4-8　電磁波セキュリティ

4-8　Electromagnetic Security

田中秀磨
TANAKA Hidema

要旨

本稿では2006年度から2009年度にセキュリティ基盤グループで行われた電磁波セキュリティの研究活動を紹介する。電磁波セキュリティの研究の目的は2つある。1つは電磁波を介して漏洩する情報量を見積もる手法の開発、もう1つはこの脅威に対する対策技術の開発である。漏洩する情報量の見積もりについては、連続通信路における通信路容量を見積もる手法を応用した。本研究では特にディスプレイに表示された情報の漏洩に注目した。

これは一般にTEMPESTと呼ばれている。対策技術としてはソフトウェアで実現できるTEMPEST対策技術を開発した。これはTEMPESTフォントと呼ばれ、特別な装置を必要としない。これに関してはベンチャー企業に技術移転を行い製品化された。最終的には、ITU-Tにおいて漏洩情報量を見積もる手法と対策技術の提供するセキュリティレベルに関して標準化を行った。

In this paper, we show the activity of research on the security analysis of electromagnetic emanation (electromagnetic security) between 2006 and 2009 in Security Fundamentals Group. The activity of electromagnetic security has two purposes; the development of evaluation method of amount of information leakage via electromagnetic emanation and the development of countermeasures against such threat. We proposed the evaluation method applying the estimation method of channel capacity of continuous channel. In particular, we focused on the threat of information leakage displayed on the monitor. Such threat is called as TEMPEST in general. And we developed the countermeasure on software (TEMPEST fonts) and it does not needs any devices. We move the technology to the venture company and they have commercialized it. At last, we successes the standardization of both of estimation method of information leakage and security level of countermeasure in ITU-T.

[キーワード]
漏洩電磁波，電磁波セキュリティ，通信路容量，TEMPEST，情報漏洩
Electromagnetic emanation, Electromagnetic security, Channel capacity, TEMPEST, Information leakage

1　まえがき

電磁波を受信してパソコンのモニターを盗み見すると聞いた時は単に理屈上成立し得る技術と思い、その装置（図1）の値段を聞けば非現実的な脅威に考えられたが、第2期の初年度が終わる頃には現実的な脅威として認識するに至った。全ての電子機器はその処理している情報に応じた雑音を発生し、これを電磁波として放射する。特に画面情報の場合、情報再現の仕組みは非常に単純でありテレビと同様のものである。ただし、画面情報

図1　TEMPEST専用装置FSET-22

を十分に含んでいる周波数及び適切な帯域幅の探索、垂直と水平の同期信号の調整が困難である。これらの探索に成功すると、電磁波を介した画面情報の漏洩は非常な脅威となる。何故ならば、漏洩電磁波は空間への直接放射だけでなく、電源ケーブルやLANケーブルを介した伝導放射を行うため、例えば建物の別の部屋にいても対象の画面情報を再現することが可能だからである。またアンテナとして機能するものも、窓のサッシやドアの金属フレーム、天井の空調のパイプなど様々なものが利用できる。また直接の文字列を盗み見するだけでなく、どのような作業や操作を行っているかを知るだけで十分な場合もある。例えば銀行のATMはタッチパネルを採用しているケースが多いが、ここで入力する暗証番号は選択したボタンの色の変化という画面情報として漏洩する。電子投票などの場合はどの候補者を選択したかを遠隔から把握できる。このように脅威の最大の問題は対象がヒューマンデバイスであるため、暗号技術で安全性を確立できず、より直接的な情報漏洩である点にある。さらに研究を進めるうちに図2に示すように、民生品の組み合わせで十分に情報の取得が可能な装置が構成できることが明らかとなった。

本研究は電磁波を介して漏洩する情報量を見積もる手法と対策技術の開発を目的とした。最初に情報が最も含まれている周波数及び必要な帯域幅の評価手法の開発を行った。これは連続通信路における通信路容量の算出手法を応用した。ただし、受信している信号も雑音でありS/Nの算出には実験結果からの経験則を用いた。この結果と、電磁波を放射しやすい画面構成の特徴を解析することで対策技術を開発した。対策技術には対策電磁波を放射するハードウェアタイプが多く存在する（図3）が、本研究では画面構成を変更するフィルタソフトによるソフトウェアタイプであることが特徴的である。これは、デスクトップPCのような据え置き型の装置だけでなくノートPCのような可搬性の装置でも利用できる点、導入コストが安価である点と既存のインフラへの導入のしやすさを重視したことによる。

対策技術が十分な安全性を有することを評価する手法の開発も重要である。例えば最も情報取得に適した周波数帯が対策できても2nd best以下でも情報の再現が可能な場合もあるからである。これの評価にはEMC的な手法が不可欠であった。そのため、本研究は情報理論的手法、暗号技術の安全性評価的な視点、電磁波測定技術の連携が重要であり、セキュリティ基盤グループとEMCグループの共同研究として遂行した。最終的に開発した対策技術はベンチャー企業により製品化され、評価手法はITU-Tにおいて標準化された。

図2 簡易TEMPEST装置
市販の装置を組み合わせたのみ

図3 TEMPEST対策機器
コネクタ間に挟むタイプ

2 情報漏洩量の見積もり

2.1 通信路容量

通信路が与えられた時、その通信路が送ることが出来る最大の情報量は通信路容量で与えられ、送受信者間の相互情報量の最大値で定義される。平均電力が制限された追加性1次元ガウス通信路の場合、信号電力をS、雑音電力をNとすれば通信路容量Cは以下のように表すことができる。

$$C = \frac{1}{2}\log_2 \frac{S+N}{N} \text{ [bit/symbol]} \quad (1)$$

さらに帯域を制限された追加性ガウス通信路の場合は、帯域幅を W とすれば

$$C = \frac{W}{2}\log_2 \frac{S+N}{N} \text{ [bit/sec]} \quad (2)$$

と表すことができる。

通信路容量は、雑音が一様分布している通信路において、送信者が確保できた信号電力と帯域によって送ることができる最大情報量を表している。通信路容量によって、送信者は送りたい情報量に対して通信路が十分であるかどうかであることや、必要な信号電力及び帯域幅を改善することによって通信の質を高めることができる。

2.2 漏洩情報量

IT 機器の放出電磁波に含まれる情報量について、IT 機器と受信者の間を帯域制限された通信路と考えることにより通信路容量の考え方を応用して算出することを考える。前述のように通信路容量は、雑音が存在する通信路において信号電力及び帯域幅を送信者が調整できる送信者側の理論である。受信者は送信者の設定した帯域幅を持つ受信機を利用することにより、送信者が意図した情報量を受け取ることができる。

