細は、『初期化エラーのトラブルシューティング 』および『Bug Toolkit』のCisco Bug ID CSCdv15391(登録ユーザ専用)を参照してください。

Q. RedHat 8.0にLinux VPN Clientをインストールしようとすると、モジュールがGCC 2でコンパイルされ、カーネルがGCC 3.2でコンパイルされているため、モジュールをロードできないというエラーが表示されます。どうすればよいのですか。

A.この問題が発生するのは、RedHatの新しいリリースに新しいバージョンのGCCコンパイラ(3.2+)が搭載されており、これにより現在のCisco VPN Clientで障害が発生するためです。この問題は修正されており、Cisco VPN 3.6.2a で提供されています。Bug Toolkit で Cisco bug ID CSCdy49082（登録ユーザ専用）を調べてより詳細な情報を得るか、VPN Software Center（登録ユーザ専用）からソフトウェアをダウンロードしてください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。

Q. Linux Client 3.5がPIXまたはVPN 3000コンセントレータへのIPsec接続を確立しようとすると、「peer no longer responding」エラーメッセージが表示されます。どうすればよいでしょうか。

A.この問題の症状は、Linuxクライアントが接続を試みているようですが、ゲートウェイデバイスから応答を受信しないことです。

Linux OS にはファイアウォール ipchains が組み込まれており、これによって UDP ポート 500、UDP ポート 1000、および Encapsulating Security Payload（ESP）パケットがブロックされます。このファイアウォールはデフォルトでオンになっているため、問題を解決するには、ファイアウォールをディセーブルにするか、または IPSec 通信の着信接続と発信接続で使用されるポートを開く必要があります。

Q. Mac OS X 10.3でCisco VPN 5000 5.2.2 Clientを実行しようとすると、カーネル拡張エラーが発生します。どうすればよいのですか。

A.製品のリリースノートに記載されているとおりに、Cisco VPN 5000 Clientはバージョン10.1.xまでサポートされているため、バージョン10.3ではサポートされていません。インストールスクリプトの実行後にインストールされた2つのファイルの権限をリセットできます。以下が一例です。

注：この設定は、シスコではサポートされていません。

```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

Q. Cisco VPN Clientの新しいバージョンをインストールできません。インストールすると、次のエラー メッセージのいずれかが表示されます。「**Error DNEinst execution error while installing DNE, return code -2146500093nstallDNE Error:DNEinst execution error while installing DNE, returncode -2147024891.**」 この問題は、Deterministic Network Enhancerをインストールしたときに発生します。

A. Deterministic Networksから最新のDNEアップグレードをインストールします 。

Q.接続を行うと、Cisco VPN Clientの次のログが表示されます。

```
208     15:09:08.619  01/17/08  Sev=Debug/7CVPND/0x63400015
Value for ini parameter VAEnableAlt is 1.

209     15:09:08.619  01/17/08  Sev=Warning/2CVPND/0xE3400003
Function RegOpenKey failed with an error code of 0x00000002(WindowsVirtualAdapter:558)

210     15:09:08.619  01/17/08  Sev=Warning/3CVPND/0xE340000C
The Client was unable to enable the Virtual Adapter because it could not open the device.
```

A.これは非常に一般的なエラーメッセージで、通常はクライアントの手動アンインストールが必要です。次のリンクで示される手順に従ってください。Removing a VPN Client Version Installed with MSI Installer.

アンインストールが終了したら、必ずリブートしてください。その後、クライアントを再インストールします。ローカル マシンの管理者権限を持つユーザとしてログインするようにしてください。

Q. Mac OSでCisco VPN Clientを接続しようとすると、次のエラーメッセージが表示されます。**Error 51- Unable to communication with the VPN subsystem.**。この問題を解決するには、どうすればよいですか。

A. VPN Clientを次のように閉じた後にサービスを再起動すると、問題を解決できます。

停止するには、次のようにします。

