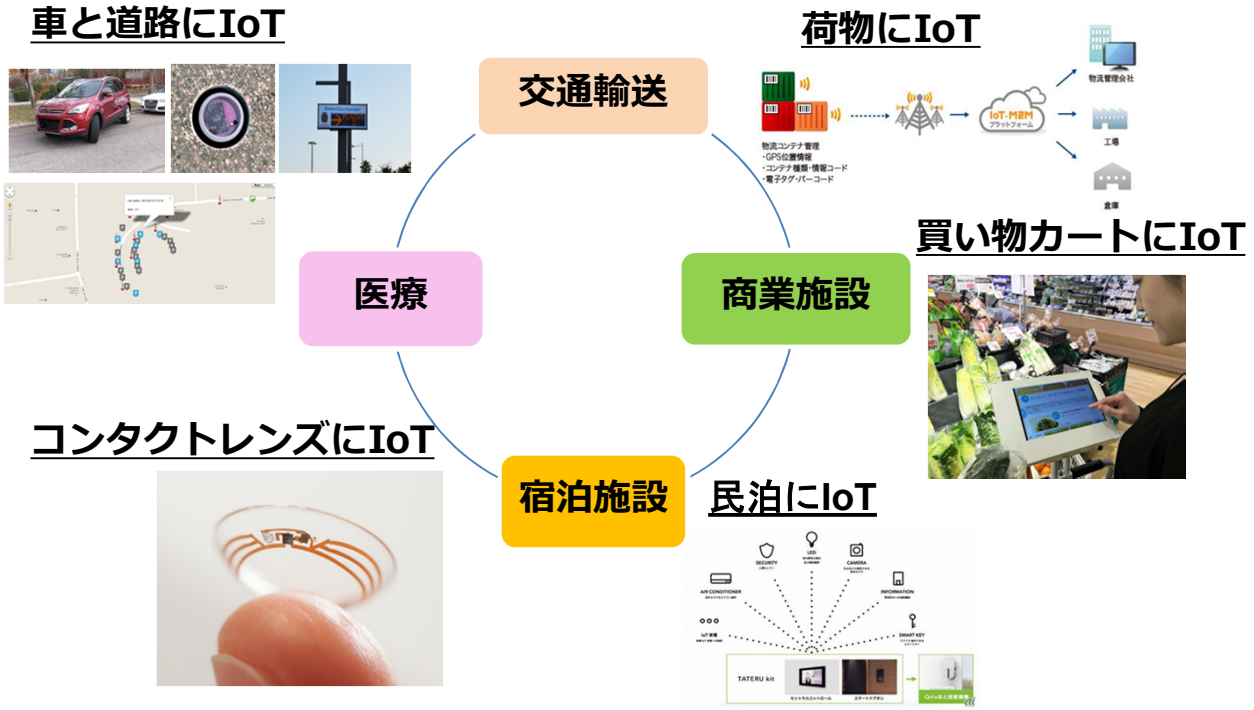
2018年度
ISSスクエアシンポジウム
研究成果報告

2019/2/22

システム分科会

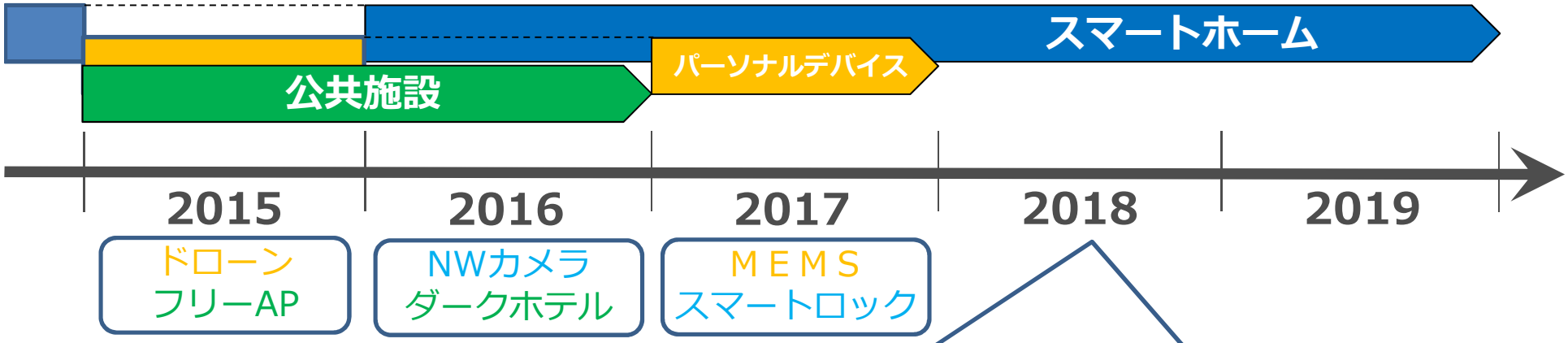
システム分科会のテーマ

- The Internet of Thing(IoT)s
  あらゆるものがインターネットにつながる
  （2020年までに200億～500億）※IDC調査



キーワード：IoTの脅威検証

今年度の取り組み



複合的脅威シナリオに基づく各脅威要素の実現性検証

- キーデバイス：「スマートスピーカー」


Google Home


Amazon Echo


LINE CLOVA

- 選定理由
  - 普及し始めたばかりで未成熟な分野
  - 新しいUIゆえに想定されていない脅威が存在

脅威シナリオ

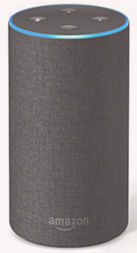
スマートスピーカーを介したホーム内への攻撃

① ホーム内への攻撃

②スマートスピーカーの不正操作

②−1 キャスト
②−2 スキル

①−1 攻撃音声
（音声コマンド）



他の音声認識デバイス

①−2 音波

