# 電子回路から守る情報セキュリティ――不正回路の挿入を未然に防ぐ技術開発

Securing Information from the Hardware Level: Developing Technology to Prevent Malicious Circuit Insertion


**衣川　昌宏**（Masahiro KINUGAWA, Ph. D.）

**福知山公立大学　情報学部　准教授　博士(工学)**

(Associate Professor, the University of Fukuchiyama, Faculty of Informatics)

IEEE　電子情報通信学会　日本災害情報学会

受賞：Richard B. Schulz Best Transactions on EMC Paper Award, IEEE (2024 年).　Richard B. Schulz Award for the Best EMC Transactions Paper - Honorable Mention, IEEE (2020 年).　イノベーション論文賞, 電子情報通信学会 暗号と情報セキュリティシンポジウム (2017 年).　研究奨励賞, 一般財団法人石田實記念財団 (2016 年)　他

著書：電磁的セキュリティと情報通信機器の信頼性確保 ハードウェアトロイによる情報漏えいの脅威, 月刊 EMC, 科学技術出版 (2021 年).　情報通信機器の入力デバイスからの電磁的情報漏えいの可能性について, 月刊 EMC, 科学技術出版 (2015 年)

研究専門分野：情報セキュリティ　環境電磁工学　電子工学　ハードウェアセキュリティ　電磁波セキュリティ　計測工学


## あらまし


情報通信機器の情報セキュリティは、アンチマルウェアソフトウェアやソフトウェアアップデートなど、主にソフトウェア面によって確保されてきた。一方で、機器を構成するハードウェアでは、ソフトウェアで処理されるデータやプログラム、機密情報などが電気信号としてやり取りされている。しかしながら、従来の電子回路には（特殊用途の機器を除き）情報の窃取や改ざん攻撃を検出する機能がほとんど実装されていなかった。その背景にはコストと検出感度の問題がある。

攻撃手法としては、情報通信機器の電子回路配線から直接信号を取得するもの、不正回路を挿入して間接的に信号を取得するもの、配線の近くに電界・磁界プローブを配置して近傍電磁界を観測するものなどが知られている。本研究では、これらの攻撃によって発生する電子回路周辺の電磁環境（電磁フィンガープリント）の変化を捉え、ハードウェアレベルから情報セキュリティを確保する手法を提案する。

情報通信機器は家電からパーソナルコンピュータに至るまで、現代の生活に広く浸透しており、多くの場合、機密情報を扱っている。本研究では、安価で高感度な電界センサであるマイクロコントローラの「静電容量式タッチセンシング機能」を応用し、電磁フィンガープリントを常時監視できる機構を開発した。その結果、信号の直接観測、不正回路の挿入、近傍電磁界プロービングなどの攻撃を、電磁フィンガープリントの変化として捉えられる可能性を示唆した。


## 1．研究背景と目的

スマートフォンやスマート家電、パーソナルコンピュータ、プリンタなど、さまざまな情報通信機器は現代社会・生活のインフラとして欠かせない存在である。そのインフラにおいて、情報セキュリティは極めて重要な要素となる。ソフトウェアに関してはアンチマルウェアソフトウェアなどによる対策が整備されており、安全性が一定程度保たれている。

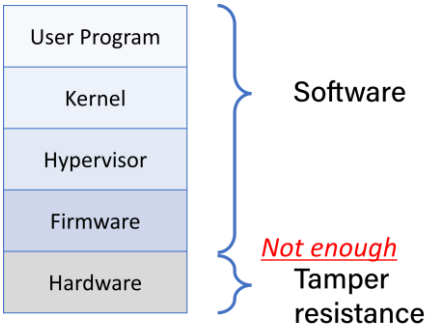


図 1 情報セキュリティの階層構造

しかし、機器で扱われる情報は電子回路によって実際に処理・伝達されており、機密情報が IC（集積回路）間を電気信号として行き来している限り、これを直接観察することで情報の窃取や改ざんが可能となる（図 1）。さらに、IC 内部に不正回路を仕込むことによって、特定の条件下で機器を異常動作させる事例も報告されている[1][2]。この不正回路は「ハードウェアトロージャン（Hardware Trojan, HT）」[3]と呼ばれ、IC の製造時に改変が行われるサプライチェーン上の問題として議論されている。

