Column

●本当のインターネットをめざして●

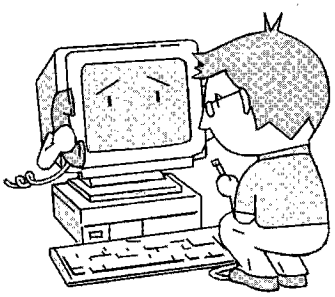
vol.31

リナンバリング

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とリナンバリング

昔はIPv4のアドレス割り当ては大らかであった．ちょっとした組織には6万4千個のアドレスが与えられた．また，アドレスは，特にまとまりなく各組織にばらばらに割り当てられた．しかし，経路表の大きさが問題になるにつれ，CIDRによる階層的割り当てに移行してきた．ISPに大きな塊でアドレスを与え，ISPの加入者はISPからアドレスの一部を受け取る．そのISPの外部では経路表エントリは1つでよく，個々の加入者ごとに経路表エントリを持つ必要はない．

ここで問題になったのがすでにアドレス割り当てを受けた組織である．それらの組織がアドレスを返納し，あらためて上流ISPからアドレスを受け取れば，経路表を小さくすることができる．しかし，そのためには組織内の全機器のアドレスの付け替えが必要だ．これがリナンバリングである．CIDR徹底のため，アドレスを割り当てる側はリナンバリングの必要性を声高に主張した．日本ではこれに馬鹿正直に従った組織もあったらしいが，世界的には誰も真面目に相手にしなかった．その理由として挙げられたのが，リナンバリングの困難さだ．リナンバリングのためには組織内の全機器の設定の変更が必要で，その最中には組織内からインターネットは利用できず業務に支障がでる．それだけの手間をかけてリナンバリングしても，数万エントリある経路表の大きさが1つ減るだけでは，引き合わない．そこで，リナンバリングは困難な問題と認識され，IPv6の設計でもその自動化が重要な目標となった．

また，IPv6のアドレスはISPを通じて階層的に割り当てられるが，その副作用として，ISPを変更するとリナンバリングも必須となる．そのためにもリナンバリングの自動化は重要である．

IPv6と設定の自動化

上流ISPが変化したとき端末のアドレスを自動的にリナンバリングするのはそれほど難しくない．IPv6のアドレス割り当て方式では，128ビットのアドレスのうちISP依存部分は常に上位48ビットなので，自分のアドレスの下位80ビットはあらかじめ設定しておき，上位48ビットは自分が所属するISPから流してもらうようにしておけばよい．

これだけならなにも問題はなかったのだが，IPv6では勢い余って端末の設定全般の完全な自動化までが目標となった．これをStateless Autoconfigurationという．確かにLANのことしか考えてないパソコン用ネットワークの設定ならかなりの程度の自動化が可能だ．IPv6でも同じことを目指したのだが，インターネットにつながる場合には少なくともセキュリティ関係の秘密情報を信頼できる方法で入力する必要があり，自動化は不可能である．そして，この程度の自動化なら旧来のDHCPで十分だ．

それにもかかわらず，IPv6の開発ではStateless Autoconfigurationの実現のための方策がいろいろと提案され，無批判に実装された結果，プロトコルや運用は無意味に複雑化し，実装は巨大化している．