MEMS（加速度センサ）

脅威要素①
ホーム内への攻撃

①-1 ホーム内への攻撃：攻撃音声

■ 攻撃音声とは

- □ 人には認識できないが、スマートスピーカーには認識できるように音声コマンドを埋め込んだ音声

■ 攻撃音声（音声コマンド）の作成検証

手法１）超音波に埋め込む

手法２）他の音声にノイズとして埋め込む

①-1 ホーム内への攻撃：攻撃音声

■ 攻撃音声とは

□ 人には認識できないが、スマートスピーカーに認識できるように音声コマンドを埋め込

■ 攻撃音声（音声コマン 検証

手法１）超音波に

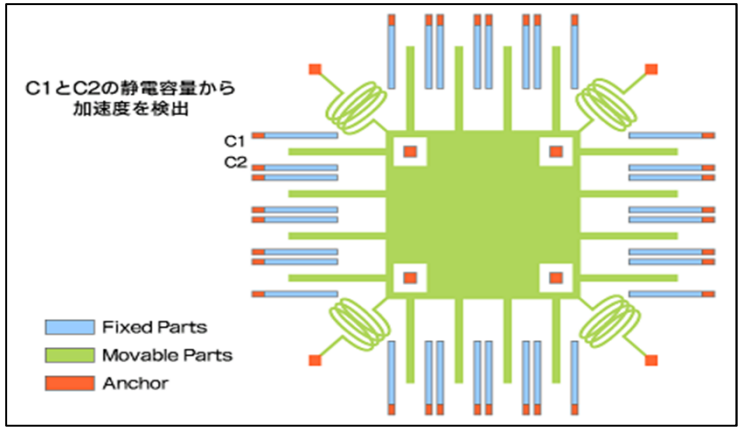
手法２） イズとして埋め込む

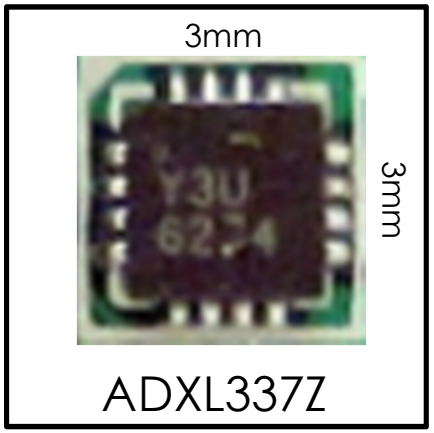
現状、攻撃音声作成には至らず

①-2 ホーム内への攻撃：MEMSへの音波攻撃

ISS square system

- MEMS加速度センサーとは
  - バネの変動から加速度を測定する微細なデバイス





  - スマートフォンやゲーム端末、医療機器などに搭載

- 共振を利用したセンサーの誤動作検証

  昨年度：センサー出力値を変動させることに成功

  今年度：センサー出力値を安定的に任意の方向に
