高信頼 AI エッジコンピューティングの基盤となる AI ハードウェアセキュリティの開拓

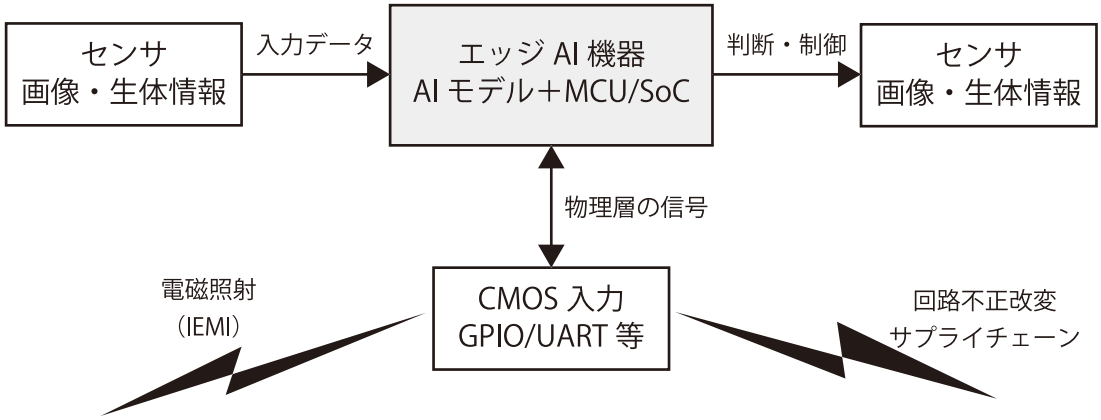
代表研究者　　衣川　昌宏　　福知山公立大学　情報学部　准教授
共同研究者　　林　優一　　奈良先端科学技術大学院大学　先端科学技術研究科　教授

1 研究の目的

本研究調査の目的は、社会インフラ、人命、生活支援に用いられるエッジ AI 機器を対象に、AI の判断そのものだけでなく、AI へ入力されるハードウェア信号の完全性を守るための AI ハードウェアセキュリティを開拓することである。クラウドへ常時接続される AI とは異なり、エッジ AI は端末内でセンシング、認識、判断、制御を完結できる。その反面、端末が物理環境に露出し、かつ出荷後は同じ電子回路を長期間使い続けるため、ソフトウェア更新だけでは対処しにくい脆弱性が残る。

自動車の運転支援、ヘルスケア機器、河川・電力・ガスなどの監視制御、工場の計装機器、家庭内のオートメーション機器では、センサ値が AI の判断を左右し、その判断が人や設備に直接作用する。したがって、センサ値や内部通信がハードウェア層で改ざんされた場合、AI モデルの認識精度が高くても、AI は誤った前提に基づいて正しくない制御を実行してしまう。情報通信システムの安全性を考える上では、ネットワークやアプリケーションの暗号化・認証に加え、端末内部で物理層から入力される信号の真正性を評価する必要がある。

本研究では、AI エッジコンピューティングの正常動作を妨げる代表的な物理層脅威として、図 1 に示すサプライチェーンに起因する回路不正改変と、外部から痕跡を残さず実施され得る電磁照射［1］による情報注入攻撃に着目した。特に本助成期間では、後者の電磁照射攻撃について、従来の単一周波数照射では困難であった再現性のあるビットレベル制御を、2 つの高周波を組み合わせることにより実現できることを実験的に示した。さらに、その脅威を AIoT/CPS 時代の情報セキュリティ問題として整理し、実装段階で講じるべき多層的な対策指針をまとめた。



AI の認識精度だけでなく、AI へ入力されるハードウェア信号の完全性を守ることが研究課題である

図 1　本研究が対象とする AI エッジ機器の脅威モデル

研究の最終的な狙いは、攻撃可能性を示すこと自体にとどまらない。攻撃原理を明らかにし、どの信号経路、どの回路構造、どのシステム運用が危険であるかを可視化することで、エッジ AI 機器の設計者が安全性を事前に評価できるようにすることが重要である。本研究成果は、環境電磁工学で扱われてきた意図的電磁妨害を、可用性の問題だけでなく、情報の完全性・真正性を侵害する情報セキュリティ問題として再定義するものである。

2 研究の背景と情報通信との関係

情報通信機器のセキュリティ設計では、通信路の暗号化、認証、アクセス制御、ログ監視など、デジタルデータとして観測できる層を中心に対策が構築されてきた。一方、端末内部の CMOS 入力、GPIO、UART、I2C、

