博士論文

# 放射電磁波と電磁妨害の双方を考慮した<br>情報セキュリティの研究

鍛治 秀伍
奈良先端科学技術大学院大学
先端科学技術研究科
情報理工学プログラム

主指導教員: 林 優一
情報セキュリティ工学研究室（情報科学領域）

令和 5 年 3 月 17 日提出

本論文は奈良先端科学技術大学院大学先端科学研究科に
博士（工学）授与の要件として提出した博士論文である.

鍛治 秀伍

審査委員：

| | | |
|---|---|---|
| 主査 | 林 優一 | （情報科学領域 教授） |
| | 井上 美智子 | （情報科学領域 教授） |
| | 岡田 実 | （情報科学領域 教授） |
| | 藤本 大介 | （情報科学領域 助教） |
| | Kim Youngwoo | （情報科学領域 助教） |

# 放射電磁波と電磁妨害の双方を考慮した情報セキュリティの研究*

鍛治 秀伍

## 内容梗概

情報通信システムは欠かせない社会インフラの一つであり、その信頼の基点となるハードウェアのセキュリティの確保が課題となっている。中でも電磁波を介したセキュリティ（電磁波セキュリティ）の脅威は、攻撃の痕跡が残らないことから深刻な問題となっている。電磁波セキュリティの脅威は、電磁波を介した情報漏えい（電磁情報漏えい）と意図的に発生させた電磁波による機器の動作妨害（意図的な電磁妨害）に分類され、その脅威の対象となるか否かは、機器からの不要放射の強度（エミッション）と電磁妨害波に対する耐性（イミュニティ）により決定される。これまで、機器のエミッションやイミュニティに基づいた電磁波セキュリティの脅威や対策技術が検討されてきたが、機器のエミッションやイミュニティが攻撃者によって制御可能な場合、これまで脅威の対象外とされていた機器にも脅威が拡大し、従来の対策技術が無効化される恐れがある。

上述の背景に基づき、本研究では、機器のエミッションとイミュニティの制御により引き起こされる電磁波セキュリティの脅威を示すと共に、セキュリティ低下のメカニズムに基づいた対策技術について示した。具体的には、これまで脅威の対象外とされてきた機器に電磁波を照射し、その反射波から機器内部で電気信号として表現される情報が取得可能であることを示した。また、電磁波の照射強度に応じて

*奈良先端科学技術大学院大学 先端科学研究科 博士論文, 令和 5 年 3 月 17 日.

エミッションが制御され、電磁情報漏えいが引き起こされる範囲を制御可能であることを示した。続いて、機器の等価回路網の一部を意図的に改変することによりイミュニティが制御され、機器内部に任意の電気信号を誘導し、機器の動作を改変可能であることを示した。さらに、エミッションとイミュニティの制御によりセキュリティが低下するメカニズムを明らかにし、そのメカニズムに基づいた脅威の検知・対策技術を提案した。

以上の結果より、本研究は環境電磁工学の知見を情報セキュリティに応用し、潜在的に電磁波セキュリティの脅威に耐性を有していた機器に対しても脅威がおよぶ可能性について検討を行うと共に、新たな脅威に対しても、電気信号として表現される情報の取得と誘導の困難化に着目することでそれらを抑止できることを示した。

**キーワード**

電磁情報漏えい, 意図的電磁妨害, IEMI, 回路改変, ハードウェアトロージャン

# Electromagnetic Information Security Focusing on the Physical Phenomenon of both Emission and Interference*

Shugo Kaji

**Abstract**

Information and communication systems are an indispensable part of social infrastructure, and ensuring the security of hardware, which is the root of trust in such systems, has become an issue. In particular, security threats to hardware through electromagnetic (EM) waves (EM information security) are a serious problem because these threats leave no trace of the attacker. EM information security threats are classified into two categories: information leakage through EM waves (EM information leakage) and interference with device operation by intentionally generated EM waves (intentional EM interference). The target devices of these threats are determined by the intensity of unintentional EM radiation from the device (emission) and the resistance of the device to EM interference (immunity). Threats and countermeasure methods for EM information security based on the emission and immunity of the device have been proposed. However, if an attacker can control the emission and immunity of a device, the threats may extend to devices that were not previously considered the target of the threat, and the conventional countermeasure methods may be disabled.

*Doctoral Dissertation, Graduate School of Science and Technology, Nara Institute of Science and Technology, March 17, 2023.

This study demonstrates the EM information security threats induced by the emission and immunity control of the devices and proposes countermeasure methods based on the mechanism of EM information security degradation. Specifically, this study shows that it is possible to obtain information expressed as electrical signals inside devices from reflected waves of irradiated EM waves on devices that are considered as the target of conventional threats. Additionally, it shows that emission is controlled according to the intensity of the EM irradiation and that the distance of EM information leakage is controllable. Moreover, this study shows that immunity can be controlled by intentionally modifying parts of the equivalent circuit of the device and arbitrary electrical signals can be induced inside the device to modify its operations. Finally, the mechanisms of EM information security degradation caused by emission and immunity control are revealed, and threat detection and countermeasure methods based on these mechanisms are proposed.

From these results, this study applied the field of EM compatibility findings to information security and investigated the threats on devices that are potentially resistant to EM information security threats. Additionally, it showed that new threats could be protected by focusing on the difficulty in obtaining and inducing information expressed as electrical signals.

**Keywords:**

Electromagnetic information leakage, intentional electromagnetic interference, IEMI, circuit modification, hardware Trojan

# 目次

# 図目次

# 表目次

# 第 1 章　序論

## 1.1　研究背景

情報通信技術の社会インフラ化に伴い、情報通信機器（以下、機器）がネットワークを介して相互に接続され、機器やセンサなどから膨大な情報やデータが得られるようになった。我が国が提唱する Society 5.0 では、仮想空間と物理空間を高度に融合させたシステムにより社会問題の解決を目指している [1]。これに伴い、機器が扱う情報やデータの重要性がより一層高まり、これらを保護する情報セキュリティ（以下、セキュリティ）が求められている [2, 3]。セキュリティは一般に、許可された利用者だけが情報にアクセスできる「機密性」、情報の改ざんや破壊がされておらず完全である状態を保持する「完全性」、許可された利用者がいつでも情報にアクセスできる「可用性」の 3 要素を確保することである。

これまで、ネットワークを介した攻撃が主たるセキュリティの脅威とされてきたが、近年では機器の信頼の基点であるハードウェアに対する物理的な攻撃の可能性が報告されている。ハードウェアへの物理的な攻撃による影響はハードウェアの処理や演算結果を信頼して動作する上位レイヤに波及することから、従来のネットワークセキュリティと同様にセキュリティの脅威からハードウェアを保護することが課題となっている。ハードウェアへの物理的な攻撃のうち、特に、電磁波を介した攻撃は機器の利用者が攻撃の実行を検知することが困難であると共に、痕跡を残さない攻撃が可能であることから深刻な脅威とされている。また、計測器の高性能化や低価格化、ソフトウェア無線 (SDR: Software Defined Radio) の普及、インターネットを介した SDR 制御プログラムの共有 [4] などによって、非専門家であっても電磁波を介した攻撃が実行可能となり現実的な脅威とされている。

電磁波を介したセキュリティ（以下、電磁波セキュリティ）の脅威は、主に環境電磁工学 (EMC: Electromagnetic Compatibility) の分野で議論されており、機器の動作に起因して生じる放射電磁波による情報漏えいの脅威と意図的に発生させた電磁波の照射による機器の動作を妨害する脅威に分類される。

## 1.2 機器の動作に起因して生じる放射電磁波を介した情報漏えいの脅威

機器内部で情報が処理・伝送される際は電気信号として表現され、電流や電圧などの電気信号に時間的な変化が生じる。このような電気信号の時間的な変化に伴い副次的に生じた電磁波（以下、エミッション）が受信・解析されることにより、機器内部の伝送情報が漏えいし機密性が損なわれる脅威（以下、電磁情報漏えい）が報告されている [5–11]。このような電磁情報漏えいの脅威は、米国連邦通信委員会 (FCC: Federal Communications Commission)、国際無線障害特別委員会 (CISPR: Comité International Spécial des Perturbations Radioélectriques) などの EMC の観点で定められた規格 [12] に適合した機器も対象となることが知られている。特に、人間を対象とした入出力機器であるディスプレイ [13–17] やキーボード [18–21]、プリンタ [22, 23] などの機器の入出力信号は、利用者による入力・解釈のため伝送情報に暗号化処理が施されておらず、これらの入出力信号が漏えいした場合は攻撃者によって即座に情報が把握される可能性がある。

図 1.1 に利用者が入力した情報が電気信号として処理・伝送される過程の例を示す。利用者による入力情報や機器内部で生成された情報は集積回路 (IC: Integrated Circuit) で処理され（図 1.1 (a)）、IC の出力回路を介して電気信号として伝送線路に出力される（図 1.1 (b)）。出力された電気信号は次の処理が行われる IC やモジュール*に伝送され（図 1.1 (c)）、伝送された電気信号は IC やモジュールで受信された後に次の処理が実行される（図 1.1 (d)）。この過程で生ずる情報を含むエミッションは、機器内部の情報を表す電気信号（ソース：図 1.2 (a)）の強度と機器の物理構造に起因したソースを機器外部に放射する機器の設計者が意図しないアンテナ構造（アンテナ：図 1.2 (b)）、そして、ソースとアンテナを接続する機器内部の電磁的な結合の経路（パス：図 1.2 (c)）の各要素の周波数特性によって決定される [24, 25]。そして、図 1.1 で示した情報が機器内部で電気信号として処理・伝送される過程で生じた信号（図 1.2 (d)）もしくは、それらの複数が混合した信号（図 1.2 (e)）が機器外部に放射される。そして、機器のエミッションが攻撃者によって

*本論文では、プリント基板 (PCB: Printed Circuit Board) や筐体などに対し、IC やその周辺回路が実装されたものを指す。

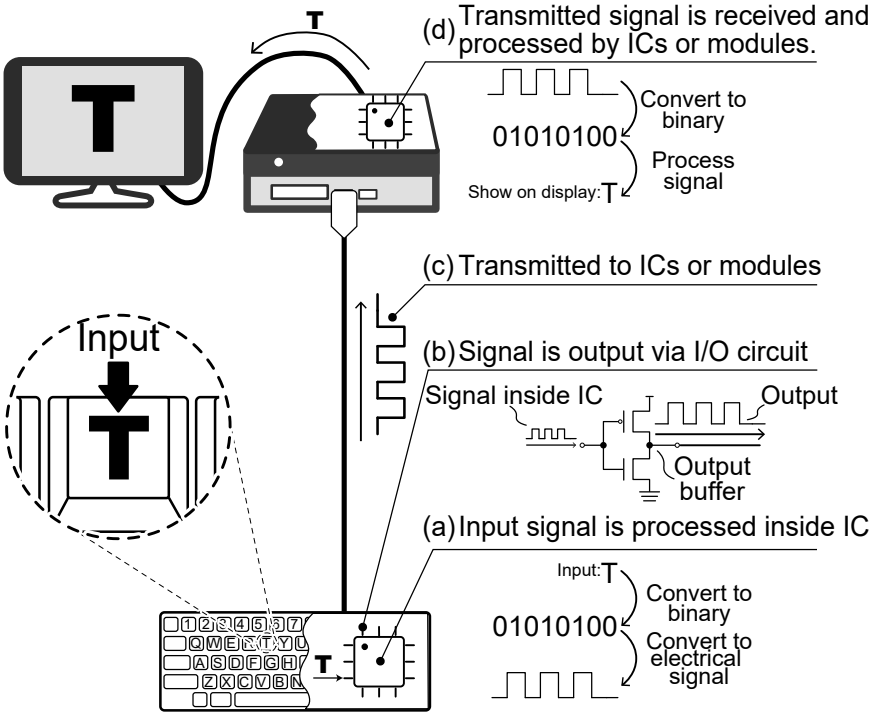


図 1.1. 電磁情報漏えいの脅威のターゲットとなる入出力機器の入力情報が機器内部で処理され電気信号として伝送される例

受信・解析されることで電磁情報漏えいが生じる。

機器のエミッションを決定する機器のソース・パス・アンテナとなる機器の要素のうち、「ソースの信号強度が弱い機器」や「パスの電磁的結合が弱い機器」、「アンテナの周波数特性が低い機器」は機器外部に放射するエミッションの強度（以下、エミッションレベル）が低く、機器の近傍において機器周辺のノイズの強度を下回る場合がある。このような機器は、攻撃者がエミッションを受信できないため電磁情報漏えいの脅威に対して耐性を有していると考えられ、電磁情報漏えいの脅威の対象外とされてきた [26, 27]。

このようなエミッションレベルが低い機器に対して、軽量・小型化した計測器を用いてターゲットとなる機器に接近しエミッションを受信する攻撃手法 [15, 28, 29] や、利得の高いアンテナや広い分解能帯域幅 (RBW: Resolution Band Width) を有する計測器を用いて機器周辺のノイズの影響を低減する攻撃手法 [30, 31]、複数

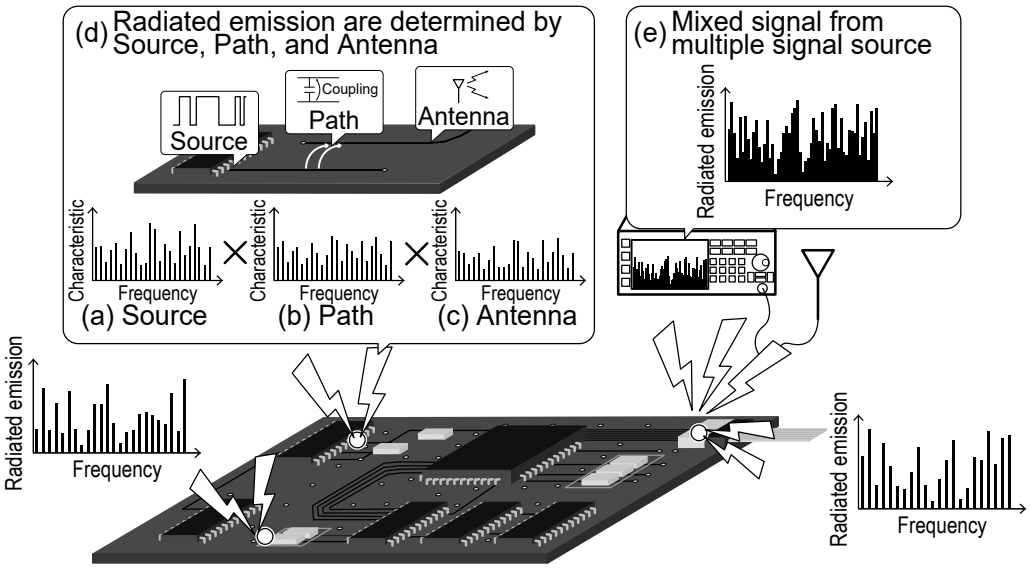


図 1.2. 機器外部で計測されるエミッションが機器のソース・パス・アンテナの各要素の周波数特性により決定される概念図

のエミッションを受信し信号処理によって機器周辺のノイズの影響を低減する攻撃手法 [14, 32] などが報告されている。

上述した攻撃への対策として、機器の筐体や接続線路、建物などに電磁波シールドを実装するシールディング [33, 34] や電源へのフィルタの実装 [35]、機器を設置した部屋や建物、その敷地などによって攻撃者が接近できる物理的な距離を確保するゾーニング [33, 34, 36] が提案されている。これらの電磁情報漏えいの対策技術は、機器のエミッションレベルを低減させることで攻撃者によるエミッションの受信を困難化させることに主眼が置かれてきた。

これまでの電磁情報漏えいの脅威や対策技術に関する検討では、「電磁情報漏えいの脅威はエミッションを受動的に計測する手法」、「エミッションレベルは機器のソース・パス・アンテナモデルによって決定され、攻撃者がエミッションレベルを制御することはできない」という前提で議論されてきた。一方、機器のエミッションレベルを制御する能動的な計測手法が成立した場合、従来の対策手法では新たな脅威に対抗できない可能性があると共に、従来の脅威対象外の機器にも電磁情報漏えいの脅威が拡大する可能性がある。このような脅威に対抗するため、能動的な計

測による電磁情報漏えいの新たな脅威の実現可能性を示すと共に、そのメカニズムを基づいた対策手法の提案が課題となる。

## 1.3 意図的な電磁波の照射による機器の正常な動作を妨害する脅威

意図的な電磁波の照射によって機器の故障や動作妨害を引き起こす電磁妨害 (IEMI: Intentional Electromagnetic Interference [37, 38]) の脅威が報告されている。IEMI は、機器が有する電磁妨害耐性（以下、イミュニティ）[39] をはるかに上回る高電力電磁波 (HPEM: High Power Electromagnetic [40, 41]) を用いて機器を破壊・無効化し（図 1.3)、可用性を損なわせる脅威と定義されている [38, 42, 43]。このような脅威に対し、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、ピーク電界強度が 100 V/m 以上を放射 HPEM 環境、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電流および電圧を伝導 HPEM 環境と定義すると共に、対策技術に関する規格の策定が進められている [44, 45]。また、意図的に照射された電磁波の伝搬過程の解明や IEMI によってシステムが受ける影響の評価、IEMI からのシステムや伝送情報の保護する手法が議論されている [37, 46]。

一方、HPEM を用いた脅威とは異なり、機器の IC や素子の破壊を伴わない低電力電磁波を用いて機器の処理や伝送情報への誤り、機器の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いる。具体的な例として、暗号デバイスに対して意図的に電磁波を照射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脅威 [47–51] や、スマートスピーカやスマートフォン、CCD (Charge Coupled Device) カメラなどに対して変調した電磁波を照射することで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情報や命令を注入する脅威 [52–58] が報告されている。

これらの脅威では、攻撃の対象となる IC や素子に対して照射された電磁波が低損失で伝搬する周波数を選択すると共に、伝送情報のプロトコルや情報が処理されるタイミングに応じた攻撃の実行が脅威の成立条件となる。特に、IC や素子に対して照射された電磁波が低損失で伝搬する周波数は、機器のイミュニティにより決

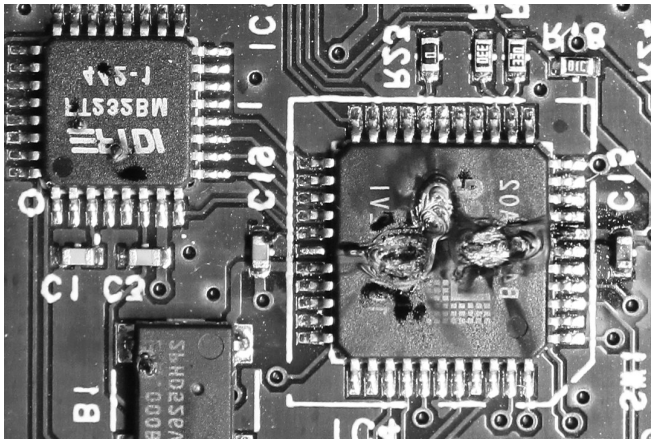

図 1.3. HPEM によって破壊された機器内部の IC

定される。この機器のイミュニティは機器の回路構造や実装素子などに影響されることから、攻撃者が機器のイミュニティを推定することは困難である。そのため、攻撃者は照射する電磁波の周波数を掃引した際の応答の計測 [50, 53, 56, 58] や機器の開封を伴う伝達特性の事前計測 [54] によって照射周波数を決定していた。このような攻撃に対して、機器の設計・製造の段階でイミュニティが低くなりえる部位や周波数をシミュレーションにより推定し、筐体や接続線路のシールディングやフィルタの実装によるイミュニティを向上させる対策が有効な手法の 1 つとされている [53, 59]。

これまで、機器のイミュニティが低い周波数や機器の部位を攻撃者が推定することは困難とされてきた。一方、機器のイミュニティを制御可能な脅威が成立する場合、従来の対策手法ではこのような脅威に対抗できない可能性がある。また、従来の脅威対象外の機器にも意図的な電磁波の照射による動作妨害の脅威が拡大する可能性がある。そのため、機器のイミュニティを制御可能な脅威の実行可能性を示すと共に、そのメカニズムを基づいた対策手法の提案が課題となる。

## 1.4　本研究の目的

前節までに、電磁波セキュリティの脅威である電磁情報漏えいの脅威と意図的な電磁波の照射による動作妨害の脅威を挙げ、従来の検討よりそれぞれの脅威を引き起こす手法やそのメカニズム、対策技術を示した。これまで、機器の構造や実装によって決定されるエミッションとイミュニティを基に電磁波セキュリティの脅威の評価や対策技術が検討されてきた。一方、機器のエミッションとイミュニティを制御する新たな脅威が成立する場合、従来の対策技術ではこれらの脅威に対抗できない可能性がある。また、このような場合には、これまで電磁波セキュリティの脅威の対象外と見なされていた機器にも脅威がおよぶ恐れがあり、新たな脅威に対抗する対策技術が求められる。

本研究では、機器のエミッションの制御により誘発される電磁情報漏えいの脅威とイミュニティの制御により誘発される意図的な電磁波の照射による動作妨害の脅威を示すと共に、それらのメカニズムを解明することを目的とする。また、それらのメカニズムに基づく対策技術を提案する。

具体的には、機器のパス・アンテナが機器外部の電磁波を受信し機器内部に伝搬する要素として捉えられることに着目し、意図的に照射した電磁波を機器内部に誘導する。そして、エミッションを決定するソースの生成回路（図 1.1 (a), (b)）の電気的な特性や状態の変化を、照射した電磁波の反射より能動的にセンシングすることでエミッションに含まれる情報と同等の情報を取得する。また、機器外部から意図的に照射した電磁波により生じる応答の強度は、電磁波の照射強度に応じて比例の関係となることが予想されるため、照射した電磁波の強度に応じてエミッションが制御される。このような脅威を従来の電磁情報漏えいの脅威対象外の機器を用いて示す。続いて、機器のパス・アンテナの等価回路網の一部を改変することで、意図的に照射した電磁波が機器内部に誘導されやすい状態を意図的に構築しイミュニティを制御する。また、意図的な電磁波の照射による動作妨害の一例として、任意の情報が機器内部に注入されることを従来の脅威対象外の機器を用いて示す。そして、能動的なセンシングと等価回路網の改変による機器のエミッションとイミュニティの制御が引き起こすセキュリティの脅威のメカニズムを解明し、そのメカニズムに基づいた対策技術を検討する。

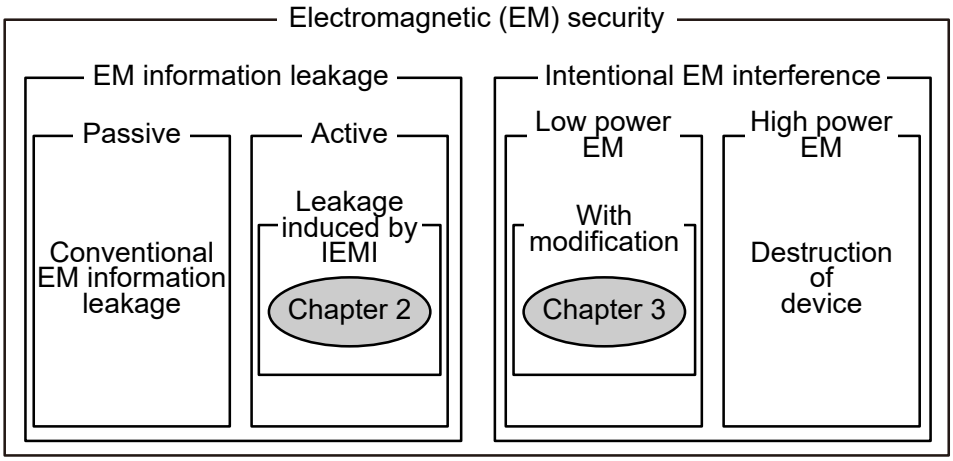


図 1.4. 本論文の構成

## 1.5 本論文の構成

本論文の構成は以下の通りである。(図 1.4)。

2 章では、意図的な照射電磁波を用いて機器内部のソースを生成する回路の電気的な特性や状態の変化を能動的にセンシングすることにより、機器のエミッションが制御されることを示す。また、電磁情報漏えいによるセキュリティの脅威が従来の脅威対象外の機器に拡張される可能性について実証すると共に、能動的なセンシングに用いる電磁波の照射強度に応じて、情報を取得可能な距離が制御可能であることを示す。そして、意図的な照射電磁波が引き起こす電磁情報漏えいのメカニズムを明らかにし、そのメカニズムに基づく対策技術を提案する。

3 章では、機器の等価回路網の一部の改変により、意図的に照射された電磁波が引き起こす機器の動作妨害によるセキュリティの脅威が、従来の脅威対象外の機器に拡張される可能性について実証する。機器の等価回路網の不正な回路改変により特定周波数に対する機器のイミュニティが制御され、電磁波が機器内部に誘導されやすい状態が生成される可能性について検討する。また、機器外部から照射された情報を含む電磁波による情報注入の実行可能性について示す。そして、不正な回路改変と意図的な照射電磁波による情報注入の脅威のメカニズムを明らかにし、その

メカニズムに基づく対策技術を提案する。

4 章では、本論文をまとめる。

# 第 2 章　意図的な照射電磁波を用いた能動的なセンシングによるエミッションの制御が引き起こす脅威

## 2.1　緒言

本章では、意図的な照射電磁波を用いた能動的なセンシングによるエミッションの制御が引き起こす脅威が、従来の電磁情報漏えいの脅威対象外の機器に拡張される可能性について実証する。 本論文では、「電磁波を用いた能動的なセンシングにより生ずる信号 (以下、Echo) を介した情報漏えいの脅威」を Echo TEMPEST と呼び、本脅威の実行可能性について民生機器を用いて実証する。

