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

楊 志勇[†1] 熊 佳[†1] 鉄 穎[†1] 田宮 和樹[†1] 西田 慎[†1] 楊 笛[†1]
藤田 彬[†2] 吉岡 克成[†2†3] 松本 勉[†2†3]

概要： スマート家電等の普及が進み，一般家庭ではネットワーク接続された IoT 機器が増加している．これらの機器の多くはリモート操作によりスマートフォンなどから便利に利用することができ，インターネット接続により多様なサービスが提供されるようになっている．このような利便性の反面，これらの機器へのサイバー攻撃が懸念されている．実際，ホームネットワークの入り口であるルータ機器へは毎日多数の攻撃が届いており，一部の脆弱なルータ機器がマルウェア感染や不正侵入の被害を受けている．また，スマート TV 等の一部の家庭用機器に感染するマルウェアも確認されている．しかし，ホームネットワークにおけるサイバー攻撃の調査，分析，研究は十分ではなく，その実態は明らかでない．そこで我々は，一般消費者の家庭環境を模擬した，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，今後想定される家庭内のサイバー攻撃について検討し，疑似的な攻撃をテストベッド内で試行することで機器への影響を検証する．さらに，これらの検証結果を基に，近年市場に現れ始めたホームネットワーク向けセキュリティ製品の効果を検証するための枠組みを検討する．

キーワード：ホームネットワークセキュリティ，IoT，サイバー攻撃，テストベッド

Observation and Analysis of Cyber attacks in Home Network Testbed

Zhiyong Yang[†1] Jia Xiong[†1] Ying Tie[†1] Kazuki Tamiya[†1] Shin Nishida[†1]
Di Yang[†1] Akira Fujita[†2] Katsunari Yoshioka[†2†3] Tsutomu Matsumoto[†2†3]

Abstract: Recently the number of connected devices is increasing rapidly. While these IoT devices receive large benefits from diverse services provided via Internet, there is a concern about cyber attacks against them. Home routers are constantly faced with number of suspicious accesses from the Internet and some of them are even compromised and infected by malware. Nevertheless, investigations and researches on cyber attacks in home networks are surprisingly few and unexplored. In this study, we develop a home network testbed with 16 connected devices and test proof-of-concept attacks that could potentially be conducted against these devices in home network and observe their effect. Finally, we discuss the framework to evaluate home network security products that have recently appeared in markets.

Keywords: Home network security, IoT, cyber attack, Testbed

1. はじめに

近年，通信機能を有するスマート家電の普及が進み一般家庭ではネットワーク接続された IoT 機器が増加している．これらの機器の多くはスマートフォン，タブレットといった端末から簡単に操作でき，インターネット接続によるクラウドとの連携により多様なサービスを享受できる．

このような利便性の反面，これらの機器へのサイバー攻撃が懸念されている．ホームネットワークの入り口であるルータ機器へは，毎日インターネット側から多数の攻撃が届いており，一部の脆弱なルータ機器はマルウェア感染や不正侵入の被害を受けている．例えば Telnet サービスを狙って感染を行うマルウェアである Mirai[1]とその亜種は 2016 年 9 月末にソースコードが公開されたこともあり[2]，大量の IoT 機器に感染した．さらに，マルウェアに感染した IoT 機器による サービス妨害攻撃により，多数のネットワークサービスが影響を受けた[3].

また，2016 年 6 月に確認された FLocker と言う Android 端末ロック型ランサムウェアの亜種が家庭内のスマートテレビを乗っ取り身代金を要求する事例も発生した[4]．しかし，このように IoT 機器へのサイバー攻撃の脅威が注目されているにも関わらず，家庭内の IoT 機器へのサイバー攻撃の実態は明らかになっていない．

そこで，家庭内サイバー攻撃の観測と検証を行うため，

†1 横浜国立大学大学院環境情報学府
Graduate School of Environment and Information Sciences, Yokohama National University
†2 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
†3 横浜国立大学大学院環境情報研究院
Faculty of Environment and Information Sciences, Yokohama National University

本研究では一般消費者の家庭環境を模擬した，16 種類のネットワーク接続可能な IoT 機器からなるホームネットワークテストベッドを構築する．そして当該テストベッドで，今後予想される様々なサイバー攻撃を試行し，設置した機器に与える影響を調査する．さらに，これらの検証結果を基に，近年市場に現れ始めたホームネットワーク向けセキュリティ製品の効果を検証するための枠組みを検討する．

2. 関連研究

IoT 機器の大量マルウェア感染の観測・分析

IoT 機器を狙うマルウェアの観測と分析について，脆弱な IoT 機器を模擬するハニーポットを運用し，大量のマルウェアを収集する先行研究として，文献[5]，[6]，[7]が挙げられる．IoT 機器のマルウェアをハニーポットにより収集して，攻撃挙動の詳細や傾向を動的に解析する研究には文献[8]が挙げられる．最近では，Mirai と呼ばれるマルウェアに感染した IoT 機器が大規模な DoS 攻撃を行った事例が報告されている．当該マルウェアの詳しい分析を行った文献[9]では，ハニーポットを利用し，Mirai の挙動を観測すること及び Mirai に感染した IoT 機器の種類を分析することにより，Mirai の変種と危険性を予測している．

