計測自動制御学会東北支部 第 254 回研究集会 (2009.12.17)
資料番号 254-6

キーボード入力情報の漏洩信号の電源線における電流分布の測定

Current Distribution Measurement of Leakage Signal of Keystroke Information on Power Line

○衣川昌宏*，林優一*，水木敬明*，曽根秀昭*

○Masahiro KINUGAWA*, Yu-ichi HAYASHI*,
Takaaki MIZUKI*, Hideaki SONE*

*東北大学

*Tohoku University

キーワード: 情報漏洩 (information leakage)，電源線 (power line)，電磁雑音 (electromagnetic noise)，情報セキュリティ（information security），キーボード（keyboard）

連絡先: 〒980-8578 宮城県仙台市青葉区荒巻字青葉 6 番 3 号 東北大学サイバーサイエンスセンター・本館・曽根研究室
衣川昌宏，Tel: (022)795-6094, Fax: (022)795-6096, E-mail: a9im4012@cs.he.tohoku.ac.jp

1. はじめに

情報処理機器に接続された電源線がアンテナとして動作し，処理情報を漏洩させることが指摘されている．[1]電源線は多くの電子機器に不可欠な部品であることから，この様な情報漏洩を引き起こすことで情報セキュリティを低下を引き起こし問題である．過去の研究 [2]では電源線がアンテナとして作用し，情報漏洩を引き起こす事が指摘されているものの，漏洩のメカニズムについては十分な検討がなされていない．そこで，本報告では，電源線によって引き起こされる情報漏洩のメカニズム解明のための基礎的検討として，電源線上の電流分布を計測することにより情報漏洩引き起こす周波数を決定する原因を明らかにする．また，情報処理機器の電源線のアース線をコンセントの接地端子に接続しない場合，アース線と電圧線およびアース線と中性線間に生じる漏洩情報を含む信号強度が増加することを考慮し [2]，アース線を開放した電源線による情報漏洩について計測する．

実験には，一般的な情報処理機器である PC（パーソナルコンピュータ）と PS/2 キーボードを用いた．情報漏洩信号（情報漏洩を引き起こす信号）は，PS/2 キーボードがキー入力情報を符号化しシリアル伝送を行う際に発生する電磁放射を対象とした．電源線はアース端子を開放した長さの異なる電源線を用いて，電源線長さによる情報漏洩信号への影響を測定した．情報漏洩信号の周波数特性の測定には，各電源線上の電流分布を電流プローブで測定を行い周波数解析を行うことで，その信号の周波数特性および電流分布を測定した．

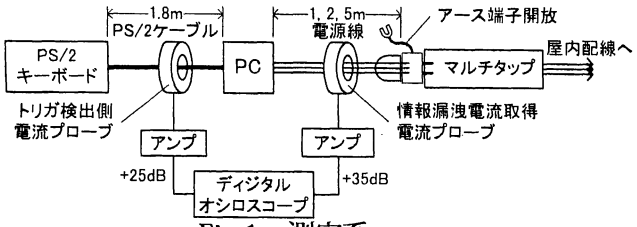

Fig.1　測定系

2. 実験

2.1 周波数特性の測定

本報告で用いた測定系を Fig.1 に示す．情報処理機器からの漏洩信号として，キーボード入力時に漏洩する情報漏洩信号を測定した．周波数特性測定には，PS/2 シリアル伝送信号のスタートビット立ち下がり時（Fig.4 の時刻 0 におけるデータ線の立ち下がり）に発生する情報漏洩信号を用いた．電源線上での情報漏洩信号の取得には，PC から 50 cm の点で電流プローブ（Fischer F-2000）を用いてオシロスコープで電流波形を取得した．電流プローブは，電源線全体および各導線（アース線，電圧線，中性線）をクランプし，それぞれについて電流波形を取得した．各導線上の電流が持つ周波数スペクトルは電流プローブ出力電圧を FFT（高速フーリエ変換）処理し，周波数パワースペクトルとして求めた．また，電源線の長さによる情報漏洩信号の周波数特性変化を測定するために，1, 2, 5 m の電源線を用いた．PS/2 キーボード，PS/2 ケーブルおよび電源線は床から 85cm，PC は床からの 88cm の高さに発泡スチロールブロックで直線上に固定した．測定環境を Fig. 2 に示す．