  変動させることに成功

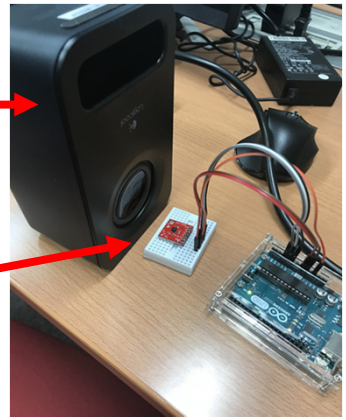
成功

①-2 ホーム内への攻撃：デモ

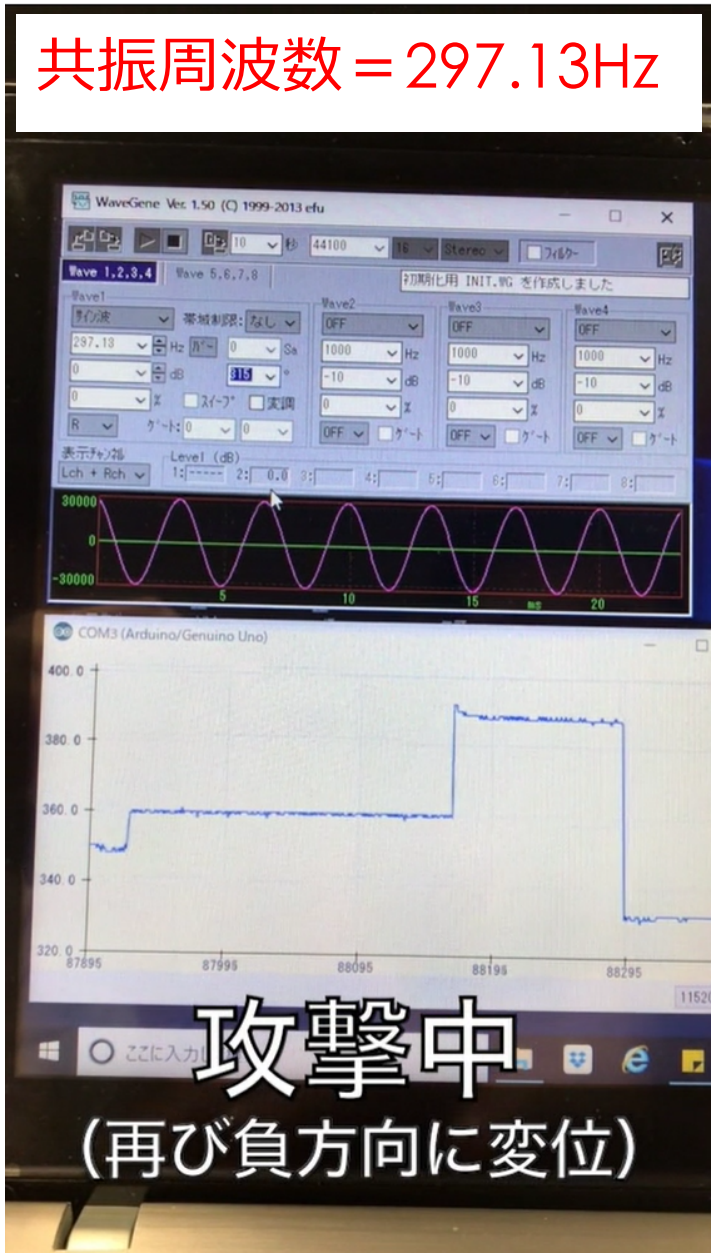
■ 音波ハッキング

スピーカー

MEMS
加速度センサー
（ADXL337）



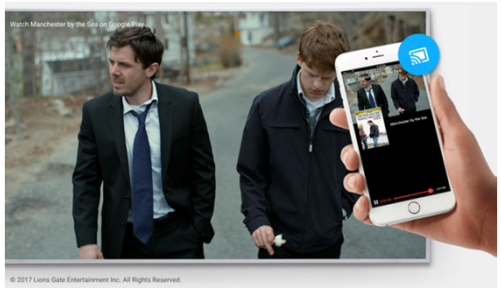
- 1つの軸の出力値をほぼ一定に変化させることができた
- 変化の方向は位相で調整



脅威要素②
スマートスピーカーの不正操作

②-1 スマートスピーカー不正操作：キャスト

- キャストとは
  - 映像・音楽を対応デバイス上で再生させる機能



Google Cast (Chromecast)

Alexa Cast

■ キャストを利用した操作検証

- Google Homeに任意の音声を再生させることに成功

端末特定が容易
認証がない

LAN内へ侵入できれば
簡単に操作できる

成功

https://www.google.com/intl/en_us/chromecast/built-in/
https://www.amazon.co.jp/b?node=5921301051

