IP in IP

●IP パケット（主に PIPA）に更に IP ヘッダ（主に GIPA）を付加してカプセル化するトンネリングプロトコル。

●認証機能や暗号化機能がないため、閉域網サービス内の使用に限定される。それゆえ、インターネット上で使用する場合には、暗号化対象が既に GIPH でカプセル化されているため、IPsec のトランスポートモードを使用（GIPH と IP パケットの間に ESP ヘッダを挿入）すればよい。

GRE (Generic Routing Encapsulation)

●最初に結論をいうと、暗号化されたマルチキャスト通信を行いたいのであれば、**GRE over IPsec**

●トンネリングは、あるプロトコルのパケットをトンネリングプロトコルでカプセル化することで実現する。そのトンネリングプロトコルの 1 つに GRE がある。

●GRE は 1 対の機器間に仮想的な専用線を構築する。GRE は IP パケットにも使えるので、インターネット VPN の様だと思うかもしれないが、暗号化機能等がないため、安全性を確保したい場合には、GRE over IPsec とする。

●GRE over IPsec とするならば、初めからインターネット VPN で事足りると思うが、IPsec はマルチキャストに対応しておらず、マルチキャストも対応できる GRE over IPsec が重宝される。

●IPsec がマルチキャストに対応していない理由は以下の 2 つある。

①IPsec はリプレイ攻撃に対応するために AH ヘッダや ESP ヘッダにシーケンス番号が格納されているため、1 対 1 の通信ならば問題ないが、マルチキャストでは極めて困難になる。マルチキャストは 1 つのアドレスで複数の宛先に送ることができるため、TCP ではなく、UDP を使う。

②共通鍵暗号方式は 1 対 1 にしか対応していない。

●ただし、GRE over IPsec は、暗号化機能等に IPsec を使用しているだけで、トンネリングは GRE で構築されているので、IPsec はトランスポートモードでいい。

●カプセル化するものが IP パケットの時、GRE ヘッダの前に付与する IP ヘッダは GIPA であり、オリジナルの IP ヘッダは PIPA で構わない。この辺りは IPsec のトンネルモードと同じである。

PPTP（Point to Point Tunneling Protocol）

●PPTP は PPP を GRE でカプセル化したもの。これでネットワークを超えることができる。PPTP は PPP の暗号化機能（RC4 アルゴリズム）があるため、VPN プロトコルである。※IPH＋GREH＋【PPPH＋IPH＋TCPH＋データ】

L2TP（Layer 2 Tunneling Protocol）

●PPTP は PPP 自体が古く暗号機能が単純なため、速度は速いが安全性が低い。よって、L2TP over IPsec を使用することで、速度は遅くなるが、IPsec により安全性は高い。

※IPH＋ESPH＋UDPH＋L2TPH＋【PPPH＋IPH＋TCPH＋データ】＋ESP トレーラ＋ESP 認証データ

いつものように、黄色が暗号化範囲、これに ESPH を加えたものが認証範囲。

※NAPT がある場合、先頭の IPH の後に UDPH を入れるので、UDPH が 2 つになる。

PPP（Point to Point Protocol）

●2 つのノード間（１対１）で通信を行う時、WAN が公衆電話網の場合、イーサネットを使うことができないため、MAC の代わりに使用するデータリンク層のプロトコル。よって PPP に IP が乗っかる。

●イーサネットは LAN ケーブル（光ファイバー及び同軸ケーブル含む）で構成されるが、その無線版が無線 LAN（Wi-Fi）なので、Wi-Fi も MAC である。

●PPP レベルのコネクションを張る時には、認証プロトコルとして、PAP（Password Authentication Protocol：クリアテキストによるユーザ ID と PW による認証）又は CHAP（Challenge Handshake Authentication Protocol：チャレンジハンドシェイク方式による認証）を使用する。※PPP はコネクション型の通信

●PPPoE：イーサネットは高速安価であるが、認証やコネクションを張る機能はないため、PPP フレームをイーサネットフレームでカプセル化して、イーサネット上で PPP の機能を実現するプロトコル。+αの機能を使うために+αの機能を持つものをカプセル化して、+αの機能を持たないもののヘッダを付ける。

●HDLC：PPP の基となったプロトコルでバイナリーデータを送るために最初に開発された。

HDLC (High level Data Link Control)

●文字データをテキストデータ、画像や音声でデータはバイナリーデータ

●ベーシック手順とはテキストデータを送受信するプロトコル

●HDLC はバイナリーデータを送受信できる最初のプロトコル

●MIME はバイナリーデータをテキストデータに変換して email を送る。その email を暗号化やデジタル署名を行う規格が S/MIME

NCP (Network Control Protocol)　LCP (Link Control Protocol)

IPCP (Internet Protocol Control Protocol)

●PPP 機能の内、上位層に依存するプロトコルが NCP であり、特に上位層が IP の時は IPCP

●IPCP は IP アドレスの自動割り当てを行う。IPA の割り当ては DHCP だけではない

●上位層に依存しないプロトコルが LCP