SPI、センサインタフェースなどは、ソフトウェアから見れば信頼済みの入力として扱われることが多い。攻撃者が外部から電磁波を照射し、端末内部の入力端子に意図した論理値を発生させることができれば、上位層の認証や暗号処理を迂回し、正規の入力のように処理させる可能性が生じる。

従来の意図的電磁妨害は、高強度電磁界により装置を停止させる、誤動作させる、または破壊するという可用性・安全性の観点で研究されることが多かった。これに対して、近年問題となる低強度・制御型の電磁照射は、装置を停止させずに特定の論理値やセンサ値だけを変える点に特徴がある。この種の攻撃では、利用者や監視者が装置の継続動作を確認していても、内部で扱われる情報の完全性が侵害される可能性がある。AI エッジ機器においては、AI が扱う入力データが改ざんされるため、モデル自体が改ざんされていなくても判断結果が操作され得る。

既存の電磁波による情報注入研究では、CMOS 入力段に存在する ESD 保護ダイオードなどの非線形素子が、外部から結合した高周波を整流し、入力端子の直流電位を変化させることが知られていた。しかし、単一周波数を用いた従来手法では、対象機器の構造、配線、電源分配網、環境条件に結果が依存し、任意のビット列を安定に注入することは容易でなかった。特に高速なデジタル信号では、入力電位の遷移時間が信号幅に追いつかず、ビットの再現性が低下するという制約があった。

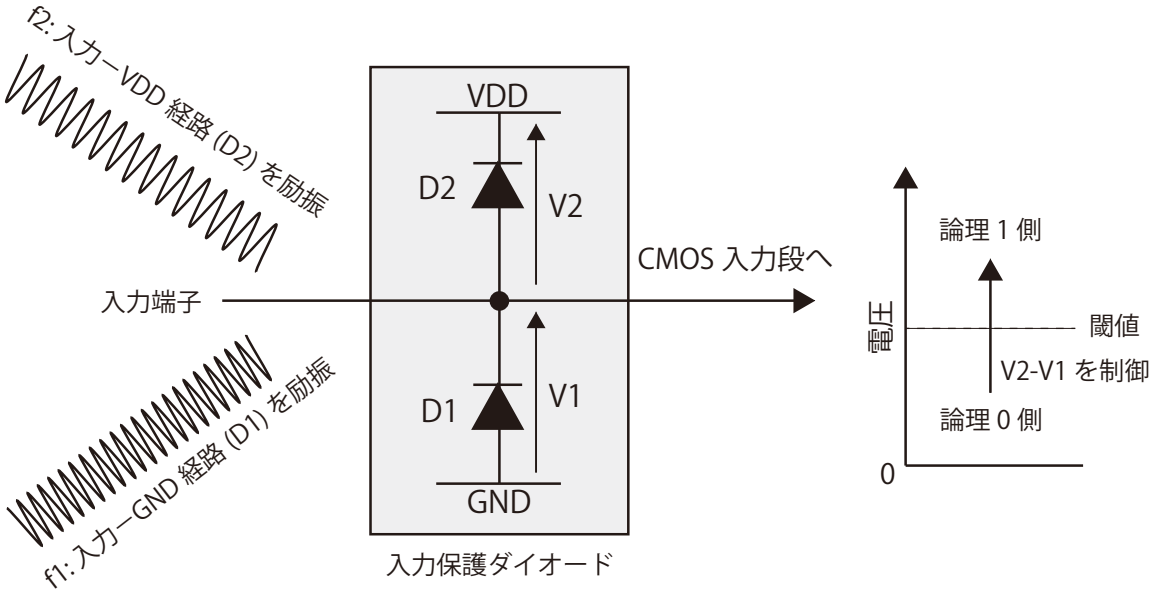
本研究は、この制約に対し、2 つの周波数を独立に用いることで CMOS 入力段の 2 つの電位経路を選択的に励振し、入力端子の実効電圧を論理しきい値の上下へ制御するという発想を採った。これにより、単に誤動作を発生させるのではなく、論理 0 と論理 1 を意図的に切り替え、通信プロトコルのビット列として入力させる可能性を評価した。この点で、本研究は電磁両立性、ハードウェアセキュリティ、情報通信システム設計を結びつける学際的研究である。

3 研究の方法

3-1 2 波電磁照射による入力電位制御の原理

CMOS デジタル IC の入力段には、入力端子と電源、入力端子とグラウンドの間に ESD 保護構造が配置される。外部から高周波電磁界が加わると、配線やパッケージ、プリント配線板、ケーブルを介して入力端子に高周波電圧が結合し、非線形素子である ESD 保護構造により直流成分が発生する。この直流成分が CMOS 入力の論理しきい値に対して十分大きくなると、ソフトウェアから見える入力値が変化する。