測定結果を Fig. 3 に示す．電源線全体は，電源線全体を電流プローブでクランプして電源線を構成する 3 芯の導線上の合計電流を示している．電源線全体をクランプした測定結果では強度およびスペクトル形状ともに変化はなかった．一方，アース線のみ信号電流解析した場合，ピークが現れる周波数は電源線の長さが長くなるほど，周波数が下がることが観測された．

2.2 電源線上の電流分布の測定

2.1 の実験で得られた，1m 電源線上の電流が

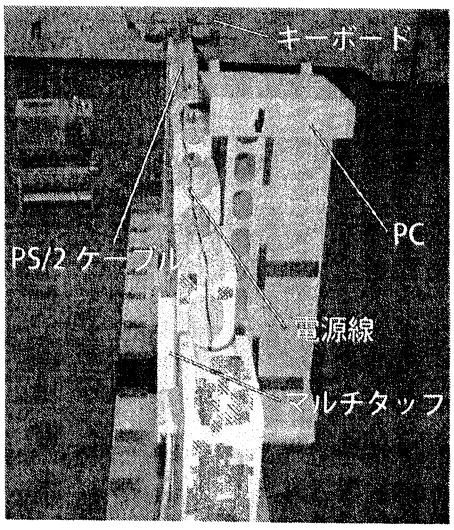

Fig.2　測定環境

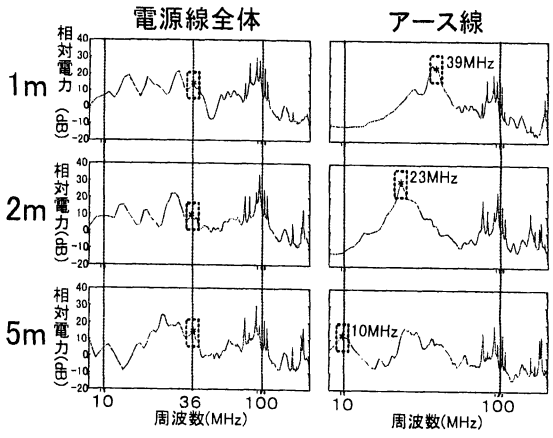

Fig.3　電線長を変化させた場合の周波数特性

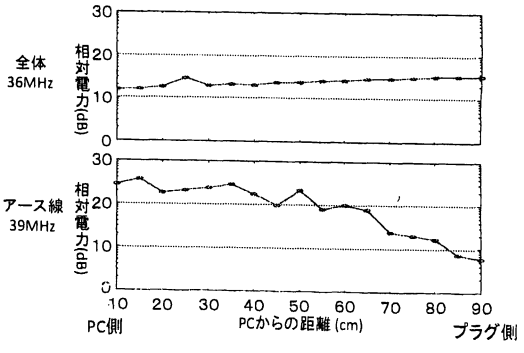

Fig. 4　電源線上の電流分布

持つ周波数スペクトルのピークについて，電源線上の電流分布を測定した．計測対象の周波数は，アース線上の電流では 39MHz に着目し，電源線全体については 36MHz に着目し測定した．測定範囲は，PC の電源線コネクタから 10cm 離れた点を起点として，5cm 間隔でプラグ手前 10cm までとした．

