

PCから放射される電磁波による 情報漏洩への対策技術

PCなどの電子機器が動作時に放射する微弱な電磁波には、さまざまな内部の電子情報が含まれており、実際にこの漏洩電磁波を傍受して、PCのディスプレイ画面を再生することが可能です。本稿では、こうした電磁波による情報漏洩から重要な情報を守り、セキュリティを確保するための、電磁波漏洩対策技術を紹介します。

すずき やすなお ますぎ まさお
鈴木 康直 / 馬杉 正男
たじま きみひろ やまね ひろし
田島 公博 / 山根 宏

NTT環境エネルギー研究所

電磁波セキュリティとは

通信装置やPCなどの電子機器からは絶えず不要な電磁波が放射され、周囲に影響を与えています。また逆に、その環境に存在する電磁波により、機器やその動作に影響を受ける場合もあります。

これらの現象を悪用すると、例えば電磁波の成分として漏洩した電子データを読み取ったり、強い電磁波を機器に照射して誤動作、故障を引き起こすなど、さまざまなセキュリティ侵害行為が可能となります。このようなセキュリティ問題を総称して、電磁波セキュリティと呼んでいます。

漏洩電磁波による情報漏洩

近年、電子回路の飛躍的な性能の向上やデータ処理容量の増大により、取り扱う信号は高速化し、これに伴って放射される漏洩電磁波の周波数も広帯域化してきました。

これらの漏洩電磁波には、機器の内部で取り扱われる電子情報が含まれています。近年の無線受信機の高性能化や信号処理技術の進歩により、これらの隠れた電子情報が再生できるようになり、セキュリティ面での新たな危険

性として注目されています。

PCディスプレイ画面の盗撮「テンペスト」

PC等から放射される漏洩電磁波を受信し、適切な方法で復調することにより、元のディスプレイ画面を再生できることが知られています⁽¹⁾。このような画面盗撮技術は、1960年代から主に欧米で軍事目的での研究が進められてきましたが、具体的な内容はほとんど秘匿され、公表されてきませんでした。

1985年にWin van Eckが発表した論文⁽²⁾を契機に、この技術が一般に知られるようになります。米国での研究中心であったNSA（国家安全保障局）がこの盗撮技術に、「TEMPEST（テンペスト）」というコードネームをつけたことから、以後この略称が広く使われ、研究も多方面で進められてきました⁽³⁾。

テンペストの脅威と特徴

ディスプレイ画像以外にも、キーボードの打鍵情報や、プリンタケーブルからの漏洩電磁波に含まれた印字情報を取得、再生可能であることが報告されています。しかしながら、これらの

漏洩電磁波の放射レベルは、画像信号のそれに比べて弱く、復号化も困難です（図1）。一方で、PCディスプレイ画面の表示情報は機密情報や個人情報も多く、キータッチパネルによる暗証番号入力情報などもその対象となることから、情報の質的な面から、より高いセキュリティが要求されています。

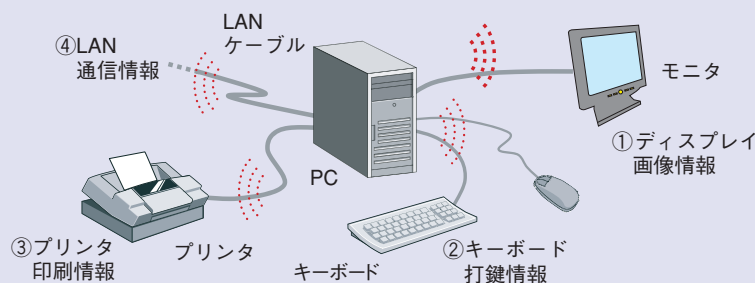
テンペストによる画面の盗撮は、ある程度のノウハウさえあれば、市販品ベースの簡易な装置で可能であり、この点もテンペストの危険性を高める要因となっています。また、テンペストによる盗撮はその痕跡が全く残らないことから、情報漏洩の事実やその原因を見逃してしまい、実際の被害が表面化しにくいことも大きな問題です。

近年、無線LAN通信等においては暗号解読による盗聴の危険性が指摘されていますが、テンペストの場合、他と全く通信していない状態でも、情報漏洩が生じる可能性があります。

