JPNIC Open Policy Meeting (IP-USERS)

プライベートIPv4アドレスとストリーミングメディア

渡辺　淳

関西医科大学　解剖学第一・大学情報センター学術部

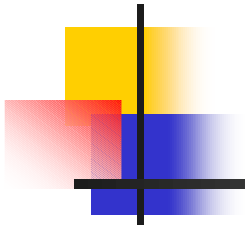
December 6, 2001 at Pacifico Yokohama

プライベートIPv4アドレスとストリーミングメディア

１ユーザから見たIPv4アドレス有効利用の問題点と解決？策

発表内容

- ブロードバンド化のもたらしたもの
- プライベートアドレスとNAT/NAPT
- プライベートでストリーミング
- ファイアウオール（FW）とストリーム
- FW+NATの下でのストリーミング利用
- もうひとつの強敵? TV（遠隔）会議
- IPv6とNAT
- まとめと提言



ブロードバンド時代の到来

- 広帯域回線が家庭にも -> CATV, DSL, FTTH
- コンテンツの変化

  文字情報、静止画像 -> 映像、アニメ、音楽
- ストリーミングメディアの浸透
- TV（遠隔）会議

  ISDN (H.320) -> Ether (H.323)

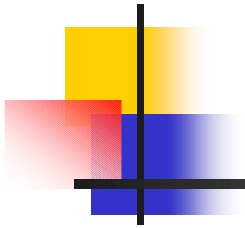
ブロードバンド化で何が起きている？（1）

- 実例：

  15歳♀にノート PCを与えて３ヶ月放置

  - インストールされていたもの
    - RealPlayer, VDOLive, QuickTime

- TVで育った世代（もちろん我々を含めて）：
  - 親しみやすさとインパクト
- テキスト情報 ＜アニメや音楽
- 大容量の最新情報に容易にアクセス可

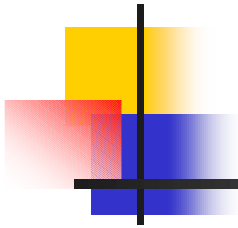


ブロードバンド化で何が起きている？ (2)

現実化しつつあるシナリオ

- ストリーミングメディアの利用増
- ストリームコンテンツの充実
- 重要な（価値の高い）情報の動画配信

ストリーム情報の不可欠化



ストリーミング

- 真のストリーミング
  - データをリアルタイムで再生（ライブ可）
  - ユーザPCにはファイルを残さない
  - （著作権の保護可能）
  - マルチキャスト・ブロードキャスト可
  - 広い接続帯域確保の必要
- 疑似ストリーミング
  - データをダウンロードして再生（ライブ不可）
  - ユーザPCにファイルが残る
  - 狭い接続帯域でも再生可能
  - ユニキャストのみ

コンテンツの変化（例：関西医科大学）

- 現在：電子化講議５科目＋画像データベース３つ運用中　　Web/HTTPが中心

  今後2-３年間にほぼ全科目で?：

  - 映像・音声教材の配信（学内へ）
  - 　　講議ポイントのVTR、手術映像など
  - 映像・音声教材の配信（学外へ）

    生命科学アニメ教材、心音、ドプラーエコー等
  - 遠隔講議
  - キャンパス（病院）間カンファレンス

ブロードバンド化でもうひとつ起こったこと

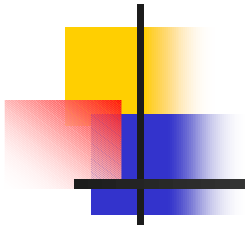
小規模ユーザ（家庭を含む）では：

- CATV，DSL，FTTHで常時接続->帯域に余裕
- 「複数のPCをインターネットに繋げたい！」

小規模（家庭内）LAN

- でもグローバルIPアドレスは多くの場合１個しか使えない
- IPv6 アドレス普及には少し時間がかかりそう

プライベート IPアドレスの利用



プライベートIPv4 アドレス （private address）

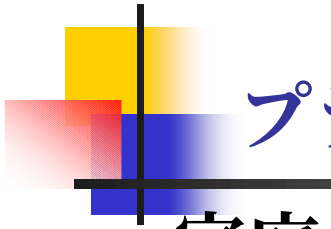
RFC 1918

- 10.0.0.0～10.255.255.255
- 172.16.0.0～172.31.255.255
- 192.168.0.0～192.168.255.255

