



# コマンド行インターフェイスの使用

この章では、CLI (コマンド行インターフェイス) を実行する場合の一般的な操作について説明します。この章の構成は、次のとおりです。

- [コマンド一覧の表示 \(P. 4-1\)](#)
- [接続の確立 \(P. 4-2\)](#)
- [VPN Client の接続解除 \(P. 4-4\)](#)
- [VPN Client 統計値の表示 \(P. 4-5\)](#)
- [イベント ロギング \(P. 4-7\)](#)

## コマンド一覧の表示

VPN Client で使用可能なコマンドを一覧で表示するには、VPN Client ソフトウェアが格納されているディレクトリに移動し、コマンド行プロンプトに対して、`vpnclient` コマンドを入力します。

次の例は、`vpnclient` コマンドに対して表示される情報を示しています。

```
%vpnclient
Cisco Systems VPN Client Version 3.7 (Rel)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686

Usage:
  vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd
<password>] [nocertpwd]
  vpnclient disconnect
  vpnclient stat [reset] [traffic] [tunnel] [route] [repeat]
  vpnclient notify
```

## 接続の確立

ここでは、`vpnclient connect` コマンドとオプションのコマンドパラメータを使用して、VPN 接続を確立する方法について説明します。



(注) Telnet または SSH を使用して VPN 装置に接続する場合は、その VPN 装置でスプリットトンネリングが許されているか確認してください。スプリットトンネルが許されていない場合は、VPN 接続の実行後、その VPN 装置への接続は解除されてしまいます。

接続を確立するには、次のコマンドを入力します。

```
vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd <password>]
[nocertpwd]
```

表 4-1 では、`vpnclient connect` コマンドのパラメータについて説明します。

表 4-1 `vpnclient connect` コマンドのパラメータ

パラメータ	説明
<profile> (必須)	接続エントリに設定するユーザプロファイルの名前を指定します (.pcf ファイル)。プロファイル名には、.pcf ファイル拡張子を付けないで入力してください。プロファイル名にスペースが含まれている場合は、コマンド行でそのプロファイル名を二重引用符で囲んでください。
user <username> (オプション)	接続エントリに設定するユーザ名を指定します。このオプションに <code>pwd</code> オプションを付けて使用すると、ユーザ名の入力を求めるプロンプトが認証ダイアログボックスに表示されません。
{ eraseuserpassword   pwd <password> } (オプション)	<ul style="list-style-type: none"> <li><code>eraseuserpassword</code> を指定すると、VPN Client ワークステーションに保存されているユーザパスワードが削除され、接続を確立するたびにパスワードの入力を求めるプロンプトが表示されます。</li> <li><code>pwd &lt;password&gt;</code> を指定すると、パスワードの入力を求めるプロンプトが認証ダイアログボックスに表示されません。</li> </ul>
nocertpwd (オプション)	証明書パスワードの入力を求めるプロンプトを非表示にして、パスワードを空白に指定します。このオプションを使用すると、証明書のパスワードを設定することはできません。詳細は、「 <a href="#">証明書パスワード</a> 」(P. 5-4) を参照してください。



(注) ユーザプロファイルの `SaveUserPassword` キーワードがデフォルトに設定されている場合は、パスワードはローカルに保存されます。

プロファイルの詳細は、[第 3 章「ユーザプロファイル」](#) を参照してください。

## 認証プロンプト

ユーザ プロファイルに設定されているパラメータに応じて、次のパスワードを入力するようにプロンプトが表示されます。

- グループパスワード
- ユーザ名
- ユーザパスワード
- 証明書パスワード

VPN Client で SecurID または RADIUS 認証を使用するように設定されている場合は、前述のパスワードも入力するようにプロンプトが表示されます。

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。

## Rekey について

接続が確立されると、VPN Client ウィンドウがフォアグラウンドに表示された状態になり、VPN 装置が行う Rekey (鍵交換) 時の再認証が可能になります。VPN Client ウィンドウをバックグラウンドに移動するには、**Ctrl-Z** を押して、コマンド行プロンプトで **bg** コマンドを入力します。

接続先の VPN 装置で Rekey のサポートが設定されている場合、VPN Client ウィンドウをバックグラウンドに移動すると、最初の Rekey 時にトンネル接続が解除されてしまいます。

VPN Client では、Rekey トリガーに対してデータではなく時間に基づいて応答します。VPN Client 接続で Rekey を行う場合は、VPN Concentrator での設定は、IKE プロポーザルの Rekey は 1800 秒ごとに、また IPSec パラメータの Rekey は 600 秒ごとにそれぞれ指定する必要があります。

## DNS サーバ設定

VPN Concentrator では、トンネル セッション時に使用する DNS サーバの IP アドレスを VPN Client に送信するように設定できます。

VPN Client が DNS サーバの設定値を受信すると、`/etc/resolv.conf` ファイルを `/etc/resolv.conf.vpnbackup` バックアップ ファイルにコピーします。トンネルがクローズすると、`/etc/resolv.conf` の元の内容が復元されます。



(注) DNS サーバの設定値については、VPN 装置の構成ガイドを参照してください。

## VPN Client の接続解除

ここでは、VPN Client の接続を解除する方法について説明します。

使用中のセッションから接続を解除するには、次のいずれかの方法を使用します。

- 次のコマンドを入力します。

```
vpnclient disconnect
```

次の例は、セキュリティの保護された接続を解除するコマンドと、その実行により接続が解除されたときに表示されるプロンプトを示しています。

```
vpnclient disconnect
Disconnecting the IPSEC link.
Your IPsec link is not connected.
```