2.2 節では、機器内部で処理・伝送される情報を能動的にセンシングするために着目する回路の電気的な特性や状態の変化について述べる。そして、その変化を機器外部から取得する能動的なセンシングによる情報漏えいのメカニズムについて述べる。2.3 節では、Echo TEMPEST の対象となる IC 内部の出力バッファを抽出した実験系を作成する。そして、当該回路に伝搬した電磁波が出力信号の値に応じて異なる振幅で反射することを計測し、Echo TEMPEST のメカニズムに基づいて情報が取得可能であることを示す。2.4 節では、機器のエミッションレベルが低いため従来の電磁情報漏えいの脅威の対象外となっていた機器に対し、Echo TEMPEST が実行される可能性を示す。また、能動的なセンシングに用いる電磁波の照射強度に応じて、情報を取得可能な距離が制御される可能性を示す。2.5 節では、本章で提案した Echo TEMPEST に対抗する対策技術を Echo の生成の困難化および Echo からの情報の取得の困難化の 2 つの観点からの対策技術について検討する。

## 2.2　Echo TEMPEST による IC の伝送情報の取得手法

本節では、機器内部で処理・伝送される情報を能動的にセンシングするために着目する回路の電気的な特性や状態の変化ついて述べる。そして、その特性や状態の変化を機器外部から取得するための能動的なセンシングにより生ずる Echo について説明する。

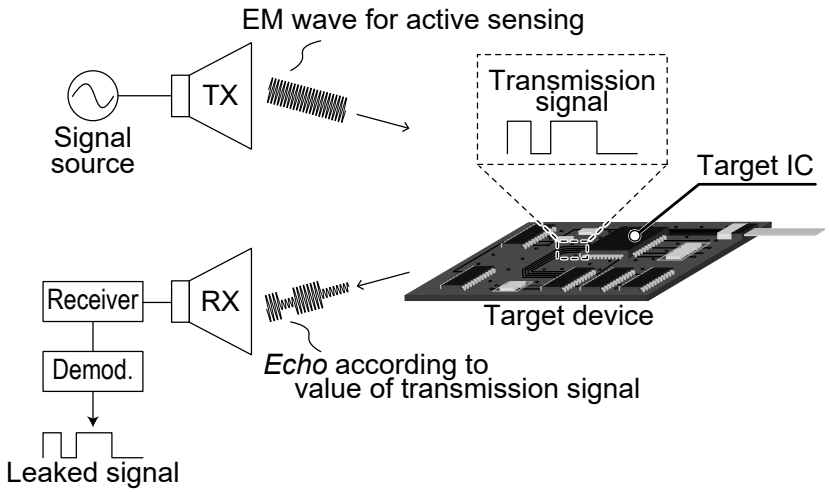


図 2.1. 機器に対する Echo TEMPEST の概念図

情報漏えいのターゲットとなる情報は、IC 内部で処理された後に IC の入出力 (I/O: Input / Output) 回路を介して電気信号として伝送される。このとき、IC の I/O 回路には、IC 間の電流値や電圧値の整合や送受信する電気信号の同期、ノイズ耐性の向上などの目的で出力バッファが設けられており [60, 61]、出力信号は出力バッファを介して IC 外部に伝送される。ここで出力バッファに着目すると、出力信号の値に応じてトランジスタのスイッチング状態が変化するため、IC 外部で計測される IC の出力端の反射係数は出力信号の値に応じて変化する。このように IC で処理された情報に応じて、能動素子やそれらが組み合わさった回路の内部状態が電気的な特性を変化させる。Echo TEMPEST では、機器外部から意図的に電磁波を照射し、機器内部の電気的な特性の変化によって生じる Echo の振幅の変化を計測することで IC の出力信号の値を推定する。

図 2.1 は Echo TEMPEST が実行される流れを示しており、意図的な電磁波の照射により機器内部で生じた Echo を受信することで IC が処理・伝送する情報が取得可能となる。Echo は、機器外部から照射された電磁波を受信する機器の非意図的なアンテナと機器内部に伝搬した電磁波を反射・透過する回路構造によって生ずる（図 2.2)。

機器外部で意図的に照射された電磁波は、機器に接続された線路や PCB 上の伝

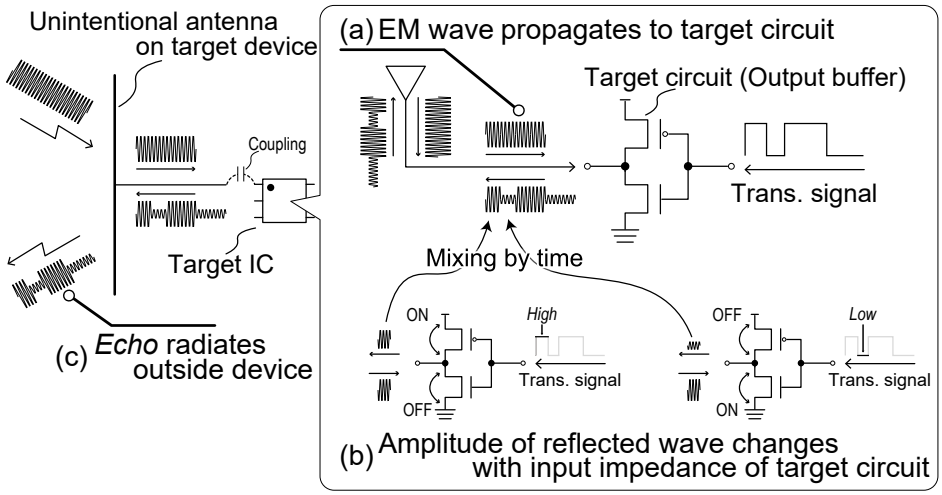


図 2.2. 能動的なセンシングによって Echo が生成されるプロセス

送線路等の非意図的なアンテナより機器内部に伝搬し、「情報漏えいのターゲットとなる情報を処理・伝送する回路（以下、ターゲット回路）」まで到達する（図 2.2 (a)）。続いて、ターゲット回路まで伝搬した電磁波は処理・伝送される情報に依存して時間的に変化し、ターゲット回路の反射係数に応じてその一部は回路内部に透過し、一部が反射する（図 2.2 (b)）。そして、反射した電磁波は、機器内部へ電磁波が伝搬した際の逆向きの経路を辿り、機器外部に Echo として放射される。放射した Echo は、ターゲット回路の反射係数の時間変化に伴い振幅が変動するため、意図的に照射された電磁波を搬送波とし、ターゲット回路の出力信号を被変調波とする振幅変調波として捉えることができる（図 2.2 (c)）。

以上より、ターゲット回路から伝送される出力信号の値が Echo を介して取得され、これに基づき IC が処理・伝送する情報の推定が可能となる。さらに、機器外部に放射される Echo の強度は、能動的なセンシングに使用する電磁波の照射強度と比例の関係にある。そのため、ターゲット回路を構成する素子や回路が動作可能な範囲で照射強度を変化させることにより、Echo の放射強度を制御することが可能となる。

## 2.3　単純な実験系による Echo TEMPEST の実証

本節では、Echo TEMPEST のターゲット回路となる I/O 回路の出力バッファを抽出した実験系を作成し、2.2 節で述べたメカニズムに基づいて Echo が生成され Echo TEMPEST が成立することを実証する。

はじめに、ターゲット回路となる I/O 回路と同等の構造を有するインバータ素子を用いた実験系を作成し、インバータ素子の出力信号の値に応じた電気的な特性の変化を計測する。続いて、計測結果より Echo が発生すると予想される周波数を選択し、当該周波数の電磁波をインバータ素子に印加する。そして、インバータ素子に印加された電磁波が出力信号の値に応じて異なる振幅で反射することを計測し、インバータ素子の出力信号の値が取得可能であることを示す。

### 2.3.1　インバータ素子を用いた実験系の作成

本実験では、Echo TEMPEST のターゲット回路となる I/O 回路の出力バッファと同等の構造を有するインバータ素子を用いてテストデバイス (DUT: Device Under Test) を作成した。図 2.3 に DUT の回路図と実装レイアウトを示す。

図 2.3 (a) は DUT の回路図である。DUT は、インバータ素子 (NXP, 74HCU04PW) とノイズによる影響の低減のための 0.1 $\mu$F のバイパスコンデンサ (BC: Bypass Capacitor) で構成され、信号の入出力端として SMA (Sub Miniature Type A) コネクタとインバータ素子の電源入力端を実装した。本実験で使用しないインバータ素子の入力端は、インバータ素子の発振を防ぐため全てグランド (GND) に接地した。図 2.3 (b) は、図 2.3 (a) に示した回路の実装レイアウトである。FR-4 (Flame Retardant 4) を基材とする基板上に線路幅 0.4 mm の配線で SMA コネクタとインバータ素子の入出力端を接続した。基板両面の GND は直径 1 mm のビアで共通化した。ただし、本実験ではインバータ素子の出力信号の値に応じた反射係数の変化を広帯域で計測することを目的としたため、特定の周波数における基板上の配線のインピーダンスは整合していない。

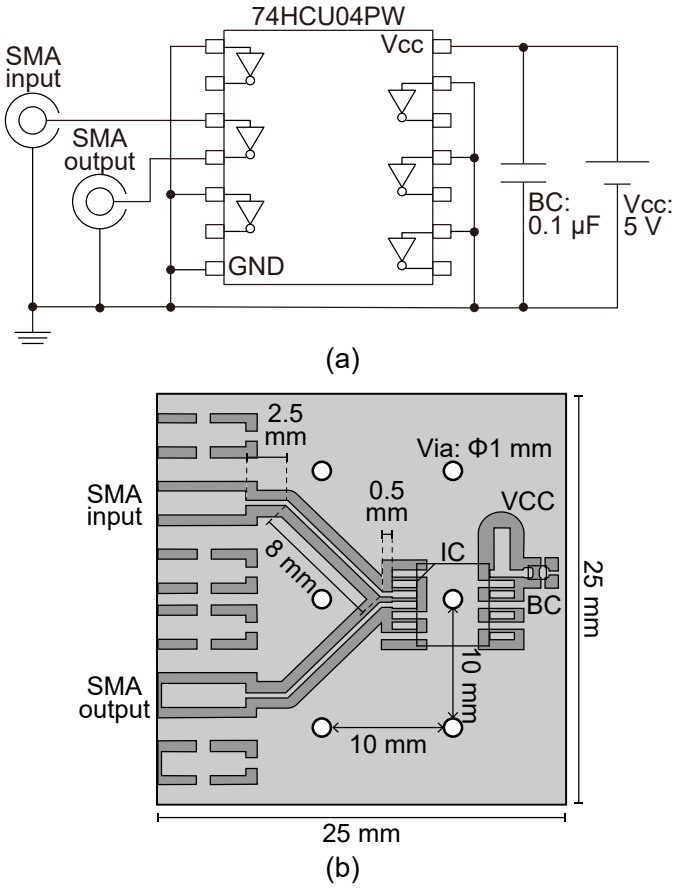


図 2.3. DUT の回路図と実装レイアウト

### 2.3.2 インバータ素子の出力信号の値に応じた反射係数の変化の計測

図 2.4 と 表 2.1 にインバータ素子の出力信号の値に応じた反射係数の変化の計測環境とパラメタを示す。

本実験では、DUT に実装したインバータ素子の出力信号の値に応じた電気的な特性の変化の計測系として、方向性結合器を接続した周波数分析器と周波数分析器のトラッキングジェネレータ機能を用いた。DUT の電源は 5 V に設定した安定化電源とし、入力は任意波形発生器、出力は方向性結合器の入力端にそれぞれ接続

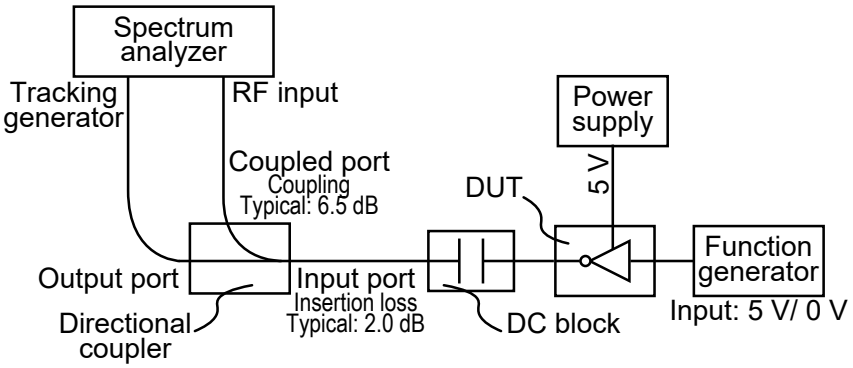


図 2.4. インバータ素子の出力信号の値に応じた反射係数の計測環境

表 2.1. インバータ素子の出力信号の値に応じた反射係数の計測環境とパラメタ

| 計測環境 | |
|---|---|
| 周波数分析器 | Rohde & Schwarz, FSV |
| 方向性結合器 | Mini-Circuits, ZFDC-6-23-S+ |
| DC ブロック | Mini-Circuits, BLK-18-S+ |
| 安定化電源 | Texio, PA18-2B |
| 任意信号生成器 | NF, WF1968 |
| DUT インバータ IC | NXP, 74HCU04PW |
| DUT 基板 | Sanhayato, No. 35R |
| **計測パラメタ** | |
| DUT 入力信号 | 0, 5 V |
| RBW | 1 MHz |
| 周波数分析器 掃引点数 | 32001 points |
| 信号生成器 出力電力 | −20 dBm |
| 印加電磁波の周波数 | 20 - 2000 MHz |

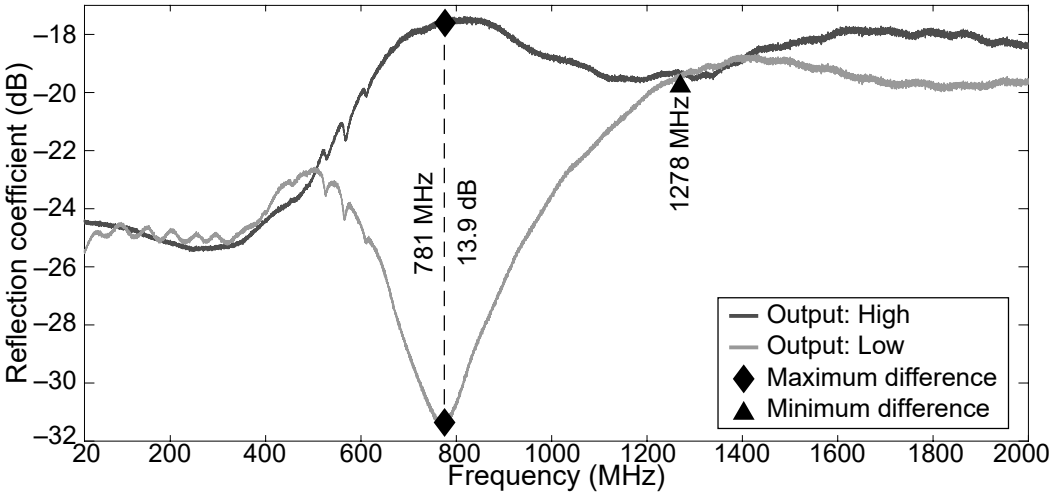


図 2.5. インバータ素子の出力信号の値に応じた反射係数の計測結果

した。このとき、周波数分析器やトラッキングジェネレータへの直流 (DC: Direct Current) 信号の流入を防ぐため、方向性結合器と DUT の間に DC ブロックを挿入して計測した。

続いて、計測パラメタについて説明する。本実験では、インバータ素子の出力信号の値の変化に応じた過渡的な応答を排除して計測するため、DUT への入力信号はインバータ素子における High (5 V) と Low (0 V) の 2 種類とした。周波数分析器が計測する周波数帯域は、方向性結合器が対応する周波数帯域である 20 – 2000 MHz とし、周波数分析器の RBW を 1 MHz、掃引点数を 32001 ポイント、トラッキングジェネレータの出力電力を −20 dBm とした。

図 2.5 にトラッキングジェネレータの入射波と周波数分析器で計測した反射波より算出したインバータ素子の出力信号の値に応じた反射係数の結果を示す。インバータ素子の出力信号の値に応じた反射係数の差は、781 MHz で最大となり、1278 MHz で最小となることが確認された。

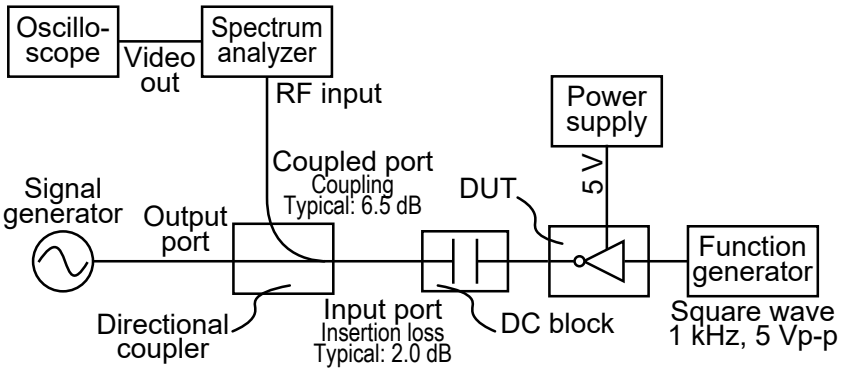


図 2.6. インバータ素子の出力信号の値に応じた反射係数の変化により生成される Echo の計測環境

### 2.3.3 インバータ素子の反射係数の変化に応じた Echo 生成の実証実験

ターゲット回路となるインバータ素子の出力信号の値に応じた反射係数の変化によって Echo が生成され、インバータ素子の出力信号の値が取得可能であることを示す。図 2.6 と表 2.2 に計測環境とパラメタを示す。

本実験では、インバータ素子の出力端に低損失で電磁波を伝搬させるため、信号発生器で生成した電磁波を同軸ケーブル経由で DUT の出力端となる SMA コネクタに入力し、インバータ素子で発生した Echo は方向性結合器を介して周波数分析器で計測した。計測した Echo は周波数分析器に搭載されたゼロスパンモードにより振幅復調され、ビデオ出力によりオシロスコープに入力した。インバータ素子の出力端に伝搬させる電磁波の周波数は、前節の計測において出力信号の値に応じた反射係数の差が最大となった 781 MHz と、出力信号の値に応じた反射係数の差が最小となった 1278 MHz を選択した。このとき、インバータ素子の入力端には任意波形発生器から 1 kHz、5 $V_{P-P}$ の方形波を入力し、その出力信号が取得可能であることを実証した。

図 2.7 にインバータ素子の出力信号と 781 MHz と 1278 MHz の電磁波をインバータ素子の出力端に伝搬させた際に計測された Echo の振幅復調波形を示す。

図 2.7 (a) にインバータ素子の出力信号を計測した波形であり、5 $V_{P-P}$ の 1 kHz

表 2.2. インバータ素子による Echo 生成の計測環境とパラメタ

| 計測環境 | |
|---|---|
| 周波数分析器 | Rohde & Schwarz, FSV |
| 方向性結合器 | Mini-Circuits, ZFDC-6-23-S+ |
| DC ブロック | Mini-Circuits, BLK-18-S+ |
| 安定化電源 | Texio, PA18-2B |
| 任意信号生成器 | NF, WF1968 |
| 信号生成器 | Keysight, N5181 |
| DUT インバータ IC | NXP, 74HCU04PW |
| DUT 基板 | Sanhayato, No. 35R |
| **計測パラメタ** | |
| DUT 入力信号 | 1 kHz, 5 $V_{p-p}$, 2.5 $V_{offset}$ |
| RBW | 5 MHz |
| 周波数分析器 掃引点数 | 32001 points |
| 信号生成器 出力電力 | −30 dBm |
| 印加電磁波の周波数 | 781, 1278 MHz |

の方形波を示す。図 2.7 (b) に 781 MHz の電磁波をインバータ素子の出力端に伝搬させた際に Echo として計測された信号を振幅復調した結果を示す。インバータ素子の出力が High の場合には Echo の振幅が大きくなり、出力が Low の場合には Echo の振幅が小さくなっていることが確認された。続いて、図 2.7 (c) に 1278 MHz の電磁波をインバータ素子の出力端に伝搬させた際に Echo として計測された信号を振幅復調した結果を示す。図 2.7 (b) で計測されたような Echo の振幅変動は確認されず、インバータ素子の出力信号の値にかかわらず振幅が一定となっていることが確認された。図 2.7 (d) に電磁波をインバータ素子の出力端に伝搬させていない場合の 781 MHz で計測された信号を振幅復調した結果を示す。図 2.7 (b) のような Echo の生成は確認されない。

図 2.7 では図 2.5 でインバータ素子の出力信号の値に応じた反射係数が最大・最

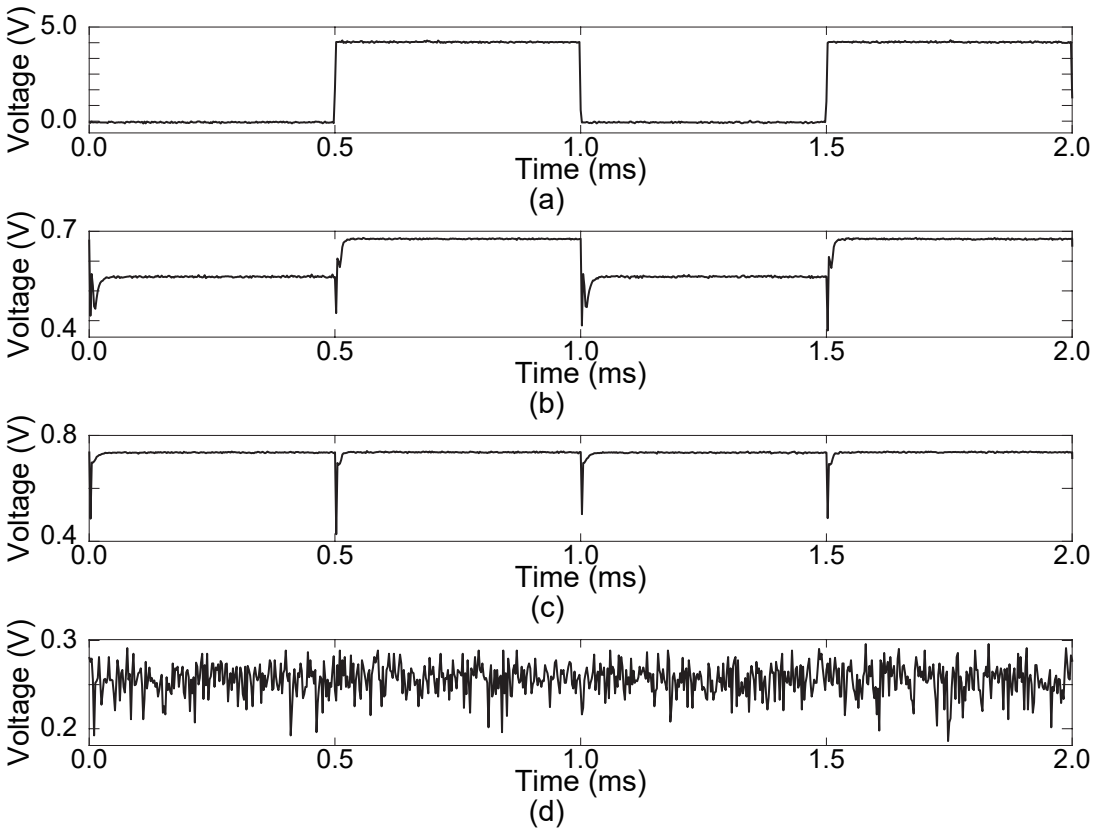


図 2.7. 電磁波をインバータ素子の出力端に伝搬させた際に Echo として計測された信号を振幅復調した結果

小となった周波数を伝搬させた場合の計測結果のみを示しているが、インバータ素子の出力信号の値に応じて反射係数に差が生じたその他の周波数 (図 2.5、約 510 – 1200 MHz) を伝搬させた場合も、出力信号の値に応じて振幅が変動した Echo が発生することが確認された。

以上の結果より、ターゲット回路と同等の構造を有するインバータ素子の出力信号の値に応じた反射係数の変化によって Echo が生成されることが確認された。そして、Echo の振幅復調によりインバータ素子の出力信号の値が取得可能であることが確認され、Echo TEMPEST が成立することが実証された。

図 2.7 (b), (c) の 0.5, 1.0, 1.5 ms で計測された立ち下がりの信号は、インバータ素子の出力信号の変化のタイミングで生じる過渡的な反射係数の変化によるものである。そのため、この立ち下がり信号からもインバータ素子の出力信号の電圧変動

のタイミングの推定が可能である。本節では、インバータ素子の出力信号の値に応じた反射係数の変化により生じた Echo の振幅変動に着目しているため議論の対象外とした。

## 2.4 民生機器を用いた Echo TEMPEST の実証

本節では、民生機器に対しても Echo TEMPEST が成立することを示す。

はじめに、Echo TEMPEST を成立させ、IC 間を伝送される情報を取得する系について述べる。続いて、Echo TEMPEST の対象とする 2 種類の機器とその伝送信号について説明する。そして、2 種類の機器を用いて、Echo TEMPEST の実行可能性と照射強度に応じて IC 間を伝送される情報が取得可能な距離が制御できることを示す。

### 2.4.1 Echo TEMPEST により IC 間の伝送情報を取得する系の構築

Echo TEMPEST による IC 間の伝送情報の取得では、ターゲット回路を含んだ機器に電磁波を照射する系とターゲット回路から反射した Echo を受信し振幅復調する系が必要となる。Echo TEMPEST を実行する送受信システムを図 2.8 に示す。

図 2.8 (a) に示す送信機 (TX) 系では、機器内部のターゲット回路まで低損失で伝搬しやすい周波数は未知のため、信号発生器を用いて電磁波の周波数と振幅を掃引しながら電磁波を照射する。図 2.8 (b) に示す受信機 (RX) 系では、ターゲット回路で生成され機器外部に放射した Echo を受信し SDR で処理される。SDR に入力された信号は、スーパーヘテロダイン方式により中間周波数信号に変換され、その信号を ADC (Analog Digital Converter) によりサンプリングし、得られたデジタル信号を包絡線検波することで振幅復調される。

本実験で使用した TX / RX 系はパーソナルコンピュータ (PC: Personal Computer) によって制御され、照射する周波数の掃引に応じて SDR の中心周波数を同期させた。このとき、SDR で計測された Echo の振幅復調波の振幅値が最も高くな