一方、放出電磁波の受信においては信号電力と雑音電力が混在し、それが信号であるか雑音であるのかの判断は受信者によって決定される。さらに通信路の性能は受信者が設定した受信機の S/N 比や帯域幅で決定される。このように放出電磁波の受信では、受信者が一方的に定めた通信路しか確立できない。

図 4 は PC から放射される電磁波を周波数領域で測定した例である。測定器（スペクトラムアナライザ）の帯域幅は 10［MHz］に設定している。周波数 285［MHz］で画像情報の再現に成功することはこれまでの実験から明らかになっており［1］、周波数約 277［MHz］～ 293［MHz］が画像情報を含む放射（信号）、その範囲外は雑音と考えることができる。また、図 5 は放出電磁波を時間領域で測定した例である。図 4 は図 5 における、放出電磁波の最大値でプロットしたものである。

周波数 f における信号電力を $S(f)$、雑音電力を $N(f)$ とすれば、周波数範囲［f_1, f_2］（ただし $f_2 > f_1$）の通信路容量 C は、単位時間当たりの相互情報量 I の最大値として与えられる。

$$I = W\int_{f_1}^{f_2} \log_2 \frac{S(f)+N(f)}{N(f)}\, df \text{ [bit/sec]} \quad (3)$$

ところで放出電磁波の受信の場合、受信機の帯域幅及び S/N 比で $S(f)$ と $N(f)$ は決定されるので、式 (3) で計算できる I 以下の情報しか受信できないことは明らかである。従って式 (3) の相互情報量は、放出電磁波受信における通信路容量そのものである。しかし前述のように通信路容量と

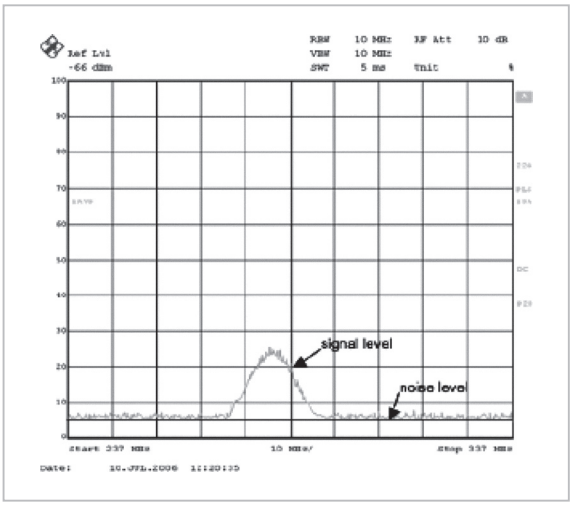

図 4 スペクトラムアナライザによる放出電磁波の測定例（周波数領域）

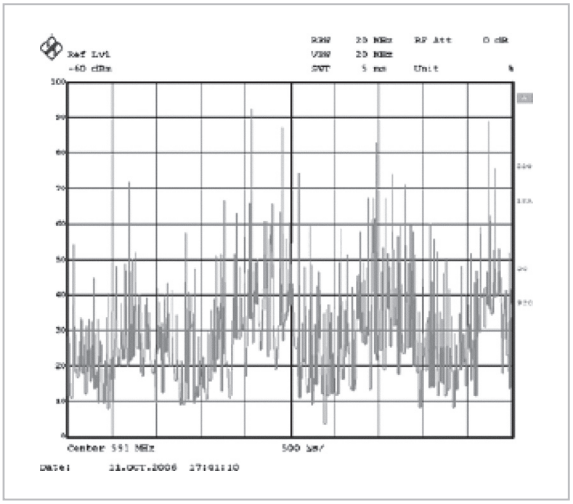

図 5 スペクトラムアナライザによる放出電磁波の測定例（時間領域）

性質が異なるので、本稿では式(3)で定義される情報量を「単位時間当りの漏洩情報量」と呼び、記号Lで表すことにより本来の相互情報量や通信路容量と区別する。

また受信機の帯域幅をWに設定した場合、受信周波数をf_0とすれば、その受信周波数範囲は$[f_0-W/2, f_0+W/2]$となる。

2.3 漏洩情報量と受信機帯域幅の関係

漏洩情報量を式(3)で定義し、放射電磁波を介して受信者が得ることができる情報量と定義した。以下では、放出電磁波を発している情報源の単位時間当たりの情報量を対象情報量と呼び、A[bps]と表す。また、漏洩情報量をL[bps]とすれば(対象情報量A)<(漏洩情報量L)の関係が成立する通信路を確立できれば受信者は単位時間内で対象情報量を全て得ることができる。

S/N比は機器固有の性能や環境によって定まる値であり、受信者が調整することはできない。従って漏洩情報量は受信機の帯域幅のみによって決定されると言える。受信機の帯域幅はS/N比と振幅確立時間に影響を与える。帯域幅が大きいほどS/N比は改善され振幅確立時間は短くなるので、放出電磁波の受信には広い帯域幅が有効と言える。なお20[MHz]以上の帯域幅を持つ受信機は高価な機材に分類され、一般に入手可能なものは10[MHz]程度である。また広い帯域幅を利用した場合、受信者にとって有意な信号以外のものも広く受信することになる。結果として信号受信としてのS/N比は改善されているものの、有意な情報受信としてのS/N比が悪くなることになりかねない。

さらに、受信対象の信号の性質によっても必要な帯域幅の設定は変わる可能性がある。例えば非接触ICカードの認証信号やキーボードの打鍵情報などの一度限りの通信を受信する場合、受信情報の欠損は情報取得において致命的失敗に繋がる。しかし静止画像を表示している画面情報の受信の場合、相関性の高い情報を繰り返し送信することになるので多少受信情報に欠損があっても訂正や修正を行うことができる。従って受信対象の源の信号が持つ情報量や性質と漏洩情報量から、適切な帯域幅を設定する必要がある。

2.4 画面情報再現実験による検証

実験概要

ここではノートPCに静止画像を表示させ、その画面情報を本体からの放出電磁波を用いて再現する実験により漏洩情報量の算出の妥当性の検証を行う。PCの画面には図6に示す静止画像が表示され、本体に密着させたプローブから放出電磁波を受信した。本実験における対象情報と受信機、その間の通信路の関係は図7のように表せる。

