VPN環境を構築する前に学んでおこう

これが知りたいVPN

本連載では、これからリモートアクセスVPNの導入を検討され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のリモートアクセス機能について説明する。　馬場達也

第3回　リモートアクセスVPNにIPsecを利用する

Supplement

■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。

■VPN（Virtual Private Network）
インターネットなどの公衆回線を仮想的な専用回線として利用することでセキュアな通信路を確保するための技術。

■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。

■IKE-CFG（The ISAKMP Configuration Method）
リモートアクセスでIKEを利用するために拡張されたもので、主にネットワーク情報やセキュリティポリシーの管理などを行う。

■DHCP（Dynamic Host Configuration Protocol）
ネットワーク上のクライアントに、IPアドレスやサブネットマスク、ゲートウェイ、DNSサーバのIPアドレスなどのネットワーク情報を動的に割り当てるプロトコル。

■XAUTH（Extended Authentication within IKE）
IKEプロトコルを拡張したもので、ワンタイムパスワードやRADIUSを利用したユーザー認証を行うもの。

IPsecのリモートアクセス機能はIKEを拡張して提供される

前回はIPsecの基本機能について解説した。その中で、リモートアクセスVPN環境に必要となる「ネットワーク情報自動設定機能」と「ユーザー認証機能」がIPsecには実装されていないことについて触れた。実は、これらの機能については、IKEの仕様を拡張することによって実現されている。

今回は、ネットワーク情報の自動設定を実現する「mode-cfg（IKE-CFG）」および「IPsec-DHCP」、ユーザー認証を実現する「XAUTH」、さらにリモートアクセスの際に必要となるNATを越えてIPsec通信を行うための技術「IPsec NATトラバーサル」について解説する。

mode-cfgはリモートアクセス端末にネットワーク情報を自動設定する

企業ネットワーク内で使用する内部ネットワーク情報をリモートアクセス端末に自動設定する仕組みとして、多くのリモートアクセス用IPsec製品で採用されているのがmode-cfgである。mode-cfgはIKEを拡張したプロトコルであり、前回解説したIKEのフェーズ1とフェーズ2の間に行われる。mode-cfgを使用することで、企業ネットワークに関するネットワーク情報をリモートアクセス端末に通知し、企業ネットワークへ接続できるようになる。通知するネットワーク情報は次のとおりだ。

- クライアントに割り当てる内部アドレスおよびネットマスク（IPv4/IPv6）
- 割り当てた内部アドレスの有効期間（秒）
- 内部DNSサーバのアドレス（IPv4/IPv6）
- 内部WINSサーバのアドレス（IPv4/IPv6）
- 内部DHCPサーバのアドレス（IPv4/IPv6）
- 内部ネットワークアドレス（IPv4/IPv6）

mode-cfgを使用する場合、IKEの動作は次のようになる。まずリモートアクセス端末と企業ネットワークのセキュリティゲートウェイの間で、IKEのフェーズ1が行われる。フェーズ1が完了すると、リモートアクセス端末はmode-cfgで定義されたISAKMP_CFG_REQUESTメッセージに、通知を要求するネットワーク情報を指定してセキュリティゲートウェイへ送信する（図1）。

例えば内部IPアドレスやネットマスク、内部DNSサーバのアドレスを要求する場合、リモートアクセス端末はISAKMP_CFG_REQUESTメッセージに「INTERNAL_IP4_ADDRESS」「INTERNAL_IP4_NETMASK」「INTERNAL_IP4_DNS」といった属性を指定してセキュリティゲートウェイへ送信する。このようにして、IPアドレスの割り当てやネットマスクおよび内部DNSサーバのアドレスの通知をセキュリティゲートウェイに要