# 電子回路から守る情報セキュリティ――不正回路の挿入を未然に防ぐ技術開発

Securing Information from the Hardware Level: Developing Technology to Prevent Malicious Circuit Insertion

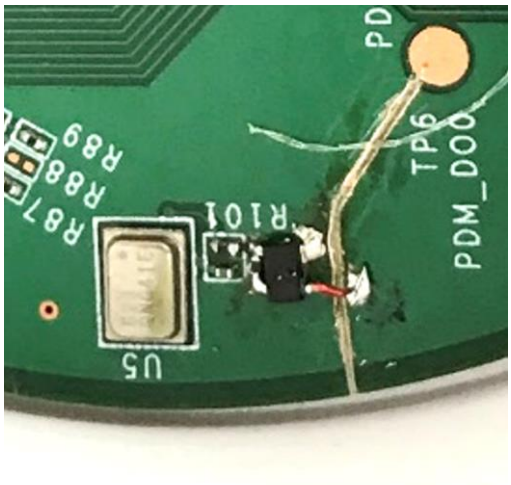


図 2　電子回路基板上に実装された
ハードウェアトロージャン

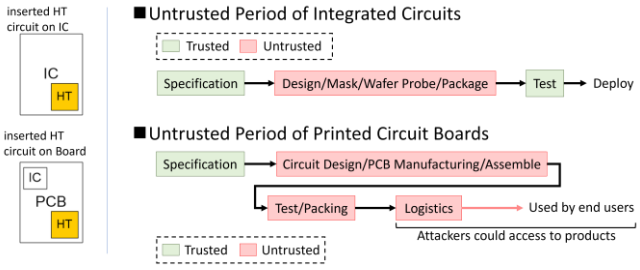


図 3　IC と電子回路基板へ不正回路が挿入
されるタイミング

同様の問題は IC が実装される電子回路基板にも存在しており[4](図 2)、不正回路の挿入が製造・流通・使用・廃棄までのライフサイクルにわたって起こりうることが報告されている(図 3)。特に電子回路基板は、機器の筐体を開封すれば後から回路改変が可能であるため、製造段階だけが危険なのではなく、ユーザが使用中から廃棄までリスクが継続する。

電子回路基板への不正回路挿入については報告こそある[4]が、その対策については十分に議論されていない。筆者らはこれまでに電子回路基板への不正回路挿入の実現性を検討し[5]、キーボードなどの低速信号からディスプレイの高速信号、暗号回路のサイドチャネル信号に至るまで、不正回路による機密情報の窃取が可能であることを示してきた。しかし、これを防御する具体的な方法は十分に確立されていない。

そこで、本研究では、製造から廃棄に至るまでのライフサイクルにおいて、電子回路基板への不正回路挿入を検出できる手法を開拓する。この手法によって、図 1 に示すハードウェア層からソフトウェア層まで一貫して情報セキュリティを確保することが可能となる。特に本研究では、コストを抑えながら高い検出感度を得るため、電子回路基板周辺の電磁環境（電磁フィンガープリント）の変化を活用する。こうして、攻撃時に生じる近傍電磁界の乱れをとらえ、不正回路の挿入を見逃さないようにすることが狙いである。

## 2．電磁フィンガープリント変動の監視手法

電子回路基板周辺の電磁フィンガープリントをリアルタイムに監視するためには、測定装置を機器の基板に組み込む必要がある。しかし、高性能の計測機器は大型かつ高価であるため、一般的な機器に実装することは困難である。

そこで本研究では、不正回路の挿入によって変化する「電界」に着目し、その変化を捉える手法を考案した。電界の変化は静電容量の変化としても捉えられるため、この値を観測できる静電容量センサを電子回路基板に実装する。さらに、既存の回路構成を大きく変えずに済むよう、あらゆる情報通信機器に搭載されているマイクロコントローラの静電容量タッチセンシング機能を流用する。

