

第8回

VPN

VPN構築のポイントを知る

VPN(Virtual Private Network)は、インターネットなどのオープンなネットワーク上で、セキュアな通信を可能にする手段として、多くの企業・組織で利用されている技術である。今回は、VPNの基本知識として、VPN技術の種類や利用形態について説明した。今回は、VPN技術の1つであるIPsecを用いてVPNを構築する際のポイントについて解説する。加えて、IPsecによるVPNの冗長構成と、IPsecに対応したVPN機器の市場動向についても説明したい。

内藤正規
ネットワンシステムズ



リモート・アクセスVPNを IPsecで構築する際のポイント

前回の本連載で説明したように、VPNを実現する代表的なコア技術としては、SSLとIPsecがある。SSLによるVPN(以下、SSL-VPN)は、クライアントソフトウェアとしてWebブラウザが利用できることなどから、最近注目を集めており、SSL-VPN機器も相次いでリリースされている。対するIPsecによるVPN(以下、IPsec-VPN)は、VPN技術としての歴史が古いや、離れた拠点間を接続する「LAN間VPN」での利用に向いていることなどから、普及という点では今のところはSSL-VPNに勝っている。

一方、技術面で見ると、SSL-VPNでは通信の可否が経路などの環境に左右されにくい、IPsec-VPNではIPsecの性質上いかなる環境でも通信が行えるとは限らない。特に、自宅や公共の場所からインターネット接続サービスを介して、拠点に設置されたVPN機器への通信を行う「リモート・アクセスVPN」をIPsecによって構築する際は、通信環境のほか、ユーザー認証についても注意を払う必要がある。そこで、まずはIPsecによるリモート・アクセスVPNを構築する際の要点を説明する。

ポイント1：VPN通信の設定

IPsecは複数のプロトコルから構成されており、その中核となるのは、IKE(Internet Key Exchange)、ESP(Encapsulating Security Payload)、AH(Authentication Header)の3つである。IKEはデータの暗号化などで用いる鍵の交換を行い、ESPとAHはデータの正当性の認証を行い、このうちESP

はデータの暗号化も行う。

IPsec-VPN機器をルータやファイアウォールの背後に設置する場合には、それらの設定を変更して、上記のプロトコルによる通信が行えるようにしておく必要がある。具体的には、IKEで用いるUDPの500番ポートへのアクセスを許可する。さらに、ESPで用いるIPプロトコル番号50、AHで用いるIPプロトコル番号51でのデータの送受を可能にする。なお、現在、リモート・アクセスVPNでは、アドレス変換もパケット改竄と見なしてしまうAHはほとんど使われておらず、通常、データ部分のみの検証と暗号化を行うESPが利用されている。

ポイント2：アドレス変換との関係

リモート・アクセスVPNにおいて、リモートのホスト(VPNクライアント)とIPsec-VPN機器との間にルータやファイアウォールが介在し、NAPT(注1)機能によるアドレス変換処理が行われる場合は注意が必要だ。というのも、IPsecは、標準仕様ではNAPTに対応していないからである。

そもそも、NAPTはIPヘッダに含まれるIPアドレスと、IPヘッダの次に位置するTCP/UDPヘッダに含まれるポート番号を変換する。しかし、一般的にリモート・アクセスVPNで利用されるESPでは、ESPヘッダを付加してTCP/UDPヘッダを含む元のパケットをカプセル化するため、IPヘッダとその次に位置するESPヘッダがNAPTの処理対象となる(図1)。だが、

注1：NAPT(Network Address Port Translation)は、IPアドレスとポート番号を基にアドレスを変換する機能であり、IPマスカレードとも呼ばれる。この機能は、プライベート・アドレスが割り当てられた複数のホストを、1つのグローバル・アドレスを用いてインターネット接続させるために使われることが多い

ESPヘッダはポート番号を持たないため、NAPTは的確な処理(アドレス変換)を行うことができないのである。

この問題は、「IPsecパススルー」と「IPsec NAT Traversal」という技術によって回避できる。前者は、ポート番号の変換処理を行わずにIPsec-VPNで送受されるパケットを転送する技術で、VPNクライアント側で利用する。一方、後者はIPsec-VPNで送受されるパケットにポート番号を持つUDPヘッダを付加してUDPパケットとして送信する技術で、IPsec-VPN機器側(IPsec-VPNサービスを提供する側)で利用する(図2)。なお、この2つの技術は、どちらか一方を有効にしておけばよい。双方を同時に用いると、障害が生じるおそれがあるので注意されたい。

