インターネットの幸せのために
フィルタリングしよう！

[ブロードバンドルータ開発の立場から]

2005年1月21日

ＮＥＣアクセステクニカ
アクセスネットワーク技術部
松浦　利光
川島　正伸

Empowered by Innovation NEC

はじめに

JPCERT/CC 戸田さんの発表では、
主要ISPにおいても本来実施すべきFilterが
なかなか実施されていないという状況について
報告いただきました。

ならば、最もユーザに近いブロードバンドルータ
の部分で何か対処できる事はないかという観点で
発表したいと思います。

目次

- ブロードバンドルータにおける
  セキュリティ機能の必要性
- パケットフィルタリング有無による性能への影響
- NAT/NAPTによる二重苦！？
- ISPとのフィルタ協調動作について

ブロードバンドルータにおけるセキュリティ機能の必要性

DoS Attackや分散型ステルススキャンなどで、
IPアドレスが詐称されたパケットが使用されているが、
ブロードバンドルータでは、Ingress/Egress共にフィルタ
されていない(事が多い。。。)
→明らかに不正なパケットをフィルタ(RFC3330など参考に)
　する事でインターネットの健全化に貢献

ゾンビPCがDDoSやspamの温床となっているが、
エンドユーザは自分が加害者になっている事を認識していない
→ルータで意図的に止めれば、ISPもユーザもHappy！？

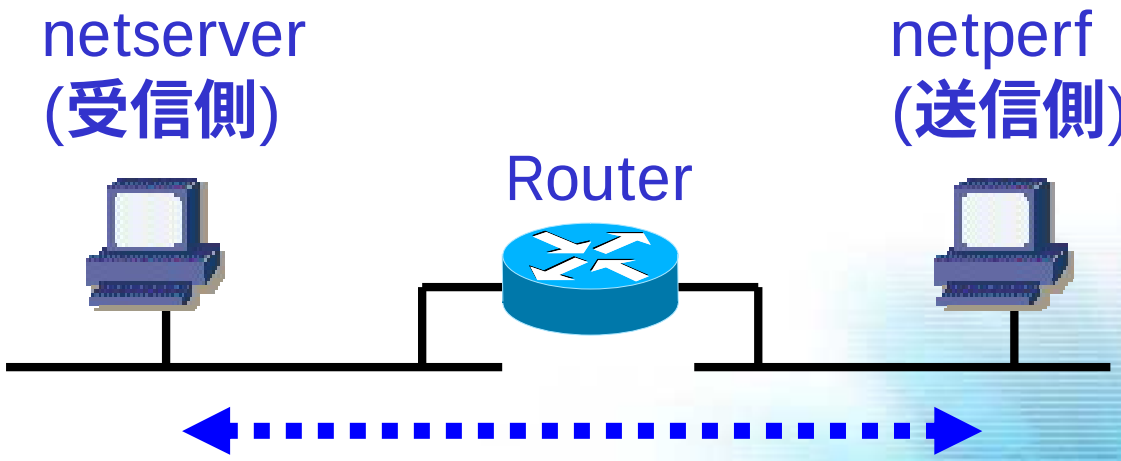
エンドユーザ任せじゃ、もう無理だよね～
ブロードバンドルータで対処可能な範囲ってあるかな。

