

2022年度 ISSスクエアシンポジウム 研究成果報告

2022/03/03
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16名、指導教授1名）

RL :情セ大 大久保 隆夫

幹事

中央大 M2 : 塚本 高大

情セ大 M1 : 一葉 修平

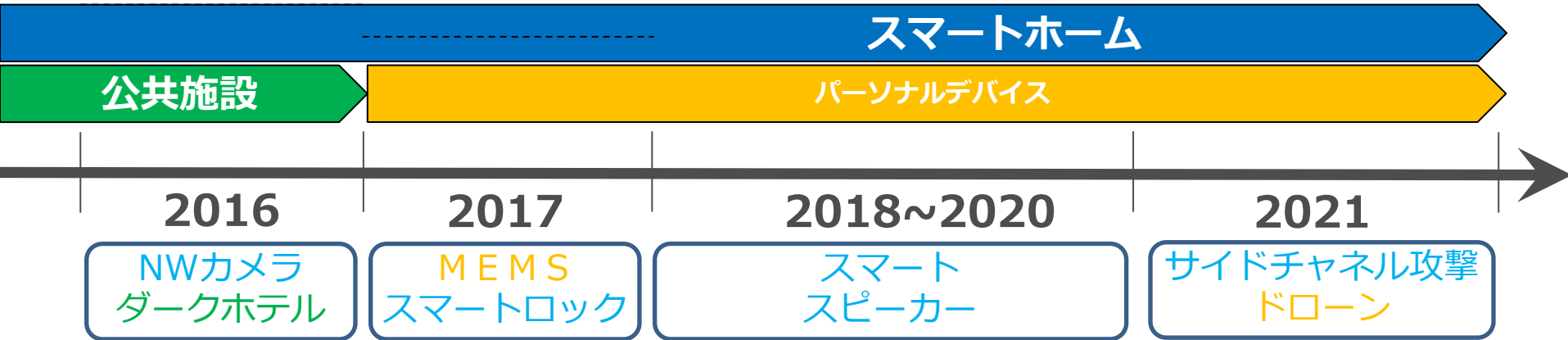
メンバー

情セ大 M2 : 上野 瑞己、梅田 真子、大矢 政基、末吉 璃子、仙田 眞之、
長谷川勇希、林 泊舟、森田 亰、米田 智紀

中央大 M2 : 東 拓矢

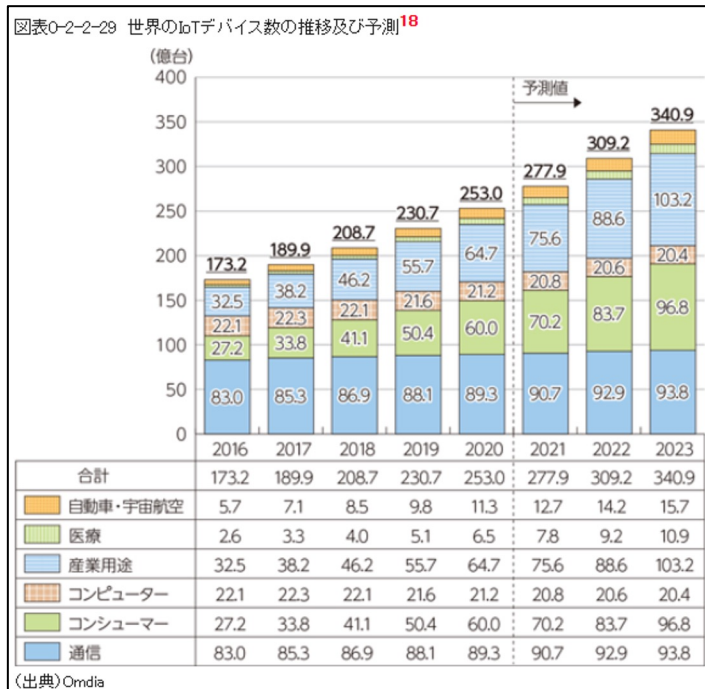
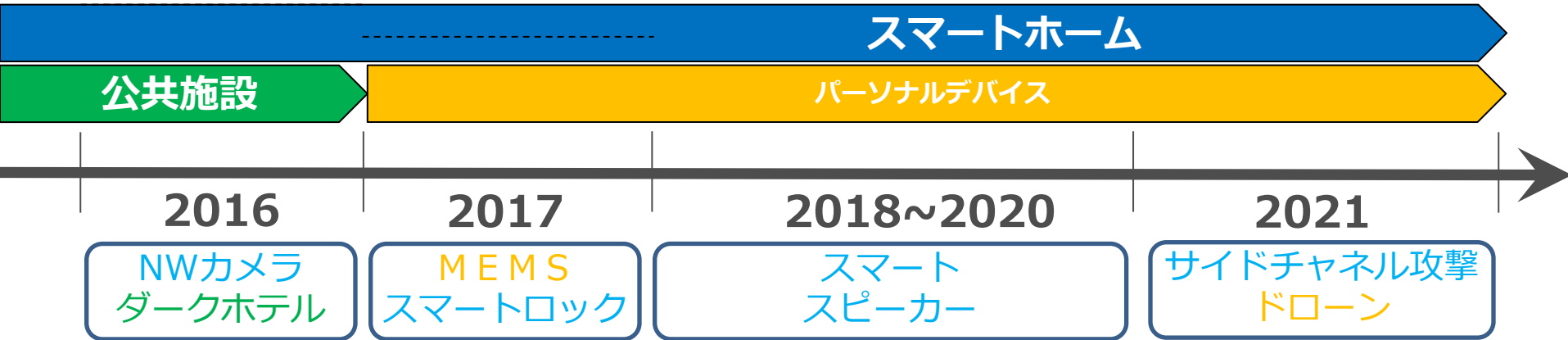
情セ大 M1 : 阿部 実洋、堺 啓介、澤田 直哉、松隈 孝志