```
sudo kextunload -b com.cisco.nke.ipsec
```

起動するには、次のようにします。

```
sudo kextload /System/Library/Extensions/CiscoVPN/CiscoVPN
```

また、VPN Client がインストールされている同じマシンで以下の機能が実行されてことを確認し

、同じ機能をディセーブルにします。

- 仮想ソフトウェア (VMware フュージョン、Parallels、クロスオーバー)
- ウイルス対策/ファイアウォール ソフトウェア
- VPN Client と 64 ビット オペレーティング システムとの互換性『Cisco VPN Client リリース ノート』を参照してください。

Q. 「Reason 442:failed to enable virtual adapter」というエラー メッセージが表示されます。このエラーを解決するにはどうすればよいのですか。

A.理由`442:failed to enable virtual adapter IP Vista` それ以降の接続失敗でも同じメッセージが表示されますが、Vista からは重複する IP アドレスが検出されたことは報告されません。この問題の解決方法についての詳細は、『Windows Vista における重複する IP アドレスが原因のエラー 442』を参照してください。

Q. Cisco VPN Clientをインストールすると、「`Deterministic Network Enhancer Add Plugin Failed`表示されます。この問題の解決方法を次に説明します。

A. DNEアダプタをインストールすると、問題が解決する可能性があります。インストールには、MSI の代わりに InstallShield バージョンを使用することをお勧めします。

Q.次のエラーが表示されました。`Reason 442:failed to enable virtual adapter.`。この問題を解決するには、どうすればよいですか。

A.このエラーは、Windows 7とWindows Vistaが重複するIPアドレスを検出したことを報告した後に表示されます。それ以降の接続失敗でも同じメッセージが表示されますが、OS からは重複する IP アドレスが検出されたことは報告されません。この問題の解決方法についての詳細は、『Windows 7 および Vista における重複する IP アドレスが原因のエラー 442』を参照してください。

Q. VPN Client 4.9 for MAC OS 10.6を起動しようとすると、次のエラーが表示されます。`Error 51:Unable to communicate with the vpn subsystem.`問題を解決するには、どうすればよいのですか。

A.この問題は、MAC OSリリース4.9のCisco VPN Clientでは64ビットサポートが利用できないために発生します。回避策として、32ビットカーネルモードでブートできます。詳細は、Cisco Bug ID CSCth11092 (登録ユーザ専用) および『MAC OSX 対応 Cisco VPN Client のリリース ノート』を参照してください。

サード パーティ製品との互換性

Q. Nortel ClientはCisco VPN 3000コンセントレータと互換性がありますか。

A.いいえ。Nortel ClientはCisco VPN 3000コンセントレータに接続できません。

Q. Nortel Contivity VPN Clientなどの他のベンダーのVPNクライアントをCisco VPN Clientと同時にインストールできますか。

A.いいえ。同じPCに複数のVPNクライアントがインストールされている場合は、既知の問題があります。

Q. Cisco VPN Clientはサードパーティ製VPNコンセントレータでサポートされていますか。

A. Cisco VPN Clientは、サードパーティ製VPNコンセントレータではサポートされていません。

[Authentication]

Q. Cisco VPN Clientバージョン1.1および3.xは、デジタル証明書(X.509v3)を内部でどのように保存するのですか。

A. Cisco VPN Client 1.1には独自の証明書ストアがあります。Cisco VPN Client 3.x では、Common-Application Programming Interface（CAPI）を使用して Microsoft の保存域に証明書を保存することも、Cisco 独自の保存域（RSA Data Security）に証明書を保存することもできます。

Q. VPNコンセントレータで同じグループ名とユーザ名を使用できますか。

A.いいえ、グループ名とユーザー名を同じにすることはできません。これはソフトウェアバージョン2.5.2および3.0で見られ、3.1.2に統合された既知の問題です。詳細については、Bug ToolkitでCisco Bug ID CSCdw29034(登録ユーザ専用)を参照してください。

