

IPv6導入でセキュリティはどう変わるか

佐藤友治

(株)ブロードバンドセキュリティ/IAjapan

本パネルの目的

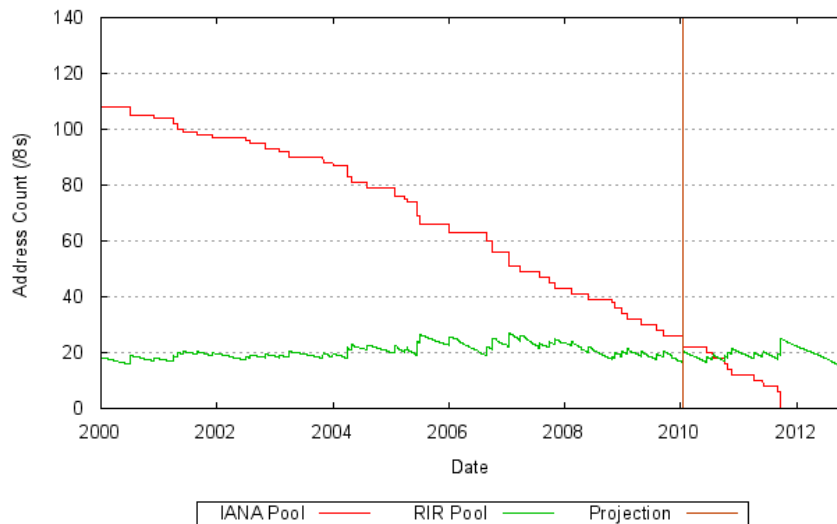
- IPv4アドレス割当枯渇が差し迫った中
 - 今、何が起きているか。
 - IPv6の導入には課題があるのか？
 - セキュリティ的に何か変わるのか？
- IPv6対応を行う際に知っておくべき基礎知識
 - 現状のセキュリティ課題の整理を行う

概要

- なぜ IPv6 への移行が必要なのか？
- 導入・移行のための設計が必要
 - IPv4 と IPv6 は、別のプロトコルである
 - コスト管理、リスク管理が必須
 - 技術的課題も
- もう考えないと間に合わない！

IPv4アドレス割当枯渇の現状

- アドレス在庫数の推移
- <http://www.potaroo.net/tools/ipv4/>



ICANNにおけるアドレス
割当枯渇は

– 2011年9月2日

RIRにおけるアドレス割
当枯渇

– 2012年8月27日

– 割当残9%

– (2010年1月18日現在)

IPv4アドレス割当消費量



- 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
 - (2010年1月15日現在)
- APNICに1/8 と 27/8 が割振られた
 - 2010年1月20日

IPv4グローバルアドレス割当枯渇の影響



- 自社が提供するサービスのお客様が他社に逃げてしまう。
 - 2011年以降、IPv6でしかアクセスできないユーザがでてくる
 - そのユーザは、サービスがIPv6に対応していない場合は利用することができないため、IPv6に対応している他社サービスに乗り換えてしまう
- インターネット上のサービスが使えなくなる。
 - 2011年以降、新規に立ち上げるサービスはIPv6でしたサービスされない可能性がある。
 - 自社ネットワークがIPv6に対応していない場合は、IPv6でしかアクセスできないサービスが利用できなくなる。

自社のビジネスを守るためにIPv6を導入しなければならないという認識が必要

- 根本的な対策はIPv6への対応(ただし、IPv4とIPv6は互換性がない！)

IPv6対応とは?

- 二つのネットワーク運用
 - IPv4ネットワークはアドレス割当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ICMP6で実現)
 - ブラングアンドプレイ／DHCPオプション
 - 全てグローバルアドレス(EtoE)
 - 拡張ヘッダ

- **影響を受けるシステム(対策の必要があるシステム)**
 - インターネットを介して、不特定多数のユーザに対してサービスを提供しているシステム(ECサイト、インターネットバンキング、ASP/SaaSなど)
- **将来影響を受ける可能性のあるシステム(対策の判断の必要があるシステム)**
 - インターネットを介してサービスを提供しているシステムであって、サービス提供側またはサービス利用側が、今後の拡張に十分なIPv4アドレスを保有していないシステム
- **影響を受けないシステム(対策の必要がないシステム)**
 - 直接インターネットを介して通信していないシステム
 - インターネットを利用しているが、既にIPv4グローバルアドレスを十分に確保している組織のみに対してサービスを提供しているシステム

セキュリティ面での懸念

- セキュリティ機器のIPv6への本格対応
- セキュリティアプライアンス機器ビジネスの弊害
- BCP(ビジネス継続)
- 監査方面、セキュリティレベルの維持
- 運用・管理面
- すでにIPv6が動いている機器の挙動把握
- セキュリティ対応の遅れによる、新インフラビジネス進展へのボトルネック
- 重要インフラシステムへの適用(スマートグリッド)
- P2Pアプリに対する日米の差
- 多段NATによる、インシデントハンドリングの難しさと一部のダークネット形成の恐れ

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

本パネルの流れ

- ISP/DC側の提供予定とIPv4アドレス枯渇対応
TFアクションプラン
 - (社)テレコムサービス協会 今井恵一 様
- IPv6のセキュリティ
 - 金沢大学 北口善明 様
- セキュリティ製品のIPv6対応
 - マカフィー(株) 野々下幸治 様
- 運用・監視していく上での課題
 - ISOG-J 許先明 様
- パネルディスカッション