拠点間ネットワークに適用可能なオーバーレイネットワークの設計と運用

2021 年 8 月

関谷 勇司[1]、田丸 健三郎[2]、大江 将史[1]、中川 あきら[1]

要旨

政府省庁においては、IT システムを構築・運用するにあたりセキュリティ的及び情報管理上の観点からシステム専用の閉域網(クローズドネットワーク)を構築し、その閉域網内にシステムが構築されている例が多い。この閉域網を構築するにあたっては、専用回線若しくは通信キャリアによる閉域網構築サービスが用いられている。

しかし、専用回線や通信キャリアによる閉域網サービスを用いなくとも、オーバーレイネットワーク技術を用いることで低コストかつ十分なセキュリティを確保した仮想的な閉域網を構築できる。また閉域網の運用においても、オーバーレイネットワーク技術による閉域網は、構成変更やアンダーレイ回線の移行を柔軟かつ短時間で行える等の利点がある。

これらオーバーレイネットワーク技術の利点を活かすためには、その用途や構成により適用すべきオーバーレイネットワーク技術及び運用方法が異なる。これらの点をふまえ、本文書はオーバーレイネットワークの設計と運用について述べる。

[1] 内閣官房政府 CIO 補佐官
[2] 内閣官房情報通信技術（IT）総合戦略室 プロジェクトマネージャー

改定履歴

改定年月日	改定箇所	改定内容
2021 年 8 月 31 日		初版

目次

１　はじめに

本節では、本文書の位置づけを定義し、オーバーレイネットワークが必要とされる背景と、オーバーレイネットワークの設計と運用の概要について述べる。

１．１　背景と目的

ネットワークはデータを伝達するための重要なインフラであり、現在の IT システムにとって欠かすことのできない情報インフラとなっている。そのため、機密性の高いデータをネットワーク経由で転送する機会も増加している。現在の一般的なネットワーク設計手法においては、通信の秘匿性を確保したい場合には、通信を暗号化したり用途に応じてネットワークを分離したりすることにより秘匿性を確保している。従来の政府省庁ネットワークにおいても、物理的な回線やネットワーク機器を分離することによって、通信の秘匿性を確保する手法が用いられてきた。物理的な分離は、物理的回線やネットワーク機器の管理が信頼に足りうるものである限り、秘匿性確保の有用な手法となる。その一方で、分離された物理ネットワークの数が増えるにつれ、設備の設置コストや管理コストは増大する。

そのため、従来のネットワーク設計においては、分離のための手法としてネットワーク仮想化が用いられている。ネットワーク回線やネットワーク機器を仮想的に分離することにより、同一の物理ネットワークの上に、複数の分離されたネットワークを仮想的に構築することが可能となる。本文書でとりあげるオーバーレイネットワークも、この仮想化ネットワークを構築するための一手法である。特に、近年は SD-WAN（Software Defined Wide Area Network）に代表されるような、オーバーレイネットワークを動的かつ自律的に構築し、構築されたネットワークをコントローラから集中管理できる技術が登場している。このような新しい技術を用いることで、オーバーレイネットワークの冗長化や、日本全国に広がるような広域オーバーレイネットワークの管理が可能となる。

政府省庁における専用ネットワークは、専用回線や通信キャリアによる広域 WAN サービスによって構築されている場合が多い。専用回線や広域 WAN サービスを利用した閉域網は安定性やセキュリティの面で優れているが、その一方で構築時のコストや構成変更を行う場合のコスト及び即時性において問題点がある。特に政府の場合には、構築や構成変更にかかるコストが高くなる程、調達に時間がかかるため、要求に応じて即時に閉域網を構築することが難しい。そこで本文書で取り上げるオーバーレイネットワーク技術を適用することで、構築や構成変更に必要となるコストと時間を削減することが可能となる。

そこで本文書では、こうした新たな技術を用いて仮想化されたネットワークを構築する手法をまとめ、政府省庁ネットワークに導入するにあたっての技術の選定方法及び構築と運用手法について述べる。

１．２　適用対象

本文書にて述べる新たなオーバーレイネットワーク構築手法は、物理的な分離を用いて構築

されている閉域網及びシステムや、従来の VPN（Virtual Private Network）技術を用いて構成されている閉域網に対して適用可能である。新たなオーバーレイネットワーク構築手法を適用することにより、閉域網の構築と運用のコスト削減及び構成変更の柔軟性と即時性がもたらされる。

１．３　位置づけ

本文書で定義するオーバーレイネットワークは、政府省庁の拠点間にて構築される閉域網にて、構築のコストと納期を短縮し、要求に応じて柔軟かつ短時間で構成変更が必要となるような閉域網に対して有用である。

１．４　用語

本文書において使用する用語は、本文書に別段の定めがある場合を除く他、標準ガイドライン群用語集の例による。

２　オーバーレイネットワーク

本節では、本文書が対象とするオーバーレイネットワークを定義し、その技術要素について概要を説明するとともに、オーバーレイネットワーク利用時の利点と欠点について述べる。

２．１　オーバーレイネットワークとは

一般的にオーバーレイネットワークとは、物理的に構成されたネットワークの上で、物理構成にとらわれずに論理的に自由に構成を定義することにより、特定の用途専用に構成されたネットワークを意味する。物理的ネットワークとは、ルータやスイッチといったネットワーク機器とそれを結ぶネットワーク回線によって構成された、機器と回線に従って構成されるネットワークを意味する。ネットワーク機器を設定することによって伝達範囲を定義し、ネットワークを構成する。この場合でも、VLAN や MPLS といった技術によって、物理ネットワークを分割して複数の専用ネットワークとして利用することができる。これらネットワーク仮想化技術は、主に単一の管理ドメイン内部で使われる技術である。つまり、事業者をまたがった広域網やインターネット上で利用される技術ではなく、物理ネットワークの上に複数の分離されたネットワークを構築するために利用される技術である。構築されたネットワークは論理的なネットワークと言えるが、あくまでも物理ネットワークの分離により構成された論理ネットワークである。