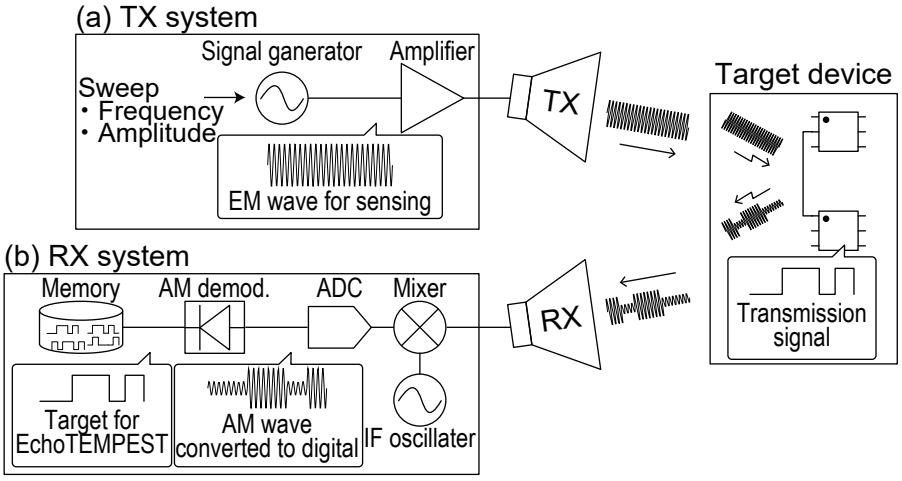


図 2.8. Echo TEMPEST を実行する送受信システム

る周波数が、機器内部のターゲット回路と TX / RX 系の間で電磁波が伝搬しやすい周波数かつターゲット回路の出力信号に応じた反射係数の差が最大となる周波数であると仮定し、IC 間を伝送される情報を取得した。

### 2.4.2 Echo TEMPEST の対象とする機器とその伝送信号

本実験では、従来の電磁情報漏えいのターゲットとして一般的に用いられるシリアル通信方式を対象として用いた。シリアル通信方式のうち、IC が出力する信号が異なる機器として、シングルエンド信号を出力する機器と差動信号を出力する機器を用いた。具体的には、シングルエンド信号を出力する機器として UART (Universal Asynchronous Receiver / Transmitter) モジュールと差動信号を出力する機器として USB (Universal Serial Bus) キーボードを使用した。

A) UART モジュール

UART は、TX と RX を伝送線路で接続することにより動作する。UART の伝送線路にはクロック (CLK: Clock) 信号が存在せず、TX / RX 間で CLK を共有していない [62]。そのため、TX / RX 間でのビットタイミングの同期のため、ボーレートを事前に共有すると共に、データビットの前後にスタートビットとストップビットを付加することでデータビットの開始と終了を表す。このとき、データビッ

表 2.3. UART モジュールの伝送線路とパラメタ

| UART モジュールと伝送線路 | |
|---|---|
| UART モジュール | Cypress, CY7C65211-24LTXI |
| 伝送線路 | 2 芯シールドケーブル |
| 伝送線路長 | 1 m |
| **UART モジュールのパラメタ** | |
| 伝送信号論理 | 正論理 |
| 伝送信号 | 0, 5 V |
| ボーレート | 115.2 kb/s |
| スタートビット | 1 bit |
| データビット | 8 bit |
| ストップビット | 1 bit |
| パリティビット | なし |

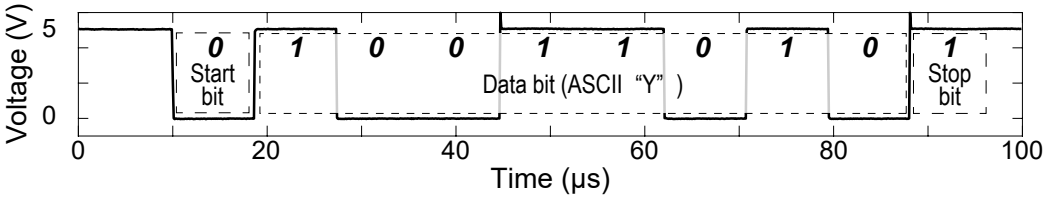


図 2.9. UART モジュールで“Y”が伝送される際に計測された伝送信号

トはデータの最下位ビットを先頭として伝送される。データのエラー検出のため、データビットの末尾にパリティビットが挿入される場合もある。

本実験で使用した UART モジュール間の伝送線路は、実験系の簡単化のため信号線と GND 線の 2 本で接続された単向通信とし、伝送線路長は 1 m とした。また、UART の伝送信号のパラメタとして、データビット数は 8 bit、各 1 bit のスタートビットとストップビットが付加された合計 10 bit を 1 フレームとした。UART のボーレートは一般的に利用される 115.2 kb/s とし、伝送信号が High および無通

信時は 5 V、伝送信号が Low の場合は 0 V として設定した（表 2.3）。

図 2.9 に使用した UART モジュールで “Y” のデータを伝送した際にオシロスコープで計測された波形を示す。図 2.9 ではスタートビット、最下位ビットを先頭としたデータビット、ストップビットを含んだ “0100110101” の電圧変動が確認された。

B) USB キーボード

USB キーボードは一般的に、伝送信号が 1.5 Mb/s である USB 2.0 Low-speed 規格 [63] が使用されている。USB キーボードの伝送線路は、$V_{BUS}$ と GND、差動信号である D+, D− で構成され、D− がプルアップ抵抗により $V_{BUS}$ に接続されている。

USB キーボードから PC へ入力情報が伝送される場合、はじめに PC から USB キーボードにトークンパケットと呼ばれる信号が伝送され、続いて USB キーボードから PC に入力情報がデータパケットとして伝送される。トークンパケットは、データの伝送元のデバイスに応じたアドレスを含むため、接続毎に異なるアドレスが付加される。各パケットは、複数のパケットフィールドで構成されており、各パケットの最後には EOP (End-of-Packet) を表すため、D+, D− 両者とも伝送信号が Low となる。これらの伝送信号は、フレームと呼ばれる単位で 1 ms 周期で伝送され、NRZI (Non Return to Zero Inversion) 方式で符号化されている。NRZI 方式は、“0” のデータが伝送される場合は D+, D-の High / Low の状態を反転させ、“1” のデータが伝送される場合は D+, D− の High / Low の状態を保持する。

本実験では、USB キーボードへの入力情報の漏えいを確認すると共に計測環境への侵襲を防ぎ実験の再現性を担保するため、入力情報を表す伝送信号と PC – USB キーボード間で定常的に伝送される信号の 2 種類を計測対象とした。図 2.10 に PC と USB キーボードを接続し “a” が入力された際に計測された入力情報を表す伝送信号、図 2.11 に USB キーボードに入力を与えなかった際に計測された PC – USB キーボード間で定常的に伝送される信号の例を示す。

図 2.10 では、PC から USB キーボードに対して伝送されるトークンパケット（図 2.10 (a)）と、USB キーボードから PC に対して伝送される “a” のキーコードの最下位ビットを先頭とする “0x04” のデータパケット（図 2.10 (b)）が確認された。

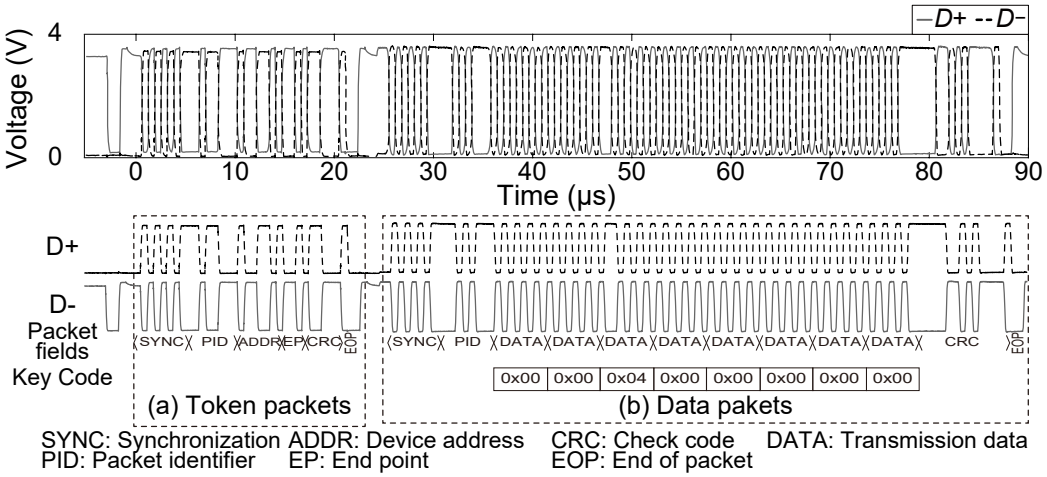


図 2.10. USB キーボードで“a”が入力された際に計測された入力情報を表す伝送信号

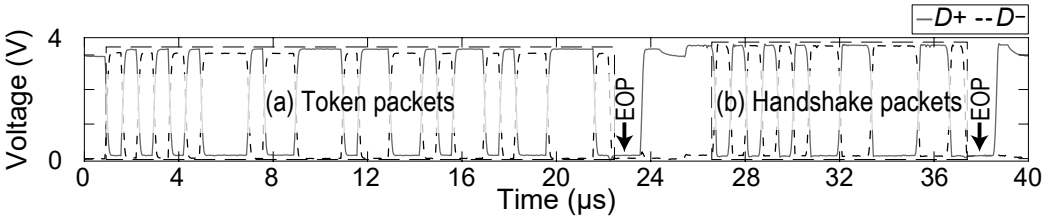


図 2.11. USB キーボードに入力を与えなかった際に計測された PC – USB キーボード間の定常的な伝送信号

続いて、図 2.11 では、PC から USB キーボードに伝送されたトークンパケット（図 2.11 (a)）と、USB キーボードから PC に伝送されたハンドシェイクパケット（図 2.11 (b)）が確認された。ハンドシェイクパケットは、図 2.10 (b) のデータパケットと同様に、USB キーボード内部の IC で処理された情報が I/O 回路を介して出力されている。そのため、ハンドシェイクパケットを表す伝送信号が Echo TEMPEST により取得することができれば、USB キーボードの入力情報も同様に取得可能であると見なすことができる。

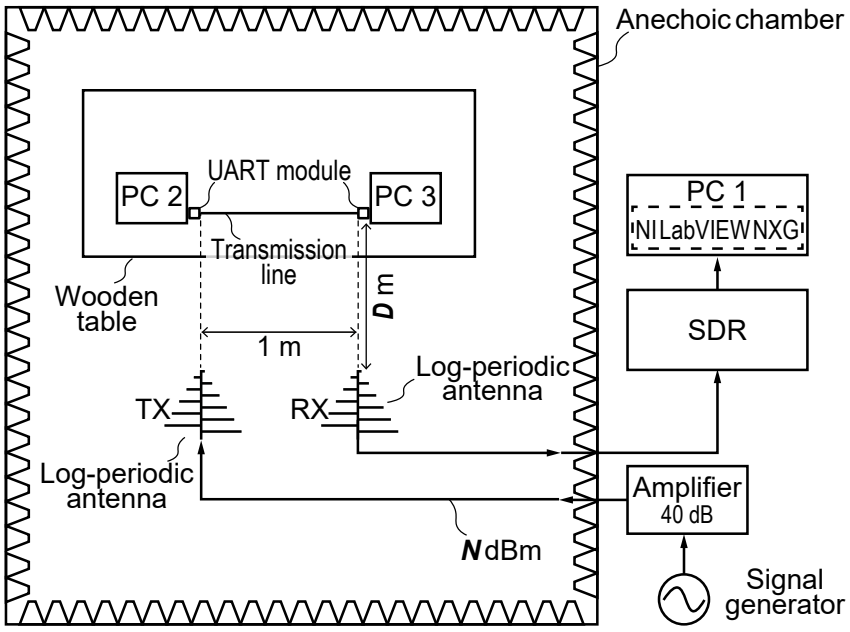


図 2.12. UART モジュールに対する Echo TEMPEST の計測環境

### 2.4.3 電磁波の照射強度に応じたエミッション制御の可能性の実証実験

本実験では、シングルエンド信号を伝送する UART モジュールの伝送情報が Echo TEMPEST により取得可能であることを示す。図 2.12 に計測環境、表 2.4 に実験に使用した計測環境とパラメタを示す。

計測対象となる UART モジュールは、電波暗室内の高さ 75 cm の木製テーブル上に設置した 2 台の PC の USB ポートに接続した。TX / RX アンテナには 2 つのログペリオディックアンテナを使用した。TX / RX アンテナは、UART モジュールの伝送線路と同じ高さとし、UART モジュール間の伝送線路から 1, 2, 3m となる $\boldsymbol{D}$ m の距離に設置した。UART モジュールに照射する電磁波は信号生成器により生成し、高周波増幅器を介して 0 – 30 dBm まで変化させ（$\boldsymbol{N}$ dBm)、TX アンテナから照射した。照射する電磁波の周波数は、波長が UART モジュール間の伝送線路の長さと同程度となる 300 MHz から送受信アンテナの周波数帯域の上限と

表 2.4. UART モジュールに対する Echo TEMPEST の計測環境とパラメタ

| 計測環境 | |
|---|---|
| SDR | Ettus Research, USRP X310 |
| SDR ドーターボード | Ettus Research, TwinRX 10-6000 MHz |
| SDR 制御ソフトウェア | NI, LabVIEW NXG 5.0 |
| 信号生成器 | Rohde & Schwarz, SMA100B |
| 高周波増幅器 | R&K, A000110-4040-R |
| TX / RX アンテナ | Ettus Research, LP0410 |
| **計測パラメタ** | |
| SDR サンプリングレート | 20 MS/s |
| 周波数 | 463 MHz |
| TX ゲイン ($\boldsymbol{N}$) | 0 – 30 dBm |
| USB キーボードと アンテナ間距離 ($\boldsymbol{D}$) | 1, 2, 3 m |
| SDR RX ゲイン | 60 dB |

なる 1000 MHz までを掃引した事前の評価において、Echo を振幅復調した波形の振幅が最も大きく計測された 463 MHz を選択した。電磁波の照射により UART モジュール内で生成され機器外部に放射した Echo は、RX アンテナを介して受信ゲインを 60 dB に固定した SDR で処理される。SDR のサンプリングレートは、サンプリング定理に従い UART のボーレートより十分に大きい 20 MS/s とした。

図 2.13 に UART モジュールに対する Echo TEMPEST の計測結果を示す。図 2.13(a) は UART モジュールの伝送線路をオシロスコープによりタッピングし、“Y” の ASCII (American Standard Code for Information Interchange) コードを伝送した際に計測された波形である。図 2.13 (b) – (c) は、送受信アンテナから UART モジュールまでの距離を $\boldsymbol{D}$ m とし、463 MHz の電磁波を $\boldsymbol{N}$ dBm で照射した際に計測された信号を振幅復調した結果である。それぞれの波形は、400 kHz のローパスフィルタ (LPF: Low-Pass Filter) を適用した後に正規化した。図 2.13

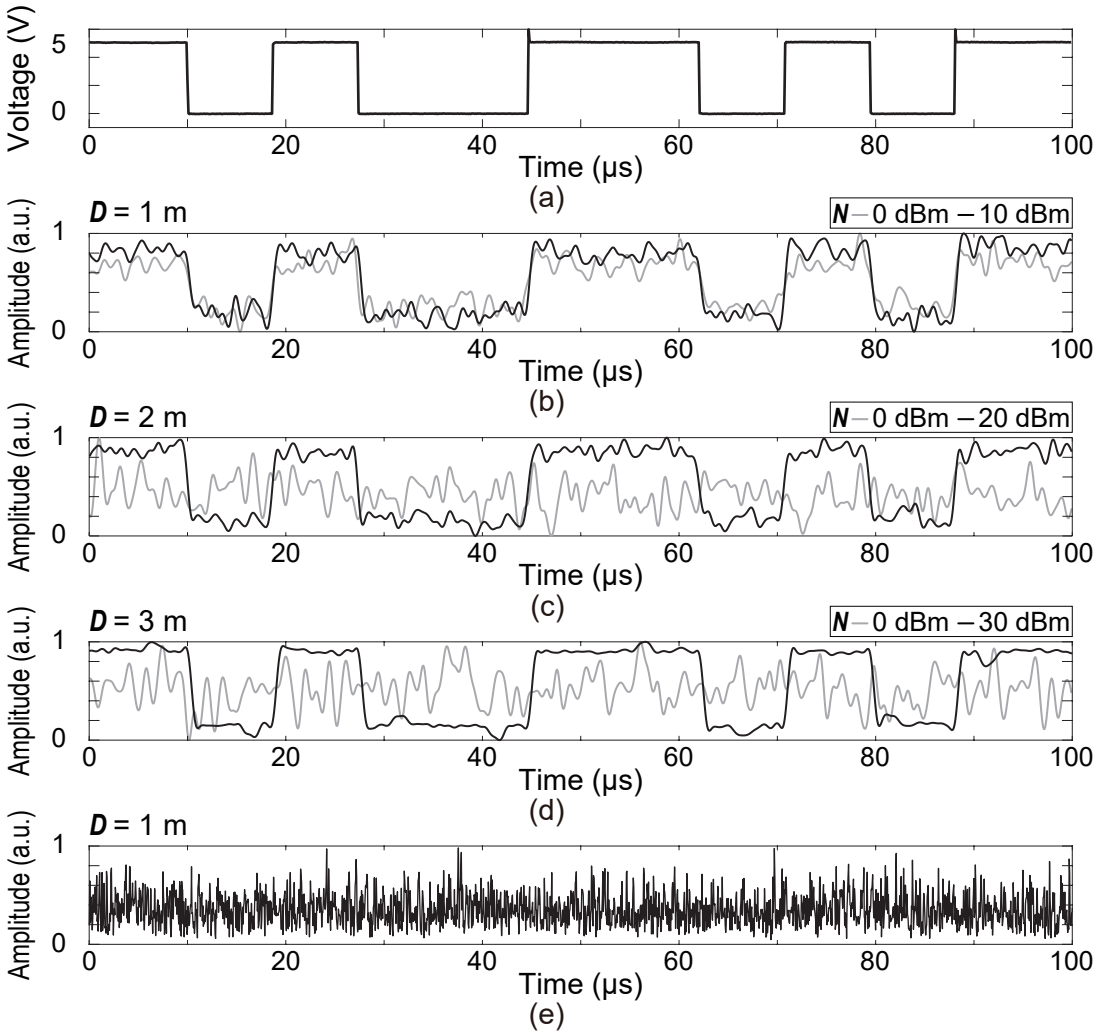


図 2.13. UART モジュールに対する Echo TEMPEST の計測結果

(b) は、距離 $\boldsymbol{D}$ を 1 m とし、電磁波の照射強度 $\boldsymbol{N}$ を 0 dBm と 10 dBm に設定した際の計測結果である。いずれの照射強度でも図 2.13 (a) と同等の電圧変動が復元されることが確認された。図 2.13 (c) と図 2.13 (d) は、距離 $\boldsymbol{D}$ を 2 m と 3 m とした際の計測結果である。いずれも、電磁波の照射強度 $\boldsymbol{N}$ が 0 dBm の場合は、ノイズの影響が大きく図 2.13 (a) のような電圧変動が確認されない。一方、電磁波の照射強度 $\boldsymbol{N}$ を 20 dBm や 30 dBm に増加させることで図 2.13 (a) と同等の電圧変動が復元されることが確認された。図 2.13 (e) は電磁波を照射せず、距離 $\boldsymbol{D}$ を

1 m とした際に従来の電磁情報漏えいの手法で計測された波形である。漏えい信号の放射強度が弱く、図 2.13 (a) と同等の電圧変動を復元することが困難であることが確認された。

以上の結果より、従来の電磁情報漏えい手法では復元が困難であった漏えい電磁波の放射強度が弱い機器に対する能動的なセンシングによって、UART モジュールが伝送する情報が漏えいすることが確認され、Echo TEMPEST が実行可能であることが示された。また、電磁波の照射強度に応じて UART モジュールが伝送した情報を取得できる距離も制御できることが確認された。本節では、UART モジュールより“Y”の ASCII コードが伝送された際の計測結果のみを示したが、同様の計測環境において、異なる ASCII コードが伝送された場合にも Echo TEMPEST が成立することを確認している。

### 2.4.4 USB キーボードの入力情報に対する Echo TEMPEST の実証実験

本実験では、差動信号を伝送する USB キーボードの入力情報が Echo TEMPEST により取得可能であることを示す。図 2.14 に計測環境、表 2.5 に使用した計測環境とパラメタを示す。

計測対象となる USB キーボードは電波暗室内の高さ 75 cm の木製テーブル上に設置し、USB アイソレータを介して電波暗室外部の PC に接続した。USB アイソレータは、PC とキーボードの電源および GND を分離し、安定化電源よりキーボードに電源を供給することで PC からの伝導ノイズの影響を低減している。本実験では、USB キーボードの入力情報が取得可能であることを実証するため、USB キーボードにキー入力を与える。そのため、評価者によって周辺の電磁環境が侵襲されアンテナを用いた計測では実験の再現性が低下する可能性がある。そこで、本実験では、インジェクションプローブとカレントプローブを使用し、それぞれを USB キーボードのキーボード部から 20 cm と 5 cm の位置に設置し電磁波の印加と Echo を計測した。電磁波は信号生成器により生成し、高周波増幅器を介して 10 dBm の強度でインジェクションプローブに印加した。印加する電磁波の周波数は、波長が USB キーボードの伝送線路の長さより長くなる 100 MHz から高周波

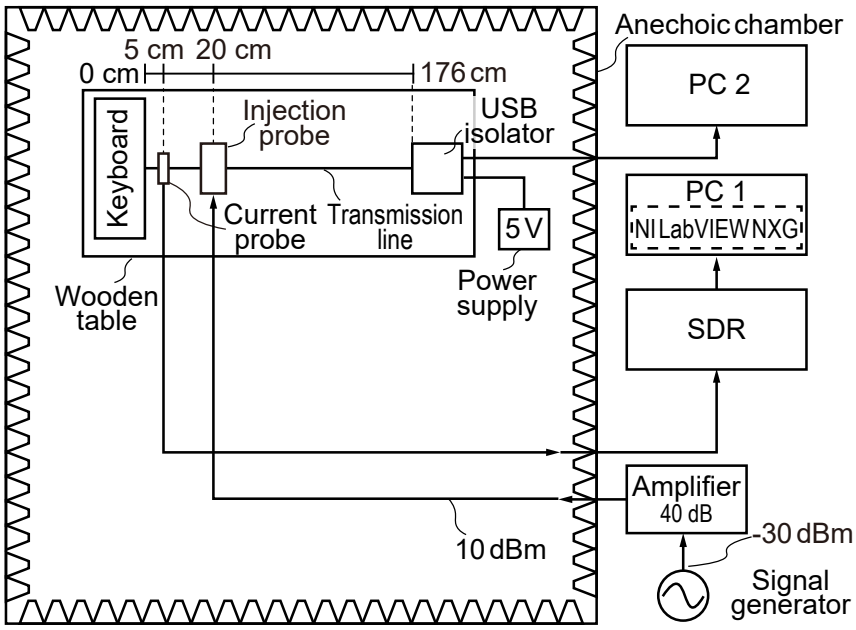


図 2.14. USB キーボードの入力情報に対する Echo TEMPEST の計測環境

増幅器の周波数帯域の上限となる 1000 MHz までを掃引した事前の評価において、Echo を振幅復調した波形の振幅が最も大きく計測された 559 MHz を選択した。電磁波の印加により USB キーボード内で生成され機器外部に放射した Echo は、カレントプローブを介して受信ゲインを 60 dB に固定した SDR で処理される。SDR のサンプリングレートは、サンプリング定理に従い USB キーボードの伝送速度より十分に大きい 20 MS/s とした。

図 2.15 に USB キーボードの入力情報に対する Echo TEMPEST の計測結果を示す。図 2.15 (a) は、事前にオシロスコープを用いて USB キーボードと PC 間の USB アイソレータ上の計測ポートをタッピングして計測された波形である。本実験では、USB キーボードの入力情報が取得できることを実証するため、“a” のキーを入力し入力情報が含まれるデータパケットを抽出し比較した。この波形より、“a” のキーコードを示す“0x04”が伝送されていることが確認された。図 2.15 (b) は、559 MHz の電磁波をインジェクションプローブより 10 dBm の強度で印加した際にカレントプローブを介して SDR が受信した波形を示す。この波形は、振幅復調

表 2.5. USB キーボードの入力情報に対する Echo TEMPEST の計測環境とパラメタ

| 計測環境 | |
|---|---|
| SDR | Ettus Research, USRP X310 |
| SDR ドーターボード | Ettus Research, TwinRX 10-6000 MHz |
| SDR 制御ソフトウェア | NI, LabVIEW NXG 5.0 |
| 信号生成器 | Rohde & Schwarz, SMA100B |
| 高周波増幅器 | R&K, A000110-4040-R |
| インジェクションプローブ | FCC, F-140 |
| カレントプローブ | FCC, F-2000 |
| USB キーボード | HP, SK-2025 |
| USB アイソレータ | Analog Devices, EVAL-ADuM4160EBZ |
| USB アイソレータ電源 | Texio, PA18-2B |
| **計測パラメタ** | |
| SDR サンプリングレート | 20 MS/s |
| 周波数 | 559 MHz |
| TX ゲイン | 10 dBm |
| SDR RX ゲイン | 60 dB |

した後に 4 MHz の LPF を適用し振幅を正規化している。図 2.15 (c) は、図 2.15 (b) で得られた振幅復調波形を信号処理により 2 値化した結果を示す。伝送信号の High / Low が変化する際に Echo の振幅が変化することに着目し、微分した振幅復調波形の極値および NRZI 符号方式に従って伝送信号を推定した。この波形より、図 2.15 (a) と同等の電圧変動が確認され“a”のキーコードを示す“0x04”が復元されていることが確認された。一方、図 2.15 (d) は、電磁波の印加を停止し USB キーボードから放射した電磁波を従来の電磁情報漏えいの手法で計測された波形を示す。伝送信号の電圧変動を復元することが困難であることが確認された。

