情報処理学会論文誌 Vol.59 No.5 1321–1333 (May 2018)

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

鉄 穎[1,a)] 楊 笛[1] 保泉 拓哉[1] 中山 颯[1] 吉岡 克成[1,2] 松本 勉[1,2]

受付日 2017年8月17日, 採録日 2018年2月1日

概要：ネットワークサービスの妨害を目的としたDDoS攻撃が全世界で増加しており，深刻な脅威となっている．特に最近では，マルウェアに感染したIoTデバイスがDDoS攻撃を行うケースが急増している．本研究ではハニーポットで収集したIoTマルウェア検体をサンドボックス内で実行し，DDoS攻撃の観測と分析を行った結果を報告する．実験では，IoTマルウェアの動的解析においてC&Cサーバに接続し，攻撃の観測を行う観測実験とC&Cサーバからの応答を蓄積したダミーC&Cサーバを用いた攻撃再現実験を行う．前者の観測実験により，攻撃対象や頻度など実際に発生している攻撃の傾向を把握し，後者の再現実験により，様々なDDoS攻撃の通信内容などの詳細な分析を行う．また，IoTマルウェアに感染することが確認されている4種類の実機を使った再現実験によりIoTデバイスによるDoS攻撃の流量を測った結果を示す．

キーワード：DDoS攻撃，IoTマルウェア，動的解析

Observation of DDoS Attacks from IoT Malware Using Sandbox Analysis

Ying Tie[1,a)] Di Yang[1] Takuya Hoizumi[1]
Sou Nakayama[1] Katsunari Yoshioka[1,2] Tsutomu Matsumoto[1,2]

Received: August 17, 2017, Accepted: February 1, 2018

Abstract: Distributed Denial of Service (DDoS) attacks against various online services are increasing all over the world and becoming a serious threat. Lately, it is reported that bot-infected IoT devices perform huge DDoS attacks. In this study, we report observation and analysis results of dynamic analysis of IoT malware collected by honeypot in order to investigate the DDoS attacks by IoT malware. There are two types of experiments: observation experiment and replay experiment. In the observation experiment, we use Internet-connected sandbox to receive real commands from actual C&C servers to grasp the tendency of attacks including attack targets and frequency. In the replay experiment, we use a dummy C&C server with accumulated C&C commands collected during the observation experiment so that we can replay the attacks to observe them in details. Moreover, in the replay experiment, we use bare-metal IoT devices to measure the volume of DoS attacks.

Keywords: DDoS attacks, IoT malware, dynamic analysis

1. はじめに

現在，世の中の様々なモノが通信機能を持ちネットワークに接続して相互に通信を行うようになってきている．IoT [1]（Internet of Things）とは，コンピュータなどの情報機器だけでなく，これらの様々なモノ（本稿ではIoTデバイスと呼称することとする）に通信機能を持たせ，ネッ

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

トワークを構成することで，そこから生み出される大量のデータを活用する技術である．インターネットに接続されるIoTデバイスは爆発的に増加しており，2020年には500億台に及ぶと予想されている．一方，IoTデバイスのセキュリティ対策は十分とはいえず，マルウェアに感染したIoTデバイスがDDoS攻撃（Distributed-Denial-of-Service Attack）[10]を行うケースが急増している[2], [27]．1 Tbpsを超える史上最大級のDDoS攻撃を引き起こしたIoTマルウェア「Mirai」[11]やその亜種[12]の多くもDDoS攻撃を行うことが知られている．文献[3]では，2016年第四半期に観測された100 Gbpsを超える大規模攻撃の数は，前年同四半期と比較して140%増加し，そのうち3件は300 Gbps以上の攻撃規模であり，マルウェアに感染したIoTデバイスがDDoS攻撃トラフィックの主な発信元であると報告されている．

このようにIoTマルウェアによるDDoS攻撃は社会的な問題になっているが，実際にIoTマルウェアに感染したIoTデバイスがどのような頻度でDDoS攻撃に悪用され，どのような流量の攻撃を発生するか，といった攻撃の実態については我々の知る限り詳細な報告がなされていない．そこで本研究ではIoTマルウェアによるDDoS攻撃の実態を分析するために，2016/10/13〜2017/05/16の期間にハニーポット[4], [5]で収集したIoTマルウェア検体の中でARM[6]，MIPS[7]，MIPSEL[8]の3種類のCPUアーキテクチャで動作する総計4,093検体をサンドボックス[32]内で実行し，その挙動を観測した．まず，解析環境においてIoTマルウェア検体を実際にC&Cサーバに接続し挙動の観測を行う観測実験を行った．検体実行後5分間のみ観測を行う短期解析の結果，4,093検体のうち99.4%にあたる4,070検体は，実行後，ただちにC&Cサーバと通信を試みるものの，わずかに1.6%にあたる65検体しかDoS攻撃の命令を受信せず，残りの検体は攻撃を開始しなかった．なお，後述のとおり，これらの検体の95.1%は実際にはDoS攻撃の機能を有していた．また，短期解析に加えて，検体実行後240時間以上にわたり挙動を観測する長期解析を行った結果，C&Cサーバとの接続を継続的に行おうとするが失敗し，3日以上経過した後，接続が成功し，その後DoS攻撃を開始した検体が1体確認された．このことから，IoTマルウェアがDoS攻撃命令を受信するのは感染直後とは限らず，継続的に観測を行う必要があるという知見を得た．また，観測実験においてSYNフラッド攻撃，UDPフラッド攻撃，HTTPフラッド攻撃を含む10種類の命令と対応する攻撃を観測した．

次に，観測されたDoS攻撃開始命令を用い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[9]を作成し，攻撃再現実験を行った．攻撃再現実験ではDoS攻撃を受信するための犠牲サーバ（図2のダミー攻撃対象サーバ）を用意することで，特にアプリケーションレイヤの攻撃についても詳細に観測できるようにした．その結果，アプリケーションレイヤにおけるDoS攻撃において利用されるHTTPメソッドの種別や，User Agentといったフィールドが偽装されることなど，攻撃の詳細が観測できた．また，観測実験時にはC&Cサーバから命令が届かずDoS攻撃を開始しなかった検体についても，ダミーC&Cサーバからの命令には反応し攻撃を開始しており，再現実験を行った143グループの検体のうち，95.1%がDoS攻撃の機能を有することが確認された．加えて，実際にIoTマルウェアに感染する脆弱性を有することが確認されている4種類の実機を用いた再現実験により，市場価格約3,000円程度の安価なWi-Fiストレージから最大約100 Mbpsの流量の通信が発生することを確認した．本研究の貢献を以下にまとめる．

- 実際のC&Cサーバ（以下，実C&Cサーバと呼ぶ）との接続による攻撃観測実験とダミーC&Cサーバによる攻撃再現実験の組合せにより，社会的な問題となっているIoTマルウェアによるDDoS攻撃の実態を観測・分析した．
- 攻撃再現実験においてサービス妨害攻撃を受信するための犠牲サーバを用意することで，特にアプリケーションレイヤのDoS攻撃の詳細観測を行う手法を示した．
- IoTマルウェアに感染する脆弱性を有する実機を用いて攻撃再現実験による攻撃の流量測定を行い，安価な機器であっても100 Mbps程度の通信を発生させられることを明らかにした．

2. 関連研究

これまで，動的解析によりマルウェアの挙動を観測する多くの研究が行われている．マルウェア検体を実行する動的解析環境のインターネット接続に関して，閉環境で解析を行う手法[19], [20], [21], [22], [23]，開環境および半開環境で解析を行う手法[24], [25], [26]がある．本研究では，iptables[14]を用いて通信をコントロールする半開環境でIoTマルウェアの動的解析を行う．文献[31]では，DDoSボットネットを静的解析し，C&Cサーバに接続するための疑似ボットクライアントを作成することでDoS攻撃命令を観測している．我々は疑似ボットクライアントではなく実際のマルウェア検体により観測を行うとともに，攻撃を犠牲サーバに転送することで攻撃の詳細を把握することを試みる．また，IoTマルウェアによるDoS攻撃の流量を測定するために実機による解析も行う．

