Vol.2019-SPT-32 No.24
2019/3/8

スマートホーム内のIoT機器を対象としたサイバー攻撃への耐性評価

坂本 憲理[1]　長友 誠[1]　岡崎 直宣[2]　朴 美娘[1]

概要：近年，一般家庭において冷蔵庫やスピーカーなどの家電製品に通信機能を搭載したIoT機器が普及している．これらの家電がインターネットにつながることで，ユーザーの利便性が向上する一方で，このようなIoT機器を対象としたサイバー攻撃による被害が後を絶たない．そこで本研究では，一般家庭向けのIoT機器を対象としたサイバー攻撃実験を行い，それに伴う影響について調査した．計12台のIoT機器からなるホームネットワークを構築し，家庭内サイバー攻撃として通信パケットの盗聴，ICMP/UDP floodによるDoS攻撃，不正操作について各種実験を行い，耐性評価を行った．その結果，平文で通信する一部の機器では動作命令や各種センサー値などの把握ができた．すべてのIoT機器においてDoS攻撃への耐性がないことを確認できた．また，1つのIoT機器においての不正操作に成功した．

キーワード：IoT，スマート家電，DoS攻撃

Resistance Evaluation of Cyber Attack for IoT Devices in Smart-Homes

Kensuke Sakamoto[1]　Makoto Nagatomo[1]　Naonobu Okazaki[2]　Mirang Park[1]

Abstract: In recent years, home appliances equipped with communication functions such as refrigerators and speakers have been spreading in most of households. User's convenience has been improving with these appliances connecting to internet. On the other hand, we have so many cyber attacks to IoT devices continuously. In this paper, we experimented these cyber attacks to IoT devices and we examined effects brought by these attacks. We constructed a Home-network consisting of 12 IoT devices and conducted various experiments on eavesdropping of communication packets, DoS attacks by ICMP / UDP flood and illegal operation as a cyber attack in a household. We evaluated the resistance in these experiments. As a result, it was possible to grasp the action command and various sensor values in devices communicating with plaintext. We confirmed that IoT devices do not have resistance to DoS attacks. In addition, we succeeded in illegal operation in one IoT device.

Keywords: IoT, Internet conected household devices, DoS

1. はじめに

近年，世界中の様々なモノがインターネットへつながるIoT(Internet of Things)時代が到来している．総務省によると2017年のコンシューマー向けIoTデバイス数は52億台に対し，2020年には76.3億台にまで増加すると予測されている[1]．それに伴い，冷蔵庫やスピーカーなどの家電製品に通信機器を搭載したスマート家電が普及し始めている．家電がインターネットにつながることで，ユーザーは様々なサービスを享受することができ，利便性が向上する．例えば，外出先からリモートで玄関の鍵の解錠や施錠を行ったり，帰宅前に自宅のエアコンの電源を入れることで到着する間に最適な温度にしたりすることができる．一

[1] 神奈川工科大学
Kanagawa Institute of Technology
[2] 宮崎大学
University of Miyazaki

方で，このような家庭内の IoT 機器に対するサイバー攻撃が懸念される．例えば，2016 年にフィンランドにおいて空調や水道の温度をコンピュータで管理しているビルが DDoS 攻撃の被害に遭い，暖房が停止した事例がある [2]．また，様々な場所に設置されているネットワークカメラの映像をまとめているサイトが存在する [3]．掲載されている映像は多岐に渡り，店舗や職場の他に一般家庭に設置されたカメラの映像も確認できる．これはカメラの閲覧に必要な認証情報を初期パスワードや単純なものを利用していることが原因である．このように身近な IoT 機器がサイバー攻撃の被害に遭うことで，人間の生活や命を脅かしたり個人のプライバシーを侵害されたりする恐れがある．

このような IoT 機器に対するサイバー攻撃が注目されていることから，実際にサイバー攻撃を行い，その影響について分析を行った研究が行われている [4], [5]．しかし，実験対象の IoT 機器を通信ポート番号が固定されているものや既に脆弱性が報告されている機器を用いているため，サイバー攻撃による影響分析は不十分である．

そこで本論文では，通信機能を有した冷蔵庫や学習リモコンなどの幅広い IoT 機器を 12 製品接続したホームネットワークを構築し，それぞれの機器に対しサイバー攻撃を行い，その耐性について評価する．以下，2. で関連研究の紹介，3. でホームネットワークの構築および対象 IoT 機器の機能について述べる．4. で実験と評価を行い，最後の 5. でまとめと今後の課題について述べる．

