CHAPTER 5

リモート ユーザに関する VPN クライアントの事前設定

この章では、リモート ユーザに関する設定を準備する方法およびそれらを配布する方法について説明します。この章は、次の項で構成されています。

ユーザ プロファイル

リモート ユーザが VPN 中央サイト デバイスへの接続に使用する接続エントリは、設定パラメータのグループによって定義されます。これらのパラメータをまとめて、プロファイルと呼ばれるファイルが構成されます。プロファイルには 2 種類あります。1 つはグローバル プロファイル、もう 1 つは個別プロファイルです。

- グローバル プロファイルは、すべてのリモート ユーザに対するルールを設定するためのもので、VPN クライアント用のパラメータがすべて含まれています。グローバル プロファイルのファイル名は vpnclient.ini です。
- 個別プロファイルは、各接続エントリに関するパラメータ設定が記述されており、その接続エントリに特化したものです。個別プロファイルの拡張子は .pcf です。

プロファイルは次の 2 つの方法で作成されます。

1. 管理者またはリモート ユーザが VPN クライアントのグラフィカル ユーザ インターフェイスを使用して接続エントリを作成する（Windows および Macintosh のみ）
2. テキスト エディタを使用して自らプロファイルを作成する

   前者の場合、リモート ユーザはテキスト エディタで編集可能なファイルも作成します。GUI を使用して生成されたプロファイル ファイルを基にして、その内容を編集することができます。この方法を用いると、VPN クライアント GUI アプリケーションで使用できない一部のパラメータを制御することができます。（自動実行またはダイヤルアップがサードパーティ ダイヤラを待つするようにするなど）。

個別プロファイルのデフォルトの場所は次のとおりです。

- Windows プラットフォームの場合：C:¥Program Files¥Cisco Systems¥VPN Client¥Profiles
- Linux プラットフォーム、Solaris プラットフォーム、および Mac OS X プラットフォームの場合：/etc/CiscoSystemsVPNClient/Profiles/

この章では、vpnclient.ini および個別プロファイルの作成方法と編集方法について説明します。どちらのファイルにも、同じ表記法が使用されます。

（注）　Windows プラットフォーム用のプロファイルを作成する方法としては、VPN クライアントを起動し、VPN クライアント GUI を使用してパラメータを設定するのが最も簡単です。この方法でプロファイルを作成すると、リモート ユーザへの配布ディスクに .pcf ファイルをコピーできます。この方法を使用すると、パラメータ入力時に生じる可能性があるエラーを回避できるほか、グループ パスワードが暗号化形式に自動で変換されます。

すべてのプロファイル ファイルに適用されるファイル書式

vpnclient.ini ファイルおよび .pcf ファイルの書式は、次のように通常の Windows.ini ファイルに準拠しています。

- コメントの先頭にはセミコロン（;）を使用します。
- セクション名は [section name] のように角カッコで囲みます。小文字と大文字は区別されません。
- *keyword* = *value* のように、キー名を使用してパラメータの値を設定します。値がないキーワードや指定されていないキーワードには、VPN クライアントのデフォルト値が使用されます。キーワードの順序は任意です。また大文字と小文字は区別されません。ただし、大文字と小文字を使い分けた方が読みやすくなります。

パラメータの読み取り専用化

VPN クライアント アプリケーション内のパラメータをクライアント ユーザが変更できないように、それらを読み取り専用にする場合は、パラメータ名の先頭に感嘆符（!）を付加します。これにより制御できるのは、VPN クライアント アプリケーション内でユーザが行える操作のみです。ユーザによる global ファイルまたは .pcf ファイルの編集や、読み取り専用指定子の削除を行えないようにすることはできません。

グローバル プロファイルの作成

グローバル プロファイルの名前は vpnclient.ini です。このファイルは、次のディレクトリに保存されています。

- Windows プラットフォームの場合：C:¥Program Files¥Cisco Systems¥VPN Client ディレクトリ
- Linux プラットフォーム、Solaris プラットフォーム、および Mac OS X プラットフォームの場合：/etc/CiscoSystemsVPNClient/vpnclient.ini

これらは、インストール時に作成されたデフォルトの場所です。

グローバル プロファイルにより制御される機能

vpnclient.ini ファイルでは、すべての VPN クライアント プラットフォームの次のような機能を制御できます。

- Start Before Logon
- 起動時におけるデフォルトの接続エントリ（デフォルトのプロファイル）への自動接続

- ログオフ時の自動接続解除
- クラス単位でのロギング サービスの制御
- 証明書登録
- HTTP トラフィックをルーティングするプロキシ サーバの識別
- 接続時に起動するアプリケーションの識別
- グループ所在不明の警告メッセージ
- ログ クラスのログ レベル
- RADIUS SDI 拡張認証処理
- GUI パラメータ：GUI アプリケーションの外観および動作

vpnclient.ini ファイルでは、Windows プラットフォームの次のような追加機能を制御できます。

- Entrust.ini ファイルの検索
- VPN クライアントと互換性がない GINA のリスト
- 自動実行
- ステートフル ファイアウォール オプションの設定
- Windows 2000 プラットフォームおよび Windows XP プラットフォームでドメイン名にサフィックスを追加するための方法
- サードパーティ ダイヤラの使用時に IP アドレスを受信してから IKE トンネルが開始されるまでの待機時間
- HTTP トラフィックをルーティングするネットワーク プロキシ サーバ
- アプリケーションの起動
- DNS サフィックス
- Windows NT、Windows 2000、または Windows XP 上のユーザに対して、キャッシュされているクレデンシャルを使用することなくネットワークからのログアウトとネットワークへの再ログインを強制する強制ネットワーク ログイン
- アクセシビリティ オプションの設定
- デフォルトの接続エントリの設定
- デフォルトの接続エントリへの接続

vpnclient.ini ファイルのサンプル

（注） VPN クライアント用のプロファイルは、プラットフォーム間で互換性があります。Windows プラットフォームに固有のキーワードは、その他のプラットフォームでは無視されます。

このサンプル ファイルは、テキスト エディタで開いた場合に表示される内容の一例を示したものです。

```
[main]
IncompatibleGinas=PALGina.dll,theirgina.dll
RunAtLogon=0
EnableLog=1
DialerDisconnect=1
AutoInitiationEnable=1
AutoInitiationRetryInterval=1
AutoInitiationRetryLimit=50
AutoInitiationList=techsupport,admin
```

```
[techsupport]
Network=175.55.0.0
Mask=255.255.0.0
ConnectionEntry=ITsupport
[admin]
Network=176.55.0.0
Mask=255.255.0.0
ConnectionEntry=Administration
Connectonopen=1
[LOG.IKE]
LogLevel=1
[LOG.CM]
LogLevel=1
[LOG.PPP]
LogLevel=2
[LOG.DIALER]
LogLevel=2
[LOG.CVPND]
LogLevel=1
[LOG.CERT]
LogLevel=0
[LOG.IPSEC]
LogLevel=3
[LOG.FIREWALL]
LogLevel=1
[LOG.CLI]
LogLevel=1
[CertEnrollment]
SubjectName=Alice Wonderland
Company=University of OZ
Department=International Relations
State=Massachusetts
Country=US
Email=AliceW@UOZ.com
CADomainName=CertsAreUs
CAHostAddress=10.10.10.10
CACertificate=CAU
[Application Launcher]
Enable=1
Command=c:\apps\apname.exe
[NetLogin]
Force=1
Wait=10
DefaultMsg=For authorized users only
Separator=************************************
[GUI]
WindowWidth=578
WindowHeight=367
WindowX=324
WindowY=112
VisibleTab=0
ConnectionAttribute=0
AdvancedView=1
DefaultConnectionEntry=ACME
MinimizeOnConnect=1
UseWindowSettings=1
ShowToolTips=1
ShowConnectHistory=1
AccessibilityOption=1
```

ここでは、vpnclient.ini ファイルに表示できるパラメータと、それらの役割および使用方法について説明します。

グローバル プロファイルの設定パラメータ

表 5-1 は、すべてのパラメータ、キーワード、および値を表にまとめたものです。また、VPN クライアント GUI アプリケーションで使用されるパラメータ名、およびアプリケーション内でそのパラメータを設定する場所についても記載されています。

各パラメータは、特に指定がない限り、すべての VPN クライアント プラットフォーム上で設定することができます。

表 5-1　vpnclient.ini ファイルのパラメータ

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
[main]	メイン セクションを表すための必須キーワードです。	[main] ファイルの先頭のエントリとして、ここに表記されているとおりに入力します。	GUI には表示されません。
DialupWait	General Packet Radio Service（GPRS）などのサードパーティ ダイヤラから IP アドレスを受信後、IKE トンネルが開始されるまでの待機時間を秒数で指定します。 十分な時間を付与すれば、初回の試行で接続を完了することができます。	キーワードおよび等号の後に、待機時間の秒数を入力します。例： DialupWait=1 デフォルト値 = 0。	GUI には表示されません。
IncompatibleGinas（Windows のみ）	シスコの GINA とは互換性がない Graphical Identification and Authentication ダイナミック リンク ライブラリ（GINA.DLL）のリストが表示されます。このリストに GINA を追加した場合、VPN クライアントでは、インストール中にその GINA が無視され、フォールバック モードが使用されます。VPN クライアントがフォールバック モードに移行するのは RunAtLogon = 1 の場合のみです。それ以外の場合、クライアントの GINA はインストールされません。（「Start Before Logon および GINA：Windows のみ」を参照）。	キーワードおよび等号の後に、GINA の名前をカンマ区切り形式で入力します。例： IncompatibleGinas= PALgina.dll, Yourgina.dll, Theirgina.dll 名前は引用符で囲まないでください。	GUI には表示されません。
MissingGroupDialog	ユーザが事前共有接続でグループ名を指定しないまま接続を試行した場合に表示されるポップアップ ウィンドウの警告を制御します。	0 =（デフォルト）警告メッセージを表示しません。 1 = 警告メッセージを表示します。	GUI には表示されません。