Empowered by Innovation NEC

パケットフィルタ有無による性能への影響

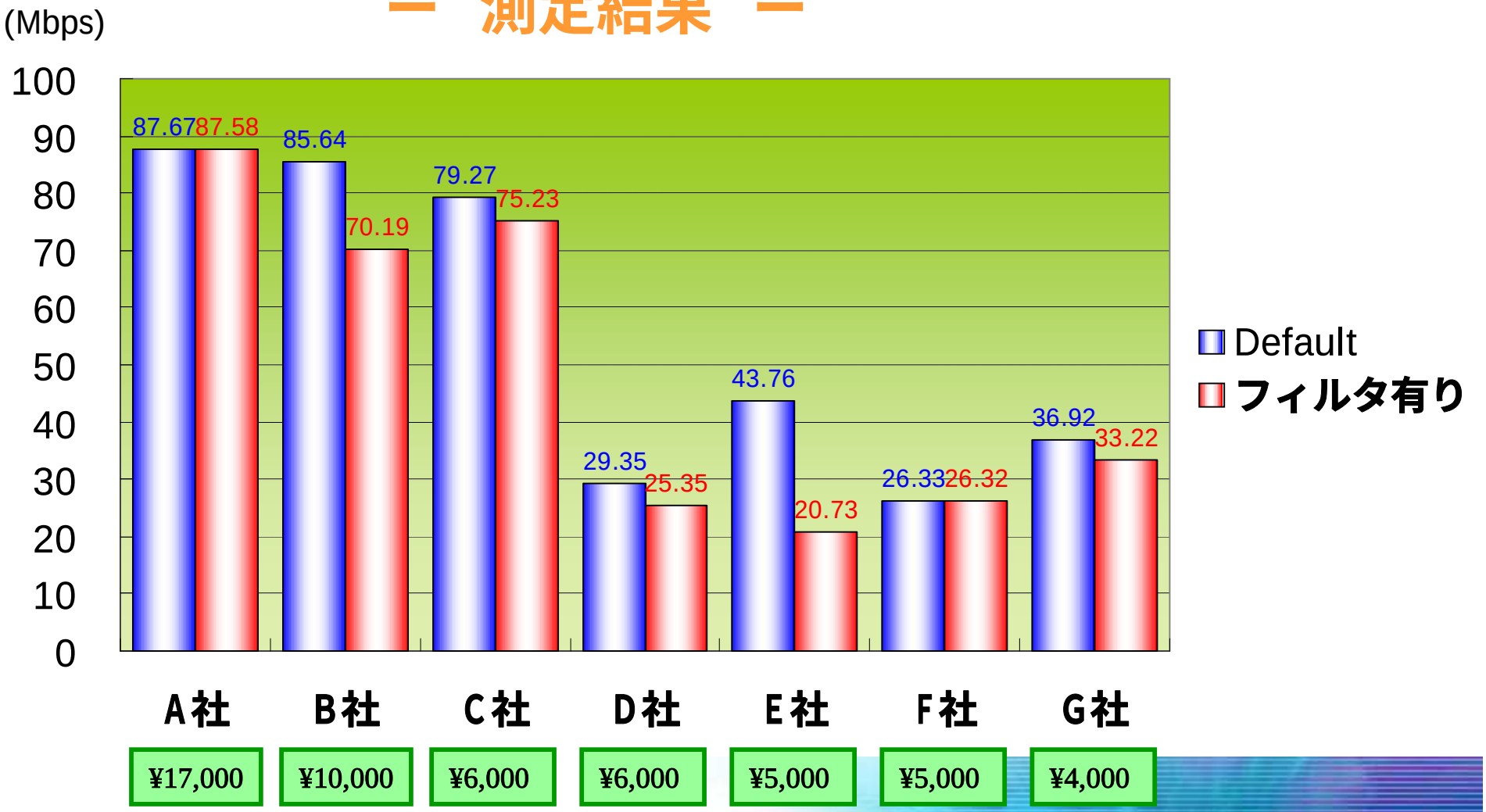
まずは、フィルタかけてみて性能低下するか調べてみよう！

Netperfを利用したIPv4 TCP Streamにて測定を実施
(Filter内容はあまり重要視せず、性能の観点で調査)



