様　式　Ｆ－１９－２

科学研究費助成事業　　研究成果報告書

令和　　３ 年　　８ 月 １３ 日現在

機関番号：１２６１２
研究種目：国際共同研究加速基金（国際共同研究強化(A)）
研究期間：2018～2020
課題番号：１８ＫＫ０３１２

研究課題名（和文）レーザを用いてセンサに誤情報を挿入する攻撃のアナログサイバーセキュリティ

研究課題名（英文）Analog Cybersecurity of Laser-Based Sensor Spoofing Attack

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）　　3,800,000円
渡航期間：　　６ヶ月

研究成果の概要（和文）：スマートフォンやスマートスピーカーで使われる小型マイクにレーザーを照射することで，実際には無音であるにも関わらず，あたかも音声を受信したかのような電気信号を発生させることができる現象を発見した．また，この現象が音声アシスタントに及ぼす脅威を明らかにした．市販されている機器に対して安全性評価を行い，レーザーポインター程度のパワーで，100メートル以上先から攻撃ができることを明らかにした．本研究成果により，セキュリティ分野のトップカンファレンスである USENIX Security に採録を受けた．本脆弱性について責任ある脆弱性開示を行い，対策構築に協力した．

研究成果の学術的意義や社会的意義
センサに誤情報を挿入する攻撃は活発に研究されているが，提案法は，物理量変換（光から振動）を伴う初めて攻撃である点に大きな学術的意義がある．また，スマートスピーカーのマイクを対象とする攻撃研究の流れとしては，従来法の数倍に攻撃可能距離を延伸した点に意義がある．また，成果への社会的関心も高く，脆弱性開示のタイミングでは，CNN を始めとする一流メディアで報道された．また，スマートスピーカーのメーカーなどの関係各所に対して脆弱性開示するとともに，攻撃の理解と対策について協力を行った．

研究成果の概要（英文）：We discovered a new attack that injects arbitrary audio signals to a target microphone by aiming an amplitude-modulated light at the microphone’s aperture, and proposed a command injection attack on voice-controllable systems such as smartphones and smart speakers. We evaluated several products showing that we can achieve a successful injection from more than 100 meters using laser power similar to ordinary laser pointers. The paper is accepted at USENIX Security 2020, which is one of the most prestigious conference in the computer-security research field. We made responsible disclosure and collaborated with the vendors for mitigating the vulnerability.

研究分野：セキュリティ

キーワード：ハードウェアセキュリティ　センサのセキュリティ　音声アシスタント　レーザー　光音響効果

様　式　Ｆ－１９－２

１．研究開始当初の背景

情報システムを実世界の機器に接続することで，自動車・ロボット・工場などを自動化する技術が期待されている．そのようなシステムの末端にはセンサがあり，ディジタルとアナログの世界を橋渡ししている．それに対し年，アナログ領域でセンサに誤信号を挿入する攻撃の脅威が注目を集めている．未だディジタル情報になっていないアナログ情報は，既存の情報セキュリティ技術では守ることができない．そのため，センサがシステムの最弱点になることが懸念される．それに対し応募者は，誤信号挿入の手段にレーザが利用された場合，遠くから大きいエネルギーを挿入できるという性質上，極めて深刻な脅威になりうるという着想を得た．そこで，攻撃の脅威と対策法を明らかにして，将来の脅威に備えるために，基課題を立案した．

基課題の研究成果として，レーザ照射によって対象物体に振動を発生させることができることが分かった．これは，マイクに誤信号を挿入する強力な手段になりうることが明らかになった．基課題は，センサの物理層を範囲としており，アプリケーションへの影響は机上検討に留めていた．しかし，予想を上回る進捗を得たことで，センサだけではなく，スマートスピーカーや自動運転車などのアプリケーションのセキュリティ（アナログサイバーセキュリティ）に研究を拡張する道筋を得た（図１）．しかし，研究の遂行には，アプリケーションのセキュリティに関する豊富な研究経験と，ケーススタディのための実験設備が不可欠である．そこで，その両者を兼ね備えた共同研究者との国際共同研究を立案するに至った．

