VPN環境を構築する前に学んでおこう

ここが知りたいVPN

本連載では、これからリモートアクセスVPNの導入を検討している読者のために、リモートアクセスVPNに利用されている技術、すなわちIPsecやPPTP、L2TP、SSL-VPNについて、それらの技術的な特徴や違いをわかりやすく解説していく。今回は、IPsecと組み合わせたL2TP（L2TP/IPsec）を使用したリモートアクセスVPNについて説明する。

馬場達也

第5回　L2TPを使用したリモートアクセスVPNの仕組み

Supplement

■L2TP（Layer 2 Tunneling Protocol）
データリンク層のレベルでPPP通信をトンネリングするためのプロトコルで、PPTPとシスコシステムズのL2Fが統合されたものである。

■PPTP（Point-to-Point Tunneling Protocol）
マイクロソフトなどが提唱した、インターネットを利用したVPNを実現するためのプロトコル。

■L2F（Layer 2 Forwarding）
シスコシステムズが開発した、インターネットを利用したリモートアクセスVPNを実現するためのプロトコル。

■IETF（Internet Engineering Task Force）
インターネットで利用されるプロトコルなどの技術を標準化する団体。標準化された技術仕様は、RFC（Request For Comments）として公開される。

■PPP（Point-to-Point Protocol）
電話回線などを使用して、コンピュータをインターネットなどのネットワークへダイヤルアップ接続するのに一般的に使われるデータリンク層プロトコル。上位プロトコルとして、TCP/IPなどさまざまなネットワーク層プロトコルを運ぶことができる。

■IPsec（IP Security）
IPパケットレベルで認証や暗号化を行うことのできるセキュリティプロトコル群。

PPTPとL2Fを統合し標準化されたトンネリングプロトコルのL2TP

L2TPは、マイクロソフトが中心となって開発した**PPTP**と、シスコシステムズが開発した**L2F**を統合し、**IETF**で標準化された、**PPP**フレームをIPネットワーク上で交換できるようにするためのトンネリングプロトコルである。L2TPの仕様は、RFC 2661に記述されている。

PPTPでは、制御用のプロトコルとデータ用のプロトコルとで異なるプロトコルを使用していたが、L2TPでは、L2TP制御メッセージとL2TPデータメッセージの両方に、L2Fと同じUDPの1701番ポートを使用する。しかし、L2TPにはセキュリティを確保する機能が存在しないため、通常は**IPsec**と組み合わせることでセキュリティを確保する。IPsecを利用してセキュリティを確保したL2TPは、L2TP/IPsecと呼ばれ、その仕様はRFC 3193に記述されている。

トンネリングや暗号化、認証機能を利用できるL2TP/IPsec

L2TP/IPsecによって提供される機能を次にまとめてみる。

■トンネリング機能

L2TPのトンネリング機能によって、インターネット経由でPPP接続することができるようになり、VPNを構築することが可能となる。L2TPでは、PPPフレームをUDPでカプセル化する（図1）。PPPはダイヤルアップ接続などの際に使用されるデータリンク層のプロトコルであり、PPP上ではIPを含むさまざまなネットワーク層プロトコルを使用できる。

L2TPヘッダのフォーマットは、図2のようになる。T（Type）ビットにはメッセージタイプが入り、「0」の場合はデータメッセージ、「1」の場合は制御メッセージとなる。L（Length）ビットが「1」の場合は長さフィールドが存在し、長さフィールドには、L2TPメッセージのサイズ（バイト数）が入る。S（Sequence）ビットが「1」のときはNsおよびNrフィールドが存在する。Nsフィールドには送信するL2TPデータメッセージまたはL2TP制御メッセージのシーケンス番号、Nrフィールドには次に受信する予定のL2TPデータメッセージまたはL2TP制御メッセージのシーケンス番号が入る。O（Offset）ビットが「1」のときはオフセット長フィールドが存在し、パディングの長さが調整される。P（Priority）ビットが「1」の場合は、パケットの送信が優先される。また、バージョンフィールドには「2」が入る（「1」はL2Fが使用する）。トンネルIDフィールドにはL2TPトンネルの識別子が入り、セッションIDにはそのL2TPトンネル内のセッションの識別子が入る。

