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　６ 年　 ６ 月　 ５ 日現在

機関番号：１２６１２
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１１８８４

研究課題名（和文）光音響効果を用いたシグナルインジェクション攻撃とその対策

研究課題名（英文）Signal Injection Attack using Photoacoustics and its Countermeasure

研究代表者
菅原　健（Sugawara, Takeshi）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：６０７８５２３６

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：ライトコマンドを生じうる物理メカニズムとして，(i) 熱弾性効果，(ii) 熱ピストン効果，(iii) 光電効果を洗い出した．その上で，各項目の寄与を同定するための実験を設計し，市販の MEMS マイクロホン 8 種を評価した．第一に，3種類の効果のうち，いずれでもライトコマンド脆弱性を生じうることが分かった．第二に，マイクロホンごとに，いずれの効果が優位になるかに大きな違いがあった．すなわち，マイクロホンの内部構造や製造方法によって，主要因が容易に変わりうることが分かった．以上の結果を元に，ライトコマンド対策への提言と，別のセンサに攻撃が拡大する可能性について考察した．

研究成果の学術的意義や社会的意義
本研究は，遠隔にいる攻撃者が，音声アシスタントに無音で音声コマンドを挿入する攻撃（ライトコマンド）に関するものである．この脆弱性は，MEMSマイクが意図せず光に感度を持つことによって生じる．本研究成果は，光が振動に変換される物理メカニズムを明らかにした．本成果は，ライトコマンドへの対策構築に必要な基礎を与える．また，同じメカニズムにより脆弱になりうるセンサを先回りして検出することができるようになる．

研究成果の概要（英文）：The main physical mechanisms of Light Commands are identified as (i) thermoelastic bending, (ii) the thermal piston effect, and (iii) the photoelectric effect. We designed an experimental method for finding the contribution of each effects, and evaluated eight commercial MEMS microphones. First, any of the three types of effects can cause the Light Command vulnerability. Second, the internal structure and manufacturing process impact microphones' light sensitivity, and we observed significant differences between the target microphones. Based on these results, we suggested countermeasures and discussed the possibility of similar attacks in other sensors.

研究分野：Security

キーワード：セキュリティ

様式 Ｃ－１９，Ｆ－１９－１，Ｚ－１９（共通）

## 1　研究開始当初の背景

情報システムが自動車・ロボット・工場などと連携するサイバーフィジカルシステムを用いて社会を自動・自律化することへの期待が高まっている．情報システムと物理世界をつなぐインタフェースであるセンサが信頼できることは，そのような技術が発展するための大前提である．それに対し，アナログ領域でセンサへ誤情報を挿入するシグナルインジェクション攻撃の脅威が指摘されている．そのような攻撃は，ディジタル情報を対象とする従来の情報セキュリティ技術では対策ができないため，アナログ情報を守るための新しいセキュリティ技術が必要である．そのような背景から，シグナルインジェクション攻撃は過去数年のうちに極めて活発に研究がされている．

申請者は，シグナルインジェクション攻撃の手段にレーザーを用いるというアプローチで研究を行い，振幅変調した光を照射することで，マイクロホンに信号を挿入できる脆弱性（ライトコマンド）を発見した．また，この脆弱性を利用すると，スマートスピーカーやスマートフォンに対し，無音でコマンドを挿入できる問題があることを実証した（図 1）．レーザーの指向性の高さにより，わずかレーザーポインタ程度のパワーで，100 メートル以上遠くから攻撃が成功することを実証した．また，光の性質上，窓ガラスなどを貫通して建物の外部から攻撃を行うことができる．

## 2　研究の目的

ライトコマンドに対策するためには，マイクロホンが光に感度を持つ原因の究明が必須である．最近のスマートスピーカーなどの機器では，MEMS (Micro Electro Mechanical Systems) マイクロホンが一般的である．機器に届いた音波は，スルーホールと開口部を通って MEMS マイクロホン内部に導かれる（図 2・左）．MEMS マイクロホンの内部には，音波によって揺れて静電容量を変化させる MEMS 振動板と，静電容量を電圧信号に変換するアナログ回路を含む半導体チップ (ASIC: Application Specific Integrated Circuit) が入っている．

