情報処理学会論文誌 Vol.61 No.3 567–580 (Mar. 2020)

実攻撃の観測と疑似攻撃の試行に基づくホームネットワークセキュリティの検証

藤田 彬[1,a)] 楊 志勇[2] 熊 佳[2] 鉄 穎[2] 楊 笛[2] 江澤 優太[2]
中山 颯[2] 田宮 和樹[2] 西田 慎[2] 吉岡 克成[1,3] 松本 勉[1,3]

受付日 2019年6月16日, 採録日 2019年11月29日

概要：近年，ホームネットワーク内のIoT機器を狙ったサイバー攻撃の脅威が顕在化している．本研究では，一般消費者の家庭のネットワーク環境を模擬したテストベッドを構築し，サイバー攻撃の観測および当該攻撃がホームネットワークに及ぼす影響の分析を行う．多くの家庭で一般的に使用されていることが見込まれるIoT機器複数台とWi-Fiルータを用意し，インターネットに接続されたネットワークを構成する．当該ネットワークの通信トラフィックを観測可能な機器を付設したうえで，疑似的に攻撃を発生させる．すでに存在が確認されている攻撃手法にくわえ，今後出現しうる攻撃手法も想定し，それらの攻撃がホームネットワークに与える影響を調査する．また，すでに流通しているホームネットワーク向けのセキュリティ製品がそれらの攻撃を検知できるか検証する．調査の結果，想定した攻撃手法の多くが実際にホームネットワークに影響を与えうることが分かった．また，検証対象としたセキュリティ製品が，本研究で想定した攻撃の大半を検知できず，検知可能な対象がポートスキャン等の一部の攻撃に限られることが分かった．

キーワード：ホームネットワーク，IoT，テストベッド

Examination of Home Network Security Considering Real and Proof-of-concept Attacks

Akira Fujita[1,a)] Zhiyong Yang[2] Jia Xiong[2] Ying Tie[2]
Di Yang[2] Yuta Ezawa[2] Sou Nakayama[2] Kazuki Tamiya[2]
Shin Nishida[2] Katsunari Yoshioka[1,3] Tsutomu Matsumoto[1,3]

Received: June 16, 2019, Accepted: November 29, 2019

Abstract: Recently, the threat of cyber attacks which is targeting IoT devices in a home network reveals. In this research, we aim to monitor the attacks and to analyze how the attacks affect to home networks, by a testbed that simulates the home network environment of a general consumer. We prepared multiple IoT devices and a Wi-Fi router that is expected to be commonly used in many homes, configured a network connected to the Internet, deployed the devices that can observe communication traffic in the network, and generated pseudo attacks. We investigated the impact of attacks that have already been confirmed and also that may emerge in the future. We also verified whether security products for home networks, which is commercially available can detect those attacks or can not. As a result of the investigation, it revealed that most of the assumed attack methods can actually affect the home network. Also, it was found that the security products for home network targeted for verification cannot detect most of the attacks assumed in our research, and the targets that can be detected are limited to some attacks such as port scan.

Keywords: home network, Internet of Thing, testbed

[1] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 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, Yokohama, Kanagawa 240–8501, Japan
[3] 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[a)] fujita@ynu.ac.jp

1. はじめに

近年，ネットワークを介した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容易に操作でき，ユーザは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．

しかしながら，このような利便性の反面で，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ゲートウェイであるルータ機器へは，日々WAN側から多数の攻撃パケットが届いており，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．

たとえば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をきっかけに [2]，多数のIoT機器に感染し，それらの機器によって行われたDDoS攻撃により多くの重要サービスが停止するという事態に陥った [3]．2016年6月にはFLockerと呼ばれるAndroid版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，ユーザに対して身代金を要求する事例が発生した [4]．ある家庭用ルータ製品では，当該製品固有の開放ポートから機器内に侵入し，DNSサーバの設定を変更することで，キャッシュポイズニングされたDNSサーバにドメイン名解決を導き，同ルータ配下の機器からのWebアクセス等を不正なサイトに誘導する攻撃が行われた [5]．これはIoT機器固有の脆弱性を突いた攻撃ととらえることができる．

このように家庭で用いられるIoT機器へのサイバー攻撃の脅威はすでに顕在化しており，攻撃のシナリオも多様化の一途をたどっている．しかしながら，各攻撃シナリオについて具体的にどのような脅威が存在するかは，十分に検証がなされていない．また，それらの脅威への対処策として，ホームネットワーク向けのセキュリティ製品が市販されているが，それらのセキュリティ製品が脅威に対して十分な効果を発揮するか，実態が明らかになっていない．

そこで本研究では，一般消費者の家庭のネットワーク環境を模擬したテストベッドを構築し，サイバー攻撃の観測および当該攻撃がホームネットワークに及ぼす影響の分析を行う．具体的には，多くの家庭で一般的に使用されていることが見込まれるIoT機器複数台とWi-Fiルータを用意し，インターネットに接続されたネットワークを構成する．当該ネットワークの通信トラフィックを観測可能な機器を付設したうえで，疑似的に攻撃を発生させる．すでに存在が確認されている攻撃手法にくわえ，今後出現しうる攻撃手法も想定し，それらの攻撃がホームネットワークに与える影響を調査する．調査の結果をふまえ，すでに流通しているホームネットワーク向けのセキュリティ製品が前述の攻撃を検知できるか確認する．

2. 関連研究

2.1 IoTセキュリティテストベッドの構築

これまで，日本国内の複数の研究機関において様々なIoTセキュリティに関するテストベッドが提案されてきた．たとえば，CSSC（Control System Security Center，制御システムセキュリティセンター）では，スマートメータシステムのセキュリティ確保に向けて，実機の活用を考慮した評価環境を構築した [6]．さらに同センターでは，9つのプラント（化学，ビル，工場，電力，ガス，広域連携等）を模擬して，重要なインフラと工場の環境を再現したテストベッド施設（略称：CSS-Base6）を構築した [7]．そのほかにも，計算機クラスタで構成されるStarBED型テストベッドでハードウェアエミュレータを用いてIoT環境を構築し，IoTセキュリティ実証実験を行う試みもある [8], [9]．この実証実験では，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．このように，IoTのセキュリティテストベッドについては重要インフラ，工場，広域連携システム等を模擬したテストベッドの研究が複数存在するが，一方でホームネットワークのセキュリティに関するテストベッドの研究は，総務省における試み [10] や文献 [11], [12] における試みがあげられるほかに事例が少なく，総合的な検証は進んでいないものと考えられる．本研究では，一般的なホームネットワーク環境を想定したテストベッドを構築し，ホームネットワークを狙った攻撃を実際に試行して，ホームネットワークが受ける影響の調査を行う．

