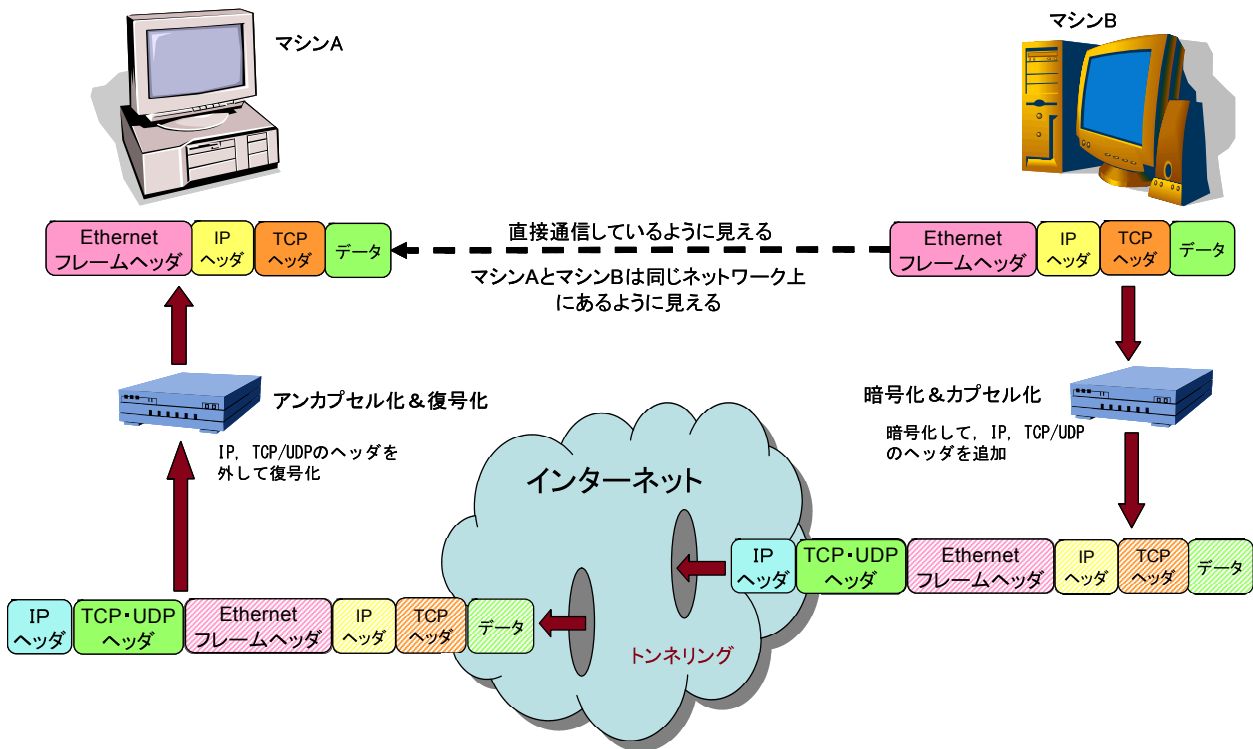


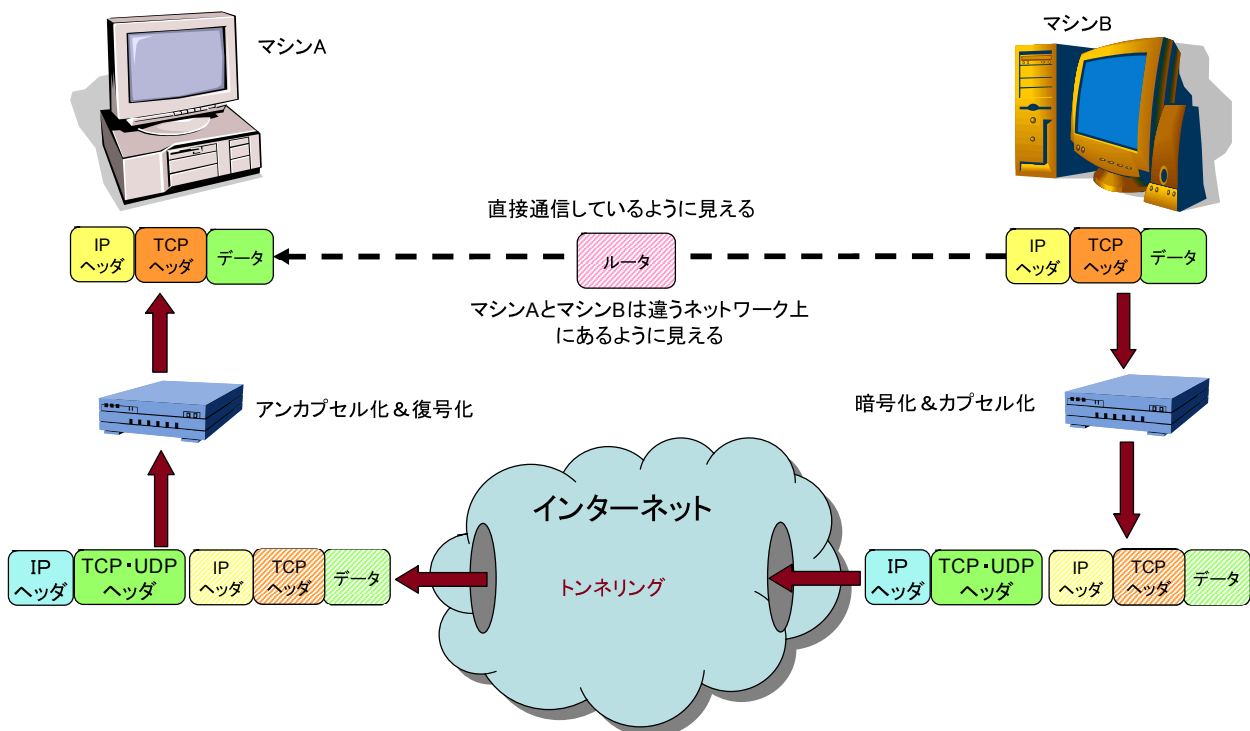
VPN (Virtual Private Network)

- ・ 定義は色々あるが、一般的には、暗号化とトンネル技術により、公共ネットワークを専用ネットワークの通信路に見せる手法。様々な手法がある。
- ・ 暗号化：公開鍵暗号方式で共通鍵暗号の共通鍵を交換する。
- ・ トンネルリング：専用ネットワーク（組織内部のネットワーク）のデータを公共ネットワーク（インターネット）の packets に包んで(カプセル化)、公共ネットワーク内を通過させること。