2. 関連研究

楊らは，家庭内サイバー攻撃の実態を明らかにするため 16 種類のネットワーク接続可能な機器からなるテストベッドを構築し，スマート家電に擬似的な攻撃を行った後の影響について検証をしている [4]．最初の実験では，疑似サイバー攻撃の試行と影響分析のため今後起きると想定される家庭内サイバー攻撃をホームネットワークテストベッド内で行い，その現実性や影響について調査している．近年マルウェアに感染した IoT 機器を踏み台にした DoS 攻撃 (Denial of Service Attack) が確認されており大きな問題となっているため，IoT マルウェアに感染した Wi-Fi ストレージの実機を用いた攻撃実験と，比較検証のため制御サーバで専用の DoS 攻撃ツールを用いた場合の攻撃を行った．この実験で攻撃対象にした IoT 機器は，クラウドサーバからの通信を受信するための待受ポートが定まっている 7 種類である．実験結果として，マルウェアに感染した IoT 機器による DoS 攻撃では攻撃通信量が少ないにもかかわらず，半分以上の IoT 機器が動作しなくなることが確認できた．また，制御サーバからの攻撃では実験対象すべての IoT 機器が動作しなくなることが確認できた．2 つ目の実験では，動作命令の通信パケットをキャプチャーし，再送するリプライ攻撃で IoT 機器の不正操作が行えるか検証している．実験対象機器は，スマートリモコン・ロボット掃除機・スマート電源プラグの 3 種類である．実験結果は，平文で通信するスマートリモコンと可読性がない通信を行うスマート電源プラグでは不正操作に成功した．しかし，暗号化通信を行うロボット掃除機では不正操作に失敗した．

本研究においても，これらの手法を基に複数の IoT 機器からなるホームネットワークを構築し，DoS 攻撃への耐性や不正操作の検証方法を検討する．また，IoT 機器における DoS 攻撃への耐性評価を行う際は，対象 IoT 機器を選出せず，幅広い IoT 機器の耐性評価を行う．

Sivaraman らは，家庭用ルータによって保護された IoT 機器をスマートフォンにインストールされたマルウェアを介して攻撃用クラウドサーバからの不正操作が可能であることを実証している [5]．一般消費者向けの IoT 機器には認証資格情報が無い．そのため，このような状況下でも家庭用ルータがあることでインターネット上から攻撃されることはない．これはポートマッピングなどの設定がされていないルータではグローバル IP アドレス宛に着信したパケットをどのプライベート IP アドレスに転送するべきか把握していないからである．しかし，家庭用ルータに接続されたスマートフォンを用いて IoT 機器に割当てられたプライベート IP アドレスをポートマッピングすることで，IoT 機器をインターネット上に公開し，外部の攻撃用クラウドサーバとの通信を可能にさせる．実験では，認証資格情報が無いスマートプラグとネットワークカメラを対象として不正操作を行っていた．

この実験で用いられた IoT 機器は 2 種類のみだが，現在では様々な種類の IoT 機器が存在している．ゆえに，対象 IoT 機器を増やした環境で検証を行う必要があると考えられる．また，ネットワークに接続された IoT 機器を検出するため SSDP(Simple Service Discovery Protocol) を使用しているが，他の種類の IoT 機器も検出可能か調査を行う必要がある．

3. ホームネットワークの構築

本章では，4 章で行うサイバー攻撃実験の対象 IoT 機器の概要と構築したホームネットワークについて述べる．

3.1 対象 IoT 機器

本研究では IoT 機器のサイバー攻撃耐性評価を行うため，以下の Wi-Fi で接続する 7 個の IoT 機器と Bluetooth で接続する 5 個の計 12 個の IoT 機器を導入した．

① 学習リモコン/ゲートウェイ
赤外線リモコンを搭載しており，アプリからエアコンやテレビなどの操作を行うことができる．また，本体に搭載している温度・湿度計や Bluetooth で接続された各種センサーから得られたデータを制御サーバに送