テンペストへの対策

PC等からのテンペストを防ぐためには、次のような対策が考えられます。

- (1) シールドによる不要放射の低減
PC等の情報端末を電磁的なシールド（電磁遮蔽）で覆ったり、シールド



漏洩電磁波の情報種別	情報量、情報の重要度	情報再生の難易度	漏洩電磁波放射レベル	情報漏洩の危険度
①ディスプレイ画像情報	大 (表示画面)	容易	強い	大
②キーボード打鍵情報	小～中 (文字情報のみ)	困難 (打鍵コードの解析・復号)	弱い	小～中
③プリンタ印刷情報	小 (印刷情報のみ)	困難 (信号の復号は機種に依存)	弱い	小
④LAN通信情報	中～大 (通信情報)	困難 (LAN信号の復号)	弱い	中

図1 漏洩電磁波に含まれる情報の種別と漏洩の危険度

います。代表的な画面モードには、VGAやSVGA、XGA、SXGAなどがあり、これらはすべて走査線に沿ってピクセル、または画素と呼ばれる表示単位で画像が表示されるインタフェース（ラスタースキャン方式）です。

ディスプレイインタフェースの信号には、3本（RGBの各色）の輝度信号と、走査線のタイミング情報である垂直、水平同期信号が含まれます。輝度信号は、各ピクセルを描画するタイミングを示すドットクロック（またはピクセルクロック）と呼ばれるパルス信号を、各色の輝度で強度変調したものとなっています。

実際のドットクロック周波数は、例えばXGAの1つのモードでは、65 MHz [ピクセル数（解像度）1024×768、水平同期周波数48.4 kHz、垂直同期周波数60 Hz] となります。

PC画面のテンペスト

PCから放射される漏洩電磁波の周波数帯域は広く、そのレベルは非常に微弱で、画像信号以外にもさまざまな不要電磁波やノイズが含まれています。そのため、テンペスト画像の再生には多少のノウハウと習熟が必要です。

実際にPCから放射された漏洩電磁波をテンペストした再生画像を図2に示します。図2(a)はディスプレイ画面に表示させた画像、図2(b)はその再生画像であり、共に電波暗室内でPCから3 m離れたアンテナで受信しました。

こうして得られた複数の画像フレームのデータを蓄積し、時間平均を取ることで、画面のノイズを減らしたより明瞭な再生画像が得られます。図2(c)は32フレーム分の平均化処理を行った

ルーム内で使用することで、外部に漏洩する電磁波を低減させることができます。しかし完全なシールドは難しく、対策費用も高額となります。

(2) テンペスト対策フォントの使用

テンペストによる盗撮画面上で、再生された文字が識別しにくくなる特殊な形状のフォントが提案されています。経済的に対策が可能ですが、通常表示でのフォントの視認性の問題や、図や絵には効果がないといった問題点があります。

(3) フィルタによる対策

PCに接続する各種インタフェースや通信線、電源線などに、漏洩信号を減衰させるフィルタを挿入することで、漏洩信号を減らすことが可能です。ただし、すべてのインタフェースに漏洩信号周波数に応じたフィルタを挿入する必要があります。またPC本体からの直接放射については効果がありません。

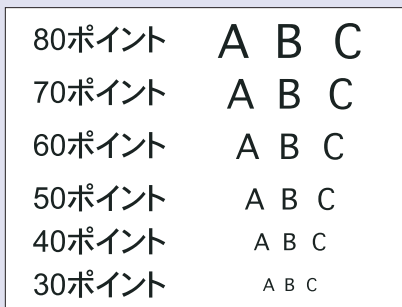
(4) 妨害波によるマスキング

漏洩電磁波より強いレベルの放射を重畳してマスキングすることで、テンペストを阻止することができます。比較的簡易な装置で効果の高い対策が可能であり、モバイル用途にも適しています。ただし、盗撮防止効果はマスキング信号の変調方式によって左右されるため、適切な方式を選ぶ必要があります。

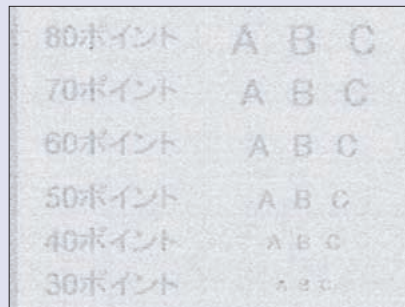
本稿では、テンペストによる盗撮を防ぐために、上記(4)の技術を採用して開発した、情報漏洩防止装置の動作原理およびその効果を示します。