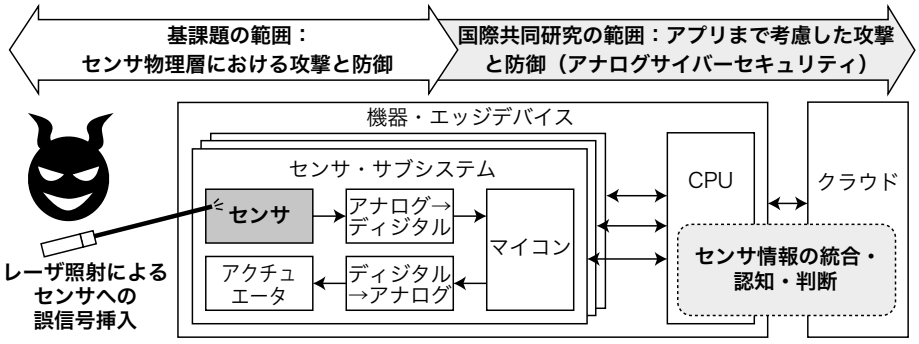

図１　センサを備えた情報システムに対する，レーザー照射によるセンサへの誤信号の挿入と，基課題と本研究課題の関係

２．研究の目的

本研究は，オフェンシブセキュリティの分野にあり，未知の脆弱性を発見し，その被害の深刻さを科学的な方法で検証した上で，関係各所と調整の上で公開することが目的である．そうすることにより，(i) その脆弱性が悪用される前に，事前に対策を行うことができる，また，攻撃技術をオープンの議論することで，社会全体としてセキュリティを高めていくことができる．

本研究は特に，基課題のテーマである「レーザー照射によるセンサへの誤信号挿入」を，オフェンシブセキュリティの観点から研究する．それにより，次の問いに答えることが目的である．

- センサに対してレーザー照射が可能なユースケースは何か？
- レーザー照射により引き起こされる被害は何か？
- 対策するにはどうしたら良いか？

３．研究の方法

まず，上記の問いを元に脅威分析を行った．「レーザー照射によるセンサへの誤信号挿入」では，対象のセンサーにレーザーを照射することが，攻撃者にとっての大きな制約となる．多くの製品では，シャーシが光を遮蔽するためである．以上の制約条件の基で検討を重ねたところ，マイクが重要なユースケースであるとの結論に至った．音波を取り入れなくてはならないという性質上，マイクは開口部を介して外界に対して露出しており，そこから光が侵入するためである．中でも特に，スマートスピーカーに代表される音声アシスタントに使われるマイクへ音声信号を挿入することができれば，情報システムにおけるセキュリティ上の被害を引き起こす可能性があることが分かった．

以上より，レーザー照射を元に，遠隔から無音で音声コマンドを挿入する LightCommands の着想に至った． LightCommands の実現可能性と，その深刻さを定量的に評価するために，以下の小課題に分解し，それぞれを解決するというアプローチで研究を行った．

- レーザー照射によってマイクに生じる電気信号の特性の評価
- 攻撃可能な距離・状況の定量的評価
- 音声コマンドの挿入により生じる被害の調査
- 対策法の検討

４．研究成果

レーザー照射によってマイクに生じる電気信号の特性の評価　スマートスピーカーなどで一般的な MEMS マイクを対象に基礎実験を行い，レーザー照射実験を行った．その結果，強度を振幅変調したレーザー光を照射すると，ほぼ線形な変調信号がマイク出力に現れることを明らかにした．これはすなわち，任意の音声信号を対象のマイクに挿入できることを意味している．また，これが，多くの MEMS マイクで生じる一般的な現象であること，レーザーポインタ程度の弱い光でも十分に生じることを明らかにした．

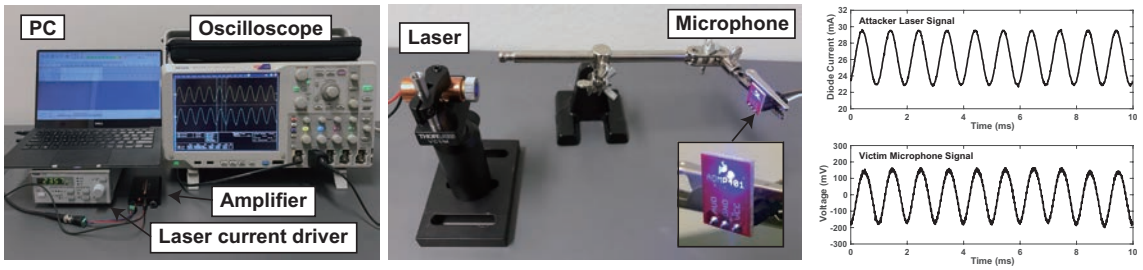

図 2　MEMS マイクを搭載した評価基板を用いた基礎実験．（左）評価装置の全体．（中央）レーザーダイオードから照射した光をマイクの開口部に照射する様子．（右）強度変調したレーザーの振幅に対応する信号が，マイクより出力された様子

