

2010年度 電気工学特別講義 第5回 次世代インターネット技術IPv6/NGNと セキュリティ



力武 健次

京都大学

学術情報メディアセンター

2010年6月1日

Kenji Rikitake OUEEES 1-JUN-2010

1

講義に関する注意

出席を取るための名簿を回します

- 自分の名前を書いてください
- 講義後毎回回収します

できるだけ音を立てないでください

- ケータイはマナーモードにしてくださいね

講義の要約や案内はWebに出します

<http://www.k2r.org/kenji/jp-oueees2010.html>

今日の講義の内容

次世代のインターネット技術: IPv6とNGN

- IPv6: これからの利用者をつなぐための技術
何が新しくなって, 何が問題になるのか
- NGN: 電話ネットワークの今後
電話をTCP/IPの上でやってしまうという発想の転換
- NGN/IPv6化に伴うセキュリティ問題
寡占化に向かうインターネットサービス
もはや「ネットワークは中立ではない」という現状



なぜアドレスは「足りなくなる」のか?

1つの答: 「固定長」だから

• 割り当て範囲の上限が決まってしまう
足りなくならないアドレスはすべて可変長

- 電話番号, 住所, 郵便番号
- ドメイン名やメールアドレス, URL

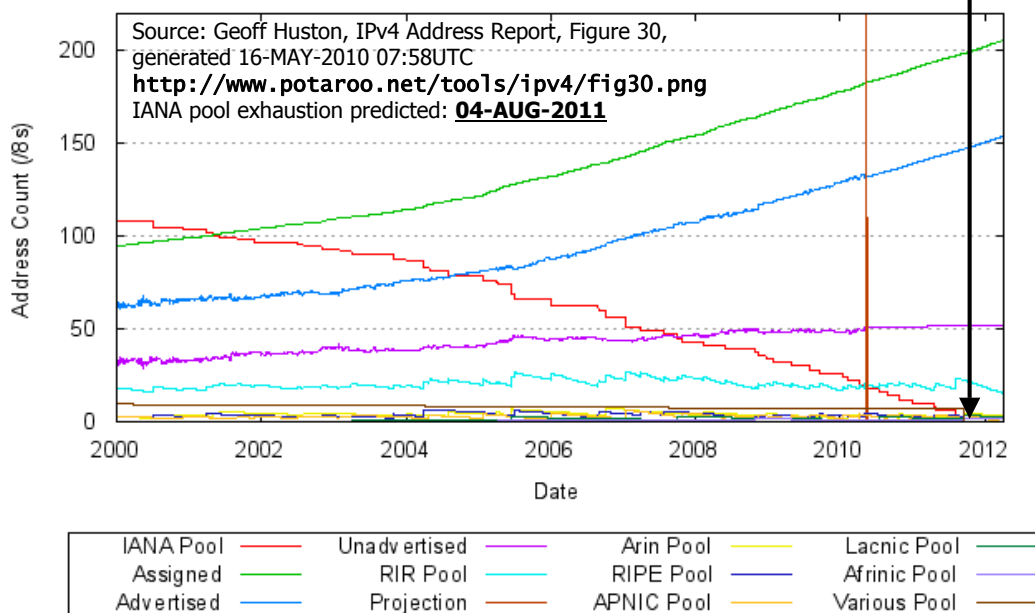
なぜ固定長にするのか?

- 高速処理できる (次のデータの予測ができる)



IPv4のアドレスはいつまで持つのか?

現在の予想: **あと1年 (2011~2012年)**



アドレスがなくなったらどうなるのか?

新しくサーバを立ち上げることができない

- サーバは接続先のアドレスを必要とする

サーバを上げられない=ビジネスができない

- この事情は個人でも大組織でも全く同じ

∴アドレスがなくなる=新規参入できない

- 今アドレスを持っている国や地域はそれでいいかもしれないが、今後参入してくる国や地域を受け入れないのは不平等であり容認できない



IPv4アドレスのやりくりは十分やっている

プライベートアドレス (RFC1918)

- 10/8, 172.16/12, 192.168/16
 - 内線番号同様重複を許すアドレス空間
 - 大半の組織や個人はこの空間を使っている
- でも外部に出るにはアドレス1個は必要
- 実際には外と中のアドレス変換 (NAT) で対応
しかしすべてをNATで対応するのは極めて困難
アドレスを共用するため利用者の識別が難しくなる



IPv6: アドレスを128ビットにしたIP

桁を増やすことでアドレス枯渇に対応した

- 1990年代前半に議論 → 1994年夏に決定
 - 2000年代前半までで基礎技術開発は完了
- 他にもIPv4の技術的問題を改良した
- ルータでのパケット再分割を禁止 → 負荷減
 - パケットの暗号化や認証の機能を必須とした
 - ヘッダを自由に拡張できるようになった
- 通信のラベル付けや優先順位処理が楽になった



