SSL-VPN（全般）

●接続先のサーバ内のアプリケーションが Web ブラウザ上で作動する場合には、HTTPS 通信を使用すれば、それが SSL-VPN となる。よって、Web ブラウザがあれば、モバイル環境やリモート環境でも SSL-VPN が構築できる。

●HTTPS 以外、例えば、LDAP over TLS や SMTP over TLS 等は、Web ブラウザではなく、SSL/TLS に対応したクライアントソフトウエアが必要になり、面倒である。

●そのため、ポートフォワーディング方式を用いることで、Java アプレットの DL 等の一定の面倒さはあるが、ポート番号は 443 になるため、FW の設定を変更する必要はない。

●L2 フォワーディングもポート番号は 443 である。

SSL-VPN（リバースプロキシ方式）

●**Web ブラウザの HTTPS 通信を使用して**、リバプロの役目を担う SSL-VPN ゲートウェイに接続する。そこから、HTTP 通信で、Web サーバ（アプリケーション）に接続する方式である。

●よって、Web ブラウザ上で動かない**アプリケーション（Outlook 等）**及びトランスポート層が TCP ではない場合には、本方式を使うことができない。なぜなら、TLS/SSL はトランスポート層のプロトコルであり、信頼性確保のため、TCP を同時に利用するため。

SSL-VPN（ポートフォワーディング方式）

●**Web ブラウザから HTTPS 通信を使用して**、VPN 装置（Web サーバに接続する直前の機器であり、リバプロと同じ位置にあると思っていい）に接続することで、クライアント PC にインストールされた Java アプレット等がポート番号を指定して、VPN 装置と SSL 通信を行う方式である。

●ポートフォワーディングするためには、TCP セグメントから TCP ヘッダ（443 ではないポート番号、例えば Outlook は 25 や 110）を取り除いた TCP ペイロード（アプリケーション層全体）を TLS でカプセル化して、それに対して、MAC、IP、TCP ヘッダ（ポート番号 443）を付けたイーサネットフレームを作る。これによって、ポート番号は 443 になるため、FW を通過できるのである。

●本方式は、リバプロ方式で使うことができなかった Web **アプリケーション**を使うことができるが、ポート番号は固定である必要がある。

SSL-VPN（L2 フォワーディング方式： L2TP over IPsec との混同注意）

●**Web ブラウザから HTTPS 通信を使用して**、VPN 装置（Web サーバに接続する直前の機器であり、リバプロと同じ位置にあると思っていい）に接続することで、クライアント PC 内に仮想 NIC を構築するソフトをインストールする。

●仮想 NIC には、接続しようとしているサーバ等がある NW と同じ NW の IPA が与えられるため、サーバ等と同じ NW（データリンク：L2）となる。つまり、データリンク層ということで、イーサネットフレームを TLS でカプセル化して、それに対して、MAC、IP、TCP ヘッダ（ポート番号 443）を付けたイーサネットフレームを作る。

●本方式は、ポート番号が動的なものにも適用できる。つまり**アプリケーション**の制約がない。

MPLS (Multi-Protocol Label Switching)

CER (Customer Edge Router)　PER (Provider Edge Router)

LER (Label Edge Router)　LSR (Label Switching Router)　LSP (Label Switch Path)

●VPN では IP を用いるものは、２つあり、IP-VPN（通信事業者が提供する専用の通信網を利用）とインターネット VPN（インターネットを利用）である。

●IP-VPN は、利用者毎のトラフィックを区別するために、IP パケットにラベルを付加して通信を制御する MPLS 技術を使用

●A 社の a 拠点 → CER → PER（LER）→ LSR → PER（LER）→ CER → A 社の b 拠点

●**PER（LER）はラベルの取り付けと取り外し。 LSR はラベルの付け替えと転送。**

●上記の LSP は片方向なので、双方向は逆向きの LSP は必要