

インターネット上での到達性の計測

インターネット上での到達性は、コントロールプレーンやデータプレーンでの計測によって確認できます。ただし、この2つの計測結果には、default経路の利用などによる差異が存在しています。ここでは、コントロールプレーンとデータプレーンの計測結果で差異が生じる理由とともに、より正確な到達性の計測方法としてdual probingによる方法を説明します。

3.1 はじめに

まず、経路制御に関する話題で頻繁に登場する、AS (Autonomous System: 自律システム)とBGP(Border Gateway Protocol)とは何かを簡単に復習しておきます。ASは、単一の管理主体によって単一の経路制御ポリシーの元で管理され運用される範囲のことです。図-1に示すように、通常は1つのASが1つのISPを表しています。ただし、1つのASが2つ以上のISPに属していたり、逆に1つのISPが2つ以上のASを持っていることもあります。また、ASには、AS番号という32ビットの数値が割り当てられています。このAS番号を使ってISPを呼ぶこともあります。たとえば、IJJのAS番号は“AS2497”ですので、IJJをAS2497と呼ぶこともあります。AS間で経路情報を交換するときには、BGP (Border Gateway Protocol)というプロトコルが使われます。各ASには、IPアドレスの一番左の桁からNビット分が共通であるアドレスのブロックが割り当てられています。これをアドレスプレフィックス、または単にプレフィックスと呼びます。BGPでは、それぞれのASが持つアドレスプレフィックスへの到達性に関する情報が交換されます。また、各ASの共通部分であるNビッ

トをプレフィックスの長さと言います。アドレスプレフィックスの長さだけに着目するときには、/Nのプレフィックスなどと表すことがあります。

インターネットでの最も基本的なサービスは、任意の2点間での到達性の提供です。しかし、私たちは、この基本的なサービスの状況を正確に把握できているとは言い難い状態です。研究者やオペレーターは、BGPのルーティング情報を調べたり(コントロールプレーンでの計測)、pingやtracerouteなどのツールを使い実際の到達性を調べたり(データプレーンでの計測)して、このサービスの状況を把握しようとしています。

ここでは、このどちらもがインターネット全体の到達性を把握するには不十分であることを示し、それを補って計測を実施しインターネットでの到達性の状況を把握する方法を示します。なお、本稿は、IJJ特別研究員のRandy Bushと、O. Maennel氏、M. Roughan氏、S. Uhlig氏が共同で実施した調査結果を日本語で解説したものです。ここで示す調査の詳細については、2009年11月ACM SIGCOMM IMC (Internet Measurement Conference)に発表された論文[1]を参照してください。

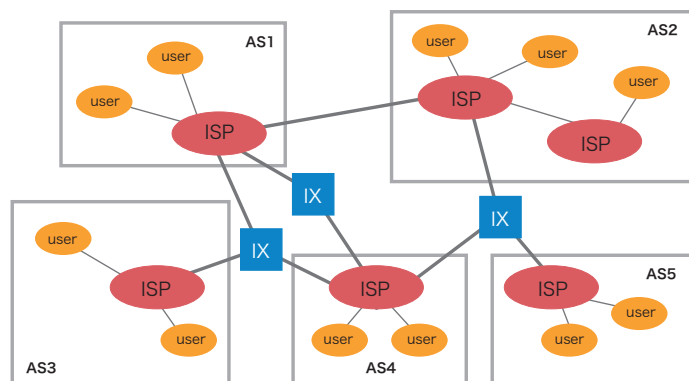


図-1 ASの概要

3.2 /25はどこまで伝搬するのか

ほとんどのプロバイダは、/24より長いプレフィックスの経路情報をフィルタによって受け取らないようにしています。これは、経路情報の処理に費やすリソースの節約や、経路の乗っ取り防止のためです。まず、このようなフィルタが実際にどの程度普及しているかを確かめてみました。

2008年6月22日にAS3130から/25のプレフィックスをアナウンスし、それがどこまで伝搬されたかをコントロールプレーンとデータプレーンの両方で計測しました。このとき、この/25を含む経路情報は、他には存在していませんでした。結果は、コントロールプレーンでの計測結果とデータプレーンでの計測結果がかなり食い違うものになりました。これは、データプレーンでの到達性を調べるときに、コントロールプレーンを調べるだけでは不十分であることを示唆しています。

コントロールプレーンでの到達性の確認は、RouteViewsやRIPE/RISといったBGPの経路モニタを参照して行いました。この結果、11個のASに/25への経路情報が伝搬されていることが確認できました。これは、/25がフィルタによって止められ遠くまで伝搬されないだろうという、私たちが予想したとおりの結果でした。

一方、データプレーンでの到達性の確認は、/25に含まれるIPアドレスをソースIPアドレスとして、インターネット上のさまざまな場所に割り当てられている多数のIPアドレスに対してpingを実行することで行いました。pingへの応答があれば、pingした相手先のIPアド

