Vol.2018-DPS-174 No.4
Vol.2018-CSEC-80 No.4
2018/3/5

IoTマルウェアサイバー攻撃インフラのアクティブ調査

高田 一樹[1,2,a)]　鉄　穎[1]　岡田 晃市郎[2]　吉岡 克成[3]　松本 勉[3]

概要：近年，IoT 機器を狙ったサイバー攻撃が社会問題となっている．特に，Mirai に代表される IoT 機器を狙ったマルウェアを用いた攻撃があり，大きな脅威となっている．IoT マルウェアに対する対策として，IoT 機器を模したハニーポットによる攻撃の実態調査や IoT 機器自体の脆弱性調査，堅牢化等多くの研究が行われている．一方で，IoT マルウェアを制御するサイバー攻撃インフラに関しては，明らかにされていない．IoT マルウェアの対策を行う上で，攻撃に用いられるサイバー攻撃基盤の実態を明らかにすることは必要不可欠であると考える．本研究では，IoT 機器を模したハニーポットと連動し，ハニーポットにより収集された IoT マルウェアのサイバー攻撃インフラである C&C サーバのアクティブ調査を行うためのシステム構築を行った．また，構築したシステムにより収集された情報の分析を実施した．

キーワード：IoT，マルウェア，C&C サーバ，ネットワークスキャン

Survey of Cyberattack Infrastructure used by IoT Malware.

Kazuki Takada[1,2,a)]　Ying Tie[1]　Koichiro Okada[2]　Katsunari Yoshioka[3]
Tsutomu Matsumoto[3]

Abstract: In late years, Cyberattack toward IoT devices is social problem. Particularly, Cyberattack using the malware toward IoT devices represented by Mirai is a big threat. As measures against IoT malware, threre are many researches such as surveying the actual situation of attack using honeypot simulating IoT device, vulnerability investigation and hardening of IoT device itself. The other hand, About cyberattack infrastructure for control of the IoT malware is not revealed enough. In order to measures against IoT malware, it is necessary to survey and reveal the infrastructure used for IoT malware. In this research, we constructed survey system of the C&C server that link with honeypot simulating IoT device. Then we analyzed the data from our survey system.

Keywords: IoT, Malware, C&C Server, Network Scan

1. はじめに

近年，サイバー攻撃が増大しており，攻撃方法や攻撃対象は多岐に渡っている．

中でも，IoT 機器を標的としたサイバー攻撃があり，Mirai などのマルウェアに感染した IoT 機器によって，大規模 DDoS 攻撃が引き起こされるなど社会問題となっている [1]．IoT の普及が進む中，IoT 機器に対するサイバー攻撃は今後も増加することが想定される．IoT 機器のセキュリティ強化は急務であり，IoT 機器を模したハニーポットの開発やそれを用いた攻撃の分析 [2][3]，IoT 機器の脆弱性調査や製造段階での堅牢化 [4][5] など国内においても様々なセキュリティ対策の取り組みが進められている．しかし，IoT 機器へのサイバー攻撃に関しては，明らかになっ

[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, Yokohama, Kanagawa 240-8501, Japan
[2] 株式会社セキュアブレイン
SecureBrain Corporation, Chiyoda, Tokyo 102-0094, Japan
[3] 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, Yokohama National University / Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240-8501, Japan
[a)] takada-kazuki-hw@ynu.jp

ていないことが多く，IoT 機器へのサイバー攻撃の実態を調査する研究が盛んに行われている．我々は，IoT 機器に感染をするマルウェアに対策するために，攻撃の根本となるサイバー攻撃基盤を明らかにする必要があると考える．

本研究では，IoT 機器を模したハニーポットシステムである IoTPOT[2] と連動し，ハニーポットシステムで収集されたマルウェアが通信を行う C&C サーバに対して，ネットワークスキャンを用いたアクティブ調査を行うシステムを構築した．本稿では，この調査システムについて概説する．また，調査の結果明らかになった C&C サーバの実態について報告する．

本稿の構成は，以下の通りである．まず，2 章で，関連研究について記述する．3 章で，アクティブ調査システムおよび調査方法について記述する．4 章で，アクティブ調査結果について記述する．5 章で，調査結果の考察を記述する．最後に 6 章でまとめと今後の課題について記述する．

2. 関連研究

関連研究として，IoT 機器の脆弱性に関する調査を行った Cui らの研究 [6] および森らの研究 [7] がある．[6] では，広域なネットワークスキャンにより，インターネット上に存在する脆弱な機器の存在を明らかにした．[7] では，IoTPOT による受動的調査結果とネットワークスキャンによる調査を組み合わせることで脆弱な IoT 機器を特定することを可能としている．笠間らの研究 [8] では，ダークネットで観測された通信の中で通信元が Windows PC 以外であるものに対しアクティブ調査を行うことで感染 IoT 機器の分類を試みている．