以上の結果より、従来の電磁情報漏えい手法では復元が困難であった漏えい電磁波の放射強度が弱い機器に対する能動的なセンシングによって、差動伝送方式であ

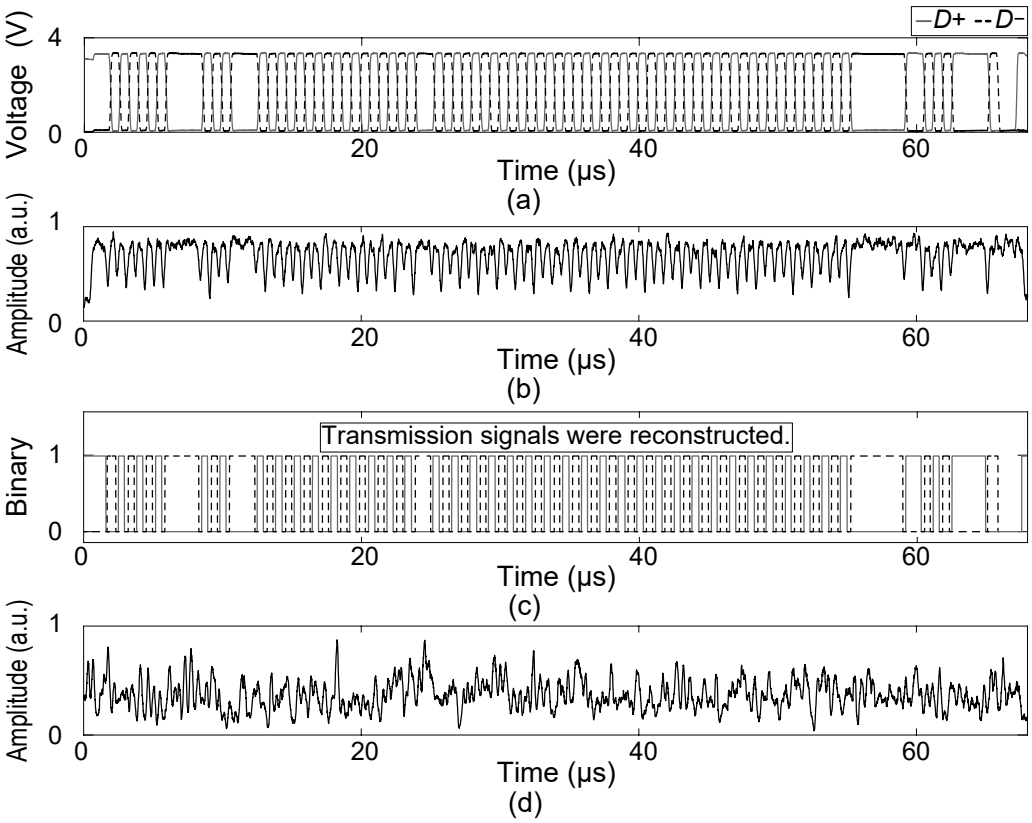


図 2.15. USB キーボードの入力情報に対する Echo TEMPEST の計測結果

る USB キーボードの入力情報を取得できることが確認された。本節では、“a”の入力情報のみを対象としたが、他の入力情報についても Echo TEMPEST により情報が取得できることを確認している。

表 2.6. Echo TEMPEST の実証に使用した USB キーボード

| No. | 製造元, モデル名 | 伝送線路長 ($\boldsymbol{L}$) [cm] |
|---|---|---|
| 1 | N/A, NBO109U01BK1 | 182 |
| 2 | Lenovo, SK-8827 | 190 |
| 3 | Lenovo, KU-1601 | 183 |
| 4 | Penixx, PERIBOARD-106 | 175 |

### 2.4.5 USB キーボードに対する遠方からの Echo TEMPEST の実証実験

前項では、USB キーボードの入力情報が Echo TEMPEST により取得可能であることを示したが、実験の再現性担保のためインジェクションプローブとカレントプローブを用いた近傍での計測にとどまっている。本実験では、USB キーボードに対してアンテナを介して遠方より Echo TEMPEST が実行される可能性を異なる 4 機種の USB キーボードを用いて示す。表 2.6 に対象とした USB キーボード、図 2.16 に計測環境、表 2.7 に使用した計測環境とパラメタを示す。

実験対象となる USB キーボードは電波暗室内の高さ 75 cm の木製テーブル上に設置し、USB キーボードの長さ $\boldsymbol{L}$（表 2.6）の伝送線路を張った状態で USB アイソレータに接続した。TX / RX アンテナは、2 つのログペリオディックアンテナを使用し、USB キーボードの伝送線路から 300 cm の位置に設置した。USB キーボードは USB アイソレータを介して電波暗室外部の PC に接続した。照射する電磁波の周波数は、計測対象の USB キーボード毎にアンテナの周波数帯域を掃引し、Echo を振幅復調した波形の振幅が最も大きく計測された周波数を選択した。また、SDR の RX ゲインは、受信信号が飽和しない強度となるように自動的に調整可能なプログラムにより決定された（表 2.7)。

異なる 4 台の USB キーボードに対する Echo TEMPEST の計測結果を図 2.17 から図 2.20 に示す。図 2.17 から図 2.20 では、対象の USB キーボード毎に以下の 4 種類の波形を示す。本実験では、計測環境への侵襲を防ぎ実験の再現性を保つた

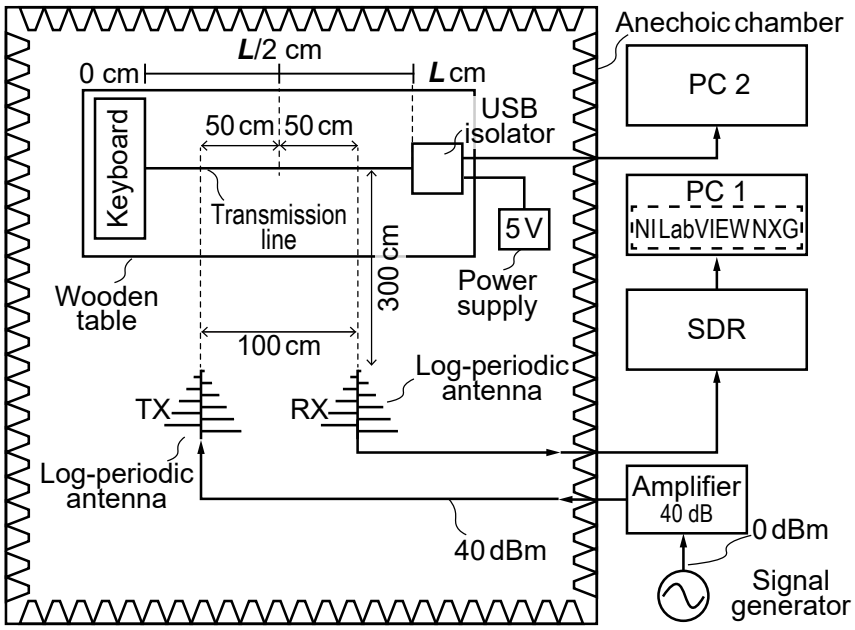


図 2.16. USB キーボードに対する遠方からの Echo TEMPEST の計測環境

め、USB キーボードに入力を与えなかった際に観測された PC – USB キーボード間で定常的に伝送される信号を Echo TEMPEST の計測対象とした。

(a) **USB キーボード未入力時に計測された波形**

事前にオシロスコープを用いて USB アイソレータ上の計測ポートをタッピングして計測した波形を示す。本実験では、異なる 4 台の USB キーボードを使用したため、それぞれ異なるアドレスを有したトークンパケットが計測された。

(b) **Echo TEMPEST により計測された信号の振幅復調波形**

電磁波の照射によって生じた Echo を振幅復調した波形を示す。グラフの縦軸は、計測された振幅変調波に 4 MHz の LPF を適用した後に、正規化した値を示している。

(c) **振幅復調後の波形を NRZI 符号方式に従って復元した波形**

(b) で得られた振幅復調波形を信号処理により 2 値化した結果を示す。具体

表 2.7. USB キーボードに対する実験に使用した Echo TEMPEST の計測環境とパラメタ

| 計測環境 | | | |
|---|---|---|---|
| SDR | | | Ettus Research, USRP X310 |
| SDR ドーターボード | | | Ettus Research, TwinRX 10-6000 MHz |
| SDR 制御ソフトウェア | | | NI, LabVIEW NXG 5.0 |
| 信号生成器 | | | Rohde & Schwarz, SMA100B |
| 高周波増幅器 | | | R&K, A000110-4040-R |
| TX / RX アンテナ | | | Ettus Research, LP0410 |
| USB アイソレータ | | | Analog Devices, EVAL-ADuM4160EBZ |
| USB アイソレータ電源 | | | Texio, PA18-2B |
| **計測パラメタ** | | | |
| SDR サンプリングレート | | | 20 MS/s |
| TX ゲイン | | | 40 dBm |
| 各 USB キーボードの計測パラメタ (No. #) | 1 | 周波数 | 922 MHz |
| | | SDR RX ゲイン | 73 dB |
| | 2 | 周波数 | 546 MHz |
| | | SDR RX ゲイン | 70 dB |
| | 3 | 周波数 | 867 MHz |
| | | SDR RX ゲイン | 68 dB |
| | 4 | 周波数 | 699 MHz |
| | | SDR RX ゲイン | 76 dB |

的には、伝送信号が変化する際に Echo の振幅が変化することに着目し、微分した振幅復調波形の極値より伝送信号を推定した。

(d) **従来の電磁情報漏えいの手法により計測された波形**

電磁波を照射しない状態で、USB キーボードから放射された電磁波を計測した結果を示す。

図 2.17 から図 2.20 は、USB キーボード No. 1 から No. 4 に対し表 2.7 のパラメタを用いた際の計測結果である。図 2.17 (b) と図 2.18 (b) では、トークンパケットとハンドシェイクパケットを含んだ Echo が計測された。また、計測された振幅復調波形を信号処理し 2 値化した図 2.17 (c) と図 2.18 (c) では、図 2.17 (a) や図 2.18 (a) と同等の電圧変動の復元が確認された。図 2.17 (b) と図 2.18 (b) で計測された Echo は、伝送信号の伝送源となるターゲット回路に応じて、異なる振幅で Echo が放射していることが確認された。図 2.19 (b) と図 2.20 (b) では、トークンパケットとハンドシェイクパケットが含まれる予想される Echo を破線で示す。いずれもハンドシェイクパケットに対応した Echo が計測され、図 2.19 (c) では、ハンドシェイクパケットと同等の電圧変動の復元が確認された。一方、図 2.20 (c) では、伝送信号の変動のタイミングの復元が困難であることが確認された。また、図 2.19 (b) と図 2.20 (b) ではトークンパケットに対応した Echo の振幅変動が小さく復元が困難であることが確認された。図 2.17 (d) から図 2.20 (d) に示す従来の電磁情報漏えい手法で取得した波形に着目すると、いずれの USB キーボードでも伝送信号の復元が困難であることが確認された。

以上の結果より、従来の電磁情報漏えい手法では情報漏えいが確認されなかった USB キーボードに対し、アンテナを用いた遠方より Echo TEMPEST を実行し、入力情報と同等のプロセスで生成されるハンドシェイクパケットを取得可能であることを示した。

一方、伝送情報を出力するターゲット回路に応じて生成される Echo の振幅に差が確認された（図 2.17 (b) から図 2.19 (b)）と共に、本提案手法を利用した場合でも伝送信号の復元が困難となる機器も確認された（図 2.20 (b)）。これは、ターゲット回路の出力信号の値に応じた入力インピーダンス値の差が小さく、ターゲット回路で反射する Echo の振幅の変動が小さくなったためと考えられる。また、TX / RX アンテナとターゲット回路間の電磁波の伝達特性も影響するため、ターゲット回路への伝搬時や生成された Echo の放射時の減衰により背景ノイズの影響を受け、ターゲット回路の情報の復元が困難となったと考えられる。

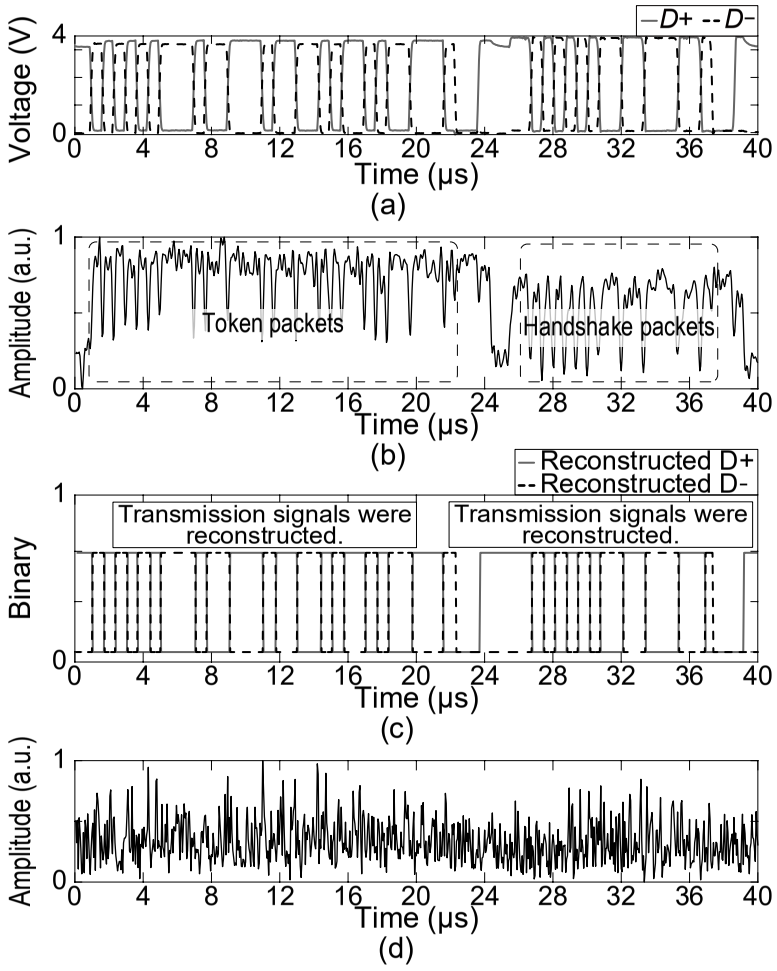


図 2.17. USB キーボード (No. 1) の Echo TEMPEST の計測結果

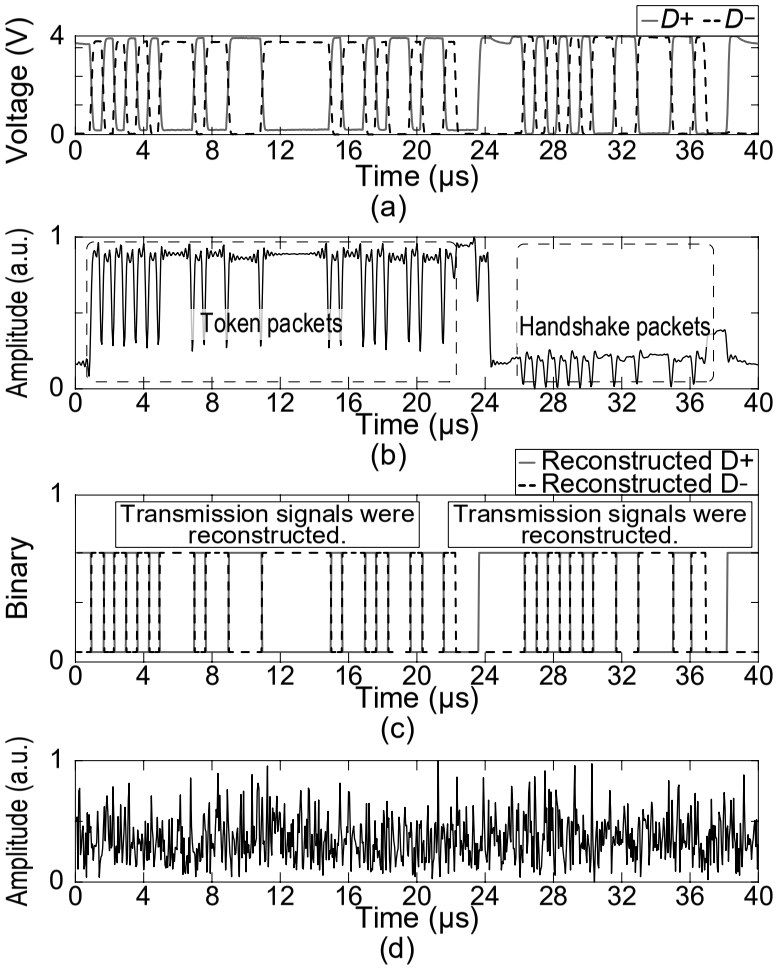


図 2.18. USB キーボード (No. 2) の Echo TEMPEST の計測結果

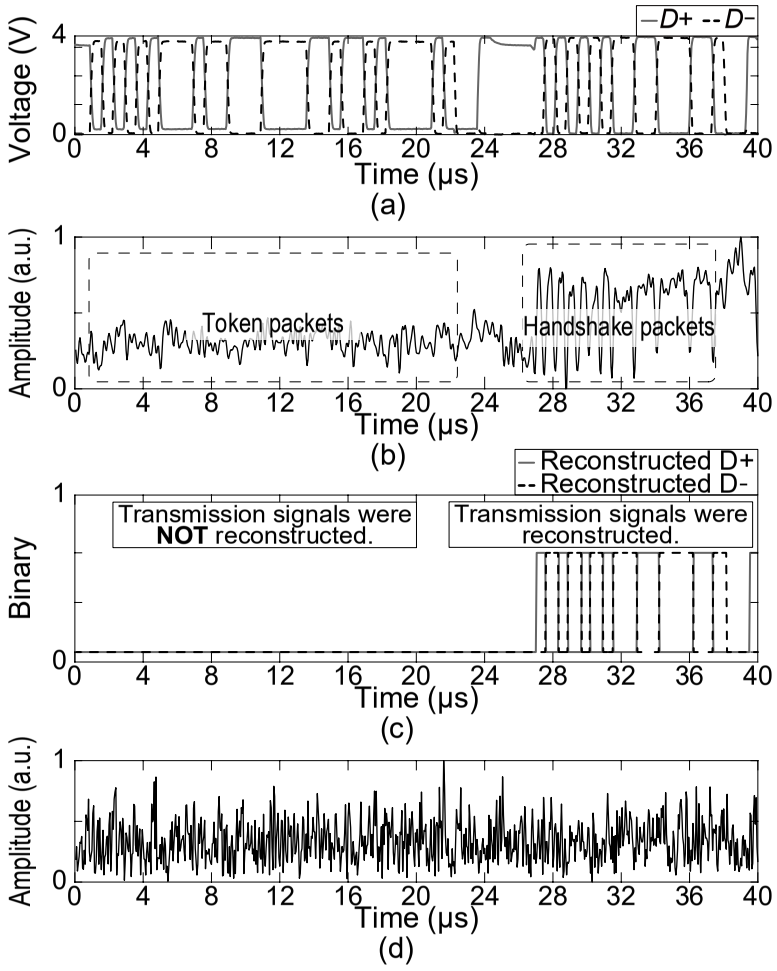


図 2.19. USB キーボード (No. 3) の Echo TEMPEST の計測結果

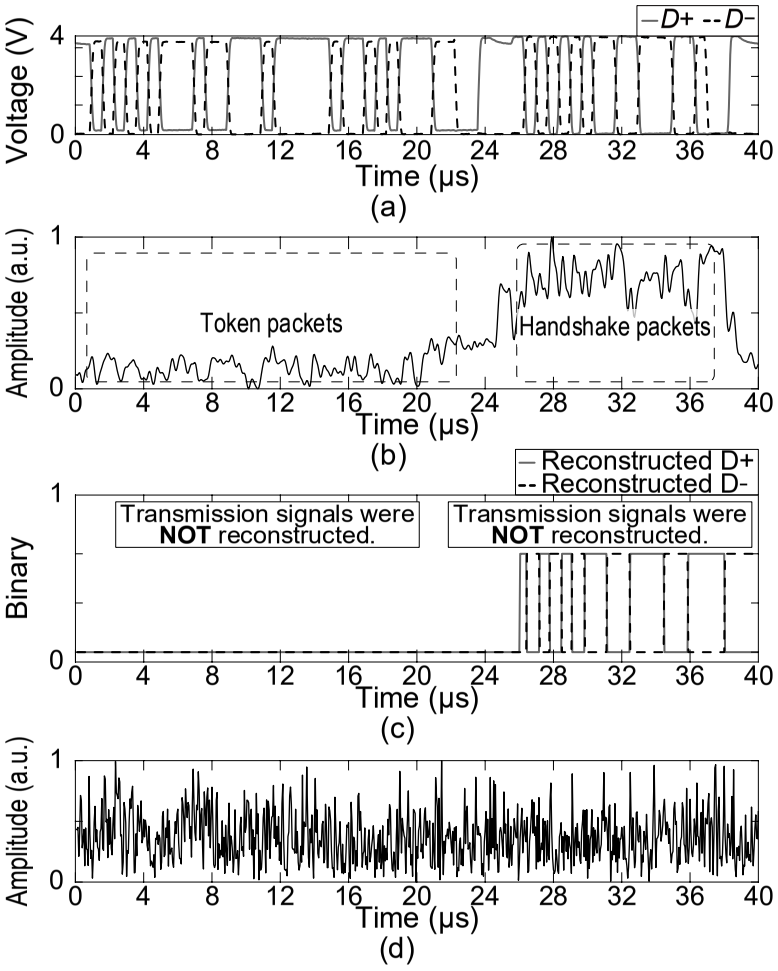


図 2.20. USB キーボード (No. 4) の Echo TEMPEST の計測結果

## 2.5 Echo TEMPEST が誘発されるメカニズムに基づく対策技術

本節では、Echo TEMPEST が誘発されるメカニズムに基づいた対策技術について検討する。Echo TEMPEST は、ターゲット回路の出力状態の変化を Echo として計測するための特定周波数の電磁波の照射する段階と、機器内部で生じた Echo が外部に放射し攻撃者により情報が復元される段階の 2 つに分類することができる。

### 2.5.1 意図的な電磁波の照射の検知による対策技術

Echo TEMPEST の誘発には、攻撃対象機器周辺の背景ノイズ以上の強度で電磁波を照射し、ターゲット回路まで所望の強度で電磁波を伝搬させる必要がある。このような場合、攻撃者による Echo を生成しうる特定周波数の電磁波の照射を検知できれば、情報の処理や伝送を中断し攻撃による影響を阻止または低減できる可能性がある。

過去の検討において、機器に伝搬する電磁波を検知する技術が提案されている。具体的には、照射された電磁波の重畳によって変動する Field-Programmable Gate Array (FPGA) 上の電源電圧の計測 [64] やリファレンス CLK と FPGA 上の CLK との位相・周波数の同期ズレの検出 [65]、伝送信号への干渉により生じるシステムの異常動作ログの解析 [66]、SDR やディスクリート部品で構成された追加のハードウェアを用いた計測 [67, 68] などを用いた検知手法が挙げられる。

これらの技術を用いることで、Echo TEMPEST が実行される前段の特定周波数の電磁波の照射を検知し、処理中の情報の伝送を中断することで攻撃者による Echo TEMPEST の実行を困難化させることができる可能性がある。

一方、本対策技術が搭載された機器に対する意図的な電磁波の照射により可用性を損なう脅威となる可能性がある。そのため、当該機器が扱う情報の重要度や脅威の影響範囲などの評価 [69] を実施し、機密性と可用性のどちらの確保に重点を置くかを決定することが望ましいと考えられる。

### 2.5.2 意図的な電磁波の照射により生ずる Echo からの情報取得の困難化による対策技術

攻撃者が機器内部の伝送情報を復元する段階に着目すると、攻撃者が故意に照射した電磁波により発生した Echo から情報を取得することができなければ本脅威は成立しない。そのため、Echo より情報の取得を困難化させる技術として、「機器から放射する Echo の計測を困難化させる方法」や「計測された Echo から情報の復元を困難化させる方法」が有効であると考えられる。

はじめに、機器から放射する Echo の計測を困難化させる方法について述べる。図 2.20 (b) で示したように、機器から放射した Echo の振幅が小さい場合、Echo が周辺の背景ノイズの影響によって攻撃者が情報を復元することが困難となる。そのため、Echo の計測を困難化させる手法として、従来の電磁情報漏えい対策技術として検討されてきたノイズを用いたジャミング [70, 71] が Echo TEMPEST の対策として適用できる可能性がある。

続いて、攻撃者により計測された Echo より情報の復元を困難化させる方法について述べる。本論文で使用した対象機器や潜在的に Echo TEMPEST の脅威対象となりえる機器は、いずれも伝送信号が暗号化されていない機器である。そのため、機器の伝送情報を暗号化することにより、Echo が生じた場合でも伝送情報を保護できる可能性がある。一方、伝送信号の暗号化は機器の設計段階で実装する必要があると共に、情報を送受信する IC 間や機器間で仕様や規格を統一する必要がある。そのため、製造済みの機器や運用されている機器に対して本対策手法を適用することは困難である。

## 2.6 結言

本章では、情報が電気信号として処理・伝送される過程で生じる回路の電気的な変化を意図的に照射した電磁波を用いて能動的なセンシングによるエミッション制御が引き起こす Echo TEMPEST の実行可能性を示した。具体的には、IC 内部で処理された情報が、I/O 回路を介して伝送される際のターゲット回路の出力状態の変化に着目し、照射した電磁波の反射と透過により生成された Echo の振幅変動より伝送情報を推定する手法を検討した。

2.2 節では、機器内部の情報を能動的にセンシングするため I/O 回路の出力バッファの状態変化に着目した。そして、I/O 回路の出力バッファの状態変化を機器外部から能動的にセンシングすることで引き起こされる Echo TEMPEST のメカニズムについて説明した。2.3 節では、ターゲット回路となる I/O 回路の出力バッファと同等の構造を有するインバータ素子を搭載した DUT を用いて、インバータ素子の出力信号の値に応じて Echo が生成されることを確認した。2.4 節では、Echo TEMPEST が民生機器にも適用される可能性について検討した。具体的には、実験対象としてシングルエンド信号を出力する UART モジュール、差動信号を出力する USB キーボードを用いて、Echo TEMPEST が実行されることを確認した。また、UART モジュールを用いて、能動的なセンシングに用いる電磁波の照射強度に応じて伝送情報が取得できる距離を制御されることを示した。2.5 節では、Echo TEMPEST が誘発される段階を、機器内部の伝送情報を Echo として計測するための特定周波数の電磁波の照射と、機器内部で生成された Echo が外部に放射し攻撃者により情報が復元される段階の 2 つに分類しそれぞれの段階における対策技術について検討した。