IoT セキュリティテストベッド

日本国内の重要インフラをサイバー攻撃から守り，制御システムのセキュリティを確保するため，各研究機関が様々な IoT セキュリティテストベッドを提案し，構築している．例えば，CSSC（Control System Security Center， 制御システムセキュリティセンター） [10]におけるテストベッド施設（略称：CSS-Base6）では，9 つのプラント（化学，ビル，工場，電力，ガス，広域連携など）を模擬して，重要なインフラと工場の環境を再現している．また，計算機クラスタで構成される StarBED 型テストベッド[11] [12]でハードウェアエミュレータを用いて大規模な IoT 環境を構築し，IoT セキュリティ実証実験を行っている．

それらのテストベッドにおいて，制御システムに模擬サイバー攻撃を行い，当該システムの堅牢性を検証するとともに，インシデントが起きた際の影響の評価や制御システムのセキュリティ強化技術の開発等を行っている．

上記のテストベッドではこれまでに，重要インフラ，工場，広域連携システム等に係る研究[13]がある一方で，ホームネットワークのテストベッドに係る研究は，総務省における試み[14]が挙げられる他に事例が少なく，総合的な検証が十分に進んでいないものと考えられる．本研究ではホームネットワークのテストベッドを構築する手法を検討し，想定するサイバー攻撃の調査及び分析を行う．

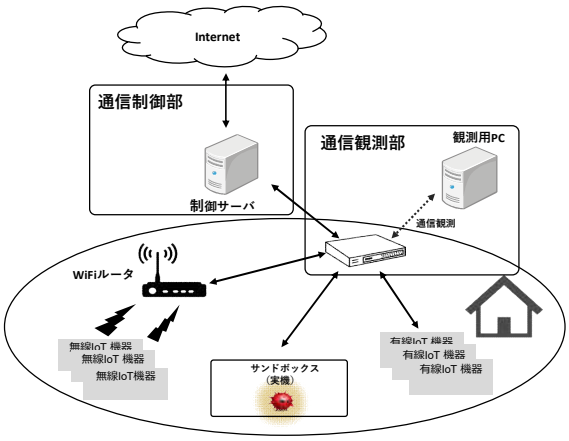

図 1 テストベッドの構成図

3. ホームネットワークテストベッド

3.1 概要

前章で示したように，現在ホームネットワークにおけるサイバー攻撃の調査及び分析は十分に行われているといえず，その実態は明らかでない． IoT 機器のセキュリティに関するこれまでの研究は，特定の IoT 機器を模擬し，インターネットから届く攻撃を観測している．家庭用ルータも攻撃対象となっている一方で，これらのルータが侵入を受けた後，ルータに接続された家庭内のネットワークに対して行われる可能性がある攻撃については観測対象としていない．

そこで本研究では，16 種類の IoT 機器からなる一般消費者の家庭環境を模擬したテストベッドを構築し，ホームネットワーク内の通信やインターネットから当該テストベッドに届く攻撃を観測する．これに加えて，家庭内ネットワークで想定される攻撃を模擬し，これらの攻撃がテストベッド内の IoT 機器やネットワークに与える影響を観測する．さらに，これらの実験を通じて，ホームネットワーク向けセキュリティ製品の効果を検証し，これらの製品が満たすべき要件を検討する．

3.2 テストベッドの構成

ホームネットワークテストベッドの構成について述べる．本テストベッドは下記を行う目的で構成する．

- ホームネットワークテストベッド内の通信の分析
- インターネットからテストベッドに届く攻撃の観測
- 今後想定される家庭内のサイバー攻撃の検討
- テストベッド内での疑似的な攻撃の試行及び同攻撃のテストベッド内機器への影響の検証

図 1 にテストベッドの構成図を示す．テストベッドは制御サーバ，通信観測部および家庭内で使用される多様な IoT 機器群で構成する．制御サーバはインターネットとホームネットワークの境界に設置し，インターネットからホ

表 1 テストベッドのスペック

	説明	概要
制御サーバ	ホームネットワーク内の通信を制御する．また，想定された攻撃を行う際，外部に影響を与えないよう，通信ルールを設定する．	Intel(R) Core(TM) i7-7700 CPU@ 3.60GHz, 2 ports Ethernet interfaces, Ubuntu 16.04
通信観測部	外部との通信，またはホームネットワーク内の通信を観測する．	12 ethernet ports switch with port mirroring
サンドボックス（実機）	マルウェアを機器内部で実行し感染させ，家庭内の機器または外部に攻撃を行う．	Wi-Fi ストレージ /ポケット Wi-Fi, MIPSEL

