

## 振り込み詐欺抑止装置の試作 —2 GHz 帯電磁波の検波実験試論—

荻窪光慈 埼玉大学教育学部技術教育講座

キーワード：振り込み詐欺、携帯電話、電磁波、電気技術

### 1. 緒言

振り込み詐欺による被害が跡を絶たない。振り込み詐欺とは、いわゆるオレオレ詐欺（親族を装った電話をかけて様々な名目で現金が至急必要であるかのよう信じ込ませ、指定した口座に現金を振り込ませるなどの手口）、架空請求詐欺（架空の料金を請求して、指定した口座に現金を振り込ませるなどの手口）、融資保証金詐欺（融資を受けるための保証金の名目で、指定した口座に現金を振り込ませるなどの手口）、還付金等詐欺（税金や医療費の還付等に必要の手続きを装って、ATM（現金自動預払機）を操作させて指定した口座に口座間送金により振り込ませるなどの手口）の4種類の詐欺の総称である<sup>[1,2]</sup>。その特徴として、電話を利用すること及び虚偽の氏名や身分を騙って他人になりすますことの2点が挙げられる。

平成15年夏頃から目立ち始めた振り込み詐欺による被害は、表1に示すように、平成16年には認知件数約25,700件、被害総額約284億円とピークに達した。その後、認知件数は漸減したものの、被害総額については毎年250億円以上の被害が発生し、ほぼ横ばいの状況であったが、平成20年には、認知件数、被害総額ともに

増加に転じ、認知件数約20,500件、被害総額約276億円と、平成16年に次ぐ被害が発生している。今日に至るまでも被害は相次いでおり、状況は極めて深刻であると同時に、安心・安全な社会生活に対する重大な脅威となっている。

振り込み詐欺は、親や祖父母が我が子や孫を想う情愛につけ込んだり、公的機関の名を騙ったりするなど、家族や社会の信頼関係を逆手に取った極めて卑劣な犯罪である。被害者の中には、日々の生活資金やかけがえのない財産を根こそぎだまし取られるのみならず、そのために一家離散や自殺に追い込まれる人もいるのであり<sup>[1]</sup>、振り込み詐欺が到底許すことのできない犯罪であることは論を俟たない。

振り込み詐欺は、また、現代社会の利便性の盲点をついた犯罪でもある。すなわち、利便性と匿名性の高い現代社会に身を潜めた犯行グループが、携帯電話、ATMサービス、転送電話サービス、私設私書箱などの現代的な様々なツールを悪用して<sup>[1]</sup>、被害者と一切対面することなく犯行を遂げているのである。

では、振り込み詐欺において、被害者と対面することのない犯行グループが、どのようにして被害金入手しているのだろうか。図1に示すように、被害者が

表1 振り込み詐欺の被害状況の推移（平成16～20年）<sup>[1]</sup>

区分	年次				
	平成16	17	18	19	20
認知件数(件)	25,667	21,612	19,020	17,930	20,481
オレオレ詐欺	14,874	6,854	7,093	6,430	7,615
架空請求詐欺	5,101	4,826	3,614	3,007	3,253
融資保証金詐欺	5,692	9,932	7,831	5,922	5,074
還付金等詐欺	—	—	482	2,571	4,539
被害総額(億円)	283.8	251.5	254.9	251.4	275.9
オレオレ詐欺	191.3	128.6	146.8	145.3	155.2
架空請求詐欺	54.1	56.1	48.9	37.7	35.9
融資保証金詐欺	38.4	66.8	54.2	38.6	37.5
還付金等詐欺	—	—	5.1	29.9	47.4

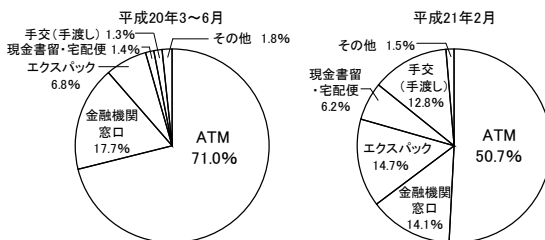


図1 振り込み詐欺における送金手段<sup>[1]</sup>

ら犯行グループへの送金手段としては、金融機関のATMを経由するケースが圧倒的に多い。その割合は、平成20年3月～6月には71.0%であり、送金手段が多様化した平成21年2月でも50.7%と過半を占めている。

送金手段としてATMが利用される場合、携帯電話が併用されるケースが少なからずある。すなわち、犯行グループは被害者に携帯電話を持参させ、ATMの前から電話をかけさせ、振込先の口座番号を指示する手口を用いる。そのため、金融機関や警察では、ATM利用者に対してATM付近での携帯電話の使用の自粛を促すなど、振り込み詐欺防止のための対策を講じており、一定の効果を挙げていると考えられるものの、被害金額の推移を見る限り、更なる対策が必要であると考えられる。

