Vol.2018-CSEC-83 No.5
2018/12/13

短距離無線通信向け脆弱性検査ツールの初期的検討

瀬川周平[†1]　辻秀典[†2]　橋本正樹[†3]

概要：近年，IoT の利用が拡大している．IoT において，小型化・軽量化技術や無線通信技術等の技術的進歩によって，様々な無線プロトコルが現在では存在するが，一般に，小型無線機器とその通信には，主としてリソースの乏しさに起因するセキュリティ上の懸念があり，特にパーソナルデータの取得のために人体に取り付けるタイプの IoT に関してはプライバシーを守る重要性が高い．本研究では，今後も様々な場面で拡大すると思われる IoT の普及を見据えて，小型無線機器のセキュリティ耐性を確認し，これを強化するための基礎とするために，通信の脆弱性検査ツールを作成する．特に IoT 利用の新しい分野においては，過渡期に暗号化通信がされていない機器のように脆弱な機器が多く出回ることが予想される．よって，いくつかのプロトコルにおいて，難読化のみの通信であればデータの解析が可能であるツールの作成を目指す．本研究の成果が，各々のベンダーによる事前の脆弱性検査とセキュリティ担保の一助となることを期待するものである．

キーワード：小型 IoT 機器，短距離無線通信，通信検査ツール

A Preliminary Study on a Vulnerability Scanner for Short-range Wireless Communication

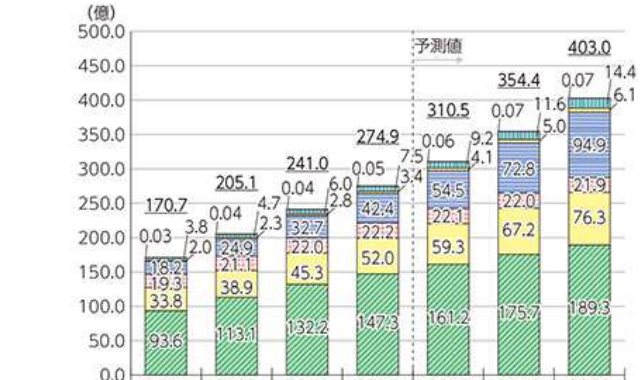
Shuhei SEGAWA[†1]　Hidenori TSUJI[†2]
Masaki HASHIMOTO[†3]

Abstract: In recent years, the use of IoT is expanding. At IoT, various wireless protocols currently exist due to technological advances such as miniaturization / lightweight technology and wireless communication technology, but in general, small wireless devices and their communication have security concerns primarily due to poor resource. Particularly with respect to IoT of the type to be attached to the human body in order to acquire personal data, it is necessary to keep privacy. Therefore, In this research, in anticipation of the spread of IoT which is expected to expand in various scenes from now on, in order to confirm the security tolerance of small radio equipment and to make it the foundation for strengthening it, we will create a communication vulnerability test tool. Particularly in new fields using IoT, it is expected that many vulnerable devices will be on the market, as in devices that do not have encrypted communication during the transition period. Therefore, in some protocols, we aim to create tools that can analyze data only if obfuscating communication only. We hope that the results of this research will be useful for preliminary vulnerability examination and security collateral by each vendor.

Keywords: Small IoT equipment, short-range wireless communication, communication test tool

1. はじめに

モノのインターネットと呼ばれる IoT (Internet of things) が各分野で注目を浴び, IoT 機器が増加している．ここで、総務省 平成 30 年版 情報通信白書の 2020 年までの世界の IoT デバイス数の推移及び予測[1]を図 1 に分野・産業別の IoT デバイス数及び成長率予測[1]を図 2 に示す．



