

Contents Layer Internet eXchange とそれを取り巻く諸問題

三 谷 和 史

はじめに

Internet は現在では The Internet を指すようになったが、元来は inter-network, 即ち個々の組織, もしくは組織の集合体のネットワーク間を (inter) 接続するネットワークという意味である。また, Internet は Internet Protocol (IP) [1]によって通信が行われるネットワークである。

つまり, ネットワークの間を接続するものがなければ Internet は成り立たず, それを行っている代表的なものが Internet eXchange なのである。

Internet eXchange (以下 IX と書く) は, 異なるネットワークを接続するポイントであり, ここを通じて組織間の IP パケットが交換される。

IX には大きくわけて, Global IX (GIX), National IX (NIX), Regional IX (RIX) の3つがあると考えられる。

GIX は国際間の IP パケットを交換する場であり, 主にアメリカに置かれている CIX (Commercial Internet eXchange) がその役割を担っている。

NIX は国内の IP パケットを交換する場である。国内では, NIX として1994年より WIDE Project (Widely Integrated Distributed Environment Project)^{†1}によって NSPIXP1 (Network Service Provider Internet eXchange Project 1) の実験運用が始まり, 現在は NSPIXP2, 3での実験運用が行われ, また商用の IX も複数現れている。

† 1 URL: <http://www.wide.ad.jp/>

RIX は地域内における IP パケットのショートカットの場として作られることが多く、組織間の合意の基に組織間のパケットのみを交換する。例えば道内では釧路管内でこのような RIX が活動している。

IX では IP パケットが直接交換される、つまり、複数のネットワークインタフェースのいずれかからやってきた IP パケットは、経路表に基づいてしかるべきネットワークインタフェースへと送られる。

図 1 に IX において IP パケットが点線を通して直接やりとりされることを示している。

多くのユーザに対してサービスを提供する場合、ユーザがどのネットワークに接続しているかに係わらずサービスの質 (WWW (World Wide Web) で URL [2] をクリックしてから実際に情報が手元に届く時間といったもの) を一定以内に保ちたいと考えると、複数のネットワークが接続している IX を介してサービスを行うことが望ましい。

しかし、既存の NIX に、ある組織が機器を持ち込んでサービスを行うことは不可能である。それでは、組織が NIX を新たに立ち上げて、複数の ISP (Internet Service Provider) 等と接続することが可能かという点、これも種々の理由で不可能なのが現実である。

しかし、既存の NIX に、ある組織が機器を持ち込んでサービスを行うことは不可能である。それでは、組織が NIX を新たに立ち上げて、複数の ISP (Internet Service Provider) 等と接続することが可能かという点、これも種々の理由で不可能なのが現実である。

そこで、本論文では IX に代わる概念として、複数の ISP との接続を行うが IP パケットの直接的な forwarding を伴わない、Internet における Layer 4†²でのアプリケーションサービスとして Contents Layer Internet eXchange (CLIX) を提案し、CLIX が複数の ISP と接続する場合に生じる諸問題と、現在実験を行おうとしている CLIX Project についての概要説明を行う。

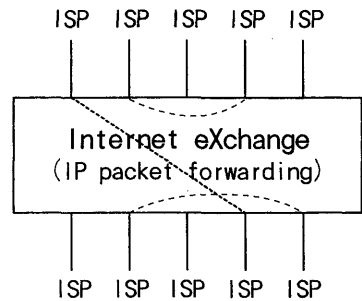


図 1 Internet eXchange

† 2 OSI 的に表現すると Layer 7

図2にCLIXの概念を示す。図1と異なるのは、CLIXを通過して直接IPパケットが交換されることはないという点である。

即ち、CLIXとやりとりされるパケットは、発信元IPアドレスがCLIXのIPアドレスであるか、相手先IPアドレスがCLIXのIPアドレスであるかのいずれかを満たしている場合に限られ、それ以外のパケットがやってくることはなく、仮にそれ以外のパケットやってくるがあっても、IXのようにそのパケットを中継することは行わない。

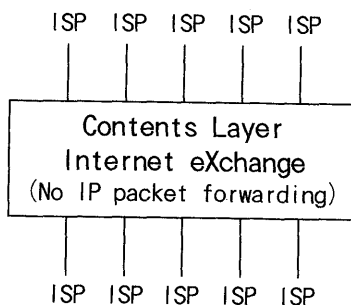


図2 CLIX

2 インターネットの接続形態

ここでは、現在のインターネットがどのような接続モデルの上で成り立っているかと、なぜ国内でNIXが増やせないのかについて説明を行う。

2.1 ASモデルとIX

現在のインターネットのモデルは、ネットワークの自律的主体範囲であるAS (Autonomous System) 番号をもつ組織と、GIXとNIX及び一部のRIXのバイパスによって成り立っている。

通常AS番号を持つ組織は、1つ以上のIXと接続を行い、他の組織と通信を行っている。通信を行うかどうかは、両方の組織のAUP (Acceptable Use Policy) によって合意可能な範囲で定める。また、通信を行うために必要となる経路表は通常BGP4[3]によって交換されている。

国内同士のパケットはNIXで交換し、海外とのパケットはGIXで交換するのが通例である。米国が現在はGIXの役割の大部分を負っている。

AS番号をもつ組織は、ISPや学術研究組織 (WIDE, SINET (Science In-

formation Network)^{†3)}等のネットワーク管理組織である。

通常このような組織はNIXに接続して、互いのAS間のパケットを交換する。これをpeeringという。NIXでのpeeringは、NIXに接続する組織全てと必ずpeeringを行うという方法と、AS同士のネゴシエーションによってpeeringを決める方法がある。

