応募区分：提言型論文

# NGN を利用した高速インターネット VPN の提案

海保　人士(かいほ　ひとし)
株式会社エヌ・ティ・ティピー・シーコミュニケーションズ

## ■ 要約

インターネットの普及に伴い、企業の拠点間でファイル共有などの情報共有のために、インターネット VPN を利用して拠点間を接続することが行われている。弊社においても導入の容易さと低い運用コストを特徴とした、ダイナミック VPN サービスをユーザーに提供しており好評を得ている。しかし、インターネットの輻輳を原因とする、通信品質の低下と遅延の大きさの改善を求める声がユーザーから多く届くようになった。そこで、低遅延、高速な通信を特徴とする NGN を利用した高速なインターネット VPN を構築しユーザーに提供することを計画したが、技術的な課題が存在し既存のソリューションだけでは提供することが困難であった。本論文では、インターネット VPN と NGN を利用した VPN の課題を整理したうえで、技術的課題の解決法を示し、ダイナミック VPN の特徴を引き継いだ、新しい高速インターネット VPN を提案する。

# 目次

# 1. 背景

## 1.1. インターネット VPN へのニーズ

### 1.1.1. 従来型インターネット VPN

Windows95 が発売されインターネットが普及し始めた 1990 年代後半から、インターネットに接続したルーター間で PPTP や IPsec といったプロトコルを用いて VPN を構成する、インターネット VPN が企業の拠点間を接続する用途で多く用いられるようになった。2000 年代半ばからは IP-VPN や広域イーサネットの低価格化にあわせて、VPN の主力はそれらになりつつあるといわれている。しかし、現在においても約半数の企業ではインターネット VPN が利用されており、より小規模の企業ではインターネット VPN の利用の割合が高くなる。[1]

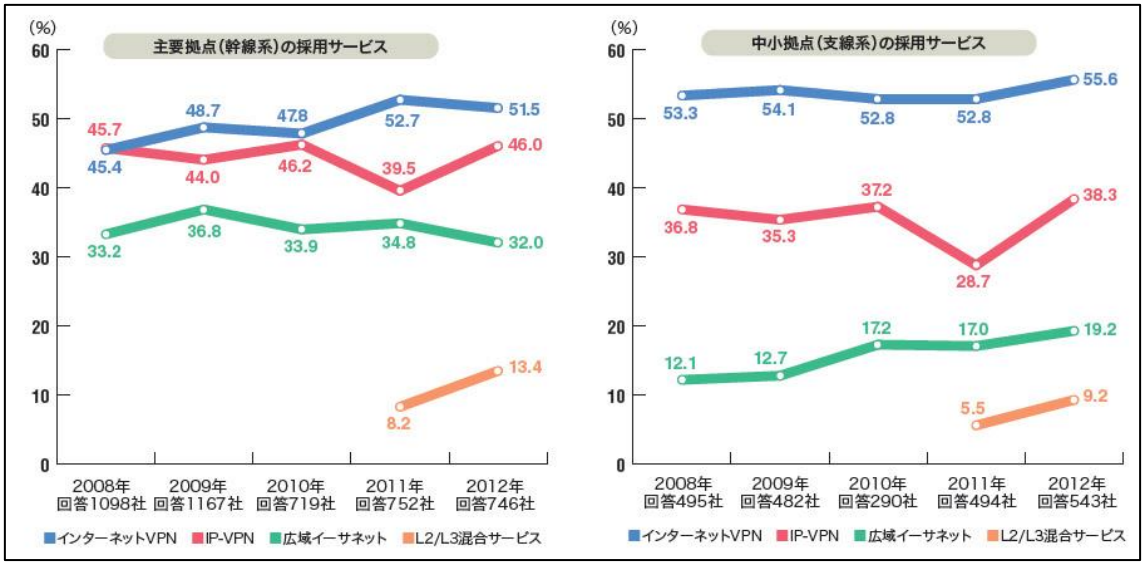


図 1 VPN の方式別シェア

(http://itpro.nikkeibp.co.jp/article/COLUMN/20121106/435342/?ST=network&P=1 より)

インターネット VPN は、インターネットに接続する環境があれば構築が容易なこと、専用線などの高価な回線が不必要なことから、これからもインターネット VPN は多く利用されていくと考えられる。

しかし、インターネット VPN を導入する上で障害となるのが、インターネット VPN を構成するルーターの設定である。従来のインターネット VPN では、各ルーターの IP アドレスはすべて固定されていることが前提であり、その上で VPN を構成するすべてのルーターにおいて VPN を接続するすべての対地について、IP アドレスや、IPsec パラメーターなどを設定する必要があった。仮に 4 拠点のインターネット VPN を構築する場合には、1 つのルーターにおいて対向の 3 拠点分の設定を行う必要がある。

さらに、新たに拠点を追加する場合には、新たに設置するルーターに対向拠点分の設定が必要になる

だけでなく、対向拠点のすべてのルーターにも追加拠点向けの IPsec の設定やルーティングの設定を追加する必要がある。つまり 1 拠点の追加を行うにはすべての拠点のルーターの設定が必要となってしまう。たとえば 3 拠点の VPN に 1 拠点を追加するために、追加拠点に他の 3 拠点用の設定を行い、既存の 3 拠点のルーターに追加拠点用の設定の変更が必要となる。

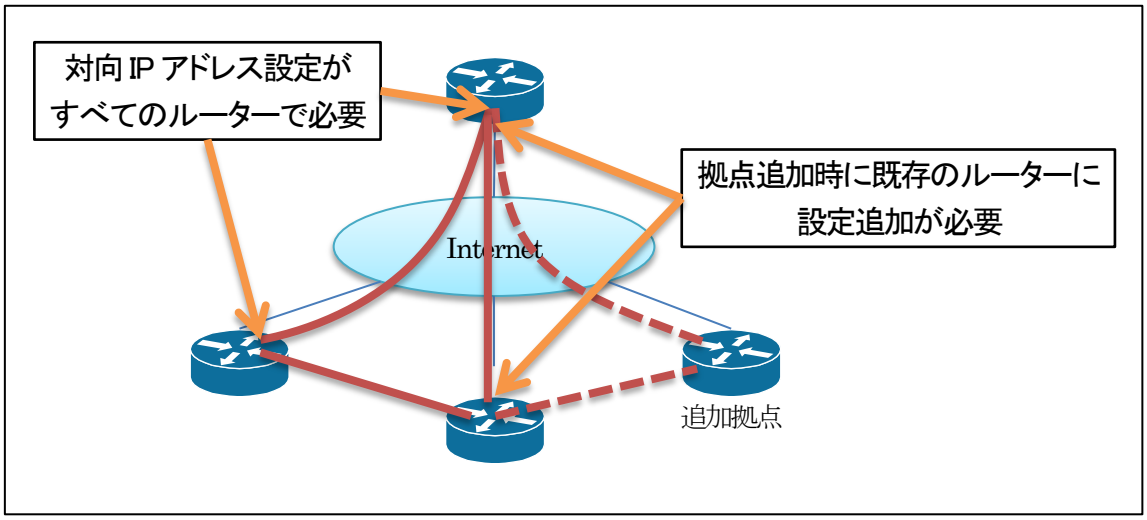


**図 2 従来のインターネット VPN**

このような従来のインターネット VPN では、初期導入時に複雑な設定が必要であるのに加え、拠点追加、構成変更といった、構築後の運用フェーズにおいても多数の設定変更が必要となり、構築、運用をアウトソースし、ルーターの設定に作業員を派遣した場合には多額の追加コストが発生してしまう。

