

2023年度 ISSスクエアシンポジウム 研究成果報告

2024/03/01
システム分科会

● 概要

“The Information Security of things”をキーワードに、一般家庭の機器に組み込まれる小さいITシステムから、社会インフラの中に組み込まれる大規模ITシステムまでを俯瞰し、それを支えるセキュリティシステム技術の現状と課題について、研究を行っている。

● メンバーリスト（院生11名、指導教授2名）

RL :情セ大 大久保 隆夫、須崎 有康

幹事

中央大 M1 : 浅田 勇飛

情セ大 M2 : 澤田 直哉

メンバー

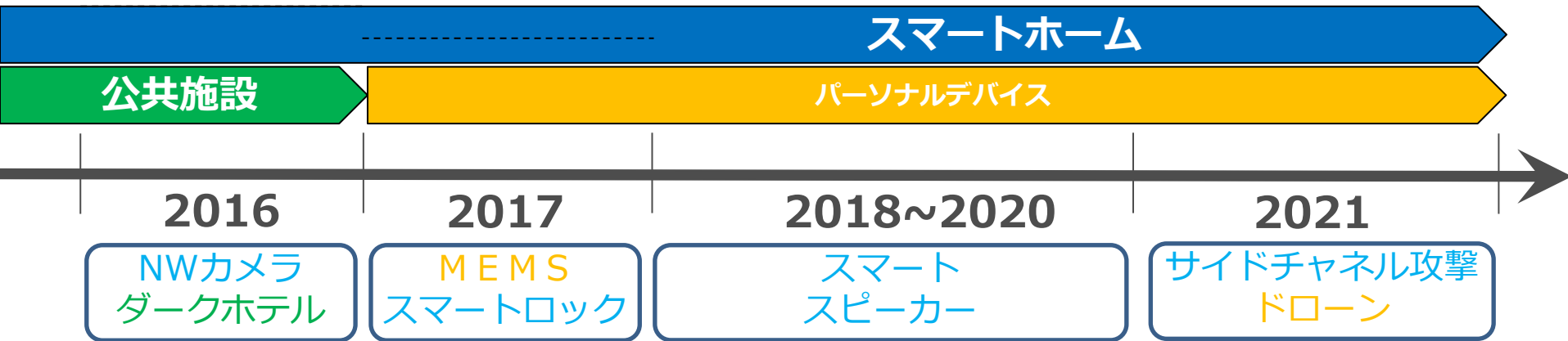
情セ大 M2 : 廣田 凧、一葉 修平

情セ大 M1 : 松坂 惇平、卓 珮如、岩崎 瞬、江 鴻浩、中村 裕太、弓濱

まどか

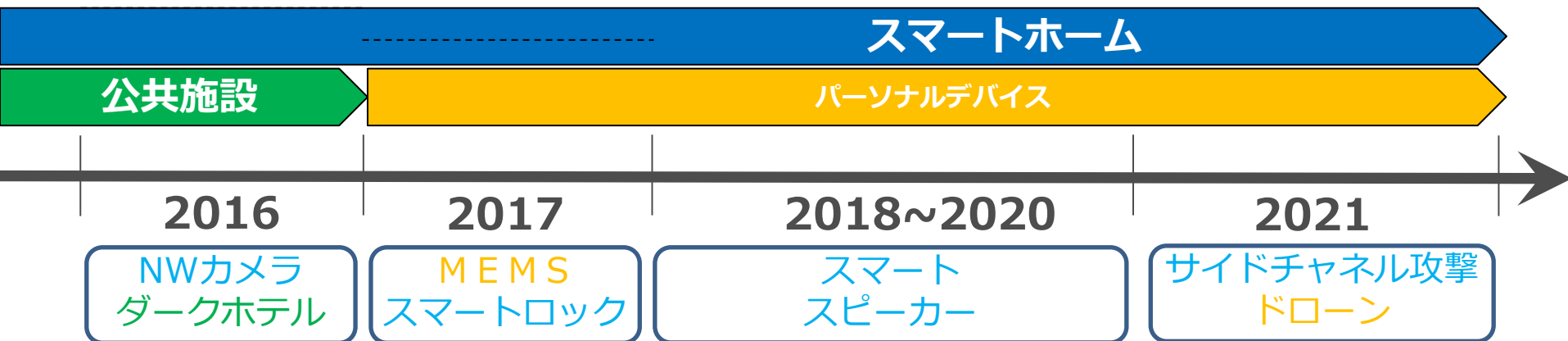
中央大 M1 : 今枝 俊輔

活動報告（これまでの取り組み）

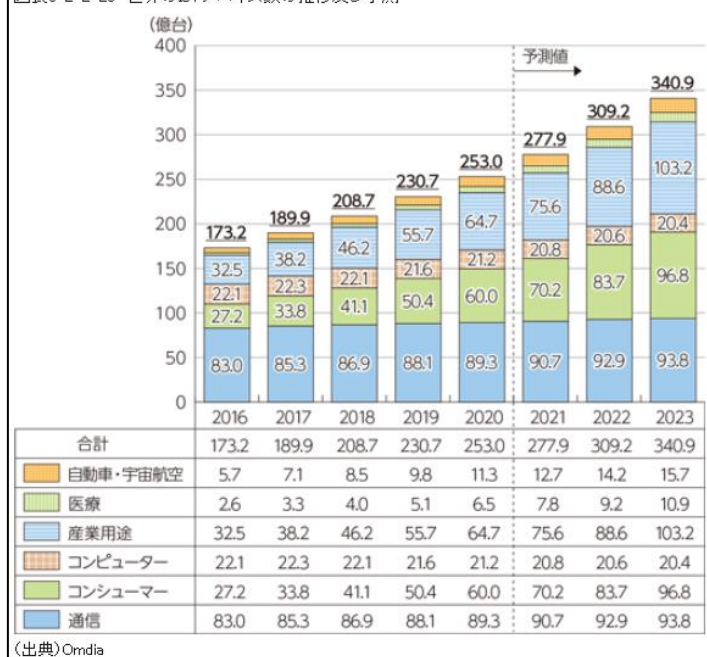


さまざまなものに
コンピュータが搭載され
それがインターネットに
接続される世の中に
(Internet Of Things)

活動報告（これまでの取り組み）