ームネットワーク内への通信及びその逆方向の通信は当該制御サーバを経由する．制御サーバ内の通信制御部で，ホームネットワーク内のサイバー模擬攻撃がホームネットワーク外に流出しないように制御する．テストベッドの通信を全体的に観測する目的で，通信観測部の一端を制御サーバに接続し，Wi-Fi ルータの WAN ポートを通信観測部に接続する．この通信観測部はリピータハブ（ポートミラーリング機能付スイッチ）と観測用 PC で構成されており，ホームネットワーク内及び外部との通信を観測できる．表 1 にテストベッドの詳細なスペックを示す．

(1) ホームネットワーク内の通信観測

ホームネットワーク内の IoT 機器間及び IoT 機器と外部のリアルタイムの通信の流れ及び通信情報を観測する．具体的には，有線接続の IoT 機器間の通信パケット， IoT 機器の管理用アプリがインストールされたスマホやタブレットと有線の IoT 機器の間での通信パケットを通信観測部において観測することで，ホームネットワーク内の通信トラフィックを監視する．

なお，本研究のルーティング設定上，Wi-Fi ルータを経由した無線接続機器間の TCP/IP 通信は，通信観測部を経由しないため通信パケットを観測できない．

(2) インターネットからの通信観測

ホームネットワーク内の IoT 機器はインターネットを介して外部ホストと通信可能である．ホームネットワーク内の IoT 機器と外部の間の通信についても，通信観測部で通信トラフィックを監視する．また，テストベッド内にハニーポット及びホームネットワーク向けセキュリティ製品を設置し，インターネットからホームネットワークへの攻撃を引き込み，ホームネットワークセキュリティ製品の反応を観察及び評価する．

(3) テストベッド内で疑似的な攻撃を行う

ホームネットワーク内に実機サンドボックスを設置し，ハニーポットで収集された IoT マルウェア検体をサンドボックス内で動作させる．その上で，C&C サーバからの応答を蓄積して任意のタイミングでマルウェアに対し攻撃命令を送信できる機能を持つダミーC&C サーバを作成する．ダミーC&C サーバからマルウェアにコマンドを送って攻撃を行い，通信観測部での観測情報から，コマンド実行時の攻撃の成否を判断する．

表 2 観測及び分析対象とする家庭内 IoT 機器の一覧

製品名	プロトコル	機能説明
学習リモコン	TCP	エアコンや TV などの家電のリモコンを登録することで，アプリから様々な家電の操作が可能となる．
ロボット掃除機	MQTT[15]（TCP）	アプリを利用して清掃命令等のリモートコントロールが可能．
スマート照明	HTTP	アプリを利用して照明の ON・OFF やライトの色の変更が可能．
スマート電源プラグ	UDP	コンセントに接続して使用する．アプリで電力使用状況の確認や電源を ON・OFF することが可能．
スマートコーヒー機	TCP	家の中でも，外出先からでもコーヒーを淹れることが可能．
プリンタ	TCP	アプリから写真やファイルのプリント操作が可能．
NAS	HTTP	インターネットに接続して使用するファイルサーバである．
IP カメラ	UDP/TCP	アプリを利用して，外出先からでも映像を確認できる．
スマート TV	TCP	インターネットに接続し，インターネット上の映像コンテンツを視聴できる．
空気清浄機	TCP	アプリで，機器の電源の ON・OFF 及び運転モードの切り替え操作が可能．

3.3 テストベッド内の IoT 機器

テストベッドのホームネットワークに，計 16 種類（学習リモコン，ロボット掃除機，スマート照明，スマート電源プラグ，スマートコーヒー機，プリンタ，NAS，IP カメラ，スマート TV，空気清浄機，据置型ゲーム機，携帯ゲーム機，タブレット，電子書籍リーダ，BD レコーダ，セットトップボックス）の IoT 機器を接続した．今回はこのうち，表 2 に示す 10 種類の機器を観測及び分析の対象とする．

4. テストベッド内での疑似サイバー攻撃の試行と影響の分析

一般家庭内において，各機器は有線及び無線の形で家庭 Wi-Fi ルータに接続してインターネットにアクセスすることになる．ホームネットワークの入り口であるルータ機器へは実際に毎日多数の攻撃が届いており，一部の脆弱なルータ機器がマルウェア感染や不正侵入の被害を受けている．Wi-Fi ルータが感染し攻撃者に侵入された場合，全ホームネットワークが脅威にさらされる恐れがある．具体的には，攻撃者が感染した Wi-Fi ルータを利用してホームネットワーク内の通信を盗聴することで，家庭内に存在している IoT 機器の情報を把握し，これらの機器を狙うサイバー攻撃を実施することが考えられる．