そこで本論文では、振り込み詐欺の被害をより一層低減させることを目的として、携帯電話の電波を検知して振り込み詐欺に対する警告メッセージを発することにより、振り込み詐欺への抑止力となる装置（以下、振り込み詐欺抑止装置と呼ぶ）を試作した。本装置をATM付近に設置することによって、携帯電話で通話しようとする被害者が、送金を行う前に振り込み詐欺に騙されていたことに気づき、振り込み詐欺を抑止するとともに被害者の財産を保全することができると考えられる。

## 2 振り込み詐欺抑止装置の設計

### 2-1 振り込み詐欺抑止装置の回路構成

振り込み詐欺抑止装置の機能ブロック図を図2に示す。まず、検波回路において、携帯電話で通話する際に発信される電波の存在を検出する。検波回路においては、電波を極めて微弱な電気信号としてしか検出できないため、次に、増幅回路においてその信号を、一般的な電子回路で信号の有無が弁別できる程度まで増

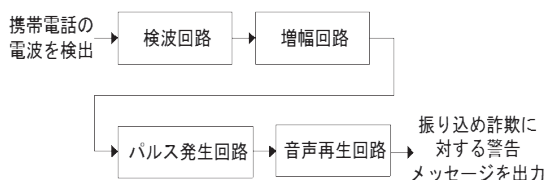


図2 振り込み詐欺抑止装置の機能ブロック図

幅する。更に、その信号を音声再生回路に入力することにより、携帯電話から発信される電波が検出される度に、振り込み詐欺に対する警告メッセージがスピーカから出力されるという構成になっている。

ただし、音声再生回路から警告メッセージが出力されている最中に、再度電波を検出した旨の信号が増幅回路から音声再生回路に入力されると、音声再生用ICの仕様により、警告メッセージが途中で終了したり、またメッセージの先頭から再生が始まったりしてしまうため、警告メッセージ出力中の音声再生回路では、増幅回路からの信号入力を受け付けないようにする必要がある。その目的で、増幅回路と音声再生回路の間にパルス発生回路を挿入した。

また、詳細は2-2(2)で後述するが、増幅回路の出力とパルス発生回路の入力の間、及びパルス発生回路の出力と音声再生回路の入力の間では、使用しているICの仕様のため、必要となる電圧信号の論理レベル（“High”または“Low”）が逆になっている。そのため、上記の各回路間に電圧の論理レベルを反転させるインバータ回路を挿入した。

以上の機能を満足する振り込み詐欺抑止装置の回路図を図3に示す。回路の電源電圧は、使用する各ICの仕様の範囲内で、かつ一般的な乾電池の電圧の整数倍となる6Vとした。