これらの研究では，攻撃対象とされる IoT 機器を特定するためにアクティブ調査を行っている．我々の調査はサイバー攻撃基盤を調査対象としており，目的が異なっている．

伊藤らの研究 [9] では，IoT 向けプロトコルである MQTT を用いたハニーポットの検討を行っている．荒木らの研究 [10] では，トラフィックデータから Mirai 等のボットによるスキャンやブルートフォース活動を分類する手法が提案されている．これらの研究は，IoT 機器に感染するマルウェアの実態を明らかにすることを目的としているが，マルウェア本体や感染ホストの特定が主たる目的であり，サイバー攻撃基盤に着目した研究ではない．

PC に感染するマルウェアの C&C サーバを特定する手法として，久山らの研究 [11] がある．[11] では，DNS 情報等を用いることで攻撃者に検知されることなく，APT 攻撃に用いられる C&C サーバを特定する手法が提案されている．本研究も C&C サーバを特定することを最終的な目的とするが，IoT マルウェアの C&C サーバは，どの様な特徴を持つかが不明確である．また，IP アドレスのみで通信するものも多く確認されている．このことから IoT マルウェアの C&C サーバの特定手法については，C&C サーバを特定するための特徴を調査する必要がある．

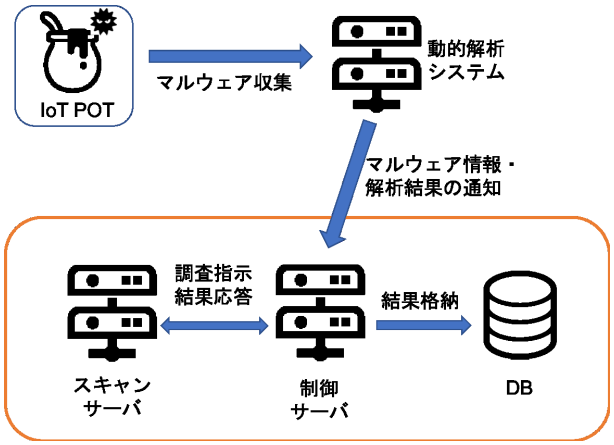

図 1　システム概要図

ネットワークスキャンを用いたアクティブ調査には，広域のネットワークスキャン結果を公開するサービスとして，Shodan[12]，Censys[13] がある．これらのサービスは非常に有用であるが，スキャンの対象およびタイミングがサービスの運用に依存してしまう．このため，必要な情報の不足や動的 IP アドレス割当による変化を排除することが難しい．このため，本稿のアクティブ調査システムを構築した．

3. アクティブ調査システム

本研究で構築したアクティブ調査システムについて述べる．システムの概要を**図 1** に示す．図 1 の枠線内が本研究で構築したシステムである．IoTPOT への攻撃通信から IoT マルウェアを収集し，即時に動的解析を行うシステムと連携して，解析結果から収集した C&C サーバ IP アドレスに対して，ネットワークスキャンを行うシステムを構築した．なお，調査システムと連携する動的解析システムは，MIPS および MIPSEL 系の CPU アーキテクチャで動作するマルウェアの動的解析を行う．

本調査システムにおける調査フローを**図 2** に示す．アクティブ調査の対象となる C&C サーバの IP アドレス情報は，以下の 2 種類である．

(1) 入力 1: マルウェア本体から strings コマンドにより，抽出した C&C サーバ IP アドレス情報およびシェルコード等のダウンロードコマンド内の IP アドレス情報
(2) 入力 2: 動的解析結果のパケットキャプチャデータの通信先情報およびペイロードを分析し抽出した C&C サーバ IP アドレス情報

入力 1，2 のどちらかが得られた段階でアクティブ調査が行われる．アクティブ調査は，masscan[14]，nmap[15] の 2 種類のスキャンツールを併用して実施する．IP アドレスが得られると masscan により，開放されているポートの調査を実施する．続いて，masscan で得られた開放ポートに