提案手法では、入力端子からグラウンド側へ現れる電位差を主に制御する周波数 f1 と、入力端子から電源側へ現れる電位差を主に制御する周波数 f2 を探索する。対象機器の電源分配網や配線のインピーダンスは周波数によって非対称であり、共振・反共振の影響を受ける。そのため、ある周波数はグラウンド側の経路を強く励振し、別の周波数は電源側の経路を強く励振する場合がある。本研究ではこの周波数依存性を利用し、2 つの電位成分の差を制御することで、入力端子を論理しきい値の上または下に移動させた。



2 つの周波数と振幅を組み合わせ、CMOS 入力の実効電圧を閾値の上下へ移動させ、ビット情報を操作する。

図 2　2 波電磁照射による CMOS 入力電位制御の概念

ビット列を注入する際には、一方の周波数を連続波として印加し、入力を基準状態に固定する。もう一方の周波数には、注入したいデータ列に対応する 100%振幅変調、すなわち OOK 変調を与える。OOK 変調によって f2 がオンとなる期間とオフとなる期間で入力電位が切り替わるため、論理 0 と論理 1 を時系列として発生させることができる。UART のような非同期シリアル通信では、ビット幅、ボーレート、スタートビット、データビット、ストップビットを変調信号側で設定することで、対象機器が正規の通信入力として解釈するデータ列を構成できる。

3-2 実験系の構築

実験では、法令と安全性に配慮して電磁照射を行うため、GTEM セルを用いた閉じた照射環境を構築した。信号発生器 2 台により f1 と f2 を生成し、必要に応じて f2 に OOK 変調を加え、合成器で 2 波を重畳した後、電力増幅器を介して GTEM セルへ入力した。対象機器の出力はオシロスコープ、スペクトラムアナライザ、または対象機器上のプログラムで観測し、照射波と出力変化の対応を確認した。

周波数探索の段階では、対象機器を接続し、所定範囲の周波数を掃引しながら出力の論理値変化を観測した。まず f1 候補を探索し、入力を安定した論理状態へ移動できる周波数と最小電力を求めた。次に f1 を印加した状態で f2 を掃引し、入力値を反転させる周波数と電力を求めた。この手順は対象 IC の内部回路、レイアウト、パッケージ構造を事前に知らないブラックボックス条件を想定しており、外部から観測できる入出力挙動だけで攻撃パラメタを同定できるかを評価するものである。

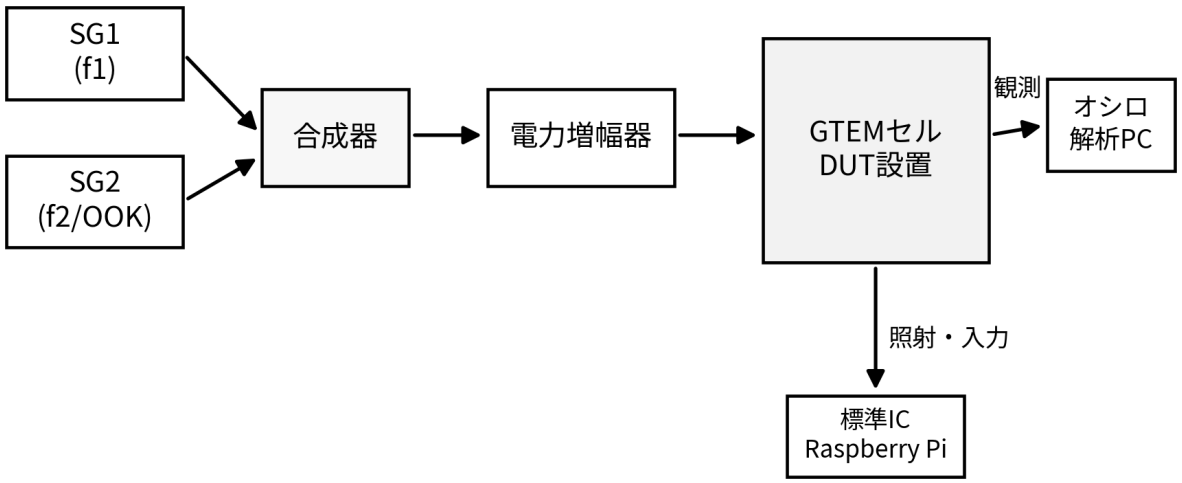


図 3　本研究で構築した 2 波電磁照射実験系の概要

評価対象は二段階に分けた。第一に、標準ロジック IC を実装した小規模なプリント配線板を用い、CMOS 入力段そのものに対して 2 波照射が論理反転を引き起こすかを検証した。第二に、実際の情報通信機器に近い実機として Raspberry Pi 4 Model B を用い、UART RX 入力に対して文字列を注入できるかを評価した。前者は攻撃原理の基礎実証、後者はシステムレベルでの実用性評価に位置付けた。