また、このようなAS番号をもつ組織は自前でGIXへの接続、いわゆる自前の海外線を持ち、海外の組織との通信は自前の海外線を通じてGIX経由で行う方法をとる。

仮に、NIXに接続する組織で海外線を持たない所があれば、その組織を海外にキャリアする契約をどこかの組織と結ばない限り、その組織はグローバルなコネクテビティを持たない。しかし、そのようなグローバルなコネクテビティを持たない組織はインターネットに接続しているとは言えない。通常NIXには自前で海外線を持つ組織が接続をしており、海外線を持たない組織は他の組織に海外線のキャリアの契約をして接続する必要がある。しかし、この場合は、その組織を海外へキャリアをしている組織の一部とみなして、ASもキャリアしている組織のASに組入れ、キャリアする組織と接続するのみで、NIXへの接続は行わないことが多い。

図3に、NIXに接続するISPが3つあり、そのうち2つがGIXと海外線で接続されている様子を示す。ここで、ISP Cが有するASは、ISP Cが海外線を持たないのであれば、この例ではISP A, Bのいずれかとキャリアをする契約を結ばなければグローバルなコネクテビティがない。

RIXはこれらと比べて意味が少し異なる。これは、AS間というよりも、組織間やローカルISP間で、バックドア的にネットワークを接続して、ローカルにパケットを交換する場所である。当然、RIXが停止してもNIX経由の経路を選択できれば組織間の通信が途絶えることは通常ない。NIXやGIXと接続しているISPがRIXと接続することは通常ない。

† 3 URL: <http://www.sinet.ad.jp/>

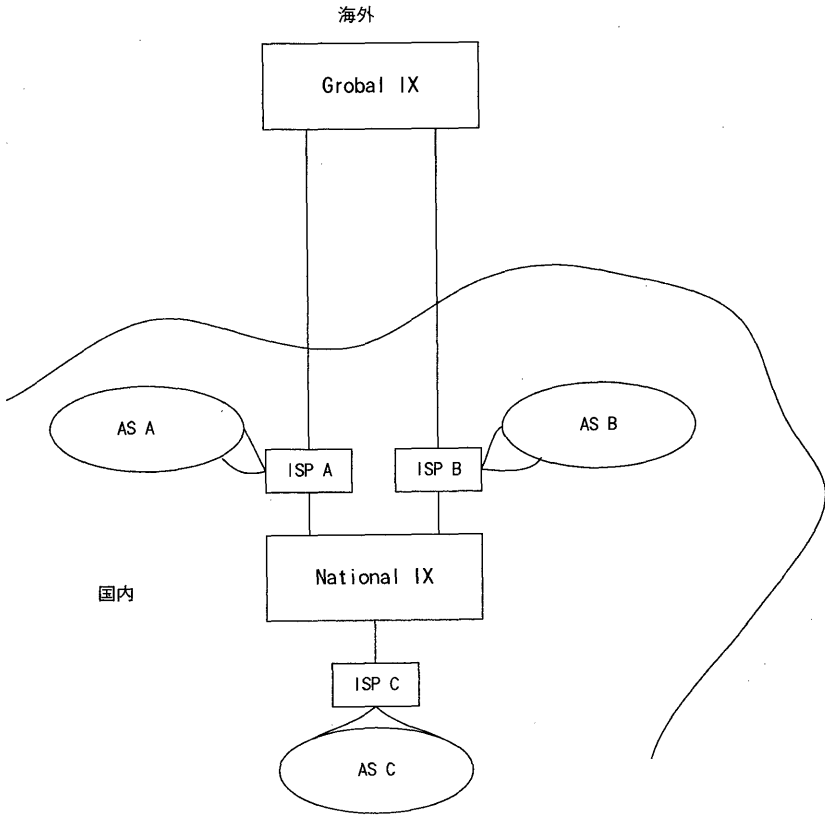


図3 ISPとIXの接続

2.2 NIXを多数作れないのは何故か

道内でも数多くのISPがサービスを行い、また大学は主にSINETによってインターネットに接続されているが、これらの間のIPパケット交換は東京または大阪に設置されたNIXを通じて行われているのが現状である。IXはトラフィックが集中するため混んでおり、また道内からは距離が離れているので当然遅延が生じる。例えば小樽商大の学生が自宅でISPと接続しているとき、自宅と大学との間の通信が内地を回るため遅延が生じ、かつパケットロスが起る可能性が高いわけである。この間の通信を札幌を中継点として行えば、

距離による遅延も少なく、NIXでのパケットの集中も緩和され、結果NIXでのパケットロスも減少し、円滑な情報交換が可能となるわけである。

NIXは現在国内ではNSPIXP 1, 2が東京で、3が大阪で稼働し、JPPIX^{†4}、MEX^{†5}といった複数の商用IXが稼働している。

地政学的には北海道と九州へのNIX設置が望ましいがまだその段階ではない(商業的にペイしない)といわれている。

NSPIXP1の実験開始後、ほぼすべての道府県から我が地域にもIXをとという声があがった。IXを設置するには場所と機材の他に、IXを安定してオペレーションできるだけの技術を持つ人間が必要であるが、そのような技術者の数は極めて少ない。さらにISPの参加は、ISPにとってオペレーションの複雑化を招くので、仮にIXを設置したとしてもISPの参加が見込めないという状況がある。

オペレーションが複雑となる原因は、現在のインターネットの経路制御においては、ISP毎に適当なCIDR [4] blockのネットワークアドレスを割り当てることにより経路をaggregateし、経路表を圧縮して経路交換を行うことが大前提となっているが、ISPは割り当てられたCIDR blockからその顧客へネットワークアドレスを割り当てる際に、地域を考慮した形での割り当てを行っておらず、IXが多数設置されてそれらと接続した場合、aggregateされない経路による経路交換をせざるを得ないからである。

