テクニカルセンター（技術情報）

手軽にセキュアなネットワーク環境を実現する L2Connect

アプリケーションへの依存性が低いレイヤ 2 レベルの仮想プライベートネットワーク（VPN）が、簡単に実現できることで有名になったSoftEtherが登場して、レイヤ2レベルで仮想ネットワーク（VPN）を構築する手法が一般にも知られるようになりました。

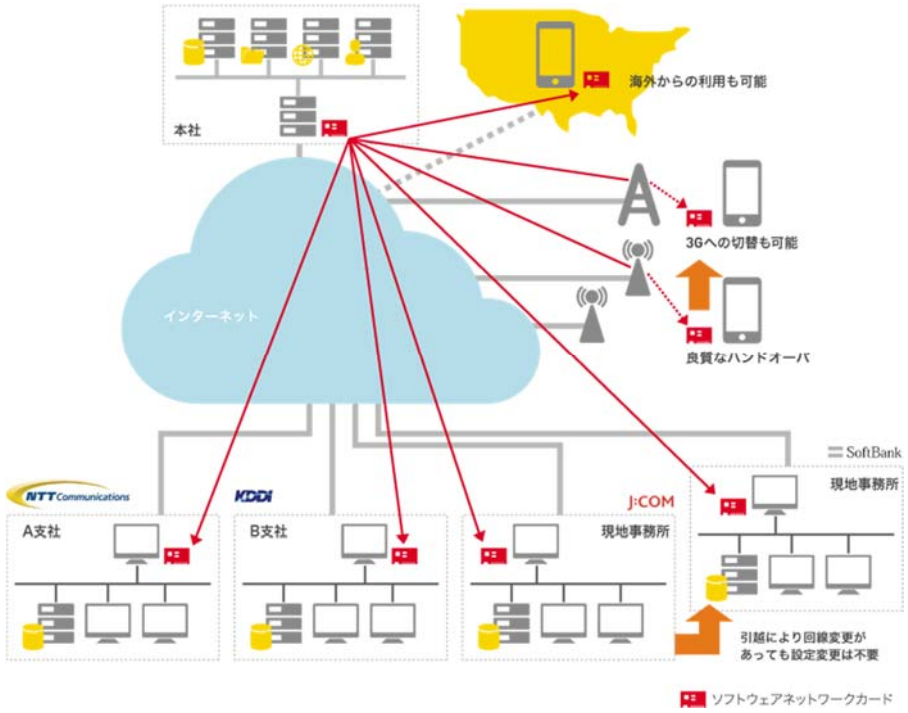
イーサネット（L2）のレベルで仮想化を行うことで、その中に通すトランスポートプロトコルやアプリケーションにまったく依存しないシステムを構築できることが、こうした技術の最も大きな魅力です。現在、運用しているアプリケーションをまったく変更しなくても、ネットワークの仮想化（VPN）を実現できるからです。

そうした長所にいち早く着目し、L2VPN ソフトウェアを開発・販売するとともに、さまざまな問題を解決できるソリューションをユーザーに提案してきました。その集大成として、企業ユーザーからのニーズをくみ上げ、エンタープライズレベルの大規模案件にもスケーラブルに対応できる優れたパフォーマンスと、多数のクライアントの管理が可能な L2Connect を開発しました。

オーバーレイネットワークの実現

L2Connect が提案するのは、簡便なインストールとシンプルな管理手法で、複数の異なるネットワークをまたがるレイヤ 2 レベルの仮想ネットワーク（VPN）の構築です。これは、“オーバーレイネットワーク”と呼ばれる技術で、既存の物理的なネットワークの上に、仮想的なネットワーク（VPN）を構築する技術です。