以上より本章では、IC が情報を電気信号として伝送する際に生ずる I/O 回路の出力バッファの状態変化が、機器外部より故意に照射された電磁波の反射より推定されることで情報漏えいが引き起こされる Echo TEMPEST の実行可能性が確認された。また、照射した電磁波の周波数に対する IC の反射係数の変化およびターゲット回路までの伝達特性が Echo TEMPEST の成立を決定させることが明らかとなった。そして、Echo TEMPEST に対抗する対策技術となりえる意図的に照射された電磁波の検知技術および Echo の情報の取得の困難化させる技術について検討した。

本章で示した実証実験は電波暗室内の理想的な環境下で実施したが、機器周辺の背景ノイズや Echo に対する照射電磁波の干渉による影響を考慮することで現実と同等の環境で脅威を評価できると考えられる。背景ノイズや Echo に対する照射電磁波の干渉は、Echo からの情報の取得を困難化させる要因である。これらを模擬した計測環境の構築には、任意信号生成器を用いた電波暗室内でのノイズの意図的な生成や Echo に対する照射電磁波の干渉が生じやすい計測環境を意図的に作り出すことが有効である可能性がある。特に、Echo に対する照射電磁波の干渉に関する問題は電波暗室内の理想的な環境下でも生じる問題であるため、本論文の付録 A および付録 B で Echo に対する照射電磁波の干渉を抑制した Echo TEMPEST について示した。

# 第 3 章　不正な回路改変による機器のイミュニティの制御と意図的な電磁波の照射が引き起こす脅威

## 3.1　緒言

本章では、不正な回路改変による機器のイミュニティ制御と意図的な電磁波の照射が引き起こす脅威が、従来の意図的な電磁波の照射の脅威対象外の機器に拡張される可能性について実証する。はじめに、機器の等価回路網の一部の不正な回路改変によって、特定周波数の意図的に照射された電磁波が機器内部に誘導されやすい状態を生成する。そして、機器内部で伝送される情報を表す電気信号を生成する回路の電気的な特性や状態の変化を模擬することで機器に情報が注入される攻撃の実行可能性を示す。

3.2 節では、意図的に照射した電磁波を機器内部に伝搬し、情報として機器に注入する手法について述べる。具体的には、機器の等価回路網の不正な回路改変により局所的なイミュニティの低下を引き起こし、特定周波数の電磁波が伝搬しやすい状態を生成する。そして、イミュニティが低下した部位より機器内部に意図的に照射した電磁波を伝搬させ、電磁波に含まれる情報が機器に注入される脅威が引き起こされる可能性について述べる。3.3 節では、対象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情報注入のための回路の実装について述べる。そして、民生機器に対する実証実験より、不正な回路改変による局所的なイミュニティの低下および意図的に照射した電磁波を用いることで機器内部への情報注入が可能であることを示す。3.4 節では、本章で提案した意図的に照射された電磁波による情報注入の脅威に対抗する技術として、機器の等価回路網の回路改変を検知する技術について検討する。

## 3.2　機器のイミュニティの制御と情報注入を実現する不正な回路改変

本節では、機器の等価回路網の不正な回路改変による局所的なイミュニティの低下により、特定周波数の電磁波が伝搬しやすい状態を生成し、情報を含んだ電磁波

の意図的な照射によって情報注入が成立する可能性について述べる。

はじめに、機器のイミュニティを低下させ特定周波数の電磁波が伝搬しやすい状態を生成する不正な回路改変について述べる。機器のイミュニティの低下は、機器の等価回路網の不正な回路改変による特定周波数の伝達特性の制御として捉えることができ、故意に照射された電磁波を機器内部に低損失で誘導させることが可能となる。そして、機器内部に誘導された電磁波が機器の伝送信号を生成する回路の電気的な特性や状態の変化を模擬する追加回路に伝搬することで、情報注入が実現することを示す。

### 3.2.1 機器の等価回路網の不正な回路改変によるイミュニティの制御手法

攻撃者が機器への侵襲が可能な場合を想定すると、機器の等価回路網の不正な回路改変により意図的にイミュニティが低下した状態を作り出すことができる可能性がある。具体的な例として、導線などの追加の導体で作成したアンテナの実装が考えられる [72, 73]。これらの手法では、攻撃者が所望した周波数に共振するアンテナの実装により、アンテナを実装した部位の伝達特性に変化が生じる。そのため、機器の等価回路網の不正な回路改変は、特定周波数に対する伝達特性の制御手法と見なすことができる。一方、機器を構成する線路や導体などに対する改変により、追加の導体の実装によって構成されたアンテナと同等の効果が得られる可能性がある。そこで本節では、機器を構成する線路や導体の一部を改変することで、特定周波数に対する伝達特性を制御できる可能性について検討する。

過去の検討より、PCB や PCB 上の配線、その接続線路などがノイズを放射するアンテナとして動作することが示されており [74–77]、電磁波の相反性よりこのような部位は機器外部より照射された電磁波の受信アンテナとしても動作することが予想される。一方、機器の PCB が筐体で覆われている場合は PCB への侵襲が困難であると共に、信号の伝送線路への改変は機器本来の動作を阻害する可能性がある。そのため、機器間の伝送線路や電源に接続された電源線路などに電磁妨害対策として施されている金属箔や金属メッシュなどの機器本来の動作を阻害する可能性が低いシールド導体に着目した。

機器の接続線路を覆うシールド導体への改変によるアンテナ構造の作成方法として、シールド導体の切断や素子の追加実装が考えられる。本論文では、シールド導体の分断は機器本来の動作を阻害する可能性があるため議論せず、フェライトコア (FC: Ferrite Core) やフェライトビーズ (FB: Ferrite Bead) の追加実装に着目する。FC や FB は機器のノイズ対策として実装されることが一般的であり、印加される周波数や電流などに応じてインピーダンスが変化する。代表的な FC や FB では、印加される周波数が低周波の場合は低インピーダンス、高周波の場合は高インピーダンスとなる。これらがシールド導体に実装された場合、実装された部位で高周波的に分離されていることに相当する。そのため、シールド導体上の 2 箇所に実装することで FC または FB 間のシールド導体が、機器やその他の機器から高周波的に分離された長さ $\boldsymbol{L}$ の導体となる。このような長さ $\boldsymbol{L}$ の導体がアンテナとして振る舞うことで、長さ $\boldsymbol{L}$ と共振する周波数に対して局所的にイミュニティが低下した状態を生成することが可能となる。また、FC や FB 間の導体の長さ $\boldsymbol{L}$ を変化させることで任意の周波数に対するイミュニティが低下した状態を生成可能となり伝達特性の制御手法となりえる。

以上のように、機器の等価回路網の不正な回路改変によって高周波的に機器から分離されたシールド導体がアンテナとして振る舞うことで、シールド導体と共振する周波数に対するイミュニティを低下させ、意図的に照射した電磁波を機器内部に低損失で誘導できる可能性がある。

### 3.2.2 不正な回路改変と意図的な電磁波の照射による情報注入手法

機器に対して意図的に照射した電磁波を用いた情報注入の実現には、機器内部に誘導された電磁波を機器に実装された IC が正規の信号として認識させる必要がある。本節では、誘導された電磁波より機器内部で伝送される電気信号を生成する方法について検討する。

機器内部の IC が伝送する電気信号を生成する例として、ハードウェアトロージャン が挙げられる。ハードウェアトロージャンは、IC の設計・製造の過程に悪意ある第三者が介入することで、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る脅威であり [78–81]、IC 内

部に実装されたバックドアより監視レーダを停止させた例などが報告されている。このようなハードウェアトロージャンの主な機能として、情報漏えい、機能改変、サービス妨害、性能低下が挙げられ、機密性・完全性・可用性を損なわせる脅威として報告されている。これらのハードウェアトロージャンによる脅威に対して、サイドチャネル情報を用いた評価、ゲートレベルの特性評価、テストベクタに対する応答の評価、電気的な特性の計測評価、機械学習を用いた評価などが提案されている [82–88]。

一方、このようなハードウェアトロージャンによる脅威は IC 内部だけに限定されず、IC 外部にも脅威がおよぶ恐れがある。機器の製造過程に着目すると、様々なベンダで製造された IC やモジュール、接続線路などが利用されており、これらに対しても悪意ある第三者が介入する可能性がある。近年では、「IC 外部の周辺機器や周辺回路に実装可能なハードウェアトロージャン [72, 89–92]」（以下、HT）が報告されていると共に、米国報道機関 Bloomberg などでは、米国大手 IT (Information Technology) 企業に納入されたサーバのマザーボードに本来の設計では存在しないスパイチップが実装されていた可能性を報告している [93, 94]。このような HT は PCB 上の配線上や接続線路に対して IC や素子、モジュールの追加実装 [72, 89, 91, 92, 94] や既存の IC の取り外し・入れ替えなど [90] によって実現される。そのため、必ずしも機器が製造されるタイミングでの実装が求められるわけではない。一例として、機器の運搬過程や販売過程、運用過程などの攻撃者が機器に侵襲可能なタイミングで HT が実装される可能性がある。本論文では、HT だけでなく機器やその接続線路などに対する IC や素子、モジュールの追加実装など、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」と定義する。

攻撃者が意図した情報を注入し IC に処理させるためには、HT を駆動するための電力の供給と注入する情報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共振する周波数をキャリアとして用い、対象機器に注入する電気信号を変調した電磁波を生成し機器外部から照射する。そのため、対象機器に実装された HT は次の 2 つの機能を持つことが求められる。

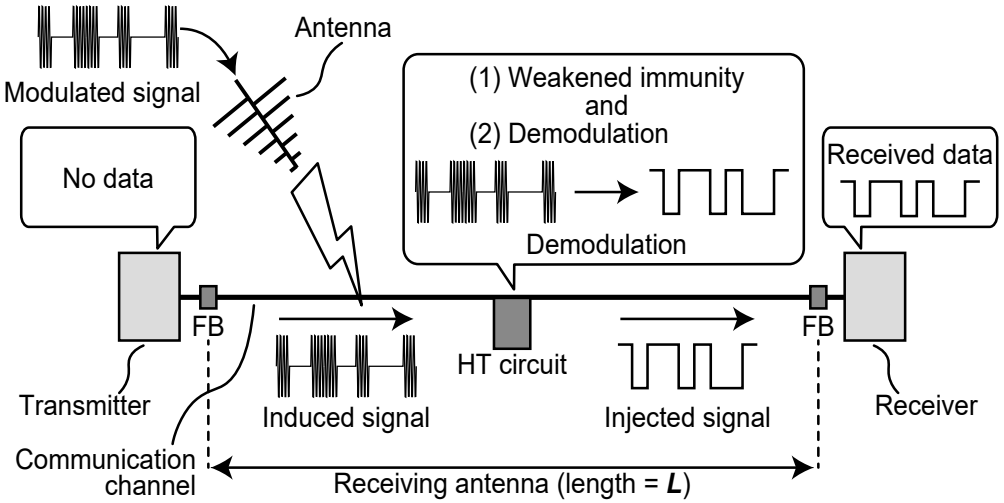


図 3.1. 不正な回路改変によるイミュニティ制御と
意図的な電磁波の照射による情報注入の概念図

**機能** 1: **シールド導体上のアンテナが受信した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変調波を整流し、HT を駆動するための DC 成分と対象機器の IC に処理させる信号を表す交流成分を得る。

**機能** 2: **復調の結果に応じた IC が処理可能な電気信号を生成する機能**

機能 1 で得られた復調の結果に従って、攻撃対象機器の IC が処理可能な電気信号を生成する。対象機器の IC で伝送される電気信号の信号レベルやプトロコルなどが異なるため、対象機器の伝送信号を生成する回路の電気的な特性や状態の変化を模擬する回路の設計が必要となる。

以上の機能を持つ HT をシールド導体上に構成されたアンテナに接続し、対象機器に注入する情報を含んだ変調波を照射することで情報注入が可能となる。対象機器への回路改変による伝達特性の制御と故意に照射された電磁波による情報注入の概念図を図 3.1 に示す。

### 3.2.3 不正な回路改変と意図的な電磁波の照射による情報注入の成立条件

本脅威が成立する条件として、以下の 3 つが存在する。

**条件 1: 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**

不正な回路改変は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実行される可能性がある。そのため、必ずしも機器のベンダへの介入が求められるわけではない。また、不正な回路改変が可能な期間に着目すると、機器がベンダから出荷されてから製品寿命を迎えるまで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。稼働している機器に対して不正な回路改変を行うには、一定時間の機器への侵襲が必要である。インフラシステムやサーバ、それらの制御装置などの機器は、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。一方、機器の納入やリプレース、メンテナンスなど、第三者が機器に侵襲する機会が存在する。また、機器の接続線路のような置換可能な対象であれば、不正な回路改変済みの接続線路を用意しておき、対象機器に侵襲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が実行される可能性がある。

**条件 2: 対象となる機器が伝送情報のプロトコル等が既知である**

攻撃対象の IC に正規の信号であると認識させるためには、IC から伝送される電気信号の信号レベルやプロトコルなどに従った信号を生成する HT の設計が必須である。

**条件 3: 意図的に照射された電磁波が機器に到達可能である**

3.2.2 節で示した 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の変調波によって駆動することから、攻撃者が照射した変調波が攻撃対象機器に到達することが必須である。そのため、シールディングされた建物 [95] 内部に攻撃対象機器が設置されている場合、本脅威は成立しない。

## 3.3　不正な回路改変と意図的な電磁波の照射による情報注入の実証

本節では、機器に対する回路改変によるイミュニティの制御と意図的に照射した電磁波を用いた情報注入の実行可能性について示す。

はじめに、対象機器に実装した HT の回路と対象機器への実装方法について述べる。続いて、アンテナとして振る舞うシールド導体に共振する周波数を搬送波とし、注入する情報を含む変調波の生成方法について述べる。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により、意図的に照射された電磁波を機器内部に誘導し、HT によって生成された電気信号により情報注入が実現することを示す。

### 3.3.1　不正な回路改変に用いる HT 回路とその実装

本実験では、2.4.2 節で Echo TEMPEST の成立が確認された UART モジュールを用いる。UART モジュール伝送線路の TX と RX は、シールド導体で覆われた信号線と GND 線の 2 本で接続された単向通信とし、伝送線路長は 1 m とした。

UART モジュールに対する特定周波数のイミュニティの制御は、UART モジュール間の伝送線路上のシールド導体を高周波的に機器から分離し、特定周波数で電気的に共振するアンテナ構造により実現した。本実験では、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 の実装後に伝送線路の被膜で再度覆うことで、伝送線路の見た目の変化を抑え、利用者に回路改変を検知されにくくすることが可能である。シールド導体に実装する FB は、照射する電磁波の周波数付近でシールド導体の特性インピーダンスに比べて十分大きなインピーダンスが得られる FB を選択する必要がある。本実験では、後述する TX アンテナの周波数帯域でおよそ 300 – 700 Ω 程度のインピーダンスが得られる FB (Murata, BLM18RK102SN1) を選択した。

続いて、対象機器内部に伝搬した変調波から、IC が正規の信号として処理可能な電気信号を生成する HT の回路構造について述べる。本実験では、情報を含む変調波として振幅変調波を用いた。図 3.2 に振幅変調波を復調し電気信号を生成する HT の回路図を示す。本実験で作成した HT は、整流回路と LPF、スイッチング回

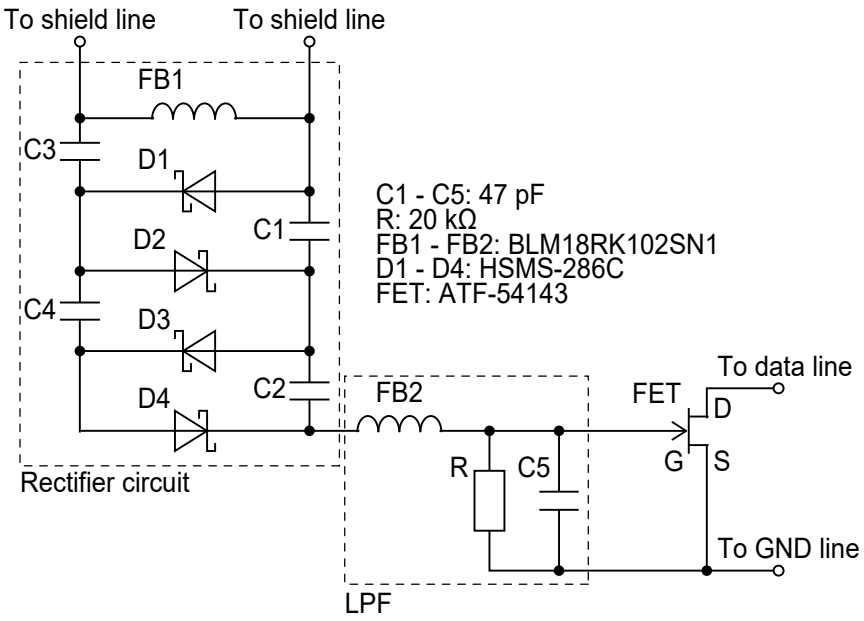


図 3.2. 伝送線路上に実装する HT の回路図

路の 3 つのコンポーネントによって構成される。HT の入力は、FB の実装によって伝送線路上に作り出されたアンテナ構造とし、スイッチング回路の出力が伝送線路上のデータ線と GND 線に接続されるように実装した。整流回路は、伝搬した振幅変調波の昇圧機能と包絡線検波する機能を持つように設計した。LPF は、機器の電気信号に起因した放射によって 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 (Field Effect Transistor) のドレイン (D: Drain) とソース (S: Source) を伝送線路上のデータ線と GND 線に接続するように実装することで（図 3.2)、ゲート (G: Gate) に入力された LPF の出力に応じて D – S 間に短絡を発生させ、情報を表す電気信号を生成する UART モジュールの I/O 回路の出力状態を模擬している。一方、作成した HT は注入する情報の電気信号を FET の D – S 間の短絡により生成しているため、情報注入が可能なタイミングは UART モジュール間が無通信状態の場合に限られる。

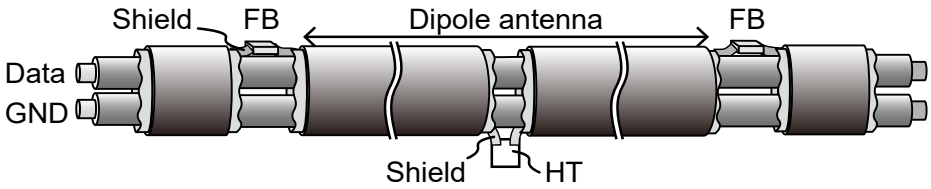


図 3.3. UART モジュール間の伝送線路に対する FB と HT の実装の概念図

図 3.3 に FB と HT の実装の概念図を示す。UART モジュール間の伝送線路のシールド導体は、シールド導体上の 2 つの FB および HT 回路内部の FB 1（図 3.2）により高周波的に分離されており、長さ $L$ のダイポールアンテナのように振る舞う。

### 3.3.2　機器に注入する情報を含んだ電磁波の生成手法

図 3.4 に計測対象である UART モジュールに“a”の情報を注入する場合を想定した振幅変調波を生成するプロセスを示す。図 3.4 では、後述する実証実験との対応のため SDR と SDR 制御ソフトウェアを用いた場合の例を示しているが、任意波形発生器などを用いる場合も同様のプロセスで振幅変調波を生成することができる。UART モジュールで伝送される情報の仕様および伝送パラメタは 2.4.2 節を参照する。

はじめに、SDR 制御ソフトウェア上で入力情報から ASCII コードに従ったビット列に変換し、最下位ビットを先頭とした UART のデータビットを生成する。続いて、データビットの前後にスタートビットとストップビットを付加し、ベースバンド信号を生成する。このとき、SDR に設定されたサンプリングレートと UART モジュールのボーレートを一致させるようにリサンプリングを行う。そして、生成したベースバンド信号を SDR に入力し、照射するキャリア周波数によって周波数変換することで情報を含んだ振幅変調波が生成される。

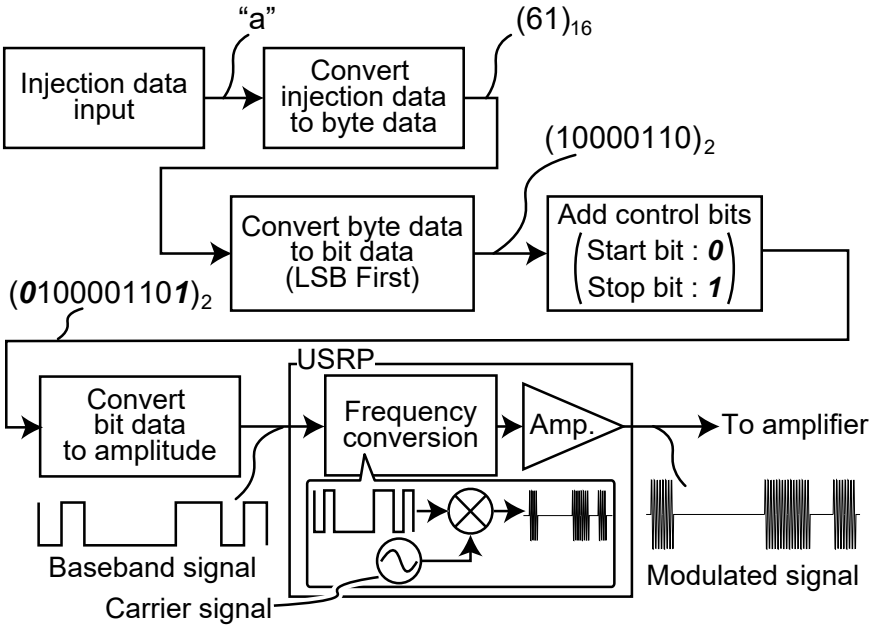


図 3.4. UART モジュールに注入する情報を含んだ振幅変調波の生成プロセス

### 3.3.3 不正な回路改変を用いた情報注入の実証実験

本実験では、UART モジュールに対する回路改変によりイミュニティが制御され、任意の周波数で情報注入が成立することを 2 種類の実験により実証する。図 3.5 および図 3.6 に UART モジュールへの情報注入を行う計測環境、表 3.1 に利用した計測環境とパラメタを示す。

UART モジュールは、電波暗室内の高さ 75 cm の木製テーブルの上に設置した 2 台の PC の USB ポートに接続した。振幅変調波を照射するアンテナとしてログペリオディックアンテナを用い、UART モジュールの伝送線路から 300 cm の位置で伝送線路と同じ高さとなる 75 cm の位置に設置した。SDR で生成された振幅変調波は、高周波増幅器を介して 40 dBm でログペリオディックアンテナから照射した。

図 3.5 に示す実験 1 では、照射する振幅変調波のキャリア周波数として 620 MHz を選択し、UART モジュール間のシールド導体の長さを振幅変調波のキャリア周波

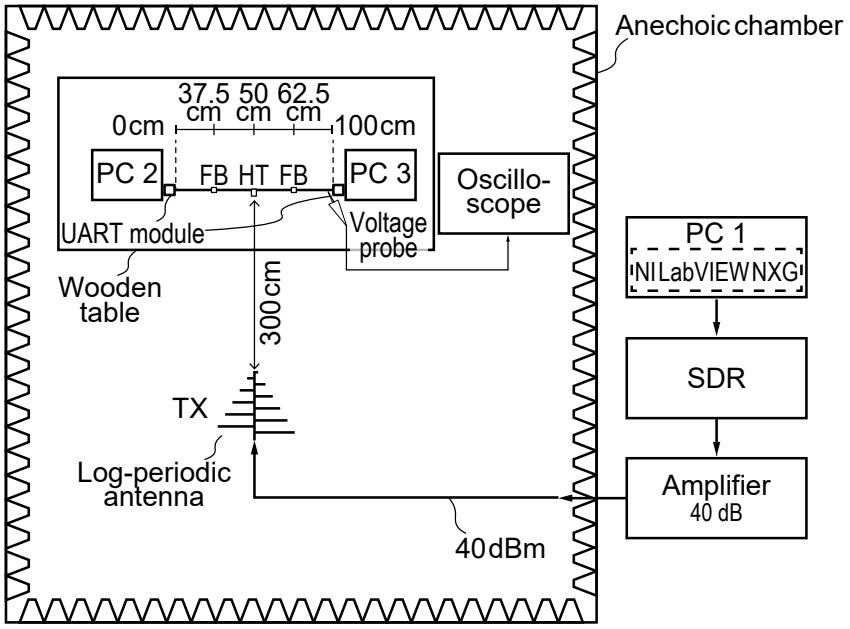


図 3.5. 回路改変と意図的な電磁波の照射による情報注入の計測環境（実験 1）

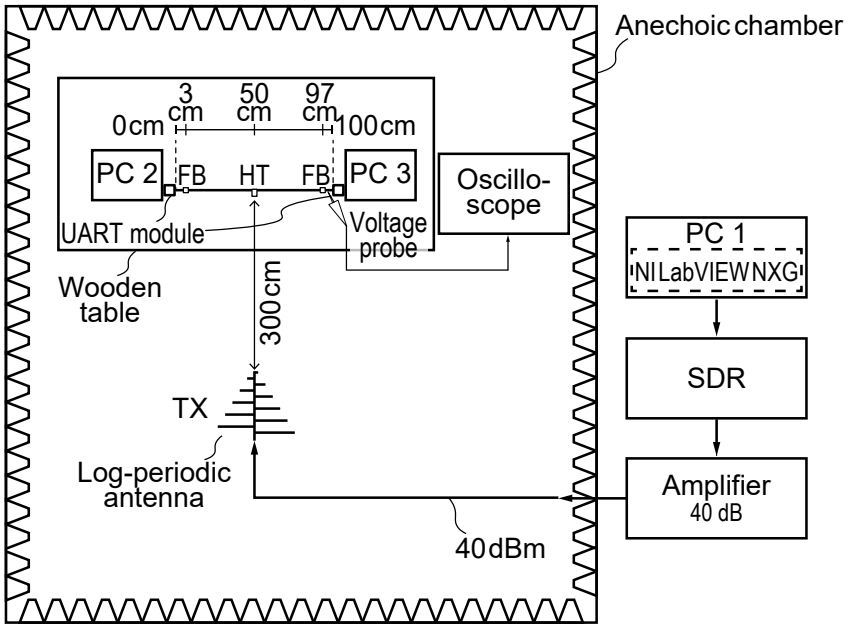


図 3.6. 回路改変と意図的な電磁波の照射による情報注入の計測環境（実験 2）

表 3.1. 情報注入の実証実験に使用した計測環境とパラメタ

| 計測環境 | | |
|---|---|---|
| SDR | Ettus Research, USRP B210 | |
| SDR 制御ソフトウェア | NI, LabVIEW NXG 5.0 | |
| 高周波電力増幅器 | R&K, A0001100-4040-R | |
| 送信アンテナ | Ettus Research, LP0410 | |
| オシロスコープ | Rohde & Schwarz, RTO2014 | |
| **回路改変および照射電磁波のパラメタ** | | |
| | 実験 1（図 3.5） | 実験 2（図 3.6） |
| HT の実装位置（UART TX からの距離） | 50 cm | |
| FB の実装位置（UART TX からの距離） | 37.5, 62.5 cm | 3, 97 cm |
| キャリア周波数 | 620 MHz | 460 MHz |
| 尖頭電力 | 40 dBm | |
| **振幅変調波の生成パラメタ** | | |
| 振幅変調の論理 | 負論理 | |
| ボーレート | 115.2 kb/s | |
| 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 | |
| 振幅変調の変調度 | 100 % | |