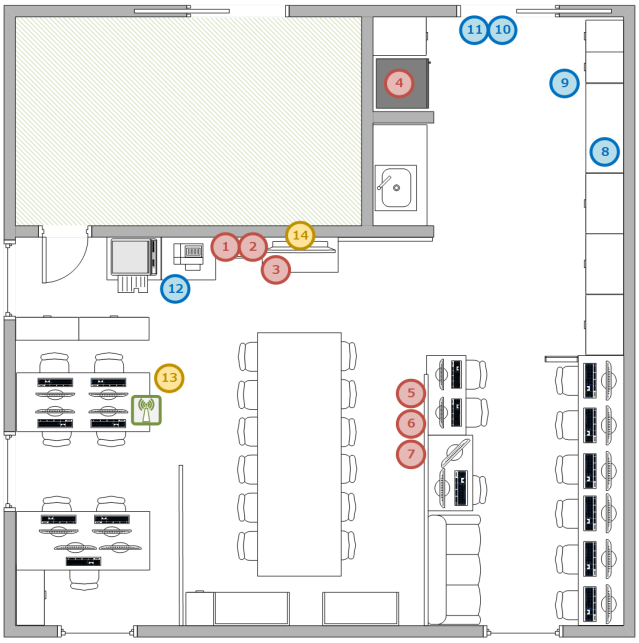

図 1 研究室に設置した IoT 機器

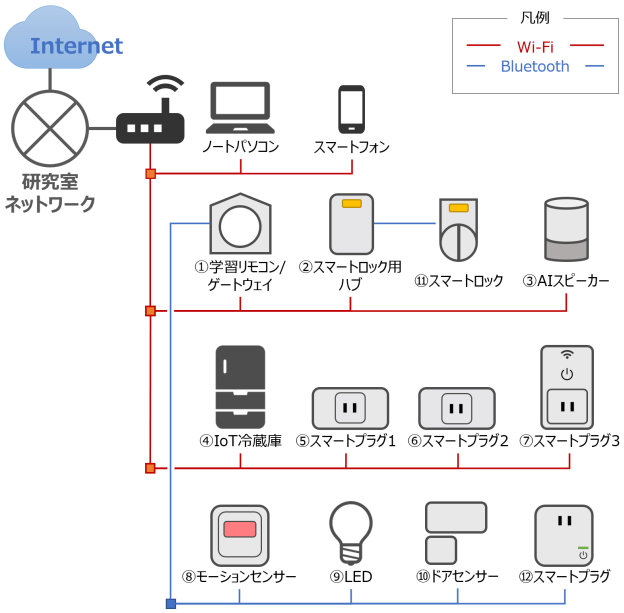

図 2 ホームネットワーク図

信する．

② スマートロック用ハブ
ハブに追加したスマートロックと BLE(Bluetooth Low Energy) で接続し，外出先から操作を行うことができる．

③ AI スピーカー
音声で対話を行い，天候やスケジューラーに登録した予定などを確認することができる．また各種サービスと連携することで音楽を再生したり，スマート家電の操作を行ったりすることができる．

④ IoT 冷蔵庫
音声で対話を行い，食品名を発言することでレシピの検索や買い物リストへの登録を行うことができる．またスマートフォンのアプリでレシピの検索結果や買い物リストのチェックを行うことができる．

⑤ スマートプラグ 1
コンセントでつないだ家電機器の電源のみコントロールできる．通信機能を有していないライトや扇風機などの白物家電をスマート家電化できる．EC サイトにて 1,000 円程度で販売されている．

⑥ スマートプラグ 2
機能は⑤と同様である．EC サイトにて 3,000 円程度で販売されている．

⑦ スマートプラグ 3
機能は⑤と同様である．EC サイトにて 4,000 円程度で販売されている．

⑧ モーションセンサー
赤外線で人の動きを感知できる．Bluetooth で①のゲートウェイと接続し，センサーの感知後は本体のインジケーターを発光させ，通知データを送信する．

⑨ LED ライト
通常の電球ソケットを持ち，Bluetooth で①のゲートウェイと接続する．ON/OFF だけでなく照度の調整もできる．

⑩ ドアセンサー
壁とドアに設置したセンサーでドアのオープン/クローズを判断し，状態に変化が生じた時に通知を送信する．Bluetooth で①のゲートウェイと接続する．

⑪ スマートロック
スマートフォンまたは②のハブと BLE で接続を行う．ドアの鍵の施錠または解錠を行う．

⑫ スマートプラグ
Bluetooth で①のゲートウェイと接続する．機能は⑤と同様である．

4 つのスマートプラグの中で⑤，⑥，⑦に関してはすべて Wi-Fi で接続し，同じ機能を有しているが，4 章の実験において価格帯の違いによる差を確認するため 3 製品導入した．

以上の製品をあらかじめ研究室に設置されている扇風機⑬とテレビ⑭やドアに配慮し，**図 1** に示すように研究室内に設置した．図 1 内の丸で囲んだ数字は IoT 機器の連番リストの数字とそれぞれ対応している．また，赤で塗りつぶした機器は Wi-Fi で通信し，青で塗りつぶした機器は Bluetooth で通信を行う．黄色で塗りつぶした機器は通信機能を有していない家電製品である．また，Wi-Fi ルータは緑色のアイコンで示した場所に設置した．

3.2 ホームネットワークの構築

3.1 節に挙げた製品群のうち Wi-Fi で接続する IoT 機器は，無線 LAN ルータと 2.4GHz 帯の無線で接続し，**図 2**

表 1　通信の可読性

対象製品	動作内容	IoT 機器⇔制御サーバ		スマートフォン⇔制御サーバ	
		プロトコル	可読性	プロトコル	可読性
①学習リモコン/ゲートウェイ	温度計測	HTTP	○ (ASCII)	MQTT	○ (ASCII)
	扇風機電源切替	HTTP	○ (ASCII)	MQTT	○ (ASCII)
	⑧モーションセンサー	HTTP	○ (ASCII)	MQTT	○ (ASCII)
	⑨LED 点灯切替	HTTP	○ (ASCII)	MQTT	○ (ASCII)
	⑩ドアセンサー	HTTP	○ (ASCII)	MQTT	○ (ASCII)
	⑫スマートプラグ	HTTP	○ (ASCII)	MQTT	○ (ASCII)
②スマートロック用ハブ	⑪解錠	TLSv1.2	×なし	TLSv1.2	×なし
	⑪施錠	TLSv1.2	×なし	TLSv1.2	×なし
③AI スピーカー	音声操作	TLSv1.2	×なし	-	-
④IoT 冷蔵庫	音声操作	TLSv1.2	×なし	TLSv1.2	×なし
⑤スマートプラグ 1	電源操作	TLSv1.2	×なし	TLSv1.2	×なし
⑥スマートプラグ 2	電源操作	TLSv1.2	×なし	TLSv1.2	×なし
⑦スマートプラグ 3	電源操作	STUN	△ (ASCII)	TLSv1.2	×なし