### 2-2 回路各部の設計と動作説明

#### (1) 検波回路

図3に示した回路図のうち、検波回路部を図4に示す。

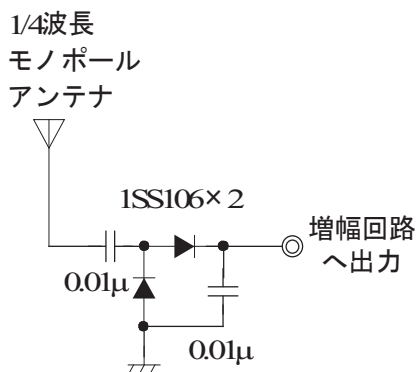


図4 検波回路

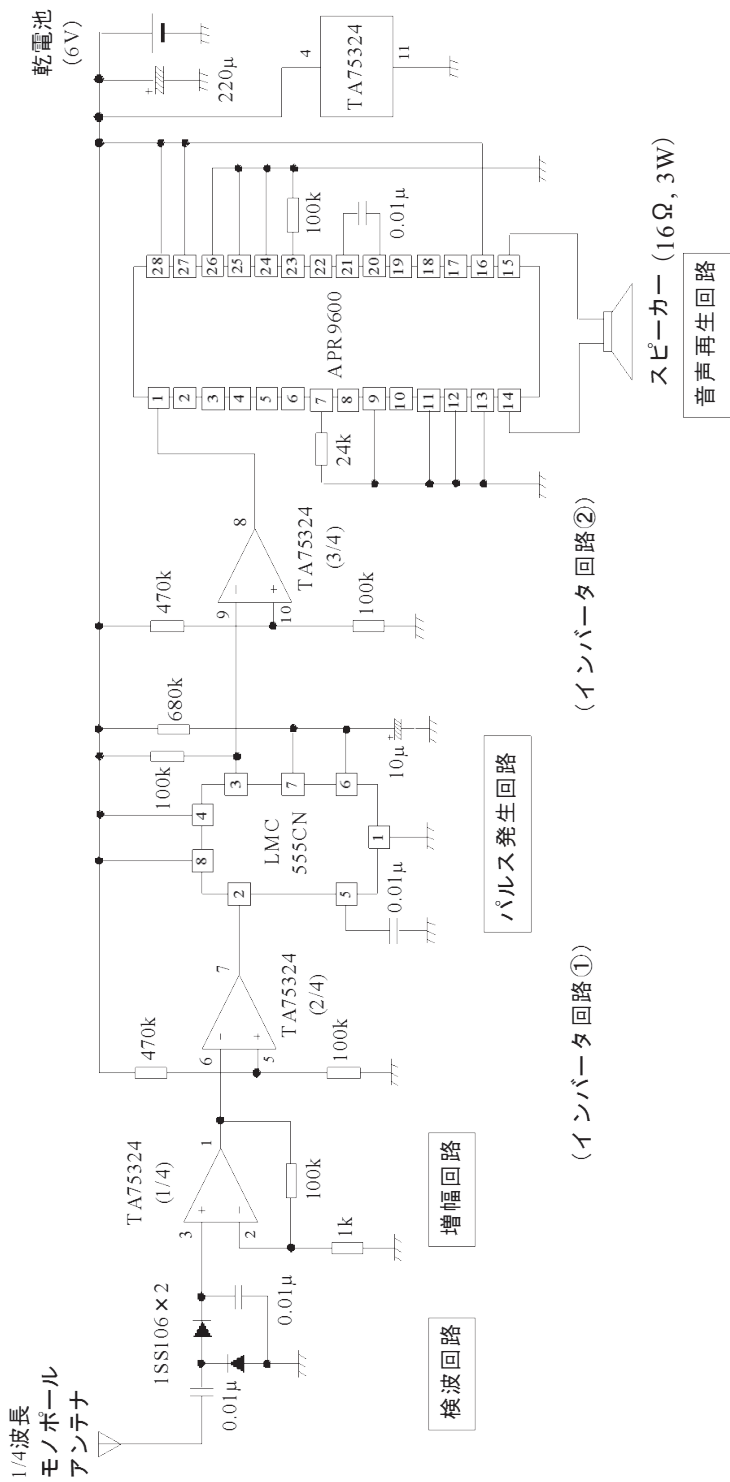


図3 振り込め詐欺抑止装置の回路図

検波回路では、携帯電話で通話する際に発信される電波を検出する。現在我が国で主流となっているいわゆる第3世代(3G)携帯電話端末においては、多くの場合その通信周波数として2GHz帯が使用されている。一般的に電波の検波と言うと、例えばラジオにおける検波回路に見られるようなコイルとコンデンサによる共振回路が思い起こされるが、本論文で扱う2GHz帯のような高周波になると、そのような共振回路では検波が不可能となってくる。なぜならば、2GHz帯の電磁波の波長は15cmであるが(波長 $L = \text{光速}c / \text{周波数}f = 3 \times 10^8 [\text{m/s}] / 2 \times 10^9 [\text{Hz}]$ )、コイルやコンデンサのような電子部品の実サイズが波長に比べて十分小さいとは言えなくなってくるため、本来の集中定数回路とは全く異なる分布定数回路としての挙動を回路が示してしまうためである。

そこで本論文では、2GHz帯の電波を捉えるためのアンテナとして、1/4波長モノポールアンテナを採用した。モノポールアンテナは、その簡便な構造のため、ダイポールアンテナと並んで携帯機器用アンテナ等としてしばしば用いられる代表的な電界検出型アンテナである。そのアンテナ長としては、電流もしくは電圧の最大値を給電点において得るために、波長の1/2もしくは1/4のものがしばしば用いられるが、本論文ではより小型化が可能な1/4波長を採用した。2GHz帯の波長は15cmであることから、本論文で用いた1/4波長モノポールアンテナのアンテナ長を約3.75cmと設定した。

アンテナで捉えられた電波は極めて微弱な電気信号であることから、それをより大きな電気信号として取り出すために、半波倍電圧整流回路を用いて検波することとした。半波倍電圧整流回路は、それぞれ2個のダイオードとコンデンサから構成され、出力電圧は入力電圧の2倍となる。ここで用いるダイオードとして、一般的なpn接合型の小信号用ダイオードは、順方向電圧 $V_F = 0.6\text{V}$ 程度と大きいため、微弱な電気信号に対する損失が大きく使用に適さない。そのため本論文では、順方向電圧 $V_F = 0.3\text{V}$ 程度と小さい小信号用ショットキーバリアダイオード(ルネサステクノロジ製1SS106)を用いた。

なお、ショットキーバリアダイオードと同様に低い順方向電圧を持つダイオードとしてゲルマニウムダイオードが挙げられるが、一般的にゲルマニウムダイオードはショットキーバリアダイオードほど周波数特性が良くない(例えば、代表例なゲルマニウムダイオード1N60の逆回復時間 $t_{rr} = 1\text{ns}$ である)ため、100MHz程度以下であれば実用的だが、2GHz帯では使用に適さないと考えられる。

また、半波倍電圧整流回路に用いるコンデンサの静電容量は、入力電波の微弱な電気信号に対する損失が十分小さくなるように、言い換えると2GHz帯における容量リアクタンスが十分低くなるように、 $0.01\mu\text{F}$ とした( $1/(2\pi fC) = 1/(2\pi \times 2 \times 10^9 \times 0.01 \times 10^{-6}) \approx 0.008\Omega$ )。