2.2 IoT機器のセキュリティ評価

Alrawiら [13] は，家庭向けIoT機器がさらされる脅威および脅威への対策に関する先行研究を集約したうえで，各研究が分析対象とした要素を分類し，先行研究を体系化した．さらに，家庭向けIoT機器の運用環境を「デバイス」「クラウドエンドポイント」「モバイルアプリケーション」「コミュニケーションチャネル」という4つのコンポーネントを用いてモデル化し，それぞれのコンポーネントについて独自に設定した評価項目に沿って，45機種の家庭向けIoT機器のセキュリティを評価している．しかしながら当該研究は，実在するマルウェアの挙動を想定したホームネットワーク内の機器の脅威分析を目的とするものではない．これに対し本研究は，実際に感染が観測されたマルウェア検体のホームネットワーク内に対する通信を分析し，その分析結果に基づいて想定できる脅威に関してIoT機器のセキュリティを評価する．このように実在する攻撃挙動を想定したアプローチをとることで，より現実に即した脅威に対するセキュリティの評価を行えることが期待できる．またAlrawiらの研究は，エンドユーザがホームネッ

トワークセキュリティに脅威を感じた際にとりうる対策にまでは言及していないが，本研究は実際にエンドユーザが対策として導入することが想定されるホームネットワーク向けセキュリティ製品の効果の評価も行う．

2.3 IoT 機器のマルウェア感染の観測・分析

脆弱な IoT 機器を模擬するハニーポットを用いて IoT 機器を狙うマルウェアを収集する先行研究として，文献 [14], [15], [16] があげられる．さらにハニーポットで収集したマルウェアの攻撃挙動の詳細や傾向を動的に解析する研究として，文献 [17] があげられる．最近では，Mirai 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が，Mirai について詳しい分析を行った文献 [18] では，ハニーポットを利用し，Mirai の挙動の観測および Mirai に感染した IoT 機器の種類の分析により，Mirai の変種の登場と危険性を予測している．

3. ホームネットワークテストベッド

これまで行われてきた IoT 機器に対するサイバー攻撃を観測する研究では，家庭用ルータが攻撃者による侵入を受けた後に LAN 内の機器に対して行われる攻撃を観測対象としていない．そこで本研究では，一般家庭における LAN を模擬した複数の IoT 機器からなるテストベッドを構築し，テストベッド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．さらにテストベッド内でのマルウェアの解析およびインターネットで実際に行われている攻撃の引き込みを行うことで，LAN 内の機器に対して行われるサイバー攻撃の実態を明らかにする．

3.1 テストベッドの構成

下記を行う目的でテストベッドを構成する．

- テストベッド内およびインターネット側との通信の観測・分析
- テストベッド内での疑似的な攻撃の試行および同攻撃のテストベッド内機器への影響の検証
- IoT マルウェア検体を動作させた後の挙動の観測・分析
- インターネット側からのテストベッドへのサイバー攻撃の引き込みおよび引き込み時のホームネットワークにおける被害の観測と分析

図 1 にテストベッドの構成を示す．テストベッドは，制御サーバ（通信制御部）および観測マシン（通信観測部），家庭内で使用される無線・有線接続の IoT 機器群で構成される．

IoT 機器群 多くの家庭で一般的に使用されていると見込まれる 10 種の IoT 機器（TV，掃除機等）およびそれらの機器をルーティングする Wi-Fi ルータである．本研究において疑似的に発生させる攻撃の攻撃対象となる．機器の詳細を，機器の製造年および機器が通信に用いるプロトコル，機器のファームウェアアップデートを行う機能の仕様とともに**表 1** に示す．ファームウェアアップデート機能において AUTO と記す機器は，新しいファームウェアが存在する場合に自動的に当該ファームウェアのダウンロードおよびインストールを実行する機能を有する．MANUAL と記す機器では，新しいファームウェアの有無の確認およびファームウェアアップデートの実行操作をユーザが自ら行う必要がある．NOTIFICATION と記す機器では，MANUAL と記す機器と同様にユーザ自身がファームウェアアップデートを実行する必要があるが，新しいファームウェアの確認を自動的に行ったうえでクライアントアプリケーション等を介してユーザに新しいファームウェアの存在を通知する機能を有する．機器のファームウェアバージョンは，すべての機器について 2017 年 7 月 20 日時点で最新のものをインストールし，攻撃の観測期間においてはファームウェアのアップデートを行わないよう設定した．

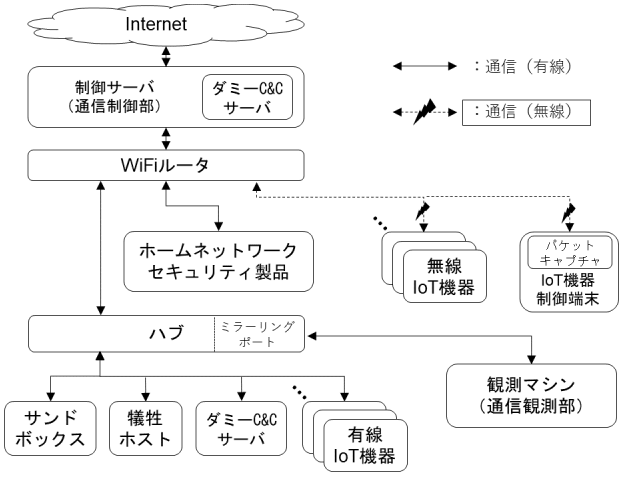


図 1 テストベッドの構成
Fig. 1 Configuration of the testbed.

IoT 機器制御端末 IoT 機器群に含まれる機器のクライアントアプリケーションがインストールされたスマートフォンである．当該アプリケーションにより，対応する IoT 機器を操作する．ルート権限を付されたパケットキャプチャアプリケーションが動作しており，無線で Wi-Fi ルータに接続する機器を当該端末のクライアントアプリケーションで操作する際に，通信を観測することができる．

制御サーバ（通信制御部） インターネットとホームネットワークの境界に設置する．インターネットからホームネットワーク内への通信およびその逆方向の通信は，当該制御サーバを経由する．模擬攻撃やマルウェアによる通信が外部に悪影響を及ぼさないよう，通信

表 1 観測および分析対象とする家庭用 IoT 機器の一覧
Table 1 List of home network IoT devices that are target of observation and analysis.

