3-13　端末からの漏えい電磁波の傍受による表示画面の再現実験

3-13 A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave

田中秀磨　滝澤　修　山村明弘
TANAKA Hidema, TAKIZAWA Osamu, and YAMAMURA Akihiro

要旨

ディスプレイなどの映像端末からノイズとして放射される漏えい電磁波を傍受することにより、表示画面を再現する実験を行った。パーソナルコンピュータを対象とし、以下の三つの手段を用いて表示画面の傍受を試みた。(1)近磁界プローブを端末に接触させた場合。(2)離れた場所からアンテナを用いた場合。(3)端末の電源ケーブルにインジェクションプローブをはさんだ場合。(1)の結果から、画面傍受が可能なだけでなく、ビデオ信号の同期周波数に関する個体ごとのわずかなばらつきによって、ターゲットの識別が可能であることを示す。(2)の結果から、VCCI で規制対象となっている 1GHz 以下の周波数でもターゲットから 4m 離れた場所から画面傍受ができることを示す。(3)の結果から、ターゲットから 30m 離れた電源ケーブルから画面傍受ができることを示す。

This paper describes the experiments and analysis of the interception of personal computer's display image using emanation of electromagnetic wave. We used personal computers as the targets and experimented on reconstruction of screen information under the following equipments and environments ; (1) using a near magnetic field probe, (2) using an antenna from away place, (3) using an injection probe over power supply cable. From the result of (1), we show that the slight difference in the synchronous frequency of video signal among PCs will become the key which recognizes the target. In the experiment (2), we succeeded from about 4 meters away place with frequency which is inside of VCCI regulations. In the experiment (3), we succeeded from about 30 meters away place.

[キーワード]
電磁波，傍受，テンペスト，セキュリティ，EMC
Electro-magnetic wave, Side-channel attack, TEMPEST, Security, EMC

1　はじめに

最近の暗号理論及び情報セキュリティ技術の研究では、通信路の盗聴以外の方法で機密情報を得る攻撃への対抗策に注目が集まりつつある。意図しない形で物理的に漏えいする情報を傍受したり、又は実装上の不具合を利用して秘匿情報を得たりする攻撃は、サイドチャネル攻撃(side-channel attack)と呼ばれる。サイドチャネル攻撃は、攻撃対象にアクセス手段を確保するか否かという観点による分類と、攻撃対象の本来の機能以外の挙動を起こさせるために破壊行為を加えるかどうかという観点による分類とがある[1]。サイドチャネル攻撃において攻撃者が利用する物理量は様々であり、消費する電力量、光、電磁波、超音波などが使われる。また、攻撃対象となる機器に対して接触をまったく行わない方法、機器そのものになんらかの細工を施す破壊的な方法及びその中間的な方法が存在する。このような攻撃を仮定する場合、観測可能な物理量を現実的な環境において測定し、その詳細を把握することは重要な課題である。Micali

とReyzinは、計算量理論に基づく安全性モデルと対比して物理観測攻撃を位置付け、物理的な情報漏えいに対する安全性モデルを定式化して提唱している[2]。彼らの目的は観測可能な物理量を仮定したときに、どのような暗号プリミティブを利用すれば安全な暗号通信が可能になるかを理論的な枠組みにおいて示すことである。そのような目的を達成するためには、観測可能な物理量を現実の環境において測定し確認することが必要となる。

パーソナルコンピュータ（以下、「PC」と呼ぶ。）のように高周波回路からなる機器からは、その動作に伴い電磁波が発生し、機器外へ漏えいする。漏えい電磁波が情報セキュリティに及ぼす脅威は二つ考えられる。暗号化処理中の信号を傍受されて暗号解析の手掛かりを入手される脅威と、暗号解析とは関係なく、より直接的にユーザの秘匿情報を傍受される脅威である。

本論文は、上記の後者に属する脅威の可能性に関する実験を行った結果について報告する。端末画面の傍受が可能であると、ネットワークにつながれていないPCからも機密情報等を傍受できることになり、ネットワークセキュリティ対策は無力となる。ブラウン管等に表示されている画面の傍受技術は古くから存在は知られているものの、その技術自体が一種の機密情報に属し、また、実験結果は機器や環境に大きく依存するため定量的な解析が困難であることもあって、具体的な測定値を含め詳細な手順と結果を明らかにした公刊文献は、これまでほとんど存在しない。具体的に漏えいするデータの質と量、実験装置、実験手法を明らかにすることは、MicaliとReyzinが提唱する物理観測攻撃モデルに沿った安全性を議論するために不可欠である。そこで本論文では、端末の画面を漏えい電磁波により傍受する手順について、実際の装置を用いた実験を行った結果を報告し、漏えいが起きる技術的原因、漏えいするデータの性質と量、攻撃にかかるコスト、それに対する対策のコストについての一つの指標となることを目指す。

2 漏えい電磁波に対する傍受の分類

漏えい電磁波による漏えい対象と傍受対象については、機器への情報の出力と入力に分類して、それぞれ表1と表2に示すようにまとめることができる[3]。表示画面だけでなく、キーボードの打鍵内容やプリンタの印字列等も傍受対象となり得る。このことは、例えば画面に現れないパスワードなども傍受の脅威にさらされることを意味する。