に示すようなネットワークを構築した．なお研究室ネットワークに IoT 機器群を接続した場合，実験中に他のコンピュータや通信に影響を与えてしまうことが考えられるため，研究室ネットワークから隔離した．

⑧モーションセンサー，⑨LED ライト，⑩ドアセンサー，⑫スマートプラグの 4 製品に関しては，専用のゲートウェイである①の機器と Bluetooth で接続している．⑪スマートロック単体ではインターネットに接続することができないため，②スマートロック専用のハブと BLE で接続している．

またネットワークには IoT 機器の他に，操作用のスマートフォンやノートパソコンなども接続されている．

4. 実験と評価

本章では，3 章で構築したホームネットワークを使用し，通信パケットの盗聴，サイバー攻撃耐性の有無の確認そして不正操作の 3 つの実験を行う．

4.1 通信パケットの盗聴

4.1.1 実験概要

ルータに脆弱性がある場合，マルウェアの感染や不正侵入によりホームネットワーク内の通信内容を攻撃者により盗聴される可能性がある．そこで，ホームネットワーク内の IoT 機器の通信を盗聴し，それぞれの IoT 機器の動作内容を把握できるか確認を行う．なお多くの IoT 機器はスマートフォンにインストールしたアプリで操作が行われるため，スマートフォンの通信も盗聴の対象とした．

実験を行う際に，IoT 機器やスマートフォンとルータ間の通信を盗聴するため，ノートパソコンを介して通信を行うようネットワークを変更した．

ノートパソコンをルータに接続し，Windows10 のモバイルスポットを用いて盗聴する機器をそれぞれ別のノートパソコンに接続した．

通信内容の盗聴には，ネットワークプロトコルアナライザーである Wireshark[6] を用いた．具体的な実験手順を以下に示す．

(1) 2 台のノートパソコンを用意し，モバイルホットスポット機能を有効にする．
(2) IoT 機器とスマートフォンを手順 (1) のノートパソコンにそれぞれ接続する．
(3) 正常に操作が行えるか確認する．
(4) 通信パケットのキャプチャーを開始する．
(5) スマートフォンまたは IoT 機器にて操作を行う．
(6) 通信パケットのキャプチャーを終了する．

4.1.2 実験結果

最初に通信パケットの送信先に着目した結果，スマートフォンで操作を行う IoT 機器では，アプリが送信した操作命令を直接 IoT 機器に送信するのではなく，外部の制御サーバを介して送信していることが確認できた．

これを踏まえ IoT 機器と制御サーバ間およびスマートフォンと制御サーバ間のそれぞれを盗聴した．その動作内容の確認についてまとめた結果を**表 1** に示す．「可読性」の項目中の「○」は IoT 機器の動作内容を把握できたことを意味し，「×」は把握できなかったことを意味する．また，「△」はペイロード部の可読性はあるものの動作内容の把握ができなかったことを意味する．

結果として，多くの IoT 機器では SSL/TLS による暗号化通信を行っているため，動作内容を把握することがで

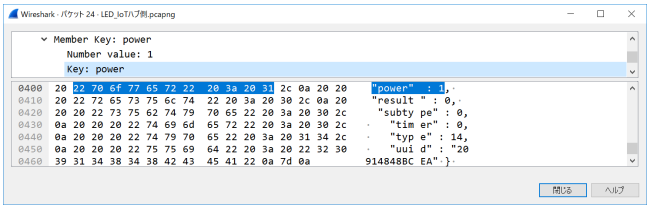

図 3　LED 点灯の返答パケット

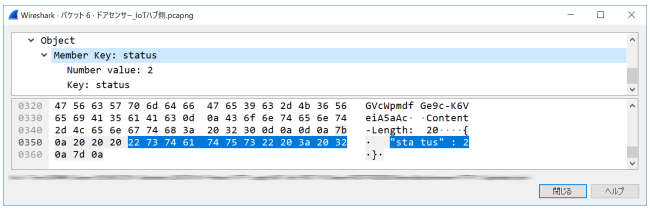

図 4　ドアセンサーの返答パケット

きなかった．しかし，一部の製品において平文で通信を行っていることが確認できた．特に①学習リモコン/ゲートウェイを経由する機器ではすべての動作内容を覗くことができた．スマートフォンのアプリにより⑨LED ライトの点灯を行った結果を返すパケットおよび⑩ドアセンサーが反応したことを通知するパケットのペイロードの部をそれぞれ図 3, 図 4 に示す．

LED 点灯の操作結果を返すパケットのペイロード内を確認したところ“power”の後に 1 が書き込まれていることが分かる．そこで消灯を行った場合のパケットと比較したところ，1 ではなく 0 が書き込まれていた．つまり，“power”の後の数字に着目することで，点灯・消灯を行った命令なのか把握できる．またこの LED は照度の調整も行うことができるが，設定した照度の値も確認することができた．