### 1.1.2. ダイナミック VPN

弊社では従来のインターネット VPN とは一線を画した、導入の容易さ、導入後の低い運用コストを特徴とした、ダイナミック VPN を提供している。[2]

ダイナミック VPN は VPN を構成するルーターとして、Cisco の ISR シリーズルーターを採用しており、ISR シリーズルーターに搭載された DMVPN（DynamicMultipointVPN）を利用している。DMVPN は、IPsec に加え mGRE(multipoint Generic Routing Encapsulation)、NHRP(Next Hop Resolution Protocol)、EIGRP や BGP といったダイナミックルーティングプロトコルを組み合わせて使用し、ハブルーターとスポークルーター間の自動トンネル作成、スポークルーターとスポークルーター間の動的なトンネル作成、ルーティング情報の流通を実現している。[3]

DMVPN の特徴である、IPsec 設定の大幅な簡略化、動的 IP アドレスでの VPN 構築(ハブルーターのみ固定 IP アドレスが必要)、ルーティング情報の設定が不要、事前に設定が必要無いフルメッシュ VPN 構築により、ダイナミック VPN の利点である容易な導入と低い運用コストを実現している。

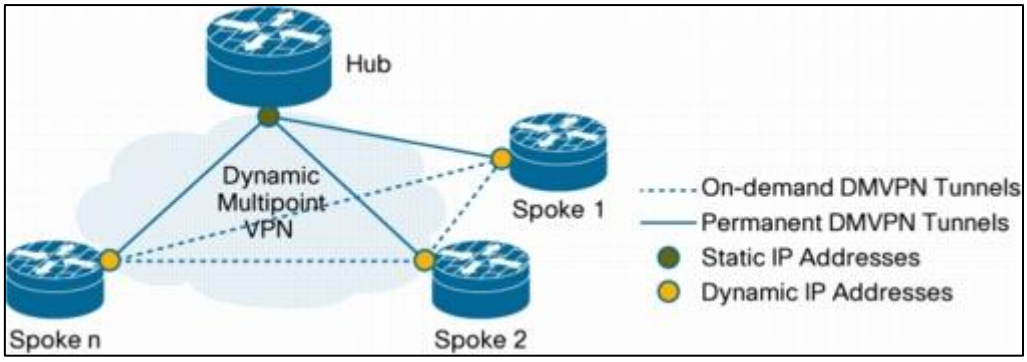


図 3 DMVPN（DynamicMultipointVPN）
(http://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html より)

また、ユーザーの初期導入工事を簡易にするため、弊社独自のアクティブスタートアップを用いた、ルーターの自動設定を採用している。アクティブスタートアップは、ISR ルーターで動作する EEM スクリプトと標準的な Linux サーバが連携して動作することで、ゼロタッチコンフィグを実現している。

エンドユーザーに出荷された全ての ISR ルーターに 、初期 Config と EEM スクリプトが格納されており、初期起動時に EEM スクリプトにより ISR ルーターが自動的にサーバに接続し、機器のシリアル番号によって識別される個々のルーターの設定をダウンロードし、自動的にルーターが設定される。設定完了後、VPN が確立されたことが確認されれば、弊社エンジニアまたはエンドユーザーに対して E メールによる通知が送られ、設定が完了したことがリアルタイムにわかるようになっている。[4]

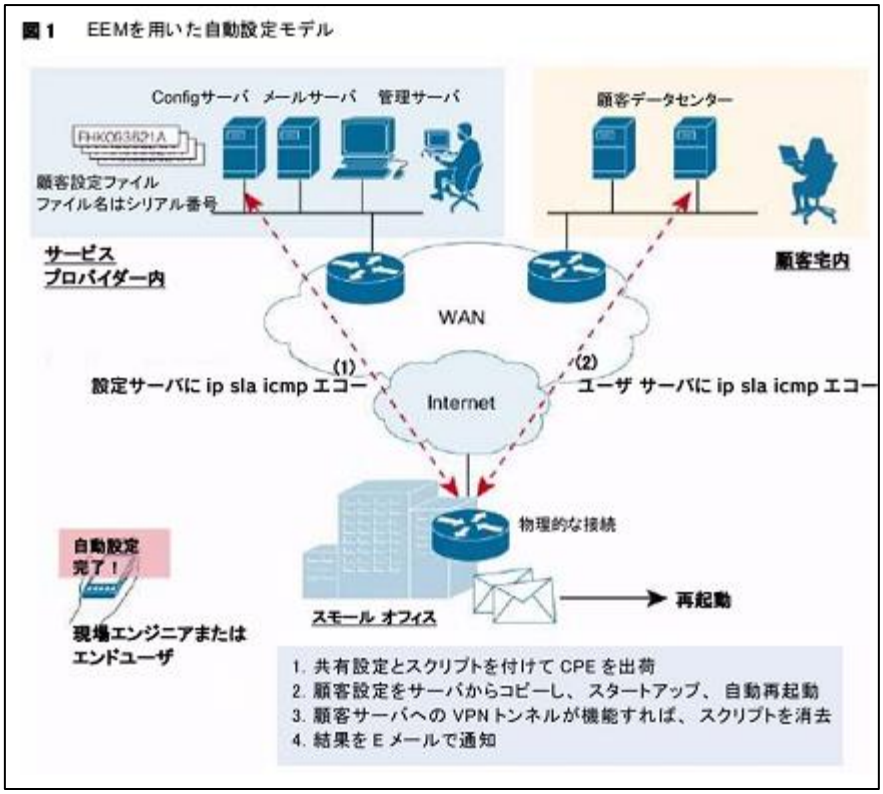


図 4 アクティブスタートアップ(自動設定)の動作
(http://www.cisco.com/web/JP/solution/netsol/routing/literature/nttpc_casestudy.pdf より)

アクティブスタートアップを利用することで、ルーターの設置作業は、ルーターを箱から取り出し、電源を接続してルーターをフレッツ回線のONUやADSLモデムといった回線終端装置に接続するだけで完了し、ルーターの設置時に技術者が設定を投入する必要が全くない。技術者を擁しないエンドユーザーによるルーター設置が可能となるため、技術者を派遣する必要が無く、初期導入時の大きなコスト要因である技術者の派遣費用を削減することが可能となった。また、弊社においても初期設置作業とトラブルシューティングの稼働およびコストが大幅に削減され、ユーザーへの提供価格の低減が可能となった。

設置後の運用においても、DMVPN を利用していることで設定が簡易になり、拠点の追加時に新規拠点のルーターのみ設定すればよく、他の拠点については設定を変更する必要が無くなった。また、既存拠点の移設などでルーターの IP アドレスが変更になる場合にも、IP アドレスが変更になる拠点のルーターの設定のみ変更すればよく、他の拠点のルーターの設定を変更する必要が無くなったため、ルーターの設定変更における作業量が大幅に減り、ユーザーが負担する運用コストの大幅な低減を実現することができた。

2006 年にダイナミック VPN サービスを開始してからすでに 7 年以上が経過しているが、ユーザーの好評を得ており、導入拠点数は増加し続けている。

## 1.2. インターネット VPN の課題

### 1.2.1. フレッツ網を利用した IPv4 インターネット

現在、日本において FTTH(光回線)は約 2500 万回線強の契約が存在するが、そのうち、約 71%、1800 万回線と大きなシェアを占めているのが NTT 東日本・西日本のフレッツ・サービスの回線である。(http://www.ictr.co.jp/report/20140704000064.html より)フレッツ・サービスでは、FTTH(光回線)のサービスを 2001 年より B フレッツとしてサービスを開始し、2008 年には NGN(次世代ネットワーク)を基盤に活用した光ネクストとしてサービスを拡充している。