	2014	2015	2016	2017	2018	2019	2020
合計	170.7	205.1	241.0	274.9	310.5	354.4	403.0
軍事・宇宙・航空	0.03	0.04	0.04	0.05	0.06	0.07	0.07
自動車	3.8	4.7	6.0	7.5	9.2	11.6	14.4
医療	2.0	2.3	2.8	3.4	4.1	5.0	6.1
産業用途	18.2	24.9	32.7	42.4	54.5	72.8	94.9
コンピューター	19.3	21.1	22.0	22.2	22.1	22.0	21.9
コンシューマー	33.8	38.9	45.3	52.0	59.3	67.2	76.3
通信	93.6	113.1	132.2	147.3	161.2	175.7	189.3

図 1　世界の IoT デバイス数の推移及び予測

†1，†2，†3 情報セキュリティ大学院大学
Institute of Information Security

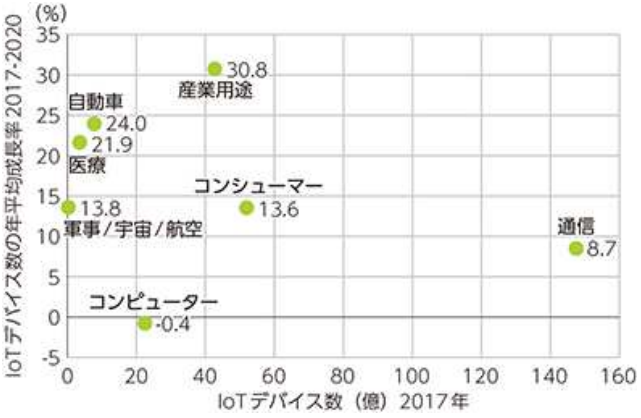


図 2　分野・産業別の IoT デバイス数及び成長率予測

各分野で成長が見込まれる中、今後大きく伸びると予測される分野に医療がある．このように，IoT 機器がパーソナルデータの取得に用いられることが期待されており，医療や健康分野において，高齢化や健康意識の高まりから，人体に接続して用いる IoT 機器（以降，人体 IoT と呼ぶ）の増加が予測されている．人体 IoT では，人体表面や内部から情報を集めることを想定しており，ここで情報をやり取りする短距離無線ネットワークのことを一般的にボディ・エリア・ネットワーク(Body Area Network：以下 BAN)と呼ぶ．今後，人体 IoT が普及すると，常時，無線通信をする機器を身につけた人々が出歩くようになり，セキュリティにおいても従来のセンサーネットワークを超えて，より注視すべき脅威に対応しなければならない．

以降本稿では，第 2 章で，研究の背景および研究の目的を説明する．人体 IoT の動向, BAN の国際規格である IEEE 802.15.6[2]の概要や他の短距離無線通信との違いを説明し，人体 IoT における短距離無線通信のセキュリティ課題を考察する．第 3 章で，人体 IoT 機器の脆弱性検査ツール開発に向けた初期的検討を行う．現状，人体 IoT 機器が数少なく手に入らないため人体 IoT 機器に求められるプロトコルの条件を定めて実験対象プロトコルの選択を行った．選択したプロトコルの通信の解析ツールを作成するにあたり，先行の解析ツールを紹介する．これは，本研究で作成を目指すツールの参考および比較対象とするツールである．第 4 章で，現在までの研究の進捗を説明する．現状は取得した信号に対して相対的にノイズの影響が大きいため，解析プログラムを作成できていない．よって，その現状を打開するための対策および今後の予定についても説明する．

2. 研究の背景

2.1 人体 IoT の動向とセキュリティの現状

人体 IoT の普及に関して，2025 年に世界で約 19 兆円 ~ 175 兆円の付加価値があるという予測がある．また，付加価値額は，先進国で 89 %を占める，との予測であることから，先進国で最も高齢化が進む日本で，特に恩恵の大きい技術であり，普及に向けた動機があると思われる[3].

人体 IoT の普及が予測される中，IoT のセキュリティに目を向けると，以下に示すように脆弱性が生じやすい背景がある[4].

