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、リモートアクセスVPNにおいて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とはどのようなものであるか、どういった機能を提供するのかを詳解する。

馬場達也

第2回　IPsecの基本を知る

Supplement

■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。

IPsecはIPにセキュリティ機能を付加する

インターネットは、そのれい明期には主に研究目的で使用されていたため、セキュリティに関してほとんど考えられていなかった。しかし、インターネットがビジネスで利用されるようになってきたため、1992年からIPにセキュリティ機能を付加するIPsecに関する議論が標準化組織である**IETF**において始まった。現在利用されているIPsecは、1998年に公開されたRFC 2401～2411、2451で定義されているバージョン2と呼ばれているものであり、Windows（Windows2000以降）やFree BSDといったBSD系OS、Linuxなどに標準で実装されているほか、多くのVPN（Virtual Private Network）製品にも利用されている。IPsecは、IPv4およびIPv6の両方で利用でき、特にIPv6では必須の機能となっている。さらに現在では、IETFにおいてIPsecのバージョン3の仕様が議論されている。

IPsecは、AHとESPの2つのプロトコルからなり、広義にはIKEやIPCompもIPsecに含まれる（表1）。AHは、IPパケットの改ざんを防止するための機能を持つプロトコルであり、IPプロトコル番号51を使用する。ESPは、IPパケットの改ざん検出に加えて、機密性を確保するための機能を持つプロトコルであり、IPプロトコル番号50を使用する。また、IPCompは、IPパケットの圧縮を行うためのプロトコルであり、IPプロトコル番号108を使用する。IKEは、これらのプロトコルで使用するアルゴリズムのネゴシエーションや、鍵のセットアップを行うためのプロトコルであり、UDPの500番ポートを使用する。

IPsecは暗号化や認証機能により安全な通信路を提供する

IPsecがIPに対して付加するセキュリティ機能にはさまざまなものが存在する。ここでは、トンネリング機能や暗号化機能など主だったものを簡単に紹介しよう。

■トンネリング機能

IPsecには、「トランスポートモード」と「トンネルモード」という2つのモードがある。トランスポートモードは、IPパケットのIPペイロード部分（IPヘッダを除いた部分）に対してIPsec処理をするものであり、エンド・ツー・エンド通信のセキュリティを確保するために使用される（図1）。これに対してトンネルモードは、IPパケット全体に対してIPsec処理を施し、それを運ぶための新たなIPヘッダを付加して送信するもので、これにより拠

プロトコル名称	プロトコル番号など	RFC文書
AH（Authentication Header）	プロトコル番号51	RFC 2402
ESP（Encapsulating Security Payload）	プロトコル番号50	RFC 2406
IPComp（IP Payload Compression Protocol）	プロトコル番号108	RFC 3173
IKE（Internet Key Exchange）	500/UDP	RFC 2409