インターネットに繋ぐには**アドレス変換**が必要

- TCP/IPでは、IPアドレスで通信相手を特定。
- インターネットでは、各ノードはすべて重複しない（一意の）アドレスを持つ必要がある。

利用増大：Yahoo検索で12,000件以上がhit！



プライベートIPv4 アドレス (2)

家庭

- 安価なDSL接続ではグローバル１個。

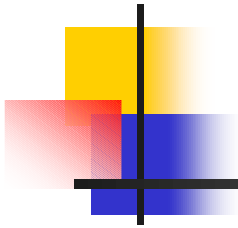
  （それもDHCPのケースが多い）

職場

- うちは約3,000台のノードに対して /24 しかない。

どうしたってプライベート使わないと

やっていけない！

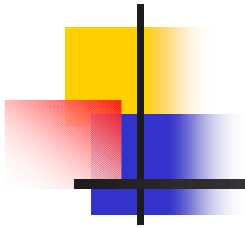


プライベートアドレスの利点

1．グローバルIPアドレスの節約
2．セキュリティー向上（外から見えない）

一石二鳥。でも・・・

インターネットに繋ぐには**アドレス変換**が必要



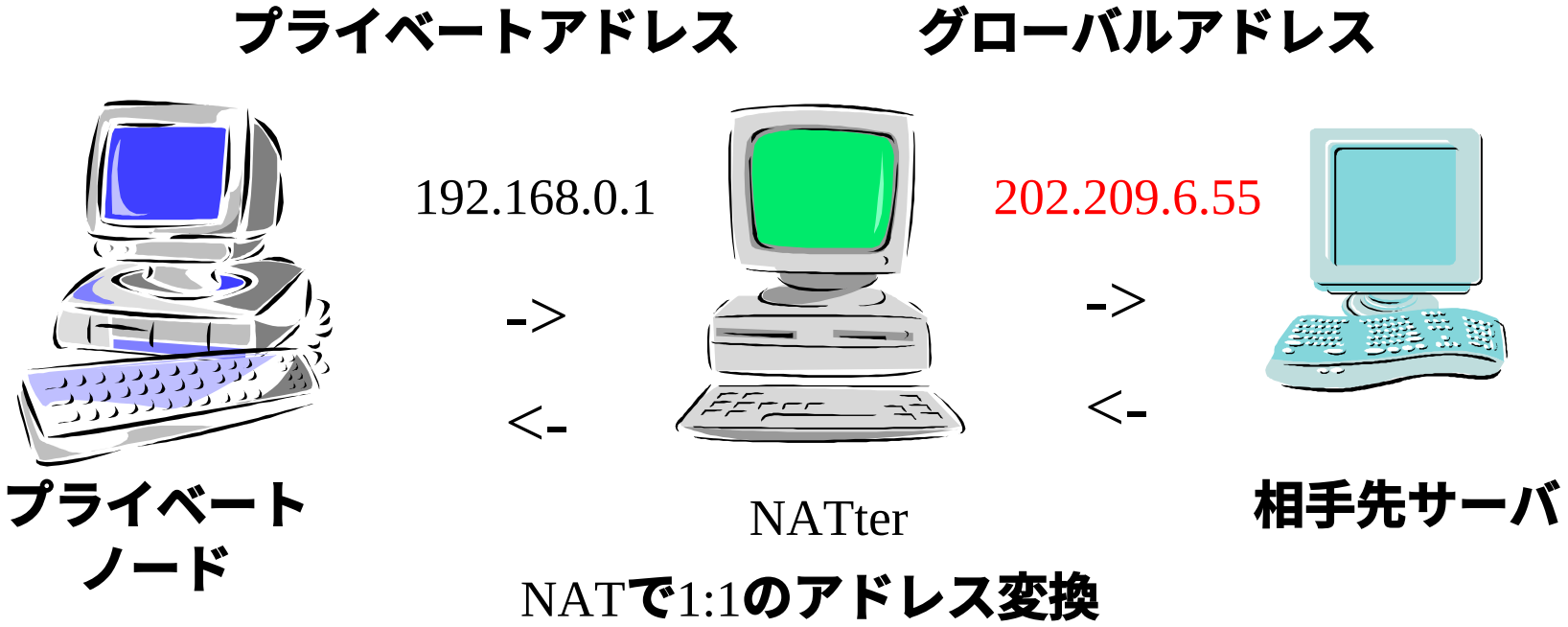
アドレス変換 NAT Network Address Translation

- RFC 1631
- プライベートアドレスと、インターネットにアクセスできるグローバルアドレスを相互に変換し、プライベートアドレスのノードから、透過的にインターネットにアクセスする技術。