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
RunAtLogon (Windows のみ)	ユーザが Microsoft ネットワークにログインする前に VPN クライアント接続を開始するかどうかを指定します。Windows NT プラットフォーム（Windows NT 4.0、Windows 2000、および Windows XP）でのみ使用できます。この機能は、NT ログオン機能と呼ばれることもあります。	0 = ディセーブル（デフォルト） 1 = イネーブル	[Options] > [Windows Logon Properties] > [Enable start before logon]
EntrustIni= (Windows のみ)	entrust.ini ファイルが default.ini ファイルとは異なる場所に存在する場合は、その所在を指定します。デフォルトの場所は、Windows システム ディレクトリです。	場所の絶対パス名	GUI には表示されません。
DialerDisconnect= (Windows のみ)	Windows NT プラットフォーム（Windows NT 4.0、Windows 2000、および Windows XP）からのログオフ時に自動的に接続を解除するかどうかを指定します。このパラメータを無効にした場合、ユーザがログオフしても VPN 接続は維持されるため、ユーザが再ログインする際には新たな接続を確立する必要はありません。	0 = ディセーブル 1 = イネーブル（デフォルト。ログオフ時に接続解除）	[Options] > [Windows Logon Properties] > [Disconnect VPN connection when logging off]
DialerDisconnect にはいくつかの制約があります。たとえば MS DUN の場合は、ユーザがログオフした時点で RAS（PPP）接続が解除されることがあります。この具体的な事例の詳細については、次の URL を参照してください。 http://support.microsoft.com/support/kb/articles/Q158/9/09.asp?LN=EN-US&SD=gn&FR=0&qry=RAS%20AND%20LOGOFF&rnk=2&src=DHCS_MSPSS_gn_SRCH&SPR=NTW40			
EnableLog=	ロギング サービスを使用するクラスに対してログ設定を無効にするかどうかを指定します。デフォルトでは、ロギングは有効です。このパラメータを使用すると、ユーザはクラスごとにログ レベルを 0 に設定することなくロギングを無効にすることができます。ロギングを無効にすると、クライアント システムのパフォーマンスを向上させることができます。	0 = ディセーブル 1 = イネーブル（デフォルト）	[Log] > [Enable/Disable]

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
StatefulFirewall= (Windows のみ)	ステートフル ファイアウォールを常時オンにしておくかどうかを指定します。ステートフル ファイアウォールを常時オンにする機能を有効にした場合、VPN 接続が有効かどうかにかかわらず、すべてのネットワークからの着信セッションは許可されません。また、ファイアウォールもトンネリングされたトラフィックと、トンネリングされていないトラフィックの両方に対してアクティブになります。	0 = ディセーブル（デフォルト） 1 = イネーブル	[Options] > [Stateful Firewall (Always On)]
StatefulFirewallAllowICMP（Windows のみ）	[StatefulFirewall (Always On)] で ICMP トラフィックを許可するかどうかを制御します。 一部の DHCP サーバでは、リースを無効にするまたは維持することができるように、ICMP ping を使用して、DHCP クライアント PC が稼動しているかどうかの検出が行われます。	0 = ディセーブル（デフォルト） 1 = イネーブル	GUI には表示されません。
AutoInitiationEnable	LAN 環境においてワイヤレス VPN 接続の確立を自動化するための手段である自動実行を有効にします。	0 = ディセーブル（デフォルト） 1 = イネーブル	[Options] > [Automatic VPN Initiation]
AutoInitiationRetry-Interval	接続の試行に失敗してから自動実行が再試行されるまでの待機時間を指定します。この時間の単位を分にするか秒にするかは、AutoInitiationRetryIntervalType パラメータで指定します。	デフォルトは 1 分です。 値の範囲は 1 ～ 10 分または 5 ～ 600 秒です。	[Options] > [Automatic VPN Initiation]
AutoInitiationRetry-IntervalType	再試行の間隔を分単位（デフォルト）で表示するか秒単位で表示するかを指定します。デフォルトは 0（分）です。	0 = 分（デフォルト） 1 = 秒	[Options] > [Automatic VPN Initiation]
AutoInitiationRetry-Limit	接続の試行が連続何回失敗すると、自動実行が取り消しになり接続の試行が中止されるのかを指定します。	1 ～ 1000 デフォルト：0（無制限）	該当なし
AutoInitiationList	vpnclient.ini ファイル内で自動実行に関連するセクション名を指定します。vpnclient.ini ファイルには、最大 64 件の自動実行リスト エントリを記述できます。	次の例のような、カンマ区切りのセクション名のリスト SJWLAN, RTPWLAN, CHWLAN	GUI には表示されません。

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
SetMTU （Windows 以外のみ、4.8.x 以降）	VPN クライアントの接続中に MTU に使用する値を指定します。ちなみに、Windows で使用されるデフォルトの値は 1300 です。	キーワードおよび等号の後に、使用する MTU 値を入力します。 • SetMTU=1356（Windows 以外のデフォルト） • SetMTU=1200（トラブルシューティングで推奨される値）	GUI には表示されません。
CertificateKeyUsage (4.8.x)	全ストアの証明書のうち使用可能なものを、証明書キーの用途に関するパラメータとして Digital Signature または Non-repudiation が指定されている証明書に制限します。 このキーワードは、プロファイルの中で CertMatchKU キーワードが使用されていない限り、CertMatchDN などその他のあらゆる証明書一致基準に優先します。	CertificateKeyUsage=0（デフォルト） CertificateKeyUsage=1 （Digital Signature または Non-repudiation に一致する証明書のみ）	GUI には表示されません。
[*section name*] （AutoInitiationList 内の項目の）	各セクションには、ネットワーク アドレス、ネットワーク マスク、接続エントリ名、および接続フラグが指定されます。Network および Mask の値によりサブネットが特定されます。接続エントリには、接続プロファイル（.pcf ファイル）を指定します。Connect フラグには、接続を自動的に開始するかどうかを指定します。	*角カッコで囲まれたセクション名* Network = *IP アドレス* Mask = *サブネット マスク* ConnectionEntry = *接続エントリ（プロファイル）の名前* Connect = 1 または 0 0 = 接続を自動的には開始しない 1 = 接続を自動的に開始する（デフォルト） 例： [SJWLAN] Network=110.110.110.0 Mask=255.255.0.0 ConnectionEntry=SantaJuan WirelessLAN	GUI には表示されません。

vpnclient.ini ファイルにおける自動実行の設定例

[main]
AutoInitiationEnable = 1—Start automatic initiation.
autoInitiationList = autonet—identifies a section name in the list for automatic initiation.
AutoInitiationRetryInterval = 60—Try to connect every 60 seconds.
AutoInitiationRetryIntervalType = 1—Set retry interval type to seconds.
AutoInitiationRetryLimit = 25—Try to connect 25 times. If connection attempts fail 25 times, stop trying to connect.
[autonet]—Start an entry in the automatic initiation list.
network = 192.168.0.0—Identify the IP address of the connection entry.
mask = 255.255.0.0—Specify the submask
connectionentry = flatirons—Specify the connection entry name s(.pcf file).

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
ConnectOnOpen	DefaultConnectionEntry パラメータで設定されたデフォルトのユーザ プロファイルに自動接続します。	0 = ディセーブル（デフォルト） 1 = イネーブル	[Main] メニュー > [Options] > [Preferences] > [Enable connect on open]
VAEnableAlt	仮想アダプタの初期化方法を、標準的な方法から別の方法に変更します。ユーザが VA を容易に初期化できない場合は、別の方法を使用することを推奨します。	0 = 別の方法を使用して VA を初期化する 1 = 標準的な方法を使用して VA を初期化する（デフォルト）	該当なし
AddDhcpRoute（Windows のみ）	DHCP サーバ宛てのトラフィックをすべてバイパスするためのルートを追加します。これは通常の動作です。ただし、サーバ上に別のサービスが存在するために、DHCP サーバ宛てのすべてのトラフィックが VPN クライアントによりバイパスされることをユーザが希望しない場合は、このパラメータを使用してソフトウェアのデフォルトの動作を変更します。	0 = DHCP サーバをバイパスするためのルートを追加しない 1 = DHCP サーバをバイパスするためのルートを追加する（デフォルト）	
以降の各クラスに対しては、LogLevel= パラメータを使用してログ レベルを 0 ～ 15 のいずれかの値に設定します。			
[LOG.IKE]	ログ レベルを設定するインターネット キー エクスチェンジ クラスを指定します。	[LOG.IKE] ここに表記されているとおりに入力します。	[Log] > [Settings]
[LOG.CM]	ログ レベルを設定する Connection Manager クラスを指定します。	[LOG.CM] ここに表記されているとおりに入力します。	[Log] > [Settings]
[LOG.XAUTH]	ログ レベルを設定する拡張認可クラスを指定します。	[LOG.XAUTH] ここに表記されているとおりに入力します。	[Log] > [Settings]
[LOG.PPP] （Windows のみ）	ログ レベルを設定する PPP クラスを指定します。	[LOG.PPP] ここに表記されているとおりに入力します。	[Log] > [Settings]
[LOG.CVPND]	ログ レベルを設定する Cisco VPN デーモン クラスを指定します。	[LOG.CVPND] ここに表記されているとおりに入力します。	[Log] > [Settings]
[LOG.CERT]	ログ レベルを設定する証明書管理クラスを指定します。	[LOG.CERT] ここに表記されているとおりに入力します。	[Log] > [Settings]
[LOG.IPSEC]	ログ レベルを設定する IPsec モジュール クラスを指定します。	[LOG.IPSEC] ここに表記されているとおりに入力します。	[Log] > [Settings]

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
[LOG.FIREWALL] (Windows のみ)	ログ レベルを設定する FWAPI クラスを指定します。	[LOG.FIREWALL] ここに表記されているとおりに入力します。	[Log] > [Settings]
[LOG.CLI]	ログ レベルを設定するコマンドライン インターフェイス クラスを指定します。	[LOG.CLI] ここに表記されているとおりに入力します。	[Log] > [Settings]
[LOG.GUI]	ログ レベルを設定するグラフィカル ユーザ インターフェイス クラスを指定します。	[LOG.GUI] ここに表記されているとおりに入力します。	[Log] > [Settings]
LogLevel=	ロギング サービスを使用する個々のクラスのログ レベルを指定します。デフォルトでは、すべてのクラスのログ レベルは Low です。このパラメータを使用すると、先行する [LOG] パラメータのデフォルト設定を上書きできます。	VPN クライアントは、1（最低）～15（最高）のログ レベルをサポートしています。 デフォルト：1 ログ レベルを設定するには、最初にロギングを有効（**EnableLog=1**）にする必要があります。	[Log] > [Settings]
[CertEnrollment]	証明書登録セクションを表すための必須キーワードです。	[CertEnrollment] ここに表記されているとおりに入力します。	GUI には表示されません。
SubjectName=	この証明書に関連付けるユーザ名を指定します。	519 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
Company=	証明書所有者の会社または組織を指定します。	129 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
Department=	証明書所有者の部署または組織ユニットを指定します。VPN 3000 Concentrator で IPsec グループごとに照合する場合は、設定内のグループ名と一致する必要があります。	129 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
State=	証明書所有者の州または県を指定します。	129 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
Country=	この証明書所有者の国を識別する 2 文字のコードを指定します。	2 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
Email=	証明書所有者の電子メール アドレスを指定します。	129 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
IPAddress	証明書所有者のシステムの IP アドレスを指定します。	ドット付き 10 進表記のインターネット アドレス。	[Certificates] > [Enroll Certificate Enrollment form]