3 CLIXとその諸問題

本章ではCLIXとは何であるか、及びCLIXがその目的のために複数のネットワークと接続した際に起こり得る諸問題について説明を行う。

† 4 URL: <http://www.jpix.ad.jp/>

† 5 URL: <http://www.mex.ad.jp/>

3.1 CLIX とは何か

CLIX とは、次の定義を満たすサーバである。

- 複数の ISP との接続を行う。
- IP パケットの直接の中継を行わない (`ip_forwarding = 0`)
- 特定の application の proxy として動作する。

特に WWW に対しては proxy & cache としての動作を行うことでトラフィックの減少に寄与することが可能である。また、複数の ISP が接続している特性を利用して

- CLIX で特定のサービスを行うサーバを設置する。

という ICP (Internet Contents Provider) 的利用方法も可能である。

proxy とは一般に代理サービスを指し、ユーザがインターネット上の資源への直接のアクセスを行う代わりに、proxy サーバに対して資源へのアクセスを要求し、proxy サーバが資源にアクセスして、そこで得た情報をユーザに返すという枠組みである。

IX が ISP へのサービスであると捉えるならば、CLIX はユーザへのサービスであるとも考えることもできる。

図 4 に、CLIX を proxy として指定した *user* からの資源アクセスのリクエストとその応答の様子を示す。

proxy は、一般に企業等で内部から外部のネットワークへはセキュリティ上の理由等から直接アクセスできない場合や、内部がプライベートアドレス [5] である環境で、外部の特定のサービスを内部から透過的に、もしくは明示的に proxy を通じることでアクセスできるようにするために使われている。

グローバルアドレスに接続可能なユーザが CLIX の proxy サービスを使う目的は、ユーザがインターネットの資源に直接アクセスする場合に比べて、proxy を経由することによって資源のアクセスにかかる時間を短縮することである。

特に、WWW の proxy & cache の場合は、複数のユーザが CLIX の proxy & cache を利用することで、自分の要求する URL の内容がキャッシュされて

いることが期待される。

一方、ISP から見た場合、CLIX は単なる顧客のネットワークとして見えるため、IX に接続するための経路制御問題の複雑さが発生せず、商用として CLIX を設置した場合でも ISP が接続をし易い形態であると考えられている。

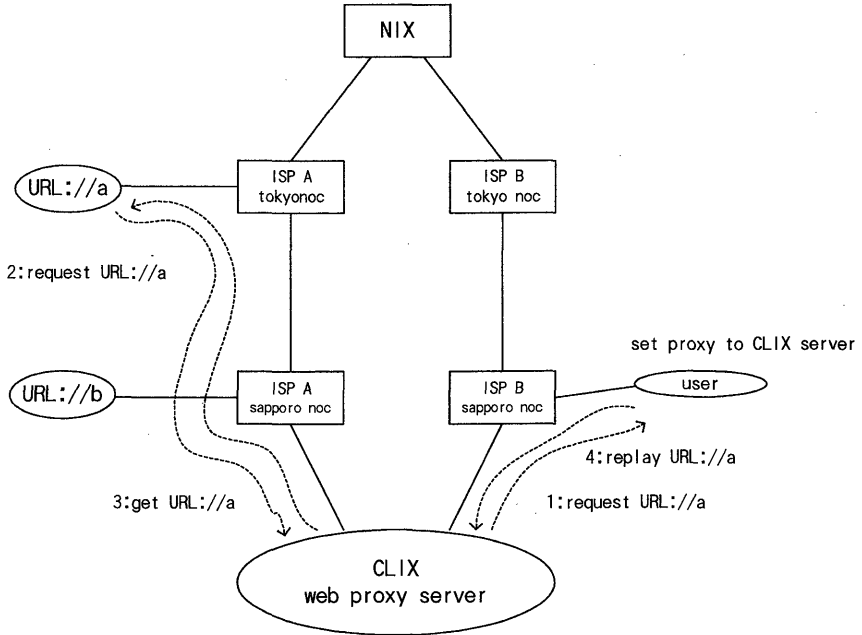


図4 CLIX の proxy 動作

3.2 CLIX の接続方式

CLIX を構築する場合、複数の ISP 等と接続をするためにはいくつかの方法が考えられる。ここでは代表的な接続方式について説明を行う。ここでの接続方法は CLIX に限らず同じような接続方法をとる場合に当てはまるものである。

自己アドレス Multihome 方式

一般に複数の経路によってインターネットに接続することを Multihome という。

自己アドレス Multihome 方式は、組織の持つネットワークアドレスを用いて複数の ISP によって外部と接続する方式である。Multihome を行うことによって、接続している ISP のいずれかとの接続が切断されたとしても、CLIX のサービスを行うことが可能である。

割り当てアドレス Multihome 方式

自己アドレス Multihome 方式が、組織の持つネットワークアドレスを複数の ISP からアドバタイズ（このネットワークへのパケットはこちらへ送れと経路情報を流すこと）することに対して、この方式は複数の ISP から割り当てられたアドレスを CLIX サーバの複数のネットワークインタフェースに割り当てる方式である。即ち、これは図 2 に示した各 ISP へのネットワークインタフェースで、各々の ISP から割り当てられたアドレスを使用することを意味する。