3-3 評価軸

本研究では、電磁波照射により単に出力が乱れるかどうかではなく、情報セキュリティ上の脅威として成立するかを評価軸に置いた。具体的には、第一に、同じ条件で同じ論理値を再現できるか、第二に、周波数と電力を系統的に探索できるか、第三に、論理値の切替が連続ビット列の速度に追従するか、第四に、実機上の通信インタフェースがそのビット列を正規の入力として処理するか、第五に、対策を設計層ごとに整理できるかを確認した。

この評価軸は、AI エッジ機器への応用を考える上で重要である。AI に入力されるデータが 1 ビットまたは 1 サンプルだけ偶然変化する場合と、攻撃者が時系列として意味を持つデータ列を注入できる場合とでは、脅威の質が大きく異なる。後者では、認証端末のコマンド入力、センサ値列、デバッグインタフェース、制御命令などが攻撃対象になり得るため、情報の完全性だけでなく、真正性、可用性、安全性にも影響が及ぶ。

4 研究結果

4-1 実験環境の整備と基礎理論実証

助成により、GTEM セル、高周波信号発生器、周辺計測機器を組み合わせた 2 波同時照射実験系を整備した。これにより、従来の単一波照射ではなく、2 つの高周波を同時に制御しながら対象機器へ照射する実験が可能になった。さらに、周波数と電力を系統的に探索する自動測定手順を整備し、対象 IC や対象機器ごとに脆弱な周波数帯を実測で推定できるようにした。この実験基盤が、本助成における最も重要な成果である 2 波電磁照射データ注入の実証を支えた。

標準ロジック IC の実験では、f1 と f2 の役割が明確に分離されることを確認した。f1 のみを照射すると、入力端子の実効電圧が一方の論理状態へ移動し、出力が反転した。一方、f2 のみでは変化がない条件でも、f1 と f2 を同時に照射すると再度出力が反転した。これは、単一周波数が偶然に誤動作を生むのではなく、2 つの周波数が別々の電位経路を制御し、論理しきい値をまたぐように入力電圧を移動させていることを示す。

標準ロジック IC では、周波数探索により f1 = 2.290 GHz、P1 = 24 dBm、f2 = 2.645 GHz、P2 = 24 dBm が入力制御に有効であることを確認した。さらに GTEM セル内での照射実験では、f1 を 42 dBm、f2 を 44 dBm とした条件で出力を制御し、f2 を 100 kHz の矩形波で OOK 変調すると、IC 出力にも同じ 100 kHz の波形が現れた。これは、2 波同時照射により、静的な論理反転だけでなく、連続的なビット列注入が可能であることを示す基礎結果である。

4-2 情報通信機器実機への UART データ注入

次に、Raspberry Pi 4 Model B を対象に、UART RX 端子へのデータ注入を評価した。周波数探索では、UART RX である GPIO15 と GND を対象とし、GPIO 状態を別端子へミラーリングして観測した。その結果、探索条件では f1 = 2.170 GHz、P1 = 18 dBm、f2 = 6.445 GHz、P2 = 22 dBm 付近に脆弱周波数が存在することを確認した。実際の UART 配線を接続したデータ注入実験では、配線の影響を含む実機条件に合わせ、f1 = 2.483 GHz、P1 = 37 dBm、f2 = 6.000 GHz、P2 = 40 dBm を用いた。

UART 通信は、アイドル状態、スタートビット、8 ビットデータ、ストップビットを含む時間構造を持つ。実験では、PC 端末で入力した文字列を UART ビット列へ変換し、そのビット列を f2 の OOK 変調に用いた。Raspberry Pi 側では、UART RX 入力に接続された端末プログラムが、照射波によって発生したビット列を受信文字列として処理した。ボーレートは 115.2 kb/s、形式は 8-N-1 であり、汎用的なデバッグ・通信インタフェースで一般的に用いられる条件である。

