Chapter-2
Filtering Technique

「Filtering Techinique」と言っても

- いろいろな話があるかと
  - 経路フィルタ
  - パケットフィルタ
  - ログやメールのフィルタなんてのも該当
- 今日はその中でも「ICMPv6」のフィルタについて議論したいと思います
  - さらにパケットを中継するノードを中心に考えましょう
- ※一部玄人さんには当たり前の話ですが復習ってことで御願いします

まずはそもそも・・・

- 中継ノードでICMPをフィルタするモチベーション
- pingやtracerouteに中継ノードが応答したくないってのが基本かと
- 全く応答したくない訳ではないが、負荷の問題があるので制限をかけるとかもあり
- ってことで、ルータ宛は全部フィルタしちゃえってことなのかと

しかし！！

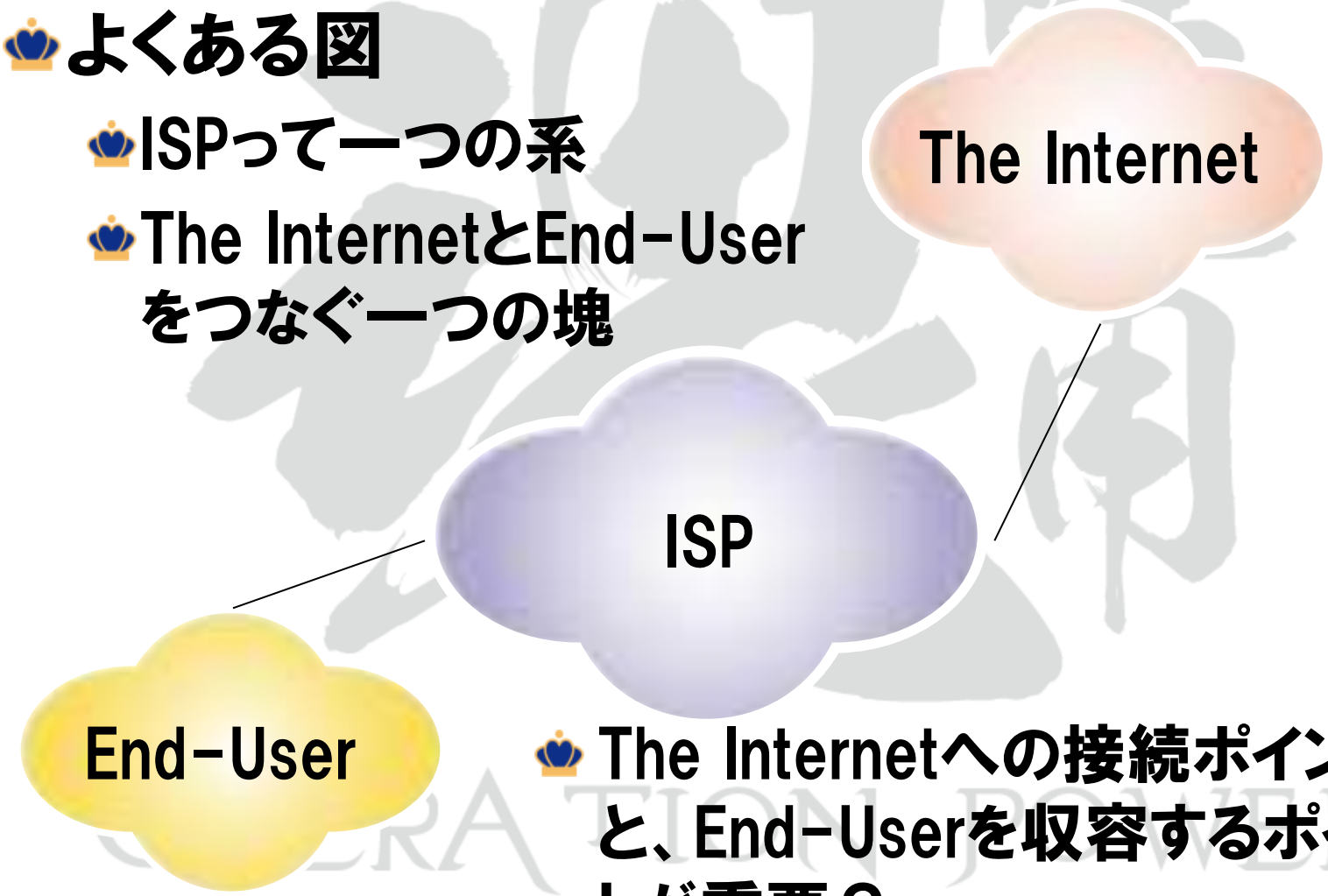
- 「もともとICMPはInternet Control Message Protocolと言うくらいで、**通信に際して非常に重要な役割**を果たしている(べき)もの 」by 許さん
  - 参照：[janog:08946]
- ということで**闇雲に止めておけばいいものではない**はず