また，DDoS攻撃の実態把握に関する研究として，文献[28], [29], [30]があげられる．文献[28], [29]は，近年のDDoS攻撃の特徴や傾向を検討した．文献[30]は，サイバー犯罪者が運営するDDoS攻撃代行サービスである“Booter”によるDDoS攻撃の実態調査をしている．具体

的には 14 種類の Booter サービスを利用し，攻撃時の流量観測を行うとともに，攻撃の特徴をまとめている．本研究では近年社会的な問題となっている IoT マルウェアによる DDoS 攻撃に注目している．

3. IoT マルウェアの動的解析による DoS 攻撃の観測と分析

3.1 概要

現在ルータやカメラといった多くの IoT デバイスがマルウェアに感染し，C&C サーバからの動作命令を受け，攻撃に利用されている [4], [5], [9], [11], [12]．そこで本研究では IoT 向けハニーポット [4], [5], [9] で収集した IoT マルウェア検体をサンドボックス内で実行し，DoS 攻撃の観測と分析を行う．ハニーポットによる IoT マルウェアの入手の流れを以下に示す（**図 1**）．

手順 1) 攻撃者の Telnet ログイン試行を受け入れる．

手順 2) 攻撃者から送られるシェルコマンドを解析し，マルウェアダウンロード用コマンドを抽出する．

手順 3) 上記の手順 2) で抽出したダウンロード用コマンドを実行し，IoT マルウェア検体を入手する．なお，IoT デバイスで使用される様々な CPU アーキテクチャに対応するため，攻撃者は各アーキテクチャに対してマルウェアバイナリを用意している．そのため，同一の Telnet 攻撃の観測により各 CPU アーキテクチャに対応した複数の検体が収集できる場合がある．このように同一の Telnet セッションから収集された検体の集合を特に検体グループと呼ぶこととする．

本研究は以下の 2 つを目的とする．

- 動的解析によってマルウェアが行う通信を観測し，攻撃対象や頻度など実際に発生している攻撃の傾向を把握する．
- 実際に IoT マルウェアに感染することが確認されている実機群を用いて DoS 攻撃の再現実験を行い，様々な DoS 攻撃の通信内容や流量などの詳細な分析を行い，IoT デバイスによる DoS 攻撃の実態を把握する．

具体的には以下に示す 2 つの手法を用いて実験を行う．

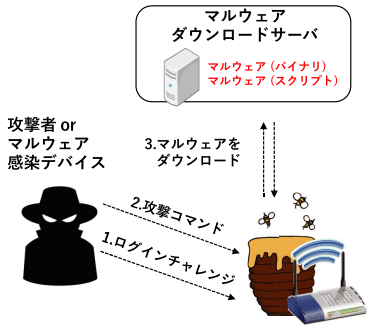


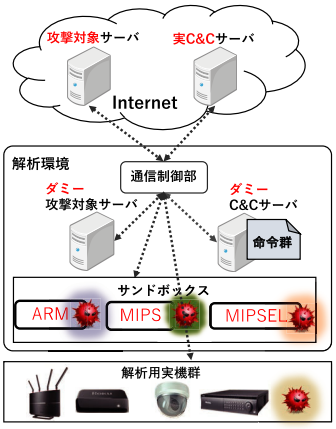
図 1 ハニーポットによるマルウェア入手方法
Fig. 1 IoT malware collection by honeypot.

- マルウェア検体を外部と通信できる環境で動的解析し，C&C サーバに接続させることでマルウェアが行う攻撃の観測を行う．なお，後述する方法で C&C 通信を判別し，C&C 以外の通信を遮断することで実際の攻撃がインターネットに流出しないようにする．
- 上の観測実験で得られた 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 サーバを作成し，これを用いた DoS 攻撃の再現実験を行う．さらに脆弱性を有する実機を用いて，実際に DoS 攻撃を行う際の通信流量を測定する．また，ダミー攻撃対象サーバを用意し，マルウェアからの DoS 攻撃を転送することで攻撃通信の詳細についても分析を行う．

3.2 解析環境

提案するマルウェア動的解析環境を**図 2** に示す．解析環境は通信制御部，マルウェアを動作させるサンドボックス（仮想環境），ダミー C&C サーバ，ダミー攻撃対象サーバ，解析用実機群から構成される．

通信制御部は，iptables [14] により実装する．観測実験と再現実験は異なる機能で通信制御を行った．観測実験の場合，マルウェアが外部ネットワークに対し攻撃を行うことを防止するため，hashlimit 機能を用いて，単位時間あたりに通信が許される外向きパケット数を制限する．再現実験の場合，ダミー C&C サーバを用いることで外部と通信を行う必要がないため，外部ネットワークへの通信はすべて禁止する．また，iptables の FORWARD および DNAT 機能を用いて，マルウェアからの実 C&C サーバへの通信をダミー C&C サーバに転送し，逆にダミー C&C サーバからの命令を実 C&C サーバからの命令としてマルウェア側に転送する．同様に，攻撃対象サーバに対する DoS 攻



解析環境スペック				
	OS	CPU	Memory	HD
解析環境	Ubuntu 14.04	Intel(R) Core(TM) i5-3317U CPU @ 1.70GHz	4GB	120G
ARM/MIPS/MIPSEL	Debian 7.3	QEMU	124MB	24GB

図 2 マルウェア解析環境
Fig. 2 Malware analysis environment.

撃を実行中のマルウェアが行った場合，通信制御部はマルウェアから攻撃対象への通信（大量のパケットなど）をダミー攻撃対象サーバに転送し，逆にダミー攻撃対象サーバからの応答を攻撃対象からの応答としてマルウェア側に転送する．

サンドボックスでは ARM，MIPS，MIPSEL の 3 つの CPU アーキテクチャをエミュレートしており，OS はそれぞれフリーの Linux ディストリビューションである Debian [13] が動作している．多くのアーキテクチャ向けにリリースされている Debian を用いることで，今後異なる CPU アーキテクチャ向けにサンドボックスを拡張することも可能である．

ダミー C&C サーバは実 C&C サーバの挙動を模擬した Python [15] スクリプトである．

ダミー攻撃対象サーバの実体は，Apache v2 であり，HTTP フラッドの場合の攻撃通信の転送先とすることで，ウェブサーバがどのような DoS 攻撃を受けたのかを明らかにする．特に攻撃対象サーバとセッションを確立するアプリケーションレイヤの DoS 攻撃の観測に利用する．

解析用実機群は，4 種類の脆弱性を有する IoT デバイスである．具体的なデバイス情報は**表 1** に示す．再現実験により，実際に発生する DoS 攻撃の流量を測定する．

長期解析実験では，同一期間中に複数のマルウェア検体を同時並列的に解析する必要があるため，多数のサンドボックスが必要となる．そのため，図 2 の解析環境におけるサンドボックスとして**図 3** に示す並列解析環境を用意する．並列解析環境には，15 の仮想 MIPS サンドボックスと 15 の仮想 ARM サンドボックスがある．互いの干渉を防ぐために，図 3 のように，1 つのサンドボックスが 1 つの仮想インタフェースと仮想ブリッジを用いて独立したローカルネットワークに接続する．30 個のサンドボックスにはそれぞれ違うセグメントの IP アドレスを割り当てる．また，長期解析環境は 1 つのグローバル IP アドレスでインターネットと通信する．

表 1 解析用の実機情報
Table 1 Information of bare-metal IoT devices.

機種	CPUアーキテクチャ	価格情報
Wi-Fi ストレージ1	MIPSEL	約3,000円
Wi-Fi ストレージ2	MIPSEL	約6,000円
ルータ	MIPS	約12,000円
IPカメラ	ARM	約40,000円

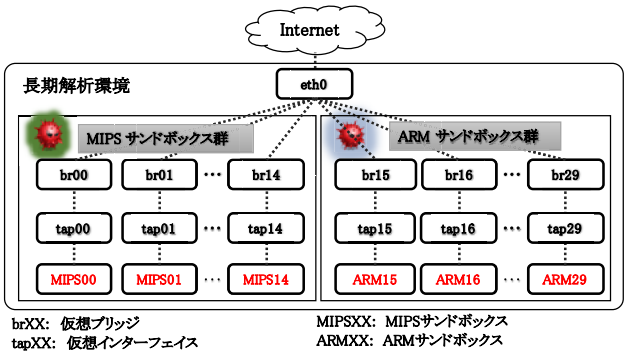


図 3 長期解析環境
Fig. 3 Long-term malware analysis environment.