今後起きることが想定される家庭内のサイバー攻撃について，その現実性や影響度を調査するため，3 章で説明

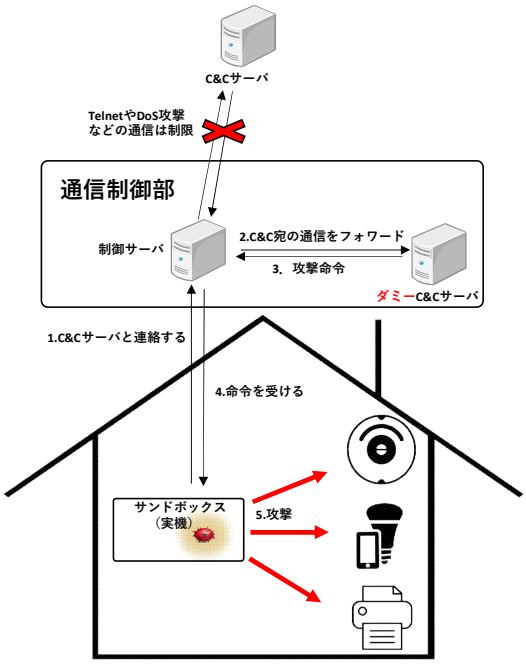

図 2 DoS 攻撃実験の実験環境の概要図

したホームネットワークテストベッド内でいくつかの疑似サイバー攻撃を行った結果を報告する．

4.1 家庭内サービス妨害攻撃

4.1.1 実験概要

家庭内の機器を狙う攻撃の一つとしてサービス妨害攻撃（Denial of Service Attack，DoS 攻撃）が想定される．DoS 攻撃とは，コンピュータや通信機器などに対して大量のデータや不正なデータを送りつけ，標的となる機器やネットワークなどを機能不全に陥らせる攻撃である．近年マルウェアに感染した IoT 機器を踏み台にした DoS 攻撃が確認されており大きな問題となっている．そこで，家庭内の IoT 機器に対して DoS 攻撃が行われた場合の影響を調査するため，テストベッド内の IoT 機器に対して実際の IoT マルウェアから DoS 攻撃を行い，各機器の反応を調査した．観測・分析対象とする 10 種の IoT 機器のうち，3 種の機器はクラウドを経由してクライアントアプリからの通信を受信する．この際，受信のための待受ポートは固定されたものではないため，ターゲットポートが定まらない．このことからこれらの 3 種の機器については，当該実験の対象から除外した．

4.1.2 実験手順

テストベッド内の IoT 機器に対する DoS 攻撃実験の手順について述べる．同実験の実験環境を図 2 に示す．

本実験では，脆弱性を持つ Wi-Fi ストレージ（市場価格 3,000 円程度）の実機を IoT マルウェア（MD5 ハッシュ値: b66d2425ea49f73c9d09f8999c26c93c, BitDefender による検知名: Gen:Variant.Backdoor.Linux.Gafgyt.1）に感染させ，攻撃を行なった．具体的な実験手順を以下に示す．

表 3 感染された IoT 実機を用いる DoS 攻撃の効果

製品名	DoS 攻撃種類/攻撃通信量	攻撃耐性	攻撃後自動的に回復可能か否か/回復時間
ロボット掃除機	SYN flood 392K Byte/s	×	自動的に回復不可 Reboot が必要
スマート照明	SYN flood 307K Byte/s	×	自動的に回復可能 15 s
学習リモコン	SYN flood 357K Byte/s	△	自動的に回復可能 28 s
NAS	SYN flood 435K Byte/s	○	
プリンター	SYN flood 225K Byte/s	○	
スマートコーヒー機	SYN flood 342K Byte/s	×	自動的に回復可能 23 s
スマート電源プラグ	UDP flood 13M Byte/s	×	自動的に回復可能 18 s

(1) 事前に入手したマルウェア検体に対応するダミー C&C サーバを作成し，制御サーバにフォワーディングの設定を行う．
(2) マルウェアバイナリファイルを Wi-Fi ストレージ機器に転送し実行する．
(3) 観測サーバを利用し，ホームネットワーク内の通信を記録する．
(4) ダミー C&C サーバから攻撃の目標 IP アドレス，攻撃ポートと攻撃持続時間（5 分間）を指定して，攻撃命令を送信する．
(5) DoS 攻撃開始前後の各機器の動作を確認する．
(6) 解析環境をクリーンアップし，通信の記録を終了する．

4.1.3 実験結果

実験の結果を表 3 に示す．「攻撃通信量」は上記の DoS 攻撃手法の実施により，感染機器から IoT 機器へ送信した毎秒あたりの通信量である．

「攻撃耐性」の項目中の「 ○ 」は攻撃を実施している際でも，機器を操作した際に機器が正常に動作したことを意味する．「 × 」は機器が操作に対し正常に動作しなかったことを意味する．また，「 △ 」は機器の操作に対し動作するまで大幅な遅延（20 秒以上）があったことを意味する．

以上の結果から，今回のテストベッド内で IoT マルウェアの DoS 攻撃によりいくつかの IoT 製品の動作が妨害されうることが実証された．次に，比較のため，制御サーバで専用の DoS 攻撃ツールである hping3[16]を用いて DoS 攻撃を実施し，攻撃通信量が多い場合の IoT 製品への影響の程度を確認した．結果を表 4 に示す．