表1●　IPsecで使用されるプロトコルの種類

点間VPNやリモートアクセスVPNを構築することが可能となる（図2）。

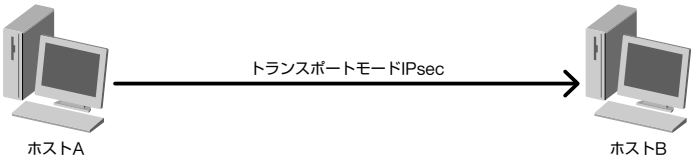

図1● トランスポートモードではエンドツーエンド通信のセキュリティを確保する

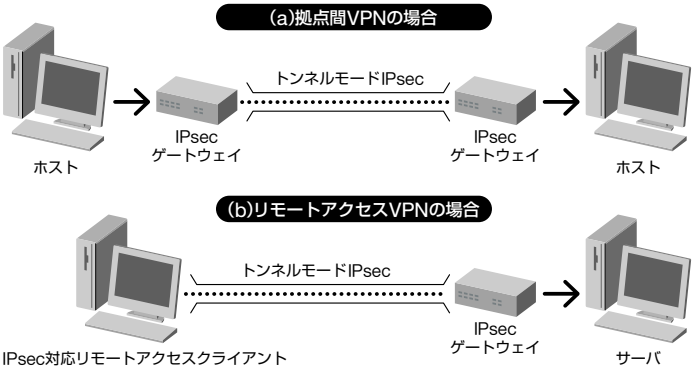

図2● トンネルモードはVPNを構築する場合に使用する

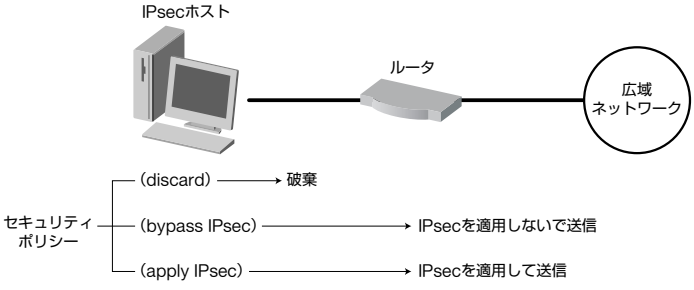

図3● IPsecではセキュリティポリシーに従ってパケットの処理方法を決定する

■暗号化機能

ESPを使用した場合、IPペイロード部（トランスポートモードの場合）またはIPパケット全体（トンネルモードの場合）を、**3DES**や**AES**などの共通鍵暗号を使用して暗号化する。IPペイロード全体を暗号化するため、送信するデータのみでなく、TCPやUCPなどのトランスポート層プロトコルのヘッダも隠すことができ、どのプロトコル（サービス）を利用しているかということも第三者から隠すことができる。

■メッセージ認証機能

AHまたはESPでは、メッセージ認証コード（**MAC**）を使用して、データの完全性を確保する。これにより、第三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。

■相手認証機能

AHまたはESPでは、メッセージ認証コードを使用することで、受信されたデータが同じ秘密鍵（認証鍵）を持つ相手から送信されたものであるかどうかを確認することができる。この認証鍵は、IKEによってデジタル署名などを利用して通信相手を認証したあと、安全にセットアップされる。

■鍵交換機能

暗号化用または認証用の秘密鍵は、IKEにより自動的にセットアップされ、また定期的に変更される。

■リプレイ防御機能

IPsecでは、送信するパケットにシーケンス番号を付与する。これにより、悪意のある第三者が、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」からの防御が可能となっている。

■アクセス制御機能

IPsecでは、セキュリティポリシーにしたがって、図3のようにパケットの「破棄（discard）」「IPsecを適用しないで送信（bypass IPsec）」「IPsecを適用して送信（apply IPsec）」の動作を決定する。これは、ファイアウォールと同等のアクセス制御機能を持っていることを意味する。

Supplement

■3DES（Triple Data Encryption Standard）
共通鍵暗号である「DES」の強度を高めるために、同暗号化方式を3重にかけるもの。「DES」は、IBMが開発した「Lucifer」を改良して作られたもので、米国の標準暗号となった。

■AES（Advanced Encryption Standard）
米国標準技術局によって定められる、米国政府の次世代標準暗号化方式のこと。従来まで標準暗号であったDESに代わるもの。

■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。

Supplement

■SA（Security Association）
IPsecで保護されたセキュアな通信路。IPsecでの暗号化や認証に必要な情報を管理する。

■SAD（Security Association Database）
SAに関するパラメータが収納されたデータベース。

■SPI（Security Parameter Index）
SAを識別するための32ビットのID。

■SPD（Security Policy Database）
パケットをどのように処理するのか、あるいは、どのように暗号化するのかなどの情報を格納する。

セキュリティアソシエーションとセキュリティポリシーの役割を知る

IPsecの仕組みについて説明する前に、まず「セキュリティアソシエーション（**SA**）」と「セキュリティポリシー」というIPsecを理解するために必要となる2つの用語について説明する。