例えば、自社内だけでなく、関連企業、外注先、顧客などとインターネットをまたいだ仮想ネットワークを作り、その中で共通のアプリケーションを使う。あるいはサーバダウン時に、ミラーリングしてある別拠点のサーバを自動的に仮想ネットワークでつないで業務停止を防ぐなど、さまざまな活用方法が考えられます。既存のネットワークに依存しないネットワークを、常時、あるいは一時的に仮想的に構築でき、柔軟な運用が可能になります。また、BCP 対策用に柔軟な価格体系のライセンスも用意しています。



L2Connectは、もちろん一般的なVPN製品としても有用ですが、もっと幅広い用途で利用できるように、オーバーレイネットワーク構築が可能なソリューションです。

L2Connect が必要な理由

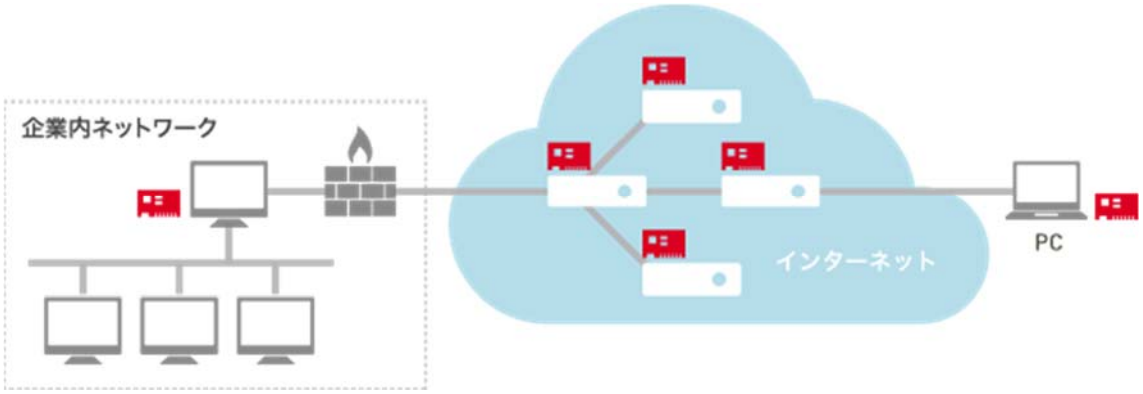
L2Connect がユニークな点は、L2 レベルの仮想化を行う技術でありながら、クライアント／サーバの形式を採用していないところにあります。

SoftEther（PacketiX）に代表される他の技術は、イーサネットをエミュレートするために、イーサネットNICと同じ振る舞いをする仮想NICをクライアントにインストールします。別途、仮想ハブを立ち上げておき、そこに接続する（仮想的なツイストペアケーブルを接続するイメージ）ことで、仮想ネットワーク（VPN）を実現している。典型的なクライアント／サーバ型ソリューションです。

仮想イーサネットであるため、トラフィックコントロールを行うには、ルーティングテーブルを作りパケットの流れをある程度制御しなければなりません。その一方で、アプリケーションからは完全に NIC として認識されるため、既存アプリケーションに対する変更は不要となります。

一方、L2Connect の仮想ネットワークも、アプリケーションから普通のイーサネットにしか見えない点は同じですが、L2Connect はイーサネット NIC やハブをエミュレートするのではなく、自身がスイッチのように振る舞います。

L2Connect ネットワークを構成するコンピュータは、すべて同じように仮想スイッチとして動作し、それぞれの仮想スイッチ間にケーブルをつなぐようにコネクションを張れば、MAC アドレスを見て仮想スイッチがパケットを目的の仮想スイッチまで届けることができます。つまり、L2Connect にはクライアントやサーバといった概念がなく、すべての構成メンバーが等価に扱われます（ほかに、オープンソースである OpenVPN が同様の形式を取っています）。



