電気学会論文誌 A（基礎・材料・共通部門誌）
IEEJ Transactions on Fundamentals and Materials
Vol.137 No.3 pp.153-157　　DOI: 10.1541/ieejfms.137.153

論　文

意図的な電磁妨害時にハードウェアトロイによって引き起こされる情報漏えい評価

非会員　衣川　昌宏*　　正　員　林　　優一**　　非会員　森　　達哉***

Evaluation of EM Information Leakage caused by IEMI with Hardware Trojan

Masahiro Kinugawa*, Non-member, Yu-ichi Hayashi**, Member, Tatsuya Mori***, Non-member

（2016 年 4 月 20 日受付，2016 年 9 月 18 日再受付）

Hardware Trojans (HT) that are implemented at the time of manufacturing ICs are being reported as a new threat that could destroy the IC or degrade its security under specific circumstances, and is becoming a key security challenge that must be addressed. On the other hand, since it is also common to use components manufactured or bought via third parties in portions outside of the substrate on which the IC is mounted or communication lines connecting the IC and the substrate, there is a possibility that HTs may also be set in the peripheral circuits of the IC in the same manner as in the IC. In this paper, we developed an HT that could be implemented in the peripheral circuits and wiring of an IC, investigated the possibility of being able to acquire information processed inside a device by measuring the electromagnetic waves generated and leaked by Intentional Electromagnetic Interference (IEMI) with HT outside the device, and investigated detection methods for cases where such HTs are implemented.

キーワード：電磁妨害，電磁情報漏洩，ハードウェアトロイ
Keywords：intentional electromagnetic interference, electromagnetic information leakage, Hardware Trojans

1. はじめに

電子機器に対する妨害には，電子機器から非意図的に発生する電磁波によって周囲の機器が電磁妨害を受ける問題（EMI: Electromagnetic Interference）と故意に電磁波を発生させ機器を妨害する問題（IEMI: Intentional Electromagnetic Interference）に大別できる。これまで環境電磁工学分野では，EMI に対し妨害電磁波を生じさせる機器に対策技術を施し妨害電磁波の発生を抑制するほか，機器のイミュニティ（妨害電磁波に対する機器の耐性）を向上させる取り組みがなされてきた[1]。これまでのこうした取り組みに基づき，機器のイミュニティに基準値が設けられ，多くの電子機器はこの基準値を満たして設計される。そのため，電子機器の非意図的な電磁波に対する耐性は向上している。

一方，IEMI に対する機器のイミュニティは EMI に対するイミュニティに比べ，より厳しい値が要求される。こうした IEMI に対しても機器の動作を保証するためには，これまでの EMI に対する基準値策定とは別の視点からの検討が必要となる。環境電磁工学の分野では，IEMI は，主に機器の可用性を損なう脅威として捉えられており，これまでに「意図的な妨害波のシステムへの伝搬過程の解明」，「意図的な電磁妨害によりシステムが受ける影響の解析」や「意図的な電磁妨害からのシステムや通信の保護」について検討がなされている[2][3]。

本稿では上述した可用性低下に加えて，IEMI により機器内部で処理される機密度の高い情報が漏えいする可能性，即ち，機密性，完全性を低下させる可能性について検討を行う。具体的には，電子機器を構成するプリント基板及び接続線路などに，設計者の意図に反した回路（ハードウェ

* 仙台高等専門学校情報ネットワーク工学科
〒989-3128　仙台市青葉区愛子中央 4-16-1
Department of Information Networks, National Institute of Technology, Sendai College
4-16-1, Ayashi-chuo, Aoba, Sendai 989-3128, Japan
** 東北学院大学工学部
〒985-8537　多賀城市中央 1-13-1
Faculty of Engineering, Tohoku Gakuin University
1-13-1, Chuo, Tagajo 985-8537, Japan
*** 早稲田大学基幹理工学部情報通信学科
〒169-8555　東京都新宿区大久保 3-4-1
Communication Engineering Department, Waseda University
3-4-1, Okubo, Shinjuku-ku, Tokyo 169-8555, Japan

