AI/IoT 社会を守る電磁波セキュリティの開拓

研究代表者	衣川昌宏	独立行政法人国立高等専門学校機構 仙台高等専門学校 総合工学科　助教
共同研究者	林　優一	奈良先端科学技術大学院大学　先端科学技術研究科 情報科学領域　教授

1 はじめに

情報通信技術の社会インフラ化により、相互に接続された情報通信機器から提供される情報（ビッグデータ）が個人から社会に及ぶ広範なデータ駆動型社会を構築している。また、より効率的な情報活用および判断の正確性、ユーザ毎に最適化された情報提供を実現するためAIおよびIoTを活用した情報システムによる社会実現が進められている。このシステム上で扱われるデータは個人情報から環境データ、経済、行政等から構成される様々なセキュリティレベルを有しており、データに応じた適切な保護がなされた流通が求められる。また、データのセキュリティだけでなく、実世界への作用も AI/IoT システムの特徴である。例えばAI/IoT システムに不具合が生じた場合の被害は、自動車の自動運転や空調制御など人命に関わるレベルのものから、スマートフォンのディスプレイを介した人間への行動指示など、軽微なものから重大なものに至る幅広いものであるが、これらは被害の程度にかかわらず単にAI/IoT システムの不具合であり、システムを構成する図1に示す各層全てがその原因となる恐れがある。

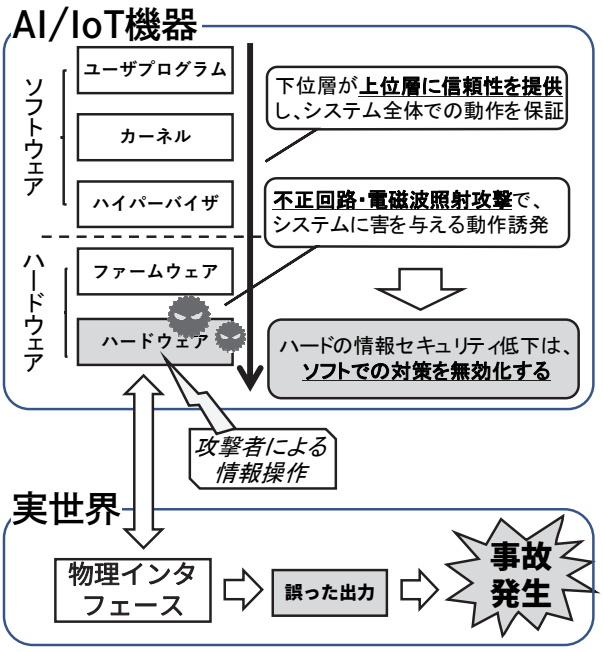

図1　AI/IoT 機器・システムのモジュール構造化によるトラストチェーンおよびその安全性の基盤となるハードウェアセキュリティ

情報と人間および社会の調和による Society 5.0[1]を実現するための基盤である AI/IoT 社会システムには、情報通信機器が社会や身の回りに普遍的に溶け込んでいる環境を実現するだけでなく、水や空気と同様に安全性も求められる。AI/IoT 機器の安全性については図1の各層間の信頼によるトラストチェーンにより担保されており、ハードウェアを最下位層の基礎とした積み上げ式のモジュール構造となっている。このモジュール構造化により、応用機器やサービスの開発時には既存の機能モジュールを組み合わせることで短期間かつ容易に機能を実装できる。しかしその反面、機能ブロックに脆弱性が含まれている場合、例え設計者が考案したアルゴリズムや構造に欠陥がなくとも脆弱性を有することとなる[2, 3]。これら機能モジュールに不具合やセキュリティの脆弱性が発見された場合、ソフトウェアは Firmware Over-the-Air (FOTA)を用いて無線ネットワーク経由で対策プログラムの適用が可能である。一方、ハードウェアの場合は Field Programmable Gate Array (FPGA)等の再構成可能集積回路（IC）を除いて、プリント配線基板上や機器筐体内部の配線、またセンサ類のハードウェア構造の改修は、AI/IoT 機器の総数が多量であることに加え、工場出荷後の物理的設置場所の特定の困難さ、改修に必要な工数・人件費を考慮すると現実的ではない。