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
Domain	証明書所有者が使用しているホストの完全修飾ドメイン名を指定します。	129 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
CADomainName=	ネットワーク登録用として、認証局が属するドメイン名を指定します。	129 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
CAHostAddress=	認証局の IP アドレスまたはホスト名を指定します。	ドット付き 10 進表記のインターネット ホスト名または IP アドレス。129 文字以下の英数字。	[Certificates] > [Enroll Certificate Enrollment form]
CACertificate=	認証局が発行する自己署名証明書の名前を指定します。	519 文字以下の英数字。 （注）：VPN クライアント GUI では、このパラメータに対する読み取り専用の設定は無視されます。	[Certificates] > [Enroll Certificate Enrollment form]
NetworkProxy= （Windows のみ）	HTTP トラフィックのルーティングに使用できるプロキシ サーバを指定します。ネットワーク プロキシの使用は、プライベート ネットワークへの不正侵入を防ぐのに有効です。	ドット付き 10 進表記の IP アドレスまたはドメイン名。519 文字以下の英数字。プロキシ設定にはポートが関連付けられる場合もあります。 （例：10.10.10.10:8080）。	GUI には表示されません。
[ApplicationLauncher] （Windows のみ）	（VPN クライアント フィールドはなし） アプリケーション ランチャ セクションを表すための必須キーワードです。	[ApplicationLauncher] セクションの先頭のエントリとして、ここに表記されているとおりに入力します。	GUI には表示されません。
Enable= （Windows のみ）	このパラメータを使用すると、VPN クライアント ユーザがプライベート ネットワークへの接続時にアプリケーションを起動できるようにすることができます。	0 = ディセーブル（デフォルト） 1 = イネーブル 無効の場合は起動できません。	[Options] > [Application Launcher]
Command= （Windows のみ）	起動するアプリケーションの名前です。この変数には、コマンドへのパス名、および引数を持つコマンドの名前を指定します。	*コマンド文字列* 512 文字以下の英数字。 例： c:\auth\swtoken.exe.	[Options] > [Application Launcher] > [Application]
[DNS] （Windows のみ）	（VPN クライアント フィールドはなし） DNS セクションを表すための必須キーワードです。	[DNS] セクションの先頭のエントリとして、ここに表記されているとおりに入力します。	GUI には表示されません。

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
AppendOriginalSuffix=（Windows のみ）	VPN クライアントでドメイン名のサフィックスを処理する方法を指定します。この表の後に記載されている「DNS サフィックスと VPN クライアント（Windows Vista、Windows XP、および Windows 2000 のみ）」を参照してください。	0：処理しない 1：VPN Concentrator により付与されるサフィックスにプライマリ DNS サフィックスを追加する。768 ビットは、デフォルト値です。 2：VPN Concentrator により付与されるサフィックスにプライマリ DNS サフィックスおよび接続別 DNS サフィックスを追加します。	GUI には表示されません。
[RadiusSDI]	RADIUS SDI 拡張認証（XAuth）セクションを表すための必須キーワードです。このセクションでは、VPN クライアントで Radius SDI 認証がネイティブの SDI 認証と同様に扱われるよう設定します。これにより、SDI を使用して認証を行う VPN クライアント ユーザにとって認証がより簡単になります。	ここに表記されているとおりに入力します。	GUI には表示されません。
EnableDNSRedirection（Windows のみ、4.8.01.x 以降）	DNS リダイレクトのデフォルト動作を変更できるようにします。	キーワードおよび等号の後に、0 または 1 のいずれかを入力します（例：EnableDNSRedirection=0（スプリット トンネリングに対するデフォルト）） EnableDNSRedirection=1（すべてのトンネルに対するデフォルト）	GUI には表示されません。

QuestionSubStr	質問形式の RADIUS SDI Xauth プロンプトを独自に指定します。	最大 32 バイト長のテキストを入力します。デフォルトのテキストは 1 つの疑問符のみです。
		例：
		`"Are you prepared to have the system generate your PIN?(y/n):"`
		`Response: _____`
			GUI には拡張認証時にこの質問が表示されます。回答用のフィールドも続けて表示されます。

NewPinSubStr	新規 PIN に関する RADIUS SDI Xauth プロンプトを独自に指定します。	最大 32 バイト長のテキストを入力します。デフォルトのテキストは "new PIN" です。 例： `"Enter a new PIN of 4 to 8 digits."`	GUI には拡張認証時に表示されます。

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
NewPasscodeSubStr	新規パスコードに関する RADIUS Xauth プロンプトを独自に指定します。	最大 32 バイト長のテキストを入力します。デフォルトのテキストは "new passcode" です。 例： "PIN accepted. Wait for the token code to change, then enter the new passcode"	GUI には拡張認証時に表示されます。
[Netlogin] (Windows のみ)	vpnclient.ini ファイルの強制ネットワーク ログイン セクションを表します。この機能は、Windows NT、Windows 2000、および Windows XP 上のユーザに対して、キャッシュされているクレデンシャルを使用することなくネットワークからのログアウトとネットワークへの再ログインを強制するためのものです。	ここに表記されているとおりに入力します。これは機能の一部として必要です。	GUI には表示されません。
（注） ユーザがダイヤルアップ（RAS）を介して接続する場合は、Microsoft のドキュメント http://support.microsoft.com/default.aspx?scid=kb;en-us;Q158909 に記載されているレジストリ キーを追加する必要があります。このレジストリ キーを追加すると、ユーザがログオフしても RAS 接続が解除されないようにすることができます。			
Force (Windows のみ)	強制ネットワーク ログイン機能に関する動作内容を指定します。このパラメータはこの機能に必須です。	0 =（デフォルト）ユーザに対してログアウトおよびログインを強制しない。 1 = オプションが選択されていない限り、待機時間を経過した時点でユーザにログアウトを強制する。 2 = オプションが選択されていない限り、待機時間を経過した時点で VPN セッションを解除する。 3 = ユーザが [Connect] または [Disconnect] を選択するまで待機する。	GUI には表示されません。
Wait (Windows のみ)	Force パラメータにより指定された動作を実行するまでの待機秒数を指定します。このパラメータはオプションです。	x 秒。 デフォルトは 5 秒です。	GUI には表示されません。
DefaultMsg (Windows のみ)	Force パラメータにより指定された動作を実行する前に表示するメッセージを指定します。メッセージは、Force の設定に応じて内容を変えることができます。このパラメータはオプションです。	1023 バイト以下の Ascii テキスト。 デフォルトのメッセージ：You will soon be disconnected.	GUI には表示されません。

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
Separator (Windows のみ)	バナー テキストとメッセージとを区切るための分離記号となるテキストを指定します。バナーが存在しない場合、この分離記号は表示されません。このパラメータはオプションです。	511 バイト以下の Ascii テキスト。 デフォルトの分離記号： ----------	GUI には表示されません。
[GUI]	ファイル内でグラフィカル ユーザ インターフェイス アプリケーションの機能を制御するためのセクションを表す必須のキーワードです。	[GUI] セクションの先頭のエントリとして、ここに表記されているとおりに入力します。	GUI には表示されません。
DefaultConnectionEntry	特に指定がない場合に VPN クライアントで接続の開始に使用される接続エントリの名前を指定します。	*ConnectionEntryName*	[Connection Entries] > [Add/Modify] > [Set as default entry]
WindowWidth	ウィンドウの横幅を制御します。	デフォルト = 578 ピクセル	Manual control
WindowHeight	ウィンドウの縦幅を制御します。	デフォルト = 367 ピクセル	Manual control
WindowX	ウィンドウの X 座標を制御します。	0 ～ 1024 ピクセル デフォルト = 324	モニタ画面に対してウィンドウが水平方向に表示される箇所
WindowY	ウィンドウの Y 座標を制御します。	0 ～ 768 ピクセル デフォルト = 112	モニタ画面に対してウィンドウが垂直方向に表示される箇所
VisibleTab	拡張モードのメイン ダイアログに現在表示されているタブ（インデックス）を追跡します。	Connection Entries 証明書 Log	VPN クライアントのメイン ダイアログ
ConnectionAttibute	ステータス バーの表示に関する現在の設定を表します。ステータス バーは、ダイアログの下部にある細長い領域に接続の状態（接続/未接続）が表示され、接続している場合は左側に接続エントリの名前が表示され、右側にはステータスが表示されます。	ステータス バーの右端にある矢印をクリックすると、ステータス バーの右側部分が変化します。この値により、現在の表示に関する選択内容が記録されます。	VPN クライアントのメイン ダイアログ > ステータス バー
AdvancedView	動作について拡張モードと簡易モードとを切り替えます。	簡易モード = 0 拡張モード = 1（デフォルト）	[Main] メニュー > [Options] メニュー > [Advanced/ Simple Mode]
MinimizeOnConnect	VPN 中央サイト デバイスへの接続時にシステム トレイ アイコンを最小化するかどうかを制御します。	0 = 最小化しない 1 = 最小化する（デフォルト）	[Main] メニュー > [Options] > [Preferences] > [Hide upon connect]
UseWindowSettings	ウィンドウ設定を保存するかどうかを制御します。	0 = しない 1 = する（デフォルト）	[Main] メニュー > [Options] > [Preferences] > [Save window settings]