図表0-2-2-29 世界のIoTデバイス数の推移及び予測¹⁸



- ・ Bluetoothデバイスを含むIoTデバイスは増加傾向
- ・ 今後も増加する予測
- ・ デバイスは生活やプライバシーに密着
- ・ 生成系AIとも組み合わせ活用方法も広がる

活動報告（今年度の取り組み～脅威シナリオ～）

人々の生活を中心に見据えた、セキュリティ脅威の検証

スマートホーム

パーソナルデバイス

2022

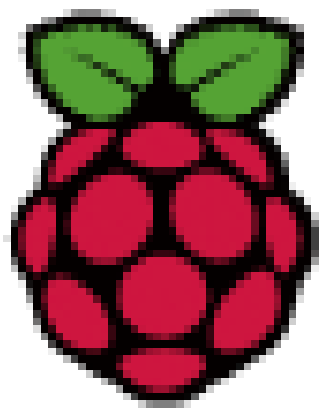
ルータ
スマートタグ

2023

ラズベリーパイ
Bluetooth機器

2024～

活動	日時		場所
第1回	2023年5月27日（土）	20:00～20:30	IISEC202教室
第2回	2023年6月17日（土）	20:00～20:30	IISEC202教室
第3回	2023年7月15日（土）	12:30～15:00	IISEC202教室
第4回	2023年10月14日（土）	13:00～15:00	IISEC202教室
第5回	2023年11月25日（土）	14:00～15:00	IISEC202教室
第6回	2023年12月23日（土）	14:00～17:00	IISEC202教室
第7回	2024年2月28日（土）	18:00～19:00	IISEC202教室、オンライン