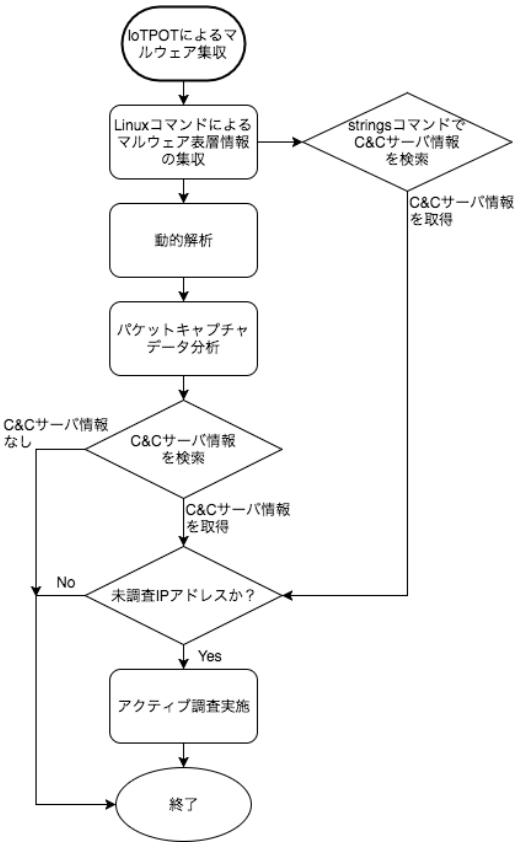

図 2　アクティブ調査フロー

表 1　アクティブ調査概要

観測期間	2017/10/25 - 2018/01/07
対象検体数	994
有効調査対象 IP アドレス数	200

対して，nmap を用いて各ポートのサービス情報や機器，OS の調査を実施する．同時に GeoIP 情報を収集する．なお，本調査システムでは，同一 IP アドレスに対しては 1 度のみ調査を行う設計となっている．また，参考情報としてアクティブ調査実施時点の Shodan，Censys の結果を収集する．

4. 調査結果

本調査システムによる調査結果について述べる．

4.1 調査概要

調査の概要を**表 1** に示す．約 2 ヶ月半の調査期間中に動的解析の対象となったマルウェアの総数は，2610 検体であった．そのうち，入力 1，2 の双方または，どちらか一方の C&C サーバ IP アドレス情報が取得できた 994 検体をアクティブ調査の対象としている．また，調査対象 IP 数は，入力 1，2 で得られたユニークな 223 個の IP アドレスのうち，ネットワークスキャンに応答のあった 200 個の IP アドレスを有効な調査対象 IP アドレス（以下，有効調査対象 IP アドレス）としている．

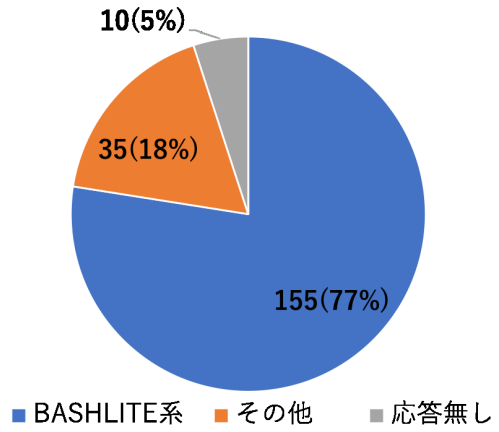

図 3　対象データの分類

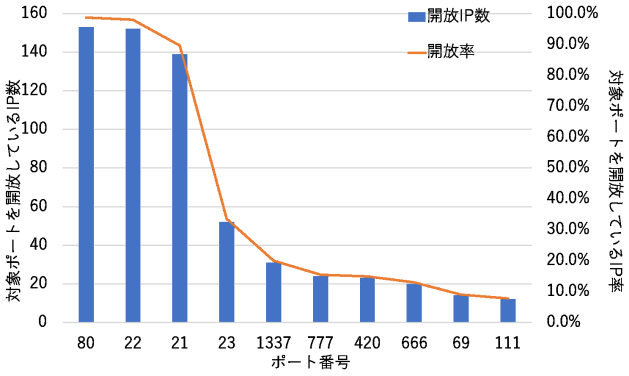

図 4　BASHLITE 系 C&C サーバで開放されている上位 10 ポート

4.2 対象データの分類

アクティブ調査結果のうち nmap を用いたポートスキャンの結果に着目して，有効調査対象 IP アドレスを分類する．BASHLITE 系マルウェアの C&C サーバは，“PING”，“SCANNER ON” 等のコマンド文字列を送信する．サーバの応答にこれらの文字列を含む調査結果のペイロードが存在した．nmap の調査結果から IP アドレスを分類した結果を**図 3** に示す．この結果から有効調査対象 IP アドレス中，77%の 155 個の IP アドレスが BASHLITE 系マルウェアの C&C サーバ（以下，BASHLITE 系 C&C サーバ）であることが分かる．