## (2) 増幅回路

図3に示した回路図のうち、増幅回路部を図5に示す。増幅回路では、検波回路の出力電圧を増幅して、一般的な電子回路で信号の有無が弁別できるようにする。

携帯電話の電波を検出することにより検波回路から出力される電圧は、条件にもよるが概ね20mV程度と非常に微弱である。したがって増幅回路において、オペアンプを用いてその電圧を一般的な電子回路で信号の有無が弁別できる2V程度まで増幅することとした。増幅回路としては、入力電圧が20mV程度するとき、出力電圧が2V程度になることを想定して、増幅度100倍(正確には101倍)の非反転増幅回路を用いた。ここで用いるオペアンプとしては、非常に微弱な正電圧のみの増幅を行うことから、負電源が不要で、かつ同相入力電圧範囲に0Vを含む動作が可能である単電源オペアンプ(東芝製TA75324、4回路入り)を用いた。このオペアンプの入力オフセット電圧は2mV程度である。したがって、今回設計した回路でも出力に現れる増幅されたオフ

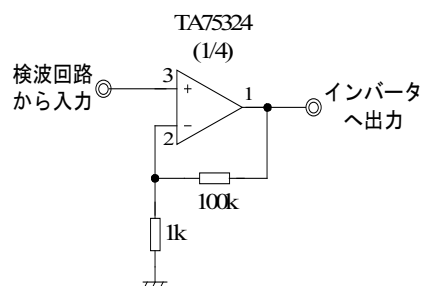


図5 増幅回路

セット電圧は0.2V程度であり、これは想定される出力電圧（2V程度）の10分の1にしかすぎないことから、オフセット電圧に起因する回路の誤動作はないと考えられる。なお、このオペアンプの出力電圧範囲は、最小値は0V、最大値は電源電圧-1.5V（本論文では6-1.5=4.5V）である。

なお、図2に示した機能ブロック図の通り、増幅回路の出力は、次にパルス発生回路に入力されるが、その際に、増幅回路の出力信号と次段のパルス発生回路への入力に必要な信号とで電圧の論理レベル（“High”または“Low”）が逆になっているという問題がある。すなわち、図6に示すように、増幅回路の出力信号は、電波を検出したときに“Low”レベルから“High”レベルに変化するが、パルス発生回路への入力には必要な信号は、パルス発生のために使用しているICの仕様上、“High”レベルから“Low”レベルに変化する信号が必要となる。そのため、電圧の論理レベルを反転させる図7のインバータ回路を、増幅回路の出力とパルス発生回路の入りの間に挿入した。インバータ回路としては、オペアンプを開ループ状態で使用したコンパレータ回路を用いた。すなわち、非反転入力端子に入力された電源電圧（6V）を470kΩと100kΩとで分圧した電圧（ $100k / (470k + 100k) \times 6 \approx 1V$ ）を基準として、反転入力端子に入力された

増幅回路の出力電圧をその基準と比較する。したがって、増幅回路出力が1V（検波回路出力10mVに相当）より高ければ、インバータ回路の出力はオペアンプの最小出力電圧（0V）となり、増幅回路出力が1Vより低ければ、インバータ回路の出力はオペアンプの最大出力電圧（4.5V）となり、電圧論理レベル（“High”または“Low”）の反転が実現される。

