

点検！IPv6のセキュリティ ～導入編～

北口 善明
金沢大学 総合メディア基盤センター

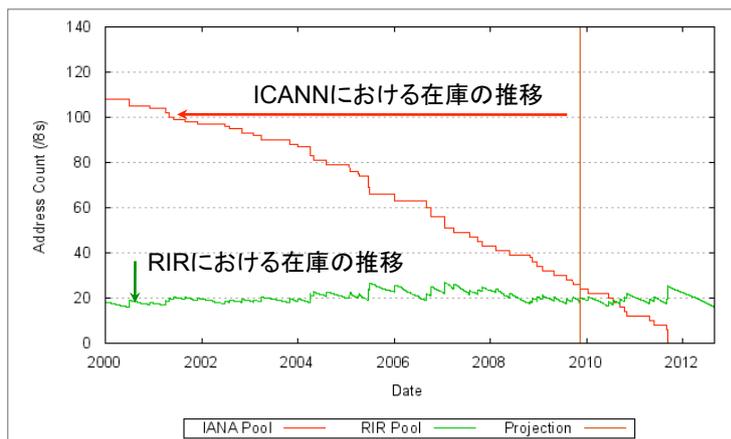
Internet Week 2009

Copyright © 2009 Yoshiaki Kitaguchi, All rights reserved.

本チュートリアルの目的

- IPv4アドレス枯渇が差し迫った中
 - IPv6の導入って課題はあるのか？
 - セキュリティ的に何か変わるの？
- IPv6対応を行う際に知っておくべき基礎知識
 - 現状のセキュリティ課題の整理を行う
 - ネットワーク・システム管理者を対象

IPv4アドレス枯渇の現状



アドレス在庫数の推移

IPv4 Address Reportより
<http://www.potaroo.net/tools/ipv4/>

ICANNにおけるアドレスの枯渇は

2011年9月2日

(2009年11月13日現在)

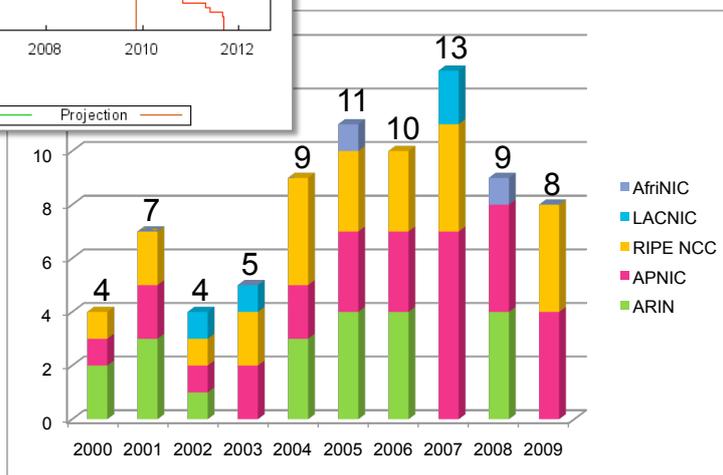
近年の消費量の推移

IANA IPv4 Address Space Registryより
<http://www.iana.org/assignments/ipv4-address-space/>

平均10ブロック/年の消費で推移

残り**26**ブロック

(2009年11月13日現在)