製品分類	製造年	機能説明	プロトコル（L7/L4）	ファームウェアアップデート機能
学習リモコン	不明（2014 年発売）	エアコンや TV 等の家電のリモコンを登録することで，アプリケーションから様々な家電の操作が可能となる．	独自/TCP	NOTIFICATION
ロボット掃除機	2016 年	アプリケーションを利用して清掃命令等のリモートコントロールが可能．	MQTT [19]/TCP	AUTO
スマート照明	2016 年	遠隔的に照明の ON/OFF や照明色の変更が可能．	HTTP/TCP	MANUAL
スマート電源プラグ	不明	コンセントに接続して使用する．アプリケーションで電力使用状況の確認や電源の ON/OFF が可能．	独自/UDP	MANUAL
スマートコーヒー機	2017 年	外出先から遠隔的にコーヒーを淹れることが可能．	独自/TCP	NOTIFICATION
プリンタ	2016 年	遠隔的に写真やファイルのプリント操作が可能．	LPR or RAW/TCP	MANUAL
NAS	不明（2015 年発売）	インターネットに接続して使用するファイルサーバ．	HTTP/TCP	NOTIFICATION
IP カメラ	2016 年	外出先から室内の映像を確認できる．	RTP/TCP or UDP	NOTIFICATION
スマート TV	2017 年	インターネットに接続し，映像コンテンツ等を視聴できる．	HTTPS/TCP	AUTO
空気清浄機	2016 年	外出先から機器の電源の ON/OFF および運転モードの切替え操作が可能．	MQTT/TCP	MANUAL

ルータを設定し，アウトバウンド通信を制御する．

観測マシン（通信観測部） Wi-Fi ルータの LAN ポートにリピータハブ（ポートミラーリング機能付きスイッチ）を接続し，リピータハブのミラーリングポートに当該マシンを接続することで，Wi-Fi ルータからホームネットワーク内への通信と，ホームネットワーク内から外への通信の観測を行う．

サンドボックス IoT マルウェア向けのサンドボックス「IoTBOX」[14] を実装した PC である．マルウェアを実行し，ホームネットワーク内部間および外部への疑似攻撃を行う．

ダミー C&C サーバ 任意のタイミングでマルウェアに対して攻撃の命令を送信する機能を持つ python スクリプトである．1）制御サーバ（通信制御部）内および 2）Wi-Fi ルータの LAN ポートに接続された PC にそれぞれ実装する．1）のダミー C&C サーバにより，WAN 側から LAN 側への攻撃命令の送信を実現し，2）のダミー C&C サーバにより，LAN 内（ホームネットワーク内部間）での攻撃命令の送信を実現する．

犠牲ホスト 実機と仮想マシンの 2 種を用意する．実機の犠牲ホストはインターネット側からの攻撃を引き込む際の攻撃対象として使用する．仮想マシンの犠牲ホストは，犠牲ホストがマルウェアに感染した後の挙動を観測する目的で設置する．仮想マシンの犠牲ホストは，すべての ID およびパスワードにより Telnet にログイン可能な設定とする．

ホームネットワークセキュリティ製品 現在，一般消費者向けに販売されている，家庭内の IoT 機器を保護するためのセキュリティ製品である．ホームネットワークを狙った攻撃に対する当該製品の効果を評価する目的で設置する．

表 2 テストベッドを構成するモジュールのスペック
Table 2 Specification of modules in the testbed.

モジュール	概要
制御サーバ	Intel(R) Core(TM) i7-7700 CPU@3.60 GHz
観測マシン	Ethernet ports switch with port mirroring
サンドボックス（実機）	Wi-Fi ストレージ/ポケット Wi-Fi MIPSEL
犠牲ホスト（実機）	ポケット Wi-Fi, MIPSEL/家庭用 Wi-Fi ルータ MIPS
犠牲ホスト（仮想マシン）	Openwrt 15.05-x86 [20]

表 2 にテストベッドを構成するモジュールのスペックを示す．

3.2 観測対象とする通信

ホームネットワーク内の通信 ホームネットワーク内の IoT 機器間の通信トラフィックを観測する．具体的には，有線接続の IoT 機器間の通信パケットおよび IoT

機器制御端末と有線のIoT機器との間の通信パケットを観測する．ルーティングの設定上，Wi-Fiルータを経由した無線接続機器間のTCP/IP通信は観測マシン（通信観測部）を経由しないため，観測マシン（通信観測部）では当該通信トラフィックを観測できない．Wi-Fiルータを経由した無線接続機器間のTCP/IP通信のうち，IoT機器制御端末上のクライアントアプリケーションでIoT機器を操作する際の通信については，IoT機器制御端末上のパケットキャプチャアプリケーションで観測する．

インターネットからの通信 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，観測マシンで通信トラフィックを観測する．

テストベッド内で行う疑似攻撃の通信 IoTマルウェア検体をサンドボックス内で動作させる．そのうえで，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サーバをホームネットワーク外部およびホームネットワーク内部に作成する．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，観測マシンでの観測結果から，コマンド実行時の攻撃の成否を判断する．

4. 既存の攻撃の観測および分析

一般家庭においては，多くの場合，IoT機器が有線もしくは無線で直接Wi-Fiルータに接続されている．ホームネットワークの入口にあたるWi-Fiルータへはつねに多数の攻撃が届いており，一部の脆弱なルータ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，当該ルータに接続された機器すべてが脅威にさらされる恐れがある．具体的には，攻撃者がマルウェアに感染した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，接続されたIoT機器の情報を把握し，当該IoT機器を狙うサイバー攻撃を実施することが考えられる．

そこで，Wi-Fiルータに感染したとき実際にLAN側に対して攻撃を行うマルウェアが，1）実際にテストベッドで観測・収集できるか（4.1節参照），2）テストベッド構築以前に収集されたマルウェアの中に存在するか（4.2節参照）という両面において調査する．また，そのようなマルウェアにWi-Fiルータが実際に感染した場合の当該マルウェアの挙動を観測することで，昨今のホームネットワークがさらされる脅威を分析する．

4.1 実攻撃の観測

インターネット側からテストベッドに届く実攻撃を観測し，当該攻撃が家庭内へ侵攻するかを検証する．テストベッドに外部から届く攻撃のうち，Wi-Fiルータのリモートアクセス機能に対応する23/tcp，2323/tcp，80/tcp，8080/tcpポートへのアクセスを，制御サーバからWi-FiルータのWANポートに転送した．当該Wi-Fiルータは，実際にTelnetに関する脆弱性を有し，頻繁にマルウェアに感染することが文献[21]で実証されているため，定期的に電源を再起動することでマルウェアをクリーンアップし，様々な検体に感染するようにした．なお，Wi-Fiルータを再起動する周期は15分とした．文献[21]では，当該Wi-Fiルータと同一機種および同一設定のルータをインターネットに接続する実験を3回繰り返したとき，平均1分50秒のうちにマルウェアに感染したことが報告されている．このことから当該Wi-Fiルータは，本観測において少なくとも15分に1回はマルウェアに感染していたものと推測される．

2017年12月9日から1週間にわたり攻撃を観測したが，Wi-Fiルータに感染したマルウェアがLAN側に対して攻撃を行う状況は観測されなかった．要因の1つとして，観測期間中に流行していたマルウェアがLAN側への攻撃を行わないものであったことが考えられる．

4.2 収集したマルウェア検体による攻撃の検証

過去に発生していたマルウェアに，LAN側への攻撃を実際に行うマルウェアが存在するか否かを調査する．ハニーポット等により事前に収集したマルウェア検体のうち，IoT機器を狙ったマルウェア検体を選定する．これらのマルウェア検体をテストベッドのWi-Fiルータ上で実行し，実際にLAN側への攻撃が発生するかを観測し，想定される脅威を分析する．

4.2.1 LANにスキャンを実行するIoTマルウェア

IoT機器を模したハニーポット「IoTPOT」[14]で収集したマルウェア検体を，収集後10分以内にテストベッド内のサンドボックスにセットし，5分間の動的解析を行った．当該サンドボックスには，Wi-FiルータによりDHCPでプライベートIPアドレス（192.168.0.0/16のうちの1つ）を割り当てた．また，当該サンドボックスにルータとしての構成は行わなかった．マルウェアの収集および動的解析期間は2016年12月20日から2017年11月30日で，解析対象となった検体は6,859検体であった．このうち，3,000検体はMIPSアーキテクチャで動作するもので，3,859検体はMIPSELアーキテクチャで動作するものである．

動的解析の結果，6,859検体のうち289検体がLAN側にスキャンを行うことが確認された．289検体のうち，90検体はMIPSで動作するマルウェアで，199検体がMIPSELで動作するマルウェアであった．これらの289検体のマルウェアファミリーに関する情報を**表3**に示す．なお，ファミリー名はアンチマルウェアソフト「Dr.Web」[22]により

表 3 IoT マルウェア検体のファミリー名
Table 3 Family names of the malwares.