数の約 1/2 波長で電気的に共振する 25 cm となるように FB を実装した。また、図 3.6 に示す実験 2 では、照射する振幅変調波のキャリア周波数として 460 MHz を選択し、UART モジュールの伝送線路上のシールド導体の長さが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 となるように FB を実装した。

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

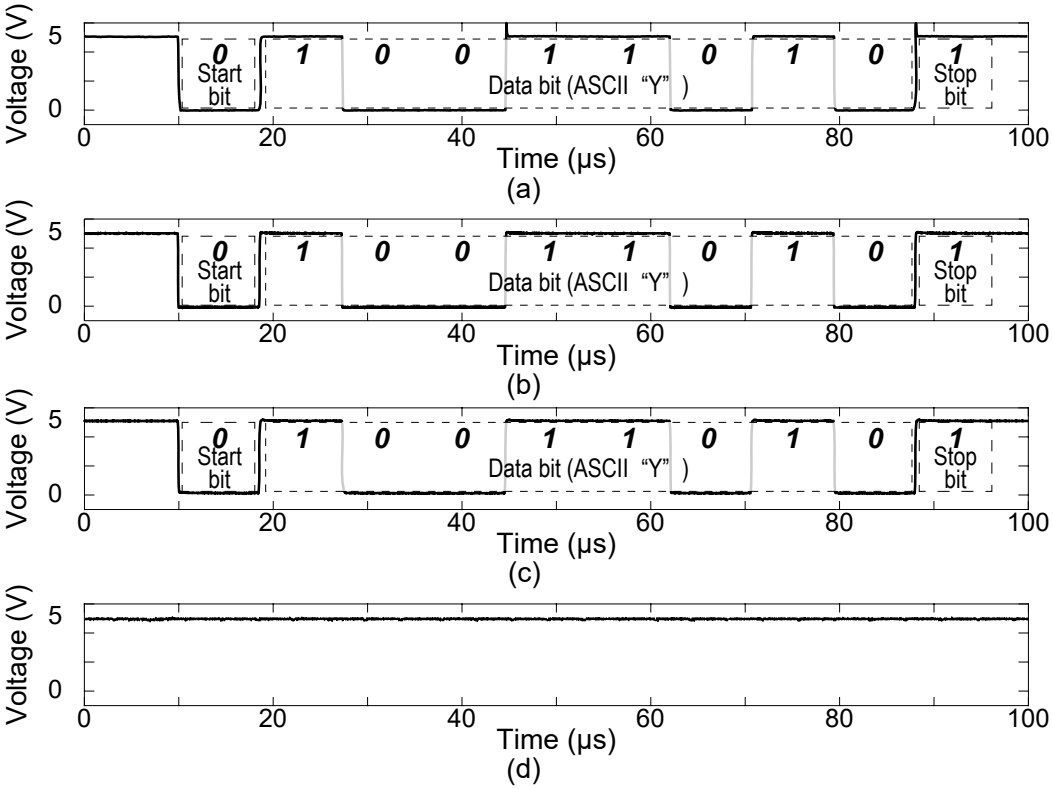


図 3.7. UART モジュールの伝送線路をタッピングした際に計測された波形

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 RX を接続した PC で確認した。図 3.7 に UART モジュールへの情報注入の計測結果を示す。

図 3.7 (a) は、不正な回路改変を行っていない UART モジュールの伝送線路をオシロスコープでタッピングし、“Y” の ASCII コードが伝送された際に計測された波形である。図 3.7 (b) と図 3.7 (c) に不正な回路改変を行った UART モジュールの伝送線路に対して振幅変調波を照射した実験 1 と実験 2 の結果を示す。いずれの場合も図 3.7 (a) で計測された UART モジュールの伝送信号と同等の電圧変動が計測され、UART モジュールの RX を接続した PC 上でも“Y”が伝送されている

ことが確認された。図 3.7 (d) は、不正な回路改変を行っていない UART モジュールの伝送線路に対して実験 1 のパラメタで振幅変調波を照射した結果である。電圧変動は確認されず UART モジュールの RX を接続した PC 上でも情報の注入は確認されていない。

以上の結果より、不正な回路改変による特定周波数に対するイミュニティの制御と情報を含んだ電磁波の照射により機器内部に情報が注入される脅威の実行可能性が示された。本実験では、“Y”の情報を含んだ振幅変調波を照射した結果のみを示しているが、他の情報を含んだ振幅変調波を照射した場合でも情報注入が実行されることを確認している。

## 3.4 不正な回路改変と意図的な電磁波の照射による情報注入に対抗する対策技術

本脅威は、意図的に照射された電磁波を機器内部に誘導し、任意の情報を示す信号を生成することができなければ成立しない。そのため、意図的な電磁波の照射の検知や特定周波数に対するイミュニティを制御する等価回路網の改変、任意の動作を付加する HT を検出する技術が有効である。攻撃者による特定周波数の電磁波の照射の検知は 2.5.1 項で述べた対策技術が利用できると考えられる。

### 3.4.1 不正な回路改変の検知による対策技術

不正な回路改変は、機器の等価回路網の改変によって特定周波数に対するイミュニティを制御し、照射された電磁波を機器内部に誘導することで情報注入を実現している。このような不正な回路改変は、電磁波の相反性の観点より、機器から放射する電磁波にも変化が生じる [77]。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、時間領域または周波数領域における変化から機器への改変が行われたことを検知できる可能性がある。具体的には、機器から放射される広帯域ノイズ源の CLK に着目し [25]、放射電磁波の歪みを計測することで回路改変の実装を検知できる可能性がある。

また、HT が実装された線路の電気的な特性が変化することが知られている。そ

のため、TDR (Time Domain Reflectometry) 法を用いて計測した線路のインピーダンスの変化を計測する手法や、IC などに搭載されたセンサを用いた線路の静電容量の変化を計測する手法により HT の実装を検知できる可能性がある [96, 97]。

## 3.5 結言

本章では、不正な回路改変により、意図的に照射された電磁波が引き起こす機器の動作妨害によるセキュリティの脅威が従来の脅威対象外の機器に拡張される可能性について実証した。具体的には、機器の等価回路網の一部の不正な回路改変によって、特定周波数の意図的に照射された電磁波が機器内部に誘導されやすい状態を生成した。そして、機器内部で伝送される情報を表す電気信号を生成する回路の電気的な特性や状態の変化を模擬することで機器に情報が注入される攻撃の実行可能性を示した。

3.2 節では、意図的に照射した電磁波を機器内部に伝搬し、情報として機器に注入する手法について述べた。具体的には、機器の等価回路網の回路改変により局所的なイミュニティの低下を引き起こし、特定周波数の電磁波が伝搬しやすい状態を生成した。そして、情報注入を実現する方法として HT を用い、伝搬した振幅変調波より IC が処理可能な電気信号を生成することで情報注入を可能とした。3.3 節では、不正な回路改変による機器のイミュニティの低下と、意図的に照射した電磁波を用いた任意の情報が注入される脅威の実現可能性を示した。本脅威により、従来の意図的な電磁波の照射による脅威の対象外であった機器に対して情報が注入されることが確認された。3.4 節では、本章で提案した不正な回路改変による機器のイミュニティの低下と意図的に照射された電磁波による情報注入の脅威に対抗する技術として、意図的に照射された電磁波の検知による対策技術と不正な回路改変の検知による対策技術について検討した。

以上より本章では、不正な回路改変が意図的な電磁波の照射による脅威の対象外とされていた機器に脅威が拡張されることが明らかとなり、電磁波を介した複合的な攻撃による新たな電磁波セキュリティの脅威が成立することが確認された。

# 第 4 章　結論

本論文の各章のまとめは以下の通りである。

1 章では、情報通信技術の信頼の基点となるハードウェアへの電磁波セキュリティの脅威として、電磁情報漏えいの脅威と意図的な電磁波の照射による動作妨害の脅威を挙げた。そして、それぞれの従来研究における課題として、機器のエミッションとイミュニティが制御されることで従来の脅威対象外の機器に脅威がおよぶ可能性について述べた。最後に本論文で取り組む課題とその目標について述べた。

2 章では、電磁波を介した能動的なセンシングによる情報漏えいを Echo TEMPEST と定義し、その実行可能性について検討した。機器が情報を処理・伝送する際に生ずる IC の I/O 回路内部の出力バッファのスイッチングにより生じる電気的な特性の変化が Echo TEMPEST で着目する特徴量であることを示した。そして、IC の出力バッファを抽出した評価環境において電磁波を介した能動的なセンシングによる情報漏えいのメカニズムを明らかにした。また、このメカニズムより、Echo TEMPEST により機器のエミッションが制御される可能性が明らかとなった。続いて、2 種類の民生機器を評価対象とした Echo TEMPEST の実証実験を行い、従来の電磁情報漏えいの脅威対象外であった機器からの情報漏えいの誘発と、能動的なセンシングに利用する電磁波の照射強度に応じて情報が漏えいする距離を制御可能であることを示した。そして、能動的なセンシングにより Echo が生成される Echo TEMPEST のメカニズムに基づき、能動的なセンシングに利用される意図的に照射された電磁波の検知および生成・放射された Echo から情報の復元を困難化させる対策技術について検討した。

3 章では、機器の等価回路網の一部の不正な回路改変により機器内部に電磁波が伝搬しやすい状態を構成し、従来の意図的な電磁波の照射による脅威対象外の機器に対して任意の情報が注入される可能性について検討した。具体的には、機器の等価回路の一部の改変によって局所的にイミュニティが低下した状態を生成し、特定周波数の電磁波が機器内部へ伝搬しやすい状態を生成した。そして、機器外部から照射された情報を含む電磁波を受信し、機器が認識可能な電気信号に変換する HT をイミュニティが低下した部位に実装することで、任意の情報が機器外部より注入可能であることを示した。そして、不正な回路改変が意図的な電磁波の照射によ

る動作妨害の脅威の対象外とされていた機器に脅威が拡張されることが明らかとなった。

本論文では、機器のエミッションとイミュニティの制御により誘発される電磁情報漏えいと意図的な電磁波の照射による動作妨害のメカニズムに基づいた対策技術を検討し、脅威の耐性獲得に関する知見を与えた。本論文で扱った電磁波セキュリティの脅威は、電波暗室内の理想的な環境下において低速かつシリアル通信の機器を用いて実証されたものである。そのため、実環境下における脅威の実行限界の評価、効果的な対策技術の提案およびその実証が今後の課題として挙げられる。これらの実現と共に電磁波セキュリティに関する脅威に対抗するため、実環境を模擬した脅威の評価手法や機器が有する脅威の耐性の評価手法に関する検討が今後求められると考える。

# 付録

## A　照射電磁波の干渉を抑制した Echo TEMPEST の提案

本付録では、Echo TEMPEST の実行時に生じる照射電磁波の干渉が引き起こす Echo の変調度の低下の問題について述べる。そして、Echo の変調度の低下を抑制した Echo TEMPEST を提案し、簡易な計測環境を用いてその有効性を示す。

### A.1　自己干渉波による Echo の変調度の低下

本節では、機器に対する Echo TEMPEST の耐性評価時に生ずる Echo の変調度の低下の問題について述べる。

Echo TEMPEST の実行時に機器に照射された電磁波は、その全てが情報漏えいの対象となる回路に伝搬するわけではない。機器の筐体や周辺回路、周辺機器による反射および送受信アンテナ間の直接的な電磁波の伝搬が生じる。このような電磁波は、機器から放射する Echo に重畳して受信機で受信され Echo の劣化を引き起こす。本論文では、照射した電磁波が Echo に干渉する問題を自己干渉、自己干渉の原因となる照射した電磁波を自己干渉波と定義して述べる。図 A.1 に示すように、自己干渉は Echo の振幅を増幅し、Echo の変調度を低下させる。変調度が低下した Echo を受信した場合には、評価対象となる伝送情報の抽出が困難化する。

これまで、自己干渉によって変調度が低下した Echo から伝送情報を抽出するためには、幅広いダイナミックレンジを有した測定器や高度な高周波測定・信号処理技術が必要とされていた [98, 99]。そのため、高価な機器や高度な高周波測定・信号処理技術を必要としない手法が実現することでより簡易で高精度に Echo TEMPEST の脅威を評価することが可能となる。

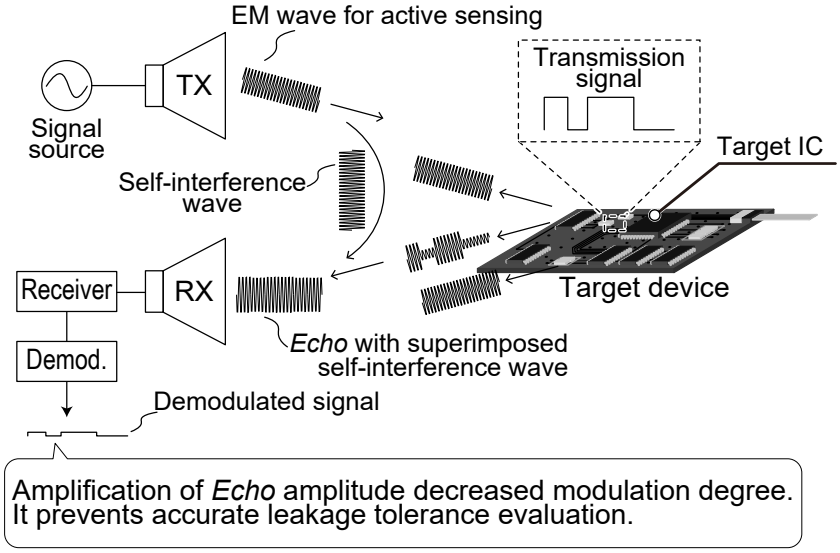


図 A.1. 照射した電磁波により生じた自己干渉波の重畳により Echo の変調度を低下する概念図

## A.2 自己干渉波を抑制した Echo TEMPEST の提案

本節では、Echo TEMPEST の実行時に生ずる自己干渉による Echo の変調度が低下する問題に着目し、その影響を抑制した Echo TEMPEST を提案する。

本手法では、変調度が低下した Echo に対して自己干渉波の逆位相となる電磁波の加算によって自己干渉波の影響を抑制する。図 A.2 に提案する自己干渉波を抑制した Echo TEMPEST 手法を示す。

受信アンテナで受信された変調度が低下した Echo は受信機に入力され、Echo に含まれる自己干渉波の位相と強度を取得する（図 A.2 (a)）。信号生成器によって取得した位相の逆位相となる電磁波を生成し（図 A.2 (b)）、受信した Echo に加算することで自己干渉波の抑制を実現する（図 A.2 (c)）。このとき、図 A.2 (b) で入力した逆位相の電磁波が測定環境に影響を与えることを防ぐため、図 A.2 (c) では方向性結合器のような一方向性の線路を有した環境を使用する。

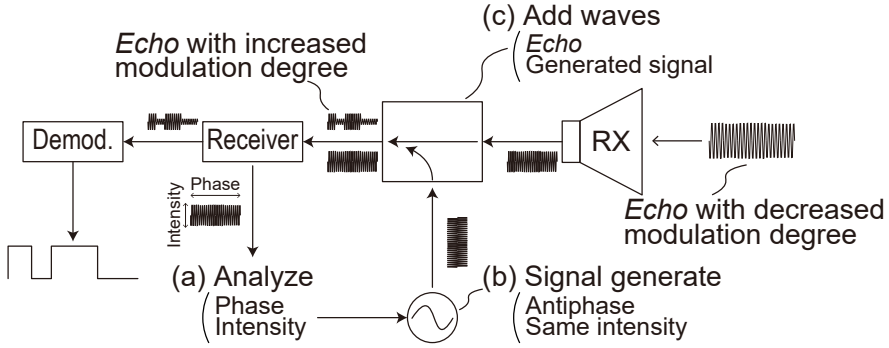


図 A.2. 自己干渉波の影響を抑制した Echo TEMPEST の提案手法

## A.3　自己干渉波の抑制手法の実証実験

本節では、提案した自己干渉の抑制手法の有効性を実験的に示す。図 A.3 に自己干渉波の計測に使用したセットアップ、表 A.1 に使用した計測環境とパラメタを示す。

本実験では自己干渉波の抑制効果のみを評価するため、評価対象機器の IC に対して直接アンテナを接続できるよう対象機器を改変し使用した。Echo TEMPEST の計測対象として同軸コネクタを実装したマイコンボード（以下、PSoC モジュール）を使用し、PSoC モジュール上の線路を切断した IC の入出力ピンとアンテナを接続した（図 A.3）。PSoC モジュールは、電磁波シールドテント内の高さ 75 cm の木製テーブル上に設置し、垂直に固定した同軸コネクタと同軸ケーブルで接続可能なロッドアンテナに接続した。Echo TEMPEST の評価用の信号として、PSoC モジュールから 800 kHz の方形波をロッドアンテナに接続した IC の出力ピンから出力した。

信号生成器 1 から出力された電磁波は、高周波増幅器によって 30 dBm に増幅されロッドアンテナから 200 cm の位置に設置した TX アンテナから照射した。PSoC モジュールで生成された Echo は、ロッドアンテナから 200 cm の位置に設置した RX アンテナで受信され、方向性結合器を介して SDR に入力される。SDR で解析した自己干渉波の位相と強度は PC より信号生成器 2 に入力され、生成された逆位相の電磁波を方向性結合器の CPL ポートに入力した。信号生成器 1 および

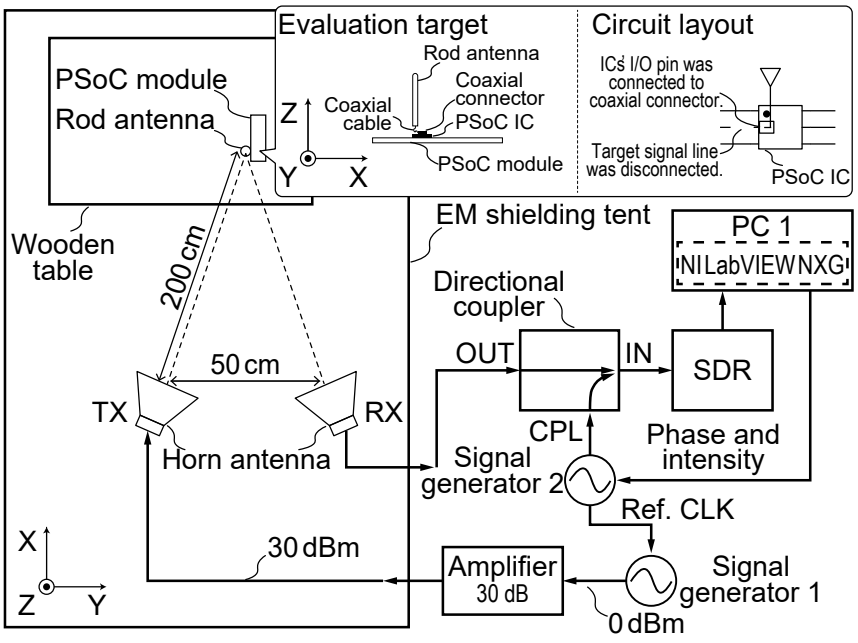


図 A.3. 自己干渉波の抑制手法の有効性の評価環境

信号生成器 2 から出力される電磁波の周波数は、周辺の無線 LAN ルータが出力する信号との干渉を避けるため 2500 MHz とした。SDR の RX ゲインは、受信信号が飽和しない強度となるように自動的に調整可能なプログラムにより決定された。また、信号生成器 1 および信号生成器 2 の基準周波数を同期するためリファレンス CLK を共有している。

図 A.4 (a) に提案手法を適用しない場合に SDR で計測されたスペクトル、図 A.4 (b) に提案手法を適用し自己干渉波の逆位相となる電磁波を加算した際に SDR で計測されたスペクトルを示す。それぞれのスペクトルで PSoC モジュールが出力する評価用の信号である 800 kHz の基本波およびその高調波が確認された。図 A.4 (a) と図 A.4 (b) の結果から、提案手法により自己干渉波が約 40 dB 低減されていることが確認された。

続いて、図 A.5 に SDR で計測された Echo を振幅復調した結果を示す。図 A.5 (a) は PSoC モジュールが出力する 800 kHz の方形波を示している。図 A.5 (b) は提案手法適用前の振幅復調波形、図 A.5 (c) は提案手法適用後の振幅復調波形を示

表 A.1. 自己干渉波の抑制の有効性評価に使用した計測環境とパラメタ

| 計測環境 | |
|---|---|
| SDR | Ettus Research, USRP X310 |
| SDR ドーターボード | Ettus Research, TwinRX 10 - 6000 MHz |
| 信号生成器 1 | Rohde & Schwarz, SMA100B |
| 信号生成器 2 | Keysight, N5181B |
| 高周波電力増幅器 | Mini-Circuits, ZVE-3W-83 |
| ホーンアンテナ | Rohde & Schwarz, HF907 |
| 方向性結合器 | Mini-Circuits, ZUDC10-83-S+ |
| マイコンボード | Cypress, CY8CKIT-059 |
| ロッドアンテナ | N/A, 2.4/5.0 GHz Wi-Fi アンテナ |
| **計測パラメタ** | |
| サンプリングレート | 20 MS/s |
| TX ゲイン | 30 dBm |
| 照射周波数 | 2500 MHz |
| 提案手法未適用時の RX ゲイン | 43 dB |
| 提案手法適用時の RX ゲイン | 64 dB |

す。これらの結果から、従来手法の場合（図 A.5 (b)）では、周期的な振幅変動が確認されていることから評価用の信号が漏えいしていると予想されるが、評価用の信号の高調波成分の欠落や背景ノイズの重畳が確認された。一方、提案手法を適用した場合（図 A.5 (c)）は、評価用の信号の方形波の高周波成分が含まれることでより精度が高い信号が復元されている。また、背景ノイズの重畳も低減されていることが確認された。

以上の結果より、提案手法によって自己干渉波による Echo の変調度の低下の問題を抑制した Echo TEMPEST の脅威の評価を実行できることが確認された。

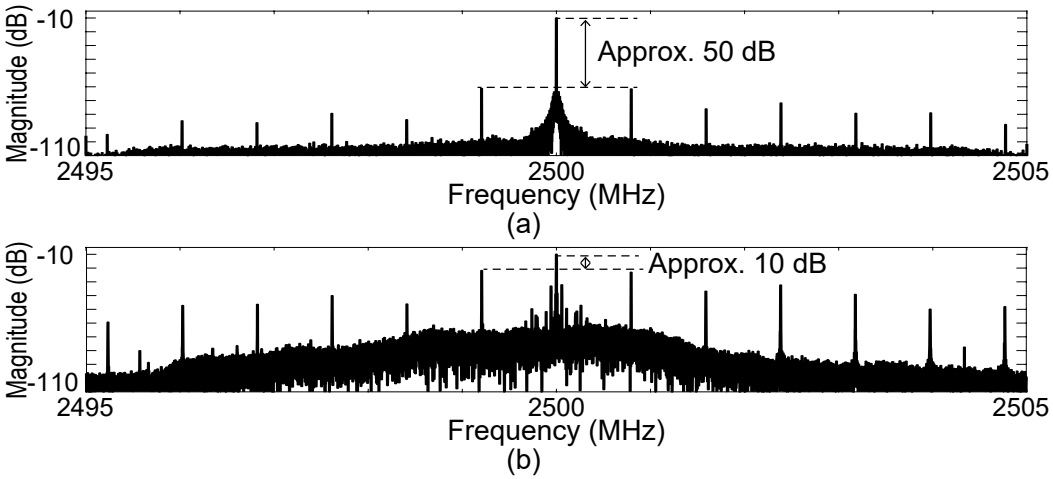


図 A.4. 提案手法による自己干渉波の抑制の有効性の計測結果

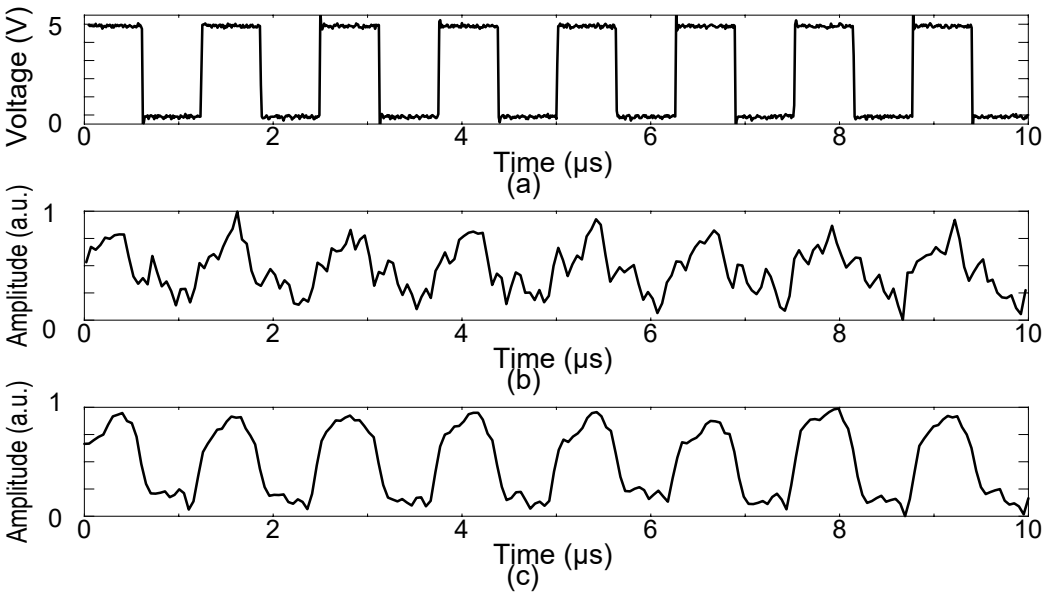


図 A.5. 提案手法による自己干渉波の抑制による Echo TEMPEST の計測結果

# B　複数周波数の照射により引き起こされる Echo TEMPEST

2 章では、単一の周波数を有した意図的な電磁波の照射によって Echo TEMPEST が引き起こされることを示した。本付録では、機器に対する複数の異なる周波数の電磁波の照射によって、照射された周波数とは異なる周波数で Echo TEMPEST を引き起こす手法の実行可能性を示す。このような手法が成立する場合、付録 A.1 で述べた自己干渉の影響を受けない Echo TEMPEST の脅威の評価手法となる可能性がある。