現在国内では、ネットワークアドレスの割り当ては ISP が JPNIC^{†6}から割り当てられたアドレスを顧客に割り当てる方式が主となっているので、ISP と契約を行う際に ISP から割り当てられたネットワークアドレスをそのまま使用する。この場合、CLIX サーバは ISP 間のトラフィックを中継することは行わないので、`ip_forwarding = 0`として、パケットの中継を止める。

仮想アドレス Multihome 方式

割り当てアドレス Multihome 方式では、CLIX サーバが持つことができる物理的ネットワークインタフェースの数が有限であるため、その数以上の ISP との接続は不可能である。

そこで、図 5、6 に示す、自前アドレス Multihome 方式と一見同様な方法で接続する ISP を増やすことを考える。自前アドレス Multihome 方式と異なる点は、太線で示すローカルネットワークが複数のアドレスをもった多重ネットワークである点である。イーサネットは 1 つのネットワークを複数のネットワークアドレスをもったネットワークとして運用できるので、このようなこと

† 6 URL: <http://www.jpnica.ad.jp/>

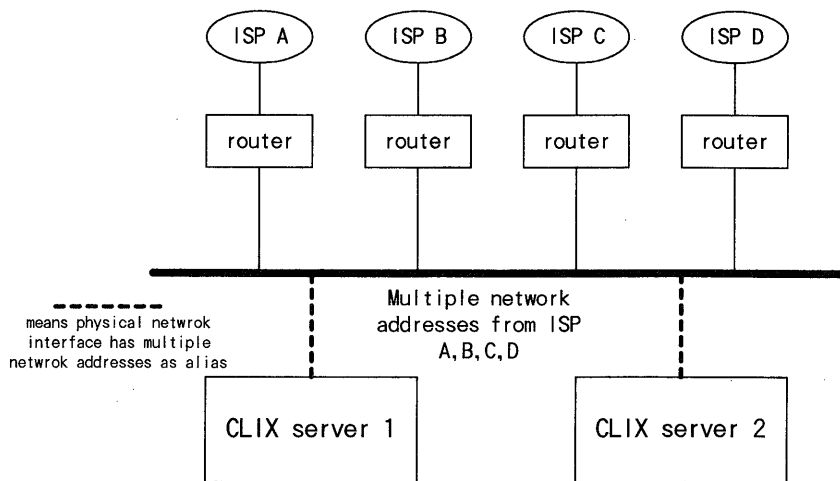


図5 多重ネットワークアドレス方式1

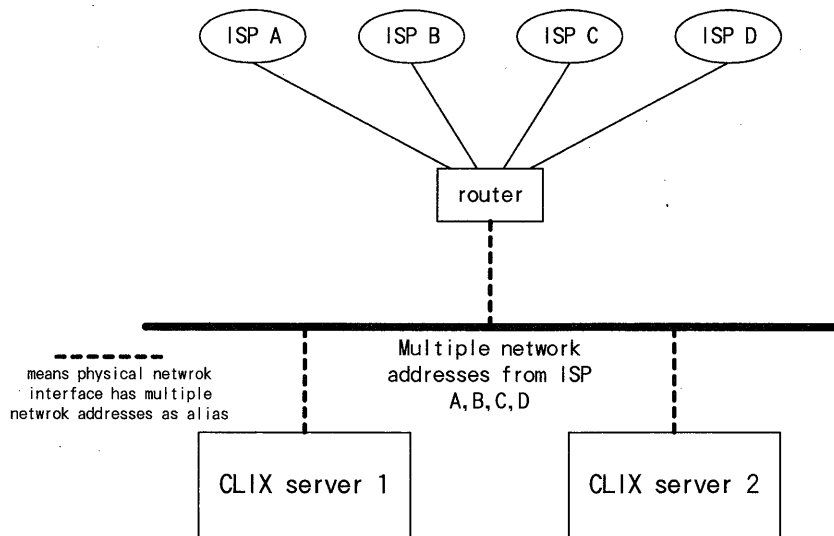


図6 多重ネットワークアドレス方式2

が可能となる。このとき、コンピュータが接続している物理的ネットワークインタフェースは1つであるが、これに仮想ネットワークインタフェースを追加することによって複数のネットワークインタフェースが接続しているかのように見せかけて運用を行う。割り当てアドレス Multihome 方式の一部のネットワークインタフェースを多重ネットワークアドレスにして運用することも考えられる。

3.3 各々の接続方式における問題点

前節で述べた接続方法で複数の ISP との接続を持った CLIX を運用する場合、いくつかの問題が発生することが予想される。ここではその問題点と解決手法について説明を行う。

3.3.1 自己アドレス Multihome 方式の問題点

CLIX が持つアドレスを使って Multihome を行う場合、CLIX のサーバが発信するパケットの経路選択をどうするかという問題が発生する。対外ルータが1台でそのルータに複数の ISP からの接続が行われている場合は、CLIX のサーバは default route を対外ルータに向けるだけでよいが、対外ルータは相手先への最適と考えられる経路を選択するために、ISP からそれぞれ full route（現在数万経路）を入手する必要がある、ISP への帯域が細い場合はそれ自体が困難である。

また、既にどこかの ISP と接続を行ってその ISP の AS の CIDR block からネットワークアドレスを割り当てられた状態で、別の ISP とも新たに接続を行って、既接続の ISP から割り当てられたネットワークアドレスをそのまま用いて Multihome をする場合は、新たに接続した ISP は自分の AS のネットワークアドレスに他の AS のネットワークアドレスを含むことになるため敬遠しがちである。特に、class C よりも小さなアドレスブロックを使っている場合は、CIDR によって経路を aggregate できなければ、新たに接続した ISP がこのネットワークアドレスを自分の AS からアドバタイズしたとしても IX

