インターネット 10min 分 講座

おさえておきたい基本や、最新動向を解説するコーナーです。

VPNとは（Virtual Private Network）

VPN（Virtual Private Network）は、通信事業者のネットワークやインターネットなどの公衆ネットワーク上で作られる、仮想的な専用ネットワークの総称です。VPNと言っても、通信事業者がサービス化しているようなVPNや、インターネットなどの公衆網を用いるVPN、スマートフォンやPCから利用するVPNのように、多種多様なVPNの仕組みやサービスが存在しています。

本稿ではVPNの入門者に向けて、インターネットや専用線などとの比較から技術的な仕組みに至るまでを全般的に取り上げ、解説します。

1 VPNが必要とされる理由

VPNを使う理由は二つあります。安価に通信内容の漏洩を防ぐことと、ある程度の通信品質を確保することです。

特定の拠点同士を結ぶ技術として、専用線やインターネットを用いた通信が挙げられます。専用線では、物理的に2点間を、他のユーザーなどと共有しない専有ネットワークとして接続します。ケーブルの物理的な経由地を指定することで地理的リスクを避けることも可能ですが、通信路を専有するため非常に高価ですし、1対1（エンドツーエンド）の接続となるため、複数の拠点がある場合にはその数だけ専用線が必要となってきます。その一方で、他のユーザーの影響で障害が発生することや、輻輳して通信ができないなどの問題を考える必要はなくなります。そのため、高信頼性を求めるようなケースで利用されます。

それに対して、インターネットを用いた通信は、通信事業者の設備を数多くのユーザーで共有しているため非常に安価ですが、その反面、通信の盗聴や改ざんなどリスクが存在します。また、インターネットで接続されているすべてのサーバや端末に対して、経由する区間で帯域が保証されていないため、混雑時に通信が遅いといった問題があります。通信内容の保護は暗号化で対応可能ですが、通信品質の確保はそのままでは困難です。

そこで、通信内容の漏洩を防ぎつつ、ある程度の通信品質を確保する手段として、VPN（Virtual Private Network）が利用されるようになってきました。多種多様なVPN技術ですが、ある地点とある地点をセキュアに通信ができるように繋ぐという目的は共通しています。具体的な利用ケースとしては、遠隔地に拠点を持っている企業が拠点間を接続する場合や、手元のPCやスマートフォンなどの端末から、企業の情報システムにインターネットを経由してアクセスする場合等に利用されます。VPNを利用することで、中継点で通信内容が盗聴されたり改ざんされたりするのを防ぎつつ、悪意のある攻撃者から通信を守ることができます。

通信事業者が提供するようなIP-VPN（L3VPN）や広域イーサネット等（L2VPN）のVPNサービスは、専用線より安価かつインターネットより高品質なネットワークとしてサービス化されていることが多いです。そのようなサービスは、インターネットのように設備を複数のユーザーで共有しますが、論理的にユーザー同士の通信を分離し、セキュアなネットワークを提供します。また、ユーザー自身でインターネット等の公衆網を利用して構築する、インターネットVPNがあります。なお、通信事業者でもインターネットを利用したVPNサービスを提供しているケースもあります。

2 VPNの基本的な仕組み

先述の通り、VPNでは多数のユーザーで設備や通信路を共有しています。その設備にユーザーを接続するだけでは、それぞれのネットワークが繋がり通信ができてしまいます。そのため、VPNを実現するためには、装置内や通信路内でユーザーのネットワークごとに論理的に分離する機能が必要になります。また、インターネットを用いたVPN（インターネットVPN）のようにインターネットを通信媒体として利用する場合は、暗号化機能や認証機能を利用するケースが多いです。

装置内でユーザーのネットワークが混ざらないようにするために、ユーザーごとにルーティングやフォワーディングを行うVRF（Virtual Routing and Forwarding）や、VLAN（Virtual Local Area Network）を用いています。また、共有する通信路でのユーザーの論理的な分離は、一般的にヘッダの中にユーザー識別子を挿入するか、データのフレームやパケットを、ユーザー識別子を含んだヘッダでカプセリングすることで実現します。

そのような技術で、ユーザーは、L2VPNではスイッチ、L3VPNではルータに接続しているようにネットワークを利用することができます。

3 VPNで利用される技術

VPNに求める機能や構成の違いにより、プロトコルや仕組みは異なります。特に、OSI参照モデルのどのレイヤーでカプセル化を行うのかにより、選択される技術は大きく異なります。また、バックボーンで利用される技術と、インターネットのような公衆ネットワークで利用される技術でも違いがあります。