IPv6アドレスの特徴

アドレスの割り当て方法が変わった

- ネットワーク部とID部が各々64ビットになった

ネットワーク部		機器識別子 (ID) 部
48bit	16bit	64bit
グローバル・プレフィクス(prefix)	サブネット番号	各ホスト毎のIDが入る (IDの形式は自由)
管理主体ごとに割り当てられる	管理主体ごとに自由に使える	(IDの既定値はEthernetアドレスより自動生成)



IPv6のアドレス表記法

128ビット→32桁の16進数で表記

- 4桁ごとにコロンで区切る

1234:5678:9abc:def0:fedc:ba98:7654:3210/64

- 途中省略可

(::は0000の連続に対応, 1度だけ使える)

ff02:0000:0000:0000:0000:0000:0000:0001

→ ff02::1

fd10:7546:0023:0100:0000:0000:0003:0001

→ fd10:7546:23:100::3:1



IPv6のアドレス拡張で何ができるか

機器同士がNATなしに直接認識できる

- サーバを介さないP2P通信への道が開ける
1990年代前半までのインターネットの姿に戻る

機器固有の情報を使って自動接続できる

- Ethernetアドレス(EUI64)からIPv6アドレスは自動生成され、機器の最初の接続に使われる

今まで通りの手動設定とも共存可能

- アドレスを秘密にしたい時も運用で対応できる



IPv6導入でアプリケーションはようになる?

トランスポート(TCP, UDP)はIPv6に対応

- ほぼそのままの形で使うことができる

IPv4とIPv6は別のネットワークとして扱う

- 基本的にはIPv4/v6両方に個別対応が必要

両方つながっているときは**IPv6が優先**

- しかしこれでは不都合が生じる場合もある
例: NTT地域会社のフレッツ網を使う時など

- とはいえv4/v6共存の時代はもうすぐやってくる



IPv6の普及への問題点

IPv4とは直接接続はできない

- すでに各OSでの対応は終わっているのだが...

期限はあと1年しかない!

ISPはもう準備を進めている, が, 問題はユーザ

日本の企業や大学は必要がないため対応が遅れている

IPv6に対応したセキュリティ対策が必要

- 直接各端末が外部接続し得る状態への対応
- 暗号化やカプセル化されたパケットへの対応



NGN: 次世代の電話ネットワーク

NGN (Next Generation Network)とは?

- 電話をTCP/IPの技術の上の実現したもの
- もともとは携帯電話のTCP/IP化から始まった

最大の動機: コストの問題

- 電話専用の機器は数は出ないし売れない
現在使われている交換機を維持し続けるのは困難
- TCP/IPの機器は競争が盛んで安い
PCを並べれば電話交換機も作れてしまう



NGNがめざすもの

目標: すべてのサービスをTCP/IPに統合

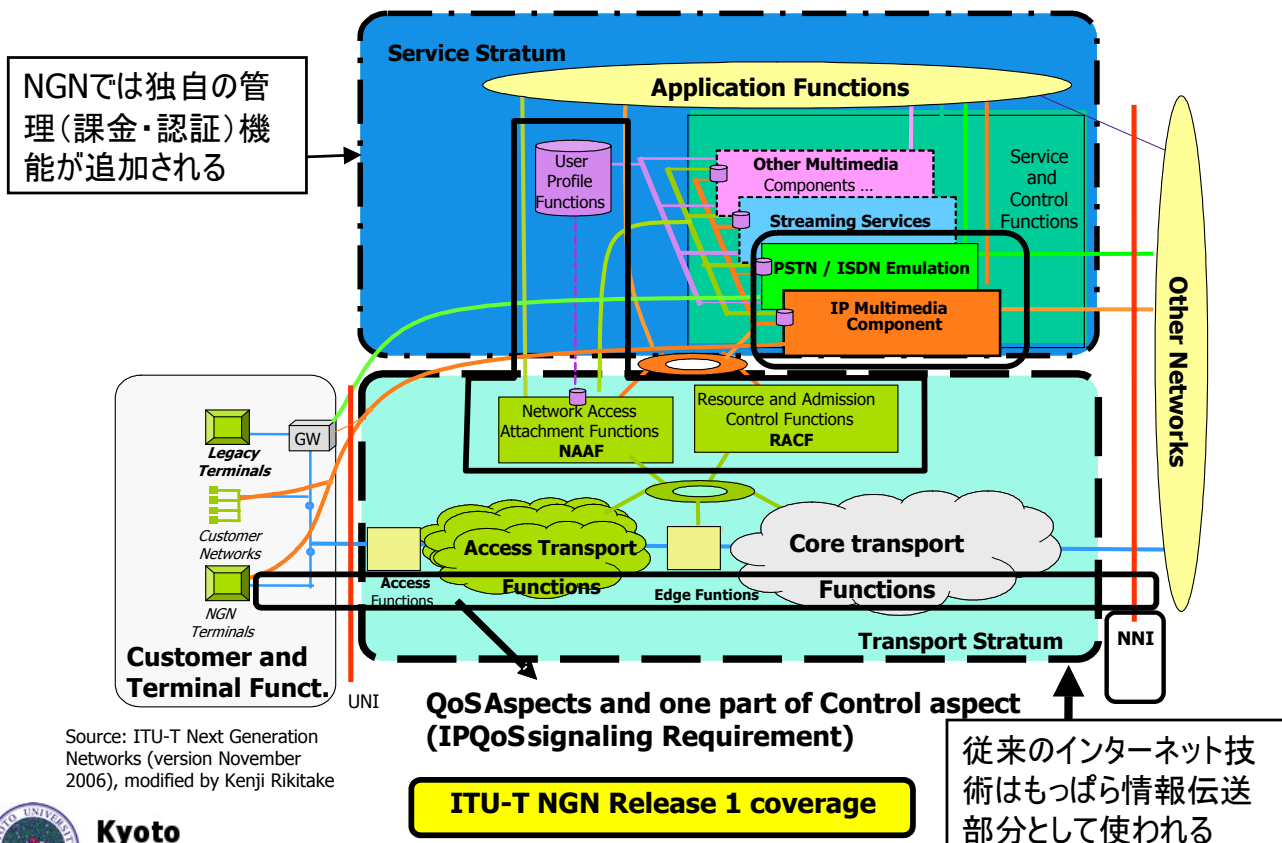
- 固定電話, ケータイ, 専用線, etc.
- 重複保守の手間とコストを減らす