- 機器のハードやソフトが非力でセキュリティ対策が不十分になりがち
- 機器を開発するベンダーのセキュリティの知識不足
- パッチをあてる仕組みが不十分
- 機器の耐用年数が長い
- 対策の責任がメーカー側にある
- 機器の種類が多く，対策に差がでる

これらは，IoT 機器における脆弱性が生じやすい背景であるが，人体 IoT 機器に関しては，特に最初に挙げた「機器のハードやソフトが非力であること」が，セキュリティが弱くなる最も大きな要因であると考えられる．つまり，機器のリソースが非常に乏しいために，セキュリティにリソースが割けないことや，妨害が比較的容易に達成されてしまう，といったことに繋がる．特に健康管理用途のように，バイタルデータを取得し，ほとんどが片側通信の機器について当てはまる．

2.2 BAN

BAN とは，体の表面や体内など，体の周辺に配置した各種のセンサーやデバイスで構築するネットワークのことである．BAN に用いられる無線プロトコルは様々であるが，ここでは BAN 向けの無線通信方式の国際規格として, 2012 年に制定された IEEE802.15.6 を紹介する. IEEE802.15.6 は，医療・健康用途への適用を前提とした規格である．

次に IEEE 802.15.6 (BAN)と主な短距離無線通信規格の比較を表 1 に示す.

表 1　BAN と代表的な近距離無線通信方式[5]

規格名	802.15.6(BAN)	BLE	ANT / ANT+
伝送距離	最大 2m 程度	最大 10m	10～15m 程度
消費電流 (電圧 3V)	10mA 以下	数 mA	数 mA～10 数 mA(ピーク) 数 μA～ 数十 μA(平均)
周波数帯	400MHz 帯, 860MHz 帯, 900MHz 帯, 950MHz 帯，2.4GHz 帯，UWB(3.1G – 10.6GHz)，人体通信	2.4GHz 帯	2.4GHz 帯
変調方式	BPSK，QPSK，GMSK	GFSK，FHSS	GFSK
パケット容量	最大 255 バイト	最大 27 バイト	8 バイト
伝送速度	最大 1M～10M ビット/秒	最大 1M ビット/秒	1M ビット/秒
ネットワーク	スター	スター	スター，ツリー，メッシュ

主な特徴として, BAN では周波数帯が多様であることがあげられる．一方，他の短距離無線通信規格では，2.4GHz 帯を使用するものが多い．BAN では，2.4GHz 帯が逼迫していることや，通信品質の確保の必要性で，アプリケーションにより，周波数を選択できる．変調方式は，低消費電力を実現する実装を容易にするための方式を採用している[6]．ネットワークについては，BAN は，スター型しか採用できない．このように BAN は，想定される利用ケースから得た技術要求に基づいた仕様である．

BAN の課題に関しては，現在各所で研究・検討が進められている [7][8][9][10]．これらの研究で指摘された BAN の特徴とセキュリティ要件の問題点を整理し，表 2 に示す．

表 2　BAN の特徴とセキュリティ要件

要件	脅威	対策	問題点
認証	偽装	認証，検知	メモリ制約
機密性	盗聴	暗号化	電力制約，メモリ制約，低計算能力
完全性	リプレイ攻撃，改ざん	認証，順序，遅延拒否	メモリ制約
可用性	DoS 攻撃，ジャミング	ネットワークコーディング	電力制約，低 SN 比
プライバシー	・(※機密性と同様) ・緩いアクセスポリシー	・(※機密性と同様) ・厳密なアクセスポリシー	・(※機密性と同様)

整理してみると，機密性およびプライバシーと，可用性のセキュリティが特に脆弱であることが分かる. 機密性は, 電力制約，メモリ制約，低計算能力により，暗号化が困難であるために弱くなる. 可用性は, 短距離通信を行うため, シグナルが元々弱く SN 比が低いのだが，この特徴のためにジャミングなどでノイズを加えると，比較的容易にパケットを破棄するといった妨害行為が可能となる．