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）



- ・ IoTデバイスは増加傾向
- ・ 今後も増加する予測
- ・ 家のルータ（WiFi）への接続機器も増加
- ・ デバイスは生活やプライバシーに密着

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

2023

脅威シナリオ検証（前年度の「スマートホーム」を拡大して生活に着目）

ルータ班

インターネットに接続される入口のセキュリティ検証

→現在購入可能なルータのセキュリティ実装状態の**認知**

→アタックツリーからの重点防御ポイントの**考察**

スマートタグ班

生活とプライバシーに直結するデバイスのセキュリティ調査

→便利かつ安全に使うための**HowTo**

→犯罪などの被害を防止、抑止するための**HowTo**





ルータ班

メンバー

情セ大M2：上野 瑞己、大矢 政基、末吉 璃子
長谷川 勇希、米田 智紀



背景



GIGAスクール構想の進展による学校と家庭の学習における
メディア利用の変化

ニュース

エレコムのルーターなどで脆弱性。サポート終了のため使用中
止を勧告



「ニンテンドーWi-Fi USBコネクタ」および
「ニンテンドーWi-Fiネットワークアダプタ」使用中止のお願い



様々な家庭用ルータを実際に検証して、実践的なルータの脆弱性と
アタックツリーを検討する
(家庭でのルータのセキュリティを守るための知見を得られるか?)



調査対象

【エレコム WRH-300KS】

→比較的安価で手に入るルータ



【Nintendo ニンテンドーWi-Fiアダプタ】

→古いルータだが、広く家庭に普及したルータ



【NEC AG2600HS2】

→比較的新しく、高価な日本製メーカーのルータ



【TP-Lin TL-WR802N】

→新興メーカーの売れ筋ルータ



価格帯、販売年度を考慮し広く調査・検証



調査・検証項目



【脆弱性調査】

- ・ 機器脆弱性調査
- ・ アップデート調査



【実機調査】

- ・ ポートスキャン
- ・ 脆弱性スキャン
- ・ パケットキャプチャ
- ・ Wi-Fiハッキング



【まとめ】

- ・ 調査結果まとめ
- ・ アタックツリー想定



脆弱性調査



調査結果

- ・ 管理画面に脆弱性が集中
- ・ 購入時点で、**全ルータが脆弱性対象**

製品名	発売日	メーカー取り扱い	脆弱性情報
エレコム WRH-300KS	2016年	在庫限り(EOL)	JVNVU#94260088 (OSコマンドインジェクション)
Nintendo ニンテンドーWi-Fiアダプタ	2008年	販売終了(EOL)	CVE-2022-36381 CVE-2022-36293 (OSコマンドインジェクション、バッファオーバーフロー)
NEC AG2600HS2	2020年	販売中	CVE-2020-5533 CVE-2020-5534 (OSコマンドインジェクション、XSS)
TP-Link TL-WR802N	2016年	販売中	JVNVU#94883311 (OSコマンドインジェクション)