図1● L2TPではPPPフレームをUDPでカプセル化する

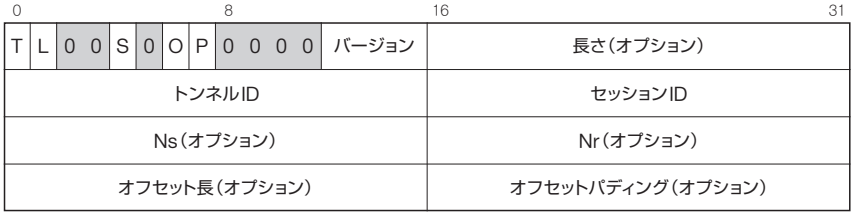

図2● L2TPヘッダのフォーマット

■ネットワーク情報自動設定機能

L2TPでは、PPPの**IPCP**によって提供されるネットワーク情報自動設定機能を使用することができる。L2TPクライアントはIPCPを介して、L2TPサーバから自分に割り当てられる内部IPアドレス、内部DNSサーバのアドレス、内部WINSサーバのアドレスを取得することができる。

■暗号化機能

L2TPには暗号化機能が備わっていないため、IPsecの**ESP**を組み合わせて使用する。ESPによりL2TPパケット全体が暗号化されるため、送信するデータを含むL2TPデータメッセージに加えて、L2TP制御メッセージの内容も暗号化される。

■メッセージ認証機能

L2TP/IPsecではIPsecの機能により、メッセージ認証コード（**MAC**）を使用してデータの完全性が確保される。このため第3者によってデータが改ざんされても、それを検知することが可能となる。

■鍵交換機能

L2TP/IPsecでは、IKEにより鍵交換機能が提供される。

■ユーザー認証機能

L2TPでは、PPPのユーザー認証機能を使用することができる。ユーザー認証方式としては、**PAP**、**CHAP**、**MS-CHAP**、**MS-CHAP v2**、**EAP-TLS**などのPPP認証プロトコルを利用できる。PAP、CHAP、MS-CHAP、MS-CHAP v2は、ユーザー名とパスワードを使用してユーザーを認証するものであり、EAP-TLSは、証明書を使用してユーザーを認証する。

なお、PAP、CHAP、MS-CHAPには、ユーザー側の認証だけを行いサーバ側の認証は行わないという問題があるため、MS-CHAP v2またはEAP-TLSを使用することが推奨されている。

■リプレイ防御機能

L2TP/IPsecではIPsecの機能により、送信されるパケットにシーケンス番号が付与される。このため、悪意のある第3者が、正規のユーザーが送信したIPsecパケットをコピーして再び利用する「リプレイ攻撃」から防御することができる。

また、次の機能はL2TP/IPsecでは利用できない。

■スプリットVPN機能

L2TP/IPsecでは、スプリットVPN機能は提供されない。このため、インターネットあてのアクセスであっても、すべてのアクセスはVPN経由で行われる。

まずIPsec SAを確立 次にL2TP制御コネクションを確立

それでは、L2TP/IPsec接続時の処理を説

Supplement

■IPCP
（Internet Protocol Control Protocol）
PPPにてTCP/IPを利用する際に用いられるIP制御プロトコル。IPアドレスやヘッダなどの圧縮方法の設定を行う。

■ESP
（Encapsulating Security Payload）
IPsecで使用されるプロトコル。IPパケットの改ざん検出や機密性を確保するための機能を持つ。

■MAC
（Message Authentication Code）
ハッシュ関数と認証鍵を使用して生成されるもので、送信するメッセージに添付される。これにより受信者はメッセージの改ざんを検出できる。

■PAP
（Password Authentication Protocol）
PPPにおいて利用される認証プロトコル。認証時に利用されるパスワードなどは通信経路上を平文のまま送信される。