このような理由から，BAN に使用される機器は，認証や暗号化を施していない通信がデフォルト設定になっている機器が大半を占める．よって，これから人体 IoT 機器が普及していくと，通信に機密性の脆弱性がある機器が出回ることが予想される．

2.3 研究の目的

これまで調査した内容から，人体 IoT 機器は，リソースが乏しく，特に機密性と可用性に弱いことが分かった．また，認証や暗号化がされていない通信をする機器が出回ることが懸念されている．このようなリソース不足に起因する懸念に加えて, 2.1 で述べたように, 脆弱性が生じやすい背景として，機器を開発するベンダーのセキュリティの知識不足も指摘されている．

本研究では，様々な無線プロトコルに対応した通信の脆弱性検査ツールの開発を目指す．開発するツールでは，人体 IoT で特に重要性の高い, 機密性に焦点をあてる. なお, 研究を検討するに当たり，平成 29 年 10 月に総務省から公表された「IoT セキュリティ総合対策」[11]も参考にしたが, これによると，具体的施策の脆弱性対策に係る体制の整備において,「簡易な脆弱性チェックソフトの開発等」が挙げられている．

3. 脆弱性検査ツール開発に向けた初期的検討

3.1 対象プロトコルの選択

開発に向けて，まずは人体 IoT に望ましいと考えられるプロトコルの要件を以下に記す.

1)　長期使用
　・低消費電力
　・通信距離が短い
　・干渉しにくい周波数帯
　・複数センサーから同時通信可能
2)　セキュリティ
　・最小限のアドホック

長期使用という要件に関しては，人体に取り付けるので長期間取り外しを行わなくて済むことが望ましい. よって, 最小限のデータ通信であることや通信距離が短いことが求められる．また，干渉しにくい周波数帯という条件については，送信時に最も電力を消費することから，干渉によりデータを再送しないことが望ましい．プロトコルによっては，再送しないプロトコルが存在し，その場合，データが失われるといった欠点もある．

セキュリティに関しては，最小限のアドホックが望ましい．ある IoT 機器が感染してしまうと，アドホックにより感染が他の機器に拡大することがあるためである[12].

続いて，開発する脆弱性検査ツールで，検査対象とする無線プロトコルの候補を表 3 に示す．記載した無線プロトコルは，ウェアラブルとして普及しているプロトコルや干渉しやすい 2.4GHz 帯以外の周波数帯で，送信電力が小さいものを選択している．これは，先に挙げた BAN に望ましい条件をより多く満たすプロトコルである．

表 3　実験に用いる無線プロトコルの候補

方式	周波数 [MHz]	通信距離 [m]	送信電力 [mW]	ネットワーク
ZigBee	2400 902-928 868-878	50	1	P2P, Star, Tree, Mesh
Sub-GHz	150-950	10-700	20 1	P2P, Star, Tree, Mesh
EnOcean	868 902 928.35	100	1	Star

IEEE802.15.6 に関しては，製品または，モジュールを対象として研究を進める予定でいたが，現在そのような機器は出回っておらず，他のプロトコルを選択することにした．しかしながら，今後 IEEE802.15.6 に従った人体 IoT 機器が出てくる可能性を勘案し，現時点では開発するツールの検査対象にはしないが，プロトコル設計に関しては BAN に望ましい設計であるため，対象プロトコルの選択の際の参考とするに留める．

3.2 解析ツールの予備評価について

表 3 の対象プロトコルの候補に対して，本研究で開発するツールと比較するために，はじめに既存解析ツールを予備評価する．表 4 に既存解析ツールの一覧を記載する．

表 4　各プロトコルの解析ツール

プロトコル	解析ツール	対象機器
ZigBee	・Atmel RzRaven USB Zigbee Sniffer / Injector ・Universal Radio Hacker ・Scapy-radio	ZigBee 製品 or 無線モジュール
Sub-GHz (独自プロトコル)	・Universal Radio Hacker ・Scapy-radio	製品 or 無線モジュール
EnOcean	・Universal Radio Hacker ・Scapy-radio	EnOecean 製品