同様にドアセンサーの反応を通知するパケットでは，ペイロード内の“status”の後が 2 であればオープン状態であり，1 であればクローズ状態である．またパケットはセンサーの反応直後に送信されることから，キャプチャーした時刻がセンサーの反応した時刻とほぼ一致する．よって動作内容を盗聴している攻撃者は，ユーザーがいつドアを開閉したのか把握することができる．

また，他のセンサーや動作内容の情報を複数組み合わせることによってユーザーが在宅しているのか外出しているのか盗聴している攻撃者が判断できる可能性がある．そのためプライバシーの侵害や空き巣の対象になる恐れがある．

さらに家庭内の通信だけでなく，外出先で公衆無線 LAN に接続してリモート操作を行った場合も第三者の盗聴により IoT 機器の操作が漏洩してしまう恐れがある．

以上より IoT 機器の操作に伴う通信データは重要なプライバシー情報であるため，リソース資源が限られている IoT 機器においても通信路の暗号化を施す必要があると思われる．

4.2　サイバー攻撃耐性

4.2.1　実験概要

近年，IoT 機器を対象にした DoS 攻撃 (Denial of Service Attack) が確認されており，問題となっている．DoS 攻撃とは，サービス不能攻撃，サービス拒否攻撃，サービス運用妨害攻撃と呼ばれ，対象機器のサービスそのものを使用不能に陥らせる攻撃である．DoS 攻撃はその攻撃方法によっていくつかに分類されるが，本実験では資源の利用消費型の DoS 攻撃を行う．資源の利用消費型は，CPU，メモリ，ディスク，回線帯域などの有限なシステム資源を使い続け，サービスを使用できなくする形態である [7]．具体的な攻撃方法として，ICMP/UDP flood 攻撃が挙げられる．

ICMP flood とは，「ICMP」という通信の制御や通信状態の調査などを行うインターネットプロトコルの ICMP エコー要求メッセージを大量に送信して攻撃を行う手法である [8]．通常 ICMP エコー要求メッセージは，通信したいホストやルータに対して，IP パケットが到達するか確認する時に使われる．ICMP エコー要求メッセージを受信した機器は，到達可能であることを示すため ICMP 応答メッセージを送信する．ICMP flood では，ICMP エコー要求メッセージをターゲットに対して大量に送りつけるため，ターゲットは ICMP 応答メッセージを返そうとするが，大量の要求メッセージを処理できず，最終的にサービス不能状態となる．

UDP flood とは，UDP パケットを大量に送信して攻撃を行う手法である．UDP はコネクションレスで通信を行うことができるため，極端に大きなサイズの UDP パケットなどを一方的に送信できる．

一般的に，IoT 機器は省電力で動作するため，ネットワークのリソース資源がコンピュータやスマートフォンよりも少ない．ゆえに，1 台のコンピュータからの DoS 攻撃でもサービス不能状態にすることが可能だと考えられる．また，SYN flood 攻撃を行う際にはターゲットポートを把握する必要があるが，ICMP/UDP flood はターゲットのポート番号を把握せず DoS 攻撃を行うことができる．ICMP flood は，ターゲットにおいて ICMP エコー要求に返答するサービスが有効でないと使用することはできないが，多くの IoT 機器では有効のままになっていることから攻撃が成立すると思われる．

そこで本節では，ホームネットワークに接続されているコンピュータや IoT 機器がマルウェアに感染し，同一ネットワークに接続されている他の IoT 機器に対して DoS 攻撃を行うことを想定した実験を行う．具体的には ICMP/UDP flood 攻撃を行い，IoT 機器の攻撃耐性について評価する．

4.2.2　実験機器と手順

サイバー攻撃の対象 IoT 機器は，Wi-Fi で通信を行う必要があるため，3 章で構築したホームネットワークに接続されている IoT 機器のうちの 7 個とした．

表 2　攻撃ホストの性能

	ノートパソコン	Raspberry Pi3
OS	Ubuntu 18.04	Raspbian GNU/Linux 9
CPU	Intel Corei7-7500U @2.70GHz	Broadcom BCM2837 チップセット @1.20GHz
メモリ	8GB(DDR4)	1GB(LPDDR2)
有線 LAN	10/100 イーサネット	10/100 イーサネット
無線 LAN	IEEE802.11 b/g/n/ac	IEEE802.11 b/g/n

攻撃ホストは，ノートパソコンとマルウェアに感染した IoT 機器の代替として Raspberry Pi3 を用いる．それぞれのスペックを**表 2** に示す．Raspberry Pi3 は有線/無線 LAN を搭載した小型のマイコンボードであり，様々なセンサーと連携できるため，ガジェットとして使われる機会が多い．ゆえに，スマートホームにおける IoT 機器と資源リソースが同等だと考えられる．サイバー攻撃を行う際は，ルータと有線で接続した場合と 2.4GHz 帯の無線で接続した場合の両方で行う．