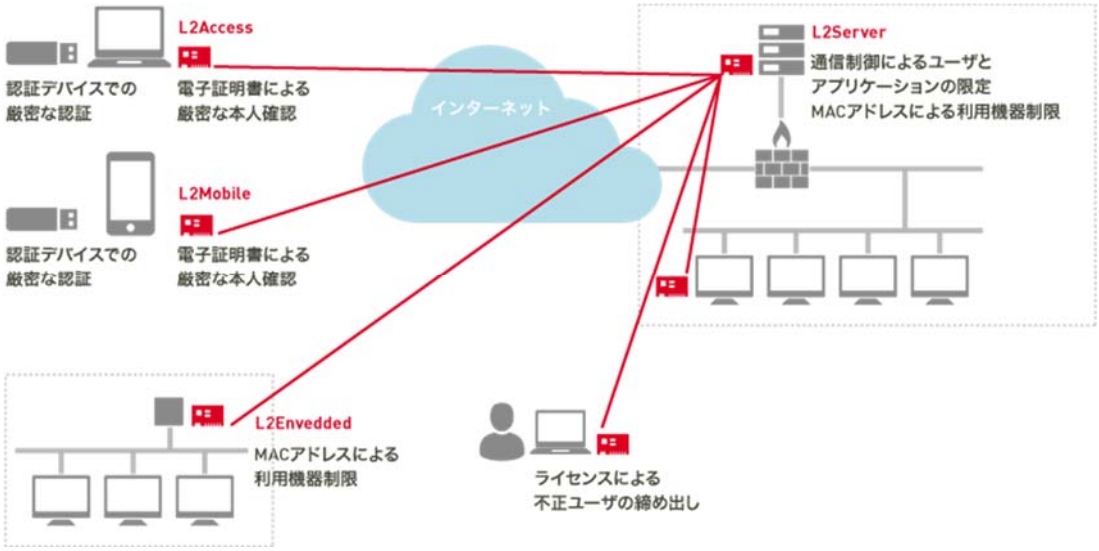
このため、大規模な仮想ネットワークを構築する際、トラフィックのコントロールをルーティングテーブルのメンテナンスで行う必要がなく、必要に応じてケーブルをつなぎ替えるようにコネクションを張るだけで運用できます。この運用の容易さが L2Connect の魅力の 1 つになっています。

またイーサネット NIC ではなく、スイッチをエミュレートする仕組みを採用したことでアーキテクチャがシンプルになり、パフォーマンスを向上させやすくなりました。トラフィックの分散が容易という特徴も、パフォーマンスを向上させるうえで重要なポイントです

つながりやすく、導入も簡単

L2Connect を用いた仮想ネットワークの構築は、実に簡単です。アプリケーションに依存しない仮想ネットワークを構築する手法としては、ほかにも IPsec があります。しかし IPsec はレイヤ 3――すなわち IP の仮想化であり、ファイアウォールや NAT などのゲートウェイを通過させるには、ゲートウェイ上で何らかの設定を行わなければならないことが多いという問題がありました。

しかし、レイヤ 2 を SSL 経由 IP ネットワーク上で実現する L2Connect ならば、そうした特別な設定を行うことなく、どこからでも、どんなアプリケーションでも透過的な通信が可能になります。



さらに L2Connect には組み込み機器向けライセンスもあり、実際に L2Connect が組み込まれた小型アダプタも発売されています。これを用いることで、自宅勤務や小規模のブランチオフィスもメンテナンスフリーで、簡単にネットワークに参加させることが可能になります。

＜OA 通信サービス様の VPN システム「L2 Connect」向けシンクライアント＞

管理面でも SNMP をサポートし、仮想スイッチをネットワーク全体の管理システムに組み込むことが容易です。添付のスイッチマネージャを用いれば、別途、管理ツールを用意しなくとも集中管理が行うことができます。

ユーザーPC へのクライアントソフトウェアの配布・配置に関しても工夫しています。一般的な setup.exe によるインストールはもちろん、オートラン機能を用いた光ディスクによる配布や、Web サイトから ActiveX を用いてインストールする手法、USB メモリの挿入による自動インストールといった手法を選択できます。もちろん、サイレントインストールに対応しているため、管理者が適切な設定をしておけば、ユーザー側に特別なインストール作業は必要ありません。