表1 出力情報の傍受

漏洩源	漏洩対象	脅威となる傍受対象例
PC、ケーブル、ディスプレイ	表示画面の内容	画面表示中の文書、メール本文など
プリンタ	印刷内容	印刷中の機密資料など
	印刷方式	印刷機材の機種情報など

表2 入力情報の傍受

漏洩源	漏洩対象	脅威となる傍受対象例
キーボード、ケーブル	打鍵内容	ログインID、パスワードなど
タッチパネル	座標値	タッチパネルによる選択、指定型の入力情報の再現など

PC等の情報通信機器における表示画面や打鍵信号は、マン－マシンインターフェースの最末端において直接人間と交わされる情報のため、暗号化は不可能であり、それらが電磁波として漏えいした場合は従来のセキュリティ保護技術では傍受を防げない。そのため、情報通信機器から漏えいする電磁波そのものを基準以下に抑えるといった機器の対策や、電磁波が建物外に漏れないように建物にシールドを施す対策、あるいは機器の設置方法を工夫するといった対策が提案されている[3]。

3 実験装置と傍受対象

我々は、表1の傍受のうち、PC端末からの漏えい電磁波を傍受し、その端末の表示画面を再現する実験を行う。本実験では、ROHDE＆SCHWARZ社製FSET22受信機（図1）とSystemWare社製の画像処理ソフトFrameControl ver. 4.24を用いた。受信機の仕様は表3のとおりである。FrameControlは受信機からの入力信号を256frames/3secで処理する能力を持ち、最大256フレームの画面を平均化することもできる上、画像処理をリアルタイムで施すこともで

きる。近磁界プローブとしてアンリツのMA2601B（周波数帯域：5MHz～1GHz）、アンテナとしてアンリツのMP666A対数周期アンテナ（周波数帯域：20～2000MHz）、インジェクションプローブとしてNECトーキンのEIP-100（周波数帯域：80KHz～30MHz）を用いた（図2及び3）。MA2601Bの磁界強度/測定電圧変換係数の値は、5MHzにおいて35dB、100MHzにおいて12dB、500MHzにおいて8dB、1GHzにおいて10dBである[4]。また、MP666Aについては、電界強度と測定電圧の変換係数が100MHzにおいて+3dB、500MHzにおいて－14dB、1GHzにおいて－21dBである[4]。