サイバー攻撃は専用の DoS 攻撃ツールである hping3[9] を用いる．これは，前節で説明した ICMP/UDP flood の両方を扱うことができる．DoS 攻撃を行う際は，送信元 IP アドレスの偽装を行う．偽装せず攻撃を行った場合，攻撃した分のパケット量を攻撃ホストでも処理する必要があるため，攻撃に支障をきたす恐れがある．

具体的な実験手順を以下に示す．

(1) IoT 機器とスマートフォンが使用可能か確認する．
(2) 攻撃ホストにターゲット IP アドレスと攻撃モードを指定する．
(3) DoS 攻撃を 1 分間行う．攻撃開始後・終了後に IoT 機器の動作を確認する．
(4) コンソール画面に表示された送信パケット数を記録する．

4.2.3　実験結果

ICMP flood および UDP flood 攻撃に対する攻撃耐性評価を**表 3** に示す．「攻撃耐性」の項目中の「×」は DoS 攻撃中に全く操作ができなかったことを意味し，「△」は操作を行うことはできたが，通常時と比べ操作を行うまで遅延があったことを意味する．「○」は DoS 攻撃を受けているが，正常に操作できたことを意味する．「通信量 (パケット)」の項目は，1 分間の DoS 攻撃で送信したパケット数である．

実験結果から DoS 攻撃によってすべての IoT 機器がサービス不能状態に陥ることが分かった．よって現状では，サイバー攻撃への耐性は不十分だと考えられる．ノートパソコンと比較して通信量が少ない Raspberry Pi3 からの DoS 攻撃でもいくつかの IoT 機器が使用不可になっている．ゆえに，ノートパソコンのような通信量が多い機器から DoS 攻撃を行う場合，ターゲットをホームネットワーク内のすべての機器にすることで，複数の IoT 機器が同時に使用不可の状態に陥ると考えられる．

家庭内機器による DoS 攻撃の対策として，主に以下の 3 つが挙げられる．1 つ目は，標準で ICMP エコー応答メッセージを送信せず，必要に応じてスマートフォンのアプリから応答を行うか切り替えられるように実装する方法，2 つ目は，今回のような DoS 攻撃による異常な通信量を検知し，機器自体でフィルタリングを行う方法，3 つ目は，近年市場で販売されるようになった家庭用侵入防止システムを導入し，パソコンやスマートフォンだけでなく IoT 機器も含めたセキュリティ対策を行う方法が考えられる．

4.3　不正操作の検証

4.1 節では，脆弱性のあるルータを使用した場合，ホームネットワーク内の通信が盗聴され，一部の IoT 機器の動作内容を把握できることを確認した．よって本節では，その盗聴内容から不正操作が行えるか検証する．

不正操作の検証には，記録したパケットに変更を加えずに送信するリプレイ攻撃と SOAP と呼ばれるプロトコルを用いて不正操作を行うためのメッセージを送信する攻撃を用いる．

4.3.1　リプレイ攻撃

4.1 節の実験においてペイロードの可読性を確認するために記録したパケットを使用し，単純なリプレイ攻撃で不正操作ができるか検証する．

尚，対象とした IoT 機器は 3.1 節で紹介した製品群のうち平文で通信が行われている①学習リモコン/ゲートウェイと⑦スマートプラグ 3 の 2 つとした．他の機器では，通信内容が暗号化されており，通信内容を復号しない限り不正操作を行うことができないため実験対象から外した．

具体的な実験手順を以下に示す．

(1) 4.1 節の実験で記録したパケットのうち，制御サーバから IoT 機器向けに送信した動作命令パケットを書き出す．
(2) 手順 (1) のパケットをホームネットワークに接続されたノートパソコンから IoT 機器に送信する．
(3) 送信後，IoT 機器が動作したか確認する．

上記の手順で不正操作を行ったが，IoT 機器が動作することはなく，不正操作に失敗した．よって同じ操作であっても，送信されるパケットのペイロード部は実行するごとに変化していると考えられる．

4.3.2　SOAP を用いた不正操作

SOAP(Simple Object Access Protocol) とは，コンピュータや DLNA に対応したテレビや Blu-ray プレーヤーなどの組込み機器上で動作するプログラム同士がネットワークを通じてメッセージを伝え合い，連携して動作するための通信規約の 1 つである．