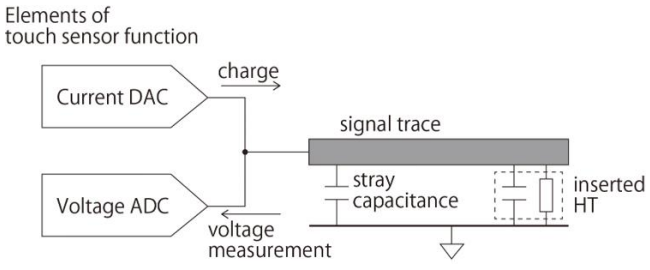


図 4　マイクロコントローラに内蔵された
タッチセンシング機能と電磁フィンガープリント計測への応用

マイクロコントローラとは、1 つの IC に CPU やメモリ、入出力ポート、シリアル通信回路などがまとま

った小型コンピュータである。近年のマイクロコントローラは、機構部品削減によるコストダウンを狙い、電気接点式スイッチの代替として静電容量式タッチセンシング機能を有している（図 4）。これは、定電流源で測定対象物を充電し、その電圧の変化を ADC（アナログ・ディジタルコンバータ）で測定する仕組みである。本研究では、この仕組みを「電磁フィンガープリント」の計測へ応用することで、既存設計への影響を最小限に抑えながら基板の監視を実現した。

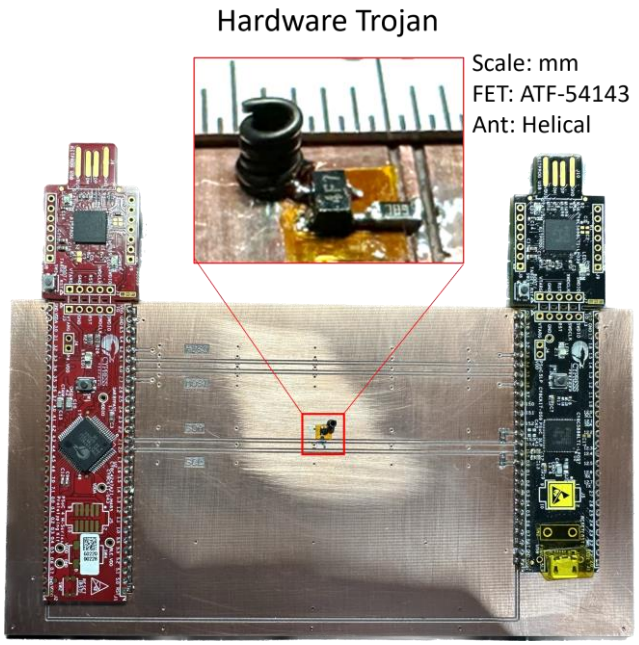


図 5　情報通信機器の電子回路基板を簡略化したモデル基板と実装された不正回路

評価実験では、情報通信機器の電子回路基板を簡略化したモデル基板（図 5）を作製し、Infineon Technologies 社の CY8C5888LTI-LP097 マイクロコントローラを用いた（図 6）。このマイクロコントローラは通常、機器各種の制御を行うために使用されるが、計測時のみ内部スイッチを介して配線へ接続するようにし（図 7）、通信信号が停止している短い期間に電磁フィンガープリントを測定する構成とした（図 8）。こうすることで、機器の通常機能を損なうことなく監視を実行できる。