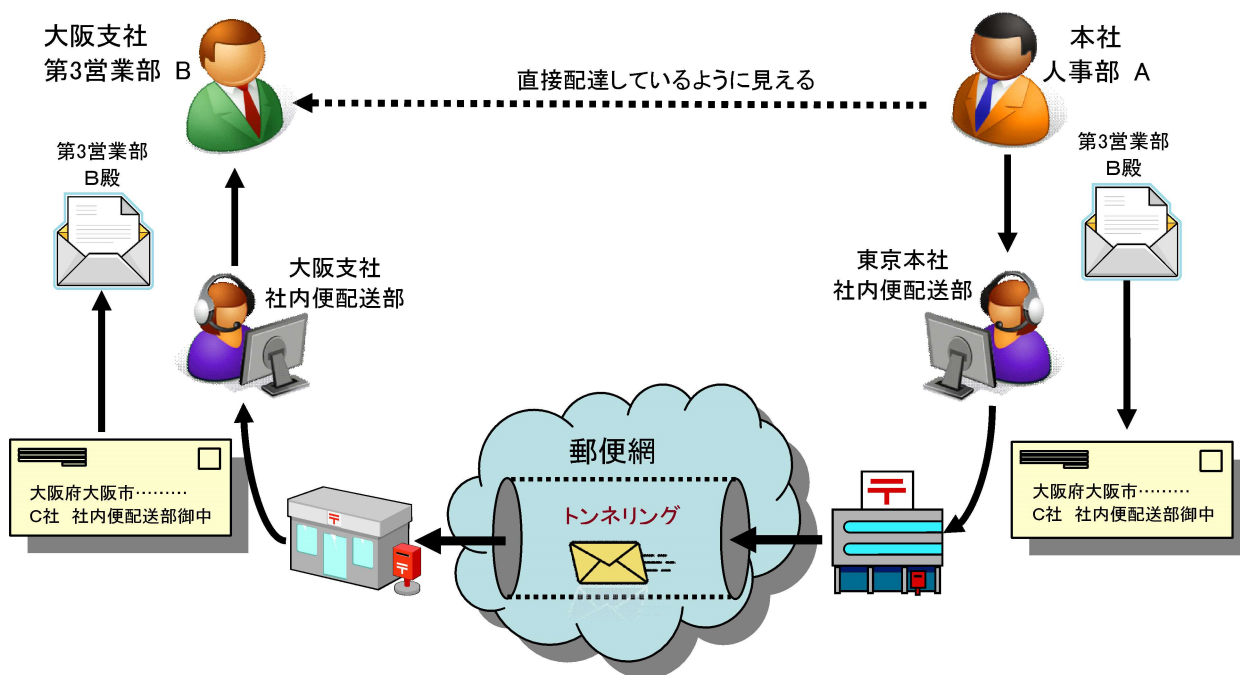
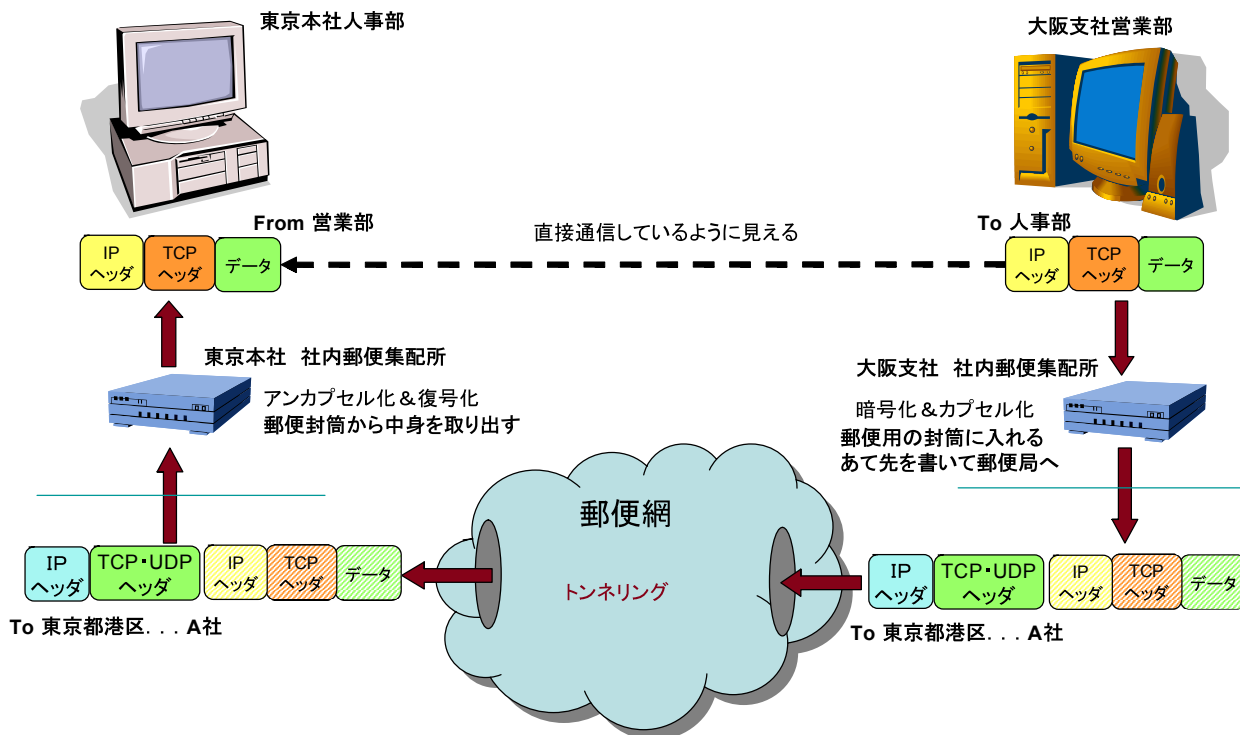
VPN (Virtual Private Network) Layer2



