IPv4枯渇への対策と
IPv6導入に向けた取り組みについて

NTTコミュニケーションズ株式会社
先端IPアーキテクチャセンタ
ネットワークプロジェクト　コアIPテクノロジ担当
経営企画部　サービス戦略担当（兼務）
担当部長　博士（工学）　宮川　晋
2011年2月

IPv4アドレス枯渇に備えて

IPアドレスは誰が割り当てている？

IANA (Internet Assigned Number Authority)
ここがおおもと

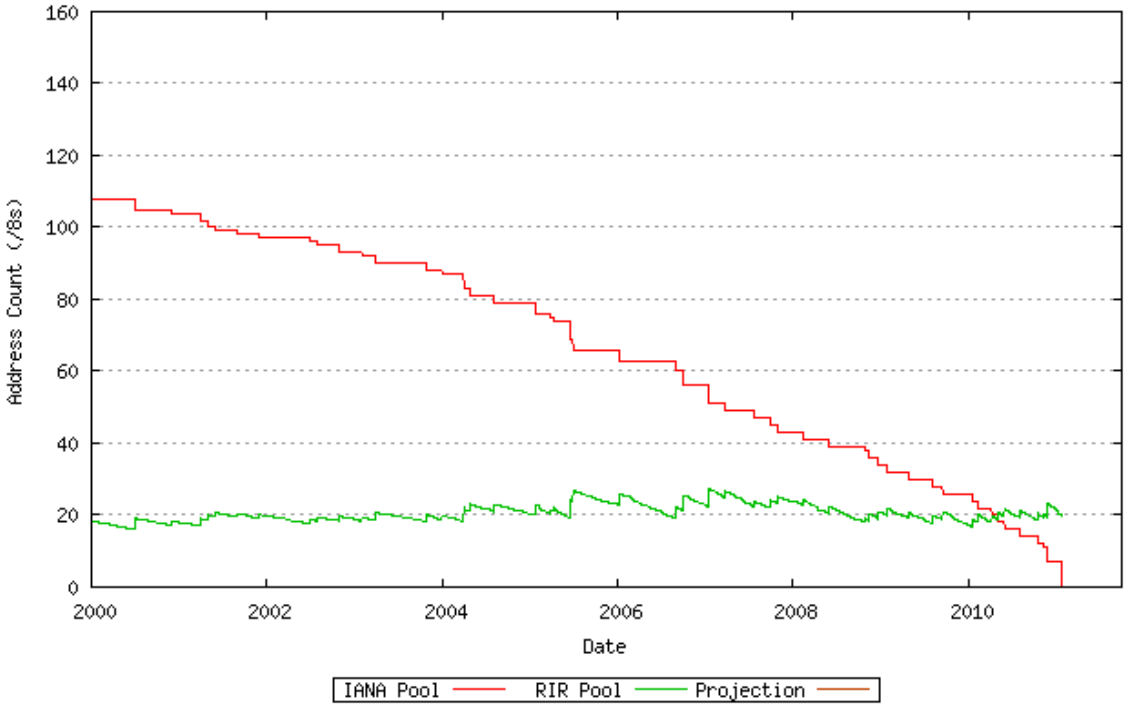
↓

RIR(Regional Internet Registry)
ARIN：北米
RIPE NCC：欧州・中東・中央アジア
APNIC：アジア・太平洋
LACNIC ：ラテンアメリカ・カリブ海
AfriNIC：アフリカ

↓

ISPなど

IPv4アドレスが枯渇します



- http://www.potaroo.net/tools/ipv4/index.html at 27-Jan-2011 07:58 UTC.
- **Projected IANA Unallocated Address Pool Exhaustion: 01-Feb-2011**
  - **一部の方々には「そうはいってもあくまでも推測でしょう？」とおもわれていたのではないかとおもいますが・・・**
  - **この日付どおりにIANA Poolは無くなりました。**
- **Projected RIR Unallocated Address Pool Exhaustion: 02-Oct-2011**
  - **ということは、この日付もかなり信憑性が高い・・・**

二つのことを同時にしなければなりません

1. IPv4の延命

☆　既存の資産を活かせるよう、IPv4を
なんとか使い続けるようにして移行の時間を稼ぐ

☆　といっても、新しいアドレスは無いので
いわば「劣化コピー」で対処する

2. IPv6の導入

☆　128ビット長の広大なアドレス空間をもつ
新しいプロトコルで本質的な対処

☆　無駄があまりでないように
スムースに導入するための工夫する

NTTコミュニケーションズの対策

1．IPv4の延命

☆　Large Scale NATの開発・標準化を世界的にリード。
世界中のベンダーと開発について協議
導入方法について検討し、実機検証中

2．IPv6の導入

☆　1990年代後半からのIPv6基盤研究・実用化を継続的に実施。
世界的にもIPv6の実用化をリード

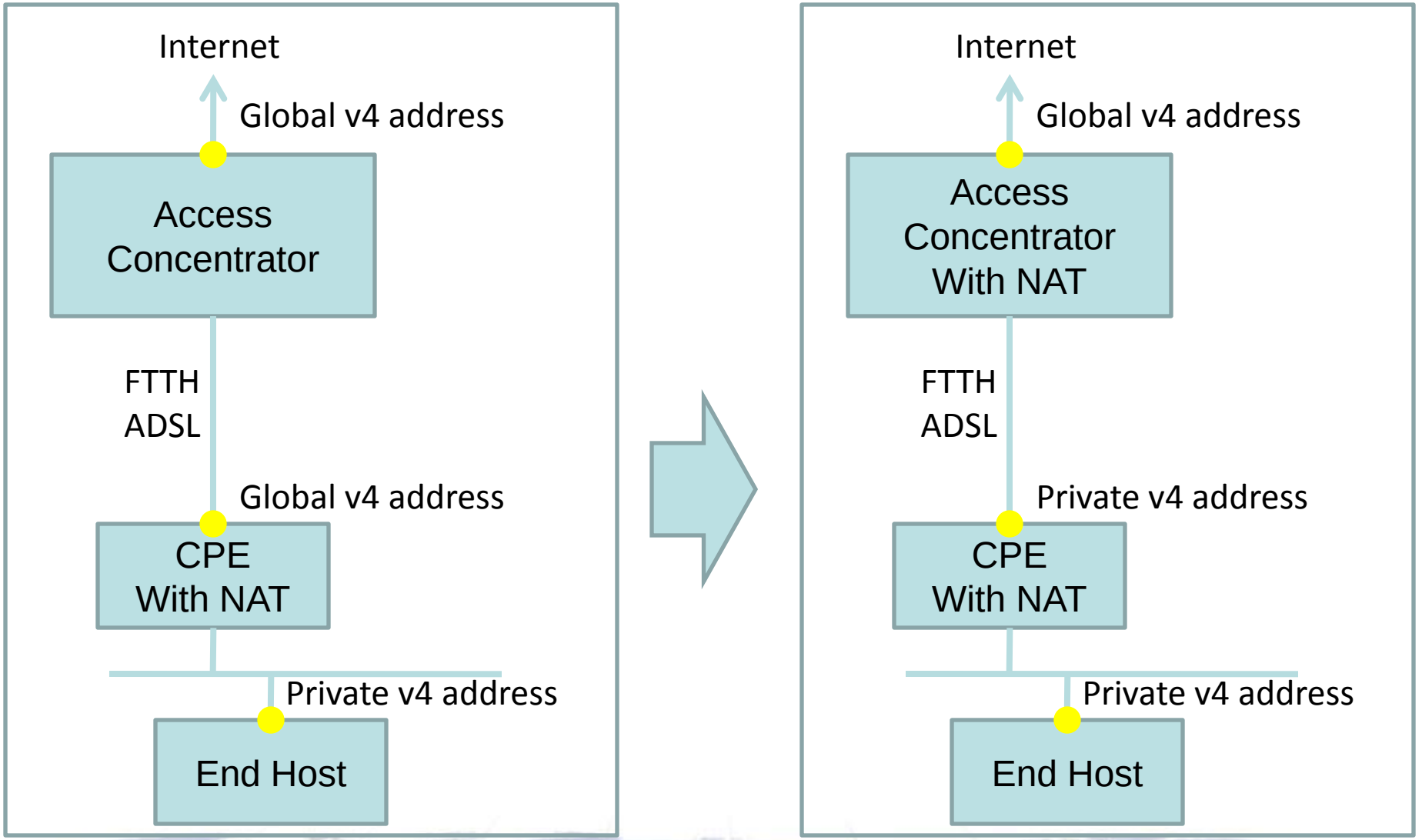
Large Scale NAT　とは？

ISP設備の集約装置側に大規模な
NAT（Network Address Translator)を導入し
グローバルIPv4アドレスを複数のユーザで共有する技術
Carrier Grade NATとも呼ばれる

