



## VPN Client の概要

---

Cisco VPN Client は、次のいずれかのオペレーティング システムを使用するコンピュータ上で動作するソフトウェア アプリケーションです。

- Linux for Intel : RedHat バージョン 6.2 以降、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 RedHat で、カーネル OS バージョンは 2.2.12 以降が使用されていること。
- Solaris UltraSPARC : 32 ビットまたは 64 ビット Solaris で、カーネル OS バージョンは 2.6 以降が使用されていること。

リモート PC 上の VPN Client は、企業ネットワーク上の Cisco VPN 装置またはサービス プロバイダーと通信するときに、インターネット上にセキュリティの保護された接続を構築します。この接続は、オンサイトのユーザがプライベート ネットワークにアクセスするように、VPN (パーチャルプライベート ネットワーク) を構築する機能です。

次の VPN 装置では、VPN Client から開始された VPN 接続を終端することができます。

- Easy VPN サーバ機能をサポートする Cisco ISO 装置
- VPN 3000 シリーズ コンセントレータ
- Cisco PIX Firewall シリーズ

VPN Client の CLI ( コマンド行インターフェイス ) を使用すると、プライベート ネットワークへの VPN 接続を確立したり、接続エントリ、証明書、およびイベント ログを管理したりできます。

この章の構成は、次のとおりです。

- [VPN Client の基本動作 \( P. 1-2 \)](#)
- [VPN Client の機能 \( P. 1-3 \)](#)

## VPN Client の基本動作

VPN Client では、Cisco VPN 装置と連携して動作し、ユーザのコンピュータとプライベート ネットワーク間でトンネルと呼ばれるセキュリティの保護された接続を構築します。また、IKE( インターネット鍵交換 ) および IPSec( インターネット プロトコル セキュリティ ) のトンネリング プロトコルを使用して、保護された接続を確立し、その管理をします。

VPN 接続を確立するときには、次に示す機能が必要に応じて使用されます。

- トンネル パラメータのネゴシエーション ( アドレス、アルゴリズム、ライフタイム )
- パラメータに応じた VPN トンネルの確立
- ユーザの認証 ( ユーザ名、グループ名とパスワード、X.509 デジタル証明書による認証 )
- ユーザのアクセス権の確立 ( アクセス時間、接続時間、許可する送信先、許可するプロトコル )
- 暗号化および復号化に必要なセキュリティ キーの管理
- トンネルを経由したデータの認証、暗号化、および復号化

たとえば、ユーザがリモート PC から自社に宛てられた E メールを読む場合、リモート接続は次のように行われます。

1. インターネットに接続します。
2. VPN Client を起動します。
3. インターネットを経由して、ユーザの組織のプライベート ネットワークへセキュリティの保護された接続を確立します。
4. E メールを開くと、次の処理が実行されます。

Cisco VPN 装置は、次のように動作します。

- IPSec を使用して E メールメッセージを暗号化します。
- このメッセージをトンネルを経由してユーザの VPN Client に送信します。

VPN Client は、次のように動作します。

- 受信したメッセージを復号化し、ユーザがリモート PC 上で読めるようにします。
- IPSec を使用してこのメッセージを処理し、メッセージを Cisco VPN 装置を経由してプライベート ネットワークに戻します。


## VPN Client の機能

ここでは、VPN Client の機能を説明します。

### 主要機能

表 1-1 では、VPN Client の主要な機能について説明します。

表 1-1 VPN Client の主要機能

機能	説明
オペレーティングシステム	<ul style="list-style-type: none"> <li>Linux (Intel)</li> <li>Solaris (UltraSPARC-32 ビットおよび 64 ビット)</li> </ul>
接続タイプ	<ul style="list-style-type: none"> <li>非同期シリアル PPP</li> <li>インターネット接続イーサネット</li> </ul> <p> (注) VPN Client では、1 つの PPP と 1 基のイーサネットアダプタだけがサポートされています。</p>
プロトコル	IP
トンネル プロトコル	IPSec
ユーザ認証	<ul style="list-style-type: none"> <li>RADIUS</li> <li>RSA SecurID</li> <li>VPN サーバ内部ユーザリスト</li> <li>PKI デジタル証明書</li> <li>NT ドメイン (Windows NT)</li> </ul>

### プログラム機能

表 1-2 では、VPN Client でサポートされているプログラム機能について説明します。

表 1-2 プログラム機能

プログラム機能	説明
サーバのサポート	<ul style="list-style-type: none"> <li>Easy VPN サーバ機能をサポートする Cisco ISO 装置</li> <li>VPN 3000 シリーズ コンセントレータ</li> <li>Cisco PIX Firewall シリーズ</li> </ul>
ローカル LAN アクセス	中央側でアクセスが認可されている場合、中央側の VPN サーバにセキュア ゲートウェイを経由して接続すると同時に、ローカル LAN 上のリソースにアクセスすることができます。
VPN Client 自動構成オプション	構成ファイルをインポートすることができます。
イベント ログिंग	ログにイベントが収集され、表示および分析されます。
NAT 透過性 (NAT-T)	VPN Client と VPN 装置で IPSec over UDP をいつ使用するかを自動的に検出するように設定し、PAT (ポート アドレス変換) 環境で正しく動作できるようにします。

表 1-2 プログラム機能 ( 続き )