様々な解析ツールが存在するが，本研究では，次節で紹介する Scapy-radio[13]と Universal Radio Hacker (以降, URH) [14]を主に評価する．また，普及しているプロトコルである ZigBee には有料の解析ツールがあるので，ZigBee プロトコルの評価をする場合は，こちらのツールも評価していく予定である．

3.3 Scapy-radio と Universal Radio Hacker (URH)

Scapy-radio と URH について説明する．これらのツールは，以下の動機により作成されたものと説明されている．

- 無線プロトコル単体のチェック機器は存在するが，独自プロトコルが頻繁に登場しているので不十分である．
- デジタル信号処理（DSP），コーディング理論，プロトコル設計の専門知識がない人でも解析をやりやすくする．

最初に，Scapy-radio について説明する．Scapy-radio は，二つの機能を組み合わせたツールである．

① ソフトウェア無線(Software-defined radio : SDR)で，各プロトコルの信号処理
② Scapy でパケット操作，SDR の自動立ち上げ，パラメータ入力

無線通信の解析をする場合，多くは，ソフトウェア無線のみで解析可能であるが，いくつかのプロトコルに対応させ，自動で解析可能にするために Scapy を加えたツールである．[12]によると，Scapy 側で解析する無線プロトコルの選択とパラメータ入力を行うことで解析に欲しい情報を自動で得られることになっている．

結果としては，Z-wave という無線プロトコルに関しては，解析と攻撃ツールの作成まで数時間で実施した．また BLE に関しては，解析後の攻撃がうまくいかなかった．と，言及があり，他のプロトコルに関して解析が成功したという報告はない．

次に，URH について説明する．URH は，2017 年の Black hat USA 2017 arsenal で発表されており，この類のツールで最新のものと思われる．ただし，使用した結果を報告したものがないため，機能だけ以下に記す．

① 送受信用のソフトウェア無線インターフェース
② DSP(デジタル信号処理)抽象化
③ 容易にカスタマイズ可能なエンコーディング
④ ロジック分析支援
⑤ ファジング

Scapy-radio と URH の特徴や違いについては，以下のように整理できる．

はじめに，Scapy-radio に関しては，Scapy-radio 内の操作で解析したい無線プロトコルを選択し，パラメータを入力するだけで解析結果が得られるツールであると思われる．

カスタマイズする場合や，解析対象のプロトコルを追加するには，SDR フローを自分で作成する必要があり，また解析プログラムが別途必要であれば，自分でコーディングする必要がある．そのためには，対象の無線プロトコルや SDR の知識が必要である．よって，ツールの完成度が高ければ迅速に解析が可能であるツールと言える．

一方，URH に関しては，機能に記したようにロジック分析支援に優れているツールである．分析機能によって様々なパラメータがあり，それらを操作し設定することで，詳細な解析を試みる．例えば，復調機能では，振幅変調(ASK)，周波数変調(FSK)，位相変調(PSK)に対応している．また，プリアンブル，データ，宛先 ID などのデータの分類機能がある．これらの備わっている機能を駆使して解析していく．ただし，既存の設定では解析ができないプロトコルがある．いくつかの機器で使用したところ，信号が弱く SN 比が低いプロトコルの通信の解析結果が正確ではない．

これらを比較して，より正確な解析をするためには，Scapy-radio タイプのツールがより良いと判断した．よって，本研究では，Scapy-radio を参考に，短距離無線通信向け脆弱性検査ツールを作成していく．