Q. Defenderなどのフルチャレンジカードは、Cisco VPN ClientからPIXでサポートされていますか。

A.いいえ。この種類のカードはサポートされていません。

VPN Client ソフトウェアのバージョン

Q. Cisco VPN Clientバージョン2.5.2以前の「Set MTU Utility」オプションはどうなりましたか。

A. Cisco VPN Client**は**、最大伝送ユニット(MTU)サイズを調整するようになりました。[Set MTU Utility] オプションは、必須のインストール ステップではなくなりました。[Set MTU] オプションは、主に接続性の問題のトラブルシューティングに使用されます。Windows マシンで [SetMTU] オプションを選択するパスは、[Start] > [Programs] > [Cisco Systems VPN Client] > [SetMTU] です。[SetMTU] オプションや他のオペレーティング システムでこのオプションを設定する方法の詳細については、「[SetMTU] オプションによる MTU サイズの変更」を参照してください。

Q. 4.0以降のCisco VPN Client GUIバージョンでは、どのような言語がサポートされていますか。

A. Cisco VPN Client GUIバージョン4.0以降でサポートされている言語は、カナダ、フランス語、日本語です。

Q. Cisco VPN Clientでは、どのパーソナルファイアウォールがサポートされていますか。

A.より高いレベルのセキュリティを提供するため、VPN Clientは、サポートされているファイアウォールの動作を強制するか、インターネットに送信されるトラフィックに対してプッシュされたステートフルファイアウォールポリシーを受信できます。

現在、VPN Client 5.0 は次のパーソナル ファイアウォールをサポートしています。

- BlackIce Defender
- Cisco Security Agent
- Sygate Personal ファイアウォール
- Sygate Personal Pro ファイアウォール
- Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

バージョン 3.1 以降では、リモート ユーザがインストールしているパーソナル ファイアウォール ソフトウェアを検出し、該当するソフトウェアがない場合はそのユーザからの接続を禁止する新しい機能が VPN 3000 コンセントレータに追加されています。この機能を設定するには、[Configuration] > [User Management] > [Groups] > [Client FW] の順に選択し、グループのタブを選択します。

Cisco VPN Client マシンでのファイアウォール ポリシーの適用の詳細については、「ファイアウォール設定のシナリオ」を参照してください。

Q. AOL 7.0でCisco VPN Client 3.xを使用する場合、接続に問題がありますか。

A. Cisco VPN Clientは、スプリットトンネリングを使用しないとAOL 7.0では動作しません。Bug Toolkit で Cisco Bug ID CSCdx04842（登録ユーザ専用）を調べると、より詳細な情報を得ることができます。

VPN Client ソフトウェアの設定

Q. Cisco VPN Clientが30分後に接続解除されるのはなぜですか。この期間を延長することはできますか。

A.この30分間にユーザ接続に通信アクティビティがない場合、システムは接続を終了します。アイドル タイムアウトのデフォルト設定は 30 分になっていますが、最小 1 分から最大 2,147,483,647 分（4,000 年超）までの値に設定可能です。

[Configuration] > [User Management] > [Groups] の順に選択して、適切なグループ名を選択して、アイドル タイムアウトの設定を変更します。[Modify Group] を選択して、[HW Client] **タブをクリックし、に移動し、望ましい値を [User Idle Timeout] フィールドに入力します。 0 を入力すると、タイムアウトがディセーブルになり、無制限にアイドルが許可されます。**

Q. Cisco VPN Clientは、すべてのパラメータを事前設定して導入できますか。

A. vpnclient.iniファイルが最初にインストールされたときにVPN Clientソフトウェアにバンドルされている場合、インストール中にVPN Clientが自動的に設定されます。またプロファイル ファイ

ル（接続エントリごとに 1 つの .pcf ファイル）を、自動設定用に事前設定された接続プロファイルとして配布することもできます。VPN Client ソフトウェアのコピーをインストールするユーザに配布するには、次の手順を実行します。