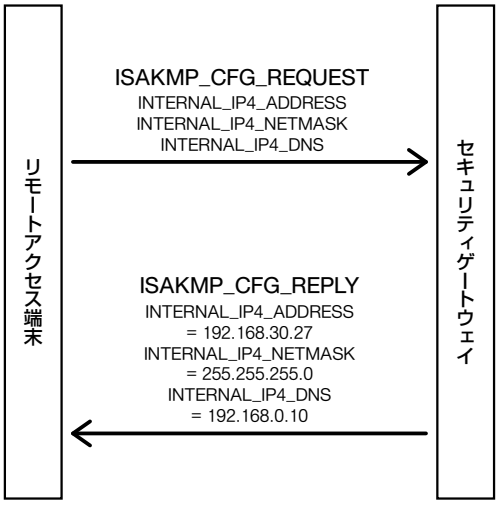

図1● mode-cfgによりネットワーク情報を通知（クライアント主導型）

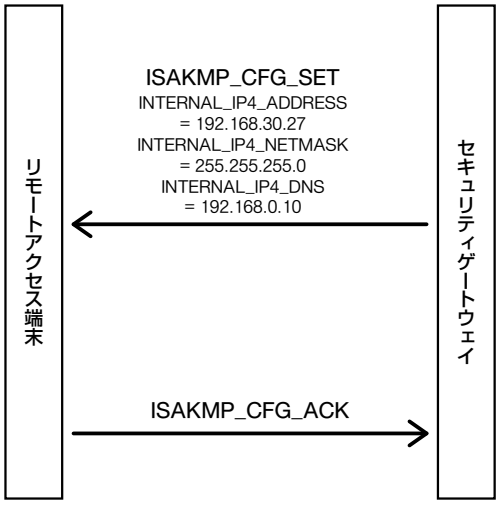

図2● mode-cfgによりネットワーク情報を通知（ゲートウェイ主導型）

求する。これらを受信したセキュリティゲートウェイは、リモートアクセス端末用の内部IPアドレスを確保し、ISAKMP_CFG_REPLYメッセージを使用して要求されたネットワーク情報をリモートアクセス端末へ返答する。

このmode-cfgの交換内容は、フェーズ1で確立されるISAKMP SAによって保護される。また、セキュリティゲートウェイ側からmode-cfgを開始することもできる（図2）。その場合はISAKMP_CFG_SETメッセージに、さきほどのISAKMP_CFG_REPLYメッセージと同じくリモートアクセス端末に設定するネットワーク情報を格納して送信する。これを受信したリモートアクセス端末は、その内容を確認してセキュリティゲートウェイにISAKMP_CFG_ACKメッセージを返すという流れだ。

mode-cfgの交換が完了したあとは、通常どおりIKEのフェーズ2が行われてIPsecトンネルが構築される。リモートアクセス端末が企業ネットワークへアクセスする際、mode-cfgによって設定された内部IPアドレスを送信元IPアドレスとして使い、IPsecトンネルを経由する。

またmode-cfgでは、セキュリティゲートウェイによって保護されている内部ネットワークアドレスをリモートアクセス端末へ通知することができるため、これを利用してスプリットトンネリング機能を実現することができる。例えば内部ネットワークアドレスとして「10.0.0.0/255.0.0.0」（「255.0.0.0」はネットマスク）が通知された場合、このアドレスに対してはVPN経由でアクセスし、それ以外のアクセスはVPNを経由せずにインターネットへ直接アクセスするといったことができるのだ。

ただしDNSの名前解決については、たとえリモートアクセス端末がインターネット上にあったとしても、必ずmode-cfgで通知された内部DNSサーバへ問い合わせてしまう。この問題を解決するために、例えばシスコシステムズの「VPN 3000シリーズ」や「Cisco VPN Client」などでは、mode-cfgで通知する項目として「Split Tunneling Network」や「Split DNS Name」を独自に追加している。これらによってリモートアクセス端末は、Split Tunneling Networkで通知されたネットワークアドレスへアクセスする場合や、Split DNS Nameで通知されたドメイン名の名前解決をする場合だけVPN経由でアクセスし、そのほかのアクセスはVPNを経由せずに直接インターネットへアクセスできるようになる。

DHCPを利用してリモートアクセス端末にネットワーク情報を通知する IPsec-DHCP

ここまでで、mode-cfgによってリモートア

Supplement

■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。

クセスに必要なネットワーク情報を設定することが可能なことがわかった。しかし、mode-cfgはIKE自身の仕様を変更するものであるため、この機能は標準のものとなっていない。その代わりとして、DHCPを用いることで、内部ネットワークのIPv4アドレスをリモートアクセス端末に仮想的に割り当てるIPsec-DHCPがRFC 3456として標準化されている。