Raspberry Pi 班

メンバー

情セ大 M2 : 一葉 修平

情セ大 M1 : 松坂 惇平、卓 珮如、江 鴻浩、弓濱 まどか

中央大 M1 : 浅田 勇飛、今枝 俊輔

スマートホームとは

エンタメ

動画・音楽などのエンターテインメントを楽しむデバイス



スマートスピーカ

声で自宅の機器を操作できる機能を搭載したデバイス



Google アシスタントで
毎日がちょっと便利に。

スマートホームデバイス

家庭に存在する機器をネットワーク化することで一括管理，簡易的にコントロールできる仕組みを活用し快適なスマートな暮らしを構築する機器

アプライアンス

白物家電にスマートホームに適合する機能を取り入れたデバイス



ホームモニタリング

自宅のセキュリティを高めるために用いられるデバイス



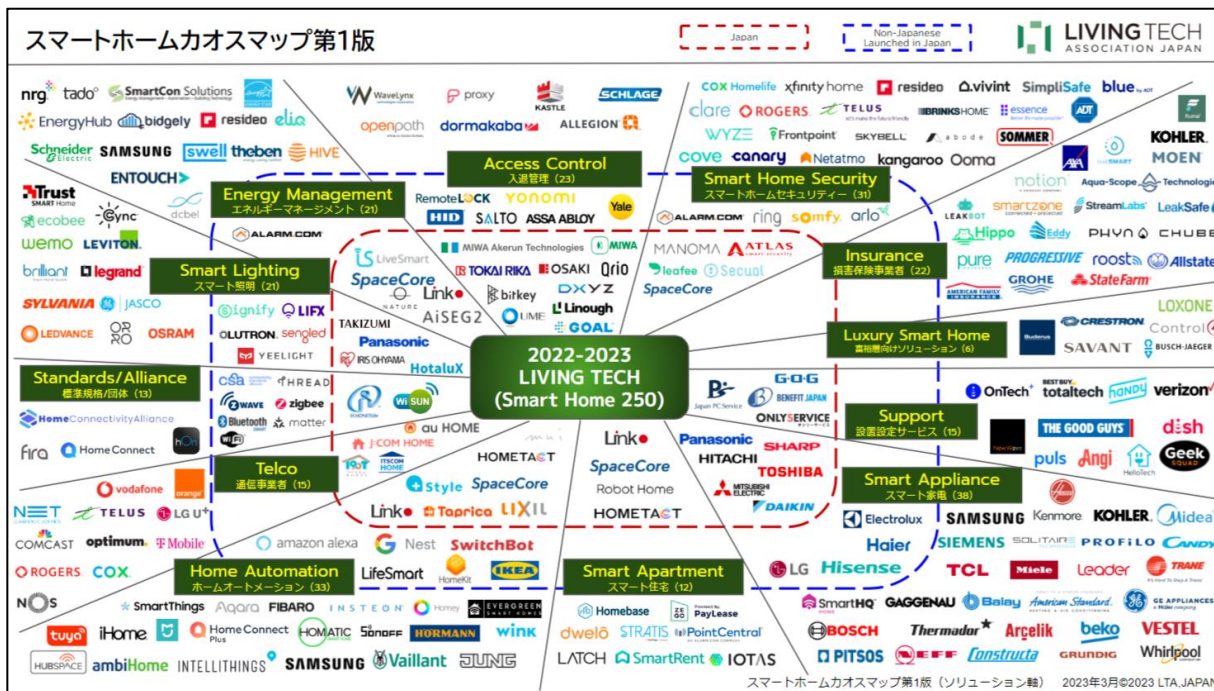
その他

証明のコントロールや自宅の室温管理など他に該当しないもの



参考：スマートホームカオスマップ

「ユーザの暮らし」を軸に、「スマートホーム」というソリューションを12ジャンルに分けたもの。(1.スマート照明2.エネルギー管理3.入退管理4.スマートホームセキュリティ5.損害保険事業者6.富裕層向けソリューション7.設置設定サービス8.スマート家電/ネットワーク家電9.スマート住宅10.ホームオートメーション11.通信12.標準規格/団体)