によっては受け入れて貰えない場合もある。

ISPとしては、元来顧客はそのISPだけが顧客のインターネットへの出口であり、default route だけが流れれば接続性が保たれると考える傾向があるが、複数のISPと接続する場合はそう簡単にはいかない。full route が入手できない場合は、少なくともISPのASの範囲についての経路を入手しなければ、適切な経路の選択は行えない。そしてそれ以外はdefault route による経路の選択となる。

また、ルータが1台ではないとすると、ルータが経路情報をCLIX内部のネットワークに流して、CLIX内部のコンピュータはどのルータを選択するか的情報を持たなくてはならなくなる。この場合もfull route が入手困難であれば、default route によつての経路選択がとなる。

いずれの場合も、default route によつての経路選択が行われたISPへのトラフィックが増大して、複数のISPと接続することの狙いの1つであった負荷分散は果たせなくなる。

さらに、1つのネットワークアドレスを複数のISPがアドバタイズする、つまり複数のASにネットワークアドレスが存在するということが現在のインターネットの流れでは排除される方向に向かいつつあり、それを避けるためにCLIXが独自にAS番号を取得することも、AS番号の資源が涸渇する恐れがあるので簡単には行えない状況である。

また、CLIXのサーバに対してコネクションを行う外部のユーザからの経路が、はたして最適な経路を通つてやってくるかどうかという問題についても、ISP同士の経路交換に全てが委ねられていて、CLIXが外部からの経路の選択を律するための手段を持たない。

このような現状であるため、複数のISPからfull route を得ることができる程度の帯域幅がある接続をしないかぎりには、負荷分散という意味で自己アドレスMultihomeを行うことは現状ではうまく機能していない。

また、full route を得ている場合でも、サービスを要求する組織に偏りがある場合に、その負荷を他のISPを経由することによつて分散させることも難しい。

た CLIX があり、ISP A から割り当てられたネットワークアドレスからアドレス a をネットワークインタフェース Ifa に、ISP B から割り当てられたネットワークアドレスからアドレス b をネットワークインタフェース Ifb に与えた状態である。

ここで、ISP B の AS に存在する $user$ がアドレス a に対してサービスを求めてコネクションを行ったとする①。このパケットは ISP A の AS に存在するアドレスの a に対するコネクションであるから、ISP B から NIX を経由して ISP A を通って CLIX の Ifa に届けられる。

このコネクションに対して CLIX が $user$ に対してパケットを送出する場合は、 $user$ が ISP B の AS に存在するので Ifb を選択することになる。②

TCP [8]による通信は、(src address, src port, dst address, dst port, TCP) の5つ組によって表わされ、CLIX ではこの5つ組が (address a , src port, $user$ address, dst port, TCP) となっている。つまり、CLIX のソースアドレスが a であるパケットが Ifb 、即ちアドレスが b であるネットワークインタフェースから送出されることになる。

図7を見てわかるように、 $user$ からやってくるパケットの経路と、 $user$ に戻るパケットの経路は異なる。異なっても通信は可能であるため、それ自体は問題となることはない。

現在、packet spoofing (偽造パケット) を用いたネットワークへの攻撃^{†7}が問題となっている。そこで、ISP では顧客からやってくるパケットのソースアドレスが ISP が顧客へ割り当たアドレスでなければパケットを中継しないというフィルターを設定することによって、packet spoofing を自分の顧客が行うことを不可能とする対策が行われ始めている。

こうなると、②の経路を通して戻るパケットは、そのソースアドレスが ISP から割り当てられたアドレスと異なる a というアドレスであるから、パケットが中継されずに、 $user$ との通信が行えない。

†7 URL: http://www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html が参考になる。

これを避けるためには、フィルタリングを行う場合は CLIX が持つ全てのアドレスについての中継を行うようなフィルターの設定を行って貰う必要がある。

3.3.3 割り当てアドレス Multihome 方式の問題点 2

前節で述べた通り、packet spoofing 対策のフィルターの適切な設定で、行きと返りの経路が異なる問題は解決できるかに見えるが、まだ同様な問題が残されている。

図 8 を使って説明を行う。user は CLIX と直接接続している ISP とは異なる、海外の ISP のユーザとする。そして、user が *Ifa* 側のアドレス *a* に対してコネクションを張ってきたとする。このとき CLIX は default route として *Ifb* を選択している状態なので、前節と同様、行きと返りの経路が異なること

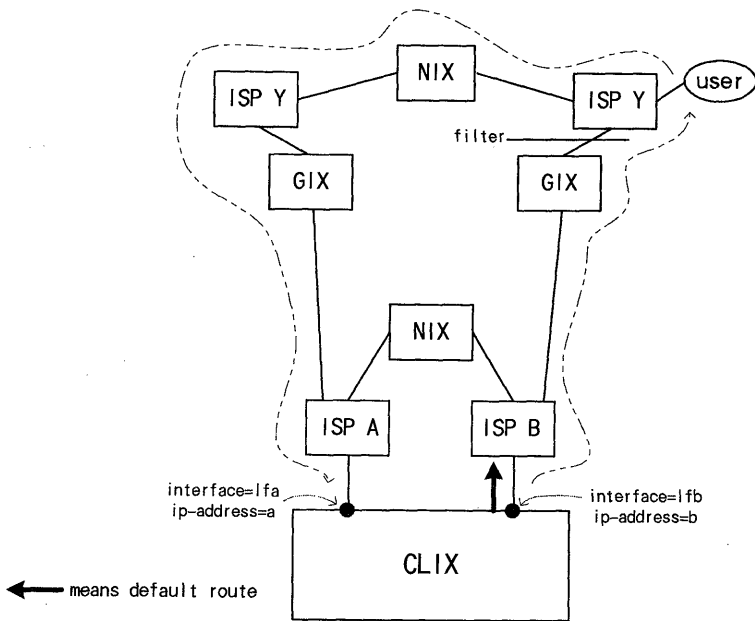


図 8 ユーザからのリクエスト経路と返りの経路 2

になる。そして、ISP Bは a という CLIX の持つアドレスがソースアドレスであるパケットも中継を認める設定をしているとする。

この場合でも、ISP Yにおいて GIX からやってくるパケットのソースアドレスが GIX に接続している AS に含まれるものでなければならない、というポリシーでフィルタリングを行うと、CLIX から *user* への返りのパケットはフィルターによって捨てられ、通信が行えない状況となる。