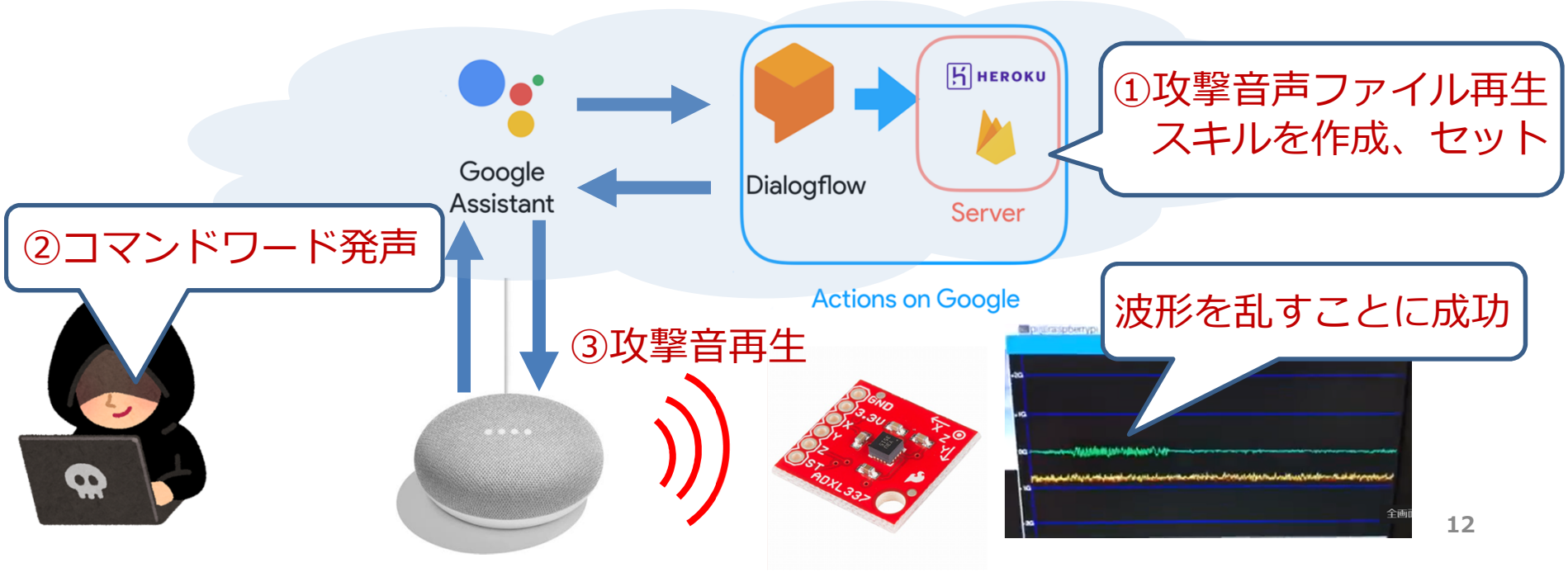
②-2 スマートスピーカー不正操作：スキル

- スキル（アクション）とは
  - 音声アシスタントの追加拡張機能（≒アプリ）
    - サードパーティサービス連携など