実験結果として、PC 側端末 A に入力された ASCII 文字列が、Raspberry Pi 側端末 B に同一の文字列として表示された。すなわち、空間を介して照射された 2 波が、対象機器内部の CMOS 入力端子において UART 信号として解釈され、実機の OS 上で正規の入力として処理された。この結果は、2 波電磁照射が単なる誤動作ではなく、情報通信機器の入力インタフェースを標的としたデータ注入攻撃として成立し得ることを示している。

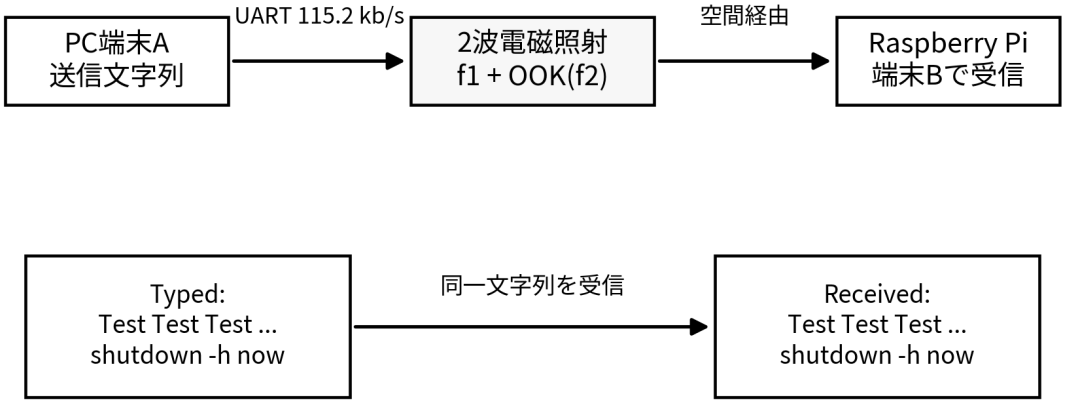


図 4　Raspberry Pi への UART データ注入実験の結果概要

表 1　主要実験結果

評価対象	探索・注入条件	確認した結果
標準 CMOS ロジック IC	探索: f1 = 2.290 GHz, P1 = 24 dBm / f2 = 2.645 GHz, P2 = 24 dBm 注入: f1 = 42 dBm, f2 = 44 dBm, f2 を 100 kHz で OOK 変調	f1 と f2 の組合せにより出力論理を制御し、100 kHz のビット列に対応する出力波形を確認
Raspberry Pi 4 Model B	探索: f1 = 2.170 GHz, P1 = 18 dBm / f2 = 6.445 GHz, P2 = 22 dBm UART 注入: f1 = 2.483 GHz, P1 = 37 dBm / f2 = 6.000 GHz, P2 = 40 dBm	UART 115.2 kb/s, 8-N-1 条件で、PC 端末 A の文字列が Raspberry Pi 端末 B に同一文字列として表示

4-3 研究成果の公表と国際的評価

本成果は、EMC Europe 2025 において「Arbitrary Data Injection into CMOS Integrated Circuits via Dual-Wave Electromagnetic Irradiation」[2]として発表し、278 編の論文の中から Best Paper Award を受賞した。電磁照射による情報注入を、単なる EMC 上の誤動作ではなく、情報セキュリティの完全性を侵害する現実的な脅威として示した点、また 2 波を用いることで従来困難であった任意データ注入に近づいた点が高く評価された。

さらに、研究内容を発展させた論文「Deterministic Dual-Frequency Data Injection Against CMOS Digital Systems」[3]は、IEEE Transactions on Electromagnetic Compatibility に掲載された。同論文では、2 波電磁照射の動作原理、周波数・電力探索手順、標準 CMOS インバータ IC および Raspberry Pi 4 Model B での実証、UART 115.2 kb/s での注入、さらに筐体・PCB・IC・ファームウェアにまたがる対策指針を体系的に整理した。

EMC Europe 2025 Best Paper Award

授賞式の様子

図 5　EMC Europe 2025 Best Paper Award と授賞式の様子

本成果は、申請時に予定していた「国際会議 1 回、論文誌 1 編」という成果公表計画を満たすだけでなく、国際会議での最優秀論文賞受賞とトップジャーナル掲載という形で、研究調査の成果を国際的に可視化するものとなった。また、論文の謝辞には本助成が明記されており、本助成が実験基盤の構築と成果公表に直接結びついたことを示している。

4-4 対策指針の整理

2 波電磁照射によるデータ注入は、特定の 1 部品や 1 製品だけに依存する現象ではなく、CMOS 入力段、ESD 保護構造、配線、電源分配網、外部ケーブルなどが組み合わさることで発生する。そのため、対策も単一層で完結しない。本研究では、施設・筐体・ケーブル、プリント配線板、IC、監視回路、ファームウェア・システム運用の各層に分けて対策を整理した。