アトロイ）を付加し，IEMI 実行時の情報漏えいの有無を実験を通じて確認する。

2. 本稿で用いる基板や接続線路に実装可能なハードウェアトロイの特徴と情報漏えいの原理

〈2･1〉 本稿で実装するハードウェアトロイの特徴

ハードウェアトロイ（HT: Hardware Trojan）は設計者の意図しない動作により，機器内部の情報を漏えいさせることが知られている[4]~[8]。そのため，新たなセキュリティの脅威として注意喚起が行われており，対処しなければならない重要なセキュリティ課題の 1 つとなっている。

これまで，IC の製造過程でその内部に実装される HT を対象に検出方法などが検討されてきたが[9]~[13]，本稿では IC の製造後に，周辺回路や配線に実装可能な HT について検討する。こうした実装が可能な場合，HT の脅威となる対象機器が拡大する恐れがあり，これまで HT の脅威を考慮する必要がなかった機器でもその対策が求められる可能性がある。さらに，実験を通じて，この HT が IEMI の実行時に動作し，情報を漏えいさせることを確認する。

具体的には，MOSFET と簡単な配線で構成される HT 回路を作製し，機器に実装する。そして，HT を実装した機器に特定の周波数の電磁波を意図的に照射し，これをキャリア信号として用い，変調信号を機器内部で処理される情報信号とした被変調信号を生成し，機器外部へ漏えいさせる。

〈2･2〉 本稿で扱う HT が引き起こす情報漏えいの原理

Fig. 1 に本稿で用いる HT の概念図を示す，回路は 1 つの MOSFET と短い配線からなり，機器外部に電磁波を通じて情報を放射するアンテナとしては，基板上の配線パターンや機器に接続された線路を用いる（以後，これらを非意図的なアンテナ（Unintentional Antenna）と呼ぶ）。また，非意図的なアンテナ構造となる場所に観測対象とする信号が伝送されているとは限らない。一方で，基板上の配線パターンや機器に接続された線路を伝搬する信号は，配線路上から他の線路，基板との結合により，基板全体，および接続線路に漏えいすることが従来研究より明らかになっているため[14][15]，漏れ信号が計測される場所と非意図的なアンテナ構造が隣接する位置に HT を実装することで，HT を動作させることが可能となる。

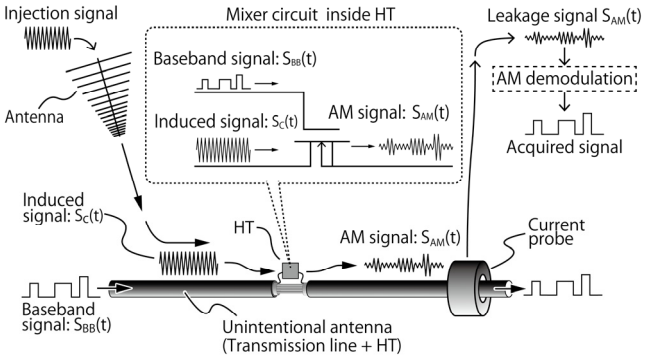

Fig. 1. Conceptual diagram of HT on substrate and attached line.

続いて HT による情報漏えいが引き起こされる原理について説明する。機器内部の情報漏えいは，非意図的なアンテナの共振周波数となる電磁波を照射した際に発生する。この時，電磁波の照射及び観測は，空間を通じてアンテナから行うことも，機器に接続された電源線などからカレントプローブなどを用いて行うことも可能である。また，それらの組み合わせでも可能である。