(出典) <https://www.ltajapan.com/industry-map/>

スマートホーム関連の事故・セキュリティ脆弱性

事件

2020年12月：Google Homeが使用不可の状態に

原因：Googleアカウントの認証を必要とするサービスに影響。データ容量を自動的に割り当てるシステムに問題発生

2020年12月：Qrio Lockがリモート開錠操作が不可に

原因：Qrio Lockサーバーにて一部通信障害。

2020年11月：Nature Remo(スマートリモコン) 不具合

原因：Nature社が利用しているクラウドサービスAWSに障害が発生したことによる影響でサービスが不安定に。

2020年4月：Sharp製スマート家電のアプリ操作不可に

原因：不織布マスク販売サイトと家電を操作するサービスを同じ認証基盤で使っていたこと。マスク販売サイトにアクセスが殺到したため

発見された脆弱性

2023年：スマートスピーカー不正アクセス

盗聴やフィッシングのための悪用。

2022年：IoTカメラの脆弱性

EZVIZのIoTカメラ複数モデルで脆弱性を発見。ビデオへの不正アクセスが可能であった。

2022年：スマートホーム製品へのアクセス制御

KalayaNetworkを使用するスマートホーム製品においてカメラ映像や屋内機器への不正アクセスの可能性を発見。

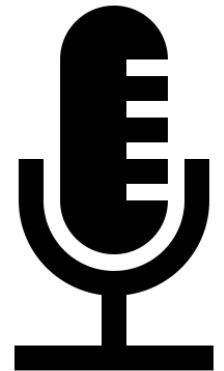
2021年：スキャナーにソフトウェア脆弱性

スマートホームスキャナー（windows版）に脆弱性が発見され不適切なアクセス制御が可能となる問題の発生。

利便性の向上が期待される一方でセキュリティの危険性が潜んでいる

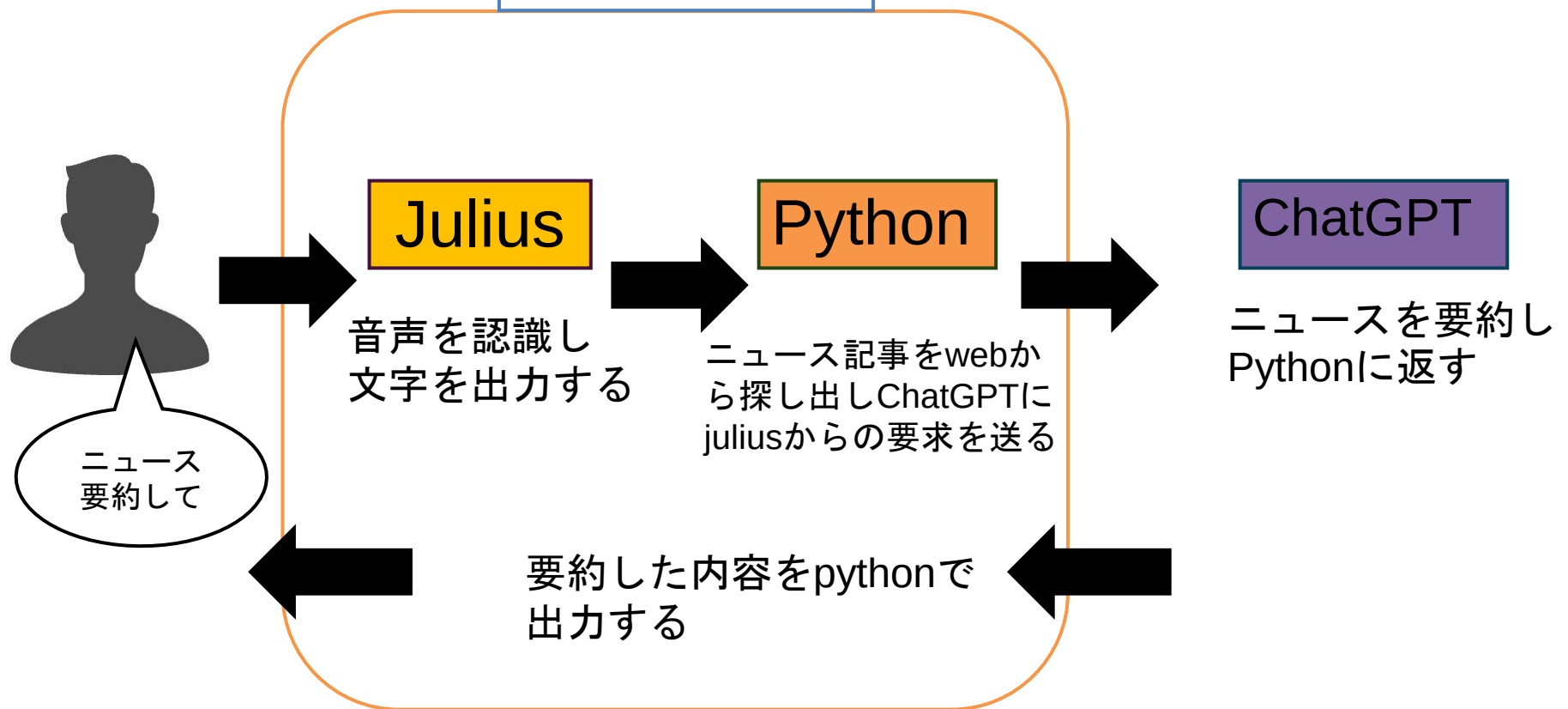
活動目標

- ChatGPTを用いたテキスト要約音声認識機能の作成
- 音声認識機能の脆弱性の検討(来年度予定)