種類	BackDoor.Fgt	Linux.Mirai	Trojan	その他
MIPS	80 検体	7 検体	1 検体	2 検体
MIPSEL	168 検体	26 検体	0 検体	5 検体

表 4 IoT マルウェア検体の LAN 側への通信
Table 4 Transmission towards LAN by the malwares.

種類	Private IP Address/All Destination IP
MIPS	0.035%
MIPSEL	0.086%

判定されたものである．また，これらの 289 検体によるスキャン試行のうち，当該試行においてスキャン対象とした IP アドレスがプライベートアドレス空間（10.0.0.0/8 および 172.16.0.0/12，192.168.0.0/16）の IP アドレスであった割合を，検体の動作アーキテクチャ別に**表 4** に示す．

表 4 にも示すように，マルウェアが LAN 側にスキャンを行う確率は小さく，これらのマルウェアの挙動が故意に LAN を狙ったものである確証はない．LAN 内で用いられるプライベート IP アドレスが偶然スキャンの宛先に選ばれたと推定することもできる．しかしながら少なくとも，Wi-Fi ルータに感染したマルウェア検体が LAN 側への攻撃を行う可能性があることが分かった．

なお，本観測および分析の結果は，あくまでも前述した構成のサンドボックスにおける観測にともなった結果である．マルウェアの挙動はサンドボックスのネットワーク構成や内部構成に影響を受けることがあり，サンドボックスの構成によっては当該結果と異なるマルウェアの挙動がみられる可能性がある．

4.2.2 IoT マルウェアの実行

テストベッド内の Wi-Fi ルータに，4.2.1 項で述べた LAN 側にスキャンを行う IoT マルウェア検体を感染させ，その挙動を観測する．当該ルータの CPU アーキテクチャは MIPS であるため，MIPS で動作する検体 90 個を用いる．これらの検体は収集してから時間が経っており，C&C サーバにつながらないため，任意のタイミングでマルウェアに対する命令を送信できる機能を持つダミー C&C サーバを用いる．観測手順は以下のとおりである．

(1) 事前に入手した IoT 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) マルウェアを Wi-Fi ルータ上で実行し，感染させる．
(3) ダミー C&C サーバから攻撃命令を送信する．
(4) Wi-Fi ルータから LAN 側へのスキャンをすべて犠牲ホストに転送する．さらに，観測マシンを使用し，Wi-Fi ルータと犠牲ホストの間の通信を観測する．
(5) 解析環境を 15 分後にシャットダウンし，検体をクリーンアップする．

この実験において，90 検体のマルウェアはすべて Wi-Fi ルータ上で実行に成功し，LAN 側を含むランダムな宛先 IP アドレスの 23/tcp ポートおよび 2323/tcp ポートにスキャンを行い，犠牲ホストの Telnet サービスへのログインを試行していた．

これらの検体が仮に当該 Wi-Fi ルータに感染した場合，その後，配下のホームネットワーク内の機器に対して「Telnet を経由したマルウェアの感染拡大を行う」もしくは「将来の攻撃実施に向けて機器の情報を収集する」等の多くの脅威が想定される．

5. 疑似攻撃の試行と影響の分析

本研究では，ホームネットワークにおいて考慮しうる様々なリスクのうちから，下記の基準に適合する攻撃シナリオを選定し，脅威を分析する．

- IoT マルウェアが家庭用ルータに侵入した後，容易に実行できてしまうコストが低い攻撃でかつ現実に生じうる攻撃であること
- 実マルウェアや実マルウェアに感染する機器を用いたリアリティの高い疑似攻撃実験が実施可能であること
- 攻撃が成功したときに生活者に直接的なインパクトがあること

これらの基準に沿って，ホームネットワークの入口にあたる Wi-Fi ルータがマルウェアに感染するケースを想定し，調査を実施した．その結果，Wi-Fi ルータに感染した際に LAN 側に対してスキャン等の挙動を見せるマルウェアが存在することが分かった．この事実を前提として，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，テストベッド内においていくつかの疑似攻撃を実施した結果について報告する．

5.1 ホームネットワーク内サービス妨害攻撃

家庭内の機器を狙う攻撃の 1 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等に対して大量のデータや不正なデータを送信し，標的となる機器やネットワーク等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．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する．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ケーション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，観測対象ポートが定まらない．このこと

から，当該3種の機器については，調査対象から除外する．

以下の手順で，テストベッド内のIoT機器に対してサービス妨害攻撃を実施する．

(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転送したIoT機器をテストベッドに接続し，マルウェアを実行する．
(3) 観測マシンで，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．

なお，攻撃に用いるIoTマルウェアには，別途入手したIoTマルウェア検体（MD5ハッシュ値：b66d2425ea49f73c9d09f8999c26c93c，BitDefender [23] による検知名：Gen:Variant.Backdoor.Linux.Gafgyt.1）を用い，マルウェアバイナリファイルを転送・実行するIoT機器には，脆弱性が確認されたWi-Fiストレージの実機を用いる．

調査結果を**表5**に示す．操作可否の項目中の「○」は攻撃を実施している際でも，機器がユーザによる操作に応じた動作を示したことを意味する．「×」は機器がユーザによる操作を受け付けなくなったことを意味する．「△」はユーザによる操作に対し機器が動作するまでに大幅な遅延（20秒以上）があったことを意味する．なおクライアントアプリケーションを介した操作が可能な機器については，当該アプリケーションを用いてユーザが操作した場合の挙動を示す．

調査結果より，攻撃通信量が小さいにもかかわらず，用意した機器の半分以上がユーザの操作に応答しなくなることが確認された．攻撃終了後，ほとんどのIoT機器は1分以内に操作を受け付ける状態に戻ったが，再起動するまで操作を受け付ける状態に戻らない機器も存在した．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，IoT機器の動作が妨害されうることが実証された．

