様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ４ 月 ２０ 日現在

機関番号：１４６０３
研究種目：若手研究
研究期間：2020～2021
課題番号：２０Ｋ１９８００

研究課題名（和文）センサに対する電磁波を通じた攻撃手法の評価および対策検討

研究課題名（英文）Evaluation of attack methods through electromagnetic waves on sensors and study of countermeasures

研究代表者

藤本　大介（Fujimoto, Daisuke）

奈良先端科学技術大学院大学・先端科学技術研究科・助教

研究者番号：６０７３２３３６

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：自律制御システムにおいて外界の情報を取得するためにセンサの需要が高まっている。そのセンサに対して非侵襲的に電磁波を通じて行う攻撃を対象に研究を行った。電磁波を通じた攻撃は外部から電磁波を当て、内部に故障を発生させる注入と機器の動作から発生する電磁波を通じて情報が漏えいする２種の攻撃に大別される。本研究では、電磁波注入に対しては、機器の温度条件により耐性が変化することを明らかにした。電磁波を通じた漏えいに関しては、漏えい源となる素子の周辺の構造により、漏えいの強度が変化することを明らかにした。これらの詳細な条件を明らかにしたことにより、電磁波攻撃に対する耐性を得ることが可能となる。

研究成果の学術的意義や社会的意義
センサに対する攻撃は今後自律制御機器が増加することを鑑みると、インフラに影響する重要な研究分野であるといえる。本研究で対象とした電磁波を通じた攻撃手法は、センサの測定メカニズムへの依存が少なく、より多くのセンサに対して適用可能な手法として懸念されている。これまでの研究では、特定の機器に対しての電磁波攻撃の成否のみに着目しており、その手法が他の機器に及ぼす影響については議論がなされていない。本研究では、電磁波による故障の注入と電磁波を通じた情報の漏えいの両者について、温度依存性や周囲の部品構成の影響などを調査し、攻撃の脅威が高まる条件を明らかにした。

研究成果の概要（英文）：There is a growing demand for sensors to acquire information about the external world in autonomous control systems. We conducted research on non-invasive attacks on these sensors through electromagnetic waves. There are two main types of electromagnetic wave attacks: external electromagnetic wave injection, which causes internal failures, and information leakage through electromagnetic waves generated by the operation of devices. In this research, it was clarified that the resistance to electromagnetic wave injection varies depending on the temperature conditions of the equipment. For leakage through electromagnetic waves, we found that the intensity of leakage varies depending on the structure around the device that is the source of leakage. By clarifying these detailed conditions, it is possible to obtain resistance to electromagnetic wave attacks.

研究分野：ハードウェアセキュリティ

キーワード：センサーセキュリティ　電磁波攻撃

１．研究開始当初の背景

近年、多くの情報機器がセンサからの情報をもとに動作している。これらのセンサで取得されたデータは測定エラーなどを除き信頼のおけるものとして扱われている。しかし，悪意のある攻撃者がセンサからの出力値を誤らせたり，計測を不可能にしたりするなどの計測におけるセキュリティリスク（計測セキュリティ）が提案されている。特に自動車においては自動運転に用いられる LiDAR に対する攻撃が提案されており[1]、人命にかかわる脅威として認識されつつある。これらの攻撃はセンサの仕組み自体を狙うものであり，センサの出力データ（デジタルデータ）からでは攻撃を検知することは困難である。様々なセンサに対する攻撃が提案されているが、既存の攻撃手法はセンサの計測原理に基づき、測定部への直接的な信号注入やセンサから出力された信号を直接観測することで攻撃に必要な計測タイミングの同期を行っていた。これに対して本研究では、情報機器のような電子回路を用いた機器においては動作した際に必ず消費電力によって電磁波が発生することに着目する。生じた電磁波から計測タイミングの同期などに使用できる情報が含まれている可能性があり、従来の攻撃とは全く異なる原理を用いたセキュリティの脅威となる可能性がある。