まずは、設備や通信路を共有した場合でも、ユーザーごとの通信が混ざらないようにするために、どのような技術を利用し実現されているのかを解説します。

通信事業者のバックボーンで利用される技術

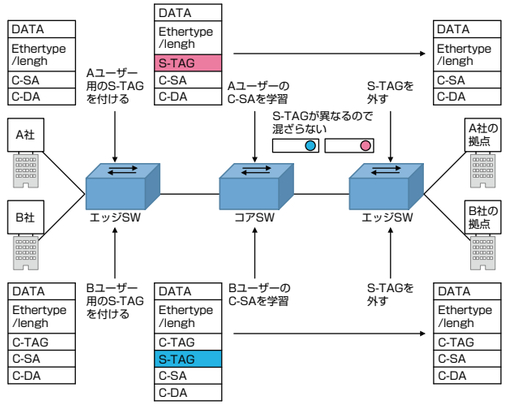
通信事業者によるVPNサービスのバックボーンは、事業者内で閉じているネットワーク（閉域網）で構築されています。また、装置が設置されているようなデータセンターや通信ビルに、関係者以外が立ち入ることができないよう物理的なセキュリティも担保されています。そのため、バックボーン内では暗号化よりも、大容量の通信を処理することができ、多数のユーザーを識別する機能が必要とされます。基本的に、通信事業者がバックボーンを持つVPNサービスでは、VPNに関わる処理は事業者のバックボーンで行われ、ユーザー拠点に設置する装置は基本的な機能のみで実現することができます。

■Layer2VPN（L2VPN）

通信事業者が提供するLayer2VPNサービスは、広域イーサネットとも呼ばれます。最も初期の段階のLayer2VPNでは、IEEE 802.1QやIEEE802.1adで規格化されているVLAN taggingやVLANを重ねる（QinQ）仕組みを用いて、ユーザーごとのネットワークの識別をしています。

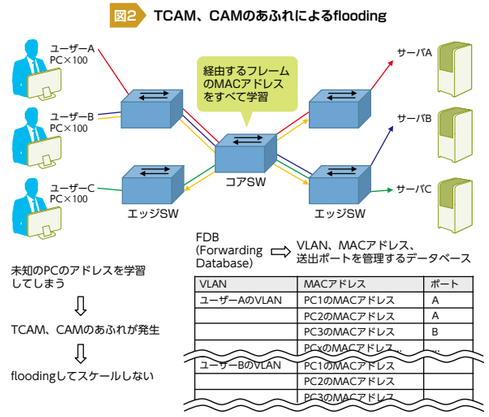
図1 Layer2VPNのイメージ

C-SA	Customer Sauce MAC Address
C-DA	Customer Destination MAC Address
C-TAG	Customer VLAN Tag
S-TAG	Service Tag



スイッチが、ユーザーを接続しているポートから受信したフレームのヘッダにVID（VLAN Identifier）を付加して、バックボーンに送信します。ユーザーの送信元MACアドレス（C-SA）は、経由するすべてのスイッチで学習され、ユーザーの送信先MACアドレス（C-DA）まで転送されます。そして、ユーザーが接続している事業者のスイッチでVIDを取り除き、ユーザーの装置へ転送されます。簡単な仕組みでユーザー分離は可能ですが、経由するスイッチすべてでユーザーのMACアドレスを学習する必要があります。図1

図2 TCAM、CAMのあふれによるflooding

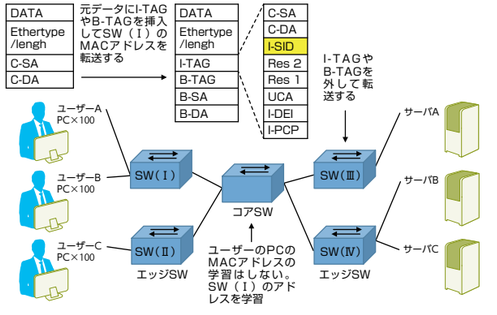


スイッチは高速にフレームを転送するために、CAM（Content Addressable Memory）やTCAM（Ternary Content Addressable Memory）等の特徴的なハードウェアを搭載しています。これらはMACアドレステーブルを検索するために利用されますが、登録できるMACアドレスの数には限りがあります。最大値を超えた場合は、登録できないMACアドレス宛の通信が繋がっているすべてのインタフェースから送信（flooding）されるため、非常に効率が悪くなります（図2の黄緑の通信）。また、VID（VLAN ID）の範囲も12bitしかないため、0-4095の範囲の4096（うち二つは予約済み）のネットワークしか識別ができません。そのため、ネットワーク全体でのユーザー収容数も限られてしまうことからスケールしない仕組みです。その結果、現在では大規模なL2VPNで利用されるケースは少なくなっています。