ポートスキャン、脆弱性スキャン

・特徴的なスキャン結果

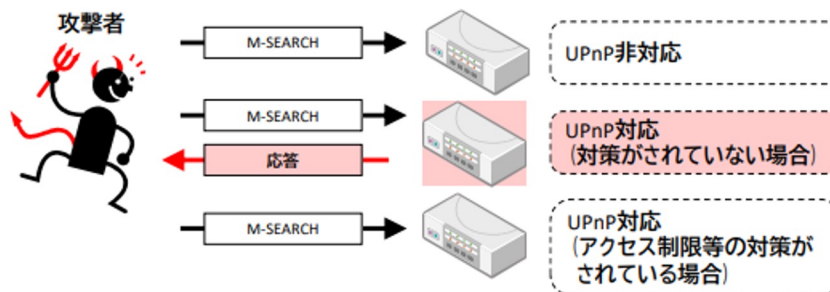
PORT	STATE	SERVICE
53/tcp	open	domain
80/tcp	open	http
52869/tcp	open	unknown

・特徴的なスキャン結果

PORT	STATE	SERVICE
53/tcp	open	domain
80/tcp	open	http
1900/tcp	open	unknown

```
kali01@kali: ~  
ファイル 操作 編集 表示 ヘルプ  
$ telnet 192.168.2.1 52869  
Trying 192.168.2.1...  
Connected to 192.168.2.1.  
Escape character is '^]'.  
pwd  
  
HTTP/1.1 501 Not Implemented  
Connection: close  
Content-type: text/html  
  
<HTML><HEAD><TITLE>501 Not Implemented</TITLE></HEAD><BODY><H1>Not  
Implemented</H1>The HTTP Method is not implemented by this server.<  
/BODY></HTML>  
Connection closed by foreign host.  
  
$
```

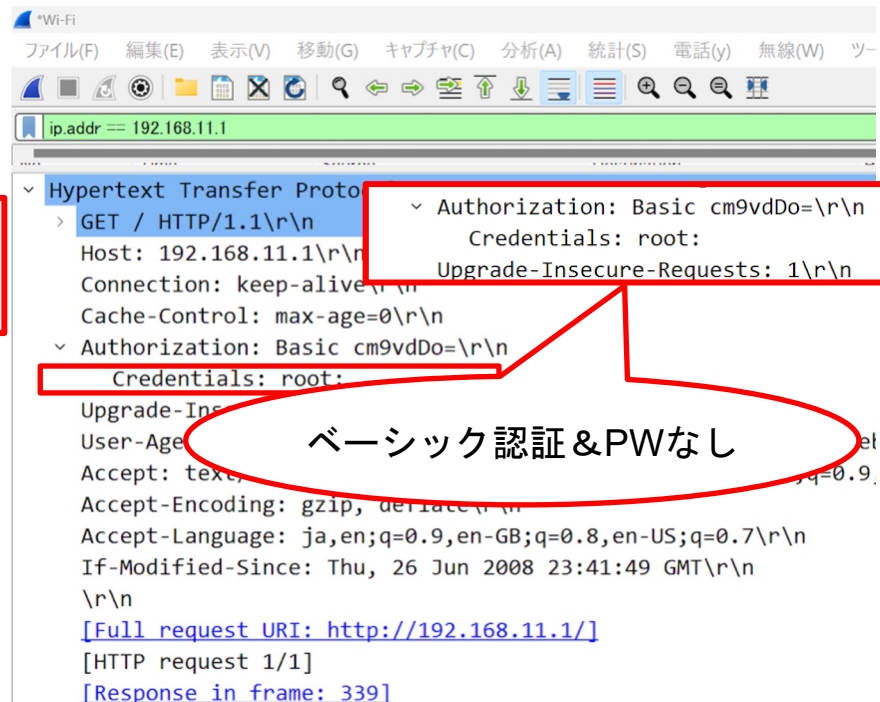
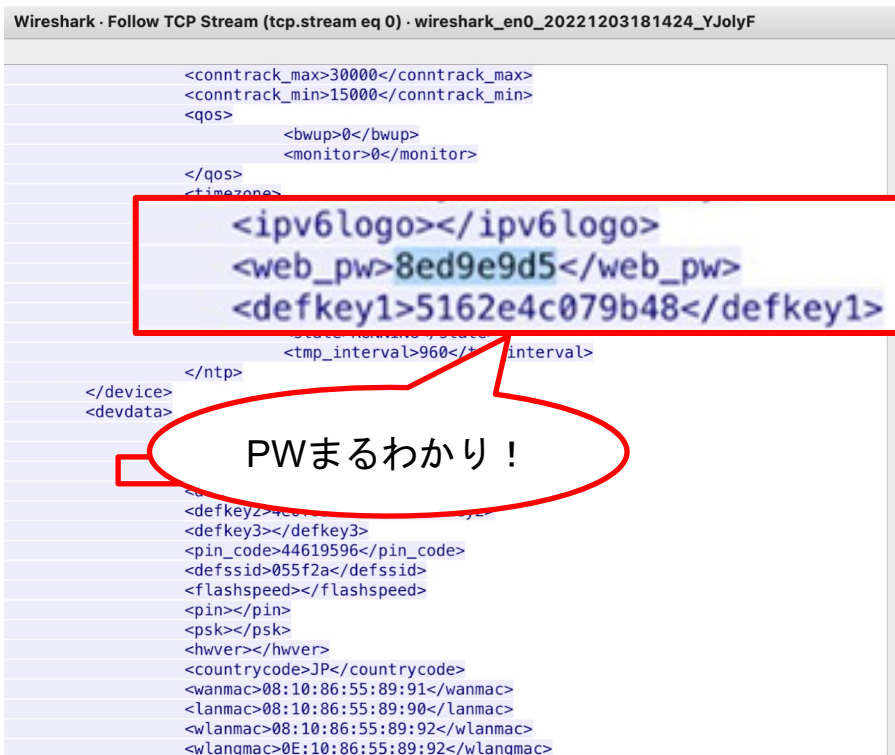
脆弱性が存在するルータを標的とした宛先ポート
52869/TCPに対するアクセス及び日本国内からの
Telnetによる探索を実施するアクセスの観測等につ
いて