さらに・・・

- IPv6におけるICMPv6の役割はさらに重要なものになっています
  - 細かい話は [janog:08906] から始まる一連のスレッド参照
- ようは、隣の機器と通信するためには**確実にNeighbor Discoveryは必要！！**
- さらに中継ノードでのfragmentが許可されないIPv6では**Path MTU discoveryがちゃんと動かないと何処でパケットを落とされるかわからない！！**
- さらにさらに、**他にも通しておくべきものはあるはず！！！**

ISPのネットワークを一つの系と捕らえると

- よくある図
  - ISPって一つの系
  - The InternetとEnd-User をつなぐ一つの塊

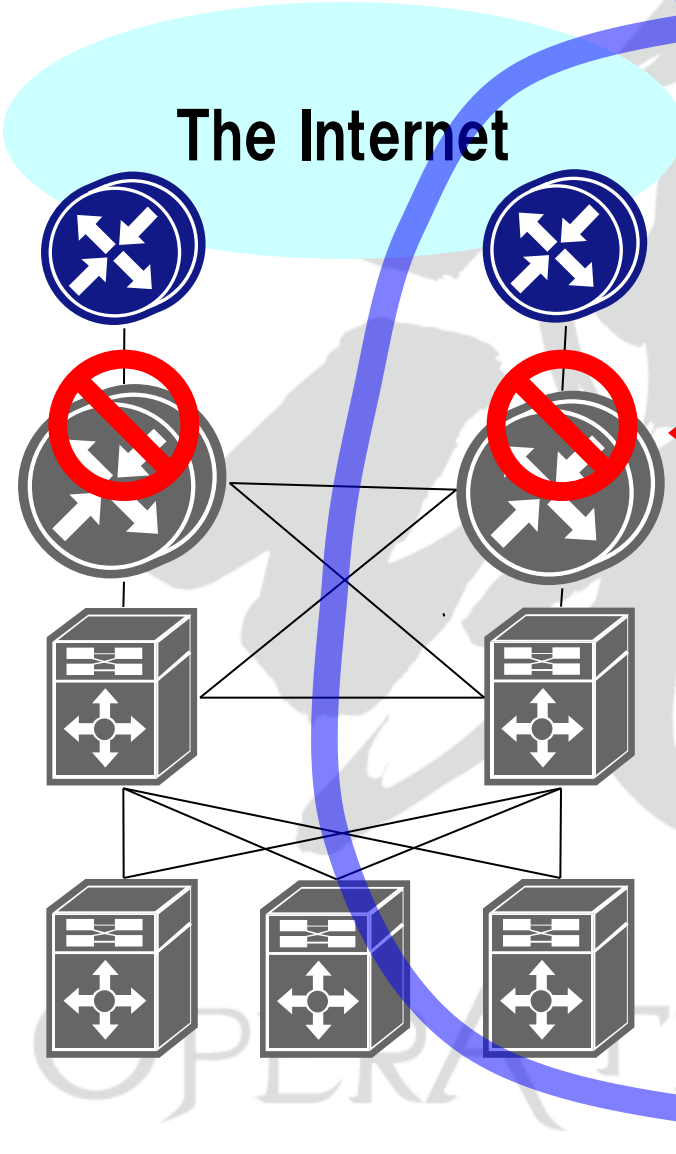


- The Internetへの接続ポイントと、End-Userを収容するポイントが重要？

守るべきものに対して何をすべきか？

- 先のスライドに書いたとおり、雲を構成する一つ一つの機器を守りたいはず
- ということは、The Internet(というか外部のネットワーク)との境界で制限するのは、自網の通信機器だけ
- で、**止めたいものと通すべきものを考えると止めたいものが多い**はず
- だったら答えは明白！
- **外部との接続ポイントで、「自網機器」向けの「止めたいもの」だけ止めればよい！！**
  - あくまでも守りたい時だけです
- いわゆる**Infrastructure ACL!!!!**