一般にVGA信号の情報量[bps]は以下のように計算できる。

$$\text{色数[bit]} \times \text{総画素数[dot]} \times \text{フレームレート[fps]} \quad (4)$$

尚、「総画素数[dot]×フレームレート[fps]」はドットクロック周波数とも呼ばれる。測定対象のディスプレイの仕様では24[bit]色画像であり、総画素数は800×600[dot]、フレームレートは60[fps]としたので、対象情報量Aは以下のように

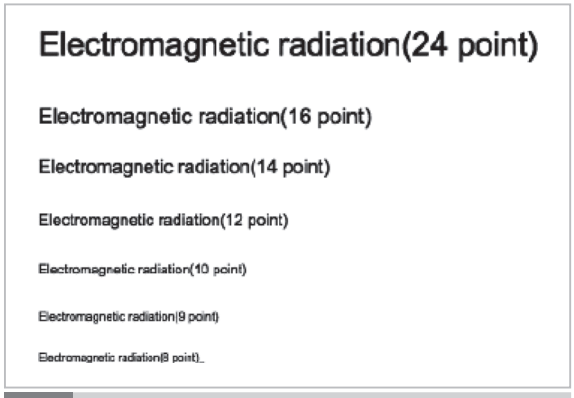

図6 PCの表示画像

図は画面全体における文字情報が表示されている部分のみ。白色背景に黒字で表示。

図7 対象情報と受信者によって確立された通信路の関係

計算できる。

$$A = 24 \times (800 \times 600) \times 60 = 691\,[\mathrm{Mbps}] \qquad (5)$$

測定結果

帯域幅の設定を10［MHz］と20［MHz］にした場合の測定結果を図8と図9にそれぞれ示す。これらより明らかに20［MHz］での測定は、10［MHz］の場合に比べて大きな漏洩情報量を持つ通信路を確立できていることが分かる。

これらの結果から漏洩情報量を算出する。帯域幅10［MHz］の時の漏洩情報量をL_{10}、帯域幅20［MHz］の時の漏洩情報量をL_{20}とする。

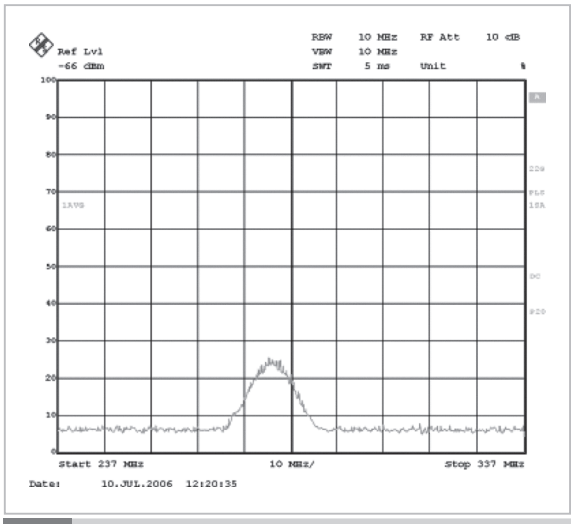

図8 帯域幅10［MHz］、測定範囲237～337［MHz］における対象PCからの放出電磁波の測定結果

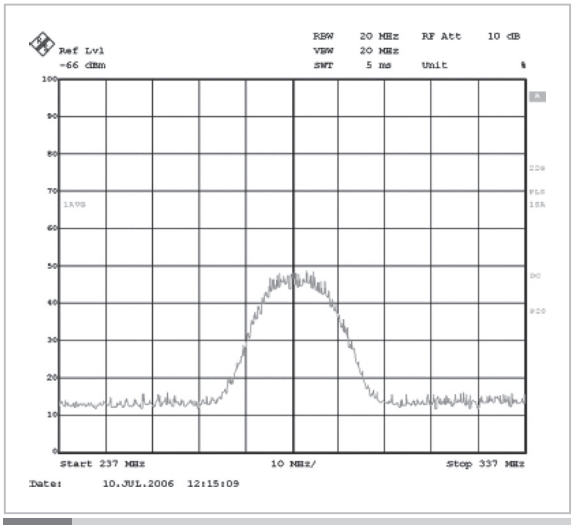

図9 帯域幅20［MHz］、測定範囲237～337［MHz］における対象PCからの放出電磁波の測定結果

$$L_{10} = W \int_{280}^{290} \log_2 \frac{S(f)+N(f)}{N(f)}\,df\ [\mathrm{Mbps}] \qquad (6)$$

$$L_{20} = W \int_{275}^{295} \log_2 \frac{S(f)+N(f)}{N(f)}\,df\ [\mathrm{Mbps}] \qquad (7)$$

対象情報量は691［Mbps］であるから、静止画像が変化しないという仮定の下で画面情報全体を得るのに帯域幅10［MHz］の場合は約25秒間の受信が、帯域幅20［MHz］の場合は約7秒間の受信が画像情報の再現に必要となる。一方で、図6は白黒2値画像であるから1［bit］色画像であり、その場合、対象情報量は約29［Mbps］と見ることができる。これは機器的仕様の上では白黒画像であっても24［bit］の情報として送信している。従って24［bit］を使って1［bit］の情報を送信していることになり、非常に冗長性の大きい通信と見なすこともできることを意味する。表示されている画面情報の性質を考えると後者のように1［bit］色画像と考えることが妥当であり、帯域幅10［MHz］でも十分に受信可能な設定と考えることができる。

漏洩情報量と再現画像の比較

受信した信号に垂直水平同期信号を与え、画像情報として再現した結果を図10と図11に示す。これらの結果は、複数のフレームの積分（平均化）などの画像処理を行っていない。

従ってこれらの再現画像は帯域幅10［MHz］の場合は約28［Mbit］、帯域幅20［MHz］の場合は約101［Mbit］の情報で構成されている。帯域幅10［MHz］の場合は画素1［dot］当たり約0.97［bit］、帯域幅20［MHz］の場合は約3.5［bit］の情報を持つ。前述のように白黒2値画像と見なせるので、帯域幅10［MHz］でも平均化処理無しでかなり鮮明な再現画像が得られた。

尚、再現画像は垂直水平同期信号の微妙なずれのため上下左右にわずかながら流れている状態である。また再現用装置の雑音等が画質に影響を与えていると考えられる。従って本論文に掲載している再現例は、再現装置上で視認するよりも上記の理由に加え印刷の都合等で見にくい可能性がある。

