ダウンロード・データあります

ご購入はこちら

パケットづくりではじめる ネットワーク入門

第61回 MACアドレス・フィルタにより不明な端末を遮断する

坂井 弘亮

本連載はネットワーク上を流れるパケットを直接扱うようなツールを自作しつつ，ネットワークの仕組みを勉強していきます．テーマは「自作」，「現物ベース」，「動く感動」の3つです．ネットワークにはイーサネットとIPを想定しています．

今回やること

前回は簡易L2スイッチに，タイマ処理の応用として，MACアドレスの学習テーブルのエージアウト処理を追加しました．

今回は登録したMACアドレスを持つ端末のみの通信を許可することで，未登録の端末の接続を無効化する機能として，MACアドレス・フィルタを追加してみます．

リスト1　MACアドレス・フィルタはMACアドレスが変更できるのでセキュリティを確保できるわけではないが誤接続防止は可能
ifconfigコマンドを使用すればネットワーク・インターフェースのMACアドレスを変更できる

```
# ifconfig em1
em1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric
                                              0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,
                   VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:11:c0:a8:01:01
        nd6 options=29<PERFORMNUD,IFDISABLED,
                                  AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT
                                    <full-duplex>)
        status: active
# ifconfig em1 ether 00:11:22:33:44:55
# ifconfig em1
em1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric
                                              0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,
                   VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:11:22:33:44:55
        nd6 options=29<PERFORMNUD,IFDISABLED,
                                  AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT
                                    <full-duplex>)
        status: active
#
```

MACアドレス・フィルタとは

● L2スイッチが備える不明な機器接続防止機能

多くのL2スイッチは，不明な機器を接続されることの防止策として，MACアドレスによるフィルタ機能を持っています．

これはあらかじめ登録されているMACアドレスの機器からの通信のみ転送し，送信元のMACアドレスが未登録の場合には通信を遮断するというものです．

具体的には，フレームの送信元MACアドレスを参照し，登録済みの場合は正常に転送し，未登録の場合にはフレームを破棄することで実現できます．

● 注意…セキュリティを確保できるわけではない

もっともMACアドレスは機器上で変更することが可能であるため，これは不正な端末の接続を完全に防止できるといったようなものではありません．

例えばFreeBSDでは，**リスト1**のようにしてifconfigコマンドで，ネットワーク・インターフェースのMACアドレスを変更することができます．

このようにしてMACアドレスを登録済みのものに変更されてしまった場合には，MACアドレス・フィルタ機能による遮断はできないため，無力です．

ただし，接続してはいけないPCを誤って(もしくは安易に)接続してしまったり，誤って別のポートに接続してしまうといったトラブルを避けることはできるでしょう．

このためセキュリティを確保するための機能というよりも，そうしたユーザの誤接続を防止するための機能と考えたほうがよいかもしれません．

簡易L2スイッチのプログラム

リスト2は，前回までに作成した簡易L2スイッチ(l2switch.c)に，MACアドレス・フィルタの機能を追加したものです．

なおこれは説明用の簡易的なサンプルです．そのた

本連載のプログラムのソースコードは以下の筆者のホームページからダウンロードできます．
ライセンスはKL-01というもので，組み込み機器などでも自由に利用できます．
http://kozos.jp/books/interface/ethernet2/