また、これらの技術は、いずれも若干の問題を抱えている。IPsecパススルーには標準規格が存在しないため、ベンダーごとに機能が異なる。安価なエントリークラスの製品の場合には、IPsecパススルーがどのように動作するのかわからず、正常に動作しなくなっても原因を突き止める手がかりさえつかめないことがある。一方、IPsec NAT Traversalの場合は、セキュリティ上の理由からUDPによる通信が禁止されていたり、MTU(Maximum Transmission Unit:1回に送信できる最大のデータ量)の値が1,500バイト未満の経路でパケットが分割されてしまったりすることが原因で、送信先のホストまでパケットが到達しないことがある(注2)。

このほか、IPsec-VPNにおけるアドレス変換の問題を回避する手段として、「IPsec over TCP」のような独自機能を実装している機器もある。IPsec over TCPでは、IPsecベースのすべての通信を1つのTCPコネクションで行うという手法が採用されている。

図1：IPパケットとIPsecパケットの構造の比較

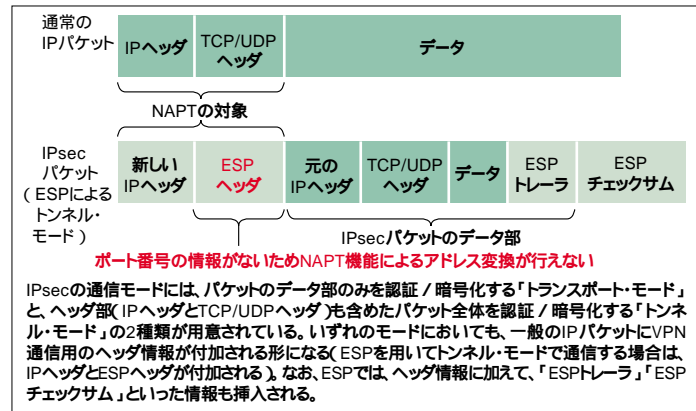
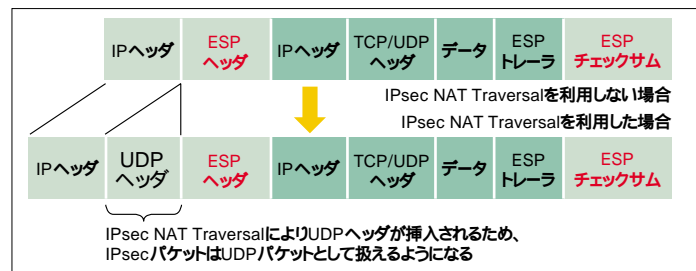


図2：IPsec NAT TraversalによりUDPヘッダが付加されたIPsecパケットの構造



ポイント3：ユーザー認証の導入

リモートアクセスVPNにおいては、ユーザー認証が必須だ。しかし、IPsec単体ではVPN通信を行うホスト自体の認証は行えるものの、ユーザー認証は行えない。したがって、IPsecでリモートアクセスVPNを構築する際は、ユーザー認証の仕組みを別途用意しなければならない。

以前は、ユーザー認証の方式には、ユーザー名とパスワードの組み合わせを利用する「古典的な方式」が使われていたが、セキュリティ意識の高まりとともに変化した。例えば、「ワンタイムパスワード」などの「2要素認証」が「現代的な方式」である。

注2：一般に、日本のブロードバンド環境では、PPPoE(PPP over Ethernet:ADSLを介してインターネットに接続するために使用される技術)などが用いられていることから、MTUの値が1,500バイト未満に制限されていることがある。この場合、ルータは1,500バイトを超えるパケットを転送できない。このようなMTUを原因とした通信障害を「MTU問題」と一般的に呼ぶ。IPsec NAT Traversalでも、このMTU問題が発生し、パケットが分割されてしまうために、送信先のホストまでパケットが到達しないことがある。本来、パケットは分割されても正常に送信されるはずだが、エントリークラスの製品のNAPTの実装では、分割されたパケットのうち最初のパケットしか転送しないなど、分割されたパケットを正常に処理できないことが多いようだ