表 5-1　vpnclient.ini ファイルのパラメータ （続き）

.ini パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアント GUI での設定場所
ShowTooltips	ツール チップを表示するかどうかを制御します。	0 = しない 1 = する（デフォルト）	[Main] メニュー > [Options] > [Preferences] > [Enable tooltips]
ShowConnectHistory	接続のネゴシエーション中に接続履歴ダイアログを表示するかどうかを制御します。	0 = しない（デフォルト） 1 = する	[Main] メニュー > [Options] > [Preferences] > [Enable Connection History Display]
AccessibilityOption	508 アクセシビリティ オプションをアクティブ化するかどうかを制御します（Windows のみ）。	0 = しない（デフォルト） 1 = する	[Main] メニュー > [Options] > [Preferences] > [Enable accessibility options]
ShowConnectionTab ShowCertificatesTab ShowLogTab （GUI クライアントのみ、4.8.x）	GUI 上でタブを非表示にできます。	次の例のように、キーワードおよび等号の後に、0 または 1 のいずれかを入力します。 • ShowConnectionTab=1（デフォルト） • ShowConnectionTab=0	GUI には表示されません。
ShowCertTabDelete Show CertTabChangePasswd （GUI クライアントのみ、4.8.x）	GUI でこれらの機能を非表示にすることで、ユーザが誤って証明書を削除したり、証明書パスワードを変更したりするのを防止することができます。	次の例のように、キーワードおよび等号の後に、0 または 1 のいずれかを入力します。 ShowCertTabDelete=1（デフォルト） ShowCertTabDelete=0（証明書削除オプションを非表示にする）	GUI には表示されません。

デジタル証明書を使用した接続

デジタル証明書を使用して VPN クライアント接続エントリを作成するためには、あらかじめ公開キー インフラストラクチャ（PKI）に登録し、認証局（CA）から承認を受けたうえで、1 つまたは複数の証明書を VPN クライアント システム上にインストールしておくことが必要です。これらの作業を行っていない場合は、デジタル証明書を取得する必要があります。Certificate Manager 機能を使用すると直接 PKI に登録してデジタル証明書を取得できるほか、Entrust Entelligence を介して Entrust プロファイルを取得することもできます。現時点でテスト済みの PKI は次のとおりです。

- Baltimore Technologies の UniCERT（www.baltimoretechnologies.com）
- Entrust Technologies の Entrust PKI™ 5.0（www.entrust.com）
- Versign（www.verisign.com）
- RSA KEON 5.7 および 6.0
- Microsoft Certificate Services 2.0

- Cisco Certificate Store

このリストのうちカッコの中に記した Web サイトには、各 PKI から入手できるデジタル証明書についての情報が記載されています。

証明書識別名の照合

Windows プラットフォームおよび Linux プラットフォームでは、プロファイル キーワードである CertMatchDN パラメータを使用して、照合するワイルドカード文字列を指定し、接続の試行時に識別名を基に所定の証明書ストアから特定の証明書を選択します。ワイルドカード文字列が複数の証明書と一致した場合は、そのワイルドカード文字列と最初に一致した証明書が選択されます。このパラメータの値は擬似正規表現で、その書式は VerifyCertDN プロファイル キーワードの書式とまったく同じです。

ワイルドカード文字列に使用できるキーワードは次のとおりです。

- "CN" SubjectCommonName
- "SN" SubjectSurName
- "GN" SubjectGivenName
- "N" SubjectUnstructName
- "I" SubjectInitials
- "GENQ" SubjectGenQualifier
- "DNQ" SubjectDnQualifier
- "C" SubjectCountry
- "L" SubjectCity
- "SP" SubjectState
- "ST" SubjectState
- "O" SubjectCompany
- "OU" SubjectDept
- "T" SubjectTitle
- "EA" SubjectEmailAddr

- "ISSUER-CN" IssuerCommonName
- "ISSUER-SN" IssuerSurName
- "ISSUER-GN" IssuerGivenName
- "ISSUER-N" IssuerUnstructName
- "ISSUER-I" IssuerInitials
- "ISSUER-GENQ" IssuerGenQualifier
- "ISSUER-DNQ" IssuerDnQualifier
- "ISSUER-C" IssuerCountry
- "ISSUER-L" IssuerCity
- "ISSUER-SP" IssuerState
- "ISSUER-ST" IssuerState

- "ISSUER-O" IssuerCompany
- "ISSUER-OU" IssuerDept
- "ISSUER-T" IssuerTitle
- "ISSUER-EA" IssuerEmailAddr

例：

```
CertMatchDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSUER-OU!*"wonderland"
CN="ID Cert"--Specifies an exact match on the CN.
OU*"Cisco"--Specifies any OU that contains the string "Cisco".
ISSUER-CN!"Entrust"--Specifies that the Issuer CN must not equal "Entrust".
ISSUER-OU!*"wonderland"--Specifies that the Issuer OU must not contain "wonderland".
```

証明書キーの用途

Windows、Linux、および Mac の各プラットフォームでは、vpnclient.ini 内の [Main] キーワード配下の CertificateKeyUsage により、全ストアにある証明書のうち使用できるものが、証明書キーの用途に関するパラメータとして Digital Signature または Non-Repudiation が指定されている証明書に制限されます。

クライアントの起動時に「CertificateKeyUsage=1」である場合、[Certificates] タブにはキーの用途が適切な証明書のみ表示されます。さらに、キーの用途が適切でない証明書を使用するようプロファイルが設定されている場合は、証明書が見つからないという内容のエラーが表示されます。

このキーワードのデフォルトは「CertificateKeyUsage=0」で、使用可能なすべての証明書を選択して使用することができます。

このキーワードは、CertMatchDN などその他のあらゆる証明書一致基準に優先します。

証明書キーの用途の照合

Windows プラットフォームおよび Linux プラットフォームの場合、証明書キー用途照合機能では DN やキーの拡張用途に関するフィールドのほか、キーの用途に基づくことによっても証明書のプロファイル選択を行うことができます。このグローバル パラメータでは、全ストアの証明書のうち使用可能なものを、証明書キーの用途に関するパラメータとして Digital Signature または Non-Repudiation が指定されている証明書に制限します。

クライアントの起動時に「CertificateKeyUsage=1」である場合、[Certificates] タブにはキーの用途が適切な証明書のみ表示されます。プロファイルにおいてキーの用途が適切でない場合は、証明書が見つからないという内容のエラーが表示されます。

このキーワードのデフォルトは「CertificateKeyUsage=0」で、使用可能なすべての証明書を選択して使用することができます。この CertificateKeyUsage キーワードは、使用中のプロファイル内で CertMatchKU キーワードによって変更されない限り、CertMatchDN などその他のあらゆる証明書一致基準に優先します。

プロファイル キーワードである CertMatchKU は、vpnclient.ini のキーワード「CertificateKeyUsage」（CSCsc32638）に優先します。

例：

```
CertMatchKU=0,3,4,5

DIGITAL_SIGNATURE  8
NON_REPUDIATION    7
KEY_ENCIPHERMENT   6
DATA_ENCIPHERMENT  5
```

```
KEY_AGREEMENT       4
KEY_CERT_SIGN       3
CRL_SIGN            2
ENCIPHER_ONLY       1
DECIPHER_ONLY       0
```

証明書が [CertMatchKU] フィールドの使用状況のいずれかに一致すると、次の基準に渡されます。いずれの用途とも一致しなかった証明書は選択されません。

次のようなプロファイルに対して、キーの用途以外は同一である 2 つの証明書が使用可能である場合は、Non-Repudiation が指定された証明書のみ選択されます。

```
[Main]
Host=1.2.3.4
AuthType=3
CertStore=2
CertName=myMultipleCerts
CertMatchKU=7
!CertSubjectName=
!CertSerialHash=
```

拡張証明書キーの用途の照合

プロファイル キーワードである CertMatchEKU パラメータには、VPN クライアントが準拠すべきキーの拡張用途に関するフィールドのリストを指定します。このプロファイル キーワードが指定されている場合、接続の試行時に VPN クライアントで認識されるのは、キーの拡張用途に関するフィールドが、プロファイルのキーワードで指定されているフィールドと一致する証明書のみです。つまり、このプロファイル キーワードが指定されている場合は、いずれの証明書についても、プロファイル キーワードに指定されたキーの拡張用途に関するフィールドのうち少なくとも 1 つが、証明書のキーの拡張用途に関するフィールドに指定されている必要があります。

このキーワードは、接続の試行に対してのみ適用され、証明書に関するその他の動作（証明書のリスト表示、証明書の内容表示など）には適用されません。このキーワードは、あらゆる基準による証明書選択（CertSerialHash、CertMatchDN、CertSubjectName、CertName など）に適用されます。このはーワードの値は、キーの拡張用途 OID 文字列で構成されるカンマ区切りのリストです。カスタムのキーの拡張用途文字列は、1.3.6.1.5.5.7.3.n という書式にする必要があります。n は任意の数字です。

例：

```
CertMatchEKU=1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.1
```

それぞれの説明は次のとおりです。

1.3.6.1.5.5.7.3.2：クライアント認証

1.3.6.1.5.5.7.3.1：サーバ認証

証明書が見つからない場合

この場合の処理は暗黙的に行われ、それに関連付けられるプロファイル キーワードはありません。各接続試行に対しては、次のキーワード（優先順に記載）の中から 1 つまたは複数を使用して証明書を選択できます。

1. CertSerialHash
2. CertMatchDN
3. CertSubjectName
4. CertName

VPN クライアントにおいて、上記すべての証明書キーワードを使用しても所定の証明書ストアから証明書が見つからない場合、その接続試行は失敗します。

以下にプロファイルのサンプルを示します。

```
[Main]
Host=10.10.10.10
AuthType=3
CertStore=2
!UserName=
!UserPassword=
CertMatchDN=issuer-ou*"vpn group",ea*"Cisco.com"
!CertSerialHash=
```

このプロファイルに一致するのは、キーの用途が「Non-Repudiation」であり、かつキーの拡張用途がクライアント認証またはサーバ認証の*いずれか*である証明書に限ります。Issuer-ou フィールドには "vpn group" を指定することが*必要*であり、ユーザ証明書の電子メール アドレスには "cisco.com"（大文字と小文字は区別される）が指定されている*必要*があります。

Windows 環境の場合（Linux および Mac 用の VPN クライアントではスマート カードをサポートしていない）、前記のシナリオでは共用のワークステーションからでもスマート カード証明書に基づいてユーザを接続することができます。ユーザは移動した先でスマート カードを挿入し、[Connect] をクリックします。この汎用プロファイルを使用すると、（クライアントのリスタートやプロファイルの修正を行うことなく）カード上で適切な証明書が検索され、ユーザに対してそれぞれの証明書パスワード、ユーザ名、およびパスワードに関するプロンプトが表示されます。また、ユーザ名を使用することなく接続し証明書のみを使用して認証が行われるよう、セキュア ゲートウェイを設定することもできます。

（注） プロファイル内で文字「!」を使用すると、接続間で以前のユーザ情報が維持されないようにすることができます。

証明書照合では、使用可能な証明書のうち証明書照合に対して設定されたルールに最初に適合したものが一致対象となります。ただしその有効性は問われないため、接続失敗の原因になることがあります。有効な証明書が使用可能な場合に、失効した証明書が選択されないようにするため、Windows 用の VPN クライアントでは現在、証明書ストア内にある無効な証明書および失効した証明書は無視されるようになっています。（CSCsd38373、CSCsd38360）。