一方、オーバーレイネットワークは、管理ドメインを超えて複数の事業者にまたがって利用することが可能である。これは、オーバーレイネットワークを実現する多くの技術が、ネットワーク層（IP 層）にて IP トンネリングと呼ばれる手法を用いているためである。インターネットにて用

いられている TCP/IP は、IP ヘッダと呼ばれる部分に送信元や送信先といった、通信に必要な情報が記述されている。図 1 に示す通り、この IP ヘッダを多重にすることをトンネリングと言い、本来の配送先と論理ネットワーク上での配送先を入れ子にして記述することで、論理ネットワークの構成を実現している。

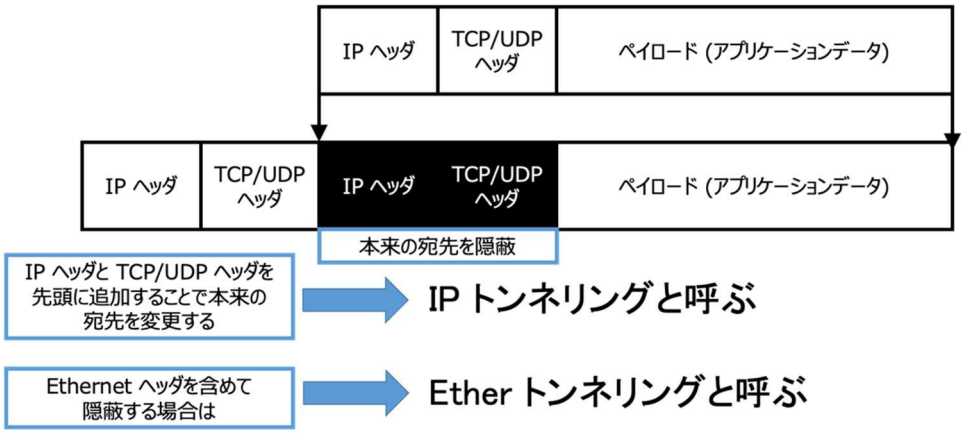

図 1： IP トンネリングによる IP ヘッダの多重化

IP ヘッダを多重化する IP トンネリング手法は、TCP/IP による IP ヘッダを用いたデータ配送の仕組みをそのまま利用できるため、事業者をまたがった広域網やインターネットにおいても利用可能である。つまり、IP トンネリング技術を用いたオーバーレイネットワーク構成技術においては、全世界を対象としたインターネット規模で論理ネットワークを構成可能である。

現在、職場や組織内の資源にアクセスするために用いられている VPN（Virtual Private Network）技術も、IP トンネリング手法を用いているものが多くあり、オーバーレイネットワークの一種と言える。しかし、通常の VPN は 1 対 1 の通信路を構成するために用いられており、網としての論理ネットワークを構成する技術ではない。本文書が意味するオーバーレイネットワークとは、図 2 に示す通り、物理ネットワークと同様に複数のデバイスや資源が同時に接続され、網を構成できる論理ネットワークを意味する。また、網を構成するとは、複数の論理パス（仮想回線）を用いて拠点や機器同士を接続し、論理ネットワーク上で経路制御を行うことを意味する。

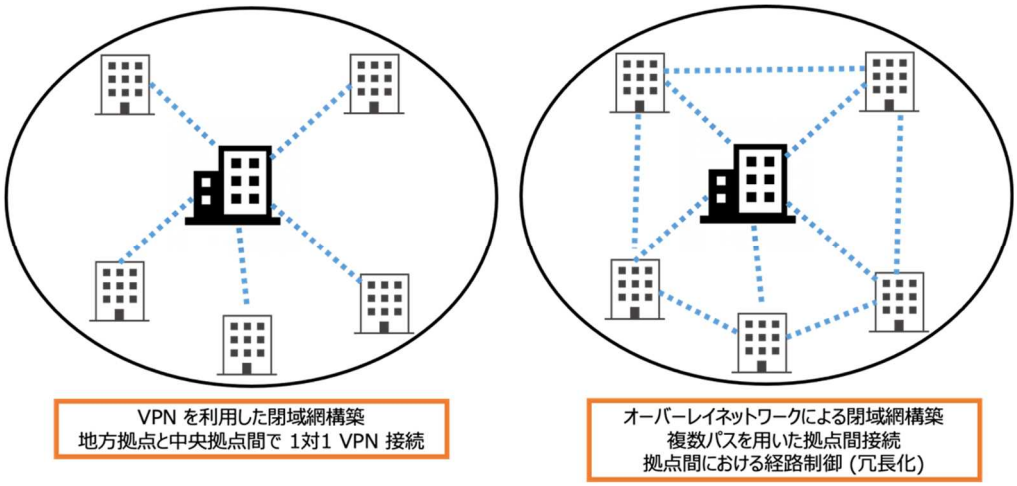

図 2 ： VPN とオーバーレイネットワークの違い

また、オーバーレイネットワークを構築する基盤となるネットワークをアンダーレイネットワークと呼ぶ。アンダーレイネットワークとは物理ネットワークであり、オーバーレイネットワークはその物理ネットワークの上に構築される仮想的な論理ネットワークと定義されることが一般的である。物理ネットワークを構成変更する場合は、その物理ネットワークを管理しているネットワーク管理者が設定変更を行う必要がある。設定変更したい範囲が複数ドメイン、すなわち複数の事業者にまたがっている場合には、それぞれの組織の管理者に対して設定変更を依頼する必要がある。実現したい構成によっては、新たな回線の敷設や、新たなネットワーク機器の導入が必要となる場合がある。