VPN (Virtual Private Network) Layer3

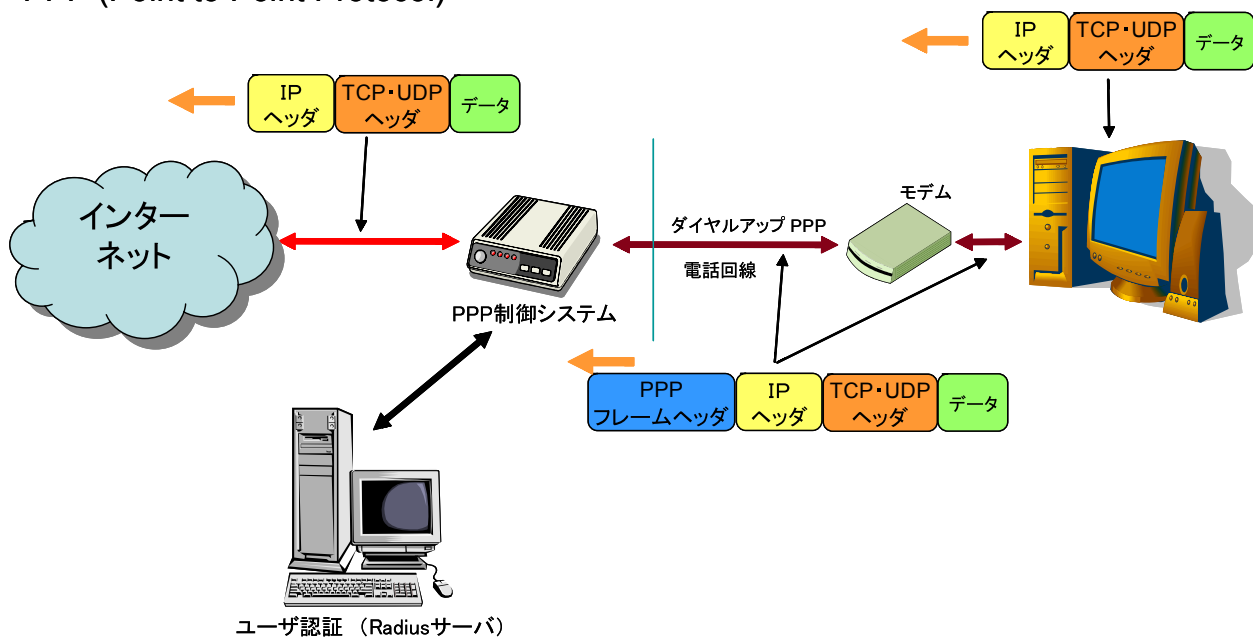


VPN (Virtual Private Network) Layer3 社内郵便との連想

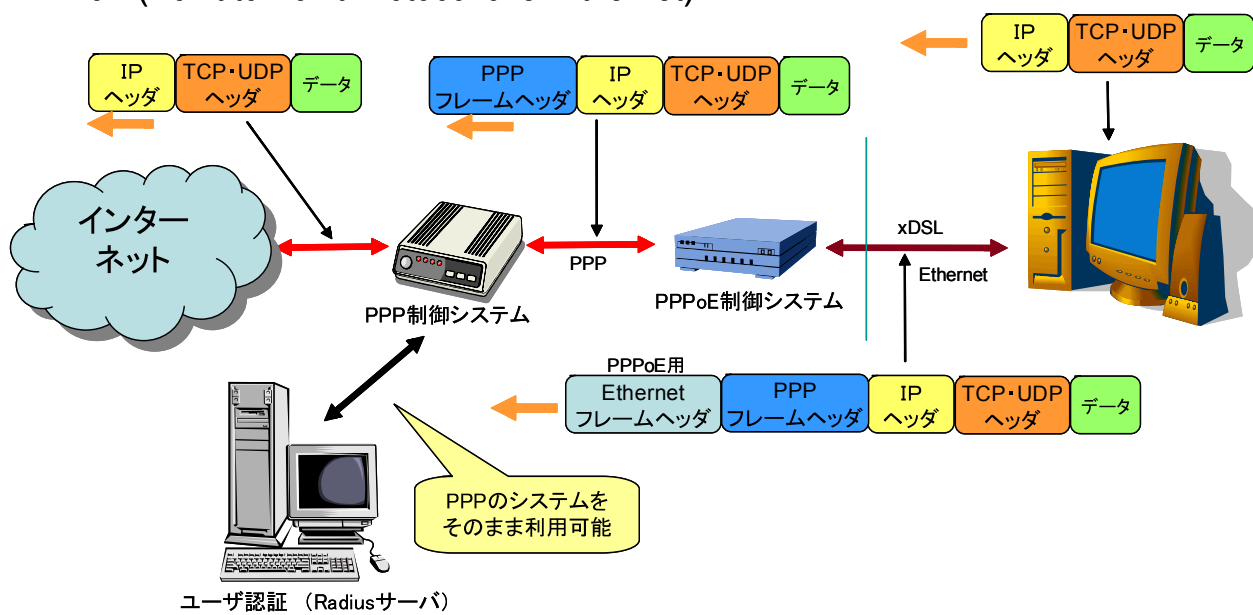


基本となる技術