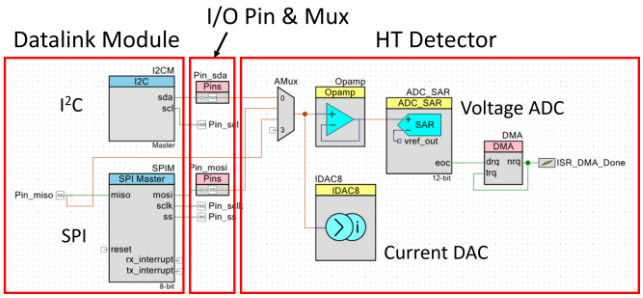


図 6　マイクロコントローラに実装した電磁フィンガープリント計測回路

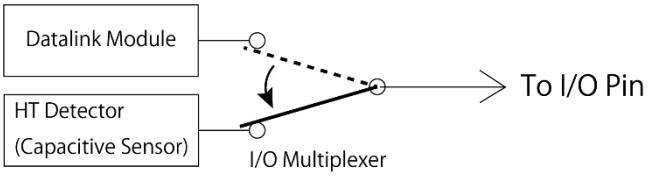


図 7　マイクロコントローラ内部のスイッチ切り替えによる通常動作と計測動作の多重化

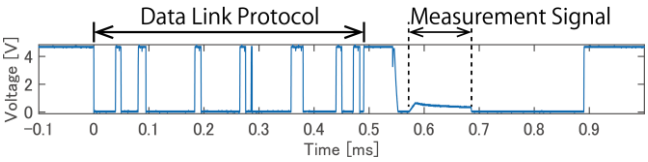


図 8　通信信号と電磁フィンガープリント計測信号の多重化

## 3．結果

図 5 のモデル基板上には、I²C 通信路を用いている。I²C は暗号回路やキーボードとのインタフェースにしばしば用いられ、機密性の高い情報を扱うことも多い。そこに不正回路（図 5）を挿入して機密情報の窃取を想定し、その際に配線周辺で生じる電界の乱れを捉えられるかを実験した。

図 9 および図 10 に示すように、静電容量計測時にはまず Charge Phase で配線を定電流で充電し、Measurement Phase で放電の仕方を観測する（図 11）。そして、Measurement Phase 中の電圧を積分した値を 1 万回取得してヒストグラム化した結果が図 12 で

ある。不正回路が挿入された場合、積分値が通常時とは異なる分布を示し、ヒストグラム上で新たなピーク（図 10 の「HT detected」部）が立つことから、攻撃を検出できることを確認した。

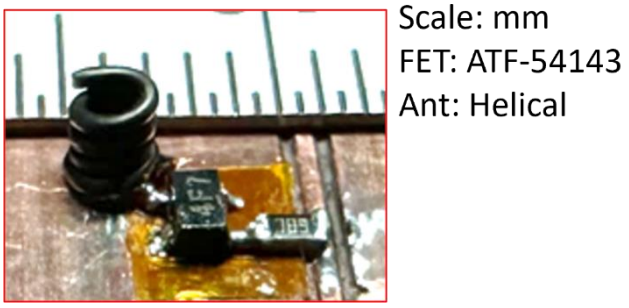


図 9　実験に用いた不正回路

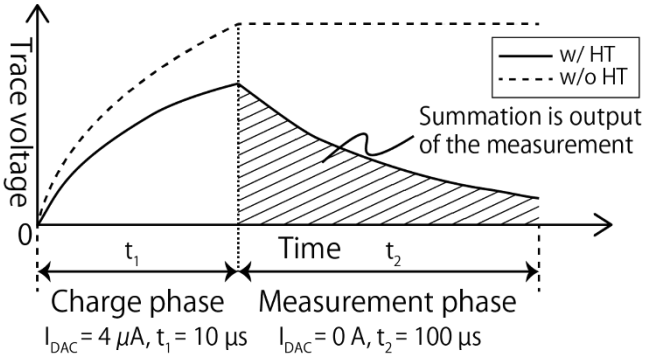


図 9 電磁フィンガープリント計測中の計測対象配線の電圧推移

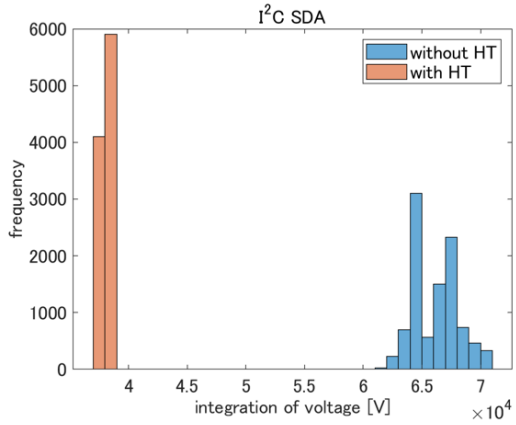


図 10　Measurement Phase での電圧を時間積分することによる電磁フィンガープリントの取得結果

本研究での評価では 0.1pF オーダの静電容量変化を捉えられるため、不正回路の挿入だけでなく、配線を直接プロービングして信号を盗み取るような攻撃についても高感度で対処できると考えられる。攻撃を検出した場合には機器をフェイルセーフモードへ移行し、機密情報を扱わない状態に切り替えることで情報窃取を防ぐことが可能である。また、不正回路が機器を誤動作させた場合には、機器をシャットダウンさせるなどの対策で被害を抑制できる。[6][7]