一方オーバーレイネットワークでは、ネットワークを導通したい端点と端点における設定変更を行うことで、新たな論理ネットワークを開通することが可能である。端点及び端点と端点を結ぶために経由している中間の物理ネットワークに対する変更は必要ない。オーバーレイネットワークは基本的に端点と端点のみで実現される論理ネットワークであり、一般のネットワーク利用者の権限で構築することができる。論理ネットワークを開通したい両端点にオーバーレイネットワークを構築できる機器を設置し適切な設定を行うことで、端点間の距離がどれだけあろうとも、インターネット上で論理ネットワークを開通することができる。アンダーレイネットワークとオーバーレイネットワークの関係を図 3 にまとめる。

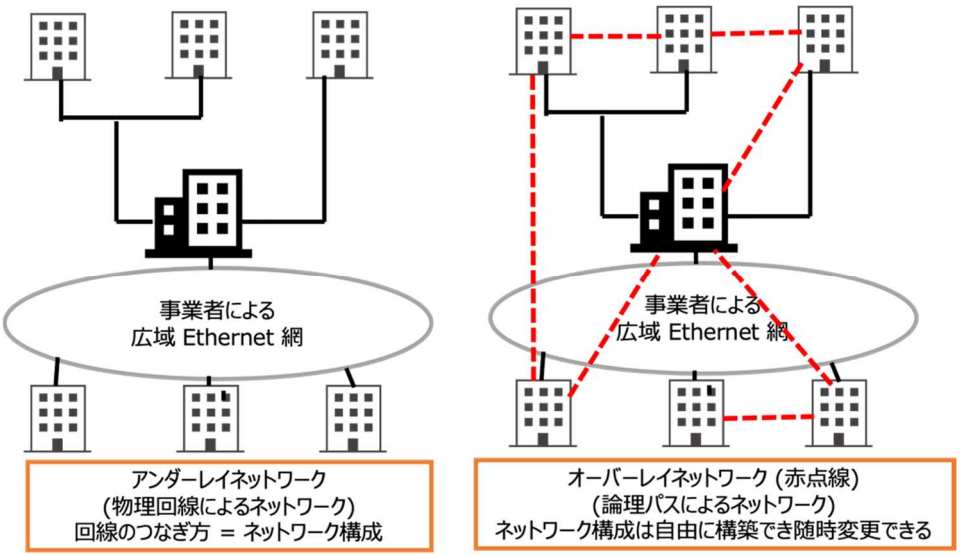

図 3 ： アンダーレイネットワークとオーバーレイネットワークの関係

２．２　オーバーレイネットワークを構成する技術

前述の通り本文書では、複数の論理パスを用いて拠点や機器同士を接続でき、かつ構成した論理ネットワーク上で経路制御が行える論理ネットワークをオーバーレイネットワークと定義する。このオーバーレイネットワークを実現するためには、基本的に IP トンネリングと呼ばれる手法が用いられる。具体的な技術としては、次のような技術があげられる。

- VXLAN
- Geneve
- NVGRE
- STT
- L2TPv3
- EVPN
- SD-WAN

どれも IP ヘッダを多重化することで、アンダーレイネットワークである TCP/IP 、すなわちインターネットの上で世界規模の論理ネットワーク構成を実現できる。これら技術の概要について述べる。

VXLAN

VXLAN (Virtual eXtensible Local Area Network) は、VXLAN ID と呼ばれる ID を用いてネットワークの識別と分離を行うオーバーレイネットワーク技術である。IP ヘッダ + UDP ヘッダを用いて多重化しており、アンダーレイネットワークにとっては UDP 通

信として認識される。VXLAN は、TCP/IP 上にて VXLAN ID を用いてネットワーク分離を行う手法のみを定義しており、論理ネットワークを構築したい拠点間を論理パスにて結ぶことは可能となるが、その論理パスを用いて経路制御を行うためには、別の技術を組み合わせる必要がある。一般的には、EVPN と呼ばれる技術と併用することでオーバーレイネットワークを構築できる。また、VXLAN では、Layer 2 / Layer 3 どちらのオーバーレイネットワークも構築可能である。図 1 に示した通り、Ethernet ヘッダーを含めた IP トンネリングを行えば、Layer 2 ネットワークを延伸することが可能である。

Geneve

Geneve(Generic Network Virtualization Encapsulation) は、他の技術と同様に IP ヘッダの多重化を用いて論理ネットワーク構築を実現している。VXLAN が VXLAN ID と呼ばれる識別子のみを用いてネットワークの分離を行っているのに対し、Geneve は単一の識別子ではなく拡張可能なフィールド（メタデータ）を用いて、複数の情報を用いてのネットワークの識別と分離が可能となっている。アンダーレイネットワークに対しては、VXLAN と同様 UDP パケットとして認識される。Geneve も論理パスの形成のみを定義しており、経路制御を行うためには別の技術との組み合わせが必要となる。また、Geneve は基本的に Layer2 オーバーレイネットワークを構築するための技術である。

NVGRE

NVGRE (Network Virtualization using Generic Routing Encapsulation) は、VSID と呼ばれる識別子を用いてネットワークの識別と分離を行う技術である。VXLAN との違いは、多重化に際して IP ヘッダと GRE ヘッダを用いている点である。拠点間を結ぶ VPN 技術として用いられている GRE という技術を拡張し、オーバーレイネットワークの構築に適用できるようにした技術である。アンダーレイネットワークにとっては、GRE の通信として認識される。前述の技術と同様、経路制御を行うためには他の技術との組み合わせが必要となる。NVGRE も Geneve と同様、Layer2 オーバーレイネットワークを構築するための技術である。

STT

STT (Stateless Transport Tunneling Protocol) は、Geneve と同様に複数の情報（メタデータ）を用いてネットワーク識別と分離を行う技術である。他の技術との違いは、IP ヘッダと TCP ヘッダを用いて多重化を行う点である。これにより、サーバのネットワーク機器に組み込まれている、TCP Offloading という機構を利用することができ、オーバーレイ処理の高速化を狙った仕様となっている。他の技術と同様に、経路制御を行う