先ほどと同じ方法で解決を行おうとすると、結局世界中の ISP 等で中継に関してフィルターをかける場合に、接続しているネットワークインタフェースからやってくると期待される AS のネットワークアドレス以外に、ISP から通過を許可されてやってくる可能性があるネットワークアドレスを考慮する必要が生じ、これは繁雑であるためうまく機能する保証はない。

同様に、図 9 に示す状況で、default route が ISP A から ISP B に変わった、

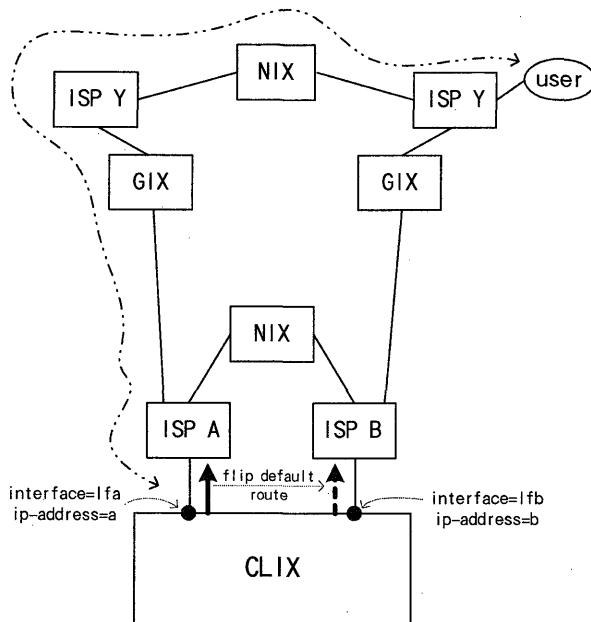


図 9 default route の変更

もしくは full route を貰っている状況で *user* に対する経路が ISP A から ISP B に変わったとする。変わる前の状況では、行きと返りは共に ISP A 側を選択している状況であったが、default route が変わることで図 8 と同じ状況となる。

但しこれらの場合は、CLIX が CLIX の近傍地域のユーザに対するサービスのために設置されていることを考慮すれば、このような接続はないものとして問題にしなければよい。但し、CLIX がユーザからリクエストを受けた資源にアクセスしている最中に default route の変更等で資源にアクセスするための経路が変更になった場合には、フィルターによってアクセスが途中で出来なくなる可能性が残る。

3.3.4 割り当てアドレス Multihome 方式の問題点の解決策

これらの問題点に対して解決策となりうるものをあげて、はたして解決策となりうるかを検討する。

ネットワークインタフェースアドレスの DNS 上の名前を異なる名前として、ユーザが適切な名前を選択して使うという方法が CLIX 側のコストを考えた際には最も安価であるが、CLIX と直接接続している ISP のユーザ以外は経路が変更される場合があり、またユーザがはたして適切な選択をするかは疑問であるため有効な手段とはならないであろう。

そこで、全てのネットワークインタフェースアドレスの名前を DNS 上では同じ名前として、DNS への問い合わせに対して問い合わせを行ってきたソースアドレスへの経路が選択されるネットワークインタフェースのアドレスを先にして返すという手法が考えられる。これは DNS round robin と似た手法であるが、CLIX で DNS の primary server を立ち上げて適切なアドレスを返すとしても、それ以外の DNS の secondary server は常に CLIX の経路表の状態を知らなければ適切なものを先頭にしてユーザへアドレスを返すことができず、また、ユーザが問い合わせた DNS のキャッシュがヒットして返されたアドレスの場合は適切であるかどうかは不明となる。

別の手法として、TCPもしくはTCPとICMP[9]の拡張を行って、TCPのコネクション要求であるSYNパケットが適切でないネットワークインタフェースのアドレス宛てであった場合は、適切なアドレス側に変更してから再接続を行うように要請する方法も考えられるが、全てのコンピュータのネットワークコードを変更することは困難であり、かつセキュリティホールとなる可能性が残る。

また、これらの方法はいずれも経路表に基づいたパケットの送出を行うことが前提であるから、経路表の変化によってパケットを送出するネットワークインタフェースが変更された場合は、フィルタリングによってパケットが届かなくなる可能性が常に残る。

逆のアプローチとして、経路表に頼らずに、TCPのSYNパケットがやってきたネットワークインタフェースを覚えておいて、返りのパケットは必ずそのネットワークインタフェースから送出するというVixilの方法[10]がある。この手法を用いれば、フィルタリングによってパケットが届かなくなる可能性は消えるが、経路が最適でないためにCLIXに期待されるショートカットによる資源アクセス時間の短縮が果たせない場合も起こり得る。また、UDP[11]についてはこの手法が適用できていない。