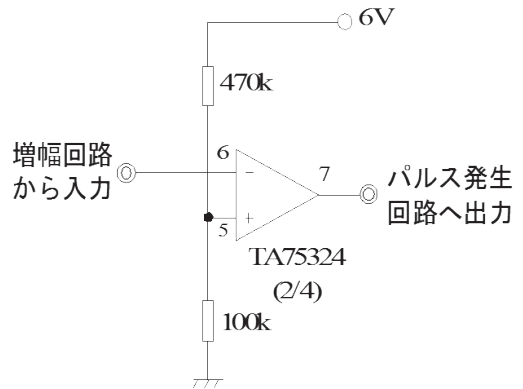


図7 インバータ回路

### (3) パルス発生回路

図3に示した回路図のうち、パルス発生回路部を図8に示す。音声再生回路に含まれる音声再生用ICの仕様

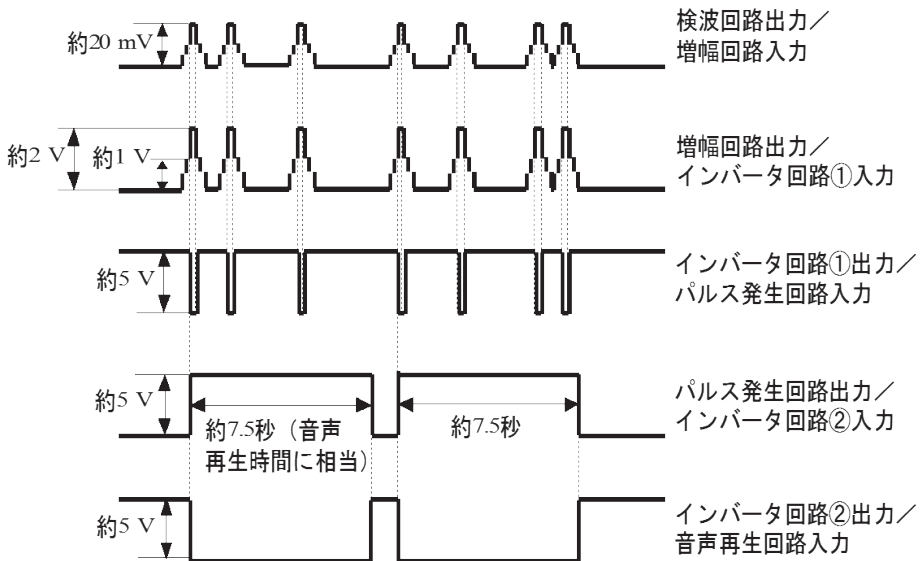


図6 各回路の入出力における電圧変化の概要

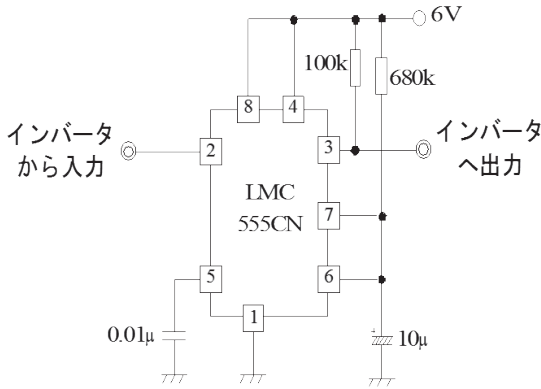


図8 パルス発生回路

により、音声再生を開始するためには、音声再生用ICの1番ピンに電圧の論理レベルの立下り（“High”から“Low”への電圧変化）を入力する必要がある。ところが、やはり音声再生用ICの仕様により、音声再生の最中に再度電圧の立下りが入力されると、そこで音声再生が停止してしまう。更に再度電圧の立下りが入力されると、先ほど途切れた箇所から音声再生が再開するのではなく、また先頭から再生が始まるというICの仕様になっている。したがって、増幅回路からの出力をそのまま音声再生回路に入力したのでは、電波を検出した旨の信号が増幅回路から音声再生回路に入力される度に、音声再生が停止を繰り返すこととなり、振り込め詐欺に対する警告メッセージとしての用をなさない。

そこで、警告メッセージを出力中の音声再生回路において、増幅回路からの信号入力を受け付けなくにする機能を持つパルス発生回路を、増幅回路と音声再生回路の間に挿入することとした。上記の目的を達成するためには、警告メッセージを出力中の音声再生回路において、音声再生用ICの1番ピンに電圧の論理レベルの立下りを入力してはならない。すなわち、警告メッセージを出力している間、音声再生用ICの1番ピンは、電圧を常時“Low”レベルに保っておく必要がある。

そのためのパルス発生回路部として、単安定マルチバイブレータ（ワンショットマルチバイブレータ）回路を用いた。すなわち、図6に示したように、電波を検

出した旨の信号が増幅回路からインバータ回路を経由してパルス発生回路へ入力されると、パルス発生回路から音声再生用ICの1番ピンに、振り込め詐欺に対する警告メッセージの再生に要する時間だけ電圧を“Low”レベル（0V）に保持する信号を出力することとした。したがって、一旦パルス発生回路出力から音声再生用ICの1番ピンに入力される電圧が“Low”になり、振り込め詐欺に対する警告メッセージの再生が開始すると、再生が終了するまでは電波を検出した旨の増幅回路出力信号は音声再生に影響しないこととなる。

図8に示したパルス発生回路の中核となる単安定マルチバイブレータ回路には、代表的なタイマICである「555」（米 National Semiconductor 製 LMC555CN）を用いた。このタイマICは、時間的精度の高いパルス信号を簡易に発生させる用途に向いており、単安定マルチバイブレータ動作または無安定マルチバイブレータ動作の2種類の動作モードでしばしば用いられる。

本論文では、単安定マルチバイブレータとして動作させており、その場合の一般的な動作及び使用方法については、図6及び図8に示した通りである。入力端子（2番ピン）に立下りパルスが入力されると出力端子（3番ピン）から一定時間“High”レベルを維持する立上りパルスが出力される。電源電圧 $-7$ 番ピン間の抵抗を  $R[\Omega]$ 、6番ピン $-GN$ 間のコンデンサを  $C[F]$  とすると、出力パルスが“High”レベルを保持する時間  $t_H$  は理論上  $t_H = 1.1 \cdot RC [\text{sec}]$  で表される仕様となっている。もちろん、出力が“High”レベルを保持している最中に入力に立下りパルスが入力されても、出力には何ら影響はない。なお、本論文では  $R = 680 \text{ k}\Omega$ 、 $C = 10 \mu\text{F}$  と設定しており、 $t_H \approx 7.5 \text{ sec}$  である。これは、今回録音した振り込め詐欺に対する警告メッセージの再生に要する時間にはほぼ等しい。