DS-LITE(Dual Stack Light): LSNの機能をCPEとの間で割り、
それらの間をなんらかのトンネル（基本的にはIPv4 over IPv6）でつなぐ

A+P:アドレスに加えてポートレンジも勘案してルーティングする。CPEは根源的な改造が必要となる
（SAM:　Stateless Address Mappingは、A+Pの一実装方法）

LSNの導入 (NAT444)



しかし、これだけで安心というわけには行かない

v4アドレスを共有するということは、インターネットの
通信のモデルの変更を意味する

あるIPアドレスから集中的に攻撃を受けたことを理由にアクセス制限リスト
（ACL：Access Control List）を書くことにしているとすると、LSN配下から攻撃さ
れると周辺のユーザも同時に制限してしまうことになってしまい副作用が大きい

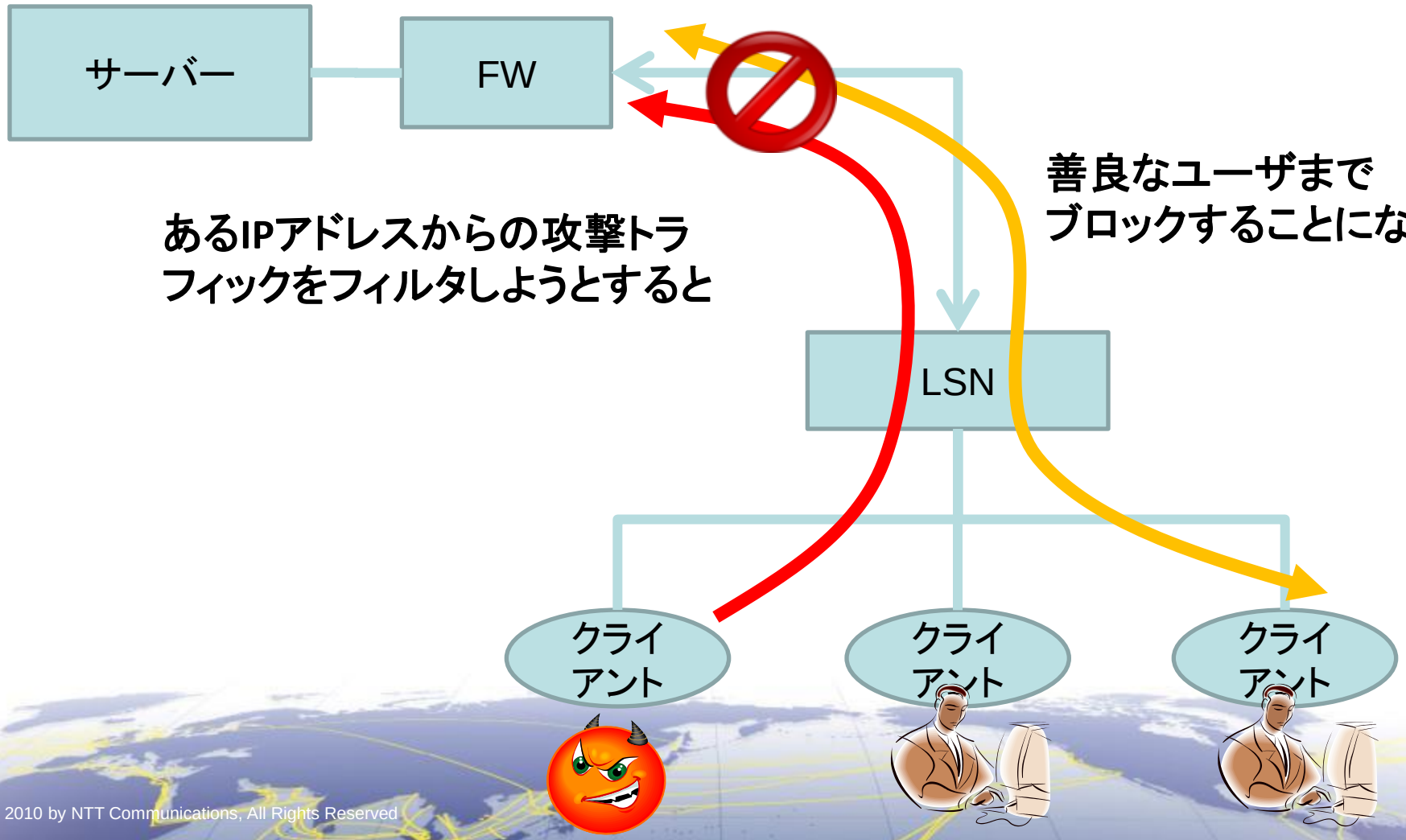
たとえば掲示板への投稿など、サーバへのアクセスは、
「どこのIPアドレスから」だけを記録するだけでは意味が無くなってしまい
「どこのIPアドレスのどのポートから」までを記録しないといけない

SIPの発着信はできるのか？検証しないとわからない

その他、さまざまな影響が考えられる

アドレスでランデブーポイントを決めている
P2Pアプリケーションが動作しなくなる可能性も

アドレスベースのアクセス制限ができない



サーバやFWのセキュリティはどうすればいい？

- IPアドレスを、（色々な意味で）ユーザ識別子として使うことをあきらめる必要がある
  - –別途の認証と組み合わせる必要。せめてクッキーか

- ログはIPアドレスとPort番号の組み合わせで記録する必要がある
  - –特にプロバイダ責任制限法からの要求をクリアするために

- Firewallベンダーに「LSNフレンドリー」な機能を要求することになるが、どういう機能が適切かはまだこれから考えなければいけない
  - –アプリケーションとLSNの組み合わせの検証は現在進行中