4. 実験

4.1 実験概要

本研究で行う観測実験とダミー C&C サーバを用いた攻撃再現実験の 2 つの実験の流れについて説明する．

観測実験の手順：

1) マルウェア検体の CPU アーキテクチャに対応するサンドボックスを使用してマルウェアを実行し，通信ログの記録を開始する．通信ログは pcap ファイルの形式で図 2 の解析環境内で記録する．

2) マルウェアを 5 分間動作させる短期解析と 240 時間以上の長期解析を行う．

3) 仮想マシンの解析環境をスナップショット機能で，初期状態に戻し，通信ログの記録を終了する．

再現実験の手順：

1) 観測実験で実 C&C サーバから受信した攻撃コマンドをダミー C&C サーバ用の命令群として蓄積する．マルウェア実行後，実 C&C サーバとの通信をダミー C&C サーバに転送するように，通信制御部のフォワーディング設定を行う．

2) HTTP フラッドなどのウェブ系攻撃を再現する場合は，通信制御部で攻撃トラフィックをダミー攻撃対象サーバに転送するように設定する．

3) マルウェアの CPU アーキテクチャに対応したサンドボックスあるいは実際の IoT デバイスを使用してマルウェアを実行し，通信ログを pcap ファイル形式で解析環境内に記録開始する．

4) ダミー C&C サーバが実行したい攻撃コマンドをマルウェアに送信し，短時間（1 分間）動作させる．

5) 仮想マシンの解析環境をスナップショット機能で，初期状態に戻し，通信ログの記録を終了する．実機群については電源再起動を行う．なお，実験で用いた実機群はいずれも読み取り専用ファイルシステムを有しており，電源再起動によりマルウェア検体のプロセスおよびファイルなどは消去される．

IoT 向けハニーポットにより収集した検体を用いて以上の 2 つの実験を行うことで，マルウェアの挙動を観測し，実 C&C サーバの情報，実 C&C サーバの挙動やマルウェアが行うポートスキャンや DoS 攻撃などの詳細な挙動の分析をする．また，再現実験では，仮想環境および実機で DoS 攻撃時の通信流量を測定する．実機（表 1）を用いた調査により，実際の機器の攻撃能力を把握することで想定される攻撃の深刻度をより正確に推定することを目的とする．

4.2 実験用マルウェア検体

IoT 向けハニーポット [4], [5], [9] によって 2016/10/13〜2017/05/16 の間に入手した 16,724 マルウェア検体のうち，対応する CPU アーキテクチャが ARM，MIPS，MIPSEL の 3 種類である総計 4,093 検体（24.5%）を実験対象とする．短期解析は全マルウェア検体に対して 5 分間ずつ行う（サンドボックス数の制限で，長時間解析ができなかったため）．なお，2016/10/13〜2017/01/12 の期間に収集した 3,239 検体については，収集後 1 週間以内に短期解析を行ったが，2016/10/13〜2017/05/16 の期間に収集した 854 検体については，収集後 10 分以内に動的解析を行った．重複期間中で収集した検体に対して 2 種類の方法で解析した．また，マルウェアの長期的な挙動を観測するため，長期解析を 2017/04/30〜2017/05/11 の期間で行い，この期間に収集された検体のうち，対応する CPU アーキテクチャが ARM，MIPS のいずれかであった 19 検体を解析対象とした．

次に再現実験では，2016/10/31〜2016/12/18 と 2017/01/01〜2017/05/16 の期間に収集された 143 の検体グループからそれぞれランダムに 1 つずつ選んだ代表検体 143 体に対して，観測実験で観測した攻撃命令を送り挙動を確認した．解析対象検体の収集時期，解析時期，行った解析の種類を**表 2** にまとめる．

アンチウィルスソフト Dr.WEB [16] によるマルウェア検体のスキャン結果を**表 3** に示す．表 3 のとおり，実験に利用した検体には大きな偏りがあり，多くの検体が BASHLITE ファミリ [34] に属しているが，これは検体を収集した IoT 向けハニーポットの実装に大きく依存している．我々が用いる IoT 向けハニーポットは多数の IP アドレスを用いて動作するエミュレータベースのものと限られた IP アドレスを用いて動作する実機ベースのものからなる．実機ベースのハニーポットは多様な検体を収集できる反面，定期的なリブートが必要であり，多数の TCP セッションを同時に処理できないといった制約から検体収集効率が悪いという特徴がある．一方，エミュレータベースのハニーポットは対応可能なセッション数が大きく同時に多数のホストからの攻撃を観測できる一方，エミュレーションの限界から収集できるマルウェアの種類に限りがある．本実験では，収集された検体の偏りの調整は行わず，検体収集期間に収集されたすべての検体を短期解析する．

表 2 実験対象のマルウェア情報
Table 2 Information of malware samples.

解析対象検体数	収集時期	解析時期	解析種類
3239	2016/10/13〜2017/01/12	2016/10/13〜2017/01/12	短期解析
854	2016/10/13〜2017/05/16	2016/10/13〜2017/05/16	短期解析（即時）
19	2017/04/28〜2017/04/30	2017/04/30〜2017/05/11	長期解析
113	2016/10/31〜2016/12/18	2016/12/04〜2016/12/07	再現実験
30	2017/01/01〜2017/05/16	2017/08/15〜2017/08/16	

表 3 実験対象のマルウェア検体の検知名
Table 3 Detected names of malware samples.

検知ファミリ名	検知した検体数	パーセンテージ
BASHLITE	3973	97.1%
Mirai	47	1.1%
tsunami	22	0.5%
Remaiten	7	0.2%
検知されず	44	1.1%

4.3 観測実験の結果

短期解析の結果，全 4,093 検体のうち，897 検体から Telnet スキャン，46 検体から DoS 攻撃の通信を観測した．また，32 検体から Telnet スキャンと DoS 攻撃の両方の通信を観測した．また，長期解析の結果，全 19 検体のうち，8 検体からも Telnet スキャンと DoS 攻撃の通信を観測した．以下では，まず短期解析に関して C&C サーバの判定，観測した攻撃コマンドの分析，DoS 攻撃の対象についてそれぞれ説明する．次に 4.3.4 項で長期解析の結果について説明する．

4.3.1 C&C サーバの判定

一般に未知のマルウェアの動的解析の結果のみから C&C サーバの判定を自動で行うことは困難である．そこで本研究では，関連研究 [4] により観測済みの C&C 命令や，Telnet，TR-069/TR-064 などの脆弱サービスへのスキャンといった既知の IoT マルウェアの挙動情報を参考に，以下のとおり，半自動で C&C サーバの判定を行った．下記の判定手順は，BASHLITE，Mirai，tsunami ファミリに（表 3）有用と考えられる．

手順 1) 動的解析時のマルウェアとの通信に，既知の攻撃命令パターンが含まれる場合，通信相手を C&C サーバと判断する．具体的には，各パケットのペイロードの先頭 “!* ” が含まれる場合，BASHLITE ファミリの攻撃命令として認識する．また，ペイロードに “irc.” や “NOTICE”，“Looking up your hostname” が含まれる場合，tsunami ファミリの C&C 通信トラフィックと判定する．そのような通信が存在しない場合，手順 2) を行う．

手順 2) TCP の宛先ポートが，スキャン対象ポートとして頻繁に使われる 23，2323，7547 ポート以外である場合，それを C&C サーバ候補と判断する．それ以外は手順 3) を行う．

手順 3) 上記の手順 2) で C&C サーバ候補とならなかった通信，すなわち，頻繁にスキャン対象となるポートへの通信については，スキャンであるか C&C 通信であるかを判別する必要がある．まずは，Mirai ファミリに属するマルウェアによるスキャンを除外する．Mirai ファミリマルウェアのスキャンパケットは TCP シーケンス番号が Telnet スキャン先の IP アドレスと一致する特徴がある [35]．具体的には，IP アドレスが “A.B.C.D” であった場合，シーケンス番号は “ $A*256^3+B*256^2+C*256+D$” と一致する．