本研究の目的は，ライトコマンドにおいて，光が振動に変換される物理メカニズムを明らかにすることで，光音響効果を用いたシグナルインジェクション攻撃とその対策のための理論を構築することを目的とする．より具体的には，攻撃の成否を決める物理パラメータを明らかにすることで系統的な対策法設計を可能にするとともに，光音響効果を手段とするシグナルインジェクション攻撃の潜在能力を明らかにする．

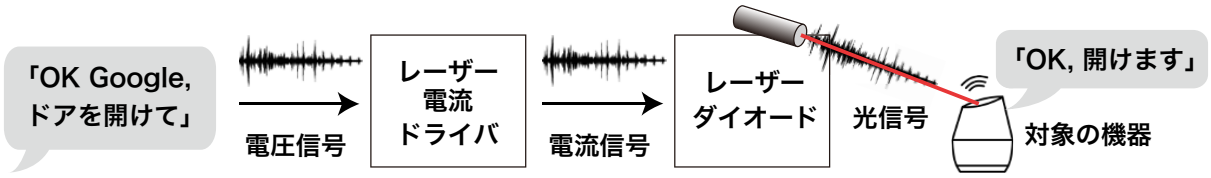


図 1　ライトコマンド: レーザーを用いて音声コマンドを挿入する攻撃

# 3　研究の方法

本研究は，以下の 3 ステップで実施した．

**モデル構築**．光がマイクロホンに影響を与えうるメカニズムとして，ASIC チップ内における光電効果と，MEMS 振動板における光音響効果が示唆される．そこで，MEMS マイクロホン，光電効果，光音響効果に関する従来研究を調査し，ありうるメカニズムの候補のリストを得る．また，各項目ごとに，対応する物理モデルを得る．続いて，各候補の切り分けを行うための実験を設計する．

**評価実験**．先の項目で設計した実験を実施する．具体的には，各効果の影響を切り分けるために，波長や気圧などのパラメータを変化させながらマイクロホンのレーザーへの感度を計測するための実験装置を試作する．その上で，市販 MEMS マイクロホンを評価する．

**考察**．評価実験の結果に基づき，MEMS マイクロホンにおいてレーザー感度を生じる主要因を分析する．そのようにして得た物理メカニズムを元に，攻撃に耐性を有する MEMS マイクロホンの設計にむけた対策法を提言する．また，マイクロホン以外のセンサで，同様のレーザー攻撃の影響を受けうるものを検討する．

# 4　研究成果

## 4.1　モデル化とパラメータ同定法

レーザーを用いた MEMS マイクロホンへのシグナルインジェクションの要因として，図 3(左) に示す 3 つを対象とした．なお，光が振動に変わる物理現象（光音響効果）には，記載以外のメカニズムも存在するが，MEMS 構造 の薄さ，エネルギー効率，想定される周波数帯などを考慮してその可能性を排除した．

- 熱弾性効果（TE）: 光が MEMS 構造を加熱する．振動板中に存在する機械的な非対称性により，加熱によって生じる材料の膨張が曲げモーメントに変換され，結果として振動板が変位する．
- 熱ピストン効果 (TD): 光が振動板を加熱し，その熱が周囲の空気に伝わる．周期的に加熱された空気柱は断熱的に膨張し，圧力波を発生させて振動板を変位させる．
- 光電効果 (PG): 光が半導体部品と相互作用して，過剰な電荷キャリアが生成される．そのような電荷キャリアが ASIC の PN 接合内で生じると, 光電流が生じる．そのような効果が，アンプなどの重要な電子回路で生じると，光電流が出力信号に現れる．