PPP (Point to Point Protocol)



PPPoE (Point to Point Protocol over Ethernet)



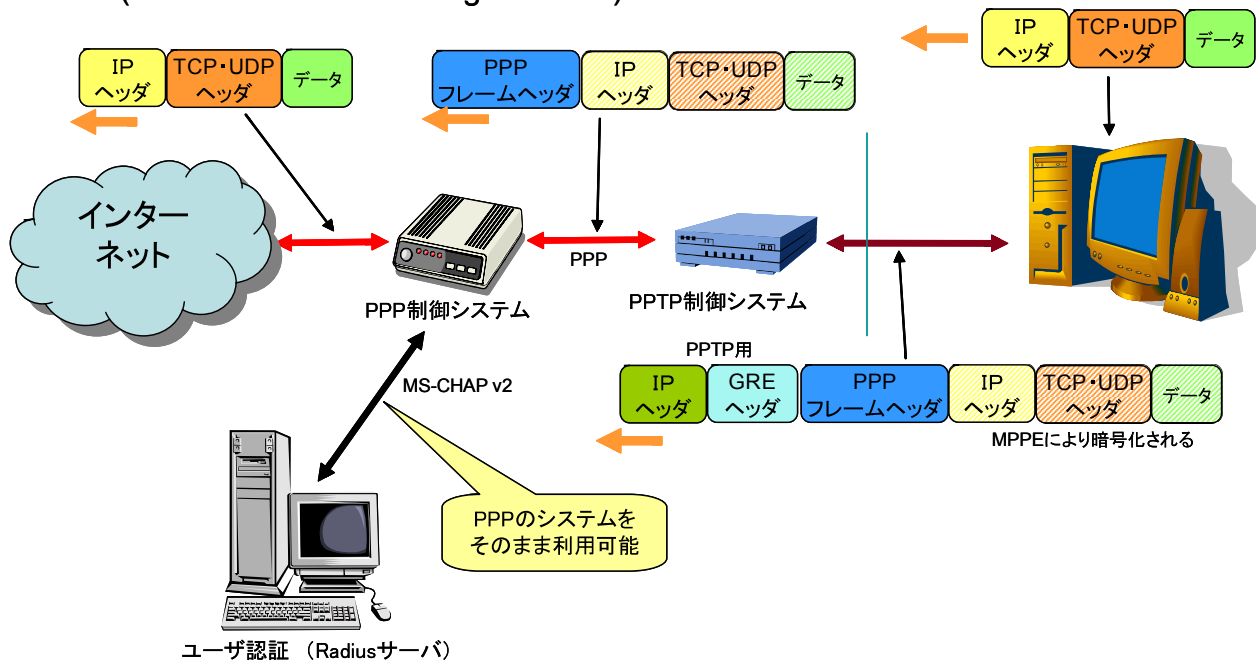
VPNの種類

・ PPTP(Point to Point Tunneling Protocol)