CertSerialHash の使用に関する重要な注意事項

以下に示すのは、DN などの一致基準を使用して証明書を検索する例です。

```
CertMatchDN=CN*"User"
!CertSerialHash=
```

この場合、CertSerialHash キーワードは直前に感嘆符（!）があることにより読み取り専用フィールドとなっているため、クライアントでは連続ハッシュ値を更新できません。正しい連続ハッシュがないと、クライアントではウォッチ タイマーを作成してスマート カードが存在するかどうかを検証することができません。

「!CertSerialHash=」がない場合、クライアントではストア内の証明書により証明書ハッシュが更新され、次の行がプロファイルに追加されます。

```
CertSerialHash=...03CF...
```

プロファイル内に「CertSerialHash=0102...xyz」などの連続ハッシュ値がすでに存在する場合、DN に一致する別の証明書の入った別のスマートカードを使用すると、スマートカード ウォッチも開始され、IPsec では CertSerialHash パラメータの連続ハッシュ値が、使用している証明書の連続ハッシュ値に更新されます。

（注） この状況では、VPN クライアントで連続ハッシュ値を目的の証明書に合わせて更新できるようにする必要があるため、「CertSerialHash=」の前に「!」を挿入*しない*ことが重要です。

デフォルトのユーザ プロファイルの作成と使用方法

VPN クライアント GUI のデフォルト接続エントリ機能と同じものであるデフォルトのユーザ プロファイルを設定することができます（『*VPN Client User Guide for Windows*』の第 4 章「Setting a Default Connection Entry」または『*VPN Client User Guide for Mac OS X*』の第 5 章「Connecting to a Default Connection Entry」を参照）。デフォルトのユーザ プロファイルの名前は、VPN クライアントの .ini ファイルにある DefaultConnectionEntry パラメータに指定します。さらに、接続オープン機能を使用すると、セキュア ゲートウェイへの接続時にデフォルトのユーザ プロファイルに接続するよう VPN クライアントを設定することができます。vpnclient.ini ファイル内のパラメータを使用してこの設定をアクティブにする手順は次のとおりです。

ステップ 1　DefaultConnectionEntry パラメータにデフォルトの接続エントリの名前を指定します（`DefaultConnectionEntry=myprofile` など）。

ステップ 2　ConnectOnOpen パラメータを有効にします（`ConnectOnOpen=1`）。

DNS サフィックスと VPN クライアント（Windows Vista、Windows XP、および Windows 2000 のみ）

ping server123 などのコマンドまたはプログラムから Windows Vista プラットフォーム、Windows XP プラットフォーム、または Windows 2000 プラットフォームへサフィックスのないホスト名が渡された場合、Windows オペレーティング システムでは、その名前を完全修飾ドメイン名（FQDN）に変換する必要があります。Windows オペレーティング システムには、ドメイン名にサフィックスを付加する方式が 2 種類あります（方式 1 と方式 2）。ここでは、これら 2 つの方式について説明します。

方式 1：プライマリ DNS サフィックスと接続別 DNS サフィックス

プライマリ DNS サフィックスは、すべてのアダプタでグローバルに使用されます。接続別 DNS サフィックスは、特定の接続（アダプタ）でのみ使用されます。これにより、接続ごとに異なる DNS サフィックスを使用することができます。

プライマリ DNS サフィックスの識別

プライマリ サフィックスは、コンピュータ名に基づいて生成されます。プライマリ DNS サフィックスの検索または割り当てを行う手順（オペレーティング システム別）は次のとおりです

Windows 2000 の場合

ステップ 1　Windows 2000 デスクトップ上で、[My Computer] アイコンを右クリックし、メニューから [Properties] を選択します。

[System Properties] ダイアログが表示されます。

ステップ 2　[Network Identification] タブを開きます。

この画面の [Full Computer Name] の横にあるエントリが、コンピュータの名前と DNS サフィックスを表します（SILVER-W2KP.tango.dance.com など）。最初のドットから後ろの部分がプライマリ DNS サフィックスです（この例では tango.dance.com）。

ステップ 3　プライマリ DNS サフィックスを変更する場合は、[Network Identification] タブの [Properties] をクリックします。

[Identification Changes] ダイアログが表示されます。

ステップ 4　[More...] をクリックします。

この操作により [DNS Suffix and Net BIOS Computer Name] ダイアログが表示されます。エントリ *Primary DNS suffix of this computer* は、プライマリ サフィックスを表します。このエントリは編集することができます。

Windows XP の場合

ステップ 1　[My Computer] をクリックし、メニューから [Properties] を選択します。

[System Properties] ダイアログが表示されます。

ステップ 2　[Computer Name] タブを開きます。

この画面の [Full Computer Name] の横にあるエントリが、コンピュータの名前と DNS サフィックスを表します（SILVER-W2KP.tango.dance.com など）。最初のドットから後ろの部分がプライマリ DNS サフィックスです（この例では tango.dance.com）。

ステップ 3　プライマリ DNS サフィックスを変更する場合は、[Computer Name] タブで [Change] をクリックします。

[Computer Name Changes] ダイアログが表示されます。

ステップ 4　[More...] をクリックします。

この操作により [DNS Suffix and Net BIOS Computer Name] ダイアログが表示されます。エントリ Primary DNS suffix of this computer は、プライマリ サフィックスを表します。このエントリは編集することができます。

接続別 DNS サフィックスの識別

接続別 DNS サフィックスは、2 種類の方法で識別できます。

1. 接続別 DNS サフィックスの値は、選択された接続に対する DNS サフィックスとして [Advanced TCP/IP Settings] ダイアログにリスト表示されます。

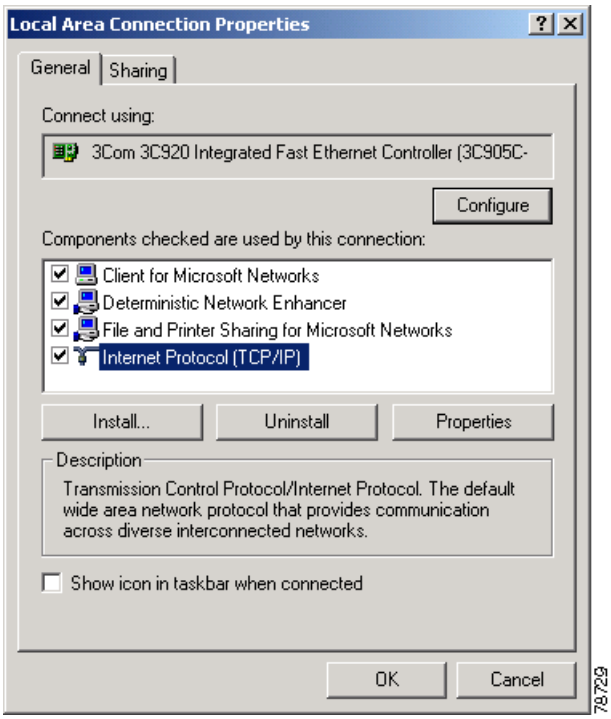
（注）　以下に示すのは、Windows 2000 プラットフォーム用の手順です。Windows XP プラットフォームでは若干異なる場合があります。

[Advanced TCP/IP Settings] ダイアログを表示する手順は次のとおりです。

ステップ 1　[My Network Places] アイコンを右クリックして [Properties] ダイアログを表示します。このダイアログには接続のリストが表示されます。

ステップ 2　いずれかの接続（local など）をダブルクリックし、その [Properties] ダイアログを表示します。図 5-1 には Local Area Connection という接続のコンポーネントが表示されていますが、接続には、ここにあるようなチェックボックスがオンになっているコンポーネントが使用されます。

図 5-1　接続に関するプロパティの表示



ステップ 3　[Internet Protocol (TCP/IP)] をダブルクリックして、そのプロパティを表示します。

ステップ 4　[Advanced] を選択します。

ステップ 5　[DNS] タブを表示し、[DNS suffix for this connection] ボックスを確認します。このボックスが空の場合は、DHCP サーバによる割り当てを受けることができます。

a. DHCP サーバにより割り当てられた接続別サフィックスを識別する場合は、**ipconfig /all** コマンド（下記の代替手段 2）および DNS サーバ アドレスを使用します。

2. コマンドライン プロンプトから **ipconfig /all** を実行すると、その出力に接続別 DNS 値がリスト表示されます。DNS サフィックス検索リスト については、[Windows 2000 IP Configuration] で確認してください。接続別 DNS サフィックス については、[Ethernet Adapter Connection Name] で確認してください。

方式 2：ユーザ定義の DNS サフィックス

この方式では、ユーザが個別にサフィックスを定義できます。サフィックスの表示および変更は、接続プロパティ ページの [DNS] タブで行えます。[Append these DNS suffixes (in order)] 編集ボックスには、編集可能な名前が表示されます。ここに入力した値は、すべてのアダプタでグローバルに使用されます。

VPN クライアントの動作

VPN クライアントでは、VPN 中央デバイス（VPN 3000 Concentrator など）への VPN トンネルが確立された場合、Windows プラットフォームで使用されている方式にかかわらず、方式 2 が使用されます。Windows プラットフォームで方式 2 が使用されている場合、VPN クライアントでは VPN 中央デバイスにより用意されたサフィックスが追加されます。これはデフォルトの動作であり、問題なく正常に実行されます。

ただし Windows で方式 1 が使用されている場合、VPN クライアントでは、プライマリ サフィックスや接続別サフィックスは追加されません。この問題は、vpnclient.ini ファイルで AppendOriginalSuffix オプションを設定すると解決できます。表 5-1 では、[DNS] セクションにこのオプションが含まれています。

[DNS]

AppendOriginalSuffix=1:

この場合 VPN クライアントでは、VPN Concentrator により用意されたサフィックスに、プライマリ DNS サフィックスが追加されます。トンネルが確立されている間 Windows には、VPN Concentrator により用意されたサフィックスとプライマリ DNS サフィックスという 2 つのサフィックスが存在することになります。

AppendOriginalSuffix=2:

この場合 VPN クライアントでは、VPN Concentrator により用意されたサフィックスに、プライマリ DNS サフィックスと接続別 DNS サフィックスが追加されます。トンネルが確立されている間 Windows には、VPN Concentrator により用意されたサフィックス、プライマリ DNS サフィックス、接続別 DNS サフィックスという 3 つのサフィックスが存在することになります。