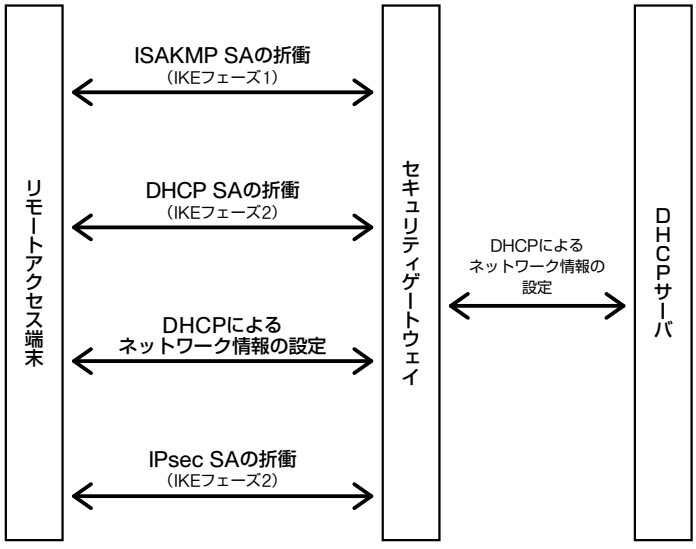

図3● IPsec-DHCPではDHCP SAでDHCPメッセージを保護する

IPsec-DHCPによる処理の手順は次のとおりである（図3）。まずリモートアクセス端末は、企業ネットワークのセキュリティゲートウェイとの間でIKEのフェーズ1を行い、その後フェーズ2において、DHCP SAと呼ばれるDHCPメッセージを交換するためだけに利用される一時的なIPsecトンネルを確立する。リモートアクセス端末は、このDHCP SAを使用してDHCPメッセージの交換を行い、企業ネットワークのDHCPサーバから内部IPアドレスの割り当てを受ける。DHCPメッセージを交換する際、セキュリティゲートウェイはリモートアクセス端末とDHCPサーバとの間でDHCPトラフィックを中継するDHCPリレーとして動作する。DHCPの設定が完了するとDHCP SAは削除され、続いてIKEのフェーズ2によってIPsecトンネルが確立される。リモートアクセス端末はDHCPサーバから割り当てられた内部IPアドレスを使用し、IPsecトンネルを経由して企業ネットワークへアクセスすることになる。

XAUTHはIPsecにユーザー認証機能を提供する

リモートアクセスでは、ワンタイムパスワードやチャレンジレスポンスなどのPKIを使用しないレガシー認証システムが多く利用されている。しかし、IKEはこういった認証システムを利用する機能を持たない。したがって、IKEの相手認証にレガシー認証システムを利用するために、IKEを拡張したXAUTHプロトコルが多くのIPsec製品で使用されている。XAUTHでは、通常のパスワードによる認証のほか、RFC 2138で定義された**RADIUS-CHAP**やRFC 2289で定義された**OTP**などの認証方式を利用できる。

XAUTH認証の際は、まずIKEのフェーズ1においてXAUTHを実装していることを示すベンダーIDペイロードを交換する。次にIKEの相手認証方式としてXAUTHの使用が確認され、フェーズ1が完了した後にXAUTH交換を行う。XAUTHに加えmode-cfgまたはIPsec-DHCPを利用する場合は、XAUTHによる認証が完了した直後にはmode-cfgやIPsec-DHCPを行う（図4）。

XAUTHを利用する時は、通常のIKEのフェーズ1で行われる相手認証に加えXAUTHによるユーザー認証を行う。XAUTH認証におけるIKEのフェーズ1の認証では、通常、事前共有鍵（pre-shared key）認証が使用される。

ユーザー認証において、通常のパスワードやSecurIDなどの認証トークンを利用する場

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。

■CHAP（Challenge Handshake Authentication Protocol）
PPPにおいて利用される認証プロトコルのひとつで、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。

■OTP（One-Time Password Authentication System）
1度きりのパスワードを用いてサーバとクライアントでの認証を行う方式。サーバがクライアントへ「チャレンジ」と呼ばれる文字列を送信し、クライアントはそのチャレンジとパスワードを利用して「レスポンス」と呼ばれる文字列を生成してサーバへ送信する。サーバはレスポンスを解析することでクライアントが正規ユーザーであるかどうかを判断する。サーバが発行するチャレンジは毎回違うものとなる。