機器が攻撃を受けた際に正しい動作を行っているか否かおよび攻撃を受けた状態からの回復の仕方は，機器の特性に依存して定まるものといえる．IoT機器には，異常な状態で動作することによって人間に被害を与えうる可動部および加熱部が機器外部に取り付けられたものが存在する．本研究で取り上げた機器の中では，ロボット掃除機が機器外部に可動部が取り付けられた機器として，スマート照明とスマートコーヒー機が機器外部に加熱部が取り付けられた機器としてそれぞれあげられる．これらの機器については，本来は異常な通信を受けた際に安全を最優先して動作を停止することが望ましいと考えられる．また攻撃を受けた後は操作どおりに機器の加熱部および可動部の制御を行えるか否かについての点検が行われてから再度動作を開始することが望ましいと考えられる．少なくとも，クライアントアプリケーションからの操作に機器が応じなくなる状態，もしくは機器本体のスイッチ類による操作を受け付けなくなる状態は，機器が稼働した状態で攻撃を受ける状況を考慮すると，安全上望ましくないといえる．

この観点では，機器が動作している状態でサービス妨害攻撃を受けた際に異常を検出して動作を停止する機器は，本試行で対象とした機器の中に存在しなかった．また，ロボット掃除機およびスマート照明，スマートコーヒー機はクライアントアプリケーションから操作することが可能であるが，攻撃を受けた際にクライアントアプリケーションからの操作を受け付けなくなっており，遠隔的な制御が効かない状態に陥ったものととらえられる．ただしスマート照明およびスマートコーヒー機は，一定の時間をあけてクライアントアプリケーションからの操作を受け付けるように回復しており，安全面での一定の妥当性を有するものと考えられる．他方でロボット掃除機は，攻撃を受けた後，人間の手により強制的に機器の再起動を行うまではクライアントアプリケーションからの操作を受け付けず，同機が動作した状態でサービス妨害攻撃を受けた場合，ユーザの意思とは関係なく機器が動作し続けることとなる．

なお，家庭内のIoT機器の動作を妨害することは，攻撃者にとって直接的な利益を生む行為ではないとも考えられるが，他方で，感染したIoT機器を故障させるマルウェ

表5 ホームネットワーク内サービス妨害攻撃の影響
Table 5 Effects by DoS attack on home network.

対象	攻撃の種別（攻撃通信量）	操作可否	攻撃後自動的に操作可能な状態に戻るか否か/回復時間
ロボット掃除機	SYN flood（392 KB/s）	×	不可（Rebootが必要）
スマート照明	SYN flood（307 KB/s）	×	自動的に操作可能な状態に戻る/15秒
学習リモコン	SYN flood（357 KB/s）	△	自動的に操作可能な状態に戻る/28秒
NAS	SYN flood（435 KB/s）	○	-
プリンタ	SYN flood（225 KB/s）	○	-
スマートコーヒー機	SYN flood（342 KB/s）	×	自動的に操作可能な状態に戻る/23秒
スマート電源プラグ	UDP flood（13 MB/s）	×	自動的に操作可能な状態に戻る/18秒

ア [24] も存在することから，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 攻撃のような異常な量の通信を検知し，フィルタリングする方法が考えられる．

5.2 ホームネットワーク内機器の不正操作

ホームネットワーク内でスマートフォン上のクライアントアプリケーション等を操作して IoT 製品を使用する場合，まずアプリケーション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，機器が命令に従って動作した後，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．そこで，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．

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．このとき，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て操作対象となる 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できる．以上の不正操作攻撃の実現可能性を検証するため，テストベッド内の機器のうち，アプリケーションを介して機器の操作を行う機器（ロボット掃除機，学習リモコンおよびスマート電源プラグ）を不正操作の調査対象とした．以下に示す手順で，調査を行う．

(1) IoT 機器の動作機能ごとに，スマートフォンでアプリケーションを操作しながら，送受信したパケットを IoT 機器制御端末上のパケットキャプチャアプリケーションでキャプチャする．
(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を抽出する．そのうえで，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 機器に送信する．この操作により同一の動作機能が再現されるか否かを確認する．

通信解析と調査の結果を**表 6** に示す．アプリケーションと機器が平文で通信する学習リモコンに対しては，不正操作によるすべての操作が成功した．アプリケーションと機器の間の通信が暗号化されているロボット掃除機については反応がなく，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．結果として，アプリケーションと機器の間で通信を行う 3 種の IoT 機器のうち，2 種（学習リモコンおよびスマート電源プラグ）で不正操作に成功した．学習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みた．結果として，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なしでの操作に成功した．スマート電源プラグでは，通信内容の可読性はないが，アプリケーションから送信された命令通信をそのまま送信することで，スマート電源プラグを操作することが可能であった．

今回の調査では，学習リモコンとスマート電源プラグのどちらの機器にも操作を行う側の認証機能が存在しないため，不正操作が成功したものと考えられる．一方で，アプリケーション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公開鍵および秘密鍵，セッション鍵の鍵交換の過程（SSL ハンドシェイク [25]）が確認された．具体的には，ロボット掃除機が使う MQTT プロトコルにのっとって，TLS/SSL を使用して暗号化が行われていた．このように通信内容の暗号化と，操作側の認証を行うことで，単純なリプレイ攻撃を防ぐことは可能と考えられる．

また，このほかにも重大な影響を及ぼしうる不正操作が存在する．マルウェア感染等により Wi-Fi ルータに侵入する経路を確保した攻撃者が，ルーティング設定を変更したり，DNS キャッシュサーバの設定を変更したりすることで，ホームネットワーク内の機器からの通信がフィッシングサイトや身代金要求サイト，ドライブバイダウンロード等の脆弱なブラウザを狙った攻撃を行う悪性サイトに誘導される恐れがある．実際にテストベッド内の Wi-Fi ルータ上で動作する通信制御用プログラムである Iptables [26] の設定を変更して，80/tcp への通信を疑似悪性サイトに転送する設定としたところ，スマートフォンやタブレット端末のブラウザ，スマート TV 等で疑似悪性サイトからのコンテンツが表示されることを確認した．金銭を要求したうえで，送金するまで正規のコンテンツとの通信をブロックするような，IoT 版のランサムウェアの出現が懸念される．また，この種の攻撃者がルーティング設定や DNS キャッシュサーバの設定を変更して機器ユーザによるアクセスをコントロールする攻撃については，IoT 機器セキュリティに限った問題ではなく，インターネットの機器全般に関す

表 6 家庭内サービス妨害攻撃の影響
Table 6 Effects by DoS attack on home network.

