



VPN Client について

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 : Red Hat 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 Red Hat で、カーネル OS バージョン 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 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、インターネット上でセキュア接続を確立します。この接続により、バーチャル プライベート ネットワーク (VPN) が構築され、オンサイトのユーザと同じようにプライベート ネットワークにアクセスできます。

次の VPN 装置では、VPN Client から開始された VPN 接続を終端できます。

- Easy VPN サーバ機能をサポートする Cisco IOS 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 の基本動作

VPN Client は、Cisco VPN 装置と連携して、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ア接続を確立します。また、Internet Key Exchange (IKE)、および Internet Protocol Security (IPSec) というトンネリング プロトコルを使用して、セキュア接続の確立と管理を行います。

VPN 接続が確立されるときの手順は、次の通りです。

- トンネル パラメータ 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、ユーザが自社宛ての E メールをリモート PC から読む場合、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 ネットワークへのセキュアな接続を確立します。
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

この後の各表は、VPN Client の機能を示しています。

VPN Client の主な機能

表 1-1 は、VPN Client の主な機能を示しています。

表 1-1 VPN Client の主な機能

機能	説明
オペレーティングシステム	<ul style="list-style-type: none"> Linux (Intel) Solaris (UltraSPARC-32 ビットおよび 64 ビット)
接続タイプ	<ul style="list-style-type: none"> Linux は、非同期シリアル PPP、インターネットに接続されたイーサネット、および ISDN をサポートしています。 Solaris は、非同期シリアル PPP、およびインターネットに接続されたイーサネットをサポートしています。 <p> (注) VPN Client は、旧バージョンの Solaris プラットフォームで使用されていた ipdptp ダイアルアップ インターフェイスをサポートしていません。</p> <ul style="list-style-type: none"> - Solaris 6 および 7 のユーザが ipdptp ダイアルアップ インターフェイスを使用し続けるには、VPN Client バージョン 3.7 以前を使用しなければなりません。 - Solaris 8 のユーザは、サンから提供されるパッチを適用して、新しい pppd 4.0 ドライバを使用できるようにしなければなりません。 <p> (注) VPN Client では、PPP アダプタとイーサネット アダプタをそれぞれ 1 つずつのみサポートしています。</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"> RADIUS。 RSA SecurID。 VPN Server 内部ユーザリスト。 PKI デジタル証明書。 NT ドメイン (Windows NT)

プログラム機能

VPN Client では、表 1-2 に示すプログラム機能をサポートしています。

表 1-2 プログラム機能


プログラム機能	説明
サポートされているサーバ	<ul style="list-style-type: none"> • 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。
ローカル LAN アクセス	中央サイトからアクセスが認可されている場合、中央サイトの VPN Server にセキュア ゲートウェイを経由して接続している間に、ローカル LAN 上のリソースにアクセスできます。
VPN Client 自動設定オプション	構成ファイルをインポートできます。
イベント ログिंग	VPN Client ログで、表示と分析用にイベントが収集されます。
NAT 透過性 (NAT-T)	VPN Client および VPN 装置が、IPSec over UDP をいつ使用する必要があるかを自動的に検知し、PAT (ポート アドレス変換) 環境で正常に機能するようにします。
中央制御バックアップ サーバリストの更新	接続の確立時にバックアップ VPN Server リストが作成されます。この機能は VPN 装置上で設定され、VPN Client で実行されます。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 ホスト名の取得) 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。すると、VPN 装置はそのホスト名を DHCP 要求に含めて送信できるようになります。その結果、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 アドレスが追加されます。
通知	接続時の、VPN Server からのソフトウェア更新通知。
理由を示して削除	<p>接続の切断時に、VPN Client から理由コードまたは理由の説明が表示されます。VPN Client は、クライアントにより実行される接続の切断、コンセントレータにより実行される接続の切断、および IPSec の削除において、理由を示して削除する機能をサポートしています。</p> <ul style="list-style-type: none"> • GUI の VPN Client を使用している場合は、接続の切断の理由を説明するポップアップメッセージが表示されます。メッセージは、通知ログに追加され、IPSec ログ (Log Viewer ウィンドウ) に記録されます。 • コマンドラインの Client を使用している場合は、メッセージが端末に表示され、IPSec ログに記録されます。 • 接続が切断されない IPSec の削除では、イベントメッセージが IPSec ログ ファイルに記録されますが、端末には表示されません。 <p> (注) この機能がサポートされるのは、VPN 装置で 4.0 以降のバージョンのソフトウェアが実行されている場合です。</p>