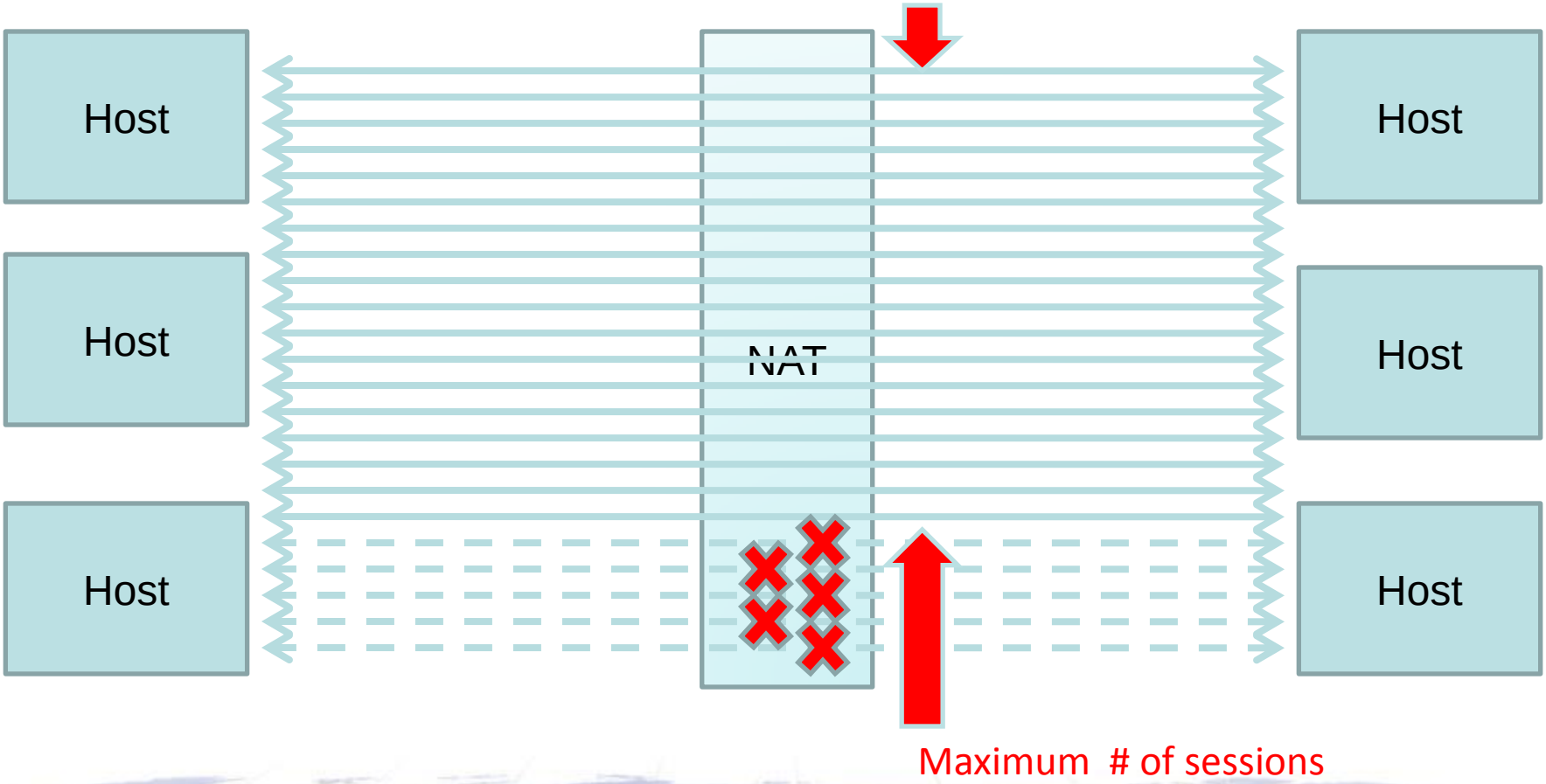
- セキュリティ面だけでなく、セッション数制限など、アプリケーションの効率や速度などにも影響する問題も深刻かも

たとえばメールシステムへの影響

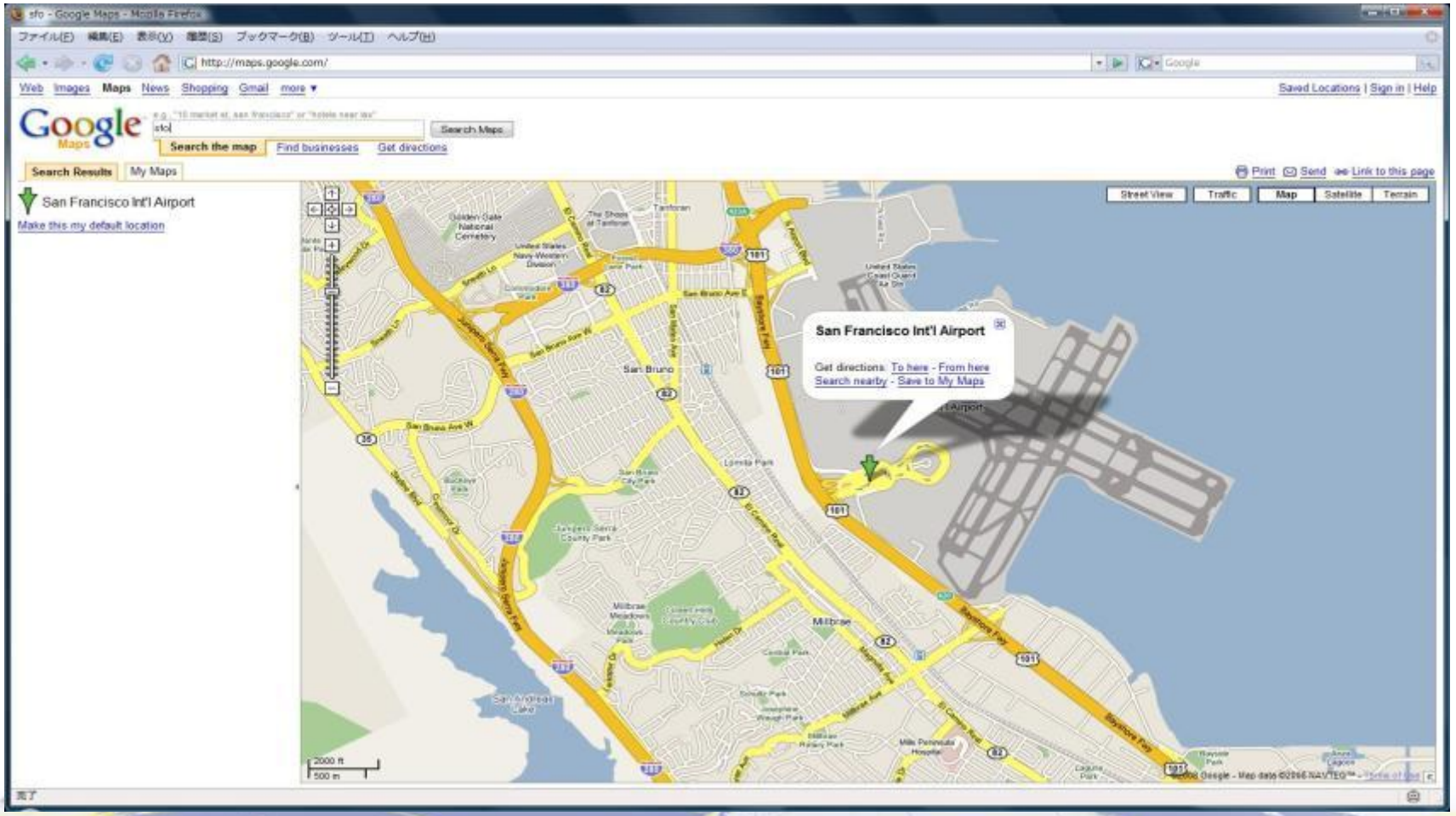
- もちろん、当然、メールシステムに対して多大な影響が出るとおもわれる
- メールクライアントのIPアドレスを逆引きしようとしても、それはLSNのアドレスになってしまうことに注意が必要
  - ISPに対して、LSNの逆引きの設定を推奨していかないといけない
- POP Before SMTPは意味が無くなる
  - Submission（SMTP　Auth)へ移行すべき：これは、まぁ、悪い話ではない
- SPAMが送られてきたときに、そのIPアドレスからのSMTPを一時的にせよ遮断する、というオペレーションは、やってはいけないことになるとおもわれる
  - ってことはRBL　（Realtime Blackhole List）による制限はどうなるのか？
  - 隣のやつがSPAMを送ると、自分までブロックされてしまうのか！？
- DDNS（Dynamic DNS)をつかってサービスを立てることは、（通常の意味では）不可能になる
  - LSN配下にスタティックフォーワードを設定してもらえばいいんですが。。。
  - MXレコードにポート番号まで書けるならいいのかもしれないけど
- とにかくLSN配下からはSPAM打ち放題になってしまわないようにしないといけないけれど、強すぎる制限は、ユーザからのクレームを招くだろう