SAは、IPsecで保護された単方向のコネクションのことである。SAは単方向であるため、行きと帰りの両方向をIPsecで保護するためには、図4のようにAHやESPなどのセキュリティプロトコルごとに、行きと帰りで別々のSAが必要となる。それぞれのSAでは、使用する暗号化アルゴリズムや認証アルゴリズム、鍵、シーケンス番号などのIPsecで使用するパラメータを管理しており、これらの情報は**SAD**と呼ばれるデータベースに格納される。SAは、IPsecが適用されたIPパケットの「宛先IPアドレス」、AHやESPなどの「セキュリティプロトコル」、SA確立時に受信側が付与する「**SPI**」の3つの情報によって識別される。

セキュリティポリシーは、前述した破棄、IPsecを適用しないで送信、IPsecを適用して送信などのIPパケットの処理方法を記述したものである。IPsecを適用する場合には、どのセキュリティプロトコル（AH/ESP/IP Comp）を適用するのか、どのアルゴリズム（暗号化アルゴリズム、認証アルゴリズム、圧縮アルゴリズム）を適用するのかといった情報も記述する。このセキュリティポリシーの情報は、**SPD**と呼ばれるデータベースに格納される。

SAとセキュリティポリシーの関係は次のようになる。IPsec機器では、最初に転送しようとするIPパケットの「送信元IPアドレス」や「宛先IPアドレス」「プロトコル」「送信元ポート番号」「宛先ポート番号」などをキーとして、SPDを検索する。該当するセキュリティポリシーが「discard」であればパケットを破棄し、「bypass IPsec」であればそのまま転送する。「apply IPsec」であった場合は、該当するSAが存在するかどうかを調べる。該当するSAが存在した場合には、SADからそのSA情報を取り出し、パケットにIPsec処理を施す。もし該当するSAが存在しなかった場合は、IKEを使用してSAを確立する。

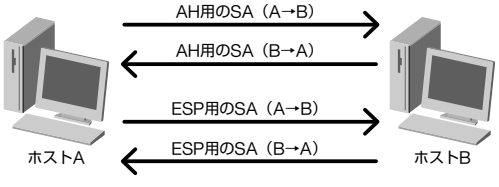

図4● IPsecではセキュリティプロトコルごとに行きと帰りで独立したSAを持つ

ESPのトンネルモードではIPパケットはどのように処理されるのか

それでは、ESPのトンネルモードの仕組みについて解説しよう。AHやトランスポートモードのESPについては、インターネットVPNでは通常使用されないので、ここでは割愛させていただく。

ESPのトンネルモードでは、図5のように、オリジナルのIPパケット全体にESPトレーラが加えられたものが、SAで決められた共通鍵暗号によって暗号化される。そして、暗号化されたデータの先頭に、トンネル配送用の新たなIPヘッダとESPヘッダが付加され、最後にESP認証データが添付される。ESPヘッダには、SAを識別するためのSPIとシーケンス番号が格納され、ESPトレーラには、パディングと暗号化されたデータの先頭に位置するヘッダ番号（トンネルモードの場合はIPv4を示す4かIPv6を示す41となる）が含まれる。さらに、ESP認証データには、ESPヘッダと暗号化されたデータ（オリジナルのIPパケットとESPトレーラ）に対するメッセージ認証コードが格納される。この認証データを受信側で検証することにより、データの内容が第三者によって改ざんされていないかどうかを確認することが可能となる。

Supplement

また、ESPをIPCompとあわせて使用した場合は、図6のように圧縮アルゴリズムによってオリジナルのIPパケット全体が圧縮され、IP CompヘッダとESPトレーラが付加される。そして、そのデータが共通鍵暗号で暗号化され、先頭にトンネル配送用の新たなIPヘッダとESPヘッダが、最後尾にESP認証データが付加される。トンネルモードのIPsecを適用するとIPパケットのサイズが大きくなってしまうという問題があるが、IPCompを適用することでそのサイズをある程度抑えることができる。

