IPsec 概要

●IPsec は IP パケットをカプセル化して伝送するものであるが、カプセル化モードで ESP を選択しないと暗号化されない。

●IPsec 機能を持つ GW（GATE WAY）は、受信したパケットのセレクタ（パケットの種類を識別する情報で IP アドレスやポート番号等）に応じて、SPD（Security Policy Database）に登録された SP に従い、以下の 3 つの動作を行う。

①PROTECT：IPsec の処理を行う。

②BYPASS：IPsec の処理は行わず、通常の処理をする。

③DISCARD：パケットを破棄する。

●ISAKMP SA や IPsec SA 等の安全性を高める観点から生存期間を定めることで、リキー（生存期間毎に共通鍵等を作り変えること）を行う。

●SPI（Security Parameter Index）は IPsec SA を識別するための 32bit の番号。ちなみに AS（自律システム）も 16bit 又 32bit の AS 番号を持つ。

IKEv1 (Internet Key Exchange ver.1)

●IPsec のセキュアな通信に先立ち、パラメータ交換や鍵交換の折衝、及び相互認証を行うプロトコルであり、IKEv1 の他に IKEv2 があるが、互換性がないことに注意。

●UDP500 番を使用。送信元はイニシエータ、受信者はレスポンダという。

●IKEv1 では、フェーズ 1 （ISAKMP SA (IKE SA)を生成するためのパラメータを交換し、ISAKMP SA を生成）とフェーズ 2（ISAKMP SA を用いて IPsec SA を生成するためのパラメータを交換し、IPsec SA を生成）がある。

IKEv1 のメインモードによるフェーズ１

●フェーズ２は ISAKMP SA を用いているので、セキュリティ処理（暗号化やメッセージ認証等）が行われているが、フェーズ１は行われていない。

●イニシエータもレスポンダも IPsec 対応ルータの様に固定された IPA をもつ基本的なモードであり、通信相手の認証に IPA から特定できる事前共有鍵を使用することが可能。そのため、ID=IPA の制約がある。以降、事前共有鍵の使用を前提とする。

●以下の①②③の手順**（鍵交換してから認証）**で ISAKMP SA を生成する。

【①折衝】イニシエータが ISAKMP SA で使用されるパラメータ（暗号化アルゴリズム、ハッシュアルゴリズム及び認証手順等）を提案し、レスポンダが受諾可能なものを選択する。

【②共通鍵の生成及び交換】イニシエータとレスポンダが DH 鍵交換アルゴリズムによって、DH 秘密鍵を共有し、それを基に４つの秘密対象鍵を生成する。この４つの鍵は独立しているのではなく、先の鍵等から後の鍵が生成されている。また、これまでのメッセージ交換から IP ヘッダを見て IP アドレスから事前共有鍵を特定する。そうしないと、次の③の時に相互認証ができない。つまり、事前共有鍵認証することを攻撃者が知っていれば、IP アドレスが ID であることも悟られてしまう。

【③認証】ID (=IPA)と認証用のハッシュ値（「これまで交換した情報」と「事前共有鍵」を連結させた文字列のハッシュ値、**つまり鍵付きハッシュアルゴリズムである HMAC を使用**）で相互認証を行う。つまり③は、エンティティ認証とメッセージ認証の両方を行っている。なお、ID と HMAC は②の秘密対象鍵の内の１つによって暗号化されている。そうしないと ID がばれる。

IKEv1 のアグレッシブモードによるフェーズ１

●モバイル接続の様に IP アドレスが固定されていない場合には、IP アドレスによって事前共有鍵が特定できないため、ID を秘密にしていても仕方がないので、①の折衝時には ID を平文で送ることにより識別してもらう。あとの流れはメインモードとほぼ同じである。

●それでも事前共有鍵認証を使用したい場合には ID に FQDN（Fully Qualified Domain Name）等を使用することで、事前共有鍵を特定できる。それでも、折衝時に ID が FQDN になるだけで、ID が平文であることには変わりがない。

●とにかく、メインモードの**【③認証】**と比較して、認証用のハッシュ値を暗号化したものを送信するものの、認証機能が脆弱（ID が平文等）であり、かつ、モバイル盗難によるナリスマシ接続もある。そこで、XAUTH という手段を用いる。

●XAUTH は、ISAKMP SA 生成後、つまり、暗号化された SA が生成後、ユーザ ID と PW 等によりユーザ認証を行う。これに成功しないと、フェーズ２に進めない仕組みである。