ハードウェアは情報セキュリティの根底であり、現在運用されている情報システムの情報セキュリティはハードウェアの信頼性に依存した構造となっている。このハードウェアの信頼性確保は、パーソナルコンピュータ（PC）アーキティクチャベースのサーバコンピュータや、情報通信網を構成するルータやスイッチ等の回線交換機の場合、ハードウェアの故障に対して予備のハードウェアを準備することによる可用性対策として実施されている。機密性や完全性の確保に関しては、機器仕様として設計・製作時に考慮されており、機器出荷後の機密性・完全性の低下防止はハードウェアの改変困難さを根拠とした信頼性に依存している。

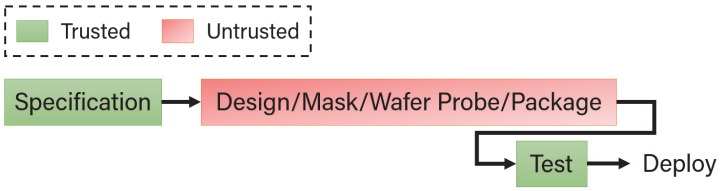

図 2　IC へハードウェアトロージャンが実装されるタイミング

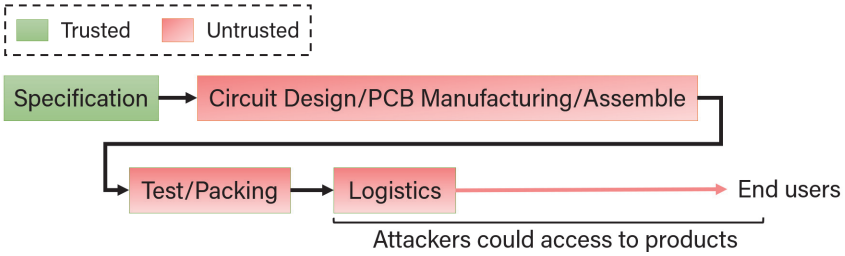

図 3　IC 周辺回路へハードウェアトロージャンが実装されるタイミング

しかしながら、この機密性や完全性を低下させる原因の一つとして、ハードウェアを構成する IC 製造時に組み込まれる不正回路の存在が指摘されており[2, 4-7]、実際にそれが原因となった機器の不具合も報告されている[4]。この不正回路はハードウェアトロージャン（Hardware Trojan）と呼ばれ、図 2 に示す IC の製造工程で組み込まれる可能性があることが報告されている[2, 4-8]。そのハードウェアトロージャンは IC 設計者や IC の利用者に発見されず、IC の特定の動作をトリガとして動作し、攻撃者が意図した異常動作や破壊等システムのセキュリティを低下させる動作を発生させる。IC のハードウェアトロージャンの混入は IC の製造工程の都合上、設計から工場での生産期間で発生する(図 2)。そのため IC のエンドユーザが真正性を確認する方法が必要となっている[8]。しかしながら、この不正回路「ハードウェアトロージャン」の問題の特性上、問題は IC だけに限定されず、IC 周辺の回路も同様に不正改変を受ける恐れがある。

IC 周辺回路、すなわちプリント配線基板や AI/IoT 機器筐体内の回路自体は IC に比較して、図 3 に示すように不正改変を受けるタイミングが長期間にわたり、攻撃者にとって攻撃難易度が低くなっている。特に AI/IoT 機器は実空間に組み込まれて使用されるため、機器設置後の機器動作の正常性確認は機器からアップロードされるデータが正常であるか、もしくは音声やアクチュエータ等の出力が正常であるか程度の確認にとどまる。そのため、AI/IoT 機器使用中に機器を構成する回路に不正回路が埋め込まれたとしても、異常動作が生じるまで攻撃が発覚しにくい。実際、サーバハードウェアのプリント配線基板上に不正な回路が実装される攻撃が報道されており[9]、この IC 周辺回路の部品レベルでのハードウェアトロージャン問題は既に現実問題となっている。