また，一般にスキャンは攻撃先を探索するために多数のホストに対して行うものであるのに対して，C&C 通信は特定の C&C サーバ群と行うものであるため，スキャン通信に比べて各宛先への通信頻度が高いことに着目する．通信先 IP アドレスごとに送信した TCP のパケット数をカウントし（オペレーティングシステムによる再送するトラフィックはシーケンス番号が同じなので，カウントしない），2 パケット以上の IP アドレスを C&C サーバ候補と判定する．また，導通テスト用のもの（baidu.com，google.com など）を事前に作成したホワイトリストを用いて除外する．対象となるすべての IP アドレスから C&C サーバ候補が見つからなかった場合，C&C サーバなしと判断する．

手順 4) 上記の手順 2)，手順 3) で C&C サーバ候補となった IP アドレスへの通信について，マニュアルで通信内容を確認し，ペイロードの内容から C&C サーバであるかを判定する．

手順 2) で抽出した C&C サーバ候補は 57 個，手順 3) で抽出した候補は 61 個であった．この合計 118 個の候補についてすべてマニュアルで確認し，いずれも C&C サーバであると判別した．短期解析で 4,093 検体を解析した際に観測された通信に対して上記の判定を行った結果，552 個の IP アドレスが C&C サーバとして判別された．これらのサーバは，主にアメリカ，次にオランダに集中していた（**表 4**）．また，IP2LOCATION [33] を用いて，C&C サーバの AS 種類を確認した結果，ほとんどの C&C サーバはホスティングサービスを利用していることが分かった（**表 5**）．また C&C サーバの分布には大きな偏りがあり，同一 IP アドレスレンジに集中して存在する場合が目立つことが分かった．同一 IP アドレスレンジに存在する C&C サーバの IP アドレス数の上位 10 の情報を**表 6** にまとめる．また，同一 IP アドレスレンジに存在する C&C サーバ数が 2 以上のレンジの分布情報を**図 4** に示す．

表 4　C&C サーバの国情報
Table 4　Country information of C&C servers.

TOP5	国コード	C&Cサーバの数	パーセンテージ
1	US	324	58.7%
2	NL	67	12.1%
3	RO	44	8.0%
4	FR	15	2.7%
5	UA	12	2.2%

表 5　C&C サーバの AS 情報
Table 5　AS information of C&C servers.

AS種類	C&Cサーバの数	パーセンテージ
HOSTING	527	95.5%
ISP	16	2.9%
OTHERS	1	0.2%
UNKNOWN	8	1.4%

4.3.2　観測した攻撃コマンド

今回の短期解析実験では，C&C サーバから 13 種類の Telnet スキャン攻撃命令と 10 種類の DoS 攻撃命令を受信した．Telnet スキャンを行った検体は 21.9%にあたる 897 体であり，DoS 攻撃を行ったのは 1.1%にあたる 46 検体であった．観測した Telnet スキャンの動作命令を**表 7**，DoS 攻撃の動作命令を**表 8** にまとめる．

表 6　同一 IP アドレスレンジにある C&C サーバの情報
Table 6　Information of C&C servers in the same IP range.

TOP10	IPアドレスレンジ	国コード	数
1	208.67.1.0/24	US	24
2	198.167.140.0/24	US	18
3	107.178.96.0/24	US	18
4	89.34.97.0/24	RO	17
5	89.34.99.0/24	RO	15
6	50.115.166.0/24	US	15
7	93.158.200/24	NL	12
8	23.94.97.0/24	US	11
9	50.115.165.0/24	US	9
10	185.61.138.0/24	UA	9

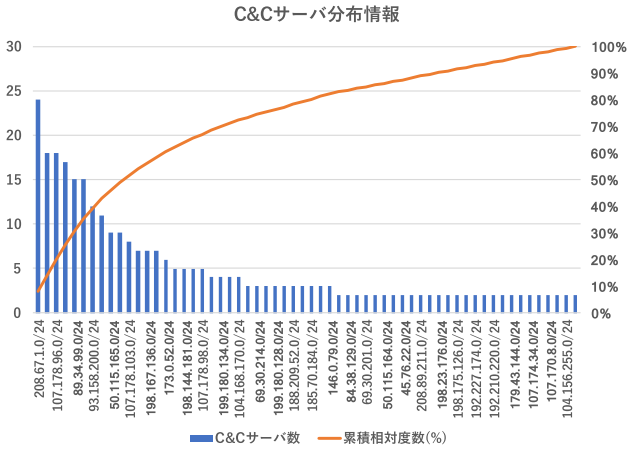


図 4　同一 IP アドレスレンジ C&C サーバの分布情報
Fig. 4　Distribution information of C&C servers in the same IP range.

表 7　観測した Telnet スキャンの動作命令の一覧
Table 7　Observed Telnet scan attack commands.

スキャン開始の動作命令	命令を受信した検体数
!* SCANNER ON	951
!* SCAN <parameter>	37
!* TELNET_SCAN ON	22
!* TELNET	25
!* SCANNER	20
!* TELNET ON	8
!* QTELNET <parameter>	3
!* TELNET_SCANNER ON	3
!* SCAN ON	3
!* IPCAM_SCANNER ON	3
!* NETIS_SCANNER ON	3
!* QTELNET ON	1
!* QSCAN <parameter>	1

表 8 観測した DoS 攻撃の動作命令一覧
Table 8 Observed DoS attack commands.

プロトコル	Dos攻撃の開始動作命令	命令を受信した検体数
HTTP	!* HTTPFLOOD POST <target IP/domain> <port> /<UNKNOWN> <duration>	1
HTTP	!* HTTP <target IP/domain> POST <port> /<UNKNOWN> <duration>	1
HTTP	!* HTTP GHP <target IP/domain> <port>/<UNKNOWN> <duration>	1
HTTP	!* HTTP <target IP/domain> <port> <duration>	2
HTTP	!* SMARTHTTPFLOOD GET <target domain> <port> /<UNKNOWN> <duration>	4
TCP	!* TCP <target IP/domain> <port> <duration> <netmask> <tcp flag> <packet size> <poll interval>	8
TCP	!* HOLD <target IP/domain> <port> <duration>	1
TCP	!* COMBOFLOOD <target IP/domain> <port> <duration>	1
UDP	!* STD <target IP/domain> <port> <duration>	18
UDP	!* UDP <target IP/domain> <port(0 for random)> <duration> <netmask> <packet size> <poll interval>	28

観測した Telnet スキャンのスキャン対象の IP アドレスの決定法は大きく分けて 3 種類存在した．1 種類目はスキャン対象 IP アドレスが 1.1.1.1，2.2.2.2 から始まり，254.254.254.254 までスキャンした後，それぞれのオクテットにランダムな数が割り当てられ，これらの数に 1 ずつインクリメントしたアドレスに対してスキャンを行った．たとえば，ランダムに 97.5.133.145 と決定されると，次のアクセス先は 98.6.134.146 といった具合である．また，いずれかのオクテットが 254 に達すると，同様にそれぞれのオクテットにランダムな数が割り当てられた．2 種類目はランダムに選んだ IP アドレスに対してスキャンを行う検体が確認された．3 種類目はある /24 ネットワークをスキャンし，これが終了するとまた別の /24 ネットワークをスキャンする検体が確認された．このスキャン対象ネットワークは実行時によって異なっており実行時に内部生成されていると思われる．