合は次のようになる(図5)。IKEのフェーズ1の完了後、セキュリティゲートウェイがリモートアクセス端末へISAKMP_CFG_REQUESTメッセージを発行してユーザー名とパスワードを要求する。これに応答して、リモートアクセス端末はISAKMP_CFG_REPLYメッセージを使ってユーザー名とパスワードを送信する。セキュリティゲートウェイはこれらの内容をRADIUSサーバへ送信して認証を行う。認証に成功した場合は、セキュリティゲートウェイはISAKMP_CFG_SETメッセージによってOKステータスを通知する。最後に、リモートアクセス端末が確認のためのISAKMP_CFG_ ACKメッセージを送信して認証が完了となる。

また、ユーザー認証にRADIUS-CHAP方式を使用する場合は次のようになる(図6)。まずセキュリティゲートウェイがリモートアクセス端末に対し、ISAKMP_CFG_REQUESTメッセージを使用してチャレンジの送信とユーザー名およびパスワードの要求を行う。リモートアクセス端末は受信したチャレンジからレスポンスを生成し、ISAKMP_CFG_REPLYメッセージによってユーザー名とパスワード(レスポンス)を送信する。認証が成功すれば、セキュリティゲートウェイはISAKMP_CFG_SETメッセージによってOKステータスを通知する。最後に、リモートアクセス端末が確認のためにISAKMP_CFG_ACKメッセージを送信して認証が完了する。

IPsec NATトラバーサルはNATを介してのIPsec通信を実現する

IPsecはNATとの相性が非常に悪い。これは、NATは通信経路の途中でパケットの情報を変換してしまうが、IPsecでは途中でデータの内容が書き換えられると、データが改ざんされたと判断してパケットを破棄してしまうからだ。