管理画面へのポートスキャン

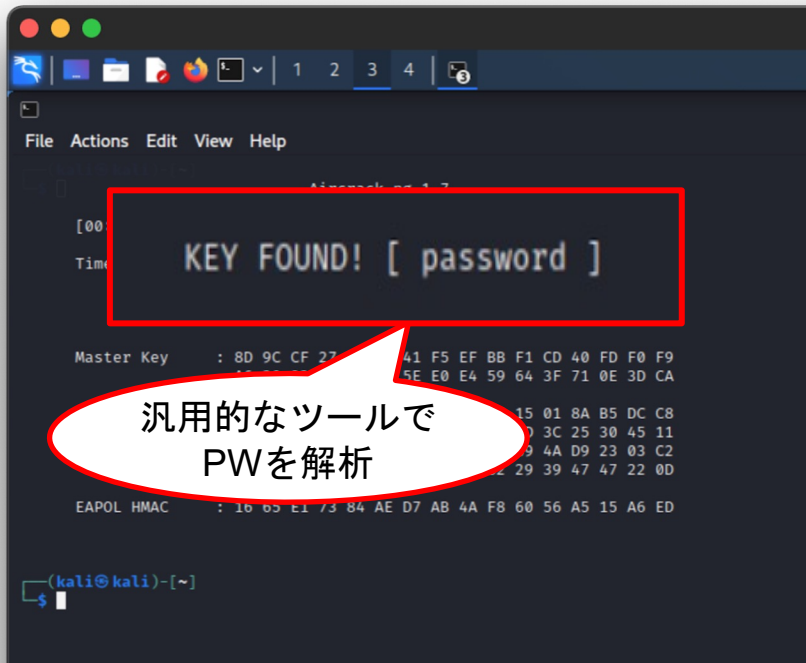
- ・基本的にhttp通信で行われているので。。。





Wi-Fiクラッキング

脆弱なPWであれば容易に解析可能





調査結果のまとめ

初期状態では
管理ページに
脆弱性が残る



PWによっては
Wi-Fiクラック
可能



WiFiルータに
攻撃者の
好きな設定を
入れられる

とはいってもルータの管理画面に“利用者”が入らないと管理画面にログインできない

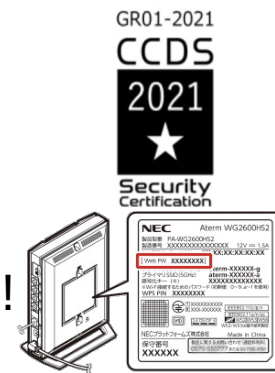




全体のまとめ

- ・ルータに報告される脆弱性は主に管理者画面
→管理者画面に入られると特にまずい
(HTTPSで暗号化してほしいけど、ブラウザの警告画面で難しいよね。。。)
- ・Wi-Fiの脆弱なPWはクラック可能
→強固なPWが望ましい
- ・利用者観点では不要なポートが開放されているものもある
→過去攻撃者の穴となり利用されていた
(脆弱性として利用されれば、利用者の管理者画面へのログインを誘発可能)

