1ZG-06

BLE 端末における ID 追跡可能性に関する検討

小山　祐佳†　　伊藤　清里菜†　　長尾　和彦†

弓削商船高等専門学校†

1.　はじめに

ICT 端末普及に伴い，無線通信を用いる多くの端末が増加している．総務省によると，2020 年には IoT 端末数が約 300 億個となる見通しである[1]．図 1 に IoT 端末数の予測を示す．

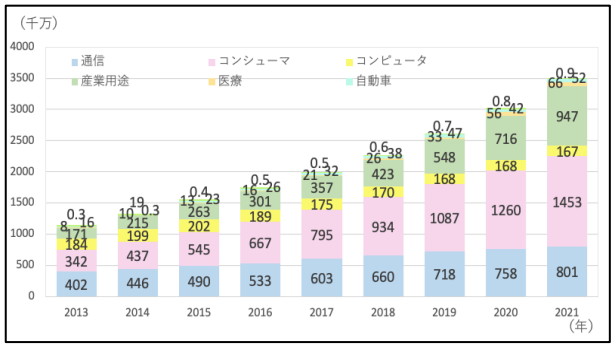

図 1. IoT 端末数の予測

特に BLE（Bluetooth Low Energy）対応端末は，SmartWatch，タグ，マウスなど様々なものがある．BLE タグは，位置情報と連携し，忘れ物防止システムとして利用されている．BLE 端末には MAC アドレスや UUID などの一意に識別するための識別子が存在する．BLE4.0 では通信時のプライバシーを保護するため，これらの値が時間や取得する機器ごとに変化するように設定されており，個々の識別ができないとされている．しかし，BLE 端末の調査は十分にされておらず，実装が正しく行われているのか確認されていない．

本研究では，複数の BLE 端末を対象として，通信時の個々の識別値の特定が可能かどうか調査を行う．また，通信条件とプライバシー保護のための対策について考察する．

2.　BLE4.0 の通信プロトコル

BLE 通信において，接続要求，通信の制御を行う側をセントラル（スマートフォン），セントラルからの要求に応える側をペリフェラル（BLE 端末）と呼ぶ．ペリフェラルは，存在を認識してもらうため電波を発し続けている（アドバタイジング）．セントラルは，Scan を行い周囲の BLE 端末を認識する．特定の BLE 端末に Connect 要求を行い，応答が返ってくると接続状態となりデータが送られてくる．

接続状態からセントラルとペリフェラルをペアリングするには，ペリフェラルからペアリング要求を行う．応答が返ってくると，PassKey を入力する．その際，STK（一時鍵）を生成し，LTK（暗号鍵）を交換することでペアリングが完了する．

本研究は，BLE 端末を用いた汎用的なシステム開発を目的としているため，ペアリングは行わずに取得できる値を調査する．

3.　iPhone を用いた ID 取得実験

3.1.　実験概要

今回の実験では，BLE 端末に対して Scan，Connect を行い，時間や取得する端末によって変化しない ID を得ることが可能かどうか調査した．実験に使用する端末（セントラル）は iPhoneXR:iOS12.2 と iPhone7:iOS12.2 である．ペリフェラルには BLE タグ 2 種，SmartWatch1 種．それぞれ 2 台用意し，比較を行なった．今回は，BLE 端末の情報を取得できるプログラムを開発した．開発環境は，Xcode10.2.1，Swift5.0.1 を使用した．実験期間は，2019/9/25～10/14 である．

3.2.　実験結果

MAC アドレスは，iPhone 側の API により，取得禁止となっている．UUID に関しても取得する端末ごとに変化することが確認された．しかし，Scan によって取得できる製品名（NA）と ManufactureData（MA），Connect によって取得できる Charactaristics の Value（CV）を組み合わせることにより端末が識別できると判明した．図 2 に実験結果を示す．

Research on traceability of ID acquisition in BLE devices
†Yuka Koyama,Serina Ito,Kazuhiko Nagao,National Institute of Technology, Yuge College