NATにはさまざまな種類があるが、通常よく利用されるものは「**NAPT**」と呼ばれるも

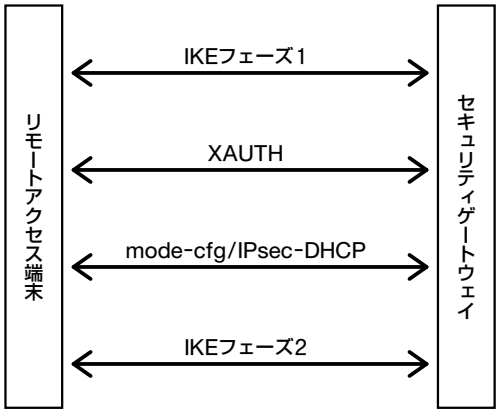

図4● XAUTHはIKEフェーズ1の直後に行われる

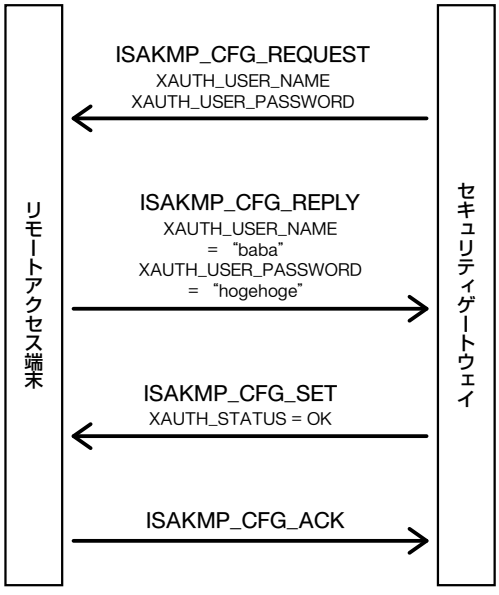

図5● XAUTHによる通常のパスワード認証の手順

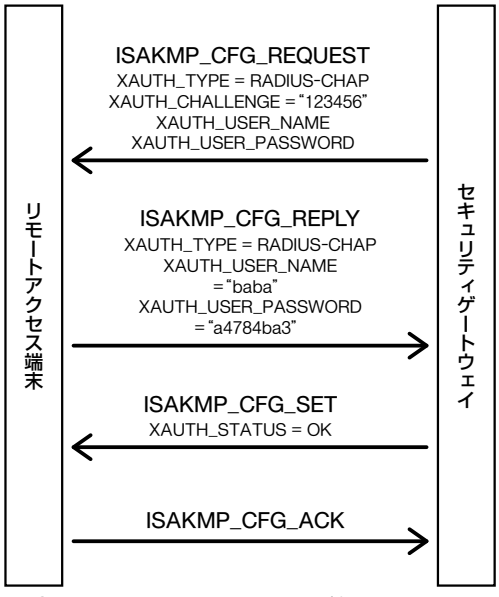

図6● XAUTHによるRADIUS-CHAP認証の手順

Supplement

■NAPT
(Network Address Port Translation)
NATと同様に、IPパケット中のIPアドレスを変換する機能。IPマスカレードとも呼ばれる。NATと異なるのはIPアドレスに加えポート番号も変換される点である。これにより1つのグローバルアドレスを複数のプライベートネットワーク内のホストで共有できる。

Supplement

■ICMP（Internet Control Message Protocol）
RFC792で定義されたTCP/IPプロトコルにおける制御用のプロトコル。TCP/IPパケットの転送中に発生するさまざまなエラーの通知や、ホスト状態の確認などに利用される。

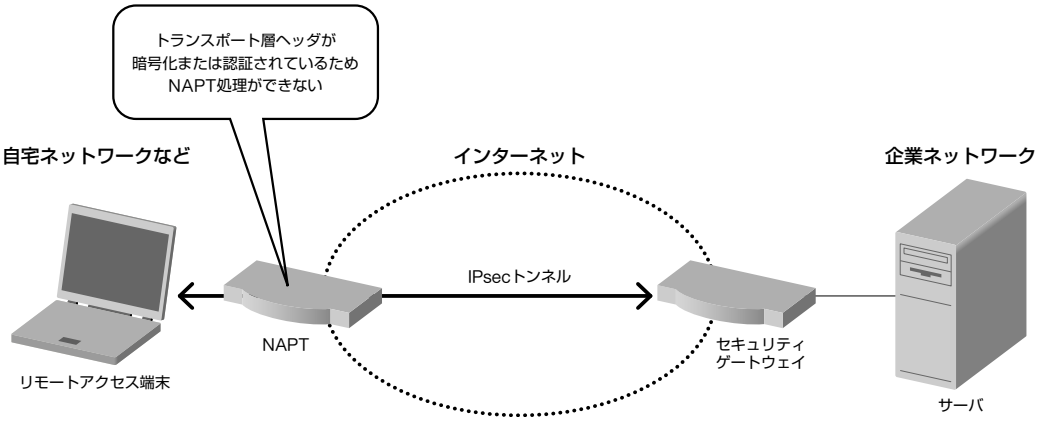

図7● NAPTを介してIPsecパケットをやり取りする場合には問題が発生する

ので、複数のアドレスを1つのアドレスに変換するものだ。NAPTでは返答パケットを元のアドレスに変換できるように、パケットの送信元IPアドレスとともに送信元ポート番号（**ICMP**であればクエリID）も変換する。またIPヘッダのアドレスを変換する際、TCPやUDPヘッダのチェックサムも同時に変更する。

ここで、リモートアクセス端末がNAPT配下に存在する場合を考えてみよう（図7）。この場合、IPsecを適用したパケットがNAPTを通過することになる。しかし通過するパケットのトランスポート層ヘッダは、暗号化または認証されているため、送信元ポート番号やチェックサムは変更できない。このため、TCPヘッダまたはUDPヘッダの送信元ポート番号を変換するNAPTはIPsecパケットに適用できないのだ。

この問題を解決する技術として、現在「IPsec NATトラバーサル」が標準化されつつある。NAPTを含めあらゆるNATを通過させるには、TCPまたはUDPで使用されるポート番号が必要である。IPsec NATトラバーサルでは、IPsecパケットをUDPでカプセル化することでこの問題を解決している。IPsec NATトラバーサルは、まだRFCとして発行されていないがほぼ仕様が確定しており、すでにさまざまなIPsec製品に実装されている。