DoS 攻撃の動作命令を受け取って，そのマルウェアに感染した機器が攻撃を始めるのが一般的な IoT デバイスによる DoS 攻撃の流れである．今回動的解析した総計 4,093 検体のうち，DoS 攻撃を行った 46 検体はすべて C&C サーバから攻撃先の IP アドレス，ポートおよび攻撃の手法などが平文で明確に示されたフォーマットの命令を受け取っていた．1 つの検体に対して DoS 攻撃の命令が複数同時に送られる場合もあった．具体的にはそれぞれ 10 種類の DoS 攻撃の動作命令を観測した．表 8 はこれらの結果をまとめたものである．<target IP/domain> は攻撃対象の IP アドレスあるいはドメイン，<port> は攻撃対象のポート番号（0 の場合ランダム値），<duration> は攻撃継続時間（秒）である．<netmask> は攻撃パケットの送信元 IP アドレスをどのネットワーク範囲まで偽装するかを指定するパラメータである．<tcp flag> は TCP パケットのヘッダの中の FLAG の値，all なら送付するパケットの FLAG 位は fin，syn，rst，psh，ack の値がすべて 1，syn の場合，SYN フラッドになる．<packet size> はパケットのデータのサイズで，<poll interval> はポーリング間隔時間である．

最も頻繁に観測されたのは UDP プロトコルをベースとした DoS 攻撃であり，特定の攻撃対象 IP アドレスとポートに対して大量の UDP パケットを送付し，帯域を圧迫するものであった．一方，命令を受信した検体数は限られるものの，攻撃対象と TCP セッションを確立し，HTTP リクエストを送信することでサーバの負荷を高めるアプリケーションレイヤの DoS 攻撃命令も 5 種類観測した．

表 9 DDoS 攻撃対象の国情報
Table 9 Country Information of DDoS attack targets.

国コード	数	パーセンテージ
US	30	62.5%
CA	4	8.3%
NL	3	6.3%
GB	3	6.3%
UNKNOWN	2	4.2%
NZ	1	2.1%
IT	1	2.1%
ES	1	2.1%
CZ	1	2.1%
BZ	1	2.1%
AU	1	2.1%

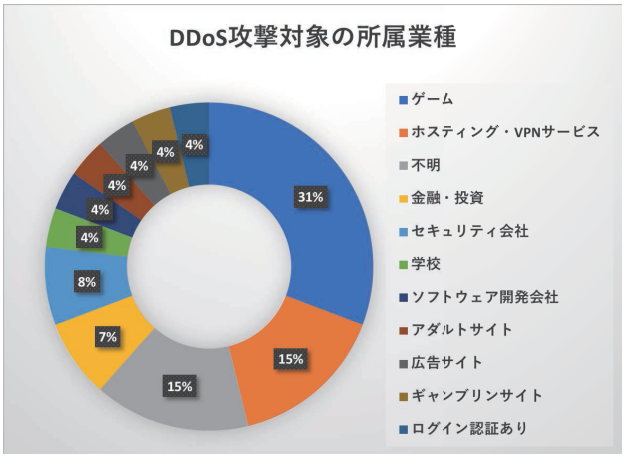


図 5 DDoS 攻撃対象の所属業種
Fig. 5 Industry types of DDoS attack targets.

4.3.3 DDoS 攻撃の対象

短期解析では，DDoS 攻撃の対象として 44 IP アドレスと 4 ドメインを観測した．パッシブ DNS データベース DNSDB [17] および位置情報を取得する GeoIP [18] を用いて，攻撃発生時の攻撃対象 IP アドレスに対応するドメイン（付録 A.3），国情報（**表 9**）を調べた結果，攻撃対象がアメリカに集中していることが分かった．また，DNSDB で得られたドメイン情報を調査し，攻撃対象の所属業種を調査した（**図 5**）．その結果，ゲーム系が最も攻撃を受けており，それ以外にも，ホスティング・VPN サービスプロバイダ，ソフトウェア開発会社，学校まで幅広く攻撃対象となっていることが分かった．攻撃先のポート番号から見ると，最も多く攻撃されたのは HTTP で標準的に使われている 80 番ポートであり，62 回のうち 34 回観測された．また DNS で使われている 53 番ポート，Xbox で使われている 3074 番ポートおよび emWave Message Service で使われている 20480 番ポートもそれぞれ 6 回観測された．

4.3.4 長期解析結果

長期解析で得られた通信に対して 4.3.1 項で示した方法と同様に C&C サーバ判定を行った結果，13 個の IP アドレスを C&C サーバとして判定した．このうち，11 個は短期解析により得られた IP アドレスと重複していた．

長期解析を行った 19 マルウェア検体（付録 A.1）のうち，10 検体は C&C サーバに接続し攻撃命令を受け取っていた．このうち，解析期間に Telnet スキャンまたは DoS 攻撃が発生した 8 検体について，スキャン対象および DoS 攻撃対象の IP アドレス数の時間推移を**図 6** に示す．8 検体のうち 6 検体については，解析開始後すぐに C&C サーバとの接続に成功し，スキャンまたは DoS 攻撃のどちらか，または両方を開始しているが，malware01 と malware15 は同一の C&C サーバへの接続を試み，3 日後に初めて接続に成功している．なお，最初に C&C サーバに接続したのは malware01 であり，あとから接続した malware15 は，1 度だけ DoS 攻撃命令を受けた後，マルウェアプロセスを停止するコマンド “!* LOLNOGTFO” を受信し，その後，DoS 攻撃命令を受信しなかった．これは malware01 と malware15 が共通のグローバル IP アドレスで同一の C&C サーバに接続していたため，後から接続した malware15 が攻撃者による操作の対象とならなかったためと思われる．図 6 に示すとおり malware01 は C&C サーバに接続してからさらに 4 日程度してから DoS 攻撃命令を頻繁に受信するようになり，最大で 1 日 30 もの宛先に DoS 攻撃を試みている．

また，malware05，malware08，malware10 はいずれも解析開始直後に DoS 攻撃命令を頻繁に受信しているものの，その後，攻撃命令が届かなくなっている．逆に，malware03 は C&C サーバへの接続は解析開始直後から成功しているものの，DoS 攻撃命令は 3 日後に初めて届いている．このように，DoS 攻撃命令が届くタイミングは各感染ホストによって様々であり，特に解析開始直後に集中するわけではないことが分かった．このことから，動的解析により DoS 攻撃を観測する場合には，長期的な観測が必要といえる．

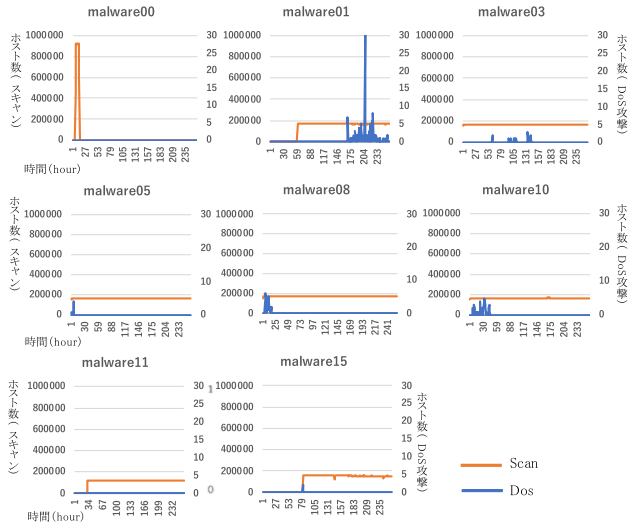


図 6 攻撃を行ったマルウェア検体の長期解析結果

Fig. 6 Long-term dynamic analysis results of malware samples that had attack behavior.