表 4　hping3 を用いた DoS 攻撃の効果

製品名	DoS 攻撃種類/攻撃通信量	攻撃耐性	攻撃後自動的に回復可能か否か/回復時間
ロボット掃除機	SYN flood 27M Byte/s	×	自動的に回復不可 Reboot 必要
スマート照明		×	自動的に回復可能 25 s
学習リモコン		×	自動的に回復可能 23 s
NAS		×	自動的に回復可能 7 s
プリンター		×	自動的に回復可能 4 s
スマートコーヒー機		×	自動的に回復可能 20 s
スマート電源プラグ	UDP flood 57M Byte/s	×	自動的に回復可能 67 s

4.1.4 考察

以上の実験結果により，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関わらず，半分以上の IoT 製品が動作しなくなることが確認された．また，攻撃通信量が多い攻撃では，今回の実験対象すべての IoT 製品が動作しなくなることを確認した． 攻撃終了後，ほとんどの IoT 製品は 1 分以内に正常な動作状態に戻ったが，機器を再起動するまで正常な状態に戻らない製品も存在した．このことから，実際に攻撃者が家庭内で IoT 機器を狙う DoS 攻撃を実施すれば，機器の動作が妨害されることがわかった．なお，家庭内の IoT 機器の動作を妨害することは攻撃者の利益に結び付かないとも考えられるが，一方で，感染した IoT 機器を故障させるマルウェア[17]も現れていることから注意が必要である．

対策としてゲートウェイやホームネットワークセキュリティ製品により DoS 攻撃のような異常に大量な通信を検知し，フィルタリングする方法が考えられる．

4.2 家庭内機器の不正操作

4.2.1 実験概要

ホームネットワーク内でスマートフォンアプリ等を操作して IoT 製品を使用する場合，まずアプリからの動作命令が家庭内の Wi-Fi ルータを経由して IoT 機器に届けられ，機器が命令にしたがって動作した後，その実施結果を同じ経路で返信するという処理が実施される．ここで，機器操作のための通信を仲介するルータを乗っ取った攻撃者による，機器不正操作攻撃を想定する．

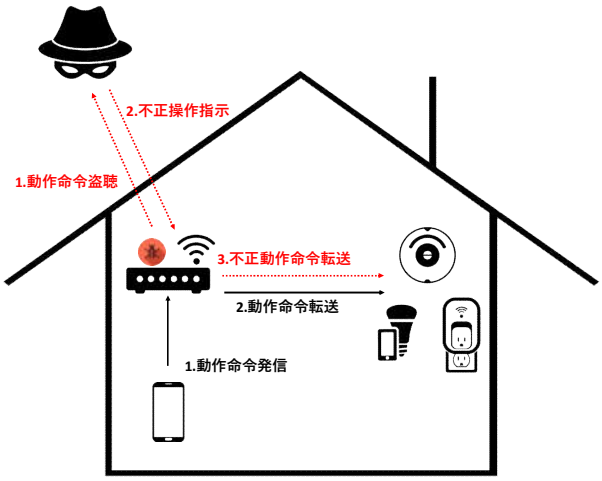

図 3 盗聴による家庭内機器の不正操作

図 3 で仮定した通り，脆弱性のある Wi-Fi ルータが攻撃者に侵入されてマルウェアに感染した状況では，ホームネットワーク内での通信が攻撃者に盗聴されていると考えられる．この時，攻撃者は通信を盗聴しながら，特定の IoT 機器の動作命令の通信パケットを記録し，攻撃者が望むタイミングで当該パケットを再現し操作対象 IoT 機器に送信することで，不正に機器の操作を行うことが想定される．

以上の不正操作攻撃の実現可能性を検証するため，以下の IoT 製品を不正操作の実験対象とした．

- TCP 通信を行うスマートリモコン
- TCP 通信を行うロボット掃除機
- UDP 通信を行うスマート電源プラグ

具体的には以下に示す二つの手法を用いて実験を行う．

(1) まず，IoT 製品の各動作機能毎に，スマートフォンでアプリを操作しながら，送信したパケットを観測サーバでキャプチャし記録する．

(2) (1)で得られた各動作機能に該当する通信パケットのペイロード部分を抽出する．その上で，同じホームネットワークにある疑似攻撃ホストから，抽出したペイロードが挿入された操作通信を IoT 製品に送信する．この操作により同一の動作機能を再現されるかどうかを確認する．

4.2.2 実験結果

通信解析と不正操作実験の結果を表 5 に示す．平文で通信するスマートリモコンに対しては不正操作による全ての操作が成功した．暗号通信を行うロボット掃除機に対しては反応がなく，不正操作に失敗した．一方で，スマート電源プラグでは操作に成功した．

