安全な AI/IoT 基盤実現を目指した ハードウェアセキュリティ技術の開拓

Development of fundamental technology for secure AI/ IoT hardware platform

2181012

研究代表者	国立高等専門学校機構 仙台高等専門学校	助　教	衣　川　昌　宏
共同研究者	奈良先端科学技術大学院大学 先端科学技術研究科	教　授	林　　優　一

［研 究 の 目 的］

AI/IoT 技術は，高度な自動制御技術である AI と実世界と情報通信世界を結びつける IoT 機器が組み合わさったものである。この表現ではこれまでのパーソナルコンピュータや自動家電と同じように思えるが，次の表現では AI/IoT が社会に及ぼす影響と責任，安全性の要求度の高さがわかる。

AI/IoT 技術とは，AI が IoT 機器を五感および手足として使い，社会の情報的最適化を達成する自動社会制御システムである。

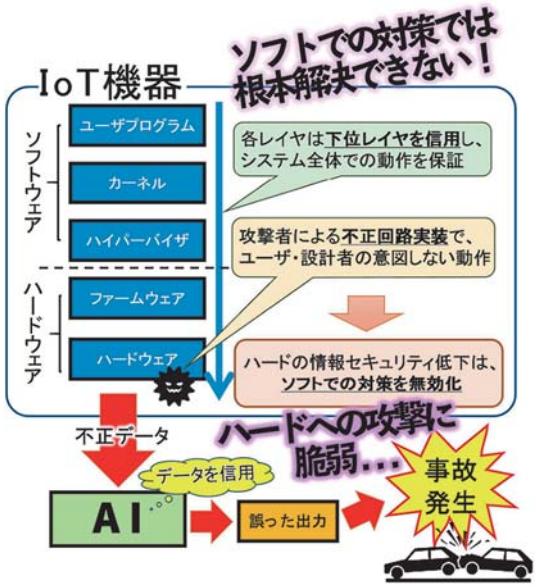

図 1　AI/IoT 機器の階層構造とリスク

かつては，専門家の道具や研究対象に限定されていた AI であるが，現在では情報通信・情報処理機器の高速化・省電力化・小型化に伴い IoT 機器を端末とした，暮らしを助ける AI の利用が一般となっている。さらに，人間起因の事故防止や負担軽減のために，自動車の自動運転技術など，画像処理やレーダをセンサとして用いた，運転制御の最適化が実用されている。このように，限定的な AI が多数存在し，知らないうちに我々の生活を支えている。

これら AI/IoT 技術は図 1 に示すように，ソフトウェアとハードウェアが組み合わさって構築されている。特に，情報セキュリティの観点からこの階層構造を観察すると，上部のソフトウェアに関してはこれまでのソフトウェアに関連する研究により，安全性を確保するための手法が確立されており，実際の開発現場で用いられている。しかし，下部のハードウェアに関しては，その情報安全性に関する議論は暗号ハードウェア等に限定されており，AI/IoT 機器を構成する電子回路全体を視野に入れた情報安全性に関しては十分に議論されていない。特に，電子回路に代表されるハードウェアは物理的に改変可能であり，工場からの出荷後はその回路に改変が加えられているのか，正常に動作しているのかを確実に監視・自己診断する手法は存

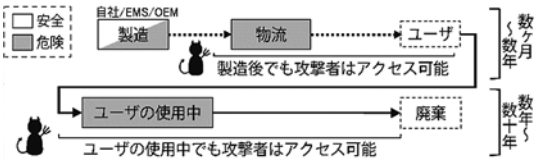

図2　ハードウェア不正改変のタイミング

在していない（図 2)。一例として，ATM に仕掛けられるスキミング装置や，コピー製品などがあり，いかにハードウェアの改変が容易になってきているかを示している。

特に我々はハードウェアセキュリティ問題の中でも，AI/IoT 機器を含む ICT 機器へ仕掛けられる不正回路に関する検討を進めてきた。そこでは，機器製造後および使用中における不正回路実装の可能性および，意図的タイミングでの情報機密性の低下（情報漏えい）が誘発可能であることを明らかとしている。これら検討の延長線上である AI/IoT システムシステムも回路改変攻撃の対象ではあるが，その攻撃は前述の自動社会制御システムを脅かす点で，広範な情報セキュリティ問題へ拡大する可能性がある。しかも，これまでの我々の成果から，IoT 機器を含む電子回路への攻撃は電磁波照射により容易に行えるだけではなく，攻撃の痕跡が残らないため，攻撃の防御が困難であることがわかっている。そのため，これら攻撃に対する早急な対策が必要であることから，IEEE EMC Society の TC 5 High Power Electromagnetics にて Low-power IEMI（低電力意図的電磁放射）問題として提起し，環境電磁工学を主軸にこの対策に取り組んでいる。