4.4 再現実験の結果

4.4.1 ダミー動作命令の有効性の検証

ダミー動作命令の有効性を検証するため，各ダミー命令を観測した元のマルウェア検体を解析対象として，ダミー動作命令を送付し，DoS 攻撃を行うことを確認した．その結果，表 8 に示す 10 種類の中，7 種類のダミー動作命令の有効性が確認された．容易に C&C になりすませることから，実験対象のマルウェアは C&C サーバの認証を行っていないと考えられる．

4.4.2 マルウェア検体が全種類の DoS 攻撃の動作命令に対する反応の観測

観測実験において 4,093 検体のうち DoS 攻撃を観測したのは全体の約 1.12%にあたる 46 検体であった．これ以外の検体が DoS 攻撃を行う機能を有しているかを確認するため，4,093 検体の中でも特に 2016/10/31～2016/12/18 と 2017/01/01～2017/05/16 の期間に入手した検体グループ 143 個からランダムに代表検体を 1 つずつ選び，4.4.1 項で有効性を確認した 7 種類のダミー命令をそれぞれ送り挙動を確認した．結果を**表 10** に示す．

総計 143 検体グループのうち，TCP フラッド命令および UDP フラッド命令に対してそれぞれ 136 グループと 135 グループの検体が DoS 攻撃を開始した．このことから，観測実験では DoS 攻撃を行わなかった多くの検体が実際には DoS 攻撃機能を有していることが分かる．

4.4.3 HTTP フラッド系の DoS 攻撃の実験結果

HTTP フラッド関係の動作命令を受け攻撃を行ったグループの割合はおよそ 10%程度であった．表 3 に示すとおり，ウイルス対策ソフトによる検知結果からは実験対象の検体の大部分は BASHLITE ファミリに属すると判定されているが，解釈可能な命令には差があり，すべての BASHLITE ファミリが HTTP フラッドなどのアプリケーションレイヤでの DoS 攻撃に対応しているわけではないことが推測される．

表 10 各ダミー命令に対する検体グループの反応

Table 10 Responses of dummy attack commands.

ダミー動作命令	命令対応した検体グループ数	パーセンテージ
!* TCP <dummy target IP> 80 30 320 all 1024 1	136	95.1%
!* UDP <dummy target IP> 80 100 32 100 10	135	94.4%
!* STD <dummy target IP> 80 60	74	51.7%
!* HTTPFLOOD GHP <dummy target domain> 80/60 750	14	9.8%
!* HTTPFLOOD POST <dummy target IP> 80 / 150 300000	18	12.6%
!* HOLD <dummy target IP> 80 30	69	48.3%
!* HTTP <dummy target domain> 20	30	21.0%

表 11 各ダミー命令に対するマルウェアの攻撃特徴
Table 11 Features of dummy attack commands.

ダミー動作命令	HTTPメソッド	User-Agentの多様化	connection
1) !* HTTPFLOOD POST <dummy target IP>	POST	YES	close
2) !* HTTP <dummy target domain> 20	GET	NO	keep-alive
3) !* HTTPFLOOD GHP <dummy target domain> 80/60 750	GHP	YES	close

ダミー C&C サーバから送信した動作命令と，その命令に対するマルウェアの攻撃の特徴について**表 11** にまとめる．「HTTP メソッド」列はマルウェアが HTTP 通信を行う際に使用したメソッド，「User-Agent の多様化」列はアクセスの際に多数の User-Agent を用いる挙動がみられたかを表している．また，「connection」列は TCP 接続の開放がされているかどうかを表している．

HTTP メソッドとしては，POST，GET に加えて GHP というメソッドが指定されていたが，これは HTTP プロトコルにおいて存在しないメソッドである．POST メソッドを用いる表 11 の 1) の攻撃では，POST とともに本来送られるはずのデータが存在していなかった．また，表 11 の 1)，3) の攻撃では多様なブラウザからのアクセスに偽装するため User-Agent が多様化されていた．以下にその一例を示す．

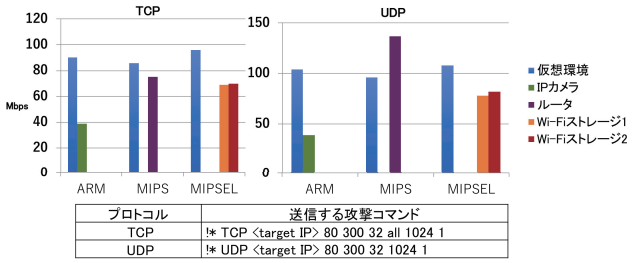
1. Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; uZardWeb/1.0; Server_JP)
2. Opera/9.80 (X11; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16
3. wii libnup/1.0
4. BlackBerry7520/4.0.0 Profile/MIDP-2.0 Configuration/CLDC-1.1 Doris/1.15 [en] (Symbian)

上記を含めて全部で 36 種類の User-Agent 情報を観測した．なお，User-Agent 情報は偽装されているものの，当該通信を構成するパケットの初期 TTL 値はすべて Linux システムや MacOS などのデフォルト TTL 値である 64 に固定されており，Uger-Agent 情報に含まれる OS 情報と一致しない場合も多いため，これを基に偽装を見破り攻撃を検知できる可能性がある．表 11 の 2) では User-Agent がファイル取得用コマンド wget と同様になっており多様化は行われていなかった．また connection の部分は Keep-Alive 状態で，検体はダミーウェブサーバと 3 ウェイハンドシェイクによるセッション確立後，一度だけ GET メソッドを送信し，その後，正常にセッションを終了していた．

4.4.4 実機を用いた DoS 攻撃通信流量の測定

機器による攻撃通信流量の比較

表 1 で示す 4 種の IoT デバイスと，それらのデバイスと共通の CPU アーキテクチャに対応する仮想環境（スペックは図 2 を参照）において，特定の検体（付録 A.2）を実行し，TCP フラッドと UDP フラッド攻撃命令を送信し，発生させた攻撃の通信流量を観測した結果を**図 7** に示す．この結果から，まず仮想環境においては CPU アーキテクチャによる DoS 攻撃の流量について大きな違いは見られなかった．これに対して実機環境では機種ごとに大きな差



プロトコル	送信する攻撃コマンド
TCP	!* TCP <target IP> 80 300 32 all 1024 1
UDP	!* UDP <target IP> 80 300 32 1024 1

図 7 Dos 攻撃時の通信流量
Fig. 7 Flow rate of communication when Dos attack occur.

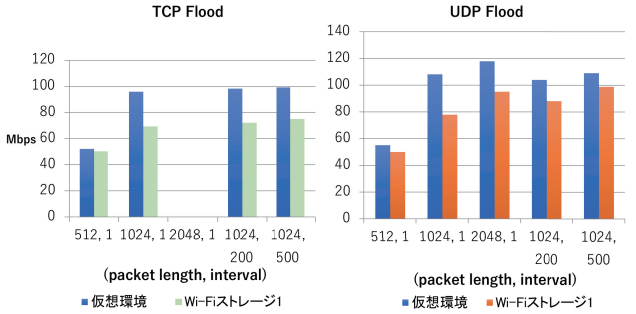


図 8 パケット長とパケット送信インターバルに変更を加えた命令で攻撃時の通信流量
Fig. 8 Flow rate of communication when using different 'packet length' or 'poll interval' Dos attack command.

が見られ，最も高価な IP カメラは，ルータや Wi-Fi ストレージの半分程度の流量しか発生させなかった．特にネットワーク機器であるルータによる UDP フラッドの流量が大きく，100 Mbps を超えていた．これは，当該ルータのみが 1 Gbps までの通信に対応した 1000 BASE-T 規格を備えており，そのほかの機器については最大 100 Mbps までの通信に対応している 10/100 BASE-TX 規格を備えていることに関連すると考えられる．

命令のチューニングによる攻撃通信流量の比較

観測実験によって得た DoS 攻撃の動作命令（表 8 参照）に対して，攻撃通信流量に直接的に関連すると考えられるパラメータである <packet size>，<poll interval> について観測時とは異なる 10 種類の値（**図 9**）を設定した．

この 10 種の命令を，MIPSEL で動作する Wi-Fi ストレージ 1 において実行したマルウェア（付録 A.2）に対して送信し，攻撃の流量を観測した．実験結果を DoS 攻撃命令の種類ごとにまとめたものを**図 8** に示す．特に，packet length が 1,024，poll interval が 500 の場合に，100 Mbps 程度の高い流量を示している．このように数千円程度の安価な機器であっても，100 Mbps という高い流量を発生させ得ることが確認できた．

5. 考察

今回の一連の実験により，ハニーポットなどで収集した IoT マルウェア検体を短期間動的解析するだけでは，ほとんどの検体は DoS 攻撃命令を受信せず，IoT マルウェアに

```
!* TCP <target IP address>80 300 32 all 512 1
!* TCP <target IP address>80 300 32 all 1024 1
!* TCP <target IP address>80 300 32 all 2048 1
!* TCP <target IP address>80 300 32 all 1024 200
!* TCP <target IP address>80 300 32 all 1024 500
!* UDP <target IP address>80 300 32 all 512 1
!* UDP <target IP address>80 300 32 all 1024 1
!* UDP <target IP address>80 300 32 all 2048 1
!* UDP <target IP address>80 300 32 all 1024 200
!* UDP <target IP address>80 300 32 all 1024 500
```

図 9 パラメータ種類一覧
Fig. 9 Parameter type list.