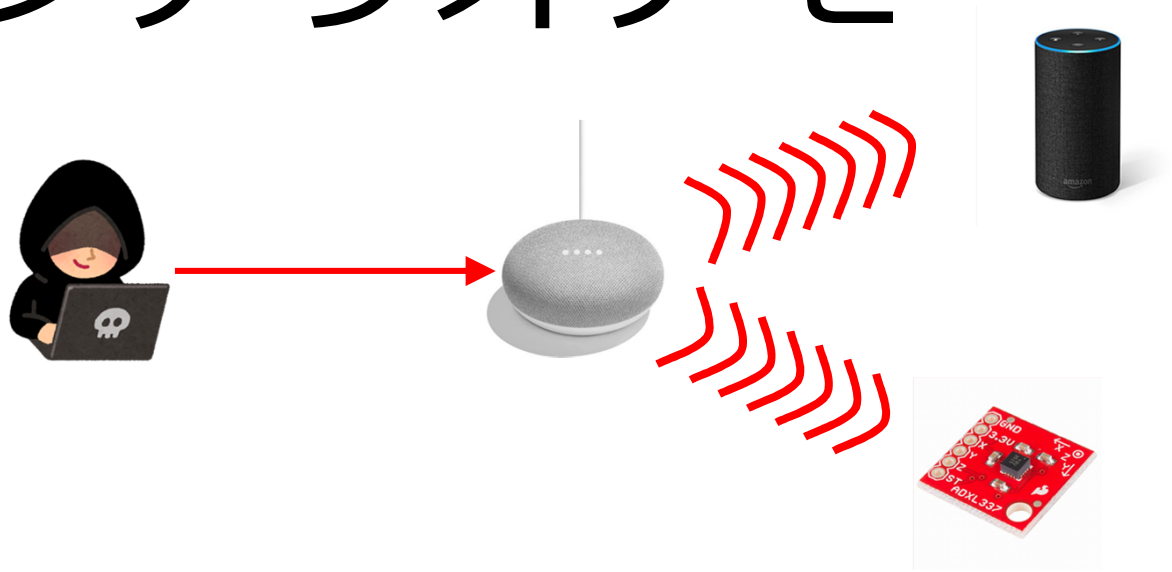
成功

■ カスタムスキルを利用した操作検証

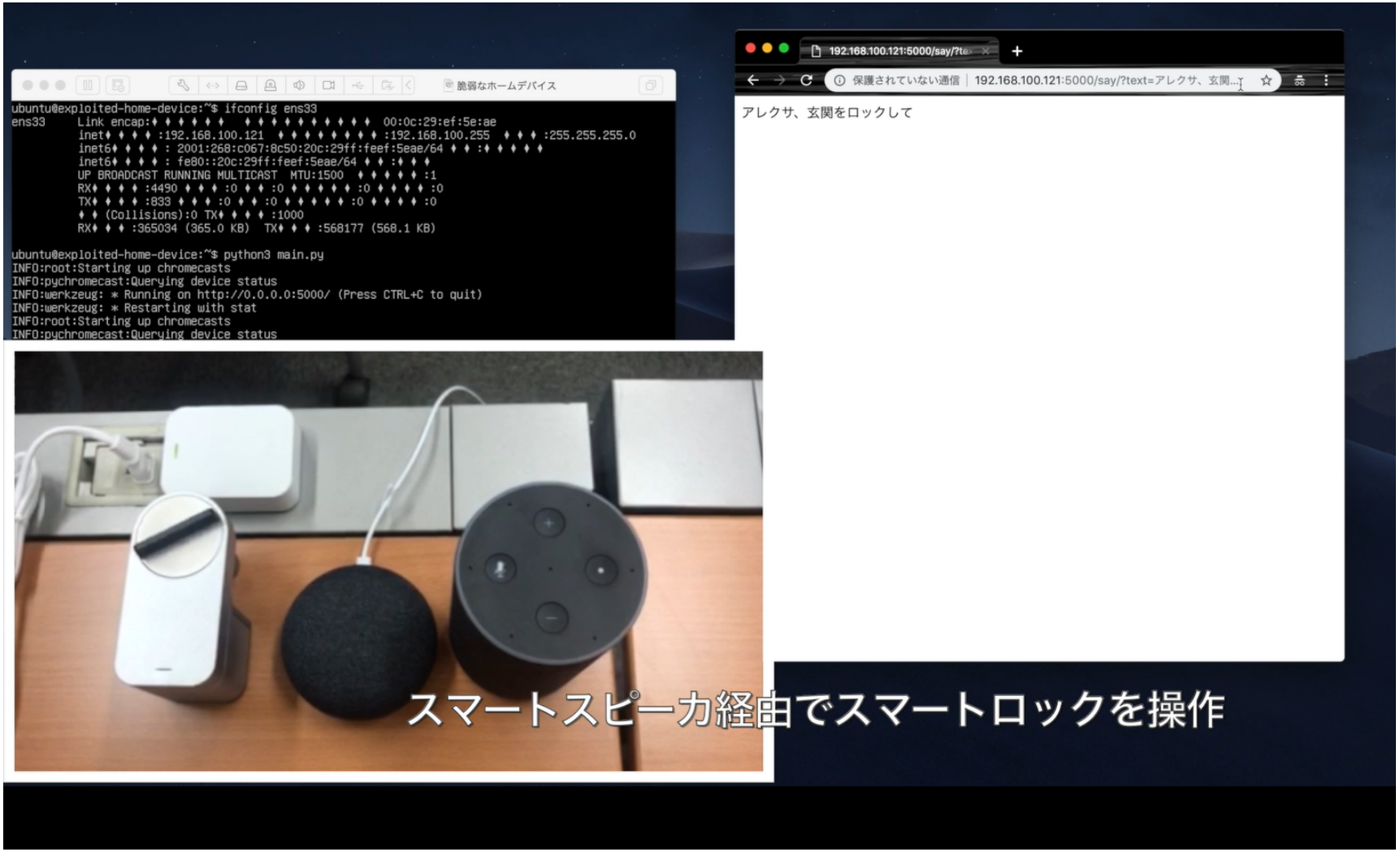
- Google Homeに任意の音声を再生させることに成功
  - MEMSのセンサー出力値を乱すことにも成功