伝送技術に依存しないサービスの提供

- 電線, 光ファイバ, 無線, CATV, etc.
- パケットのQuality-of-Service (QoS) 機構による優先順位付けで伝送品質を保証する
- 課金や認証などの管理機能を統合する



NGNの概念図



NGNの大前提

できるだけ外部と直接接続しない

- TCP/IP技術は使うが侵入者は最大限防ぐ
- 内部の経路制御を最大限安定させる
- ルータの負荷を予測し, 障害を未然に防ぐ
- QoSによる優先順位を徹底して守らせる
- 動画や音声の品質保証はこれが前提
- あくまで「電話のIP化」に徹する
- インターネットとは違うものだという自覚が必要



現実の日本のNGNの混乱(1)

日本のNGN = NTT東西のフレッツ網 + α

- ITU-Tの定義には必ずしも従っていない
- 信頼性は電話に匹敵するとはいえない
- 例: NTT東日本の「ひかり電話」の事故
- 2007年5月15日に7時間の障害
- 原因はルータの過負荷によるものと推定
- 当時の内部の経路数は約1万
- 障害を起こしたルータは全体4千個の半分の2千個



現実の日本のNGNの混乱(2)

NGNとインターネットの間の相互接続問題

- ISPのIPv6接続にはNGNの利用は不可欠
- しかしNTT-NGNの直結は認めたくない
インターネットが事実上1社独占になってしまう!
- NTTのNGNもすべてのISPを接続はできない
ルータの経路処理能力, 組織の運用能力の問題
→「代表ISP」を3社選定(2009年12月)
BBIX, インターネットマルチフィード, JPIX



代表ISP方式の問題

1社独占ではないが, 1+3社独占になった

- 代表以外のISPはすべて代表ISPを経由して
接続しないといけなくなった

代表ISPの責任範囲は?

- 他のISPの運用上の問題まで面倒を見る?
- 日本のISP全部に一斉に規制がかからないか?

代表ISP以外のISPはどうなる?

- もうインターネット接続では生き残れないのか?



「ネットワークは中立ではない」という問題

中立性 (neutrality) とは?

- アプリケーションに対する中立性

特定のアプリケーションだけを制限してはいけない

→ 現実にはP2Pのファイル転送は制限せざるを得ない

→ 最近リアルタイム動画転送にも制限がかかりつつある

- ISPに対する中立性

ISPによって使えないサービスがあってはならない

→ 現実にはSPAM(迷惑メール)の発信元制限や、ビジネス上の判断に基づく経路情報交換の制限がかかっている



インターネット上の紛争解決の歴史

組織間の問題は当事者同士で解決

- かつては研究者同士で話し合うことができた

国家主権との矛盾

- 通信や放送は各国・地域が決定権を持つ
- しかしインターネットは歴史的当事者が支配
DNSのRoot Servers, ICANNによるドメイン名支配
- 今の無秩序ともいえる状態は維持されるのか?
国家管理の強化は是非は別として不可避?



インターネット運用の「当事者」の変化

かつては「通信事業者」だった

- 回線を物理的に握るものが支配していた

しかし今は「コンテンツ事業者」が台頭

- 通信の中身を配る会社が強くなっている

Google, Facebook, Yahoo!, YouTube,
Microsoft, Akamai, etc.

- 著作権侵害に対する国際的厳罰化の動き

DMCA, 日本の著作権法, LOPPSI → ACTA条約



次回予告

- インターネットのサービスはいつまで広告収入だけで成り立っていくだろうか？

- ケータイやインターネットのルールは、誰がどう決めていて、どのように守られるのか？

そしてインターネット上の「通信の秘密」は、本当に守られていくのだろうか？