（注） Windows で方式 2 が使用されている場合は、これらの値を vpnclient.ini ファイルに追加しても効力はありません。

VPN クライアントでは、トンネルが確立されるたびにこれらの値が設定され、トンネルが切断された時点で元の設定が回復されます。

RADIUS SDI 拡張認証の設定

VPN クライアントでは RADIUS SDI 認証が、よりシームレスで簡単に使用できる「ネイティブ」の SDI 認証と同様に扱われるよう設定することができます。この設定を行うと、ユーザは RSA SecurID ソフトウェア インターフェイスを使用する必要がなくなります。これは、VPN クライアント ソフトウェアが RSA SecurID ソフトウェアと直接連動するためです。

RADIUS SDI 認証の自動処理を有効にするためには、プロファイル（.pcf）パラメータを 1 つ設定する必要があるほか、場合によってはさらに 3 つのグローバル（vpnclient.ini）パラメータを設定することも必要です。

- vpnclient.ini ファイルには、次の情報を入力します。（これらのパラメータに関する詳細については、表 5-1 を参照してください）。
  - RadiusSDI：RADIUS SDI の設定セクションを表します。
  - 質問プロンプトを指定するための質問のサブ文字列（「?」など）。
  - 新規 PIN に関するプロンプトを指定するための新規 PIN のサブ文字列。
  - 新規パスコードに関するプロンプトを指定するための新規パスコードのサブ文字列。

- プロファイル（接続エントリ）ファイルの Main セクションに、パラメータ「RadiusSDI = 1」を入力します。（表 5-2 を参照）。

これにより、VPN クライアントでは要求が到達した場合、それが RADIUS SDI 拡張認証要求と見なされ、その要求が既知の方法で処理されます。

接続プロファイルの作成

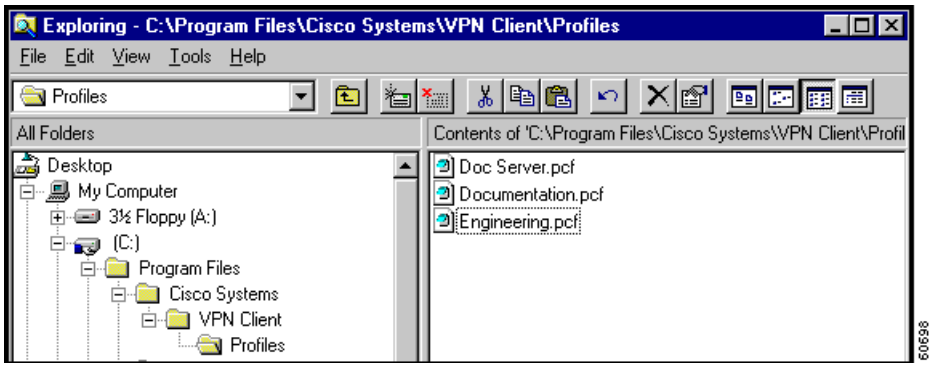
VPN クライアントで使用されるパラメータは、プライベート ネットワークのリモート ユーザごとに個別に設定する必要があります。これらのパラメータをまとめて、ユーザ プロファイルが構成されます。これは、VPN クライアント ユーザのローカル ファイル システムにある以下のディレクトリ配下のプロファイル コンフィギュレーション ファイル（.pcf ファイル）に記述されます。

- Windows プラットフォームの場合：Program Files¥Cisco Systems¥VPN Client¥Profiles（ソフトウェアがデフォルトの場所にインストールされている場合）
- Linux プラットフォーム、Solaris プラットフォーム、および Mac OS X プラットフォームの場合：/etc/CiscoSystemsVPNClient/Profiles/

これらのパラメータでは、数ある機能や要件のうち、使用される認証のタイプ、リモート サーバ アドレス、IPsec グループの名前およびパスワード、ログ ファイルの使用、バックアップ サーバの使用、ダイヤルアップ ネットワーキングを介した自動インターネット接続を指定します。各接続エントリには、個別の .pcf ファイルが使用されます。たとえば、Doc Server、Documentation、Engineering という 3 つの接続エントリがある場合、Profiles ディレクトリには .pcf ファイルのリストが表示されます。

図 5-2 は、Windows プラットフォームにおけるユーザ プロファイルのディレクトリ構造を示したものです。

図 5-2　　.pcf ファイルのリスト



接続ファイルで制御される機能

接続プロファイル（.pcf ファイル）では、すべてのプラットフォームにおける次のような機能を制御します。

- 接続プロファイルの説明
- リモート サーバのアドレス
- 認証タイプ
- リモート ユーザが属する IPsec グループの名前

- グループのパスワード
- ダイヤルアップ ネットワーキングを介したインターネットへの接続
- リモート ユーザの名前
- リモート ユーザのパスワード
- バックアップ サーバ
- スプリット DNS
- ダイヤルアップ ネットワーキング接続のタイプ
- トランスペアレント トンネリング
- TCP トンネリング ポート
- ローカル LAN アクセスの許可
- IKE キープアライブおよび ESP キープアライブの有効化
- ピアの応答タイムアウトの設定
- 証明書接続用の証明書パラメータ
- 証明書チェーンの設定
- Diffie-Hellman グループ
- ピア証明書の DN の検証
- RADIUS SDI 拡張認証の設定
- SDI ハードウェア トークン使用の設定
- スプリット DNS の設定
- レガシー IKE ポート使用の設定

接続プロファイル（.pcf ファイル）では、Windows プラットフォームにおける次のような追加機能を制御します。

- Microsoft 用のダイヤルアップ ネットワーキング電話帳エントリ
- ISP 経由の接続に使用するコマンド文字列
- NT ドメイン
- Microsoft ネットワークへのログインと証明書
- デフォルト IKE ポートの 500/4500 からの変更（明示的に追加することが必要）
- Windows NT、Windows 2000、および Windows XP 上のユーザに対して、キャッシュされているクレデンシャルを使用することなくネットワークからのログアウトとネットワークへの再ログインを強制する強制ネットワーク ログインの有効化
- すべての接続タイプを対象とした VPN クライアント上のブラウザ プロキシ設定の有効化 / 無効化

.pcf ファイルのサンプル

（注）　VPN クライアント用の接続プロファイルは、プラットフォーム間で互換性があります。Windows プラットフォームに固有のキーワードは、その他のプラットフォームでは無視されます。

次に示す .pcf プロファイルのサンプルは、事前共有キーを使用した接続エントリです。ただし、プレフィクス enc_（enc_GroupPwd など）は、このパラメータの値が暗号化されていること、および VPN クライアントによって書き込まれることを表します。

```
[main]
Description=connection to TechPubs server
Host=10.10.99.30
AuthType=1
GroupName=docusers
GroupPwd=
enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C851ECF2DCC8BD488857EFA
FDE1397A95E01910CABECCE4E040B7A77BF
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=alice
SaveUserPassword=0
UserPassword=
enc_UserPassword=
NTDomain=
EnableBackup=1
BackupServer=Engineering1, Engineering2, Engineering 3, Engineering4
EnableMSLogon=0
MSLogonType=0
EnableNat=1
EnableLocalLAN=0
TunnelingMode=0
TCPTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName
SendCertChain=0
VerifyCertDN=CN=”ID Cert”,OU*”Cisco”,ISSUER-CN!=”Entrust”,ISSURE-OU!*”wonderland”
DHGroup=2
PeerTimeOut=90
ForceNetLogin=1
```

接続エントリごとにプロファイル コンフィギュレーション ファイルを作成することにより VPN クライアントでリモート ユーザに関する設定を行い、VPN クライアント ソフトウェアで .pcf ファイルを配布することができます。これらのコンフィギュレーション ファイルには、すべてのパラメータ設定を記述することもその一部のみを記述することもできます。ユーザが設定する必要があるのは、これらのうち未設定のものです。

また、コンフィギュレーション ファイルを使用することなく VPN クライアントをユーザに配布し、各ユーザが独自に設定を行うこともできます。この場合、VPN クライアント プログラムを使用して設定を完了した時点で、実質的には接続エントリごとに、編集および共有できる .pcf ファイルを作成したことになります。

システムのセキュリティを保護するため、リモート ユーザ用の .pcf ファイルには、IPsec グループのパスワード、認証ユーザ名、認証パスワードなどの重要なセキュリティ パラメータを記述*しない*ことが推奨されます。

（注）　どのような事前設定を行った場合でも、ユーザに対しては VPN クライアントの設定に必要な情報を提供する必要があります。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「Gathering Information You Need」を参照してください。

接続プロファイル用 .pcf ファイルの作成

ユーザにはそれぞれ、独自のコンフィギュレーション ファイルが必要です。各ファイルの作成および編集には、メモ帳などの ASCII テキスト エディタを使用します。書式設定のないテキストのみのファイルとして保存してください。

接続プロファイルの名前指定

Windows プラットフォームでは、スペースが含まれたプロファイル名を作成できます。ただし、プロファイルを他のプラットフォーム（Linux、Mac OS X、または Solaris）に配布する場合は、名前にスペースを使用することはできません。

接続プロファイルの設定パラメータ

表 5-2 は、すべてのパラメータ、キーワード、および値を表にまとめたものです。また、キーワードに対応する VPN クライアント パラメータ名（存在する場合）および VPN クライアント GUI での設定場所も記載されています。

各パラメータの設定は、特に指定がない限り、すべての VPN クライアント プラットフォーム上で行うことができます。

表 5-2　.pcf ファイルのパラメータ

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
`[main]`	（VPN クライアント フィールドはなし） メイン セクションを表すための必須キーワードです。	`[main]` ファイルの先頭のエントリとして、ここに表記されているとおりに入力します。	GUI には表示されません。
`Description=`	説明 この接続エントリについて説明した 1 行のテキスト。任意。	任意のテキスト。 246 文字以下の英数字。	[Connection Entry] > [New/Modify]
`Host=`	リモート サーバのアドレス リモート ユーザが接続するシスコのリモート アクセス サーバ（VPN 中央サイト デバイス）のホスト名または IP アドレス。	ドット付き 10 進表記のインターネット ホスト名または IP アドレス。 255 文字以下の英数字。	[Connection Entry] > [New/Modify]

表 5-2　.pcf ファイルのパラメータ （続き）

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
AuthType=	認証タイプ 認証および認証タイプの詳細については、ご使用のプラットフォームに対応する VPN クライアントのユーザ ガイドを参照してください。	このユーザの認証タイプ。 1 = 事前共有キー（デフォルト） 3 = RSA シグニチャを使用したデジタル証明書。 5 = 相互認証（下記の注を参照）	[Connection Entry] > [New/Modify] > [Authentication]