4.3 開放ポート

BASHLITE 系 C&C サーバである 155 個の IP アドレスにおいて開放されているポート番号の調査結果について述べる．これらの IP アドレスにおいて開放されていたポート番号のうち多くの IP アドレスで開放されていた上位 10 ポートをまとめた結果を**図 4** に示す．この結果から，上位 3 ポートが非常に多くの C&C サーバで開放されていることが分かる．上位 3 ポートの詳細は，80 番が 98.7%，22 番が 98.1%，21 番が 89.7%であった．次節以降に，この上位 3 ポートの調査結果について述べる．

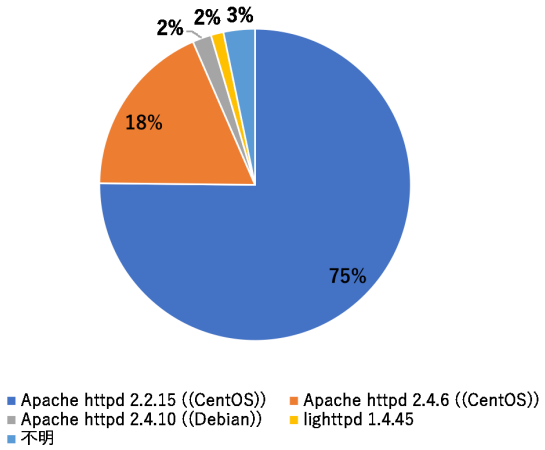

図 5　80 番ポートで公開されているサービスの割合

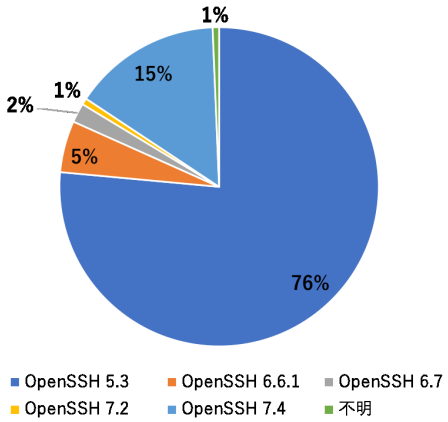

図 6　22 番ポートで公開されているサービスの割合

4.3.1　80 番ポート

BASHLITE 系 C&C サーバで開放されていた 80 番ポートの分析結果について述べる．80 番ポートが開放されていた C&C サーバは，98.7%でほぼ全ての C&C サーバで開放されていた．80 番ポートで公開されているサービスの調査結果を図 **5** に示す．この結果からサービス情報が取得できた 97%の C&C サーバ全てで HTTP サービスが提供されていることが分かる．このことから，BASHLITE 系 C&C サーバでは，HTTP サービスが公開されていると考えられる．HTTP サービスは，マルウェア，ツール等のダウンロード元として利用されていると考えられる．また，BASHLITE 系マルウェアの本体内から strings コマンドで収集した文字列内に “wget” 等で HTTP サービスを指定しているものが存在していることを確認した．このことからも，HTTP サービスとマルウェアが連動していることが推定される．

HTTP サービスのバージョン情報を確認すると 95%の C&C サーバでは，Apache2 系のサービスが公開されていることが分かる．残り 2%の C&C サーバでは，lighttpd のサービスが公開されている．また，Apache2 系のサービス情報からホスト OS の情報を確認することが可能である．この結果から 93%が CentOS で構築されたサーバであることが分かる．なお，HTTP サービスを公開している複数の IP アドレスを抽出し Web アクセスを行ったところ TOP ページには，Apache のデフォルトページが公開されていることを確認した．このことから，通常の HTTP サービスを公開しているサーバを乗っ取り等で C&C サーバとして利用している可能性は低いと考えられる．

4.3.2　22 番ポート

BASHLITE 系 C&C サーバで開放されていた 22 番ポートの分析結果について述べる．22 番ポートが開放されていた C&C サーバは，98.1%でほぼ全ての C&C サーバで開放されていた．22 番ポートで公開されているサービスの調査結果を図 **6** に示す．この結果からサービス情報が取得できた 99%の C&C サーバ全てで SSH サービスが提供されていることが分かる．また，22 番ポート以外で SSH サービスが提供されている IP アドレスも存在していた．このことから，BASHLITE 系 C&C サーバでは，SSH サービスが公開されていると考えられる．SSH サービスは，サーバを遠隔操作するために用いられていると考えられる．

また，公開されている SSH サービスの Fingerprint 情報を収集した．この結果，Fingerprint が一致するサーバは存在しないことが分かった．このことから，1 つのサーバが IP アドレスの割当変更により，調査対象となっている様なケースは存在せず，IP アドレス毎にユニークなサーバが存在していると考えられる．

