経路情報の認証へむけて

石黒 邦宏

<kunihiro@digital-magic.co.jp>

今のままではよくないのか？

- Webは見れるし、メールはよめる
- 本も買えるし、空き家も探せる
- 分からないことは検索エンジン
- 最新ニュースもすぐに読める
- オークションや、個人売買の場もある
- NANOGにいけなくても後で見ることができる
- 仕事も増える

だからよくない。。。。。

- 突然インターネットがつながらなくなったら？
- それも、インターネットのすべてが機能を停止したら？
- 非常に困る。。。。。
- 実験ネットワークからインフラストラクチャーへ

かつて不幸な事故がありました

- 1997年　4月　AS7007事件
- 1997年10月　UUNET (AS701) 事件
- ルーティングメルトダウン
- BGPスピーカーは誰でも経路を突っ込むことができる
- 非常に効果的なDoS
- オペレータ側に事故を防ぐことのできる機構が必要

2つの方法

- DNSを使う方法
  draft-bates-bgp4-nlri-orig-verif-00.txt
- 経路レジストリーを使う方法
  RPSLで記述

DNSを用いた経路認証

- DNSの階層構造に割当構造を当てはめることができる
- これまで実績のあるDNSを用いるため新たな機構を導入するよりリスクが少ない
- 新たなリソースレコードASの導入
- 正確には経路情報のオリジンASの認証
- BGPで受け取った経路をDNSで認証する

卵が先かにわとりが先か

- DNSに問い合わせをするためには、まず経路情報が必要
- その経路情報を認証するためにDNSへの問い合わせが必要
- ｏｏｏｏｏｏ
- とりあえず、経路を受け取り、２４時間後に認証問い合わせをおこなう

どのように設定するか？

- bgp.in-addr.arpaドメインを使用か？
- アドレスの委任構造に沿ったDNSゾーン権限の委任
- 非オクテット境界の割り当ては、NSレコードとCNAMEレコードで解決する
- ASリソースレコードには、AS番号とプレフィックスを記述する

AS RR

- **記法**:

  <name>　AS　<AS number> <prefix length>

- **例**

  125.128.bgp.in-addr.arpa.　AS　47　16

- **プレフィックス**128.125/16 **は** AS 47**に割り当てられていることを示す**

特殊なAS番号

- AS 0
  - **未認証**
- AS 65535
  - **プレフィックスはアナウンスされてはいけない**
  - **認証失敗**

認証結果

- 未認証
- 認証
- 認証失敗
- オペレータは認証結果に対するアクションを定義できる

魔の設定例 (1)

- **プレフィックス**10/8 **が** AS 1**に割り当て**:

```
$ORIGIN   bgp.in-addr.arpa.
10            NS      ns1.as1.net
```

- AS 1 **は全体を集成し、**
  10.1/16**を** AS 2**に割り当て**:

```
$ORIGIN  10.bgp.in-addr.arpa.
@             AS      1       8
1             NS      ns1.as2.net
```

魔の設定例 (2)

- AS 2 は 10.1/16 で集成を行い10.1.128/19 をAS 3に割り当てる:

```
$ORIGIN    1.10.bgp.in-addr.arpa.
@          AS      2        16
128/19     NS      ns1.as3.net
128        CNAME   128/19.1.10.bgp.in-addr.arpa.
129        CNAME   128/19.1.10.bgp.in-addr.arpa.
...
159        CNAME   128/19.1.10.bgp.in-addr.arpa.
```

魔の設定例（3）

- **もし1つのオクテット中で複数の割り当てが行われた場合。。。。**

  128/17.1.10.bgp.in-addr.arpa.

  192/18.128/17.1.10.bgp.in-addr.arpa.

  224/19.192/18.128/17.1.10.bgp.in-addr.arpa.

  240/20.224/19.192/18.128/17.1.10.bgp.in-addr.arpa.

様々な側面

- セキュリティーはDNSSECでばっちりか？
- 5万個のUDP問い合わせがボーダールーター1台ずつにに発生する可能性がある
- 問い合わせを受ける側の負荷はだいじょうぶか？
- IXなどでは、100万クエリー以上が発生？
- IXにはキャッシュマシンが必要？
- そもそも皆設定するだろうか？

稼動に必要な条件

- AS RR をサポートした、DNSサーバー
- BIND 8．1．2はまだ未サポート
- AS RR の問い合わせをサポートした、BGPルーター
- 全世界のAS管理ドメインごとに、AS RRの設定がされていること

RRと比較したメリット

- すぐに動くことが期待できる
- DNS設定に関する知識が普及している
- 割り当て構造を反映した階層的な認証ツリーを構築することが可能
- 認証、未認証、認証失敗と3段階のステータスを持つ

RRと比較したデメリット

- 非常に多くの問い合わせが発生する
- UDPのタイムアウト管理（5万セッション以上？）
- プレフィックスのリストの作成は不可能
- ASをキーにした経路のLookupはできない
- ASマクロでのフィルターリングはできない
- named,ルーターのアップデートが必要

RRに登録されているプレフィックス数

1998･3

- RAdb 42775
- MCI 40233
- RIPE 17016
- ANS 9083
- Canet 9083