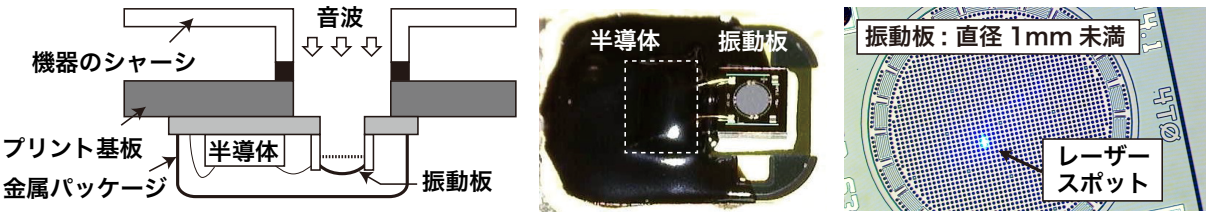


図 2　（左）MEMS マイクロホンへ音波を導く仕組み，（中）不透明な樹脂により，半導体への光を遮断した様子，（右）振動板のみに対し，局所的にレーザーを照射した様子

## 4.2　実験評価

以上のモデルの元で，各項目の寄与を同定するための実験を設計した．切り分けのための基本的な基本的な戦略は，(i) シリコンのバンドギャップを超えることができない，波長が長い赤外線レーザーを用いて光電効果の影響を排除することと，(ii) 真空容器内で実験を行うことで空気の密度を変化させ，熱ピストン効果の影響を排除することにある．

図 3(右) に示すセットアップを構築した．MEMS マイクロホンを真空容器に入れて気圧を変化させながら評価を行うことで，熱ピストン効果に関わる空気の密度を変化させることができる．光学系は，入射するレーザーと観察用するカメラをダイクロイックミラーで合流した同軸光学系である．光源は半導体レーザーであり，4 種類の波長 (1470nm, 904nm, 638nm, および 450nm) を用いる．本セットアップにおいて，市販の MEMS マイクロホン 8 種を評価した．

結果の要約として，表 1 に，各波長について，各効果の測定可能な寄与を A (寄与が支配的) から C (寄与が最も小さい) までランク付けしたものを示す．まず第一に，3 種類の効果のいずれでもライトコマンド脆弱性を生じうることが分かった．第二に，マイクロホンごとに，いずれの効果が優位になるかに大きな違いがあった．すなわち，マイクロホンの内部構造や製造方法によって，主要因が容易に変わりうることが分かった．

全体の傾向として，ほとんどのマイクロホンで最大の影響を生じるのは，904nm の近赤外レーザーを照射した際の光電効果であった．マイクロホンの開口部から ASIC に至るためには MEMS ダイアフラムと ASIC 上の樹脂を貫通する必要があるが，近赤外光はそれらを効率的に透過するため，ASIC に直接影響を与えることができるものと考えられる．次に支配的となる要因は熱ピストン効果であった．その影響は，1 つのマイクロホンを除く全てのマイクロホンにおいて，熱弾性効果よりも著しく強かった．この傾向は，入射光の大部分が MEMS 振動板の透過率が低い（すなわち吸収率が高い）可視光レーザーにおいて顕著であった．