4.3.3　21 番ポート

BASHLITE 系 C&C サーバで開放されていた 21 番ポートの分析結果について述べる．21 番ポートは，89.7%の C&C サーバで開放されていた．21 番ポートで公開されているサービスの調査結果を図 **7** に示す．この結果からサービスが取得できた 99%の C&C サーバ全てで FTP サービスが提供されていることが分かる．BASHLITE 系 C&C サーバでは，FTP サービスが公開されていると考えられる．FTP サービスは，HTTP サービスと同様に，マルウェア，ツール等のダウンロード元として利用されていると考えられる．

21 番ポートが開放されていた 139 個の IP アドレス中，78.3%の 108 個の IP アドレスで “Anonymous” でログイン可能な状態であった．また，“Anonymous” でログイン可能なサーバのうち 77.7 %の 83 個の IP アドレスで，BASHLITE 系マルウェアの本体内から strings コマンドで収集した文字列に含まれる “ftpget” 等のファイル取得コマンドで指定された Shell スクリプトファイルが取得可能な状態であることを確認した．このことからも，FTP サービスとマルウェアが連動していることが推定される．また，FTP サービスで公開されているファイルリストは，ほぼ同一の

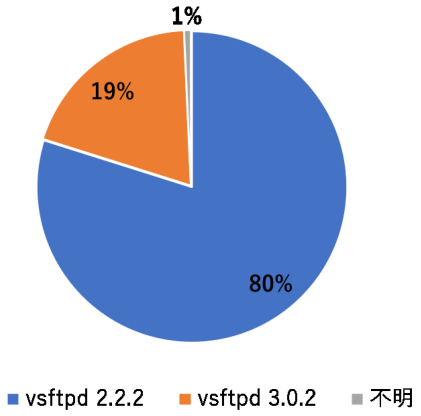

図 7　21 番ポートで公開されているサービスの割合

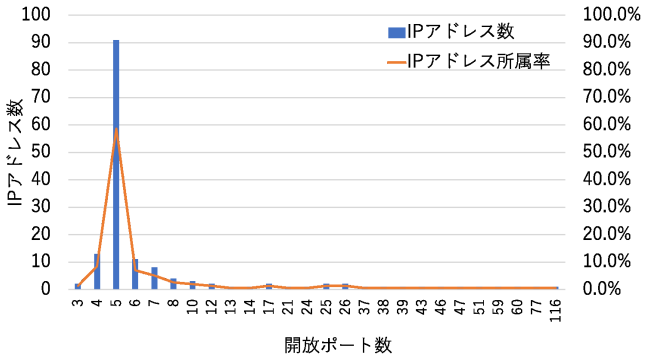

図 8　開放ポート数の分布

内容であるものが多数を占めていた．なお，BASHLITE 系 C&C サーバの特徴を持たない IP アドレスで公開されている FTP サービスにも同様のファイルを公開しているものが多数見られた．このことから，マルウェア，ツール等のダウンロード専用サーバが存在すると考えられる．

4.3.4　開放ポートの組み合わせ

BASHLITE 系 C&C サーバで開放されているポートの組み合わせについて述べる．BASHLITE 系 C&C サーバで開放されているポート数の調査結果を**図 8** に示す．この結果から開放ポート数 5 が最も多く，58.7%の C&C サーバで 5 ポートが開放されていた．また，開放ポート数 4〜7 に集中しており，79.5%の C&C サーバが開放ポート数 4〜7 であった．ポート（サービス）の組み合わせとしては，21 番 FTP，22 番 SSH，80 番 HTTP と C&C サーバの独自サービスと思われる 2 サービスの組み合わせが最多であった．C&C サーバの独自サービスと思われる 2 サービスは，以下の 2 サービスであった．

(1) コマンド発行: TCP アクセスで BASHLITE 系のコマンド応答を確認
(2) Shell のログイン画面と思われる応答: TCP アクセスで Shell 画面制御コード+Username，Password 等の文字列応答を確認

この結果から，BASHLITE 系 C&C サーバは，基本的に FTP，SSH，HTTP，コマンド発行，Shell 応答の 5 サービスを公開していると考えられる．

4.4　IP アドレス分析

有効調査対象 IP アドレスの分析結果について述べる．

4.4.1　設置国

有効調査対象 IP アドレスの設置国の分布を GeoIP 情報で調査した結果を**図 9** に示す．図 9 より，C&C サーバが最も多く設置されている国は US で，30%であった．2 番めに多い国は，IT で 20%であった．調査対象 IP アドレスのうち 50%がこの 2 カ国に存在していることが分かる．また，C&C サーバーの多くが欧州圏に存在していることが分かる．