そこで、本研究ではこれらハードウェアトロージャン問題のうち、AI/IoT 機器を構成する IC 周辺回路への攻撃について、特に攻撃の痕跡が残りにくい電磁波照射を併用した攻撃について、その攻撃の原理解明および対策手法の開発を以下の 4 項目に関して行った。

a)　電子回路基板の回路改変が行われる可能性の調査
b)　回路改変と電磁波攻撃の併用攻撃が情報セキュリティへ与える影響の評価
c)　回路改変を必要としない電磁波照射による情報漏えい現象の発見と原理解明
d)　製造後の AI/IoT 機器への回路改変と電磁波攻撃の基礎的対策技術の開発

2 電子回路基板の回路改変が行われる可能性の調査

2-1 AI/IoT 機器の内部構造調査

AI/IoT 機器に対する回路改変攻撃について、実際の AI/IoT 機器の構造を解析することにより、攻撃の難易度を調査し、本攻撃手法が図 3 に示す攻撃可能な期間に発生する可能性を調査した。

スマートスピーカなどに代表される AI/IoT 機器を分解調査した結果､現在の AI/IoT 機器はインターネット上のサーバでの情報処理能力に強く依存しており、AI/IoT 機器自体が有する機能をセンサやアクチュエータの操作に絞り込むことによる AI/IoT 機器の低コスト化や、それら限定された機能の内蔵機器を応用したサービスプラットフォームの提供に徹していることが判明した。この結果は、AI/IoT サービスの開発コストはソフトウェア重視となっていることを示しており、AI/IoT 機器自体のハードウェアは汎用部品が中心となったアーキティクチャで内部構造も予想しやすい。さらに、汎用部品を使用するため、セキュリティが考慮されていない回路内通信プロトコルが用いられており、機器内部の信号に干渉することにより容易に情報窃盗や意図的な誤動作・誤作動を発生可能であることも明らかとなった。