（注） ユーザ用に相互認証またはハイブリッド認証の設定について
この認証方式を使用するには、VPN クライアント システムにインストールされているルート証明書と一致するルート証明書（相互信頼が生じるためには双方で使用されているクレデンシャルが一致することが必要）から派生した ID 証明書が VPN 中央サイト デバイスにインストールされている必要があります。インストール時にルート証明書をリモート ユーザに配布する方法については、ご使用のプラットフォームに対応するユーザ ガイドのインストールに関する項を参照してください。VPN Concentrator の設定情報については、「相互グループ認証の設定」（P.1-13）を参照してください。

GroupName=	グループ名 このユーザが属する IPsec グループの名前。事前共有キーと共に使用します。	VPN 中央サイト デバイスで設定された IPsec グループの正確な名前。 32 文字以下の英数字。大文字と小文字は区別されます。	[Connection Entry] > [New/Modify] > [Authentication]
GroupPwd=	グループのパスワード このユーザが属する IPsec グループのパスワード。事前共有キーと共に使用します。 このパスワードは、VPN クライアントでの初回読み込み時に、暗号化されたパスワード（enc_GroupPwd）に置き換えられます。	VPN 中央サイト デバイスで設定された IPsec グループの正確なパスワード。 4 文字以上 32 文字以下の英数字。大文字と小文字が区別されるクリア テキスト。	[Connection Entry] > [New/Modify] > [Authentication]
encGroupPwd=	このユーザが属する IPsec グループのパスワード。事前共有キーと共に使用します。これは、GroupPwd の暗号化バージョンです。	英数字として表現されたバイナリ データ。	GUI には表示されません。
EnableISPConnect=（Windows のみ）	ダイヤルアップ ネットワーキングを介したインターネットへの接続 VPN クライアントが、IPsec 接続を開始する前に ISP へ自動で接続するかどうかを指定します。これにより PppType パラメータを使用するかどうかが決まります。	0 = ディセーブル（デフォルト） 1 = イネーブル VPN クライアント GUI では、このパラメータに対する読み取り専用の設定は無視されます。	[Connection Entry] > [New/Modify] >[Dial-Up] > [Connect to the Internet via dial-up]

表 5-2　.pcf ファイルのパラメータ （続き）

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
ISPConnectType=（Windows のみ）	ダイヤルアップ ネットワーキング接続エントリのタイプ 使用するタイプとして ISPConnect または ISPCommand を指定します。	0 = ISPConnect（デフォルト） 1 = ISPCommand VPN クライアント GUI では、このパラメータに対する読み取り専用の設定は無視されます。	[Connection Entry] > [New/Modify] > [Dial-Up] > （[DUN] または [Third Party]（コマンド）のいずれかを選択）
ISPConnect=（Windows のみ）	ダイヤルアップ ネットワーキング電話帳エントリ（Microsoft） このパラメータを使用すると、Microsoft ネットワークにダイヤルすることができます。ダイヤル先となるのは、ユーザの接続に対して指定されたダイヤルアップ ネットワーキング電話帳エントリです。 EnableISPconnect=1 および ISPConnectType=0 の場合にのみ適用されます。	*phonebook_name* この変数には、DUN に対する電話帳エントリの名前として、256 文字以下の英数字を指定します。 VPN クライアント GUI では、このパラメータに対する読み取り専用の設定は無視されます。	[Connection Entry] > [New/Modify] > [Dial-Up] > [Microsoft Dial-Up Networking] > [Phonebook]
ISPCommand=（Windows のみ）	ダイヤルアップ ネットワーキング電話帳エントリ（コマンド） このパラメータを使用すると、ユーザの ISP ダイヤラにダイヤルするためのコマンドを指定できます。 EnableISPconnect=1 および ISPConnectType=1 の場合にのみ適用されます。	*コマンド文字列* この変数には、次の例のように、コマンドへのパス名、および引数を持つコマンドの名前を指定します。 `c:\isp\ispdialer.exe dialEngineering` 512 文字以下の英数字。	[Connection Entry] > [New/Modify] > [Dial-Up] > [Third party dialup program] > [Application]
Username=	ユーザ認証：ユーザ名 GroupName に指定されている IPsec グループの有効なメンバとしてユーザを認証するための名前。	正確なユーザ名。32 文字以下のクリア テキストで、大文字と小文字は区別されます。 VPN クライアントではユーザ認証の際、ユーザに対してこの値に関するプロンプトが表示されます。	[Connection Entry] > [New/Modify] > [Authentication]

表 5-2　.pcf ファイルのパラメータ （続き）

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
UserPassword=	ユーザ認証：パスワード 拡張認証の際に使用するパスワード。 このパスワードは、VPN クライアントでの初回読み込み時に enc_UserPassword としてファイルに保存され、クリア テキスト バージョンは削除されます。SaveUserPassword が無効の場合、VPN クライアントでは UserPassword が削除され、暗号化バージョンは作成されません。 プロファイルを管理するための GUI インターフェイスがない場合、このパラメータの修正は手動でのみ行ってください。	32 文字以下の英数字で、大文字と小文字は区別されます。	[Connection Entry] > [New/Modify] > [Authentication]
encUserPassword	ユーザ パスワードの暗号化バージョン。	英数字として表現されたバイナリ データ。	GUI には表示されません。
SaveUserPassword	プロファイルの中でユーザ パスワードまたはその暗号化バージョンを有効にするかどうかを指定します。 この値は、VPN 中央サイト デバイスからプッシュされます。	0 =（デフォルト）ユーザがパスワード情報をローカルに保存できないようにする。 1 = ユーザがパスワードをローカルに保存できるようにする。	GUI には表示されません。
NTDomain= (Windows のみ)	ユーザ認証：ドメイン ユーザの IPsec グループに対して設定された NT ドメイン名。Windows NT ドメイン サーバを介したユーザ認証に対してのみ適用されます。	NT ドメイン名。14 文字以下の英数字。アンダーバーは使用できません。	[Connection Entry] > [New/Modify]
EnableBackup=	バックアップ サーバの有効化 プライマリ サーバが使用できない場合にバックアップ サーバを使用するかどうかを指定します。	0 = ディセーブル（デフォルト） 1 = イネーブル	[Connection Entry] > [New/Modify] > [Backup Servers]
BackupServer=	(バックアップ サーバ リスト) バックアップ サーバのホストアドレスまたは IP アドレスのリスト。 EnableBackup=1 の場合のみ適用されます。	ドット付き 10 進表記による正規のインターネット ホスト名または IP アドレス。エントリが複数の場合はカンマで区切ります。長さは 255 文字以内です。	[Connection Entry] > [New/Modify] > [Backup Servers]

表 5-2　.pcf ファイルのパラメータ （続き）

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
EnableMSLogon=（Windows のみ）	Microsoft ネットワークへのログイン ユーザが Microsoft ネットワークへログインするよう指定します。 Windows 9x が実行されているシステムに対してのみ適用されます。	0 = ディセーブル 1 = イネーブル（デフォルト）	[Connection Entry] > [New/Modify] > [Microsoft Logon] Windows 98 および Windows ME でのみ使用できます。
MSLogonType=（Windows のみ）	デフォルトのシステム ログイン クレデンシャルを使用。 ネットワーク ログイン クレデンシャルに関するプロンプトを表示。 ユーザがログインに使用する Windows のユーザ名およびパスワードを Microsoft ネットワークが受け入れるかどうか、または Microsoft ネットワークによりユーザ名およびパスワードに関するプロンプトを表示するかどうかを指定します。 EnableMSLogon=1 の場合のみ適用されます。	0 =（デフォルト）システム ログイン クレデンシャルを使用する。つまり、Windows のログイン用のユーザ名およびパスワードを使用する。 1 = ネットワークのログイン用のユーザ名およびパスワードに関するプロンプトを表示する。	[Connection Entry] > [New/Modify] > [Microsoft Logon] Windows 98 および Windows ME でのみ使用できます。
EnableNat=	トランスペアレント トンネリングの有効化 ファイアウォールとして機能するルータを介した VPN クライアントとセキュア ゲートウェイとの間のセキュアな転送を許可します。この場合 NAT または PAT を実行することも可能です。	0 = ディセーブル 1 = イネーブル（デフォルト）	[Connection Entry] > [New/Modify] > [Transport]
TunnelingMode=	UDP 上または TCP 上でのトランスペアレント トンネリングのモードを指定します。接続に使用しているセキュア ゲートウェイでのモードと一致する必要があります。	0 = UDP（デフォルト） 1 = TCP	[Connection Entry] > [New/Modify] > [Transport]
TCPTunnelingPort=	TCP ポート番号を指定します。セキュア ゲートウェイで設定されたポート番号と一致する必要があります。	1 ～ 65545 のポート番号。 デフォルト = 10000	[Connection Entry] > [New/Modify] > [Transport]
EnableLocalLAN=	ローカル LAN アクセスを許可 セキュア ゲートウェイを介して中央サイトの VPN デバイスに接続中、クライアント サイトのローカル LAN 上にあるリソースにアクセスできるようにするかどうかを指定します。	0 = ディセーブル（デフォルト） 1 = イネーブル	[Connection Entry] > [New/Modify] > [Transport]

表 5-2　.pcf ファイルのパラメータ （続き）

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
PeerTimeout=	ピアの応答タイムアウト トンネルの接続先である VPN 中央サイト デバイスが応答しない場合に、接続の終了を待機する秒数。	秒数 最小 = 30 秒 最大 = 480 秒 デフォルト = 90 秒	[Connection Entry] > [New/Modify] > [Transport]
CertStore=	証明書のストア 設定済みの証明書を格納するストアのタイプを指定します。	0 = 証明書なし（デフォルト） 1 = Cisco 2 = Microsoft VPN クライアント GUI では、このパラメータに対する読み取り専用（!）の設定は無視されます。（注を参照）。	Windows GUI GUI には表示されません。[Certificates] タブで確認できます。 Mac OS X GUI [Connection Entry] > [New/Modify] > [Transport]

（注）　通常、パラメータが読み取り専用に指定されている場合は、GUI でチェックボックスがオフまたは編集ボックスが無効になるため、ユーザがパラメータの値を変更することはできません。ただしこのことは、Certificate パラメータには当てはまりません。これらの値をファイル内で上書きすることはできません。ユーザは GUI 画面でこれらを変更することができますが、その変更内容は保存されません。