ためには別の技術との組み合せが必要であり、基本的に Layer2 オーバーレイネットワークを構築するための技術である。

L2TPv3

L2TPv3 (Layer 2 Tunneling Protocol version 3) は、その名前の通り Layer2 のオーバーレイネットワークを構築するための技術である。他の技術のように、何らかの識別子を用いてネットワークの識別と分離を行うのではなく、物理ネットワークの Layer2 情報をそのままオーバーレイネットワークを用いて伝搬する技術である。つまり、ネットワークの分離と識別には、物理ネットワークで利用されている VLAN などの手法が用いられる。また、他の技術と同様に論理パスの形成を行う技術であり、経路制御は他の技術を併用することで実現される。

EVPN

EVPN (Ethernet VPN)は、Ethernet 上で Layer2 及び Layer3 の VPN を構成するための制御情報を交換する技術である。BGP (Border Gateway Protocol) の機能を拡張し、BGP のメッセージを用いて VPN の制御情報を交換する。これにより、VPN を構成する技術に関わらず、VPN の構成情報とネットワーク内部の制御情報を交換し、VPN 上のネットワーク網制御を行うことができる。オーバーレイネットワーク上の通信制御情報を交換する、実質上の標準技術である。

SD-WAN

オーバーレイネットワークを構築する一つの手法として SD-WAN (Software Defined Wide Area Network) と呼ばれる製品が登場し普及しつつある。SD-WAN は、オーバーレイネットワークを構築するための論理パス技術 (データプレーン) と経路制御技術(コントロールプレーン)、オーバーレイネットワークを構築する機器の管理軽減 (ゼロタッチプロビジョニング)及びそれらを管理するための統合管理ソフトウェア (オーケストレータ) を組み合わせることで、オーバーレイネットワークをすぐに構築し運用開始できるパッケージとして提供されている。

なお、SD-WAN は特定の技術を示す用語ではなく、オーバーレイネットワークをすぐに開始できる統合ソフトウェアパッケージの総称となっている。SD-WAN 製品は複数社から販売されており、付加機能としてセキュリティ機能、トラフィック識別機能、通信高速化機能などが搭載されている。どの製品も、拠点に設置する機器の統合管理、トラフィック制御、セキュリティ機能等が備わっており、オーバーレイネットワークを構成するのに最も適した製品となっている。

以上の通り、オーバーレイネットワークを構築するための技術について、概要をまとめた。

EVPN を除くこれら技術は、あくまでも拠点間（端点間）の論理的な通信路を形成する技術であり、その上でどうデータを伝達するか、すなわち通信の経路制御を行うかは別の技術と組み合わせることで実現される。一般的には EVPN や RSVP (Resource reSerVation Protocol)といった論理ネットワークを制御するための技術と組み合わせて用いられる。

２．３　セキュリティの確保

オーバーレイネットワークは、特定の用途に使う端末や機器だけが接続される、機密性の高い閉域網である場合が多い。すなわち、アンダーレイネットワークとしてインターネットを用いている場合でも、オーバーレイネットワークには高い機密性が求められる。このような用途においては、分離されるそれぞれのネットワーク間でお互いの通信内容を傍受や改ざんすることができないこと、また、アンダーレイからオーバーレイネットワーク内部の通信内容を傍受や改ざんできないことが求められる。また、オーバーレイネットワークの経路制御も同様であり、管理者以外の第三者がコントロールプレーンの通信を傍受や改ざんできないことが必要となる。

このような機密性を確保するために、暗号化技術との組み合せによる論理パス形成が必要となる。具体的には SSL 技術や IPsec 技術を用いた通信内容の暗号化と送信元の保証が必要となる。

オーバーレイネットワークを構築する場合には、通信の機密性を考慮し、どの論理ネットワークに対してセキュリティ技術を適用すべきかの検討が必要となる。また、アンダーレイネットワークがインターネットであるのか、若しくは自組織が管理する物理ネットワークのみによって構成されるのかによっても、オーバーレイネットワークに導入すべき機密性、すなわちセキュリティのレベルが異なる。基本的には、データプレーンもコントロールプレーンも暗号化されるべきであるが、例えばデータセンター内部のネットワークのように、アンダーレイネットワークが自組織の物理ネットワークのみで構築されており、第三者によって通信が傍受されたり改ざんされたりする可能性がないのであれば、オーバーレイネットワークの暗号化を省ける場合もある。

前述の SD-WAN 製品は、これらの暗号化と送信元の保証が導入されている製品がほとんどであり、傍受や改ざんがほぼ不可能なオーバーレイネットワークを実現している。逆に言えば、この要件を満たさない SD-WAN においては、アンダーレイネットワークとしてインターネットを利用すべきではない。

２．４　オーバーレイネットワークの利点と欠点

オーバーレイネットワークの利点は、回線事業者に依頼すること無くネットワーク管理者が自身にて自由なネットワークを構成できることである。また、経路制御によって複数の物理パスを動的に切り替え、論理パスの冗長性を確保できるという利点もある。

例えばアンダーレイネットワークとして通信事業者による光回線と携帯受け（LTE や 5G）の両方を利用することで、光回線に障害が発生した場合にも自動的に携帯回線側に通信を迂回し、通信を継続することができる。

一方で、オーバーレイネットワークの欠点としては、まず通信性能の低下があげられる。オーバーレイネットワークを実現する機器によっては、IP ヘッダの多重化といったオーバーレイ通信の処理をハードウェアにて行えるものもあるが、SD-WAN に代表される多くの製品は、オーバーレイ通信処理をソフトウェアにて行っている。そのため、物理ネットワークよりもオーバーレイネットワークの方が通信速度が低下する傾向にある。さらに、前述の暗号化などのセキュリティ処理を行うと通信時の処理時間が増えるため、さらに通信速度が低下する。オーバーレイネットワークを利用するユーザ数や通信量に応じて、適切な処理性能を有したオーバーレイ技術、もしくは製品を選定する必要がある。