PCのディスプレイインタフェース

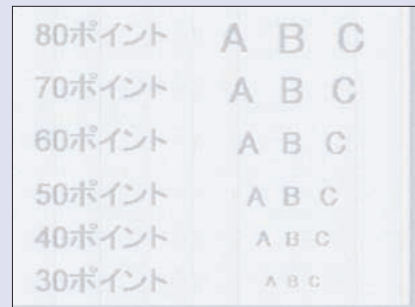
現在PC等で一般に使用されているディスプレイインタフェースは、ビデオ周辺機器に関する標準化団体であるVESA（Video Electronics Standards Association）で規格化されて



(a) PCのディスプレイに表示した画像



(b) 再生画像（平均化処理なし）



(c) 再生画像（32フレーム分を平均化）

図2 テンペストによる再生画像

再生画像ですが、図2(b)よりも明瞭な画像が再生されていることが分かります。

情報漏洩防止装置「テンペストガード」

今回開発した情報漏洩防止装置の外観を図3に示します。テンペストから情報を保護するという意味で、この装置を「テンペストガード」と呼んでいます。

テンペストガードはPC等の外部映像出力端子に装着し、電源をUSBポート、もしくはACアダプタから供給します。デスクトップPCで使用する場合には、もう一方の端に出力端子を設け、そこからモニタディスプレイに画像信号を供給します。

テンペストガードの動作原理

テンペストガードの内部では、まずPC等から受け取った画像信号を基にドットクロックパルスを再生します。次にこのドットクロックパルスを変調して、マスキングを行う防止信号を生成します。ドットクロックの周波数はPCごとに微妙に異なり、また環境条件によっても変動しますが、防止信号をこ

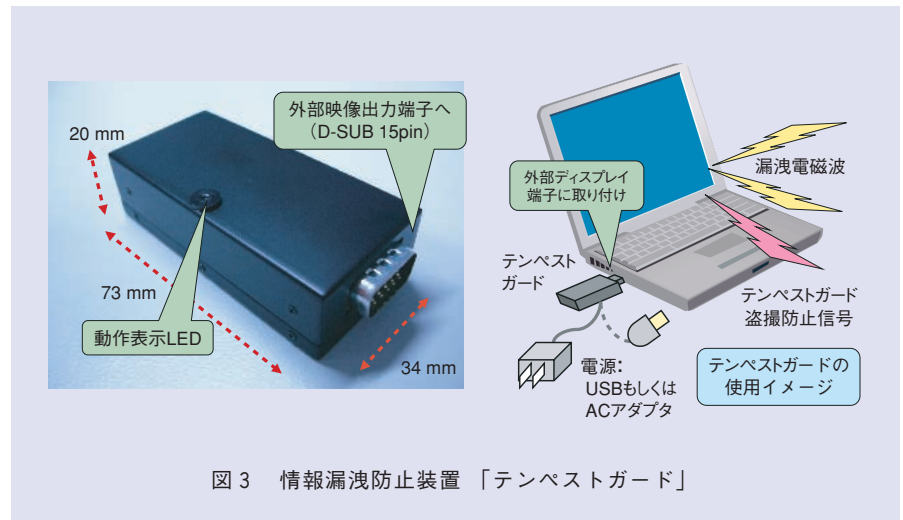


図3 情報漏洩防止装置「テンペストガード」

れに同期させることで、個々のPCに合わせた効果的な盗撮防止が可能です。

こうして生成した防止信号は、PCの外部映像出力端子にコモンモード（信号線～アース間電圧）で印加されます。漏洩電磁波の発生源となる輝度信号のコモンモード成分は、この防止信号によってかく乱されますが、ノーマルモード（信号対線間電圧）の輝度信号自体には影響を与えません。また、防止信号も元の漏洩電磁波も同じPC（および周辺機器等）から放射されるため、放射電磁波強度の空間的な分布状態もほぼ同様のものとなります。

前述した再生画像フレームの平均化処理への対抗策として、防止信号を水平・垂直同期信号に同期させた一定のパターンで変調する方式を採用しました。こうすることで、再生画面には常に一定の固定パターンが表示され、このパターンは平均化処理で打ち消されることがないために、再生画面の読み取りがより困難になります。