はじめに、複数の異なる周波数の電磁波の照射により機器内部で周波数変換が生じ、照射した電磁波と異なる周波数の電磁波が生成されることを示す。そして、2.4.4 節で Echo TEMPEST の脅威が確認された USB キーボードを用いた実験により、周波数変換により生成された電磁波によって Echo TEMPEST が引き起こされることを示す。

## B.1　複数周波数が非線形素子に伝搬することで生じた電磁波により誘発される Echo TEMPEST

はじめに、2 つの周波数の入力により周波数変換がなされる周波数混合器について述べる。そして、周波数変換により生じた電磁波により照射した電磁波と異なる周波数で Echo TEMPEST が誘発される可能性について述べる。

無線通信などの分野では、2 つの周波数の乗算に周波数混合器が利用される。具体的な例として SDR のようなスーパーヘテロダイン方式の送受信機が挙げられ、ある周波数の信号を所望する周波数に変換する際に利用されている。2 つの周波数 $f_1$, $f_2$ が周波数混合器に対して入力された場合、周波数変換により $(f_1 + f_2)$ および $(f_1 - f_2)$ の周波数が生成される。

このような周波数変換を機器内部で実行する場合、通常、機器の設計段階でダイオードやトランジスタなどが有する非線形特性を用いて専用の回路として実装される。一方、現在広く普及している機器の内部にはダイオードやトランジスタなどの様々な非線形素子が多数実装されている。そのため、機器外部から機器内部に効率良く伝搬する周波数が照射された場合、機器の設計者が意図しない部位が周波

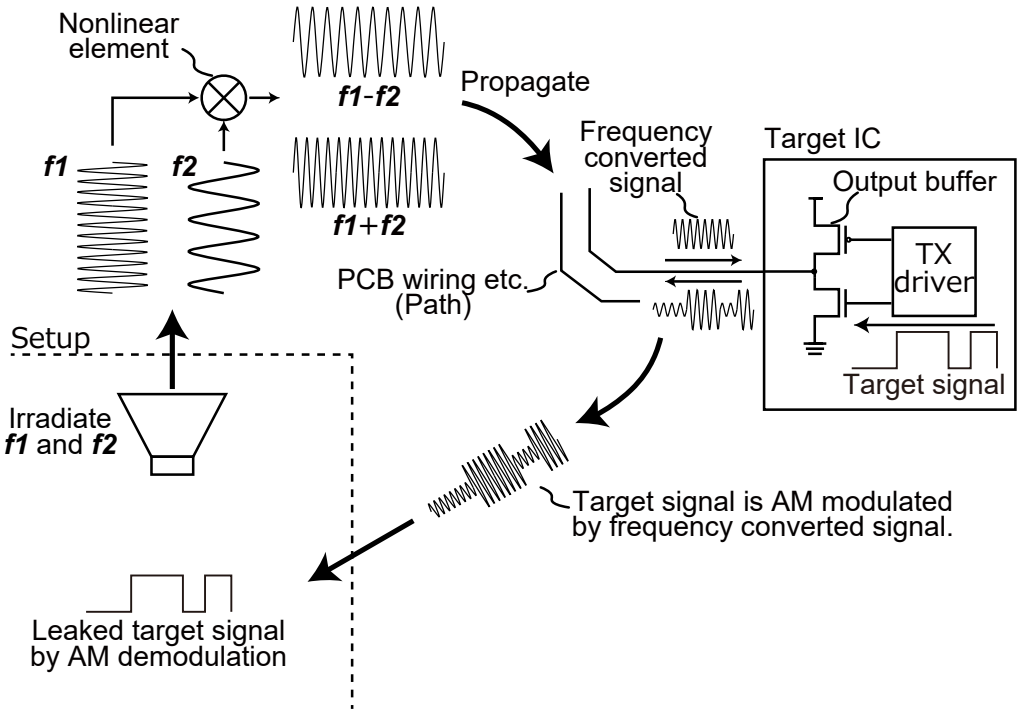


図 B.1. 複数周波数の照射により引き起こされる Echo TEMPEST の概念図

数混合回路のように振る舞い、機器内部で周波数変換が生じる可能性がある。そして、周波数変換により生成された電磁波が 2 章で述べたターゲット回路に伝搬することで Echo TEMPEST が生じる。周波数変換により生成された電磁波が Echo TEMPEST を誘発する概念図を図 B.1 に示す。

## B.2 複数周波数の照射による周波数変換と周波数変換により生じた電磁波により誘発される Echo TEMPEST の実証実験

複数周波数の照射により機器内部で周波数変換が生じ、照射した周波数と異なる周波数で Echo TEMPEST を誘発することを示す。図 B.2 に計測環境、表 B.1 に使用した計測環境およびパラメタを示す。

本実験では、2.4.4 節で Echo TEMPEST の脅威が確認された USB キーボード

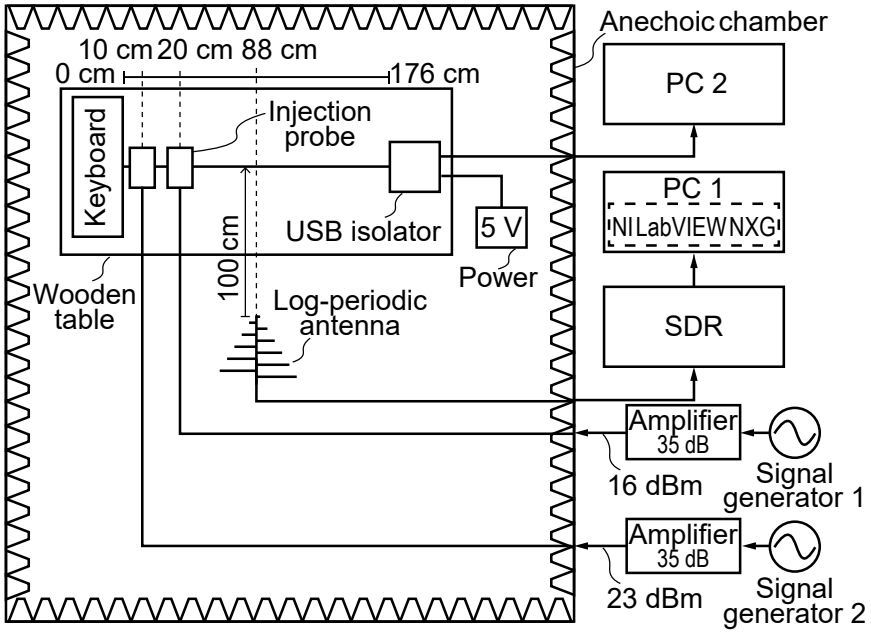


図 B.2. USB キーボードに対する複数周波数の照射により誘発される Echo TEMPEST の計測環境

を用いた。計測対象となる USB キーボードは、電波暗室内の高さ 75 cm の木製テーブル上に設置し、USB アイソレータを介して電波暗室外の PC に接続した。本実験では、2 つの信号発生器から異なる周波数の $f_1$, $f_2$ を生成し増幅した後に、USB キーボードのキーボード部から 10, 20 cm の位置に設置したインジェクションプローブを用いて印加し、機器内部で生成された Echo を USB キーボードの伝送線路から 100 cm 離れた位置のログペリオディックアンテナで計測した。SDR のサンプリングレートは、USB キーボードの通信信号を欠損なく取得するために 20 MS/s とした。事前の計測により、799 MHz において Echo TEMPEST が成立することが確認されたため、周波数変換によって 799 MHz が得られるように、$f_1$ を 1129 MHz とし、$f_2$ を 330 MHz とした。また、当該の周波数における伝達特性を考慮し、$f_1$ の照射強度を 23 dBm、$f_2$ の照射強度を 16 dBm とした。

表 B.1. USB キーボードに対する複数周波数の照射により誘発される Echo TEMPEST の計測パラメタ

| 計測環境 | |
|---|---|
| SDR | Ettus Research, USRP X310 |
| SDR ドーターボード | Ettus Research, TwinRX 10-6000 MHz |
| SDR 制御ソフトウェア | NI, LabVIEW NXG 5.0 |
| 信号生成器 1 | Rohde & Schwarz, SMA100B |
| 信号生成器 2 | Keysight, N5181B |
| 高周波電力増幅器 | Mini-Circuits, ZFL2500VH |
| インジェクションプローブ | FCC, F-140 |
| 受信アンテナ | Schwarzbeck, USLP 9143 |
| USB キーボード | HP, SK-2025 |
| USB アイソレータ | Analog Devices, EVAL-ADuM4160EBZ |
| USB アイソレータ電源 | Texio, PA18-2B |
| **計測パラメタ** | |
| 周波数 $f_1$ | 1129 MHz |
| 周波数 $f_1$ 印加強度 | 23 dBm |
| 周波数 $f_2$ | 330 MHz |
| 周波数 $f_2$ 印加強度 | 16 dBm |
| サンプリングレート | 20 MS/s |
| SDR 中心周波数 | 799 MHz |
| 受信ゲイン | 93 dB |

はじめに、USB キーボードに対して $f_1$ および $f_2$ の周波数の電磁波を印加した際に生じる周波数変換によって、799 MHz の信号が生成されることを示す。図 B.3 にログペリオディックアンテナで受信した信号を周波数分析器で計測した際のスペクトルを示す。図 B.3 (a) や図 B.3 (b) のように、$f_1$ または $f_2$ のいずれかを印加しなかった場合には当該の周波数の生成は確認されない。一方、図 B.3 (c) に示すように、USB キーボードに対して $f_1$ および $f_2$ の周波数の電磁波を印加すること

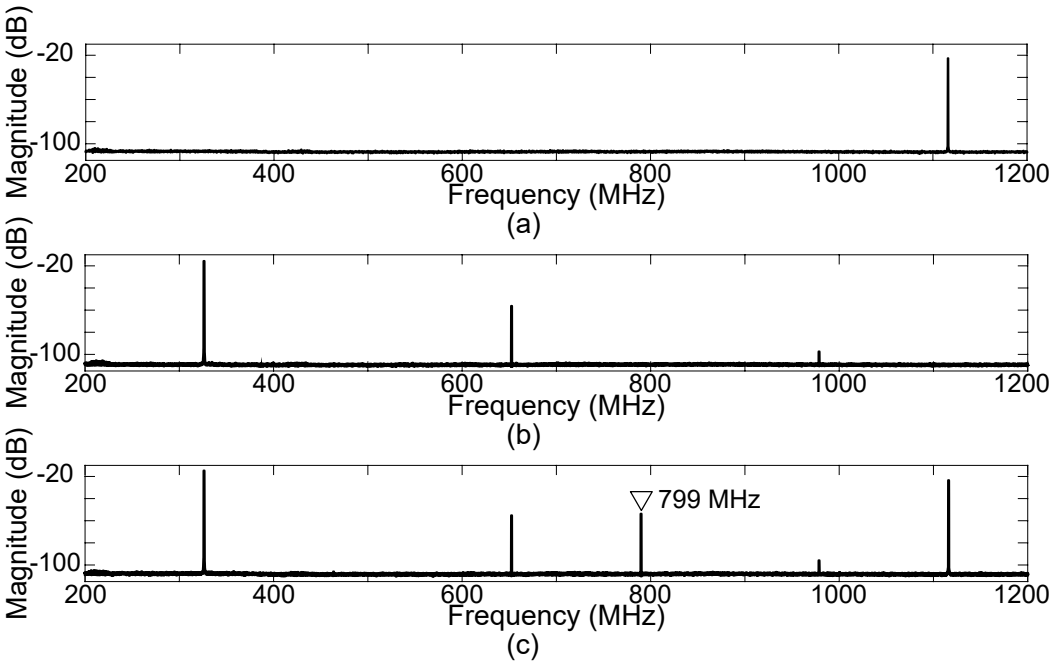


図 B.3. USB キーボードに対する複数周波数の印加時に計測された放射信号

で 799 MHz の信号が生成されていることが確認された。この結果より、機器内部に含まれる非線形素子が周波数混合器のように振る舞うことで周波数変換が生じ、印加した電磁波の周波数と異なる周波数の電磁波が生成されることが確認された。

図 B.4 に、複数周波数の照射により誘発された Echo TEMPEST の計測結果を示す。図 B.4 (a) は、USB キーボードと USB アイソレータ間の線路で定常的に伝送される信号のうち、ハンドシェイクパケットに着目した波形である。図 B.4 (b) は、$f_1$ および $f_2$ の電磁波を印加し、SDR の中心周波数を 799 MHz、受信ゲインを 93 dB に設定した際の受信信号を、包絡線検波した波形である。また、図 B.4 (c) は、図 B.4 (b) で得られた波形をしきい値と NRZI 符号化の原理に基づいて伝送信号を復元した波形である。図 B.4 (a) で得られた波形と同等の波形が復元されていることが確認された。図 B.4 (d) は、電磁波の印加を停止した際に従来の電磁情報漏えいの手法で計測された波形であり、伝送信号の漏えいは確認されない。

以上の結果より、機器に対する複数の異なる周波数の電磁波の印加により、印加

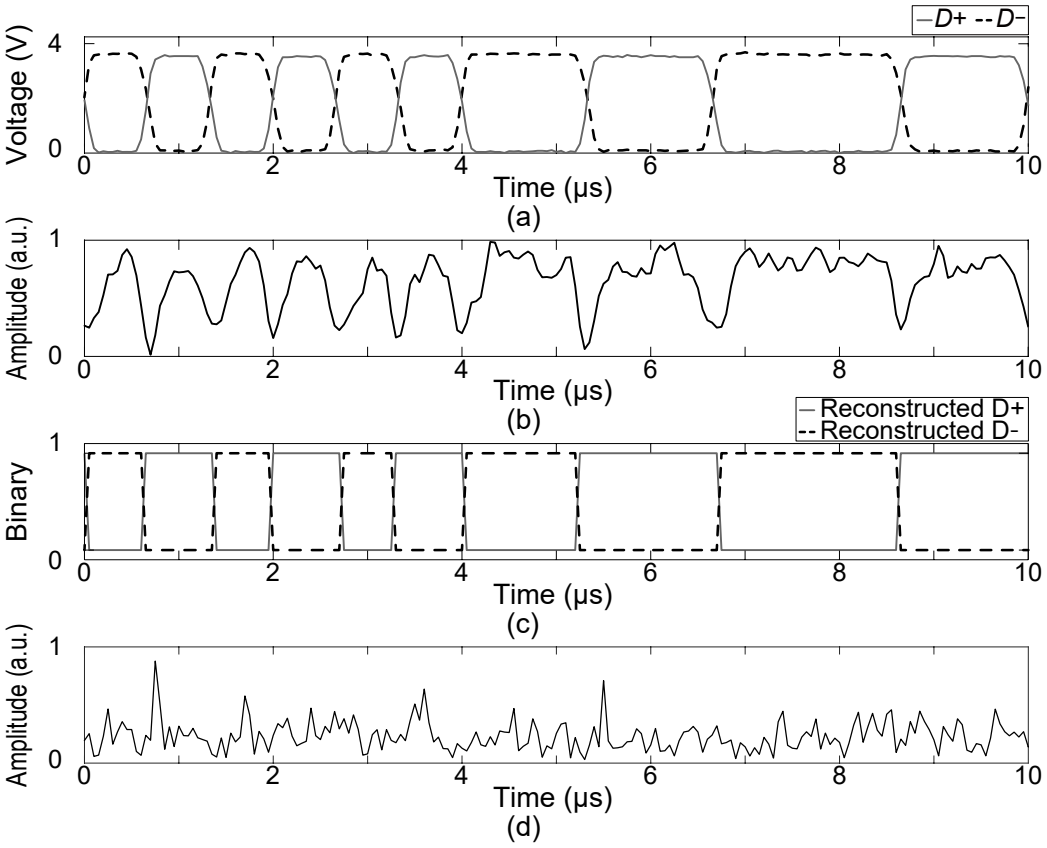


図 B.4. USB キーボードに対する複数周波数の照射により誘発される Echo TEMPEST の計測結果

された周波数とは異なる周波数で Echo TEMPEST が誘発されることが確認された。本手法により自己干渉波による Echo の変調度の低下の問題を抑制し、高精度な Echo TEMPEST の脅威の評価手法となる可能性が示された。

# 謝辞

本論文は、奈良先端科学技術大学院大学先端科学技術研究科情報セキュリティ工学研究室において筆者が行った研究をまとめたものです。

奈良先端科学技術大学院大学情報セキュリティ工学研究室林優一教授には、修士論文から引き続き本論文の主指導教員を引き受けて頂くと共に、丁寧かつ熱心なご指導とご鞭撻を賜りました。林教授から、研究や教育に対する姿勢や論文の執筆、発表資料の作成、日々の立ち振る舞い、研究室運営の基礎まで研究室生活の全てを学ばせて頂きました。また、多くの学会発表や国際共同研究の機会を与えて頂き、大変貴重な経験をさせて頂きました。ここに深謝の意を表すと共に、心より厚く御礼申し上げます。

同学ディペンダブルシステム学研究室井上美智子教授と同学ネットワークシステム学研究室岡田実教授には、修士論文から引き続き本論文の副指導教員を引き受けて頂きました。数々の有益なご指摘とご助言を賜ったことを心から謝意を表します。

同学情報セキュリティ工学研究室藤本大介助教には、修士論文から引き続き本論文の副指導教員を引き受けて頂きました。また、研究室生活において丁寧かつ熱心なご指導、ご鞭撻をはじめ、研究方針のご討論、実験のご指導やご助言、論文の執筆など、あらゆる方面で多大なご尽力を賜ったことを心から謝意を表します。

同学情報セキュリティ工学研究室 Youngwoo Kim 助教には、本論文の副指導教員を引き受けて頂きました。また、研究室生活において丁寧かつ熱心なご指導、ご鞭撻をはじめ、研究方針のご討論、実験のご指導やご助言、論文の執筆など、あらゆる方面で多大なご尽力を賜ったことを心から謝意を表します。

福知山公立大学情報学部衣川昌宏准教授には、研究方針のご討論、実験のご指導やご助言、論文の執筆など多大なご尽力を賜りました。衣川准教授からは、本論文に関わる多くの部分において技術的なご助言とご協力を賜ったことを心から謝意を表します。

東北大学電気通信研究所本間尚文教授と神戸大学大学院科学技術イノベーション研究科永田真教授には、意図的な電磁妨害により引き起こされる情報漏えいに関する検討において熱心なご討論とご助言を賜ったことを深く感謝申し上げます。

TELECOM Paris, Jean-Luc Danger 教授と Laurent Sauvage 博士には、同学へのインターンシップをはじめ、放射電磁波を用いた電子機器の個体識別手法に関して様々なご協力とご討論を賜ったことを深く感謝申し上げます。

電子情報通信学会ハードウェアセキュリティ研究会と同学会環境電磁工学研究会およびその他の研究会の関係各位には、本研究に関する熱心なご討論とご助言を賜ったことを深く感謝申し上げます。

奈良先端科学技術大学院大学情報セキュリティ工学研究室秘書の石谷由美様、大槻優花里様、佐山美奈子様、松永恵子様には、学会活動の事務手続きの代行や研究室運営などをはじめ、様々な面でお世話になったことを深く感謝申し上げます。

同学情報セキュリティ工学研究室を修了された同期と後輩の皆様には、実験にご協力頂くと共に、日々のご討論の機会を与えて頂きましたことを深く感謝申し上げます。特に、2019 年度に修了された川上莉穂さんには、意図的な電磁妨害により引き起こされる情報漏えいの高精度評価に関する検討においてご協力頂いたことを深く感謝申し上げます。また、2021 年度に修了された上田浩行さん、太刀掛彩希さん、西鳥羽陽さん、湯川大雅さんの精力的な取り組みに深く感謝申し上げます。

同学情報セキュリティ工学研究室に在籍する学生の皆様には、日々のご討論の機会を与えて頂くと共に研究室運営にご協力頂いたことを深く感謝申し上げます。特に、和田慎平さんには、博士後期課程の同期として研究の助言や議論だけでなく、精神的な支えとなって頂いたことを深く感謝申し上げます。また、高野誠也さんの意図的な電磁妨害により引き起こされる情報漏えいに関する検討への精力的な取り組みに深く感謝申し上げます。

日本学術振興会特別研究員制度により、研究費および経済的支援を頂いたことを深く感謝申し上げます。

公益財団法人アイコム電子通信工学振興財団と公益財団法人東電記念財団の奨学金給付制度により、経済的支援を頂いたことを深く感謝申し上げます。

最後に、博士後期課程までの生活を支え、学生生活を応援して頂いた家族に心から感謝の意を表します。

# 参考文献


[1] 内閣府, "Society 5.0." https://www8.cao.go.jp/cstp/society5_0/. Accessed: 2022-10-1.

[2] 情報処理推進機構, "情報セキュリティ白書 2022." https://www.ipa.go.jp/files/000100472.pdf, 2022. Accessed: 2022-10-1.

[3] 研究開発戦略センター, "Society 5.0 時代の 安心・安全・信頼を支える 基盤ソフトウエア技術." https://www.jst.go.jp/crds/pdf/2020/SP/CRDS-FY2020-SP-06.pdf, 2020. Accessed: 2022-10-1.

[4] "The big list of rtl-sdr supported software." https://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/, 11 Feb. 2014. Accessed: 2022-11-1.

[5] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?," *Comput. Secur.*, vol. 4, pp. 269–286, 1 Dec. 1985.

[6] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," in *Information Hiding* (D. Aucsmith, ed.), vol. 1525 of *Lecture notes in computer science*, pp. 124–142, Berlin, Heidelberg: Springer Berlin Heidelberg, 1998.

[7] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley, 14 Apr. 2008.

[8] E. MacAskill and J. Borger, "New nsa leaks show how us is bugging its european allies," *The Guardian*, 30 June 2013.

[9] Y. Su, D. Genkin, D. Ranasinghe, and Y. Yarom, "Usb snooping made easy : Crosstalk leakage attacks on usb hubs," in *SEC'17 Proceedings of the 26th USENIX Conference on Security Symposium*, pp. 1145–1161, 2017.

[10] J. L. Esteves, E. Cottais, and C. Kasmi, "Second order soft tempest: from internal cascaded electromagnetic interactions to long haul covert channels," in *2019 URSI Asia-Pacific Radio Science Conference (AP-RASC)*, pp. 1–3, IEEE, Mar. 2019.

[11] J. Choi, H.-Y. Yang, and D.-H. Cho, "Tempest comeback: A realistic audio

eavesdropping threat on mixed-signal socs," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, (New York, NY, USA), pp. 1085–1101, Association for Computing Machinery, 30 Oct. 2020.

[12] International Electrotechnical Commission, "Cispr 32:2015 electromagnetic compatibility of multimedia equipment - emission requirements," tech. rep., 31 Mar. 2015.

[13] H. S. Lee, D. H. Choi, K. Sim, and J.-G. Yook, "Information recovery using electromagnetic emanations from display devices under realistic environment," *IEEE Trans. Electromagn. Compat.*, vol. 61, pp. 1098–1106, Aug. 2019.

[14] P. de Meulemeester, B. Scheers, and G. A. E. Vandenbosch, "Eavesdropping a (ultra-)high-definition video display from an 80 meter distance under realistic circumstances," in *2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI)*, pp. 517–522, ieeexplore.ieee.org, July 2020.

[15] Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone, "A threat for tablet pcs in public space: Remote visualization of screen images using em emanation," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, (New York, NY, USA), pp. 954–965, Association for Computing Machinery, 3 Nov. 2014.

[16] N. Zhang, Y. Lu, Q. Cui, and Y. Wang, "Investigation of unintentional video emanations from a vga connector in the desktop computers," *IEEE Trans. Electromagn. Compat.*, vol. 59, pp. 1826–1834, Dec. 2017.

[17] V. Yli-Mayry, D. Miyata, N. Homma, T. Aoki, and Y. Hayashi, "On the evaluation of electromagnetic information leakage from mobile device screens," in *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*, pp. 1050–1052, IEEE, May 2018.

[18] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanations

of wired and wireless keyboards," in *USENIX security symposium*, vol. 1, (Montreal, Canada), pp. 1–16, USENIX Association Berkeley, CA, USA, 2009.

[19] M. Vuagnoux and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," in *2010 IEEE International Symposium on Electromagnetic Compatibility*, pp. 121–126, IEEE, July 2010.