■CHAP
（Challenge Handshake Authentication Protocol）
PPPにおいて利用される認証プロトコルの1つで、サーバから送信されたチャレンジと呼ばれる乱数文字列とパスワードを組み合わせたものにハッシュを適用することによってレスポンスを生成し、その結果をサーバに送信する。レスポンスが盗聴されても、その内容から実際のパスワードは知ることはできない。

■MS-CHAP
（Microsoft Challenge Authentication Protocol）
マイクロソフトがCHAPを拡張して作成した認証プロトコル。

■MS-CHAP v2
（MS-CHAP version 2）
MS-CHAPの新しいバージョン。MS-CHAP v2では、相互認証やより強力な初期データ暗号化キーが利用可能となっている。

■EAP-TLS
（Extensible Authentication Protocol-Transport Layer Security）
PPPを拡張した認証プロトコルの1つで、認証方式としてTLSを使用する。電子証明書を利用してサーバとクライアントで相互認証を行うことができる。

Supplement

■LCP（Link Control Protocol）
PPPにおけるコネクションの確立や切断、さらに認証プロトコルやパケット情報の設定などを行うプロトコル。

■CCP（Compression Control Protocol）
PPP接続時におけるデータ圧縮や、データ圧縮のネゴシエーション方法を規定するプロトコル。

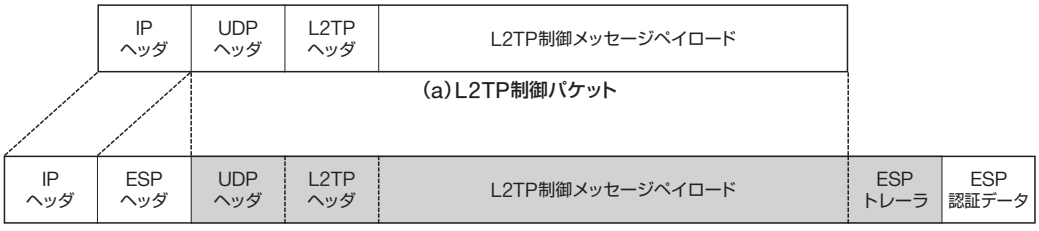

図3● L2TP/IPsecでのL2TP制御パケットフォーマット（網掛け部は暗号化されている）

明しよう。L2TP/IPsecの接続は、L2TPトラフィックをIPsecで保護するため、まずIPsec SAを確立する。IPsec SAの確立手順は、本誌2004年4月号の本連載第2回で説明した手順と同じなので、ここでは省略する。

L2TP/IPsecにおいては、L2TPによってトンネリングが行われる。このため、IPsecではトンネルモードではなくトランスポートモードが使用される。また、暗号化が必要となるためESPが使用される。さらに、L2TP/IPsecパケットがNATを通過するためには、本誌2004年5月号の本連載第3回で紹介した「IPsec NATトラバーサル」機能が必要となるので注意が必要だ。

IPsec SAが確立されると、IPsec SA上でL2TPトンネル（L2TP制御コネクション）が構築され、さらにトンネル内でPPPフレームを流すためのコールセッションが確立される。この際に、図3のようなL2TP制御メッセージが交換される。

L2TP接続時の処理は、本誌2004年6月号の本連載第4回で説明したPPTPと非常によく似ている（図4）。まずL2TPクライアントは、L2TPサーバの1701/UDPポートに接続し、L2TPの制御メッセージである「Start-Control-Connection-Request」メッセージを発行して、L2TP制御コネクションの確立を要求する。このときクライアントは、サーバからクライアントに送信するL2TPパケットに付与するトンネルIDを指定する。これに対してL2TPサーバは、「Start-Control-Connection-Reply」メッセージを返答する。このメッセージでは、クライアントからサーバに送信するL2TPパケットに付与するトンネルIDを指定する。その後、L2TPクライアントが「Start-Control-Connection-Connected」を送信することで、L2TP制御コネクション（L2TPトンネル）が確立される。L2TPサーバはこの返答として、ACKを示すデータ部から空のL2TPメッセージ（ZLB ACK）を送信する。