脅威シナリオデモ



キャストによる攻撃デモ



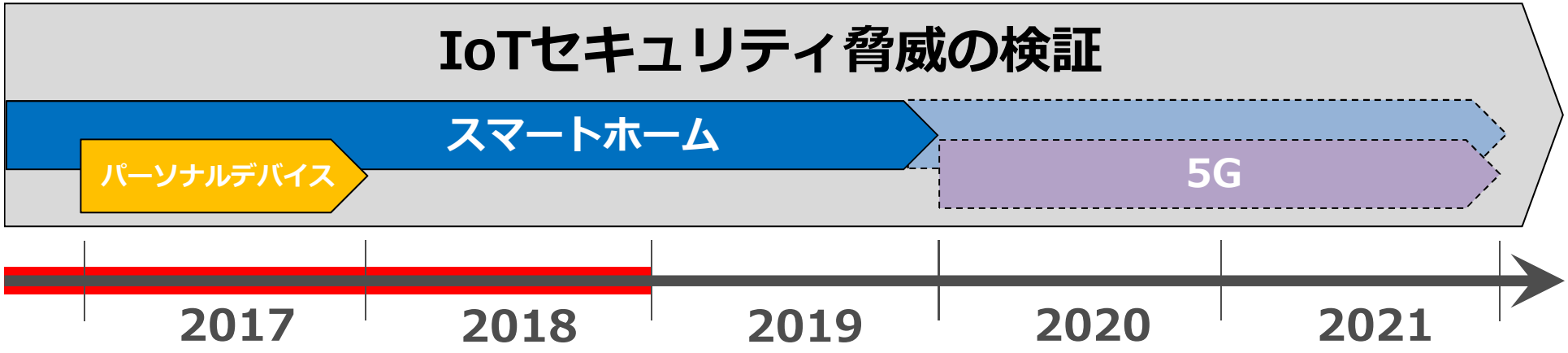
デモ補足

- 多様な攻撃ベクター
  - 同様な操作はスキルでも可能
  - 音波を出してセンサを狂わせることも可能

- 対策提言
  - 利用者視点
    - ⑩怪しいスキルは入れない
    - ⑩ウェイクワード・デバイス名はデフォルトから変更
    - ⑩スマートスピーカーの近くに音声認識デバイスを置かない
  - 開発者視点
    - ⑩ セキュアなスキルマーケット設計
    - ⑩ 音声認証やそれ以外の技術を用いた発話者認証機構
      - ⑩ GoogleアシスタントにはあるがAmazonAlexaにはない

今後

今後のロードマップ



スマートロックの
脆弱性調査

スマートスピーカーの
脆弱性調査

ホームコントロールの
脆弱性調査

MEMSの
音波ハッキング

スマートホームの脅威シナリオ検証（継続予定）

- 攻撃音声
  - トップカンファレンスに取り上げられている
    トピック（＝難しい）だが引き続きチャレンジ
- センサー
  - 加速度センサー搭載製品に攻撃
  - 加速度センサーを誤作動させることによる
    脅威シナリオの検討