1. 配布用 CD-ROM から、vpnclient.ini（グローバル）ファイルおよび特定のユーザ群に対して個別の接続ファイルを作成した各ディレクトリへ VPN クライアント ソフトウェア ファイルをコピーします。**注：**Mac OS Xプラットフォームでは、VPN Clientをインストールする前に、事前設定されたファイルがProfilesフォルダとResourcesフォルダに配置されます。vpnclient.ini ファイルは、インストーラのディレクトリに配置されます。VPN クライアント インストーラのディレクトリ内にあるカスタム vpnclient.ini ファイルは、Profiles フォルダおよび Resources フォルダと同じレベルに配置する必要があります。詳細は、『VPN Client User Guide for Mac OS X』の第2章を参照してください
2. バンドルされたソフトウェアを準備し、それを配布します。CD-ROM またはネットワークによる配布。vpnclient.ini ファイルおよびプロファイル ファイルが、すべての CD-ROM イメージ ファイルと同じディレクトリにあることを確認します。ユーザは、このディレクトリからネットワーク接続を使用してインストールできます。または、配布用の新しい CD-ROM にすべてのファイルをコピーできます。もしくは、このディレクトリにあるすべてのファイルを含む自己解凍 zip ファイルを作成し、それをユーザがダウンロードして、ソフトウェアをインストールできます。
3. ユーザに対し、設定に必要なその他の情報や指示を与えます。ご使用のプラットフォームに対応する『VPN Client User Guide』の第 2 章を参照してください。

Q. Cisco VPN ClientがNICカードと競合しているようです。どのようにトラブルシューティングすればよいのですか。

A. NICカードで最新のドライバを実行していることを確認します。これは常に行うことをお勧めします。可能であれば、問題がオペレーティング システム、PC ハードウェア、および他の NIC カードに固有であるかどうかを確認するために、テストを行ってください。

Q.ダイヤルアップネットワークからのCisco VPN Client接続を自動化するにはどうすればよいのですか。

A. VPN接続へのダイヤルアップを完全に自動化するには、**[Options] > [Properties] > [Connections]の順に選択**し、ダイヤルアップネットワークの電話帳エントリをCisco VPN Clientがプルダウンできるように設定します。

Q. VPNクライアントのアップデートをリモートユーザに通知するには、Cisco VPN 3000コンセントレータをどのように設定すればよいのですか。

A.リモートシステム上のVPN Clientソフトウェアを更新する時間になったら、VPN Clientユーザに通知できます。段階的な手順については、「リモート ユーザへのクライアント アップデートの通知」を参照してください。このプロセスのステップ 7 に記載されているとおり、必ずリリース情報を「(Rel)」と入力してください。

Q. Cisco VPN Clientが表示される前に、特に[Start Before Logon]オプションが有効になっている場合に遅延が発生する原因は何ですか。

A. Cisco VPN Clientはフォールバック*モード*です。このことが遅延に影響しています。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。フォールバック モードで動作する場合、VPN Client では必要な Windows サービスが起動しているかどうか確認されません。その結果、Cisco VPN Clientをアンインストールし、問題のアプリケーションを削除して、「フォールバック」モードにならずに起動できるようにしてください。その後、Cisco VPN Client を再インストールします。フォールバック モードの詳細については、「Start Before Logon」を参照してください。

Bug Toolkit で Cisco Bug ID CSCdt88922（登録ユーザ専用）と CSCdt55739（登録ユーザ専用）を調べると、より詳細な情報を得ることができます。

Q. ipsecdialer.exeとvpngui.exeの違いを理解する必要があります。Windows XP のスタートアップに vpngui.exe がインストールされているのに、会社のリソースにアクセスするために ipsecdialer.exe を手動で起動する必要があるのはなぜですか。サイズの違いを除けば、これらのプログラムは同じことをして会社のネットワークに VPN ログオンしているように見えます。

A. ipsecdialer.exeは、Cisco VPN Clientバージョン3.xの最初の起動メカニズムでした。GUI がバージョン 4.x で変更された際に、vpngui.exe という新しい実行可能ファイルが作成されました。ipsecdialer.exe ファイルは下位互換性のために名前のみを継承したものであり、単に vpngui.exe を起動するだけです。ファイル サイズが異なっているのはこのためです。