本稿で検討を行う IC の周辺回路や配線に実装可能な HT の具体的な原理は 2 つの信号の乗算を行うミキサ回路の動作で示される。ミキサ回路は漏えい対象とする機器内部の信号 $s_{BB}(t)$ と外部から照射した電磁波により誘起された信号 $s_C(t)$ を乗じ，$s_C(t)$ をキャリア信号，$s_{BB}(t)$ をベースバンド信号とする振幅変調 (AM) 信号 $s_{AM}(t)=s_{BB}(t)s_C(t)$ を発生させる。そして，$s_{BB}(t)$ の時間変化は AM 信号 $s_{AM}(t)$ として，非意図的なアンテナにより機器外部に放射される。本稿で用いる HT は 1 つの MOSFET から構成される受動ミキサ回路と見なすことができる。

続いて，振幅変調された漏えい電磁波 $s_{AM}(t)$ を，機器に照射した周波数で受信し，その周波数をキャリアとみなし，AM 復調することで，機器内部の観測対象とする信号 $s_{BB}(t)$ を取得できる。こうした動作は，アクティブ型の攻撃[16]とパッシブ型[17]の攻撃を組み合わせて情報を取得する攻撃と捉えることもできる。

また，キャリアとなる信号 $s_C(t)$ は機器外部から照射する電磁波により機器内部に誘起されるため，照射する強度を変化させることで，変調される信号強度も異なる。そのため，MOSFET が動作する範囲内の強い強度で電磁波を照射することにより，放射信号を増大させることが可能となるため，観測距離を制御することが可能となる。

3. キーボードへの HT の埋め込みと漏えいした情報の取得

本章では HT を実装し，機器内部の情報を取得する具体的な対象としてキーボードを用いる。まず，対象となるキーボードの制御回路と PC とを接続する信号線路に HT を実装し，外部から照射する電磁波の周波数を用いて機器内部の情報を振幅変調して機器外部に放射させる。さらに，機器外部でそれらを AM 復調することでキー入力情報を取得可能であることを示す。

〈3･1〉 ターゲットとなるキーボードの説明

ターゲットとなる PS/2 キーボードは内蔵されたマイクロコンピュータによってキーマトリクス上のキー入力を検出し，各キーに割り当てられたスキャンコード値をホストへ送信している。Fig. 2 にキーボードから送信されるキー入力情報および通信信号の概略図を示す。

ホストとはデータとクロックバス，正負の電源ラインを含んだ 4 芯シールドケーブルで接続される。通信信号は電源ラインのグラウンド電位を基準とした TTL レベルの正論理 2 値信号として，データバスとクロックバスへ送出される。送出される信号は同期シリアル信号であり，データバ

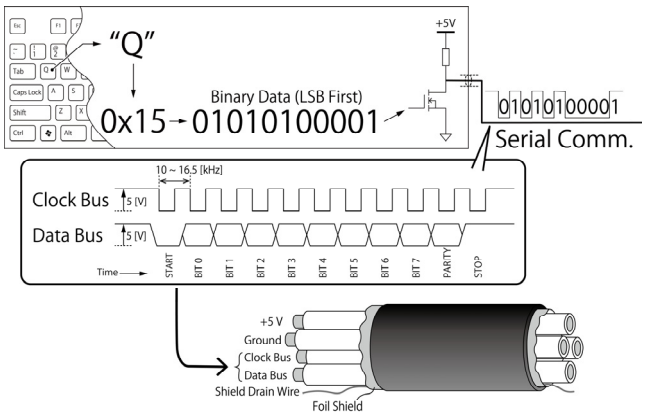

Fig. 2. Target keyboard.

スの値はクロックバスの信号立ち上がり時に確定される。ホストへ送信されるデータは 11 ビットであり，スタートビット，最下位ビットを先頭とした 8 ビットのデータ，奇数パリティビット，ストップビットから構成される。クロック周波数は 10〜16.5 kHz である。

キー入力に対応したスキャンコードは 1 バイト以上のデータであり，前述のシリアルデータとして 1 バイトごと順次ホスト PC へ送信される。

本稿では HT を用いて，シリアルデータとしてホスト PC に送信される信号を取得し，機器外部へ漏えいさせる。

〈3･2〉 HT 回路とその実装 続いて，実験で用いた HT の回路図及び実装方法を Fig. 3 に示す。本回路は MOSFET と抵抗及び基板からなる。入出力端子としては Fig. 3 に示す様に Pin1 から Pin3 までを備えている。