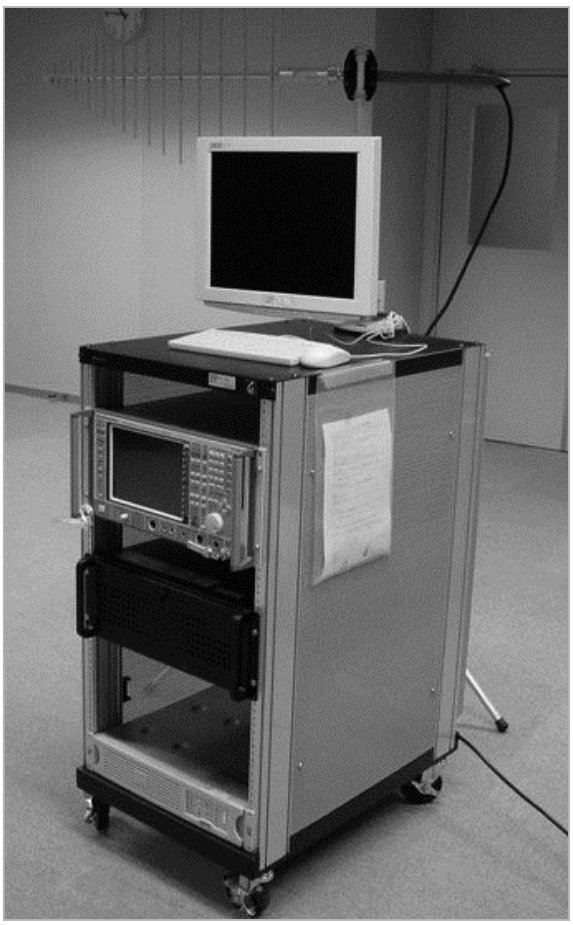

図1　実験に使用した受信機

表3　実験に使用した受信機の仕様

受信周波数帯	10Hz ～ 22GHz
周波数分解能	0.1Hz
バンド幅	100Hz ～ 500MHz
平均ノイズフロアレベル	-142dBm以下（1MHz）

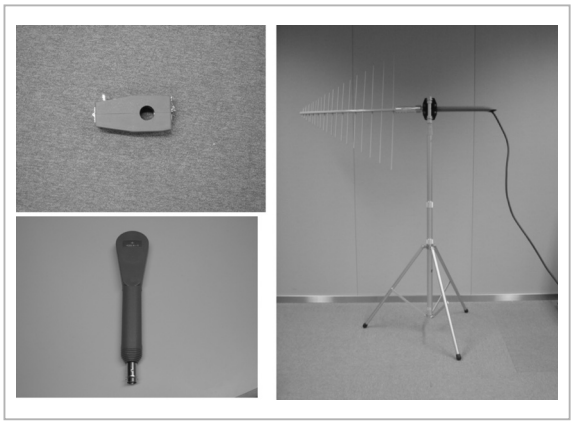

図2　使用機器
（左上）インジェクションプローブ
（左下）近磁界プローブ（右）アンテナ

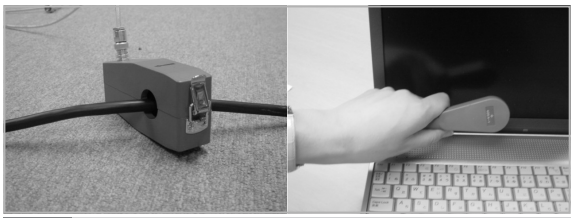

図3　使用方法
（左）インジェクションプローブ
（右）近磁界プローブ

今回の実験では、デスクトップ型PCとノート型PCを傍受対象とした。デスクトップ型では3種類のビデオカード（ATI社製Radeon 9700、NVIDIA社製Geforce2 MX/MX400 PCI、NVIDIA社製Geforce3 Ti500）と、マザーボードに直付け（Intel社製82845 G/GL）のものを合わせて合計4種類のビデオ信号処理ユニットについて実験を行った。以下ではビデオ信号処理ユニットを組み込んだテスクトップ型PCを「デスクトップPC」と呼び、ノート型PCを「ノートPC」と呼ぶ。ノートPCはSONY社製VAIO V505を対象とした。さらに、DELL社製16インチ液晶ディスプレイ（以下では「LCD」と呼ぶ）及びNANAO社製21インチCRTディスプレイFlexScan 77F 21（以下では「CRT」と呼ぶ）を使用した。なお、デスクトップPCは図4に示す画面を、ノートPCには図5に示す画面を表示させて、傍受対象とした。

図4 デスクトップ PC の傍受対象画面

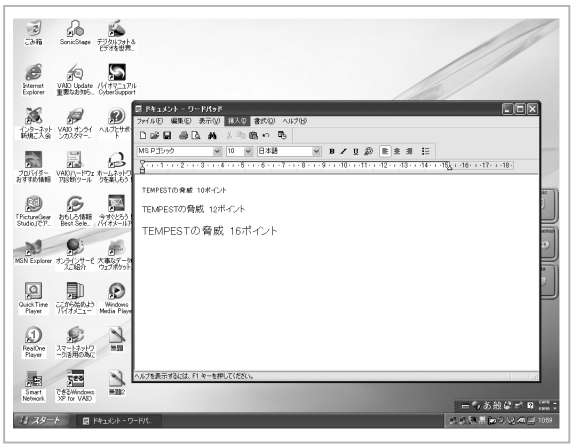

図5 ノート PC の傍受対象画面

4 傍受実験

4.1 各実験と使用した機材との関係

本節で述べる各実験と、使用した機材との関係を表 4 にまとめる。「＋」の記号は接続を意味し、例えば「デスクトップ PC+LCD」はビデオ信号処理ユニットを格納したデスクトップ型 PC を液晶ディスプレイに接続して実験を行ったことを示す。

デスクトップ PC を対象として、近磁界プローブ及びアンテナを用いた実験に関しては、デスクトップ PC+LCD の結果と、デスクトップ PC+CRT の結果とがほとんど変わらなかったため、本論文ではデスクトップ PC+LCD の結果についてのみ述べる（実験 A 及び C）。なお、実験は電波暗室のような電磁的に静穏な環境ではなく、通常の実験室で行った。

表4 各実験と使用した機材の組み合わせ

	デスクトップ PC+LCD	デスクトップ PC+CRT	ノートPC	ノートPC+CRT
近磁界プローブ(4.2節)	実験A		実験B	
アンテナ(4.3節)	実験C		実験D	
インジェクションプローブ(4.4節)	実験E	実験F	実験G	実験H

4.2 近磁界プローブを用いた接触傍受

表示画面を傍受するためには、後述するとおり、対象となる機器のビデオ信号の同期周波数を正確に把握する必要がある。同期周波数は機器固有の値であり、漏えいする電磁波の周波数帯には無関係である。そのため、本実験ではまず図 3 に示すように傍受対象とする機器の筐体に近磁界プローブを接触させて、同期周波数を取得する可能性を検証する。

以下では、ATI 社製 Radeon 9700 の場合について実験手順と結果を示す（実験 A）。

［手順－1］

同期周波数は、画面の広さと色数に応じて VESA 規格（Video Electronics Standards Association）で定まっている[5]。本実験では傍受対象の水平同期周波数を 64KHz、垂直を 60Hz に設定した。受信機の同期周波数も初期値としてこの値に合わせておく。

［手順－2］

傍受対象の機器筐体から強く電磁波が漏えいしている箇所を探すため、対象とする機器の各部位に近磁界プローブを近づけて測定する。その結果、顕著に電磁波が漏えいしていると思われる箇所として以下の傾向が見られた。