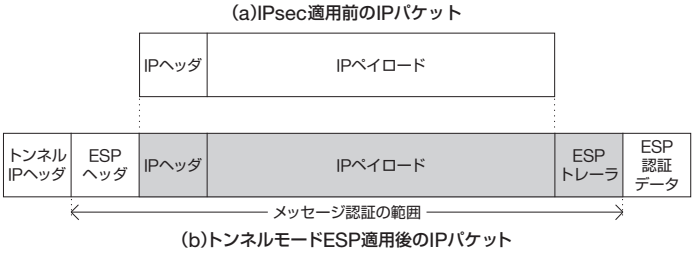

図5● トンネルモードESPを適用したパケットのフォーマット（網掛け部分は暗号化されている）

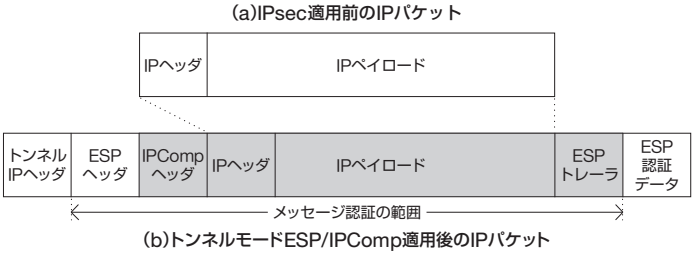

図6● トンネルモードESP/IPCompを適用したパケットのフォーマット（網掛け部分は暗号化されている）

認証とSAの確立を実行し共有鍵を管理するIKE

IKEは、セキュリティポリシーの内容を基にしてSAを自動的に確立するためのプロトコルである。IKEが提供する主な機能は次の3つである。

①相手認証

秘密鍵を共有する際には、相手の認証を行う必要がある。IKEでは、次の4種類の相手認証方式が定められている。

事前共有秘密鍵認証方式

事前共有秘密鍵認証方式では、あらかじめ何らかの方法で秘密の鍵を共有しておき、互いに同じ鍵を持っていることを確認することで相手を認証する。この秘密の鍵は、事前共有秘密鍵（Pre-shared Key）と呼ばれる。

デジタル署名認証方式

デジタル署名認証方式では、互いに相手のデジタル署名を検証することによって相手を認証する。デジタル署名のアルゴリズムとしては、RSAやDSAなどが利用できる。

公開鍵暗号化認証方式

公開鍵暗号化認証方式では、乱数値を相手の公開鍵を使って暗号化して送信する。そして、その乱数値が相手側で正しく復号されたことを確認することで相手を認証する。公開鍵暗号には、RSAやElGamalが利用できる。

改良型公開鍵暗号化認証方式

改良型公開鍵暗号化認証方式は、公開鍵暗号化認証方式の時間のかかる処理を減らし、性能を向上させた方式である。

実際のVPN製品では、事前共有秘密鍵認証方式とデジタル署名認証方式の2種類をサポートしていることが多い。また、現在検討されているIKEの次期バージョンであるIKEv2では、公開鍵暗号化認証方式と改良型公開鍵暗号化認証方式はサポートされなくなる予定である。

②SAのネゴシエーション

IKEでは、IKEを開始するイニシエータ（始動者）が複数のSAパラメータの組み合わせを提案し、それに対して、レスポンダ（応答者）がその中から1つの組み合わせを選択することでSAの確立を行う。

Supplement

■Diffie-Hellman鍵共有
DiffieとHellmanが1976年に発表した鍵交換方式で、乱数と秘密鍵から生成した情報を利用するもの。

③共有秘密鍵の管理

IKEでは、**Diffie-Hellman鍵共有**アルゴリズムを使用して、IPsecで使用する暗号化用の秘密鍵および認証用の秘密鍵をセットアップする。また、定期的に鍵を変更する。

IKEが行う処理の過程であるフェーズ1とフェーズ2を具体的に見てみよう

IKEには、フェーズ1とフェーズ2と呼ばれる2つの段階がある。フェーズ1では、ISAKMP SA（IKE SAともいう）と呼ばれるフェーズ2における交換内容を保護するためのSAを確立する。次に、事前共有鍵（Pre-shared Key）やデジタル署名などを使用して相手を認証する。フェーズ2では、IPsecで使用するIPsec SAを確立する。