対象	L7 プロトコル	ペイロードの可読性	成功した操作
ロボット掃除機	MQTT	なし（SSL で暗号化）	（なし）
学習リモコン	Raw TCP	あり（ASCII コードで記載）	TV 電源の ON/OFF，TV 音量調整，TV チャンネル調整
スマート電源プラグ	Unknown	なし（バイナリデータ）	電源 ON/OFF

る問題であることに留意されたい．

これらの疑似攻撃はホームネットワークに一定程度の影響を与えて，ユーザに不便をもたらすため，対策が必要といえる．

6. ホームネットワークセキュリティ製品の評価

6.1 ホームネットワークセキュリティ製品について

近年，ホームネットワーク向けのセキュリティ製品が消費者の注目を集めている [30]．これらの製品は，家庭のホーム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接続された機器およびそのユーザを保護する．

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．

リモートアクセス試行の通知および遮断機能 ホームネットワーク内の機器に対してリモートアクセスツールによる試行があった場合に，ユーザに通知し，ユーザの判断に応じて当該リモートアクセスを遮断する．

ホームネットワーク内通信の監視および遮断機能 ホームネットワークに接続した機器間の通信を監視し，不審な通信と判断された場合は遮断する．

不正サイトへのアクセスブロック機能 マルウェア感染やフィッシング詐欺等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，ビデオゲーム機のような，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．

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，一覧できるように表示する．また，接続されている機器をスキャンし，脆弱性があるか否かを検知する．

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たりし，かつスマートフォンもしくはタブレットに当該製品の管理用アプリケーションをインストールして使用する必要がある．

6.2 ホームネットワークセキュリティ製品の評価

ホームネットワークセキュリティ製品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，5 章で述べたような疑似的な攻撃をテストベッド内で試行することで当該製品の効果を検証する．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，遮断できるかどうかを調査する．

これらの調査を実施するため，製品のセキュリティ機能について評価するべき項目（以下，評価項目）を検討する．以下に，評価項目の大項目を示す．

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な攻撃を行い，セキュリティ製品が検知・遮断できるか否かを調査する．以下，「内→内」と略記する．

ホームネットワークから外部への攻撃の検知・遮断 マルウェアに感染した家庭内の機器もしくは攻撃ツールで，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．以下，「内→外」と略記する．

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およ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．以下，「外→内」と略記する．

その他 セキュリ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否かを調査する．

詳細な評価項目と評価の実施方法および使用ツールを**表 7** に示す．

6.3 評価事例

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 7 の一部分の評価項目について調査を行い，製品 A と B の効果を検証した．製品 A および製品 B が有する機能を**表 8** に示す．表 8 において記号「○」はその製品が当該機能を有する旨が公表されていることを，記号「−」は当該機能を有する旨が公表されていないことを示す．また，表 8 に示す各機能は，前述のホームネットワーク製品が持つ機能（5 種）に対応する．製品 A は Wi-Fi ルータに接続して使用する．製品 B は Wi-Fi ルータに接続するか，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，どちらも Wi-Fi ルータに接続するモードを選択して，評価を実施した．以下では，行った評価およびその結果について述べる．評価試行の結果の詳細を**表 9** に示す．

(1) ホームネットワーク内部での攻撃（内→内）疑似攻撃ホストから，ポートスキャンツール Nmap [27] を用いて，Wi-Fi ルータとセキュリティ製品を含むテストベッド内の全機器に対して，TCP 全ポートに対するスキャンを実施した．また，metasploit [28] により，脆弱性スキャンおよび Telnet ログインを試行した．さらに，事前に収集したマルウェア検体（MD5 ハッシュ値：b66d2425ea49f73c9d09f8999c26c93c，BitDefender による検知名：Gen:Variant.Backdoor.Linux.Gafgyt.1）をサンドボックスで実行し，テストベッド内の IoT 機器に DoS 攻撃を実施した．製品 A が Wi-Fi ルータおよびセキュリティ製品本体に対する直接的なポートス

表 7 セキュリティ製品の評価項目
Table 7 Evaluation items for security products.

大項目	種類	項目	実施方法
内→内	Scan/Exploit	Port scan	Nmap [27], Malware
		Vulnerability Scan/SQL injection	metasploit [28]
		Remote access (ssh, telnet)	metasploit
	DoS	DoS	Malware
内→外	Scan/Exploit	Port scan	Nmap, Malware
		Vulnerability Scan/SQL injection	metasploit
		Remote access (ssh, telnet)	metasploit
	DoS	DoS	Malware
	URL Block	URL Block	PhishTank [29] の 1 週間分の URL List
外→内	Scan/Exploit	Port scan	Nmap, Malware
		Vulnerability Scan/SQL injection	metasploit
		Remote access (ssh, telnet)	metasploit
	DoS	DoS	Malware
	悪性サイトへの誘導	悪性サイトへの誘導	ルーティング設定の変更
	実攻撃の検知	実攻撃の検知	Malware
その他	脆弱性診断	脆弱性診断	脆弱な機器を設置

表 8 評価対象とするホームネットワークセキュリティ製品が持つ機能の公表状況
Table 8 Declared functions in evaluated security products.

機能	製品 A	製品 B
侵入防御機能	○	○
リモートアクセス試行の通知および遮断機能	○	−
ホームネットワーク内通信の監視および遮断機能	○	−
不正サイトへのアクセスブロック機能	○	○
接続機器の脆弱性検知機能	○	−

キャンを検知し，当該スキャンを遮断した．

(2) ホームネットワーク内部から外部への攻撃（内→外）
評価試行 (1) と同様の攻撃を，ホームネットワーク外部に設置した犠牲ホストに対して実施した．また，フィッシングサイトへのアクセスを検出できるか否かを確認するため，PhishTank [29] において収集した 1 週間分のフィッシングサイトの URL に対してアクセスした．製品 A が攻撃対象から応答があった Telnet ログイン試行を検知した．また，製品 A および製品 B がおよそ 80%の検知率で，フィッシングサイトへのアクセスを検知・遮断（ブロック）した．

(3) 外部からホームネットワーク内部への攻撃（外→内）
評価試行 (1) と同様の攻撃を，外部に設置したホストからホームネットワーク内部の機器に対して実施した．また，Wi-Fi ルータのルーティングの改竄，および当該 Wi-Fi ルータをマルウェアに感染させる試行を実施した．製品 A が「Wi-Fi ルータが感染し，さらに内部のホストが攻撃を受け，内部のホストが応答した場合」のみ，攻撃を検知した．

(4) ホームネットワーク内の機器の脆弱性診断（その他）
ホームネットワーク内に設置した機器のうち，機器管理用の WebUI に認証が必要な機器と，Telnet サービスが動作する機器について，それぞれ弱いログイン ID/パスワード（admin/admin）を設定した．製品 A が，内蔵する ID/パスワードリストで IoT 機器の WebUI の認証機構にログイン試行を実施し，十分な強度を持つ ID/パスワードを用いているかについて検証を行った．その結果，ベーシック認証過程を持つ機器についてのみ，弱いログイン ID/パスワードの検知に成功した．

製品 A は，いくつかの試行項目について攻撃を検知したが，大半の攻撃については検知しなかった．製品 B については，フィッシングサイトへのアクセスのブロック以外に効果を確認できなかった．

現時点で市販されているホームネットワークセキュリティ製品は，他にも存在する．しかしながら，本研究において調査した範囲では，いずれの製品も検知可能なホームネットワークへの攻撃の種類が少なく，Wi-Fi ルータおよび当該ルータに接続された IoT 機器を保護する能力が十分ではない可能性がある．

ホームネットワークセキュリティ製品は，その製品がホームネットワーク内のどのポイントに接続され，どのような仕組みで通信をタッピングし，どのように通信を分析するかによって，検出できる問題および対処できる範囲が

表 9 セキュリティ製品の評価試行と各製品の挙動
Table 9 Evaluation attempts for security products and their behaviors.

