



ユーザ プロファイル

VPN Client 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 ユーザごとに固有に構成する必要があります。ここで固有に構成されるパラメータはプロファイル構成ファイル(.pcf ファイル) 内のプロファイルと組み合わせられて、ユーザ プロファイルが作成されます。ユーザ プロファイルは、デフォルト ディレクトリの /etc/CiscoSystemsVPNClient/Profiles/ に置かれているか、VPN Client のインストール時に指定したディレクトリに置かれています。

ユーザ プロファイルのパラメータには、リモート サーバ アドレス、IPSec グループ名とパスワード、ログファイルの使用、バックアップ サーバの使用、および起動時の自動接続があります。それぞれの接続エントリには、そのエントリに固有のユーザ プロファイルがあります。



ヒント

VPN Client のユーザ プロファイルは、OS のプラットフォーム間で互換性があります。

この章では、VPN Client ユーザ プロファイルを作成する方法について説明します。この章の構成は、次のとおりです。

- [サンプル プロファイルについて \(P. 3-2\)](#)
- [サンプル プロファイルの変更 \(P. 3-2\)](#)
- [ユーザ プロファイルの作成 \(P. 3-3\)](#)

グローバル プロファイルをすべてのユーザに設定するには、『Cisco VPN Client アドミニストレータ ガイド』を参照してください。

サンプルプロファイルについて

ユーザプロファイルを作成するには、次の2通りの方法があります。

- テキストエディタを使用して、VPN Client インストーラに付属のサンプルプロファイルの内容を変更し、そのファイル名を変更する。
- テキストエディタを使用して、独自のユーザプロファイルを作成する。

ユーザプロファイルは、接続ごとに1つだけ作成してください。

VPN Client ソフトウェアには、サンプルユーザプロファイルが付属しています。ファイル名は、sample.pcf です。

次の例は、インストーラに付属のサンプルユーザプロファイルを示しています。

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=gawf
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

サンプルプロファイルの変更

サンプルプロファイルの内容を変更する手順は、次のとおりです。

ステップ1 テキストエディタを使用して、サンプルユーザプロファイルを開きます。

ステップ2 目的のキーワードを変更します。

IP アドレス、ユーザ名、およびセキュリティ情報については、システム管理者に問い合わせてください。

ステップ3 変更したプロファイルに固有の名前を付けて、/etc/CiscoSystemsVPNClient/Profiles/ ディレクトリに保存します。

vpncient connect コマンドを使用して接続を確立する際は、新しいプロファイル名を使用してください。

ユーザプロフィールの作成

テキストエディタを使用すると、新規に独自のユーザプロフィールを作成できます。

ユーザプロフィールには、少なくとも、次のキーワードを指定する必要があります。

- [main]
- Host
- AuthType
- GroupName
- Username

作成したプロフィールを /etc/CiscoSystemsVPNClient/Profiles/ ディレクトリに保存します。IP アドレス、ユーザ名、およびセキュリティ情報については、システム管理者に問い合わせてください。

表 3-1 では、ユーザプロフィールに指定可能なキーワードについて説明します。ここで記述するキーワードには、特に指示のある場合を除いて、大文字と小文字の区別はありません。

表 3-1 ユーザプロフィールのキーワード

キーワード	説明
[main]	メイン セクションを指定する必須のキーワードです。ユーザプロフィールの最初のエントリに、表示されているとおりに正確に入力します。
Description = 文字列	ユーザプロフィールの内容を説明するオプションのキーワードです。説明は、最長 246 文字の英数字です。
Host = IP アドレスまたはホスト名	接続したい VPN 装置のホスト名または IP アドレスを指定します。ホスト名は、最長 255 文字の英数字です。
AuthType = { 1 3 }	ユーザが使用する認証タイプを指定します。 <ul style="list-style-type: none"> • 1 は、事前共有鍵です。 • 3 は、RSA 署名を使用するデジタル証明書です。 AuthType 1 を選択する場合は、GroupName と GroupPwd も設定する必要があります。
GroupName = 文字列	VPN 装置に設定するユーザが属している IPSec グループの名前を指定します。名前は、最長 32 文字の英数字です。このキーワードの大文字と小文字には区別があります。
GroupPwd = 文字列	ユーザが属している IPSec グループのパスワードを指定します。このパスワードは、4 ~ 32 文字の英数字です。このキーワードの大文字と小文字には区別があり、平文で入力されます。
encGroupPwd = 文字列	ユーザプロフィールのグループパスワードを暗号化形式で表示します。このパスワードは、英数字の文字列で表示されるバイナリ データです。
Username = 文字列	GroupName で指定されている IPSec グループの有効なメンバーとして、ユーザを識別する名前を指定します。ユーザ認証時にこの名前を入力するようにプロンプトが表示されます。名前は、最長 32 文字の英数字です。このキーワードの大文字と小文字には区別があり、平文で入力されます。

表 3-1 ユーザプロフィールのキーワード (続き)