もう一点、オーバーレイネットワークにおける設計上の留意点としては、アンダーレイネットワークとの構成不整合があげられる。オーバーレイネットワークは、拠点間で自由に論理パスを形成することができるため、図 4 のようにアンダーレイネットワークの構成と論理パスの形成の仕方によっては、一部の物理ネットワーク回線や拠点に通信が集中してしまう場合がある。オーバーレイネットワークの構成を考えるにあたっては、物理ネットワークの構成も考慮したネットワーク構成が望ましい。

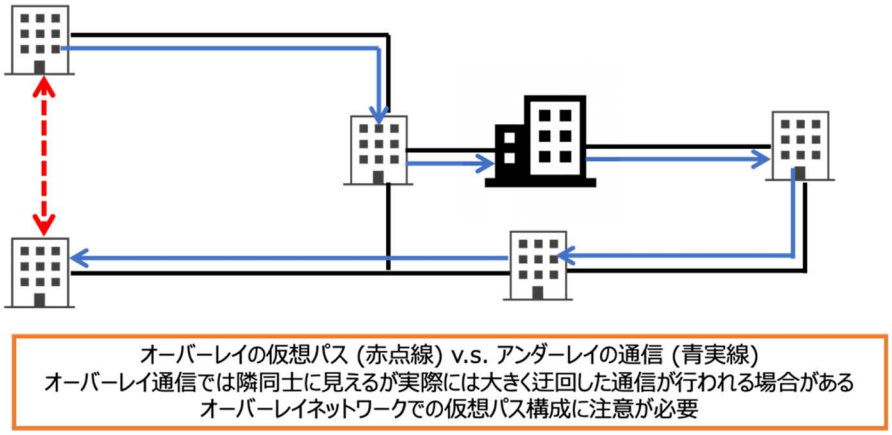

図 4 ： 非効率なオーバーレイネットワーク通信例

3 導入と運用

本節では、前節までに述べたオーバーレイネットワークの技術及び技術的な利点欠点をふまえ、導入形態に基づいた技術と製品の選定について述べる。

3．1 ネットワーク構成に応じた技術の選定

オーバーレイネットワークを導入するにあたり、オーバーレイネットワークの利点が活かせるネットワーク要求と構成となるようにする必要がある。

専用回線かオーバーレイネットワークか

拠点間の距離が近く、かつ大容量の通信を行う場合には、キャリアによる専用回線やダークファイバを用いた物理回線で構成される拠点間ネットワークを検討するべきである。この場合の専用回線とは、複数顧客を集約接続して帯域を保証しないベストエフォート回線ではなく、キャリアによって帯域が保証され、拠点間にて物理的に専用回線を敷設するものを意味する。目安としては、常時 1Gbps 以上の通信が行われ、かつ拠点間の距離が 10km 以内であるならば、帯域保証専用回線若しくはダークファイバを敷設する方が安価かつ要求に応えられる構成となる。

また、拠点が複数あるネットワーク構成では、物理回線の場合にはスター型構成の中心となる拠点を選出し、そこに中心点となるネットワーク機器を設置する必要がある。一方で、オーバーレイネットワークの場合には端点に設置された機器のみで、複数拠点が相互に連結されたネットワーク網を構築することができる。そのため、ネットワークに参加する拠点数が多い場合には、オーバーレイネットワークの方が有利となる。この場合は、複数拠点を接続できるオーバーレイネットワーク技術を選択する必要がある。

まとめると、**(1)拠点間の距離が近くマルチポイント構成若しくはスター型構成が必要であれば専用線の敷設、(2)拠点間の距離が離れておりマルチポイント構成が必要であればオーバーレイネットワーク、(3)拠点間の距離が離れているスター型構成の場合は、専用線とオーバーレイネットワークのどちらが有利かをコストにて判断**する。

バックアップとしてのオーバーレイネットワーク活用

拠点間を物理回線にて接続した場合には、バックアップとしてオーバーレイネットワークを活用する構成が考えられる。バックアップ回線にベストエフォート型の回線を採用し、それをアンダーレイネットワークとしてオーバーレイネットワークを構築することで、安価かつ簡易にバックアップ網を構成することができる。

オーバーレイネットワーク構築技術の選定

前述の通り、オーバーレイネットワークを構築するにあたっては複数のトンネリング技術が存在する。また、オーバーレイネットワーク網にて経路制御を行うためには、EVPN と組み合わせた運用が必要となる。基幹ネットワークにオーバーレイネットワークを導入する場合には、物理ネットワーク上に複数のオーバーレイネットワークが構成され、通信容量も大きなものになると想定される。この場合には、前述の IP トンネリング処理をハードウェアで行うことができる機器を導入し、IP トンネリングと EVPN の組み合わせによるオーバーレイネットワーク構成が適している。これらの観点から、**基幹ネットワークにオーバーレイネットワークを導入するにあたっては、VXLAN + EVPN によるオーバーレイネットワーク構成が最適**である。市販のネットワークスイッチには、VXLAN のハードウェア処理をサポートしているものが多く、また VXLAN 自体が十分に標準化されている仕様であるため、異なったベンダーによるネットワークスイッチ間でも相互

接続可能となっている。また、インテグレータも VXLAN であれば構築経験を有している社が多いため、設定等も問題なく行える。

一方、地方合同庁舎の遠隔拠点と本省を接続する等、インターネットをアンダーレイネットワークとして**距離の離れた拠点同士をオーバーレイネットワークにて接続する場合には、ソフトウェアにてオーバーレイネットワークを実現する安価な機器を導入すべき**である。典型的な利用形態として、地方合同庁舎と本省の間でオーバーレイネットワークを構成する場合を想定する。この場合は、一種類の閉域網を構成する、若しくは多くても数種類の閉域網を構成する場合がほとんどであり、通信量も 1Gbps 以下である場合が多い。このような用途には、IP トンネリングをハードウェア処理する機器よりも、ソフトウェア処理にてオーバーレイネットワークを実現する、安価で小型な機器が適している。これらの観点から、インターネット経由で本省と地方合同庁舎間にてオーバーレイネットワークを構成する場合には、**ベストエフォート型のコンシューマー回線と暗号化 VPN 機能を備えた小型ルータ機器、若しくは SD-WAN 製品の組み合わせ**が適している。暗号化 VPN の場合には、L2TPv3、GRE + IPsec 等の技術が適用できる。