フレッツ・サービスにおける IPv4 インターネット接続サービスでは、エンドユーザーが PPP(PPPoE)を利用して ISP を選択することができるサービスである。

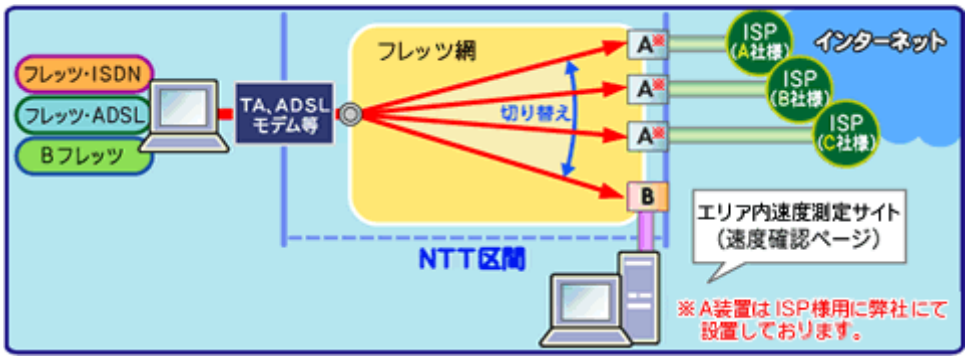


図 5 フレッツ・サービスの概要

(https://flets.com/customer/tec/square/speed/speed1.html より)

フレッツ・サービスを提供しているフレッツ網の構成はエンドユーザーからは直接見えないが、実際のフレッツ網では、エンドユーザーからの IP パケットはブロードバンドルーター等で PPP でカプセリングされた後、ユーザー宅に設置された回線終端装置(ONU)から光ファイバで、最寄りの電話局(光収容ビル)まで伝送される。その後、光収容ビルに設置された BRAS(BroadbandRemoteAccessServer)によって、PPP の認証情報に基づいて各 ISP の網終端装置(NTE)へ向けて、光収容ビルと POI(ISP との接続点)ビルとを結んでいる地域 IP 網を通して転送され、最後に網終端装置で PPP のカプセリングを解かれ、各 ISP に転送される。

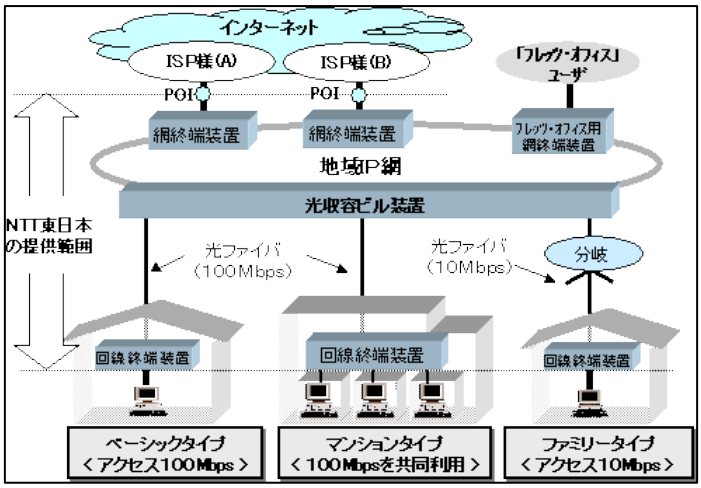


図 6 フレッツ・サービスの網構成

(https://www.ntt-east.co.jp/release/0106/010628b.html　より)

地域 IP 網は県単位に存在し、当初は ISP が県単位で NTT 東日本・西日本と契約して、ISP が各県を結ぶネットワークを構築し、そのネットワークを利用してインターネットに接続する形態であった。その後、地域 IP 網構成の変更や、NGN へのマイグレーションが行われているが、IPv4 インターネット接続サービスについては、当初と同様のサービスが提供されている。

1.2.2. エンドツーエンドの遅延

一般的な ISP は、フレッツ網との POI(接続点)で受け取った IP パケットを自社ネットワークを通してインターネットに転送しているが、日本においてはインターネットの相互接続点の多くが東京に存在するため、ISP のネットワークもその経済性から東京に一極集中する構成となっていることが多い。(一部は大阪に存在するが、トラフィックの多くが東京に集中する。)

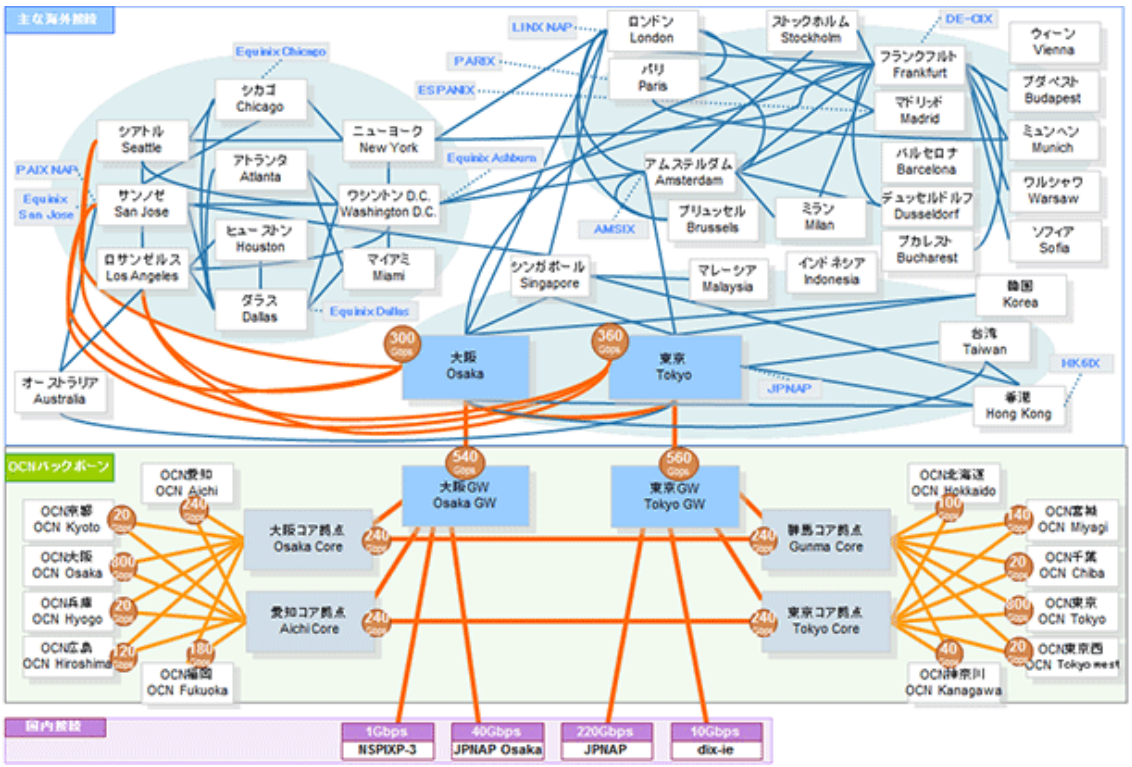


図 7 一般的な ISP(OCN)のネットワーク構成
(http://www.ocn.ne.jp/business/bocn/backbone/　より)