さらに別の方法としては、各ISPはCLIXに対して自分が割り当てたネットワークアドレス以外のCLIXの有するネットワークアドレスについても、経路情報を流すというものが考えられる。この場合、ISP自身のASの範囲内からCLIXに自分が割り当てたアドレス以外にCLIXが有するアドレス p へのコネクション要求があった場合にも、そのISPが割り当てたアドレスを持つネットワークインタフェースにパケットを送り、そのISPのASの範囲外には、 p のアドレスを割り当てたISPとCLIXとの間のネットワークが切断されてない限り、 p のアドレスを割り当てたISPを通してCLIXにパケットが送られるが、切断されたときは自分のASを経由してパケットを届けることができるような経路情報を送る。

また、フィルタリングを行う場合も、当然CLIXのもつ全てのネットワーク

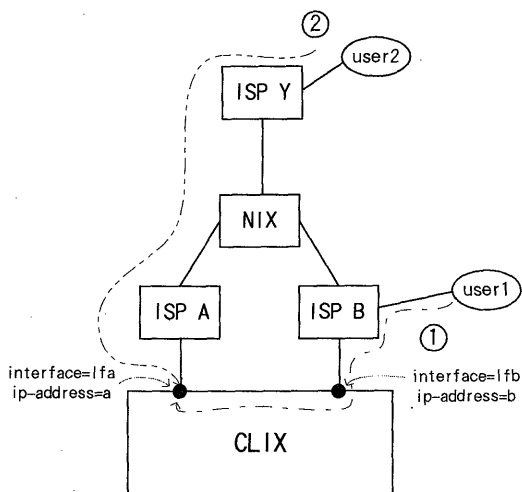


図10 CLIX の持つ別のアドレスの経路情報を流す場合の経路 1

アドレスを通過させることが必要となる。

図10において、ISP B の AS 内の *user1* が CLIX に ISP A から割り当てられたアドレスを持つネットワークインタフェース *Ifa* に向けてパケットを送る場合、①の経路を通過して ISP B から CLIX に割り当てられたアドレスをもつネットワークインタフェース *Ifb* を経由して *Ifa* に届けられるが、他の ISP の *user2* からのパケットは②の経路を通過してネットワークインタフェース *Ifa* に届く。

ここで、図11のように ISP A と CLIX の間が切断された場合は、ISP B 以外の *user2* からのパケットもネットワークインタフェース *Ifb* を経由してネットワークインタフェース *Ifa* に届けられ、図12のように ISP B と CLIX との間が切断された場合には ISP B の AS 内の *user1* からのパケットは、NIX を経由してネットワークインタフェース *Ifa* に届けられることになる。

この方法がうまく機能すると、複数の ISP と接続することによるバックアップ機能が達成されるが、経路情報の複雑化と、IX によっては aggregate されていない小さなアドレスブロックの経路情報は受け付けない場合があるので、実現が困難な場合が多い。

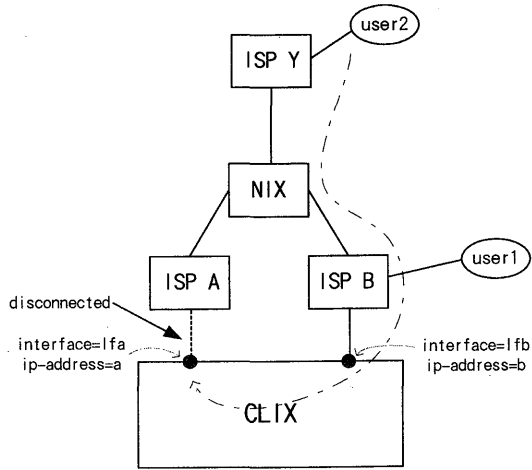


図11 CLIX の持つ別のアドレスの経路情報を流す場合の経路 2

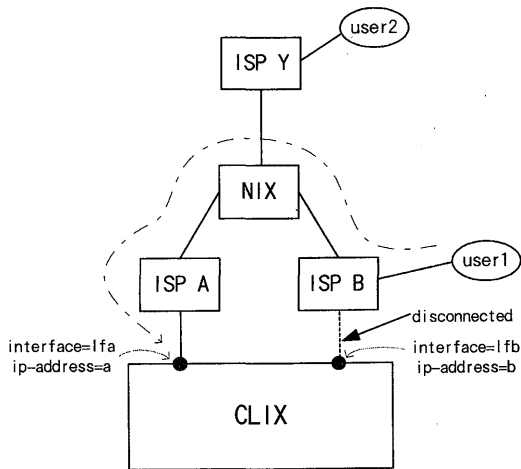


図12 CLIX の持つ別のアドレスの経路情報を流す場合の経路 3

3.3.5 仮想アドレス Multihome 方式の問題点

仮想アドレス Multihome 方式での問題点は、これまでの2つの方式における問題点に準ずる。

また、実際のネットワークインタフェースの1つに仮想ネットワークインタフェースをつけた場合、経路情報を仮想ネットワークインタフェースから受けたものが正しく経路表に登録されるか、及び、CLIX サーバからコネクションを張る場合の CLIX 側のソースアドレスが正しく選択できるか、という問題がある。

4 CLIX 実験の概要

本章では現在準備が進められている CLIX 実験の概要を説明する。CLIX は財団法人札幌エレクトロニクスセンター^{†8}の事業として実験を行っており、CLIX サーバの運用実験を CLIX 研究会が行う予定である。

今回の CLIX 実験での接続方式は、接続する ISP の数が少ないため割り当てアドレス Multihome 方式を用いることにする。

CLIX サーバは札幌エレクトロニクスセンターに設置され、接続する ISP は、札幌エレクトロニクスセンターが現在接続している OCN^{†9} (1.5M) 及び IJ^{†10} (128K), TokyoNet^{†11} (128K) を予定している。