セッション数制限の話

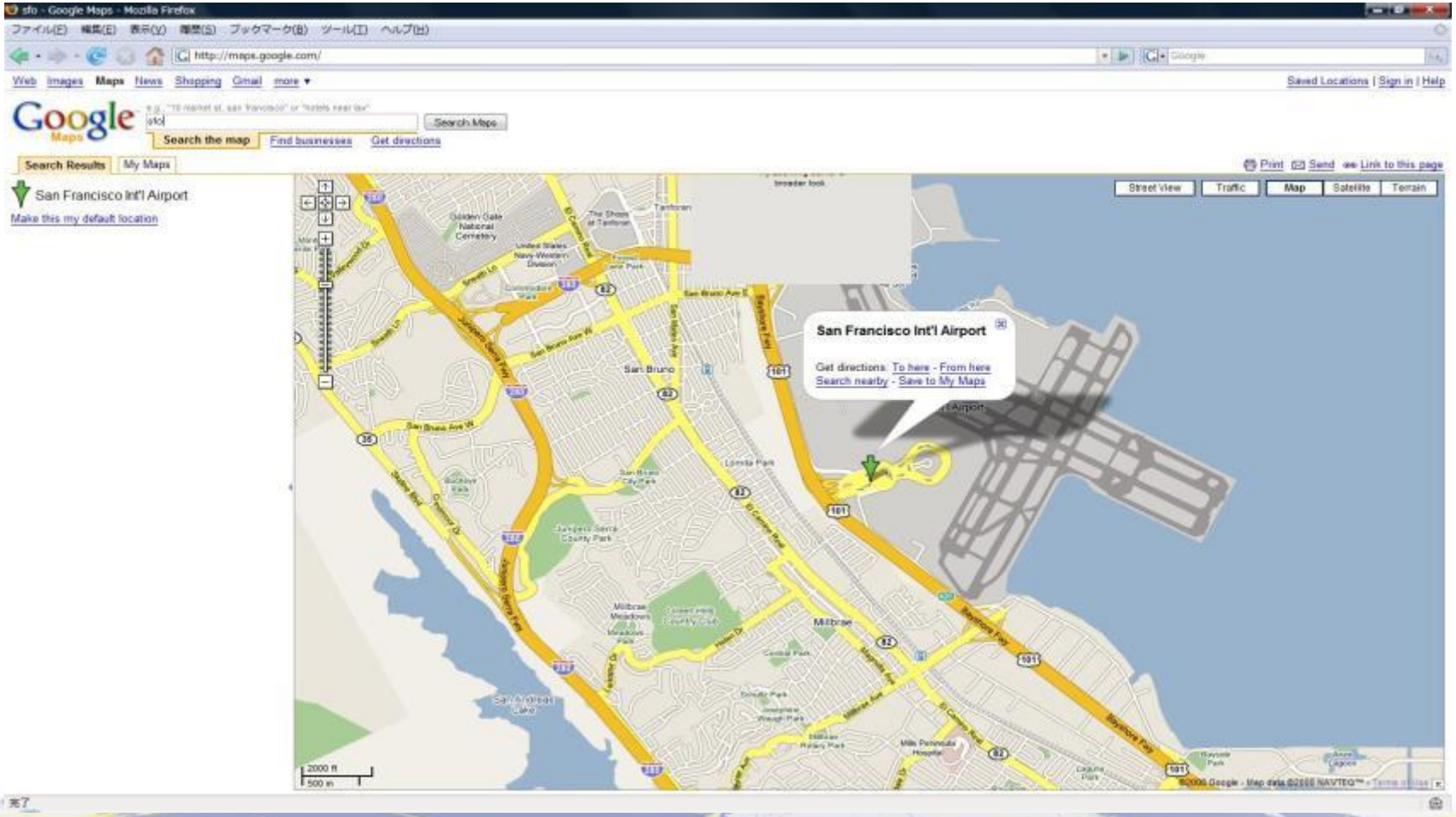
セッション数の制限



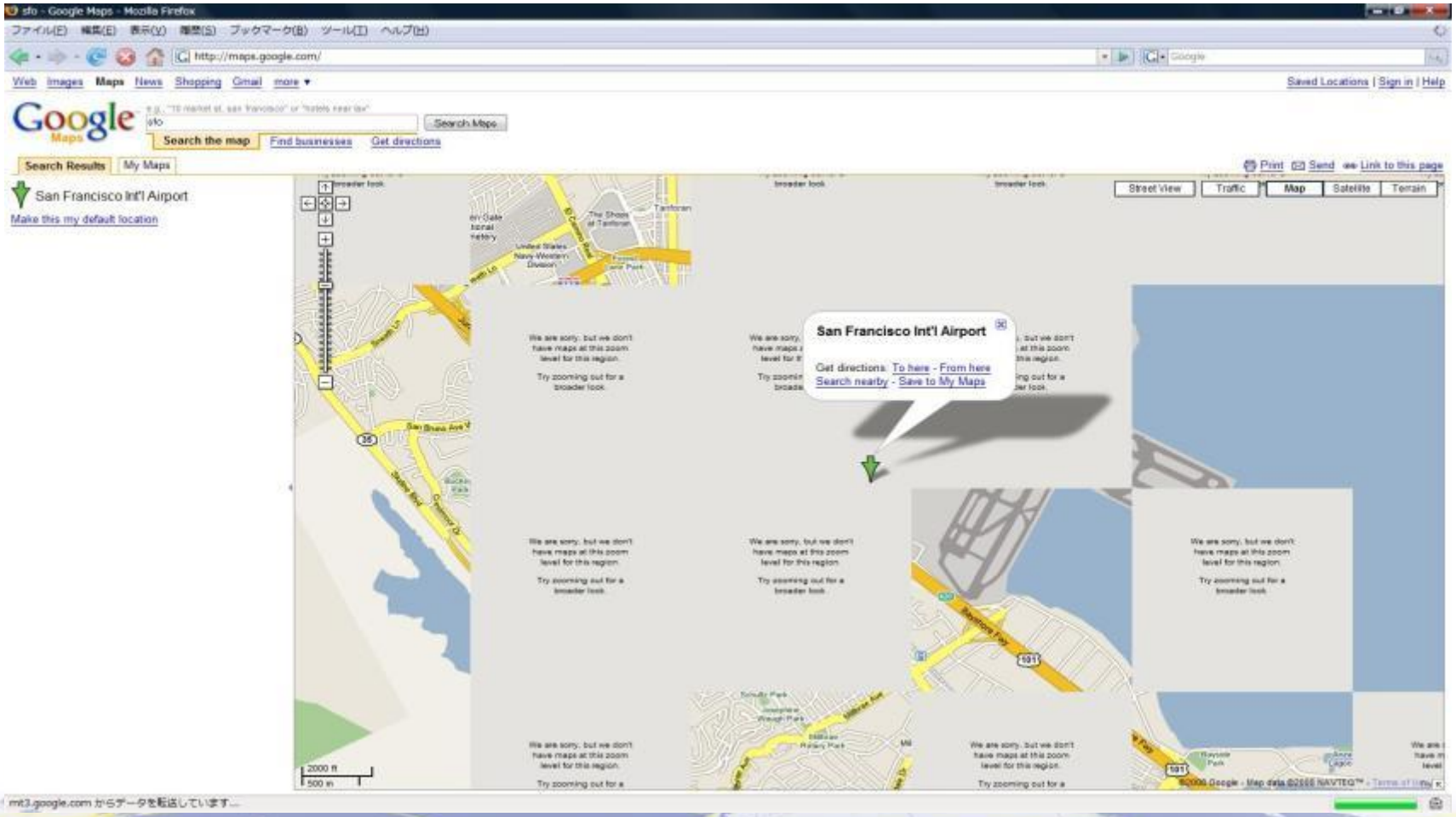
Max 30 Connections



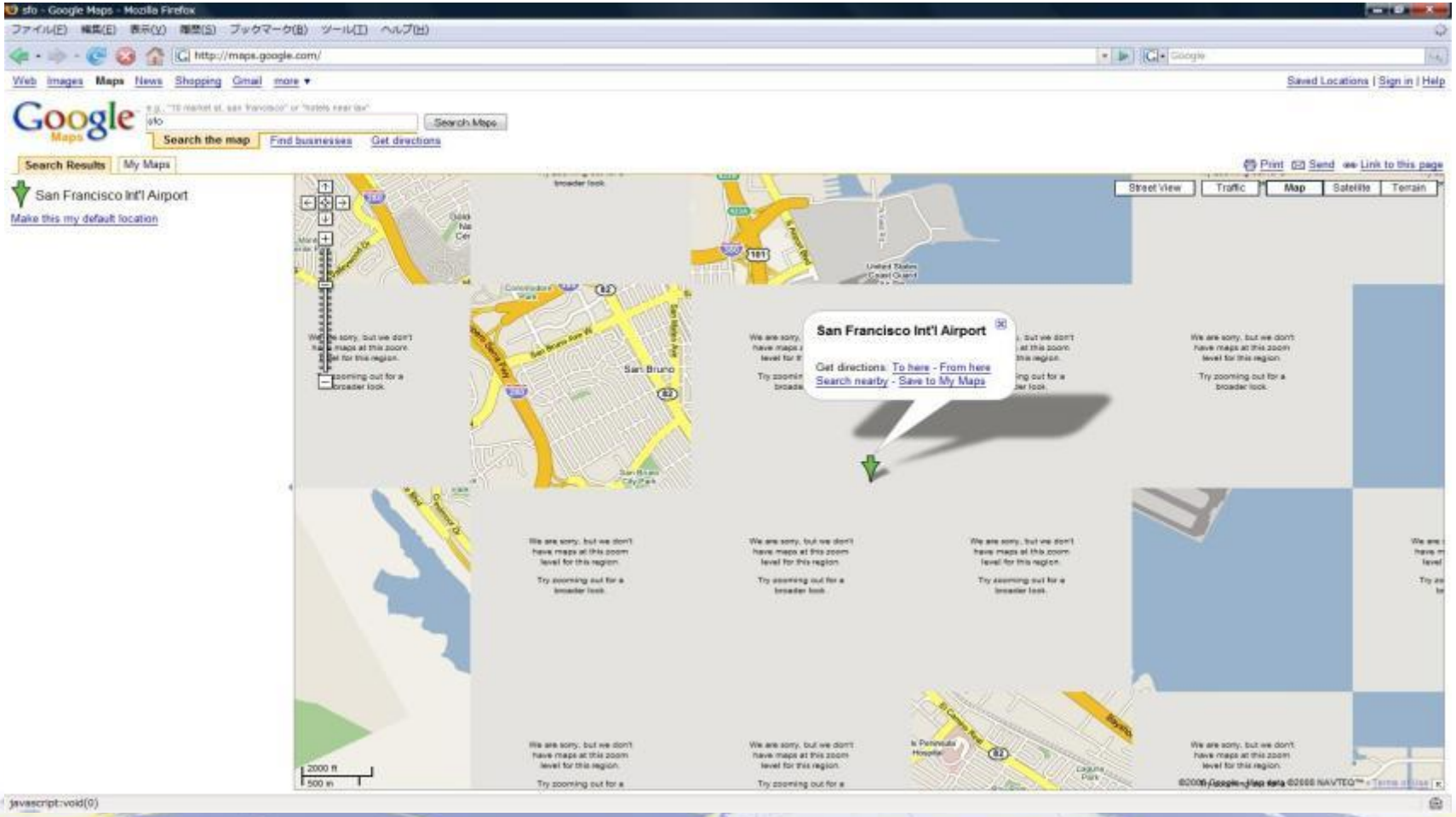
Max 20 Connections



Max 15 Connections



Max 10 Connections



Max 5 Connections

セッション数の例

Webpage	# of sessions
No operation	5～10
Yahoo top page	10～20
Google image search	30～60
Nico Nico Douga	50～80
OCN　photo friend	170～200+
iTunes	230～270
iGoogle	80～100
Rakuten	50～60
Amazon	90
HMV	100
YouTube	90

いろいろと起こりそうなことを予測し対策していますが・・・

IPv4の延命対策だけをやりつづけると、
際限なくコストがかさみ、セキュリティ上も問題を