- ・市販の家庭用ルータの特性を**認知**
- ・ルータ製品としても、**CCDS Level1程度の要件は満たす必要がある**のではないかと
- ・消費者としての対策として、**管理者画面への認証が一番危険**
不必要にはアクセスせず、PWも厳重で利用し漏洩を防ぐべき！





スマートタグ班



メンバー

情セ大M2：林 泊舟

中央大M2：塚本 高大

情セ大M1：阿部 実洋、一葉 修平、堺 啓介、
澤田 直哉、松隈 孝志

背景

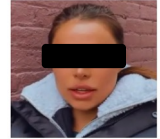
勝手にコートに入れられ…「AirTag」による犯罪被害に女性が注意喚起



2022/12/22(木) 17:03 配信 32



COSMOPOLITAN



Instagram / @si_swimsuit

アップル「エアタグ」を"無音"に改造 浮気調査や元交際相手への
使用例も… 商標法違反疑い男逮捕 千葉県警

2022/12/1(木) 11:53 配信 14



千葉日報



容疑者の関係先から押収するなどしたAirTag=30日、千葉南署



女性の車に「AirTag」取り付けストーカーか 会社員を書類送検

2022年12月1日 20時47分



実機を実際に検証して、現実的なスマートタグのセキュリティに関するHowToを考える。

(ストーカー規制法などの法整備も進んでいるが、被害に遭う前にセキュリティを高めることはできないか?)

出展：

<https://news.yahoo.co.jp/articles/4f3a59a4e46de7643e299b1ef98b97f3448ac996>

<https://news.yahoo.co.jp/articles/e5bdcd02d6532a66797ddaedca15f2a5ee9c2f5c>

<https://www3.nhk.or.jp/news/html/20221201/k10013910341000.html>



調査・検証項目

#	Category	Investigation	proposer	Result	data	InCharge
1	調査（ドキュメント）	電池はどのくらい持つ？	堺	そもそも公式ドキュメントはないっぽい		堺
2	調査（ドキュメント）/実験	ペアリング機とどのくらいの時間離れているとアラームが鳴る？	堺	8-24hのうちランダム？ →実験結果？平均は？→仕様上なので実験します！		阿部
3	実験	ペアリング機とどのくらいの時間離れているとアラームが鳴る？	堺		写真or地図情報	澤田
4	実験	方向が分かるのは、上下（1階2階とか）も分かる？	堺	iphone上で矢印がでるからどうにかなるけど、距離的に階が別だときつ	キャプチャ	堺
5	実験	sysdiagnodeのログに何が出る？	堺	めばしい情報を確認できず	sysdiagnode	堺
6	実験	初期化の方法（紐づけ機器の変更）	堺	https://support.apple.com/ja-jp/HT212251	doc	堺
7	実験	位置情報の履歴は出る？	堺	sysdiagnodeを確認→めばしい情報なし icloudにログイン→めばしい情報なし	sysdiagnode icloud画面キャプチャ	堺
8	実験	位置情報の精度はどの程度か。（どこのお店でランチしているか分かる？） ※夜のお店（仮定）に忘れたら、彼女にバレるかという体裁だと 発表が面白いかも	堺	いいね	画面キャプチャ 地図情報	堺・一葉
9	実験	家族共有でも見えるか？	堺	見れないっぽい（あくまで持ち物だから？）	icloudログイン状況	堺
10	実験	ストーリー（仮定）に荷物に紛れ込まれたら気付くか？ （iphoneを持っている場合、荷物に他人のairtagがまぎれていたらアラーム等が鳴る？）	堺	同じ研究室で何時間いても鳴らない→接続されたiphoneが近くにあれば鳴らない。		堺・一葉
11	実験	airtagかくれんぼ（逃げる人：androidユーザ、追う人：だれか、時間：？？、場所：？？）	堺	-	写真とか 移動履歴データ	ボツ
12	実験	Tracker Detectによる検出実験	堺	検出できない。。。。		堺
13	実験	AirGuardによる検出実験	堺	検出できない。。。。	-	堺
14	調査（ドキュメント）/実験	AirTagのMacアドレス？固有番号？はどうやって調べる？	堺			一葉
15	実験	Tileってどうよ？Prox4（堺、一葉で検証）	堺	-	-	堺・一葉
16	調査（ドキュメント）/実験	AirTagの音量は上げられる？	堺	あげられない。 14.5以降のバージョンで少し大きくなったらしい		堺
17	実験	Bluetoothのペアリングを解析してみる	堺	-	-	ボツ
18	実験	AirTagの音を切ることはできる？（物理的にスピーカーを切断）	阿部	聞けるしかない・・・		阿部
19	実験	タグを検知する方法は？（Tile）	堺	公式にある！	画像、実験結果	堺・一葉
20	実験	Androidユーザがタグを検知する方法は？（AirTag）	松隈	Appleの公式アプリTrackerDetectを利用する。同期しているデバイスが →検証ならびに資料作成、ありがとうございました！ 堺の（やっすい）中華タブレットだと何故かうまく検出できませんで ちゃんとAndroidを使っている方に実験して頂くのは大事ですね！	Slack参照	松隈
21	調査（ドキュメント）/実験	AirTagのファームウェア変更・抽出（ハッキングできる？）	林	https://insomniasec.com/blog/airtag-hacking		林
22	調査（ドキュメント）/実験	Androidユーザが、（例えばこっそり入れられた）AirTagを検知する方法はあるか？	松隈	同#20		松隈
23	調査（ドキュメント）/実験	Airtagの既存の脆弱性	林	https://medium.com/@bobbyrsec/zero-day-hijacking-icloud-credentials-v		林
24	調査（ドキュメント）/実験	少しだっぴろいところで、iphoneを持っている人と一緒にない場合にどのくらいの精度が出るか （実際にものをなくした。盗まれた時のイメージ） （子供x3にくっつけて実験してみる？）	堺	誰が使っていない（実験が終わった）AirTagを分けてください。。。2個希望		堺

