column

●本当のインターネットをめざして

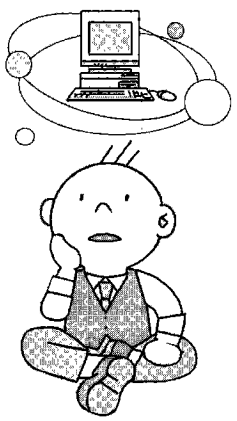
vol.30

マルチホーミング

太田 昌孝

東京工業大学 情報理工学研究科

mohta@necom830.hpcl.titech.ac.jp



IPv4インターネットの時代

現在のインターネットプロトコルであるIPv4が20年前に設計されたとき，254個までの端末を含む最少のクラスのLANは200万個あっても大丈夫なように設計された．そして，アドレスは要求に応じてLAN単位に割り当てられた．

しかし，インターネットを構成するLANが増え，すぐに破綻が明らかになった．アドレスをLAN単位にばらばらにふると，大域的経路表の大きさはLANの数だけ必要だったからだ．

そこで，サブネットやCIDRという技法が導入され，組織やISP単位でまとまったアドレスをふるようになった．サブネットを導入して組織内のLANにひとまとまりのアドレスをふれば，組織の外からは一組織につき1つの経路表エントリさえ用意しておけば，その組織に到達でき，LAN単位の経路表は組織内だけで持てばよい．CIDRを導入してISPとその加入組織にひとまとまりのアドレスをふれば，ISPの外からは一ISPにつき1つの経路表エントリさえ用意しておけば，そのISPに到達でき，組織単位の経路表はISP内だけで持てばよい．

サブネット導入以前のLANごとにばらばらな割り当てや，CIDR導入以前の組織ごとにばらばらな割り当てにより，CIDR導入時点では経路表の大きさは数万エントリまでふくらんでいた．すでに割り当てたアドレスを回収して，サブネットやCIDRの構造にあうように割り当てなおせば，経路表の大きさを大幅に減らせるが，せっかく割り当てられたアドレスを返納して別のに付け替えるのは大仕事なので，わざわざそんなことに付き合ってくれる管理者はいない．アドレスの付け替えは，事実上不可能である．しかし，新規割り当てについてはCIDRの考えを忠実に守ることにより，現在も経路表は十万エントリ程度に収まっている．

IPv6インターネットへ

CIDRによる割り当てルールでは，ISPの必要アドレスが増えた場合には，できるだけもとのアドレス範囲を覆う連続したブロックとして追加割り当てが行われるが，それが不可能な場合は，アドレスをすべて付け替えることになっている．しかし，アドレスの付け替えは事実上不可能であり，強要すればグローバルアドレスをあきらめNATを促進するだけである．

前回の議論と同様，IPv4の延命のために小細工を弄してNATを促進しては本末転倒だ．IPv6に移行して問題が解決するなら，IPv4の経路表は再現なく大きくし，IPv6への移行の推進力にしてしまえばいい．

IPv6では，最初からCIDRによりアドレスを割り当てる．IPv6の普通のユニキャストアドレスは最初が'001'というビットで始まる．次の13ビットをTLA（Top Level Aggregation ID）といい，トップレベルISPに割り当てる．TLAは一応13ビットしかないので，大域的経路表のエントリ数も8,192個ですむ．

IPv6アドレスの次の8ビットは予備（ここを使ってTLAを増やすこともできる）で，その次の24ビットがNLA（Next Level Aggregation ID）だ．NLAの上位ビットで次レベルISPを識別し，残りのビットで次レベルISP内の個別の加入者を識別する．個別の加入者内部のLANの識別に次の16ビットが使われることは，前回述べたとおりである．