システムフロー

ラズパイ



研究の機材

ラズパイ (Raspberry PI4 MODEL B)



Julius

- ・音声を認識し文字に起こすことができる。

Python

- ・Juliusで認識した文字を読み取る
- ・ニュース記事を持ってくる
- ・ChatGPTにニュース記事を渡し、音声認識でニュースを要約するように要求する

ChatGPT

- ・Pythonからの要求を行う

現在の進捗状況

Julius

- 音声認識を可能
- 音声聴き取りの正確性が低い

Python

- Juliusから文字を取り出し成功
- ニュース記事を持つてくることができた
- Juliusからの文字をChatGPTに送ることができていない。

ChatGPT

- ニュースを要約しPythonに返すことは成功



実際の音声認識

Shell

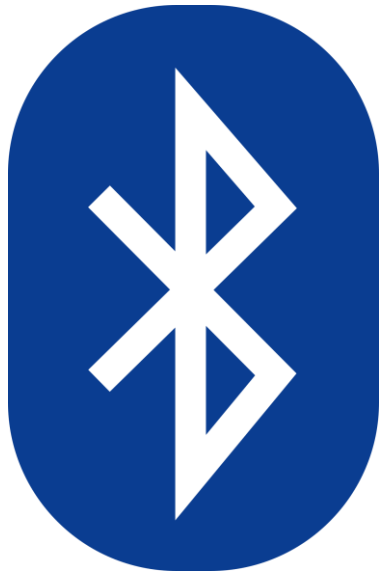
Python 3.7.3 (/u

>>>

```
0.1F word: ここ。
4.1B
0.1F word:
4.1B
0.1F word: なに
4.1B
0.1F word: なにも
4.1B
0.1F word: なにもなし
4.1B
0.1F word: なにもなし。
4.1B
0.1F word:
4.1B
0.1F word: ババ
4.1B
0.1F word: ババ。
4.1B
0.1F word:
4.1B
0.1F word: は
4.1B
0.1F word: は。
4.1B
0.1F word:
4.1B
0.1F word: 特に
4.1B
0.1F word: 特にぞ
4.1B
0.1F word: 特にぞ。
4.1B
0.1F word:
4.1B
0.1F word: 画像
4.1B
0.1F word: 画像なし
4.1B
0.1F word: 画像なし。
4.1B
```


- Juliusの音声認識内容をChatGPTに反映させる
- Juliusの音声認識精度の向上
- スマートスピーカーの脆弱性を考え、作成したもので実験する

来年度の活動



Bluetooth班

メンバー

情セ大M2：澤田 直哉、廣田 凧
情セ大 M1：岩崎 瞬、中村 裕太



背景：Bluetooth機器は2027年までに76億台出荷されると予想される

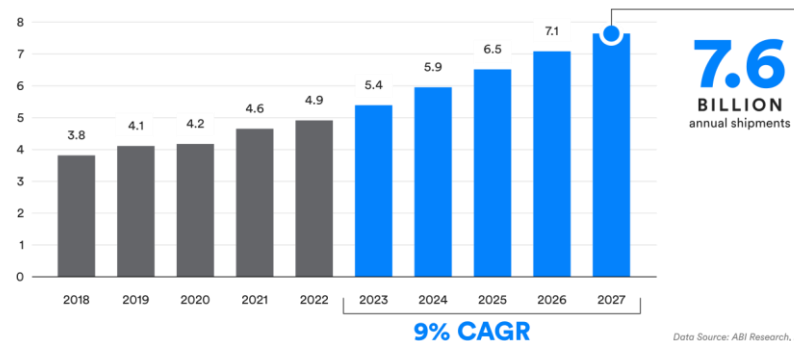


背景

- Bluetoothデバイスは様々な用途で活用され、その総出荷台数は増加し続けている。
- 2027年までに**年間76億台**のBluetooth対応デバイスが出荷され、今後5年間の年平均成長率は9%になるとの予測
- Eスポーツ界でもBluetooth機器の使用実績あり**
- Bluetooth 周辺機器の出荷台数は、2023年にはプラットフォームデバイスの出荷台数の2倍になる見込みです。

