修士論文

回路改変を行った機器に対する
電磁波を用いたデータ注入に関する研究

鍛治 秀伍

2019 年 3 月 15 日

奈良先端科学技術大学院大学
情報科学研究科

本論文は奈良先端科学技術大学院大学情報科学研究科に
修士（工学）授与の要件として提出した修士論文である。

鍛治 秀伍

審査委員：

林　　優一　教授　（主指導教員）
井上　美智子 教授　（副指導教員）
岡田　　実　教授　（副指導教員）
藤本　大介　助教　（副指導教員）

回路改変を行った機器に対する電磁波を用いたデータ注入に関する研究*

鍛治 秀伍

内容梗概

高出力電磁波を用いた意図的電磁妨害（IEMI: Intentional Electromagnetic Interference）は、従来研究において機器を破壊し、可用性を損なわせる脅威とみなされてきた。近年提案された、潜在的に電磁波耐性（イミュニティ）が低い機器に対する低出力電磁波を用いた IEMI は、機器の機密性・完全性を損なわせる脅威として議論が行われている。一方、機器設計時に高いイミュニティが備わっている機器も存在し、こうした機器は従来脅威の対象外であった。これに対し、本論文では、故意に機器のイミュニティを低下させる不正な回路改変と低出力電磁波を用いた IEMI の組み合わせによって機密性・完全性が損なわれる新たな脅威について検討し、従来まで低電力電磁波を用いた IEMI による脅威の対象外であった高いイミュニティを有する機器に対して、任意データを含んだ低出力電磁波を用いた IEMI を照射し、機器内部にデータが注入される攻撃の実現可能性を示す。また、このような脅威への対策技術として、電子部品を実装する際に生ずる機器周囲の電磁環境の変化に着目し、イミュニティを低下させる不正な回路改変を検出する手法について提案を行う。

キーワード

意図的電磁妨害，イミュニティ，ハードウェアトロイ，トロイ検出

*奈良先端科学技術大学院大学 情報科学研究科 修士論文, 2019 年 3 月 15 日.

Study on Data Injection Threats Using Electromagnetic Waves Against Electronic Devices with Circuit Modification*

Shugo Kaji

Abstract

Intentional electromagnetic interference (IEMI) with high-power electromagnetic (EM) waves has been characterized as a threat to destroy electronic devices and degrade the availability of devices in previous research. In recent years, IEMI with low-power EM waves against devices with low EM tolerance (immunity) has been reported and discussed as a threat against the confidentiality and integrity of devices. On the other hand, some devices have high-immunity at the design stage, and were not regarded as threat targets. By contrast, in this thesis, I considered a new threat against the confidentiality and integrity posed by a combination of malicious circuit modifications that intentionally weaken the immunity of the device and IEMI with low-power EM waves. Furthermore, I show the possibility of arbitrary data being injected into the high-immunity device which had been regarded as free from the threat of IEMI with low-power EM waves. As a countermeasure against such attack, I propose a method to detect malicious circuit modification that weakens device immunity, focusing on the change in the EM environment around the device when mounting electronic components.

Keywords:

Intentional electromagnetic interference, immunity, hardware Trojan, Trojan detection

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 15, 2019.

目次

図目次

第 1 章　緒論

1.1　研究背景

1.1.1　電磁波が電子機器におよぼす動作妨害

電磁環境両立性（EMC: Electromagnetic Compatibility）の分野では、電子機器の伝送信号や電源、自然界における落雷などに起因して生じる電磁波が、周辺の回路や集積回路（IC: Integrated Circuit）、電子機器などの動作を妨害する問題（EMI: Electromagnetic Interference）について検討されてきた [1]。そのため、EMC の分野では、電子機器の動作に起因して放射する電磁波（エミッション）の抑制と、機器外部から侵入する電磁波による故障・誤動作を引き起こさない電磁妨害耐性（イミュニティ）の向上が課題となっている。このような問題に対して、国際電気標準会議（IEC: International Electrotechnical Commission）や国際電気通信連合（ITU-T: International Telecommunication Union Telecommunication Standardization Sector）では、EMI 対策手段の標準化が推進され、工業製品や市販製品に対してエミッションの抑制やイミュニティの許容値の規格が定められている [2]。

前述した EMI に関する問題は、電子機器のエミッションや自然界の電磁波に起因する非意図的に発生した電磁波による電子機器の動作妨害である。一方、意図的に発生させた電磁波によって電子機器の故障や動作妨害が引き起こされる問題（IEMI: Intentional Electromagnetic Interference）がある [3][4]。

IEMI は、主に電子機器が有するイミュニティをはるかに上回る高電力電磁波（HPEM: High Power Electromagnetic [5][6]）を用いて、電子機器内部のイミュニティが低い IC や電子部品を破壊し、電子機器を破壊・無効化することで可用性を損なわせる脅威として捉えられている（図 1.1）。こうした問題に対して IEC や ITU-T では、「放射 HPEM 環境」を「ピーク電界強度が 100 V/m 以上」とし、「伝導 HPEM 環境」を「電圧レベルが 1 kV を超えるケーブルや電線に結合または注入される大電力電磁電流および電圧」と定義し、IEMI の一般化と対策技術の規格策定が進められている [7][8]。そのほかにも、EMC の分野では「意図的な妨害波の伝搬過程の解明」や「意図的な電磁妨害によってシステムが受ける影響の解析」、

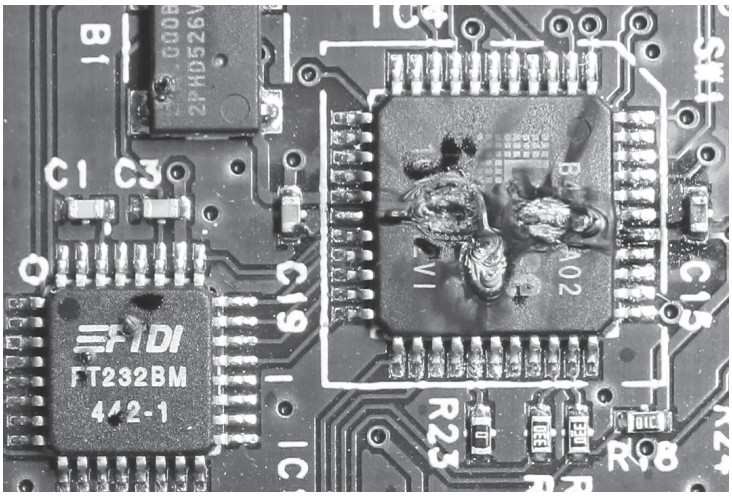


図 1.1　HPEM によって破壊された機器内部の IC

「意図的な電磁妨害からのシステムや通信の保護」についても検討が進められている [9][10]。

従来まで、IEMI に用いる HPEM の生成や放射には、巨大で高価な機材と専門的な知識が必要とされていた。しかし、近年の電子機器の製造技術の発達により信号発生器や信号増幅器の小型化・低価格化が進むと共に、非専門家であっても手軽に利用できるソフトウェア無線送受信機（SDR: Software Defined Radio）が普及したことで、IEMI の敷居が下がり、より身近で現実的な脅威として捉えられるようになった。

1.1.2　情報セキュリティ分野における低電力電磁波を用いた IEMI の検討

前節で述べたように、EMC の分野において IEMI は、HPEM を用いて電子機器の IC や電子部品を破壊し、可用性を損なわせる脅威として捉えられている。一方、近年の情報セキュリティの分野では、電子機器の IC や電子部品の破壊を伴わない低電力電磁波の利用によって電子機器の処理や信号に誤りや誤動作を引き起こし、機密性や完全性を損なわせる攻撃が報告されている。しかし、本攻撃の実現可能性や対策手法に関する検討は未だ十分ではない。