レスからこの/25のネットワークへの経路が存在していることとなります。これに対して、応答がないときには、pingした相手先ホストがダウンしているか、相手先ホストから/25に対する経路が確立されていないかは区別できません。このため、ここでは、応答があったときのみを考慮することにしました。

私たちの予想に反して、結果は、1,024個ものASがこの/25への到達性を持っていました。これは、実験を行ったときの全AS数の5%に相当します。インターネット全体において、この割合は大きなものではありませんが、コントロールプレーンであるBGPの経路情報を調べた結果と比べると非常に大きな数字です。

さらに、BGP経路モニタによると、/25に対する経路情報を持っていたASは、AS3130からASホップ数で2ホップ以内であることも分かりました*1。つまり、2つ隣のASまでしか届かなかったという事です。ホップ数ごとのAS数の分布を、図-2に実線で示します。経路情報をアナウンスしたAS3130は2つの1次プロバイダに接続されており、この/25はそこからさらに1ホップ先までしか伝搬しなかったため、インターネットの中心部にしか伝わらなかったこととなります。

また、pingに回答したIPアドレスまでのASホップ数をtracerouteで測定した結果を、図-2に破線(青色)で示します。こちらは、以前に/20のプレフィックスでの到達性を調べたときの結果(図-2での赤色の破線)とほとんど変わりません。データプレーンでの計測結果は、BGP経路モニタでの結果(最大2ホップ)に比べて、より遠くのAS(最大4ホップ)から/25に到達可能であることを示しています

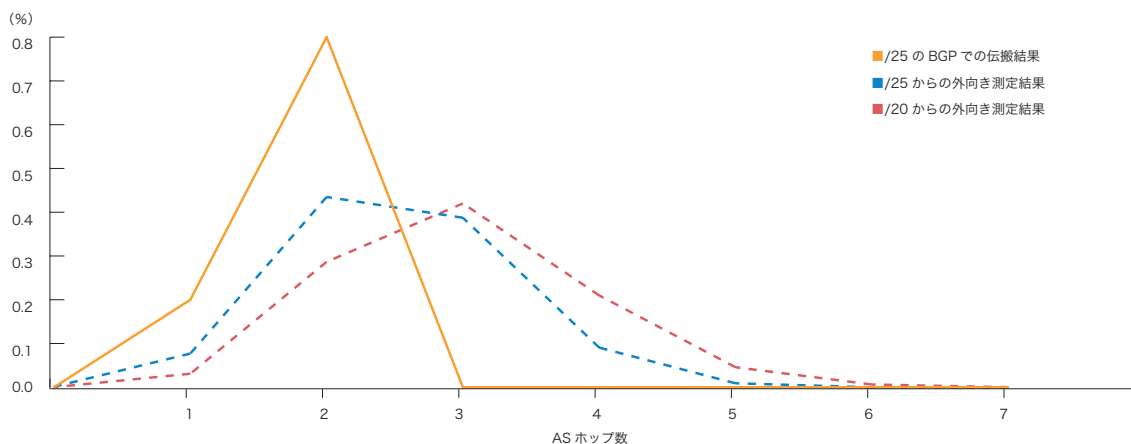


図-2 /25へのASホップ数分布

*1 本稿では、論文[1]とはホップ数の数え方を変えて、3.3.2節でのホップ数の数え方に統一した。

このような結果から、コントロールプレーンでの計測結果とデータプレーンでの計測結果に食い違いがあることが分かります。ただし、実際のパケットはデータプレーンで運ばれるため、データプレーンでの計測結果が優先されるべきでしょう。

では、なぜ、このような食い違いが生じるのでしょうか。考えられる理由には、次の2つがあります。

- コントロールプレーンにおいて、BGP経路モニターは観測不能なサイトにも経路情報が届いていた
- default経路によって、/25の経路情報がなくても到達可能なASが存在した

データプレーンで到達可能だったASの75%がいわゆるスタブAS*2でした。スタブASではdefault経路が使われる可能性が高いと考えられるため、次にdefault経路に関して調べてみることにしました。

3.3 default経路の利用状況

ここでは、ASパスボイズニングという手法でdefault経路がどの程度使われているかを調べてみます。図-3に示すように、AS3130内の計測用マシンから上位の1次プロバイダに対して、いくつかの実験用プレフィックスに対する経路情報をアナウンスします。ただし、計測対象のASにはこの経路情報が伝搬しないようにするために、ASパスに、計測対象のAS番号を付加した上でアナウンスします。

たとえば、AS2が計測対象のASであったときには、“3130 2 3130”というASパスを持つ経路情報をアナウンスします。AS2がこの経路情報を受け取ると、自分のAS番号である“2”がすでにASパスに含まれているので、ループ回避のためにこの経路情報の受け取りを拒否します。このようにすることで、AS2がdefault経