- 広義のNAT
  - NAT （狭義のNAT)
  - NAPT/IP masquerade
  - Proxy （Proxy（代理）サーバでもアドレス変換可能)

NAT （狭義のNAT）Network Address Translation

- プライベートとグローバルを１：１対応でアドレス変換（アドレスのみ変換）



NAPT/IP masquerade

Network Address Port Translation

プライベートとグローバルを多：１でアドレス変換

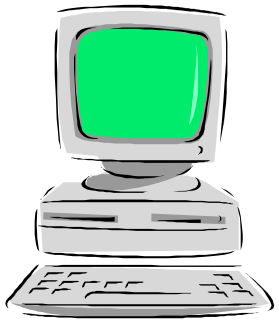
同時にTCPやUDPのポート番号も変換！

192.168.0.1

192.168.0.2

192.168.0.3

->
<-



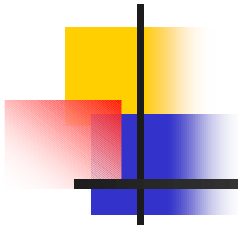
NATter

202.209.6.55

->
<-

相手先サーバ

NAT**で多：１の**
アドレス変換

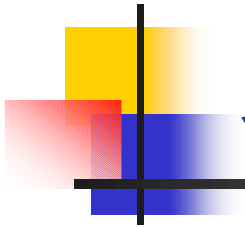


ネットワーク アドレス変換のしくみ (1)

- プライベートアドレスのノードからの要求パケット
- 送信先　アドレス　：接続先のグローバルIアドレス
- 送信元 アドレス　：要求元のプライベート アドレス
- 送信先ポート　　：接続先の TCP/UDP ポート
- 送信元ポート　　：送信元アプリの TCP/UDPポート

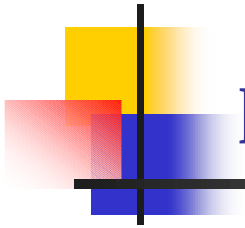
- NAPT機でのアドレス変換

  （送信元 IP アドレスと送信元ポートを変換表に記録しておく）
- 送信先 IP アドレス：接続先のアドレス
- 送信元 IP アドレス：NAPT機のグローバルアドレス
- 送信先ポート　　：　接続先の TCP/UDP ポート
- 送信元ポート　　：新たにNAPTでマップされた送信元アプリのポート



ネットワーク アドレス変換のしくみ (2)

- 接続先のサーバは、NAPT に返事を返す
  - 送信先IPアドレス ： NAPTのグローバルアドレス
  - 送信元 IP アドレス ： サーバのグローバルアドレス
  - 送信先ポート ： NAPTでマップされた送信元のポート
  - 送信元ポート ： サーバの TCP/UDP ポート
- NAPT は変換表をもとにクライアントに転送
  - 送信先 IP アドレス ： 要求ノードのプライベート IP アドレス
  - 送信元 IP アドレス ： 接続先（グローバル）IP アドレス
  - 送信先ポート ： 要求ノードのアプリの TCP/UDP ポート
  - 送信元ポート ： 接続先の TCP/UDP ポート

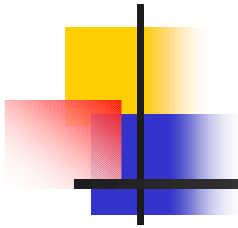


NAPT/IP masqueradeまたはproxy

- 1つのグローバルアドレスで、プライベートアドレスを持つ複数ノードをカバーできる

- 自分のネットワーク情報が外から見えない
  -> セキュリティー面で有利（NATも同じ）

ストリーミングとの相性は？



ストリーミングの主要プロトコール

- 1) RTP/RTSP（事実上の Defact Standard ?)