本論文では、機器の破壊を伴う 100 V/m 以上の電界強度を用いた IEMI を High-power IEMI とし、機器の破壊を伴わない数十 V/m 程度の電界強度を用いた IEMI を Low-power IEMI と分類した上で、電子機器の処理や信号に誤りや誤動作を引き起す可能性がある Low-power IEMI を用いた攻撃について論ずる。

電子機器はアナログセンサや IC などの測定・演算結果を信頼して動作しているため、Low-power IEMI を用いた攻撃によって発生した誤りや誤動作が連鎖的に上位レイヤのシステムに伝搬し、情報機器の動作に悪影響を与える [11]。すでに、Low-power IEMI を用いた攻撃として、暗号デバイスの電源線に対して電磁波を印加することで処理の一部に誤りを引き起こし、機器が保持する機密情報を解析する攻撃（フォルト注入攻撃）[12] や、マイクやスマートフォンに対して変調した電磁波を照射することで電子機器内部の信号に誤りや誤動作を引き起こし、本来は発行されていないデータやコマンドを注入する攻撃（データ注入攻撃）[11][13] が報告されている。

これらの Low-power IEMI を用いた攻撃は、全ての電子機器に対して誤りや誤作動を引き起すことができるわけではなく、攻撃で用いる電磁波に対するイミュニティが低い電子機器に限られている。電子機器が有するイミュニティは、電子機器の回路構造や筐体・接続線路のシールディング状態、電子機器が設置された場所、その周辺電磁環境、電子機器が曝される電磁波など、様々な物理的な条件によって決定される。そのため、これまでに報告された Low-power IEMI を用いた攻撃は、攻撃対象機器への電磁波の伝達効率やその周辺環境などを調査した上で、攻撃のタイミングや照射する電磁波の周波数など、機器のイミュニティが低い状態となる全ての物理的な条件を満たすことによって攻撃を成立させていた。

このような Low-power IEMI を用いた攻撃手法に対して、攻撃対象機器のイミュニティが低い状態となる物理的な条件を満たす必要がない攻撃手段が 2 種類考えられる。

手法 1: 攻撃対象機器のイミュニティを上回る電界強度の電磁波を用いる方法

電子機器のイミュニティ試験の 1 つである放射イミュニティ試験では、「80 MHz - 1000 MHz において 80 %の AM 変調を 3 V/m（住宅用・商業用）または 10 V/m（産業機器）の電界で照射した際に、電子機器製品の性能劣化

が生じず適切に動作するか*」と定義されている [1][2]。そのため、これらで定義されている電界強度以上の電磁波を用いることで電子機器の内部に電磁波を伝搬できる可能性がある。

手法 2: 攻撃対象機器に改変を加え、イミュニティを局所的に低下させる方法

攻撃対象機器や対象機器に接続された周辺機器・ケーブルの一部を改変し、それらを表す等価回路網を変化させることにより特定周波数に対するイミュニティを低下させ、当該周波数の電磁波を用いることで電子機器の内部に電磁波を伝搬できる可能性がある。

手法 1 は手法 2 と異なり、攻撃対象機器への侵襲が不要であり攻撃の実施が容易であるため、より現実的な攻撃手法であると考えられる。しかし、電子機器内部に実装された IC や電子部品にはイミュニティの高低差が存在し、印加された電磁波に対してイミュニティが低い IC や電子部品に破壊や故障が生じる可能性がある。そのため、Low-power IEMI を用いて電子機器内部の処理や信号に誤りや誤動作を引き起こすことを目的とした攻撃には不向きであるといえる。

一方、手法 2 は攻撃対象機器への侵襲を必要とするが、機器やその周辺機器などに対して改変を行うことで対象機器の等価回路網を変化させ、局所的に特定周波数の電磁波が伝搬しやすい（イミュニティが低下した）部位を作成することができれば、対象機器内部の IC や電子部品に破壊や故障を発生させることなく誤りや誤作動を引き起こす可能性がある。このような誤りや誤動作が交通網や電力網、通信網を担う機器やその周辺機器に生じた場合、わずかな誤りが重大な事故を招く恐れがある。

1.1.3 電子機器に対する改変の既存研究と本論文における不正な回路改変の定義

電子機器に対する改変の代表的な例として、IC 内部に実装されたハードウェアトロイ（HT: Hardware Trojan [14][15]）が挙げられる。HT は、本来の IC の設計には存在しなかった論理や回路を追加し、設計者が意図しない動作や機能を付加す

*適切に動作とは、評価対象機器の試験中と試験後に、設計者が意図したとおりに動作を継続し、性能の劣化や機能の低下が生じないことを指す。

る脅威である。主な機能として、情報の漏えい、機能の改変、機能の低下（信頼性の低下やサービス妨害を含む）の 3 つが存在する [16][17][18]。このような HT は、IC の製造過程に悪意のあるサードパーティの半導体製造企業が介入していることが主な原因とされ、製造過程で実装される可能性が示唆されている [19]。しかし、IC の製造過程において HT を実装するには、高いコストと高い技術が求められるため組織や国家レベルの介入が必要であると考えられる。

一方、一般的な電子機器の製造には、サードパーティ製のプリント基板や周辺機器、通信線路などが利用されることが多く、これらに対しても同様に HT が実装される可能性がある。近年では、IC 外部の周辺機器や周辺回路に実装可能な HT [20][21][22] が報告されていると共に、米国報道機関 Bloomberg では、企業に納入されたサーバのプリント基板上に本来の設計では存在しない電子部品が実装されていた可能性を報告している [23]。このような IC 外部に実装可能な HT は、プリント基板に対する表面実装もしくは、周辺回路網への電子部品の追加実装によって実現できる。そのため、必ずしも電子機器が製造されるタイミングでの HT の実装が求められるわけではなく、機器の運搬過程や販売過程、運用過程などのわずかな時間で実装される可能性があるため、組織・国家レベルの介入がなくとも、電子回路の知識を持った技術者であれば IC 外部への HT の実装が可能である。本論文では、IC 外部の HT だけでなく、電子機器や周辺回路網に対する電子部品の追加実装など、機器の等価回路網を変化させる改変を総じて「不正な回路改変」と定義して論ずる。

1.2 研究目的

これまで電子機器の可用性を損なわせる脅威とされてきた High-power IEMI を用いた攻撃に対して、近年ではフォルト注入攻撃やデータ注入攻撃などの機密性や完全性を損なわせる Low-power IEMI を用いた攻撃の脅威が報告されている。このような Low-power IEMI を用いた攻撃は、電子機器が有するイミュニティに依存しており、イミュニティを低下させる物理的な条件を全て満たした場合に成立するとされていたが、これらの物理的な条件を満たす必要がない攻撃の可能性が存在する。

そこで、本論文では、機器の機密性と完全性を損なわせる新たな脅威として、不正な回路改変を行った機器に対して任意のデータを注入する Low-power IEMI を用いた攻撃が実現可能であることを示すと共に、不正な回路改変への対策技術の提案を目的とする。

これまでの Low-power IEMI を用いた攻撃では、潜在的にイミュニティが低い機器を対象としており、対象機器への電磁波の伝搬効率や機器周辺の環境などを事前に調査し、伝搬効率の良い電磁波の周波数を選択することで攻撃を成立させていた。しかし、電子機器のイミュニティを意図的に低下させることが可能となれば、これまで攻撃の対象外と見なされていた機器に対しても脅威が拡大する可能性がある。

本論文では、不正な回路改変による電子機器のイミュニティ低下の実現と、Low-power IEMI を用いた機密性・完全性を損なわせる脅威の対象拡大の可能性を示すために、攻撃に用いる電磁波に対してイミュニティが高い電子機器を攻撃の対象として使用する。そして、不正な回路改変を行うことでイミュニティが低下した電子機器に対して、Low-power IEMI を用いた攻撃の一種であるデータ注入攻撃によって任意のデータが注入される攻撃の実現可能性を示す。また、このような攻撃への対策技術として、不正な回路改変の実装を検出する手法についての基礎的な検討を行う。