フェーズ1では、「メインモード」と「アグレッシブモード」の2つのモードがある。メインモードでは図7のように、6つのメッセージを交換する。最初のメッセージ交換（図7中の①および②）では、ISAKMP SAのパラメータのネゴシエーションを行う。これは、イニシエータ（最初のIKEメッセージの送信側）が、自身のセキュリティポリシーにあった複数のパラメータのセットを優先順位をつけてレスポンダ（最初のIKEメッセージの受信側）に提案し、応答者がその中から自身のセキュリティポリシーにあったものを1つ選択することで成立する。

そして、次のメッセージ交換（図7中の③および④）では、ISAKMP SAで使用する暗号化用の鍵と認証用の鍵のセットアップを行う。

最後のメッセージ交換（図7中の⑤および⑥）では、それぞれのID（IPアドレスやホスト名、ユーザ名など）を交換し、その認証情報を交換することで、相手の認証が行われる。例えば、デジタル署名認証方式を使用している場合は、ここで公開鍵証明書と署名を交換する。この最後のメッセージ交換では、最初のメッセージ交換でネゴシエーションされたアルゴリズムと、2回目のメッセージ交換でセットアップされた鍵を使用して、暗号化とメッセージ認証が施される。このため、交換されるIDの内容を第三者に知られることはない。

これに対して、アグレッシブモードは、図8のように3つのメッセージを使用する。アグレッシブモードにおいても、メインモードと同様にISAKMP SAを確立することは可能であるが、ネゴシエーションできるパラメータが制限されたり、IDが保護されないといった問題がある。なお、次期バージョンのIKEv2では、4つのメッセージでISAKMP SA（IKE SA）を確立するモードが検討されている。

このフェーズ1でネゴシエーションされるISAKMP SAパラメータは表2のとおりである。暗号化アルゴリズムには、AES-CBCを選択することを勧めるが、実装されていなければ3DES-CBCを選択しておけばよいだろう。ハッシュアルゴリズムには、現在のところ第1希望としてSHA-1、第2希望としてMD5を

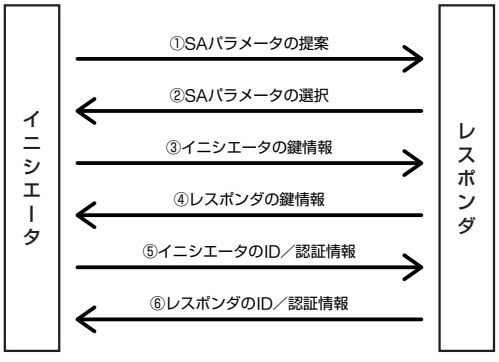

図7● フェーズ1のメインモードでは6つのメッセージを使用してISAKMP SAを確立する

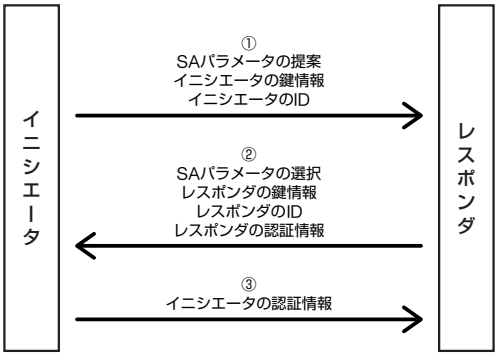

図8● フェーズ1のアグレッシブモードでは3つのメッセージでISAKMP SAを確立する

選択しておけばよい。Diffie-Hellmanグループは、鍵のセットアップに使用するDiffie-Hellman鍵共有アルゴリズムの強度であると考えてよいが、グループ5（1,536ビット）あたりを選択しておけばよい（ビット数が大きいほど強度が高い）。また、ISAKMP SAの有効期間は、8時間や12時間程度を指定しておけば十分である。この有効期間が切れる直前に、自動的にフェーズ1の交換が行われ、新たなISAKMP SAが確立される。