また、図6に示したように、単安定マルチバイブレータを用いたパルス発生回路の出力パルスは“Low”から“High”への立上りパルスであるが、次段の音声再生回路の入力には立下りパルスが必要となるため、パルス発生回路の出力と音声再生回路の入力の間にインバータ回路を挿入している。

#### (4) 音声再生回路



図3に示した回路図のうち、音声再生回路部を図9に示す。音声再生回路では、携帯電話の電波を検出した旨の信号が検波回路、増幅回路、パルス発生回路の3つ

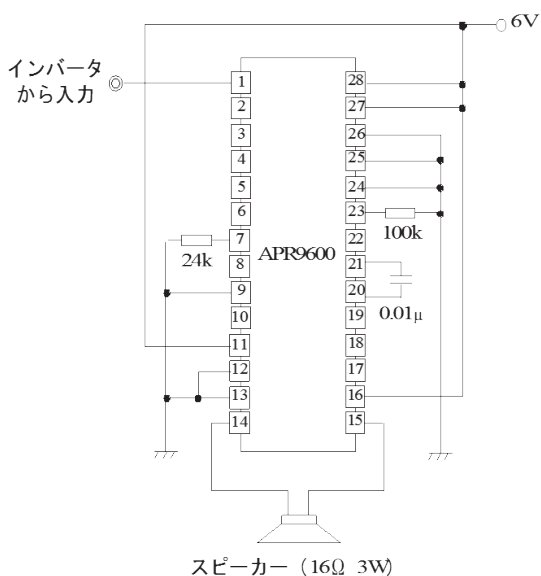


図9 音声再生回路

を経て入力されることにより、振り込め詐欺に対する注意を喚起し、ATM付近での携帯電話の使用の自粛を促す旨の警告メッセージがスピーカーから出力される。

音声再生回路では、その中核に音声録音・再生専用IC (台湾APLUS Integrated Circuits製 APR9600) を用いた。このICは、最大で8つの音声メッセージを合計60秒まで録音・再生できる機能を持つ。録音された音声データはIC内部の不揮発性メモリに記録されるため、ICへの電源供給がなくても音声データが消えることはない。本論文では、APLUS社から提供されているデータシートに基づき、回路を作成した。なお、今回用いたICへの音声メッセージの録音は事前に完了しているため、図3及び図9では、音声の録音に必要な回路は省略し、音声の再生のみに必要な回路を示している。

警告メッセージの再生は、音声再生用ICの1番ピンに電圧の論理レベルの立下り (“High”から“Low”への電圧変化) が入力されることにより開始される。先述したよ

うに、“Low”に変化した入力電圧は、警告メッセージの再生が終了するまで約7.5秒間保持され、警告メッセージの終了とはほぼ同時に“High”に戻る。その後再び携帯電話の電波が検出されれば、再度警告メッセージが再生されることとなる。

### 3. 振り込め詐欺抑止装置の製作

#### 3-1 振り込め詐欺抑止装置の組み立て

本論文では、ユニバーサル基板上に振り込め詐欺抑止装置の回路を組み立て、製作した。その外観を図10に示す。なお、大きさの比較のため、十円玉を基板近傍に配置している。

検波回路部の半波倍電圧整流回路については、極めて微弱な入力電波の電気信号を効率よく検出するため、2-2(1)で述べたように、2GHz帯の波長 (15cm) と比べて回路サイズがなるべく小さくなるように製作する必要がある。本論文では、中学校技術科などにおける教材化の可能性を念頭に置いて、はんだ付け等の製作作業の容易さを重視したため、チップ部品ではなくリード部品を用いたが、図11に示すように、約1cm四方以内に収まる回路サイズで製作を行った。

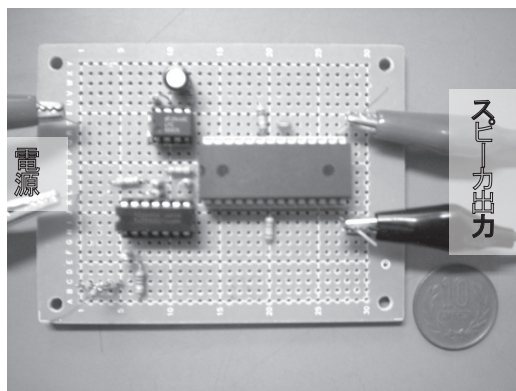


図10 振り込め詐欺抑止装置の外観

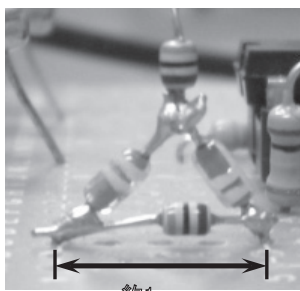


図11 検波回路部・半波倍電圧整流回路の製作例

使用した部品の価格としては、音声再生用IC APR9600 (参考価格380円) 及びスピーカ (同420円) が比較的高価ではあるが、その他の部品はある程度部品のまとめ買いをするという前提ならば、1個当たり数十円程度あるいはそれ以下であり、製作費用の概算は高く見積もっても1500円程度と極めて安価である。