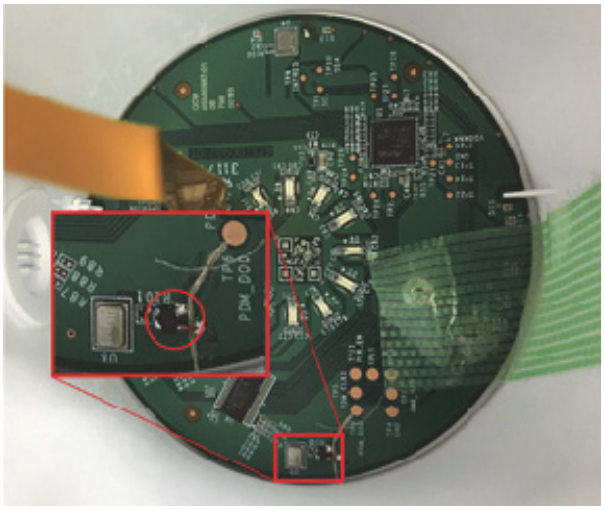

図 4　スマートスピーカ内部に実装されたハードウェアトロージャン（丸囲み内の素子）

実際にスマートスピーカへ不正回路を実装した例を図 4 に示す。回路改変に電磁波照射を併用する攻撃では、機器内部の情報を外部へ漏えいさせる際にインターネット接続等の通信チャネルを必要とせず、機器に照射された電磁波をそのまま変調することにより、機器外部へ無線通信により情報を漏えいすることが可能である。そのため、インターネットや Bluetooth 等へのデータ送出に必要なプロトコルスタックのハードウェア実装が不要となり、電磁波を変調する機構が実装されるだけで攻撃が成立する。電磁波を変調する機構は単純な高周波信号のミキサ回路で実装可能であり、AI/IoT 機器内部の IC 間通信信号であれば 1 つの FET で、その通信信号を漏えいさせるハードウェアトロージャンを実装可能である。図 4 はスマートスピーカを操作する際に生じる入力情報をタッピングし、さらに機器のプリント配線基板をそのままアンテナとして用いることにより情報漏えいを生じさせている例である。図 4 に示したハードウェアトロージャンの動作概要を図 5 に示す。ハードウェアトロージャンはタッピングした信号と照射された電磁波を混合（乗算）することにより振幅変調信号を生成し、プリント配線基板自体をアンテナとして利用することで攻撃者へタッピングした信号を送信している。攻撃者は受信した信号を振幅復調することにより、機器内部のデータを取得することが可能である。このように、1 つの部品を既存回路に挿入するだけで攻撃準備が完了し、実際の攻撃は遠隔から任意のタイミングで電磁波を照射するだけで可能となる。

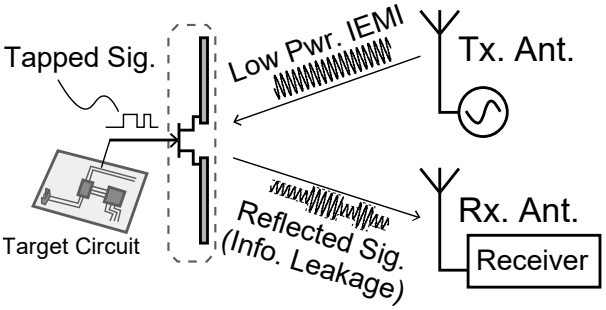

図5　機器内に実装されたハードウェアトロージャンと電磁波照射を併用した情報窃盗の原理

本調査の結果、AI/IoT 機器のセンサやアクチュエータ等の入出力機能および機器を構成する IC 間の通信信号は、機器機能の実装に要するコストを抑えると共に、機能のモジュール化に伴った共通の IC 間通信プロトコルを用いていることから、それら信号をハードウェアトロージャンでタッピングすることにより容易に機器の情報処理へ介入可能であることが明らかとなった。さらに、その実装は 1 つの FET を実装するだけで完了することから、図 3 に示した攻撃可能なタイミングで十分実装可能であることが示された。

3 電磁波攻撃が情報セキュリティへ与える影響の評価

2 章の調査結果から、AI/IoT 機器構造を単純化したモデルを用いた電磁波照射併用型の回路改変攻撃について検討を進めた。また、本調査の途上で回路改変不要の電磁波照射による情報窃盗の可能性を発見し、その原理および情報窃盗の可能性についても検討を進めた。

3-1 回路改変と電磁波攻撃の併用攻撃が情報セキュリティへ与える影響の評価

本節では AI/IoT 機器を単純化したモデルを作成し、回路改変と電磁波照射による情報漏えいの定量的評価につながる評価手法の検討を進めた。AI/IoT 機器内部での攻撃対象となる信号を IC 間通信プロトコルとして、その信号電圧および周波数における漏えい信号の評価システムを構築した。単純化モデルを図 6 に、評価システムを図 7、測定結果を図 8 に示す。