AirTagを主眼においてスマートタグ （忘れ物防止タグ）について調査・検証



- ・ 通常利用する観点
 - AirTagの探し方
 - AirTagの精度（街中/広い空間）
 - AirTagの初期化・譲渡
- ・ 犯罪捜査の観点
 - AirTagの固有識別番号
- ・ 犯罪の防止、被害軽減の観点
 - AirTagの見つけ方（iPhone/Android）
 - AirTagを見つけた時の対応
- ・ AirTag以外のスマートタグに関する調査

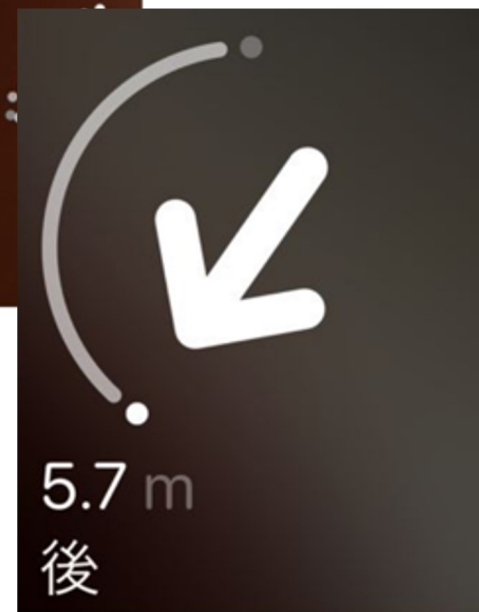


AirTagの探し方

- ・ iPhoneかiPadが必須
- 探す > 持ち物を探す (地図) > 探す (近くなったら)