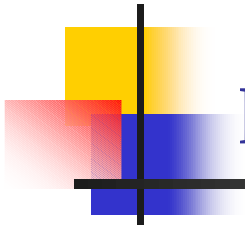
  RTP and /or RTSPを用いたサービスの例

  - RealSystem (RealVideo, RealAudio)
  - QuickTime
  - WindowsMedia

- 2) HTTP疑似ストリーミング

- 3) その他

  - 携帯電話用 など



RTPとRTSP

- RTP　（ストリーム実データの配信）

  Real-Time Transport Protocol (RFC1889)

  - マルチメディアデータストリームのパケットフォーマット
  - RTSPやH.323のプロトコルのデータ部分に使用
  - UDPタイプのプロトコル

- RTSP（制御用プロトコール）

  - Real Time Streaming Protocol（RFC2326）
  - RTPデータストリームの配信制御（巻き戻しなどのVCR形式の制御、この他にPNAなど）
  - 時間に基づく配信が必要なアプリに対応
  - マルチキャスト配信の制御可

RTP　Real Time Transport Protocol

- オーバーヘッドの小さいUDPを使用
- クライアントのリクエスト（たとえばTCP）に対して、UDPデータストリームを返す。

TCP リクエスト　->

<- UDP データストリーム

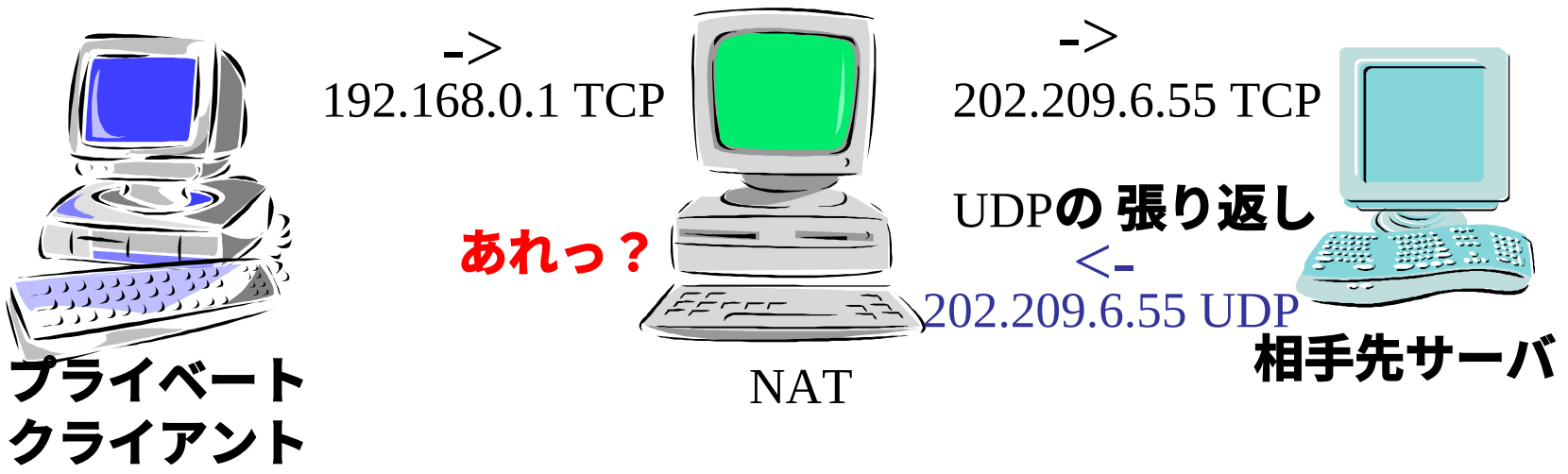
クライアント　　サーバ

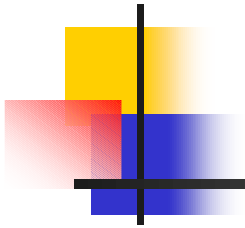
UDPについては、サーバからクライアントに向けて新たなセッションを張ることになる。

もし、プライベートアドレス だったら？

プライベートからのストリーミング 利用（1）

- インターネット接続にはNAT/NAPTが必要。
- クライアントのリクエスト（たとえばTCP）はNAT/NAPTされる。
- このとき、送信要求パケットの送信元ヘッダはNAT/NAPT機のアドレスに書き換えられる