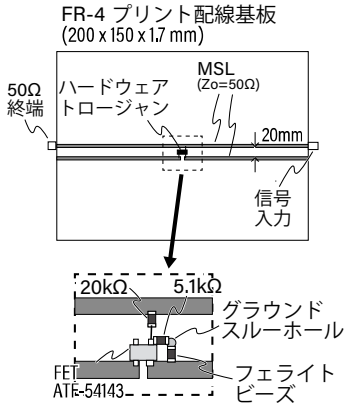

図 6　機器とハードウェアトロージャンの単純化モデル

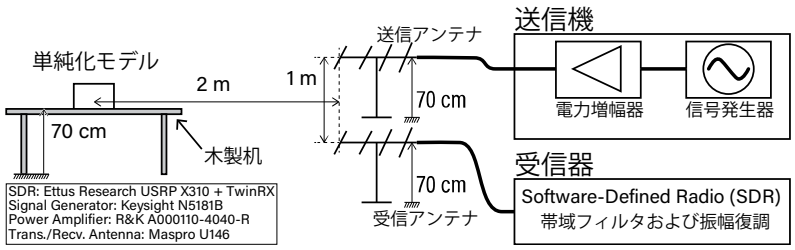

図 7　評価システムおよびその配置

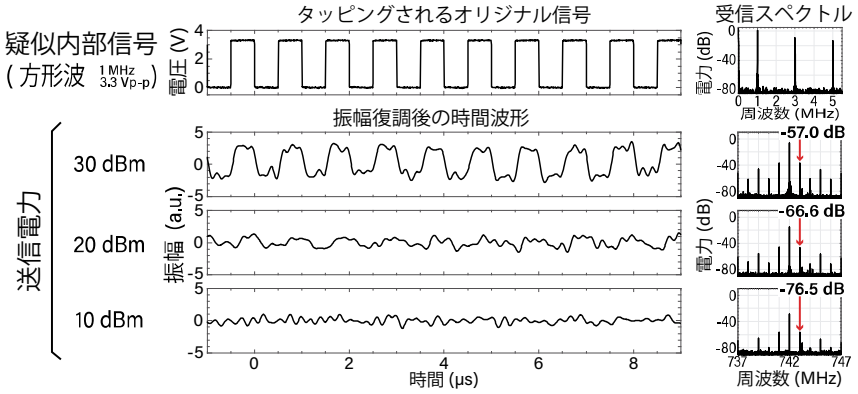

図 8　評価結果（オリジナル信号形状復元の忠実度評価および、情報を含むスペクトル強度による漏えい有無の評価）

上記評価結果から、AI/IoT 機器に実装されたハードウェアトロージャンは、照射信号強度に比例した強度の漏えい信号を発生させ、外部へ漏えいさせることが明らかとなった。この結果は、攻撃者が漏えい信号強度を任意に操作可能であることを示しており、従来の情報通信機器に関する電磁波を通じた情報漏えい問題である TEMPEST に比較し、より遠方から情報窃盗が可能になるだけで無く、攻撃者が攻撃対象機器に近接している場合は、攻撃を察知されない程度の微弱な電磁波照射で攻撃が可能であることが分かる。また、それと同時に攻撃タイミングも制御可能であることから、従来の TEMPEST と比較して脅威の度合いが高いことが示された。

3-2 回路改変を必要としない電磁波照射による情報漏えい現象の発見と原理解明

図 5 に示した FET から構成されるハードウェアトロージャン構造は、AI/IoT 機器に用いられるマイクロコントローラ（マイコン）内部に、マイコンの信号出力端子として存在する。この構造はマイコンの General-purpose input/output (GPIO) として、汎用マイコンの標準的機能として実装されており、2 章で

述べた IC 間通信の信号送信および受信にも用いられている。この GPIO はデータシート上では数十 MHz 程度の動作速度であると記載されているが、マイコンを構成する半導体プロセスの高速化などにより通常の Complementary metal–oxide–semiconductor（CMOS）構造であっても、GHz オーダの信号に対しての応答が可能な特性を示している。これはデータシートには記載されておらず、またマイコン設計者の意図した使用方法ではない。

