

## TEMPEST 技術を用いた映像傍受の実験 An Experimental Evaluation of Visual Eavesdropping via TEMPEST

○饗庭海斗<sup>1</sup>, 瀧川道生<sup>2</sup>, 三枝健二<sup>2</sup>\*Kaito Aeba<sup>1</sup>, Michio Takikawa<sup>2</sup>, Kenji Saegusa<sup>2</sup>

Abstract: An experimental evaluation was carried out to investigate visual data recovery on HDMI cables using TEMPEST. Clear images appeared at about 297 MHz, twice the pixel clock frequency, while metallic surroundings reduced leakage. This shows that the second harmonic of the pixel clock is most effective, and that metal shielding can suppress electromagnetic information leakage.

### 1. まえがき

情報社会の発展に伴い、電磁波セキュリティの重要性が高まっている。その脅威の一つとして、テンペスト技術が挙げられる。テンペスト技術とは電子機器が動作するとき外部に漏れる微弱な電波を検知し、処理・伝送されている信号やデータを傍受する技術である。これまでも HDMI ケーブルやディスプレイからの漏洩電波を用いて画像を再構成する研究や、情報流出の評価と対策を行った研究などが報告されている[1]。したがって、日常的に使用される機器からの漏洩電波の傍受の可能性を明らかにすることは、電磁波セキュリティにおいて重要であると言える。本稿では SDR(Software Defined Radio)を使用して、テンペスト技術による映像傍受の実験を行っていく。

### 2. 実験構成

図 1, 2 に本研究の実験構成を示す。図 1 はホイップアンテナを用いた構成、図 2 は八木宇田アンテナを用いた構成である。モニターと傍受用 PC をケーブルで接続し、ケーブルから漏洩する電波をソフトウェアツールを使用し、SDR で傍受する。ケーブルは HDMI1.4, SDR は HackRF One[3], ソフトウェアツールは TempestSDR を使用する。TempestSDR は電子機器から漏洩する電波を受信し、そこに含まれる映像信号を再構成するツールである[4]。SDR は観測用 PC と接続する。実験構成②ではアンテナと SDR の間に 300MHz の増幅器を設置する。

実験構成①のとき、受信周波数の変化、ケーブル周りの環境を変化させる。受信周波数はピクセルクロックの周波数に相当する。ピクセルクロックは水平のピクセル数と垂直のピクセル数、フレームレートを乗算した値である[2]。今回、解像度は $1920 \times 1080$ [px], リフレッシュレートは 60[Hz]で測定をした。本来、映像信号は画素だけでなく、余白・同期期間のブランキン

グも含めるので、水平、垂直の総ピクセル数はそれぞれ 2200[px], 1125[px]となる。これらの値を計算すると、ピクセルクロックは式(1)のように求められる[2]。

$$\begin{aligned} (\text{ピクセルクロック}) &= 2200 \times 1125 \times 60 \\ &= 148,500,000[\text{Hz}] \\ &= 148.5[\text{MHz}] \end{aligned} \quad (1)$$

式(1)で得られる周波数は映像モードに対応するピクセルクロックであり、HDMI の TMDS 符号化における基準周波数である。このピクセルクロックを 1 倍波とし、符号化方式やビット深度に応じて 1.25 倍, 1.5 倍, 2 倍といった高次の周波数成分が現れるため、今回の実験において、基準となる周波数とその倍波を対象に測定を行う。ケーブル周りの変化は金属とプラスチックの筒を使用し、筒の中にケーブルを通して測定する。