- 本体側のコネクタ付近
- ディスプレイ側のコネクタ付近
- ディスプレイのスイッチボタン近辺の隙間や液晶パネルのベゼル近傍

漏えいが顕著と思われる箇所を図 6 に示す。

［手順－3］

傍受に適した受信周波数を、傍受画面を目視することにより探索する。この段階では手順－1 において設定した同期周波数の調整は行わず、受信周波数だけを調整する。PC は様々な周波数

の電磁波を発しているため、画面を傍受するのに適した受信周波数として複数の候補が得られる。我々の実験結果では、近磁界プローブを用いた場合、500MHz～1GHz で画面の傍受に適した受信周波数が得られる場合が多かった。

［手順－4］

手順－3 において、ほとんどの受信周波数では、図 7 に示すように単なるノイズだけの画面であるが、特定の受信周波数において、傍受対象の表示画面の特徴を表した画面が得られる。ATI 社製 Radeon 9700 の場合は、530MHz 付近で現れた。最適な受信周波数に近づくと、図 8 のように同期がずれた画面が得られる。ただし、使用した実験装置では、色情報を再現する機能を有していないため、オリジナルがカラー画面であってもモノクロ画面として表示される。

［手順－5］

図 8 のように得られた画面は静止した状態ではなく、上下左右に流れた状態である。そこで水平同期周波数と垂直同期周波数を調整して静止させる。我々が用いた実験装置では、水平同期周波数を 10^{-6}KHz、垂直同期周波数を 10^{-6}Hz のステップで調整できる。ここでは、受信周波数の調整とプローブの接触に適した箇所の探索も併せて行う。さらに、画面をより鮮明化するため、傍受画面を複数フレーム受信して平均化する処理を行う。その結果、図 9 に示すような静止した傍受画面が得られる。この傍受画面の場合、10 ポイント以上のフォントサイズの文字の読み取りが可能であった。図 9 の中央にある黒い横棒の上は、Windows 画面の下側に配置されているタスクバーであるが、最右端にある時計の文字列も読み取りが可能であった。