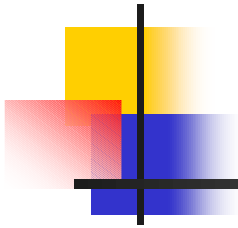




プライベートからのストリーミング 利用 (2)

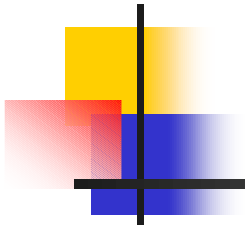
- 要求を受けたサーバはNAT/NAPT機のアドレスしか知らない
- そこで、サーバはNAT/NAPT機に向けてUDPデータストリームを送る
- NAT/NAPT機は、出ていったパケットと異なったプロトコールのパケットを受け取る
- これは変換テーブルで処理できない

- UDPデータストリームは要求元に届かない



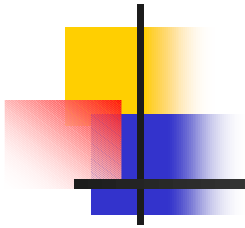
ストリーミング・NAT/NAPT問題 の 解決策

- 後ろ向き？の対応
  - 1）疑似ストリーミング (HTTP対応リソース)
    HTTPでダウンロード・再生
- 前向き？の対応
- 1）高性能NAT （RTP/RTSP対応NAT)
  - RTP/RTSP 接続時の制御用TCPパケット情報をもとに、要求元クライアントとのUDP接続を実現
- 2）HTTP Tunneling (HTTP encapsulation)
  - RTP/RTSPパケットをHTTPで包む



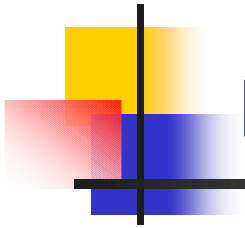
ファイアウオールの下でのストリーム利用 (1)

- ファイアウォール(FW)では、通常、外から内へのUDPパケット列（データストリーム）の流入を止めている
- 1) パケットフィルタ
  - FWの穴あけ
  - RTP/RTSP proxy
- 2) アプリケーションゲートウエイ
  - 多くのFWアプリはRTP/RTSPをサポート



ファイアウオールの下でのストリーム利用 (2)

- パケットフィルタの問題点
  - FWの穴あけ
    - 開ける穴が多いとセキュリティー低下
- 一番お手軽（かつ比較的安全）な解決策
  - HTTP Tunneling (HTTP encapsulation)
    - RealVideo,
    - QuickTime
    - VDOLive
    - Windows MediaPlayer (?)



FW+NAT存在下でのストリーミング利用 (1)

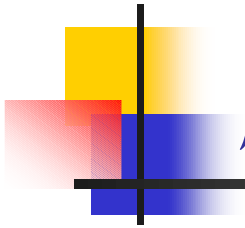
- FWに穴開けまくり
  （一部のアプリは今でも必要）
- RTP/RTSP proxy 設置
- HTTP Tunneling
  (HTTP encapsulation)

FW+NAT存在下でのストリーミング利用 (2)

- HTTP Tunneling (HTTP encapsulation)
  - NATしようがFWがあろうが面倒な設定なしにユーザが透過的にストリームを利用できる

    問題点
  - HTTP proxyの性能。

    リクエストが多くなると負荷が・・・
  - 少し前まで：SUN SS20 (1 CPU：160MHz x1 256MB)
    Solaris 2.6.1+Delegate
    (Delegateではなくマシンの性能不足)
  - 現在：SUN UL250 (2 CPU：400MHz x2, 1GB),
    Solaris 2.6.1+ Squid

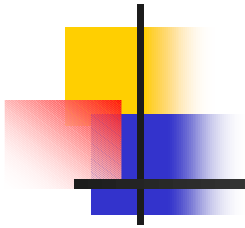


厄介者だった（過去形？）某社製品

○○ NetMeeting 、○○　○○○○○○ Messengerなど

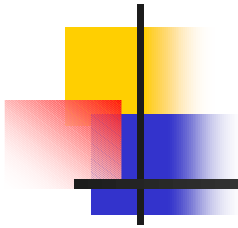
- Solution?
  - Universal Plug and Play (UPnP)
- 対応製品は？
  - HTTP Tunneling (HTTP encapsulation) は？
  - 非対応製品の場合は処置なし？
  - ○○社のOSならサポート