東京一極集中のネットワーク構成のため、東京から遠い県の拠点同士で通信する場合、パケットは通信元から一度東京まで転送され、また東京から通信先まで転送されるという経路を通ることになる。また、同一県内での通信でも ISP が異なる拠点同士が通信する場合、ISP と ISP の相互接続点が東京であることが多いため、通信元の ISP 網で東京まで行って東京から通信先の ISP で折り返ってくることとなる。どちらの場合も直線距離とは比例しない大きな遅延が発生してしまう。
インターネット VPN もインターネット接続自体の遅延の影響を直接受けるため、同一県や隣接県の拠点を接続するにもかかわらず、VPN で接続することには問題ないが、通信遅延が大きく、ファイル共有などの遅延に影響を受けやすいアプリケーションの使用感が非常に悪くなってしまう可能性がある。

### 1.2.3. 輻輳による通信品質低下

フレッツ網において、ISP と契約したユーザーの通信はユーザーの住んでいる県(もしくは地域)の網終端装置に集約される。1 台の網終端装置に集約されているユーザー数などの情報は公開されていないが、ユーザーへの提供価格から推定すると集約度はかなり高いと考えられる(1 回線あたりの割り当て帯域は数百 kbps 程度とされている)。そのため、少数のユーザーでも短時間に大量の通信を行うと、網終端装置において輻輳が発生し、同一の網終端装置に接続されている他のユーザーの通信でパケットロスが大量に発生したり、通信遅延が非常に大きくなるなどの大きな影響を及ぼしてしまう。

実際に過去、Winny や Share といった P2P ファイルシェアリングソフトが少数のユーザーで利用されただけで、網終端装置において輻輳が発生し、多数のユーザーのインターネットとの接続品質が悪くなったり大きな遅延が発生するといったことが頻繁に発生し、多数の ISP がその対応に追われることとなった。[5]
フレッツ網を利用したインターネット VPN は、網終端装置での輻輳の影響を直接受け、一般ユーザーのトラフィックが多くなる夜間になると VPN の通信品質が低くなり、夜間のバッチ作業によるトラフィックの転送がうまくできなくなるといったことが多く発生した。

# 2. NGN を用いた高速インターネット VPN の提案

## 2.1. NGN について

### 2.1.1. NGN とは

NGN とは従来の回線交換型の電話網と、インターネットを代表とするデータ通信網を統合し、フル IP ネットワークによって電話、データ通信、放送を電話並の品質、セキュリティでユーザーに提供することを目的として構築されるネットワークの総称である。[6]
日本においては、NTT 東日本・西日本がフレッツ・光ネクストのサービス基盤として、IPv6 を用いた IP ネットワークを構築し、インターネット接続サービス、電話サービス、テレビサービス等の様々なサービスを提供している。[7]
フレッツ・光ネクストのインターネット接続サービスは、従来の PPPoE による IPv4 インターネット接続に加え、PPPoE による IPv6 インターネット接続、IPoE による IPv6 インターネット接続が提供されており、ユーザーの選択により組み合わせて利用することが可能である。

### 2.1.2. NGN の網構成

NGN の IPv6 インターネット接続は、NGN に接続した VNE( VirtualNetworkEnabler)を通して提供される。ユーザーが VNE を選択し NTT 東日本・西日本に申し込むと、VNE 毎に異なる IPv6 アドレスが割り当てられ、NGN 網内でユーザーが選択した VNE にルーティングされる。ユーザーと VNE 間の通信は NGN 網内でルーティングされるが、PPPoE を利用したインターネット接続とは異なり、間に網終端装置に相当する機器が存在しない。

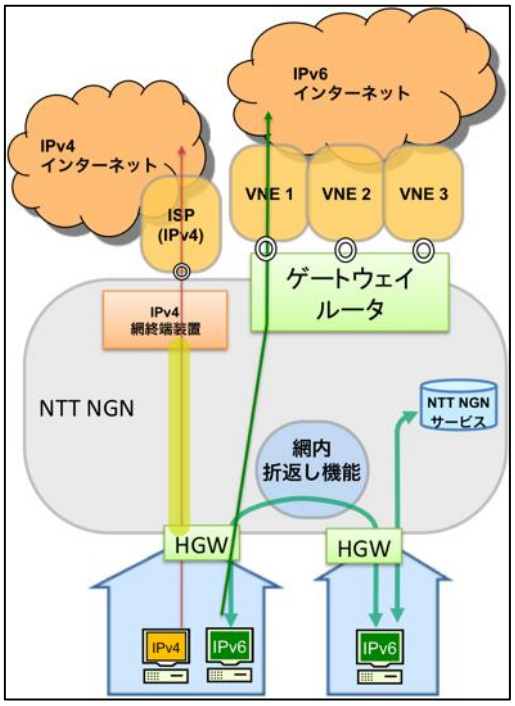


図 8 NGN 網の構成
(http://www.geekpage.jp/blog/?id=2013/1/11/1 より)

また、ユーザー～ユーザー間の通信については、網内折り返し機能により、NGN 網内を最短でルーティングされ、PPPoE を利用したインターネット接続のように、異なる VNE を選択したユーザー間でも、パケットがいったん東京まで行って折り返してくるといったことが発生しない。

### 2.1.3. NGN の特徴

NGN は各種の認証サーバやトラフィック制御システム、キャリアグレードの通信機器等のシステムを実装することで、その特徴である品質確保、セキュリティ、信頼性、オープンなインターフェースを実現している。[8]

インターネット接続では、広大な IPv6 ネットワーク、網終端装置の無いネットワーク構成、NGN 網内は直接通信といったネットワーク構成による、高速で低遅延な通信が可能になったことが大きな特徴である。

しかし、広大な IPv6 ネットワークを採用し、ユーザー毎に異なる VNE へとルーティングしなければいけないため、NGN 網内のルーティングは非常に大きな負荷となっている。また、ユーザーに割り当てられる IPv6 アドレスは NGN 網から払い出されるが、NGN 網の都合により変更されることがあるため、PPPoE を利用した IPv4 のサービスのように ISP が IP アドレスを固定してユーザーに割り当てることができない。

## 2.2. NGN を用いた高速インターネット VPN

### 2.2.1. 新たな VPN を開発するに至った背景

ダイナミック VPN をユーザーに提供開始し、FTTH(B フレッツ)が普及し始めた頃から、VPN で接続した拠点間における通信の遅延と通信品質の悪化を改善することがユーザーから求められるようになった。当時はトラフィックが急激に増加している時期であったため、NTT 東日本、NTT 西日本と弊社のネットワークの接続点である網終端装置において、大量の通信による輻輳がたびたび発生することでパケットの損失率と遅延が大きくなり、ユーザーの使用感が大きく損なわれることがあった。
そのような状況のなか、NGN の提供が開始され、NGN の特徴である低遅延、輻輳の発生しやすい網終端装置を通過しない IPv6 ネットワークを利用して VPN を構築することができれば、課題を改善できるのではないかと考えられた。しかし、その時点では NGN の環境が整わないことと、DMVPN が IPv6 に対応していなかったことから、ユーザーへの提供はできなかった。
その後、NGN の普及とサービスの拡充がされるとともに、DMVPN が IPv6 に対応することで環境が整い、ダイナミック VPN の利点である、低コストと構築の容易さを引き継ぎつつ、低遅延かつ通信品質の高い新しい VPN を提供することができるようになった。