先述のMACアドレスの増大やVIDの不足を解決するために、IEEE802.1ah（PBB）ないしは類似の独自規格を利用してL2VPNを構築することができます。通称Mac-in-Macと呼ばれるこの仕組みは、通常のフレームにバックボーン区間装置インタフェースのMACアドレスとI-TAG（Service Instance Tag）やB-TAG（Backbone Tag）を付加することで、カプセリングを行います。その結果、コアスイッチは網内にある装置のMACアドレスを学習するだけで済むようになります。ユーザー装置のMACアドレスをコアスイッチが学習する必要がなくなるため、スケールするネットワークとなります。図3

図3 Mac-in-Macのしくみ

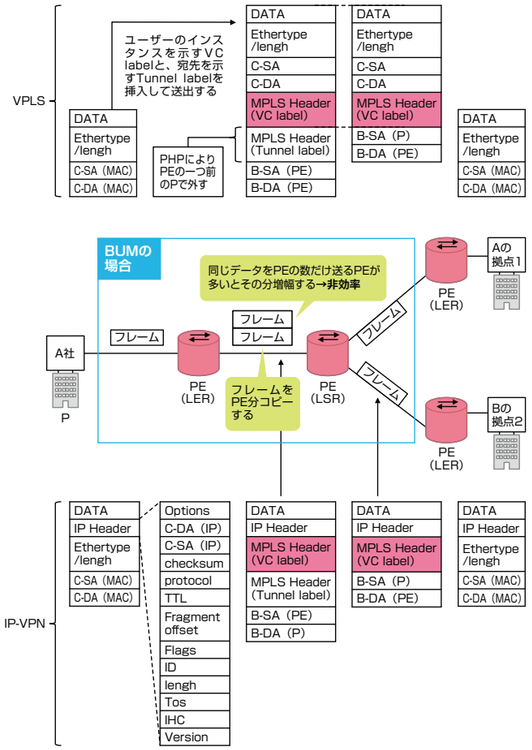
C-DA	Customer Destination MAC Address	B-SA	Backbone Sauce MAC Address
C-SA	Customer Sauce MAC Address	I-TAG	Backbone Sauce Instance Tag
B-DA	Backbone Destination MAC Address	B-TAG	Backbone VLAN Tag
		I-SID	Backbone Service Instance Identifier



しかし、この技術だけで構築するL2VPNには課題があります。標準のEthernet Frameには、ループを防ぐような仕組みがありません。そのため、物理的にループとなるようなトポロジを作ると、BUM（Broadcast, Unknown Unicast, Multicast）がループし続けることになります。ループを防ぐために、送信元MACアドレスを用いたフィルタを行うことや、Spanning Tree系統のプロトコルを利用しブロッキングポート（通信しないポート）を作る必要があります。場合によっては、物理的には隣接する装置であっても、他の離れた場所にあるスイッチを経由するなど、トラフィックの制御が難しい部分もあります。IEEE802.1aq（SPB）とPBBを用いて通信を行うことで、効率的なL2ネットワークを構築することもできますが、導入はデータセンター間のネットワーク等限定的のようです。

前述のIEEE802.1adやIEEE802.1ahでは、EthernetでL2VPNを実現する仕組みでしたが、MPLS（Multi Protocol Label Switching）ラベルを用いた仕組みでL2VPNを実現するためのVPLS（Virtual Private LAN Service）が、RFC 4761／RFC 4762で標準化されています。VPLSは、ユーザーから見ると通常のL2スイッチに接続しているように見えますが、バックボーンでは元のデータにユーザーネットワークを識別するラベル（VC Label）と、ルータ間の転送用（Tunnel label）の二つのMPLSヘッダを付けて転送されます。そのため、コアルータでユーザーのMACアドレスを学習する必要がなく、ユーザーが接続されているPE（Provider Edge）ルータでのみ学習を行えば良いことになります。また、バックボーン区間はL2ネットワークではないため、ループなどの問題を解決することができ、効率的なネットワークの利用が可能となります。