これで管理者は本当にHappyになったのだろうか？？？



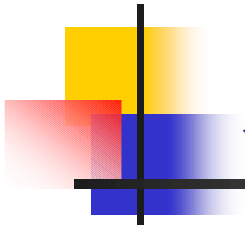
もうひとつの強敵?：TV（遠隔）会議

- データストリームはRTP
  - ブロードバンド化にともなってISDN（H.320）から Ether（H.323）にシフト中
- NAT時には通常のストリーミングと同じ問題
  - 『H.323対応TV会議製品はNAT環境では使えない？』
- dtc-forum 10/25-11/15，2001
  - 『ＮＡＴをくぐり抜けるテレビ会議』
  - 『NAT 問題（本当はインターネット接続の問題）』



TV（遠隔）会議（2）

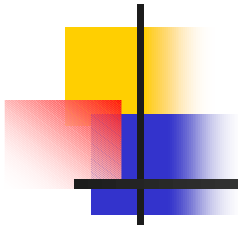
- 例『インターネット３』
  - 全国約2,000校に高速回線+テレビ会議システム（IP接続利用）設置
  - 多くの学校でプライベートアドレス使用
  - NATとファイヤーウォール越えが問題
    - 「NATルータの前にHubを置いてバイパスするラインを１本確保すればいいのでしょうか？」
- NATを乗り超える実装
  - CuSeeMe Ver5, Via Video, Vchat, Cuweb etc.



ストリーミングメディアとTV会議の違い

使われ方が違う！

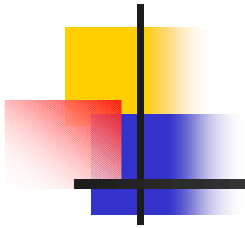
- ストリーミングメディア
  - ユニキャスト、マルチキャスト、ブロードキャスト
  - 不特定の相手からの要求に対して配信
- TV会議
  - 1：1、1：多
  - 特定の相手と通信



TV会議 NAT問題のソリューション

- TV会議：基本的に相手が特定できる
- VPNの利用
  - VPNを通してしまうことで FWの問題もNATの問題もほとんど解決
  - さらにセキュリティーも向上
  - FW越えもVPN利用で可能
  - NAPTしてからIPsec方式のVPNを通す場合には問題あり？
    - IPsecのESP が多重化できない。
    - ESPをUDPでwrapping?

      ESP: Encapsulating Security Payload 暗号化された通信内容+SPI+シーケンス番号フィールド+認証データ

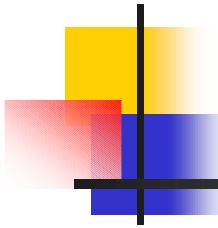


プライベートIPアドレスの利用

- 以前：IP不足に悩むネットワーク管理者の問題
- 現在：一般家庭の問題
- 大事なこと
  - 機器やアプリの対応
  - インフォメーションの提供

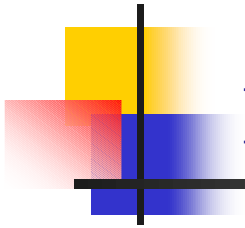
    『NATはできないんでしょうか？』は不親切？

    『こうやって対応すればプライベートでもいろいろなサービスが使えますよ。だからNATしてね。』
- プライベートアドレスへの対応が誠実でなく、セキュリティにも問題の多いサービス（あえて言及しません）を、駆逐できると良いのですが・・



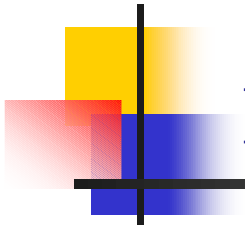
IPv6 の世界とNAT (1)

- プライベートアドレスとFWの世界にIPv6がやってくる
- IPv6アドレス空間は十分あるからNATなんてもう要らない？->『NAT悪人説』
- ある日一斉にv4からv6に変更なんて大技はできない
- 現実には、時間をかけてv4からv6に移行
- v4とv6の混在、FWとIPsecの並行使用？
  - FW: 境界型セキュリティー
  - IPsec: End to end 型セキュリティー
- IPv6にNATは必要か？



IPv6 の世界とNAT (2)

- NATはアドレス節約だけのため？
  - 『IPv6にNATは本当に無用な存在か』
    白橋明弘さん (2001)
- セキュリティー
  - 現状：ローカルネットワークを外から隠す
  - IPv6： IPv6アドレス初期設定では下位64bitが
    MACアドレス
- MACアドレスを不特定の他人に知らせたい？？？
  - ホスト側で定期的に付け替え？それとも、ここでNAT?