本実験では，各 Pin をキーボードの通信線に接続し，情報漏えいを誘発する。Pin1 はデータバス，Pin2 はキーボード側のシールドドレイン線，Pin3 はホスト側のシールドドレイン線に接続し，照射した電磁波により Pin2-Pin3 間に生じた交流信号と MOSFET を用いて Pin1 から入力されたキーボードの通信信号を乗じることにより，振幅変調された信号が生成される。そして，本信号が非意図的なアンテナに伝搬することにより，機器外部への放射が発生する。さらに，これらを機器外部で AM 復調することにより，キー入力に応じて生ずるデータ信号の取得が可能となる。

本実験で試作した HT は実験の了解性を高めるため基板実装を行ったため，ケーブルの外皮で覆うにはサイズが大きい。一方で，本実験と同等の機能を有する HT を MOSFET と配線のみで構成することも可能であり，これらは外皮などで覆うことが容易である。

〈3･3〉 実験環境 実験環境とパラメタを Fig. 4 及び Table 1 に示す。HT が動作するトリガとなる電磁波は，機器外部からログペリオディックアンテナを用いてキーボードにむけて照射する。また，照射する周波数はキーボードのケーブル長がおおよそ半波長となる 330 MHz とし，給電電力は 29 dBm とした。

機器外部から照射された電磁波によってケーブルに誘起されたキャリア信号を，FET のゲートに接続したキーボードの通信を流れる情報信号を用いて，遮断／導通させることにより，シールド外皮に AM 信号が生ずる。

そして，この AM 信号をキーボードの接続線路上にクランプした電流プローブを用いて取得することで，漏えいの有無を確認する。

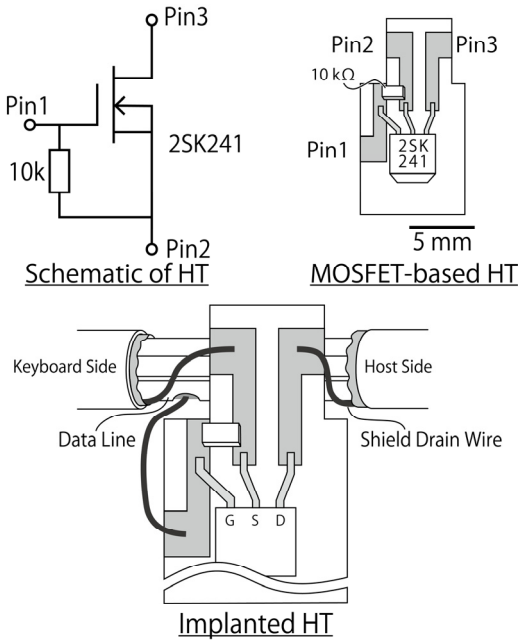

Fig. 3. Employed HT and mounting position.

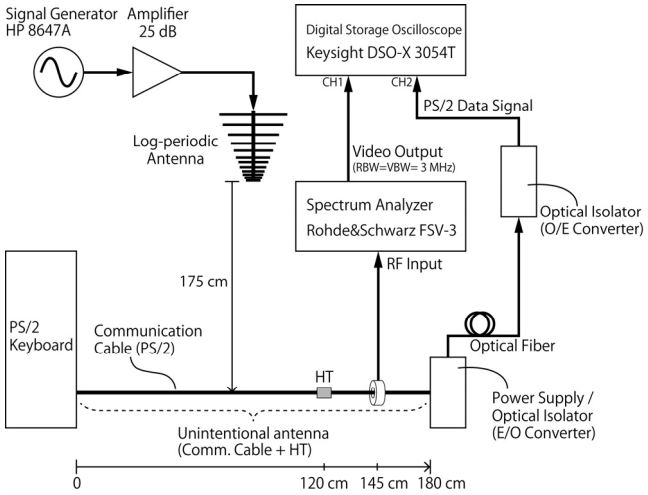

Fig. 4. Block diagram of experimental environment.