## 4．将来展望

本研究で提案した電磁フィンガープリントによる不正回路挿入の検出手法は、安価なマイクロコントローラのみで構成できるため、あらゆる情報通信機器に導入可能である。また、検出感度が高いため、小型化した不正回路でも見逃さずに検出できる。さらに、この手法を製造段階から導入し監視を行えば、機器のライフタイム全般にわたってハードウェアの安全性を担保できる。

ハードウェアセキュリティはシステム信頼性の根幹を支えるものである（図 1）。これが堅牢になれば、ソフトウェア面のセキュリティ対策と合わせて、より強固な情報通信機器のセキュリティを実現することが可能となる。真に安全な情報社会を実現するために、ハードウェアからのアプローチは今後さらに重要性を増すと考えられる。

## おわりに

本研究では、情報セキュリティの中核を担う電子回路に対して、不正改変攻撃（不正回路の挿入など）を検知するための新たな監視手法を提案した。この手法によって、不正回路による機密情報の窃取や機器の不正操作を困難にし、ハードウェアからソフトウェアまで一貫した情報セキュリティの確保が可能となる。さらに、特別な高価・大型の計測装置を必要とせず、既存のマイクロコントローラ機能を利用するだけで導入できる点も大きな特徴である。

また、製造段階から電磁フィンガープリントを常時監視し続けることで、サプライチェーンにおける不正改変も含め、機器のライフタイム全体にわたる真正性

の維持が可能となる。今後は、この技術をさらに発展させ、多様な機器や環境に適用できるハードウェアセキュリティ技術として成熟させていきたいと考えている。

**用語解説**

*1 **電磁フィンガープリント**
機器の周囲で観測される電界・磁界などの固有パターンのこと。配線や部品の配置が変わるとパターンがわずかに変化するため、不正改変の検出に利用できる。

*2 **マイクロコントローラ**
1 つの IC に CPU、メモリ、入出力ポートなどを集積した小型コンピュータのこと。家電など幅広い機器に搭載されており、本研究ではタッチセンシング機能を流用して電磁フィンガープリントを監視する。

*3 **静電容量**
どれだけ電気を蓄えられるかを示す指標のこと。配線や電子部品の配置など周辺環境が変わるとわずかに変化し、その変化を正確に計測することで不正改変を検出できる。

*4 **ハードウェアトロージャン（HT）**
IC や電子回路基板などに密かに組み込まれた不正回路のこと。特定条件で機器を誤動作させたり、機密情報を盗み出したりするため、深刻なセキュリティリスクとなる。

**参考文献**

[1] S. Adee, "The Hunt For The Kill Switch," in *IEEE Spectrum*, vol. 45, no. 5, pp. 34-39, May 2008.

[2] Mitra, Subhasish, H-S. Philip Wong, and Simon Wong. "Stopping hardware Trojans in their tracks." *IEEE Spectrum* 20 (2015): 2015.

[3] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," in IEEE Design & Test of Computers, vol. 27, no. 1, pp. 10-25, Jan.-Feb. 2010.

[4] Robertson, Jordan, and Michael Riley. "The big hack: How china used a tiny chip to infiltrate us companies." *Bloomberg Businessweek* 4.2018 (2018).

[5] Kinugawa, Masahiro, Daisuke Fujimoto, and Yuichi Hayashi "Electromagnetic information extortion from electronic devices using interceptor and its countermeasure," *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019), pp. 62-90, 2019.

[6] M. Kinugawa and Y. Hayashi, "Board-Level Hardware Trojan Detection Using on-Chip Touch Sensor," *2022 International Symposium on Electromagnetic Compatibility – EMC Europe*, Gothenburg, Sweden, 2022, pp. 168-171.

[7] M. Kinugawa and Y. Hayashi, "Detecting Hardware Trojans on Inter-IC Serial Data Links Through Capacitance Sensors," *2023 IEEE Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMC+SIPI)*, Grand Rapids, MI, USA, 2023, pp. 485-485.

**この研究は、令和２年度ＳＣＡＴ研究助成の対象として採用され、令和３～５年度に実施されたものです。**