情報漏洩防止装置の対策効果

PCから放射された漏洩電磁波の周波数スペクトル（青線）と、同じPCにテンペストガードを装着した場合の

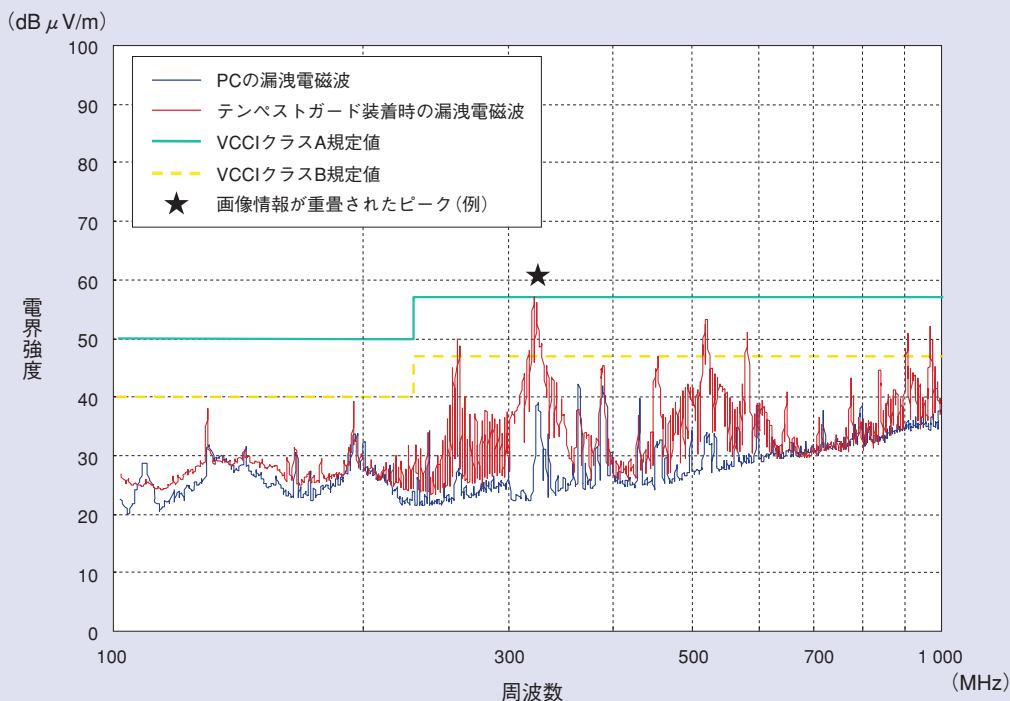


図4 漏洩電磁波の周波数特性 (例)

周波数スペクトル (赤線) を図4に示します。両者のスペクトルはほぼ同様な形状を示していますが、放射レベルは全体的に後者の方がより高く、特にいくつかの放射ピークにおいてはその傾向が顕著です。漏洩画像は通常、放射ピークに重畳されているため、テンベストガードにより、広い帯域にわたって十分なマスキング効果を得られることが分かります。

次に、テンベストガードを装着した場合の再生画像を図5に示します。図2および図5はいずれも、図4中に★印で示した放射ピークを受信、復調した結果です。

図5(a)はドットクロックの変調を行わなかった場合、図5(b)は縦縞の固定パターンで変調を行った場合であり、いずれも、図2(a)に示した画像の再生

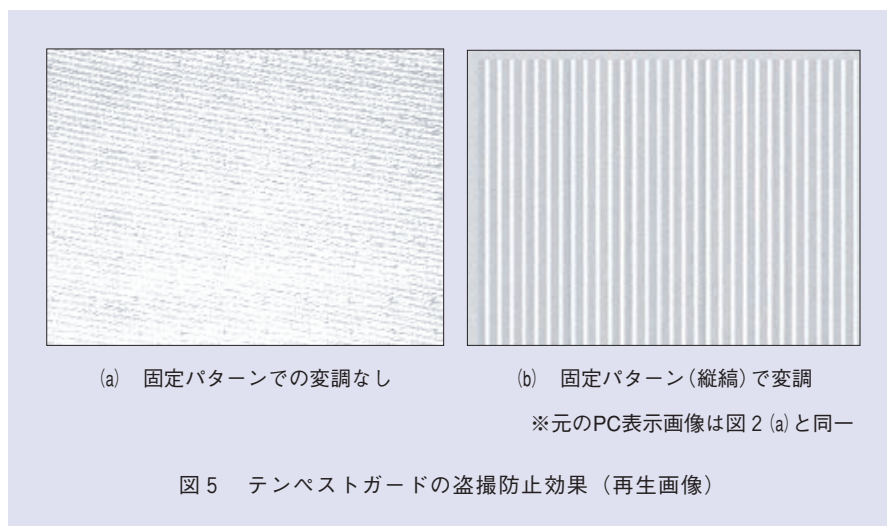


図5 テンベストガードの盗撮防止効果 (再生画像)