［手順終］

以上の手順を、ノート PC に対しても行った（実験 B）。

ノート PC の場合、顕著に電磁波が漏えいしていると思われる箇所として以下の傾向が見られた。

- 液晶画面を開いた状態でキーボードの左上のヒンジの接合部分
- 液晶画面の左側のベゼル近傍
- ヒンジの裏側と液晶画面の裏側
- キーボード全面

漏えいが顕著と思われる箇所を図 10 に示す。また、傍受された画面を図 11 に示す。

以上の手順を経て、実験 A と B について得られた同期周波数を表 5 に示す。表 5 に示すとお

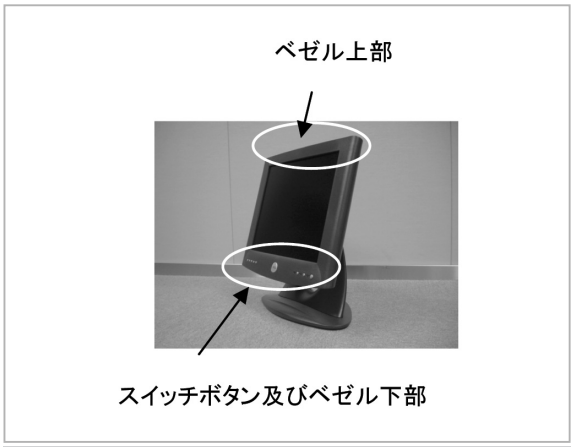

図6 液晶ディスプレイにおいて顕著に電磁波の漏えいが観測された箇所（白円の内側）

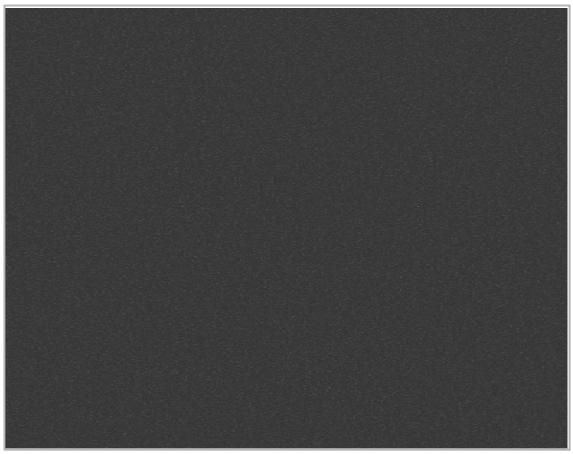

図7 同調前のノイズ画面

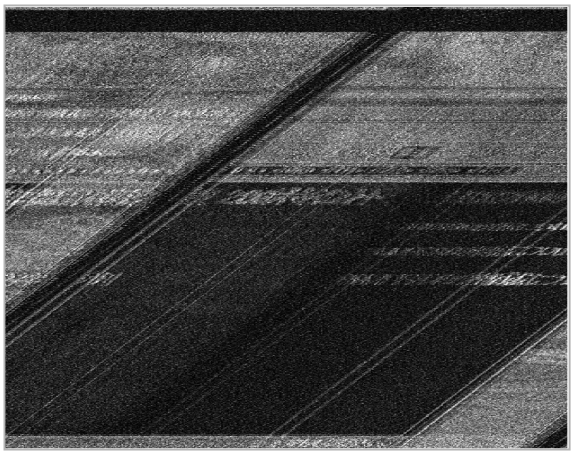

図8 同調後の傍受画面（未処理）

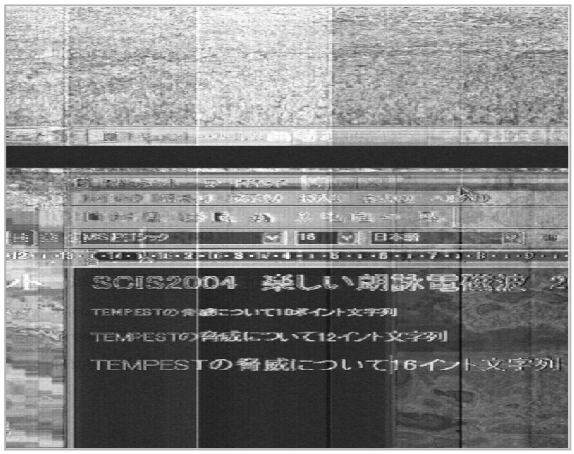

図9 実験 A における最も鮮明な傍受画面（32 枚の画面を平均化した結果）

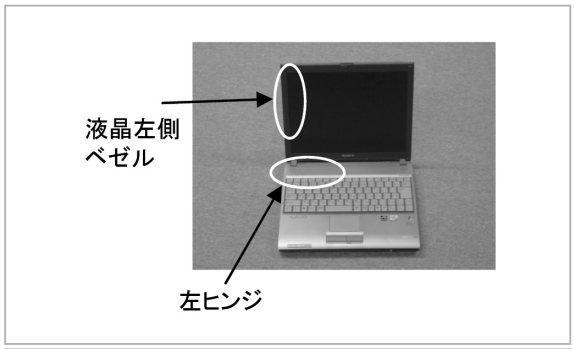

図10 ノート PC において顕著に電磁波の漏えいが観測された箇所

図11 実験 B における最も鮮明な傍受画面（32 枚の画面を平均化した結果）

り、測定された同期周波数にはわずかなばらつきがある。このばらつきは、構成部品の不均一など様々な要因によって生じるものと考えられ、各機器に固有で、時間的な変動は少ない値と見なせる。このばらつきは、通常の使用には全く影響を与えないが、漏えい電磁波による画面傍受においては、測定された同期周波数から小数点以下 2 桁程度以上のずれがあると同期が大きく狂い、傍受画面を視認できなくなる。以上のことは、漏えい電磁波による画面傍受のためには極めて精密に同期周波数を合わせなければならないこととともに、多数のコンピュータが同時に稼働している環境であっても、特定の一台の画面をねらって傍受することが可能であることを意味する。

表5 同期周波数の同調結果

	水平同期周波数[KHz]	垂直同期周波数[Hz]
Radeon 9700	63.892403	59.9362
Geforce2	63.953513	60.012
Geforce3	63.99952	59.9944
Intel 82845	63.974302	60.04
VAIO V505	48.338321	59.973150

4.3 アンテナを用いた空間放射の傍受

近磁界プローブにより正確な同期周波数を把握した後は、アンテナを用いた空間放射の傍受が容易になる。そこで次に、デスクトップ PC とノート PC に対する空間放射による画面傍受実験を行った（実験 C 及び D）。

図 12 に実験環境を示す。実験 C では、ビデオカードは ATI 社製 Radeon 9700 を使用した。表 5 で得た同期周波数である水平同期周波数 63.892403KHz、垂直同期周波数 59.9362Hz に受信機を合わせ、傍受対象とアンテナとの間の距離を 4m に設定し、画面の傍受を行った。傍受画面を見ながら、より鮮明な画面を再現できるように、傍受する周波数帯やアンテナの向きを調整した。図 13 に傍受画面の例を示す。実験 C の場合、傍受に最適な受信周波数は 919.9MHz 付近であり、9 ポイント以上のフォントサイズの文字が読み取り可能であった。

同様に、実験 D としてノート PC についても測定を行った。4m 離れた場所から傍受した画面の例を図 14 に示す。実験 D の場合、最適な受信周波数は 844.8MHz 付近であり、 9 ポイント以上のフォントサイズの文字まで読み取り可能であった。同じ実験 D において 6m の距離を置

いた場合の傍受画面の例を図 15 に示す。この場合の傍受に最適な受信周波数は 989.4MHz 付近となった。文字の読み取りは困難であったが画面の動的な変化、例えばアプリケーションの起動やスクリーンセーバーなどは認識可能であったため、使用者がどのような作業を行っているかを攻撃者は推測できた。

本実験では、デスクトップ PC に接続されているディスプレイが CRT でも LCD でも同じように傍受が可能で、どちらの場合も受信周波数は同じであった。また、傍受対象の方向へアンテナを向けても必ずしも鮮明な画面が得られるわけではなく、壁などで反射された電磁波を受信する方が鮮明な画面が得られる場合が多かった。そのため、傍受に最適なアンテナの向きを探索する際には試行錯誤を必要とした。