4.4.2　上位 10 個の IP アドレス

調査期間中に実施した動的解析の結果から抽出された数が多い上位 10 個の IP アドレスの分析結果を**表 2** に示す．表 2 より，No.1 の 191.96.112.100 と通信をした検体が最も多く 78 検体存在していた．続いて，No.2 の 188.213.161.46 で 48 検体，No.3 の 80.211.133.73 で 21 検体となっており，No.1 の 191.96.112.100 と通信するマルウェアが突出して多いことが分かる．

開放ポートに着目すると，No.1 の 191.96.112.100 では 27 ポート，No.2 の 188.213.161.46 では 25 ポートと多くのポートが開放されている．しかし，いずれもサービスの公開が確認できたものは，FTP，SSH，HTTP，C&C サーバのコマンド発行，Shell 応答の 5 サービスであり，BASHLITE 系 C&C サーバの特徴に合致していることを確認した．また，No.3 の 80.211.133.73 で公開サービスが全て不明であったことを除くと，No.4〜No.10 までのいずれの IP アドレスでも同様に BASHLITE 系 C&C サーバの特徴に合致していた．なお，No.4 の 80.211.192.237 では，コマンド発行サービスが 2 ポート，Shell 応答が 2 ポートと複数のマルウェアを管理していると思われる特徴が見られた．また，No.10 の 94.177.230.28 では，BASHLITE 系 C&C サーバの特徴である 5 サービスに加えて，SSL/TSL，VPN のサービスが公開されていることを確認した．

設置国に着目すると，図 9 で最も多く見られた US に所属する IP アドレスは，表 2 には，含まれていなかった．また，IT に所属する IP アドレスが 4 個，NL に所属する IP アドレスが 3 個，他 1 カ国づつ 3 個の IP アドレスという結果であった．図 9 から，IT，NL は，US に次いで C&C サーバ数が多い．これは，US には C&C サーバは多数存在するが，各サーバに所属するマルウェア数は少なく，IT，NL の各国には，設置された C&C サーバ数および各サーバに所属するマルウェア数が共に多いと考えられる．