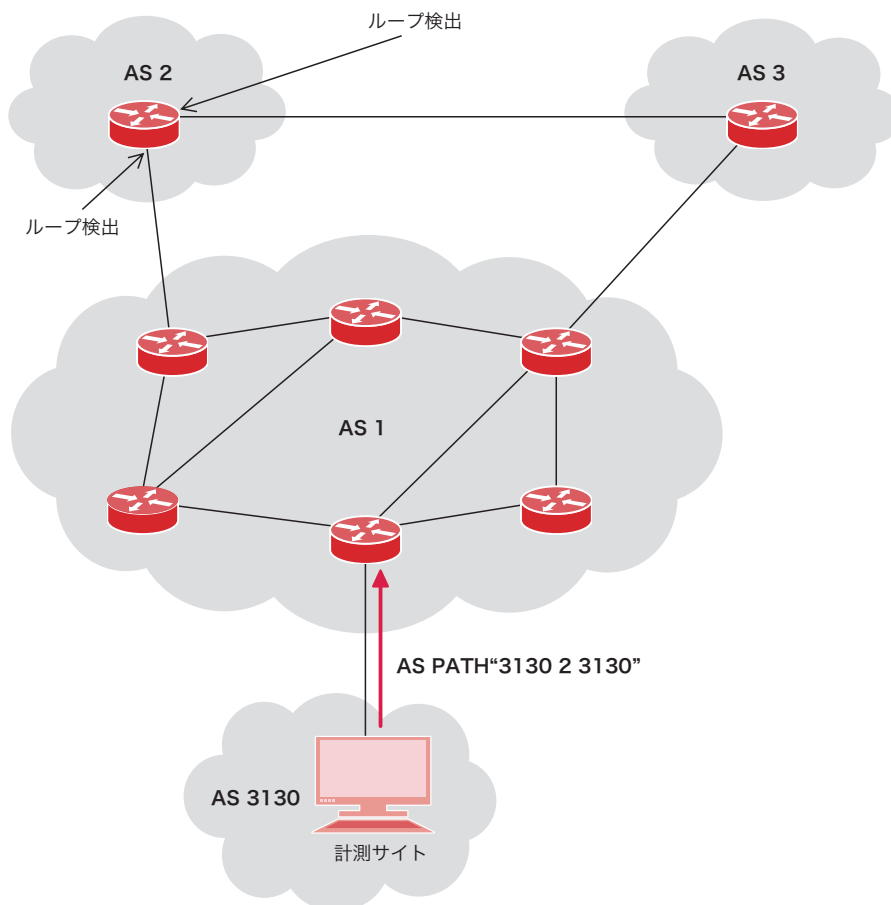


図-3 ASパスボイズニング

*2 他のAS同士の通信を中継しないASをスタブASと呼ばれる。一方で、他のAS同士の通信を中継するASはトランジットASと呼ばれる。

路を持っていない限り、こちらの実験用プレフィックスに含まれるIPアドレスに到達できない状況を作ることができます。これをASパスポイズニングと呼びます。この方法によって、2009年4月18日～5月1日の13日間に、25,780個のASでのdefault経路の利用状況を調査しました。実験用プレフィックスには98.128.0.0/16を/24に分割して用い、次の順序で、インターネット上の広範囲に対して並行して調査を実施しました。

1. ポイズニングしていないプレフィックスのアドレスから調査対象のASが到達できる状態であることを事前に確認します
2. 次に、実験用プレフィックスのアナウンスを止め、フラップダンピングの影響が消えるまで1.5時間待ちます
3. そして、相手先ASのAS番号を付加した実験用プレフィックスをアナウンスし、経路情報が伝搬するまで20分間待ちます
4. 実験用プレフィックス内のIPアドレスから、調査対象ASのIPアドレスリストに対してpingを送り調査を開始します

通常、1回の調査に、およそ2～3時間を要します。これを並列して行うことで、多くのASを調査しました。また、調査期間中、実験用プレフィックス以外のアドレスから調査対象ASにpingを送り続け、到達可能な状態が継続していることも確認しました。この結果、99.2%のASが継続的に到達可能な状態でした。

結果は、調査した全IPアドレスリスト中の64%がASパスポイズニングの実施後も到達可能でした。同一のASで複数のIPアドレスをテストしましたので、AS単位では74.8% (19,291個)のASがパスポイズニング実施後も到達可能でした。つまり、多くのASでdefault経路が

用いられているということです。

残りのうち20.9% (5,381個)のASからは、まったく応答がありませんでした。また、4.3% (1,108個)のASからは、アドレスによって応答があったりなかったりしました。事前調査段階から到達不能なASも少数ですが0.7%ありました。これは、おそらくbogonフィルタの影響だと思われます。