測定結果を Fig. 4 に示す．電源線全体で測定した 36MHz のピーク値は電源線の全範囲にお

いてほぼ変化は無い．しかし，アース線はプラグ側を開放しているため電流が流れず，プラグ側へ向かって電流の低下が発生していることが観測された．

2.3 ピーク周波数帯が持つ漏洩情報の比較

2.1 の実験で得られた電源線上の電流が持つ周波数スペクトルのピークにおいて，1m の電源線で現れたピーク周波数帯（電源線全体は 36MHz，アース線は 39MHz）について，それぞれの周波数帯に含まれる漏洩情報を比較した．漏洩情報の取得には，ピーク周波数中心とする 1MHz の帯域幅でピークレベルの時間変化を解析した．PS/2 キーボードのクロック周波数が 10～16KHz であることから，取得したピークレベルの時間変化波形に対して 20KHz のローパスフィルタを適用した．

解析結果を Fig.5 に示す．電源線全体で観測された 36MHz ピーク周波数帯および，アース線で観測された 39MHz ピーク周波数帯において，電流ピークレベルの変化として PS/2 シリアル通信のクロックに同期したパルスを取得することが可能であることが解った．また，データの立ち下がりに応じて Fig.5 内の点線枠に示す特徴的な波形変化も観測された．

3. 考察

2.1 および 2.2 節の結果から，プラグ端を非接地としたため，アース線においてはプラグ端を節とする定在波が生じていることが確認できる．このことから，アース線に生じる情報漏洩信号のピーク周波数は，電源線長によって決定される定在波が原因となり生じていることが明らかとなった．また，電源線全体を測定した際に生じているピークは機器依存の放射であることが明らかとなった．

さらに，2.3 節の結果はアース線に生じるピークの周波数帯域および，電源線全体に生じるピークの周波数帯域の両方から符号化されたキーボード入力情報を取得可能であることを示しているため，それら電流のピークは情報漏洩信号であることが明らかとなった．以上の結果から，機器依存の情報漏洩信号が持つ周波数スペクトルは攻撃者が事前に予測し観測することは困難である．そのため，電源線からの漏洩情報取得では，機器の物理的配置から推測可能な電源線長に依存するアース線上の定在波の波長を攻撃方法が有効であることが示される．そのため，電源線からの情報漏洩抑制には，機器からの放射を抑制するだけでなく，電源線のアース線に発生する定在波も抑制する必要がある．

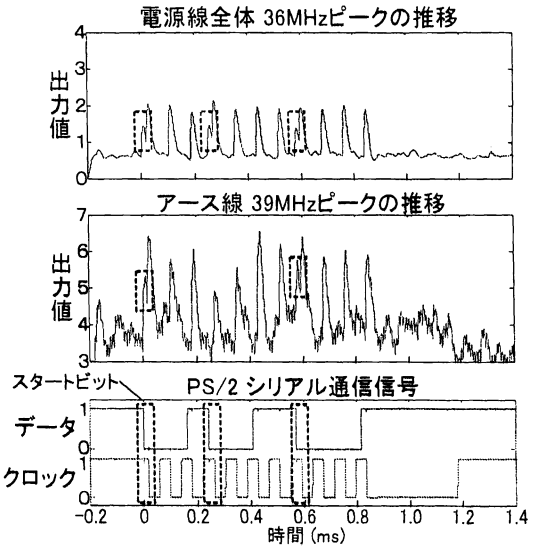

Fig. 5　ピーク周波数帯が持つ漏洩情報

4. おわりに

本報告ではキーボード入力に応じて電源線に生ずる情報漏洩信号の周波数特性を決定する原因を実験により考察した．その結果，電源線で放射される電磁波は機器依存の放射周波数特性と，アース端子が開放されているときに生じる定在波の周波数帯の 2 種類に分類できることを明らかにした．

参考文献

1) 関口秀紀，瀬戸信二: 電磁環境に起因する情報セキュリティ —IT 機器の emission と TEMPEST セキュリティ—，電気学会論文誌 A，129-1，1/6 (2009)
2) 衣川昌宏，林優一，水木敬明，曽根秀昭: 電源線のアース線が情報の機密性へ与える影響の測定，計測自動制御学会東北支部 45 周年学術記念講演会，1304, (2009)