DNSとリナンバリング

たとえ，個々の端末のアドレスを完全に自動的にリナンバリングできたとしても，それだけではリナンバリング問題は解決しない．

端末の設定情報の多くは，他の端末のアドレスを含み，リナンバリングにより他の端末のアドレスが変わった場合，変更が必要となる．一般的に，自分のアドレスが他の

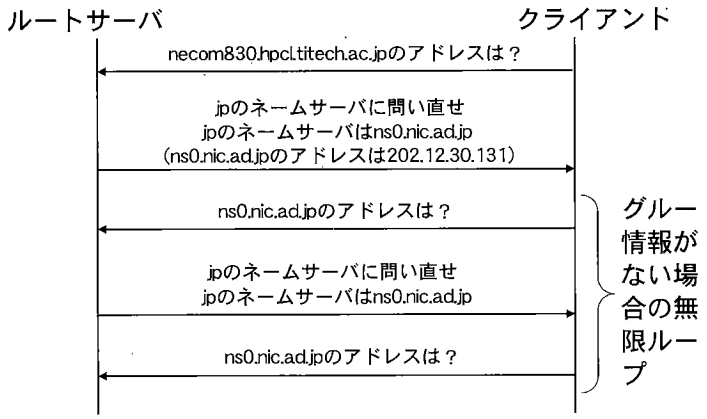


図-1　ドメイン名からアドレスへの変換（括弧内がグルー情報）

端末の設定情報に含まれていることは知りようが無いため，アドレスが変わった場合の設定の変更は手作業となる．

この問題の単純で効果的な解決策は，他の端末をアドレスではなくDNSのドメイン名で識別することだ．DNSには動的変更機能が追加されており，リナンバリングの際に自分のドメイン名の表すアドレスを更新できる．もちろん，自分のドメイン名を他人にのっとられないようにするため，変更には適切なセキュリティが必要で端末の設定自動化は不可能である．ドメイン名を利用する側では設定情報読み込みの時にドメイン名をアドレスに変換すれば，常にリナンバリング後の最新のアドレスが得られる．

ただ問題は，DNSを利用するためには，DNSサーバに問い合わせなければならず，そのアドレスが設定情報として必要なことだ．そのうちいくつかはドメイン名で置き換え可能だが，どうしても生のIPアドレスが必要な部分が2種類だけ残る．

そのひとつは，DNSサーバの最上位に位置するルートサーバのアドレスである．DNSでは，問い合わせ相手の見当がつかない場合，とにかくルートサーバに問い合わせるため，ルートサーバのアドレスだけは各端末が知っておく必要がある．

幸いルートサーバをリナンバリングする必要はない．ルートサーバは全インターネットに十数個しかない極めて重要なサーバである．そこで，たとえルートサーバを取り巻く環境が変わってCIDRのためにはアドレスの変更が必要になったとしても，古いアドレスを使いつづければよい．たかだか経路表のエントリが十数個増えるだけである．

もう一箇所DNSで生のIPアドレスが必要な場所がグルー（糊）情報である．DNSのドメイン名は木構造を持つが，この構造はネットワークのトポロジやIPアドレスの構造とは無関係である．ある組織の複数の事務所は，それぞれの地点で異なるISPに属し全然違うIPアドレスを使うかもしれないが，その組織の持つドメイン名を共同で利用することができる．ドメイン名からIPアドレスへの変換は，ドメイン名の木構造に沿って複数のDNSサーバをたどって行われる．問題は，ドメイン名の構造とDNSサーバの構造が食い違いループが生じる場合である．たとえば日本のjpドメインのDNSサーバの1つは，ns0.nic.ad.jpというドメイン名を持つ．すると，ns0.nic.ad.jpというドメイン名をアドレスに変換しようとしても，問い合わせるべきDNSサーバのアドレスがわからない．このような事態を防ぐため，DNSの適切な場所（上位のDNSサーバ）にはグルーとよばれる下位DNSサーバの生アドレス情報が格納されている（**図-1**）．DNSサーバのリナンバリングの際にはグルー情報も変更する必要があるが，グルー情報の格納場所である上位のDNSサーバが何であるかは一般に下位からはわからないので，自動的なリナンバリングは無理だ．

リナンバリングの今後

現在IPv6でマルチホーミングやリナンバリング問題にどう対応するかは混迷しており，それに応じてDNSでIPv6アドレスをどう表現するかもちゃんと決まっていない状態だ．しかし，IPv6によりリナンバリングの苦労がある程度軽減されることと，それでも完全な自動化は不可能であることは確かだ．

実は，IPv4でリナンバリングが受け入れられなかったことには，リナンバリングの困難以前に問題があった．経路表と同時にアドレス空間の節約も重要であるという考えでは，ある組織がリナンバリングのために6万4千個のアドレスを返納しても，上流ISPからもらえるのはその時点で実際に必要な数のアドレスだけである．わざわざアドレスを減らしてまでリナンバリングに協力する奇特な組織はそうはない．

逆にいうと，IPv6時代のリナンバリングは，Stateless Autoconfigurationという見果てぬ夢を追いかけずとも，現状程度でなんとか物になりそうだ．

（平成13年9月17日受付）