## 4.3　対策・他のセンサにおける脅威

実験結果を元に，ライトコマンド対策への提言と，別のセンサに攻撃が拡大する可能性について考察した．

### 4.3.1　対策の提言

- 適切な材料で ASIC をカバーすることで光電効果を対策する

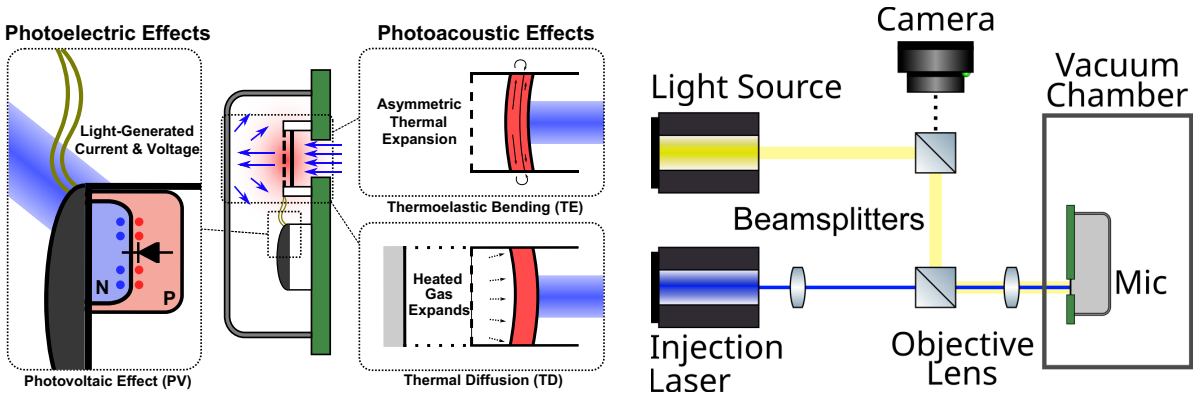


図 3　（左）3 つの主要な物理現象の概要．（右）実験セットアップ．

- 音波は通過するが光は遮断する構造を利用して，ダイアフラムに当たる光量を減らす
- 熱弾性効果を生じる構造的・材料的な非対称性を減らす
- レーザー照射によって生じる信号の特徴を利用して異常検知を行う
- レーザー照射を検出するセンサを搭載する

#### 4.3.2 他のセンサへの影響

- パッケージ内部に ASIC を持ち，そこにレーザー光が届きうるセンサは，シグナルインジェクション攻撃に対して脆弱となる可能性がある．それらの 特徴を持つセンサとして，超音波センサ，圧力センサ，湿度センサ，化学センサなどがある．パッケージが封印されている場合であっても，特定の波長の光が透過してしまう可能性がある．特に，MEMS の多くはシリコンを用いて 製造されるため，特定の赤外光に対して高い透過率を持ってしまう．
- 稼働する機械構造が外界に露出したセンサは，光音響効果によりレーザー光に感度を持つ可能性がある．また，稼働部が露出していない場合でも影響を受ける可能性がある．熱ピストン効果は，空気が周期的に加熱されるだけで生じるため，パッケージの表面で熱ピストン効果が生じ，センサ全体を揺らす可能性があるためである．

### 4.4 その他の成果

並行して関連するシグナルインジェクション攻撃についても研究を行い，以下の成果を得た．

- レーザーを用いて遠隔から振動を計測する装置（レーザードップラー振動計）が生じる盗聴攻撃の脅威
- 低温輸送で使われる温度センサへの電磁干渉 (EMI) 脅威に関する安全性評価
- 人工衛星に搭載されたセンサへのシグナルインジェクション攻撃に関するリスクアセスメント

表 1　各対象・条件における，各効果の出力電圧信号への影響度．A(最大)∼C(最小)

| | IR 1470nm | | | IR 904nm | | | Red 638nm | | | Blue 450nm | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Device | TE | TD | PG | TE | TD | PG | TE | TD | PG | TE | TD | PG |
| CMM3526 | – | A | – | – | B | A | – | A | B | – | A | – |
| SPU0410 | A | B | – | – | – | A | A | C | B | A | C | B |
| ICS41350 | B | A | – | B | – | A | B | A | – | B | A | – |
| ADMP401 | – | A | – | – | – | A | – | B | A | – | A | B |
| SPA1687 | B | A | – | – | – | A | B | A | C | B | A | – |
| SPH0641 | – | A | – | – | – | A | – | A | – | – | A | – |
| VM1010 | – | A | – | – | A | B | – | A | – | – | A | – |
| VM3000 | – | A | – | – | A | – | – | A | – | – | A | – |