今回は、応答がない場合は、そのASでdefault経路を使用していないと解釈しました。しかし、AS内のすべてのアドレスでdefault経路を使用していないかどうかはわかりませんので、この解釈は若干不正確かもしれません。また、応答があったりなかったりする場合は、相手先ASで複雑なネットワーク運用を行っていることが考えられます。たとえば、あるASでは、BGPの経路ではdefault経路を採用していないが、IP-TVやVoIPサービスのために一部のルータに手動でdefault経路を書き込んでいるそうです。このように統一されていないポリシーで運用されているASがあることも判明しました。興味深い点としては、default経路の使用に文化的な差異があったことです。ある調査では、日本のASの60%がdefault経路を使用しておらず、36%が使用し、4%が混在しているという結果が出たそうです。

今回の調査結果は、Webサイトで公開し、調査対象のASからのフィードバックを受け付けました。回答がくれた191個のASのうち、94%が今回の調査結果が正しいことを確認してくれました。また、pingを送ったIPアドレスリストのアドレスが、そのASから他のASに委譲されたアドレスブロックに属している場合もありました。驚くべきことに、自分たちがdefault経路を使用していることを知らなかったAS管理者もいました。これは、たとえば、上位プロバイダから流れてくるdefault経路をフィルタ処理せずに受け取っていたなどの理由によるものです。

3.3.1 ASのタイプによる変化

直観的には、トランジットサービスを提供しているASのほうがスタブASよりもdefault経路の使用率が低そうです。今回の調査結果をこの観点からも分析してみました。ここでは、ASの分類は、参考文献[2]の分類に従って行いました。

表-1 ASカテゴリ別のdefault利用率分布

	調査数	Defaultあり	Defaultなし	混在
スタブ	24,224	77.1%	19.3%	3.6%
小ISP	1,307	44.5%	42.2%	13.3%
大ISP	246	17.1%	60.6%	22.3%

表-1に示すように、スタブ、小ISP、大ISPに移るに従って、default経路の利用率が下がっています。また、自AS内でのdefault経路の利用あり/なしが混在しているケースは、ISPが大きくなるに従って増えています。これは、ISPが大きくなるほど運用が複雑になっていることを表しています。ただし、大きなASになるほど、今回の調査でpingを送ったIPアドレスの個数も増えるため、この点も考慮して結果を解釈する必要があります。

図-4は、今回の調査結果を他のASとのpeerの数の分布で表したものです。少なくとも100個のASとpeerを持つまでは、default経路の利用が減少していくことが分かります。また、20個以下のpeerしか持たないASの80%がdefault経路に依存していますし、300個以上のpeerを持つASでは、default経路を使っているものが15%以下になります。

ASのタイプによってdefault経路の利用率が異なるという調査結果は、非常に興味深いものです。たとえば、スタブASでtracerouteを用いる場合、最初の数ホップは相手への明示的な経路情報がなくてもdefault経路によって進んでいけるが、大きなISPに到達したところでdefault経路が無くなり、そこで止まってしまう場合があるという事です。しかし、これは、tracerouteが止まった地点に問題があったことを示しているわけではありません。そこまでtracerouteが実行できたこと自体が、コントロールプレーンの情報から得た到達性と食い違っているということで、コントロールプレーンでの計測かデータプレーンでの計測のどちらか一方のみでは不十分であるということを示しています。

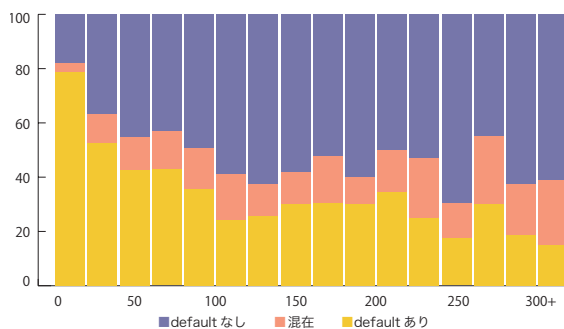


図-4 ASのpeer数ごとのdefault利用率

3.3.2 default経路の影響

default経路の存在がインターネットの計測に対して与える影響を考察するために、参考文献[2]にあるASトポロジーデータを用いたシミュレーションを行いました。シミュレーションでは、今回の測定結果でのdefault経路利用確率を用いて、トポロジーデータ内のスタブASの77.1%、小ISPの44.5%、大ISPの17.1%にそれぞれdefault経路を持たせました。なお、混在のケースはdefault経路なしに含めました。また、default経路を持たせる際にどのASに経路を向けるのかを決める方法として、ここでは2つの方法を採用しました。1つはそのASの上位プロバイダからランダムに選ぶ方法(ランダム選択)、もう1つはそのASの上位プロバイダのうち最も顧客数の多いASを選ぶ方法(max選択)です。

