## ケーブル技術スタッフの機器チェック!

日々開発されるケーブルテレビ関連機器を、技術スタッフが厳しい目でチェック! 実用性に焦点を当てて報告します。

No. 56

# uRPF

豊島ケーブルネットワーク(株) 技術部 部長　上山裕史

**今回はuRPFの外部接続ルータとCMTSへの設定について紹介します。**

私たちケーブルテレビ局の技術者はISP(インターネット・サービス・プロバイダ)として顧客のセキュリティや自ネットワークからの不正パケットの送出を防ぐために不断の努力をしています。

今回はオープンリゾルバ(Open resolver)対策として、uRPF(Unicast Reverse Path Forwarding)の外部接続ルータとCMTS(センターモデム)への設定を紹介します。

オープンリゾルバは、ネームサーバへの攻撃手段として広く知られています。広く使われる原因の一つは、ソースアドレス(送信元)を偽造されたパケットをISPのネットワークが通してしまうことにあります。自ネットワーク発のパケットが、想像もしない外国のサーバに迷惑行為を働いて、クレームのメールを受けるということがあります。これを防ぐためuRPFをルータに設定します。

uRPFは、インターネットの世界で教科書にあたるBCP(Best Current Practice:最も優れた事例)のNo.84として、インターネット技術の国際標準を策定しているIETFのサイトに掲載されています。ここではIngress filtering(入り口でパケットフィルタの設置をして効果を得る方法)として紹介されています。

ケーブル局のHFC(光同軸ハイブリッド)方式の流合ノイズもIngress Noise(イングレスノイズ)と呼ばれ、「Ingress:ネットワークの入り口(ユーザ宅)」で発生するノイズです。uRPFを設定するルータを図1に示します。

複数のCM(ケーブルモデム)を束ねるセンターモデム(CMTS)と外部接続ルータに設定を入れます。図2が設定を反映させた様子を示します。設定が完了して数十秒がたてば、図3に示すようにshow ip interfaceコマンドでuRPFに違反するとして破棄(ドロップ)されたパケット数が表示されます。

このようにして設定が有効なことを確認することができます。他にshow ip trafficコマンドでも確認できます。以上のコマンドの設定はシスコ社のルータ、CMTSで設定を行いました。写真1、写真2に設定したルータとCMTSの外観を示します。

迷惑メールや不正パケットを出し続けるISPは特に欧米の大手ISPからは設備を損壊する恐れのあるものとして、入り口でパケットを遮断される可能性があります。そうなればユーザからメールが届かない、Web閲覧ができないといったクレームが出てきます。また、疎通を回復するために英語で膨大なやり取りを強いられ、自社設備の防止設定をすることが再開の条件であったりします。常に自ネットワークをクリーンに保つようにすることでこのような事態を回避できます。

ケーブル局の技術者はメールサーバやWWWサーバのアウトソーシング化でインターネットの知識が不要になることは無く、顧客へのサービス品質を上げるために自ネットワークのクリーン化を進めると同時に、ますますインターネットの知識が必要になっていくと考えます。

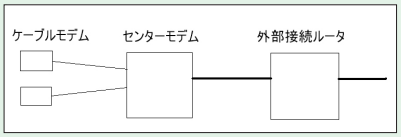


図1:設定するルータ

```
GW01(config)#interface GigabitEthernet1/1
GW01(config-if)#ip verify unicast source reachable-via any     <======  uRPF loose設定


GW01# show cef interface GigabitEthernet 1/1
GigabitEthernet1/1 is up (if_number 8)
  IP unicast RPF check is enabled                          <======  uRPF enabled
  Input features: Ingress-NetFlow, Access List, uRPF       <======  uRPF 反映された
```

図2:設定するコンフィグ

```
show ip interface gigabitEthernet 1/1
IP verify source reachable-via ANY
   24845 verification drops
```

図3:パケット破棄の確認

写真1:設定したルータ群

写真2:設定したCMTS群