３．２　オーバーレイネットワークの設計と構築

典型的な事例と要件に基づいた、オーバーレイネットワークの設計と構築について述べる。

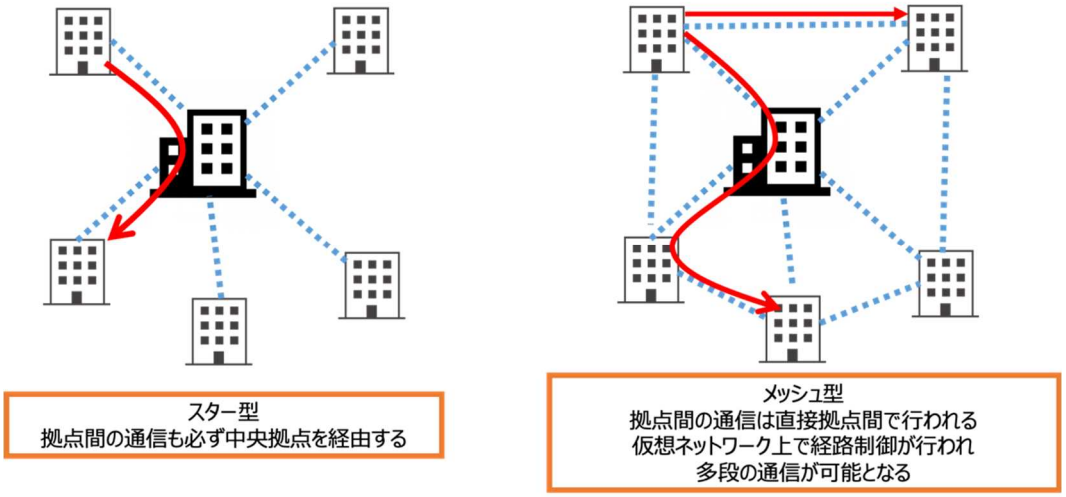

図 5 ： スター型とメッシュ型

スター型構成

本省と地方合同庁舎との通信のように、中央と遠隔地との間の通信が大部分であり、遠隔地同士の通信はほとんど行われない場合には、図 5 に示すスター型構成が適している。この構成では、遠隔拠点の間で通信を行う場合にもすべての通信が中央を経由する。製品としては、前述の通り**暗号化 VPN が利用可能な小型 VPN 機器**が適している。中央にて複数の VPN を

終端し、遠隔拠点同士をルーティングする設定を行うことで、オーバーレイネットワークを実現できる。しかし、スター型構成で小型 VPN 機器を利用する場合には、多くの場合が集中管理には適しておらず、個々の機器を個別に設定する必要がある。また、複数の回線(例えばベストエフォート型回線と LTE の併用等)を利用した、回線障害に対応できる冗長構成の実現は難しい。構築と運用を簡易に行いたい、若しくはオーバーレイネットワークに冗長性を導入したいのであれば、SD-WAN 製品を導入すべきである。

メッシュ型構成

遠隔拠点同士で頻繁に通信を行う場合、若しくは拠点間の通信に冗長性を持たせたい場合には、図 5 に示すメッシュ型構成が適している。構成としては、遠隔拠点にはインターネット接続としてベストエフォート型回線を導入し、中央省庁や地方合同庁舎の大きな拠点には専用回線によるインターネット接続を導入し、オーバーレイネットワークを構成する機器を各拠点に導入する。この際に導入する機器は、SD-WAN 製品が適している。SD-WAN 製品は、CPE (Customer Premises Equipment) と呼ばれる機器を各拠点に設置することで、GRE + IPsec 等(若しくは製品によって異なるプロトコルや独自のプロトコルを利用)を用いて、CPE 間でメッシュ型の仮想パスを自動的に構成する。この際、経路制御も自動的に行われ、ある物理回線に障害が発生し仮想パスが通信不能になった場合にも、別の物理回線(例えばベストエフォート型回線に障害があった場合には LTE 回線)を利用し、別の仮想パスを用いて通信を迂回する機能を有している。また、各拠点に設置された CPE を統合管理することができ、設定変更などを一斉に行うこともできる。

すなわち、**冗長性を有したオーバーレイネットワークの構築や、ベストエフォート光回線を用いたインターネット経由のオーバーレイネットワーク構築、CPE の統合管理、通信制御等を行いたい場合**には、SD-WAN の導入が有効である。

SD-WAN 製品の選定

上記の構成による機能要件をまとめると、SD-WAN 製品を選定するにあたっての機能要件は次の通りである。

(1)オーバーレイネットワーク上で複数拠点を経由したマルチホップ通信が可能であること
(2)複数物理回線を利用した仮想パス切替えが可能であること
(3)物理回線の通信品質や通信断を定常的に監視していること
(4)CPE の統合管理機能を有していること
(5)アプリケーションブレークアウト機能(後述)を有していること
(6)セキュリティ機能を有していること
(URL フィルタリング、IP ブラックリストによる遮断、DPI 等)

３．３　オーバーレイネットワークの運用

オーバーレイネットワークの到達性や通信性能は、アンダーレイネットワークの安定性や通信性能に影響される。

スター型構成

スター型構成の場合には、通常は固定的な経路制御となる。すなわち、マルチホップでの通信や障害時に複数パスを利用した通信迂回は利用できない。マルチホップ通信による拠点間通信や、複数アンダーレイネットワーク回線を利用した冗長化を利用したい場合には、各機器に適切な経路を設定する必要がある。