シミュレーションでは、1,000個のASを任意に選び、それらからdefault経路のみを使っていくつのASに到達できるかを計算しました。

シミュレーションした結果、default経路のみでは、わずかな数のASにしか到達できませんでした。インターネットの全体構造が比較的フラットなものであるため、スタブASからdefault経路によって上位に移っても、1～3ホップ程度でdefault経路を持たない1次プロバイダに到達して、そこで止まってしまうからです。default経路のみで到達できるAS数は、最大でも5でした。

ここで、自分のプレフィックスに関する経路情報のアナウンスが、1ホップ先の自分の上位プロバイダのみに伝搬し、そこから先のASには伝搬しないようなケー

スを想定してみます。

図-5は、任意のASから到達可能なAS数の累積分布の補分布(Complementary Cumulative Distribution Function)を示しています。このグラフを見ると、default経路で経路を向けるASをmax選択で選んだ場合、約半数のASが1,000個のASに到達でき、3分の1のASが2,000個のASに到達できることが分かります。また、ランダム選択の場合でも、到達先は減りますが、それでも非常に多くのASに到達可能です。

さらに、図-5には、経路情報のアナウンスが自分から2ホップ先のASまで伝搬すると想定したときの結果も示してあります。この場合、到達可能な範囲は広がり、およそ半数のASが6,000個のASに到達できます。最大で19,000個のASに到達可能な場合もありました。

実際には、3.2の/25の到達性で考察したように、単純なホップカウントのみでなく、各ASが持っている経路フィルタの状況なども考慮しなければなりません。しかし、このシミュレーションにより、/25の経路情報であっても、自分の上位プロバイダにさえ伝搬すれば、そこから先のASにはほとんど経路情報が届いていない状況であっても、インターネットのかなり広い範囲に到達可能になることが解ります。そして、ここでの結果が、コントロールプレーンでの計測では到達できないはずなのに、データプレーンでの計測では到達できてしまうという現象をうまく説明していると考えられます。

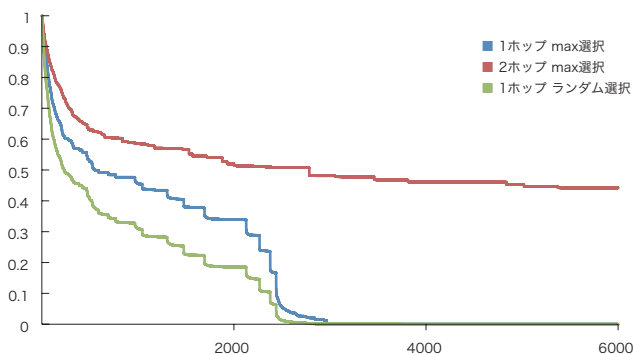


図-5 到達可能なAS数の分布

3.4 dual probingによる到達性の検査

default経路の存在は、コントロールプレーンの観測による予測に限界があることを示しています。コントロールプレーンでの計測のみで何らかの議論を行うときには、この点に注意すべきです。一方、今回の調査で用いてきたデータプレーンでの計測にも限界があります。相手先のホストや経路上に設置された機器などの振る舞いがさまざまに変化する状況下では、pingの結果を解釈することさえ難しい状況が簡単に起こります。到達性の計測が難しい理由は、次の2つの側面を考慮しなければならないためです。

- 自分から世界がどのように見えるのか
- 世界から自分がどのように見えるのか

前者は、ルータがルーティングプロトコルから得る情報に基づいたものになります。到達性の問題を解決するときにはオペレータが知りたい情報は後者のものです。つまり、インターネットの他の部分から自分のネットワークがどのように見えているかということです。しかし、残念ながら、この情報を直接得る方法はネットワーク層に用意されていません。

BGPモニタのようなサービス、looking glassやtracerouteサーバなどを用いれば、外からの見え方を知ることは可能です。しかし、それらは、一部のASのみが公開しているサービスであり、このようなサービスから見えるものをすべて集めても、結局はインターネットの一部からの見え方しか解らないのです。

また、このようなサービスを公開しているASは一般的に大きなISPであり、結果はインターネットの中心部からの見え方に偏ったものになります。たとえば、このような中心に近いISPは、スタブISPに比べると良好な到達性を保っているため、スタブISPの到達性を検証するには役に立ちません。したがって、インターネット全体のさまざまな視点から到達性を検証できる方法が必要になります。

ここでは、dual probingという、より広範囲な状況に適用可能なデータプレーンでの調査方法を提案します。

あるネットワーク管理者が外のホストから自分のネットワークへの到達性を確認したいとします。単純な方法として、インターネットの広い部分をカバーするIPアドレス群を選び、それらに対してpingを送る方法があります。それらのIPアドレスからpingへの応答があれば、そのIPアドレスの場所からpingを送り出したマシンへの到達性があることになります。この方法を「外向き調査 (out-probe)」と呼びます。