4. EnOcean の解析実験

4.1 解析実験の概要

EnOcean（表 4）は，第 4.1 節で示した人体 IoT に望ましい条件に近いプロトコルである．EnOcean は，エネルギーハーベスト技術を有しており，これは，周囲の環境からエネルギーを得て，それをデータの取得や送信に使用する．人体 IoT は，長期使用が求められるため，この技術は親和性が高い．また，得られた極小のエネルギーを効率良く使用する独自のプロトコルが優れているため，最初の解析実験対象として選択した．表 5 に EnOcean テクニカルデータを示す．

表 5　EnOcean のテクニカルデータ

周波数	928MHz 帯
通信到達距離(屋内)	10m
伝達速度	125kbps
変調方式	ASK，FSK

4.2 URH による EnOcean の解析実験

まず，EnOcean に対して，URH を用いて解析を試みた．以下は研究に用いた機器である．

- 解析対象機器
  EnOcean STM431J (温度センサー)
- URH の環境
  ubuntu-16.04.2-desktop-amd64-gnuradio-3.7.11.iso
- フロントエンド
  DS-DT305WH

次に，データ取得時の概要図を図 3 に示す．

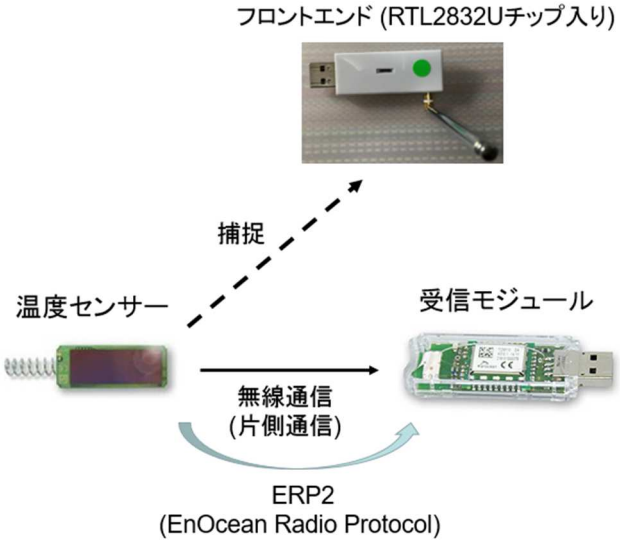


図 3　EnOcean データ取得の概要図

注意点としては，温度センサーとフロントエンド(アンテナ)との間は密着させない．というのも，敵対者を想定したときに無線が届く範囲で取得するはずで，機器に密着した状態で取得することは稀だからである．

今回の温度センサーの場合は，固有のセンサーID および本データである温度情報を解析できれば解析を成功したとする．解析するプロトコルは，EnOcean Radio Protocol 2 である．URH を使用した解析結果を表 6 に記載する．

表 6　URH による EnOcean の解析結果

項目	結果	正解データ
周波数	928.350MHz	928.350MHz
変調方式	特定できず	FSK
パケット出力時間	1ms 未満	0.992ms
ビットレート	確認	125kbps
パケットサイズ	特定できず	124bit
センサーID	特定できず	04 01 30 DE
データ	特定できず	00 00 54 08

4.3 Scapy-radio による EnOcean の解析実験

次に，Scapy-radio タイプのツールの基礎となる SDR で解析を試みる．以下は研究に用いた機器である．

- 解析対象機器
  EnOcean STM431J (温度センサー)
- SDR の環境
  ubuntu-16.04.2-desktop-amd64-gnuradio-3.7.11.iso
- フロントエンド
  DS-DT305WH

データ取得の環境は，図 1 の通りである．SDR は，オープンソースである GNU Radio companion[15]を用いた．図 4 に SDR のフロー図を示す．