また，メッセージ通信のために，ネットワークに接続された機器を検出するための技術として SSDP(Simple Service

表 3　DoS 攻撃の結果

製品名	攻撃元	方式	ICMP攻撃に対する効果 通信量	評価	攻撃中の詳しい状況	UDP攻撃に対する効果 通信量	評価	攻撃中の詳しい状況
①学習リモコン/ゲートウェイ	PC	有線	9405627	×	操作不可	8946538	×	操作不可
	PC	無線	1663659	×	操作不可	1559392	×	操作不可
	Raspberry Pi3	有線	1985134	×	操作不可	1948111	×	操作不可
	Raspberry Pi3	無線	268377	△	やや遅延するが，操作可能	340343	△	大幅に遅延した
②スマートロック用ハブ	PC	有線	9401179	×	操作不可	8955315	×	操作不可
	PC	無線	2255324	×	操作不可	1928017	×	操作不可
	Raspberry Pi3	有線	2120943	△	操作可能，アプリは失敗表記	1967619	×	操作不可
	Raspberry Pi3	無線	322973	△	操作可能，アプリは失敗表記	321522	×	操作不可
③AIスピーカー	PC	有線	9062481	×	操作不可，エラーの報告	9051916	×	操作不可，問題発生の報告
	PC	無線	1110248	△	音声が途中で途切れる	1330835	×	操作不可，エラーの報告
	Raspberry Pi3	有線	1968020	×	操作不可	1910079	×	操作不可
	Raspberry Pi3	無線	350185	△	やや遅延するが，操作可能	257859	○	問題なし
④IoT冷蔵庫	PC	有線	10420762	×	操作不可	11834036	×	操作不可
	PC	無線	2859147	×	操作不可	3519808	×	操作不可
	Raspberry Pi3	有線	1877915	×	操作不可	2188529	×	操作不可
	Raspberry Pi3	無線	257567	×	操作不可	401119	×	操作不可
⑤スマートプラグ1	PC	有線	9792347	×	操作不可	8999856	×	操作不可
	PC	無線	1375238	×	操作不可	2106351	×	操作不可
	Raspberry Pi3	有線	1955251	×	操作不可	1758879	×	操作不可
	Raspberry Pi3	無線	278313	×	操作不可	299554	×	操作不可
⑥スマートプラグ2	PC	有線	8860171	△	大幅に遅延した	8987228	×	操作不可
	PC	無線	1444735	△	やや遅延するが，操作可能	1793401	△	やや遅延するが，操作可能
	Raspberry Pi3	有線	1902777	△	操作可能，エラー表示あり	2015606	×	操作不可
	Raspberry Pi3	無線	233555	△	やや遅延するが，操作可能	370696	○	問題なし
⑦スマートプラグ3	PC	有線	8915854	×	操作不可	9234061	×	操作不可，機器の検出も不可
	PC	無線	2710458	×	操作不可	1513952	×	操作不可
	Raspberry Pi3	有線	2092590	×	操作可能	1947832	×	操作不可
	Raspberry Pi3	無線	157145	△	やや遅延するが，操作可能	244590	×	操作不可

Discovery Protocol) と呼ばれる技術がある．SSDP ではネットワークに接続されている機器を検出するため，M-SEARCH と呼ばれる探索リクエストに宛先 IP アドレス：239.255.250.250，ポート番号：1900 に設定したメッセージを UDP でマルチキャストする．加えて，ネットワークに接続されている他の機器に対し自身の存在を知らせる NOTIFY と呼ばれる広告リスクエストを送信することがある．

いずれの規格も UPnP と呼ばれるネットワークに接続するだけで組込み機器やパソコンなどの機器同士が相互に連携できるための仕組みである．

文献 [5] では，スマートプラグとネットワークカメラを SSDP で検出している．そこで，本実験でもホームネットワークに接続したノートパソコンから SSDP 検出を行い，接続されている IoT 機器が検出できるか調査する．

今回の実験では，ノートパソコンの Ubuntu 上で，UPnP ノードを一覧で表示するための GUPnP パッケージ [10] を用いて SSDP 検出を行った．

結果として 7 種類設置した IoT 機器のうち⑦スマートプラグ 3 のみ検出することができた．パッケージ内の GUPnP

名前	値
場所	http://192.168.11.24:49153/setup.xml
UDN	uuid:Socket-1_0-221626K01021B2
タイプ	urn:　:service:manufacture:1
ベースURL	http://192.168.11.24:49153/setup.xml
サービスID	urn:　:serviceId:manufacture1
サービスURL	http://192.168.11.24:49153/manufacture.xml
コントロールURL	http://192.168.11.24:49153/upnp/control/manufacture1
イベント購読URL	http://192.168.11.24:49153/upnp/event/manufacture1

図 5　SSDP 検出結果

ユニバーサルコントロールポイントで SSDP 検出を行った結果を図 5 に示す．スマートプラグから送信された広告リクエストが表示されていることが確認できる．複数存在する項目の中で，ベース URL に記載された URL にアクセスすることでそのデバイスの情報や制御方法などが記載されているデバイス記述ファイル（XML ファイル）を入手することができる．

また，ノートパソコンでコントロールポイントを実行中，スマートプラグの電源切替を Off にすると，イベント通知欄にスマートプラグのホスト名と状態変数 BinaryState が 0 になったイベントが表示された（図 6）．同様に，電源切

時間	デバイス	サービス	状態変数	値
11:53	[redacted]	urn:[redacted]:serviceId:basicevent1	BinaryState	0
11:53	[redacted]	urn:[redacted]:serviceId:basicevent1	BinaryState	1
11:53	[redacted]	urn:[redacted]:serviceId:basicevent1	BinaryState	0

図 6 イベント通知欄

替を On にすると状態変数 BinaryState の変数が 1 になったイベントが表示された．ゆえに，スマートプラグの状態変数 BinaryState 内の数値を変更することで，不正操作を行える可能性がある．