### 2.2.2. 新たな VPN への要求

NGN を用いた高速インターネット VPN をユーザーに提供するにあたり、既存ユーザーのマイグレーションへの適用、他社サービスとの差別化の面から、機能面ではダイナミック VPN と同様以上のサービスとすることが必須であった。そのため、VPN の構築には CiscoISR ルーターと DMVPN を引き続き採用することとし、DMVPN とアクティブスタートアップによるダイナミック VPN の容易な初期導入、運用コストの低減という利点を引き継いで提供することとした。
VPN を接続する際、NGN は IPoE を利用した IPv6 通信のみ、その特徴である低遅延、網終端装置を通過しない通信を行うことができるため、ルーター間は IPv6 を利用して VPN を接続する必要がある。また、ユーザートラフィックは現時点では IPv4 のパケットがほとんどを占めているため、VPN の内部は IPv4 が利用できることが必要であった。
DMVPN の IPv6 対応は IOS のバージョンアップにより機能が拡充され、12.4(20)T における IPv6 サポート開始から始まり、15.2(1)T において IPv6 トランスポートが実装された。[9]それにより、弊社が必要と考えた機能を実現可能な NGN を利用したインターネット VPN をサービスとして提供できるようになった。

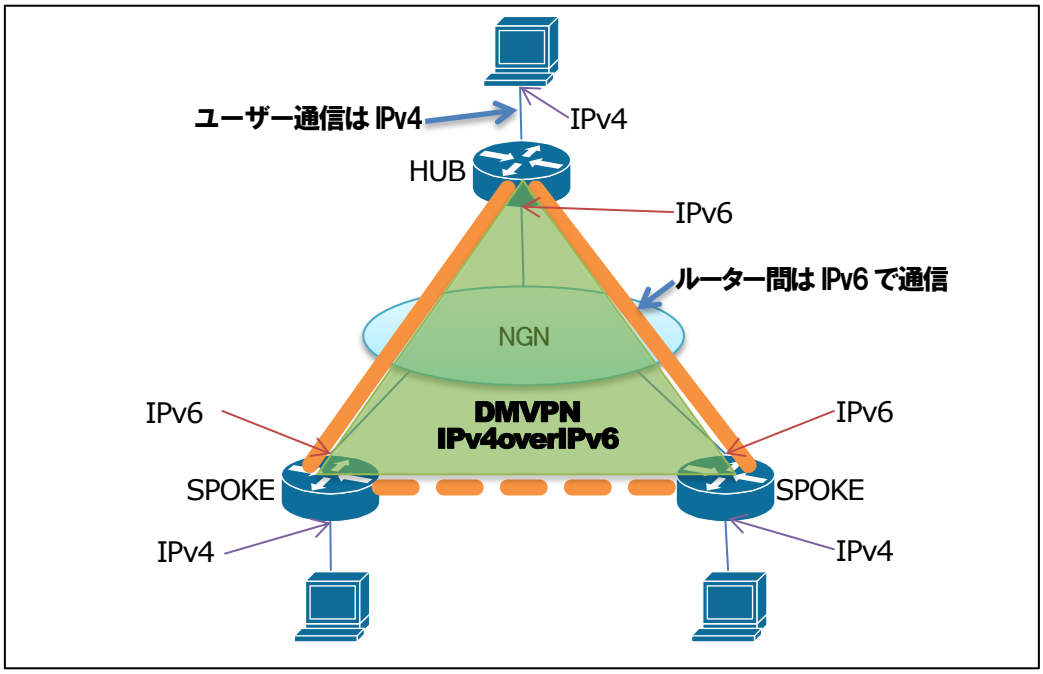


図 9 NGN を用いた IPv6 インターネットの構成

2.2.3. 技術的な課題

DMVPN を使用して VPN を構築する際には、SPOKE 拠点の IP アドレスは不定でも良いが HUB 拠点の IP アドレスは固定されている必要がある。しかし、NGN ではユーザーに割り当てられる IPv6 アドレスが固定されておらず、NGN の都合により変更されることがある(半固定)。IPv4(PPPoE)によるインターネット接続のダイナミック IPv4 アドレスアサインのように、接続毎に IPv6 アドレスが変更されることはないが、ユーザーが使用中でも網側のリクエストによって IPv6 アドレスが変更になる可能性があり、そのタイミングは不定で事前に通知されることもない。

さらに、ユーザーに割り当てられる IPv6 アドレスは事前に通知されることがなく、割り当てられる IPv6 アドレスを知るためには、実際に PC やルーターを ONU に接続し、NGN から実際に RA で割り当てられた IPv6 アドレスを見る必要がある。そのため、VPN を構築するルーターに事前に HUB ルーターの IPv6 アドレスや SPOKE ルーターの IPv6 アドレスを設定することができない。

また、DDNS(ダイナミック DNS)サーバのようなネットワーク上に設置したサーバにルーターから割り当てられた IPv6 アドレスを通知し、それを管理してルーターからの問い合わせに答えるようなサーバを設置してシステムを構築することも考えられたが、サーバの管理コストやサーバの故障時にすべての VPN が利用できなくなる危険性から、ルーターのみで課題を解決することが求められた。

2.2.4. 技術的な課題に対する解決策

前項の問題の中で最も解決が難しい問題は、IP(IPv6)アドレスが固定されないことである。DMVPN では HUB ルーターの IPv6 アドレスは固定されている、もしくは FQDN で解決できることが必要となる。

NGN を利用する限り、NGN の仕様であるアドレスの半固定を回避する方法が無い。また、FQDN で解決できるためには、IPv6 が固定されていて事前に DNS サーバに設定を行うか、IPv6 に対応したダイナミック DNS サービスを利用する必要がある。しかし、今回は外部サーバを利用した構成を採用しないこととしたため FQDN による解決ができない。
そこで、IPv6 インターネットだけではなく IPv4 インターネットを併用することとし、IPv6 インターネットでは DMVPN を動作させながら、EEM(tcl)スクリプトによって、IPv4 インターネット経由で HUB ルーターと SPOKE ルーター間で IPv6 アドレスを交換して Config に動的に HUB ルーターの IPv6 アドレスを設定することで、IPv6 アドレスが固定されない環境でも DMVPN が利用できるようにした。

実際の動作は以下のような動作とした。

**(1)初回接続時の動作**

① IPv4 インターネットへの接続

HUB ルーター、SPOKE ルーター共に DialerInterface(PPPoE)で IPv4 インターネットに接続。その際、IPv4 アドレスが固定のサービスを利用する。

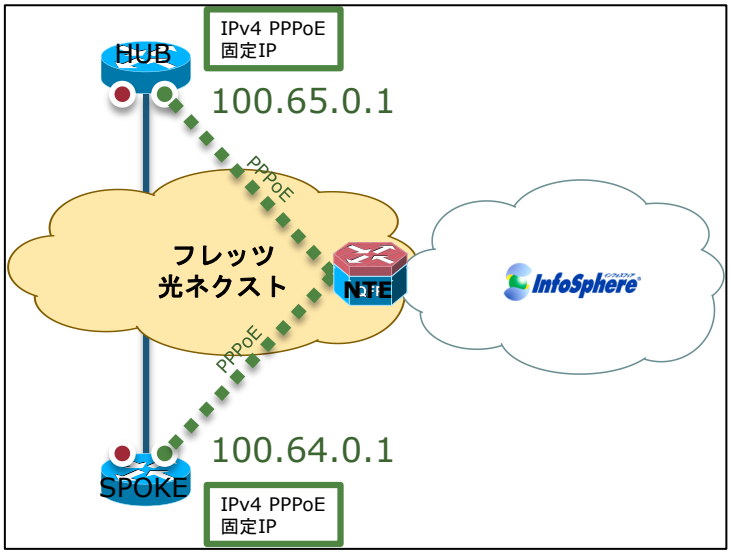


**図 10 動作①IPv4 インターネットへの接続**

② IPv6 アドレスの取得と、HUB ルーターでの IPv6 アドレスの公開

HUB ルーター、SPOKE ルーターともに IPoE の IPv6 インターネットに接続し、NGN 網より RA で IPv6 プレフィックスを取得し、インターフェースアドレスと組みあわせ IPv6 アドレスを設定する。HUB ルーターは EEM(tcl スクリプト)でインターフェースに設定された IPv6 アドレスを取得し、IPv4 インターネットを経由して SPOKE ルーターが HUB ルーターの IPv6 アドレスを取得できるよう公開する。