2019/9/25									
	端末	NA	MA	CV		端末	NA	MA	CV
XR	端末A1	MYNT	0000cc78ab16f683	複数あり	7	端末A1	MYNT	0000cc78ab16f683	複数あり
	端末A2	MYNT	0000247189e899a1	複数あり		端末A2	MYNT	0000247189e899a1	複数あり
	端末B1	Tile	なし	0xc29f0aa4f6d14fc2		端末B1	Tile	なし	0xc29f0aa4f6d14fc2
	端末B2	Tile	なし	0x046e975aecc44c18		端末B2	Tile	なし	0x046e975aecc44c18
	Watch1	Y5-F272	0x661882bff272cdab0e00	0x661882bff272		Watch1	Y5-F272	0x661882bff272cdab1000	0x661882bff272
	Watch2	Y5-4B99	000095119a624b99cdab2000	0x95119a624b99		Watch2	Y5-4B99	000095119a624b99cdabf00	0x95119a624b99

2019/10/14									
	端末	NA	MA	CV		端末	NA	MA	CV
XR	端末A1	MYNT	0000cc78ab16f683	複数あり	7	端末A1	MYNT	0000cc78ab16f683	複数あり
	端末A2	MYNT	0000247189e899a1	複数あり		端末A2	MYNT	0000247189e899a1	複数あり
	端末B1	Tile	なし	0xc29f0aa4f6d14fc2		端末B1	Tile	なし	0xc29f0aa4f6d14fc2
	端末B2	Tile	なし	0x046e975aecc44c18		端末B2	Tile	なし	0x046e975aecc44c18
	Watch1	Y5-F272	0x661882bff272cdab1100	0x661882bff272		Watch1	Y5-F272	0x661882bff272cdab0100	0x661882bff272
	Watch2	Y5-4B99	000095119a624b99cdab0d00	0x95119a624b99		Watch2	Y5-4B99	000095119a624b99cdab0f00	0x95119a624b99

図 2. 実験結果

4. RaspberryPi を用いた MAC アドレスの取得

4.1. 実験概要

iPhone の API 制限により，MAC アドレスを取得することができなかった．そのため，RaspberryPi を使用して，各 BLE 端末の MAC アドレスを取得する実験を行なった．実験に使用する端末（セントラル）は RaspberrypiZeroW である．ペリフェラルには BLE タグを使用した．その際，3. iPhone を用いた ID 取得実験の端末 B1，B2 を使用した．実験期間は，12/21 と 12/23 の 2 日間である．

4.2. 実験結果

実験に使用した BLE タグは MAC アドレスのタイプは random になっているが，アドレスは変化していないことが確認された．MAC アドレス取得の実験結果を図 3 に示す．

2019/12/21		
端末 A1	Name	Tile
	アドレスタイプ	random
	MAC アドレス	e1:9c:17:06:e1:2f
端末 A2	Name	Tile
	アドレスタイプ	random
	MAC アドレス	d7:11:49:00:c1:71

2019/12/23		
端末 A1	Name	Tile
	アドレスタイプ	random
	MAC アドレス	e1:9c:17:06:e1:2f
端末 A2	Name	Tile
	アドレスタイプ	random
	MAC アドレス	d7:11:49:00:c1:71

図 3. MAC アドレス取得の実験結果

5. まとめ

本研究により，一定の条件下で識別値の特定が可能であることが確認された．また iPhone では，確認できなかった MAC アドレスも RaspberryPi での実験によりアドレスが時間ごとに変化しないことが判明した．これは，BLE 端末の実装上の脆弱性とあると言える．判明した識別値の対策として CV の値を定期的に変更するように設定する，特定のアプリケーションしか接続できないようするなどが挙げられる．BLE 端末を製造する側でもペアリング以前のセキュリティを強化すべきである．また，日常的に持ち歩くスマートフォンで MAC アドレスが確認できる場合，ストーカー被害を受ける可能性が高い．そのため iPhone のように確認ができないようする，BLE 端末の MAC アドレス自体も必ず定期的に変更するといった対策を行うべきである．

しかし，判明した識別値の有効利用として，汎用的な紛失物対策システム等に役立てることも可能であると考える．

6. 今後の課題

今後，BLE 端末の調査数を増やし，どのくらいの BLE 端末がプライバシー対策を行なっているのかを調査していく．また，BLE5.0 や Bluetooth を使用したイヤホン等の調査も進めていきたい．

7. 参考文献

[1]総務省　情報通信白書平成 29 年度版
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc133100.html