本申請の研究期間中では，AI/IoT システムへの電磁波照射攻撃に関して，以下の情報機密性の低下を中心とした原理解明，対策手法の検討を行った。

① 不正回路実装による情報機密性低下の評価
② 機器の潜在的電磁照射攻撃脆弱性の調査

②は研究途上で発見した問題であり，事前の研究計画および本問題の影響範囲・危険性の想定を大きく超える問題であったため，研究期間後半は②に関する原理解明，対策に主眼を置いた。①の検討では不正回路改変による悪性回路の実装での情報機密性低下について扱ってきた。しかし，①が用いている情報機密性低下の機構は，情報機器を構成するディジタル回路自体に存在することから，不正回路改変がなされていない正常な機器であったとしても，電磁波照射攻撃により情報機密性低下が生じ，機器内部の情報を取得できることを明らかとした。次節ではこれら成果の詳細を述べる。

［研究の内容，成果］

1　不正回路実装による情報機密性低下の評価

不正回路実装による情報機密性低下の基本原理を図 3 に示す。機器内部に図 4 のように実装された能動素子（図 3，4 の例では FET）が，機器内部の情報を有する信号に応じて，外部から照射された電磁波の反射率を変化させることにより，振幅変調信号として情報を機器外部へ漏えいさせる。このとき，この不正回路を構成するアンテナは機器の一部であるケーブルをア

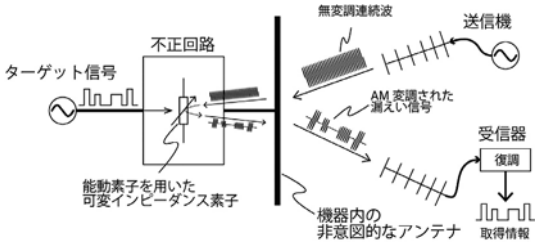

図3　不正回路実装による情報機密性低下

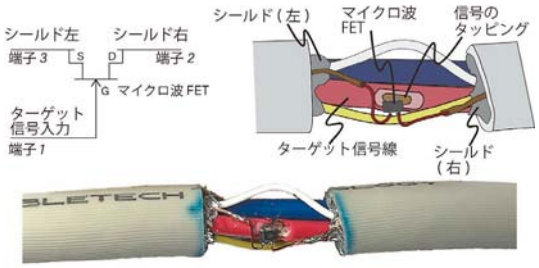

図4　機器ケーブル内に仕掛けられた不正回路

ンテナの素子とできる。

この動作原理について検討を進めた結果，本不正回路による情報漏えいを生じさせる信号の生成は，RFID 等の原理と同様に，アンテナとそのアンテナに接続された負荷素子のインピーダンスマッチングによって引き起こされていることが分かった。しかしながら，不正回路で使用されるマイクロ波 FET はそのデータシートに記載された使用方法から逸脱しており，上記インピーダンスマッチング・アンマッチングがどのような条件で生じるかは実験的，および技術的な勘に頼っていた。そこで，図 5 に示すベクトルネットワークアナライザを用いた反射法によるインピーダンス測定により，FET の動作範囲を明確にし，FET がカバーするターゲット信号の範囲を明確にする手法を考案した。

図 5 のシステムでの計測例を図 6 に示す。図中赤枠で囲む部分は，ターゲット信号を音声信号とした場合に有効となる範囲を示している。赤枠内に傾きがある場合，不正回路に有効な素子として動作することを示している。