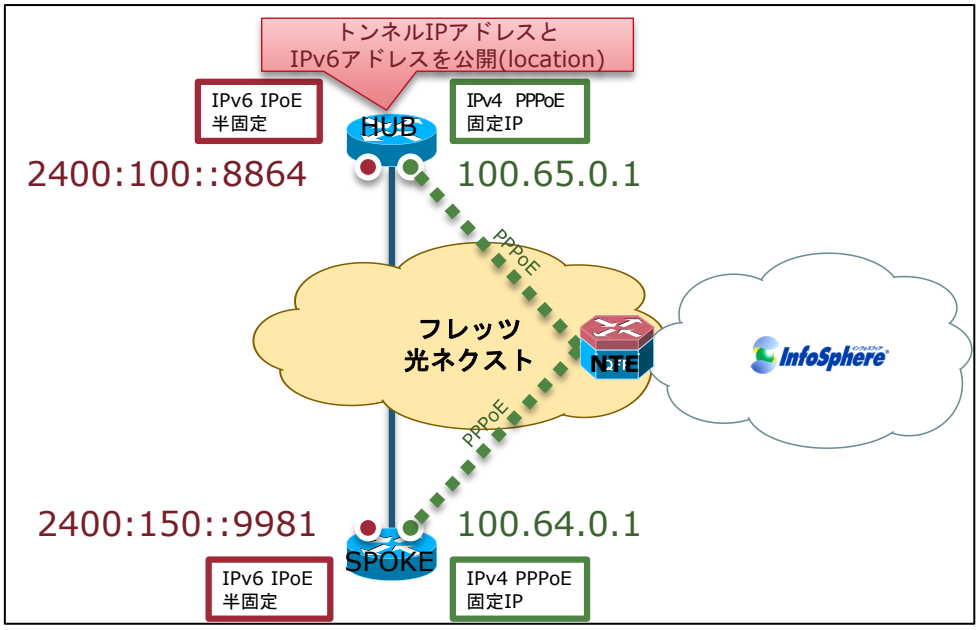


図 11 動作②IPv6 アドレスの取得と、HUB ルーターでの IPv6 アドレスの公開

③ SPOKE ルーターが HUB ルーターの IPv6 アドレスを取得

SPOKE ルーターは EEM(tcl スクリプト)を実行し、HUB の IPv4 アドレスに対し IPv4 インターネット経由でアクセスして HUB ルーターの IPv6 アドレスを取得する。取得した IPv6 アドレスは環境変数に格納する。

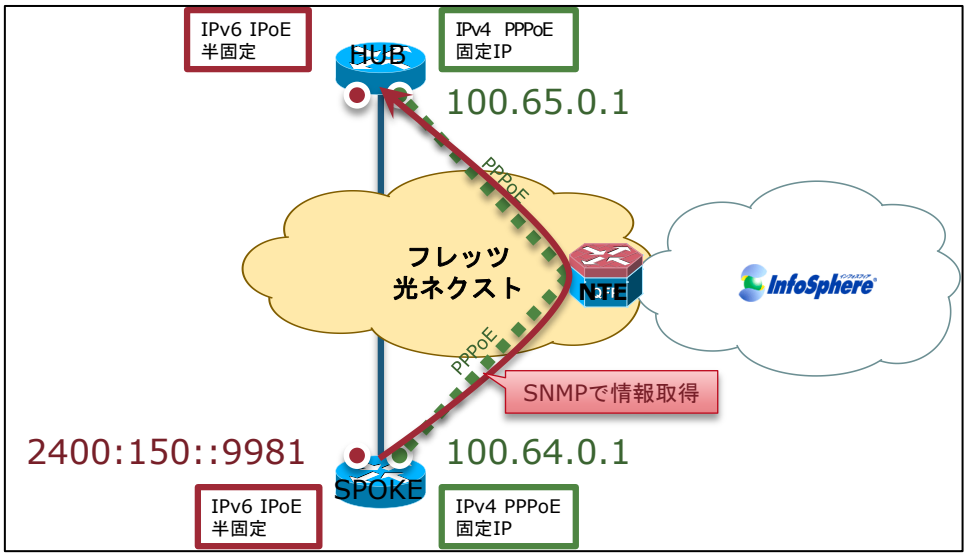


図 12 動作③SPOKE ルーターが HUB ルーターの IPv6 アドレスを取得

④ VPN の接続

SPOKE ルーターは環境変数に格納された HUB ルーターの IPv6 アドレスを、Config における

DMVPN の HUB ルーターの NBMA アドレスとして設定する。その後、DMVPN の動作により自動的に VPN が接続される。

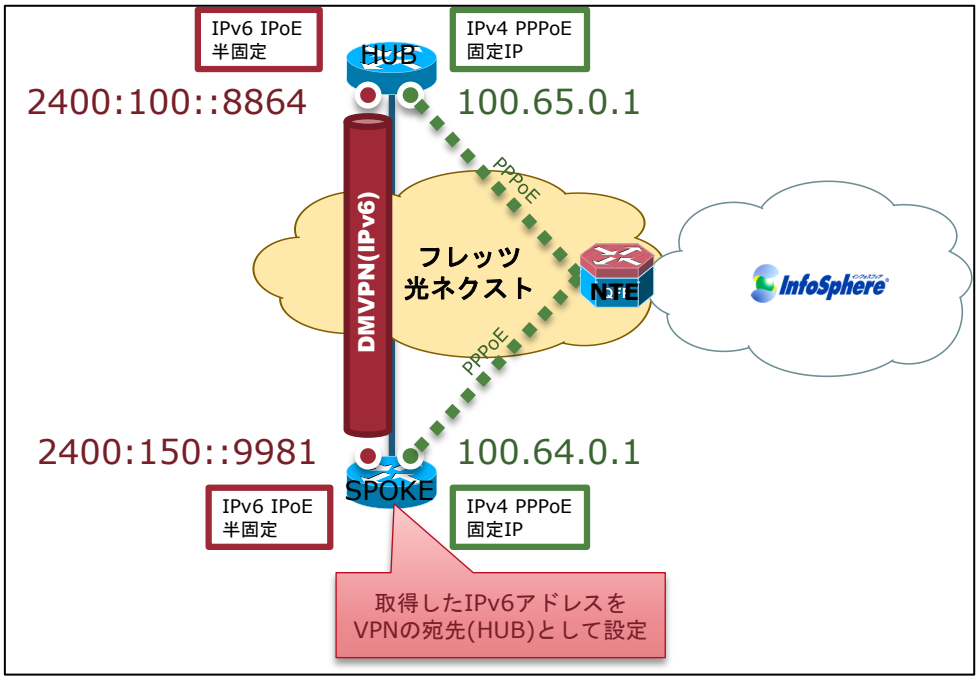


図 13 動作④VPN の接続

以上の動作は 1 分に 1 回の間隔で実行され、電源投入時に ONU に接続されていなかったり、何らかの原因で NGN に接続できない場合も、NGN に接続された時点で自動的に VPN が接続されるようにしている。