図-6に、外向き調査の考え方を示します。この図に示す黒色の実線は、従来からの方法であり、公開されているlooking glassなどから試験するサイトに向かって内向きに調査する方法です。一方、外向き調査では、緑色の破線で示すように、到達性を試験するネットワークから、広範囲に分布する外のサイトに向かってpingなどで調査パケットを送付します。この際、パケットのソースIPアドレスには試験するアドレス空間に属するIPアドレスを設定します。この場合、到達性があることは、pingを送った相手から自サイトへ応答が戻ってくることで確認できます。

pingに応答がなかったときには、次の理由が考えられます。

- IPアドレスを持つホストがpingに答えなかった
- IPアドレスを持つホストに到達する前に、ファイアウォールなどでpingパケットが落とされた
- IPアドレスを持つホストはpingに応答したが、応答が返ってくる途中で廃棄された
- IPアドレスを持つホストからpingを送り出したホストへの経路が確立されていなかった

3番目と4番目の理由がネットワークの到達性に関連しています。ただし、ICMPのパケットはTCP等の他のパケットに比べて優先度が低いため、3番目の理由に到達性がないことの証拠にするには弱いかもしれません。いずれにせよ、応答がなかったことだけでは情報として不十分だと言えます。

では、あらかじめどのような結果になるかが想定できているときはどうでしょうか。「3.3 default経路の利

用状況」で事前調査を行った後に実際の調査を行ったように、想定される結果に対して実際の調査結果がどのようであったかを比較することで有益な情報を得ることができます。つまり、調査を2回に分けることで、2回目の調査結果をより深く解釈できるのです。また、調査の回数を分けるだけでなく、pingを送る相手のIPアドレスを複数用いることなども可能です。この方法を「dual probing」と呼ぶことにします。ただし、「dual」と言っても、この方法には3つ以上の調査を含めることも可能です。

dual probingでは、実験用プレフィックスからの調査結果と、基準プレフィックスからの調査結果を比較します。基準プレフィックスには、以前から利用し、非常に良好な到達性を持つことが確認できているプレ

フィックスを選びます。この比較によって、実験用プレフィックスのみの調査に比べて、より深く状況を理解できるようになります。仮に、基準プレフィックスからのpingに応答がなかったときには、実験用プレフィックスから調査する必要はありませんし、どちらに対しても応答があったときには到達性に問題がないことが分かります。また、基準プレフィックスには応答があったが、実験用プレフィックスに応答がなかったときには、pingの送り先のIPアドレスから当該サイトまでのどこかに到達性に関する問題があることが分かります。ICMPの優先度の問題でパケットが落とされている可能性は残りますが、何回か計測を繰り返すことで結論を得られるはずで