続いてL2TPクライアントは、L2TPサーバから送信されるL2TPデータパケットに付与するセッションIDを指定した「Incoming-Call-Request」メッセージを発行する。これに対してL2TPサーバは、クライアントから送信されるL2TPデータパケットに付与するセッションIDを指定した「Incoming-Call-Reply」メッセージを返答する。その後、L2TPクライアントは「Incoming-Call-Connected」メッセージをL2TPサーバに送信し、L2TPサーバがZLB ACKを返答する。これにより、L2TPクライアントとL2TPサーバの間でL2TPコールセッションが確立され、PPPフレームを送信することができるようになる。

このコールセッションは、同じL2TPトンネルの中に複数確立することが可能である。L2TPコールセッションが確立されると、PPPの**LCP**によって利用する認証プロトコルなどのPPPパラメータのネゴシエーションが行われる。利用する認証プロトコルがネゴシエーションされると、その認証プロトコルを使用してユーザー認証が行われる。さらにPPPの**CCP**により、圧縮を行うかどうかのネゴシエーションが行われる。また、このCCPのネゴシエーションと並行して、L2TPクライアントはPPPのIPCPを利用し、L2TPサーバから内部IPアドレスの割り当てや内部DNSサーバ、内部WINSサーバのアドレスの通知を受ける。

Supplement

ここまでの処理は、すべてIPsecのESPによりセキュリティが確保されているため、PPTPのように盗聴によってネゴシエーションの情報が外部に漏れる心配はない。

L2TPの接続が完了すると、IPパケットなどのデータを含むPPPフレームを送信できるようになる。IPパケットをL2TPコールセッションを使用して送信する場合は、まず送信するIPパケットの直前にPPPヘッダが付加され、PPPフレームが作成される（図5）。次にL2TPトンネルのエンドポイント間を運ぶためのトンネルIPヘッダとUDPヘッダ、L2TPヘッダが付加され、PPPフレームをカプセル化したL2TPパケットが作成される。さらに、この作成されたL2TPパケットに対しトランスポートモードのESPが適用される。