また、オーバーレイネットワークの健全性を監視するためには、アンダーレイネットワークの回線障害や通信性能劣化を監視する必要がある。アンダーレイネットワークにて、**仮想パス対向点となる中央拠点までの到達性を監視し、通信断や通信性能の劣化を検知**した場合には、**別の物理回線に仮想パスを切り替える**といった対応が必要となる。これら監視や切替えを自動的に行うためには、スター型構成においても前述の通り SD-WAN を導入する必要がある。

さらに、オーバーレイネットワーク上を流れる通信量を監視する必要がある。オーバーレイネットワークにおいても、通常のネットワークと同様、物理回線の通信量を監視する必要がある。その上で、さらに仮想パスを流れる通信量を監視する必要がある。これにより、オーバーレイネットワーク上でどの拠点間で通信量が多いのか、若しくは仮想パスの通信性能(オーバーレイネットワーク機器のオーバーレイ通信性能)を超えた通信が発生していないか、を監視することができる。すなわち、**物理回線と仮想パスの通信量の両方を監視することで、通信性能の劣化が発生した場合に物理回線が逼迫しているのか、若しくは仮想パスの通信性能が逼迫しているのかを判断**することができる。

仮想パスの通信量を減らすには、**アプリケーションブレークアウト**という手法が有効である。図 6 に示す通り、指定したアプリケーションはアンダーレイネットワークを用いて通信し、拠点間通信に必要なアプリケーションのみをオーバーレイネットワークを用いて通信する手法である。この際注意すべき点は、指定したアプリケーションは拠点からアンダーレイネットワークにて直接インターネット通信が行われるため、オーバーレイネットワーク上にあるセキュリティ機器による検査を受けずに通信が行われることである。そのため、アプリケーションブレークアウトによる通信は、拠点の小型 VPN 機器、若しくは CPE 内部にてセキュリティ検査を行う必要がある。

これらアプリケーションブレークアウトとセキュリティ機能を備えた小型 VPN 機器も存在するが、これら機能を利用するにあたってはこれらの機能を有した SD-WAN 製品を導入する方が安全である。

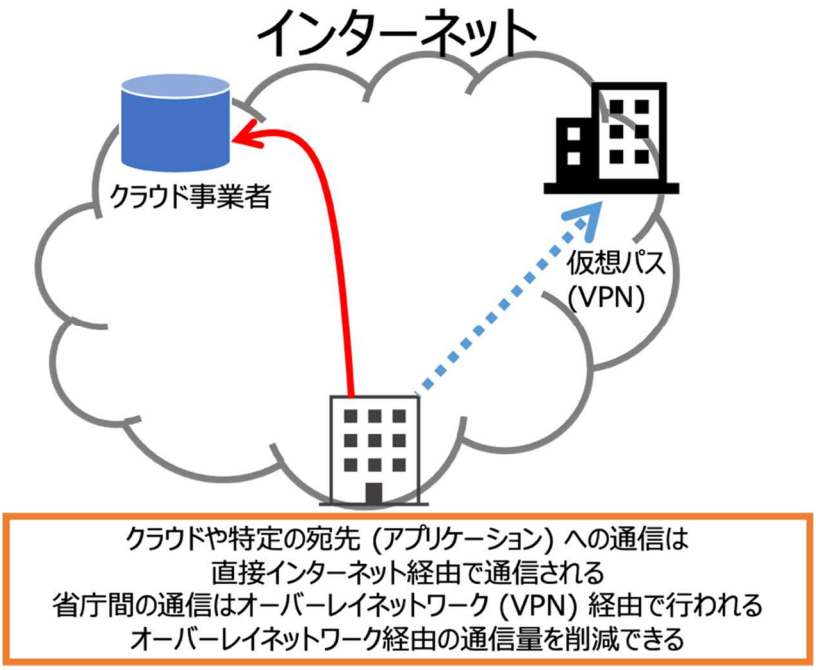

図 6 ： アプリケーションブレークアウト

メッシュ型構成

SD-WAN 製品を利用したメッシュ型オーバーレイネットワーク構成の場合には、メッシュを構成しているそれぞれの仮想パスにおいて、到達性と通信品質の監視が必要となる。ある仮想パスで通信断や通信品質の低下が観測された場合には、その仮想パスが利用している物理回線を外し、別の物理回線を用いて仮想パスを構成し直す必要がある。また、メッシュ型構成の利点を活かすために、マルチホップ通信を行えるよう経路設定、若しくは経路制御が行われていることが望ましい。**ほとんどの SD-WAN 製品では、これらの監視と障害検知、通信迂回などの機能を有している**。したがって、SD-WAN 製品が提供するこれらの機能を、**ダッシュボード等の管理画面から監視できる機能を有した製品を選定すべき**である。また、仮想パスの通信容量逼迫を防ぐためにアプリケーションブレークアウトの機能と、URL フィルタリング、IP アドレスブラックリスト、DPI 等のセキュリティ機能を有した SD-WAN 製品が望ましい。

相互接続性

オーバーレイネットワークの運用にあたって、VXLAN 等の標準化が行われている技術に関しては、複数ベンダーの製品を混在して運用することが可能である。その一方で、SD-WAN と呼ばれる製品はオーバーレイネットワークを構成するにあたってどのような技術を用いているか一般的に公開されておらず、またオーバーレイネットワーク上で経路制御を行うための技術も

製品によって異なっている。そのため、複数ベンダーの製品を混在して使うことはできない。

基幹ネットワークにて VXLAN + EVPN にてオーバーレイネットワークを構成する場合や、小型ルータにて L2TPv3 を用いて小規模なオーバーレイネットワークを構築する場合には、相互接続性が保たれる場合がある。これは、VXLAN + EVPN や L2TPv3 といった技術は、IETF(Internet Engineering Task Force)等の国際標準化会議において仕様が標準化されているため、異なったベンダーの製品間において相互接続可能な場合もある。しかし、相互接続が可能であったとしても、製品毎に仕様の差異があるなど、制御のための手法が異なっている場合が多い。そのため、オーバーレイネットワークを構築、運用するにあたってはベンダーを統一した構成が望ましい。