**⑵IPv6 アドレスが変更になった際の再接続動作**

IPv6 アドレスが変更になった場合にも、VPN を自動的に再接続するため、以下のような動作とした。

① VPN の接続確認

VPN が接続できているかどうか、SPOKE ルーターから Tunnel 内を通過して HUB ルーターの Tunnel アドレスまでの IP SLA によって確認を行う。確認の間隔は 1 分に 1 回とした。これは、IPv6 アドレスが変更された際に、1 分程度で VPN が再接続することを意図している。

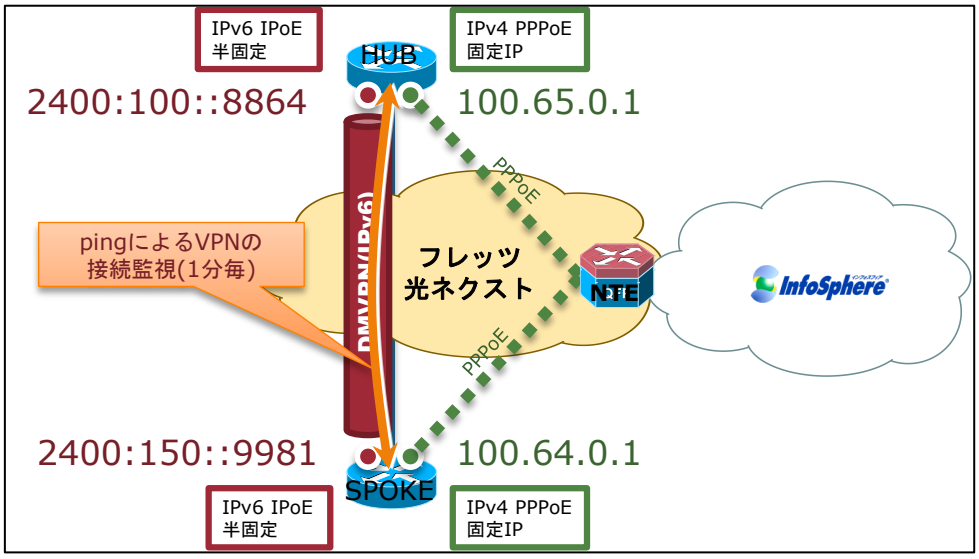


図 14 動作①VPN の接続確認

② HUB ルーターの IPv6 アドレス変更の検知

IPv6 アドレスの変更により、VPN が切断されると、IP SLA が Down し HUB ルーターの IPv6 アドレスが変更されたと判断する。

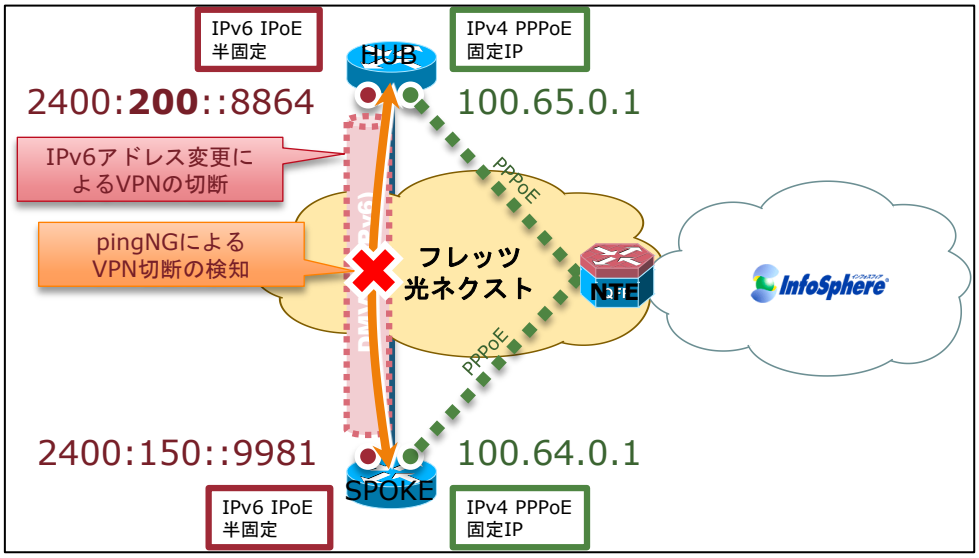


図 15 動作②HUB ルーターの IPv6 アドレス変更の検知

③ HUB ルーターの IPv6 アドレスを問い合わせ

SPOKE ルーターは HUB ルーターの IPv6 アドレスが変更されたと判断すると、HUB ルーターの IPv4 アドレスにアクセスし、HUB ルーターの IPv6 アドレスを取得する。

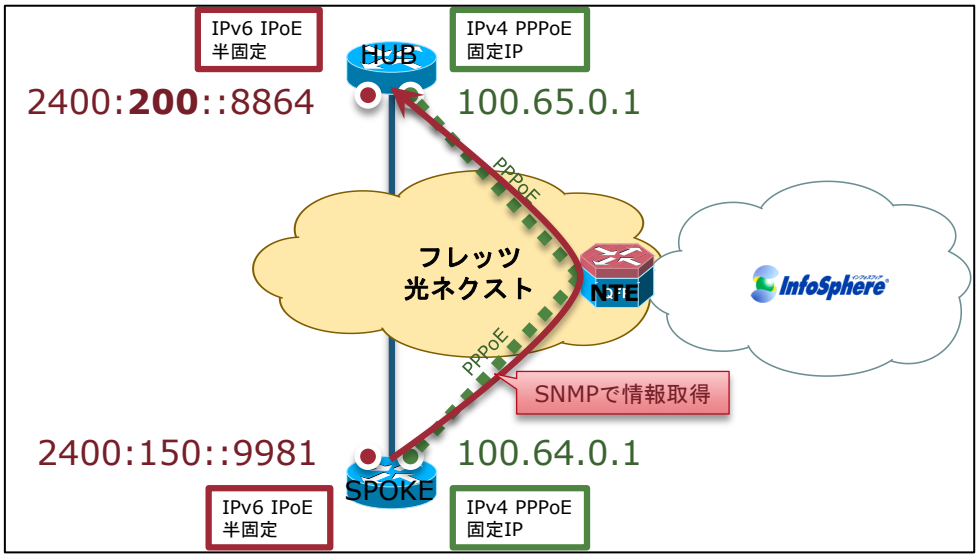


図 16 動作③HUB ルーターの IPv6 アドレスを問い合わせ

④ VPN の再接続

SPOKE ルーターは取得した新しい HUB ルーターの IPv6 アドレスを、HUB ルーターの新しい NBMA アドレスとして再設定する。その後、MDVPN の動作により自動的に VPN が再接続される。