抱え続けることになるとおもわれます

IPv4の延命といっても、あくまでも「暫定対処」であり、「最後の時」がくるのを遅くするだけで、セッション数のことを考えても、10年程度しかできないのではないかとおもいます。プロトコルの総取替えという大事業ということを考えると、本当に充分といえるのでしょうか？？

どうせ機材やアプリケーションをアップグレードしなければならないなら、
IPv6対応に真剣に取り組み
IPv4からとっとと全体を移行してしまったほうが、
コストが安いということになります

v6の導入

ISPアクセスサービスへのv6の導入

v4のパケットにv6をくるんでとどけてしまう

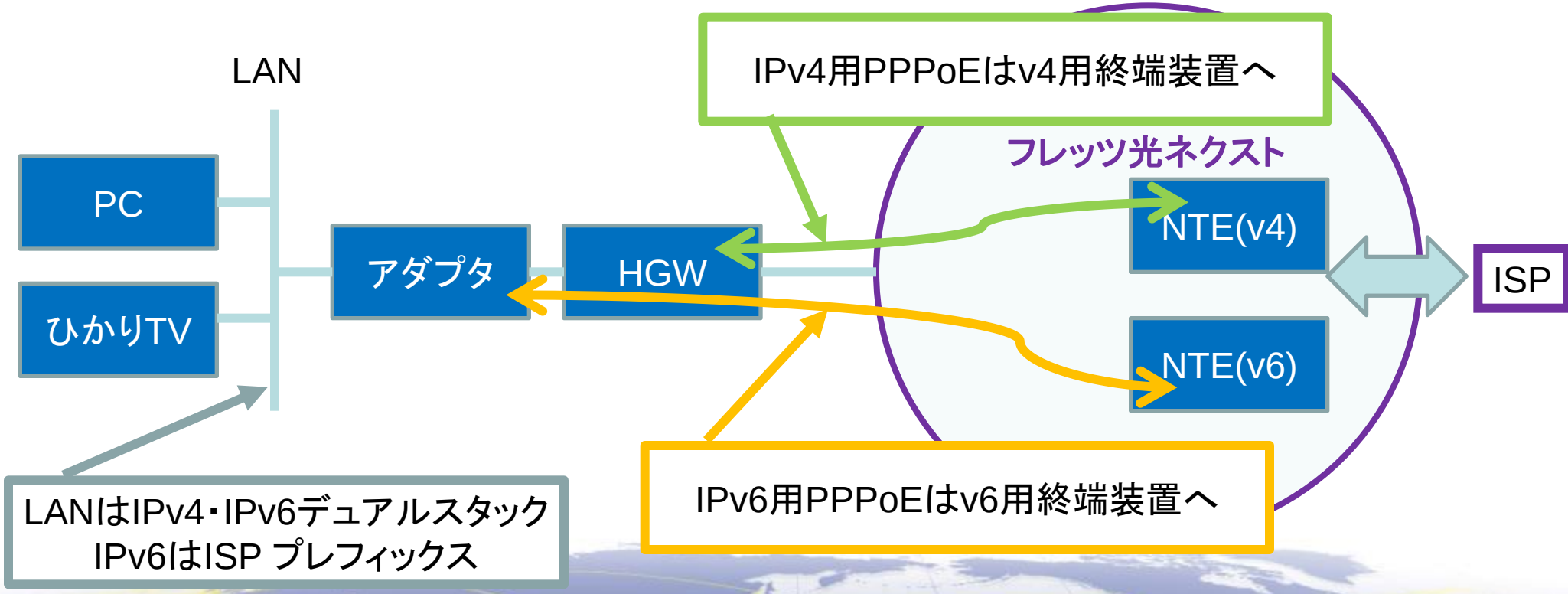
v4のパケットと並列にv6をとどける

実は今までv4パケットをくるんで届けていたv6網をインターネットに接続する

ケースバイケースで色々なパターンがあり、IPTVやVoIP電話などの組み合わせも考えて、なおかつ、お客様の機材のアップグレードを最小限にとどめられつつも、最大限のパフォーマンスを出せる方策を検討し、実際のネットワーク環境でテストしながら、必要な機材や運用技術を開発しています