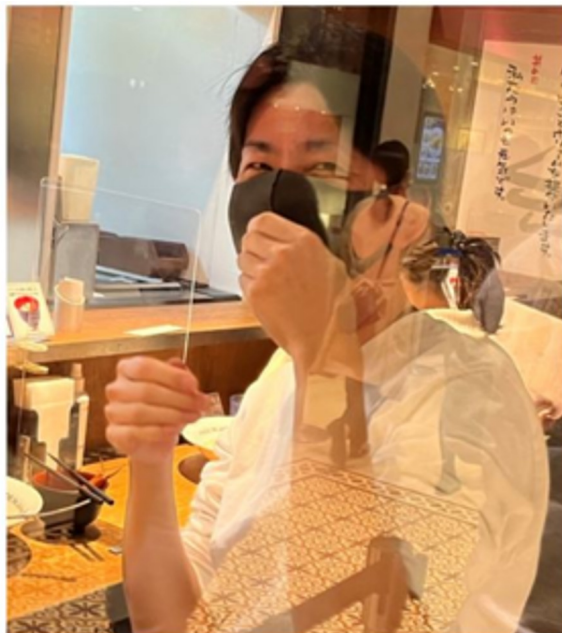
信号を探しています...
別の場所に移動してみてください。





AirTagの精度（街中）

- ・建物（鉄筋）の違う階だと検出不可
- ・同じ階なら、方向も分かるので、探し当てることが可能
- ・音も鳴らせるけど、ガヤガヤしている中だと分からない





AirTagの精度（街中）

- ・ 移動先のお店が特定可能（笑）





AirTagの精度（広い空間）

- iPhoneが本当に近くないと（人が密集していないと）
正確な場所とはならず、検出時間に応じて
搜索範囲を広げる必要がある



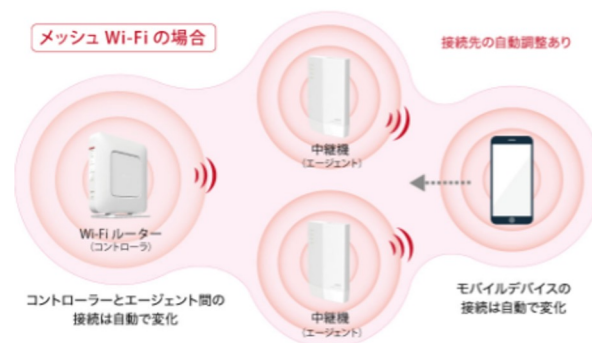
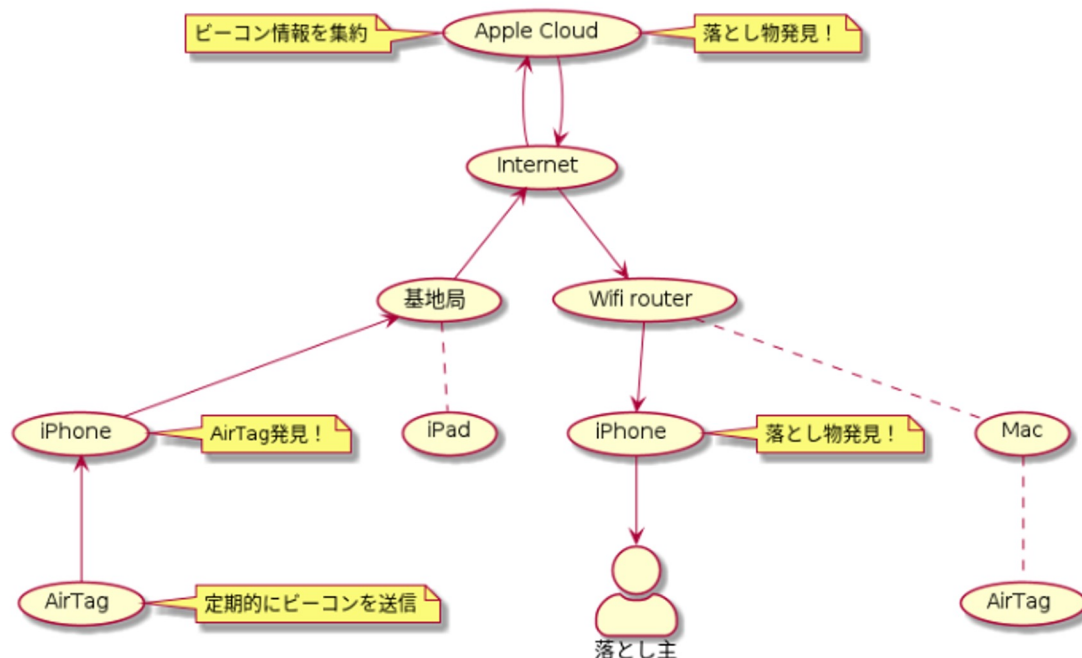
本当の現在地



- ・ 近くのAppleDeviceを頼りに位置情報を更新



Connect to the Find My network



参考：メッシュWiFiの模式図

画像出展：

<https://developer.apple.com/find-my/>

<https://umu-mu.hatenablog.com/entry/2021/04/25/193855>

<https://www.buffalo.jp/topics/select/detail/meshwifi.html>



AirTagの初期化・譲渡

- ・ 自分で初期化
探す>AirTagを選択>持ち物を削除
- ・ 強制初期化
電池を外して5回付けなおしでリセット





AirTagの固有番号



「探す」アプリ

同一のシリアルナンバー



電池を外した状態
(かなり文字が小さく、撮影は不可能)



AirTagの見つけ方 (iPhone/Android)

- iPhoneを持っている場合
→数時間で勝手に検知
- Androidを持っている場合 (iPhoneが無い場合)
→Tracker Detect (Apple公式アプリ)
で検出した10分後からサウンド再生で搜索可

スキャン中...