- VPN Client ウィンドウの表示中に、Ctrl-C を押します。

## VPN Client 統計値の表示

ここでは、VPN Client 統計値コマンド `vpnclient stat` と、そのオプションのパラメータについて説明します。

現在使用中の接続についてのステータス情報を生成するには、次のコマンドを入力します。

```
vpnclient stat [reset][traffic][tunnel][route][repeat]
```

`vpnclient stat` コマンドにオプション パラメータを指定しないで入力すると、すべてのステータス情報が表示されます。表 4-2 では、オプション パラメータについて説明します。

表 4-2 `vpnclient stat` コマンドのオプション パラメータ

パラメータ	説明
<code>reset</code>	すべての接続カウントをゼロから再開します。
<code>traffic</code>	入力バイト数と出力バイト数、暗号化パケット数と復号化パケット数、およびバイパス パケット数と廃棄パケット数の一覧を表示します。
<code>tunnel</code>	IPSec トンネリング情報を表示します。
<code>route</code>	設定されているルートを表示します。
<code>repeat</code>	連続して表示し、数秒ごとに画面を更新します。連続表示を終了するには、 <b>Ctrl-C</b> を押します。

### 例

ここでは、`vpnclient stat` コマンドに対して、オプションを変えて指定した場合の出力例を示します。

### オプションなし

次の例は、`vpnclient stat` コマンドにオプションを指定しない場合の出力を示しています。

```
vpnclient stat

IPSec tunnel information.
Client address: 209.154.64.50
Server address: 10.10.32.32
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000

VPN traffic summary.
Time connected: 0 day<s>, 00:18.32
Bytes out: 3420
Bytes in: 3538
Packets encrypted: 23
Packets decrypted: 57
Packets bypassed: 102
Packets discarded: 988

Configured routes
Secured  Network Destination  Netmask  Bytes
*        10.10.32.32  255.255.255.255  7638
*        0.0.0.0    0.0.0.0    1899
```

## reset オプション

すべての接続カウンタをリセットするには、**vpnclient stat reset** コマンドを使用します。

```
vpnclient stat reset
Tunnel statistics have been reset.
```

## traffic オプション

次の例は、**vpnclient stat** コマンドに **traffic** オプションを指定する場合の出力を示しています。

```
vpnclient stat traffic

VPN traffic summary
Time connected: 0 day<s>, 00:30:04
Bytes out: 5460
Bytes in: 6090
Packets encrypted: 39
Packets decrypted: 91
Packets bypassed: 159
Packets discarded: 1608
```

## tunnel オプション

次の例は、**vpnclient stat** コマンドに **tunnel** オプションを指定する場合の出力を示しています。**vpnclient stat tunnel** コマンドでは、トンネリング情報だけが表示されます。

```
vpnclient stat tunnel

IPSec tunnel information.
Client address: 220.111.22.30
Server address: 10.10.10.1
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000
```

## route オプション

次の例は、**vpnclient stat** コマンドに **route** オプションを指定する場合の出力を示しています。

```
vpnclient stat route

Configured routes
Secured  Network Destination  Netmask  Bytes
*        10.10.02.02  255.255.255.255  17638
*        0.0.0.0     0.0.0.0         18998
```

## イベント ログ

ここでは、ログ情報を取り込む方法、またその情報を表示する方法など、イベント ログについて説明します。

### ログ機能のイネーブル化

ログ機能をイネーブルにできる人は、システム管理者またはグローバル プロファイル ( `vpnclient.ini` ) へのアクセス権限があるユーザーに限られます。 `/etc/CiscoSystemsVPNClient/vpnclient.ini` ディレクトリ下に格納されているグローバル プロファイルには、次のパラメータが設定されている必要があります。

```
[main]
EnableLog=1
[LOG.IKE]
LogLevel=3
[LOG.CM]
LogLevel=3
[LOG.PPP]
LogLevel=3
[LOG.CVPND]
LogLevel=3
[LOG.CERT]
LogLevel=3
[LOG.IPSEC]
LogLevel=3
```

グローバル プロファイルを設定する方法については、『Cisco VPN Client アドミニストレータ ガイド』を参照してください。

### ログ ファイルの表示

ログ情報を表示するには、次のコマンドを入力します。

```
/usr/local/bin/ipseclog /directory/clientlog.txt
```



(注) インストール時にデフォルトの `/usr/local/bin` ディレクトリを使用しなかった場合は、インストール中に選択したパスを使用してログ コマンドを入力してください。

ログ情報をリアルタイムで表示するには、`ipseclog` を起動した後に次のコマンドを入力します。

```
tail -f /directory/clientlog.txt
```

`ipseclog` は、自動的にバックグラウンドに移動しません。`ipseclog` をバックグラウンドに移動するには、`Ctrl-Z` を押した後、コマンド行で `bg` と入力します。または、次の例のように、`view` コマンドの最後にアンパサンド記号 (`&`) を入力します。

```
/usr/local/bin/ipseclog /directory/clientlog.txt &
```

`ipseclog` がバックグラウンドで動作している場合は、VPN Client アプリケーションを終了する前に、`ipseclog` をフォアグラウンドに移動する必要があります。`ipseclog` をフォアグラウンドに移動するには、コマンド行で `fg` と入力します。

## Client 自動更新メッセージ

VPN Client が VPN リモート アクセス装置から自動更新の通知を受信すると、その通知はログに記録されます。ログの記録以外のアクションは実行されません。自動更新メッセージを受信したときに記録されるメッセージの形式は、次のとおりです。

```
688 10:14:23.811 08/08/2001 Sev=Info/4 IKE/0x4300005B^M CLIENT_UPDATE_NOTIFICATION:
Client Type="linux" Revisions="3.0.5" URL="tftp://x:/y/z"
```

自動更新メッセージおよびその他の通知をネットワーク管理者から受信するには、`vpnclient notify` コマンドを使用します。