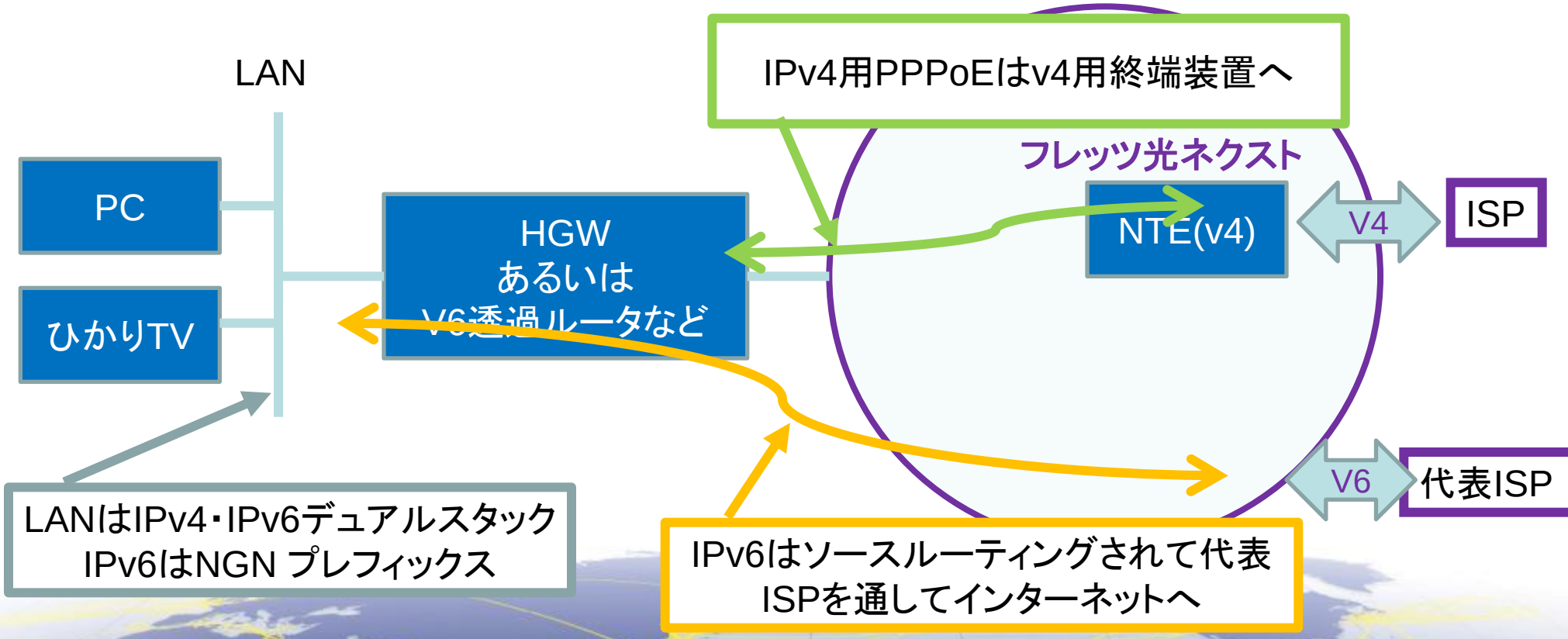
案2と呼ばれる導入方法

- NTTのNGN網（フレッツ光ネクスト）の上で、ISPがIPv6を顧客に提供する方法のひとつがいわゆる「案2」です
- 案2は、簡単に言えば、今までPPPoEでIPv4を提供していたことと同様に、もうひとつのPPPoEでIPv6を提供します
- お客様側では案2用アダプタ（あるいは案2用ルータ）で終端することができます



案4と呼ばれる導入方法

- 案4は、ISPに向かうPPPoEでv4を提供することは変わりませんが、IPv6はフレッツ光ネクスト自体を「代表ISP」を通じてインターネットに接続し、ルーティングを行うことでIPv6を提供する方式です



コムが開発している案2用アダプタの機能

NTTコミュニケーションズが開発中の案2用のアダプタには以下のような機能が具備されます

- NAT66
  - ISPとのトラフィックはそのまま通過させ、フレッツ内部との通信は、フレッツから付与されたプレフィクスに付け替えてNATして行います
- MLD Proxy
  - ひかりTVなどのマルチキャスト通信はフレッツへとつなぎ込みます
- DNS Proxy
  - アダプタ配下のマシンは、DNSサーバとしてアダプタを指定するようにします
  - アダプタはflets-east.jpなどのフレッツの内部で用いられるドメインはフレッツのDNSサーバに問い合わせを行い、それ以外は、ISPのDNSサーバに問い合わせを行うようにします
- NDP Proxy
  - フレッツのUNIは、RAを吹いてLANを接続しようとするため、アダプタ配下のマシンのアドレス解決は、網側の機械に通知を行う必要があります。そのため、ISP側へはルータ接続をしてるようにみせる一方で、フレッツ側にはブリッジ接続（ただしNATしてますが）をシミュレーションする機能が必要となっています
- 経路情報取得や自動コンフィグ機能などの補完機能
  - その他、どのアドレスがフレッツ内部のアドレスなのかといった情報を取得する機能など、補完機能を搭載しています

案2によるISP　IPv6の提供について

- 案2には、いろいろな良い点と悪い点があると考えていますが、現時点で、もっとも現実的なやり方で安定的なサービスを提供できるスキームであると考えています
- インターネット通信は、IPv6パケットであっても、かならずPPP終端装置までトンネルの中を通過してしまいますので、P2Pトラフィックなどが必ずしも効率的に運べるとは限らない一方で、エンドユーザ側がBOT化されて多くの場所から同時多発的にサイバー攻撃が起こるという最悪の事態に対しても、トラフィックを制御しやすい構造で安定性が高いといえます
- お客様から故障申告が有った場合に、現在の故障対応フローと同様に、PPP終端装置を切り分けのポイントとし、PPP終端装置からお客様までの疎通確認と、PPP終端装置からISPまでの疎通確認をうまく分けて行うことが出来ますので、迅速かつ的確な故障診断と対処が可能になると考えています
- DoSやアタックが横行する現代のインターネットではPC直収のISPサービス形態は非常に危険であり、HGWやルータを通してファイアウォールを構成してから接続することは常識だと考えられます。そのため、コムが提供するアダプタは、それ単体でもIPv4のPPPoEを終端することも可能であり、必ずしもHGWが提供されない場合でもインターネット接続を行うことができますので、箱が無意味に増える、ということにはならないと考えています

近未来のネットワークの姿としては

- IPv6とIPv4のデュアルスタックになっていく
- IPv4でしかうごかないアプリケーション・サービスを順次、IPv6にも対応させていくことが必要です
  - 既にGoogleなどは、本格的に対応してきています
- IPv4はすぐにはなくならない・なくせない
  - Windows XPのDNSがIPv4でしかひけなかったりするし
- とはいえ、IPv4は枯渇していくのでLSNも必要悪としては残る
- 完全に新しいアプリケーションはIPv6でつくると良い感じです
  - たとえば、省エネルギー用のセンサーとか
- 総合的に勘案して、IPv6の導入は日本では今年から本格化し可能な限りスムースに行うようにしていって・・・
- 2020年過ぎ頃を目標にだんだんとIPv4を衰退させることがいいとおもわれます