図4 VPLSとIP-VPNの比較



一方で、BUMの処理には課題があります。通常のL2スイッチでBUMを受信した場合は、接続されているリンクすべてにフレーム送信（Flooding）が行われます。VPLSでは、BUMを受信したPEルータが他のPEルータ宛に送信します。この時PEルータは、自分以外のPEルータの数だけフレームをコピーして網に送信します。その結果、必要のないPEルータにも送信することや、増幅したBUMトラフィックが同じリンクに何度も流れることで、帯域の使用効率が非常に悪くなります。図4 また、ユーザーネットワークの数が増えるとPEルータ間の仮想的なトンネル（PW: Pseudo Wire）が大量になり、スケールが難しくなるという課題もあります。

最近では、EVPN（RFC 7432／RFC 7623）のように、Data PlaneとControl Planeを分離した仕組みも標準化されてきました。それぞれのPEルータがData PlaneでMACアドレスを学習していたVPLSの仕組みとは異なり、Control Plane（MP-BGP）で広告することでUnknown Unicastの抑制も実現されています。このような新しい技術も出てきてはいますが、広域イーサネットサービスではMac-in-Macやそれに類する技術、VPLSがまだまだ主流のようです。

■Layer3VPN（L3VPN）

L3VPNでも、VPLS同様にMPLS技術を用いたIP-VPN（RFC2547bis）が利用されています。ユーザーから見ると、IP-VPNのバックボーンが一つの大きなルータのように見えるネットワークを構成します。

IP-VPNでは、MP-BGPによりPEルータが接続されているユーザーのネットワーク情報をそれぞれのPEルータが持っているため、VPLSのようにData PlaneからMACアドレスを学習する必要はありません。ユーザーが接続するPEルータはユーザーごとにVRFを持つことで、個別のRIB（Routing Information Base）を持ちます。パケットを受信したら、宛先のネットワークアドレスをもとに、VC LabelとTunnel Labelが付加されMPLS網へ送られます。最後のPEルータの一つ手前のP（Provider）ルータやPEルータで、Tunnel LabelとVCラベルが取り外され、適切なVRFへ送られルーティングされます。図4

インターネットVPNで利用される技術

インターネットVPNでは、通信事業者が持つようなバックボーンが存在しないため、ユーザーの拠点に置かれる装置の機能を利用し、インターネット経由でそれぞれの装置を接続します。さまざまなプロトコルが存在しますが、多くのルータでIPsecの実装があり利用されています。

IPsecは、暗号化技術や認証技術を用いて、通信が盗聴されたとしても内容が漏れることを防ぐことや、改ざんの検知などを行えるようにするための仕組みです。IPsecでは目的ごとにプロトコルを選択することができ、暗号化により通信が漏れても内容がわからないようにするためのESP（Encapsulating Security Payload）や、ESPよりも多くのヘッダ部分も認証をすることでより強力な認証機能を提供するAH（Authentication Header）があります。一般的に、ESPによる暗号化と認証で十分なケースが多いためESPが選択されます。

IPsecで通信を行う場合、SA（Security Association）を利用して暗号化等を行います。SAには暗号化のための鍵や、暗号化やハッシュのアルゴリズムなどの情報を含んでいます。手動で設定をすることもできますが、一般的にIKE（Internet Key Exchange）を用いて自動的に生成します。一定期間ごとや通信量ごとに新しいSAを生成することで、盗聴された場合でも解読を困難にしています。

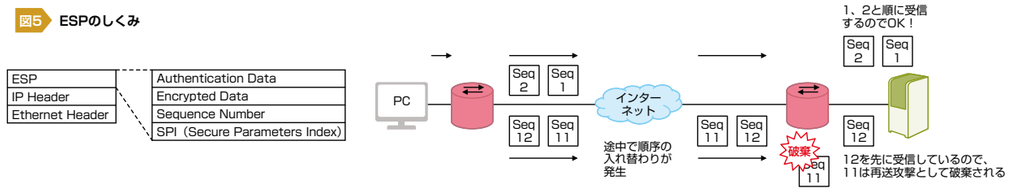
ESPには、TCPやUDPのようにポート番号などの概念がありません。そのため、一般的な家庭やオフィスで利用されているような、NAPT（Network Address Port Translation）を利用しているプライベートネットワークで利用することができません。しかしそのような場合であっても、NAT-T（Traversal）を利用することでIPsecによる通信が可能となります。NAT-Tは、ESPパケットをUDPでカプセリングすることで通信を可能にします。