NAT 技術との併用

NAT 技術は多くの政府省庁ネットワークにて導入されている。一般的には、オーバーレイネットワークを構築する機器にはグローバル IPv4 アドレスが必要となるが、製品によっては、IPv6 を用いてオーバーレイネットワークを構築できるものもある。一部の SD-WAN 製品では、NAT 配下に CPE を設置した場合にも、オーバーレイネットワークが構築可能である。しかし、導入されている NAT 製品の種類にも依存し、必ずオーバーレイネットワークを構成できるわけではない。そのため、拠点間でオーバーレイネットワークを構築する機器若しくは CPE には、グローバル IPv4 アドレスを付与することが望ましい。その場合、セキュリティ上の観点から、オーバーレイネットワークを構成する機器をファイアウォール配下に置く場合が多いと思われる。オーバーレイネットワークを構築するために必要となるプロトコル(例えば VXLAN の場合には UDP ポート番号 4789)が通過できるよう、ファイアウォール機器を適切に設定する必要がある。

４　まとめ

以上の通り、オーバーレイネットワークの導入基準と利点を活かすことのできる適用構成、製品の選定基準についてまとめるとともに運用上の注意についても記述した。

オーバーレイネットワークは、ある程度距離の離れた多数の拠点で専用網を構築する場合には、専用線に代わる有効な手段となる。また、基幹ネットワークにオーバーレイネットワークを導入するにあたっては、VXLAN + EVPN を用いて構成し、かつ VXLAN をハードウェア処理できる機器を導入すべきである。一方で、遠隔拠点にオーバーレイネットワークを導入するにあたってはスター構成若しくはメッシュ構成の選択肢がある。スター構成の場合には小型 VPN 機器を用いてオーバーレイネットワークを構成することも可能であるが、メッシュ構成の場合は SD-WAN 製品が必要となる。冗長性を有したオーバーレイネットワークが必要となる場合には、どちらの構成においても SD-WAN 製品の導入が望ましい。さらに、オーバーレイネットワークの運用においては、物理回線と仮想パス両方の監視が重要となるため、それが実現できる製品を選ぶべきである。

まとめると、SD-WAN 製品を選定する場合の条件は、以下の通りである。(1)～(4)は必須要件、(5)、(6)は付加的要件である。

(1)オーバーレイネットワーク上でマルチホップ通信が可能であること
(2)複数物理回線を利用した仮想パス切り替えが可能であること
(3)物理回線の通信品質や通信断を定常的に監視していること
(4)拠点に設置した機器の統合管理機能を有していること
(5)拠点に設置した機器がアプリケーションブレークアウト機能を有していること
(6)拠点に設置した機器がセキュリティ機能を有していること
(URL フィルタリング、IP ブラックリストによる遮断、DPI 等)

５　参考情報

[1] Mallik Mahalingam, Dinesh Dutt, Kenneth Duda, Puneet Agarwal, Larry Kreeger, T. Sridhar, Mike Bursell, and Chris WrightVirtual, “eXtensible Local Area Network (VXLAN) : A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks”, Internet Engineering Task Force, Request for Comments 7348, Aug. 2014.

[2] John Drake, Wim Henderickx, Ali Sajassi, Rahul Aggarwal, Nabil Bitar, Aldrin Isaac, and Jim Uttaro, “BGP MPLS-Based Ethernet VPN”, Internet Engineering Task Force, Request for Comments 7432, Feb. 2015.

[3] Ali Sajassi, John Drake, Nabil Bitar, Ravi Shekhar, Jim Uttaro,and Wim Henderickx, “A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)”, Internet Engineering Task Force, Request for Comments 8365, Mar. 2018.

[4] Juniper Networks,Inc., “EVPN-VXLAN とは”, https://www.juniper.net/jp/jp/products-services/what-is/evpn-vxlan/, 2021 年 2 月確認.

[5] 大平 伸一, “Cisco Nexus スイッチで VXLAN EVPN ファブリックを作ろう！”, Cisco Japan Blog, https://gblogs.cisco.com/jp/2017/04/create-vxlan-evpn-fabric-with-cisco-nexus-switch/, 2021 年 2 月確認.

[6] Wikipedia, “SD-WAN”, Wikipedia Foundation, Inc., https://en.wikipedia.org/wiki/SD-WAN, 2021 年 2 月確認

[7] Wikipedia, “オーバーレイ・ネットワーク”, Wikipedia Foundation, Inc., https://ja.wikipedia.org/wiki/%E3%82%AA%E3%83%BC%E3%83%90%E3%83%BC%E3%83%AC%E3%82%A4%E3%83%BB%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AF, 2021 年 2 月確認

[8] Mark Townsley, Rahul Aggarwal, and Maria Santos, “Transport of Ethernet Frames over

Layer 2 Tunneling Protocol Version 3 (L2TPv3)", Internet Engineering Task Force, Request for Comments 4719, Nov. 2006.

[9] Pankaj Garg and Yu-Shun Wang, "NVGRE: Network Virtualization Using Generic Routing Encapsulation", Internet Engineering Task Force, Request for Comments 7637, Sep. 2015.

[10] B. Davie, Ed. and J. Gross, "A Stateless Transport Tunneling Protocol for Network Virtualization (STT)", Internet Engineering Task Force, Internet-Draft, draft-davie-stt-08, Apr. 2016.

[11] Jesse Gross, Ilango Ganga, and T. Sridhar, "Geneve: Generic Network Virtualization Encapsulation", Internet Engineering Task Force, Request for Comments 8926, Nov. 2020.