APPENDIX

攻撃音声

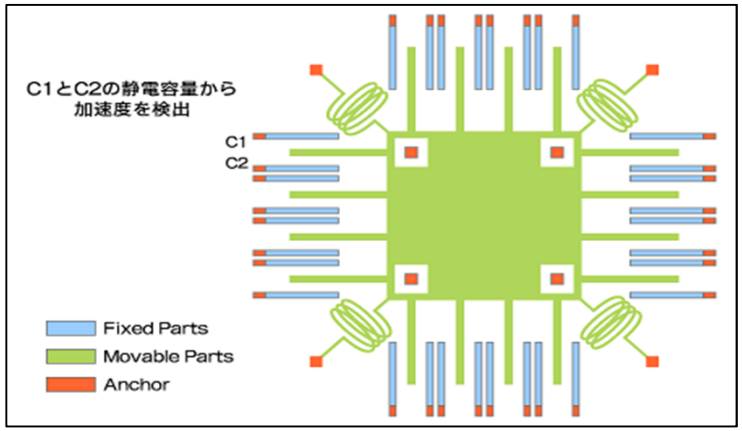
攻撃音声に関する既存研究

- 超音波に音声コマンドを埋め込む方法
  - Zhang, G. et al.: **DolphinAttack: Inaudible Voice Commands**. CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp.103-117. 2017. (https://acmccs.github.io/papers/p103-zhangAemb.pdf)
- 他の音声にノイズとして音声コマンドを埋め込む方法
  - Carlini,N. and Wagner,D.: **Audio Adversarial Examples: Targeted Attacks on Speech-to-Text**, arXiv:1801.01944, 2018. (https://arxiv.org/abs/1801.01944)
  - "**Targeted Adversarial Examples on Speech-to-Text systems**", https://github.com/carlini/audio_adversarial_examples
  - Yakura,H. and Sakuma,J.: **Robust Audio Adversarial Example for a Physical Attack**, arXiv:1810.11793, 2018. (https://arxiv.org/abs/1810.11793)
  - Taori,R. et al.: **Targeted Adversarial Examples for Black Box Audio Systems**, arXiv:1805.07820, 2018. (https://arxiv.org/abs/1805.07820)
  - "**Targeted Adversarial Examples for Black Box Audio Systems**", https://github.com/rtaori/Black-Box-Audio

MEMS

MEMS加速度センサー

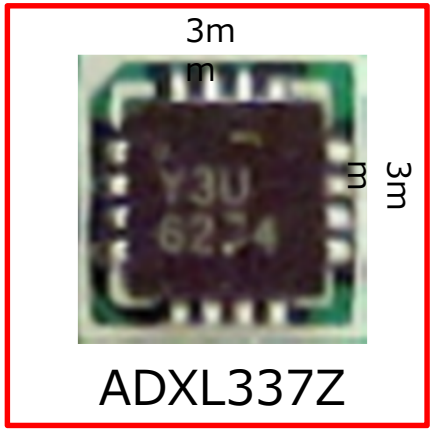
- 構造



＊1

- Movable Partsが静電容量を変化させ、これをFixed Partsが読み取る
- 静電容量を検出の部分で、バネと繋がっているところから誤差を出す

- センサーに対する音波ハッキング
  - ⑩ 先行研究*2で「音波を使ってデバイスをハッキングする方法」が発見される
  - ⑩ センサを使った検証を、やってみた



*1 "Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks", Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, Kevin Fu IEEE European Symposium on Security & Privacy, 2017.

*2 EDN Japan, いまさら聞けない加速度センサ入門 http://ednjapan.com/edn/articles/1205/16/news110.html

搭載製品例

型番	主な用途	搭載製品例
H3LIS331	ゲームリモコン	
IIS2DH	産業用機器	
LIS3DH	ゲーム機、携帯電話、リモコン	iPhone4
ADXL362	補聴器	
ADXL350	携帯端末、医療機器	
ADXL345	医療機器、HDD保護	
ADXL337	スマートフォン	galaxy s5
BMA220	携帯電話、携帯音楽プレーヤー	iPhone 5s
MPU6050	携帯端末、健康器具	iPhone 6/6s

