基盤技術の標準化・ディプロイメント状況

関谷 勇司 / 東京大学情報基盤センター

本発表の概要

- 新技術動向について説明
  - IETF/IRTF 動向
    - 普及状況
- 項目
  - ルーティングエリア
  - DNS エリア
  - セキュリティエリア(主にルーティング)

ルーティングエリア

- 4 bytes AS
- Routing and Addressing Separation

4 bytes AS

- IPv4: 全経路(23万経路)中 9経路くらい？
- IPv6: 全経路(850経路)中 5経路くらい？
  - 依然発展途上段階
    - ベンダーの本格的なサポートはこれから
    - 一部ルータでの不審な挙動
  - . (dot) 表記による混乱

Routing and Addressing

- IETF RAM (Routing and Addressing Mailing List)
  - 背景：経路表の急速な増大
  - ID と Locator の分離
    - すなわちIPアドレスとルーティング情報の分離
- LISP (Locator / ID Separation Protocol)
  - Locator と ID のマッピングは別データベースにて管理
  - UDP tunneling

DNSエリア

- DNSSEC
- IPv6/DNSSEC/IDN for ROOT

DNSSEC

- リソースレコードの起源を保証する
  - 暗号化ではない
  - まだ仕様の更新が行われている (DNSSECbis)
    - NSEC3
    - DNSSEC Opt-in
- 運用上の問題は依然残ったまま
  - 誰が鍵を管理するのか

IPv6/DNSSEC/IDN for ROOT

- IPv6 transport
  - 一部 ROOT DNS サーバにて提供されている
    - http://www.root-servers.org/
- AAAA records in ROOT
  - パケットサイズ問題があいかわらず
  - EDNS0 にて解決する方向

IPv6/DNSSEC/IDN for ROOT

- DNSSEC による ROOT zone の署名
  - IPv6 より道は険しい ??
  - http://www.dnssec-deployment.org/
  - 鍵管理、再署名の問題
    - あくまでも運用上の問題であるが、それが最大の問題
    - 推進派の人々はやはり ROOT からやりたい

IPv6/DNSSEC/IDN for ROOT

- IDN (Internationalized Domain Name)
  - .日本　とか
  - TLD を IDN にしたいという動き
  - 実験は行われ、技術的問題はクリア
  - 本当に大丈夫か？

セキュリティエリア

- 主にルーティングに関するセキュリティ
- IETF SIDR (Secure Inter Domain Routing) WG
  - S-BGP
  - soBGP
  - psBGP

S-BGP

- Secure BGP
  - Origin AS が正しいか検証
  - AS path が正しいか検証
- 検証にPKIを利用
  - AS単位で公開鍵を用いて経路情報を署名
  - 最上位の鍵はレジストリ
- 当然ながらルータの負荷は増大

soBGP

- Secure Origin BGP
- AS単位で公開鍵を持つ
- 信用できるもの同士で署名し合い、Chain of Trust を形成
- 分散型の信頼モデル形成
- 受け取ったASパス情報を後ほど検証することが可能なため、ルータには多少やさしい

psBGP

- Pretty Secure BGP
- あるASが他のASを評価するという形で信頼性の rating を行う
  - この評価値に基づいて、信頼/破棄を決定
  - そのため、受け取った AS パス情報は手元にて評価
    可能
  - あくまでも rating
    - だから “Pretty Secure”

結局は

- どれもまだ提案状態
  - 現状実運用には導入されていない
    - BGP TTL hack で十分 ??
    - RR(Routing Registry) を利用するのが現状
- あまり複雑なものは普及しない
  - S/so/ps BGP 系の話題はあまり元気がない

まとめ

- “データ起源の保証”というのが時流
  - そのために別途認証の仕組みやデータベースを必要とする
- DNSSEC や S/so BGP がその例
  - 課題はやはり鍵管理に落ち着く
  - 運用上の問題が最大の問題
  - プロトコル仕様定義だけでは解決できない