- ポイント・ツー・ポイント・トンネリング・プロトコル. PPP (Point to Point Protocol) のパケットを IP パケット + GRE (Generic Routing Encapsulation: 汎用カプセル化プロトコル) で包み込んでトンネリングを行なう.
- 認証には MS-CHAP (Microsoft - Challenge Handshake Authentication Protocol), 暗号化には MPPE (Microsoft Point to Point Encryption) が使われる.

PPP の機器や環境, ソフトを流用できるという利点がある.

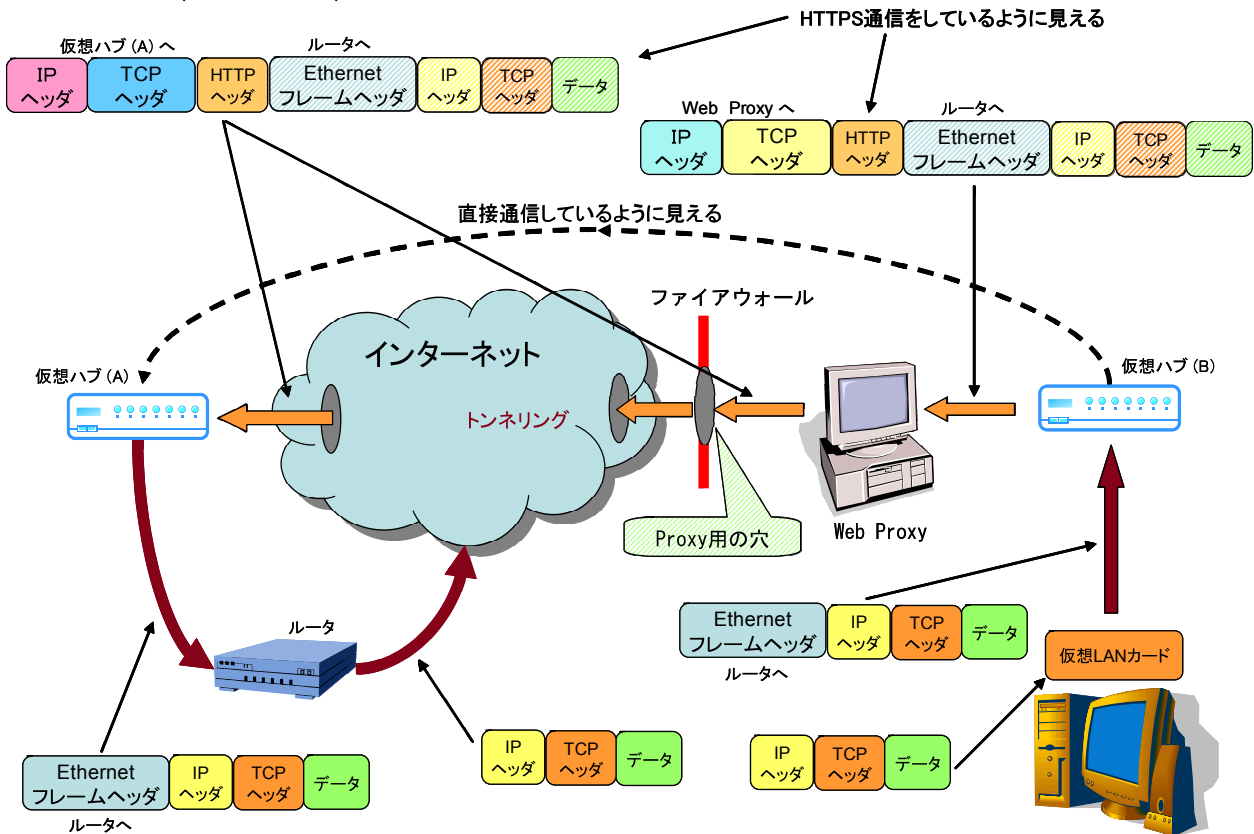
PPTP (Point to Point Tunneling Protocol)