CertName=	証明書名 VPN 中央サイト デバイスへの接続に使用する証明書を指定します。	129 文字以下の英数字。 VPN クライアント GUI では、このパラメータに対する読み取り専用の設定は無視されます。	[Certificates] > [View]
CertPath=	証明書ファイルが格納されているディレクトリの絶対パス名。	259 文字以下の英数字。 VPN クライアント GUI では、このパラメータに対する読み取り専用の設定は無視されます。	[Certificates] > [Import]
CertSubjectName	証明書の所有者の完全修飾識別名（DN）。もし存在すれば、VPN ダイヤラではこのパラメータの値が入力されます。	このパラメータは、指定しないか空のままにするかのどちらかにしてください。 VPN クライアント GUI では、このパラメータに対する読み取り専用の設定は無視されます。	[Certificates] > [View]
CertSerialHash	証明書の全内容のハッシュ。これは証明書の信頼性を検証する手段となるものです。もし存在すれば、VPN ダイヤラではこのパラメータの値が入力されます。	このパラメータは、指定しないか空のままにするかのどちらかにしてください。 VPN クライアント GUI では、このパラメータに対する読み取り専用の設定は無視されます。	[Certificates] > [View]

表 5-2　.pcf ファイルのパラメータ （続き）

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
（注） ソフトウェアでは、証明書認証の処理を行う際、次のフィールド（優先順に記載）が使用されます。 CertSerialHash CertSubjName CertName 同じ DN または CN を持つ証明書が 2 つ存在する場合、ソフトウェアでは最初の証明書が選択されます。			
SendCertChain	ID 証明書の検証を行うため、ルート証明書と ID 証明書との間の CA 証明書チェーン、および ID 証明書をピアへ送信します。	0 = ディセーブル（デフォルト） 1 = イネーブル	• [Connection Entry] > [New/Modify] • [Certificates] >[Export]
VerifyCertDN	不正に入手した有効な証明書または IP アドレスを使用してユーザが有効なゲートウェイに接続できないようにします。ピア証明書のドメイン名を検証しようとして失敗した場合は、クライアント接続も失敗します。	サブジェクトと発行元の両方の証明書 DN 値を指定します。 **-_@<>().,** およびワイルドカードを含むすべての有効な ASCII 文字を使用できます。以下の例を参照してください。	GUI には表示されません。
例：VerifyCertDN=CN=”ID Cert”,OU*”Cisco”,ISSUER-CN!=”Entrust”,ISSUER-OU!*”wonderland” *CN=”ID Cert”*—Specifies an exact match on the CN. *OU*”Cisco”*—Specifies any OU that contains the string “*Cisco*”. *ISSUER-CN!”Entrust”*—Specifies that the Issuer CN must not equal “*Entrust*”. *ISSUER-OU!*”wonderland”*—Specifies that the Issuer OU must not contain “*wonderland*”.			
DHGroup	Diffie- Hellman キー ペアの生成に使用する VPN デバイス上で、ネットワーク管理者がデフォルトのグループ値を上書きできるようにします。	1 = modp group 1 2 = modp group 2（デフォルト） 5 = modp group 5 （注）この値は事前共有キーに対してのみ事前設定されます。証明書により認証された接続の場合は、DHGroup 番号のネゴシエートが行われます。	GUI には表示されません。
RadiusSDI	VPN クライアントにおいて、拡張認証（XAuth）に Radius SDI が使用されていると見なされるよう指定します。	0 = しない（デフォルト） 1 = する	このパラメータを有効にした場合、SDI 認証に関する GUI のプロンプトは Radius SDI から表示され、vpnclient.ini ファイル内のパラメータを使用して設定されます。
SDIUseHardwareToken	接続エントリで RSA SoftID ソフトウェアが使用されないようにします。	0 = RSA SoftID を使用する（デフォルト） 1 = PC 上にインストールされている RSA SoftID ソフトウェアを無視する。	GUI には表示されません。

表 5-2　.pcf ファイルのパラメータ （続き）

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
EnableSplitDNS	クリア テキストのパケットをインターネット経由で外部 DNS のドメインに送信したり、IPsec トンネルを介して社内 DNS のドメインに送信したりすることができる splitDNS を接続エントリで使用するかどうかを指定します。この機能は、VPN 3000 Concentrator 上で設定され、スプリットトンネリング接続で使用されます。 **（注）** また、接続先である VPN 中央サイト デバイス上ではこの機能を有効にする必要があります。	0 = しない 1 = する（デフォルト）	GUI には表示されません。
UseLegacyIKEPort	デフォルトの IKE ポートを 500/4500 から、すべての接続時に使用するダイナミック ポートに変更します。このパラメータは、.pcf ファイルに明示的に入力する必要があります。	0 =（リリース 4.8.01 以降ではデフォルト）レガシー設定を無効にし、cTCP でダイナミック ポートを使用する。 1 = レガシー設定 500/4500 を維持する。この場合、cTCP をサポートする VPN 中央サイト デバイスで TCP/UDP が使用しやすくなります。この設定により、VPN クライアントでスタティック ポート割り当てを使用する必要がある VPN 中央サイト デバイスとの相互運用が可能となります。このパラメータを有効にすると、特定バージョンの Windows との相互運用ができなくなります。	GUI には表示されません。
ForceNetlogin (Windows のみ)	この接続プロファイルに対して強制ネットワーク ログイン機能を有効にします。	0 = ユーザに対してログアウトおよびログインを強制しない（デフォルト）。 1 = オプションが選択されていない限り、待機時間を経過した時点でユーザにログアウトを強制する。 2 = オプションが選択されていない限り、待機時間を経過した時点で VPN セッションを解除する。 3 = ユーザが [Connect] または [Disconnect] を選択するまで待機する。	GUI には表示されません。

表 5-2　.pcf ファイルのパラメータ （続き）

.pcf パラメータ（キーワード）	VPN クライアント パラメータの説明	値	VPN クライアントでの設定場所
ForceNatT	接続の試行に NAT デバイスが関与していない場合でも、NAT-T が使用可能であれば VPN クライアントでそのネゴシエートが行われるようにします。これにより、一部のファイアウォールで VPN クライアントとの接続が不意に解除されるという問題が解決される場合があります。	ForceNatT=0（デフォルト） ForceNatT=1（NAT-T が使用可能であればそのネゴシエートを行う）	GUI には表示されません。
以下では、プロファイル内で文字「!」を使用すると、接続間で以前のユーザ情報が維持されないようにすることができます。			
CertMatchDN	VPN クライアントによる証明書選択の際に、ワイルドカードを使用して証明書の識別名を照合できるようにします。	CertMatchDN=CN="ID Cert", OU* "Cisco", Issuer-CN!= "Entrust", Issuer-OU!*"wonderland"	GUI には表示されません。
CertMatchKU	VPN クライアントによる証明書選択の際に、ワイルドカードを使用して証明書のキーの用途に関するフィールドを照合できるようにします。	CertMatchKU=0,3,4,5	GUI には表示されません。
CertMatchEKU	VPN クライアントによる証明書選択の際に、ワイルドカードを使用して証明書のキーの拡張用途に関するフィールドを照合できるようにします。 このキーワードは、接続の試行に対してのみ適用され、証明書に関するその他の動作（証明書のリスト表示、証明書の内容表示など）には適用されません。このキーワードは、あらゆる基準による証明書選択（CertSerialHash、CertMatchDN、CertSubjectName、CertName など）に適用されます。このはーワードの値は、キーの拡張用途 OID 文字列で構成されるカンマ区切りのリストです。カスタムのキーの拡張用途文字列は、1.3.6.1.5.5.7.3.n という書式にする必要があります。n は任意の数字です。	CertMatchEKU=1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.1 それぞれの説明は次のとおりです。 1.3.6.1.5.5.7.3.2：クライアント認証 1.3.6.1.5.5.7.3.1：サーバ認証	GUI には表示されません。

ユーザへの設定済み VPN クライアント ソフトウェアの配布

VPN クライアント プロファイル コンフィギュレーション ファイルの作成が完了したら、ユーザに対してそれを単独または VPN クライアント ソフトウェアの一部として配布することができます。

単独での配布

コンフィギュレーション ファイルを単独で配布する手順、およびユーザがそれを各自の PC 上にインストールしさらに VPN クライアントにインポートする手順は次のとおりです。

（注）　Mac OS X プラットフォームの場合、VPN クライアントがインストールされる前に、コンフィギュレーション ファイルが Profiles フォルダに配置されます。詳細については、『*VPN Client User Guide for Mac OS X*』の第 2 章を参照してください。

ステップ 1　適切なプロファイル ファイルを、任意のメディアを介してユーザに配布します。

ステップ 2　必要な設定情報をユーザに提供します。

ステップ 3　ユーザに次の操作を行うよう指示します。

a. 使用しているプラットフォームに対応した『*VPN Client User Guide*』に記載されている手順に従って、VPN クライアントをインストールする。

b. VPN クライアントを開始した後、使用しているプラットフォームに対応した『*VPN Client User Guide*』の第 5 章に記載されている操作を実行する。「Importing a VPN Client Configuration File」という項を参照（Windows のみ）。

c. 使用しているプラットフォームに対応した『*VPN Client User Guide*』の第 4 章に記載されている手順に従って、VPN クライアントの設定を完了する。

d. プライベート ネットワークに接続した後、使用しているプラットフォームに対応した『*VPN Client User Guide*』の第 5 章に記載されている手順に従ってパラメータを入力する。

VPN クライアント ソフトウェアによる配布

初回インストール時の VPN クライアント ソフトウェアに vpnclient.ini ファイルがバンドルされている場合は、VPN クライアントの設定がインストール中に自動で行われます。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。

インストール用として VPN クライアント ソフトウェアの事前設定済みコピーをユーザに配布する手順は次のとおりです。

ステップ 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 プラットフォームの場合、VPN クライアントがインストールされる前に、コンフィギュレーション ファイルが Profiles フォルダおよび 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。詳細については、『*VPN Client User Guide for Mac OS X*』の第 2 章を参照してください。

ステップ 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 ファイルは、すべての CD-ROM イメージ ファイルと共に必ず同じディレクトリ内に配置してください。このディレクトリからネットワーク接続を介してユーザにインストールさせることができるほか、新規 CD-ROM にすべてのファイルをコピーしてそれを配布することも、このディレクトリ内のすべてのファイルを格納した自己解凍 ZIP ファイルを作成し、それをユーザにダウンロードさせて、ソフトウェアをインストールさせることもできます。

ステップ 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。