大項目	項目	実施方法	製品 A の反応	製品 B の反応
内→内	Port scan	Nmap で IoT 機器の全 TCP ポートにポートスキャンを実行	Wi-Fi ルータへのスキャンのみ検知・遮断	検知せず
	Vulnerability Scan	metasploit で家庭内の IoT 機器に脆弱性スキャンを実行	検知せず	検知せず
	Remote access (telnet)	metasploit で家庭内の IoT 機器に Telnet ログイン試行を実施	検知せず	検知せず
	DoS	Malware	検知せず	検知せず
内→外	Port scan	Nmap でグローバル IP の全 TCP ポートにポートスキャンを実施	検知せず	検知せず
	Vulnerability Scan	metasploit で Wi-Fi ルータに脆弱性スキャンを実行	検知せず	検知せず
	Remote access (ssh, telnet)	metasploit で外部のホストに Telnet ログイン試行を実施	セッション確立時に検知	検知せず
	DoS	Malware	検知せず	検知せず
	URL Block	PhishTank の 1 週間分の URL List（URL 総数 2,088）	検知率 80.7%（1,684/2,088）	検知率 77.2%（1,612/2,088）
外→内	Port scan	Nmap で Wi-Fi ルータの WAN 側全 TCP ポートにポートスキャンを実行	検知せず	検知せず
	Vulnerability Scan	metasploit で外部から Wi-Fi ルータに脆弱性スキャンを実行	検知せず	検知せず
	Remote access (telnet)	metasploit で外部から Wi-Fi ルータに Telnet ログイン試行を実施	検知せず	検知せず
	DoS	Malware	検知せず	検知せず
	悪性サイトへの誘導	Wi-Fi ルータの WAN 側からルーティング設定の改ざんを実行	検知せず	検知せず
	実攻撃の検知	Malware	感染時に検知	検知せず
その他	脆弱性診断	認証機能（Web，Telnet）に弱い ID およびパスワードが設定された機器を設置	WebUI のベーシック認証のみ検知	検知せず

異なる．たとえば，ホームネットワークセキュリティ製品には製品自体が Wi-Fi ルータとなるモードを有するものも存在し，この場合はルータの LAN ポートに製品をつなぐ場合に比べて分析できる通信が多いものと考えられる．また，通信パケットのペイロードまで検査するか否か，ペイロードの検査についてどのような検査手段を備えているかによって，検出できる攻撃の種類も異なる．本研究で調査対象とした機器は特に通信をタッピングする仕組みがブラックボックスであるため詳細を考察できないが，ホームネットワークセキュリティ製品がホームネットワークを保護する能力に関しては，本来，製品の接続方法および通信タッピングの仕組み，タッピングした通信の分析方法も含めて評価を行うことが妥当といえる．

7. おわりに

本研究では，一般消費者の家庭のネットワーク環境を模擬したテストベッドを構築し，サイバー攻撃の観測および攻撃による影響の分析を行った．IoT 機器複数台と Wi-Fi ルータで構成されたネットワークに，当該ネットワーク内の通信トラフィックを観測可能な機器を設置し，すでに存在が確認されている攻撃手法および今後出現しうる攻撃手法も想定したうえで，それらの攻撃がホームネットワークに与える影響を検証した．検証の結果，家庭用ルータが攻撃者により侵入を受けた後，さらに LAN 内の機器を狙ったサイバー攻撃が実行されうることが分かった．また，想定した LAN 内の機器への攻撃手法の多くが，ホームネットワークに一定程度の影響を与え，ユーザに不便をもたらすことが分かった．検証の結果をふまえ，すでに流通しているホームネットワーク向けのセキュリティ製品が本研究で想定した攻撃を検知できるか確認した．その結果，確認対象としたセキュリティ製品のいずれについても，本研究で想定した攻撃の大半を検知できず，検知可能な対象がポートスキャン等の一部の攻撃に限られることが分かった．ホームネットワーク内の機器に対する攻撃を体系化し，系統別の対策を講じる必要がある．

今後は，攻撃観測用の IP アドレスを増やして観測期間を長期化することで，外部からルータに届く攻撃および当該攻撃により想定される被害を，より網羅的に把握する．ま

た，UPnP 等により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家庭内に引き入れる機器の挙動の分析，ならびにランサムウェアによる IoT 機器への攻撃の可能性を検討する．

ホームネットワークにおけるリスクおよび対処方法については，複数のガイドラインがまとめられている [31], [32]．これらのガイドラインには，マルウェア感染やデータ改ざん，情報漏洩等多様なリスクを考慮したうえで，ホームネットワークのほか多種のユースケースを想定した脅威分析とともに，総合的な観点での IoT セキュリティの評価方法が示されている．しかしながら本研究で取り上げたリスクは，これらのガイドラインに対応付けて選定されたものではない．今後は，当該ガイドラインのようなネットワーク上のリスクを総合した資料と，研究において分析対象とするリスクが，どのような対応関係をとるかを明らかにするべきである．

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．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．