プログラム機能	説明
中央制御バックアップサーバリストの更新	接続が確立されると、バックアップ VPN サーバリストが確認されます。この機能は VPN 装置上で設定され、VPN Client にプッシュされます。各接続エントリのバックアップサーバは、Backup Servers タブに表示されます。
MTU サイズの設定	ユーザの環境に最適なサイズが自動的に設定されます。ただし、ユーザが手動で MTU サイズを設定することもできます。MTU サイズの調整については、『Cisco VPN Client アドミニストレータガイド』を参照してください。
ダイナミック DNS ( DDNS ホスト名 ) のサポート	接続が確立されると、VPN Client のホスト名が VPN 装置に送信されます。この場合、VPN 装置はそのホスト名を DHCP 要求で送信できます。この結果、DNS サーバのデータベースが更新され、新しいホスト名と VPN Client アドレスが組み込まれます。

## IPSec 機能

表 1-3 では、VPN Client でサポートされている IPSec 機能について説明します。

表 1-3 IPSec 機能

IPSec 機能	説明
トンネル プロトコル	IPSec
透過的トンネリング	<ul style="list-style-type: none"> <li>NAT と PAT に使用する IPSec over UDP</li> <li>NAT と PAT に使用する IPSec over TCP</li> </ul>
鍵管理プロトコル	IKE ( インターネット鍵交換 )
IKE キープアライブ	ピアが連続して存在していることをモニタし、VPN Client が連続して存在していることをそのピアに報告するツール。このツールにより、ピアが存在しなくなったことがユーザに通知されます。もう 1 つのタイプのキープアライブは、NAT ポートを継続してアクティブにします。
スプリットトンネリング	パケットを平文および IPSec トンネル経由の暗号文で同時にインターネットに送信することができます。VPN 装置は、トンネル化されたトラフィックに必要なネットワーク リストを VPN Client に渡します。ユーザは VPN Client でスプリットトンネリングを使用可能にし、VPN 装置でそのネットワーク リストを設定します。
スプリット DNS のサポート	インターネット上で外部 DNS ( ユーザの ISP を処理 ) を経由して処理されるドメインに、または IPSec トンネルを経由して企業 DNS で処理されるドメインに、DNS パケットを平文で送信することができます。VPN サーバはドメイン リストを VPN Client に渡し、プライベートネットワークの宛先へのパケットをトンネリングします。たとえば、corporate.com 宛のパケットの照会には、トンネルを経由してプライベートネットワークの DNS で処理されるのに対して、myfavoritesearch.com 宛のパケットの照会には、ISP の DNS で処理されることとなります。この機能は、VPN サーバ ( VPN Concentrator ) で設定し、VPN Client ではデフォルトのまま使用可能にしておきます。スプリット DNS を使用するには、スプリットトンネリングも設定しておく必要があります。

## IPSec 属性

表 1-4 では、VPN Client でサポートされている IPSec 属性について説明します。

表 1-4 IPSec 属性

IPSec 属性	説明
メイン モードおよびアグレッシブモード	ISAKMP SA (セキュリティ アソシエーション) を確立するフェーズ 1 をネゴシエーションする方法です。
認証アルゴリズム	<ul style="list-style-type: none"> <li>MD5 (メッセージ ダイジェスト 5) ハッシュ機能をもつ HMAC (Hashed Message Authentication Coding)</li> <li>SHA-1 (セキュア ハッシュ アルゴリズム) ハッシュ機能をもつ HMAC</li> </ul>
認証モード	<ul style="list-style-type: none"> <li>事前共有鍵 (Preshared Keys)</li> <li>X.509 デジタル証明書</li> </ul>
Diffie-Hellman グループ	<ul style="list-style-type: none"> <li>1</li> <li>2</li> </ul>
暗号化アルゴリズム	<ul style="list-style-type: none"> <li>56 ビット DES (データ暗号化規格)</li> <li>168 ビット トリプル DES</li> <li>AES 128 ビットおよび 256 ビット</li> </ul>
拡張認証 (XAUTH)	IKE 内でユーザを認証することができます。この認証は、IPSec 装置が相互に認証する、通常の IKE フェーズ 1 認証に追加されるものです。IKE 内の拡張認証交換は、既存の IKE 認証に代わるものではありません。
モード構成 (Mode Configuration)	ISAKMP Configuration Method と呼ばれています。
トンネル カプセル化モード	<ul style="list-style-type: none"> <li>IPSec over UDP (NAT/PAT)</li> <li>IPSec over TCP (NAT/PAT)</li> </ul>
LZS を使用した IP 圧縮 (IPCOMP)	データ圧縮アルゴリズム

## 認証機能

表 1-5 では、VPN Client でサポートされている認証機能について説明します。

表 1-5 認証機能

認証機能	説明
中央側の VPN 装置を経由したユーザ認証	<ul style="list-style-type: none"> <li>VPN 装置のデータベースを経由した内部認証</li> <li>RADIUS</li> <li>NT ドメイン (Windows NT)</li> <li>RSA (旧 SDI) SecurID または SoftID</li> </ul>
証明書管理 (Certificate Management)	証明書ストアで証明書を管理することができます。
認証機関 (CA)	PKI SCEP 登録をサポートしている認証機関

表 1-5 認証機能

認証機能	説明
スマートカードを使用した認証機能	パスコードの生成に必要な物理的な SecurID カードまたはキーチェーンフォップ
ピア証明書識別名の確認 (Peer Certificate Distinguished Name Verification)	盗用した証明書やハイジャックした IP アドレスを使用した「なりすまし」の不正なゲートウェイには接続できないようにします。ピア証明書のドメイン名の確認が失敗すると、VPN Client の接続も失敗します。