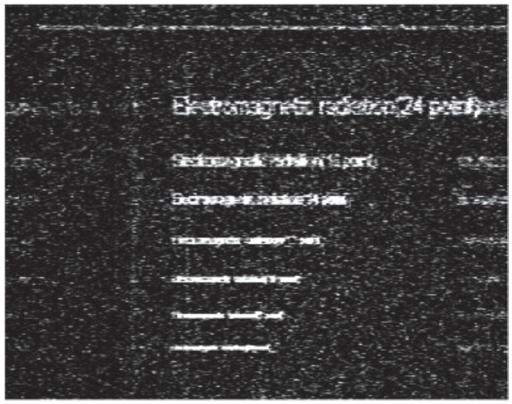

図 10 帯域幅 10 [MHz] で再現した画面情報
平均化などの画像処理無し

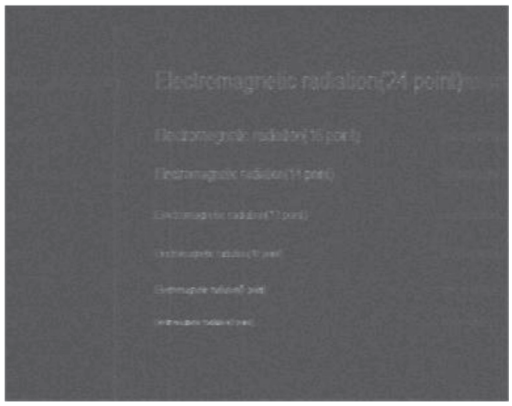

図 11 帯域幅 20 [MHz] で再現した画面情報
平均化などの画像処理無し

3 画面情報の再現

対象となった画面情報を表示している装置は、水平同期信号と垂直同期信号を発生させているが、同じ VESA 規格に従っていても画質に影響を与えない範囲で誤差がある。この誤差は機器ごとに異なるため、これを利用して特定の機器からの情報を得ることができる。従って、同じメーカ、同じ型番の機器が同時に動作しているオフィスのような環境下であっても直感と異なり、対象を限定して画面情報を再現できる。

さらに画面情報を再現する電磁波の受信には様々な手法が考えられる。空間を伝搬する電磁波をアンテナで取得する方法や、電源ケーブルなどを伝搬した電磁波を取得するなどである。しかしながら、電磁波の質がそれぞれ異なること、取得すべき周波数と帯域幅などが変化する。

そこで、いくつかのケースを仮定して実現性の検証を行った。

表 1 FSET22 仕様

Frequency range	100 Hz ~ 22 GHz
Frequency resolution	0.1 Hz
Bandwidth	10 Hz ~ 500 MHz in steps of 1/2/5
Average noise level	< -142 dBm (1 MHz)

装置

実験には Tempest 受信機として ROHDE & SCHWALZ 製 FSET22 と画像処理ソフト FrameControl ver. 4.24 を使用した。FSET22 の仕様を表 1 に示す。

FrameControl は FSET22 からの信号を 256 frames/3s で処理可能である。Tempest での画像再現には画像処理ソフトの性能が大きく影響を与える。本実験で使用した画像処理ソフトは、256 frame の画像を積分することにより、ノイズを除去し鮮明な画像を作成することができる。受信用のアンテナやプローブは、アンリツ製 MP666A logarithm periodic antenna (20 ~ 2000 MHz)、アンリツ製 MA2601B/C の近磁界プローブ (5 ~ 1000 MHz) と TOKIN 製 EIP-100 インジェクションプローブ (80 KHz ~ 30 MHz) を使用した。

対象となったものは、ノート PC として SONY 製 VAIO (以下、VAIO)、IBM 社製 ThinkPad (以下、IBM) 及び一般的なデスクトップ PC に接続された CRT モニター (以下、CRT) である。CRT モニターは液晶画面との比較のために用意した。これは、液晶ディスプレイに比べて CRT の方がより強い不要電磁波を放射していると考えられたためである。

実験環境

本実験では以下のような攻撃シナリオを想定して、近磁界プローブを使った実験、アンテナを使った実験、インジェクションプローブを使った実験を行った。

- 攻撃者はターゲットの PC の近く (机の下など) に近磁界プローブを設置した。

- 攻撃者は隣の部屋や外からアンテナによってターゲットのPCから漏洩した電磁波の傍受を試みた。
- 攻撃者はターゲットのPCが使用している電源線からの傍受を同じ建物の別の部屋から傍受を試みた。

後者に行くほど、現実的な脅威が大きくなると考えられる。逆に、前者ほどターゲットの近傍なため、より鮮明な傍受画像を得ることができる。

近磁界プローブを用いた実験

本実験では、近磁界プローブを対象PCの間近に設置し傍受を行った。再現した画像を図12に示す。VAIOの結果とIBMの結果に差異が無かったので、VAIOの結果は省略している。また、表2にTempest受信機の設定値を示す。図12の結果から、文字がはっきりと読み取ることができる。特に意味のある文章であれば、数文字認識できなくても意味は読み取れると考えられる。

以下の実験でも、文字が読み取れるか否かで実験の成否を判定しているが、読み取れるかどうかの判断は個人差が大きく、また印刷された画像よりもTempest装置の画面から読み取る方がより判別しやすい。さらに、Tempest装置の画面は静止画像ではないため印刷が難しい反面、長らく目視している受信者は順応して文字の認識が容易になってくる。

アンテナを用いた実験

アンテナを用いた傍受は、近磁界プローブを用いた傍受よりも現実的な脅威と考えられる。本実験では、対象PCから約4[m]離れた場所からの傍受を試みた。実験はNICT小金井本部5号館3階エレベータホールの見通しの良い場所で行った。IBMを対象とした実験は失敗したため、図13にはVAIOとCRTの再現結果を示し、表3にTempest受信機の設定値を示す。IBMの実験が失敗した原因は、機器に固有の問題と考えられる。複数の実験経験から、ノートパソコンで最も電磁波が漏洩している箇所はヒンジ部分であるが、IBMはこの部品が金属製であるのに対してVAIOなど大多数のものはプラスティック製である。また、薄型液晶ディスプレイは経験上、非常に大きい電磁波を放射する。近磁界プローブを使った実験結果よりも、不鮮明な傍受画像であるが、実際のTempest受信機からの読み取りでは文字の認識には全く問題がなかった。