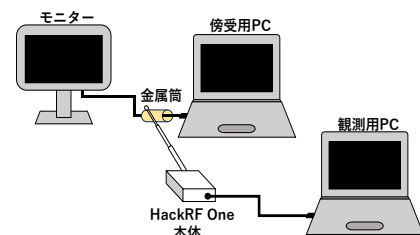


図 1 実験構成①

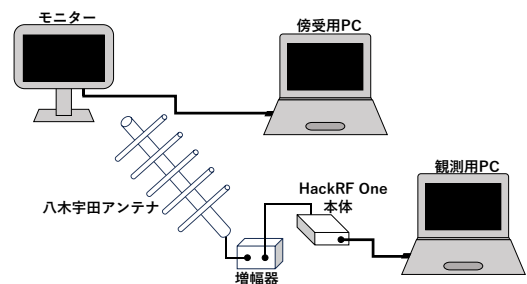


図 2 実験構成②

### 3. 実験結果

1: 日大理工・学部・電子 2: 日大理工・教員・電子

図3~8に1~6倍波の時の比較を示す。図4より、2倍波の297MHzの場合が最も鮮明に見えることが分かる。次いで、4倍波の場合が鮮明に見えるがコントラストがはっきりしない。

次に図9、10にそれぞれ金属、プラスチックの筒にケーブルを通した時の比較を示す。ケーブル周りの変化無しは前述の最も鮮明に見えた2倍波のものを使用する。ケーブルを筒に通した場合、プラスチック筒はほぼ変化が無かったが、金属筒に通すと文字の判別が難しくなることが分かる。このことから、ケーブル周りに金属があるとシールドの役割を果たし、電波をある程度遮断するが、プラスチックでは映像を傍受できてしまうことが分かった。

実験構成②ではケーブルから約50cm離して傍受することができた。図11に傍受画像を示す。距離を離して傍受をすることはできたが、あまり鮮明に見ることができなかった。これはアンテナの仕様周波数が325MHzで観測したい周波数297MHzとの差で本来の10[dB]の利得より低下してしまい、受信信号が弱まってしまったと考えられる。また、周囲の金属や壁で反射がおき、直接波と反射波の干渉で周波数成分が弱まると考えられる。



図3 1倍波(148.5MHz)



図4 2倍波(297MHz)



図5 3倍波(445.5MHz)



図6 4倍波(594MHz)



図7 5倍波(742.5MHz)



図8 6倍波(891MHz)



図9 金属筒



図10 プラスチック筒

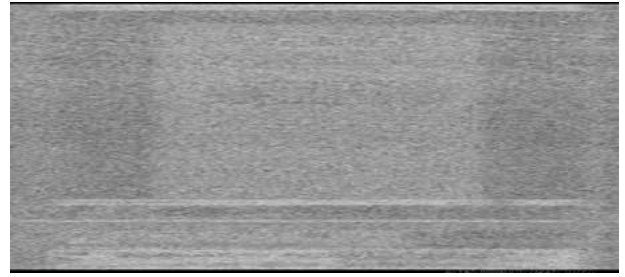


図11 八木宇田アンテナを用いた測定

#### 4. まとめ

本研究では、HDMIケーブルからの漏洩電波を利用したTEMPEST攻撃による映像傍受の実験的評価を行った。その結果、ピクセルクロック148.5MHzの2倍波に相当する297MHzにおいて最も鮮明な盗視画像が得られることを確認した。また、金属筒にケーブルを通した場合には画面文字の判別が困難となり、金属がシールドとして作用して漏洩を数dB低減する効果が確認できた。

さらに、八木宇田アンテナと増幅器を用いた実験では、ケーブルから約50cm離れた位置でも傍受が可能であることを確認したが、画像のコントラストは低下した。これらの結果から、今回の実験ではピクセルクロックの高調波が盗視に有効であり、特に2倍波の297MHzが有利であること、またケーブル周囲の金属環境が漏洩電波の遮蔽に効果的であることが明らかになった。

#### 参考文献

- [1] Cornell University, Deep-TEMPEST, arXiv, [https://arxiv.org/abs/2407.09717?utm\\_source=chatgpt.com](https://arxiv.org/abs/2407.09717?utm_source=chatgpt.com), 2025年9月28日
- [2] XILINX, AMD, <https://docs.amd.com/v/u/ja-JP/pg236-v-hdmi-rx-ss>, 2025年9月16日
- [3] <https://greatscottgadgets.com/hackrf/one/>, 2025年4月26日
- [4] <https://s34s0n.github.io/2019/07/10/TempestSDR/>, 2025年5月22日