IPsec NATトラバーサルを利用するには、通信する各機器がこの機能を実装している必要がある。自分の端末がIPsec NATトラバーサルを実装している場合、フェーズ1の最初の交換でこの機能を実装していることを示すベンダーIDペイロードを相手へ送信する。互いにIPsec NATトラバーサルを実装していることを確認すると、フェーズ1の次の交換時に、両者の間にNATが存在するかどうかを調べるため、IKEパケットで使用する送信元IPアドレスおよび送信元ポート番号のハッシュ値と、宛先IPアドレスおよび宛先ポート番号のハッシュ値を含むNAT-D（NAT Discovery）ペイロードをそれぞれが相手へ送信する。

NAT-Dペイロードに含まれているハッシュ値と受信したパケットのIPアドレスおよびポート番号から生成したハッシュ値が異なる場合は、経路上にNATが存在すると判断できる。NATが存在する場合には、IKEのポートを500から4500に変更してフェーズ1の最後の交換とフェーズ2を行う。フェーズ2では、自分と相手のIPアドレスを含むNAT-OA（NAT Original Address）ペイロードを交換する。これによって受信側は、NATで変換される前のオリジナルの送信元IPアドレスを知ることができる。さらにフェーズ2完了後、ESPを4500番ポートのUDPでカプセル化して送信する（図8）。受信側でTCPやUDPのチェックサムを検証する際は、NAT変換後の送信元IPアドレスではなく、フェーズ2のNAT-OAペイロードで交換されるオリジナルの送信元IPアドレスを使用する。

IKEの次バージョン「IKEv2」ではリモートアクセス用機能が標準に

現在IETFでは、IKEの後継であるIKEv2について議論されている。IKEv2では、これまで述べたようなリモートアクセス用の機能が標準装備される予定である。

内部ネットワーク情報の自動設定については、mode-cfgの機能がIKEv2の「設定ペイロード（Configuration Payload）」として実装される予定だ。またユーザー認証については、新たに「**EAP**ペイロード」を定義し、RFC 2284で定義されたEAPがIKEv2で利用可能となる予定である。さらに、IPsec NATトラバーサルの機能も標準で組み込まれる予定だ。

このように、IKEv2の仕様がRFCとして発行され各製品に実装されるようになれば、リモートアクセスVPNに必要な機能が標準で利用できるようになる。

ネットワーク環境や導入製品でVPN環境の構成は変わる

IPsecを使用したリモートアクセスVPNを導入する場合、企業ネットワーク側にはIPsec-VPNを確立するためのIPsecゲートウェイ（セキュリティゲートウェイ）やユーザー認証を行うRADIUSサーバ、内部IPアドレスの割り当てと内部ネットワーク情報の通知を行うDHCPサーバ（IPsec-DHCPを使用する場合）などが必要となる（図9）。

ただし、IPsecゲートウェイ製品によってはRADIUSサーバやDHCPサーバと同等の機能が組み込まれている場合も多いので、導入する製品の機能を事前にチェックしておくほうがよい。また、使用するIPsecゲートウェイ製品に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上にあらかじめインストールしておく必要がある。クライアントソフトウェアには、IPsecゲートウェイのアドレスなどの情報を設定する。製品によっては、必要な情報を設定済みのインストール用プログラムを管理者が配布できるものもあるので、この点も製品を選択するうえでポイントとなるだろう。

またファイアウォールに関しては、IKE（500/UDP）およびESP（IPプロトコル番号50）に加えて、NATが存在した場合を考慮してカプセル化ESP（4500/UDP）の通過を許可する設定が必要となる。

通信のセキュリティは強力だがネットワークの細かい設定が必要

ここまで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IPsecを使用したリモートアクセスVPNの長所と短所をあげてみる。

トンネルIPヘッダ	ESPヘッダ	IPヘッダ	IPペイロード	ESPトレーラ	ESP認証データ

（a）IPsec NATトラバーサル適用前のIPsec（ESP）パケット

トンネルIPヘッダ	UDPヘッダ	ESPヘッダ	IPヘッダ	IPペイロード	ESPトレーラ	ESP認証データ

（b）IPsec NATトラバーサル適用後のIPsec（ESP）パケット

図8● IPsec NATトラバーサルによってESPパケットがUDPでカプセル化される（網掛部は暗号化）

Supplement

■EAP（PPP Extensible Authentication Protocol）
RFC 2284で定義されたPPP（Point-to-Point Protocol）を拡張したプロトコル。認証方式の違いにより、CHAPと同様の認証を行うEAP-MD5、証明書による相互認証を行うEAP-TLS（Transport Layer Security）、証明書による認証とPAP/CHAPなどの認証を組み合わせたEAP-TTLSなどがある。