不明なAirTag

最初に確認されたのはたった今です



不明なAirTag

最初に確認されたのはたった今です



不明なAirTag

最初に確認されたのはたった今です

3個の持ち物トラッカーが見つかりました

不明なAirTag

最初に確認されたのは7分前です



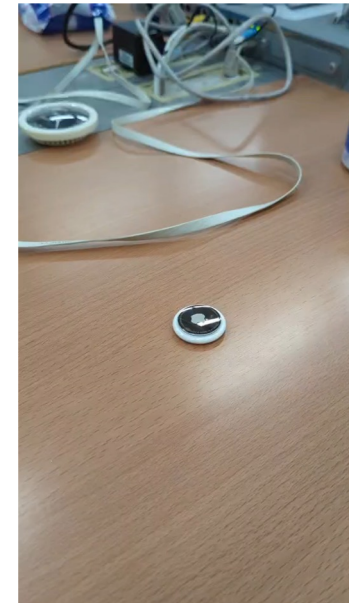
サウンドを再生

あと3分

このAirTagが近くにあると10分経つと、サウンドを再生することができます。

この持ち物トラッカーについての詳しい情報

無効にする手順





AirTagを見つけた時の対応

- ・電池を外せば無効化される

※最後に外した場所が、悪意を持った人には表示され続ける

→自宅で外すと・・・orz

→ダミーの場所か、警察署などで外す方が無難

この持ち物トラッカーを無効にする



バッテリーを取り外すことで、“探す”ネットワークほかの人がこのAirTagを探せないようにすることができます。

AirTagの裏蓋を押し込み、反時計回りに回します。裏蓋を外して、バッテリーを取り外しま





AirTag以外のスマートタグ

- 売れ筋
AirTag, Tile, MAMORIO
- AirTagとの大雑把な違い
 - androidでもiphoneでも
 - 1000～1500円くらい安い
 - 電池交換はできたりできなかったり
 - 最後にBT接続した場所を記録
 - 駅には忘れ物用AP（繋がったら通知）
 - 検出（ストーカー対策）は手動



AirTag以外のスマートタグ

- Tileの特徴
 - 登録用アプリに検出機能あり（ストーカー対策）
 - 有料（月額）だと移動履歴が見れる。
 - 利用者間ネットで検出も。
 - 地図以外での検索は音で行う（マナーでも鳴る）
 - タグからもスマホを探せる！（一番便利かも）
 - 置き忘れ通知が有料オプション（月額）。。。。
- MAMORIOの特徴
 - 検出は新しい機器登録時に気付く。。。かも
 - 地図以外での検索はカメラのARで行う
 - 利用者間ネットで検出可
 - 保険がある（年額1100円、検索支援＋保証最大3万）



まとめと目標に対する成果

- ・ 通常使用（忘れ物防止）という意味では他のメーカーのものでも十分（個人的所感）
- ・ 場所を探したいなら、シェアが多いと感じるAirTag
- ・ 海外の飛行機に乗せる預け荷物につけるならAirTag
（要航空会社の規約確認。なお、私は新婚旅行で大変な目に遭いました。笑）
- ・ スマホをよく無くす人はTil
- ・ ストーカーが気になる場合は、メジャーなメーカーは数のタグ検出を試行する
- ・ 電池を抜いたり、無効化する場所に注意
（何故か、どのブログにも書いていない）

**目標としていた、
現実に則したHowToの知見を得た**





まとめ（補足）

- ・ 迷子タグ的に使うには懸念が多々
 - 小さい子供服は、ベルトタグがそもそもない
 - バッグは忘れたり、そこら辺に投げ捨てられる
 - ベルトタグがある位のサイズに成長すると動きが激しくて、タグが無くなる
 - 誘拐の場合は、
 - ・ 犯人のiphoneが近いと通知される
 - ・ 郊外や鉄筋などの室内だと場所がでない（ずれる）等の点に注意
- ・ あくまで、忘れ物防止タグということを念頭に



ウェアラブルデバイス？ 5G？

2023