結果です (32フレーム分を平均化処理)。図5(b)では、縦縞パターンのコントラストが強く出ており、元の漏洩画像をマスクすることで、画像の識別を困難にしています。

PCからの漏洩電磁波の放射パター

ン (放射レベルの方位依存性) の一例を図6に示します。PCのみの場合もテンベストガード装着時も、漏洩電磁波はPCの周囲にほぼ等方的に放射されています。どの方向でも前者よりも後者の放射レベルが高いことから、方

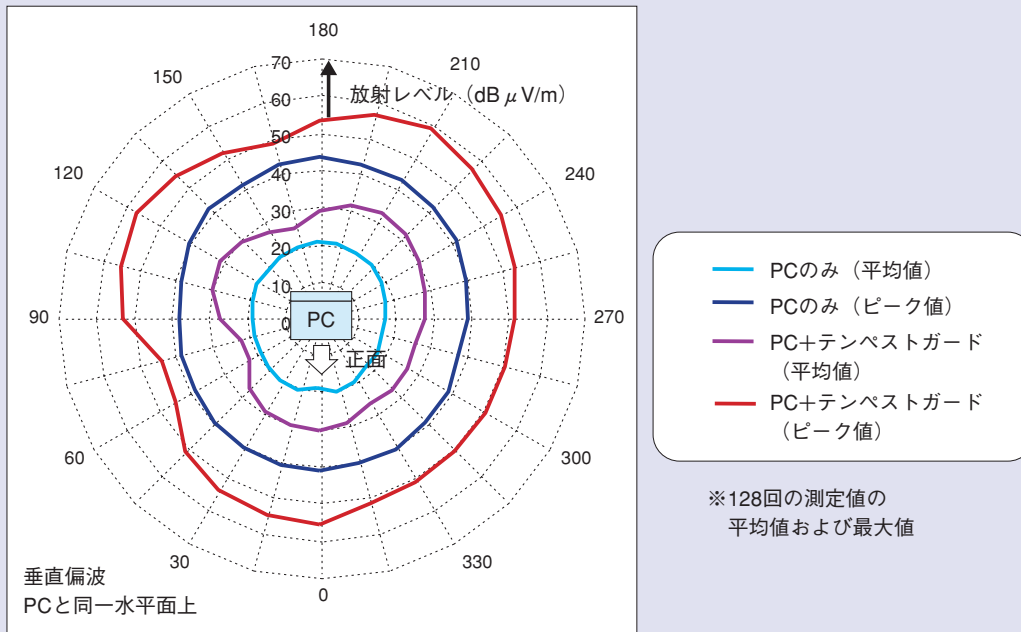


図6 テンペストガードの放射パターン (例)

向によらずほぼ様な盗撮防止効果が得られていることが分かります。

今後の展開

PC等からの漏洩電磁波による テンペストへの対策として開発した、テンペストガードを紹介しました。漏洩電磁波の周波数や放射方向によらず、平均化处理などの高度な盗撮手段にも耐え得る、良好な盗撮防止効果が得られました。

今後は、盗撮防止効果の定量的な評価指標に関する検討や、漏洩電磁波自体の打消しによるテンペスト対策の検討を行う予定です。

参考文献

(1) 鈴木・馬杉・田島・山根：“PCから放射される電磁波による情報漏洩への対策技術,” 平成20電学全大, シンポジウム1-S2-8, pp.21-24, 2008.3.

(2) W. Eck：“Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?,” Computers & Security, Vol.4, No.4, pp.269-286, 1985.

(3) <http://cryptome.org/nacsim-5000.htm>



(左から) 鈴木 康直/ 田島 公博 / 馬杉 正男/ 山根 宏

通信インフラの保守、保全を通して通信サービスの品質、信頼性を支える基盤となる通信EMC技術を研究しています。また、そのノウハウを活かし、電磁波セキュリティ対策品などのプロダクト開発を進めています。

◆問い合わせ先

NTT環境エネルギー研究所
エネルギーシステムプロジェクト
TEL 0422-59-3776
FAX 0422-59-3314
E-mail suzuki.yasunao@lab.ntt.co.jp