1.3 本論文の構成

本論文の構成は以下の通りである。

2 章では、電子機器に対する不正な回路改変手法を示し、局所的なイミュニティ低下の発生メカニズムと Low-power IEMI を用いたデータ注入攻撃の実現方法を論ずる。そして、電子機器に対して不正な回路改変が実装されるタイミングや方法、本攻撃の成立条件について示し、電子機器への不正な回路改変を用いたデータ注入攻撃が実現する可能性について論ずる。

3 章では、2 章で説明した不正な回路改変を用いた電子機器のイミュニティの低下と、Low-power IEMI を用いたデータ注入攻撃の実現可能性について検証する実験を行う。実験では、電子機器のイミュニティの低下と任意のデータの注入が実現可能であることを示し、不正な回路改変の実装を検出する手法を示す。

4 章では、本論文の結論を述べる。

第 2 章　不正な回路改変によるイミュニティ低下と Low-power IEMI を用いたデータ注入手法

本章では、電子機器に対する不正な回路改変手法を示し、局所的なイミュニティ低下の発生メカニズムと Low-power IEMI を用いたデータ注入攻撃の実現方法について論ずる。

最初に、不正な回路改変を用いた電子機器のイミュニティを意図的に低下させる方法について論ずる。続いて、イミュニティが低下した電子機器に対する Low-power IEMI を用いた任意データの注入方法について論ずる。そして、最後に、電子機器に対して不正な回路改変を実装するタイミングとその方法、本章で示した攻撃が成立する条件について論ずる。

2.1　不正な回路改変を用いたイミュニティの低下手法

電子機器に対する Low-power IEMI を用いた攻撃の成立には、照射・印加した電磁波に対してイミュニティが低い部分から機器内部に電磁波を伝搬させる必要がある。しかし、前章で述べたように、電子機器のイミュニティは回路構造や筐体の状態、周辺の電磁環境など様々な物理的な条件によって変化するため、攻撃者が事前に伝搬効率のよい電磁波の周波数を知ることは困難である。よって、攻撃者が Low-power IEMI を用いた攻撃をより容易に成立させる方法として、電子機器のイミュニティを決定する物理的な条件に依存しない状態を作り出すことが考えられる。

物理的な条件に依存しない状態は、攻撃に用いる電磁波に対してイミュニティが低下した部位、すなわち、電磁波を効率良く受信し電子機器内部に伝搬させる部位を作り出すことで実現可能である。このような部位を作り出す方法として、当該周波数の電磁波を受信するアンテナ構造を電子機器上に作成する方法が以下の 2 つ考えられる。

方法 1: 導線等で作成したアンテナを電子機器に実装する方法

攻撃者が事前に導線や金属体などの導体を用いてアンテナを作成し、電子機器上のイミュニティを低下させたい部位に対して実装する。

方法 2: 電子機器の一部を利用し、アンテナ構造を作成する方法

電子機器内部の機密情報を含む電気信号がプリント基板の配線パターンや接続線路から放射する電磁波を介して漏えいすることが報告されている [24][25]。電磁波の相反定理より、このような部位は電磁波の伝搬効率を高めると考えられるため、攻撃者が事前にアンテナを作成するのではなく、プリント基板上の配線パターンや接続線路などを用い、特定周波数で効率良く受信する長さに切断または分離し、アンテナ構造を作成する。

方法 2 は方法 1 に比べ、実装が困難であると考えられるが、元より電子機器に利用されていた導体をアンテナとして動作させるため、電子機器に対する不正な回路改変を利用者に察知されにくくなるため、攻撃者がこの方法を選択する可能性が高い。そのため、本論文では方法 2 に着目し、電子機器の一部を利用したアンテナ構造の作成によって局所的なイミュニティの低下が実現する可能性について論ずる。

一般的な電子機器のプリント基板は筐体で覆うことで物理的な接触・接近から保護されており、攻撃者が直接電子機器内部のプリント基板に改変を行うことは難しい。しかし、電子機器間の通信線路や商用電源に接続された電源線路などの接続線路は筐体外部に接続されているため、筐体の開封を伴うプリント基板への改変に比べて容易に改変を行うことが可能であると考えられる。そこで本論文では、一般的な電子機器の接続線路に EMI、IEMI 対策として実装されている金属箔や金属メッシュなどのシールド導体に着目し、この金属導体に改変を行うことで作成されたアンテナ構造を用いて局所的なイミュニティ低下を実現する。

電子機器の接続線路を覆うシールド導体に対する、不正な回路改変を用いたアンテナ構造の作成方法は 3 つ存在し、1 つ目は、シールド導体を切断する方法、2 つ目は、フェライトコア（FC: Ferrite Core）をケーブルの上から装着する方法、3 つ目は、シールド導体にフェライトビーズ（FB: Ferrite Bead）を実装する方法がある。1 つ目のシールド導体の分断は、機器本来の動作を妨害する可能性があり、本攻撃の目的にそぐわないため本論文では扱わない。2 つ目、3 つ目の方法は、FC や FB を装着・実装した部分でシールド導体を高周波的に分離することに相当し、こ

れらの装着・実装によって電子機器本来の動作を妨害することはない。そのため、電子機器の接続線路上の 2 箇所に装着・実装された FC または FB 間のシールド導体は、電子機器やその他の機器から高周波的に分離された長さ L の金属導体となり、長さ L の金属導体と電気的に共振する周波数の電磁波を受信するアンテナとして動作させることができる。よって、このような不正な回路改変により高周波的に電子機器から分離された金属導体は、特定周波数の電磁波を効率良く受信する部位となり、イミュニティを決定する物理的な条件に依存しない、局所的にイミュニティが低下した状態を作り出すことが可能となる。

2.2 Low-power IEMI を用いた任意データの注入手法

電子機器に対する Low-power IEMI を用いた任意データの注入を実現させるためには、機器の外部で生成された電磁波を内部まで伝搬させ、機器本来の処理や信号を模倣する必要がある。しかし、電子機器の内部信号は事前に決められた周期や形式によって伝送されており、機器外部で生成された電磁波を任意のデータとして機器に処理させることは困難である。そのため、機器外部で生成した電磁波を任意のデータとして機器に処理させるためには、機器内部の IC が正規の信号として処理することが可能な周期や形式を保ちながら、時間的に変化する電気信号の生成が必要である。このような電気信号を生成する具体的な方法として、電子機器の接続線路上のシールド導体に構成されたアンテナにより局所的にイミュニティが低下した部位に対して IC 外部の HT を実装する。

IC 外部の HT を用いて電子機器内部を伝搬する正規の信号を模倣し、攻撃者が意図した任意のデータを IC に処理させるためには、IC 外部の HT を駆動するための電力の供給と任意のデータを表す電気信号の生成が必要である。そこで、前節で作成したシールド導体上のアンテナと電気的に共振する周波数の電磁波をキャリアとして用い、攻撃対象機器に注入する電気信号を振幅変調した電磁波（振幅変調波）を生成し、機器外部から攻撃対象機器に対して照射する。そのため、攻撃対象機器に実装された IC 外部の HT は、以下の 2 つの機能を持つことが求められる。

機能 1: シールド導体上のアンテナが受信した振幅変調波を復調する機能

シールド導体上に構成されたアンテナから伝搬した振幅変調波を整流し、IC 外部の HT を駆動するための直流成分と攻撃対象機器の IC に処理させる信号を表す交流成分を得る。

機能 2: 復調信号に応じて、対象機器の IC が処理可能な電気信号を生成する機能

機能 1 で得られた交流成分に従って、攻撃対象機器の IC が処理可能な電気信号を生成する。攻撃対象機器の IC によって、必要とされる信号の形式（アナログ信号もしくはデジタル信号など）が異なるため、対象機器の仕様に応じて HT を設計する必要がある。