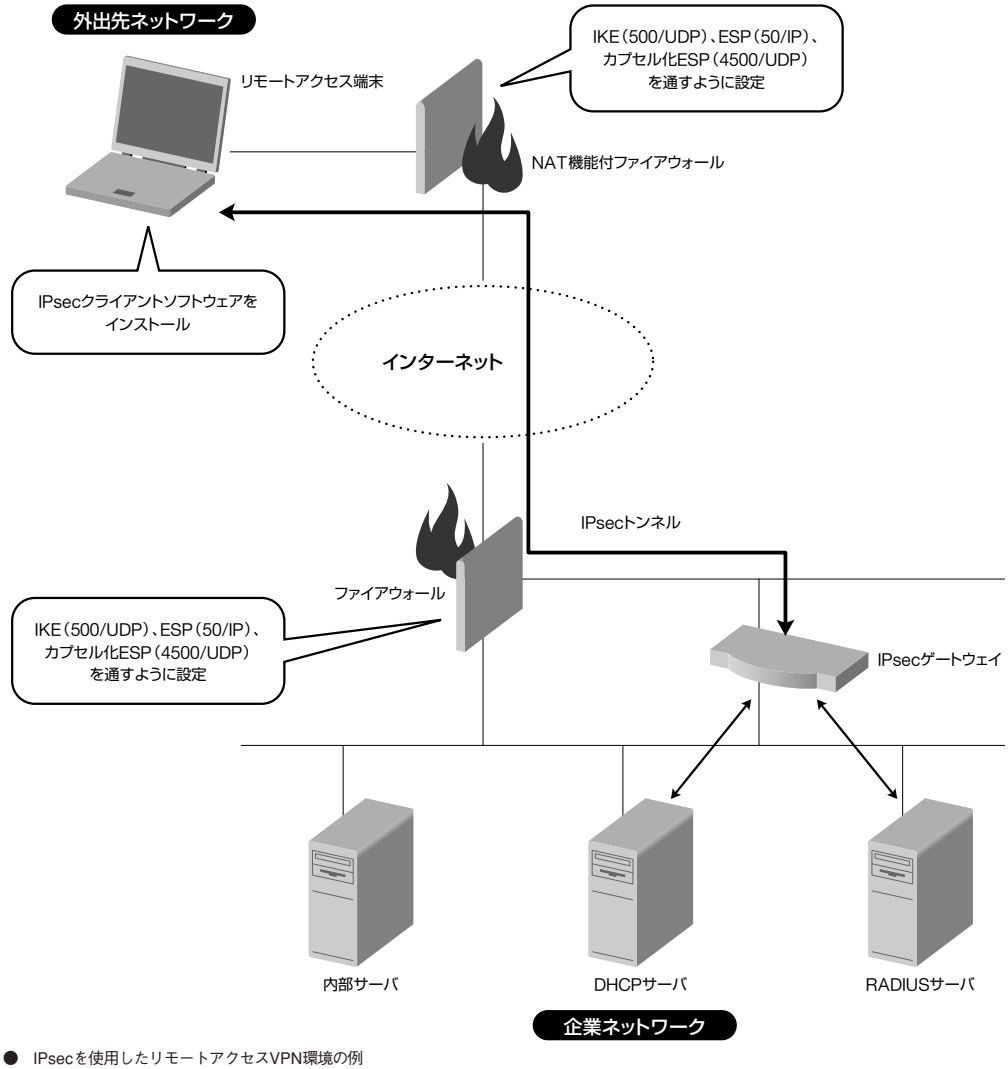

図9● IPsecを使用したリモートアクセスVPN環境の例

■長所

・IPレベルでセキュリティが確保されるので、マルチキャストを使用するアプリケーションを除くすべてのIP上のアプリケーションで利用可能である。
・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ので、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へスムーズに乗り換えることができる。

■短所

・リモートアクセス端末上に、使用するIPsecゲートウェイと同じベンダーのIPsecクライアントソフトウェアをあらかじめ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も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、IPsecを用いたリモートアクセスVPNについて述べた。次回は「PPTP-VPN」について解説する。

NTTデータ　馬場達也