よる DoS 攻撃は十分に観測できないことが分かった．このため，長期動的解析により観測を行う方法が考えられるが，長期解析では解析中サンドボックスを占有するため，観測のコストが増加する．そのため，C&C サーバの接続可否のみを定常監視する機能と組み合わせて，C&C サーバが活動状態にある検体を優先的に解析するなど，限りあるサンドボックスを有効活用する方法が考えられる．また，外部接続に用いるグローバル IP アドレスを複数のサンドボックスが共有する場合は，C&C サーバから接続拒否されないように，複数検体が同一の C&C サーバに接続しないような検体の選別が重要といえる．今回は長期解析を手動で行っていたが，今後 IoT マルウェアがさらに増えていくと考えられるため，マルウェアの長期解析を自動化することが必要である．なお，評価実験で用いた C&C サーバの判定手法は，既知の C&C 通信の特徴や C&C 通信の候補に対してマニュアルでの確認をしていることから，誤検知の可能性は低いと考えられるが，C&C サーバとの通信が確立されていない場合には，見逃しが発生する恐れがある．これは，詳細な静的解析を行わずに通信内容のみから C&C サーバの判定を行う提案手法の限界といえる．

また，前述のとおり，今回の実験では，ハニーポットで収集された検体に対して特にマルウェアファミリの偏りを緩和するような調整を行わなかったが，様々なマルウェアファミリの活動を観測するためには，動的解析対象の検体の種類に基づく選定方法も重要となる．

今回の実験では，動的解析時に観測した DoS 攻撃通信はいずれも検知が容易な平文の C&C 命令により行われていたが，今後は C&C 通信が暗号化され，単純なパターンマッチなどでは攻撃命令の識別が難しくなることが考えられる．しかし，その場合でも，今回の実験結果が示すとおり，通常の C&C サーバとの連絡通信（たかだか数百キロバイト）や他の脆弱性ある IoT デバイスの探索（たかだか数十メガバイト）と比べ，DoS 攻撃の通信量は 5 分間で百メガバイトを超え，場合によって，1 ギガバイトを超えており，マルウェア動的解析時の通信量から DoS 攻撃の頻度や対象を調査するアプローチは，一定の有効性が保たれると予想される．

攻撃者は，仮想マシン検知などによりサンドボックスを検知し，観測を回避する可能性がある．そのような解析回避に対しては，本研究でも実施した実機による動的解析が有効となりうる．また，動的解析環境からは実際に DoS 攻撃の通信が外部に送信されることをブロックしているため，攻撃者はこのような通信制御の有無を確認することで解析環境を検知する可能性がある．そのような攻撃者による解析環境の検知の実態調査については今後の課題としたい．

6. まとめと今後の課題

本研究では，実際に IoT マルウェアを C&C サーバに接続し，攻撃の観測を行う観測実験と C&C サーバからの応答を蓄積したダミー C&C サーバを用いた攻撃再現実験を行った．前者の観測実験により，DoS 攻撃の観測には一定期間の動的解析による観測が必要であることが分かった．また，後者の再現実験により，大多数の IoT マルウェア検体は DoS 攻撃機能を有していることや，アプリケーションレイヤの DoS 攻撃の実態が把握できた．また，実機での再現実験により低価格の IoT デバイスでも，100 Mbps 程度の攻撃トラフィックを生成できることを確認した．

謝辞 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．本研究成果の一部は，国立研究開発法人情報通信研究機構（NICT）の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」により得られた．

参考文献

[1] Gubbi, J. et al.: Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Generation Computer Systems*, Vol.29, No.7, pp.1645–1660 (2013).
[2] Lucian Constantin IDG News Service：IoT 機器を踏み台にした史上最大規模の DDoS 攻撃が続々発生，入手先 ⟨http://itpro.nikkeibp.co.jp/atcl/idg/14/481542/092800277/⟩（参照 2017-07-21）.
[3] akamai の［インターネットの現状］/セキュリティ，入手先 ⟨https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-executive-summary.pdf⟩（参照 2017-07-21）.
[4] Pa, Y.M.P. et al.: IoTPOT: Analysing the Rise of IoT Compromises, *9th USENIX Workshop on Offensive Technologies* (*WOOT 15*), USENIX Association (2015).
[5] 鈴木将吾ほか：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，研究報告セキュリティ心理学とトラスト（SPT），pp.1–6 (2016).
[6] ARM，入手先 ⟨https://www.arm.com/ja/⟩（参照 2017-07-21）.
[7] MIPS Processors - Imagination Technologies, available from ⟨https://imgtec.com/mips/⟩ (accessed 2017-07-21).
[8] MIPSel- Wikipedia, available from ⟨https://de.wikipedia.org/wiki/MIPSel⟩ (accessed 2017-07-21).
[9] 中山 颯ほか：IoT 機器への Telnet を用いたサイバー攻撃の分析，コンピュータセキュリティシンポジウム 2016 論文集，pp.870–877 (2016).

[10] 寺田真敏ほか：DoS 攻撃：1. DoS/DDoS 攻撃とは，情報処理，Vol.54, No.5, pp.428–435 (2013).
[11] ESET：Linux IoT デバイスを狙う「Mirai」ボットネットの拡散と DDoS 攻撃に注意，入手先 ⟨https://eset-info.canon-its.jp/malware_info/news/detail/161006.html⟩（参照 2017-07-21）.
[12] IoT 機器を狙う「Mirai」やその亜種の感染を目的とするアクセスが増加（警察庁），入手先 ⟨https://scan.netsecurity.ne.jp/article/2017/01/23/39367.html⟩（参照 2017-07-21）.
[13] Debian - ユニバーサルオペレーティングシステム，入手先 ⟨https://www.debian.org/index.ja.html⟩（参照 2017-07-21）.
[14] The netfilter.org “iptables” project, available from ⟨http://www.netfilter.org/projects/iptables/index.html⟩ (accessed 2017-07-21).
[15] python, available from ⟨https://www.python.org/about/⟩ (accessed 2017-07-21).
[16] Dr.WEB, 入手先 ⟨https://www.drweb.co.jp/⟩（参照 2017-07-25）.
[17] DNSDB, available from ⟨https://api.dnsdb.info/⟩ (accessed 2017-07-28).
[18] GeoIP, available from ⟨http://dev.maxmind.com/geoip/legacy/geolite/⟩ (accessed 2017-07-28).
[19] Inoue, D. et al.: Automated malware analysis system and its sandbox for revealing malware’s internal and external activities, *IEICE Trans. Information and Systems*, Vol.92, No.5, pp.945–954 (2009).
[20] Bayer, U. et al.: Dynamic analysis of malicious code, *Journal in Computer Virology*, Vol.2, No.1, pp.67–77 (2006).
[21] Willems, C. et al.: Toward automated dynamic malware analysis using cwsandbox, *IEEE Security & Privacy*, Vol.5, No.2 (2007).
[22] Bayer, U. et al.: Ttanalyze: A tool for analyzing malware, *Proc. 15th European Institute for Computer Antivirus Research* (*EICAR 2006*) *Annual Conference*, Vol.4 (2006).
[23] Norman Sandbox, available from ⟨http://www.norman.com/en-ww/homepage⟩ (accessed 2017-07-28).
[24] 鉄 穎ほか：マルウェアのポート待ち受け状態を考慮した並列動的解析環境のネットワーク制御，コンピュータセキュリティシンポジウム 2013 論文集，pp.761–768 (2013).
[25] 鉄 穎ほか：多数のマルウェア検体を並列解析可能な動的解析システムの提案，コンピュータセキュリティシンポジウム 2012 論文集，pp.728–735 (2012).
[26] Lin, Y. et al.: Secure and transparent network traffic replay, redirect, and relay in a dynamic malware analysis environment, *Security and Communication Networks*, Vol.7, No.3, pp.626–640 (2014).
[27] Angrishi, K.: Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets, arXiv preprint arXiv:1702.03681 (2017).
[28] Hoque, N., Bhattacharyya, K.D. and Kalita, J.K.: Botnet in DDoS attacks: Trends and challenges, *IEEE Communications Surveys & Tutorials*, Vol.17, No.4, pp.2242–2270 (2015).
[29] Zargar, S.T. et al.: A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, *IEEE Communications Surveys & Tutorials*, Vol.15, No.4, pp.2046–2069 (2013).
[30] de Santanna, J.J.C. et al.: Booters: An analysis of DDoS-as-a-service attacks, *2015 IFIP/IEEE International Symposium Integrated Network Management* (*IM*) (2015).
[31] Arne, W. et al.: On Measuring the Impact of DDoS Botnets, *7th European Workshop on Systems Security* (*EuroSec 2014*) (2014).
[32] サンドボックスとは，入手先 ⟨http://blogs.mcafee.jp/mcafeeblog/2015/07/6-5b8c.html⟩（参照 2017-08-09）.
[33] IP2LOCATION, available from ⟨https://www.ip2location.com/⟩ (accessed 2017-08-13).
[34] Inocencio, R.: BASHLITE Affects Devices Running on BusyBox, available from ⟨http://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-affects-devices-running-on-busybox/⟩ (accessed 2017-11-21).
[35] IIJ-SECT：Hajime, Mirai による通信の推移，入手先 ⟨https://sect.iij.ad.jp/d/2017/09/072602.html⟩（参照 2017-11-22）.

