



## VPN Client のインストール

---

この章では、ワークステーションに VPN Client ソフトウェアをインストールする方法について説明します。

ここで説明する手順を実行するには、UNIX コンピュータへのソフトウェアのインストール方法に関する知識が必要です。

VPN Client は、次のコンポーネントから構成されています。

- ドライバ (ロード可能モジュール)
- シェルからアクセス可能なコマンド群 (アプリケーションへのアクセスに使用)

これらのコマンドとドライバの一部は、バイナリ形式でのみ配布されます。

## 旧バージョンの Client のアンインストール

ここでは、旧バージョンの VPN Client のアンインストール方法について説明します。

- 新バージョンの VPN Client Solaris 版をインストールする場合は、事前に旧バージョンの VPN Client をアンインストールしておく必要があります。
- 新バージョンの VPN Client Linux 版をインストールする場合は、事前に旧バージョンの VPN Client をアンインストールしておく必要はありません。
- VPN Client をインストールする場合は、すべてのバージョンの VPN 5000 Client を事前にアンインストールしておく必要があります。詳細は、Cisco VPN 5000 Client のマニュアルを参照してください。

### VPN Client Solaris 版のアンインストール

VPN Client Solaris 版がすでにインストールされている場合は、インストール済みの VPN Client を削除してから、新しいバージョンの VPN Client をインストールする必要があります。

パッケージをアンインストールするには、`pkgrm` コマンドを使用します。たとえば、次のように入力します。

```
pkgrm vpnclient
```

### VPN Client Linux 版のアンインストール

VPN Client Linux 版をアンインストールする手順は、次のとおりです。

---

ステップ 1 次のコマンドを実行します。

```
sudo /usr/local/bin/vpn_uninstall
```

ステップ 2 すべてのプロファイルと証明書の削除を確認するプロンプトが表示されます。

- YES を選択すると、バイナリ ファイル、起動スクリプト、証明書、プロファイル、およびインストール中に作成されたディレクトリがすべて削除されます。
  - NO を選択すると、バイナリ ファイルと起動スクリプトがすべて削除されます。ただし、証明書、プロファイル、および `vpnclient.ini` ファイルは削除されません。
-

## 必要な情報の収集

VPN Client を設定して使用するには、次の情報が必要です。

この情報は、通常、アクセスするプライベート ネットワークのシステム管理者から取得します。システム管理者が、この情報の多くを事前に設定していることがあるからです。

- 接続先のセキュア ゲートウェイのホスト名または IP アドレス
- IPSec グループ名 (事前共有キー用)
- IPSec グループ パスワード (事前共有キー用)
- デジタル認証による認証の場合は、証明書の名前
- 次の方法での認証の場合は、ユーザ名とパスワード
  - セキュア ゲートウェイの内部サーバ
  - RADIUS サーバ
  - NT ドメイン サーバ
- トークン ベンダーによる認証の場合は、ユーザ名と PIN
- バックアップ サーバへの接続を設定する場合は、バックアップ サーバのホスト名と IP アドレス

## システム要件の確認

ここでは、各オペレーティング システムを使用する場合の VPN Client のシステム要件について説明します。

### Linux のシステム要件

VPN Client Linux 版は、Red Hat バージョン 6.2 Linux (Intel) または glibc バージョン 2.1.1-6 以降の互換ライブラリを備えた Red Hat で、カーネル バージョン 2.2.12 以降をサポートしています。



(注) VPN Client Linux 版では、カーネル バージョン 2.5 または SMP (マルチプロセッサ) カーネルをサポートしていません。

### ファイアウォールについて

ipchains や iptables などの Linux ファイアウォールを実行している場合は、次のトラフィックのパススルーが許されていることを確認してください。

- UDP ポート 500
- UDP ポート 10000 (または IPSec/UDP に使用されているポート番号)
- IP プロトコル 50 (ESP)
- IPSec/TCP に設定されている TCP ポート
- NAT-T (標準準拠の NAT 透過性) ポート 4500