IPv4アドレス枯渇への一般的な対策

IPv4アドレスの入手

利用されていないIPv4アドレスを外部組織から入手する

利点：現行システムのまま運用可
 欠点：アドレス市場が存在しない
対策としての寿命が一番短い

IPv4アドレスの節約

外部到達性が不要な個所のグローバルIPv4アドレスを使い回す

利点：既存システムの改変が小さい
 欠点：リナンバリングが発生
 プライベートIPv4を利用することによる制限の発生

IPv6への対応

新規サービスにIPv6アドレスの割り当てを行う

利点：根本的な解決と拡張性
 欠点：サーバ側だけの対応では解決が不可能
 ISP側の対応が不可欠

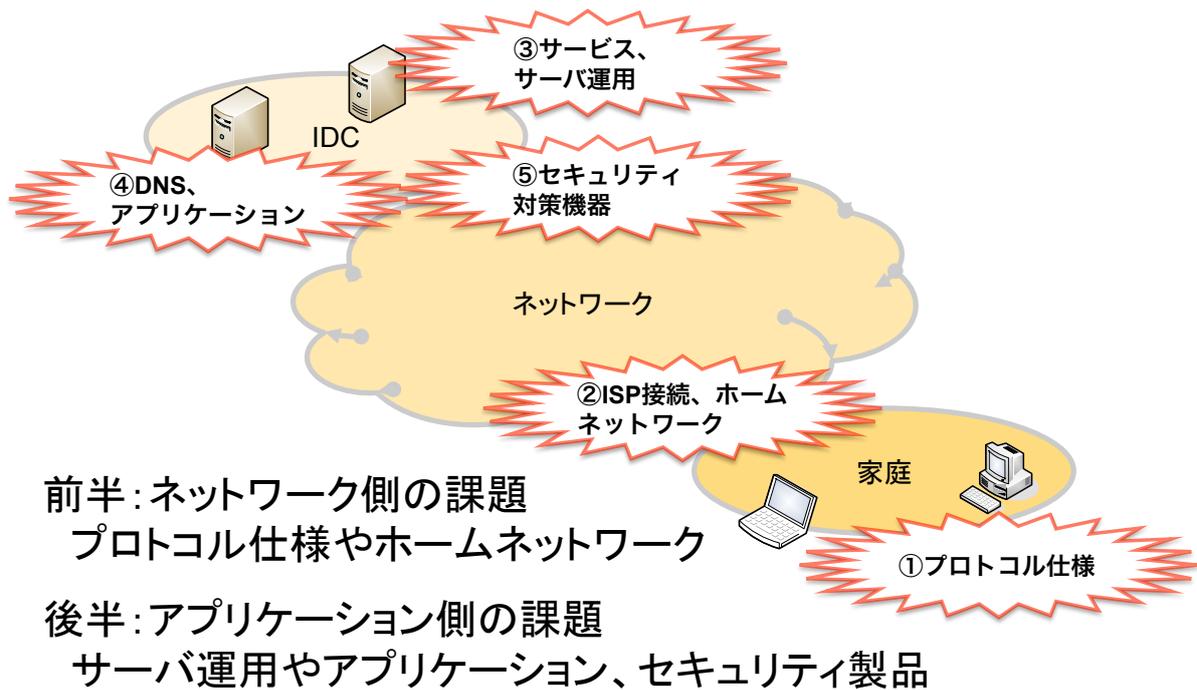
IPv6対応とは？

- 二つのネットワーク運用
 - IPv4ネットワークは枯渇を迎えたとしても止まらない
 - 三つの視点での考慮が必要
 - IPv4ネットワーク
 - IPv6ネットワーク
 - デュアルスタックネットワーク
- IPv4との主な相違点
 - アドレス表記／アドレス空間
 - フラグメント手法（経路中でフラグメントしない）
 - ARP⇒NDP（ARPの機能をICMPv6で実現）
 - プラグアンドプレイ／DHCPオプション
 - 全てグローバルアドレス（EtoE）
 - 拡張ヘッダ

IPv6におけるセキュリティ課題の整理

- 課題の分類
 - 影響対象
 - ネットワーク、アプリケーション、ノード（サーバ／端末）
 - 原因
 - 仕様上の問題、実装上の問題
 - IPv4と同等の問題、IPv6固有の問題
 - デュアルスタック運用における問題
 - IPv6導入により
 - 拡大する問題、縮小する問題、変わらない問題
 - 攻撃手段
 - DoS、侵入、不正アクセス、なりすまし、通信傍受

本チュートリアルの流れ（1）



本チュートリアルの流れ（2）

● 講演者紹介

< ネットワーク側の課題整理 >

● プロトコル仕様

● アラクサラネットワークス株式会社 鈴木 伸介 様

● ISP接続、ホームネットワーク

● NTT PF研/慶応義塾大学大学院 藤崎 智宏 様

< アプリケーション側の課題整理 >

● サービス、サーバ運用

● 株式会社クララオンライン 白畑 真 様

● DNSとアプリケーション

● 独立行政法人 情報通信研究機構 力武 健次 様

● セキュリティ対策製品

● マカフィー株式会社 野々下 幸治 様

本チュートリアルの流れ（3）

● それぞれ30分の講義内容

講演(20分)	議論(10分)
---------	---------

- 議論の時間では会場からのご質問もお受けします

● タイムテーブル

時間	内容	
14:00 – 14:20	導入	
14:20 – 14:50	点検！プロトコル	鈴木様
14:50 – 15:20	点検！ホームネットワーク	藤崎様
15:20 – 15:30	休憩	
15:30 – 16:00	点検！サービスのセキュリティ	白畑様
16:00 – 16:30	点検！DNSとアプリケーション	力武様
16:30 – 17:00	点検！セキュリティ対策製品	野々下様

言葉の整理

● シングルスタック

- IPv4もしくはIPv6どちらかの機能しか持たない状態

● デュアルスタック

- IPv4とIPv6両方の機能を有する状態

● ネットワークのデュアルスタック

- ルータがデュアルスタックになっていて双方のプロトコルでの通信が可能な状態

● サーバのデュアルスタック

- サーバがデュアルスタックになっていて双方のプロトコル機能を有効にしている状態