高いセキュリティと利便性を両立

セキュリティ面でもいくつかの特徴があります。一般的な ID とパスワードによる RADIUS 認証に対応するほか、電子証明書による認証もサポート。USB キーなど、外部の認証デバイスを活用することも可能です。

また、SoftEther などでは Windows 上から NIC としてクライアントソフトウェアが認識されるため、Windows 自身の機能で簡単に社内ネットワークなどとブリッジすることが可能になってしまいます。しかし、L2Connect では通常のアクセス用クライアント（L2Connect Remote Access）とブリッジが可能なクライアント（L2Connect Remote Bridge）のライセンスを分けることで、意図しない接続を防いでいます。

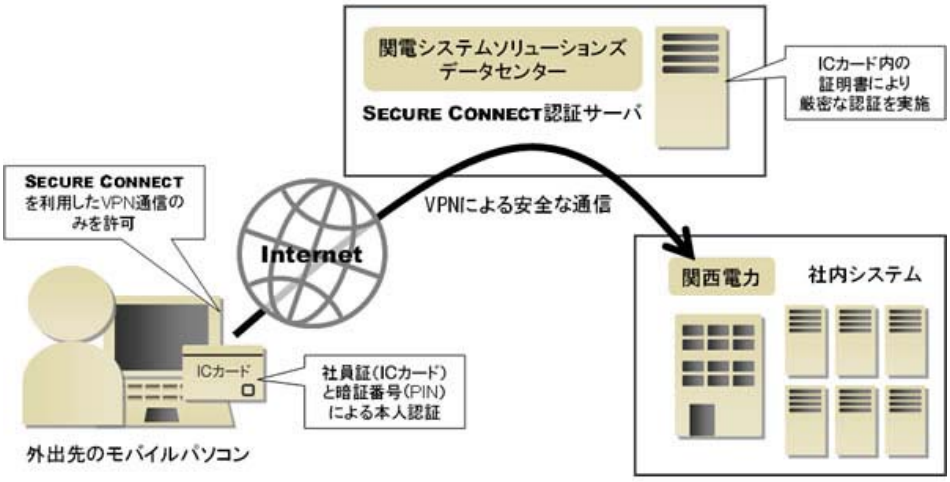
加えて接続先がどちらのクライアントソフトウェアを用いているかを判別できるため、ブリッジ可能なユーザーや機器を限定し、クライアント PC 側の運用によってセキュリティホールが発生しないように配慮しています。もちろん、MAC アドレスによるアクセス制御を行うことも可能です。

暗号化に関しても、OpenSSL を使用しており、万一、脆弱性が発見された場合でも速やかにアップデートできるというメリットがあります。OpenSSL は、広く使われているオープンソースであるため、セキュリティレベルや暗号強度、バグなどの点が実証されている点も重要な点です。大規模運用の実績も多数あり、数千人規模の仮想ネットワークにおいても高いスケーラビリティを発揮しています。

レイヤ 2 仮想ネットワークのソリューションの創成期から加わっていたので、過去の事例やサポートの実績が豊富にあります。その結果をフィードバックし、高いセキュリティレベルを維持したまま、オーバーレイネットワークを可能な限りシンプルに構築できるように設計しました。