したがって、Cisco VPN Client をバージョン 4.x からバージョン 3.x にダウングレードすると、ipsecdialer.exe ファイルを使用して VPN Client を起動する必要があります。

Q.スタートアップVPNアイコンを安全に削除できますか。これはなぜ必要なのですか。

A.起動フォルダのCisco VPN Clientは、「Start Before Logon」機能をサポートしています。この機能を使用しない場合、スタートアップ フォルダにこのアイコンを置く必要はありません。

Q. ipsecdialer.exeのショートカットに「user_logon」が追加されているのはなぜですか。「user_logon」の目的は何ですか。

A. 「Start Before Logon」機能には「user_logon」が必要ですが、ユーザによるCisco VPN Clientの通常の起動では必要ありません。

NAT/PAT の問題

Q.ポートアドレス変換(PAT)デバイスを介して接続できるVPNクライアント（リリース3.3以前）が1つだけの場合に問題が発生しています。この問題を改善するにはどうすればよいですか。

A.複数のネットワークアドレス変換(NAT)/PATの実装に不具合があり、1024未満のポートが変換されません。Cisco VPN Client 3.1では、NAT透過が有効になっている場合でも、Internet Security Association and Key Management Protocol(ISAKMP)セッションではUDP 512が使用されます。最初のVPNクライアントはPATデバイスを通過し、外部の送信元ポート5112112を112のままにします。2 番目の VPN Client が接続するときには、ポート 512 はすでに使用中になっています。そのため、接続に失敗します。

考えられる回避策は 3 つあります。

- PAT デバイスを修理する。
- VPN Client を 3.4 にアップグレードし、TCP カプセル化を使用する。
- すべての VPN Client に代えて VPN 3002 をインストールする。

Q. 2台のラップトップを同じ場所からCisco VPN Clientに接続できますか。

A. SOHOルータ/ファイアウォールなどのPATを実行するデバイスの背後にクライアントが両方とも存在しない限り、2つのクライアントが同じ場所から同じヘッドエンドに接続できます。多くの PAT デバイスでは、1 つの VPN 接続をその背後のクライアントにマッピングできますが、2 つをマッピングすることはできません。PAT デバイスの背後の同じ場所から 2 台の VPN Client を接続できるようにするためには、NAT-T、IPSec over UDP、IPSec over TCP など、何らかのカプセル化をヘッド エンドでイネーブルにします。一般には、クライアントとヘッド エンドの間に NAT デバイスが存在する場合は、NAT-T か別のカプセル化をイネーブルにします。

その他

Q.ラップトップを使用してオフィスのネットワークに接続し、ラップトップを自宅に持ち帰ると、自宅からVPN 3000コンセントレータに接続できません。この問題の原因は何ですか?

A.ノートPCがLAN接続からのルーティング情報を保持している可能性があります。この問題の解決方法についての詳細は、『VPN クライアント使用時における Microsoft のルーティング問題』を参照してください。

Q. VPNクライアントがVPNコンセントレータに接続されているかどうかは、どのように確認できますか。

A. HKLM\Software\Cisco Systems\VPN Client\TunnelEstablishedという名前のレジストリキーを確認します。トンネルがアクティブな場合、値は1です。トンネルがない場合、値は0です。

Q. VPNコンセントレータの背後にあるPCからVPNクライアントへのNetMeeting接続に問題がありますが、PCからVPNコンセントレータの背後にあるVPNクライアントへの接続は機能します。これを解決するにはどうすればいいですか。

A.接続設定を制御するには、次の適切な手順に従います。

- PC のメインドライブで、[Program Files] > [Cisco Systems] > [VPN Client] > [Profiles] の順に選択します。使用しているプロファイルを右クリックし、サブメニューから [Open With] を選択し、Notepad などのプログラムでプロファイルを開きます（使用するプログラムを選択するときに、必ず [Always use this program to open these files] というボックスのチェックマークを外してください）。 ForcekeepAlives のプロファイル パラメータを探し、値を 0 から 1 に変更して、プロファイルを保存します。または