Table 1. Experimental parameters.

Target keyboard	PS/2 109 Keyboard
Transmission antenna	Ettus Research LP0410
Current probe (Receiver)	FCC F-2000
Arbitrary-signal generator	HP 8647A (330 MHz, 4 dBm)
Spectrum analyzer	Rohde&Schwarz FSV-3 (fc = 330 MHz, RBW/VBW = 3 MHz)
Oscilloscope	Keysight DSO-X 3054T

本実験で電流プローブにより観測した信号は，通信線路上に分布した線路をアンテナとして分布するコモンモード電流であり，これにより機器外部への放射が発生する。また，こうした電流は機器に接続された電源線などに伝搬することが知られており[14][18]，電源線やそれらが接続される配電盤などにおいても漏えい情報が観測できる可能性がある。

観測する周波数は照射する周波数と同様の 330 MHz であり，観測後，Fig. 4 に示すスペクトラムアナライザのゼロスパンを用いて AM 復調を行うことで，PS/2 通信線のデータ信号を取得する。

また，電流プローブにより取得した信号が PS/2 通信線を流れるデータ信号と同等であることを確認するために，Fig. 4 内の Optical Isolator を用いて，PS/2 通信線を流れるデータ信号を参照データとして取得した。

〈3･4〉　HT により漏えいした情報の取得　続いて HT を実装したキーボードからの情報漏えいの可能性について実験を通じて具体的に検討する。

Fig. 5(a) に「Q」を入力した場合に PS/2 通信線のデータ信号を機器内部でタッピングして観測した波形を示す。時間に応じて電圧が変動することで，キー固有の信号パターンを表していることが分かる。

続いて，Fig. 5(b) に HT に意図的な電磁妨害を行った場合に電流プローブで観測される時間領域波形を示す。本条件では HT によって，キーボード内部の信号と同様の時間変化をしている信号が計測され，キー入力に対応する信号が漏えいしていることがわかる。

続いて，電磁波の照射を停止し，HT が動作しない場合に電流プローブで計測される波形を Fig. 5(c) に示す。キー入力を行っているにも関わらず，Fig. 5(a), (b) で観測された様なキーの入力に応じて発生する固有の信号パターンは観測されない。

本計測結果より，外部から照射した電磁波により，機器内部のデータ信号をタッピングして得られた Fig. 5(a) の結果と同様の入力キーに対応する電圧の時間変動を計測できていることが分かる。また，本節では「Q」を入力した結果のみを示しているが，他のキーにおいても同様の漏えいが生ずることを確認した。

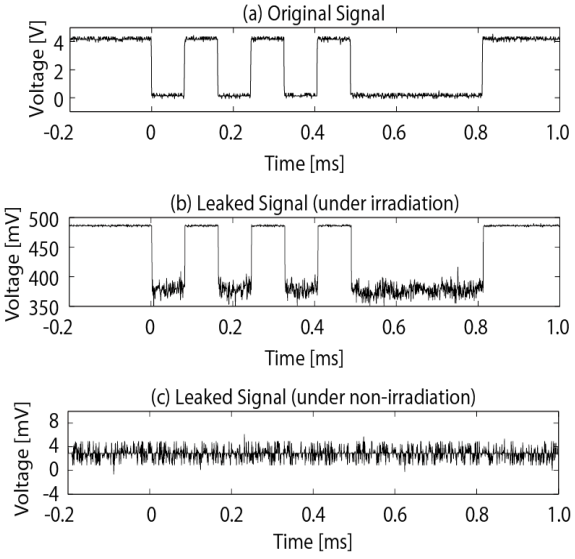

Fig. 5.　Leakage signals caused by HT.