[20] L. Wang and B. Yu, "Analysis and measurement on the electromagnetic compromising emanations of computer keyboards," in *2011 Seventh International Conference on Computational Intelligence and Security*, pp. 640–643, Dec. 2011.

[21] D.-J. Sim, H. S. Lee, J.-G. Yook, and K. Sim, "Measurement and analysis of the compromising electromagnetic emanations from usb keyboard," in *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, vol. 01, pp. 518–520, May 2016.

[22] T. Tosaka, K. Taira, Y. Yamanaka, A. Nishikata, and M. Hattori, "Feasibility study for reconstruction of information from near field observations of the magnetic field of laser printer," in *2006 17th International Zurich Symposium on Electromagnetic Compatibility*, pp. 630–633, IEEE, Feb. 2006.

[23] C. Ulaş, U. Aşık, and C. Karadeniz, "Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines," *Comput. Secur.*, vol. 58, pp. 250–267, 1 May 2016.

[24] H. W. Ott, *Electromagnetic Compatibility Engineering.* John Wiley & Sons, 20 Sept. 2011.

[25] C. R. Paul, *Introduction to Electromagnetic Compatibility.* John Wiley & Sons, 3 Jan. 2006.

[26] V. Yli-Mäyry, D. Miyata, N. Homma, Y. Hayashi, and T. Aoki, "Statistical test methodology for evaluating electromagnetic information leakage from mobile touchscreen devices," *IEEE Trans. Electromagn. Compat.*, vol. 61, pp. 1107–1114, Aug. 2019.

[27] T.-L. Song, Y.-R. Jeong, and J.-G. Yook, "Modeling of leaked digital video signal and information recovery rate as a function of snr," *IEEE Trans. Electromagn. Compat.*, vol. 57, pp. 164–172, Apr. 2015.

[28] F. Elibol, U. Sarac, and I. Erer, "Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system," in *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, pp. 1767–1771, Aug. 2012.

[29] Y. Hayashi, N. Homma, Y. Toriumi, K. Takaya, and T. Aoki, "Remote visualization of screen images using a pseudo-antenna that blends into the mobile environment," *IEEE Trans. Electromagn. Compat.*, vol. 59, pp. 24–33, Feb. 2017.

[30] P. Juyal, S. Adibelli, N. Sehatbakhsh, and A. Zajic, "A directive antenna based on conducting disks for detecting unintentional em emissions at large distances," *IEEE Trans. Antennas Propag.*, vol. 66, pp. 6751–6761, Dec. 2018.

[31] H. Sekiguchi and S. Seto, "Study on maximum receivable distance for radiated emission of information technology equipment causing information leakage," *IEEE Trans. Electromagn. Compat.*, vol. 55, pp. 547–554, June 2013.

[32] P. De Meulemeester, B. Scheers, and G. A. E. Vandenbosch, "A quantitative approach to eavesdrop video display systems exploiting multiple electromagnetic leakage channels," *IEEE Trans. Electromagn. Compat.*, vol. 62, pp. 663–672, June 2020.

[33] International Telecommunication Union Telecommunication Standardization Sector, "K.115: Mitigation methods against electromagnetic security threats," tech. rep., https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12664&lang=en, Nov. 2015.

[34] V. Bîndar, M. Popescu, and A. Vulpe, "Considerations regarding shielding effectiveness and testing of electromagnetic protected enclosures used in communications security," in *2014 10th International Conference on Com-*

*munications (COMM)*, pp. 1–6, ieeexplore.ieee.org, May 2014.

[35] C. Kasmi, D. Coiffard, M. Hélier, and M. Darces, "Performance analysis of a power network counter-tempest filter in realistic cabling scenarios," in *2014 International Symposium on Electromagnetic Compatibility*, pp. 1166–1169, ieeexplore.ieee.org, Sept. 2014.

[36] H. Sekiguchi and S. Seto, "Estimation of receivable distance for radiated disturbance containing information signal from information technology equipment," in *2011 IEEE International Symposium on Electromagnetic Compatibility*, pp. 942–945, Aug. 2011.

[37] 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, pp. 314–321, Aug. 2004.

[38] E. Savage and W. Radasky, "Overview of the threat of iemi (intentional electromagnetic interference)," in *2012 IEEE International Symposium on Electromagnetic Compatibility*, pp. 317–322, Aug. 2012.

[39] International Electrotechnical Commission, "Electromagnetic compatibility (emc) - part 4-3 : Testing and measurement techniques - radiated, radio-frequency, electromagnetic field immunity test," Tech. Rep. IEC 61000-4-3:2020, https://webstore.iec.ch/publication/59849, 8 Sept. 2020.

[40] M. W. Wik and W. A. Radasky, "Development of high-power electromagnetic (hpem) standards," *IEEE Trans. Electromagn. Compat.*, vol. 46, pp. 439–445, Aug. 2004.

[41] D. V. Giri, F. M. Tesche, and C. E. Baum, "An overview of high-power electromagnetic (hpem) radiating and conducting systems," *URSI Radio Science Bulletin*, vol. 2006, no. 318, pp. 6–12, 2006.

[42] W. A. Radasky, "Fear of frying electromagnetic weapons threaten our data networks. here's how to stop them," *IEEE Spectrum*, vol. 51, pp. 46–51, Sept. 2014.

[43] International Telecommunication Union Telecommunication Standardiza-

tion Sector, “K.87: Guide for the application of electromagnetic security requirements –overview,” Tech. Rep. K.87, 2022.

[44] International Electrotechnical Commission, “Electromagnetic compatibility (emc) part 2-13: Environment high-power electromagnetic (hpem) environments radiated and conducted,” Tech. Rep. IEC 61000-2-13:2005, https://webstore.iec.ch/publication/4131, 9 Mar. 2005.

[45] International Telecommunication Union Telecommunication Standardization Sector, “K.81: High-power electromagnetic immunity guide for telecommunication systems,” Tech. Rep. K.81, https://www.itu.int/rec/T-REC-K.81-201606-I/en, 29 June 2016.

[46] International Electrotechnical Commission, “Electromagnetic compatibility (emc) - part 1-5: General - high power electromagnetic (hpem) effects on civil systems,” Tech. Rep. IEC TR 61000-1-5:2004, https://webstore.iec.ch/publication/4124, 15 Nov. 2004.

[47] S. Ordas, L. Guillaume-Sage, and P. Maurine, “Em injection: Fault model and locality,” in *2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 3–13, IEEE, Sept. 2015.

[48] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, “Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures,” *Proc. IEEE*, vol. 100, pp. 3056–3076, Nov. 2012.

[49] P. Maurine, “Techniques for em fault injection: Equipments and experimental results,” in *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pp. 3–4, ieeexplore.ieee.org, Sept. 2012.

[50] Y.-I. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, and H. Sone, “Non-invasive trigger-free fault injection method based on intentional electromagnetic interference,” *Non-Invasive Attack Testing Workshop, NIAT-2011*, pp. 1–4, 2011.

[51] M. Dumont, M. Lisart, and P. Maurine, “Electromagnetic fault injection : how faults occur ?,” in *2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 9–16, 2019.

[52] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Yongdae Kim, and Wenyuan Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*, pp. 145–159, IEEE, May 2013.

[53] C. Kasmi and J. Lopes Esteves, "Iemi threats for information security: Remote command injection on modern smartphones," *IEEE Trans. Electromagn. Compat.*, vol. 57, pp. 1752–1755, Dec. 2015.

[54] Y. Zhong, Q. Huang, T. Enomoto, S. Seto, K. Araki, and C. Hwang, "Measurement-based characterization of buzz noise in wireless devices," in *2018 IEEE Symposium on Electromagnetic Compatibility, Signal Integrity and Power Integrity (EMC, SI PI)*, pp. 134–138, July 2018.

[55] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap 'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 620–637, IEEE, May 2019.

[56] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Trans. Microw. Theory Tech.*, vol. 69, pp. 2642–2650, May 2021.

[57] K. Wang, R. Mitev, C. Yan, X. Ji, A.-R. Sadeghi, and W. Xu, "Ghosttouch: Targeted attacks on touchscreens without physical touch," in *31st USENIX Security Symposium (USENIX Security 22). USENIX Association, Boston, MA. https://www. usenix. org/conference/usenixsecurity22/presentation/wang-kai*, pp. 1543–1559, 2022.

[58] S. Köhler, R. Baker, and I. Martinovic, "Signal injection attacks against ccd image sensors," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '22, (New York, NY, USA), pp. 294–308, Association for Computing Machinery, 30 May 2022.

[59] W. Zhang, S. Xia, X. Fang, X. Wang, T. Enomoto, H. Shumiya, K. Araki, and C. Hwang, "A spice-compatible model to simulate rfi-induced buzz

noise problem in a camera," *IEEE Trans. Electromagn. Compat.*, pp. 1–12, 2022.

[60] J. M. Rabaey, *Digital Integrated Circuits: A Design Perspective*. Prentice Hall, 1996.

[61] S.-M. s. Kang and Y. Leblebici, *CMOS Digital Integrated Circuits Analysis & Design*. New York, NY: McGraw-Hill Education, 4 ed., 29 Oct. 2002.

[62] U. Nanda and S. K. Pattnaik, "Universal asynchronous receiver and transmitter (uart)," in *2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 01, pp. 1–5, Jan. 2016.

[63] USB Implementers Forum, "Universal serial bus specification revision 2.0," Apr. 2000.

[64] D. Fujimoto, Y. Hayashi, A. Beckers, J. Balasch, B. Gierlichs, and I. Verbauwhede, "Detection of iemi fault injection using voltage monitor constructed with fully digital circuit," in *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*, pp. 753–755, ieeexplore.ieee.org, May 2018.

[65] N. Miura, Z. Najm, W. He, S. Bhasin, X. T. Ngo, M. Nagata, and J.-L. Danger, "Pll to the rescue: A novel em fault countermeasure," in *2016 53rd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, ieeexplore.ieee.org, June 2016.

[66] C. Kasmi, J. Lopes-Esteves, N. Picard, M. Renard, B. Beillard, E. Martinod, J. Andrieu, and M. Lalande, "Event logs generated by an operating system running on a cots computer during iemi exposure," *IEEE Trans. Electromagn. Compat.*, vol. 56, pp. 1723–1726, Dec. 2014.

[67] J. F. Dawson, I. D. Flintoft, P. Kortoci, L. Dawson, A. C. Marvin, M. P. Robinson, M. Stojilovic, M. Rubinstein, B. Menssen, H. Garbe, W. Hirschi, and L. Rouiller, "A cost-efficient system for detecting an intentional electromagnetic interference (iemi) attack," in *2014 International Symposium on Electromagnetic Compatibility*, pp. 1252–1256, Sept. 2014.

[68] A. K. Bellamkonda, P. H. Rao, and S. Saxena, “Intentional electromagnetic interference reception in 0.5–2.0 ghz,” *IEEE Trans. Electromagn. Compat.*, pp. 1–7, 2022.

[69] 経 済 産 業 省, “情 報 セ キ ュ リ テ ィ 管 理 基 準,” tech. rep., https://www.meti.go.jp/policy/netsecurity/is-kansa/, 2016.

[70] T.-L. Song, Y.-R. Jeong, H.-S. Jo, and J.-G. Yook, “Noise-jamming effect as a countermeasure against tempest during high-speed signaling,” *IEEE Trans. Electromagn. Compat.*, vol. 57, pp. 1491–1500, Dec. 2015.

[71] Y. Suzuki and Y. Akiyama, “Jamming technique to prevent information leakage caused by unintentional emissions of pc video signals,” in *2010 IEEE International Symposium on Electromagnetic Compatibility*, pp. 132–137, July 2010.

[72] M. Ossmann, “The nsa playset: A year of toys and tools,” *black hat USA (2015-8)*, 2015.

[73] “Nsa ant catalog.” `https://www.eff.org/document/20131230-appelbaum-nsa-ant-catalog`, 6 Jan. 2014. Accessed: 2022-6-20.

[74] Y. Kayano, M. Tanaka, and H. Inoue, “Identifying the frequency response of common-mode current on a cable attached to a pcb,” *IEICE Transactions on Electronics*, vol. E87-C, no. 8, pp. 1268–1276, 2004.

[75] Hwan-Woo Shim and T. H. Hubing, “Model for estimating radiated emissions from a printed circuit board with attached cables due to voltage-driven sources,” *IEEE Trans. Electromagn. Compat.*, vol. 47, pp. 899–907, Nov. 2005.

[76] B. Archambeault, S. Connor, M. S. Halligan, J. L. Drewniak, and A. E. Ruehli, “Electromagnetic radiation resulting from pcb/high-density connector interfaces,” *IEEE Trans. Electromagn. Compat.*, vol. 55, pp. 614–623, Aug. 2013.

[77] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J.-L. Danger, “Analysis of electromagnetic information leakage from cryp-

tographic devices with different physical structures," *IEEE Trans. Electromagn. Compat.*, vol. 55, pp. 571–580, June 2013.

[78] 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, IEEE, June 2008.

[79] S. Adee, "The hunt for the kill switch," *IEEE Spectrum*, vol. 45, pp. 34–39, May 2008.

[80] 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, IEEE, Nov. 2009.

[81] 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.

[82] R. Rad, J. Plusquellic, and M. Tehranipoor, "Sensitivity analysis to hardware trojans using power supply transient signals," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 3–7, June 2008.

[83] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty, "Towards trojan-free trusted ics: Problem analysis and detection scheme," in *2008 Design, Automation and Test in Europe*, pp. 1362–1365, Mar. 2008.

[84] G. Zarrinchian and M. S. Zamani, "Latch-based structure: A high resolution and self-reference technique for hardware trojan detection," *IEEE Trans. Comput.*, vol. 66, pp. 100–113, Jan. 2017.

[85] J. He, Y. Zhao, X. Guo, and Y. Jin, "Hardware trojan detection through chip-free electromagnetic side-channel statistical analysis," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 25, pp. 2939–2948, Oct. 2017.

[86] A. Bazzazi, M. T. Manzuri Shalmani, and A. M. A. Hemmatyar, "Hardware trojan detection based on logical testing," *J. Electron. Test.*, vol. 33, pp. 381–395, 1 Aug. 2017.

[87] Y. Tang, L. Fang, and S. Li, "Activity factor based hardware trojan detection and localization," *J. Electron. Test.*, vol. 35, pp. 293–302, 1 June 2019.

[88] L. N. Nguyen, B. B. Yilmaz, M. Prvulovic, and A. Zajic, "A novel golden-chip-free clustering technique using backscattering side channel for hardware trojan detection," in *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, IEEE, 7 Dec. 2020.

[89] A. Greenberg, "Planting tiny spy chips in hardware can cost as little as $200," *Wired*, 10 Oct. 2019.

[90] J. Harrison, N. Asadizanjani, and M. Tehranipoor, "On malicious implants in pcbs throughout the supply chain," *Integration, the VLSI Journal*, vol. 79, pp. 12–22, July 2021.

[91] M. Kinugawa, D. Fujimoto, and Y. Hayashi, "Electromagnetic information extortion from electronic devices using interceptor and its countermeasure," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, no. 4, pp. 62–90, 2019.

[92] S. Wakabayashi, S. Maruyama, T. Mori, S. Goto, M. Kinugawa, Y.-I. Hayashi, and M. Smith, "A feasibility study of radio-frequency retroreflector attack," in *WOOT@ USENIX Security Symposium*, 2018.

[93] "The big hack: How china used a tiny chip to infiltrate u.s. companies," *Bloomberg News*, 4 Oct. 2018.

[94] D. Mehta, H. Lu, O. P. Paradis, M. A. M. S., M. T. Rahman, Y. Iskander, P. Chawla, D. L. Woodard, M. Tehranipoor, and N. Asadizanjani, "The big hack explained: Detection and prevention of pcb supply chain implants," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 16, pp. 1–25, 27 Aug. 2020.

[95] 澁谷紳一, "建築におけるシールド技術を用いた電磁波セキュリティ対策法," **電子情報通信学会 通信ソサイエティマガジン**, vol. 2009, no. 10, pp. 28–35, 2009.

[96] D. Fujimoto, S. Nin, Y.-I. Hayashi, N. Miura, M. Nagata, and T. Mat-

sumoto, “A demonstration of a ht-detection method based on impedance measurements of the wiring around ics,” *IEEE Trans. Circuits Syst. Express Briefs*, vol. 65, pp. 1320–1324, Oct. 2018.

[97] 西鳥羽陽, 鍛治秀伍, 衣川昌宏, 藤本大介, and 林優一, “オンチップセンサを用いた線路上のハードウェアトロージャン検知に関する基礎検討,” **信学技報**, vol. 121, no. 206, pp. 38–42, 2021.

[98] H. Li, J. Van Kerrebrouck, O. Caytan, H. Rogier, J. Bauwelinck, P. Demeester, and G. Torfs, “Self-interference cancellation enabling high-throughput short-reach wireless full-duplex communication,” *IEEE Trans. Wireless Commun.*, vol. 17, pp. 6475–6486, Oct. 2018.

[99] J. Xing, S. Ge, Y. Liu, Q. Wang, and J. Meng, “Analysis of dac impact on digital-controlled self-interference cancellation,” in *2019 Joint International Symposium on Electromagnetic Compatibility, Sapporo and Asia-Pacific International Symposium on Electromagnetic Compatibility (EMC Sapporo/APEMC)*, pp. 544–547, June 2019.

# 業績リスト

## 論文誌（査読有り）

1. Shugo Kaji, Daisuke Fujimoto, Masahiro Kinugawa, and Yuichi Hayashi, “Echo TEMPEST: EM Information Leakage Induced by IEMI for Electronic Devices,” *IEEE Transactions on Electromagnetic Compatibility*, 2022.（採録決定済み）（2 章）

2. Shugo Kaji, Masahiro Kinugawa, Daisuke Fujimoto, and Yuichi Hayashi, “Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1115–1121, Aug. 2019, doi: 10.1109/TEMC.2018.2849105.（3 章）

3. Youngwoo Kim, Daisuke Fujimoto, Shugo Kaji, Shinpei Wada, Hyunwook Park, Daehwan Lho, Joungho Kim, and Yuichi Hayashi, “Segmentation Method based Modeling and Analysis of a Glass Package Power Distribution Network (PDN),” *Nonlinear Theory and Its Applications (IEICE)*, vol. 11, no. 2, pp. 170-188, Apr., 2020, doi: 10.1587/nolta.11.170.

## 国際会議（査読有り）

1. Shugo Kaji, Daisuke Fujimoto, Youngwoo Kim, Yuichi Hayashi, “A Fundamental Evaluation of EM Information Leakage Induced by IEMI for a Device with Differential Signaling,” in *2021Asia-Pacific International Symposium on Electromagnetic Compatibility(APEMC2021)*, 2021, SS-02-7, doi: 10.1109/APEMC49932.2021.9597081.（2 章）

2. Shugo Kaji, Masahiro Kinugawa, Daisuke Fujimoto, and Yuichi Hayashi, “Data Injection Attacks Using a Hardware Trojan on a Transmission Line,” in *IEEE International Symposium on Electromagnetic Compatibility and IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*,

2018, TU-PM-I-TC-05-3, doi: 10.1109/ISEMC.2018.8394010.（3 章）

3. Shugo Kaji, Masahiro Kinugawa, Daisuke Fujimoto, Laurent Sauvage, Jean-Luc Danger, and Yuichi Hayashi, “Method for Identifying Individual Electronic Devices Focusing on Differences in Spectrum Emissions,” in *2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility (EMC Sapporo & APEMC 2019)*, 2019, ThuPM2C.2.

## 国内会議・シンポジウム等における発表（査読無し）

1. 高野誠也, 鍛治秀伍, 衣川昌宏, 藤本大介, 林優一, “意図的な電磁妨害により生ずる情報漏えいのモデル化に向けた評価環境の構築,” 信学技報, 122 (206), pp. 93-96, 2022.
2. 鍛治秀伍, 太刀掛彩希, 藤本大介, 林優一, “静電容量センサの出力分布に着目した ID 生成手法に関する基礎検討,” 信学技報,122 (11), pp. 19-23, 2022.
3. 鍛治秀伍, 藤本大介, 林優一, “位相限定相関法を用いた意図的な電磁情報漏えい耐性評価法,” 2022 年 電子情報通信学会総合大会, A-19-5, 2022.
4. 湯川大雅, 鍛治秀伍, 藤本大介, 林優一, “通信線路上のハードウェアトロイによる電磁情報漏えい評価法の検討～変調度と放射強度に着目した評価～,” 信学技報, 121 (413), pp.153-157, 2022.
5. 太刀掛彩希, 鍛治秀伍, 藤本大介, 林優一, “静電容量センサを用いたプリント基板の個体差の検出に関する基礎検討,” 信学技報, 121 (206), pp. 49-52, 2021.
6. 西鳥羽陽, 鍛治秀伍, 衣川昌宏, 藤本大介, 林優一, “オンチップセンサを用いた線路上のハードウェアトロージャン検知に関する基礎検討,” 信学技報, 121 (206), pp. 38-42, 2021.
7. 鍛治秀伍, 藤本大介, 林優一, “複数の周波数印加による電磁的情報漏えい誘発に関する検討,” 2021 年暗号と情報セキュリティシンポジウム (SCIS2021), 2D3-4, 2021.

8. 上田浩行, 鍛治秀伍, 藤本大介, キムヨンウ, 林優一, “接触境界の表面粗さとトルク値がコネクタ高周波特性に与える影響に関する基礎検討,” 信学技報, 120 (425),pp. 40-43, 2021.

9. Hiroyuki Ueda, Shugo Kaji, Youngwoo Kim, Daisuke Fujimoto, Taiki Kitazawa, Takashi Kasuga, and Yuichi Hayashi, “Fundamental Evaluation of Impedance Variations in the Connector Caused by High-Frequency Noise Propagation,” 信学技報, 120 (275), pp. 34-38, 2020.

10. 鍛治秀伍, 藤本大介, 衣川昌宏, 林優一, “意図的に引き起こされる電磁的情報漏えい評価法の検討 ～デジタル出力回路のインピーダンス変化に着目した評価～,” 信学技報, 120 (211), pp. 13-17, 2020.（2 章）

11. 鍛治秀伍, 藤本大介, 林優一, “意図的な電磁妨害時に生ずる情報漏えいの基礎評価,” 信学技報, 120 (83), pp. 25 - 28, 2020.（2 章）

12. 鍛治秀伍, 藤本大介, 衣川昌宏, 林優一, “電子機器への連続波注入による強制的な電磁情報漏えい誘発に関する基礎検討,” 2020 年暗号と情報セキュリティシンポジウム (SCIS 2020), 3E3-3, 2020.（2 章）

13. 川上莉穂, 鍛治秀伍, 衣川昌宏, 藤本大介, 林優一, “複数のデータ伝送路を有する IC から強制的に引き起こされる電磁的情報漏えいに関する検討,” ハードウェアセキュリティフォーラム 2019, 2019.

14. 鍛治秀伍, 衣川昌宏, 藤本大介, 林優一, “電磁的情報漏えいを強制的に誘発する照射周波数推定法に関する基礎検討,” 信学技報, 119 (143), pp. 235-238, 2019.

15. 川上莉穂, 鍛治秀伍, 衣川昌宏, 藤本大介, 林優一, “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,” 信学技報, 119 (2), pp. 31-35, 2019.

16. 鍛治秀伍, 衣川昌宏, 藤本大介, Laurent Sauvage, Jean-Luc Danger, 林優一, “製造・実装ばらつきに起因する放射スペクトルの違いを用いた電子機器の個体識別手法に関する基礎検討,” 信学技報, 118 (458), pp.163-167, 2019.

17. 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,” 信学技報, 118 (162), pp.49-54, 2018.（3 章）

18. 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.（3 章）

## 招待講演

1. 鍛治秀伍, “模造半導体とハードウェアトロージャンが引き起こすセキュリティ脅威,” 電子材料・デバイス技術専門委員会デバイス・ハードウェアセキュリティ技術分科会, 2022.

2. Shugo Kaji, Daisuke Fujimoto, Masahiro Kinugawa and Yuichi Hayashi, “Fundamental Study on Forcible EM Information Leakage Caused by Continuous Waves Injection into Electronic Devices,” *The 16th International Workshop on Security (IWSEC 2021)*, 2021.

3. Shugo Kaji, Masahiro Kinugawa, Daisuke Fujimoto, and Yuichi Hayashi, “Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan,” *IEEE EMC-S Japan Joint / Sendai Chapter*, 2020.

## 外部資金

1. 日本学術振興会, “電磁的情報漏えいの脅威に対抗するトロージャンフリーなハードウェア設計技術の開拓,”JP20J14937, 日本学術振興会特別研究員 (DC2), 2020 – 2022.

## 受賞

1. Richard B. Schulz Award for the Best EMC Transactions Paper - Honorable Mention, “Data Injection Attack against Electronic Devices with Locally Weakened Immunity using a Hardware Trojan,”IEEE Electromagnetic Compatibility Society, 2020.
2. ハードウェアセキュリティ研究会若手優秀賞, “意図的に引き起こされる電磁的情報漏えい評価法の検討 〜 デジタル出力回路のインピーダンス変化に着目した評価 〜,” 電子情報通信学会 ハードウェアセキュリティ研究会, 2020.
3. EMCJ 若手研究者発表会 JIEP 電磁特性技術委員会賞, “意図的な電磁妨害時に生ずる情報漏えいの基礎評価,” 一般社団法人エレクトロニクス実装学会 電磁特性技術委員会, 2020.
4. 暗号と情報セキュリティシンポジウム論文賞, “電子機器への連続波注入による強制的な電磁情報漏えい誘発に関する基礎検討,” 電子情報通信学会 情報セキュリティ研究会, 2020.
5. 奈良先端科学技術大学院大学, 優秀学生, 2019.
6. ハードウェアセキュリティサマーセミナー最優秀ポスター賞, “物理構造に着目した電磁的情報漏えいを誘発させる照射周波数推定法に関する検討,” 2019.
7. ハードウェアセキュリティ夏のワークショップ最優秀ポスター賞, “不正な回路改変を用いた機器のイミュニティ操作に関する研究,” 2018.