攻撃可能な距離・状況の定量的評価　複数の音声アシスタント（Amazon Alexa，Apple Siri，Facebook Portal，そして Google Assistant）に対応する機器（スマートフォンとスマートスピーカーを含む合計 18 機種）を評価し，その全てでレーザー照射による音声コマンド挿入が行えることを明らかにした．また，以下の写真に示すようなセットアップで実験を行い，攻撃可能な距離を定量的に評価した．その結果，特に感度が高い機器では，レーザーポインタ程度の弱い光でも 110 メートル以上の遠方から攻撃できることを示した．

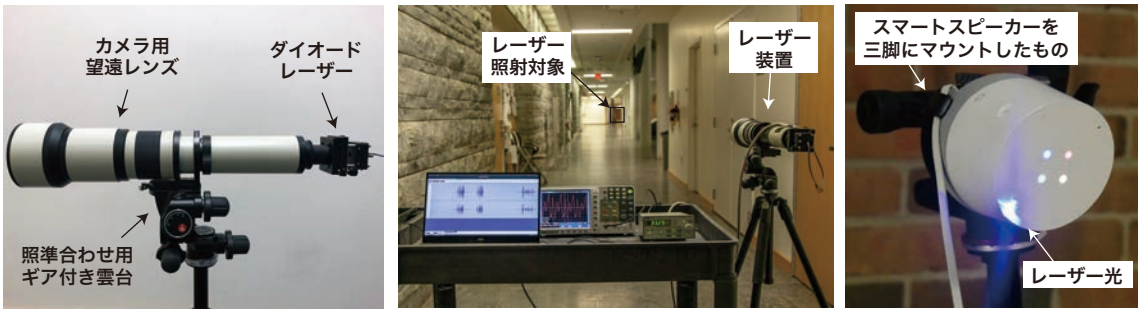

図 3.　攻撃可能な距離を調べる実験の様子：（左）レーザーを望遠レンズにマウントした装置，（中）110 メートル遠方にあるスマートスピーカーに照準合わせをしている様子，（右）対象にレーザーが当たっている様子

また，制御されていないより現実的な状況でも攻撃が可能であることを示すために，図 4 に示すように，70 メートル離れた建物から，隣の建物の一室に対して窓ガラスを貫通してレーザー照射を行い，その場合でも攻撃が可能であることを実証した．

図 4　70 メートル離れた隣の建物から，窓ガラス越しにレーザーを照射することで音声コマンドを挿入する実証実験の様子

音声コマンドの挿入により生じる被害の調査　LightCommands により，攻撃者は，正規所有者に気づかれること無く，遠隔から音声コマンドを挿入することができる．そのことが，どのような脅威を引き起こしうるのかを研究した．音声アシスタントは，さまざまな周辺機器と連携して動作するため，脅威は，それらの周辺機器の提供する機能に対応する．そこで，セキュリティ上の意義が大きいと思われる周辺機器をリスト化し，安全性評価を行った．

研究の結果，音声アシスタントにはセキュリティの認証が全く無い場合や，もしあったとしても不適切な実装がされている（例: PIN を総当りできる）場合があることを明らかにした．その結果，(i) スマートロックの解錠，(ii) ガレージドアの開放，(iii) E コマースサイトによる買い物，および (iv) VCS に接続された特定車種（Tesla および Ford）の位置特定，解錠，およびエンジン始動が行えることを示した．

対策法　以上の評価実験における知見を元に，いくつかの対策法を提案した．(ハードウェア再設計を伴わない) ソフトウェアによる対策法としては，認証の層を追加することで攻撃を緩和できることを示した．また，ユーザと機器の間で簡単なインタラクションをすることや，複数マイクを用いて異常検知を行うことでも攻撃の難易度を上げることができることを示した．ハードウェアによる対策としては，機器をカバーなどで覆うことで，攻撃者からマイクまでの視線を遮ることことが対策になることを示した．