本現象は、AI/IoT 機器からの電磁波照射による情報窃盗には回路改変が不要であることを示している。攻撃者は情報窃盗のターゲットである信号線に効率よく電磁波を注入可能な周波数を探すことで、遠方からその周波数を照射することで機器内部情報を取得可能となる。この周波数は、同じ設計の機器であれば配線の長さが同じであることから、機器を事前に入手可能であれば容易に事前調査可能である。また、多少周波数が異なったとしても、攻撃時に周波数をスキャンすることにより目的の信号を得ることが可能である。

本問題の検討を進めるため、図 9 に示す単純化モデルを用いて、実際に AI/IoT 機器で用いられているマイコンから電磁波照射による情報漏えい発生について評価を行った。単純化モデルの構造は、1 つのマイコンとそのGPIOに接続された配線からなるプリント配線基板とした。図10に本モデルからの漏えい信号を示す。

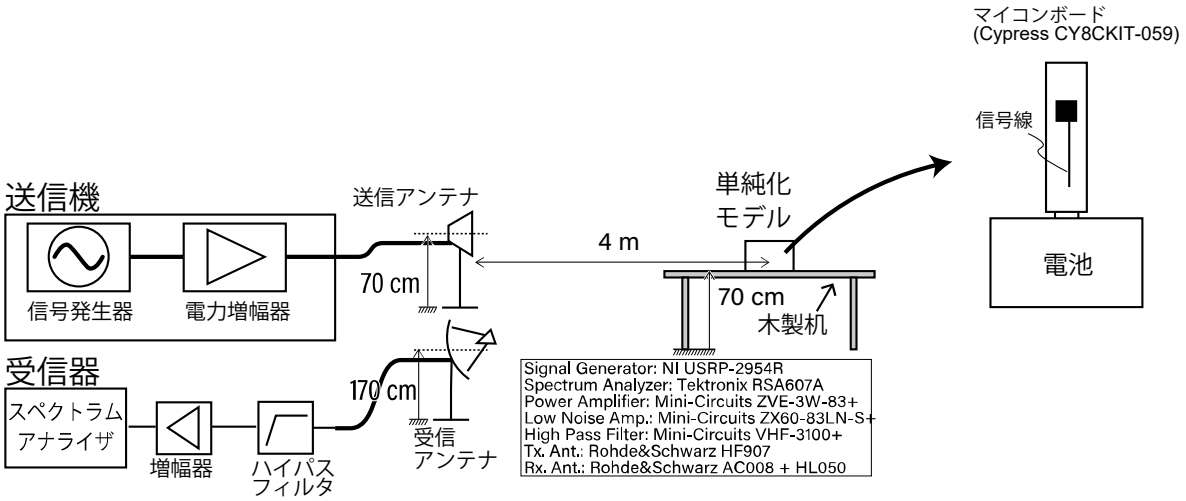

図 9　AI/IoT 機器の単純化モデルを用いた回路改変無しターゲットに対する情報漏えい評価システム

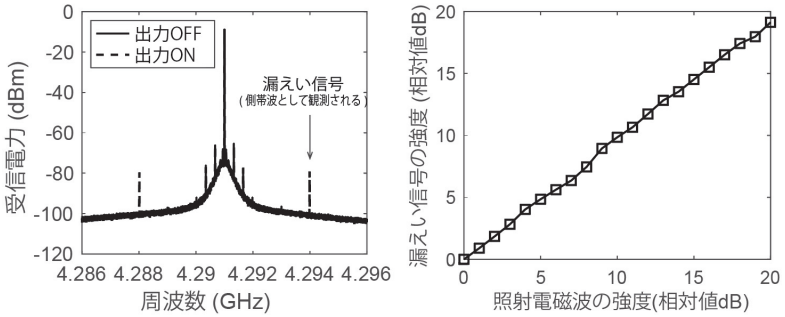

図 10　単純化モデルへの電磁波照射により観測された漏えい信号および照射強度に対する漏えい強度の変化

観測の結果、回路改変を有する攻撃と同様に照射電力に比例した漏えい信号が観測された。これは、IC が潜在的に有する脆弱性として考えられ、本実験で用いたマイコン以外の IC に関しても評価の実施が必要である。本現象については研究期間の後半に発見されたため、現象観測にとどまっている。継続課題では本現象の発生メカニズムを解明すると共に、対策手法を IC および IC 周辺回路の構造の両面で検討を進める予定である。