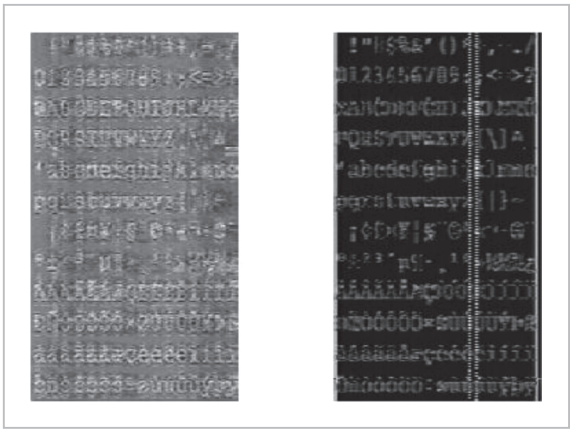

図12 近磁界プローブを用いた再現画像
128枚のFrameを積分（左）IBM（右）CRT

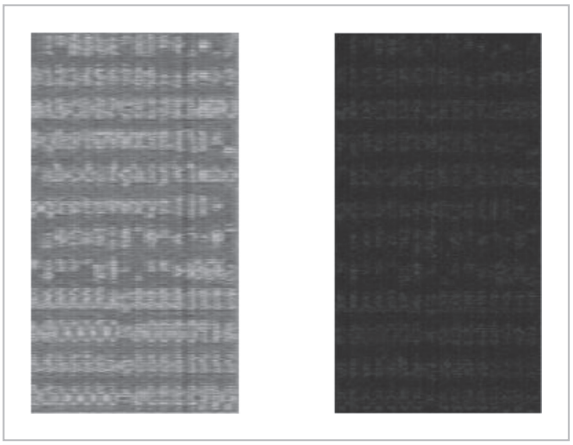

図13 約4[m]離れた場所でアンテナを用いた再現画像
128枚のFrameを積分（左）VAIO（右）CRT

表2 近磁界プローブを用いた実験における設定値

	Frequency [MHz]	Bandwidth [MHz]
IBM	461.2	20.0
CRT	57.4	20.0

表3 アンテナを用いた実験における設定値

	Frequency [MHz]	Bandwidth [MHz]
VAIO	844.8	20.0
CRT	973.2	20.0

インジェクションプローブを用いた実験

インジェクションプローブを用いた攻撃シナリオは最も現実的な脅威と考えられる。これは同一建物内であれば、ほとんど漏洩電磁波が減衰せずに伝搬する上、攻撃者はその存在を知られるリスクが小さくなるからである。本実験では、対象PCから30[cm]離れた場所にプローブを設置した場合と30[m]の延長ケーブル越しで設置した場合で実験を行った。

その結果に差異が無かったので、30[m]の延長ケーブル越しに行ったCRTについて図14に再現結果を、表4にTempest受信機の設定値を示す。尚、VAIOとIBMではACアダプタが原因で画像情報を取得できないと考えられたが、実験に成功している。しかし、インジェクションプローブを使った実験では、ノイズが多く乗る傾向が他2つの実験に比べて大きく、場合によっては平均化処理を行うことでよりノイズの情報が強くなり文字の読み取りが難しくなる場合もあった。しかしながら、一般的には他の実験と同様に文字の読み取りは可能であった。

また、アンテナや近磁界プローブの場合は、位置や向きに結果が影響されるが電源線を対象にしたインジェクションプローブの場合は、安定した結果が得られた。また、30m程度であれば距離にも大きく影響されない。このことからもインジェクションプローブを用いた盗聴が最も脅威であることが確認できた。

表4 インジェクションプローブを用いた実験における設定値

	Frequency [MHz]	Bandwidth [MHz]
CRT	23.8	20.0

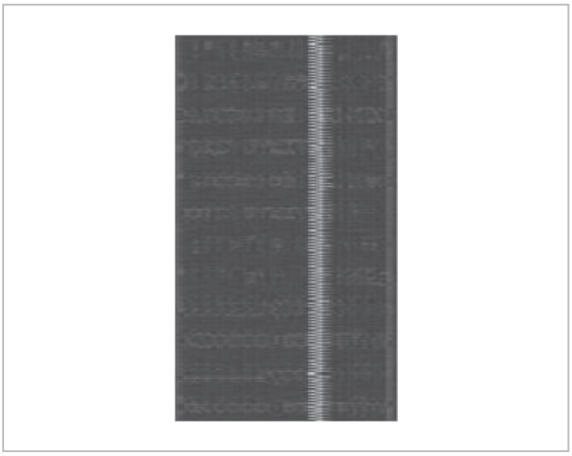

図14 約30[m]離れた場所でインジェクションプローブを用いた再現画像
128枚のFrameを積分

4 対策技術開発

Tempest fontsの解析

Tempest fontsは、元のフォントの画像から水平方向の周波数成分の上位30%に離散フーリエ変換を施すことにより除去し、作成されている[2]。これは、Tempestにおいて水平方向の周波数成分の上位30%が再現画像に影響を与えることが根拠となっている。**3**で示した受信実験は実はこのTEMPESTフォントを対象にした。図15にTempest fontsの拡大図を示す。この図から、文字を構成する線の周りにディザが生じているのが分かる（文字の周りの白いブロックノイズ状のもの）。さらに、図16に別画像処理の図を示す。

これは白黒反転させただけのものであるが、ディザがきれいに再現され、それ故に文字の形状が崩れないため再現画像から文字の認識が行えることが分かる。特に直線で構成される文字は形が崩れる傾向が少なく、文字として認識しやすいことが明らかとなった。KuhnとAndersonの実験結果[2]では文字が完全に消滅していたが、本実験で示すように実際にはディザを強調させることにより文字の認識が行える。これはKuhnとAndersonが実験を行った時に比べて、画像処理技術が向上したことが原因と考えられる。