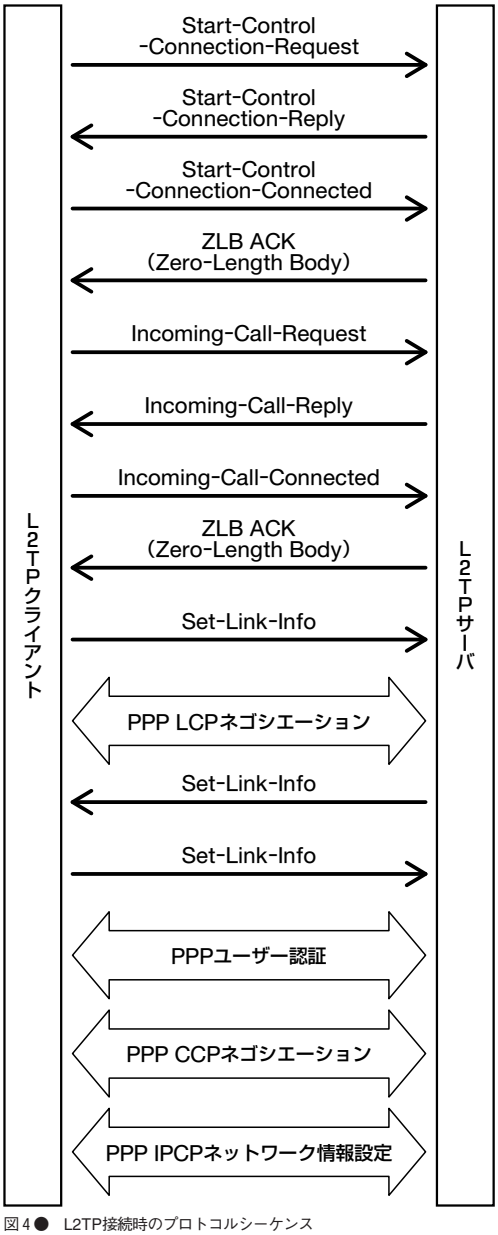

図4● L2TP接続時のプロトコルシーケンス

PPP切断とL2TP制御コネクション切断によりL2TP接続は終了する

次にL2TP終了時の処理を見ていこう（次ページの図6）。まずL2TPクライアントはL2TP制御コネクションを使用して、L2TPサーバに対し「Set-Link-Info」メッセージを送信する。次にL2TPコールセッションを使用して、PPPのリンク制御プロトコル（LCP）の「Terminate-Request」メッセージを送信し、PPP接続の切断を要求する。これに対してL2TPサーバは、L2TP制御コネクションを使用して、L2TPクライアントに「Set-Link-

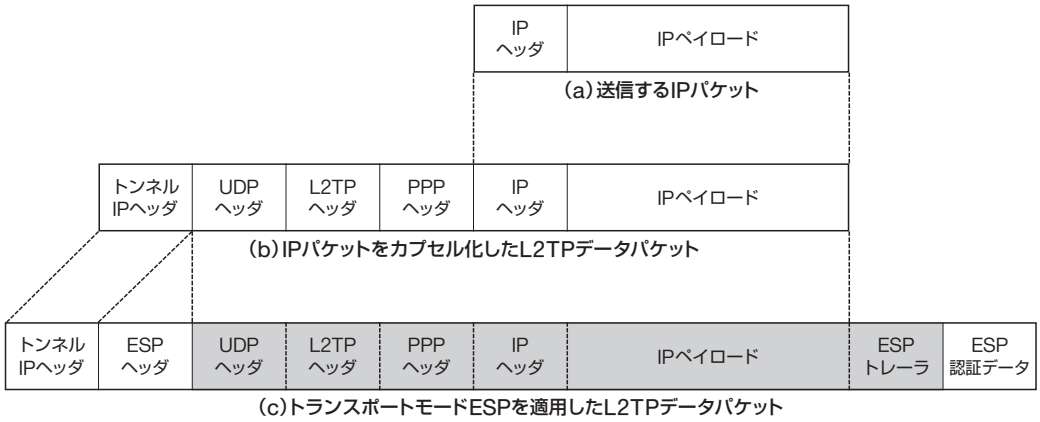

図5● L2TP/IPsecでのIPパケット送信時のフォーマット（網掛け部は暗号化されている）

Supplement

■RADIUS（Remote Authentication Dial In User Service）
米国リビングストンが開発した、ダイヤルアップユーザー認証方式。RFC 2138/2139にて標準化されている。ユーザー情報をデータベースで管理する。

■NAT（Network Address Translator）
IPパケット中のIPアドレスを変換する機能。この機能により、プライベートアドレスが割り当てられたノードから透過的に、グローバルアドレスが用いられるインターネットへのアクセスが可能となる。

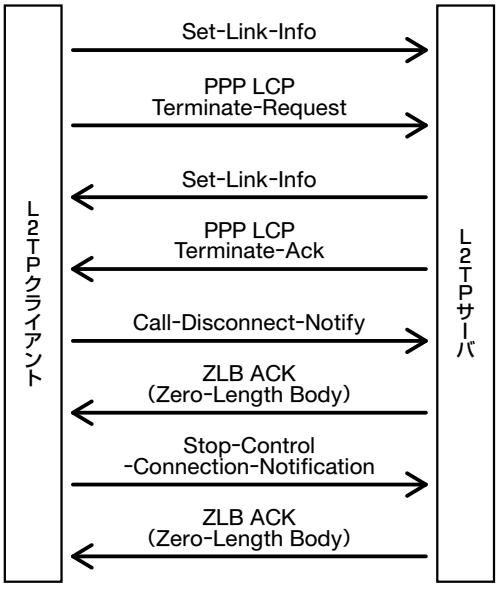

図6● L2TP終了時のプロトコルシーケンス

Info」メッセージを送信する。さらにサーバは、L2TPコールセッションを使用して、さきほどの「Terminate-Request」メッセージの返答として、LCPの「Terminate-Ack」メッセージを送信し、PPP接続を切断する。