### トラブルシューティングのヒント

Linux でのインストールの場合、次に示す 2 行が /etc/sysconfig/ipchains ディレクトリにデフォルトで追加されることがあります。Red Hat では、/etc/sysconfig/ipchains ディレクトリに追加されます。これらの 2 つのコマンドは、UDP トラフィックのパススルーを回避する場合があります。

```
-A input -p udp -s 0/0 -d 0/0 0:1023 -j REJECT
-A input -p udp -s 0/0 -d 0/0 2049 -j REJECT
```

UDP トラフィックに障害がある場合は、次のいずれかの方法を試してください。

- 上記の 2 つの REJECT 行を削除してから、次の 2 つのコマンドを入力します。

```
/etc/init.d/ipchains stop
/etc/init.d/ipchains start
```



(注) ipchains は iptables に置き換えられる場合があります。または、Linux ディストリビューションの別のディレクトリに置かれる場合があります。

- 次の規則をデフォルトの ipchains ファイアウォール構成に追加するか、上記の UDP の REJECT 行のいずれかに追加します。

```
-A input -p udp -s 0/0 -d 0/0 500 -j ACCEPT
```

この規則により、VPN Client の接続に必要な UDP ポート 500 を使用できるようになります。

## Solaris システム要件

VPN Client Solaris 版は、32 ビットまたは 64 ビット Solaris カーネル OS バージョン 2.6 以降を搭載する UltraSPARC コンピュータで動作します。

### カーネルバージョンの変更

32 ビット版または 64 ビット版のカーネルを実行する VPN Client (32 ビット モードまたは 64 ビット モード) をインストールできます。いずれかのモードで VPN Client をインストールまたは実行する際に問題が発生した場合は、もう一方のモードを試してください。

どのモードでシステムが動作しているかを確認するには、次のコマンドを入力します。

```
isainfo -kv
```

cipsec モジュールが正常にロードされている場合、dmesg ログに次のようなメッセージが表示されます。

```
Oct 29 11:09:54 sol-2062 cipsec:[ID 952494 kern.notice] Cisco Unity IPSec Module Load OK
```



(注) dmesg ログに cipsec ログメッセージが表示されない場合は、もう一方のモードに切り替える必要があります。

32 ビット モードに切り替える手順は、次のとおりです。

- 一時的に切り替えるには、次のコマンドを入力します (ok はシステム プロンプトを表しています)。

```
ok boot kernel/unix
```

- 永続的に切り替えるには、root として次のコマンドを入力し、コンピュータを再起動します。

```
eeeprom boot-file=/platform/sun4u/kernel/unix
```

64 ビット モードに切り替える手順は、次のとおりです。

- 一時的に切り替えるには、次のコマンドを入力します (ok はシステム プロンプトを表しています)。

```
ok boot kernel/sparcv9/unix
```

- 永続的に切り替えるには、root として次のコマンドを入力し、コンピュータを再起動します。

```
eeeprom boot-file=/platform/sun4u/kernel/sparcv9/unix
```

## VPN Client ファイルの解凍

VPN Client は、圧縮された tar ファイルとして出荷されています。

この圧縮ファイルを解凍する手順は、次のとおりです。

- 
- ステップ 1 社内ネットワークまたはシスコの Web サイトから、圧縮ファイルを任意のディレクトリにダウンロードします。
  - ステップ 2 選択したディレクトリにこの VPN Client ファイルをコピーします。
  - ステップ 3 `zcat` コマンドと `tar` コマンドを使用してこのファイルを解凍します。

たとえば、Linux では次のコマンドを入力します。

```
zcat vpnclient-linux-3.7.xxx-K9.tar.gz | tar xvf -
```

Solaris では次のコマンドを入力します。

```
zcat vpnclient-solaris-3.7.xxx-K9.tar.Z | tar xvf -
```

このコマンドを実行すると、現在のディレクトリ内に `vpnclient` ディレクトリが作成されます。

---

## ソフトウェアのインストール

ここでは、オペレーティングシステムごとに、VPN Client をインストールする手順を説明します。

### VPN Client Linux 版のインストール

新しいバージョンの VPN Client をインストールする場合、または現在のバージョンを再インストールする場合は、事前に **stop** コマンドを使用して VPN サービスを無効にしておく必要があります。

VPN 5000 Client から新しい VPN Client にアップグレードする場合は、次の **stop** コマンドを使用します。

```
/etc/rc.d/init.d/vpn stop
```