また、実験環境において人の出入りがあった場合、人の動きで傍受画面が乱れることもあった。特に、アンテナと傍受対象の間に人が入った場合は顕著である。情報処理装置等電波障害自主規制協議会（VCCI）[6]の規制対象となっている 1GHz 以下の電磁波については国内メーカ製の PC では漏えい電磁波が少ないと予想したが、1GHz 以下の周波数に同調させて画面を傍受できる場合もあった。このように、現時点での自主規制内の非常に微弱な電磁波でも画面傍受が行えることは注意を要する。なお、1.2GHz 近傍の周波数でも同様に画面を傍受できることを確認している。

図12 アンテナを用いた傍受実験環境（対象との距離は 4m）

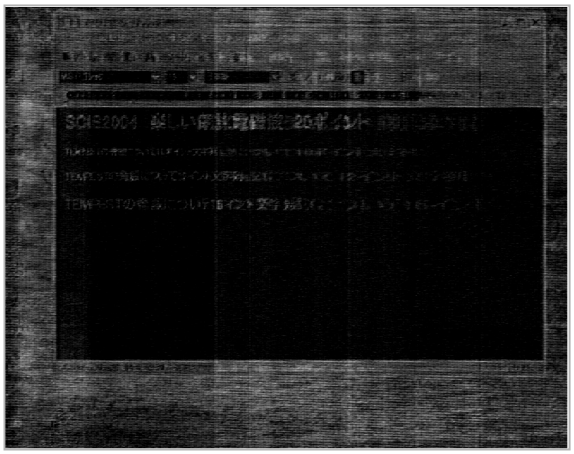

図13 実験 C における最も鮮明な傍受画面（32 枚の画面を平均化した結果）

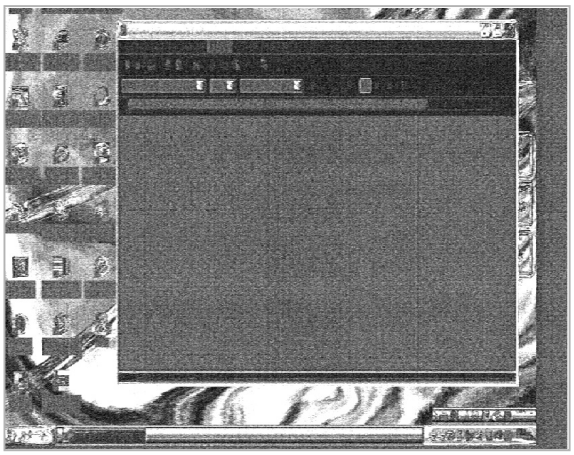

図14 実験 D における最も鮮明な傍受画面（距離 4m の場合）（32 枚の画面を平均化した結果）

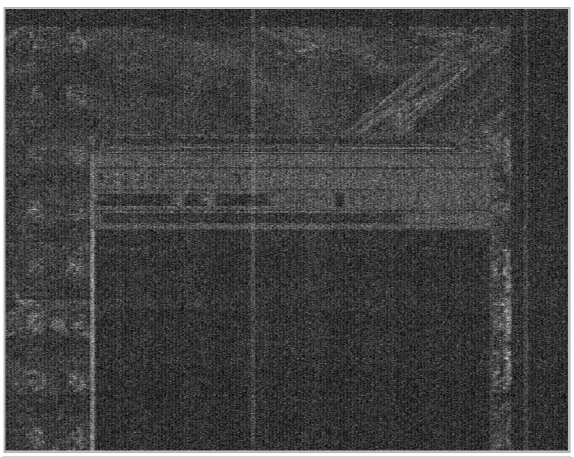

図15 実験 D における最も鮮明な傍受画面（距離 6m の場合）（32 枚の画面を平均化した結果）

4.4 インジェクションプローブを用いた電源ケーブル経由の傍受

本節では、インジェクションプローブをはさんで電源ケーブル経由の漏えいを傍受した実験を示す。空間放射とは異なり、ケーブル上を伝導しやすい電磁波は一般に低い周波数となる。そのため、前節まではおおむね 500MHz 以上の高い領域を傍受対象としていたのに対し、本節ではおおむね 30MHz 以下の低い領域を対象とする。

デスクトップ PC の場合、画面の出力先として LCD（実験 E）と CRT（実験 F）の両方を試みたところ、実験Eでは鮮明な傍受結果は得られなかったのに対し、実験 F では 20 ポイントのフォントサイズの文字がなんとか読み取れる結果が得られた

一方、ノート PC を対象とした場合（実験 G）、AC アダプタの位置関係により結果に違いがあった。プローブをはさむ位置関係は、図 16 に示すように、AC アダプタに対して条件Ⅰと条件Ⅱの二通りが考えられる。結果として、条件Ⅱの場合は傍受できたが、条件Ⅰの場合は可能な場合もあったが全く不可能な場合もあった。その原因として、AC アダプタ内において交流が直流に変換されるため、この変換過程で画面信号の電源側への漏えいが阻止されるアダプタもあると考えられる。そのため、アダプタとインジェクションプローブの相性の問題が生じたためと考えられる。