その後L2TPクライアントは、L2TP制御コネクションを使用して、L2TPサーバに対し、L2TPコールセッションの切断を通知するための「Call-Disconnect-Notify」メッセージを送信する。これに対してL2TPサーバは、ZLB ACKをクライアントに返答する。さらにL2TPクライアントは「Stop-Control-Connection-Notification」メッセージを送信して、L2TP制御コネクションの切断を通知する。これに対してL2TPサーバは、ZLB ACKをL2TPクライアントに送信し、L2TP制御コネクションを切断する。

リモートアクセスVPNでL2TP/IPsecを利用する際の注意点

L2TP/IPsecを使用したリモートアクセスVPNを導入する場合は、企業ネットワーク側にL2TP/IPsec-VPNを確立するためのL2TPサーバや、ユーザー認証を行うための**RADIUS**サーバが必要となる（図7）。ただし、多くのL2TPサーバ製品にはRADIUSサーバと同等の機能が組み込まれているので、導入する製品の機能を事前にチェックしておくとよいだろう。

また、使用するL2TPサーバ製品がWindows標準のL2TP/IPsecクライアントに対応していない場合は、対応したクライアントソフトウェアをリモートアクセス端末にあらかじめインストールする必要がある。さらにこのクライアントソフトウェアには、L2TPサーバのアドレスなどの情報を設定しなければならない。しかし製品によっては、このような設定をすでに行った状態のインストール用プログラムを配布することができるものも多いので、この点も製品を選択するためのポイントとなるだろう。

また、ファイアウォールではIKE（500/UDP）およびESP（IPプロトコル番号50）に加えて、**NAT**が存在した場合のために、カプセル化ESP（4500/UDP）の通過を許可する必要がある。

よりセキュアな通信を提供するが環境を整えるために準備が必要

ここまで、L2TP/IPsecのリモートアクセスVPN機能について述べてきたが、最後にL2TP/IPsecを使用したリモートアクセスVPNの長所と短所についてまとめたい。

■長所

- **L2TPによりPPPフレームをカプセル化できるので、IPを使用するアプリケーションはもちろん、IPXやAppleTalkなどのプロトコルを使用したアプリケーションにおいても安全な通信が実現できる。**
- **IPsecでは、使用する暗号化アルゴリズムや認証アルゴリズムが容易に追加できる仕組みになっているため、使用しているアルゴリズムにセキュリティ上の欠陥が見つかっても、別の強力なアルゴリズムに容易に乗り換えることができる。**