キーワード	説明
UserPassword = 文字列	<p>拡張認証時に使用するパスワードを指定します。</p> <ul style="list-style-type: none"> • SaveUserPassword が使用可能である場合、このパスワードが初めて読み取られた際に encUserPassword としてユーザプロフィールに保存され、平文のパスワードは削除されます。 • SaveUserPassword が使用不可である場合、ユーザプロフィールの平文のユーザパスワードは削除されます。暗号化されたパスワードは作成されません。
encUserPassword = 文字列	<p>ユーザプロフィールのユーザパスワードを暗号化形式で表示します。このパスワードは、英数字の文字列で表示されるバイナリデータです。</p>
SaveUserPassword = { 0 1 }	<p>ユーザプロフィールのユーザパスワードで平文または暗号化形式のどちらを有効にするかを指定します。</p> <ul style="list-style-type: none"> • 0 を指定すると、ユーザパスワードが平文でユーザプロフィールに表示され、ローカルに保存されます (デフォルト)。 • 1 を指定すると、ユーザパスワードが暗号化形式でユーザプロフィールに表示されます。このパスワードは、ローカルに保存されません。 <p>この値は、VPN 装置に設定されます。VPN Client には設定されません。</p>
EnableBackup = { 0 1 }	<p>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。</p> <ul style="list-style-type: none"> • 0 を指定すると、バックアップサーバが使用不可になります (デフォルト)。 • 1 を指定すると、バックアップサーバが使用可能になります。 <p>BackupServer も指定する必要があります。</p>
BackupServer = IP アドレス またはホスト名	<p>バックアップサーバの IP アドレスまたはホスト名を指定します。複数ある場合は、エントリをコンマで区切ります。ホスト名は、最長 255 文字の英数字です。</p>
EnableLocalLAN = { 0 1 }	<p>ローカル LAN へのアクセスを指定します。</p> <ul style="list-style-type: none"> • 0 を指定すると、ローカル LAN アクセスが使用不可になります (デフォルト)。 • 1 を指定すると、ローカル LAN アクセスが使用可能になります。
EnableNAT = { 0 1 }	<p>ファイアウォールの役目をするルータを経由した VPN Client と VPN 装置間の保護された伝送を、使用可能にするかどうかを指定します。NAT プロトコルも使用している場合があります。</p> <ul style="list-style-type: none"> • 0 を指定すると、IPSec through NAT モード (NAT 経由) が使用不可になります (デフォルト)。 • 1 を指定すると、IPSec through NAT モード (NAT 経由) が使用可能になります。

表 3-1 ユーザプロフィールのキーワード (続き)

キーワード	説明
TunnelingMode = { 0 1 }	<p>使用する NAT 横断の形式を指定します。</p> <ul style="list-style-type: none"> • 0 を指定すると、NAT 透過性に IPsec over UDP が指定されます (デフォルト) • 1 を指定すると、NAT 透過性に IPsec over TCP が指定されます。 <p>IPsec through NAT も使用可能にする必要があります。</p>
TCP TunnelingPort = { 0 65535 }	cTCP プロトコルに使用する TCP ポートを指定します。デフォルトは、10000 です。また、IPsec through NAT を使用可能にし、Tunneling Mode を IPsec over TCP に指定する必要があります。
ForceKeepAlives = { 0 1 }	<p>接続に対して IKE と ESP キープアライブを約 20 秒間隔で送信し続けるよう指定します。その結果、ESP 対応の NAT/Firewall 上のポートがクローズしません。</p> <ul style="list-style-type: none"> • 0 を指定すると、キープアライブが使用不可になります (デフォルト) • 1 を指定すると、キープアライブが使用可能になります。
PeerTimeout = 数字	トンネルの相手側にある VPN 装置が応答しないときに、接続の終端まで待機する秒数を指定します。この秒数は、30 ~ 480 秒です。デフォルトは 90 です。
CertStore = { 0 1 }	<p>設定済みの証明書が入っているストアのタイプを指定します。</p> <ul style="list-style-type: none"> • 0 = なし (デフォルト) • 1 = Cisco
CertName = 文字列	VPN 装置との接続に使用する証明書を指定します。この名前は、最長 129 文字の英数字です。
CertPath = 文字列	証明書ファイルが入っているディレクトリのパス名です。このパス名は、最長 259 文字の英数字です。
CertSubjectName = 文字列	証明書の所有者の修飾識別名 (DN) を指定します。このキーワードはユーザプロフィールに指定しないことも、またはエントリを空白のままにすることも可能です。
CertSerialHash = 文字列	証明書のすべての内容のハッシュを指定します。これにより、証明書の信頼性が確認されます。このキーワードはユーザプロフィールに指定しないことも、またはエントリを空白のままにすることも可能です。
DHGroup = { 1 2 }	<p>VPN 装置で Diffie-Hellman 鍵ペアを生成するのに使用される設定済みのグループ値をネットワーク管理者が指定します。</p> <ul style="list-style-type: none"> • 1 = modp group 1 • 2 = modp group 2 <p>デフォルトは 2 です。VPN Concentrator の IKE Proposal 設定と VPN Client の DHGroup は一致しなければなりません。AuthType が 3 (デジタル証明書) に設定されている場合は、このキーワードは VPN Client で無効になります。</p>