そこで、一般的なノート PC における妥当な使用方法と考えられる、PC からの画面出力を CRT に入力する使用法を想定した実験を行った（実験 H）。実験Hの実験環境を図 17 に示す。ここではノート PC 及び CRT に対して、30m の延長電源コードを介して電源を供給し、延長電源コードの壁コンセント側にインジェクションプローブをはさんだ。したがって、プローブは傍受対象から仮想的に 30m 離れた場所に配置したことになる。傍受画面を図 18 に示す。受信周波数は 23.8MHz であり、図 18 では 128 枚の画面を平均化して示している。12 ポイント以上のフォントサイズの文字が判別できた。また、スクリーンセーバーなどの動的な画面の変化は視認

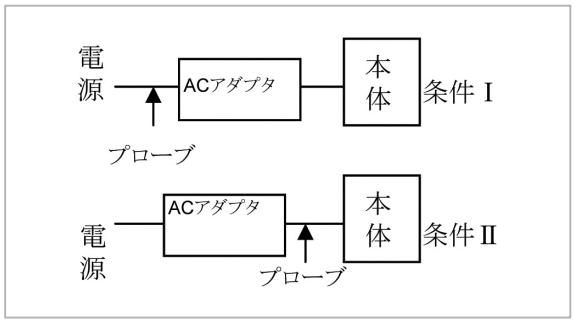

図16 AC アダプタとプローブの位置関係

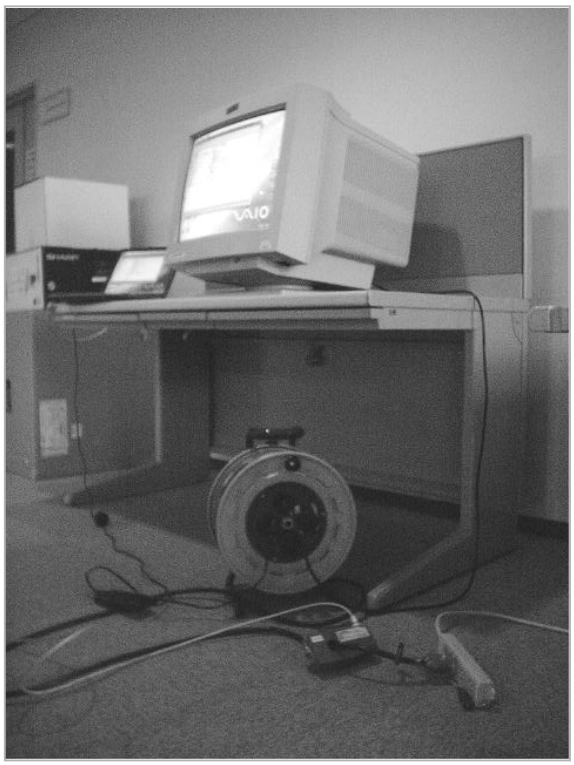

図17 実験Ｈの実験環境

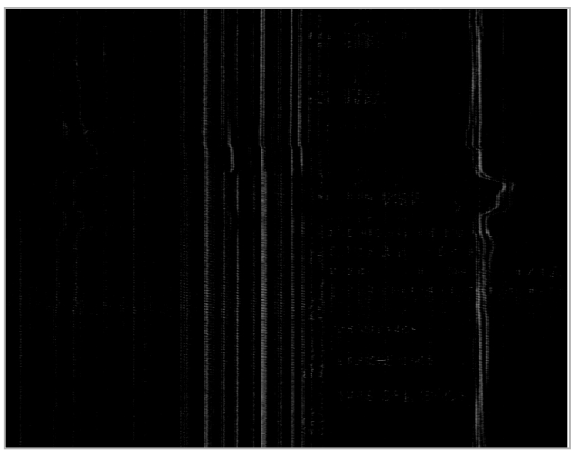

図18 実験Ｈにおける最も鮮明な傍受画面（128 枚の画面を平均化した結果）

できた。図 19 に、図 18 の右下部分を拡大して示す。数字やカタカナなど、特徴が大きく出やすい文字なら読み取れることを示す。なお、図 17 では延長コードを巻き取っているが、延ばした状況でも得られた傍受画面の鮮明さは変わらなかった。

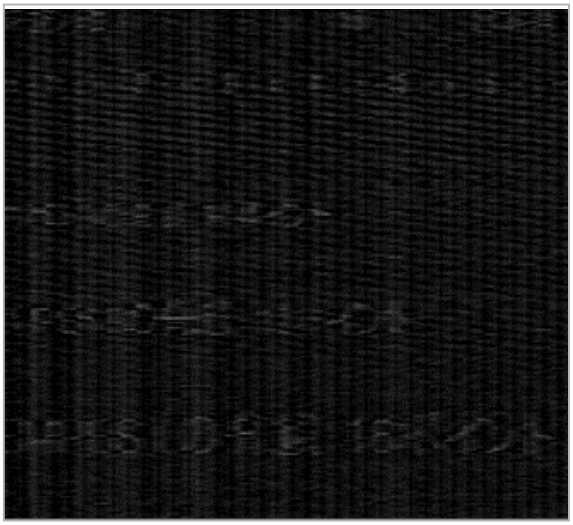

図19　図 18 の拡大画面

5　考察

4 で示した漏えい電磁波を用いた画面傍受の実験結果から、受信技術に関して以下のことを明らかにした。

- 電磁波が漏えいする箇所は、対象の筐体の材質と形状により変化する。
- CRT と LCD の違いは、傍受の困難さに影響を与えない。
- 傍受の困難さの観点からはデスクトップ PC とノート PC において差はない。