以上の機能を持つ IC 外部の HT をシールド導体上に構成されたアンテナに接続し、攻撃対象機器に注入する信号の振幅変調波を照射することで Low-power IEMI を用いた任意データの注入が可能となる。

攻撃対象機器への不正な回路改変とデータ注入の攻撃イメージを図 2.1 に示す。

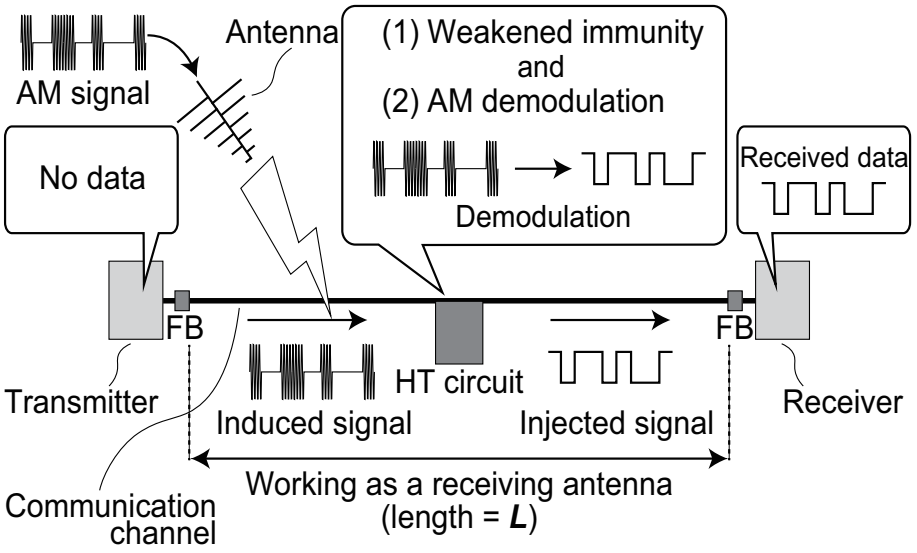


図 2.1　攻撃対象機器の接続線路に対する不正な回路改変とデータ注入のイメージ

2.3 電子機器に対する不正な回路改変を用いたデータ注入攻撃の方法

本節では、本論文で提案した不正な回路改変を用いたデータ注入攻撃が成立する方法として、電子機器に対する不正な回路改変の実施方法と、Low-power IEMI を用いたデータ注入攻撃の成立条件について論ずる。

2.3.1 提案した不正な回路改変が行われるタイミングとその方法

(1) 電子機器に対して不正な回路改変が行われるタイミング

本章で提案した不正な回路改変は、既存の電子機器に対しても実装が可能なため、電子機器の製造過程だけでなく運搬過程や販売過程、運用過程などのタイミングで不正な回路改変が行われる可能性がある。そのため、必ずしも電子機器の製造企業への介入が求められるわけではなく、これまでの IC 内部の HT の実装に比べて攻撃コストは低い。また、不正な回路改変が可能な期間に着目すると、数日から数ヶ月間の電子機器の製造過程だけでなく、電子機器が製造企業から出荷されてから製品寿命を迎えるまでの数年から数十年間の長期にわたって不正な回路改変が行われる可能性がある。

(2) 攻撃者が製造後の電子機器に対して不正な回路改変を行う方法

攻撃対象機器への不正な回路改変を行うには、一定時間の接触・接近が必要であるが、インフラシステムやサーバ、それらの制御装置などの重要な電子機器は、一般的に扉や壁によって設置場所への物理的なアクセスが制限されている。しかし、これらの電子機器であっても機器の納入やリプレース、メンテナンスなど、攻撃者が接触・接近する機会が存在するため、不正な回路改変を行うことが可能である。また、電子機器の接続線路のような置換可能な対象であれば、あらかじめ不正な回路改変を行った接続線路を用意しておき、対象機器に接触・接近したタイミングですり替えることで、より短い時間で不正な回路改変を行うことが可能である。

2.3.2 Low-power IEMI を用いたデータ注入攻撃が成立する条件

本論文で提案した攻撃が成立する条件として、以下の 3 つが存在する。

条件 1: 電子機器に対する不正な回路改変を行うタイミングが存在する
条件 2: 不正な回路改変を行う部位に伝搬する信号の周期や形式（プロトコル等）が調査・取得可能である
条件 3: データ注入攻撃で用いる Low-power IEMI が攻撃対象機器に到達可能である

前節までに述べたように本攻撃が成立するためには、Low-power IEMI に対する攻撃対象機器のイミュニティを低下させ、機器内部の IC が正規の信号として認識する電気信号の注入を行う必要がある。そのため、本攻撃の成立条件として、電子機器への不正な回路改変を行うタイミングと、IC 外部の HT が生成しなければならない電気信号の仕様や条件の把握が必要である。また、本論文で提案する IC 外部の HT は、シールド導体上に作成したアンテナと電気的に共振する周波数で変調した振幅変調波がトリガとなって動作するため、攻撃者が照射した振幅変調波が攻撃対象機器に到達することが必須条件である。よって、シールディングされた場所や建物の内部に攻撃対象機器が設置されている場合は、本論文で提案する不正な回路改変を伴う Low-power IEMI を用いたデータ注入攻撃は成立しない。

2.4 まとめ

本章では、電子機器に対する不正な回路改変によってイミュニティを局所的に低下させる方法と Low-power IEMI を用いて任意のデータを機器内部に注入する方法について論じた。そして、本攻撃が実現する攻撃方法として、電子機器に対して不正な回路改変が行われるタイミングと機器に対する不正な回路改変の方法、Low-power IEMI を用いた本攻撃の成立条件について検討した。

第 3 章　不正な回路改変を用いたデータ注入攻撃の実証

本章では、2 章で論じた電子機器に対する不正な回路改変による局所的なイミュニティの低下と Low-power IEMI を用いた任意データの注入の実現可能性について示す。

最初に、本論文で提案する不正な回路改変によって局所的にイミュニティを低下させ、任意データを注入する攻撃対象機器の仕様とその構成について論ずる。続いて、攻撃対象機器に実装した不正な回路改変の構成と対象機器への実装方法について論ずる。そして、不正な回路改変による局所的なイミュニティの低下と Low-power IEMI を用いた攻撃によって任意データの注入が可能であることを実証実験によって示す。最後に、本論文で提案した不正な回路改変の実装を検出する方法に関する基礎的な検討を行う。

3.1　本攻撃の攻撃対象となる電子機器とその仕様

本実験では、情報処理機能を有する機器や設備でローエンドモデルからハイエンドモデルまで幅広く利用されている UART（Universal Asynchronous Receiver Transmitter）通信を攻撃対象として用いる。UART は調歩同期式シリアル通信であり、電子機器間の通信線路上でボーレートに従い、ビット単位でデータを逐次的に伝送する通信方式である。UART では、ボーレートはビットレート（bps）と等価であるが、ビット同期に必要なクロック等のタイミング情報は通信線路上には独立した信号として存在しない。そのため、ビット同期は、受信時の通信信号からビットの開始・終了タイミングの抽出によって行い、それによりビットをデコードしている。また、UART は非同期式通信であり、データの開始・終了を受信端に通知する必要があるため、データの先頭にスタートビット、末尾にストップビットを付加しデータの開始・終了を識別している。すなわち、UART に対するデータ注入攻撃は、ビット同期およびデータの開始・終了タイミングの同期が不要であるため、任意のタイミングで開始可能である。

本実験における UART のデータ伝送パラメタは、データ単位は 8 bit、スタートビットおよびストップビットは 1 bit、ボーレートは 9.6 kbps とした。また、通信