２．研究の目的

本研究では、センサにおける電磁波による情報漏えいおよび測定値の操作に対してその可能性を検討し、メカニズム解明を行いその対策手法について検討することを目的とする。
この目的を達成するために、高精度な電磁界計測技術に基づく電磁的漏えいの測定および電磁波注入を行う評価環境を構築し、攻撃の成立条件を明らかにする。その結果を用いることにより、攻撃メカニズムに基づいた対策手法の提案を目指す。

３．研究の方法

電磁波を通じた攻撃は外部から電磁波を当て、内部に故障を発生させる注入と機器の動作から発生する電磁波を通じて情報が漏えいする２種の攻撃に大別される。両者を同時に評価することは困難であり、かつ評価系が複雑になることが予想される。そのため、それぞれに対して別々の評価系を用意して要素を簡略化することで、効率的に評価をすすめる。
電磁波を注入する対象として、対象となるデバイスのみを搭載した

電磁波を通じて漏えい評価として、ソナーセンサなどで用いられる音声情報を対象とする。音声情報は低周波で扱いやすく、広帯域に電磁波に情報が重畳することが知られている[2]。そのため、漏えい源である素子の周辺の構造や周辺の物体の影響による漏えいの強度の変化の評価に適している。本研究では、電磁波に影響を与える導体を対象として機器の周辺に設置する非接触環境と USB ケーブルなどの直接的な挿入に対する影響を評価する。

４．研究成果

(1) LiDAR などの測定信号を外部に送信するセンサはその測定タイミングを取得されることにより攻撃者が攻撃信号を生成することが可能となる。測定タイミングを得る手法としては測定信号を直接観測することが考えられるが、センサが駆動する際には電力が消費されその結果電磁波が発生する。本研究では電磁波を通じた内部信号の漏えいとして広帯域に情報が重畳するスピーカーフォンを対象として周囲構造の漏えいに与える変化を調査した。結果として、金属体が漏えい源である素子の近傍に近づいた際に漏えいが強まる現象を確認した。このことから、機器単体でのテストで漏えいが確認できない場合でも利用環境によっては漏えいが発生する可能性があることを示した。これを防ぐためには、金属体の有無を加味した評価や、金属体が接近した場合でも影響を受けない設計が求められる。

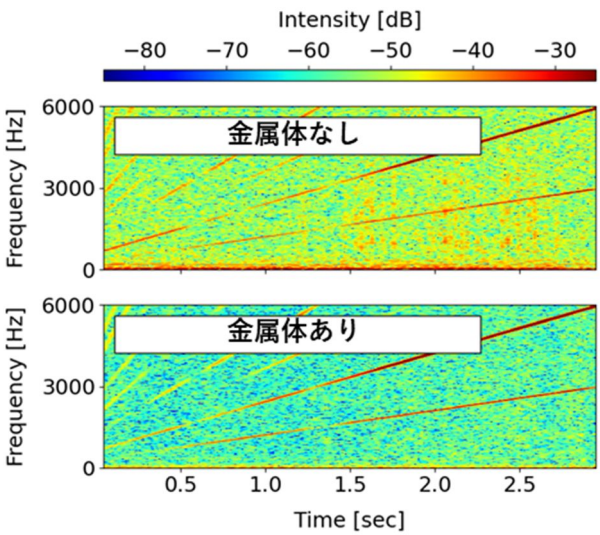

図 1 金属体の有無による音声漏えい強度の変化

(2) 攻撃者が電磁波を通じてセンサ内部の情報を盗聴する際には、情報を含んだ電磁波の強度に

より届く距離が決定される。漏えいする電磁波の強度は機器の設計により決定されるが、機器同士を接続するコネクタ部を含んだ試験を行うことは容易ではない。本研究では、同一規格のＵＳＢコネクタを用いた場合においても製造メーカの違いにより、伝送効率の差異が生じ、放射する電磁波の強度が異なる可能性があることを明らかにした。そのため、試験段階での結合試験で基準を突破したとしても漏えいの可能性があるため、ワーストケースを考慮した試験を実施する必要がある。