表 1-2 プログラム機能 (続き)

プログラム機能	説明
単一 SA	VPN 接続ごとに単一セキュリティ結合 (SA) をサポートする機能。スプリット トンネリング ネットワークごとにホストとネットワーク間のセキュリティ結合 (SA) のペアを作成する代わりに、「ホストとすべてのネットワーク間」方式を使用します。この方式では、スプリット トンネリングが使用されているかどうかに関係なく、すべてのネットワーク トラフィックに対して、トンネルを 1 つずつ作成します。

IPSec 機能

VPN Client では、表 1-3 に示す IPSec 機能をサポートしています。


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"> • NAT と PAT に使用する IPSec over UDP。 • NAT と PAT に使用する IPSec over TCP。
鍵管理プロトコル	IKE (Internet Key Exchange)
IKE キープアライブ	ピアの継続的な存在をモニタリングし、VPN Client の継続的な存在をピアに報告するツール。これにより、ピアが存在しなくなったときに、VPN Client から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が、NAT ポートを継続的にアクティブ状態に保ちます。
スプリット トンネリング	クリア テキストのパケットは直接インターネット上で、暗号化されたパケットは IPSec トンネル経由で、同時に送信できます。トンネル トラフィックに必要なネットワーク リストが、VPN 装置から VPN Client に提供されます。ユーザは VPN Client でスプリット トンネリングを有効にし、VPN 装置でネットワーク リストを設定します。
スプリット DNS のサポート	DNS パケットを、ISP の外部 DNS のドメインにインターネット経由でクリア テキストのまま、または企業 DNS のドメインに IPSec トンネル経由で送信できます。VPN Server から VPN Client に、プライベート ネットワーク内の宛先へパケットをトンネリングするときに必要なドメイン リストが提供されます。たとえば、corporate.com 宛のパケットのクエリーは、トンネル経由でプライベート ネットワーク上の DNS に転送されます。また、myfavoritesearch.com 宛のパケットのクエリーは、ISP の DNS で処理されます。この機能は、VPN Server (VPN Concentrator) 側で設定し、VPN Client 側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

VPN Client では、表 1-4 に示す IPSec 属性をサポートしています。

表 1-4 IPSec 属性

IPSec 属性	説明
Main モードおよび Aggressive モード	ISAKMP Security Association (SA) を確立するときの Phase 1 のネゴシエートの方法。
認証アルゴリズム	<ul style="list-style-type: none"> • HMAC (Hashed Message Authentication Coding) で、MD5 (Message Digest 5) ハッシュ関数を使用するもの。 • HMAC で、SHA-1 (Secure Hash Algorithm) ハッシュ関数を使用するもの。
Authentication モード	<ul style="list-style-type: none"> • 事前共有キー。 • X.509 デジタル証明書。
Diffie-Hellman グループ	<ul style="list-style-type: none"> • 1 (DES) • 2 (DES および 3DES) • 5 <p> (注) DH グループ 5 の詳細は、『Cisco VPN Client アドミニストレータガイド』を参照してください。</p>
暗号化アルゴリズム	<ul style="list-style-type: none"> • 56 ビット DES (データ暗号化規格) • 168 ビット Triple-DES。 • AES 128 ビットおよび 256 ビット。
拡張認証 (XAUTH)	IKE 内でユーザを認証できます。この認証は、IPSec 装置が相互に認証し合う通常の IKE Phase 1 認証に追加されます。IKE 内の拡張認証交換は、既存の IKE 認証に置き換わるものではありません。
モード設定	ISAKMP Configuration Method と呼ばれます。
Tunnel Encapsulation モード	<ul style="list-style-type: none"> • IPSec over UDP (NAT/PAT) • IPSec over TCP (NAT/PAT)
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

VPN Client では、表 1-5 に示す認証機能をサポートしています。

表 1-5 認証機能

認証機能	説明
中央サイトの VPN 装置を使用するユーザ認証	<ul style="list-style-type: none">• VPN 装置のデータベースを使用する内部認証。• RADIUS。• NT ドメイン (Windows NT)。• RSA (旧 SDI) SecurID または SoftID。
証明書管理	証明書ストアの証明書を管理できるようにします。
認証機関 (CA)	PKI SCEP 登録をサポートする CA。
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。
ピア証明書の識別名の検証	VPN Client が、盗まれた有効な証明書やハイジャックされた IP アドレスを使用して無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の確認が失敗すると、VPN Client の接続も失敗します。