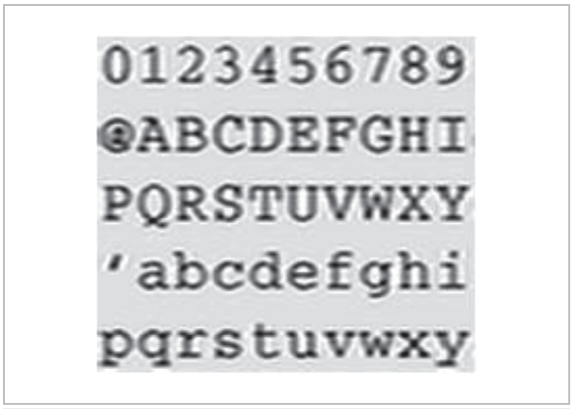

図15 Tempest fontsの拡大図

このようにディザが生じることにより、Tempestに対する安全性が低下してしまうことが考えられるので、ディザを無くすことにより改良できると推測した。本論文では、Tempest fontsの特性を失わずにディザを無くす方法としてガウスフィルタを適用することを考えた。画像の高周波数成分は、隣り合うピクセルの相関が低いときに発生する。ガウスフィルタは隣り合うピクセルの相関を高めるので、離散フーリエ変換で除去された以上の周波数成分を発生することはない。

離散フーリエ変換とガウスフィルタは、画像全体を平滑にするので全体的にぼやけた画像になり、現在対象にしているフォントのような文字には適さない処理なので、視認性を失わずにTempestに対する効果を失わないようなパラメータ設定を探索する必要がある。本論文では実験的に探索し、半径3.0ピクセル、しきい値25.0ピクセルの時を最適と判断した。

一方でガウスフィルタの効果は式(3)から漏洩情報量での評価も可能である。図17を元にガウスフィルタを用いた対策技術の効果を検証する。図17に対して半径1[pix]の処理を施したものを処理画像1とする（図18）。また、図17に対して半径2[pix]の処理を施したものを処理画像2と呼ぶ（図19）。紙面の都合上、図17～19は区別がつきにくいが最下段の文字列（8ポイント）のぼかし具合や最上段の文字列（24ポイント）のエッジの甘さ加減などから処理によって生じた影響が分かる。尚、画面上でははっきりとした区別がつき、ぼかしの効果が大きい処理画像2では10ポイント以下の文字列は見にくい印象がある。また24ポイントの文字列であってもフォーカスが甘く感じられる。

これら画像に対して、放射電磁波受信による画面情報の再現実験を行った。測定対象のディスプ

図16　図12（左）に白黒反転処理を施した画像

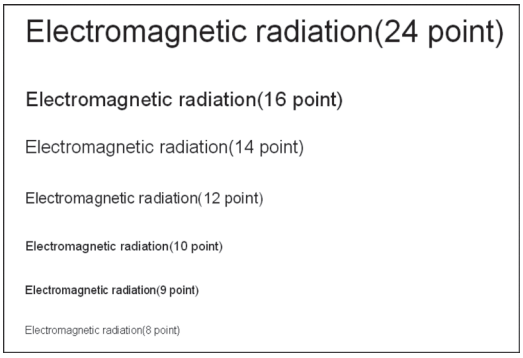

図17　源画像

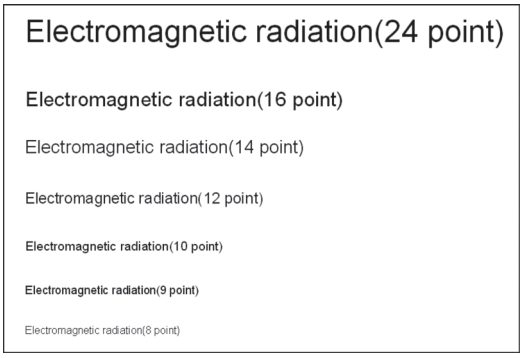

図18　処理画像1

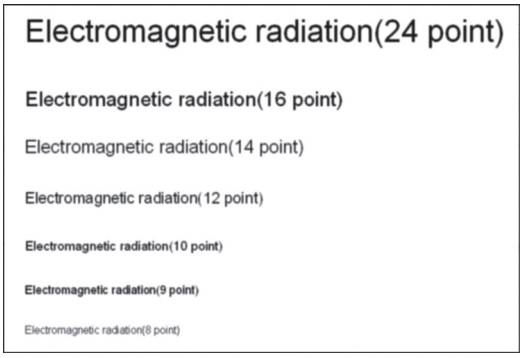

図19　処理画像2

レイカードの仕様では24 [bit] 色画像であり、総画素数は800 × 600 [dot]、フレームレートは60 [fps] である。受信周波数は335.4 [MHz]、帯域幅20 [MHz]、インジェクションプローブをVGAケーブルに密着させて受信した。

漏洩情報量的解析

ここでは、源画像と処理画像2の比較を漏洩情報量の観点から行う。源画像は白黒2値画像であるから、源画像の対象情報量 A_0 は1 [bit] 色画像と考え以下のように計算できる。

$$A_0 = 1 \times (800 \times 600) \times 60 = 29\,[\mathrm{Mbps}] \qquad (8)$$

一方、処理画像2の場合はぼかし効果によりグラデーションが発生したため白黒256階調 (8 [bit] 輝度画像) である。よって対象情報量 A_2 は8 [bit] 色画像と考え以下のように計算できる。

$$A_2 = 8 \times (800 \times 600) \times 60 = 232\,[\mathrm{Mbps}] \qquad (9)$$

放出電磁波の測定結果をそれぞれ図20と図21に示す。これらから、源画像に対する漏洩情報量 L_0 と処理画像2に対する漏洩情報量 L_2 は以下のように計算できる。

$$L_0 = W \int_{325.4}^{345.4} \log_2 \frac{S(f)+N(f)}{N(f)}\, df \qquad (10)$$
$$= 83.1\,[\mathrm{Mbps}]$$

$$L_2 = W \int_{325.4}^{345.4} \log_2 \frac{S(f)+N(f)}{N(f)}\, df \qquad (11)$$
$$= 49.8\,[\mathrm{Mbps}]$$

これらの結果から $L_0 > A_0$ であり、平均化処理を行わない場合、単位時間当り1 [dot] 当り約2.9 [bit] の情報を用いて再現画像を構成していることになる。源画像の場合は平均化処理を行わなくても文字の読み取りが可能であったことが情報理論的にも確かめられた。また $L_2 < A_2$ であり、平均化処理を行わない場合は処理画像2の場合は1 [dot] 当り8 [bit] の画像情報を約1.7 [bit] で構成することになり情報の欠落により十分な再現ができないことが分かる。しかしながら平均化処理を行った場合は、使用したフレーム数倍に情報が増えるはずである。処理画像2の場合、8フレーム利用したので1.7 × 8 [bit] になり十分な再現が行えると予想されるがそのような結果には至っていない。