2要素認証は、ユーザー名やパスワードといった固定の情報と、パスワード生成装置や認証情報が記録されたデバイス(注3)の2つの要素を用いて認証を行う技術である。どちらか一方の要素が漏洩/盗難に遭っても、不正に侵入される危険性を抑えられるため、認証手段として強力である。

その2要素認証の1要素となるワンタイム・パスワードは、毎回使い捨ての異なるパスワードを利用してユーザー認証を行う技術で、固定パスワードによる認証で発生する可能性のある、メモ書きやのぞき見によるパスワード漏洩のリスクを回避可能である。

結論的に言えば、IPsecによるリモート・アクセスVPNに効果的な認証方法としては、PKI(注4)やワンタイム・パスワードなどが挙げられる。この両者を厳密に比較すると、数学的な強度ではPKIに軍配が上がるが、どちらも十分に実用に耐えうる技術だ。ただし、運用コストで見るとPKIのほうが高つくため、VPNのみの利用ならばワンタイム・パスワードを採用したほうがよい。Web認証や電子決済システムなどの利用まで視野に入れるならば、汎用性や拡張性の高いPKIを選択するとよい。

なお、PKIでは認証に電子証明書を利用するため、それを発行する認証局を構築/運用する必要があるが、認証局に関連した一連の作業を代行するサービスを利用すれば、その手間は省ける。しかしながら、PKIの電子証明書は、一般的な認証とは少し概念が異なるうえ、その仕組みも許可/拒否といった二者択一を行う認証サーバとは違って複雑だ。そのため、他の認証方式と比べ管理/運用に手間がかかることは間違いない。



機器と経路の冗長化で フォルト・トレランスを確保する

VPNは普及当初から、機器の冗長化を含むフォルト・トレランス(耐障害性)の実現に苦労していると

言っても過言ではない。そこで、次に、IPsecによるVPNの冗長構成について説明しよう。

そもそも、VPNはインターネットなど信頼性の低い経路を介して通信を行ううえ、通常の通信に用いる機器に加えてVPN機器を設置することになるため、専用線に比べて信頼性に劣る。そこで、機器の故障に備えたそれ自身の冗長化と、回線の障害に備えた経路(ルータやファイアウォールなど)の冗長化という2つの側面から対策を講じることで、VPNの可用性を高めるといった対策がとられている(表1)。

まず、機器自体の冗長化については、機器を複数用意して、それらを冗長構成にすればよい。冗長構成のパターンとしては、機器が停止した際に手動で代替機に切り替える方法(コールド・スタンバイ)と、代替機が障害を検知して故障機に代わって自動的に処理を開始する方法(ホット・スタンバイ)がある。

このように、機器の冗長化は構成パターンが決まっているためそれほど難しくはないが、経路の冗長化はそう簡単にはいかない。元来、TCPベースの通信では、データ転送の開始から切断まで一連のセッションが確立されるため、冗長化されたルータやファイアウォールは、このセッションを監視することで異常終了などが検知されたら、機器の自動切り替えを行う。一方、IPsecによる通信では、データの転送を行う前に、送信先のホストとの間でSA(Security Association)と呼ばれる暗号化や認証の方式に関する取り決めを確立するが、TCPベースの通信のようにセッションは確立しない。そのため、IPsecによる通信では、「永遠に送信できない」か「送信できる可能性がある」という判断しかできず、セッションを基

注3：2要素認証向けのデバイスとしては、専用の認証装置だけでなく、ICカードや携帯電話機(で動作するアプリケーション)などもある。企業では、2要素認証向けのデバイスとして、社員証と兼用のICカードや、携帯電話機で動作するアプリケーションを用いることで、実行するユーザーの負荷を極力減らすという方向へ向かっているようだ

注4：PKI(Public Key Infrastructure)は、公開鍵暗号技術(対になる2つの鍵を使ってデータの暗号化・復号化を行う技術)と電子証明書を使って、安全な通信を可能にする仕組み