パケットフィルタ有無による性能への影響

ー　測定結果　ー



パケットフィルタ有無による性能への影響

＜わかったこと＞

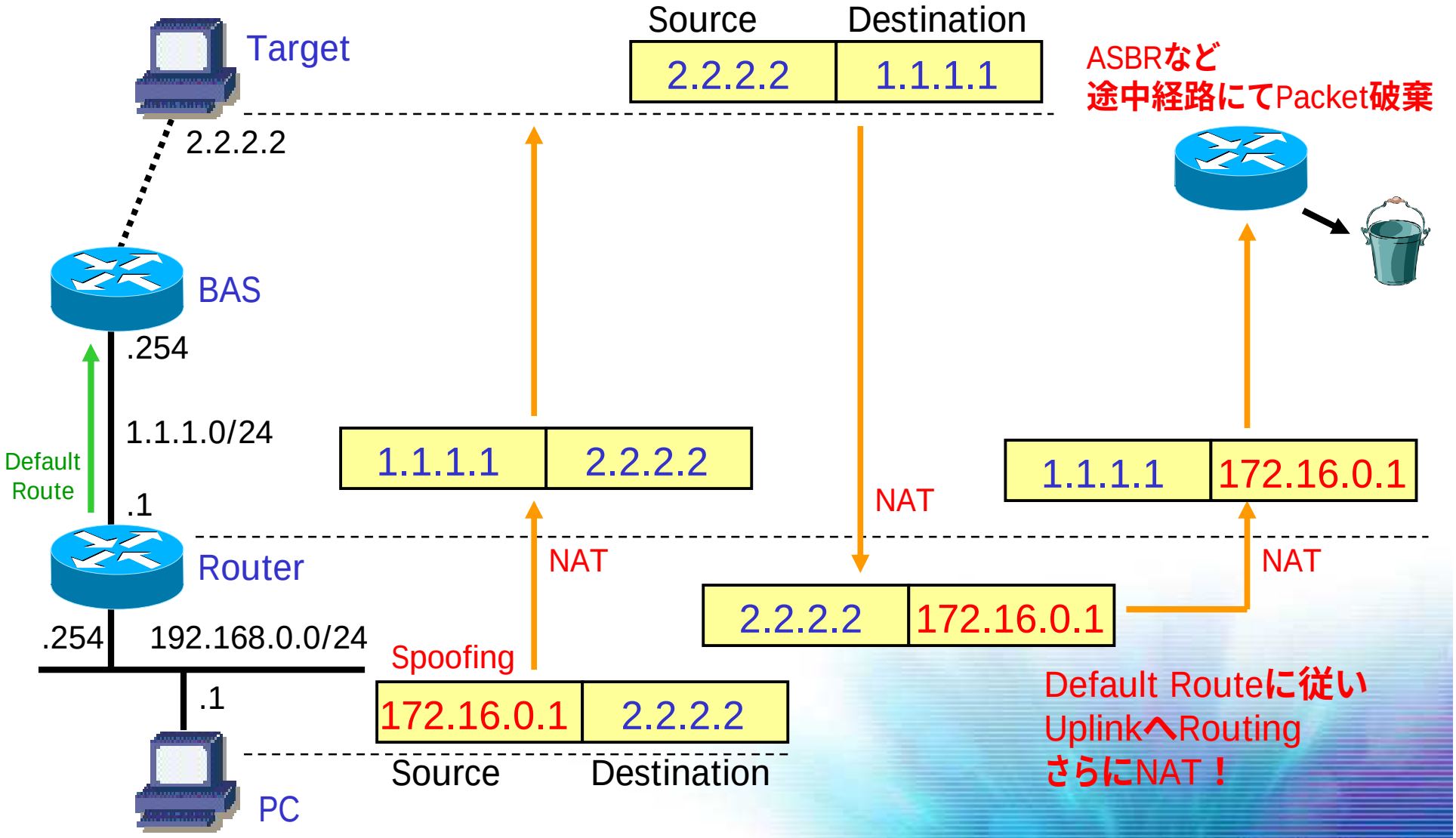
・カタログ通りの性能が出ない。。。まぁこれは当然か。

・安価なルータは、フィルタすると少なからず性能低下する。
→製品によっては、50%以上も性能低下している。
→25番ポートブロックやコンテンツフィルタなど
上位Layerを覗くのは、荷が重いかも。。。

・そもそも送信元アドレスをサブネット指定でフィルタ
できなかったりする。。。(T_T

・送信元アドレスを詐称しても、NAT/NAPTしてくれる。(:p

NAT/NAPTによる二重苦！？



NAT/NAPTによる二重苦！？

＜わかったこと＞

・送信元アドレスが詐称されたSYN Flood攻撃などが
実施された場合、攻撃対象からのSYN ACKは
さらにNAT/NAPT変換され、ゴミパケットとして
ISP内で破棄される。
→1つのPacketで2度も迷惑。。。(1粒で2度まずい。)

・ブロードバンドルータでも、最低限のフィルタを
できるようにしよう！
→ゆくゆくは、uRPFも実装しちゃう？(なぁんてね)(^^

ISPとのフィルタ協調動作について

ISPとフィルタの協調動作をするのもいいけど、
方式等について標準化されていないと
各社の要求仕様ごとに機能実装しないといけないから
かなりしんどいよぉ。。。でもそこが腕の見せ所！？

みんなで仕組み考えようか！

あっ、某社のSMFが特許になってるよ。。。(T_T