フェーズ2は、クイックモードと呼ばれるメッセージ交換を使用する。クイックモードでは、図9のように3つのメッセージを交換する。最初のメッセージ交換（図中の①および②）では、IPsec SAのパラメータのネゴシエーションと、IPsec SAで使用する鍵のセットアップ、IPsecを適用するトラフィック（送信元IPアドレス、宛先IPアドレス、プロトコルなど）の確認を行う。そして最後に、始動者からレスポンダにSAのセットアップが完了したことを示すメッセージが送信される。このフェーズ2においてネゴシエーションされるIPsec SAパラメータは表3のとおりである。

VPNを構築する場合は、セキュリティプロトコルとしてESP（またはESP+IPComp）、カプセル化モードとしてトンネルモードを選択する。また、ESPで使用するための暗号化アルゴリズムおよび認証アルゴリズムを選択する（IPCompを使用する場合は圧縮アルゴリズムも選択する）。暗号化アルゴリズムは、ISAKMP SAの場合と同様にAES-CBCを選択し、実装されていなければ3DES-CBCを選択しておけばよいだろう。認証アルゴリズムは、第1希望としてHMAC-SHA1-96、第2希望としてHMAC-MD5-96を選択しておけばよい。Diffie-Hellmanグループは、グループ5（1,536ビット）を選択しておこう。IPsec SAの有効期間は、暗号化およびメッセージ認証で使用する鍵を交換する間隔であると考えてよく、通常は1時間程度を指定しておけばよい。この有効期間が切れる直前に、自動的にフェーズ2の交換が行われ、新たなIPsec SAが確立される。

パラメータ	例
暗号化アルゴリズム	3DES-CBC、AES-CBCなど
ハッシュアルゴリズム	MD5、SHA-1など
相手認証方式	事前共有秘密鍵、RSA署名、DSS署名など
Diffie-Hellmanグループ	1024ビット、1536ビットなど
ISAKMP SAの有効期間	8時間、12時間など

表2● フェーズ1でネゴシエーションされるISAKMP SAパラメータ

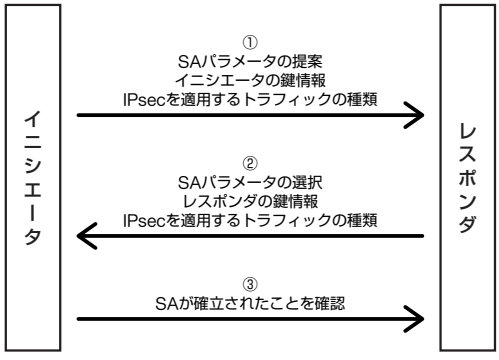

図9● フェーズ2では3つのメッセージでIPsec SAを確立する

パラメータ	例
セキュリティプロトコル	AH、 ESP、 IPComp
暗号化アルゴリズム（ESP）	3DES-CBC、AES-CBCなど
認証アルゴリズム（AH、ESP）	HMAC-MD5-96、HMAC-SHA1-96など
圧縮アルゴリズム（IPComp）	DEFLATE、LZSなど
Diffie-Hellmanグループ	1,024ビット、1,536ビットなど
IPsec SAの有効期間	1時間など
カプセル化モード	トンネルモード、トランスポートモード

表3● フェーズ2でネゴシエーションされるIPsec SAパラメータ

リモートアクセスVPN構築にはIPsecの基本機能だけでは不十分である

これまでに述べたIPsecの機能を利用することで、拠点間VPNを構築することが可能である。しかし、リモートアクセスVPNで利用するには、このようなIPsecの通常の機能だけでは難しい。通常、リモートアクセスでは、**RADIUS**ベースのユーザ認証が利用されるが、IPsecにおいては標準ではサポートされていない。また、接続先のネットワーク情報を取得して設定する機能も標準ではサポートされていない。これらの機能は、**XAUTH**やmode-cfg（**IKE-CFG**）などの標準ではない機能を利用することで実現することが可能となる。次回は、これらのリモートアクセス用の機能について解説する。

NTTデータ　馬場達也

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。RFC2138/2139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。

■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。

■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。