

# 無線 LAN の基本と セキュリティ技術

長谷川 滋郎, 倉本 雅史, 渋谷 忠正

無線 LAN は、パソコンやゲーム機などで普及している。しかし、無線 LAN 接続機能を自分の設計する組み込みシステムに搭載する際には、いくつかの課題がある。ここでは、無線 LAN の基本と無線ならではの課題、および今後ますます重要度が増すと思われるセキュリティの考え方について解説する。  
(編集部)

## 1. 無線 LAN の基本

無線 LAN は Ethernet 相当の MAC 層プロトコル最近のパソコンやゲーム機は、当たり前のように無線 LAN 接続機能を搭載しています。ここで言う無線 LAN は、現時点では IEEE 802.11a/b/g として規格化されているものを指します。これは、ネットワーク・プロトコル(TCP/IP など)の下層に位置する MAC(Media Access Control)層のプロトコルです。

MAC 層のプロトコルとしては、Ethernet(IEEE 802.3)が有名です。無線 LAN は、Ethernet などのメタル(電線)接続と異なり、空气中を飛び交う電波にプロトコルを乗せて通信します。無線であることから Ethernet のようなメタル接続の通信と比べて、回線を維持するために考慮すべき事項が増えます。昨今、無線 LAN と同じような技術を用いた電力線搬送通信(PLC: Power Line Communication)なども使われ始めましたが、電波を介した通信の中では無線 LAN は、最適な MAC 層プロトコルの一つと言えます。

パソコンで使用するための無線 LAN のカードやモジュールが多数市販されています。筆者らは、Atheros Communication 社のモジュールを使って、組み込みシステムに無線 LAN 接続機能を付加しています。

### 無線 LAN の通信の流れ

ここでは組み込みシステムで使うということで、ステーション(Client)にフォーカスして話を進めます。

まず、無線 LAN の通信の様子を有線 LAN(Ethernet)

と比較してみましょう(表1)。

基本的にシーケンス4~6は、有線 LAN も無線 LAN も同じ処理になります。当たり前のことと言われればそれまでですが、これがネットワークの階層構造のすばらしい点です。MAC 層である有線 LAN、無線 LAN の概念は、ネットワーク通信の IP 層以上の概念とは独立して考えられるのです。

ここで、有線 LAN と違って厄介なのが、リンクの確立(シーケンス2,3)と、リンクの監視(シーケンス7,8)です。逆に言えば、無線 LAN としてはこれらリンクの状態保持を行うための処理が本質であるということになります。

メディアの品質、つまり有線 LAN で言うところのケーブルの品質の確保は、そのほとんどの部分をカードやモジュールの内部のチップが行います。ソフトウェア的に考えると、その品質に応じた通信状態を維持することが大切です。

以下では、このリンク状態の保持を行うための、ソフトウェアで考慮する必要のある項目をリストアップして検討してみます。

ビーコンを受信することで接続状態を検知

有線 LAN でリンクを張るハブは人間が目で見つけて探します。無線 LAN では AP(Access Point)が、その存在を示すパケットを定期的に出します。これをビーコン・パケットと言います。

ビーコン・パケットには、それがどのような AP であるかを示す以下の情報が含まれています。

- AP の暗号設定
- AP の伝送速度の設定



「無線 LAN 搭載」って意外と難しい

現在，組み込み機器において無線通信というと，IrDA や Bluetooth，無線 LAN などがあります．通信速度を十分に必要とする機器の場合，無線 LAN しか選択肢がない場合が見受けられます．しかし，無線 LAN を組み込み機器に搭載することは，現時点ではいろいろな意味でハードルが高い選択肢でもあります．

筆者らは，無線 LAN のドライバ・ソフトウェアを，μITRON などを使用している機器メーカーに販売するというビジネスを行っています．しかし，「ドライバを搭載したい」という引き合いに対して，実際に搭載までごぎつける件数はどうしても少なくなります．理由としては，システム要件やコスト，モジュール供給，認証といった問題が挙げられます．

システム要件

IEEE 802.11a/b/g などのモジュールの市場はパソコン中心です．パソコンが中心ということは，秋葉原などで簡単にモジュールを入手できるということなので，無線 LAN を採用しやすいとも考えられます．しかし，パソコンを前提としている以上，PCI，USB 2.0 などのインターフェースに接続することになります．この「入手しやすい」モジュールは，CPU パワーや消費電流を考えると，意外と組み込み機器には「組み込み」にくいものだったりします．

コスト

現在市場でシェアを占めている，実績のある無線 LAN コントローラ LSI のメーカーは，非常に激しい技術競争を行っています．そのためか，無線 LAN 対応 LSI の情報や，ドライバのソース・コードなどは，入手するのが非常に困難です．

また，LSI やモジュールに搭載されるファームウェアも頻繁に更新され，パソコン・ユーザにはダウンロードという形で最新版のファームやドライバが常に供給されている状態です．Windows 対応のドライバを組み込み機器用の OS に移植し，常に最新のドライバに対応していくのは至難の業です．

組み込み機器の構成や機能要件にもよりますが，通常，組み込み機器ですぐに動作する無線 LAN ドライバというものは

ありません．なんらかの移植作業が必要になる上に，その作業に必要な情報は非常に限られ，少ない情報に基づく移植作業には手間とコストがかかります．

上述のシステム要件についても，無線 LAN 搭載のために現状のシステムを変更しなくてはならないとすれば，大きなコスト上昇の要因となります．

モジュール供給

無線 LAN モジュールを「入手しやすい」と書きましたが，入手しやすいモジュールは，一般に製品寿命も短い場合が多いようです．また，製品としての型番が変わっていても，搭載された LSI が新しくなっていたり，見た目は全く変わらないのにファームウェアが更新されていたりします．もちろん，これらすべてにおいてドライバを修正しなくては動作しません．

Windows であれば，添付のドライバや Web サイトからダウンロードすることで対応できるので，逆にファームウェアなどは割と頻繁に更新されています．

このようなモジュール側の変更に追従するには，ハードウェアの安定供給，ファームウェア・アップデートのタイミングや方法について，モジュール・メーカーとの情報交換や取り決めが必要になります．

このようなモジュール・メーカーをうまく見つけられるかどうかは無線 LAN モジュール利用の一つの鍵になります．

無線認証

本文でも触れていますが，実は，筆者らが「組み込み機器に無線 LAN を搭載したい」と考えているメーカーを訪問したときに，もっとも多いのが認証に関する質問です．各国の電波法の解釈にはグレー・ゾーンも多く，非常に不安なところ です．

\* \*

以上，組み込み機器に無線 LAN 接続機能を載せることのハードルはいろいろとありますが，そもそも新しいインターフェースを搭載することは簡単にはいかないものです．今後も Wireless USB や高速 PLC といった高周波技術が広まっていくにつれて，避けては通れないハードルもたくさん出てくることでしょう．

表 1  
有線 LAN と無線 LAN の違い

シーケンス	有線 LAN	無線 LAN
1	ハブを幹線に接続する	Access Point( AP )を幹線に接続する
2	ケーブルで機器をハブに接続する	ステーションが適切な AP を探し出す
3	ハブとリンクが確立する	ステーションが AP にアソシエーションする
4	IP アドレスを割り振る	IP アドレスを割り振る
5	ARP パケットで相手を探す	ARP パケットで相手を探す
6	TCP/IP で通信をする	TCP/IP で通信をする
7	ケーブルが抜ける	ビーコンが途絶える AP が接続解除する
8	ケーブルで機器をハブに接続する	ステーションが適切な AP を探し出す