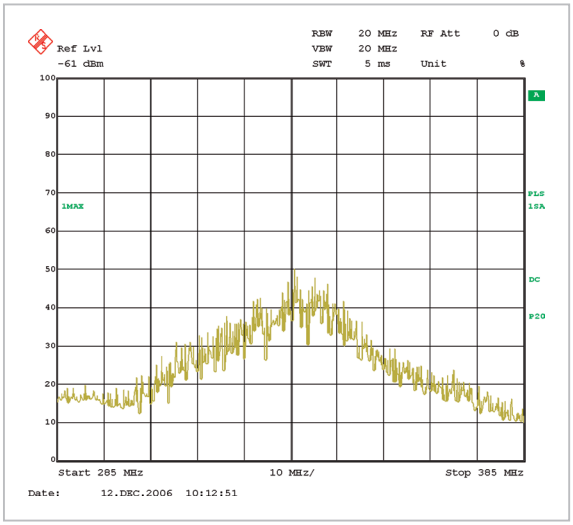

図20 スペクトラムアナライザによる放出電磁波の測定（源画像）

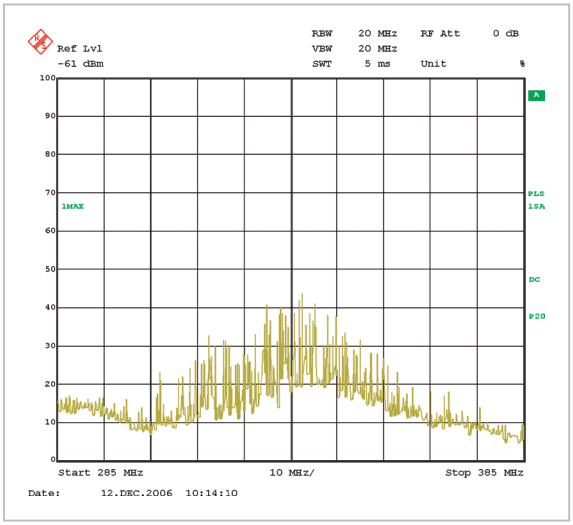

図21 スペクトラムアナライザによる放出電磁波の測定（処理画像2）

画像処理的解析

図22に処理画像2の再現画像、図23に処理画像2の輝度に関するヒストグラムを示す。ここから源画像は白黒2値、処理画像は256階調程度の画像に変換されたことが確認できる。これまでの画像再現実験から画像における白→黒（もしくは黒→白）の変化点で最も大きい放射電磁波が観測されている。ガウスフィルタは白→黒（もしくは

黒→白）の変化点でぼかし効果を与え、グラデーションを発生させる。従って白→黒のような急峻な変化ではなく、白→白灰色→黒灰色→黒のように段階を踏んでの変化となる。結果として放射電磁波の大きさが小さくなり、受信レベルが小さくなるので再現が難しくなると考えられる。これは図20と図21に示したスペクトラムアナライザによる観測結果の比較からも確認できる。

ところで、画像において放射電磁波を発生する部分は色情報が変化する部分である。例えば数字2の底辺部分の直線はバックグラウンドの白から文字の黒に変化した点で電磁波が放射され、再びバックグラウンドの白へ変化するまで電磁波の放射は行われない。つまり水平方向への画像の変化が無い部分では放射電磁波を受信しないので、再現画像では構成されない。このように、画面情報は放射電磁波へ影響を与えている時点で既に元の情報から欠損している。従って*A/L*だけの情報を蓄えて平均化処理などを施しても、画面情報を完全に再現することはできない。

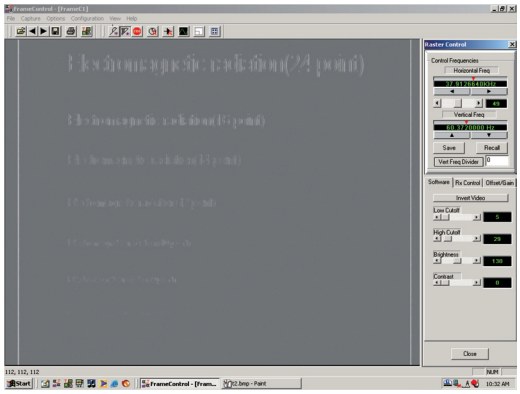

図22　処理画像2の再現画像

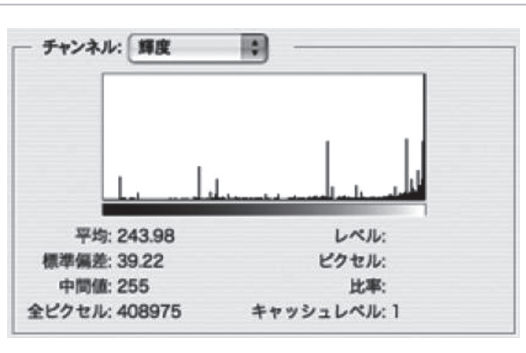

図23　処理画像2のヒストグラム

5　製品化及び標準化活動

以上のように画面情報における水平周波数成分の上位30%を削除したガウスフィルタ処理による対策が有効であることが分かった。実際にこの手法を適用しようとすれば、予め処理した画像情報を保存しておく必要がある。先行研究であるTEMPESTフォント[3]はそれに当り、処理済みのフォントが欧米フォントの一部で提供されている。我が国の場合は文字数が多いため、そのようなデータを作成することが極めて困難である。また、既に指摘したように文字情報の読み取りだけが情報漏洩の問題ではない。このような問題を包括的に解決するため、電磁雑音をソフトウェア的に発生させフィルタ処理をリアルタイムで行うミドルウェアを開発した。この中で特に文字表示に効果的な文字修飾を行うソフトウェアとしてCrypTypeを開発した[4]。これはフォントにそのままガウスフィルタ処理すると視認性が失われる問題を解決するものである。これをOpenXMLフォーマットを活用してMicrosoft OfficeのWord2007へ実装した。図24は本ソフトウェアの効果のデモンストレーションである。図24に見られるように、Word画面のうち、対策をした部分以外は電磁波からの傍受で画面情報の再現が可能であるが、対策部分は全く情報が漏れないことを示すことができた。また、これはリアルタイム処理のため平均化処理に対する対策も可能であり、タッチパネルのようなユーザインタフェースに適用した場合でも十分な効果が発揮できる。本ソフトウェアの開発には（株）ビヨンディットと共同で行い、マイクロソフト社イノベーションアワード賞を受賞した[5][6]。