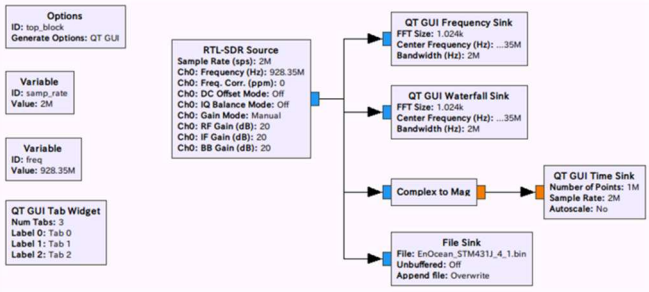


図 4　SDR のフロー図

最初は，最もシンプルな構成で試みた．主に変更するパラメータは，サンプルレートと RF Gain(dB)である．サンプルレートは，1 秒あたりに取得するサンプル数である．サンプルレートを変更してデータを取得する理由は，変調方式が FSK であり，取得するデータが時間変化に対応したものではないためであり，1 周期あたりのサンプル数の変化で変調をとらえる．RF Gain はアンテナのゲインに合わせるが，アンテナと同じゲインできれいなデータが得られるとは限らないので，RF Gain をいくつか変更してサンプルを取得した．その中で現時点において最もきれいに取得できたデータを示す．サンプルデータ 3M/s，RF Gain : 25dB で取得したデータをエクセルにプロットしたものを図 5 に示す．

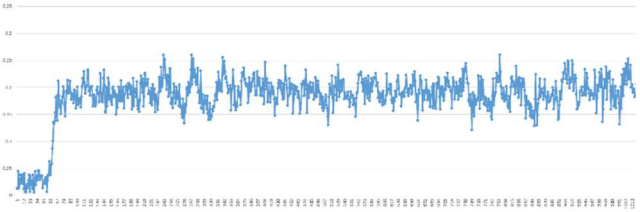


図 5　SDR から得たデータをプロットした図

4.4 解析実験結果の考察

はじめに，URH による解析結果については，FSK で指定すると 30bit や 40bit 周辺の結果を出力してくるため，正解データには程遠い結果であった．ただ，EnOcean は低消費電力のプロトコルであり信号も弱いため，データ取得環境の違いやフロントエンドの性能により上手く解析できていない可能性がある．よって，環境を変更して，もう一度解析を試みる予定である．次に，Scapy-radio による解析結果については，EnOcean STM431J 温度センサーデータの解析の成功には至っていない．信号が弱いため，本来の信号であるシグナル(Signal)とノイズ(Noise)の比である SN 比が低くなりノイズの影響が相対的に大きくなってしまっている．そのため，このデータからは正確に復調ができていない．

これら予備評価としての解析実験の課題については，以下の対策が考えられる．

1. SDR フローの機能を活用する
2. EnOcean の受信機がどのようにデータを取得しているのか調べる
3. ノイズを極力小さくする環境を作ってデータを取得し，分析する

1. については，現在の SDR の解析フローでは使用していない信号の増幅機能やノイズ軽減機能を使用する．現状では SN 比が低いために得られたデータを復調するプログラムを作成できていないと考察しているが，この対策により SN 比を高くすることを試みる．また，データの取得は，これまでと同様に攻撃者の環境を考慮してセンサーとフロントエンドは密着させない．

2. については，EnOcean の受信機は正しく復調してデータを取得している．そこで、EnOcean の仕様等をより詳しく調べ，どう復調しているかを調査することと，EnOcean 受信機からデータをキャプチャし，解析のヒントを得ることを試みる予定である．

3. については，攻撃者の環境を考慮していないが，1.と同じく，できるだけ SN 比を高くして解析をすることが目的である．その際に，まずは現状のシンプルな SDR の解析フローで試みる．得られたデータで復調できるならば，その解析方法で通常環境でも解析が可能かを調べる．

5. おわりに

本稿では，第 2 章で，研究の背景および研究の目的を説明し，人体 IoT の動向や BAN の国際規格である IEEE 802.15.6 の概要，人体 IoT における短距離無線通信のセキュリティ課題を考察した．第 3 章で，人体 IoT 機器の脆弱性検査ツール開発に向けた初期的検討で，対象プロトコルの選定と先行の解析ツールを紹介した．先行ツールの性能