線路上のビットと電圧値の対応は正論理とし、1 を 5 V、0 を 0 V、無通信時は常時 1 として 5 V とした。図 3.1 に本パラメタの UART で文字列“ABC”が伝送される際の電気信号の変化の概念図、表 3.1 に攻撃対象となる UART モジュールおよび通信パラメタを示す。また、実験環境を一般化および簡略化するため、2 台の UART のそれぞれを送信専用機と受信専用機として利用し、1 m の 2 芯シールドケーブルを用いてデータと GND を UART モジュール間で共有した。UART モジュールは Cypress 社の CY7C65211-24LTXI USB Serial Bridge を利用した。

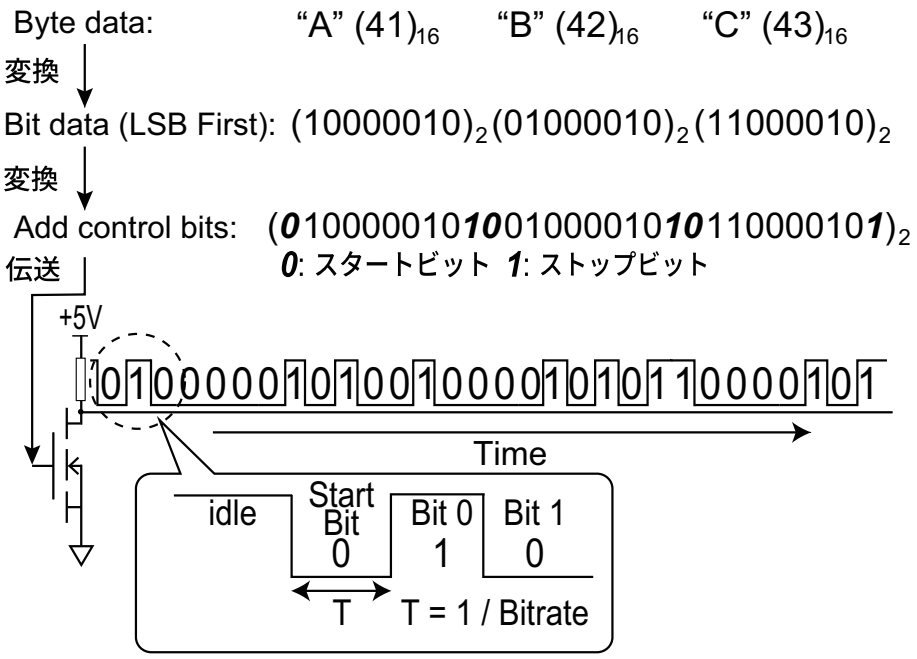


図 3.1　UART で文字列"ABC"が伝送された場合の電圧変動の概念図

表 3.1　攻撃対象となる UART モジュールのパラメタ

UART 通信モジュールと通信線路	
送受信用 IC	Cypress CY7C65211-24LTXI
信号電圧	5 V CMOS レベル
通信線路	2 芯シールドケーブル
通信線路長	1 m
UART の通信パラメタ	
論理	正論理
無通信時	論理 1（5 V）
ボーレート	9.6 kbps
スタートビット	1 bit
ストップビット	1 bit
パリティビット	なし

3.2　不正な回路改変に用いる回路とその実装

本実験では攻撃対象機器に対して、局所的なイミュニティの低下と、攻撃対象機器内部に伝搬した電磁波から IC が正規の信号として処理可能な時間的に変動する電気信号を生成する不正な回路改変を行う。

攻撃対象機器の局所的なイミュニティの低下は、対象機器内部への電磁波の伝搬効率を高めることで実現が可能である。そのため、本実験では、UART モジュール間の通信線路上のシールド導体を高周波的に機器から分離し、特定周波数の電磁波と電気的に共振することで効率良く電磁波を受信するアンテナ構造とした。通信線路上のシールド導体を高周波的に分離する方法として、FC を通信線路に装着する方法があるが、通信線路の見た目を変化させてしまい回路改変を行ったことが利用者に察知される可能性があるため、UART モジュール間の通信線路上のシールド導体を一度切断し FB [†]を用いて再接続することで、高周波的に分離されたシールド

[†]フェライトビーズには、ビーズ状のものとチップ状のものが存在するが、本論文では、主に表面実装に用いられるチップ状のフェライトビーズを用いる。

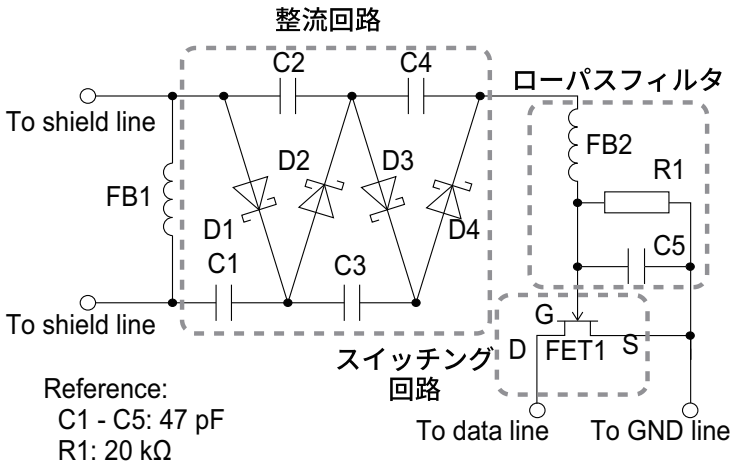
導体を作り出しアンテナ構造として用いる方法を採用した。このような方法であれば、FB の実装後に通信線路の被膜で再度覆うことで、通信線路の見た目の変化を抑え、利用者に不正な回路改変を察知されにくくすることが可能である。

本実験では、シールド導体から作り出したアンテナが攻撃時に照射する電磁波の約 3/2 波長で電気的に共振するように FB を実装しているが、FB の実装位置を調整することによって異なる周波数の電磁波の伝搬効率を高めることも可能である。そのため、電磁波を照射する機器に発振周波数の制限がある場合や通信線路の長さによって FB の実装位置を変更することで、異なる周波数や通信線路長にも本攻撃の適用が可能であるまた、FB のモデルを選択する場合は、シールド導体のインピーダンスに比べ、照射する電磁波の周波数付近で十分大きなインピーダンス値が得られるモデルを選択する必要がある。

続いて、対象機器内部に伝搬した振幅変調波から、IC が正規の信号として処理可能な時間的に変動する電気信号を生成する IC 外部の HT の回路構造について説明する。本論文で用いた IC 外部の HT は、整流回路とローパスフィルタ、スイッチング回路の 3 つのコンポーネントによって構成され、FB の実装によって通信線路上に作り出されたアンテナ構造を入力とし、スイッチング回路の出力が通信線路のデータ線と GND 線に接続されるように実装した（図 3.2, 3.3)。整流回路は、受信アンテナとなる高周波的に攻撃対象機器から分離されたシールド導体に接続され、伝搬した振幅変調波を包絡線検波する機能と、低出力の振幅変調波の照射で IC 外部の HT を駆動させるための昇圧の機能を持つように設計した。ローパスフィルタは、機器本来の通信信号に起因する信号によって IC 外部の HT が誤動作することを防いでいる。そして、スイッチング回路である FET のドレーン・ソースを通信線路のデータ線と GND 線に接続するように実装することで（図 3.2)、整流回路とローパスフィルタの出力に応じた通信線路上のデータ線と GND 線の短絡が発生し、UART モジュール間の通信線路上に任意のデータを表す電気信号の生成が可能となる[‡]。

以上のように、任意データを表す電気信号は、IC 外部の HT に実装された FET のスイッチング動作によるデータ線と GND 線の短絡によって生成されているた

[‡]本論文では、デジタル信号が伝送される UART モジュールを攻撃対象として IC 外部の HT を設計したため、他の電子機器を攻撃対象とした場合には異なる設計が必要となる。



Reference:
C1 - C5: 47 pF
R1: 20 kΩ
FB1 - FB2:
Murata BLM18RK102SN1
D1 - D4:
Broadcom HSMS-286C
FET1:
Broadcom ATF-54143