- VPN Client で、[Options] > [Properties] > [General] の順に選択し、この『サンプル ウィンドウ』に示すように、「Peer response timeout」の値を入力します。タイムアウトの間隔は 30 ~ 480 秒の範囲で指定できます。または
- VPN コンセントレータで、[Configuration] > [User Management] > [Groups] > [modify group]

の順に選択します。[IPSec] タブで、このサンプル ウィンドウに示すように、IKE キープアライブのオプションを選択します。

Dead Peer Detection（DPD）のインターバルは、間隔設定によって異なります。応答が受信されなくなると、さらにアグレッシブなモードに移行し、ピア応答のしきい値に達するまで 5 秒ごとにパケットが送信されます。その時点で、接続が切断（クリア）されます。キープアライブはディセーブルにできますが、そうすると、接続が実際に切断された場合は、タイムアウトになるまで待機する必要があります。最初は間隔値をきわめて低く設定することをお勧めします。

Q. Cisco VPN Clientは二重認証をサポートしていますか。

A.いいえ。二重認証はCisco VPN Clientではサポートされていません。

Q.アグレッシブモードではなく、メインモードで接続するようにCisco VPN Clientを設定するにはどうすればよいのですか。

A. Cisco VPN Clientがメインモードで接続できるようにするには、デジタル署名（証明書）を使用する必要があります。これを実現するに次の 2 つの方法があります。

1. ルータおよびすべての Cisco VPN Client で、サードパーティ認証プロバイダー（たとえば、Verisign または Entrust）から CA 証明書を取得します。同じ CA サーバから ID 証明書を登録し、Cisco VPN Client とルータ間で認証する方法としてデジタル署名を使用します。この設定についての詳細は、「Entrust 証明書を使用する Cisco IOS ルータと Cisco VPN Client の間の IPSec の設定」を参照してください。
2. 2 番目のオプションは、リモート アクセス VPN へのヘッドエンドとともに CA サーバとしてルータを設定する方法です。証明書（および他のすべて）をインストールすると、ルータが CA サーバとして動作する以外、前のリンクで説明されているとおりになります。詳細については、「ハブ設定の例で IOS CA を使用した Cisco IOS ルータ間のダイナミック LAN-to-LAN VPN」を参照してください。

Q. VPN Clientアクセスファイルで必要なパラメータを読み取り専用にするにはどうすればよいのですか。

A.パラメータを読み取り専用にするには、.pcfファイルの各パラメータの前に感嘆符(!)を追加します。

VPN Client のユーザは感嘆符（！）で始まるパラメータの値を変更できません。GUI 内のこれらの値のフィールドはグレー表示されます（読み取り専用）。

次に設定例を示します。

元の .pcf ファイル

```
[main]

Description=connection to TechPubs server

Host=10.10.99.30

AuthType=1
```

```
GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C85
             1ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

Username=alice
```

変更された .pcf ファイル

```
[main]

!Description=connection to TechPubs server

!Host=10.10.99.30

AuthType=1

!GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C
          851ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

!Username=alice
```

この例では、ユーザは Description、Host、GroupName、および Username の値を変更できません。

Q. MACアドレスに基づいてVPNクライアントへのアクセスを制限することはできますか。

A.いいえ。MACアドレスに基づいてVPNクライアントへのアクセスを制限することはできません。

関連情報

- Cisco VPN 3000 クライアントに関するサポート ページ
- Cisco VPN Client に関するサポート ページ

- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- テクニカル サポートとドキュメント – Cisco Systems