などを比較し，本研究では Scapy-radio タイプのツールを作成するという決定に至る経緯を説明した．第 4 章で，現在までの研究の進捗と現状を打開するための対策を説明した．対策としては，信号が弱いために SN 比が低くなり，復調するプログラムを構築できない問題があるため，最初の対策として，SN 比を上げてデータを取得する対策を行っていく．

今後の取り組み予定に関しては，第 4 章の「4.4 解析実験結果の考察」で述べたように，現状で出来ていない EnOcean の通信データの解析の対策を行い，SDR による解析を試みる．その解析が成功した後は，「3.1 対象プロトコルの選択」の「表 3 実験に用いる無線プロトコルの候補」で挙げた他のプロトコルで解析を試みる．Sub-GHz 帯の独自プロトコルモジュール，次に ZigBee の 2.4GHz 帯ではない周波数帯のモジュールおよび製品で解析を試みる．また，EnOcean プロトコルに対して SDR の解析が終われば，他のプロトコルの SDR 解析フローの作成と並行して，Scapy-radio を参考に解析の自動化および操作性の向上を試みる予定である．

参考文献

[1] “総務省 平成 30 年版 情報通信白書 第 1 節 世界と日本の ICT 市場の動向” http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/n1100000.pdf
[2] 802.15.6-2012-IEEE Standard for Local and metropolitan area networks-Part 15.6：Wireless Body Area Networks http://standards.ieee.org/findstds/standard/802.15.6-2012.html
[3] MCKINSEY GLOBAL INSTITUTE “THE INTERNET OF THINGS:MAPPING THE VALUE BEYOND THE HYPE ”. http://semanticsoftware.com/media/1101/unlocking_the_potential_of_the_internet_of_things_executive_summary.pdf
[4] “Security of Things (モノのセキュリティ) の時代” https://www.tel.co.jp/museum/magazine/communication/160129_report02_01/index.html
[5] “BAN とは” https://tech.nikkeibp.co.jp/dm/article/WORD/20140217/334502/?ST=health
[6] 滝沢賢一，李還幇，三浦龍．“無線ボディエリアネットワーク技術使用の国際標準化動向”． http://www.bme-emc.jp/pdf/24no3Takizawa.pdf
[7] Garth V. Crosby, Tirthankar Ghosh, Renita Murimi, Craig A. Chin. “Wireless Body Area Networks for Healthcare: A Survey.” International Journal of Ad hoc，Sensor & Ubiquitous Computing (IJASUC) Vol.3，No.3，June 2012
[8] Saeideh Sadat Javadi, M.A. Razzaque.“Security and Privacy in Wireless Body Area Networks for Health Care Applications.” Wireless Networks and Security pp 165-187，2013
[9] Samaher Al-Janabi, Ibrahim Al-Shourbaji, Mohammad Shojafar, Shahaboddin Shamshirband. “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications.” Egyptian Informatics Journal 18 (2017) 113-122
[10] Shihong Zou, Yanhong Xu, Honggang Wang, Zhouzhou Li, Shanzhi Chen，Bo Hu. “A Survey on Secure Wireless Body Area Networks.” Security and Communication Networks Volume 2017 (2017)，Article ID 3721234，9 pages
[11] 総務省「IoT セキュリティ総合対策」 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html
[12] Eyal Ronen, Adi Shamir, Achi-Or Weingarten, Colin O’Flynn. “IoT Goes Nuclear:Creating a ZigBee Chain Reaction.” 2017 IEEE Symposium on Security and Privacy
[13] Jean-Michel Picod, Arnaud Lebrun, Jonathan-Christofer Demay. “Bringing Software Defined Radio to the Penetration Testing Community”. Black Hat USA Conference，2014
[14] https://www.blackhat.com/us-17/arsenal.html
[15] “GNURadioCompanion” https://wiki.gnuradio.org/index.php/GNURadioCompanion