Github 上に，本実験に使用したスマートプラグを不正に操作するプログラムが公開されている [11]．プログラム内の処理を確認したところ，前述した BinaryState 内の数値を変更する処理が施されていた．このプログラムを実行したが，スマートプラグが動作することはなかった．しかし，別のプログラム言語で書かれた同機能のプログラムを実行したところ，不正操作を行うことができた．この不正操作を行うためには，同一の LAN からパケットを送信する必要があるが，コンピュータやスマートフォンを踏み台にして攻撃する手法やポートマッピングにより外部から直接攻撃する手法 [5] などにより不正操作を行うことができるため注意が必要である．

このスマートプラグでは，通信相手に対して認証を行わずにすべての操作命令を受け入れているため上述した不正操作が成功したと考えられる．不正操作の対策として，4.1 節でも述べた通信路の暗号化や工場出荷時の認証資格情報を強化することが挙げられる．

5. おわりに

本研究では，近年普及し始めているスマートホームにおける IoT 機器のサイバー攻撃耐性の評価を行うための 12 個の IoT 機器からなるホームネットワークを構築した．その後，構築したネットワーク内で，通信の盗聴，サイバー攻撃耐性，そして不正操作の検証を行った．通信路を盗聴した結果，多くの IoT 機器は SSL/TLS により暗号化されていたが，一部の機器は平文で通信されており，動作内容を把握することができた．擬似サイバー攻撃では，IoT 機器に対し ICMP/UDP flood を行った．その結果，操作ができないまたは完了するまで大幅な遅延が生じ，すべての IoT 機器において耐性がないことを確認した．また，最後に平文で通信を行う IoT 機器を対象に不正操作の検証を行った．その結果，1 つのスマートプラグのみ UPnP の 1 つである SOAP を用いてメッセージを送信することで不正操作を行うことができた．このような DoS 攻撃や不正操作から IoT 機器を防ぐために通信路の暗号化や異常な通信量を検知した際にフィルタリングを行う手法が考えられる．

今後の課題として以下の 2 点が挙げられる．

- ターゲットを複数にした場合の DoS 攻撃
  本論文では，1 台ずつ IoT 機器に対し DoS 攻撃を行い，送信パケット数が少ない Raspberry Pi3 でも IoT 機器をサービス不能状態にすることが確認できた．ゆえに，1 台のコンピュータからホームネットワーク上のすべての IoT 機器に対し一斉に DoS 攻撃を行い，すべての IoT 機器がサービス不能状態に陥るか確認する実験を行う．
- 別の手法による不正操作
  今回行った実験では平文で通信する 2 つの IoT 機器に対し，片方の機器のみ不正操作に成功した．もう一方の IoT 機器に対し不正操作を行うことができるかを確認するため，正規のクラウドサーバと同様の機能を有したダミーサーバを構築し，実験を行う．

参考文献

[1] 総務省：平成 30 年版情報通信白書 (online)，入手先 ⟨http://www.soumu.go.jp/johotsusintokei/whitepaper/h30.html⟩ (参照 2018-11-07).
[2] ASCII.jp：DDoS 攻撃でビルの暖房が使えなくなり凍死寸前!?(online)，入手先 ⟨http://ascii.jp/elem/000/001/405/1405563/⟩ (参照 2018-11-07).
[3] Insecam : World biggest online cameras directory(online)，入手先 ⟨http://www.insecam.org/⟩ (参照 2018-11-07).
[4] 楊志勇，熊佳，鉄穎，田宮和樹，西田慎，楊笛，藤田彬，吉岡克成，松本勉，ホームネットワークテストベッドによるサイバー攻撃の観測と検証，情報処理学会コンピュータセキュリティシンポジウム (CSS2017) 論文集, pp. 29-35, 2017.
[5] Vijay Sivaraman, Dominic Chan, Dylan Earl, Roksana Boreli, *Smart-Phones Attacking Smart-Homes*, WiSec'2016 Proceedings of the 9th ACM Conference on Security&Privacy in Wireless and Mobile Networks, pp.195-200, 2016.
[6] Wireshark(online)，入手先 ⟨https://wireshark.org/⟩ (参照 2018-11-19).
[7] 寺田真敏，*DoS/DDoS* 攻撃とは，情報処理，vol. 5，pp. 428-435，2013.
[8] 日立ソリューションズ 情報セキュリティブログ:ICMP Flood 攻撃とは (online)，入手先 ⟨https://securityblog.jp/words/icmp_flood.html⟩ (参照 2018-11-20).
[9] hping: Active Network Security Tool(online)，入手先 ⟨http://www.hping.org⟩ (参照 2018-11-19).
[10] Projects/GUPnP(online)，入手先 ⟨https://wiki.gnome.org/Projects/GUPnP⟩ (参照 2018-11-22).
[11] Isaac Kelly: Hacking the WeMo Switch(online)，入手先 ⟨https://github.com/issackelly/wemo⟩ (参照 2018-11-22).