図 3.2　IC 外部の HT の回路図

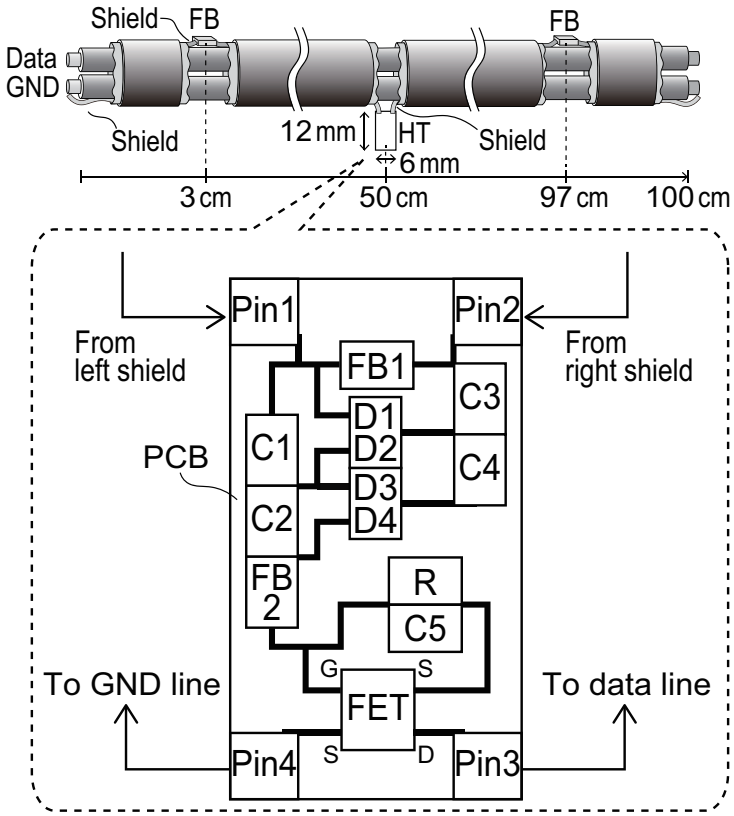


図 3.3　UART の通信線路に対する FB と IC 外部の HT の実装方法

め、攻撃のタイミングは UART モジュール間の通信線路上のデータ線が無通信状態に限られる。

続いて、任意データの注入に用いる振幅変調波の信号の特性について説明する。前述の IC 外部の HT は、機器内部に伝搬した振幅変調波が IC 外部の HT の動作電圧しきい値を超えた際に、UART モジュール間の通信線路上のデータ線と GND 線を短絡させ電位を変化させる。そのため、データを注入する際に必要となる振幅変調波は、UART モジュールに注入するビット情報を反転させた信号を変調信号とし、受信アンテナとなるシールド導体と電気的に共振する周波数の電磁波をキャリアとする。

3.3 不正な回路改変を用いたデータ注入の実証実験

図 3.4 に UART モジュールへのデータ注入を行う実験環境、表 3.2 に実験で利用した実験機器とパラメタを示す。

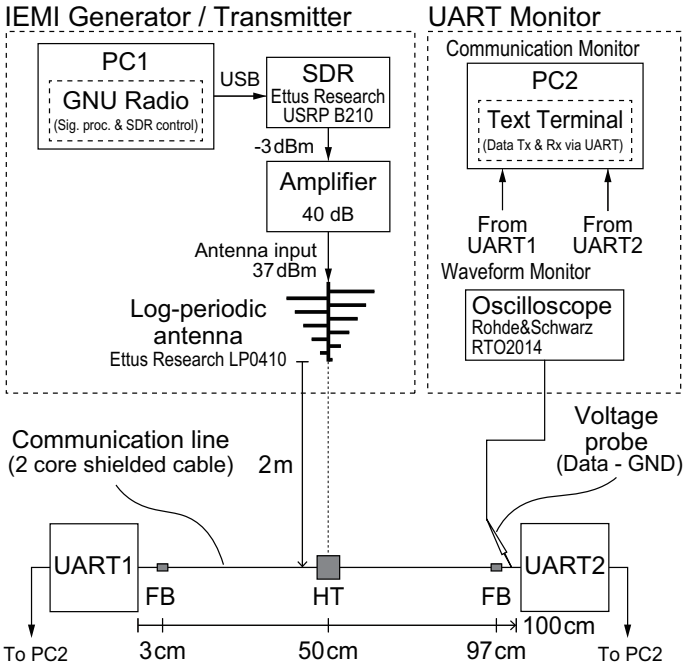


図 3.4 データ注入を行う実験セットアップ

表 3.2　実験機材および使用するパラメタ

実験機材	
SDR	Ettus Reserch USRP B210
SDR ソフトウェア	GNU Radio 3.7.12
高周波電力増幅器	アールアンドケー A000110-4040-R
振幅変調波の照射アンテナ	Ettus Reserch LP0410
オシロスコープ	Rohde & Schwarz RTO2014
振幅変調波のパラメタ	
キャリア周波数	460 MHz
尖頭電力	37 dBm (5 W)
振幅変調の変調度	100 %
注入する信号のパラメタ	
振幅変調の論理	負論理
ボーレート	9.6 kbps
スタートビット	1 bit
ストップビット	1 bit
パリティビット	なし

本実験では、SDR（Ettus Research USRP B210）と信号処理・制御ソフトウェア（GNU Radio 3.7.12）、高周波電力増幅器（アールアンドケー A000110-4040-R）、ログペリオディックアンテナ（Ettus Research LP0410）を利用した。GNU Radio と USRP を用いた、振幅変調波生成のデータ・信号処理のフローを図 3.5 に示す。生成した振幅変調波は、UART モジュール間の通信線路に対して平行に配置したログペリオディックアンテナによって照射した。本実験で照射した振幅変調波のキャリア周波数は、本実験で利用したログペリオディックアンテナの帯域が 400 MHz–1G Hz に制限されていることより 460 MHz を選択し、UART モジュール間のシールド導体の長さは振幅変調波のキャリア周波数の約 3/2 波長で電気的に共振する 94 cm とした。そして、ログペリオディックアンテナ入力部の尖頭電力は 37

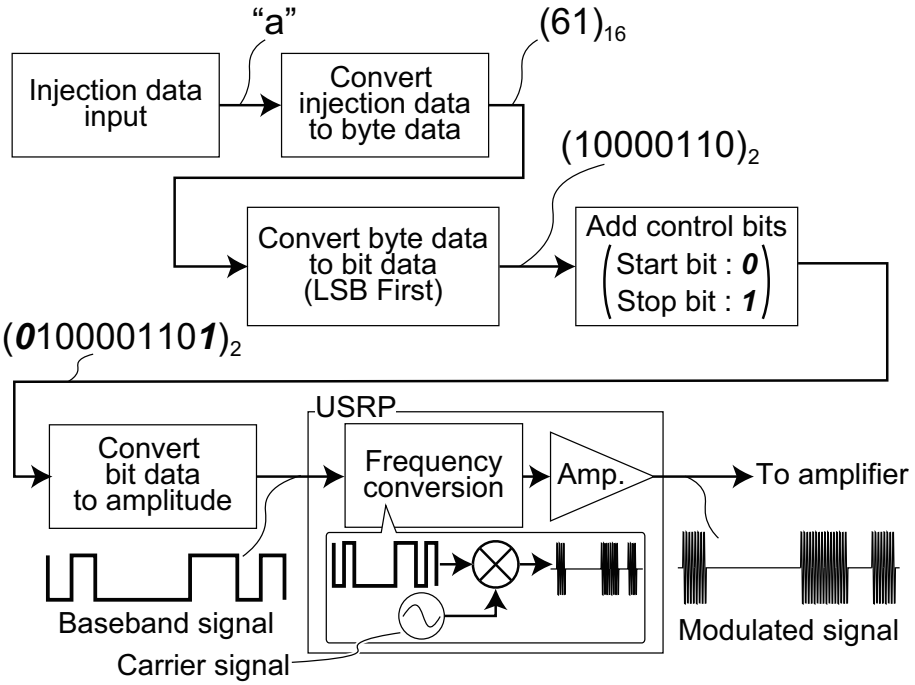


図 3.5　振幅変調波の生成フロー

dBm、振幅変調波の変調度は 100 %、変調信号の論理は負論理とした。また、注入するデータのボーレートおよびスタートビット、ストップビットは表 3.1 の UART の通信パラメタを利用した。