### 3-2 振り込め詐欺抑止装置の動作

振り込め詐欺抑止装置と携帯電話が約30 cm離れている状態で、携帯電話をかけたところ、本装置から振り込め詐欺に対する警告メッセージが出力された。その際に、携帯電話から発信される電波を検波回路において検出・観測したオシロスコープ波形を図12に示す。

電波を検出したときの検波回路からの出力電圧は約20 mV～60 mVであることが観測され、回路設計時の目標とした20 mV以上となっていることが確認された。

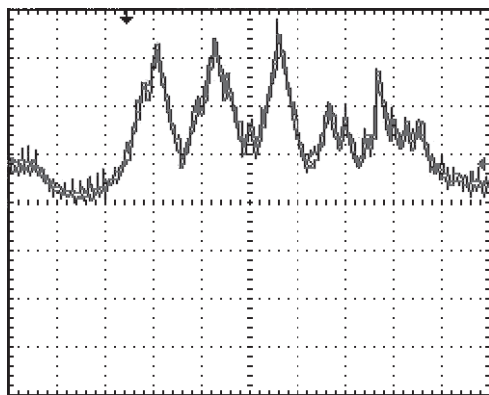


図12 検波回路における電波の検出  
(縦軸: 20 mV/div, 横軸: 10 ms/div)

### 3-3 考察と今後の課題

本論文で試作した振り込め詐欺抑止装置により、携帯電話から通話の際に発信される電波を検出して、振り込め詐欺に対する警告メッセージを発するという所期の目的を達成することができた。携帯電話の端末については、NTTドコモ、au、ソフトバンクの3社から発売されている第3世代(3G)携帯電話端末に関して、本装置がいずれも同様に動作することを確認した。

ただし、本装置の動作は、まだ限定された条件下でのみ可能であると考えられる。今後、本装置の更なる性能向上のため、少なくとも以下の2点について改善が必要である。

1点目は、振り込め詐欺抑止装置の検波感度の問題である。現状では本装置と携帯電話との距離が概ね30 cm程度までしか装置が正常に動作しない。それ以上離れると、携帯電話の電波を検出しにくいのである。この点は、アンテナの種類や形状を工夫するなどして、より長距離で使用可能となるべく感度向上に努めたい。また、目的とする2GHz帯の電磁波に対する感度の他に、選択性の問題も重要である。例えば、携帯電話以外の電磁波発生源 (例えば電子レンジ) が本装置の近傍にあると、その電磁波 (2.4 GHz 帯) を本装置が検出してしまい、携帯電話で通話していなくても本装置が動作してしまう可能性が考えられる。銀行等金融機関の店舗内の場合にはATMの近傍に電子レンジが存在することはまず考えられないが、例えばコンビニエンスストアの店内ではATMの近傍に電子レンジが設置してあることも考えられるため、周波数に対する選択性を高める、すなわち携帯電話で用いられている2GHz帯の電磁波のみを効率良く捉えることができるよう、アンテナ技術に工夫を凝らすことについても検討したい。本論文では電界検出型アンテナを用いたが、よりノイズの影響を受けにくい磁界検出型アンテナを採用することも一つのアイデアである。

2点目は、スピーカから出力される音声の問題である。現状では音量が十分ではないと考えられる。音声再生用ICからスピーカへの最大出力電力は12.2 mWしかないが、例えば、日中の街中にあるATMなどでは周囲の雑音がより大きく、振り込め詐欺に対する警告メッセージ



がATM利用者には十分届かない可能性がある。この点は、音声再生用ICの出力端子とスピーカの間にはアンプを挿入することにより、大音量化を図りたい。

なお、本論文における振り込め詐欺に対する警告メッセージは、あらかじめ音声再生用ICに録音専用回路を用いて録音されたものであり、本装置を用いて警告メッセージを新たに録音することはできない。今後、任意のメッセージを録音可能とする機能を付加したい。

#### 4. 結言

本論文で試作した振り込め詐欺抑止装置を使用した結果、本装置と携帯電話が30 cm程度離れていても、携帯電話から通話の際に発信される電波を検出することに成功し、振り込め詐欺に対する警告メッセージを再生することができた。本装置が、振り込め詐欺を抑止するきっかけとなり、卑劣な犯罪の被害者と加害者が一人でも多く減少する結果がもたらされれば、筆者にとって望外の喜びである。

本論文では、ATMにおける振り込みのまさに寸前で振り込め詐欺を抑止するための装置を、電気技術を駆使して試作した。本装置によって振り込め詐欺を抑止することに成功したとすれば、それは技術の勝利である。だが、それは問題を表面的にしか解決しない対症療法に過ぎない。