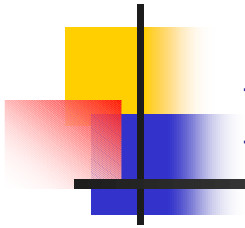


IPv6 の世界とNAT (3)

- IPv4メインの世界
  - たとえば IPv6 over IPv4（トンネル）
- IPv4，IPv6混在期
  - IPv6アドレスをプライベートアドレスの代わりに使う？
  - 相手の状態でv6->v4，v4->v6にNAT?
    (V4-> V6 はNATだがV6->V4はNAPT?)
  - V4のFWをV6が（VPNを通さずに）通るには？

  などなど・・・
- セキュリティーに加えて、移行期にもNATが活躍？

  移行期のネットワークの複雑化によって、現状よりも大変な状態になる可能性がある？

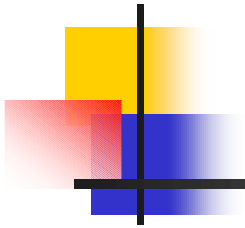


IPv6 の世界とNAT（4）

- デュアルスタック環境による同時アクセス
  - ノードが両プロトコルを同時に実行し、アプリケーションを1つずつIPv6トランスポートに移行する
- IPv4ネットワークでのトンネリングによる相互通信（RFC 3056）
- トランスレータの使用（NAT-PT　RFC2766）
  - インターネットのエッジ部においてIPv4とIPv6アドレス（およびIPヘッダフォーマット）を変換

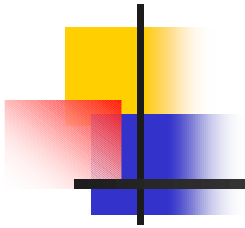
まだまだNATはなくならない！

IPv6への移行期には、プライベートアドレスとストリーミング問題の代わりに、v6アドレスとストリーミングの問題が出現？



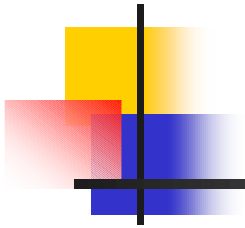
まとめ１

- 利用度の高いストリーミングメディアのいくつかについては、ある程度の対応策があります。
- これらについては、対応策を積極的に告知／広告することで、アドレス節約をしてゆきましょう。
- JPNICも積極的に告知／広告していただけると嬉しいです。



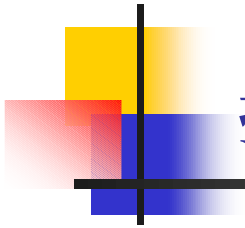
まとめ２

- こうしてグローバルアドレス節約を心掛けても、技術的に難しいメディアがあります。
- ブロードバンド化で、このようなメディアが今後、エンドユーザにどんどん浸透してゆく可能性があります。
- また、携帯電話などを中心に、新しいストリーミングメディアが次々とあらわれて来ることも予測されます。



まとめ３

- IPv6化に伴って プライベートアドレスがIPv6に置き換わってゆく場合、移行の経過中にIPv6からv4グローバルへのNATが必要となるケースが出てくる可能性が考えられます。
  - たとえば、ネットワーク境界部で、サブネットごと、まとめてNATするケースなど
- このとき、NAPTは容易でなく、IPv6とIPv4アドレスを1:1で変換（NAT）しなければならなくなる可能性があります。



提言

- JPNICのアドレスの割り振り割り当てのルールを、アプリケーション側の要因およびIPv6移行時の問題に対応させるようにしてゆく必要性があるのではないでしょうか？
  - 「必要なところに必要なだけ割り当てる」であるなら、プライベートで利用し難いタイプのストリーミングメディア／TV会議、そしてIPv6-NATなどは「必要」とみなせるものに該当するのでしょうか？
  - 「プライベートを使ってグローバルIPv4アドレス節約に協力したのに、そのせいでバカを見る」ってことにならないでしょうか？
- 皆様の御検討をお願いしたいと存じます。