

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62回 簡易L2スイッチに認証機能を実装する

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。ネットワークはイーサネットとIPを想定しています。

### 今回やること

今回は簡易L2スイッチに、MACアドレス・フィルタの機能を追加しました。

今回は、MACアドレス・フィルタによるフィルタリング動作を応用して、簡易的な認証機能を追加します。

### 簡易認証機能の概要

#### ● MACアドレス・フィルタの機能を応用できる

特定のポートに不正なノードを接続されないようにしたり、接続による課金を計算したりするには、認証機能が必要です。高機能なL2スイッチであれば、そうした認証機能を持っていることが多いです。

認証機能は、MACアドレス・フィルタを応用して実現できます。標準ではMACアドレスの登録がないパケットをフィルタリングによって破棄します。新しいノードが認証されることでMACアドレスがL2スイッチに登録されればフィルタを通過し通信を正常に行えるようになります。

#### ● 簡易的な認証を行う

今回実装する簡易認証機能は、次のようなものです。

- 認証されていない状態では、MACアドレス・フィルタによりパケット破棄される
- 認証用パケットを受信すると認証され、そのMACアドレスがMACアドレス・フィルタに登録されてパケットが転送されるようになる
- 一定時間が経過するとタイムアウトし、登録されたMACアドレスが削除される

宛て先MACアドレス	送信元MACアドレス	タイプ	パスワード	...
イーサネット・ヘッダ(14バイト)				

図1 今回作成する認証用パケットのフォーマット

- 認証されている状態で認証用パケットを再度受信すると、タイマが更新される

認証用パケットにはパスワードを格納し、単純なパスワードによる認証とします。

#### ● 認証用パケットのフォーマット

認証用のパケットは、独自フォーマットとし、図1のようにしました。

今回の簡易認証は、パスワードは暗号化などせずにそのまま送っていて、フィルタリングもMACアドレス・ベースで行われるため詐称が可能で、セキュリティ的には大変弱いものです。あくまで認証動作の簡易的な実験のためのものと考えてください。

### 簡易L2スイッチのプログラム

#### ● 簡易認証の機能を追加

リスト1に示すのは、前回までに作成した簡易L2スイッチ(l2switch.c)に、簡易認証の機能を追加したものです。

本プログラムは説明用の簡易的なサンプルです。バッファやパケットのサイズ・チェックなどが省略されている部分があり、実際にはそれらのエラー対策が必要です。

#### ● 処理1: パスワードの設定

今回実装する簡易認証は、インターフェース単位で行われます。

このため261行目で、インターフェースのオプション領域にパスワード文字列を格納するためのメンバを追加しました。