こうしたL2Connectの機動性、機能性、安全性などに呼応して、L2Connectとともに動作するサードパーティ製品との組み合わせも可能です。

＜関電システムソリューションズ様の SECURE CONNECT＞



在宅勤務（テレワーク）に最適

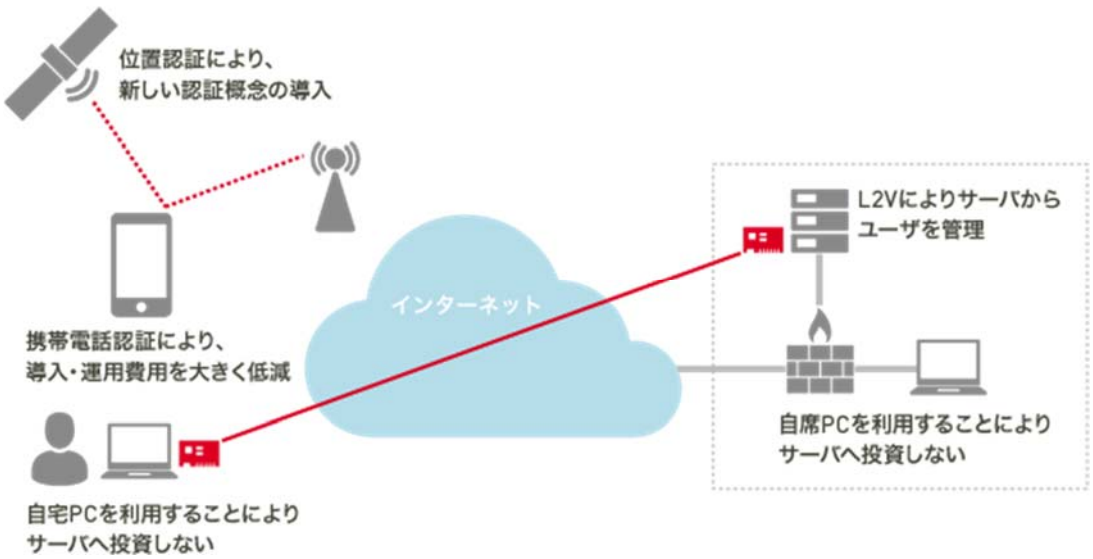
私物 PC をシンクライアント化して仕事に使わせる方法として、最も分かりやすいのが、会社の机にある PC を自宅などから遠隔操作する方法です。

普段、会社で使っている PC をそのまま遠隔操作するため、新たに仮想 PC のライセンスやアプリケーションを追加購入したり、データをクラウドサービス側に移行したりする必要はありません。PC 環境はそのままなので、「午前中は会社の PC で作業し、午後から自宅の私物 PC で作業する」といったこともスムーズに実現できます。

この仕組みには、Windows の標準機能である「リモートデスクトップ」を活用します。この機能を利用する場合、VPN を使ってインターネット経由で社内 LAN に入れるようにする仕組みと、リモートで会社の PC の電源を入れる仕組みの二つが必要になります。

VPN 経由で社内 LAN に入る仕組みでは、リモートデスクトップサービスの通信プロトコル（RDP）を利用できるようにして置きます。遠隔から PC の電源を操作する方法としては、インテルの「vPro テクノロジー」を搭載したマザーボードや、「Wake On LAN」機能がある LAN カードを使います。

＜KDDI 様の在宅勤務システム＞



従業員のワークライフバランス確保を目的に、早くから在宅勤務システムに取り組んできた KDDI。L2Connect を利用したそのユニークなシステムは、テレワーク優秀賞を受賞するほど高い評価を得ています。このシステムは、3.11 の震災直後は BCP を支え、その後は節電対策の切り札としても利用されました。

少しずつ段階的な導入が可能

そのシンプルな構成と簡単な運用。それに柔軟性と安全性に富んだセキュリティ機能などは、すべてソフトウェアのみで実現されているうえ、既存ネットワーク機器の再設定が不要であるため、小規模な導入試験から徐々にネットワーク構成を変更していくことが可能です。システムやアプリケーションの再構築を一気に進める必要がないことも大きな特徴です。

BizMobile 株式会社　（ビズモバイル株式会社）
〒101-0043　東京都千代田区神田富山町 5-1　神田ビジネスキューブ 3F
http://www.bizmobile.co.jp/