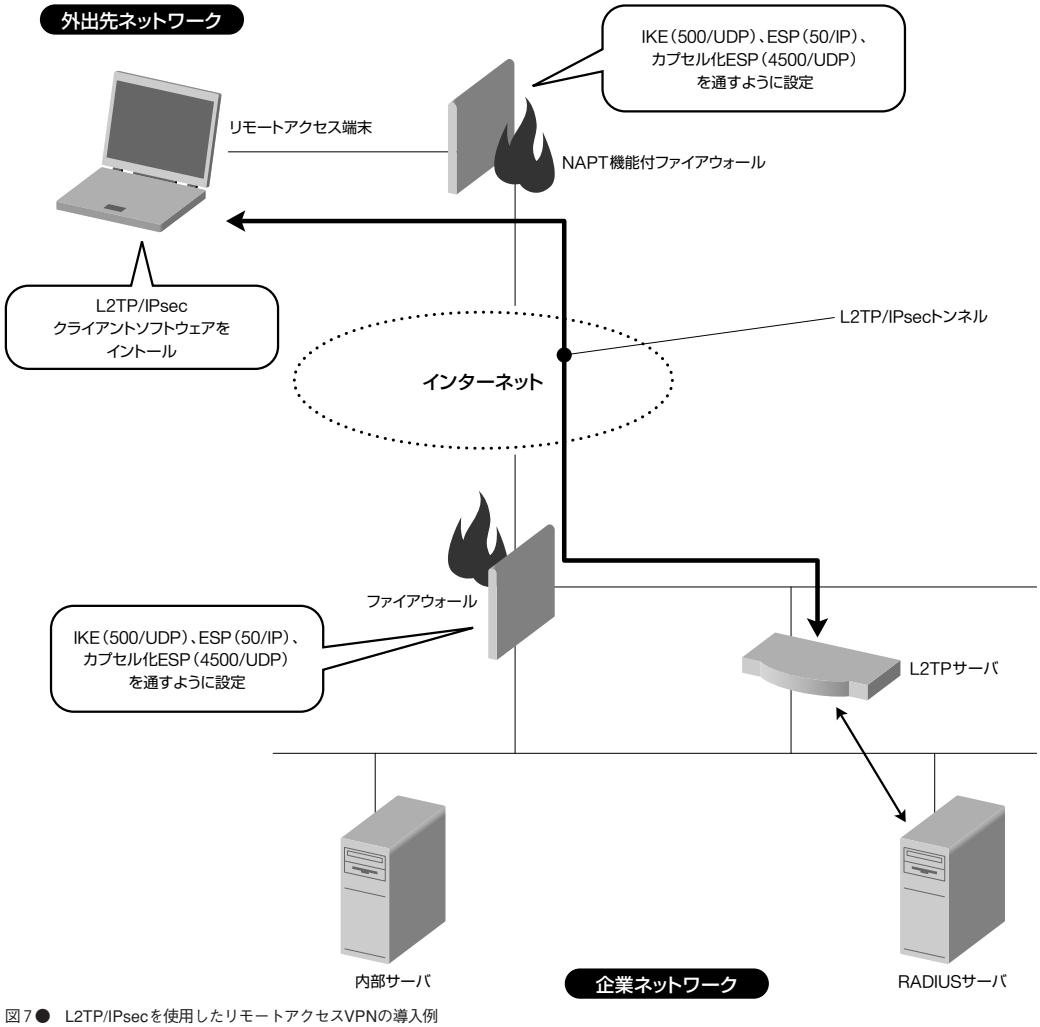

図7● L2TP/IPsecを使用したリモートアクセスVPNの導入例

・IETF標準のプロトコルであるため、異なるベンダーの製品でも相互接続可能な場合が多い（相互接続可能かどうかは各ベンダーに問い合わせてほしい）。特に、Windows 2000/XP標準のL2TP/IPsecクライアントや、マイクロソフトから提供されているWindows98/Me/NT用の「Microsoft L2TP/IPSec VPN client」との接続を保証しているL2TPサーバ製品が多い。

■短所

・OS標準のL2TP/IPsecクライアントと相互接続が保証されていないL2TPサーバ製品を使用する場合は、すべてのリモートアクセス端末に、指定されたL2TP/IPsecクライアントソフトウェアをインストールしておく必要がある。
・ファイアウォールをまたぐ場合、ESP（IPプロトコル番号50）およびIKE（500/UDP）の通過を許可する設定が必要である。またNATを介する場合は、4500/UDPを通すように設定する必要がある。これらの設定が行われていない場合、リモートアクセスユーザーが目的のネットワークへVPN接続することはできない。

以上、L2TP/IPsecを用いたリモートアクセスVPNについて述べた。次回は「SSL-VPN」について解説する。

NTTデータ　馬場達也

Supplement

■IKE（Internet Key Exchange）
セキュリティポリシーの内容を基にして、SA（セキュリティアソシエーション）を自動的に確立するためのプロトコル。IKEは、相手認証方式、SAのネゴシエーション、共有秘密鍵の管理といった主に3つの機能を提供する。