本実験では、振幅変調波の照射時に UART モジュール間の通信線路上に任意のデータを表す電気信号が注入されていることを、データ線と GND 線をタッピングしたパッシブプローブとオシロスコープで確認した。また、注入した電気信号が UART モジュール内の IC で正しく処理されることを UART モジュールの受信端に接続した PC で確認した。

続いて、図 3.6 に上述の実験環境を用いた UART モジュールへのデータ注入の結果を示す。図 3.6 に UART モジュールのデータ線と GND 線間の時間領域波形について、不正な回路改変を行っていない通信線路で UART モジュール同士の通信時に伝送される“Y”の観測波形を（a)、不正な回路改変を行った通信線路に対して“Y”のデータを振幅変調波として照射した場合の観測波形を（b)、不正な回路改変が行っていない通信線路に対して“Y”のデータを振幅変調波として照射し

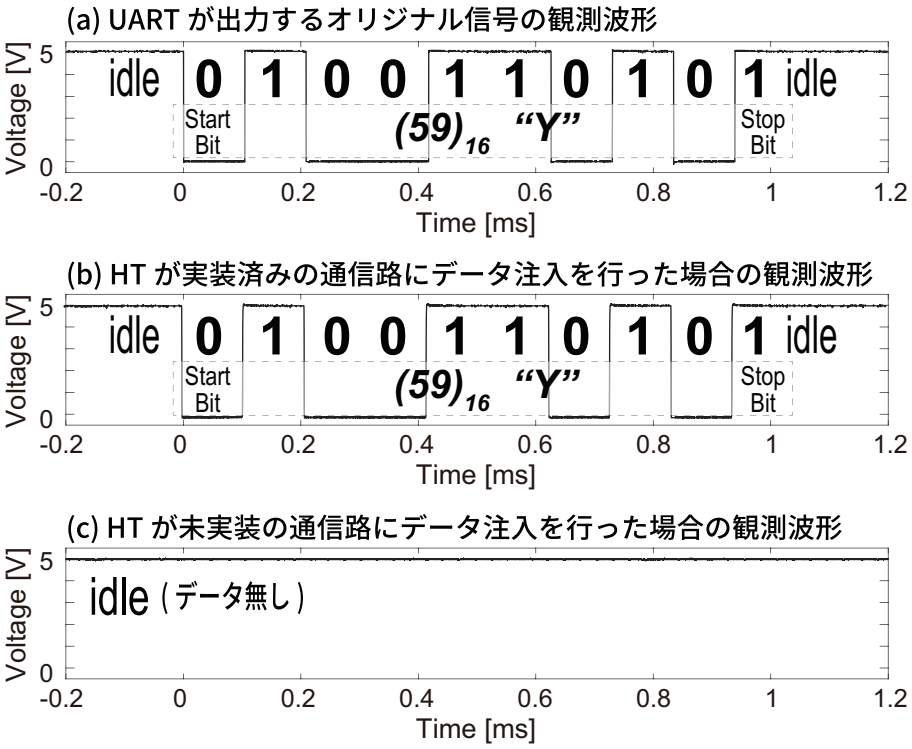


図 3.6　UART モジュールの通信線路をタッピングした時間領域波形

た場合の観測波形を（c）に示す。

図 3.6（a）では、時間経過に応じて電気信号が変化し、スタートビット、最下位ビットを先頭とする“Y”の ASCII コード、ストップビットが観測された。図 3.6（b）では、図 3.6（a）で観測された UART 通信の電気信号の変化と同等の変化が観測され、UART モジュールの受信端を接続した PC 上でも“Y”のデータの注入が確認された。図 3.6（c）では、図 3.6（a）や図 3.6（b）のような固有の電気信号の変化は観測されず、UART モジュールの受信端を接続した PC 上でも“Y”のデータの注入は確認できない。

本実験結果より、潜在的に高いイミュニティを有する電子機器に対して不正な回路改変を行うことによって、機器のイミュニティを局所的に低下させることが可能であることを示した。また、電子機器の機密性・完全性を低下させる Low-power IEMI を用いた任意データの注入が可能であることが示された。

本節では“Y”のデータを注入した結果のみを示しているが、他のデータを含んだ振幅変調波の照射によってもデータの注入が可能であることを確認している。

3.4 不正な回路改変の検出手法の基礎的な検討

本論文で提案した不正な回路改変は、攻撃対象機器のイミュニティを意図的に低下させ、機器外部で照射された電磁波を機器内部に伝搬させることでデータ注入を可能にしている。このようなイミュニティの低下は、機器の等価回路網を変化させることに相当するため、機器から放射する電磁波の時間領域波形や周波数領域波形に変化が生じる [26]。よって、機器から定期的に放射される信号をマーカとして観測することで、時間領域波形または周波数領域波形の変化から機器に電気的な改変が行われたことが観測できる可能性がある。例えば、機器から放射される広帯域ノイズ源のクロックに着目し [27]、放射される時間領域波形もしくは周波数領域波形の歪みを観測することで不正な回路改変の実装を検知できる可能性がある。

3.5 まとめ

本章では、2 章で論じた電子機器のイミュニティを局所的に低下させる不正な回路改変と、Low-power IEMI を用いて任意のデータを機器内部に注入される脅威の実現可能性を示すため、シリアル通信の UART を攻撃対象機器として実験を行った。UART モジュールに対して FB と IC 外部の HT から成る不正な回路改変を行うことによって、改変前は照射した Low-power IEMI が機器内部に伝搬しないのに対して、改変後は同強度で照射した Low-power IEMI が機器内部に伝搬し、UART モジュールが生成する正規の信号を模した電気信号の生成を可能とした。また、生成した電気信号が UART モジュールの IC に到達することで正規の信号として処理され、UART モジュールの受信端を接続した PC 上で任意のデータの注入が確認できた。そして、本論文で提案した不正な回路改変で用いられる電子部品の実装の際に生ずる機器周辺の電磁環境の変化を観測して不正な回路改変を検出する方法に関する基礎的な検討を行った。

第 4 章　結論

EMC の分野において、高電力電磁波を用いた IEMI は機器を破壊し、可用性を損なわせる脅威であるとされてきたが、近年の情報セキュリティの分野では、低電力電磁波を用いた IEMI によって機器に誤りや誤動作を引き起こし、機密性や完全性を損なわせる脅威が報告されてきた。本論文では、破壊を伴わない数十 V/m 程度の IEMI を Low-power IEMI と定義し、Low-power IEMI を用いた攻撃の新たな脅威について論じた。従来の Low-power IEMI を用いた攻撃は、全ての機器が攻撃の対象となるわけではなく、潜在的にイミュニティが低い機器が対象となっていた。しかし、不正な回路改変によって機器のイミュニティを意図的に低下させることが可能となれば、これまで攻撃の対象外と見なされていた電子機器に対しても Low-power IEMI を用いた攻撃の脅威が拡大する可能性がある。そのため、本論文の各章では、次のような議論を行った。

