連　載

セキュリティー機器やロボットを作ろう

# やってみよう！PICマイコン

## 〈第4回〉ワイヤレス施錠送信機の製作

落合 正弘
Masahiro Ochiai

無線LANやBluetoothなど，無線を使った通信が本格的に普及してきました．JR東日本のSUICAや電子マネーのEdyも非接触のICカードを採用しているので，広い意味で無線通信と言えるでしょう．

### ● 車のキーレス・エントリのようなものを作る

無線通信を行うには高周波の技術が必要ですが，より簡単に扱うことができる無線モジュールを使ってちょっとした無線通信を行ってみたいと思います．そこで今回と次回の2回に渡りPICマイコンを使った簡単なワイヤレス施錠装置を製作します．今回は**写真4－1**に示す送信器を作ります．

身近なところで車のキーレス・エントリを考えてみてください（**図4－1**）．キーに付いているボタンを押すと，車のドアがロックされ，もう一度押すとドアがアンロックされます．キーで操作できる車は1台であり，ほかの車のドアを操作することはできません．これと同じ機能を，PICマイコンを使って実現してみたいと思います．

受信器をドアや引き出しなどにセットしておけば，大事なものを守れるかもしれません．

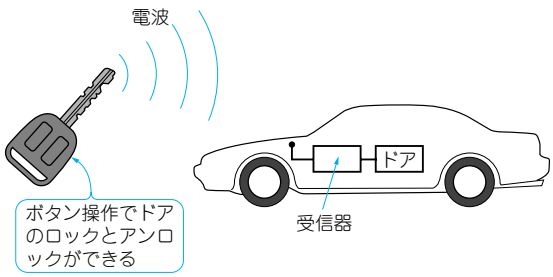
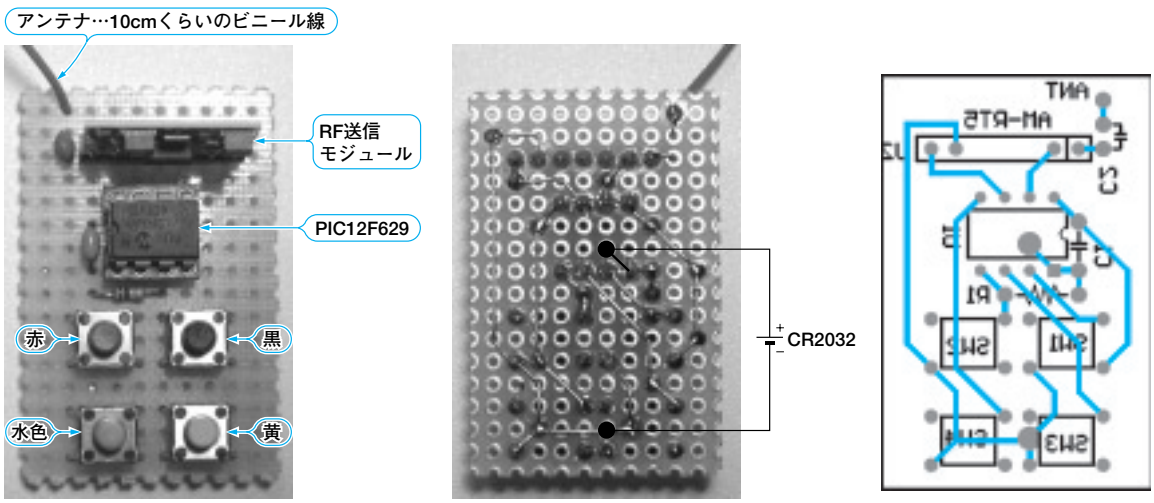



**図4－1　車の鍵の開閉を電波によって行うキーレス・エントリ**

## 製作のポイント

### ● コピーできないようにして安全性を高める

今回製作する回路は，基本的に赤外線を使ったリモ




（a）表面　　（b）裏面　　（c）裏面の配線図

**写真4－1　製作した送信基板の外観**

コンと同じ回路です．光を使っていないので，受信器のほうへ送信器を向ける必要はありませんし，途中に障害物があっても動作させることができます．逆にいえば隣の部屋からも動作させることができてしまいます．赤外線は障害物でさえぎられますが，電波は思わぬところまで届いてしまうことがあるのです．