表 5 通信解析と不正操作の結果

製品名	アプリケーション層プロトコル	ペイロードの可読性	操作機能	不正操作の結果
学習リモコン	Raw TCP	あり (ASCII コードで記載)	TV 電源 ON	成功
			TV 電源 OFF	成功
			TV 音量調整	成功
			TV チャンネル調整	成功
ロボット掃除機	MQTT	なし (SSL で暗号化)	掃除開始	失敗
			掃除一時中止	失敗
			掃除停止	失敗
スマート電源プラグ	Unknown (UDP)	なし (バイナリデータ)	電源 ON	成功
			電源 OFF	成功

4.2.3 考察

前述の実験では，三つの IoT 製品中のうちスマートリモコン及び電源プラグに対して不正操作に成功した．

スマートリモコンで使うプロトコルは平文の TCP であることから，同じホームネットワークにある疑似攻撃ホストで Telnet クライアントを用いた操作を試した．結果として，図 4 に示す通り，得られた平文の動作命令を用いてユーザ名とパスワード無しでの操作に成功した．

```
root@[redacted]:/ # telnet 192.168.10.109  51013
Trying 192.168.10.109...
Connected to 192.168.10.109.
Escape character is '^]'.
*is;1
is;ok
```

図 4 Telnet クライアントを用いた操作結果

電源プラグでは通信内容の可読性はないが，アプリから送信された命令通信をそのまま送信することで，電源プラグを操作することが可能であった．

即ち，今回の実験でスマートリモコンと電源プラグに対する不正操作が成功した原因は，操作を行う側の認証機能がないためと考えられる．この解析結果はしかるべき機関に情報提供を行う予定である．

一方で，アプリとロボット掃除機のコネクションが成立する際の流れを観測すると，SSL 接続を確立するための「SSL ハンドシェイク」[18]と呼ばれる，公開鍵及び秘密鍵，セッション鍵の鍵交換の過程が確認された．つまり，ロボット掃除機が使う MQTT プロトコル上で，TLS/SSL が使用され暗号化されていた．このことから，他の二つの機器よりセキュリティが高く，単純なリプレイ攻撃を防ぐことが可能であることが確認された．

今回発見した不正操作の原因は主に二つある．一つは通信内容が暗号化されていない．もう一つは，操作する際に認証を行なっていないことである．

5. ホームネットワークセキュリティ製品の評価フレームワーク

5.1 ホームネットワークセキュリティ製品

近年ホームネットワーク向けセキュリティ製品（以下，ホームネットワークセキュリティ製品）が消費者の注目を集めている．ホームネットワークセキュリティ製品[19]は家庭のネットワークに接続する機器を外部からの攻撃や有害サイトへのアクセスから防御する．これらの製品は主に以下のような機能によって，ホームネットワークに繋がる機器を保護する．

- **侵入防御機能**
  ホームネットワーク内の通信データを監視し，家庭内の機器に存在する脆弱性を突いた攻撃が行われた場合に，攻撃を判定して遮断する．
- **不正サイトへのアクセスブロック機能**
  ウィルス感染やフィッシング詐欺などの恐れのあるウェブサイトへのアクセスをブロックする．特に，ゲーム機のような，ブラウザを搭載しているがセキュリティソフトウェアがインストールされていない機器に当該機能が必要である．
- **ホームネットワーク接続機器の脆弱性検知機能**
  ホームネットワーク内に接続されている機器を検知し一覧で表示する．また，接続されている機器をスキャンし，脆弱性があるかを検知する．

これらの製品は，家庭の Wi-Fi ルータに接続したり，直接 Wi-Fi ルータとして使用し，スマホまたはタブレットに管理用アプリをインストールする必要がある．

5.2 評価項目

ホームネットワークセキュリティ製品は前節に示したセキュリティ機能によって，家庭内の機器を保護する．その効果を検証するため，テストベッド内に脆弱性を持つ機器

表 6 セキュリティ製品の評価項目

前提	種類	項目	実施方法
内→内	Scan/ exploit	Port scan	Nmap
		脆弱性 scan/ SQLinjection	metasploit
		Remote access (ssh,telnet)	script
	DoS	DoS	Malware/tool
内→外	Scan/ exploit	Port scan	Nmap
		脆弱性 scan/ SQLinjection	metasploit
		Remote access (ssh,telnet)	script
	DoS	Malware/tool	Malware/tool
	URL Block	URL Block	Black list top1000
外→内	Scan/ exploit	Port scan	Nmap
		脆弱性 scan/ SQLinjection	metasploit
		Remote access (ssh,telnet)	script
	DoS	DoS	Malware/tool
その他	脆弱性診断	脆弱性診断	脆弱な機器を設置

を設置し，セキュリティ検知情報を調査する．また，想定される家庭内のサイバー攻撃について検討し，疑似的な攻撃をテストベッド内で試行することで効果を検証する．さらに，インターネットからの攻撃を受けた際，セキュリティ製品が攻撃を検知，遮断することができるかどうかを調査する．そこで，製品のセキュリティ機能について，評価の枠組みを検討した．以下に評価の枠組みを説明する．