に「送信できなくなった」という通信の異常終了などの情報を検知することはできない。

こうしたIPsecの通信の仕組みは、経路の冗長構成を実現するにあたって大きな障壁となった。つまり、TCPベースの通信で用いてきた、セッションを基にルータやファイアウォールなどの機器を切り替えるという方法がIPsec-VPNでは利用できないのである。そこで、キープ・アライブ(注5)という機能を実装することで、IPsec-VPNにおいて機器や経路の障害を検知し、それを通信の異常終了として扱う機器が現れた。こうした機器を使えば、IPsec-VPNで回線中断などの障害が発生した際にも、経路を自動的に切り替えることができるわけだ。

また、オンデマンド(ユーザーからの要求を受けてサービスを提供する)形式での接続の際に必ず起きる「次に接続可能かどうかを判定できない」という問題も、IPsecの経路の冗長化構成での障壁となった。この問題は静的な経路(確実につながるという前提の経路)を確保しておくことで対処可能だ。ただし、通信サービスの停止が許されない場合や、十分にリソースがある場合などは、動的なルーティング・プロトコルによる経路制御に基づき、経路の冗長構成を図ることがある。このようなケースでは、専用線と同様に、メッシュ構成といった設計手法を取り入れて、冗長構成を構築する。



低価格化とともに操作性の向上が進むIPsec-VPN機器

最後に、IPsec-VPN機器の市場動向を説明して、本稿の締めくくりとしたい。

IPsec-VPN機器は登場当初、比較的高価だったが、普及が進むにつれてコスト・パフォーマンスが改善され、昨年辺りから一気に安価な機器が出回り始めた。この背景には、Mbps単位の速度でのインターネット接続を可能にしたブロードバンドの普及がある。

表1：冗長構成の種類

| 冗長構成のタイプ | 長所 | 短所 | |
|----------|------------------------|---|---|
| 機器 | 手動切り替え (コールド・スタンバイ) | <ul style="list-style-type: none"> 構築が容易である 機器の切り替えが確実に実行される | <ul style="list-style-type: none"> 切り替え作業に管理者が立ち会う必要がある ダウン・タイムが長くなる |
| | 自動切り替え (ホット・スタンバイ) | <ul style="list-style-type: none"> 機器の切り替えに手間がかからない | <ul style="list-style-type: none"> 短時間ではあるがダウン・タイムが発生することがある 回線障害では機器の切り替えが行われない製品がある |
| 回線 | キープ・アライブと静的な経路の確保 | <ul style="list-style-type: none"> バックアップ用の経路が信頼できるかぎり、経路の確実な自動切り替えが期待できる | <ul style="list-style-type: none"> 回線品質が低い場合に誤検知が発生する |
| | 動的ルーティングによる経路変更 | <ul style="list-style-type: none"> 経路の切り替えが確実に自動実行される ダウン・タイムが短い 回線障害に即座に対応できる | <ul style="list-style-type: none"> 構築が複雑で、専門知識が必要である 回線品質が低い場合に誤検知が発生する |

ブロードバンドによって、小規模企業 / SOHOユーザーが高速・広帯域の回線を低コストで利用できるようになったため、それらのユーザーを対象としたVPN接続サービスも増加傾向にあり、それに合わせてより低価格な機器のリリースが相次いでいるのだ。

実際、従来は10Mbps程度のスループットで、ADSL向けとされていた機器が20万円前後だったのに対し、現在は数十Mbpsのスループットで、光ファイバにも対応可能な機器が10万円を切る価格で販売されている。もちろん、両者の間には管理機能やログ機能に大きな差があり、後者の安価な機器はこれらの機能が「貧弱」だが、装備する機能を限定したことで操作性はかえって向上している。こうした機器は機能がシンプルな分、障害が発生する可能性も低く、専任の管理者がいない企業の拠点での利用にも適している。

また、安価な機器であれば、障害対策用として複数台購入し、冗長構成をとることも難しくないだろう。それにより、障害発生から復旧までの期間を短縮することができる。また、機器が安価であれば普及しやすく、それにより機器のさらなる低価格化が進むため、IPsec-VPN機器の普及が一層加速することも見込まれる。

CW

注5：キープ・アライブとは、通信が正常に行えることを確認するために定期的に行われる通信。通信先となる機器は、正常に稼働していることを知らせるためにハートビートという信号を一定時間ごとに発信する。これが途切れると、通信先の機器に何らかの障害が発生したと判定される