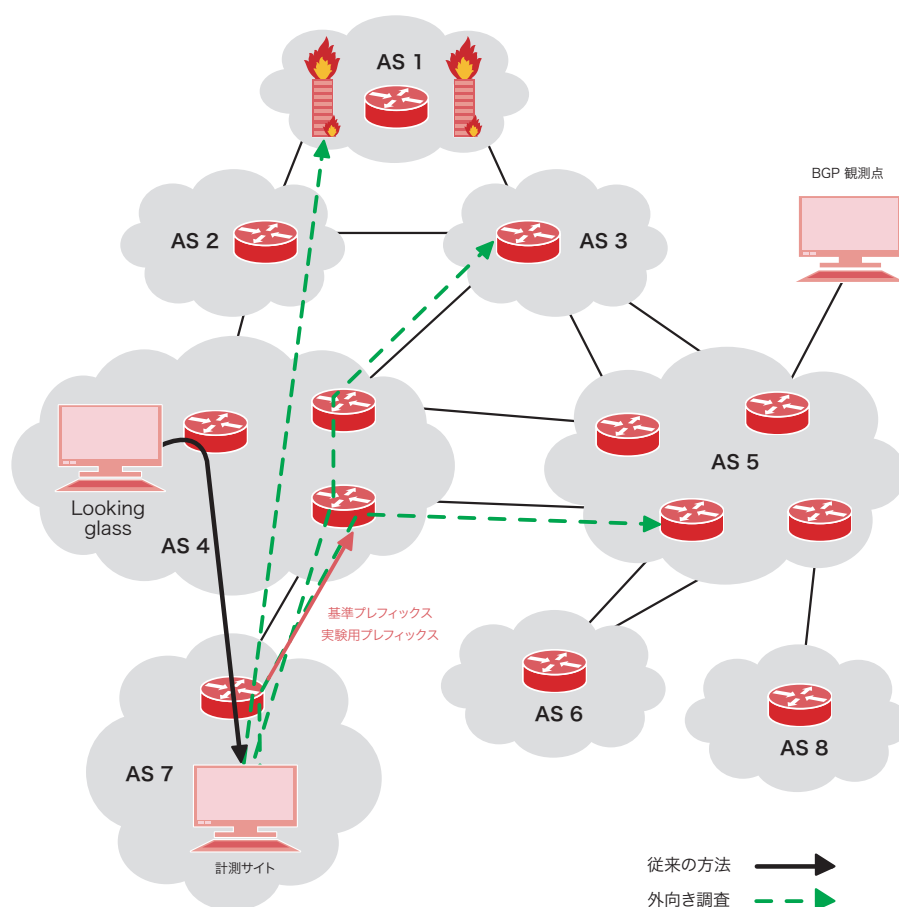


図-6 Dual Probingの考え方

3.4.1 間違ったbogonフィルタの検出

bogonとは、間違った経路情報アナウンスのことです。bogonは、何かの事故によって発生したり、アドレス空間のハイジャックを狙って意図的に送られたりします。したがって、ISPは流されるはずのない経路情報に対して実際にパケット転送が起らないようにするために、コントロールプレーンかデータプレーンにフィルタを設定しています。通常行われる方法は、まだレジストリからISPに割り振られていないプレフィックスからのトラフィックや経路アナウンスを拒絶するためにフィルタを設定する方法です。ただし、この場合、プレフィックスが割り振られ正当な経路アナウンスが始まっても、フィルタの設定が変更されず、そのプレフィックスへの到達性に問題が起こることがあります。従来の方法では、この間違ったbogonフィルタがどこにあるかを検出することが困難でした。今回、dual probingを応用して、間違ったbogonフィルタを検出する実験を行いました。

実験のために、新たに173.0.0.0/16と174.128.0.0/16をARINから割り振ってもらいました。今回、このアドレス空間に属する5つの小さな実験用プレフィックスを5か所からアナウンスしました。PSGNet(米国、シアトル)、Verio(米国、アッシュバーン)、SpaceNet(ドイツ、ミュンヘン)、CityLink(ニュージーランド、ウェ

リントン)、そしてIJ(日本、東京)の5か所です。各ISPに実験用ホストを設置し、ISPが通常利用しているIPアドレスを割り当て、そのIPアドレスを基準アドレスとしました。そして、実験用プレフィックスから実験用IPアドレスを選び、実験用ホストの同じインターフェースにセカンダリーアドレスとして設定しました。

実験は、2008年4月14日、2008年5月27日、2008年6月12日の3つの時期に、それぞれ1週間程度の期間で行いました。1回目の実験は、実験用プレフィックスが割り振られたことをARINが公表する前に行いました。つまり、1回目の実験の目的は、正当なbogonフィルタがどの程度採用されているかを確認することでした。1回目の実験の後に、ARINが新たなプレフィックスを割り振ったので、bogonフィルタ用リストから外すべきであること、が公表されました。そして、私たちは、1回目の実験でフィルタを設定していたASの担当者宛に、フィルタを解除するように電子メールで依頼しました。したがって、2回目の実験で到達性が得られなかったとすると、大きな問題です。3回目の実験は、時間の経過とともに到達性に関する問題がどのように変化するかを観察するためのものでした。

また、到達性に関する問題を正確に把握するため、今回の実験では、基準アドレスに5回以上の応答があるにもかかわらず実験アドレスに1回も応答がないときに

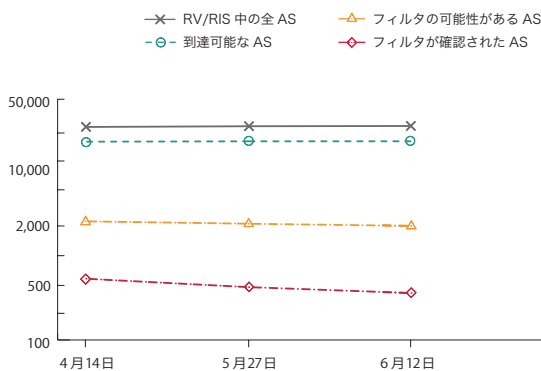


図-7 bogonフィルタ検出実験

限って、到達性に問題があると結論づけることにしました。実験アドレスに1回も応答がなくても基準アドレスへの応答が5回未満であったときには、問題の「可能性がある」とするにとどめました。

図-7に、実験の結果を示します。ここで、黒色の実線が全ASを表しています。また、緑色の破線が問題のなかったASです。bogonフィルタの設置が確認されたASは、赤色の破線で示した、およそ500個でした。また、黄色の破線で示した2,000個近くのASにもフィルタが設定されているようでした。

この実験結果から、インターネット全体の2～7%のASで、新たに割り当てられたアドレスが見えなかったこととなります。また、2回目と3回目の実験で、到達性の問題がほとんど改善されていないことも分かります。これは大きな問題です。