施設・筐体・ケーブルの層では、外部からの電磁波が機器内部の入出力端子へ結合する経路を減らすことが重要である。シールド、貫通部の接地、ケーブルのボンディング、コモンモードチョーク、フィードスルーコンデンサなどを適切に用いることで、筐体外から入力端子へ伝搬する高周波電流を抑制できる。特に、デバッグポートや外部端子に接続されるケーブルは、攻撃波の結合経路になりやすいため、製品設計時に高周波の侵入経路として評価する必要がある。

PCB レベルでは、入力端子から IC 内部へ高周波が流入し、ESD 保護構造で整流されることを抑える設計が求められる。入出力端子付近の直列抵抗、バイパス容量、グラウンドプレーンの強化、電源分配網の共振把握、端子インピーダンスの制御は有効な対策候補である。ただし、抵抗や容量を追加すると通常動作時の信号品質にも影響するため、通信速度、立上り時間、負荷条件、EMC 規格を同時に満たす設計最適化が必要となる。

IC レベルでは、Schmitt トリガ入力によりしきい値近傍の微小変動に対する耐性を高めること、対称性の高い ESD 保護構造を用いて整流に起因する直流オフセットを抑えること、パッド近傍に高周波をバイパスする容量を配置することが有効である。さらに、高信頼用途では I/O パッド周辺や電源分配網に電圧・電流センサ、RF 検出器を配置し、通常時のノイズレベルを超える異常な高周波注入をリアルタイムに検出することも考えられる。

ファームウェア・システム層では、UART、JTAG、SWD などのデバッグポートを出荷時に無効化し、必要時のみ真正性確認後に有効化する運用が重要である。また、通信プロトコルにパリティ、CRC、フレーム境界検査、レート制限、異常ログ記録を組み込むことで、物理層で生成された不自然なビット列が上位層へ通過することを抑えられる。AI エッジ機器では、電磁照射検知情報を AI 入力として利用し、通常ノイズと攻撃性のある外乱を識別するフェイルセーフ機構へ発展させることも今後の重要課題である。

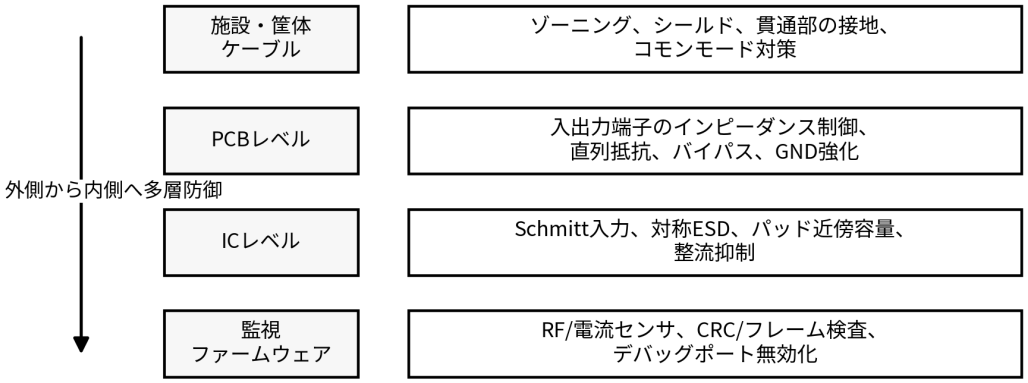


図 6　2 波電磁照射データ注入に対する多層的対策指針

4-5 申請時計画との対応

申請時の研究計画では、回路不正改変の検出、検知情報を AI 入力へフィードバックするフェイルセーフ、電磁照射による AI 入力改変の検証、電磁照射検知情報を用いた安全性担保を掲げた。本助成期間の成果は、このうち電磁照射による情報入力改変の検証と、その対策整理を中心に大きく進展した。特に、GTEM セルと高周波機器を用いた実験基盤を整備したことで、AI 入力の前段に存在する CMOS デジタル入力が、外部電磁界によりどのように操作され得るかを、実測に基づいて示すことができた。

また、回路不正改変と電磁照射攻撃は、攻撃の実施方法こそ異なるものの、AI へ到達する入力信号をハードウェア層で変化させるという点で共通している。本研究で得た 2 波電磁照射の知見は、入力端子、電源分配網、プリント配線板、IC 保護構造、システム監視のどの層に異常が現れるかを整理する基礎となる。したがって、今後の回路不正改変検知や AI を用いたフェイルセーフへ展開する際にも、物理層の異常を数値化し、AI が扱える特徴量として入力するという研究方針に直接つながる。