Total Annual Bluetooth® Device Shipments

NUMBERS IN BILLIONS



様々なBluetooth機器を実際に検証して、Bluetooth機器との関わり方を検討する。

出典・参考：2023年市場動向 | Bluetooth®テクノロジーサイト

<https://www.bluetooth.com/ja-jp/2023-market-update/>

「完全ワイヤレスでゲームってどうなの？」ソニー株式会社 | 広報

<https://note.com/sonycorporation/n/nd0066702926a>



調査対象

【Apple Air Pods pro 2】

→完全ワイヤレスイヤホンのシェアランキング
第1位はApple AirPods である。



【Sony WH-1000XM4】

→日本を代表するメーカーであるソニー
が発売した1つ前の世代のヘッドホン



【Nintendo プロコントローラー】→任天堂Switch
で利用できる純正コントローラー



【Wireless Controller Macro YSBR-BC002】

→連打コントローラーとして某電気屋に陳列されて
いる



3つの検証アプローチと具体的ツール

■ 脆弱性テスト

セキュリティの脆弱性を特定、評価、報告するプロセス

□ BLE Suite

BLEデバイスのスキャンと検出、サービスと特性探索、データの読み書きを通じての脆弱性テスト等が可能なBluetooth Low Energy (BLE) デバイスに焦点を当てた脆弱性テストツール

■ ジャミング(電波妨害)

無線通信において意図的に電波を妨害する行為

□ Ocramoi/bluetooth-jammer

Bluetoothデバイスを継続的にスキャンし、潜在的な接続を停止するためにpingを実行するBashスクリプト。

□ Yasher201/Bluetooth-DOS-Attack

ターゲット・デバイスに対してDoS攻撃を行うことで、それぞれのブルートゥース・セキュリティ・アーキテクチャを比較する

■ MITM(中間者攻撃)

通信している二者間に第三者が不正に介入し、通信を盗聴したり、データを改ざんしたりするサイバーセキュリティ攻撃

□ Bettercap

ネットワーク攻撃と監視のためのツール。BLEデバイスのスキャンと監視、デバイス間の通信の傍受と分析、MITM (Man-In-The-Middle) 攻撃を通じてBLE通信の操作が可能。



3つの検証アプローチと具体的ツール

■ 脆弱性テスト

セキュリティの脆弱性を特定、評価、報告するプロセス

□ BLE Suite

BLEデバイスのスキャンと検出、サービスと特性探索、データの読み書きを通じての脆弱性テスト等が可能なBluetooth Low Energy (BLE) デバイスに焦点を当てた脆弱性テストツール

■ ジャミング(電波妨害)

無線通信において意図的に電波を妨害する行為

選択した攻撃ツール

スキャンし、潜在的な接続を停止するために

□ Yasher201/Bluetooth-DOS-Attack

ターゲット・デバイスに対してDoS攻撃を行うことで、それぞれのブルートゥース・セキュリティ・アーキテクチャを比較する

■ MITM(中間者攻撃)

通信している二者間に第三者が不正に介入し、通信を盗聴したり、データを改ざんしたりするサイバーセキュリティ攻撃

□ Bettercap

ネットワーク攻撃と監視のためのツール。BLEデバイスのスキャンと監視、デバイス間の通信の傍受と分析、MITM (Man-In-The-Middle) 攻撃を通じてBLE通信の操作が可能。



方法(1/4) :
実験環境の構成は図のようになっている

スマートフォン等
例: iPhone SE 2nd



接続中

or

ペアリング試行中(例)