- **ホームネットワーク内の攻撃の検知・遮断**

  ホームネットワーク内において様々なシナリオで家庭内の機器に疑似的に攻撃を行い,セキュリティ製品が検知・遮断できるかを調査する．

- **ホームネットワークから外部への攻撃の検知・遮断**

  感染された家庭内の機器,または攻撃ツールで外部への攻撃を行い，セキュリティ製品の検知・遮断状況を調査する．

- **外部からホームネットワークへの攻撃の検知・遮断**

  インターネットからの実攻撃及び制御サーバからのマルウェアや攻撃ツールを用いた家庭内の機器に対する攻撃をセキュリティ製品が検知･遮断できるかを調査する．

- **その他**

  セキリュティ製品が家庭内の機器の脆弱性を能動的に検知するかを調査する．

詳細な評価項目と実施方法を表 6 に示す．

5.3 評価例

我々は現在市販されているホームネットワークセキュリティ製品 A と B を選択し，テストベッドにより，表 6 の一部分の評価項目の実験を行い，製品 A と B の効果を検証した．製品 A は Wi-Fi ルータに接続して使用する．製品 B は Wi-Fi ルータに接続する，あるいは直接 Wi-Fi ルータとして使用することが可能である．本研究では製品 A と B どちらにおいても Wi-Fi ルータに接続するモードを選択した．以下，行った評価実験と結果を説明する．

表 7 セキュリティ製品の評価実験と各製品の反応

大項目	項目	実施方法	製品 A 反応	製品 B 反応
内→内	スキャン	Nmap	Wi-Fi ルータとセキュリティ製品本体に対する全ポートスキャンを検知・遮断した．	反応なし
内→内	DoS	Malware/tool	反応なし	反応なし
内→外	スキャン	Malware	反応なし	反応なし
その他	脆弱性診断	脆弱な機器を設置	IoT 機器のベーシック認証の Web UI の弱い ID とパスワードを検知した．	反応なし

(1) ホームネットワーク内部間のポートスキャン

疑似攻撃ホストから，ポートスキャンツール nmap[20]を利用し，家庭内の IoT 機器及び Wi-Fi ルータとセキュリティ製品に全ポートスキャンを行った．

(2) ホームネットワーク内部間 DoS 攻撃

4 章の家庭内サービス妨害攻撃実験を行い，Wi-Fi ルータに接続されたセキュリティ製品がこの大量のトラフィックに対して，検知・遮断できるかを調査した．

(3) ホームネットワーク内部から外へのスキャン

実機サンドボックス内でマルウェアを実行し，ダミー C&C サーバから命令を送ることで，大量のグローバル IP の 23 番ポートをスキャンした．ただし，制御サーバでスキャンのトラフィックを止め外部に影響が出ないように設定した．その上で，セキュリティ製品がこのスキャンのトラフィックを検知・遮断できるかを調査した．

(4) セキュリティ製品を用いてホームネットワーク内の IoT 機器診断

ホームネットワーク内に設置した機器のうち Web UI を持ち，かつ認証方法にベーシック認証[21]とフォーム認証[22]の二つがある機器に対して，弱いログイン ID とパスワード（admin/admin）を設定した．その上で，セキュリティ製品を Wi-Fi ルータに接続し，この弱い ID/パスワード設定の脆弱性を認識するかを調査した．

5.4 評価結果

(1)～(4)の評価実験におけるセキュリティ製品の反応を表 7 に示す． 以下に，評価実験別に評価結果を説明する．

(1) ホームネットワーク内部間のポートスキャンの結果

Wi-Fi ルータとホームネットワークセキュリティ製品本体に全ポートスキャンを行ったところ，製品 A は当該操作を検知・遮断した．しかし，Wi-Fi ルータと製品本体以外の IoT 機器に対するスキャンは検知しなかった．

(2) ホームネットワーク内部間 DoS 攻撃及び (3) ホームネットワーク内部から外へのスキャンの結果

(2)と(3)の攻撃実験を行ったところ，当該操作に対して，

製品 A と B は共に攻撃を検知・遮断しなかった．

(4) セキュリティ製品を用いてホームネットワーク内の IoT 機器脆弱性診断

製品 A の脆弱性診断の機能を用いて，IoT 機器の Web UI の ID とパスワードの脆弱性をチェックしたが，認証方法がベーシック認証のみである Web UI を持つ機器に対して脆弱性を検知した．製品 B はこの IoT 機器の脆弱性を検知しなかった．

(1)，(2)，(3)の評価実験により，製品 A と B 共にホームネットワーク内部間の攻撃に対しては検知能力が十分ではないといえる．

6. まとめと今後の課題

本研究では，一般消費者の家庭環境を模擬した 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，疑似的な攻撃をテストベッド内で試行することで機器への影響を検証した．テストベッド内での疑似サイバー攻撃の結果，家庭内の多くの IoT 機器が影響を受けることがわかった．また，ホームネットワーク向けセキュリティ製品において評価の枠組みを検討し，その一部分について評価実験を行った．実験の結果から，今回検証に用いたセキュリティ製品ではホームネットワーク内部間の通信の検査が十分とはいえないと考えられる．