ESPでは、シーケンス番号により再送攻撃を防いでいます（anti-replay）。順番に数字を大きくしていくことで、受信したシーケンス番号よりも小さな番号のパケットを受信した場合に破棄を行います。そのため、パケットが送信した順番通りに到達する通信路で利用する場合では効果的です。しかし、インターネットのように到着順が保証されていないネットワークでは、パケット順序の入れ替わりなどは恒常的に発生します。そのため、インターネットVPNでIPsecを利用する場合は、anti-replayを無効化するなどの検討も必要になります。図5

IPsec以外のプロトコルでは、OpenVPNなどの実装もあります。OpenVPNでは、NAT配下のネットワークからでも、TCPやUDPを利用してVPN接続を行うことができます。PCやサーバ上で動作する実装となっているため、一般的なルータ等では実装されていません。

インターネットVPNでは、文字通りインターネットを利用しています。そのため、通信事業者が提供する閉域網のようにインターネットから繋がらないVPNと比較して、インターネット自体の障害の影響を受けることや、攻撃を受ける可能性があります。またIKEなどの、UDPで通信を行うプロトコルを利用していることも多いため注意が必要です。認証に対するレスポンスを行うため、詐称した送信元アドレスに対してDoSを行ってしまうケースもあり注意が必要です。
https://jvn.jp/vu/JVNVU91475438/

図5 ESPのしくみ



4 インターネットVPNのトポロジ

インターネットVPNでは、特定の終端装置が決まっていないため、さまざまな形のトポロジを取ることができます。具体的には、ハブアンドスポーク型やフルメッシュ型のトポロジを作ることが多いのではないでしょうか。

ハブアンドスポーク型では、センターとなる装置に対して、それぞれの拠点から接続をします。拠点同士の通信は必ずセンター拠点を経由します。そのため、通信が遠回りする結果、遅延や速度が出ないなどの問題が発生する場合があります。しかし、新しく接続先を追加するときには、新しいルータの設定とセンター側の設定のみで済むため非常に安易です。

フルメッシュ型では、すべての拠点のルータ間でVPN接続をするため、拠点同士で直接通信ができて効率的です。しかし、新しい拠点のルータを追加するたびに、設定済みのすべてのルータを再設定する必要があります。また、VPNの接続先が増えてきた場合に、装置の最大VPN数を超えてしまうと、すべての拠点で装置を増強しなくてはなりません。

最近では、ダイナミック（マルチポイント）VPNの実装がある装置も増えてきています。ダイナミックVPNは、通常はハブアンドスポーク型でセンター拠点に対してVPN接続をしますが、拠点間の通信が発生した場合に、拠点間で通信ができるVPNを自動で構成します。設定は簡易となり、フルメッシュ型の恩恵を受けることもできる仕組みです。ベースには標準的なプロトコルが利用されていますが、さまざまな標準的なプロトコルを組み合わせた独自プロトコルであるケースが多いです。

5 セキュリティとVPN

ここまでセキュリティの向上を目的としたVPNについて説明をしてきましたが、悪意のある攻撃者が通信を秘匿するために、カプセリングや暗号化が利用されるケースも多々あります。

VPNで利用されるような技術が悪意のある通信で用いられると、管理者はVPNを利用しているという事実やVPNを終端している対向装置のIPアドレスや通信量などの、限られた情報しか知ることができません。そのため、通信内容を確認することができず、正規の通信か悪意のある通信か判断をすることができません。

通信内容の判断できないため、企業内ではVPNで利用されるプロトコルをファイアウォール等で制限する場合があります。しかし、マルウェアは標準的なVPN用のプロトコルが利用できない環境でも動作するように、一般的なHTTPやHTTPS、ICMP、DNS等のプロトコルを用いることで、通信を行うケースがあります。データを埋め込むことが可能なフィールドに、暗号化したデータを埋め込むことで実現が可能です。データの内容で判断できないため、通信の傾向を監視するなどの対策が必要となります。

6 最後に

本稿では、VPNの入門者を対象として、過去の技術から現在一般的な技術について簡単に紹介をしてきました。新しいプロトコル等が出てきていますが、核となる技術は変わっていないため、まずは基本について理解を深めることが大切です。

VPNサービスはその特性上、一つの事業者の中で閉じてしまう傾向が強いネットワークサービスです。しかし、現在ではオンプレミス型の業務システムではなく、クラウド上のサーバで業務システムを動作させる企業なども増えてきています。そのため、今後は事業者内で閉じたネットワークから、他事業者も含めセキュアに相互接続し、環境の変化に耐えられることを期待します。

（インターネットマルチフィード株式会社 高橋祐也）