4.4.3　生存期間の推定

C&C サーバの生存期間を推定する．本調査では，IP ア

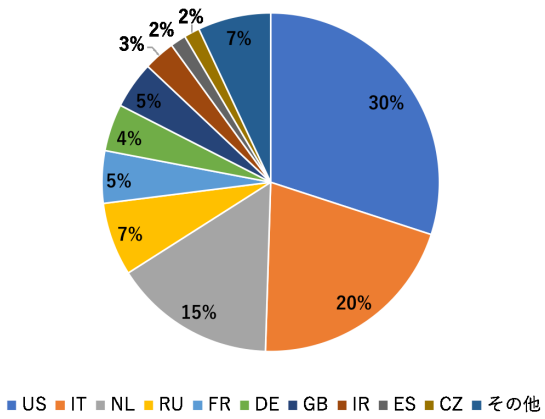

図 9　C&C サーバ設置国の分布

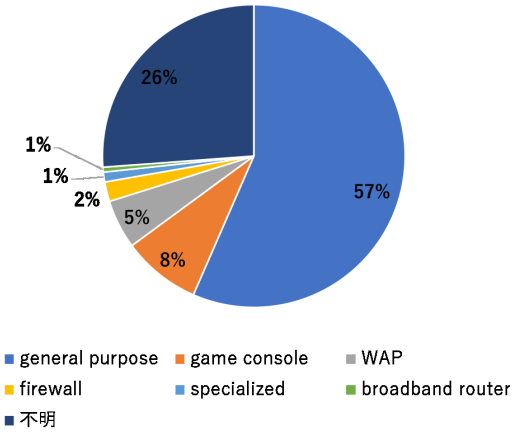

図 10　C&C サーバの機器推定結果

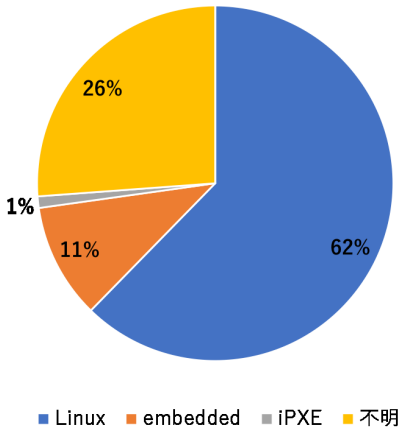

図 11　C&C サーバの OS 推定

ドレスが入力として得られた初回のみアクティブ調査を実施する設計となっているため C&C サーバの生存期間は不明である．そこで，入力として IP アドレスが得られた初回の日時と調査期間内で最後に同一 IP アドレスが得られた日時の期間は，該当 IP アドレスが C&C サーバとして稼働していたものとして生存期間を推定する．表 2 から最も多くの検体が所属する No.1 の 191.96.112.100 では，生存期間は 5 日間であった．これに対し，最も生存期間が長かったのは No.5 の 191.96.112.115 で，27 日間であった．また，**表 3** に推定生存期間の長い上位 10 個の IP アドレスを示す．表 3 では，表 2 に存在しない 4 個の IP アドレスが入っている．これらの結果から，C&C サーバに所属するマルウェアの数と生存期間の長さには相関は見られなかった．また，表 3 にも US に所属する IP アドレスは確認されなかった．一方で，IT，NL に所属する IP アドレスは，それぞれ IT が 2 個，NL が 4 個，含まれていた．このことから，IT，NL に設置された C&C サーバは生存期間が長いものが多い可能性が高い．

4.5　C&C サーバを構成する機器，OS の推定

C&C サーバを構成する機器，OS の推定結果について述べる．**図 10** に機器推定，**図 11** に OS 推定の結果を示す．

機器推定では，図 10 の結果から game console，WAP 等，多数の機器の可能性が推定されている．しかし，general purpose が 57%，機器不明が 26%となっており，どの様な機器であるかが不明であるものが 80%を超える結果であった．

OS 推定では，図 11 の結果から 62%が Linux 系 OS，11%が組込機器の可能性が推定されていた．また，26%が OS 不明と言う結果であった．

4.3.1 の結果では，CentOS で構築されるサーバが多いことを示していた．このことから，OS 推定の結果，Linux 系 OS が多い傾向であることは 4.3.1 の結果と類似しており，Linux 系 OS が多数使用されていることが分かる．

しかし，機器推定の結果では，機器の種類が特定できていないものが多く，OS 推定でも不明なものが多く，いずれの結果も十分な精度が出ているとは言い難い結果である．このため，機器，OS の推定手法は改善する必要があると考える．

5.　考察

本調査の結果から BASHLITE 系 C&C サーバの特徴を明らかにした．BASHLITE 系 C&C サーバでは，FTP，SSH，HTTP，コマンド発行，Shell 応答（ログイン画面）の 5 サービスを公開する特徴を有していることが明らかになった．また，BASHLITE 系 C&C サーバでは，nmap によるサービス調査や TCP コネクションのみでコマンド発行等の特徴通信を確認することが可能であることが判明した．

BASHLITE 系 C&C サーバ設置国の調査結果から，C&C サーバは，US および欧州圏に多くが存在していると考えられる．また，攻撃活動が活発な C&C サーバは欧州圏に多く存在すると考えられる．

表 2　動的解析結果に多く含まれた IP アドレス 上位 10IP

No	IP アドレス	解析数	開放ポート数	確認されたサービス	国名コード	推定生存期間（日）
1	191.96.112.100	78	27	FTP, SSH, HTTP, C&C, Shell 応答	NL	5
2	188.213.161.46	48	25	FTP, SSH, HTTP, C&C, Shell 応答	IT	7
3	80.211.133.73	21	16	全て不明	IT	2
4	80.211.192.237	11	7	FTP, SSH, HTTP, C&C × 2, Shell 応答× 2	CZ	9
5	191.96.112.115	10	5	FTP, SSH,HTTP, C&C, Shell 応答	NL	27
6	94.177.218.37	10	5	FTP, SSH,HTTP, C&C, Shell 応答	IT	2
7	185.148.39.193	8	5	FTP, SSH,HTTP, C&C, Shell 応答	RU	21
8	94.177.218.245	8	5	FTP, SSH,HTTP, C&C, Shell 応答	IT	13
9	191.96.112.120	8	5	FTP, SSH,HTTP, C&C, Shell 応答	NL	9
10	94.177.230.28	7	7	FTP, SSH, HTTP, SSL/TSL, C&C, VPN, Shell 応答	DE	9

表 3　推定生存期間が長い IP アドレス 上位 10IP

IP アドレス	解析数	国名コード	推定生存期間（日）
191.96.112.115	10	NL	27
185.148.39.193	8	RU	21
80.211.153.181	4	IT	14
94.177.218.245	8	IT	13
191.96.112.113	5	NL	13
191.96.112.108	6	NL	11
185.165.29.77	4	IR	11
80.211.192.237	11	CZ	9
191.96.112.120	8	NL	9
94.177.230.28	7	DE	9