IPv6では階層的に整然とアドレスを割り当ててゆくことにより，現状のIPv4よりかなり小さな経路表で，はるかに多くの加入者を扱うことができる．

しかし，これには落とし穴がある．

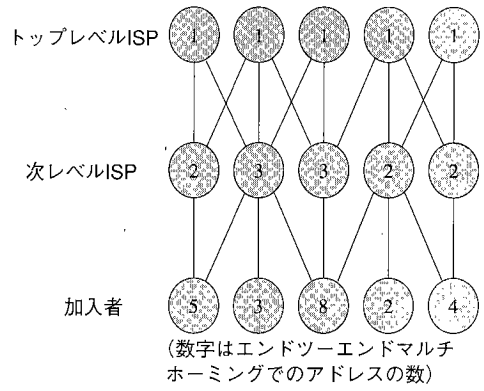


図-1　IPv6でのマルチホーミングの様子

マルチホーミング

前章のアドレス割り当て方式は，ISPと加入者が整然とした木構造をなすことを前提としている．ところがIPv4の現状をみても，多くの加入者は複数のISPを同時に利用するマルチホーミングを行っている．データセンターのように高信頼性が要求される場合には，マルチホーミングは必須である．どれかのISPが落ちてもインターネット接続性は失われないからだ．複数のISP間の相互接続性があまりよくない場合も，それぞれにマルチホームすれば，各ISPの加入者と快適に通信できる．マルチホーミングを行うとISP料金は余計にかかるが，すべてのISPが動作している平常時には，それぞれに負荷を振り分けると速度が向上するので，無駄ではない．

IPv4では，マルチホーミングした加入者は，独自のアドレスを持ちすべてのISPに自分への経路を通知する．すると，経路制御プロトコルがそれぞれのISP経由の複数の経路から通信相手からみて最短のものを自動的に選択してくれる．加入者のアドレスをどれかのISPからCIDR方式で割り当てても，他のISP内では加入者個別に経路を扱うしかないので，マルチホーミングした組織は，それぞれ個別に大域的経路表エントリを消費している．現在ではIPv4経路表の増大の大きな原因はマルチホーミングであるといわれている．

IPv6でも，同様のマルチホーミングを行おうとする加入者は，独自のTLAが必要だ．IPv6の次レベルISPには，データセンター同様，あるいはそれ以上に高い信頼性が必要とされるため，当然マルチホーミングを行い（**図-1**）TLAを消費することになる．結局TLAは際限なく増え，経路表の爆発は防げず，インターネットは崩壊してしまう．

そこで，筆者が提唱しているIPv6向けのマルチホーミング方式がエンドツーエンドマルチホーミングだ．マルチホームした組織では，各ホストにそれぞれのISPから取得した複数のアドレスをあたえ，各ISPにはそこから取得したアドレスについての経路だけを通知すれば，各ISPではCIDRにより経路情報をまとめることができる．

ただ，各ホストは複数のアドレスを持つことになる（図-1）．IPv4のマルチホーミングでは，同じアドレスへの複数の経路のうち最適なものを網中の経路制御プロトコルが選択してくれたが，エンドツーエンドマルチホーミングでは，選択権はホストに移り，通信相手の複数のアドレスのうち最適なものを自己責任で選択しなければならない．一見大変そうだが，もともとエンドツーエンド原理に基づくインターネットでは，網にたよらずにホストが自己責任で判断するのは当然である．アドレス選択のヒントとして，経路表は重要だが，マルチホーミング問題さえ解決すればIPv6の経路表は小さいので，各ホストがそれぞれ保持できる．

エンドツーエンドマルチホーミングの難点は，ホストのすべてのアプリケーションプログラムを改造しなければならないことだが，そう大変でもない．通信相手のすべてのアドレスを得るにはDNSが使える．IPv4でも，DNSが複数のアドレスを返すことはあり，その場合，インターネットで最も基本的なアプリケーションであるDNSと電子メールでは，サーバの複数のアドレスをすべて試すようになっている．TCPのAPIをいじって同様の処理を組み込んでしまえば，TCPしか利用しない多くのアプリケーションは，ほとんどそのまま動作する．通信中に現在のアドレスでは相手と通信できなくなったような場合，適当なタイムアウトで相手の別のアドレスを試す必要があり，一般にはタイムアウトはアプリケーションによって異なるが，TCPでは適切なデフォルトを定めればいい．

マルチホーミング問題を放置したままIPv6が普及していたらインターネットはすぐに破綻せざるを得ないので，今後これをどう解決するにせよ，IPv6の普及が遅れたのは実は幸いであったことになる．

（平成13年8月20日受付）