(3) 外部から電磁波を注入し、機器に故障を発生させる手法として、機器のクロック信号に電磁波を重畳させ、意図的にクロック周期を早める手法が提案されている。過去の検討においては、機器の動作条件は室温条件のみで行われており、実際の攻撃環境を想定した評価はなされていなかった。しかし、機器の動作速度は温度に依存することが知られており、利用環境や攻撃者による温度操作により、想定より故障が発生しやすくなる可能性がある。本研究では、温度変化が機器の電磁波による故障耐性に影響を及ぼすことを明らかにした。これにより、機器の熱設計や夏季の屋外で利用されるデバイスに対してはより厳しい評価が必要となる可能性を示唆した。

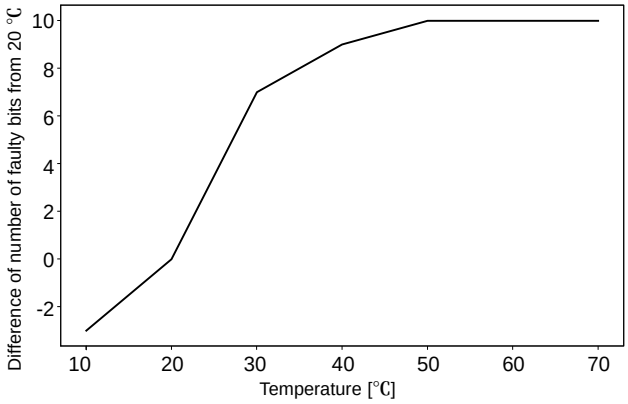

図 2 周辺温度の変化による誤りビット数の変化

(4) センサに対する攻撃は、センサの測定原理毎に攻撃に対する耐性が異なる。そのため、電磁波を通じた攻撃を行った際にも、対象のデバイスの測定手法によっては攻撃による距離改ざんがなされない場合がある。しかし、センサーフュージョンなどの複雑な測定原理を持つセンサに対しては、攻撃の成立条件を調査すること自体が困難になる。本研究では、単純な攻撃に対して耐性を有していると考えられるセンサーフュージョンを行うデバイスに対して、時間的な攻撃パラメータと空間的な攻撃パラメータを分類し、網羅的な評価項目の提案を行った。また、実デバイスに対して提案手法を適用し、時間・空間両者の攻撃条件が成立した場合にのみ攻撃の耐性を有しないことを示した。このことより、独立して時間的・空間的に条件を合わせた評価だけでは不十分な場合があることが明らかとなった。

引用文献

[1] J. Petit, B. Stottelaar, M. Feiri, F. Kargl, “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR, ”Black Hat Europe 2015, November.2015.

[2] 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, Virtual Event USA, Oct. 2020, pp. 1085–1101.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 藤本 大介、林 優一
２．発表標題 ディジタル回路の遅延変化を用いた電磁波印加攻撃検知手法
３．学会等名 暗号と情報セキュリティシンポジウム
４．発表年 2021年

１．発表者名 福嶋 章悟、藤本 大介、林 優一
２．発表標題 リモートワーク環境におけるスピーカーフォンからの電磁波を通じた情報漏えい評価
３．学会等名 暗号と情報セキュリティシンポジウム
４．発表年 2021年

１．発表者名 上田浩行、藤本 大介、林 優一
２．発表標題 製造メーカの異なるコネクタの相互接続時に生ずる接触境界部の高周波特性の基礎評価
３．学会等名 電気情報通信学会ソサイエティ大会
４．発表年 2020年

１．発表者名 Daisuke Fujimoto, Yuichi Hayashi
２．発表標題 Investigation of the Effect of Temperature on Fault Injection Using Intentional Electromagnetic Interference
３．学会等名 2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)（国際学会）
４．発表年 2021年

１．発表者名
Hikaru Nishiyama, Daisuke Fujimoto, Youngwoo Kim, Yuichi Hayashi

２．発表標題
IEMI Fault Injection Method using Continuous sinusoidal Wave with Controlled Frequency , Amplitude, and Phase

３．学会等名
The 13th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo 2021)（国際学会）

４．発表年
2022年

１．発表者名
上田浩行，高野誠也，藤本大介，林　優一

２．発表標題
音声の周波数スペクトルに着目したスピーカーフォンからの電磁的情報漏えい評価法

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
鈴木雅人，藤本大介，林　優一

２．発表標題
マトリクス型Direct ToF Lidarの攻撃耐性評価環境の構築

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関