VPN 3000 Client から新しい VPN Client にアップグレードする場合は、次の **stop** コマンドを使用します。

```
/etc/rc.d/init.d/vpnclient_init stop
```

VPN Client Linux 版をインストールする手順は、次のとおりです。

**ステップ 1** インストール スクリプトを実行するためにスーパーユーザ権限を取得します。

**ステップ 2** 次のコマンドを入力します。

```
cd vpnclient
./vpn_install
```

バイナリ、カーネル、VPN モジュール、およびプロファイルのデフォルト ディレクトリが、インストール中に表示されます。

インストール中に次のプロンプトが表示されます。

- Directory where binaries will be installed [/lib/modules/<kernel version>/build/] (バイナリがインストールされるディレクトリ [/lib/modules/<カーネルのバージョン>/build/])
- Automatically start the VPN service at boot time [yes] (ブート時の VPN サービスの自動起動 [yes])
- Directory containing linux kernel source code [/usr/src/linux] (Linux カーネルのソースコードを含むディレクトリ [/usr/src/linux])
- Is the above correct [y] (以上の入力内容で正しいですか [y])

**ステップ 3** [Enter] キーを押してデフォルトの入力内容を選択します。ディレクトリの選択時にデフォルトのディレクトリを選択しない場合、別のディレクトリをユーザのパスに入力する必要があります。

**ステップ 4** インストーラがこれらの設定を自動的に検出できない場合は、次のプロンプトが表示されます。

- Directory containing init scripts: (init スクリプトを含むディレクトリ)
  - これは、ブート時に実行されるスクリプトが保存されるディレクトリです。通常、このディレクトリは /etc/init.d または /etc/rc.d/init.d です。
- Directory containing run level directories (rcX.d): (実行レベルのディレクトリ (rcX.d) を含むディレクトリ)
  - これは、init の実行レベルのディレクトリを含むディレクトリです。通常、このディレクトリは /etc または /etc/rc.d です。

ステップ 5 次のいずれかの方法で、VPN サービスを有効にします。

- コンピュータを再起動します。
- コンピュータを再起動しないでサービスを有効にするには、次のコマンドを入力します。

```
/etc/rc.d/init.d/vpnclient_init start
```

## カーネルソースの要件

VPN Client をインストールするには、システムで実行されているカーネルの構築に使用されたカーネルソースが必要です。Linux ディストリビューションで提供されたカーネル、またはカスタムビルドカーネルをシステムで使用している場合は、次のように、カーネルコードをそれぞれ異なる方法で入手できます。

- ディストリビューションで提供されたカーネルが実行されている場合：対応するカーネルソース rpm をインストールする必要があります。vpn\_install スクリプトによりカーネルソースが自動検出される必要があります。
- カスタムビルドカーネルが実行されている場合：実行されているカーネルの構築に使用したものと同一カーネルソースのコピーを使用する必要があります。ただし、使用しているバージョンのカーネルのソースコードを解凍するだけでは不十分です。カーネルがコンパイルされるときには、VPN Client が使用するいくつかのファイルが生成されます。これらのファイルは、実行されているカーネルと正確に一致していなければなりません。一致していないと、VPN Client のインストールが失敗します。



(注)

ワークステーションのカーネルにパッチをインストールする場合は、これらのガイドラインに従って VPN Client を再インストールする必要があります。

## VPN Client Linux 版 インストールスクリプトについて

インストール中に、次の処理が行われます。

1. モジュールは、コンパイルとリンクが行われ、`/lib/modules/preferred/CiscoVPN` ディレクトリ(存在する場合) または `/lib/modules/system/CiscoVPN` にコピーされます。ここでの `system` は、カーネルバージョンを表します。
2. アプリケーションバイナリは、指定されたディレクトリにコピーされます。
3. VPN サービスを有効または無効にする起動ファイル `/etc/rc.d/init.d/vpnclient_init` が作成されます。
4. `/etc/rc3.d/s85vpnclient` リンクおよび `etc/rc5.d/s85vpnclient` リンクが追加され、ブート時に起動が要求された場合にレベル 3 およびレベル 5 で実行されます。