本実験では，非意図的なアンテナ上にクランプした電流プローブにより漏えい電磁波を計測したが，本電流が放射を引き起こす主要因の 1 つであることから，キーボード周囲に設置したアンテナなどにより，漏えいを確認することも可能であると考えられる。また，前述した様に，これらの電流が PC などに接続された電源線などに伝搬することにより，電源線上，その先にある配電盤などにおいても漏えい信号を確認することが可能になると考えられる。

4.　対策手法の検討

本実験で実装した HT は，機器外部から意図的な電磁妨害を行うことで動作し，機器内部の情報を振幅変調し，電磁波を通じて機器の内部情報を外部に漏えいさせる。

一方で，漏えい対象となるキーボードの信号は一定の周期を有することが過去の検討で明らかとなっている。そのため，文献(19)の様に，機器外部から機器に電磁波を広帯域に照射し，同時に機器周辺での電磁波を計測し，広帯域にわたって AM 復調を行い，内部の信号と同様の周期が復調後に観測されるか否かについて確認することで，IC の周辺回路や配線に HT が仕掛けられているか否かを検出できる可能性がある。

ただし，一般環境で放射できる電磁波の周波数は法律により制限されているため，こうした試験を行う際には，電波暗室などの設備が整備された環境下で行うことが必要となる。

5.　ま と め

本稿では IC の周辺回路や配線に実装された HT が IEMI の実行時に情報を漏えいさせる可能性について検討を行った。実験で用いた HT は MOSFET と短い配線からなる簡単な回路で構成され，容易に実装可能な回路とした。また，IEMI の実行時のみ HT が動作し，機器内部の情報を照射した周波数で振幅変調した信号を外部へ放射することで情報の漏えいを生じさせることを確認した。

さらに，機器内部の配線構造や基板に接続された通信線などの非意図的なアンテナを用いて振幅変調された信号を放射させることで，機器外部で漏えい信号を観測し，情報を復元できることを確認した。

本稿では HT を実装する対象をキーボードとしたが，これまで電磁波を通じた情報漏えいが確認されている様々なデバイスについて同様の脅威が存在する可能性があるため，今後はこうしたデバイスについても HT が実装される可能性について検討を行う予定である。また，効果的な対策手法及びより詳細な漏えいのメカニズムについても，検討を進める予定である。