今後は，外部からホームルータを経由して届く攻撃の実態把握，UPnP 等によりホームルータのポートフォワーディング設定を自動的に行うことで外部からの攻撃を直接家庭内に引き入れてしまう機器の影響の分析，IoT 機器におけるランサムウェアによる攻撃の可能性を検討すると共にホームネットワークセキュリティ製品の効果をより正確に把握するため，評価項目を補足し，評価実験を続けたい．

7. 謝辞

本研究成果の一部は，BB ソフトサービス株式会社との共同研究により得られた．

また，本研究の一部は文部科学省国立大学改革強化推進事業の支援を受けて行われた．

8. 参考文献

[1] “Mirai: New wave of IoT botnet attacks hits Germany”. http://www.symantec.com/connect/blogs/mirai-new-wave-iot-botnet-attacks-hits-germany, (参照 2017-08-04).

[2] “Source Code for IoT Botnet ‘ Mirai’ Released”. https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, (参照 2017-08-04).

[3] “DDoS on Dyn Impacts Twitter, Spotify, Reddit”, https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitterspotify-reddit/, (参照 2017-08-04).

[4] “モバイル向けランサムウェア「FLocker」，スマートテレビにも影響”. http://blog.trendmicro.co.jp/archives/13453, (参照 2017-08-08).

[5] Yin Minn Pa Pa, S. Suzuki, K. Yoshioka, T.Matsumoto, T.Kasama, C.Rossow .. IoTPOT:Analaysing the Rise of IoT Compromises. USENIX/WOOT’15, 2015.

[6] 鈴木将吾，インミンパパ，江澤優太，鉄穎，中山颯，吉岡克成，松本勉．組込み機器への攻撃を観測するハニーポット IoTPOT の機能拡張．電子情報通信学会 信学 技報, vol.115, no.488, ICSS2015-47, pp.1-6, 2016.

[7] 中山颯，鉄穎，楊笛，田宮和樹，吉岡克成，松本勉. IoT 機器への Telnet を用いたサイバー攻撃の分析．情報処理学会コンピュータセキュリティシンポジウム 2016，セッション 3E1, 2016.

[8] 楊笛，保泉拓哉，中山颯，鉄穎，吉岡克成，松本勉. IoT マルウェアによる DDoS 攻撃の動的解析による観測と分析．暗号と情報セキュリティシンポジウム 2017，セッション 3E1-3, 2017.

[9] April, Manos Antonakakis Tim, et al.. Understanding the Mirai Botnet. USENIX Security Symposium, 2017.

[10] “制御システムセキュリティの脅威と対策の動向および CSSC の研究概要について”. http://www.css-center.or.jp/pdf/about_CSSC.pdf, (参照 2017-08-04).

[11] 宮地利幸，中田潤也，知念賢一，三輪信介，岡田崇，三角真，篠田陽一. StarBED: 大規模ネットワーク実証環境．情報処理 2008, 49(1), 57-70.

[12] 岩橋紘司，井上朋哉，篠田陽一． Internet of Things を対象とした大規模実証実験環境構築に関する研究．マルチメディア，分散協調とモバイルシンポジウム 2014 論文集 2014, 1258-1263, 2014-07-02.

[13] 目黒有輝，村瀬一郎，細川嵩．スマートメーターシステムのセキュリティ確保に向けた CSSC の取り組み．自動制御連合講演会講演論文集 第 59 回自動制御連合講演会, 2016.

[14] “スマートホームを想定した連携 IoT 機器のセキュリティ検証用テストベッドの構築”, http://www.soumu.go.jp/main_content/000423702.pdf, 3p, (参照 2016-06-28)

[15] “MQTT - A lightweight messaging protocol for small sensors and mobile devices”, http://mqtt.org/, (参照 2017-03-15)

[16] “Hping - Active Network Security Tool”, www.hping.org, (参照 2017-07-23)

[17] “Brickerbot botnet, the thingbot that permanently destroys IoT devices”, http://securityaffairs.co/wordpress/57839/malware/brickerbot-botnet-iot.html, (参照 2017-08-04).

[18] Wagner, David, and Bruce Schneier. Analysis of the SSL 3.0 protocol , The Second USENIX Workshop on Electronic Commerce Proceedings. Vol. 1. No. 1. 1996.

[19] “新たなサーバー攻撃から家を守るための’ホームネットワークセキュリティ’とは〜機器ごとではなく丸ごと保護”, http://internet.watch.impress.co.jp/docs/special/1069738.html, (参照 2016-08-20).

[20] “nmap”, https://nmap.org/, (参照 2016-08-20).

[21] “Basic 認証(基本認証)でアクセス制限をかける方法”, https://allabout.co.jp/gm/gc/23780/, (参照 2016-08-20).

[22] “フォーム認証の概要”, https://msdn.microsoft.com/ja-jp/library/7t6b43z4(v=vs.100).aspx, (参照 2017-04-17)