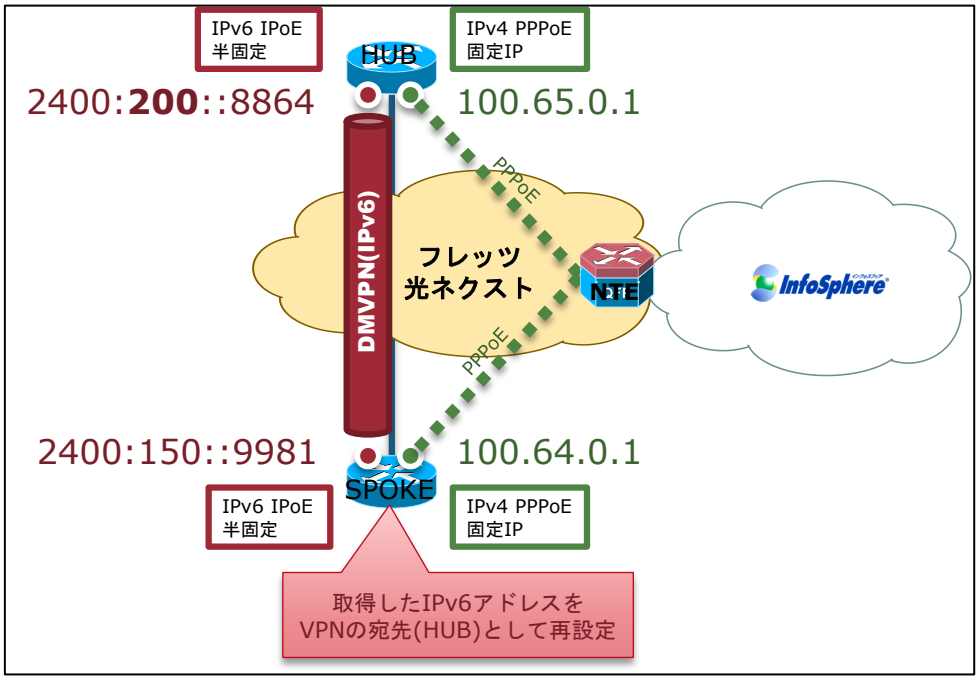


図 17 動作④VPN の再接続

初回起動時の VPN 接続動作、HUB ルーターの IPv6 アドレスが変更された際の再接続動作を実装することで、新しい NGN を用いたインターネット VPN へ求められる機能を満たすことができ、ユーザーに提供可能なネットワークを構築することができた。

#### 2.2.5. 動作の確認とその効果

弊社環境にて前項の解決策を実装した VPN を実際に構築し、想定通りに動作をすることを確認した。ISR シリーズルーターにおいて EEM スクリプトは想定通り動作しており、試験期間の約一ヶ月間に渡ってエラー無く動作することが確認できた。弊社ではユーザーへのサービス展開に耐える信頼性を有していると考え、サービス提供に向けて準備を行っている。

Cisco ISR シリーズルーターと DMVPN、EEM スクリプトを使用することで、NGN の利点とダイナミック VPN の利点の双方を取り入れた VPN サービスを実現し、これまでのインターネット VPN の課題であった遅延と通信品質の悪化を解決しつつ、これまでとほぼ変わらないコストでユーザーに VPN サービスを提供することが可能となった。

## 3. 今後の展開

### 3.1. さらなる自動化の推進

本論文で提案している VPN はダイナミック VPN と同様にアクティブスタートアップによる、ゼロタッチコンフィグを実現しているが、VPN 構築の迅速化とコスト削減を目的に、さらなる自動化を進め、最終的にはユーザーの発注から開通まで完全自動化(ゼロタッチ・デプロイ)することを目指している。

現在、ユーザーの発注から開通まではすべて電子ファイルやオーダーシステムによって管理されているが、複数の社内システムへの投入や、ルーターベンダーへの発注、設定情報の作成は手作業で行っている部分が多い。しかし、これまでの業務改善により申込書から設定情報の作成まで、各パラメーター間の関係や、情報の流れが最適化され、見える化が図られているため、システム化が可能な状態にある。

今後、クラウド上に構築したオーダー管理システムと既存システムを組み合わせて、ユーザーが申込み画面から VPN の作成や拠点追加、設定変更を申し込むと、自動的に必要な社内処理が実行されてユーザーの手元にルーターが配送されるような環境を構築したい。併せて、ルーターの設定はオーダー管理システムからアクティブスタートアップや onePK を利用して実施するようなシステムを実装することで、ユーザーの申し込みから開通までが完全に自動的に行われる、ゼロタッチ・デプロイを実現したいと考えている。

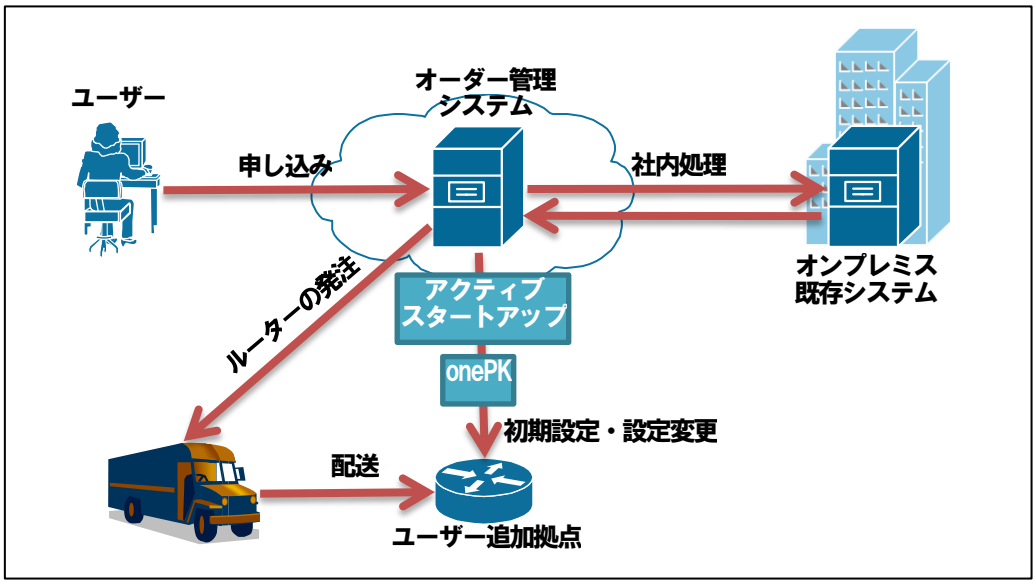


図 18 ゼロタッチ・デプロイ概念

ルーターにおいてプログラムの実行が可能な EEM、API によるルーターの設定が可能となる onePK、設定の大幅な削減が可能な DMVPN 等、CiscoISR ルーターに搭載されている機能と、弊社が得意とするネットワークインフラやアプリケーション開発リソースを組み合わせ、ユーザーの高い要望に応える、より柔軟かつ投資効果の高いネットワークサービスを、今後も継続して開発、提供していきたい。

## 4. 参考文献

[1] IT Pro(日経コミュニケーション)、企業ネット実態調査 2012、http://itpro.nikkeibp.co.jp/article/COLUMN/20121106/435342/?ST=network&P=1

[2] 株式会社エヌ・ティ・ティピー・シーコミュニケーションズ、ダイナミック VPN、http://www.sphere.ne.jp/services/secure/vpn/

[3] シスコシステムズ合同会社、Dynamic Multipoint IPsec VPN (マルチポイント GRE/NHRP を使用した IPsec VPN のスケーリング)、http://www.cisco.com/cisco/web/support/JP/100/1006/1006430_dmvpn-j.html

[4] シスコシステムズ合同会社、株式会社 NTTPC コミュニケーションズが自動設定機能を用いてサービスプロバイダー マネージド サービスを提供、http://www.cisco.com/web/JP/solution/netsol/routing/literature/nttpc_casestudy.pdf

[5] 総務省、P2P ネットワークの在り方に関する作業部会報告書、http://warp.ndl.go.jp/info:ndljp/pid/283520/www.soumu.go.jp/s-news/2007/pdf/070629_11_1.pdf

[6] 一般社団法人日本ネットワークインフォメーションセンター(JPNIC)、ニュースレターNo.31、

https://www.nic.ad.jp/ja/newsletter/No31/020.html
[7] 西日本電信電話株式会社、NGN を用いたサービスの概要、http://www.ntt-west.co.jp/ngn/about/2nd.html
[8] 西日本電信電話株式会社、NGN の特徴、http://www.ntt-west.co.jp/ngn/about/index.html
[9] Cisco Systems, Inc.、Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T IPv6 over DMVPN、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-ip6-dmvpn.html