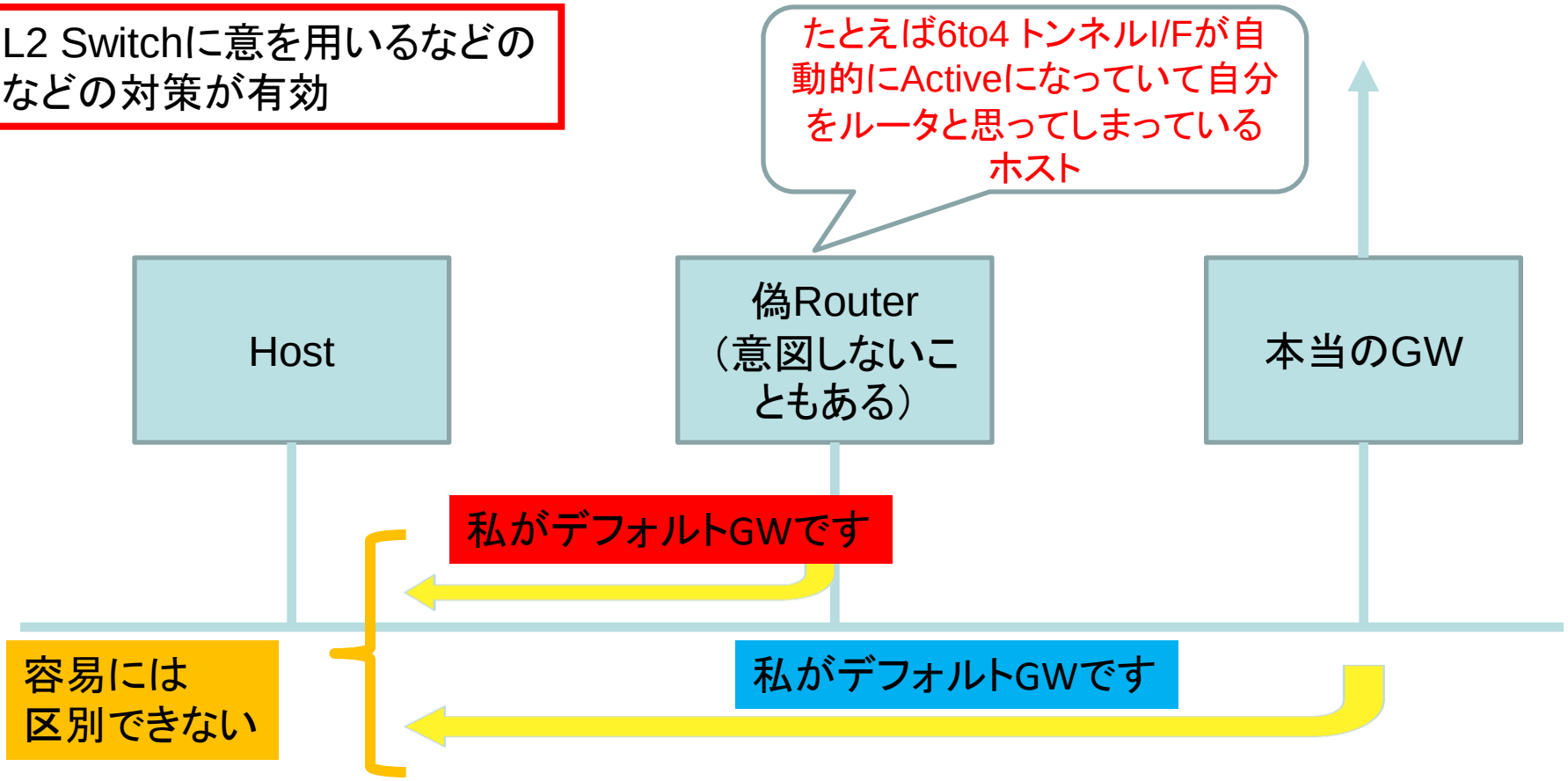
v6の運用やセキュリティは？

v4と基本的に同じではあるのですが、
v6ならではの特徴があり、
運用方法や、セキュリティに関しても、
全て細かく再検討しなければならないのも事実です

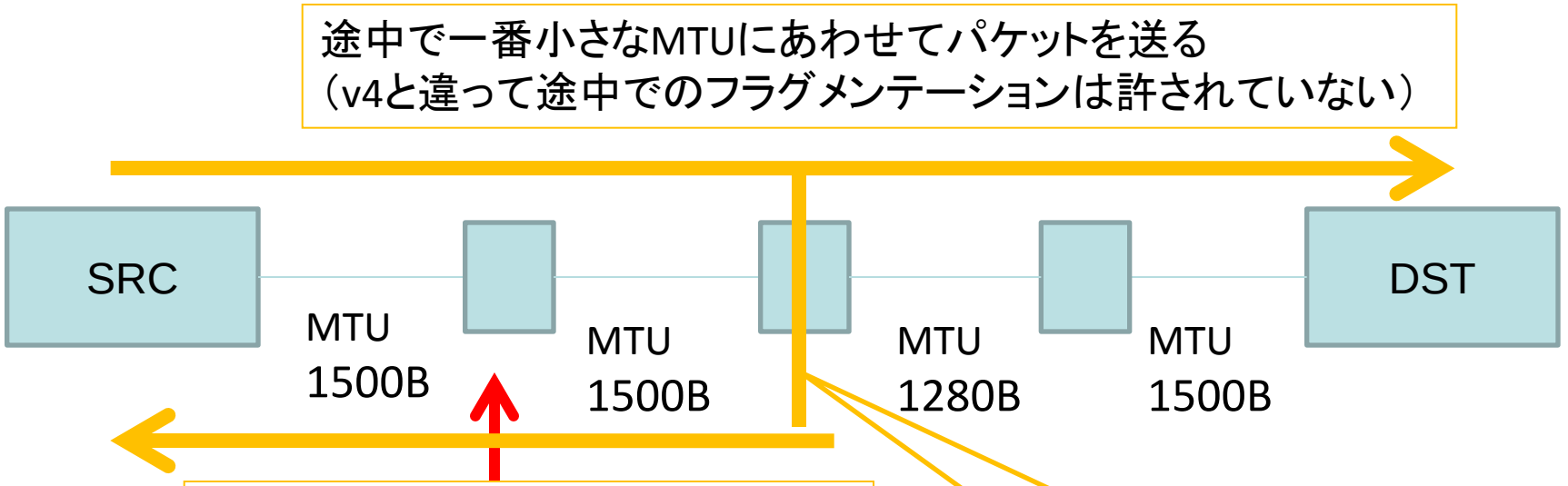
たとえば、ICMPのファイアウォールでの取り扱い方、偽ルータ対策、
ファイアウォールでのフラグメンテーションの取り扱い方、などなど、
細かい部分での検証と再構成が必要であり、
プロバイダーには高度なノウハウが求められます
今回はその例をご紹介してみます