警察などの捜査機関においては、振り込め詐欺の抑止に向けて、2つの方向性で取り組みがなされている<sup>[1]</sup>。1つ目は「犯行ツールの一掃」である。第1章でも述べたように、犯行グループは携帯電話を始めとする現代的な様々なツールを悪用している。そこで、例えば携帯電話販売会社等の民間団体と協力して、一人当たりの契約台数の制限、契約時の本人確認の強化、契約者情報の共有による審査強化などを導入することにより、犯行ツールの調達に際してのコスト及びリスクを高め、振り込め詐欺を断念させる環境づくりへの取り組みが進められている。2つ目は「官民一体となった予防活動の推進」である。振り込め詐欺は、強盗や殺人と異なり、被害者が騙されることがなければ防げる犯罪である。したがって、銀行等金融機関やコンビニエンスス

トア事業者等の民間団体と協力して、第1章でも述べたようなATM利用者に対する声かけなどの注意喚起や窓口における本人確認の徹底を行うなど、国民全体の防犯意識を、絶対に騙されない水準まで引き上げる取り組みが進められている。このような警察と各種民間団体が協力した取り組みによって振り込め詐欺を抑止することに成功したとすれば、それは社会の勝利である。だが、問題の根本的解決には、まだ不十分であると考えられる。

問題を根本的に解決するためには、平然と他人を騙すことができる人間を生み出さないような環境づくりが大切である。それは、人間の心の問題であり、教育の問題に大きく関わっていると言える。

では、振り込め詐欺に手を染める犯罪者とは、どのような人間なのであろうか。全国都道府県の警察が2007年1月～2008年4月に逮捕した振り込め詐欺の容疑者568人のうち297人について、その容疑者像を警察庁が調査した結果が2009年に発表された<sup>[2]</sup>。刑法における推定無罪の原則により、必ずしも容疑者イコール犯罪者とは限らないことをあらかじめ断っておくが、この調査結果によると、297人中20代の若者が63% (187人)と極めて多く、30代(62人)と合わせると全体の84% (249人)に達する。この中には複数の現役大学生も含まれており、就学中もしくは学校教育を終えて間もない多くの若者が振り込め詐欺に手を染めている様子が窺える。また、逮捕時に無職の者57% (169人)に対し、何らかの職業に就いている者は43% (128人)と決して少なくない。更に、親や配偶者など家族と同居する者が47% (141人)とほぼ半数を占めている。これらの事実から、必ずしも職を持たない孤独な若者ばかりが振り込め詐欺に手を染めている訳ではなく、むしろごく普通の社会生活を送っている若者が、小遣い稼ぎなどの軽い気持ちから、大した罪悪感も無いままに犯行に走ってしまうケースの多いことが筆者には見て取れる。

以上の調査結果から、人が平然と他人を騙すことのできる人間になるかどうかは、その人に対する心の教育がしっかりと出来ているかどうかにかかっているのであり、そのような人間を生み出さない環境づくりは、家庭教育や学校教育を含めた教育界全体が総力を挙げ

て取り組まなければならない喫緊の課題であると思われる。

なお、先の調査では297人中、関東に居住する者は約68%(201人)と圧倒的に多い。関東地方に位置し、埼玉県を始めとして関東地方の教育界にも多くの人材を輩出している埼玉大学の責務は著しく大きいと言わざるを得ない。

今後、埼玉大学並びに教育学部における人材育成がより一層充実して、振り込め詐欺の撲滅に大いに寄与し、また、人類が英知を結集して、このような卑劣な犯罪行為に対する完膚なきまでの勝利を収める日が来ることを願いつつ、筆を置くこととする。

#### 参考文献

- [1] 警察庁：平成21年版警察白書、ぎょうせい、p. 1-11 (2009).
- [2] 法務省法務総合研究所：平成21年版犯罪白書、太平印刷社、p. 14-15 (2009).
- [3] 朝日新聞社：朝日新聞、2009年5月6日朝刊、p. 1, p. 34 (2009).

(2010年 9 月30日提出)

(2010年10月15日受理)

## **Development of the Device that Restrains Phishing Scams - Experiment for Detection of 2GHz Band Electromagnetic Wave -**

**OGIKUBO, Koji**

Faculty of Education, Saitama University

Phishing scams often occur every day, and it is still not showing signs of decline. The recognized number of criminal damage was about 20,500 and the amount of damage was about 27.6 billion Japanese yen in 2008. This is a very serious problem and a great pressure to the society. To reduce such social anxiety, the device that restrains phishing scams was developed in this study. The most important aim of this study is to detect the existence of the 2GHz band high frequency electromagnetic wave emitted from a mobile phone.

As the result of the production of the device, the expected detection of the electromagnetic wave from a mobile phone could be achieved within the distance of 30 cm at least. Further several improvements, e.g. the improvement in sensitivity of the antenna and so on, will be added to the device in the future.

Keywords : Phishing scam, Mobile phone, Electromagnetic wave, Electric and electronic technology