ビデオ信号の同期周波数は、表示される画面の大きさと色数に応じて VESA の仕様で決定される。この同期周波数の値について、以下のことを明らかにした。

- 仕様の値と比較して、わずかなばらつきがある。
- 同期周波数のばらつきは機器固有であり、これにより傍受対象となる PC を弁別することが可能

である。

また、傍受する電磁波に関しては、以下のような特性を明らかにした。

- VCCI 規制内である 1GHz 以下の微弱な電磁波でも傍受可能である。
- 電源線からも傍受可能である。

ただし電源線を利用した場合は、傍受の対象とプローブの間に AC アダプタなどがあるノート型 PC や液晶ディスプレイを対象とする場合はアダプタとプローブの相性問題などに成否が依存する傾向があるが、一般的なデスクトップ PC や CRT の場合であれば比較的遠方や障害物に無関係に傍受することが容易であり、それゆえに現実的な脅威になりやすいことが分かった。

表 6 に、各実験の難易度と脅威の関係を整理して示す。「◎」は、文字の読み取りが異論なく可能と思われる傍受画面が得られたことを示す。「○」は、実験者には文字の読み取りが可能と思われる傍受画面が得られたことを示す。「×」が文字の読み取りができなかったことを示す。「○／×」は図 16 で示した AC アダプタとプローブとの相対的位置関係によって異なる結果が得られたことを示す。「—」は実験を行わなかったことを示す。画面傍受において文字の読み取りが可能か否かの評価は、文脈や予備知識に影響され、客観的には難しい。本研究は第三者が再現実験を行えることを目指して実験方法を具体的に示すことをまず目標としたため、表 6 の結果は実験者自身による主観的な評価にとどまっているが、今後は特に「○」の結果が得られた実験を中心に、客観的な評価方法を検討する必要があると考える。

表 6 に示すように、インジェクションプローブを用いた場合、例えば同一の変圧器下であれば別室であっても画面の傍受が可能であると考えられ、ATM や電子投票機など固定された機器の傍受が可能であるため、最も現実的な脅威度が高いと考えられる。次いでアンテナを用いた

表6　各実験の難易度と脅威の度合い

	PC+LCD	PC+CRT	ノート	ノート+LCD	ノート+CRT	脅威
近磁界プローブ	◎	◎	◎	—	—	低
アンテナ	◎	◎	◎	—	—	中
インジェクションプローブ	×	○	○／×	○／×	○	高

画面傍受も脅威と考えられるが、アンテナの大きさは受信周波数に依存するため装置が大がかりになり、また障害物の影響を受けやすい困難さがある。近磁界プローブを用いた場合は、容易に鮮明な傍受画面が得られる反面、プローブを対象機器に接触させる必要があるため、現実的な脅威としては想定しにくい。このように、現実的な脅威の大きさと得られる画面の鮮明度とはおおむね反対の関係があるといえるが、いずれの場合も現状の技術で画面の傍受が可能であることを示し、電磁波受信技術や画像処理技術の今後の進歩に伴い、漏えい電磁波による画面傍受への対抗策は重要になってくると結論付けられる。

6 おわりに

本論文では、これまで具体的にはほとんど明らかにされていなかった、漏えい電磁波を通じて端末の表示画面を傍受する可能性について、実験の装置、手順、結果の具体例を示した。画面傍受の結果は装置を含む実験環境に依存するため、本論文では少ない傍受対象による定性的な評価にとどめたが、第三者が再現実験を行える程度まで具体的に実験概要を示したことに本論文の意義があり、本論文の結果は漏えい電磁波傍受対策に関する研究の発展に寄与すると考える。

参考文献

1 J.J.Quisquater and F.Koeune, "Side Channel Attacks", CRYPTREC Report 1047, 2002. (available at http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf)
2 S.Micali and L.Reyzin, "Physically observable cryptography", Theory of Cryptography Conference 2004 (TCC2004), Lecture Notes in Computer Science, Vol.2951 Springer-Verlag, pp.278-296, 2004.
3 IST(Information Security Technology Study Group)研究会，新情報セキュリティ技術研究会(IST)報告書，2002.
4 アンリツ株式会社，RF/マイクロ波用測定器カタログ，2004.
5 http://www.vesa.org/, 2004.
6 http://www.vcci.or.jp/, 2004.

田中秀磨（たなかひでま）
情報通信部門セキュリティ基盤グループ研究員　博士(工学)
暗号理論、情報セキュリティ

滝澤　修（たきざわ　おさむ）
情報通信部門セキュリティ高度化グループ主任研究員　博士(工学)
コンテンツセキュリティ、非常時防災通信

山村明弘（やまむらあきひろ）
情報通信部門セキュリティ基盤グループリーダー　Ph.D.
暗号理論、情報セキュリティ