産業界への還元　責任ある脆弱性開示（Responsible Disclosure）の実践に従い，関連企業・機関に対して事前に脆弱性開示を行い，合意した情報解禁日(2019 年 11 月 4 日)に公知化した．また，関連企業・機関の技術者と連携して，発見した攻撃の理解と緩和法構築に協力した．事前に連絡を行った企業・機関は以下の通りである：Google, Amazon, Apple, August（スマートロック製造者), Ford, Tesla, Analog Devices（MEMS マイクの製造者), ICS-CERT（産業機器に関する脆弱性を取り扱うコーディネーター), およびアメリカ食品医薬品局（FDA）.

出版物　セキュリティ分野のトップカンファレンスである USENIX Security Symposium 2020 に（採録率 16.1%, T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, “Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems,” USENIX Security Symposium 2020, 2020）に採録を受けたのが主たる研究成果である．この成果を国内に周知することを目的に，国内学会（コンピュータセキュリティシンポジウム 2020）において日本語でも発表した．また，複数の学会・学会研究会において招待講演を行った:

- SPQR Laboratory Embedded Security Workshop
- 暗号と情報セキュリティワークショップ 2020
- 第 5 回 IoT セキュリティフォーラム
- FIT2021 トップコンファレンスセッション（発表予定）

また，上記発表に関連して，電子情報通信学会・情報セキュリティ研究会・研究会活動貢献感謝状の授与を受けた．

アウトリーチ活動　本研究のインパクトは大きく，一般メディア（New York Times, CNN, Washington Post ほか）および技術メディア（Wired, Ars Technica）で報道がされた．著者によるデモ動画は YouTube において，累計 30 万回以上再生された．また，技術メディアによる

研究紹介の動画は，執筆次点で 430 万回以上再生された.

研究の発展　LightCommands の研究の過程で，レーザー照射による音声信号の挿入は，光電効果と光音響効果が混ざった複雑なメカニズムによって生じていることが明らかになった．脆弱性の根本的な解決には，レーザー照射により音声信号が挿入できる物理メカニズムの解明が必要であるとの知見に至り，メカニズム解明のための実験と研究テーマ立案を行った．本項目については，2021 年度より，基盤（C）の枠組みで研究を継続する．その基盤（C）も，ミシガン大学と共同で実施する.国際科研により得た機会を,継続的な共同研究に発展させることができた.

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu	４．巻 2020
２．論文標題 Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems	５．発行年 2020年
３．雑誌名 USENIX Security Symposium 2020	６．最初と最後の頁 2631--2648
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス 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 －

〔学会発表〕　計4件（うち招待講演　3件／うち国際学会　0件）

１．発表者名 菅原 健, シア ベンジャミン, ランパッジ サラ, ゲンキン ダニエル, フー ケビン
２．発表標題 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．学会等名 コンピュータセキュリティシンポジウム2020
４．発表年 2020年

１．発表者名 菅原健
２．発表標題 ライトコマンド: レーザー照射により音声コマンドを挿入する攻撃
３．学会等名 第5回 IoTセキュリティフォーラム（招待講演）
４．発表年 2020年

１．発表者名 T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu
２．発表標題 Light Commands: レーザーを用いて音声コマンドを挿入する攻撃
３．学会等名 暗号と情報セキュリティワークショップ2020（招待講演）
４．発表年 2020年

１．発表者名
T. Sugawara

２．発表標題
Laser Injection Attacks on Integrated Circuits and Sensors

３．学会等名
SPQR Laboratory Embedded Security Workshop（招待講演）

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
Laser-Based Audio Injection on VCS
https://lightcommands.com
レーザーを用いて音声コマンドを挿入する攻撃
https://lightcommands.com/index_jp.html
Youtube にアップロードした解説動画
https://www.youtube.com/channel/UC2y3z169n9xXxPEBtxcAYjA

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
主たる渡航先の主たる海外共同研究者	Ｆｕ　Ｋｅｖｉｎ (Fu Kevin)	ミシガン大学・EECS・Associate Professor	

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			
米国	ミシガン大学			