2 章では、不正な回路改変を用いたイミュニティの低下手法と Low-power IEMI を用いた任意のデータ注入手法について論じた。本論文で提案した不正な回路改変は、通信線路上のシールド導体を高周波的に攻撃対象機器から分離することで、特定周波数の電磁波の伝搬効率を高めイミュニティを低下させた。そして、任意のデータを注入する方法として、IC 外部に実装可能な HT を用い、伝搬した振幅変調波を攻撃対象機器内部の IC が処理可能な信号に変換することで任意のデータの注入を実現する方法を提案した。また、不正な回路改変を用いた攻撃が実現する可能性について、電子機器への不正な回路改変のタイミングと改変の手法、不正な回路改変と Low-power IEMI を用いた攻撃を組み合わせた際の攻撃成立条件について論じた。

3 章では、2 章で提案した不正な回路改変によるイミュニティの低下と、Low-power IEMI を用いた任意のデータ注入攻撃の実現可能性を示した。実証実験では、高いイミュニティを有する通信機器を攻撃の対象とし、不正な回路改変を行うことによってイミュニティが低下と、Low-power IEMI を用いたデータ注入攻撃が成立することを示した。また、不正な回路改変を行う際の電子部品の実装によって生じる機器周辺の電磁環境の変化を取得することで不正な回路改変が検出できる可能性を示した。

以上の議論より、本論文で提案した不正な回路改変と Low-power IEMI を用いたデータ注入の組み合わせにより、機器の機密性や完全性が損なわれる新たな脅威となり得ることを示した。本論文では、電子機器の接続線路に対して着目し、不正な回路改変による脅威について示したが、本論文で検討していないプリント基板やその他の電子機器も同様の脅威が発生する可能性がある。そのため、これらへの攻撃の可能性の検討と共に、不正な回路改変の検知や検出だけでなく、改変を行わせないための設計や対策を検討していくことが必要であると考える。

謝辞

本研究は、奈良先端科学技術大学院大学情報科学研究科情報科学専攻情報セキュリティ工学研究室（林研究室）において行った研究をまとめたものです。

主指導教員の林優一教授には、丁寧かつ熱心な御指導、御鞭撻を賜りました。また、多くの学会発表と国際共同研究への従事の機会を与えて頂き、大変貴重な経験を得ることができました。ここに心より厚く御礼申し上げます。

副指導教員の井上美智子教授ならびに岡田実教授には、本論文の執筆にあたり有益な御助言、御討論を賜りました。深く感謝申し上げます。

本研究室の藤本大介助教には、研究生活において丁寧かつ熱心な御指導、御助言をはじめ、様々な御支援を頂きました。深く感謝申し上げます。

仙台高等専門学校の衣川昌宏助教には、研究方針の御討論、実験の御指導、御助言、論文の執筆に至るまで御指導を頂きました。深く感謝申し上げます。

本研究室秘書の石谷由美様には、学会参加のお手続きや研究室運営などをはじめ、様々な面でお世話になりました。深く感謝申し上げます。

本研究室の博士前期課程 2 年の皆様には、林研究室の第 1 期生として入学当初から御協力頂くと共に、日々の討論の機会を与えて頂きました。深く感謝申し上げます。

本研究室の博士前期課程 1 年の皆様には、多くの実験指導の機会を与えて頂きました。深く感謝申し上げます。

最後に、家族には、学業生活を様々な面から支えて頂きました。心より厚く御礼申し上げます。

参考文献

[1] H. W. Ott 著, 出口博一・田上雅照・高橋丈博 訳（2013）「詳解 EMC 工学 実践ノイズ低減技法」, 東京電機大学出版局.

[2] Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test, IEC 61000-4-3, 2006.

[3] M. W. Wik and W. A. Radasky,“Intentional Electromagnetic Interference (IEMI) - Background and Status of the Standardization Work in the International Electrotechnical Commission (IEC),” URSI Gen. Assem. 2002.

[4] W. A. Radasky, "Fear of frying electromagnetic weapons threaten our data networks. Here's how to stop them," IEEE Spectrum, vol. 51, no. 9, pp. 46–51, Sept. 2014.

[5] M. W. Wik and W. A. Radasky, “Development of High-Power Electromagnetic (HPEM) Standards,” IEEE Trans. Electromagn. Compat., vol. 46, no. 3, pp. 439–445, Aug. 2004.

[6] D. V. Giri, F. M. Tesche, and C. E. Baum, “An Overview of High-power Electromagnetic (HPEM) Radiating and Conducting Systems,” URSI Radio Sci. Bull., vol. 2006, no. 318, pp. 6–12, 2006.

[7] High-power electromagnetic (HPEM) environments Radiated and conducted, IEC 61000-2-13, 2005.

[8] High-power electromagnetic immunity guide for telecommunication systems, ITU K. 81, 2016.

[9] High-power electromagnetic (HEPM) Effects on civil systems, IEC 61000-1-5, 2004.

[10] 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. Compat., vol. 46, no. 3, pp. 314–321, 2004.

[11] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu,“Ghost Talk: Mitigating EMI Signal Injection Attacks against

Analog Sensors," in 2013 IEEE Symposium on Security and Privacy, pp. 145–159, 2013.

[12] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, "Transient IEMI Threats for Cryptographic Devices," IEEE Trans. Electromagn. Compat., vol. 55, no. 1, pp. 140–148, Feb. 2013.

[13] C. Kasmi and J. Lopes Esteves, "IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones," IEEE Trans. Electromagn. Compat., vol. 57, no. 6, pp. 1752–1755, Dec. 2015.

[14] M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer Science & Business Media, 2011.

[15] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog Malicious Hardware," in 2016 IEEE Symposium on Security and Privacy (SP), pp. 18–37, 2016.

[16] M. Rostami, F. Koushanfar, and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," Proc. IEEE, vol. 102, no. 8, pp. 1283–1295, Aug. 2014.

[17] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," IEEE Des. Test Comput., vol. 27, no. 1, pp. 10–25, 2010.

[18] W. Xiaoxiao, M. Tehranipoor, and J. Plusquellic, "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions," in 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 15–19, 2008.

[19] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," in 2009 IEEE International High Level Design Validation and Test Workshop, pp. 166–171, 2009.

[20] M. Ossmann, "The NSA Playset: RF Retroreflectors," DEF CON 22, 2014.

[21] M. Ossmann, "The NSA Playset: A Year of Toys and Tools," black hat USA, 2015.

[22] M. Kinugawa, Y. Hayashi, and T. Mori, "Evaluation of EM Information

Leakage caused by IEMI with Hardware Trojan," IEEJ Trans. Fundam. Mater., vol. 137, no. 3, pp. 153–157, 2017.

[23] Bloomberg, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," [Online]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies, 2018.

[24] 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.

[25] 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. Electromagn. Compat., vol. 55, no. 3, pp. 555–563, June 2013.

[26] Y. Hayashi, N. Homma. T. Mizuki, T. Aoki, H. Sone, L. Sauvage, J. L. Danger, "Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures," IEEE Trans. Electromagn. Compat., vol. 55, no. 3, pp. 571–580, 2013.

[27] C. R. Paul, Introduction to Electromagnetic Compatibility, K. Chang, ed., John Wiley & Sons, New York, 1992.

著者発表論文

[1] Shugo Kaji, Masahiro Kinugawa, Daisuke Fujimoto, and Yu-ichi Hayashi, “Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan,” IEEE Transactions Electromagnetic Compatibility, DOI: 10.1109/TEMC.2018.2849105, 2018.

[2] Shugo Kaji, Masahiro Kinugawa, Daisuke Fujimoto, and Yu-ichi Hayashi, “Data injection attacks using a hardware Trojan on a transmission line,” in 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), 2018.

[3] 鍛治秀伍, 衣川昌宏, 藤本大介, 林優一, “HT を用いて局所的にイミュニティを低下させた電子機器へのデータ注入攻撃,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 1D2-3, 2018.

[4] 鍛治秀伍, 衣川昌宏, 藤本大介, 林優一, “ハードウェアトロイを用いた情報通信機器へのデータ注入攻撃に関する基礎検討,”環境電磁工学研究会 (EMCJ) 若手研究者発表会, pp. 49–54, 2018.