電磁波セキュリティに関する標準化機関としては、ITU-T（International Telecommunication Union-Telecommunication sector：国際電気通信連合電気通信標準化セクタ）の勧告X.1050が該当する。これは情報セキュリティ管理システムの仕様であり、各種システムセキュリティ管理ガイドラインへ適用されている。この中のITU-T SG（Sub Group）5の課題15において、通信分野の電磁波セキュリティ関連について2005年から議論が

開始され、2009年に勧告化された。

- K.sec：Guide for the application of electromagnetic security requirements
- K.hemp：Application of requirements against HEMP to telecommunication systems
- K.hpem：Application of requirements against HPEM to telecommunication systems
- K.leakage：Test methods and guide against information leaks through unintentional EM emissions
- K.secmlti：Mitigation methods against EM security threats

情報漏洩に関する国際規格はK.leakageが最初のものである。様々な文書においても電磁波を介した情報漏洩の脅威とその対策の必要性は指摘されているが、具体的な技術指標が示されたものは、この規格のみと言って差し支えない。測定法[7]-[9]、許容値に関して本研究の成果が展開されている。

6 むすび

2006年度から2010年度までにセキュリティ基盤グループで行われた電磁波セキュリティに関する研究成果の概要を述べた。実際はEMCグループと共同で測定手法に関する研究も進めたが紙面の都合上割愛し、理論ベースでの議論から実証実験までを行った電磁波による情報漏洩量の定量的評価手法について述べた。

電磁波セキュリティでの活動は画面情報の再現だけでなく、キーボード打鍵の際に生じる電磁波を観測することにより入力キーを特定する実験やSUICAの読み込みの際に生じる電磁波を観測しての攻撃など行った。さらに画面情報漏洩に関してはATM実機を持ち込んでの実験を行い（図25）、簡易型測定装置でも暗証番号の入力程度であれば十分に盗み見できることが分かった。このように、実生活で利用する電子機器、インフラへの攻撃可能性が明らかとなったが、社会への影響を考え発表には慎重にならざるを得なかった。

当初はノートPCに対するTEMPESTは実行が難しかったが、年を追う毎に簡単になった。これは盗聴技術の習熟が上がったこともあるが、年々、ノートPCが薄くなったことが理由に挙げられる。特にディスプレイが薄くなったことから防磁が十分になされず放出する電磁波が大きくなった。さらに低価格化により作りが簡易になった点も原因の1つである。また、携帯電話の画面に対する盗聴も試みたが、この研究期間では成功しなかった。2006年前後の携帯電話の画面では同期信号の発見が非常に難しかったからである。しかしながら昨今爆発的に普及しているスマートフォンは、ノートPCと同様のVESA規格に則った画面表示を行っているので、簡単に行えるのではないかと危惧する。

本研究活動は学術成果から技術移転による製品化、2件の競争的外部資金の獲得、国際標準化など、少ない人数で、4年間で実行したことは、非常に実りが多く充実した研究成果であったと言える。

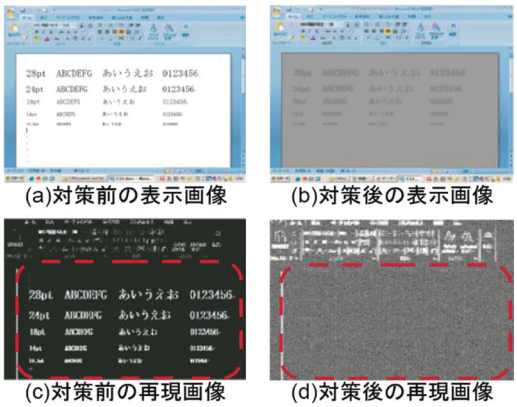

図24 CrypTypeの効果のデモンストレーション

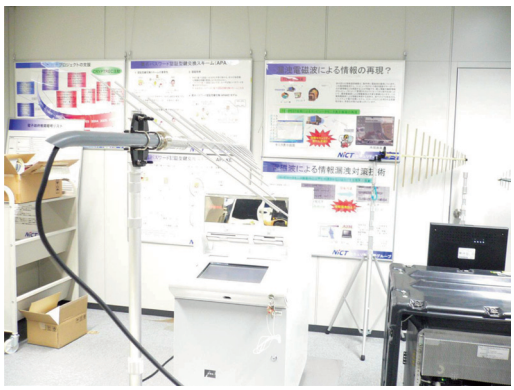

図25 ATM実機に対する実験風景

謝辞

関口秀紀専攻研究員（当時）、瀬戸信二短時間研究員（当時）には大変感謝します。特に少ない予算を補うためにSCOPEなどの外部資金の獲得に成功した反面、研究や実験に支障が出るくらいの書類仕事が増えてしまいましたが、精力的に処理して協力してくださいました。また、標準化ではNTT東日本（当時）の富永哲欣様に大変お世話になりました。感謝いたします。最後に測定だけでなく様々な助言をくださったEMCグループの山中グループリーダー（当時）、福永主任研究員（当時）、登坂専攻研究員（当時）に感謝いたします。

参考文献

1 H.Tanaka, “Evaluation of Information Leakage via Electromagnetic Emanation and Effectiveness of Tempest,” IEICE - Transactions on Information and Systems archive Vol. E91-D Issue 5, pp. 1439–1446, May 2008.
2 M.G.Kuhn and R.J.Anderson, “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations,” Information Hiding 1998, Lecture Notes in Computer Science Vol. 1525, pp. 200–210, Springer-Verlag, 1998.
3 True Type Tempest font, SearchFreeFont.com
4 セキュリティ産業新聞（2007年9月25日）.
5 月刊アスキー2007年12月号（2007年10月25日）.
6 関口，宮田，“TEMPESTソフトウェアCrypTypeの開発,” 2008年電子情報通信学会基礎・境界ソサイエティ大会，A-7-4, 2008.
7 登坂，山中，福永，服部，“プリンタから漏洩する電磁波に基づく印字情報再現性の評価,”平成20年電気学会全国大会，S2-7, 2008.
8 関口，瀬戸，“電磁雑音によるPCモニタ表示画像の情報漏洩評価方法,” 平成20年電気学会全国大会，S2-9, 2008.
9 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年電気学会全国大会，S2-8, 2008.

（平成23年6月15日 採録）

田中秀磨（たなかひでま）
ネットワークセキュリティ研究所
セキュリティ基盤研究室室長
博士（工学）
情報セキュリティ、暗号技術、情報理論