ゲームコントローラ等
WIRELESS
CONTROLLER
MACRO



Windows 11

PCホストOS: Windows 11

DoS攻撃

仮想化ソフト: VMware



ゲストOS: Kali Linux 2023.4



Python3

BLUETOOTH-DOS-
ATTACK-SCRIPT

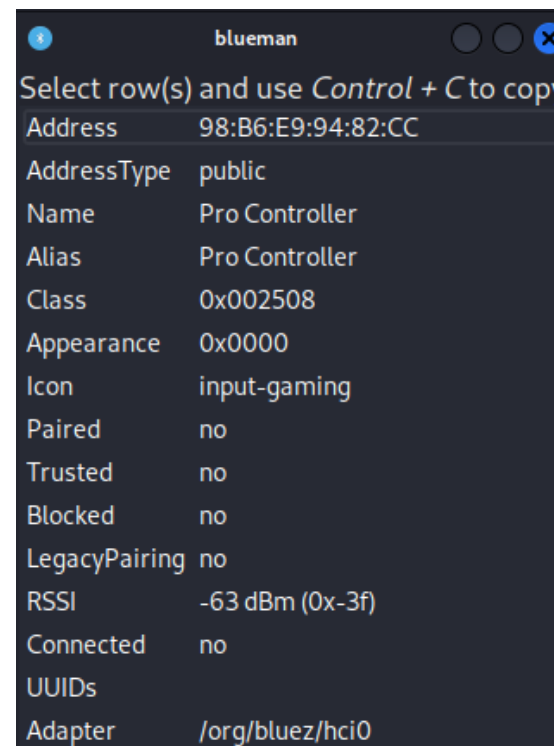
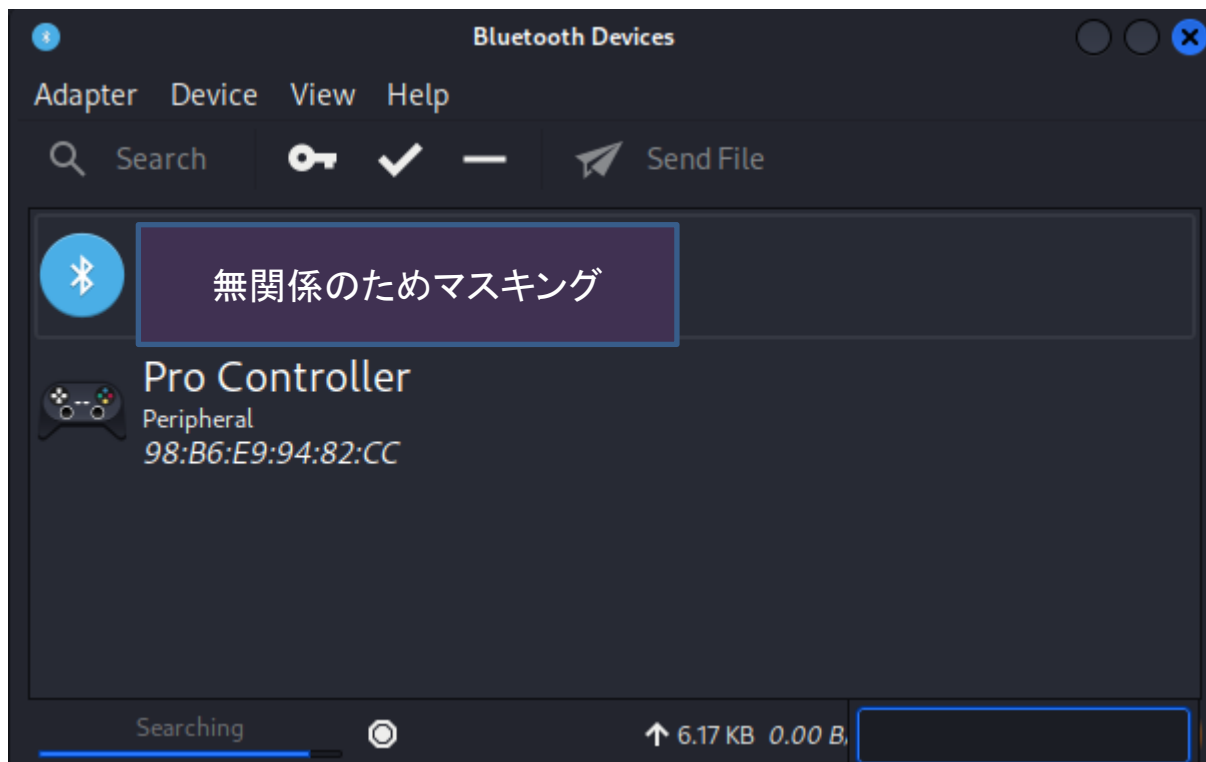