付　　録

A.1 長期解析マルウェアの情報

マルウェアID	MD5ハッシュコード
malware00	ec1263f9ba78d57e6f50292a8fb059c9
malware01	15c670e40c2ce79a6180c665ec7ab1f3
malware02	t32b314a2020b8c06ba22516d0823d196
malware03	t390b5484016253705df99d8f08adbd27
malware04	t454bc356ce47540eabf1c9abccc28568
malware05	t681f9c51578a539f868422a5900b409f
malware06	t7271c3f35f40d8f094a26d0bc2cbce08
malware07	t8868097ec9b409df5fbd61b94841dc42
malware08	t8d27e525f145ab2a2f3a4e057e97a7a8
malware09	t9d4eeeee151606f6d978e7a150f8ead9
malware10	tb512fd404ad2975612789ae38199550b
malware11	tdd5a884e28240096f3c74925f848c3da
malware12	1eb39c658f8c23585be6c3d361e6f831
malware13	340505202503fc5841d6331a98ad8267
malware14	53345fbc16926b453bef41c512ea81ad
malware15	0351c3fd16f8094cf71d84d3dc142dcd
malware16	25a39027667c33dca1b21eb6f03ef6ac
malware17	260decfec629b2b7a48a8e34de318719
malware18	56d447b0e83d4069134cb0451393c3ba

A.2 DoS 攻撃流量測定用のマルウェア情報

機種	攻撃使用プロトコル	マルウェアMD5ハッシュコード
Wi-Fi ストレージ1 Wi-Fi ストレージ2	TCP	b66d2425ea49f73c9d09f8999c26c93c
	UDP	63d21ed68531897db97772b49d58e3e7
ルータ	TCP	3c9970cd70fdb040871e676659ead12c
	UDP	d994a13b3911750d2ce17f6e2b19b3ea
IPカメラ	TCP	719109c1f6f88770989ada25e0e4ef8f
	UDP	74300f8b8d20be96df1d0705d678f45a

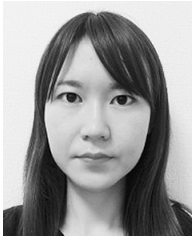
A.3 DDoS 攻撃対象および DNSDB の検索結果

攻撃対象は一部の文字列をマクス化した.

DDos攻撃対象	攻撃ポート	DNSDB検索結果
XXX.136.122.253	80/UDP	-
XXX.54.77.255	80/UDP	-
XXX.61.111.248	80/UDP	-
XXX.141.4.82	53/UDP	-
XXX.59.190.144	80/TCP	bXXXXXXXXe.evobinary.com.
XXX.56.107.124	80/TCP	cXXXXXXc.com.
XXX.58.22.140	80, 8080/UDP	mXXXXXXe.ddns.net.
XXX.216.133.244	3074/UDP	-
XXX.106.116.166	80/UDP	dXXXXXd.bluematt.me
XXX.62.189.139	80, 20480/UDP	bXXXXXXs-fun.com
XXX.146.44.1	80, 53/UDP	nX1.taintedgamers.org
XXX.141.60.28	53/UDP	iXXXXb.biz
XXX.240.01.234	80/UDP	-
XXX.4.153.169	80/UDP	Xe-self006.nos-avg.cz
XXX.125.252.66	80/UDP	nXXXXXXXXe.nl.
XXX.232.96.203	80/UDP	-
XXX.101.121.210	80/TCP	-
XXX.113.230.121	58619/UDP	-
XXX.187.74.211	28416, 5632/UDP 80/TCP	mXXXXXXXXp.com.
XXX.36.116.45	53/UDP	aXi.scoutadvisor.com.
XXX.142.151.113	80/UDP	-
XXX.40.162.28	80/TCP	ip-XXX-40-162-28.ip.secureserver.net
XXX.101.1.144	80/TCP	eXXXXXXXXXs.com.
XXX.166.138.130	20480/UDP	pXXXXXXXXXXXXXXXXXXXs.com.
XXX.4.207.99	80/TCP	cXXXXXXc.com.
XXX.7.70.244	20480/UDP	tXXXXXXg.com
XXX.11.231.68	3074/UDP	-
XXX.200.57.102	3074/UDP	-
XXX.52.63.214	20480/UDP	-
XXX.96.81.69	80/UDP	nXXXXXXXXXXXXXXXXXXXXa.gen.antigen.ru.
XXX.118.26.240	80/UDP	dXXXXc.us
XXX.74.76.184	80/UDP	-
XXX.92.134.233	80/UDP	-
XXX.14.101.150	80/UDP	-
XXX.161.88.229	80/TCP	-
XXX.58.159.73	53, 1618/UDP	-
XXX.57.237.201	524/UDP	-
XXX.91.119.239	3074/UDP	c-XXX-91-119-239.premium-chicago.nfoservers.com.
XXX.91.121.234	60144/TCP	v-XXX-91-121-234.managed-vds.internap-atlanta.nfoservers.com
XXX.193.229.41	3074/UDP	-
XXX.177.199.19	20480/UDP 80/TCP	rXXXXXXXXXs.tk
XXX.215.60.234	20480/UDP	rXXXXXXXXy.sologigabit.com.
XXX.89.125.193	80/UDP	-
XXX.18.16.98	53, 3074/UDP	-
fXXXXXXXXi.ru	80, 443/TCP	
jXXXXXl.com	443/TCP	
pXXXXXXXXXg.net	80/TCP	
www.hXXXXXXXXXXXXXXt.com	80/TCP	

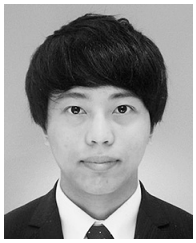
鉄 穎 （学生会員）

2014 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前期修了．修士（情報学）．同年 4 月同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に進学．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．



楊 笛

2015 年 10 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前期に進学．情報セキュリティ，特に DDoS 攻撃の観測・分析の研究に従事．



保泉 拓哉

2017 年 4 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前期に進学．情報セキュリティ，特に DDoS 攻撃の観測・分析の研究に従事．

中山 颯

2016 年横浜国立大学卒業．学士（工学）．同年 4 月同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前期に進学．情報セキュリティ，特に IoT 機器に対する攻撃の観測・分析の研究に従事．

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で研究員として勤務．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），2016 年産学官連携功労者表彰総務大臣賞，2017 年情報セキュリティ文化賞をそれぞれ受賞．

松本 勉 （正会員）

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（IAS-YNU）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，耐タンパー技術，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）各受賞．