これらのリンクにより、トンネルサーバがブート時に起動し、レベル 3 およびレベル 5 で実行されます。

## VPN Client Solaris 版のインストール

新しいバージョンの VPN Client をインストールする場合、または現在のバージョンを再インストールする場合は、既にインストールされている VPN Client をアンインストールしておく必要があります。詳細は、「旧バージョンの Client のアンインストール」(P. 2-2) を参照してください。



(注)

VPN Client Solaris 版のリリース 3.7 以降をバージョン 2.6 の Solaris プラットフォームにインストールする場合、VPN Client のインストール中に次のメッセージが表示されます。「Patch 105181 version 29 (or higher) to Solaris 2.6 is required for the client to function properly. (クライアントを正しく機能させるには、Solaris 2.6 のパッチ 105181 バージョン 29 以降が必要です。) Installing without this patch will cause the kernel to crash as soon as the client kernel module is loaded. (このパッチを適用しないでインストールを行うと、クライアントのカーネル モジュールがロードされると同時にカーネルがクラッシュします。) This patch is available from Sun as part of the "Recommended Solaris Patch Cluster". (このパッチは、「Recommended Solaris Patch Cluster」の一部としてサンから入手できます。) If you proceed with installation, the kernel module will not be enabled. (インストールを続行すると、カーネルモジュールは使用不可になります。) After you have installed the patch, you may enable the kernel module by uncommenting all lines in /etc/iu.ap that contain 'cipsec'. (パッチをインストールすると、「cipsec」を含む /etc/iu.ap のすべての行をアンコメントしてカーネル モジュールを使用可能にできます。)」

VPN Client Solaris 版をインストールする手順は、次のとおりです。

**ステップ 1** インストール スクリプトを実行するためにスーパーユーザ権限を取得します。

**ステップ 2** 次のコマンドを入力します。

```
pkgadd -d . vpnclient
```

バイナリ、カーネル、VPN モジュール、およびプロファイルのデフォルト ディレクトリが、インストール中に表示されます。

インストール中に次のプロンプトが表示されます。

- Directory where binaries will be installed [/usr/local/bin] (バイナリがインストールされるディレクトリ [/usr/local/bin])
- Is the above correct [y] (以上の入力内容で正しいですか [y])
- インストーラで VPN Client と別のアプリケーションとの競合が見つかった場合、次のメッセージが表示されます。

The following files are already installed on the system and are being used by another package:<installer lists files> Do you want to install these conflicting files [y,n,?,q] (次のファイルはすでにシステムにインストールされ、別のパッケージにより使用されています : <表示されているファイル> これらの競合ファイルをインストールしますか [y,n,?,q])

- The following files are being installed with setuid and/or setgid permissions:<installer lists files>Do you want to install these as setuid/setgid files [y,n,?,q] (次のファイルが setuid と setgid の権限でインストールされます:<表示されているファイル> これらのファイルを setuid/setgid ファイルとしてインストールしますか [y,n,?,q])
- This package contains scripts which will be executed with super-user permission during the process of installing this package. (このパッケージには、パッケージのインストール中にスーパーユーザ権限で実行されるスクリプトが含まれています。) Do you want to continue with the installation of <vpnclient> [y,n,?] ( <vpnclient> のインストールを続行しますか [y,n,?])

**ステップ 3** [Enter] キーを押してデフォルトの入力内容を選択します。ディレクトリの選択時にデフォルトのディレクトリを選択しない場合、別のディレクトリをユーザのパスに入力する必要があります。

**ステップ 4** コンピュータを再起動します。

## VPN Client Solaris 版インストール スクリプトについて

インストール中に、次の処理が行われます。

1. 次の行が /etc/uu.ap ファイルに追加され、起動時に自動プッシュ機能が有効になります。

```
<dev_name> -1 0 cipsec
```

ここでの dev\_name は後続の数字が付いていないインターフェイスの名前です (例: ipdtp、le、hme)。検出されたサポートされているネットワーク装置ごとに 1 行追加されます。

2. VPN モジュールが /kernel/strmod ディレクトリ (システムのモジュール検索パス内) にコピーされます。

**pkginfo** コマンドを実行すると、インストールされているパッケージの情報が表示されます。パッケージに関連するその他のコマンドの情報を表示するには、次のコマンドを入力します。

```
man pkgadd
```