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　4件／うちオープンアクセス　4件）

| | |
|---|---|
| １．著者名<br>Doi Kohei、Sugawara Takeshi | ４．巻<br>--- |
| ２．論文標題<br>Poster: Inaudible Acoustic Noise from Silicon Capacitors for Voice-Command Injection | ５．発行年<br>2022年 |
| ３．雑誌名<br>ACM CCS 2022 | ６．最初と最後の頁<br>--- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1145/3548606.3563526 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Benjamin Cyr, Yan Long, Takeshi. Sugawara, and Kevin Fu | ４．巻<br>--- |
| ２．論文標題<br>Position Paper: Space System Threat Models Must Account for Satellite Sensor Spoofing | ５．発行年<br>2023年 |
| ３．雑誌名<br>SpaceSec 2023 | ６．最初と最後の頁<br>--- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.14722/spacesec.2023.231491 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| １．著者名<br>Long Yan、Rampazzi Sara、Sugawara Takeshi、Fu Kevin | ４．巻<br>55 |
| ２．論文標題<br>Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats | ５．発行年<br>2021年 |
| ３．雑誌名<br>Biomedical Instrumentation and Technology | ６．最初と最後の頁<br>112～117 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.2345/0890-8205-55.3.112 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| １．著者名<br>Cyr Benjamin、Sugawara Takeshi、Fu Kevin | ４．巻<br>2021 |
| ２．論文標題<br>Why Lasers Inject Perceived Sound Into MEMS Microphones: Indications and Contraindications of Photoacoustic and Photoelectric Effects | ５．発行年<br>2021年 |
| ３．雑誌名<br>2021 IEEE Sensors | ６．最初と最後の頁<br>1～4 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/SENSORS47087.2021.9639744 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>該当する |

| | |
|---|---|
| １．著者名<br>Cyr Benjamin、Sumaria Vedant、Long Yan、Tadigadapa Srinivas、Sugawara Takeshi、Fu Kevin | ４．巻<br>--- |
| ２．論文標題<br>How Lasers Exploit Photoacoustic and PhotoelectricPhenomena to Inject Signals into MEMS Microphones | ５．発行年<br>2024年 |
| ３．雑誌名<br>Research Square | ６．最初と最後の頁<br>--- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.21203/rs.3.rs-4197809/v1 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

〔学会発表〕　計5件（うち招待講演　1件／うち国際学会　0件）

| |
|---|
| １．発表者名<br>土井康平，菅原健 |
| ２．発表標題<br>自己混合干渉法による安価なレーザー振動計を用いた盗聴攻撃 |
| ３．学会等名<br>2023年暗号と情報セキュリティシンポジウム（SCIS2023），2E3-1，2023 |
| ４．発表年<br>2023年 |

| |
|---|
| １．発表者名<br>Yan Long，Sara Rampazzi，菅原健，Kevin Fu |
| ２．発表標題<br>ワクチン低温物流に関わる温度センサのアナログサイバーセキュリティ， |
| ３．学会等名<br>2022年暗号と情報セキュリティシンポジウム（SCIS2022），3C3-4 |
| ４．発表年<br>2022年 |

| |
|---|
| １．発表者名<br>土井康平，菅原健 |
| ２．発表標題<br>レーザー振動計を用いたMLCCからの音響サイドチャネルリークの測定 |
| ３．学会等名<br>2022年暗号と情報セキュリティシンポジウム（SCIS2022），3C3-5 |
| ４．発表年<br>2022年 |

| |
|---|
| １．発表者名<br>土井康平，菅原健 |
| ２．発表標題<br>レーザー振動計を用いた音響サイドチャネル攻撃の基礎実験 |
| ３．学会等名<br>IEICE 2021年ソサイエティ大会 |
| ４．発表年<br>2021年 |

| |
|---|
| １．発表者名<br>菅原健 |
| ２．発表標題<br>アナログ領域でセンサーへ誤情報を挿入する攻撃 |
| ３．学会等名<br>ハードウェアセキュリティフォーラム2023（招待講演） |
| ４．発表年<br>2024年 |

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（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 |
|---|---|