こんな感じ



インフラ機器を通過するICMPv6の通信には関与しない

ここで、内部の全てのリンクと機器に設定したloopbackアドレスに対してのFilterを設定する

内部リンクって多くない？
Loopbackを/128で設定していく？

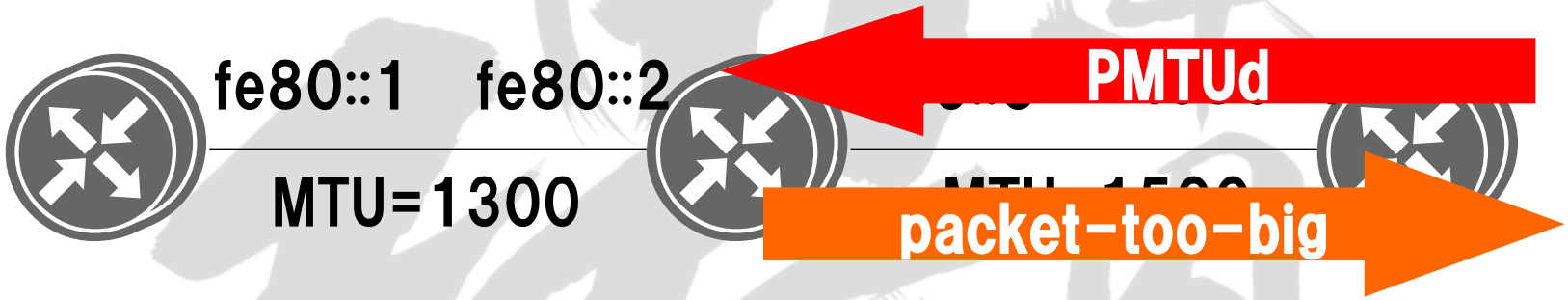
⇒アドレス設計をしっかりしてまとめて設定できるようにするとよい！

系の中の中間ノードは？

- 外部境界で守られていると思えば、特に何もしなくてもよいかもしれない
  - と思ったけど、filter設定するんなら中間ノードでもしますよね
- さらに、本気で外部から隠蔽したいのでLink-Localアドレスだけで構成する可能性もある
- ただし、**ノードにGlobal Unicast IPv6アドレスが全く設定されていない場合**、**外部からのPMTUdを止めてしまう！！**
  - ここは [janog:08912] 石田さんと [janog:08913] 松崎さん

こんな感じ

- Linkは全てLink-Localアドレスのみ
- Loopbackも設定せず



- MTUの小さいリンクがあった場合・・・
- ICMPv6のエラーメッセージを返すためのアドレスは？
  - Link-Localになる(しかない)はず
- 設定していたとしても相手が知らないアドレスだったらどうなる？
  - Link-Localは隣接しか知らないし・・・

外部網との接続ポイントでのフィルタ

- **自社網に設定したGlobal Unicast Address**(各Link/Loopback)に対して**外部網から通信させたくないものだけfilter**する
  - 中間ノードでも外部網へ返答する可能性があることを踏まえ、**必ず一つはGlobal Unicast Addressを設定**する(**そのアドレスを広告する**)
  - ※また、全てのノードについて、隣接機器とのLinkはGlobal Unicast Addressを設定せずLink-Local Addressだけ設定してもパケットを転送することは可能だが、Linkの死活監視がそれぞれの機器からしかできなくなるというデメリットがあることを忘れない

自社のユーザーからは？

- 自網機器へのpingとかtracerouteは止めなくてもよいのでは？
- となると、End-Userを収容するIFでICMPv6のフィルタを書く必要はあるのか？
- 何か設定しておいた方がいいもの・いいことってありますか？
  - uRPFかなぁ・・・IPv6でちゃんと動くの？

実際に設定すると・・・

- よくある話ですが、access-listやfirewall-ruleってのには「**暗黙のdeny/permit**」ってのがあったりする
  - なかには、暗黙のrate-limitもある？
- これに頼ってしまうとよくない
- 当初の設計をちゃんと引き継いでいければいいが、**どこかのタイミングで何故このfilterがかかってるのかもめる**ことになるかも。**何でdeny/permitがないの？**って話になりかねない

まとめ

- デフォルトで止めていて必要なものを空けるのではなく、**どうしても許可させたくない通信だけ止める**のがよい
  - 基本的にわからないなら設定しない
- Filterをかける場合、**機器に設定するアドレスを無計画にしておく**とFilterの行数が多くなってしまう等の**デメリット**がある
- 機器によって存在する「**暗黙のpermit/deny等々**」はできれば**明示的に設定して表示される**方がよい
- ま、何だかんだ言って**基本はno-filter**でしょ！

（第3回）
IPv6 オペレーションズフォーラムのご案内

- **日時**
  2010年4月23日（金） 午後半日
- **場所**
  サンケイビル（大手町）
- **概要（案）**
  （1）アップデート （ IETF情報等 ）
  （2）IPv6 技術 / IPv6 地雷セッション（公募?）
  （3）IPv6時代のIPv4
- **主催**
  IPv6オペレーションズフォーラム 実行委員会

IPv6普及・高度化推進協議会

IPv4/IPv6共存WG サービス移行サブWGからのお知らせ

- サービス移行サブWGで作成した「IPv4サーバ環境へのIPv6導入ガイドライン」が昨年の11月に公開されました
- ホスティング事業者等の主にWebサービスを展開する事業者向けにIPv6対応について記載しています
- 以下URLで公開しておりますので御確認くださいませ！！
  http://www.v6pc.jp/jp/entry/wg/2009/11/ipv4ipv6.phtml