参考文献

[1] Symantec Corporation: Mirai: New wave of IoT botnet attacks hits Germany, available from ⟨http://www.symantec.com/connect/blogs/mirai-new-wave-iot-botnet-attacks-hits-germany⟩.
[2] Krebs, B.: Source Code for IoT Botnet ‘Mirai’ Released, available from ⟨https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/⟩.
[3] Krebs, B.: DDoS on Dyn Impacts Twitter, Spotify, Reddit, available from ⟨https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/⟩.
[4] Trend Micro Incorporated：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—トレンドマイクロセキュリティブログ，入手先 ⟨https://blog.trendmicro.co.jp/archives/13453⟩.
[5] Trend Micro Incorporated：ルータに存在する脆弱性，DNS ポイズニングに誘導—トレンドマイクロセキュリティブログ，入手先 ⟨https://blog.trendmicro.co.jp/archives/9146⟩.
[6] 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，Vol.59, pp.1121–1124 (2016).
[7] 技術研究組合制御システムセキュリティセンター：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，入手先 ⟨http://www.css-center.or.jp/pdf/about_CSSC.pdf⟩.
[8] 宮地利幸，中田潤也，知念賢一，Razvan, B.，三輪信介，岡田 崇, 三角 真, 宇多 仁, 芳炭 将, 丹 康雄, 中川晋一，篠田陽一：StarBED：大規模ネットワーク実証環境，情報処理，Vol.49, No.1, pp.57–70 (2008).
[9] 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，Vol.2014, pp.1258–1263 (2014).
[10] 総務省：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，入手先 ⟨http://www.soumu.go.jp/midika-iot/admin/wp-content/uploads/2016/07/H27-2_Report.pdf⟩.
[11] Tong, J., Sun, W. and Wang, L.: A Smart Home Network Simulation Testbed for Cybersecurity Experimentation, *Testbeds and Research Infrastructure: Development of Networks and Communities*, pp.136–145, Springer, Cham (2014).
[12] Saxena, U., Sodhi, J.S. and Singh, Y.: Analysis of security attacks in a smart home networks, *2017 7th International Conference on Cloud Computing, Data Science & Engineering – Confluence*, pp.431–436, IEEE (2017).
[13] Alrawi, O., Lever, C., Antonakakis, M. and Monrose, F.: SoK: Security Evaluation of Home-Based IoT Deployments, *2019 IEEE Symposium on Security and Privacy*, pp.208–226 (2019).
[14] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: Analysing the Rise of IoT Compromises, *USENIX/WOOT*, Vol.15 (2015).
[15] 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, pp.1–6 (2016).
[16] 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，情報処理学会論文誌，Vol.58, No.9, pp.1399–1409 (2017).
[17] 鉄 穎，楊 笛，保泉拓哉，中山 颯，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，情報処理学会論文誌，Vol.59, No.5, pp.1321–1333（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/170000149503/ja/⟩ (2018).
[18] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. and Zhou, Y.: Understanding the Mirai Botnet, *26th USENIX Security Symposium*, pp.1093–1110 (2017).
[19] Stanford-Clark, A.J. and Nipper, A.: MQTT – A lightweight messaging protocol for small sensors and mobile devices, available from ⟨http://mqtt.org/⟩.
[20] OpenWrt Project: OpenWrt, available from ⟨https://openwrt.org/⟩.
[21] 田宮和樹，中山 颯，江澤優太，鉄 穎，呉 俊融，楊笛，吉岡克成，松本 勉：IoT マルウエア駆除と感染防止に関する実機を用いた実証実験，暗号と情報セキュリティシンポジウム（SCIS）(2017).
[22] Doctor Web Ltd: Dr.Web, available from ⟨https://www.drweb.ru/⟩.
[23] SOFTWIN: Bitdefender, available from ⟨https://bitdefender.com/⟩.
[24] Paganini, P.: Brickerbot botnet, the thingbot that permanently destroys IoT devicesSecurity Affairs, available from ⟨http://securityaffairs.co/wordpress/57839/malware/brickerbot-botnet-iot.html⟩.
[25] Wagner, D. and Schneier, B.: Analysis of the SSL 3.0 protocol, *Proc. 2nd Conference on USENIX Workshop on Electronic Commerce*, Vol.2, p.4, USENIX Association (online), available from ⟨https://dl.acm.org/citation.cfm?id=1267171⟩ (1996).
[26] Russell, R.: iptables, available from ⟨https://linux.die.net/man/8/iptables⟩.
[27] Lyon, G.F.: *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*, Insecure, USA (2009).
[28] Rapid7 LLC: metasploit, available from ⟨https://www.

metasploit.com/⟩.
[29] PhishTank: PhishTank, available from ⟨https://www.phishtank.com/⟩.
[30] Impress Corporation：新たなサイ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 – INTERNET Watch，入手先 ⟨https://internet.watch.impress.co.jp/docs/special/1069738.html⟩.
[31] 独立行政法人情報処理推進機構：IoT 開発におけるセキュリティ設計の手引き，入手先 ⟨https://www.ipa.go.jp/files/000052459.pdf⟩.
[32] 一般社団法人 JPCERT コーディネーションセンター：IoT セキュリティチェックリスト，入手先 ⟨https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html⟩.

藤田 彬 （正会員）

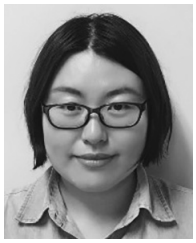
2012 年 12 月横浜国立大学大学院環境情報学府博士課程後期修了，博士（情報学）．2013 年 1 月横浜国立大学成長戦略研究センター産学官連携研究員．同年 8 月大学共同利用機関法人情報・システム研究機構国立情報学研究所特任研究員．2015 年 6 月同特任助教．2017 年 1 月より横浜国立大学先端科学高等研究院特任教員（助教）．能動的観測および受動的観測による IoT 機器への攻撃リスクの検知，攻撃の観測等ネットワークセキュリティに関する研究に従事．

楊 志勇

2016 年 10 月横浜国立大学大学院環境情報学府博士課程前期進学．IoT 家電のセキュリティ等，ネットワークセキュリティの研究に従事．

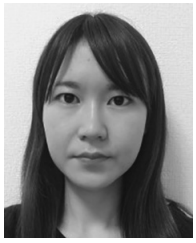
熊 佳

2017 年 4 月横浜国立大学大学院環境情報学府博士課程前期に進学．IoT 家電のセキュリティ等，ネットワークセキュリティに関する研究に従事．2019 年 3 月横浜国立大学大学院環境情報学府博士課程前期修了．修士（情報学）．2019 年 4 月よりテクマトリックス（株）でネットワークセキュリティ事業部に従事．



鉄 頴

2018 年 6 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（情報学）．情報セキュリティ，特にネットワーク攻撃観測・分析等のネットワークセキュリティ研究に従事．2018 年 8 月よりトヨタ自動車（株）で自動車の安全とセキュリティに関する研究に従事．



楊 笛

2015 年 10 月横浜国立大学大学院環境情報学府博士課程前期進学．ネットワークセキュリティの研究に従事．

江澤 優太

2016 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業，学士（工学）．同年 4 月横浜国立大学大学院環境情報学府博士課程前期に進学．ネットワークセキュリティに関する研究に従事．

中山 颯

2016 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業，学士（工学）．同年 4 月横浜国立大学大学院環境情報学府博士課程前期に進学．ネットワークセキュリティに関する研究に従事．

田宮 和樹

2017 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業，学士（工学）．同年 4 月横浜国立大学大学院環境情報学府博士課程前期に進学．ネットワークセキュリティに関する研究に従事．

西田 慎

2017 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業，学士（工学）．同年 4 月横浜国立大学大学院環境情報学府博士課程前期に進学．ネットワークセキュリティに関する研究に従事．

吉岡 克成 （正会員）

2005 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了，博士（工学）．同年 4 月独立行政法人情報通信研究機構研究員．2007 年 12 月より横浜国立大学学際プロジェクト研究センター特任教員（助教）．2011 年 4 月より横浜国立大学大学院環境情報研究院准教授．マルウェア解析やネットワーク攻撃観測・検知等のネットワークセキュリティの研究に従事．2009 年文部科学大臣表彰・科学技術賞（研究部門）受賞．

松本 勉

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月同大学大学院環境情報研究院教授．2014 年 12 月より同大学先端科学高等研究院主任研究者を兼務．ネットワーク・ソフトウェア・ハードウェアセキュリティ，暗号，耐タンパ技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．2005～2010 年国際暗号学会 IACR 理事．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞，2008 年第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞（研究部門）受賞．