図-8は、フィルタの設定が確認されたASと、フィルタがある可能性のあるASの分布を、ASのタイプ別に示しています。この図では、ほとんどがスタブASであり、インターネットの外縁部で問題が発生していることを表しています。ただし、トランジットASに問題があるにもかかわらず、スタブASに問題があると誤解することもあるため、この点には注意が必要です。

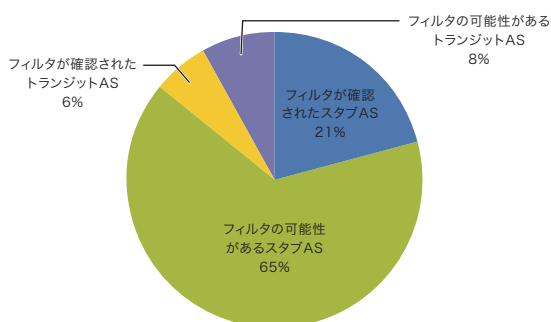


図-8 ASタイプ別分布

3.5 計測結果の確からしさに影響する項目

ここまで、コントロールプレーンからの計測が到達性の状況を正しく表していないこと、そして、データプレーンでの計測によってそれを補えること、を示してきました。しかし、データプレーンでの計測にも限界があります。ここでは、データプレーンでの計測で考慮すべき課題を3つの観点から簡単にまとめます。

3.5.1 トポロジー上でカバーする範囲

外向き計測の実施目的は、BGPモニタやlooking glassではカバーしきれない範囲をカバーすることです。つまり、インターネットの中心部でなく外縁部からの到達性を見ることです。このためには、「3.4 dual probingによる到達性の検査」で用いたようなインターネット全体をカバーするIPアドレスリストを作成することが重要です。このアドレスリストには、広範囲をカバーし、AS内部で統一されていない設定パラメータなども調査できるものであることと、必要最小限の個数であることが要求されます。作成するIPアドレスリストの質によって、実際の計測の質が左右されます。

3.5.2 IPアドレスとAS番号のマッピング

IPアドレスが属するASを決めることも重要な課題です。これには、BGPのルーティングテーブルを参照するなどの方法が採られます。しかし、たとえば、トランジットプロバイダが顧客のプロバイダを接続する際に、自分のASに割り振られたアドレスブロックからIPアドレスを提供することがあります。このとき、この顧客ASのボーダーにあるルータがbogonフィルタ等によって特定のプレフィックスへの到達性を持っていない場合であっても、上位プロバイダからの到達性がないと判断してしまう可能性があります。

また、IPアドレスとAS番号の正しい対応表を作った後には、そのメンテナンスも重要です。たとえば、私たちが2007年に作った対応表と、2009年に作った対応表を見比べてみると、同じASに対応するプレフィックスは88%しかありませんでした。IPアドレスとAS番号の対応に誤りがあると、観測結果の解釈を間違えてしまいます。

3.5.3 どの計測ツールを使うか

データプレーンでの計測に用いるツールの選び方も重要です。pingを使うのか、tracerouteを使うのか。また、pingを使うにしても、ICMP、UDP、TCPなど、どのタイプのパケットを用いるかも大切な選択です。今回の調査を実施する際に分かったことは、ICMPでは約70%のIPアドレスに到達可能でしたが、UDPではわずか30%にしか到達できませんでした。これは、ファイアウォールやNATによってフィルタされてしまうためです。TCPでは、さらに状況が悪化し、たった5%しか到達できませんでした。

参考文献

- [1] R. Bush, O. Maennel, M. Roughan, S. Uhlig, "Internet Optometry: Assessing the Broken Glasses in Internet Reachability", ACM SIGCOMM IMC, 2009.
- [2] R.Oliveria, B. Zhang, "IRL - Internet Topology Collection," 2009.

執筆者:

浅羽 登志也(あさば としや)

株式会社IIJノベーションインスティテュート代表取締役社長。1992年、IIJの設立とともに入社し、バックボーンの構築、経路制御、国内外ISPとの相互接続等に従事。1999年取締役、2004年より取締役副社長として技術開発部門を統括。2008年6月に株式会社IIJノベーションインスティテュートを設立、同代表取締役社長に就任。

3.6 結論

ここでは、インターネットでの実際の到達性を知ることが、公開されているBGPサーバなどのデータで見るとははるかに複雑なものであり、コントロールプレーンで得られる情報とデータプレーンで得られる情報に食い違いがあることを示しました。また、default経路の使用によって、経路情報が伝搬しないときにもパケットの到達性が提供されることも示しました。さらに、経路情報のボイズニングやdual probingといった到達性を検証するための新たな方法も提案しました。IIJでは、インターネットが安全で安定した社会基盤として機能するよう、自社のバックボーンの安定運用に努めるとともに、本稿で示したような、インターネット全体の安定運用に関する調査と情報発信を継続してまいります。