・ Soft Ether (PacketiX VPN)

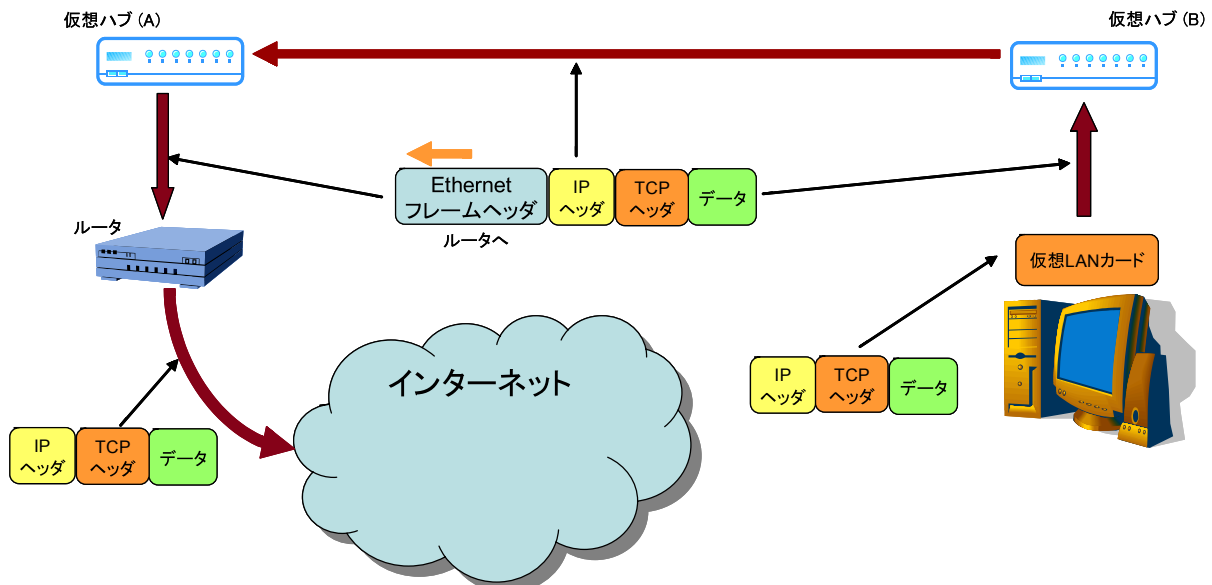
- 最近の流行. 仮想ネットワークカード, 仮想ハブ (共にソフトウェア) を用意し, これを拠点にしてトンネリングを行う. トンネリング時の仮想ハブが使用するTCPポートには色々なポートを使用できる. アルゴリズムは非公開.
- いわゆるファイアウォール越えを狙ったソフト. 外部に接続可能な仮想ハブがあれば, 簡単にファイアウォールを越えられる. 故にネットワーク管理者からは嫌われている.

Soft Ether (TCP over TCP)



Soft Ether (簡略化した図)

(TCP over TCP) ユーザから見たネットワーク (全て同じネットワーク上にあるように見える)



・ IPsec (IP Security)

- IP (ネットワーク) 層で作動する暗号化プロトコル。IPv6 ではデフォルトでサポートされる (IPv4 ではオプション)。VPN のトンネリングプロトコルとしても使用可能。ただし、データ部の書き換えが不可能、処理が重いといった欠点もある。
- ESPヘッダ: パケット暗号化するためのヘッダ。
- AHヘッダ: 認証ヘッダ。送信者の署名とパケット (IP ヘッダを含む) のハッシュ値を含む。送信者の認証やデータ改ざんの検出に用いる。