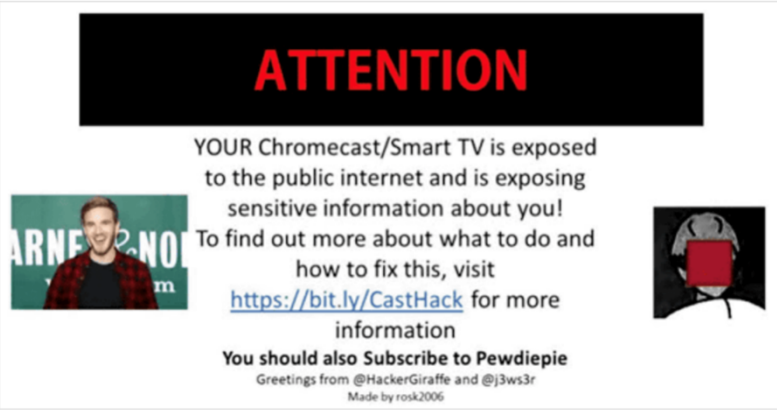
キャスト

キャストの脅威事例

2019年01月04日 13時00分

セキュリティ

Googleのストリーミング端末「Chromecast」がハッキングされ人気YouTuberの宣伝を垂れ流す



ハッキングされたTVに表示された画面

ハッキング画面で指示されたWebページ

- ホームルータの脆弱性（UPnPの設定不備など）を突いて、遠隔アクセスしたとみられている
  - 同様の攻撃はGoogle Homeでも成立する

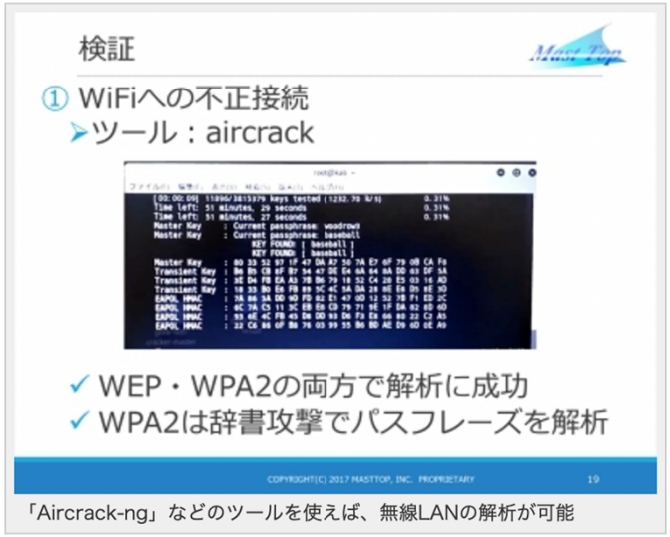
https://gigazine.net/news/20190104-google-chromecast-hijacked-pewdiepie/

スマートホームへの侵入経路（Wifi）

スマートホームが隣人に操作される可能性も、市販IoT機器にセキュリティ問題

マストトップ・松本潤氏、IoT機器におけるセキュリティ検証の重要性を強調

森田 秀一　2017年11月24日 06:00



「Aircrack-ng」などのツールを使えば、無線LANの解析が可能

一度宅内ネットワークに侵入されると、「Zenmap」のような一般的なポートスキャンツールがあれば機器構成が丸裸に

- Wifiへの不正接続からホーム内IoT機器に不正ログインされうることを検証
  - Wifi侵入後はデモと同様の攻撃が可能

https://internet.watch.impress.co.jp/docs/event/1093083.html

踏み台にされうるIoT機器の脅威

meross-mss110-vuln

A short writeup on a telnet vulnerability in the Meross MSS110 Smart Plug which is way too common in IoT devices.

```
root@kali:~# telnet 192.168.1.51
Trying 192.168.1.51...
Connected to 192.168.1.51.
Escape character is '^]'.
Login as:^]
telnet> set crlf
Will send carriage returns as telnet <CR><LF>.
^MInvalid User Name
Login as:admin^MPassword:^M
CFG>ls^Mget         set         del         prof
```

実際にtelnetログインした様子

画像にマウスを合わせると拡大されます

wifiスマートプラグ スマートコンセント 音声コントロール 直差しコンセント 2ピン 遠隔操作 日本語アプリ Googleホーム対応 スケジュール設定 電気スイッチコントロール 2個入り

Conico

★★★★☆ 83件のカスタマーレビュー | 7人が質問に回答しました

ベストセラー1位 - カテゴリ 電設用コンセント・プラグ

価格: ~~¥ 2,999~~

セール特価: ¥ 2,549 通常配送無料 詳細

OFF: ¥ 450 (15%)

クーポン 500円OFFクーポンの適用 詳細

100% カートに入りました

2/21 木曜日 にお届けするには、今から1 時間 54 分以内に当日お急ぎ便（代金引換未対応）を選択して注文を確定してください（Amazonプライム会員は無料 詳細を見る

この商品は、ConicoDirectが販売し、Amazon.co.jp が発送します。 この出品商品にはコンビニ・ATM・ネットバンキング・電子マネー払いが利用できます。 ギフトラッピングを利用できます。

新品の出品：1¥ 2,999より

Amazon Certified

works with alexa Alexa デバイスの音声を介して、この商品をお客様の声でコントロールします

同一メーカの製品（2019/2/20時点でベストセラー1位）

- メジャーなスマートコンセントに
  ハードコードされたtelnet脆弱性（CVE-2018-6401）

https://garrettmiller.github.io/meross-mss110-vuln/

スキル

スキルの脆弱性に関する既存研究

- Ron Marcovich, Yuval Ron, Amichai Shulman and Tal Be’ery, “**Open Sesame: Picking Locks with Cortana**”, BlackHat USA 2018, 2018

- Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Henne nfent, Joshua Mason, Adam Bates, and Michael Bailey, “**Skill Squatting Attacks on Amazon Alexa**”, 27th USENIX Security Symposium (USENIX Security 18), 2018