機器，OS 推定の結果から，BASHLITE 系 C&C サーバの多くは，Linux 系 OS，特に CentOS で構築されていることが考えられる．しかし，機器，OS 推定は nmap による調査だけでは精度が不十分であり，調査手法を検討する必要がある．

今回の調査では，IP アドレスの所属する AS 等の情報について明らかになっていない．調査済の IP アドレスに対し，追加調査を行う必要がある．

6. まとめと今後の課題

本稿では，IoTPOT による受動的調査と連携して，稼働中の C&C サーバを即時に調査可能なアクティブ調査システムを構築し，調査した結果について報告した．本調査では，BASHLITE 系 C&C サーバについて公開されているサービスの特徴および設置地域の分布について明らかにした．また，BASHLITE 系 C&C サーバは，特殊なプロトコルを用いずに nmap や TCP コネクションのみで検出可能であることが判明した．

今後の課題として，今回の調査結果で得られた IP アドレスの詳細な AS 情報等の追加調査を実施し，BASHLITE 系 C&C サーバが AS や IP レンジにどの様に分布するかを分析する．分析の結果に基づき被疑 IP アドレス帯から BASHLITE 系 C&C サーバを検出するプロービングシステムを検討する．また，現在のパケットキャプチャデータ分析手法では，BASHLITE 系 C&C サーバ以外の IP アドレスが収集できない可能性が高いため分析の精度を改善し，調査対象のマルウェアを増やす必要がある．加えて，収集可能なマルウェアの種類を増加させるために IoTPOT の機能改良を進める．また，機器，OS の推定精度が低いため推定手法を検討し，精度向上を図り C&C サーバの詳細な実態を把握する．

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．

参考文献

[1] @IT: DNS サービス「Dyn」への大規模 DDoS 攻撃、発信源は 10 万台の IoT 機器，（オンライン），入手先 ⟨http://itpro.nikkeibp.co.jp/atcl/idg/14/481542/102800290/⟩（参照 2018-01-20）．

[2] Yin, Minn Pa, P., Shogo, S., Katsunari, Y., Tsutomu, M., Takahiro, K. and Christian, R.: IoTPOT: A Novel Honeypot for Revealing Current IoT Threats, 情報処理学会論文誌， Vol. 57, No. 4 (2016).

[3] 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).

[4] 総務省：IoT 機器に関する脆弱性調査等の実施，（オンライン），入手先 ⟨http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_04000088.html⟩（参照 2018-01-20）．

[5] 情報処理推進機構：IoT のセキュリティ，（オンライン），入手先 ⟨https://www.ipa.go.jp/security/iot/index.html⟩（参照 2018-01-27）．

[6] Cui, A. and Stolfo, S. J.: A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-area Scan, *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC '10, pp. 97–106 (2010).

[7] 森博志，　鉄穎，小山大良，　藤田彬，吉岡克成，　松本勉：能動的観測と受動的観測による IoT 機器のセキュリティ状況の把握，技術報告 27 (2017).

[8] 笠間貴弘，井上大介：大規模ダークネット観測と能動的スキャンによるマルウェア感染 IoT 機器の分類，情報処理学会論文誌，Vol. 58, No. 9, pp. 1388–1398 (2017).

[9] 伊藤克恭，長谷川皓一，山口由紀子，　嶋田創：IoT 向けプロトコル用ハニーポットの初期検討，電子情報通信学会技術研究報告 Vol.116 No.522，pp. 103–108 (2017).

[10] 荒木翔平，　胡博，永渕幸雄，小山高明，　三好潤，嶋田創，高倉弘喜：ボットによるスキャン及びブルートフォース活動のクラスタリング手法，電子情報通信学会技術研究報告 Vol.116 No.522，pp. 1–6 (2017).

[11] 久山真宏，柿崎淑郎，佐々木良一：攻撃者に察知されにくい情報を用いた C&C サーバの検知手法の提案と評価，情報処理学会論文誌，Vol. 58, No. 9, pp. 1410–1418 (2017).
[12] Censys: (online), available from ⟨https://censys.io/⟩ (accessed 2018-01-22).
[13] Shodan: (online), available from ⟨https://www.shodan.io/⟩ (accessed 2018-01-22).
[14] Graham, R.: MASSCAN: Mass IP port scanner, (online), available from ⟨https://github.com/robertdavidgraham/masscan⟩ (accessed 2018-01-23).
[15] nmap: (online), available from ⟨https://nmap.org/⟩ (accessed 2018-01-23).