**図4－2**のように送信器を操作している間に悪意をもった第3者にその信号の情報を読み取られてしまったとします．そうした場合，第3者がその信号とまったく同じ信号を発信する装置を使って受信器を動作させてしまうことが可能になってしまいます．クローンができてしまうというわけです．これでは安全とはいえません．実用にするには簡単に偽造やコピーができないように工夫を行います．

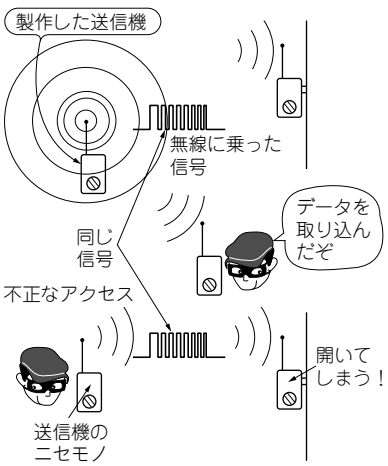



**図4－2　無線によるワイヤレス施錠装置**

### ● 偽造や不正操作を防止するチャレンジ・レスポンス方式の採用

不正操作を防止するには，いくつかの方法が考えられます．**図4－3**のように双方に送信と受信の機能をもたせ，はじめに受信側からランダムな数値を送信します．それを受け取った送信器は，その値に秘密の計算を行って，その結果を受信器に送信します．

図では2乗した結果の下4桁という演算を行っています．受信器側でそれを確認して認証します．そうすれば，飛び交う信号は毎回異なり，秘密の演算方法がわからなければ，解読できません．このしくみを応用したのがチャレンジ・レスポンス方式と呼ばれる方式です．

今回はこの方式をベースに独自の方式で暗号化を図ります．詳細は後述します．

## ハードウェアの製作

### ● 回路の製作

回路図を**図4－4**に，部品表を**表4－1**に示します．PICマイコンとボタン4個，無線送信モジュールだけの簡単な構成です．ユニバーサル基板を切って小さくまとめてみました．専用基板にすればキーホルダくら

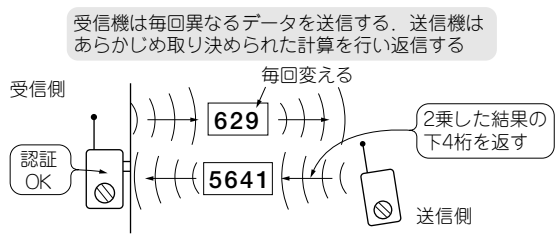



**図4－3　チャレンジ・レスポンス方式の通信プロトコル**

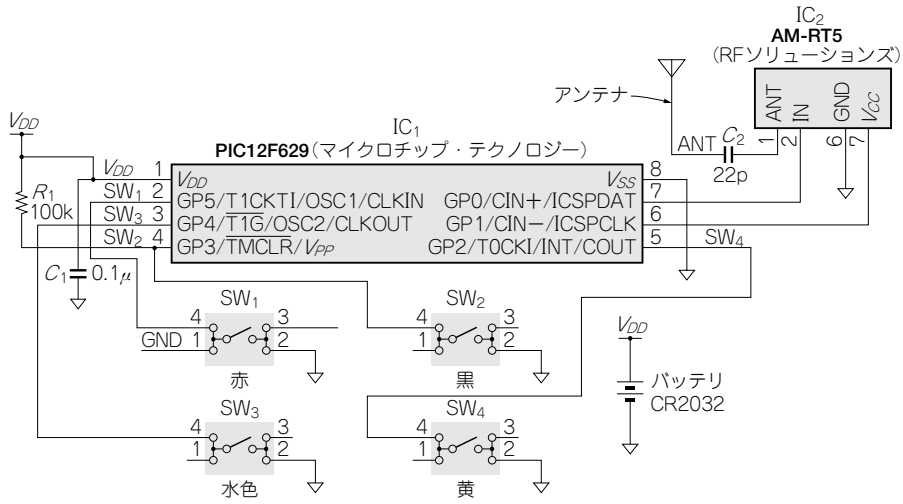



**図4－4　製作したワイヤレス施錠装置の送信部の回路図**