成果公表の面でも、申請時に想定した国際会議発表および論文誌投稿を達成した。中間報告時点で予想以上に順調と整理していた周波数探索の自動化、情報通信機器実機への注入実証、攻撃パラメタの実測推定は、その後の論文として統合された。これにより、本研究調査は単年度の装置整備や予備実験にとどまらず、AI ハードウェアセキュリティという研究分野を国際的に提示する成果へ到達した。

5 研究成果の意義

本研究成果の第一の意義は、電磁照射による情報注入を「再現性の低い誤動作」から「周波数・振幅・変調で制御できるデータ注入」へと引き上げた点にある。2 つの周波数がそれぞれ異なる入力経路を励振するという考え方により、単一波照射の限界であった遷移時間の問題を緩和し、ビット列として意味を持つ信号の注入を

可能にした。これにより、IEMI を可用性だけでなく、情報の完全性・真正性の観点から評価すべきであることを実証した。

第二の意義は、攻撃パラメタをブラックボックス条件で探索する手順を示した点である。対象機器の内部設計情報、IC の詳細なモデル、基板レイアウト、パッケージパラメタを知らなくても、外部から観測できる入出力挙動をもとに脆弱周波数帯を探索できることは、実際の製品評価において重要である。これは攻撃者の視点では現実性を高める一方、防御者の視点では、製品出荷前のセキュリティ評価項目として周波数掃引・電力掃引を導入すべきことを示す。

第三の意義は、AI エッジコンピューティングの安全性を、AI モデル単体ではなく、物理層からの入力信号、電子回路、通信インタフェース、ファームウェアを含むシステム全体で考える必要性を示した点である。AI モデルの堅牢性研究では、画像やセンサデータに対する敵対的サンプルが議論されることが多い。しかし、エッジ AI 機器では、そのデータがセンサから AI へ届くまでの回路と通信も攻撃対象である。本研究は、AI への入力がハードウェア層で作られる以上、ハードウェアセキュリティは AI セキュリティの基盤であることを明確にした。

第四の意義は、環境電磁工学と情報セキュリティの研究コミュニティを接続した点である。EMC 分野では、外来電磁ノイズによる機能停止や誤動作を防ぐ設計が長年研究されてきた。一方、情報セキュリティ分野では、攻撃者が意図を持って外乱を与える状況、上位層の認証を迂回する状況、ログに残りにくい入力改ざんを行う状況を考える必要がある。本研究は、これらの観点を統合し、EMC 評価を情報セキュリティ保証へ拡張する具体例を示した。

第五の意義は、具体的な対策の方向性を同時に提示した点である。攻撃原理を明らかにしただけでは、社会実装に不安を残す。本研究では、筐体、ケーブル、PCB、IC、監視、ファームウェアをまたぐ多層防御を整理し、設計者がどの層で何を評価すべきかを示した。特に、Schmitt 入力、対称 ESD、RF 検出、CRC やフレーム検査、デバッグポート管理など、既存技術を組み合わせることでリスクを低減できることを示した点は、実用上の意義が大きい。

社会実装上の観点では、本成果は製造後に現場で長期間使われる AIoT/CPS 機器の保守にも関係する。ハードウェア層の脆弱性は、ソフトウェアのように容易に差し替えることができないため、出荷前の評価、保守時の監視、異常検知時の安全側制御を組み合わせる必要がある。特に、現場に設置された端末がネットワークから切り離され、スタンドアロンで判断する状況では、クラウド側の監視だけでは入力改ざんを検出できない。本研究で示した脅威モデルは、設計段階で入出力端子をどのように保護すべきか、運用段階でどのログを取得すべきかを検討する材料となる。

さらに、AI エッジ機器では、攻撃が成功した場合の影響がデジタル情報の漏えいに限られず、物理的な動作へ波及する可能性がある。鍵、モータ、バルブ、ロボット、医療・ヘルスケア機器などでは、入力データの改ざんが直接的な制御の変化を引き起こす。したがって、本研究で得られた「入力端子での完全性保証」という考え方は、情報セキュリティと機能安全をつなぐ接点でもある。今後、AI 機器の安全評価では、AI モデルの精度、ソフトウェアの脆弱性、通信路の認証に加え、物理層からの意図的外乱に対する耐性を総合的に評価する枠組みが必要になる。