謝　辞

本研究は科研費（16H02831）の助成を受けたものである。

文　　献

(1) C. R. Paul : Introduction to Electromagnetic Compatibility, Wiley Series in Microwave and Optical Engineering, Wiley-Interscience, New York (2006)
(2) IEC SC77C : Electromagnetic compatibility (EMC)－Part 1-5: General－High power electromagnetic (HPEM) effects on civil systems, IEC TR 61000-1-5 (2004-11)
(3) W. A. Radasky, C. E. Baum, and M. W. Wik : "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)", *IEEE Trans. Electromagn. Compatibility*, Vol.46, No.3, pp.314-321 (2004-8)
(4) Z. Gong and M. X. Makkes : "Hardware Trojan side-channels based on physical unclonable functions", WISTP 2011, LNCS 6633, pp.293-303 (2011)
(5) J. Clark, S. Leblanc, and S. Knight : "Risks associated with USB Hardware Trojan devices used by insiders", 2011 IEEE International on Systems Conference (SysCon), pp.201-208 (2011-4)
(6) M. Ossmann : "The NSA Playset: RF Retroreflectors", DEF CON 22 (2014-8)
(7) M. Ossmann : "The NSA Playset: A Year of Toys and Tools", black hat USA (2015-8)
(8) R. J. Anderson : Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley-Interscience, New York (2008)
(9) R. Rad, J. Plusquellic, and M. Tehranipoor : "Sensitivity analysis to hardware Trojans using power supply transient signals", IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), pp.3-7 (2008-6)
(10) J. Yier, N. Kupp, and Y. Makris : "Experiences in Hardware Trojan design and implementation", IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), pp.50-57 (2009-7)
(11) L. Lin, W. Burleson, and C. Paar : "MOLES: malicious off-chip leakage enabled by side-channels", IEEE/ACM International Conference on Computer-Aided Design (ICCAD '09), pp.117-122 (2009-11)
(12) S. Bhasin, J.-L. Danger, S. Guilley, X. T. Ngo, and L. Sauvage : "Hardware Trojan Horses in Cryptographic IP Cores", Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp.15-29 (2013-8)
(13) M. Kasper, A. Moradi, G. T. Becker, O. Mischke, T. Güneysu, C. Paar, and W. Burleson : "Side channels as building blocks", *J. Cryptographic Eng.*, Vol.2, No.3, pp.143-159 (2012-10)
(14) Y. Hayashi, N. Homma, T. Mizuki, T. Sugawara, Y. Kayano, T. Aoki, S. Minegishi, A. Satoh, H. Sone, and H. Inoue : "Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current", *IEICE Trans. Electronics*, Vol.E95-C, No.6, pp.1089-1097 (2012-6)
(15) Y. Hayashi, N. Homma, T. Mizuki, H. Shimada, T. Aoki, H. Sone, L. Sauvage, and J.-L. Danger : "Efficient Evaluation of EM Radiation Associated with Information Leakage from Cryptographic Devices", *IEEE Trans. EMC*, Vol.55, No.3, pp.555-563 (2013-6)
(16) S. Mangard, E. Oswald, and T. Popp : Power Analysis Attacks – Revealing the Secrets of Smart Cards, Springer-Verlag, New York, NY, USA (2007)
(17) M. Joye and M. Tunstall : Fault Analysis in Cryptography, Springer-Verlag, New York, NY, USA (2012)
(18) M. Kinugawa, Y. Hayashi, T. Mizuki, and H. Sone : "Information leakage from the unintentional emissions of an integrated RC oscillator", EMC Compo 2011 - 8th Workshop on Electromagnetic Compatibility of Integrated Circuits, pp.24-28 (2011-11)
(19) 林　優一・本間尚文・鳥海陽平・高谷和宏・青木孝文：「電磁的画面盗視における漏えいパラメタの高速推定法に関する検討」，2016 年暗号と情報セキュリティシンポジウム (SCIS2016) 予稿集，2F2-2 (2016-1)

衣　川　昌　宏

（非会員） 2004 年 3 月会津大学コンピュータ理工学部卒業。2006 年 3 月同大学大学院コンピュータ理工学研究科博士前期課程修了。同年 4 月（株）Eyes, JAPAN 入社。2009 年 3 月同退職。2010 年 9 月東北大学大学院情報科学研究科博士前期課程修了。2013 年 3 月同博士課程修了。同年 4 月仙台高等専門学校助教。環境電磁工学，情報セキュリティ，レーダ信号処理に関する研究に従事。博士（情報科学）。電子情報通信学会会員。

林　　優　一

（正員） 2003 年 3 月会津大学コンピュータ理工学部卒業。2009 年 3 月東北大学大学院情報科学研究科博士課程修了。同年東北大学大学院工学研究科 COE フェロー。2012 年同大学大学院情報科学研究科准教授。2015 年東北学院大学工学部准教授。環境電磁工学，情報セキュリティの研究に従事。博士（情報科学）。IEEE EMC Society 電磁情報漏えいに関する分科委員会委員長（第 5 技術委員会）。IEEE，電子情報通信学会会員。

森　　達　哉

（非会員） 1997 年早稲田大学理工学部応用物理科卒業。1999 年同大学大学院修士課程修了。同年日本電信電話（株）入社。2007～2008 年米国ウィスコンシン州立大学マディソン校客員研究員。2013 年より早稲田大学基幹理工学部准教授。情報セキュリティに関する研究に従事。情報科学博士。2009 年電子情報通信学会英文 B 誌論文賞，2010 年電気通信普及財団テレコムシステム技術賞受賞。電子情報通信学会，情報処理学会，ACM，IEEE，USENIX 会員。