本結果については，現在情報セキュリティに関する国際会議に投稿中である。

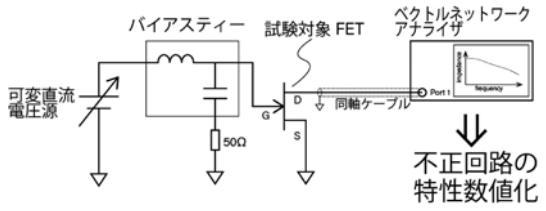

図 5　不正回路内 FET の特性測定システム

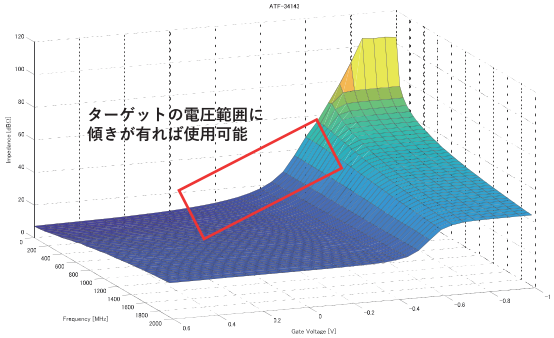

図 6　マイコン GPIO ピンのインピーダンス特性

2　機器の潜在的電磁照射攻撃脆弱性の調査

前節 1 では，図 3 で示す可変インピーダンス素子としてマイクロ波 FET を使用していた。しかし，IC 製造プロセスの微細化と高速化により，マイクロ波 FET を用いずとも，マイコン等の GPIO ピンで同様に高周波を変調可能であることが考えられる。そこで，2010 年代後半に製造された汎用 32 ビットマイコンについて，その IO ピンのインピーダンス測定を図 5 のシステムで行った。その結果，図 7 に示すように 6 GHz 近辺でも変調素子として有効に動作することを確認した。

さらに，同マイコンを実装した機器に対して電磁波照射攻撃を実施したところ，図 8 のようにマイコンのピンに出力されている信号を取得することができた。これは，機器に不正回路を実装せず，出荷状態でも攻撃可能であることを示しており，機器の設計によって潜在的な脆弱性が非意図的に埋め込まれた結果を示している。

この脆弱性の有無の判断手法として，意図的電磁照射に対する応答を計測する試験が有効であると考えられる。しかし，本脆弱性は IC のデータシート外での動作によるものであるから，設計時には想定することが困難である。

今後は，IC を実装するプリント配線基板お

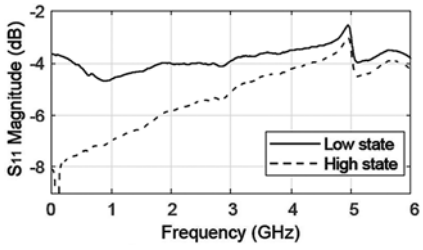

図 7　マイコン GPIO ピンのインピーダンス特性

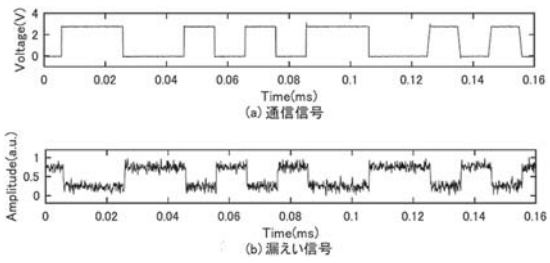

図 8　不正回路無しの機器からの漏えい信号

よび機器筐体など，IC 周辺回路での対策手法について検討を進め，安全な AI/IoT 機器実現に向けて設計手法を示すことを目標とする。

本成果は 6 月開催の 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo（EMC Sapporo & APEMC 2019）にて発表予定である。

［今後の研究の方向，課題］

本研究期間では，IC 自体が有する電磁照射攻撃による情報機密性低下問題を新たに発見した。本問題は IC の設計，IC を実装するプリント配線基板，および機器筐体等の IC 周辺部位を含んだ広範にわたる問題である。そのため，下記のアプローチで問題解決を検討する。

・漏えい信号の定量的測定手法確立
・電磁波照射時の IC および周辺部位の動作解明
・既存部品等での対策手法

さらに，本研究の過程で漏えい信号を高感度に受信可能な受信器の設計が必要となった。そのため，本問題と分離して，「アナログ高周波回路およびソフトウェア無線送受信機を用いた，不要信号抑圧による受信器の高感度化」にも取り組む予定である。

［成果の発表，論文等］

［1］ M. Kinugawa and Y. Hayashi, “A Study on Feasibility of Electromagnetic Information Leakage Caused Forcibly by Low-power IEMI,” EMC Sapporo & APEMC 2019, Jun. 2019.（招待講演発表予定）