6 今後の課題と展望

今後の第一の課題は、対象機器の種類を増やし、2 波電磁照射に対する脆弱性を定量的に分類することである。本研究では標準ロジック IC と Raspberry Pi 4 Model B で実証したが、実際の AI エッジ機器では、センサモジュール、AI アクセラレータ搭載マイクロコントローラ、モータ制御 IC、通信モジュール、電源回路など、多様な構成が存在する。機器クラスごとに、どの周波数帯、どの端子、どの配線構造が脆弱になりやすいかを整理することで、設計段階のリスク評価が可能になる。

第二の課題は、電磁界解析と回路解析を接続した予測モデルの構築である。2 波注入は、外部電磁界から配線への結合、電源分配網の周波数特性、ESD 保護構造の非線形整流、CMOS しきい値、通信プロトコルの時間構造が連鎖して発生する複合現象である。現状では、製品 IC やパッケージの詳細パラメタが公開されていないことが多く、完全なシミュレーションは難しい。したがって、構造情報を開示した評価用プラットフォームを作り、実測とモデルを比較できる基盤を整備する必要がある。

第三の課題は、対策の有効性を情報セキュリティ指標として測定することである。従来の EMC 試験では、機能停止の有無や誤動作の有無を基準に合否を判定することが多い。しかし、本研究で示した脅威では、装置が動作し続けていても、入力データの一部が攻撃者の意図どおりに変化する可能性がある。今後は、注入可能な

ビット誤り率、攻撃成立に必要な電力、必要な照射距離、検出率、誤検出率、通信プロトコル上の防御効果などを統合した評価指標を構築する必要がある。

第四の課題は、AI を用いた異常検知・フェイルセーフ機構との接続である。申請時の構想では、回路不正改変や電磁照射の検知情報を AI の入力へフィードバックし、通常利用に伴うノイズと攻撃による外乱を識別することを掲げた。本助成で得られた 2 波照射実験データ、周波数探索データ、入力論理の変化データは、そのような検知 AI の学習・評価データとして活用できる。今後は、電磁照射検知回路、センサログ、通信ログ、AI 判断結果を統合し、攻撃時に安全側へ遷移するシステム設計へ展開したい。

第五の課題は、標準化・ガイドライン化への展開である。エッジ AI 機器は今後、社会インフラ、医療、交通、家庭内支援などに広く浸透する。これらの機器に対して、物理層からの情報注入をセキュリティ評価項目として組み込むことは、社会的に重要である。本研究で得られた成果を、国内外の研究会、国際会議、論文誌、企業との共同研究を通じて共有し、AI ハードウェアセキュリティの評価・設計指針として発展させる。

7 まとめ

本研究調査では、高信頼 AI エッジコンピューティングの基盤となる AI ハードウェアセキュリティの確立を目指し、電磁照射による情報注入攻撃の原理解明、実験系構築、実機実証、対策指針の整理を行った。2 つの周波数を組み合わせることで CMOS 入力の実効電圧を制御し、標準 CMOS ロジック IC ではビット列に対応する波形を発生させ、Raspberry Pi 4 Model B では UART 115.2 kb/s の文字列注入を実証した。

この成果は、EMC Europe 2025 で Best Paper Award [2]を受賞し、IEEE Transactions on Electromagnetic Compatibility に論文 [3] として掲載された。これにより、本助成で構築した実験基盤と研究成果が、国際的にも高い学術的価値を持つことが示された。今後は、対象機器の拡大、評価指標の整備、対策効果の定量化、AI による検知・フェイルセーフ化を進め、情報通信システムの最下層であるハードウェアからエッジ AI の信頼性を支える研究へ発展させる。

【参考文献】

[1] 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 Transactions on Electromagnetic Compatibility, vol. 46, no. 3, pp. 314-321, Aug. 2004, doi: 10.1109/TEMC.2004.831899.

[2] M. Kinugawa and Y. Hayashi, “Arbitrary Data Injection into CMOS Integrated Circuits via Dual-Wave Electromagnetic Irradiation,” EMC Europe 2025, Paris, France, 2025. (Best Paper Award)

[3] M. Kinugawa and Y. Hayashi, “Deterministic Dual-Frequency Data Injection Against CMOS Digital Systems,” IEEE Transactions on Electromagnetic Compatibility, 2026, doi: 10.1109/TEMC.2026.3687600.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Deterministic Dual-Frequency Data Injection Against CMOS Digital Systems	IEEE Transactions on Electromagnetic Compatibility, doi: 10.1109/TEMC.2026.3687600	2026 年 5 月
Arbitrary Data Injection into CMOS Integrated Circuits via Dual-Wave Electromagnetic Irradiation	EMC Europe 2025 (Best Paper Award)	2025 年 9 月