USB ドングル
例: Bluetooth(R)
USB アダプター
LBT-UAN05C2



方法(2/4) : デバイスの情報収集をする

- デバイスのMACアドレスを調べる
 - ゲームコントローラ 98:B6:E9:82:CC
 - スマートフォン 90:8C:43:E1:F5:D2





Bluetooth-DOS-Attack.pyを実行する

```
(bt)-(kali㉿kali)-[~/bt]
$ ls
bin Bluetooth-DOS-Attack.py bt3jammer2.sh
```

Bluetooth-DOS-Attack.pyという名前で保存

```
(bt)-(kali㉿kali)-[~/bt]
$ sudo python3 Bluetooth-DOS-Attack.py
```

管理者権限、Python3で実行

Bluetooth DOS Script

```
THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. YOU MAY USE T
SER. THE DEVELOPERS ASSUME NO LIABILITY AND ARE NOT RESPONSIBLE FOR ANY MISUS
Do you agree? (y/n) > y
```

警告にはyを入力

Bluetooth DOS Script

```
Scanning ...
|id | mac_addres | device_name|
|0 | 98:B6:E9:94:82:CC | ProController|
Target id or mac > 0
```

ターゲットのMACアドレスを入力

Bluetooth DOS Script

```
Scanning ...
|id | mac_addres | device_name|
|0 | 98:B6:E9:94:82:CC | ProController|
Target id or mac > 0
Packages size > 600
Threads count > 100
```

パケットサイズとスレッド数を入力する
今回は600、100を指定した



方法(3/4)

実際にプログラムを実行する①

ペアリング試行中にコントローラーへ攻撃をする

```
17 bytes from 98:B6:E9:94:82:CC id 21 time 395.70ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 395.82ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 395.59ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 393.27ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 395.32ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 393.37ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 393.85ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 393.48ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 394.87ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 396.62ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 394.77ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 395.72ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 396.01ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 396.10ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 394.58ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 395.99ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 392.37ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 392.98ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 396.54ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 394.02ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 395.35ms
17 bytes from 98:B6:E9:94:82:CC id 21 time 391.90ms
```

Kali Linuxの画面



iPhoneの画面

ペアリング試行中の機器に対して攻撃した結果

使用したUSB Dongle	LBT-UAN05C2				UB500	
使用した機器	任天堂 プロコント ローラ	連打コント ローラ YSBR- BC002	AirPods Pro（第2世 代）	Sony WF- 1000XM4	DUALSHO CK 4	DualSense
検証結果	ペアリング 失敗	ペアリング 失敗	ペアリング 失敗	ペアリング 失敗	ペアリング 失敗	ペアリング 失敗

Bluetooth機器に対するDoS攻撃でスマートフォンへのペアリングを妨害できるか検証した



ペアリング試行



ペアリング後の機器に対して攻撃した結果

使用した USB ドングル	LBT-UAN05C2				UB500	
使用した機器	任天堂 プロコント ローラ	連打コント ローラ YSBR- BC002	AirPods Pro（第2世 代）	Sony WF- 1000XM4	DUALSHO CK 4	DualSense
検証結果	問題なく使 用可能	問題なく 使用可能	20秒程度攻 撃継続でス マホとの接 続が切断	問題なく 使用可能	問題なく 使用可能	問題なく 使用可能

Bluetooth機器に対するDoS攻撃でスマートフォンとの通信を妨害できるか検証した



接続中



- ペ어링試行中に攻撃を行うと、新規接続が不可能になる事例があった。
- AirPodsPro2nd にDoS攻撃を行うと、iPhoneとの接続が切断された。つまり、ターゲットとなるAirPodsPro2ndのMACアドレスを知っていれば、音楽の再生を妨げられる。

目標であるBluetoothへの攻撃については
特定条件下でのDoS攻撃に成功した。

活動予定（今後のロードマップ）

セキュリティ脅威の検証

スマートホーム

パーソナルデバイス

スマートホーム？自動運転？

ウェアラブルデバイス？5G？

2023

2024

脅威シナリオ検証

来年度のメンバーにて討議し
時代に応じた有意義な
シナリオ、テーマを選定する