4 製造後の AI/IoT 機器への回路改変と電磁波攻撃の基礎的対策技術の開発

本セキュリティ問題に対する基礎的試験手法を開発することで対策技術につなげた。これまでの電磁波による情報漏えい試験方法は、旧来の TEMPEST を基本としており、環境電磁工学における不要電磁放射測定の延長上であった。そこで、本問題の特徴である電磁波照射時のみに生ずる現象を観測するため、電磁照射と電磁漏えいを同時に測定可能な測定系を提案した。本課題の継続課題では、本測定システムの検査高精度化を行うため、照射電磁波と漏えい電磁波の分離技術、試験対象物による製造ばらつきを考慮した統計的判断手法について検討を進める

さらに上記問題に共通する事項は、環境電磁工学における意図的電磁照射と不要電磁放射の問題および現象である。そこで、IEEE EMC Society の TC 5 High Power Electromagnetic において、共同研究者の林が Subcommittee として EM Leakage 問題の一つとして Low-power IEMI（低電力意図的電磁照射）問題を示し、それによる情報漏えいや意図的な情報操作などについての議論の場を構築した。

5 まとめ

本研究期間では AI/IoT 機器のハードウェアセキュリティの脆弱性として、IC 周辺回路の不正改変および電磁波照射時に生じる情報漏えいについて検討を進めた。その結果、攻撃に必要となる回路改変は、機器本体をアンテナとして用いることで、1 つの部品の追加のみで実施可能であることが明らかとなった。さらに同様の脆弱性は IC 内部に潜在的に存在していることを発見し、AI/IoT 機器に用いられるマイコンを用いた実験を通じて情報漏えいの発生を確認した。上記問題への対策および脆弱性の評価は既存の環境電磁工学分野での評価手法に存在しないため、IEEE TC 5 にて Low-power IEMI 問題として提案し、継続的に手法を検討する。

【参考文献】

[1] “Society 5.0「科学技術イノベーションが拓く新たな社会」説明資料,” 内閣府, 2018.

[2] Sharad Malik, “Detecting Hardware Trojans: A Tale of Two Techniques,” 2015 Formal Methods in Computer-Aided Design (FMCAD), 2015.

[3] “ソフトウェアの信頼性向上と安全な利用環境の構築に向けて,” 独立行政法人情報処理推進機構, 2013.

[4] Brian Sharkey, “TRUST in Integrated Circuits Program: Briefing to Industry,” DARPA Microsystems Technology Office (MTO), 2007

[5] Sally Adee, “The Hunt for the Kill Switch,” IEEE Spectrum May 2006.

[6] Introduction to Hardware Security and Trust, M. Tehranipoor and C. Wang, Eds., Springer, 2012.

[7] M. Tehranipoor, H. Salmani, and X. Zhang, Integrated circuit Authentication – Hardware Trojans and Counterfeit Detection, Springer, 2014.

[8] 永田 真, “IC チップの真正性の確保と対策-ハードウェアセキュリティの根源的課題に向き合う-,” IEICE Fundamentals Review, Vol.8, No.3, pp.172-182, 2015.

[9] “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies,” Bloomberg Businessweek, 2018.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の抑制に関する基礎検討	電子情報通信学会技術研究報告, Vol.119, No.2, HWS2019-6 , pp.31-35	2019 年 4 月
A Study on Feasibility of Electromag-	2019 Joint International Sym-	2019 年 6 月

netic Information Leakage Caused Forcibly by Low-Power IEMI	posium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo	
Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure	Conference on Cryptographic Hardware and Embedded Systems (CHES) 2019	投稿中