偽ルータ告知（Rogue RA）

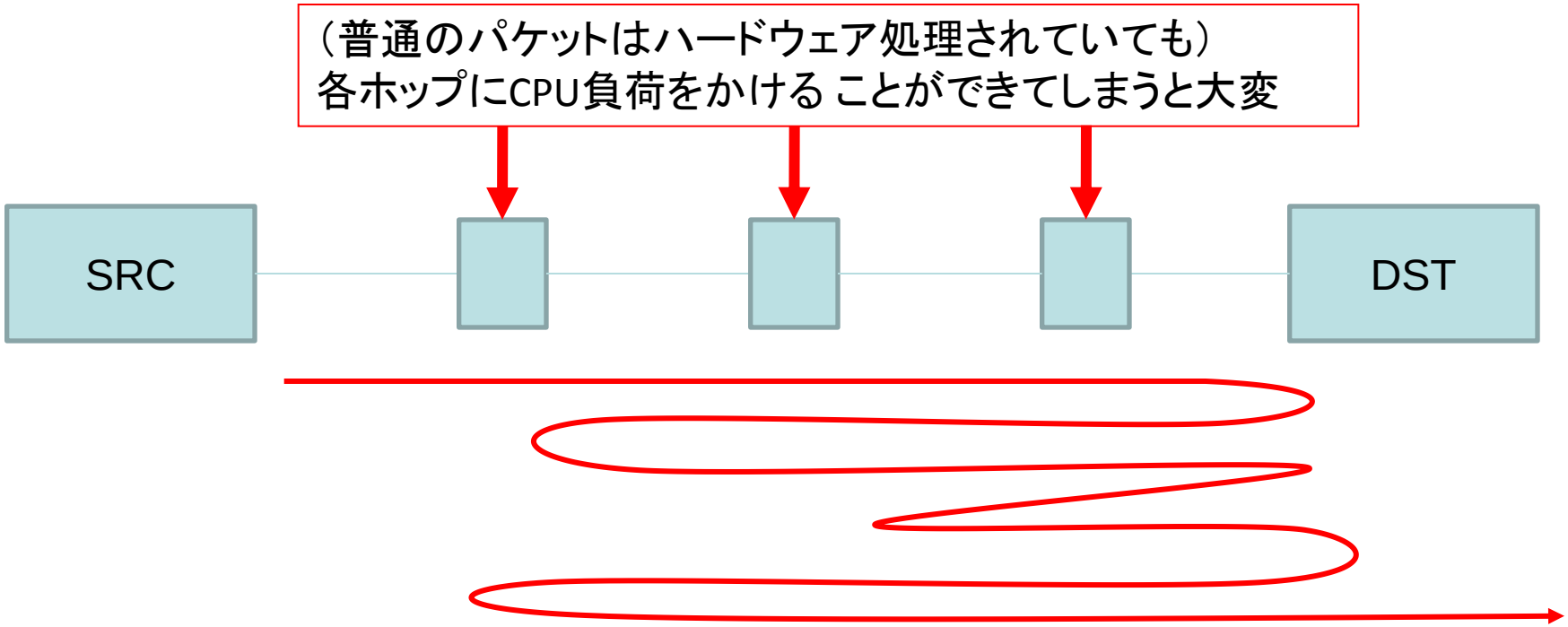
L2 Switchに意を用いるなどの
などの対策が有効



ICMPが大事（たとえばPath MTU Discovery)



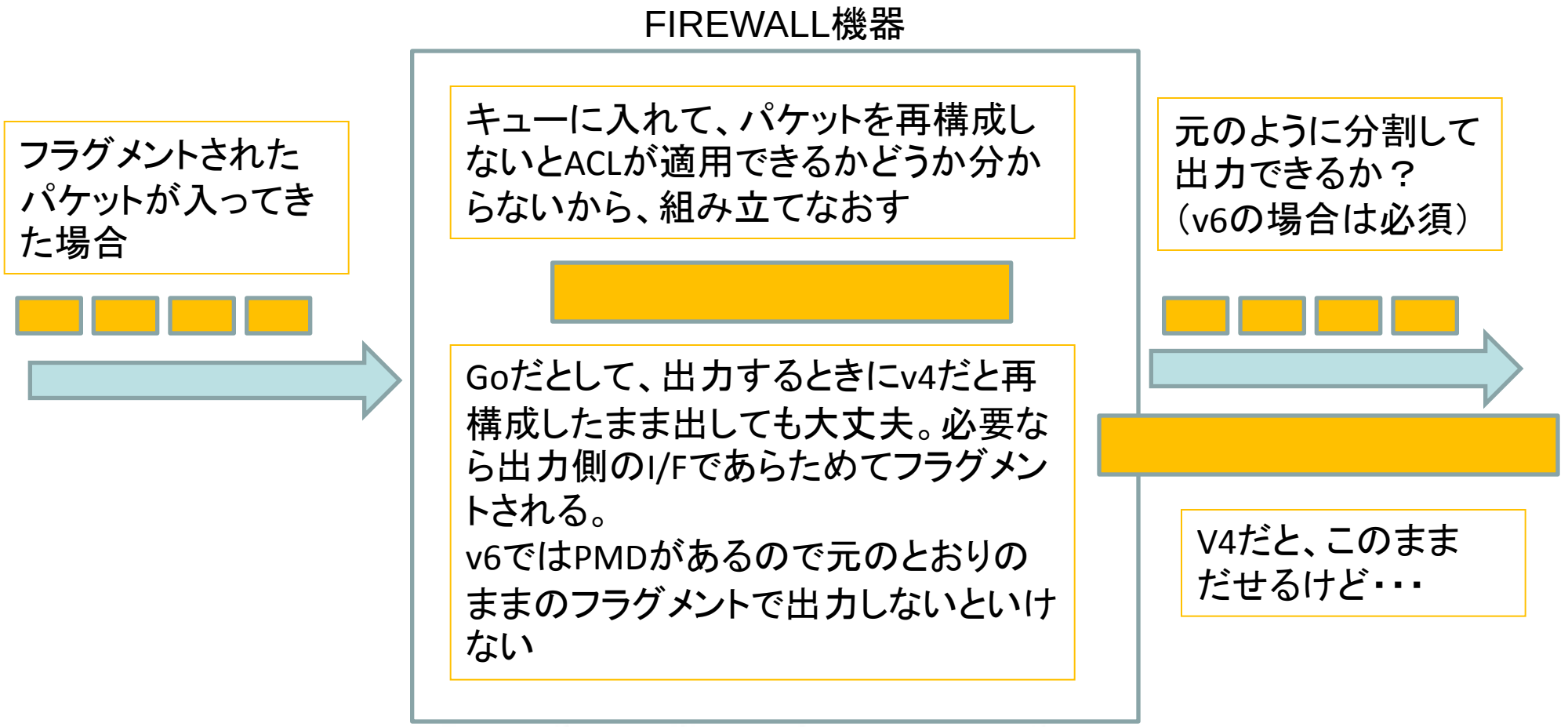
ヘッダ（特にHop by hopなど）に注意



IPv6にはヘッダを複数つけることが出来る
各Hopごとに処理すべきヘッダがあると途中の全てのルータにストレスがかかる
ルーティングヘッダを複数重ねればかなりのループを作れる可能性も

実装やルールで禁止や制限がちゃんとかかるようにすることに留意しておく

FIREWALLでAccess Control Listを書いてパケットのGo/No Goを制御したいが…



この動作は実装が面倒なので、
意外と有名な実装でもフラグメントされたv6パケットはACLできない場合がある
またACLで制御できても不完全動作したり、CPUをたくさん消費する場合も

アダプタ開発とその検証について

- NGN用のIPv6対応アダプタについて、技術検証を行うためには実際のネットワークで動作することができる試作機と、可能な限り本物にちかい検証環境が必要であると判断しています
- 2009年からアダプタの試作を開始し、昨年から本格展開用の開発を行っています
- 検証環境については、v4枯渇対策・v6移行のためだけでなく、広くさまざまな技術開発・検証に供するため弊社の商用ネットワークとは独立したAS番号とCIDRブロック、TLAを完備しつつ、可能な限り商用ISP設備と同じレベルの機能・性能を備えたネットワークAS38639(HANABI)を用意し、実際のひかりTVなどのアプリケーションも用意して、上位層のアプリケーション対応を含めて、万全な体制で検証を行っております

最後に

- IPv4アドレスの枯渇は間近ですので、きちんと対応しないといけませんが
- インターネットの技術者と言いながらIPv6のことを分かっていない人、触ったことが無い人が意外に多いです。
- 実際に触ってみることが必要です。人材育成も急務です。
- NTTコミュニケーションズは業界のリーダーとしてこれまでもさまざまな貢献をおこなってまいりましたが、これからも引き続きトップランナーとして動き続けたいとおもいます
- 引き続き調査・研究・開発および実用化を積極的に進展させ、サービスの拡充・整備をおこなうとともに、関係の皆様に発信していきたいと考えています