4.1 実験用 CLIX マシンのスペック

CLIX 実験で使用するサーバマシンは、sunny soft 社^{†12}製の表1のようなスペックを持つラックマウント PC である。この PC は Byte benchmark test で70を超える性能をもち、PC を用いたインターネットサーバとしては最高速

† 8 URL: <http://www.sec.or.jp/>

† 9 URL: <http://www.ocn.ad.jp/>

† 10 URL: <http://www.ij.ad.jp/>

† 11 URL: <http://www.TokyoNet.ad.jp/>

† 12 URL: <http://www.sunny.co.jp/>

表1 CLIX サーバハードウェア諸元

CPU	PentiumII/400MHz x 2
Mem	SDRAM CAS Latency 2clock(8ns) 128MB DIMM x 4 (Total 512MB)
MB	Intel 440BX 100MHz FSB
CDROM	ATAPI x8 speed
SCSI	UltraWide x 3ch / PCI
NIC	10/100Mbps x 4ch / PCI 10Mbps x 2ch / ISA (NE2000 Compatible)
Video	AGP 4MB
HDD	9GB UltraWide SCSI x 7 (1 spare drive included)
RAIDctrl	UltraWide SCSI x 3ch, 64MB cache mem, Hotswap available
HDDcase	4U Rack mount, Dual Power Unit, with Hot swap tray x 2 Chassis
CPUcase	4U Rack mount, ATX form
Rack	EIA 20U Height, with AC Fan x 3 and Front door(70W x 100H x 80D)
Weight	Approx. 150Kg
CRT	9" Monochrome
K/B	Japanese Mini Keyboard

の範疇に入る。この他に、CLIX サーバでのトラフィック等を可視化して表示するためのPCが加わる。

4.2 実験用 CLIX のソフトウェア

CLIX 実験で使用するサーバマシンの代表的なソフトウェアを、表2に示す。これは、PC上でFreeなUNIXを動作させてネットワークサーバを運用する場合のほぼ標準的なソフトウェア構成である。

4.3 CLIX の実験予定

現在CLIXサーバの組み立てが終わり、ISPとの回線が開通するのをまっ

表2 CLIX サーバソフトウェア(主なもの)

Operating System	FreeBSD 2.2.7R MaxProc 660, MaxFDs 8192 IP forwarding off ipfw on
sendmail	sendmail-8.9.1
inetd	xinetd-2.2.1
ssh	ssh-1.2.26
www server	Apache 1.3.3
proxy server	Squid 2.1
MRTG	MRTG 2.5.4c

て実験を開始する状況にある。

当初は www の proxy & cache としての動作を行うが、順次他のサービスも組み込んでいく。

現在考えているサービスは、

- www mirror
- anonymous ftp
- www active cache
- stream 系サービスの reflector
- ICP を使った squid の協調動作

等である。

また、個人が読む情報（電子メールや NetNews）の中に書かれた URL の情報を前もって集めて、個人が実際にその情報をアクセスする前に URL を pre cache しておくという切り口を proxy サービスに組み込むことも行う予定である。

5 ま と め

「実時間通信に必要なものは3つある。帯域幅、帯域幅、そして帯域幅だ」というのは、インターネットについてよく言われることである。

実時間通信のみならず、帯域幅が広がればある程度の問題は解決がされるであろう。しかし、帯域幅を広げるにはコストがかかるため、当面 CLIX 的サービスの需要は存在する。

本論文では CLIX によって複数の ISP と接続を行う場合に起こり得る問題点を指摘し、それを避けるためにはどのようにすべきかについて述べ、そして現在進行している CLIX 実験についての概略を説明した。

実験を通じて CLIX でのサービスをどのようにしていけばいいかを考察し、改めて報告する予定である。

また平成14年の義務教育へのコンピュータの導入に伴って、教育現場に有害なコンテンツを持ち込まないようにする、いわゆる kid's mode と呼ばれるフィルターの導入が要請されており、学校側に対する proxy サービスを含めた CLIX with kid's mode が必要となるので、その実現に向けた取り組みも行っていきたい。

謝 辞

日頃から御討論、貴重な御意見を頂いている CLIX 研究会のメンバー諸氏に感謝する。

参 考 文 献

- [1] J. Postel, *Internet Protocol*, **RFC791**, Sep., 1981.
- [2] T. Berners-Lee, L. Masinter & M. McCahill, *Uniform Resource Locators (URL)*, **RFC1738**, Dec., 1994.
- [3] Y. Rekhter & T. Li, *A Border Gateway Protocol 4 (BGP-4)*, **RFC1771**, Mar., 1995.
- [4] V. Fuller, T. Li, J. Yu, & K. Varadhan, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*, **RFC1591**, Sep., 1993.
- [5] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot & E. Lear, *Address Allocation for Private Internets*, **RFC1918**, Feb., 1996.
- [6] P.V. Mockapetris, *Domain names - concepts and facilities*, **RFC1034**, Nov., 1987.
- [7] P.V. Mockapetris, *Domain names - implementation and specification*, **RFC1035**, Nov., 1987.
- [8] J. Postel, *Transmission Control Protocol*, **RFC793**, Sep., 1981.
- [9] J. Postel, *Internet Control Message Protocol*, **RFC792**, Sep., 1981.
- [10] Paul Vixil, *Non-BGP Multihoming for Web Hosts*, North American Network Operators' Group February 1997 Meeting Notes,
URL:<http://www.academ.com/nanog/feb1997/multihoming.html>, Feb., 1997.
- [11] J. Postel, *User Datagram Protocol*, **RFC768**, Aug., 1980.

